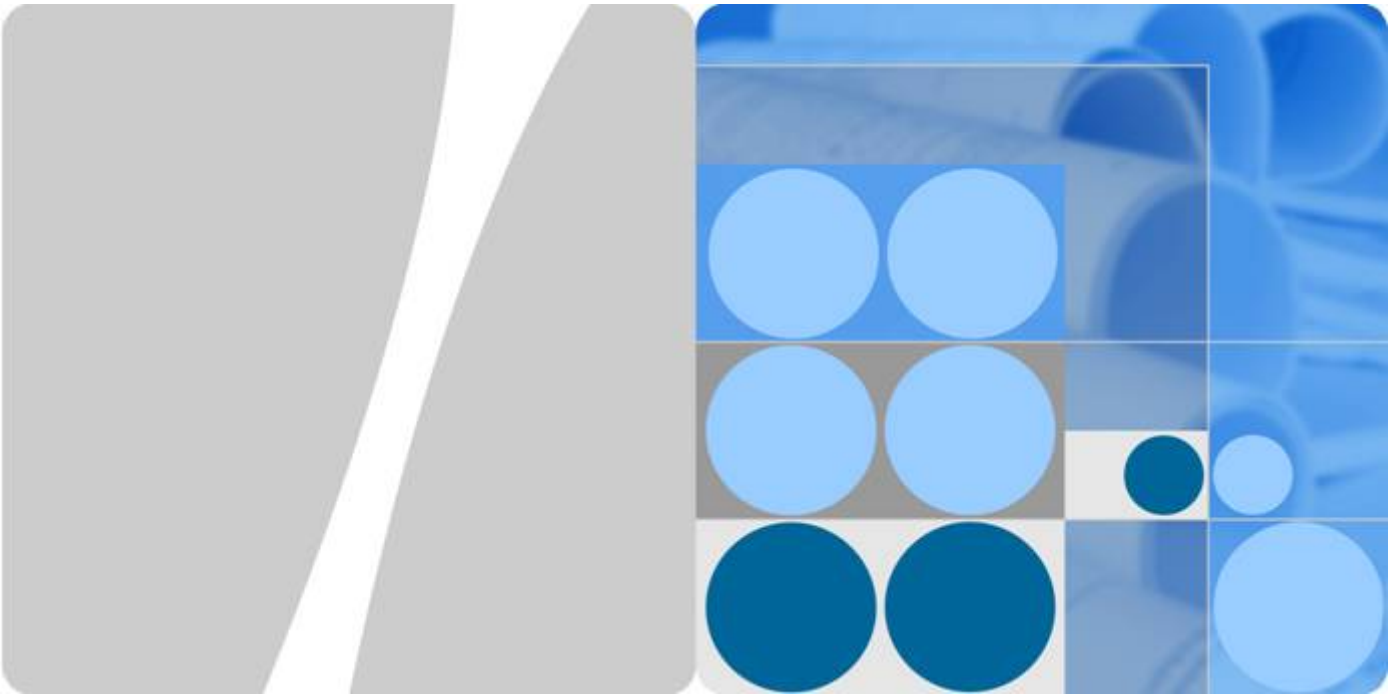


Huawei AR G3 Series Enterprise Routers

V200R002C01

Web System Guide

Issue 01

Date 2012-04-20

HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2012. All rights reserved.

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

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute the warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://www.huawei.com

Email: support@huawei.com

About This Document

Intended Audience

This document describes how to configure and maintain your routers using the web network management client. The web network management system provides a device overview and configuration wizard for you to configure the routers.

This document is intended for:

- Data configuration engineers
- Commissioning engineers
- Network monitoring engineers
- System maintenance engineers

Symbol Conventions

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

Symbol	Description
DANGER	Alerts you to a high risk hazard that could, if not avoided, result in serious injury or death.
WARNING	Alerts you to a medium or low risk hazard that could, if not avoided, result in moderate or minor injury.
CAUTION	Alerts you to a potentially hazardous situation that could, if not avoided, result in equipment damage, data loss, performance deterioration, or unanticipated results.
TIP	Indicates a tip that may help you solve a problem or save time.
NOTE	Provides additional information to emphasize or supplement important points in the main text.

Copyright © Huawei Technologies Co., Ltd.

Change History

Changes between document issues are cumulative. The latest document issue contains all changes made to previous issues.

Issue 01 (2012-04-20)

Initial commercial release.

Copyright © Huawei Technologies Co., Ltd.

Contents

About This Document.....ii

1 Product Function Overview.....1

2 Web NMS Overview.....2

3 Enabling the Web NMS.....3

3.1 Logging In to the Router Through the Console Port.....4
3.2 Setting the Management IP Address of the router.....6
3.3 (Optional) Uploading the Web Page File.....7
3.4 (Optional) Loading the Web Page File.....9
3.5 (Optional) Creating User Accounts for the Web NMS.....9

4 Web Page Introduction.....11

4.1 Logging In to the Web NMS.....12
4.2 Web Page Layout.....15
4.3 User Levels and Rights.....18
4.4 Web Page Controls and List Operations.....26

5 Device Overview.....29

5.1 Viewing Device Information.....30

6 Configuration Wizard.....35

6.1 Overview.....36
6.2 Going Online Using a Dynamic IP Address.....37
6.3 Going Online Using PPPoE.....40
6.4 Going Online Using a Static IP Address.....42

7 Configuring Broadband Access.....46

7.1 Overview.....47
7.2 Going Online Using a Dynamic IP Address.....47
7.3 Going Online Using PPPoE.....49
7.4 Going Online Using a Static IP Address.....51

8 Going Online Through 3G.....54

9 Connecting LANs Using a Transparent Bridge.....56

10 Creating and Connecting VLANs.....58

Copyright © Huawei Technologies Co., Ltd.

10.1 Creating VLANs....59
10.2 Connecting VLANs....62
11 Connecting Wireless Users to LANs....65
12 Configuring Network Services....69
12.1 Configuring the DDNS Client....70
12.2 Configuring Advanced NAT....72
12.2.1 (Optional) Configuring ALG....73
12.2.2 Configuring a Virtual Server....73
12.2.3 (Optional) Configuring One-to-One Address Translation....75
12.3 Configuring a DHCP Address Pool....77
12.4 Configuring Static Routes....80
13 Configuring Network Security....83
13.1 Overview....84
13.2 Configuring Basic Security Features....85
13.2.1 Configuring the Firewall....85
13.2.2 Configuring MAC Address Filtering....86
13.2.3 Configuring Protection Against ARP Attacks....88
14 Configuring Network Bandwidth Guarantee....91
14.1 Overview....92
14.2 Configuring User Bandwidth Limiting....92
14.3 Configuring Advanced Bandwidth Limiting....93
14.4 Configuring Advanced Bandwidth Guarantee....95
14.5 Configuring Session Count Limiting....98
15 Configuring a VPN....100
15.1 Overview....101
15.2 Configuring an L2TP VPN....101
15.2.1 Configuring an L2TP Client....101
15.2.2 Configuring an L2TP Server....102
15.3 Configuring IPSec VPN....105
15.4 Configuring SSL VPN....107
15.4.1 Configuring Basic SSL VPN Functions....107
15.4.2 Managing SSL VPN Users....109
15.4.3 Configuring SSL VPN Services....112
15.4.4 Configuring an Authentication Policy for SSL VPN....116
16 Device Maintenance and Management....118
16.1 Managing Users....119
16.2 Basic Device Management....120
16.2.1 Device Restart....120
16.2.2 One-Key Restoration....122
16.2.3 Maintaining the Configuration....123

Copyright © Huawei Technologies Co., Ltd.

16.2.4 Software Upgrade....124
16.2.5 Time Settings....125
16.3 Managing the Router Remotely....127
16.3.1 Configuring TR-069....127
16.3.2 Configuring SNMP....128
16.3.3 Managing Syslog....132
16.3.4 Configuring Remote Management....135
16.4 System Maintenance....137
16.4.1 Locating Device Faults....137
16.4.2 Log Management....139
17 Configuration Examples....141
18 Appendix A Fault Diagnosis....146
19 Appendix B Device Default Settings....148

Copyright © Huawei Technologies Co., Ltd.

1 Product Function Overview

The product provides the following functions:

- High-speed Internet access and multiple access authentication modes

  You can access the Internet in wired or wireless mode.
- Multiple LANs and security isolation

  You can quickly create LANs without changing any hardware or communication links.
- Wireless internal network and flexible access modes

  You can access a LAN using a computer that supports wireless access, without cabling the computer and network. You can also name wireless LANs and perform user-specific access control.
- Robust firewall that secures the intranet

  The BizNavigator supports ARP attack defense, MAC-based filtering, and basic firewall functions.
- Virtual private network (VPN) that secures data transmission

  VPNs extend an enterprise intranet by setting up a reliable and secure connection between the intranet and remote users, enterprise branches, partners, or suppliers. The BizNavigator provides multiple VPN functions, including IPSec, L2TP, and SSL VPN.
- Quality of service (QoS), traffic policing, and session restricting that transmit key service data first

Copyright © Huawei Technologies Co., Ltd.

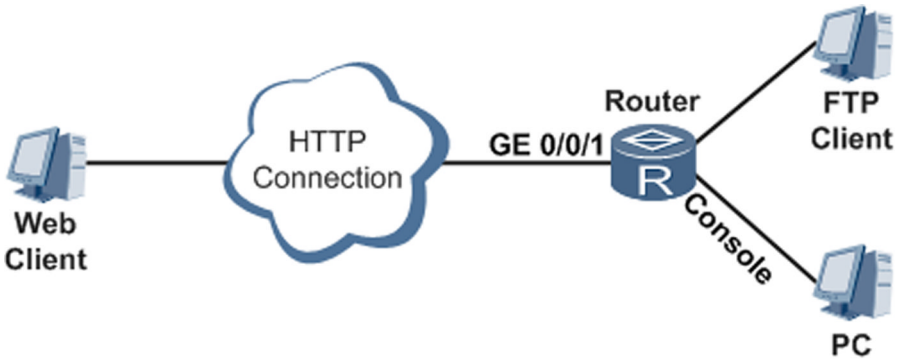
2 Web NMS Overview

The Web Network Management System (NMS) enables users to manage and maintain the router on a graphical user interface (GUI).

To help users to manage and maintain the router,the router provides a built-in web server to enable a connected terminal (for example, a PC) to access the Web NMS.

Figure 2-1 shows the running environment of the Web NMS.

Figure 2-1 Running environment of the Web NMS



Copyright © Huawei Technologies Co., Ltd.

3 Enabling the Web NMS

About This Chapter

This section describes how to load the web page file and create user accounts for the Web Network Management System (NMS).

3.1 Logging In to the Router Through the Console Port
This section describes how to log in to the router through the Console port.

3.2 Setting the Management IP Address of the router
This section describes how to set the management IP address of the router.

3.3 (Optional) Uploading the Web Page File
This section describes how to use the PC as the FTP server to upload the web page file to router.

3.4 (Optional) Loading the Web Page File
This section describes how to load the web page file.

3.5 (Optional) Creating User Accounts for the Web NMS
When the client logs in to the router through the web NMS, there must be user accounts for the web NMS on the router.

Copyright © Huawei Technologies Co., Ltd.

3.1 Logging In to the Router Through the Console Port

This section describes how to log in to the router through the Console port.

Context

To establish a local configuration environment through the Console port, you can connect your PC to the router using the Windows HyperTerminal.

Procedure

Step 1 Use the Console cable to connect the PC's COM port to the router's Console port.

Step 2 Start the HyperTerminal on the PC.

This document takes Windows XP as example. Choose **Start** > **All Programs** > **Accessories** > **Communications** > **HyperTerminal**. The HyperTerminal is displayed.

Step 3 Create a connection.

In the **Name** text box shown in **Figure 3-1**, enter the connection name, select an icon, and click **OK**.

Figure 3-1 Creating a connection

Step 4 Select a connection port.

In the **Connect To** window shown in **Figure 3-2**, select a connection port from the **Connect using** drop-down list box, and click **OK**.

Copyright © Huawei Technologies Co., Ltd.

Figure 3-2 Selecting a connection port

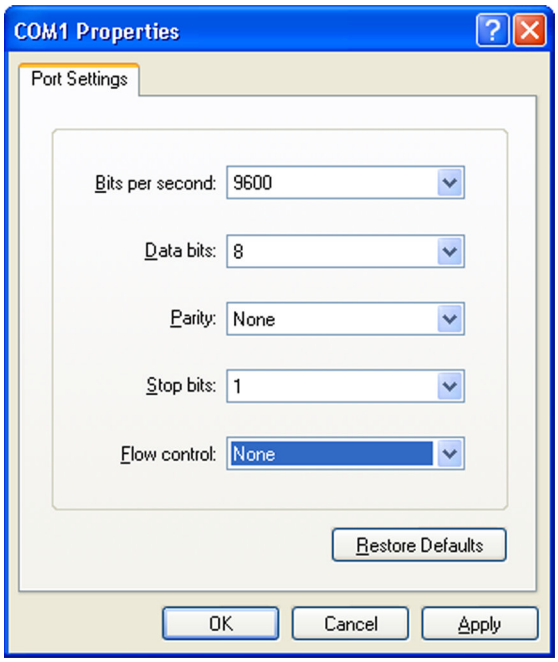
Step 5 Set the communication parameters.

In the **COM1 Properties** window shown in **Figure 3-3**, set the communication parameters to the default parameter values on the router.

NOTE

On other Windows operating systems, **Bits per second** may be described as **Baud rate**, and **Flow control** as **Traffic control**.

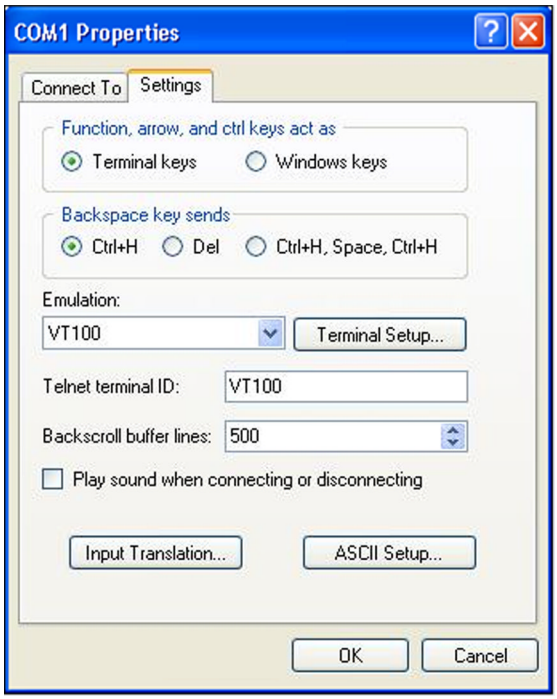
Figure 3-3 Setting the communication parameters



Step 6 Start the HyperTerminal, choose **File** > **Properties**. The window for connection properties is displayed, as shown in **Figure 3-4**. Click the **Settings** tab, select **Auto detect** or **VT100** from the **Emulation** drop-down list box.

Copyright © Huawei Technologies Co., Ltd.

Figure 3-4 Selecting a terminal type



Input the login password, and press **Enter**. If the <Huawei> prompt is displayed, you have logged in to the router.

----End

3.2 Setting the Management IP Address of the router

This section describes how to set the management IP address of the router.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **interface** *interface-type interface-number* command to enter the interface view.

Step 3 Run the **ip address** *ip-address* { *mask* | *mask-length* } command to set the management IP address.

NOTE

By default, LAN ports of AR150 and AR200 series are added to VLAN 1. The IP address of VLANIF 1 is 192.168.1.1, which can be used as the management IP address on any LAN port.

