2 Classics Edition

About This Chapter

The windows layout of the web system of the classics edition is based on the refined and comprehensive web network management functions it provides.

2.1 Obtaining Technical Support
2.2 Product Function Overview
2.3 Switching from the Web System to the CLI
2.4 Precautions for Using the Web Platform
2.5 Logging In to the Web System
2.6 Help and Version of the Web Platform
2.7 Switching the WLAN Mode
2.8 Initial Configuration of the Web Platform
2.9 Device Information
2.10 Configuration Wizard
2.11 LAN Access
2.12 WAN Access
2.13 WLAN AC
2.14 IP Services
2.15 Security
2.16 QoS
2.17 VPN
2.18 Voice Management
2.19 System Management

 Copyright © Huawei Technologies Co., Ltd.

2.20 User Management

2.1 Obtaining Technical Support

If you fail to locate or rectify the faults encountered during maintenance or troubleshooting by following instructions in this document, use the following methods to obtain technical support:

- Contact the technical support personnel in Huawei's local office.

  NOTE

  For contact information about local offices, access **https://support.huawei.com/enterprise**.

- To view technical documents on Huawei enterprise service technical support website, access **https://support.huawei.com/enterprise**.

2.2 Product Function Overview

The web platform provides various functions.

- Flexible local area network (LAN) access, implementing secure isolation among LANs.

  You can quickly construct LANs on a network without changing hardware or communication cables. You can use a station (STA) to connect to a LAN over a wireless local area network (WLAN). No network cable is required between the STA and the LAN, which is a great advantage when cabling is restricted. You can also configure different WLANs, access rights, and security mechanisms for different departments. For example, configure a dedicated WLAN name for visitors.

- Diversified wide area network (WAN) functions and flexible access authentication methods.

  You can access the Internet through uplink interfaces, including Ethernet interfaces, digital subscriber line (DSL) interfaces, and 3G interfaces. After accessing the Internet, you can chat online, receive and send emails, and obtain required information.

- Rich IP services, ensuring transmission of enterprise service data.

  IP services include Dynamic Host Configuration Protocol (DHCP) server, DHCP relay, Network Address Translation (NAT), domain name system (DNS) dynamic domain resolution, IP accounting, and route querying. These IP services facilitate user communication.

- Comprehensive security mechanisms, ensuring security of the enterprise intranet.

  Security mechanisms include access control list (ACL), firewall, security protection, Secure Sockets Layer (SSL), public key infrastructure (PKI), Authentication, Authorization and Accounting (AAA) and network behavior management. These mechanisms ensure user access security.

- Quality of service (QoS), managing traffic, limiting the traffic rate on interfaces, and allowing high-priority services to be transmitted first.

 Copyright © Huawei Technologies Co., Ltd.

- Virtual private network (VPN), ensuring secure data transmission.

  VPNs ensure security of data transmission between the enterprise intranet and remote users, enterprise branches, commercial partners, or suppliers. The web platform supports VPN functions including Internet Protocol Security (IPSec) and Layer 2 Tunneling Protocol (L2TP).
- Basic IPPBX services, providing basic voice services for enterprises.

  Basic IPPBX services include the incoming call service, outgoing call service, and short number dialing, which save voice communication costs.
- Supplementary IPPBX services, providing supplementary voice services for enterprises.

  Supplementary IPPBX services include interactive voice response (IVR), calling number restriction, and ringback tone (RBT), which enrich communication methods for enterprises.
- System Management services, supporting device reboot, upgrade, patch installation, factory settings restoration, and so on.
- User Management services, providing services for an administrator to create, modify, and delete local users.

2.3 Switching from the Web System to the CLI

Prerequisites

- The PuTTY software must be loaded, and you can only switch from the web platform to the CLI through the Internet Explorer.

  When you use the Internet Explorer to switch from the web platform to the CLI for the first time, a dialog box will be displayed. In the displayed dialog box, click **Download the Telnet client** to download the **putty.exe** file. After downloading the file, click **Configure the path** in the displayed dialog box and select the downloaded **putty.exe** file. Then click **OK** in the displayed dialog box. Click **CLI** in the lower right corner to switch to the CLI.
- If the Internet Explorer is used, the security level must be set to **Low**.

  Open the Internet Explorer, choose **Tools** > **Internet Options** > **Security**. Choose **Internet** and click **Custom level**. Click **Enable** under **Initialize and script ActiveX controls not marked as safe**, **Script ActiveX controls marked safe for scripting***, **Run ActiveX controls and plug-ins**, and **Active scripting**. Choose **Local intranet** and **Trusted sites**, and set the security levels of both zones to **Low**. The Internet Explorer 8.0 is used in the preceding example.

  NOTE

  If the CLI cannot be accessed after the security level of the Internet Explorer is set to **Low**, refresh or restart the Internet Explorer and perform the switching again.
- When switching from the web platform to the CLI, note the following:

  a. You must log in to the web platform as a user with administrator rights.

  b. The device initiates a Telnet connection with a client and it cannot determine whether the connection is successful.

  c. You cannot switch to the CLI if you log in to the web platform using the URL or based on IP address and port mapping.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Log in to the web system and click **CLI** in the lower right corner to display the CLI, as shown in **Figure 2-1**.

Figure 2-1 Switching to the CLI



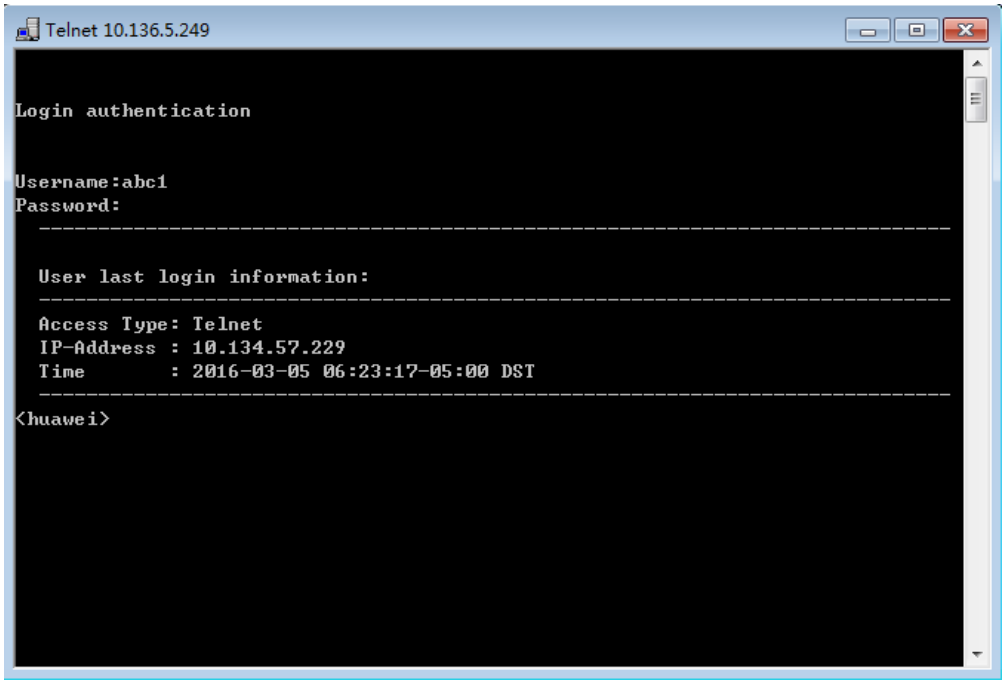
NOTE

If the Chrome or Firefox browser is used to switch from the web system to the CLI, the browser attempts to invoke the default Telnet client in the Windows OS and display the **External Protocol Request** dialog box after you click **CLI** in the lower right corner. Click **Launch Application** in the **External Protocol Request** dialog box. The CLI will be displayed.

Step 2 Enter the configured Telnet user name and password to log in to the router, as shown in **Figure 2-2**. You can manage and maintain the router on the CLI.

For details about how to configure the Telnet user name and password, see **2.20.1 User Management**.

Figure 2-2 CLI



----End

2.4 Precautions for Using the Web Platform

Copyright © Huawei Technologies Co., Ltd.

- The web platform supports multiple browsers. You can log in to the web platform using Firefox 46 to 66, Google Chrome 46 to 60, Internet Explorer 10.0 or later, or Windows Edge. If an exception occurs when you use Internet Explorer 10.0 to log in to the web platform, use a later version.
- If Internet Explorer is used and you want to access the CLI by clicking **CLI** in the lower right corner or to transfer files, set the security level of the browser to **Low** as follows (Internet Explorer 10.0 is used as an example):
  a. Open Internet Explorer, and choose **Tools** > **Internet Options** > **Security**.
  b. Click **Internet** and then **Custom level**, and select **Enable** for **Initialize and script ActiveX controls not marked as safe**, **Script ActiveX controls marked safe for scripting***, **Run ActiveX controls and plug-ins**, and **Active scripting**.
  c. Click the **Local intranet** and **Trusted sites** zones and set their security levels to **Low**.
- If you log in to the web platform using Firefox, choose **Tools** > **Options** > **Content** and select **Enable JavaScript**, and choose **Tools** > **Options** > **Privacy** and select **Access cookies from sites** and **Access third-party cookies**. Otherwise, web pages cannot be displayed. (Firefox 46 is used as an example.)
- If you log in to the web platform using Google Chrome, choose **Settings** > **Show advanced settings** > **Privacy** > **Content settings**, set **JavaScript** to **Allow all sites to run JavaScript (recommended)**, and set **Cookie** to **Allow local data to be set (recommended)**. Otherwise, web pages cannot be displayed. (Google Chrome 46 is used as an example.)
- If you log in to the web platform using Windows Edge, choose **Settings** > **View advanced settings** > **Cookie** > **Don't block cookie**. Otherwise, web pages cannot be displayed. (Windows Edge 25 is used as an example.)
- If the device software version changes, for example, the software version is upgraded or rolled back, clear the browser cache before using the web platform. Otherwise, web pages may be incorrectly displayed.
  - Internet Explorer: Choose **Tools** > **Internet Options** > **General**, click **Delete**, select **Temporary Internet files** and **Cookie**, and click **Delete** to clear the browser cache. (Internet Explorer 10.0 is used as an example.)
  - Firefox: Choose **Tools** > **Options** > **Privacy**, click **Clear your recent history**, select **Cookie** and **Cache**, and click **Clear Now** to clear the browser cache. (Firefox 46 is used as an example.)
  - Google Chrome: Choose **Settings** > **Show advanced settings** > **Privacy** > **Clear browsing data**, select **Delete cookies and other site and plug-in data**, and click **Clear browsing data** to clear the browser cache. (Google Chrome 46 is used as an example.)
  - Windows Edge: Choose **Settings** > **Choose what to clear**, select **Browsing history** and **Cookies and saved website data**, and click **Clear** to clear the browser cache. (Windows Edge 25 is used as an example.)
- The web platform does not support back, forward, and refresh buttons on the browser. If you click these buttons, the web platform may return to the login page.
- After the web platform runs for a long period of time, the browser will occupy increasing memory with a certain probability. As a result, you cannot log in to

 Copyright © Huawei Technologies Co., Ltd.

the web page or the web page is displayed abnormally. In this case, restart the browser, open the web platform, and log in to the system again.

NOTE

Windows Edge translates numbers into telephone numbers and automatically turns the numbers into clickable links. If you click or select the number, the message "You'll need a new app to open this tel" will be displayed. Ignore the message.

2.5 Logging In to the Web System

2.5.1 Logging In to the Device

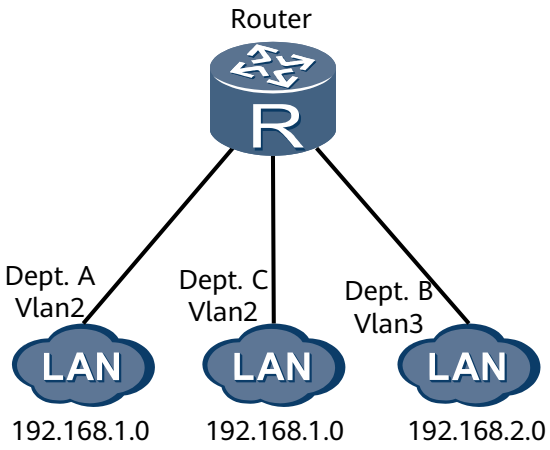
Context

You can use the device's factory settings to directly log in to the web system to manage and maintain the device.

Alternatively, you can configure the device's IP address, web system parameters, and a web system account, and then log in to the web system. For details about the configuration, see Web System Login Configuration.

As shown in **Figure 2-3**, you can log in to the device through the web system, and configure and manage the device on the PC.

Figure 2-3 Web system networking



Pre-configuration Tasks

Before logging in to the device through the web system, complete the following tasks:

- Configure an IP address for the device's access interface.

Copyright © Huawei Technologies Co., Ltd.

NOTE

The factory settings of the device include the IP address 192.168.1.1 and subnet mask 255.255.255.0. The access interface is the management interface under which the silkscreen **Management** or **MGMT** is printed. HTTP and HTTPS services are enabled on the device. For more details, see **FAQs** > **Basic Configuration** > **Which Interface Is Configured with the Default Management IP Address?** in the *AR Router Troubleshooting Guide*.

- Use a network cable to connect the PC to the device.

NOTE

If you cannot log in to the web using the PC that automatically acquires an IP address, configure a static IP address that is in the same network segment as the IP address of the device for the PC and then log in to the web.

- The device is running properly.
- Install the browser software on the PC.

Procedure

Step 1 Open the browser on the PC. Windows IE8.0 is used in this example. Enter **https://192.168.1.1** in the address box and press **Enter**. The web system login page is displayed, as shown in **Figure 2-4**.

Figure 2-4 Web system login page



NOTE

You can use the web mode to configure voice services only when the device works in PBX mode. You can log in to the voice self-service system using either of the following methods:

- On the web platform, click **Enter voice self-service system**.
- Run the **self-service-http-server** command in the voice view to access the self-service HTTP server configuration view, and then run the **self-service http secure-server enable** command to enable the self-service HTTPS server. You can enter **https://192.168.1.1:1443/professional/user/login.html** in the address box to access the voice self-service system. In the configuration view of the self-service HTTPS server, you can run the **self-service http secure-server port** command to change the port number of the self-service HTTPS server. The default port number is 1443.

Step 2 Enter login information.

1. Select a language.

The system supports English and Chinese. By default, the system uses the same language as the browser.

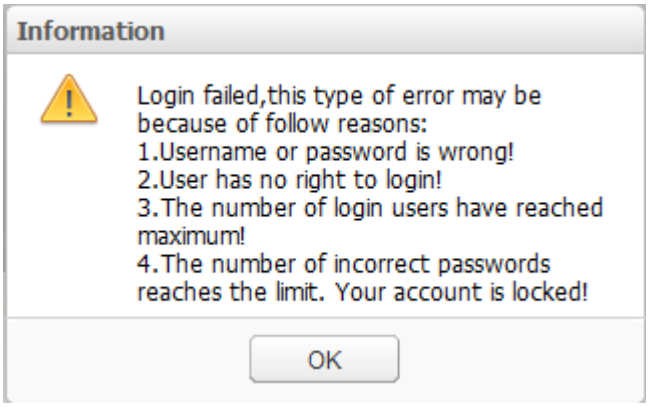
2. Enter the user name and password.

   The default username and password are available in *AR Router Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it.

3. Click **Login**.

   The system displays a message about login failure in situations shown in **Figure 2-5**.

   Figure 2-5 Login failure

   Check the cause of the login failure based on the prompt message. If the number of incorrect password attempts reaches the upper limit, the current account will be locked. By default, a locked account is automatically unlocked after 5 minutes.

NOTE

After a user logs in, the web system automatically displays the last login time, IP address, and login mode of the user.

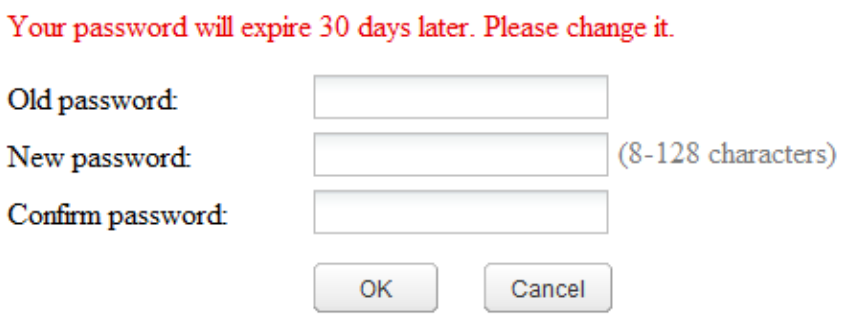
Step 3 Change the login password.

The system asks you to change the password in the following situations, as shown in **Figure 2-6**.

- If the login password expires, the system forcibly requires you to change the password.
- If you log in to the system for the first time after the password is changed by another user, the system forcibly requires you to change the password.
- If you log in to the system within the password expiration notification period, the system notifies you of the password expiration time and advises you to change the password.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-6 Password change page



NOTE

- If the parameters are marked with a red asterisk (*), the system forcibly requires you to change the password. After changing the password, click **OK**. If the password is changed successfully, the system displays the message "Your password has been modified successfully". Click **OK**. The login page is displayed. If you do not change the password, click **Cancel**. The login page is displayed and you cannot log in to the web system.
- If the parameters are not marked with a red asterisk (*), the system asks you to change the password. After changing the password, click **OK**. If the password is changed successfully, the system displays the message "Your password has been modified successfully". Click **OK**. The login page is displayed. If you do not change the password, click **Cancel**. The **Device Information** page is displayed.

Step 4 Click **Logout** in the upper right corner of the page to return to the login page.

Step 5 If you do not perform any operations within a period (10 minutes by default) after logging in to the web system, the system automatically logs you out. Click **OK** to return to the login page.

----End

(Optional) Basic Configuration After First Login

After logging in to the device through the web system for the first time, you can configure basic settings, such as configuring a web user and the device's IP address for remote login and management.

- For details about how to configure a web user, see **User Management**.
- For details about how to configure the device's IP address, see **Ethernet Interface**.

2.5.2 Common Misconfigurations

This section describes common faults caused by incorrect configurations and provides the troubleshooting procedure.

2.5.2.1 Device Login Through the Web Platform Fails

 Copyright © Huawei Technologies Co., Ltd.

Symptom

The device cannot be logged in through the web platform.

Procedure

Step 1 Check whether the AR and client can ping each other.

1. Run the **ping** command on the Windows Command Prompt of the PC to check whether the PC can ping the AR.

   When the system displays the message "Request time out", the target device is unreachable.
2. Run the **display this** command in the interface view to check whether the IP address is configured correctly.
3. If the IP address is incorrect, run the **ip address** *ip-address* { *mask* | *mask-length* } command in the interface view to reconfigure the IP address.
4. Open the web platform again and ensure that the input IP address in **https://*IP address:port*** is the same as that configured on the AR.

Step 2 Check whether the browser configuration is correct.

1. Configure the browser according to **2.4 Precautions for Using the Web Platform** and log in to the web platform again.
2. Log in to the web platform through another browser and check whether the IE browser limits the login to the web platform.

Step 3 Check whether the HTTPS server configuration is correct.

1. Check whether the HTTPS server is enabled.

   Run the **display http server** command in any view. If the value of **HTTPS server status** is **Disabled**, run the **http secure-server enable** command in the system view to enable the HTTPS server.
2. Check the port number of the HTTPS server.

   Run the **display http server** command in any view to check the value of **HTTPS server port**.

   Ensure that the input port number in the address bar is the same as the value of **HTTPS server port**.

   Run the **http secure-server port** command in the system view to configure the port number of the HTTPS server.

Step 4 Check whether the number of login web users has reached the maximum value.

Run the **display http server** command in any view to check values of **Current online users** and **Maximum users allowed**.

If the values of **Current online users** and **Maximum users allowed** are the same, log in again after other users go offline.

Step 5 Check whether the interface that allows access to the web platform is configured.

Run the **display current-configuration filter http server** command in any view to check whether there is the configuration of **http server permit interface**.

If the interface that allows access to the web platform Is configured and the interface that accesses the web platform is not allowed, run the **undo http server**

 Copyright © Huawei Technologies Co., Ltd.

permit interface command in the system view to cancel the configuration of the interface that allows access to the web platform or run the **http server permit interface** command in the system view to reconfigure the interface that allows access to the web platform.

Step 6 Check whether the web user is configured correctly.

1. Run the **display this** command in the AAA view to check whether the web user is correctly configured.
   - If there is the configuration of **local-user** *user-name* **password irreversible-cipher** *password*, an AAA user with the user name specified by *user-name* is configured.
   - If there is the configuration of **local-user** *user-name* **privilege level** *level*, the level of an AAA user with the user name specified by *user-name* is specified by *level*.
   - If there is the configuration of **local-user** *user-name* **service-type http**, an AAA user with the user name specified by *user-name* uses HTTP access.
2. If any of the preceding configurations is lost, run the following commands in the AAA view as required.
   - Run the **local-user** *user-name* **password irreversible-cipher** *password* command to set the web user name and password.
   - Run the **local-user** *user-name* **privilege level** *level* command to set the web user level.
   - Run the **local-user** *user-name* **service-type http** command to configure the service type of the web user to HTTP.

   For example, configure a user with the user name of **admin**, password of **Helloworld@6789**, level 15, and HTTP access mode.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] local-user admin password irreversible-cipher Helloworld@6789
[Huawei-aaa] local-user admin privilege level 15
[Huawei-aaa] local-user admin service-type http
[Huawei-aaa] quit
```

Step 7 Check whether access control is configured for the web client.

1. Run the **display current-configuration filter http acl** command in any view to check whether there is the configuration of **http acl** *acl-number*.

   If there is the configuration of **http acl** *acl-number*, record the ACL number.
2. Run the **display acl** *acl-number* command in any view to check whether the IP address of the web client is denied in the ACL.

   If the IP address of the web client is denied in the ACL, run the **undo rule** *rule-id* command to delete the ACL rule and use a command to modify the ACL to allow the IP address of the web client.

Step 8 Check whether the browser is problematic.

----End

2.5.2.2 The Web System Page Is Not Completely Displayed After Successful Device Login Through the Web System

 Copyright © Huawei Technologies Co., Ltd.

Symptom

After successful device login through the web system, the web system page is not completely displayed, or only several options are displayed.

Procedure

Step 1 Check whether the web user level is too low.

If the user level is 1, the user is a common administrator and can only access **Device Information** and change the password in **User Management**. If the user level is 2, the user is an enterprise administrator and has most operating rights in the web system. If the user level is 3 to 15, the user is a super administrator and has all operating rights in the web system.

Run the **display this** command in the AAA view to check the web user level. If the value of *level* is too small in the **local-user** *user-name* **privilege level** *level* configuration, some functions cannot be displayed in the web system. Run the **local-user** *user-name* **privilege level** *level* command in the AAA view to set the web user level to 3 or higher so that the web user has all operating rights in the web system.

Step 2 Check whether the device version is correct.

Run the **display version** command in any view to check the device version. If the value of *Version* is too small in the **VRP (R) software, Version** *Version* configuration, the device does not support some functions in the web system. Upgrade the device to a proper version.

----End

2.5.3 FAQ About Web System Login

This section describes common problems you may encounter during the configuration and provides the solutions to these problems.

2.5.3.1 Does the AR Series Support the Web NMS?

The AR series supports the web network management system (NMS) from V200R002C01. You can use the web network management system to manage and maintain AR series.

2.5.3.2 How Do I Configure the Web User Level?

Run the **local-user** *user-name* **privilege level** *level* command in the AAA view to set the web user level.

- If the user level is 1, the user is a common administrator and can only access **Device Information** and change the password in **User Management**.
- If the user level is 2, the user is an enterprise administrator and has most operating rights in the web system.
- If the user level is 3 to 15, the user is a super administrator and has all operating rights in the web system.

You are advised to set *level* to 3 or higher.

 Copyright © Huawei Technologies Co., Ltd.

2.5.3.3 What Should I Do If I Forget the Web System Login Password?

If you forget or want to change the web system login password, log in to the device through the console port, Telnet, or STelnet and set a new password after login.

NOTE

Telnet has security vulnerabilities. You are advised to log in to the device using STelnet V2.

Set the password to **Huawei@123** for the user **admin123**. The configuration is as follows:

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] local-user admin123 password irreversible-cipher Huawei@123
[Huawei-aaa] local-user admin123 service-type http
[Huawei-aaa] local-user admin123 privilege level 15
[Huawei-aaa] return
<Huawei> save
```

2.5.3.4 What Is the Default Login Password?

The default username and password are available in *AR Router Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it.

NOTE

For security purposes, you are advised to change the default password for the device.

2.5.3.5 What Should I Do If the Account Is Locked?

By default, a locked account is automatically unlocked after 5 minutes. You can wait until the account is automatically unlocked, and enter the correct user name and password to log in to the device again.

You can also log in to the device using the CLI mode when the account is locked, and run the **local-user** *user-name* **state active** command in the AAA view to unlock the account.

2.5.3.6 How Do I Obtain the Web Page File?

The system software contains the web page file. After new system software is loaded to the device, the web page file **web.zip** is directly decompressed from the system software and saved to the memory.

2.5.3.7 How Do I Change the Port Number for Web System Login?

Procedure

You can run the **http secure-server port** *port-number* command in the system view to reconfigure the port number of the HTTPS server.

 Copyright © Huawei Technologies Co., Ltd.

More Information

- Changing the port number of the HTTPS service forces all online users to go offline. Therefore, exercise caution when performing this operation.
- The default port number of the HTTPS server is 443. If you access and control the device through the web platform, you do not need to specify the port number. If the default port number is used, attackers may access this port continuously, consuming bandwidth resources and degrading security performance of the server. As a result, authorized users cannot access the device. If the default port number is used by another service, users cannot log in to the device through the web platform. This command allows you to set another port number for the HTTPS service to avoid such attacks.

2.5.3.8 How Do I Change the IP Address for Web Platform Login?

You can change the IP address for web platform login using the command-line interface (CLI) or web platform.

1. You can configure a management IP address on the CLI using either of the following methods:

a. Configure a management IP address on the management interface of the AR router. For example, the management interface is GE0/0/0. Set the management IP address to 192.168.1.10 and the mask length to 24.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 0/0/0
[Huawei-GigabitEthernet0/0/0] ip address 192.168.1.10 24
```

b. Configure a management IP address on a VLANIF interface. For example, all LAN interfaces on the router are added to VLAN 1. Set the management IP address to 192.168.1.10 and the mask length to 24.

NOTE

In the factory settings, all LAN interfaces on the AR150&AR160&AR200 are added to VLAN 1 by default. The default IP address 192.168.1.1/24 is configured for VLANIF 1. Any LAN interface can use this IP address as the management IP address.

