

**Huawei OptiXstar K572  
V500R024C00**

# **Web Page Reference**

**Issue**            01  
**Date**             2024-12-06



**Copyright © Huawei Technologies Co., Ltd. 2024. 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**



HUAWEI 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 a warranty of any kind, express or implied.

## **Huawei Technologies Co., Ltd.**

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





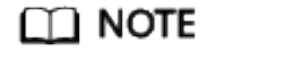
Website: <https://www.huawei.com>

Email: [support@huawei.com](mailto:support@huawei.com)

# Symbol Conventions

## Symbol Conventions

The following symbols may be found in this document. They are defined as follows:

Symbol	Description
	Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
	Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
	Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury.
	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.
	Calls attention to important information, best practices and tips. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.

---

# Change History

## Change History

Issue	Date	Description
01	2024-11-25	This is the first official release.

---

# Contents

---

<b>Symbol Conventions.....</b>	<b>ii</b>
<b>Change History.....</b>	<b>iii</b>
<b>1 Locally Logging in to the Web Interface.....</b>	<b>1</b>
<b>2 Internet Guide.....</b>	<b>5</b>
<b>3 Web Page Reference (Route mode).....</b>	<b>13</b>
3.1 Homepage.....	13
3.2 Internet Access.....	14
3.3 My Wi-Fi.....	15
3.4 Terminal.....	18
3.5 More.....	19
3.5.1 System Information.....	19
3.5.1.1 Device Information.....	19
3.5.1.2 WAN Information.....	20
3.5.1.3 WLAN Information.....	21
3.5.1.4 Home Network Information.....	23
3.5.2 WLAN.....	24
3.5.2.1 Wi-Fi Advanced Configuration.....	24
3.5.2.2 Wi-Fi Coverage Management.....	26
3.5.2.3 MLO Advanced Network.....	30
3.5.2.4 Automatic Wi-Fi Shutdown.....	32
3.5.2.5 Multi-AP Role Settings.....	33
3.5.3 Network Configuration.....	33
3.5.3.1 LAN Settings.....	33
3.5.3.2 IPv6.....	35
3.5.3.3 DDNS Function.....	36
3.5.3.4 UPnP Function.....	38
3.5.4 Security Configuration.....	39
3.5.4.1 Wi-Fi MAC Address Filtering Configuration.....	39
3.5.4.2 Firewall Configuration.....	40
3.5.4.3 Parental Control.....	40
3.5.4.4 DMZ Function.....	41
3.5.4.5 IPv4 Port Mapping.....	42

3.5.4.6 Port Trigger Configuration.....	45
3.5.4.7 Device Access Control.....	47
3.5.4.8 PSK Crack Defense.....	48
3.5.5 System Management.....	48
3.5.5.1 Upstream Network Port Settings.....	48
3.5.5.2 TR-069.....	49
3.5.5.3 SP Management Platform.....	53
3.5.5.4 Software Upgrade.....	54
3.5.5.5 Account Management.....	54
3.5.5.6 Time Setting.....	55
3.5.5.7 Backup and Recovery.....	57
3.5.5.8 Open Source Software Notice.....	57
3.5.5.9 Indicator Status Management.....	58
3.5.5.10 Security Self-Check.....	59
3.5.6 Maintenance Diagnosis.....	59
3.5.6.1 Maintenance.....	59
3.5.6.2 User Log.....	61
3.5.6.3 AP Log.....	62
3.5.6.4 Firewall Log.....	62
3.5.6.5 Debug Log.....	63
3.5.6.6 Intrusion Detect Log.....	64
3.5.6.7 Fault Info Collect.....	65
3.5.6.8 Remote Mirror.....	66
<b>4 Web Page Reference (Bridge mode).....</b>	<b>68</b>
4.1 Homepage.....	68
4.2 My Wi-Fi.....	69
4.3 More.....	70
4.3.1 System Information.....	70
4.3.1.1 Device Information.....	70
4.3.1.2 WLAN Information.....	71
4.3.2 WLAN.....	74
4.3.2.1 Wi-Fi Advanced Configuration.....	74
4.3.2.2 Smart Network Connection.....	76
4.3.2.3 Wi-Fi Repeater.....	76
4.3.2.4 Multi-AP.....	77
4.3.3 Security Configuration.....	78
4.3.3.1 Device Access Control.....	78
4.3.4 System Management.....	79
4.3.4.1 Upstream Network Port Settings.....	79
4.3.4.2 TR-069.....	80
4.3.4.3 Software Upgrade.....	84
4.3.4.4 Account Management.....	84

---

4.3.4.5 Time Setting.....	85
4.3.4.6 Backup and Recovery.....	87
4.3.4.7 Open Source Software Notice.....	87
4.3.4.8 Indicator Status Management.....	88
4.3.4.9 Security Self-Check.....	89
4.3.5 Maintenance Diagnosis.....	89
4.3.5.1 Maintenance.....	89
4.3.5.2 User Log.....	90
4.3.5.3 AP Log.....	91
4.3.5.4 Debug Log.....	92
4.3.5.5 Fault Info Collect.....	92

# 1 Locally Logging in to the Web Interface

---

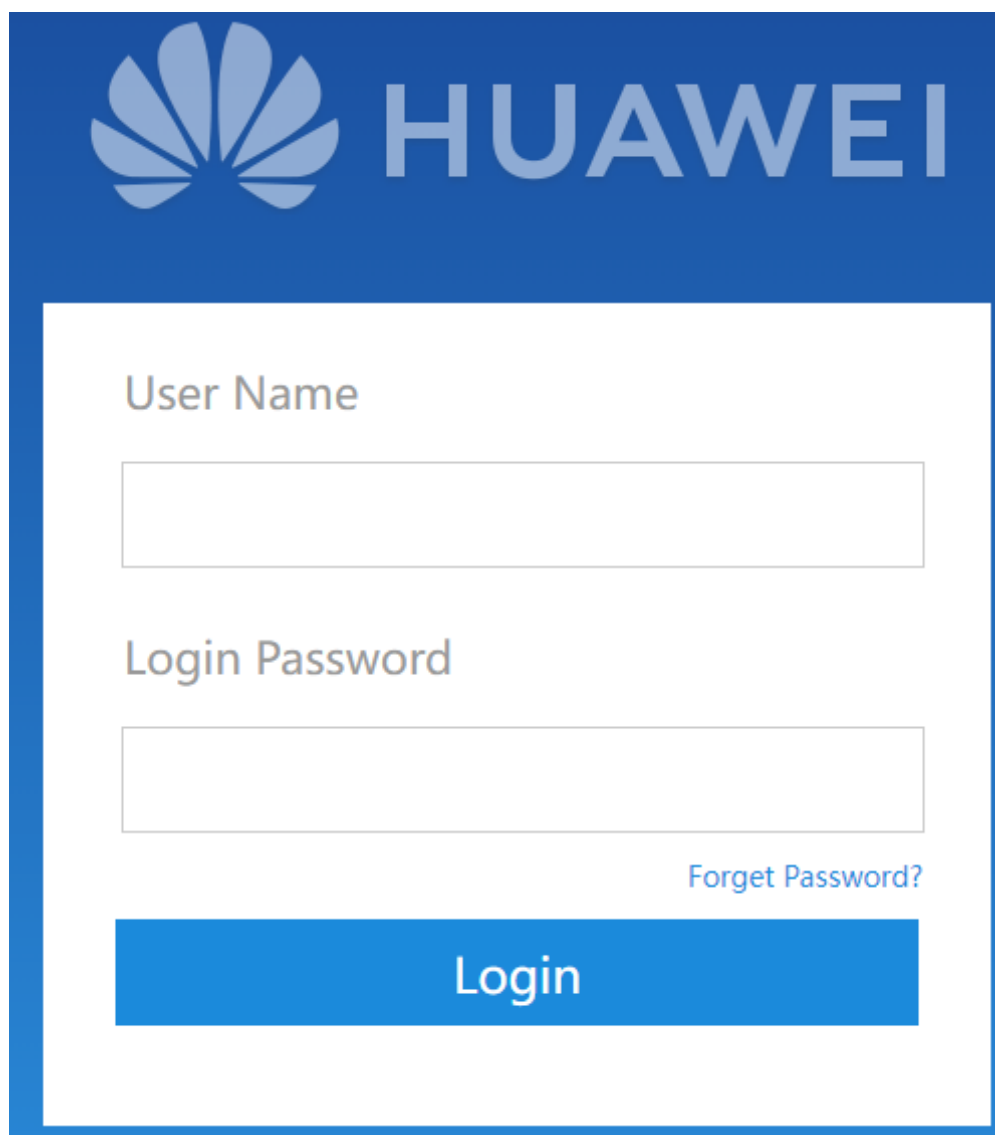
This topic describes the procedure for logging in to the web configuration interface.

## Wireless login

1. Connect a phone or PC to the Wi-Fi of the edge ONT. For the Wi-Fi name and password, see the SSID and WLAN Key on the device nameplate.
2. Open the browser. The configuration page is automatically displayed.



**Figure 1-1** Web configuration interface



The image shows the Huawei web configuration interface. At the top, there is a blue header with the Huawei logo and the word "HUAWEI" in white. Below the header, there is a white login form with a blue border. The form contains two input fields: "User Name" and "Login Password". Below the "Login Password" field, there is a blue link that says "Forget Password?". At the bottom of the form, there is a large blue button with the word "Login" in white text.

**NOTE**

- Some mobile phones automatically display the configuration page following the Wi-Fi connection page.
- If the configuration page is not automatically displayed, enter the IP address in the address box of a browser. (For details about the IP address, see the product nameplate.)
- To enhance system security, change the password to a password that meets security requirements after the first successful login. It is recommended that you change the password periodically.

## Wired login

- **Data plan**

Before setting up the configuration environment, ensure that data information listed in [Table 1-1](#) is available.