For example, set the management IP address of GE0/0/0 to 192.168.1.1 and mask length to 24.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 0/0/0
[Huawei-GigabitEthernet0/0/0] ip address 192.168.1.1 24
```

----End

Copyright © Huawei Technologies Co., Ltd.

3.3 (Optional) Uploading the Web Page File

This section describes how to use the PC as the FTP server to upload the web page file to router.

Context

Ensure that the route between the router and the FTP server is reachable. If the new software package that contains the web page file has been uploaded to the router, you do not need to upload the web page file again.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **ftp server enable** command to start the FTP server.

Step 3 Run the **aaa** command to enter the AAA view.

Step 4 Run the **local-user** *User name* **password** { **simple** | **cipher** } *password* command to set the local user name and password.

Step 5 Run the **local-user** *User name* **service-type ftp** command to set the service type of the local user to FTP.

Step 6 Run the **local-user** *User name* **ftp-directory** *directory* command to set the FTP directory.

Step 7 On the FTP server, choose **Start** > **All Programs** > **Accessories** > **Command Prompt**. The command-line interface (CLI) is displayed.

Step 8 Access the directory that stores the web page file, for example, **D:\ftp**.

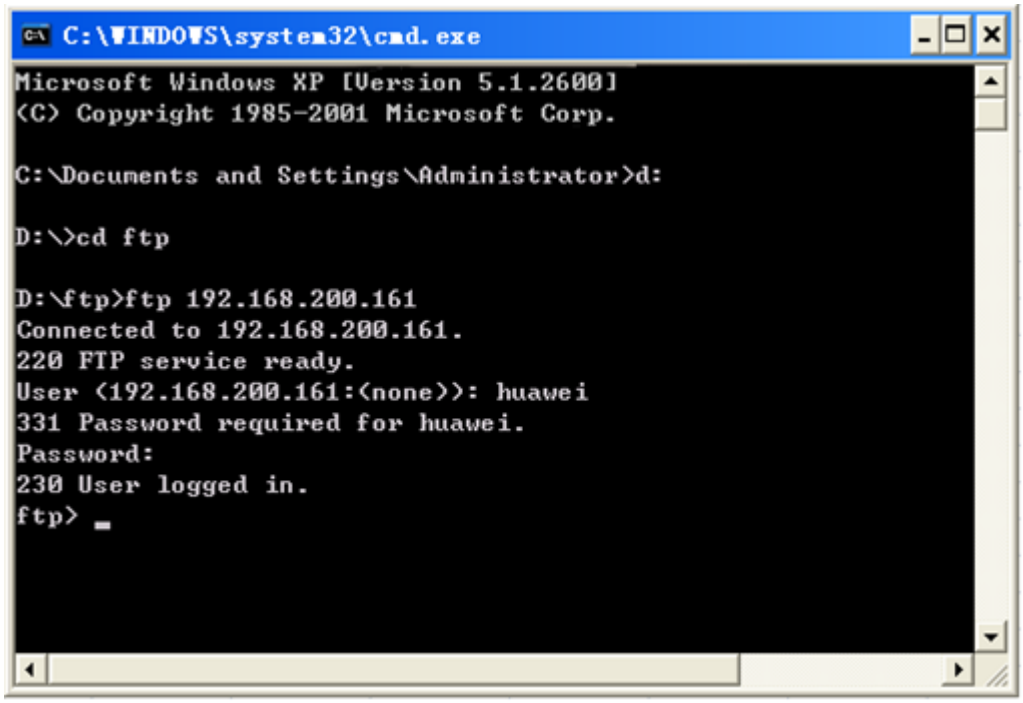
Step 9 Run the **ftp** *IP address* command to log in to the router using FTP.

In the preceding command, *IP address* indicates the management IP address of the router.

Enter the user name and password, and press **Enter**. If the command prompt in the FTP client view is displayed, for example, **ftp>**, you have accessed the FTP directory, as shown in **Figure 3-5**.

Copyright © Huawei Technologies Co., Ltd.

Figure 3-5 Logging in to the FTP server



Step 10 Run the **binary** command to enter the binary mode.

NOTE

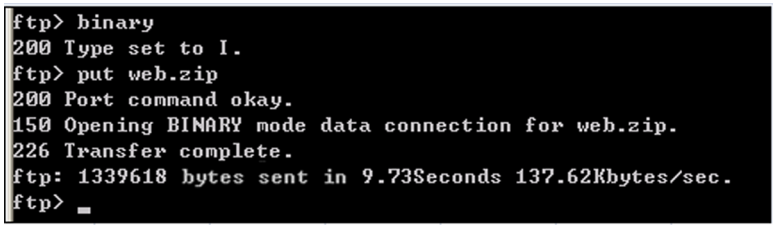
The FTP supports the following transmission modes:

- ASCII: Text files are transmitted using ASCII characters, separated by a new-line character.
- Binary: Binary files are transmitted directly.

The default transmission mode is ASCII, but the binary mode is recommended here. You can run the **ascii** or **binary** command to switch between the two modes.

Step 11 Run the **put** ***.zip* command to upload the web page file from the FTP server to the router. In the preceding command, ***.zip* indicates the name of the web page files, as shown in **Figure 3-6**.

Figure 3-6 Uploading the web page file



Step 12 On the router, run the **dir** command to check the existence of the web page file in the current storage directory.

Copyright © Huawei Technologies Co., Ltd.

NOTE

If the size of the web page file on the router is different from that on the FTP file server, a transmission exception may occur. Upload the web page files again.

----End

3.4 (Optional) Loading the Web Page File

This section describes how to load the web page file.

Context

Before loading the web page file, ensure that the file has been uploaded to the router. The web page file is in .zip format. The web page file name is in the *.zip format. If the router has loaded the new software package that contains the web page file, you do not need to load the web page file again.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **http server enable** command to enable the HTTP service.

Step 3 Run the **http server load** *file-name* command to load the web page file.

----End

3.5 (Optional) Creating User Accounts for the Web NMS

When the client logs in to the router through the web NMS, there must be user accounts for the web NMS on the router.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **http server enable** command to enable the HTTP service.

Step 3 Run the **aaa** command to enter the AAA view.

Step 4 Run the **local-user** *user-name* **password** *password* command to set the HTTP user name and password.

Step 5 Run the **local-user** *User name* **privilege level** *level* command to set the user level.

NOTE

The default user name and password on the router are both admin. You are advised to change the password after logging in to the router for security.

By default, the user level is common user. Mappings between user levels and users are as follows:

- 0-1: common user
- 2: enterprise administrator
- 3-15: super user

Copyright © Huawei Technologies Co., Ltd.

Step 6 Run the **local-user** *user name* **service-type http** command to set the user access type to HTTP.

Step 7 Run the **quit** command to return to the system view.

Step 8 (Optional) Run the **http timeout** *timeout* command to set the timeout interval for HTTP sessions. In the command, *timeout* is in minutes.

The default timeout interval is 3 minutes.

----End

Copyright © Huawei Technologies Co., Ltd.

4 Web Page Introduction

About This Chapter

This section describes the login, page layout, and operations for the Web NMS.

4.1 Logging In to the Web NMS
This section describes how to log in to and log out of the Web NMS.

4.2 Web Page Layout
This section describes the page layout of the Web NMS and help system.

4.3 User Levels and Rights
This section describes user levels and rights in the Web NMS.

4.4 Web Page Controls and List Operations
This section describes the web page controls and operations that you can perform for lists on web pages.

Copyright © Huawei Technologies Co., Ltd.

4.1 Logging In to the Web NMS

This section describes how to log in to and log out of the Web NMS.

Prerequisites

Before logging in to the Web NMS, ensure that:

- The IP address of the device's access port has been configured.

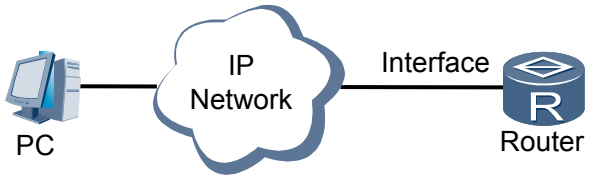
  NOTE

  By default, LAN ports of AR150 and AR200 series are added to VLAN 1. The IP address of VLANIF 1 is 192.168.1.1, and subnet mask is 255.255.255.0.

  If default settings are not modified, ports from Ethernet0/0/0 to Ethernet0/0/7 can be used as access ports.
- The device and your PC are properly connected.
- The device is running properly and the HTTP or HTTPS service is correctly configured.
- The web browser software has been installed on your PC.
  - Windows: Internet Explorer 7.0 or later
  - Linux: Firefox

Figure 4-1 shows the running environment of the Web NMS that can be managed and configured on your PC.

Figure 4-1 Running environment of the Web NMS



Procedure

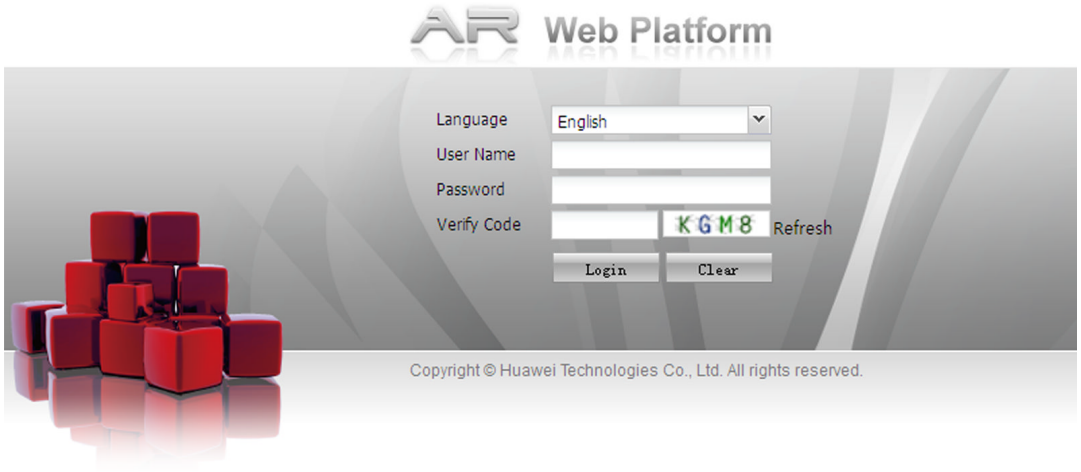
Step 1 Open the web browser, enter the URL of the Web NMS, and press **Enter**. The Web NMS login page is displayed, as shown in Figure 4-2.

NOTE

This document assumes that URL of the Web NMS is http://192.168.1.1. If the HTTPS service is enabled and the port number is set to 1278, the URL of the Web NMS is https://192.168.1.1:1278.

Copyright © Huawei Technologies Co., Ltd.

Figure 4-2 Login page



Step 2 Enter the login information.

1. Select a language.

   English and Chinese are supported. The default language is Chinese. To use English, select English.

2. Enter a user name and password.

   The default user name and password are **admin**.

3. Enter the verification code (case-insensitive).

   To obtain a new verification code, click **Refresh**.

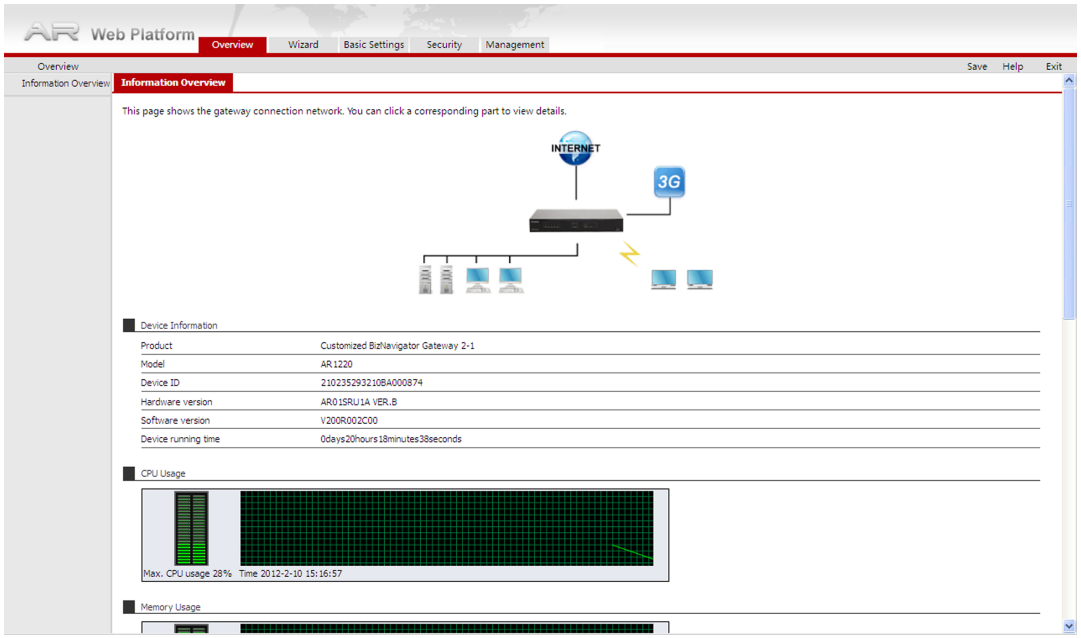
4. Click **Login**. The page shown in **Figure 4-3** is displayed.

   NOTE

   You can click **Clear** and enter the user name, password, and verification code again.

Copyright © Huawei Technologies Co., Ltd.

Figure 4-3 Web NMS home page



NOTE

- If the **Invalid verify code** dialog box is displayed, as shown in **Figure 4-4**, click **OK** and enter the verification code again.
- If the **Incorrect verify code** dialog box is displayed, as shown in **Figure 4-5**, click **OK** and enter the verification code again.
- If the **Authentication failure** dialog box is displayed, as shown in **Figure 4-6**, click **OK** and enter the user name and password again.
- If the **Sufficient online users** dialog box is displayed, as shown in **Figure 4-7**, the concurrent online users reach the maximum. By default, the Web NMS supports a maximum of five concurrent online users.
- If the **Invalid client address** dialog box is displayed, as shown in **Figure 4-8**, the current host IP address is not in the trusted IP address list.
- The same user name can be used for login at only one client at a time.

Figure 4-4 Invalid verify code

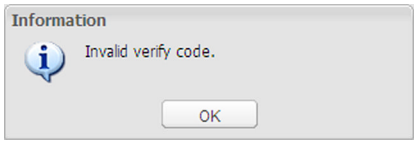
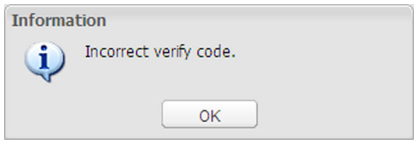


Figure 4-5 Incorrect verify code



Copyright © Huawei Technologies Co., Ltd.

Figure 4-6 Authentication failure

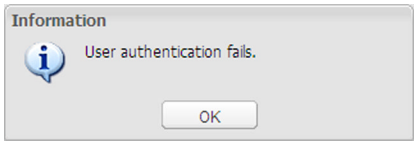


Figure 4-7 Sufficient online users

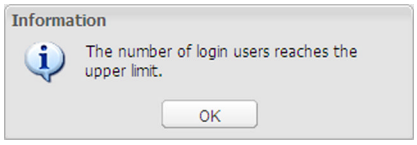
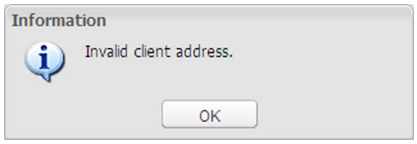


Figure 4-8 Invalid client address



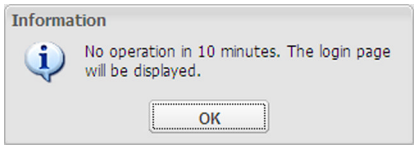
Step 3 To log out of the web page, click **Logout** at the upper-right corner of the page shown in **Figure 4-3**. The login page is displayed.

NOTE

If no operation is performed in a specified period (default: 10 minutes), the system automatically logs out, as shown in **Figure 4-9**.

To log out of the web page, click **Logout**. If you do not click **Logout** but close the browser, you cannot log out of the web page. In this case, if you need to log in to the web page again, you can log in to the web page when the login timeout period expires.

Figure 4-9 Login timeout



----End

4.2 Web Page Layout

This section describes the page layout of the Web NMS and help system.

Page Layout

Figure 4-10 shows the page layout of the Web NMS.

Copyright © Huawei Technologies Co., Ltd.

Figure 4-10 Page layout of the Web NMS

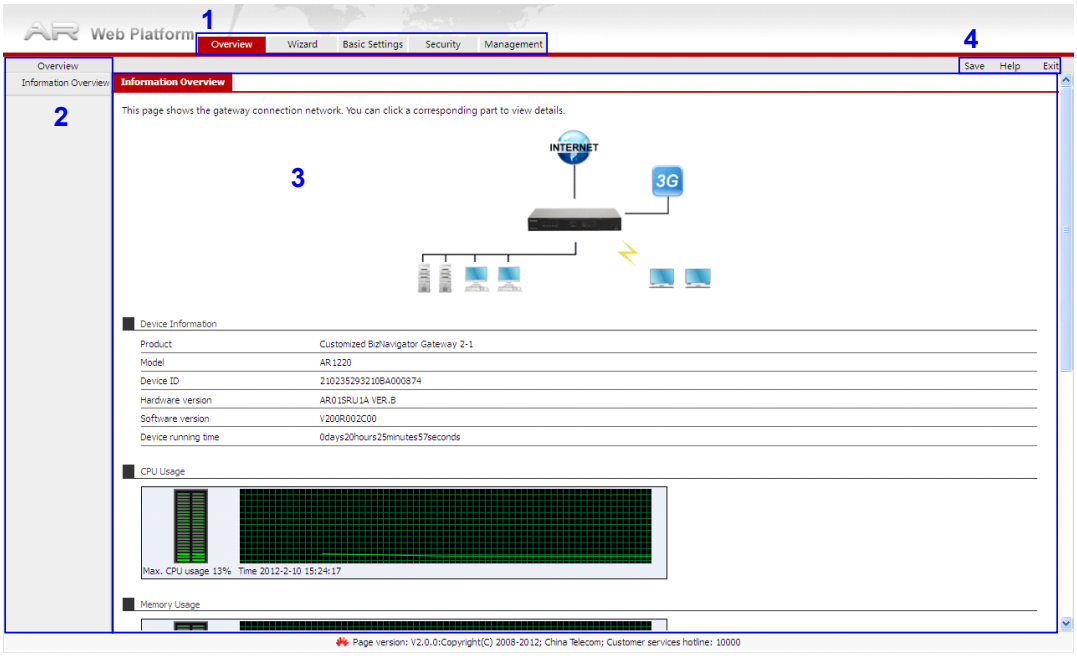


Table 4-1 Page layout of the Web NMS

Area	Name	Description
1	Menu bar	Displays functional module tabs.
2	Navigation bar	Displays specific function categories in tree mode. Items marked with + can be expanded.
3	Operation area	Displays specific functions for users to configure.
4	Auxiliary area	Allows users to save the current configuration, obtain help, and log out of the Web NMS.

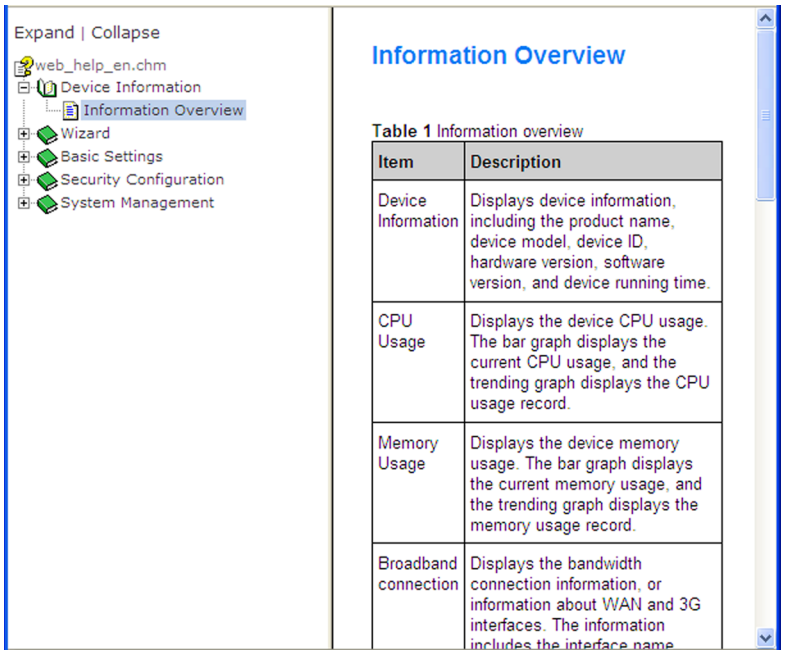
Help System

Click **Help** in the auxiliary area, and select **Local Help**, **Online Help**, or **About** to obtain help information.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Local Help	Click **Local Help** or press F1 on any page. The help information window is displayed to show parameter description of the current page, as shown in **Figure 4-11**. If the IE browser blocks pop-up windows, configure the browser to allow pop-up windows. In the displayed help information window, you can view parameter description of any page in the navigation tree.
Online Help	Click **Online Help** on any page. The http://support.huawei.com/support/ page is displayed. You can obtain online help information on this page.
About	Click **About** on any page. The page shown in **Figure 4-12** is displayed to show Web NMS version information.

Figure 4-11 Local Help



Copyright © Huawei Technologies Co., Ltd.

Figure 4-12 About

4.3 User Levels and Rights

This section describes user levels and rights in the Web NMS.

The Web NMS provides the following user levels with the rights in ascending order: common user, enterprise administrator, and super administrator.

Table 4-2 shows the rights of different user levels.

NOTE

In Table 4-2, **Y** means that the permission is supported, and **-** means that the permission is not supported.

- Common user: manages value-added services (VAS).
- Enterprise administrator: manages enterprise LANs.
- Super administrator: maintain devices.

Table 4-2 User levels and rights in the Web NMS

Function				Common User		Enterprise Administrator		Super Administrator	
				Read	Write	Read	Write	Read	Write
Device overview	Information overview	Device information	Product name	Y	-	Y	-	Y	-
			Device model	Y	-	Y	-	Y	-
			Device ID	Y	-	Y	-	Y	-
			Hardware version	Y	-	Y	-	Y	-

Copyright © Huawei Technologies Co., Ltd.

Function				Common User		Enterprise Administrator		Super Administrator	
				Read	Write	Read	Write	Read	Write
			Software version	Y	-	Y	-	Y	-
			Device running time	Y	-	Y	-	Y	-
		CPU usage	-	Y	-	Y	-	Y	-
		Memory usage	-	Y	-	Y	-	Y	-
		Broadband connection information	-	Y	-	Y	-	Y	-
		3G data card connection status	3G network information	Y	-	Y	-	Y	-
			3G modem status	Y	-	Y	-	Y	-
			UIM card status	Y	-	Y	-	Y	-
			Signal strength	Y	-	Y	-	Y	-
		LAN information	-	Y	-	Y	-	Y	-
		Wireless network information	SSID	Y	-	Y	-	Y	-
			Service status	Y	-	Y	-	Y	-
			Supported PCs	Y	-	Y	-	Y	-
		Service information	Service name	Y	-	Y	-	Y	-
			Current status	Y	-	Y	-	Y	-

Copyright © Huawei Technologies Co., Ltd.

Function				Common User		Enterprise Administrator		Super Administrator	
				Read	Write	Read	Write	Read	Write
			Detailed configuration	Y	-	Y	-	Y	-
		Recent system logs	-	Y	-	Y	-	Y	-
Configuration wizard	Configuration wizard	Configuration wizard description	-	-	-	Y	-	Y	-
		Broadband connection configuration	WAN port	-	-	Y	-	Y	Y
			Connection mode	-	-	Y	-	Y	Y
		LAN settings	LAN port IP	-	-	Y	Y	Y	Y
			DHCP	-	-	Y	Y	Y	Y
		Wireless routing	Enable wireless	-	-	Y	Y	Y	Y
			SSID	-	-	Y	Y	Y	Y
			SSID hiding	-	-	Y	Y	Y	Y
			Encryption mode	-	-	Y	Y	Y	Y
			Encryption key	-	-	Y	Y	Y	Y
Basic settings	Interface	WAN interface	WAN	-	-	Y	-	Y	Y
		LAN interface	VLAN interface	-	-	Y	Y	Y	Y
			VLAN	-	-	Y	Y	Y	Y
		WLAN interface	Basic settings	-	-	Y	Y	Y	Y

Copyright © Huawei Technologies Co., Ltd.

Function				Common User		Enterprise Administrator		Super Administrator	
				Read	Write	Read	Write	Read	Write
			Advanced settings	-	-	Y	Y	Y	Y
		3G interface	Basic settings	-	-	Y	Y	Y	Y
			Advanced settings	-	-	Y	Y	Y	Y
	Network settings	DDNS	Domain name	-	-	Y	Y	Y	Y
			Server	-	-	Y	Y	Y	Y
			User name	-	-	Y	Y	Y	Y
			Interface binding	-	-	Y	Y	Y	Y
		Advanced NAT settings	ALG	-	-	-	-	Y	Y
			Virtual server	-	-	-	-	Y	Y
			One-to-one address translation	-	-	-	-	Y	Y
		DHCP address pool	Basic LAN port network settings	-	-	Y	Y	Y	Y
		Route settings	Static route	-	-	-	-	Y	Y
	VPN	L2TP VPN	L2TP Client	-	-	-	-	Y	Y
			L2TP Server	-	-	-	-	Y	Y
		IPSec VPN	Connection name	-	-	-	-	Y	Y
			Gateway information	-	-	-	-	Y	Y
			Filter	-	-	-	-	Y	Y

Copyright © Huawei Technologies Co., Ltd.

Function				Common User		Enterprise Administrator		Super Administrator	
				Read	Write	Read	Write	Read	Write
			Advanced settings	-	-	-	-	Y	Y
		SSL VPN	SSL Settings	-	-	-	-	Y	Y
			Service management	-	-	-	-	Y	Y
			User management	-	-	-	-	Y	Y
			Resource management	-	-	-	-	Y	Y
			Domain management	-	-	-	-	Y	Y
	QoS	Bandwidth limiting	Limiting type	-	-	Y	Y	Y	Y
			Start and end IP addresses	-	-	Y	Y	Y	Y
			Interface	-	-	Y	Y	Y	Y
			Type	-	-	Y	Y	Y	Y
			Traffic direction and rate	-	-	Y	Y	Y	Y
		Advanced bandwidth limiting	Traffic processing	-	-	Y	Y	Y	Y
			Match criteria	-	-	Y	Y	Y	Y
		Advanced bandwidth assurance	Interface bandwidth	-	-	Y	Y	Y	Y
			Application bandwidth	-	-	Y	Y	Y	Y

Copyright © Huawei Technologies Co., Ltd.

Function				Common User		Enterprise Administrator		Super Administrator	
				Read	Write	Read	Write	Read	Write
		Session count restriction	Enable session count restriction	-	-	Y	Y	Y	Y
			Total session count restriction	-	-	Y	Y	Y	Y
	Remote management	TR-069	ACS	-	-	-	-	Y	Y
			CPE	-	-	-	-	Y	Y
		SNMP	SNMP version	-	-	-	-	Y	Y
			Contact information	-	-	-	-	Y	Y
			System name	-	-	-	-	Y	Y
			Device location	-	-	-	-	Y	Y
			Security user name	-	-	-	-	Y	Y
			Authentication password	-	-	-	-	Y	Y
			Encryption password	-	-	-	-	Y	Y
			SNMP read-only password	-	-	-	-	Y	Y
			SNMP read-write password	-	-	-	-	Y	Y
			Trap password	-	-	-	-	Y	Y

Copyright © Huawei Technologies Co., Ltd.

Function				Common User		Enterprise Administrator		Super Administrator	
				Read	Write	Read	Write	Read	Write
			Trap receiving host	-	-	-	-	Y	Y
		Syslog management	Local log	-	-	-	-	Y	Y
			Remote log	-	-	-	-	Y	Y
		Remote management	Remote access protocol and port	-	-	Y	Y	Y	Y
			Remote trust host IP	-	-	-	-	Y	Y
Security settings	Basic settings	Firewall	Enable firewall	-	-	Y	Y	Y	Y
		MAC address filtering	Filtering type	-	-	Y	Y	Y	Y
			MAC address settings	-	-	Y	Y	Y	Y
		ARP defense	ARP defense	-	-	Y	Y	Y	Y
			Manual IP_MAC binding	-	-	Y	Y	Y	Y
System management	Restart device	-	-	-	-	Y	Y	Y	Y
	User management	Create local user	User name	-	-	Y	Y	Y	Y
			Password	-	-	-	Y	-	Y
			Confirm password	-	-	-	Y	-	Y
		User list	Change password	-	Y	-	Y	-	Y

Copyright © Huawei Technologies Co., Ltd.

Function				Common User		Enterprise Administrator		Super Administrator	
				Read	Write	Read	Write	Read	Write
	One-key restoration	Restore factory settings	-	-	-	-	-	Y	Y
		Restore installation configuration	-	-	-	-	-	Y	Y
	Configuration maintenance	Save configuration	-	-	-	-	-	Y	Y
		Import and export configuration	-	-	-	-	-	Y	Y
		Upload configuration	-	-	-	-	-	Y	Y
	Upgrade software	-	-	-	-	-	-	Y	Y
	Troubleshooting tool	Ping	-	-	-	Y	Y	Y	Y
		Tracert	-	-	-	Y	Y	Y	Y
		Http Get	-	-	-	Y	Y	Y	Y
		DNS Query	-	-	-	Y	Y	Y	Y
	Time settings	NTP	NTP settings	-	-	-	-	Y	Y
			System time settings	-	-	-	-	Y	Y
	Log management	Log query	-	-	-	-	-	Y	Y

Copyright © Huawei Technologies Co., Ltd.

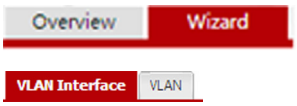
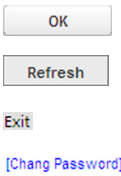
4.4 Web Page Controls and List Operations

This section describes the web page controls and operations that you can perform for lists on web pages.

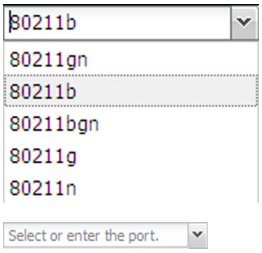
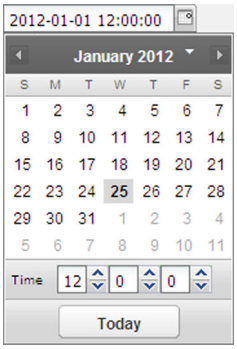
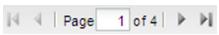
Web Page Controls

Web page controls include buttons, check boxes, and icons.

Table 4-3 Web page controls

Name	Figure	Function
Tab		Click a tab to display the page for configuring a functional module. An active tab is distinguished from other tabs in color and form.