```
<Huawei> system-view
[Huawei] vlan 1
[Huawei-vlan1] quit
[Huawei] interface vlanif 1
[Huawei-Vlanif1] ip address 192.168.1.10 24
[Huawei-Vlanif1] quit
```

2. Configure a management IP address using the web platform.

Log in to the web platform. Choose **WAN Access** > **Ethernet Interface**. Find the corresponding management interface on the **Ethernet Interface** page. Click  next to the interface to configure an IP address for the interface.

2.6 Help and Version of the Web Platform

The **Help** and **About** icons are at the upper right corner on the web platform. **Table 2-1** describes the icons.

 Copyright © Huawei Technologies Co., Ltd.

Table 2-1 Description of the **Help** and **About** icons

Icon	Description
Help	You can click **Help** or press **F1** on any page to view help information about the current page, including the configuration procedure and parameters. If the browser automatically blocks pop-up windows, configure the browser to allow the display of pop-up windows. In the displayed help window, you can view help information about any page in the navigation tree on the left side.
About	You can click **About** at any page to view the version of the web platform.

2.7 Switching the WLAN Mode

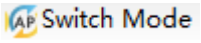
Context

The device supports the WLAN AP and AC modes and can switch between the two modes.

NOTE

- Only models whose name contain W supports WLAN mode switching.
- By default, the AR121W, AR129W, AR129CVW, AR121GW-L, AR129GW-L, AR129CGVW-L, AR109W, AR109GW-L, AR151W-P, AR156W, AR157W, AR157VW, AR158EVW, AR161W, AR161EW, AR161EW-M1, AR161FGW-L, AR161FGW-Lc, AR169W, AR161FW, AR161FW-P-M5, AR161FGW-La, AR169FVW, AR169FVW-8S, AR169JFVW-4B4S, AR169JFVW-2S, AR169CVW-4B4S, AR169EGW-L, AR169EW, AR169CVW, AR169FGVW-L, AR169FGW-L, AR169W-P-M9, AR169RW-P-M9, AR201VW-P, AR207VW, AR1220W, AR1220EVW, and AR1220VW works in AP mode and other devices work in AC mode.

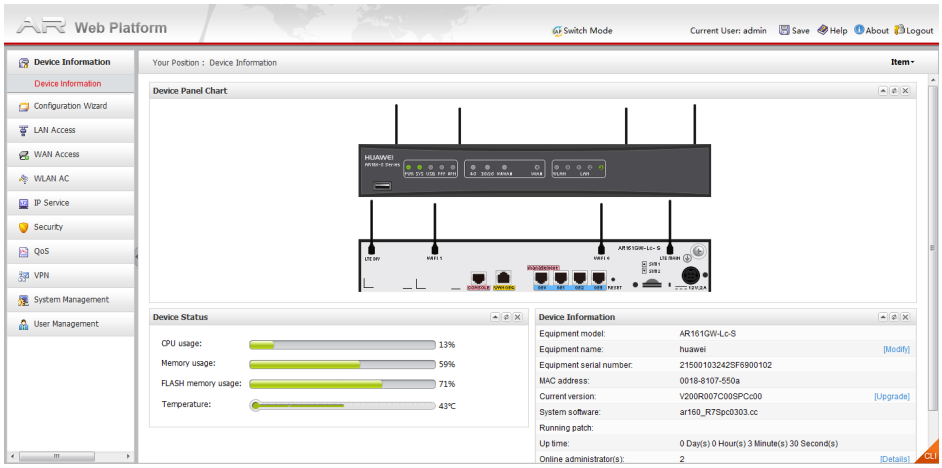
Procedure

- Switch from the AC mode to the AP mode.
  a. Log in to the web platform, and click 

in the upper right corner of the page to switch to the AP mode, as shown in **Figure 2-7**.

Copyright © Huawei Technologies Co., Ltd.

Figure 2-7 Switching from the AC mode to the AP mode

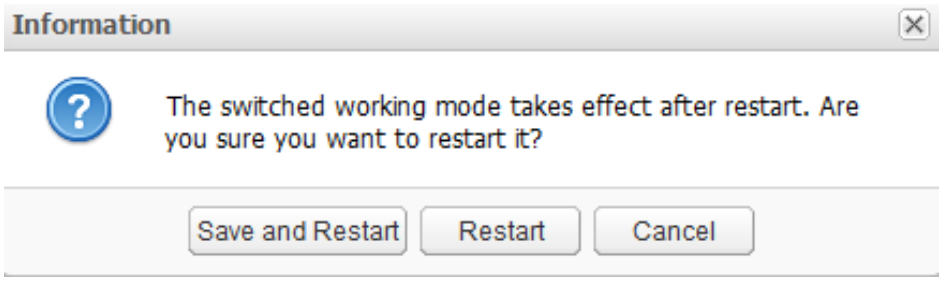


NOTE

The Switch Mode button is displayed upon login only when the device is working in AC mode.

b. In the **Information** dialog box that is displayed, select **Save and Restart**, as shown in **Figure 2-8**. The device switches to the AP mode after the device configuration is saved and the device restarts.

Figure 2-8 Confirming the mode switching

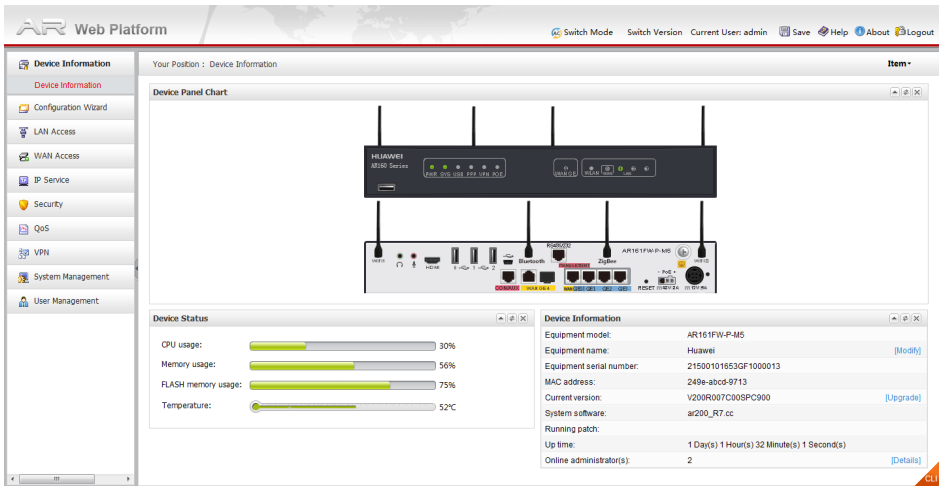


- Switch from the AP mode to the AC mode.

  a. Log in to the web platform, and click Switch Mode in the upper right corner of the page to switch to the AC mode, as shown in **Figure 2-9**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-9 Switching from the AP mode to the AC mode

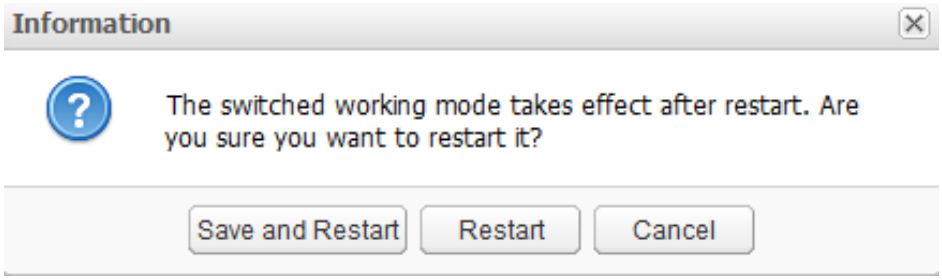


NOTE

The Switch Mode button is displayed upon login only when the device is working in AP mode.

b. In the **Information** dialog box that is displayed, select **Save and Restart**, as shown in **Figure 2-10**. The device switches to the AC mode after the device configuration is saved and the device restarts.

Figure 2-10 Confirming the mode switching



----End

2.8 Initial Configuration of the Web Platform

Context

When logging in to the web platform, you need to perform initial configurations to implement basic communications.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Choose **Configuration Wizard** > **Internet Access Wizard**.

Configure interfaces connected to the Internet, set parameters for accessing the Internet, and configure LAN information according to **Internet Access Wizard**.

After these configurations are complete, hosts on the LAN can access the Internet using the router.

Step 2 Check the software version and license.

1. Click **Device Information**.
2. In the **Device Information** window, view the software version.

   To view the latest software version, access the technical support center on the Huawei website.

   After downloading the latest version, see **System Software** to upgrade system software.
3. In the **License Information** window, view license information.

   Some functions of the router are restricted by the license, so you must check whether information about the current license is the same as information about the purchased one. If the value of **License Status** is **not activated**, see **License Management** to apply and activate the license. If license information is different from information about the purchased information, see **Obtaining Technical Support** to contact technical support personnel for help.

NOTE

Only super administrators (levels 3 to 15) can upgrade system software and view license authorization information.

Step 3 Back up the configuration file.

After completing the initial configuration, click **Save** in the upper right corner. Choose **System Management** > **Upgrade and Maintenance** > **Restart Device**. Click **Export Configuration File** to back up the configuration file for diagnosing or rectifying faults in the future. You are advised to back up the configuration file when the router configuration is changed a lot.

NOTE

Only super administrators (levels 3 to 15) can back up configuration files.

----End

2.9 Device Information

Background

You can view router information, including the real-time running status of a router.

- **Customized Display Mode**

 Copyright © Huawei Technologies Co., Ltd.

- Device Panel Chart
- Device Status
- Device Information
- Card Information
- License Information
- Service
- 3G/LTE
- LAN
- WAN
- Log

Customized Display Mode

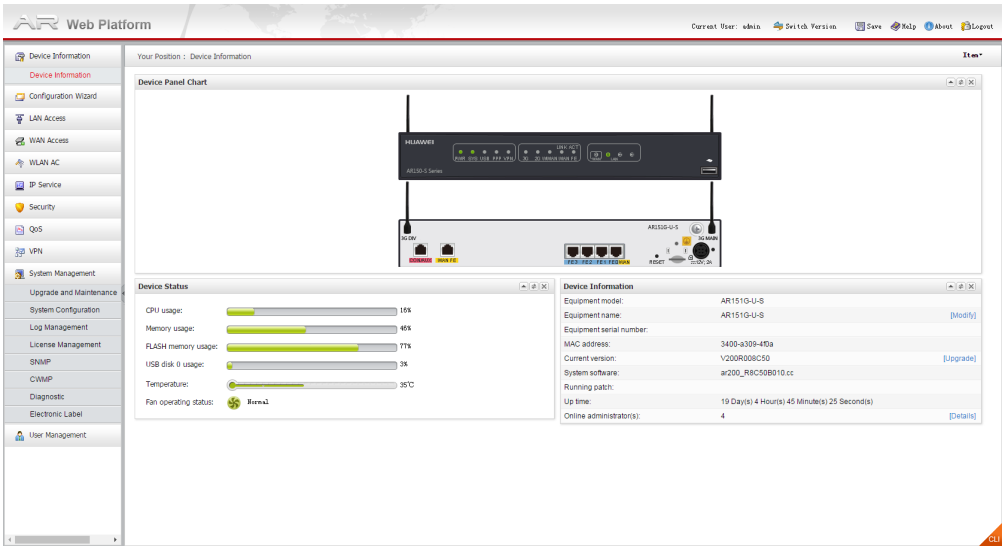
The web platform provides multiple windows to display router information. You can customize the status window display mode.

NOTE

Router status varies according to models and configurations.

1. Choose **Device Information** > **Device Information** to access the **Device Information** page, as shown in Figure 2-11.

   Figure 2-11 Device Information



2. Click **Item**.
3. Select status windows you want to view.

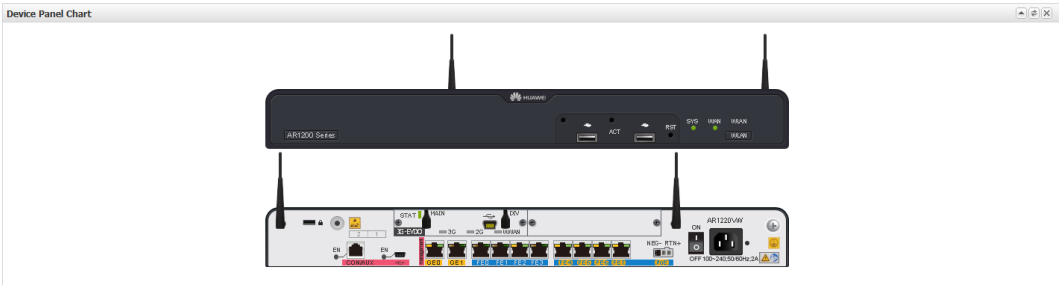
   The selected windows are displayed in the **Device Information** page.

-

Device Panel Chart

You can view the router panel chart in the **Device Panel Chart** window. The router panel chart simulates the front and rear panels, and provides indicator and interface information, as shown in **Figure 2-12**.

Figure 2-12 Device Panel Chart



NOTE

Indicators vary according to the router model and configuration.

Different indicator status indicates different status of an interface.

- If the indicator is steady on, the interface is connected.
- If the indicator is off, the interface is not connected.

When you move the cursor to an interface, information about this interface, including the interface name and status, is displayed.

Table 2-2 describes indicators on the router panel.

Table 2-2 Indicator description

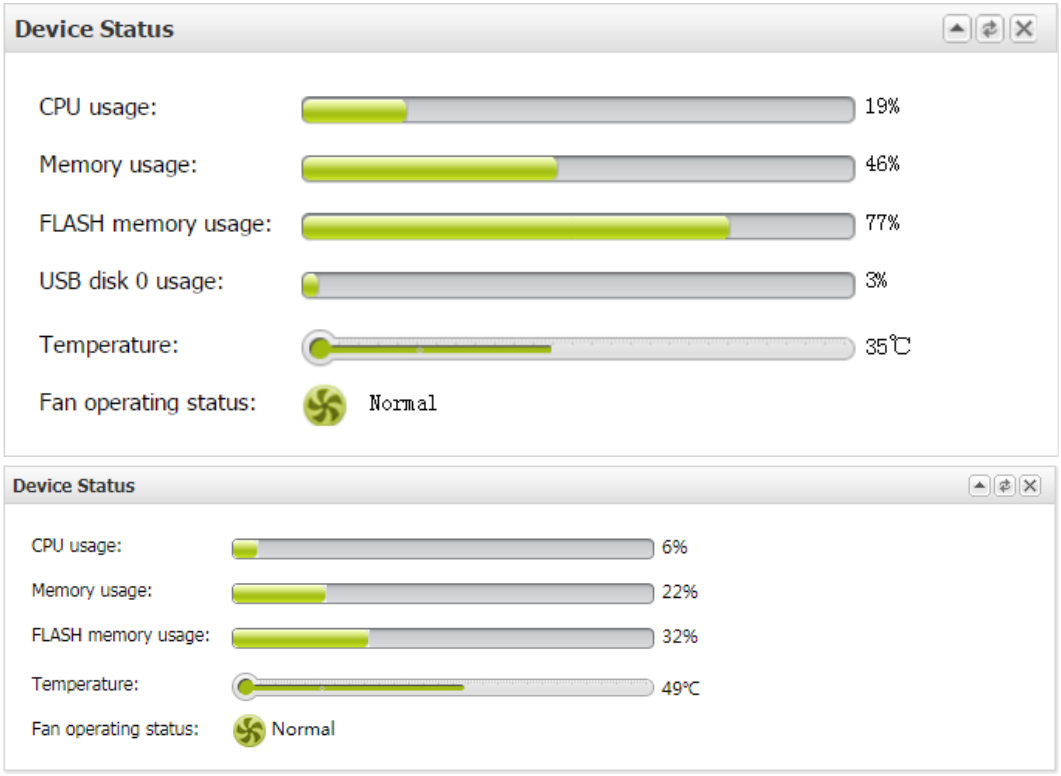
Indicator	Color	Description
STATUS	Green	Steady on: The card is running properly Off: The board is faulty or powered off.
PWR	Green	Steady on: The power module is running properly. Off: The power module is faulty or not connected.

Device Status

You can view router resource information including the CPU usage, memory usage, flash memory usage, USB disk usage, temperature, and fan operating status in the **Device Status** window, as shown in **Figure 2-13**.

Copyright © Huawei Technologies Co., Ltd.

Figure 2-13 Device Status

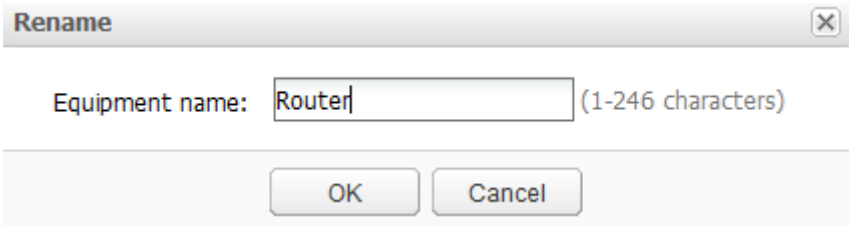


Device Information

You can view router information in the **Device Information** window, as shown in **Figure 2-17**.

- Equipment model: router model.
- Equipment name: router name. To change the router name, click **Modify**. When the page shown in **Figure 2-14** is displayed, click **OK**.

  Figure 2-14 Changing the equipment name

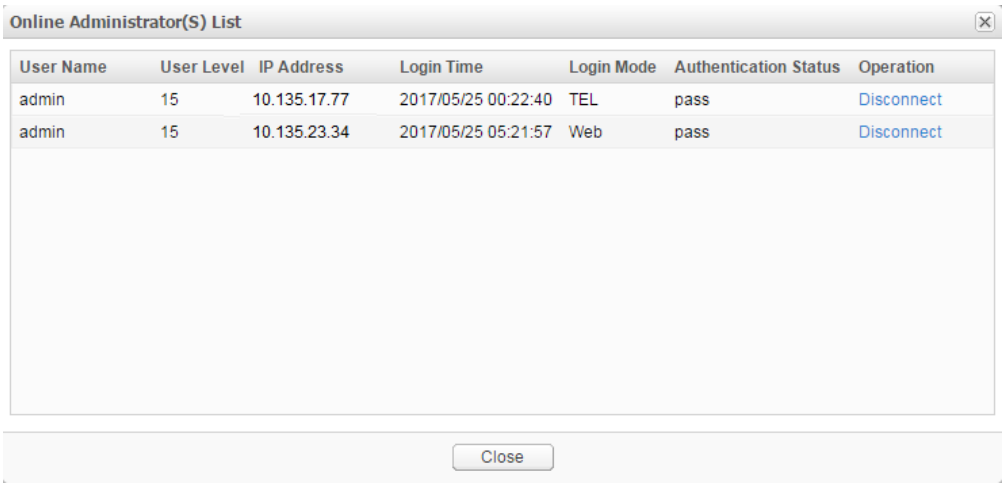
  

- Equipment serial number: sequence number of a router. Each router has a unique sequence number.
- MAC address: MAC address of a router.
- Current version: software version of the current system. To upgrade system software, click **Upgrade** to access the **upgrade and maintenance** > **Restart Device** page.
- System software: name of system software.

 Copyright © Huawei Technologies Co., Ltd.

- Running patch: the patch that is running on the router.
- Up time: how the router has been running.
- Online administrator(s): number of administrators of the router you log in to. To view detailed information about administrators, click **Details**, as shown in **Figure 2-15**.

Figure 2-15 Details about administrators



To force a user offline, select **Disconnect** in the **Operation** column. When the page shown in **Figure 2-16** is displayed, click **OK**.

Figure 2-16 Forcing a user offline

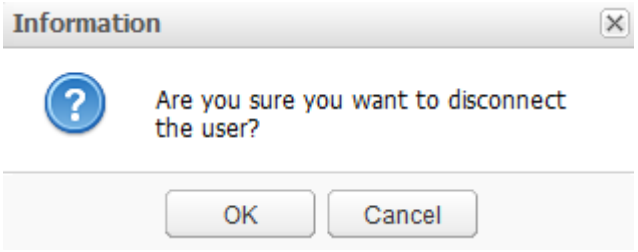


Figure 2-17 Device Information

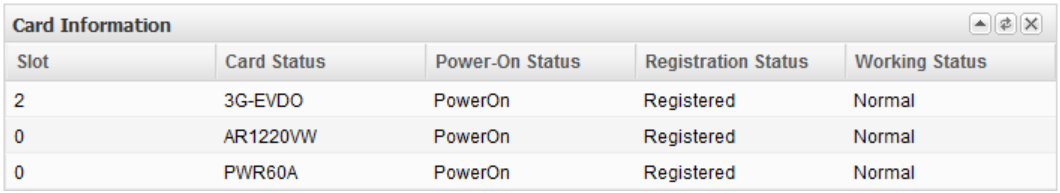


 Copyright © Huawei Technologies Co., Ltd.

Card Information

You can view card information including the slot, card status, power-on status, registration status, and working status in the **Card Information** window, as shown in **Figure 2-18**.

Figure 2-18 Card Information



License Information

You can view license information in the **License Information** window, as shown in **Figure 2-19**.

Figure 2-19 License Information

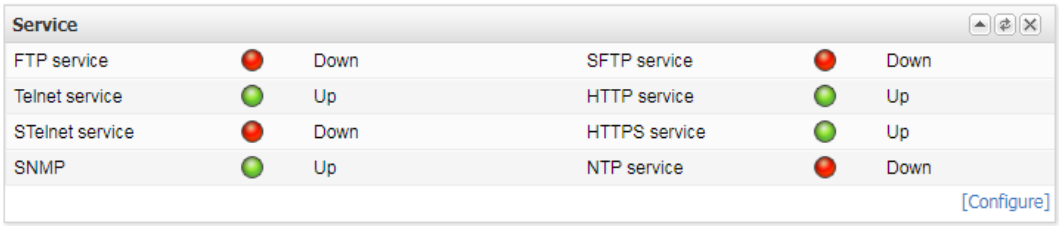


You can click **Configure** to access the **License Management** page.

Service

You can view enabled or disabled services on the router in the **Service** window, including FTP, SFTP, Telnet, HTTP, STelnet, HTTPS, SNMP, CWMP, and NTP, as shown in **Figure 2-20**.

Figure 2-20 Service



3G/LTE

You can view information about the 3G/LTE wireless card in the **3G/LTE** window, including the interface name, network mode, signal strength, working status, roaming status, carrier, IP address, and SIM card status. You can check whether the

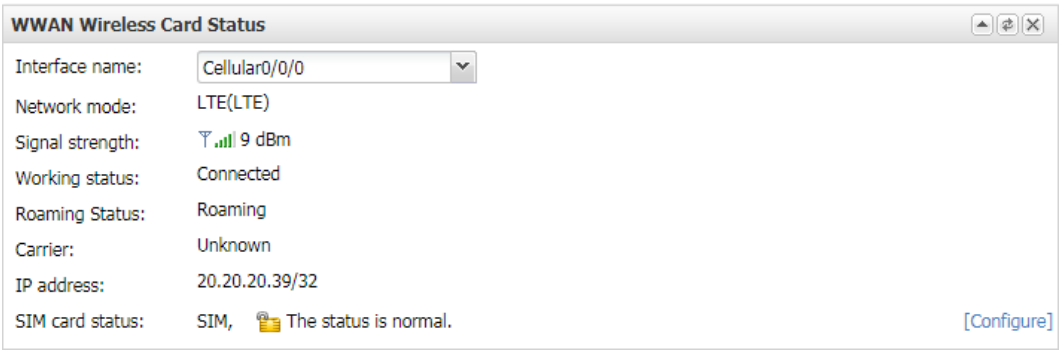
Copyright © Huawei Technologies Co., Ltd.

router can access the Internet using the 3G/LTE wireless card based on the preceding information, as shown in **Figure 2-21**.

NOTE

To view information in this window, ensure that the 3G data card and the corresponding SIM card have been installed on the router.

Figure 2-21 3G/LTE Wireless Card Status



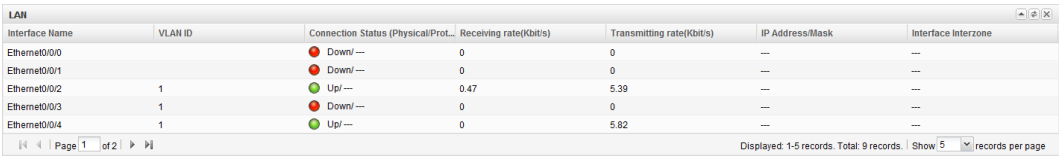
You can select an interface from the **Interface name** drop-down list box to view.

You can click **Configure** to access the **3G/LTE Interface** page. On this page, you can view and modify detailed information about 3G/LTE interfaces.

LAN

You can view LAN information about the router in the **LAN** window, including the interface name, VLAN ID, connection status, receive rate, transmit rate, IP address/mask, and interface interzone, as shown in **Figure 2-22**.

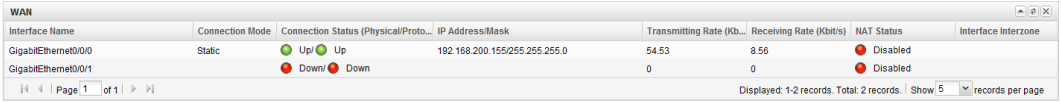
Figure 2-22 LAN



WAN

You can view WAN information about the router in the **WAN** window, including the interface name, connection mode, connection status, IP address, transmit rate, receive rate, NAT status, and interface interzone, as shown in **Figure 2-23**.

Figure 2-23 WAN

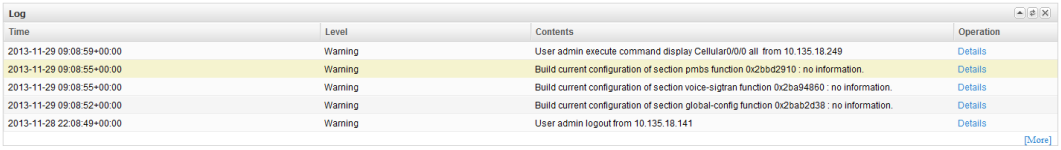


 Copyright © Huawei Technologies Co., Ltd.

Log

You can view system logs in the **Log** window, including the log generation time, log level, and log details, as shown in **Figure 2-24**.

Figure 2-24 Log



2.10 Configuration Wizard

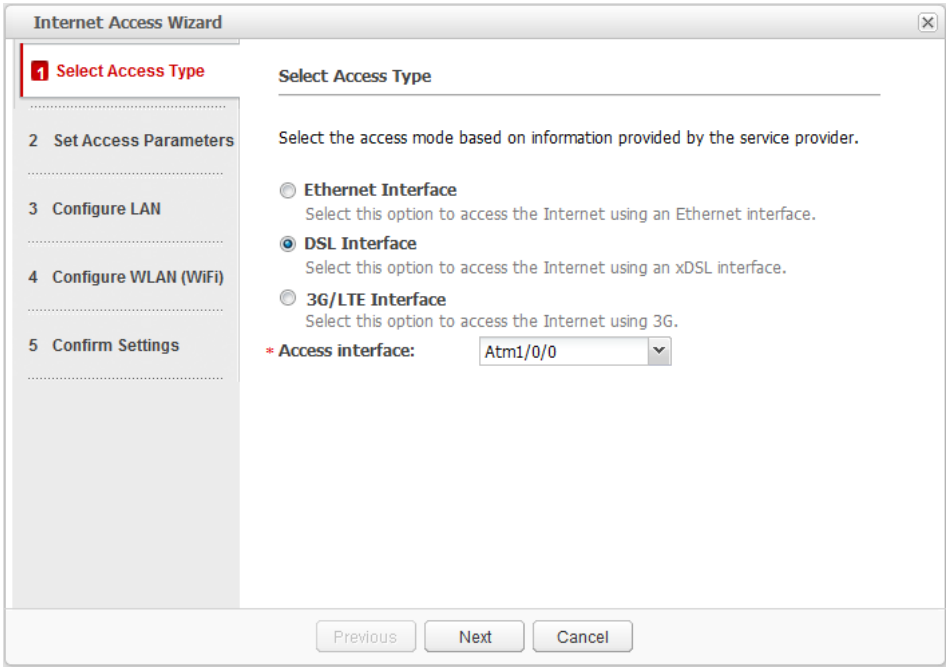
2.10.1 Internet Access Wizard

Procedure

Step 1 Select the access type.

1. Choose **Configuration Wizard** > **Internet Access Wizard**.
2. Set parameters on the **Select Access Type** tab page. The parameters are as described in **Table 2-4**.

Figure 2-25 Select Access Type



 Copyright © Huawei Technologies Co., Ltd.

3. Click **Next**.

Table 2-3 Selecting the access type

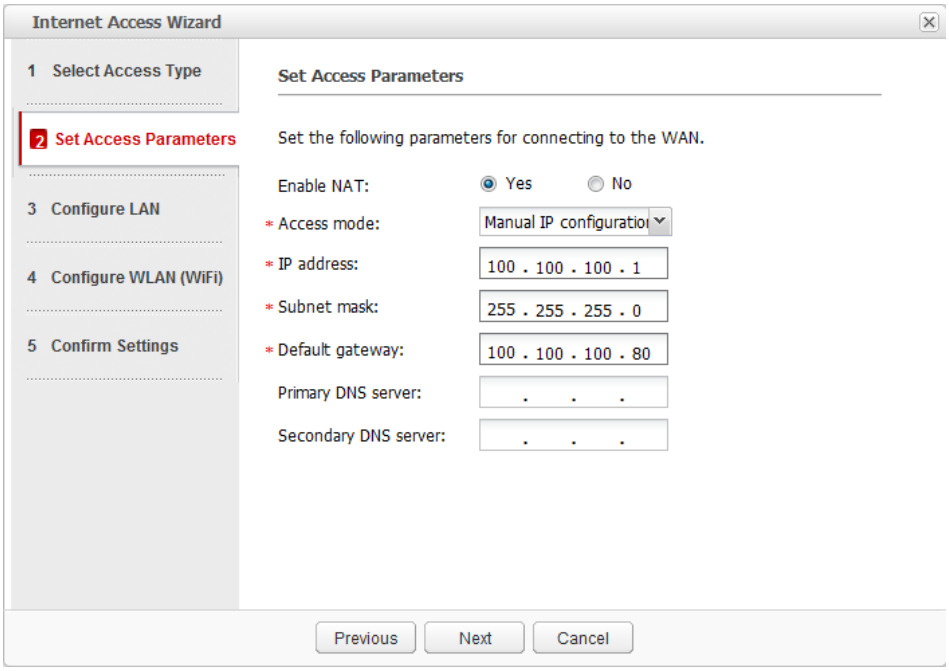
Parameter	Description
Select Access Type	Internet access method. • Set this parameter to **Ethernet Interface** when you use an Ethernet interface to access the Internet. For details about access parameters of an Ethernet interface, see **Table 2-4**. • Set this parameter to **DSL Interface** when you use a DSL interface to access the Internet. For details about access parameters of a DSL interface, see **Table 2-5**. **NOTE** The value **DSL Interface** is available only when the router is inserted with a DSL card. • Set this parameter to **3G/LTE Interface** when you use a 3G/LTE interface to access the Internet. For details about access parameters of a 3G/LTE interface, see **Table 2-6**. **NOTE** The value **3G/LTE Interface** is available only when the router is inserted with a 3G/LTE data card.
Access interface	Interface used to access the Internet.

Step 2 Set access parameters.

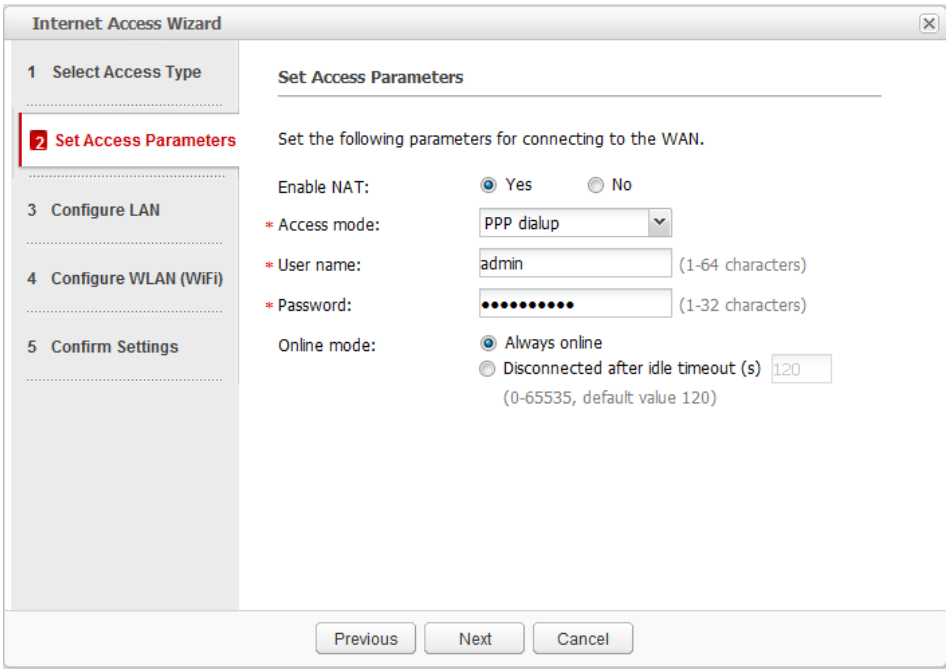
1. Set parameters on the **Set Access Parameters** tab page. The parameters are described in the following tables.
2. Click **Next**.

Copyright © Huawei Technologies Co., Ltd.

- **Figure 2-26** Connect to the WAN using an Ethernet interface (Manual IP configuration)

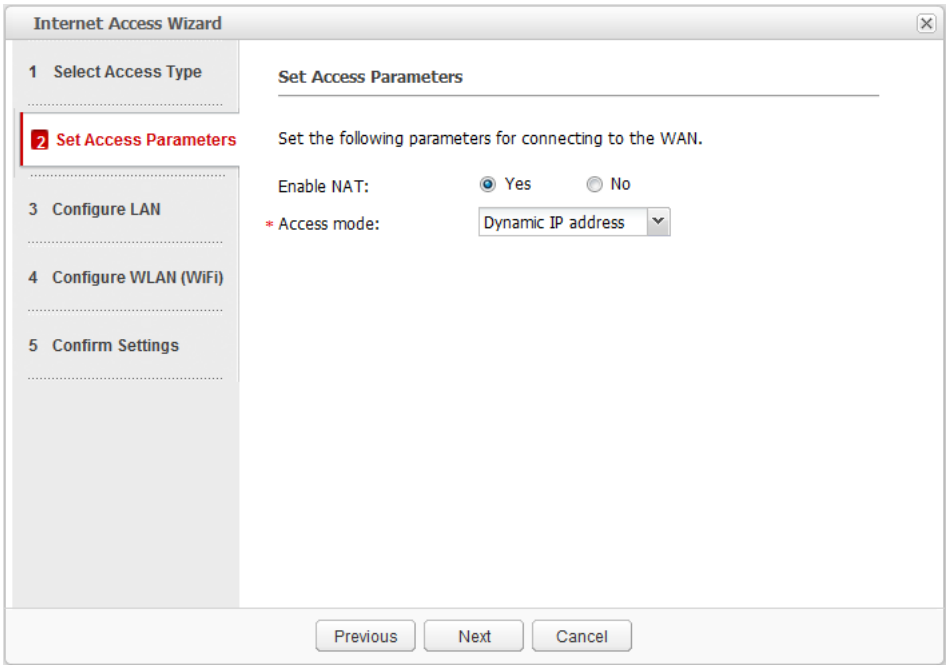


- **Figure 2-27** Connect to the WAN using an Ethernet interface (PPP dialup)

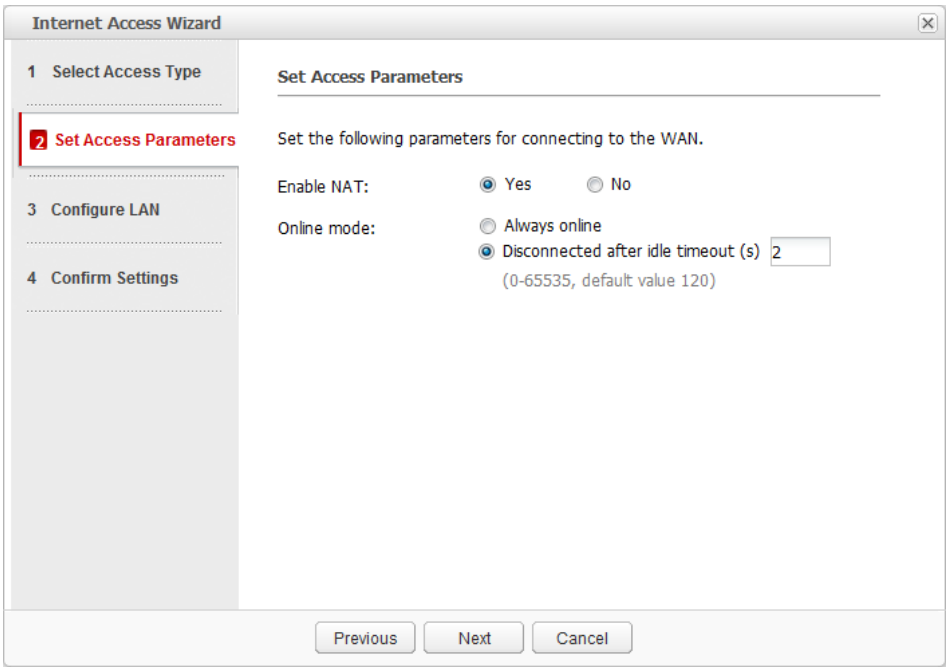


 Copyright © Huawei Technologies Co., Ltd.

- **Figure 2-28** Connect to the WAN using an Ethernet interface (Dynamic IP address)



- **Figure 2-29** Connect to the WAN using a 3G/LTE interface



 Copyright © Huawei Technologies Co., Ltd.

Table 2-4 Configuring access parameters of an Ethernet interface

Parameter	Description
NAT status	NAT enabled when private PCs on the LAN are connected to the Internet.
Access mode	Internet access mode. • Set this parameter to **Manual IP configuration** when the interface IP address is manually configured, as shown in **Figure 2-26**. For details about static IP address parameters, see **Table 2-7**. • Set this parameter to **PPP dialup** when the interface obtains an IP address through Point-to-Point Protocol (PPP) negotiation, as shown in **Figure 2-27**. For details about PPP dialup parameters, see **Table 2-8**. • Set this parameter to **Dynamic IP address** when the interface automatically obtains an IP address through DHCP, as shown in **Figure 2-28**.

Table 2-5 Configuring access parameters of a DSL interface

Parameter	Description
NAT status	NAT enabled when private PCs on the LAN are connected to the Internet.
PVC(VPI/VCI)	Permanent virtual circuit (PVC) used by a link.
Encapsulation type	ATM Adaptation Layer Type 5 (AAL5) encapsulation type of the PVC. • Set this parameter to **aal5snap** when multiple protocols need to be transmitted over a single PVC. • Set this parameter to **aal5mux** when each protocol runs on an independent PVC.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Access mode	Internet access mode: • Manual IP configuration: Users access the Internet in IP over ATM (IPoA) mode, and the interface IP address must be manually configured. For details about static IP address parameters, see **Table 2-7**. • PPP dialup: Users access the Internet in Point-to-Point Protocol over Ethernet over ATM (PPPoEoA) mode, and the interface automatically obtains an IP address through DHCP. For details about PPP dialup parameters, see **Table 2-8**. • Dynamic IP address: Users access the Internet in IP over Ethernet over ATM (IPoEoA) mode, and the interface automatically obtains an IP address through DHCP.

Table 2-6 Configuring access parameters of a 3G/LTE interface

Parameter	Description
NAT status	NAT enabled when private PCs on the LAN are connected to the Internet.
User name	The user name sent from the local device to the remote device in PPP authentication. **NOTE** This parameter is valid only for CDMA2000 networks.
Password	The password sent from the local device to the remote device in PPP authentication. **NOTE** This parameter is valid only for CDMA2000 networks.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Online mode	3G/LTE dialup mode. • When this parameter is set to **Permanently online**, the dial control center (DCC) automatically attempts to dial the remote end after a router starts. The dialing process is not triggered by data packets. If a connection cannot be established with the remote end, the router retries at an interval. The value **Permanently online** applies to scenarios where traffic and online duration are not charged. • When this parameter is set to **Disconnected after idle timeout (s)**, a link is established only when data is transmitted. When no traffic exists on the link within a specified period, the router removes the link to save traffic. The value **Disconnected after idle timeout (s)** applies to scenarios where traffic and online duration are charged. When setting this parameter to **Disconnected after idle timeout (s)**, specify the link idle timeout period. The default value is 120.

Table 2-7 Static IP address parameters

Parameter	Description
IP address	IP address of the interface. The IP address of the interface cannot conflict with the IP address of any other interfaces or devices.
Subnet mask	Subnet mask of the interface.
Default gateway	Default gateway address of the interface. The default gateway address and IP address of the interface must be in the same network segment.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Primary DNS server	Primary DNS server address assigned to DHCP clients.
Secondary DNS server	Secondary DNS server address assigned to DHCP clients.

Table 2-8 PPP dialup parameters

Parameter	Description
User name	User name used for PPP dialup.
Password	Password used for PPP dialup.
Online mode	PPP dialup mode. • When this parameter is set to **Permanently online**, the DCC automatically attempts to dial the remote end after a router starts. The dialing process is not triggered by data packets. If a connection cannot be established with the remote end, the router retries at an interval. The value **Permanently online** applies to scenarios where traffic and online duration are not charged. • When this parameter is set to **Disconnected after idle timeout (s)**, a link is established only when data is transmitted. When no traffic exists on the link within a specified period, the router removes the link to save traffic. The value **Disconnected after idle timeout (s)** applies to scenarios where traffic and online duration are charged. When setting this parameter to **Disconnected after idle timeout (s)**, specify the link idle timeout period. The default value is 120.

Step 3 Configure the LAN.

1. Set parameters on the **Configure LAN** tab page. The parameters are as described in **Table 2-9**.

Copyright © Huawei Technologies Co., Ltd.

Figure 2-30 shows **Configure LAN** page.

NOTE

If there is no available LAN interface for the current device, you can select a WAN interface for LAN configuration.

2. Click **Next**.

Figure 2-30 Configure LAN

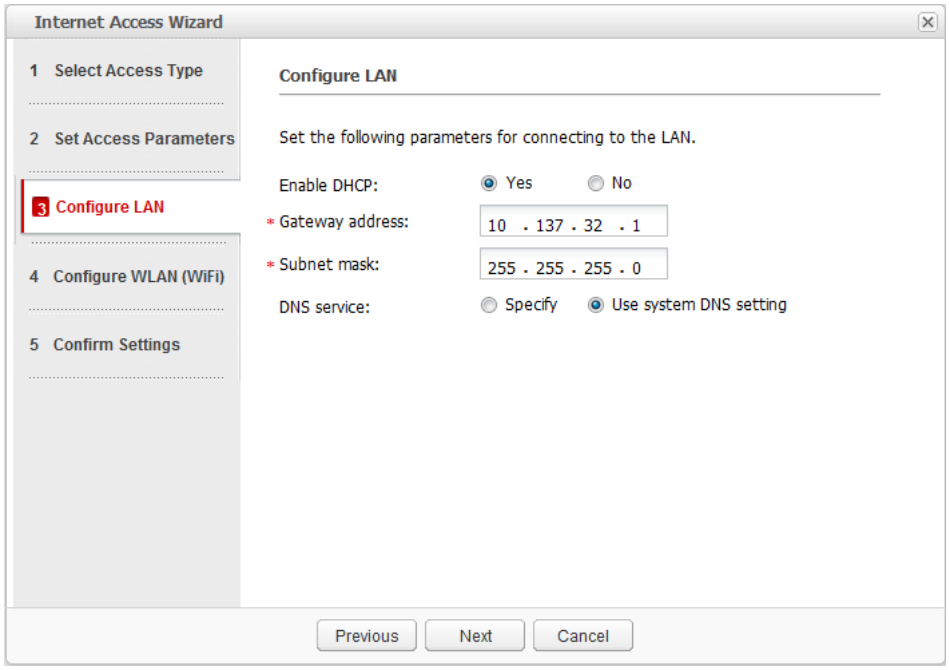


Table 2-9 Configuring the LAN

Parameter	Description
Enable DHCP	Whether to enable the DHCP server function on the interface. After you enable the DHCP server function on an interface, users in the LAN can obtain IP addresses from the DHCP address pool.
Gateway address	Egress gateway address for the DHCP clients, that is, the IP address of VLANIF1 interface.
Subnet mask	Subnet mask of the egress gateway.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
DNS service	DNS service on the VLANIF interface. This parameter is valid only when DHCP is enabled. The value can be: • Use system DNS setting: The system delivers the DNS server IP address that is the same as the gateway IP address. • Specify: An IP address must be specified for the DNS server.
Primary DNS server	IP address of the primary DNS server. This parameter is available only after you click **Specify**.
Secondary DNS server	IP address of the secondary DNS server. This parameter is available only after you click **Specify**.

Step 4 Configure the WLAN (Wi-Fi).

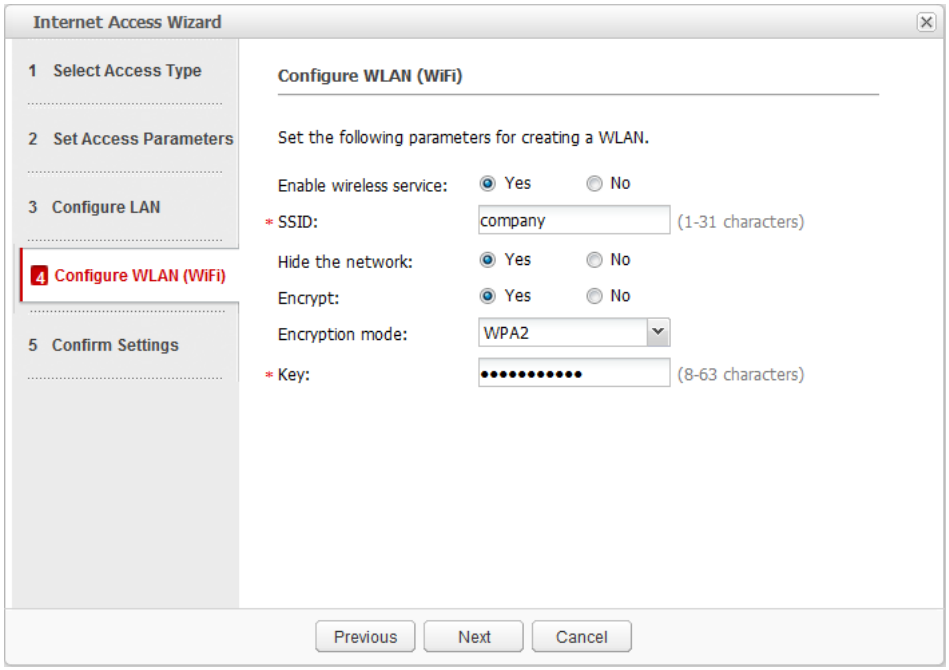
NOTE

The **Configure WLAN (WiFi)** tab page is displayed when the router supports WLAN.

By default, users are added to VLAN1 when a WLAN established through the configuration wizard on the web platform.

1. Set parameters on the **Configure WLAN (WiFi)** tab page. The parameters are as described in **Table 2-10**. **Figure 2-31** shows **Configure WLAN (WiFi)** page.
2. Click **Next**.

Figure 2-31 Configure WLAN (WiFi)



 Copyright © Huawei Technologies Co., Ltd.

Table 2-10 Configuring the WLAN (Wi-Fi)

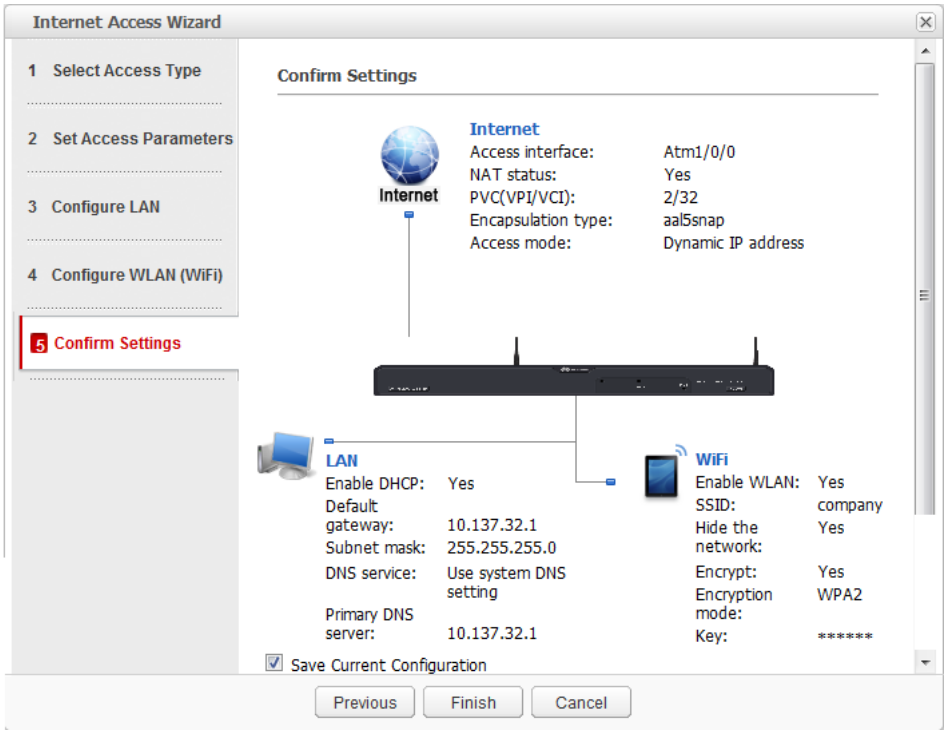
Parameter	Description
Enable wireless service	Whether to enable the WLAN service. After WLAN is enabled, you can configure basic parameters and security options for the WLAN so that wireless users can access the Internet.
SSID	Service set identifier (SSID) that uniquely identifies a WLAN. A station (STA) scans all WLANs and selects one based on the SSID.
Hide the network	Whether to add SSIDs into Beacon frames. By default, the Beacon frames contain SSIDs. If the Beacon frames do not contain SSIDs, users must configure the SSIDs on STAs. **NOTE** Only super administrators at levels 3 to 15 can check and configure this parameter.
Encrypt	Whether to encrypt the WLAN service.
Encryption mode	The following encryption algorithms are supported: • WEP • WPA • WPA2 • WAPI
Key	Configured password.

Step 5 Confirm the settings.

1. Click **Save Current Configuration** on the **Confirm Settings** tab page where detailed information about Internet access is displayed. **Figure 2-32** shows **Confirm Settings** page.

Copyright © Huawei Technologies Co., Ltd.

Figure 2-32 Confirm Settings



2. Click **Finish**.

----End

2.10.2 IPSec VPN Configuration Wizard

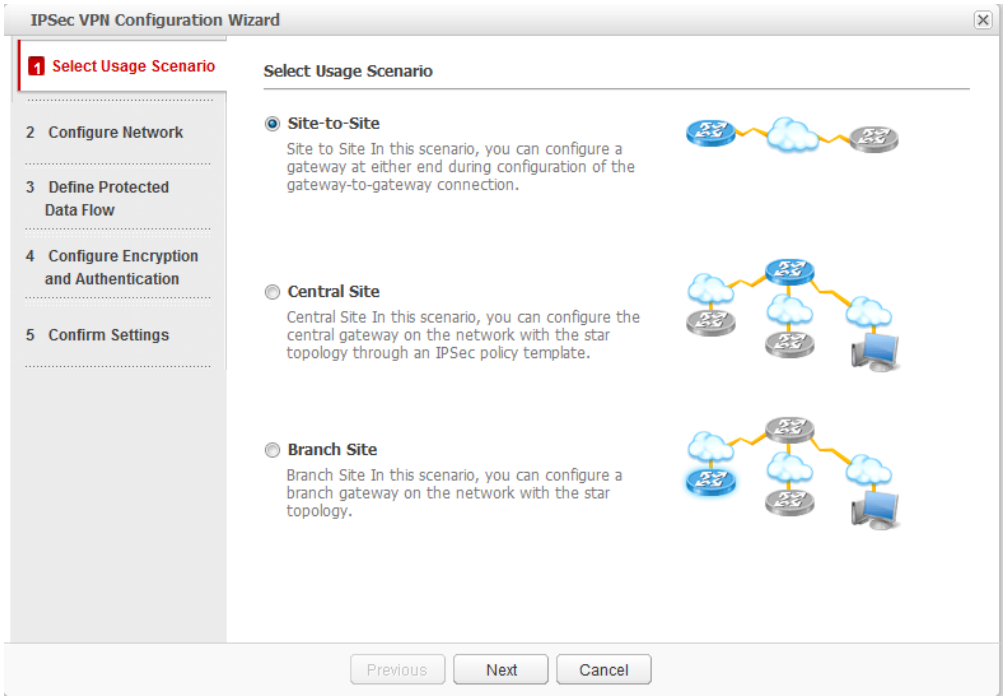
Procedure

Step 1 Select a usage scenario.

1. Choose **Configuration Wizard** > **IPSec VPN Configuration Wizard**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-33 IPSec VPN Configuration Wizard



2. Select one from the usage scenarios listed as follows:
   - **Site-to-Site**

     Select **Site-to-Site** when both the local device and the peer device can function as the initiator. Parameters on the local and peer devices must be the same.
   - **Central Site**

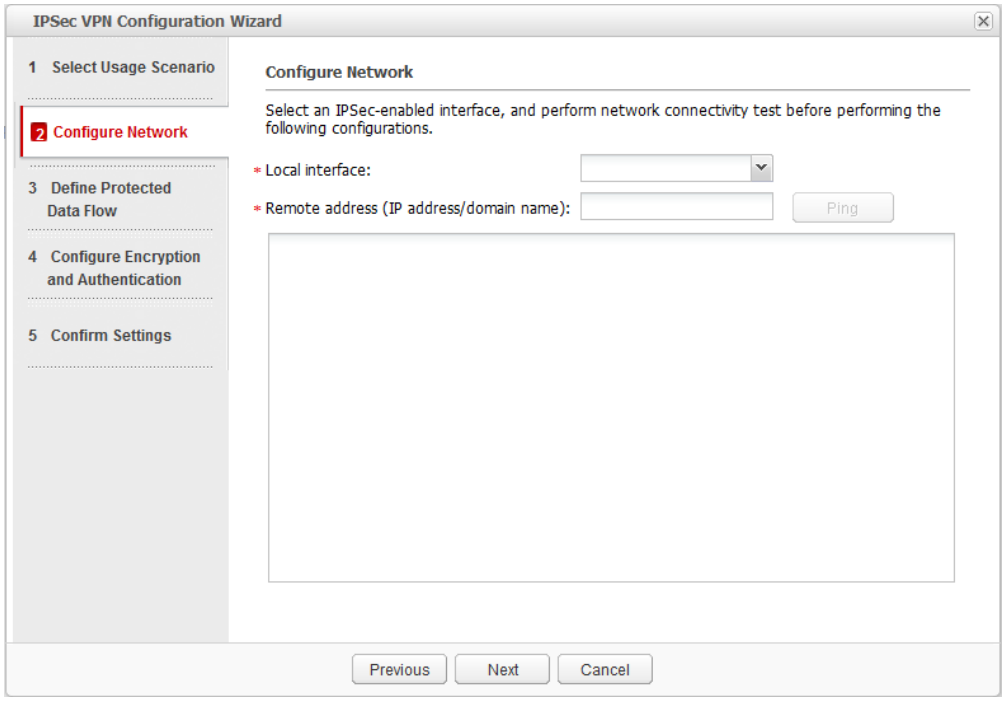
     Select **Central Site** when the peer device has no fixed IP address or the IP address is unknown. In this scenario, the local device functions as the responder to respond to negotiation request initiated by the peer device.
   - **Branch Site**

     Select **Branch Site** when the local device actively sets up an IPSec tunnel with the **Central Site**. In this scenario, the local device functions as the initiator.
3. Click **Next**.

Step 2 Configure the network.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-34 Configure the network



1. Configure the interface where the IPSec policy is applied and determine the outbound interface for data flows protected by IPSec.
2. Configure the IP address or domain name for the peer device and click **Ping** to test network connectivity.

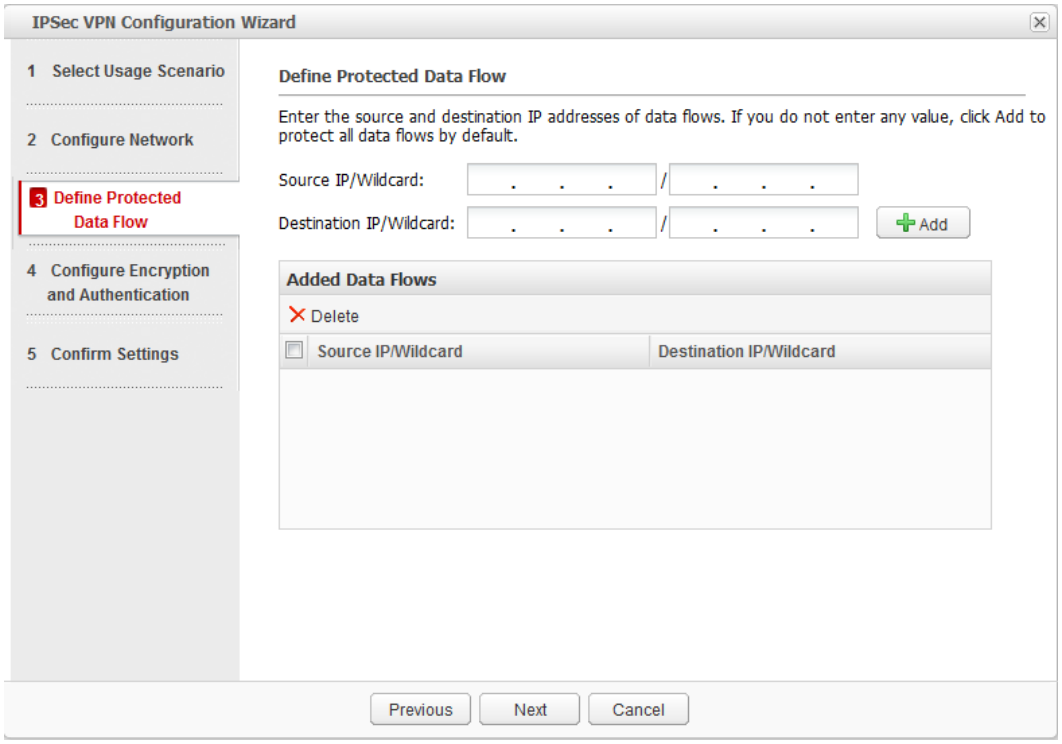
   NOTE

   This step is not required when you select **Central Site**.
3. Click **Next**.

Step 3 Define the protected data flow.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-35 Define the protected data flow



NOTE

This step is optional when you select **Central Site**.

1. Enter the source IP address, destination IP address, and wildcards of source and destination IP addresses of a protected data flow. If this parameter is not specified, any data flow can be used as the protected data flow.

   Configurations on the local and peer devices must mirror each other.

   NOTE

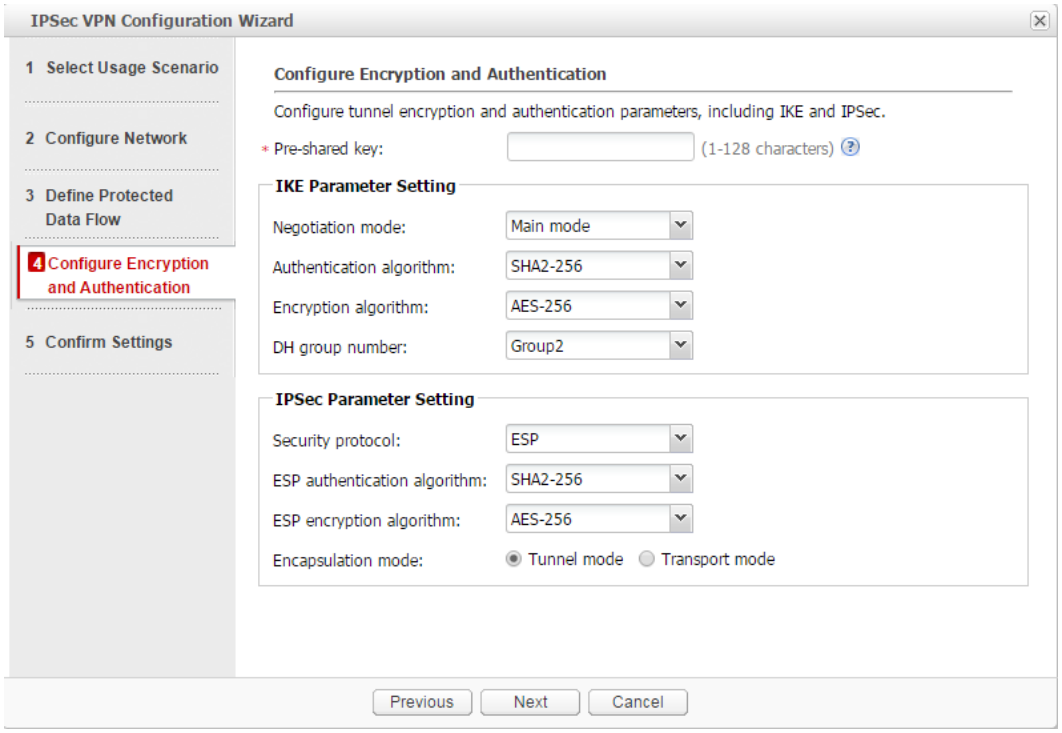
   You can define multiple data flows that are protected by IPSec.

2. Click **Next**.

Step 4 Configure encryption and authentication.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-36 Configure encryption and authentication



To ensure successful IPSec negotiation, configurations of the following parameters must be the same on the local and peer devices.

1. Configure the pre-shared key. The value is a string of characters, it contains 1 to 128 characters. If the character string contains question mark (?) or space, you need to put the key in double quotation marks ("). The local and remote ends of IKE negotiation must be configured with the same authenticator.
2. Configure IKE parameters shown in **Table 2-11**.

   Internet Key Exchange (IKE) provides the functions of key negotiation and SA establishment to simplify IPSec usage and management. After IPSec peers establish an IKE SA and complete identity authentication and key exchange, they negotiate a pair of IPSec SAs based on security parameters such as AH or ESP. Then data exchanged between the IPSec peers is encrypted and transmitted over the IPSec tunnel.

 Copyright © Huawei Technologies Co., Ltd.

Table 2-11 IKE parameter settings

Parameter	Description
Negotiation mode	The negotiation mode for IKEv1 negotiation phase 1. – Main mode: The main mode encrypts identity information to improve security. However, the negotiation speed is slow. – Aggressive mode: Compared with the main mode, the aggressive mode establishes an IKE SA more quickly. However, the aggressive mode does not encrypt identity information.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Authentication algorithm	The authentication algorithm used by IKE. – SHA1: The SHA-1 algorithm uses a 160-bit key. – MD5: The MD5 algorithm uses a 128-bit key. – AES-XCBC-MAC-96: The AES-XCBC-MAC-96 algorithm uses a 128-bit key. **NOTE** The AES-XCBC-MAC-96 algorithm only supports in IKEv2. The AES-XCBC-MAC-96 algorithm does not supported in V200R010C10 and later versions. – SHA2-256: The SHA2-256 algorithm uses a 256-bit key. – SHA2-384: The SHA2-384 algorithm uses a 384-bit key. – SHA2-512: The SHA2-512 algorithm uses a 512-bit key. – SM3: The SM3 algorithm uses a 256-bit key. **NOTE** The SM3 algorithm only supports in IKEv1. The authentication algorithm and encryption algorithm of ESP cannot be kept blank simultaneously. Note that MD5 and SHA1 authentication algorithms cannot ensure security. You are advised to use another authentication algorithm.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Encryption algorithm	The encryption algorithm used by IKE. – 3DES: The 3DES algorithm uses a 168-bit key. – AES–128: The AES–128 algorithm uses a 128-bit key. – AES–192: The AES–192 algorithm uses a 192-bit key. – AES–256: The AES–256 algorithm uses a 256-bit key. – DES: The DES algorithm uses a 56-bit key. – SM1: SM1 encryption algorithm. – SM4: SM4 encryption algorithm. Note that 3DES and DES encryption algorithms cannot ensure security. You are advised to use another encryption algorithm.
DH group number	The Diffie-Hellman group used in IKE negotiation. – Group1: Group1 uses the 768-bit Diffie-Hellman group. – Group2: Group2 uses the 1024-bit Diffie-Hellman group. – Group5: Group5 uses the 1536-bit Diffie-Hellman group. – Group14: Group14 uses the 2048-bit Diffie-Hellman group. – Group19: Group19 uses the 256-bit ECP Diffie-Hellman group. – Group20: Group20 uses the 384-bit ECP Diffie-Hellman group. – Group21: Group21 uses the 521-bit ECP Diffie-Hellman group.

3. Configure IPSec parameters shown in **Table 2-12**.

Copyright © Huawei Technologies Co., Ltd.

Table 2-12 IPSec parameter settings

Parameter	Description
Security protocol	A security protocol used by IPSec. – AH: Authentication Header (AH) only authenticates packets. – ESP: Encapsulating Security Payload (ESP) can encrypt/ authenticate, or encrypt and authenticate packets. – AH–ESP: AH authenticates packets, and ESP can encrypt and authenticate packets.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
AH authentication algorithm	AH provide data origin authentication and data integrity check. – MD5: The MD5 algorithm uses a 128-bit key. – SHA1: The SHA1 algorithm uses a 160-bit key. – SHA2–256: The SHA2–256 algorithm uses a 256-bit key. – SHA2–384: The SHA2–384 algorithm uses a 384-bit key. – SHA2–512: The SHA2–512 algorithm uses a 512-bit key. – SM3: The SM3 algorithm uses a 256-bit key. **NOTE** 1. The SM3 algorithm only supports in IKEv1. Note that MD5 and SHA1 authentication algorithms cannot ensure security. You are advised to use another authentication algorithm. **NOTE** AR100&AR120 series, AR161, AR161W, AR161EW, AR161EW-M1, AR161G-L, AR161G-Lc, AR161G-U, AR169, AR169G-L, AR169CVW, AR169CVW-4B4S, AR169W, AR169W-P-M9, AR169RW-P-M9, AR169EW, AR169EGW-L, AR1220C, AR1220-8GE, AR2204-27GE, AR2204E-D-27GE, AR2204-24GE, AR2204-27GE-P, AR2204-48GE-P, AR2204-51GE, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D, AR2204XE, and AR2204XE-DC do not support SHA2-384 and SHA2-512 authentication algorithms.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
ESP authentication algorithm	ESP provide data origin authentication and data integrity check. – Non-authentication – MD5: The MD5 algorithm uses a 128-bit key. – SHA1: The SHA1 algorithm uses a 160-bit key. – SHA2–256: The SHA2–256 algorithm uses a 256-bit key. – SHA2–384: The SHA2–384 algorithm uses a 384-bit key. – SHA2–512: The SHA2–512 algorithm uses a 512-bit key. – SM3: The SM3 algorithm uses a 256-bit key. **NOTE** 1. The SM3 algorithm only supports in IKEv1. 2. When configures the SM3 algorithm, the ESP encryption algorithm must select **SM1**, **SM4**, or **Non-encryption**. Note that MD5 and SHA1 authentication algorithms cannot ensure security. You are advised to use another authentication algorithm. **NOTE** AR100&AR120 series, AR161, AR161W, AR161EW, AR161EW-M1, AR161G-L, AR161G-Lc, AR161G-U, AR169, AR169G-L, AR169CVW, AR169CVW-4B4S, AR169W, AR169W-P-M9, AR169RW-P-M9, AR169EW, AR169EGW-L, AR1220C, AR1220-8GE, AR2204-27GE, AR2204E-D-27GE, AR2204-24GE, AR2204-27GE-P, AR2204-48GE-P, AR2204-51GE, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D, AR2204XE, and AR2204XE-DC do not support SHA2-384 and SHA2-512 authentication algorithms.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
ESP encryption algorithm	ESP encrypts packet payloads encryption. – •Non-encryption – DES: The DES algorithm uses a 56-bit key. – 3DES: The 3DES algorithm uses a 168-bit key. – AES–128: The AES–128 algorithm uses a 128-bit key. – AES–192: The AES–192 algorithm uses a 192-bit key. – AES–256: The AES–256 algorithm uses a 256-bit key. – SM1: SM1 encryption algorithm. – SM4: SM4 encryption algorithm. **NOTE** 1. SM1 and SM4 only support IKEv1. 2. When configures SM1 or the SM4 algorithm, the ESP certification algorithm must select **SHA1**, **SM3**, or **Non-authentication**. Note that 3DES and DES encryption algorithms cannot ensure security. You are advised to use another encryption algorithm.

Copyright © Huawei Technologies Co., Ltd.

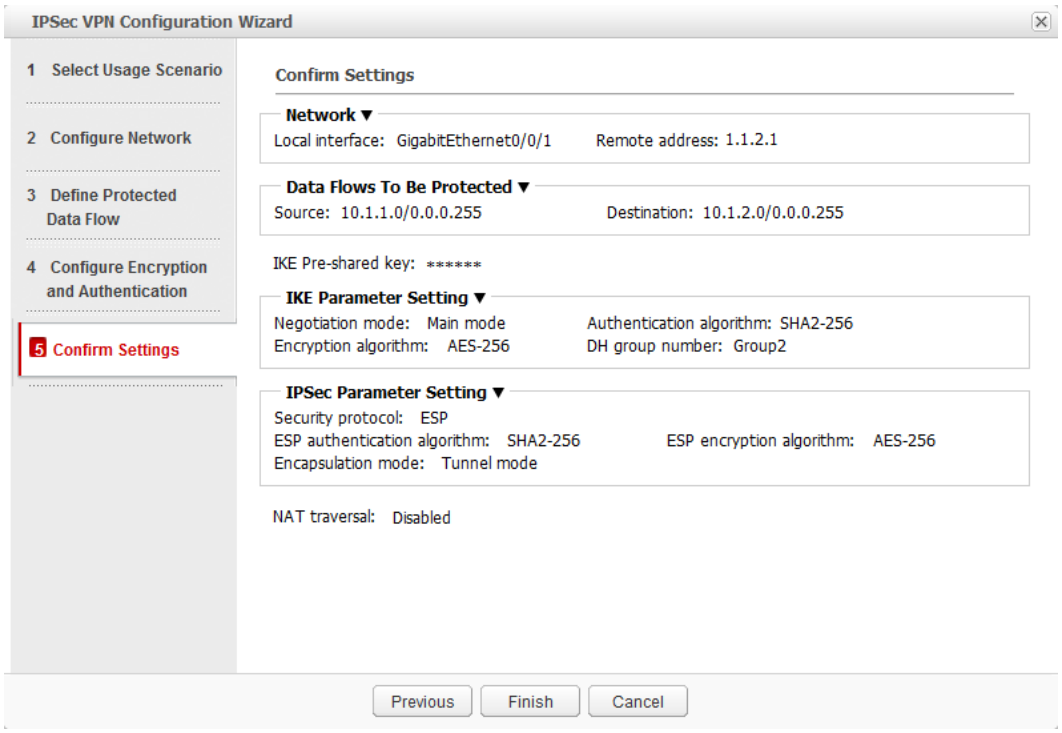
Parameter	Description
Encapsulation mode	IPSec encapsulates IP packets by adding an AH or ESP header and ESP tail to original IP packets for authentication and encryption. – Tunnel mode: An AH or ESP header is inserted before the original IP header, and the new IP header (IP address of the local device) is then inserted before the AH or ESP header. The tunnel mode shields internal host IP addresses and protects security of original data packets on an end-to-end connection. Generally, the tunnel mode is used for data encapsulation between forwarding devices. – Transport mode: An AH or ESP header is inserted between the IP header and the transport-layer protocol header. The transport mode protects the original data packet payloads. The transport mode is used for data encapsulation between hosts or between hosts and gateways.

4. Click **Next**.

Step 5 Confirm settings.

Copyright © Huawei Technologies Co., Ltd.

Figure 2-37 Confirm settings



Check the IPSec VPN configuration in details, and click **Finish**.

----End

2.10.3 Deep Security Configuration Wizard

Context

In the deep security configuration wizard, the intrusion defense policy and URL filtering policy use default settings. You can modify their settings according to your needs. For details, see **2.15.3 Deep Security**.

NOTE

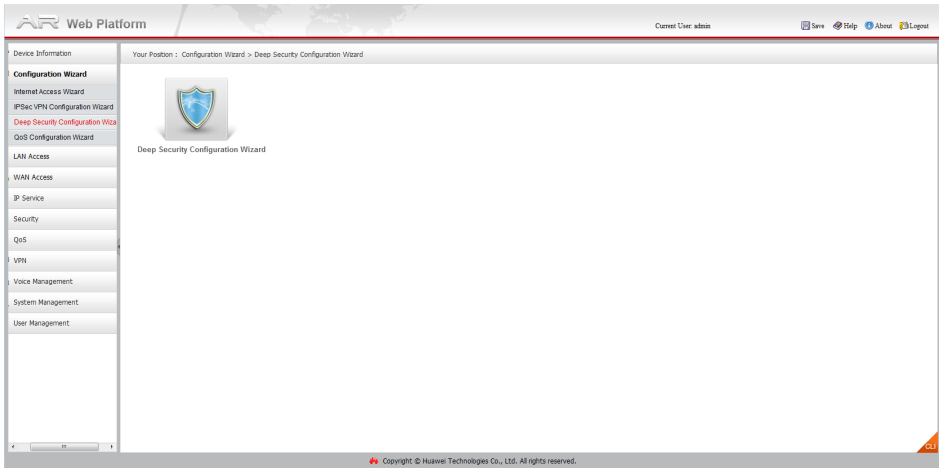
- The following product models support IPS function:
  - AR160 series: AR169BF, AR169FGW-L, AR169FGVW-L, AR169FVW-8S, AR169JFVW-4B4S, AR169JFVW-2S, AR169EGW-L, AR169EW, AR168F-4P, AR161EW, AR161EW-M1, AR161FW, AR161FV-1P, and AR169FVW.
  - AR1200 series: AR1220E, AR1220EV, and AR1220EVW.
  - AR2200 series: AR2204, AR2204XE, AR2204XE-DC, AR2220, AR2220E, AR2240, and AR2240C.
  - AR3200 series: All models.
- The following product models support URL filtering function:
  - AR100&AR120&AR150&AR160&AR200&AR3200 series: All models.
  - AR1200 series: AR1220C, AR1220-8GE, AR1220E, AR1220EV, and AR1220EVW.
  - AR2200 series: all models except AR2201-48FE, AR2202-48FE, and AR2204.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Configure Zone

1. Choose **Configuration Wizard** > **Deep Security Configuration Wizard** to open the **Deep Security Configuration Wizard** page.



2. Set **Source zone** and **Destination zone**. **Table 2-13** describes the parameters.

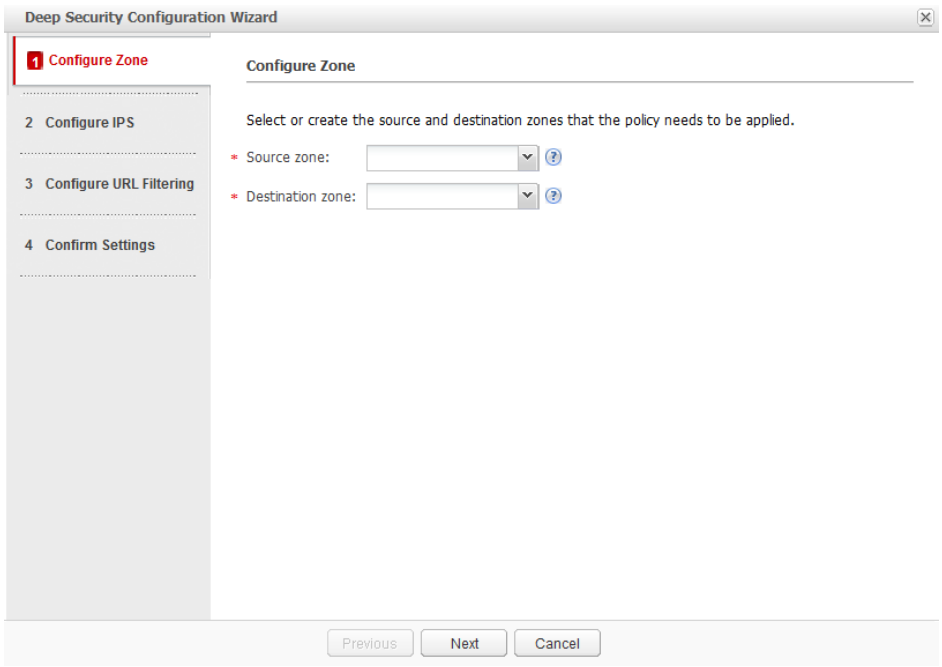


Table 2-13 Parameters for configuring zones

Parameter	Description
Source zone	Security zone from which traffic is sent, which has a high security. The source zone can be the default or user-defined security zone. For details about how to configure a security zone, see **2.15.2.1 Zone Policy**.

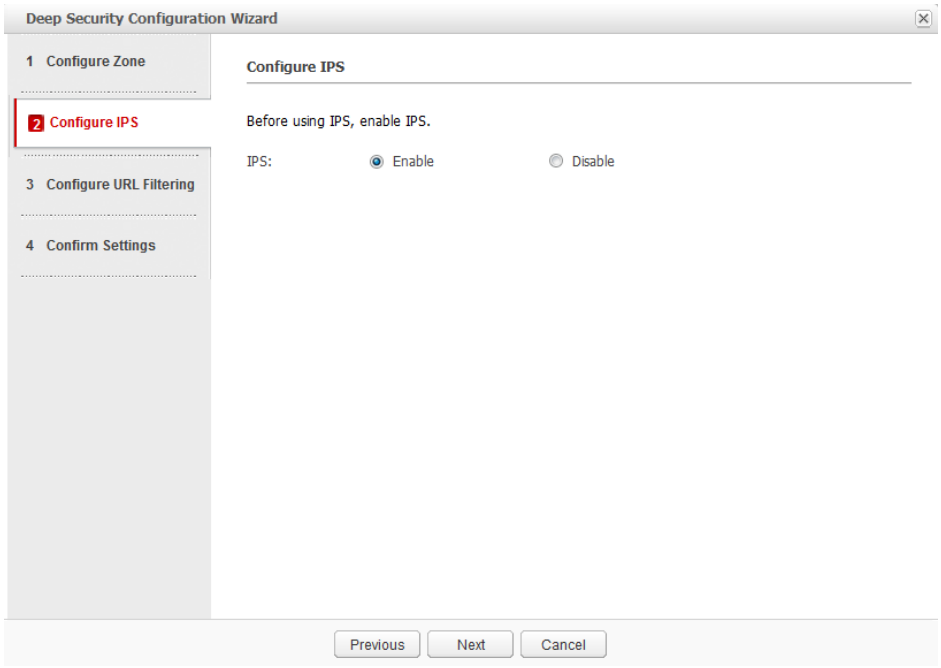
 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Destination zone	Security zone for which traffic is destined, which has a low priority. The destination zone must exist. For details about how to configure a security zone, see **2.15.2.1 Zone Policy**.

3. Click **Next**.

Step 2 Configure IPS

Click **Configure IPS**, open the **Configure IPS** page. Select **Enable** for **IPS** and click **Next**.



Step 3 Configure URL Filtering

1. Select **Enable** for **URL Filtering**.

Table 2-14 describes the parameters.

Copyright © Huawei Technologies Co., Ltd.

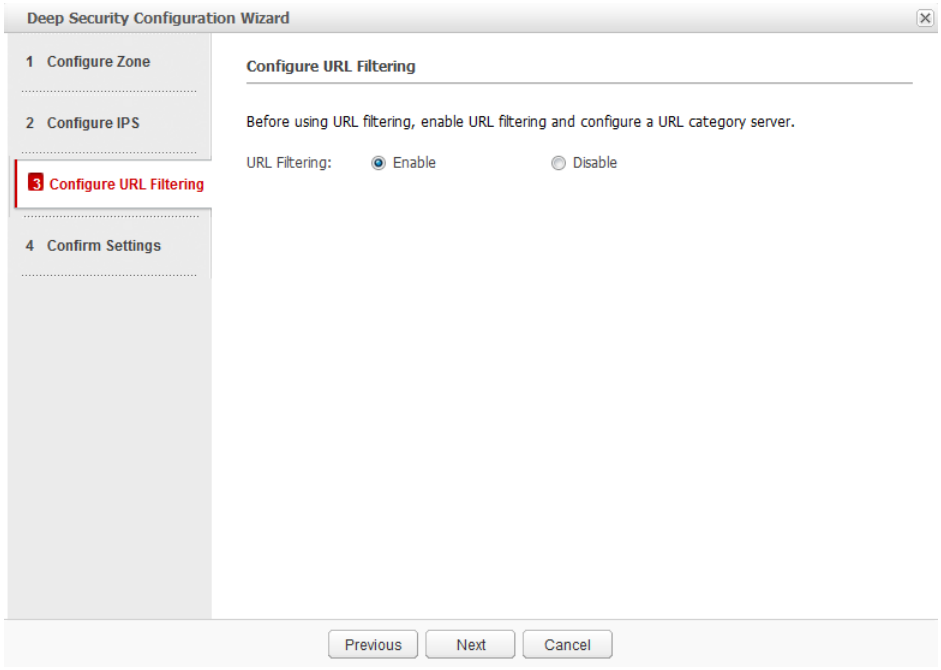
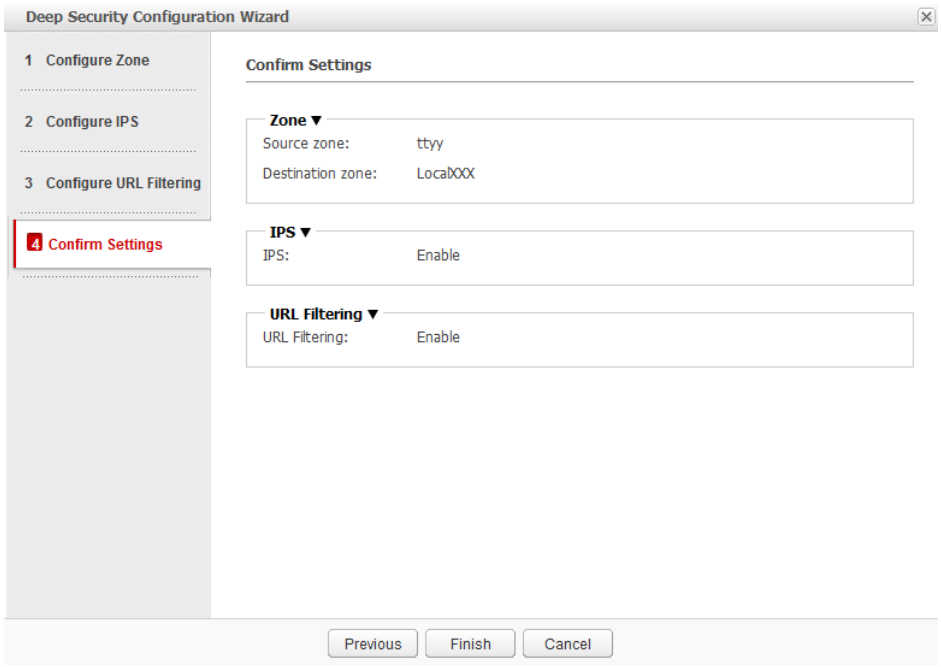


Table 2-14 Parameters for configuring URL filtering

Parameter	Description
URL Filtering	Whether the URL filtering function is enabled.

Step 4 Confirm Settings

Click **Finish**. The configuration is complete.



----End

 Copyright © Huawei Technologies Co., Ltd.

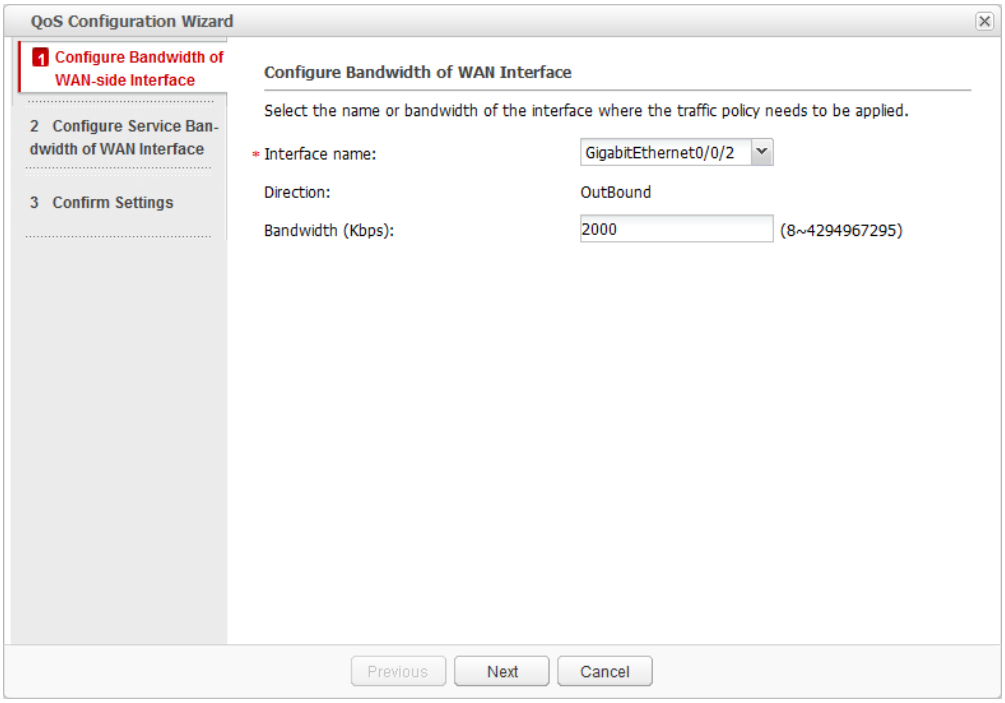
2.10.4 QoS Configuration Wizard

Procedure

Step 1 Configure rate limit on the WAN-side interface.

1. Choose **Configuration Wizard** > **QoS Configuration Wizard**.

Figure 2-38 QoS Configuration wizard page



2. Configure rate limit on the WAN-side interface, and select or set parameters according to **Table 2-15**.

Table 2-15 Description of parameters for rate limit on the WAN-side interface

Item	Description
Interface Name	Indicates the interface to which the traffic policy is applied.

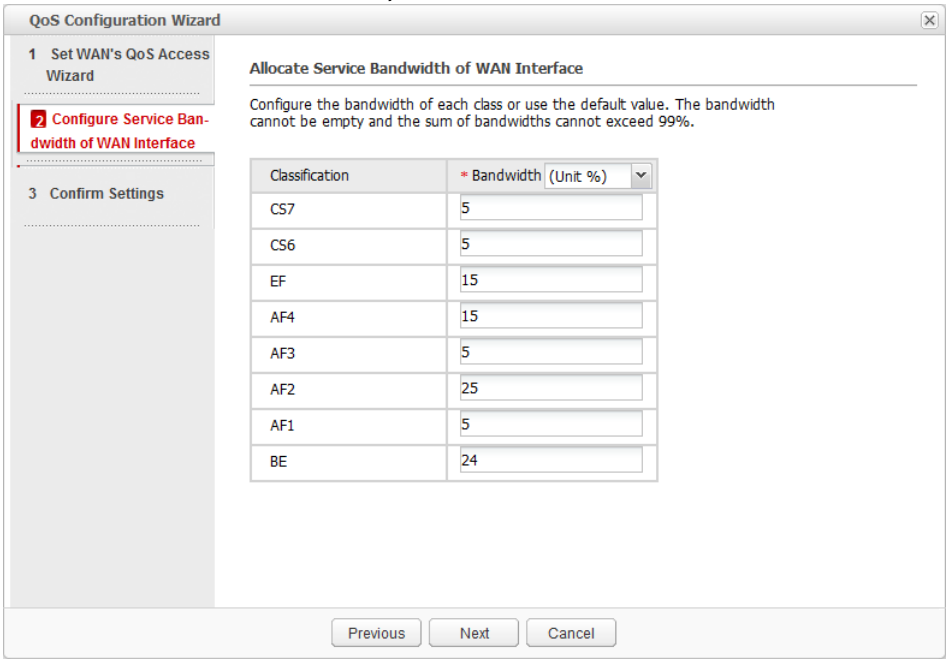
 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Direction	Indicates the direction to which the traffic policy is applied. **NOTE** This parameter cannot be modified. **OutBound** indicates the outbound direction to which the traffic policy is applied on an interface. Here, the reference bandwidth for service scheduling is configured in the outbound direction. Inbound rate limit is often configured on the upstream device, which is seldom used. Inbound rate limiting is not implemented currently.
Bandwidth (Kbps)	Specifies the available bandwidth of an interface, in kbit/s. The parameter is optional and used to shape traffic on the interface and limit the rate of outgoing packets.

3. Click **Next**.

Step 2 Configure service bandwidth of WAN interface.

1. Configure the bandwidth based on DSCP priorities. You can also use default values. The bandwidth cannot be empty and the sum of the bandwidth cannot exceed 99% of the rate limit. At least 1% of the bandwidth is allocated to the default flow queue.

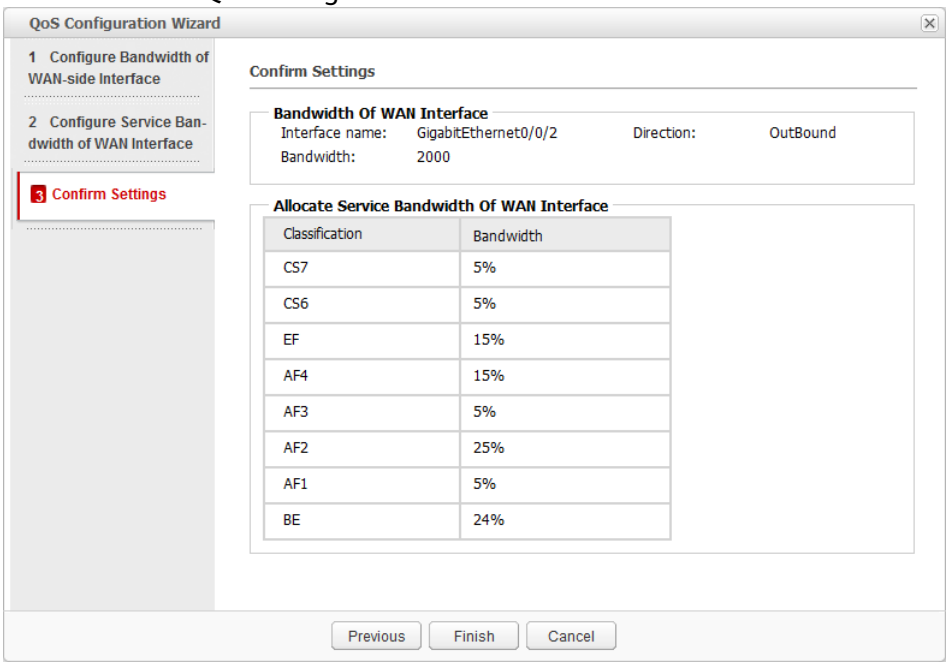


2. Click **Next**.

Step 3 Confirm the configurations.

 Copyright © Huawei Technologies Co., Ltd.

1. Check detailed QoS configurations.



2. Click **Finish**.

----End

2.11 LAN Access

2.11.1 LAN

2.11.1.1 Physical Interface

Context

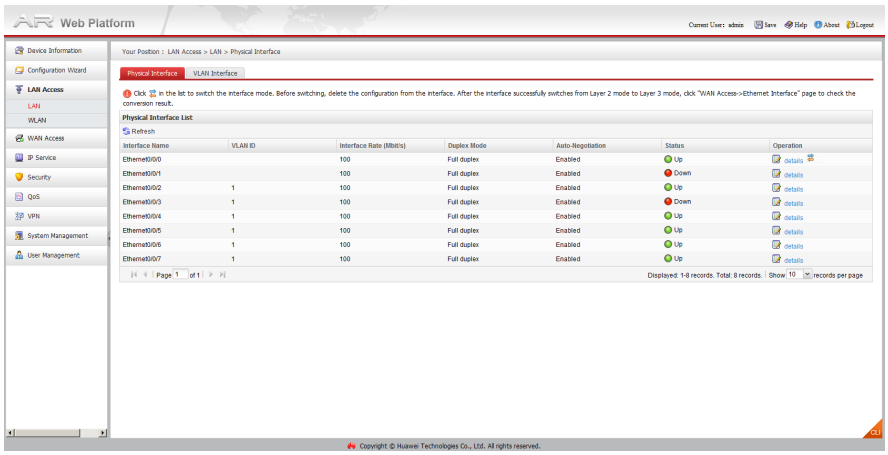
To identify an interface, you can set the description of the interface. You can query and configure physical interfaces based on the site requirements.

Procedure

- Configuring a physical interface
  a. Choose **LAN Access** > **LAN** > **Physical Interface**, as shown in **Figure 2-39**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-39 Physical interface page



b. In the **Modify Interface List** area, click  corresponding to a physical interface in the **Operation** column.

c. In the **Modify Physical Interface** dialog box, set parameters listed in **Table 2-16**.

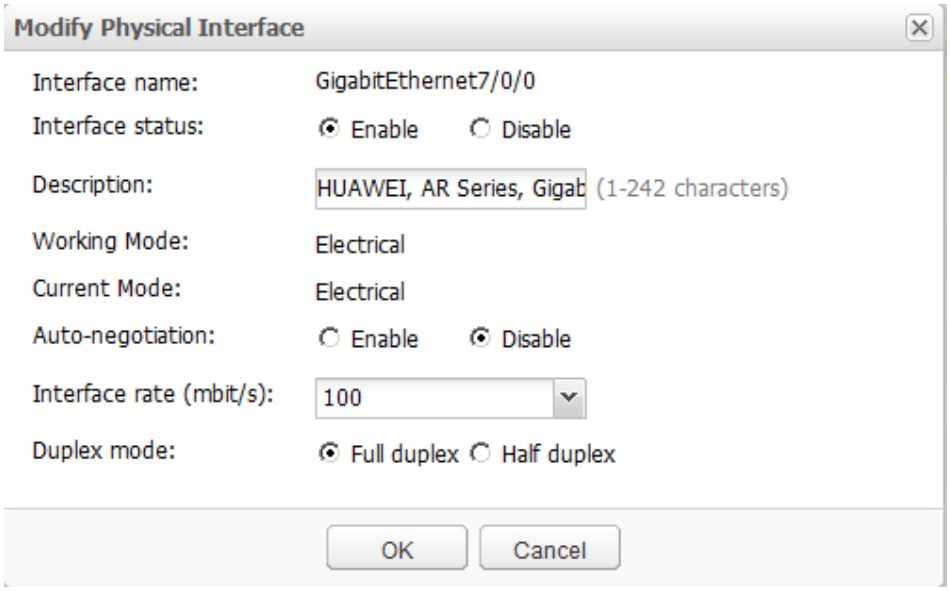


Table 2-16 Physical interface parameters

Parameter	Description
Interface name	Name of a physical interface.
Interface status	Status of a physical interface: enabled or disabled.
Description	Description of a physical interface, for example, **HUAWEI, AR Series, GigabitEthernet7/0/0 Interface**.

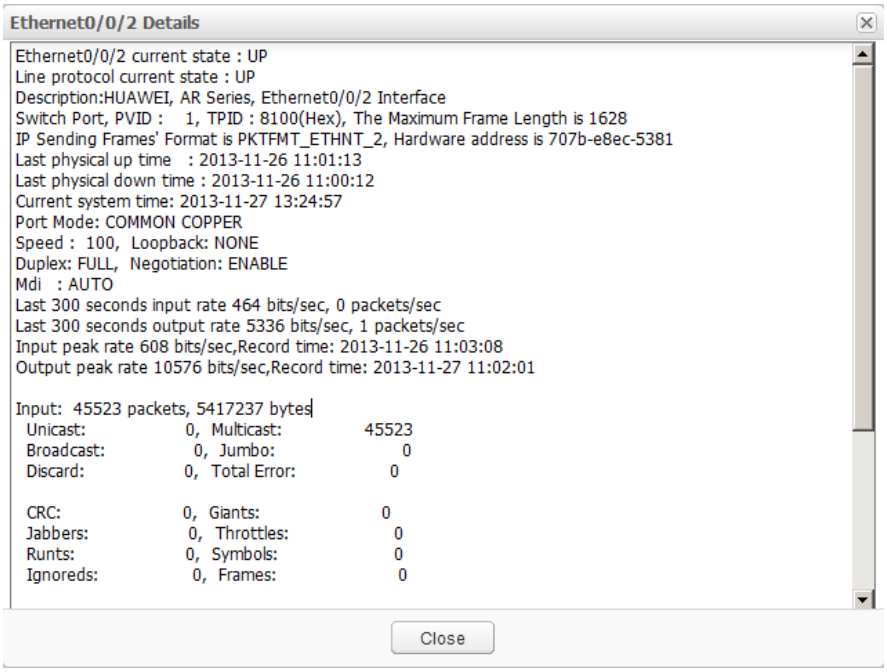
 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Working Mode	Type of a physical interface.
Current Mode	Current working mode of a physical interface.
Auto-negotiation	By default, auto-negotiation is enabled and the interface rate and duplex mode cannot be configured. If auto-negotiation is disabled, the interface rate and duplex mode can be configured.
Interface rate	Transmission of an interface, in Mbit/s.
Duplex mode	Duplex mode of an interface, including full duplex and half duplex. By default, the full duplex mode is enabled on an interface. To enable an interface to send and receive packets at the same time, enable the full-duplex mode on the interface. To disable an interface from sending and receiving packets at the same time, enable the half-duplex mode on the interface.

d. Click **OK** to save the settings.

- Viewing detailed information about a physical interface
  a. Choose **LAN Access** > **LAN** > **Physical Interface**, as shown in **Figure 2-39**.
  b. In the **Physical Interface List** area, click **details** corresponding to a physical interface in the **Operation** column to view detailed information about the physical interface.

Copyright © Huawei Technologies Co., Ltd.



- Switch a physical interface from Layer 2 mode to Layer 3 mode.

  NOTE

  Eth0/0/0 to Eth0/0/3 on the AR120 (except the AR129CV, AR129CVW, and AR129CGVW-L) and AR150 series can be changed from Layer 2 mode to Layer 3 mode.

  GE0/0/0 to GE0/0/3 on the AR100 series, AR129CV, AR129CVW, AR129CGVW-L, and AR160 series can be changed from Layer 2 mode to Layer 3 mode.

  Eth0/0/0 to Eth0/0/7 on the AR200 series, AR1220, AR1220V, AR1220W, AR1220VW, and AR1220F can be changed from Layer 2 mode to Layer 3 mode.

  GE0/0/0 to GE0/0/7 on the AR1220C, AR1220E, AR1220EV, and AR1220EVW can be changed from Layer 2 mode to Layer 3 mode.

  Eth0/0/0 and Eth0/0/47 on the AR2201-48FE and AR2202-48FE can be changed from Layer 2 mode to Layer 3 mode.

  GE0/0/3 to GE0/0/50 on the AR2204-51GE-P, AR2204-51GE-R, and AR2204-51GE can be changed from Layer 2 mode to Layer 3 mode.

  GE0/0/3 to GE0/0/26 on the AR2204-27GE-P, AR2204E-D-27GE, and AR2204-27GE can be changed from Layer 2 mode to Layer 3 mode.

  The working modes of all interfaces on the 24GE Ethernet LAN cards can be changed from Layer 2 mode to Layer 3 mode. After the reserved VLAN ID of the 9ES2 Ethernet LAN card (excluding the 9ES2 Ethernet LAN card, 8FE1GE Ethernet electrical interface card, and 4ES2G-S Ethernet LAN card installed on the AR1200 series router) is delivered using the **set reserved-vlan** command, the working modes of all interfaces on the card can be changed from Layer 2 mode to Layer 3 mode.

  AR2220E, AR2240, and AR3260 can run the **portswitch** command to change the working mode of all interfaces on the SRU200, SRU400, 4GECS, and 2X10GL from Layer 3 mode to Layer 2 mode. The interfaces that change the working mode to layer 2 only support VXLAN.

  a. Choose **LAN Access** > **LAN** > **Physical Interface**, as shown in **Figure 2-39**.

  b. In the **Physical Interface List** area, click  corresponding to a physical interface in the **Operation** column to switch the physical interface between Layer 2 and Layer 3 modes.

 Copyright © Huawei Technologies Co., Ltd.

c. In the **Information** dialog box, click **OK**. The physical interface switches from Layer 2 mode to Layer 3 mode.

NOTE

- Interfaces supporting switching between Layer 2 and Layer 3 modes cannot be used as access interfaces to connect to the AR platform. Otherwise, when an interface switches between Layer 2 and Layer 3 modes, you may fail to connect to the AR platform.
- You must delete other configuration on an interface before switching the interface between Layer 2 and Layer 3 modes.

----End

2.11.1.2 VLAN Interface

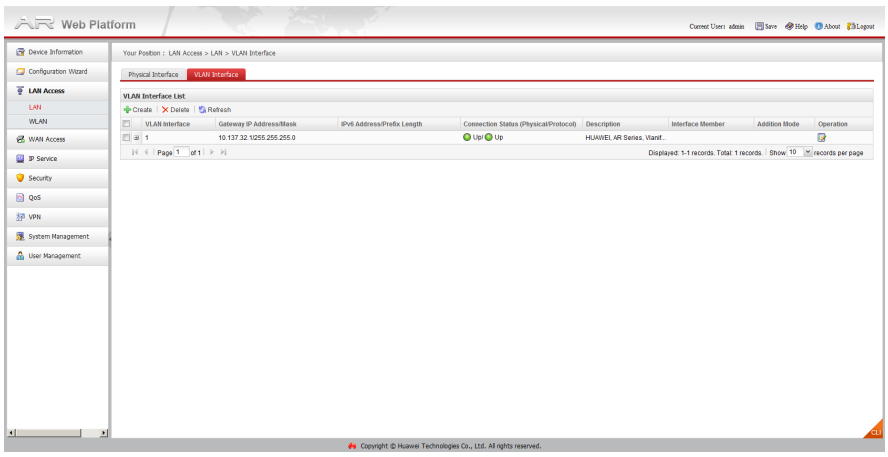
Context

Departments in different network segments need to communicate with each other. The gateway allows communication among different LANs. You can configure and enable interface-based DHCP on VLAN interfaces to dynamically set network parameters such as the IP address for departments in an enterprise, implementing communication among departments.

Procedure

- Creating a VLAN interface
  a. Choose **LAN Access** > **LAN** > **VLAN Interface**, as shown in **Figure 2-40**.

  Figure 2-40 VLAN interface configuration page

  b. In the **VLAN Interface List** area, click **Create**.
  c. In the **Create VLAN Interface** dialog box that is displayed, set parameters listed in **Table 2-17** based on the site requirements.

 Copyright © Huawei Technologies Co., Ltd.

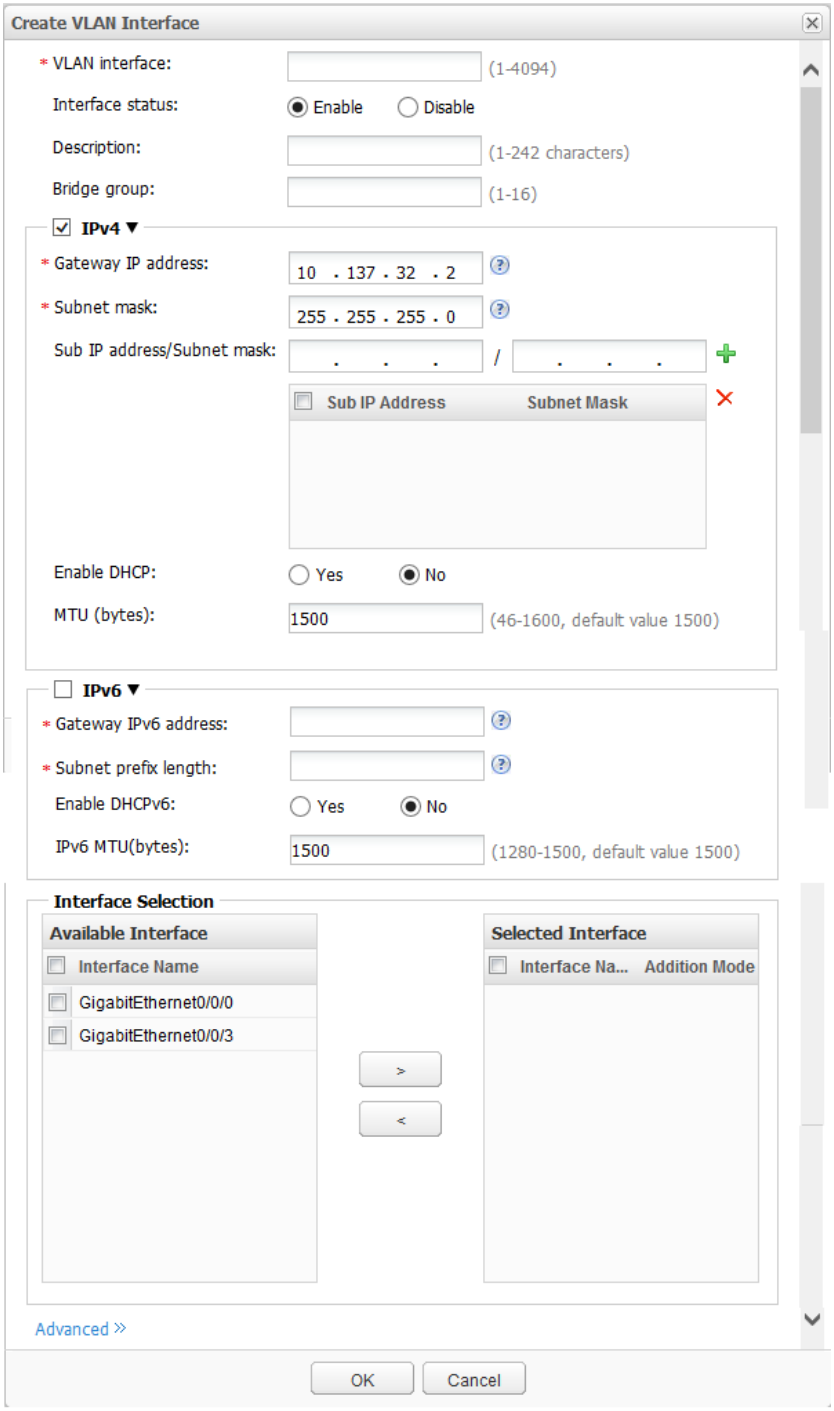


Table 2-17 VLAN interface parameters

Parameter	Description
VLAN interface	ID of a VLAN to be created.
Interface status	Status of a VLAN interface: enabled or disabled.
Description	Description of a VLAN interface, for example, **HUAWEI, AR Series, Vlanif1 Interface**.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Bridge group	Bridge group to which a VLAN interface is added.
IPv4	
Gateway IP address	IP address of a VLAN interface, that is, the default gateway IP address of the user host. **NOTE** After reserved IP addresses are added, the gateway IP address cannot be changed. To change the gateway IP address, clear all reserved IP addresses.
Subnet mask	Subnet mask of a VLAN interface. **NOTE** After reserved IP addresses are added, the subnet mask cannot be changed. To change the subnet mask, clear all reserved IP addresses.
Sub IP address/ Subnet mask	IP address and Subnet mask of a VLAN interface. **NOTE** V200R010C10 and later versions support this parameter.
Whether to enable DHCP	Whether to enable or disable the DHCP server function on a VLAN interface. After you enable the DHCP server function on a VLAN interface, users in the corresponding VLAN can obtain IP addresses from the DHCP address pool on the VLAN interface.
DNS service	DNS service for VLAN interfaces. The DNS service can be configured only when the DHCP service is enabled. You can select: • **Using system DNS setting**: DNS server IP address allocated by the system, which is the same as the gateway IP address. • **Specify**: DNS IP address specified by the user.
Primary DNS server	IP address of the primary DNS server for VLAN interfaces. This parameter is available only when **Specify** is selected.
Secondary DNS server	IP address of the secondary DNS server for VLAN interfaces. This parameter is available only when **Specify** is selected.
MTU(Bytes)	Maximum transmission unit (MTU) of a VLAN interface.
IPv6	
Gateway IP address	IP address of a VLAN interface, that is, the default gateway IPv6 address of the user host. **NOTE** After reserved IPv6 addresses are added, the gateway IPv6 address cannot be changed. To change the gateway IPv6 address, clear all reserved IPv6 addresses.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Subnet mask	Set the subnet prefix length of the IP address of the VLANIF interface.
Whether to enable DHCPv6	Whether to enable or disable the DHCPv6 server function on a VLAN interface. After you enable the DHCPv6 server function on a VLAN interface, users in the corresponding VLAN can obtain IPv6 addresses from the DHCPv6 address pool on the VLAN interface.
IPv6 DNS service	IPv6 DNS service for VLAN interfaces. The IPv6 DNS service can be configured only when the DHCPv6 service is enabled. You can select: • **Using system DNS setting**: DNS server IP address allocated by the system, which is the same as the gateway IP address. • **Specify**: DNS IP address specified by the user.
Primary IPv6 DNS server	IP address of the primary DNS server for VLAN interfaces. This parameter is available only when **Specify** is selected.
Secondary IPv6 DNS server	IP address of the secondary DNS server for VLAN interfaces. This parameter is available only when **Specify** is selected.
IPv6 MTU(Bytes)	Maximum transmission unit (MTU) of a VLAN interface.
Available Interface	Physical interfaces on the device.
Selected Interface	Physical interfaces to be added to a VLAN.
Interface name	Type and number of a Layer 2 interface.
Addition mode	Link type of an interface, including access and trunk. • access: An access interface connects to a user terminal and can join only one VLAN. • trunk: A trunk interface connects to a switching device and can join multiple VLANs.
Advanced	
Zone	A zone to which VLAN interfaces are added.
VPN instance	A VPN instance to which VLAN interfaces are added.

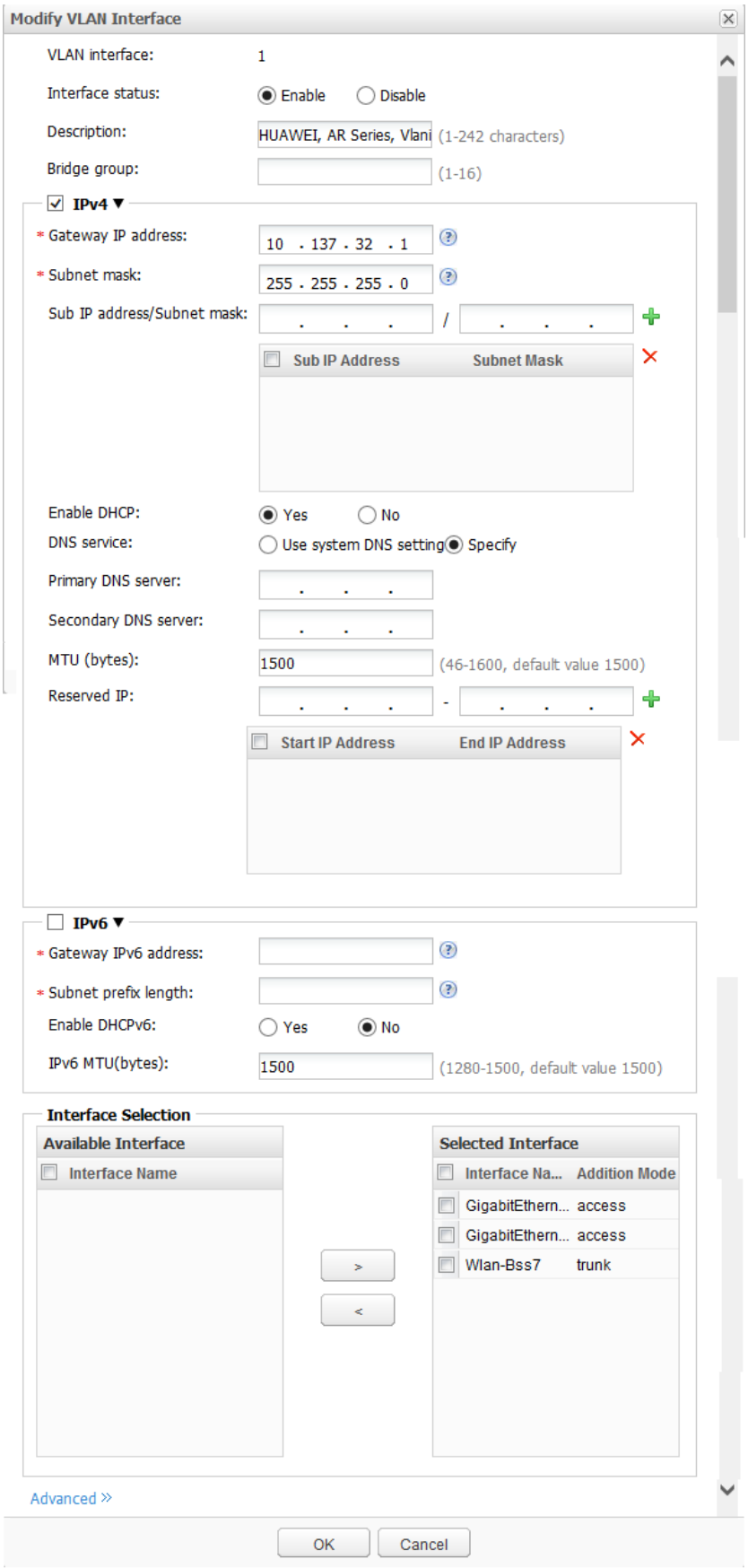
d. Click **OK** to save the settings.

To configure multiple VLAN interfaces, repeat steps 2 and 3.

 Copyright © Huawei Technologies Co., Ltd.

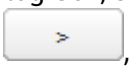
- Modifying a VLAN interface
  a. Choose **LAN Access** > **LAN** > **VLAN Interface**, as shown in **Figure 2-40**.
  b. In the **VLAN Interface List** area, select a VLAN interface, and click  .
  c. In the **Modify VLAN Interface** dialog box, modify parameters listed in **Table 2-17**. The **VLAN interface** parameter cannot be modified.

 Copyright © Huawei Technologies Co., Ltd.

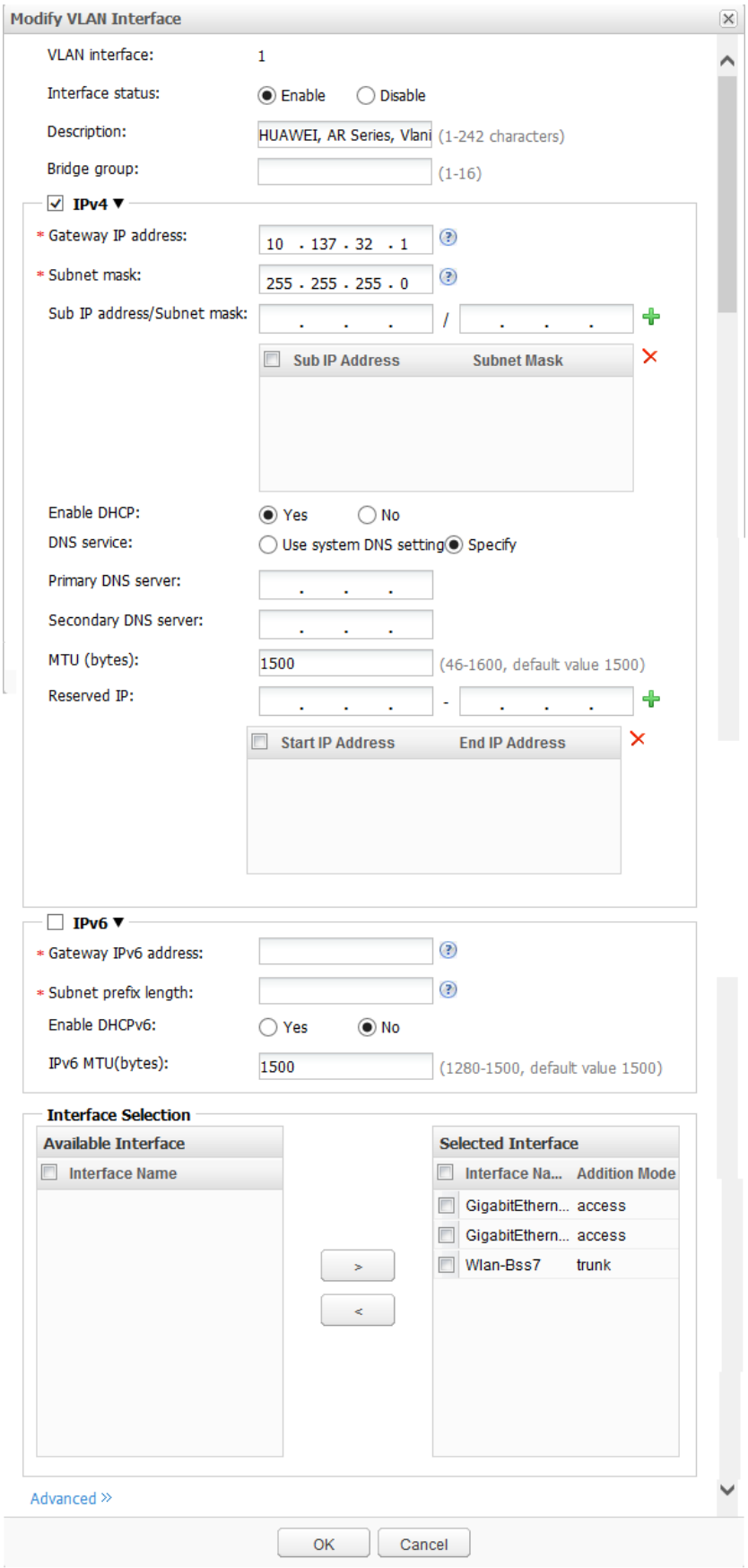


 Copyright © Huawei Technologies Co., Ltd.

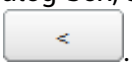
d. Click **OK** to save the settings.

- Deleting a VLAN interface
  a. Choose **LAN Access** > **LAN** > **VLAN Interface**, as shown in **Figure 2-40**.
  b. In the **VLAN Interface List** area, select a VLAN interface, and click  .
  c. In the dialog box that is displayed, click **OK**.
- Adding interfaces to a VLAN
  a. Choose **LAN Access** > **LAN** > **VLAN Interface**, as shown in **Figure 2-40**.
  b. In the **VLAN Interface List** area, select a VLAN interface, and click  .
  c. In the **Modify VLAN Interface** dialog box, select interfaces from the **Available Interface** list, and click  , and set **Addition mode** in the **Select Addition Mode** dialog box that is displayed. Click **OK**. The selected interfaces are added to the **Selected Interface** list. To move interfaces in the **Selected Interface** list back to the **Available Interface** list, select interfaces and click  . Click **OK** to add interfaces in the **Selected Interface** list to the VLAN.

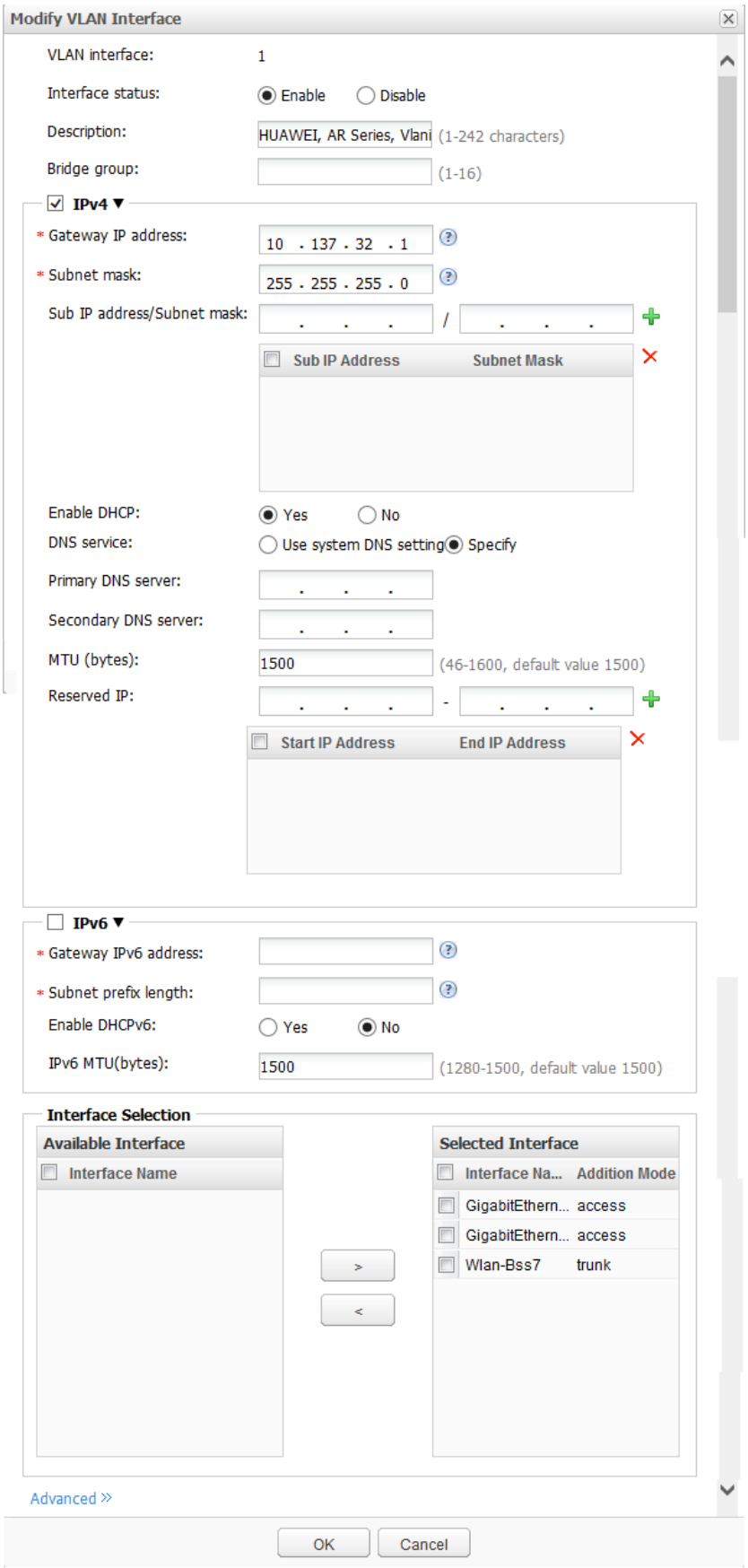
Copyright © Huawei Technologies Co., Ltd.



 Copyright © Huawei Technologies Co., Ltd.

- Changing the adding mode of an interface
  a. Choose **LAN Access** > **LAN** > **VLAN Interface**, as shown in **Figure 2-40**.
  b. In the **VLAN Interface List** area, select a VLAN interface, and click  .
  c. In the **Modify VLAN Interface** dialog box, select an interface from the **Selected Interface** list, and click  . The selected interface is moved back to the **Available Interface** list. Click  , and set **Addition mode** in the **Select Addition Mode** dialog box that is displayed. Click **OK**. The interface whose adding mode is changed is added to the **Selected Interface** list.

 Copyright © Huawei Technologies Co., Ltd.



 Copyright © Huawei Technologies Co., Ltd.

d. Click **OK** to save the settings.

----End

2.11.2 WLAN

This section describes how to configure wireless users to access a local network.

Context

A wireless local area network (WLAN) connects two or more computers or devices by using the wireless telecommunication technology to provide fast Ethernet access. It allows terminals, such as computers, to access a network through a wireless medium rather than a physical cable. This facilitates network construction and allows users to move around without interrupting communication.

Compared with a wired access network, a WLAN is easier to construct and requires lower maintenance cost. One or multiple access points (APs) can provide wireless access for a building or an area.

NOTE

WLAN is applicable only to the AR121W, AR129W, AR129CVW, AR121GW-L, AR129GW-L, AR129CGVW-L, AR109W, AR109GW-L, AR151W-P, AR156W, AR157W, AR157VW, AR158EVW, AR161W, AR161EW, AR161EW-M1, AR161FGW-L, AR161FGW-Lc, AR169W, AR161FW, AR161FW-P-M5, AR161FGW-La, AR169FVW, AR169FVW-8S, AR169JFVW-4B4S, AR169JFVW-2S, AR169CVW-4B4S, AR169EGW-L, AR169EW, AR169CVW, AR169FGVW-L, AR169FGW-L, AR169W-P-M9, AR169RW-P-M9, AR201VW-P, AR207VW, AR1220W, AR1220EVW, and AR1220VW.

The web platform does not support the SSID with spaces.

2.11.2.1 WLAN Management

Context

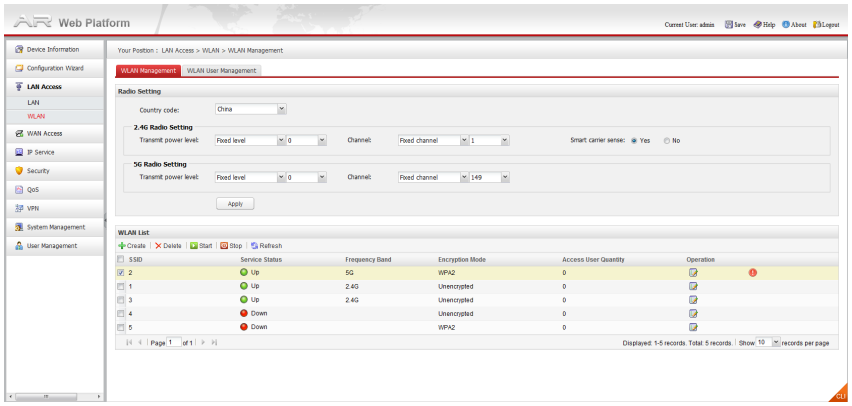
A complete WLAN configuration process includes radio setting and WLAN configuration. In the radio setting, basic radio parameters are set for a router. In WLAN configuration, WLAN is configured to provide different access services for wireless users.

Procedure

- Radio setting
  a. Choose **LAN Access** > **WLAN** > **WLAN Management**, as shown in **Figure 2-41**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-41 WLAN Management



b. In the **Radio Setting** area, set parameters listed in **Table 2-18**.

c. Click **Apply** to make the settings take effect.

Table 2-18 Radio parameters

Parameter	Description
Country code	Country code of a router.
Frequency band	Working frequency of the radio, which can be the 2.4 or 5 GHz frequency band. **NOTE** The working frequency may vary depending on the product model and local country. The actual working frequency on a device shall prevail. Configure the transmit power and working channel based on the working frequency.
Transmit power level	Maximum transmission power of the radio. • Auto: Radio output power is automatically selected according to the radio environment. • Fixed level: Output power is specified by users.

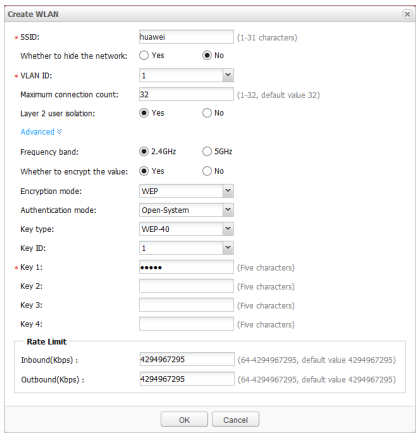
 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Channel	Channel of the radio. • Auto: Channels are automatically selected to adapt to the radio environment. • Fixed channel: Channels are specified by users. The manual mode provides an alternative way. You can use this mode if you want to avoid frequent channel adjustment, which may cause intermittent service interruption. **NOTE** You are advised to use the automatic mode because you do not need to specify a channel for each radio.
Smart carrier sense	Indicates whether to enable smart carrier receiver sensitivity adjustment. • Yes: indicates to enable smart carrier receiver sensitivity adjustment. When a large number of wireless interference sources exist in the surroundings of an AP, the access rate of STAs is decreased. This function improves the anti-interference capability of the AP. By default, this function is enabled. • No: indicates to disable carrier receiver sensitivity adjustment. **NOTE** This configuration is supported only by the AR109W, AR109GW-L, AR129CGVW-L, AR129CVW, AR169CVW-4B4S, AR169CVW operating on the 2.4 GHz band.

- WLAN configuration
  - Create a WLAN.
    i. Choose **LAN Access** > **WLAN** > **WLAN Management**.
    ii. Click **Create** in the **WLAN List** area.
    iii. In the **Create WLAN** dialog box, set WLAN basic parameters listed in **Table 2-19**, as shown in **Figure 2-42**.

Copyright © Huawei Technologies Co., Ltd.

Figure 2-42 Create WLAN



iv. Click **OK** to save the settings.

v. Select the configured WLAN, and click **Start**.

NOTE

STAs can access a local network only after WLAN is enabled.

On the **Create WLAN** page as shown in **Figure 2-42**, the value range of **Maximum connection count** varies depending on the device model. The value range for the AR129CVW, AR129CGVW-L, AR169CVW, AR169CVW-4B4S, AR109W, AR109GW-L is 1 to 32. The value range for other models is 1 to 128.

Table 2-19 WLAN parameters

Parameter	Description
SSID	Name of a WLAN.
Whether to hide the network	Whether to hide the WLAN name. • Yes: indicates that the WLAN name is hidden. • No: indicates that the WLAN name is displayed. **NOTE** Only super administrators at levels 3 to 15 can check and configure this parameter.
VLAN ID	VLAN that WLAN users belong to.
Maximum connection count	Maximum number of access users that a WLAN supports. When multiple WLANs are configured on a device, only the maximum number of access users supported by one WLAN is displayed.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Layer 2 user isolation	Whether to enable Layer 2 user isolation. • Yes: indicates that Layer 2 user isolation enabled. • No: indicates that Layer 2 user isolation is disabled. **NOTE** This parameter is supported in V200R010C10 and later versions.
Frequency band	Working frequency. **NOTE** The working frequency may vary depending on the product model and local country. The actual working frequency on a device shall prevail.
Whether to encrypt the value	Whether to enable the security policy. • Yes: indicates that the security policy is enabled. • No: indicates that the security policy is disabled.
Encryption mode	Security policy of a WLAN. WLAN security policies are as follows: • Wired Equivalent Privacy (WEP) using the RC4 algorithm • Wi-Fi Protected Access (WPA) using TKIP encryption • WPA2 using CCMP encryption • WLAN Authentication and Privacy Infrastructure (WAPI) (It is a Chinese National Standard developed based on IEEE 802.11.) **NOTE** Encryption modes may vary depending on the product module. The actual encryption mode supported by a device shall prevail. **Table 2-20** describes parameters of each encryption mode.
Inbound(Kbps)	Indicates the rate limit for packets sent from all clients to the device.
Outbound(Kbps)	Indicates the rate limit for packets sent from the device to clients.

Copyright © Huawei Technologies Co., Ltd.

Table 2-20 Parameters of each encryption mode

Encryption Mode	Parameter	Description
WEP	Authentication mode	Authentication mode when the security policy is WEP. • Open-System: WEP open authentication, that is no authentication • Share-Key: WEP shared key authentication (a WLAN client and a WLAN server must use the same shared key)
	Key type	Encryption mode, which can be WEP40 or WEP104. • WEP40: indicates that you can enter a string of 10 hexadecimal characters or 5 ASCII characters • WEP104: indicates that you can enter a string of 26 hexadecimal characters or 13 ASCII characters The key improves security of data transmission between the WLAN client and the WLAN server.
	Key ID	Key ID. You can select a key as the WEP key for encryption and decryption. Assume that you select ID 1, the key mapping ID 1 takes effect. • When WEP40 is used, enter a string of 5 characters.
	Key 1	
	Key 2	
	Key 3	

Copyright © Huawei Technologies Co., Ltd.

Encryption Mode	Parameter	Description
	Key 4	• When WEP104 is used, enter a string of 13 characters.
WPA	Authentication mode	Authentication mode when the security policy is WPA. • 802.1x: authentication using the RADIUS server and Extensible Authentication Protocol (EAP). 802.1x only controls the authentication process, and authentication protocols complete authentication. 802.1x is applicable to large enterprises with high security requirements. • PSK: Wi-Fi protected access pre-shared key (WPA-PSK) authentication mode, which does not require a dedicated authentication server. Users only need to set a pre-shared key on each WLAN node. A WLAN client can access the WLAN if its shared key is the same as that configured on the WLAN server.

Copyright © Huawei Technologies Co., Ltd.

Encryption Mode	Parameter	Description
	Encryption mode	Encryption mode used by WPA. • CCMP: Counter Mode with CBC-MAC Protocol (CCMP) uses the Advanced Encryption Standard (AES) algorithms to periodically update the key on hardware, improving WLAN security. • TKIP: Temporal key Integrity Protocol (TKIP) also uses the RC4 algorithms but it is more secure than WEP.
	Key	Pre-shared key used by PSK.

Copyright © Huawei Technologies Co., Ltd.

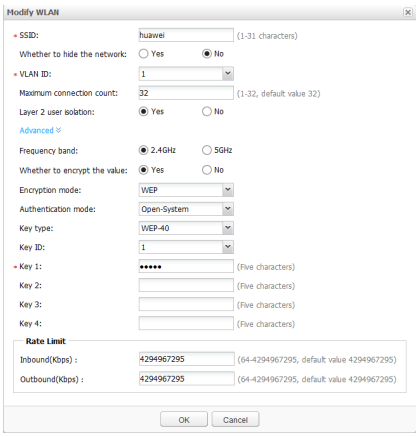
Encryption Mode	Parameter	Description
WPA2	Authentication mode	Authentication mode when the security policy is WPA2. • 802.1x: authentication using the RADIUS server and EAP. 802.1x only controls the authentication process, and authentication protocols complete authentication. 802.1x is applicable to large enterprises with high security requirements. • PSK: WPA-PSK authentication mode, which does not require a dedicated authentication server. Users only need to set a pre-shared key on each WLAN node. A WLAN client can access the WLAN if its shared key is the same as that configured on the WLAN server.
	Encryption mode	Encryption mode used by WPA. • CCMP: CCMP uses the AES algorithms to periodically update the key, improving WLAN security. • TKIP: TKIP also uses the RC4 algorithms but it is more secure than WEP.
	Key	Pre-shared key used by PSK.

Copyright © Huawei Technologies Co., Ltd.

Encryption Mode	Parameter	Description
WAPI	Authentication Mode	PSK authentication mode used by WAPI.
	Key	Pre-shared key used by PSK.

- Modifying a WLAN
  i. Choose **LAN Access** > **WLAN** > **WLAN Management**.
  ii. In the **WLAN List** area, select a WLAN, and click  .
  iii. In the **Modify WLAN** dialog box, as shown in **Figure 2-43**, set parameters listed in **Table 2-19** based on the site requirements.

  Figure 2-43 Modify WLAN

  iv. Click **OK** to save the settings.
- Deleting a WLAN
  i. Choose **LAN Access** > **WLAN** > **WLAN Management**.
  ii. In the **WLAN List** area, select a WLAN, and click **Delete**.
  iii. In the **Information** dialog box, click **OK**.

  NOTE

  If some users are connected to the WLAN to be deleted, you must click **Stop** first and then perform steps 1 to 3 to delete the WLAN.

----End

2.11.2.2 WLAN User Management

Context

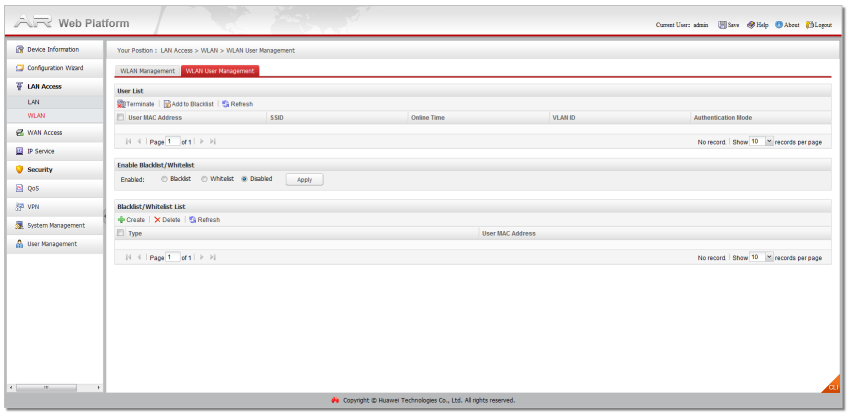
You can establish a WLAN user database on an AP to maintain user information and manage users.

On a WLAN, you can configure the STA blacklist and whitelist to control STA access. You also can add unauthorized STAs that have been connected to the WLAN to the blacklist.

Procedure

- Managing the user list
  a. Choose **LAN Access** > **WLAN** > **WLAN User Management**, as shown in **Figure 2-44**.

  Figure 2-44 WLAN User Management

  b. In the **User List** area, view all access STAs. **Table 2-21** listed user parameters.
  c. Select a STA and click **Terminate** to make the STA go offline, or click **Add to Blacklist** to forbid the STA to access the WLAN.

  NOTE

  The Enterprise administrator is not allowed to disconnect existing STAs.

  d. In the dialog box that is displayed, click **OK** to save the settings.

Table 2-21 User parameters

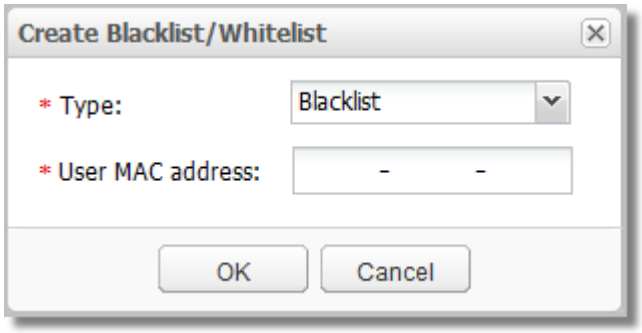
Parameter	Description
User MAC Address	MAC address of a user.
SSID	Name of the WLAN that STAs access.
Online Time	Online duration of a WLAN user.
VLAN ID	VLAN that a user belongs to.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Authentication Mode	Security policy used by a user.

- Configuring a blacklist or whitelist
  a. Choose **LAN Access** > **WLAN** > **WLAN User Management**.
  b. In the **Blacklist/Whitelist List** area, click **Create**.
  c. Set parameters listed in **Table 2-22** based on the site requirements, as shown in **Figure 2-45**.

Figure 2-45 Create Blacklist/Whitelist



  d. Click **OK** to save the settings.

     The created blacklist or whitelist is displayed in the **Blacklist/Whitelist List** area.

Table 2-22 Blacklist or whitelist parameters

Parameter	Description
Type	Access mode of WLAN users. • Blacklist: disables STAs matching MAC addresses in the blacklist from associating with an AP so that these STAs cannot access WLAN network resources. • Whitelist: enables STAs matching MAC addresses in the blacklist to associate with an AP so that these STAs can access WLAN network resources. **NOTE** If the whitelist function is enabled and the whitelist is empty, all STAs can access WLAN network resources.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
User MAC address	MAC addresses of STAs that are added to the blacklist or whitelist.

e. In the **Enable Blacklist/Whitelist** area, click **Blacklist** to enable the blacklist function; or click **Whitelist** to enable the whitelist function.

f. Click **Apply** to save the settings.

- Deleting a blacklist or whitelist

a. Choose **LAN Access** > **WLAN** > **WLAN User Management**.

b. In the **Blacklist/Whitelist List** area, select a MAC address, and click **Delete**.

c. In the dialog box that is displayed, click **OK**.

----End

Precautions

1. A blacklist takes effect only after the blacklist function is enabled.
2. A whitelist takes effect only after the whitelist function is enabled.

2.12 WAN Access

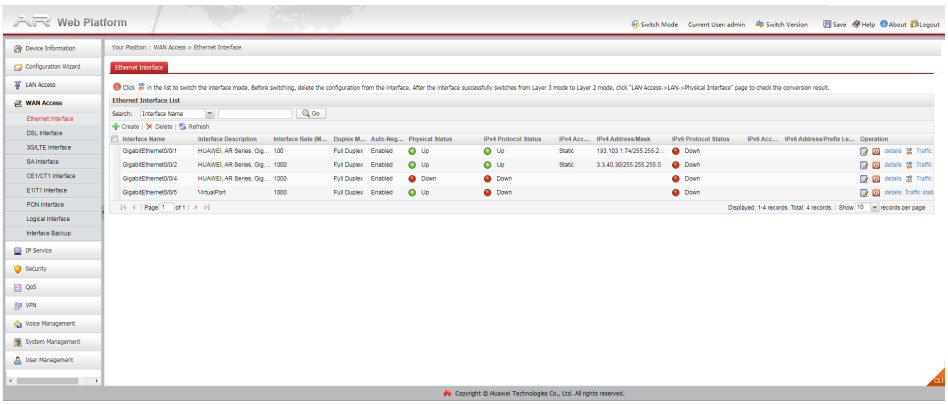
2.12.1 Ethernet Interface

Procedure

- Creating an Ethernet interface

a. Choose **WAN Access** > **Ethernet Interface**. The **Ethernet Interface** page is displayed.

Figure 2-46 Ethernet Interface page



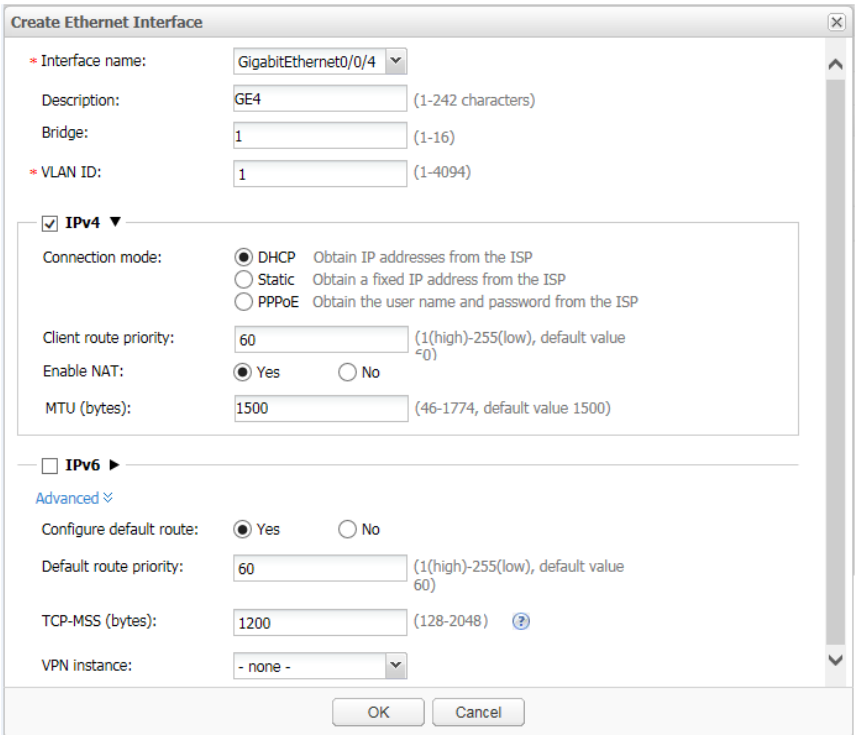
 Copyright © Huawei Technologies Co., Ltd.

b. Click **Create**. The page for creating an Ethernet interface is displayed.

c. Set the parameters described in **Table 2-23**.

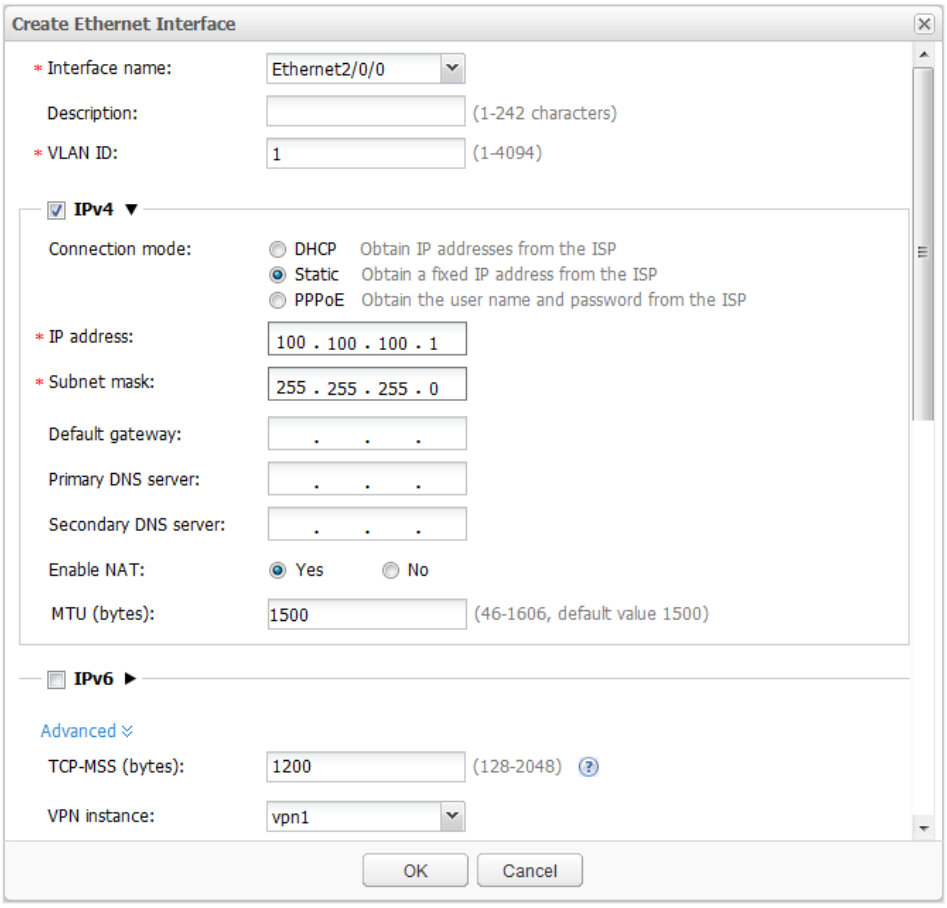
d. Click **OK**.

– **Figure 2-47** Creating an Ethernet interface (connection mode is IPv4 DHCP)



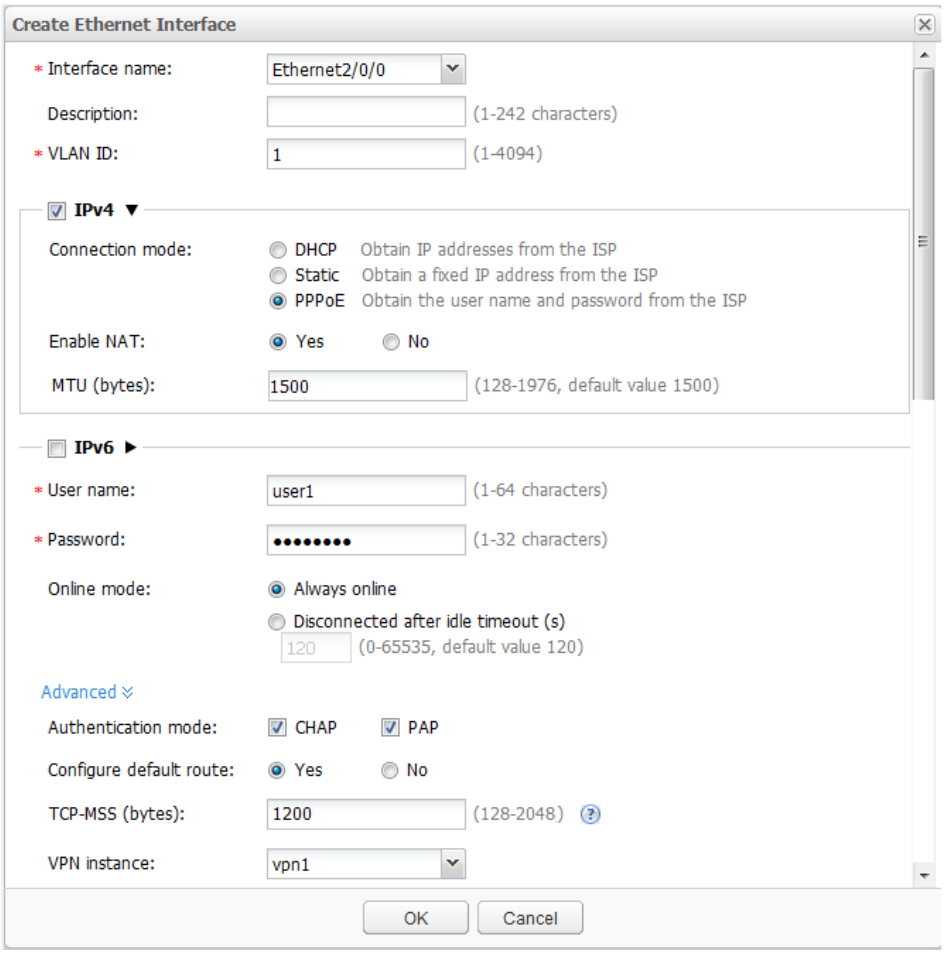
 Copyright © Huawei Technologies Co., Ltd.

– **Figure 2-48** Creating an Ethernet interface (connection mode is IPv4 Static)



 Copyright © Huawei Technologies Co., Ltd.

– **Figure 2-49** Creating an Ethernet interface (connection mode is IPv4 PPPoE)



 Copyright © Huawei Technologies Co., Ltd.

– **Figure 2-50** Creating an Ethernet interface (connection mode is IPv6 ND)

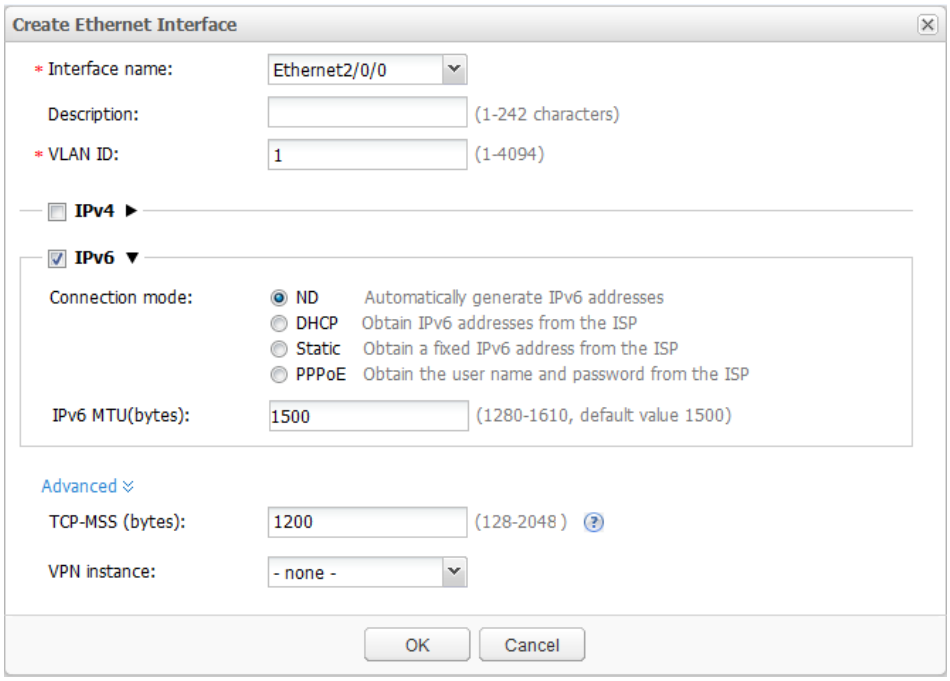


Table 2-23 Description of the Ethernet interface parameters

Parameter	Description
Interface name	Type and number of an interface. • This parameter cannot be modified when the Ethernet interface configuration is modified. • When you set the parameters for creating an Ethernet sub-interface, select the Ethernet interface for which the sub-interface needs to be created.
Description	Description of an interface. By default, the description of an interface is empty.
Bridge	ID of the Bridge-if interface that the VLAN interface joins. The value is an integer that ranges from 1 to 16.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
VLAN ID	This parameter must be specified when a user VLAN is terminated through a sub-interface. You can set this parameter only when creating an Ethernet sub-interface.
IPv4	IPv4 configuration parameters. The **Connection mode** parameter specifies the mode in which an interface obtains an IPv4 address. The options for **Connection mode** are as follows: • DHCP: indicates that the interface IPv4 address is automatically obtained using DHCP, as shown in **Figure 2-47**. For the description of DHCP parameters, see **Table 2-24**. • Static: indicates that the interface IPv4 address is manually configured, as shown in **Figure 2-48**. For the description of Static parameters, see **Table 2-25**. • PPPoE: indicates that the interface IPv4 address is obtained through PPP negotiation, as shown in **Figure 2-49**. For the description of PPPoE parameters, see **Table 2-26**. **NOTE** You must select either IPv4 or IPv6 configuration.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
IPv6	IPv6 configuration parameters. The **Connection mode** parameter specifies the mode in which an interface obtains an IPv6 address. The options for **Connection mode** are as follows: • ND: indicates that the interface IPv6 address is automatically configured. For the description of ND parameters, see **Table 2-27**. • DHCP: indicates that the interface IPv6 address is automatically obtained using DHCP. For the description of DHCP parameters, see **Table 2-28**. • Static: indicates that the interface IPv6 address is manually configured. For the description of Static parameters, see **Table 2-29**. • PPPoE: indicates that the interface IPv6 address is obtained through PPP negotiation. For the description of PPPoE parameters, see **Table 2-30**. **NOTE** You must select either IPv4 or IPv6 configuration.

Table 2-24 Description of the DHCP parameters (IPv4)

Parameter	Description
Client route priority	Priority of the routing protocol. The value is an integer that ranges from 1 to 255, and the default value is 60.
NAT status	NAT must be enabled when a PC on the private network of a LAN connects to the Internet.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
MTU (bytes)	MTU of an interface. If the MTU is set too small and the size of packets is large, packets will be broken into a great number of fragments and be discarded by QoS queues. If the MTU is too large, packets are transmitted slowly or even lost. The default value of **MTU** is 1500.
Configure default route	Whether a default route is configured.
Default route priority	Priority of the default route. The value is an integer that ranges from 1 to 255, and the default value is 60.
TCP-MSS (bytes)	MSS of TCP packets on an interface. The MSS refers to the maximum length of a TCP packet segment sent from the peer device to the local device. During TCP connection negotiation, devices at both ends record the MSS of each other. When sending TCP packets, the devices limit the size of TCP packets within the MSS. The recommended value of **TCP-MSS** is 1200.
VPN instance	VPN instance bound to an interface. **NOTE** Before setting this parameter, you must create an IPv4 VPN instance. For the detailed procedure, see **2.17.4 VPN Instance**.

Table 2-25 Description of the Static parameters (IPv4)

Parameter	Description
IP address	IP address of an interface. The interface IP address cannot conflict with the IP addresses of other interfaces on the device or other devices in the network.
Subnet mask	Subnet mask of an interface.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Default gateway	Default gateway address of an interface. The default gateway address must be in the same network segment as the interface IP address.
Primary DNS server	Primary DNS server address assigned to a DHCP client.
Secondary DNS server	Secondary DNS server address assigned to a DHCP client.
NAT status	NAT must be enabled when a PC on the private network of a LAN connects to the Internet.
MTU (bytes)	MTU of an interface. If the MTU is set too small and the size of packets is large, packets will be broken into a great number of fragments and be discarded by QoS queues. If the MTU is too large, packets are transmitted slowly or even lost. The default value of **MTU** is 1500.
TCP-MSS (bytes)	MSS of TCP packets on an interface. The MSS refers to the maximum length of a TCP packet segment sent from the peer device to the local device. During TCP connection negotiation, devices at both ends record the MSS of each other. When sending TCP packets, the devices limit the size of TCP packets within the MSS. The recommended value of **TCP-MSS** is 1200.
VPN instance	VPN instance bound to an interface. **NOTE** Before setting this parameter, you must create an IPv4 VPN instance. For the detailed procedure, see **2.17.4 VPN Instance**.

Copyright © Huawei Technologies Co., Ltd.

Table 2-26 Description of the PPPoE parameters (IPv4)

Parameter	Description
NAT status	NAT must be enabled when a PC on the private network of a LAN connects to the Internet.
MTU (bytes)	MTU of an interface. If the MTU is set too small and the size of packets is large, packets will be broken into a great number of fragments and be discarded by QoS queues. If the MTU is too large, packets are transmitted slowly or even lost. The default value of **MTU** is 1500.
User name	User name for PPPoE dial-up.
Password	Password for PPPoE dial-up.
Online mode	PPPoE dial-up mode. ● Always online: The DCC attempts to dial the remote end immediately after the device starts. The dialing process is not triggered by data packets. If a connection cannot be established with the remote end, the DCC retries at an interval. This mode applies to the scenarios in which users are not charged based on traffic or time. ● Disconnected after idle timeout (s): The device triggers the process of establishing a link only when there is data to be transmitted. When the time during which no traffic is transmitted on the link exceeds the timeout duration, the device disconnects the link to save traffic. This mode applies to the scenarios in which users are charged based on traffic or time. If this mode is used, the link idle time must be specified. The default link idle time is 120.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Authentication mode	Authentication mode for PPPoE dial-up. • PAP: Passwords are sent over links in plain text. After a PPP link is established, the authenticated device repeatedly sends the user name and password until the authentication finishes. This mode cannot ensure high security. • CHAP: a three-way handshake authentication protocol. In CHAP authentication, the authenticated device sends only the user name to the authenticating device. Compared with PAP, CHAP features higher security because passwords are not transmitted.
Configure default route	Whether to configure a default route from the local host to the PPPoE server.
TCP-MSS (bytes)	MSS of TCP packets on an interface. The MSS refers to the maximum length of a TCP packet segment sent from the peer device to the local device. During TCP connection negotiation, devices at both ends record the MSS of each other. When sending TCP packets, the devices limit the size of TCP packets within the MSS. The recommended value of **TCP-MSS** is 1200.
VPN instance	VPN instance bound to an interface. **NOTE** Before setting this parameter, you must create an IPv4 VPN instance. For the detailed procedure, see **2.17.4 VPN Instance**.

Table 2-27 Description of the ND parameters

Parameter	Description
IPv6 MTU (bytes)	MTU of an interface. The default value of **MTU** is 1500.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
TCP-MSS (bytes)	MSS of TCP packets on an interface. The MSS refers to the maximum length of a TCP packet segment sent from the peer device to the local device. During TCP connection negotiation, devices at both ends record the MSS of each other. When sending TCP packets, the devices limit the size of TCP packets within the MSS. The recommended value of **TCP-MSS** is 1200.
VPN instance	VPN instance bound to an interface. **NOTE** Before setting this parameter, you must create an IPv6 VPN instance. For the detailed procedure, see **2.17.4 VPN Instance**.

Table 2-28 Description of the DHCP parameters (IPv6)

Parameter	Description
IPv6 MTU (bytes)	MTU of an interface. The default value of **MTU** is 1500.
TCP-MSS (bytes)	MSS of TCP packets on an interface. The MSS refers to the maximum length of a TCP packet segment sent from the peer device to the local device. During TCP connection negotiation, devices at both ends record the MSS of each other. When sending TCP packets, the devices limit the size of TCP packets within the MSS. The recommended value of **TCP-MSS** is 1200.
VPN instance	VPN instance bound to an interface. **NOTE** Before setting this parameter, you must create an IPv6 VPN instance. For the detailed procedure, see **2.17.4 VPN Instance**.

Copyright © Huawei Technologies Co., Ltd.

Table 2-29 Description of the Static parameters (IPv6)

Parameter	Description
IPv6 address	IPv6 address of an interface.
Subnet prefix length	Length of the IPv6 address prefix.
IPv6 default gateway	Default gateway address of an interface.
IPv6 primary DNS server	Primary DNS server address assigned to a DHCPv6 client.
IPv6 secondary DNS server	Secondary DNS server address assigned to a DHCPv6 client.
IPv6 MTU (bytes)	MTU of an interface. The default value of **MTU** is 1500.
TCP-MSS (bytes)	MSS of TCP packets on an interface. The MSS refers to the maximum length of a TCP packet segment sent from the peer device to the local device. During TCP connection negotiation, devices at both ends record the MSS of each other. When sending TCP packets, the devices limit the size of TCP packets within the MSS. The recommended value of **TCP-MSS** is 1200.
VPN instance	VPN instance bound to an interface. **NOTE** Before setting this parameter, you must create an IPv6 VPN instance. For the detailed procedure, see **2.17.4 VPN Instance**.

Table 2-30 Description of the PPPoE parameters (IPv6)

Parameter	Description
IPv6 MTU (bytes)	MTU of an interface. The default value of **MTU** is 1500.
User name	User name for PPPoE dial-up.
Password	Password for PPPoE dial-up.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Online mode	PPPoE dial-up mode. ● Always online: The DCC attempts to dial the remote end immediately after the device starts. The dialing process is not triggered by data packets. If a connection cannot be established with the remote end, the DCC retries at an interval. This mode applies to the scenarios in which users are not charged based on traffic or time. ● Disconnected after idle timeout (s): The device triggers the process of establishing a link only when there is data to be transmitted. When the time during which no traffic is transmitted on the link exceeds the timeout duration, the device disconnects the link to save traffic. This mode applies to the scenarios in which users are charged based on traffic or time. If this mode is used, the link idle time must be specified. The default link idle time is 120.
Authentication mode	Authentication mode for PPPoE dial-up. ● PAP: Passwords are sent over links in plain text. After a PPP link is established, the authenticated device repeatedly sends the user name and password until the authentication finishes. This mode cannot ensure high security. ● CHAP: a three-way handshake authentication protocol. In CHAP authentication, the authenticated device sends only the user name to the authenticating device. Compared with PAP, CHAP features higher security because passwords are not transmitted.

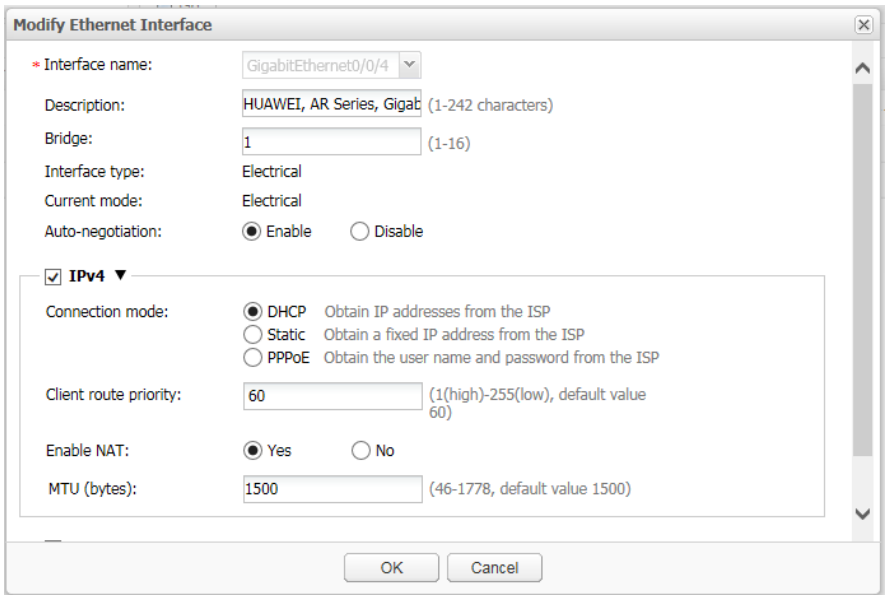
Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Configure default route	Whether to configure a default route from the local host to the PPPoE server.
TCP-MSS (bytes)	MSS of TCP packets on an interface. The MSS refers to the maximum length of a TCP packet segment sent from the peer device to the local device. During TCP connection negotiation, devices at both ends record the MSS of each other. When sending TCP packets, the devices limit the size of TCP packets within the MSS. The recommended value of **TCP-MSS** is 1200.
VPN instance	VPN instance bound to an interface. **NOTE** Before setting this parameter, you must create an IPv6 VPN instance. For the detailed procedure, see **2.17.4 VPN Instance**.

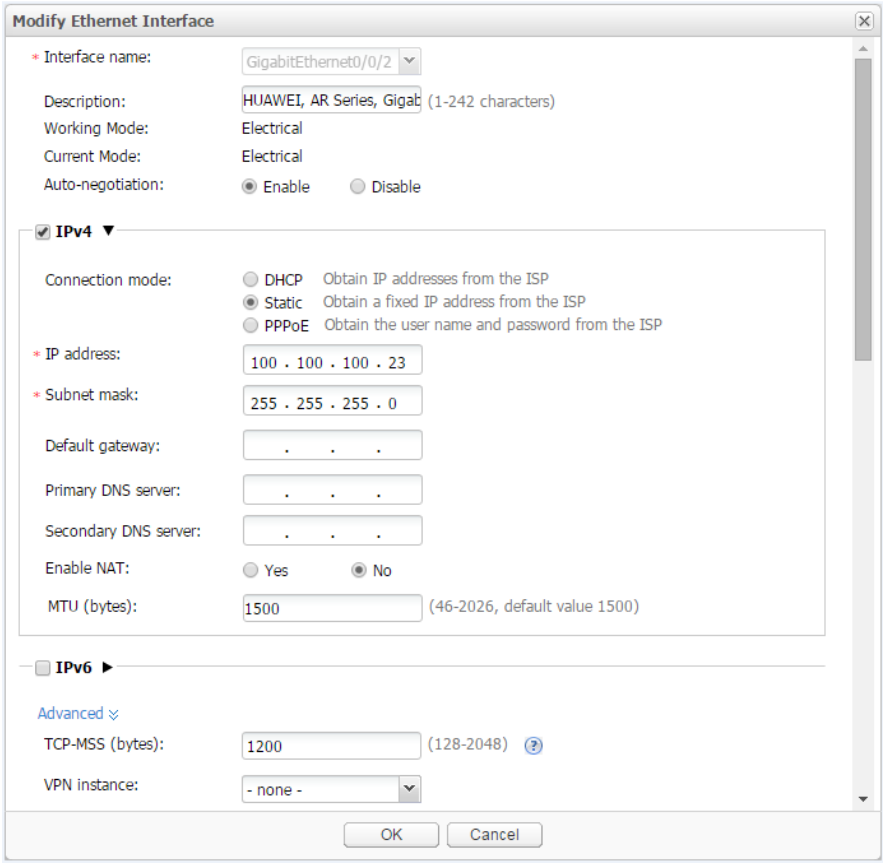
- Modifying Ethernet interface configurations
  a. Choose **WAN Access** > **Ethernet Interface**. The **Ethernet Interface** page is displayed.
  b. Click  corresponding to the Ethernet interface to be configured in the **Operation** column of **Ethernet Interface List**. The modification page is displayed.

Copyright © Huawei Technologies Co., Ltd.

- **Figure 2-51** Modifying an Ethernet Interface (connection mode is IPv4 DHCP)

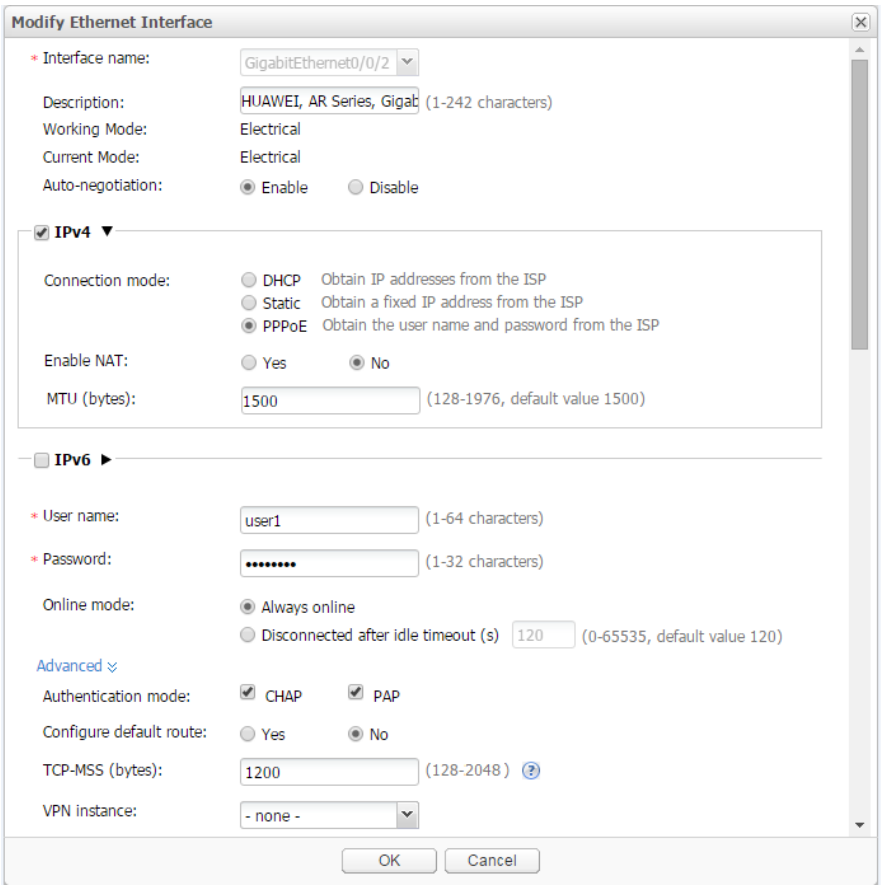


- **Figure 2-52** Modifying an Ethernet Interface (connection mode is IPv4 Static)



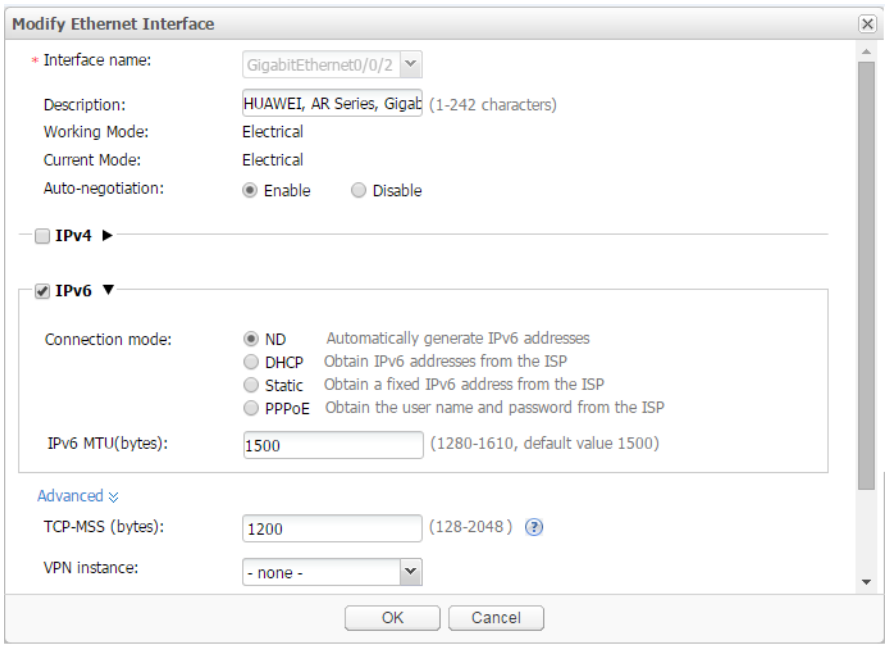
 Copyright © Huawei Technologies Co., Ltd.

- **Figure 2-53** Modifying an Ethernet Interface (connection mode is IPv4 PPPoE)



 Copyright © Huawei Technologies Co., Ltd.

- **Figure 2-54** Modifying an Ethernet Interface (connection mode is IPv6 ND)

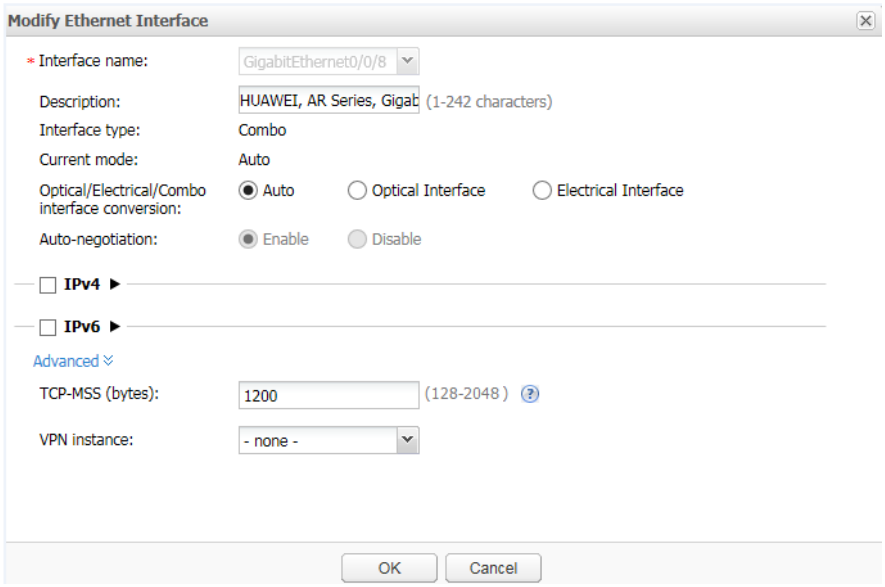


NOTE

A combo interface works in auto mode and automatically works as an optical or electrical interface by default.

Figure 2-55 shows how to change the working mode of a combo interface.

Figure 2-55 Modifying an Ethernet interface



 Copyright © Huawei Technologies Co., Ltd.

c. Set the parameters described in **Table 2-31**.

d. Click **OK**.

Table 2-31 Description of the Ethernet interface parameters

Parameter	Description
Interface name	Type and number of an interface. • This parameter cannot be modified when the Ethernet interface configuration is modified. • When you set the parameters for creating an Ethernet sub-interface, select the Ethernet interface for which the sub-interface needs to be created.
Description	Description of an interface. By default, the interface description is "HUAWEI, AR Series, interface-type interface-number Interface."
Bridge	ID of the Bridge-if interface that the VLAN interface joins. The value is an integer that ranges from 1 to 16.
Interface type	Working mode of an interface. • Combo: indicates that the current interface is a combo interface. • Optical: indicates that the current interface is an optical interface. • Electrical: indicates that the current interface is an electrical interface.
Current mode	Current working mode of an interface. • Auto: indicates that the current interface is a combo interface. • Optical: indicates that the current interface is used as an optical interface. • Electrical: indicates that the current interface is an electrical interface.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Optical/Electrical/Combo interface conversion	Working mode of a combo interface. • By default, a combo interface works in auto mode. • Optical Interface: indicates that a combo interface uses optical fibers to transmit data. • Electrical Interface: indicates that a combo interface uses network cables to transmit data.
Auto-negotiation	Whether auto negotiation is enabled on an interface.
Interface rate (Mbit/s)	Rate of an Ethernet interface in non-automatic negotiation mode.
Duplex mode	Duplex mode on an Ethernet electrical interface in non-auto-negotiation mode.
IPv4	IPv4 configuration parameters. The **Connection mode** parameter specifies the mode in which an interface obtains an IPv4 address. The options for **Connection mode** are as follows: • DHCP: indicates that the interface IPv4 address is automatically obtained using DHCP, as shown in **Figure 2-51**. For the description of DHCP parameters, see **Table 2-32**. • Static: indicates that the interface IPv4 address is manually configured, as shown in **Figure 2-52**. For the description of Static parameters, see **Table 2-33**. • PPPoE: indicates that the interface IPv4 address is obtained through PPP negotiation, as shown in **Figure 2-53**. For the description of PPPoE parameters, see **Table 2-34**. **NOTE** You must select either IPv4 or IPv6 configuration.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
IPv6	IPv6 configuration parameters. The **Connection mode** parameter specifies the mode in which an interface obtains an IPv6 address. The options for **Connection mode** are as follows: • ND: indicates that the interface IPv6 address is automatically configured. For the description of ND parameters, see **Table 2-35**. • DHCP: indicates that the interface IPv6 address is automatically obtained using DHCP. For the description of DHCP parameters, see **Table 2-36**. • Static: indicates that the interface IPv6 address is manually configured. For the description of Static parameters, see **Table 2-37**. • PPPoE: indicates that the interface IPv6 address is obtained through PPP negotiation. For the description of PPPoE parameters, see **Table 2-38**. **NOTE** You must select either IPv4 or IPv6 configuration.

Table 2-32 Description of the DHCP parameters (IPv4)

Parameter	Description
Client route priority	Priority of the routing protocol. The value is an integer that ranges from 1 to 255, and the default value is 60.
NAT status	NAT must be enabled when a PC on the private network of a LAN connects to the Internet.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
MTU (bytes)	MTU of an interface. If the MTU is set too small and the size of packets is large, packets will be broken into a great number of fragments and be discarded by QoS queues. If the MTU is too large, packets are transmitted slowly or even lost. The default value of **MTU** is 1500.
TCP-MSS (bytes)	MSS of TCP packets on an interface. The MSS refers to the maximum length of a TCP packet segment sent from the peer device to the local device. During TCP connection negotiation, devices at both ends record the MSS of each other. When sending TCP packets, the devices limit the size of TCP packets within the MSS. The recommended value of **TCP-MSS** is 1200.
VPN instance	VPN instance bound to an interface. **NOTE** Before setting this parameter, you must create an IPv4 VPN instance. For the detailed procedure, see **2.17.4 VPN Instance**.

Table 2-33 Description of the Static parameters (IPv4)

Parameter	Description
IP address	IP address of an interface. The interface IP address cannot conflict with the IP addresses of other interfaces on the device or other devices in the network.
Subnet mask	Subnet mask of an interface.
Default gateway	Default gateway address of an interface. The default gateway address must be in the same network segment as the interface IP address.
Primary DNS server	Primary DNS server address assigned to a DHCP client.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Secondary DNS server	Secondary DNS server address assigned to a DHCP client.
NAT status	NAT must be enabled when a PC on the private network of a LAN connects to the Internet.
MTU (bytes)	MTU of an interface. If the MTU is set too small and the size of packets is large, packets will be broken into a great number of fragments and be discarded by QoS queues. If the MTU is too large, packets are transmitted slowly or even lost. The default value of **MTU** is 1500.
TCP-MSS (bytes)	MSS of TCP packets on an interface. The MSS refers to the maximum length of a TCP packet segment sent from the peer device to the local device. During TCP connection negotiation, devices at both ends record the MSS of each other. When sending TCP packets, the devices limit the size of TCP packets within the MSS. The recommended value of **TCP-MSS** is 1200.
VPN instance	VPN instance bound to an interface. **NOTE** Before setting this parameter, you must create an IPv4 VPN instance. For the detailed procedure, see **2.17.4 VPN Instance**.

Table 2-34 Description of the PPPoE parameters (IPv4)

Parameter	Description
NAT status	NAT must be enabled when a PC on the private network of a LAN connects to the Internet.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
MTU (bytes)	MTU of an interface. If the MTU is set too small and the size of packets is large, packets will be broken into a great number of fragments and be discarded by QoS queues. If the MTU is too large, packets are transmitted slowly or even lost. The default value of **MTU** is 1500.
User name	User name for PPPoE dial-up.
Password	Password for PPPoE dial-up.
Online mode	PPPoE dial-up mode. ● Always online: The DCC attempts to dial the remote end immediately after the device starts. The dialing process is not triggered by data packets. If a connection cannot be established with the remote end, the DCC retries at an interval. This mode applies to the scenarios in which users are not charged based on traffic or time. ● Disconnected after idle timeout (s): The device triggers the process of establishing a link only when there is data to be transmitted. When the time during which no traffic is transmitted on the link exceeds the timeout duration, the device disconnects the link to save traffic. This mode applies to the scenarios in which users are charged based on traffic or time. If this mode is used, the link idle time must be specified. The default link idle time is 120.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Authentication mode	Authentication mode for PPPoE dial-up. • PAP: Passwords are sent over links in plain text. After a PPP link is established, the authenticated device repeatedly sends the user name and password until the authentication finishes. This mode cannot ensure high security. • CHAP: a three-way handshake authentication protocol. In CHAP authentication, the authenticated device sends only the user name to the authenticating device. Compared with PAP, CHAP features higher security because passwords are not transmitted.
Configure default route	Whether to configure a default route from the local host to the PPPoE server.
TCP-MSS (bytes)	MSS of TCP packets on an interface. The MSS refers to the maximum length of a TCP packet segment sent from the peer device to the local device. During TCP connection negotiation, devices at both ends record the MSS of each other. When sending TCP packets, the devices limit the size of TCP packets within the MSS. The recommended value of **TCP-MSS** is 1200.
VPN instance	VPN instance bound to an interface. **NOTE** Before setting this parameter, you must create an IPv4 VPN instance. For the detailed procedure, see **2.17.4 VPN Instance**.

Table 2-35 Description of the ND parameters (IPv6)

Parameter	Description
IPv6 MTU (bytes)	MTU of an interface. The default value of **MTU** is 1500.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
TCP-MSS (bytes)	MSS of TCP packets on an interface. The MSS refers to the maximum length of a TCP packet segment sent from the peer device to the local device. During TCP connection negotiation, devices at both ends record the MSS of each other. When sending TCP packets, the devices limit the size of TCP packets within the MSS. The recommended value of **TCP-MSS** is 1200.
VPN instance	VPN instance bound to an interface. **NOTE** Before setting this parameter, you must create an IPv6 VPN instance. For the detailed procedure, see **2.17.4 VPN Instance**.

Table 2-36 Description of the DHCP parameters (IPv6)

Parameter	Description
IPv6 MTU (bytes)	MTU of an interface. The default value of **MTU** is 1500.
TCP-MSS (bytes)	MSS of TCP packets on an interface. The MSS refers to the maximum length of a TCP packet segment sent from the peer device to the local device. During TCP connection negotiation, devices at both ends record the MSS of each other. When sending TCP packets, the devices limit the size of TCP packets within the MSS. The recommended value of **TCP-MSS** is 1200.
VPN instance	VPN instance bound to an interface. **NOTE** Before setting this parameter, you must create an IPv6 VPN instance. For the detailed procedure, see **2.17.4 VPN Instance**.

Copyright © Huawei Technologies Co., Ltd.

Table 2-37 Description of the Static parameters (IPv6)

Parameter	Description
IPv6 address	IPv6 address of an interface.
Subnet prefix length	Length of the IPv6 address prefix.
IPv6 default gateway	Default gateway address of an interface.
IPv6 primary DNS server	Primary DNS server address assigned to an IPv6 DHCP client.
IPv6 secondary DNS server	Secondary DNS server address assigned to an IPv6 DHCP client.
IPv6 MTU(bytes)	MTU of an interface. The default value of **MTU** is 1500.
TCP-MSS (bytes)	MSS of TCP packets on an interface. The MSS refers to the maximum length of a TCP packet segment sent from the peer device to the local device. During TCP connection negotiation, devices at both ends record the MSS of each other. When sending TCP packets, the devices limit the size of TCP packets within the MSS. The recommended value of **TCP-MSS** is 1200.
VPN instance	VPN instance bound to an interface. **NOTE** Before setting this parameter, you must create an IPv6 VPN instance. For the detailed procedure, see **2.17.4 VPN Instance**.

Table 2-38 Description of the PPPoE parameters (IPv6)

Parameter	Description
IPv6 MTU(bytes)	MTU of an interface. The default value of **MTU** is 1500.
User name	User name for PPPoE dial-up.
Password	Password for PPPoE dial-up.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Online mode	PPPoE dial-up mode. ● Always online: The DCC attempts to dial the remote end immediately after the device starts. The dialing process is not triggered by data packets. If a connection cannot be established with the remote end, the DCC retries at an interval. This mode applies to the scenarios in which users are not charged based on traffic or time. ● Disconnected after idle timeout (s): The device triggers the process of establishing a link only when there is data to be transmitted. When the time during which no traffic is transmitted on the link exceeds the timeout duration, the device disconnects the link to save traffic. This mode applies to the scenarios in which users are charged based on traffic or time. If this mode is used, the link idle time must be specified. The default link idle time is 120.
Authentication mode	Authentication mode for PPPoE dial-up. ● PAP: Passwords are sent over links in plain text. After a PPP link is established, the authenticated device repeatedly sends the user name and password until the authentication finishes. This mode cannot ensure high security. ● CHAP: a three-way handshake authentication protocol. In CHAP authentication, the authenticated device sends only the user name to the authenticating device. Compared with PAP, CHAP features higher security because passwords are not transmitted.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Configure default route	Whether to configure a default route from the local host to the PPPoE server.
TCP-MSS (bytes)	MSS of TCP packets on an interface. The MSS refers to the maximum length of a TCP packet segment sent from the peer device to the local device. During TCP connection negotiation, devices at both ends record the MSS of each other. When sending TCP packets, the devices limit the size of TCP packets within the MSS. The recommended value of **TCP-MSS** is 1200.
VPN instance	VPN instance bound to an interface. **NOTE** Before setting this parameter, you must create an IPv6 VPN instance. For the detailed procedure, see **2.17.4 VPN Instance**.

- Switching an Ethernet interface from the Layer 3 mode to Layer 2 mode

  NOTE

  Eth0/0/0 to Eth0/0/3 on the AR120 (except the AR129CV, AR129CVW, and AR129CGVW-L) and AR150 series can be changed from Layer 2 mode to Layer 3 mode.

  GE0/0/0 to GE0/0/3 on the AR100 series, AR129CV, AR129CVW, AR129CGVW-L, and AR160 series can be changed from Layer 2 mode to Layer 3 mode.

  Eth0/0/0 to Eth0/0/7 on the AR200 series, AR1220, AR1220V, AR1220W, AR1220VW, and AR1220F can be changed from Layer 2 mode to Layer 3 mode.

  GE0/0/0 to GE0/0/7 on the AR1220C, AR1220E, AR1220EV, and AR1220EVW can be changed from Layer 2 mode to Layer 3 mode.

  Eth0/0/0 and Eth0/0/47 on the AR2201-48FE and AR2202-48FE can be changed from Layer 2 mode to Layer 3 mode.

  GE0/0/3 to GE0/0/50 on the AR2204-51GE-P, AR2204-51GE-R, and AR2204-51GE can be changed from Layer 2 mode to Layer 3 mode.

  GE0/0/3 to GE0/0/26 on the AR2204-27GE-P, AR2204E-D-27GE, and AR2204-27GE can be changed from Layer 2 mode to Layer 3 mode.

  The working modes of all interfaces on the 24GE Ethernet LAN cards can be changed from Layer 2 mode to Layer 3 mode. After the reserved VLAN ID of the 9ES2 Ethernet LAN card (excluding the 9ES2 Ethernet LAN card, 8FE1GE Ethernet electrical interface card, and 4ES2G-S Ethernet LAN card installed on the AR1200 series router) is delivered using the **set reserved-vlan** command, the working modes of all interfaces on the card can be changed from Layer 2 mode to Layer 3 mode.

  AR2220E, AR2240, and AR3260 can run the **portswitch** command to change the working mode of all interfaces on the SRU200, SRU400, 4GECS, and 2X10GL from Layer 3 mode to Layer 2 mode. The interfaces that change the working mode to layer 2 only support VXLAN.

Copyright © Huawei Technologies Co., Ltd.

  - Choose **WAN Access** > **Ethernet Interface**. The **Ethernet Interface** page is displayed.
  - Click  corresponding to the Ethernet interface whose mode needs to be switched in the **Operation** column of **Ethernet Interface List**.
  - Click **OK**.

  NOTE

  Choose **LAN access** > **LAN** > **Physical Interface**. Check the switching result. You can also switch the interface from Layer 2 mode to Layer 3 mode.

- Disabling an Ethernet interface or sub-interface
  a. Choose **WAN Access** > **Ethernet Interface**. The **Ethernet Interface** page is displayed.
  b. Click  corresponding to the Ethernet interface or sub-interface to be disabled in the **Operation** column of **Ethernet Interface List**.
  c. Click **OK**.
- Enabling an Ethernet interface or sub-interface
  a. Choose **WAN Access** > **Ethernet Interface**. The **Ethernet Interface** page is displayed.
  b. Click  corresponding to the Ethernet interface or sub-interface to be enabled in the **Operation** column of **Ethernet Interface List**.
  c. Click **OK**.
- Deleting an Ethernet sub-interface
  a. Choose **WAN Access** > **Ethernet Interface**. The **Ethernet Interface** page is displayed.
  b. Select the check box of the interface to be deleted and click **Delete** in the **Interface Name** column.
  c. Click **OK**.
- Viewing the bandwidth of a Layer 3 interface
  a. Choose **WAN Access** > **Ethernet Interface**. The **Ethernet Interface** page is displayed.
  b. Click **Details** of an Ethernet interface in the **Operation** column of **Ethernet Interface List**.
- Viewing the details of an Ethernet interface or Ethernet sub-interface

  NOTE

  V200R010C10 and later versions support viewing**Details**.

  a. Choose **WAN Access** > **Ethernet Interface**. The **Ethernet Interface** page is displayed.
  b. Click **Details** of an Ethernet interface or Ethernet sub-interface in the **Operation** column of **Ethernet Interface List**.
  c. Click **Close**.
- Viewing the traffic statistics of an Ethernet interface or Ethernet sub-interface

  NOTE

  V200R010C10 and later versions support viewing**Traffic statistics**.

 Copyright © Huawei Technologies Co., Ltd.

a. Choose **WAN Access** > **Ethernet Interface**. The **Ethernet Interface** page is displayed.

b. Click **Traffic statistics** of an Ethernet interface or Ethernet sub-interface in the **Operation** column of **Ethernet Interface List**.

c. Click **Close**.

----End

2.12.2 DSL Interface

Context

NOTE

- The 1ADSL-A/M and 1ADSL-B/J interface cards support ADSL interfaces. For the mapping between the device and interface card, see *1ADSL-A/M and 1ADSL-B/J (1-Port-ADSL2+ ANNEX A/M and B/J WAN Interface Card)* in the *Huawei AR Series Access Routers Get to Know the Product-Hardware Description-Cards-xDSL/xPON Interface Card*.

  Among the AR150&AR160&AR200 series, only the AR156, AR156W, AR157 series, AR206, and AR207 series support ADSL interfaces.

  The 1ADSL-A/M and 1ADSL-B/J interface cards support ADSL interfaces. For the mapping between the device and interface card, see 1ADSL-A/M (1-Port ADSL2+ ANNEX A/M WAN Interface Card) or 1ADSL-B/J (1-Port ADSL2+ ANNEX B/J WAN Interface Card) in the *Huawei AR Series Access Routers Get to Know the Product-Hardware Description-Cards-xDSL Card*.

  AR1200, AR2200 (except AR2201-48FE and AR2202-48FE), AR3200, and AR3600 series provide ADSL-A/M and ADSL-B/J boards. Only the ADSL-A/M boards support AnnexM. Only the ADSL-B/J boards support AnnexJ.

- The VDSL2 and 2VDSL2 interface cards support VDSL interfaces. For the mapping between the device and interface card, see VDSL2 (1-Port VDSL2 over POTS WAN Interface Card) or 2VDSL2 (2-Port VDSL2 over POTS with Bonding WAN Interface Card) in the *Huawei AR Series Access Routers Get to Know the Product-Hardware Description-Cards-xDSL Card*.

  The AR109, AR109W, AR109GW-L, AR129, AR129CVW, AR129CV, AR129GW-L, AR129CGVW-L, AR129W, AR169, AR169CVW, AR169CVW-4B4S, AR169EW, AR169EGW-L, AR169F, AR169BF, AR169FVW, AR169FVW-8S, AR169FGW-L, AR169G-L, AR169JFVW-4B4S, AR169JFVW-2S, AR169-P-M9, AR169W-P-M9, AR169RW-P-M9, and AR169FGVW-L support VDSL interfaces.

- The 4G.SHDSL and 1GBIS4W interface cards support PON interfaces. For the mapping between the device and interface card, see *G.SHDSL (1-Port-4-Channel G.SHDSL WAN Interface Card)* in the *Huawei AR Series Access Routers Get to Know the Product-Hardware Description-Cards-xDSL/xPON Interface Card*.

  Among the AR150&AR160&AR200 series, the AR158E, AR158EVW, only the AR168F, AR168F-4P, AR208E support G.SHDSL interfaces.

2.12.2.1 ATM

Context

The device supports the ADSL, VDSL, and G.SHDSL interface cards (together called DSL interface cards). DSL links can be used to connect the device to the Internet.

The VDSL and G.SHDSL interfaces can work in Asynchronous Transfer Mode (ATM) or Packet Transfer Mode (PTM) mode and switch between these two modes. An ADSL interface works only in ATM mode.

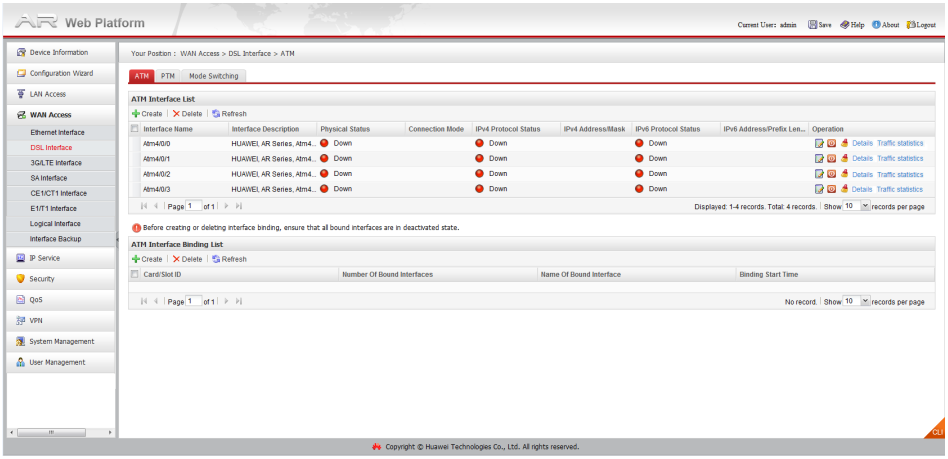
 Copyright © Huawei Technologies Co., Ltd.

ATM cells are transmitted over DSL interfaces working in ATM mode. Service traffic can be transmitted over DSL links only when the interfaces work in the same mode as the peer device.

Procedure

- Creating an ATM sub-interface
  a. Choose **WAN Access** > **DSL Interface** to display the **DSL Interface** page. **Figure 2-56** shows **DSL Interface** page.
  b. Click **ATM** to display the **ATM** page.

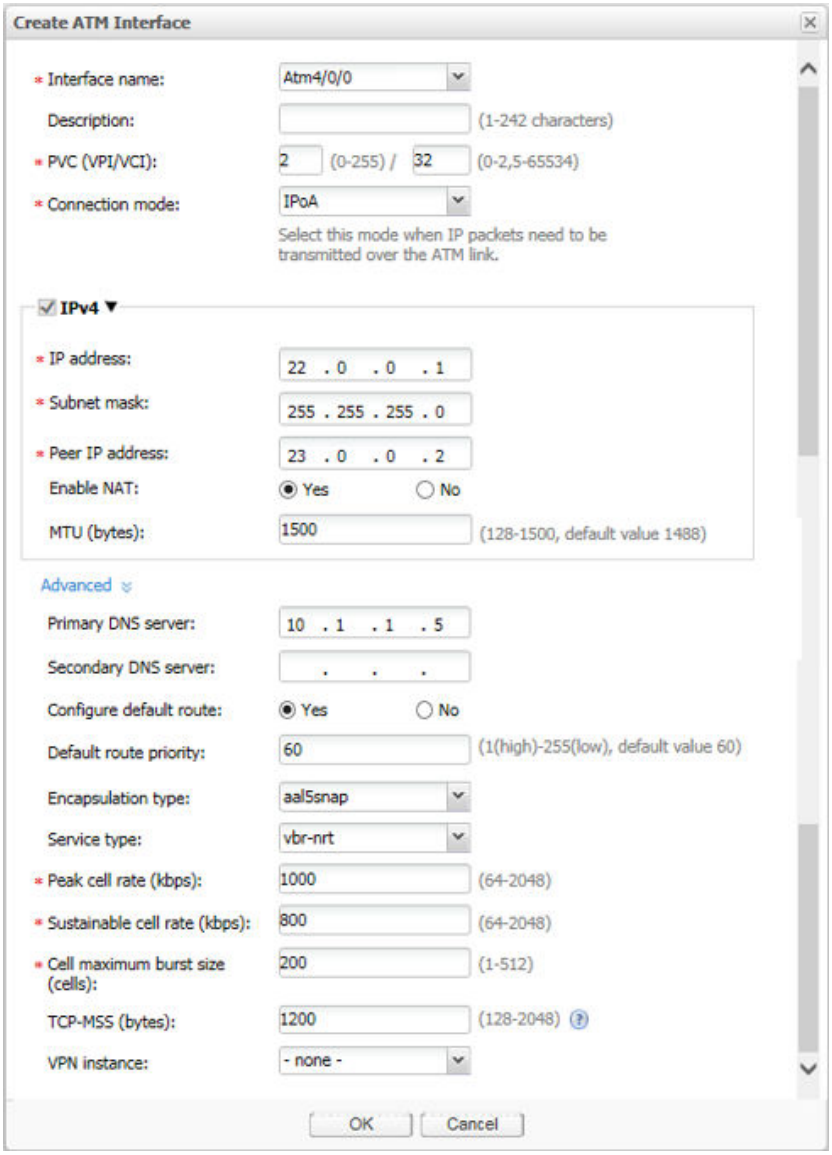
  Figure 2-56 ATM



  c. Click **Create** in **ATM Interface List** to display the page for creating an ATM interface.