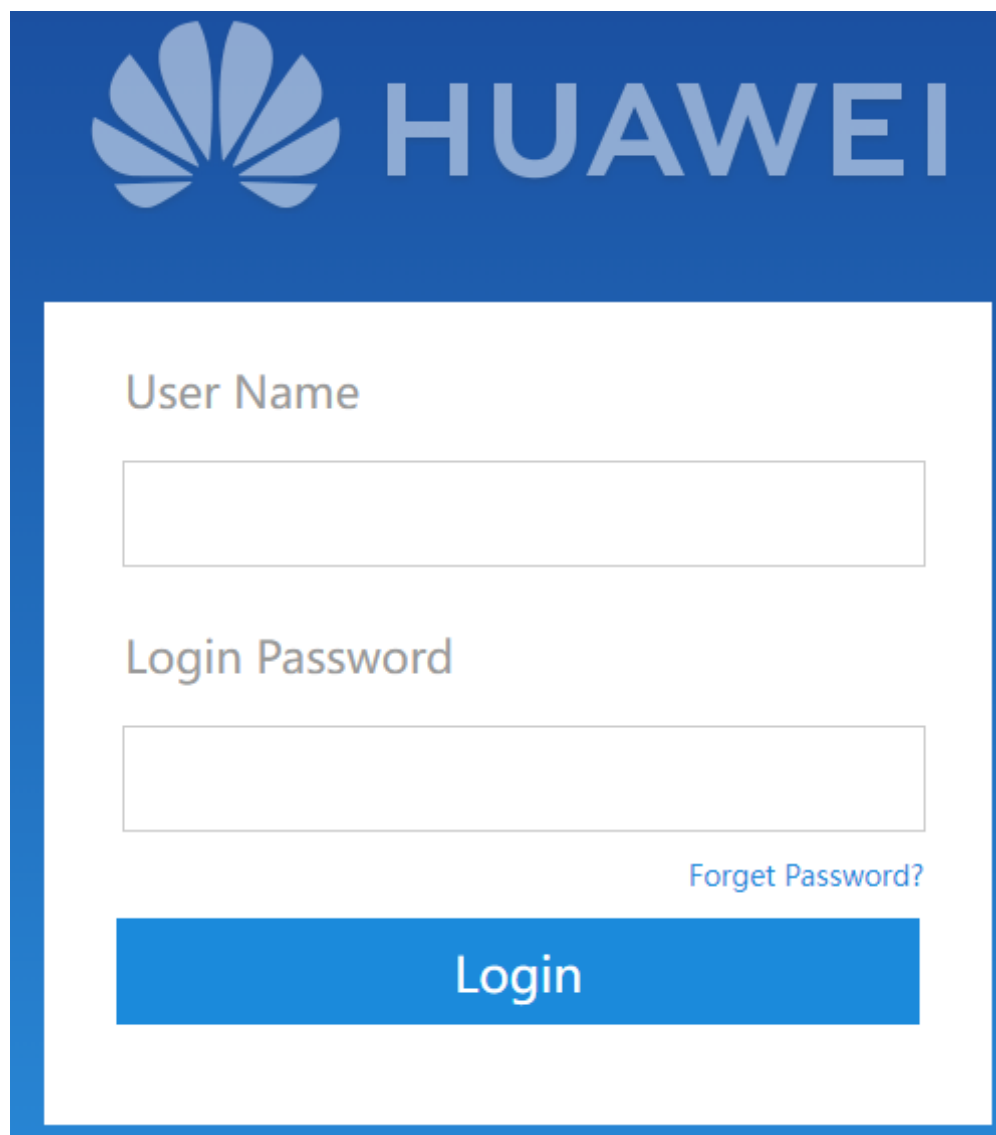
**Table 1-1** Data plan

Item	Description
LAN IP address and subnet mask of the edge ONT	Default settings: <ul style="list-style-type: none"><li data-bbox="746 387 1098 421">● IP address: 192.168.101.1</li><li data-bbox="746 430 1139 463">● Subnet mask: 255.255.255.0</li></ul>
IP address and subnet mask of the PC	Configure the IP address of the PC to be in the same subnet as the LAN IP address of the edge ONT. For example: <ul style="list-style-type: none"><li data-bbox="746 607 1134 640">● IP address: 192.168.101.100</li><li data-bbox="746 649 1139 683">● Subnet mask: 255.255.255.0</li></ul>

- **Procedure**

1. Use a network cable to connect the network port of the edge ONT to a PC.
2. Ensure that the browser on the computer does not use a proxy server. The procedure is as follows:
  - a. Open **Control Panel** and choose **Internet Options**.
  - b. In the **Internet Options** interface, click the **Connections** tab, and then click **LAN settings**.
  - c. In the **Proxy server** area, ensure that the **Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections)** check box is not selected (that is, without the "√" sign). If the check box is selected, deselect it, and then click **OK**.
3. Set the IP address and subnet mask of the PC. For details, see [Table 1-1](#).
4. Enter `http://192.168.101.1` in the address bar of the browser (192.168.101.1 is the default IP address of the edge ONT), and then press **Enter** to display the web configuration interface, as shown in [Figure 1-2](#).

Figure 1-2 Web configuration interface



The image shows a web configuration interface for Huawei. At the top, there is a blue header with the Huawei logo and the word "HUAWEI" in white. Below the header, there is a white login form with a blue border. The form contains two input fields: "User Name" and "Login Password". Below the "Login Password" field, there is a blue link labeled "Forget Password?". At the bottom of the form, there is a large blue button labeled "Login".

 NOTE

- The web interfaces in this document may differ from the actual interfaces. The actual interfaces prevail.
- The web page login supports SSL3.0, TLS1.0, TLS1.1, and TLS1.2. It is recommended that you use high-security TLS1.1 or TLS1.2 if you log in to the edge ONT using https. The TCP port 80 is used for listening for HTTPS packets. You need to type "https://192.168.101.1:80" in the address bar of IE and press **Enter** to log in to the edge ONT.
- To enhance system security, change the password to a password that meets security requirements after the first successful login. It is recommended that you change the password periodically.
- You are advised to use the latest browser to log in to the web configuration page. Chrome 58/Edge 14/Firefox 54/Safari 10/Opera 55 or later is recommended. If the browser of an earlier version is used, compatibility issues may occur.

# 2 Internet Guide


1. After logging into the edge ONT, the edge ONT will automatically detect your Internet access mode.
2. Configure the Internet access based on the detection result.
  - If the detected Internet access mode is automatic IP address obtaining, go to step 3.
  - If the detected Internet access mode is dial-up access, enter the broadband account and password, and click **Next**. Then go to step 3.

Internet Guide

Your Internet access mode is

PPPoE     DHCP     Static     Wi-Fi Uplink

Broadband Account

Broadband Password  

Next

 **NOTE**

- If you forget the broadband account and password, contact your ISP to retrieve the account and password.
  - To enhance system security, change the password to a password that meets security requirements after the first successful login. It is recommended that you change the password periodically.
- No drop cable is detected.



- If you click **Re-check**, the device checks the Internet access mode again.
  - If you click **Wi-Fi Uplink**, the Internet access mode is set to Wi-Fi uplink, and the operation in step 4 is required.
  - If you click **continue the configuration without inserting the network cable**, you need to manually select an Internet access mode. If you set the mode to dial-up access or automatic IP address obtaining, the interface in step 3 is displayed. If you set the mode to the Wi-Fi uplink, the interface in step 4 is displayed.
3. Select an **Area** as instructed by your service provider, the **Server address** field is automatically populated after you select an **Area**. You can also manually enter a **Server address**. Then select the privacy statement, and click **Apply** to enable the function of service provider remote management. You can also click **Skip**, and configure this option on the **SP Management Platform** page later.

**Figure 2-1** Service Provider Remote Management Platform

The screenshot shows a configuration page titled "Service Provider Remote Management Platform". It features a dropdown menu for "Area" and a text input field for "Server address". Below these fields is a note: "Select an option as instructed by your service provider. If the selection is incorrect, the remote software upgrade function of the device will be unavailable." At the bottom, there is a checked checkbox with the text "I know that the service provider remote management platform collects device data to the server address and understand the protocols, contracts, and privacy policies of network service provider." Two blue buttons, "Skip" and "Apply", are positioned at the bottom of the form.

4. Set a new Wi-Fi SSID and management password of the edge ONT. Click **Next**. The interface in step 6 is displayed.
  - Enable Dual-Band Steering

The screenshot shows a configuration page titled "Set your Wi-Fi name and password." It features a "Dual-Band Steering" toggle switch which is turned on. Below the toggle is a note: "If the 2.4 GHz and 5G Wi-Fi frequency bands are used together, the device automatically selects a faster Wi-Fi frequency band. If this switch is turned off, the Wi-Fi frequency band can be set manually." There are two input fields: "Wi-Fi Name" with the value "2.4GSSID111" and "Wi-Fi Password" with masked characters and a visibility icon. A note below the password field reads: "To ensure network security, keep your password safe." Two blue buttons, "Next" and "Skip", are positioned at the bottom of the form.

- Disable Dual-Band Steering


**Set your Wi-Fi name and password.**

Dual-Band Steering

If the 2.4 GHz and 5G Wi-Fi frequency bands are used together, the device automatically selects a faster Wi-Fi frequency band. If this switch is turned off, the Wi-Fi frequency band can be set manually.

Wi-Fi Name

5G Wi-Fi Name

Wi-Fi Password  

To ensure network security, keep your password safe.

**NOTICE**

To enhance system security, change the password to a password that meets security requirements after the first successful login. It is recommended that you change the password periodically.







Parameter	Description
Dual-Band Steering	If the 2.4G Wi-Fi and 5G Wi-Fi frequency bands are used together, the device automatically selects a faster Wi-Fi frequency band. If this switch is turned off, the Wi-Fi frequency band can be set manually.
Wi-Fi Name	Wi-Fi name of dual-band Wi-Fi (dual-band steering is enabled). 2.4G Wi-Fi name (dual-band steering is disabled).
5G Wi-Fi Name	5G Wi-Fi name.
Wi-Fi Password	Wi-Fi Password.