Navigation tree		Click a node in the navigation tree to display the configuration page. Nodes marked with + can be expanded.
Button		Click a button to perform an operation. A button is presented in icon and text.
Option button		Click an option box to select an item. Only one option can be selected among a group of items.
Check box		Click a check box to select an item, and click it again to deselect the item. Multiple options can be selected among a group of items.
Text box		Enter a value in a text box. Text boxes for entering IPv4 addresses are displayed in dotted decimal notation to avoid incorrect IP address format.

Copyright © Huawei Technologies Co., Ltd.

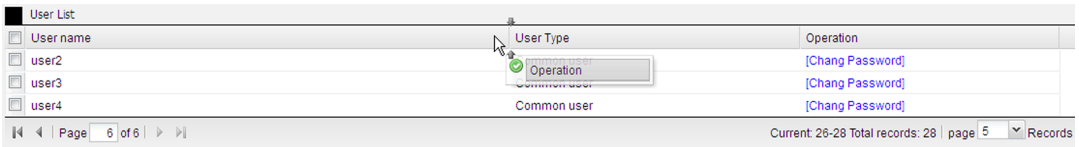
Name	Figure	Function
Drop-down list box		Click the arrow and select a value from a list. A drop-down list box may support text input.
Date		Click a date control to set the date.
Browse		Click **Browse** and select a file.
Modify		Click the icon to modify an item in a list.
Delete		Click the icon to delete an item in a list.
Paging		The four arrows indicate the first, previous, next, and end pages respectively. Enter a page number in the text box and press **Enter** to go the specified page.

List Operations

The Web NMS allows you to adjust the table header display sequence and displays lists in pages for you to query.

- Adjust the table header display sequence. To move a table header, move the cursor to the table header and drag the table header to another table header position, as shown in **Figure 4-13**.

Figure 4-13 Adjusting the table header display sequence

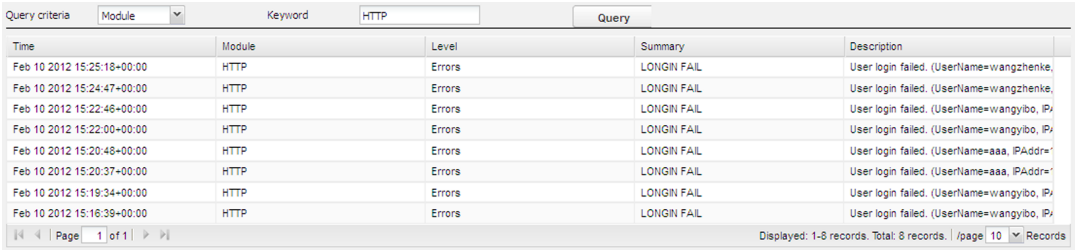


- Display items on multiple pages. Items are displayed on multiple pages when one page cannot accommodate all the items.

Copyright © Huawei Technologies Co., Ltd.

- Query a list. Users can query a list by query criteria and keyword.

Figure 4-14 Querying a list



Copyright © Huawei Technologies Co., Ltd.

5 Device Overview

About This Chapter

This section describes how to view device information.

5.1 Viewing Device Information
This section describes how to view device information.

Copyright © Huawei Technologies Co., Ltd.

5.1 Viewing Device Information

This section describes how to view device information.

Context

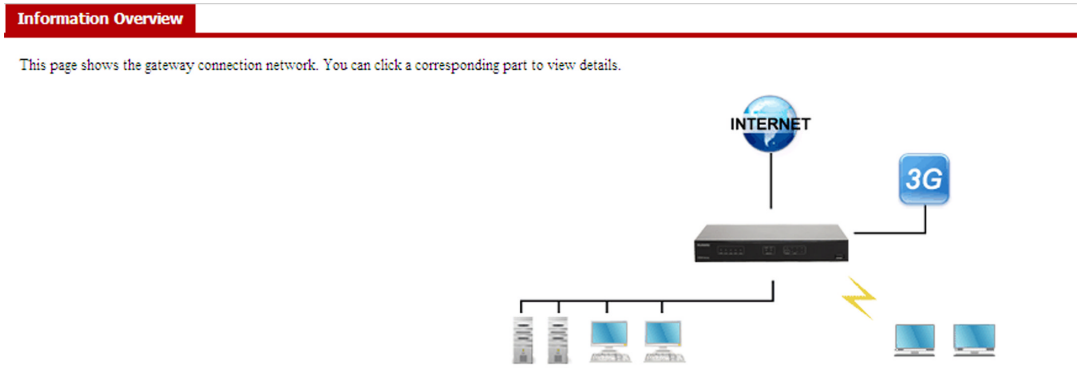
You can view the following information on the **Information Overview** page:

- **Device information**
- **CPU usage**
- **Memory usage**
- **Broadband connection**
- **3G data card connection**
- **LAN**
- **Wireless network**
- **Service information**
- **Recent system logs**

Procedure

Step 1 Choose **Device Overview** > **Information Overview**. The **Information Overview** page is displayed, as shown in **Figure 5-1**.

Figure 5-1 Information Overview



Step 2 Click the device in **Figure 5-1**. As shown in **Figure 5-2**, the device information is displayed, including the product name, device model, device ID, hardware version, software version, and device running time.

Copyright © Huawei Technologies Co., Ltd.

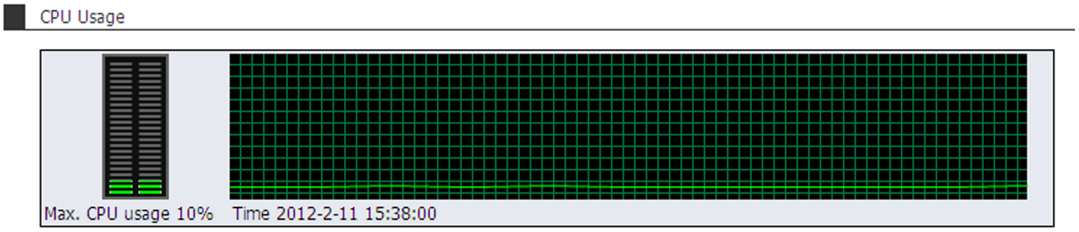
Figure 5-2 Device information

Device Information

Product	Customized BizNavigator Gateway 2-1
Model	AR2240
Device ID	2102113373P0BA000232
Hardware version	AR01SRU3A VER.B
Software version	V200R002C00
Device running time	0 days 20 hours 51 minutes 53 seconds

Step 3 View the CPU usage of the device, as shown in **Figure 5-3**.

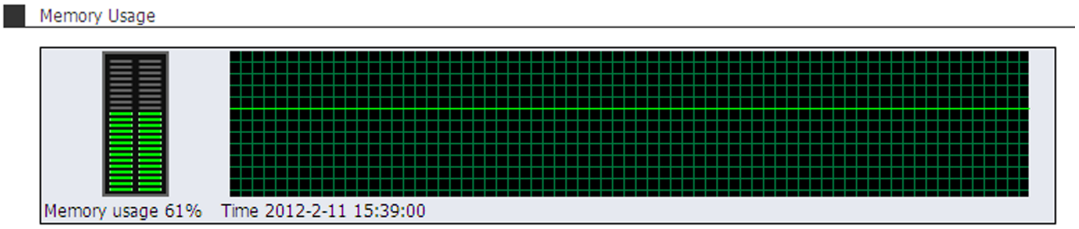
Figure 5-3 CPU usage



In **Figure 5-3**, the left part shows the highest CPU usage, and the right part shows the CPU usage trend from right to left and the time when the highest CPU usage is reached.

Step 4 View the memory usage of the device, as shown in **Figure 5-4**.

Figure 5-4 Memory usage



In **Figure 5-4**, the left part shows the current memory usage, and the right part shows the memory usage trend from right to left and the current time.

Step 5 Click 

in **Figure 5-1** to view broadband connection information, as shown in **Figure 5-5**.

Copyright © Huawei Technologies Co., Ltd.

Figure 5-5 Broadband connection

Broadband connection

Interface name	Connection status	IP address
Ethernet1/0/0	Connected	114.1.1.1
Ethernet1/0/1	Connected	
Ethernet2/0/0	Connected	202.1.1.2
Ethernet2/0/1	Connected	10.1.2.1
GigabitEthernet0/0/0	Connected	192.168.200.177
GigabitEthernet0/0/1	Connected	116.1.1.1
GigabitEthernet0/0/2	Unconnected	

Step 6 Click  in **Figure 5-1** to view information about the 3G data card connection, as shown in **Figure 5-6**.

Figure 5-6 3G data card connection

3G Data Card Connection

Cellular 0/0/0	Unconnected
3G Modem	Card-inserted
UIM card status	No card
Signal strength	

To view details about the 3G Modem, UIM card, and 3G network, click **More**, as shown in **Figure 5-7**.

Figure 5-7 3G information

Cellular 0/0/0

3G Modem Information

3G Modem	Card-inserted
Model	EC1261-2
Vendor	HUAWEI TECHNOLOGIES CO., LTD
ESN	Inactive
Hardware version	CE64TCPU
Firmware version	11.106.03.02.000
PRL version	0
Power supply voltage	3354 mV

UIM Card Information

UIM card status	No card
IMSI	

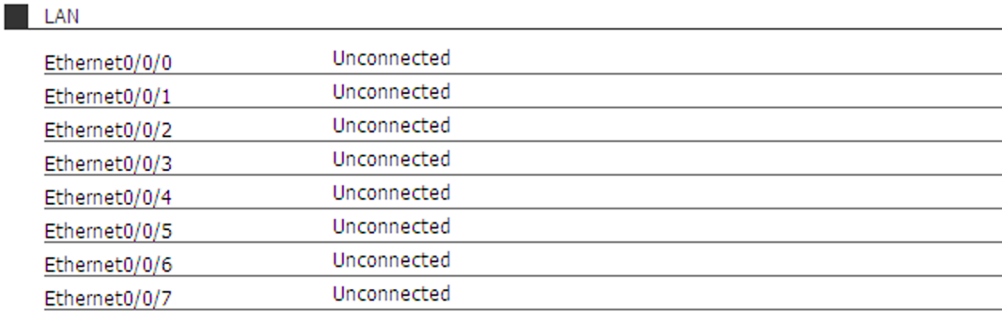
3G Network Information

Carrier	
Working status	Unconnected
Signal strength	

Copyright © Huawei Technologies Co., Ltd.

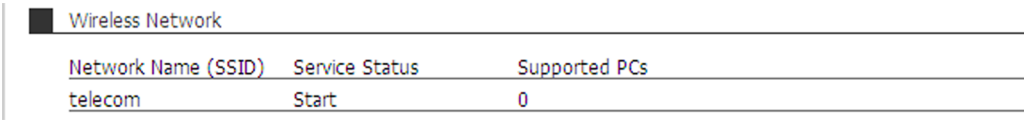
Step 7 Click  in **Figure 5-1** to view LAN information, as shown in **Figure 5-8**.

Figure 5-8 LAN information



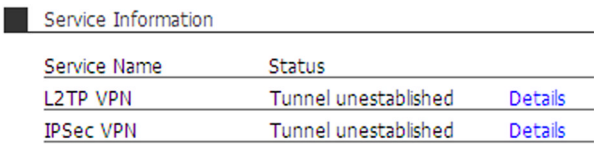
Step 8 Click  in **Figure 5-1** to view wireless network information, as shown in **Figure 5-9**.

Figure 5-9 Wireless network



Step 9 View service information shown in **Figure 5-10**.

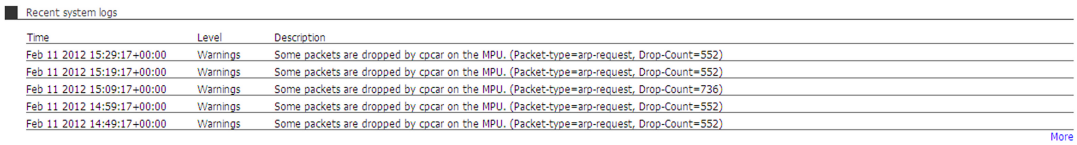
Figure 5-10 Service information



To view detailed service information, click **Details**.

Step 10 View recent system logs shown in **Figure 5-11**.

Figure 5-11 Recent system logs



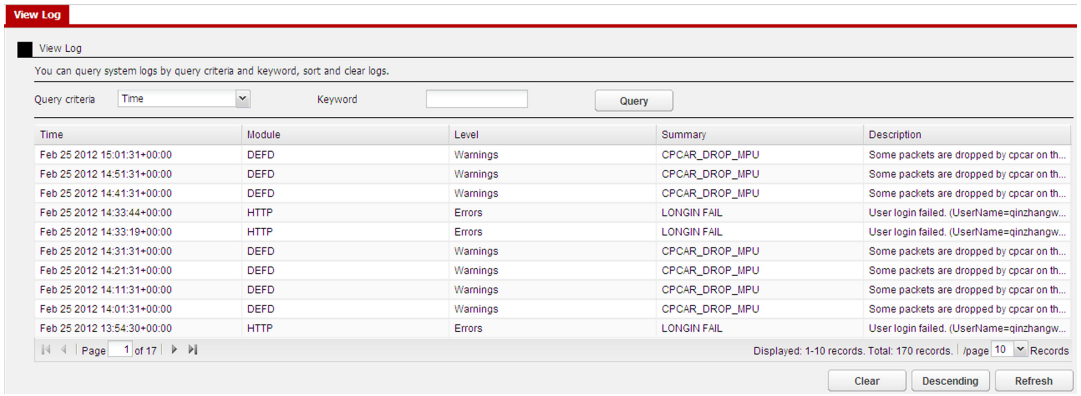
NOTE

A maximum of five logs can be displayed on a page.

To view more logs, click **More**, as shown in **Figure 5-12**. For details about log-related operations, see **Log Management**.

Copyright © Huawei Technologies Co., Ltd.

Figure 5-12 Log information



Step 11 To specify the refresh interval, select a value from the Refresh Interval Manual drop-down list box.

To refresh the **Information Overview** page, click Refresh.

NOTE

- If you select **manual**, you need to click **Refresh** to refresh the **Information Overview** page.
- If you select a refresh interval, you do not need to click **Refresh**. For example, if you select **10 seconds**, the **Information Overview** page is automatically refreshed once every 10 seconds.

----End

Copyright © Huawei Technologies Co., Ltd.

6 Configuration Wizard

About This Chapter

This section describes how to use the configuration wizard to enable quick Internet access.

6.1 Overview
This section describes the configuration procedure involved in the configuration wizard.

6.2 Going Online Using a Dynamic IP Address
This section describes how to go online quickly by using an IP address obtained from the carrier.

6.3 Going Online Using PPPoE
This section describes how to go online quickly using PPPoE.

6.4 Going Online Using a Static IP Address
This section describes how to go online using a static IP address allocated by the carrier.

Copyright © Huawei Technologies Co., Ltd.

6.1 Overview

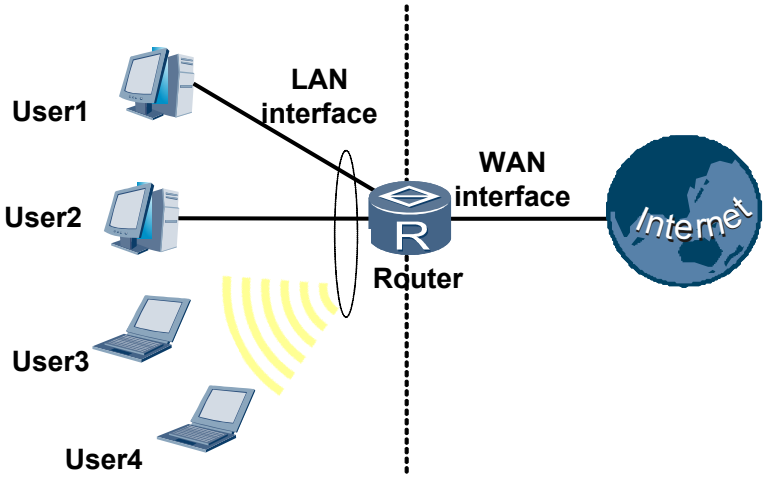
This section describes the configuration procedure involved in the configuration wizard.

The configuration wizard enables you to easily configure required network parameters. With the configuration wizard, you can configure:

1. Broadband connection information
2. LAN information
3. Wireless routing (only AR1220W and AR1220VW support wireless routing configuration)

Figure 6-1 shows the networking of Internet access. The interface that connects a router to the Internet is called WAN interface, and the interface that connects users is called LAN interface. A LAN interface can be an Ethernet interface in wired mode or a WLAN-BSS interface in wireless mode.

Figure 6-1 Networking of Internet access



Limitations

- Common users cannot use the configuration wizard.
- Enterprise administrators can configure and query LAN interface parameters, but can only query WAN interface parameters.
- Super users can configure and query all parameters involved in the configuration wizard.

Connecting to the Internet at the WAN Side

The following table shows three methods for a WAN interface to obtain an IP address:

Table 6-1 Three methods for a WAN interface to obtain IP addresses

Method to Obtain IP	Required Parameter
Automatically	Interface connected to the Internet

Copyright © Huawei Technologies Co., Ltd.

Method to Obtain IP	Required Parameter
PPPoE	● Interface connected to the Internet ● Account ● Password
Manually	● Interface connected to the Internet ● Static IP address and subnet mask assigned by a carrier

Connecting to Users at the LAN Side

LAN users can have specified IP addresses or obtain IP addresses from the DHCP server

When an IP address is configured statically, ensure that the IP address is in the same network segment as the IP addresses if the LAN interface on the router.

When IP addresses are configured dynamically, configure the DHCP Server function on the router. If the network segment that the LAN interface's IP address belongs to is changed, IP addresses of LAN users must be released.

6.2 Going Online Using a Dynamic IP Address

This section describes how to go online quickly by using an IP address obtained from the carrier.

Context

To start the wizard, click **Wizard** in the navigation tree. This wizard helps you quickly set the Internet access parameters. You can click **Previous** anytime to modify your settings.

Procedure

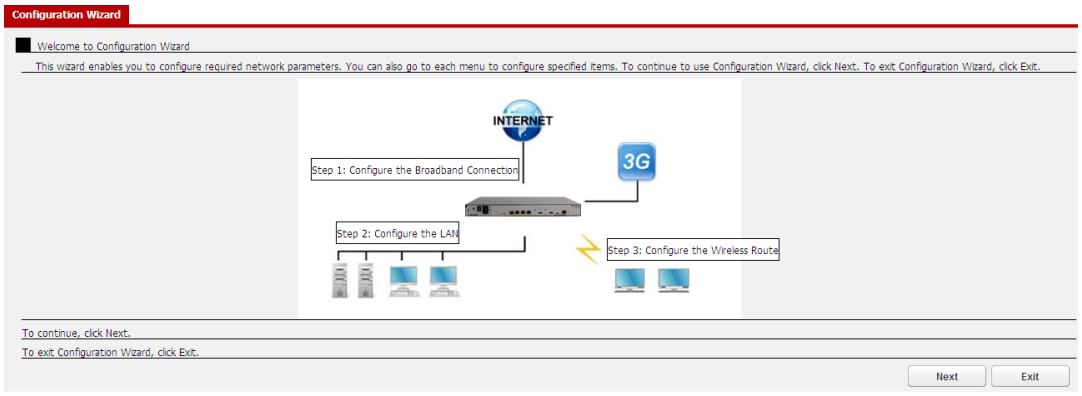
Step 1 (Optional) Configure VLANs. To add an Ethernet interface to a VLAN, see **10.1 Creating VLANs**. To add a WLAN-BSS interface to a VLAN, see **11 Connecting Wireless Users to LANs**.

By default, all LAN-side interfaces on a router belong to VLAN 1. To add a LAN-side interface to another VLAN, perform this step; otherwise, skip this step and start the wizard.

Step 2 Open the **Wizard** page.

1. Click **Wizard** in the navigation tree to open the following page:

Copyright © Huawei Technologies Co., Ltd.

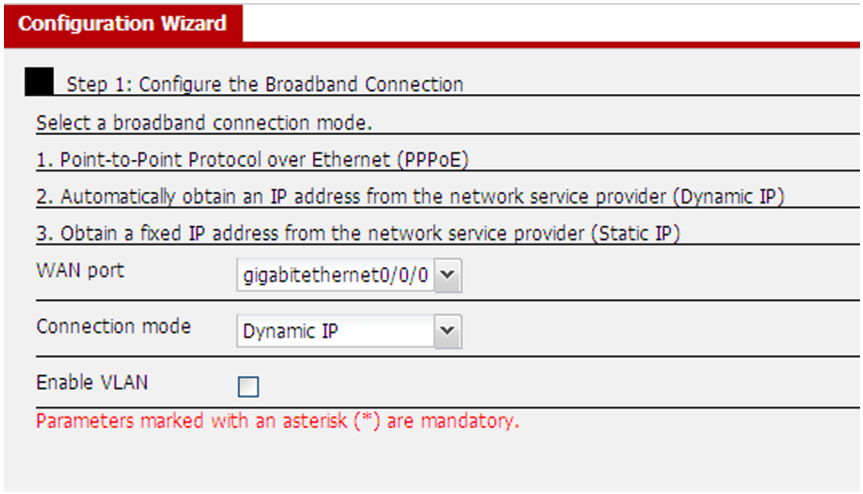


2. Click **Next** to configure a WAN connection.

Step 3 Configure a WAN connection.

1. Set WAN connection parameters.

   Set **Connection mode** to **Automatically obtain IP**.

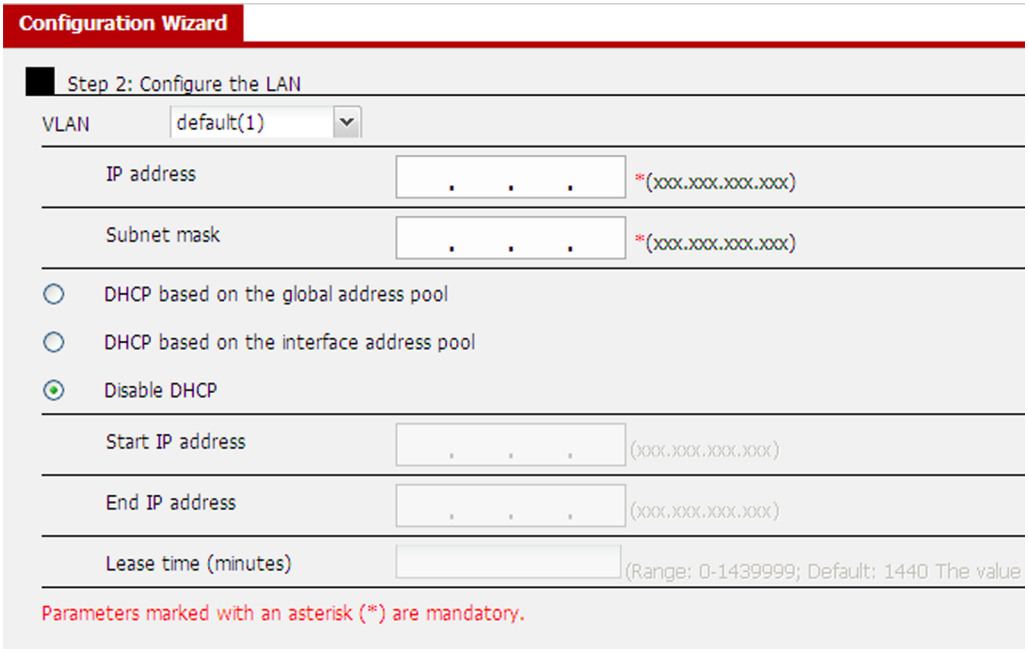


2. Click **Next** to finish the WAN connection configuration and open the **Configure the LAN** page.

Step 4 Configure LAN access.

1. Set LAN access parameters.

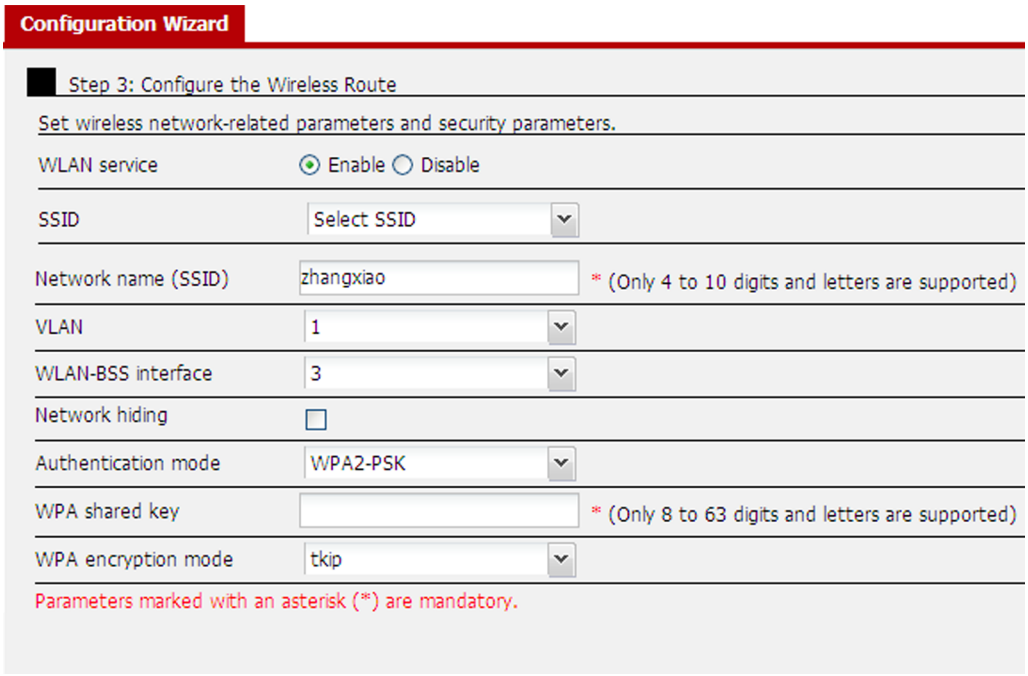
Copyright © Huawei Technologies Co., Ltd.



2. Click **Next** to finish the LAN access configurations. If your router supports WLAN, the web system displays the WLAN configuration page. If your router does not support WLAN, the web system displays the **Finish** page. Skip to step 6.

Step 5 Configure WLAN access.

1. Set WLAN parameters.



2. Click **Next** to finish the WLAN access configurations and open the **Finish Configuration Wizard** page.

Step 6 Confirm the configurations.

Copyright © Huawei Technologies Co., Ltd.

View the configurations on the **Finish Configuration Wizard** page. To confirm the configurations, click **Finish**. To modify the configurations, click **Previous**. If you quit the wizard without clicking **Finish**, the configurations will not take effect.

----End

6.3 Going Online Using PPPoE

This section describes how to go online quickly using PPPoE.

Context

To start the wizard, click **Wizard** in the navigation tree. This wizard helps you quickly set Internet access parameters. You can click **Previous** anytime to modify your settings.

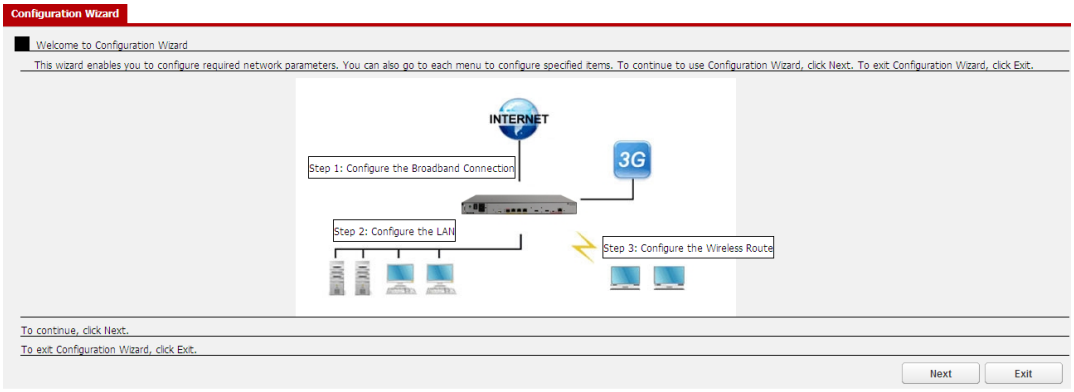
Procedure

Step 1 (Optional) Configure VLANs. To add an Ethernet interface to a VLAN, see **10.1 Creating VLANs**. To add a WLAN-BSS interface to a VLAN, see **11 Connecting Wireless Users to LANs**.

By default, all LAN-side interfaces on a router belong to VLAN 1. To add a LAN-side interface to another VLAN, perform this step; otherwise, skip this step and start the wizard.

Step 2 Open the **Wizard** page.

1. Click **Wizard** in the navigation tree to open the following page.



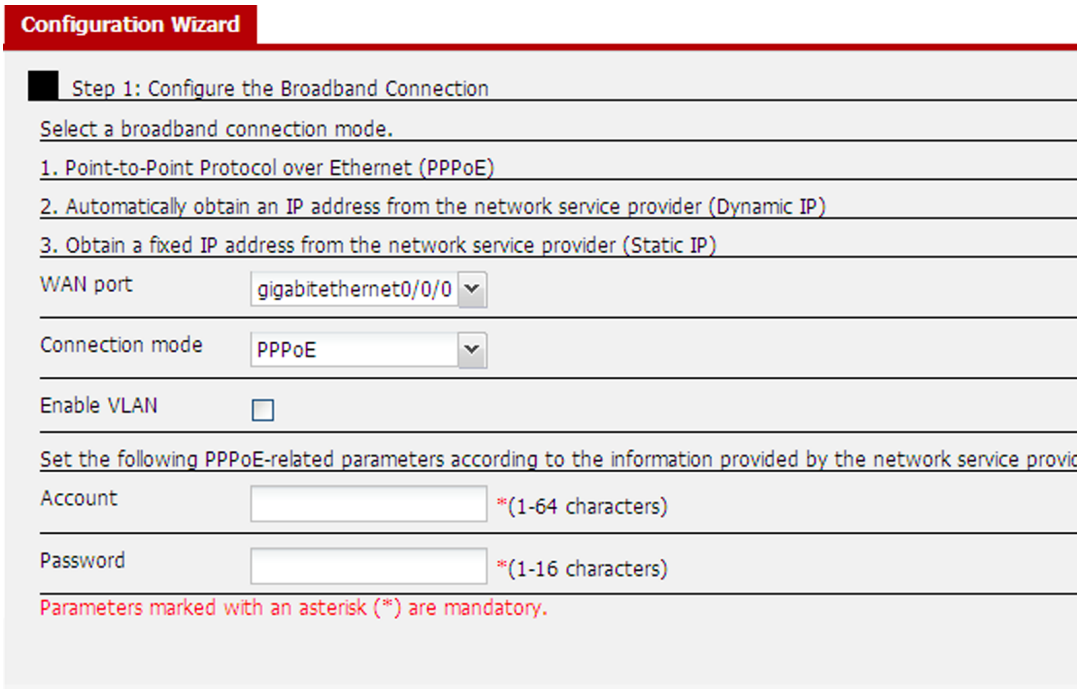
2. Click **Next** to configure a WAN connection.

Step 3 Configure a WAN connection.

1. Set WAN connection parameters.

   Set **Connection mode** to **PPPoE**.

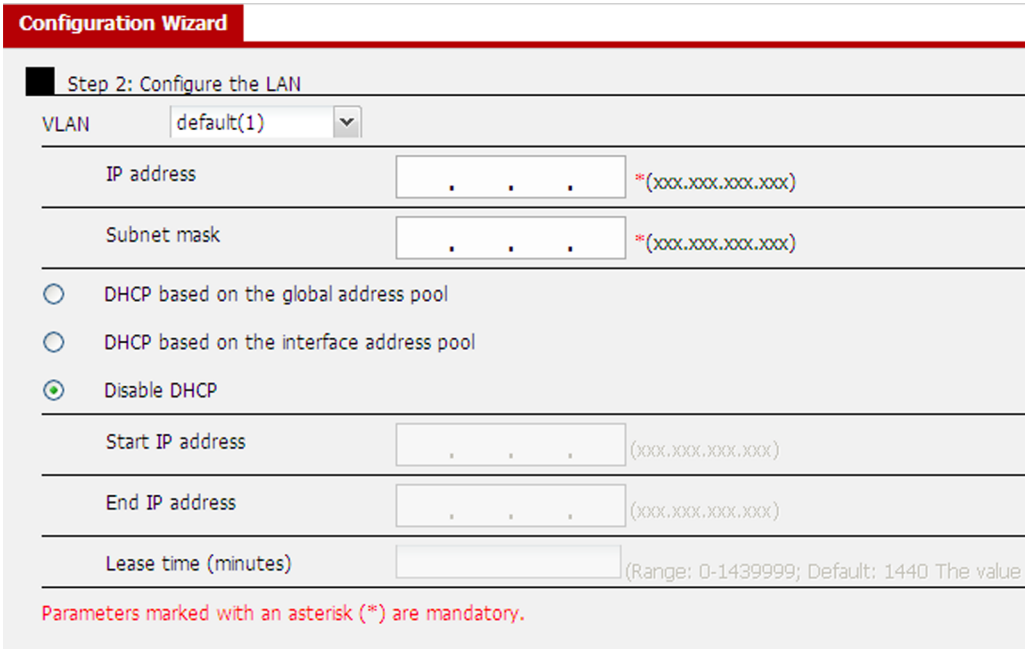
Copyright © Huawei Technologies Co., Ltd.



2. Click **Next** to finish the WAN connection configuration and open the **Configure the LAN** page.

Step 4 Configure LAN access.

1. Set LAN access parameters.

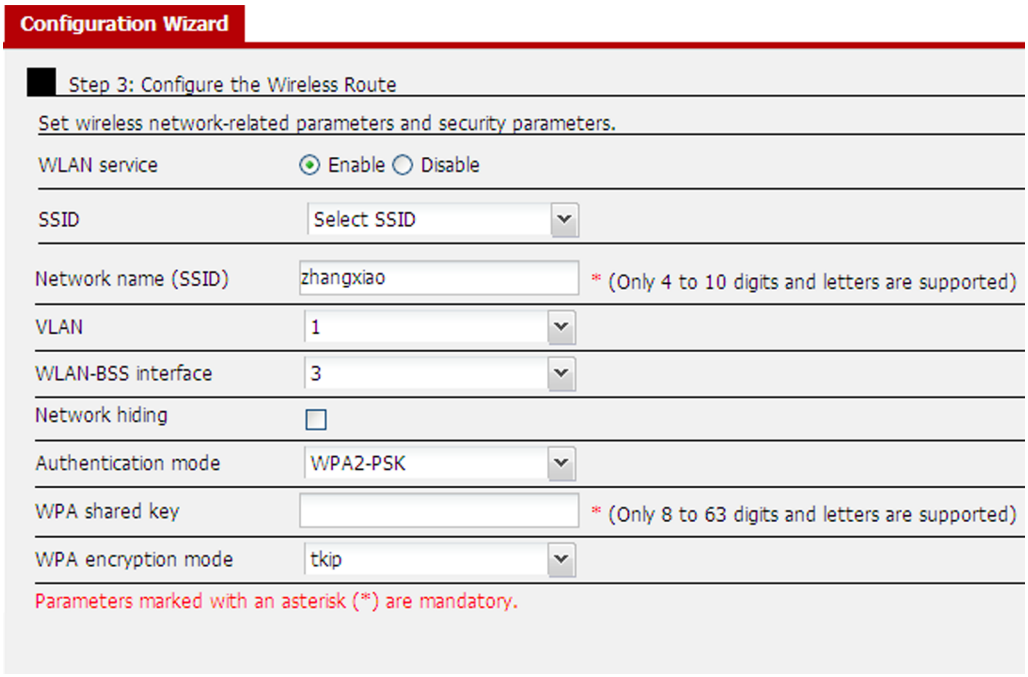


2. Click **Next** to finish the LAN access configurations. If your router supports WLAN, the web system displays the WLAN configuration page. If your router does not support WLAN, the web system displays the **Finish** page. Skip to step 6.

Step 5 Configure WLAN access.

1. Set WLAN parameters.

Copyright © Huawei Technologies Co., Ltd.



2. Click **Next** to finish the WLAN access configurations and open the **Finish Configuration Wizard** page.

Step 6 Confirm the configurations.

View the configurations on the **Finish Configuration Wizard** page. To confirm the configurations, click **Finish**. To modify the configurations, click **Previous**. If you quit the wizard without clicking **Finish**, the configurations will not take effect.

----End

6.4 Going Online Using a Static IP Address

This section describes how to go online using a static IP address allocated by the carrier.

Context

To start the wizard, click **Wizard** in the navigation tree. This wizard helps you quickly set Internet access parameters. You can click **Previous** anytime to modify your settings.

Procedure

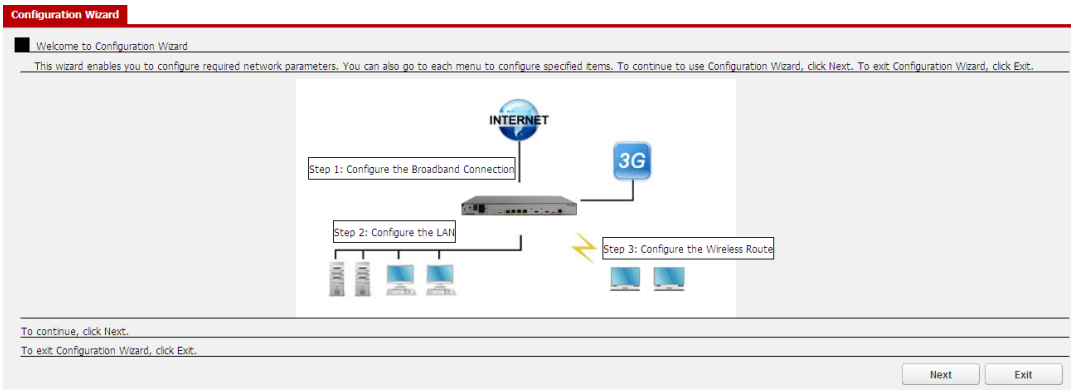
Step 1 (Optional) Configure VLANs. To add an Ethernet interface to a VLAN, see **10.1 Creating VLANs**. To add a WLAN-BSS interface to a VLAN, see **11 Connecting Wireless Users to LANs**.

By default, all LAN-side interfaces on a router belong to VLAN 1. To add a LAN-side interface to another VLAN, perform this step; otherwise, skip this step and start the wizard.

Step 2 Open the **Wizard** page.

1. Click **Wizard** in the navigation tree to open the following page:

Copyright © Huawei Technologies Co., Ltd.

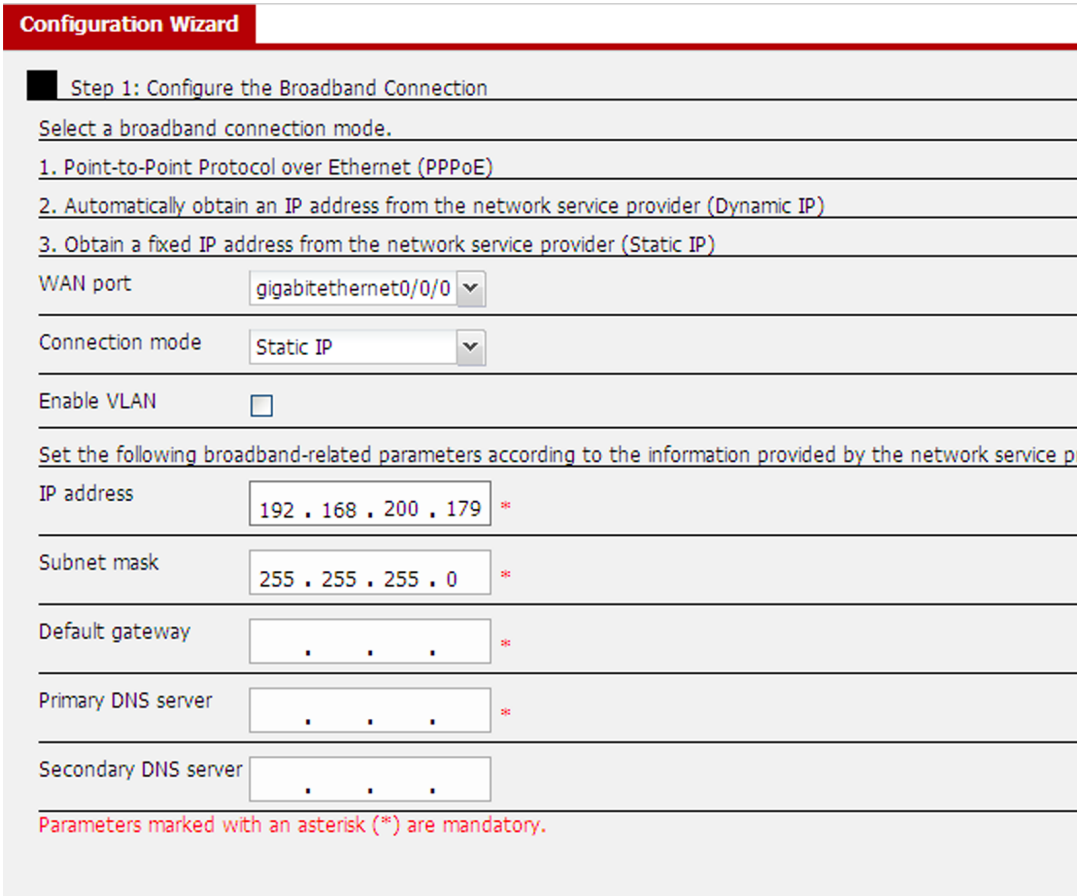


2. Click **Next** to configure a WAN connection.

Step 3 Configure a WAN connection.

1. Set WAN connection parameters.

   Set **Connection mode** to **Manually specify the IP address**.

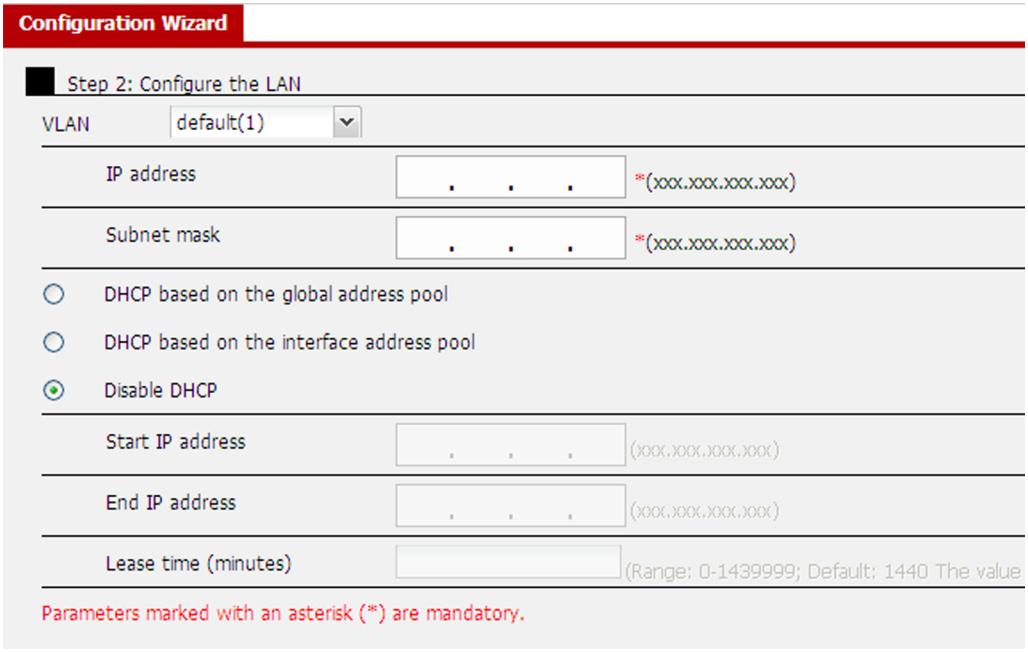


2. Click **Next** to finish the WAN connection configuration and open the **Configure the LAN** page.

Step 4 Configure LAN access.

1. Set LAN access parameters.

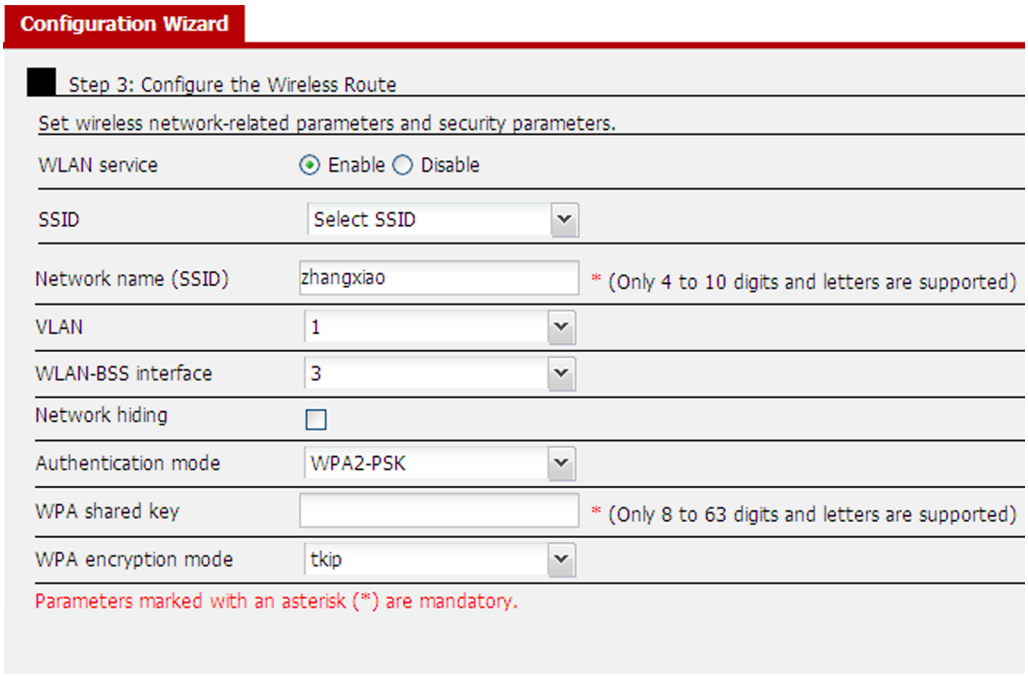
Copyright © Huawei Technologies Co., Ltd.



2. Click **Next** to finish the LAN access configurations. If your router supports WLAN, the web system displays the WLAN configuration page. If your router does not support WLAN, the web system displays the **Finish** page. Skip to step 6.

Step 5 Configure WLAN access.

1. Set WLAN parameters.



2. Click **Next** to finish the WLAN access configurations and open the **Finish Configuration Wizard** page.

Step 6 Confirm the configurations.

Copyright © Huawei Technologies Co., Ltd.

View the configurations on the **Finish Configuration Wizard** page. To confirm the configurations, click **Finish**. To modify the configurations, click **Previous**. If you quit the wizard without clicking **Finish**, the configurations will not take effect.

----End

Copyright © Huawei Technologies Co., Ltd.

7 Configuring Broadband Access

About This Chapter

This section describes how to configure broadband access to the Internet.

7.1 Overview

7.2 Going Online Using a Dynamic IP Address
This section describes how to go online through DHCP.

7.3 Going Online Using PPPoE
This section describes how to go online through PPPoE.

7.4 Going Online Using a Static IP Address
This section describes how to go online using a static IP address allocated by the carrier.

Copyright © Huawei Technologies Co., Ltd.

7.1 Overview

Routers provide three broadband access methods:

- DHCP: User hosts automatically obtain IP addresses from the carrier.
- Static: After subscribing to the broadband service, users obtain fixed IP addresses from the carrier.
- PPPoE: Users subscribe to the PPPoE service to obtain an account and a password from the carrier.

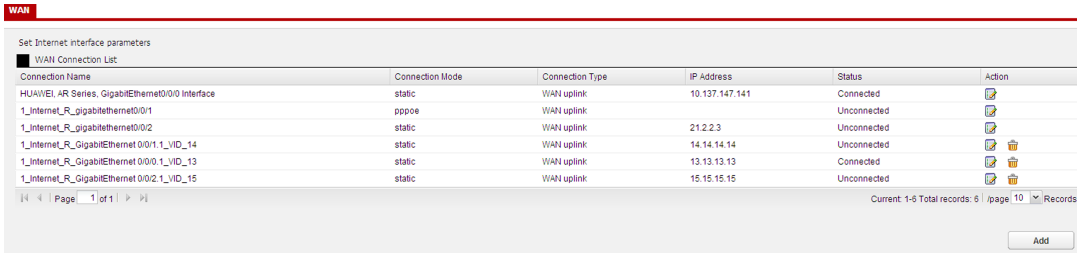
7.2 Going Online Using a Dynamic IP Address

This section describes how to go online through DHCP.

Procedure

Step 1 Choose **Basic Settings** > **Interface** > **WAN** to open the page shown in **Figure 7-1**. The web system displays the connection mode, connection type, IP address, and status of the uplink interfaces.

Figure 7-1 WAN information



Step 2 Use either of the following methods to configure broadband access through DHCP:

- Configure broadband access on a WAN-side interface.

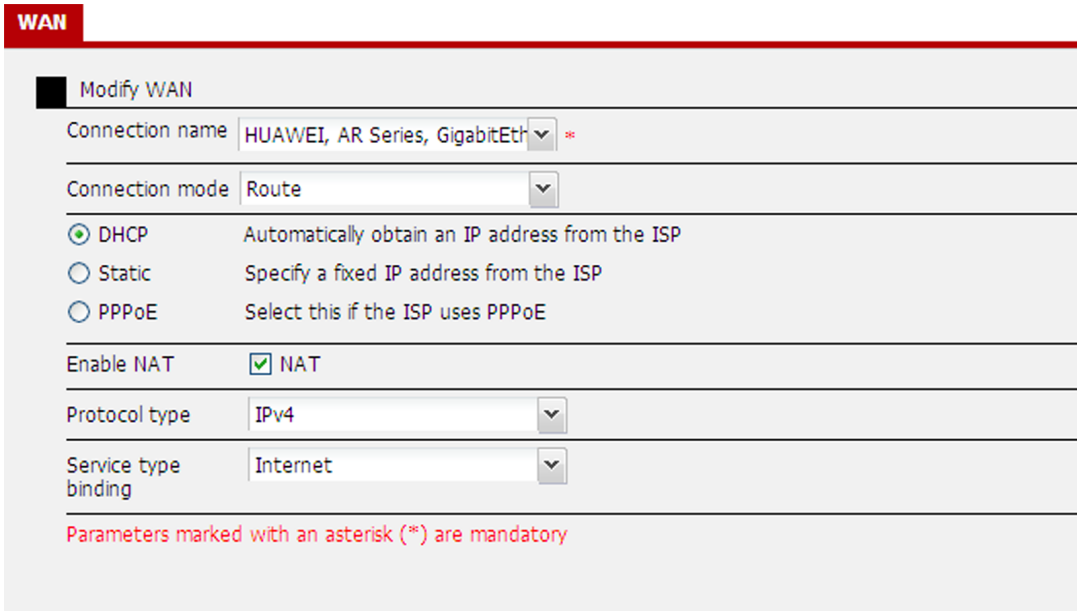
  NOTE

  The web network management system does not support broadband access through an ATM interface.

  Click to open the WAN-side interface setting page, as shown in **Figure 7-2**. Modify the parameters.

Copyright © Huawei Technologies Co., Ltd.

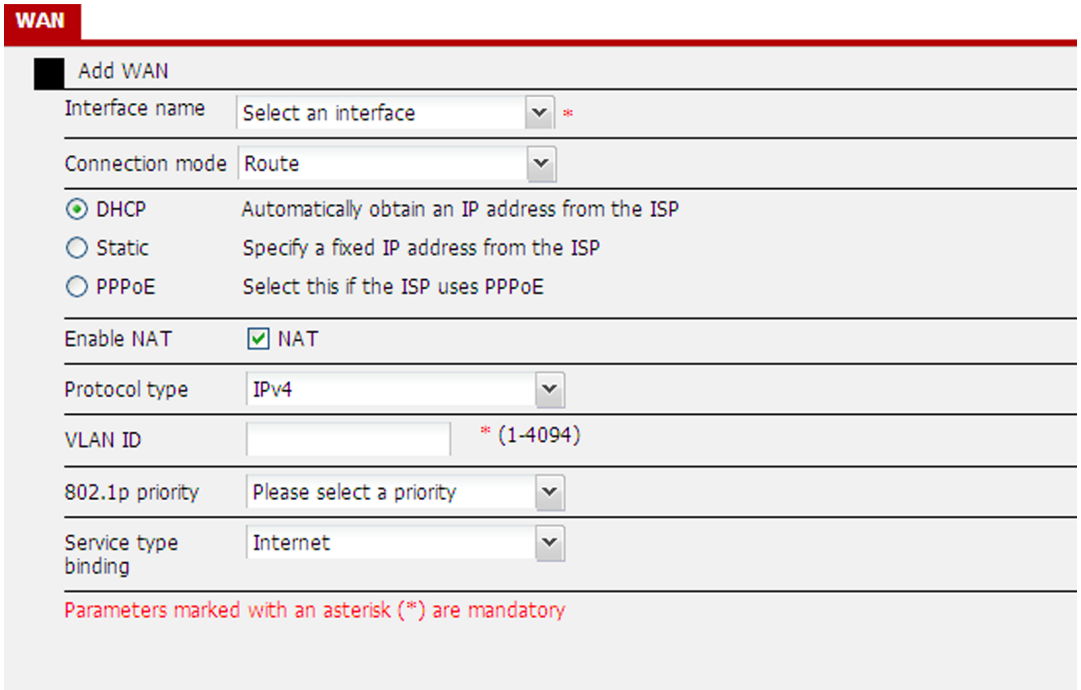
Figure 7-2 Configuring a WAN-side interface



- Configure broadband access on a WAN-side sub-interface.