  d. Set the parameters described in **Table 2-39**.
  e. Click **OK** to complete the configuration.

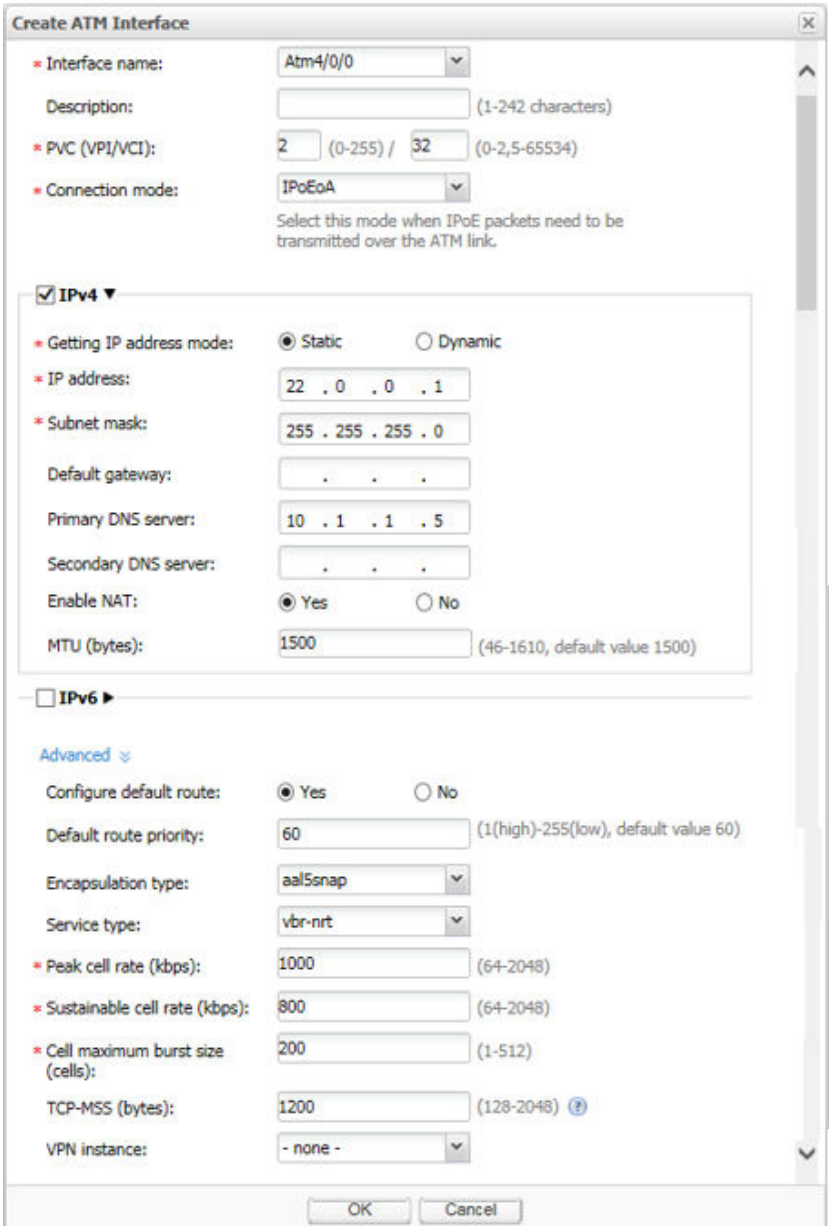
 Copyright © Huawei Technologies Co., Ltd.

- **Figure 2-57** Create ATM Interface (Connection mode is IPoA)



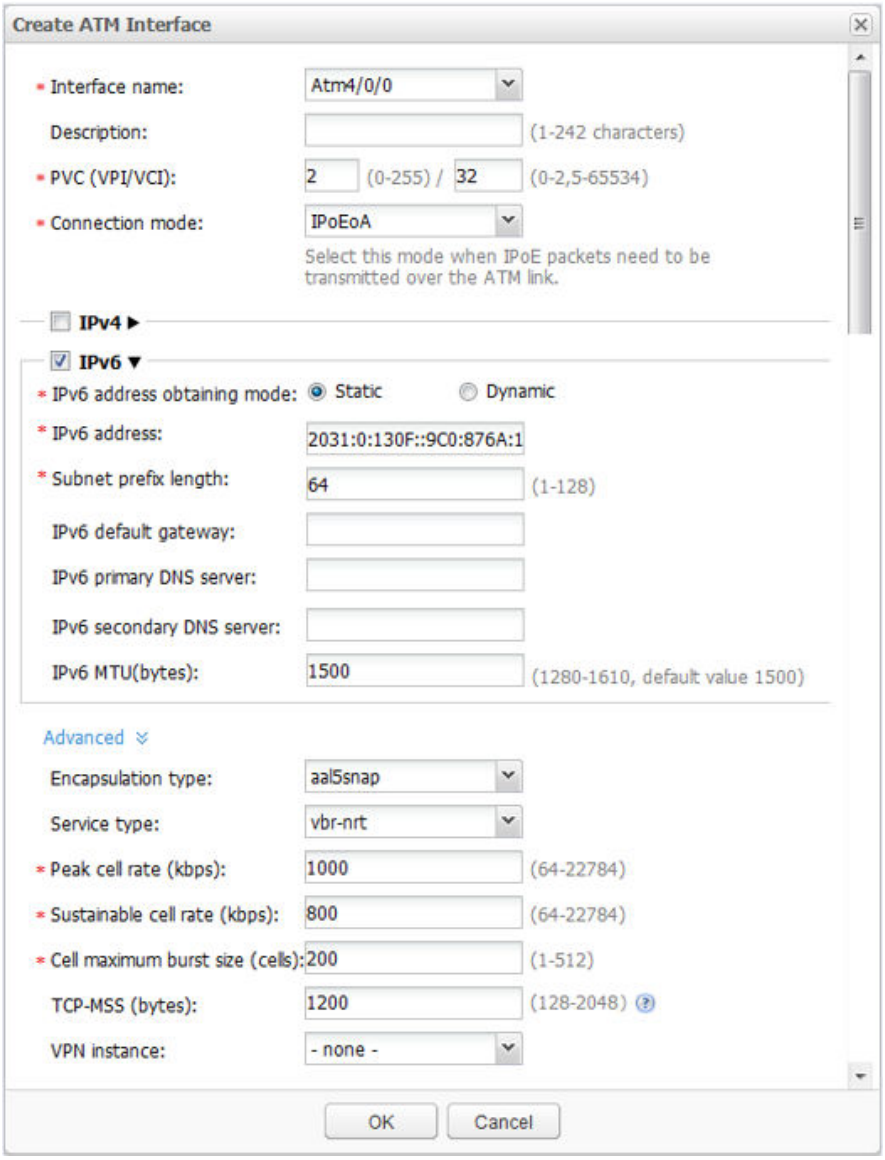
 Copyright © Huawei Technologies Co., Ltd.

- **Figure 2-58** Create ATM Interface (Connection mode is IPv4 IPoEoA)



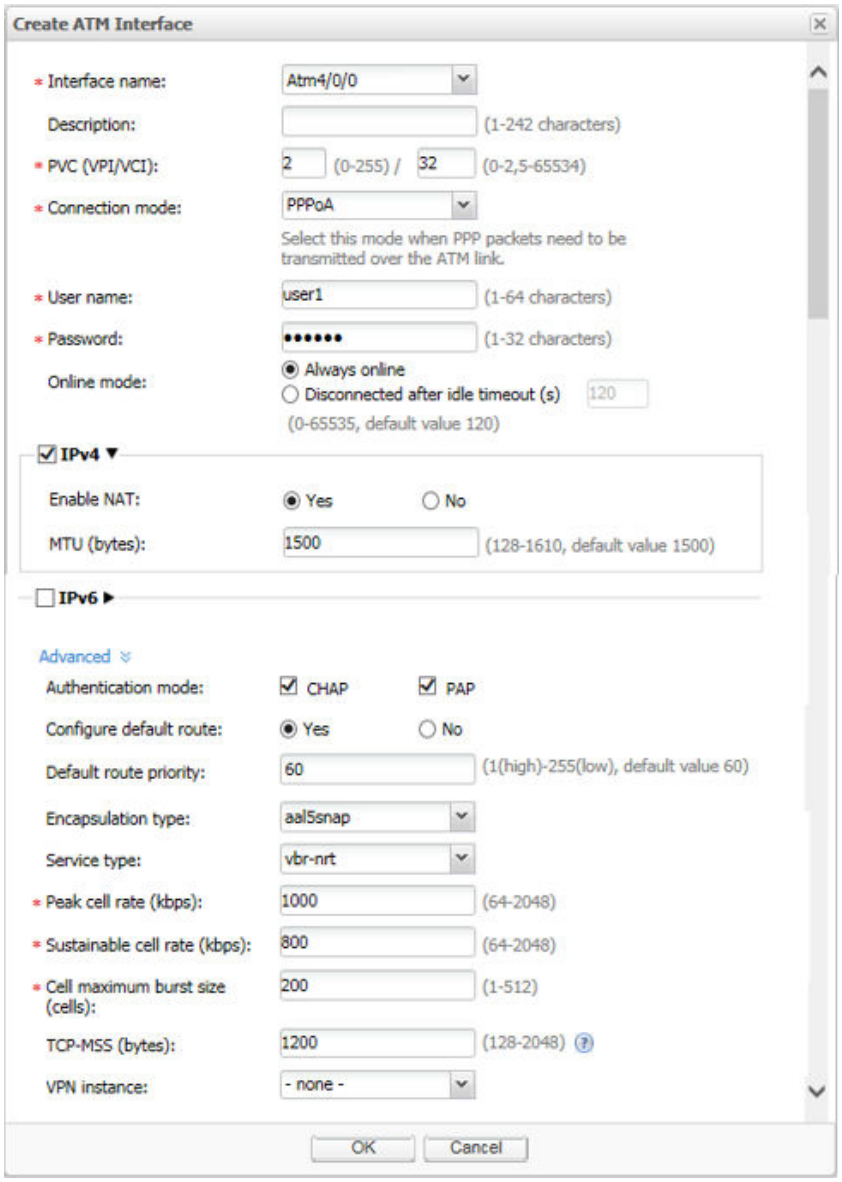
 Copyright © Huawei Technologies Co., Ltd.

- **Figure 2-59** Create ATM Interface (Connection mode is IPv6 IPoEoA)



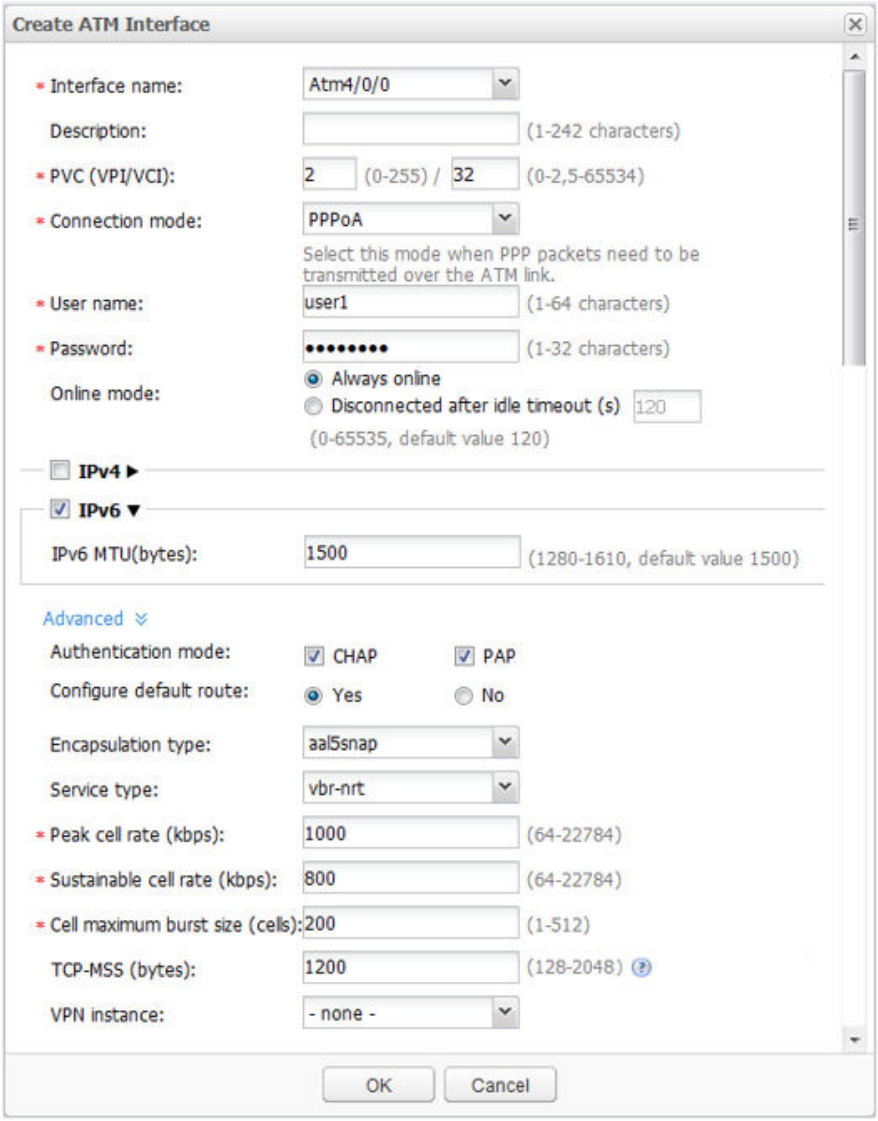
 Copyright © Huawei Technologies Co., Ltd.

- **Figure 2-60** Create ATM Interface (Connection mode is IPv4 PPPoA/PPPoEoA)



 Copyright © Huawei Technologies Co., Ltd.

- **Figure 2-61** Create ATM Interface (Connection mode is IPv6 PPPoA/PPPoEoA)



 Copyright © Huawei Technologies Co., Ltd.

Table 2-39 Description of the ATM interface parameters

Parameter	Description
Interface name	Type and number of an interface. • This parameter cannot be modified when the ATM interface configuration is modified. • When you set the parameters for creating an ATM sub-interface, select the ATM interface for which the sub-interface needs to be created.
Description	Description of an interface. By default, the description of an interface is empty.
PVC (VPI/VCI)	PVC used by links.
Connection mode	Type of packets on the interface. • IPoA: indicates that IP packets are transmitted over ATM links, as shown in **Figure 2-57**. For the description of IPoA parameters, see **Table 2-40**. • IPoEoA: indicates that IPoE packets are transmitted over ATM links, as shown in **Figure 2-58** or **Figure 2-59**. For the description of IPoEoA parameters, see **Table 2-41** or **Table 2-43**. • PPPoA: indicates that PPP packets are transmitted over ATM links, as shown in **Figure 2-60** or **Figure 2-61**. For the description of PPPoA parameters, see **Table 2-42** or **Table 2-44**. • PPPoEoA: indicates that PPPoE packets are transmitted over ATM links, as shown in **Figure 2-60** or **Figure 2-61**. For the description of PPPoEoA parameters, see **Table 2-42** or **Table 2-44**. **NOTE** You must select either IPv4 or IPv6 configuration.

Copyright © Huawei Technologies Co., Ltd.

Table 2-40 Description of the IPoA parameters

Parameter	Description
IP address	IP address of an interface. The interface IP address cannot conflict with the IP addresses of other interfaces on the device or other devices in the network.
Subnet mask	Subnet mask of an interface.
Peer IP address	Peer IP address that is mapped to the PVC. An IP address cannot be mapped to different ATM interfaces on the device; otherwise, forwarding is interrupted.
Enable NAT	NAT must be enabled when a PC on the private network of a LAN connects to the Internet.
MTU(bytes)	MTU of an interface. If the MTU is set too small and the size of packets is large, packets will be broken into a great number of fragments and be discarded by QoS queues. If the MTU is too large, packets are transmitted slowly or even lost. The default value of **MTU** is 1500.
Primary DNS server	Primary DNS server address assigned to a DHCP client.
Secondary DNS server	Secondary DNS server address assigned to a DHCP client.
Configure default route	Whether to configure a default route from the local host to the IPoA server.
Default route priority	Specifies the default route priority.
Encapsulation type	AAL5 encapsulation type of the PVC. ● aal5snap: When multiple protocols run on the same PVC, aal5snap encapsulation is adopted. ● aal5mux: When each protocol runs on an individual PVC, aal5mux encapsulation is adopted.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Service type	Service type of the PVC. • ubr: unspecified bit rate • cbr: constant bit rate • vbr-nrt: non real time-variable bit rate • vbr-rt: real time-variable bit rate
Confirm rate (kbps)	Peak rate of sending ATM cells. **NOTE** This parameter is optional when **Service type** is set to **ubr**. This parameter is valid only when **Service type** is set to **cbr**.
Peak cell rate (kbps)	Peak rate of sending ATM cells. **NOTE** This parameter is valid only when **Service type** is set to **vbr-nrt** or **vbr-rt**.
Sustainable cell rate (kbps)	Sustainable rate of sending ATM cells. **NOTE** This parameter is valid only when **Service type** is set to **vbr-nrt** or **vbr-rt**.
Cell maximum burst size (cells)	Maximum burst size of ATM cells that are sent. **NOTE** This parameter is valid only when **Service type** is set to **vbr-nrt** or **vbr-rt**.
TCP-MSS(bytes)	MSS of TCP packets on an interface. The MSS refers to the maximum length of a TCP packet segment sent from the peer device to the local device. During TCP connection negotiation, devices at both ends record the MSS of each other. When sending TCP packets, the devices limit the size of TCP packets within the MSS. The recommended value of **TCP-MSS** is 1200.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
VPN instance	VPN instance bound to an interface. **NOTE** Before setting this parameter, you must create an IPv4 VPN instance. For the detailed procedure, see **2.17.4 VPN Instance**.

Table 2-41 Description of the IPoEoA parameters (IPv4)

Parameter	Description
Getting IP address mode	Mode of obtaining an IP address.
IP address	IP address of an interface. The interface IP address cannot conflict with the IP addresses of other interfaces on the device or other devices in the network. **NOTE** This parameter is valid only when **Getting IP address mode** is set to **Static**.
Subnet mask	Subnet mask of an interface. **NOTE** This parameter is valid only when **Getting IP address mode** is set to **Static**.
Default gateway	Default gateway address of an interface. The default gateway address must be in the same network segment as the interface IP address. **NOTE** This parameter is valid only when **Getting IP address mode** is set to **Static**.
Primary DNS server	Primary DNS server address assigned to a DHCP client. **NOTE** This parameter is valid only when **Getting IP address mode** is set to **Static**.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Secondary DNS server	Secondary DNS server address assigned to a DHCP client. **NOTE** This parameter is valid only when **Getting IP address mode** is set to **Static**.
Enable NAT	NAT must be enabled when a PC on the private network of a LAN connects to the Internet.
MTU(bytes)	MTU of an interface. If the MTU is set too small and the size of packets is large, packets will be broken into a great number of fragments and be discarded by QoS queues. If the MTU is too large, packets are transmitted slowly or even lost. The default value of **MTU** is 1500.
Encapsulation type	AAL5 encapsulation type of the PVC. ● aal5snap: When multiple protocols run on the same PVC, aal5snap encapsulation is adopted. ● aal5mux: When each protocol runs on an individual PVC, aal5mux encapsulation is adopted.
Service type	Service type of the PVC. ● ubr: unspecified bit rate ● cbr: constant bit rate ● vbr-nrt: non real time-variable bit rate ● vbr-rt: real time-variable bit rate
Confirm rate (kbps)	Peak rate of sending ATM cells. **NOTE** This parameter is optional when **Service type** is set to **ubr**. This parameter is valid only when **Service type** is set to **cbr**.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Peak cell rate (kbps)	Peak rate of sending ATM cells. **NOTE** This parameter is valid only when **Service type** is set to **vbr-nrt** or **vbr-rt**.
Sustainable cell rate (kbps)	Sustainable rate of sending ATM cells. **NOTE** This parameter is valid only when **Service type** is set to **vbr-nrt** or **vbr-rt**.
Cell maximum burst size (cells)	Maximum burst size of ATM cells that are sent. **NOTE** This parameter is valid only when **Service type** is set to **vbr-nrt** or **vbr-rt**.
TCP-MSS(bytes)	MSS of TCP packets on an interface. The MSS refers to the maximum length of a TCP packet segment sent from the peer device to the local device. During TCP connection negotiation, devices at both ends record the MSS of each other. When sending TCP packets, the devices limit the size of TCP packets within the MSS. The recommended value of **TCP-MSS** is 1200.
VPN instance	VPN instance bound to an interface. **NOTE** Before setting this parameter, you must create an IPv4 VPN instance. For the detailed procedure, see **2.17.4 VPN Instance**.

Table 2-42 Description of the PPPoA/PPPoEoA parameters (IPv4)

Parameter	Description
User name	User name for PPPoA/PPPoEoA dial-up.
Password	Password for PPPoA/PPPoEoA dial-up.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Online mode	PPPoA/PPPoEoA dial-up mode. • Always online: The DCC attempts to dial the remote end immediately after the device starts. The dialing process is not triggered by data packets. If a connection cannot be established with the remote end, the DCC retries at an interval. This mode applies to the scenarios in which users are not charged based on traffic or time. • Disconnected after idle timeout (s): The device triggers the process of establishing a link only when there is data to be transmitted. When the time during which no traffic is transmitted on the link exceeds the timeout duration, the device disconnects the link to save traffic. This mode applies to the scenarios in which users are charged based on traffic or time. If this mode is used, the link idle time must be specified. The default link idle time is 120.
Enable NAT	NAT must be enabled when a PC on the private network of a LAN connects to the Internet.
MTU(bytes)	MTU of an interface. If the MTU is set too small and the size of packets is large, packets will be broken into a great number of fragments and be discarded by QoS queues. If the MTU is too large, packets are transmitted slowly or even lost. The default value of **MTU** is 1500.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Authentication mode	Authentication mode for PPPoA/ PPPoEoA dial-up. ● PAP: Passwords are sent over links in plain text. After a PPP link is established, the authenticated device repeatedly sends the user name and password until the authentication finishes. This mode cannot ensure high security. ● CHAP: a three-way handshake authentication protocol. In CHAP authentication, the authenticated device sends only the user name to the authenticating device. Compared with PAP, CHAP features higher security because passwords are not transmitted.
Configure default route	Configure a default route from the local hosts to the PPPoA or PPPoE server.
Default route priority	Specifies the default route priority.
Encapsulation type	AAL5 encapsulation type of the PVC. ● aal5snap: When multiple protocols run on the same PVC, aal5snap encapsulation is adopted. ● aal5mux: When each protocol runs on an individual PVC, aal5mux encapsulation is adopted.
Service type	Service type of the PVC. ● ubr: unspecified bit rate ● cbr: constant bit rate ● vbr-nrt: non real time-variable bit rate ● vbr-rt: real time-variable bit rate

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Confirm rate (kbps)	Peak rate of sending ATM cells. **NOTE** This parameter is optional when **Service type** is set to **ubr**. This parameter is valid only when **Service type** is set to **cbr**.
Peak cell rate (kbps)	Peak rate of sending ATM cells. **NOTE** This parameter is valid only when **Service type** is set to **vbr-nrt** or **vbr-rt**.
Sustainable cell rate (kbps)	Sustainable rate of sending ATM cells. **NOTE** This parameter is valid only when **Service type** is set to **vbr-nrt** or **vbr-rt**.
Cell maximum burst size (cells)	Maximum burst size of ATM cells that are sent. **NOTE** This parameter is valid only when **Service type** is set to **vbr-nrt** or **vbr-rt**.
TCP-MSS(bytes)	MSS of TCP packets on an interface. The MSS refers to the maximum length of a TCP packet segment sent from the peer device to the local device. During TCP connection negotiation, devices at both ends record the MSS of each other. When sending TCP packets, the devices limit the size of TCP packets within the MSS. The recommended value of **TCP-MSS** is 1200.
VPN instance	VPN instance bound to an interface. **NOTE** Before setting this parameter, you must create an IPv4 VPN instance. For the detailed procedure, see **2.17.4 VPN Instance**.

Copyright © Huawei Technologies Co., Ltd.

Table 2-43 Description of the IPoEoA parameters (IPv6)

Parameter	Description
IPv6 address obtaining mode	Mode of obtaining an IPv6 address.
IPv6 address	IPv6 address of an interface. **NOTE** This parameter is valid only when **IPv6 address obtaining mode** is set to **Static**.
Subnet prefix length	Length of the IPv6 address prefix. **NOTE** This parameter is valid only when **IPv6 address obtaining mode** is set to **Static**.
IPv6 default gateway	Default gateway address of an interface. The default gateway address must be in the same network segment as the interface IP address. **NOTE** This parameter is valid only when **IPv6 address obtaining mode** is set to **Static**.
IPv6 primary DNS server	Primary DNS server address assigned to a DHCPv6 client. **NOTE** This parameter is valid only when **IPv6 address obtaining mode** is set to **Static**.
IPv6 secondary DNS server	Secondary DNS server address assigned to a DHCPv6 client. **NOTE** This parameter is valid only when **IPv6 address obtaining mode** is set to **Static**.
Automatic mode	Mode of automatically obtaining an IPv6 address. **NOTE** This parameter is valid only when **IPv6 address obtaining mode** is set to **Dynamic**.
IPv6 MTU(bytes)	MTU of an interface. The default value of **MTU** is 1500.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Encapsulation type	AAL5 encapsulation type of the PVC. • aal5snap: When multiple protocols run on the same PVC, aal5snap encapsulation is adopted. • aal5mux: When each protocol runs on an individual PVC, aal5mux encapsulation is adopted.
Service type	Service type of the PVC. • ubr: unspecified bit rate • cbr: constant bit rate • vbr-nrt: non real time-variable bit rate • vbr-rt: real time-variable bit rate
Confirm rate (kbps)	Peak rate of sending ATM cells. **NOTE** This parameter is optional when **Service type** is set to **ubr**. This parameter is valid only when **Service type** is set to **cbr**.
Peak cell rate (kbps)	Peak rate of sending ATM cells. **NOTE** This parameter is valid only when **Service type** is set to **vbr-nrt** or **vbr-rt**.
Sustainable cell rate (kbps)	Sustainable rate of sending ATM cells. **NOTE** This parameter is valid only when **Service type** is set to **vbr-nrt** or **vbr-rt**.
Cell maximum burst size (cells)	Maximum burst size of ATM cells that are sent. **NOTE** This parameter is valid only when **Service type** is set to **vbr-nrt** or **vbr-rt**.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
TCP-MSS(bytes)	MSS of TCP packets on an interface. The MSS refers to the maximum length of a TCP packet segment sent from the peer device to the local device. During TCP connection negotiation, devices at both ends record the MSS of each other. When sending TCP packets, the devices limit the size of TCP packets within the MSS. The recommended value of **TCP-MSS** is 1200.
VPN instance	VPN instance bound to an interface. **NOTE** Before setting this parameter, you must create an IPv6 VPN instance. For the detailed procedure, see **2.17.4 VPN Instance**.

Table 2-44 Description of the PPPoA/PPPoEoA parameters (IPv6)

Parameter	Description
User name	User name for PPPoA/PPPoEoA dial-up.
Password	Password for PPPoA/PPPoEoA dial-up.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Online mode	PPPoA/PPPoEoA dial-up mode. • Always online: The DCC attempts to dial the remote end immediately after the device starts. The dialing process is not triggered by data packets. If a connection cannot be established with the remote end, the DCC retries at an interval. This mode applies to the scenarios in which users are not charged based on traffic or time. • Disconnected after idle timeout (s): The device triggers the process of establishing a link only when there is data to be transmitted. When the time during which no traffic is transmitted on the link exceeds the timeout duration, the device disconnects the link to save traffic. This mode applies to the scenarios in which users are charged based on traffic or time. If this mode is used, the link idle time must be specified. The default link idle time is 120.
IPv6 MTU(bytes)	MTU of an interface. The default value of **MTU** is 1500.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Authentication mode	Authentication mode for PPPoA/ PPPoEoA dial-up. ● PAP: Passwords are sent over links in plain text. After a PPP link is established, the authenticated device repeatedly sends the user name and password until the authentication finishes. This mode cannot ensure high security. ● CHAP: a three-way handshake authentication protocol. In CHAP authentication, the authenticated device sends only the user name to the authenticating device. Compared with PAP, CHAP features higher security because passwords are not transmitted.
Configure default route	Configure a default route from the local hosts to the PPPoA or PPPoE server.
Default route priority	Specifies the default route priority.
Encapsulation type	AAL5 encapsulation type of the PVC. ● aal5snap: When multiple protocols run on the same PVC, aal5snap encapsulation is adopted. ● aal5mux: When each protocol runs on an individual PVC, aal5mux encapsulation is adopted.
Service type	Service type of the PVC. ● ubr: unspecified bit rate ● cbr: constant bit rate ● vbr-nrt: non real time-variable bit rate ● vbr-rt: real time-variable bit rate

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Confirm rate (kbps)	Peak rate of sending ATM cells. **NOTE** This parameter is optional when **Service type** is set to **ubr**. This parameter is valid only when **Service type** is set to **cbr**.
Peak cell rate (kbps)	Peak rate of sending ATM cells. **NOTE** This parameter is valid only when **Service type** is set to **vbr-nrt** or **vbr-rt**.
Sustainable cell rate (kbps)	Sustainable rate of sending ATM cells. **NOTE** This parameter is valid only when **Service type** is set to **vbr-nrt** or **vbr-rt**.
Cell maximum burst size (cells)	Maximum burst size of ATM cells that are sent. **NOTE** This parameter is valid only when **Service type** is set to **vbr-nrt** or **vbr-rt**.
TCP-MSS(bytes)	MSS of TCP packets on an interface. The MSS refers to the maximum length of a TCP packet segment sent from the peer device to the local device. During TCP connection negotiation, devices at both ends record the MSS of each other. When sending TCP packets, the devices limit the size of TCP packets within the MSS. The recommended value of **TCP-MSS** is 1200.
VPN instance	VPN instance bound to an interface. **NOTE** Before setting this parameter, you must create an IPv6 VPN instance. For the detailed procedure, see **2.17.4 VPN Instance**.

- Modifying ATM interface configuration
  a. Choose **WAN Access** > **DSL Interface** to display the **DSL Interface** page.
  b. Click **ATM** to display the **ATM** page.

Copyright © Huawei Technologies Co., Ltd.

c. Click  corresponding to the ATM interface to be configured in the **Operation** column of **ATM Interface List** to display the modification page.

d. Set the parameters described in **Table 2-39**.

e. Click **OK** to complete the configuration.

- Disabling an ATM interface
  a. Choose **WAN Access** > **DSL Interface** to display the **DSL Interface** page.
  b. Click **ATM** to display the **ATM** page.
  c. Click  corresponding to the ATM interface to be configured in the **Operation** column of **ATM Interface List**.
  d. Click **OK**.
- Enabling an ATM interface
  a. Choose **WAN Access** > **DSL Interface** to display the **DSL Interface** page.
  b. Click **ATM** to display the **ATM** page.
  c. Click  corresponding to the ATM interface to be configured in the **Operation** column of **ATM Interface List**.
  d. Click **OK**.
- Clearing an ATM interface
  a. Choose **WAN Access** > **DSL Interface** to display the **DSL Interface** page.
  b. Click **ATM** to display the **ATM** page.
  c. Click  corresponding to the ATM interface to be configured in the **Operation** column of **ATM Interface List**.
  d. Click **OK**.
- Viewing the details of an ATM interface

  NOTE

  V200R010C10 and later versions support viewing**Details**.
  a. Choose **WAN Access** > **DSL Interface** to display the **DSL Interface** page.
  b. Click **ATM** to display the **ATM** page.
  c. Click **Details** corresponding to the ATM interface to be configured in the **Operation** column of **ATM Interface List**.
  d. Click **OK**.
- Viewing the traffic statistics of an ATM interface

  NOTE

  V200R010C10 and later versions support viewing**Traffic statistics**.
  a. Choose **WAN Access** > **DSL Interface** to display the **DSL Interface** page.
  b. Click **ATM** to display the **ATM** page.
  c. Click **Traffic statistics** corresponding to the ATM interface to be configured in the **Operation** column of **ATM Interface List**.
  d. Click **OK**.
- Deleting an ATM sub-interface

Copyright © Huawei Technologies Co., Ltd.

a. Choose **WAN Access** > **DSL Interface** to display the **DSL Interface** page.
b. Click **ATM** to display the **ATM** page.
c. Select the check box of the interface to be deleted and click **Delete** in the **Interface Name** column of **ATM Interface List**.
d. Click **OK**.

- Binding ATM interfaces

  NOTE

  Before binding interfaces, ensure that these interfaces have been deactivated and that slave interfaces are not configured with any service. Among the bound interfaces, the first bound interface is the master interface, and other bound interfaces are slave interfaces.

  a. Choose **WAN Access** > **DSL Interface** to display the **DSL Interface** page.
  b. Click **ATM** to display the **ATM** page.
  c. Click **Create** in **ATM Interface Binding List** to display the page for binding ATM interfaces.
  d. Set the parameters described in **Table 2-45**.

Figure 2-62 Create ATM Interface Binding

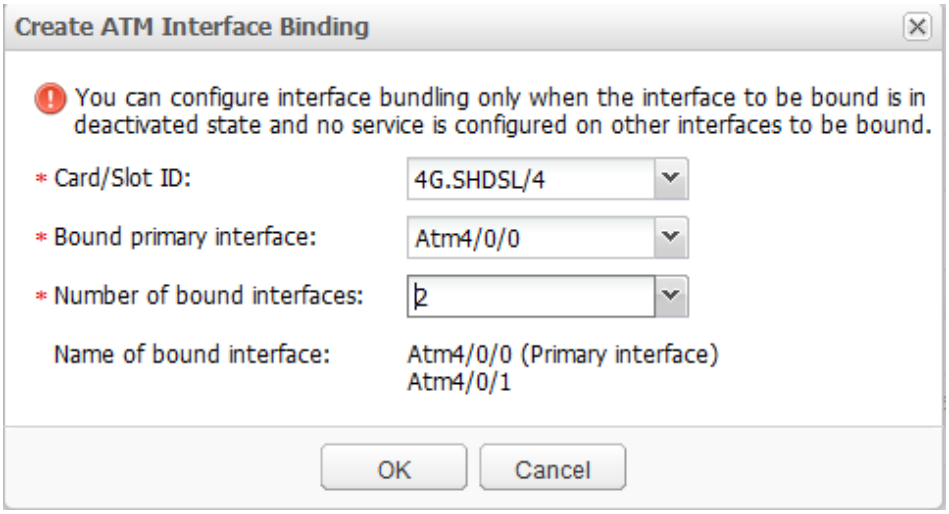


Table 2-45 Description of the parameters for binding ATM interfaces

Parameter	Description
Card/Slot ID	Name and slot ID of a G.SHDSL board.
Bound primary interface	The number of the first interface to be bound must be 0 or 2, and the first bound interface is the primary interface.
Number of bound interfaces	Number of interfaces to be bound.

Copyright © Huawei Technologies Co., Ltd.

- Unbinding ATM interfaces

  NOTE

  Before unbinding interfaces, ensure that these interfaces have been deactivated.

  a. Choose **WAN Access** > **DSL Interface** to display the **DSL Interface** page.
  b. Click **ATM** to display the **ATM** page.
  c. Select the check box of the interface to be unbound and click **Delete** in the **Card/Slot ID** column of **ATM Interface Binding List**.
  d. Click **OK**.

----End

2.12.2.2 PTM

Context

The device supports the ADSL, VDSL, and G.SHDSL interface cards (together called DSL interface cards). DSL links can be used to connect the device to the Internet.

The VDSL and G.SHDSL interfaces can work in Asynchronous Transfer Mode (ATM) or Packet Transfer Mode (PTM) mode and switch between these two modes. An ADSL interface works only in ATM mode.

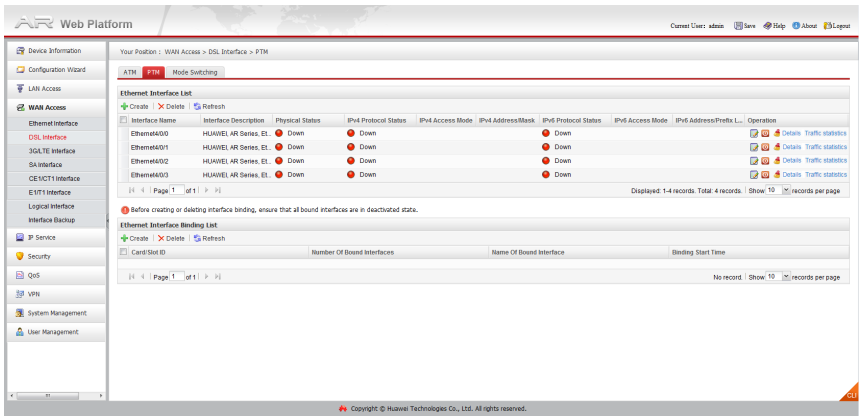
Ethernet packets are transmitted over DSL interfaces working in PTM mode. Service traffic can be transmitted over DSL links only when the interfaces work in the same mode as the peer device.

Procedure

- Creating an Ethernet sub-interface

  a. Choose **WAN Access** > **DSL Interface** to display the **DSL Interface** page. **Figure 2-63** shows **DSL Interface** page.
  b. Click **PTM** to display the **PTM** page.

  Figure 2-63 PTM

  c. Click **Create** in **Ethernet Interface List** to display the page for creating an Ethernet interface.

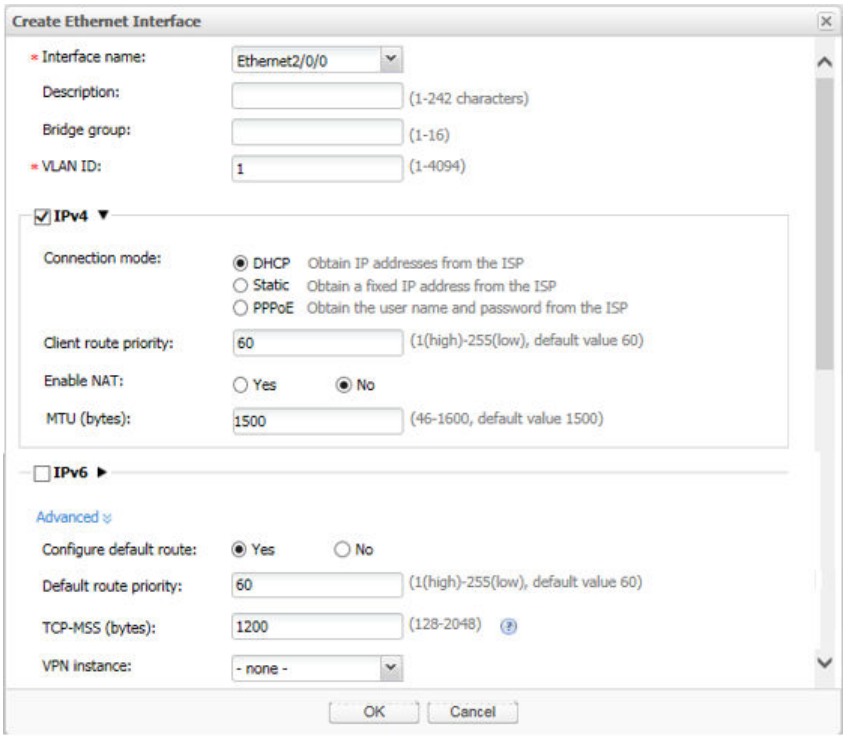
d. Set the parameters described in **Table 2-46**.

e. Click **OK** to complete the configuration.

NOTE

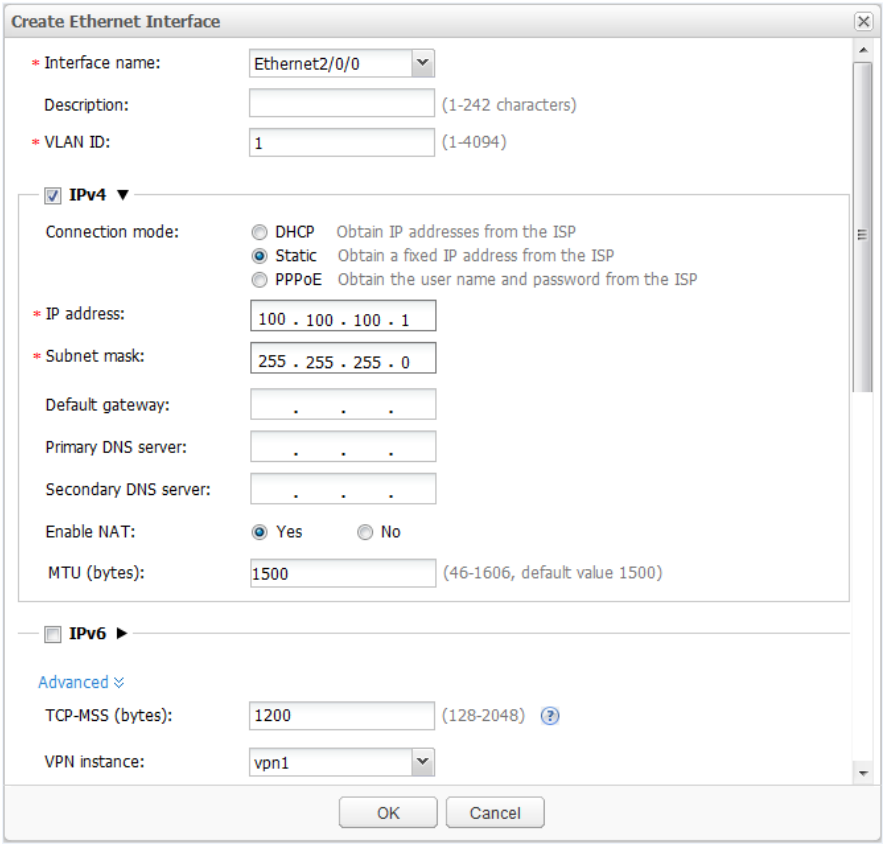
The parameters for creating an Ethernet interface are the same as those in **2.12.1 Ethernet Interface**. After select an Ethernet interface from the **Interface name** drop-down list box, you can set the parameters according to the page (shown in the following figures) in **2.12.1 Ethernet Interface**.

- **Figure 2-64** Create Ethernet interface (Connection mode is IPv4 DHCP)



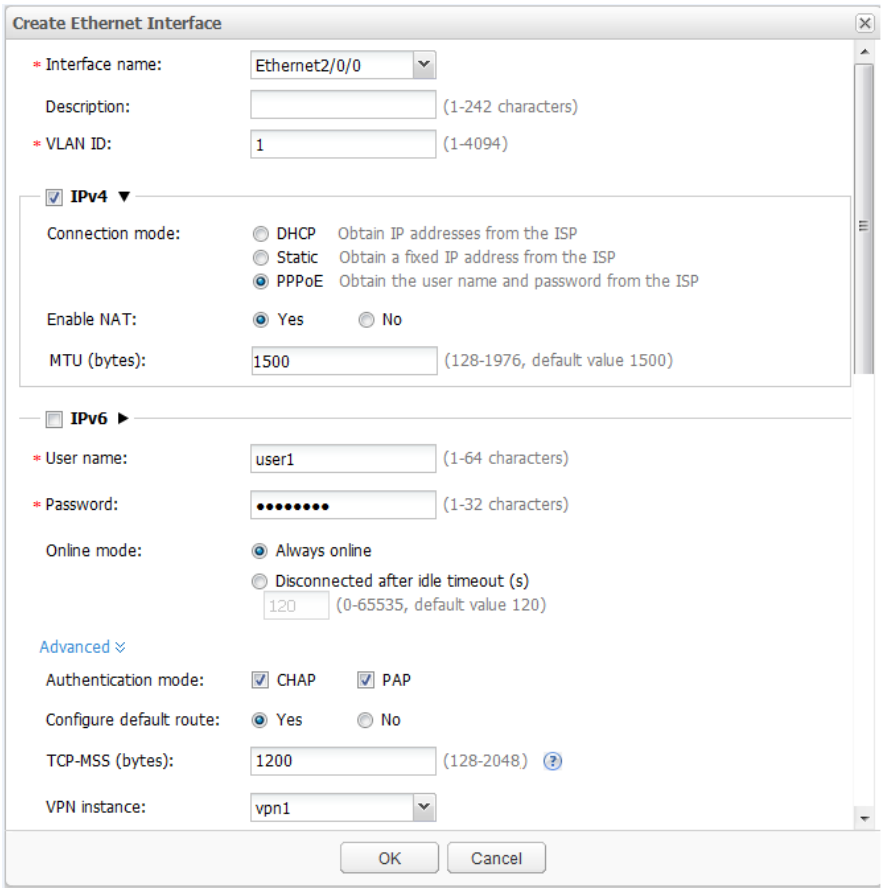
Copyright © Huawei Technologies Co., Ltd.

- **Figure 2-65** Create Ethernet interface (Connection mode is IPv4 Static)

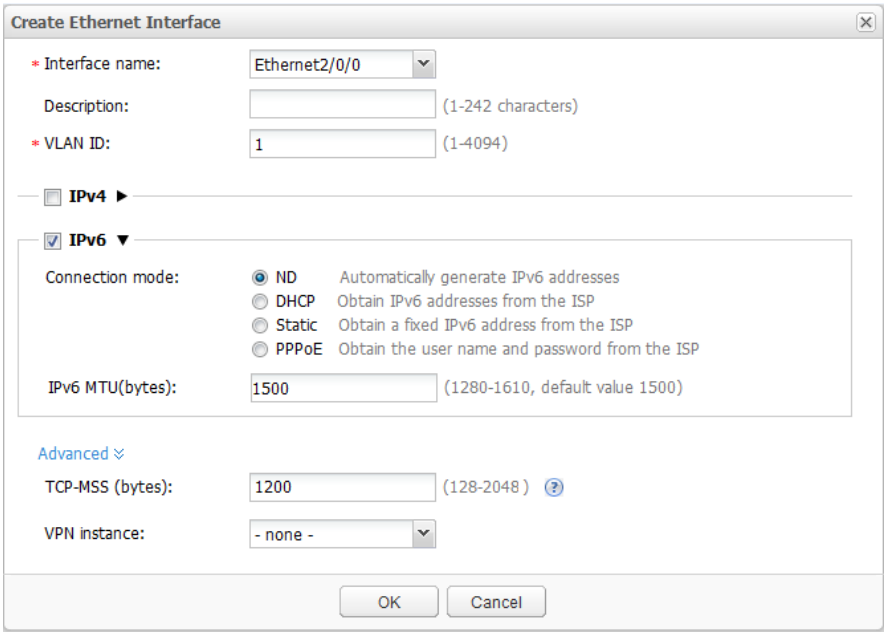


 Copyright © Huawei Technologies Co., Ltd.

- **Figure 2-66** Create Ethernet interface (Connection mode is IPv4 PPPoE)

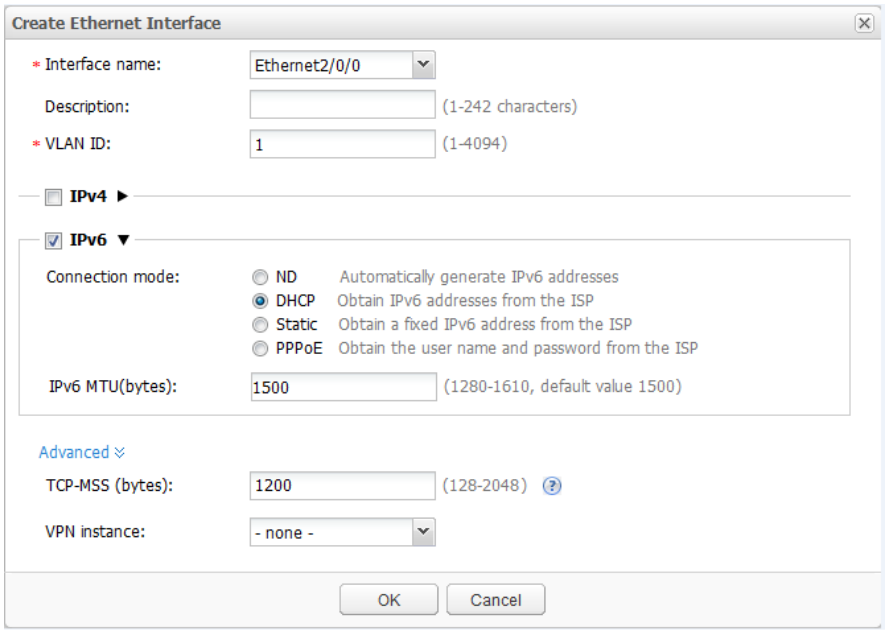


- **Figure 2-67** Create Ethernet interface (Connection mode is IPv6 ND)

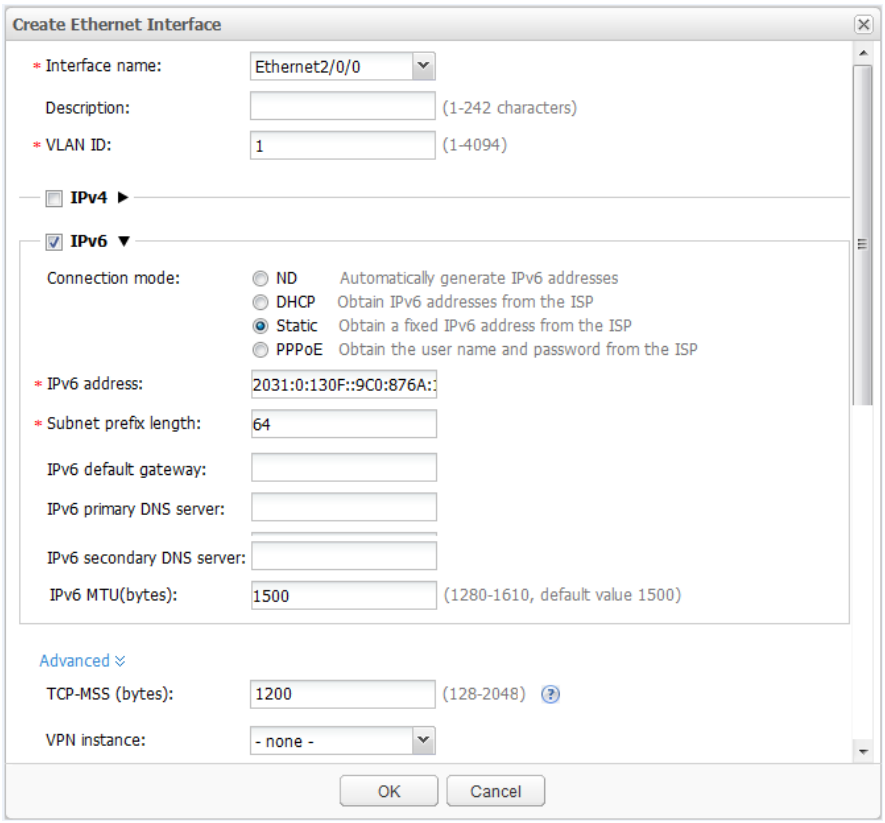


 Copyright © Huawei Technologies Co., Ltd.

- **Figure 2-68** Create Ethernet interface (Connection mode is IPv6 DHCP)



- **Figure 2-69** Create Ethernet interface (Connection mode is IPv6 Static)



 Copyright © Huawei Technologies Co., Ltd.

- **Figure 2-70** Create Ethernet interface (Connection mode is IPv6 PPPoE)

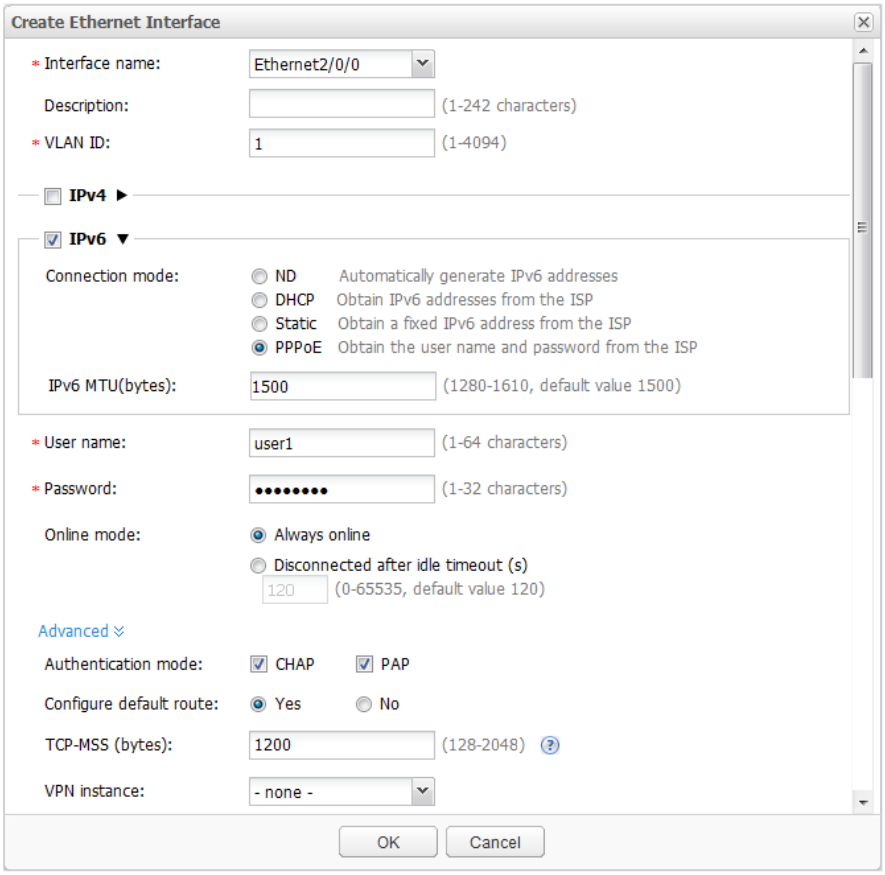


Table 2-46 Description of the Ethernet interface parameters

Parameter	Description
Interface name	Type and number of an interface. • This parameter cannot be modified when the Ethernet interface configuration is modified. • When you set the parameters for creating an Ethernet sub-interface, select the Ethernet interface for which the sub-interface needs to be created.
Description	Description of an interface. By default, the description of an interface is empty.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Bridge group	Description of a bridge group. The value is an integer.
VLAN ID	The VLAN ID must be entered when a user VLAN is terminated through a sub-interface. You can set this parameter only when creating an Ethernet sub-interface.
IPv4	IPv4 configuration parameters. The **Connection mode** parameter specifies the mode in which an interface obtains an IPv4 address. The options for **Connection mode** are as follows: • DHCP: indicates that the interface IPv4 address is automatically obtained using DHCP. For the description of DHCP parameters, see **Table 2-47**. • Static: indicates that the interface IPv4 address is manually configured. For the description of Static parameters, see **Table 2-48**. • PPPoE: indicates that the interface IPv4 address is obtained through PPP negotiation. For the description of PPPoE parameters, see **Table 2-49**. **NOTE** You must select either IPv4 or IPv6 configuration.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
IPv6	IPv6 configuration parameters. The **Connection mode** parameter specifies the mode in which an interface obtains an IPv6 address. The options for **Connection mode** are as follows: • ND: indicates that the interface IPv6 address is automatically configured. For the description of ND parameters, see **Table 2-50**. • DHCP: indicates that the interface IPv4 address is automatically obtained using DHCP. For the description of DHCP parameters, see **Table 2-51**. • Static: indicates that the interface IPv4 address is manually configured. For the description of Static parameters, see **Table 2-52**. • PPPoE: indicates that the interface IPv4 address is obtained through PPP negotiation. For the description of PPPoE parameters, see **Table 2-53**. **NOTE** You must select either IPv4 or IPv6 configuration.

Table 2-47 Description of the DHCP parameters (IPv4)

Parameter	Description
NAT status	NAT must be enabled when a PC on the private network of a LAN connects to the Internet.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
MTU (bytes)	MTU of an interface. If the MTU is set too small and the size of packets is large, packets will be broken into a great number of fragments and be discarded by QoS queues. If the MTU is too large, packets are transmitted slowly or even lost. The default value of **MTU** is 1500.
TCP-MSS (bytes)	MSS of TCP packets on an interface. The MSS refers to the maximum length of a TCP packet segment sent from the peer device to the local device. During TCP connection negotiation, devices at both ends record the MSS of each other. When sending TCP packets, the devices limit the size of TCP packets within the MSS. The recommended value of **TCP-MSS** is 1200.
VPN instance	VPN instance bound to an interface. **NOTE** Before setting this parameter, you must create an IPv4 VPN instance. For the detailed procedure, see **2.17.4 VPN Instance**.

Table 2-48 Description of the Static parameters (IPv4)

Parameter	Description
IP address	IP address of an interface. The interface IP address cannot conflict with the IP addresses of other interfaces on the device or other devices in the network.
Subnet mask	Subnet mask of an interface.
Default gateway	Default gateway address of an interface. The default gateway address must be in the same network segment as the interface IP address.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Primary DNS server	Primary DNS server address assigned to a DHCP client.
Secondary DNS server	Secondary DNS server address assigned to a DHCP client.
NAT status	NAT must be enabled when a PC on the private network of a LAN connects to the Internet.
MTU (bytes)	MTU of an interface. If the MTU is set too small and the size of packets is large, packets will be broken into a great number of fragments and be discarded by QoS queues. If the MTU is too large, packets are transmitted slowly or even lost. The default value of **MTU** is 1500.
TCP-MSS (bytes)	MSS of TCP packets on an interface. The MSS refers to the maximum length of a TCP packet segment sent from the peer device to the local device. During TCP connection negotiation, devices at both ends record the MSS of each other. When sending TCP packets, the devices limit the size of TCP packets within the MSS. The recommended value of **TCP-MSS** is 1200.
VPN instance	VPN instance bound to an interface. **NOTE** Before setting this parameter, you must create an IPv4 VPN instance. For the detailed procedure, see **2.17.4 VPN Instance**.

Table 2-49 Description of the PPPoE parameters (IPv4)

Parameter	Description
NAT status	NAT must be enabled when a PC on the private network of a LAN connects to the Internet.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
MTU (bytes)	MTU of an interface. If the MTU is set too small and the size of packets is large, packets will be broken into a great number of fragments and be discarded by QoS queues. If the MTU is too large, packets are transmitted slowly or even lost. The default value of **MTU** is 1500.
User name	User name for PPPoE dial-up.
Password	Password for PPPoE dial-up.
Online mode	PPPoE dial-up mode. ● Always online: The DCC attempts to dial the remote end immediately after the device starts. The dialing process is not triggered by data packets. If a connection cannot be established with the remote end, the DCC retries at an interval. This mode applies to the scenarios in which users are not charged based on traffic or time. ● Disconnected after idle timeout (s): The device triggers the process of establishing a link only when there is data to be transmitted. When the time during which no traffic is transmitted on the link exceeds the timeout duration, the device disconnects the link to save traffic. This mode applies to the scenarios in which users are charged based on traffic or time. If this mode is used, the link idle time must be specified. The default link idle time is 120.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Authentication mode	Authentication mode for PPPoE dial-up. • PAP: Passwords are sent over links in plain text. After a PPP link is established, the authenticated device repeatedly sends the user name and password until the authentication finishes. This mode cannot ensure high security. • CHAP: a three-way handshake authentication protocol. In CHAP authentication, the authenticated device sends only the user name to the authenticating device. Compared with PAP, CHAP features higher security because passwords are not transmitted.
Configure default route	Configure a default route from the local hosts to the PPPoE server.
TCP-MSS (bytes)	MSS of TCP packets on an interface. The MSS refers to the maximum length of a TCP packet segment sent from the peer device to the local device. During TCP connection negotiation, devices at both ends record the MSS of each other. When sending TCP packets, the devices limit the size of TCP packets within the MSS. The recommended value of **TCP-MSS** is 1200.
VPN instance	VPN instance bound to an interface. **NOTE** Before setting this parameter, you must create an IPv4 VPN instance. For the detailed procedure, see **2.17.4 VPN Instance**.

Copyright © Huawei Technologies Co., Ltd.

Table 2-50 Description of the ND parameters

Parameter	Description
IPv6 MTU (bytes)	MTU of an interface. The default value of **MTU** is 1500.
TCP-MSS (bytes)	MSS of TCP packets on an interface. The MSS refers to the maximum length of a TCP packet segment sent from the peer device to the local device. During TCP connection negotiation, devices at both ends record the MSS of each other. When sending TCP packets, the devices limit the size of TCP packets within the MSS. The recommended value of **TCP-MSS** is 1200.
VPN instance	VPN instance bound to an interface. **NOTE** Before setting this parameter, you must create an IPv6 VPN instance. For the detailed procedure, see **2.17.4 VPN Instance**.

Table 2-51 Description of the DHCP parameters (IPv6)

Parameter	Description
IPv6 MTU (bytes)	MTU of an interface. The default value of **MTU** is 1500.
TCP-MSS (bytes)	MSS of TCP packets on an interface. The MSS refers to the maximum length of a TCP packet segment sent from the peer device to the local device. During TCP connection negotiation, devices at both ends record the MSS of each other. When sending TCP packets, the devices limit the size of TCP packets within the MSS. The recommended value of **TCP-MSS** is 1200.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
VPN instance	VPN instance bound to an interface. **NOTE** Before setting this parameter, you must create an IPv6 VPN instance. For the detailed procedure, see **2.17.4 VPN Instance**.

Table 2-52 Description of the Static parameters (IPv6)

Parameter	Description
IPv6 address	IPv6 address of an interface.
Subnet prefix length	Length of the IPv6 address prefix.
IPv6 default gateway	Default gateway address of an interface. The default gateway address must be in the same network segment as the interface IP address.
IPv6 primary DNS server	Primary DNS server address assigned to a DHCPv6 client.
IPv6 secondary DNS server	Secondary DNS server address assigned to a DHCPv6 client.
IPv6 MTU (bytes)	MTU of an interface. The default value of **MTU** is 1500.
TCP-MSS (bytes)	MSS of TCP packets on an interface. The MSS refers to the maximum length of a TCP packet segment sent from the peer device to the local device. During TCP connection negotiation, devices at both ends record the MSS of each other. When sending TCP packets, the devices limit the size of TCP packets within the MSS. The recommended value of **TCP-MSS** is 1200.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
VPN instance	VPN instance bound to an interface. **NOTE** Before setting this parameter, you must create an IPv6 VPN instance. For the detailed procedure, see **2.17.4 VPN Instance**.

Table 2-53 Description of the PPPoE parameters (IPv6)

Parameter	Description
IPv6 MTU (bytes)	MTU of an interface. The default value of **MTU** is 1500.
User name	User name for PPPoE dial-up.
Password	Password for PPPoE dial-up.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Online mode	PPPoE dial-up mode. • Always online: The DCC attempts to dial the remote end immediately after the device starts. The dialing process is not triggered by data packets. If a connection cannot be established with the remote end, the DCC retries at an interval. This mode applies to the scenarios in which users are not charged based on traffic or time. • Disconnected after idle timeout (s): The device triggers the process of establishing a link only when there is data to be transmitted. When the time during which no traffic is transmitted on the link exceeds the timeout duration, the device disconnects the link to save traffic. This mode applies to the scenarios in which users are charged based on traffic or time. If this mode is used, the link idle time must be specified. The default link idle time is 120.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Authentication mode	Authentication mode for PPPoE dial-up. • PAP: Passwords are sent over links in plain text. After a PPP link is established, the authenticated device repeatedly sends the user name and password until the authentication finishes. This mode cannot ensure high security. • CHAP: a three-way handshake authentication protocol. In CHAP authentication, the authenticated device sends only the user name to the authenticating device. Compared with PAP, CHAP features higher security because passwords are not transmitted.
Configure default route	Configure a default route from the local hosts to the PPPoE server.
TCP-MSS (bytes)	MSS of TCP packets on an interface. The MSS refers to the maximum length of a TCP packet segment sent from the peer device to the local device. During TCP connection negotiation, devices at both ends record the MSS of each other. When sending TCP packets, the devices limit the size of TCP packets within the MSS. The recommended value of **TCP-MSS** is 1200.
VPN instance	VPN instance bound to an interface. **NOTE** Before setting this parameter, you must create an IPv6 VPN instance. For the detailed procedure, see **2.17.4 VPN Instance**.

- Modifying Ethernet interface configuration
  a. Choose **WAN Access** > **DSL Interface** to display the **DSL Interface** page.
  b. Click **PTM** to display the **PTM** page.

Copyright © Huawei Technologies Co., Ltd.

c. Click  corresponding to the Ethernet interface to be configured in the **Operation** column of **Ethernet Interface List** to display the modification page.

d. Set the parameters described in **Table 2-46**.

e. Click **OK** to complete the configuration.

- Disabling an Ethernet interface

  a. Choose **WAN Access** > **DSL Interface** to display the **DSL Interface** page.

  b. Click **PTM** to display the **PTM** page.

  c. Click  corresponding to the Ethernet interface to be configured in the **Operation** column of **Ethernet Interface List**.

  d. Click **OK**.

- Enabling an Ethernet interface

  a. Choose **WAN Access** > **DSL Interface** to display the **DSL Interface** page.

  b. Click **PTM** to display the **PTM** page.

  c. Click  corresponding to the Ethernet interface to be configured in the **Operation** column of **Ethernet Interface List**.

  d. Click **OK**.

- Clearing an Ethernet interface

  a. Choose **WAN Access** > **DSL Interface** to display the **DSL Interface** page.

  b. Click **PTM** to display the **PTM** page.

  c. Click  corresponding to the Ethernet interface to be configured in the **Operation** column of **Ethernet Interface List**.

  d. Click **OK**.

- Viewing the details of an Ethernet interface

  NOTE

  V200R010C10 and later versions support viewing**Details**.

  a. Choose **WAN Access** > **DSL Interface** to display the **DSL Interface** page.

  b. Click **PTM** to display the **PTM** page.

  c. Click **Details** corresponding to the Ethernet interface to be configured in the **Operation** column of **Ethernet Interface List**.

  d. Click **Close**.

- Viewing the traffic statistics of an Ethernet interface

  NOTE

  V200R010C10 and later versions support viewing**Traffic statistics**.

  a. Choose **WAN Access** > **DSL Interface** to display the **DSL Interface** page.

  b. Click **PTM** to display the **PTM** page.

  c. Click **Traffic statistics** corresponding to the Ethernet interface to be configured in the **Operation** column of **Ethernet Interface List**.

  d. Click **Close**.

- Deleting an Ethernet sub-interface

 Copyright © Huawei Technologies Co., Ltd.

a. Choose **WAN Access** > **DSL Interface** to display the **DSL Interface** page.
b. Click **PTM** to display the **PTM** page.
c. Select the check box of the interface to be deleted and click **Delete** in the **Interface Name** column of **Ethernet Interface List**.
d. Click **OK**.

- Binding Ethernet interfaces

  NOTE

  Before binding interfaces, ensure that these interfaces have been deactivated and that slave interfaces are not configured with any service. Among the bound interfaces, the first bound interface is the master interface, and other bound interfaces are slave interfaces.

  a. Choose **WAN Access** > **DSL Interface** to display the **DSL Interface** page.
  b. Click **PTM** to display the **PTM** page.
  c. Click **Create** in **Ethernet Interface Binding List** to display the page for binding Ethernet interfaces.
  d. Set the parameters described in **Table 2-54**.

Figure 2-71 Create Ethernet Interface Binding

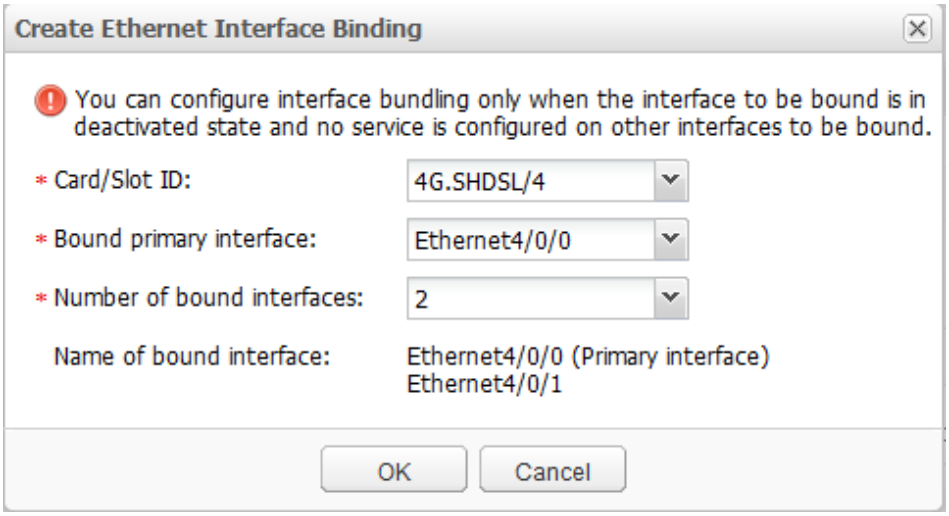


Table 2-54 Description of the parameters for binding Ethernet interfaces

Parameter	Description
Card/Slot ID	Name and slot ID of a G.SHDSL board.
Bound primary interface	The number of the first interface to be bound must be 0 or 2, and the first bound interface is the primary interface.
Number of bound interfaces	Number of interfaces to be bound.

Copyright © Huawei Technologies Co., Ltd.

- Unbinding Ethernet interfaces

  NOTE

  Before unbinding interfaces, ensure that these interfaces have been deactivated.

  a. Choose **WAN Access** > **DSL Interface** to display the **DSL Interface** page.
  b. Click **PTM** to display the **PTM** page.
  c. Select the check box of the interface to be unbound and click **Delete** in the **Card/Slot ID** column of **Ethernet Interface Binding List**.
  d. Click **OK**.

----End

2.12.2.3 Mode Switching

Context

The VDSL and G.SHDSL interfaces can work in ATM or PTM mode and switch between these two modes. An ADSL interface works only in ATM mode.

The VDSL and G.SHDSL interfaces support the following transfer modes:

- Asynchronous Transfer Mode (ATM): ATM cells are transmitted over VDSL and G.SHDSL lines.
- Packet Transfer Mode (PTM): Ethernet frames are transmitted over VDSL and G.SHDSL lines.

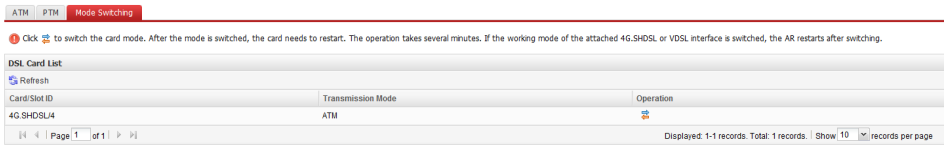
The device functions as a CPE and must have the same interface transfer mode as the peer device. For example, when the G.SHDSL interface of the peer device works in ATM mode, the G.SHDSL interface of the device must also work in ATM mode. The device can communicate with the peer device only when the device's G.SHDSL interface has the same transfer mode as the peer device.

Procedure

- Switching the transfer mode

  a. Choose **WAN Access** > **DSL Interface** to display the **DSL Interface** page.
  b. Click **Mode Switching** to display the **Mode Switching** tab page. **Figure 2-72** shows **Mode Switching** page.

  Figure 2-72 Mode Switching

  c. Click in the **Operation** column of **DSL Card List**.
  d. Click **OK**.

  The configuration takes effect after several minutes.

----End

Copyright © Huawei Technologies Co., Ltd.

2.12.3 3G/LTE Interface

Context

Although wired WAN access technologies such as access through the optical fiber, xDSL interface, or E1/T1 interface are mature and widely used, wired WAN access service may meet the bottleneck in the following scenarios:

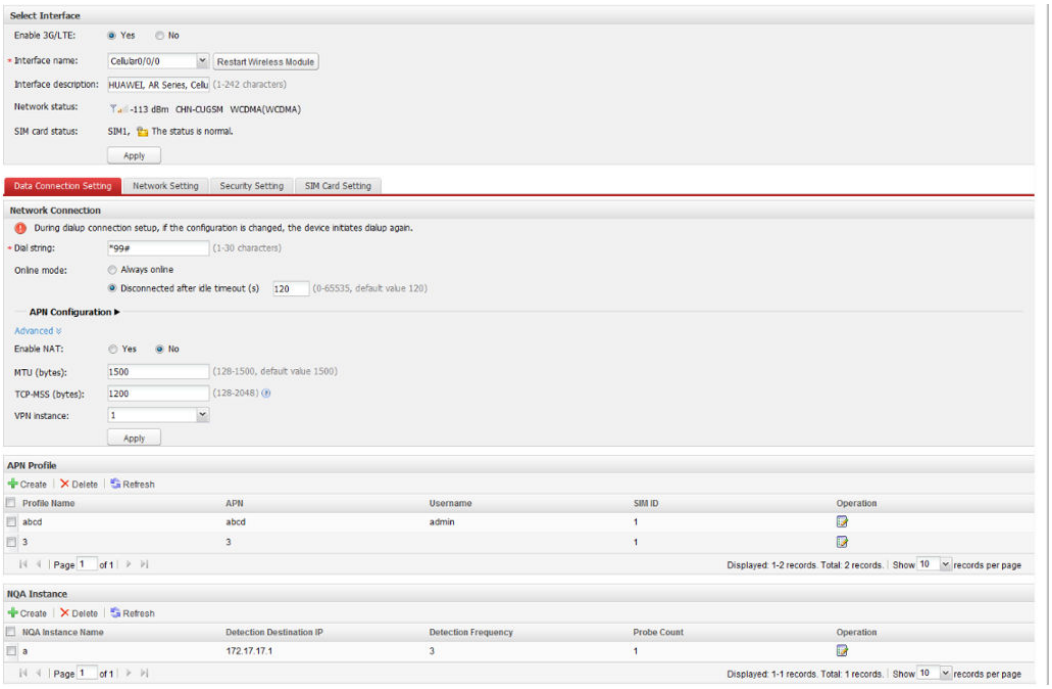
- In remote branch companies or offshore oil fields, the wired WAN access service may be unavailable or too expensive.
- The wired WAN access service is restored on the disaster site only after wires are connected quickly and in a timely manner.
- The wired WAN cannot cover all gas stations and ATMs that are widely distributed.
- Enterprise staff require mobile office applications.

In these scenarios, wireless WAN access service is required. A 3G/LTE cellular interface is a physical interface supporting 3G/LTE technology. It provides users with an enterprise-class wireless WAN access services.

Procedure

Step 1 Choose **WAN Access** > **3G/LTE Interface** to display the 3G/LTE Interface page, as shown in **Figure 2-73**.

Figure 2-73 3G/LTE Interface Page



Step 2 Select the 3G/LTE interface to be configured, as shown in **Table 2-55**. After you finish the configuration, click **Apply**.

Copyright © Huawei Technologies Co., Ltd.

Table 2-55 Selecting a 3G/LTE interface

Parameter	Description
Enable 3G/LTE	Only after the 3G/LTE function is enabled, 3G/LTE dialup can be triggered.
Interface name	Type and number of an interface. **NOTE** The interface can be configured only when a 3G/LTE Interface and the corresponding SIM card are inserted into the device. When you need to manually restart the 3G/LTE Interface, click **Restart Wireless Module**.
Interface description	Description of an interface. By default, the interface description is "HUAWEI, AR Series, *interface-type interface-number* Interface."
Network status	Signal strength, carrier, and network mode of the 3G/LTE wireless WAN card. **NOTE** The information is displayed only when a 3G/LTE Interface and the corresponding SIM card are inserted into the device.
SIM card status	Status of an SIM card.

Step 3 Click **Data Connection Setting** to set data connection parameters.

1. (Optional) Configure a test instance.

   This step is mandatory if you want to test the 3G/LTE link status using an NQA test instance.

   a. Click **Create** in the **NQA Instance** area to create an NQA test instance, as shown in **Figure 2-74**.
   b. Set the parameters described in **Table 2-56**.
   c. Click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-74 Create NQA Instance Page

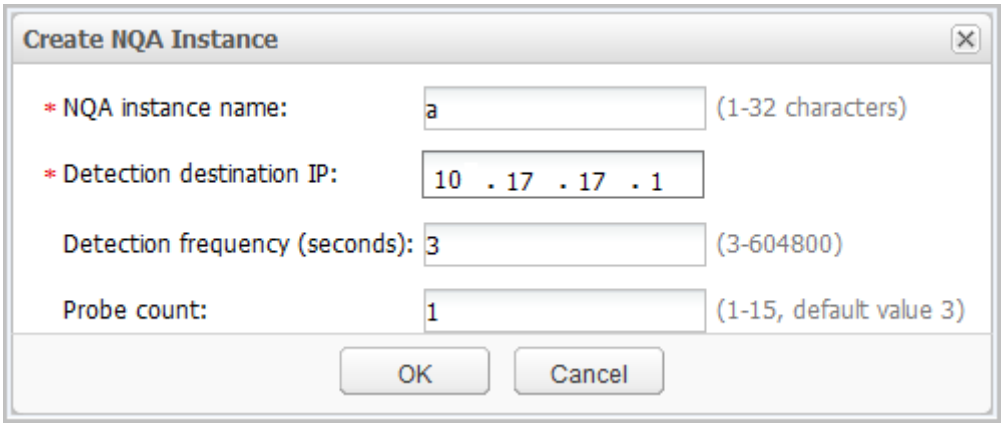


Table 2-56 Parameters for creating a test instance

Parameter	Description
NQA Instance name	Name of an NQA test instance.
Detection Destination IP	Destination address of the NQA test instance. **NOTE** The route from the device to the destination address of the NQA test instance must be reachable.
Detection frequency (seconds)	Interval for automatically performing the NQA test, in seconds.
Probe count	Number of probes to be sent each time for the NQA test instance.

NOTE

To modify an NQA test instance, find it in the **Operation** column of **NQA Instance**, click , and set the parameters described in **Table 2-56**.

2. Configure an APN profile.

NOTE

APN profiles only need to be configured for the 3G/LTE Interfaces in WCDMA and LTE networks. Skip this step if you use the 3G interface in CDMA2000 networks.

You can create an APN profile and configure an APN in the profile so that you can access external PDN networks using the configured APN.

a. Click **Create** in the **APN Profile** area to create an APN profile, as shown in **Figure 2-75**.

 Copyright © Huawei Technologies Co., Ltd.

b. Set the parameters described in **Table 2-57**.

c. Click **OK**.

Figure 2-75 Create APN Profile Page

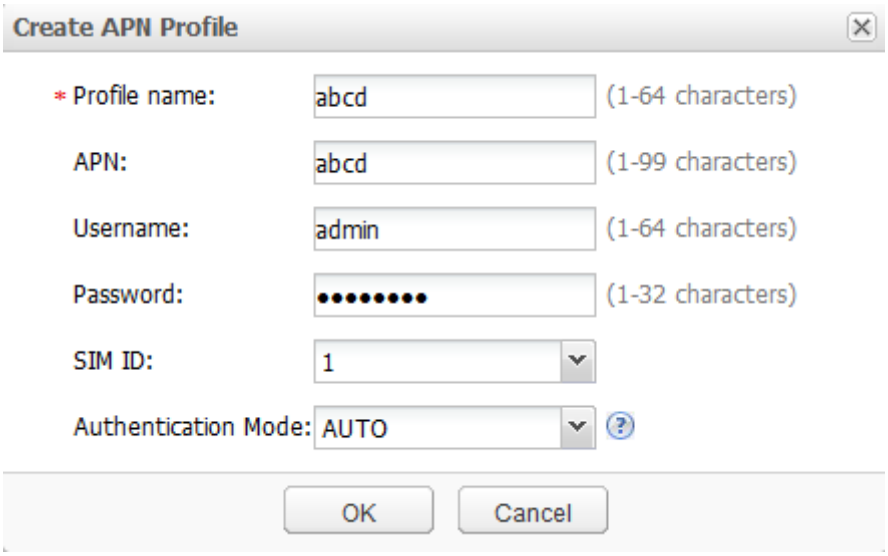


Table 2-57 Parameters for creating an APN profile

Parameter	Description
Profile Name	Name of the APN profile.
APN	APN specified. **NOTE** APNs are provided by the carrier.
Username	User name for accessing an external PDN network, which is provided by the carrier.
Password	User password for accessing an external PDN network, which is provided by the carrier.
SIM ID	Specifies the ID of a SIM card.

NOTE

To modify an APN profile, find it in the **Operation** column of **APN Profile**, click , and set the parameters described in **Table 2-57**.

3. Set the network connection parameters described in **Table 2-58**.

 Copyright © Huawei Technologies Co., Ltd.

Table 2-58 Network connection parameters

Parameter	Description
Dial string	Dialup string that is provided by the carrier. – The default dialup string is *99# when the 3G/LTE Interface supports WCDMA or LTE standard. – The default dialup string is #777 when the 3G/LTE Interface supports CDMA2000 standard.
Online mode	Dialup mode. – When this parameter is set to **Always online**, the DCC immediately attempts to dial the remote end after a router starts. The dialing process is not triggered by data packets. If a connection cannot be established with the remote end, the router retries at an interval. The value **Always online** applies to scenarios where traffic and online duration are not charged. – When this parameter is set to **Disconnected after idle timeout (s)**, a link is established only when data is transmitted. When no traffic exists on the link within a specified period, the router removes the link to save traffic. The value **Disconnected after idle timeout (s)** applies to scenarios where traffic and online duration are charged. When setting this parameter to **Disconnected after idle timeout (s)**, specify the link idle timeout period. The default value is 120.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
APN Configuration	Bind the APN profile to a 3G/LTE interface. – The APN profile priority must be specified when multiple SIM cards can be inserted into a 3G/LTE data card. – The test instance must be specified if you want to test the 3G/LTE link status using an NQA test instance. **NOTE** To bind multiple APN profiles to a 3G/LTE interface, click  . To unbind an APN profile from a 3G/LTE interface, click  .
Enable NAT	NAT must be enabled when a PC on a private network connects to the Internet.
MTU (bytes)	MTU of an interface. If the MTU is set too small and the size of packets is oversized, packets will be divided into a great number of fragments, and be discarded by QoS queues. If the MTU is set too large, packets are transmitted at a low speed, and even some packets are lost. After changing the MTU of the interface, restart the interface to make the configuration take effect. The default value of **MTU** is 1500.
TCP-MSS (bytes)	MSS of TCP packets on the interface. The MSS refers to the maximum length of a TCP packet segment sent from the peer device to the local device. During TCP connection negotiation, devices at both ends record the MSS of each other. When sending TCP packets, devices at both ends limit the size of TCP packets within the MSS. The recommended value of **TCP-MSS** is 1200.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
VPN instance	VPN instance bound to the interface.

4. Click **Apply**.

Step 4 Click **Network Setting** to configure the network connection mode of the 3G/LTE Interface, as shown in **Table 2-59**. After completing the configuration, click **Apply**.

Table 2-59 Network setting (CDMA2000)

Parameter	Description
1xrtt-only	Indicates that a 3G data card connects to a 1x radio transmission technology (1xRTT) network.
evdo-only	Indicates that a 3G data card connects to an evolution-data optimized (EV-DO) network.
hybrid	Indicates that a 3G data card connects to a 1xRTT and EV-DO combined network.

Table 2-60 Network setting (WCDMA)

Parameter	Description
gsm-only	Indicates that a 3G data card connects to a GSM network.
gsm-precedence	Indicates that a 3G data card preferentially connects to a GSM network.
wcdma-only	Indicates that a 3G data card connects to a WCDMA network.
wcdma-precedence	Indicates that a 3G data card preferentially connects to a WCDMA network.

Table 2-61 Network setting (LTE)

Parameter	Description
auto	Indicates that an LTE data card automatically connects to a network.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
gsm-only	Indicates that an LTE data card connects to a GSM network.
lte-only	Indicates that an LTE data card connects to a LTE network.
umts-gsm	Indicates that an LTE data card connects to either a UMTS or GSM network and preferentially connects to the UMTS network. **NOTE** The 1LTEC interface card and 1LTE-Lt-7 interface card supports this parameter.
umts-only	Indicates that an LTE data card connects to either a WCDMA or TD-SCDMA network. **NOTE** The 1LTEC interface card and 1LTE-Lt-7 interface card supports this parameter.
wcdma-gsm	Indicates that an LTE data card connects to either a WCDMA or GSM network and preferentially connects to the WCDMA network. **NOTE** The 1LTEC interface card and 1LTE-Lt-7 interface card does not support this parameter.
wcdma-only	Indicates that an LTE data card connects to a WCDMA network. **NOTE** The 1LTEC interface card and 1LTE-Lt-7 interface card does not support this parameter.

Step 5 Click **Security Setting** to set a PIN code, as shown in **Table 2-62**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-76 Security Setting Page

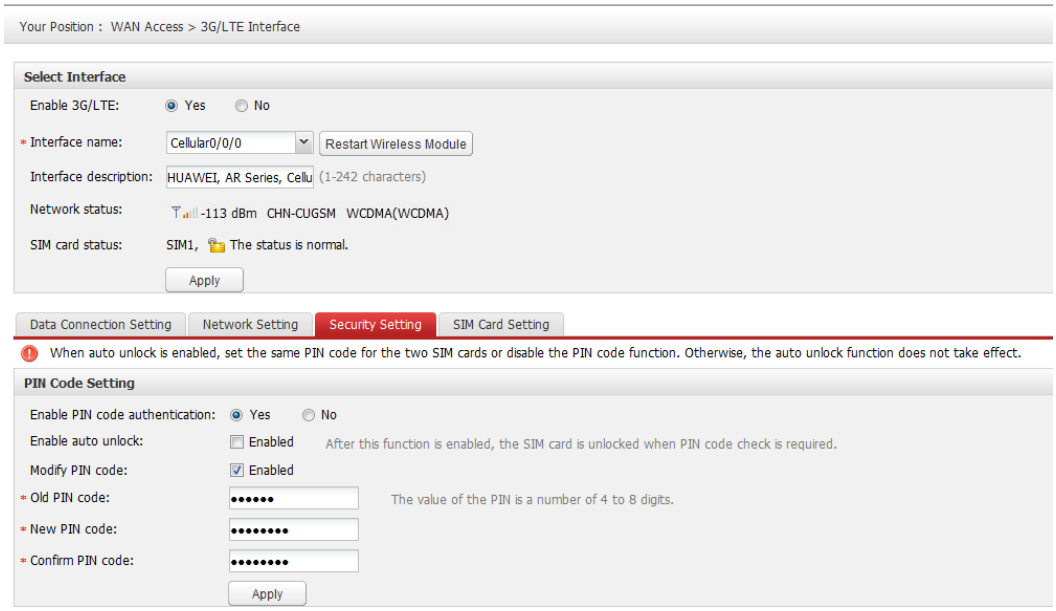


Table 2-62 Parameters for setting a PIN code

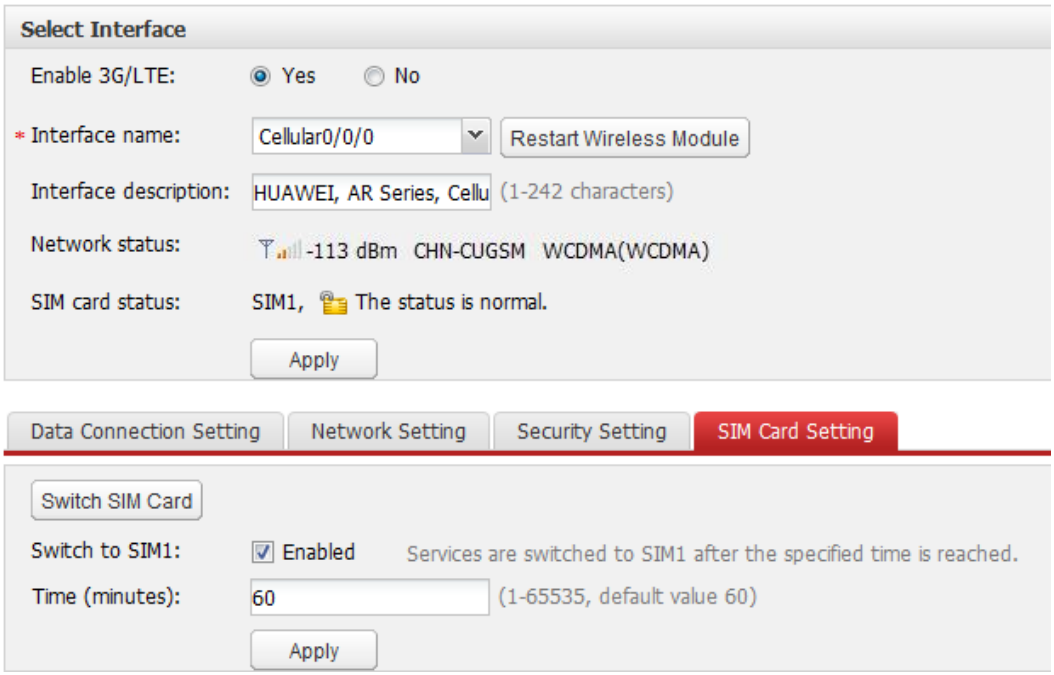
Parameter	Description
Enable PIN code authentication	Whether PIN authentication is performed.
PIN code	PIN code to be entered for authentication. After you enter the PIN code, click **Apply**. **NOTE** If you enter incorrect PINs three consecutive times, the SIM card is locked. You must use the PUK code to unlock the SIM card. After you enter the PUK code and new PIN code, click **Apply**.
Enable auto unlock	Indicates automatic PIN authentication. This parameter can be specified if you do not require high security of the SIM card. After this parameter is specified, you do not need to enter the PIN every time you restart the 3G/LTE Interface.
Modify PIN code	Whether a PIN code is modified.
Old PIN code	Enter the old PIN code.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
New PIN code	Enter the new PIN code.
Confirm PIN code	Enter the new PIN code again.

Step 6 Click **SIM Card Setting** to set the SIM cards for the 3G/LTE interface that has dual SIM cards, as shown in **Table 2-63**. After you finish the configuration, click **Apply**.

Figure 2-77 SIM Card Setting Page



NOTE

The dual-SIM functions can be configured only on the LTE cellular interface (Cellular 0/0/0) supported by the AR109GW-L, AR121GW-L, AR129GW-L, AR129CGVW-L, AR161FG-Lc, AR161FG-L, AR169FGW-L, AR169FGVW-L, AR169G-L, AR169EGW-L, AR161G-L, AR161G-Lc, AR161FGW-La, AR161FGW-Lc, and AR161FGW-L.

Table 2-63 SIM Card Setting

Parameter	Description
Switch to SIM1	Whether the backup SIM card is enabled to automatically switch to the primary SIM card. Click **Switch SIM Card** to manually switch the SIM card.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Time (minutes)	Time after which the backup SIM card can automatically switch to the primary SIM card if the function is enabled.

----End

2.12.4 SA Interface

Context

NOTE

The 1SA/2SA/8SA interface cards support serial interfaces. For the mapping between the device and interface card, see 1SA (1-Port-Synchronous/Asynchronous WAN Interface Card), 2SA (2-Port-Synchronous/Asynchronous WAN Interface Card) or 8SA (8-Port Synchronous/Asynchronous WAN Interface Card) in the *Huawei AR Series Access Routers Get to Know the Product-Hardware Description-Cards-Synchronous/Asynchronous Card*.

The AR162F and AR2202-48FE routers support serial interfaces.

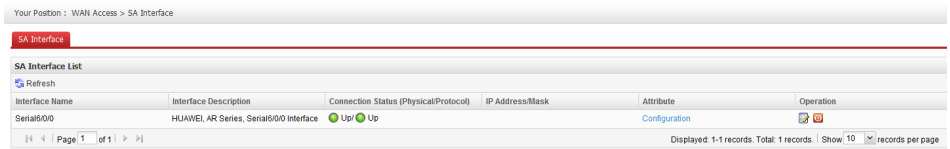
The serial interface on the AR162F and the main control board of AR2202-48FE can work only in synchronous mode and function as only a DTE interface.

Synchronous SA interfaces are used for enterprise branches to communicate with the headquarters through PPP or HDLC links.

Procedure

- Modifying SA interface configuration
  a. Choose **WAN Access** > **SA Interface** to display the **SA Interface** page. **Figure 2-78** shows **SA Interface** page

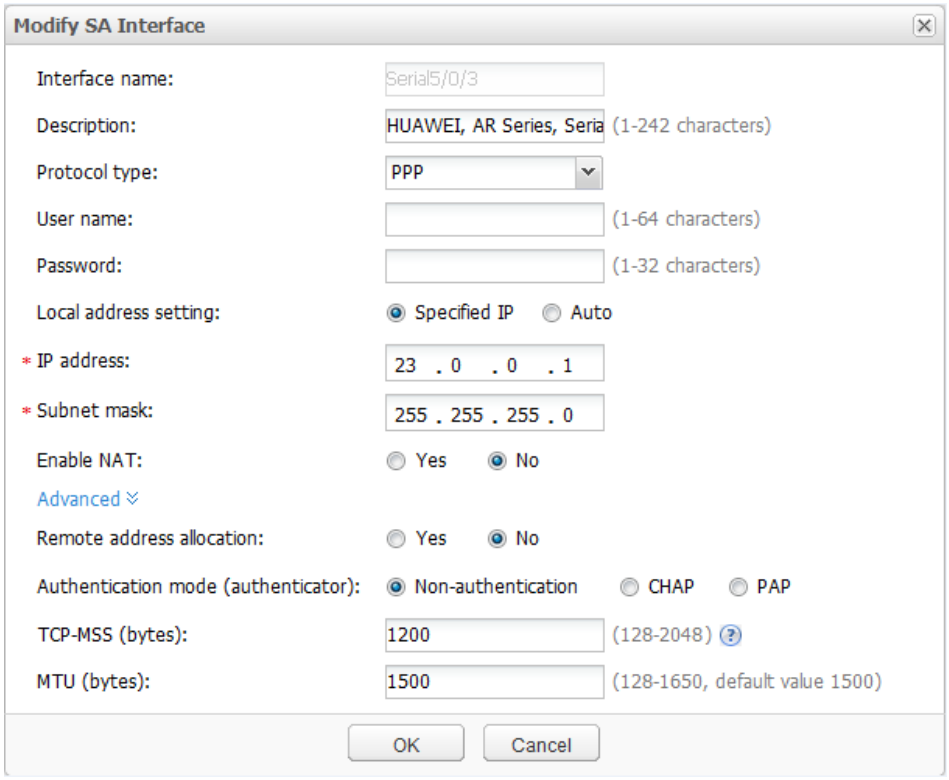
     Figure 2-78 SA Interface Page

  b. Click  corresponding to the SA interface to be configured in the **Operation** column of **SA Interface List** to display the modification page.
  c. Set the parameters described in **Table 2-64**.
  d. Click **OK** to complete the configuration.

 Copyright © Huawei Technologies Co., Ltd.

– **Figure 2-79** Modify SA Interface (Protocol type is PPP)



– **Figure 2-80** Modify SA Interface (Protocol type is HDLC)

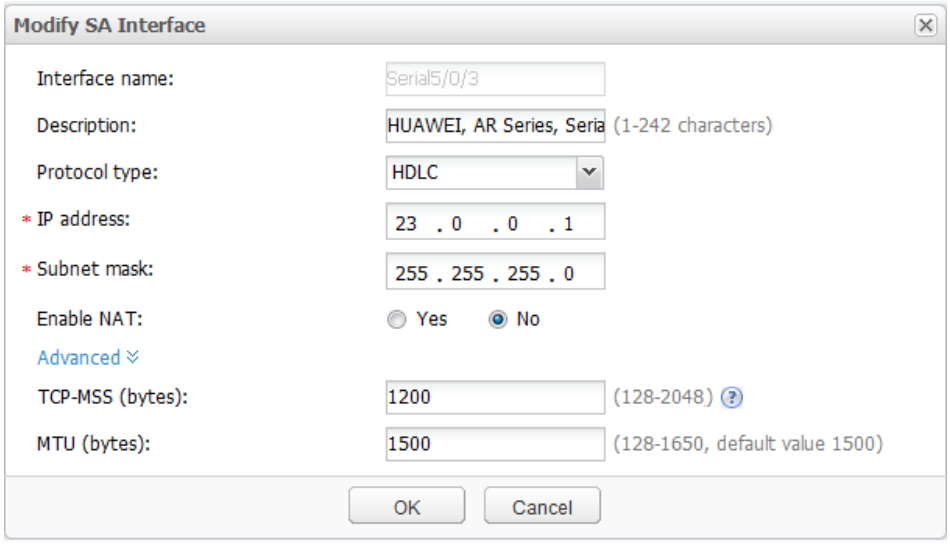


Table 2-64 Description of the SA interface parameters

Parameter	Description
Interface name	Type and number of an interface.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Description	Description of an interface. By default, the description of an interface is empty.
Protocol type	Link layer protocol of an SA interface. • PPP: indicates that the link layer protocol of an SA interface is PPP, as shown in **Figure 2-79**. For the description of PPP protocol parameters, see **Table 2-65**. • HDLC: indicates that the link layer protocol of an SA interface is HDLC, as shown in **Figure 2-80**. For the description of PPP protocol parameters, see **Table 2-66**.

Table 2-65 Description of the PPP protocol parameters

Parameter	Description
User name	User name of the device that functions as the authenticated party.
Password	Password of the device that functions as the authenticated party.
Local address setting	Mode in which an interface obtains an IP address. • Specified IP: indicates that an IP address is manually configured on the interface. • Auto: indicates that an IP address is obtained through PPP negotiation.
IP address	IP address of an interface. The interface IP address cannot conflict with the IP addresses of other interfaces on the device or other devices in the network. **NOTE** This parameter is valid only when **Local address setting** is set to **Specified IP**.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Subnet mask	Subnet mask of an interface. **NOTE** This parameter is valid only when **Local address setting** is set to **Specified IP**.
Enable NAT	NAT must be enabled when a PC on the private network of a LAN connects to the Internet.
Remote address allocation	Whether the local device assigns an IP address for the peer device. **NOTE** This parameter is valid only when **Local address setting** is set to **Specified IP**.
Remote address	The IP address assigned by the local device for the remote device. **NOTE** This parameter is valid only when **Remote address allocation** is set to **Yes**.
Authentication mode (authenticator)	Authentication mode of the device that functions as the authenticated party. PPP authentication can be performed on the device. • Non-authentication: indicates that PPP authentication is not performed on the device. • PAP: indicates that the PPP authentication mode is PAP. • CHAP: indicates that the PPP authentication mode is CHAP.
TCP-MSS (bytes)	MSS of TCP packets on an interface. The MSS refers to the maximum length of a TCP packet segment sent from the peer device to the local device. During TCP connection negotiation, devices at both ends record the MSS of each other. When sending TCP packets, the devices limit the size of TCP packets within the MSS. The recommended value of **TCP-MSS** is 1200.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
MTU (bytes)	MTU of an interface. If the MTU is set too small and the size of packets is quite large, packets will be broken into a great number of fragments and be discarded by QoS queues. If the MTU is too large, packets are transmitted slowly or even lost. After modifying the interface MTU, you must restart the interface to make the MTU setting take effect. The default value of **MTU** is 1500.

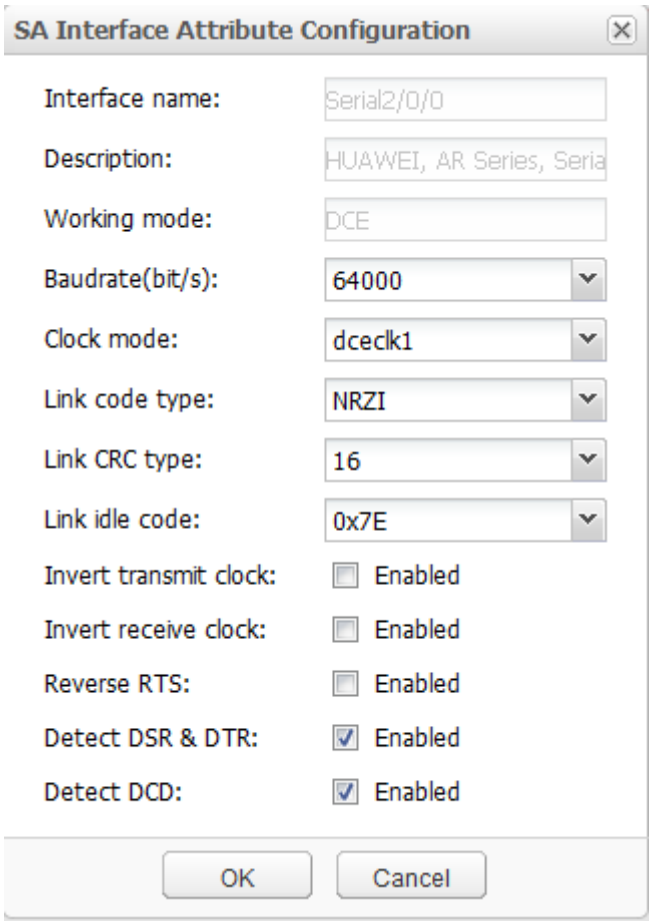
Table 2-66 Description of the HDLC protocol parameters

Parameter	Description
IP address	IP address of an interface. The interface IP address cannot conflict with the IP addresses of other interfaces on the device or other devices in the network.
Subnet mask	Subnet mask of an interface.
Enable NAT	NAT must be enabled when a PC on the private network of a LAN connects to the Internet.
TCP-MSS (bytes)	MSS of TCP packets on an interface. The MSS refers to the maximum length of a TCP packet segment sent from the peer device to the local device. During TCP connection negotiation, devices at both ends record the MSS of each other. When sending TCP packets, the devices limit the size of TCP packets within the MSS. The recommended value of **TCP-MSS** is 1200.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
MTU (bytes)	MTU of an interface. If the MTU is set too small and the size of packets is quite large, packets will be broken into a great number of fragments and be discarded by QoS queues. If the MTU is too large, packets are transmitted slowly or even lost. After modifying the interface MTU, you must restart the interface to make the MTU setting take effect. The default value of **MTU** is 1500.

- Configuring the physical attributes and link layer attributes of an SA interface
  a. Choose **WAN Access** > **SA Interface** to display the **SA Interface** page.
  b. Click **Configuration** in the **Attribution** column of **SA Interface List** to display the page for configuring the SA interface attributes.
  c. Set the parameters described in **Table 2-67** or **Table 2-68**.
  d. Click **OK** to complete the configuration.
  – **Figure 2-81** SA Interface Attribute Configuration (DCE mode)



Copyright © Huawei Technologies Co., Ltd.

– **Figure 2-82** SA Interface Attribute Configuration (DTE mode)

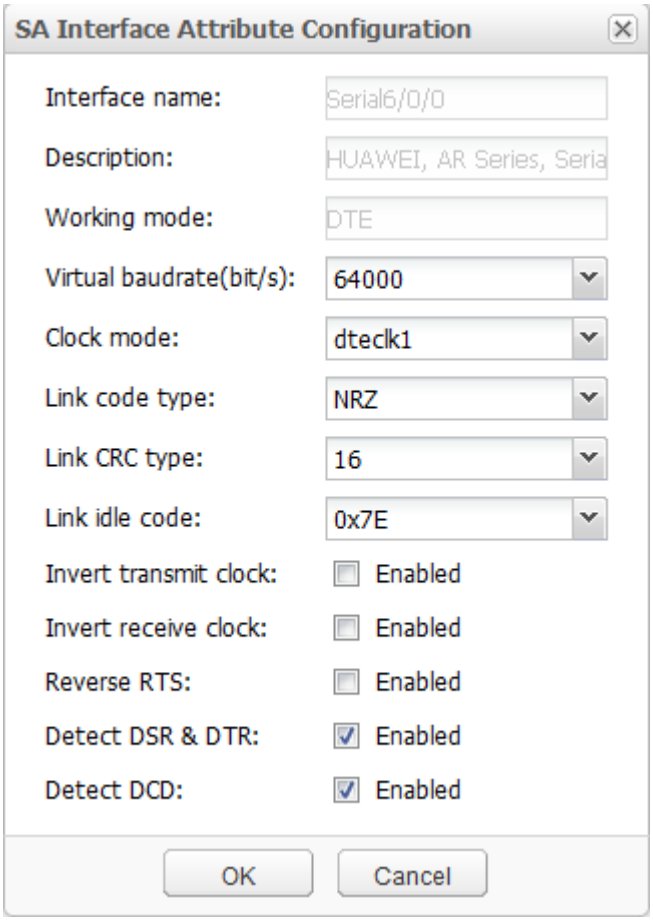


Table 2-67 Description of the SA interface's physical attributes and link layer attributes (DCE mode)

Parameter	Description
Interface name	Type and number of an interface.
Description	Description of an interface. By default, the interface description is "HUAWEI, AR Series, interface-type interface-number Interface."
Working mode	Working mode of an SA interface including DTE mode and DCE mode.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Baudrate(bit/s)	Baud rate of an SA interface. The baud rate can be set only when the device functions as the DCE. The baud rate range varies depending on the cable type. ● V.24DTE/DCE: 1200 bit/s to 64000 bit/s ● V.35DTE/DCE, X.21DTE, RS449DTE/DCE, and RS530DTE/DCE: 1200 bit/s to 2048000 bit/s
Clock mode	Clock mode for an SA interface on the DCE. ● dceclk1: indicates that the clock mode of an SA interface is set to dceclk1 on the DCE. ● dceclk2: indicates that the clock mode of an SA interface is set to dceclk2 on the DCE. ● dceclk3: indicates that the clock mode of an SA interface is set to dceclk3 on the DCE.
Link code type	Link code type of an SA interface. ● NRZ: Non Return to Zero ● NRZI: Non Return to Zero Inverted If two devices communicate using SA interfaces, the two devices must have the same encoding and decoding mode. Otherwise, received data frames will be decoded incorrectly and discarded as error frames.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Link CRC type	CRC mode of an SA interface. ● 16: indicates that the 16-bit CRC is used for an SA interface. ● 32: indicates that the 32-bit CRC is used for an SA interface. ● none: indicates that CRC is not performed for an SA interface. The interfaces on both ends of a link must use the CRC of the same length. If lengths of the CRCs used on two ends are different, the two devices cannot communicate with each other.
Link idle code	Line idle code type of an SA interface. ● 0x7E ● 0xFF Two devices can communicate properly only when the same line idle code is set for the interfaces on both devices.
Invert transmit clock	Whether clock signals transmitted by an SA interface are inverted.
Invert receive clock	Whether clock signals received by an SA interface are inverted.
Reverse RTS	Whether RTS signals of an SA interface are inverted.
Detect DSR & DTR	Whether detection of DSR and DTR signals on an SA interface is enabled.
Detect DCD	Whether detection of DCD signals on an SA interface is enabled.

Table 2-68 Description of the SA interface's physical attributes and link layer attributes (DTE mode)

Parameter	Description
Interface name	Type and number of an interface.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Description	Description of an interface. By default, the interface description is "HUAWEI, AR Series, interface-type interface-number Interface."
Working mode	Working mode of an SA interface including DTE mode and DCE mode.
Virtual baudrate(bit/s)	Virtual baud rate of an SA interface. The virtual baud rate can be set only when the device functions as the DTE. **NOTE** Ensure that the configured virtual baud rate is the same as that on the remote end (DCE). Otherwise, some packets will be discarded.
Clock mode	Clock mode for an SA interface on the DTE. ● dteclk1: indicates that the clock mode of an SA interface is set to dteclk1 on the DTE. ● dteclk2: indicates that the clock mode of an SA interface is set to dteclk2 on the DTE. ● dteclk3: indicates that the clock mode of an SA interface is set to dteclk3 on the DTE.
Link code type	Link code type of an SA interface. ● NRZ: Non Return to Zero ● NRZI: Non Return to Zero Inverted If two devices communicate using SA interfaces, the two devices must have the same encoding and decoding mode. Otherwise, received data frames will be decoded incorrectly and discarded as error frames.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Link CRC type	CRC mode of an SA interface. • 16: indicates that the 16-bit CRC is used for an E1 interface. • 32: indicates that the 32-bit CRC is used for an E1 interface. • none: indicates that CRC is not performed for an E1 interface. The interfaces on both ends of a link must use the CRC of the same length. If lengths of the CRCs used on two ends are different, the two devices cannot communicate with each other.
Link idle code	Line idle code type of an SA interface. • 0x7E • 0xFF Two devices can communicate properly only when the same line idle code is set for the interfaces on both devices.
Invert transmit clock	Whether clock signals transmitted by an SA interface are inverted.
Invert receive clock	Whether clock signals received by an SA interface are inverted.
Reverse RTS	Whether RTS signals of an SA interface are inverted.
Detect DSR & DTR	Whether detection of DSR and DTR signals on an SA interface is enabled.
Detect DCD	Whether detection of DCD signals on an SA interface is enabled.

- Disabling an SA interface
  a. Choose **WAN Access** > **SA Interface** to display the **SA Interface page.**
  b. Click corresponding to the SA interface to be configured in the **Operation** column of **SA Interface List**.
  c. Click **OK**.
- Enabling an SA interface
  a. Choose **WAN Access** > **SA Interface** to display the **SA Interface page.**
  b. Click corresponding to the SA interface to be configured in the **Operation** column of **SA Interface List**.

Copyright © Huawei Technologies Co., Ltd.

c. Click **OK**.

----End

2.12.5 CE1/CT1 Interface

Context

NOTE

- The 1E1/T1-M, 2E1/T1-M, 4E1/T1-M, and 8E1/T1-M interface cards support CE1/PRI interfaces. For the mapping between the device and interface card, see *1/2/4/8 Port-Channelized E1/T1/PRI/VE1 Multiflex Trunk Interface Card* in the *Huawei AR Series Access Routers Get to Know the Product-Hardware Description-Cards-WAN Interface Card*.
- The 1E1/T1-M and 2E1/T1-M interface cards support CT1/PRI interfaces. For the mapping between the device and interface card, see *1/2/4/8 Port-Channelized E1/T1/PRI/VE1 Multiflex Trunk Interface Card* in the *Huawei AR Series Access Routers Get to Know the Product-Hardware Description-Cards-WAN Interface Card*.

A CE1/CT1 interface is a physical interface in the E1/T1 system, which can transmit voice, data, and video service packets.

Procedure

- Modifying CE1/CT1 interface configuration
  a. Choose **WAN access** > **CE1/CT1 Interface**. Click **CE1 Interface** or **CT1 Interface** to display the **CE1 Interface** or **CT1 Interface** tab page. **Figure 2-83** shows **CE1 Interface** page and **CT1 Interface** page.

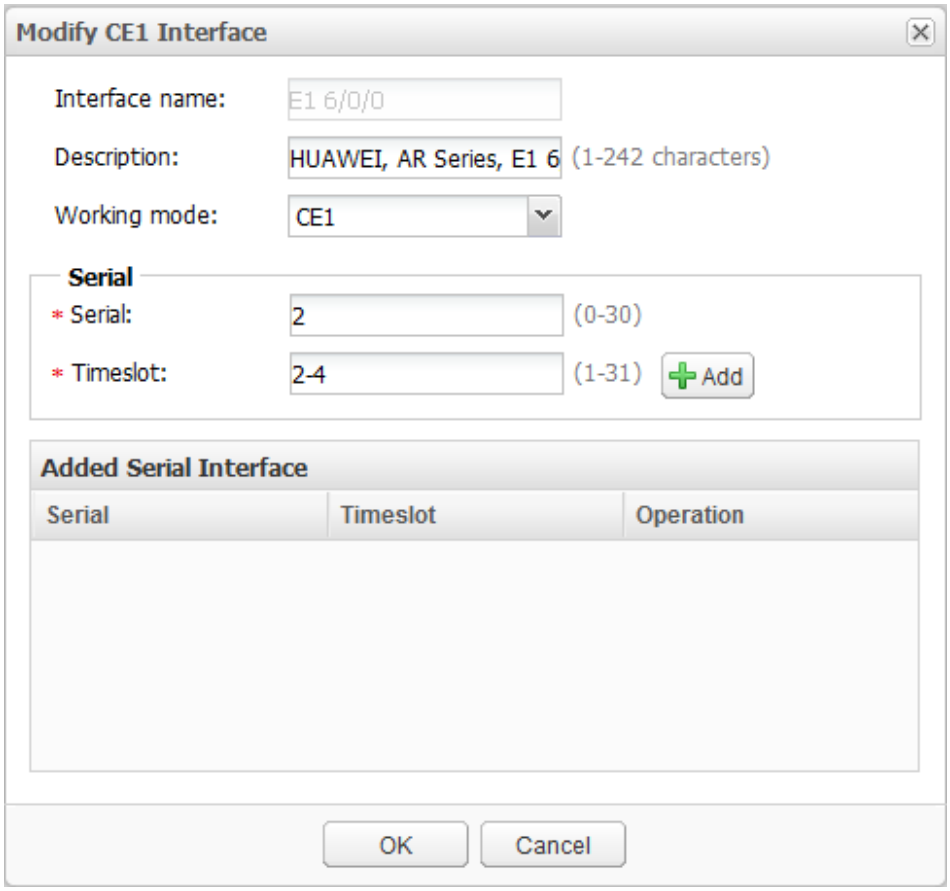
  Figure 2-83 CE1 Interface Page

  b. Click  corresponding to the CE1 or CT1 interface to be configured in the **Operation** column of **CE1 Interface List** or **CT1 Interface List** to display the modification page.
  c. Set the parameters described in **Table 2-69**.
  d. Click **OK** to complete the configuration.

Copyright © Huawei Technologies Co., Ltd.

– **Figure 2-84** Modify CE1 Interface



 Copyright © Huawei Technologies Co., Ltd.

– **Figure 2-85** Modify CT1 Interface

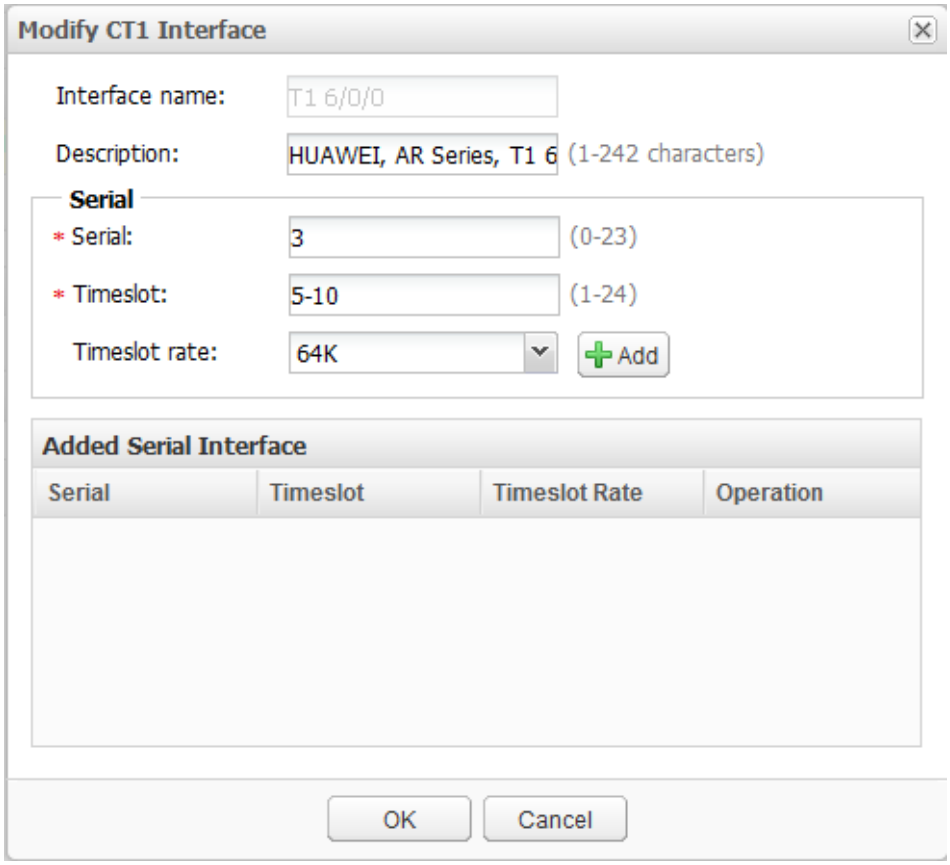


Table 2-69 Description of the CE1/CT1 interface parameters

Parameter	Description
Interface name	Type and number of an interface.
Description	Description of an interface. By default, the description of an interface is empty.
Working mode	Working mode of a CE1 interface. • CE1: indicates that a CE1 interface works in CE1 mode. • E1: indicates that a CE1 interface works in E1 mode.
serial	Serial number of the specified channel when a CE1/CT1 interface works in CE1/CT1 mode.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Timeslot	Timeslot of the channel after the channel number is specified. **NOTE** To create a channel, click **Add**.

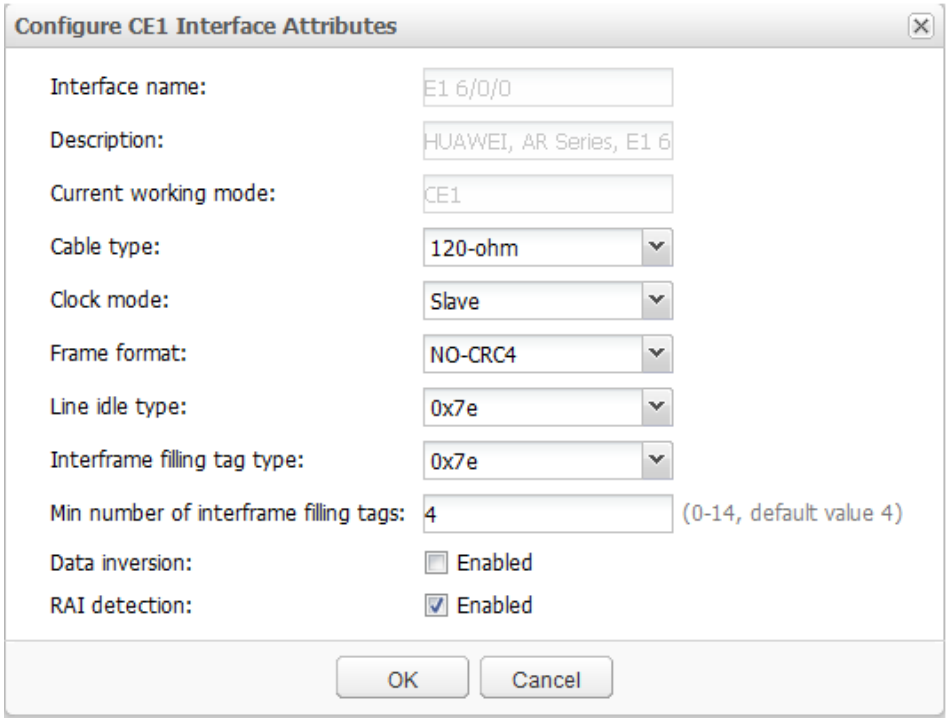
After the CE1/CT1 interface configuration is complete, the system creates one or more serial interfaces whose logical features are the same as those of a synchronous serial interface.

- To modify the serial interface configuration, see **Modifying a serial interface configuration**.
- To delete a serial interface, see **Deleting a serial interface**.
- To disable a serial interface, see **Disabling a serial interface**.
- To enable a serial interface, see **Enabling a serial interface**.

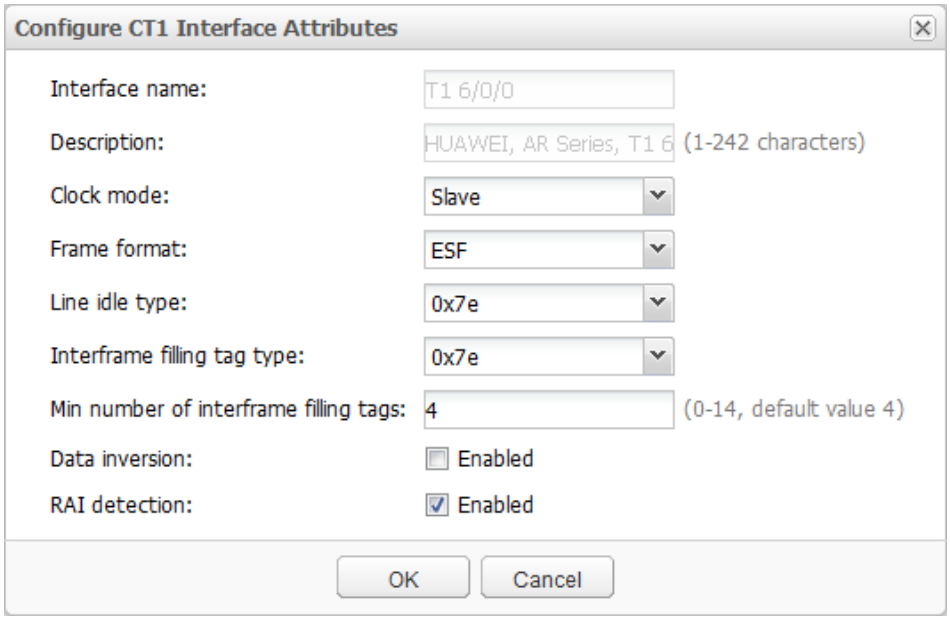
- Configuring the physical attributes and link layer attributes of a CE1/CT1 interface
  a. Choose **WAN access** > **CE1/CT1 Interface**. Click **CE1 Interface** or **CT1 Interface** to display the **CE1 Interface** or **CT1 Interface** tab page.
  b. Click **Configure Interface Attribution** in the **Interface Attribution** column of **CE1 Interface List** or **CT1 Interface List** to display the interface attribute configuration page.
  c. Set the parameters.
     - For the physical attributes and link layer attributes of a CE1 interface, see **Table 2-70**.
     - For the physical attributes and link layer attributes of a CT1 interface, see **Table 2-71**.
  d. Click **OK** to complete the configuration.

Copyright © Huawei Technologies Co., Ltd.

– **Figure 2-86** Configure CE1 Interface Attributes



– **Figure 2-87** Configure CT1 Interface Attributes



 Copyright © Huawei Technologies Co., Ltd.

Table 2-70 Description of the CE1 interface's physical attributes and link layer attributes

Parameter	Description
Cable type	Cable type applicable to a CE1 interface. • 120-ohm: indicates that a CE1 interface connects to a 120 ohm balanced cable (twisted pair). • 75-ohm: indicates that a CE1 interface connects to a 75 ohm non-balanced cable (coaxial cable).
Clock mode	Clock mode of a CE1 interface. • Master: indicates the master clock mode (internal clock mode). • Slave: indicates the slave clock mode (line clock mode). • System: indicates the system clock mode. **NOTE** This parameter takes effect only when it is configured on interfaces of the 4E1T1-M/8E1T1-M interface card. When two routers are directly connected using two CE1 interfaces, one CE1 interface must work in master clock mode and the other must work in slave clock mode. When the MPU on the router obtains the clock with high accuracy from the upstream device and the router needs to synchronize the clock to downstream device, the interface on the router must be configured to work in system clock mode. Moreover, the interface on the downstream device must be configured to work in slave clock mode.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Frame format	Frame format of a CE1 interface. • CRC4: indicates the CRC4 frame format. • NO-CRC4: indicates the non-CRC4 frame format (basic frame format). Two devices can communicate properly only when the same frame format is set for the interfaces on both devices. Otherwise, a CRC4 alarm is generated. **NOTE** This attribute is valid only when **Working mode** in Table 2-69 is set to **CE1**.
Line idle type	Line idle code type of a CE1 interface. • 0x7e • 0xff Two devices can communicate properly only when the same line idle code is set for the interfaces on both devices.
Interframe filling tag type	Interframe filling tag type of a CE1 interface. • 0x7e • 0xff Interfaces on both ends can communicate only when the same interframe filling tag and the same minimum number of interframe filling tags are set for them.
Min number of interframe filling tags	Minimum number of interframe filling tags of a CE1 interface. Interfaces on both ends can communicate only when the same interframe filling tag and the same minimum number of interframe filling tags are set for them.
Data inversion	Whether data inversion is configured for a CE1 interface. CE1 interfaces on both ends can communicate only when they have the same data inversion configuration.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
RAI detection	Whether Remote Alarm Indication (RAI) detection is enabled for a CE1 interface. **NOTE** This attribute is valid only when **Working mode** in **Table 2-69** is set to **CE1**.
AIS detection	Whether Alarm Indication Signal (AIS) detection is enabled for a CE1 interface. **NOTE** This attribute is valid only when **Working mode** in **Table 2-69** is set to **E1**. If the CE1 interface works in E1 mode, AIS detection must be disabled.

Copyright © Huawei Technologies Co., Ltd.

Table 2-71 Description of the CT1 interface's physical attributes and link layer attributes

Parameter	Description
Clock mode	Clock mode of a CT1 interface. ● Master: indicates the master clock mode (internal clock mode). ● Slave: indicates the slave clock mode (line clock mode). ● System: indicates the system clock mode. **NOTE** This parameter takes effect only when it is configured on interfaces of the 4E1T1-M/8E1T1-M interface card. When two routers are directly connected using two CT1 interfaces, one CT1 interface must work in master clock mode and the other must work in slave clock mode. When the MPU on the router obtains the clock with high accuracy from the upstream device and the router needs to synchronize the clock to downstream device, the interface on the router must be configured to work in system clock mode. Moreover, the interface on the downstream device must be configured to work in slave clock mode.
Frame format	Frame format of a CT1 interface. ● ESF: indicates the Extended Super Frame (ESF) format. ● SF: indicates the Super Frame (ESF) format. Two devices can communicate properly only when the same frame format is set for the interfaces on both devices. Otherwise, a CRC4 alarm is generated.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Line idle type	Line idle code type of a CT1 interface. ● 0x7e ● 0xff Two devices can communicate properly only when the same line idle code is set for the interfaces on both devices.
Interframe filling tag type	Interframe filling tag type of a CT1 interface. ● 0x7e ● 0xff Interfaces on both ends can communicate only when the same interframe filling tag and the same minimum number of interframe filling tags are set for them.
Min number of interframe filling tags	Minimum number of interframe filling tags of a CT1 interface. Interfaces on both ends can communicate only when the same interframe filling tag and the same minimum number of interframe filling tags are set for them.
Data inversion	Whether data inversion is configured for a CT1 interface. CT1 interfaces on both ends can communicate only when they have the same data inversion configuration.
RAI detection	Whether RAI detection is enabled for a CT1 interface.

- Disabling a CE1/CT1 interface
  a. Choose **WAN access** > **CE1/CT1 Interface**. Click **CE1 Interface** or **CT1 Interface** to display the **CE1 Interface** or **CT1 Interface** tab page.
  b. Click  corresponding to the CE1 or CT1 interface to be configured in the **Operation** column of **CE1 Interface List** or **CT1 Interface List**.
  c. Click **OK**.
- Enabling a CE1/CT1 interface
  a. Choose **WAN access** > **CE1/CT1 Interface**. Click **CE1 Interface** or **CT1 Interface** to display the **CE1 Interface** or **CT1 Interface** tab page.

Copyright © Huawei Technologies Co., Ltd.

b. Click corresponding to the CE1 or CT1 interface to be configured in the **Operation** column of **CE1 Interface List** or **CT1 Interface List**.

c. Click **OK**.

- Switching the mode of a CE1/CT1 interface

  NOTE

  The 4E1T1-M/8E1T1-M interface card only works in CE1/PRI mode and does not support working mode switching.

  a. Choose **WAN access** > **CE1/CT1 Interface** > **Switch Mode** to display the **Switch Mode** tab page.

  b. Click corresponding to the CE1 or CT1 interface whose mode needs to be switched in the **Operation** column of **CE1 Card List** or **CT1 Card List**.

  Only the 1E1T1-M/2E1T1-M board supports mode switching.

  c. Click **OK**.

  The configuration takes effect after several minutes.

- Modifying serial interface configuration

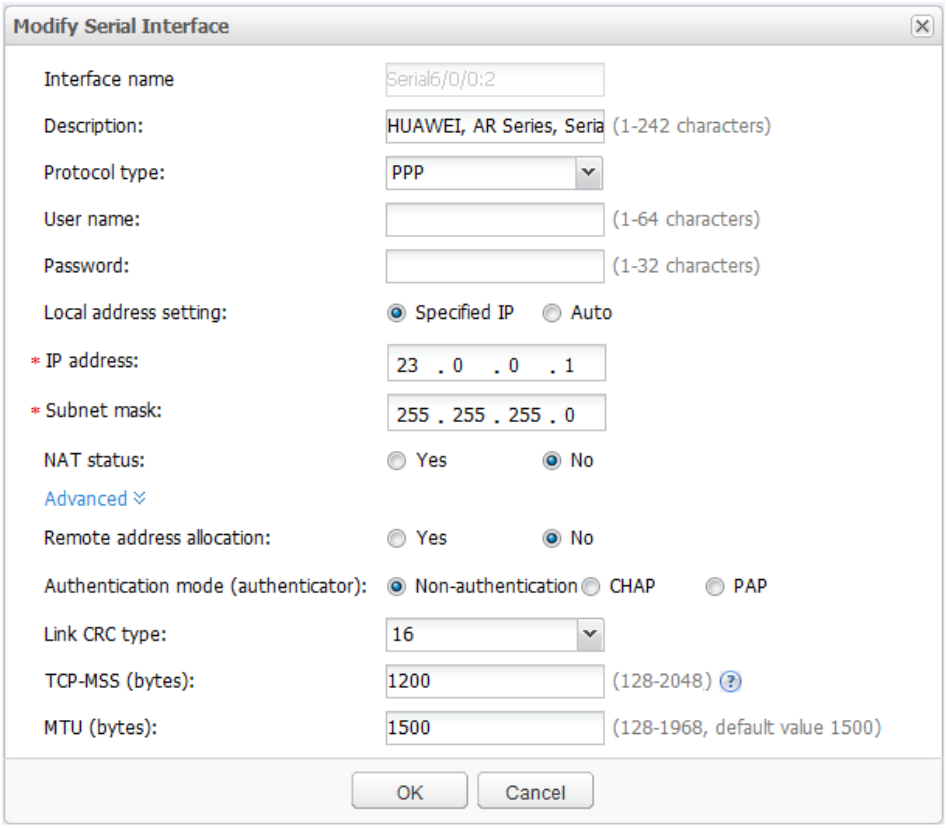
  a. Choose **WAN access** > **CE1/CT1 Interface**. Click **CE1 Interface** or **CT1 Interface** to display the **CE1 Interface** or **CT1 Interface** tab page.

  b. Click corresponding to the serial interface to be configured in the **Operation** column of **Serial Interface List** to display the modification page.

  c. Set the parameters described in **Table 2-72**.

  d. Click **OK** to complete the configuration.

  – **Figure 2-88** Modify Serial Interface (Protocol type is PPP)



 Copyright © Huawei Technologies Co., Ltd.

– **Figure 2-89** Modify Serial Interface (Protocol type is HDLC)

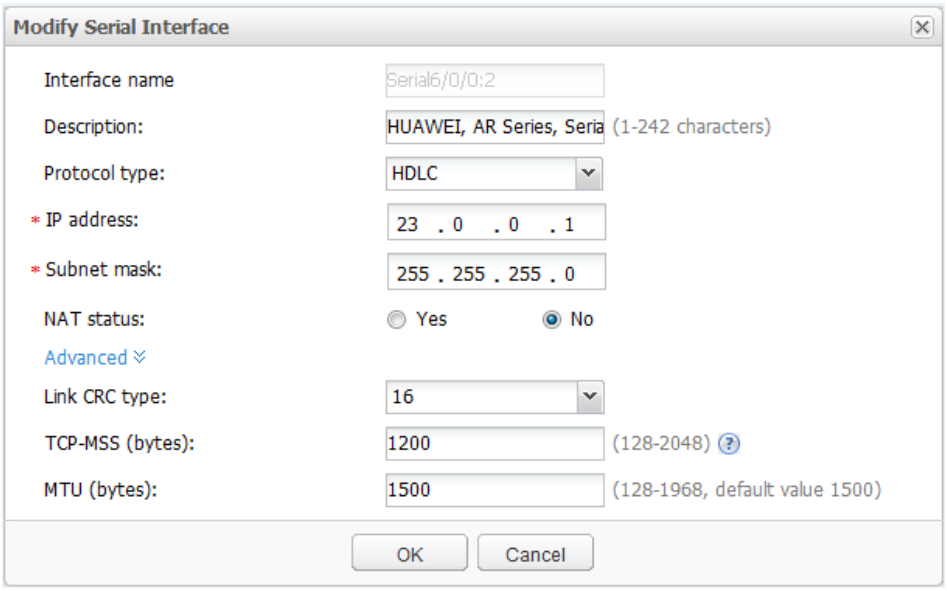


Table 2-72 Description of the serial interface parameters

Parameter	Description
Interface name	Type and number of an interface. • This parameter cannot be modified when the serial interface configuration is modified.
Description	Description of an interface. By default, the interface description is "HUAWEI, AR Series, interface-type interface-number Interface."
Protocol type	Link layer protocol of a serial interface. • PPP: indicates that the link layer protocol of a serial interface is PPP, as shown in **Figure 2-88**. For the description of PPP protocol parameters, see **Table 2-73**. • HDLC: indicates that the link layer protocol of an SA interface is HDLC, as shown in **Figure 2-89**. For the description of PPP protocol parameters, see **Table 2-74**.

Copyright © Huawei Technologies Co., Ltd.

Table 2-73 Description of the PPP protocol parameters

Parameter	Description
Username	User name of the device that functions as the authenticated party.
Password	Password of the device that functions as the authenticated party.
Local address setting	Mode in which an interface obtains an IP address. • Specified IP: indicates that an IP address is manually configured on the interface. • Auto: indicates that an IP address is obtained through PPP negotiation.
IP address	IP address of an interface. The interface IP address cannot conflict with the IP addresses of other interfaces on the device or other devices in the network.
Subnet mask	Subnet mask of an interface.
NAT status	NAT must be enabled when a PC on the private network of a LAN connects to the Internet.
Remote address allocation	Whether the local device assigns an IP address for the peer device. **NOTE** This parameter is valid only when **Local address setting** is set to **Specified IP**.
Remote address	The IP address assigned by the local device for the remote device. **NOTE** This parameter is valid only when **Remote address allocation** is set to **Yes**.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Authentication Mode (Authenticator)	Authentication mode of the device that functions as the authenticated party. PPP authentication can be performed on the device. • Non-authentication: indicates that PPP authentication is not performed on the device. • PAP: indicates that the PPP authentication mode is PAP. • CHAP: indicates that the PPP authentication mode is CHAP.
CRC format	CRC mode of an interface. • 16: indicates that the 16-bit CRC is used for an interface. • 32: indicates that the 32-bit CRC is used for an interface. • none: indicates that CRC is not performed for an interface. The interfaces on both ends of a link must use the CRC of the same length. If lengths of the CRCs used on two ends are different, the two devices cannot communicate with each other.
TCP-MSS (bytes)	MSS of TCP packets on an interface. The MSS refers to the maximum length of a TCP packet segment sent from the peer device to the local device. During TCP connection negotiation, devices at both ends record the MSS of each other. When sending TCP packets, the devices limit the size of TCP packets within the MSS. The recommended value of **TCP-MSS** is 1200.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
MTU (bytes)	MTU of an interface. If the MTU is set too small and the size of packets is large, packets will be broken into a great number of fragments and be discarded by QoS queues. If the MTU is too large, packets are transmitted slowly or even lost. After modifying the interface MTU, you must restart the interface to make the MTU setting take effect. The default value of **MTU** is 1500.

Table 2-74 Description of the HDLC protocol parameters

Parameter	Description
IP address	IP address of an interface. The interface IP address cannot conflict with the IP addresses of other interfaces on the device or other devices in the network.
Subnet mask	Subnet mask of an interface.
NAT status	NAT must be enabled when a PC on the private network of a LAN connects to the Internet.
CRC format	CRC mode of an interface. ● 16: indicates that the 16-bit CRC is used for an interface. ● 32: indicates that the 32-bit CRC is used for an interface. ● none: indicates that CRC is not performed for an interface. The interfaces on both ends of a link must use the CRC of the same length. If lengths of the CRCs used on two ends are different, the two devices cannot communicate with each other.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
TCP-MSS (bytes)	MSS of TCP packets on an interface. The MSS refers to the maximum length of a TCP packet segment sent from the peer device to the local device. During TCP connection negotiation, devices at both ends record the MSS of each other. When sending TCP packets, the devices limit the size of TCP packets within the MSS. The recommended value of **TCP-MSS** is 1200.
MTU (bytes)	MTU of an interface. If the MTU is set too small and the size of packets is large, packets will be broken into a great number of fragments and be discarded by QoS queues. If the MTU is too large, packets are transmitted slowly or even lost. After modifying the interface MTU, you must restart the interface to make the MTU setting take effect. The default value of **MTU** is 1500.

- Deleting a serial interface
  a. Choose **WAN access** > **CE1/CT1 Interface**. Click **CE1 Interface** or **CT1 Interface** to display the **CE1 Interface** or **CT1 Interface** tab page.
  b. Select the check box of the interface to be deleted and click **Delete** in the **Interface Name** column of **Serial Interface List**.
  c. Click **OK**.
- Disabling a serial interface
  a. Choose **WAN access** > **CE1/CT1 Interface**. Click **CE1 Interface** or **CT1 Interface** to display the **CE1 Interface** or **CT1 Interface** tab page.
  b. Click corresponding to the serial interface to be configured in the **Operation** column of **Serial Interface List**.
  c. Click **OK**.
- Enabling a serial interface
  a. Choose **WAN access** > **CE1/CT1 Interface**. Click **CE1 Interface** or **CT1 Interface** to display the **CE1 Interface** or **CT1 Interface** tab page.
  b. Click corresponding to the serial interface to be configured in the **Operation** column of **Serial Interface List**.
  c. Click **OK**.

----End

Copyright © Huawei Technologies Co., Ltd.

2.12.6 E1/T1 Interface

Context

NOTE

- The 1E1/T1-F, 2E1/T1-F, 4E1/T1-F, and 8E1/T1-F interface cards support E1-F interfaces. For the mapping between the device and interface card, see *1/2/4/8-Fractional Channelized E1/T1 WAN Interface Card* in the *Huawei AR Series Access Routers Get to Know the Product-Hardware Description-Cards-WAN Interface Card*.

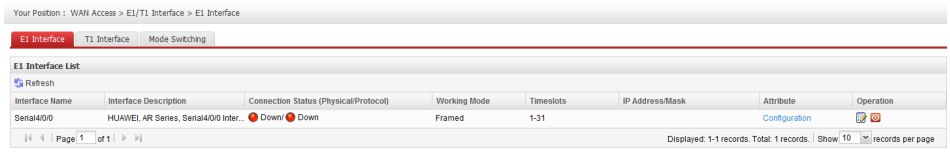
  The AR2202-48FE supports E1-F interfaces.
- The 1E1/T1-F and 2E1/T1-F interface cards support T1-F interfaces. For the mapping between the device and interface card, see *1/2/4/8-Fractional Channelized E1/T1 WAN Interface Card* in the *Huawei AR Series Access Routers Get to Know the Product-Hardware Description-Cards-WAN Interface Card*.

If E1/T1 access does not require multiple channel sets or ISDN PRI, using a CE1/CT1 interface is a waste of resources. In this scenario, you can use an E1/T1 interface to provide the E1/T1 access service. Compared with a CE1/CT1 interface, an E1/T1 interface provides E1/T1 access at a low cost.

Procedure

- Modifying E1/T1 interface configuration
  a. Choose **WAN access** > **E1/T1 Interface** and click **E1 Interface** or **T1 Interface** to display the **E1 Interface** or **T1 Interface** tab page. **Figure 2-90** shows **CE1 Interface** page and **CT1 Interface** page.

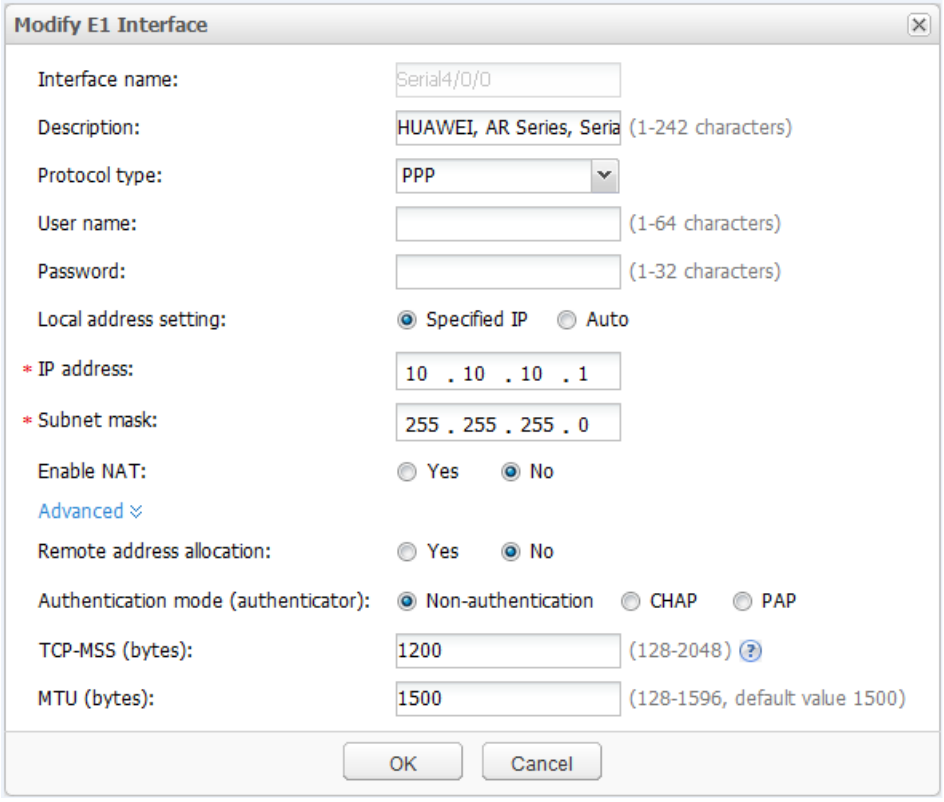
     Figure 2-90 E1 Interface Page

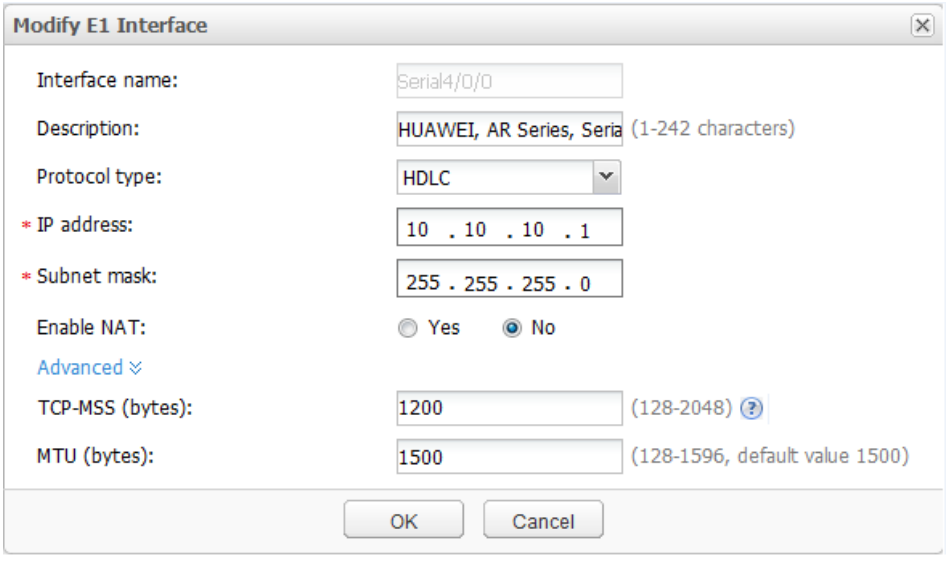
  b. Click  corresponding to the E1 or T1 interface to be configured in the **Operation** column of **E1 Interface List** or **T1 Interface List** to display the modification page.
  c. Set the parameters described in **Table 2-75**.
  d. Click **OK** to complete the configuration.

 Copyright © Huawei Technologies Co., Ltd.

– **Figure 2-91** Modify E1 Interface (Protocol type is PPP)



– **Figure 2-92** Modify E1 Interface (Protocol type is HDLC)



NOTE

The parameters for modifying a T1 interface are the same as those for modifying an E1 interface. You can set the parameters for modifying a T1 interface according to the page for modifying an E1 interface.

 Copyright © Huawei Technologies Co., Ltd.

Table 2-75 Description of the E1/T1 interface parameters

Parameter	Description
Interface name	Type and number of an interface. • This parameter cannot be modified when the E1/T1 interface configuration is modified.
Description	Description of an interface. By default, the description of an interface is empty.
Protocol type	Link layer protocol of an E1/T1 interface. • PPP: indicates that the link layer protocol of a serial interface is PPP, as shown in **Figure 2-91**. For the description of PPP protocol parameters, see **Table 2-76**. • HDLC: indicates that the link layer protocol of an SA interface is HDLC, as shown in **Figure 2-92**. For the description of PPP protocol parameters, see **Table 2-77**.

Table 2-76 Description of the PPP protocol parameters

Parameter	Description
User name	User name of the device that functions as the authenticated party.
Password	Password of the device that functions as the authenticated party.
Local address setting	Mode in which an interface obtains an IP address. • Specified IP: indicates that an IP address is manually configured on the interface. • Auto: indicates that an IP address is obtained through PPP negotiation.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
IP address	IP address of an interface. The interface IP address cannot conflict with the IP addresses of other interfaces on the device or other devices in the network.
Subnet mask	Subnet mask of an interface.
Enable NAT	NAT must be enabled when a PC on the private network of a LAN connects to the Internet.
Remote address allocation	Whether the local device assigns an IP address for the peer device. **NOTE** This parameter is valid only when **Local address setting** is set to **Specified IP**.
Remote address	The IP address assigned by the local device for the remote device. **NOTE** This parameter is valid only when **Remote address allocation** is set to **Yes**.
Authentication mode (authenticator)	Authentication mode of the device that functions as the authenticated party. PPP authentication can be performed on the device. • Non-authentication: indicates that PPP authentication is not performed on the device. • PAP: indicates that the PPP authentication mode is PAP. • CHAP: indicates that the PPP authentication mode is CHAP.
TCP-MSS (bytes)	MSS of TCP packets on an interface. The MSS refers to the maximum length of a TCP packet segment sent from the peer device to the local device. During TCP connection negotiation, devices at both ends record the MSS of each other. When sending TCP packets, the devices limit the size of TCP packets within the MSS. The recommended value of **TCP-MSS** is 1200.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
MTU (bytes)	MTU of an interface. If the MTU is set too small and the size of packets is large, packets will be broken into a great number of fragments and be discarded by QoS queues. If the MTU is too large, packets are transmitted slowly or even lost. After modifying the interface MTU, you must restart the interface to make the MTU setting take effect. The default value of **MTU** is 1500.

Table 2-77 Description of the HDLC protocol parameters

Parameter	Description
IP address	IP address of an interface. The interface IP address cannot conflict with the IP addresses of other interfaces on the device or other devices in the network.
Subnet mask	Subnet mask of an interface.
Enable NAT	NAT must be enabled when a PC on the private network of a LAN connects to the Internet.
TCP-MSS (bytes)	MSS of TCP packets on an interface. The MSS refers to the maximum length of a TCP packet segment sent from the peer device to the local device. During TCP connection negotiation, devices at both ends record the MSS of each other. When sending TCP packets, the devices limit the size of TCP packets within the MSS. The recommended value of **TCP-MSS** is 1200.

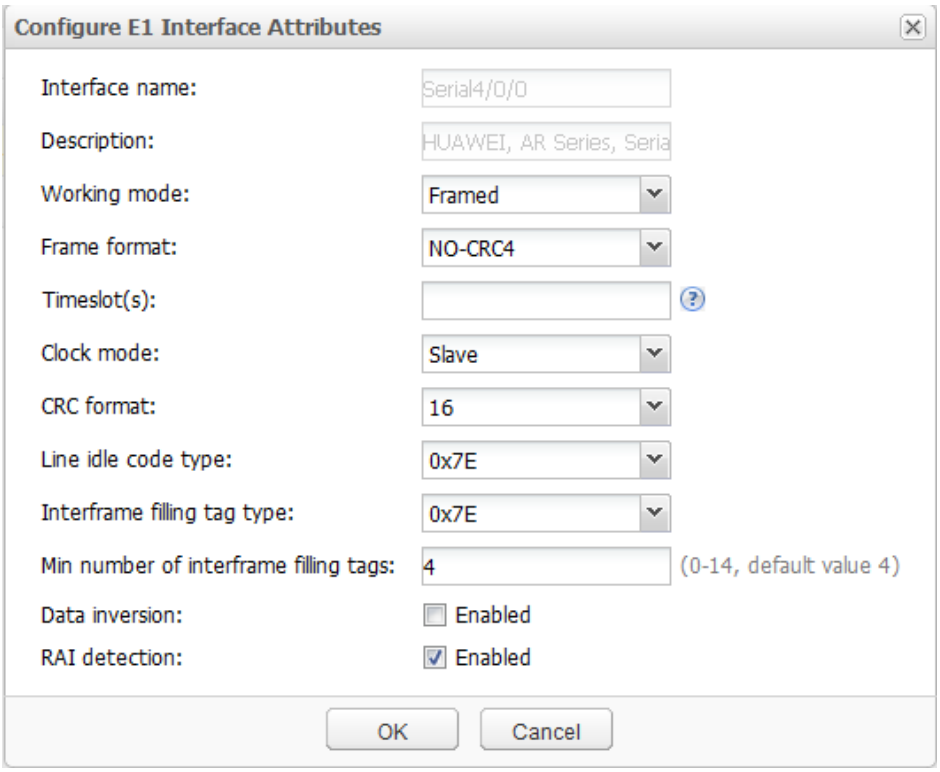
Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
MTU (bytes)	MTU of an interface. If the MTU is set too small and the size of packets is large, packets will be broken into a great number of fragments and be discarded by QoS queues. If the MTU is too large, packets are transmitted slowly or even lost. After modifying the interface MTU, you must restart the interface to make the MTU setting take effect. The default value of **MTU** is 1500.

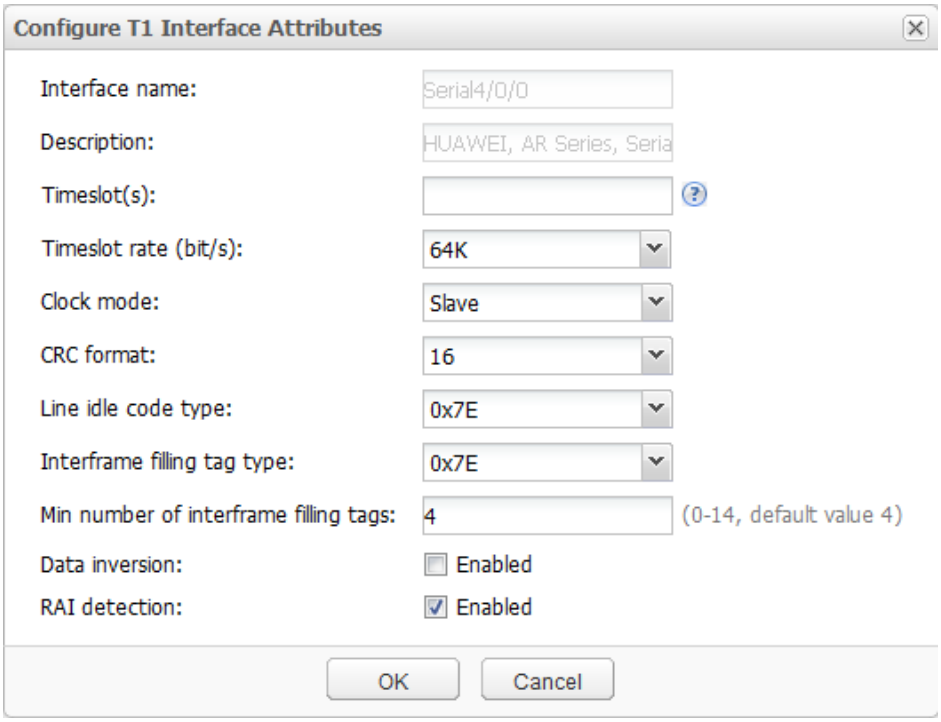
- Configuring the physical attributes and link layer attributes of an E1/T1 interface
  a. Choose **WAN access** > **E1/T1 Interface** and click **E1 Interface** or **T1 Interface** to display the **E1 Interface** or **T1 Interface** tab page.
  b. Click **Configure Interface Attribution** in the **Interface Attribution** column of **E1 Interface List** or **T1 Interface List** to display the interface attribute configuration page.
  c. Set the parameters.
     - For the physical attributes and link layer attributes of an E1 interface, see **Table 2-78**.
     - For the physical attributes and link layer attributes of a T1 interface, see **Table 2-79**.
  d. Click **OK** to complete the configuration.

Copyright © Huawei Technologies Co., Ltd.

– **Figure 2-93** Configure E1 Interface Attributes



– **Figure 2-94** Configure T1 Interface Attributes



 Copyright © Huawei Technologies Co., Ltd.

Table 2-78 Description of the E1 interface's physical attributes and link layer attributes

Parameter	Description
Interface name	Type and number of an interface.
Description	Description of an interface. By default, the interface description is "HUAWEI, AR Series, interface-type interface-number Interface."
Working mode	Working mode of an E1 interface. ● Framed: indicates that an E1 interface works in framed mode. ● Unframed: indicates that an E1 interface works in unframed mode.
Frame format	Frame format of an E1 interface. ● CRC4: indicates the CRC4 frame format. ● NO-CRC4: indicates the non-CRC4 frame format (basic frame format). Two devices can communicate properly only when the same frame format is set for the interfaces on both devices. Otherwise, a CRC4 alarm is generated.
Timeslots	E1 interface timeslots that are bound. By default, all timeslots (except timeslot 0) of an E1 interface are bound. **NOTE** This attribute is valid only when **Working mode** is set to **Framed**.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Clock mode	Clock mode of an E1 interface. • Master: indicates the master clock mode (internal clock mode). • Slave: indicates the slave clock mode (line clock mode). • System: indicates the system clock mode. When two routers are directly connected using two E1 interfaces, one E1 interface must work in master clock mode and the other must work in slave clock mode. When the MPU on the router obtains the clock with high accuracy from the upstream device and the router needs to synchronize the clock to downstream device, the interface on the router must be configured to work in system clock mode. Moreover, the interface on the downstream device must be configured to work in slave clock mode.
CRC format	CRC mode of an E1 interface. • 16: indicates that the 16-bit CRC is used for an E1 interface. • 32: indicates that the 32-bit CRC is used for an E1 interface. • none: indicates that CRC is not performed for an E1 interface. The interfaces on both ends of a link must use the CRC of the same length. If lengths of the CRCs used on two ends are different, the two devices cannot communicate with each other.
Line idle code type	Line idle code type of an E1 interface. • 0x7E • 0xFF Two devices can communicate properly only when the same line idle code is set for the interfaces on both devices.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Interframe filling tag type	Interframe filling tag type of an E1 interface. • 0x7E • 0xFF Interfaces on both ends can communicate only when the same interframe filling tag and the same minimum number of interframe filling tags are set for them.
Min number of interframe filling tags	Minimum number of interframe filling tags of an E1 interface. Interfaces on both ends can communicate only when the same interframe filling tag and the same minimum number of interframe filling tags are set for them.
Data inversion	Whether data inversion is configured for an E1 interface. E1 interfaces on both ends can communicate only when they have the same data inversion configuration.
RAI detection	Whether Remote Alarm Indication (RAI) detection is enabled for an E1 interface. **NOTE** This attribute is valid only when **Working mode** is set to **Framed**.
AIS detection	Whether Alarm Indication Signal (AIS) detection is enabled for an E1 interface. **NOTE** This attribute is valid only when **Working mode** is set to **Unframed**. If the E1 interface works in unframed mode, AIS detection must be disabled.

Table 2-79 Description of the T1 interface's physical attributes and link layer attributes

Parameter	Description
Interface name	Type and number of an interface.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Description	Description of an interface. By default, the interface description is "HUAWEI, AR Series, interface-type interface-number Interface."
Timeslots	T1 interface timeslots that are bound. By default, all timeslots (except timeslot 0) of a T1 interface are bound.
Timeslot rate (bit/s)	Timeslot rate of a T1 interface. ● 64K: indicates that the timeslot rate of a T1 interface is 64 kbit/s. ● 56K: indicates that the timeslot rate of a T1 interface is 56 kbit/s.
Clock mode	Clock mode of a T1 interface. ● Master: indicates the master clock mode (internal clock mode). ● Slave: indicates the slave clock mode (line clock mode). ● System: indicates the system clock mode. When two routers are directly connected using two T1 interfaces, one T1 interface must work in master clock mode and the other must work in slave clock mode. When the MPU on the router obtains the clock with high accuracy from the upstream device and the router needs to synchronize the clock to downstream device, the interface on the router must be configured to work in system clock mode. Moreover, the interface on the downstream device must be configured to work in slave clock mode.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
CRC format	CRC mode of a T1 interface. ● 16: indicates that the 16-bit CRC is used for a T1 interface. ● 32: indicates that the 32-bit CRC is used for a T1 interface. ● none: indicates that CRC is not performed for a T1 interface. The interfaces on both ends of a link must use the CRC of the same length. If lengths of the CRCs used on two ends are different, the two devices cannot communicate with each other.
Line idle code type	Line idle code type of a T1 interface. ● 0x7E ● 0xFF Two devices can communicate properly only when the same line idle code is set for the interfaces on both devices.
Interframe filling tag type	Interframe filling tag type of a T1 interface. ● 0x7E ● 0xFF Interfaces on both ends can communicate only when the same interframe filling tag and the same minimum number of interframe filling tags are set for them.
Min number of interframe filling tags	Minimum number of interframe filling tags of a T1 interface. Interfaces on both ends can communicate only when the same interframe filling tag and the same minimum number of interframe filling tags are set for them.
Data inversion	Whether data inversion is configured for a T1 interface. T1 interfaces on both ends can communicate only when they have the same data inversion configuration.
RAI detection	Whether RAI detection is enabled for a T1 interface.

Copyright © Huawei Technologies Co., Ltd.

- Disabling an E1/T1 interface
  a. Choose **WAN access** > **E1/T1 Interface** and click **E1 Interface** or **T1 Interface** to display the **E1 Interface** or **T1 Interface** tab page.
  b. Click corresponding to the E1 or T1 interface to be configured in the **Operation** column of **E1 Interface List** or **T1 Interface List**.
  c. Click **OK**.
- Enabling an E1/T1 interface
  a. Choose **WAN access** > **E1/T1 Interface** and click **E1 Interface** or **T1 Interface** to display the **E1 Interface** or **T1 Interface** tab page.