5. Select the Wi-Fi name to be connected, enter the Wi-Fi password, and click **Next**.


**Your Internet access mode is**

PPPoE     DHCP     Static     Wi-Fi Uplink

Select the Wi-Fi to be connected Re-scan

WPA2-EAP	
WPA2-EAP	
OPEN	
WPA/WPA2-PSK	
WPA/WPA2-PSK	
WPA/WPA2-PSK	


Wi-Fi Name

Wi-Fi Password  

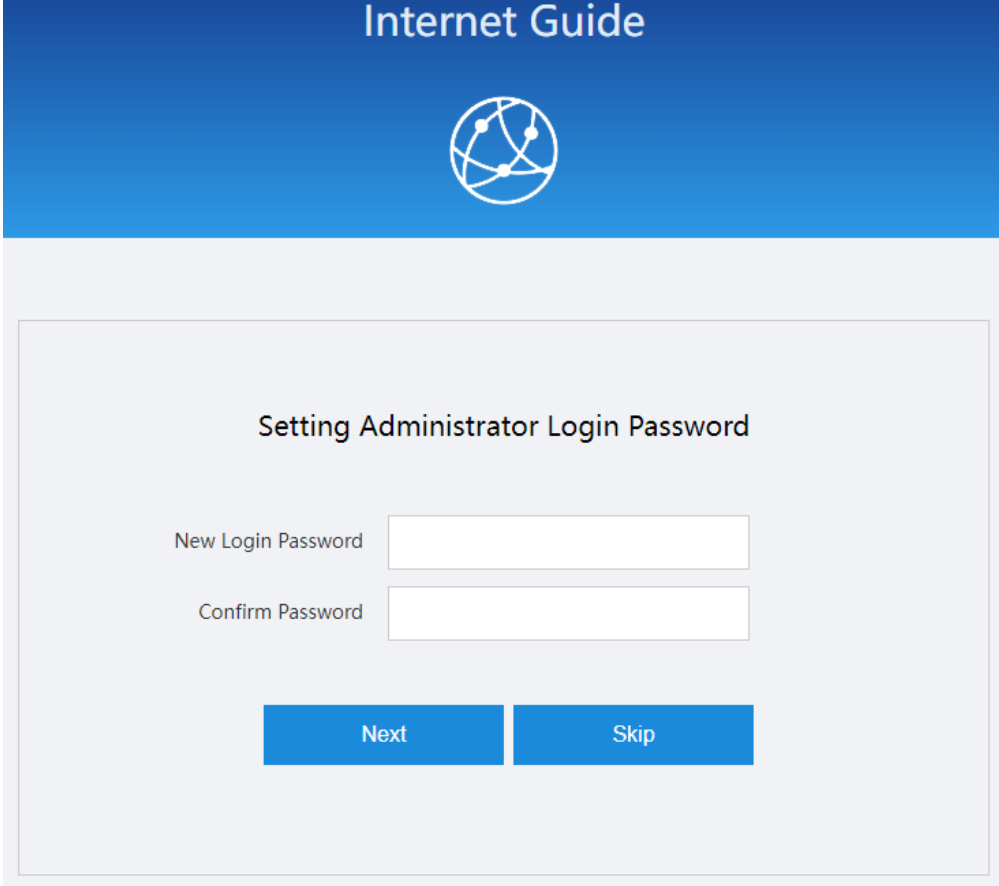
After the connection is set up, the Wi-Fi name and password of the local repeater are the same as those of the active router.

 **NOTE**

-  Indicates that the Wi-Fi of the gateway supports the one-click pairing.
- Set the administrator login password. Click **Next**.





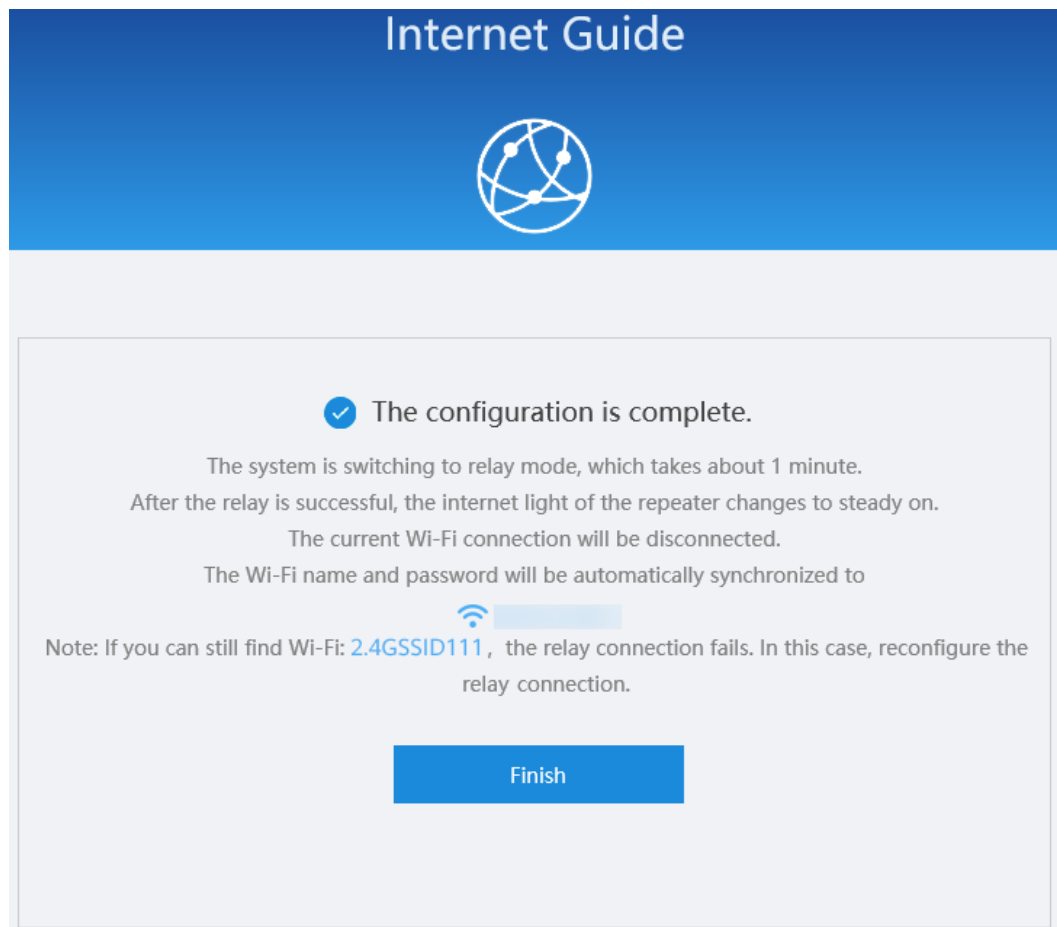
The screenshot shows a web interface titled "Internet Guide" with a blue header and a white network icon. The main content area is titled "Setting Administrator Login Password" and contains two input fields: "New Login Password" and "Confirm Password". Below the fields are two blue buttons labeled "Next" and "Skip".

 **NOTE**

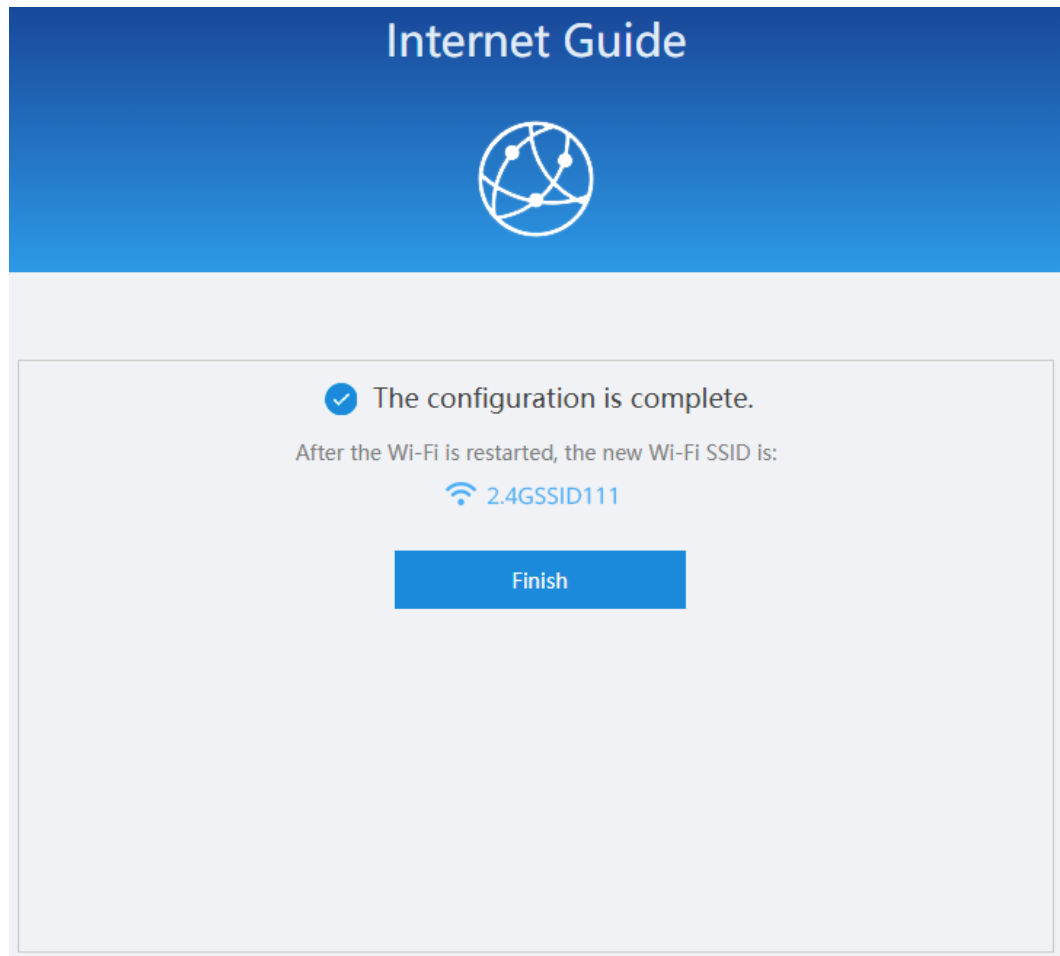
The device automatically checks whether the Wi-Fi upstream transmission is successfully configured.