  Click **Add** to display the page for creating a sub-interface, as shown in **Figure 7-3**. Modify the parameters.

Figure 7-3 Creating a sub-interface



Copyright © Huawei Technologies Co., Ltd.

Step 3 Click **OK** to save the configurations to the configuration file.

----End

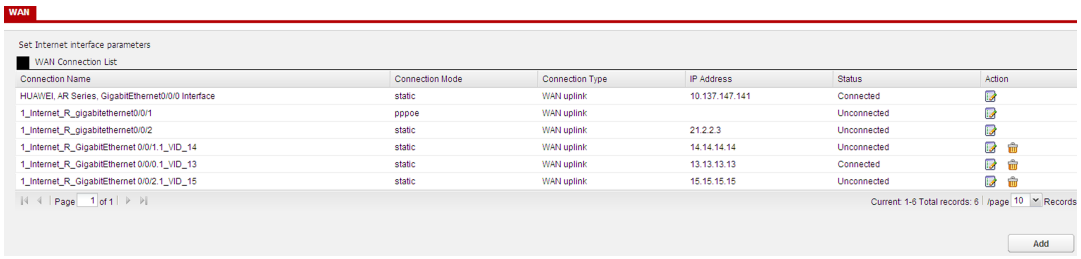
7.3 Going Online Using PPPoE

This section describes how to go online through PPPoE.

Procedure

Step 1 Choose **Basic Settings** > **Interface** > **WAN** to open the page shown in **Figure 7-4**. The web system displays the connection mode, connection type, IP address, and status of the uplink interfaces.

Figure 7-4 WAN information



Step 2 Use either of the following methods to configure broadband access through PPPoE:

- Configure broadband access on a WAN-side interface.

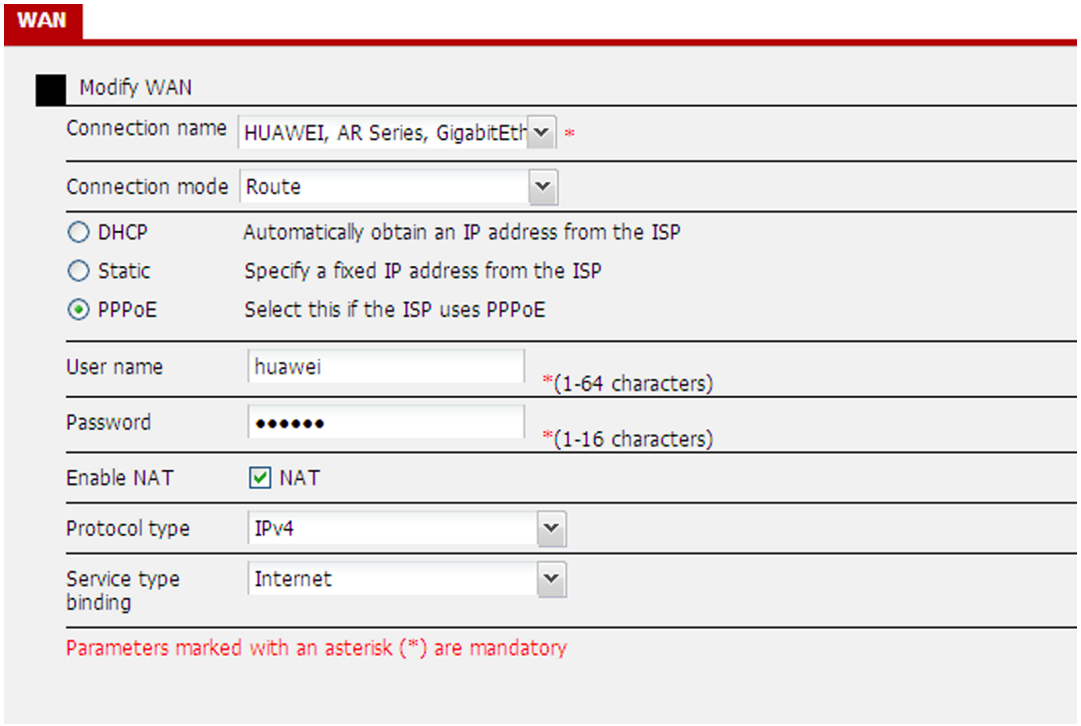
  NOTE

  The web network management system does not support broadband access through an ATM interface.

  Click  to open the WAN-side interface setting page, as shown in **Figure 7-5**. Modify the parameters.

Copyright © Huawei Technologies Co., Ltd.

Figure 7-5 Configuring a WAN-side interface

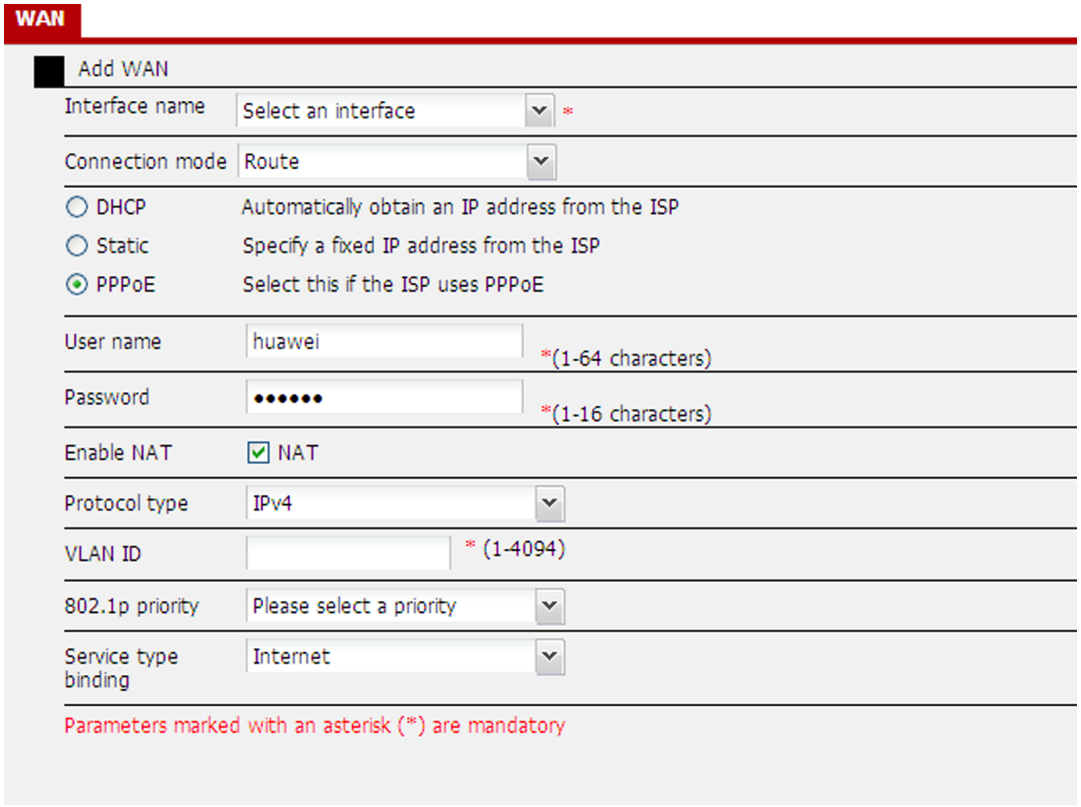


- Configure broadband access on a WAN-side sub-interface.

  Click **Add** to display the page for creating a sub-interface, as shown in **Figure 7-6**. Modify the parameters.

Copyright © Huawei Technologies Co., Ltd.

Figure 7-6 Configuring a sub-interface



Step 3 Click **OK** to save the configurations to the configuration file.

----End

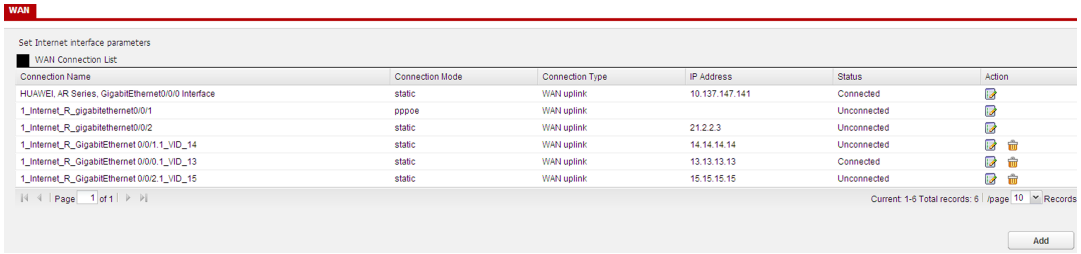
7.4 Going Online Using a Static IP Address

This section describes how to go online using a static IP address allocated by the carrier.

Procedure

Step 1 Choose **Basic Settings** > **Interface** > **WAN** to open the page shown in **Figure 7-7**. The web system displays the connection mode, connection type, IP address, and status of the uplink interfaces.

Figure 7-7 WAN information



Copyright © Huawei Technologies Co., Ltd.

Step 2 Use either of the following methods to configure broadband access using static IP addresses:

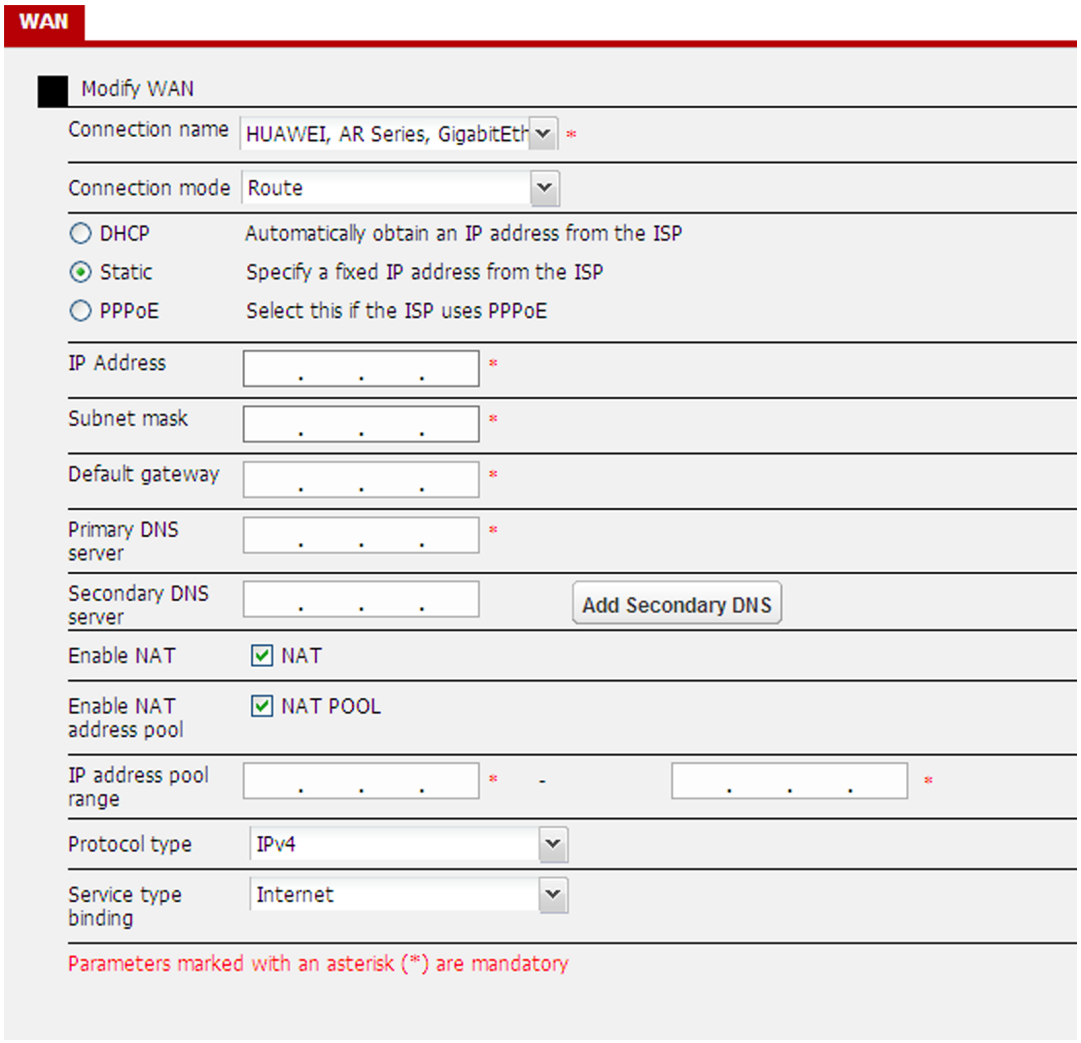
- Configure broadband access on a WAN-side interface.

  NOTE

  The web network management system does not support broadband access through an ATM interface.

  Click to open the WAN-side interface setting page, as shown in **Figure 7-8**. Modify the parameters.

Figure 7-8 Configuring a WAN-side interface

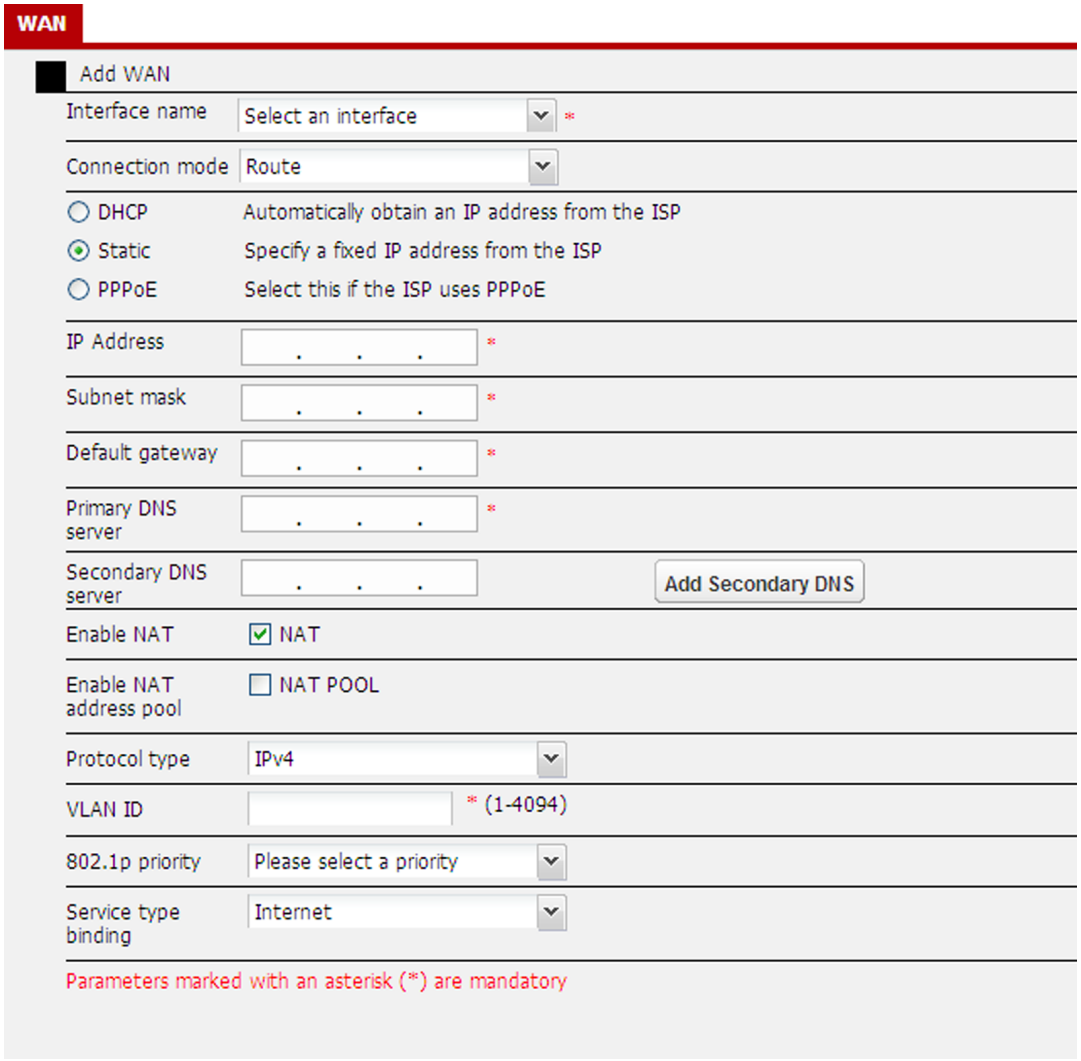


- Configure broadband access on a WAN-side sub-interface.

  Click **Add** to display the page for creating a sub-interface, as shown in **Figure 7-9**. Modify the parameters.

Copyright © Huawei Technologies Co., Ltd.

Figure 7-9 Creating a sub-interface



Step 3 Click **OK** to save the configurations to the configuration file.

----End

Copyright © Huawei Technologies Co., Ltd.

8 Going Online Through 3G

This section describes how to go online through 3G.

Context

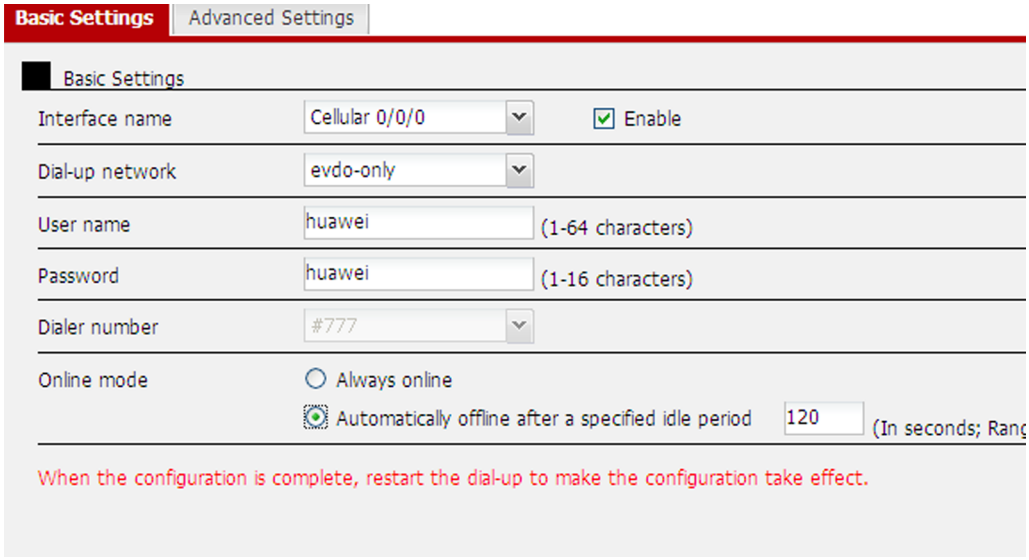
After you subscribe to the 3G service from your carrier and install the wireless card on your router, you can use the 3G service to connect to the Internet. If you fail to go online through broadband, try the 3G mode.

Procedure

Step 1 Set basic 3G parameters.

Choose **Basic Settings** > **Interface** > **3G** to open the page shown in **Figure 8-1**.

Figure 8-1 Basic 3G parameters



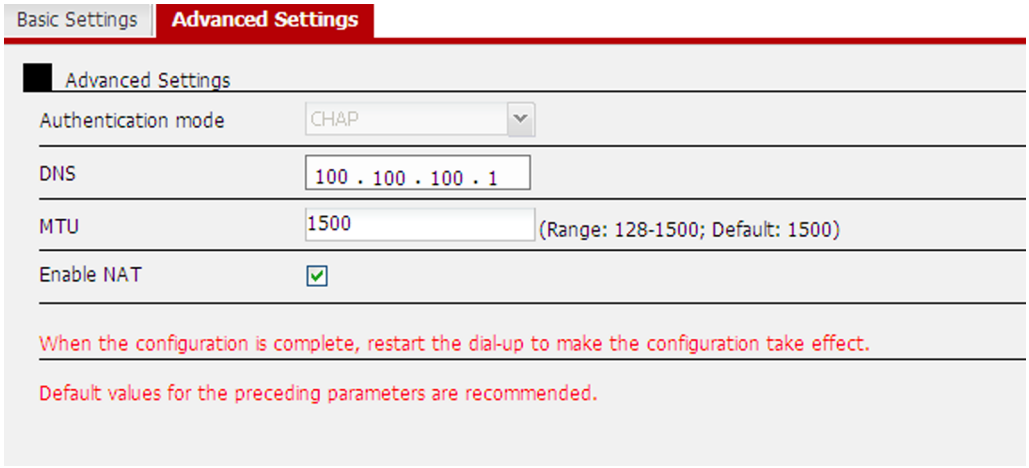
After completing the configuration, click **OK** to make the settings take effect.

Step 2 (Optional) Set advanced 3G parameters.

Copyright © Huawei Technologies Co., Ltd.

Choose **Basic Settings** > **Interface** > **3G** > **Advanced Settings** to open the page shown in **Figure 8-2**.

Figure 8-2 Advanced 3G parameters



After completing the configuration, click **OK** to make the settings take effect.

----End

Copyright © Huawei Technologies Co., Ltd.

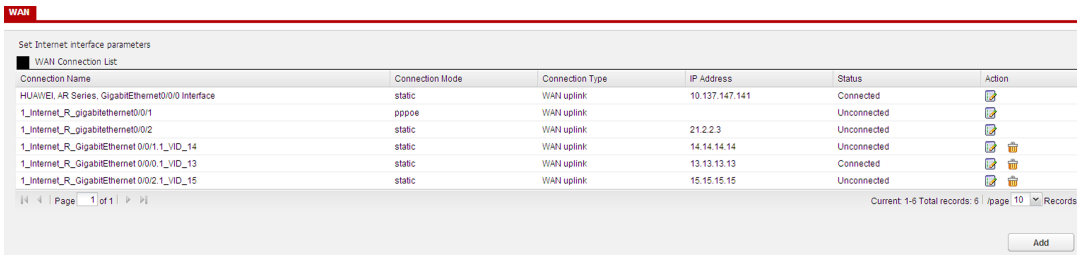
9 Connecting LANs Using a Transparent Bridge

This section describes how to connect LANs using a transparent bridge.

Procedure

Step 1 Choose **Basic Settings** > **Interface** > **WAN** to open the page shown in **Figure 9-1**. The web system displays the connection mode, connection type, IP address, and status of the uplink interfaces.

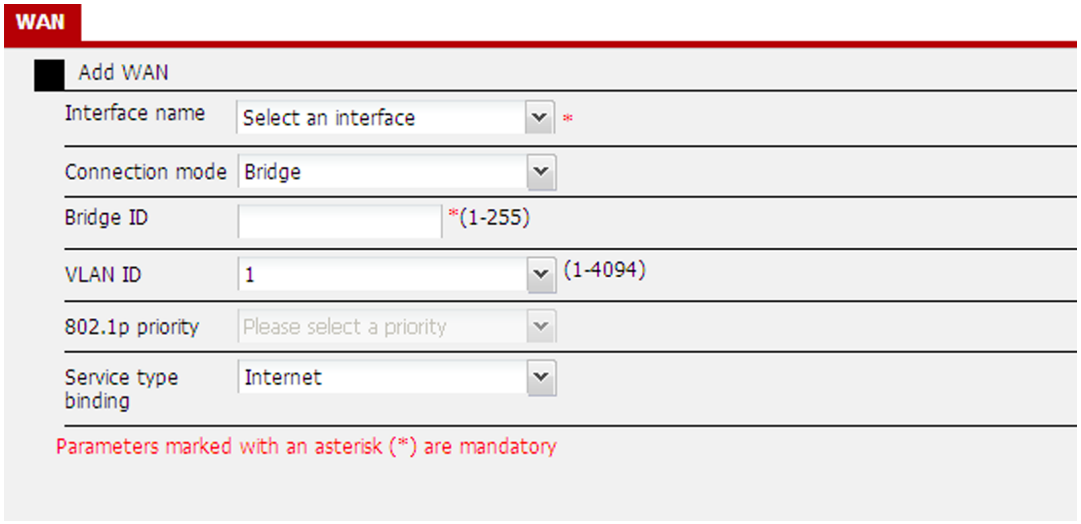
Figure 9-1 WAN information



Step 2 Click **Add** to display the page for creating a sub-interface, as shown in **Figure 9-2**. Modify the parameters.

Copyright © Huawei Technologies Co., Ltd.

Figure 9-2 Configuring bridge on a sub-interface



Step 3 Click **OK** to save the configurations to the configuration file.

----End

Copyright © Huawei Technologies Co., Ltd.

10 Creating and Connecting VLANs

About This Chapter

This section describes how to create and connect virtual local area networks (VLANs).

10.1 Creating VLANs
This section describes how to create virtual local area networks (VLANs).

10.2 Connecting VLANs
This section describes how to configure the VLANIF interface and DHCP service to connect VLANs.

Copyright © Huawei Technologies Co., Ltd.

10.1 Creating VLANs

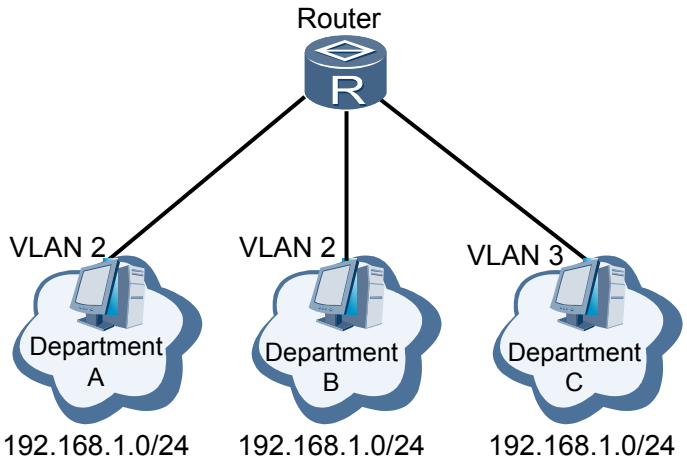
This section describes how to create virtual local area networks (VLANs).

Context

To isolate a department from other departments in an enterprise, create VLANs on the router and add departments to different VLANs.

As shown in **Figure 10-1**, departments A, B, and C are located on the same LAN and are assigned IP addresses in the same network segment. To isolate department C from the others, create a different VLAN for department C.

Figure 10-1 Creating VLANs



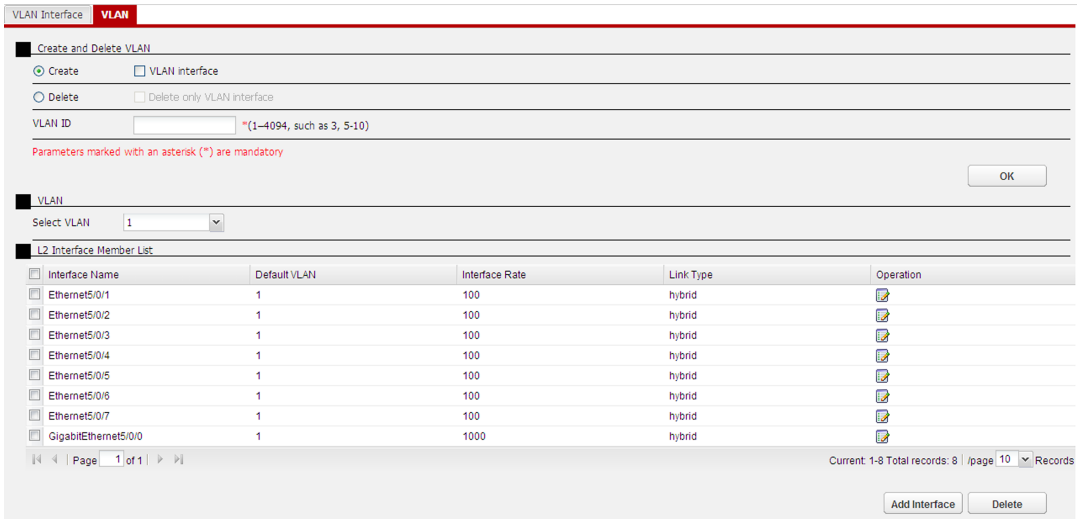
Procedure

Step 1 Enter the **VLAN** page.

After you log in to the Web NMS, choose **Basic Settings** > **Interface** > **LAN** > **VLAN**. The **VLAN** page is displayed, as shown in **Figure 10-2**.

Copyright © Huawei Technologies Co., Ltd.

Figure 10-2 VLAN settings



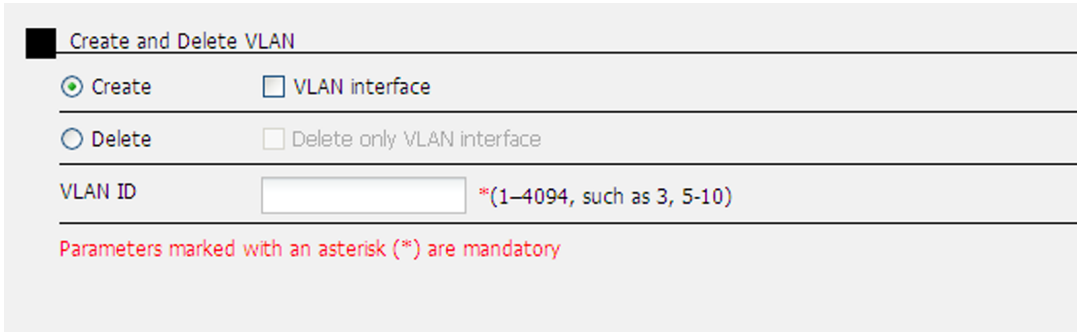
Step 2 Create a VLAN.

Select **Create**, set the VLAN ID to 2, and click **OK**.

Perform the similar operations to create VLAN 3.

CAUTION

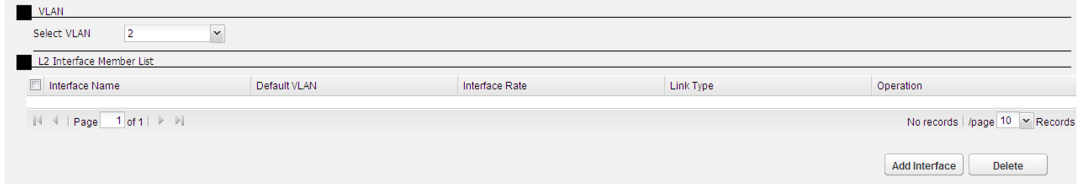
Do not create VLANIF interfaces when creating VLANs.



Step 3 Add interfaces to the VLAN.

1. As shown in **Figure 10-3**, select VLAN 2 and click **Add Interface**. The **Add Member Interface** page is displayed.

Figure 10-3 Adding interfaces to the VLAN

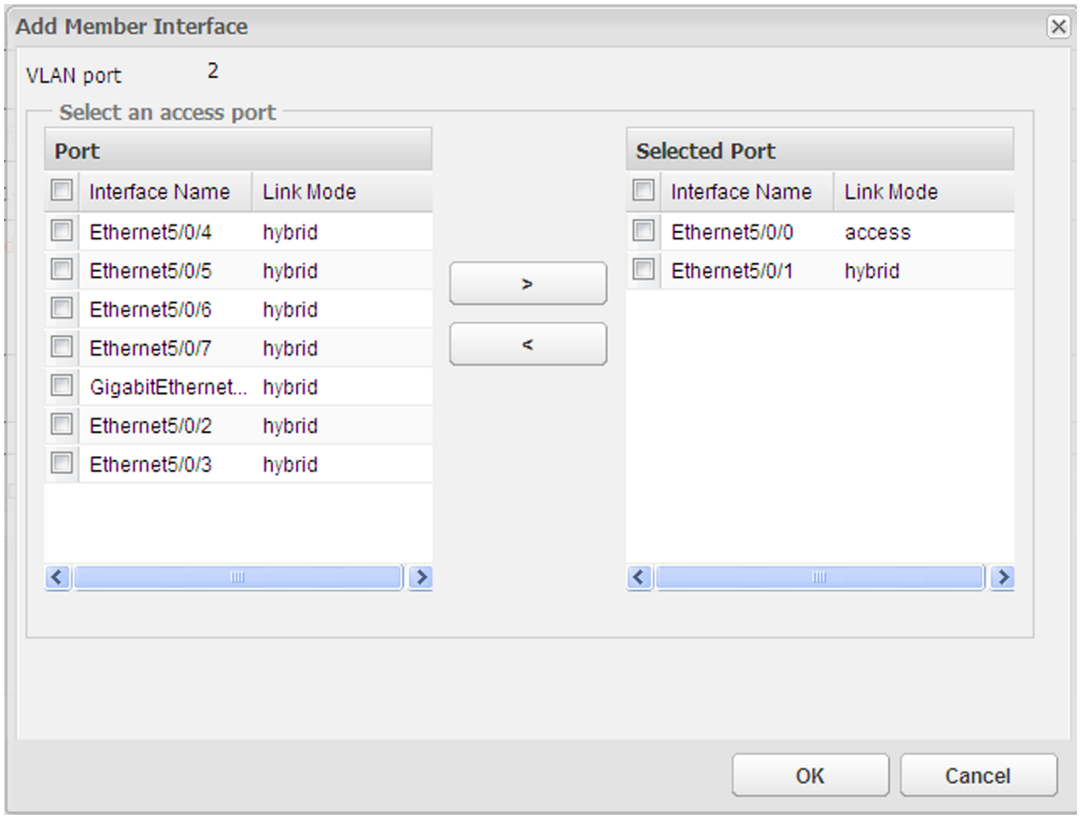


Copyright © Huawei Technologies Co., Ltd.

2. As shown in **Figure 10-4**, add selected interfaces to VLAN 2.
   - Select interfaces in the **Interfaces to select** list on the left and click >. The selected interfaces are added to the **Interfaces selected** list on the right.
   - To remove interfaces from the **Interfaces selected** list on the right, click <<.
   - Click **OK**. The interfaces in the **Interfaces selected** list are added to VLAN 2.

   Perform the similar operations to add interfaces to VLAN 3.

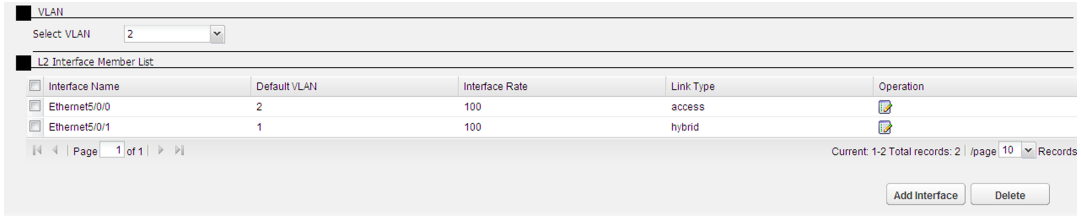
Figure 10-4 Adding interfaces



Step 4 Change the interface type.

1. As shown in **Figure 10-5**, select VLAN 2 from the drop-down list box. The list of interfaces added to VLAN 2 is displayed. Click . In a displayed dialog box, click **OK**.

Figure 10-5 VLAN interface member list

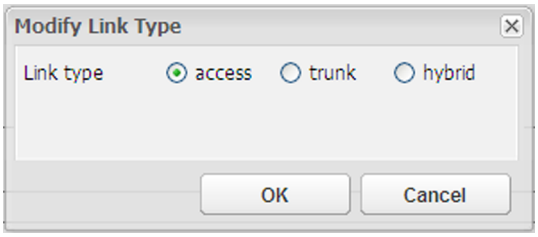


2. As shown in **Figure 10-6**, in the **Modify Link Mode** dialog box, select **access** and click **OK**.

Copyright © Huawei Technologies Co., Ltd.

Perform the similar operations to change the link type of the VLAN 3 interface to **access**.

Figure 10-6 Changing the link type of a VLAN interface



----End

10.2 Connecting VLANs

This section describes how to configure the VLANIF interface and DHCP service to connect VLANs.

Context

You can use gateways to enable users in different VLANs to communicate with each other.

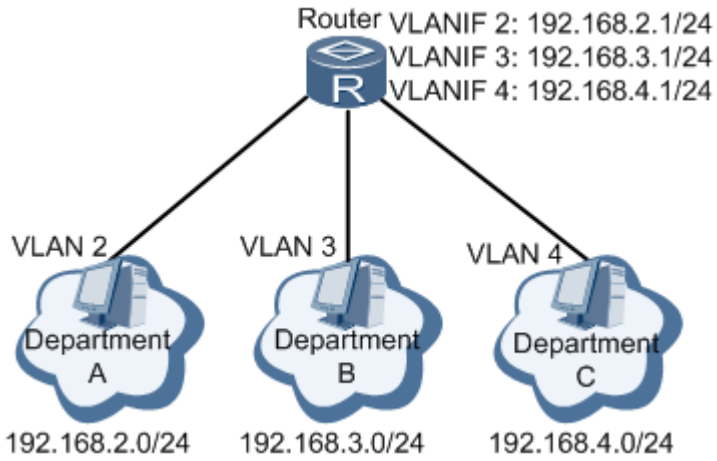
The IP address of the VLANIF interface is used as the gateway address and the VLANIF interface is enabled with DHCP so that user terminals connected to the VLANIF interface can dynamically obtain network parameters such as IP addresses using DHCP.

As shown in **Figure 10-7**, departments A, B, and C belong to different network segments and require communication. You can create VLANIF interfaces for the three departments on the router, configure the VLANIF interface's IP address as the gateway address, and enable DHCP on each VLNAIF interface so that user terminals can obtain network parameters such as the IP address using DHCP.

NOTE

If a DHCP server has been deployed on the network, the DHCP server function can be disabled on the VLANIF interface, the DHCP server can be disabled.

Figure 10-7 Connecting VLANs



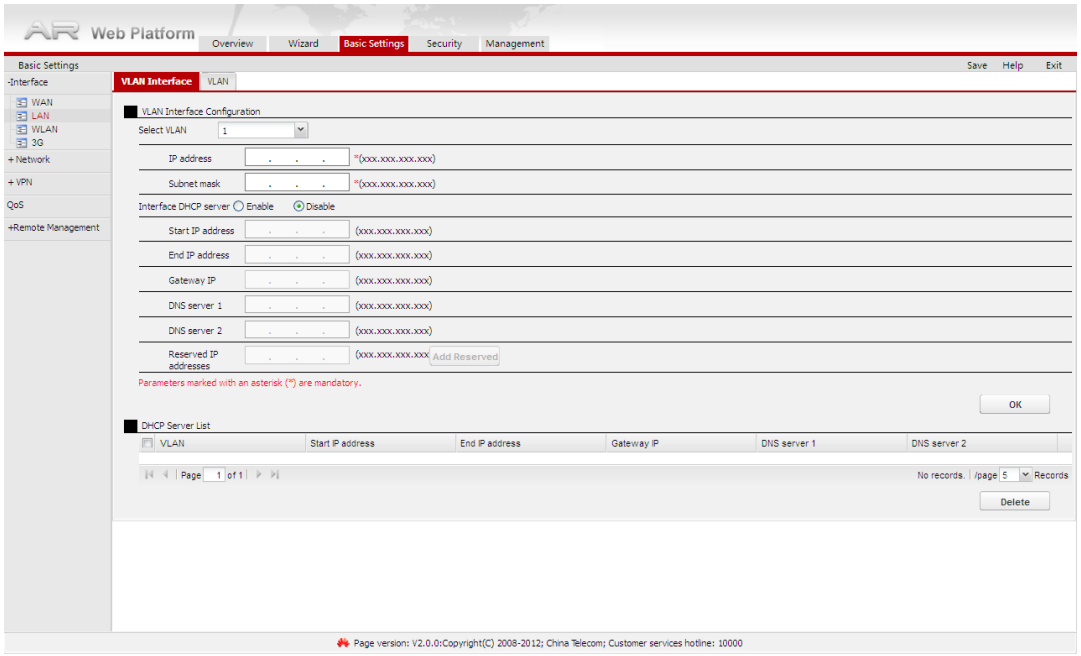
Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Create VLAN 2, VLAN 3, and VLAN 4, add interfaces to VLANs, and change the link type of interfaces to **access**. For details, see **10.1 Creating VLANs**.

Step 2 Choose **Basic Settings** > **Interface** > **LAN** > **VLAN Interface**. The **VLAN Interface** page is displayed, as shown in **Figure 10-8**.

Figure 10-8 VLAN interface settings (1)



Step 3 Configure and enable the DHCP service.

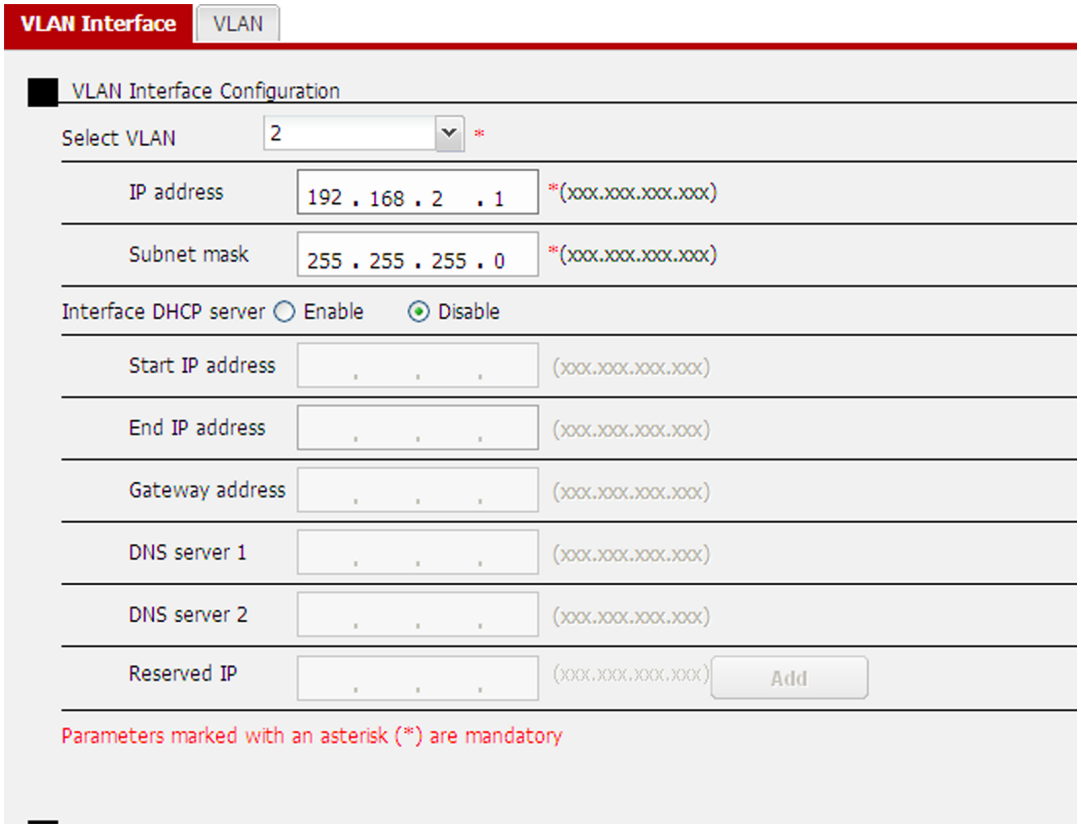
In **Figure 10-9**, select VLAN 2, and enter the IP address 192.168.2.1 and subnet mask 255.255.255.0. Select **Enable** for the DHCP server function on the VLANIF interface. Then the system generates an IP address pool and a gateway address. The IP address pool and gateway IP address are automatically generated. Click **OK**.

Perform the similar operations to configure VLANIF 3, with the IP address set to 192.168.3.1 and subnet mask set to 255.255.255.0.

Perform the similar operations to configure VLANIF 4, with the IP address set to 192.168.4.1 and subnet mask set to 255.255.255.0.

Copyright © Huawei Technologies Co., Ltd.

Figure 10-9 VLAN interface settings (2)

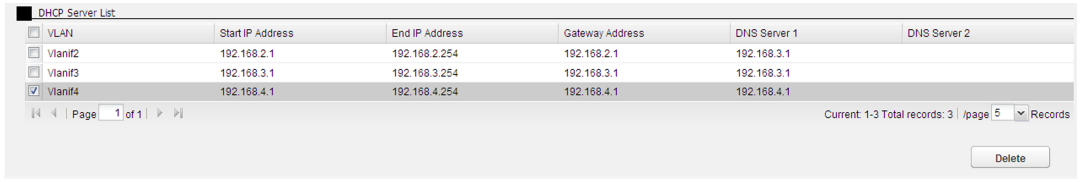


NOTE

- If all IP addresses of user terminals are assigned statically, select **Disable** for the DHCP server function on the VLANIF interface.
- If some IP addresses of user terminals are assigned statically, add the static IP addresses to the **Reserved IP addresses** text box. You can add a maximum of eight reserved IP addresses.
- If user terminals require DNS resolution, add the DNS server IP address to the **DNS server 1** text box. The **DNS server 2** text box is for a standby IP address.

Step 4 (Optional) If a VLANIF interface uses a static IP address, delete the DHCP server configuration from the VLANIF interface, as shown in **Figure 10-10**.

Figure 10-10 DHCP server list



----End

Copyright © Huawei Technologies Co., Ltd.

11 Connecting Wireless Users to LANs

This section describes how to connect wireless users to LANs.

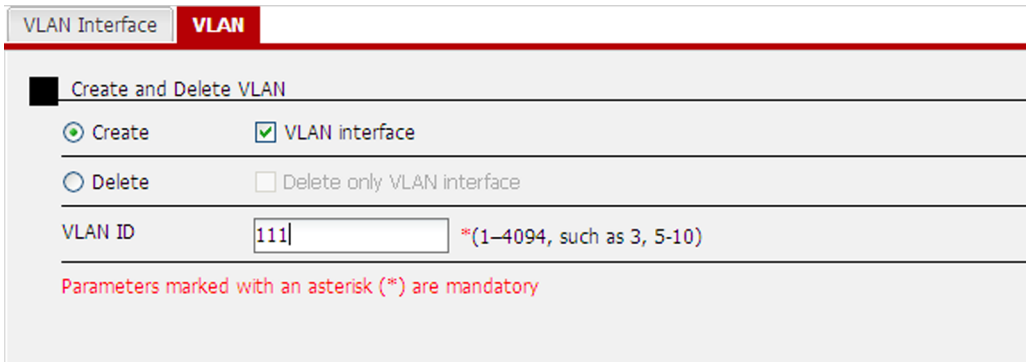
Procedure

Step 1 Create a VLAN that wireless users belong to.

Choose **Basic Settings** > **Interface** > **LAN** > **VLAN**. The **VLAN** page is displayed, as shown in **Figure 11-1**. Select **Create** and **Create VLAN interface**. Enter the ID of the VLAN you have just created.

Click **OK**.

Figure 11-1 Creating a VLAN



Step 2 Configure the VLANIF interface and DHCP server.

Choose **Basic Settings** > **Interface** > **LAN** > **VLAN Interface**. The **VLAN Interface** page is displayed, as shown in **Figure 11-2**. Select the created VLAN from the **Select VLAN** drop-down list box and configure an IP address for the VLANIF interface. Select **Enable** for the DHCP server function on the VLANIF interface, and set the DHCP and DNS. To prevent the DHCP server from assigning some IP addresses, enter the IP addresses in the **Reserved IP addresses** text box.

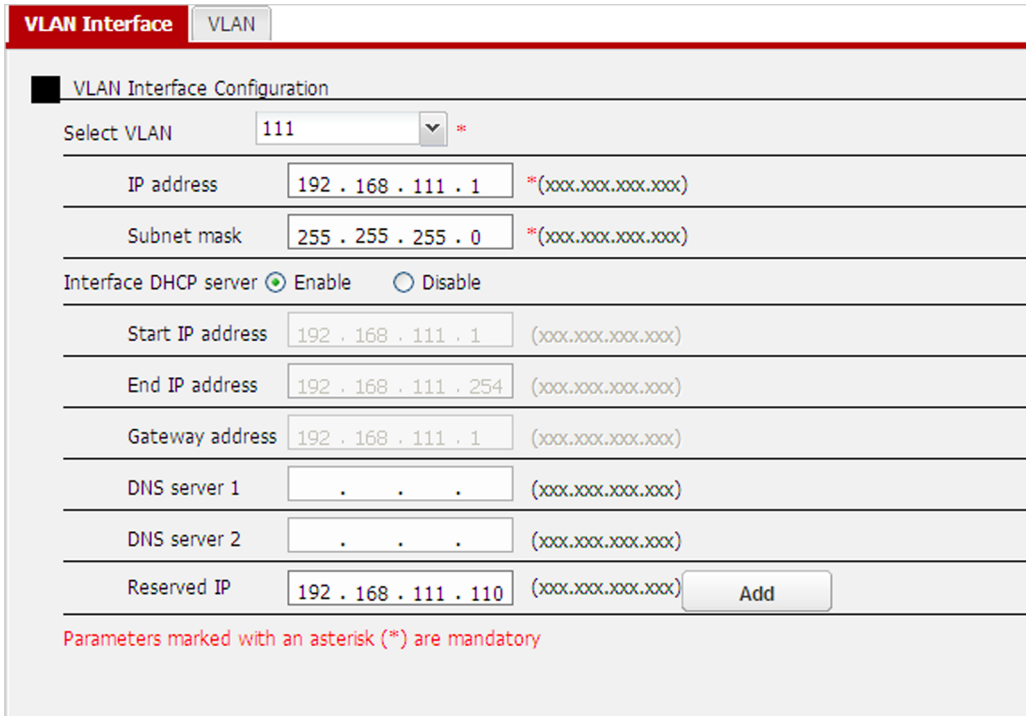
NOTE

If a DHCP server has been deployed on the network to assign IP addresses to all connected users, no more DHCP server needs to be configured.

Click **OK**.

Copyright © Huawei Technologies Co., Ltd.

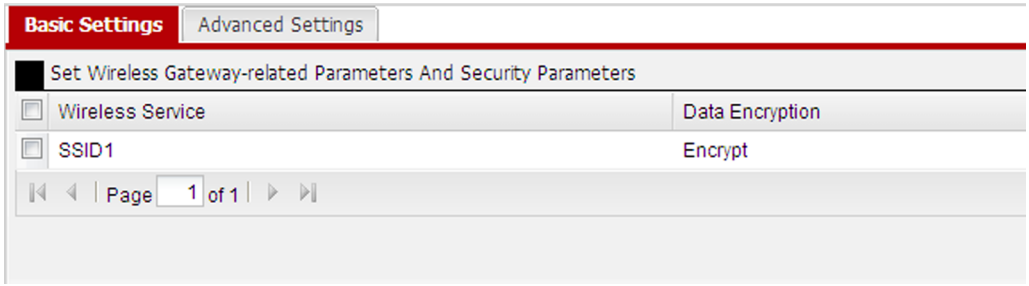
Figure 11-2 VLAN interface settings



Step 3 Create and configure the wireless service.

Choose **Basic Settings** > **Interface** > **WLAN**. The **WLAN** page is displayed, as shown in **Figure 11-3**.

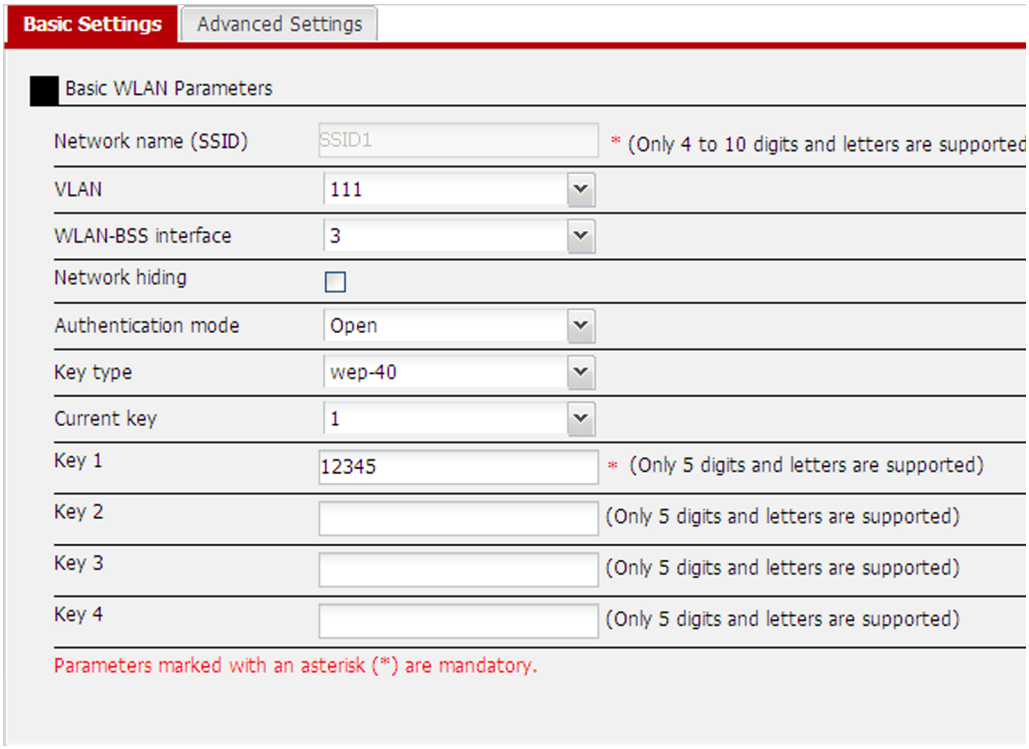
Figure 11-3 WLAN interface settings



- Created wireless services are displayed in **Wireless Service**. To modify parameters, click **Operation**.
- To create wireless services, click **Create**. The page for basic wireless service settings is displayed, as shown in **Figure 11-4**.

Copyright © Huawei Technologies Co., Ltd.

Figure 11-4 Basic WLAN interface settings

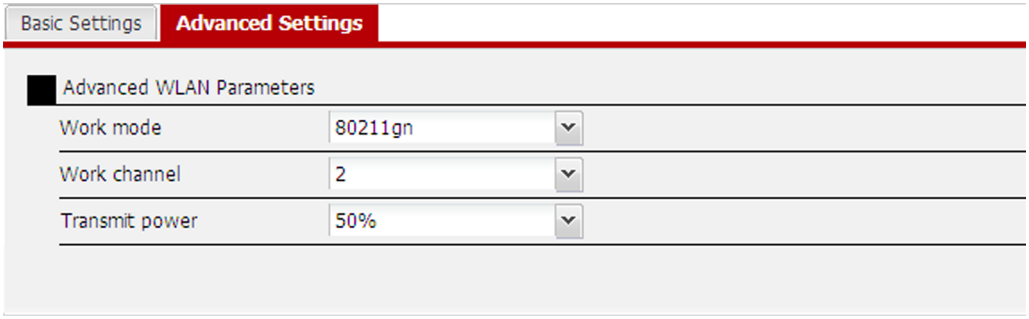


To configure advanced WLAN interface settings, click **Advanced Settings**. The page for advanced wireless service settings is displayed, as shown in **Figure 11-5**.

NOTE

Advanced WLAN interface settings only need to be performed on ARs but not clients.

Figure 11-5 Advanced WLAN interface settings



Click **Apply**.

Click **OK**.

Step 4 Enable a wireless service.

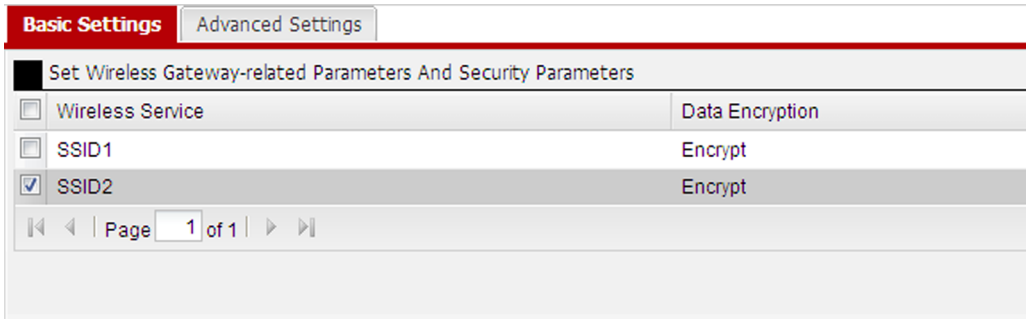
Choose **Basic Settings** > **Interface** > **WLAN**. The **WLAN** page is displayed, as shown in **Figure 11-6**. Select a disabled service and click **Start**.

NOTE

By default, the wireless service is enabled when it is created.

Copyright © Huawei Technologies Co., Ltd.

Figure 11-6 Enabling a wireless service



----End

Copyright © Huawei Technologies Co., Ltd.

12 Configuring Network Services

About This Chapter

This section describes how to configure network services on the router, including DDNS, advanced NAT, and DHCP.

12.1 Configuring the DDNS Client
The Dynamic Domain Name System (DDNS) client notifies the DDNS server of the changes in mappings between domain names and IP addresses in real time. This function allows the DNS server to maintain the latest mappings between domain names and IP addresses so that it can correctly resolve domain names.

12.2 Configuring Advanced NAT
Using the advanced NAT function, internal servers can provide services to external networks, and internal hosts can use fixed public IP address to access external networks.

12.3 Configuring a DHCP Address Pool
This section describes how to configure a DHCP address pool.

12.4 Configuring Static Routes
This section describes how to configure static routes.

Copyright © Huawei Technologies Co., Ltd.

12.1 Configuring the DDNS Client

The Dynamic Domain Name System (DDNS) client notifies the DDNS server of the changes in mappings between domain names and IP addresses in real time. This function allows the DNS server to maintain the latest mappings between domain names and IP addresses so that it can correctly resolve domain names.

Context

If users of an enterprise go online through PPPoE, the enterprise's servers use the virtual server function (configured in **12.2.2 Configuring a Virtual Server**) to obtain a public IP address and provide services. A server obtains a different IP address every time it dials up. If the server cannot correctly resolve the domain name, the user cannot access the server.

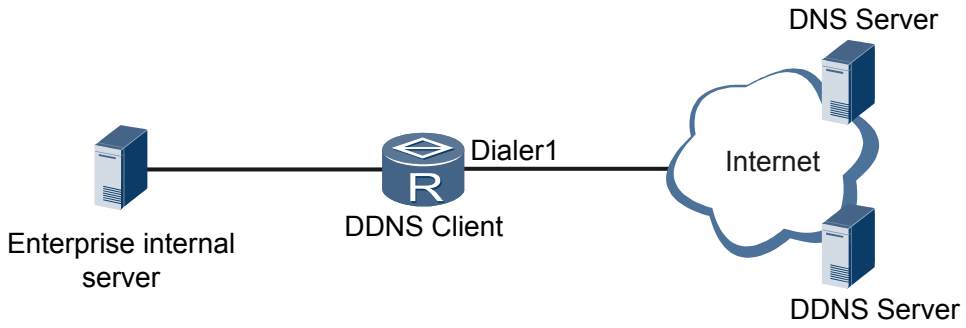
After a DDNS client is configured, the AR router can notify the DDNS server of the latest public IP address of the server. The DDNS server then updates the mappings between domain name and IP address on the DNS server so that the DNS server can resolve the server's domain name into a correct IP address.

NOTE

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

Figure 12-1 shows the DDNS network. The enterprise's server accesses the Internet through PPPoE on Dialer1 of the AR router, and provides services using the IP address of Dialer1. The DDNS client is configured on the AR router. The DDNS client notifies the DDNS server when the public IP address of the server changes, and then the DDNS server notifies the DNS server. Therefore, the DNS server maintains the latest mappings between domain names and IP addresses.

Figure 12-1 Typical networking of DDNS



Prerequisites

You have obtained an account and domain name on the DDNS service provider's website.

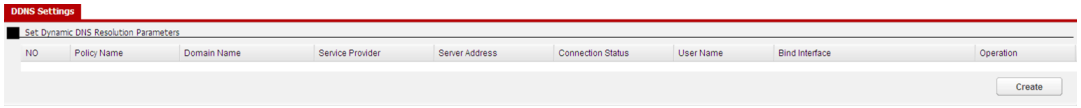
Procedure

- Create a DDNS client.

Copyright © Huawei Technologies Co., Ltd.

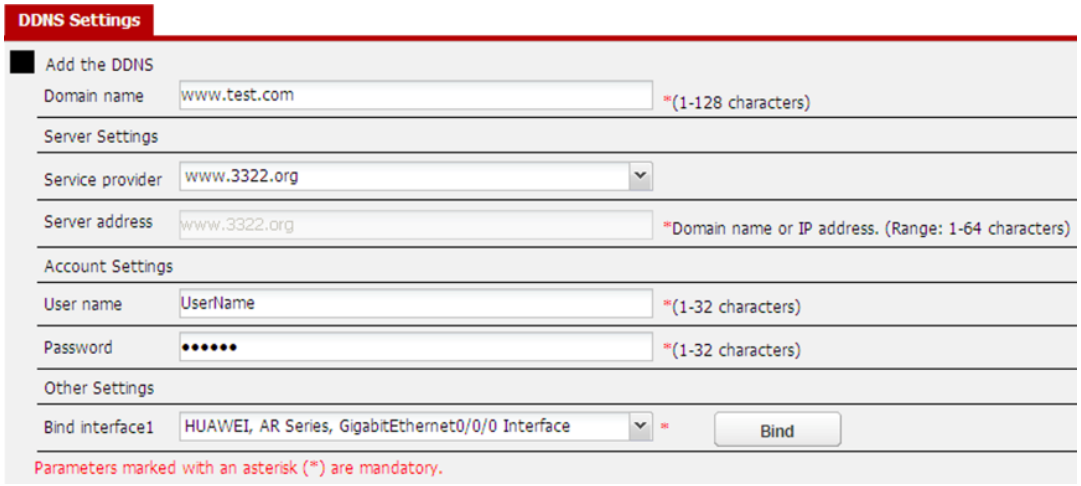
1. Choose **Basic Settings** > **Network** > **DDNS** to open the **DDNS Settings** page, as shown in **Figure 12-2**.

Figure 12-2 Configuring DDNS



2. Click **New** and set the DDNS parameters, as shown in **Figure 12-3**.

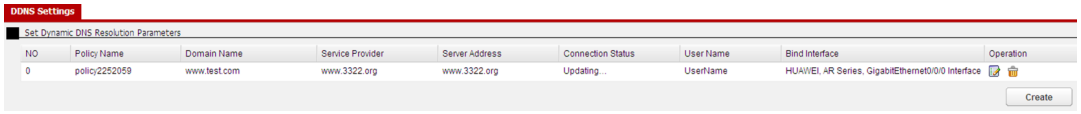
Figure 12-3 Editing DDNS



3. Click **OK** to finish DDNS client configuration.

- Modify the DDNS client.
  1. Open the **DDNS Settings** page. The created DDNS clients are displayed, as shown in **Figure 12-4**.

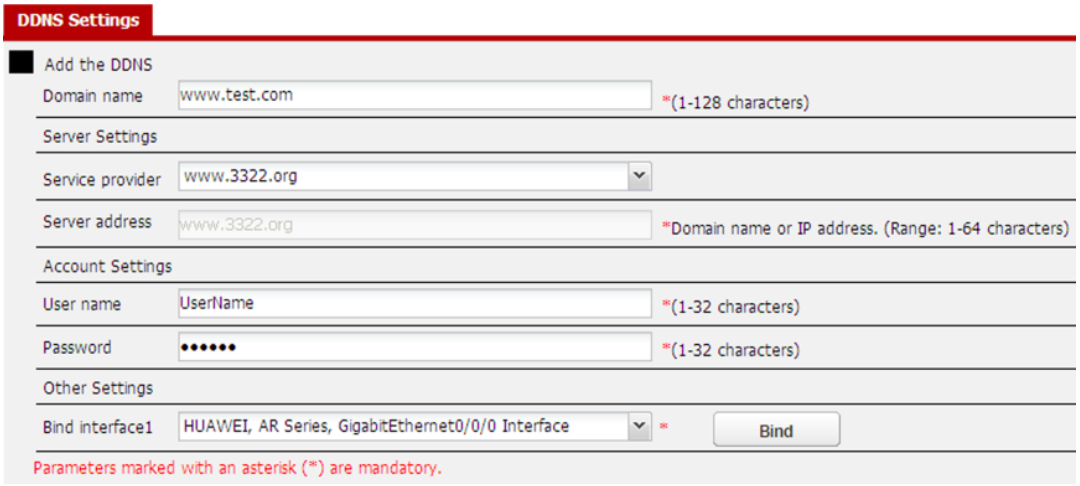
Figure 12-4 DDNS client list



2. Click  to modify DDNS parameters, as shown in **Figure 12-5**.

Copyright © Huawei Technologies Co., Ltd.

Figure 12-5 Editing DDNS parameters

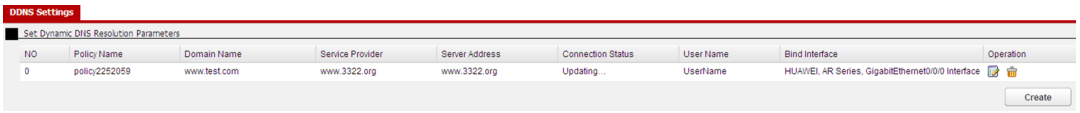


3. Click **OK** to finish DDNS client modification.

- Delete a DDNS client.

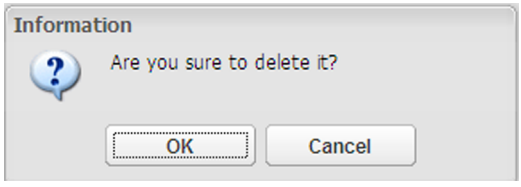
1. Open the **DDNS Settings** page. The created DDNS clients are displayed, as shown in **Figure 12-6**.

Figure 12-6 DDNS client list



2. Select a record and click . The dialog box as shown in **Figure 12-7** is displayed.

Figure 12-7 Deleting a DDNS client



3. Click **OK** to delete the DDNS client.

----End

12.2 Configuring Advanced NAT

Using the advanced NAT function, internal servers can provide services to external networks, and internal hosts can use fixed public IP address to access external networks.

Copyright © Huawei Technologies Co., Ltd.

12.2.1 (Optional) Configuring ALG