  b. Click corresponding to the E1 or T1 interface to be configured in the **Operation** column of **E1 Interface List** or **T1 Interface List**.
  c. Click **OK**.
- Switching the mode of an E1/T1 interface

  NOTE

  The 4E1T1-F/8E1T1-F interface card only works in E1-F mode and does not support working mode switching.

  a. Choose **WAN access** > **E1/T1 Interface** > **Mode Switching** to display the **Mode Switching** tab page.
  b. Click corresponding to the E1 or T1 interface whose mode needs to be switched in the **Operation** column of **E1 Card List** or **T1 Card List**.
  c. Click **OK**.

     The configuration takes effect after several minutes.

----End

2.12.7 PON Interface

Context

NOTE

The 1PON interface card supports PON interfaces. For the mapping between the device and interface card, see *1PON (1-Port GPON/EPON Dual-Mode Interface Card)* in the *Huawei AR Series Access Routers Get to Know the Product-Hardware Description-Cards-xDSL/xPON Interface Card*.

A PON network consists of only passive optical components. This technology has the following advantages:

- Prevents electromagnetic interference and lightning damages generated by active electronic components.
- Reduces failure rate of lines and devices.
- Simplifies power supply configuration and network topology.
- Improves system reliability.
- Saves maintenance costs.

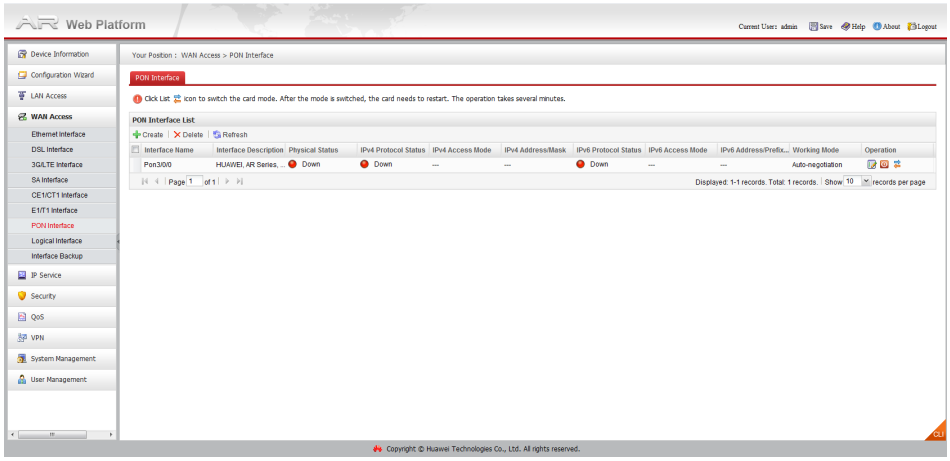
Theoretically, a PON network can transmit signals of any format at any rate.

Copyright © Huawei Technologies Co., Ltd.

Procedure

- Creating a PON sub-interface
  a. Choose **WAN Access** > **PON Interface** to display the **PON Interface** page. **Figure 2-95** shows **PON Interface** page.

     Figure 2-95 PON Interface Page

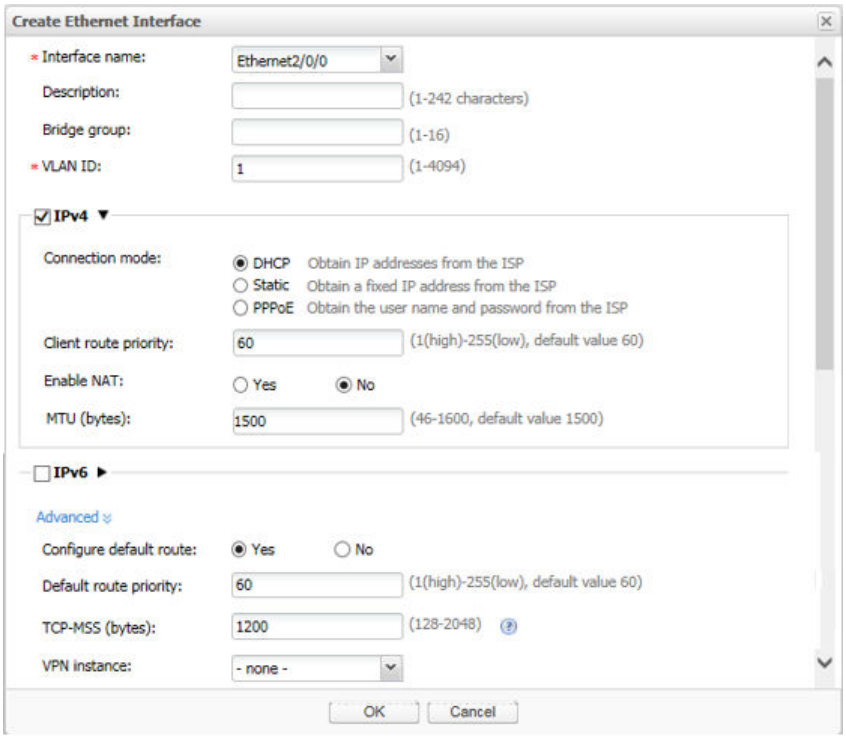
  b. Click **Create** to display the page for creating a PON interface.
  c. Set the parameters described in **Table 2-80**.
  d. Click **OK** to complete the configuration.

  NOTE

  The parameters for creating a PON interface are the same as those for creating an Ethernet interface. After select an PON interface from the **Interface name** drop-down list box, you can set the parameters according to the page (shown in the following figures) for creating a PON interface.

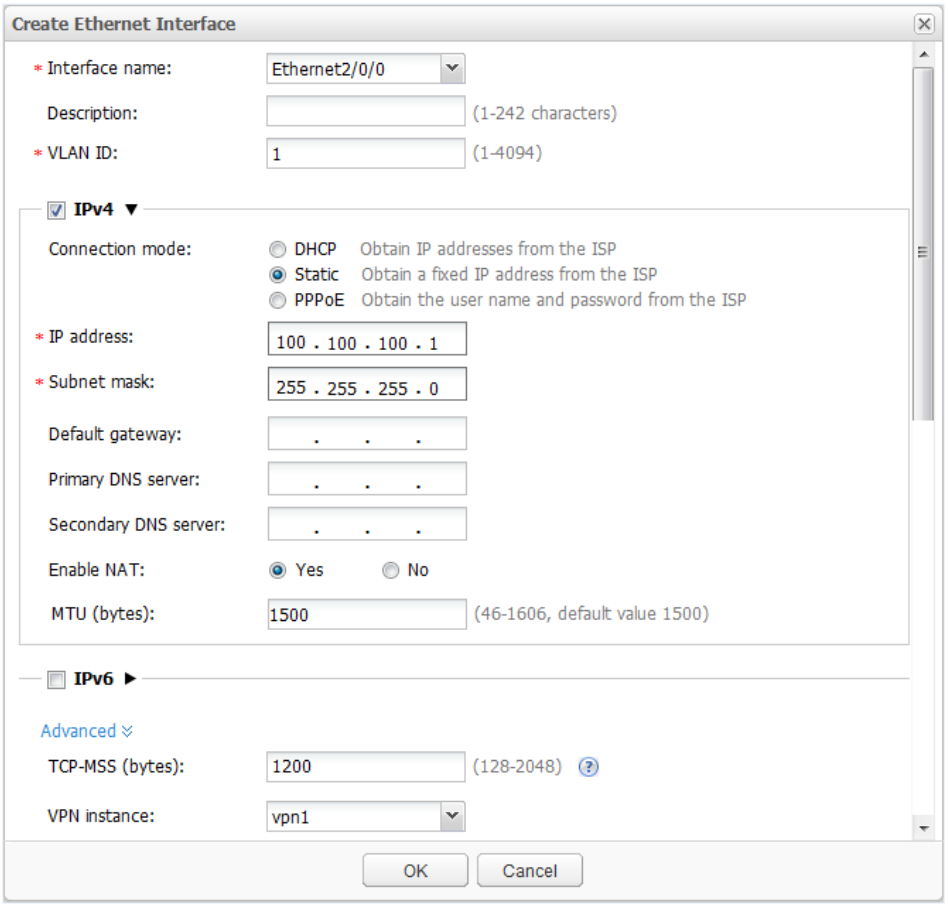
 Copyright © Huawei Technologies Co., Ltd.

– **Figure 2-96** Create Ethernet interface (Connection mode is IPv4 DHCP)



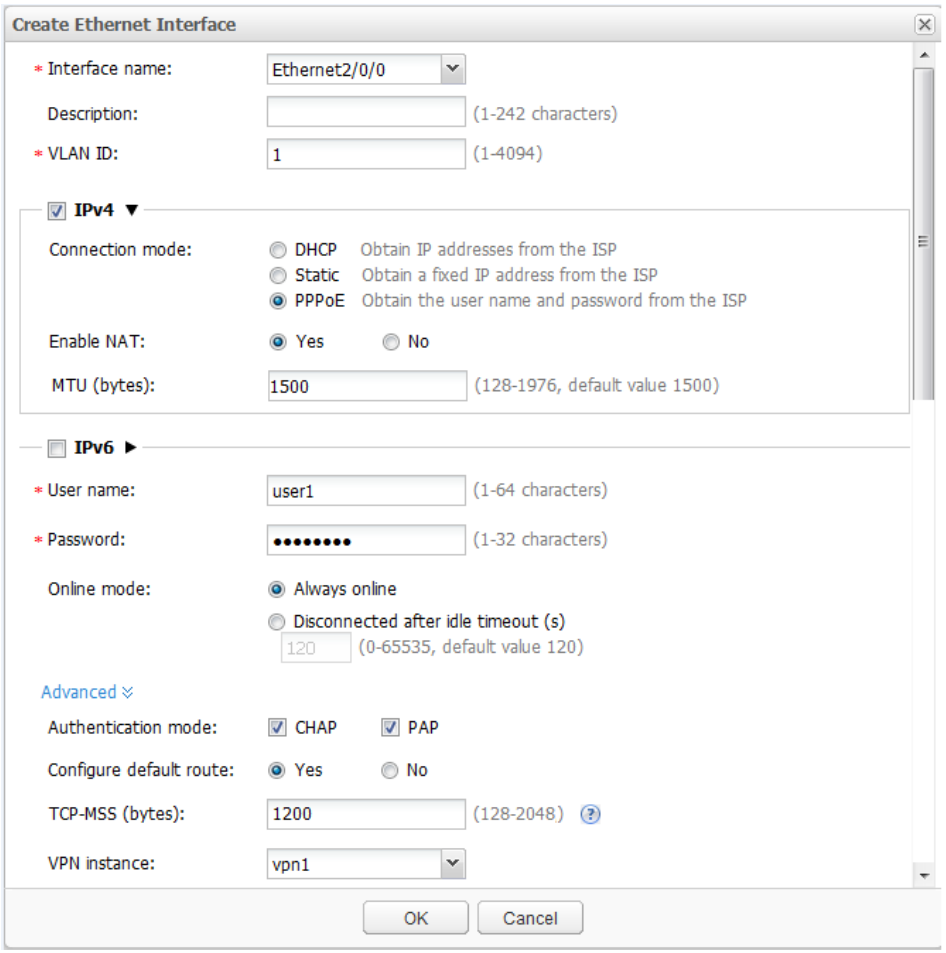
 Copyright © Huawei Technologies Co., Ltd.

– **Figure 2-97** Create Ethernet interface (Connection mode is IPv4 Static)



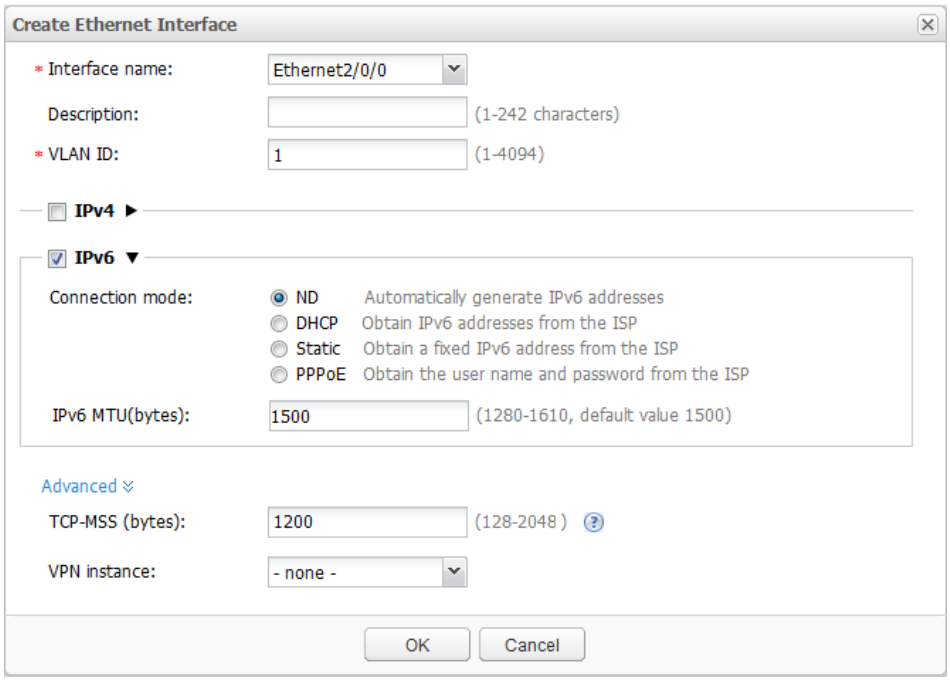
 Copyright © Huawei Technologies Co., Ltd.

– **Figure 2-98** Create Ethernet interface (Connection mode is IPv4 PPPoE)

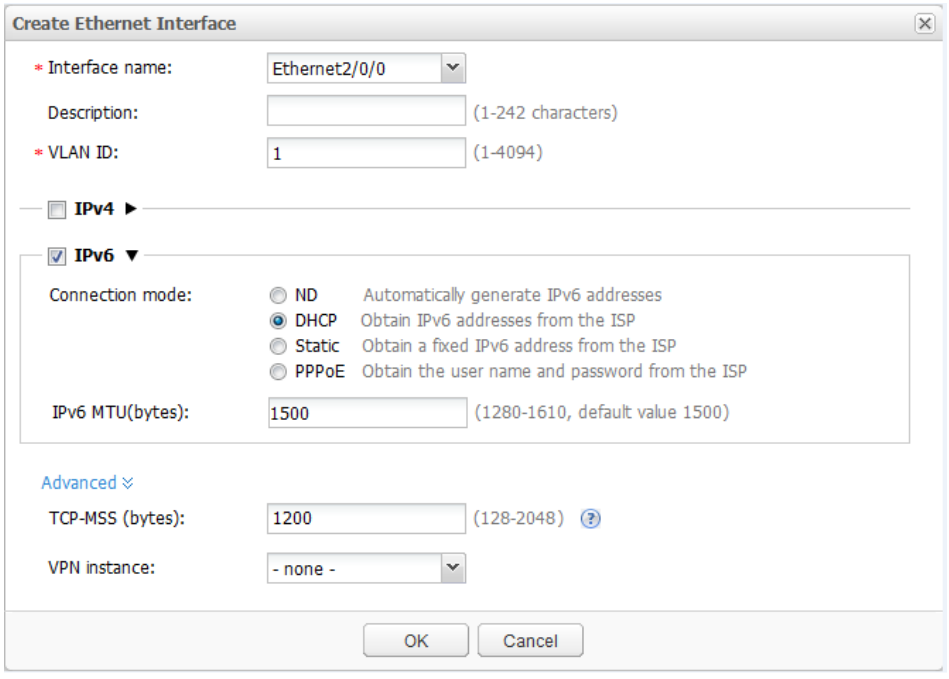


 Copyright © Huawei Technologies Co., Ltd.

– **Figure 2-99** Create Ethernet interface (Connection mode is IPv6 ND)

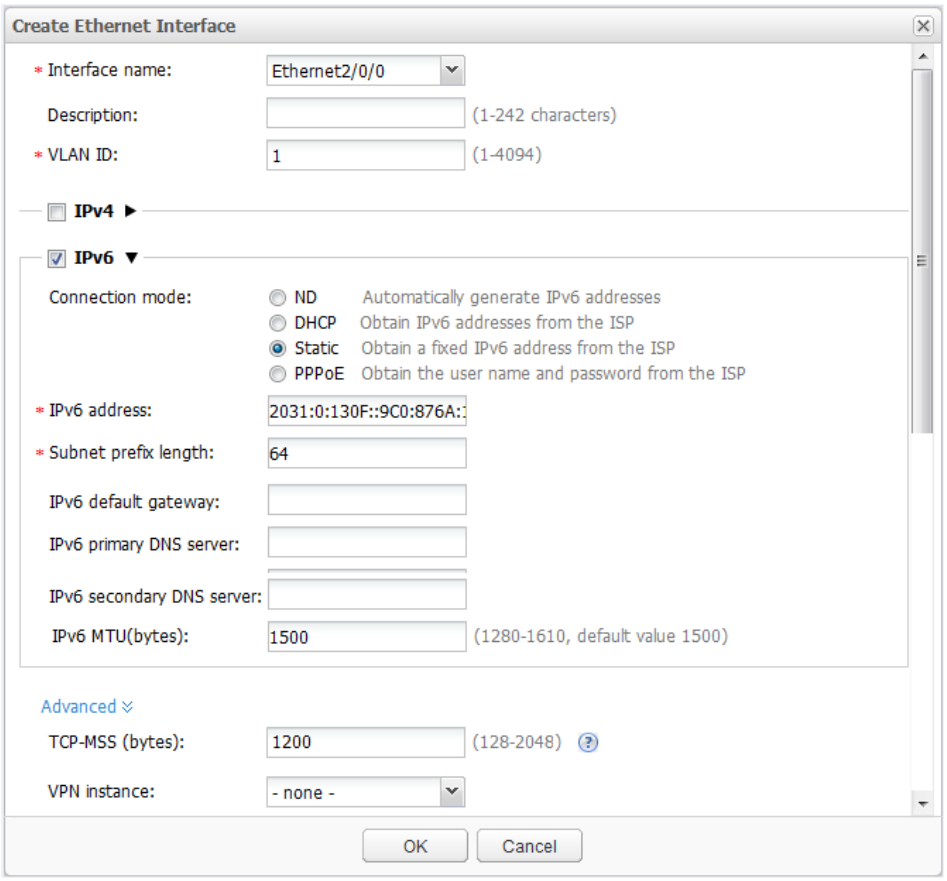


– **Figure 2-100** Create Ethernet interface (Connection mode is IPv6 DHCP)



 Copyright © Huawei Technologies Co., Ltd.

– **Figure 2-101** Create Ethernet interface (Connection mode is IPv6 Static)



 Copyright © Huawei Technologies Co., Ltd.

– **Figure 2-102** Create Ethernet interface (Connection mode is IPv6 PPPoE)

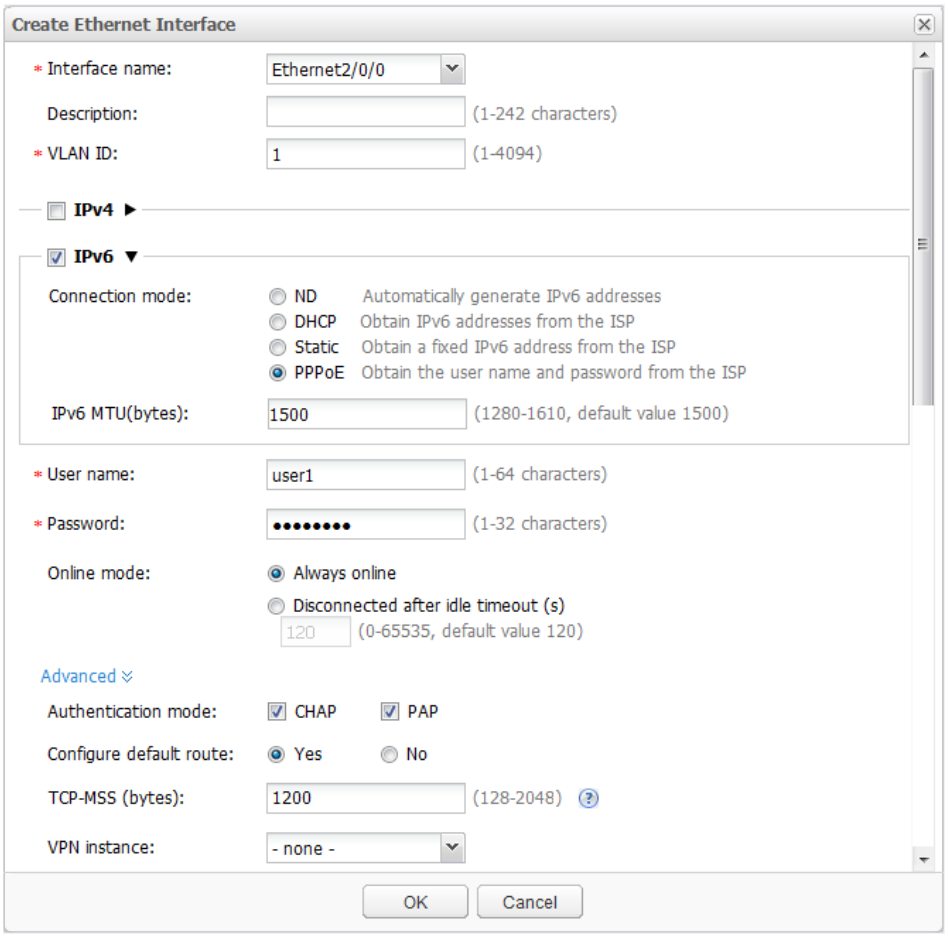


Table 2-80 Description of the PON interface parameters

Parameter	Description
Interface name	Type and number of an interface. • This parameter cannot be modified when the PON interface configuration is modified. • When you set the parameters for creating a PON sub-interface, select the PON interface for which the sub-interface needs to be created.
Description	Description of an interface. By default, the description of an interface is empty.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
VLAN ID	The VLAN ID must be entered when a user VLAN is terminated through a sub-interface. You can set this parameter only when creating a PON sub-interface.
IPv4	IPv4 configuration parameters. The **Connection mode** parameter specifies the mode in which an interface obtains an IPv4 address. The options for **Connection mode** are as follows: • DHCP: indicates that the interface IPv4 address is automatically obtained using DHCP. For the description of DHCP parameters, see **Table 2-81**. • Static: indicates that the interface IPv4 address is manually configured. For the description of Static parameters, see **Table 2-82**. • PPPoE: indicates that the interface IPv4 address is obtained through PPP negotiation. For the description of PPPoE parameters, see **Table 2-83**. **NOTE** You must select either IPv4 or IPv6 configuration.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
IPv6	IPv6 configuration parameters. The **Connection mode** parameter specifies the mode in which an interface obtains an IPv6 address. The options for **Connection mode** are as follows: • ND: indicates that the interface IPv6 address is automatically configured. For the description of ND parameters, see **Table 2-84**. • DHCP: indicates that the interface IPv4 address is automatically obtained using DHCP. For the description of DHCP parameters, see **Table 2-85**. • Static: indicates that the interface IPv4 address is manually configured. For the description of Static parameters, see **Table 2-86**. • PPPoE: indicates that the interface IPv4 address is obtained through PPP negotiation. For the description of PPPoE parameters, see **Table 2-87**. **NOTE** You must select either IPv4 or IPv6 configuration.

Table 2-81 Description of the DHCP parameters (IPv4)

Parameter	Description
NAT status	NAT must be enabled when a PC on the private network of a LAN connects to the Internet.
MTU (bytes)	MTU of an interface. If the MTU is set too small and the size of packets is large, packets will be broken into a great number of fragments and be discarded by QoS queues. If the MTU is too large, packets are transmitted slowly or even lost. The default value of **MTU** is 1500.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
TCP-MSS (bytes)	MSS of TCP packets on an interface. The MSS refers to the maximum length of a TCP packet segment sent from the peer device to the local device. During TCP connection negotiation, devices at both ends record the MSS of each other. When sending TCP packets, the devices limit the size of TCP packets within the MSS. The recommended value of **TCP-MSS** is 1200.
VPN instance	VPN instance bound to an interface. **NOTE** Before setting this parameter, you must create an IPv4 VPN instance. For the detailed procedure, see **2.17.4 VPN Instance**.

Table 2-82 Description of the Static parameters (IPv4)

Parameter	Description
IP address	IP address of an interface. The interface IP address cannot conflict with the IP addresses of other interfaces on the device or other devices in the network.
Subnet mask	Subnet mask of an interface.
Default gateway	Default gateway address of an interface. The default gateway address must be in the same network segment as the interface IP address.
Primary DNS server	Primary DNS server address assigned to a DHCP client.
Secondary DNS server	Secondary DNS server address assigned to a DHCP client.
NAT status	NAT must be enabled when a PC on the private network of a LAN connects to the Internet.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
MTU (bytes)	MTU of an interface. If the MTU is set too small and the size of packets is large, packets will be broken into a great number of fragments and be discarded by QoS queues. If the MTU is too large, packets are transmitted slowly or even lost. The default value of **MTU** is 1500.
TCP-MSS (bytes)	MSS of TCP packets on an interface. The MSS refers to the maximum length of a TCP packet segment sent from the peer device to the local device. During TCP connection negotiation, devices at both ends record the MSS of each other. When sending TCP packets, the devices limit the size of TCP packets within the MSS. The recommended value of **TCP-MSS** is 1200.
VPN instance	VPN instance bound to an interface. **NOTE** Before setting this parameter, you must create an IPv4 VPN instance. For the detailed procedure, see **2.17.4 VPN Instance**.

Table 2-83 Description of the PPPoE parameters (IPv4)

Parameter	Description
NAT status	NAT must be enabled when a PC on the private network of a LAN connects to the Internet.
MTU (bytes)	MTU of an interface. If the MTU is set too small and the size of packets is large, packets will be broken into a great number of fragments and be discarded by QoS queues. If the MTU is too large, packets are transmitted slowly or even lost. The default value of **MTU** is 1500.
User name	User name for PPPoE dial-up.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Password	Password for PPPoE dial-up.
Online mode	PPPoE dial-up mode. ● Always online: The DCC attempts to dial the remote end immediately after the device starts. The dialing process is not triggered by data packets. If a connection cannot be established with the remote end, the DCC retries at an interval. This mode applies to the scenarios in which users are not charged based on traffic or time. ● Disconnected after idle timeout (s): The device triggers the process of establishing a link only when there is data to be transmitted. When the time during which no traffic is transmitted on the link exceeds the timeout duration, the device disconnects the link to save traffic. This mode applies to the scenarios in which users are charged based on traffic or time. If this mode is used, the link idle time must be specified. The default link idle time is 120.
Authentication mode	Authentication mode for PPPoE dial-up. ● PAP: Passwords are sent over links in plain text. After a PPP link is established, the authenticated device repeatedly sends the user name and password until the authentication finishes. This mode cannot ensure high security. ● CHAP: a three-way handshake authentication protocol. In CHAP authentication, the authenticated device sends only the user name to the authenticating device. Compared with PAP, CHAP features higher security because passwords are not transmitted.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Configure default route	Configure a default route from the local hosts to the PPPoE server.
TCP-MSS (bytes)	MSS of TCP packets on an interface. The MSS refers to the maximum length of a TCP packet segment sent from the peer device to the local device. During TCP connection negotiation, devices at both ends record the MSS of each other. When sending TCP packets, the devices limit the size of TCP packets within the MSS. The recommended value of **TCP-MSS** is 1200.
VPN instance	VPN instance bound to an interface. **NOTE** Before setting this parameter, you must create an IPv4 VPN instance. For the detailed procedure, see **2.17.4 VPN Instance**.

Table 2-84 Description of the ND parameters

Parameter	Description
IPv6 MTU (bytes)	MTU of an interface. After modifying the interface MTU, you must restart the interface to make the MTU setting take effect. The default value of **MTU** is 1500.
TCP-MSS (bytes)	MSS of TCP packets on an interface. The MSS refers to the maximum length of a TCP packet segment sent from the peer device to the local device. During TCP connection negotiation, devices at both ends record the MSS of each other. When sending TCP packets, the devices limit the size of TCP packets within the MSS. The recommended value of **TCP-MSS** is 1200.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
VPN instance	VPN instance bound to an interface. **NOTE** Before setting this parameter, you must create an IPv6 VPN instance. For the detailed procedure, see **2.17.4 VPN Instance**.

Table 2-85 Description of the DHCP parameters (IPv6)

Parameter	Description
IPv6 MTU (bytes)	MTU of an interface. The default value of **MTU** is 1500.
TCP-MSS (bytes)	MSS of TCP packets on an interface. The MSS refers to the maximum length of a TCP packet segment sent from the peer device to the local device. During TCP connection negotiation, devices at both ends record the MSS of each other. When sending TCP packets, the devices limit the size of TCP packets within the MSS. The recommended value of **TCP-MSS** is 1200.
VPN instance	VPN instance bound to an interface. **NOTE** Before setting this parameter, you must create an IPv6 VPN instance. For the detailed procedure, see **2.17.4 VPN Instance**.

Table 2-86 Description of the Static parameters (IPv6)

Parameter	Description
IPv6 address	IPv6 address of an interface.
Subnet prefix length	Length of the IPv6 address prefix.
IPv6 default gateway	Default gateway address of an interface. The default gateway address must be in the same network segment as the interface IP address.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
IPv6 primary DNS server	Primary DNS server address assigned to a DHCPv6 client.
IPv6 secondary DNS server	Secondary DNS server address assigned to a DHCPv6 client.
IPv6 MTU (bytes)	MTU of an interface. The default value of **MTU** is 1500.
TCP-MSS (bytes)	MSS of TCP packets on an interface. The MSS refers to the maximum length of a TCP packet segment sent from the peer device to the local device. During TCP connection negotiation, devices at both ends record the MSS of each other. When sending TCP packets, the devices limit the size of TCP packets within the MSS. The recommended value of **TCP-MSS** is 1200.
VPN instance	VPN instance bound to an interface. **NOTE** Before setting this parameter, you must create an IPv6 VPN instance. For the detailed procedure, see **2.17.4 VPN Instance**.

Table 2-87 Description of the PPPoE parameters (IPv6)

Parameter	Description
IPv6 MTU (bytes)	MTU of an interface. The default value of **MTU** is 1500.
User name	User name for PPPoE dial-up.
Password	Password for PPPoE dial-up.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Online mode	PPPoE dial-up mode. ● Always online: The DCC attempts to dial the remote end immediately after the device starts. The dialing process is not triggered by data packets. If a connection cannot be established with the remote end, the DCC retries at an interval. This mode applies to the scenarios in which users are not charged based on traffic or time. ● Disconnected after idle timeout (s): The device triggers the process of establishing a link only when there is data to be transmitted. When the time during which no traffic is transmitted on the link exceeds the timeout duration, the device disconnects the link to save traffic. This mode applies to the scenarios in which users are charged based on traffic or time. If this mode is used, the link idle time must be specified. The default link idle time is 120.
Authentication mode	Authentication mode for PPPoE dial-up. ● PAP: Passwords are sent over links in plain text. After a PPP link is established, the authenticated device repeatedly sends the user name and password until the authentication finishes. This mode cannot ensure high security. ● CHAP: a three-way handshake authentication protocol. In CHAP authentication, the authenticated device sends only the user name to the authenticating device. Compared with PAP, CHAP features higher security because passwords are not transmitted.

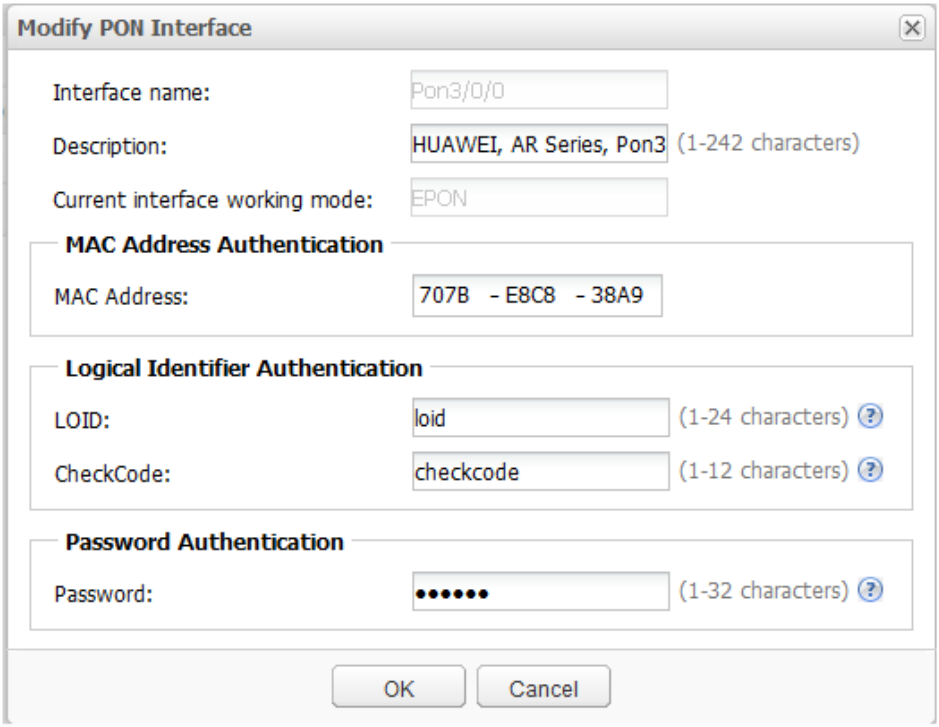
Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Configure default route	Configure a default route from the local hosts to the PPPoE server.
TCP-MSS (bytes)	MSS of TCP packets on an interface. The MSS refers to the maximum length of a TCP packet segment sent from the peer device to the local device. During TCP connection negotiation, devices at both ends record the MSS of each other. When sending TCP packets, the devices limit the size of TCP packets within the MSS. The recommended value of **TCP-MSS** is 1200.
VPN instance	VPN instance bound to an interface. **NOTE** Before setting this parameter, you must create an IPv6 VPN instance. For the detailed procedure, see **2.17.4 VPN Instance**.

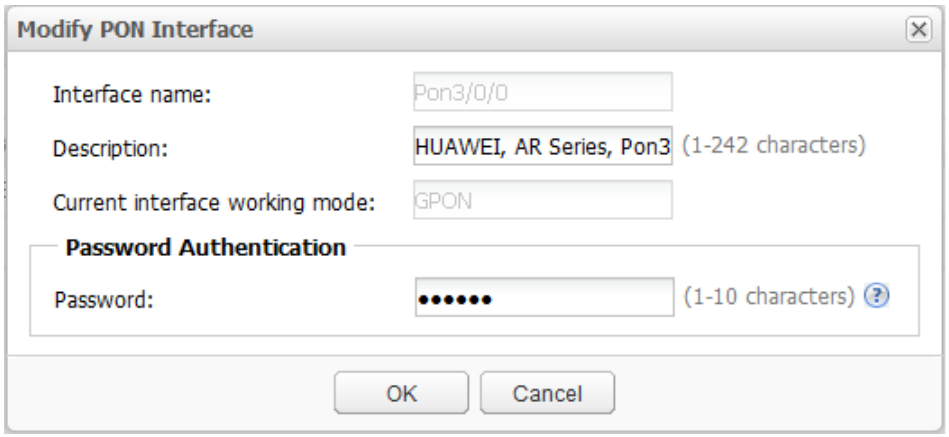
- Modifying PON interface configuration
  a. Choose **WAN Access** > **PON Interface** to display the **PON Interface** page.
  b. Click  corresponding to the PON interface to be configured in the **Operation** column of **PON Interface List** to display the modification page.
  c. Set the parameters described in **Table 2-88**.
  d. Click **OK** to complete the configuration.

Copyright © Huawei Technologies Co., Ltd.

– **Figure 2-103** Modify PON Interface (EPON Mode)



– **Figure 2-104** Modify PON Interface (GPON Mode)



 Copyright © Huawei Technologies Co., Ltd.

Table 2-88 Description of the PON interface parameters

Parameter	Description
Interface name	Type and number of an interface. • This parameter cannot be modified when the PON interface configuration is modified. • When you set the parameters for creating a PON sub-interface, select the PON interface for which the sub-interface needs to be created.
Description	Description of an interface. By default, the interface description is "HUAWEI, AR Series, interface-type interface-number Interface."
Current interface working mode	Working mode of a PON interface. • EPON: indicates that the working mode of a PON interface is EPON, as shown in **Figure 2-103**. For the description of EPON mode parameters, see **Table 2-89**. • GPON: indicates that the working mode of a PON interface is GPON, as shown in **Figure 2-104**. For the description of EPON mode parameters, see **Table 2-90**. • Adapt: indicates that a PON interface works in auto-sensing mode.

Table 2-89 Description of the EPON mode parameters

Parameter	Description
MAC Address	MAC address used when logical identifier authentication is performed on the device.
LOID	Logical identifier used when logical identifier authentication is performed on the device.
CheckCode	Verification code used when logical identifier authentication is performed on the device.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Password	Password used when password authentication is performed on the device.

Table 2-90 Description of the GPON mode parameters

Parameter	Description
Password	Password used when password authentication is performed on the device.

- Disabling a PON interface
  a. Choose **WAN Access** > **PON Interface** to display the **PON Interface** page.
  b. Click corresponding to the PON interface to be configured in the **Operation** column of **PON Interface List**.
  c. Click **OK**.
- Enabling a PON interface
  a. Choose **WAN Access** > **PON Interface** to display the **PON Interface** page.
  b. Click corresponding to the PON interface to be configured in the **Operation** column of **PON Interface List**.
  c. Click **OK**.
- Deleting a PON sub-interface
  a. Choose **WAN Access** > **PON Interface** to display the **PON Interface** page.
  b. Select the check box of the interface to be deleted and click **Delete** in the **Interface Name** column.
  c. Click **OK**.
- Switching the mode of a PON interface
  a. Choose **WAN Access** > **PON Interface** to display the **PON Interface** page.
  b. Click corresponding to the PON interface whose mode needs to be switched in the **Operation** column of **PON Interface List**.
  c. Select a mode in the dialog box that is displayed and click **OK**.
  The configuration takes effect after several minutes.

----End

Copyright © Huawei Technologies Co., Ltd.

2.12.8 Logical Interface

Context

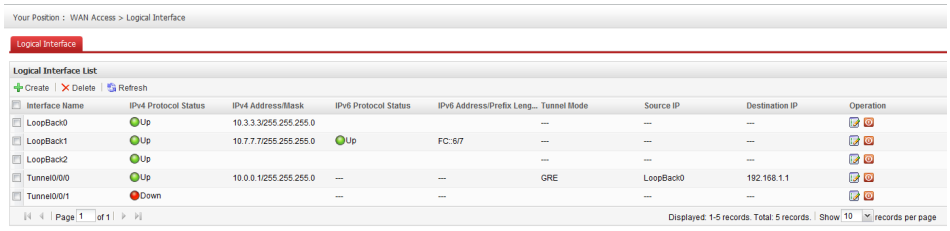
The web platform supports the configuration of logical interfaces including loopback interfaces and tunnel interfaces.

- A loopback interface is always Up at the physical layer and link layer unless it is manually shut down. You can configure loopback interfaces to enhance network reliability.
- Tunnel interfaces are used to establish tunnels.

Procedure

- Creating a logical interface
  a. Choose **WAN Access** > **Logical Interface**.

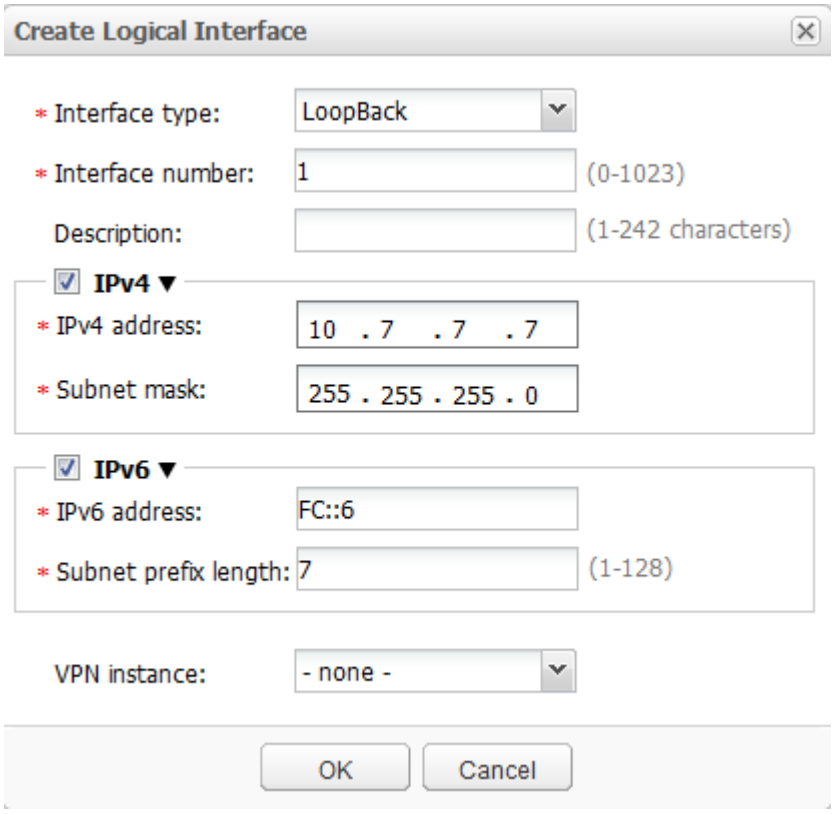
  Figure 2-105 Logical Interface Page

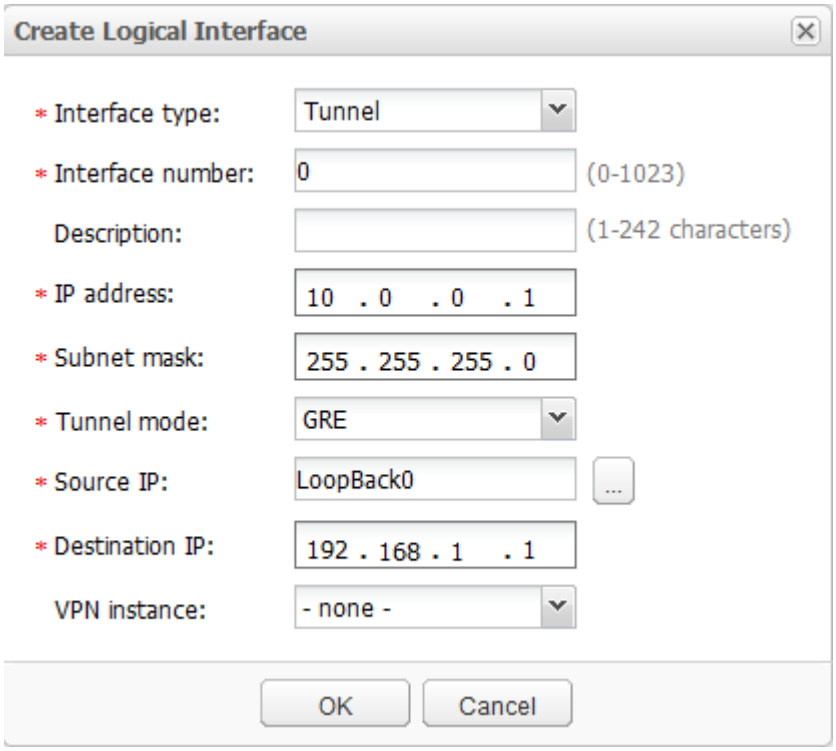
  b. Click **Create**.
  c. Set parameters in the **Create Logical Interface** dialog box. The parameters are as described in **Table 2-91**.

Copyright © Huawei Technologies Co., Ltd.

- **Figure 2-106** Create Logical Interface (Interface type is LoopBack)



- **Figure 2-107** Create Logical Interface (Interface type is Tunnel)



 Copyright © Huawei Technologies Co., Ltd.

Table 2-91 Logical interface parameters

Parameter	Description
Interface type	Logical interface type. Loopback interfaces and tunnel interfaces are supported, see **Figure 2-106** and **Figure 2-107** respectively.
Interface number	Logical interface number.
Description	Description of an interface. By default, the description of an interface is empty.
IP address	IPv4 address of the interface. The IP address of the interface cannot conflict with the IP address of any other interfaces or devices. **NOTE** For a loopback interface, this parameter is available when the **IPv4** check box is selected.
Subnet mask	Subnet mask of the interface. **NOTE** For a loopback interface, this parameter is available when the **IPv4** check box is selected.
IPv6 address	IPv6 address of an interface. **NOTE** This parameter is available only when **Interface type** is set to **LoopBack** and the **IPv6** check box is selected.
Subnet prefix length	Length of the IPv6 address prefix. **NOTE** This parameter is available only when **Interface type** is set to **LoopBack** and the **IPv6** check box is selected.
Tunnel mode	This parameter is valid when you create a tunnel interface. The following tunnel modes are supported: • IPSec • GRE

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Source IP	Source address of the tunnel interface. • Generic Routing Encapsulation (GRE) tunnels use tunnel interfaces at both endpoints of the tunnels. The source address of the local tunnel interface is the destination address of the peer tunnel interface. The destination address of the local tunnel interface is the source address of the peer tunnel interface. • Two or more tunnel interfaces encapsulated by the same protocol cannot be configured with the same source or destination address. Two or more point-to-multipoint (P2MP) tunnel interfaces cannot be configured with the same source address.
Destination IP	Destination address of the tunnel interface. On GRE tunnels, the source address of the local tunnel interface is the destination address of the peer tunnel interface, and the destination address of the local tunnel interface is the source address of the peer tunnel interface.
VPN instance	VPN instance bound to an interface. **NOTE** Before setting this parameter, you must create a VPN instance. For the detailed procedure, see **2.17.4 VPN Instance**.

d. Click **OK**.

- Modifying logical interface configuration
  a. Choose **WAN Access** > **Logical Interface**
  b. Click  corresponding to the logical interface to be configured in the **Operation** column of **Logical Interface List** to display the modification page.

Copyright © Huawei Technologies Co., Ltd.

c. Set the parameters described in **Table 2-91**.
d. Click **OK** to complete the configuration.

- Deleting a logical interface
  a. Choose **WAN Access** > **Logical Interface**.
  b. Select the check box next to a logical interface, and click **Delete**.
  c. Click **OK**.
- Disabling a logical interface
  a. Choose **WAN Access** > **Logical Interface** to display the **Logical Interface** page.
  b. Click corresponding to the logical interface to be disabled in the **Operation** column of **Logical Interface List**.
  c. Click **OK**.
- Enabling a logical interface
  a. Choose **WAN Access** > **Logical Interface** to display the **Logical Interface** page.
  b. Click corresponding to the logical interface to be disabled in the **Operation** column of **Logical Interface List**.
  c. Click **OK**.

----End

2.12.9 Interface Backup

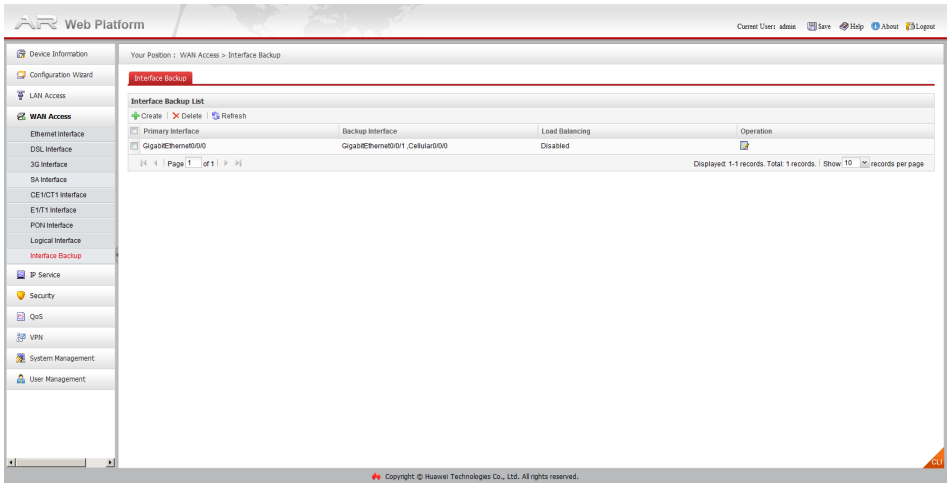
Context

The interface backup function allows a backup interface to transmit traffic when the primary interface is faulty or load balance traffic when bandwidth of the primary interface is insufficient.

Procedure

- Create interface backup.
  a. Choose **WAN Access** > **Interface Backup**, as shown in **Figure 2-108**.

Figure 2-108 Interface backup configuration page



 Copyright © Huawei Technologies Co., Ltd.

b. Click **Create** in **Interface Backup List**.

c. On the **Create Interface Backup** page, set parameters. **Table 2-92** describes the parameters.

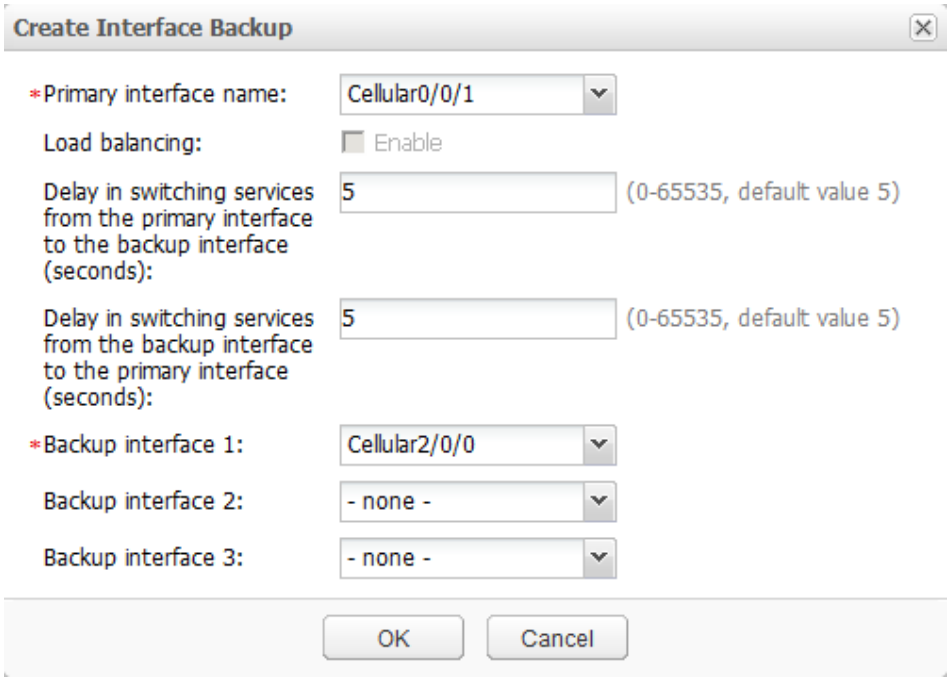


Table 2-92 Description of parameters for creating interface backup

Parameter	Description
Primary interface name	Selects a physical interface on the router.
Load balancing	Enables or disables load balancing.
Backup interface 1	Selects a physical interface on the router.
Backup interface 2	Selects a physical interface on the router.
Backup interface 3	Selects a physical interface on the router.
Available bandwidth (Kbps)	Indicates the maximum bandwidth of the primary interface in load balancing mode. **NOTE** The value 0 indicates that the actual physical bandwidth of a physical interface is used as the available bandwidth of the primary interface.
Upper threshold of traffic in load balancing mode (%)	Sets the upper threshold of the traffic volume in load balancing mode. **NOTE** The upper threshold of the traffic volume must be larger than the lower threshold.

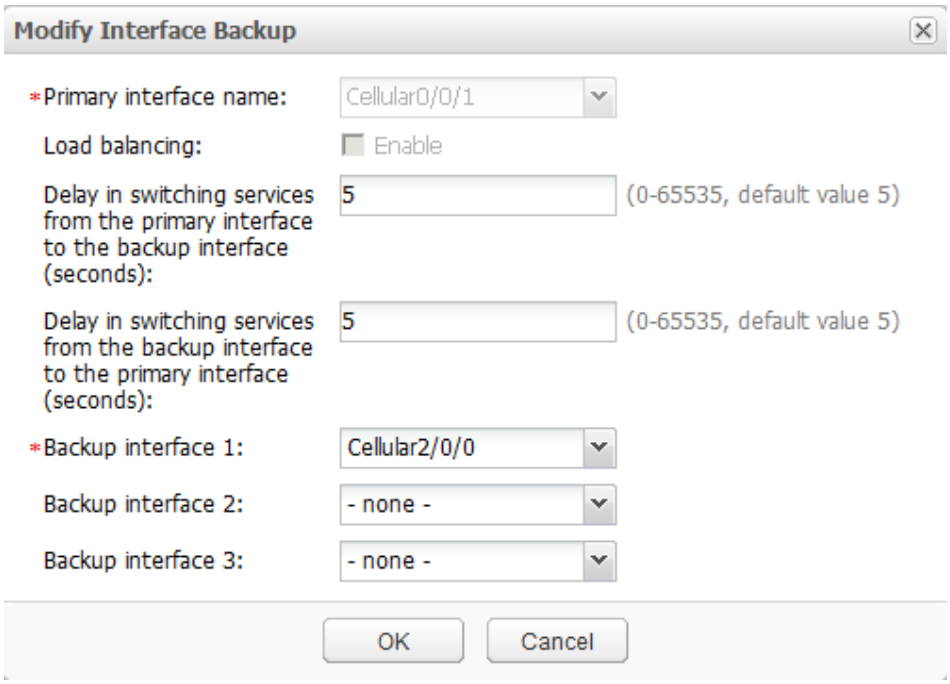
Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Delay in switching services from the primary interface to the backup interface (seconds)	Indicates the delay in switching services from the primary interface to the backup interface in active/standby mode.
Lower threshold of traffic in load balancing mode (%)	Sets the lower threshold of the traffic volume in load balancing mode. **NOTE** The lower threshold of the traffic volume must be smaller than the upper threshold.
Delay in switching services from the backup interface to the primary interface (seconds)	Indicates the delay in switching services from the backup interface to the primary interface in active/standby mode.

d. Click **OK**.

- Modify interface backup.
  a. Choose **WAN Access** > **Interface Backup**, as shown in **Figure 2-108**.
  b. In **Interface Backup List**, select a backup interface to be modified and right-click  .
  c. In the **Modify Interface Backup** dialog box, modify parameters, as shown in **Table 2-92**. The value of **Primary interface name** cannot be changed.

Copyright © Huawei Technologies Co., Ltd.



d. Click **OK**.

- Delete interface backup.
  a. Choose **WAN Access** > **Interface Backup**, as shown in **Figure 2-108**.
  b. In **Interface Backup List**, select a backup interface to be deleted and right-click .
  c. Click **OK** in the displayed dialog box.

----End

2.13 WLAN AC

NOTE

- The Classic web platform does not support WLAN AC. To use WLAN AC functions, choose **WLAN AC** > **WLAN AC**. A dialog box is displayed, asking "Classic web does not provide the WLAN AC function. If the WLAN AC function is required, use EasyOperation web. Switch to EasyOperation web immediately?" Click **Yes** to switch to the EasyOperation web platform.
- The AR109, AR109W, and AR109GW-L on the EasyOperation web platform do not support the WLAN AC function. Therefore, the WLAN AC function cannot be configured for these models on the EasyOperation web platform.

2.14 IP Services

2.14.1 DHCP

Copyright © Huawei Technologies Co., Ltd.

2.14.1.1 DHCP Configuration

Context

The Dynamic Host Configuration Protocol (DHCP) dynamically assigns IPv4 addresses to users and manages user configurations in a centralized manner.

The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) assigns IPv6 addresses, prefixes, and other network configuration parameters to hosts.

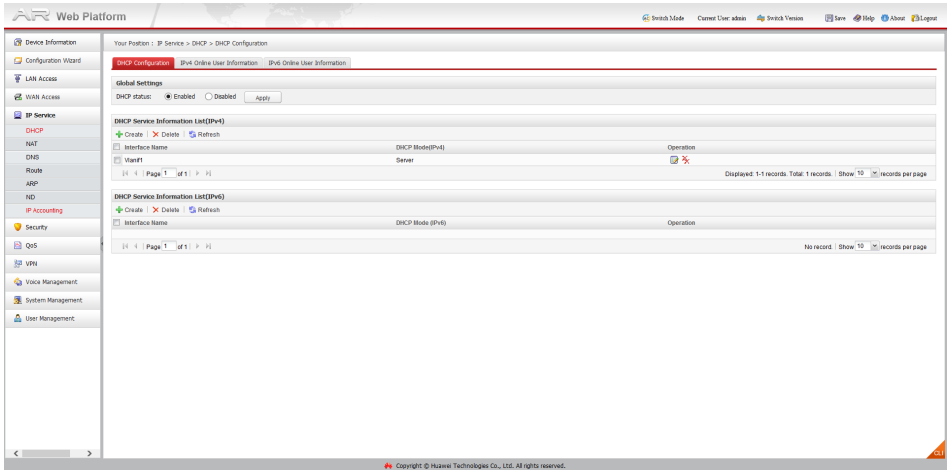
An interface that is assigned an IPv4 or IPv6 address and enabled with DHCP can assign IPv4 or IPv6 addresses to its connected terminals. DHCP helps centrally manage terminals.

A device can be configured as a DHCP server based on an interface address pool to assign dynamically IPv4 or IPv6 addresses to users. The addresses are on the network segment to which user interface addresses belong. The interface can be a Layer 3 physical interface or a logical interface such as a VLANIF interface. For the interface-related operations, see **2.11.1.1 Physical Interface** and **2.11.1.2 VLAN Interface**.

Procedure

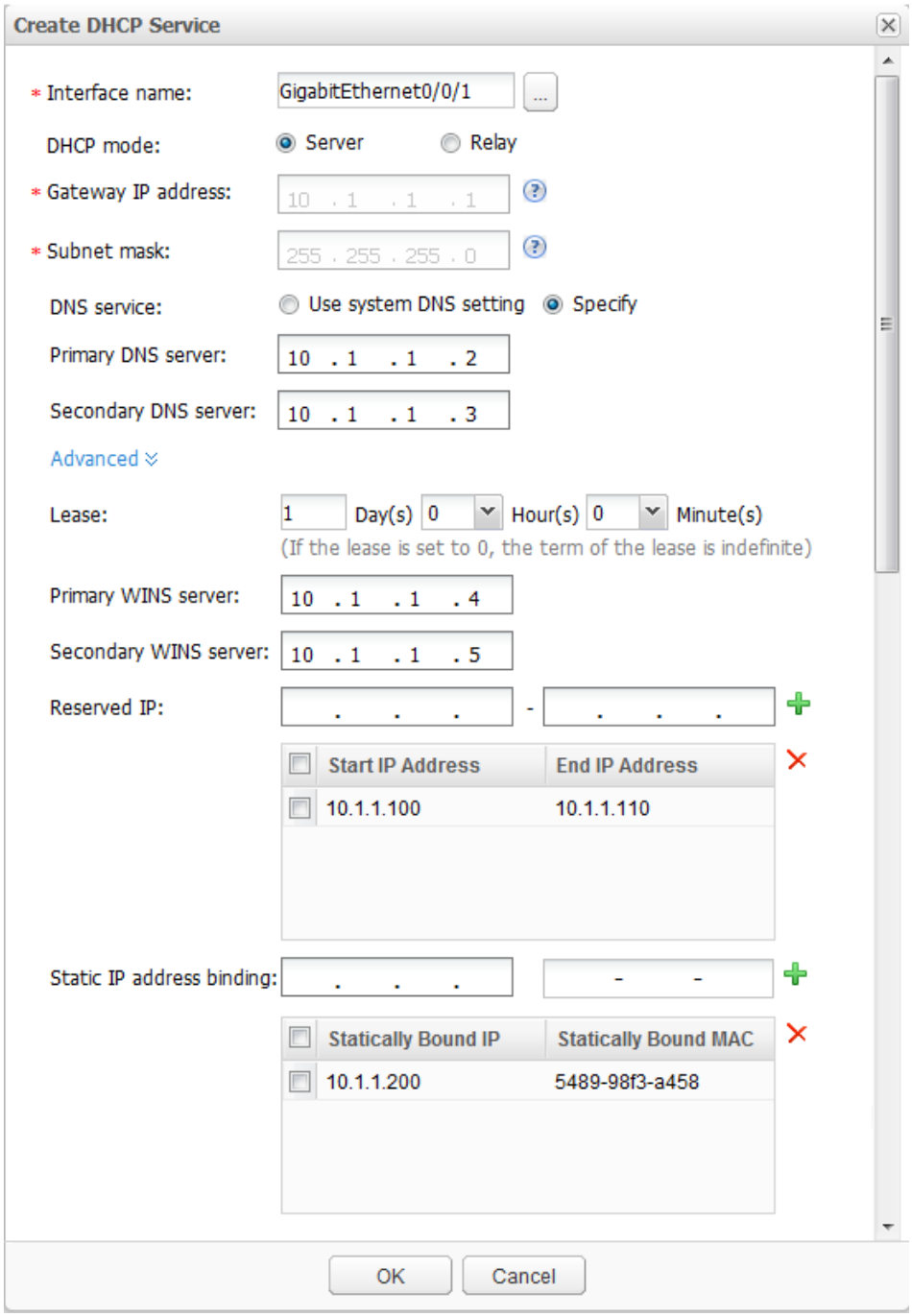
- Creating the DHCP service (IPv4)
  a. Log in to the web platform and choose **IP Service** > **DHCP** > **DHCP Configuration**, as shown in **Figure 2-109**.

     Figure 2-109 DHCP Configuration page

  b. Set **DHCP status** to **Enabled** and click **Apply**. DHCP is globally enabled.
  c. Click **Create** in the **DHCP Service Information List(IPv4)** area, and set DHCP service parameters in the **Create DHCP Service** dialog box that is displayed. **Table 2-93** describes the parameters.

Copyright © Huawei Technologies Co., Ltd.



d. Click **OK**.

Table 2-93 DHCP service parameters

Parameter	Description
Interface name	Name of the interface mapping the interface address pool on a DHCP server. The DHCP server can assign the IP addresses on the network segment to which the interface IP address belongs.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
DHCP mode	DHCP mode on the interface. The options are as follows: • **Server**: The DHCP server can assign the IP addresses on the network segment to which the interface IP address belongs. • **Relay**: DHCP relay is enabled on the interface. When the interface works in DHCP relay mode, the IP address of the destination DHCP server must be specified.
Gateway IP address	Gateway IP address of DHCP clients. The system specifies the interface IP address as the gateway IP address.
Subnet mask	Subnet mask of the IP address assigned to a DHCP client. The system specifies the interface subnet mask as the subnet mask assigned to the DHCP client. The gateway IP address and subnet mask identify the range of the address pool on an interface.
DNS service	DNS server address assigned to DHCP clients. When DHCP clients use domain names to access network services, configure the IP address of the DNS server. Ensure that the route between the DNS server and the DHCP server is reachable. Set the IP address of the DNS server in either of the following ways: • **Use system DNS setting**: DHCP server uses the default gateway IP address as the IP address of the DNS server. • **Specify**: Directly specify the IP address of the DNS server.
Primary DNS server	Primary DNS server address assigned to DHCP clients. When **DNS service** is set to **Specify**, set this parameter.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Secondary DNS server	Secondary DNS server address assigned to DHCP clients. When the primary DNS server fails to perform domain name resolution, the DHCP client sends a domain name resolution request to the secondary DNS server.
Lease	IP address lease of DHCP clients, that is, duration during which IP addresses assigned to DHCP clients take effect. Set this parameter based on the duration during which DHCP clients of the interface address pool are connected to the network. For example, set a short lease, such as 8 hours, for wireless clients that frequently connect to and disconnect from the wireless network. Set a long lease even a permanent lease for stable clients.
Primary WINS server	Primary WINS server address assigned to DHCP clients. DHCP clients running the Windows operating system use the Network Basic Input Output System (NetBIOS) protocol for communication. The NetBIOS server translates host names to IP addresses for the clients. The resolution of the NetBIOS name to an IP address is done locally, by broadcasts, or by a WINS server. Ensure that the route between the primary WINS server and the DHCP server is reachable.
Secondary WINS server	Secondary WINS server address assigned to DHCP clients. When the primary WINS server fails to perform NetBIOS name resolution, the DHCP client sends a NetBIOS name resolution request to the secondary WINS server. Ensure that the route between the secondary WINS server and the DHCP server is reachable.

Copyright © Huawei Technologies Co., Ltd.

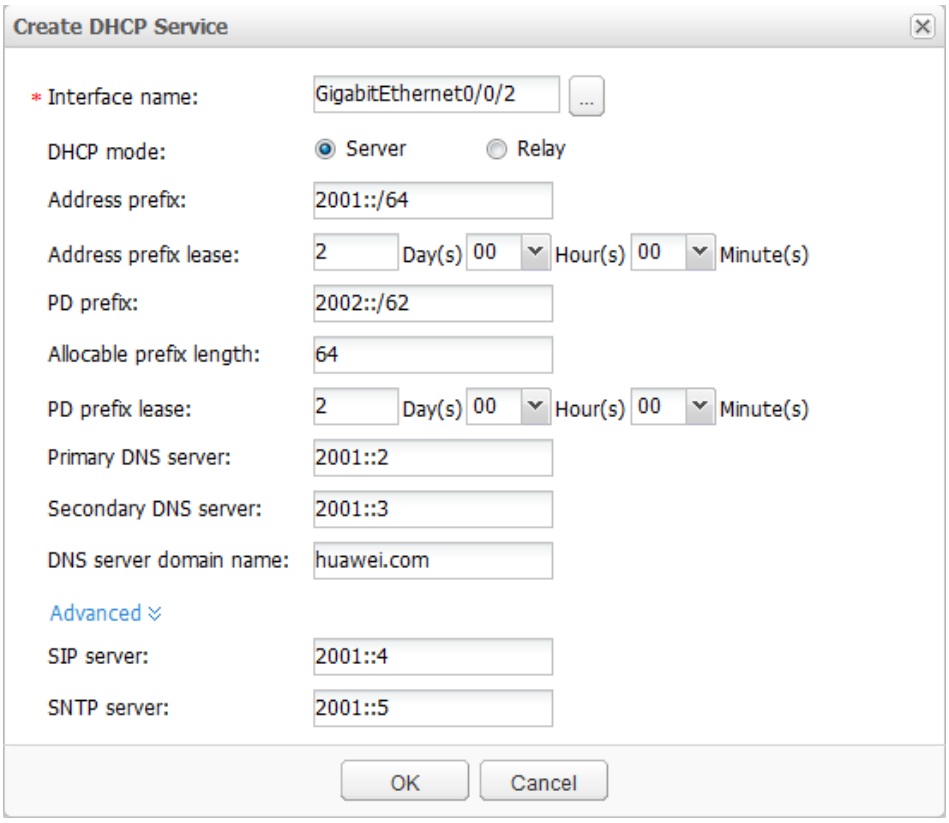
Parameter	Description
Reserved IP	IP address that will not be dynamically assigned. When IP addresses are assigned to other servers such as DNS servers, the IP addresses cannot be assigned to DHCP clients. Specify these IP addresses as reserved IP addresses. This operation avoids IP address conflicts and shortens the IP address detection time during IP address assignment, which improves DHCP efficiency. Perform the following operation to create or delete a reserved IP address (segment): • Creating a reserved IP address: Enter the start and end IP addresses and click  . To create multiple reserved IP addresses or IP address segments, repeat this operation. • Deleting a reserved IP address: Select the check box of a reserved IP address or select the check box next to **Start IP Address**, and click  .
Start IP Address	Start IP address that will not be dynamically assigned. When the start IP address is assignable, the configuration takes effect.
End IP Address	End IP address that will not be dynamically assigned. The end IP address must be in the same network segment with the start IP address. When the end IP address is assignable, the configuration takes effect. If no end IP address is assigned or the end IP address is the same as the start IP address, only the start IP address is reserved.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Static IP address binding	Binding between assignable IP addresses and MAC addresses of the clients. When receiving a request for applying for an IP address from a client matching the MAC address, the DHCP server assigns the fixed IP address bound to the client's MAC address to this client. Perform the following operation to create or delete a static IP address entry: • Creating a static IP address binding entry: Enter the IP address and MAC address to bind and click . To create multiple static IP address binding entries, repeat this operation. • Deleting a static IP address binding entry: Select the check box of a static IP address binding entry or select the check box next to **Static IP address binding**, and click  .
Statically Bound IP	IP address to be bound to a MAC address. When the IP address is assignable, the configuration takes effect.
Statically Bound MAC	MAC address of a host.

- Creating the DHCP service (IPv6)
  a. Log in to the web platform and choose **IP Service** > **DHCP** > **DHCP Configuration**.
  b. Set **DHCP status** to **Enabled** and click **Apply**. DHCP is globally enabled.
  c. Click **Create** in the **DHCP Service Information List(IPv6)** area, and set DHCP service parameters in the **Create DHCP Service** dialog box that is displayed. **Table 2-94** describes the parameters.

Copyright © Huawei Technologies Co., Ltd.



d. Click **OK**.

Table 2-94 DHCP service parameters

Parameter	Description
Interface name	Name of the interface mapping the interface address pool on a DHCPv6 server. The DHCPv6 server can assign the IPv6 addresses on the network segment to which the interface IP address belongs.
DHCP mode	DHCP mode on the interface. The options are as follows: • **Server**: The DHCPv6 server can assign the IPv6 addresses on the network segment to which the interface IP address belongs. • **Relay**: DHCPv6 relay is enabled on the interface. When the interface works in DHCPv6 relay mode, the IPv6 address of the destination DHCPv6 server must be specified.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Address prefix	Network prefix of the interface IPv6 address, which identifies a network segment. The clients can obtain IPv6 addresses on this network segment. The value is in the X:X::X:X/M format, for example, 2001::1/64. You must specify this parameter when clients need to obtain IPv6 addresses from the DHCPv6 server.
Address prefix lease	Lease of the IP addresses assigned to DHCPv6 clients. You must specify this parameter when clients need to obtain IPv6 addresses from the DHCPv6 server. Set this parameter based on the duration during which DHCPv6 clients are connected to the network. For example, set a short lease, such as 8 hours, for wireless clients that frequently connect to and disconnect from the wireless network. Set a long lease for stable clients.
PD prefix	Address prefix (network segment) assigned to a DHCPv6 client. The value is in the X:X::X:X/M format, for example, 2001::/62. You must specify this parameter when clients need to obtain IPv6 address prefixes from the DHCPv6 server.
Allocable prefix length	Length of the address prefix assigned to a DHCPv6 client. The value of this parameter must be greater than or equal to the value of **PD prefix**, and the difference between them must be smaller than or equal to 16. You must specify this parameter when clients need to obtain IPv6 address prefixes from the DHCPv6 server.
PD prefix lease	Lease of the IP address prefixes assigned to DHCPv6 clients.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Primary DNS server	Primary DNS server IPv6 address assigned to DHCPv6 clients.
Secondary DNS server	Secondary DNS server IPv6 address assigned to DHCPv6 clients. When the primary DNS server fails to perform domain name resolution, the DHCPv6 client sends a domain name resolution request to the secondary DNS server.
DNS server domain name	Domain name suffix assigned to a DHCPv6 client.
SIP server	Session Initiation Protocol (SIP) server IPv6 address assigned to DHCPv6 clients.
SNTP server	Simple Network Time Protocol (SNTP) server IPv6 address assigned to DHCPv6 clients.

- Modifying the DHCP service
  a. Log in to the web platform and choose **IP Service** > **DHCP** > **DHCP Configuration**.
  b. Select the DHCP configuration in the **DHCP Service Information List(IPv4)** or **DHCP Service Information List(IPv6)** area, and click  .
  c. In the **Change DHCP Service** dialog box that is displayed, modify parameters listed in **Table 2-93** for IPv4 or **Table 2-94** for IPv6.
  d. Click **OK**.
- Deleting the DHCP service
  a. Log in to the web platform and choose **IP Service** > **DHCP** > **DHCP Configuration**.
  b. Select the check box of the DHCP configuration in the **DHCP Service Information List(IPv4)** or **DHCP Service Information List(IPv6)** area and click **Delete**.
  c. In the dialog box that is displayed, click **OK**.
- Resetting the gateway IP address used by DHCP clients

  NOTE

  This function is supported in V200R010C10 and later versions.

  a. Log in to the web platform and choose **IP Service** > **DHCP** > **DHCP Configuration**. On the DHCP configuration page that is displayed, check DHCP related parameters.
  b. On the **DHCP Service Information List(IPv4)** toolbar, select the DHCP service to be reset and click  on the right.

 Copyright © Huawei Technologies Co., Ltd.

c. In the dialog box that is displayed, click **OK** to reset the gateway IP address used by DHCP clients.

----End

2.14.1.2 IPv4 Online User Information

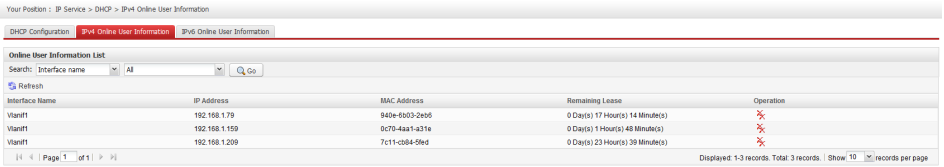
Context

You can view the IP address, MAC address, and time when the IP address lease has used of DHCP clients on the **Online User Information** tab page.

Procedure

- Viewing information about online users
  a. Log in to the web platform and choose **IP Service** > **DHCP** > **IPv4 Online User Information**, as shown in **Figure 2-110**.

  Figure 2-110 IPv4 Online User Information page

  b. View information about a specified user in either of the following ways:
     - Select **Interface name** from the **Item** drop-down list box and select the interface name to view.
     - Select **IP Address** from the **Item** drop-down list box and enter the IP address to view.
  c. Click **Search**. **Table 2-95** describes online user parameters.

  Table 2-95 Online user parameters

Parameter	Description
Interface Name	Name of the interface mapping the interface address pool on a DHCP server.
IP Address	IP address that the DHCP server assigns to a DHCP client.
MAC Address	MAC address of the DHCP client.
Time Elapsed Remaining Lease	Time the lease expires, that is, time when IP addresses of DHCP clients expire.

- Resetting IP addresses assigned to DHCP clients

 Copyright © Huawei Technologies Co., Ltd.

NOTE

This function is supported in V200R010C10 and later versions.

a. Log in to the web platform and choose **IP Service** > **DHCP** > **IPv4 Online User Information**. On the **IPv4 Online User Information** page that is displayed, check information about IPv4 online users.

b. On the **Online User Information List** toolbar, check the interfaces whose IP addresses need to be reset and click on the right.

c. In the dialog box that is displayed, click **OK** to reset the IP addresses that the DHCP server assigns to DHCP clients.

----End

2.14.1.3 IPv6 Online User Information

Context

You can view online user information and conflict addresses assigned by the DHCPv6 server.

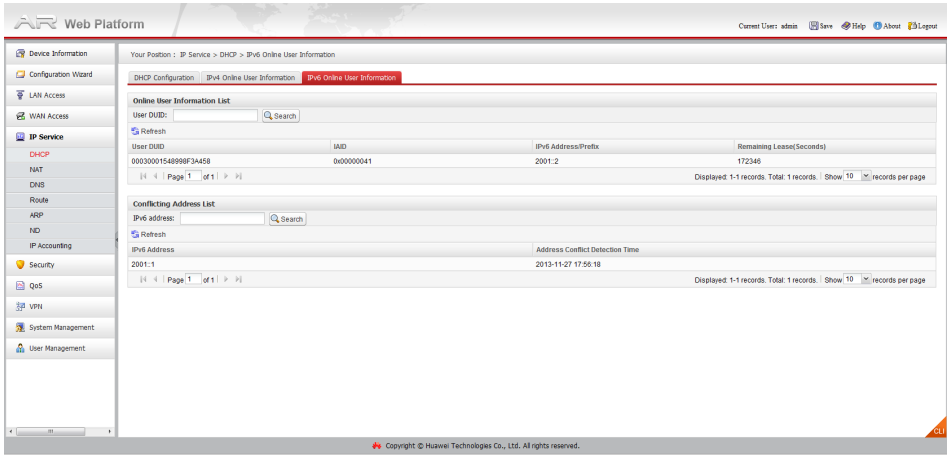
- **Online User Information List** area: displays the DHCPv6 unique identifiers (DUID), identity association identifier (IAID), IPv6 address and prefix assigned by the DHCPv6 server, and remaining lease of the IPv6 address.
- **Conflicting Address List** area: displays conflict IPv6 addresses that the DHCPv6 server assigns to the DHCPv6 clients.

Procedure

- Viewing information about online users

  a. Log in to the web platform and choose **IP Service** > **DHCP** > **IPv6 Online User Information**. **Online User Information List** is displayed, as shown in **Figure 2-111**.

  Figure 2-111 IPv6 Online User Information page

  b. In the **Online User Information List** area, set **User DUID** and click **Search**. The search result is displayed. **Table 2-96** describes the parameters.

 Copyright © Huawei Technologies Co., Ltd.

Table 2-96 Online user information parameters

Parameter	Description
User DUID	DUID of the DHCPv6 client.
IAID	IAID of the DHCPv6 client.
IPv6 Address/Prefix	IPv6 address and prefix obtained by the DHCPv6 client.
Remaining Lease(Seconds)	Remaining lease of the IPv6 address obtained by the DHCPv6 client.

- Viewing conflict addresses
  a. Log in to the web platform and choose **IP Service** > **DHCP** > **IPv6 Online User Information**. **Conflicting Address List** is displayed.
  b. In the **Conflicting Address List** area, enter an IPv6 address in the **IPv6 address** text box and click **Search**. The search result is displayed. **Table 2-97** describes the parameters.

  Table 2-97 Conflict address list parameters

Parameter	Description
IPv6 Address	Conflict IPv6 address.
Address Conflict Detection Time	Time when the conflict IPv6 address is detected.

----End

2.14.2 NAT

2.14.2.1 Global Settings

Context

Generally, NAT translates only the address in the IP packet header and the port number in the TCP/UDP header. Packets of some protocols such as DNS and FTP contain the IP address or port number in the data fields. Such contents cannot be translated through NAT. Therefore, communication between the internal network and external networks will fail.

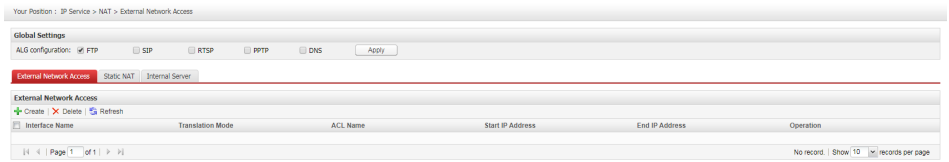
To solve this problem, NAT must be able to identify the IP address or port information in the data field. The application level gateway (ALG) function enables the NAT device to identify the IP address or port number in the data field, and translate addresses according to the mapping table. The device provides the ALG function, so the device can support various special application protocols, including DNS, FTP, SIP, PPTP and RTSP.

Copyright © Huawei Technologies Co., Ltd.

Procedure

- Configuring the ALG
  a. Log in to the web platform, and choose **IP Service** > **NAT**. **Figure 2-112** shows the **Global Settings** area.

     Figure 2-112 Global Settings area

  b. In the **Global Settings** area, select application protocols supported by ALG.
  c. Click **Apply**. In the dialog box indicating that the operation succeeds that is displayed, click **OK**. The ALG configuration is complete.

----End

2.14.2.2 External Network Access

Context

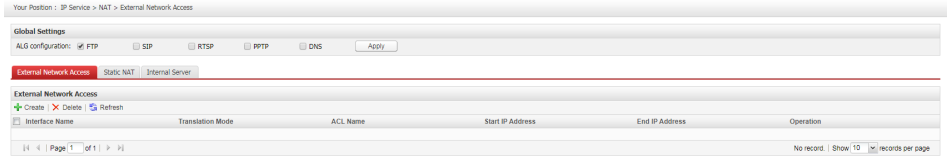
When enterprise users access the Internet using NAT, network address port translation (NAPT) can be configured to implement concurrent address translation. NAPT allows multiple internal addresses to be mapped to the same public address. It is also called many-to-one address translation or address multiplexing. NAPT translates the IP address and port number of a packet so that multiple private users can use the same public IP address to access the Internet.

Easy IP uses access control lists (ACLs) to control the private IP addresses that can be translated. Easy IP applies to the scenario where hosts on small-scale LANs access the Internet. Generally, small-scale LANs are deployed at small- and medium-sized cybercafes or small-sized offices where only a few internal hosts are used and the outbound interface obtains a temporary public IP address through dial-up. Internal hosts use the temporary public IP address to access the Internet.

Procedure

- Creating an external network access configuration
  a. Log in to the web platform, and choose **IP Service** > **NAT**. The **External Network Access** tab page is displayed, as shown in **Figure 2-113**.

     Figure 2-113 External Network Access tab page

  b. Click **Create**, and set parameters in the **Create External Network Access** dialog box that is displayed. **Table 2-98** describes the parameters.

 Copyright © Huawei Technologies Co., Ltd.

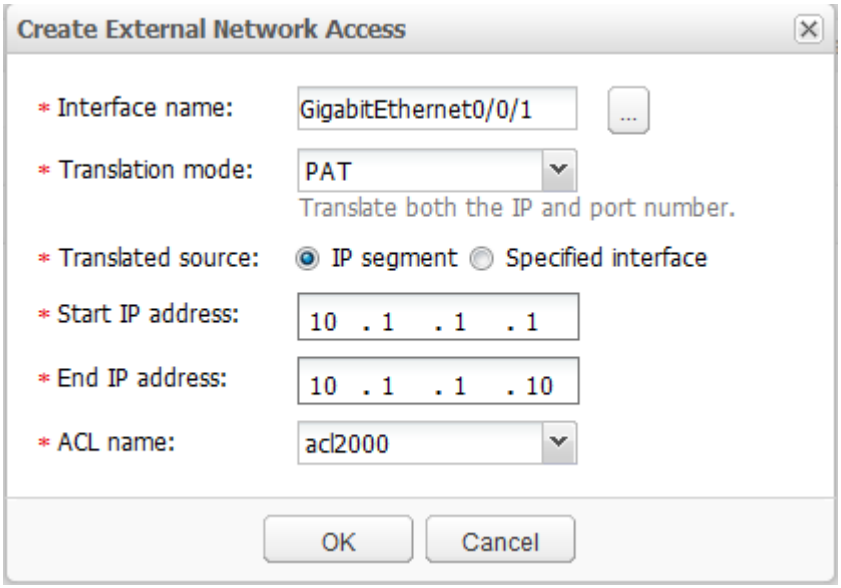


Table 2-98 External network access parameters

Parameter	Description
Interface name	Name of an interface where network access is to be enabled. Generally, Layer 3 interface is configured, except loopback and NULL interfaces.
Translation mode	IP address translation mode used by internal users to access external servers. Translation modes are as follows: • PAT (Port Address Translation): The IP address and port number in a data packet are translated at the same time. • Easy IP: The IP address of the selected interface is used as the translated public IP address. • NO-PAT: Only the IP address in a data packet is translated. The port number is not used. **NOTE** If users access a network through dialup such as Point-to-Point Protocol over Ethernet (PPPoE), you can select **Easy IP**.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Translated source	Translated source address in PAT mode. • IP segment: Specifies an IP address segment of the translated source IP address (the network segment of the NAT address pool). • Specified interface: Specifies a specified interface IP address as the translated source IP address.
Specified interface	Specified interface IP address, which is used as the translated source IP address.
Start IP address	Start IP address of the NAT address pool.
End IP address	End IP address of the NAT address pool. The end IP address must be not smaller than the start IP address. A maximum of 255 IP addresses can be configured in the NAT address pool.
ACL name	ACL for internal users.

c. Click **OK**.

- Modifying an external network access configuration
  a. Log in to the web platform, and choose **IP Service** > **NAT**. The **External Network Access** tab page is displayed.
  b. In the **External Network Access** area, click  corresponding to an external network access configuration.
  c. In the **Modify External Network Access** dialog box, modify parameters listed in **Table 2-98** based on the site requirements. The **Interface name** parameter cannot be modified.
  d. Click **OK** to make the settings take effect.
- Deleting an external network access configuration
  a. Log in to the web platform, and choose **IP Service** > **NAT**. The **External Network Access** tab page is displayed.
  b. In the **External Network Access** area, select the check box next to an external network access configuration, and click **Delete**.
  c. In the dialog box that is displayed, click **OK**.
- Updating the external network access entry
  a. Log in to the web platform and choose **IP Service** > **NAT** > **External Network Access** to check the configured external network access entry.
  b. Click **Refresh** to update the external network access entry.

----End

 Copyright © Huawei Technologies Co., Ltd.

2.14.2.3 Static NAT

Context

Some enterprise hosts must use fixed IP addresses to access public networks when NAT is enabled. Static NAT maps a public IP address to a fixed private IP address.

NOTE

When establishing static binding between private IP addresses and public IP addresses, ensure that the public IP address is on the same network segment as the IP address of the interface enabled with static NAT. Packets sent to public network servers can be correctly forwarded to the interface enabled with static NAT.

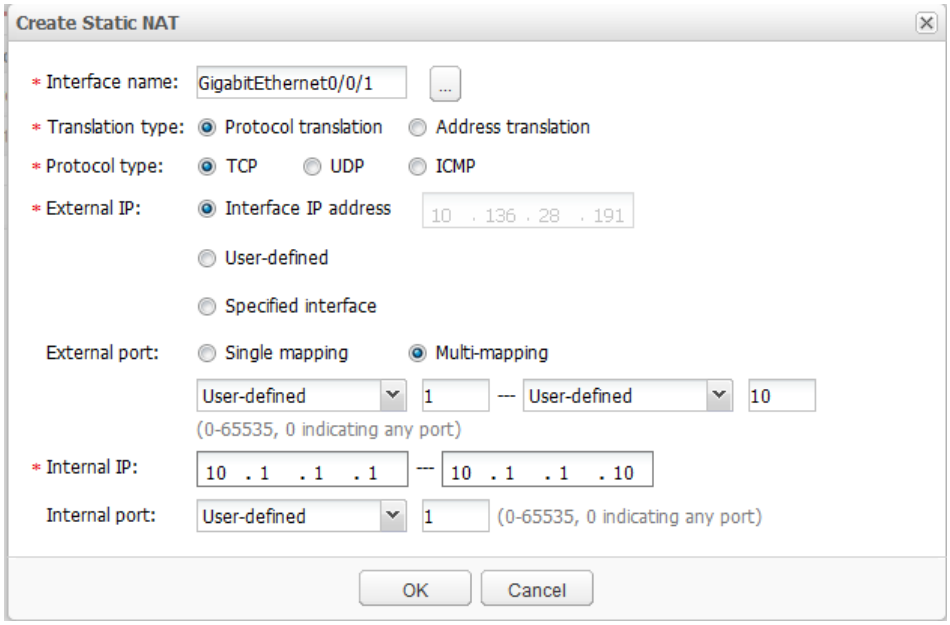
Procedure

- Creating a static NAT configuration
  a. Log in to the web platform and choose **IP Service** > **NAT** > **Static NAT**, as shown in **Figure 2-114**.

  Figure 2-114 Static NAT page

  b. Click **Create** in the **Static NAT** area and set parameters in the **Create Static NAT** dialog box that is displayed. **Table 2-99** describes the parameters.

 Copyright © Huawei Technologies Co., Ltd.

Table 2-99 Static NAT parameters

Parameter	Description
Interface name	Name of an interface where static NAT is to be enabled. Generally, Layer 3 interface is configured, except loopback and NULL interfaces.
Translation type	Whether to translate addresses according to the protocol type: • Protocol translation: translates addresses only when IP packets are transmitted on the specified protocol. • Address translation: translates IP addresses when IP packets are transmitted on any protocol.
Protocol type	Protocol type for which NAT is used. Currently, the following protocols are supported: Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP). **NOTE** When this parameter is set to ICMP, you need to set only **External IP** and **Internal IP**.
External IP	Public IP address used by private network users to access public network servers. The options are as follows: • Interface IP address: The IP address of the selected interface is used as the translated public IP address. • User-defined: A public IP address is manually specified. The specified IP address cannot be in use. The public IP address must be on the same network segment as the IP address of the NAT-enabled interface. • Specified interface: A specified interface address is used as the public IP address. **NOTE** If users access a network through dialup such as PPPoE, you can select **Interface IP address**.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
External port	Port number used by private network users to access public network servers. You can select a value from the drop-down list box or enter a port number. • Single mapping: indicates that a public IP address (with a specified port number) is mapped to one private IP address (with a specified port number). • Multi-mapping: indicates that a public IP address (with a group of port numbers) is mapped to multiple private IP addresses (with a specified port number).
Internal IP	IP address of a private network user.
Internal port	Source port number used by private network users to access public networks. You can select a value from the drop-down list box or enter a port number.

c. Click **OK**.

- Modifying a static NAT entry
  a. Log in to the web platform and choose **IP Service** > **NAT** > **Static NAT**.
  b. Select a static NAT entry, and click  .
  c. In the **Modify Static NAT** dialog box that is displayed, modify parameters listed in **Table 2-99**. The parameter **Interface name** cannot be modified.
  d. Click **OK**.
- Deleting a static NAT entry
  a. Log in to the web platform and choose **IP Service** > **NAT** > **Static NAT**.
  b. Select a static NAT entry, and click **Delete**.
  c. In the dialog box that is displayed, click **OK**.
- Updating the static NAT entry
  a. Log in to the web platform and choose **IP Service** > **NAT** > **Static NAT** to check the configured static NAT entry.
  b. Click **Refresh** to update the static NAT entry.

----End

2.14.2.4 Internal Server

Context

NAT can hide internal hosts. An enterprise network can use NAT to communicate with external networks, but external users cannot access internal servers. After the

 Copyright © Huawei Technologies Co., Ltd.

mappings between "public IP address+port number" and "private IP address+port number" are defined on a virtual server, external users can access internal servers.

As shown in **Figure 2-115**, a company is connected to the WAN through the device enabled with the network address translation (NAT) function. The company provides the web server for users on the public network to access. The private IP address of the web server is 192.168.1.2 and its public address is the interface address of GE1/0/0, 1.1.1.1.

Figure 2-115 Networking diagram for configuring the NAT server



The following table describes the mapping between public IP address+port number (port protocol name) and private IP address+port number (port protocol name). The mapping needs to be established in **Figure 2-115**.

Public IP Address+Port Number (Port Protocol Name)	Private IP Address+Port Number (Port Protocol Name)
1.1.1.1+80(WWW)	192.168.1.2+80(WWW)

Procedure

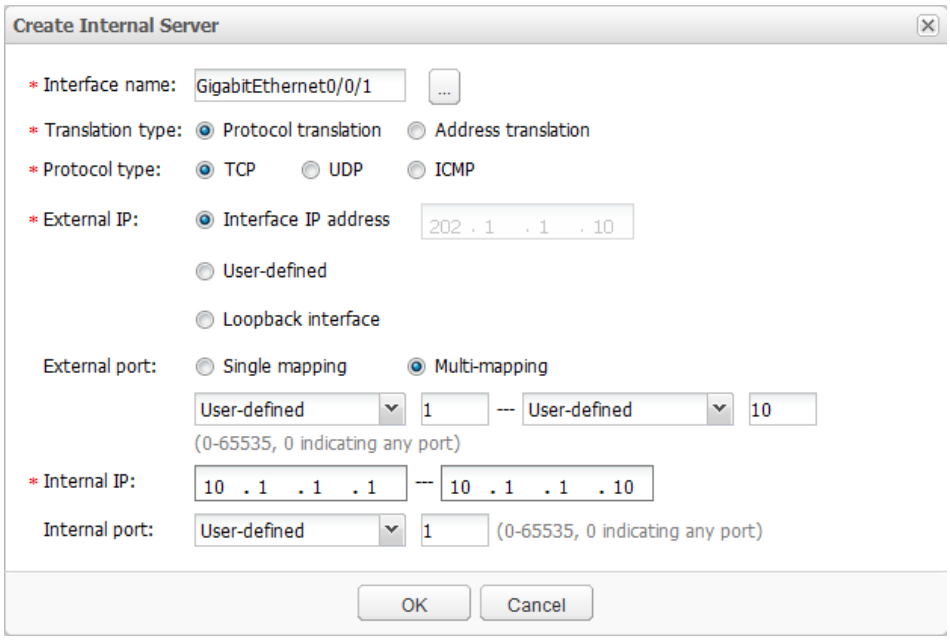
- Creating an internal server
  a. Log in to the web platform and choose **IP Service** > **NAT** > **Internal Server**, as shown in **Figure 2-116**.

     Figure 2-116 Internal Server page

  b. Click **Create** in the **Internal Server** area and set parameters in the **Create Internal Server** dialog box that is displayed. **Table 2-100** describes the parameters.

 Copyright © Huawei Technologies Co., Ltd.



c. Click **OK**. An internal server is added to the internal server list.

Table 2-100 Internal server parameters

Parameter	Description
Interface name	Name of an interface where NAT is to be enabled. Generally, Layer 3 interface is configured, except loopback and NULL interfaces.
Translation type	Whether to translate addresses according to the protocol type: • Protocol translation: translates addresses only when IP packets are transmitted on the specified protocol. • Address translation: translates IP addresses when IP packets are transmitted on any protocol.
Protocol type	Protocol type over the internal server. Currently, the following protocols are supported: TCP, UDP, and ICMP. **NOTE** When this parameter is set to ICMP, you need to set only **External IP** and **Internal IP**.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
External IP	Public IP address used by users to access external servers. The options are as follows: • Interface IP address: The IP address of the selected interface is used as the translated public IP address. • User-defined: A public IP address is manually specified. The specified IP address cannot be in use. The public IP address must be on the same network segment as the IP address of the NAT-enabled interface. • Specified interface: A specified interface address is used as the public IP address. **NOTE** If users access a network through dialup such as PPPoE, you can select **Interface IP address**.
External port	Port number used by external users to access internal servers. You can select a value from the drop-down list box or enter a port number. • Single mapping: indicates that a public IP address (with a specified port number) is mapped to one private IP address (with a specified port number). • Multi-mapping: indicates that a public IP address (with a group of port numbers) is mapped to multiple private IP addresses (with a specified port number).
Internal IP	IP address of an internal server.
Internal port	Port number of an internal server. You can select a value from the drop-down list box or enter a port number.

- Modifying an internal server
  a. Log in to the web platform and choose **IP Service** > **NAT** > **Internal Server**.
  b. Select an internal server in the **Internal Server** area, and click .
  c. In the **Modify Internal Server** dialog box that is displayed, modify parameters listed in **Table 2-100**. The parameter **Interface name** cannot be modified.

Copyright © Huawei Technologies Co., Ltd.

d. Click **OK**.

- Deleting an internal server
  a. Log in to the web platform and choose **IP Service** > **NAT** > **Internal Server**.
  b. Select an internal server and click **Delete**.
  c. In the dialog box that is displayed, click **OK**.
- Updating the internal server configuration
  a. Log in to the web platform and choose **IP Service** > **NAT** > **Internal Server** to check the configured internal server entry.
  b. Click **Refresh** to update the internal server entry.

----End

2.14.3 DNS

2.14.3.1 DNS

Context

Domain Name System (DNS) is a distributed database used in TCP and IP applications and completes resolution between IP addresses and domain names. Users can use the simple and meaningful domain names instead of the complicated IP addresses to access hosts. The DNS server then resolves the domain name into a correct IP address.

The device can parse IPv4 and IPv6 addresses.

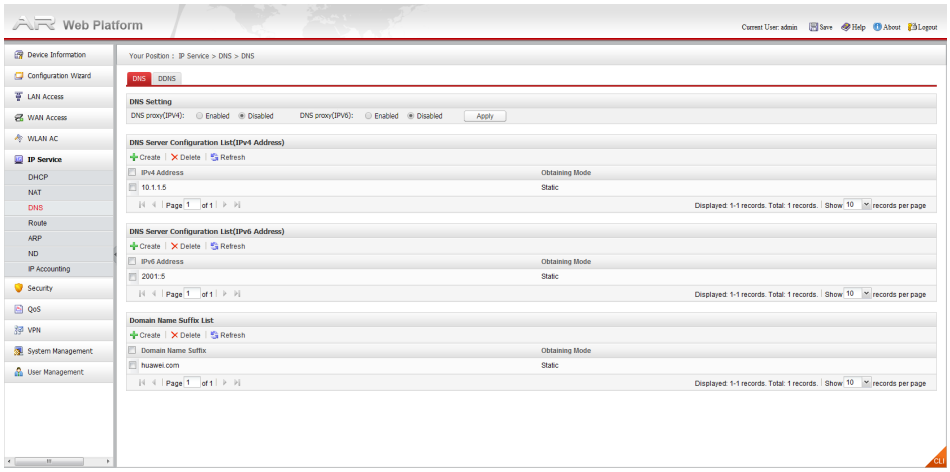
DNS proxy is used to forward DNS request and reply packets between the DNS client and DNS server. The DNS client sends DNS request packets to the DNS proxy. The DNS proxy forwards DNS request packets to the DNS server and sends reply packets to the DNS client. After DNS proxy is enabled, if the IP address of the DNS server changes, you only need to change the configuration on the DNS proxy.

Procedure

- Creating DNS configuration
  a. Log in to the web platform and choose **IP Service** > **DNS** > **DNS**, as shown in **Figure 2-117**.

 Copyright © Huawei Technologies Co., Ltd.

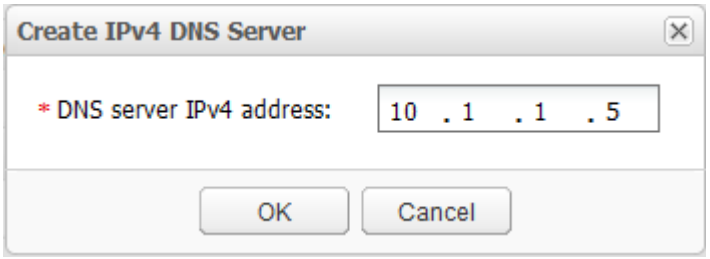
Figure 2-117 DNS page



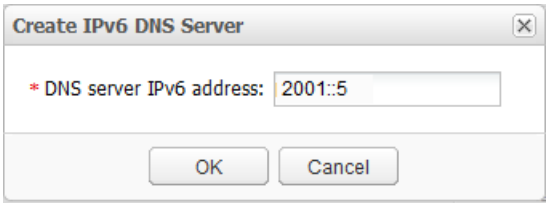
b. Set **DNS proxy** to **Enable** in the **DNS Setting** area, and click **Apply**.

c. Configure an IP address for the DNS server in the **DNS Server Configuration List(IPv4 Address)** or **DNS Server Configuration List(IPv6 Address)** area based on the IP address type.

- To configure an IPv4 address for the DNS server, click **Create** in the **DNS Server Configuration List(IPv4 Address)** area, and enter an IPv4 address in the **Create DNS Server IPv4 Address** dialog box that is displayed.



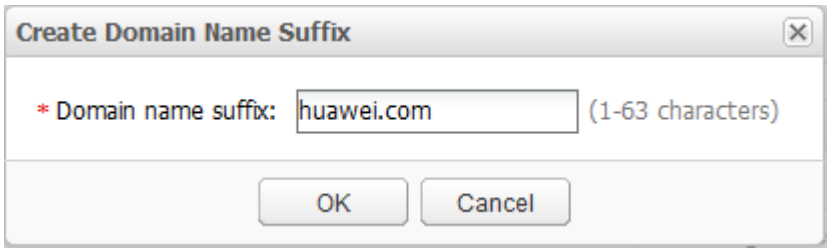
- To configure an IPv6 address for the DNS server, click **Create** in the **DNS Server Configuration List(IPv6 Address)** area, and enter an IPv6 address in the **Create DNS Server IPv6 Address** dialog box that is displayed.



d. Click **OK**. The default obtaining mode of the DNS server IP address is **Static**.

e. Click **Create** in the **Domain Name Suffix List** area, and set **Domain name suffix** in the **Create Domain Name Suffix** dialog box that is displayed.

 Copyright © Huawei Technologies Co., Ltd.



f. Click **OK**. The default obtaining mode of the DNS domain name is **Static**. **Table 2-101** describes the parameters.

Table 2-101 DNS parameters

Parameter	Description
DNS server IPv4 address	IPv4 address of a DNS server. This parameter is displayed after you click **Create** in the **DNS Server Configuration List(IPv4 Address)** area. **NOTE** A maximum of six DNS server IPv4 addresses can be configured. A previous configured DNS server takes priority over a later one. A device sends domain name resolution requests to DNS servers based on their priorities in descending order.
DNS server IPv6 address	IPv6 address of a DNS server. This parameter is displayed after you click **Create** in the **DNS Server Configuration List(IPv6 Address)** area. **NOTE** A maximum of six DNS server IPv6 addresses can be configured for DNS servers. A previous configured DNS server takes priority over a later one. A device sends domain name resolution requests to DNS servers based on their priorities in descending order.
Domain name suffix	DNS domain name suffix configured on the DNS client. You can pre-configure domain name suffixes. You only need to enter partial content of a domain name, and the system adds a suffix to the domain name for resolution. **NOTE** A maximum of 10 DNS domain names can be configured.

Copyright © Huawei Technologies Co., Ltd.

- Deleting DNS configuration
  a. Log in to the web platform and choose **IP Service** > **DNS** > **DNS**.
  b. Select the check box of a DNS server IP address in the **DNS Server Configuration List(IPv4 Address)** or **DNS Server Configuration List(IPv6 Address)** area, and click **Delete**.
  c. In the dialog box that is displayed, click **OK**.
  d. Select the check box of a domain name suffix in the **Domain Name Suffix List** area, and click **Delete**.
  e. In the dialog box that is displayed, click **OK**.
- Refreshing the DNS dynamic cache list
  a. Log in to the web platform and choose **IP Service** > **DNS** > **DNS**. The DNS page is displayed.
  b. On the **DNS Dynamic Cache List** toolbar, click **Refresh** to refresh the DNS dynamic cache list.

----End

2.14.3.2 DDNS

Context

When the enterprise server's IP address changes, the DNS server needs to dynamically update the mapping between its domain name and IP address. Internet users often use domain names to access servers such as HTTP and FTP servers that provide application layer services. When the server IP address changes, the server functions as the DDNS client and sends a DDNS request for updating the mapping between its domain name and IP address to the DDNS server. Other users can still access the server using the domain name when the server IP address changes.

After a DDNS client is configured, the router can notify the DDNS server of the latest public IP address of the server. The DDNS server then updates the mapping between domain name and IP address on the DNS server so that the DNS server can resolve the server's domain name into a correct IP address.

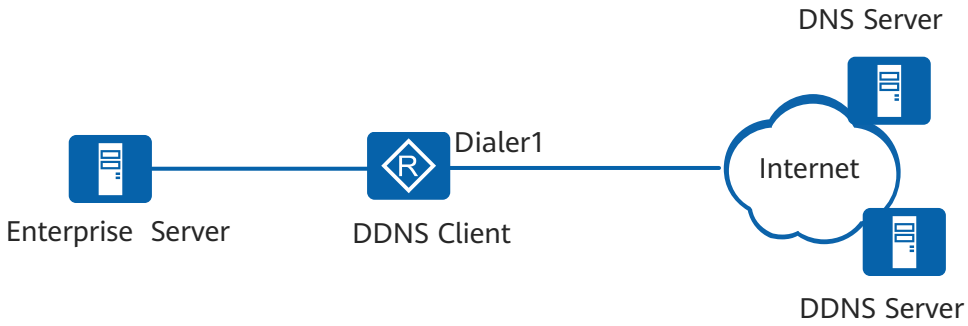
NOTE

If the public IP address of the enterprise's server does not frequently change, you do not need to configure DDNS.

Figure 2-118 shows the DDNS networking. The enterprise's server accesses the Internet through PPPoE on Dialer1 of the router and provides services using the IP address of Dialer1. The DDNS client is configured on the router. The DDNS client notifies the DDNS server when the public IP address of the server changes, and the DDNS server notifies the DNS server. Therefore, the DNS server maintains the latest mappings between domain names and IP addresses.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-118 Typical networking of DDNS



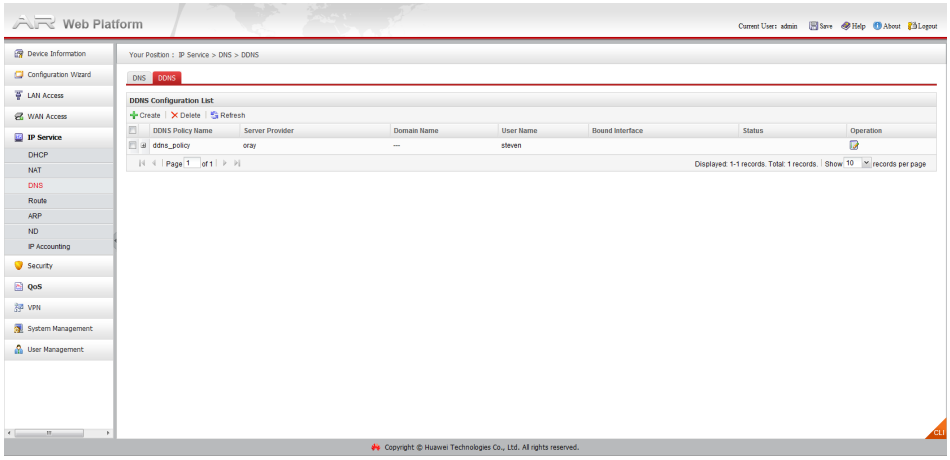
Pre-configuration Tasks

- You have obtained an account and domain name on the DDNS service provider's website.
- On the **DNS** page, you have configured the IP address of the DNS server on the public network.

Procedure

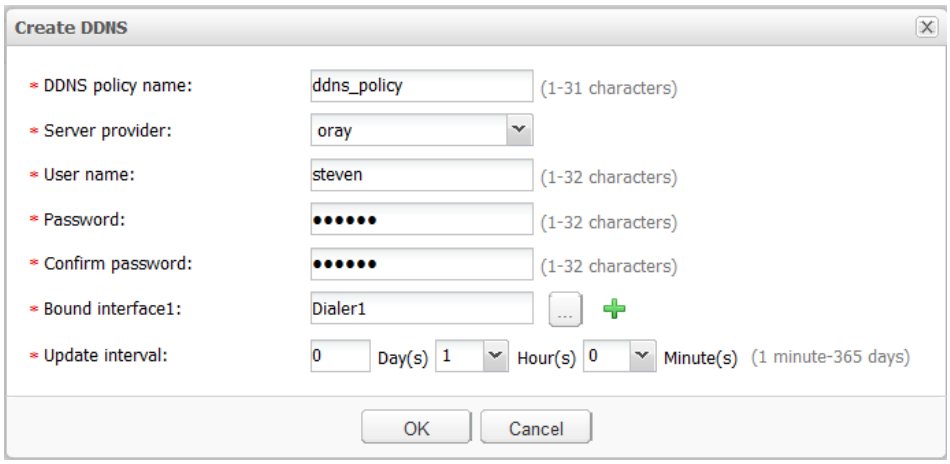
- Creating a DDNS client
  a. Log in to the web platform and choose **IP Service** > **DNS** > **DDNS**, as shown in **Figure 2-118**.

  Figure 2-119 DDNS page

  b. Click **Create** in the **DDNS Configuration List** area and set DDNS parameters. **Table 2-102** describes the parameters.

 Copyright © Huawei Technologies Co., Ltd.



c. Click **OK**.

Table 2-102 DDNS parameters

Parameter	Description
DDNS policy name	Name of a DDNS policy.
Server provider	Domain name of the DDNS service provider (DDNS server). The options are as follows: • User-defined: a user-defined DDNS server. • oray: a DDNS server with the domain name as www.oray.cn. • dyndns: a DDNS server with the domain name as www.dyndns.org. • 3322: a DDNS server with the domain name as www.3322.org. **NOTE** When the device functions as the DDNS client and communicates with Siemens DDNS server, the device needs to encrypt packets using SSL. The DDNS policy needs to be bound to the SSL policy only when the device functions as the DDNS client and communicates with Siemens DDNS server.
User name	User name obtained from the DDNS service provider. You must register an account including the user name and password with the DDNS server provider's website.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Password	Password used by the DDNS client to access the DDNS server. You must register an account including the user name and password with the DDNS server provider's website.
Confirm password	Re-enter the password that is set.
Bound interface	DDNS client interface bound to a DDNS policy. Ensure that the route between the DDNS client and the DDNS server is reachable. Click  to add an interface. You can bind a maximum of eight interfaces to a DDNS policy.
Update interval	Interval for sending DDNS Update requests.

- Modifying a DDNS client
  a. Log in to the web platform and choose **IP Service** > **DNS** > **DDNS**.
  b. Select a DDNS policy in the **DDNS Configuration List** area, and click  .
  c. In the **Modify DDNS** dialog box that is displayed, modify parameters listed in **Table 2-102**. The parameter **DDNS policy name** cannot be modified.
  d. Click **OK**.
- Deleting a DDNS client
  a. Log in to the web platform and choose **IP Service** > **DNS** > **DDNS**.
  b. Select the check box of a DDNS policy and click **Delete**.
  c. In the dialog box that is displayed, click **OK**.

----End

2.14.4 Route

2.14.4.1 Viewing the Routing Table

You can check the routing table to view routing information about the device, which helps you manage the networks.

Context

A routing table contains the following key data for each IP packet.

 Copyright © Huawei Technologies Co., Ltd.

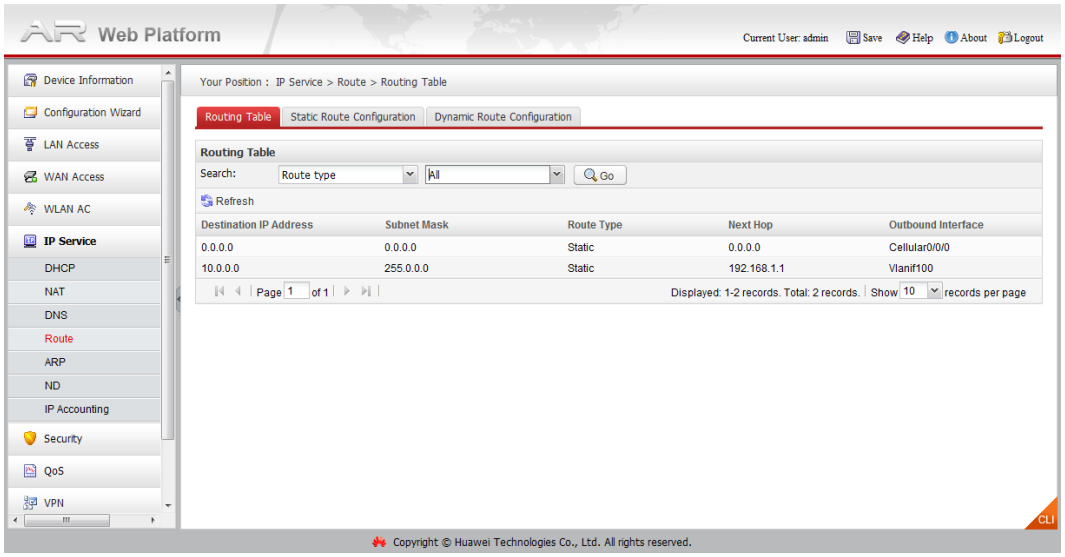
Item	Description
Destination IP Address	Indicates the destination IP address or network of IP packets.
Subnet Mask	Indicates the subnet mask length of the destination address. The network mask is used with the destination address to identify the address of the network segment where the destination host or router resides.
Route Type	Indicates the routing protocol.
Next Hop	Indicates the next hop address of the route, that is, next-hop device to which packets are forwarded.
Outbound Interface	Indicates the outbound interface of the route, that is, local router interface from which packets are forwarded.

Procedure

Step 1 Choose **IP Service** > **Route** > **Routing Table**.

Step 2 View all the routing tables or specified routes based on the route type or destination IP address/subnet mask.

Figure 2-120 View the routing table



----End

2.14.4.2 Configuring Static Routes

This section describes how to configure static routes.

Context

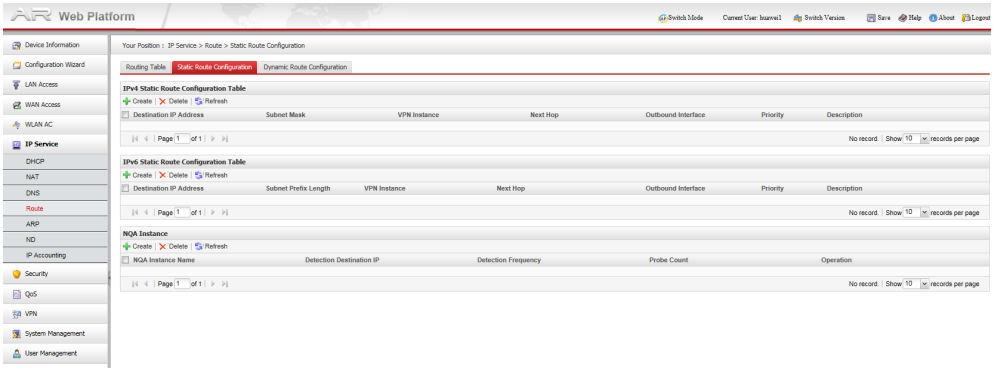
Generally, static routes are applicable to the networks with simple structures. Configuring static routes facilitates route management.

Procedure

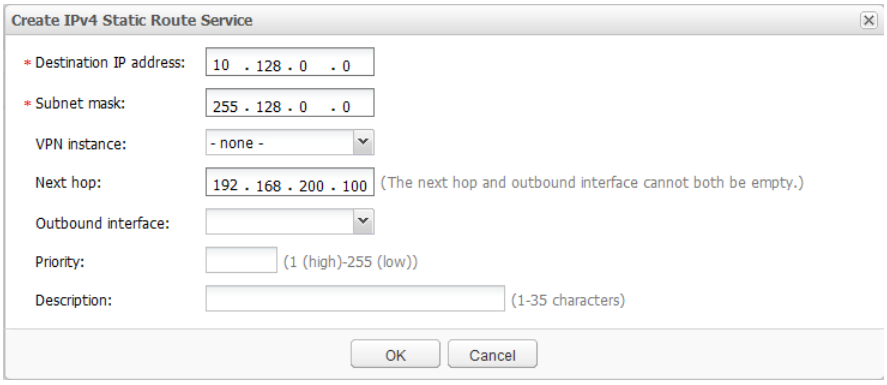
Step 1 Create a static route.

1. Choose **IP Service** > **Route** > **Static Route Configuration**.

Figure 2-121 Static route configuration



2. Configure IPv4 or IPv6 static routes or NQA instance as required.
   - Configure an IPv4 static route.
     i. In **IPv4 Static Route Configuration Table**, click **Create**. The **Create IPv4 Static Route Service** page is displayed.



     ii. Set parameters and click **OK**.

Table 2-103 IPv4 static route configuration

Item	Description
Destination IP address	Set the destination IP address of a IPv4 static route.

 Copyright © Huawei Technologies Co., Ltd.

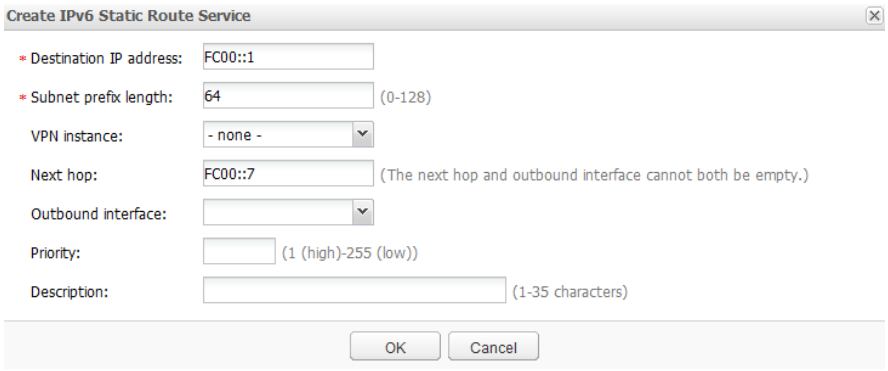
Item	Description
Subnet mask	Set the subnet mask of a IPv4 static route in dotted decimal notation.
VPN instance	Specifies the name of a VPN instance. If the VPN instance name is specified, a static route searches the routing table of the VPN instance for an outbound interface according to **Next hop**.
Next hop	Set the next-hop IP address of a IPv4 static route.
Outbound interface	Configure an outbound interface for a IPv4 static route.
Priority	Set the priority of a IPv4 static route. A smaller value indicates a higher priority.
Description	Set the description information of a IPv4 static route.

NOTE

- When both the destination IP address and mask are 0.0.0.0, the configured route is the default route.
- If the outbound interface is not a point-to-point interface, the next hop address must be specified.

– Configure an IPv6 static route.

i. In **IPv6 Static Route Configuration Table**, click **Create**. The **Create IPv6 Static Route Service** page is displayed.



ii. Set parameters and click **OK**.

Table 2-104 IPv6 static route configuration

Item	Description
Destination IP address	Set the destination IPv6 address of a IPv6 static route.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Subnet prefix length	Set the prefix length of the destination IPv6 address.
VPN instance	Specifies the name of a VPN instance. If the VPN instance name is specified, a static route searches the routing table of the VPN instance for an outbound interface according to **Next Hop**.
Next hop	Set the next-hop IPv6 address of a IPv6 static route.
Outbound interface	Configure an outbound interface for a IPv6 static route.
Priority	Set the priority of a IPv6 static route. A smaller value indicates a higher priority.
Description	Set the description information of a IPv6 static route.

NOTE

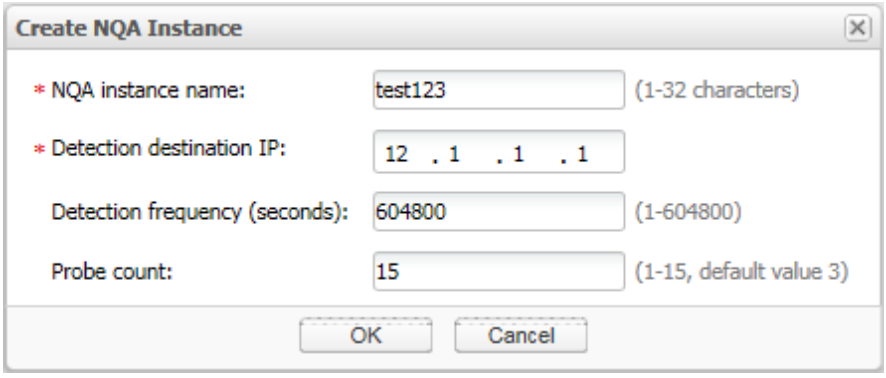
- When both the destination IPv6 address and subnet prefix length are ::, the configured route is the default route.
- If the outbound interface is not a point-to-point interface, the next hop address must be specified.

– Configure an NQA test instance.

NOTE

Only V200R010C10 and later versions support association between NQA and static routes.

i. In the **NQA Instance** area, click **Create**. The **Create NQA Instance** dialog box is displayed.



ii. Set parameters and click **OK**.

Copyright © Huawei Technologies Co., Ltd.

Table 2-105 Configuring an NQA test instance

Parameter	Description
NQA instance name	Specifies the name of an NQA test instance.
Detection destination IP	Specifies the destination address in an NQA test instance. **NOTE** There must be reachable routes between the device and this destination address.
Detection frequency (seconds)	Specifies the interval at which an NQA test instance is automatically performed. The value is an integer in the range from 1 to 604800, in seconds.
Probe count	Specifies the number of probes to be sent each time in an NQA test instance. The value is an integer in the range from 1 to 15. The default value is 3.

Step 2 Delete static routes.

1. In **IPv4 Static Route Configuration Table** or **IPv6 Static Route Configuration Table** or **NQA Instance**, select the static route to be deleted and click **Delete**.
2. Click **OK** in the **Information** dialog box that is displayed.

----End

2.14.4.3 Configuring Dynamic Routes

This section describes how to configure dynamic routes in the web management system.

2.14.4.3.1 Configuring OSPF

This section describes how to configure Open Shortest Path First (OSPF) in the web management system.

Context

OSPF is a link-state Interior Gateway Protocol (IGP) developed by the Internet Engineering Task Force (IETF). OSPF describes the network topology through link-state advertisements (LSAs), generates a shortest path tree (SPT) based on the network topology, and calculates shortest paths to all destinations on the network, that is, OSPF routes to all destination network segments are generated.

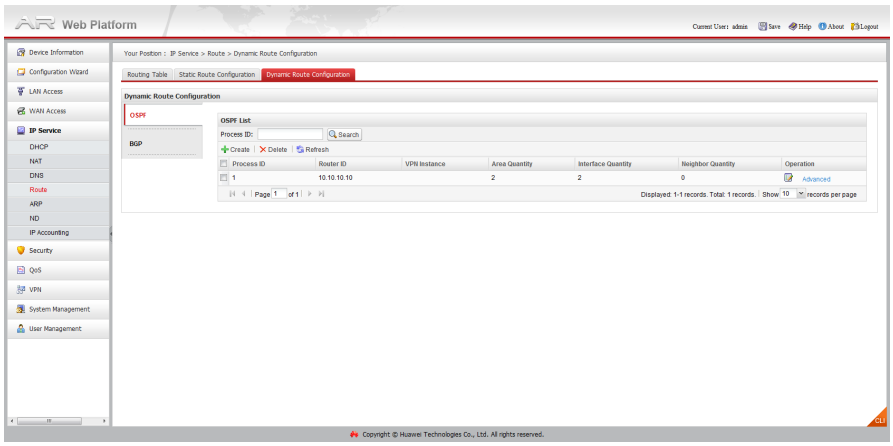
OSPF is generally used on complex networks, facilitating accurate route selection.

 Copyright © Huawei Technologies Co., Ltd.

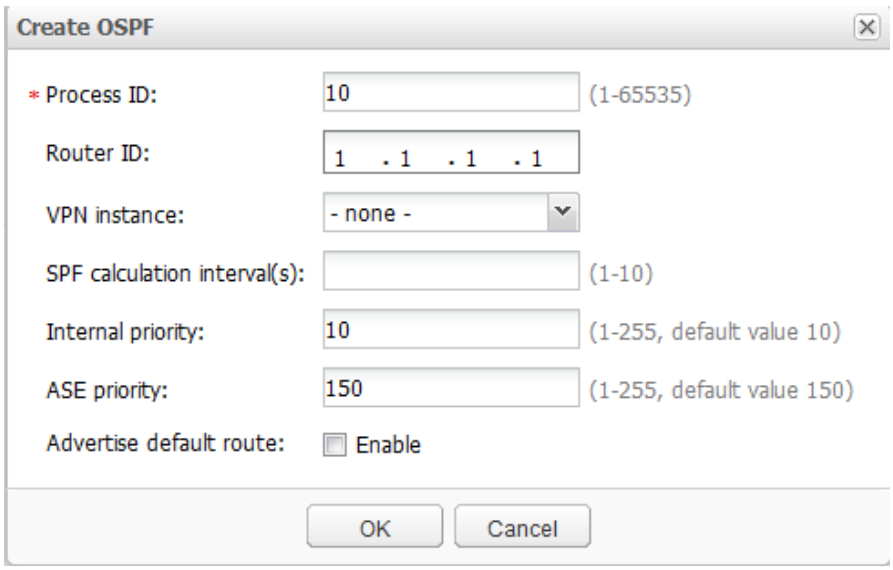
Procedure

- Creating OSPF
  a. Create an OSPF process.
     i. Choose **IP Service** > **Route** > **Dynamic Route Configuration** > **OSPF**.

Figure 2-122 OSPF List



     ii. In the **OSPF List** area, click **Create**. The **Create OSPF** dialog box is displayed.



     iii. Set parameters and click **OK**.

Table 2-106 Parameters for creating an OSPF process

Parameter	Description
Process ID	ID of an OSPF process.

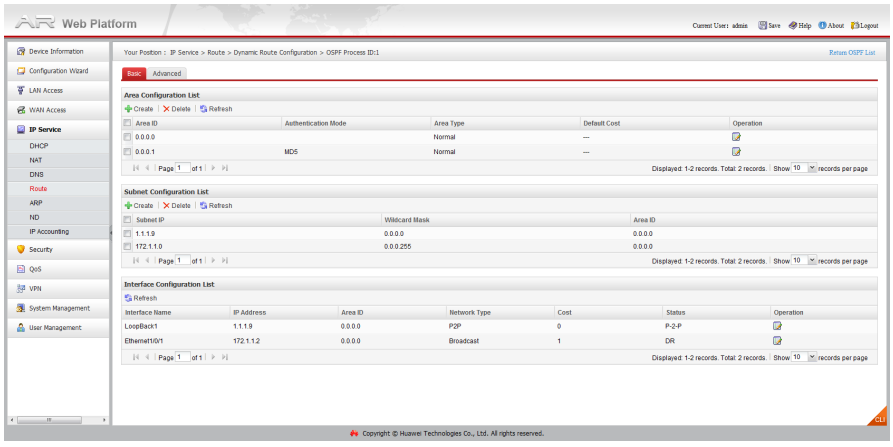
 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Router ID	ID of a router running OSPF. **NOTE** The Router ID in each OSPF process must be unique on the OSPF network. Otherwise, the OSPF neighbor relationship cannot be established and the routing information is incorrect.
VPN instance	VPN instance of the OSPF process. If no VPN instance is specified, the OSPF process belongs to the public VPN instance.
SPF calculation interval(s)	Interval of shortest path first (SPF) calculation.
Internal priority	Priority of OSPF routes except the AS-External routes. A smaller value indicates a higher priority.
ASE priority	Priority of OSPF AS-External routes. A smaller value indicates a higher priority.
Advertise default route	Default route advertised by a router. If you set this parameter to **Enable**, the router generates and advertises a default route regardless of whether an activated non-OSPF default route exists.

b. Set basic parameters of an OSPF process.

i. In the **OSPF List** area, select the new OSPF process and click **Advanced**. The **Basic** tab page is displayed.

Figure 2-123 Basic tab page

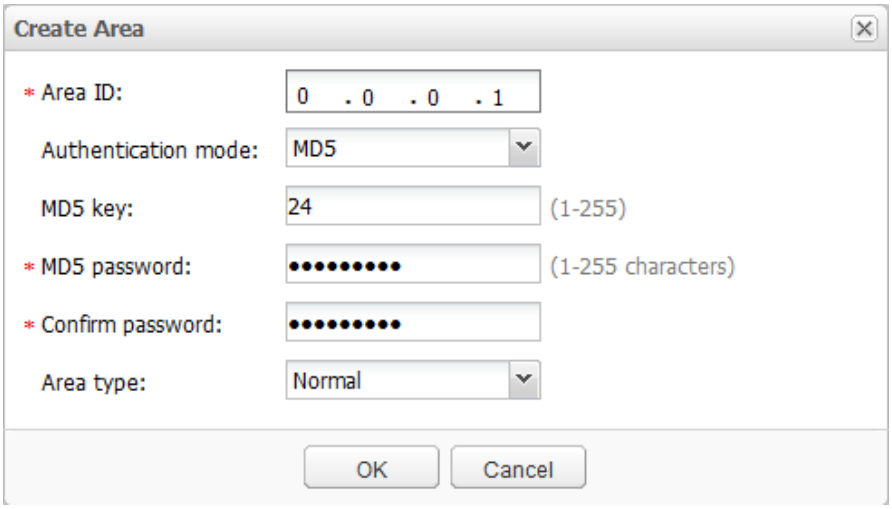


NOTE

When the **OSPF List** contains many OSPF processes, enter a value in the **Process ID** and click **Search**. Only OSPF processes related to the entered value are displayed. For example, if you enter 1 in the **Process ID**, only OSPF processes with IDs containing 1 (such as processes with IDs 1, 10, or 11) are displayed.

 Copyright © Huawei Technologies Co., Ltd.

ii. In the **Area Configuration List** area, click **Create**. The **Create Area** dialog box is displayed.



iii. Set parameters and click **OK**.

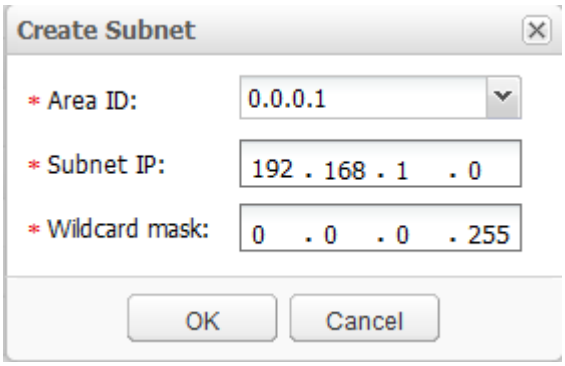
Table 2-107 Parameters for creating an area

Parameter	Description
Area ID	ID of an OSPF area.
Authentication mode	Authentication mode used in the OSPF area. • If you set this parameter to **Simple**, set a password for simple authentication and confirm it. • If you set this parameter to **MD5**, set an MD5 key value and a password, and confirm the password. • If you set this parameter to **HMAC-MD5**, set an HMAC-MD5 key value and a password, and confirm the password. **NOTE** Simple, MD5 and HMAC-MD5 authentication has potential risks.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Area type	Type of the OSPF area, stub or Not-So-Stubby Area (NSSA). • If you set the area type to **Stub**, set the default cost and determine whether the stub area is a complete stub area. • If you set the area type to **NSSA**, set the default cost and determine whether to advertise the default route to the NSSA, whether to import external routes, and whether the NSSA is a complete NSSA. **NOTE** The backbone area with the ID of 0.0.0.0 cannot be set to a stub area or NSSA. The default cost applies only to area border routers (ABRs) of the stub area or NSSA, which indicates the cost of the Type 3 default route to the stub area or NSSA.

iv. In the **Subnet Configuration List** area, click **Create**. The **Create Subnet** dialog box is displayed.



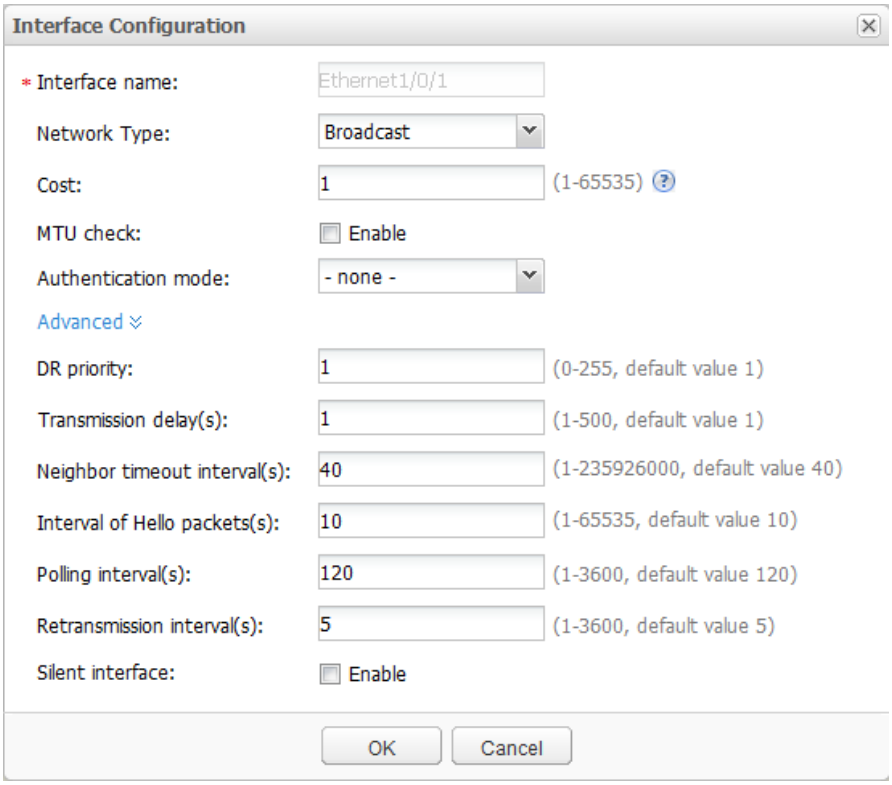
v. Set parameters and click **OK**.

Table 2-108 Parameters for creating a subnet

Parameter	Description
Area ID	ID of the area to which the interface running OSPF belongs.
Subnet IP	Network segment of the interface.
Wildcard mask	Wildcard mask of the IP address. A wildcard mask is a reverse of an IP address mask. That is, 0 in the mask becomes 1, and 1 in the mask becomes 0. In a wildcard mask, 1 indicates that the corresponding bit in the IP address is ignored, and 0 indicates that the bit must be reserved.

Copyright © Huawei Technologies Co., Ltd.

vi. In the **Interface Configuration List** area, select the interface running OSPF and click . The **Interface Configuration** dialog box is displayed.



vii. Set parameters and click **OK**.

Table 2-109 Parameters for configuring an interface

Parameter	Description
Interface name	Name of the interface running OSPF.
Network Type	Network types of the interface. By default, the network type of an interface depends on the type of the physical interface. The network type of the Ethernet interface is **Broadcast**, the network type of the serial interface encapsulating Point-to-Point Protocol (PPP) or High-Level Data Link Control (HDLC) is **P2P**, and the network type of the ATM and frame relay (FR) interfaces is **NBMA**.
Cost	Cost of the interface running OSPF. By default, OSPF automatically calculates the cost of the interface according to the interface bandwidth.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
MTU check	Maximum transmission unit (MTU) that the interface fills in a data description (DD) packet to be enabled. **NOTICE** After MTU check is enabled, the router automatically restarts the OSPF process. Exercise caution when enabling MTU check.
Authentication mode	Authentication mode on the interface. • If you set this parameter to **Simple**, set a password for simple authentication and confirm it. • If you set this parameter to **MD5**, set an MD5 key value and a password, and confirm the password. • If you set this parameter to **HMAC-MD5**, set an HMAC-MD5 key value and a password, and confirm the password. **NOTE** The parameter **Authentication-Null** indicates an authentication mode, which does not indicate that no authentication is configured.
DR priority	Priority of the interface that participates in the DR election. This parameter is valid only when the network type is **Broadcast** or **NBMA**.
Transmission delay(s)	Delay of transmitting LSAs on the interface.
Neighbor timeout interval(s)	OSPF neighbor timeout period. **NOTE** Setting the neighbor timeout period to a value greater than 20s is recommended. If the neighbor timeout period is smaller than 20s, sessions between OSPF neighbors may be closed. The neighbor timeout period of the interface running OSPF must be longer than the interval for sending Hello packets, and the values **Neighbor timeout interval(s)** on the routers in the same network segment must be the same. By default, the neighbor timeout period is four times the interval for sending Hello packets.
Interval of Hello packets(s)	Interval for sending Hello packets on the interface.
Polling interval(s)	Interval for sending poll Hello packets on the interface. **NOTE** This parameter is valid only when the network type of the interface is **NBMA**.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Retransmission interval(s)	Interval for retransmitting LSAs on the interface.
Silent interface	Whether to forbid the interface from receiving and sending OSPF packets.

NOTE

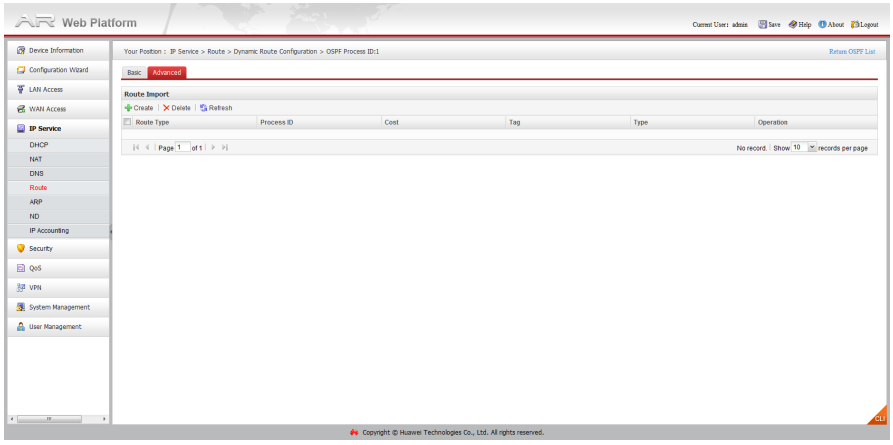
To set parameters such as **DR priority**, **Transmission delay(s)**, **Neighbor timeout interval(s)**, **Interval of Hello packets(s)**, **Polling interval(s)**, **Retransmission interval(s)**, and **Silent interface**, click **Advanced** in the **Interface Configuration** dialog box.

c. Set advanced parameters of an OSPF process.

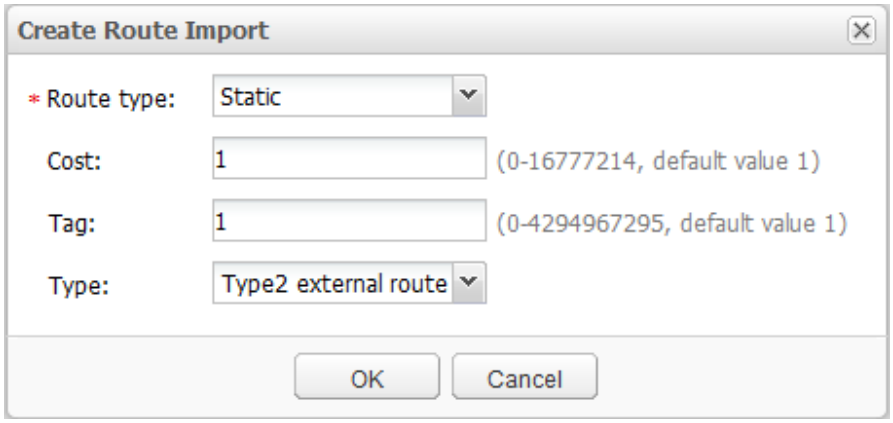
i. In the **OSPF List** area, select the new OSPF process and click **Advanced**. The **Basic** tab page is displayed.

ii. Click the **Advanced** tab. The **Advanced** tab page is displayed.

Figure 2-124 Advanced tab page



iii. In the **Route Import** area, click **Create**. The **Create Route Import** dialog box is displayed.



iv. Set parameters and click **OK**.

Copyright © Huawei Technologies Co., Ltd.

Table 2-110 Parameters for importing routes

Parameter	Description
Route type	Routing protocol of an imported external route. When this parameter is set to **OSPF**, **RIP**, or **ISIS**, you need to configure a corresponding process ID.
Cost	Cost of an imported external route.
Tag	Tag value of an imported external route.
Type	Type of an imported external route, which includes: • Type1 external routes have high reliability. The OSPF protocol considers that the cost of a Type1 external route equals the cost of an AS internal route. Cost of a Type1 external route = Cost of the route from the router to the corresponding ASBR + Cost of the route from the ASBR to the destination • Type 2 external routes have low reliability. The OSPF protocol considers that the cost of the route from the ASBR to the destination outside an AS is much greater than the cost of any internal route to an ASBR. Cost of a Type2 external route = Cost of the route from an ASBR to the destination outside an AS

- Modifying OSPF
  - Modify OSPF parameters.
    i. In the **OSPF List** area, select an OSPF process and click  . The **Modify OSPF** dialog box is displayed.
    ii. Modify the parameters and click **OK**.
  - Modify basic parameters of an OSPF process.
    i. In the **OSPF List** area, select an OSPF process and click **Advanced**. The **Basic** tab page is displayed.
    ii. In the **Area Configuration List** area, select an area and click  . The **Modify Area** dialog box is displayed.
    iii. Modify the parameters and click **OK**.
    iv. In the **Interface Configuration List** area, select an area and click  . The **Interface Configuration** dialog box is displayed.
    v. Modify the parameters and click **OK**.
  - Modify advanced parameters of an OSPF process.
    i. In the **OSPF List** area, select an OSPF process and click **Advanced**. The **Basic** tab page is displayed.

Copyright © Huawei Technologies Co., Ltd.

ii. Click the **Advanced** tab. The **Advanced** tab page is displayed.

iii. Select an imported external route and click  . The **Modify Route Import** dialog box is displayed.

iv. Modify the parameters and click **OK**.

- Deleting OSPF
  - Delete an OSPF process.
    i. In the **OSPF List** area, select an OSPF process and click **Delete**.
    ii. In the **Information** dialog box that is displayed, click **OK**.
  - Delete basic parameter settings of an OSPF process.
    i. In the **OSPF List** area, select an OSPF process and click **Advanced**. The **Basic** tab page is displayed.
    ii. In the **Subnet Configuration List** area, select a network segment and click **Delete**.
    iii. In the **Information** dialog box that is displayed, click **OK**.
    iv. In the **Area Configuration List** area, select an area and click **Delete**.
    v. In the **Information** dialog box that is displayed, click **OK**.
  - Delete advanced parameter settings of an OSPF process.
    i. In the **OSPF List** area, select an OSPF process and click **Advanced**. The **Basic** tab page is displayed.
    ii. Click the **Advanced** tab. The **Advanced** tab page is displayed.
    iii. In the **Route Import** area, select an imported external route and click **Delete**.
    iv. In the **Information** dialog box that is displayed, click **OK**.

----End

2.14.4.3.2 Configuring BGP

This section describes how to configure Border Gateway Protocol (BGP) in the web management system.

Context

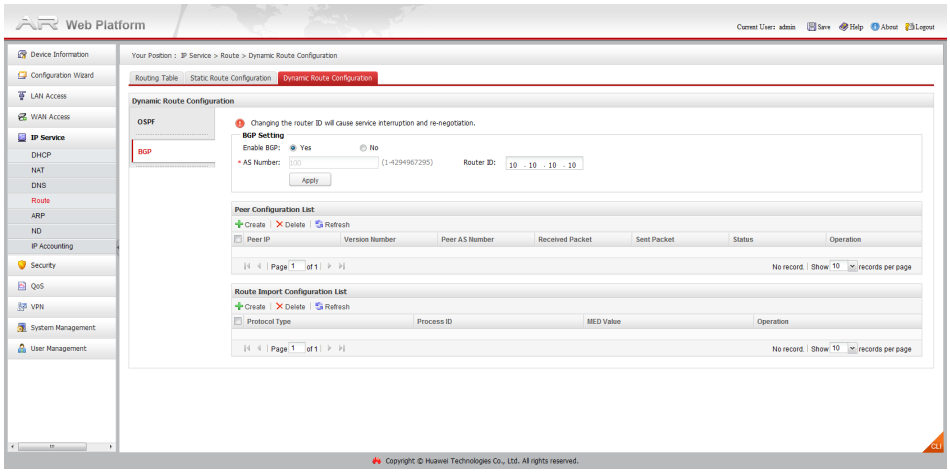
BGP is a dynamic routing protocol that allows for reachable routes between autonomous systems (ASs) and selects the optimal routes. BGP is usually used on large and complex networks.

Procedure

- Enabling BGP
  a. Choose **IP Service** > **Route** > **Dynamic Route Configuration** > **BGP**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-125 BGP configuration



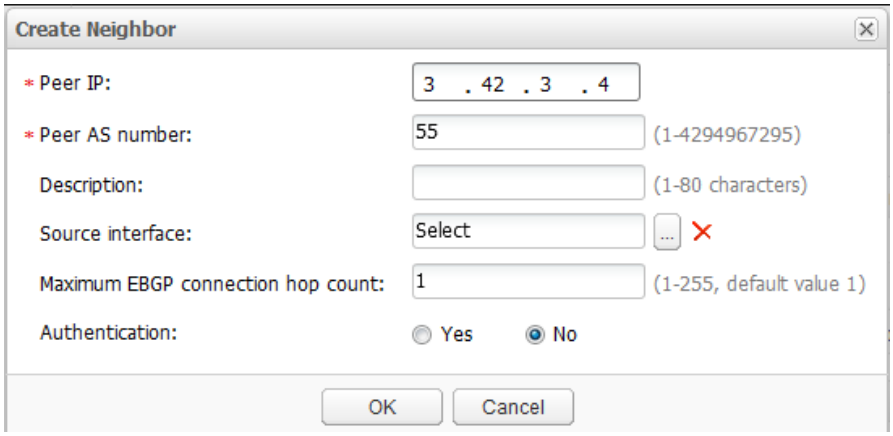
b. In the **BGP Setting** area, set parameters and click **Apply**.

Table 2-111 Parameters for configuring BGP

Parameter	Description
Enable BGP	Whether BGP is enabled. The value can be **Yes** or **No**.
AS number	Number of the local AS.
Router ID	ID of a router running BGP. **NOTE** The Router ID of each router must be unique in the AS. Otherwise, the BGP peer relationship cannot be established and the routing information is incorrect.

c. Create a BGP peer.

i. In the **Peer Configuration List** area, click **Create**. The **Create Neighbor** dialog box is displayed.



ii. Set parameters and click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

Table 2-112 Parameters for creating a BGP peer

Parameter	Description
Peer IP	IP address of the BGP peer.
Peer AS number	AS number of the BGP peer.
Description	Description of the BGP peer.
Source Interface	Source interface sending BGP packets.
Maximum EBGP connection hop count	Maximum number of hops for External Border Gateway Protocol (EBGP) peer neighbors. **NOTE** When AS numbers on the local device and its peer are different, they set up an EBGP peer relationship. If the maximum number of hops is 1, a device cannot establish an EBGP connection with a peer on an indirectly-connected network.
Authentication	Whether to authenticate BGP peers. When you set this parameter to **Yes**, set a password and confirm it.

d. Configure BGP to import external routes.

i. In the **Route Import Configuration List** area, click **Create**. The **Create Route Import** dialog box is displayed.

ii. Set parameters and click **OK**.

Table 2-113 Parameters for importing routes

Parameter	Description
Protocol type	Routing protocol of an imported external route. When this parameter is set to **OSPF**, **RIP**, or **ISIS**, you need to configure a corresponding process ID.
MED value	Multi-Exit Discrimination (MED) value of an imported external route.

- Modifying BGP
  - Modify BGP parameters.

NOTICE

Changing the Router ID will result in service interruption and renegotiation. Exercise caution when changing the router ID.

Copyright © Huawei Technologies Co., Ltd.

In the **BGP Setting** area, set a new router ID and click **Apply**.

- Modify BGP peer parameters.
  i. In the **Peer Configuration List** area, select a BGP peer and click . The **Modify Neighbor** dialog box is displayed.
  ii. Modify the parameters and click **OK**.
- Modify BGP parameters for importing external routes.
  i. In the **Route Import Configuration List** area, select an imported external route and click . The **Modify Route Import** dialog box is displayed.
  ii. Modify the parameters and click **OK**.

- Deleting BGP
  - Disable BGP.

    NOTICE

    Disabling BGP will delete all BGP configurations. Exercise caution when disabling BGP.

    In the **BGP Setting** area, set **Enable BGP** to **No** and click **Apply**.
  - Delete a BGP peer.
    i. In the **Peer Configuration List** area, select a BGP peer and click **Delete**.
    ii. In the **Information** dialog box that is displayed, click **OK**.
  - Delete external routes imported by BGP.
    i. In the **Route Import Configuration List** area, select an imported external route and click **Delete**.
    ii. In the **Information** dialog box that is displayed, click **OK**.

----End

2.14.5 ARP

Context

The Address Resolution Protocol (ARP) maps IP addresses to MAC addresses.

ARP entries include dynamic and static ARP entries according to the mode in which they are generated.

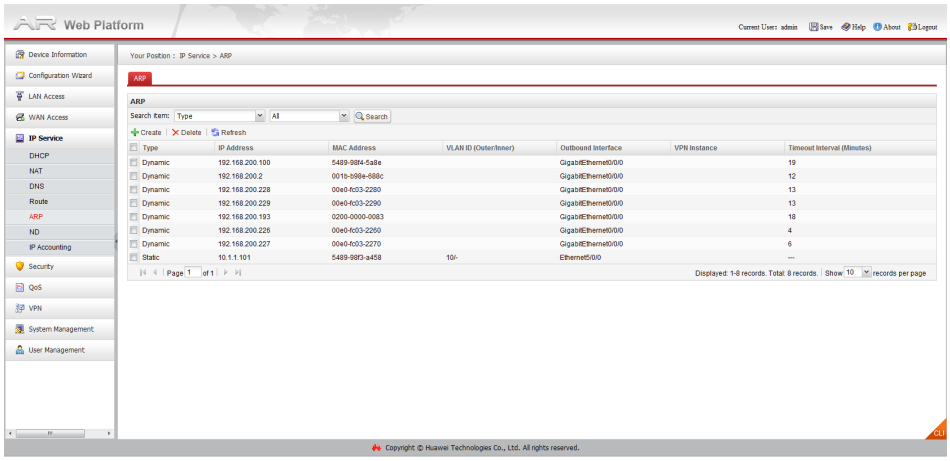
- Dynamic ARP entries: are automatically generated and maintained through ARP. Each dynamic ARP entry has a lifetime. Dynamic ARP entries can be updated or overwritten by static ARP entries.
- Static ARP entries: are configured manually to record mappings between IP addresses and MAC addresses. Mappings cannot be changed dynamically.

 Copyright © Huawei Technologies Co., Ltd.

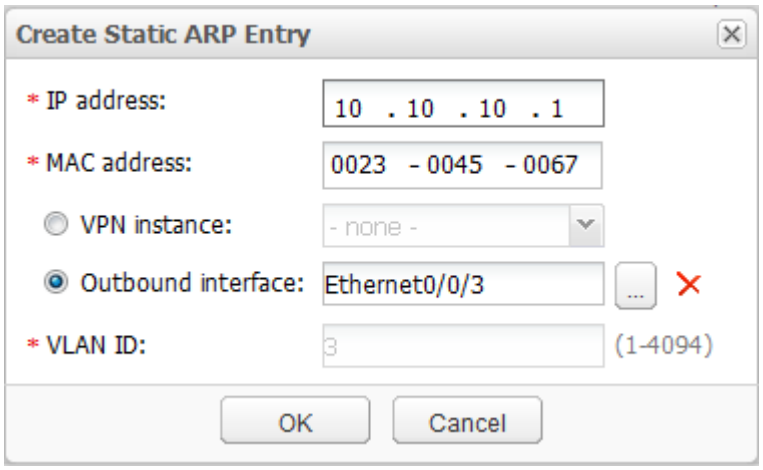
Procedure

- Create a static ARP entry.
  a. Log in to the web NMS and choose **IP Service** > **ARP**. The **ARP** page is displayed, as shown in **Figure 2-126**.

  Figure 2-126 ARP page

  b. Click **Create**. In the **Create Static ARP Entry** dialog box that is displayed, select or enter each parameter to configure a static ARP entry. For description of the parameters, see **Table 2-114**.

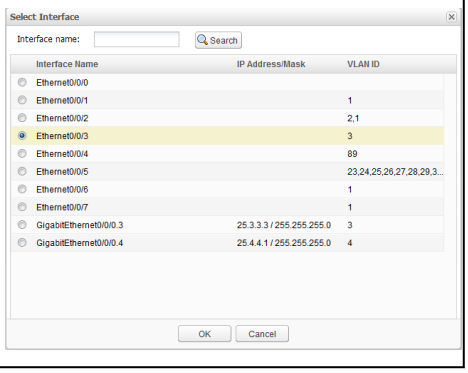
  

  c. Click **OK** to complete the configuration.

  Table 2-114 Parameter description of creating static ARP entries

Parameter	Description
IP address	IP address of a static ARP entry.
MAC address	MAC address of a static ARP entry.
VLAN ID	ID of the VLAN to which a static ARP entry belongs.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
VPN instance	Name of a VPN instance. **NOTE** Create a VPN instance before specifying this parameter. For details, see **2.17.4 VPN Instance**.
Outbound interface	Outbound interface of a static ARP packet. Click . In **Select Interface**, use either of the following methods to select an outbound interface: • Enter keywords in the **Interface name** text box and click **Search**. Select an interface in the **Interface Name** list and click **OK**. • Select an interface in the **Interface Name** list and click **OK**. **NOTE** If the selected outbound interface is added to **VLAN**, and the VLANIF interface corresponding to the VLAN is assigned an IP address, the specified IP address in a static ARP entry should be on the same network segment as the IP address of the VLANIF interface, and the ID of the VLAN to which a static ARP entry belongs should be the same as the ID of the VLAN to which the outbound interface belongs. 

- Delete an ARP entry.
  a. Log in to the web NMS and choose **IP Service** > **ARP**. The **ARP** page is displayed. You can view the configured static ARP entries or the generated dynamic ARP entries.
  b. Select the check box next to the ARP entry to be deleted and click **Delete**.
  c. In the dialog box that is displayed, click **OK** to delete the APR entry.

Copyright © Huawei Technologies Co., Ltd.

- Update ARP entries.
  a. Log in to the web NMS and choose **IP Service** > **ARP**. The **ARP** page is displayed. You can view the configured static ARP entries or the generated dynamic ARP entries.
  b. Click **Refresh** to update ARP entries.
- Search for an ARP entry.
  a. Log in to the web NMS and choose **IP Service** > **ARP**. The **ARP** page is displayed. You can view the configured static ARP entries or the generated dynamic ARP entries.
  b. Select search items in the two drop-down lists next to **Search item**.
     - Select **Type** in the first drop-down list, select **Static** or **Dynamic** in the second drop-down list, and click **Search** to search for an ARP entry according to the type.
     - Select **IP address** in the first drop-down list, enter the corresponding IP address in the second drop-down list, and click **Search** to search for an ARP entry according to the IP address.
     - Select **MAC address** in the first drop-down list, enter the corresponding MAC address in the second drop-down list, and click **Search** to search for an ARP entry according to the MAC address.
     - Select **VPN instance** in the first drop-down list, enter the corresponding VPN instance name in the second drop-down list, and click **Search** to search for an ARP entry according to the VPN instance name.

     For description of the parameters, see **Table 2-115**.

Table 2-115 Parameter description of ARP entries

Parameter	Description
Type	Type of an ARP entry. • Static: a manually configured ARP entry. • Dynamic: an automatically generated ARP entry.
IP Address	IP address of an ARP entry.
MAC Address	MAC address of an ARP entry.
VLAN ID(Outer/Inner)	ID of the inner VLAN or outer VLAN that an ARP entry belongs to. **NOTE** Currently, a static ARP entry can only be configured with an outer VLAN ID.
Outbound Interface	Outbound interface of an ARP entry.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
VPN Instance	VPN instance to which an ARP entry belongs.
Timeout Interval(Minutes)	Remaining lifetime of an ARP entry, in minutes. This parameter is valid only for dynamic ARP entries. Each dynamic ARP entry has a lifetime. When the remaining lifetime of an ARP entry is 0, the ARP entry will be deleted.

----End

2.14.6 ND

Context

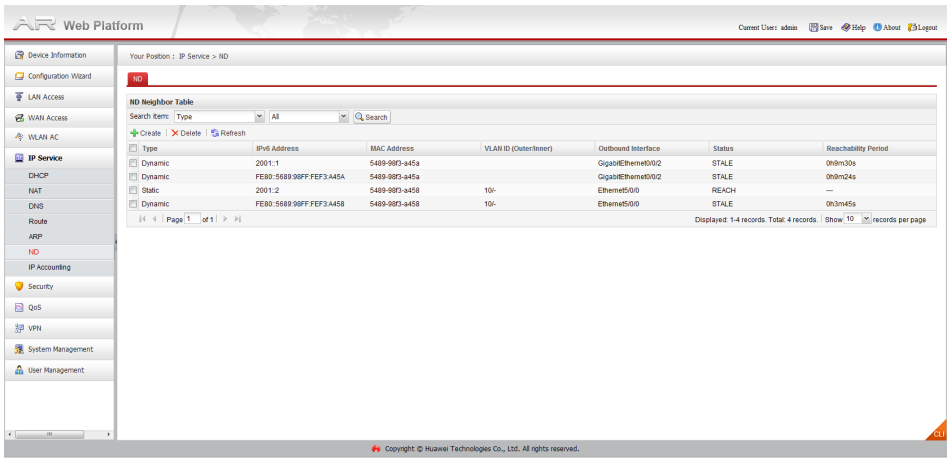
The Neighbor Discovery Protocol (NDP) is one important IPv6 basic protocol. NDP replaces the Address Resolution Protocol (ARP) of IPv4 and the Internet Control Message Protocol (ICMP) Router Discovery Protocol. NDP uses ICMPv6 packets to implement address resolution, neighbor tracking, duplicate address detection (DAD), router discovery, and redirection.

A host must obtain the MAC address of a target host to communicate with the target host. A device can dynamically generate neighbor entries using ND or be configured with static neighbor entries.

Procedure

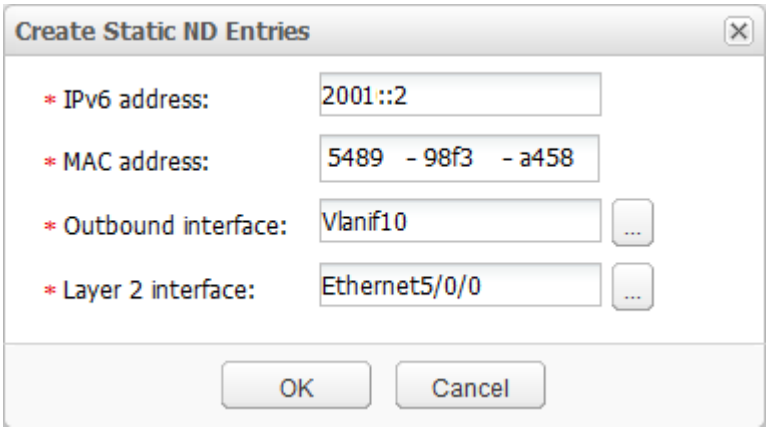
- Creating a static ND entry
  a. Log in to the web platform and choose **IP Service** > **ND**. The **ND** page is displayed, as shown in **Figure 2-127**.

Figure 2-127 ND page



 Copyright © Huawei Technologies Co., Ltd.

b. Click **Create**. In the **Create Static ND Entries** dialog box that is displayed, set parameters to configure static ND entries. **Table 2-116** describes the parameters.



c. Click **OK**. Static ND entries are configured.

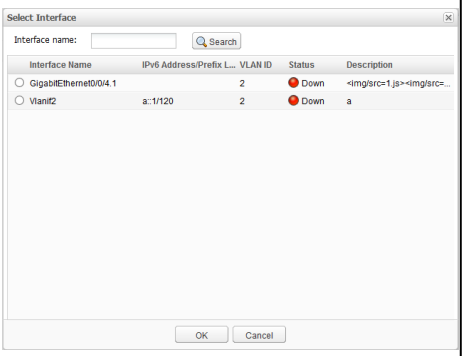
NOTE

A maximum of 700 static ND entries can be configured in web mode.

Table 2-116 Parameters for creating static ND entries

Parameter	Description
IPv6 address	IPv6 address of a neighbor.
MAC address	MAC address of a neighbor.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Outbound interface	Outbound interface in the static ND entry. Click … and use either of the following methods to select an outbound interface in the **Select Interface** dialog box: • Enter a keyword in the **Interface name** text box, and click **Search**. Select an interface in the **Interface Name** area, and click **OK**. • Select an interface in the **Interface Name** area, and click **OK**. 
VLAN ID	This parameter is displayed when an Ethernet subinterface is configured as the outbound interface and a VLAN ID is configured. For details about how to configure an Ethernet subinterface, see **2.12.1 Ethernet Interface**.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Layer 2 interface	When a VLANIF interface is configured as the outbound interface, you must specify a physical interface for the outbound interface. Click  and use either of the following methods to select a Layer 2 interface in the **Select Interface** dialog box: • Enter a keyword in the **Interface name** text box, and click **Search**. Select an interface in the **Interface Name** area, and click **OK**. • Select an interface in the **Interface Name** area, and click **OK**. **NOTE** Only Layer 2 interfaces added to VLANs are displayed in the interface list. For details about how to add interfaces to VLANs, see **2.11.1.2 VLAN Interface**.

- Deleting an ND entry
  a. Log in to the web platform and choose **IP Service** > **ND**. The configured static ND entries or dynamically generated ND entries are displayed on the **ND** page.
  b. Select the check box of the required ND entry and click **Delete**.
  c. In the dialog box that is displayed, click **OK**.
- Updating an ND entry
  a. Log in to the web platform and choose **IP Service** > **ND**. The configured static ND entries or dynamically generated ND entries are displayed on the **ND** page.
  b. Click **Refresh**. ND entries are updated.
- Querying an ND entry
  a. Log in to the web platform and choose **IP Service** > **ND**. The configured static ND entries or dynamically generated ND entries are displayed on the **ND** page.
  b. Set **Search item** as follows:
     - Select **Type** from the first drop-down list box and **Static** or **Dynamic** from the second drop-down list box, and click **Search**. ND entries meeting the search criteria are displayed.
     - Select **IPv6 address** from the Search item drop-down list box and enter an IPv6 address in the text box, enter an IPv6 address, and click **Search**. ND entries meeting the search criteria are displayed.

Copyright © Huawei Technologies Co., Ltd.

- Select **MAC address** from the Search item drop-down list box and enter an IPv6 address in the text box, enter a MAC address, and click **Search**. ND entries meeting the search criteria are displayed.

Table 2-117 describes the parameters.

Table 2-117 ND entry parameters

Parameter	Description
Type	Type of ND entries. • **Static**: manually created ND entries • **Dynamic**: automatically generated ND entries
IPv6 Address	IPv6 address in ND entries.
MAC Address	MAC address in ND entries.
VLAN ID(Outer/Inner)	Inner and outer VLAN IDs of the outbound interface.
Outbound Interface	Outbound interface in ND entries.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Status	ND entry status: • INCMP: indicates that the neighbor is unreachable. In this state, the device is parsing the neighbor's MAC address. If the device parses the address successfully, the device sets the ND entry status to REACH. • REACH: indicates that the neighbor is reachable. In this state, the neighbor is reachable within a specified period of time (30s by default). If the ND entry is not used when the specified period of time is reached, the ND entry enters the STALE state. • STALE: indicates that whether the neighbor is reachable is unknown. The neighbor is not used within the specified period of time (30s by default). The device detects whether the neighbor is reachable only when the device wants to send packets to the neighbor. • DELAY: indicates that whether the neighbor is reachable is unknown. In this state, the device has sent neighbor solicitation (NS) packets to the neighbor. If the device does not receive any response within the specified period of time, the device sets the ND entry status to PROBE. If the device receives a response, the device sets the ND entry status to REACH. • PROBE: indicates that whether the neighbor is reachable is unknown. In this state, the device sends NS packets to the neighbor at a specified interval to detect whether the neighbor is reachable. If the device receives a response within the specified period of time, the device sets the ND entry status to REACH. If the device does

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
	not receive any response within the specified period of time, the device sets the ND entry status to INCMP.
Reachability Period	Period of time after an ND entry is generated. This parameter is valid only for dynamic ND entries.