7. The configuration is complete, reconnect to Wi-Fi.

**Figure 2-2** The configuration is complete-Wi-Fi relay



**Figure 2-3** The configuration is complete-route mode



# 3 Web Page Reference (Route mode)

## 3.1 Homepage

- On the homepage, you can view the home network connection status, Internet access mode, system running duration, and local IP address.
- A click on the icon of a device displays the details about a connected device and allows management on the connected device. For details, see [3.4 Terminal](#).




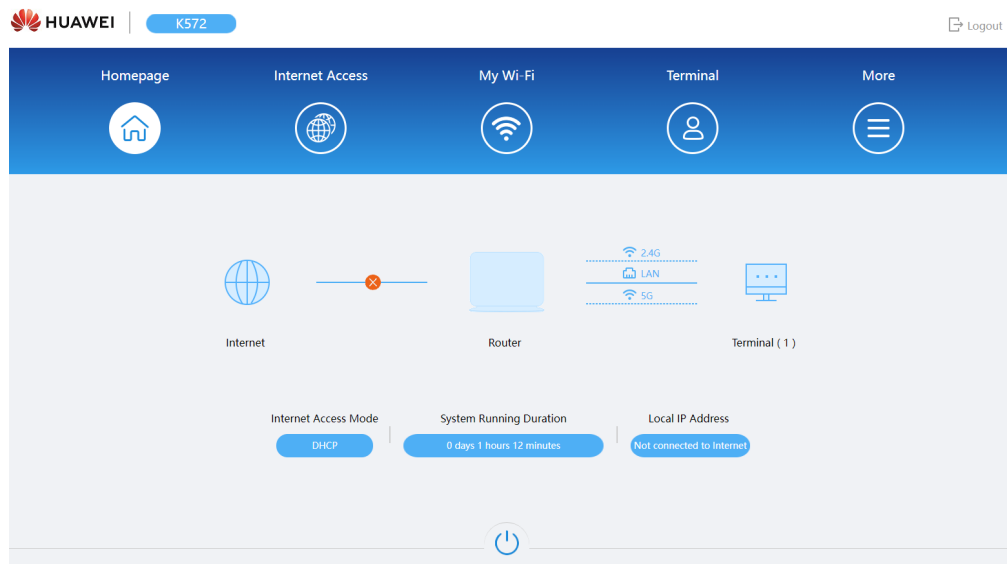
- A click on  restarts the edge ONT.

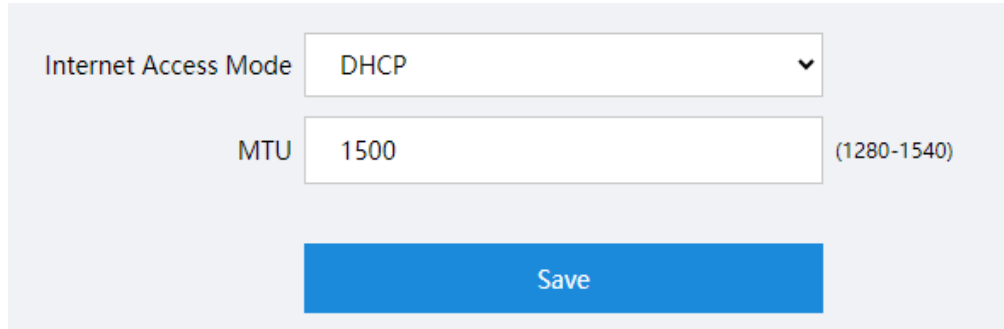
Figure 3-1 Homepage



## 3.2 Internet Access

On this page, you can set an Internet access mode of the edge ONT. There are three Internet access modes:

- Automatic IP address obtaining (DHCP)

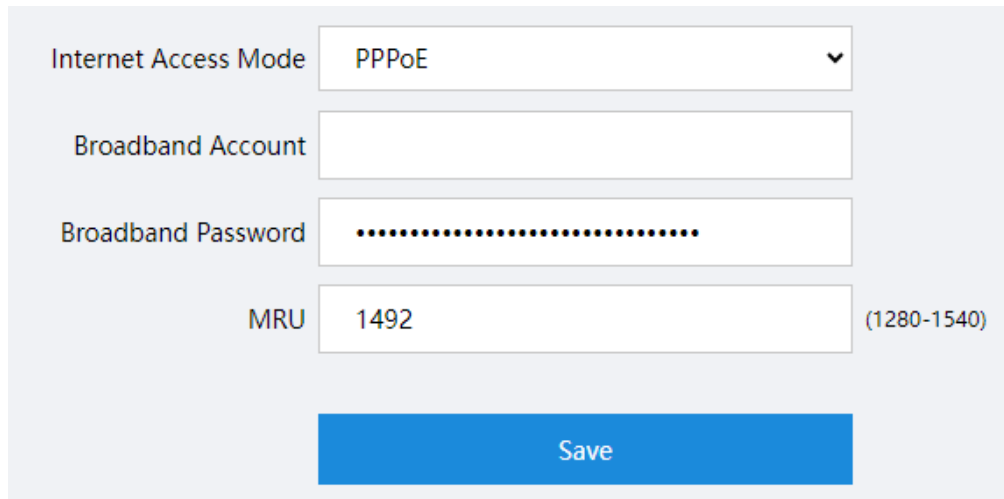


Internet Access Mode: DHCP

MTU: 1500 (1280-1540)

Save

- PPPoE



Internet Access Mode: PPPoE

Broadband Account: [Empty]

Broadband Password: [Masked]

MRU: 1492 (1280-1540)

Save

### NOTE

- If you forget the broadband account and password, contact your ISP to retrieve the account and password.
- To enhance system security, change the password to a password that meets security requirements after the first successful login. It is recommended that you change the password periodically.
- Manual IP address input (static IP address): Enter the information provided by the operator during the subscription to the broadband service, including the fixed IP address, subnet mask, default gateway, primary DNS server IP address, and secondary DNS server IP address.

Internet Access Mode: Static IP address

IP Address \*

Subnet Mask \*

Default Gateway

Primary DNS Server

Secondary DNS Server

MTU: 1500 (1280-1540)

Save

### 3.3 My Wi-Fi

On this page, you can configure Wi-Fi parameters.

- Enable Dual-Band Combination

Dual-Band Steering

If the 2.4 GHz and 5G Wi-Fi frequency bands are used together, the device automatically selects a faster Wi-Fi frequency band. If this switch is turned off, the Wi-Fi frequency band can be set manually

Wi-Fi

Wi-Fi Name

Encrypt

Wi-Fi Password

Wi-Fi Power Mode

- Disable Dual-Band Combination

**Dual-Band Steering**

If the 2.4 GHz and 5G Wi-Fi frequency bands are used together, the device automatically selects a faster Wi-Fi frequency band. If this switch is turned off, the Wi-Fi frequency band can be set manually

**2.4G Wi-Fi**

Wi-Fi Name

Encrypt

Wi-Fi Password

**5G Wi-Fi**

Wi-Fi Name

Encrypt

Wi-Fi Password

Wi-Fi Power Mode

**Apply**

**NOTICE**

To enhance system security, change the password to a password that meets security requirements after the first successful login. It is recommended that you change the password periodically.



**Table 3-1** Wi-Fi parameters

Parameter	Description
Dual-Band Steering	If the 2.4G Wi-Fi and 5G Wi-Fi frequency bands are used together, the device automatically selects a faster Wi-Fi frequency band. If this switch is turned off, the Wi-Fi frequency band can be set manually.
Wi-Fi/2.4G Wi-Fi/5G Wi-Fi	Enable or disable Wi-Fi.
Wi-Fi Name	Wi-Fi name.
Encrypt	Indicates the authentication mode for the STA to request access to the wireless network. The mode can be OPEN, WPA2-PSK, WPA/WPA2-PSK. It is set to WPA/WPA2-PSK by default.
Wi-Fi Password	Wi-Fi password.
Wi-Fi Power Mode	The mode can be set to the following as required: <ul style="list-style-type: none"> <li>Through-wall (high power, better signal)</li> <li>Standard (standard power, common signal)</li> <li>Sleep (low power, weak signal)</li> </ul>

## 3.4 Terminal

On this page, you can view details about devices connected to the edge ONT and perform operations on the connected devices.

- A click on **Details** displays details about connected devices.
- A click on **Add to Blacklist** blacklists the device. A blacklisted device is not allowed to connect to the edge ONT.

**Figure 3-2** Terminal

Currently in list mode, click to switch to Topo chart mode

Device Name	MAC Address	IP Address	Device Status	Connection Duration	Operations
--	84:a9:3e:8a	192.168.101.100	Online	0 hour 9 minutes	<a href="#">Details</a> <a href="#">Add to Blacklist</a>

**Figure 3-3** User Device Information

User Device Information	
On this page, you can query the details about the user device, including the host name, device type, IP address, MAC address, device status, port type, port ID, online and offline duration, IP acquisition mode, and remaining lease time.	
Host Name:	--
Device Type:	--
IP Address:	192.168.101.100
MAC Address:	00:e0:4c:9a: [obscured]
Device Status:	Online
Online Duration:	1 hour 1 minute
Port Type:	ETH
Port ID:	LAN1
NegotiationRate:	1000 Mbps
IP Acquisition Mode:	Static
Remaining Lease Time:	--

## 3.5 More

A click on **More** displays the page for configuring more functions.