The Application Level Gateway (ALG) allows internal servers to provide certain services, such as the FTP and DNS services, to external networks using NAT.

Context

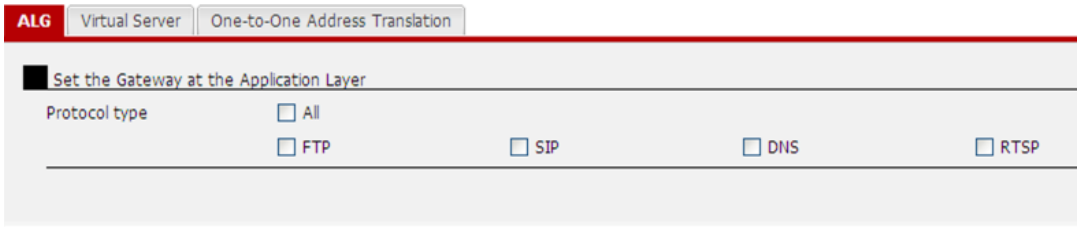
Generally, NAT translates only the address in the IP packet header and the port number in the TCP/UDP header. Packets of some protocols such as DNS and FTP contain the IP address or port number in the data fields. Such contents cannot be translated through NAT. Therefore, communication between the internal 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 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. AR routers provide the ALG function, so they can support various special application protocols, including DNS, FTP, SIP, and RTSP.

Procedure

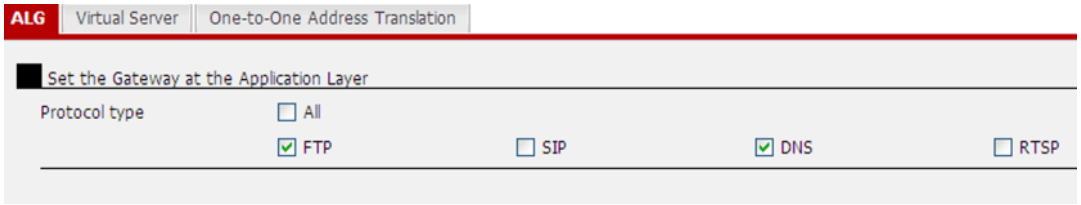
Step 1 Choose **Basic Settings** > **Network** > **NAT** > **ALG** to open the **ALG** page, as shown in **Figure 12-8**.

Figure 12-8 Configuring ALG



Step 2 Select the application protocols used by the enterprise's server, as shown in **Figure 12-9**.

Figure 12-9 Selecting protocols



Step 3 Click **OK** to finish ALG configuration.

----End

12.2.2 Configuring a Virtual Server

After an internal virtual server is configured, external users can access internal servers.

Copyright © Huawei Technologies Co., Ltd.

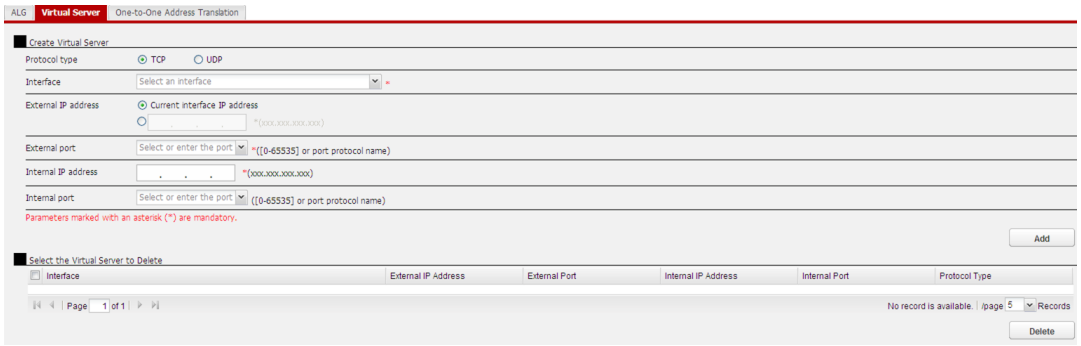
Context

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 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.

Procedure

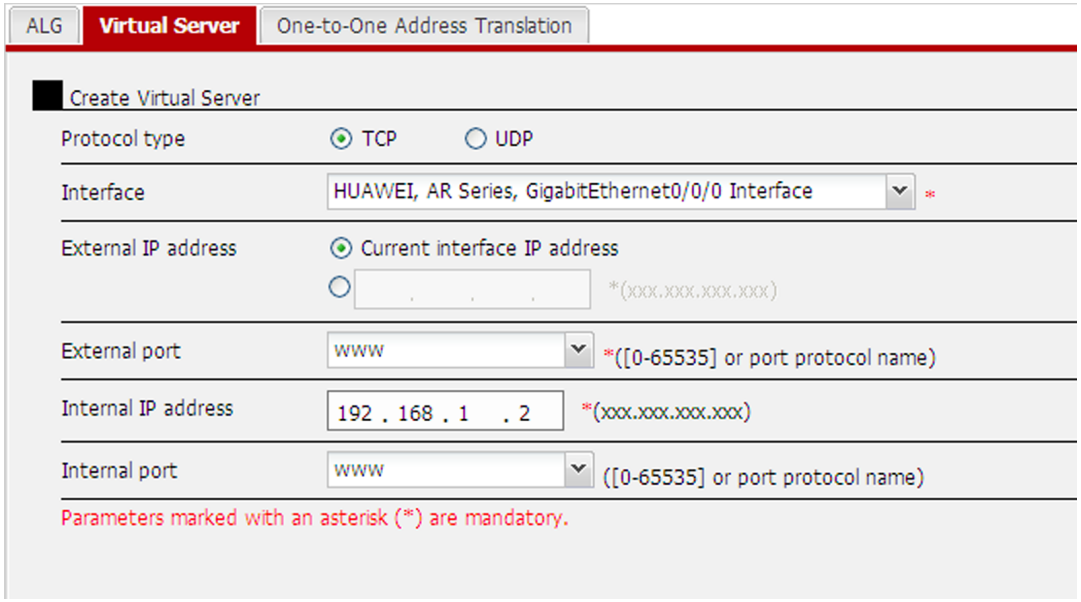
- Create the virtual server.
  1. Choose **Basic Settings** > **Network** > **NAT** > **Virtual Server** to open the **Virtual Server** page, as shown in **Figure 12-10**.

Figure 12-10 Virtual server information



  2. Configure the virtual server, as shown in **Figure 12-11**.

Figure 12-11 Creating a virtual server



  3. Click **Add** to create the virtual server.

Copyright © Huawei Technologies Co., Ltd.

NOTE

The total number of virtual server rules and global static address translation rules varies according to the product model:

- Huawei AR150&200 and AR1200 series: 128
- Huawei AR2200 series: 256
- Huawei AR3200 series: 512

- Delete a virtual server.
  1. Select the virtual server that you want to delete, as shown in **Figure 12-12**.

Figure 12-12 Deleting a virtual server

  2. Click **Delete**.

----End

12.2.3 (Optional) Configuring One-to-One Address Translation

After one-to-one address translation is configured, internal hosts use fixed public IP addresses to communicate with external networks.

Context

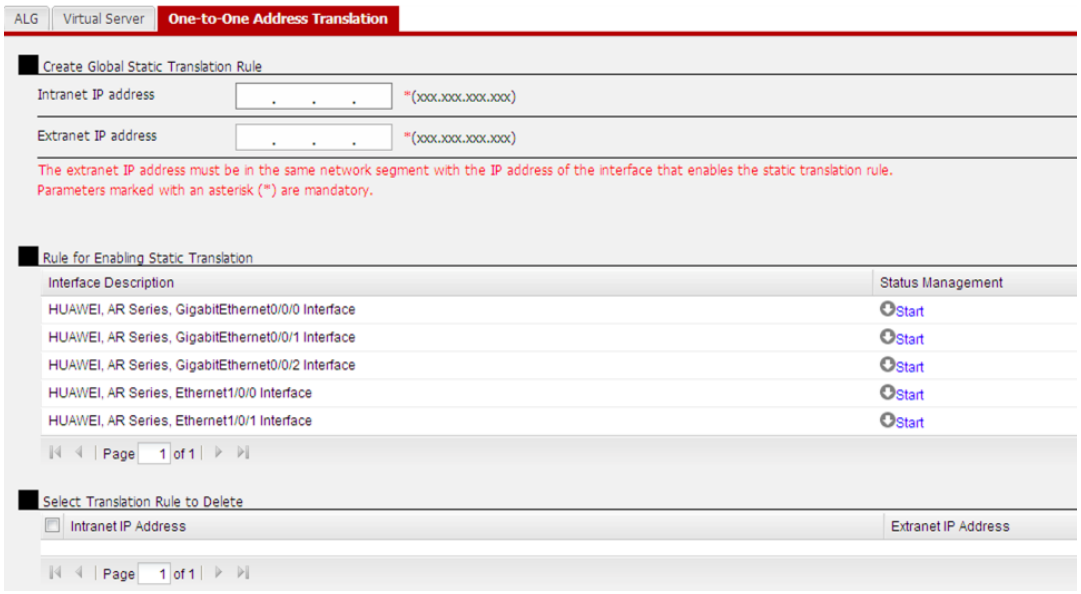
NAT cannot ensure that an internal host use the same IP address to access external networks; however, some hosts must use fixed IP addresses to access external networks. One-to-one address translation maps each public IP address to a fixed internal IP address.

Procedure

- Configure one-to-one address translation.
  1. Choose **Basic Settings** > **Network** > **NAT** > **One-to-one address translation** to open the **One-to-one address translation** page, as shown in **Figure 12-13**.

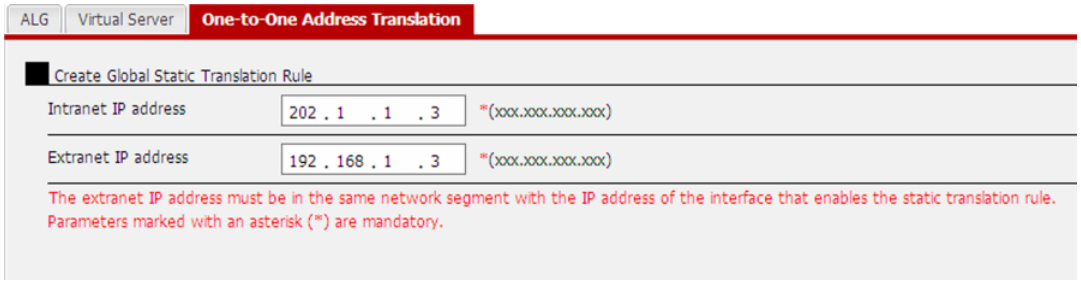
Copyright © Huawei Technologies Co., Ltd.

Figure 12-13 Configuring one-to-one address translation



2. Create a global static address translation rule, as shown in **Figure 12-14**.

Figure 12-14 Creating a global static address translation rule



3. Click **Add**.

   NOTE

   The total number of virtual server rules and global static address translation rules varies according to the product model:

   - Huawei AR150&200 and AR1200 series: 128
   - Huawei AR2200 series: 256
   - Huawei AR3200 series: 512

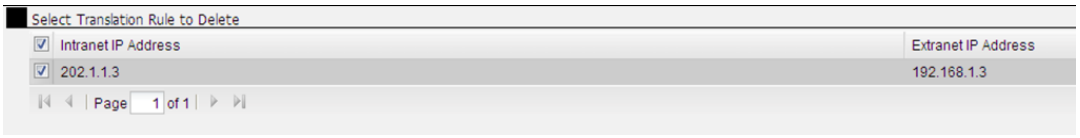
4. Enable the static address translation rule on the interface:
   - The status of the interface with the static address translation rule disabled is Start. Clicking this button can enable the rule.
   - The status of the interface with the static address translation rule enabled is Stop. Clicking this button can disable the rule.

Copyright © Huawei Technologies Co., Ltd.

Figure 12-15 Interfaces with static address translation rule enabled and disabled

- Delete a static address translation rule.
  1. Select the rule that you want to delete, as shown in **Figure 12-16**.

Figure 12-16 Deleting a static address translation rule



  2. Click **Delete**.

----End

12.3 Configuring a DHCP Address Pool

This section describes how to configure a DHCP address pool.

Context

An interface that is assigned an IP address and enabled with DHCP can allocate IP addresses to the connected terminals. DHCP helps uniformly manage IP addresses for terminals.

NOTE

An interface can provide the DHCP service based on the global or interface address pool:

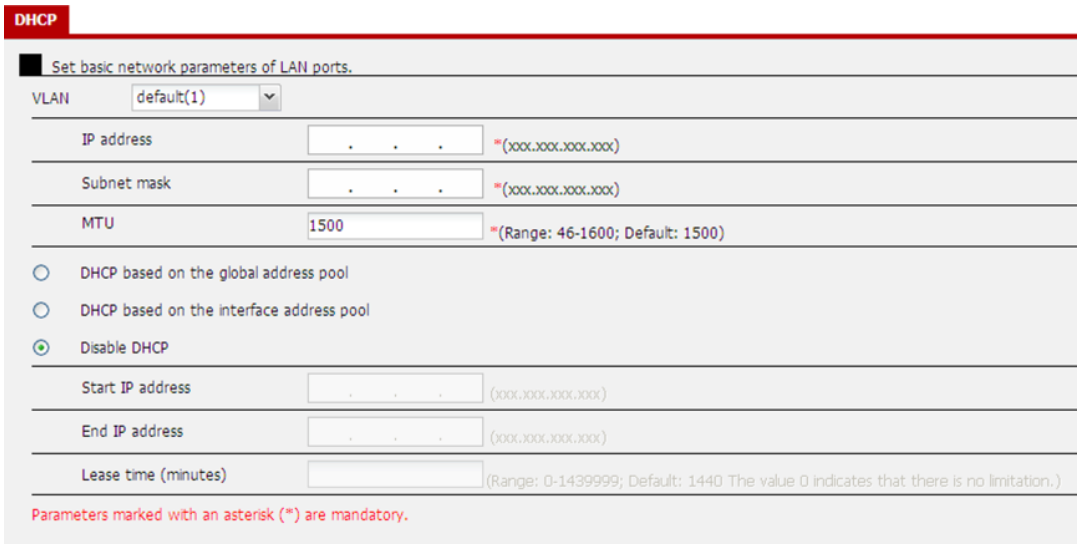
- DHCP service based on the global address pool: The DHCP server allocates IP addresses in the global address pool to DHCP clients. IP addresses in the global address pool and the IP address of the interface where the global address pool is configured can be on the same network segment or different network segments. If they are on different network segments, the interface can use a DHCP relay agent to allocate IP addresses to DHCP clients on different network segments.
- DHCP service based on the interface address pool: The DHCP server allocates IP addresses in the interface address pool to DHCP clients.

Procedure

- Enable the DHCP service based on the global address pool.
  1. Log in to the web network management system and choose **Basic Settings** > **Network** > **DHCP**. The **DHCP** page is displayed, as shown in **Figure 12-17**.

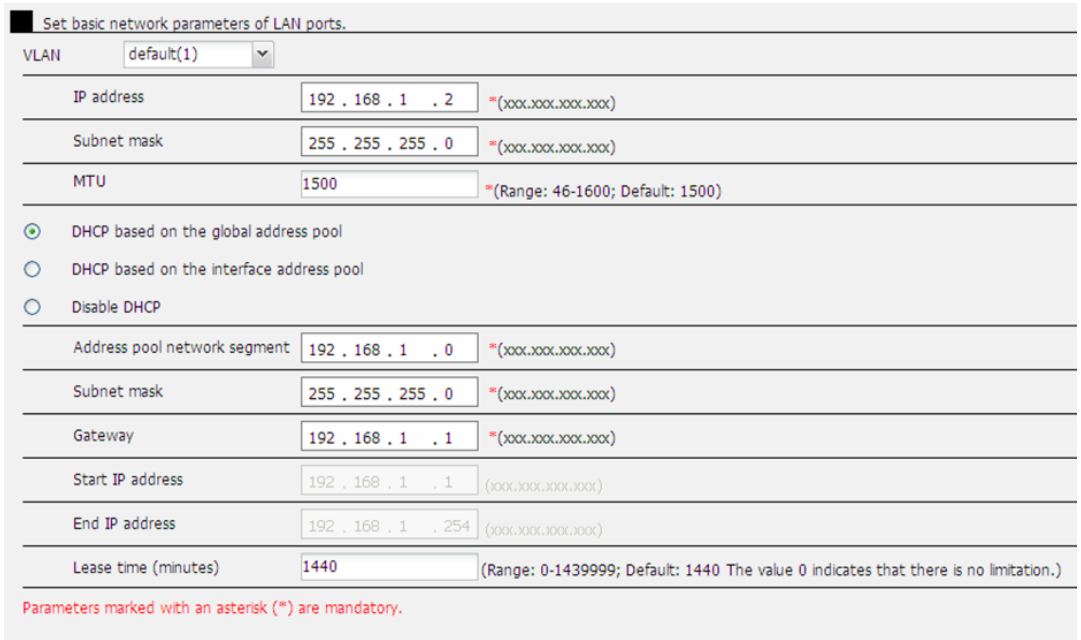
Copyright © Huawei Technologies Co., Ltd.

Figure 12-17 DHCP address pool page



2. Set the interface to be configured with the DHCP service, MTU, and IP address lease, enable the DHCP service based on the global address pool, and configure the global address pool.

Figure 12-18 Enabling the DHCP service based on the global address pool



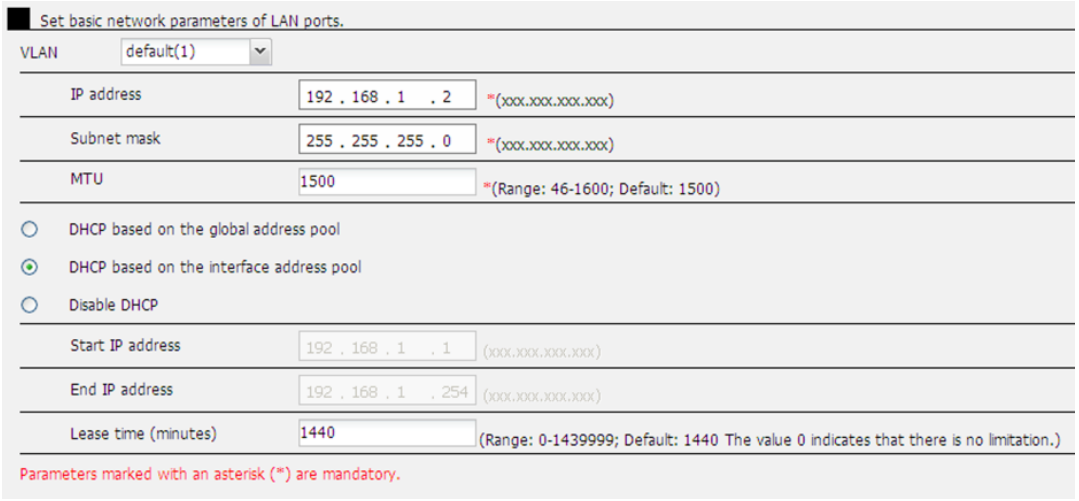
3. Click **OK**.

- Enable the DHCP service based on the interface address pool.
  1. Log in to the web network management system and choose **Basic Settings** > **Network** > **DHCP**. The **DHCP** page is displayed, as shown in **Figure 12-17**.

Copyright © Huawei Technologies Co., Ltd.

2. Set the interface to be configured with the DHCP service, MTU, and IP address lease, and enable the DHCP service based on the interface address pool.

Figure 12-19 Enabling the DHCP service based on the interface address pool

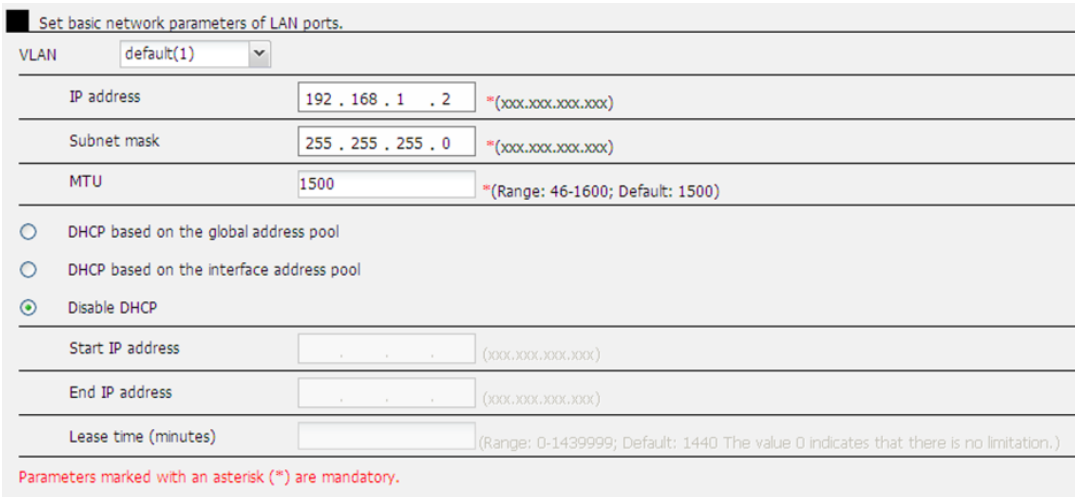


3. Click **OK** to enable the DHCP service.

- Disable the DHCP service.

1. Log in to the web network management system and choose **Basic Settings** > **Network** > **DHCP**. The **DHCP** page is displayed, as shown in **Figure 12-17**.
2. Select the interface where the DHCP service needs to be disabled.

Figure 12-20 Disabling the DHCP service



3. Click **OK** to disable the DHCP service.

----End

Copyright © Huawei Technologies Co., Ltd.

12.4 Configuring Static Routes

This section describes how to configure static routes.

Context

On an IPv4 network, configuring IPv4 static routes facilitate route management.

Procedure

Step 1 Choose **Basic Settings** > **Network** > **Route** to open the **Static Route** page, as shown in **Figure 12-21**.

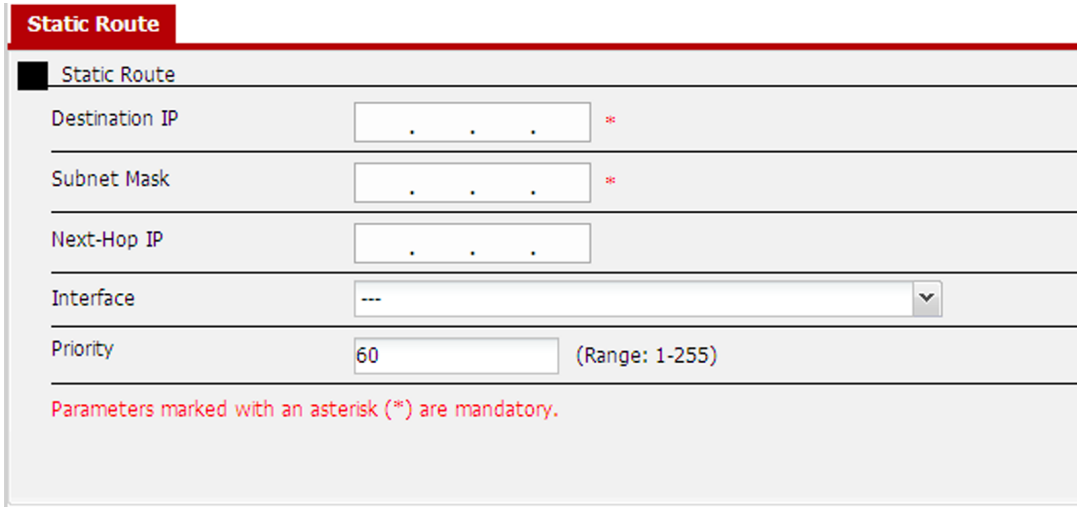
Figure 12-21 Static route list

Step 2 Configure a static route.

1. Create a static route.

   Click **New** on the page shown in **Figure 12-22**. The parameter setting page shown in **Figure 12-22** is displayed.

Figure 12-22 Setting static route parameters



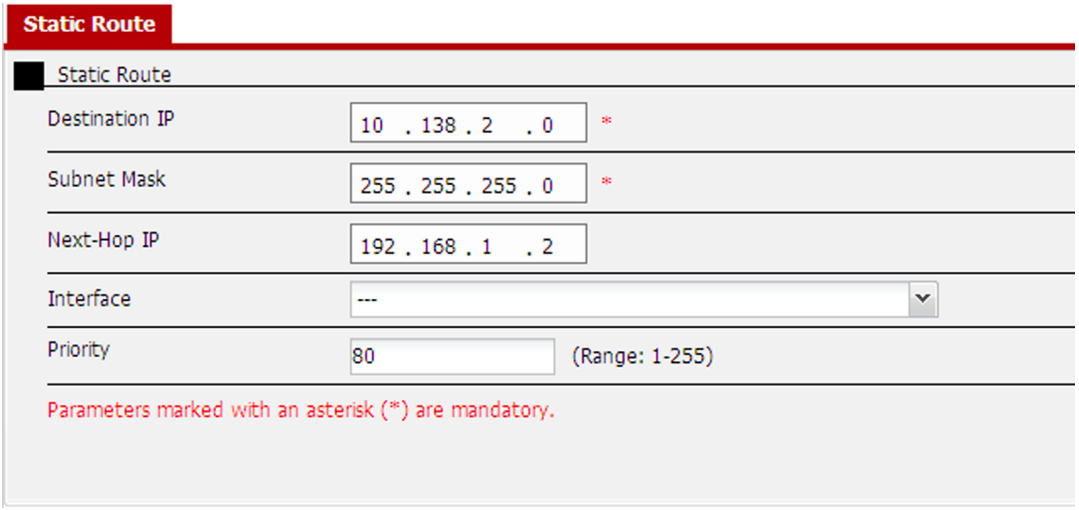
Copyright © Huawei Technologies Co., Ltd.

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.

As shown in **Figure 12-23**, set the destination network segment to 10.138.2.0/24, next hop address to 192.168.1.2, and route priority to 80. Click **OK**.

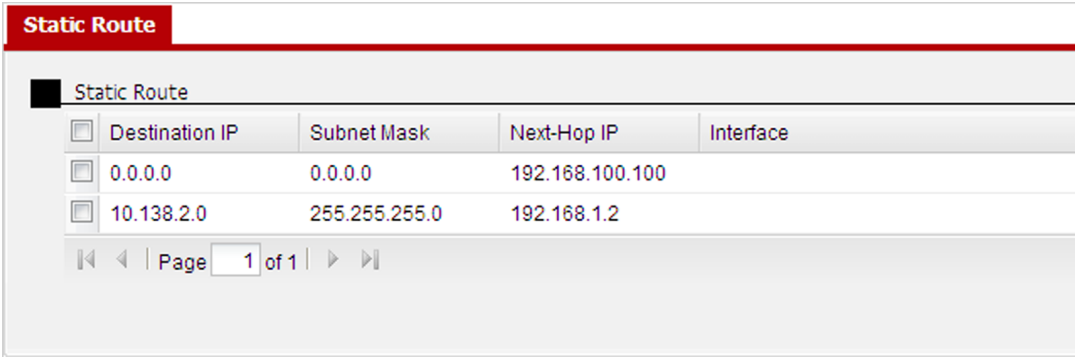
Figure 12-23 Setting static route parameters



2. Modify a static route.

   As shown in **Figure 12-24**, Click behind the route that you want to modify and modify its parameters.

Figure 12-24 Static route list

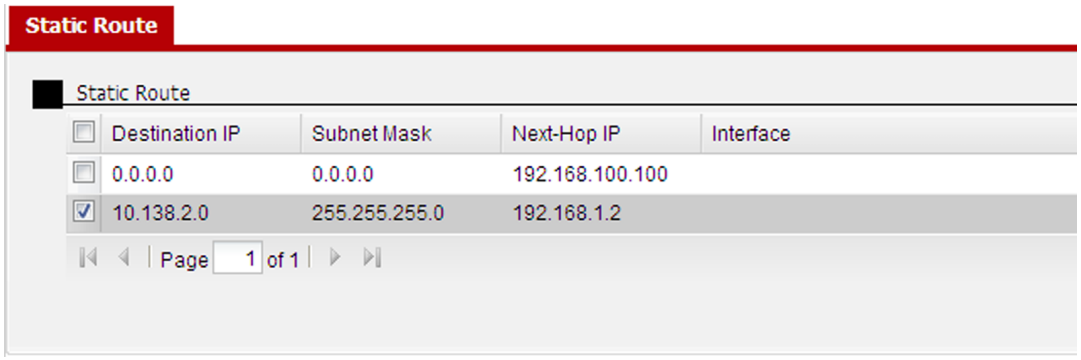


3. Delete static routes.

   As shown in **Figure 12-25**, select the static routes that you want to delete and click **Delete**. Alternatively, click behind the route that you want to delete.

Copyright © Huawei Technologies Co., Ltd.

Figure 12-25 Static route list



----End

Copyright © Huawei Technologies Co., Ltd.

13 Configuring Network Security

About This Chapter

This section describes how to configure network security.

13.1 Overview
This section describes the implementation and configuration roadmap of network security.

13.2 Configuring Basic Security Features
This section describes how to configure the basic security features, including firewall and MAC address filtering.

Copyright © Huawei Technologies Co., Ltd.

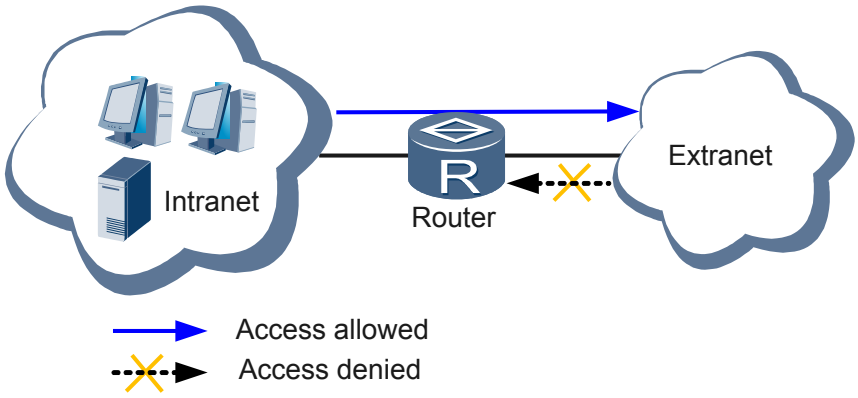
13.1 Overview

This section describes the implementation and configuration roadmap of network security.

- Firewall

  An attack defense system is the first line of defense that protects an internal network against attacks from external networks. The line is usually established by firewalls.

  Figure 13-1 Networking diagram of a firewall

  After the firewall function is enabled on the router, users on the internal network can access external networks, but users on external networks cannot access the internal network unless they are permitted to do so.

- MAC address filtering

  A MAC address filtering table needs to be configured on the firewall. The firewall permits or rejects access to the internal network from LAN-side users in the table.

  Configuration roadmap:

  - Configure the MAC address filtering table.
  - Select the filtering type.

- ARP attack defense

  ARP-oriented attacks include ARP spoofing attacks and ARP flood attacks.

  - ARP spoofing

    An attacker sends forged ARP packets to devices on a network. The devices then modify their ARP entries, causing forwarding failures.

  - ARP flood

    An attacker sends a large number of bogus ARP Request packets or gratuitous ARP packets to network devices. The network devices are busy with ARP processing for a long period and cannot process other services. When the ARP packet rate exceeds the limit and ARP entries overflows, the ARP entries of valid users cannot be buffered and packet forwarding is affected.

  You can configure the following features on the Web page to prevent ARP spoofing:

  - IP address and MAC address binding

    After the IP address and MAC address binding table is configured, if the device receives an ARP packet in which the IP and MAC addresses do not match the ARP entry, it does

Copyright © Huawei Technologies Co., Ltd.

not change the ARP entry. Instead, the device sends a unicast packet to the MAC address in the ARP entry to make a confirmation.

- Automatic learning

  Using this function, the device learns only the ARP Reply to the ARP Request sent by its own, but does not learn the ARP Reply to the ARP Request sent by other devices. When the received ARP Request does not match the ARP entry, the device sends an ARP Request to the computer. After the device receives an ARP Reply from the computer, it updates the ARP entry by adding the MAC address of the computer to the corresponding ARP entry.

- ARP broadcast interval

  After the AR router is configured to periodically send gratuitous ARP packets, the AR router can update the gateway MAC addresses in users' ARP entries.

Additionally, you can set the ARP flooding thresholds to control the rate of ARP packets sent to the main control board. This efficiently prevents ARP flooding attacks.

13.2 Configuring Basic Security Features

This section describes how to configure the basic security features, including firewall and MAC address filtering.

13.2.1 Configuring the Firewall

This section describes how to configure the firewall function.

Context

Preventing external data from being transmitted to an enterprise network can defend against most attacks. After the firewall is configured on the network, internal users can access external network, but external users cannot access the internal network unless they are permitted to do so.

NOTE

After a VLANIF interface is created, it is automatically added to the trusted zone. After a WAN interface is created, it is automatically added to the untrusted zone. The firewall is deployed in the interzone, which is between the trusted zone and untrusted zone.

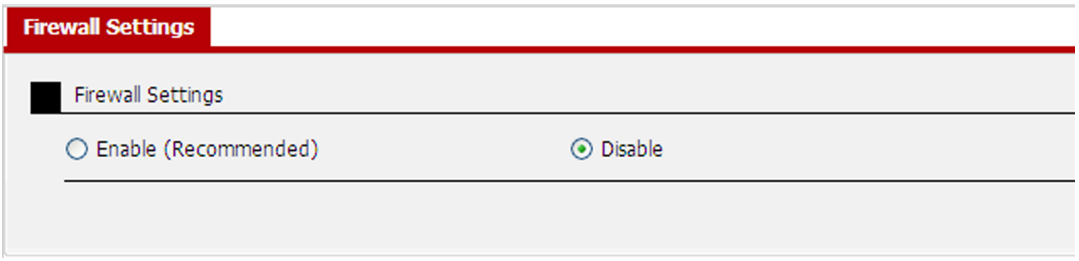
After the firewall function is enabled on the router, users in the trusted zone can access the untrusted zone, but users in the untrusted zone cannot access the trusted zone unless they are permitted to do so.

Procedure

Step 1 Choose **Security** > **Basic Settings** > **Firewall** to open the **Firewall Settings** page, as shown in **Figure 13-2**.

Copyright © Huawei Technologies Co., Ltd.

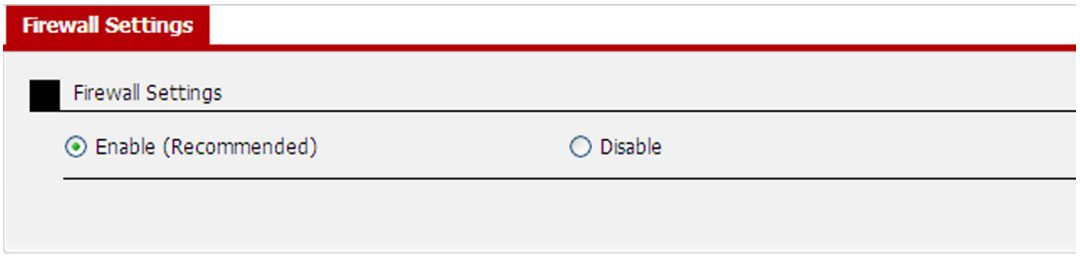
Figure 13-2 Configuring the firewall



Step 2 Configure the firewall function.

As shown in **Figure 13-3**, select **Enable** or **Disable** and click **OK**.

Figure 13-3 Enabling the firewall



----End

13.2.2 Configuring MAC Address Filtering

This section describes how to configure MAC address filtering.

Context

To limit users' network access rights, configure MAC address filtering.

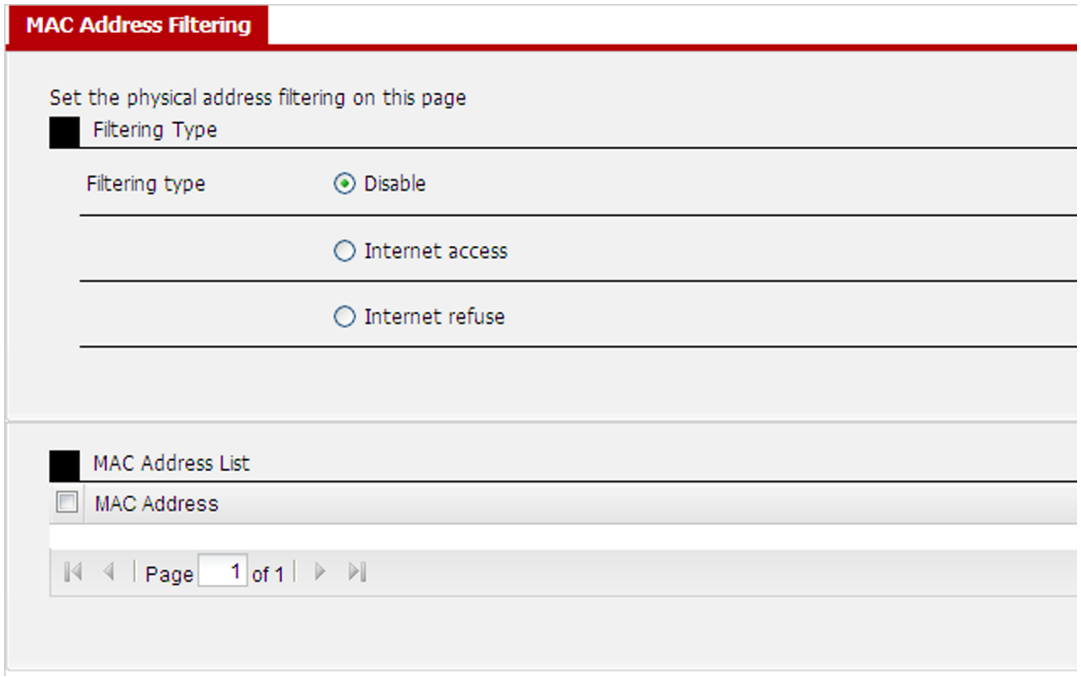
To configure MAC address filtering, add users' MAC addresses to the MAC address filtering table and specify whether to permit or reject the users listed in the table.

Procedure

Step 1 Choose **Security** > **Basic Settings** > **MAC Address Filtering** to open the **MAC Address Filtering** page, as shown in **Figure 13-4**.

Copyright © Huawei Technologies Co., Ltd.

Figure 13-4 MAC address filtering

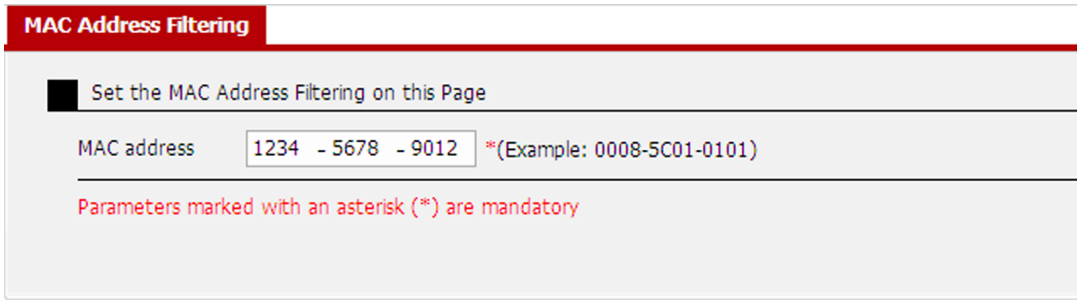


Step 2 Add or delete MAC addresses.

1. Add MAC addresses to the table.

   As shown in **Figure 13-4**, click **Create**. The page shown in **Figure 13-5** is displayed.

Figure 13-5 Adding MAC addresses



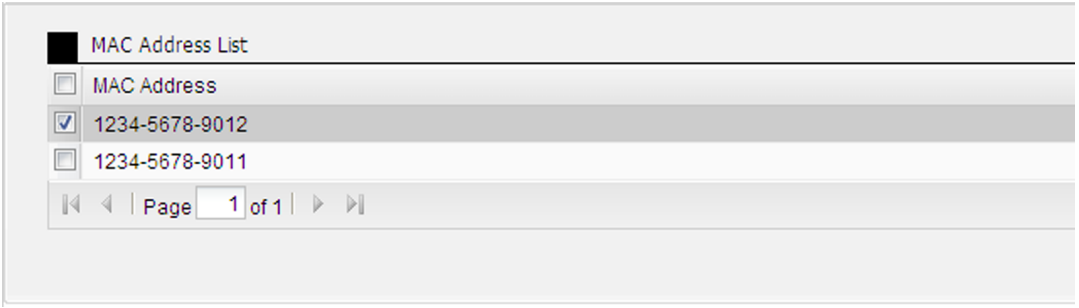
   Enter a MAC address and click **OK**.

2. (Optional) Delete MAC addresses from the table.

   As shown in **Figure 13-6**, to delete MAC address 1234-5678-9012, select it and click **Delete**. When the **Are you sure to delete it?** dialog box is displayed, click **OK**.

Copyright © Huawei Technologies Co., Ltd.

Figure 13-6 Deleting MAC addresses



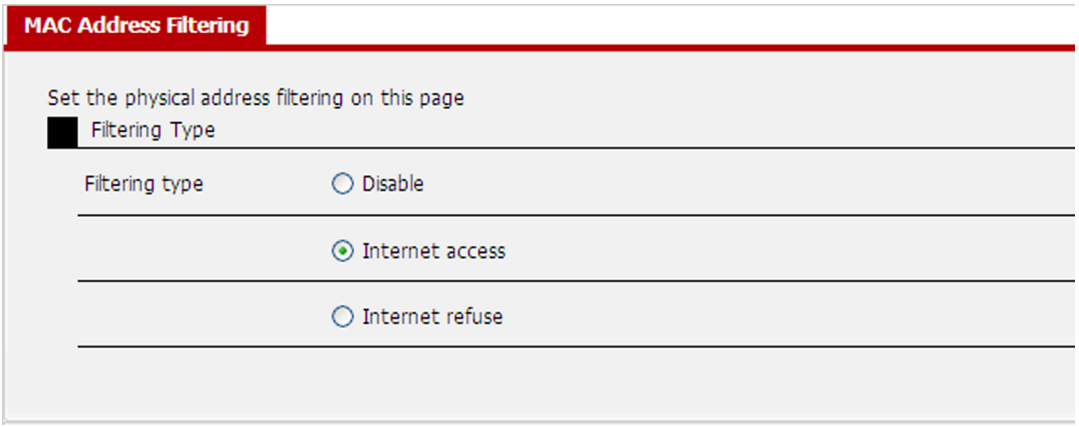
NOTE

To delete all MAC addresses from the table, select **MAC Address List** and click **Delete**.

Step 3 Select the filtering type.

As shown in **Figure 13-7**, set the filtering type to **Disable**, **Internet access**, or **Internet refuse**, and click **OK**.

Figure 13-7 Setting the filtering type



----End

13.2.3 Configuring Protection Against ARP Attacks

This section describes how to configure protection against ARP attacks.

Context

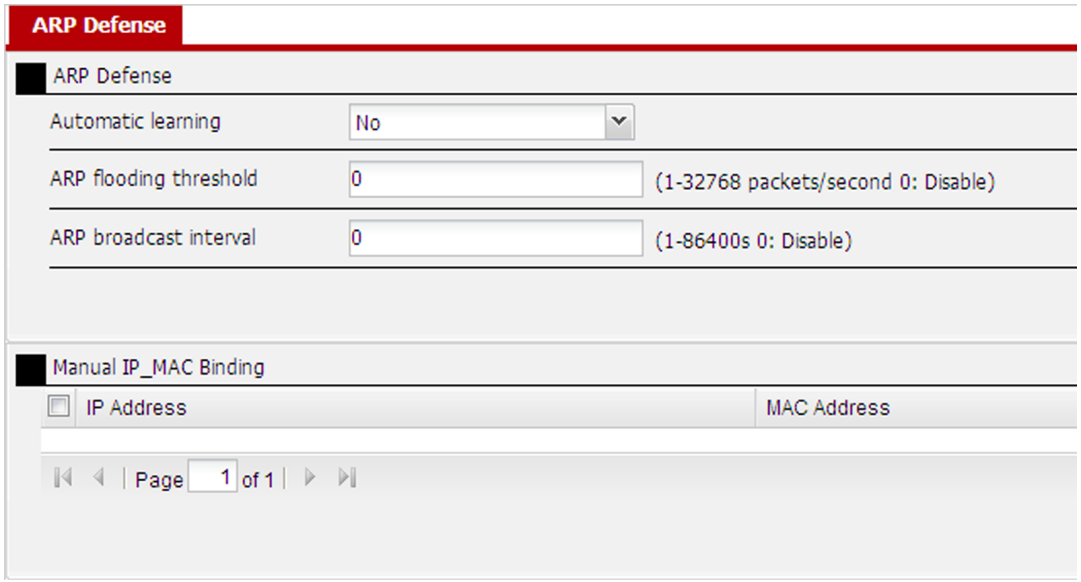
ARP is easy to use but has no security mechanisms. Attackers often use ARP to attack network devices. ARP attacks and viruses have posed a threat to LAN security. To ensure security, AR routers provide various technologies to detect and defend against ARP attacks.

Procedure

Step 1 Choose **Security** > **Basic Settings** > **ARP Defense** to open the **ARP Defense** page, as shown in **Figure 13-8**.

Copyright © Huawei Technologies Co., Ltd.

Figure 13-8 Configuring protection against ARP attacks

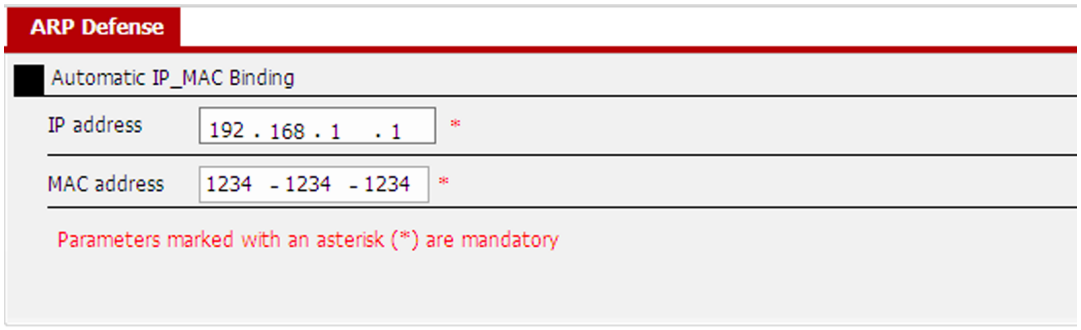


Step 2 Configure an ARP table.

1. Add entries to an ARP table.

   Click **Create** on the **ARP Defense** page. The page shown in **Figure 13-9** is displayed.

Figure 13-9 Configuring IP-to-MAC mapping



   Enter the IP and MAC addresses, and click **OK**.

2. (Optional) Delete entries from an ARP table.

   To delete an entry, select it and click **Delete**.

   NOTE

   To delete all entries from the ARP table, select **IP Address** and click **Delete**.

NOTE

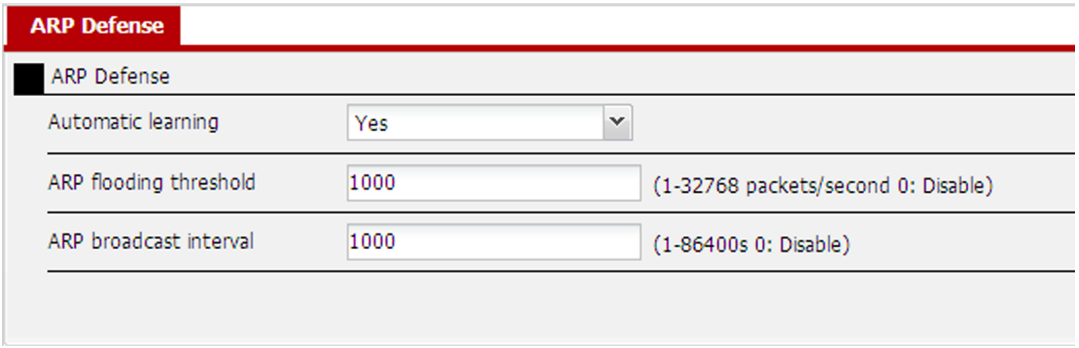
By default, the binding table check function is disabled. After the IP address and MAC address binding table (static ARP table) is configured, enabling any ARP security function (such as automatic learning) will cause the binding table check function to be invalid.

Copyright © Huawei Technologies Co., Ltd.

Step 3 Configure protection against ARP attacks.

On the page shown in **Figure 13-10**, configure protection against ARP attacks.

Figure 13-10 Configuring protection against ARP attacks



After completing the configuration, click **OK** to make the settings take effect.

----End

Copyright © Huawei Technologies Co., Ltd.

14 Configuring Network Bandwidth Guarantee

About This Chapter

This section describes how to configure network bandwidth guarantee.

14.1 Overview
Network bandwidth guarantee includes user bandwidth limiting, advanced bandwidth limiting, advanced bandwidth guarantee, and session count limiting.

14.2 Configuring User Bandwidth Limiting
This section describes how to limit the upload and download rates based on users' IP addresses.

14.3 Configuring Advanced Bandwidth Limiting
This section describes how to configure advanced bandwidth limiting.

14.4 Configuring Advanced Bandwidth Guarantee
This section describes how to configure advanced bandwidth guarantee.

14.5 Configuring Session Count Limiting
Too many TCP and UDP sessions occupy resources, so you need to limit the number of sessions set up by users.

Copyright © Huawei Technologies Co., Ltd.

14.1 Overview