----End

2.14.7 IP Accounting

2.14.7.1 Viewing IP Traffic Statistics

Context

This section describes how to view statistics about IP packets.

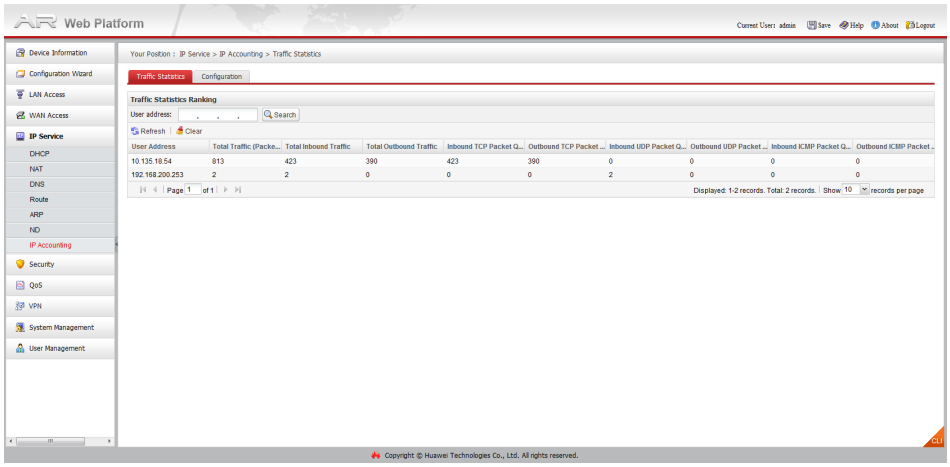
You can collect statistics about IP packets in the common method or based on the packet priority. The web management system supports only the common method to collect statistics about incoming and outgoing IP packets.

The web management system does not allow you to configure rules for collecting IP traffic statistics.

Procedure

- Querying and ranking IP traffic statistics
  a. Choose **IP Service** > **IP Accounting** > **Traffic Statistics**, as shown in Figure 2-128.

Figure 2-128 Viewing IP Traffic Statistics page



 Copyright © Huawei Technologies Co., Ltd.

b. Click **Refresh**.

The current IP traffic statistics are displayed in **Traffic Statistics Ranking**. For details about parameters in **Traffic Statistics Ranking**, see **Table 2-118**.

Table 2-118 Parameter description

Parameter	Description
User Address	User's IP address.
Total Traffic (Packets)	Total number of collected packets.
Total Inbound Traffic	Total number of collected incoming packets.
Total Outbound Traffic	Total number of collected outgoing packets.
Inbound TCP Packet Quantity	Total number of collected incoming TCP packets.
Outbound TCP Packet Quantity	Total number of collected outgoing TCP packets.
Inbound UDP Packet Quantity	Total number of collected incoming UDP packets.
Outbound UDP Packet Quantity	Total number of collected outgoing UDP packets.
Inbound ICMP Packet Quantity	Total number of collected incoming ICMP packets.
Outbound ICMP Packet Quantity	Total number of collected outgoing ICMP packets.

c. Click **Total Traffic (Packets)** on the top of the list, and rank the traffic statistics in ascending or descending order.

- Querying IP traffic statistics based on the IP address
  a. Choose **IP Service** > **IP Accounting** > **Traffic Statistics**.
  b. Enter an IP address and click **Search**.

  Statistics about traffic on the specified IP address are displayed. For details about parameters, see **Table 2-118**.
- Deleting IP traffic statistics
  a. Choose **IP Service** > **IP Accounting** > **Traffic Statistics**.
  b. Click **Clear**. Current IP traffic statistics are deleted, and traffic statistics are collected again.

----End

2.14.7.2 Configuring IP Traffic Statistics Collection

Copyright © Huawei Technologies Co., Ltd.

Context

This section describes how to configure IP traffic statistics collection on Layer 3 interfaces.

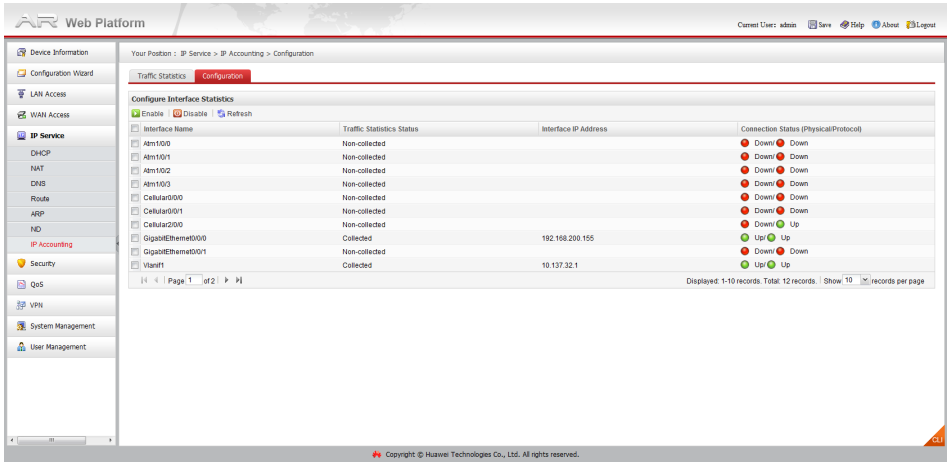
NOTE

IP traffic statistics must be collected on LAN-side interfaces; otherwise, correctness of the statistics is affected.

Procedure

- Querying IP traffic statistics on an interface
  a. Choose **IP Service** > **IP Accounting** > **Configuration**.
  b. Click **Refresh**.as shown in **Figure 2-129**.

Figure 2-129 Configuring IP Traffic Statistics Collection page



IP traffic statistics collection status on a Layer 3 interface is displayed in **Configure Interface Statistics**. For details about parameters in **Configure Interface Statistics**, see **Table 2-119**.

Table 2-119 Parameter description

Parameter	Description
Interface Name	Interface's type and number.
Traffic Statistics Status	Statistics collection status. The value can be **Collected** or **Non-collected**.
Interface IP Address	Interface's IP address.
Connection Status (Physical/ Protocol)	Status of physical and protocol connections. The value can be **Up** or **Down**.

- Enabling the IP traffic statistics collection function on an interface

 Copyright © Huawei Technologies Co., Ltd.

a. Choose **IP Service** > **IP Accounting** > **Configuration**.
b. Select an interface in **Configure Interface Statistics**.

NOTE

You can select multiple interfaces to enable the function in batches.

c. Click **Enable**.
Statistics collection status of all selected interfaces is **Collected**.

- Disabling the IP traffic statistics collection function on an interface
  a. Choose **IP Service** > **IP Accounting** > **Configuration**.
  b. Select an interface in **Configure Interface Statistics**.

NOTE

You can select multiple interfaces to disable the function in batches.

  c. Click **Disable**.
  Statistics collection status of all selected interfaces is **Non-collected**.

----End

2.15 Security

2.15.1 ACL

2.15.1.1 Basic ACL Setting

Context

After basic ACL rules are configured, routers classify IPv4 or IPv6 packets based on information such as source IP addresses, and time ranges in the packets.

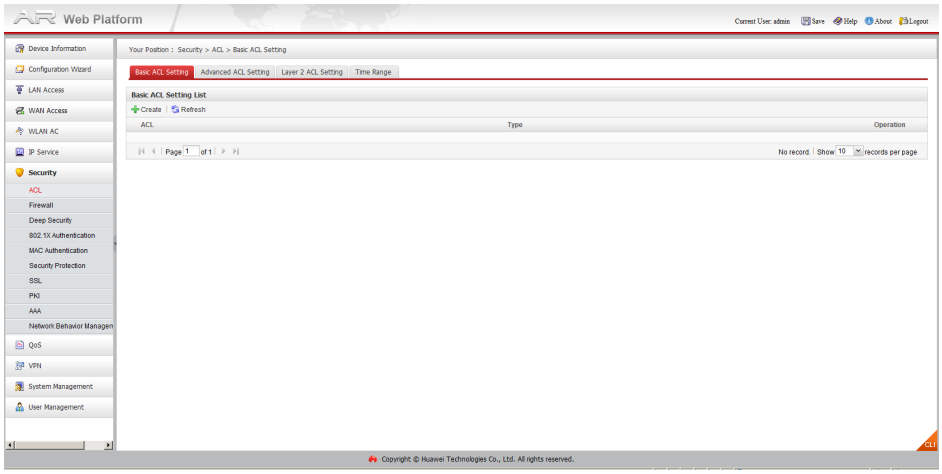
Procedure

- Creating a basic ACL rule
  a. Access the **Basic ACL Setting** tab page.

  Log in to the web platform and choose **Security** > **ACL** > **Basic ACL Setting**, as shown in **Figure 2-130**.

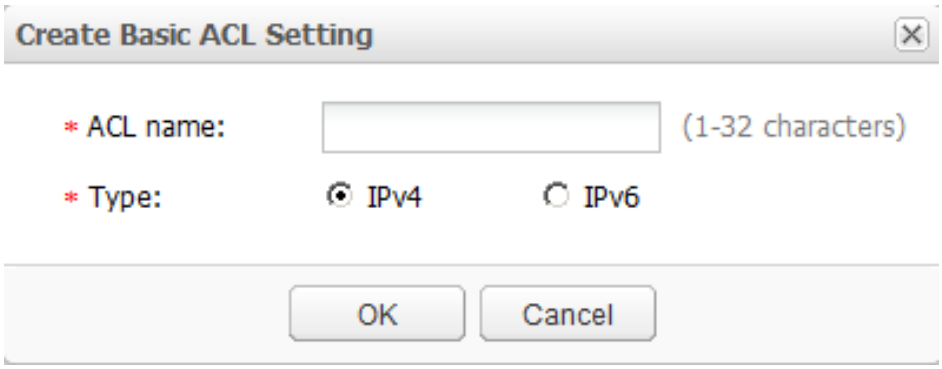
 Copyright © Huawei Technologies Co., Ltd.

Figure 2-130 Basic ACL Setting



b. Click **Create** in the **Basic ACL Setting List** area. Enter an ACL rule name in the **Create Basic ACL Setting** dialog box, as shown in **Figure 2-131**. To create a basic ACL4 rule, click **IPv4**; to create a basic ACL6 rule, click **IPv6**.

Figure 2-131 Create Basic ACL Setting



NOTE

The value of **ACL name** is a string of 1 to 32 characters without spaces or question marks (?) and must start with a letter.

c. Click **OK**.

d. Click **Add rules** and set parameters to add basic ACL rules in the ACL rule entry, as shown in **Figure 2-132**. **Table 2-120** describes the parameters.

Figure 2-132 Add rules



e. Click . To delete a basic ACL rule, click .

 Copyright © Huawei Technologies Co., Ltd.

Table 2-120 Basic ACL rule parameters

Parameter	Description
Rule number	ACL rule number. **NOTE** If you do not specify a rule number, the system allocates a number for the rule. The rule number cannot be changed.
Action	Whether to permit or deny packets.
Source IP/Prefix Length(Wildcard)	Source IP address of packets to be matched by the ACL rule. • When the ACL type is IPv4, enter the source IP address and wildcard both in dotted decimal notation. • When the ACL type is IPv6, enter the source IP address and prefix length. The source IP address is in colon hexadecimal notation. The prefix length is an integer that ranges from 1 to 128.
Time Range	Name of a time range during which ACL rules take effect. **NOTE** The time range name is displayed on the **Time Range** tab page. If this parameter is not specified, ACL rules are always valid.

- Deleting a basic ACL rule
  a. Access the **Basic ACL Setting** tab page.

     Log in to the web platform and choose **Security** > **ACL** > **Basic ACL Setting**.

  b. Click  next to a basic ACL rule.
  c. In the dialog box that is displayed, click **OK**.

----End

2.15.1.2 Advanced ACL Setting

Context

After advanced ACL rules are configured, routers classify IPv4 or IPv6 packets based on information such as source IP addresses, destination IP addresses, source port numbers, destination port numbers, protocols, priorities, and time ranges in the packets.

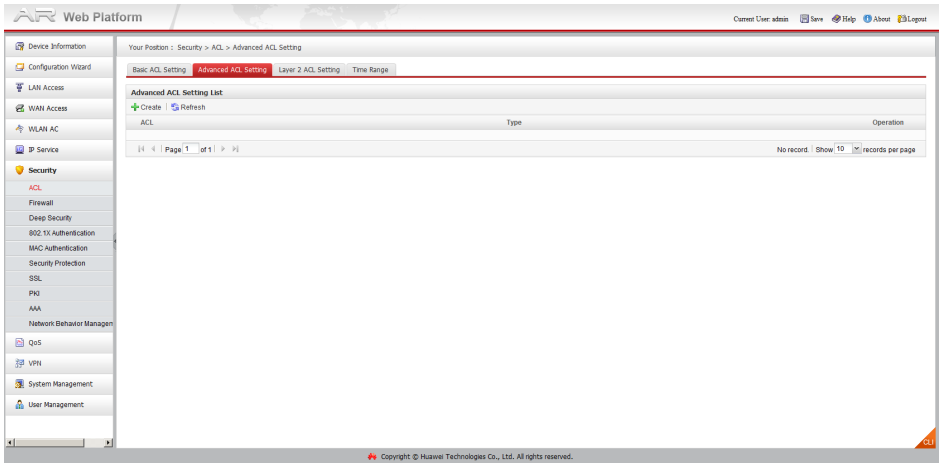
Copyright © Huawei Technologies Co., Ltd.

Procedure

- Creating an advanced ACL rule
  a. Access the **Advanced ACL Setting** tab page.

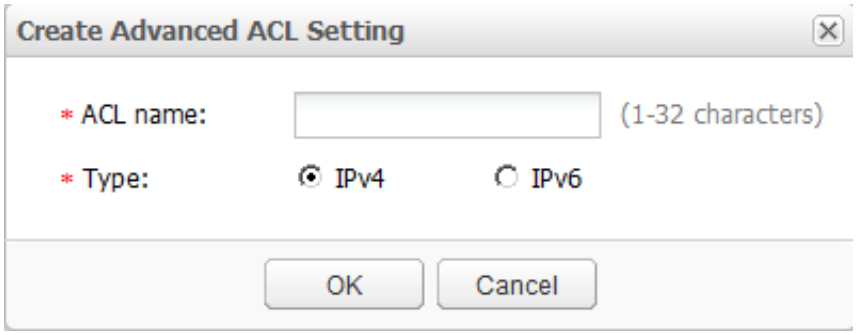
     Log in to the web platform and choose **Security** > **ACL** > **Advanced ACL Setting**, as shown in **Figure 2-133**.

     Figure 2-133 Advanced ACL Setting

  b. Click **Create** in the **Advanced ACL Setting List** area. Enter an ACL rule name in the **Create Advanced ACL Setting** dialog box, as shown in **Figure 2-134**. To create an advanced ACL4 rule, click **IPv4**; to create an advanced ACL6 rule, click **IPv6**.

     Figure 2-134 Create Advanced ACL Setting

     NOTE

     The value of **ACL name** is a string of 1 to 32 characters without spaces or question marks (?) and must start with a letter.

  c. Click **OK**.

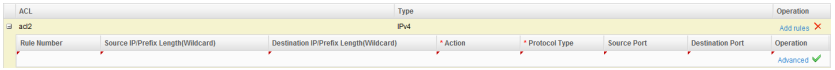
  d. Click **Add rules** to add advanced ACL rules. You can add advanced ACL rules in either of the following ways:

 Copyright © Huawei Technologies Co., Ltd.

- In the ACL rule list

  1) Set parameters in the ACL rule list, as shown in **Figure 2-135**. **Table 2-121** describes the parameters.

  Figure 2-135 ACL rule list

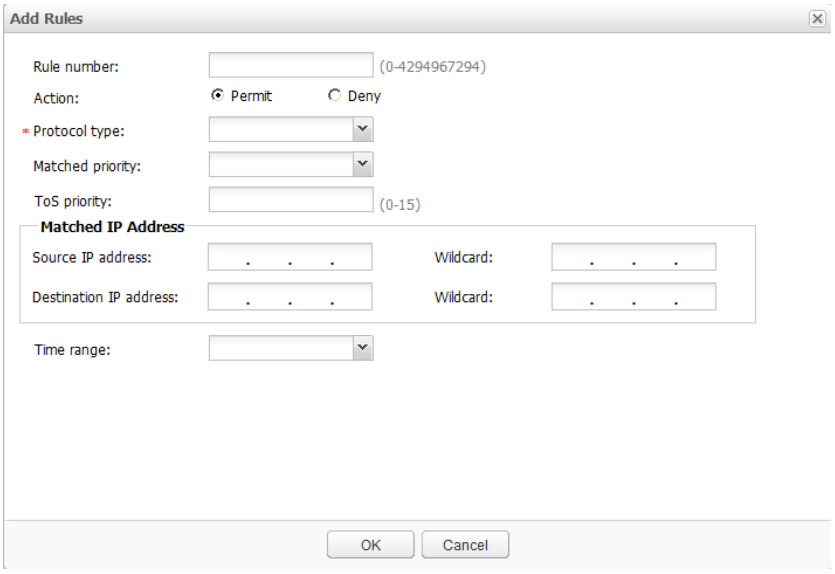
  

  2) Click . To delete an advanced ACL rule, click .

- In the **Add Rules** dialog box

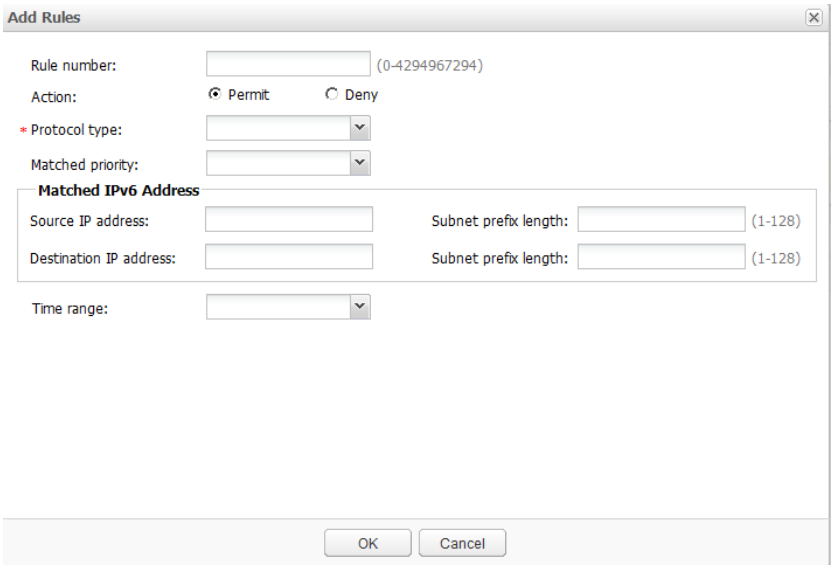
  1) Click **Advanced** and set parameters in the **Add Rules** dialog box, as shown in **Figure 2-136** and **Figure 2-137**. **Table 2-121** describes the parameters.

  Figure 2-136 Add IPv4 ACL Rules

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-137 Add IPv6 ACL Rules



2) Click **OK**. To delete an advanced ACL rule, click  .

Table 2-121 Advanced ACL rule parameters

Parameter	Description
Rule number	ACL rule number. **NOTE** If you do not specify a rule number, the system allocates a number for the rule. The rule number cannot be changed.
Action	Whether to permit or deny packets.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Protocol Type	Advanced ACL4 rules support the following protocols: • ICMP (1) When this parameter is set to **ICMP(1)**, set **ICMP parameter** whose value is in the format of ICMP message type/message code. • IGMP (2) • GRE (47) • IP • IPINIP (4) • OSPF (89) • TCP (6) • UDP (17) • User-defined type Advanced ACL6 rules support the following protocols: • GRE (47) • ICMPV6 (58) When this parameter is set to **ICMPV6(58)**, set **ICMP parameter** whose value is in the format of ICMP message type/message code. • IPV6 • OSPF (89) • TCP (6) • UDP (17) • User-defined type **NOTE** The value of **User-defined type** is valid only in the **Add Rules** dialog box. When this parameter is set to **User-defined type**, enter a protocol number in the **User-defined parameter** text box.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Matched priority	An advanced ACL4 rule can match the following types of priorities: ● Differentiated services code point (DSCP) priority The ACL rule filters packets based on the DSCP value. Enter a DSCP priority in the text box displayed after you select **DSCP priority**. ● IP priority The ACL rule filters packets based on the IP priority field. Enter an IP priority in the text box displayed after you select **IP priority**. An advanced ACL6 rule can match the following types of priorities: ● Differentiated services code point (DSCP) priority The ACL rule filters packets based on the DSCP value. Enter a DSCP priority in the text box displayed after you select **DSCP priority**. ● IP priority The ACL rule filters packets based on the IP priority field. Enter an IP priority in the text box displayed after you select **IP priority**. ● Type of service (ToS) priority The ACL rule filters packets based on the ToS field. Enter a ToS priority in the text box displayed after you select **ToS priority**.
ToS priority	ToS priority based on which an advanced ACL4 rule filters packets.
Source IP/Prefix Length(Wildcard)	Source IP address of packets to be matched by the ACL rule. ● When the ACL type is IPv4, enter the source IP address and wildcard both in dotted decimal notation. ● When the ACL type is IPv6, enter the source IP address and prefix length. The source IP address is in colon hexadecimal notation. The prefix length is an integer that ranges from 1 to 128.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Wildcard	Wildcard matching the source or destination IP address of packets to be matched by the ACL rule. The wildcard is in dotted decimal notation. Set this parameter only when the ACL type is IPv4.
Subnet prefix length	Length of the subnet prefix matching the source or destination IP address of packets to be matched by the ACL rule. The value is an integer that ranges from 1 to 128. Set this parameter only when the ACL type is IPv6.
Source IP address	Source IP address of packets to be matched by the ACL rule. ● When the ACL type is IPv4, enter the source IP address in dotted decimal notation. ● When the ACL type is IPv6, enter the source IP address in colon hexadecimal notation.
Destination IP/Prefix Length(Wildcard)	Destination IP address of packets to be matched by the ACL rule. ● When the ACL type is IPv4, enter the destination IP address and wildcard both in dotted decimal notation. ● When the ACL type is IPv6, enter the destination IP address and prefix length. The destination IP address is in colon hexadecimal notation. The prefix length is an integer that ranges from 1 to 128. **NOTE** If **Destination IP/Prefix Length(Wildcard)** is not specified, the packets with any destination address are matched with the ACL rule.
Destination IP address	Destination IP address of packets to be matched by the ACL rule. ● When the ACL type is IPv4, the destination IP address is in dotted decimal notation. ● When the ACL type is IPv6, the destination IP address is in colon hexadecimal notation.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Source Port	This parameter is valid only when the protocol is TCP or UDP. If this parameter is not specified, Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) packets with any source port are matched.
Destination Port	This parameter is valid only when the protocol is TCP or UDP. If this parameter is not specified, TCP or UDP packets with any destination port are matched.
Time range	Name of a time range during which ACL rules take effect. **NOTE** The time range name is displayed on the **Time Range** tab page. If this parameter is not specified, ACL rules are always valid.

- Deleting an advanced ACL rule
  a. Access the **Advanced ACL Setting** tab page.

     Log in to the web platform and choose **Security** > **ACL** > **Advanced ACL Setting**.

  b. Click  next to an advanced ACL rule.
  c. In the dialog box that is displayed, click **OK**.

----End

2.15.1.3 Layer 2 ACL Setting

Context

After layer 2 ACL rules are configured, routers classify packets based on link-layer information such as source MAC addresses, destination MAC addresses, and Layer 2 protocol type in the packets.

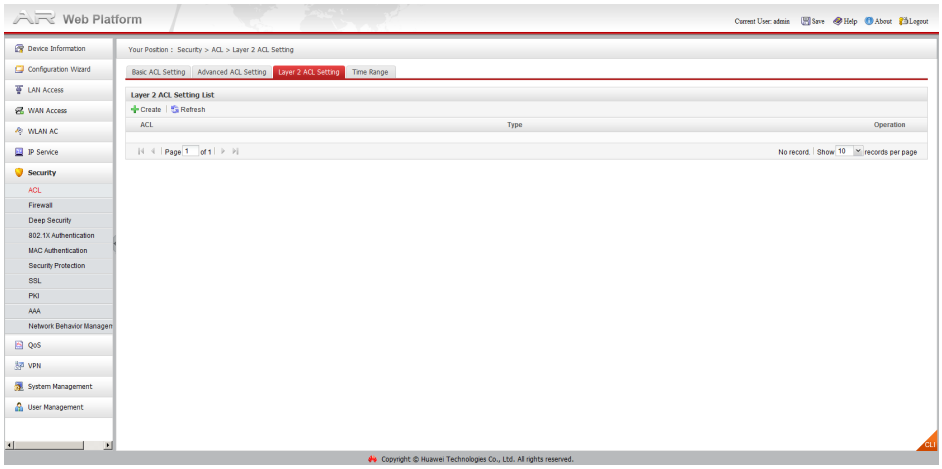
Procedure

- Creating a layer 2 ACL rule
  a. Access the **Layer 2 ACL Setting** tab page.

     Log in to the web platform and choose **Security** > **ACL** > **Layer 2 ACL Setting**, as shown in **Figure 2-138**.

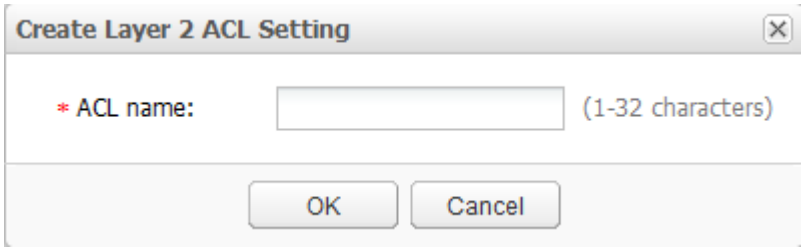
Copyright © Huawei Technologies Co., Ltd.

Figure 2-138 Layer 2 ACL Setting



b. Click **Create** in the **Layer 2 ACL Setting List** area. Enter an ACL rule name in the **Create Layer 2 ACL Setting** dialog box, as shown in **Figure 2-139**.

Figure 2-139 Create Layer 2 ACL Setting



NOTE

The value of **ACL name** is a string of 1 to 32 characters without spaces or question marks (?) and must start with a letter.

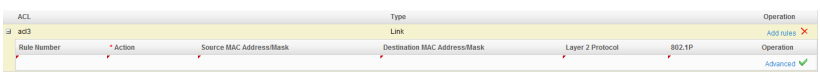
c. Click **OK**.

d. Click **Add rules** to add advanced ACL rules. You can add advanced ACL rules in either of the following ways:

- In the ACL rule list

  1) Set parameters in the ACL rule list, as shown in **Figure 2-140**. **Table 2-122** describes the parameters.

  Figure 2-140 ACL rule list

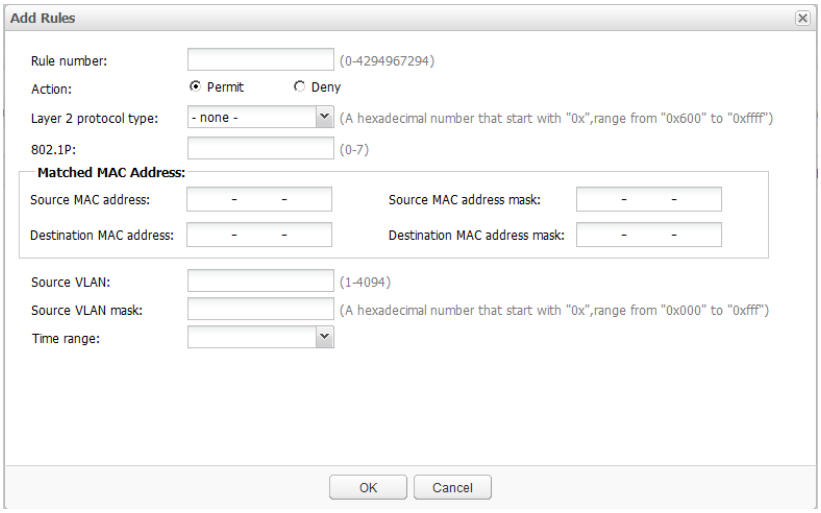
  2) Click ✓. To delete a layer 2 ACL rule, click ✗.

 Copyright © Huawei Technologies Co., Ltd.

- In the **Add Rules** dialog box

  1) Click **Advanced** and set parameters in the **Add Rules** dialog box, as shown in **Figure 2-141**. **Table 2-122** describes the parameters.

  Figure 2-141 Add Layer 2 ACL Rules



  2) Click **OK**. To delete a layer 2 ACL rule, click  .

Table 2-122 Layer 2 ACL rule parameters

Parameter	Description
Rule number	ACL rule number. **NOTE** If you do not specify a rule number, the system allocates a number for the rule. The rule number cannot be changed.
Action	Whether to permit or deny packets.
Layer 2 Protocol	Protocol type of Layer 2 ACL rules. The value can be a hexadecimal number or either of the following: • ARP • IP • MPLS • RARP
802.1P	An ACL rule that matches the 802.1p fields in outer VLAN tags of packets.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Source MAC address	Source MAC address of packets to be matched by the ACL rule. The value is in H-H-H format. H contains 1 to 4 hexadecimal digits.
Source MAC address mask	Source MAC address mask of packets to be matched by the ACL rule. The value is in H-H-H format. H contains 1 to 4 hexadecimal digits.
Destination MAC address	Destination MAC address of packets to be matched by the ACL rule. The value is in H-H-H format. H contains 1 to 4 hexadecimal digits.
Destination MAC address mask	Destination MAC address mask of packets to be matched by the ACL rule. The value is in H-H-H format. H contains 1 to 4 hexadecimal digits.
Source VLAN	An ACL rule that matches the outer VLAN IDs of packets.
Source VLAN mask	An ACL rule that matches the outer VLAN ID masks of packets.
Time range	Name of a time range during which ACL rules take effect. **NOTE** The time range name is displayed on the **Time Range** tab page. If this parameter is not specified, ACL rules are always valid.

- Deleting a layer 2 ACL rule
  a. Access the **Layer 2 ACL Setting** tab page.

     Log in to the web platform and choose **Security** > **ACL** > **Layer 2 ACL Setting**.

  b. Click  next to a layer 2 ACL rule.
  c. In the dialog box that is displayed, click **OK**.

----End

2.15.1.4 Time Range

Context

To start services or functions periodically or in a specified period of time, you can set a time range for ACL rules.

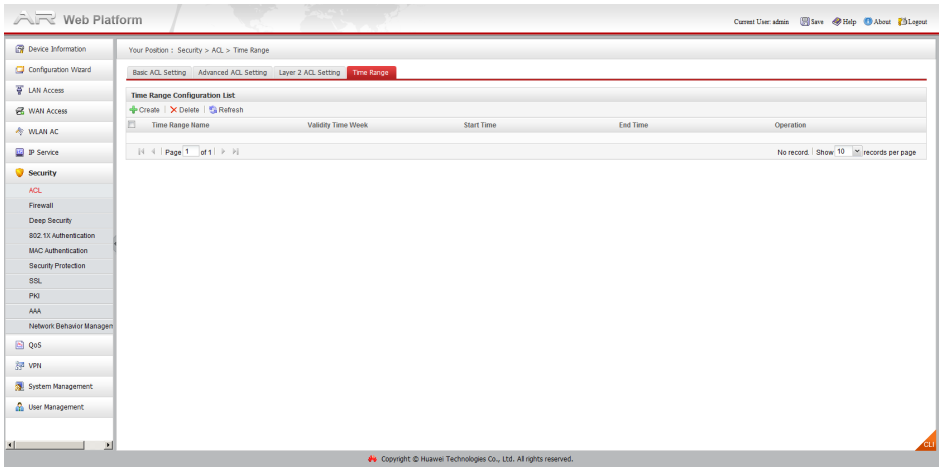
Copyright © Huawei Technologies Co., Ltd.

Procedure

- Creating a time range
  a. Access the **Time Range** tab page.

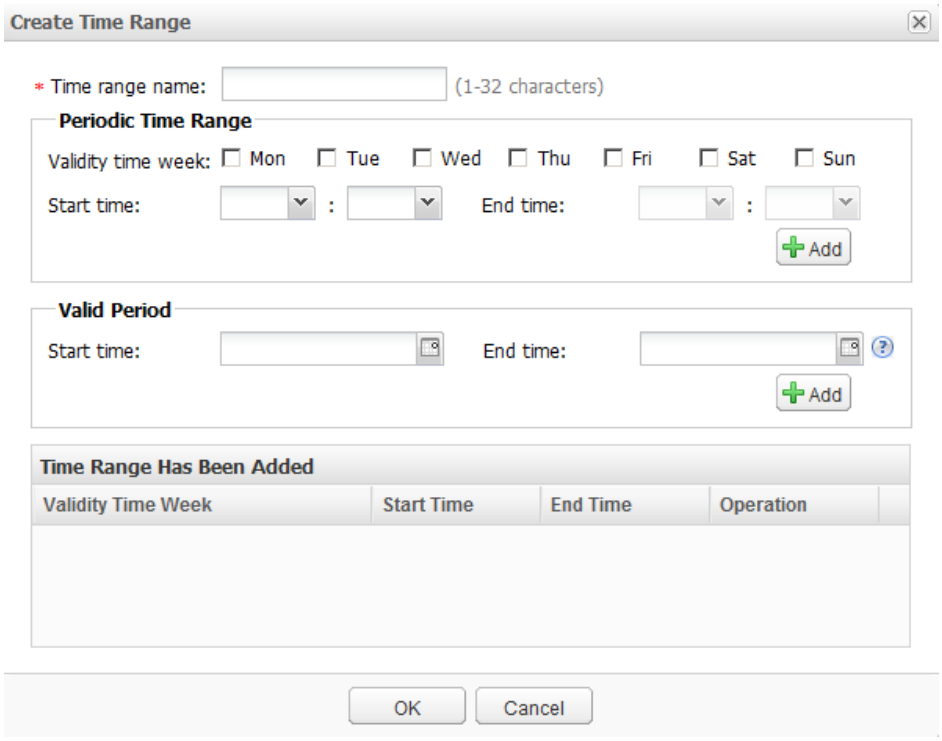
     Log in to the web platform and choose **Security** > **ACL** > **Time Range**, as shown in **Figure 2-142**.

     Figure 2-142 Time Range

  b. Click **Create** and set parameters in the **Create Time Range** dialog box, as shown in **Figure 2-143**. **Table 2-123** describes the parameters.

     Figure 2-143 Create Time Range

 Copyright © Huawei Technologies Co., Ltd.

c. Click **OK**. The created time range is displayed.

Table 2-123 Time range parameters

Parameter	Description
Time range name	Name of a time range during which ACL rules take effect.
Periodic Time Range	Period during which ACL rules take effect. The **Periodic Time Range** area has parameters **Validity time week**, **Start time**, and **End time**. Set **Validity time week** to one or more days of the week. Both the values of **Start time** and **End time** range from 00:00 to 23:59. When both the start time and end time are set to 00:00, the ACL validity period starts at 0 am and ends at 12 pm. After setting the three parameters, click **Add**. To create multiple ACL validity periods, repeat this procedure.
Valid Period	Time range during which ACL rules take effect. The **Valid Period** area has parameters **Start time** and **End time**. After setting the two parameters, click **Add**. To create multiple validity time ranges, repeat this procedure. **NOTE** If the end time is not specified, the device takes the allowed maximum value, for example, 23:59 2099/12/31.

- Modifying a time range
  a. Access the **Time Range** tab page.

     Log in to the web platform and choose **Security** > **ACL** > **Time Range**.

  b. Click  next to a time range.
  c. In the **Modify Time Range** dialog box, modify the parameters listed in **Table 2-123**. The parameters are the same as those in **Figure 2-143**. The parameter **Time range name** cannot be modified. To delete a validity time range, click  in the **Time Range Has Been Added** area.
  d. Click **OK**.
- Deleting a time range
  a. Access the **Time Range** tab page.

     Log in to the web platform and choose **Security** > **ACL** > **Time Range**.

Copyright © Huawei Technologies Co., Ltd.

b. Select the check box of a validity period and click **Delete**.
c. In the dialog box that is displayed, click **OK**.

----End

2.15.2 Firewall

2.15.2.1 Zone Policy

Context

Before configuring a firewall, you need to create related zones. You can deploy security services according to the security priorities of the zones. The device considers that data transmission within a zone is reliable; therefore, it does not enforce any security policy on intra-zone data transmission. The device verifies the data and enforces the security policies only when data flows from one zone to another.

You must configure a priority for a zone before making other configurations. The priority cannot be changed. The priorities of zones cannot be the same. A larger value indicates a higher priority.

The device automatically creates a zone named **Local**. The **Local** zone has the highest priority and cannot be deleted. In addition, the priority of this zone cannot be changed, and no interface can be added to this zone. To apply the firewall function to the control packets that need to be processed by the device, use the **Local** zone.

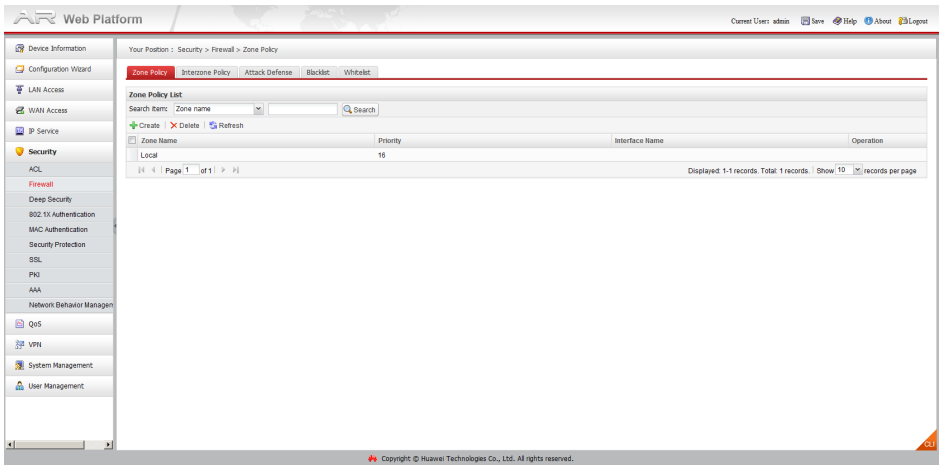
The firewall takes effect only after interfaces are added to the zone.

Procedure

- Creating a zone policy
  a. Access the **Zone Policy** tab page.

     Log in to the web platform and choose **Security** > **Firewall** > **Zone Policy**, as shown in **Figure 2-144**.

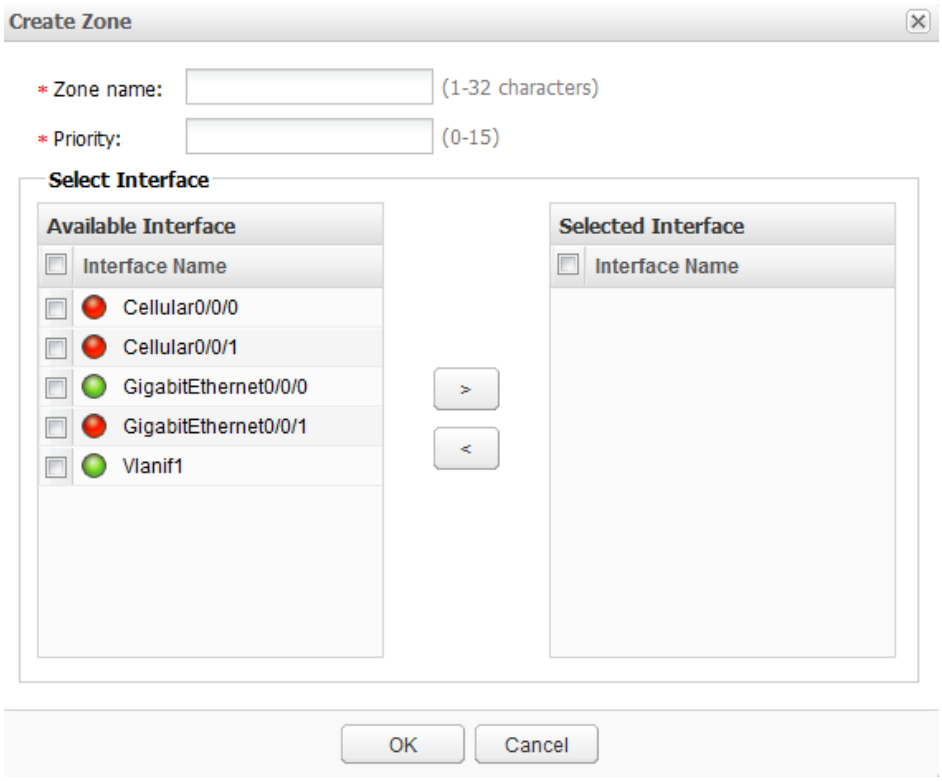
     Figure 2-144 Configuring zone policy



b. Click **Create** and set parameters in the **Create Zone** dialog box that is displayed, as shown in **Figure 2-145**. **Table 2-124** describes the parameters.

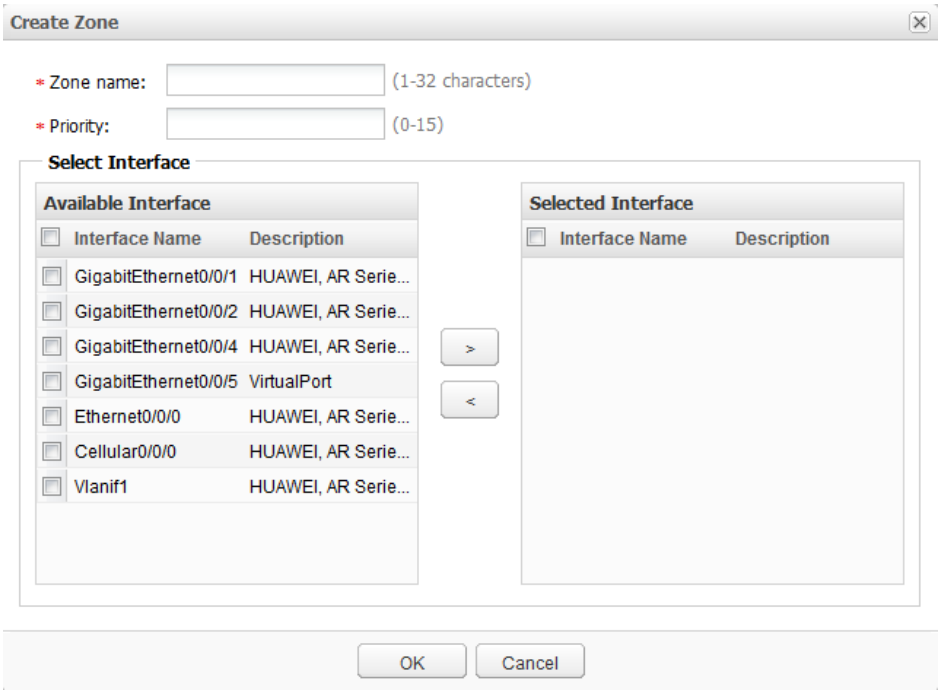
Figure 2-145 Creating a zone

In the V200R010C00 version:



In V200R010C10 and later versions:

Copyright © Huawei Technologies Co., Ltd.



c. Click **OK**. A zone policy is added to the zone policy list.

Table 2-124 Zone policy parameters

Parameter	Description
Zone name	Name of a zone. A domain named **local** exists on the device by default. The priority of this domain varies according to device model.
Priority	Priority of the zone. The priority of this domain varies according to device model.
Select Interface	Interfaces added to the zone. Interfaces in the **Available Interface** area can be added to the zone, and interface in **Selected Interface** area have been added to the zone. You can click > or < to move interfaces to one area to another.

- Modifying a zone policy
  a. Access the **Zone Policy** tab page.

     Log in to the web platform and choose **Security** > **Firewall** > **Zone Policy**.

 Copyright © Huawei Technologies Co., Ltd.

b. Click  of a zone policy.

c. In the **Modify Zone** dialog box that is displayed, modify parameters listed in **Table 2-124**. The parameters are the same as those in **Figure 2-145**.

d. Click **OK**.

- Deleting a zone policy

a. Access the **Zone Policy** tab page.

Log in to the web platform and choose **Security** > **Firewall** > **Zone Policy**.

b. Select a zone policy and click **Delete**. In the **Information** dialog box that is displayed, click **OK**.

- Search a zone policy

a. Access the **Zone Policy** tab page.

Log in to the web platform and choose **Security** > **Firewall** > **Zone Policy**.

b. Select **Zone name** or **Interface name** from the **Search item** drop-down list box, enter a keyword, click **Search**. You can view, modify, or delete a searched zone policy.

----End

2.15.2.2 Interzone Policy

Context

Any two zones form an interzone. Each interzone has an independent interzone view. Most firewall configurations are performed in the interzone views. After the firewall function is configured, the device checks data transmitted between zones.

The configured firewall functions take effect only after you enable firewall in the interzone.

When data is transmitted between two zones, the ACL-based packet filtering firewall enforces the packet filtering policies according to ACL rules.

Procedure

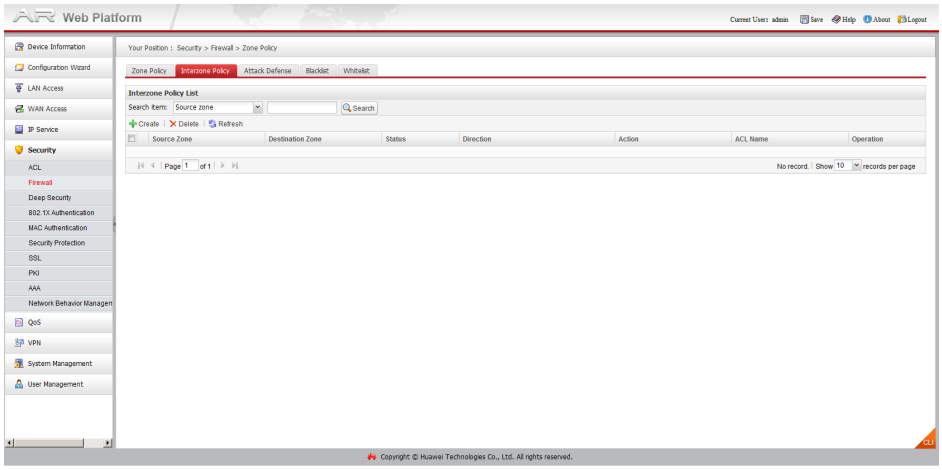
- Creating an interzone policy

a. Access the **Interzone Policy** tab page.

Log in to the web platform and choose **Security** > **Firewall** > **Interzone Policy**, as shown in **Figure 2-146**.

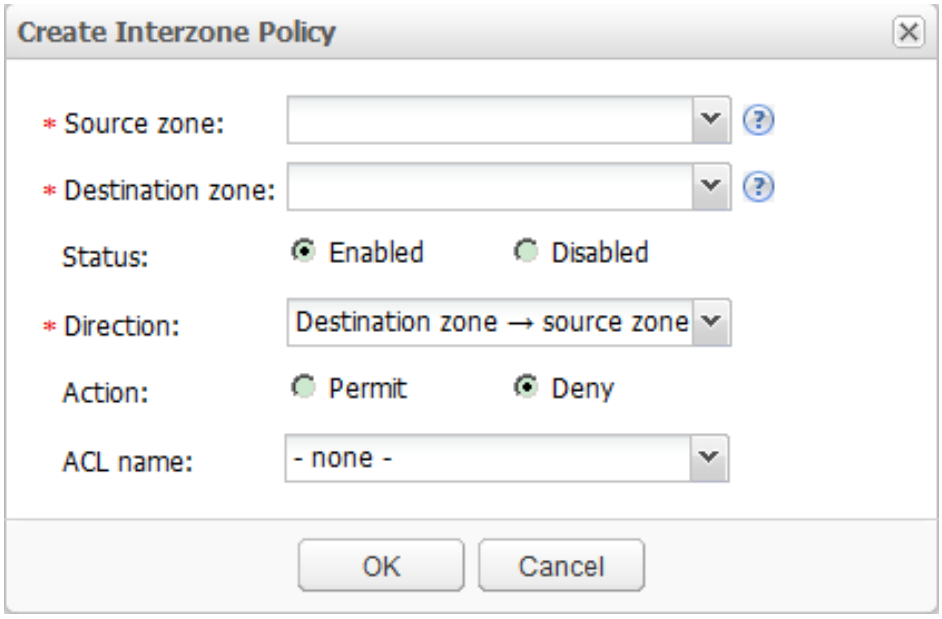
Copyright © Huawei Technologies Co., Ltd.

Figure 2-146 Configuring zone policy



b. Click **Create** and set parameters in the **Create Interzone Policy** dialog box that is displayed, as shown in **Figure 2-147**. **Table 2-125** describes the parameters.

Figure 2-147 Creating interzone policy



c. Click **OK**. An interzone policy is added to the interzone policy list.

 Copyright © Huawei Technologies Co., Ltd.

Table 2-125 Interzone parameters

Parameter	Description
Source zone	A source zone must be a created zone. The source zone priority must be equal to or higher than the destination zone priority.
Destination zone	A destination zone must be a created zone. The destination zone priority must be equal to or lower than the source zone priority.
Status	Whether to enable or disable the firewall function.
Direction	Direction from the source zone to the destination zone or from the destination zone to the source zone.
Action	Action of permit or deny.
ACL name	Name of the ACL for packet filtering. The ACLs include basic ACL and advanced ACL.

- Modifying an interzone policy
  a. Access the **Interzone Policy** tab page.

     Log in to the web platform and choose **Security** > **Firewall** > **Interzone Policy**.

  b. Click next to an interzone policy.

  c. Click of a direction.

  d. In the **Modify Interzone Policy** dialog box that is displayed, modify parameters listed in **Table 2-125**. The parameters are the same as those in **Figure 2-147**. The parameters **Source zone**, **Destination zone**, and **Direction** cannot be modified.

  e. Click **OK**.
- Deleting an interzone policy
  a. Access the **Interzone Policy** tab page.

     Log in to the web platform and choose **Security** > **Firewall** > **Interzone Policy**.

  b. Select an interzone policy and click **Delete**. In the **Information** dialog box that is displayed, click **OK**.
- Search an interzone policy
  a. Access the **Interzone Policy** tab page.

     Log in to the web platform and choose **Security** > **Firewall** > **Interzone Policy**.

Copyright © Huawei Technologies Co., Ltd.

b. Select **Source zone** or **Destination zone** from the **Search item** drop-down list box, enter a keyword, click **Search**. You can view, modify, or delete a searched interzone policy.

----End

2.15.2.3 Attack Defense

Context

The attack defense function protects the CPU from attacks and ensures the proper running of the server even when it is attacked.

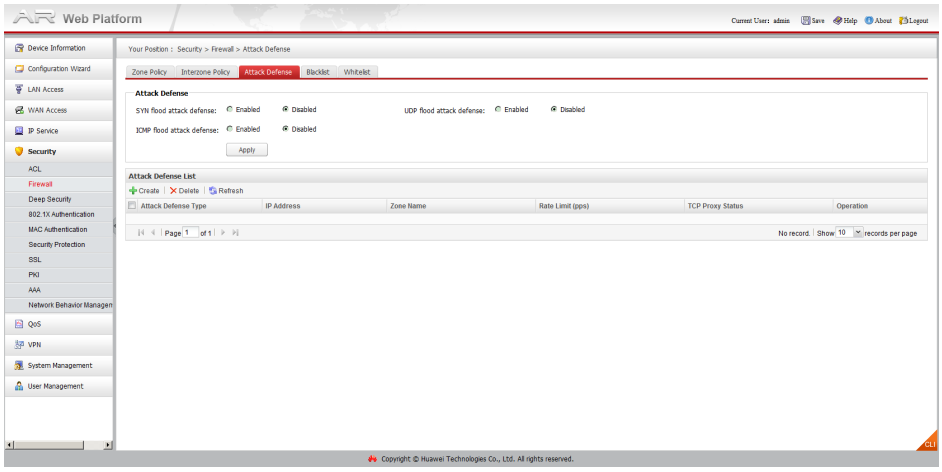
To prevent flood attacks, you need to specify the zones or IP addresses to be protected; otherwise, the attack defense parameters are invalid. You can also specify the maximum session rate. When the session rate exceeds the limit, the device considers that an attack occurs and takes measures.

Procedure

- Enabling or disabling the attack defense function
  a. Access the **Attack Defense** tab page.

     Log in to the web platform and choose **Security** > **Firewall** > **Attack Defense**, as shown in **Figure 2-148**.

     Figure 2-148 Configuring attack defense

  b. Enable or disable defense against SYN flood attacks, UDP flood attacks, or ICMP flood attacks in the **Attack Defense** area.

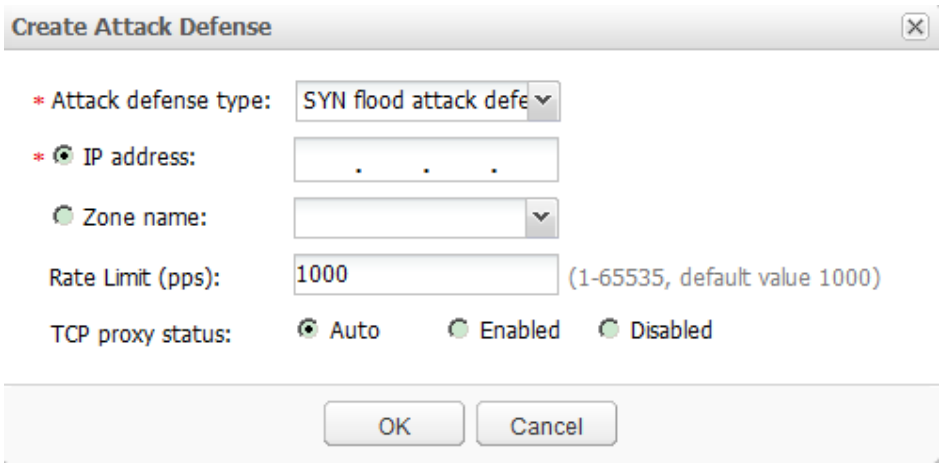
  c. Click **Apply**.

- Creating an attack defense entry
  a. Access the **Attack Defense** tab page.

     Log in to the web platform and choose **Security** > **Firewall** > **Attack Defense**.

b. Click **Create** in the **Attack Defense List** area and set parameters in the **Create Attack Defense** dialog box that is displayed, as shown in **Figure 2-149**. **Table 2-126** describes the parameters. Only one of the parameters between **IP address** and **Zone name** can be set.

Figure 2-149 Creating attack defense policy



c. Click **OK**. An attack defense entry is added to the attack defense list.

Table 2-126 Attack defense parameters

Parameter	Description
Attack defense type	The attack defense type can be SYN flood attack defense, UDP flood attack defense, or ICMP flood attack defense.
IP address	Protected IP address. The value is a valid IPv4 address.
Zone name	Protected zone. The zone must be an existing zone.
Rate Limit (pps)	Maximum session rate. The value is an integer that ranges from 1 to 65535, in seconds. The default value is 1000.
TCP proxy status	Status of the TCP proxy. The value can be **Auto**, **Enabled**, or **Disabled**. **NOTE** This parameter is valid only for the SYN flood attack defense.

- Modifying an attack defense entry
  a. Access the **Attack Defense** tab page.

     Log in to the web platform and choose **Security** > **Firewall** > **Attack Defense**.

Copyright © Huawei Technologies Co., Ltd.

b. Click  of an attack defense entry.

c. In the **Modify Attack Defense** dialog box that is displayed, modify parameters listed in **Table 2-126**. The parameters are the same as those in **Figure 2-149**. The parameters **Attack defense type**, **IP address**, and **Zone name** cannot be modified.

d. Click **OK**.

- Deleting an attack defense entry

a. Access the **Attack Defense** tab page.

Log in to the web platform and choose **Security** > **Firewall** > **Attack Defense**.

b. Select an attack defense entry and click **Delete**. In the **Information** dialog box that is displayed, click **OK**.

----End

2.15.2.4 Blacklist

Context

A blacklist filters packets based on source IP addresses. Compared with the ACL, the blacklist uses simpler matching fields to implement high-speed packet filtering. Packets from certain IP addresses can be effectively filtered out.

After an IP address is added to the blacklist, the firewall denies the packets from this IP address until this entry ages.

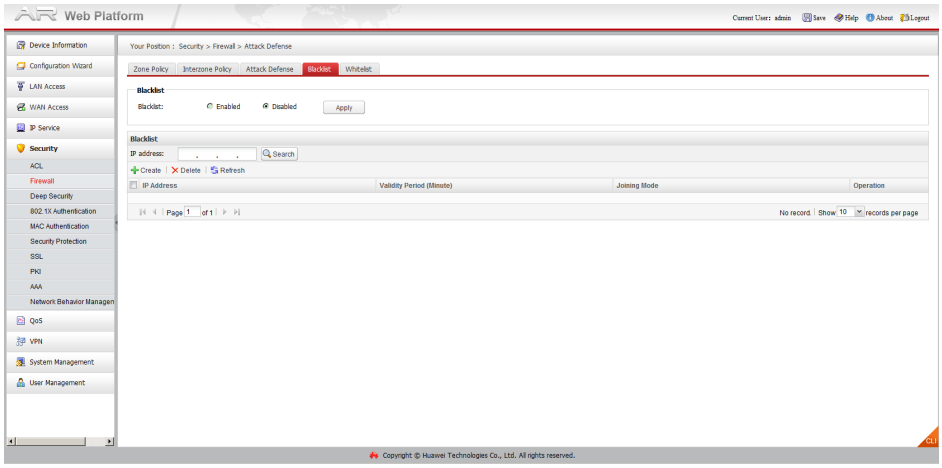
Procedure

- Enabling or disabling the blacklist function

a. Access the **Blacklist** tab page.

Log in to the web platform and choose **Security** > **Firewall** > **Blacklist**, as shown in **Figure 2-150**.

Figure 2-150 Configuring blacklist



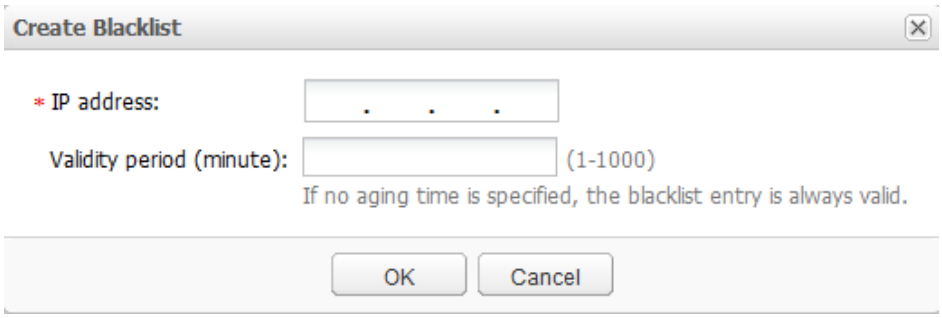
 Copyright © Huawei Technologies Co., Ltd.

b. Set **Blacklist** to **Enabled** or **Disabled**.
c. Click **Apply**.

- Creating a blacklist entry
  a. Access the **Blacklist** tab page.

     Log in to the web platform and choose **Security** > **Firewall** > **Blacklist**.
  b. Click **Create** and set parameters in the **Create Blacklist** dialog box that is displayed, as shown in **Figure 2-151**. **Table 2-127** describes the parameters.

     Figure 2-151 Creating a blacklist

  c. Click **OK**. A blacklist entry is added to the blacklist.

     Table 2-127 Blacklist parameters

Parameter	Description
IP address	IP address to be added to the blacklist. The value is a valid IPv4 address.
Validity period (minute)	Aging time of a blacklist entry. The value is an integer that ranges from 1 to 1000, in minutes. If no aging time is specified, the IP address is always valid in the blacklist.

- Modify a blacklist entry
  a. Access the **Blacklist** tab page.

     Log in to the web platform and choose **Security** > **Firewall** > **Blacklist**.
  b. Click  of a blacklist entry.
  c. In the **Modify Blacklist** dialog box that is displayed, modify parameters listed in **Table 2-127**. The parameters are the same as those in **Figure 2-151**. The parameter **IP address** cannot be modified.
  d. Click **OK**.
- Deleting a blacklist entry
  a. Access the **Blacklist** tab page.

Copyright © Huawei Technologies Co., Ltd.

Log in to the web platform and choose **Security** > **Firewall** > **Blacklist**.

b. Select a blacklist entry and click **Delete**. In the **Information** dialog box that is displayed, click **OK**.

- Searching a blacklist entry

a. Access the **Blacklist** tab page.

Log in to the web platform and choose **Security** > **Firewall** > **Blacklist**.

b. Enter an IP address in the **IP address** text box and click **Search**. You can view, modify, or delete the searched blacklist entry.

----End

2.15.2.5 Whitelist

Context

The whitelist is applicable to the network where some devices send valid service packets that look like IP sweeping attacks or port scanning attacks. The whitelist prevents these devices from being added to the blacklist.

A whitelist filters packets based on source IP addresses. IP addresses in the whitelist are not added to the static or dynamic blacklist.

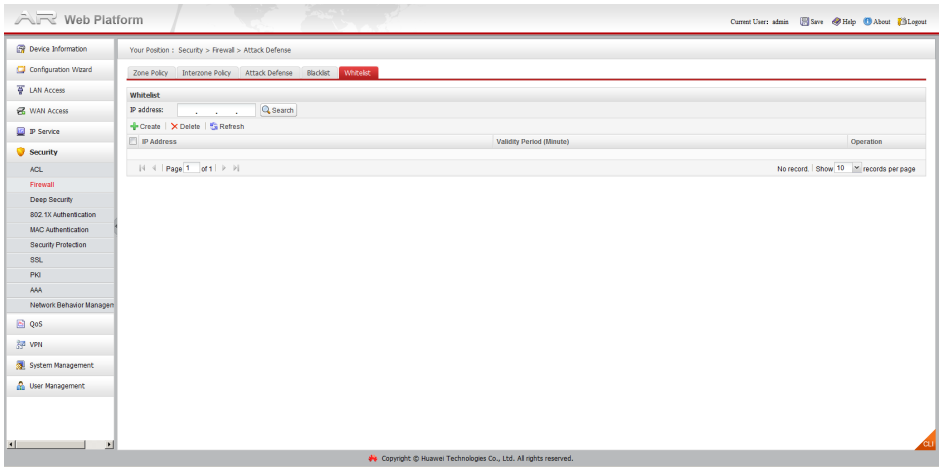
Procedure

- Create a whitelist entry

a. Access the **Whitelist** tab page.

Log in to the web platform and choose **Security** > **Firewall** > **Whitelist**, as shown in **Figure 2-152**.

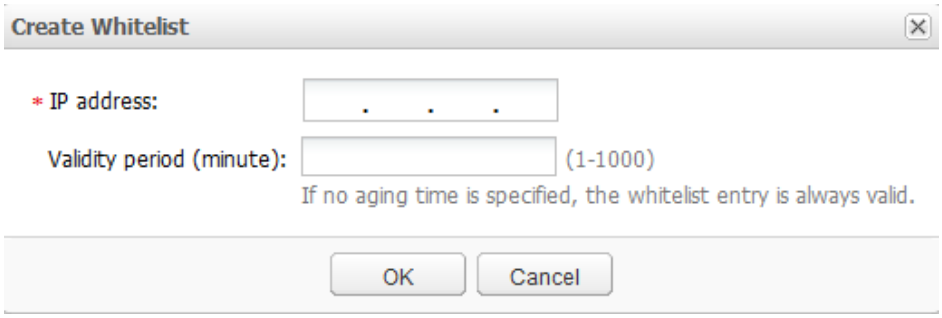
Figure 2-152 Configuring whitelist



b. Click **Create** and set parameters in the **Create Whitelist** dialog box that is displayed, as shown in **Figure 2-153**. **Table 2-128** describes the parameters.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-153 Creating a whitelist



c. Click **OK**. A whitelist entry is added to the whitelist.

Table 2-128 Whitelist parameters

Parameter	Description
IP address	IP address to be added to the whitelist. The value is a valid IPv4 address.
Validity period (minute)	Aging time of a whitelist entry. The value is an integer that ranges from 1 to 1000, in minutes. If no aging time is specified, the IP address is always valid in the whitelist.

- Modify a whitelist entry
  a. Access the **Whitelist** tab page.

     Log in to the web platform and choose **Security** > **Firewall** > **Whitelist**.
  b. Click  of a whitelist entry.
  c. In the **Modify Whitelist** dialog box that is displayed, modify parameters listed in **Table 2-128**. The parameters are the same as those in **Figure 2-153**. The parameter **IP address** cannot be modified.
  d. Click **OK**.
- Deleting a whitelist entry
  a. Access the **Whitelist** tab page.

     Log in to the web platform and choose **Security** > **Firewall** > **Whitelist**.
  b. Select a whitelist entry and click **Delete**. In the **Information** dialog box that is displayed, click **OK**.
- Searching a whitelist entry
  a. Access the **Whitelist** tab page.

     Log in to the web platform and choose **Security** > **Firewall** > **Whitelist**.
  b. Enter an IP address in the **IP address** text box and click **Search**. You can view, modify, or delete the searched whitelist entry.

----End

 Copyright © Huawei Technologies Co., Ltd.

2.15.2.6 IP Source Guard

Context

IP Source Guard (IPSG) implements source IP address filtering based on Layer 2 interfaces. IPSG is used to prevent network access from malicious hosts using stolen IP addresses. In addition, IPSG prevents unauthorized hosts from accessing or attacking networks with forged IP addresses.

As networks continue to increase in scale, many attackers are forging source IP addresses to initiate network attacks (IP address spoofing attacks). Some attackers steal the IP addresses of authorized users to obtain network access rights and access networks. As a result, authorized users are unable to access networks or sensitive information may be intercepted. IPSG provides a mechanism to effectively defend against IP address spoofing attacks.

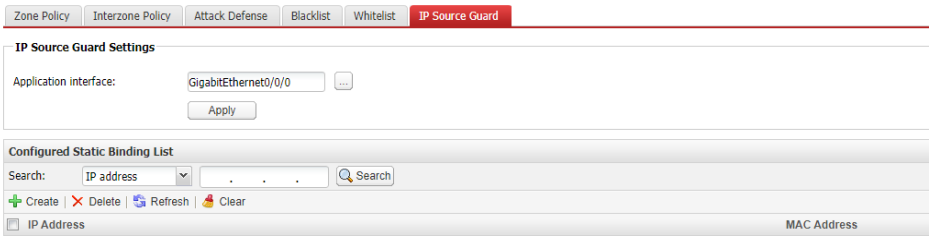
NOTE

This function is supported in V200R010C10 and later versions.

Procedure

- Setting IPSG
  a. Choose **Security** > **Firewall** > **IP Source Guard**. The **IP Source Guard** tab page is displayed, as shown in **Figure1**.

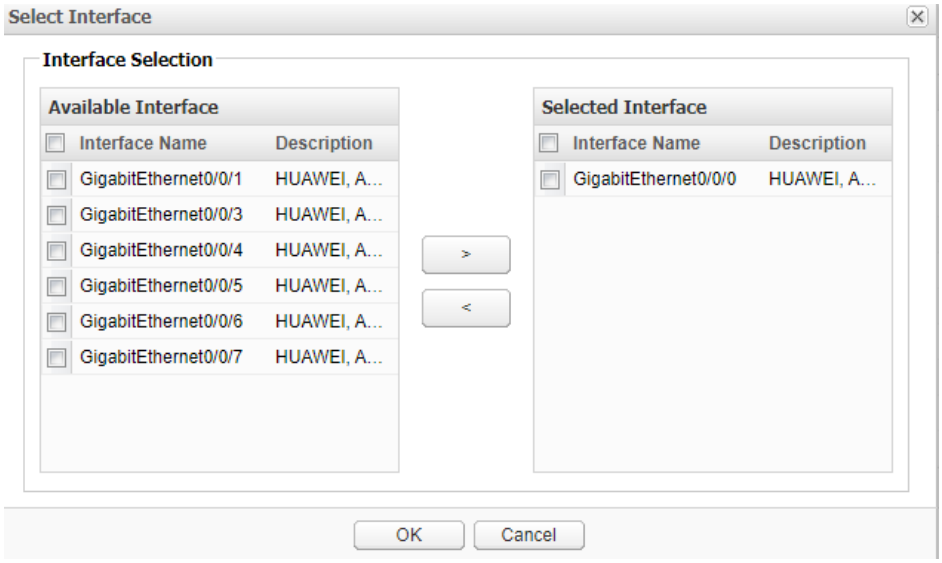
     Figure 2-154 IP Source Guard

  b. In the **IP Source Guard Settings** area, click  next to **Application interface** to select an interface, as shown in **Figure2**.

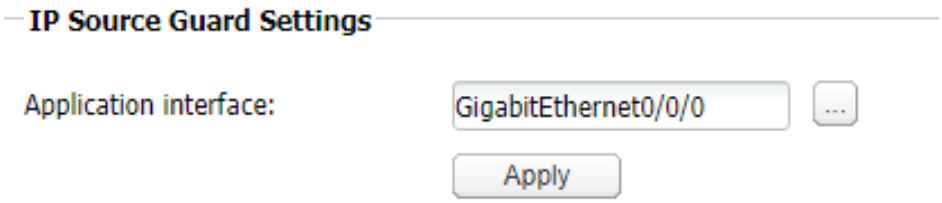
 Copyright © Huawei Technologies Co., Ltd.

Figure 2-155 Application interface Select



c. Click **OK**. The selected interface name is displayed in the **Application interface** text box under **IP Source Guard Settings**, as shown in **Figure3**.

Figure 2-156 Application interface

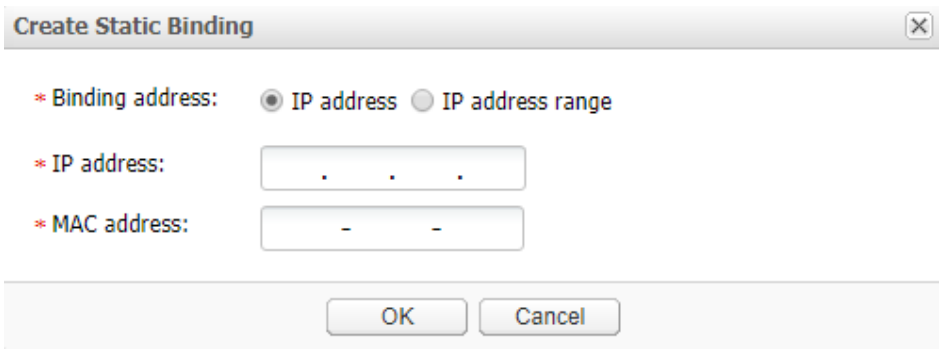


d. Click **Apply**. The application interface of IP source guard is configured.

- Create Static Binding

a. In **Configured Static Binding List**, click **Create**. In the **Create Static Binding** dialog box that is displayed, set parameters, as shown in **Figure4**. For detailed parameter descriptions, see **Table1**

Figure 2-157 Create Static Binding



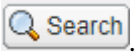
b. Click **OK**. The newly created static binding is added to the configured static binding list.

Copyright © Huawei Technologies Co., Ltd.

Table 2-129 Create Static Binding parameters

Parameter	Description
Binding address	Specifies the type of the IP address for static binding. Two options are available: • IP address • IP address range
IP address	Specifies the user IP address in a static binding entry. The value is in dotted decimal notation.
IP address range	Specifies the user IP address range in a static binding entry.
MAC address	Specifies the user MAC address in a static binding entry. The value is in the format of H-H-H. Each H indicates a hexadecimal number of 1 to 4 digits.

- Search Static Binding

  In the **Configured Static Binding List** area, select a search type from the drop-down list on the right, for example, IP address and MAC address. In the search text box, enter the corresponding content and click 

. The information searched out will be displayed in **Configured Static Binding List**.
- Delete Static Binding
  a. On the **IP Source Guard** tab page, view information in the **Configured Static Binding List** area. Click **Refresh**. You can view the list of static binding entries configured on the device.
  b. Select the static binding entry to be deleted and click **Delete**. In the displayed dialog box, click **OK**.
- Clear Static Binding

  Click **Clear**. In the displayed dialog box, click **OK**.

----End

2.15.3 Deep Security

NOTE

- The following product models support IPS function:
  - AR160 series: AR169BF, AR169FGW-L, AR169FGVW-L, AR169FVW-8S, AR169JFVW-4B4S, AR169JFVW-2S, AR169EGW-L, AR169EW, AR168F-4P, AR161EW, AR161EW-M1, AR161FW, AR161FV-1P, and AR169FVW.
  - AR1200 series: AR1220E, AR1220EV, and AR1220EVW.
  - AR2200 series: AR2204, AR2204XE, AR2204XE-DC, AR2220, AR2220E, AR2240, and AR2240C.
  - AR3200 series: All models.

Copyright © Huawei Technologies Co., Ltd.

NOTE

- The following product models support URL filtering function:
  - AR100&AR120&AR150&AR160&AR200&AR3200 series: All models.
  - AR1200 series: AR1220C, AR1220-8GE, AR1220E, AR1220EV, and AR1220EVW.
  - AR2200 series: all models except AR2201-48FE, AR2202-48FE, and AR2204.

2.15.3.1 Policy Application

Context

A security policy controls traffic forwarding on devices and detects the traffic content.

After policy application is configured, a device performs content security detection on all traffic between the source and destination zones. If traffic matches the rules of the security policy, the device takes actions defined by the security policy, securing enterprise networks.

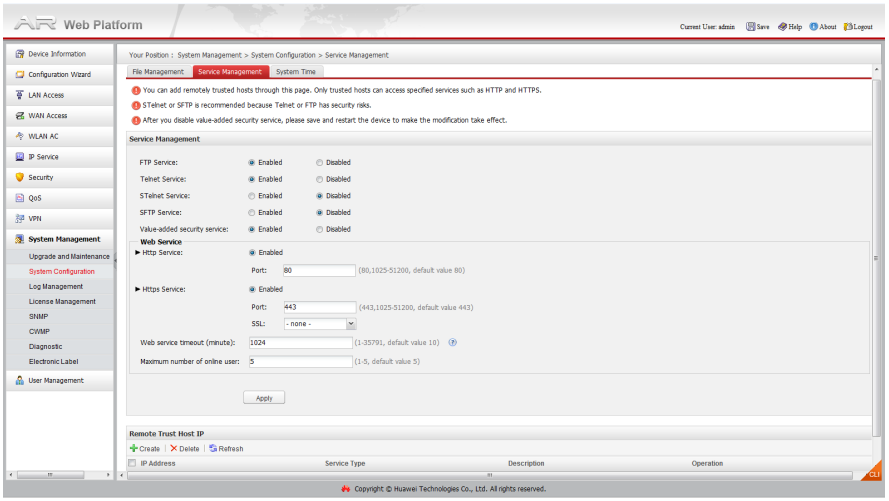
Prerequisite

To use the deep security function, you must enable it. By default, the deep security function is disabled.

1. Open the **Service Management** page.

   Log in to the web system, choose **System Management** > **System Configuration** > **Service Management** to open the **Service Management** page, as shown in **Figure 2-158**.

   Figure 2-158 Service Management tab page



2. Enable or disable deep security.
   - Enable deep security.

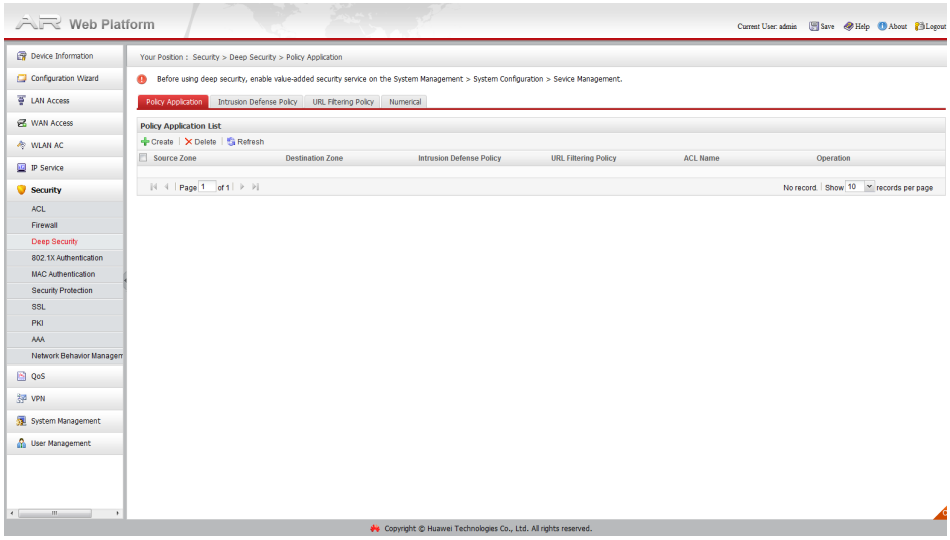
     In the **Service Management** area, click **Enabled** > **Apply** of **Value-added security service** to enable the deep security function.

– Disable deep security.
To disable deep security, click **Disable** and **Apply**, and restart the device. After the device restarts, the deep security configurations are deleted.

Procedure

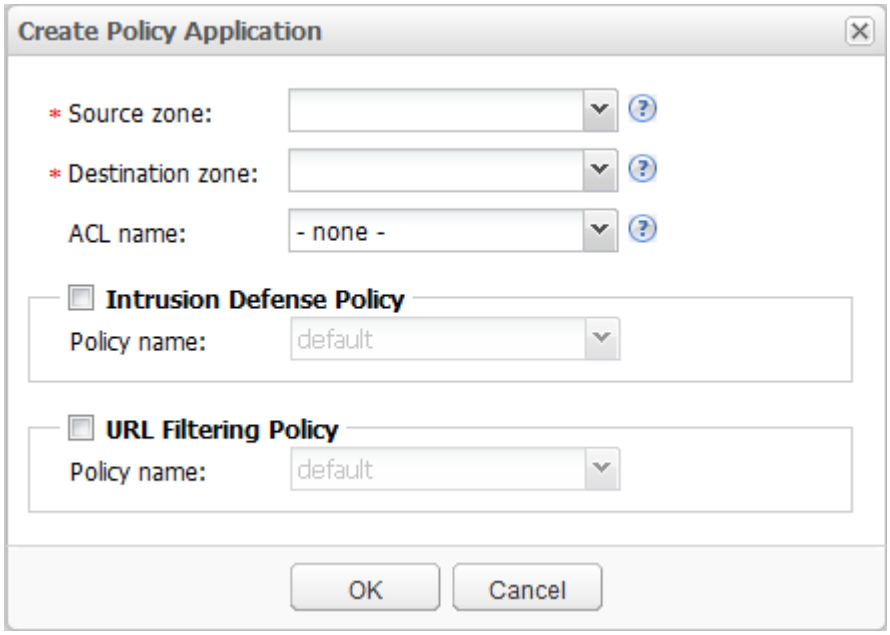
- Creating an applied policy
  a. Access the **Policy Application** tab page, as shown in **Figure 2-159**.
  Log in to the tab page**Deep Security** and choose **Policy Application**.

  Figure 2-159 Policy Application tab page



  b. In the **Policy Application List** area, click **Create** and set policy application parameters. **Table 2-130** describes the parameters, as shown in **Figure 2-160**.

  Figure 2-160 Create Policy Application tab page



 Copyright © Huawei Technologies Co., Ltd.

c. Click **OK**.

Table 2-130 Policy application parameters

Parameter	Description
Source zone	Security zone from which traffic is sent, which has a high security. The source zone can be the default or user-defined security zone. For details about how to configure a security zone, see **2.15.2.1 Zone Policy**.
Destination zone	Security zone for which traffic is destined, which has a low priority. The destination zone must exist. For details about how to configure a security zone, see **2.15.2.1 Zone Policy**.
ACL name	Object on which content security detection is performed, such as a period of time and IP address segment. The ACL rule must exist. **NOTE** The policy takes effect only when the ACL rule is set to permit. For details about how to configure an ACL, see **ACL**.
Intrusion Defense Policy	The intrusion defense policy must exist. After an intrusion defense policy is configured in the policy application list, a device compares the traffic content against the intrusion defense library to detect attacks such as overflow attacks in the buffer, Trojan horses, and worm viruses, defending against attacks at the application layer. For details about how to configure an intrusion defense policy, see **2.15.3.2 Intrusion Defense Policy**.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
URL Filtering Policy	The URL filtering policy must exist. After a URL filtering policy is configured in the policy application list, a device controls URLs that users can access to allow or forbid the users to access specified website resources. For details about how to configure a URL filtering policy, see **2.15.3.3 URL Filtering Policy**.

- Modifying an applied policy
  a. In the **Policy Application List** area, select a policy and click  on the right.
  b. In the **Modify Policy Application List** dialog box that is displayed, modify the parameters. The parameters are the same as those in **Figure 2-160**
  c. Click **OK**.
- Deleting an applied policy
  a. In the **Policy Application List** area, select a policy and click **Delete**.
  b. In the dialog box that is displayed, click **OK**.

----End

2.15.3.2 Intrusion Defense Policy

Context

An intrusion prevention system (IPS) prevents and detects intrusions based on the intrusion defense library. Before configuring intrusion defense policies, load the intrusion defense library.

After the intrusion defense library is loaded, a large number of unclassified signatures are generated and characteristics in some signatures do not exist on the live network. You must use a signature filter to filter out the signatures and configure a unified action for the signatures. To configure specified actions for specified signatures, you must set the signatures as exception signatures, bringing heavy workload.

To resolve this problem, configure intrusion defense policies. You can configure only one signature filter but multiple exception signatures in an intrusion defense policy. After the signature filter and exception signatures are configured, signatures matching the network characteristics are selected. Intrusion defense policies can prevent intrusions on the device.

The device has multiple default intrusion prevention profiles for different application scenarios. The default intrusion prevention profiles can be displayed, cloned, or referenced in security policies, but cannot be modified or deleted.

Copyright © Huawei Technologies Co., Ltd.

- **strict**: It contains all signatures and the action is block. Apply to all protocols and categories. The intrusion prevention profile applies to the scenarios in which the device is required to block all matched packets.
- **web_server**: It contains all signatures and the action is the default actions. Apply to DNS, HTTP, FTP protocols and all categories. The intrusion prevention profile applies to the scenarios in which the device is deployed in front of a web server.
- **file_server**: It contains all signatures and the action is the default actions. Apply to DNS, SMB, NETBIOS, NFS, SUNRPC, MSRPC, FILE, TELNET protocols and all categories. The intrusion prevention profile applies to the scenarios in which the device is deployed in front of a file server.
- **dns_server**: It contains all signatures and the action is the default actions. Apply to DNS protocol and all categories. The intrusion prevention profile applies to the scenarios in which the device is deployed in front of a DNS server.
- **mail_server**: It contains all signatures and the action is the default actions. Apply to DNS, IMAP4, SMTP, POP3 protocols and all categories. The intrusion prevention profile applies to the scenarios in which the device is deployed in front of a mail server.
- **inside_firewall**: It contains all signatures and the action is the default actions. Apply to all protocols and categories. The intrusion prevention profile applies to the scenarios in which the device is deployed behind a firewall.
- **dmz**: It contains all signatures and the action is the default actions. Apply to all protocols except NETBIOS, NFS, SMB, TELNET TFTP and categories. The intrusion prevention profile applies to the scenarios in which the device is deployed behind a firewall. The intrusion prevention profile applies to the scenarios in which the device is deployed in front of a DMZ.
- **outside_firewall**: It contains all signatures and the action is the default actions. Apply to all protocols and categories except Scanner. The intrusion prevention profile applies to the scenarios in which the device is deployed in front of a firewall.
- **ids**: It contains all signatures and the action is alert. Apply to all protocols and categories. The intrusion prevention profile applies to the scenarios in which the device is deployed off-line as an IDS.
- **default**: It contains all signatures and the action is the default actions. Apply to all protocols and categories. The intrusion prevention profile applies to the scenarios in which the device is deployed in-line as an IPS.

Prerequisite

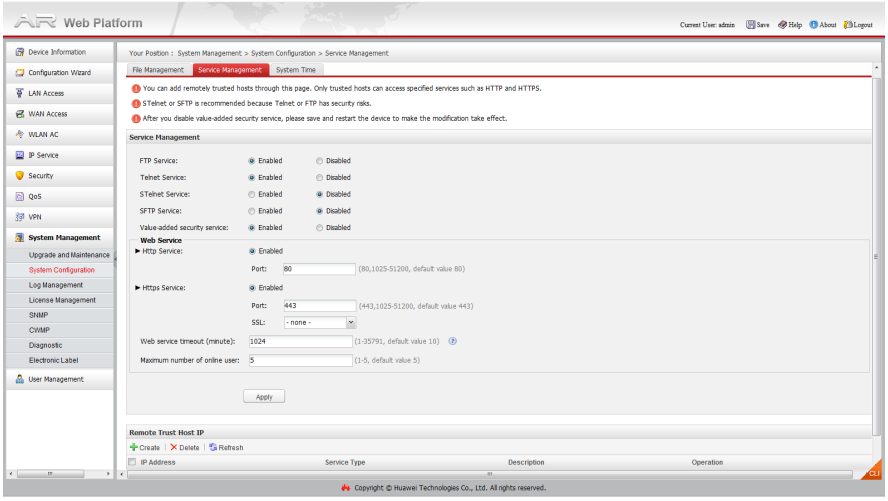
To use the deep security function, you must enable it. By default, the deep security function is disabled.

1. Open the **Service Management** page.

   Log in to the web system, choose **System Management** > **System Configuration** > **Service Management** to open the **Service Management** page, as shown in **Figure 2-161**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-161 Service Management tab page



2. Enable or disable deep security.
   - Enable deep security.

     In the **Service Management** area, click **Enabled** > **Apply** of **Value-added security service** to enable the deep security function.
   - Disable deep security.

     To disable deep security, click **Disable** and **Apply**, and restart the device.

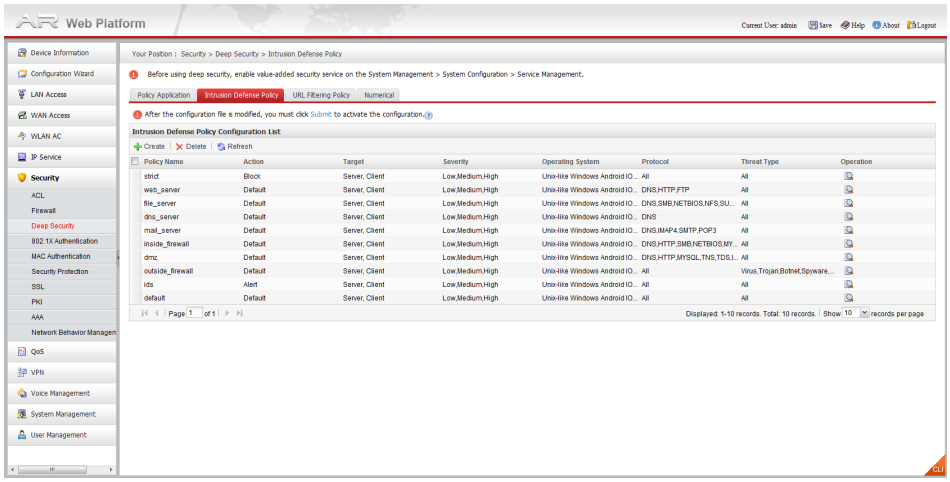
     After the device restarts, the deep security configurations are deleted.

Procedure

- Creating an intrusion defense policy
  a. Access the **Intrusion Defense Policy** tab page, as shown in **Figure 2-162**.

     Log in to the tab page **Deep Security** and choose **Intrusion Defense Policy**.

Figure 2-162 Intrusion Defense Policy tab page



 Copyright © Huawei Technologies Co., Ltd.

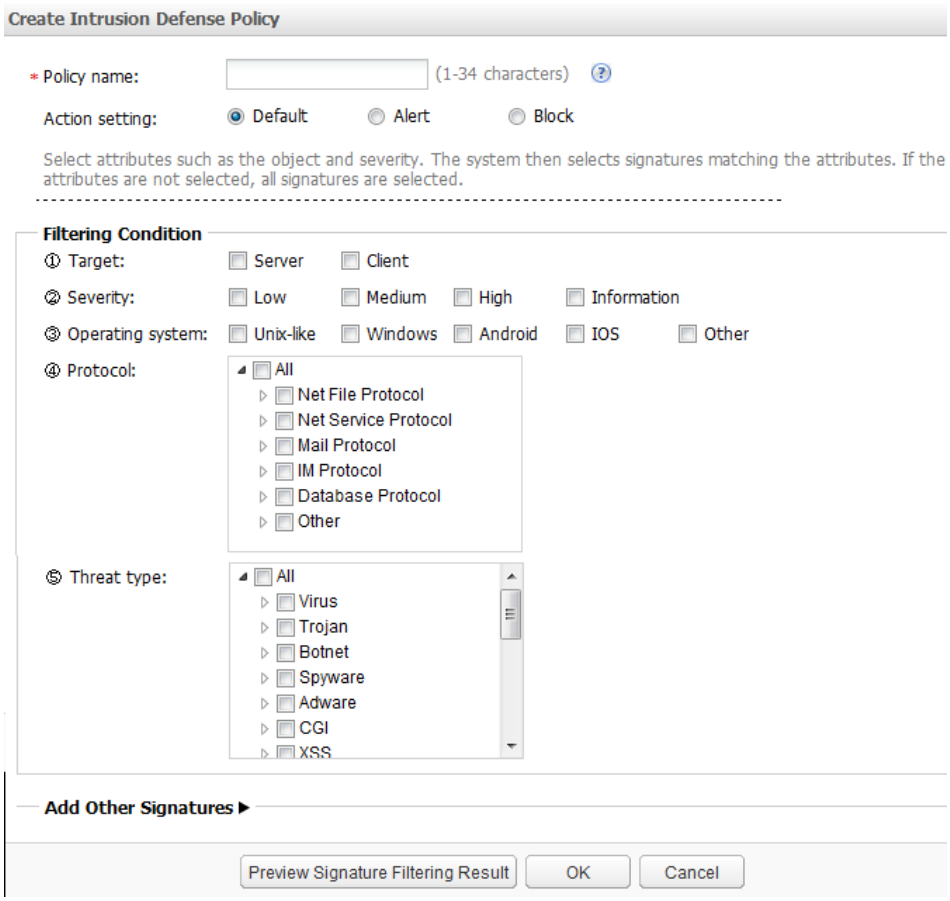
b. Click **Create** in the **Intrusion Defense Policy Configuration List** area. Set parameters in the **Create Intrusion Defense Policy** dialog box. **Table 2-131** describes the parameters, as shown in **Figure 2-163**.

Table 2-131 Parameters for creating an intrusion defense policy

Parameter	Description
Policy name	Name of the intrusion defense policy. The policy name cannot be changed after the intrusion defense policy is configured.
Action setting	Action of the signature filter. • **Default**: A signature has a predefined default action (**Block** or **Alert**). • **Alert**: When a packet matches a signature, the packet is allowed to pass, which is recorded in the log. • **Block**: When a packet matches a signature, the packet is discarded, which is recorded in the log. By default, the signature filter uses the default action of a signature.
Target	Targets to be filtered. You can select multiple targets. The signature filter can filter out signatures with specified targets.
Severity	Severity of intrusions to be filtered. You can select multiple severity values. The signature filter can filter out signatures with specified severity values.
Operating system	Operating systems to be filtered. You can select multiple operating systems. The signature filter can filter out signatures with specified operating systems.
Protocol	Protocols to be filtered. You can select multiple protocols. The signature filter can filter out signatures with specified protocols.
Threat type	Threat types to be filtered. You can select multiple threat types. The signature filter can filter out signatures with specified threat types.

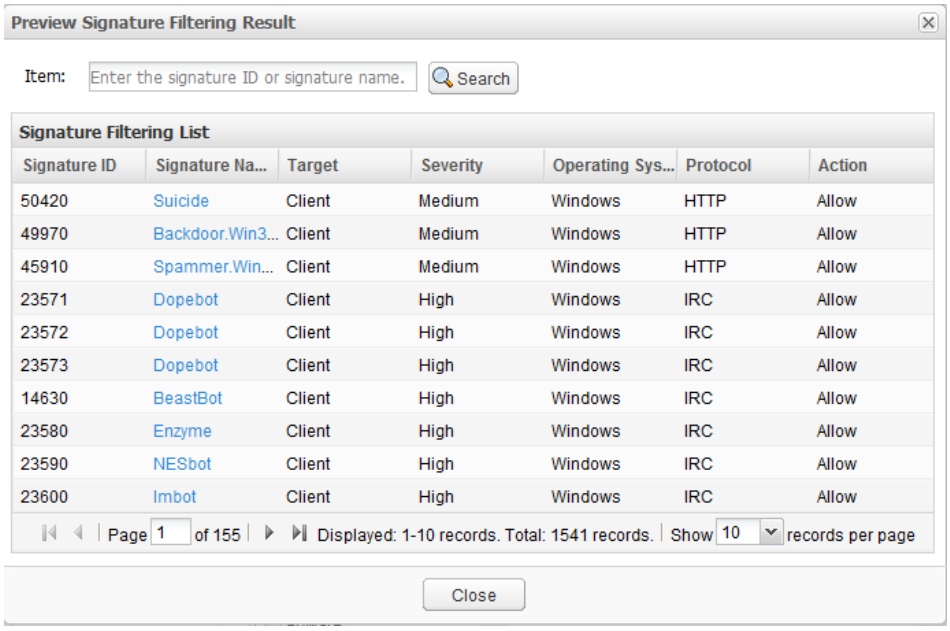
Copyright © Huawei Technologies Co., Ltd.

Figure 2-163 Create Intrusion Defense Policy dialog box



c. Click **Preview Signature Filtering Result**. Signatures that are filtered out by the intrusion defense policy are displayed, as shown in **Figure 2-164**.

Figure 2-164 Preview Signature Filtering Result page



 Copyright © Huawei Technologies Co., Ltd.

d. Click ▶ next to **Add Other Signatures**. Set **Signature ID** to complete the signature adding, as shown in **Figure 2-165**.

Figure 2-165 Add Other Signatures



NOTE

You can check mistakenly filtered signature IDs based on the log or in other ways. After adding these signatures to the list, you can modify the signature actions.

e. Set parameters in **List of Other Signatures**. **Table 2-132** describes the parameters.

Table 2-132 Parameters in the list of exception signatures

Parameter	Description
Signature ID	This parameter is set by the system and cannot be changed.
Signature name	This parameter is set by the system and cannot be changed.
Action	Action of the exception signature. • **Pass**: When a packet matches the exception signature, the packet is allowed to pass, which is not recorded in the log. • **Alert**: When a packet matches the exception signature, the packet is allowed to pass, which is recorded in the log. • **Block**: When a packet matches the exception signature, the packet is discarded, which is not recorded in the log. The default action of an exception signature is pass.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Operation	You can click  next to an exception signature to delete it.

f. Click **OK**. The configuration is added to **Intrusion Defense Policy Configuration List**.

g. On the **Intrusion Defense Policy** tab page, click **Submit** above **Intrusion Defense Policy Configuration List**. In the **Information** dialog box, click **OK**. The intrusion defense policy configuration is activated.

NOTE

After an intrusion defense policy is created or modified, you must click **Submit** to make the configuration take effect. The activation takes a long period. You are advised to submit the configuration after modifying the intrusion defense policy.

- Modifying an intrusion defense policy

  a. Select an intrusion defense policy in the **Intrusion Defense Policy Configuration List** area and click  .

  NOTE

  You cannot modify the predefined intrusion defense policies.

  b. In the **Modify Intrusion Defense Policy** dialog box, modify the parameters as described in **Table 2-131**, among which **Policy name** cannot be changed.

  c. Click **Preview Signature Filtering Result**. Signatures that are filtered out by the intrusion defense policy are displayed.

  d. Click **OK**. The configuration is saved.

  e. On the **Intrusion Defense Policy** tab page, click **Submit** above **Intrusion Defense Policy Configuration List**. In the **Information** dialog box, click **OK**. The intrusion defense policy configuration is activated.

- Deleting an intrusion defense policy

  a. Select an intrusion defense policy in the **Intrusion Defense Policy Configuration List** area and click **Delete**. In the **Information** dialog box, click **OK**. The selected intrusion defense policy is deleted.

  b. On the **Intrusion Defense Policy** tab page, click **Submit** above **Intrusion Defense Policy Configuration List**. In the **Information** dialog box, click **OK**. The intrusion defense policy configuration is activated.

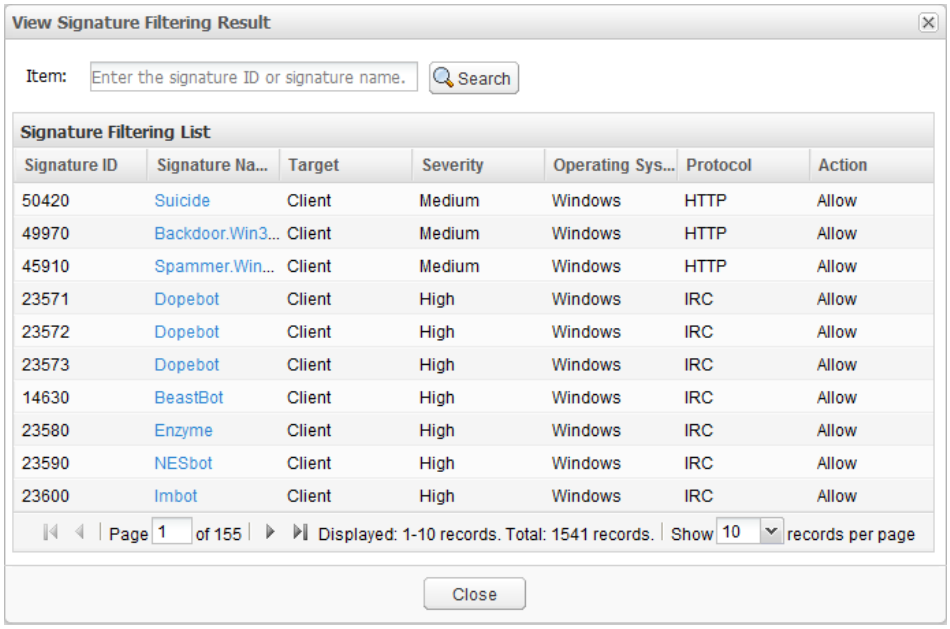
- Searching an intrusion defense policy

  a. Select an intrusion defense policy in the **Intrusion Defense Policy Configuration List** area and click  .

  b. Set the signature ID or name in **Item** and click **Search**. The predefined signature in the intrusion defense policy is displayed, as shown in **Figure 2-166**.

Copyright © Huawei Technologies Co., Ltd.

Figure 2-166 View Signature Filtering Result



c. Click **Signature name**. Information about the predefined signature is displayed.

----End

2.15.3.3 URL Filtering Policy

Context

As Internet applications rapidly develop, the computer network is widely applied, which facilitates information obtaining, sharing, and spreading. However, this brings enterprises the following threats:

- Employees access the websites that are irrelevant to their jobs, affecting working efficiency.
- Employees access illegal or malicious websites that may cause attacks caused by viruses including Trojan horses, and worms.

URL filtering is used to control URLs that users access. Website resources that are open to users are limited.

By default, one URL filtering policy is predefined on a device. If the predefined intrusion defense policy meets scenario requirements, you can reference the predefined URL filtering policy. The following parameters are used to distinguish the predefined URL filtering policy and its scenario:

- **default**

  Default policy. This policy contains all signatures and its action is **Allow** and HTTP packets are allowed to pass without any processing.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

•The following product models support URL filtering function:

- AR100&AR120&AR150&AR160&AR200&AR3200 series: All models.
- AR1200 series: AR1220C, AR1220-8GE, AR1220E, AR1220EV, and AR1220EVW.
- AR2200 series: all models except AR2201-48FE, AR2202-48FE, and AR2204.

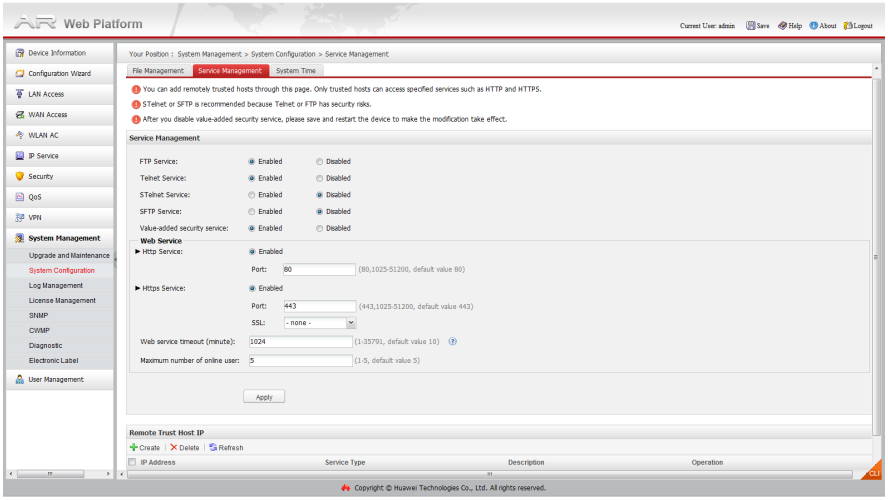
Prerequisite

To use the deep security function, you must enable it. By default, the deep security function is disabled.

1. Open the **Service Management** page.

   Log in to the web system, choose **System Management** > **System Configuration** > **Service Management** to open the **Service Management** page, as shown in **Figure 2-167**.

   Figure 2-167 Service Management tab page



2. Enable or disable deep security.
   - Enable deep security.

     In the **Service Management** area, click **Enabled** > **Apply** of **Value-added security service** to enable the deep security function.
   - Disable deep security.

     To disable deep security, click **Disable** and **Apply**, and restart the device.

     After the device restarts, the deep security configurations are deleted.

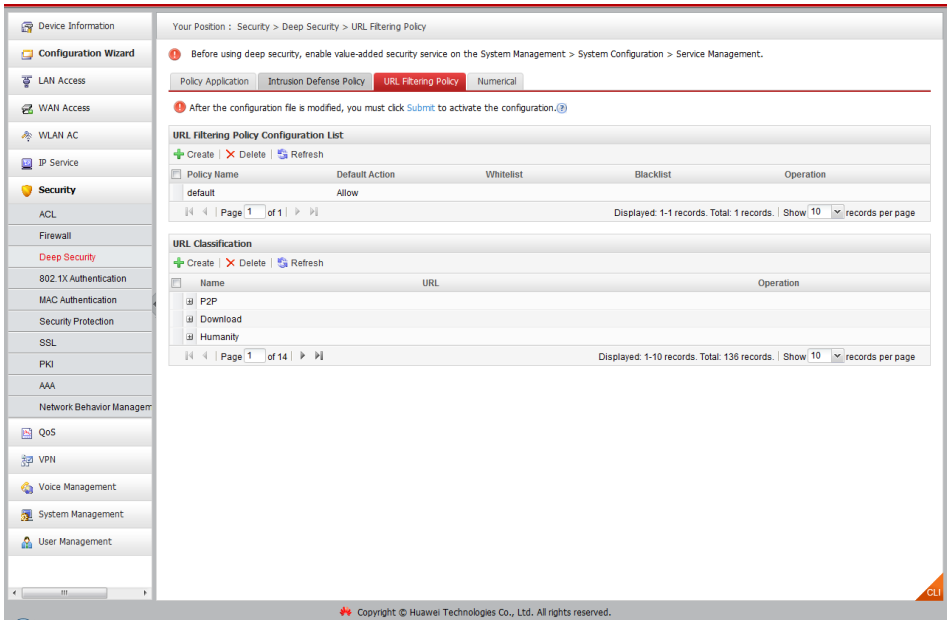
Procedure

- Configuring a URL filtering policy list
  - Creating a URL filtering policy

  a. Access the **URL Filtering Policy** tab page, as shown in **Figure 2-168**.

     Log in to the tab page**Deep Security** and choose **URL Filtering Policy**.

Figure 2-168 URL Filtering Policy tab page



b. In the **URL Filtering Policy Configuration List** area, click **Create** and set parameters of the URL filtering policy. **Table 2-133** describes the parameters, as shown in **Figure 2-169**.

Table 2-133 URL filtering policy parameters

Parameter	Description
Policy name	Name of the URL filtering policy.
Default action	Default action. • Allow: HTTP packets are allowed to pass without any processing. • Block: HTTP packets are discarded, which is recorded in the log. A block page is displayed on the terminal of the user that sends HTTP requests. • Alert: HTTP packets are allowed to pass, which is recorded in the log. All URL categories without actions configured use the default action.

Parameter	Description
URL classification	• **Enable Predefined URL Classification** is chosen by default, it can be used to control user access to common websites, by default, **Filtering Level** is low. Set the filtering level, for details, see **Table 2-134**. • **Enable User-Defined URL Classification** can be used to control user access to websites that are not controlled by predefined categories and websites defined by the administrator. After clicking **Enable User-Defined URL Classification**, you can add, modify, or delete a URL category. For details, see **Configuring a URL category**. If no action is configured for a URL category, the default action **Allow** is used. To modify the action, select the URL category and choose **Alert** or **Block** from the **Action** drop-down list box.
URL whitelist	URL whitelist containing learning websites that employees can access at any time. 1. Click **Enabled**. The URL whitelist function is enabled. 2. Enter a URL on each line in the dialog box. You can add the wildcard (*) indicating any character to the start or end of the URL. **NOTE** The whitelist is prior to the blacklist. If the URL that a user wants to access is in the URL whitelist, packets from the user are allowed to pass and the URL is not compared against the URL blacklist.

Copyright © Huawei Technologies Co., Ltd.

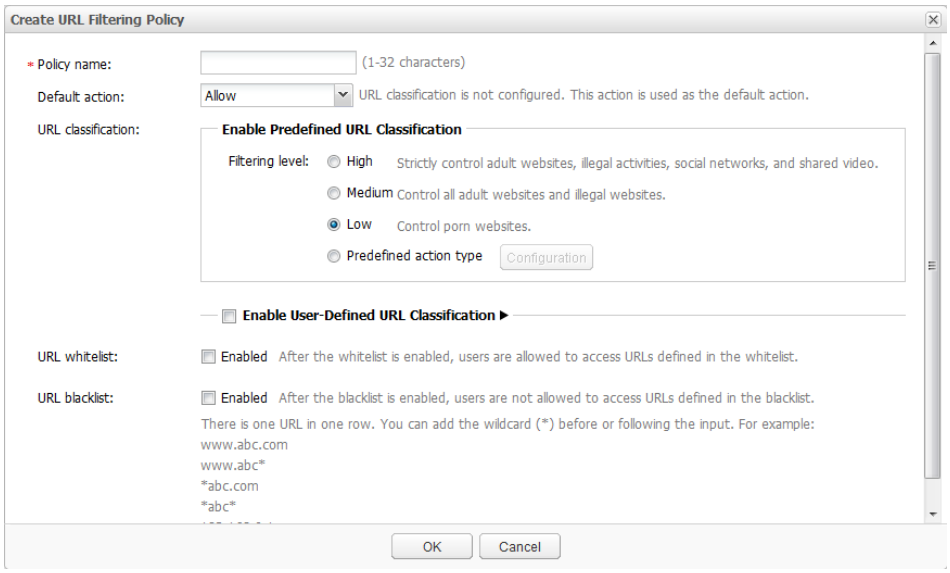
Parameter	Description
URL blacklist	URL blacklist containing websites that employees cannot access at any time, including the entertainment, game, and video websites. 1. Click **Enabled**. The URL blacklist function is enabled. 2. Enter a URL on each line in the dialog box. You can add the wildcard (*) indicating any character to the start or end of the URL. **NOTE** If the URL that a user wants to access is not in the URL whitelist, the URL is compared against the URL blacklist. If the URL is in the URL blacklist, the URL is blocked. If the URL is not in the URL blacklist, the device queries the URL category.
Encrypted traffic filtering	Set the status of the encrypted traffic filtering function. 1. Click **ON** to enable the Encrypted traffic filtering. 2. The URL requests sent by users to access desired websites are transmitted using HTTP or HTTPS. For HTTP traffic, the Router can properly implement URL filtering. For HTTPS traffic, the Router can implement URL filtering only after encrypted traffic filtering is configured. 3. Encrypted traffic filtering takes effect only when it is enabled in the URL filtering profile. If encrypted traffic filtering is disabled in the URL filtering profile, the URL filtering profile does not take effect for HTTPS traffic. **NOTE** This parameter is supported in V200R010C10 and later versions.

Copyright © Huawei Technologies Co., Ltd.

Table 2-134 Filtering levels of the predefined URL category library

Filtering Level	Description
High	Strictly controls access to all adult websites, illegal websites, social websites, and video sharing websites.
Medium	Controls access to all adult websites and illegal websites.
Low	Controls access to porn websites.
Predefined action type	1. Click **Configuration**. The **Set Predefined Classification Action** dialog box is displayed. 2. Set the predefined actions in either of the following ways: • Select a main category such as **Download** and set an action (allow, alert, or block) for the category. • Click ⊞ and select a subcategory (such as **e-Books** under **Download**). Set an action for the subcategory for accurately controlling the URL category. 3. Click **OK**.

Figure 2-169 Create URL Filtering Policy



Copyright © Huawei Technologies Co., Ltd.

c. Click **OK**.

– Modifying a URL filtering policy

a. Select a URL filtering policy in the **URL Filtering Policy Configuration List** area and click  .

b. In the **Modify URL Filtering Policy** dialog box, modify the parameters, among which **Policy name** cannot be changed.

c. Click **OK**.

– Deleting a URL filtering policy

a. Select a URL filtering policy in the **URL Filtering Policy Configuration List** area and click **Delete**.

b. In the dialog box that is displayed, click **OK**. The URL filtering policy is deleted.

- Configuring a URL category

  – Creating a user-defined URL category

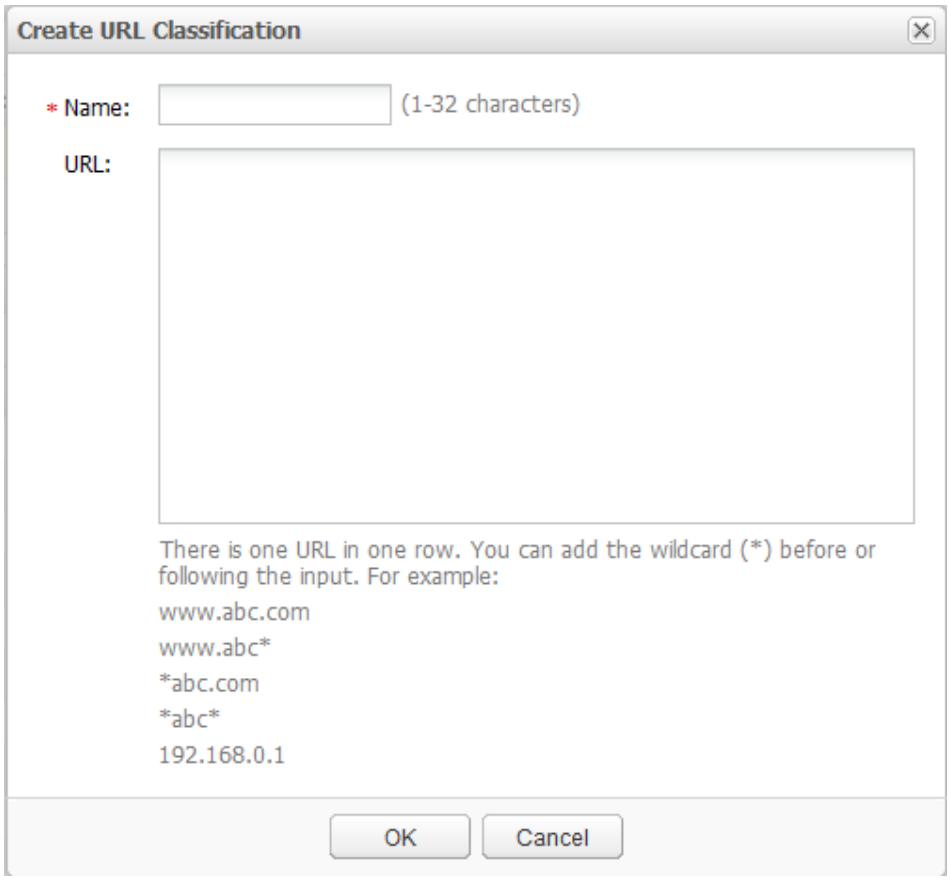
  a. Click **Create** in **URL Classification** and set parameters. **Table 2-135** describes the parameters.

Table 2-135 URL category parameters

Parameter	Description
Name	Name of the URL category.
URL	Specified URL. Enter a URL on each line. You can add the wildcard (*) indicating any character to the start or end of the URL.

Copyright © Huawei Technologies Co., Ltd.

Figure 2-170 Create URL Classification



b. Click **OK**.

– Modifying a user-defined URL category

a. Select **User-defined Classification** in **URL Classification** and click .

b. In the **Modify URL Classification** dialog box, modify the parameters, among which **Name** cannot be changed.

c. Click **OK**. The URL category is modified.

– Deleting a user-defined URL category

a. Select **User-defined Classification** in **URL Classification** and click **Delete**.

b. In the dialog box that is displayed, click **OK**. The user-defined URL category is deleted.

- Committing the configuration

  After the preceding configurations are complete, click **Submit** to make the configurations take effect. In the dialog box that is displayed, click **OK**.

----End

2.15.3.4 Numerical

Context

You can view intrusion defense statistics to check detection and defense records on the network threats such as Trojan horses and worm viruses. In this way, you

 Copyright © Huawei Technologies Co., Ltd.

can learn about the historical and current threat events and adjust the security policy or take defense measures.

You can view URL filtering statistics to know statistics about URLs that users access or attempt to access and match the URL whitelist and blacklist.

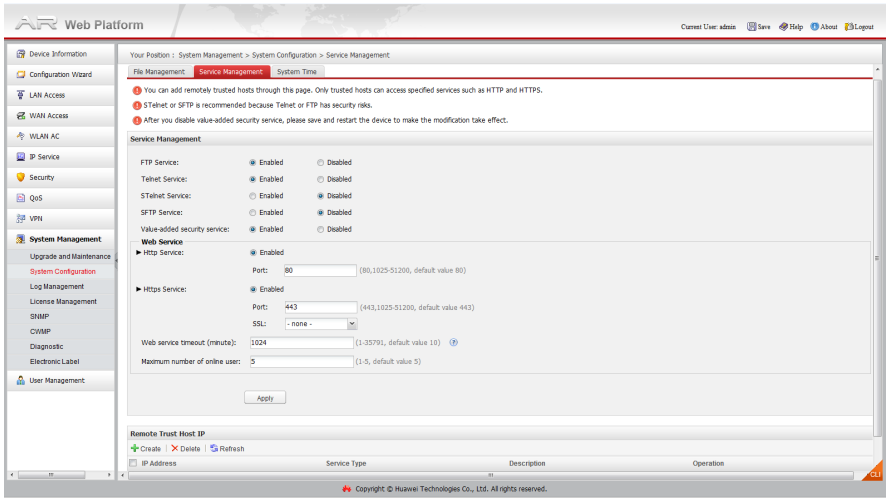
Prerequisite

To use the deep security function, you must enable it. By default, the deep security function is disabled.

1. Open the **Service Management** page.

   Log in to the web system, choose **System Management** > **System Configuration** > **Service Management** to open the **Service Management** page, as shown in **Figure 2-171**.

   Figure 2-171 Service Management tab page



2. Enable or disable deep security.
   - Enable deep security.

     In the **Service Management** area, click **Enabled** > **Apply** of **Value-added security service** to enable the deep security function.
   - Disable deep security.

     To disable deep security, click **Disable** and **Apply**, and restart the device.

     After the device restarts, the deep security configurations are deleted.

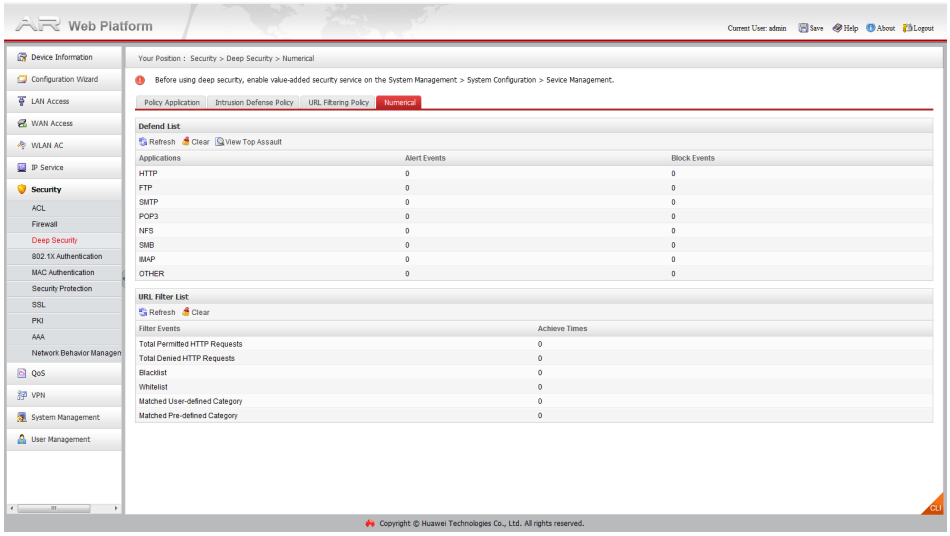
Procedure

- Intrusion defense list
  - Viewing the intrusion defense list

  a. Access the **Numerical** tab page, as shown in **Figure 2-172**.

     Log in to the tab page**Deep Security** and choose **Numerical**.

Figure 2-172 Numerical tab page



b. In the **Defend List** area, click **Refresh**.

Current statistics about intrusions on the device are displayed in the **Defend List** area. **Table 2-136** describes the parameters in the **Defend List** area.

Table 2-136 Intrusion defense list parameters

Parameter	Description
Applications	Application type of an intrusion detected by the intrusion defense policy.
Alert Events	Number of alarm events detected by the intrusion defense policy.
Block Events	Number of block events detected by the intrusion defense policy.

– Viewing top intrusions

a. In the **Defend List** area, click **View Top Assault**. Detailed information about intrusions is displayed. **Table 2-137** describes the parameters, as shown in **Figure 2-173**.

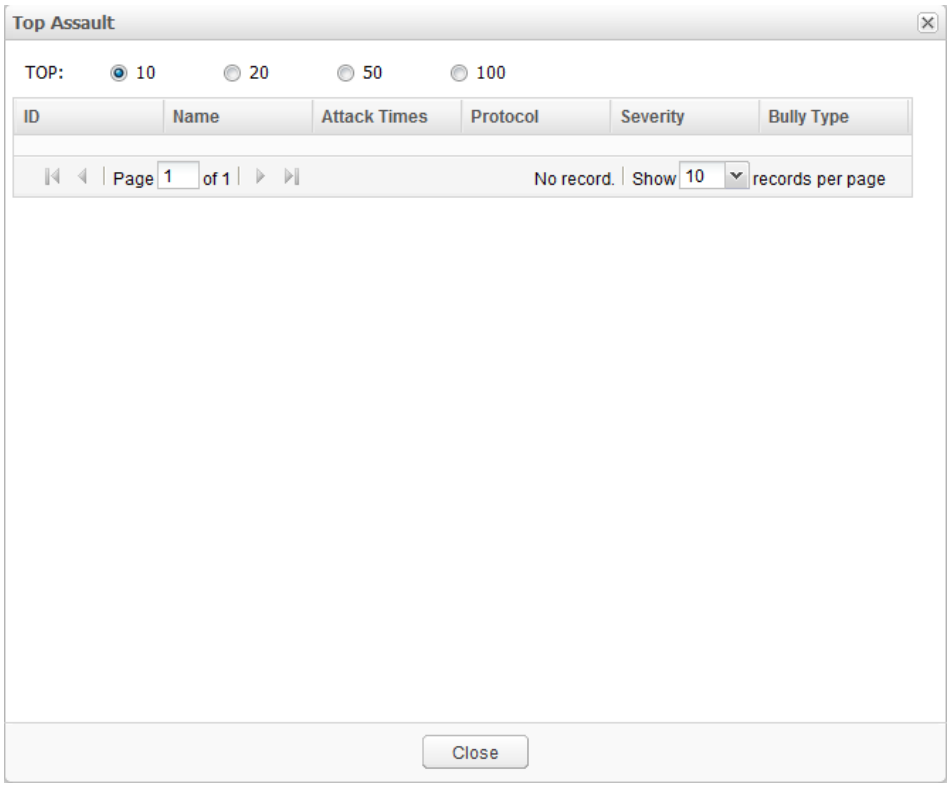
 Copyright © Huawei Technologies Co., Ltd.

Table 2-137 Intrusion parameters

Parameter	Description
TOP Assault	Number of intrusions whose detailed information is to be queried, such as 10, 20, 50, or 100. For example, when this parameter is set to 10, detailed information about the top 10 intrusions is displayed in the **TOP Assault** area.
ID	Signature ID of an intrusion detected by the intrusion defense policy.
Name	Signature name of an intrusion detected by the intrusion defense policy. Click **Name**. The **Predefined Signature Details** page is displayed. You can view detailed information about intrusions on this page.
Attack Times	Number of intrusions detected by the intrusion defense policy.
Protocol	Protocol of an intrusion detected by the intrusion defense policy.
Severity	Severity of an intrusion detected by the intrusion defense policy.
Bully Type	Threat type of an intrusion detected by the intrusion defense policy.

Copyright © Huawei Technologies Co., Ltd.

Figure 2-173 TOP Assault



  - Clearing the intrusion defense list
  a. In the **Defend List** area, click **Clear**. In the dialog box that is displayed, click **OK**. Current intrusion defense statistics are cleared.

- URL filtering list
  - Viewing the URL filtering list
  a. In the **URL Filter List** area, click **Refresh**.

     Current URL filtering statistics on the device are displayed in the **URL Filter List** area. **Table 2-138** describes the parameters.

     Table 2-138 URL filtering statistics parameters

Parameter	Description
Filter Events	Type of users' HTTP request packets detected by the URL filtering policy.
Achieve Times	Number of times that the URLs in users' HTTP request packets match filtering rules.

  - Clearing the URL filtering list
  a. In the **URL Filter List** area, click **Clear**. In the dialog box that is displayed, click **OK**. Current URL filtering statistics are cleared.

----End

Copyright © Huawei Technologies Co., Ltd.

2.15.4 Security Protection

2.15.4.1 ACL Filtering

Context

An ACL is a set of rules that can only differentiate packets.

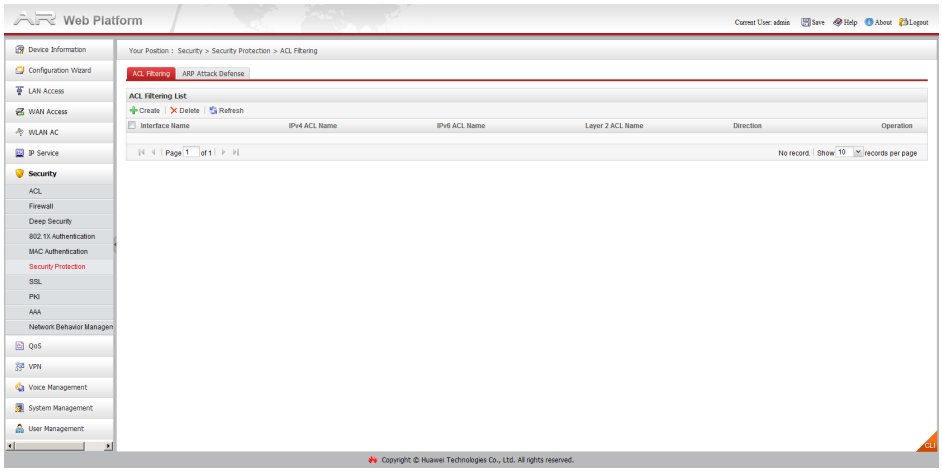
After ACLs are configured, you can configure ACL filtering to apply the ACLs so that packets are filtered.

Procedure

- Creating an ACL filtering rule
  a. Access the **ACL Filtering** tab page.

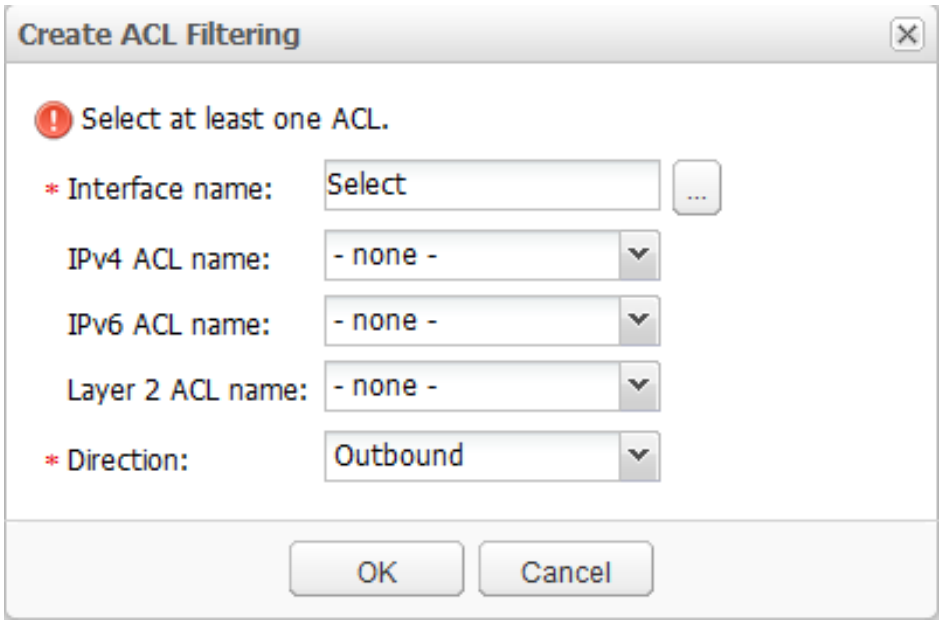
     Log in to the web platform and choose **Security** > **Security Protection** > **ACL Filtering**, as shown in **Figure 2-174**.

     Figure 2-174 ACL Filtering

  b. Click **Create** and set parameters in the **Create ACL Filtering** dialog box as shown in **Figure 2-175**. **Table 2-139** describes the parameters.

Figure 2-175 Create ACL Filtering



c. Click **OK**. An ACL filtering rule is added to the ACL filtering list.

Table 2-139 ACL filtering rule parameters

Parameter	Description
Interface name	Name of the interface where an ACL filtering rule is applied.
IPv4 ACL name	Name of a IPv4 ACL to apply. **NOTE** You can select a created **basic ACL** or **advanced ACL** from the **ACL name** drop-down list box.
IPv6 ACL name	Name of a IPv6 ACL to apply. **NOTE** You can select a created **basic ACL** or **advanced ACL** from the **ACL name** drop-down list box.
Layer 2 ACL name	Name of a layer 2 ACL to apply. **NOTE** You can select a created **Layer 2 ACL** from the **ACL name** drop-down list box.
Direction	Direction of the interface where an ACL filtering rule is applied.

- Modifying an ACL filtering rule
  a. Access the **ACL Filtering** tab page.

 Copyright © Huawei Technologies Co., Ltd.

Log in to the web platform and choose **Security** > **Security Protection** > **ACL Filtering**.

b. Click  of an ACL filtering rule.

c. In the **Modify ACL Filtering** dialog box, modify the parameters listed in **Table 2-139**. The parameters are the same as those in **Figure 2-175**. The parameters **Interface name** and **Direction** cannot be modified.

d. Click **OK**.

- Deleting an ACL filtering rule

a. Access the **ACL Filtering** tab page.

Log in to the web platform and choose **Security** > **Security Protection** > **ACL Filtering**.

b. Select the check box of an ACL filtering rule and click **Delete**.

c. In the dialog box that is displayed, click **OK**.

----End

2.15.4.2 ARP Attack Defense

Context

To defend against ARP address spoofing attacks, configure ARP anti-spoofing. The mutually exclusive anti-spoofing modes **fixed-mac**, **fixed-all**, and **send-ack** are applicable to different scenarios:

- **fixed-mac** mode: When receiving an ARP packet, the device discards the packet if its MAC address matches no ARP entry. If the MAC address in the ARP packet matches an ARP entry but the port number or VLAN ID matches no ARP entry, the device updates the port number or VLAN ID mapping the MAC address in the ARP table. This mode applies to networks that use static IP addresses and have redundant links. When services are switched on the link, port information in the ARP entry can change rapidly.
- **fixed-all** mode: When the MAC address, port number, and VLAN ID of an ARP packet match an ARP entry, the device updates other information in the ARP entry. This mode applies to networks that use static IP addresses and have no redundant link, and users with the same IP address access the device using the same port.
- **send-ack** mode: When receiving an ARP packet with a changed MAC address, port number, or VLAN ID, the device does not immediately update the corresponding ARP entry. Instead, the device sends a unicast ARP Request packet to the user with the IP address mapping the original MAC address in the ARP entry, and determines whether to change the MAC address, VLAN ID, or port number in the ARP entry depending on the response from the user. This mode applies to networks that use dynamic IP addresses and have redundant links.

The device needs to process a large number of ARP packets, which increases the CPU load. The device also learns ARP entries from these packets, which causes ARP entry resources to be occupied by invalid ARP entries. As a result, the device cannot learn ARP entries from APR packets of authorized packets and communication is interrupted. The device updates ARP entries by learning bogus

 Copyright © Huawei Technologies Co., Ltd.

ARP packets, which leads to failures in communicating with authorized users. To address the problems, enable strict ARP learning.

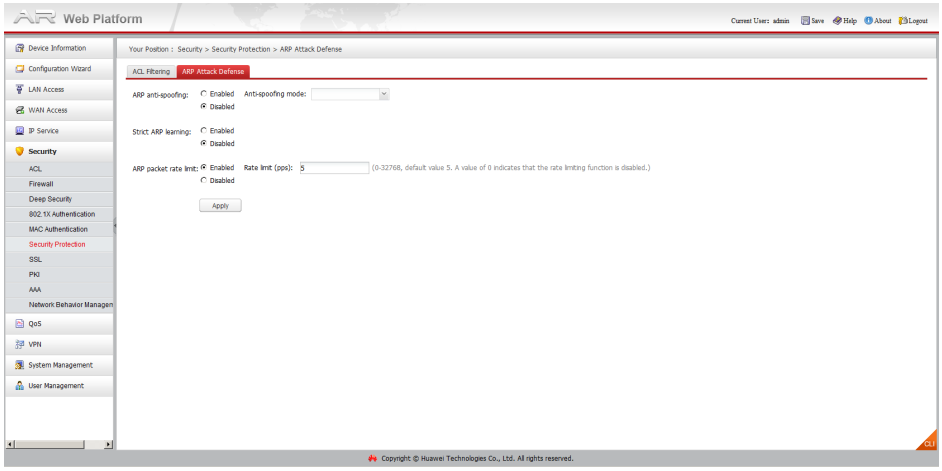
After strict ARP learning is enabled, the device learns ARP entries only from ARP Reply packets in response to the ARP Request packets sent by itself, and does not learn ARP entries from ARP Request packets from other devices. This method prevents most attacks from ARP packets.

The device may have no sufficient CPU resources to process other services when processing a large number of ARP packets. To protect CPU resources of the device, limit the rate of ARP packets.

Procedure

- Enabling ARP anti-spoofing
  a. Log in to the web platform and choose **Security** > **Security Protection** > **ARP Attack Defense**. The **ARP Attack Defense** tab page is displayed, as shown in **Figure 2-176**.

  Figure 2-176 ARP Attack Defense

  b. Set **ARP anti-spoofing** to **Enabled**, set **Anti-spoofing mode**, and click **Apply**. In the **Information** dialog box that is displayed, click **OK**.
- Disabling ARP anti-spoofing
  a. Log in to the web platform and choose **Security** > **Security Protection** > **ARP Attack Defense**. The **ARP Attack Defense** tab page is displayed.
  b. Set **ARP anti-spoofing** to **Disabled**, and click **Apply**. In the **Information** dialog box that is displayed, click **OK**.
- Enabling strict ARP learning
  a. Log in to the web platform and choose **Security** > **Security Protection** > **ARP Attack Defense**. The **ARP Attack Defense** tab page is displayed.
  b. Set **Strict ARP learning** to **Enabled**, and click **Apply**. In the **Information** dialog box that is displayed, click **OK**.
- Disabling strict ARP learning
  a. Log in to the web platform and choose **Security** > **Security Protection** > **ARP Attack Defense**. The **ARP Attack Defense** tab page is displayed.

 Copyright © Huawei Technologies Co., Ltd.

b. Set **Strict ARP learning** to **Disabled**, and click **Apply**. In the **Information** dialog box that is displayed, click **OK**.

- Enabling ARP packet rate limiting
  a. Log in to the web platform and choose **Security** > **Security Protection** > **ARP Attack Defense**. The **ARP Attack Defense** tab page is displayed.
  b. Set **ARP packet rate limit** to **Enabled**, enter a limit in the **Rate limit (pps)** text box, and click **Apply**. In the **Information** dialog box that is displayed, click **OK**.

  NOTE

  By default, ARP packet rate limiting is enabled; the default rate limit is 5 pps. When **Rate limit (pps)** is set to 0, ARP packet rate limiting is disabled.
- Disabling ARP packet rate limiting
  a. Log in to the web platform and choose **Security** > **Security Protection** > **ARP Attack Defense**. The **ARP Attack Defense** tab page is displayed.
  b. Set **ARP packet rate limit** to **Disabled**, and click **Apply**. In the **Information** dialog box that is displayed, click **OK**.

----End

2.15.5 SSL

Context

A router supports server Secure Sockets Layer (SSL) policies and client SSL policies.

- To use a router as an SSL server, configure a server SSL policy on the router. During an SSL handshake, the router uses SSL parameters in the server SSL policy to negotiate session parameters with an SSL client. After the handshake is complete, the router establishes a session with the client.
- To use a router as an SSL client, configure a client SSL policy on the router. During an SSL handshake, the router uses SSL parameters in the client SSL policy to negotiate session parameters with the SSL server. After the handshake is complete, the router establishes a session with the server.

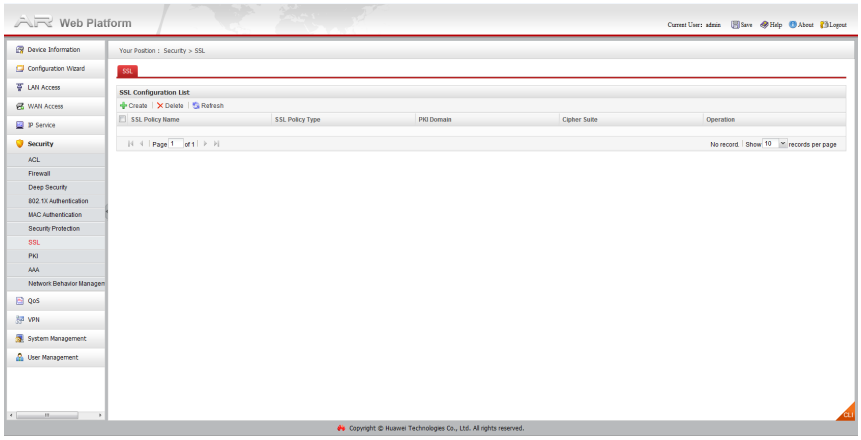
Procedure

- Creating an SSL policy
  - Creating a server SSL policy
    i. Access the **SSL** tab page.

    Log in to the web platform and choose **Security** > **SSL**. As shown in **Figure 2-177**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-177 SSL



ii. Click **Create** and set parameters in the **Create SSL Policy** dialog box that is displayed. Set **SSL policy type** to **Server**. **Table 2-140** describes other parameters. As shown in **Figure 2-178**.

iii. Click **OK**. A server SSL policy is added to the SSL policy list.

Figure 2-178 Create SSL Policy

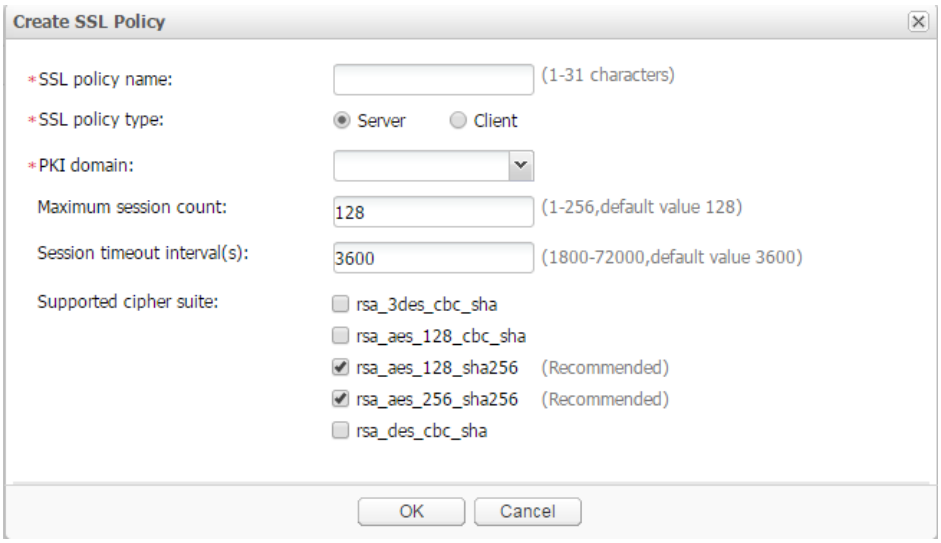


Table 2-140 Server SSL policy parameters

Parameter	Description
SSL policy name	Name of an SSL policy. The value is a string of case-sensitive characters without spaces.
SSL policy type	Choose SSL policy type, the type is Server.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
PKI domain	Name of a PKI domain. For details about the PKI domain configuration, see **PKI**.
Maximum session count	Maximum number of sessions that can be saved on the SSL server.
Session timeout interval(s)	Timeout period of a saved session. The value is an integer, in seconds.
Supported cipher suite	Cipher suite supported by the server SSL policy.

- Creating a client SSL policy
  i. Access the **SSL** tab page.
     Log in to the web platform and choose **Security** > **SSL**.
  ii. Click **Create** and set parameters in the **Create SSL Policy** dialog box that is displayed. Set **SSL policy type** to **Client**. **Table 2-141** describes other parameters. As shown in **Figure 2-179**.
  iii. Click **OK**. A client SSL policy is added to the SSL policy list.

Figure 2-179 Create SSL Policy

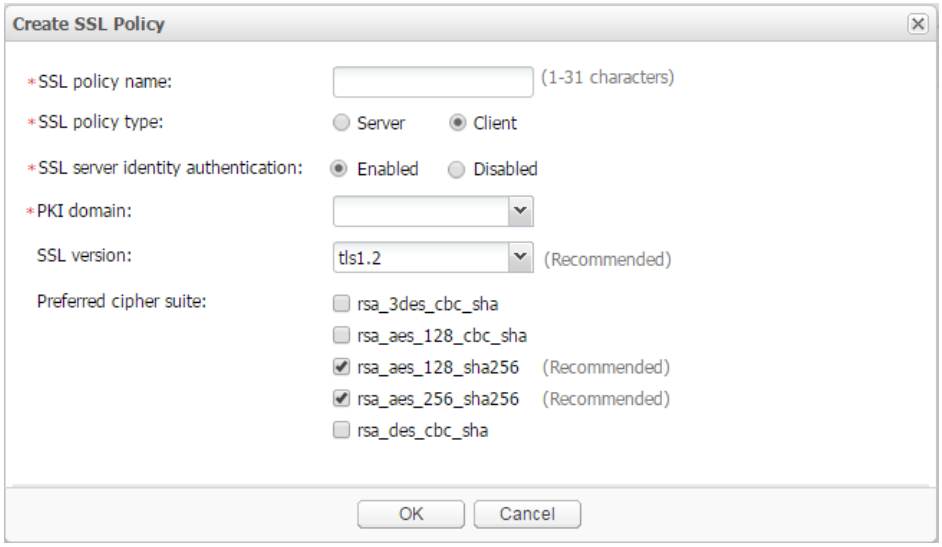


Table 2-141 Client SSL policy parameters

Parameter	Description
SSL policy name	Name of an SSL policy. The value is a string of case-sensitive characters without spaces.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
SSL policy type	Choose SSL policy type, the type is Client.
SSL server identity authentication	Whether to enable SSL server identity authentication.
PKI domain	Name of a PKI domain. For details about the PKI domain configuration, see **PKI**.
SSL version	SSL protocol version.
Preferred cipher suite	Cipher suite used by the client SSL policy.

- Modifying an SSL policy
  a. Access the **SSL** tab page.

     Log in to the web platform and choose **Security** > **SSL**.
  b. Click  of an SSL policy in the **SSL Configuration List** area.
  c. In the **Modify SSL Policy** dialog box that is displayed, modify parameters listed in **Table 2-140** or **Table 2-141**. The parameter **SSL policy name** and **SSL policy type** cannot be modified. The parameters are the same as those in **Figure 2-179**
  d. Click **OK**.
- Deleting an SSL policy
  a. Access the **SSL** tab page.

     Log in to the web platform and choose **Security** > **SSL**.
  b. Select an SSL policy and click **Delete**. In the **Information** dialog box that is displayed, click **OK**.

----End

2.15.6 PKI

2.15.6.1 PKI Entity

Context

A certificate binds a public key to a set of information that uniquely identifies a public key interface (PKI) entity. The parameters of an entity indicate the identity information of the entity. A Certificate Authority (CA) uniquely identifies a certificate applicant based on identity information provided by an entity.

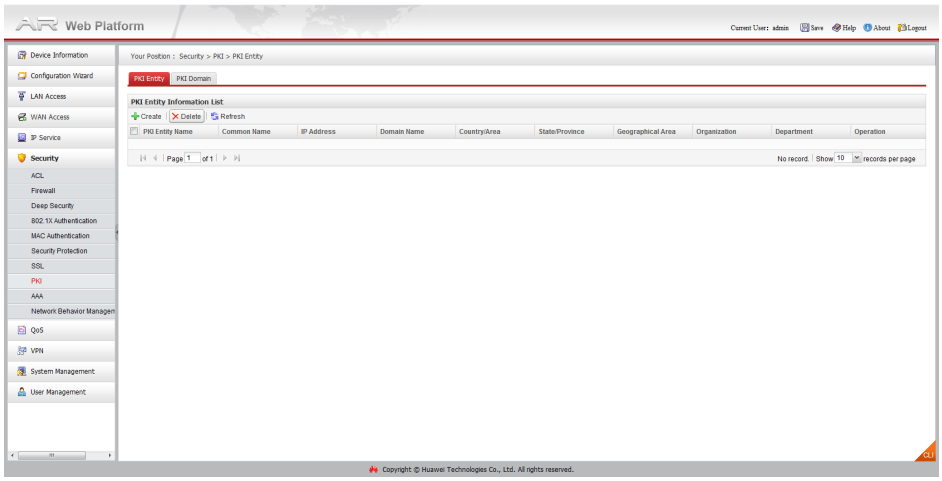
Procedure

- Creating a PKI entity
  a. Access the **PKI Entity** tab page.

     Log in to the web platform and choose **Security** > **PKI** > **PKI Entity**. As shown in **Figure 2-180**.

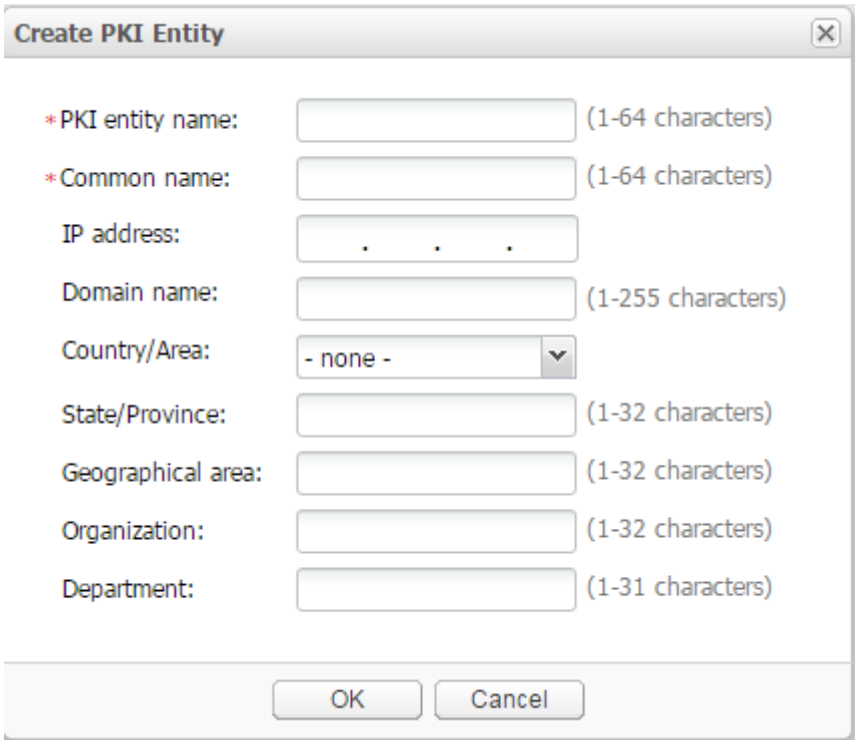
Copyright © Huawei Technologies Co., Ltd.

Figure 2-180 PKI Entity



b. Click **Create** and set parameters in the **Create PKI Entity** dialog box that is displayed. **Table 2-142** describes the parameters. As shown in **Figure 2-181**.

Figure 2-181 Create PKI Entity



 Copyright © Huawei Technologies Co., Ltd.

Table 2-142 PKI entity parameters

Parameter	Description
PKI entity name	Name of a PKI entity.
Common name	Common name of a PKI entity.
IP address	IP address of a PKI entity.
Domain name	Fully qualified domain name (FQDN) of a PKI entity.
Country/Area	Country name or province name of a PKI entity.
State/Province	State name or province name of a PKI entity.
Geographical area	Geographic area of a PKI entity.
Organization	Organization name of a PKI entity.
Department	Department name of a PKI entity.

c. Click **OK**.

- Modifying a PKI entity
  a. Access the **PKI Entity** tab page.

     Log in to the web platform and choose **Security** > **PKI** > **PKI Entity**.

  b. Select a PKI entity in the **PKI Entity Information List** area, and click  .
  c. In the **Modify PKI Entity** dialog box that is displayed, modify the parameters. The parameter **PKI entity name** cannot be modified. The parameters are the same as those in **Figure 2-181**
  d. Click **OK**.
- Deleting a PKI entity
  a. Access the **PKI Entity** tab page.

     Log in to the web platform and choose **Security** > **PKI** > **PKI Entity**.

  b. Select the check box of a PKI entity and click **Delete**.
  c. In the dialog box that is displayed, click **OK**.

     NOTE

     When a PKI entity is referenced by a PKI domain, delete the PKI entity from the PKI domain before you delete the PKI entity.

----End

Copyright © Huawei Technologies Co., Ltd.

2.15.6.2 PKI Domain

Context

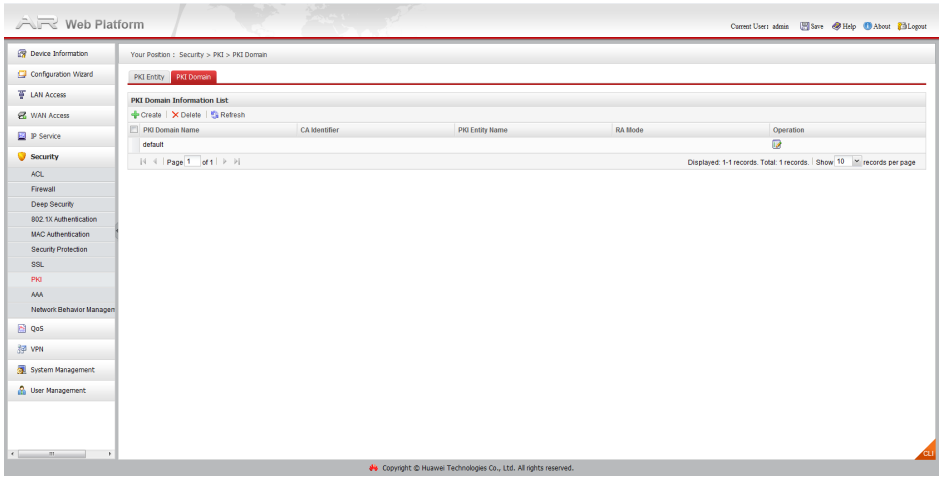
Before an entity applies for a certificate, some enrollment information must be configured. The collection of the enrollment information is called the PKI domain of an entity.

Procedure

- Creating a PKI domain
  a. Access the **PKI Domain** tab page.

     Log in to the web platform and choose **Security** > **PKI** > **PKI Domain**. As shown in **Figure 2-182**.

     Figure 2-182 PKI Domain

  b. Click **Create** and set parameters in the **Create PKI Domain** dialog box that is displayed. **Table 2-143** describes the parameters. As shown in **Figure 2-183**.

Figure 2-183 Create PKI Domain

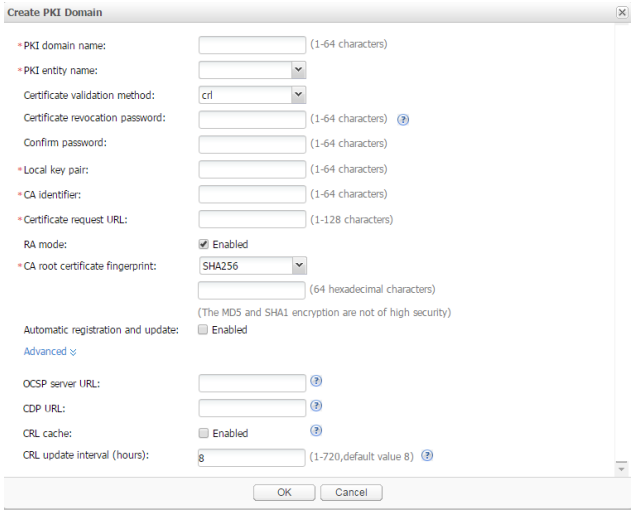


Table 2-143 PKI domain parameters

Parameter	Description
PKI domain name	Name of a PKI domain.
PKI entity name	Name of a created PKI entity.
Certificate validation method	Certificate check mode of crl, ocsp, or none.
Certificate revocation password	Revocation password of the certificate. The password must meet complexity requirements. A password should consist of at least 6 characters, and contain at least two types of the following: lowercase letters, uppercase letters, numerals, special characters (such as ! $ # %). The password cannot contain spaces and question marks.
Confirm password	Confirmed revocation password of the certificate.
Automatic registration and update	Whether to enable the automatic certificate enrollment and update function.
Local key pair	The name of local key pair.
CA identifier	ID of a CA.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Certificate request URL	Enrollment URL. The URL is in the format of http://*server_location*/*ca_script_location*. The *server_location* field supports only the IP address format and the *ca_script_location* field is the path where CA's application script is located, for example, http://10.137.145.158:8080/certsrv/mscep/mscep.dll.
RA mode	Whether to enable the registration authority (RA) mode.
CA root certificate fingerprint	CA certificate fingerprint used in CA certificate authentication. The options are as follows: • MD5: message digest algorithm 5 • SHA1: secure hash algorithm 1 • SHA2: secure hash algorithm 2 The default value is SHA2.
OCSP server URL	URL of the Online Certificate Status Protocol (OCSP) server.
CDP URL	CRL distribution point (CDP) URL. CRL refers to certificate revocation list.
CRL cache	Whether to use the buffered CRL in the PKI domain.
CRL update interval (hours)	Interval for updating the CRL.

c. Click **OK**.

- Modifying a PKI domain
  a. Access the **PKI Domain** tab page.

     Log in to the web platform and choose **Security** > **PKI** > **PKI Domain**.
  b. Select a PKI domain in the **PKI Domain Information List** area, and click  .
  c. In the **Modify PKI Domain** dialog box that is displayed, modify the parameters. The parameter **PKI domain name** cannot be modified. The parameters are the same as those in **Figure 2-183**
  d. Click **OK**.
- Deleting a PKI domain
  a. Access the **PKI Domain** tab page.

Copyright © Huawei Technologies Co., Ltd.

Log in to the web platform and choose **Security** > **PKI** > **PKI Domain**.

b. Select the check box of a PKI domain and click **Delete**.

c. In the dialog box that is displayed, click **OK**.

----End

2.15.7 AAA

2.15.7.1 AAA Scheme

Context

Authentication, Authorization, and Accounting (AAA) provides a management mechanism for network security.

AAA provides the following functions:

- Authentication: determines the users who can access the network. Authentication modes are as follows:
  - Non-authentication: Users are trusted without the check on their validity. This mode is rarely used.
  - Local authentication: Information about users is configured on a network access server (NAS). Local authentication features fast processing and low operation cost, whereas the amount of information that can be stored is limited by the hardware capacity of the device.
  - Remote authentication: Information about users is configured on an authentication server. Remote authentication supports the Remote Authentication Dial In User Service (RADIUS) protocol and the Huawei Terminal Access Controller Access Control System (HWTACACS) protocol.
- Authorization: authorizes users to use particular services. Authorization modes are as follows:
  - Non-authorization: Users are not authorized.
  - Local authorization: Users are authorized based on related attributes of the local user accounts configured on the NAS.
  - HWTACACS authorization: A HWTACACS server authorizes users.
  - if-authenticated authorization: Users are authorized after the users pass the authentication in either local or remote authentication mode.
  - RADIUS authorization: Users pass the RADIUS authorization upon passing the RADIUS authentication. RADIUS integrates authentication and authorization. Therefore, RADIUS authorization cannot be performed separately.
- Accounting: records the use of network resources by users. Accounting modes are as following:
  - Non-accounting: Users are not charged.
  - Remote accounting: A RADIUS server or a HWTACACS server performs remote accounting.

 Copyright © Huawei Technologies Co., Ltd.

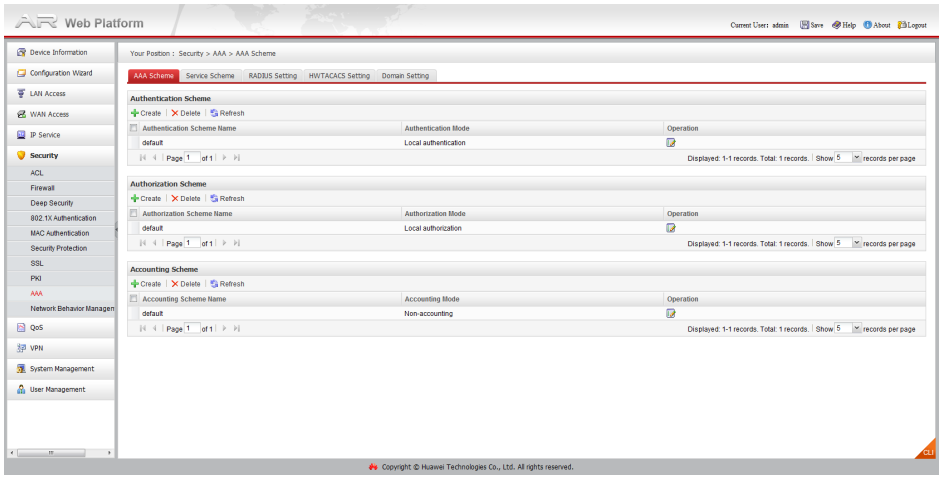
Procedure

- Authentication scheme
  - Creating an authentication scheme

  a. Access the **AAA Scheme** tab page.

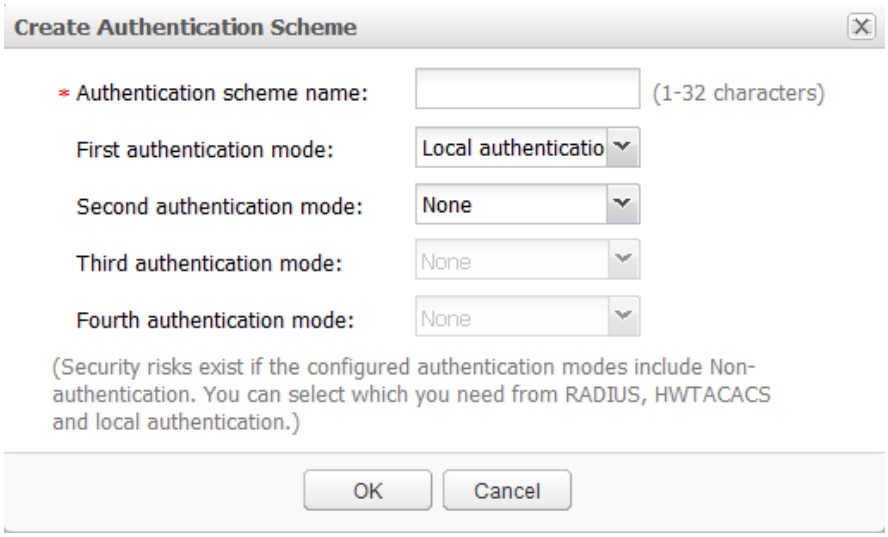
  Log in to the web platform and choose **Security** > **AAA** > **AAA Scheme**. As shown in **Figure 2-184**.

  Figure 2-184 AAA Scheme



  b. Click **Create** in the **Authentication Scheme** area, and set parameters in the **Create Authentication Scheme** dialog box that is displayed. **Table 2-144** describes the parameters. As shown in **Figure 2-185**.

  Figure 2-185 Create Authentication Scheme



 Copyright © Huawei Technologies Co., Ltd.

Table 2-144 Authentication scheme parameters

Parameter	Description
Authentication scheme name	Name of an authentication scheme.
First authentication mode	The value can be RADIUS authentication, HWTACACS authentication, local authentication, or non-authentication. **NOTE** Security risks exist if the configured authentication modes include Non-authentication. You can select which you need from RADIUS, HWTACACS and local authentication.
Second authentication mode	The value can be a mode except the first authentication mode. When the authentication server of the first authentication mode does not respond, the second authentication mode is triggered. When the first authentication mode is non-authentication, the second authentication mode cannot be configured.
Third authentication mode	The value can be a mode except the first and second authentication modes. When the authentication servers of the first and second authentication modes do not respond, the third authentication mode is triggered. When the second authentication mode is non-authentication or not configured, the third authentication mode cannot be configured.
Fourth authentication mode	The parameter must be set to non-authentication. When the authentication servers of the first, second, and third authentication modes do not respond, the fourth authentication mode is triggered. When the third authentication mode is non-authentication or not configured, the fourth authentication mode cannot be configured.

Copyright © Huawei Technologies Co., Ltd.

c. Click **OK**.

– Modifying an authentication scheme

a. Access the **AAA Scheme** tab page.

Log in to the web platform and choose **Security** > **AAA** > **AAA Scheme**.

b. Select an authentication scheme in the **Authentication Scheme** area, and click .

c. In the **Modify Authentication Scheme** dialog box that is displayed, modify the parameters. The parameter **Authentication scheme name** cannot be modified. The parameters are the same as those in **Figure 2-185**

d. Click **OK**.

– Deleting an authentication scheme

a. Access the **AAA Scheme** tab page.

Log in to the web platform and choose **Security** > **AAA** > **AAA Scheme**.

b. Select the check box of an authentication scheme in the **Authentication Scheme** area, and click **Delete**.

c. In the dialog box that is displayed, click **OK**.

- Authorization scheme

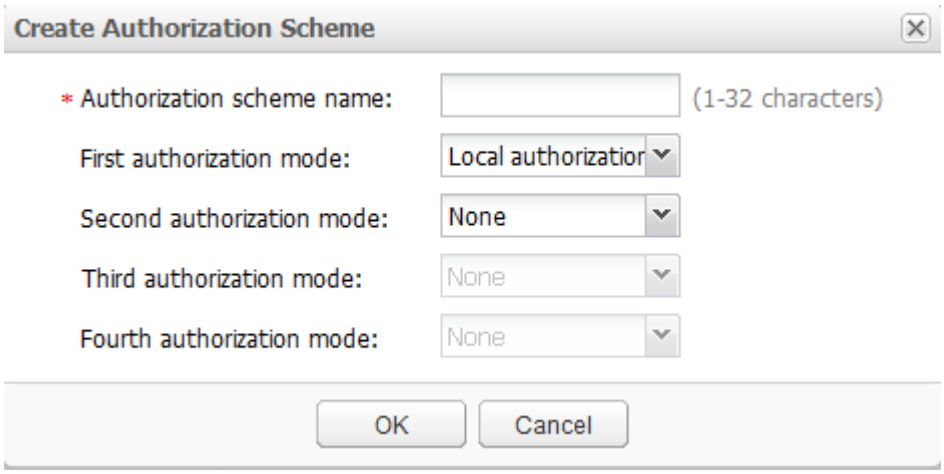
– Creating an authorization scheme

a. Access the **AAA Scheme** tab page.

Log in to the web platform and choose **Security** > **AAA** > **AAA Scheme**.

b. Click **Create** in the **Authorization Scheme** area, and set parameters in the **Create Authorization Scheme** dialog box that is displayed. **Table 2-145** describes the parameters. As shown in **Figure 2-186**.

Figure 2-186 Create Authorization Scheme



 Copyright © Huawei Technologies Co., Ltd.

Table 2-145 Authorization scheme parameters

Parameter	Description
Authorization scheme name	Name of an authorization scheme.
First authorization mode	The value can be IF-AUTHENTICATED authorization, HWTACACS authorization, local authorization, or non-authorization.
Second authorization mode	The value can be a mode except the first authorization mode. When the authorization server of the first authorization mode does not respond, the second authorization mode is triggered. When the first authorization mode is non-authorization, the second authorization mode cannot be configured.
Third authorization mode	The value can be a mode except the first and second authorization modes. When the authorization servers of the first and second authorization modes do not respond, the third authorization mode is triggered. When the second authorization mode is non-authorization or not configured, the third authorization mode cannot be configured.
Fourth authorization mode	The parameter must be set to non-authorization. When the authorization servers of the first, second, and third authorization modes do not respond, the fourth authorization mode is triggered. When the third authorization mode is non-authorization or not configured, the fourth authorization mode cannot be configured.

c. Click **OK**.

– Modifying an authorization scheme

a. Access the **AAA Scheme** tab page.

Log in to the web platform and choose **Security** > **AAA** > **AAA Scheme**.

Copyright © Huawei Technologies Co., Ltd.

b. Select an authorization scheme in the **Authorization Scheme** area, and click .

c. In the **Modify Authorization Scheme** dialog box that is displayed, modify the parameters. The parameter **Authorization scheme name** cannot be modified. The parameters are the same as those in **Figure 2-186**

d. Click **OK**.

– Deleting an authorization scheme

a. Access the **AAA Scheme** tab page.

Log in to the web platform and choose **Security** > **AAA** > **AAA Scheme**.

b. Select the check box of an authorization scheme in the **Authorization Scheme** area, and click **Delete**.

c. In the dialog box that is displayed, click **OK**.

- Accounting scheme

– Creating an accounting scheme

a. Access the **AAA Scheme** tab page.

Log in to the web platform and choose **Security** > **AAA** > **AAA Scheme**.

b. Click **Create** in the **Accounting Scheme** area, and set parameters in the **Create Accounting Scheme** dialog box that is displayed. **Table 2-146** describes the parameters. As shown in **Figure 2-187**.

c. Click **OK**.

Figure 2-187 Create Accounting Scheme

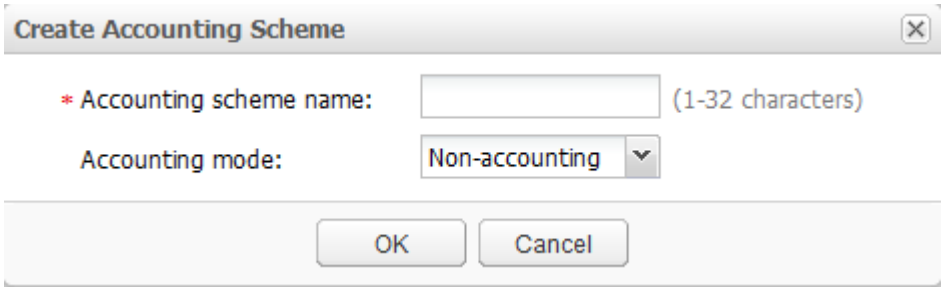


Table 2-146 Accounting scheme parameters

Parameter	Description
Accounting scheme name	Name of an accounting scheme.
Accounting mode	The value can be RADIUS accounting, HWTACACS accounting, or non-accounting.

– Modifying an accounting scheme

Copyright © Huawei Technologies Co., Ltd.

a. Access the **AAA Scheme** tab page.

Log in to the web platform and choose **Security** > **AAA** > **AAA Scheme**.

b. Select an accounting scheme in the **Accounting Scheme** area, and click .

c. In the **Modify Accounting Scheme** dialog box that is displayed, modify the parameters. The parameter **Accounting scheme name** cannot be modified. The parameters are the same as those in **Figure 2-187**

d. Click **OK**.

– Deleting an accounting scheme

a. Access the **AAA Scheme** tab page.

Log in to the web platform and choose **Security** > **AAA** > **AAA Scheme**.

b. Select the check box of an accounting scheme in the **Accounting Scheme** area, and click **Delete**.

c. In the dialog box that is displayed, click **OK**.

----End

2.15.7.2 Service Scheme

Context

Access users must obtain authorization information before going online. Authorization information about users can be managed by configuring a service scheme.

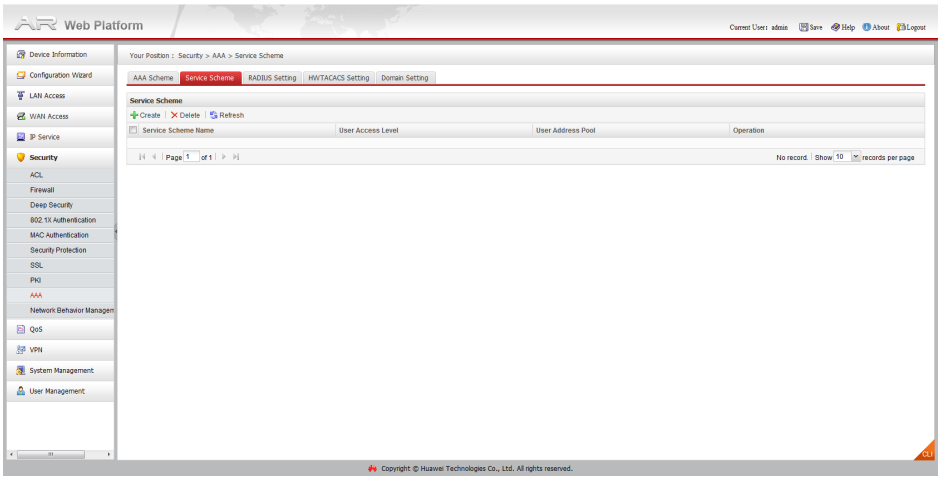
Procedure

- Creating a service scheme

a. Access the **Service Scheme** tab page.

Log in to the web platform and choose **Security** > **AAA** > **Service Scheme**. As shown in **Figure 2-188**.

Figure 2-188 Service Scheme



b. Click **Create** and set parameters in the **Create Service Scheme** dialog box that is displayed. **Table 2-147** describes the parameters. As shown in **Figure 2-189**.

Figure 2-189 Create Service Scheme

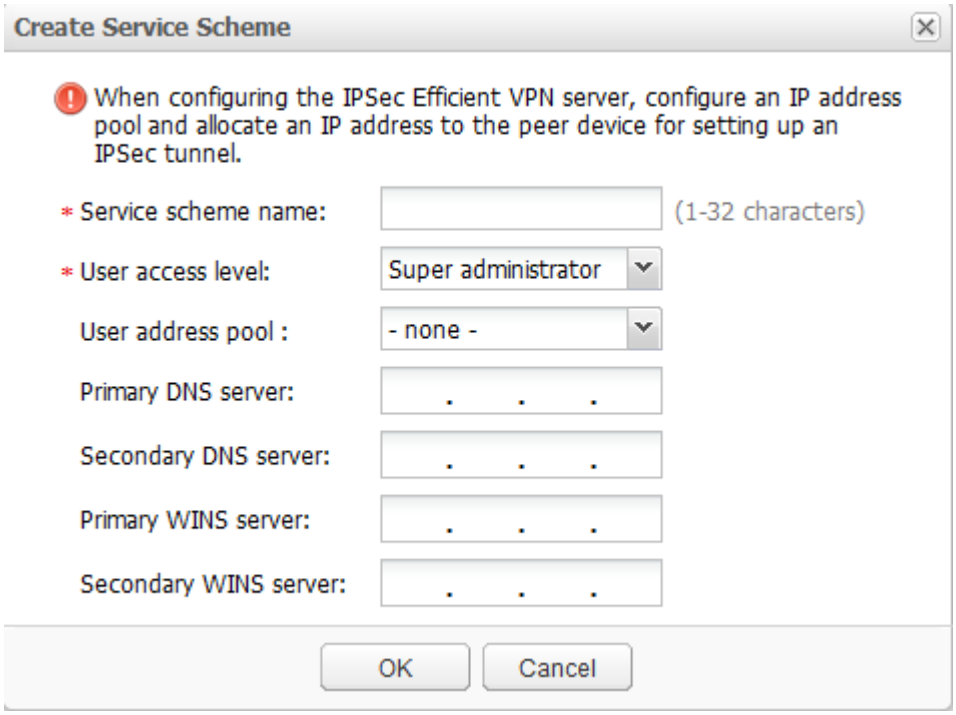


Table 2-147 Service scheme parameters

Parameter	Description
Service scheme name	Name of a service scheme.
User access level	The value can be common administrator, enterprise administrator and super administrator.
User address pool	Created user address pool. Alternatively, you can create a user address pool by selecting **Create** from the **User address pool** drop-down list box and setting the user address pool name, user address pool IP address and mask, and default gateway on the **Create User Address Pool** dialog box that is displayed.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Primary DNS server	IP address of the primary DNS server.
Secondary DNS server	IP address of the secondary DNS server.
Primary WINS server	IP address of the primary WINS server.
Secondary WINS server	IP address of the secondary WINS server.

c. Click **OK**.

- Modifying a service scheme
  a. Access the **Service Scheme** tab page.

     Log in to the web platform and choose **Security** > **AAA** > **Service Scheme**.

  b. Select a service scheme in the **Service Scheme** area, and click  .
  c. In the **Modify Service Scheme** dialog box that is displayed, modify the parameters. The parameter **Service scheme name** cannot be modified. The parameters are the same as those in **Figure 2-189**
  d. Click **OK**.
- Deleting a service scheme
  a. Access the **Service Scheme** tab page.

     Log in to the web platform and choose **Security** > **AAA** > **Service Scheme**.

  b. Select the check box of a service scheme in the **Service Scheme** area, and click **Delete**.
  c. In the dialog box that is displayed, click **OK**.

----End

2.15.7.3 RADIUS Setting

Context

RADIUS protects a network from unauthorized access. It is often used on the networks that require high security and remote user access control.

0

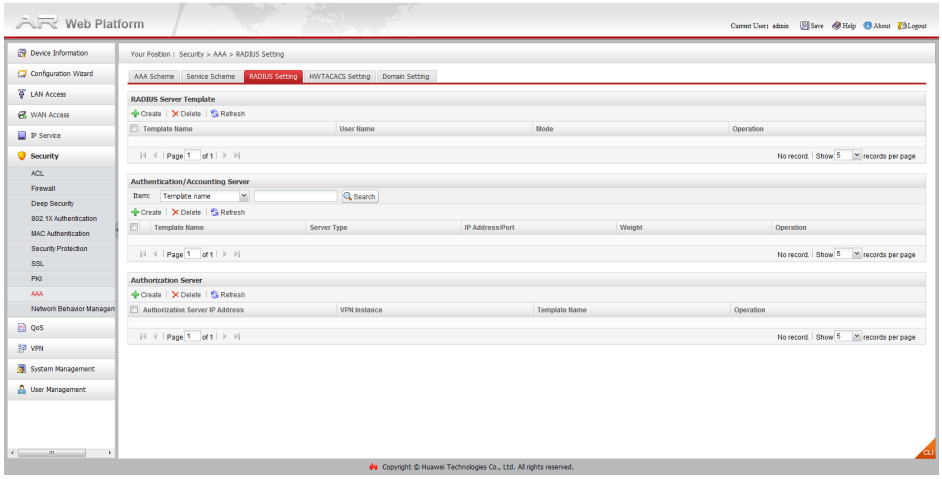
Procedure

- RADIUS server template
  – Creating a RADIUS server template
  a. Access the **RADIUS Setting** tab page.

Copyright © Huawei Technologies Co., Ltd.

Log in to the web platform and choose **Security** > **AAA** > **RADIUS Setting**. As shown in **Figure 2-190**.

Figure 2-190 RADIUS Setting



b. Click **Create** in the **RADIUS Server Template** area, and set parameters in the **Create RADIUS Server Template** dialog box that is displayed. **Table 2-148** describes the parameters. As shown in **Figure 2-191**.

Figure 2-191 Create RADIUS Server Template

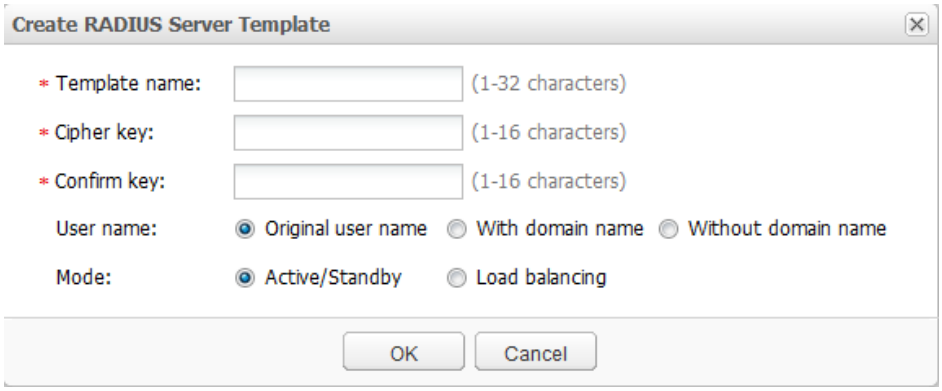


Table 2-148 Parameters for creating a RADIUS server template

Parameter	Description
Template name	Name of a RADIUS server template.
Cipher key	Shared key for the RADIUS server. The shared key is used to encrypt the password and generate the response authenticator.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Confirm key	Confirmed shared key of the RADIUS server.
User name	Whether the packets sent by the device to the RADIUS server contain domain names. • Original user name • With domain name • Without domain name **NOTE** If the RADIUS server does not accept the user names carrying domain names, select **Without domain name**. Then the device removes domain names from the user names.
Mode	RADIUS server mode: • Active/Standby: When multiple RADIUS authentication or accounting servers are configured, the server with the highest weight becomes the active server, and the other servers are backup servers. Among the backup servers, the servers with higher weight have higher priority. If the servers have the same weights, they are selected in the sequence in which they were configured. • Load balancing: The device distributes authentication or accounting packets to the RADIUS servers based on the weights of the servers. For example, the weights of server A, server B, and server C are 80, 80, and 40. The possibilities that the device sends packets to the servers are as follows: 1. Server A: 80/(80 + 80 + 40) = 40% 2. Server B: 80/(80 + 80 + 40) = 40% 3. Server C: 40/(80 + 80 + 40) = 20%

Copyright © Huawei Technologies Co., Ltd.

c. Click **OK**.

– Modifying a RADIUS server template

a. Access the **RADIUS Setting** tab page.

Log in to the web platform and choose **Security** > **AAA** > **RADIUS Setting**.

b. Select a RADIUS server template in the **RADIUS Server Template** area, and click .

c. In the **Modify RADIUS Server Template** dialog box that is displayed, modify the parameters. The parameter **Template name** cannot be modified. The parameters are the same as those in **Figure 2-191**

d. Click **OK**.

– Deleting a RADIUS server template

a. Access the **RADIUS Setting** tab page.

Log in to the web platform and choose **Security** > **AAA** > **RADIUS Setting**.

b. Select the check box of a RADIUS server template in the **RADIUS Server Template** area, and click **Delete**.

c. In the dialog box that is displayed, click **OK**.

- Authentication/Accounting server

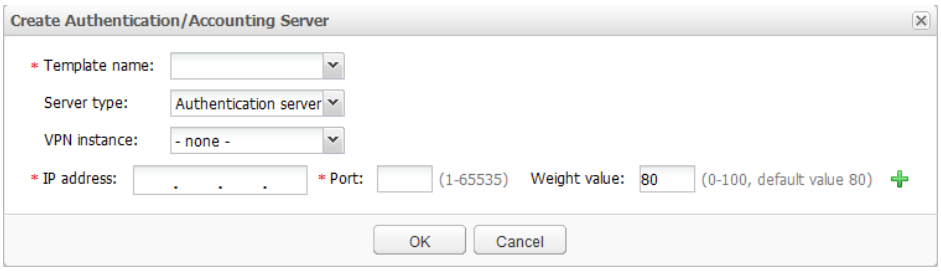
– Creating an authentication or accounting server

a. Access the **RADIUS Setting** tab page.

Log in to the web platform and choose **Security** > **AAA** > **RADIUS Setting**.

b. Click **Create** in the **Authentication/Accounting Server** area, and set parameters in the **Create Authentication/Accounting Server** dialog box that is displayed. **Table 2-149** describes the parameters. As shown in **Figure 2-192**.