### 3.5.1 System Information

This topic describes the basic information about an edge ONT on the web page, including the device, WLAN and Home Network information.

#### 3.5.1.1 Device Information

In the navigation tree on the left, choose **System Info > Device Information**. In the pane on the right, you can view the product name, hardware version, and software version, as shown in [Figure 3-4](#).

**Figure 3-4** Device Information

### Device Information

On this page, you can view basic device information.

#### Basic Information

Device Type:	K572
Description:	OptiXstar K572 GE Terminal (PRODUCT ID: [REDACTED])
MAC:	00:25:9E:[REDACTED]
Hardware Version:	[REDACTED]
Software Version:	V5R024 [REDACTED]
Manufacture Info:	[REDACTED]
CPU Usage:	2%
Memory Usage:	64%
Custom Info:	[REDACTED]
System Time:	[REDACTED]

Refresh

#### Secure Boot Settings

Secure Boot:	Enable
Hash Value of Level-1 BIOS:	[REDACTED]
Hash Value of Level-2 BIOS:	[REDACTED]
Firmware Package Signature Result:	<input type="button" value="Download"/>

### 3.5.1.2 WAN Information

In the navigation tree on the left, choose **System Info > WAN Information**. Then, in the pane on the right, you can view the WAN information such as the status of the WAN interface, as shown in [Figure 3-5](#).

**Figure 3-5** WAN Information

### WAN Information

On this page, you can query the connection and line status of the WAN port.

IPv4 Information (Click any table cell for details)

WAN Name	Status	IP Address	VLAN/Priority	Connect
1_TR069_IPTV_INTERNET_R_VID_	Disconnected	--	-/-	Always On

### WAN Port Status Information

WAN Name	Status	Receive (RX)		Transmit (TX)	
	Link	Bytes	Packets	Bytes	Packets
1_TR069_IPTV_INTERNET_R_VID_	Disconnected	0	0	0	0

## 3.5.1.3 WLAN Information

In the navigation tree on the left, choose **System Info > WLAN Information**. Then, in the pane on the right, you can query the information such as WLAN status, Wi-Fi packet statistics, and STA information, as shown in **Figure 3-6**.

**Figure 3-6** WLAN Information

### WLAN Information

On this page, you can query the WLAN information, WLAN packet statistics, and SSID information.

2.4 GHz wireless network information       5 GHz wireless network information

Wireless Configuration Information	Neighbor AP and STA Information	Wireless Statistics	Wireless Diagnosis
------------------------------------	---------------------------------	---------------------	--------------------

### WLAN Info

WLAN Status: Enabled

WLAN Channel: 5

### SSID Information

SSID Index	SSID Name	Security Configuration	Authentication Mode	Encryption Mode
1	2.4GSSID111	Configured	WPA/WPA2 PreSharedKey	TKIP&AES

Wireless Configuration Information	Neighbor AP and STA Information	Wireless Statistics	Wireless Diagnosis
------------------------------------	---------------------------------	---------------------	--------------------

STA Information

Query

MAC Address	SSID Name	Connection Duration (s)	Sending Rate (Mbps)	Receiving Rate (Mbps)	Signal Strength (dBm)	Noise (dBm)	Signal-to-Noise Ratio (dB)	Signal Quality (dBm)	Antenna Num	11k	11v	DualBand
-------------	-----------	-------------------------	---------------------	-----------------------	-----------------------	-------------	----------------------------	----------------------	-------------	-----	-----	----------

STA Boost Function

Query

STA Index	MAC Address	Online Status	Release Time	Boost Button
-----------	-------------	---------------	--------------	--------------

Neighbor AP Information

Query

Note: Querying neighbor AP information may disconnect all STA connections.

SSID Name	MAC Address	Network Type	Channel	Signal Strength (dBm)	Noise (dBm)	DTIM Interval	Beacon Period (ms)	Authentication Mode	Working Mode	Max. Rate (Mbps)	Multi-Link
-----------	-------------	--------------	---------	-----------------------	-------------	---------------	--------------------	---------------------	--------------	------------------	------------

Wireless Configuration Information	Neighbor AP and STA Information	Wireless Statistics	Wireless Diagnosis
------------------------------------	---------------------------------	---------------------	--------------------

WLAN Packet Statistics

SSID Index	SSID Name	Receive (RX)				Transmit (TX)			
		Bytes	Packets	Error	Discarded	Bytes	Packets	Error	Discarded
1	2.4GSSID111	0	0	0	0	0	0	0	0

STA Event Log

Download Log File

```

Manufacturer:Huawei Technologies Co., Ltd;
ProductClass:K572;
SerialNumber:
IP:192.168.101.1;
HWVer:
SWVer:V5R024
:0818031 [5G] [vap4] hmac_config_down_sync_all: WLAN DOWN success
:078213 [2G] [vap0] hmac_config_down_sync_all: WLAN DOWN success
:267242 [2G] [vap0] hmac_config_down_sync_all: WLAN DOWN success
:728427 [5G] [vap4] hmac_config_down_sync_all: WLAN DOWN success
:199160 [5G] [vap4] hmac_config_down_sync_all: WLAN DOWN success
    
```

Wireless Configuration Information	Neighbor AP and STA Information	Wireless Statistics	Wireless Diagnosis
------------------------------------	---------------------------------	---------------------	--------------------

### WLAN Health Diagnosis Report

WLAN Information	
2.4G WLAN Status:	Enabled
Working Mode:	802.11b/g/n/ax/be
Channel check:	5(Auto)
Frequency bandwidth mode:	20 MHz
Current working frequency bandwidth:	20 MHz
Whitelist/Blacklist filtering:	Off
MAC address check:	OK
Difference of antenna signal strength:	RSSI difference between antennas is less than or equal to 10.
Interference:	254
Calibration parameter:	Normal

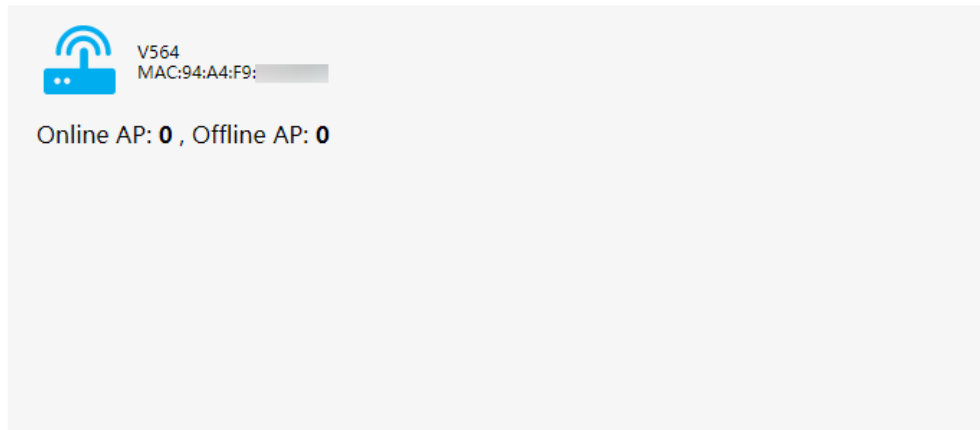
### 3.5.1.4 Home Network Information

In the navigation tree on the left, choose **System Info > Home Network Information**. In the right pane, check the device status, statistical information, and neighbor AP information of external APs in the Wi-Fi network, as shown in [Figure 3-7](#).

**Figure 3-7** Home Network Information

### Home Network Information

On this page, you can query the device status, statistics information, and neighbor AP information in the Wi-Fi network.



#### Information About the Selected External AP

Model	Serial Number	Hardware Version	Software Version	Online Duration	Frequency Band	SSID Connection	Upper-level Cascade Channel	Downlink Channel	Uplink Signal Strength (dBm)
--	--	--	--	--	--	--	--	--	--

#### Frequency Band of the Selected External AP

Devices Associated with External APs			External APs Neighbor Information					External AP Wi-Fi Statistics				
SSID Name	MAC Address	Connection Duration (s)	Receiving Rate (Mbps)	Sending Rate (Mbps)	Signal Strength (dBm)	Noise (dBm)	Signal-to-Noise Ratio (dB)	Signal Quality (dBm)	Antenna Num	11k	11v	DualBand
--	--	--	--	--	--	--	--	--	--	--	--	--

## 3.5.2 WLAN

This topic describes how to configure WLAN through the Web page, including WLAN Advanced Configuration, Wi-Fi Coverage Management, and Automatic Wi-Fi Shutdown.

### 3.5.2.1 Wi-Fi Advanced Configuration

1. In the navigation tree on the left, choose **WLAN > Wi-Fi Advanced Network Settings**. In the right pane, configure the advanced parameters of 2.4G and 5G Wi-Fi, as shown in **Figure 3-8**.

**Figure 3-8** WLAN Advanced Configuration  
WLAN Advanced Configuration

You can customize the wireless network to adapt to various wireless network environments.

### 2.4G Wi-Fi

**Broadcast SSID:**

Regulatory Domain:  ▼

Channel:  ▼

Channel Width:  ▼

Mode:  ▼

If the Wi-Fi cannot be found or connected when 802.11be is enabled, upgrade the wireless network adapter driver.

### 5G Wi-Fi

**Broadcast SSID:**

Regulatory Domain:  ▼

Channel:  ▼

Channel Width:  ▼

Mode:  ▼

If the Wi-Fi cannot be found or connected when 802.11be is enabled, upgrade the wireless network adapter driver.