Network bandwidth guarantee includes user bandwidth limiting, advanced bandwidth limiting, advanced bandwidth guarantee, and session count limiting.

The web system supports the following bandwidth guarantee functions:

- User bandwidth limiting

  Limits the upload and download rates based on users' IP addresses.

- Advanced bandwidth limiting

  Limits traffic rate at the IP layer, which is similar to user bandwidth limiting. Compared with user bandwidth limiting, advanced bandwidth limiting:

  - Classifies packets based on the priority, inbound interface, protocol type, and port number, and can have a validity period.
  - Re-marks DSCP fields or 802.1p priorities of the packets matching certain conditions.

- Advanced bandwidth guarantee

  The following functions are available:

  - Interface bandwidth limiting: Uses a token bucket to limit the rate of all packets sent by an interface. User bandwidth limiting and advanced bandwidth limiting are implemented at the IP layer. They can limit packet rates based on packet types. However, they are invalid for the packets that do not pass the IP layer. To limit the rate of all packets passing an interface, interface bandwidth limiting is recommended because it is easy to implement.
  - Application bandwidth limiting: Uses the Class-based Queuing (CBQ) technology to place packets into different queues based on user-defined conditions when congestion occurs, and provides differentiated services to the packets leaving the queues.

  Advanced bandwidth guarantee is only valid for the packets sent by an interface.

- Session count limiting

  Too many TCP and UDP sessions on a network occupy resources and congest the network, and other service traffic may not be forwarded. This function limits the number of TCP and UDP sessions set up by users.

14.2 Configuring User Bandwidth Limiting

This section describes how to limit the upload and download rates based on users' IP addresses.

Context

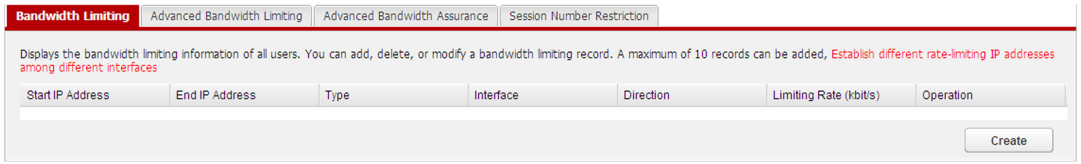
Total bandwidth on an enterprise network is limited, so you need to limit the upload and download rates of some users.

Procedure

Step 1 Choose **Basic Settings** > **QoS** > **Bandwidth Limiting** to open the **Bandwidth Limiting** page, as shown in **Figure 14-1**.

Copyright © Huawei Technologies Co., Ltd.

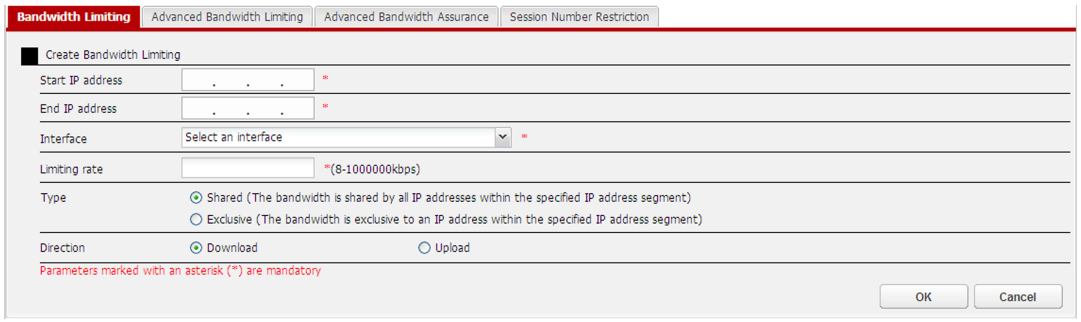
Figure 14-1 User bandwidth limiting



Step 2 Configure a user bandwidth limit.

Click **Create** on the page shown in **Figure 14-1**. The parameter setting page shown in **Figure 14-2** is displayed. Set the parameters and click **OK**.

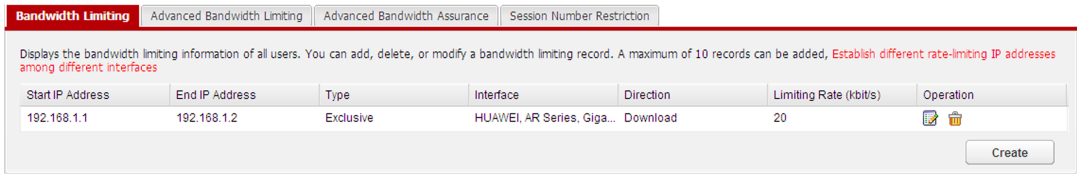
Figure 14-2 Configuring a user bandwidth limit



Step 3 (Optional) Modify and delete user bandwidth limits.

- As shown in **Figure 14-3**, click behind the record that you want to modify, and modify the parameters.
- As shown in **Figure 14-3**, click behind the record that you want to delete.

Figure 14-3 User bandwidth limiting information



----End

14.3 Configuring Advanced Bandwidth Limiting

This section describes how to configure advanced bandwidth limiting.

Context

Advanced bandwidth limiting classifies packets based on priority, inbound interface, protocol type, and port number, and provides differentiated services to the packets matching different classification rules.

For example, from 09:00 to 18:00 on Monday to Friday, users on the IP address segment 192.168.1.1/24-192.168.1.254/24 are allowed to access the Internet through Eth2/0/0. The total upload rate of these users is 2048 kbit/s (2 Mbit/s), and the DSCP field of the uploaded packets is re-marked 12.

Copyright © Huawei Technologies Co., Ltd.

Procedure

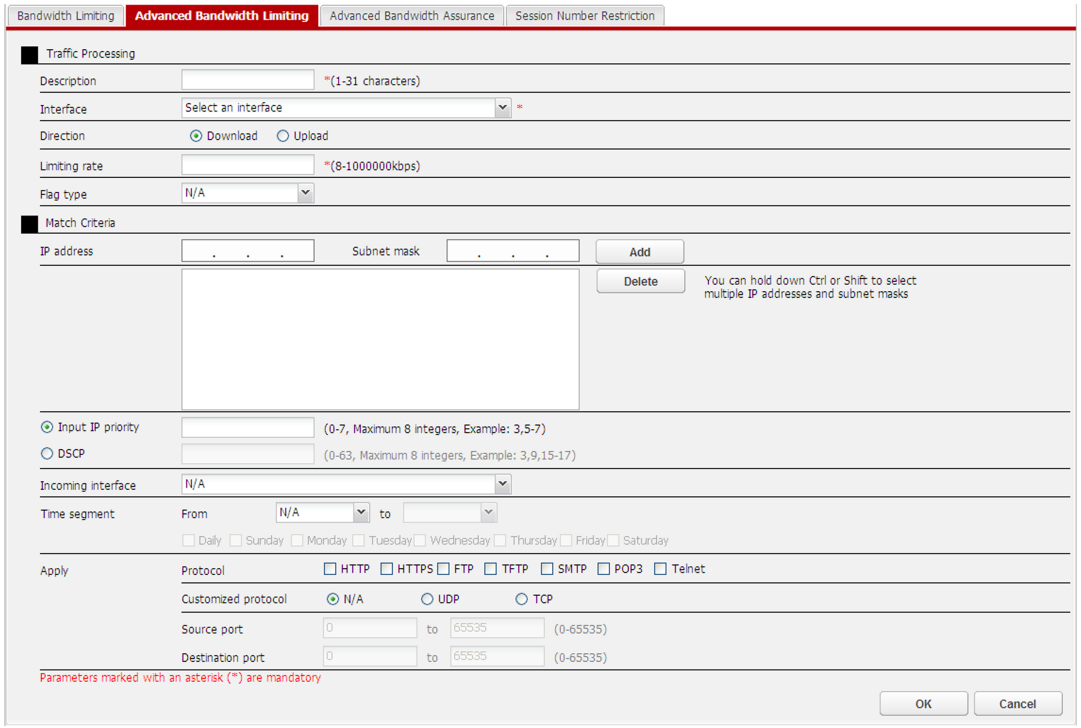
Step 1 Choose **Basic Settings** > **QoS** > **Advanced Bandwidth Limiting** to open the **Advanced Bandwidth Limiting** page, as shown in **Figure 14-4**.

Figure 14-4 Advanced bandwidth limiting

Step 2 Configure an advanced bandwidth limit.

Click **Create** on the page shown in **Figure 14-4**. The parameter setting page shown in **Figure 14-5** is displayed. Set the parameters, click **Add** to add IP addresses, and click **OK**.

Figure 14-5 Configuring an advanced bandwidth limit



Step 3 (Optional) Modify and delete advanced bandwidth limits.

- As shown in **Figure 14-6**, click behind the record that you want to modify, and modify the parameters.
- As shown in **Figure 14-6**, click behind the record that you want to delete.

Copyright © Huawei Technologies Co., Ltd.

Figure 14-6 Advanced bandwidth limiting information

----End

14.4 Configuring Advanced Bandwidth Guarantee

This section describes how to configure advanced bandwidth guarantee.

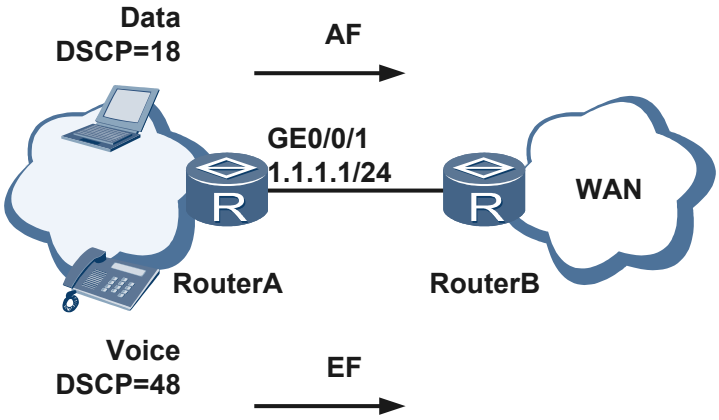
Context

Advanced bandwidth guarantee includes:

- Interface bandwidth limiting: limits the rate of all packets passing an interface.
- Application bandwidth limiting: uses CBQ to classify packets based on the IP precedence or DSCP field, inbound interface, or 5-tuple (protocol type, source IP address and mask, destination IP address and mask, source port range, and destination port range), and places packets into different queues:
  - Expedited Forwarding (EF) queues: used for delay-sensitive services.
  - Assured Forwarding (AF) queues: used for key data services that require assured bandwidth.

As shown in **Figure 14-7**, the enterprise network connects to the WAN through GE0/0/1 on Router A. The average rate on GE0/0/1 is 2048 kbit/s (2 Mbit/s). The voice packets (with DSCP field 48) of the enterprise are placed into the EF queue, and the maximum bandwidth is 512 kbit/s. The data packets (with the DSCP field 18) of the enterprise are placed into the AF queue, and the minimum bandwidth is 1024 kbit/s.

Figure 14-7 Advanced bandwidth guarantee

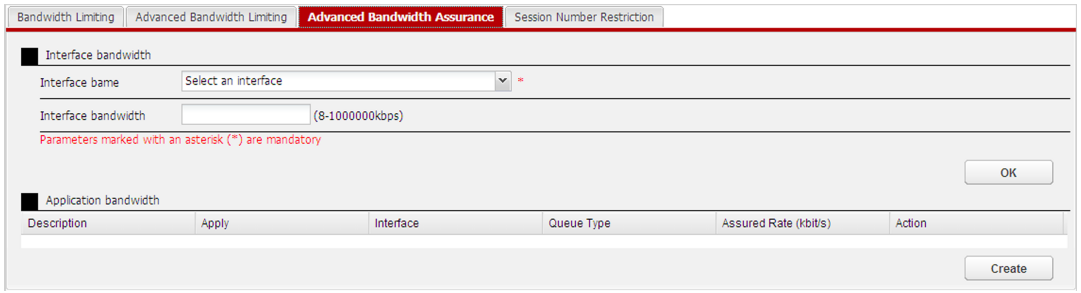


Procedure

Step 1 Choose **Basic Settings** > **QoS** > **Advanced Bandwidth Assurance** to open the **Advanced Bandwidth Assurance** page, as shown in **Figure 14-8**.

Copyright © Huawei Technologies Co., Ltd.

Figure 14-8 Advanced bandwidth guarantee

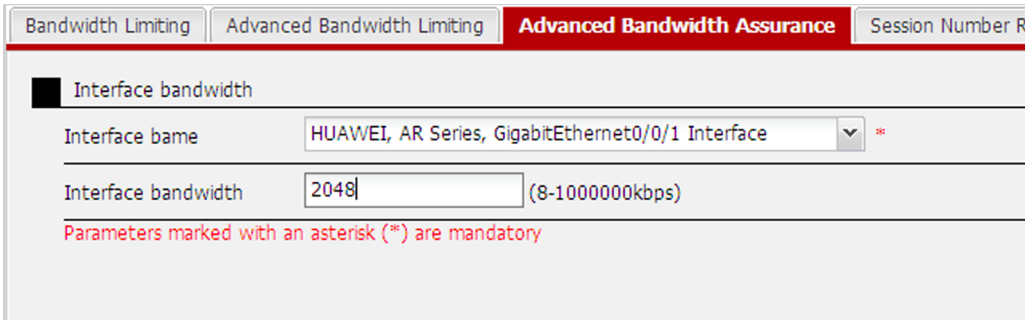


Step 2 Configure advanced bandwidth guarantee.

1. Configure interface bandwidth limiting.

   As shown in **Figure 14-9**, select an interface and set the bandwidth limiting, and click **OK**.

   Figure 14-9 Configuring interface bandwidth limiting

2. Configure application bandwidth limiting.

   Click **Create** on the page shown in **Figure 14-8**. Set the parameters and click **OK**.

   - Configure a bandwidth limit for voice packets according to **Figure 14-10**.
   - Configure a bandwidth limit for data packets according to **Figure 14-11**.

Copyright © Huawei Technologies Co., Ltd.

Figure 14-10 Configuring a bandwidth limit for voice packets

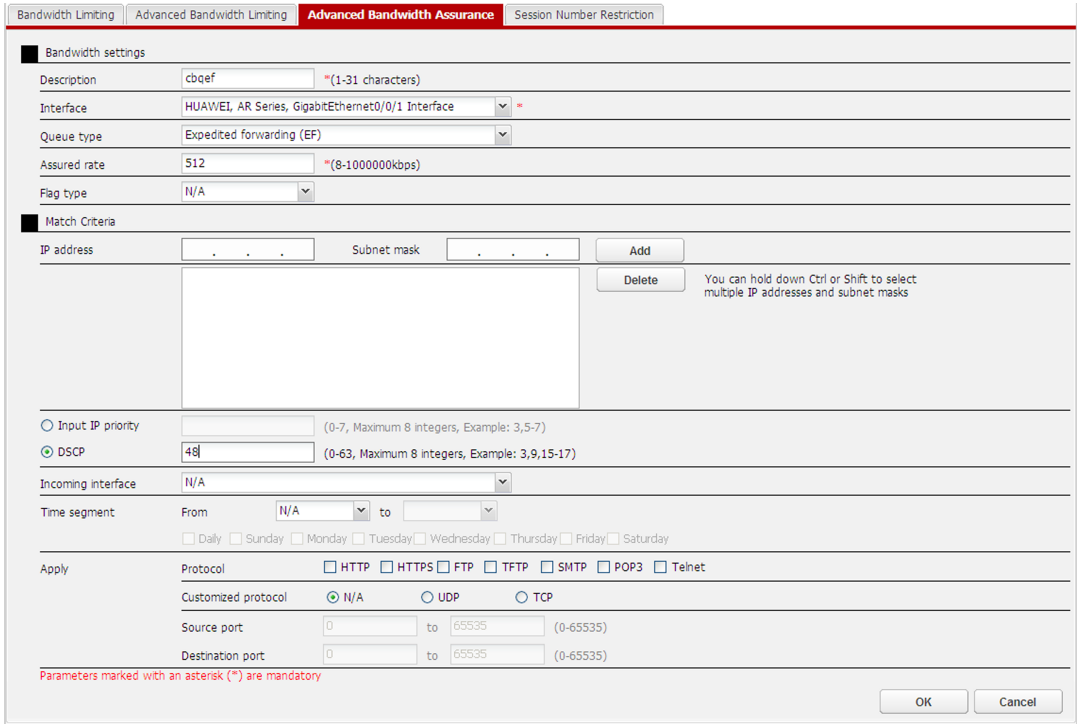
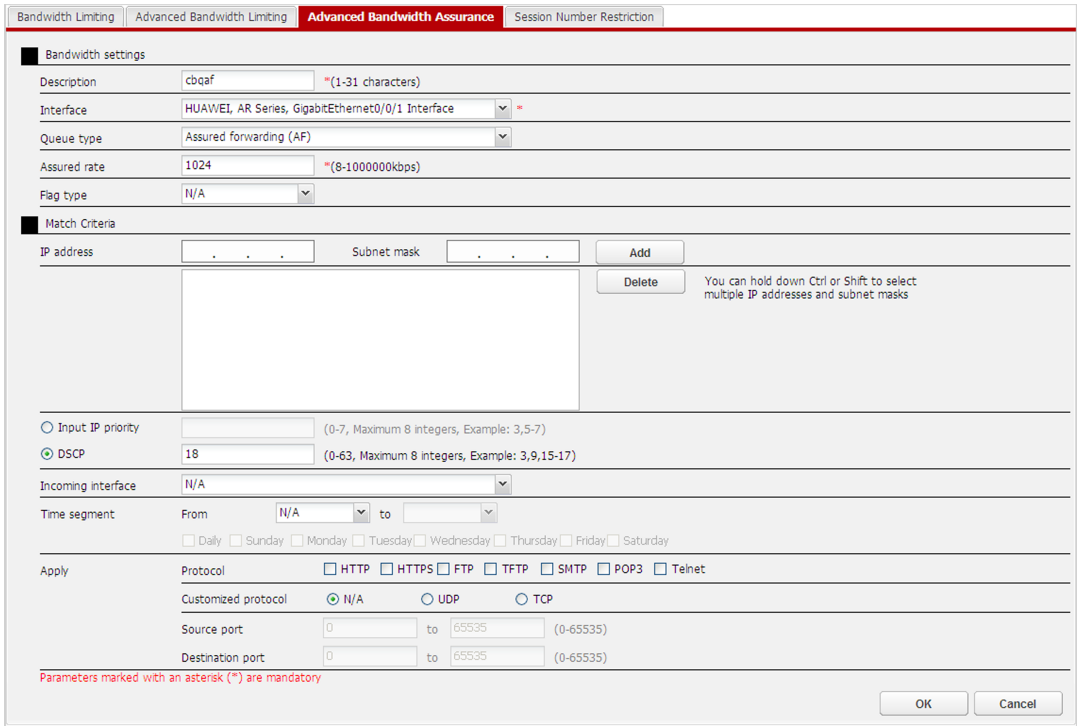


Figure 14-11 Configuring a bandwidth limit for data packets



Step 3 (Optional) Modify and delete advanced bandwidth guarantee records.

1. Modify and delete an interface bandwidth limit.

   As shown in **Figure 14-9**, select an interface and set the bandwidth limit, and click **OK**.

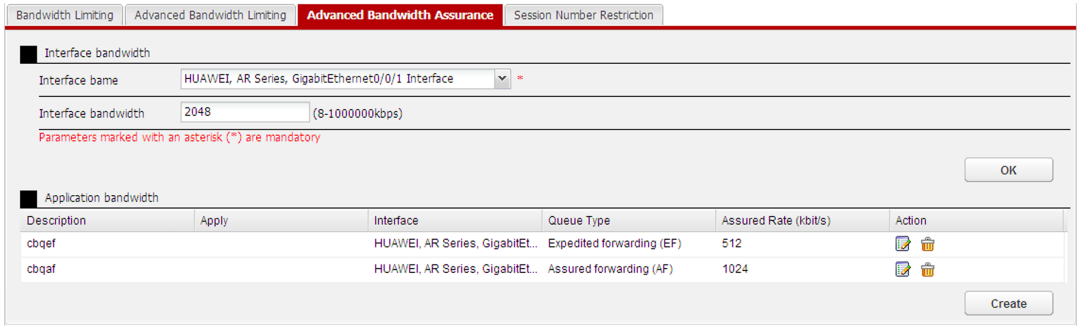
Copyright © Huawei Technologies Co., Ltd.

NOTE

To cancel bandwidth limiting on the interface, leave the **Interface Bandwidth** text box blank and click **OK**.

2. Modify and delete application bandwidth limits.
   - As shown in **Figure 14-12**, click behind the record that you want to modify, and modify the parameters.
   - As shown in **Figure 14-12**, click behind the record that you want to delete.

Figure 14-12 Advanced bandwidth guarantee information



----End

14.5 Configuring Session Count Limiting

Too many TCP and UDP sessions occupy resources, so you need to limit the number of sessions set up by users.

Context

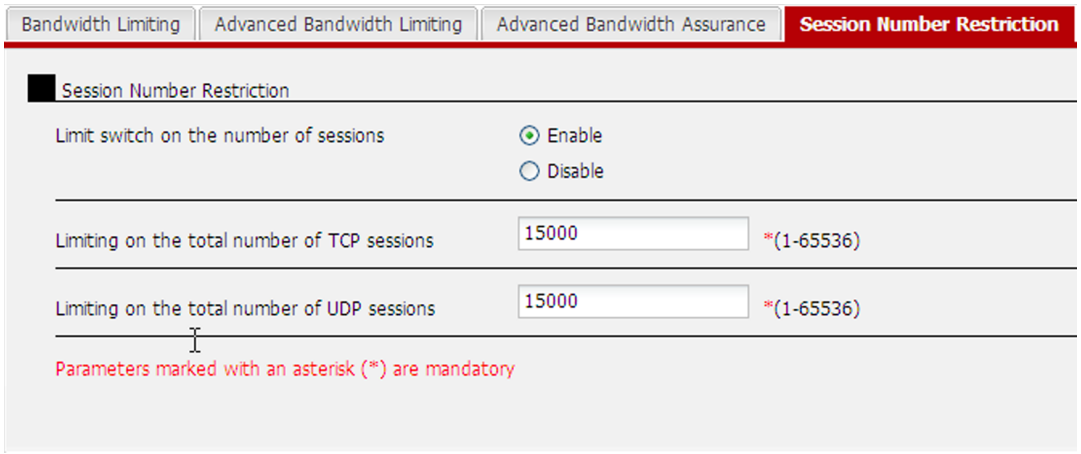
After the session count limiting function is enabled, the router starts to count the TCP and UDP sessions. When the number of sessions exceeds the threshold, the router rejects new sessions until the number of sessions falls below the threshold.

Procedure

Step 1 Choose **Basic Settings** > **QoS** > **Session Number Restriction** to open the page shown in **Figure 14-13**.

Copyright © Huawei Technologies Co., Ltd.

Figure 14-13 Configuring session count limiting



After completing the configuration, click **OK** to make the settings take effect.

----End

Copyright © Huawei Technologies Co., Ltd.

15 Configuring a VPN

About This Chapter

This section describes how to configure a VPN.

15.1 Overview
VPNs transmit private network data over a public network.

15.2 Configuring an L2TP VPN
This section describes how to configure an L2TP VPN.

15.3 Configuring IPSec VPN
This section describes how to configure IPSec VPN.

15.4 Configuring SSL VPN
This section describes how to configure SSL VPN.

Copyright © Huawei Technologies Co., Ltd.

15.1 Overview

VPNs transmit private network data over a public network.

The web system supports the following VPN functions:

- L2TP

  The Layer 2 Tunneling Protocol (L2TP) allows enterprise users, small-scale ISPs, and mobile office users to access a VPN over a public network.

  L2TP uses a dedicated encryption protocol to establish secure VPNs for enterprises over a public network. Branches and traveling staff remotely access the headquarters over tunnels on a public network. Users on the public network cannot access enterprise resources

- IPSec

  On IP networks, most data is transmitted in plain text, causing security risks. For example, bank accounts and passwords may be intercepted, and user information may be forged. IPSec can protect transmitted IP packets to reduce the risk of information leak.

  IPSec has the following advantages:

  - Reduces the risk of information leak and interception, ensuring secure service transmission.
  - Eliminates the need for other security features such as Transport Layer Security (TLS) at the application layer, reducing the service deployment cost.

- SSL VPN

  An SSL VPN gateway is located at an intranet's edge, and works with the browsers installed on remote terminals or with clients downloaded using browsers to protect user data on the Internet. Additionally, the SSL VPN gateway functions as the proxy to allow users to access internal servers.

  Employees, customers, and partners can use various types of terminals to access an enterprise intranet anytime and anywhere. Using an SSL VPN gateway, the enterprise can strictly control access to the intranet based on user privileges.

15.2 Configuring an L2TP VPN

This section describes how to configure an L2TP VPN.

15.2.1 Configuring an L2TP Client

This section describes how to configure an L2TP client.

Context

An L2TP access concentrator (LAC) is an L2TP client that initiates an L2TP tunnel with an L2TP network server (LNS).

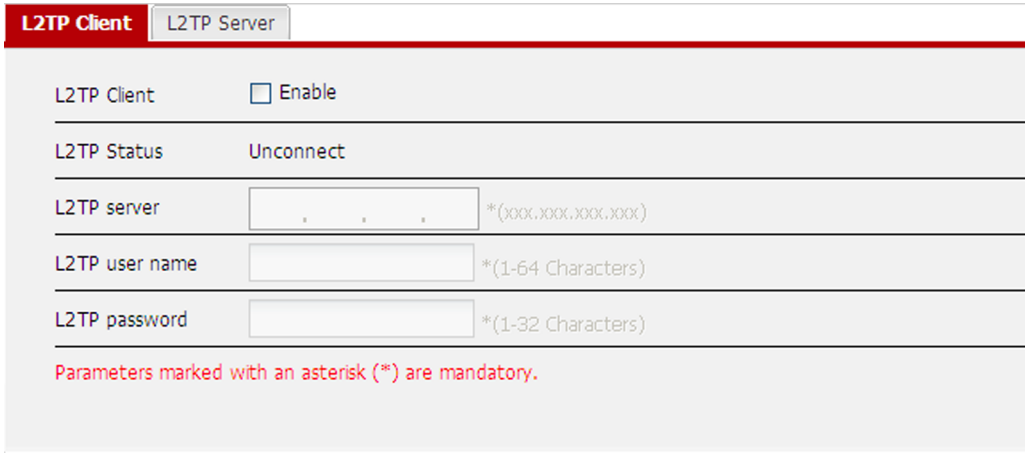
An LAC initiates an L2TP tunnel with an LNS only for authorized access users. The LAC determines whether a user is an authorized access user according to user information. If the user is an authorized user, the LAC uses the IP address of an LNS's WAN interface to initiate a connection with the LNS.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Choose **Basic Settings** > **VPN** > **L2TP VPN** > **L2TP Client** to open the **L2TP Client** page, as shown in **Figure 15-1**.

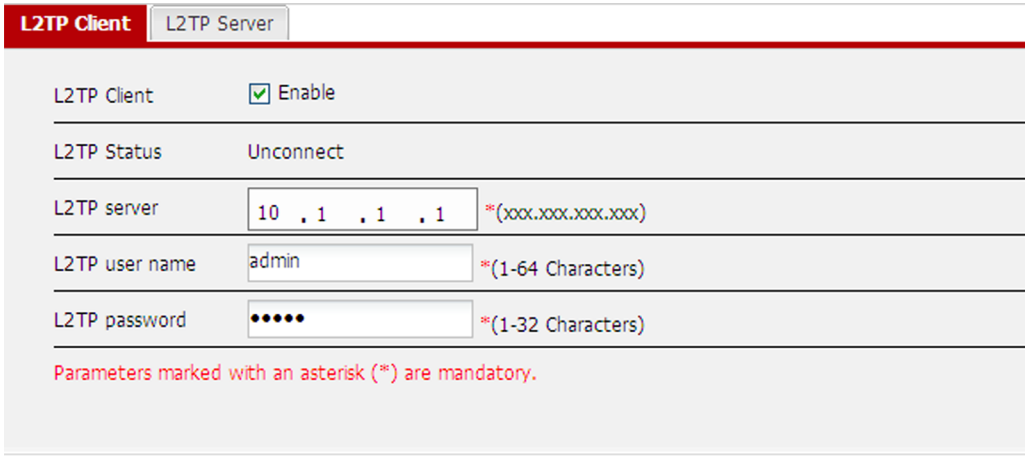
Figure 15-1 Configuring an L2TP client



Step 2 Configure an L2TP client.

Select **Enable** on the page shown in **Figure 15-2**, set L2TP client parameters, and click **OK**.

Figure 15-2 Setting L2TP client parameters



NOTE

After an L2TP connection is established, refresh the **L2TP Client** page. If the L2TP status displays **Connected**, the L2TP connection has been established.

----End

15.2.2 Configuring an L2TP Server

This section describes how to configure an L2TP server.

Copyright © Huawei Technologies Co., Ltd.

Context

An L2TP network server (LNS) accepts and processes L2TP tunnel requests. Users can access resources on a VPN after they are authenticated by the LNS.

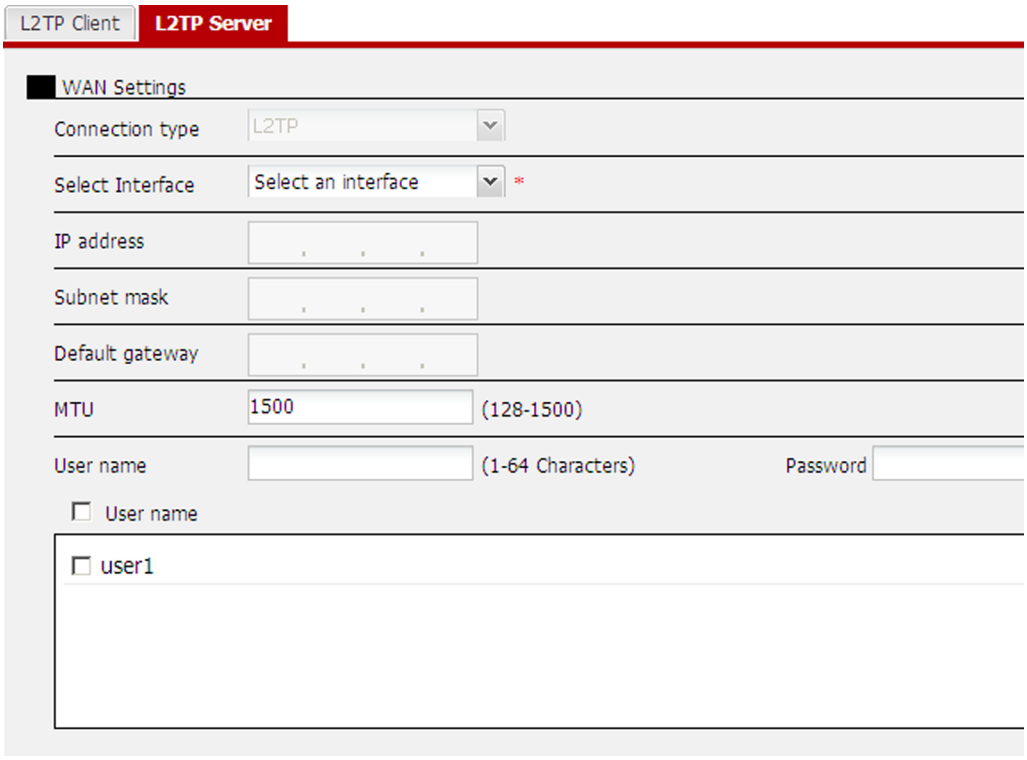
An LNS and an L2TP access concentrator (LAC) are two endpoints of an L2TP tunnel. The LAC initiates an L2TP tunnel, while the LNS accepts L2TP tunnel requests.

An LNS, residing on the border between a VPN and a public network, is usually a gateway of an enterprise's headquarters. The gateway provides the network access and LNS function.

Procedure

Step 1 Choose **Basic Settings** > **VPN** > **L2TP VPN** > **L2TP Server** to open the **L2TP Server** page, as shown in **Figure 15-3**.

Figure 15-3 Configuring an L2TP server



Step 2 Configure an L2TP server.

Set L2TP server parameters on the page shown in **Figure 15-5** and click **OK**.

1. Configure a WAN interface.

   After a WAN interface is selected, the interface IP address, subnet mask, and default gateway address are displayed. You can set the MTU of the VT interface.

2. Configure a user.

   - To add a user, enter a user name and password, click **Add** and select the user from the user list, as shown in **Figure 15-5**.
   - To configure an existing user, select the user from the user list.

Copyright © Huawei Technologies Co., Ltd.

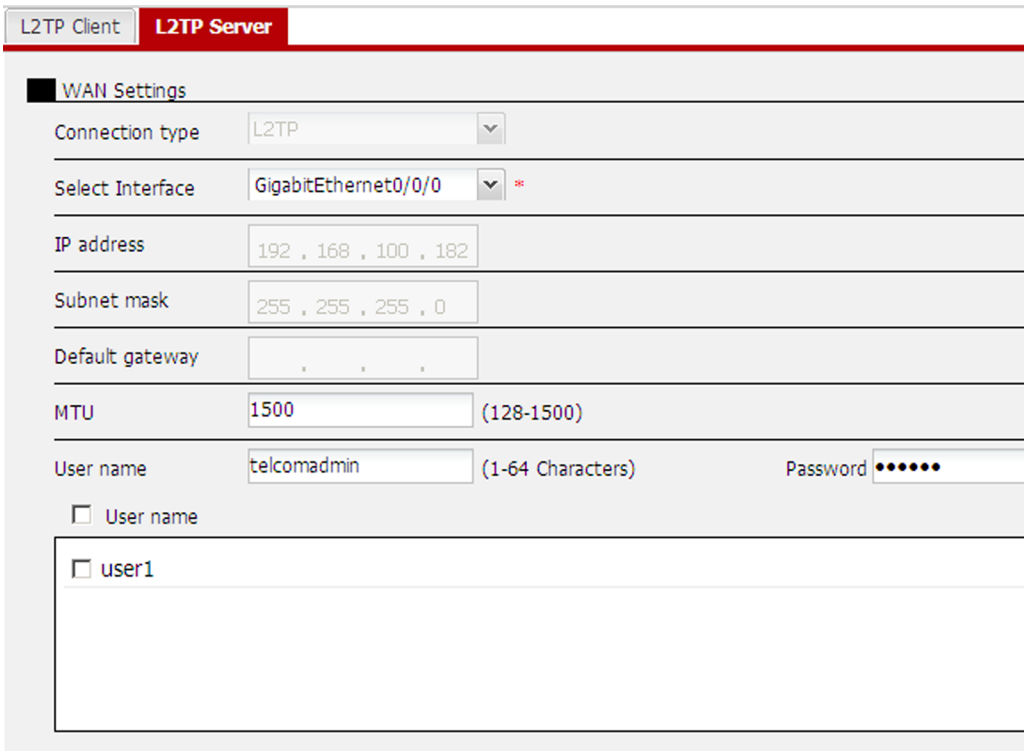
NOTE

An L2TP tunnel can be established only when the L2TP client and server use the same non-empty user name and password.

- To delete a user, select the user from the user list and click **Delete**.

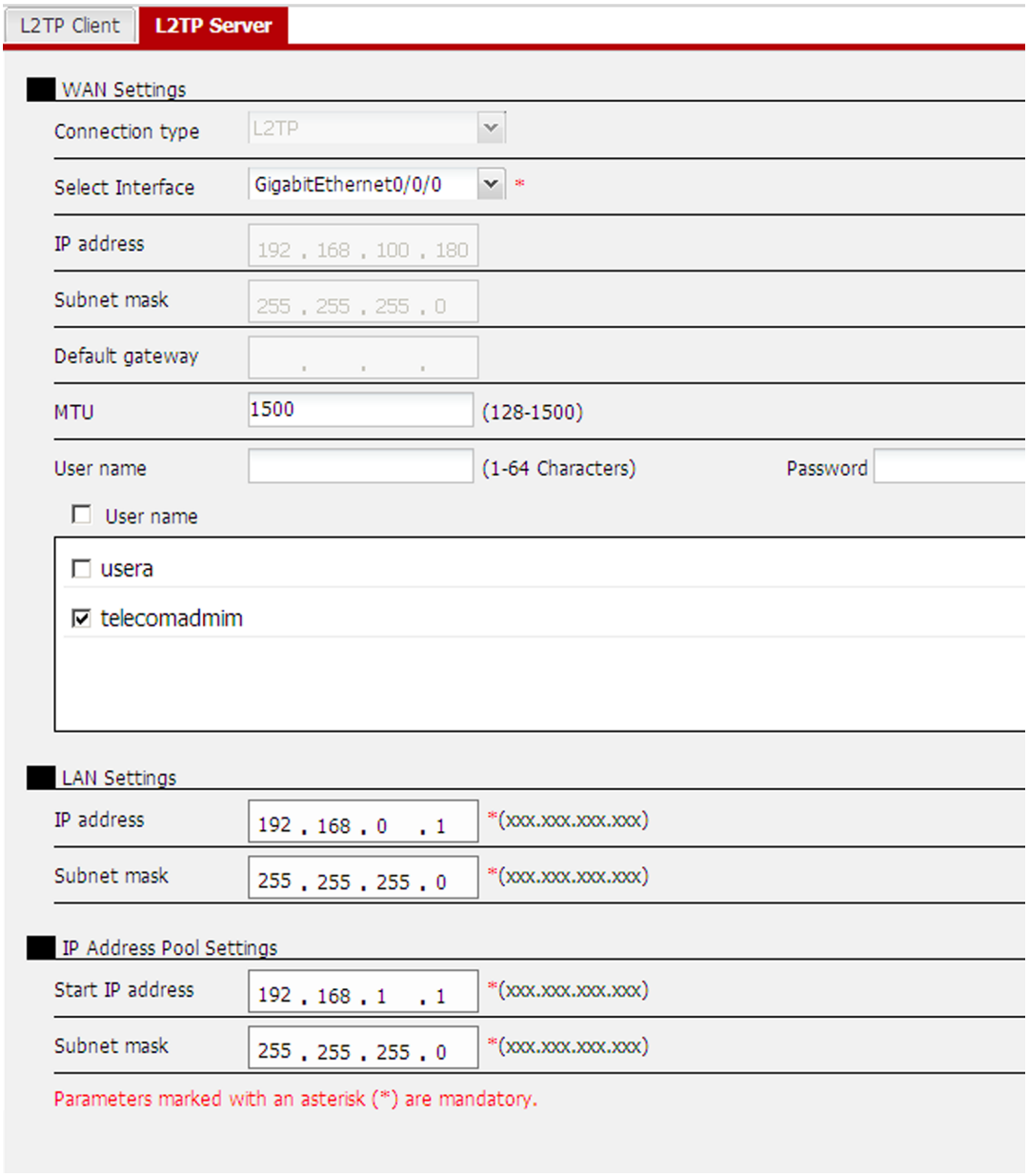
3. Configure the LAN: configure a private IP address and subnet mask.
4. Configure an IP address pool: configure the start IP address and subnet mask for the IP address pool. The start IP address of the IP address pool must be on the same network segment as the IP address entered in the **LAN Settings** text box.

Figure 15-4 Configure an L2TP server user



Copyright © Huawei Technologies Co., Ltd.

Figure 15-5 Setting L2TP server parameters



----End

15.3 Configuring IPSec VPN

This section describes how to configure IPSec VPN.

Context

On IP networks, most data is transmitted in plain text, causing security risks. For example, bank accounts and passwords may be intercepted, and user information may be forged. IPSec can protect transmitted IP packets to reduce the risk of information leak.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Choose **LANSettings** > **VPN** > **IPSec VPN** to open the **IPSec VPN** page, as shown in **Figure 15-6**.

Figure 15-6 Configuring IPSec VPN

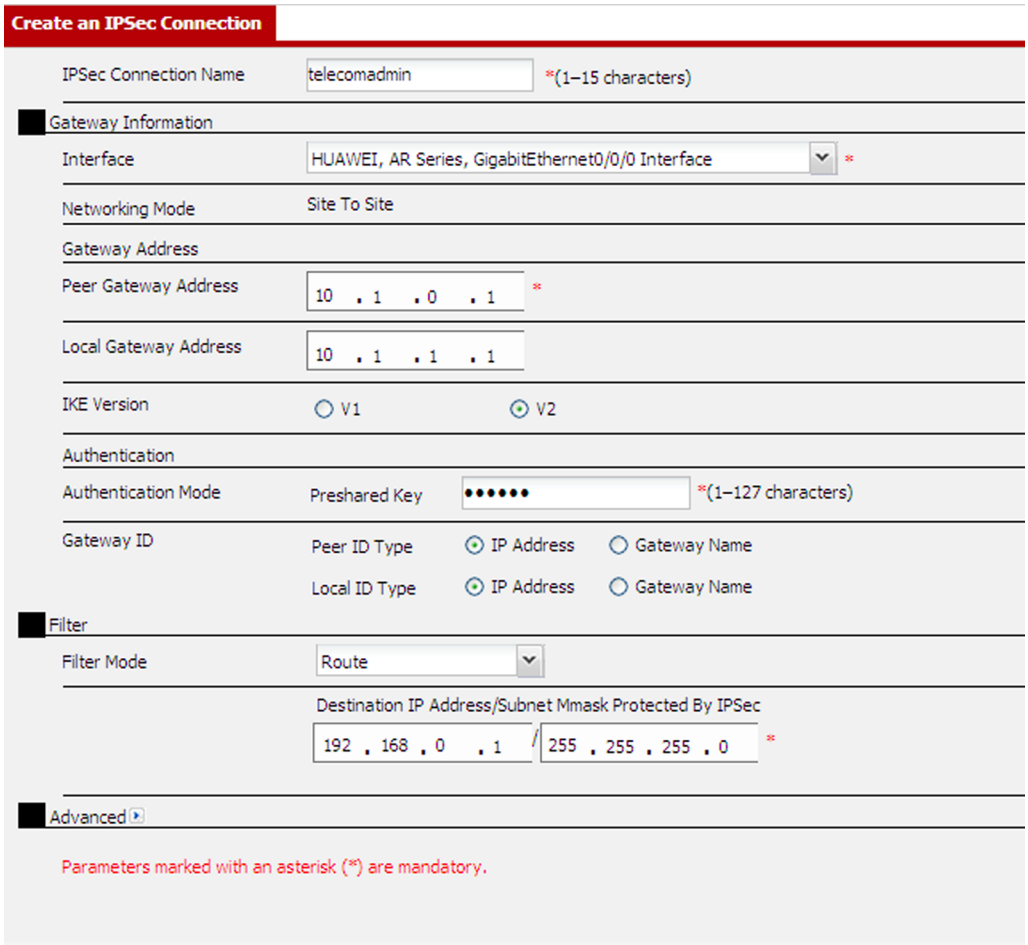
Step 2 Create an IPSec connection.

Click **Creat** on the page shown in **Figure 15-6**. The page shown in **Figure 15-7** is displayed. Set IPSec connection parameters and click **OK**.

NOTE

Configure the same IKE version and pre-shared key for both ends of an IPSec connection.

Figure 15-7 Setting IPSec connection parameters

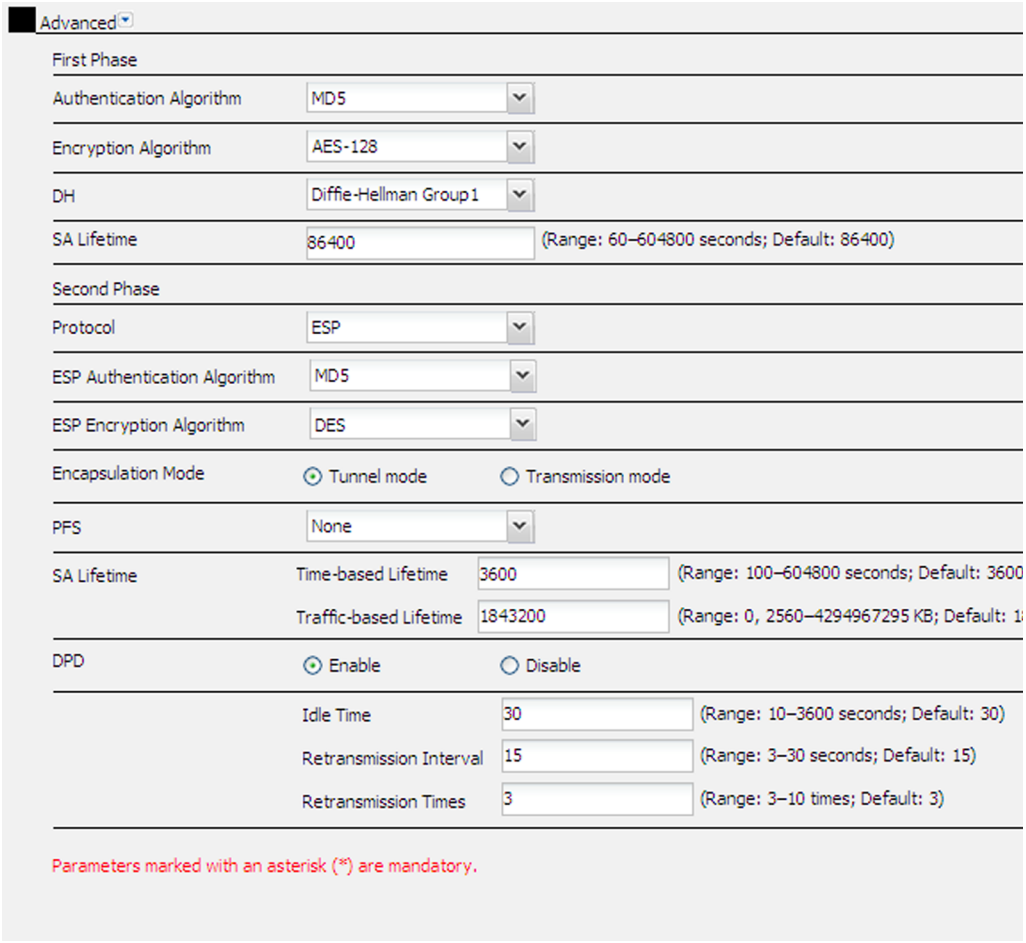


Step 3 (Optional) Set advanced IPSec parameters.

Click next to **Advance** on the page shown in **Figure 15-7**. The page shown in **Figure 15-8** is displayed. Set advanced IPSec parameters and click **OK**.

Copyright © Huawei Technologies Co., Ltd.

Figure 15-8 Setting advanced IPSec parameters



----End

15.4 Configuring SSL VPN

This section describes how to configure SSL VPN.

15.4.1 Configuring Basic SSL VPN Functions

This section describes how to configure basic SSL VPN functions.

Context

Based on the Hypertext Transfer Protocol Secure (HTTPS) protocol, Security Socket Layer (SSL) VPN uses the data encryption, user identity authentication, and message integrity check mechanisms of the SSL protocol to ensure secure remote access to enterprise intranets.

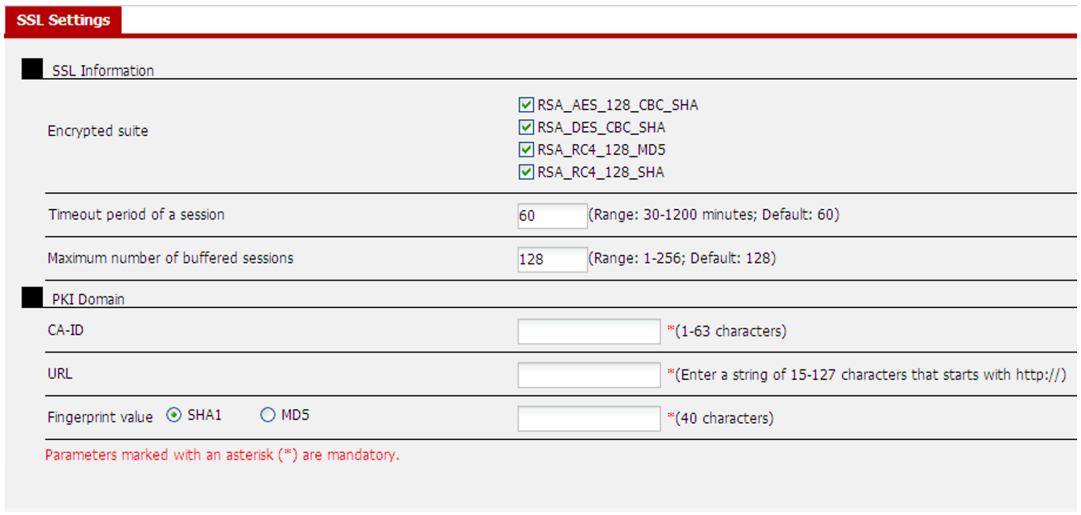
An SSL VPN gateway is located at an intranet's edge, and works with the browsers installed on remote terminals or with clients downloaded using browsers to protect user data on the Internet. Additionally, the SSL VPN gateway functions as the proxy to allow users to access internal servers.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Choose **Basic Settings** > **VPN** > **SSL VPN** to open the **SSL Settings** page, as shown in **Figure 15-9**.

Figure 15-9 Configuring SSL VPN



Step 2 Configure SSL VPN.

Click **SSL Settings** on the page shown in **Figure 15-9**. The page shown in **Figure 15-10** is displayed. Set SSL parameters and click **Apply**.

NOTE

When you log in to the web NMS using HTTPS, SSL configuration cannot be modified.

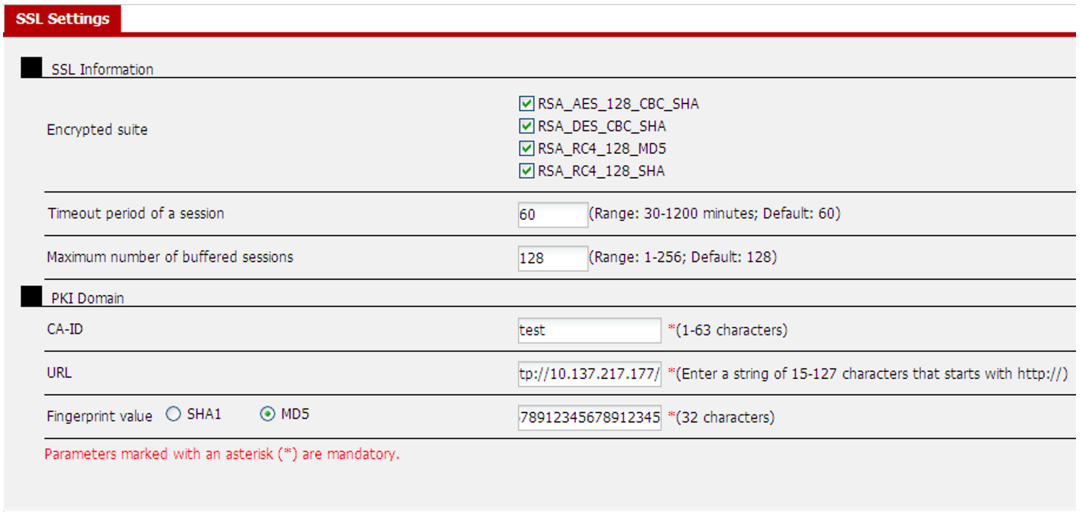
Before enabling the HTTPS service, ensure that the system date displayed on your PC (web client) is the same as that on the router.

The number of buffered sessions varies according to the product model:

- Huawei AR150&200 series: The value ranges from 1 to 64, and the default value is 32.
- Huawei AR1200&AR2200 series: The value ranges from 1 to 256, and the default value is 128.
- Huawei AR3200 series: The value ranges from 1 to 512, and the default value is 256.

Copyright © Huawei Technologies Co., Ltd.

Figure 15-10 Setting SSL VPN parameters



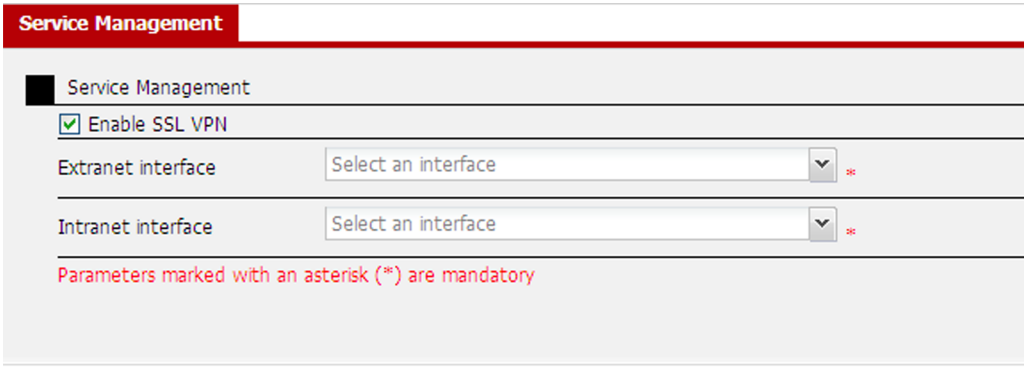
Step 3 Enable the SSL VPN function.

Choose **Basic Settings** > **VPN** > **SSL VPN** > **Service Management** on the page shown in **Figure 15-9**. The page shown in **Figure 15-11** is displayed. Select **Enable SSL VPN**, configure intranet and extranet interfaces, and click **Apply**.

NOTE

To make the configuration take effect, configure Layer 3 interfaces as intranet and extranet interfaces and assign IP addresses to the two interfaces.

Figure 15-11 Enabling the SSL VPN function



----End

15.4.2 Managing SSL VPN Users

This section describes how to manage SSL VPN users.