Figure 2-192 Create Authentication/Accounting Server



 Copyright © Huawei Technologies Co., Ltd.

Table 2-149 Parameters for creating an authentication or accounting server

Parameter	Description
Template name	Name of the created RADIUS server template.
Server type	RADIUS server type: authentication or accounting server.
VPN instance	Created VPN instance.
IP address	IP address of the RADIUS authentication/accounting server.
Port	Port number of the RADIUS authentication/accounting server.
Weight value	Weight of the RADIUS authentication/accounting server.

NOTE

You can quickly search for the created authentication or accounting servers based on the specified criteria.

A maximum of four RADIUS servers can be configured in a RADIUS template. The device sends authentication or accounting packets to the servers in the configured mode.

c. Click **OK**.

– Modifying an authentication or accounting server

a. Access the **RADIUS Setting** tab page.

Log in to the web platform and choose **Security** > **AAA** > **RADIUS Setting**.

b. Select an authentication or accounting server in the **Authentication/Accounting Server** area, and click  .

c. In the **Modify Authentication/Accounting Server** dialog box that is displayed, modify the parameters. The parameters **Template name** and **Server type** cannot be modified. The parameters are the same as those in **Figure 2-192**

d. Click **OK**.

– Deleting an authentication or accounting server

a. Access the **RADIUS Setting** tab page.

Log in to the web platform and choose **Security** > **AAA** > **RADIUS Setting**.

b. Select the check box of an authentication or accounting server in the **Authentication/Accounting Server** area, and click **Delete**.

Copyright © Huawei Technologies Co., Ltd.

c. In the dialog box that is displayed, click **OK**.

- Authorization server
  - Creating an authorization server

  a. Access the **RADIUS Setting** tab page.

  Log in to the web platform and choose **Security** > **AAA** > **RADIUS Setting**.

  b. Click **Create** in the **Authorization Server** area, and set parameters in the **Create Authorization Server** dialog box that is displayed. **Table 2-150** describes the parameters. As shown in **Figure 2-193**.

  Figure 2-193 Create Authorization Server

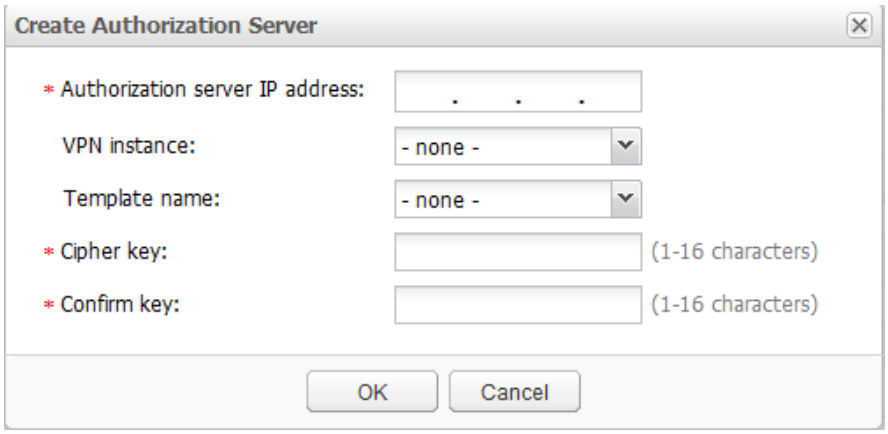


  Table 2-150 Parameters for creating an authorization server

Parameter	Description
Authorization server IP address	IP address of an authorization server.
VPN instance	Created VPN instance.
Template name	Name of the created RADIUS server template.
Cipher key	Shared key of the RADIUS authorization server.
Confirm key	Confirmed shared key of the RADIUS authorization server.

  c. Click **OK**.

  - Modifying an authorization server

  a. Access the **RADIUS Setting** tab page.

  Log in to the web platform and choose **Security** > **AAA** > **RADIUS Setting**.

Copyright © Huawei Technologies Co., Ltd.

b. Select an authorization server in the **Authorization Server** area, and click .

c. In the **Modify Authorization Server** dialog box that is displayed, modify the parameters. The parameters **Authorization server IP address** and **VPN instance** cannot be modified. The parameters are the same as those in **Figure 2-193**

d. Click **OK**.

– Deleting an authorization server

a. Access the **RADIUS Setting** tab page.

Log in to the web platform and choose **Security** > **AAA** > **RADIUS Setting**.

b. Select the check box of an authorization server in the **Authorization Server** area, and click **Delete**.

c. In the dialog box that is displayed, click **OK**.

----End

2.15.7.4 HWTACACS Setting

Context

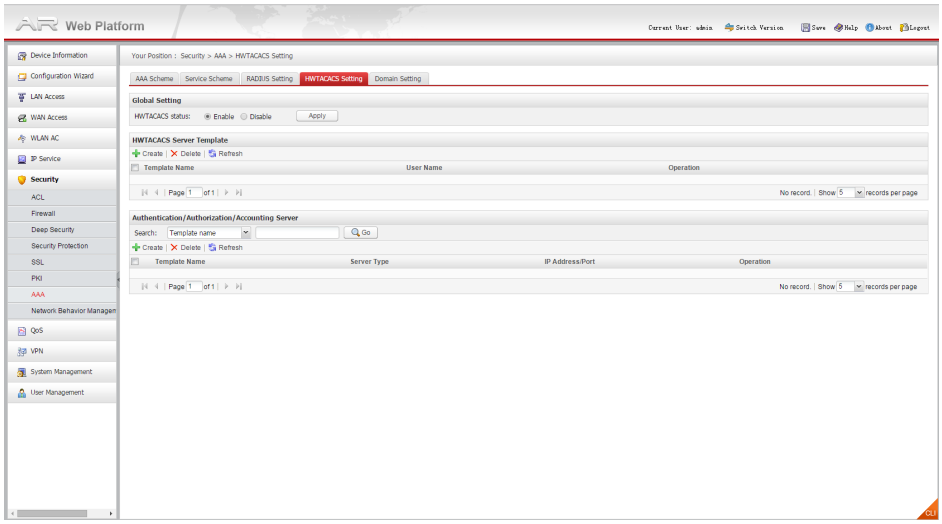
HWTACACS prevents unauthorized users from attacking a network and supports command-line authorization. Compared with RADIUS, HWTACACS is more reliable in transmission and encryption, and is more suitable for security control.

Procedure

- Global Setting

a. Log in to the web platform and choose **Security** > **AAA** > **HWTACACS Setting**, as shown in **Figure 2-194**.

Figure 2-194 HWTACACS Setting



b. Click **Enable** > **Apply** to enable global HWTACACS function.

- HWTACACS Server Template
  - Creating a HWTACACS server template

  a. Access the **HWTACACS Setting** tab page.

  Log in to the web platform and choose **Security** > **AAA** > **HWTACACS Setting**.

  b. Click **Create** in the **HWTACACS Server Template** area, and set parameters in the **Create HWTACACS Server Template** dialog box that is displayed. **Table 2-151** describes the parameters. As shown in **Figure 2-195**.

Figure 2-195 Create HWTACACS Server Template

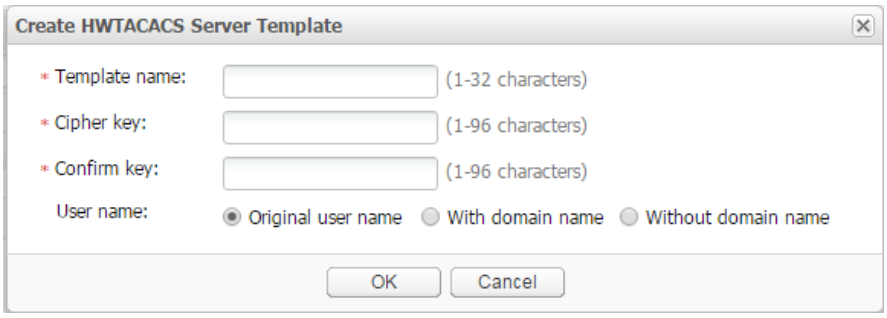


Table 2-151 Parameters for creating a HWTACACS server template

Parameter	Description
Template name	Name of a HWTACACS server template.
Cipher key	Shared key for the HWTACACS server. The shared key is used to encrypt the password and generate the response authenticator.
Confirm key	Confirmed shared key of the HWTACACS server.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
User name	Whether the packets sent by the device to the HWTACACS server contain domain names. • Original user name • With domain name • Without domain name **NOTE** If the HWTACACS server does not accept the user names carrying domain names, select **Without domain name**. Then the device removes domain names from the user names.

c. Click **OK**.

– Modifying a HWTACACS server template

a. Access the **HWTACACS Setting** tab page.

Log in to the web platform and choose **Security** > **AAA** > **HWTACACS Setting**.

b. Select the HWTACACS server template in the **HWTACACS Server Template** area, and click  .

c. In the **Modify HWTACACS Server Template** dialog box that is displayed, modify the parameters. The parameter **Template name** cannot be modified. The parameters are the same as those in **Figure 2-195**

d. Click **OK**.

– Deleting a HWTACACS server template

a. Access the **HWTACACS Setting** tab page.

Log in to the web platform and choose **Security** > **AAA** > **HWTACACS Setting**.

b. Select the check box of the HWTACACS server template in the **HWTACACS Server Template** area, and click **Delete**.

c. In the dialog box that is displayed, click **OK**.

- Authentication/Authorization/Accounting server

– Creating an authentication, authorization, or accounting server

a. Access the **HWTACACS Setting** tab page.

Log in to the web platform and choose **Security** > **AAA** > **HWTACACS Setting**.

b. Click **Create** in the **Authentication/Authorization/Accounting Server** area, and set parameters in the **Create Authentication/Authorization/Accounting Server** dialog box that is displayed. **Table 2-152** describes the parameters. As shown in **Figure 2-196**.

Copyright © Huawei Technologies Co., Ltd.

Figure 2-196 Create Authentication/Authorization/Accounting Server

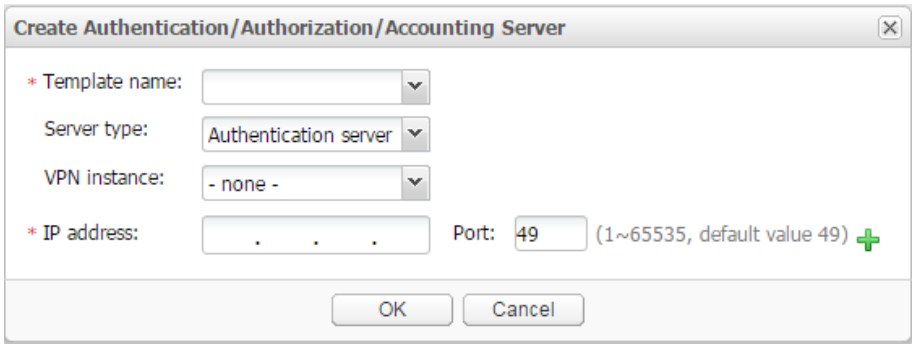


Table 2-152 Parameters for creating an authentication, authorization, or accounting server

Parameter	Description
Template name	Name of the created HWTACACS server template.
Server type	HWTACACS server type: authentication, authorization, or accounting server.
VPN instance	Created VPN instance.
IP address	IP address of the authentication, authorization, or accounting server.
Port	Port number of the authentication, authorization, or accounting server.

c. Click , adding the ip address, port number for the other authentication, authorization, or accounting server.

Addresses of three servers can be configured.

d. Click **OK**.

NOTE

You can quickly search for the created authentication, authorization, or accounting servers based on the specified criteria.

– Modifying an authentication, authorization, or accounting server

a. Access the **HWTACACS Setting** tab page.

Log in to the web platform and choose **Security** > **AAA** > **HWTACACS Setting**.

b. Select an authentication, authorization, or accounting server in the **Authentication/Authorization/Accounting Server** area, and click .

 Copyright © Huawei Technologies Co., Ltd.

c. In the **Modify Authentication/Authorization/Accounting Server** dialog box that is displayed, modify the parameters. The parameters **Template name** and **Server type** cannot be modified. The parameters are the same as those in **Figure 2-196**

d. Click **OK**.

– Deleting an authentication, authorization, or accounting server

a. Access the **HWTACACS Setting** tab page.

Log in to the web platform and choose **Security** > **AAA** > **HWTACACS Setting**.

b. Select the check box of an authentication, authorization, or accounting server in the **Authentication/Authorization/Accounting Server** area, and click **Delete**.

c. In the dialog box that is displayed, click **OK**.

----End

2.15.7.5 Domain Setting

Context

The created authentication, authorization, and accounting schemes take effect only after being applied to a domain.

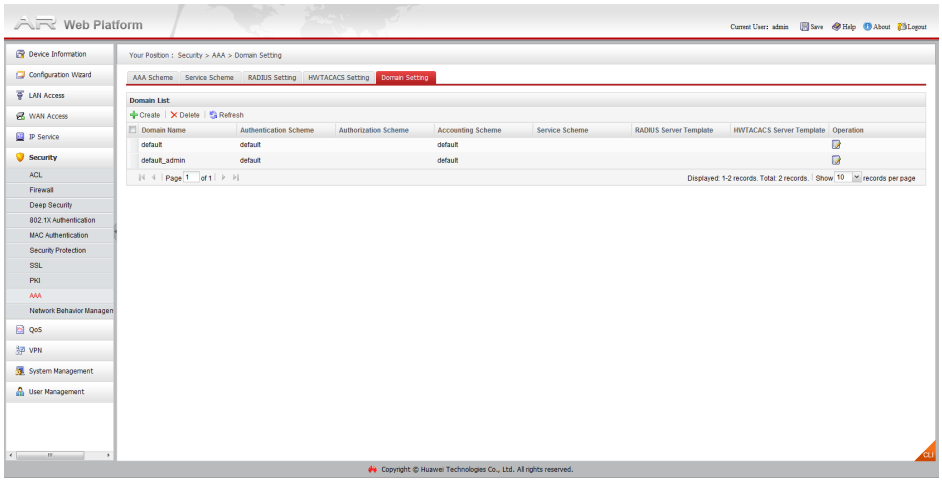
Procedure

- Creating a domain

a. Access the **Domain Setting** tab page.

Log in to the web platform and choose **Security** > **AAA** > **Domain Setting**. As shown in **Figure 2-197**.

Figure 2-197 Domain Setting



Copyright © Huawei Technologies Co., Ltd.

b. Click **Create** and set parameters in the **Create Domain** dialog box that is displayed. **Table 2-153** describes the parameters. As shown in **Figure 2-198**.

Figure 2-198 Create Domain

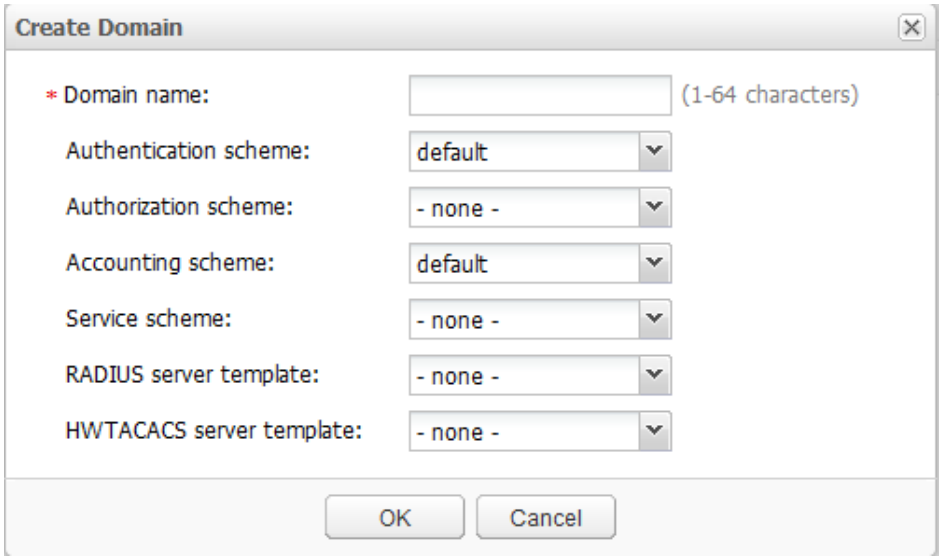


Table 2-153 Domain parameters

Parameter	Description
Domain name	Name of a domain.
Authentication scheme	Created authentication scheme.
Authorization scheme	Created authorization scheme.
Accounting scheme	Created accounting scheme.
Service scheme	Created service scheme.
RADIUS server template	Created RADIUS server template.
HWTACACS server template	Created HWTACACS server template.

c. Click **OK**.

- Modify a domain

a. Access the **Domain Setting** tab page.

Log in to the web platform and choose **Security** > **AAA** > **Domain Setting**.

b. Select a domain in the **Domain list** area, and click .

 Copyright © Huawei Technologies Co., Ltd.

c. In the **Modify Domain** dialog box that is displayed, modify the parameters. The parameter **Domain name** cannot be modified. The parameters are the same as those in **Figure 2-198**

d. Click **OK**.

- Deleting a domain

a. Access the **Domain Setting** tab page.

Log in to the web platform and choose **Security** > **AAA** > **Domain Setting**.

b. Select the check box of a domain in the **Domain list** area, and click **Delete**.

c. In the dialog box that is displayed, click **OK**.

----End

2.15.8 Online Behavior Management

NOTE

For SAC-capable devices, their licensing requirements for the SAC function are as follows:

- AR100&AR120 series: SAC is a basic feature of the device and is not under license control.
- AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600 series: By default, this function is disabled on a new device. To use the SAC function, apply for and purchase the following license from the Huawei local office.
  - AR150&160&200 series: AR150&160&200 value-added service package for security services
  - AR1200 series: AR1200 value-added service package for security services
  - AR2200 series: AR2200 value-added service package for security services
  - AR3200 series: AR3200 value-added service package for security services
  - AR3600 series: AR3600 value-added service package for security services

2.15.8.1 Basic Configuration

Context

To identify and classify application-based protocols to provide differentiated services for different applications, you can configure the online behavior management function.

Network behavior management detects and identifies packets of dynamic protocols such as Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), and Real-Time Transport Protocol (RTP) by checking Layer 4 to Layer 7 information in the packets. In this manner, online behavior management identifies protocols and applications on the network so that differentiated services are provided for different applications.

On the **Basic Configuration** tab page, you can create applications and configure online behavior management.

 Copyright © Huawei Technologies Co., Ltd.

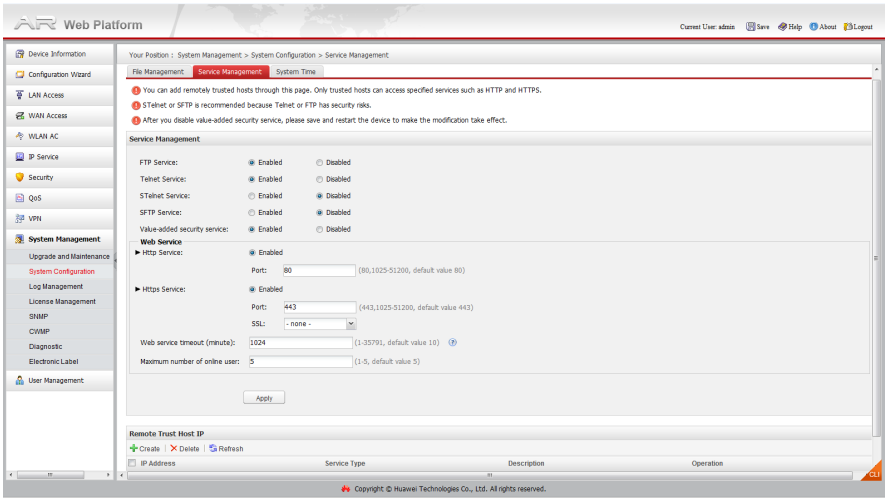
Prerequisite

To use the deep security function, you must enable it. By default, the deep security function is disabled.

1. Open the **Service Management** page.

   Log in to the web system, choose **System Management** > **System Configuration** > **Service Management** to open the **Service Management** page, as shown in **Figure 2-199**.

   Figure 2-199 Service Management tab page

2. Enable or disable deep security.
   - Enable deep security.

     In the **Service Management** area, click **Enabled** > **Apply** of **Value-added security service** to enable the deep security function.
   - Disable deep security.

     To disable deep security, click **Disable** and **Apply**, and restart the device.

     After the device restarts, the deep security configurations are deleted.

Procedure

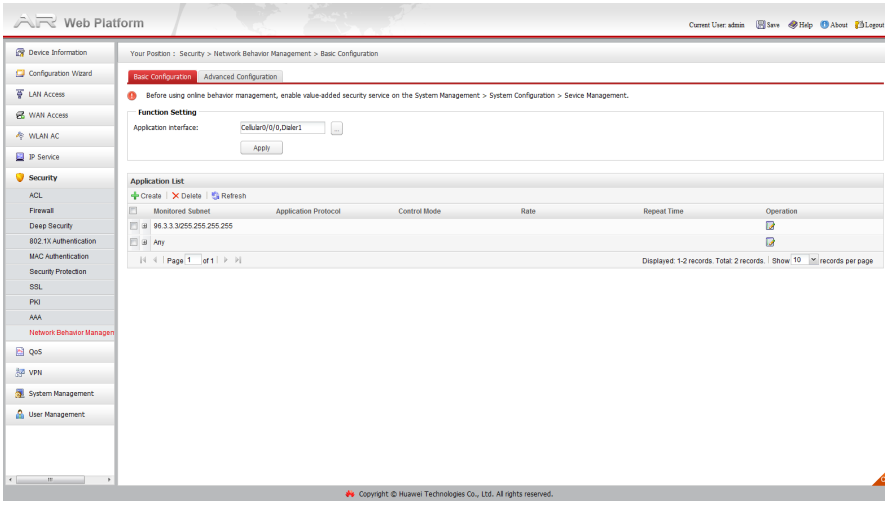
Step 1 Configuring **Application interface**

1. Access the **Basic Configuration** tab page.

   Log in to the web management system, and choose **Security** > **Network Behavior Management** > **Basic Configuration**, as shown in **Figure 2-200**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-200 Basic Configuration



2. In the **Function Setting** area, select interfaces to be enabled with online behavior management.

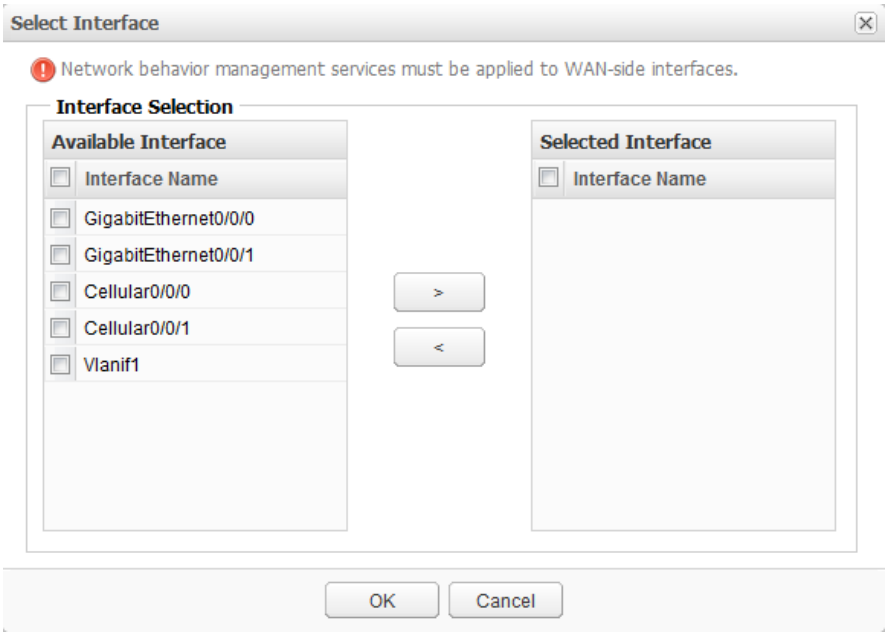
   Interfaces in the **Selected Interface** area have this function enabled. You can click > or < to move interfaces in areas **Interface Selection** and **Selected Interface** from one to another, as shown in **Figure 2-201**.

   NOTE

   Online behavior management services must be applied to WAN-side interfaces.

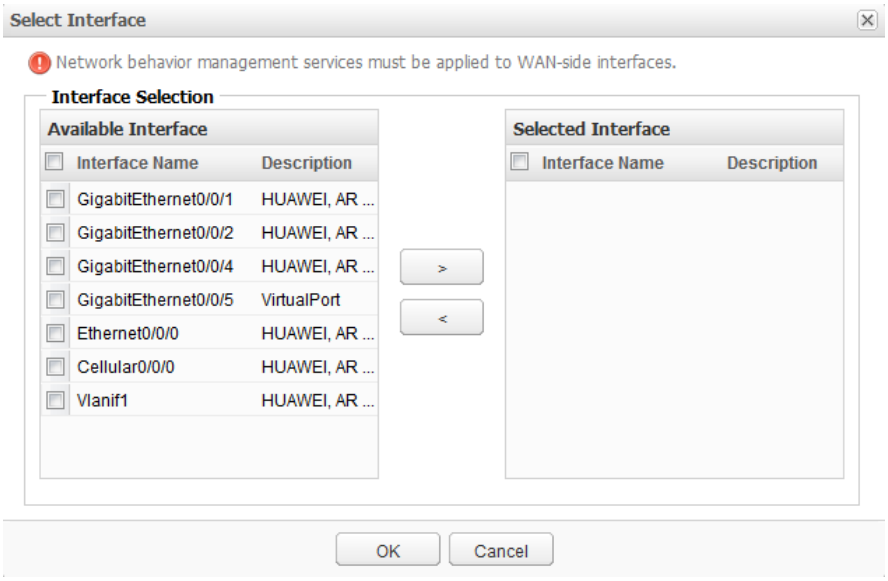
Figure 2-201 Select Interface

In the V200R010C00 version:



In V200R010C10 and later versions:

 Copyright © Huawei Technologies Co., Ltd.



3. Click **Apply**.

Step 2 Managing **Application List**

- Creating an application

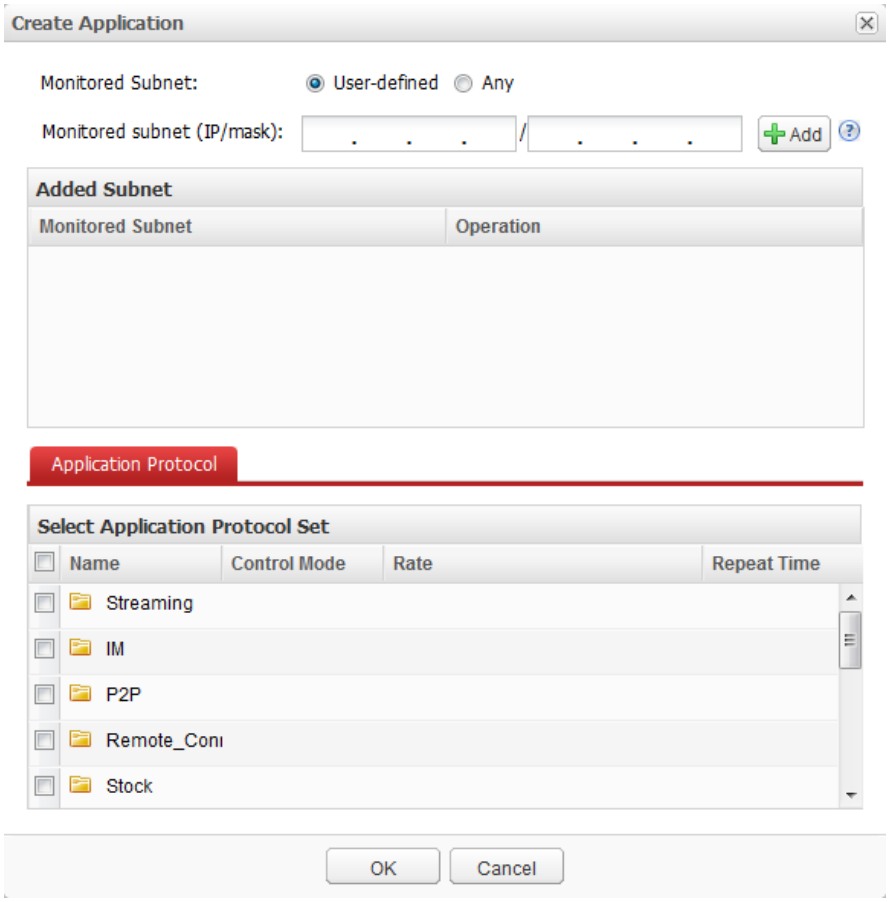
1. Access the **Basic Configuration** tab page.

   Log in to the web management system, and choose **Security** > **Network Behavior Management** > **Basic Configuration**, as shown in **Figure 2-200**.

2. In the **Application List** area, click **Create**, as shown in **Figure 2-202**. In the **Create Application** dialog box, set parameters listed in **Table 2-154**. **Table 2-155** describes the application protocol set.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-202 Create Application



3. Click **OK**. The new application is added.

Table 2-154 Parameters for creating an application

Parameter	Description
Monitored Subnet	Network segment to be monitored. You can set this parameter to **User-defined** or **All**.
Monitored subnet (IP/mask)	Specific network segment to be monitored. The IP address and subnet mask are both in dotted decimal notation. This parameter is available only when **Monitored Subnet** is set to **User-defined**. You can delete a monitored network segment from the **Added Subnet** area.
Application Protocol	Application protocol set of the application. Select an application protocol set in the **Select Application Protocol Set** area.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Control Mode	Control mode of the application protocol set: – Deny: discards packets meeting the requirements. – Flow limiting: limits the rate of packets meeting the requirements.
Rate	Rate limit of packets in the application protocol set. The value is an integer that ranges from 8 to 4294967295, in kbit/s. This parameter is available only when **Control Mode** is set to **Flow limiting**.
Repeat Time	Time when the application protocol set takes effect. The validity period of the application protocol is set on the **Advanced Configuration** tab page.

Table 2-155 Description of the application protocol set

Item	Description
AppDownload	Application downloading.
Attack	Network attack software.
Auth_Service	Identity authentication service provided on a network to ensure security.
Browser_Plugin	Supplements and extensions to a web browser.
CloudService	Cloud services.
Data_Backup	An important data recovery tool for enterprise users, which ensures security and integrity of enterprise data.
Database	A piece of data management software that provides functions such as data storage, access, protection, and backup.
Electronic_Business	Business activities conducted on the Internet in compliance with laws and regulations.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Email	An application that enables users to write, send, and receive mails over the Internet.
Encrypted_Tunnel	A method of using a network tunneling protocol to transfer packets of another network protocol.
Enterprise_Application	Enterprise application software provided to meet application requirements of enterprises.
FileShare_P2P	A point-to-point model that allows users to share files on a network.
File_Access	Access to a file.
File_Sharing	Sharing files with other users on a network.
Finance	Online banking and stock trading.
Game	Online gaming service provided on the Internet, which enables entertainment and communication using servers of game providers and computers of users.
General_TCP	General TCP application.
General_UDP	General UDP application.
IM_File_Transfer	A function of instant messaging software that enables file transfer between two or more users on a network.
Infrastructure	A collection of rules for communication between network devices, servers, and computers. An infrastructure protocol defines the formats of information that must be used in communication and meanings of the formats. Commonly used infrastructure protocols include HTTP and DNS.
Instant_Messaging	An application that allows two or more users to exchange text messages, files, voice, and video instantly on a network.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Internet_Conferencing	An application that allows users to share documents, make presentations, and hold meetings with others on a network.
Ip_Protocol	IP layer protocol.
Media_Sharing	Sharing audio and video with other users on a network.
MicroBlog	A platform where users share, propagate, and obtain information based on relationships with other users.
Network_Admin	Network management.
Network_Storage	Web disk application.
News_Group	News group.
Other	Applications other than UDP and TCP applications.
PeerCasting	Video transfer in point-to-point mode.
Proxy	Network proxy service that allows one network terminal to establish an indirect connection with another network terminal, to guarantee privacy and security and prevent network attacks.
Remote_Access	Any software that provides the remote access service, for example, the application software that allows one computer to access and control another computer.
Search_Engines	An application that automatically collects information from the Internet and provides it to users after analyzing and arranging the information.
Social_Networking	A platform that supports communication between users with the same interests and taking part in same activities on the Internet.
Software_Update	Upgrade of a software program using an upgrade patch downloaded from a network server.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Utility	Tools available on the Internet, such as the IP address location query tool.
VoIP	An application that enables users to make calls and transfer text, voice, and video at lower costs over an IP network.
WebMail	Web mailbox.
Web_Browsing	Display of text, image, video, and other information using a web browser.
Web_Content_Aggregate	Providing useful and specific information by manually sorting, analyzing, and classifying information and resources on the Internet.
Web_Desktop	A browser-based virtual operating system, on which users can perform operations on application programs using web browsers.
Web_Posting	Online discussion web site.
Web_Spider	A type of application that automatically collects specific information from the Internet.
Web_Video	Video portal web site.
Wireless	An application used on mobile phones to support wireless network access.

- Modifying an application

1. In the **Application List** area, click  corresponding to the required application.
2. In the **Modify Application** dialog box, modify parameters listed in **Table 2-154**. The parameters are the same as those in **Figure 2-202**.
3. Click **OK**.

- Deleting an application

  In the **Application List** area, select the required application, and click **Delete**. In the **Information** dialog box, click **OK**.

----End

Copyright © Huawei Technologies Co., Ltd.

2.15.8.2 Advanced Configuration

Context

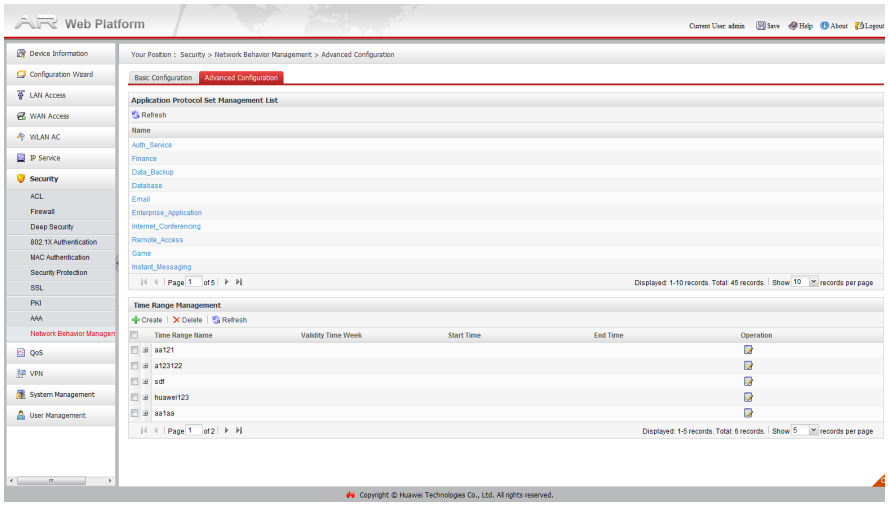
To identify application protocols on the network and implement online behavior management, manage application protocols on the **Advanced Configuration** tab page.

You can manage application protocol sets and their validity periods on the **Advanced Configuration** tab page.

Procedure

- Managing an application protocol set
  a. Access the **Advanced Configuration** tab page.
     Log in to the web management system, and choose **Security** > **Network Behavior Management** > **Advanced Configuration** as shown in **Figure 2-203**.

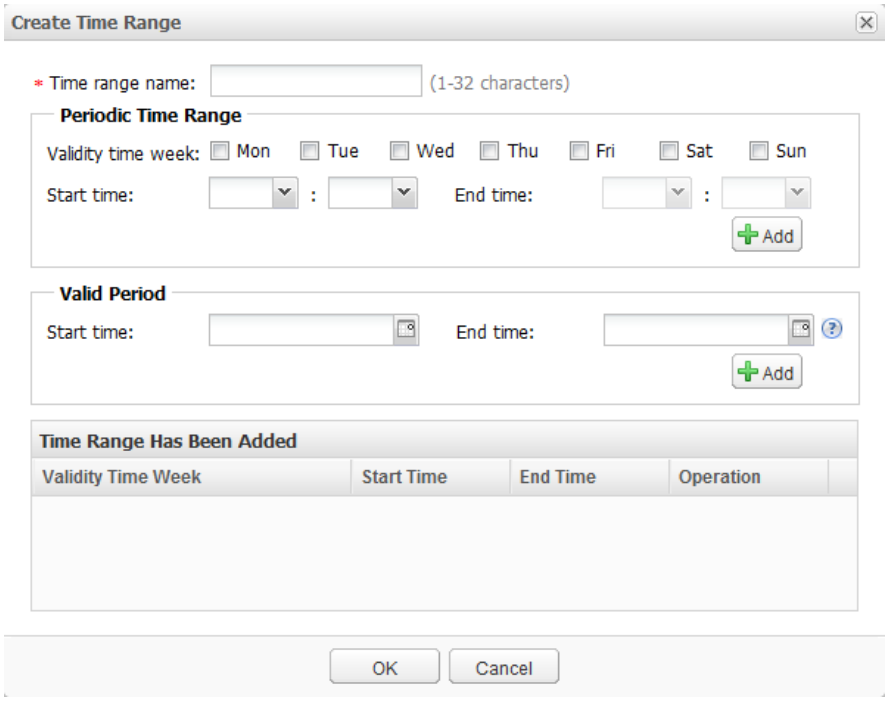
     Figure 2-203 Advanced Configuration

  b. Click **Refresh**.
     The advanced configuration can only be displayed, but cannot be added, modified, or deleted.
     Click the application protocol set name to view detailed information.
- Managing the validity period
  – Creating a validity period
    i. Access the **Advanced Configuration** tab page.
       Log in to the web management system, and choose **Security** > **Network Behavior Management** > **Advanced Configuration** as shown in **Figure 2-203**.
    ii. In the **Time Range Management** area, click **Create**. In the **Create Time Range** dialog box, as shown in **Figure 2-204**, set parameters listed in **Table 2-156**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-204 Create Time Range



iii. Click **OK**. A validity period is added.

Table 2-156 Parameters for creating a validity period

Parameter	Description
Time range name	Name of the time range. The value is a string of 1 to 32 case-sensitive characters without question marks (?) and spaces. The first character must be a letter. A time range name cannot contain the word **all**.
Validity time week	Day when the application protocol set takes effect: • Monday • Tuesday • Wednesday • Thursday • Friday • Saturday • Sunday Multiple days can be set.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Start time(Periodic Time Range)	Start time when the application protocol set takes effect. The value is in HH:MM format and ranges from 00:00 to 23:59.
End time(Periodic Time Range)	End time when the application protocol set takes effect. The value is in HH:MM format and ranges from 00:00 to 23:59.
Start time(Valid Period)	Start time of the time range. The format is YYYY-MM-DD HH:MM:SS, in which SS is invalid. The value ranges from 1970-01-01 00:00 to 2099-12-31 23:59.
End time(Valid Period)	End time of the time range. The format is YYYY-MM-DD HH:MM:SS, in which SS is invalid. The value ranges from 1970-01-01 00:00 to 2099-12-31 23:59.

- Modifying a validity period
  i. In the **Time Range Management** area, click  corresponding to the required validity period.
  ii. In the **Modify Time Range** dialog box, modify parameters listed in **Table 2-156**. The parameters are the same as those in **Figure 2-204**. The parameter **Time range name** cannot be modified.
  iii. Click **OK**.
- Deleting a validity period
  In the **Time Range Management** area, select the required validity period, and click **Delete**. In the **Information** dialog box, click **OK**.

----End

2.16 QoS

2.16.1 Traffic Management

2.16.1.1 Traffic Policy Application

Context

After parameters of a traffic policy are set, apply the traffic policy to the interface to implement differentiated services.

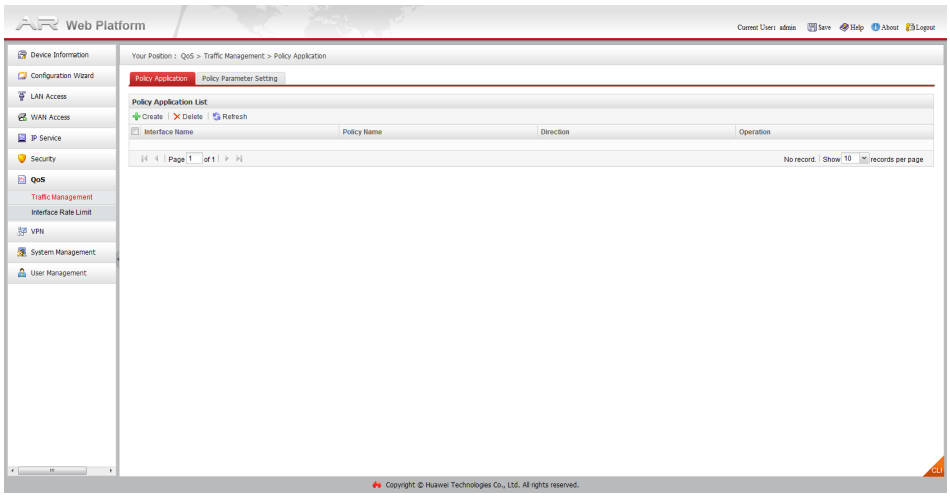
Only one traffic policy can be applied to one direction on an interface, but a traffic policy can be applied to different directions on different interfaces.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

- Create traffic policy application.
  a. Choose **QoS** > **Traffic Management** > **Policy Application** to open the **Policy Application** page. The page shown in **Figure 2-205** is displayed.

Figure 2-205 Policy Application



  b. Click **Create** in **Policy Application List**.
  c. On the **Create Policy Application** page, set parameters. **Table 2-157** describes the parameters. The page shown in **Figure 2-206** is displayed.

Figure 2-206 Create Policy Application

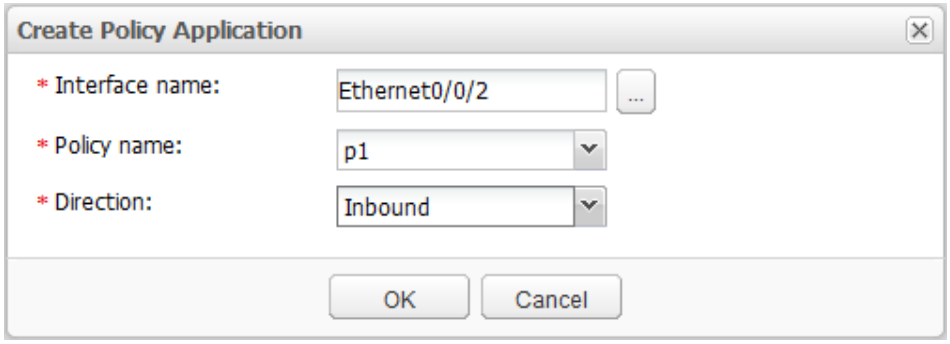


Table 2-157 Parameters for creating traffic policy application

Item	Description
Interface name	Indicates the interface to which the traffic policy is applied.

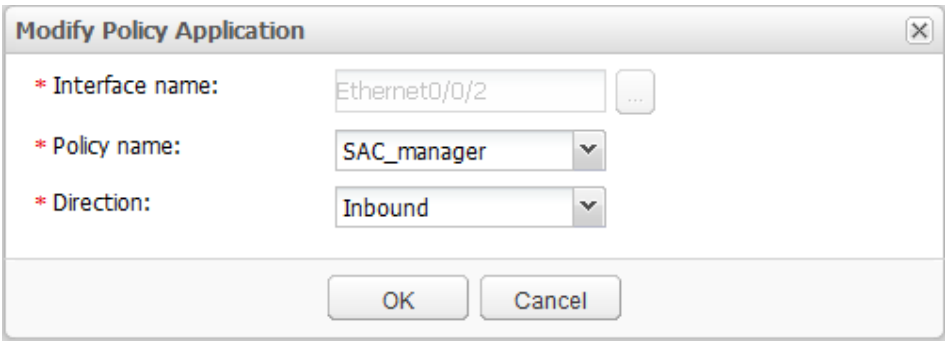
 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Policy name	Indicates the name of the traffic policy to be applied. Select the traffic policy from the drop-down list box. The traffic policy has been configured on the **Policy Parameter Setting** tab page.
NAT pre-classification **NOTE** This parameter is available when traffic policy application is created or modified and a Layer 3 interface is specified.	Indicates NAT pre-classification: • Enabled: NAT pre-classification is enabled on the interface. • Disabled: NAT pre-classification is disabled on the interface.
Direction	Indicates the direction to which the traffic policy is applied. The value is **Inbound** or **Outbound**.
Bandwidth (kbit/s)	Indicates the available bandwidth of the interface, in kbit/s. The parameter is used to shape traffic on the interface and limit the rate of outgoing packets. The parameter is available only when **Direction** is **Outbound**.

d. Click **OK** to save the configurations.

- Modify a traffic policy application.
  a. Choose **QoS** > **Traffic Management** > **Policy Application** to open the **Policy Application** page. The page shown in **Figure 2-205** is displayed.
  b. In **Policy Application List**, select a traffic policy application to be modified and click  in the **Operation** column.
  c. On the **Modify Policy Application** page, modify parameters, as shown in **Table 2-157**. The interface name cannot be modified. The page shown in **Figure 2-207** is displayed.

Figure 2-207 Modify Policy Application



 Copyright © Huawei Technologies Co., Ltd.

d. Click **OK** to save the configurations.

- Delete a traffic policy application.
  a. Choose **QoS** > **Traffic Management** > **Policy Application** to open the **Policy Application** page. The page shown in **Figure 2-205** is displayed.
  b. In **Policy Application List**, select a traffic policy application and click **Delete**.
  c. Click **OK** in the displayed dialog box.

----End

2.16.1.2 Policy Parameter Configuration

Context

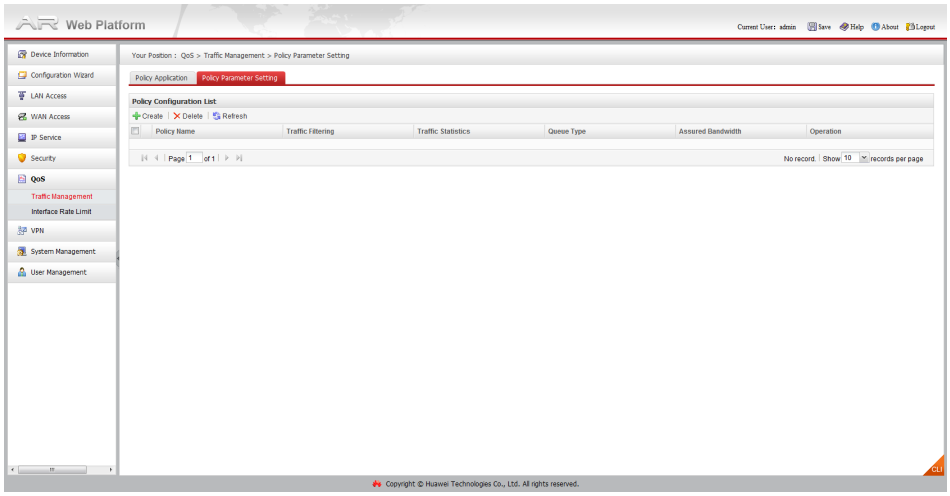
A traffic policy is configured by binding traffic classifiers to traffic behaviors. A traffic classifier defines a group of matching rules to classify packets. A traffic behavior defines actions to be taken for the packets matching the traffic classifier, such as traffic statistics, traffic filtering, and re-marking.

Here, the binding between a traffic classifier and a traffic behavior is defined as classification. By default, the name of the traffic classifier or traffic behavior is the same as the classification name.

Procedure

- Create a traffic policy.
  a. Choose **QoS** > **Traffic Management** > **Policy Parameter Setting** to open the **Policy Parameter Setting** page. The page shown in **Figure 2-208** is displayed.

Figure 2-208 Policy Parameter Setting



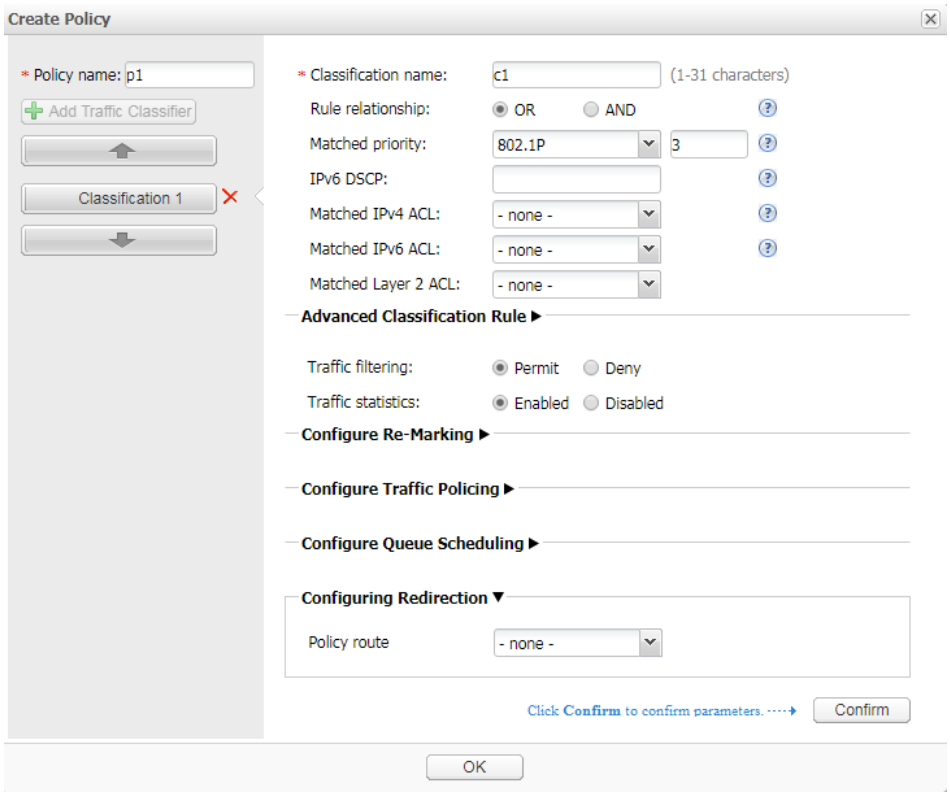
  b. Click **Create** in **Policy Configuration List**.

Copyright © Huawei Technologies Co., Ltd.

c. On the **Create Policy** page, set parameters and configure the traffic classifier and traffic behavior. **Table 2-158** describes the parameters. The page shown in **Figure 2-209** is displayed.

Enter the classification name. The traffic classifier and traffic behavior with the same name as the classification name are created by default.

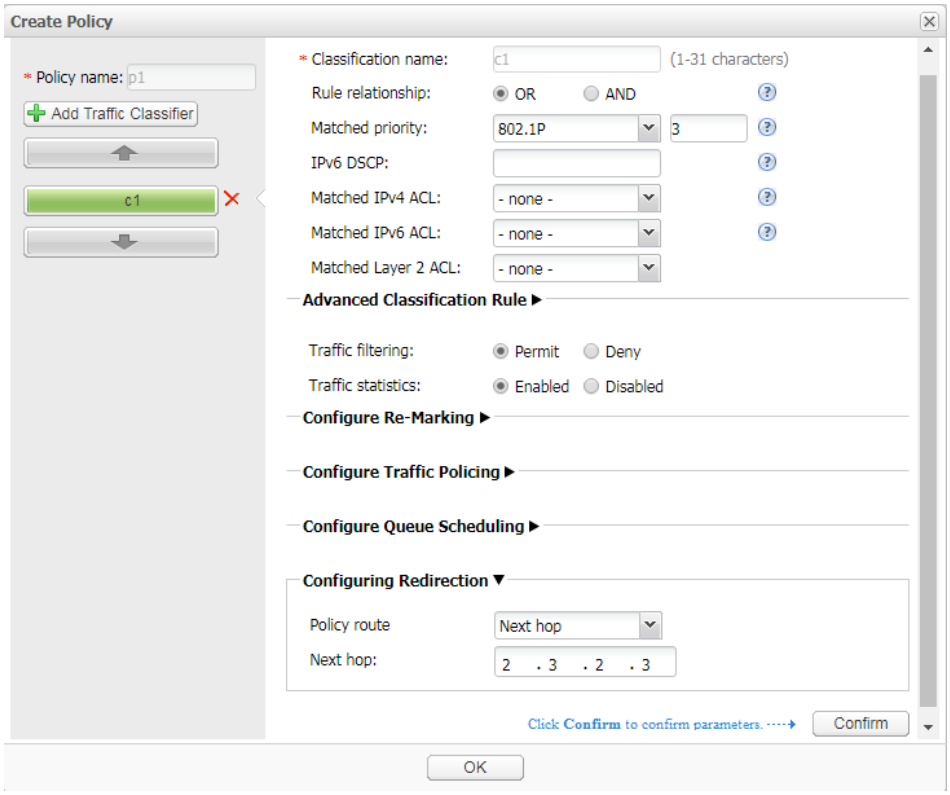
Figure 2-209 Create Policy



d. Click **Confirm** to confirm the configurations. The page shown in **Figure 2-210** is displayed.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-210 Finish Create Policy



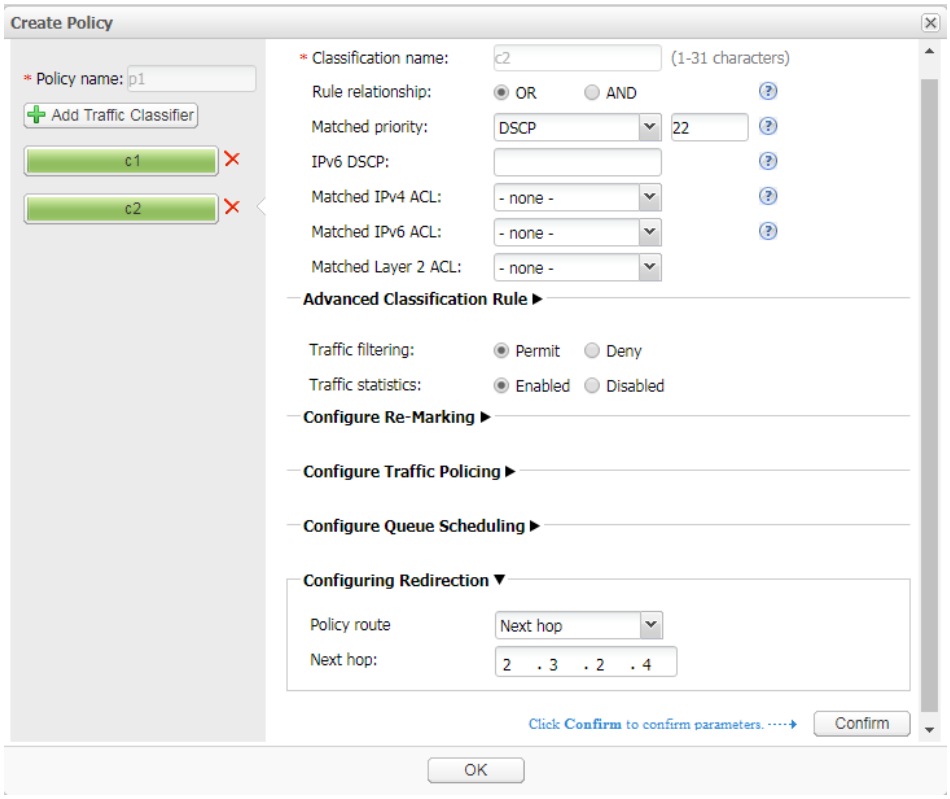
e. (Optional) Click **Add Traffic Classifier**, and select or enter parameters on the **Add Traffic Classifier** page. Click **Confirm** to confirm the configurations. The page shown in **Figure 2-211** is displayed.

   To configure multiple traffic classifiers, repeat step 5.

   A traffic policy allows a maximum of 16 traffic classifiers.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-211 Add Traffic Classifier



f. Click **OK** to save the configurations.

Table 2-158 Description of parameters for creating a traffic policy

Item	Description
Policy name	Indicates the name of a traffic policy.
Classification 1	Indicates the name of the binding between a traffic classifier and a traffic behavior. After parameters on the **Create Policy** page are set, click **Confirm**. The value of this field is updated automatically.
Classification name	Indicates the classification name.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Rule relationship	Indicates the relationship between rules in a traffic classifier: • OR: Packets match a traffic classifier as long as the packets match one or more rules in the traffic classifier. • AND: Packets match a traffic classifier only when the packets match all rules in the traffic classifier.
Matched priority	Indicates the priority used to match packets. • IP • 802.1p • DSCP • MPLS-EXP Only one type of priority can be configured in each traffic classifier. A traffic classifier can define eight priority values. The relationship between multiple priority values is OR.
IPv6 DSCP	Indicates the DSCP priority is used to match IPv6 packets.
Matched IPv4 ACL	Indicates the IPv4 ACL used to match packets. You can configure a basic IPv4 ACL, advanced IPv4 ACL, or Layer 2 IPv4 ACL. If an IPv4 ACL contains multiple rules with different numbers, packets match the IPv4 ACL as long as the packets match one rule. Choose **Security** > **ACL** and configure an IPv4 ACL on the ACL page.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Matched IPv6 ACL	Indicates the IPv6 ACL used to match packets. You can configure a basic or advanced IPv6 ACL. If an IPv6 ACL contains multiple rules with different numbers, packets match the IPv6 ACL as long as the packets match one rule. Choose **Security** > **ACL** and configure an IPv6 ACL on the ACL page.
Matched Layer 2 ACL	Indicates the Layer 2 ACL used to match packets. If a Layer 2 ACL contains multiple rules with different numbers, packets match the Layer 2 ACL as long as the packets match one rule. Choose **Security** > **ACL** and configure a Layer 2 ACL on the ACL page.
Advanced Classification Rule	Indicates the advanced classification rule: • Layer 2 protocol: ARP, IP, MPLS, RARP, or user-defined protocol • Inbound interface
Traffic filtering	Indicates the traffic filtering action in a traffic behavior: • Permit: permits packets matching rules to pass through. • Deny: rejects packets matching rules.
Traffic statistics	Indicates the traffic statistics action in a traffic behavior: • Enable: enables traffic statistics. • Disable: disables traffic statistics.
Configure Re-Marking	Indicates the re-marking action in a traffic behavior. The device can re-mark DSCP priorities, 802.1p priorities, MPLS EXP priorities, or local precedences in packets.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Configure Traffic Policing	Indicates the traffic policing action in a traffic behavior: • CIR (kbit/s): specifies the committed information rate (CIR), which is the guaranteed average transmission rate, in kbit/s. • CBS (byte): specifies the committed burst size (CBS), which is the average volume of burst traffic that can pass through an interface, in bytes. • PIR (kbit/s): specifies the peak information rate (PIR), which is the maximum transmission rate, in kbit/s. • PBS (byte): specifies the peak burst size (PBS), which is the maximum volume of burst traffic that can pass through an interface, in bytes.
Configure Queue Scheduling	Indicates the queue scheduling action in a traffic behavior. You can specify the queue type and assured bandwidth.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Queue type	Indicates the queue type in queue scheduling: ● AF: AF ensures low drop probability of packets when the rate of outgoing service traffic does not exceed the minimum bandwidth. It is applied to services of heavy traffic that needs to be ensured. ● EF: After packets matching traffic classification rules enter EF queues, they are scheduled in Strict Priority (SP) mode. Packets in other queues are scheduled only after all the packets in EF queues are scheduled. EF is applied to the services requiring the low delay, low drop probability, assured bandwidth, and occupying low bandwidth, for example, voice packets. ● LLQ: LLQ queues are special type of EF queues and use the SP mode. The device uses traffic policing to process packets in LLQ queues, ensuring a short delay because traffic policing does not buffer packets. **NOTE** **Assured bandwidth** is mandatory when **Queue type** is used.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Assured bandwidth	Indicates the assured bandwidth or bandwidth percentage: • The guaranteed bandwidth of an AF queue is the minimum bandwidth. • The guaranteed bandwidth of an EF queue is the minimum bandwidth. • The guaranteed bandwidth of an LLQ queue is the maximum bandwidth. When you configure assured bandwidth for queues of the same type in a traffic policy, use either the bandwidth value or bandwidth percentage. If you use both the bandwidth value and bandwidth percentage, the traffic policy may fail to be applied.
Configuring Redirection	Indicates the redirection action in a traffic behavior. Redirection to the next hop or outbound interface can be specified. **NOTE** This parameter is supported only in V200R010C10 and later versions.
Next hop	Indicates the action of redirecting packets to the next hop in a traffic behavior. **NOTE** This parameter is supported only in V200R010C10 and later versions.
Outbound interface	Indicates the action of redirecting packets to a specified interface in a traffic behavior. **NOTE** This parameter is supported only in V200R010C10 and later versions.

- Modify a traffic policy.
  a. Choose **QoS** > **Traffic Management** > **Policy Parameter Setting** to open the **Policy Parameter Setting** page. The page shown in **Figure 2-208** is displayed.
  b. In **Policy Configuration List**, select a traffic policy to be modified and click  in the **Operation** column.

Copyright © Huawei Technologies Co., Ltd.

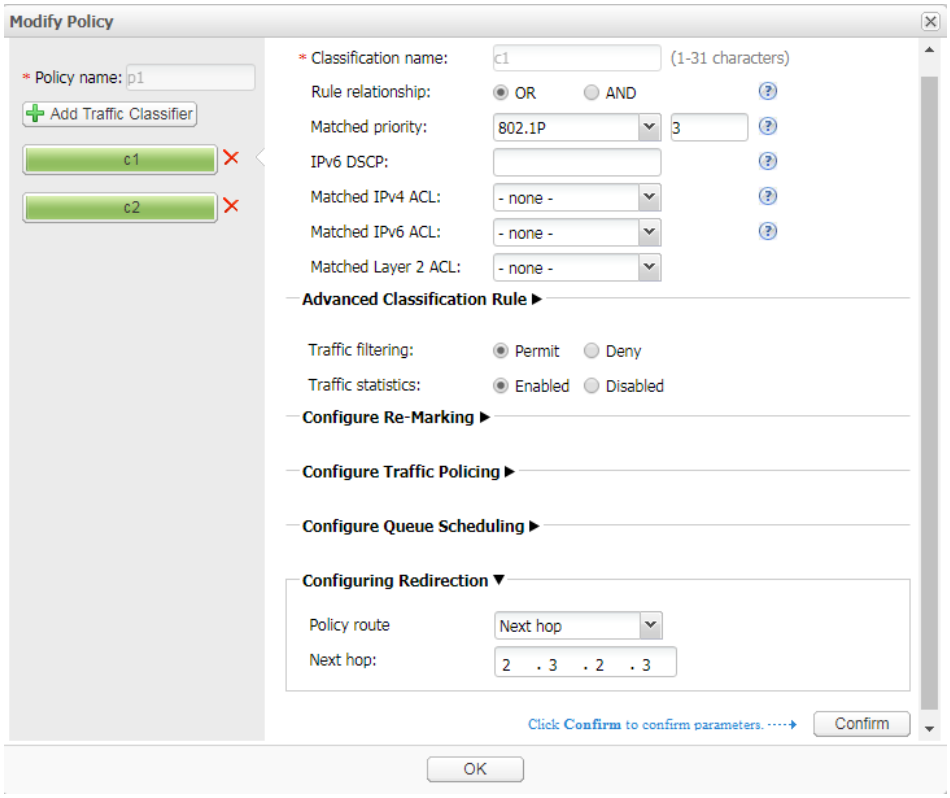
c. On the **Modify Policy**, you can modify, add, or delete traffic classifiers. The page shown in **Figure 2-212** is displayed.

- To modify classification, select classification to be modified and configure parameters, as shown in **Table 2-158**. The values of **Policy name** and **Classification name** cannot be changed.
- To add classification, click **Add Traffic Classifier** and configure parameters, as shown in **Table 2-158**.
- To delete classification, select classification to be deleted, click , and click **OK** in the dialog box that is displayed. If the traffic policy contains only one classification, configured parameters are deleted and the name is restored to be **Classification 1**.

  NOTE

  In **Policy Configuration List**, select the traffic policy to be modified, click , and click in the **Operation** column to delete classification.

Figure 2-212 Modify Policy



d. Click **Confirm**.

e. Click **OK** to save the configurations.

- Delete a traffic policy.

  a. Choose **QoS** > **Traffic Management** > **Policy Parameter Setting** to open the **Policy Parameter Setting** page. The page shown in **Figure 2-208** is displayed.

 Copyright © Huawei Technologies Co., Ltd.

b. In **Policy Configuration List**, select a traffic policy and click **Delete**.

c. Click **OK** in the displayed dialog box.

If the traffic policy that you want to delete has been applied to an interface, unbind the traffic policy from the interface on the **Policy Application** tab page, and perform step 1 to step 3.

----End

2.16.2 Interface Rate Limit

Context

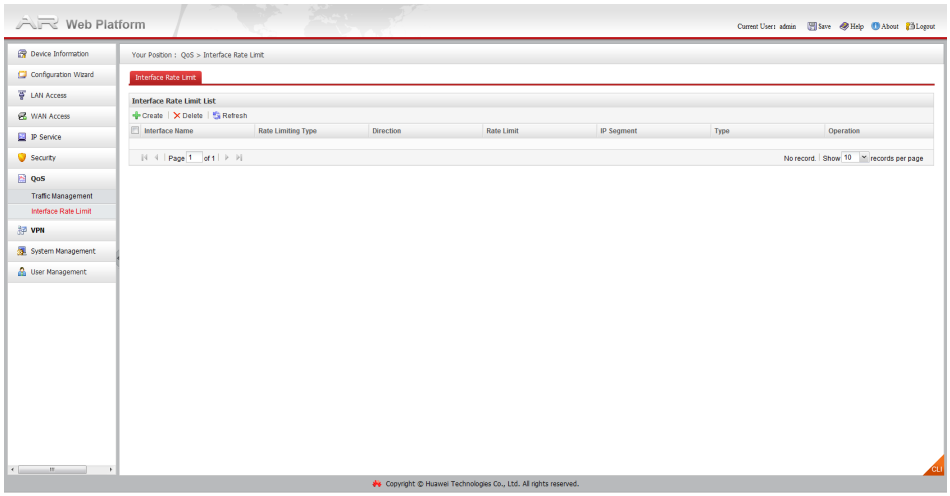
When data is sent from a high-speed link to a low-speed link, the bandwidth on the interface of the low-speed link is insufficient. As a result, a large number of packets are discarded. The data traffic rate needs to be limited. To solve the problem, configure the rate limit in the outbound direction on the interface of the high-speed link. The interface then discards the packets whose rate exceeds the rate limit so that traffic is limited in a specified range. You can also configure the rate limit in the inbound direction on the interface of the low-speed link. When the rate of received packets is greater than the rate limit, the interface discards the packets.

You can configure rate limit for all packets on the inbound or outbound interface or packets on the specified source/destination IP address segment.

Procedure

- Create interface rate limit.
  a. Choose **QoS** > **Interface Rate Limit** to open the **Interface Rate Limit** page. The page shown in **Figure 2-213** is displayed.

  Figure 2-213 Interface Rate Limit

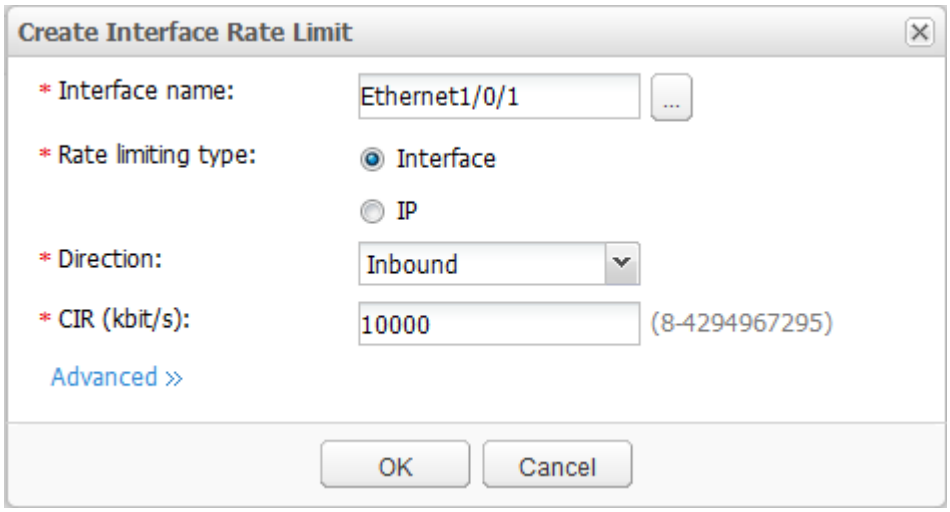
  

  b. Click **Create** in **Interface Rate Limit List**.

  c. On the **Create Interface Rate Limit** page, set parameters. **Table 2-159** describes the parameters. The page shown in **Figure 2-214** is displayed.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-214 Create Interface Rate Limit



d. Click **OK** to save the configurations.

Table 2-159 Description of parameters for creating interface rate limit

Item	Description
Interface name	Indicates the name of the interface where rate limit will be configured.
Rate limiting type	Indicates the rate limit type: • Interface: limits the rate of all packets in the inbound or outbound direction of an interface. • IP: limits the rate of packets based on IP addresses. – destination: limits the rate of packets on the specified destination IP address segment. – source: limits the rate of packets on the specified source IP address segment.
Direction	Indicates the direction to which rate limit is applied: • Inbound: limits the rate of packets entering the interface. • Outbound: limits the rate of packets going out of the interface.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Start source IP	Indicates the first IP address of the source IP address segment. This parameter is available only when **IP** is **source**.
End source IP	Indicates the last IP address of the source IP address segment. This parameter is available only when **IP** is **source**.
Start destination IP	Indicates the first IP address of the destination IP address segment. This parameter is available only when **IP** is **destination**.
End destination IP	Indicates the last IP address of the destination IP address segment. This parameter is available only when **IP** is **destination**.
Type	Indicates the type of bandwidth used by packets on the source/destination IP address segment: • Shared: Specified source/destination IP address segment shares the available bandwidth. • Exclusive: Each IP address of the specified source/destination IP address segment exclusively uses the available bandwidth. This parameter is available only when **Rate limiting type** is **IP**.
CIR (kbit/s)	Specifies the committed information rate, which is the guaranteed average transmission rate, in kbit/s.

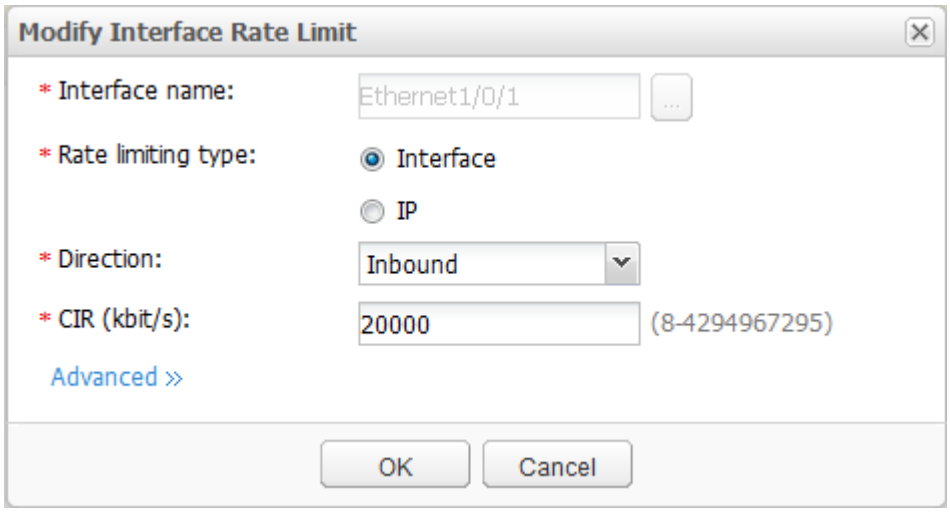
Copyright © Huawei Technologies Co., Ltd.

Item	Description
Advanced	Indicates other parameters: • PIR (kbit/s): specifies the peak information rate, which is the maximum transmission rate, in kbit/s. • CBS (byte): specifies the committed burst size (CBS), which is the average volume of burst traffic that can pass through an interface, in Bytes. • PBS (byte): specifies the peak burst size (PBS), which is the maximum volume of burst traffic that can pass through an interface, in Bytes. The default settings are as follows: • If the PIR is not set or the PIR equals the CIR, the CBS is 188 times the CIR and the PBS is 313 times the CIR. • If the PIR is set and is different from the CIR, the CBS is 125 times the CIR and the PBS is 125 times the PIR. LAN interfaces do not support this parameter.

- Modify interface rate limit.
  a. Choose **QoS** > **Interface Rate Limit** to open the **Interface Rate Limit** page. The page shown in **Figure 2-213** is displayed.
  b. In **Interface Rate Limit List**, select an interface and click  in the **Operation** column. The page shown in **Figure 2-215** is displayed.

Copyright © Huawei Technologies Co., Ltd.

Figure 2-215 Modify Interface Rate Limit



c. On the **Modify Interface Rate Limit** page, modify parameters, as shown in **Table 2-159**. The interface name cannot be modified.

d. Click **OK** to save the configurations.

- Delete interface rate limit.
  a. Choose **QoS** > **Interface Rate Limit** to open the **Interface Rate Limit** page. The page shown in **Figure 2-213** is displayed.
  b. In **Interface Rate Limit List**, select a traffic policy and click **Delete**.
  c. Click **OK** in the displayed dialog box.

----End

2.17 VPN

2.17.1 IPSec VPN

2.17.1.1 Overview

Concepts

IPSec

IPSec is a protocol suite defined by the Internet Engineering Task Force (IETF) for securing IP communication by authenticating and encrypting each IP packet of a communication session. Two communicating parties can encrypt data and authenticate the data origin at the IP layer to ensure data confidentiality and integrity and prevent replay of data packets.

IPSec uses two security protocols: Authentication Header (AH) protocol and Encapsulating Security Payload (ESP). Key exchange and SA establishment in IPSec

 Copyright © Huawei Technologies Co., Ltd.

is implemented by the IKE protocol, which simplifies use and management of IPSec.

IPSec Security Protocol

AH defines the authentication method and checks data integrity and data origin. ESP defines the encryption and authentication methods and ensures data reliability.

- AH: provides data origin authentication, data integrity check, and the anti-replay service. The sender performs hash calculation on the IP payload and all header fields of an IP packet except for variable fields to generate a message digest. The receiver calculates a message digest according to the received IP packet and compares the two message digests to determine whether the IP packet has been modified during transmission. AH does not encrypt the IP payload.
- ESP: encrypts the IP payload in addition to providing all the functions of AH. ESP can encrypt and authenticate the IP payload but does not authenticate the IP packet header.

IPSec Peer

IPSec provides secure IP communication between two endpoints. The two endpoints are called IPSec peers.

Security Association (SA)

A security association (SA) is a set of algorithms such as the encryption algorithm and parameters such as keys for secure data transmission between IPSec peers.

Encapsulation Mode

- Transport mode: inserts an IPSec header between the IP header and the header of the upper-layer protocol (AH or ESP). In this mode, the protocol type field in the IP header is changed to AH or ESP, and the checksum in the IP header is recalculated. The transport mode applies to communication between two hosts or between a host and a security gateway.
- Tunnel mode: encapsulates an IPSec header (AH or ESP) on the original IP header and adds a new IP header. In this mode, the original IP packet is transmitted as the payload of the packet and is protected by IPSec. The tunnel mode applies to communication between two security gateways. Packets encrypted by one security gateway must be decrypted by the other security gateway.

Authentication Algorithm and Encryption Algorithm

- IPSec uses the Message Digest 5 (MD5) algorithm, Secure Hash Algorithm (SHA-1) or Secure Hash Algorithm (SHA-2) for authentication. The MD5 algorithm computes faster than the SHA-1 algorithm, but the SHA-1 algorithm is more secure than the MD5 algorithm. SHA-2 increases the number of encrypted data bits and is more secure than SHA-1.
- IPSec uses the DES, Triple Data Encryption Standard (3DES), or Advanced Encryption Standard (AES) algorithm for encryption. The AES algorithm encrypts plain text by using a key of 128 bits, 192 bits, or 256 bits.

 Copyright © Huawei Technologies Co., Ltd.

Establishing an IPSec Tunnel Using IKE Negotiation

IKE

IKE builds upon the Internet Security Association and Key Management Protocol (ISAKMP) and provides the key negotiation, identity authentication, and SA establishment functions to simplify IPSec use and management.

IKE Version

IKE supports IKEv1 and IKEv2 versions.

- IKEv1: defines two phases for IPSec key negotiation. IKEv1 phase 1 operates in either main mode or aggressive mode. The aggressive mode allows two IPSec peers to establish an IKE SA more quickly than in main mode. In main mode, only IP addresses can be used to identify IPSec peers. In aggressive mode, both IP addresses and names can be used to identify IPSec peers.
- IKEv2: defines three types of exchanges and enables two IPSec peers to establish an IKE SA more quickly than IKEv1.

IKE Security Mechanism

- Diffie-Hellman (DH) algorithm: DH algorithm is a public key algorithm. The two communicating parties do not transmit a key but exchange data to calculate a shared key. They use the calculated shared key to encrypt data and exchange the encrypted data. IKE-enabled devices never directly transmit a key on an insecure network. Instead, the devices calculate a shared key by exchanging data. Even though a third party (such as a hacker) intercepts all exchanged data for key calculation, it cannot calculate the actual key.
- Perfect Forward Secrecy (PFS): PFS is a property that prevents other keys from being decoded when one key is decoded. The key used in IPSec phase 2 is derived from the key used in IPSec phase 1. After intercepting the key used in phase 1, an attacker may collect enough information to calculate the key to be used in phase 2. PFS provides an additional DH key exchange to secure the key used in phase 2.
- Identity authentication: authenticates identities of the two communicating parties including pre-shared key authentication and digital certificate authentication. In pre-shared key authentication, two communicating parties use a shared key to calculate a digest for a received packet and compare the digest with the digest field in the packet. If the calculated digest is the same as that in the packet, authentication succeeds; otherwise, authentication fails. In digital certificate authentication, two communicating parities use an agreed algorithm to calculate the digest for a packet. The sender uses its own private key to encrypt the digest field and generates a digital signature. The receiver uses the sender's public key to decrypt the digital signature and compares the calculated digest with the original digest field. If the calculated digest is the same as the original digest of the packet, authentication succeeds; otherwise, authentication fails.

Establishing an IPSec Tunnel Using an IPSec Virtual Tunnel Interface

An IPSec virtual tunnel interface is a Layer 3 logical interface supporting dynamic routing protocols. All packets passing through the IPSec virtual tunnel interface are protected by IPSec.

After an IPSec tunnel is established using an IPSec virtual tunnel interface, data flows routed to the IPSec virtual tunnel interface are protected by IPSec.

 Copyright © Huawei Technologies Co., Ltd.

Compared to using an ACL to determine data flows to be protected, using routing to determine the flows to be protected simplifies the IPSec policy deployment and prevents IPSec configuration from being affected by the network plan. This enhances network scalability and reduces network maintenance costs.

Establishing an IPSec Tunnel Using An Efficient VPN Policy

Efficient VPN

IPSec Efficient VPN has high security, reliability, and flexibility and has become the first choice for enterprises to establish VPNs. When establishing an IPSec tunnel between a branch and headquarters, an enterprise must configure IPSec and other network resources on the branch. If the network has hundreds of sites, IPSec configurations are complex and network maintenance is difficult.

The Efficient VPN solution integrates IPSec and other configurations on the Efficient VPN server. When basic parameters for establishing an SA are configured on the remote device, the remote device initiates a negotiation with the server and establishes an IPSec tunnel. After the IPSec tunnel is established, the server allocates other IPSec attributes and network resources to the remote device. Efficient VPN simplifies configurations and maintenance of IPSec and network resources for the branches.

Efficient VPN Operation Modes

- Client mode: A remote device configured with IPSec Efficient VPN connects to the headquarters and automatically applies to the server for an IP address and other network resources such as DNS domain, DNS server address, WINS server address, and delivered ACL resources. The remote device allocates these resources to PCs at the remote end using DHCP. The remote device automatically enables NAT. When receiving a packet from a PC on the remote subnet, the remote device translates the source IP address of the packet matching the pushed ACL resources and sends the packet to the server through an IPSec tunnel. Packets that do not match the pushed ACL resources are not translated by NAT and are not allowed to pass through the IPSec tunnel. These packets are forwarded to the Internet.
- Network mode: Unlike the client mode, IP addresses of branches and headquarters are configured beforehand in network mode. The remote device does not apply to the server for an IP address or enable NAT.
- Network-plus mode: The network-plus mode is a combination of the network mode and client mode. IP addresses of branches and headquarters are configured beforehand. The remote device applies to the server for an IP address. The server uses the IP address to perform ping, Telnet mode, or other management and maintenance operations. NAT is not performed on packets to be protected.

Efficient VPN License

The Efficient VPN function is used with a license. To use the Efficient VPN function, apply for and purchase the following license from the Huawei local office:

NOTE

The AR100&AR120 series can use the Efficient VPN feature without a license.

- AR150&AR160&AR200 series: AR150&160&200 Value-Added Security Package

 Copyright © Huawei Technologies Co., Ltd.

- AR1200 series: AR1200 Value-Added Security Package
- AR2200 series: AR2200 Value-Added Security Package
- AR3200 series: AR3200 Value-Added Security Package
- AR3600 series: AR3600 Value-Added Security Package

2.17.1.2 IPSec Policy Management

Context

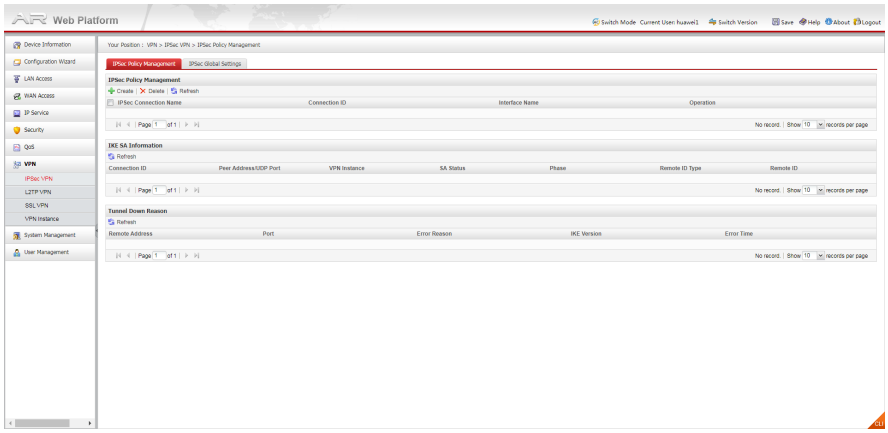
Authentication and encryption parameters in an IPSec policy must be consistent on two devices

For details about basic IPSec concepts, see **Overview**.

Procedure

- Creating an IPSec policy
  a. Choose **VPN** > **IPSec VPN** > **IPSec Policy Management**.

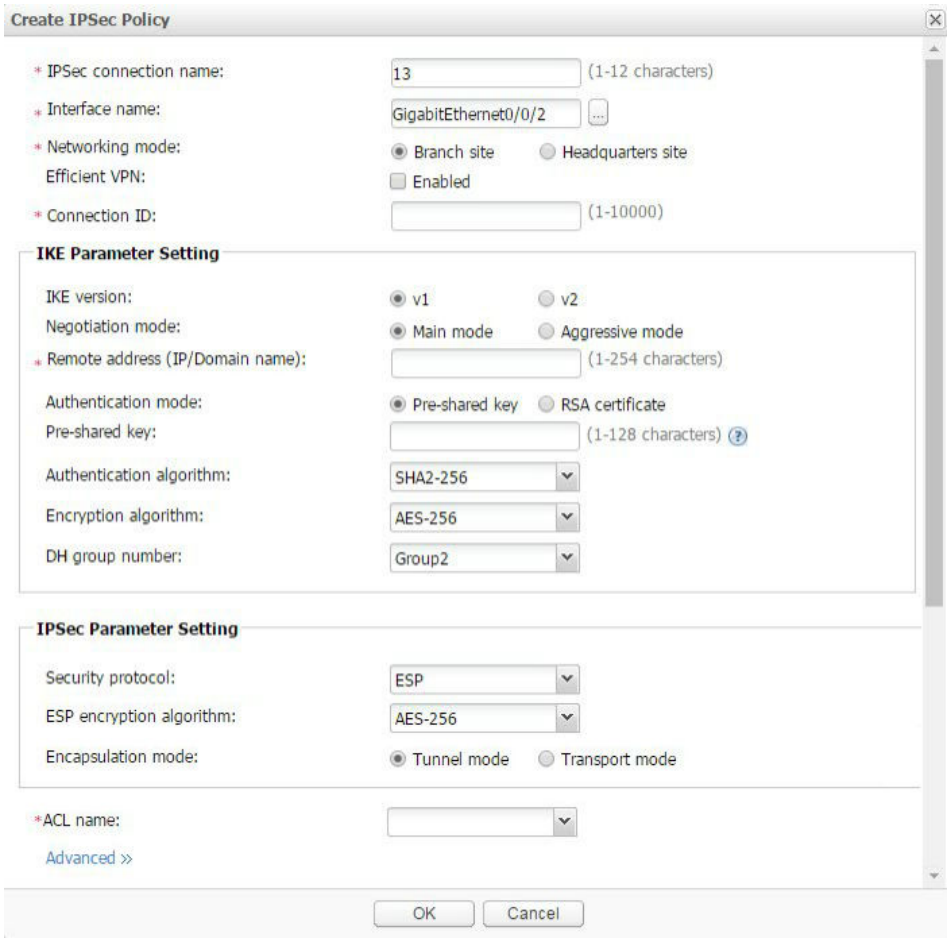
  Figure 2-216 IPSec Policy Management

  b. Click **Create** and set **IPSec connection name** and **Interface name** in the **Create IPSec Policy** dialog box that is displayed, and click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-217 Create IPSec Policy



c. Set other parameters listed in **Table 2-160** based on the site requirements.

d. Click **OK**.

The created IPSec policy is displayed in the **IPSec Policy Management** area.

Table 2-160 IPSec policy parameters

Parameter		Description
IPSec policy parameter setting	IPSec connection name	Name of an IPSec policy. The IPSec policy name cannot be changed after an IPSec policy is configured.

Copyright © Huawei Technologies Co., Ltd.

Parameter		Description
	Interface name	Name of the interface where an IPSec policy is applied. Click  , select an interface in the interface list, and click **OK**. If a tunnel interface is selected, instead of ACLs, a virtual tunnel interface is used to establish an IPSec tunnel to protect data flows. For details about the tunnel interface configuration, see **Logical Interface**. The interface cannot be changed after an IPSec policy is configured.
	Networking mode	Networking mode of a router: • Branch site: The router functions as the enterprise branch gateway and establishes IPSec tunnels between a branch and the headquarters or among different branches. A branch site can be configured as an Efficient VPN remote end. • Headquarters site: The router functions as the headquarters gateway and establishes IPSec tunnels with a branch after receiving an IPSec connection request from the branch. A headquarters site can be configured as an Efficient VPN server. The networking mode cannot be changed after an IPSec policy is configured.
	Efficient VPN	Whether to enable Efficient VPN for a branch site. The Efficient VPN configuration cannot be changed after an IPSec policy is configured.
	Connection ID	ID of an IPSec policy. The **IPSec connection name** and **Connection ID** parameters identify an IPSec policy. Multiple IPSec policies with the same IPSec connection name constitute an IPSec policy group. An IPSec policy group contains a maximum of 16 IPSec policies, and an IPSec policy with the smallest ID has the highest priority. After an IPSec policy group is applied to an interface, all IPSec policies in the group are applied to the interface to protect different data flows.
IKE parameter setting	IKE version	ID of an IKE version, including IKEv1 or IKEv2.

Copyright © Huawei Technologies Co., Ltd.

Parameter		Description
	Negotiation mode	IKEv1 negotiation mode. • Main mode: The main mode separates the key exchange information from identity authentication information. This provides higher security. • Aggressive mode: The aggressive mode does not provide identity authentication but can meet special network requirements. This mode can be used to establish an IKE SA more quickly when the IP address of the SA initiator is unknown or keeps changing, and both ends need to use the pre-shared key authentication to establish the IKE SA.
	Mode	Efficient VPN mode when the device is configured as an Efficient VPN remote end. The Efficient VPN modes are as follows: • Client • Network • Network-plus
	Remote address (IP/ Domain name)	IP address or domain name of the remote IKE peer.
	Authentication mode	Authentication method used by IKE: • Pre-shared Key • RSA certificate By default, the IKE uses pre-shared key authentication.
	Pre-shared Key	Pre-shared key used by IKE for authentication. The value is a string of characters. A plain text key contains 1 to 128 characters, and a cipher text password contains 48 to 188 characters. If the character string contains question mark (?) or space, you need to put the key in double quotation marks ("). The local and remote ends of IKE negotiation must be configured with the same authenticator.
	PKI Domain	Configured public key infrastructure (PKI) domain. When IKE uses the Rivest-Shamir-Adleman Algorithm (RSA) certificate for authentication, set this parameter. For details about the PKI domain configuration, see **PKI Domain**.
	OCSP	Whether to enable Online Certificate Status Protocol (OCSP)

Copyright © Huawei Technologies Co., Ltd.

Parameter		Description
	Authentication algorithm	Authentication algorithm used by the IKE: • MD5: specifies HMAC-MD5 as the authentication algorithm. • SHA1: specifies HMAC-SHA-1 as the authentication algorithm. • AES-XCBC-MAC-96: specifies AES-XCBC-MAC-96 as the authentication algorithm. **NOTE** The AES-XCBC-MAC-96 algorithm only supports in IKEv2. The AES-XCBC-MAC-96 algorithm does not supported in V200R010C10 and later versions. • SHA2-256: SHA-256 as the authentication algorithm. • SHA2-384: SHA-384 as the authentication algorithm. • SHA2-512: SHA-512 as the authentication algorithm. • SM3: SM3 as the authentication algorithm. **NOTE** The SM3 algorithm only supports in IKEv1. The MD5 algorithm uses a 128-bit key, and the SHA-1 algorithm uses a 160-bit key. The SHA-256, SHA-384, and SHA-512 algorithms use 256-bit, 384-bit, and 512-bit keys respectively. A larger number of key bits indicate a more secure algorithm but a slower calculation speed. Only IKEv2 supports the AES-XCBC-MAC-96 algorithm. By default, the IKE uses the SHA2-256 algorithm. Note that MD5 and SHA1 authentication algorithms cannot ensure security. You are advised to use another authentication algorithm.

Copyright © Huawei Technologies Co., Ltd.

Parameter		Description
	Encryption algorithm	Encryption algorithm used by the IKE: ● 3DES: indicates that the IKE uses the 168-bit Triple Data Encryption Standard (3DES) encryption algorithm in CBC mode. ● AES-128: indicates that the IKE uses the 128-bit Advanced Encryption Standard (AES) encryption algorithm. ● AES-192: indicates that the IKE uses the 192-bit AES algorithm encryption. ● AES-256: indicates that the IKE uses the 256-bit AES algorithm encryption. ● DES: indicates that the IKE uses the DES-CBC encryption algorithm. ● SM1:SM1 encryption algorithm. ● SM4:SM4 encryption algorithm. By default, the IKE uses the AES-256 encryption algorithm. Note that 3DES and DES encryption algorithms cannot ensure security. You are advised to use another encryption algorithm.
	DH group number	Diffie-Hellman group used in IKE negotiation, which is key negotiation: ● Group1: uses the 768-bit Diffie-Hellman group. ● Group2: uses the 1024-bit Diffie-Hellman group. ● Group5: uses the 1536-bit Diffie-Hellman group. ● Group14: uses the 2048-bit Diffie-Hellman group. ● Group19: uses the 256-bit ECP Diffie-Hellman group. ● Group20: uses the 384-bit ECP Diffie-Hellman group. ● Group21: uses the 521-bit ECP Diffie-Hellman group. Group1 provides the lowest encryption, while Group14 provides the strongest encryption. By default, the Group14 is used in IKE negotiation.

 Copyright © Huawei Technologies Co., Ltd.

Parameter		Description
IPSec parameter setting	Security protocol	Security protocol used by an IPSec: • AH: indicates that the IPSec uses the AH protocol defined by RFC 2402. The AH protocol authenticates the data source, verifies the data integrity, and prevents packet replay. This protocol uses the MD5 authentication algorithm by default and does not support encryption. • AH-ESP: indicates that the IPSec proposal encapsulates packets through ESP, then through AH. • ESP: indicates that the IPSec uses the ESP protocol defined by RFC 2406. The ESP protocol uses the DES encryption algorithm. The AH protocol uses the MD5 authentication algorithm by default. By default, the IPSec uses the ESP protocol.
	AH authentication algorithm	Authentication algorithm used by AH in the IPSec: • MD5 • SHA1 • SHA2-256 • SHA2-384 • SHA2-512 • SM3 **NOTE** The SM3 algorithm only supports in IKEv1. By default, AH uses the SHA2-256 authentication algorithm. Note that MD5 and SHA1 authentication algorithms cannot ensure security. You are advised to use another authentication algorithm. **NOTE** AR100&AR120 series, AR161, AR161W, AR161EW, AR161EW-M1, AR161G-L, AR161G-Lc, AR161G-U, AR169, AR169G-L, AR169CVW, AR169CVW-4B4S, AR169W, AR169W-P-M9, AR169RW-P-M9, AR169EW, AR169EGW-L, AR1220C, AR1220-8GE, AR2204-27GE, AR2204E-D-27GE, AR2204-24GE, AR2204-27GE-P, AR2204-48GE-P, AR2204-51GE, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D, AR2204XE, and AR2204XE-DC do not support SHA2-384 and SHA2-512 authentication algorithms.

Copyright © Huawei Technologies Co., Ltd.

Parameter		Description
	ESP authentication algorithm	Authentication algorithm used by ESP in the IPSec: • Non-authentication • MD5 • SHA1 • SHA2-256 • SHA2-384 • SHA2-512 • SM3 **NOTE** 1. The SM3 algorithm only supports in IKEv1. 2. When configures the SM3 algorithm, the ESP encryption algorithm must select **SM1**, **SM4**, or **Non-encryption**. The authentication algorithm and encryption algorithm of ESP cannot be kept blank simultaneously. By default, ESP uses the SHA2-256 authentication algorithm. Note that MD5 and SHA1 authentication algorithms cannot ensure security. You are advised to use another authentication algorithm. **NOTE** AR100&AR120 series, AR161, AR161W, AR161EW, AR161EW-M1, AR161G-L, AR161G-Lc, AR161G-U, AR169, AR169G-L, AR169CVW, AR169CVW-4B4S, AR169W, AR169W-P-M9, AR169RW-P-M9, AR169EW, AR169EGW-L, AR1220C, AR1220-8GE, AR2204-27GE, AR2204E-D-27GE, AR2204-24GE, AR2204-27GE-P, AR2204-48GE-P, AR2204-51GE, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D, AR2204XE, and AR2204XE-DC do not support SHA2-384 and SHA2-512 authentication algorithms.

Copyright © Huawei Technologies Co., Ltd.

Parameter		Description
	ESP encryption algorithm	Encryption algorithm used by ESP in the IPSec: • Non-encryption • DES: indicates that the IKE uses the DES-CBC encryption algorithm. • 3DES: indicates that the IKE uses the 168-bit 3DES encryption algorithm in CBC mode. • AES-128: indicates that the IKE uses the 128-bit AES encryption algorithm. • AES-192: indicates that the IKE uses the 192-bit AES algorithm encryption. • AES-256: indicates that the IKE uses the 256-bit AES algorithm encryption. • SM1:SM1 encryption algorithm. • SM4:SM4 encryption algorithm. **NOTE** 1. The SM1 and SM4 algorithm only supports in IKEv1. 2. When configures SM1 or the SM4 algorithm, the ESP certification algorithm must select **SHA1**, **SM3**, or **Non-authentication**. By default, ESP uses the AES-256 encryption algorithm. Note that 3DES and DES encryption algorithms cannot ensure security. You are advised to use another encryption algorithm.
	Encapsulation mode	Encapsulation mode that IPSec uses to encapsulate IP packets: • Tunnel mode • Transport mode
ACL parameter setting	ACL name	Name of a configured ACL that IPSec uses to protect data flows. When the router functions as the headquarters site, you can configure no ACL to protect all data flows on the interface. For details about the ACL configuration, see **Advanced ACL Setting**. IPSec supports ACL rules based on the source IP address, destination IP address, destination port number, and protocol number to protect data flows.

Copyright © Huawei Technologies Co., Ltd.

Parameter		Description
Advanced	IKE negotiation	Mode in which IKE SAs are triggered: • Auto: After an IPSec policy is applied, the system completes IKE negotiation and establishes an IPSec tunnel. • Traffic-based: When an interface receives packets, the system completes IKE negotiation and establishes an IPSec tunnel. By default, the IKE negotiation uses auto mode.
	Local identity type	Type of the local ID used in IKE negotiation: • IP address: The interface IP address is used as the local ID. When performing IKE negotiation with the peer, the local device exchanges identity information with the peer. • Name: A string of characters is used as the local ID. You can set **Device local name** in **IPSec Global Setting** to identify the local device. When **Device local name** is left blank, the device name is used. By default, the IP address of the local end is used as the local ID.
	Locale ID	ID of the local in IKE negotiation.
	Peer identity type	Type of the remote ID used in IKE negotiation: • IP address: value of **Peer address (IP/Domain name)**. • Name: value of **Peer name**. By default, the IP address of the remote end is used as the remote ID.
	Remote ID	ID of the peer in IKE negotiation. The value must be the local ID configured on the peer.
	Re-authentication interval (seconds)	The IKEv2 re-authentication interval is set. By default, IKEv2 re-authentication is not performed.
	DPD(Dead Peer Detection)	Whether to enable the dead peer detection (DPD) function. IKE peers send DPD packets to check whether the other party is alive. By default, DPD is disabled.

Copyright © Huawei Technologies Co., Ltd.

Parameter		Description
	DPD type	DPD mode: • on-demand: indicates the on-demand DPD mode. If the local end does not receive any packets from the remote peer within the specified period, it sends a DPD packet to check whether the remote peer is available. • periodic: indicates the periodic DPD mode. If the local end does not receive any packets from the remote peer for a long time, it sends DPD packets at specific intervals to check whether the remote peer is available.
	The sequence of the payload in DPD packets	Sequence of the payload in DPD packets: • seq-hash-notify: indicates that the payload of DPD packets is in the sequence of hash-notify. • seq-notify-hash: indicates that the payload of DPD packets is in the sequence of notify-hash. By default, the payload in DPD packets is in the sequence of notify-hash.
	Idle time for DPD detection (seconds)	Idle time for sending DPD packets. The default idle time for DPD is 30 seconds.
	DPD packet retransmission interval (seconds)	Interval for retransmitting DPD packets. The default interval for retransmitting DPD packets is 15 seconds.
	DPD packet retransmission count	Maximum number of times DPD packets are retransmitted. The default maximum number of times DPD packets are retransmitted is 3.

Copyright © Huawei Technologies Co., Ltd.

Parameter		Description
	PRF algorithm	Algorithm used to generate the pseudo random number: ● PRF-HMAC-MD5: indicates the HMAC-MD5 algorithm. ● PRF-HMAC-SHA: indicates the HMAC-SHA-1 algorithm. ● PRF-AES-XCBC-128: indicates the AES-XCBC-128 algorithm. ● PRF-HMAC-SHA2-256: indicates the HMAC-SHA-256 algorithm. ● PRF-HMAC-SHA2-384: indicates the HMAC-SHA-384 algorithm. ● PRF-HMAC-SHA2-512: indicates the HMAC-SHA-512 algorithm. By default, the PRF-HMAC-SHA2-256 algorithm is used.
	PFS	The Perfect Forward Secrecy (PFS) enables IPSec to perform an additional round of key exchange in phase 2 of IKE negotiation to improve communication security: ● none: the PFS feature is disabled. ● Group1: indicates the 768-bit Diffie-Hellman group. ● Group2: indicates the 1024-bit Diffie-Hellman group. ● Group5: indicates the 1536-bit Diffie-Hellman group. ● Group14: indicates the 2014-bit Diffie-Hellman group. ● Group19: uses the 256-bit ECP Diffie-Hellman group. ● Group20: uses the 384-bit ECP Diffie-Hellman group. ● Group21: uses the 521-bit ECP Diffie-Hellman group. By default, the PFS feature is disabled.
	IKE SA lifetime (seconds)	Lifetime of IKE SAs. Both ends negotiate a new SA before the old one times out. The old SA is still used prior to the establishment of the new SA. By default, the lifetime of an IKE SA is 86400 seconds.

Copyright © Huawei Technologies Co., Ltd.

Parameter		Description
	IPSec SA aging mode	SA lifetime in an IPSec policy. In IPSec negotiation, the SA uses the shorter lifetime between the lifetime set on the local end and that set on the remote end. The SA lifetime can be measured by time or by traffic: • Time-based (s): indicates the period of time an SA can exist after being established. • Traffic-based (KB): indicates the maximum traffic volume that an SA can process. By default, the time-based SA lifetime is 3600 seconds and the traffic-based SA lifetime is 1843200 Kbytes. When the specified time or traffic volume is reached, the SA becomes invalid. When the SA is about to expire, IPSec negotiates a new SA. By default, when no IPSec SA lifetime is set for the IPSec policy, the global IPSec SA lifetime is used. The global IPSec SA lifetime is set by the parameter **IPSec SA aging management** in **IPSec Global Setting**. If **IPSec SA aging management** is not set, the default value is used.
	Local IP address	Whether to set the IP address of the local end. By default, the local end address is the IP address of the interface bound to the IPSec policy.
	Address mode	Type of the local IP address. • Interface: The local end address is the IP address of the interface bound to the IPSec policy. • IP address: When the outbound interface has a primary address and a secondary address, enter an IP address in the **IP address** text box.
	IP address	IP address of the local end in IKE negotiation.
	Route import	Whether to enable the route import function.
	Route import type	Route import mode: • Static: The route of the IPSec peer is added to the local routing table upon device startup and remains unchanged. • Dynamic: Route reachability is determined based on IPSec tunnel status. If the IPSec tunnel is Up, the route of the IPSec peer is added to the local routing table and advertised on the network. If the IPSec tunnel is Down, the route of the IPSec peer is deleted and withdrawn.

Copyright © Huawei Technologies Co., Ltd.

Parameter		Description
	Route priority	Priority of an injection route. By default, the priority is 60.
	Pre-extraction of original IP packets	Pre-extraction of original IP packets is enabled. By default, pre-extraction of original IP packets is disabled. In tunnel mode, QoS parameters such as the packet header and protocol type in original packets are hidden after IP packets are encapsulated through IPSec. Although IPSec uses the DSCP field in original packets as the DSCP field in the IP packet header, some QoS solutions require quintuple information. The encryption device can pre-extract quintuple information including the source address, destination address, protocol type, source port number, and destination port number to facilitate refined QoS management on IPSec packets.

- Modifying an IPSec policy

  NOTE

  If an IPSec policy configured by a command is not applied to a specified interface, the policy is not displayed on the IPSec policy management page.

  a. Choose **VPN** > **IPSec VPN** > **IPSec Policy Management**.
  b. Select an IPSec to modify in the **IPSec Policy Management** area and click .
  c. In **Modify IPSec Policy** dialog box that is displayed, modify parameters listed in **Table 2-160** based on the site requirements.
  d. Click **OK**.
- Deleting an IPSec policy
  a. Choose **VPN** > **IPSec VPN** > **IPSec Policy Management**.
  b. Select an IPSec to delete in the **IPSec Policy Management** area and click **Delete**.

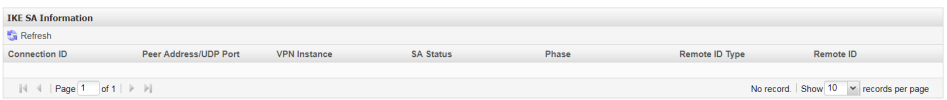
     The selected IPSec policy is not displayed in the **IPSec Policy Management** area.
- Viewing IKE SA information

  NOTE

  This function is supported only in the V200R010C10 and later versions.

  You can refresh and view information about the SA set up using IKE negotiation through the **IKE SA Information** window.

Figure 2-218 IKE SA Information



 Copyright © Huawei Technologies Co., Ltd.

- Viewing tunnel failure information.

  NOTE

  This function is supported only in the V200R010C10 and later versions.

  In **Tunnel Down Reason**, click **Refresh** to refresh and view tunnel failure information

  Figure 2-219 Tunnel Down Reason

----End

2.17.1.3 IPSec Global Settings

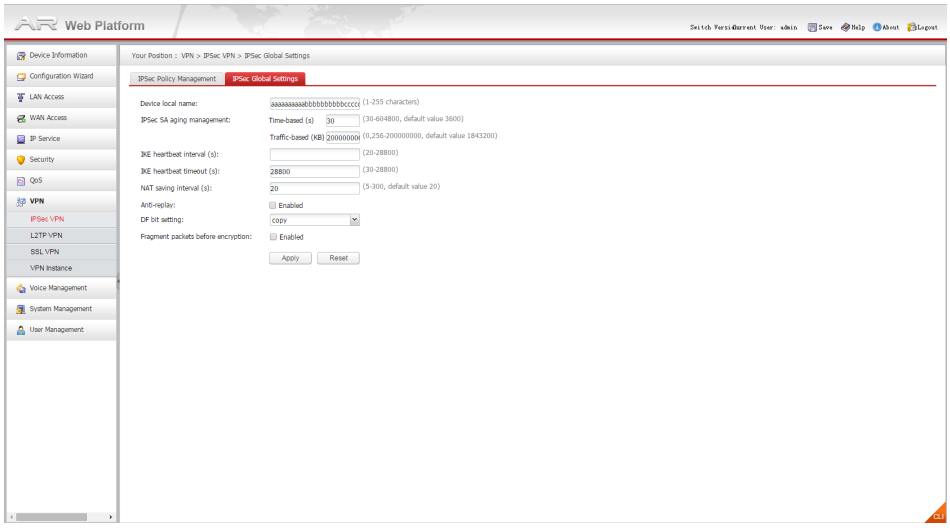
Context

This section describes how to set optional global IPSec parameters.

Procedure

- Setting global IPSec parameters
  a. Choose **VPN** > **IPSec VPN** > **IPSec Global Setting**.

  Figure 2-220 Setting global IPSec parameters

  b. Set parameters listed in **Table 2-161**.
  c. Click **Apply** to make the settings to take effect.
  To restore the default settings of all parameters, click **Reset**.

 Copyright © Huawei Technologies Co., Ltd.

Table 2-161 Global IPSec parameters

Parameter	Description
Device local name	Local host name used in IKE negotiation, which is case-insensitive. You can configure IPSec policies on the **IPSec Policy Management** tab page. You need to set **Device local name** only when **Local identity type** is set to **Name**. The value of **Device local name** must be the same as the value of **Peer name** set on the peer device. By default, no local host name is configured for IKE negotiation. The device name is used as the local name. To view or change the device name, see device information in **Device Information**.
IPSec SA aging management	Global SA lifetime in an IPSec policy. In IPSec negotiation, the SA uses the shorter lifetime between the lifetime set on the local end and that set on the remote end. The SA lifetime can be measured by time or by traffic: • Time-based (s): indicates the period of time an SA can exist after being established. • Traffic-based (KB): indicates the maximum traffic volume that an SA can process. When the specified time or traffic volume is reached, the SA becomes invalid. When the SA is about to expire, IPSec negotiates a new SA. If **SA aging mode** is set on the **IPSec Policy Management** tab page, the global SA lifetime does not take effect. By default, the time-based global SA lifetime is 3600 seconds, and the traffic-based global SA lifetime is 1843200 KB.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
IKE heartbeat interval (s)	Interval for sending heartbeat packets. If no heartbeat packet is received during the duration specified by **IKE heartbeat timeout**, the IPSec SA is deleted. Therefore, the timeout duration of heartbeat packets must be set longer than the interval for sending heartbeat packets.
IKE heartbeat timeout (s)	Timeout interval during which an IKE SA waits for a heartbeat packet. On a network, packet loss rarely occurs more than three consecutive times. Therefore, the timeout interval of heartbeat packets on one end can be set to three times the interval for sending heartbeat packets on the other end.
NAT saving interval (s)	Interval for sending NAT keepalive packets. If the IPSec tunnel with NAT traversal enabled is established and no packet passes through the NAT gateway in a long period, NAT session entries are aged and deleted on the NAT gateway. In this case, data cannot be transmitted through the IPSec tunnel. Therefore, to retain NAT session entries, configure the device to send NAT keepalive packets periodically. By default, the interval for sending NAT keepalive packets is 20 seconds.
Anti-replay	Whether to enable the anti-replay function. After the anti-replay function is enabled, the system discards replayed packets and does not encapsulate them, saving system resources. By default, the anti-replay function is enabled.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
DF bit setting	Don't fragment (DF) flag bit: • **clear**: If the DF flag bit is 0, IP packets can be fragmented. • **set**: If the DF flag bit is 1, no IP packet is fragmented. • **copy**: Specifies the flag bit of original packets. By default, the DF flag bit on an IPSec tunnel is the flag bit of original packets.
Fragment packets before encryption	Whether to enable packet fragment before encryption when the DF flag bit is 0. Before IP packets are encapsulated with the IPSec header, the system calculates the predicted length of the encapsulated IP packets. If the predicted length of the encapsulated IP packets exceeds the MTU of the outbound interface, the router fragments the IP packets before encryption. The IKE peer of the router decrypts and assembles IPSec fragments. This reduces the CPU usage of the router. By default, IP packets are fragmented after being encrypted on an IPSec tunnel.

----End

2.17.2 L2TP VPN

2.17.2.1 Overview

As enterprises develop and services increase, many branches are set up in different locations. Some staff often go on business trips, and some may work at home. They require fast, secure, and reliable network connections with the headquarters. On traditional dial-up networks, they use phone lines leased by the Internet Service Provider (ISP) and apply for a dial string or IP addresses from the ISP. This results in high costs. Besides, leased lines cannot provide services for the off-site staff especially the staff on business trips. To use the PSTN or ISDN and make it easy for users at different locations to access the headquarters network, VPDN is used. VPDN establishes a transparent point-to-point virtual link between remote users and the headquarters gateway.

Layer 2 Tunneling Protocol (L2TP) is a Virtual Private Dial-up Network (VPDN) technology that enables users to dial up to establish tunnel connections with a

Copyright © Huawei Technologies Co., Ltd.

remote end. L2TP uses PSTN or ISDN and is based on PPP negotiation to establish tunnels. It expands applications of the Point-to-Point Protocol (PPP) and is an important VPDN technology used by remote dial-up users to access the headquarters network. The PPP over Ethernet (PPPoE) technology expands applications of L2TP and can establish L2TP tunnels between remote users and the headquarters over Ethernet and Internet.

L2TP tunnels are established between the L2TP Network Server (LNS) and the L2TP Access Concentrator (LAC). When L2TP tunnels are established, remote users can access resources in the headquarters.

The LAC is an L2TP client, and the LNS is an L2TP server. A device can be deployed as the LAC or the LNS.

2.17.2.2 L2TP Client

Context

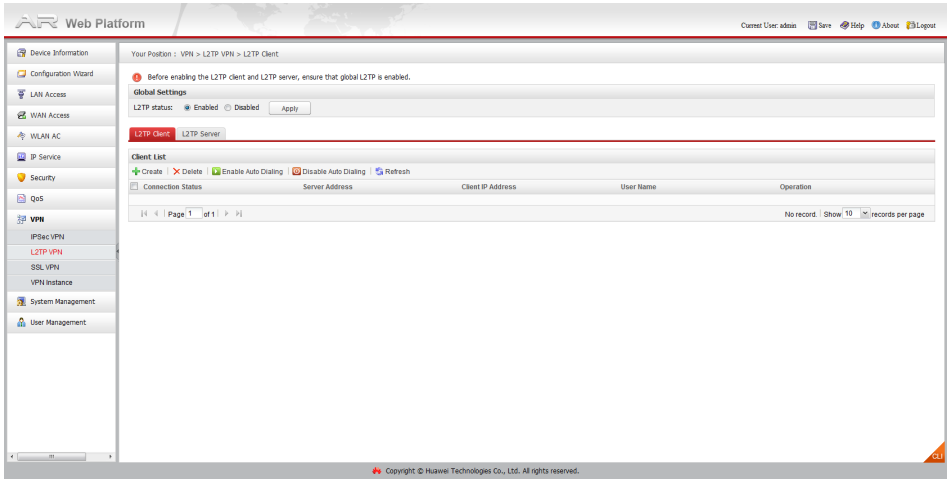
An L2TP client is deployed on the remote user side and connects to the L2TP server in automatic dialup mode.

An L2TP client initiates a virtual dialup request and sends information about itself to the L2TP server. The L2TP server authenticates L2TP client information and completes establishing the L2TP connection. Therefore, after a remote user can use an L2TP client access to connect to the L2TP server, the remote user can access resources in the headquarters where the L2TP server locates without any extra configuration.

Procedure

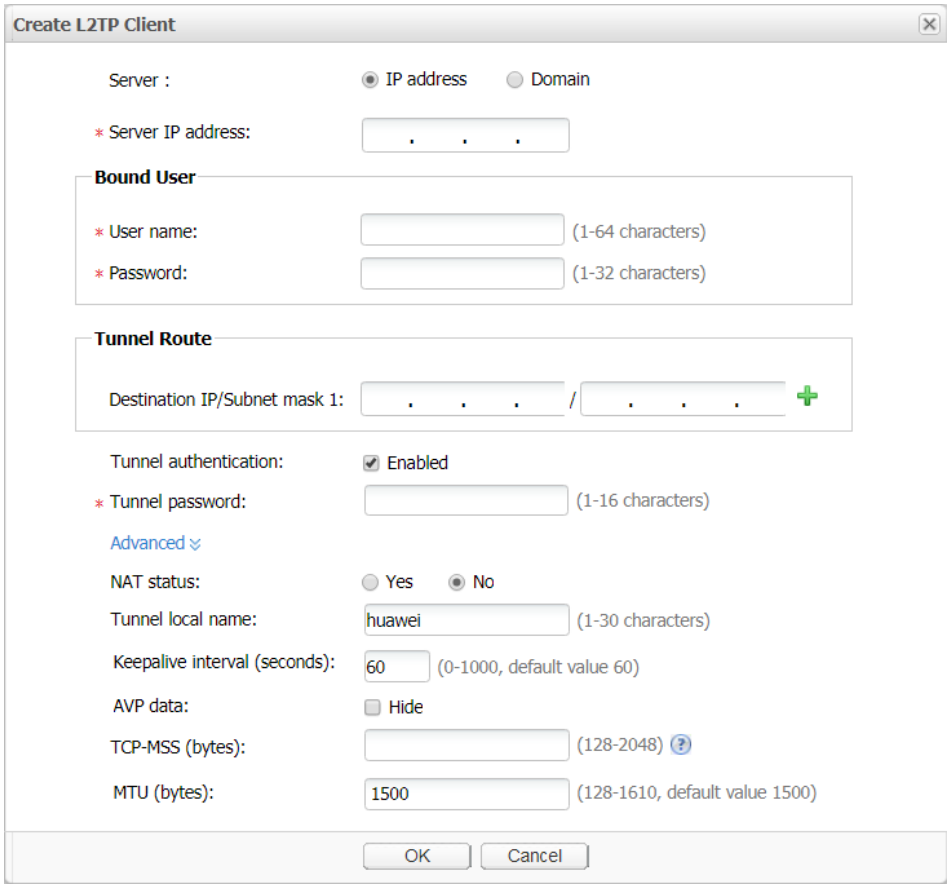
- Creating an L2TP client
  a. Choose **VPN** > **L2TP VPN** > **L2TP Client**.

  Figure 2-221 L2TP Client



  b. In the **Global Settings** area, set **L2TP status** to **Enable**, and click **Apply**.

c. Click **Create** in the **Client List** area.



d. In the **Create L2TP Client** dialog box, set parameters listed in **Table 2-162** based on the site requirements.

e. Click **OK**.

The created L2TP client is displayed in the **Client List** area. **Table 2-163** describes parameters in the client list.

f. Select the new L2TP client in the **Client List** area, and click **Enable Auto Dialing**.

Table 2-162 L2TP client parameters

Parameter	Description
Server IP address	IP address of the L2TP server.
Server Domain	The domain name of the L2TP server.
User name	User name of an L2TP client. An L2TP tunnel can be set up only when the same L2TP user name and password are configured on the L2TP client and L2TP server. You cannot set this parameter to the name of an online user.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Password	Password of an L2TP client.
Destination IP/Subnet mask 1	Allowed IP address segments on the L2TP server. Data of users who access the L2TP server is forwarded through the L2TP tunnel. An L2TP client supports a maximum of 10 IP address segments.
NAT status	The value **Yes** indicates that the source IP address of the data flow forwarded through the L2TP tunnel is replaced with the IP address allocated to the L2TP client by the L2TP server. By default, NAT is disabled.
Tunnel local name	Tunnel name of an L2TP client. By default, the device name is used as the tunnel name. To view or change the device name, see device information in **Device Information**.
Tunnel authentication	If tunnel authentication is enabled on the L2TP server, tunnel authentication must be enabled on the L2TP client. By default, tunnel authentication is disabled.
Tunnel password	Password for tunnel authentication. The tunnel password set on the L2TP client must be the same as that set on the L2TP server; otherwise, the L2TP client cannot pass the authentication. The value is a string of 1 to 16 case-sensitive characters without metacharacters, such as spaces and question marks. By default, no tunnel password is set.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Keepalive interval (seconds)	Interval for sending Hello packets through the tunnel. After a tunnel is set up between an L2TP client and the L2TP server, the L2TP client sends Hello packets to the L2TP server at a specified interval to check the connection. If the L2TP client receives no response from the L2TP server after sending five consecutive Hello packets, the tunnel connection between the L2TP client and the L2TP server automatically terminates. The default value is 60 seconds.
AVP data	AVP parameter encryption in L2TP packets. After setting this parameter, L2TP negotiation packets are encrypted during the L2TP session setup process, which improves security but increases the tunnel setup time. L2TP negotiation can be properly performed only when AVP parameter encryption is enabled on both the L2TP client and L2TP server. By default, AVP parameters are not encrypted.
TCP-MSS (bytes)	Maximum length of TCP packets on an interface. The recommended value of TCP-MSS is 1200 bytes.
MTU(bytes)	Maximum transmission unit (MTU) of an interface. The default MTU of an interface 1500 bytes.

Table 2-163 Parameters in the client list

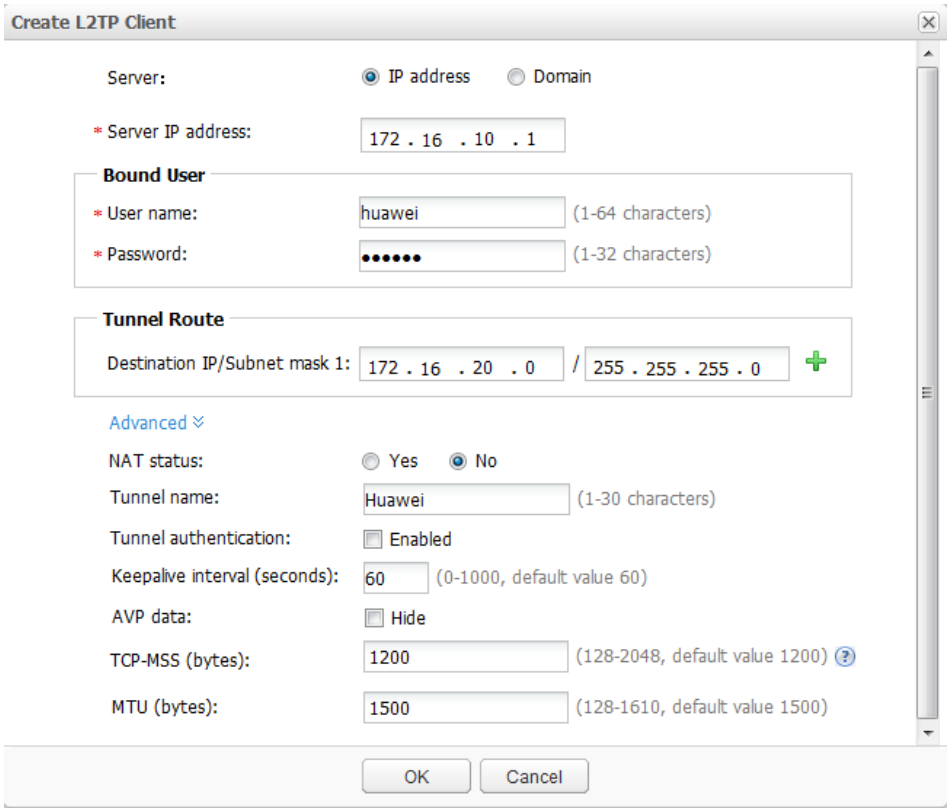
Parameter	Description
Connection Status	Whether the L2TP tunnel between the L2TP client and the L2TP server is set up.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Server Address	IP address of the L2TP server.
Client IP Address	IP address of an L2TP client.
User Name	User name of an L2TP client.

- Modifying an L2TP client
  a. Choose **VPN** > **L2TP VPN** > **L2TP Client**.
  b. In the **Client List** area, select an L2TP client, and click **Disable Auto Dialing**. The L2TP client is in **Down** state.
  c. Click  on the right.
  d. In the **Modify L2TP Client** dialog box, set parameters listed in **Table 2-162**.

  Figure 2-222 Modify L2TP Client



  e. Click **OK** to make the settings take effect.
- Deleting an L2TP client
  a. Choose **VPN** > **L2TP VPN** > **L2TP Client**.
  b. In the **Client List** area, select an L2TP client, and click **Disable Auto Dialing**. The L2TP client is in **Down** state.

 Copyright © Huawei Technologies Co., Ltd.

c. Click **Delete**.

d. In the dialog box that is displayed, click **OK**.

The deleted L2TP client is not displayed in the **Client List** area.

----End

2.17.2.3 L2TP Server

Context

An L2TP server is deployed in the headquarters and functions as the gateway.

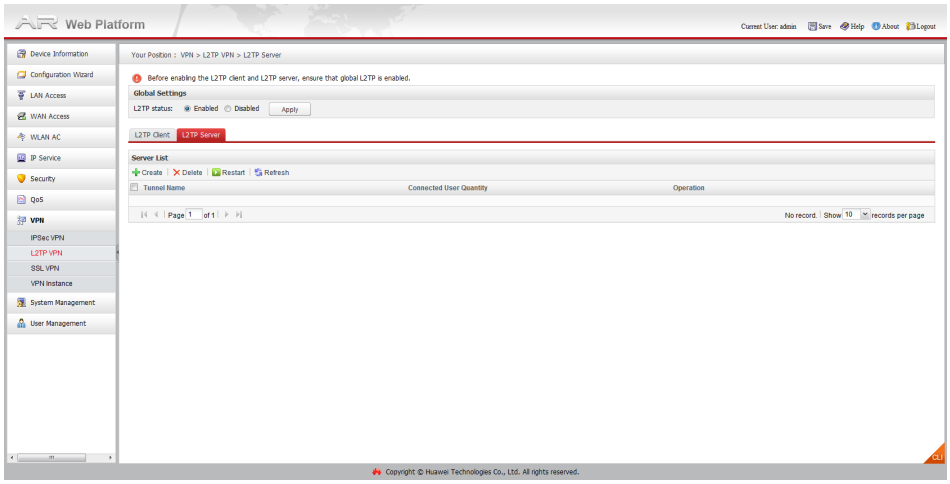
After receiving user information from an L2TP client, the L2TP server authenticates the user and responds to the L2TP tunnel setup request from the L2TP client. Then an L2TP connection is set up between the L2TP server and the L2TP client.

Procedure

- Creating an L2TP server

a. Choose **VPN** > **L2TP VPN** > **L2TP Server**.

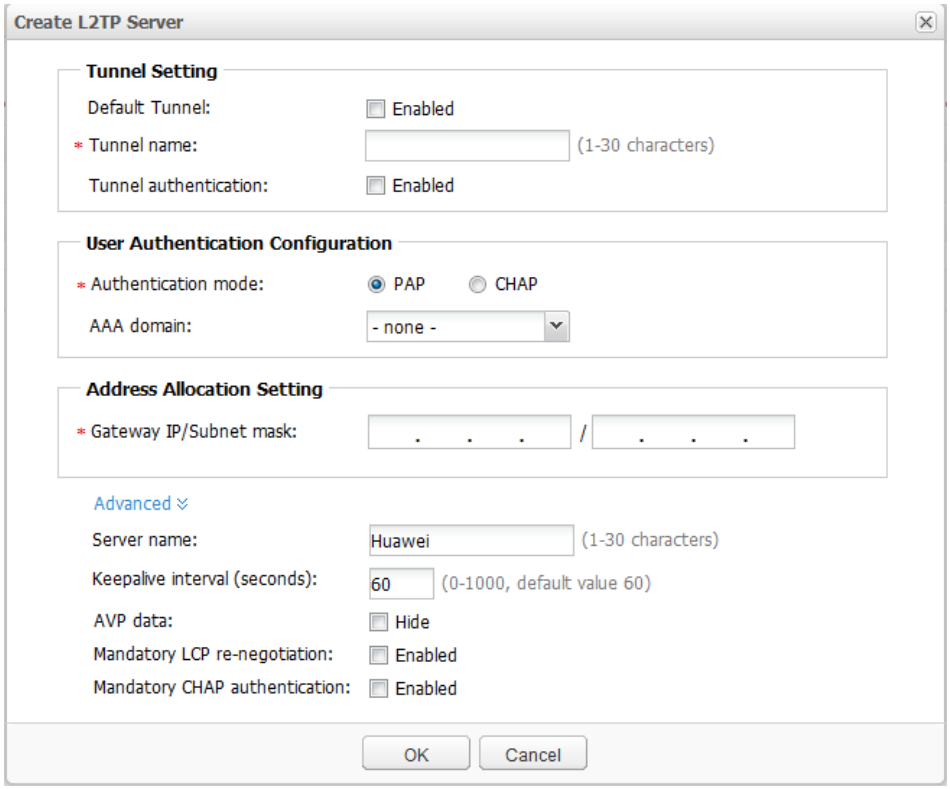
Figure 2-223 L2TP Server



b. In the **Global Settings** area, set **L2TP status** to **Enable**, and click **Apply**.

c. Click **Create** in the **Service List** area.

Figure 2-224 Create L2TP Server



d. In the **Create L2TP Server** dialog box, set parameters listed in **Table 2-164** based on the site requirements.

e. Click **OK**.

The created L2TP server is displayed in the **Service List** area. **Table 2-165** describes parameters in the service list.

Table 2-164 L2TP server parameters

Parameter	Description
Default Tunnel	Whether to configure a default L2TP tunnel. When a default L2TP tunnel is used, any L2TP client can establish an L2TP connection with the L2TP server. The default L2TP tunnel cannot be changed to a non-default L2TP tunnel.
Tunnel name	Tunnel name of an L2TP client that can access the L2TP server.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Tunnel authentication	When this parameter is selected, the L2TP server authenticates the L2TP client that initiates the tunnel setup request. An L2TP tunnel can be set up only when tunnel authentication is enabled and the same tunnel password is set on the L2TP server and client.
Tunnel password	If tunnel authentication is enabled, the tunnel password is required. An L2TP tunnel can be set up only when tunnel authentication is enabled and the same tunnel password is set on the L2TP server and client.
Confirm password	To prevent you from entering an incorrect password, enter the password again in the **Confirm password** text box.
Authentication mode	Authentication mode for L2TP clients. • PAP: two-way handshake authentication protocol that transmits passwords in plain text. PAP is used on networks that do not require high security. • CHAP: three-way handshake authentication protocol that transmits passwords in cipher text. On networks requiring high security, CHAP authentication is used to establish a PPP connection. In practice, CHAP authentication is widely used.
AAA domain	AAA domain. If you select a domain, the authentication mode of the domain is used. By default, an AAA domain named **default** exists on the router, and the **default** domain uses the authentication mode named **default**.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Gateway IP/Subnet mask	Private IP address and address pool of the L2TP server. In the **Gateway IP/Subnet mask** parameter, **Gateway IP** indicates the gateway address of the L2TP client, and **Subnet mask** indicates the IP address that is allocated to the L2TP client.
Server name	Tunnel name of an L2TP server. By default, no tunnel name is configured for the L2TP server. The device name is used as the tunnel name. To view or change the device name, see device information in **Device Information**.
Keepalive interval (seconds)	Interval for sending Hello packets through the tunnel. After a tunnel is set up between an L2TP client and the L2TP server, the L2TP server sends Hello packets to the L2TP client at a specified interval to check the connection. If the L2TP server receives no response from the L2TP client after sending 5bei consecutive Hello packets, the tunnel connection between the L2TP client and L2TP server automatically terminates. The default value is 60 seconds.
AVP data	AVP parameter encryption in L2TP packets. After setting this parameter, L2TP negotiation packets are encrypted during the L2TP session setup process, which improves security but increases the tunnel setup time. L2TP negotiation can be properly performed only when AVP parameter encryption is enabled on both the L2TP client and L2TP server. By default, AVP parameters are not encrypted.

Copyright © Huawei Technologies Co., Ltd.

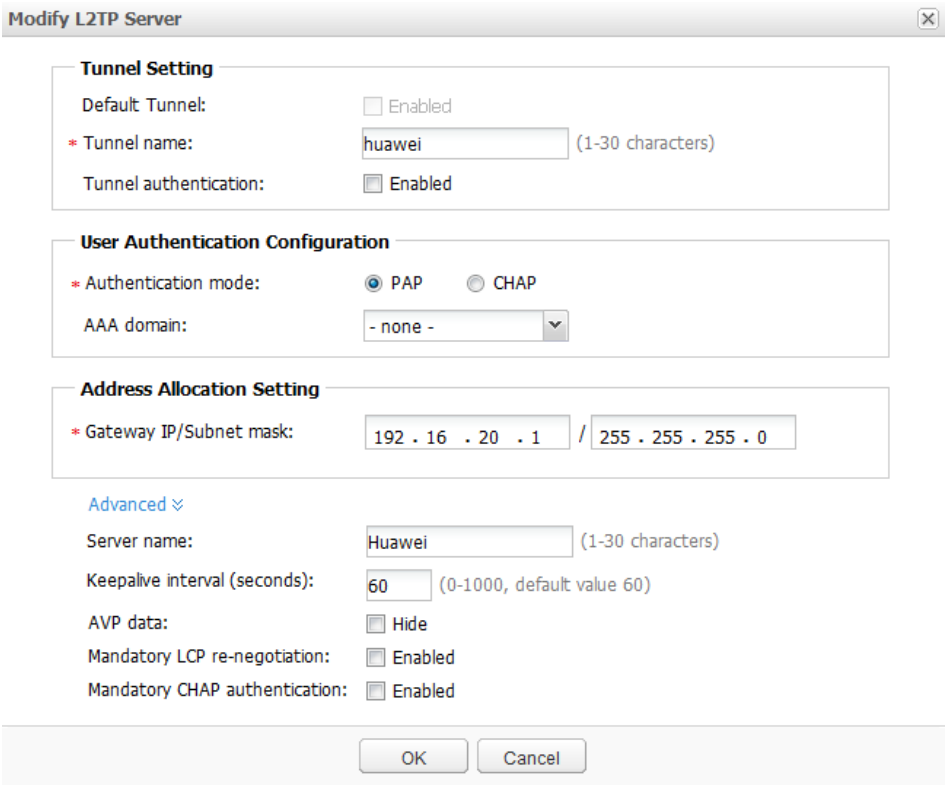
Parameter	Description
Mandatory LCP re-negotiation	LCP renegotiation. If mandatory LCP renegotiation is enabled, the L2TP performs second authentication after the first LCP negotiation is complete. The L2TP client needs to initiate the second negotiation, and the L2TP connection can be set up only after the second negotiation succeeds. Mandatory LCP renegotiation is applicable to scenarios that require high network security, and increases tunnel setup time. By default, mandatory LCP renegotiation is disabled. **NOTE** Some PPP clients may not support the second authentication. In this case, the L2TP connection fails when LCP renegotiation is enabled. When LCP renegotiation and mandatory CHAP authentication are configured simultaneously in an L2TP group, the LCP renegotiation takes effect.
Mandatory CHAP authentication	Mandatory CHAP authentication. If mandatory CHAP authentication is enabled, the L2TP server performs only CHAP authentication on L2TP clients. If CHAP authentication fails, the session cannot be set up. Mandatory CHAP renegotiation is applicable to scenarios that require high network security, and increases tunnel setup time. By default, mandatory CHAP authentication is disabled. **NOTE** Some PPP clients may not support the second authentication. In this case, the L2TP connection fails when mandatory CHAP authentication is enabled. When LCP renegotiation and mandatory CHAP authentication are configured simultaneously in an L2TP group, the LCP renegotiation takes effect.

Copyright © Huawei Technologies Co., Ltd.

Table 2-165 Parameters in the service list

Parameter	Description
Tunnel Name	Tunnel name of an L2TP client that can access the L2TP server. You do not need to specify the tunnel name when configuring the default tunnel.
Connected User Quantity	Number of access users on the L2TP server. You can click **Details** to manage access users.

- Modifying an L2TP server
  a. Choose **VPN** > **L2TP VPN** > **L2TP Server**.
  b. In the **Service List** area, select an L2TP server, and click  on the right.



  c. In the **Modify L2TP Server** dialog box, modify parameters listed in **Table 2-164**.
  d. Click **OK** to save the settings.
- Deleting an L2TP server
  a. Choose **VPN** > **L2TP VPN** > **L2TP Server**.
  b. In the **Service List** area, select an L2TP server to delete, and click **Restart** to terminate the tunnel connection.
  c. Click **Delete**.

 Copyright © Huawei Technologies Co., Ltd.

d. In the dialog box that is displayed, click **OK**.
The deleted L2TP server is not displayed in the **Service List** area.

- Managing access users on the L2TP server
  a. Choose **VPN** > **L2TP VPN** > **L2TP Server**.
  b. Select an L2TP server and click **Details** next to the number of access users.
  c. In the **Connected User** window, view information about access users listed in **Table 2-166**. You can query access users by the user name or IP address, and select a user and click **Disconnected Forcibly** to terminate the L2TP connection.

Table 2-166 Parameters of access users

Parameter	Description
User Name	Name of a remote user.
IP Address	IP address that the L2TP server allocates to a remote user.

----End

2.17.2.4 L2TP Information

Context

You can check L2TP tunnel and user session information.

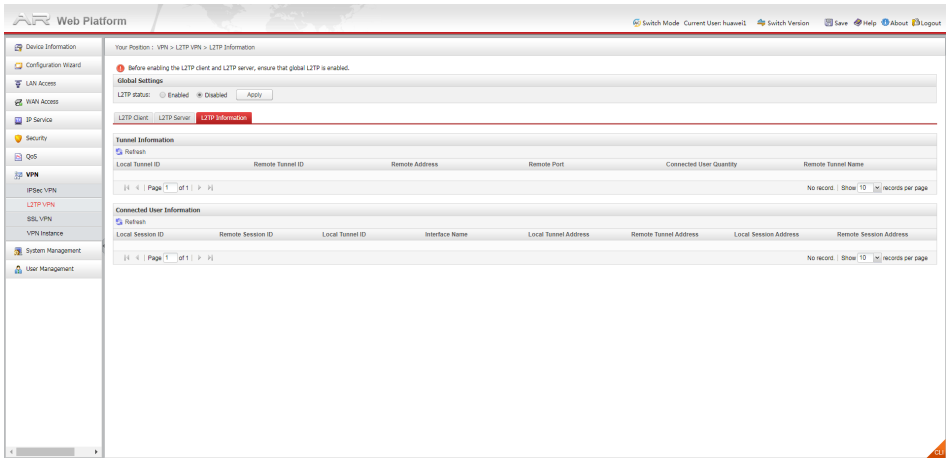
NOTE

This function is supported only in V200R010C10 and later versions.

Procedure

Step 1 Choose **VPN** > **L2TP VPN** > **L2TP Information**. The **L2TP Information** page is displayed.

Figure 2-225 L2TP Information page



 Copyright © Huawei Technologies Co., Ltd.

Step 2 Check L2TP information.

- In **Tunnel Information**, click **Refresh** to refresh and check L2TP tunnel information, as shown in **Figure 2-226**.

  Figure 2-226 Tunnel Information

- In **Connected User Information**, click **Refresh** to refresh and check user session information, as shown in **Figure 2-227**.

  Figure 2-227 Connected User Information

----End

2.17.3 SSL VPN

NOTE

The feature is just for beta test, and is not for commercial use. If the feature is required in the test, contact Huawei technical support personnel.

2.17.3.1 Overview

As the Internet technologies develop, people can access an enterprise's internal resources whether they are at home, at work, or on the move. Enterprise employees, customers, and partners desire access to enterprises' intranets anywhere and anytime. Unauthorized users or insecure access hosts may threaten security of enterprises' intranets.

SSL VPN is a type of secure access VPN technology. Based on the HTTPS protocol, SSL VPN uses the data encryption, user identity authentication, and message integrity check mechanisms of the SSL protocol to help ensure that remote access to enterprise intranets is safe and secure.

An SSL VPN gateway is located at an intranet edge, and works with the browsers installed on remote terminals or with clients downloaded using browsers to protect service data on the Internet. Additionally, the SSL VPN gateway functions as the proxy to allow users to access internal servers.

2.17.3.2 Virtual Gateway Management

Context

As an SSL VPN gateway, a device can function as multiple virtual gateways. The administrator configures services for each virtual gateway to meet different access

 Copyright © Huawei Technologies Co., Ltd.

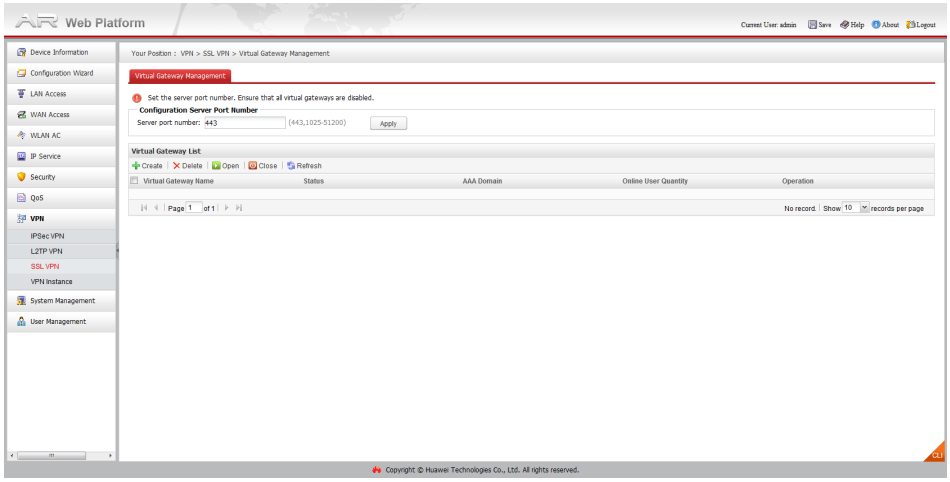
requirements of users. The mechanism that a device functions as multiple virtual gateways enables different user groups to access their own virtual gateways, which saves the enterprise costs. To deploy the SSL VPN function on a device, the administrator creates multiple virtual gateways on the device and configures the basic functions, web proxy, port forwarding, network extension, and page customization.

After a virtual gateway is configured, ensure that the HTTPS service runs properly. By default, the HTTPS service is disabled on the router. For details on how to configure the HTTPS service, see **Service Management**.

Procedure

- Creating a virtual gateway
  a. Choose **VPN** > **SSL VPN** > **Virtual Gateway Management**.

  Figure 2-228 Virtual Gateway Management

  b. (Optional) Set **Server port number** to the port number used by the SSL VPN, and click **Apply**.

  By default, port 443 is used by the SSL VPN.

  Before configuring the service port number, ensure that all virtual gateways in the **Virtual Gateway List** area are in **closed** state. You can select the check box next to a virtual gateway that is in **enabled** state, and click **Close** to disable the virtual gateway.

  c. In the **Virtual Gateway List** area, click **Create**.

  d. In the **Create Virtual Gateway** dialog box, set **Virtual gateway name** and click **OK**.

  e. In the **Virtual Gateway List** area, click **configurations** corresponding to the created virtual gateway to access the configuration page, and set parameters on the **Basic Configurations** tab page. Set parameters on the **Web Proxy**, **Port Forwarding**, **Network Extension**, and **Page Customization** based on the service requirements.

  f. Click **Return** in the upper right corner of the configuration page. The system returns to the **Virtual Gateway Management** page.

 Copyright © Huawei Technologies Co., Ltd.

The created virtual gateway in **closed** state is displayed in the **Virtual Gateway List** area. **Table 2-167** describes parameters in the Virtual Gateway Name.

g. A virtual gateway can take effect only after the virtual gateway is enabled. Select the check box next to the created virtual gateway, and click **Open**.

The virtual gateway is in **enabled** state.

Table 2-167 Parameters in the Virtual Gateway Name

Parameter	Description
Virtual Gateway Name	Name of a virtual gateway. Virtual gateway name is a part of the virtual gateway URL used by remote users for accessing. The URL is in the format of https://*device IP address or domain name*:*service port number*/*virtual gateway name*.
Status	Virtual gateway status. • enabled: Remote users can access the virtual gateway. • closed: Remote users cannot access the virtual gateway.
AAA Domain	AAA domain bound to a virtual gateway. A virtual gateway uses an AAA domain to manage access users, including local and remote authentication. For details on how to configure an AAA domain, see **Domain Setting**.
Online User Quantity	Number of access users. You can click **Details** next to the number of access users to view detailed information in the **Connected User** dialog box that is displayed. **Table 2-168** describes parameters of access users.
Operation	You can click **configurations** to access the configuration page.

Copyright © Huawei Technologies Co., Ltd.

Table 2-168 Parameters of access users

Parameter	Description
User Name	Name of a user that access the virtual gateway. You can click **Forcible logout** to terminate the connection of a user.
Online Duration (Minute)	Online time of a user, in minutes.
Authentication Mode	Authentication mode of the virtual gateway. • Local authentication: When receiving an access request from a remote user, the virtual gateway performs remote authentication based on user information saved on the local device. • Remote authentication: When receiving an access request from a remote user, the virtual gateway sends user information to the RADIUS server for authentication.

- Modifying a virtual gateway
  a. Choose **VPN** > **SSL VPN** > **Virtual Gateway Management**.
  b. Click **configurations** of the virtual gateway, and modify parameters on the **Basic Configurations**, **Web Proxy**, **Port Forwarding**, **Network Extension**, and **Page Customization** tab pages based on the site requirements.

     NOTE

     To modify the parameter **AAA domain** or **Internal interface** on the **Basic Configurations** tab page, disable the virtual gateway first.
  c. Click **Return** in the upper right corner of the configuration page. The system returns to the **Virtual Gateway Management** page.
  d. A virtual gateway can take effect only after the virtual gateway is enabled. Select the modified virtual gateway and click **Open**.
- Deleting a virtual gateway
  a. Choose **VPN** > **SSL VPN** > **Virtual Gateway Management**.
  b. Click **Delete**, and click **OK** in the dialog box that is displayed.
     The deleted virtual gateway is not displayed in the **Virtual Gateway List** area.

----End

Copyright © Huawei Technologies Co., Ltd.

2.17.3.3 Basic Configurations

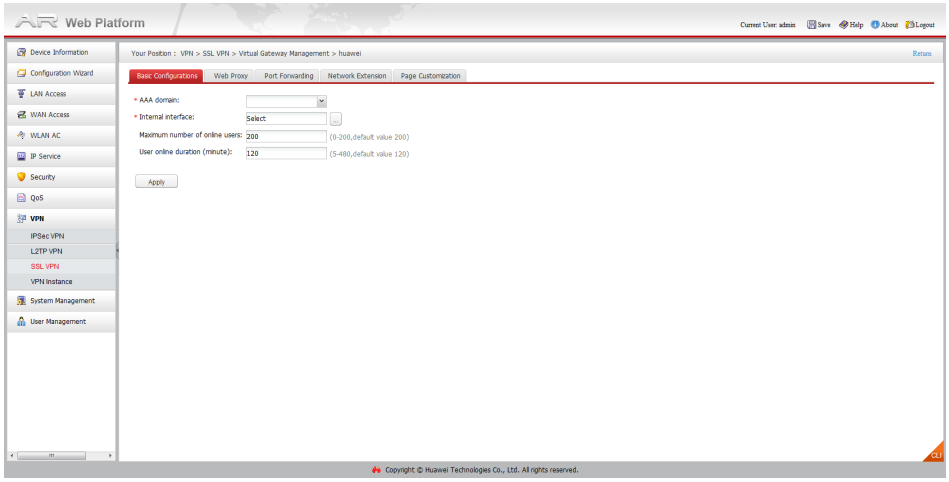
Context

Before enabling a virtual gateway, set basic parameters including the maximum number of online users and internal interface.

Procedure

Step 1 Choose **VPN** > **SSL VPN**, and click **configurations** of a virtual gateway. The **Basic Configurations** tab page is displayed.

Figure 2-229 Basic Configurations



Step 2 Set parameters listed in **Table 2-169**.

Step 3 Click **Apply**.

The system displays the message "Operation succeeded."

Table 2-169 Basic parameters

Parameter	Description