2. Click **Apply**.

**Table 3-2** describes the WLAN advanced parameters.



**Table 3-2** WLAN advanced parameters

Parameter	Description
Broadcast SSID	<p>Indicates whether to enable or hide broadcast.</p> <ul style="list-style-type: none"> <li>• If the option box is selected, it indicates that the SSID broadcast function is enabled. The edge ONT periodically broadcasts the SSID, that is, the name of the wireless network. In this way, any STA can search for the wireless network.</li> <li>• If the option box is not selected, it indicates that the SSID broadcast function is disabled. The SSID is hidden, and the STA cannot search for the wireless network. The SSID can be obtained only through a request.</li> </ul>
Channel	Indicates the channel of the wireless network. The channel varies with the value of Regulatory Domain.
Channel Width	<p>Indicates the wireless channel width.</p> <ul style="list-style-type: none"> <li>• 2.4G Wi-Fi can be set to <b>Auto 20/40 MHz, 20 MHz</b> or <b>40 MHz</b>.</li> <li>• 5G Wi-Fi can be set to <b>Auto 20/40 MHz, 20 MHz , 40 MHz, Auto 20/40/80 MHz</b> or <b>Auto 20/40/80/160 MHz</b>.</li> </ul>
Mode	<p>Indicates the supported wireless network mode.</p> <ul style="list-style-type: none"> <li>• 2.4G Wi-Fi can be set to <b>802.11b, 802.11g, 802.11b/g, 802.11b/g/n, 802.11b/g/n/ax</b> or <b>802.11b/g/n/ax/be</b>.</li> <li>• 5G Wi-Fi can be set to <b>802.11a, 802.11a/n, 802.11a/n/ac, 802.11a/n/ac/ax</b> or <b>802.11a/n/ac/ax/be</b>.</li> </ul>

### 3.5.2.2 Wi-Fi Coverage Management

1. In the navigation tree on the left, choose **WLAN > Wi-Fi Coverage Management**. In the right pane, specify the SSID used for smart Wi-Fi coverage and add the identified external AP devices to the Wi-Fi network, as shown in [Figure 3-9](#) and [Figure 3-10](#).

### Figure 3-9 Wi-Fi Parameter Configuration Wi-Fi Coverage Management

On this page, you can specify the SSID for a Wi-Fi network and add the scanned external AP to this Wi-Fi network. Then, the external AP and this device construct an entire Wi-Fi network and your wireless devices can seamlessly access this network.

Enable Wi-Fi coverage (taking effect after the ONT resets)

Wi-Fi Parameter Setting	Wi-Fi Network Management
-------------------------	--------------------------

Set 2.4G Parameters

Go to the 2.4G Basic Network Settings web page

SSID Name	Broadcast SSID	Authentication and Encryption Mode	Password
2.4GSSID	Enabled	WPA-WPA2-Personal	<input type="password" value="....."/> <input checked="" type="checkbox"/> Hide

Set 5G Parameters

Go to the 5G Basic Network Settings web page

SSID Name	Broadcast SSID	Authentication and Encryption Mode	Password
2.4GSSID_5G	Enabled	WPA-WPA2-Personal	<input type="password" value="....."/> <input checked="" type="checkbox"/> Hide

Select a policy to synchronize Wi-Fi parameters to the newly detected external AP.

Do not enable automatic synchronization.

Specify the SSID for automatic synchronization.

Enable best-effort synchronization based on AP capabilities.

External AP List

Device Model	Serial Number	Status	Online Duration	Configuration Status
--	--	--	--	--

**Figure 3-10** Wi-Fi Network Management

### Wi-Fi Coverage Management

On this page, you can specify the SSID for a Wi-Fi network and add the scanned external AP to this Wi-Fi network. Then, the external AP and this device construct an entire Wi-Fi network and your wireless devices can seamlessly access this network.

Enable Wi-Fi coverage (taking effect after the ONT resets)

Wi-Fi Parameter Setting

Wi-Fi Network Management

Synchronize WLAN frequency band status to the external AP

Enable to synchronize with the gateway smartlink to force the use of https connection

Enable Video Retransmission Switch

RTCP Port  1~65535, default value:8027

Apply

Cancel

### Wi-Fi Link Switching Sensitivity

○ ————— ● ————— ○  
Low                      Medium                      High

Apply

Cancel

### Wi-Fi Operation for Entire Network

Forced channel  
reselection

Start

### Automatic Network Topology Adjustment Policy

No cascaded STAs

Deteriorated cascade link

The cascade link rate is lower than the threshold.

The air interface packet loss rate of the cascade link exceeds the threshold.

Apply

Cancel

### Cascade Link Threshold

Name	Value	Description
Low rate threshold	<input type="text" value="200"/>	kbps (0 to 65535; default value: 200)
PLR threshold	<input type="text" value="5"/>	% (0 to 100; default value: 5)

Apply

Cancel

**Table 3-3** describes the Wi-Fi coverage management parameters.

**Table 3-3** Wi-Fi coverage management parameters

Parameter	Description
Enable Wi-Fi coverage	Adds detected external APs to the smart Wi-Fi coverage network after this option is selected. The added external APs and the device form a complete Wi-Fi network. Within the coverage, the APs can seamlessly connect to the network. By default, it is selected.
<b>Wi-Fi Parameters Configuration</b>	
Set 2.4G Parameters	Displays 2.4G Wi-Fi parameter settings configured on <b>My Wi-Fi</b> and <b>WLAN Advanced Configuration</b> pages.
Set 5G Parameters	Displays 5G Wi-Fi parameter settings configured on <b>My Wi-Fi</b> and <b>WLAN Advanced Configuration</b> pages.
Select a policy to synchronize Wi-Fi parameters to the newly detected external AP	Selects either of the following policies: <ul style="list-style-type: none"> <li>• <b>Do not enable automatic synchronization.</b></li> <li>• <b>Specify the SSID for automatic synchronization.</b> (If the device has multiple SSIDs, specify one of the SSIDs to be synchronized to an external AP.)</li> <li>• <b>Enable best-effort synchronization according to AP capabilities.</b></li> </ul>
<b>Wi-Fi Network Management</b>	
Synchronize WLAN frequency band status to the external AP	Synchronizes the enabling status of the 2.4G and 5G Wi-Fi frequency bands to an external AP after this option is selected. For example, if the 5G Wi-Fi frequency band is disabled on the device, the 5G Wi-Fi frequency band will be also disabled on the external AP.
Enable to synchronize with the gateway smartlink to force the use of https connection	Whether to use HTTPS forcibly for hilink message interaction between primary devices and secondary devices.
Enable Video Retransmission Switch	Used to connect the device to an upstream device in dual-channel upstream mode. When this function is disabled, the device uses a single channel (2.4G or 5G) for upstream transmission.

Parameter	Description
Wi-Fi Link Switching Sensitivity	Sets the Wi-Fi sensitivity applied during Wi-Fi roaming. Sensitivity options are as follows: <ul style="list-style-type: none"><li>• <b>Low</b> (no active switching)</li><li>• <b>Medium</b> (default value)</li><li>• <b>High</b> (active switching)</li></ul>
Forced channel reselection	Re-assess network-wide Wi-Fi channels and re-selects a channel after you click <b>Start</b> .
Automatic Network Topology Adjustment Policy	<ul style="list-style-type: none"><li>• <b>No cascaded STAs:</b> After this option is selected, automatic network topology adjustment is implemented only when no STA is connected to the network.</li><li>• <b>Deteriorated cascade link:</b> Automatic network topology adjustment is implemented when the quality of cascading links deteriorates. You can set the link quality deterioration criteria to <b>The cascade link rate is lower than the threshold</b> or <b>The air interface packet loss rate of the cascade link exceeds the threshold</b>. The threshold refers to the settings in the <b>Cascading Link Threshold</b> field.</li></ul>
Cascading Link Threshold	Sets the low rate threshold and packet loss rate threshold for a cascading link to determine whether the link quality deteriorates.

2. Click **Apply**.

### 3.5.2.3 MLO Advanced Network

1. In the navigation tree on the left, choose **WLAN > MLO Advanced Network Settings**. In the right pane, select **MLO Network**, and set your MLO network, as shown in [Figure 3-11](#).

**Figure 3-11** MLO Network  
MLO Network

Create your MLO network, then its connected Wi-Fi 7 clients can simultaneously send and receive data across different bands, greatly improving the transmission rate and reliability(When the 2.4GHz or 5Ghz wireless network is disabled, this page is blank).

**⚠ Caution:**

Devices supporting Wi-Fi 7 can be connected through multiple links, improving the rate and reducing the delay. Some devices may have compatibility issues.

**Advanced Configuration**

MLO Network:

Band:  2.4G  
 5G

SSID Name:  \*(1-32 characters)

Authentication Mode:

WPA PreSharedKey:  \*(8-63 characters or 64 hexadecimal characters)

**Apply** **Cancel**

**Table 3-4** describes the MLO network parameters.

**Table 3-4** MLO Network parameters

Parameter	Description
MLO Network	Indicates a Multi-Link Operation (MLO) network of WiFi 7, which can enable devices to simultaneously send and receive data across different frequency bands and channels.
Band	Indicates the 2.4G Wi-Fi or 5G Wi-Fi frequency band. If the 2.4G Wi-Fi and 5G Wi-Fi frequency bands are used together, the device automatically selects a faster Wi-Fi frequency band. If this switch is turned off, the Wi-Fi frequency band can be set manually.
SSID Name	Indicates the name of the wireless network. It is used to differentiate different wireless networks. It consists of a maximum of 32 characters, without space or Tab character.

Parameter	Description
Authentication Mode	Indicates the authentication mode for the STA to request access to the wireless network. The mode can be WPA2 PreSharedKey, WPA3 SAE, or WPA2/WPA3 PSKandSAE.
WPA Preshared Key	Set the encryption password of a user. The password can be hidden. Restrictions: 8-63 characters or 64 hexadecimal characters.

2. Click **Apply**.

### 3.5.2.4 Automatic Wi-Fi Shutdown

1. In the navigation tree on the left, choose **WLAN > Automatic Wi-Fi Shutdown**. In the right pane, configure the scheduled Wi-Fi shutdown time segment, to enable the Wi-Fi network to be automatically shut down when the Wi-Fi network is not in use, as shown in **Figure 3-12**.