Context

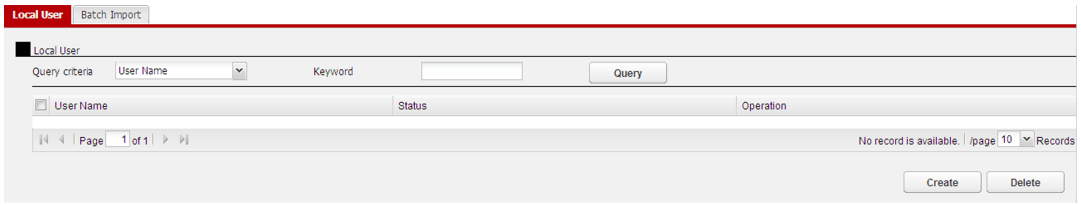
To log in to a virtual gateway, each user needs a user name and a password. All the user names and passwords of the locally authenticated users are stored on the virtual gateway. After a user enters the user name and password, the virtual gateway checks whether they are identical with the locally stored user name and password of this user. If they are identical, the virtual gateway allows the user to log in.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Choose **Basic Settings** > **VPN** > **SSL VPN** > **User Management** to open the **User Management** page, as shown in **Figure 15-12**.

Figure 15-12 Managing SSL VPN users



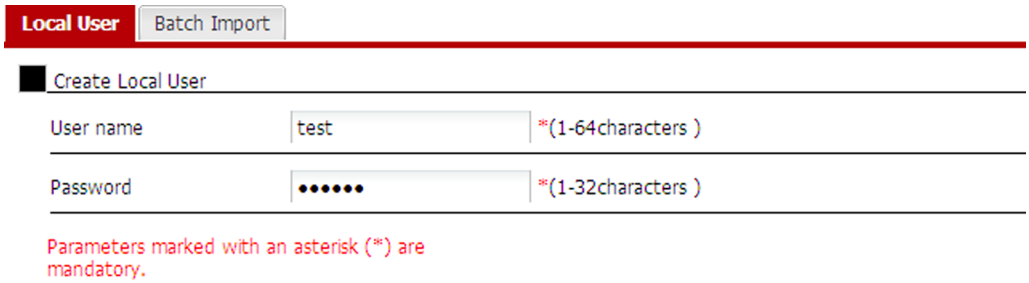
Step 2 (Optional) Add users.

You can create a single user or import user information from a file to add multiple users at one time.

- Create a local user.

  Choose **User Management** > **Local User** > **Create** to open the page shown in **Figure 15-13**. Set user parameters and click **OK**.

  Figure 15-13 Creating a local user

- Import users in batches.

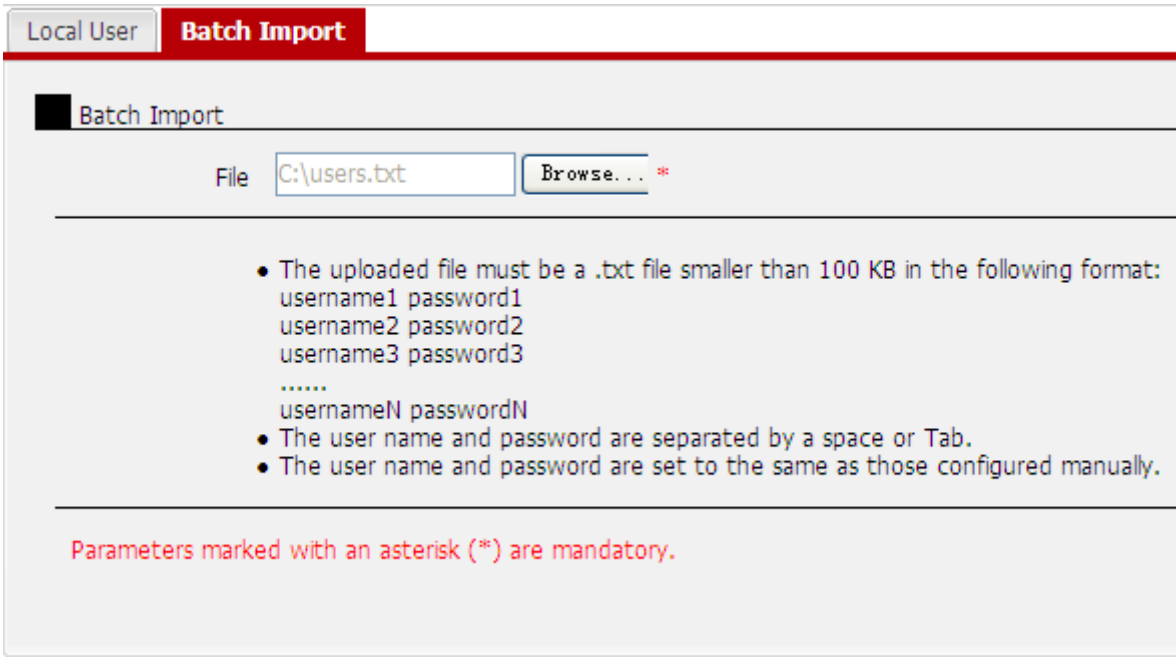
  Choose **User Management** > **Batch Import** to open the page shown in **Figure 15-14**. Import the file that lists the user names and passwords of multiple users and click **OK**.

  NOTE

  Some browsers request you to install ActiveX before batch import is performed.

Copyright © Huawei Technologies Co., Ltd.

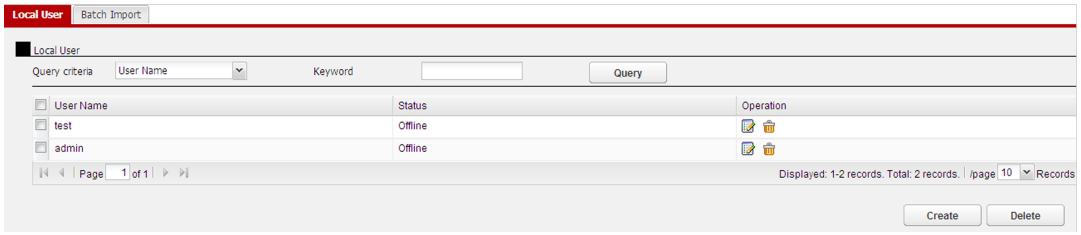
Figure 15-14 Importing users in batches



Step 3 (Optional) Modify parameters of an SSL VPN user.

Click on the page shown in **Figure 15-15** to modify parameters of a specified user.

Figure 15-15 Modifying or deleting SSL VPN users



Step 4 (Optional) Delete an SSL VPN user.

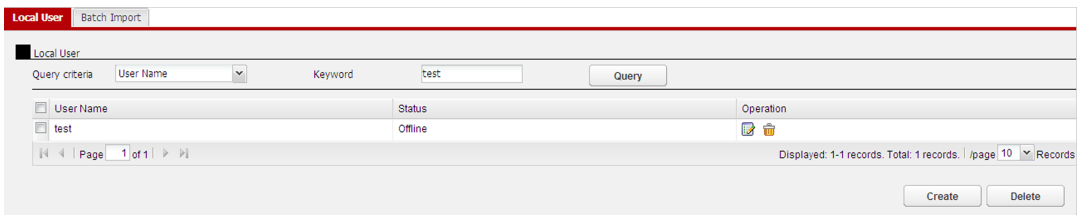
Click on the page shown in **Figure 15-15** to delete a specified user.

Alternatively, select a user and click **Delete** to delete the user.

Step 5 (Optional) Search for an SSL VPN user.

On the page shown in **Figure 15-16**, select a query type, enter a keyword, and click **Query** to search for a user.

Figure 15-16 Searching for an SSL VPN user



----End

Copyright © Huawei Technologies Co., Ltd.

15.4.3 Configuring SSL VPN Services

This section describes how to configure SSL VPN services.

Configuring the Web Proxy Service

This section describes how to configure the web proxy service for SSL VPN.

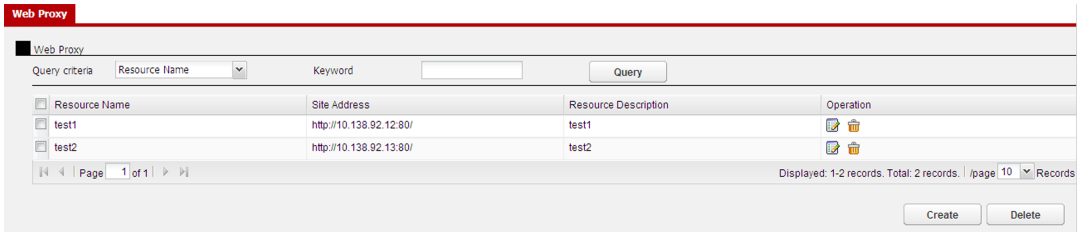
Context

Users use a browser to access an internal web server through an SSL VPN gateway in HTTPS mode. The SSL VPN gateway functions as a proxy that forwards data between users and the internal web server. This function ensures secure access to the internal web server.

Procedure

Step 1 Choose **Basic Settings** > **VPN** > **SSL VPN** > **Resource Management** > **Web Proxy** to open the **Web Proxy** page, as shown in **Figure 15-17**.

Figure 15-17 Configuring the web proxy service



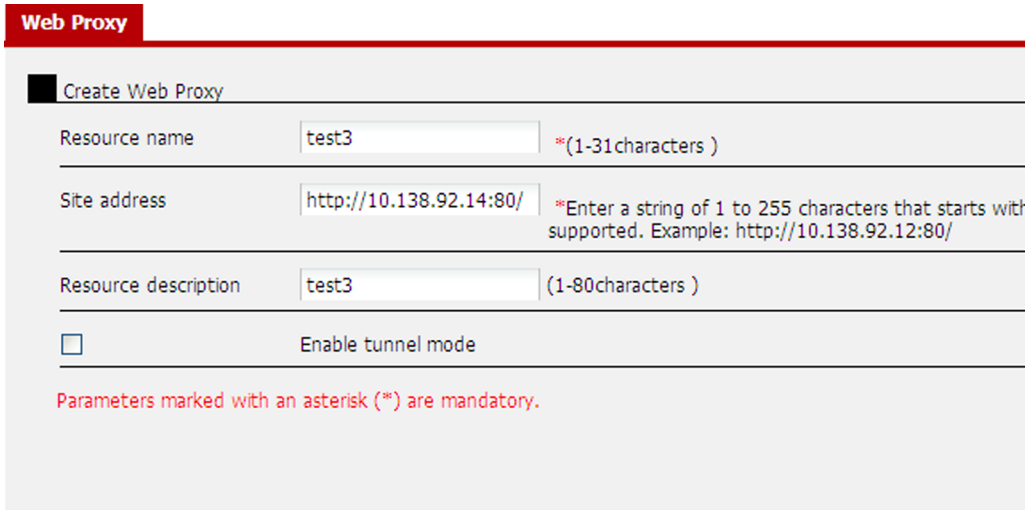
Step 2 Create a web proxy.

Click **Create** on the page shown in **Figure 15-17**. The page shown in **Figure 15-18** is displayed. Set web proxy parameters and click **OK**.

NOTE

Site addresses and resource description are case sensitive.

Figure 15-18 Creating a web proxy



Copyright © Huawei Technologies Co., Ltd.

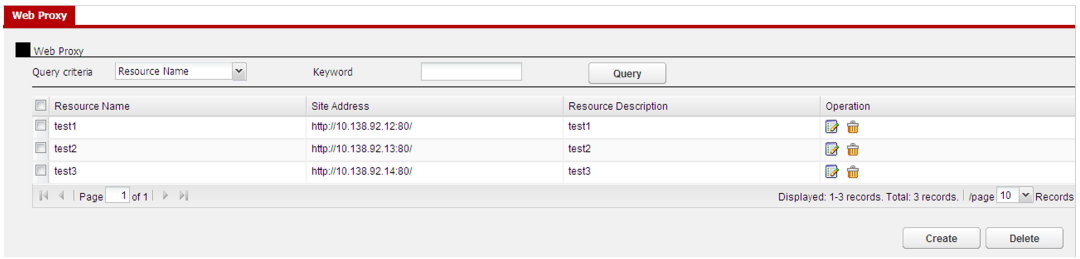
Step 3 (Optional) Modify web proxy parameters.

Click on the page shown in **Figure 15-19** to modify the parameters of a specified web proxy.

NOTE

Changing the resource name is not allowed.

Figure 15-19 Modifying or deleting a web proxy



Step 4 (Optional) Delete a web proxy.

Click on the page shown in **Figure 15-19** to delete a specified web proxy.

Alternatively, select a web proxy resource and click **Delete** to delete the specified web proxy.

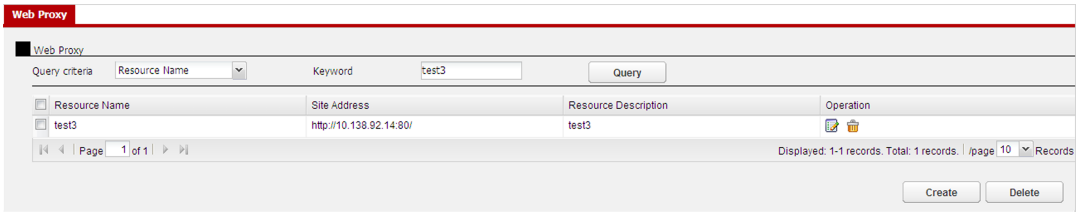
Step 5 (Optional) Search for a web proxy.

On the page shown in **Figure 15-20**, select a query type, enter a keyword, and click **Query** to search for a web proxy.

NOTE

Site addresses and resource description are case sensitive.

Figure 15-20 Searching for a web proxy



----End

Configuring the Port Forwarding Service

This section describes how to configure the port forwarding service for SSL VPN.

Context

Users can access the TCP-based services on an internal network. The typical port forwarding services include Telnet login, desktop sharing, and email.

Procedure

Step 1 Choose **Basic Settings** > **VPN** > **SSL VPN** > **Resource Management** > **Port Forwarding** to open the **Port Forwarding** page, as shown in **Figure 15-21**.

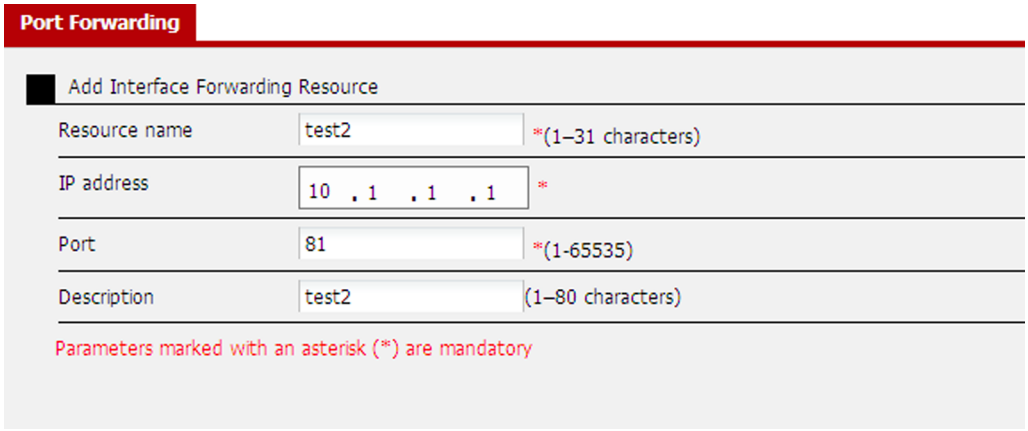
Copyright © Huawei Technologies Co., Ltd.

Figure 15-21 Port forwarding service configuration

Step 2 Create a port forwarding resource.

Click **Create** on the page shown in **Figure 15-21**. The page shown in **Figure 15-22** is displayed. Set port forwarding parameters and click **OK**.

Figure 15-22 Creating a port forwarding resource



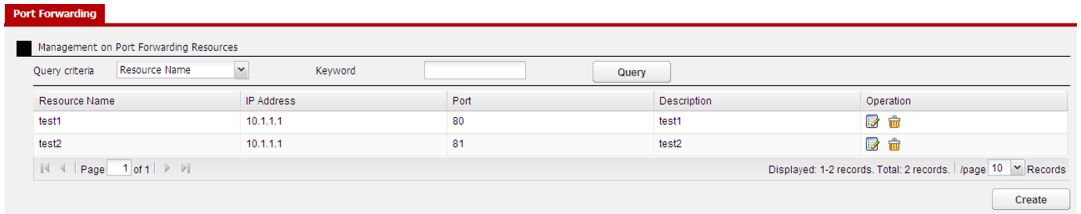
Step 3 (Optional) Modify port forwarding parameters.

As shown in **Figure 15-23**, click to Modify a port forwarding resource.

NOTE

Changing the resource name is not allowed.

Figure 15-23 Modifying or deleting a port forwarding resource



Step 4 (Optional) Delete a port forwarding resource.

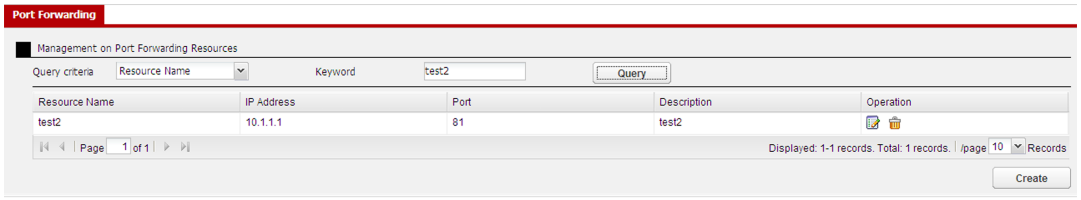
As shown in **Figure 15-23**, click to delete specified port forwarding resources.

Step 5 (Optional) Search for port forwarding resources.

As shown in **Figure 15-24**, select a query item, enter a keyword, and click **Query** to search for port forwarding resources that meet the search criteria.

Copyright © Huawei Technologies Co., Ltd.

Figure 15-24 Searching for port forwarding resources



----End

Configuring the IP Forwarding Service

This section describes how to configure the IP forwarding service for SSL VPN.

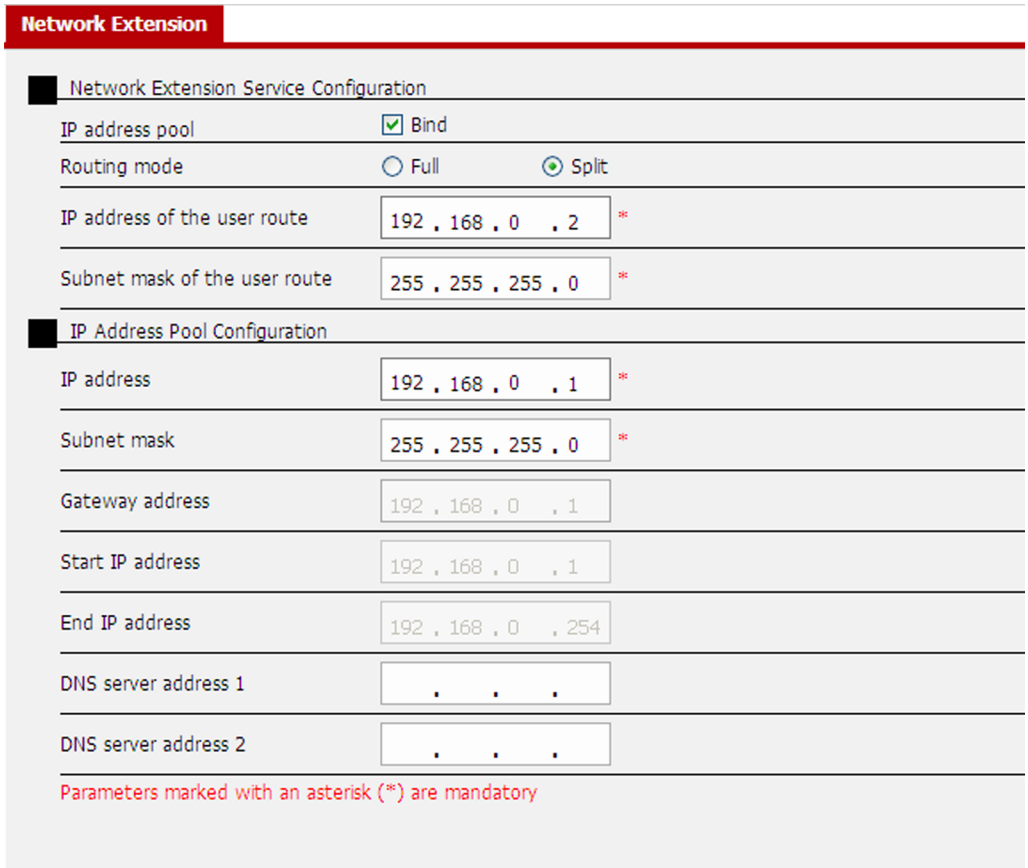
Context

The IP forwarding function allows remote terminals to communicate with internal servers at the network layer. For example, remote terminals are allowed to ping internal servers.

Procedure

Step 1 Choose **Basic Settings** > **VPN** > **SSL VPN** > **Resource Management** > **Network Extension** to open the **Network Extension** page, as shown in **Figure 15-25**.

Figure 15-25 Configuring the IP forwarding service



Copyright © Huawei Technologies Co., Ltd.

Step 2 Set IP forwarding parameters and click **Apply**.

----End

15.4.4 Configuring an Authentication Policy for SSL VPN

This section describes how to configure an authentication policy for SSL VPN.

Context

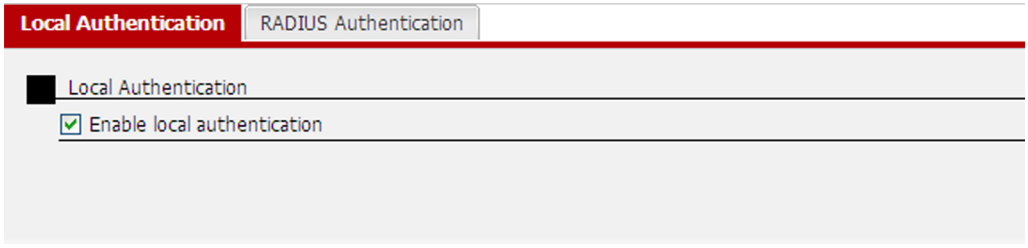
If users need to be authenticated but no RADIUS server is deployed on the network, use local authentication. Local authentication features fast authentication and low operation cost, whereas the amount of information that can be stored is limited by the device hardware.

RADIUS protects a network from unauthorized access. It is often used on the networks that require high security and remote user access control.

Procedure

Step 1 Choose **Basic Settings** > **VPN** > **SSL VPN** > **Domain Management** > **Verification Policy** to open the **Verification Policy** page, as shown in **Figure 15-26**.

Figure 15-26 Configuring an authentication policy



Step 2 Select local or RADIUS authentication according to network requirements.

- Local authentication

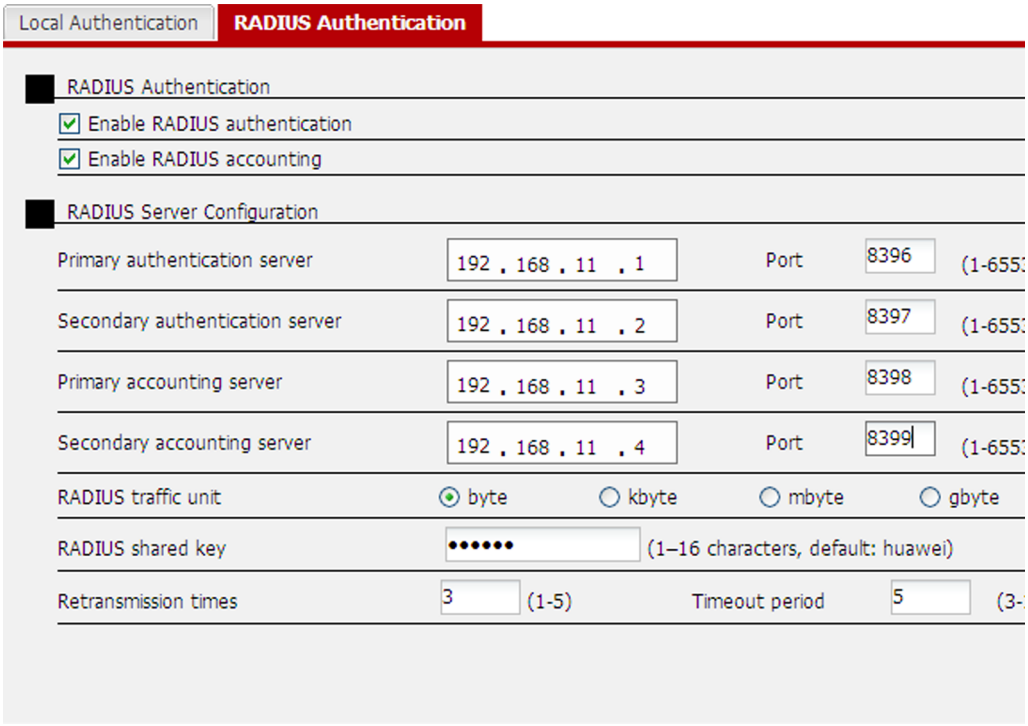
  As shown in **Figure 15-26**, click **Local Authentication**, select **Enable local authentication**, and click **Application** to configure local authentication.

- RADIUS authentication

  As shown in **Figure 15-26**, click **RADIUS authentication**. The page shown in **Figure 15-27** is displayed. Set RADIUS authentication parameters and click **Application**.

Copyright © Huawei Technologies Co., Ltd.

Figure 15-27 Setting RADIUS authentication parameters



----End

Copyright © Huawei Technologies Co., Ltd.

16 Device Maintenance and Management

About This Chapter

This section describes how to maintain and manage the device, including user management, basic device management, remote management, and system maintenance.

16.1 Managing Users
This section describes how to create users, change user passwords, and delete users.

16.2 Basic Device Management
Basic device management includes device restart, one-key restoration, configuration maintenance, software upgrade, and time settings.

16.3 Managing the Router Remotely
Remote management includes TR-069, SNMP, Syslog, and remote access.

16.4 System Maintenance
System maintenance includes troubleshooting tool management and log management.

Copyright © Huawei Technologies Co., Ltd.

16.1 Managing Users

This section describes how to create users, change user passwords, and delete users.

Context

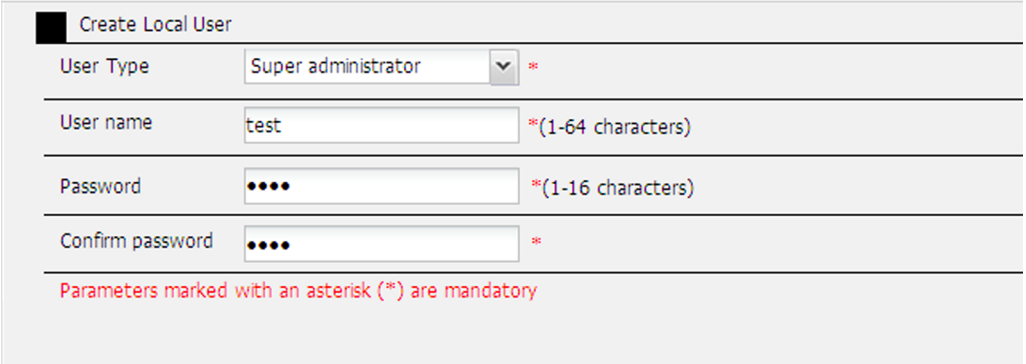
Different online users cannot use the same user account.

Procedure

Step 1 Choose **Management** > **User Management**.

Step 2 Enter the user name and password, and click **OK**, as shown in **Figure 16-1**.

Figure 16-1 Creating a user

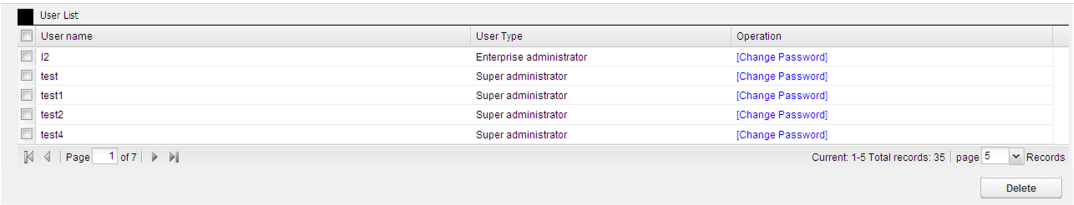


NOTE

Only super administrators have the right to create users, including super administrators, enterprise administrators, or common users.

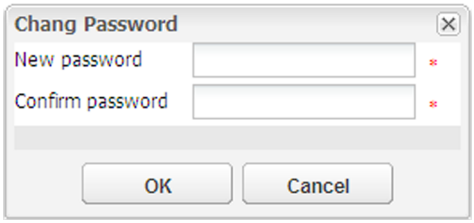
Step 3 Change passwords and delete users in the user list, as shown in **Figure 16-2**.

Figure 16-2 User list



1. Click **Change Password** next to an account and enter a new password, as shown in **Figure 16-3**.

Figure 16-3 Changing password



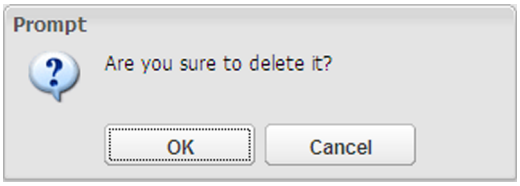
Huawei Proprietary and Confidential
Copyright © Huawei Technologies Co., Ltd.

NOTE

The user of a higher level can change its own password and the passwords at lower levels. A common user can only change its own password.

2. Select the user that you want to delete and click **Delete**. When the dialog box shown in **Figure 16-3** is displayed, click **OK**.

Figure 16-4 Deleting a user



NOTE

Only super administrators have the right to delete users.

Super administrators and enterprise administrators cannot be deleted.

You can select multiple users to delete them in a batch.

----End

16.2 Basic Device Management

Basic device management includes device restart, one-key restoration, configuration maintenance, software upgrade, and time settings.

16.2.1 Device Restart

This section describes how to restart the device.

Context

After specifying the configuration file for next startup, restart the device to make the configuration take effect.

CAUTION

Before restarting the device, save the configuration by referring to **Saving Configuration**. Otherwise, unsaved configuration will be lost. After the device restarts, you must enter the user name and password to log in to the Web NMS.

Procedure

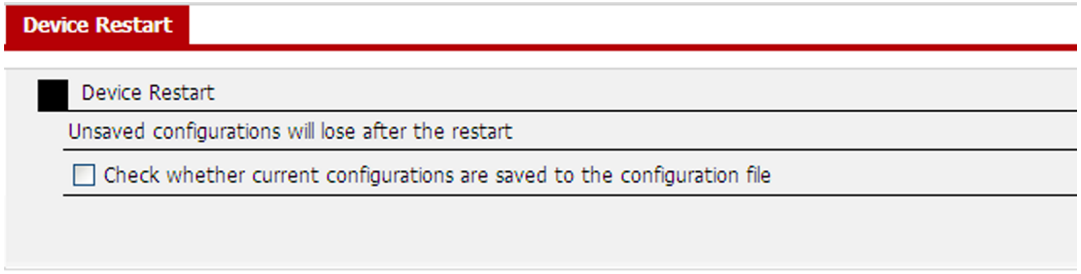
Step 1 Choose **Management** > **Device Restart**. The **Device Restart** page is displayed, as shown in **Figure 16-5**.

NOTE

To save the current configuration, select **Check whether current configurations are saved to the configuration file**. It is recommended that you select this check box.

Copyright © Huawei Technologies Co., Ltd.

Figure 16-5 Restarting the device



Step 2 Click **Restart**.

- If the **Check whether current configurations are saved to the configuration file.** check box is selected, the system will save the configuration and then restart the device.

Figure 16-6 Save

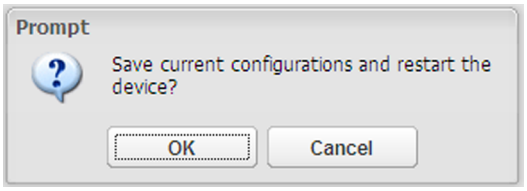


Figure 16-7 Saving the current configuration

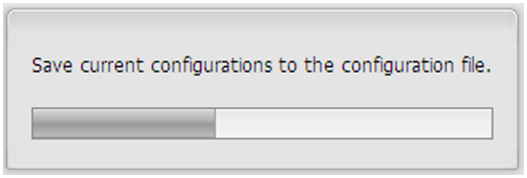
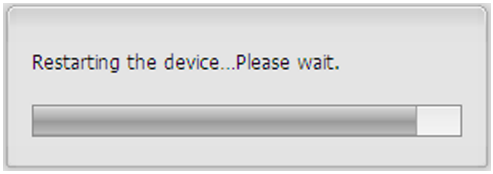
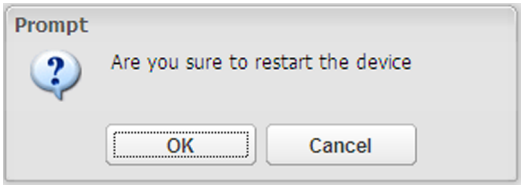


Figure 16-8 Restart



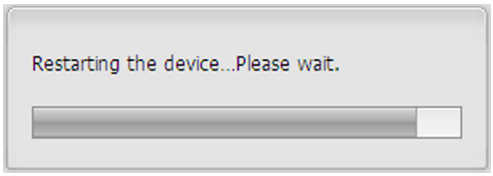
- If the **Check whether current configurations are saved to the configuration file.** check box is not selected, select **OK** in the dialog box shown in **Figure 16-9** to restart the device. During the device restart, the dialog box shown in **Figure 16-10** is displayed.

Figure 16-9 Confirm



Copyright © Huawei Technologies Co., Ltd.

Figure 16-10 Restart



----End

16.2.2 One-Key Restoration

This section describes how to restore the factory settings or previously saved installation configuration.

Context

Only AR200 supports one-key restoration.

If the **Saving Installation Configuration** function is not enabled, this operation restores the factory settings.

If the **Saving Installation Configuration** function is enabled, this operation restores the previously saved installation configuration.

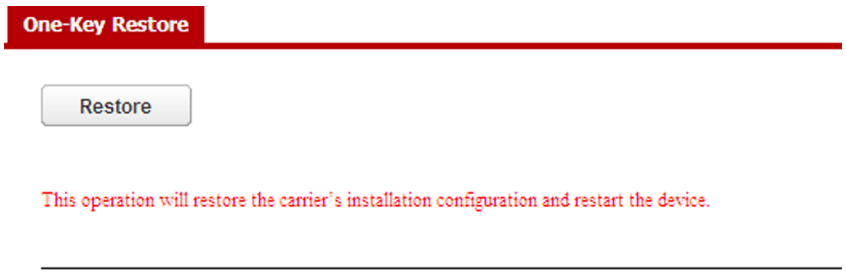
CAUTION

The one-key restoration function will restart the device. Perform this operation only when necessary.

Procedure

Step 1 Choose **Management** > **One Key Restore**. The **One Key Restore** page is displayed, as shown in **Figure 16-11**.

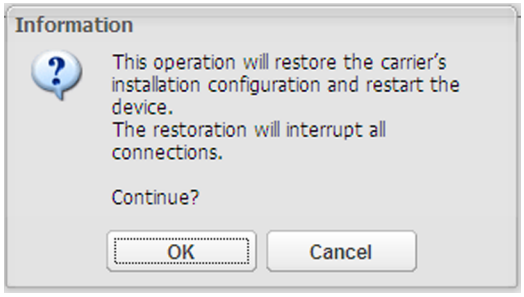
Figure 16-11 One-Key Restore



Step 2 Click **Restore**. The page shown in **Figure 16-12** is displayed.

Copyright © Huawei Technologies Co., Ltd.

Figure 16-12 Prompt



Step 3 Click **OK** to restart the device.

----End

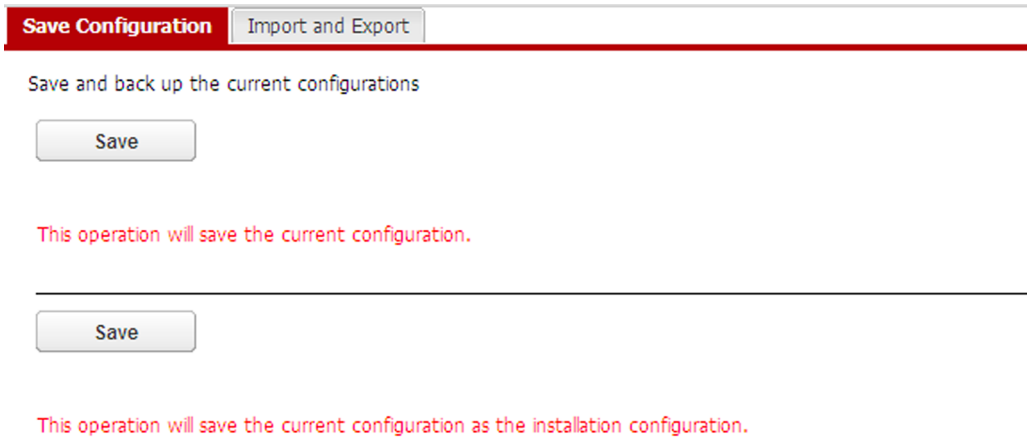
16.2.3 Maintaining the Configuration

You can save the configuration, import or export the configuration file.

Procedure

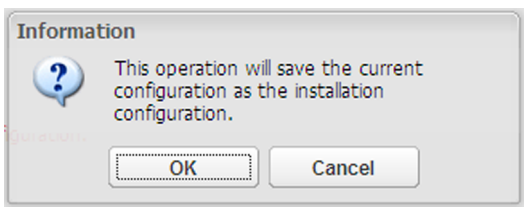
- Save the configuration.
  1. Choose **Management** > **Maintenance** > **Save Configuration** to open the page shown in **Figure 16-13**.

     Figure 16-13 Saving the configuration

  2. Click **Save** to save the current configuration. After the current configuration is saved, the saved configuration is loaded during the next device restart.
  3. Click **Save**. The page shown in **Figure 16-14** is displayed. Click **OK** to save the current configuration as the installation settings. After the installation settings are saved, the current configuration will not be lost when you restore the installation settings.

     Figure 16-14 Save the current configuration as the installation settings

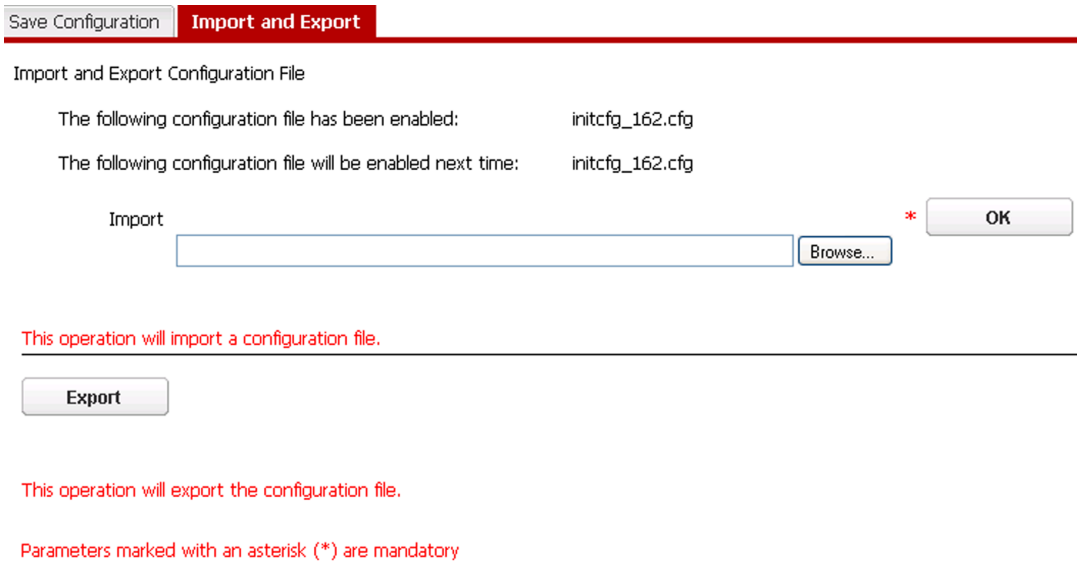
Copyright © Huawei Technologies Co., Ltd.

NOTE

Only the AR200 supports the function that saves the installation settings.

- Import or export the configuration file.
  - Import the configuration file.
    1. Choose **Management** > **Maintenance** > **Import and Export** to open the page shown in **Figure 16-15**.

Figure 16-15 Importing or exporting the configuration file



    2. Click **Browse** to select the configuration file with the file name extension .zip or .cfg to import.
    3. Click **OK** to configure the imported configuration file as the configuration file for next startup.
  - Export the configuration file.

    Click **Export** to export the configuration file for next startup to a specified directory.

----End

16.2.4 Software Upgrade

This section describes how to upgrade the software.

Context

CAUTION

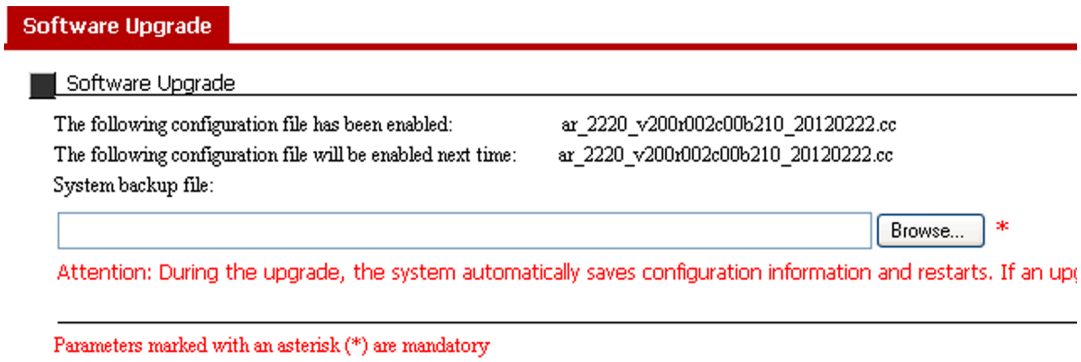
Software upgrade will restart the device and interrupt services. Perform this operation only when necessary.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Choose **Management** > **Software Upgrade**. The **Software Upgrade** page is displayed, as shown in **Figure 16-16**.

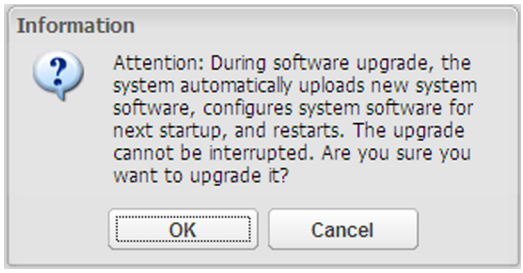
Figure 16-16 Software Upgrade



Step 2 Click **Browse** to select the software to upgrade.

Step 3 Click **OK**. The page shown in **Figure 16-17** is displayed.

Figure 16-17 Information



Step 4 Click **OK** to start software upgrade.

----End

16.2.5 Time Settings

This section describes how to set the system time.

Context

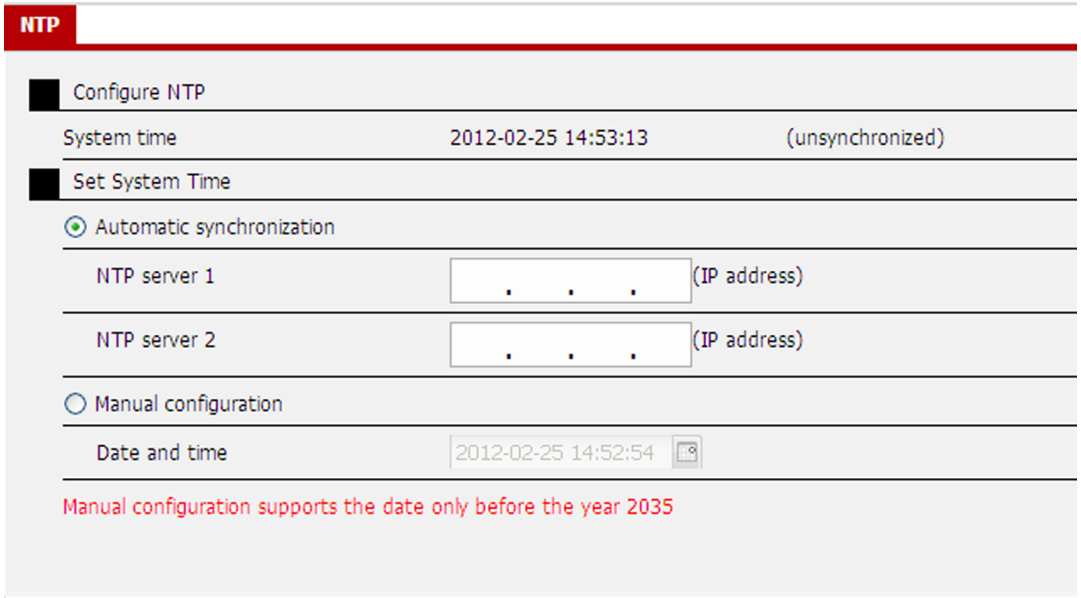
You can set the system time by enabling automatic synchronization between the device and the NTP server. You can also set the time manually. The first method is recommended.

Procedure

- Synchronize the time between the device and the NTP server.
  1. Choose **System Management** > **Time Settings**. In the **Time Settings** page that is displayed, select **Automatic synchronization**, as shown in **Figure 16-18**.

Copyright © Huawei Technologies Co., Ltd.

Figure 16-18 Automatic synchronization



2. Enter the NTP server IP addresses in the **NTP server 1** and **NTP server 2** text boxes.

   NOTE

   The Web NMS supports two NTP servers. The system selects an NTP server based on the primary clock levels of the NTP servers. If NTP server 1 has a higher primary clock level than NTP server 2 does, the router synchronizes the system time with NTP server 1.

3. Click **Apply**.

   NOTE

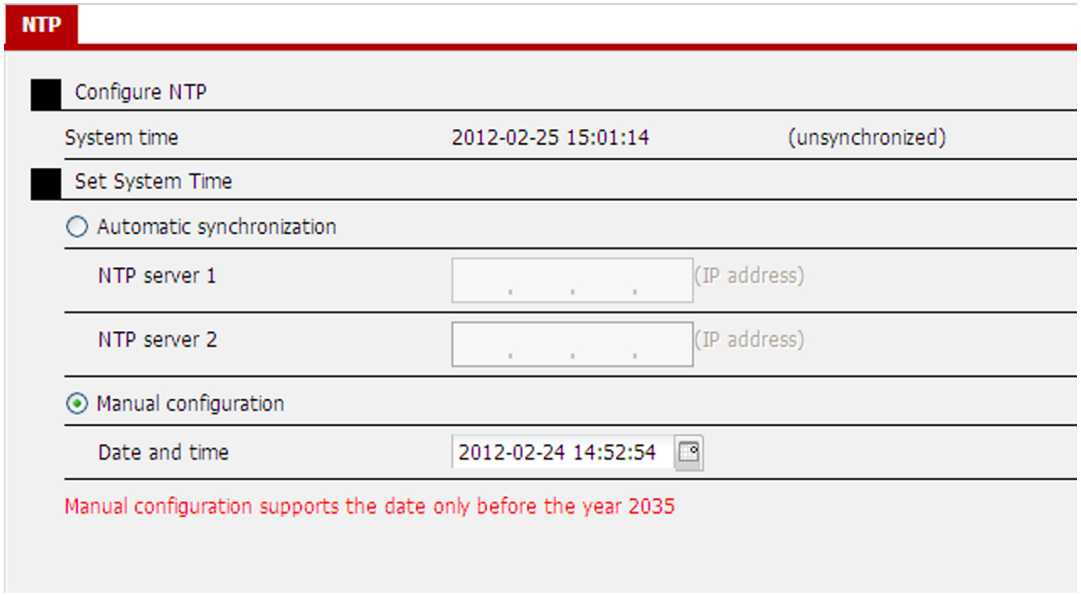
   If the router has a higher primary clock level than NTP servers 1 and 2 do, the router does not synchronize the system time with the NTP servers.

- Manually set the system time.

  1. Choose **System Management** > **Time Settings**. In the **Time Settings** page that is displayed, select **Manual configuration**, as shown in **Figure 16-19**.

Copyright © Huawei Technologies Co., Ltd.

Figure 16-19 Manual configuration



2. Enter the date and time.
3. Click **Apply**.

----End

16.3 Managing the Router Remotely

Remote management includes TR-069, SNMP, Syslog, and remote access.

16.3.1 Configuring TR-069

TR-069 defines the communication mechanism between Customer Premises Equipment (CPE) and Auto-Configuration Server (ACS) and enables the ACS to manage CPEs. AR routers are CPEs.

Context

TR-069, also called CPE WAN Management Protocol (CWMP), is drafted by the Digital Subscriber's Line (DSL) forum.