AAA domain	AAA domain bound to a virtual gateway. A virtual gateway uses an AAA domain to manage access users, including local and remote authentication. For details on how to configure an AAA domain, see **Domain Setting**.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Internal interface	Interface for connecting the intranet server. You can click  and select an interface in the **Select Interface** dialog box that is displayed, and click **OK**. **NOTE** Only interfaces with IP addresses configured are displayed in the **Select Interface** dialog box.
Maximum number of online users	Maximum number of users that can access a virtual gateway. When setting the maximum number of online users for multiple virtual gateways, ensure that the total number does not exceed the number of online users supported by the device and the license. The device specifications are as follows: ● AR100&AR120&AR150&AR160&AR200 series: 10 ● AR1200 series, AR2201-48FE, AR2202-48FE, AR2204, AR2204-27GE, AR2204E-D-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D: 50 ● AR2220, AR2220E, AR2240, AR2240C: 100 ● AR2204XE, AR2204XE-DC, AR3200&AR3600 series: 200
User online duration (minute)	Duration that a user can be online. After a user logs in to a virtual gateway, the user will be forcibly logged out when the online duration reaches the limit. The default maximum user online duration is 120 minutes.

----End

Copyright © Huawei Technologies Co., Ltd.

2.17.3.4 Web Proxy

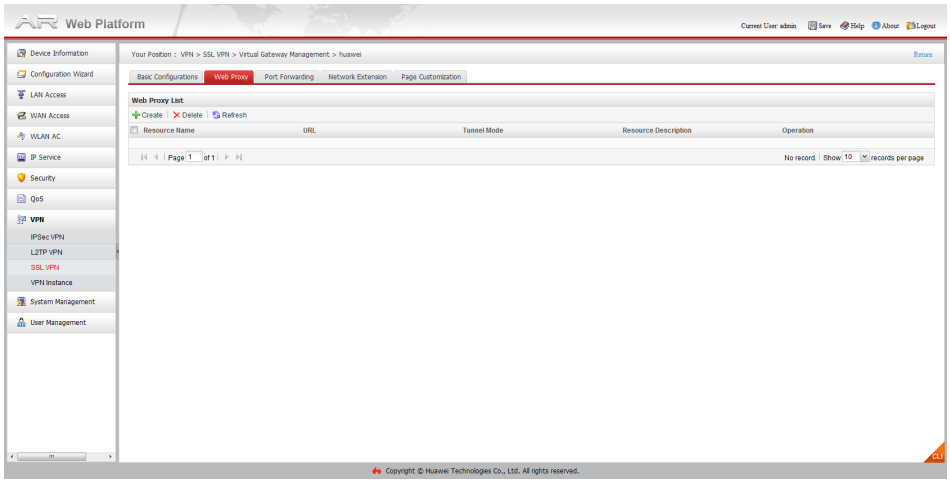
Context

When remote users want to access resources of the intranet server, the virtual gateway can provide web proxy services to forward data between remote users and the intranet server. This function ensures that access to the intranet server is secure.

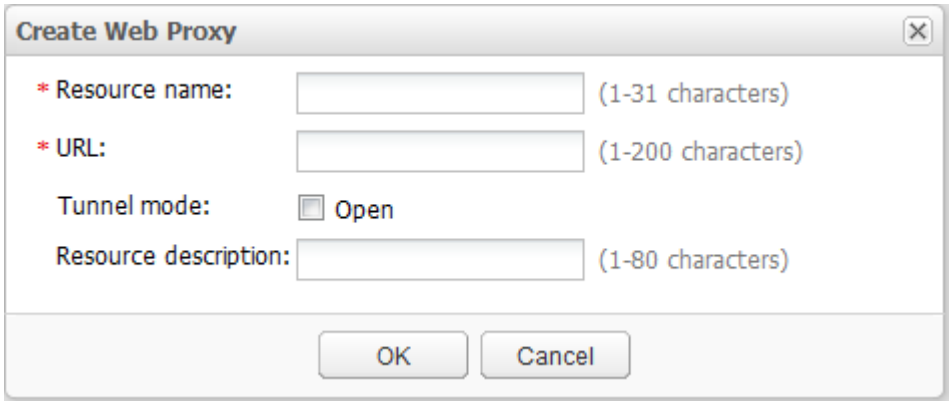
Procedure

- Creating a web proxy service
  a. Choose **VPN** > **SSL VPN**, and click **configurations** of a virtual gateway, and click the **Web Proxy** tab.

     Figure 2-230 Web Proxy Tab

  b. In the **Web Proxy List** area, click **Create**. The **Create Web Proxy** dialog box is displayed.

  c. In the **Create Web Proxy** dialog box, set parameters listed in **Table 2-170** based on the site requirements.
  d. Click **OK**.

     The created web proxy service is displayed in the **Web Proxy List** area. **Table 2-171** describes parameters in the web proxy list.

Copyright © Huawei Technologies Co., Ltd.

Table 2-170 Web proxy parameters

Parameter	Description
Resource name	Name of a web proxy service. To change the resource name, delete the web proxy service and create a web proxy service.
URL	URL of the intranet server that remote user access. The URL starts with **http://** or **https://**. You can enter an IP address or a domain name after **http://** or **https://**.
Tunnel mode	Whether to enable the tunnel mode. • Open: web proxy in tunnel mode. When a remote user logs in to a virtual gateway, the terminal of the remote user installs the Java plug-in. When the remote user clicks the link of the web proxy, the Java plug-in automatically adds the external header with the virtual gateway address as the destination address to the HTTP Request packet. After receiving the HTTP Request packet, the virtual gateway removes the external header and sends the packet to the intranet server. • Not open: web proxy in URL change mode. Java plug-in is not required. The virtual gateway changes the URL on each page of the intranet server that responds to remote users.
Resource description	Description of a web proxy service, which helps the administrator manage the virtual gateway.

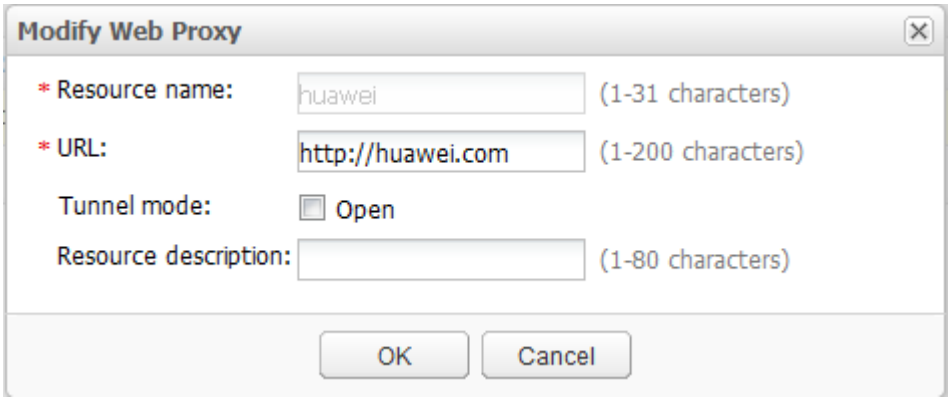
Table 2-171 Parameters on the web proxy list

Parameter	Description
Resource Name	Name of a web proxy service.
URL	URL in a web proxy service.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Tunnel Mode	Whether to enable the tunnel mode. • Yes: web proxy in tunnel mode. • No: web proxy in URL change mode.
Resource Description	Detailed description of a web proxy.

- Modifying a web proxy service
  a. Choose **VPN** > **SSL VPN** > **Virtual Gateway Management**.
  b. Click **configurations** of the virtual gateway. The configuration page is displayed.
  c. Click the **Web Proxy** tab.
  d. In the **Web Proxy List** area, and click  corresponding to a web proxy service. The **Modify Web Proxy** dialog box is displayed.



  e. Modify parameters based on the site requirements, and click **OK**.
- Deleting a web proxy service
  a. Choose **VPN** > **SSL VPN** > **Virtual Gateway Management**.
  b. Click **configurations** of the virtual gateway. The configuration page is displayed.
  c. Click the **Web Proxy** tab.
  d. In the **Web Proxy List** area, select a web proxy service, and click **Delete**.
  The deleted web proxy service is not displayed in the **Web Proxy List** area.

----End

2.17.3.5 Port Forwarding

Context

Remote users require TCP-based services on the intranet server, such as remote access, desktop sharing, and email. The virtual gateway can provide port forwarding services to ensure that access to the intranet server is secure.

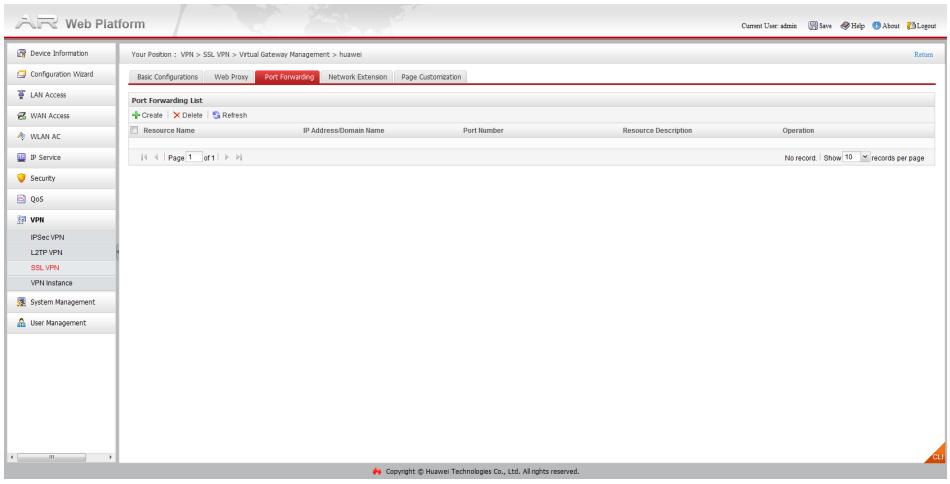
 Copyright © Huawei Technologies Co., Ltd.

The TCP-based port numbers on the remote terminal and application server must be the same; otherwise, the port forwarding service will fail.

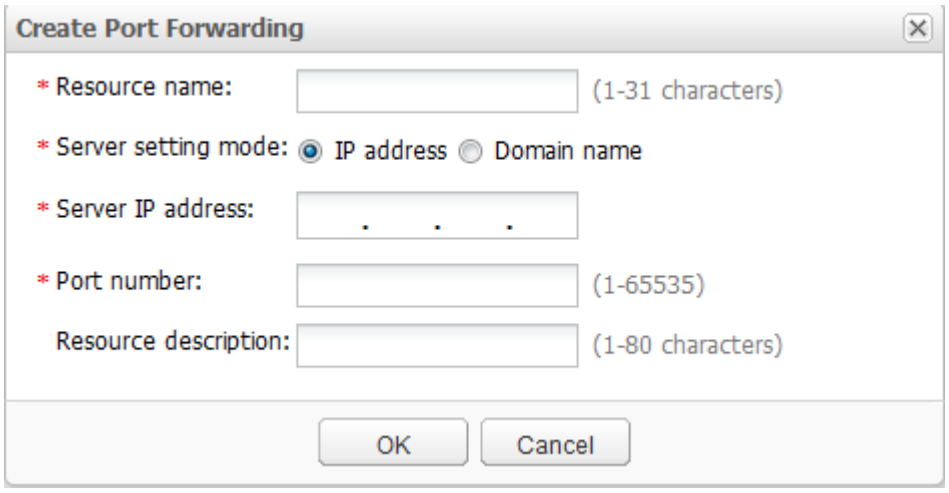
Procedure

- Creating a port forwarding service
  a. Choose **VPN** > **SSL VPN**, and click **configurations** of a virtual gateway, and click the **Port Forwarding** tab.

     Figure 2-231 Port Forwarding

  b. In the **Port Forwarding List** area, click **Create**.

  c. In the **Create Port Forwarding** dialog box, set parameters listed in **Table 2-172** based on the site requirements.

  d. Click **OK**.

     The created port forwarding service is displayed in the **Port Forwarding List** area. **Table 2-173** describes parameters in the port forwarding list.

Copyright © Huawei Technologies Co., Ltd.

Table 2-172 Port forwarding parameters

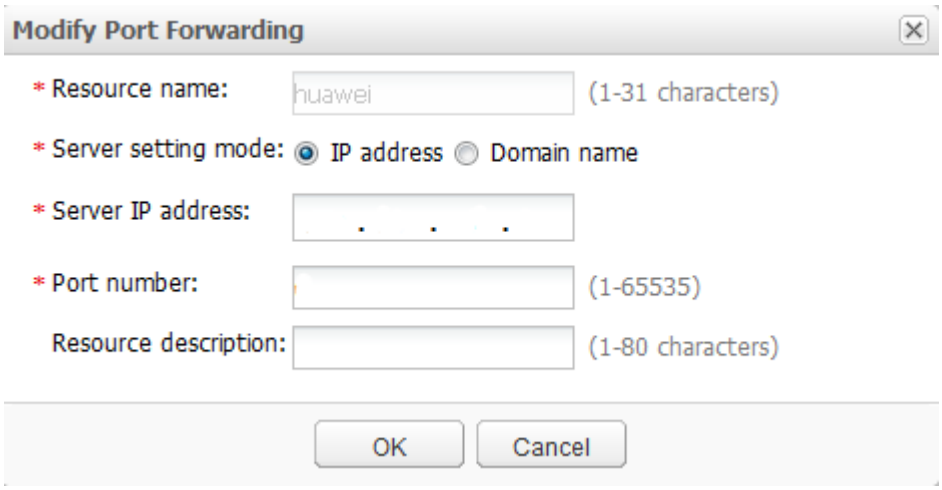
Parameter	Description
Resource name	Name of a port forwarding service. To change the resource name, delete the port forwarding service and create a port forwarding service.
Server setting mode	Intranet server address type. • IP address: the parameter **Server IP address** is enabled. You must set the IP address of the intranet server. • Domain name: the parameter **Server domain name** is enabled. You must set the domain name of the intranet server.
Server IP address	IP address of the intranet server.
Server domain name	Domain name of the intranet server.
Port number	TCP-based service port number.
Resource description	Description of a port forwarding service, which helps the administrator manage the virtual gateway.

Table 2-173 Parameters in the port forwarding list

Parameter	Description
Resource Name	Name of a port forwarding service.
IIP Address/Domain Name	IP address or domain name of the intranet server.
Port Number	TCP-based service port number.
Resource Description	Detailed description of a port forwarding service.

- Modifying a port forwarding service
  a. Choose **VPN** > **SSL VPN** > **Virtual Gateway Management**.
  b. Click **configurations** of the virtual gateway. The configuration page is displayed.
  c. Click the **Port Forwarding** tab.
  d. In the **Port Forwarding List** area, and click  corresponding to a port forwarding service. The **Modify Port Forwarding** dialog box is displayed.

Copyright © Huawei Technologies Co., Ltd.



e. Modify parameters based on the site requirements, and click **OK**.

- Deleting a port forwarding service
  a. Choose **VPN** > **SSL VPN** > **Virtual Gateway Management**.
  b. Click **configurations** of the virtual gateway. The configuration page is displayed.
  c. Click the **Port Forwarding** tab.
  d. In the **Port Forwarding List** area, select a port forwarding service, and click **Delete**.
     The deleted port forwarding service is not displayed in the **Port Forwarding List** area.

----End

2.17.3.6 Network Extension

Context

Remote users need to communicate with the intranet server in a secure mode. The virtual gateway can provide the network extension service to ensure communication security between remote users and the intranet server.

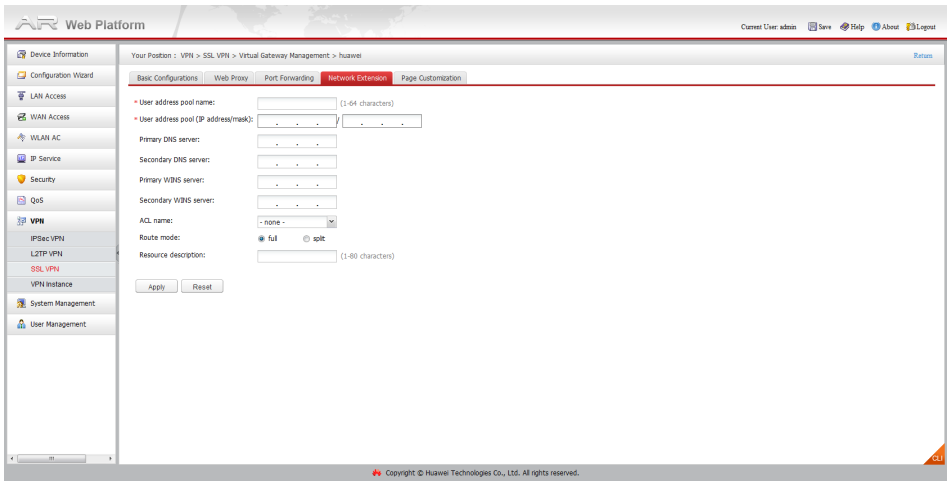
Before remote terminals access the intranet server through the network extension service, the dedicated client must be installed on remote terminals. You can download the client from the virtual gateway on web pages, and install a virtual network adapter on the remote terminal. The client sets up a secure sockets layer (SSL) connection between the remote terminal and the virtual gateway, requests an IP address for the virtual network adapter, and creates a route with the virtual network adapter as the outbound interface.

Procedure

- Configuring the network extension service
  a. Choose **VPN** > **SSL VPN** > **Virtual Gateway Management**.
  b. Click **configurations** of the virtual gateway. The configuration page is displayed.
  c. Click the **Network Extension** tab.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-232 Network Extension



d. Set parameters listed in **Table 2-174**.

e. Click **Apply**. A message is displayed indicating that the operation succeeds.

Table 2-174 Network extension parameters

Parameter	Description
User address pool name	Address pool name of remote users.
User address pool (IP address/mask)	Address pool used by remote users. When the network extension service is enabled for a remote user, an IP address is dynamically allocated to the virtual network adapter. The IP address is set to the gateway address of the remote virtual network adapter, and the subnet mask specifies the available address range.
Primary DNS server	Primary DNS server address that the virtual gateway allocates to remote users.
Secondary DNS server	Secondary DNS server address that the virtual gateway allocates to remote users.
Primary WINS server	Primary WINS server address that the virtual gateway allocates to remote users.
Secondary WINS server	Secondary WINS server address that the virtual gateway allocates to remote users.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
ACL name	ACL bound to a virtual gateway, which controls access permissions of remote users. For details on how to configure an ACL, see **ACL**.
Route mode	Route mode used by the network extension service. • full: A remote terminal can communicate with intranet servers in all IP address segments. • split: A remote terminal can communicate only with intranet servers in specified IP address segments. You can set **Accessible networks** to specified IP address segments.
Accessible networks	IP address segments that remote users can access in split route mode. The value is in the format of *IP address*/*subnet mask*. A maximum of 10 IP address segments can be set.
Resource description	Description of the network extension service, which helps the administrator maintain the virtual gateway.

- Deleting the network extension service
  a. Choose **VPN** > **SSL VPN** > **Virtual Gateway Management**.
  b. Click **configurations** of the virtual gateway. The configuration page is displayed.
  c. Click the **Network Extension** tab.
  d. Click **Reset**, and click **OK** in the dialog box that is displayed.
     All parameters of the network extension service are cleared.

----End

2.17.3.7 Page Customization

Context

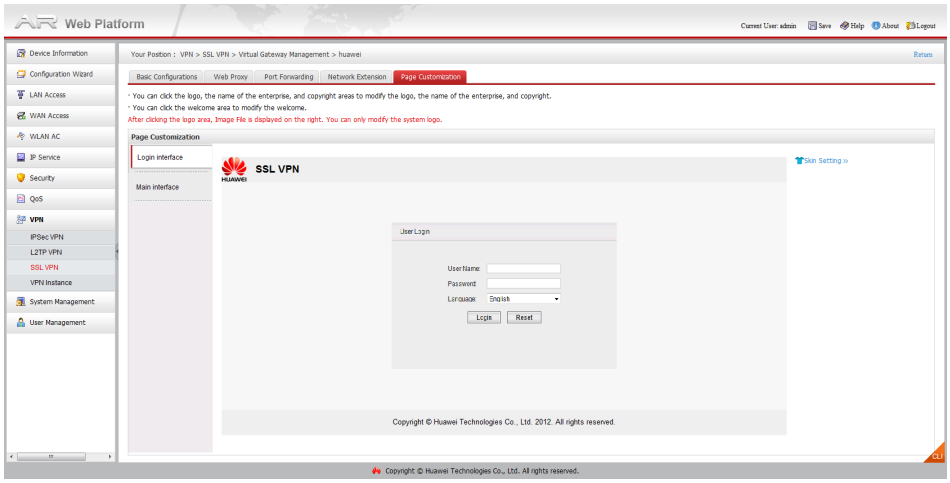
After completing service configurations of the virtual gateway, a remote user needs to log in to the virtual gateway on web pages to access internal enterprise resources. An enterprise user can customize web pages of the virtual gateway.

Copyright © Huawei Technologies Co., Ltd.

Procedure

- Customizing the login page
  a. Choose **VPN** > **SSL VPN** > **Virtual Gateway Management**.
  b. Click **configurations** of the virtual gateway. The configuration page is displayed.
  c. Click the **Page Customization** tab, and click **Login interface**.

  Figure 2-233 Login interface



  d. Click specified areas to customize elements displayed on the simulated login page. Table 2-175 describes parameters on the login page.

Table 2-175 Page customization parameters

Parameter	Description
Skin Setting	Background color of the login page and main page. • Grey: gray • Yellowish brown: gold • Light blue: blue After you select a skin color, the configuration result is displayed on the simulated login page. Click **Apply** to make the settings take effect. By default, pages of a virtual gateway use the gray skin.

Copyright © Huawei Technologies Co., Ltd.

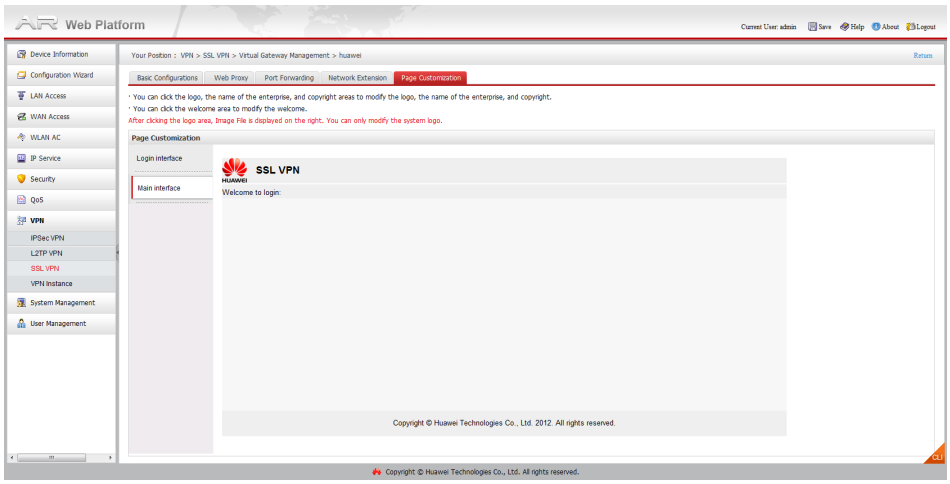
Parameter	Description
LOGO	Enterprise logo that locates in the upper left corner of the login page. By default, the logo is Huawei's logo. Click the logo icon, and select a GIF file from the drop-down list box that is displayed on the right. You can select a logo in the following ways: ● Upload Image: When you select **Upload Image**, the **Upload Image** dialog box is displayed. Click **Browser** to select a GIF file, and click **Upload**. ● Default LOGO: When you select **Default LOGO**, Huawei's logo is used. The size of a GIF file cannot exceed 6K bytes. After a GIF is uploaded, click **Apply** to make the setting take effect. **NOTE** A logo is not displayed in the simulated login page after being uploaded. You can view the uploaded logo when you log in to the virtual gateway.
Title of the page	Page title next to the logo. Generally, the page tile is the enterprise name. You can click this area to edit the page title, and click any place out of this area to make the setting take effect.
Help information at the bottom	Help information at the bottom of the login page. Generally, help information includes the copyright, enterprise address, and contact information. You can click this area to edit help information, and click any place out of this area to make the setting take effect.

- Customizing the main page
  a. Choose **VPN** > **SSL VPN** > **Virtual Gateway Management**.
  b. Click **configurations** of the virtual gateway. The configuration page is displayed.

 Copyright © Huawei Technologies Co., Ltd.

c. Click the **Page Customization** tab, and click **Main interface**.

Figure 2-234 Main interface



d. Click the area under the logo to set the welcome words.

After completing the configuration, click **Apply**. The message "Operation succeeded." is displayed. You can view the new welcome words on the simulated login page.

----End

2.17.4 VPN Instance

Context

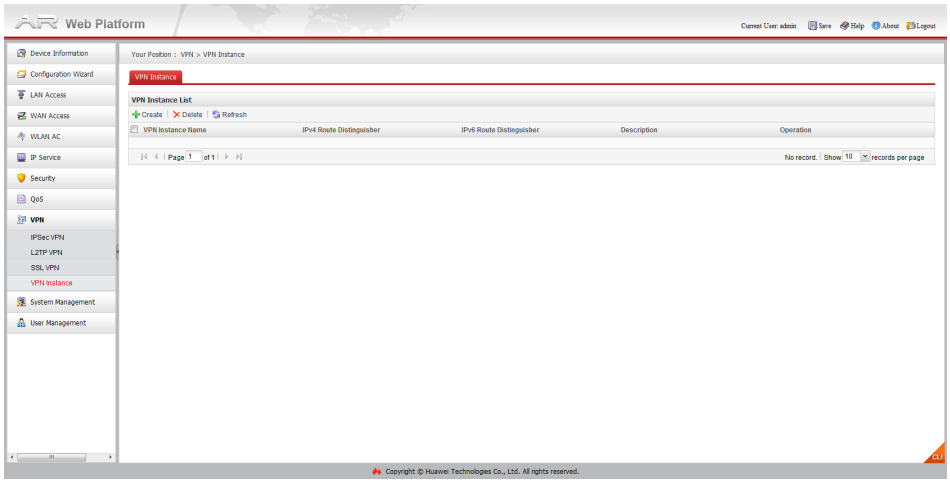
Each VPN instance maintains forwarding information about a local VPN. When router interfaces connect to VPNs having the same IP address, you can bind the interfaces to different VPN instances. In this way, each VPN instance has its own routing table and forwards packets independently.

Procedure

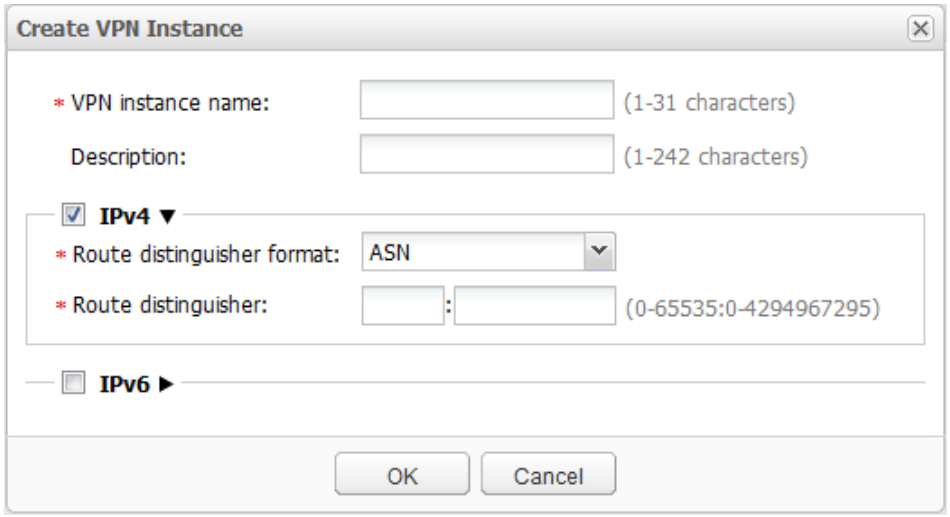
- Creating a VPN instance
  a. Choose **VPN** > **VPN Instance**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-235 VPN Instance



b. Click **Create** in the **VPN Instance List** area.



c. Set parameters in the **Create VPN Instance** dialog box. **Table 2-176** describes the parameters.

d. Click **OK**.

The created VPN instance is displayed in the VPN instance list.

Table 2-176 VPN instance parameters

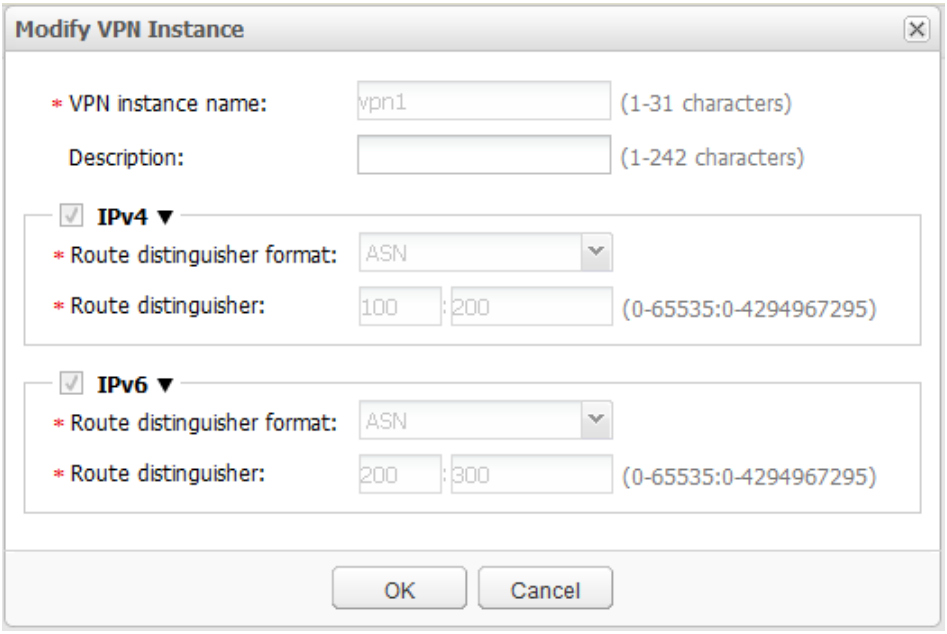
Parameter	Description
VPN instance name	Name of a VPN instance. The value is a string of case-sensitive characters without question marks (?).
Description	Description of the VPN instance, which helps network administrators to manage device configuration.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
IPv4	The IPv4 address family of the VPN instance is enabled. Select this parameter when you configure an IPv4 VPN instance. After you select this parameter, set **Route distinguisher format** and **Route distinguisher**.
IPv6	The IPv6 address family of the VPN instance is enabled. Select this parameter when you configure an IPv6 VPN instance. After you select this parameter, set **Route distinguisher format** and **Route distinguisher**.
Route distinguisher format	Route distinguisher (RD) format of a VPN instance. The value cannot be changed after being set. The value can be: • ASN: autonomous system number • IP
Route distinguisher	Route distinguisher (RD) of the VPN instance. • When the RD is of ASN type, the value is in the format of 16-bit AS number: 32-bit user-defined number. For example: 101:3. The AS number and user-defined number cannot be 0 simultaneously. That is, the RD cannot be 0:0. • When the RD is of IP type, the value is in the format of 32-bit IP address: 16-bit user-defined number. For example, 192.168.122.15:1.

- Modifying a VPN instance
  You can modify only the description of a VPN instance.
  a. Choose **VPN** > **VPN Instance**.
  b. Click of a VPN instance.

Copyright © Huawei Technologies Co., Ltd.



c. Set **Description**.
d. Click **OK**.
The description of the VPN instance is modified.

- Deleting a VPN instance
  a. Choose **VPN** > **VPN Instance**.
  b. Select a VPN instance to delete.
  c. Click **Delete**.
  d. In the dialog box that is displayed, click **OK**.
  The VPN instance is deleted from the VPN instance list.

----End

2.18 Voice Management

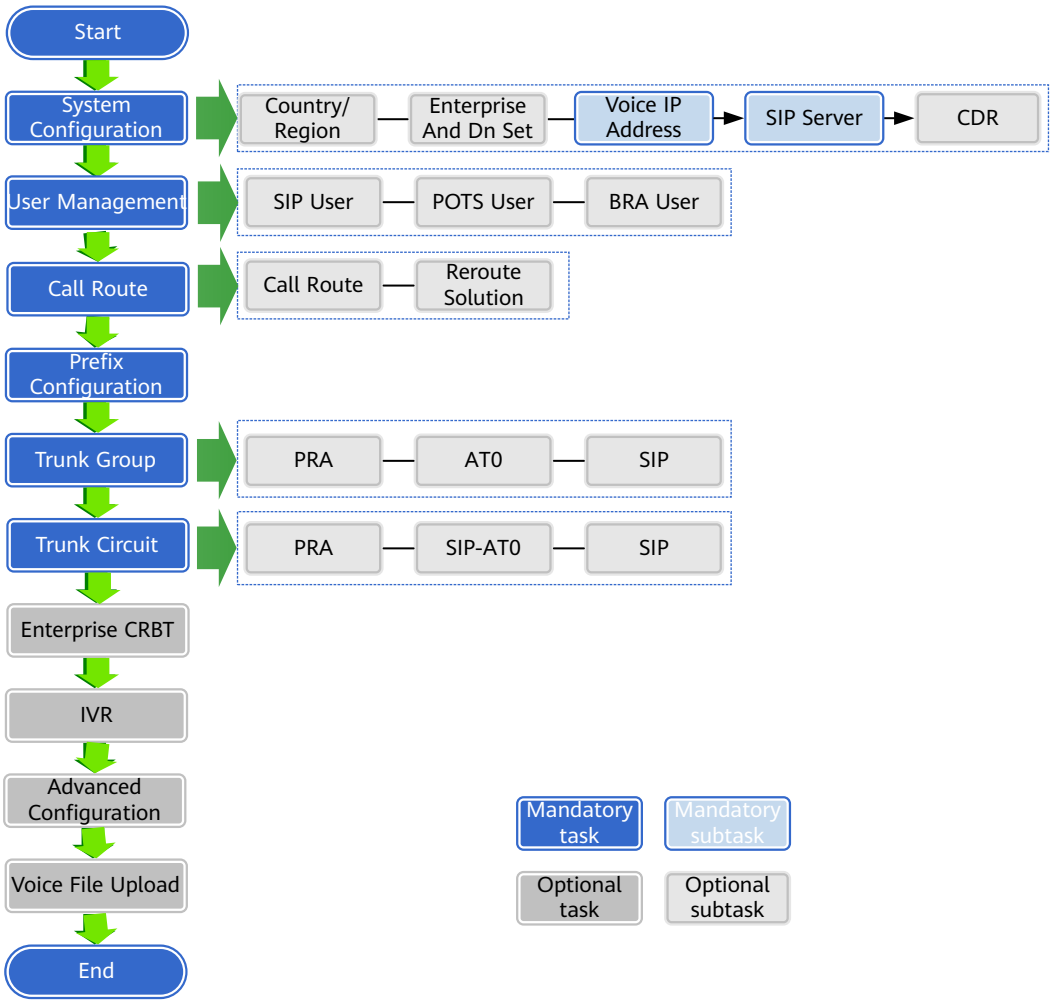
2.18.1 Configuration Process

This section describes the process for configuring voice service data on the PBX. In the configuration process, optional tasks and subtasks are performed according to your site requirements.

Figure 2-236illustrates the PBX configuration process.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-236 PBX configuration process



2.18.2 Wizard-based Quick Configuration

Context

NOTICE

The configuration in each step of the configuration wizard takes effect in real time.

Only one user can log in to a web browser at the same time. If you want to log in as another user, log out the current user first.

Usage Scenario

This configuration wizard applies to configuring the voice service for the first time or adding an intra-office or outgoing call (which is, adding call prefixes, users,

 Copyright © Huawei Technologies Co., Ltd.

trunk groups, trunk circuits, and call routes under the default enterprise and dial plan).

NOTE

For voice service configuration using the configuration wizard, the enterprise and dial plan to use are the default enterprise (**default**) and default dial plan (**DefaultDialPlan**).

Pre-configuration Task

Before using the configuration wizard, choose **Voice Management** > **System Configuration** > **Voice IP Management** to create a signaling IP address and a media IP address for the voice service.

Wizard Function

The configuration wizard allows users to quickly complete the intra-office or outgoing call configuration task.

NOTE

In the actual application, if the wizard-based configuration fails to meet the requirements, users can access the configuration pages of the corresponding functions from the navigation bar for optimization.

Configuration Example

An enterprise has two POTS users (user A and user B) and a SIPUE user (user C). The following data is used as an example:

- Country/Region information: The value of **Country/Region** is 990.
- Enterprise information: **Enterprise name** is **HUAWEI** and the dial plan is **123**.
- Voice IP information: **Interface description** is **HUAWEI, AR Series, GigabitEthernet0/0/0 Interface** and **IP address** is **10.166.70.213**.
- SIP server: URI and domain name being **abcd.com**
- User information: POTS user 7000, SIP user 7100, and BRA user 7200
- Route information: route 1 (reroute of route 2)
- Prefix information: local prefix 7
- Trunk group information: PRA trunk group **trunkgroup1**
- Trunk circuit information: The PRA trunk name is 12 and the E1 port is port 1; the SIP-AT0 trunk name is 44, the called number is 28980808, and the register ID is 7000; the AT0 trunk name is 33 and the called number for the incoming call is 28980808.

Procedure

Step 1 Configure the country code and region code.

1. Click **Start Config** to access the country/region configuration page.
2. Click **Create**.

NOTE

Before your creation, check whether the configuration you require already exists in the country/region list. The system provides some country/region information by default.

 Copyright © Huawei Technologies Co., Ltd.

3. Configure the country/region information.
4. Click **OK**.

Step 2 Configure the enterprise information.

1. On the country/region configuration page, click **next** to access the enterprise management page.
2. Click **Create**.
3. In the **Create Enterprise** dialog box, configure related information.
4. Click **OK**.
5. Click **Dial Plan** for **HUAWEI**.
   The **Dial Plan List** dialog box is displayed.
6. Click **Create**.
7. In the **Create Dial Plan** dialog box, configure related information.
8. Click **OK**.

Step 3 Configure the voice IP information.

1. On the enterprise management page, click **Next** to access the voice IP management page.
2. Click **Create**.
3. In the **Create Voice IP** dialog box, configure related information.
4. Click **OK**.

Step 4 On the voice IP management page, click **Next** to access the SIP server configuration page.

1. Configure related information.

   NOTE

   After the SIP server is configured, the system automatically restarts for the data to take effect. After the system restart, the system automatically displays the **User Management** page.

Step 5 Configure users.

- Configure a SIP user.
  a. Click **Create**.
  b. In the **Create SIP User** dialog box, configure related information.
  c. Click **OK**.
- Configure a POTS user.
  a. Click the **POTS User** tab.
  b. Click **Create**.
  c. In the **Create POTS User** dialog box, configure related information.
  d. Click **OK**.
- Configure a BRA user.
  a. Click the **BRA User** tab.
  b. Click **Create**.
  c. In the **Create BRA User** dialog box, configure related information.

 Copyright © Huawei Technologies Co., Ltd.

d. Click **OK**.

Step 6 Configure a call route.

- Configure a call route.
  a. On the **User Management** page, click **Next**.
  b. Click **Create**.
  c. In the **Create Call Route** dialog box, configure related information.
  d. Click **OK**.
- Configure a reroute scheme.
  a. Click the **Reroute** tab.
  b. Click **Create**.
  c. In the dialog box that is displayed, configure related information.
  d. Click **OK**.

Step 7 Configure a prefix.

1. On the **Call Route** page, click **Next**.
2. Click **Create**.
3. In the **Create Call Prefix** dialog box, configure related information.
4. Click **OK**.
5. Click **Call Route** next to the call prefix.
6. In the **Configure Call Route** dialog box that is displayed, click **Create**.
7. In the **Create Call Route** dialog box, set parameters.
8. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.

Step 8 Configure a trunk group.

1. On the **Prefix Configuration** page, click **Next**.
2. Click **Create**.
3. In the **Create Trunk Group** dialog box, configure related information.
4. Click **OK**.

Step 9 Configure trunk circuits.

- Configure a PRA trunk.
  a. Click **Create**.
  b. In the **Create PRA Trunk** dialog box, configure related information.
  c. Click **OK**.
- Configure a SIP-AT0 trunk.
  a. Click the **SIP-AT0 Trunk** tab and click **Create**.
  b. In the **Create SIP-AT0 Trunk** dialog box, configure related information.
  c. Click **OK**.
- Configure an AT0 trunk.
  a. Click the **AT0 Trunk** tab and click **Create**.
  b. In the **Create AT0 Trunk** dialog box, configure related information.

 Copyright © Huawei Technologies Co., Ltd.

c. Click **OK**.

----End

2.18.3 System Configuration

After you configure system information on the PBX, it obtains basic data and is ready for subsequent number, networking, and service configurations.

2.18.3.1 Country/Region

After configuring the country code and region code, you can normalize called numbers for calls from different regions or countries.

Context

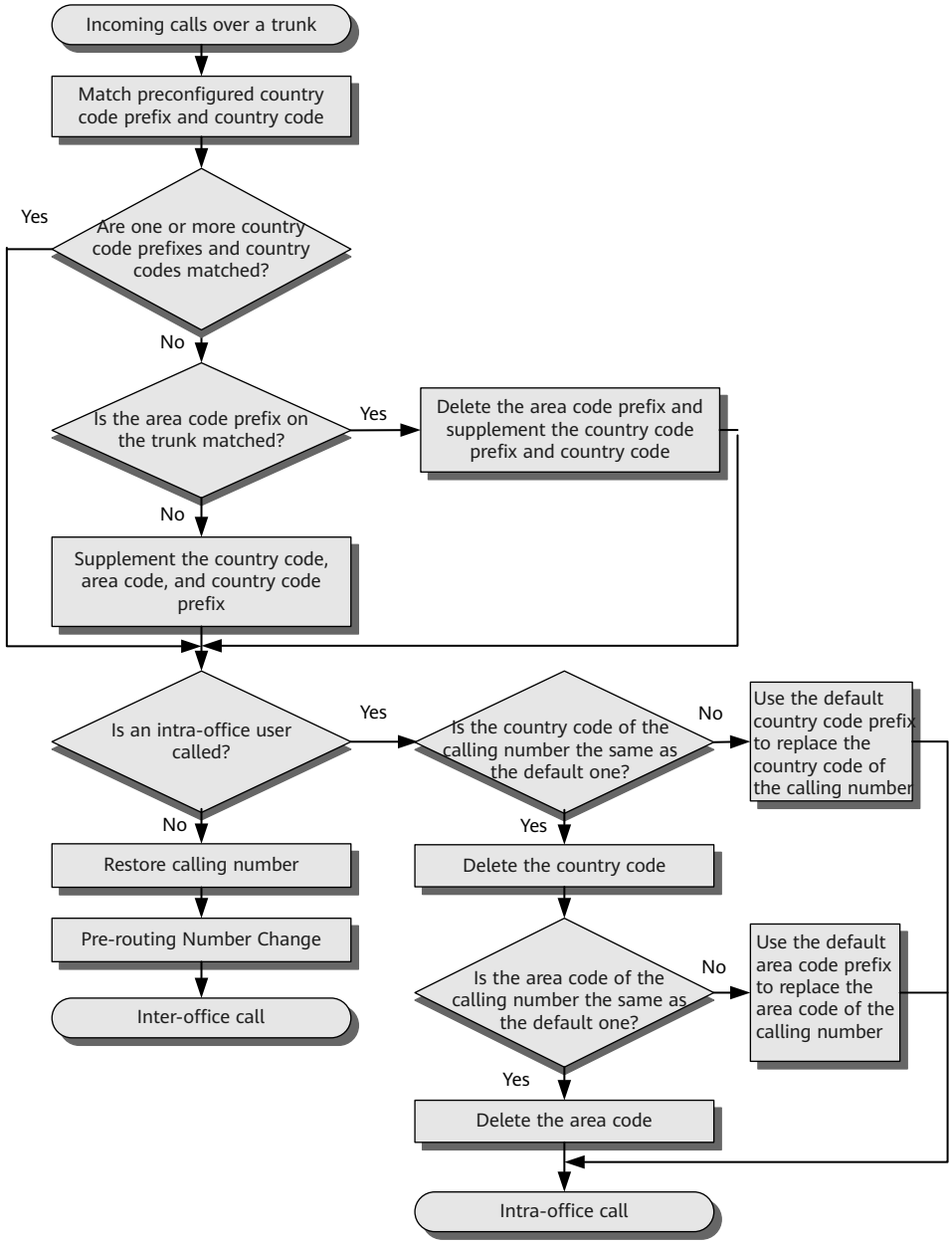
The PBX adds digits to calling numbers to display incoming numbers, meeting user needs. It regulates called numbers to accurately locate called parties.

NOTE

- Digits are collected at one time. The PBX cannot collect digits one by one.
- The PBX does not support number regulation over an R2 trunk.

- **Figure 2-237** shows the calling number regulation process for incoming calls over a trunk.

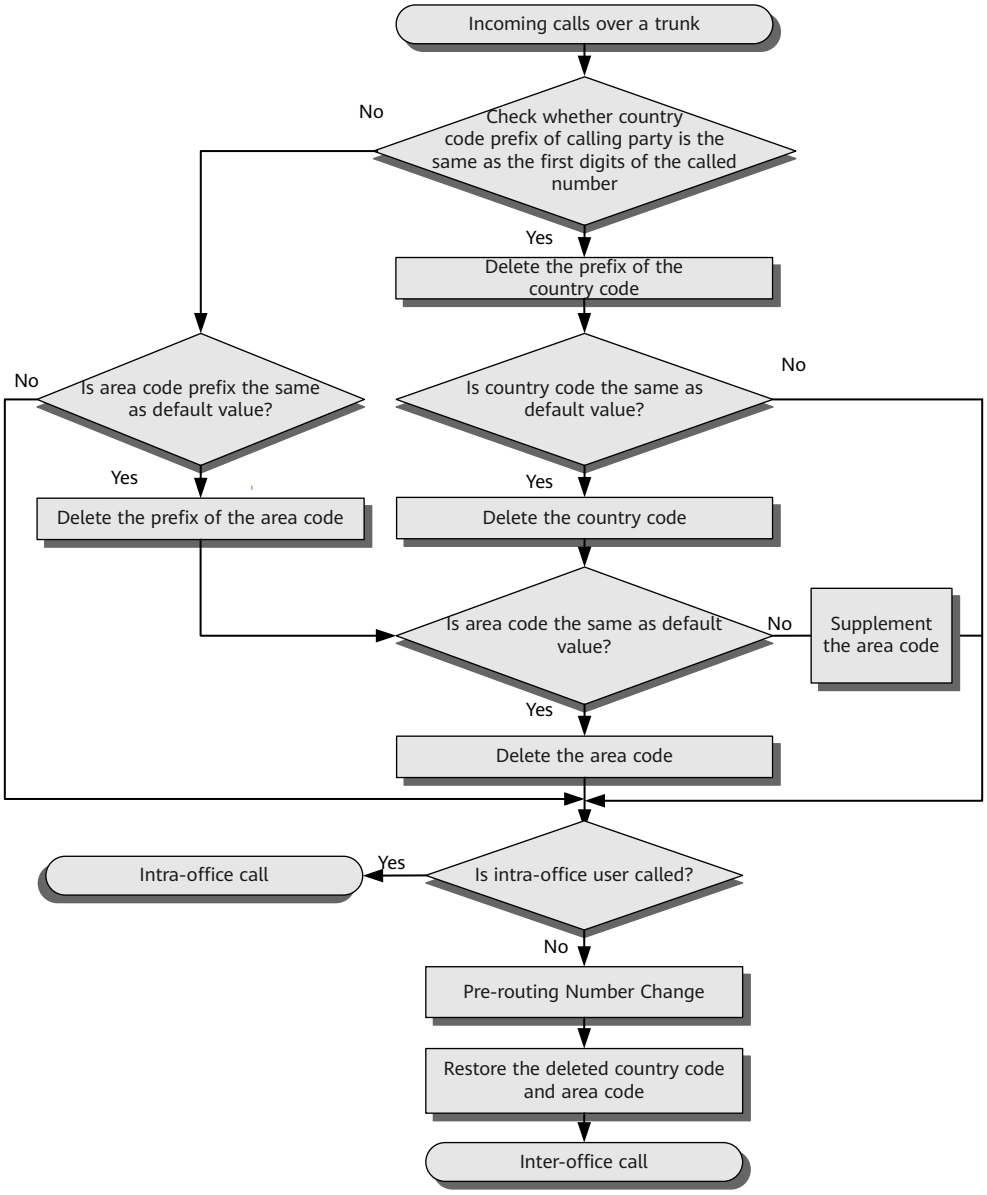
Figure 2-237 Calling number regulation process



- **Figure 2-238** shows the called number regulation process for incoming calls over a trunk.

 Copyright © Huawei Technologies Co., Ltd.

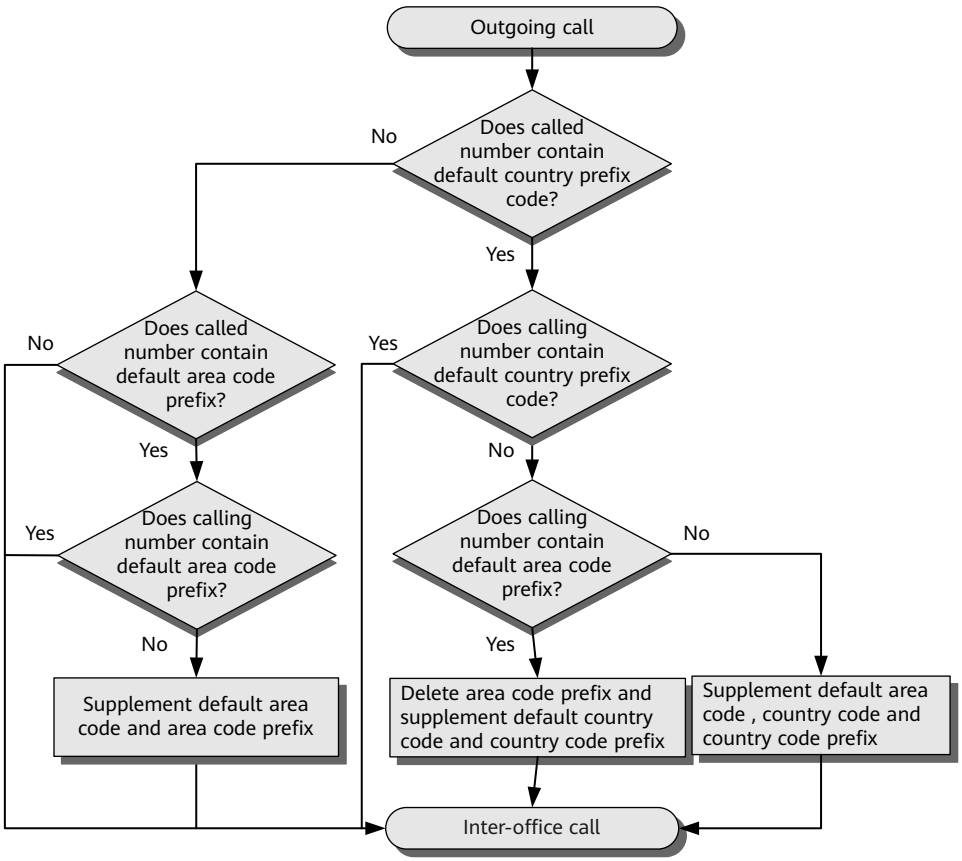
Figure 2-238 Called number regulation process



- **Figure 2-239** shows the intra-office call number regulation process.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-239 Intra-office call number regulation process



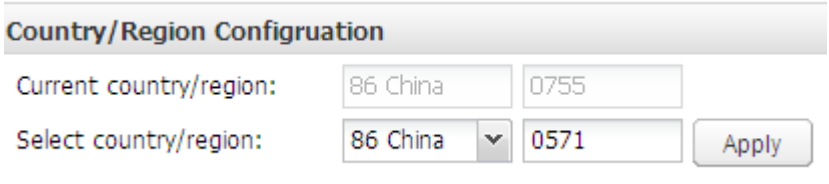
Accessing a Page

Choose **Voice Management** > **System Configuration** > **Country/Region**.

Procedure

- Configure the current country/region code.
  a. In **Country/Region Configuration**, set **Select Country/Region**.
  b. Click **Apply**.
  Figure 2-240 shows the **Country/Region Configuration** area.

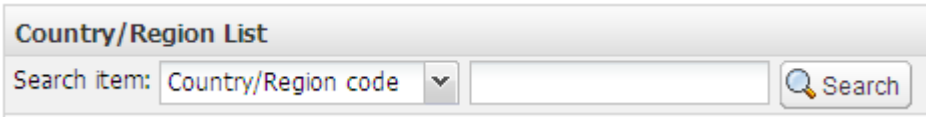
  Figure 2-240 Configuring the current country/region code



 Copyright © Huawei Technologies Co., Ltd.

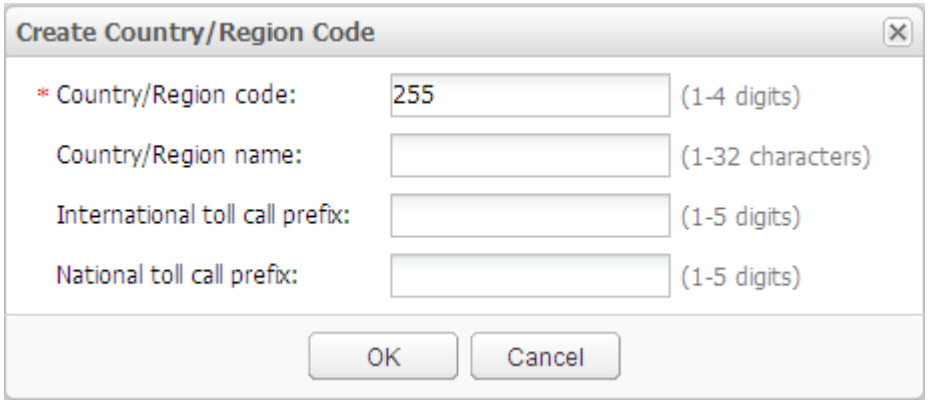
- Search for a country/region code.
  a. In the **Country/Region List** area, select a search item from the **Search item** drop-down list box, and enter the search content.
  b. Click **Search**.
  Figure 2-241 shows the **Country/Region List** area.

  Figure 2-241 Searching for a country/region code



- Create a country/region code.
  a. Click **Create**.
  b. Set parameters in the **Create Country/Region Code** dialog box.
  Figure 2-242 shows the **Create Country/Region Code** dialog box.

  Figure 2-242 Creating a country/region code



  c. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.
- Modify a country/region code.
  a. Click  next to the country/region code.
  b. Set parameters in the **Modify Country/Region Code** dialog box.
  c. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.
- Delete a country/region code.
  a. Select the country/region code to be deleted, and click **Delete**.
  b. In the **Information** dialog box, click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.

----End

 Copyright © Huawei Technologies Co., Ltd.

Parameter Description

Parameter	Description
Country/Region code	Code of the country or region, for example, 86.
Country/Region name	Name of the country or region.
International toll call prefix	International toll call prefix of the country or region.
National toll call prefix	National toll call prefix of the country or region.

2.18.3.2 Enterprise and DN Set

After multiple enterprises are configured on the device in PBX mode, they share the PBX. A DN set consists of an enterprise's number rules. When one enterprise shares a PBX, you do not need to configure enterprises. When one DN set meets enterprise requirements, you do not need to configure DN sets.

Context

When multiple enterprises need to share one PBX, you can configure enterprises on the PBX and virtualizes the PBX into multiple PBXs. Configuring enterprises on the PBX facilitates management on different enterprise users. Each terminal user is included in an enterprise, and enterprises are independent and make inter-office calls.

NOTE

By default, the enterprise **default** exists on the PBX.

You can create DN sets for enterprises and bind DN sets to users and call prefixes when you configure **User Management** and **Prefix Configuration**. After DN sets are bound to users and call prefixes, define number rules in the DN sets. For example, if a user must dial 9 for a local call and 90 for a long-distance call, 9 and 90 can be contained in a DN set. You can define multiple DN sets for an enterprise based on number rules.

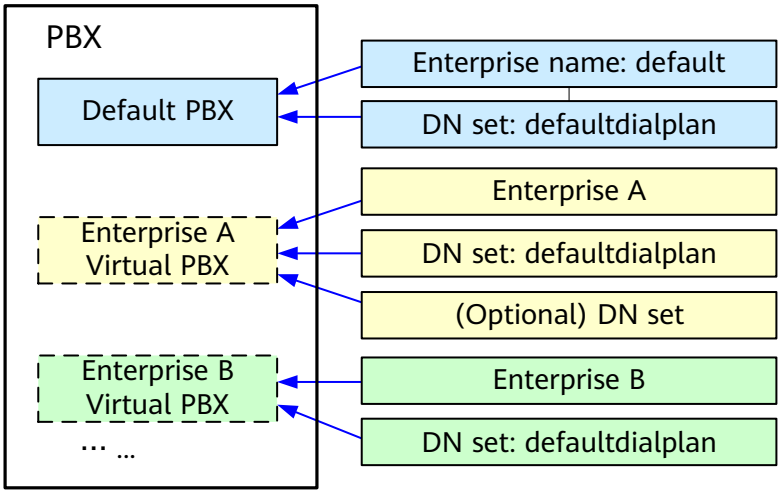
NOTE

By default, the PBX provides the DN set **defaultdialplan** for the enterprise **default** and new enterprises.

Figure 2-243 shows the mapping between the PBX, enterprise, and DN set.

Copyright © Huawei Technologies Co., Ltd.

Figure 2-243 Mapping between the PBX, enterprise, and DN set



Assessing a Page

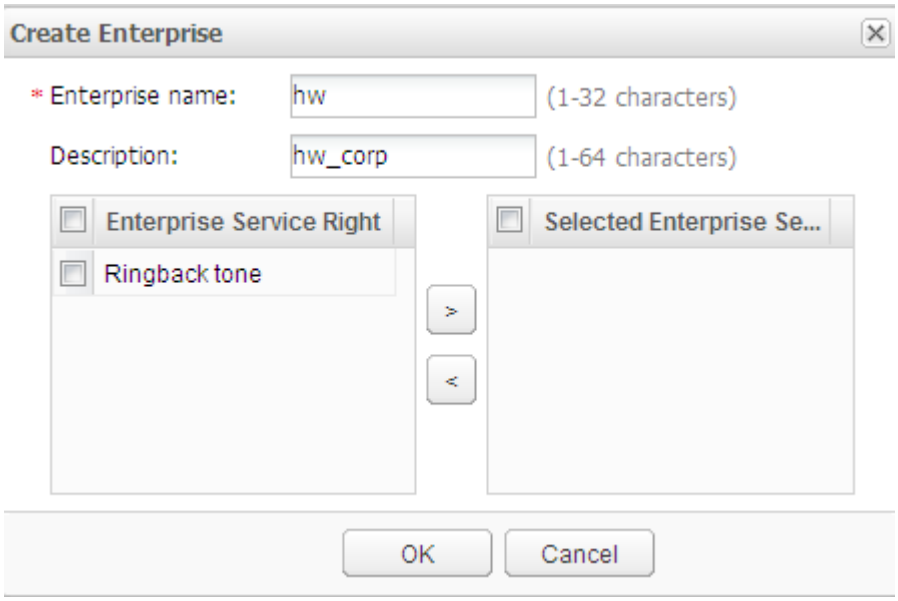
Choose **Voice Management** > **System Configuration** > **Enterprise And Dn Set**.

Procedure

- Create an enterprise.
  a. Click **Create**.
  b. Set parameters in the **Create Enterprise** dialog box.
  Figure 2-244 shows the **Create Enterprise** dialog box.

 Copyright © Huawei Technologies Co., Ltd.

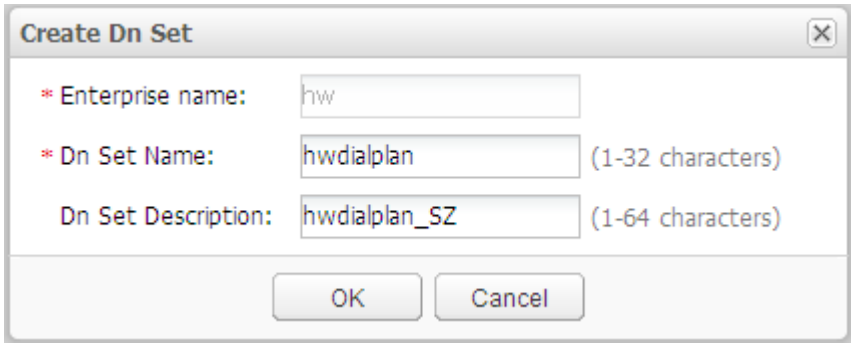
Figure 2-244 Create Enterprise dialog box



c. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.

- Modify an enterprise.
  a. Click  next to the enterprise.
  b. Set parameters in the **Modify Enterprise** dialog box.
  c. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.
- Delete an enterprise.
  a. Select the enterprise you want to delete and click **Delete**.
  b. In the **Information** dialog box, click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.
- Create a DN set.
  a. Click **Dn Set** next to the enterprise.
  b. Click **Create** in the **Dn Set List** dialog box.
  c. Set parameters in the **Create Dn Set** dialog box.
  Figure 2-245 shows the **Create Dn Set** dialog box.

Figure 2-245 Create Dn Set dialog box



Copyright © Huawei Technologies Co., Ltd.

d. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.

- Modify a DN set.
  a. Click **Dn Set** next to the enterprise.
  b. Click  next to the DN set.
  c. Set parameters in the **Modify Dn Set** dialog box.
  d. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.
- Delete a DN set.
  a. Click **Dn Set** next to the enterprise.
  b. Select the DN set you want to delete and click **Delete**.
  c. In the **Information** dialog box, click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.

----End

Parameter Description

Parameter	Description
Enterprise name	-
Description	Enterprise description, helping differentiate enterprises.
Enterprise Service Right	Select a check box, and click  or to set the service rights, such as ringback tone (RBT) for users.
Dn Set Name	-
Dn Set Description	DN set description, helping differentiate DN sets.

NOTE

When you set **Description**, **Dn Set Name** and **Dn Set Description**, enter character strings with spaces included in double quotation marks (""), for example, "this is an example".

2.18.3.3 Voice IP Address

This section describes how to configure voice IP addresses, media IP addresses, and signaling IP addresses for interfaces on the PBX, so that the PBX can connect to the IP network.

Copyright © Huawei Technologies Co., Ltd.

Context

The voice IP address pool stores signaling IP addresses of PBX interfaces and IP addresses of media streams controlled by signaling protocols. The media and signaling IP address addresses can be the same.

Media and signaling IP addresses must be available and routes are reachable.

Prerequisites

Ethernet interfaces have been configured for WAN interconnection.

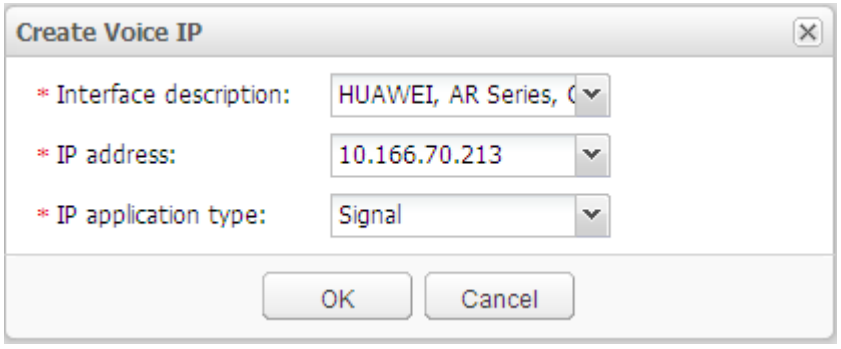
Assessing a Page

Choose **Voice Management** > **System Configuration** > **Voice IP Address**.

Procedure

- Create a voice IP address.
  a. Click **Create**.
  b. Set parameters in the **Create Voice IP** dialog box.
  Figure 2-246 shows the **Create Voice IP** dialog box.

  Figure 2-246 Create Voice IP dialog box

  c. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.
- Delete a voice IP address.
  a. Select the IP address you want to delete and click **Delete**.
  b. In the **Information** dialog box, click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.

----End

Parameter Description

Parameter	Description
Interface description	Interface on which a media or signaling IP address needs to be configured.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
IP address	Used IP addresses. Set a media IP address or a signaling IP address based on the setting of **Interface description**.
IP application type	Application type of the voice IP address. The value can be **Signal** or **Media**.

2.18.3.4 SIP Server

This section describes how to configure parameters of a SIP server, including the IP address, URI, and home domain. SIP server is an important entity in the SIP protocol architecture. The PBX can function as the SIP server to accept registration information of SIP users, save the information in the address information database, and manage and maintain users' registration information.

Assessing a Page

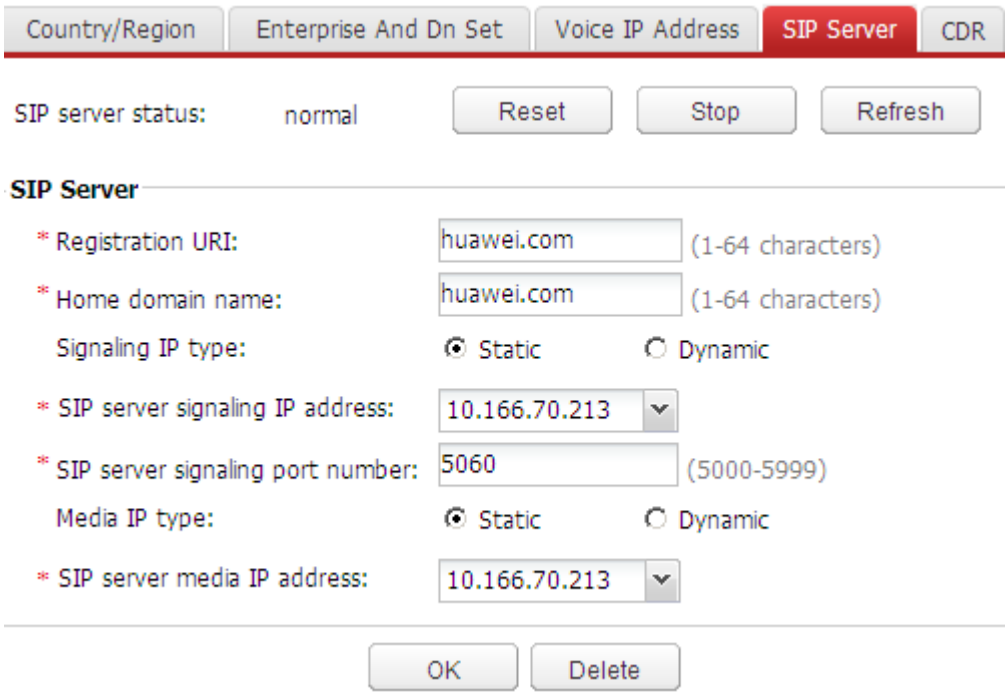
Choose **Voice Management** > **System Configuration** > **SIP Server**.

Procedure

Step 1 Set parameters in the **SIP Server** area.

Figure 2-247 shows the **SIP Server** area.

Figure 2-247 SIP Server area



 Copyright © Huawei Technologies Co., Ltd.

Step 2 Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.

Step 3 The system resets the SIP server. After a few seconds, a dialog box is displayed, indicating that the operation succeeds. Click **OK**.

----End

Parameter Description

Parameter	Description
Registration URI	Uniform resource identifier of the SIP server for SIP user registration.
Home domain name	Name of the home domain to which the SIP server belongs. The value of this parameter is used as the user domain name in the **From** field carried in the SIP message header.
Signaling IP type	Signaling IP type of the SIP server. • Static: The static IP address is used as the signaling IP address. • Dynamic: The dynamically allocated IP address is used as the signaling IP address. For example, the IP address can be dynamically allocated through PPPoE or by the DHCP server.
Signaling domain name	Signaling domain name for the SIP server using a dynamic signaling IP address.
DDNS client name	Dynamic domain name system (DDNS) name for the SIP server using a dynamic signaling IP address. This parameter is used to update the mapping between the signaling domain name and IP address.
Dynamic signaling address name	Interface name of the signaling IP address for the SIP server using a dynamic signaling IP address. The interface must be configured with dynamic IP address allocation and added to the dynamic signaling IP address pool.
SIP server signaling IP address	Specify an IP address in the signaling address pool as the signaling IP address of the SIP server.
SIP server signaling port number	Signaling port number of the SIP server.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Media IP type	Media IP type of the SIP server. • Static: The static IP address is used as the media IP address. • Dynamic: The dynamically allocated IP address is used as the media IP address. For example, the IP address can be dynamically allocated through PPPoE or by the DHCP server.
SIP server media IP address	Specify an IP address in the media address pool as the media IP address of the SIP server.
Dynamic media address name	Interface name of the media IP address for the SIP server using a dynamic media IP address. The interface must be configured with dynamic IP address allocation and added to the dynamic media IP address pool.
SIP server status	Status of the SIP server. Click **Reset** or **Stop** to manage the SIP server status.

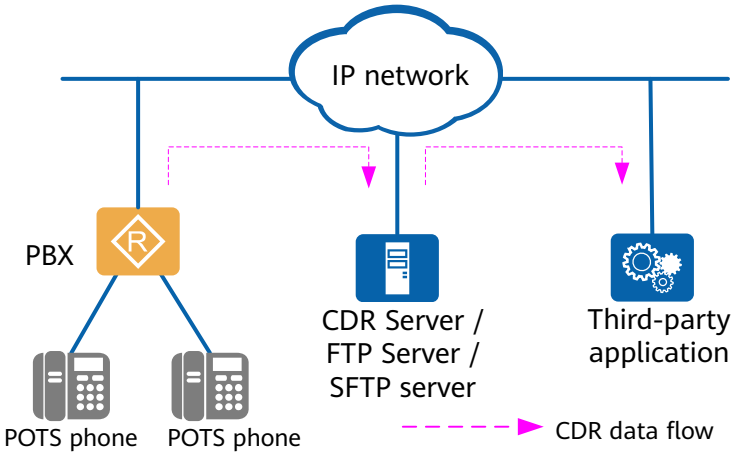
2.18.3.5 CDR

You can configure the call detail record (CDR). The device sends generated CDRs to the CDR server.

Context

CDRs generated for voice services are directly saved in the built-in CDR pool on the PBX. CDRs in the CDR pool can be saved on the CDR server in binary format or be saved on the FTP/SFTP server in binary or text format through the CDR interface. **Figure 2-248** shows the networking.

Figure 2-248 Connecting to the CDR/FTP/SFTP server



Copyright © Huawei Technologies Co., Ltd.

NOTICE

The PBX and CDR server must be deployed on a trusted network. Otherwise, there will be security risks.

The PBX can be connected to the CDR/FTP/SFTP server using the following two protocols:

- TCP: Using this protocol, the PBX directly sends CDRs to the CDR server. The CDR format is **UCBILL**.
- FTP/SFTP: Using this protocol, the PBX sends CDRs to the FTP/SFTP server, providing CDR information for the third-party billing system and billing center. The CDR formats are **CDR** (used in the CC08 environment), **SOFTX** (used in the SOFTX3000 environment), and **MINI** (used when only CDRs need to be checked and charging is ignored).

  NOTE

  UCBILL, **CDR**, and **SOFTX** CDRs are in binary format. **MINI** CDRs are in text format.

Accessing a Page

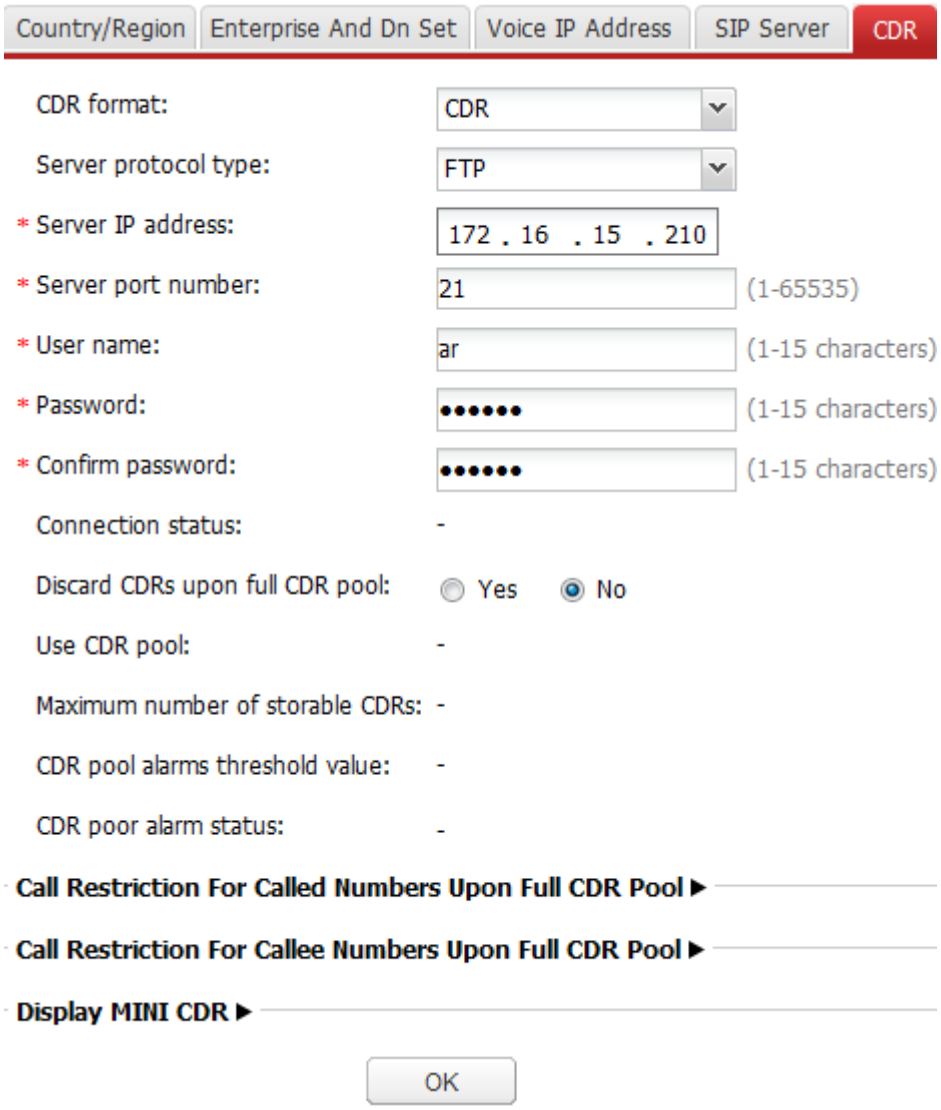
Choose **Voice Management** > **System Configuration** > **CDR**.

Procedure

- Provide CDRs through FTP/SFTP.
  a. Set parameters on the **CDR** page.
  Figure 2-249 shows the **CDR** page.

Copyright © Huawei Technologies Co., Ltd.

Figure 2-249 CDR page

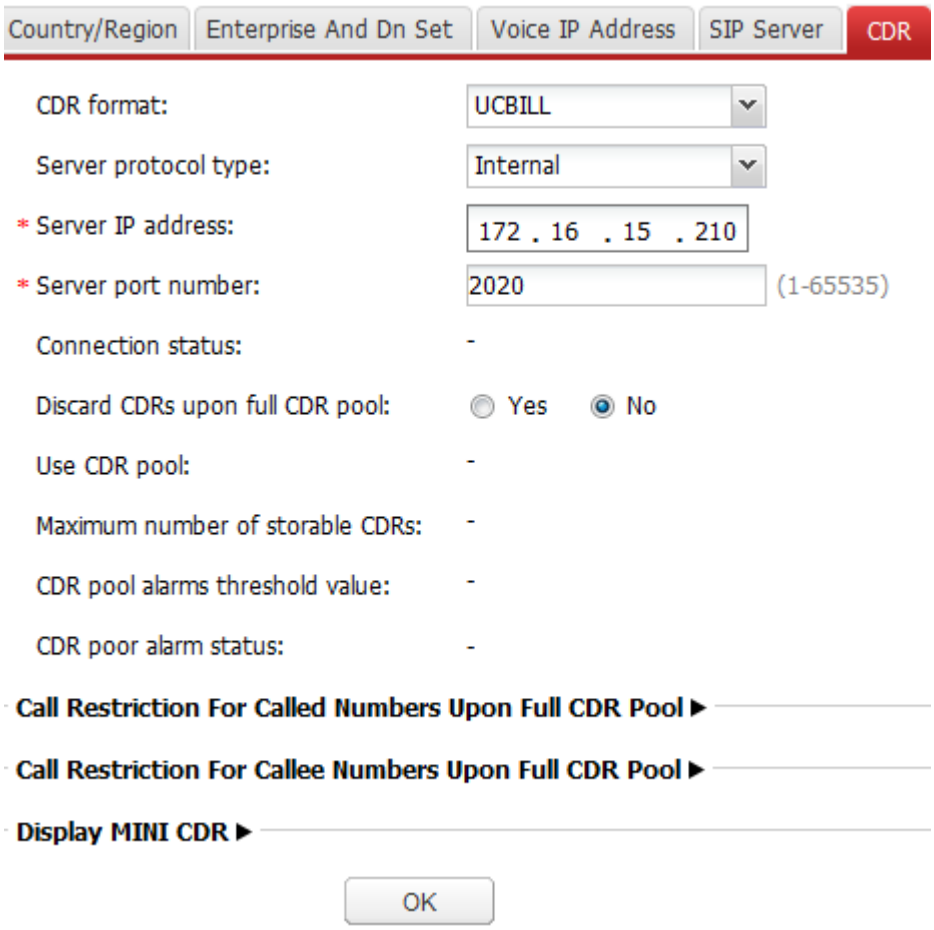


b. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.

- Provide CDRs through TCP.
  a. Set parameters on the **CDR** page.
  Figure 2-250 shows the **CDR** page.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-250 CDR page



b. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.

----End

Parameter Description

Parameter	Description
CDR format	CDR formats include: • CDR: CDR binary format • SOFTX: SOFT X3000 binary format • MINI: MINI text format • UCBILL: U1900 CDR
Server protocol type	• When **CDR format** is **CDR**, **SOFTX**, or **MINI**, the server protocol type is **FTP/SFTP**. • When **CDR format** is **UCBILL**, the server protocol type is **Internal**.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Server IP address	IP address of the CDR server.
Server port number	Port number of the CDR server.
User name	Defined user name when FTP/SFTP is used.
Password	Defined password when FTP/SFTP is used.
Confirm password	The parameter is used to check the FTP/SFTP password and ensure that the password is entered correctly.
CDR format	-
Discard CDRs upon full CDR pool	-
Call Restriction For Callee Numbers Upon Full CDR Pool	You can click ▶ to configure call restrictions for called numbers when the CDR pool is full.
Display MINI CDR	When the value of **CDR format** is **MINI**, you can click ▶ to configure displayed elements of CDRs in MINI format.

2.18.4 User Management

You can configure telephone numbers and different rights for different user types according to actual networking and user planning. Terminal users on the PBX contain POTS, SIP, and BRA users.

2.18.4.1 SIP User

After a number and call right are configured for a Session Initiation Protocol (SIP) user, the SIP user device such as an IP phone can make incoming and outgoing calls.

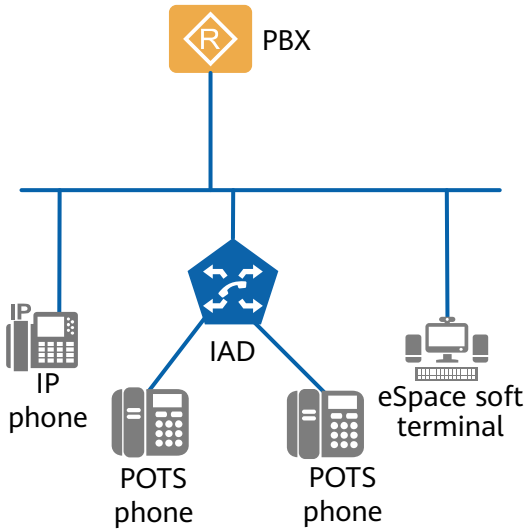
Context

A SIP user connects calls on the SIP server through SIP. SIP user devices can be IP phones, eSpace software terminals, and POTS phones connected to the eSpace IAD. The PBX as the SIP server receives registration and session requests of SIP users.

As shown in **Figure 2-251**, the PBX connects to SIP users.

Copyright © Huawei Technologies Co., Ltd.

Figure 2-251 PBX connects to SIP users



You can configure a single SIP user or multiple SIP users in batches. Select a configuration mode based on the number plan. If the batch configuration mode is used, the PBX configures multiple SIP users based on the start terminal ID, step, and user number, improving configuration efficiency. After you configure a SIP user, you can configure the call rights and service rights for the user. The call rights and service rights of different users may differ according to actual requirements.

After a user is configured, you can log in to the PBX web system using the user name and password. The default username and password are available in *AR Router Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it. If you forget the password after changing it, the administrator can restore the default password.

Assessing a Page

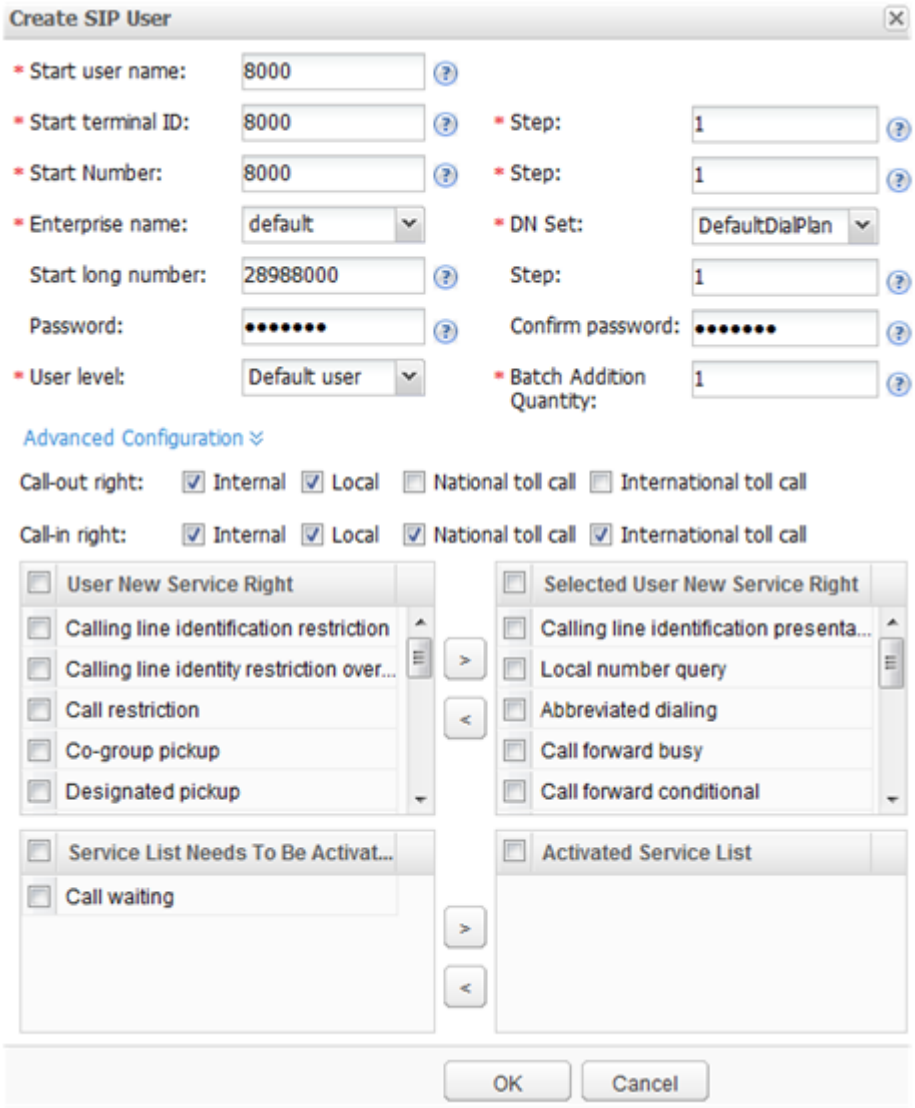
Choose **Voice Management** > **User Management** > **SIPUE User**.

Procedure

- Create a SIP user.
  a. Click **Create**.
  b. Set parameters in the **Create SIP User** dialog box.
  Figure 2-252 shows the **Create SIP User** dialog box.

Copyright © Huawei Technologies Co., Ltd.

Figure 2-252 Create SIP User dialog box



c. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.

- Modify a SIP user.
  a. Click next to the user.
  b. Set parameters in the **Modify SIP User** dialog box.
  c. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.
- Delete a SIP user.
  a. Select the SIP user you want to delete and click **Delete**.
  b. In the **Information** dialog box, click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.
- Reset the password for logging in to the web system.

 Copyright © Huawei Technologies Co., Ltd.

a. Click **Reset Password** next to the user.

b. In the **Information** dialog box, click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.

----End

Parameter Description

Parameter	Description
Start user name	User names cannot be duplicate with each other. It is recommended that you use the phone number to be assigned to a user as the user name.
Start terminal ID	Terminal identifier, that is, the registration account of a SIP user. The terminal IDs cannot be duplicate with each other. The terminal ID of a SIP user must be the same as that configured on the SIP trunk. It is recommended that you use the phone number to be assigned to a user as the terminal ID.
Step (Start user name/Start terminal ID)	Difference between two neighboring user names or terminal IDs. For example, if **Start user name** or **Start terminal ID** is set to **8000**, **Step** is set to **2**, and **Batch Addition Quantity** is set to **3**, the user names or terminal IDs of the three users are 8000, 8002, and 8004 respectively.
Start Number	Short code of the first user.
Step (Start Number)	Difference of two neighboring user numbers. For example, if **Start Number** is set to **8000**, **Step** is set to **2**, and **Batch Addition Quantity** is set to **3**, the short codes of the three users are 8000, 8002, and 8004 respectively.
Enterprise name	Enterprise to which the PBX user belongs.
DN Set	DN set to which the user is bound.
Start long number	Long code of the first user. Long codes are assigned by the carrier network such as the PSTN. Inter-office users can dial the long code directly to call a user.
Step (long code)	Difference between two neighboring long codes. For example, if **Start long number** is set to **28988000**, **Step** is set to **2**, and **Batch Addition Quantity** is set to **3**, the long codes of the three users are 28988000, 28988002, and 28988004 respectively.
Password	Authentication password for a SIP user. Please configure an authentication password for the user. If no authentication password is configured, the user account may be stolen by unauthorized users.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Confirm password	Password used to confirm that a correct password is entered.
Batch Addition Quantity	Number of users to be created.
User level	You need to set this parameter when the trunk group is bound to a call route using the routing policy with **User level** specified. A user can be the default user, common user, advanced user, or super user.
Call-out right	Call out rights of a user. The value can be **Internal**, **Local**, **National toll call**, or **International toll call**.
Call-in right	Call in rights of a user. The value can be **Internal**, **Local**, **National toll call**, or **International toll call**.
User status	User status. The value can be **normal** or **Forbidden**.
Service Right	Select a check box, and click > or < to set the service rights for users.
Activating Services	After the call waiting or call barring service right is added, you must activate the service. Select a check box, and click > or < to activate the service for users.

2.18.4.2 POTS User

After a number and call right are configured for a Plain Old Telephony Service (POTS) user, the POTS user device such as a POTS phone can make incoming and outgoing calls.

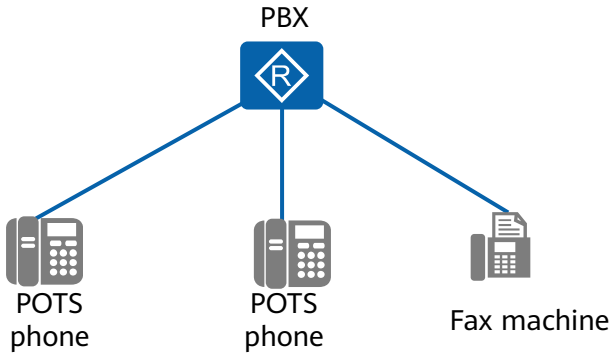
Context

A POTS user refers to a user of an analog phone or fax machine. POTS users connect to PBX's voice boards equipped with FXS ports using common phone cables.

As shown in **Figure 2-253**, the PBX connects to POTS users.

Copyright © Huawei Technologies Co., Ltd.

Figure 2-253 PBX connects to POTS users



You can configure a single POTS user or multiple POTS users in batches. Select a configuration mode based on the number plan. If the batch configuration mode is used, the PBX configures multiple POTS users based on the start terminal ID, step, and user number, improving configuration efficiency. After you configure a POTS user, you can configure the call rights and service rights for the user. The call rights and service rights of different users may differ according to actual requirements.

After a user is configured, you can log in to the PBX web system using the user name and password. The default username and password are available in *AR Router Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it. If you forget the password after changing it, the administrator can restore the default password.

Assessing a Page

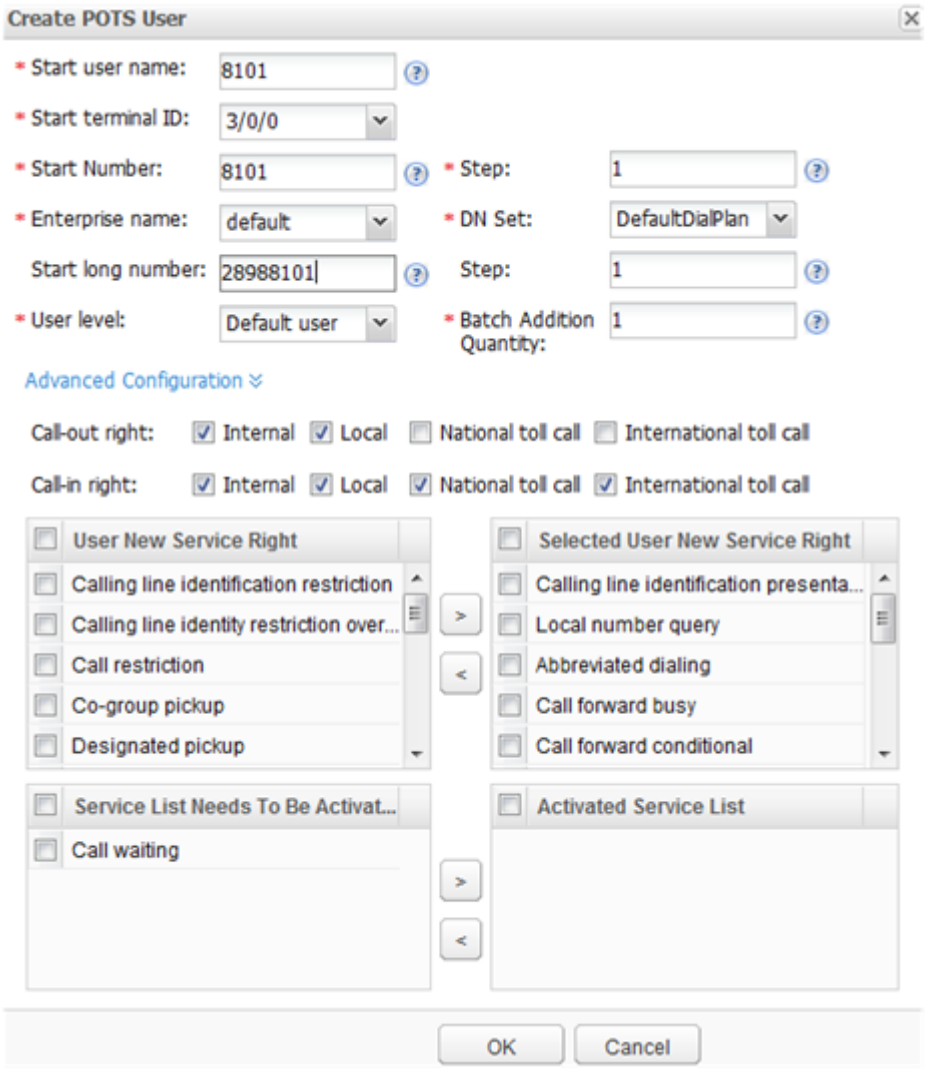
Choose **Voice Management** > **User Management** > **POTS User**.

Procedure

- Create a POTS user.
  a. Click **Create**.
  b. Set parameters in the **Create POTS User** dialog box.
  Figure 2-254 shows the **Create POTS User** dialog box.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-254 Create POTS User dialog box



c. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.

- Modify a POTS user.
  a. Click  next to the user.
  b. Set parameters in the **Modify POTS User** dialog box.
  c. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.
- Delete a POTS user.
  a. Select the POTS user you want to delete and click **Delete**.
  b. In the **Information** dialog box, click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.
- Reset the password for logging in to the web system.
  a. Click **Reset Password** next to the user.

 Copyright © Huawei Technologies Co., Ltd.

b. In the **Information** dialog box, click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.

----End

Parameter Description

Parameter	Description
Start user name	User names cannot be duplicate with each other. It is recommended that you use the phone number to be assigned to a user as the user name.
Start terminal ID	Number of the physical interface to which the first user is bound. The interface number is in the format of slot ID/subcard ID/interface sequence number.
Start Number	Short code of the first user.
Step (user name and user number)	Difference between two neighboring user names or user numbers. For example, if **Start user name** or **Start Number** is set to **8100**, **Step** is set to **2**, and **Batch Addition Quantity** is set to **3**, the names or numbers of the three users are 8100, 8102, and 8104 respectively.
Enterprise name	Enterprise to which the PBX user belongs.
DN Set	DN set to which the user is bound.
Start long number	Long code of the first user. Long codes are assigned by the carrier network such as the PSTN. Inter-office users can dial the long code directly to call a user.
Step (long code)	Difference between two neighboring long codes. For example, if **Start long number** is set to **28988000**, **Step** is set to **2**, and **Batch Addition Quantity** is set to **3**, the long codes of the three users are 28988000, 28988002, and 28988004 respectively.
User level	You need to set this parameter when the trunk group is bound to a call route using the routing policy with **User level** specified. A user can be the default user, common user, advanced user, or super user.
Batch Addition Quantity	Number of users to be created.
Call-out right	Call out rights of a user. The value can be **Internal**, **Local**, **National toll call**, or **International toll call**.
Call-in right	Call in rights of a user. The value can be **Internal**, **Local**, **National toll call**, or **International toll call**.
User status	User status. The value can be **normal** or **Forbidden**.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Service Right	Select a check box, and click > or < to set the service rights for users.
Activating Services	After the call waiting or call barring service right is added, you must activate the service. Select a check box, and click > or < to activate the service for users.

2.18.4.3 BRA User

After a number and call rights are configured for a BRA user, its Integrated Service Data Network (ISDN) phone can make incoming and outgoing calls.

Context

A BRA user connects to the 2BST card of the PBX through an ISDN telephone line, and the 2BST card must work in NT mode.

You can configure a single BRA user or multiple BRA users in batches. Select a configuration mode based on the number plan. If the batch configuration mode is used, the PBX configures multiple BRA users based on the start terminal ID, step, and user number, improving configuration efficiency. After you configure a BRA user, you can configure the call rights and service rights for the user. The call rights and service rights of different users may differ according to actual requirements.

After a user is configured, you can log in to the PBX web system using the user name and password. The default username and password are available in *AR Router Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it. If you forget the password after changing it, the administrator can restore the default password.

Prerequisites

- The 2BST card has been configured to work in NT mode using the **set workmode slot** *slot-id* **bri bri-voice** { **nt-mode** } command in the system view.
- The remote power supply of the interface has been configured. For details, see the *Configuring an ISDN User* of *CLI-based Configuration*.

Assessing a Page

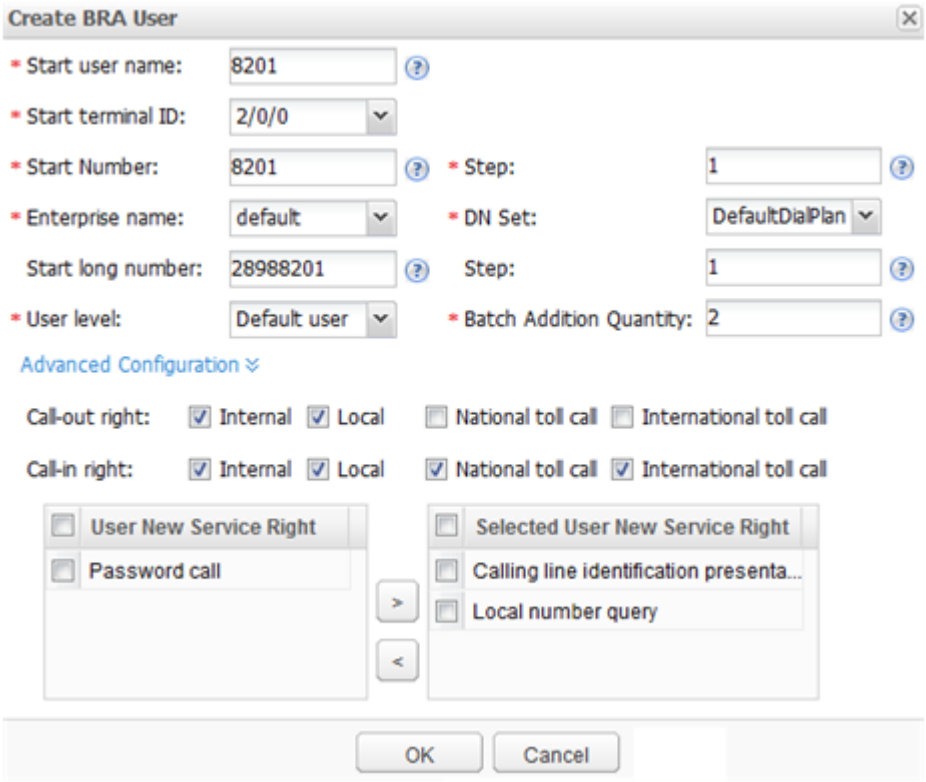
Choose **Voice Management** > **User Management** > **BRA User**.

Copyright © Huawei Technologies Co., Ltd.

Procedure

- Create a BRA user.
  a. Click **Create**.
  b. Set parameters in the **Create BRA User** dialog box.
  Figure 2-255 shows the **Create BRA User** dialog box.

  Figure 2-255 Create BRA User dialog box



  c. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.
- Modify a BRA user.
  a. Click  next to the user.
  b. Set parameters in the **Modify BRA User** dialog box.
  c. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.
- Delete a BRA user.
  a. Select the BRA user you want to delete and click **Delete**.
  b. In the **Information** dialog box, click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.
- Reset the password for logging in to the web system.
  a. Click **Reset Password** next to the user.

Copyright © Huawei Technologies Co., Ltd.

b. In the **Information** dialog box, click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.

----End

Parameter Description

Parameter	Description
Start user name	User names cannot be duplicate with each other. It is recommended that you use the phone number to be assigned to a user as the user name.
Start terminal ID	Number of the physical interface to which the first user is bound. The interface number is in the format of slot ID/subcard ID/interface sequence number.
Start Number	Short code of the first user.
Step (user name and user number)	Difference between two neighboring user names or user numbers. For example, if **Start user name** or **Start Number** is set to **8100**, **Step** is set to **2**, and **Batch Addition Quantity** is set to **3**, the names or numbers of the three users are 8100, 8102, and 8104 respectively.
Enterprise name	Enterprise to which the PBX user belongs.
DN Set	DN set to which the user is bound.
Start long number	Long code of the first user. Long codes are assigned by the carrier network such as the PSTN. Inter-office users can dial the long code directly to call a user.
Step (long code)	Difference between two neighboring long codes. For example, if **Start long number** is set to **28988000**, **Step** is set to **2**, and **Batch Addition Quantity** is set to **3**, the long codes of the three users are 28988000, 28988002, and 28988004 respectively.
User level	You need to set this parameter when the trunk group is bound to a call route using the routing policy with **User level** specified. A user can be the default user, common user, advanced user, or super user.
Batch Addition Quantity	Number of users to be created.
Call-out right	Call out rights of a user. The value can be **Internal**, **Local**, **National toll call**, or **International toll call**.
Call-in right	Call in rights of a user. The value can be **Internal**, **Local**, **National toll call**, or **International toll call**.
User status	User status. The value can be **normal** or **Forbidden**.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Service Right	Select a check box, and click > or < to set the service rights for users.
Activating Services	After the call waiting or call barring service right is added, you must activate the service. Select a check box, and click > or < to activate the service for users.

2.18.4.4 Querying Historical Call Records

This section describes how to query the historical call records of online users.

Context

You can query the historical call records of online users. Each record contains five fields: calling number, called number, call start time, call end time, and call duration. You can obtain the latest CDR data to analyze whether the charging based on the call duration is correct.

NOTE

V200R010C10 and later versions support the function.

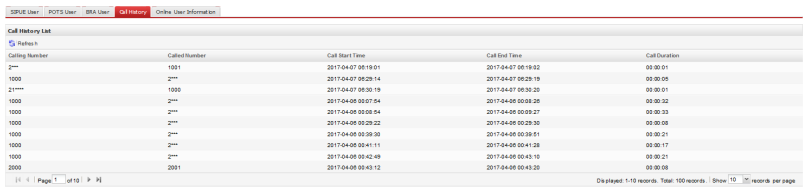
Accessing a Page

Choose **Voice Management** > **User Management** > **Call History**.

Procedure

- Click **Call History** to view historical call records.
  Figure 2-256 shows the **Call History** page.

  Figure 2-256 Querying historical call records

----End

 Copyright © Huawei Technologies Co., Ltd.

Parameter Description

Parameter	Description
Calling Number	The outer-office number is the called number in an outgoing call and is the calling number in an incoming call. If an outer-office number contains more than four digits, the last four digits are hidden. If an outer-office number contains one to four digits, only the first digit is displayed. If an outer-office number contains one digit, the digit is hidden. Digits in intra-office numbers are not hidden.
Called Number	The outer-office number is the called number in an outgoing call and is the calling number in an incoming call. If an outer-office number contains more than four digits, the last four digits are hidden. If an outer-office number contains one to four digits, only the first digit is displayed. If an outer-office number contains one digit, the digit is hidden. Digits in intra-office numbers are not hidden.
Call Start Time	Time when a call starts, in the format YYYY-MM-DD hh:mm:ss. • YYYY specifies the year. The value is an integer in the range from 1970 to 2099. • MM specifies the month. The value is an integer in the range from 1 to 12. • DD specifies the day. The value is an integer in the range from 1 to 31. • hh indicates the hour. The value is an integer in the range from 0 to 23. • mm indicates the minute. The value is an integer in the range from 0 to 59. • ss indicates the second. The value is an integer in the range from 0 to 59.
Call End Time	Time when a call ends, in the format YYYY-MM-DD hh:mm:ss. • YYYY specifies the year. The value is an integer in the range from 1970 to 2099. • MM specifies the month. The value is an integer in the range from 1 to 12. • DD specifies the day. The value is an integer in the range from 1 to 31. • hh indicates the hour. The value is an integer in the range from 0 to 23. • mm indicates the minute. The value is an integer in the range from 0 to 59. • ss indicates the second. The value is an integer in the range from 0 to 59.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Call Duration	Time difference between the start time and end time of a call.

2.18.4.5 Querying Online Users

This section describes how to query information about online users.

Context

After users are configured, you can query information about online users.

NOTE

V200R010C10 and later versions support the function.

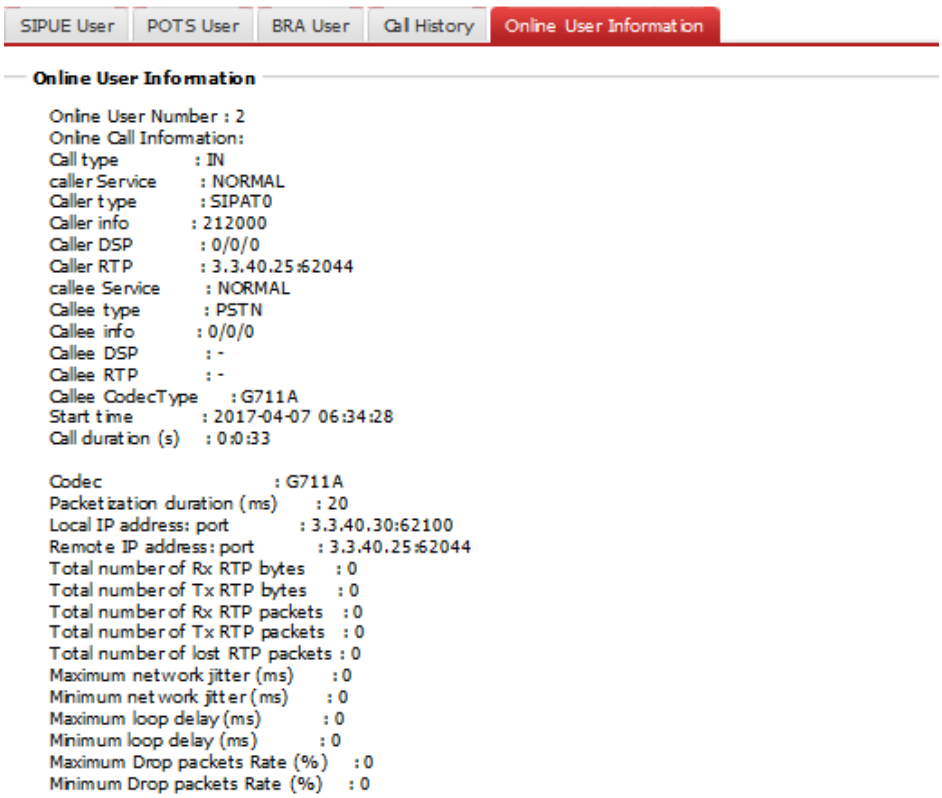
Accessing a Page

Choose **Voice Management** > **User Management** > **Online User Information**.

Procedure

- Click **Online User Information** to view the online user records.
  Figure 2-257 shows the **Online User Information** page.

  Figure 2-257 Online user records



 Copyright © Huawei Technologies Co., Ltd.

----End

Parameter Description

Parameter	Description
Online User Number	Number of online users.
Online Call Information	Online call information.
Call type	Call type.
caller Service	Service type.
Caller type	Type of the calling party.
Caller info	Terminal identifier of the calling party.
Caller DSP	DSP used by the calling party.
Caller RTP	IP address and port number used by the calling party to send and receive RTP packets during a call.
callee Service	Service type.
Callee type	Called number type.
Callee info	Terminal identifier of the called party.
Callee DSP	DSP used by the called party.
Callee RTP	IP address and port number used by the called party to send and receive RTP packets during a call.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Callee CodecType	Codec type, including: • G711U • G726 • G723 • G711A • G722 • G728 • G729 • G723Low • g726-16k • g726-24k • g726-32k • g726-40k • R2198 • R2833 • v150 • clearmode • T.38 • T.38+2
Start time	Call start time.
Call duration (s)	Duration in which a call lasts.
Codec	Codec.
Packetization duration (ms)	Packetization duration.
Local IP address: port	Local IP address and port number.
Remote IP address: port	Remote IP address and port number.
Total number of Rx RTP bytes	Total number of bytes received at the local end.
Total number of Tx RTP bytes	Total number of bytes sent by the local end.
Total number of Rx RTP packets	Total number of packets received at the local end.
Total number of Tx RTP packets	Total number of packets sent by the local end.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Total number of lost RTP packets	Total number of lost RTP packets.
Maximum network jitter (ms)	Maximum network jitter.
Minimum network jitter (ms)	Minimum network jitter.
Maximum loop delay (ms)	Maximum round-trip delay (RTD).
Minimum loop delay (ms)	Minimum RTD.
Maximum Drop packets Rate (%)	Maximum packet loss ratio.
Minimum Drop packets Rate (%)	Minimum packet loss ratio.

2.18.5 Call Route

You can configure call routes so that the PBX can provide correct routes for outgoing calls.

2.18.5.1 Call Route

A call route defines the routing rules for outgoing calls. It consists of call prefixes and trunk groups.

Context

The PBX can select routes according to routing policies defined by subscribers. The PBX intelligently selects trunk links for voice transmission to minimize costs and implement load balancing. The routing policies are classified into the following types:

- Time-based: The PBX selects different routes for outgoing calls based on the time period. For example, outgoing calls are made through the R2 trunk from 08:00:00 to 18:00:00, and are made through the SIP trunk at other times.
- Charge-rate-based: The PBX selects different routes for outgoing calls based on the charge rate. For example, charge rates for outgoing calls made through the R2 trunk and SIP trunk are 1 and 2 respectively.
- Load sharing: The PBX performs route polling according to trunk group numbers in ascending order till it finds a route that has an idle circuit.

Copyright © Huawei Technologies Co., Ltd.

- Percentage load sharing: The PBX selects routes for outgoing calls based on the call percentage. For example, 30% outgoing calls are made through the R2 trunk and the other 70% through the SIP trunk.
- Subscriber level: The PBX selects routes for outgoing calls based on the subscriber right level. For example, calls from subscribers with default rights are made through the R2 trunk, and calls from subscribers with common rights are made through the SIP trunk.
- Load balancing: The PBX performs route polling according to trunk group numbers in ascending order till it finds an office direction that has the largest number of idle circuits.
- Calling number: The PBX selects routes based on the calling number. For example, internal numbers of two intra-office subscribers are 6000 and 8000 respectively. You can configure the SIP1 trunk for outgoing calls made by the subscriber whose call prefix is 6 and the SIP2 trunk for the subscriber whose call prefix is 8.

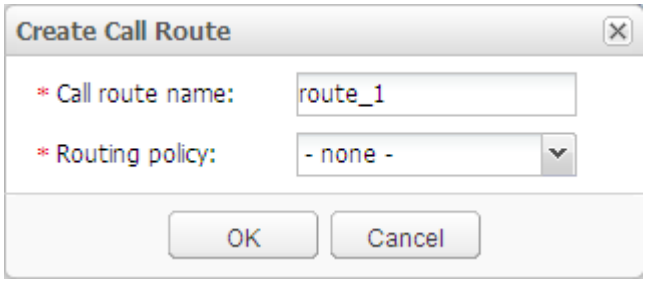
Accessing a Page

Choose **Voice Management** > **Call Route** > **Call Route**.

Procedure

- Create a call route.
  a. Click **Create**.
  b. Set parameters in the **Create Call Route** dialog box.
  Figure 2-258 shows the **Create Call Route** dialog box.

  Figure 2-258 Create Call Route dialog box

  c. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.
- Modify a call route.
  a. Click next to the route.
  b. Set parameters in the **Modify Call Route** dialog box.
  c. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.
- Delete a call route.
  a. Select the route to be deleted, and click **Delete**.

Copyright © Huawei Technologies Co., Ltd.

b. In the **Information** dialog box, click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.

----End

Parameter Description

Parameter	Description
Call route name	-
Routing policy	Select a routing policy in the drop-down list box. When no routing policy is used, select **none**.

2.18.5.2 Reroute Solution

If the PBX fails to select a route according to a configured routing policy, the PBX reselects a route according to the backup routing policy.

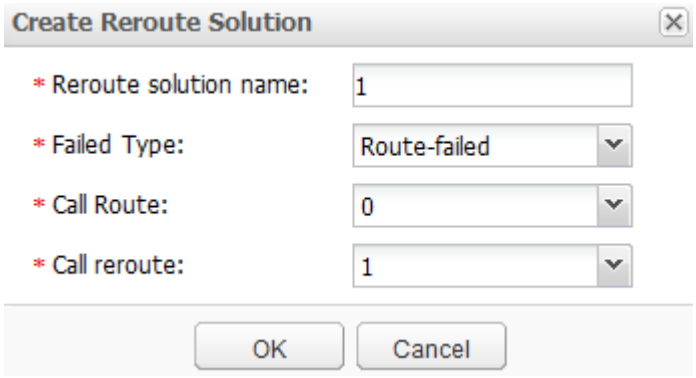
Accessing a Page

Choose **Voice Management** > **Call Route** > **Reroute Solution**.

Procedure

- Create a reroute solution.
  a. Click **Create**.
  b. Set parameters in the **Create Reroute Solution** dialog box.
  Figure 2-259 shows the **Create Reroute Solution** dialog box.

  Figure 2-259 Create Reroute Solution dialog box

  c. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.
- Modify a reroute solution.
  a. Click  next to the reroute solution.

Copyright © Huawei Technologies Co., Ltd.

b. Set parameters in the **Modify Reroute Solution** dialog box.
c. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.

- Delete a reroute solution.
  a. Select the reroute solution to be deleted, and click **Delete**.
  b. In the **Information** dialog box, click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.

----End

Parameter Description

Parameter	Description
Reroute solution name	-
Failed Type	Failed type including: ● Route-failed: The cause is that the trunk link is faulty. ● Call-failed: The possible cause is that the SIP trunk link is faulty or the remote device is faulty.
Call Route	In the drop-down list box, select the name of the call route that needs to be configured with a call reroute.
Call reroute	In the drop-down list box, select the name of the call reroute. It indicates that if **Call Route** cannot be selected, **Call reroute** is used.

2.18.6 Prefix Configuration

After intra-office and inter-office prefixes are configured on the PBX, intra-office users can call each other, and intra-office users can call inter-office users.

Context

A call prefix is a string of consecutive digits starting from the first digit of a called number. It can be the first digit or several digits starting from the first digit of a called number. That is, a call prefix is a subset of a called number. For example, you can define either of the following intra-office call prefixes for the called number 1234:

- First digit: 1
- First two digits: 12
- First three digits: 123
- Called number: 1234

A group of call prefixes configured on the PBX constitutes a DN set. If the preceding call prefixes all exist in the DN set, the PBX analyzes the called number

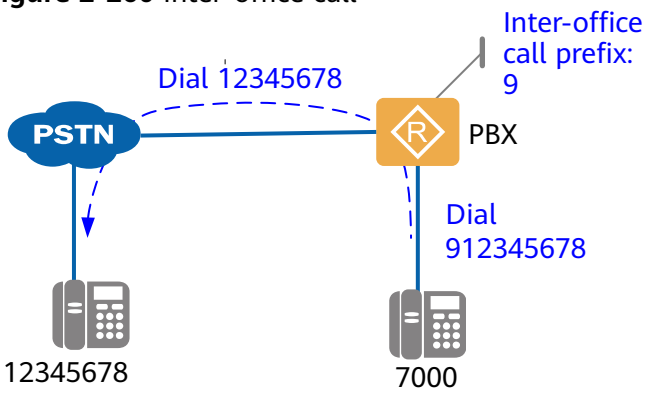
 Copyright © Huawei Technologies Co., Ltd.

according to the longest match principle. For example, a user calls 1234. If call prefixes 1, 12, and 1234 are configured in a DN set, the PBX matches the called number with the call prefix 1234 according to the longest match principle.

Call prefixes are classified into the following types:

- Intra-office call prefix: is applicable to scenarios where intra-office and inter-office users call intra-office users. For example, the intra-office number range is 7000 to 7099. You can configure the intra-office call prefix 7. You need to dial only the intra-office user number such as 7001 when calling an intra-office user.
- Inter-office call prefix: is used by intra-office users to make outgoing calls, for example, intra-office users make local calls, national toll calls, and international toll calls. Assuming that the inter-office call prefix is 9, intra-office user 7000 can dial 912345678 when calling inter-office user 12345678. The PBX parses and changes the number (for example, delete 9) to make outgoing calls.

Figure 2-260 Inter-office call



NOTE

A call prefix can be flexibly configured depending on the user number plan.

You can configure a call prefix for basic services, new services, supplementary services, and the Interactive Voice Response (IVR) service. The call prefix for the IVR service is called the service access code. For example, you can set a call prefix ***192*** for the self-number query service.

In the prefix query result, **#***** and ******** are prefixes reserved by the system and are used for the conference service, **#99*** is used for turning on the MWI, and ***99*** is used for turning off the MWI.

Prerequisites

Call Route has been configured.

Assessing a Page

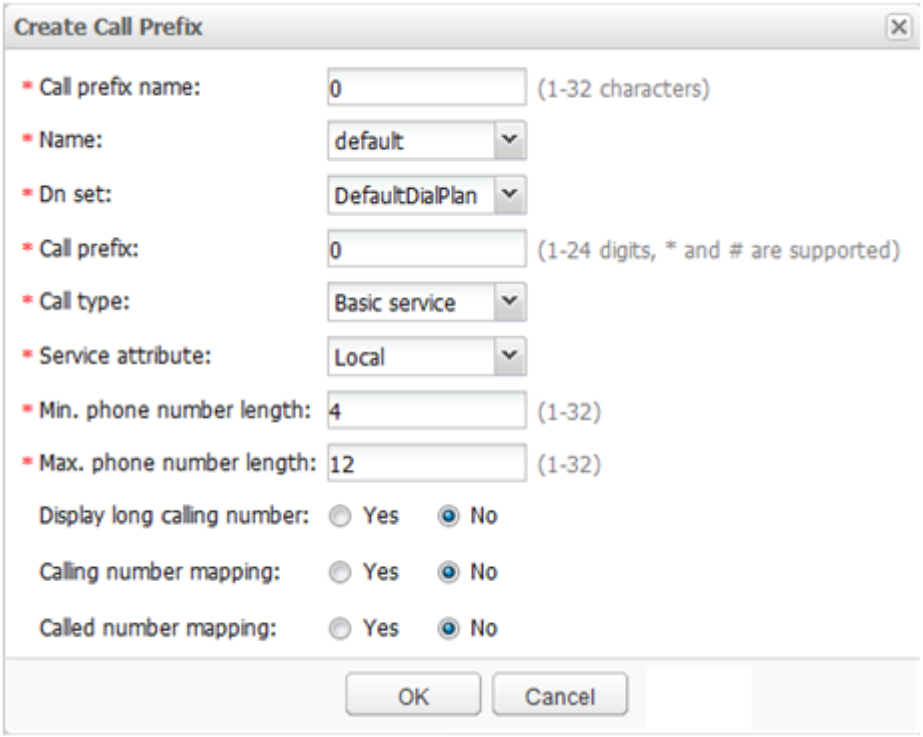
Choose **Voice Management** > **Prefix Configuration**.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

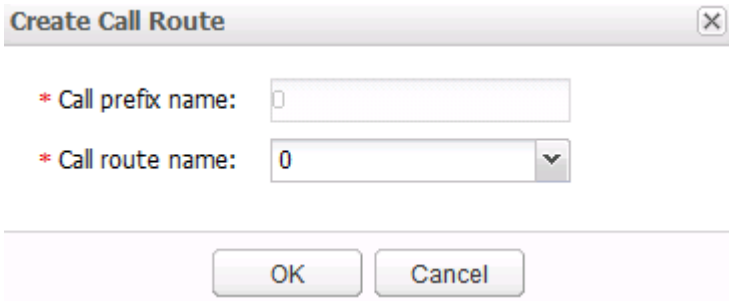
- Create a call prefix.
  a. Click **Create**.
  b. Set parameters in the **Create Call Prefix** dialog box.
  Figure 2-261 shows the **Create Call Prefix** dialog box.

  Figure 2-261 Create Call Prefix dialog box



  c. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.
  d. Click **Call Route** next to the call prefix.
  e. In the **Configure Call Route** dialog box that is displayed, click **Create**.
  f. In the **Create Call Route** dialog box, set parameters.
  Figure 2-262 shows the **Create Call Route** dialog box.

  Figure 2-262 Create Call Route dialog box



Copyright © Huawei Technologies Co., Ltd.

g. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.

- Modify a call prefix.
  a. Click  next to the call prefix.
  b. Set parameters in the **Modify Call Prefix** dialog box.
  c. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.
- Delete a call prefix.
  a. Select the call prefix you want to delete and click **Delete**.
  b. In the **Information** dialog box, click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.

----End

Parameter Description

Parameter	Description
Call prefix name	Name of a call prefix name. It is recommended that the call prefix name be the same as the call prefix. **NOTE** If spaces are used, include the string with spaces in double quotation marks (""), such as, "this is an example".
Name	Name of the enterprise to which the call prefix belongs.
Dn set	DN set bound to the call prefix.
Call prefix	Call prefix.
Call type	Call type of the call prefix. • When you configure an intra-office or inter-office call prefix, select **Basic service**. • When you configure a call prefix for service registration or deregistration, select **New service and supplementary service management** or **Supplementary service**. • When you configure a call prefix for the switchboard, select **IVR**.
Service attribute	Service attribute of the call prefix. Configure this parameter only when the call type is not IVR. The listed service attributes vary according to the call type.
Service	IVR service for the call prefix. Configure this parameter only when the call type is IVR. The listed service names are defined in the IVR scripts configured in the system or uploaded to the PBX.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
VU loop count	Number of times the IVR voice file for the call prefix can be played. Configure this parameter only when the call type is IVR.
Call-out right	Configure this parameter only when the call type is IVR. The call-out right can be **Internal**, **Local**, **National toll call**, or **International toll call**.
Min. phone number length	Minimum length of a number that can be parsed (with the call prefix included).
Max. phone number length	Maximum length of a number that can be parsed (with the call prefix included).
Display long calling number	Whether the long calling number (for example, 28980001) is displayed when the user (for example, 8001) makes an outgoing call using the call prefix. You are advised to select **Yes** when a long calling number is configured. For details on how to configure a long calling number, see **2.18.4 User Management**.
Calling number mapping	Whether the mapped calling number (for example, 28988010) is displayed when the user (for example, 8001) makes an outgoing call using the call prefix. You are advised to select **Yes** when **Number Mapping** is configured.
Called number mapping	Whether called number mapping is enabled during number parsing based on the current call prefix for incoming calls. If this function is enabled, the call number 28988010 is changed to an intra-office short code 8001. You are advised to select **Yes** when **Number Mapping** is configured.
Call route name	Call route bound to the call prefix.

2.18.7 Trunk Group

Trunk groups are used to constitute a route. Generally, a group of trunk circuits with the same attributes in the same direction are called a trunk group.

2.18.7.1 PRA Trunk Group

This section describes how to configure a PRA trunk group to implement voice communication between PBX users and inter-office users. You can set parameters such as signaling mode, access mode, circuit selection mode, outgoing call right, and call route.

Copyright © Huawei Technologies Co., Ltd.

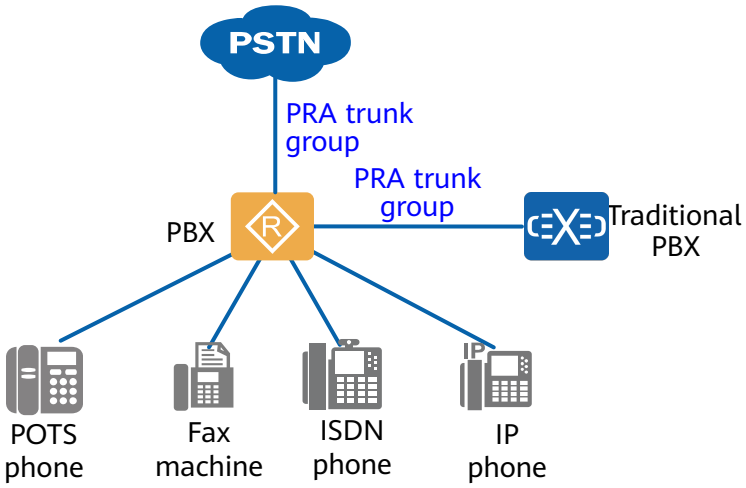
Context

A PRA trunk group uses Digital Subscriber Signaling No.1 (DSS1) or Q Signaling (QSIG) as the control signaling and can work at the user or network side.

A trunk group must be bound to a specific call route. You can configure the routing plan for the trunk group based on the routing policy of the call route. If a time-based routing policy is used, select the time segment index when you select a specific call route.

In a PBX, you can use a PRA trunk group to implement upstream connection to the PSTN or downstream connection to the existing PBX devices in an enterprise, to protect customer investment and ensure smooth expansion. **Figure 2-263** shows the PRA trunk group networking.

Figure 2-263 PRA trunk group networking



Prerequisites

- **Call Route** has been configured.
- **Routing Time Range Index** has been configured if you bind a trunk group to a call route using time-based routing policy.
- The VE1 interface has been configured. For details, see the *Configuring a PRA Trunk Group* of *CLI-based Configuration*.

Assessing a Page

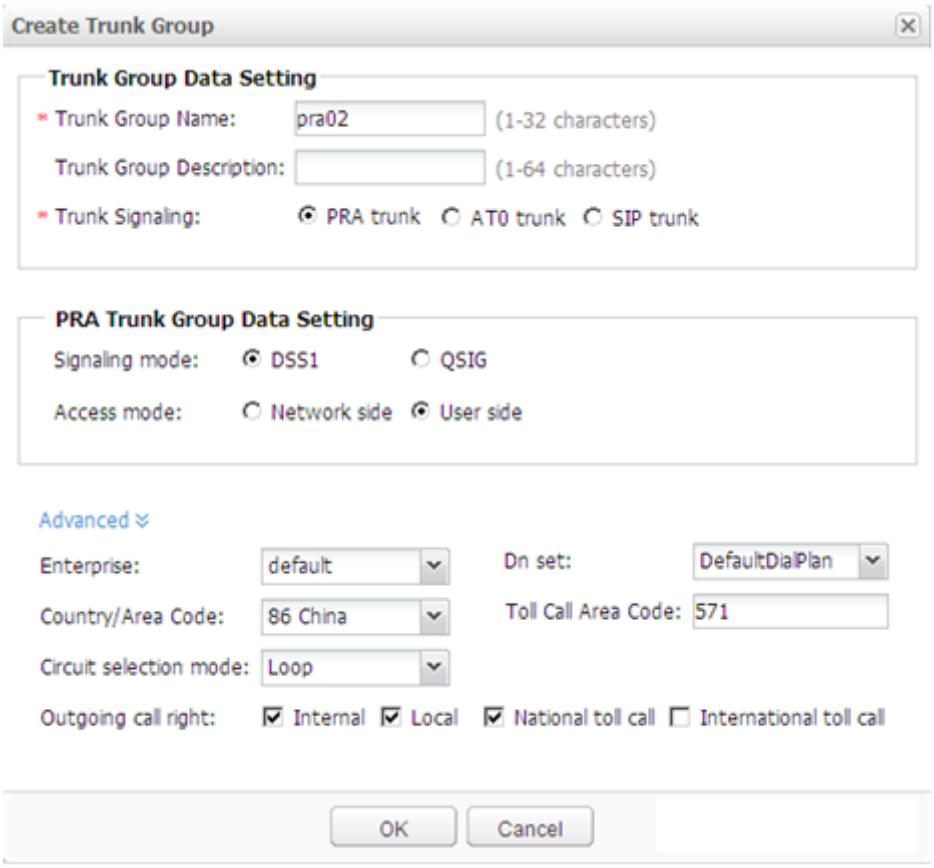
Choose **Voice Management** > **Trunk Group**.

Procedure

- Create a trunk group.
  a. Click **Create**.
  b. Select **PRA trunk** and set parameters in the **Create Trunk Group** dialog box.
  Figure 2-264 shows the **Create Trunk Group** dialog box.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-264 Create Trunk Group dialog box

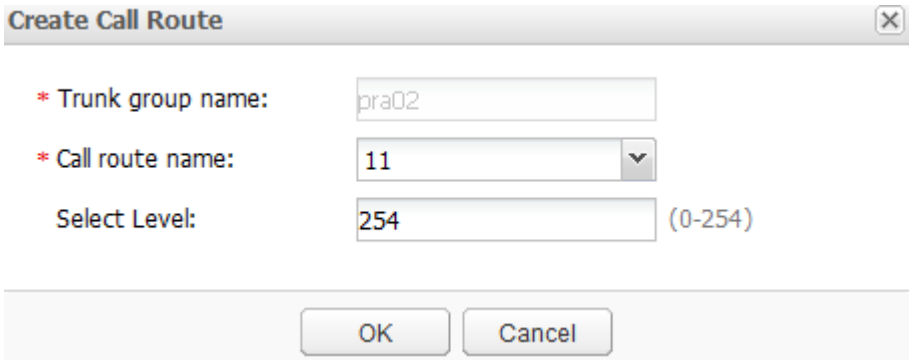


c. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.

- Modify a trunk group.
  a. Click  next to the trunk group.
  b. Set parameters in the **Modify Trunk Group** dialog box.
  c. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.
- Delete a trunk group.
  a. Select the trunk group you want to delete and click **Delete**.
  b. In the **Information** dialog box, click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.
- Create a call route.
  a. Click **Call Route** next to the trunk group.
  b. Click **Create** in the **Configure Call Route** dialog box.
  c. Select a call route in the **Create Call Route** dialog box.
  Figure 2-265 shows the **Create Call Route** dialog box.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-265 Create Call Route dialog box



d. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.

- Modify a call route.
  a. Click **Call Route** next to the trunk group.
  b. Select the call route you want to modify in the **Configure Call Route** dialog box and click next to the call route.
  c. Set parameters in the **Modify Call Route** dialog box.
  d. In the **Information** dialog box, click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.
- Delete a call route.
  a. Click **Call Route** next to the trunk group.
  b. Select the call route you want to delete in the **Configure Call Route** dialog box and click **Delete**.
  c. In the **Information** dialog box, click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.

----End

Parameter Description

Parameter	Description
Trunk Group Name	Unique identifier of a trunk group.
Trunk Group Description	Description of the trunk group, helping differentiate trunk groups.
Signaling mode	Signaling type used by the trunk group. The value can be **DSS1** or **QSIG**. Ensure that the signaling mode is the same as that used by the remote device.
Access mode	Access mode, which can be network side or user side. One of the two devices connected through the PRA trunk group must be used as the user-side device, and the other must be used as the network-side device.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Enterprise	Enterprise to which the trunk group belongs.
Dn set	DN set to which the trunk group is bound.
Country/Area Code	Country or area code of an incoming call through the trunk group. If the incoming call does not contain a country or area code, the system automatically adds the country or area code, so that users can view the country or area code through the Calling Line Identification Presentation (CLIP) function.
Toll Call Area Code	Area code of an incoming toll call through the trunk group. If the incoming call does not contain an area code, the system automatically adds the country or area code, so that users can view the country or area code through the CLIP function.
Circuit selection mode	Circuit selection mode used by the trunk group. The value can be **Loop**, **Increase**, **Decrease**, or **Master** (controled by the user).
Outgoing call right	Outgoing call rights of the trunk group. The value can be **Local**, **Internal**, **National toll call**, or **International toll call**.
Call route name	Call route bound to the trunk group.
Time segment index	You need to set this parameter when the trunk group is bound to a call route using time-based routing policy. This parameter is optional and is defined in **2.18.11.2 Time Segment Index**.
Percentage	You need to set this parameter when the trunk group is bound to a call route using the routing policy with **Load percentage** specified. The unit is %.
Charging rate	You need to set this parameter when the trunk group is bound to a call route using the routing policy with **Based on charging rate** specified.
User level	You need to set this parameter when the trunk group is bound to a call route using the routing policy with **User level** specified.

NOTE

When you set **Trunk Group Name** and **Trunk Group Description**, enter character strings with spaces included in double quotation marks (""), such as, "this is an example".

2.18.7.2 SIP Trunk Group

This section describes how to configure a SIP trunk group to implement voice communication between PBX users and inter-office users. You can set parameters

Copyright © Huawei Technologies Co., Ltd.

such as trunk registration mode, transmission mode, circuit selection mode, outgoing call right, and call route.

Context

There are three SIP trunk groups based on the registration mode, as shown in **Table 2-177**.

Table 2-177 SIP trunk groups

Type	Description
SIP IP trunk group	The PBX at one end of a SIP IP trunk group does not need to register with the device at the other end. Unlike a circuit trunk group that defines a physical channel, a SIP IP trunk group defines a logical channel and solves authentication and addressing problems between local and remote offices. When you configure a SIP IP trunk group for the PBX, the remote end must be the device supporting SIP IP trunks.
SIP AT0 trunk group	After an enterprise applies for SIP users from the carrier, configure a SIP AT0 trunk group to implement voice communication between PBX users and inter-office users. A SIP AT0 trunk group, similar to an AT0 trunk group based on POTS users, works over the IP network and uses SIP. The SIP users are separately registered on the carrier network such as IMS networks. Then trunks of the SIP AT0 trunk group are formed. The carrier network connects to common SIP users, and does not learn about the private network. An enterprise user occupies one trunk of the SIP AT0 trunk group to make outgoing calls. Incoming calls are made through the enterprise switchboard or an enterprise user.
SIP PRA trunk group	After an enterprise applies for SIP users from the carrier, configure a SIP PRA trunk group to implement voice communication between PBX users and inter-office users. Unlike a SIP AT0 trunk group, a SIP PRA trunk group uses trunk group registration. That is, the SIP PRA trunk group sends a registration message to complete number registration of a group of SIP users. Then trunks of the SIP PRA trunk group are formed. The carrier network connects to common SIP users, and does not learn about the private network. An enterprise user occupies one trunk of the SIP PRA trunk group to make outgoing calls. Incoming calls are made through the enterprise switchboard or an enterprise user.

Table 2-178 describes the transport protocols that can be used by a SIP trunk group.

Copyright © Huawei Technologies Co., Ltd.

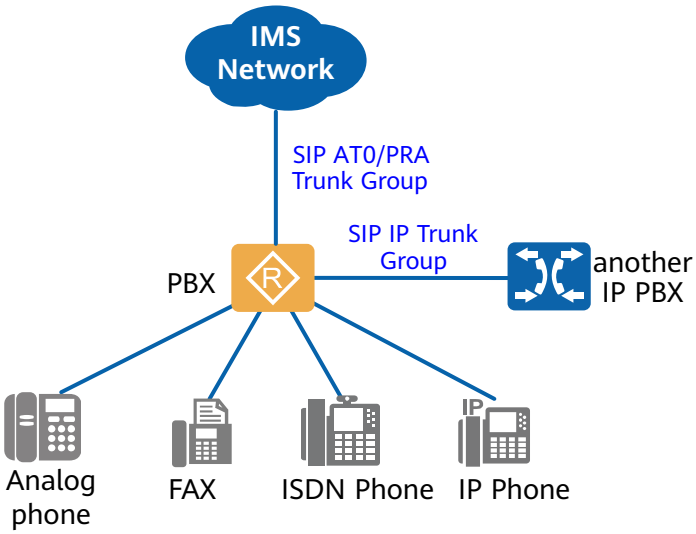
Table 2-178 Transport protocols that can be used by a SIP trunk

Transport Protocol	Description
UDP	Connectionless transport-layer protocol that provides event-based, simplified, and unreliable information transmission. When UDP is used to transmit data, each datagram is independent and contains the source and destination. Because UDP is unreliable, data may not reach the destination, and the time data reaches the destination and data integrity cannot be ensured.
TCP	Connection-oriented protocol. Before data transmission, both ends must establish a virtual channel.

A trunk group must be bound to a specific call route. You can configure the routing plan for the trunk group based on the routing policy of the call route. If a time-based routing policy is used, select the time segment index when you select a specific call route.

The PBX connects to the carrier network and an IP PBX through SIP trunk groups, as shown in **Figure 2-266**.

Figure 2-266 Networking of SIP trunk groups



Prerequisites

- **Voice IP Address** has been configured.
- **Call Route** has been configured.
- **Routing Time Range Index** has been configured if you bind a trunk group to a call route using time-based routing policy.

Copyright © Huawei Technologies Co., Ltd.

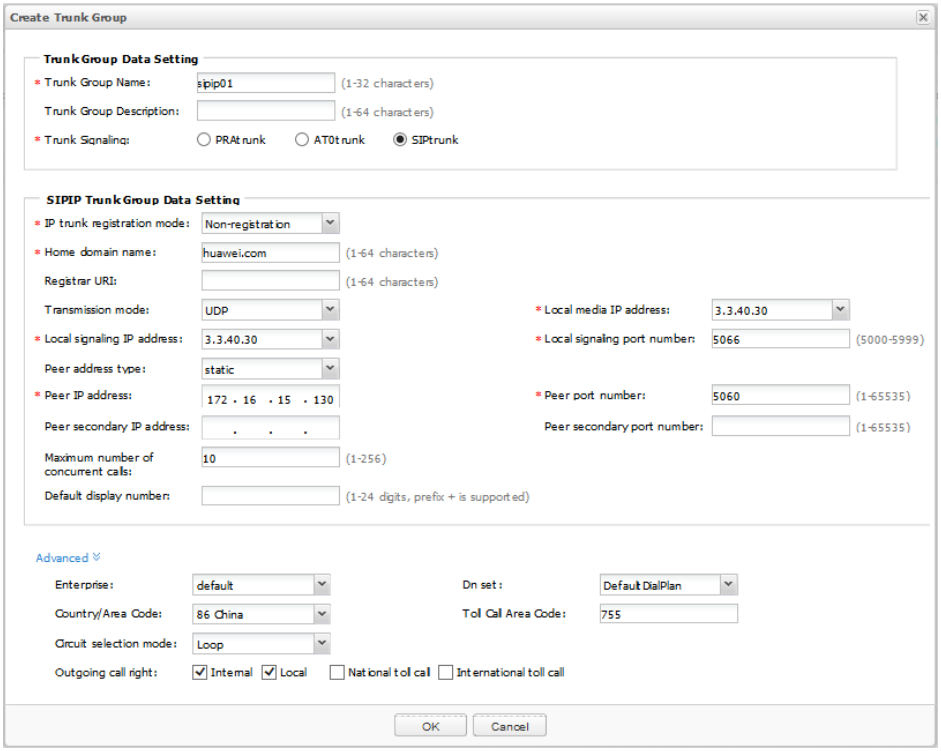
Assessing a Page

Choose **Voice Management** > **Trunk Group**.

Procedure

- Create a trunk group.
  a. Click **Create**.
  b. Select **SIP trunk** and set parameters in the **Create Trunk Group** dialog box.
  Figure 2-267 shows the data configuration dialog box (for example, for configuring a SIP IP trunk group).

  Figure 2-267 Create Trunk Group dialog box



  NOTE

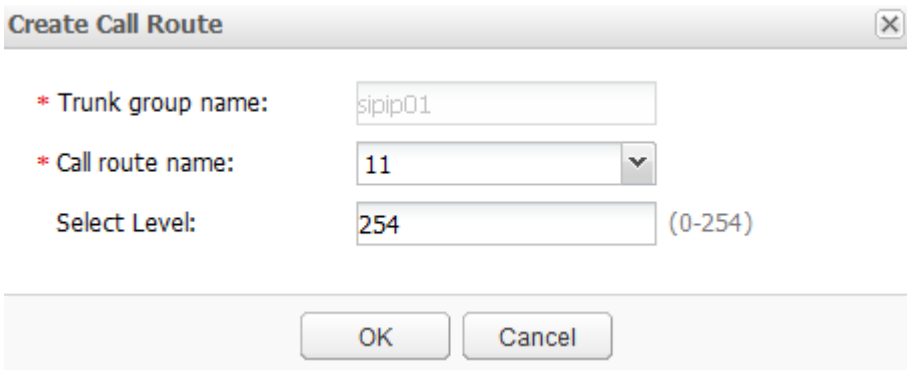
  V200R010C10 and later versions support the configuration of **Peer address type**.
  c. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.
- Modify a trunk group.
  a. Click  next to the trunk group.
  b. Set parameters in the **Modify Trunk Group** dialog box.
  c. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.
- Delete a trunk group.

 Copyright © Huawei Technologies Co., Ltd.

a. Select the trunk group you want to delete and click **Delete**.
b. In the **Information** dialog box, click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.

- Create a call route.
  a. Click **Call Route** next to the trunk group.
  b. Click **Create** in the **Configure Call Route** dialog box.
  c. Select a call route in the **Create Call Route** dialog box.
  Figure 2-268 shows the **Create Call Route** dialog box.

  Figure 2-268 Create Call Route dialog box



  d. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.
- Modify a call route.
  a. Click **Call Route** next to the trunk group.
  b. Select the call route you want to modify in the **Configure Call Route** dialog box and click  next to the call route.
  c. Set parameters in the **Modify Call Route** dialog box.
  d. In the **Information** dialog box, click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.
- Delete a call route.
  a. Click **Call Route** next to the trunk group.
  b. Select the call route you want to delete in the **Configure Call Route** dialog box and click **Delete**.
  c. In the **Information** dialog box, click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.

----End

Parameter Description

Parameter	Description
Trunk Group Name	Unique identifier of a trunk group.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Trunk Group Description	Description of the trunk group, helping differentiate trunk groups.
IP trunk registration mode	• When you configure a SIP IP trunk, select **Non-registration**. • When you configure a SIP AT0 trunk, select **Trunk group registration**. • When you configure a SIP PRA trunk, select **Trunk circuit registration**.
Home domain name	Name of the domain to which the SIP trunk group belongs, such as **abcd.com**.
Registrar URI	URI address of a registration server. The value must be the same as that of **Home domain name**.
Registration account	User name for trunk group registration. This parameter is available only when you configure a SIP PRA trunk group.
Registration password	Password of a public account for trunk group registration. This parameter is available only when you configure a SIP PRA trunk group.
Confirm registration password	Password used to confirm that a correct password is entered. This parameter is available only when you configure a SIP PRA trunk group.
Transmission mode	Transport protocol used by the trunk group, including UDP (default) and TCP. For details about UDP and TCP, see **Table 2-178**.
Local media IP address	This parameter is optional and is defined in **2.18.3.3 Voice IP Address**.
Local signaling IP address	This parameter is optional and is defined in **2.18.3.3 Voice IP Address**.
Local signaling port number	Number of a local signaling port. When the same signaling IP address is used, ensure that the two port numbers (for example, the local port and the SIP server) do not conflict with each other.
Peer address type	Address type of a remote device connected to the trunk group. • **static**: When the peer address type is set to **static**, configure **Peer IP address** and **Peer port number**. • **dnsA**: When the peer address type is set to **dnsA**, configure **Peer domain name** and **Peer port number**. **NOTE** V200R010C10 and later versions support this parameter.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Peer domain name	Domain name of a remote device connected to the trunk group. **NOTE** V200R010C10 and later versions support this parameter.
Peer IP address	IP address of a remote device connected to the trunk group.
Peer port number	Port number of a remote device connected to the trunk group.
Maximum number of concurrent calls	Maximum number of concurrent calls.
Default display number	Default called number of the trunk group.
Client mode	Working mode of the trunk group for reliable connections. ● client: The trunk group functions as a client which initiates unidirectional connection requests to other devices. ● server: The trunk group functions as a server which accepts connection requests from other devices. ● client_server: The trunk group functions as a client and a server which can set up bidirectional connections. The PBX must negotiate with the remote device to obtain the client mode configuration of the remote device.
Enterprise	Enterprise to which the trunk group belongs.
Dn set	DN set to which the trunk group is bound.
Country/Area Code	Country or area code of an incoming call through the trunk group. If the incoming call does not contain a country or area code, the system automatically adds the country or area code, so that users can view the country or area code through the Calling Line Identification Presentation (CLIP) function.
Toll Call Area Code	Area code of an incoming toll call through the trunk group. If the incoming call does not contain an area code, the system automatically adds the country or area code, so that users can view the country or area code through the CLIP function.
Circuit selection mode	Circuit selection mode used by the trunk group. The value can be **Loop**, **Increase**, **Decrease**, or **Master** (controled by the user).
Outgoing call right	Outgoing call rights of the trunk group.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Call route name	Call route bound to the trunk group.
Time segment index	You need to set this parameter when the trunk group is bound to a call route using time-based routing policy. This parameter is optional and is defined in **2.18.11.2 Time Segment Index**.
Percentage	You need to set this parameter when the trunk group is bound to a call route using the routing policy with **Load percentage** specified. The unit is %.
Charging rate	You need to set this parameter when the trunk group is bound to a call route using the routing policy with **Based on charging rate** specified.
User level	You need to set this parameter when the trunk group is bound to a call route using the routing policy with **User level** specified.

NOTE

When you set **Trunk Group Name** and **Trunk Group Description**, enter character strings with spaces included in double quotation marks (""), such as, "this is an example".

2.18.7.3 AT0 Trunk Group

This section describes how to configure an AT0 trunk group to implement voice communication between PBX users and inter-office users. You can set parameters such as circuit selection mode, outgoing call right, and call route.

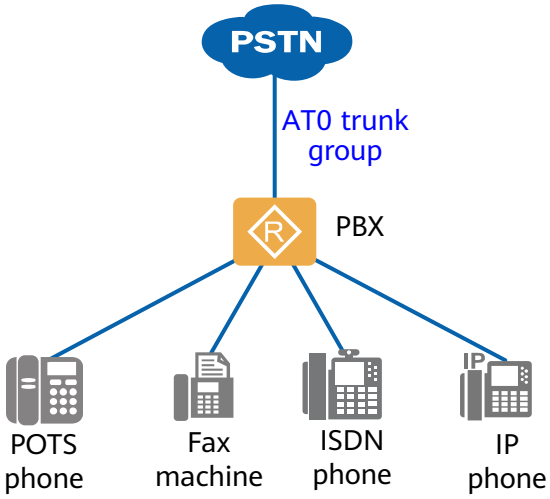
Context

Enterprises request PSTN telephone numbers of a certain number, and use common telephone lines as AT0 trunk lines so that enterprise users can share the trunk lines. Outgoing calls occupy one trunk line, and the PSTN telephone number is displayed. After calls are ended, the trunk line is released. Incoming calls reach the PBX through the AT0 trunk, and then the PBX forwards the incoming calls to a PBX user or access number of the enterprise switchboard. The trunk line use efficiency is high, and enterprises do not need to request independent PSTN telephone numbers for all enterprise employees.

The PBX connects to the PSTN through an AT0 trunk group, as shown in **Figure 2-269**.

Copyright © Huawei Technologies Co., Ltd.

Figure 2-269 AT0 trunk group networking



Prerequisites

- **Call Route** has been configured.
- **Routing Time Range Index** has been configured if you bind a trunk group to a call route using time-based routing policy.

Assessing a Page

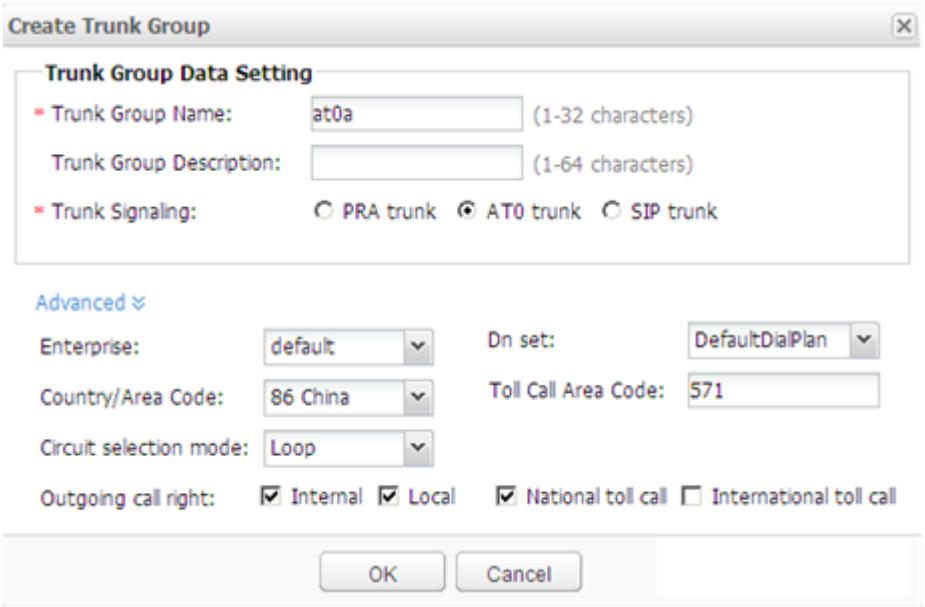
Choose **Voice Management** > **Trunk Group**.

Procedure

- Create a trunk group.
  a. Click **Create**.
  b. Select **AT0 trunk** and set parameters in the **Create Trunk Group** dialog box.
  Figure 2-270 shows the **Create Trunk Group** dialog box.

Copyright © Huawei Technologies Co., Ltd.

Figure 2-270 Create Trunk Group dialog box

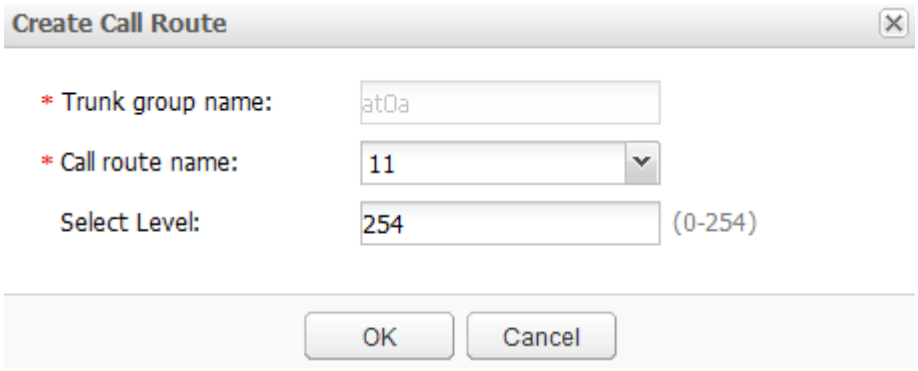


c. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.

- Modify a trunk group.
  a. Click  next to the trunk group.
  b. Set parameters in the **Modify Trunk Group** dialog box.
  c. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.
- Delete a trunk group.
  a. Select the trunk group you want to delete and click **Delete**.
  b. In the **Information** dialog box, click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.
- Create a call route.
  a. Click **Call Route** next to the trunk group.
  b. Click **Create** in the **Configure Call Route** dialog box.
  c. Select a call route in the **Create Call Route** dialog box.
  Figure 2-271 shows the **Create Call Route** dialog box.

Copyright © Huawei Technologies Co., Ltd.

Figure 2-271 Create Call Route dialog box



d. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.

- Modify a call route.
  a. Click **Call Route** next to the trunk group.
  b. Select the call route you want to modify in the **Configure Call Route** dialog box and click next to the call route.
  c. Set parameters in the **Modify Call Route** dialog box.
  d. In the **Information** dialog box, click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.
- Delete a call route.
  a. Click **Call Route** next to the trunk group.
  b. Select the call route you want to delete in the **Configure Call Route** dialog box and click **Delete**.
  c. In the **Information** dialog box, click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.

----End

Parameter Description

Parameter	Description
Trunk Group Name	Unique identifier of a trunk group.
Trunk Group Description	Description of the trunk group, helping differentiate trunk groups.
Enterprise	Enterprise to which the trunk group belongs.
Dn set	DN set to which the trunk group is bound.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Country/Area Code	Country or area code of an incoming call through the trunk group. If the incoming call does not contain a country or area code, the system automatically adds the country or area code, so that users can view the country or area code through the Calling Line Identification Presentation (CLIP) function.
Toll Call Area Code	Area code of an incoming toll call through the trunk group. If the incoming call does not contain an area code, the system automatically adds the country or area code, so that users can view the country or area code through the CLIP function.
Circuit selection mode	Circuit selection mode used by the trunk group. The value can be **Loop**, **Increase**, **Decrease**, or **Master** (controled by the user).
Outgoing call right	Outgoing call rights of the trunk group.
Call route name	Call route bound to the trunk group.
Time segment index	You need to set this parameter when the trunk group is bound to a call route using time-based routing policy. This parameter is optional and is defined in **2.18.11.2 Time Segment Index**.
Percentage	You need to set this parameter when the trunk group is bound to a call route using the routing policy with **Load percentage** specified. The unit is %.
Charging rate	You need to set this parameter when the trunk group is bound to a call route using the routing policy with **Based on charging rate** specified.
User level	You need to set this parameter when the trunk group is bound to a call route using the routing policy with **User level** specified.

NOTE

When you set **Trunk Group Name** and **Trunk Group Description**, enter character strings with spaces included in double quotation marks (""), such as, "this is an example".

2.18.8 Trunk Circuit

Trunk circuits are used to constitute a trunk group. PBX supports three trunk circuits: PRA, SIP-AT0, and AT0.

Copyright © Huawei Technologies Co., Ltd.

2.18.8.1 PRA Trunk

This section describes how to configure PRA trunks in a PRA trunk group. A PRA trunk is a digital circuit trunk and uses an E1 interface on the PBX to connect to the remote device through an E1 trunk line.

Context

A PRA trunk can use the E1 interface not the T1 interface to connect the PBX to the remote device. An E1 interface on a PRA trunk provides 32 channels which are also called timeslots. Channels 0 and 16 are signaling channels, and all the other channels are voice channels. If **Board full configuration** is set to **Yes** when you configure a PRA trunk, all the 30 voice channels of the trunk are used. If **Board full configuration** is set to **No**, only the specified voice channel of the trunk is used. After a PRA trunk is configured, you can block, restore, and release voice channels of the trunk.

The PBX can add several trunks of the same type to a trunk group, which are invoked by call routes. Even if there is only one trunk, a trunk group needs to be configured to facilitate trunk management.

Prerequisites

2.18.7.1 PRA Trunk Group has been configured.

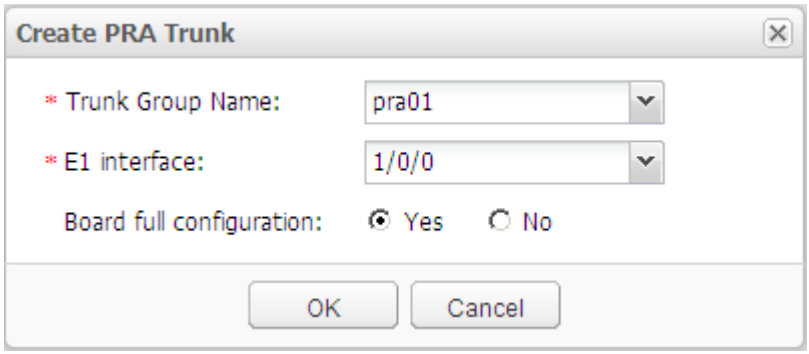
Assessing a Page

Choose **Voice Management** > **Trunk Circuit** > **PRA Trunk**.

Procedure

- Create a trunk.
  a. Click **Create**.
  b. Set parameters in the **Create PRA Trunk** dialog box.
  Figure 2-272 shows the **Create PRA Trunk** dialog box.

  Figure 2-272 Create PRA Trunk dialog box



  c. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.

Copyright © Huawei Technologies Co., Ltd.

- Delete a trunk.
  a. Select the trunk you want to delete and click **Delete**.
  b. In the **Information** dialog box, click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.
- Manage voice channels.
  a. Click  next to the trunk group.
  b. Select the target channel in the **PRA Trunk Circuit Timeslot Status List** dialog box to manage the channel.
     You can perform either of the following operations on a voice channel.
     - Switch Status: Block a channel that is in **normal** state or restore a channel from the **block** state to **normal** state.
     - Release Channel: Release the channel of the trunk.
  c. Click **OK** to return to the **PRA Trunk List** window.

----End

Parameter Description

Parameter	Description
Trunk Group Name	Name of the trunk group to which the PRA trunk belongs.
E1 interface	Physical interface on the PRA trunk. The interface number is in the format of slot ID/subcard ID/interface sequence number.
Board full configuration	If you want to use all the 30 voice channels (channels 1 to 15, and 17 to 31) on the E1 interface, select **Yes**. If you want to use specified voice channels on the E1 interface only, select **No**.
Start channel	Start voice channel on the E1 interface that is added to the PRA trunk. This parameter is available when **Board full configuration** is set **No**.
Number of channels	Number of voice channels on the E1 interface that are added to the PRA trunk. This parameter is available when **Board full configuration** is set **No**.

2.18.8.2 SIP AT0 Trunk

This section describes how to configure SIP AT0 trunks in a SIP AT0 trunk group. A SIP AT0 trunk connects SIP users on the PBX to the carrier network and registers the number of each SIP user separately.

 Copyright © Huawei Technologies Co., Ltd.

Context

After an enterprise applies for SIP users from the carrier network such as the IMS network, the SIP users are separately registered on the carrier network. Then trunks of the SIP AT0 trunk group are formed.

The PBX can add several trunks of the same type to a trunk group, which are invoked by call routes. Even if there is only one trunk, a trunk group needs to be configured to facilitate trunk management.

Prerequisites

- 2.18.7.2 SIP Trunk Group has been configured.
- The format of the user name for user authentication has been configured. For details, see the *Configuring a SIP AT0 Trunk Group* of *CLI-based Configuration*.

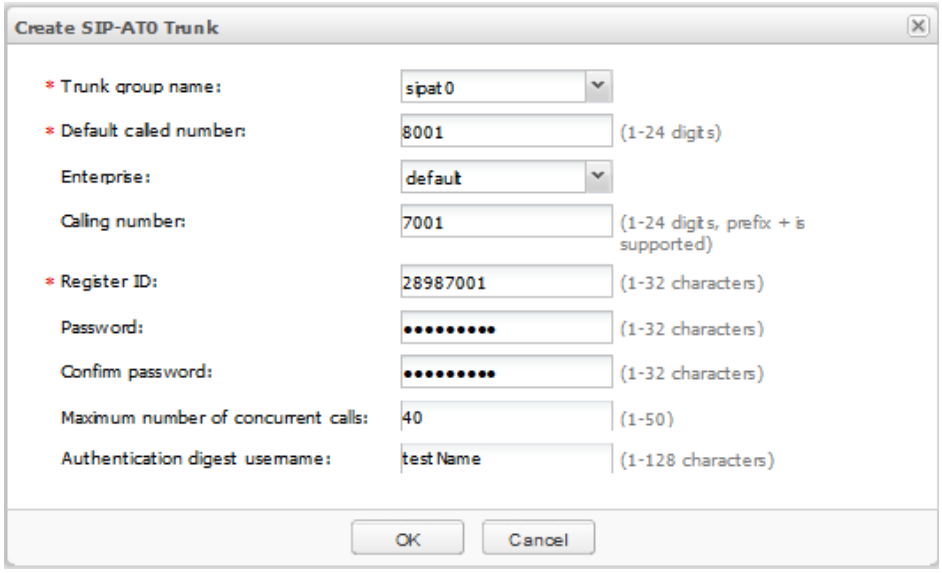
Assessing a Page

Choose **Voice Management** > **Trunk Circuit** > **SIP-AT0 Trunk**.

Procedure

- Create a trunk.
  a. Click **Create**.
  b. Set parameters in the **Create SIP-AT0 Trunk** dialog box.
  Figure 2-273 shows the **Create SIP-AT0 Trunk** dialog box.

  Figure 2-273 Create SIP-AT0 Trunk dialog box



NOTE

V200R010C10 and later versions support the configuration of **Authentication digest username**.

Copyright © Huawei Technologies Co., Ltd.

c. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.

- Modify a trunk.
  a. Click  next to the trunk.
  b. Set parameters in the **Modify SIP-AT0 Trunk** dialog box.
  c. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.
- Delete a trunk.
  a. Select the trunk you want to delete and click **Delete**.
  b. In the **Information** dialog box, click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.

----End

Parameter Description

Parameter	Description
Trunk group name	Name of the trunk group to which the SIP-AT0 trunk belongs.
Default called number	Specify whether an incoming call is transmitted over the trunk to an intra-office user (dedicated access) or access number of the switchboard (switchboard access).
Enterprise	Name of the enterprise to which a calling number belongs.
Calling number	Calling number of an outgoing call transmitted over the trunk.
Register ID	Trunk identifier, that is the user name used for registration. **NOTE** If spaces are used, include the string with spaces in double quotation marks (""), such as, "this is an example".
Password	Password used for trunk registration.
Confirm password	Password used to confirm that a correct password is entered.
Maximum number of concurrent calls	Maximum number of concurrent calls.
Authentication digest username	Authentication digest user name. **NOTE** V200R010C10 and later versions support this parameter.

Copyright © Huawei Technologies Co., Ltd.

2.18.8.3 AT0 Trunk

This section describes how to configure AT0 trunks in the AT0 trunk group. An AT0 trunk is an analog circuit trunk and it uses an FXO interface to connect to Public Switch Telephone Network (PSTN) through a common telephone line.

Context

AT0 trunks must have voice cards such as 4FXS1FXO and 4FXO installed to provide FXO interfaces.