**Figure 3-12** Automatic Wi-Fi Shutdown

#### Automatic Wi-Fi Shutdown

On this page, you can enable automatic Wi-Fi shutdown in a specified period as required.

#### Automatic Shutdown Configuration

<input checked="" type="checkbox"/> Enable automatic Wi-Fi shutdown							New		Delete	
	Start	End	Mon	Tues	Wed	Thur	Fri	Sat	Sun	All
<input type="checkbox"/>	00:00	07:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

System Time: 1981-01-01 00:19:48

The current system time is incorrect. Exercise caution when using the scheduled Wi-Fi shutdown function.

Apply

Cancel

2. Click **Apply**.

The following table describes the parameters related to scheduled shutdown of the Wi-Fi network.

**Table 3-5** Parameters related to scheduled shutdown of the Wi-Fi network

Parameter	Description
Enable automatic Wi-Fi shutdown	Indicates whether to enable the scheduled wireless network shutdown function.

Parameter	Description
End	Indicates the end time to shut down the Wi-Fi network automatically which can be set after <b>Enable automatic Wi-Fi shutdown</b> is selected.
Start	Indicates the start time to shut down the Wi-Fi network automatically which can be set after <b>Enable automatic Wi-Fi shutdown</b> is selected.

### 3.5.2.5 Multi-AP Role Settings

1. In the navigation tree on the left, choose **WLAN > Multi-AP Role Settings**. In the right pane, set the mesh device role to controller or agent, as shown in [Figure 3-13](#).

Figure 3-13 Multi-AP

#### Multi-AP

On this page, you can set EasyMesh device role to Controller, Agent.

Enable EasyMesh	<input checked="" type="checkbox"/> (Need to restart to take effect)
Role Settings	
Role Setting	<input checked="" type="radio"/> Controller <input type="radio"/> Agent
Current Role	Controller
<input type="button" value="Apply"/>	

2. Click **Apply**.

### 3.5.3 Network Configuration

This topic describes how to configure network through the Web page, including LAN Settings, IPv6, DDNS Function and UPnP Function.

#### 3.5.3.1 LAN Settings

1. In the navigation tree on the left, choose **Network Configuration > LAN Settings**. In the pane on the right, configure LAN parameters, as shown in [Figure 3-14](#).



**Figure 3-14** LAN Settings

### LAN Settings

On this page, you can set LAN parameters.

#### Primary Address Pool

LAN IP address:

Enable the DHCP server:

IP Address Allocation Range: 192.168.101.  --

Lease Time:

**Apply**

#### Static IP address list

	MAC Address	IP Address
----	----	----

MAC Address:  (AA:BB:CC:DD:EE:FF)

IP Address:

**Apply** **Cancel**

2. Click **Apply**.

The following table describes the LAN parameters.

**Table 3-6** LAN parameters

Parameter	Description
LAN IP address	<p>Indicates the management IP address of the local LAN of the device.</p> <p><b>NOTE</b> Ensure that the IP address of the LAN-side device is in the same network segment as the configured management IP address. Based on this premise, you can access the edge ONT on the web page, and perform query, configuration, and management operations.</p> <ul style="list-style-type: none"> <li>You can set the IP address of the LAN-side device to be in the same network segment as the management IP address.</li> <li>Alternatively, start the DHCP server and set the IP address of the DHCP address pool to be in the same network segment as the management IP address.</li> </ul>
Enable the DHCP server	Indicates whether to enable the DHCP server.
IP Address Allocation Range	Specifies the start and end of IP addresses allocated by the DHCP server. The default range is 192.168.101.2 to 192.168.101.254.
Lease Time	Indicates the lease time of the IP address pool on the DHCP server. Options: minute, hour, day, and week.
Static IP address List	Specifies an IP address for a specified MAC address.
MAC Address	Specifies a MAC address.
IP Address	Specifies an IP address.

### 3.5.3.2 IPv6

1. In the navigation tree on the left, choose **Network Configuration > IPv6**. In the right pane, determine whether to enable the IPv6, as shown in **Figure 3-15**.

**Figure 3-15** IPv6

IPv6

On this page, you can enable or disable the IPv6 function.

IPv6

2. Click **Apply**.

### 3.5.3.3 DDNS Function

Dynamic domain name service (DDNS) associates a static domain name with the dynamic IP address of its host.

Assume that server A provides HTTP or FTP service and it is connected to the Internet using routers. If server A obtains an IP address through DHCP, or server A is connected to the Internet through PPPoE, PPTP, or L2TP, the IP address is a dynamic IP address. That is, its IP address may change each time when server A initializes its connection to the Internet.

The mapping between the domain name and IP address provided by the domain name service (DNS) server is static, and the mapping does not update when the IP address changes. Therefore, when the IP address of server A changes, users on the Internet cannot access server A with domain names.

With DDNS, which associates a static domain name with the dynamic IP address of its host, users on the Internet can access the server only with domain names.

1. In the navigation tree on the left, choose **Network Configuration > DDNS Function**. In the right pane, configure DDNS parameters, including **Service Provider**, **Host Name**, **Service Port**, **Domain Name**, **Username**, and **Password**, as shown in [Figure 3-16](#).

**Figure 3-16 DDNS Function**

**DDNS Function**

To obtain the dynamic DNS service, you must apply for a domain name from the dynamic DNS service provider to obtain the configuration information, including the host, user name, and password. None of currently supported service providers use secure encryption algorithm, please use DDNS services with caution.

New
Delete

	WAN Name	Status	Service Provider	Domain Name
----	----	----	----	----

**DDNS Service Information:**

Enable DDNS:

WAN Name:

Domain Name:  \*(1-255 characters)

**Service provider information:**

Service Provider:

Host of the Service Provider:  \*(1-255 characters)

Service Port:  \*(1-65535)

User Name:  \*(1-256 characters)

Password:  (0-256 characters)

Encryption Mode:

Apply
Cancel

**DDNS Service State:**

WAN Name	Domain Name	Run State	Last Update Time	Last Error
--	--	--	--	--

2. Click **Apply**.

The following table describes the DDNS Function parameters.

Parameter	Description
Enable DDNS	Determine whether to enable DDNS.
WAN Name	Indicates the name of the WAN interface used by a network-side client to access an intranet device.
Domain Name	Indicates the complete domain name that has been obtained.

Parameter	Description
<b>Service provider information</b>	
Service Provider	Indicates the service provider corresponding to the domain name.
Host of the Service Provider	Indicates the host of a service provider after you select the service provider.
Service Port	Indicates the port ID of the SIP server.
User Name/ Password	Indicates the user name and password registered on the service provider's website.
Encryption Mode	<p>Indicates the encryption mode associated by a service provider. It cannot be configured. Different service providers may have different encryption modes for user names and passwords. To ensure information security, you are advised to select a service provider that provides a higher level of security. Encryption modes with security levels from high to low are as follows: MD5, Base64, no encryption.</p> <p><b>NOTICE</b> MD5/BASE64 is an insecure encryption algorithm, and can be used only in a secure environment.</p>

### 3.5.3.4 UPnP Function

Universal Plug and Play (UPnP) is the name of a group of protocols. The UPnP supports zero configuration networking and automatic discovery of different network devices. If the UPnP is enabled, the UPnP-enabled device can be dynamically connected to the network to obtain the IP address, obtain the transfer performance, discover other devices, and learn the performance of the other devices. The UPnP-enabled device can be automatically disconnected from the network, without affecting the device or other devices.

When the UPnP is enabled, the LAN-side PC automatically finds the edge ONT, which is considered as a peripheral device of the PC and is plug-and-play. After running application software on the PC, port mapping entries are automatically generated on the edge ONT through the UPnP protocol, thus improving the running speed.

In the navigation tree on the left, choose **Network Configuration > UPnP Function**. In the right pane, determine whether to enable the UPnP, as shown in [Figure 3-17](#).

**Figure 3-17** UPnP Function

### UPnP Function

On this page, you can enable or disable the universal plug-and-play (UPnP) function, which supports automatic discovery of multiple types of network devices. If this function is enabled for a device, the device can access networks, obtain an IP address, transmit data, discover other devices, and acquire the data of other devices.

Enable UPnP:

Number	Description	External Port	Internal Port	Protocol	IP Address	Status
--	--	--	--	--	--	--

<< < 0/0 > >>

Page  Go

## 3.5.4 Security Configuration

This topic describes how to configure the security through the web page.

### 3.5.4.1 Wi-Fi MAC Address Filtering Configuration

In the navigation tree on the left, choose **Security Configuration > Wi-Fi MAC Address Filtering**. In the right pane, enable WLAN MAC Filter, and configure the filtering information, as shown in **Figure 3-18**.

**Figure 3-18** Wi-Fi MAC Address Filtering

### Wi-Fi MAC Address Filtering

On this page, you can configure MAC filter to prohibit some PCs from accessing the Internet.

Enable WLAN MAC Filter:

Filter Mode:

	SSID Index	Device Name	Source MAC Address
----	----	----	----

SSID Index:

Device Name:

Source MAC Address:  \*(AA:BB:CC:DD:EE:FF)

### 3.5.4.2 Firewall Configuration

In the navigation tree on the left, choose **Security Configuration > Firewall Configuration**. In the right pane, configure the firewall, as shown in **Figure 3-19**.