To enable an ACS to manage a CPE, a connection is required between the ACS and the CPE. During connection setup, the CPE or ACS needs to be authenticated. The connection can be set up only after the CPE or ACS is authenticated. After the connection is set up, the ACS invokes Remote Procedure Call (RPC) methods to manage and maintain 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 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.

Copyright © Huawei Technologies Co., Ltd.

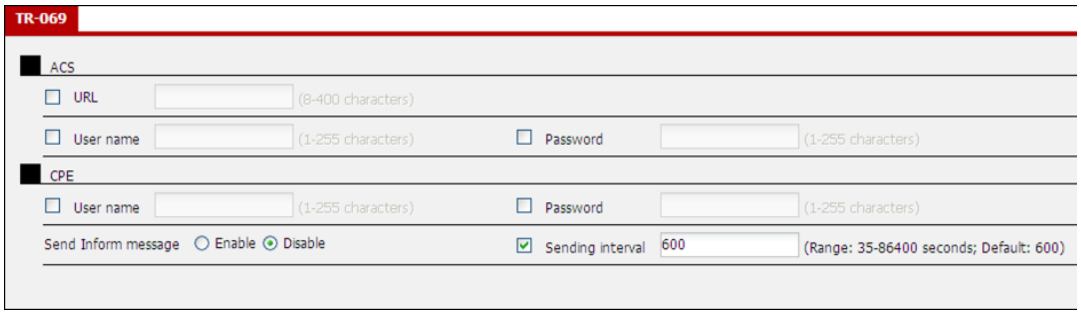
- Connection initiated by an ACS

  After the ACS sends an 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 if the ACS has communicated with the CPE at least once through a session that the CPE initiates by sending a Connection Request.

Procedure

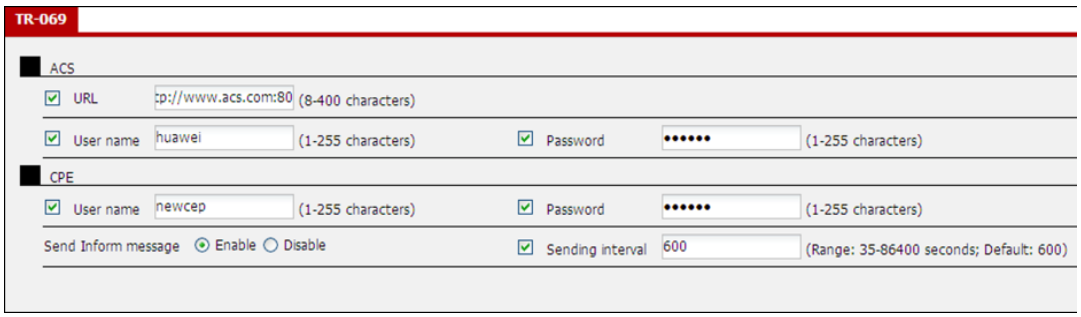
Step 1 Choose **Basic Settings** > **Remote Management** > **TR-069** to open the page shown in **Figure 16-20**.

Figure 16-20 Configuring TR-069



Step 2 Set the TR-069 parameters.

Figure 16-21 Configuring TR-069



Step 3 Click **Apply** to complete TR-069 configuration.

----End

16.3.2 Configuring SNMP

The router uses SNMP to send traps to the network management station.

Context

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 16-1 Usage scenarios of SNMP

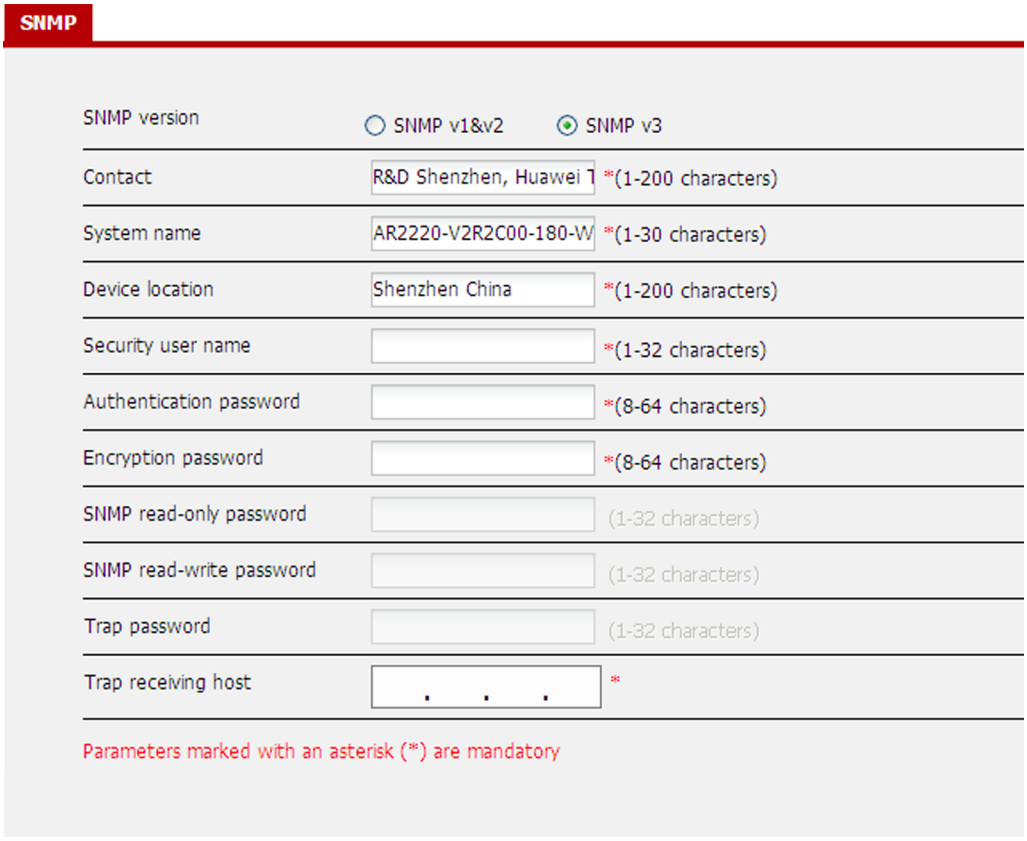
Version	Usage Scenario
SNMPv1	Applicable to small-sized networks. The networks have simple structures, have low security requirements or are not prone to attacks, and have stable topologies. For example, campus networks and small enterprise networks.
SNMPv2	Applicable to medium- or large-sized networks. 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. If the network management station and managed devices communicate over the public network, SNMPv3 is recommended.

Procedure

Step 1 Choose **Basic Settings** > **Remote Management** > **SNMP** to open the page shown in **Figure 16-22**. By default, the SNMP version is SNMPv3.

Copyright © Huawei Technologies Co., Ltd.

Figure 16-22 Configuring SNMP



Step 2 Configure the SNMP function.

- Configure SNMPv1&SNMPv2.

1. Set the SNMP version to SNMPv1&SNMPv2, indicating that the router supports both SNMPv1 and SNMPv2.

   NOTE

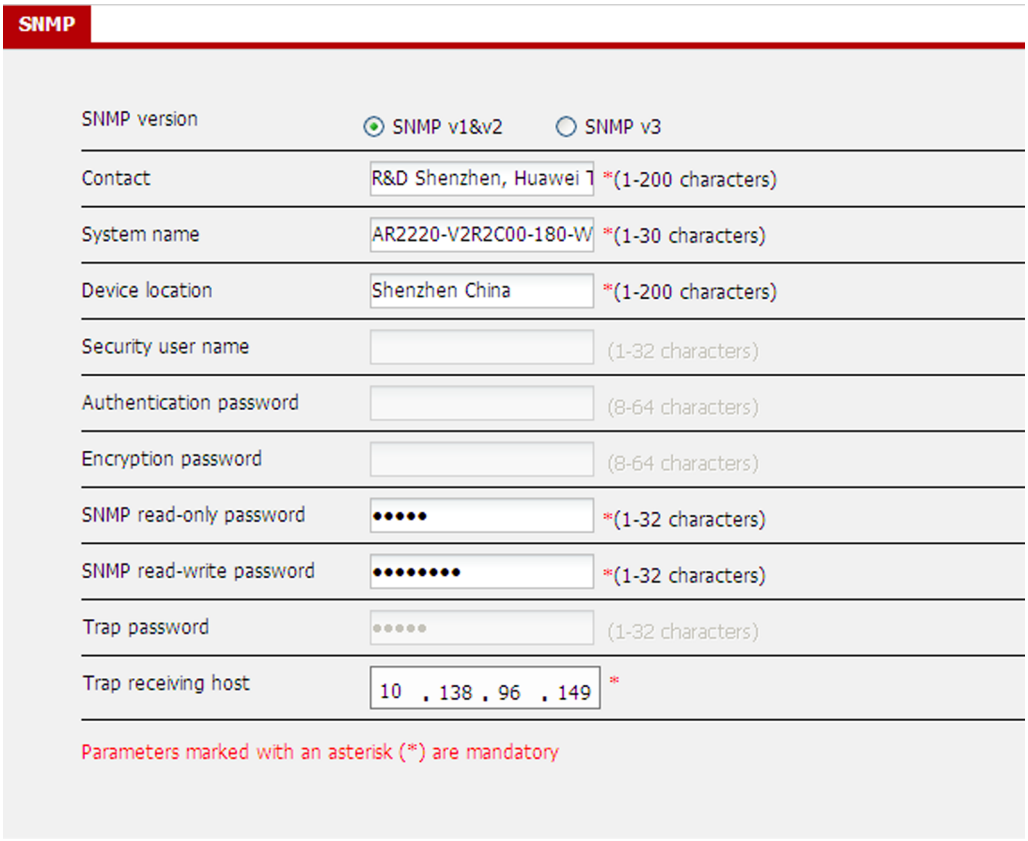
   The parameters of SNMPv1 and SNMPv2 are the same.

   The password for the read operation must be different from the password for the read-write operation.

2. Set the parameters on the page shown in **Figure 16-23**.

Copyright © Huawei Technologies Co., Ltd.

Figure 16-23 Configuring SNMPv1&SNMPv2



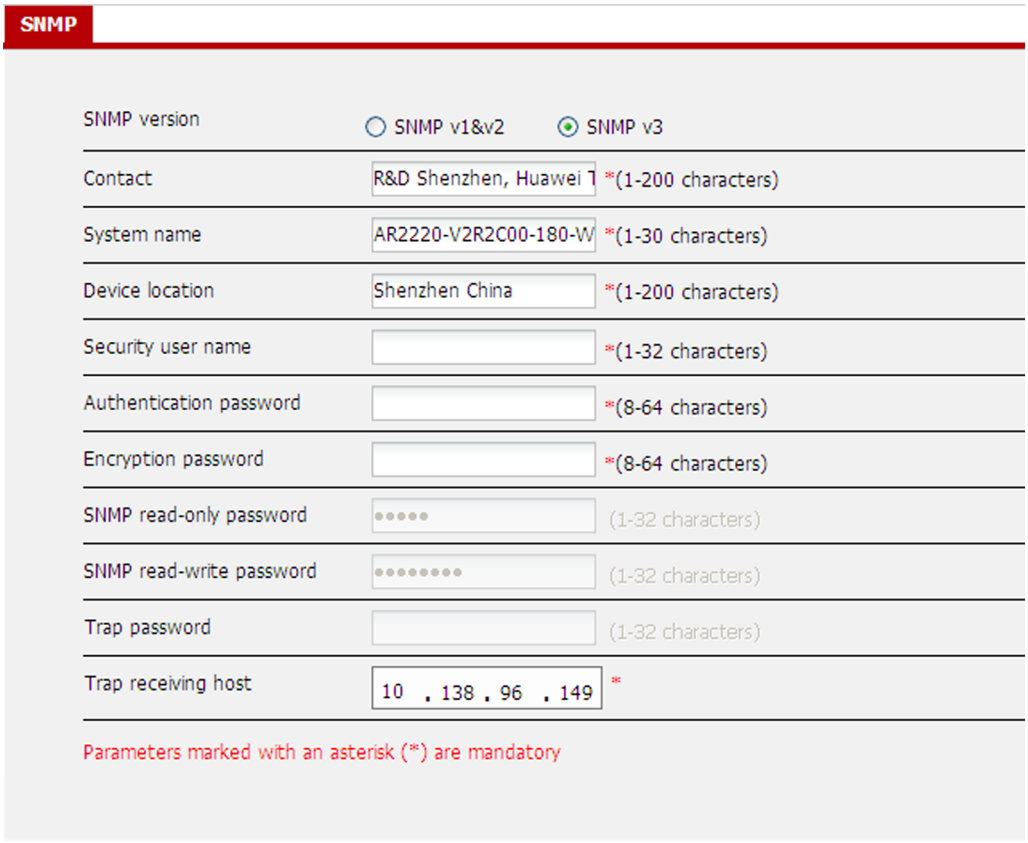
3. Click **OK**.

- Configure SNMPv3.

1. Set the SNMP version to SNMPv3.
2. Set the parameters on the page shown in **Figure 16-24**.

Copyright © Huawei Technologies Co., Ltd.

Figure 16-24 Configuring SNMPv3



3. Click **OK**.

----End

16.3.3 Managing Syslog

Using the Syslog management function, you can configure logs locally or remotely.

Procedure

Step 1 Configure logs locally.

1. Choose **Basic Settings** > **Remote Management** > **Syslog Management** > **Local** to open the page shown in **Figure 16-25**.

Copyright © Huawei Technologies Co., Ltd.

Figure 16-25 Configuring logs locally

2. Select **Fault encoding level** and **Subtype**, and click **Query**.

   NOTE

   After you click **Query**:

   - The logs of the selected type are displayed.
   - The router records only the logs of the specified type and with the specified severity and higher severities. The processing methods for the logs of other types are not changed. For example, after you set the severity to error and type to DHCP, the router records only the logs with the severity error and higher severities for the DHCP module. The logs of other types are recorded using original methods.

   Table 16-2 lists the log severity. A small value indicates a high severity.

Table 16-2 Log severities

Value	Severity	Description
0	Emergencies	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.
1	Alert	A fault needs to be rectified immediately. For example, memory usage of the system reaches the upper limit.
2	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.
3	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.
4	Warning	Some events or operations may affect device running or cause service processing faults, which requires full attention. For example, users disable a routing process; BFD detects packet loss; error protocol packets are detected.

Copyright © Huawei Technologies Co., Ltd.

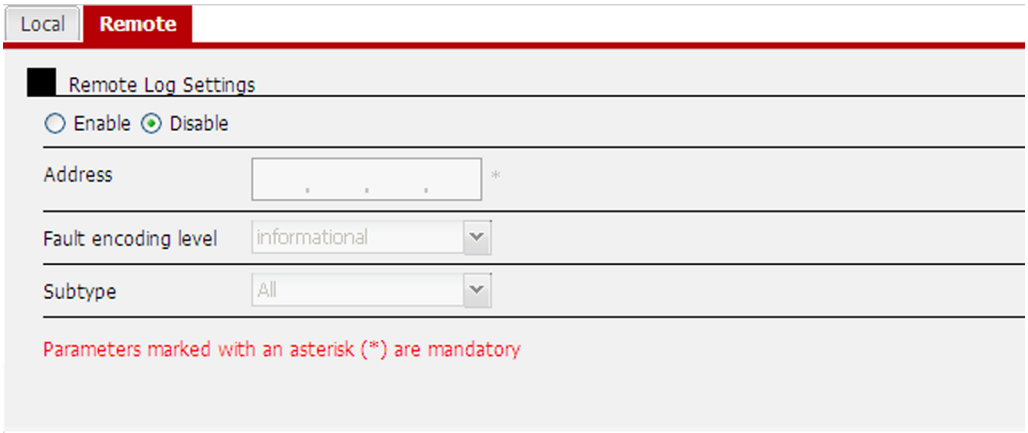
Value	Severity	Description
5	Notification	A key operation is performed to keep the device running normally. For example, the **shutdown** command is run; a neighbor is discovered; protocol status changes.
6	Informational	A normal operation is performed. For example, a **display** command is run.

3. To update the displayed log information, click **Refresh**.
4. To clear log information, click **Clear**.

Step 2 Configure logs remotely so that the logs can be sent to a remote log server.

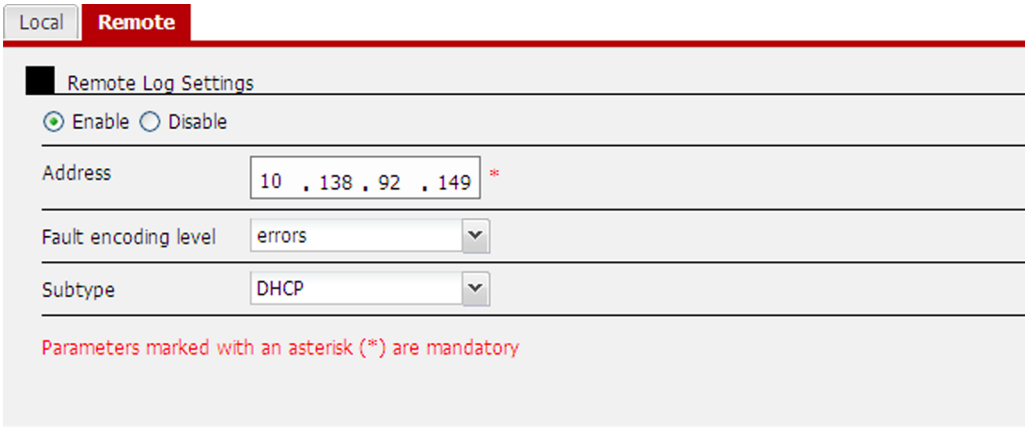
1. Choose **Basic Settings** > **Remote Management** > **Syslog Management** > **Remote** to open the page shown in **Figure 16-26**.

Figure 16-26 Configuring logs remotely



2. Select **Enable** and enter the IP address of the log server. Set **Fault encoding level** and **Subtype** to define the log filtering conditions, as shown in **Figure 16-27**.

Figure 16-27 Configuring logs remotely



3. Click **OK** to make the settings take effect.

Copyright © Huawei Technologies Co., Ltd.

NOTE

After you click **OK**, the router sends only the logs of the specified severity and type to the remote log server. As shown in **Figure 16-27**, after you click **OK**, the router sends only the DHCP-related logs with the severity error and higher severities to the remote log server 10.138.92.149.

----End

16.3.4 Configuring Remote Management

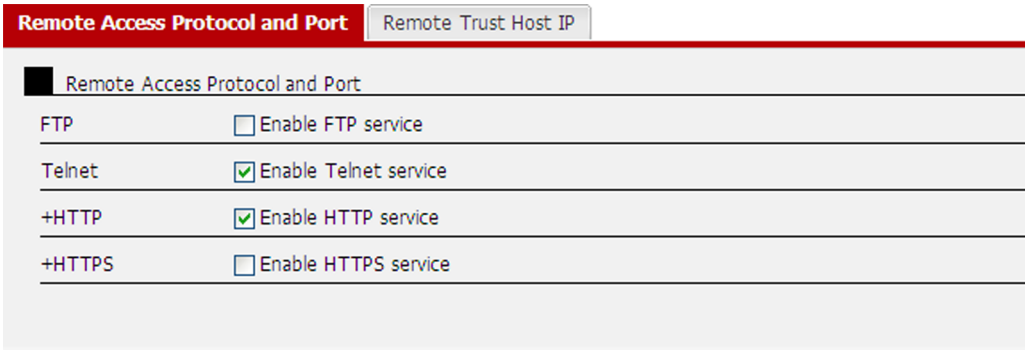
Remote access configurations include configuring the remote access protocol, port, and IP address of trusted host.

Procedure

Step 1 Configure the remote access protocol and port.

1. Choose **Basic Settings** > **Remote Management** > **Remote Management** > **Remote Access Protocol and Port** to open the page shown in **Figure 16-28**.

Figure 16-28 Configuring remote access protocol and port

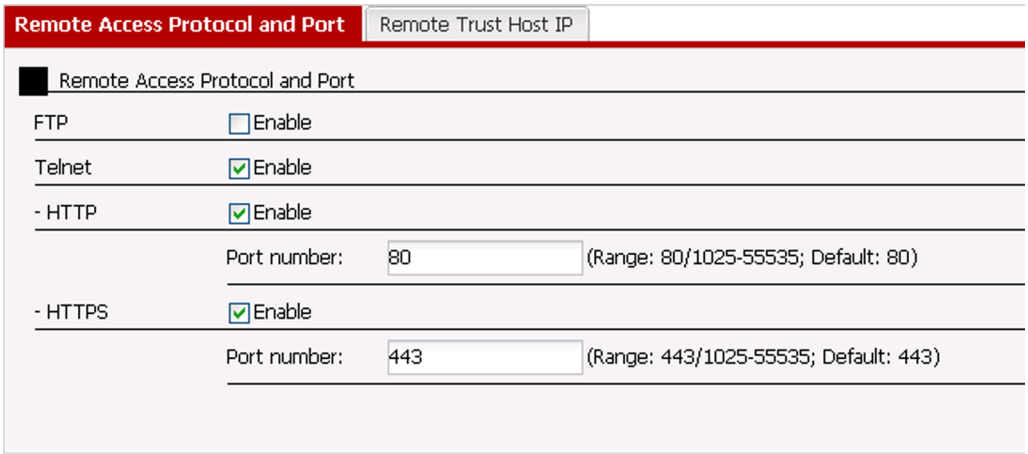


2. Specify the protocol and port used by other devices to access the AR router.

   By default, other devices can access the AR router using Telnet or HTTP.

   Click + to specify the access ports for HTTP and HTTPS, as shown in **Figure 16-29**.

Figure 16-29 Configuring access ports



Copyright © Huawei Technologies Co., Ltd.

After you change the port number and click **OK**, the current connection is torn down. Log in again using the new address in the format http://host:port or https://host:port. host is the IP address or domain name; port is the new port number.

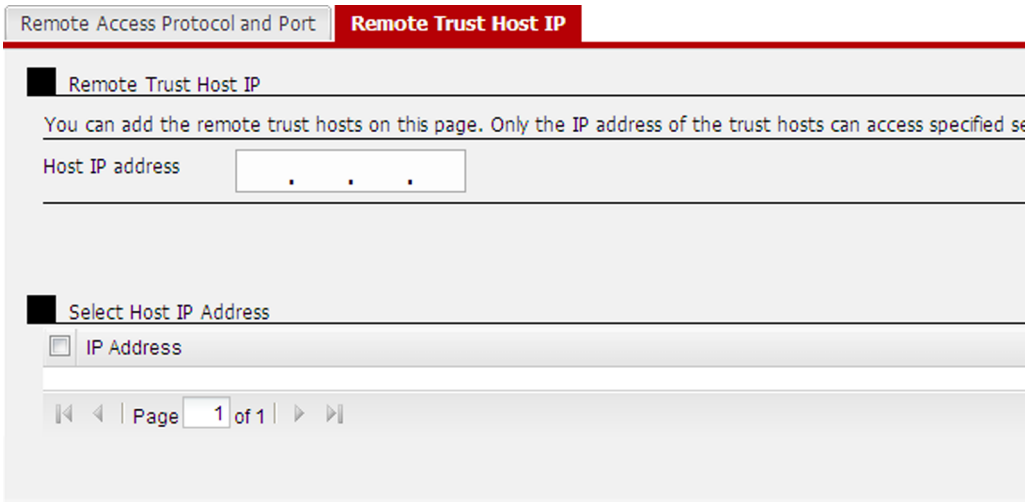
If you select **HTTPS**, run commands on the AR router to configure the SSL policy; otherwise, the HTTPS service does not take effect.

3. Click **OK** on the page shown in **Figure 16-29**.

Step 2 Configure the IP address of a trusted host.

1. Choose **Basic Settings** > **Remote Management** > **Remote Management** > **Remote Trust Host IP** to open the page shown in **Figure 16-30**.

Figure 16-30 Configuring a trusted host



2. Enter the IP address of the trusted host and click **Add**.

NOTE

If you do not specify a trusted host, all hosts can access the router through the WAN-side interface.

Figure 16-31 Configuring the trusted host

3. To delete a trusted host, select its IP address and click **Delete**.

----End

Copyright © Huawei Technologies Co., Ltd.

16.4 System Maintenance

System maintenance includes troubleshooting tool management and log management.

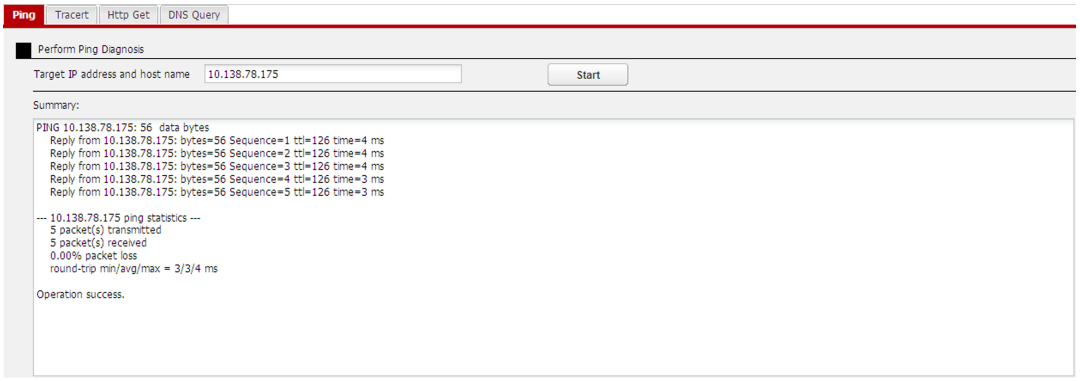
16.4.1 Locating Device Faults

When a network fault occurs, use troubleshooting tools to locate the fault. The router provides various troubleshooting tools, including ping, tracert, HTTP Get, and DNS query.

Procedure

- Perform a ping operation to check network connectivity and host reachability.
  1. Choose **Management** > **Troubleshooting Tool** > **Ping** to open the page shown in **Figure 16-32**.

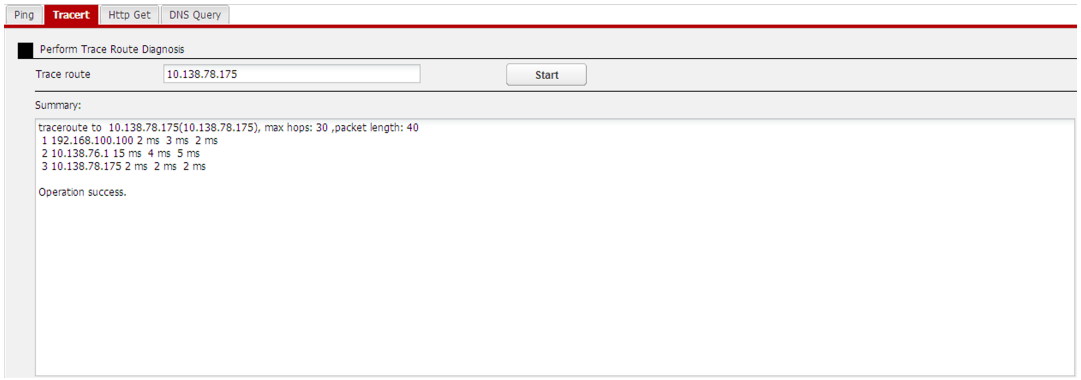
Figure 16-32 Ping



  2. Enter the destination IP address or host name in the **Target IP Address/Host Name** text box.
  3. Click **Start** to perform a ping operation. The diagnostic result is displayed in the **Summary** text box.
- Perform a tracert operation to test the gateways that packets pass through when traveling from the source host to the destination host.
  1. Choose **Management** > **Troubleshooting Tool** > **Tracert** to open the page shown in **Figure 16-33**.

Copyright © Huawei Technologies Co., Ltd.

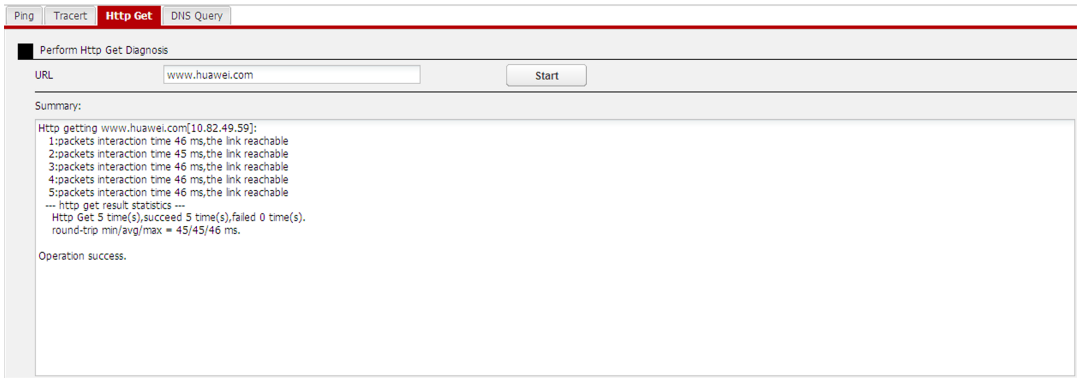
Figure 16-33 Tracert



2. Enter the destination IP address or host name in the **Trace Route** text box.
3. Click **Start** to perform a tracert operation. The diagnostic result is displayed in the **Summary** text box.

- Perform Http Get to check whether the URL is reachable.
  1. Choose **Management** > **Troubleshooting Tool** to open the page shown in **Figure 16-34**.

Figure 16-34 HTTP Get operation

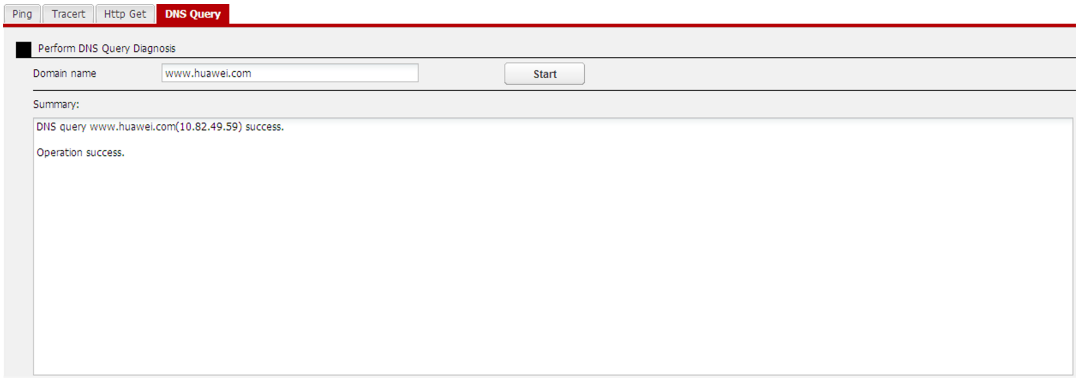


2. Enter the website address in the **URL** text box.
3. Click **Start** to perform an HTTP Get operation. The diagnostic result is displayed in the **Summary** text box.

- Perform DNS query to check whether the DNS server is reachable.
  1. Choose **Management** > **Troubleshooting Tool** to open the page shown in **Figure 16-35**.

Copyright © Huawei Technologies Co., Ltd.

Figure 16-35 DNS query operation



2. Enter the domain name in the **Domain name** text box.
3. Click **Start** to perform a DNS query operation. The diagnostic result is displayed in the **Summary** text box.

----End

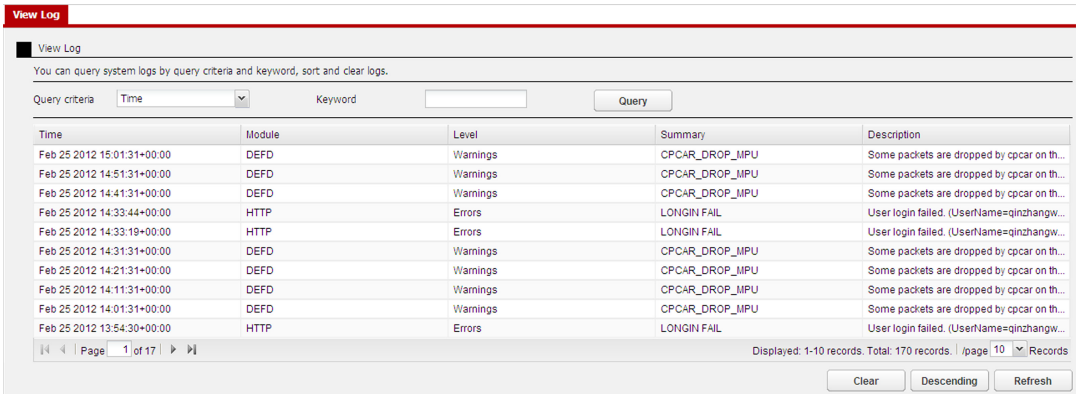
16.4.2 Log Management

This section describes how to view, query, refresh, and clear logs.

Procedure

- View logs.
  1. Choose **Management** > **Log Management**. The **Log Management** page is displayed, as shown in **Figure 16-36**.

Figure 16-36 Log information



2. Click **Ascending** or **Descending** to list logs in chronological order.

Copyright © Huawei Technologies Co., Ltd.

NOTE

The default display mode is **Ascending**.

- Ascending: Recent logs are displayed first.
- Descending: Recent logs are displayed at the end.

- Query logs.
  1. Select a query item from the **Query criteria** drop-down list box, as shown in **Figure 16-36**. Query criteria include time, module, level, summary, and description.

     Logs are displayed in time order by default.
  2. Enter the keyword in the **Keyword** text box. If **Time** is selected as the query item, enter the date in the **Keyword** text box.
  3. Click **Query**.
- Refresh logs.

  Click **Refresh** at the lower-right corner of **Figure 16-36**. The query results are refreshed.
- Clear logs.

  Click **Clear** at the lower-right corner of **Figure 16-36**. The system logs are cleared.

  NOTE

  Cleared logs cannot be restored. Perform this operation only when necessary.

----End

Copyright © Huawei Technologies Co., Ltd.

17 Configuration Examples

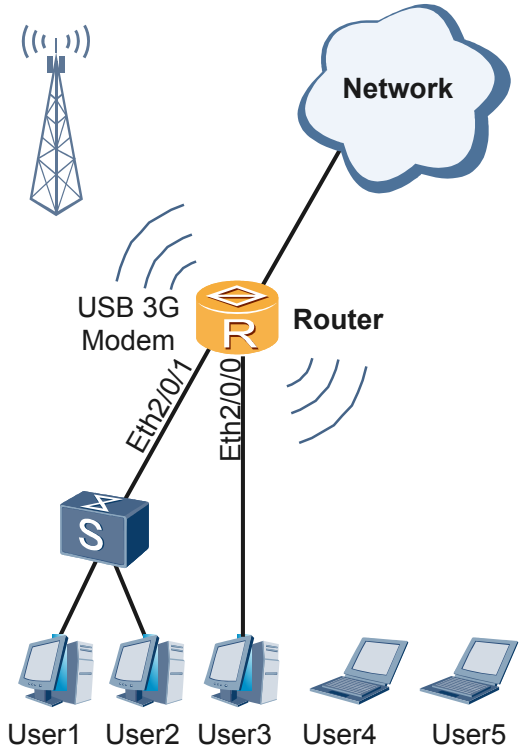
This section provides an example for configuring user access to a network.

Networking Requirements

As shown in **Figure 17-1**,

- The Router connects to the upstream network through a WAN-side interface GE0/0/0 and a USB 3G modem.
- Users can access the Router through a switch or wireless network or directly connect to the Router.
- Protection against ARP attacks is required on the LAN.

Figure 17-1 Networking diagram of user network access configuration



Copyright © Huawei Technologies Co., Ltd.

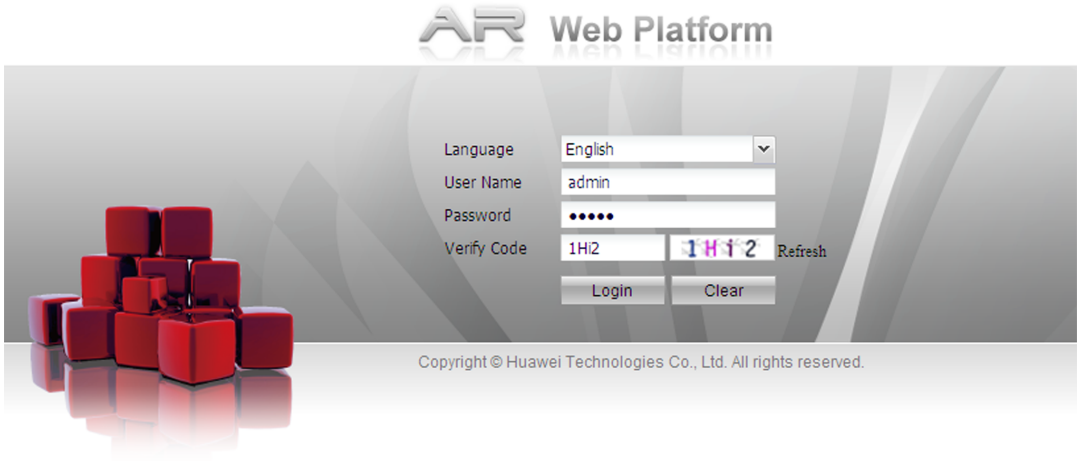
Configuration Roadmap

The configuration roadmap is as follows:

1. Connect the Router's interface GE0/0/0 to the upstream network in PPPoE mode, and connect the Router to a CDMA network through a USB 3G modem interface.
2. Enable the DHCP server function on the Router to allow it to assign IP addresses to hosts on the LAN.
3. Configure ARP mapping to protect against ARP attacks.

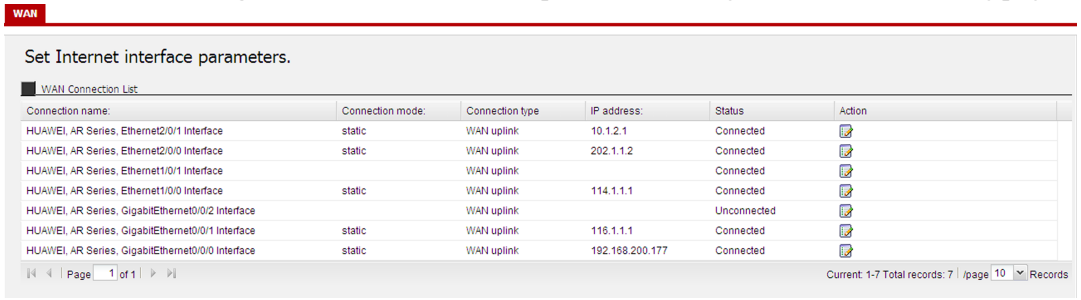
Procedure

Step 1 Start the web browser on a PC, enter website address http://192.168.1.1 in the address box, and press **Enter**. The following web login page is displayed.



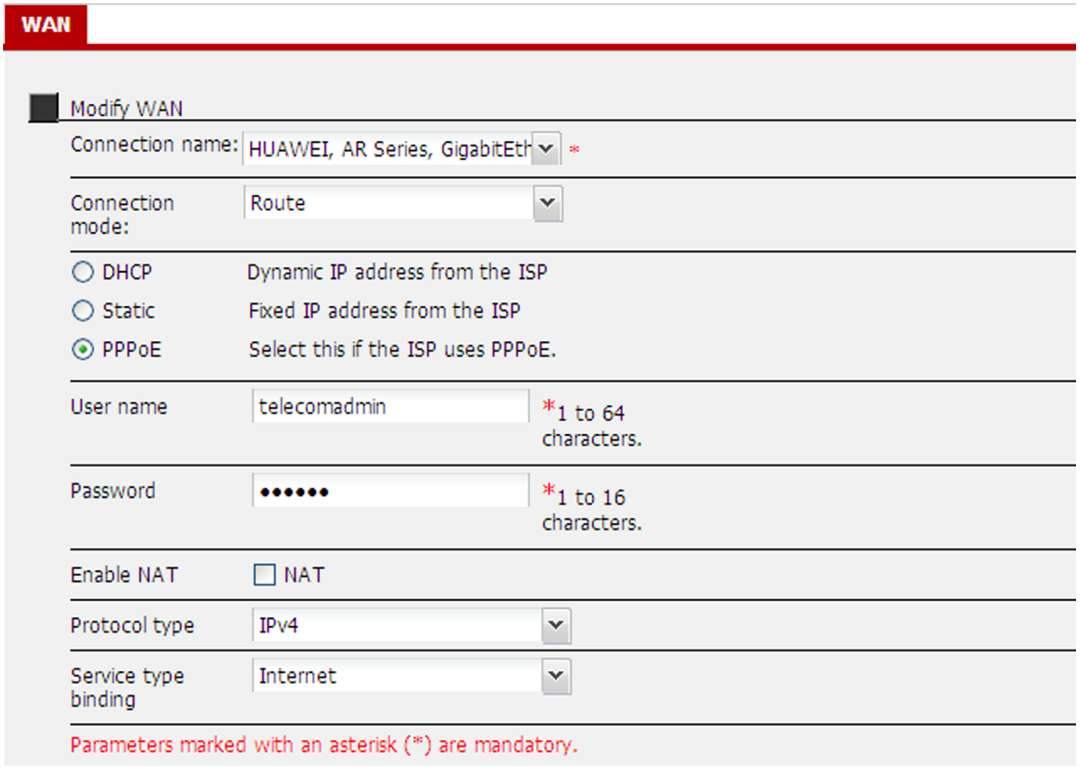
Step 2 Connect the Router's interface GE0/0/0 to the upstream network in PPPoE mode.

Choose **Basic Settings** > **Interface** > **WAN** to open the following WAN interface setting page.



Select GE0/0/0 and click . The following WAN setting page is displayed. Modify the parameters of the WAN interface and click **OK**.

Copyright © Huawei Technologies Co., Ltd.

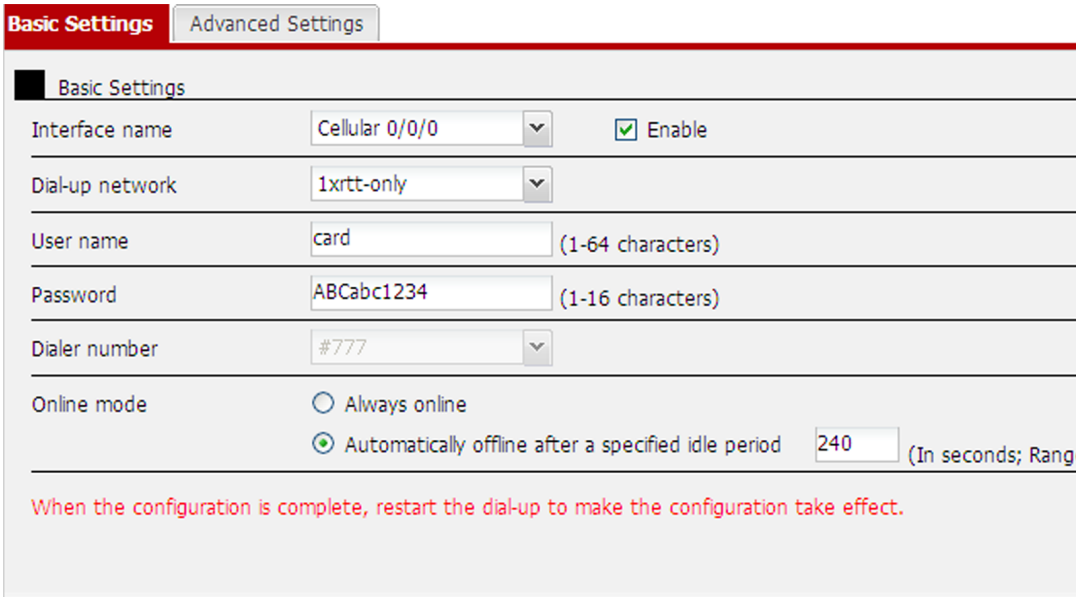


Step 3 Connect the Router to a CDMA network through a USB 3G modem interface.

Choose **Basic Settings** > **Interface** > **3G**. The following 3G interface setting page is displayed. Set 3G network parameters and click **OK**.

NOTE

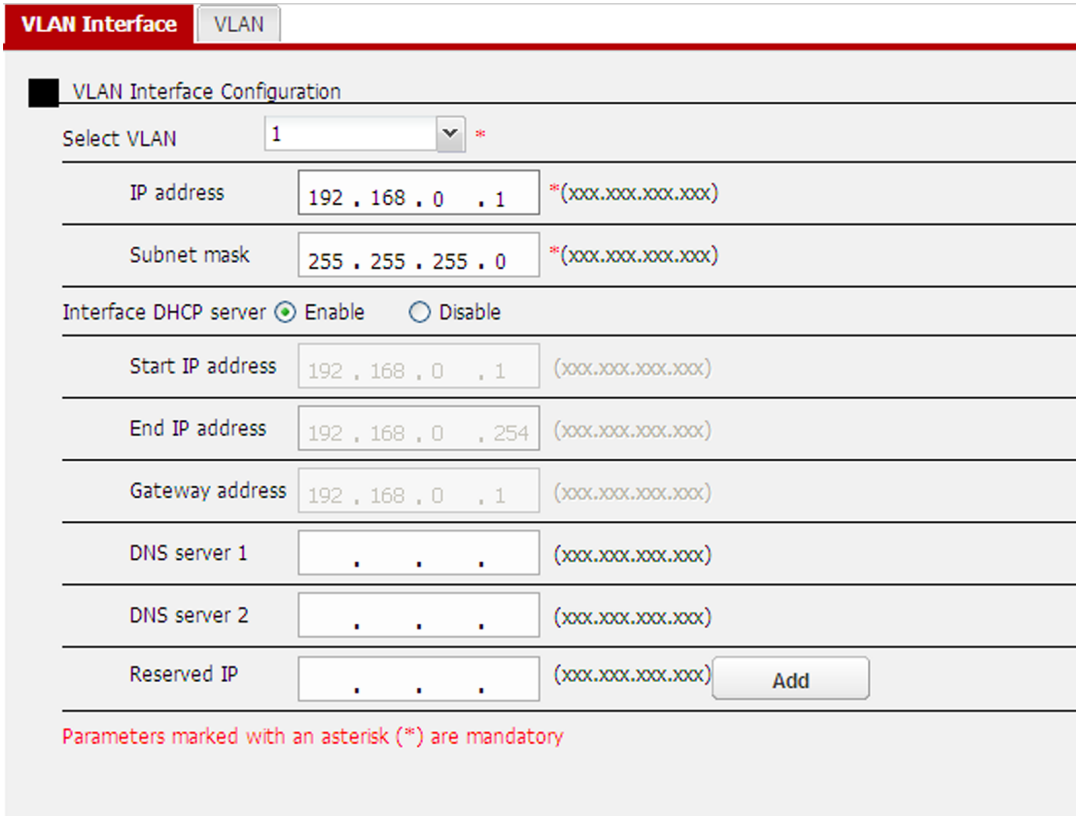
Ensure that the 3G modem has the UIM card installed.



Step 4 Enable the DHCP service on a VLANIF interface.

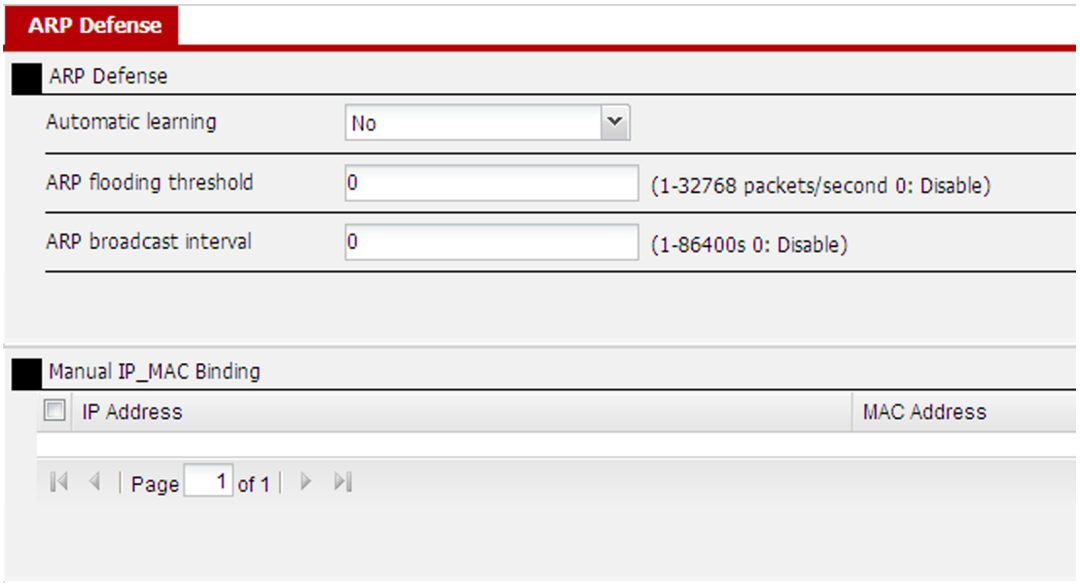
Choose **Basic Settings** > **Interface** > **LAN** > **VLAN Interface**. The following VLAN interface setting page is displayed. Set VLAN interface parameters and click **OK**.

Copyright © Huawei Technologies Co., Ltd.



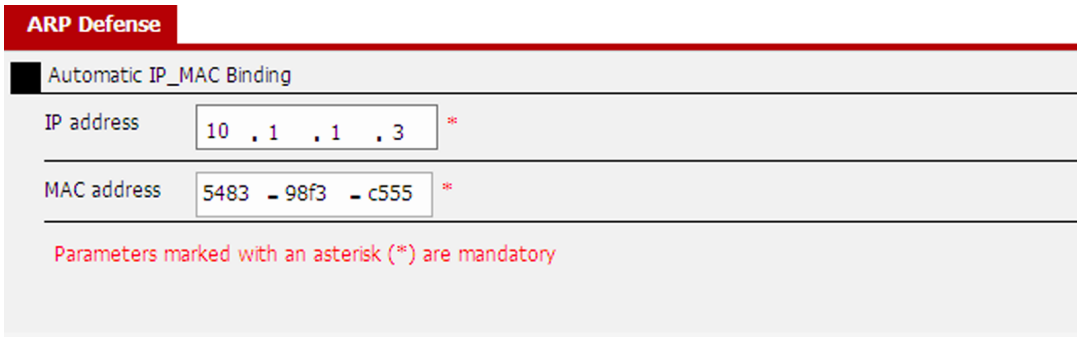
Step 5 Configure protection against ARP attacks on the LAN.

Choose **Security** > **Basic Settings** > **ARP Defense**. The following page is displayed. Click **New**.

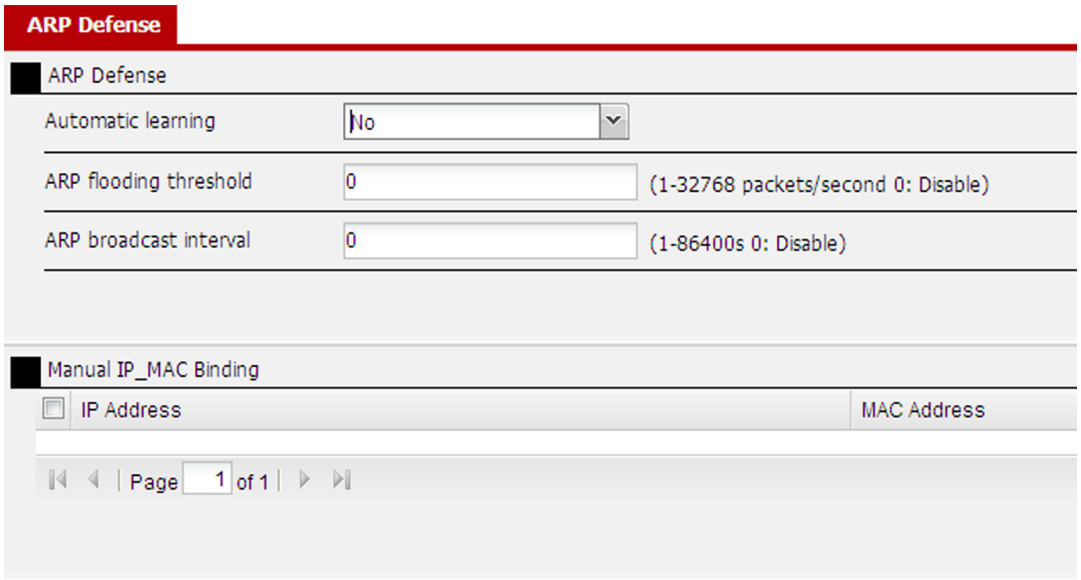


On the following page, specify the IP and MAC addresses and click **OK**.

Copyright © Huawei Technologies Co., Ltd.



Enable ARP mapping, set parameters, and click **OK**.



----End

Copyright © Huawei Technologies Co., Ltd.

18 Appendix A Fault Diagnosis

This section describes how to diagnose faults.

This section describes common fault diagnosis methods. If the fault persists, contact Huawei technical support personnel.

Quick Fault Identification

Table 18-1 Fault diagnosis

Fault	Troubleshooting
The power indicator is off.	1. Ensure that a correct power adapter is used. 2. Ensure that the power cable is connected properly. 3. Ensure that the power switch is on.
The WAN-side interface indicator is off.	1. Ensure that the interface is connected correctly. 2. Ensure that the physical connection of the interface is correct.
The LAN-side interface indicator is off.	1. Ensure that the type of the network cable between the router and PC is correct. 2. Ensure that the physical connection of the interface is correct. 3. Ensure that the PC's network interface card (NIC) indicator is on. 4. Ensure that the NIC is working properly. Check the device name below the network adapter in the equipment manager of the Windows operating system. If the device name is marked a question mark (?) or an exclamation mark (!), reinstall the NIC driver or insert the NIC to another slot. If the fault persists, change the NIC.

Copyright © Huawei Technologies Co., Ltd.

Fault	Troubleshooting
Failed to log in to the router on a web page.	1. Use the ping command to check the network connection: ● Ping IP address 127.0.0.1 to check whether the TCP/IP protocol has been installed. ● Ping the IP address of the router's LAN interface to check whether the PC is correctly connected to the router. 2. Run the **display ip interface** [*interface-type interface-number*] command to view the IP address of the router's LAN interface to check whether the input IP address is correct. 3. If the PC uses a static IP address, ensure that this IP address is on the same network segment as that of the router's LAN interface. 4. Check whether the number of existing users on the router exceeds the maximum value (5). If so, try later. 5. Check whether a proxy server or dialup connection is configured on the web browser. If so, delete such configuration.
Users on a LAN are forced offline and fail to access the Internet.	1. Ensure that the network cable of the switch connected to the router and the network cable of the router's WAN interface are securely connected. 2. Ensure that IP and MAC addresses of all hosts on the LAN are bound in ARP mappings.

Copyright © Huawei Technologies Co., Ltd.

19 Appendix B Device Default Settings

This section describes the router's default settings.

Table 19-1 lists the router's default settings.

Table 19-1 Default settings

Item			Default Settings
Interface		VLANIF Interface IP Address	None. **NOTE** By default, LAN ports of AR150 and AR200 series are added to VLAN 1. The IP address of VLANIF 1 is 192.168.1.1, and subnet mask is 255.255.255.0.
		LAN Interface Parameter	Default VLAN: VLAN 1 Link type: hybrid Interface DHCP server: Disable
		3G	MTU: 1500
Network		Virtual Server	Protocol type: TCP External address: Interface IP address
		DHCP	VLAN: default(1) MTU: 1500 DHCP based on the global address pool: enable
VPN	L2TP VPN	L2TP Client	Enable
	IPSec VPN	IKE version	V1
		Exchange mode	Master
		Peer ID type	IP Address

Copyright © Huawei Technologies Co., Ltd.

Item			Default Settings
		Local ID type	IP Address
		Authentication algorithm	SHA1
		Encryption algorithm	DES
		DH	Diffie-Hellman Group1
		Protocol	ESP
		ESP authentication algorithm	MD5
		ESP encryption algorithm	DES
		PFS	None
	SSL VPN	Local Authentication	Enable local authentication
Security		ARP Defense	Disable
		Firewall	Disable
		MAC Address Filtering	Disable
Management		Set System Time	Automatic synchronization
Remote Management		SNMP version	SNMP v3
		Telnet	Enable
		HTTP	Enable

Copyright © Huawei Technologies Co., Ltd.