The PBX can add several trunks of the same type to a trunk group, which are invoked by call routes. Even if there is only one trunk, a trunk group needs to be configured to facilitate trunk management.

Prerequisites

2.18.7.3 AT0 Trunk Group has been configured.

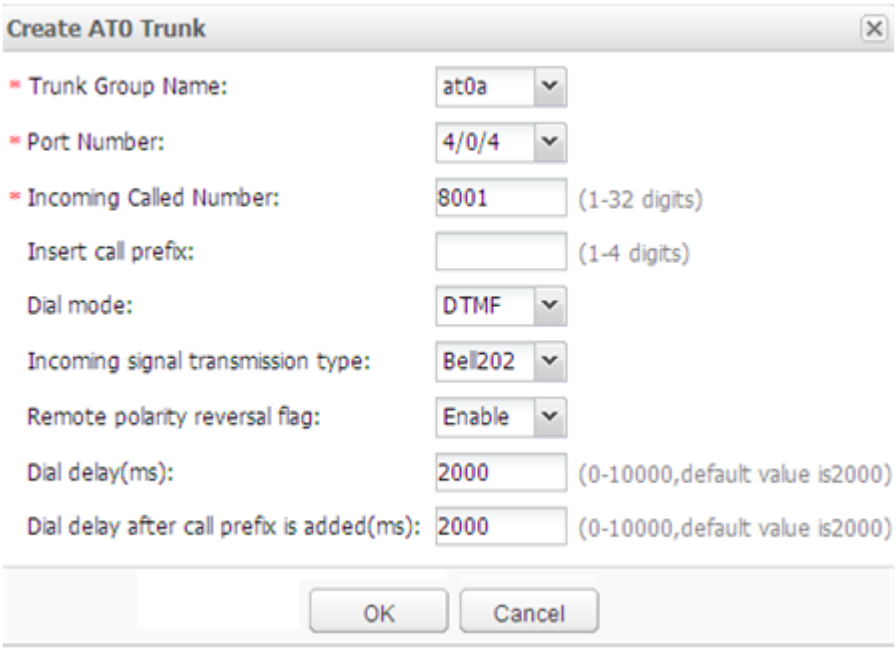
Assessing a Page

Choose **Voice Management** > **Trunk Circuit** > **AT0 Trunk**.

Procedure

- Create a trunk.
  a. Click **Create**.
  b. Set parameters in the **Create AT0 Trunk** dialog box.
  Figure 2-274 shows the **Create AT0 Trunk** dialog box.

Figure 2-274 Create AT0 Trunk dialog box



 Copyright © Huawei Technologies Co., Ltd.

c. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.

- Modify a trunk.
  a. Click  next to the trunk.
  b. Set parameters in the **Modify AT0 Trunk** dialog box.
  c. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.
- Delete a trunk.
  a. Select the trunk you want to delete and click **Delete**.
  b. In the **Information** dialog box, click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.

----End

Parameter Description

Parameter	Description
Trunk Group Name	Name of the trunk group to which the AT0 trunk belongs.
Port Number	Number of the trunk's FXO physical interface, in the format of slot ID/subcard ID/interface sequence number.
Incoming Called Number	Specify whether an incoming call is transmitted over the trunk to an intra-office user (dedicated access) or access number of the switchboard (switchboard access).
Insert call prefix	Call prefix inserted to outgoing calls routed through the trunk.
Dial mode	The available dial modes are: ● DTMF: dual tone multiple frequency (default) ● PULSE: pulse dialing **NOTICE** If **Dial mode** is set to **PULSE**, run the **pbx number-parameter** command in the voice view on the CLI to change the value of control point 40 to 5 after completing the configuration of the AT0 trunk. If this control point value is not changed, pulse dialing fails on the AT0 trunk.
Incoming signal transmission type	Signal transmission type for the CLIP service. Set the signal transmission type based on the requirements of the remote end.
Remote polarity reversal flag	Whether polarity reversal detection is activated. Polarity reversal detection is used to implement instant accounting. The trunk notifies the accounting terminal of the accounting starting point and stop point using polarity reversal during a conversation or when the conversation ends. Select **Disable** when polarity reversal detection is not activated at the remote end.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Dial delay(ms)	Maximum dial interval. If no digit is entered after the maximum dial interval expires, the PBX sends the previously entered digits out.
Dial delay after call prefix is added(ms)	Dial delay after a call prefix is inserted by the AT0 trunk.

2.18.9 Enterprise CRBT

This topic describes the enterprise CRBT file management and CRBT configuration.

Enterprise CRBT is a piece of music or sound customized by an enterprise. After an enterprise registers the CRBT service, the user can set different CRBTs for a calling party or a group of calling parties in different periods.

2.18.9.1 CRBT File Management

This topic describes how to manage the enterprise CRBT file.

Prerequisites

- The CRBT service has been enabled. For details, see **2.18.3.2 Enterprise and DN Set**.
- **Voice File Upload** has been configured.
- The CRBT configurations have been deleted if you want to delete the CRBT file. For details, see **2.18.9.2 CRBT Configuration**.

Accessing Configuration Pages

Choose **Voice Management** > **Enterprise CRBT** > **CRBT File Management**.

Procedure

- Create a CRBT file.
  a. Click **Create**.
  b. In the **Create CRBT file** dialog box, set parameters.
  Figure 2-275 shows the parameter settings.

  Figure 2-275 Creating a CRBT file



 Copyright © Huawei Technologies Co., Ltd.

c. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.

- Modify the CRBT file.
  a. In the **Operation** column of the CRBT to modify, click  .
  b. In the **Modify CRBT File** dialog box, set parameters.
  c. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.
- Delete the enterprise CRBT.
  a. Select the CRBT to delete, and click **Delete**.
  b. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.

----End

Parameter Description

Parameter	Description
Select a CRBT file	Specifies the CRBT file.
CRBT description	Specifies the CRBT file description.
Enterprise description	Specifies the enterprise for using the CRBT file.

2.18.9.2 CRBT Configuration

This topic describes how to configure the enterprise ring-back-tone (CRBT).

Prerequisites

- The CRBT service has been enabled. For details, see **2.18.3.2 Enterprise and DN Set**.
- **Voice File Upload** has been configured.

Accessing Configuration Pages

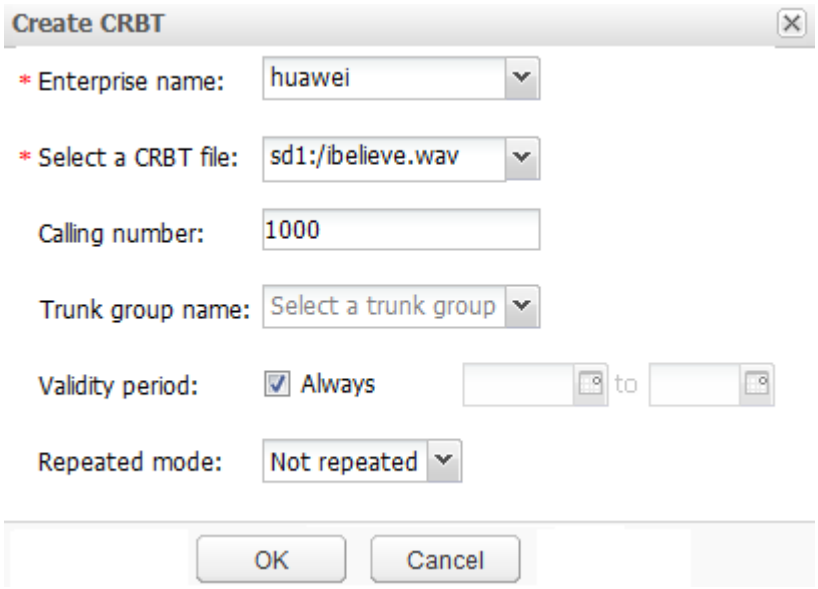
Choose **Voice Management** > **Enterprise CRBT** > **CRBT Configuration**.

Procedure

- Create a CRBT.
  a. Click **Create**.
  b. In the **Create CRBT** dialog box, set parameters.
  Figure 2-276 shows the parameter settings.

Copyright © Huawei Technologies Co., Ltd.

Figure 2-276 Creating a CRBT



c. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.

- Modify the enterprise CRBT.
  a. In the **Operation** column of the CRBT to modify, click .
  b. In the **Modify CRBT** dialog box, set parameters.
  c. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.
- Delete the enterprise CRBT.
  a. Select the CRBT to delete, and click **Delete**.
  b. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.

----End

Parameter Description

Parameter	Description
Enterprise description	Specifies the enterprise for using the CRBT file.
Select a CRBT file	Specifies the CRBT file.
Calling number	Specifies the calling number to which the CRBT is played. By default, the CRBT is played to all calling numbers.
Trunk group name	Specifies the trunk name.
Validity period	Specifies the validity period of the CRBT. If the default value is used, the CRBT is always valid.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Repeated mode	Specifies the repetition mode of the CRBT within the validity period, including not repeat, manual, monthly, weekly, and daily.

2.18.10 IVR

IVR refers to the interactive voice response (IVR) service. When there is an incoming call dialing the access code of an IVR service after the service is configured, the user is prompted to directly dial the extension number or listen to the next prompt tone.

Context

Before configuring the IVR service, complete the following operations:

- **Voice File Upload**
- **Voice Resource**
- **IVR Time Segment Index**

After **IVR Configuration** or the **Script Resource** configuration is completed, perform the task of **Prefix Configuration**. When configuring IVR prefixes, select the corresponding **service name**. Then users can hear the tone after dialing an IVR prefix.

NOTE

When configuring IVR prefixes, associate **service name** with the voice file configured in **IVR Configuration** or **Script Resource** to ensure that the value of **service name** is the same as that configured in **IVR Configuration** or **Script Resource**.

2.18.10.1 Voice Resource

Voice resources include menu voice files and welcome voice files that are used for the IVR switchboard to display prompt tones.

Context

A voice file must be in the WAV format and cannot be larger than 480 KB.

Prerequisites

- The voice file has been recorded. For details, see **CLI-based Configuration** > **Configuration Guide - Voice** > **PBX Configuration** > **Advanced Configuration** > **Recording and Switching a Phone System Announcement**.
- **2.18.12 Voice File Upload** has been configured.

Accessing a Page

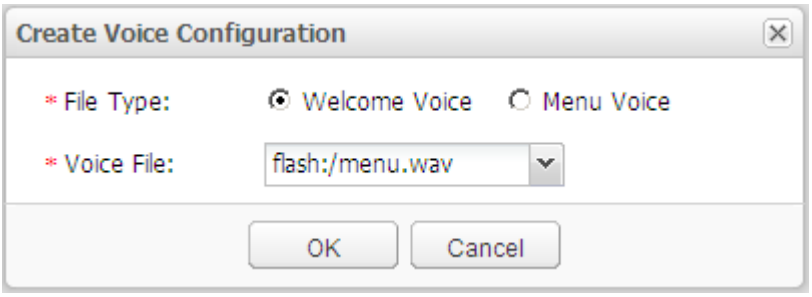
Choose **Voice Management** > **IVR** > **Voice Resource**.

Copyright © Huawei Technologies Co., Ltd.

Procedure

- Create a voice file.
  a. Click **Create**.
  b. Set parameters in the **Create Voice Configuration** dialog box.
  [Figure 2-277](#) shows the **Create Voice Configuration** dialog box.

  Figure 2-277 Create Voice Configuration dialog box



  c. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.
- Download a voice file.
  a. Click  next to the voice file.
  b. In the **File Download** dialog box, click **Save** to save the voice file to the local computer.
- Delete a voice file.
  a. Select the voice file to be deleted, and click **Delete**.
  b. In the **Information** dialog box, click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.

NOTICE

It takes one minute to release an IVR prompt tone. Therefore, after a voice file is deleted, you need to wait at least one minute to reconfigure the voice file.

----End

Parameter Description

Parameter	Description
File Type	Type of the voice file.
Voice File	Whether a voice file functions as a **Welcome Voice** or **Menu Voice**.

Copyright © Huawei Technologies Co., Ltd.

2.18.10.2 IVR Time Segment Index

The IVR time segment index is used to specify the available time of the IVR switchboard.

Context

To use the IVR switchboard in a specified time segment, you can associate the IVR time segment index. IVR time segment can be configured using the day, date, time, and holiday.

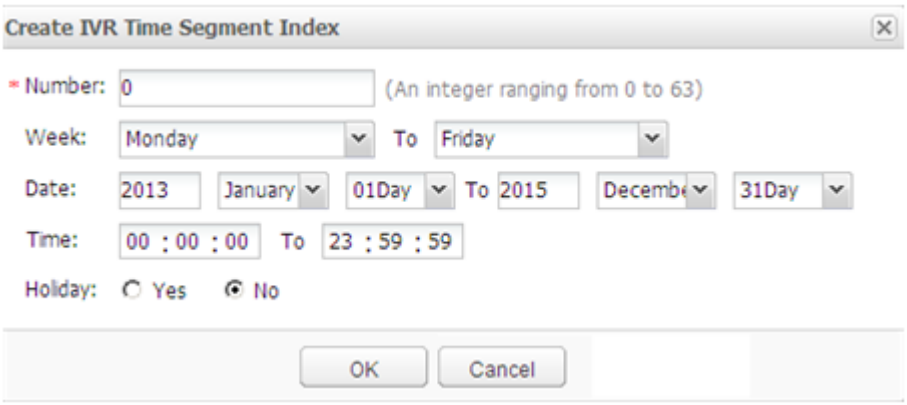
Accessing a Page

Choose **Voice Management** > **IVR** > **IVR Times Segment Index**.

Procedure

- Create an IVR time segment index.
  a. Click **Create**.
  b. Set parameters in the **Create IVR Time Segment Index** dialog box. Figure 2-278 shows the **Create IVR Time Segment Index** dialog box.

  Figure 2-278 Create IVR Time Segment Index dialog box

  c. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.
- Modify an IVR time segment index.
  a. Click next to the IVR time segment index.
  b. Set parameters in the **Change IVR Time Segment Index** dialog box.
  c. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.
- Delete an IVR time segment index.
  a. Select the IVR time segment index to be deleted, and click **Delete**.
  b. In the **Information** dialog box, click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.

----End

Copyright © Huawei Technologies Co., Ltd.

Parameter Description

Parameter	Description
Number	-
Week	IVR time segment is configured using the day. ● When both the start day and end day are **none**, the IVR switchboard is available on all days. ● When the start day is **none**, the current day must be the end day or earlier than the end day. ● When the end day is **none**, the current day must be the start day or later than the start day. ● When the start day is the end day, the IVR switchboard is available only on the day. ● When the start day is later than the end day, the IVR switchboard is available between the two days. For example, the start day is **Saturday** and the end day is **Monday**, the IVR switchboard is available on Saturdays, Sundays, and Mondays.
Date	IVR time segment is configured using the date. ● If no date is specified, the IVR switchboard usage is not restricted by the date. ● The end date must be later than the start date.
Time	IVR time segment is configured using the time. ● When the default values are used, the IVR switchboard usage is not restricted by the time. ● The end time must be later than the start time.
Holiday	When multiple time segments conflict with each other: ● When **Yes** is selected, the time segment index is used by default. ● When **No** is selected, the time segment index configured first is used.

2.18.10.3 IVR Configuration

The interactive voice response (IVR) service allows enterprises to customize their IVR menus and prompt tones, improving the user experience.

Context

The IVR service provides IVR menu and prompt tone customization functions. When an external line calls the switchboard number, the device uses IVR to provide services to the external line, such as transferring the call or playing the prompt tone.

Copyright © Huawei Technologies Co., Ltd.

Prerequisites

2.18.10.1 Voice Resource has been configured.

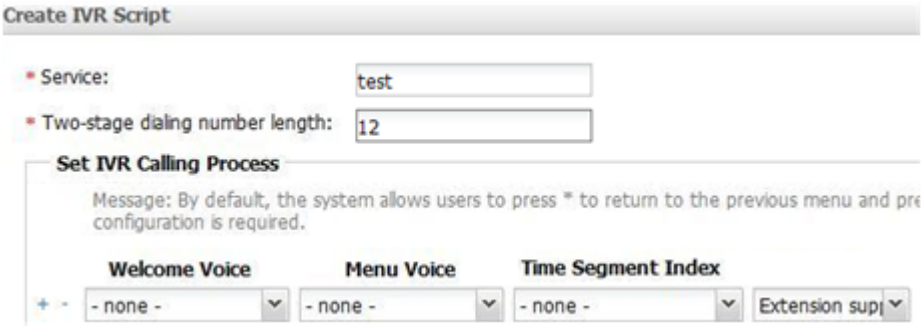
Accessing a Page

Choose **Voice Management** > **IVR** > **IVR Configuration**.

Procedure

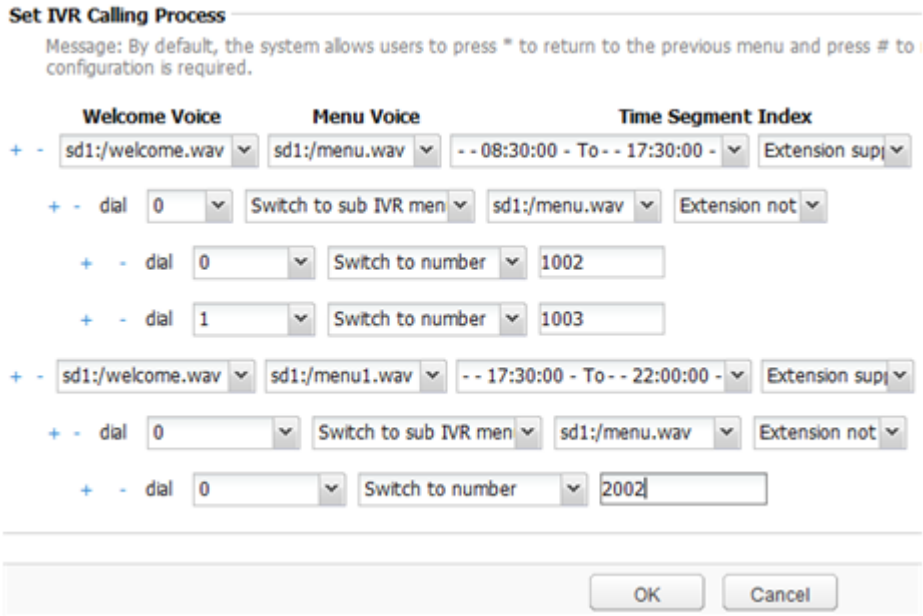
- Create an IVR script.
  a. Click **Create**.
  b. Set parameters in the **Create IVR Script** dialog box.
  Figure 2-279 shows the **Create IVR Script** dialog box.

  Figure 2-279 Create IVR Script dialog box



  c. In the **Set IVR Calling Process** area, click **Create Self-Defined Voice** to configure the IVR calling process.
  Figure 2-280 shows the **Set IVR Calling Process** area.

  Figure 2-280 Set IVR Calling Process area



 Copyright © Huawei Technologies Co., Ltd.

NOTE

- You can configure a maximum of three time segments for an IVR calling process.
- You can click **+** before an IVR calling process to add a process of the same level, or click **-** to delete a process of the same level.
- When multiple time segments configured for IVR calling processes overlap, the system preferentially enters the process with the time segment configured as holiday. If the **Holiday** parameters for the time segments are the same, the system preferentially enters the process with the time segment that has a smaller value of **Name**. For example, if the value of **Name** for one time segment is **0** and that for another time segment is **1**, the system preferentially enters the process with the name of **Name** being **0**.

d. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.

- Modify an IVR script.
  a. Click  next to the IVR script.
  b. In the **Modify IVR Script** dialog box, set parameters or modify an IVR calling process.
  c. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.
- Download an IVR script.
  a. Click **Script Download** next to the IVR script.
  b. In the **File Download** dialog box, click **Save** to save the IVR script to the local computer.
- Delete an IVR script.
  a. Select the IVR script to be deleted, and click **Delete**.
  b. In the **Information** dialog box, click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.

----End

Parameter Description

Parameter	Description
Service	The value of this parameter is the same as that of **Service** for the IVR prefix. This parameter is used for associating the announcement file during IVR prefix configuration.
Two-stage dialing number length	Two-stage dialing number length.
Extension supported	If you have configured **Extension supported** in the IVR menu, you can directly dial a user extension number (for example, user 6000). If you have configured **Extension not supported** in the IVR menu, you can dial a number only following the dialing rule provided by the menu, for example, dialing **0** and dialing user number 1002 as prompted.

Copyright © Huawei Technologies Co., Ltd.

2.18.10.4 Script Resource

You can directly upload scripts instead of configuring IVR scripts.

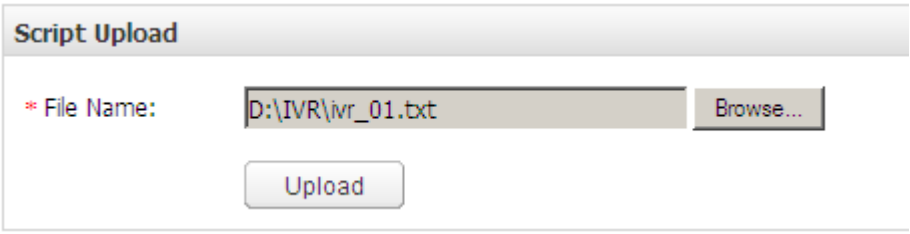
Accessing a Page

Choose **Voice Management** > **IVR** > **Script Resource**.

Procedure

- Upload a script file.
  a. In the **Script Upload** area, click **Browse...** to select the script file to be uploaded.
  b. Click **Upload**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.
  Figure 2-281 shows the **Script Upload** area.

  Figure 2-281 Script Upload area

- Download a script file.
  a. Click  next to the script file.
  b. In the **File Download** dialog box, click **Save** to save the script file to the local computer.
- Delete a script file.
  a. Select the script file to be deleted, and click **Delete**.
  b. In the **Information** dialog box, click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.

----End

2.18.11 Advanced Configuration

The advanced configuration includes the number change, routing time segment index, and number mapping.

2.18.11.1 Number Change

Number change plans includes the calling number discrimination plan, pre-routing number change plan, and post-routing number change plan.

 Copyright © Huawei Technologies Co., Ltd.

Context

Calling Number Discrimination Plan

You can configure calling number discrimination plans to change calling or called numbers to new numbers for outgoing calls.

- If the calling number needs to be displayed as a specified number, change the calling number to a new number.
- If the called number needs to be changed, change the called number to a new number.

Pre-routing Number Change Plan

The pre-routing number change plan changes a calling or called number before route selection.

You can configure pre-routing number change plans to provide various dialing modes and change the calling number displayed on the called party's phone. For example, a POTS subscriber (using the number 28761000) connected to a PBX makes a local call (the called number is 28961000) by dialing 928961000. The configured call prefix for outgoing calls is 2896. Therefore, a pre-routing number change plan needs to be configured to remove 9 from the called number. You can use pre-routing number change plans to delete the call prefix for the device to correctly locate the called party. After number analysis, the calling or called number is changed before route selection. Second-time number analysis is performed and the two-stage dial tone is played after number change.

Post-routing Number Change

The post-routing number change plan changes a calling or called number after route selection.

You can configure post-routing number change plans to provide various dialing modes and change the calling number displayed on the called party's phone. A post-routing number change plan can change a called number to a long number to ensure that it complies with the required number format. For example, a POTS subscriber (using the number 7000) connected to a PBX makes a national toll call by dialing 057128980000. A post-routing number change plan adds 12523 to the called number 057128980000. 12345 is the call prefix defined by the carrier for the enterprise. When the carrier's device detects the call prefix 12345, it connects the outgoing call through the matching trunk. This reduces the call fees of the enterprise. You can use post-routing number change plans to delete the call prefix for the device to correctly locate the called party.

Accessing a Page

Choose **Voice Management** > **Advanced Configuration** > **Number Change**.

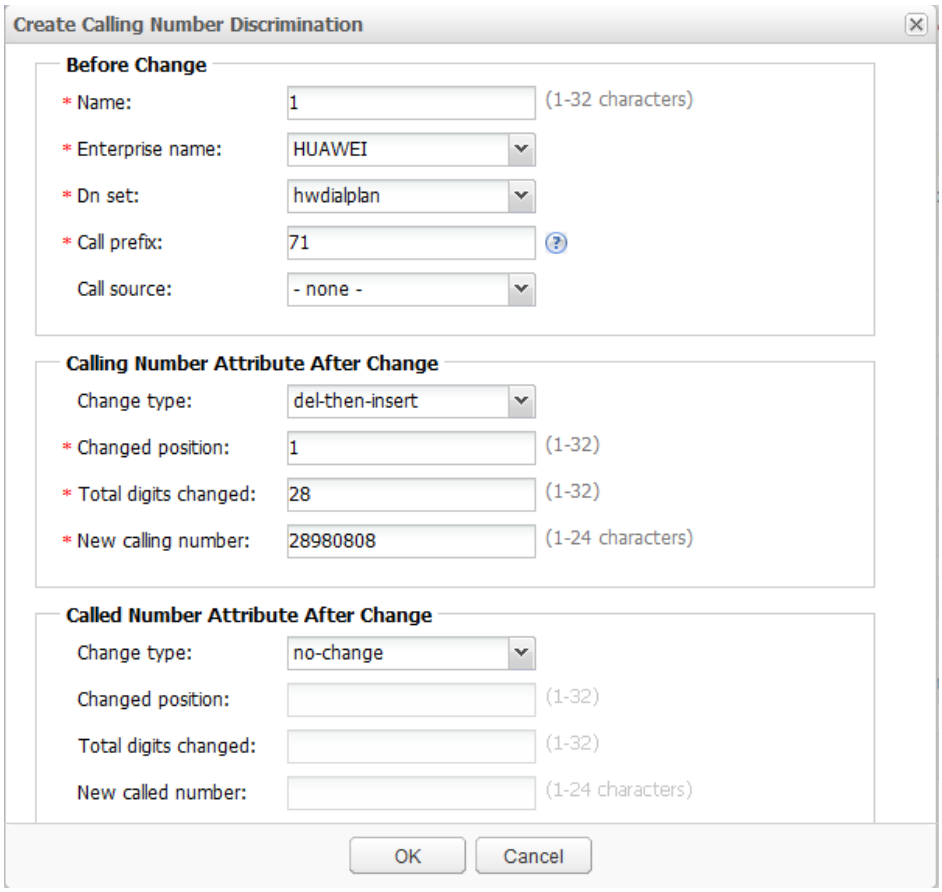
Procedure

- Create a calling number discrimination plan.
  a. In the **Calling Number Discrimination List** area, click **Create**.
  b. Set parameters in the **Create Calling Number Discrimination** dialog box.

     Figure 2-282 shows the **Create Calling Number Discrimination** dialog box.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-282 Create Calling Number Discrimination dialog box



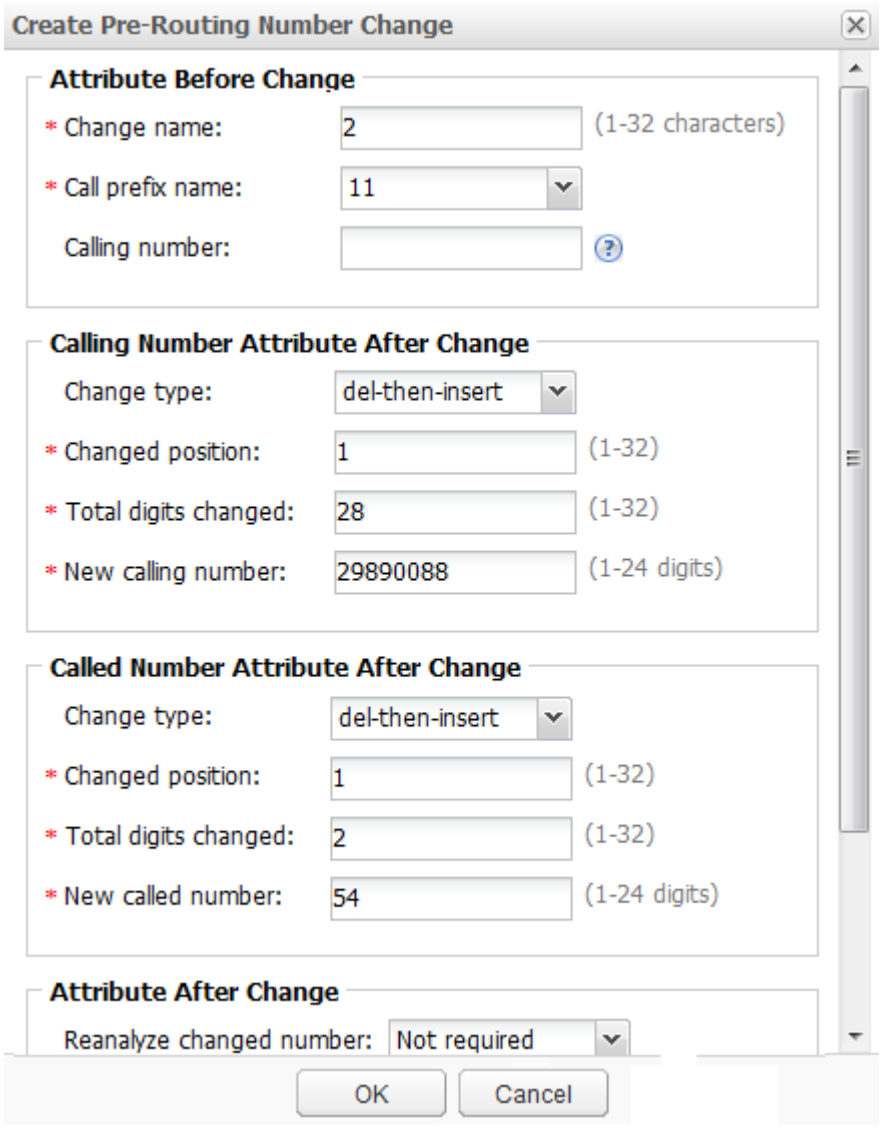
c. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.

- Modify a calling number discrimination plan.
  a. Click  next to the calling number discrimination plan.
  b. Set parameters in the **Modify Calling Number Discrimination** dialog box.
  c. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.
- Delete a calling number discrimination plan.
  a. Select the calling number discrimination plan to be deleted, and click **Delete**.
  b. In the **Information** dialog box, click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.
- Create a pre-routing number change plan.
  a. In the **Pre-Routing Number Change List** area, click **Create**.
  b. Set parameters in the **Create Pre-Routing Number Change** dialog box.

  Figure 2-283 shows the **Create Pre-Routing Number Change** dialog box.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-283 Create Pre-Routing Number Change dialog box



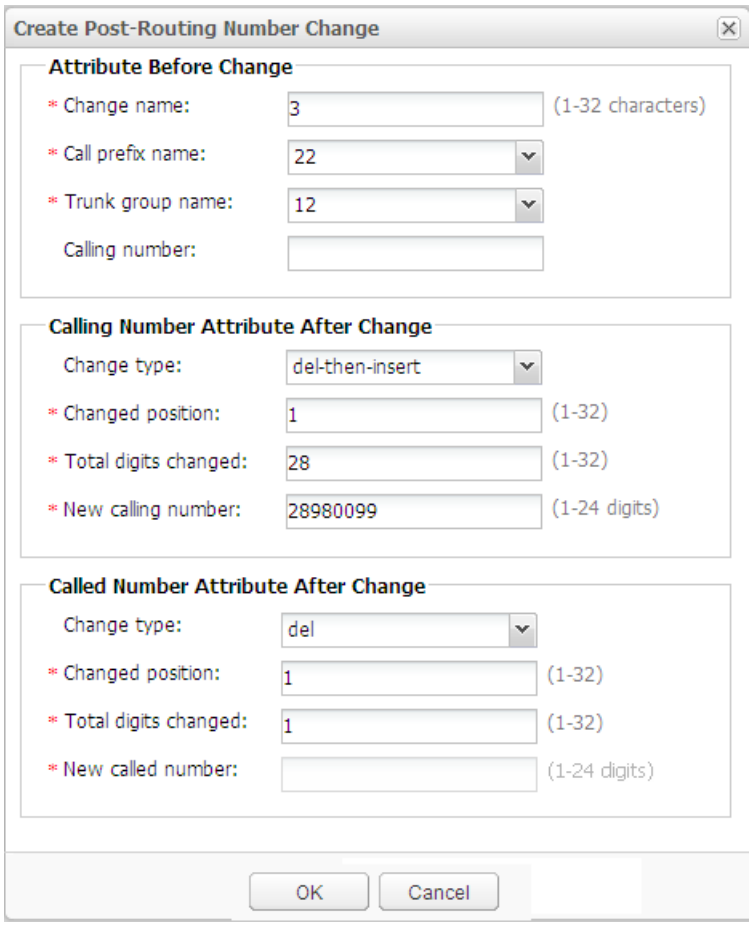
c. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.

- Modify a pre-routing number change plan.
  a. Click  next to the pre-routing number change plan.
  b. Set parameters in the **Modify Pre-Routing Number Change** dialog box.
  c. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.
- Delete a pre-routing number change plan.
  a. Select the pre-routing number change plan to be deleted, and click **Delete**.
  b. In the **Information** dialog box, click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

- Create a post-routing number change plan.
  a. In the **Post-Routing Number Change List** area, click **Create**.
  b. Set parameters in the **Create Post-Routing Number Change** dialog box.
  Figure 2-284 shows the **Create Post-Routing Number Change** dialog box.

  Figure 2-284 Create Post-Routing Number Change dialog box



  c. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.
- Modify a post-routing number change plan.
  a. Click  next to the post-routing number change plan.
  b. Set parameters in the **Modify Post-Routing Number Change** dialog box.
  c. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.
- Delete a post-routing number change plan.
  a. Select the post-routing number change plan to be deleted, and click **Delete**.

 Copyright © Huawei Technologies Co., Ltd.

b. In the **Information** dialog box, click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.

----End

Parameter Description

Parameter	Description
Name	Name used to uniquely identify the calling number discrimination plan.
Enterprise name	Name of the enterprise that the calling number discrimination plan is applied to. Select an enterprise from the drop-down list box.
Dn set	DN set that the calling number discrimination plan is applied to. Select a DN set from the drop-down list box.
Call prefix	Call prefix.
Call source	Name of the call source that the calling number discrimination plan is applied to. Select an enterprise from the drop-down list box.
Change type	Change type of the calling number. You can change, delete, or insert digits into the calling number, or do not change the calling number.
Changed position	Number change start point.
Total digits changed	Length of digits that need to be replaced or deleted when you change or delete digits in the calling number.
New calling number	• When digits in the calling number are changed, the digit change range is determined by the number change start point and number change length. You can replace digits in the range with a new number. • When digits are inserted into the calling number, the insertion start point is determined by the number change start point. You can insert a new number in the insertion start point of the original number.
Change type	Change type of the called number. You can change, delete, or insert digits into the calling number, or do not change the called number.
Changed position	Number change start point.
Total digits changed	Length of digits that need to be replaced or deleted when you change or delete digits in the called number.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
New called number	• When digits in the called number are changed, the digit change range is determined by the number change start point and number change length. You can replace digits in the range with a new number. • When digits are inserted into the called number, the insertion start point is determined by the number change start point. You can insert a new number in the insertion start point of the original number.
Change name	Name used to uniquely identify the pre-routing number change plan.
Call prefix name	Call prefix bound to the pre-routing number change plan.
Calling number	Calling number that needs to be changed before route selection.
Reanalyze changed number	-
Play two-stage dial tone	-
New enterprise name	Indicates the new enterprise name after pre-routing number change.
Dn Set	Name of the DN Set of the new enterprise.
Change name	Name used to uniquely identify the post-routing number change plan.
Call prefix name	Call prefix bound to the post-routing number change plan.
Trunk group name	Trunk group bound to the post-routing number change plan.
Calling number	Calling number that needs to be changed after route selection.

2.18.11.2 Time Segment Index

The device uses the time-based routing policy to select different routes for outgoing calls based on the time segment. Time segment indexes indicate different time segments. You can associate the time segment index with routes or with trunk groups.

Accessing a Page

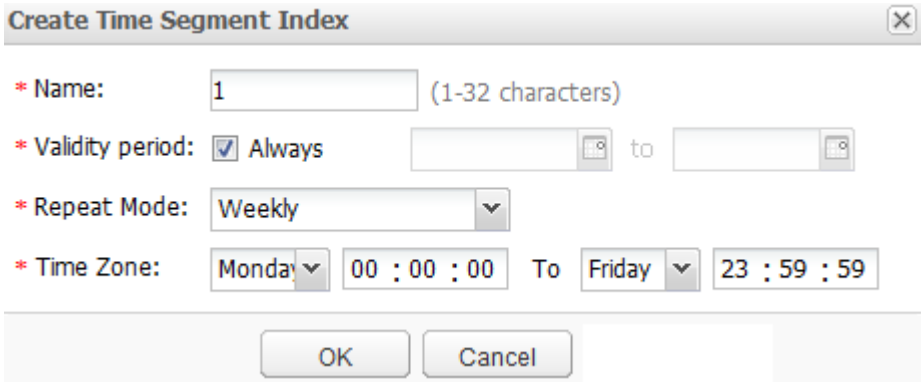
Choose **Voice Management** > **Advanced Configuration** > **Time Segment Index**.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

- Create a time segment index.
  a. Click **Create**.
  b. Set parameters in the **Create Time Segment Index** dialog box.
  Figure 2-285 shows the **Create Time Segment Index** dialog box.

  Figure 2-285 Create Time Segment Index dialog box



  c. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.
- Modify a time segment index.
  a. Click  next to the time segment index.
  b. Set parameters in the **Modify Time Segment Index** dialog box.
  c. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.
- Delete a time segment index.
  a. Select the time segment index to be deleted, and click **Delete**.
  b. In the **Information** dialog box, click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.

----End

Parameter Description

Parameter	Description
Name	Unique index used to identify the time segment.
Validity period	Specifies the validity period of the Time Segment. If the default value is used, the Time Segment is always valid.
Repeat Mode	Select the repeat mode of the time segment from the drop-down list box.
Time Zone	Time period of the time segment.

Copyright © Huawei Technologies Co., Ltd.

2.18.11.3 Number Mapping

You can configure a number mapping for subscribers without long numbers. For an incoming call, the device maps the external number to an internal number, analyzes the number, and locate the called party according to the matched prefix.

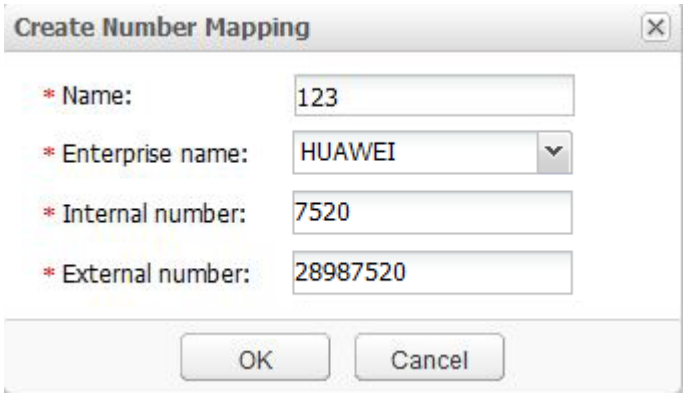
Accessing a Page

Choose **Voice Management** > **Advanced Configuration** > **Number Mapping**.

Procedure

- Create a number mapping.
  a. Click **Create**.
  b. Set parameters in the **Create Number Mapping** dialog box.
  Figure 2-286 shows the **Create Number Mapping** dialog box.

  Figure 2-286 Create Number Mapping dialog box



  c. Click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.
- Delete a number mapping.
  a. Select the number mapping to be deleted, and click **Delete**.
  b. In the **Information** dialog box, click **OK**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.

----End

Parameter Description

Parameter	Description
Name	Unique index used to identify the number mapping.
Enterprise name	Name of the enterprise that the number mapping is applied to. Select an enterprise from the drop-down list box.
Internal number	Private number.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
External number	Long number.

2.18.12 Voice File Upload

You can upload voice files to the device for IVR voice and Ring Back Tone (RBT) services.

Accessing a Page

Choose **Voice Management** > **Voice File Upload**.

Procedure

Step 1 Click **Browse...** to select the voice file directory (for example, D:\VOICE).

Figure 2-287 shows the **Uploading a voice file**.

Figure 2-287 Uploading a voice file



Step 2 Click **Upload**. A dialog box is displayed, indicating that the operation succeeds. Click **OK**.

----End

2.19 System Management

2.19.1 Upgrade and Maintenance

2.19.1.1 Restarting the Device

Context

After the system is upgraded or when the device configuration is changed, restart the device to make the new configuration take effect. You are advised to save the current configuration and back up the current configuration file before restarting

 Copyright © Huawei Technologies Co., Ltd.

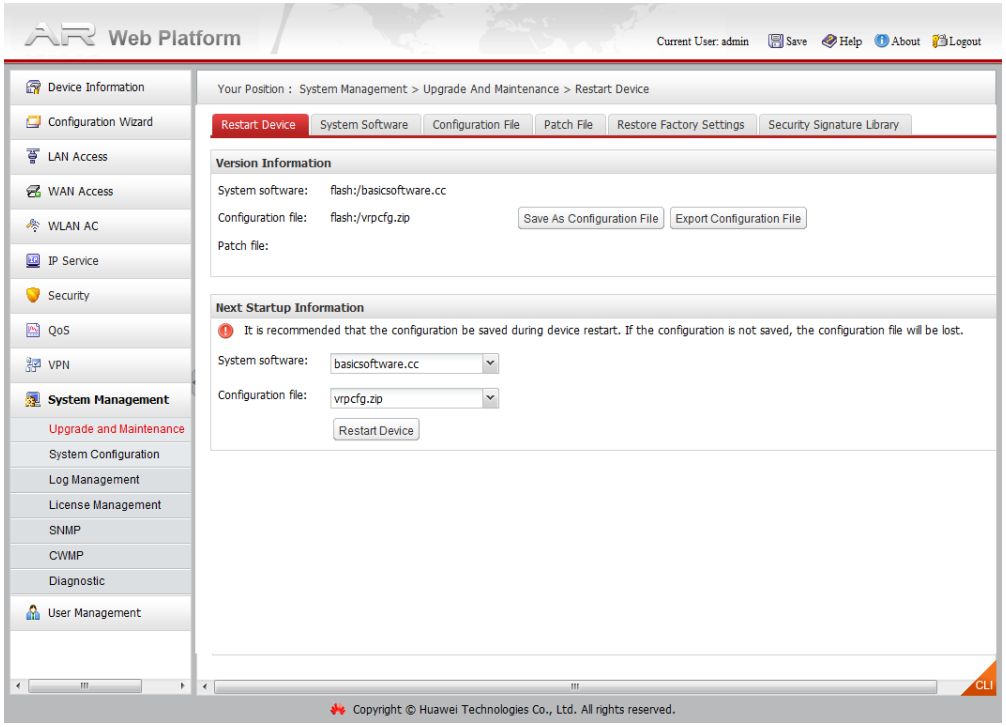
the system. Ensure that the system software of the standby MPU is the same as that of the active MPU before restarting the device with active and standby MPUs.

Procedure

Step 1 Click **Save** to save the current configuration.

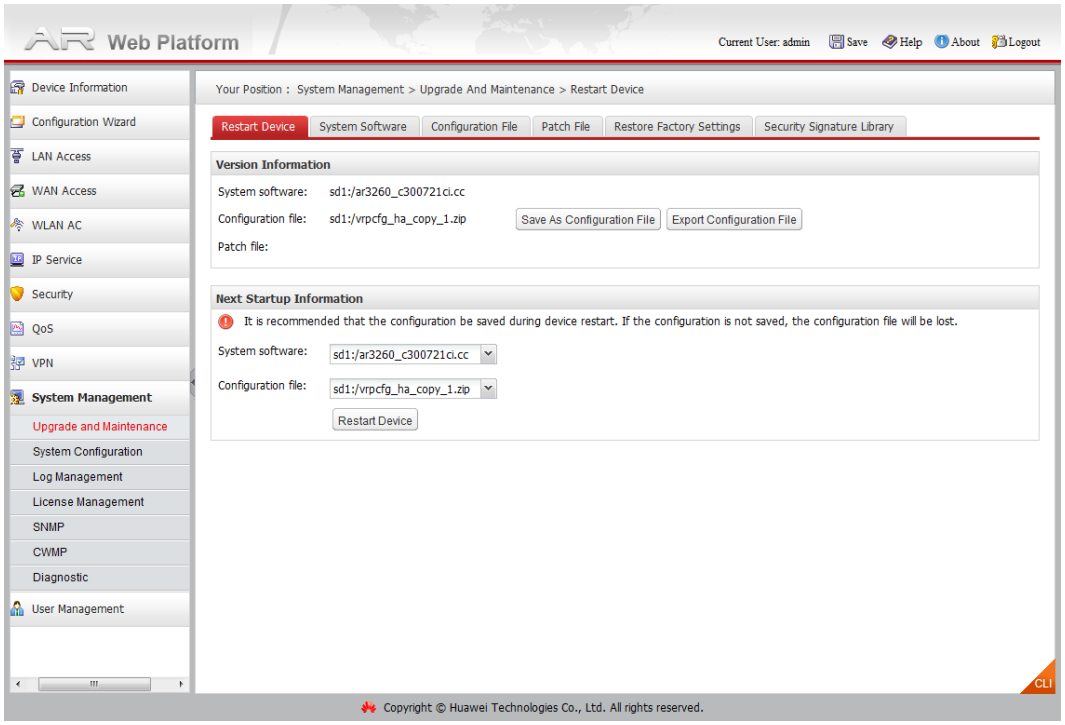
Step 2 Choose **System Management** > **Upgrade and Maintenance** > **Restart Device**, as shown in **Figure 2-288** and **Figure 2-289**.

Figure 2-288 Restart Device page



 Copyright © Huawei Technologies Co., Ltd.

Figure 2-289 Restart page of the device with active and standby MPUs



Step 3 Click **Save As Configuration File** to back up the configuration file to the storage device of the router.

Step 4 Click **Export Configuration File** to back up the configuration file to the local PC.

Step 5 Set **System software** to specify the system software to use during the next startup.

Step 6 Set **Configuration file** to specify the configuration file to use during the next startup.

Step 7 Click **Restart Device**. The device prompts whether to check system software. The device with active and standby MPUs checks whether the two MPUs have the same system software. If not, the standby MPU spends 1 to 3 minutes copying the system software from the active MPU. The message "Is the configuration saved?" is displayed.

- To save the current configuration and restart the device, click **Yes**.
- To restart the device without saving the current configuration, click **No**.
- To cancel the configuration, click **Cancel**.

----End

2.19.1.2 System Software

Context

The device software includes BootROM software and system software. After the device is powered on, it runs the BootROM software to initialize the hardware and

display hardware parameters, and then runs the system software. The system software provides drivers and adaptation functions for hardware, and offers service features. The BootROM software and system software are prerequisites for device startup and operation, providing support, management, and services for the device.

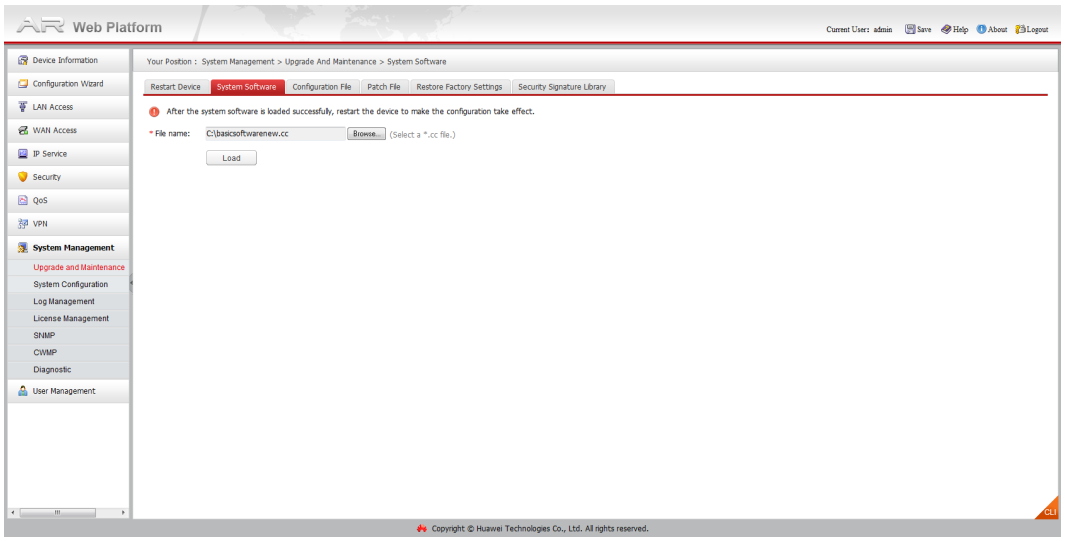
NOTE

The BootROM software is included in the system software package (.cc file) of the device. The BootROM software is automatically upgraded in system software upgrade.

Procedure

Step 1 Choose **System Management** > **Upgrade and Maintenance** > **System Software**, as shown in **Figure 2-290**.

Figure 2-290 System Software page



Step 2 Click **Browse** and select the system software to upload.

Step 3 Click **Load** to upload the system software to the device. The loaded system software is specified as the next startup system software.

You must restart the device to make the system software take effect.

----End

2.19.1.3 Configuration File

Context

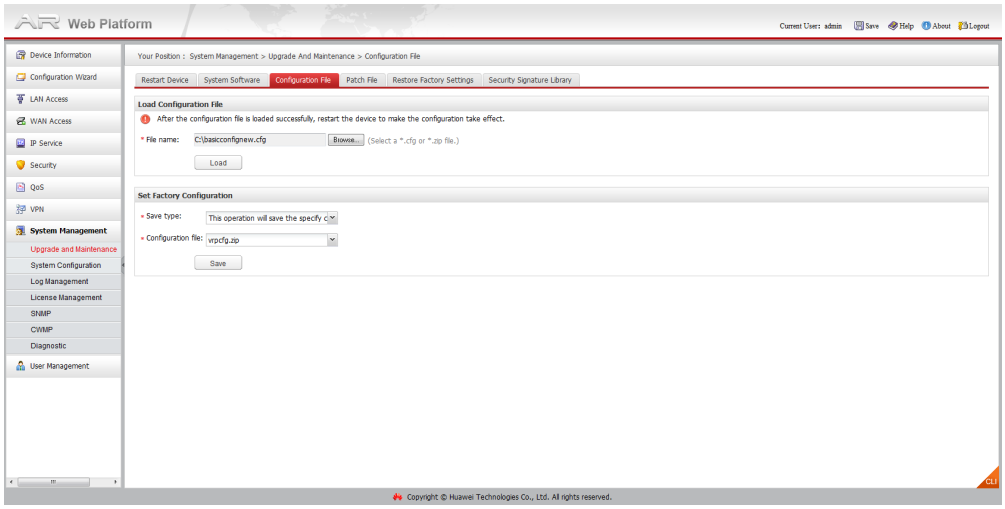
A configuration file is a collection of command lines. The current configurations are saved in configuration files, and continue to take effect after the device restarts. You can view configurations in configuration files or upload the files to other devices to implement batch configuration.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Choose **System Management** > **Upgrade and Maintenance** > **Configuration File**, as shown in **Figure 2-291**.

Figure 2-291 Configuration File page



Step 2 Click **Browse** and select the configuration file to upload.

Step 3 Click **Load** to upload the configuration file to the device.

You must restart the device to make the configuration file take effect.

Step 4 Set the factory configuration in the **Set Factory Configuration** area.

- Select **This operation will save the specify configuration as the factory configuration** from the drop-down list of **Save type**, and then specify the required configuration file in **Configuration file**.
- Select **This operation will save the current configuration as the factory configuration** from the drop-down list of **Save type**

Step 5 Click **Save** to save the factory configuration.

----End

2.19.1.4 Patch File

Context

A patch is a kind of software compatible with the system software. It is used to remove the urgent bugs of the system software. Patches can also fix errors or improve adaptation of the system software. For example, patches can fix defects of the system and optimize some functions to meet service requirements.

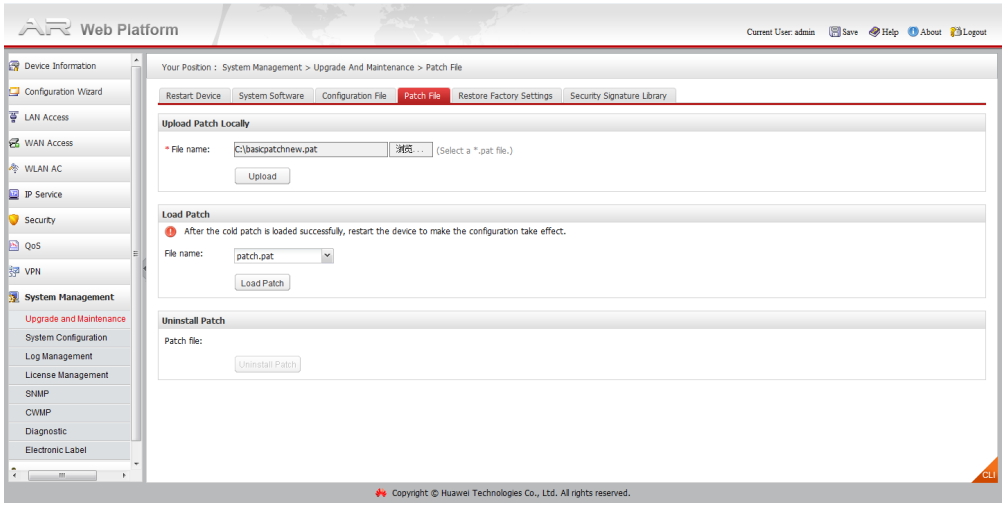
The patches are released in patch files. A patch file may contain one or more patches with different functions. When patch files are loaded from the storage device to the patch area in the memory, a unique sequence number is assigned to each patch file to identify, manage, and operate the patches.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Choose **System Management** > **Upgrade and Maintenance** > **Patch File**, as shown in **Figure 2-292**.

Figure 2-292 Patch File page



Step 2 Click **Browse** and select the patch to upload.

Step 3 Click **Upload** to upload the patch to the device.

Step 4 Select a patch to load in the **Load Patch** area and click **Load Patch**. The patch is loaded.

Step 5 To uninstall the current patch, click **Uninstall Patch**.

----End

2.19.1.5 Restore Factory Settings

Context

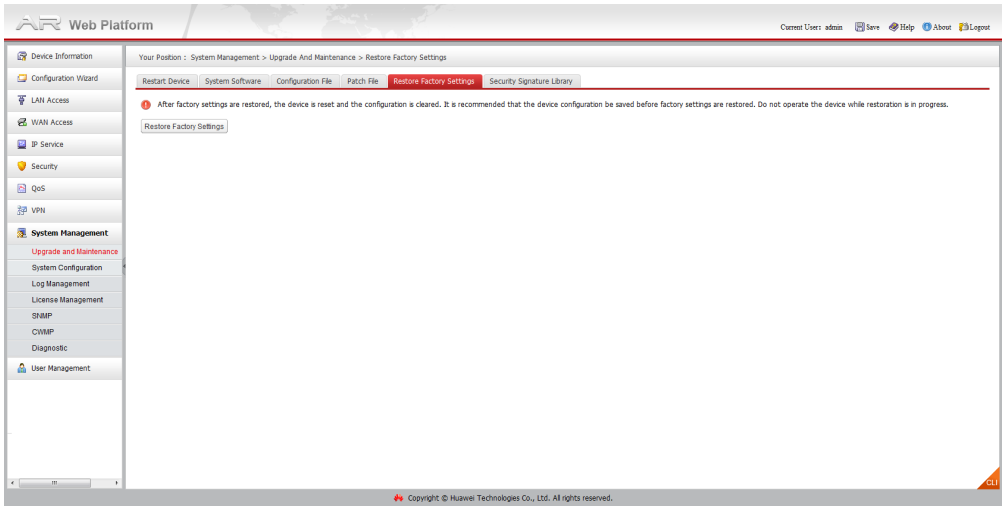
The device is delivered with basic configurations so that it can start and work properly when no configuration file exists or the configuration file is lost or damaged.

Procedure

Step 1 Choose **System Management** > **Upgrade and Maintenance** > **Restore Factory Settings**, as shown in **Figure 2-293**.

Copyright © Huawei Technologies Co., Ltd.

Figure 2-293 Restore Factory Settings page



Step 2 Click **Restore Factory Settings**.

----End

2.19.1.6 Security Signature Library

Context

NOTE

- The following product models support IPS function:
  - AR160 series: AR169BF, AR169FGW-L, AR169FGVW-L, AR169FVW-8S, AR169JFVW-4B4S, AR169JFVW-2S, AR169EGW-L, AR169EW, AR168F-4P, AR161EW, AR161EW-M1, AR161FW, AR161FV-1P, and AR169FVW.
  - AR1200 series: AR1220E, AR1220EV, and AR1220EVW.
  - AR2200 series: AR2204, AR2204XE, AR2204XE-DC, AR2220, AR2220E, AR2240, and AR2240C.
  - AR3200 series: All models.

NOTE

- The following product models support URL filtering function:
  - AR100&AR120&AR150&AR160&AR200&AR3200 series: All models.
  - AR1200 series: AR1220C, AR1220-8GE, AR1220E, AR1220EV, and AR1220EVW.
  - AR2200 series: all models except AR2201-48FE, AR2202-48FE, and AR2204.

Security signature libraries include the intrusion defense library. You can upgrade the library to improve device capabilities of identifying intrusions.

An IPS prevents and detects intrusions based on the intrusion defense library in which IPS signatures are predefined. IPS signatures describe characteristics of attacks on the network. A device compares the packet content against IPS signatures to detect and defend against attacks. If a data flow matches the characteristics in an IPS signature, the device processes the data flow based on the action matching the IPS signature.

 Copyright © Huawei Technologies Co., Ltd.

The libraries are upgraded in the security center in real time. After purchasing the library license, you can obtain the latest libraries to upgrade the security signature libraries.

You can upgrade the libraries locally or directly in the security center.

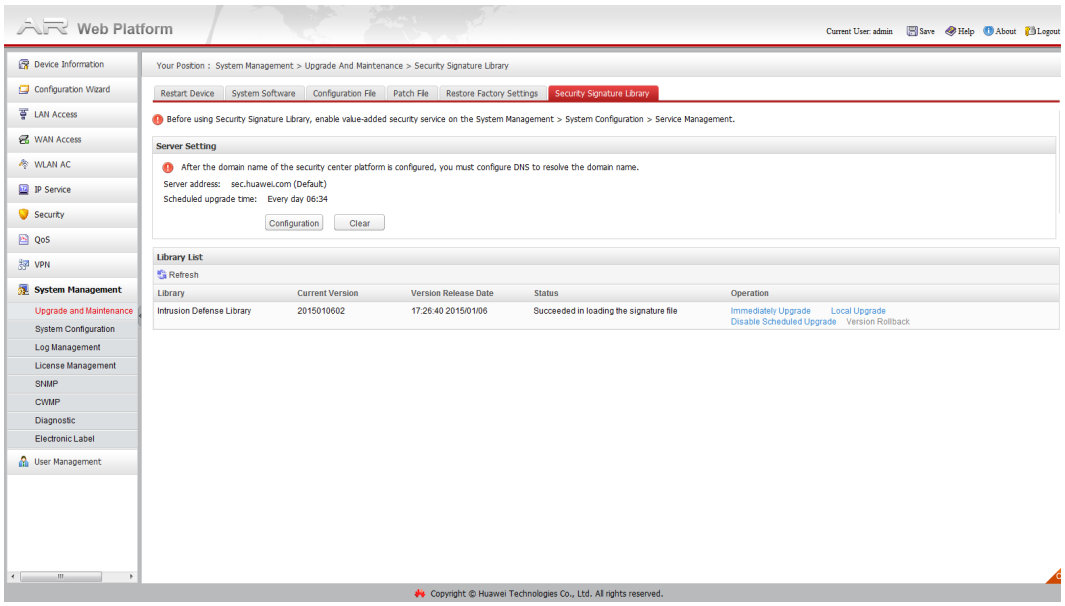
- Upgrade in the security center: You must purchase a license to connect a device to the server deployed by Huawei. The domain name of the security center is **sec.huawei.com**. If the device can access the security center, you can upgrade the libraries in either of the following modes:
  - Scheduled upgrade: You can specify the time when the libraries are upgraded. To prevent upgrade failures due to unstable networks, you are advised to set the upgrade time to the time when the volume of network traffic is small.
  - Immediate upgrade: When a new attack is detected on the network but the scheduled upgrade time is not reached, you can immediately upgrade the libraries to allow the device to defend against the new attack.
- Local upgrade: When the device cannot access the security center, you can download the latest library upgrade packages from the security center and save them locally. Then you can upload the upgrade packages to the device on the web platform so that the device upgrades the libraries.

Procedure

Step 1 Access the **Security Signature Library** page.

Log in to the web platform and choose **System Management** > **Upgrade and Maintenance** > **Security Signature Library** , as shown in **Figure 2-295**.

Figure 2-294 Security Signature Library page



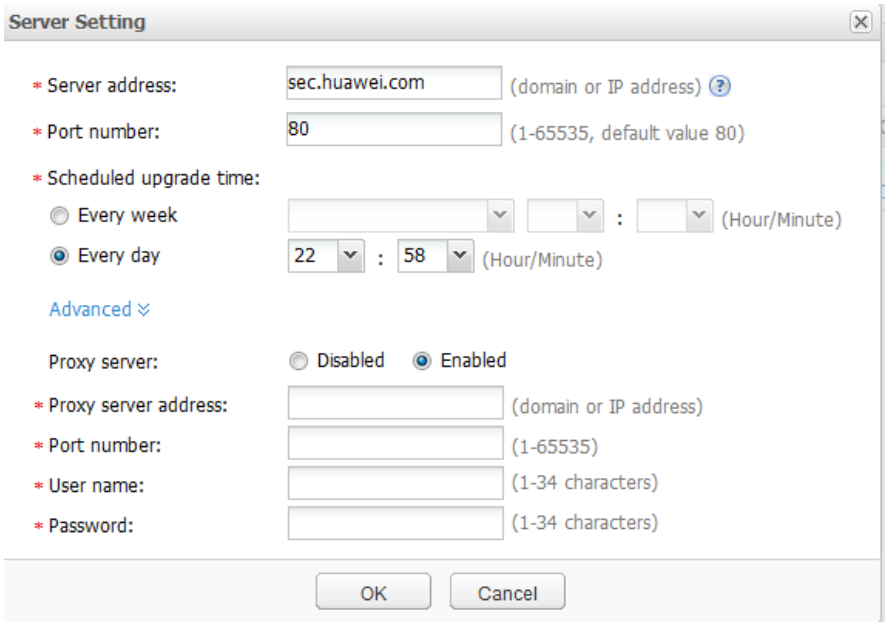
Step 2 In the **Server Setting** area, click **Configuration**. In the **Server Setting** dialog box that is displayed,, as shown in **Figure 2-295**, set parameters described in **Table 2-179**.

Table 2-179 Server parameters

Parameter	Description
Server address	Domain name of the security center. By default, the domain name of the security center is **sec.huawei.com**.
Port number	Port number of the security center. By default, the port number of the security center is 80.
Scheduled upgrade time	Time when the library is upgraded. • Every week: select one day from Monday to Sunday, and specify the hour and minute when the scheduled upgrade is performed. • Every day: select the upgrade time on each day. **NOTE** The configured scheduled upgrade time takes effect only after the scheduled upgrade function is enabled.
Proxy server	Whether a proxy server is used, that is, whether a proxy server is configured. • Disabled • Enabled
Proxy server address	Domain name or IP address of the proxy server. This parameter is available only when **Enabled** is set for **Proxy server**.
Port number	Port number of the proxy server. This parameter is available only when **Enabled** is set for **Proxy server**.
User name	User name used to log in to the proxy server. The user name must exist on the proxy server. This parameter is available only when **Enabled** is set for **Proxy server**.
Password	Password used to log in to the proxy server. This password must be the same as the password matching the user name for logging in to the proxy server. This parameter is available only when **Enabled** is set for **Proxy server**.

Copyright © Huawei Technologies Co., Ltd.

Figure 2-295 Server Setting parameters



Step 3 Click **OK**.

Step 4 In the **Library List** area, view the library status and upgrade the library. **Table 2-180** describes library upgrade operations.

Table 2-180 Library upgrade operations

Parameter	Description
Immediately Upgrade	Click **Immediately Upgrade**, and click **OK** in the **Information** dialog box.
Local Upgrade	Click **Local Upgrade**. In the dialog box that is displayed, click **Browse**, select the local upgrade package, and click **Upgrade**. After the upgrade succeeds, **Status** of the library is **Succeeded in loading the signature file** and **Current Version** is correct.
Enable Scheduled Upgrade	Click **Enable Scheduled Upgrade** or **Disable Scheduled Upgrade** to enable or disable the scheduled upgrade function. The default value is **Enable Scheduled Upgrade**.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Version Rollback	Click **Version Rollback**. In the **Information** dialog box that is displayed, click **OK**. You can roll back the library to the last version as required, for example, when an upgrade fails. **NOTICE** A library version can be rolled back only once. The library version is switches between the two versions if you perform rollback operations multiple times.

----End

2.19.2 System Configuration

2.19.2.1 File Management

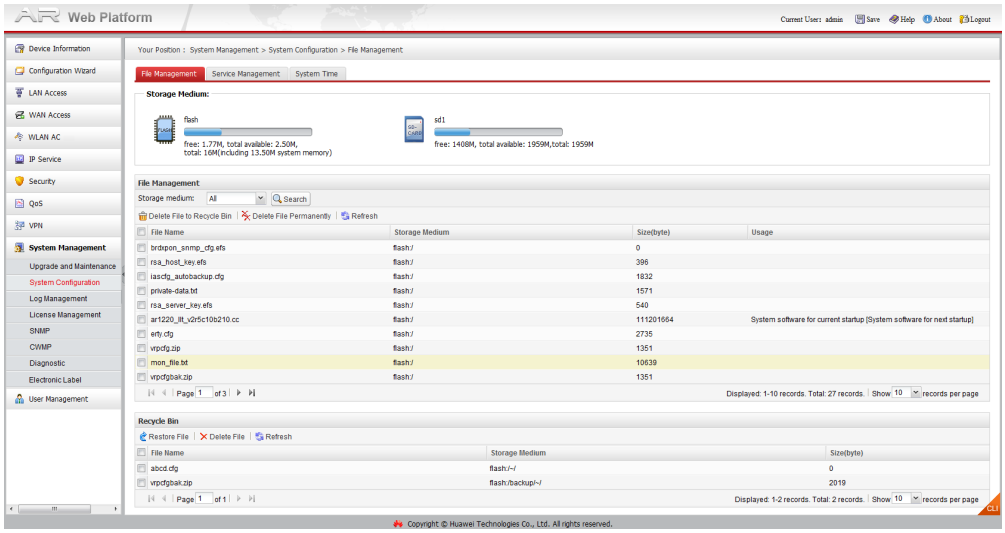
Context

The file system manages files on the storage devices.

Procedure

Step 1 Choose **System Management** > **System Configuration** > **File Management**, as shown in **Figure 2-296**.

Figure 2-296 File Management page



Step 2 In the **Storage Medium** area, check the remaining space, available space, and total space of the storage device.

NOTE

Storage devices supported by the device include the flash memory, SD card, hard disk, and USB flash drive. Different models support different storage devices. For details about storage devices supported by each model, see File System Overview.

Step 3 Manage files in the **File Management** area.

- To search all files in a storage medium or all the storage media, click **Search**.
- To move a file to the recycle bin, select the file and click **Delete File to Recycle Bin**. You can restore the deleted file in the **Recycle Bin** area.
- To permanently delete a file, select the file and click **Delete File Permanently**.
- To refresh the file list, click **Refresh**.

Step 4 Manage files in the **Recycle Bin** area.

- To restore a file in the recycle bin, select the file and click **Restore File**.
- To permanently delete a file from the recycle bin, select the file and click **Delete File**.
- To refresh the file list, click **Refresh**.

----End

2.19.2.2 Service Management

Context

In the TCP/IP protocol suite, the Telnet protocol applies to the application layer. The Telnet protocol provides remote login and virtual terminal functions through networks. Telnet is implemented based on the client/server model. Telnet clients send requests to the Telnet server that provides the Telnet service.

NOTE

The Telnet protocol poses a security risk, and therefore the STelnet protocol is recommended.

The FTP applies to scenarios that do not require high file transfer security. FTP is widely used for version upgrades.

NOTE

The FTP protocol will bring risk to device security. The SFTP mode is recommended.

STelnet ensures secure Telnet services. STelnet secures client access on a traditional insecure network by authenticating the client and encrypting data bidirectionally.

The SFTP secures file transfer on a traditional insecure network by authenticating the client and encrypting data bidirectionally.

After value-added security service is enabled. The device uses security policies to provide deep security defense based on the application layer. It protects users against attacks from various network threats.

 Copyright © Huawei Technologies Co., Ltd.

After the HTTP or HTTPS service is enabled, log in to a router functioning as the web server through HTTP or HTTPS to remotely configure and manage the router. Compared to HTTP, HTTPS is more secure.

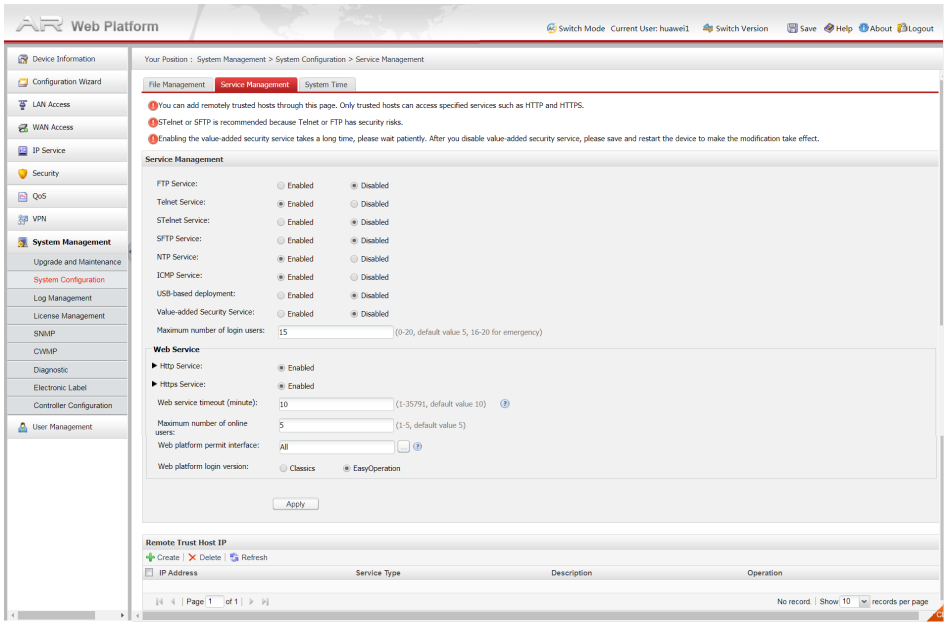
If you do not perform any operation before the web service times out, the system forcibly logs you out and prompts you to log in to the web platform again when you perform an operation. The default web service timeout period, 10 minutes, is recommended.

NTP synchronizes time among a set of distributed time servers and clients. If a device does not need to synchronize the clock with external servers or peers or it does not need to provide a clock reference source for external clients, you can disable the NTP function on the device.

Procedure

- Perform service management.
  a. Choose **System Management** > **System Configuration** > **Service Management** to access the **Service Management** page, as shown in Figure 2-297.

Figure 2-297 Service Management page



  b. Set **FTP Service** to **Enabled** or **Disabled** to enable or disable FTP.
  c. Set **Telnet Service** to **Enabled** or **Disabled** to enable or disable Telnet.
  d. Set **STelnet Service** to **Enabled** or **Disabled** to enable or disable STelnet.
  e. Set **SFTP Service** to **Enabled** or **Disabled** to enable or disable SFTP.
  f. Set **NTP Service** to **Enabled** or **Disabled** to enable or disable the NTP function of the local device.
  g. Set **ICMP Service** to **Enabled** or **Disabled** to enable or disable ICMP.
  h. Set **USB-based deployment** to **Enabled** or **Disabled** to enable or disable USB-based deployment.

 Copyright © Huawei Technologies Co., Ltd.

i. Set **USB-based deployment** to **Enabled**.

ii. Enter a password in **Authentication password**.

i. Set **Value-added security service** to **Enabled** or **Disabled** to enable or disable value-added security.

j. Set **Maximum number of login users** to set the maximum number of VTY user interfaces.

By default, the maximum number of login users is 5, which is the sum of Telnet users and SSH users.

NOTE

When the maximum number of VTY user interfaces is set to 0, users (including Telnet and SSH users) cannot log in to the device through VTY, and web users cannot log in to the device through the web system.

When the maximum number of VTY user interfaces is set to 15, the maximum number of login users can be set to 16 to 20. This setting is used only in emergency situations.

k. Click ▶ next to **Http Service**, and enter a port number in the **Port** text box.

l. Set **Https Service** to **Enabled** to enable HTTPS.

- Click ▶ next to **Https Service**.
- Enter a port number in the **Port** text box.
- Enter a management interface number in the **Manager port** text box.
- Select an SSL policy in the **SSL** text box.

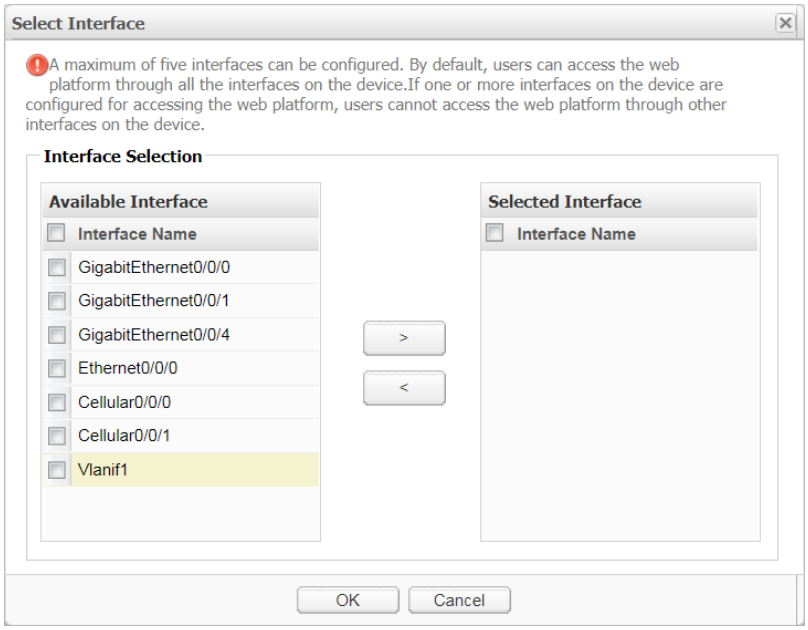
m. Set **Web service timeout** to set the timeout period for the web server.

n. Set **Maximum number of online user** to set the maximum number of concurrent online users allowed by the web system.

o. Click  on the right of **Web platform permit interface**. In the displayed **Select Interface** dialog box, select the required interfaces to configure the interfaces that are allowed access to the web system, and click **OK**, as shown in **Figure 2-298**.

Copyright © Huawei Technologies Co., Ltd.

Figure 2-298 Select Interface



NOTE

A maximum of five interfaces can be configured. By default, users can access the web platform through all the interfaces on the device. If one or more interfaces on the device are configured for accessing the web platform, users cannot access the web platform through other interfaces on the device.

p. Set **Web platform login version** to **EasyOperation** or **Classics** to configure the web system version for the next login.

By default, the EasyOperation version is used for web system login.

NOTE

If you log out and then log in again, the web system login version is not switched. You need to open the web browser again to switch the web system login version.

q. Click **Apply**.

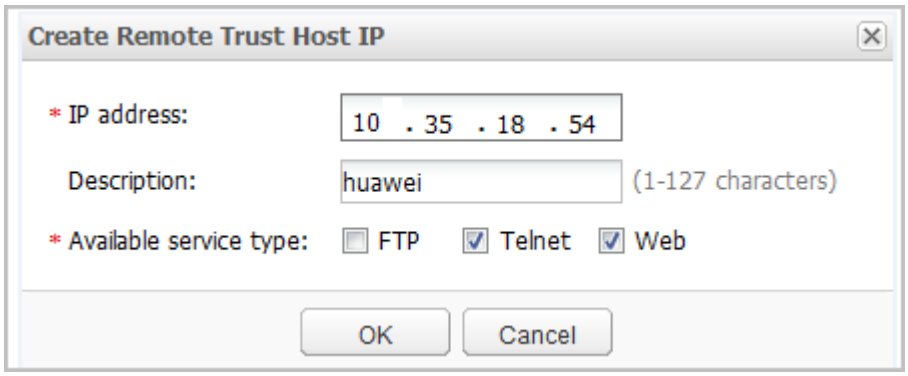
NOTE

V200R010C10 and later versions support **ICMP Service**, **USB-based deployment**, **Maximum number of login users**, **Web platform login version**, and **Web platform permit interface**.

- Create a remotely trusted host.
  a. Choose **System Management** > **System Configuration** > **Service Management**.
  b. Click **Create** in **Remote Trust Host IP** to create a remotely trusted host, as shown in **Figure 2-299**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-299 Creating a remote trust host



c. Set parameters on the **Create Remote Trust Host IP** page, as described in **Table 2-181**.

d. Click **OK**.

Table 2-181 Description of parameters for creating a remotely trusted host

Parameter	Description
IP Address	IP address of the remotely trusted host.
Description	Description of the remotely trusted host.
Available service type	Service type of the remotely trusted host.

- Delete a remotely trusted host.

  a. Choose **System Management** > **System Configuration** > **Service Management**.

  b. Select remotely trusted hosts that you want to delete.

  c. Click **Delete** in **Remote Trust Host IP**.

----End

2.19.2.3 System Time

Context

To ensure communication between the router and other devices, set the accurate system time. The router support automatic system time synchronization with the NTP server or manual system time setting. The first method is recommended.

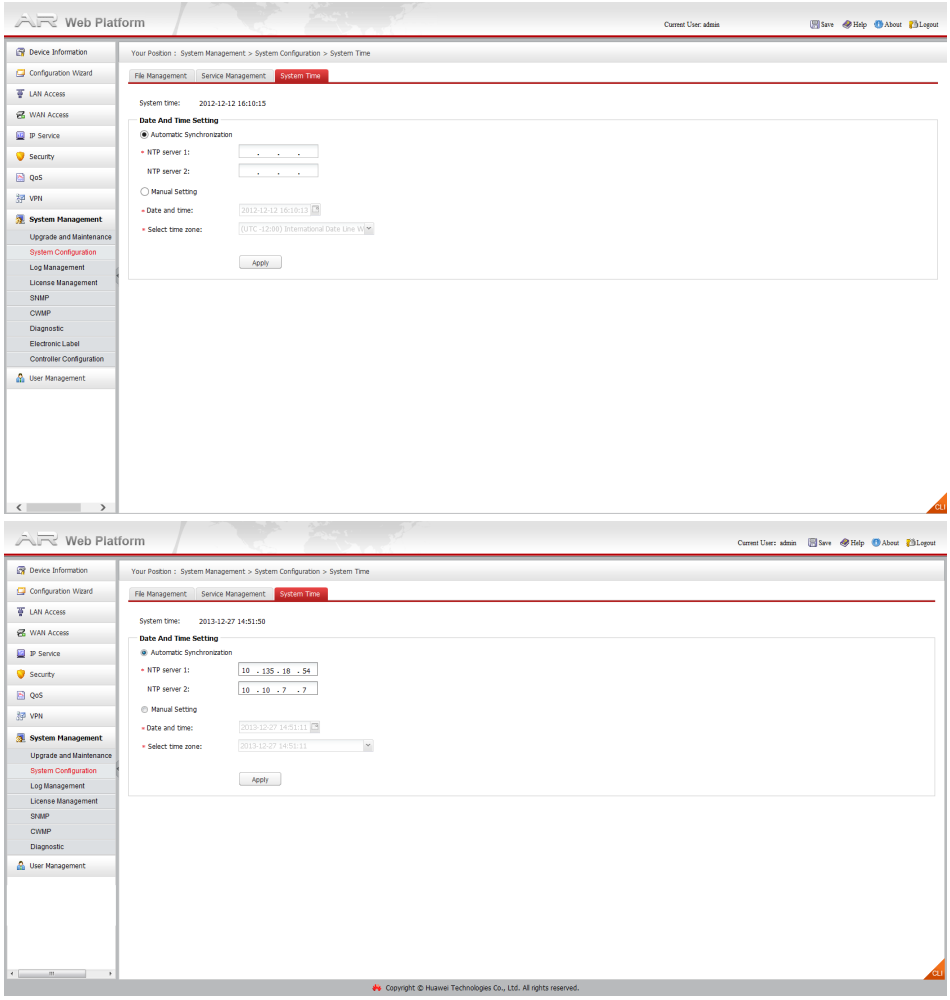
Procedure

- Automatic synchronization

  a. Choose **System Management** > **System Configuration** > **System Time**, as shown in **Figure 2-300**.

Copyright © Huawei Technologies Co., Ltd.

Figure 2-300 Automatic Synchronization page



b. In the **Date And Time Setting** area, click **Automatic Synchronization**.

c. Set **NTP server 1** to the IP address of the NTP server 1.

d. (Optional) Set **NTP server 2** to the IP address of the NTP server 2.

e. Click **Apply**.

f. In the **Information** dialog box that is displayed, click **OK**.

NOTE

The web platform supports two NTP servers and synchronizes the system time with the NTP server whose primary clock level is higher. For example, NTP1 has a higher primary clock level than NTP2, so the router synchronizes time with NTP1.

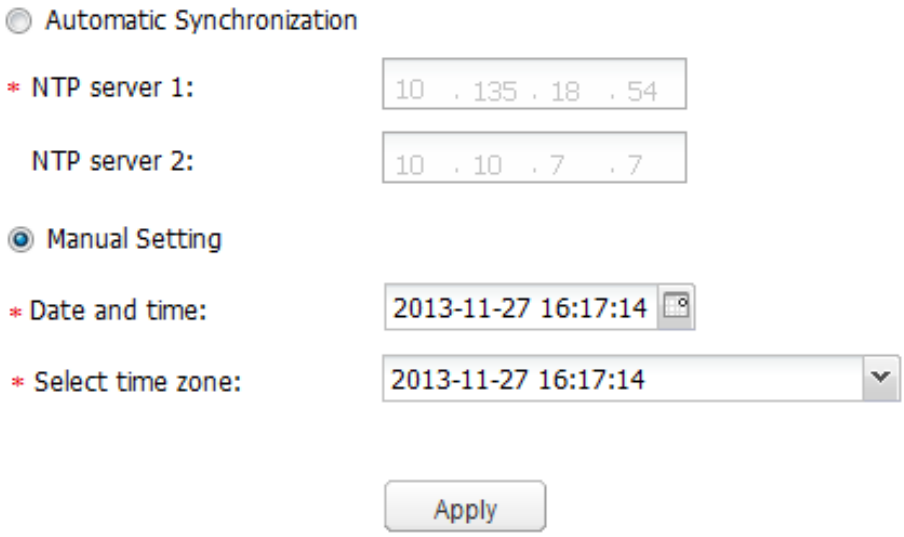
If the primary clock level of the web platform is higher than the NTP servers, the web platform does not synchronize the system time with the NTP server.

- Manual setting

  a. Choose **System Management** > **System Configuration** > **System Time**.

  b. In the **Date And Time Setting** area, click **Manual Setting**, as shown in **Figure 2-301**.

Figure 2-301 Manual Setting page



c. In the **Date And Time Setting** area, set the date and time.
d. Click the **Select time zone** drop-down list box, and select the time zone.
e. Click **Apply**.
f. In the **Information** dialog box that is displayed, click **OK**.

----End

2.19.3 Log Management

2.19.3.1 View Logs

Context

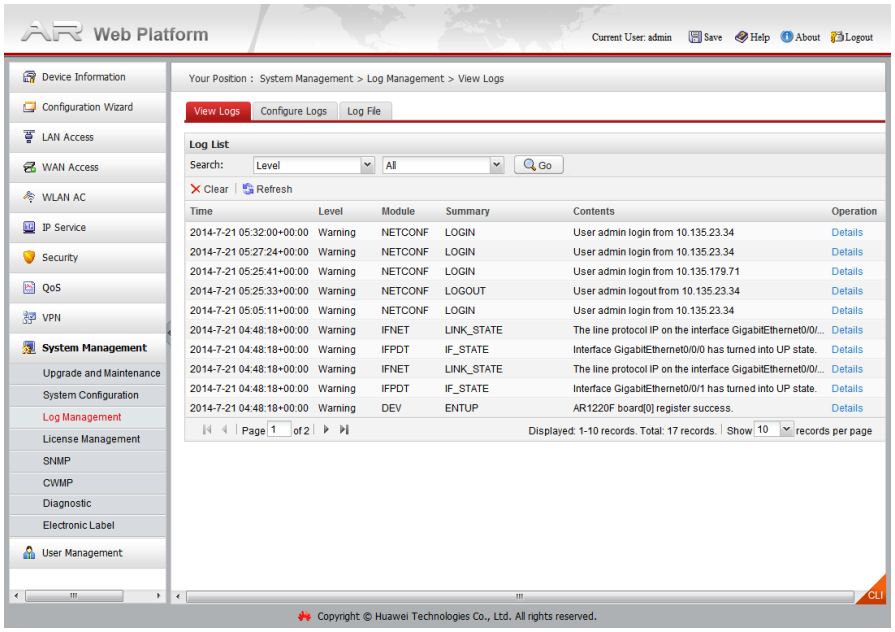
Logs are displayed in a log list. You can view logs of a specified type and delete logs.

Procedure

- Viewing logs
  a. Choose **System Management** > **Log Management** > **View Logs**, as shown in **Figure 2-302**.

 Copyright © Huawei Technologies Co., Ltd.

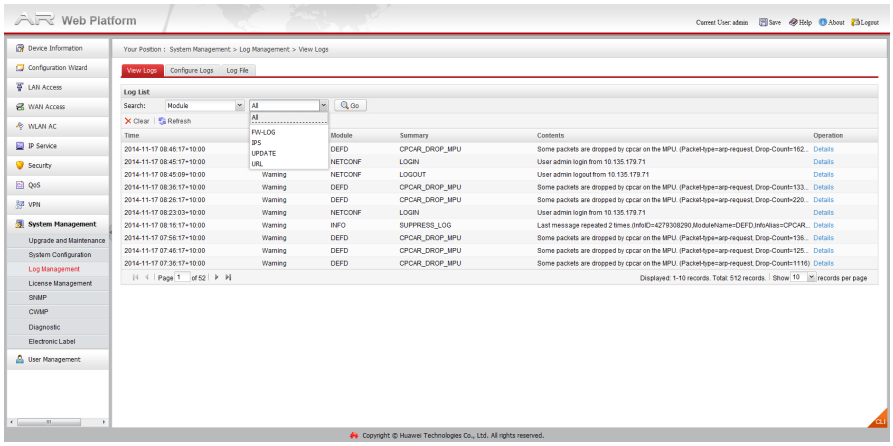
Figure 2-302 View logs



b. Select **Module** or **Level** from the **Search item** drop-down list box, and select the log module or level from the subsequent drop-down list box.

- The registered module varies depending on devices. **Module** displays the module names of all the received logs, as shown in **Figure 2-303**.

  Figure 2-303 Log browsing page

  To check logs of a specified module, you can enter the module name in this drop-down list box. Fuzzy search is supported. For example, you can enter **net** to check logs of all modules whose name contains **net** and **NET**.

- **Table 2-182** describes log levels.

Table 2-182 Log levels

Level	Description
Emergency	A fault causes the device to fail to run normally unless it is restarted. For example, the device is restarted because of program exceptions or a memory error is detected.
Alert	A fault needs to be rectified immediately. For example, memory usage of the system reaches the upper limit.
Critical	A fault needs to be analyzed and processed. For example, the memory usage falls below the lower threshold; temperature falls below the alarm threshold; BFD detects that a device is unreachable or detects locally generated error messages.
Error	An improper operation is performed or exceptions occur during service processing. The fault does not affect services but needs to be analyzed. For example, users enter incorrect commands or passwords; error protocol packets are received from other devices.
Warning	Some events or operations may affect device running or cause service processing faults, which requires full attention. For example, a routing process is disabled; BFD detects packet loss; error protocol packets are detected.
Notification	A key operation is performed to keep the device running normally. For example, the shutdown command is run; a neighbor is discovered; protocol status changes.
Informational	A normal operation is performed. For example, the display commands are run.

Copyright © Huawei Technologies Co., Ltd.

Level	Description
Debugging	A routine operation is performed, and no action is required.

c. Click **Search**.

Logs of the specified level are displayed in the log list. **Table 2-183** describes parameters in the log list.

Table 2-183 Parameters in the log list

Parameter	Description
Time	Log time.
Level	Log level.
Module	Module where a log is generated.
Summary	Brief information about a log.
Contents	Contents of a log.
Operation	Operation that the system allows on a log. To view complete information about a log, click **Details**. The log details can be copied.

- Clearing logs
  a. Choose **System Management** > **Log Management** > **View Logs**.
  b. Click **Clear**.
  c. In the **Information** dialog box, click **OK**.
  ALL Logs are deleted from the log list.

----End

2.19.3.2 Configuring Logs

Context

You can save logs in either of the following ways:

- Configure the log buffer. A router reserves a certain size of flash memory to save a small number of logs.
- Configure a log host to save logs.

Copyright © Huawei Technologies Co., Ltd.

NOTE

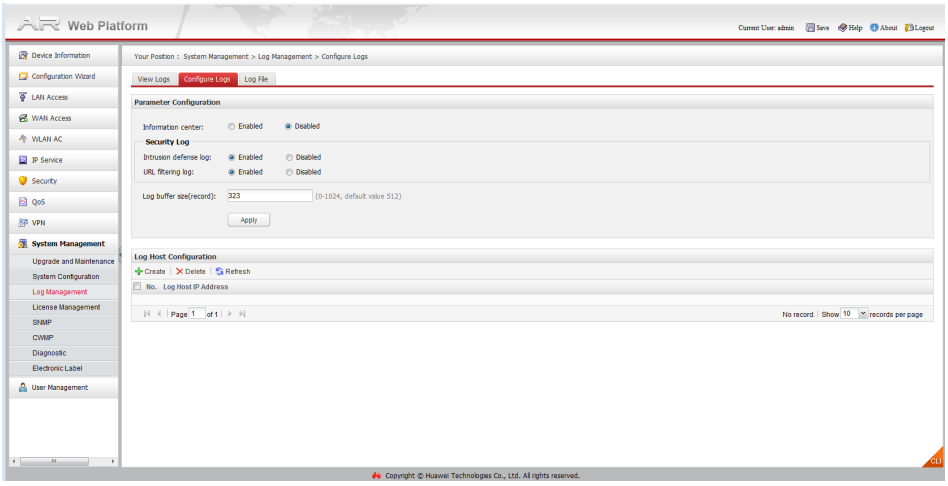
The web platform supports 8 log hosts. When the number of configured log hosts exceeds that limited by the web platform, a dialog box is displayed indicating the number of log hosts reaches the maximum.

If the device does not support depth security or depth security is not enabled, some security logs cannot be displayed.

Procedure

- Configuring log parameters
  a. Choose **System Management** > **Log Management** > **Configure Logs**, as shown in **Figure 2-304**.

  Figure 2-304 Configure Logs

  b. Set **Information center** to **Enable** in the **Parameter Configuration** area.
  c. Set **Intrusion defense log** to **Enable** in the **Parameter Configuration** area.
  d. Set **URL filtering log** to **Enable** in the **Parameter Configuration** area.
  e. Set **Log buffer size(record)**.

     By default, the log buffer can store 512 logs.
  f. Click **Apply**.
- Configuring a log host
  – Creating a log server
    i. Choose **System Management** > **Log Management** > **Configure Logs**.
    ii. Click **Create** in the **Log Host Configuration** area.
    iii. Enter the IP address of the log server in the **Create A Log Host** dialog box.
    iv. Click **OK**.

    The created log host is displayed in the **Log Host Configuration** area. You can add a maximum of eight log hosts by repeating the preceding operations.

 Copyright © Huawei Technologies Co., Ltd.

– Deleting a log server

i. Choose **System Management** > **Log Management** > **Configure Logs**.

ii. Select a log server or all log servers in the **Log Host Configuration** area.

iii. Click **Delete**.

iv. In the **Information** dialog box that is displayed, click **OK**.

The log host is deleted.

----End

2.19.3.3 Saving Logs as Log Files

Context

This section describes how to save logs in the user log buffer and diagnosis log buffer as log files.

- Logs in the user log buffer are saved as the file **log.log**.
- Logs in the diagnosis log buffer are saved as the file **log.dblg**.

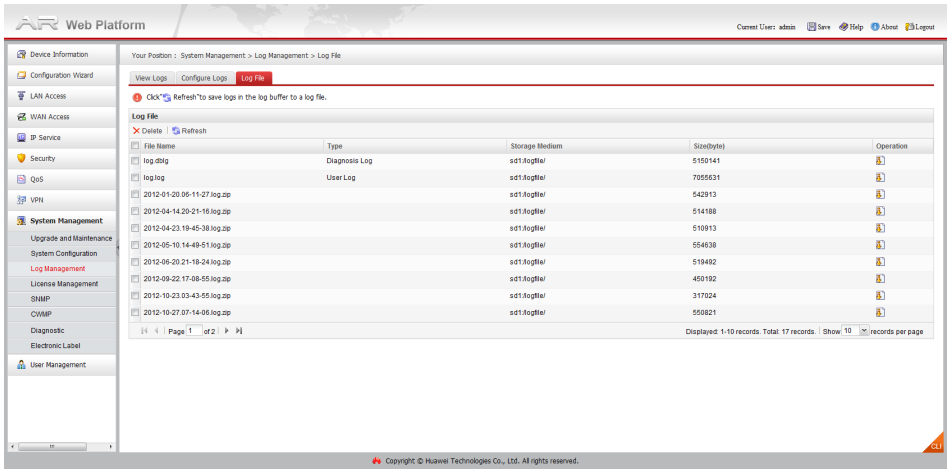
When the size of a log file exceeds the threshold, the log file is automatically compressed as a **.zip** file.

Procedure

- Querying log information

a. Choose **System Management** > **Log Management** > **Log File**, as shown in **Figure 2-305**.

Figure 2-305 Log file



b. Click **Refresh**.

Information about log files is displayed in **Log File**. For details about parameters in **Log File**, see **Table 2-184**.

Copyright © Huawei Technologies Co., Ltd.

Table 2-184 Parameter description

Parameter	Description
File Name	Name of the log file.
Type	Type of the log file.
Storage Medium	Directory where the log file is stored.
Size	Size of the log file, in bytes.
Operation	To download the log file, you can click  .

- Downloading a log file
  a. Choose **System Management** > **Log Management** > **Log File**.
  b. Find the required log file from the log file list, and click  mapping the log file. The **File Download** dialog box is displayed.
  c. Click **Save As**.
  d. Select the directory for storing the log file and click **Save**.
- Deleting a log file
  a. Choose **System Management** > **Log Management** > **Log File**.
  b. Select a log file in the log file list.
  c. Click **Delete**.
  d. In the dialog box that is displayed, click **OK**. The log file is deleted.

----End

2.19.4 License Management

2.19.4.1 Introduction

A license is used to authorize users to use a specified feature, version, or capacity or use services in a certain period. A license contains a license file and a license authorization certificate.

After purchasing or renew a license, you can obtain a license authorization certificate. To use resources controlled by the license, you have to apply for a license file. Only one license file is generated on a device even if you have purchased multiple licenses. Each license file is bound to an Equipment Serial Number (ESN). A license file belongs to only one device.

Obtain the following information before applying for a license file:

- Obtain the Contract number from the license authorization certificate.
- Obtain the License Authorization Code (LAC) from the license authorization certificate.
- Obtain the ESN on the **Device Information** page. Log in to the web platform, click **Device Information**, and select **Device Information** from the **Item**

 Copyright © Huawei Technologies Co., Ltd.

drop-down list box at the upper right corner. You can view the ESN in the **Device Information** area.

Agents and common users can use Huawei flexnet operations (ESDP) to obtain license files.

NOTE

The uniform resource locator (URL) of the Huawei ESDP is http://app.huawei.com/isdp.

2.19.4.2 Activating a License

Context

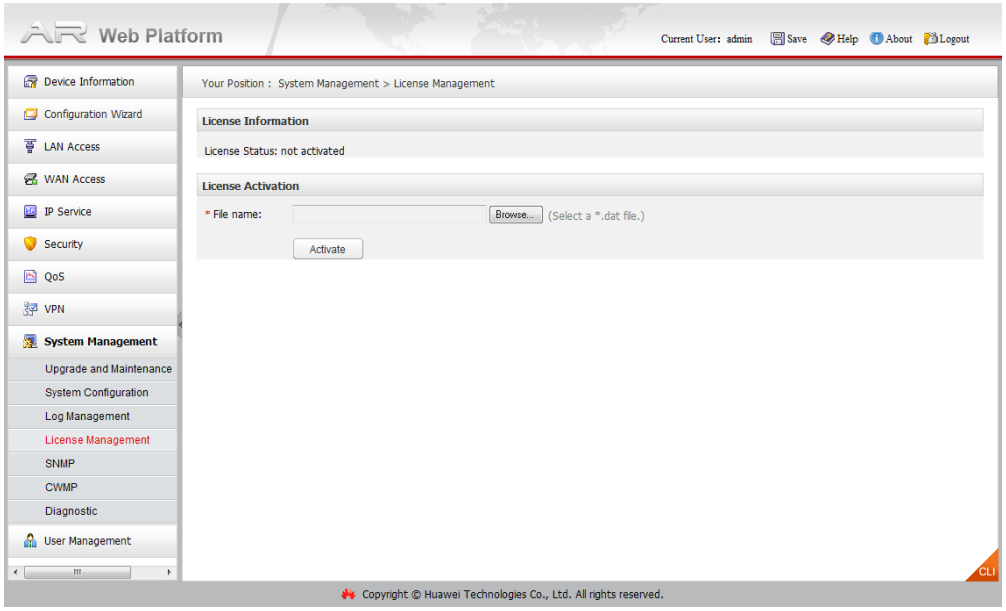
You need to activate licenses in either of the following situations:

- Purchasing a license to obtain permissions on related functions after you purchase a new device.
- Applying for a new license file, and upgrade and activate the license file when the license file is activated on the device and a new feature is required.

Procedure

Step 1 Choose **System Management** > **License Management**.

Figure 2-306 License Management



Step 2 Click **Browse** in the **License Activation** area and select the license file to upload.

Step 3 Click **Activate**. The current license file is activated.

NOTE

If you need to adjust a license file between devices (for example, move a license file from device A to device B) without changing the license authorization certificate or an upgraded license file is incompatible with the original one, click **Revoke** in the **License Information** area to obtain a license revocation code. Use the license revocation code to obtain a new license file, and activate the license file.

You can view the license status, resources controlled by the license, and authorization information in the **License Information** area. **Table 2-185** describes license parameters.

Table 2-185 License parameters

Parameter	Description
License Status	**not activated**: default status. By default, a license is not activated after the system starts or when it is invalid. **Normal**: A commercial license enters the Normal state after it is activated. **Trial**: A license enters the Trial state when the activated ESN does not match the license or after the license expires. **Demo**: A temporary license enters the Demo state after it is activated. **Emergency**: When a license enters the Emergency state, dynamic resources on the device are free from the license controls. That is, the device runs with the maximum configurations of dynamic resources. A license can remain in Emergency state for at most seven days. After seven days, the license enters the original state.
Control Resource	Resources controlled by the license.
Authorization Information	Authorization information of the resources controlled by the license.

----End

2.19.5 SNMP

Context

The Simple Network Management Protocol (SNMP) is a network management standard widely used on TCP/IP networks. SNMP uses a central computer (a network management station) that runs network management software to manage network elements.

The web system supports SNMPv1, SNMPv2, and SNMPv3. The router and network management station must use the same SNMP version.

Copyright © Huawei Technologies Co., Ltd.

Table 2-186 Usage scenarios of SNMP

Version	Usage Scenario
SNMPv1	Applicable to small networks. The networks have simple structures, have low security requirements or are not prone to attacks, and have stable topologies. For example, campus networks and small enterprise networks.
SNMPv2	Applicable to medium or large networks. The networks have low security requirements or are not prone to attacks, have high service traffic volume, and may be congested by traffic. For example, VPNs.
SNMPv3	Applicable to all networks, especially the networks have high security requirements. SNMPv3 allows only authorized administrators to manage the network. When the network management station and managed devices communicate over the public network, SNMPv3 is recommended.

NOTE

AR100&AR120 series (except AR129CV&AR129CVW&AR129CGVW-L) do not support SNMP.

2.19.5.1 Global Configuration

Context

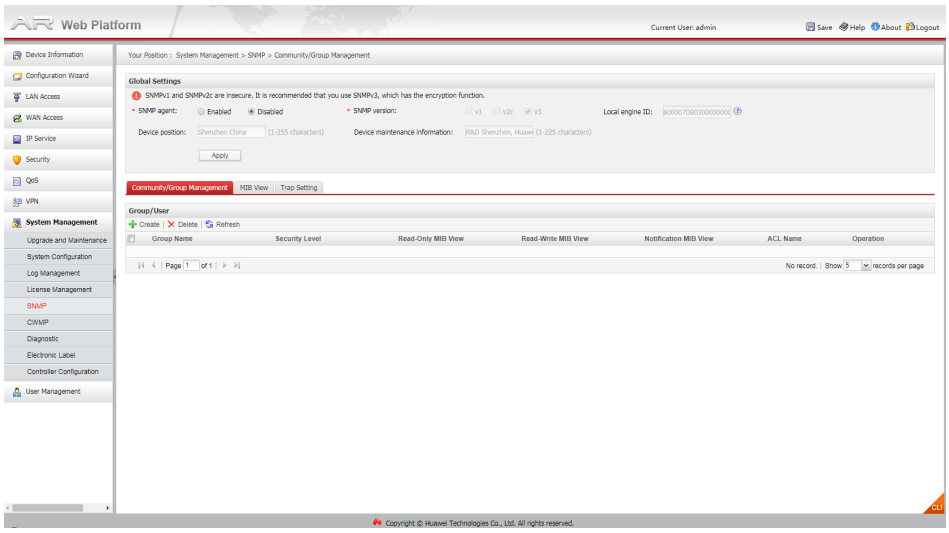
After the SNMP agent starts, you can perform the SNMP global configuration to confirm the SNMP version and device maintenance information.

Procedure

Step 1 Choose **System Management** > **SNMP**, as shown in **Figure 2-307**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-307 Configuring SNMP globally



Step 2 Set **SNMP agent** to **Start**.

Step 3 Set **SNMP version**.

By default, the web platform supports SNMPv3. You can select one or multiple versions. The router and network management station must use the same SNMP version.

NOTE

SNMPv1 and SNMPv2c are insecure. It is recommended that you use SNMPv3, which has the encryption function.

Step 4 Enter the position of the router in the **Device position** text box.

When **Device position** is not set, click **Apply**. The factory setting is displayed.

Step 5 Enter device maintenance information in the **Device maintenance information** text box.

When **Device maintenance information** is not set, click **Apply**. The factory setting is displayed.

Step 6 Click **Apply**.

Step 7 In the **Information** dialog box that is displayed, click **OK**.

----End

2.19.5.2 Community/Group Management

Context

In different SNMP versions, community/group management configurations are different. After the global configuration is applied, you must configure the community/group management. **Table 2-187** describes mappings between SNMP versions and community/group management.

Table 2-187 Mappings between SNMP versions and community/group management

Version	Configuration Scenario
SNMPv1	Community management
SNMPv2c	Community management
SNMPv1 and SNMPv2c	Community management
SNMPv3	Group management
SNMPv1 and SNMPv3	Community management and group management
SNMPv2c and SNMPv3	Community management and group management
SNMPv1, SNMPv2c, and SNMPv3	Community management and group management

NOTE

The web platform supports a maximum of 20 communities and 20 groups. The number of users in all groups cannot exceed 20. A dialog box is displayed when the number of communities, groups, or users exceeds the limit on the web platform.

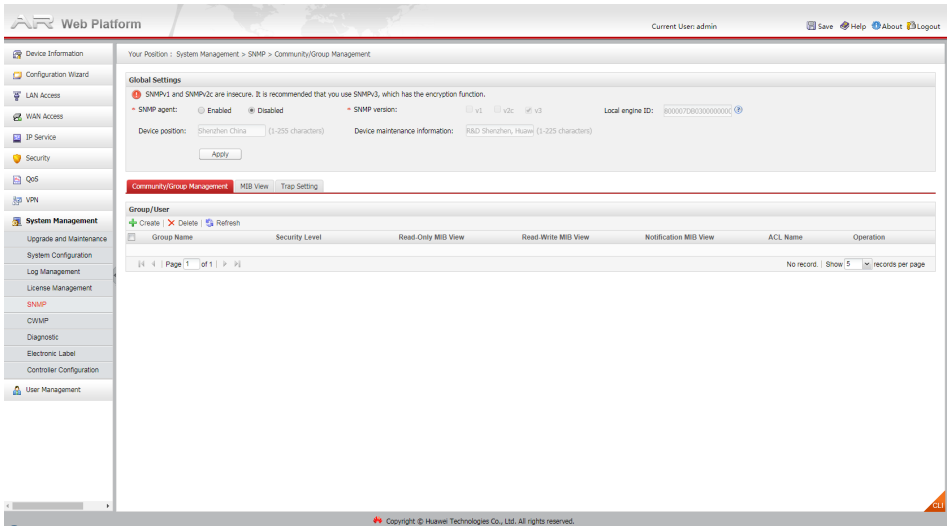
Procedure

- Community management

  Creating a community

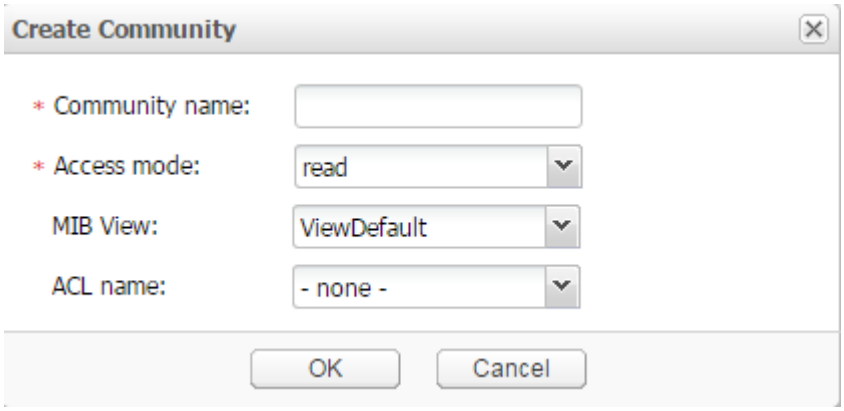
  a. Choose **System Management** > **SNMP** > **Community/Group Management**, as shown in **Figure 2-308**.

  Figure 2-308 Community/Group Management page



b. In the **Community** area, click **Create**, as shown in **Figure 2-309**.

Figure 2-309 Creating a community name



c. In the dialog box that is displayed, set parameters listed in **Table 2-188**.

d. Click **OK**.

The created community is displayed in the **Community** area. The community name is displayed in cipher text. To create more communities, repeat the preceding steps.

Table 2-188 Community parameters

Parameter	Description	Value
Community name	SNMPv1 or SNMPv2c read/write community name, which is the password that the NMS uses to perform the read and write operations on an SNMP agent. The password configured on the SNMP agent must be the same as that configured on the NMS.	The value is a string of the community name length must not be less than 6 without spaces.
Access mode	Access permission of a community in a specified MIB view.	The value can be: • read • Read-write
MIB View	MIB objects monitored and managed by the NMS.	-
ACL name	ACL that limits the device management rights of the NMS.	-

Modifying a community

 Copyright © Huawei Technologies Co., Ltd.

a. Choose **System Management** > **SNMP** > **Community/Group Management**.

b. In the **Community** area, click  corresponding to the community you want to modify.

c. In the dialog box that is displayed, set parameters listed in **Table 2-188**. The parameter **Community Name** cannot be modified.

d. Click **OK**.

If the operation is successful, the **Community** area is displayed and the information about the community changes in the list.

Deleting a community

a. Choose **System Management** > **SNMP** > **Community/Group Management**.

b. In the **Community** area, select the check box next to the community you want to delete, or select the check box next to **Community Name** to select all communities.

c. Click **Delete**.

d. In the **Information** dialog box that is displayed, click **OK**.

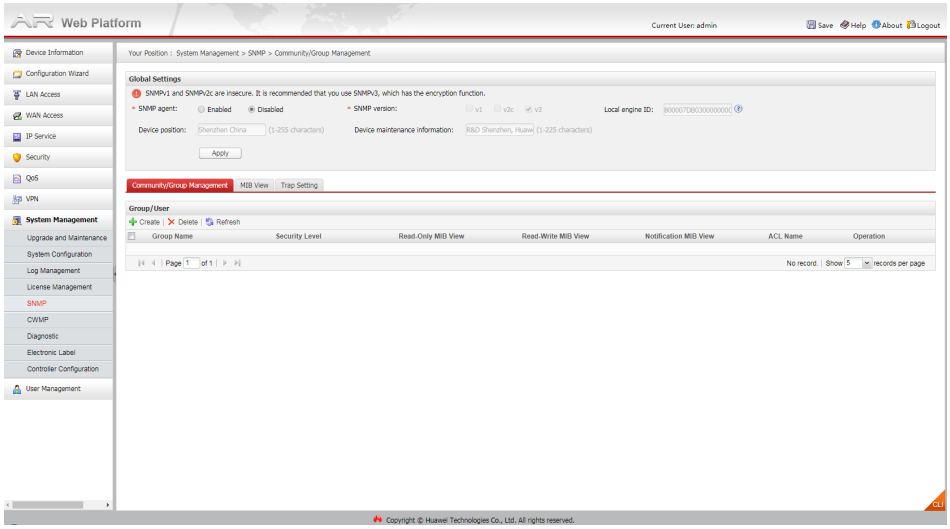
The deleted community is not displayed in the **Community** area.

- Group management

  Creating a group

  a. Choose **System Management** > **SNMP** > **Community/Group Management**, as shown in **Figure 2-310**.

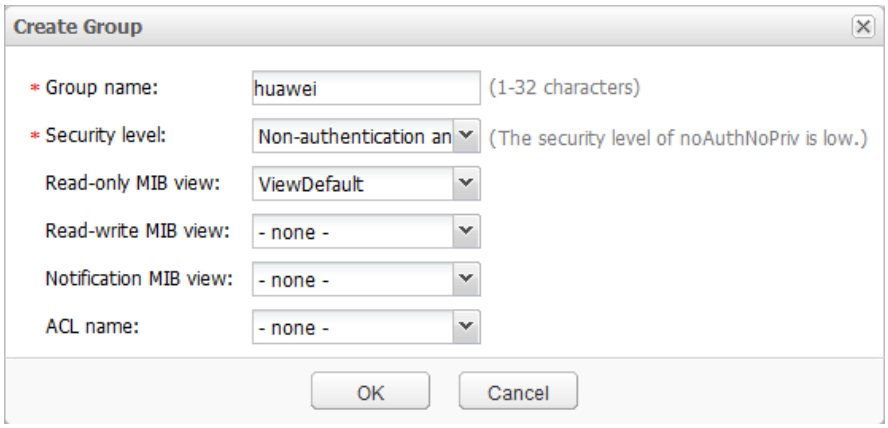
  Figure 2-310 Configuring group management

  b. In the **Group/User** area, click **Create**, as shown in **Figure 2-311**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-311 Creating groups



c. In the dialog box that is displayed, set parameters listed in **Table 2-189**.

d. Click **OK**.

The created group is displayed in the **Group/User** area. To create more groups, repeat the preceding steps.

Table 2-189 Group parameters

Parameter	Description	Value
Group name	Name of an SNMPv3 user group.	The value is a string of 1 to 32 characters.
Security level	Security level of a SNMPv3 group.	Security levels include: • Non-authentication and non-encryption • Authentication and non-encryption • Authentication and encryption
Read-only MIB view	MIB object that the NMS can read only.	-
Read-write MIB view	MIB object that the NMS can read and write.	-
Notification MIB view	MIB object that sends notifications to the NMS.	-
ACL name	ACL that limits the device group management rights of the NMS.	-

Creating a user

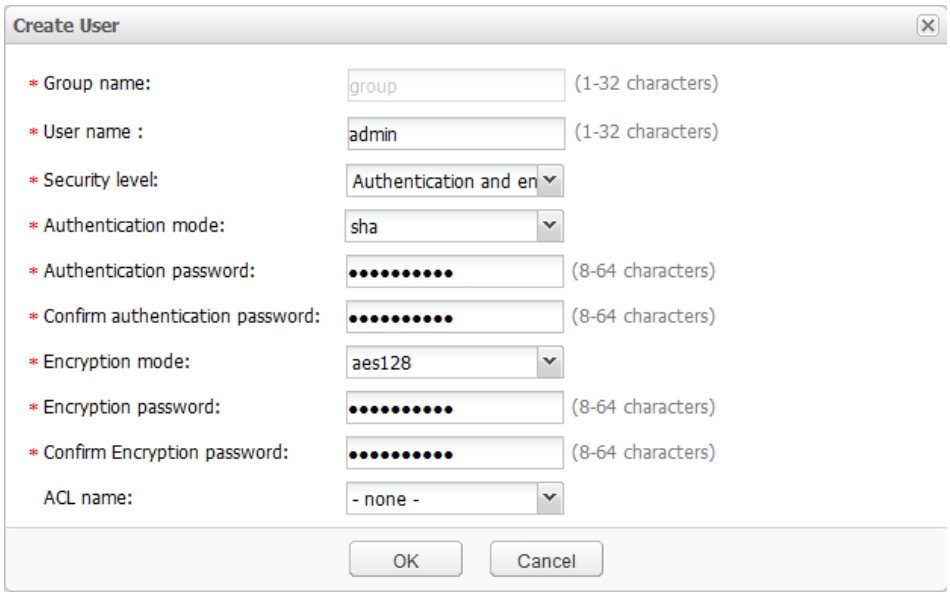
Copyright © Huawei Technologies Co., Ltd.

a. Choose **System Management** > **SNMP** > **Community/Group Management**.

b. In the **Group/User** area, click **Add User** corresponding to the group to which you want to add users, as shown in **Figure 2-312**.

The security level of a user cannot lower than that of the group to which the user belongs.

Figure 2-312 Creating SNMP users



c. In the dialog box that is displayed, set parameters listed in **Table 2-190**. The parameter **Group Name** cannot be modified.

d. Click **OK**.

The created user is displayed in the **Group/User** area. To create more users, repeat the preceding steps. To view users in a group, click next to **Group Name**.

Table 2-190 User parameters

Parameter	Description	Value
Group name	SNMPv3 user group that cannot be configured.	-
User name	User name of an SNMPv3 user.	The value is a string of 1 to 32 characters.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
Security level	Security level of a SNMPv3 group.	Security levels include: • Non-authentication and non-encryption • Authentication and non-encryption • Authentication and encryption **NOTE** The **non-authentication and non-encryption** level is not secure. It is recommended that you select the **authentication and non-encryption** or **authentication and encryption** level.
Authentication mode	Authentication mode.	The value can be: • md5 • sha **NOTE** The **md5** authentication mode is not secure. It is recommended that you select the **sha** authentication mode.
Authentication password	Authentication password for SNMPv3 users.	The value is a string of 8 to 64 characters.
Confirm authentication password	Password for confirming that SNMPv3 users are authenticated.	-
Encryption mode	Encryption mode for PDU in a packet.	The value can be: • aes128 • des56 **NOTE** The **des56** encryption mode is not secure. It is recommended that you select the **aes128** encryption mode.
Encryption password	Encryption password for the PDU part in a packet.	The value is a string of 8 to 64 characters.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
Confirm Encryption password	Password for confirming that the PDU part in a packet is encrypted.	-
ACL name	ACL that limits the device group management rights of the NMS.	-

Modifying a group

a. Choose **System Management** > **SNMP** > **Community/Group Management**.

b. In the **Group/User** area, click  corresponding to the group you want to modify.

c. In the dialog box that is displayed, set parameters listed in **Table 2-189**. The parameter **Group Name** cannot be modified.

d. Click **OK**.

The **Group/User** area is displayed and the information about the group changes in the list.

Modifying a user

a. Choose **System Management** > **SNMP** > **Community/Group Management**.

b. Click  next to **Group Name** to view users in the group.

c. In the **Group/User** area, click  corresponding to the group whose users you want to modify.

d. In the dialog box that is displayed, set parameters listed in **Table 2-190**. The parameters **Group Name** and **User Name** cannot be modified.

e. Click **OK**.

The **Group/User** area is displayed and the information about the user changes in the list.

Deleting a user

a. Choose **System Management** > **SNMP** > **Community/Group Management**.

b. Click  next to **Group Name** to view users in the group.

c. In the **Group/User** area, click  corresponding to the user you want to delete.

d. In the **Information** dialog box that is displayed, click **OK**.

The deleted user is not displayed in the **Group/User** area. To delete more users, repeat the preceding steps.

Deleting a group

Copyright © Huawei Technologies Co., Ltd.

a. Choose **System Management** > **SNMP** > **Community/Group Management**.

b. In the **Group/User** area, select the check box next to the group you want to delete, or select the check box next to **Group Name** to select all groups.

c. Click **Delete**.

d. In the **Information** dialog box that is displayed, click **OK**.

The deleted group is not displayed in the **Group/User** area, and users in this group are deleted at the same time.

----End

2.19.5.3 MIB View

Context

A MIB view is an abstract set of all managed objects. The NMS manages the device by reading and writing the managed objects in the MIB. A MIB view defines management information included and excluded in this MIB view, which is implemented in the following ways:

- When the NMS cannot manage a small number of MIB objects on the managed device or the NMS needs to be disabled from managing some MIB objects in the existing MIB view, exclude these MIB objects.
- When the NMS cannot manage most MIB objects on the managed device or the NMS needs to be enabled to manage some new MIB objects in the existing MIB view, add these MIB objects.

NOTE

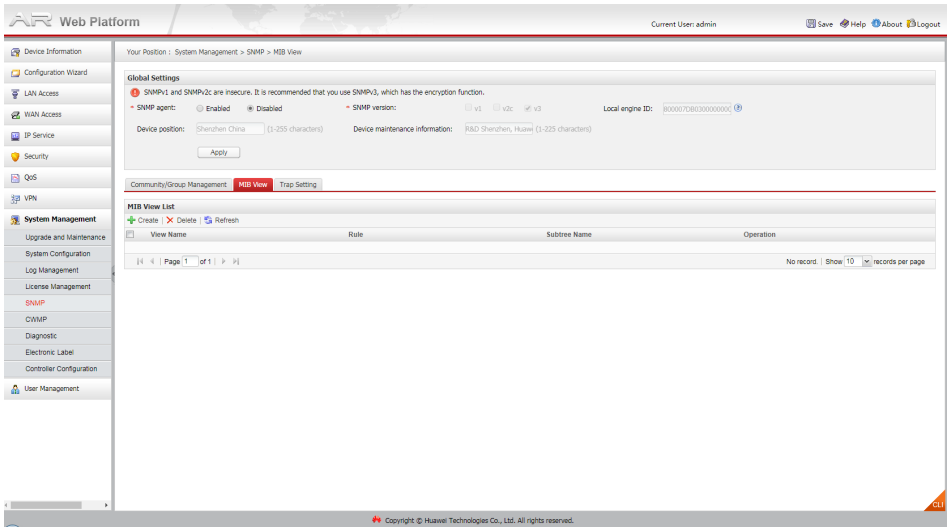
The web platform supports a maximum of 20 rules in all MIB views among which 4 rules are configured in the default MIB view. You can add only 16 rules. When the total number of rules exceeds 20, the system prompts you with a message.

Procedure

- Creating a MIB view

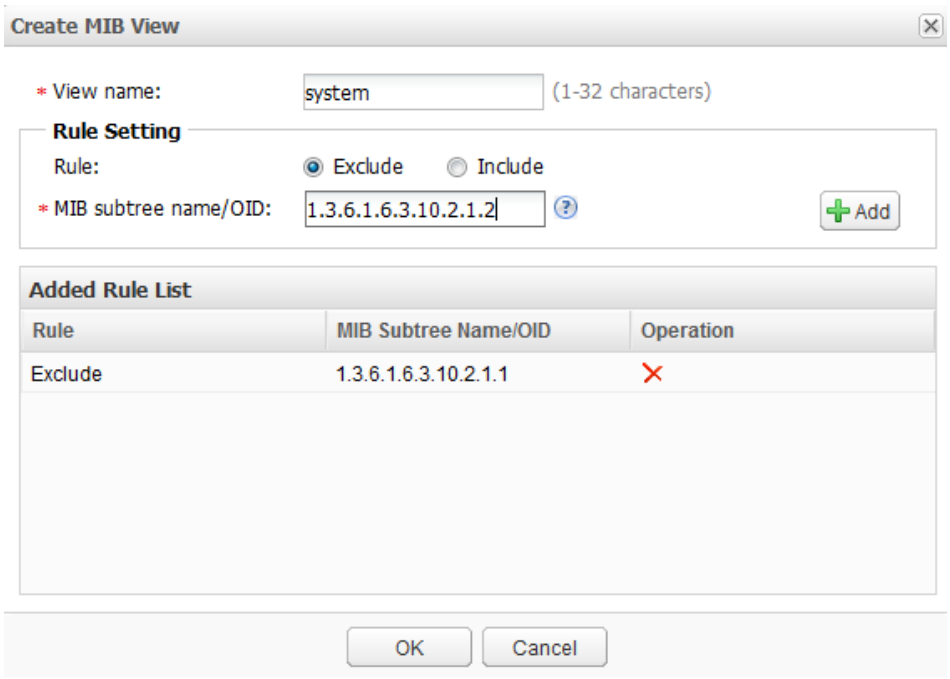
  a. Choose **System Management** > **SNMP** > **MIB View**, as shown in **Figure 2-313**.

Figure 2-313 MIB View page



b. Click **Create** in the **MIB View List** area, as shown in **Figure 2-314**.

Figure 2-314 Creating a MIB view



c. Perform the following operations in the **Create MIB View** dialog box.

Creating a rule

i. Enter a MIB view name in the **View name** text box.

ii. Set **Rule** to configure the method of processing MIB sub-trees in the MIB view. The options are **Exclude** and **Include**.

iii. Enter a MIB subtree name or IOD in the **MIB subtree name/OID** test box. Click **Add**.

The new rule is displayed in the **Added Rule List** area. To create multiple rules, repeat the preceding steps.

 Copyright © Huawei Technologies Co., Ltd.

Deleting a rule

i. Click  next to a rule in the **Added Rule List** area.

The rule is deleted from the rule list. To delete multiple rules, repeat the preceding step.

d. Click **OK**.

New MIB views are displayed on the **MIB View** tab page. You can click  to view information about a MIB view. To create multiple MIB views, repeat the preceding steps.

- Modifying a MIB view
  a. Choose **System Management** > **SNMP**.
  b. Click  of a MIB view in the MIB view list.
  c. Perform the following operations in the **Modify MIB View** dialog box that is displayed. The parameter **View name** cannot be modified.

     Creating a rule

     i. Set **Rule** to configure the method of processing MIB sub-trees in the MIB view. The options are **Exclude** and **Include**.
     ii. Enter a MIB subtree name or IOD in the **MIB subtree name/OID** test box. Click **Add**.

     The new rule is displayed in the **Added Rule List** area. To create multiple rules, repeat the preceding steps.

     Deleting a rule

     i. Click  next to a rule in the **Added Rule List** area.

     The rule is deleted from the rule list. To delete multiple rules, repeat the preceding step.

  d. Click **OK**.

     The **MIB View** tab page is displayed. You can click  to view the configuration change.

- Deleting a MIB view
  a. Choose **System Management** > **SNMP** > **MIB View**.
  b. Select the check box of a MIB view in the MIB view list or select the check box next to **View Name** to select all MIB views.
  c. Click **Delete**.
  d. In the **Information** dialog box that is displayed, click **OK**.

     The MIB view is deleted.

----End

2.19.5.4 Trap Setting

 Copyright © Huawei Technologies Co., Ltd.

Context

A managed device sends a trap to the NMS so that the administrator can discover exceptions of the device. The NMS receives a trap from a managed device without confirmation.

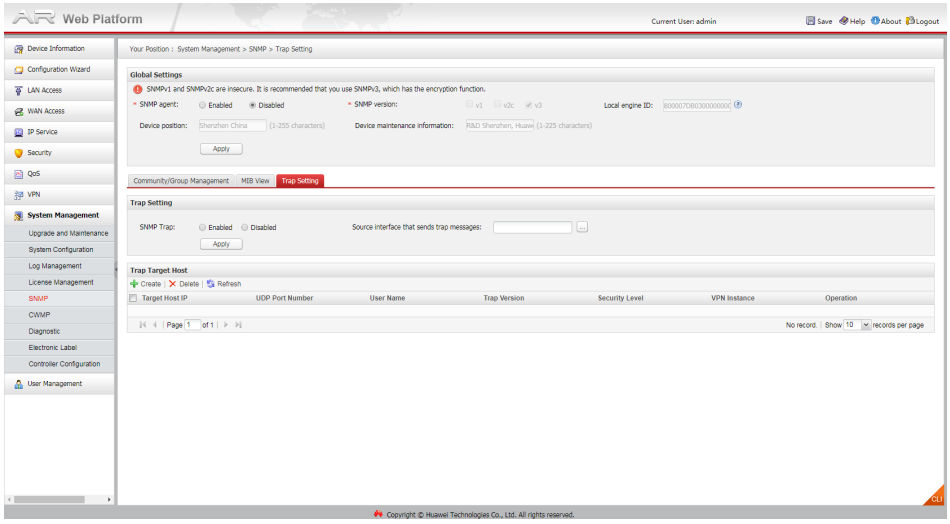
NOTE

The web platform supports 20 trap destination hosts. When the number of configured trap destination hosts exceeds that limited by the web platform, a dialog box is displayed indicating that the number of trap destination hosts reaches the maximum.

Procedure

- Trap setting
  a. Choose **System Management** > **SNMP** > **Trap Setting**, as shown in **Figure 2-315**.

  Figure 2-315 Trap Setting page

  b. Set **SNMP Trap** to **Enable** or **Disable**.
  c. Click the button next to the **Source interface that sends trap messages** text box to select an interface for sending Trap messages.

     To delete an incorrect source interface or restore the default setting, move the cursor to the **Source interface that sends trap messages** text box, and press **Backspace**.
  d. In the **Select Interface** dialog box that is displayed, select an interface in either of the following ways:

     - In the interface list, select the option button next to an interface.
     - In the **interface-name** text box, enter an interface name, and click **Search**. Select the option button next to an interface from the listed interfaces.

     When there are several interfaces, use the first method to select an interface. When there are many interfaces in the list, use the second method to select an interface.

 Copyright © Huawei Technologies Co., Ltd.

e. Click **Apply**.

The **Trap Setting** tab page is displayed, and information in the **Source interface that sends trap messages** text box changes to the specified interface.

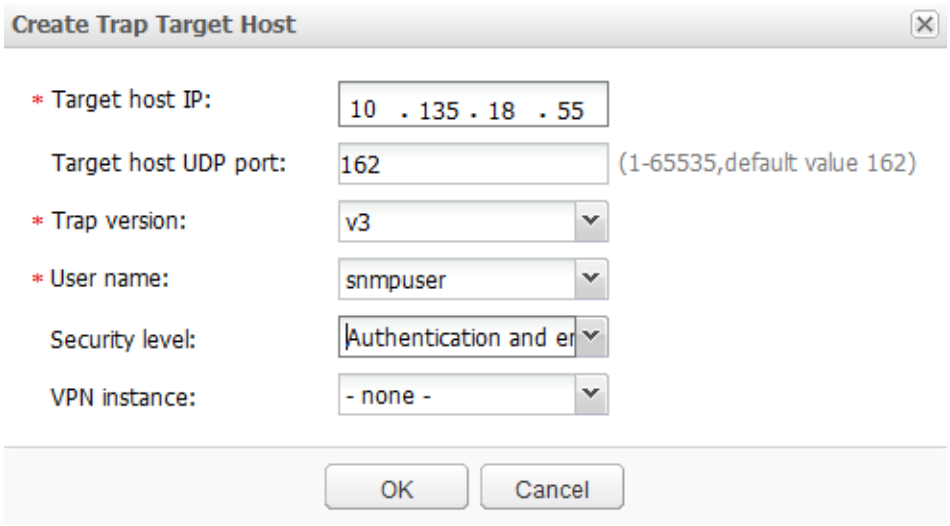
- Trap target host

  Creating a trap destination host

  a. Choose **System Management** > **SNMP** > **Trap Setting**.

  b. In the **Trap Target Host** area, click **Create**, as shown in **Figure 2-316**.

  Figure 2-316 Creating a trap target host

  c. In the **Create Trap Destination Host** dialog box that is displayed, set parameters listed in **Table 2-191**.

  d. Click **OK**.

  The created trap destination host is displayed in the **Trap Target Host** area. To create more trap destination hosts, repeat the preceding steps.

Table 2-191 Host parameters

Parameter	Description	Value
Destination host IP	IP address of the destination host.	-
Destination host UDP port	Port number used to receive Trap messages on the destination host.	The value is an integer that ranges from 1 to 65535. The default value is 162.
Trap version	SNMP version mapping the trap.	Versions include: • v1 • v2c • v3

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
User name	Community name and group name. • When the trap version is v1 or v2c, select the community name. • When the trap version is v3, select the group name.	-
Security level	Security level configured for SNMPv3.	Security levels include: • Non-authentication and non-encryption • Authentication and non-encryption • Authentication and encryption
VPN instance	Name of a VPN instance.	-

Modifying a trap destination host

a. Choose **System Management** > **SNMP** > **Trap Setting**.

b. In the **Trap Target Host** area, click  corresponding to the trap destination host you want to modify.

c. In the dialog box that is displayed, set parameters listed in **Table 2-191**. The parameter **Destination Host IP** cannot be modified.

d. Click **OK**.

The **Trap Target Host** area is displayed and the information about the trap destination host changes in the list.

Deleting a trap destination host

a. Choose **System Management** > **SNMP** > **Trap Setting**.

b. In the **Trap Target Host** area, select the check box next to the trap destination host you want to delete, or select the check box next to **Destination Host IP** to select all trap destination hosts.

c. Click **Delete**.

d. In the **Information** dialog box that is displayed, click **OK**.

The deleted trap destination host is not displayed in the **Trap Target Host** area.

----End

2.19.6 CWMP

Copyright © Huawei Technologies Co., Ltd.

Context

When a router functions as a customer premises equipment (CPE), you can enable CPE WAN Management Protocol (CWMP) on the auto-configuration server (ACS) to remotely manage the CPE. A connection can be initiated by a CPE or an ACS.

- Connection initiated by a CPE

  After the CPE sends an Inform message containing a uniform resource locator (URL) address to the ACS, the ACS authenticates the CPE by using the user name and password. After being authenticated, the CPE can set up a connection with the ACS.

- Connection initiated by an ACS

  After the ACS sends a Hypertext Transfer Protocol (HTTP) packet containing the IP address of the CPE, the CPE authenticates the ACS by using the user name and password. After being authenticated, the ACS can set up a connection with the CPE. This connection initiation mode can be used only when the ACS has communicated with the CPE at least once through a session that the CPE initiates.

The ACS's URL is in the HTTP or Hypertext Transfer Protocol Secure (HTTPS) format. The HTTPS format can ensure the communication security and data integrity between the ACS and CPE.

NOTE

The AR120 series (except AR129CV, AR129CVW and AR129CGVW-L) do not support CWMP.

Procedure

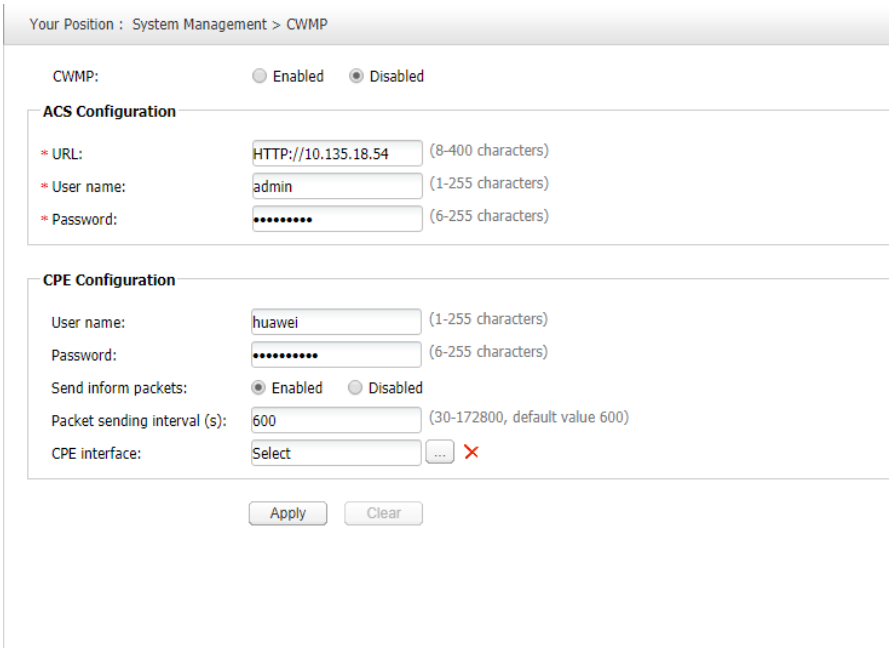
- Configuring CWMP
  a. Choose **System Management** > **CWMP**.
  b. Set **CWMP** to **Enable**.
  c. Configure the ACS.

     When the ACS's URL is in the HTTP format:

     i. Enter a URL of the HTTP format in the **URL** text box, as shown in **Figure 2-317**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-317 Configuring a URL in the HTTP format

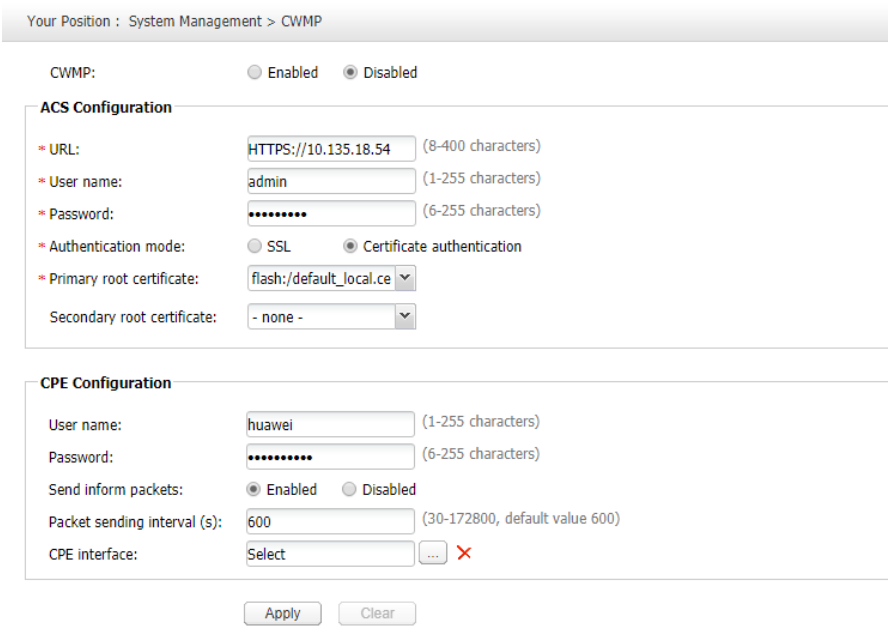


ii. Enter the user name and password in the **User name** and **Password** test boxes.

When the ACS's URL is in the HTTPS format:

i. Enter a URL of the HTTPS format in the **URL** text box.
In this scenario, URL authentication must be configured.

Figure 2-318 Configuring a URL in the HTTPS format



ii. Enter the user name and password in the **User name** and **Password** test boxes.

 Copyright © Huawei Technologies Co., Ltd.

iii. Set **Authentication mode**.

iv. When **Authentication mode** is set to SSL, select an SSL policy from the **SSL** drop-down list box.

v. When **Authentication mode** is set to **Certificate authentication**, select **Upload The Certificate** from the **Primary root certificate** drop-down list box. Click **Browse** in the displayed **Upload The Certificate** dialog box, select the certificate to upload, and click **Upload**.

To use a certificate that has been uploaded to the device, select the certificate from the **Primary root certificate** drop-down list box.

vi. (Optional) When **Authentication mode** is set to **Certificate authentication**, select **Upload The Certificate** from the **Secondary root certificate** drop-down list box. Click **Browse** in the displayed **Upload The Certificate** dialog box, select the certificate to upload, and click **Upload**.

To use a certificate that has been uploaded to the device, select the certificate from the **Secondary root certificate** drop-down list box.

d. (Optional) Configure the CPE.

i. Enter the user name and password in the **User name** and **Password** test boxes.

ii. Set **Send inform packets** to **Enable**.

A CPE can set up a connection with the ACS in Inform remote procedure call (PRC) mode. By default, the CPE does not send Inform packets periodically.

iii. Set **Packet sending interval (s)**.

NOTE

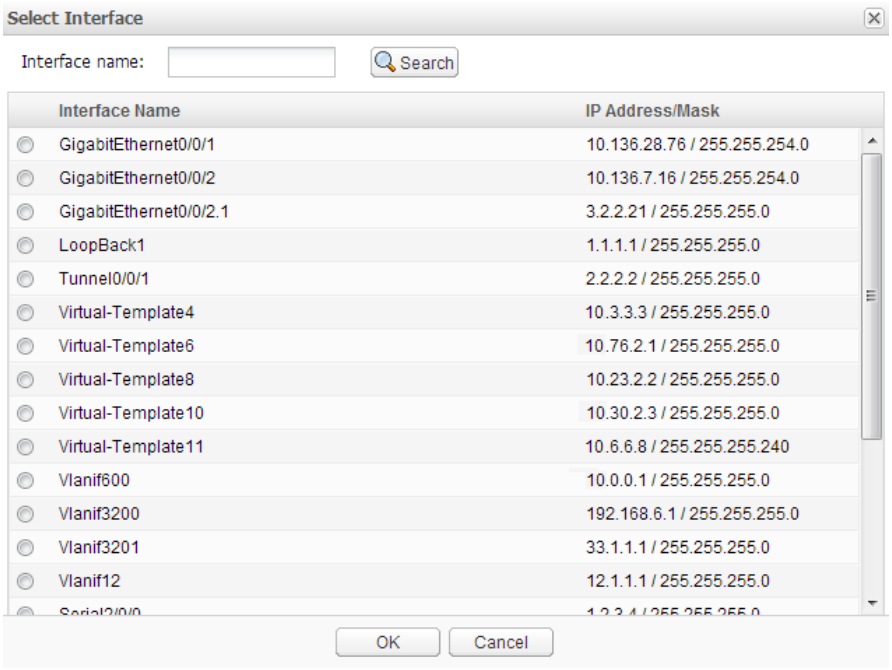
V200R010C00: The value is an integer that ranges from 30 to 86400, in seconds.

V200R010C10 and later versions: The value is an integer that ranges from 30 to 172800, in seconds.

iv. Click the option icon of **CPE interface** to configure the CPE interfaces, as shown in **Figure 2-319**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-319 Configuring the CPE interfaces



v. In the **Select Interface** dialog box, select source interfaces in either of the following ways:
   - Select the option buttons of required interfaces in the interface list.
   - Enter the interface name in the **CPE interface** text box and click **Search**. Select the option buttons of required interfaces in the interface list.

vi. Click **OK**.

Selected CPE interfaces are displayed in the **CPE interface** test box.

e. Click **Apply**.

f. In the **Prompt** dialog box that is displayed, click **OK**.

- Deleting the CWMP configuration
  a. Choose **System Management** > **CWMP**.
  b. Click **Clear** in the **CWMP** page.
  c. In the **Prompt** dialog box that is displayed, click **OK**.
  The **CWMP** page is displayed, and the CWMP configuration is deleted.

----End

Copyright © Huawei Technologies Co., Ltd.

Configuration Parameters

Table 2-192 CWMP configuration parameters

Parameter	Description
ACS	Set ACS parameters. The ACS uses TR-069 to remotely manage the CPE. • URL: URL of the ACS. The URL is in the format of http://host:port or https://host[:port]/path. Assume that the IP address of the ACS is 192.168.10.2. The URL is http://192.168.10.2:80. • User name: user name used to connect the CPE to the ACS. • Password: password used to connect the CPE to the ACS. • SSL: SSL policy used for HTTPS authentication. • Certificate authentication: certification used for HTTPS authentication. **NOTE** The connection between the ACS and the CPE is set up only after the ACS and CPE are authenticated by each other.
CPE	Set CPE parameters. The ACS uses TR-069 to remotely manage the CPE. • User name: user name used to connect the ACS to the CPE. • Password: password used to connect the ACS to the CPE. • Send inform packets: whether to enable or disable the CPE to send or from sending Inform messages to the ACS. A CPE can connect to an ACS automatically by sending an Inform message. • Packet sending interval (s): interval at which a CPE sends Inform messages.

2.19.7 Diagnostic

2.19.7.1 Ping

Context

A ping test checks whether a destination host is reachable to determine network connectivity to the host.

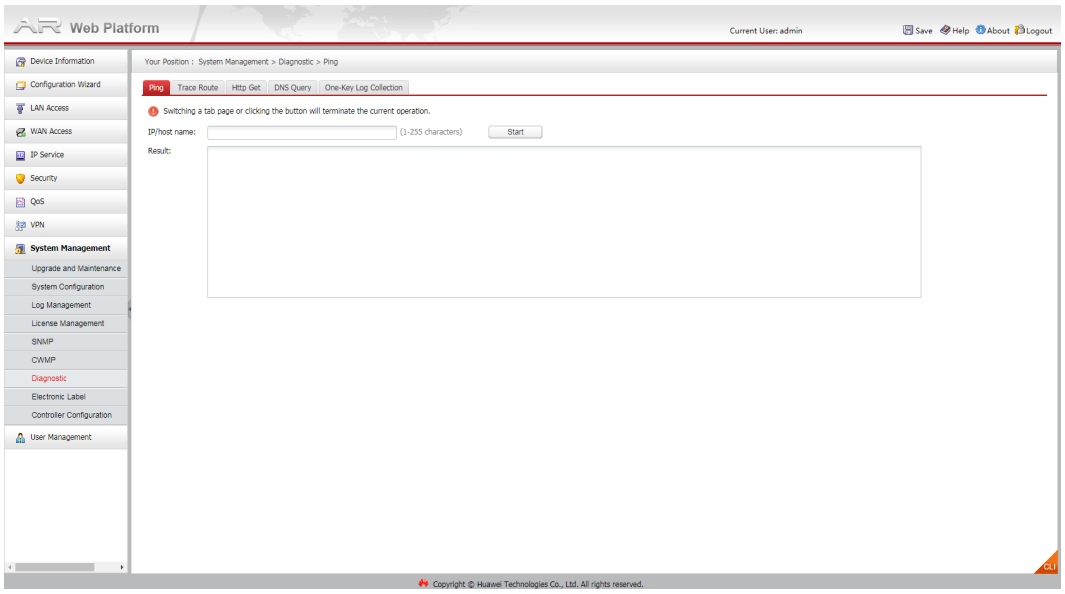
When a ping operation is complete, the result is displayed in the **Result** text box.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Choose **System Management** > **Diagnostic Tools** > **Ping**, as shown in **Figure 2-320**.

Figure 2-320 Ping page



Step 2 In the **IP/host name** text box, enter the destination IP address or host name.

Step 3 Click **Start**.

----End

2.19.7.2 Trace Route

Context

A trace route test tracks the forwarding path from a source device to a destination device. When a network failure occurs, you can use the tracert tool to locate the fault. You can specify a destination IP address or host name.

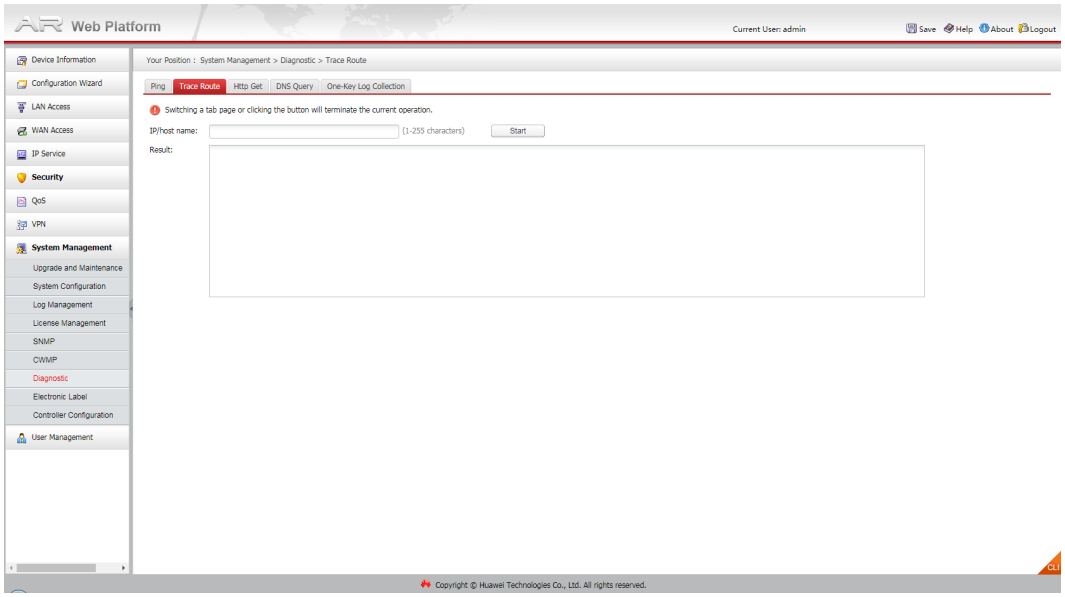
After the tracert operation is complete, the result is displayed in the **Result** text box.

Procedure

Step 1 Choose **System Management** > **Diagnostic Tools** > **Trace Route**, as shown in **Figure 2-321**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-321 Trace Route page



Step 2 In the **IP/host name** text box, enter the destination IP address or host name.

Step 3 Click **Start**.

----End

2.19.7.3 Http Get

Context

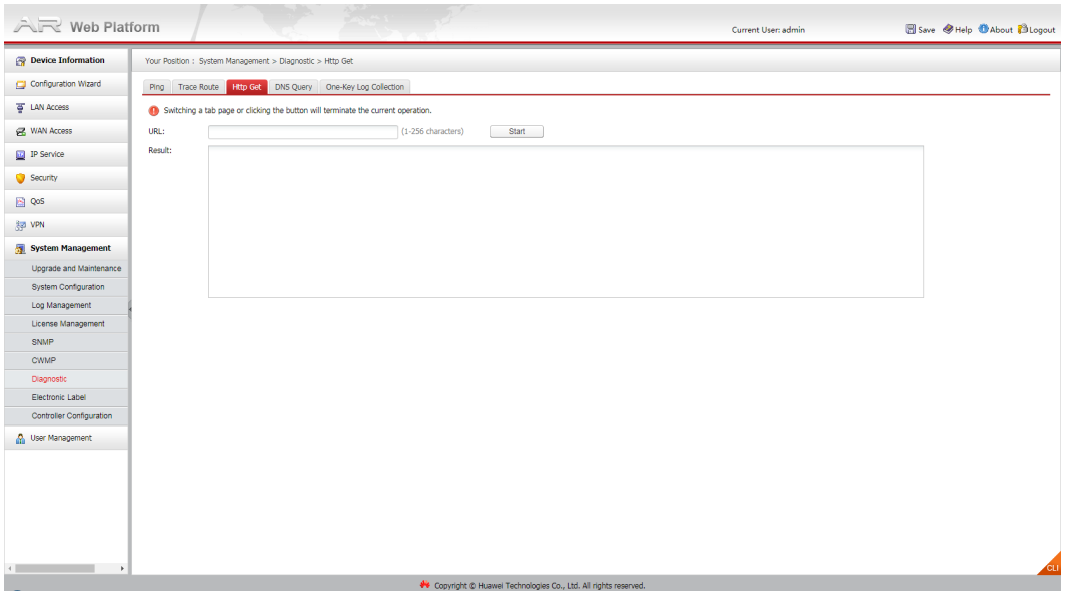
You can use HTTP Get to check whether the host with the specified URL provides the HTTP service.

When an HTTP Get operation is complete, the result is displayed in the **Result** text box.

Procedure

Step 1 Choose **System Management** > **Diagnostic Tools** > **Http Get**, as shown in **Figure 2-322**.

Figure 2-322 Http Get page



Step 2 In the **URL** text box, enter the website address.

Step 3 Click **Start**.

----End

2.19.7.4 DNS Query

Context

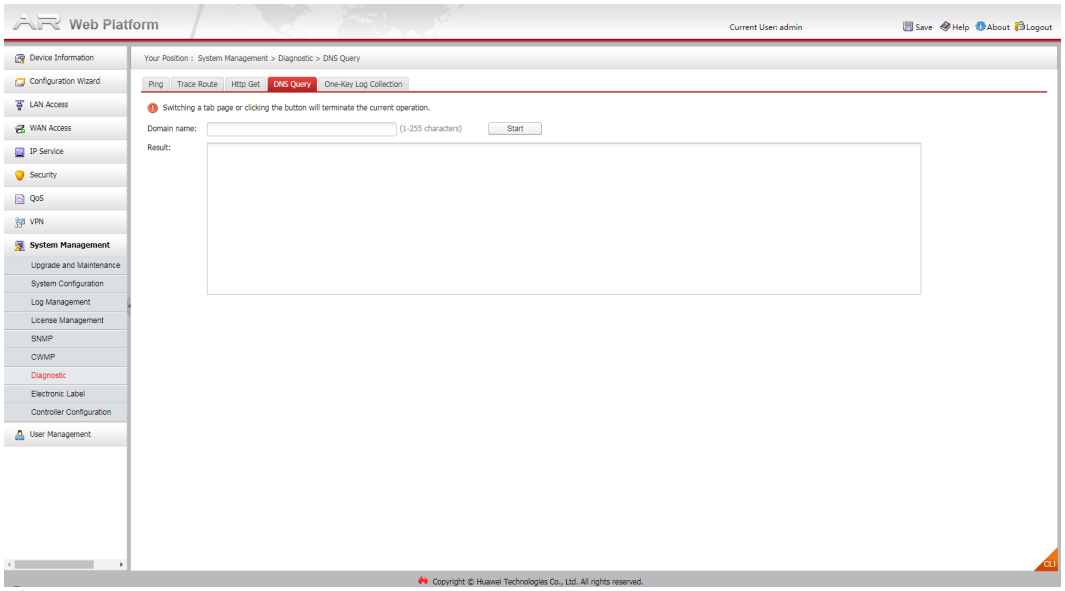
The DNS query allows you to obtain the IP address mapped to a specified domain name.

After the DNS query operation is complete, the result is displayed in the **Result** text box.

Procedure

Step 1 Choose **System Management** > **Diagnostic Tools** > **DNS Query**, as shown in **Figure 2-323**.

Figure 2-323 DNS Query page



Step 2 In the **Domain name** text box, enter the domain name.

Step 3 Click **Start**.

----End

2.19.7.5 One-Key Log Collection

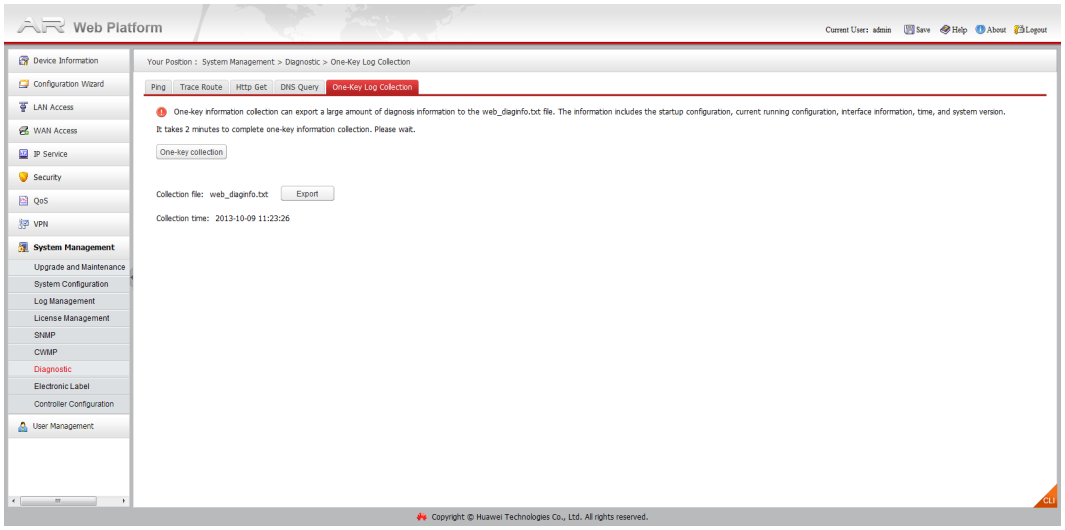
Context

The one-key log collection function exports a large amount of diagnosis information running on the device to the **web_diaginfo.txt** file. The information includes startup configuration, current configuration, interface information, time, and system version.

Procedure

Step 1 Choose **System Management** > **Diagnostic** > **One-Key Log Collection**.

Figure 2-324 One-Key Log Collection



Step 2 Click **One-Key Collection**. In the **Information** dialog box that is displayed, click **OK**.

Step 3 Click **Export** to export the current **web_diaginfo.txt** file.

The **web_diaginfo.txt** file can be exported only when the collection is completed.

----End

2.19.7.6 Packet Capture

Context

The packet capture function exports service packets matching specified rules to the **web_packet.cap** file.

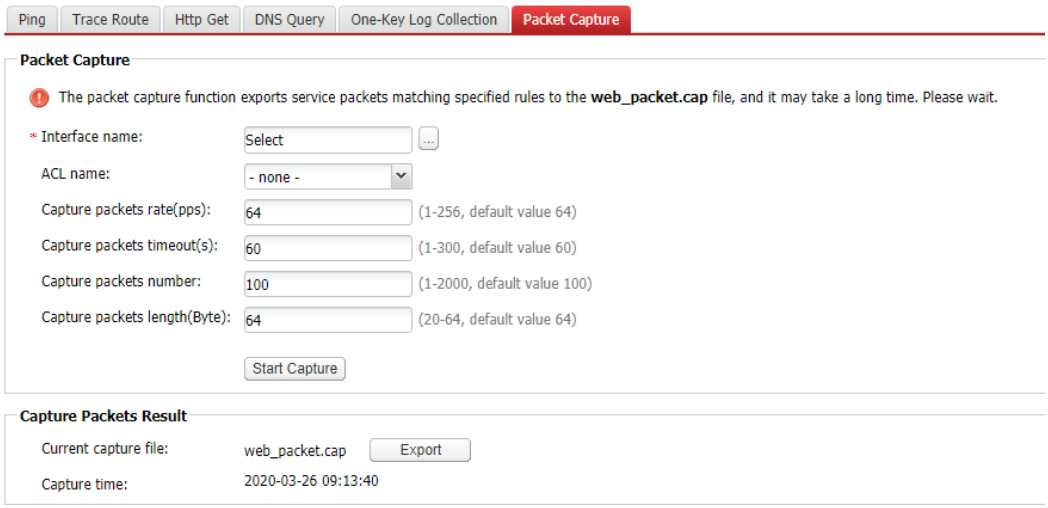
NOTE

This function is supported in V200R010C10 and later versions.

Procedure

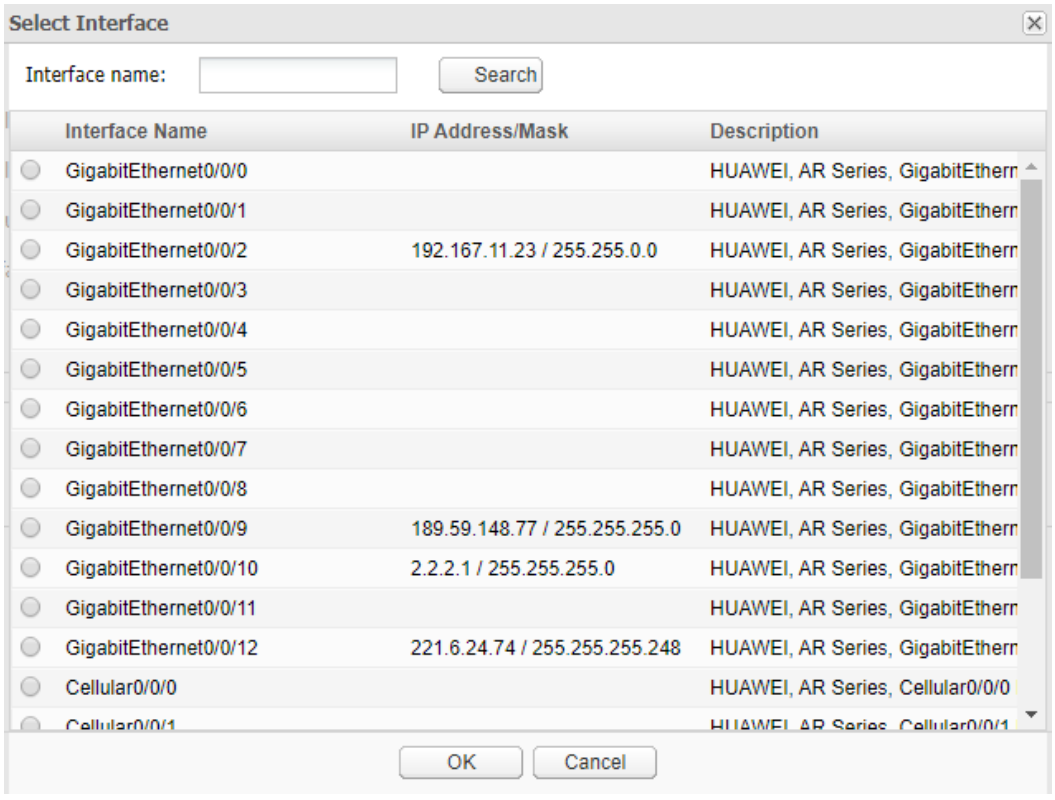
Step 1 Choose **System Management** > **Diagnostic** > **Packet Capture**. The **Packet Capture** tab page is displayed, as shown in **Figure1**.

Figure 2-325 Packet Capture



Step 2 Click ... next to **Interface name** and select the interface to be connected, as shown in **Figure2**.

Figure 2-326 Select Interface



Step 3 In the **Select Interface** dialog box, select an interface in either of the following ways:

- Select the interface from the interface list.
- Enter the interface name in the **Interface name** text box and click **search**. Then select the interface from the interface list.

 Copyright © Huawei Technologies Co., Ltd.

Step 4 Click **OK**. If the operation is successful, the system returns to the **Packet Capture** tab page and the information in the **Interface name** text box changes to the specified interface.

Step 5 In **Packet Capture**, set parameters, as shown in **Figure3**. For detailed parameter descriptions, see **Table1**.

Figure 2-327 Packet Capture

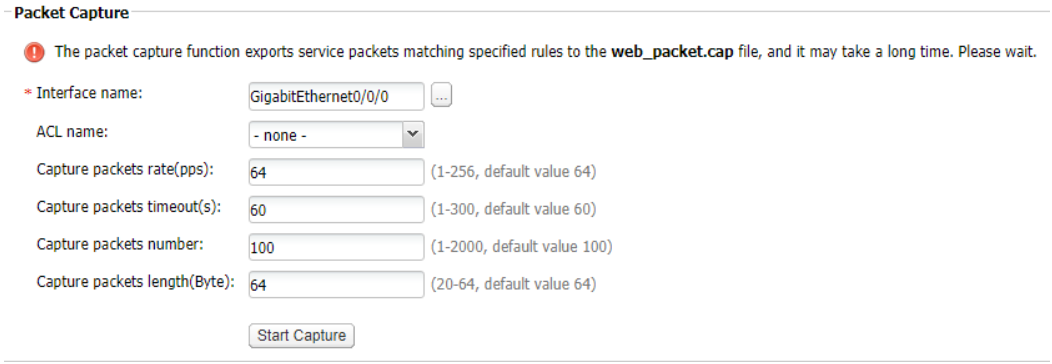
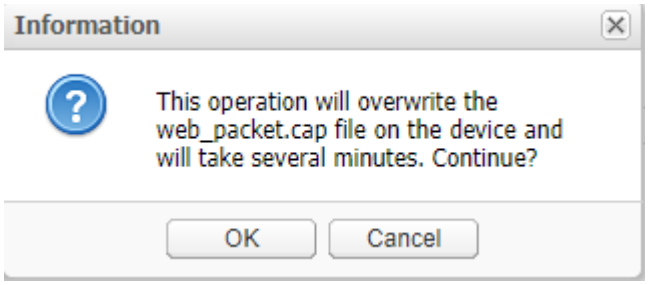


Table 2-193 Packet Capture parameters

Parameter	Description
Interface name	Specifies the interface for capturing packets.
ACL name	Name of an ACL. Packets matching the specified ACL will be captured.
Capture packets rate(pps)	Rate at which packets are captured.
Capture packets timeout(s)	Timeout period of packet capture. After the timeout period expires, packet capture is automatically disabled.
Capture packets number	After a specified number of packets are captured, packet capture is automatically disabled.
Capture packets length(Byte)	Length of each packet displayed on a terminal or stored in the storage medium.

Step 6 Click **Start Capture**. The **Information** dialog box shown in **Figure4** is displayed.

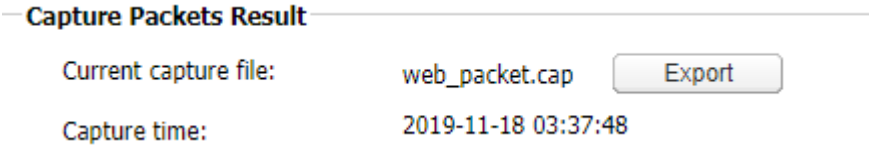
Figure 2-328 Packet capture information



Copyright © Huawei Technologies Co., Ltd.

Step 7 Click **OK**. The packet capture result is displayed in **Capture Packets Result**, as shown in **Figure5**.

Figure 2-329 Capture Packets Result



Step 8 Click **Export** to export the **web_packet.cap** file.

NOTE

The **web_packet.cap** file can be exported only when the packet capture task is successfully completed.

----End

2.19.8 Electronic Label

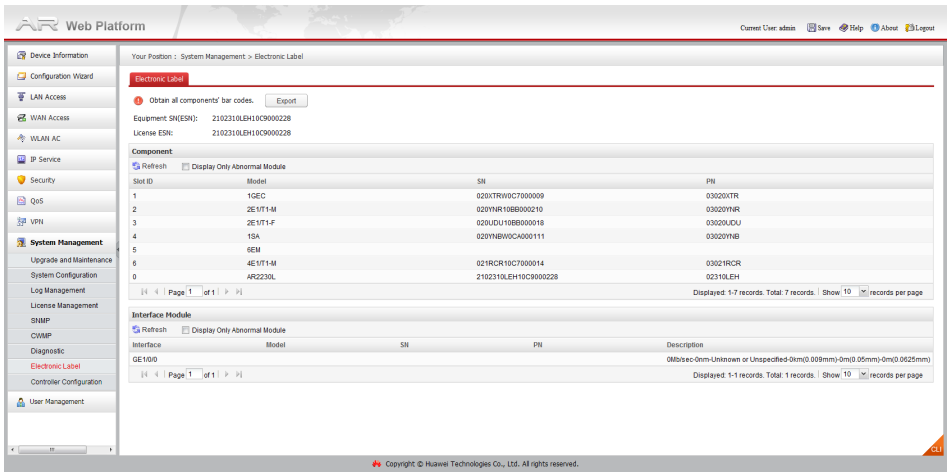
Context

Users can view e-labels based on the component or interface, and export electronic labels of all components.

Procedure

- Electronic Label
  a. Choose **System Management** > **Electronic Label**, as shown in **Figure 2-330**.

Figure 2-330 electric labels



----End

2.19.9 Configuring Controller

Context

You can use the web page to specify the IP address, port number, and VPN instance of the controller so that the AR can interwork with the controller.

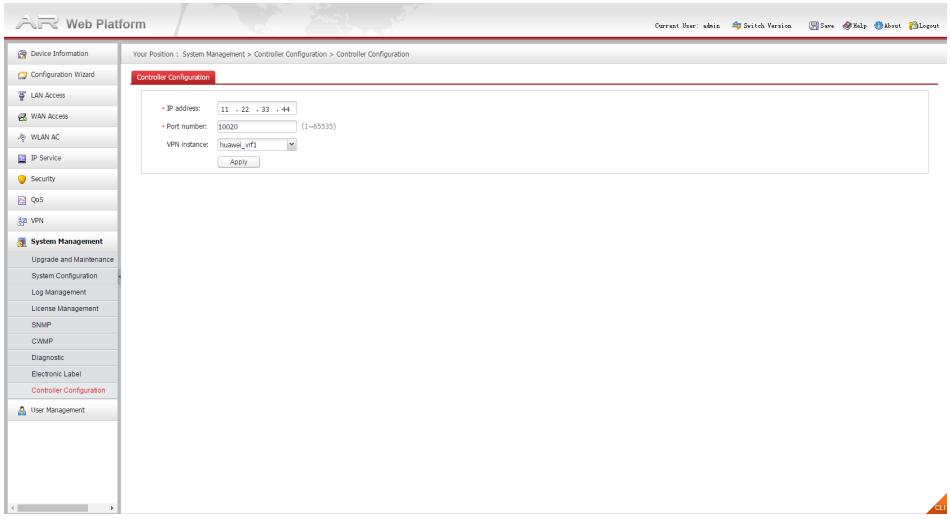
NOTE

Only AR3670, AR169-P-M9, AR169W-P-M9, AR161G-Lc, and AR161FW-P-M5 support controller configuration.

Procedure

- Configure the controller.
  a. Choose **System Management** > **Controller Configuration**, as shown in **Figure 2-331**.

  Figure 2-331 Controller Configuration

  b. Enter the IP address, port number, and VPN instance of the controller in **IP address**, **Port number**, and **VPN instance**.
  c. Click **Apply**.

----End

2.20 User Management

2.20.1 User Management

Context

An administrator can create, modify, and delete local users on the **User Management** tab page.

Copyright © Huawei Technologies Co., Ltd.

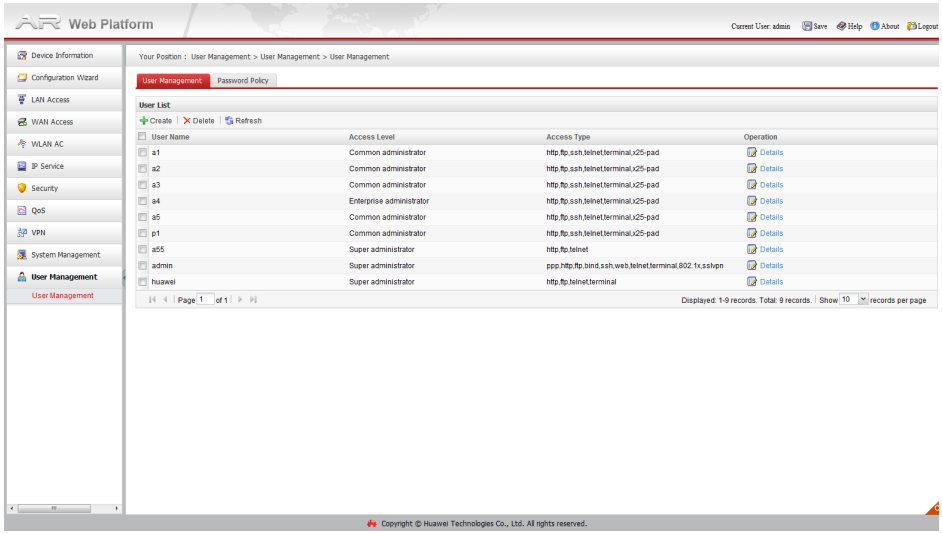
NOTE

Only a super administrator can add and delete local user accounts as well as view administrator details.

Procedure

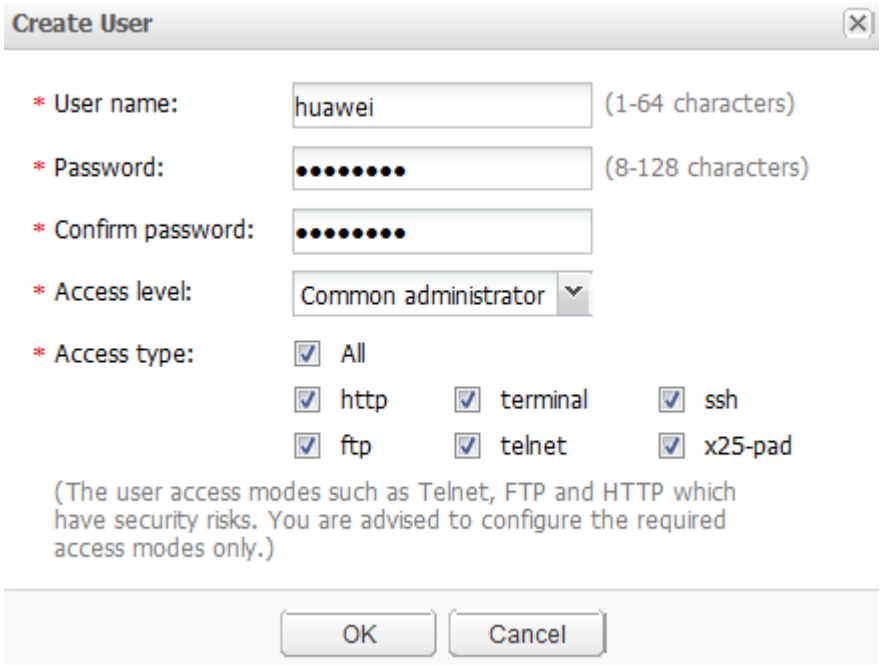
- Creating a local user
  a. Choose **User Management** > **User Management**, as shown in **Figure 2-332**.

Figure 2-332 User Management page



  b. Click **Create** in the **User List** area, as shown in **Figure 2-333**.

Figure 2-333 Creating users



 Copyright © Huawei Technologies Co., Ltd.

c. Set parameters in the **Create User** dialog box. **Table 2-194** describes the parameters.

Table 2-194 Local user parameters

Parameter	Description
User name	Name of a local user.
Password	Password of a local user. **NOTE** A simple password brings security risks. It is mandatory that you change the password to a complicated one after logging in to the web network management system using the default account. A password should consist of at least 8 characters, and contain at least two types of the following: lowercase letters, uppercase letters, numerals, special characters (such as ! $ # %). The password cannot contain spaces and single quotation marks ('). In addition, the password cannot be the same as the user name or the mirror user name.
Confirm password	Confirmed password of a local user. The value must be the same as the value of **Password**.
Access level	Access level of a local user. Four local user levels are defined (in ascending order): common user, common administrator, enterprise administrator, super administrator.
Access type	Access type of a local user. **NOTE** By default, the access type of the local account is empty. You can select the access type as needed. The new user supports management user access modes such as Telnet, FTP and HTTP which have security risks. You are advised to configure the required access modes only.

d. Click **OK**.

A user is added to the user list.

e. To create multiple users, repeat this procedure.

- Modifying a local user

a. Choose **User Management** > **User Management**.

b. Click  of a local user in user list.

c. Set the related parameters.

Copyright © Huawei Technologies Co., Ltd.

- When a user changes the personal password, the user sets **Old password**, **New password**, **Confirm password**, and **Access type**.
- When a super administrator changes the password of another user, the super administrator sets **New password**, **Confirm password**, **Access level**, and **Access type**.

  NOTE

  After the super administrator changes the password of another user, the user is required to change the password in first login.
- When **Access level** is changed from common user to administrator (common administrator, enterprise administrator, super administrator), the administrator sets **New password**, **Confirm password**.

d. Log out users.

NOTE

Only the users logging in through Telnet or HTTP can be forcibly logged out.

- When the super administrator changes the password, access level, or access type of another user, the system display the dialog box **Are you disconnect the user?**, and **Yes** is selected for the user, the user is forcibly logged out. When the user logs in again, the modification takes effect. If the super administrator has modified the user information but selects **No**, the modification for the user does not take effect until the user logs in again.
- After a super administrator has logged in to multiple pages, if the password, access level, or access type of the super administrator is changed on one page, the system display the dialog box **Are you disconnect the user?**, and **Yes** is selected for the super administrator, the super administrator is still online on the current page, but is logged out of other pages.

e. Click **OK**.

- Deleting a local user

  a. Choose **User Management** > **User Management**.

  b. Select the check boxes of users in the user list or select the check box next to **User Name** to select all users.

  c. Click **Delete**.

  Users are deleted from the user list.

  NOTE

  The administrator cannot delete the online user that has logged in to the web platform.

- Refreshing the user list

  Click **Refresh**.

- Click **Details** to view details about the administrator. **Table 2-195** describes the parameters.

Copyright © Huawei Technologies Co., Ltd.

The **Details** button is displayed for only administrators. Only a super administrator is allowed to view details.

Table 2-195 User Details

Parameter	Description
Original password or not	Whether the administrator is using the original password. The value is **Yes** or **No**.
Recent password change time	Time when the administrator changes the password last time. **NOTE** This parameter is available only when the value of **Original password or not** is **No**.
Password setting time	Time when the administrator changes the password. **NOTE** This parameter is available only when the value of **Original password or not** is **Yes**.
Whether the password has been expired	Whether the password used by the administrator has expired. The value is **Yes** or **No**.

----End

2.20.2 Password Policy

Context

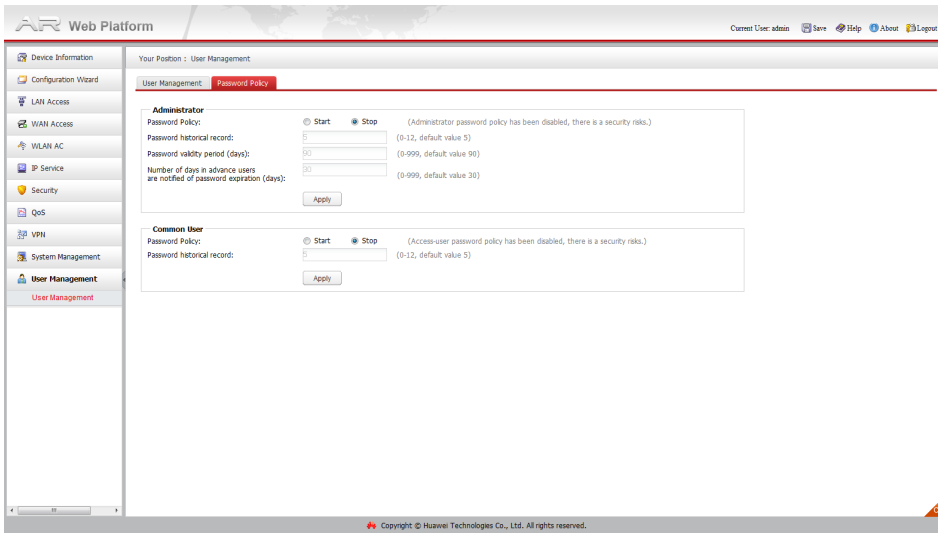
A super administrator can change the password policy to manage the password change period of users.

Procedure

Step 1 Choose **User Management** > **Password Policy**, as shown in **Figure 2-334**.

Copyright © Huawei Technologies Co., Ltd.

Figure 2-334 Password Policy page



Step 2 Manage the password policy in the **Administrator** area.

- Select **Start** to enable the password policy function. This function is disabled by default.
- Set **Password historical record**. The value ranges from 0 to 12. The default value 5 indicates that the new password cannot be the same as any of five history passwords (including the current password).
- Set **Password validity period**. The value ranges from 0 to 999. The default value 90 indicates that the password must be changed within 90 days.
- Set **Number of days in advance users are notified of password expiration**. The value ranges from 0 to 999. The default value 30 indicates that the system prompts the login user to change the password 30 days before the password expiry time.
- Click **Apply**. The modification takes effect.

Step 3 Manage the password policy in the **Common User** area.

- Select **Start** to enable the password policy function. This function is disabled by default.
- Set **Password historical record**. The value ranges from 0 to 12. The default value 5 indicates that the new password cannot be the same as any of five history passwords (including the current password).
- Click **Apply**. The modification takes effect.

----End

2.20.3 Customizing Web Pages

Context

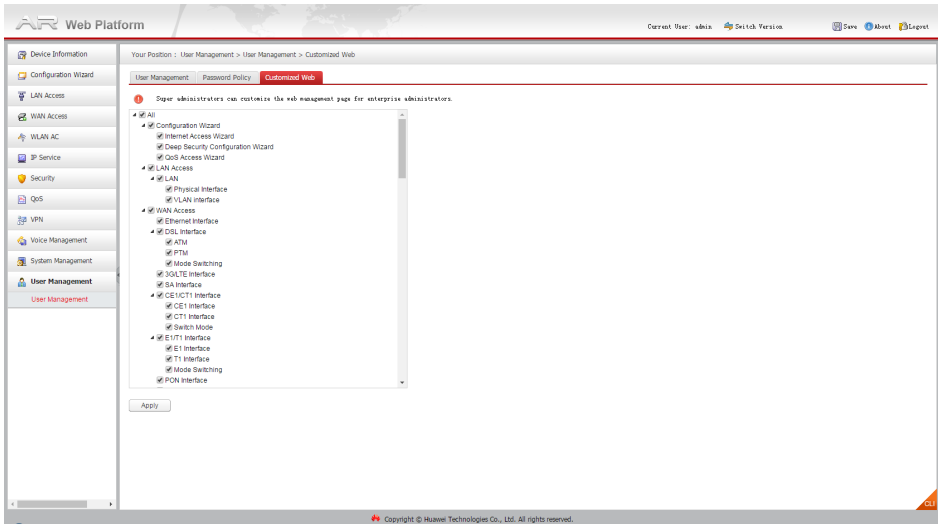
The super administrator can customize web pages that can be viewed by the enterprise administrator.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

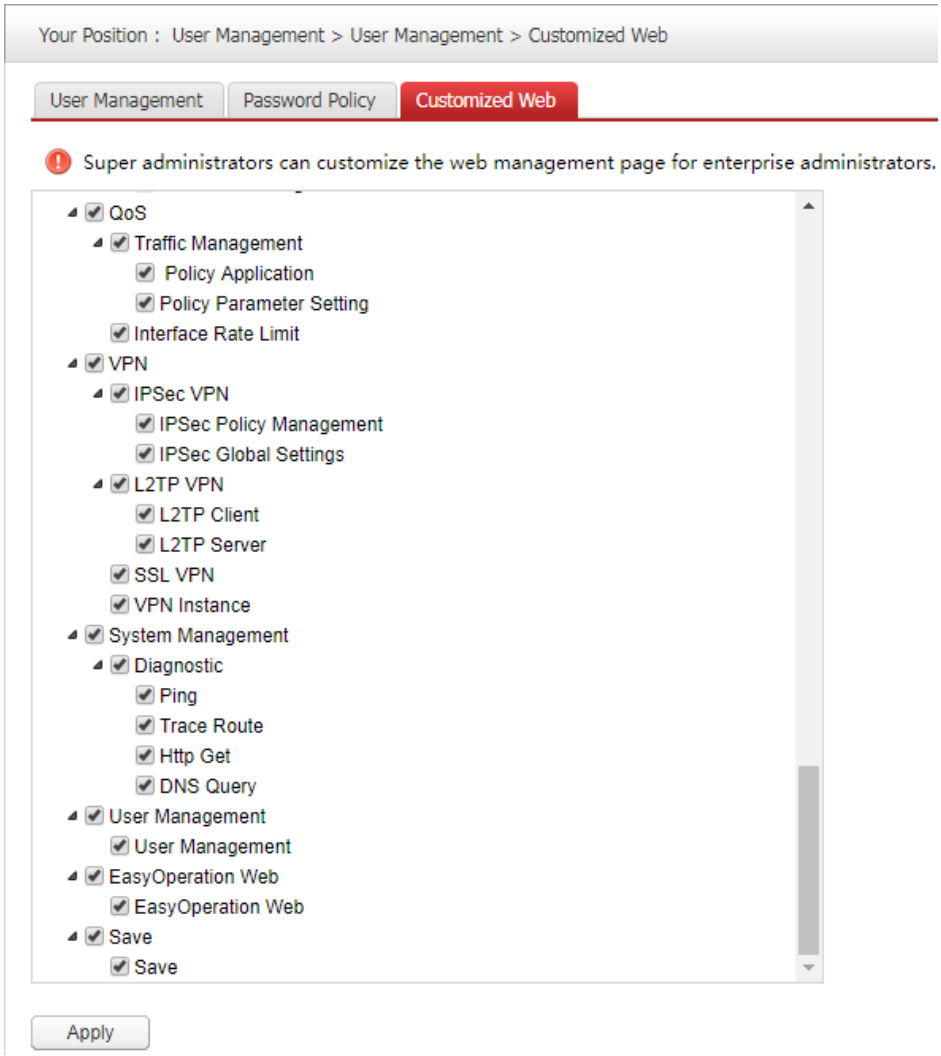
Step 1 Choose **User Management** > **Customized Web**, as shown in **Figure 2-335**.

Figure 2-335 Customizing web pages



Step 2 Select **Save** to enable the enterprise administrator to save configurations, as shown in **Figure 2-336**.

Figure 2-336 Customizing the configuration save function



Step 3 Choose web pages to be displayed and click **Apply**.

----End

 Copyright © Huawei Technologies Co., Ltd.