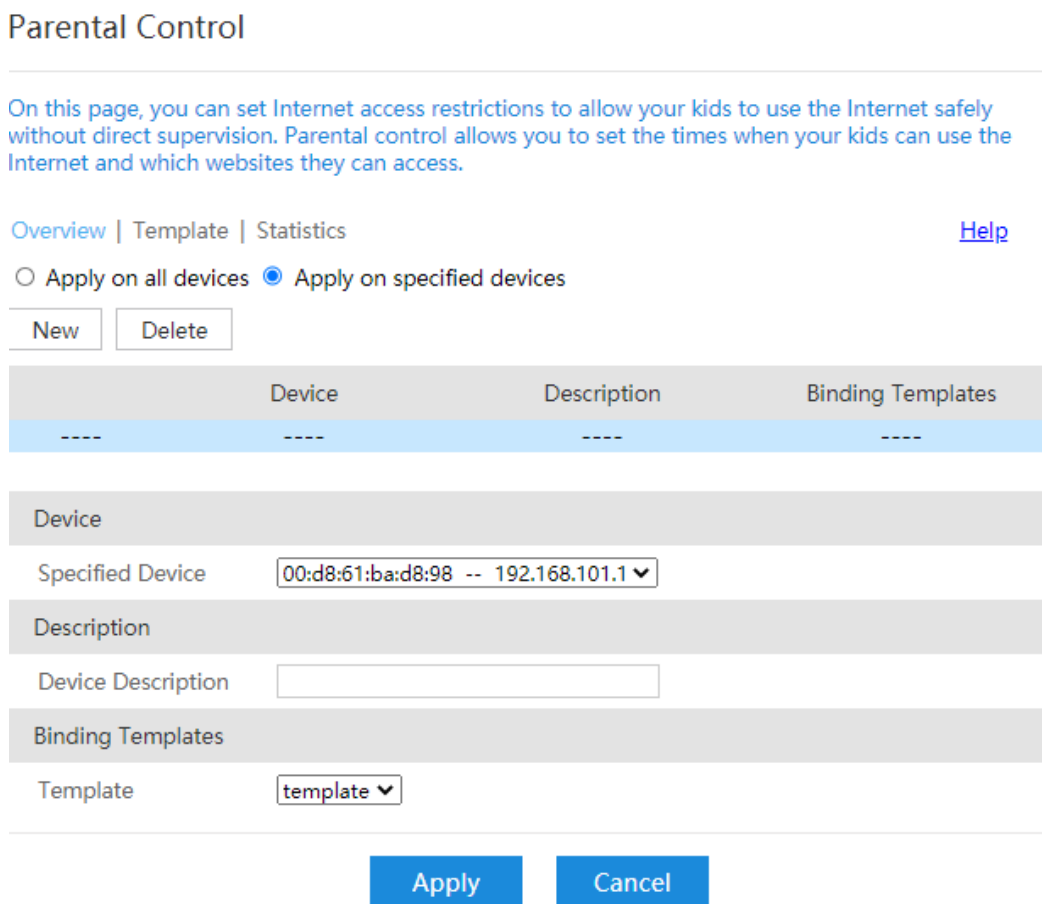
**Figure 3-19** Firewall Configuration



### 3.5.4.3 Parental Control

In the navigation tree on the left, choose **Security Configuration > Parental Control**. In the right pane, configure different constraints for the network surfing time and website access on working days and holidays. In this way, their children are allowed to access networks in specified time segments and free from age inappropriate contents, as shown in **Figure 3-20**.

**Figure 3-20** Parental Control



**Table 3-7** describes the parameters related to the Parental Control.

**Table 3-7** Parameters related to the Parental Control

Parameter	Description
Apply on all devices	Indicates the Internet access constraints takes effect on all devices.
Apply on specified devices	Indicates the Internet access constraints takes effect on some specified devices.
Specified Device	Indicates the device to be restricted in the Internet access. This parameter can be set after <b>Apply on specified devices</b> is selected.
Device Description	Indicates the description of the device to be restricted in the Internet access.
Template	Indicates the template of Internet access constraints.

 **NOTE**

Configure the template by following the instructions provided in the wizard. You can click **Help** in the upper right to view the online help about the template configuration if required.

### 3.5.4.4 DMZ Function

1. In the navigation tree on the left, choose **Security Configuration > DMZ Function**. In the right pane, click **New**. In the dialog box that is displayed, set the parameters related to the DMZ, as shown in **Figure 3-21**.

**Figure 3-21** DMZ Function

#### DMZ Function

On this page, you can configure DMZ parameters. The DMZ device restricts unreliable external connections from linking up to the device. It is a buffer between a secure system and an insecure system. If the WAN port is not listed in the port mapping table, the application requests from the WAN connection are forwarded to the DMZ device.

New
Delete

	WAN Name	Enable DMZ	Host Address
----	----	----	----

Enable DMZ:

WAN Name:

Host Address:

Apply
Cancel



2. Click Apply.

#### NOTICE

- If the LAN-side device does not provide website service or other network services, do not set the device to a DMZ host because all ports of a DMZ host are opened to the Internet.
- If remote diagnosis needs to be performed on the WAN-side access page, do not configure DMZ rules.

**Table 3-8** describes the parameters related to the DMZ.

**Table 3-8** Parameters related to the DMZ

Parameter	Description
Enable DMZ	Indicates whether to enable the DMZ.
WAN Name	Indicates the name of the WAN interface. If the WAN interface is not in the port mapping table, the application requests from the WAN connection are directly forwarded to the host in the DMZ.
Host Address	Indicates the IP address of the DMZ host.

### 3.5.4.5 IPv4 Port Mapping

Port mapping indicates that the Intranet server is allowed to be open to the Extranet (for example, the Intranet provides the Extranet with a WWW server or FTP server). Port mapping is to map the Intranet host IP address and port ID to Extranet IP address and corresponding port ID so that users from Extranets can access the Intranet server. With port mapping, the users cannot see the Intranet IP address and they see the Extranet IP address.

#### Navigation Path

1. In the navigation tree on the left, choose **Security Configuration > IPv4 Port Mapping**. In the right pane, set the parameters related to port mapping, as shown in **Figure 3-22**.

**Figure 3-22 IPv4 Port Mapping**

### IPv4 Port Mapping

On this page, you can set port mapping parameters to set up virtual servers on the LAN network and allow these servers to be accessed from the Internet.

Note: The well-known ports for voice services cannot be in the range of the mapping ports. Connected APs cannot function as internal hosts.

New
Delete

	Mapping Name	WAN Name	Internal Host	External Host	Enable
----	----	----	----	----	----

Type:  User-defined  Application

Application:

Enable Port Mapping:

Mapping Name:

WAN Name:

Internal Host:  \*

External Source IP Address:  --

Protocol:  External source port number:  --

Internal port number:  --  \* External port number:  --

Delete

Add

Apply
Cancel

2. Click **Apply**.

### Configuration Example

Enable the packets sent from the WAN side to the edge ONT whose the destination WAN port number is 2000 to be forwarded to the LAN-side PC whose IP address is 192.168.100.106, and the port number is changed to 3000.

## IPv4 Port Mapping

On this page, you can set port mapping parameters to set up virtual servers on the LAN network and allow these servers to be accessed from the Internet.  
Note: The well-known ports for voice services cannot be in the range of the mapping ports.

New
Delete

Mapping Name	WAN Name	Internal Host	External Host	Enable
----	----	----	----	----

Type:  User-defined  Application

Application:

Enable Port Mapping:

Mapping Name:

WAN Name:

Internal Host:  \*

External Source IP Address:  --

Protocol:  Internal port number:  --  \*

External port number:  --  External source port number:  --

## Parameter Description

[Table 3-9](#) describes the parameters related to IPv4 port mapping.

**Table 3-9** Parameters related to IPv4 port mapping

Parameter	Description
Type	Indicates the type, which can be <b>User-defined</b> or <b>Application</b> . If the type is set to <b>Application</b> , you can select a server from the <b>Application</b> drop-down list box.
Enable Port Mapping	Indicates whether to enable port mapping.
Mapping Name	Indicates the name of the port mapping rule.

Parameter	Description
WAN Name	Indicates the name of the WAN interface where port mapping is enabled.
Internal Host	Indicates the IP address of the host to which the port is mapped.
External Source IP Address	Indicates the source IP address of the external data packet.
Protocol	Indicates the protocol type of port mapping packet, which may be TCP, UDP, or TCP/UDP.
External port number	Indicates the destination start and end port numbers of the extranet data packet.
Internal port number	Indicates the intranet destination start and end port numbers of the port mapping.
External source port number	Indicates the source start and end port numbers of the extranet data packet.

### 3.5.4.6 Port Trigger Configuration

The port trigger indicates that a specific Extranet port is automatically enabled when a corresponding Intranet port sends a packet and the packet is mapped to the Intranet port on the host. A specific mapping packet is sent from the edge ONT through the Intranet so that specific packets of the Extranet can be mapped to the corresponding host. A specified port on the gateway firewall is open to some applications for remote access. The port trigger can dynamically enable the open port of the firewall.

1. In the navigation tree on the left, choose **Security Configuration > Port Trigger Configuration**. In the right pane, click **New**. In the dialog box that is displayed, set the parameters related to the port trigger, as shown in [Figure 3-23](#).

**Figure 3-23** Port Trigger Configuration

Port Trigger Configuration

On this page, you can configure the range of the ports that are used by LAN-side applications to access the Internet. You can also enable the port automatically.

Note: The well-known ports for voice services cannot be in the range of open ports.

New
Delete

	WAN Name	Enable Port Trigger	Trigger Port	Open Port	Trigger Protocol	Open Protocol
----	----	----	----	----	----	----

Enable Port Trigger:

WAN Name:

Trigger Protocol:

Open Protocol:

Start Trigger Port: \*

End Trigger Port: \*

Start Open Port: \*

End Open Port: \*

Apply
Cancel

2. Click Apply.

**Table 3-10** describes the parameters related to the port trigger.

**Table 3-10** Parameters related to the port trigger

Parameter	Description
Enable Port Trigger	Indicates whether to enable the port trigger.
WAN Name	Indicates the name of the WAN interface where the port trigger is enabled.
Trigger Protocol	Indicates the protocol type of the port trigger packet, which may be TCP, UDP, or TCP/UDP.
Open Protocol	Indicates the protocol type of the open data packet.
Start Trigger Port	Indicates the destination start port of the port trigger packet.
End Trigger Port	Indicates the destination end port of the port trigger packet.

Parameter	Description
Start Open Port	Indicates the destination start port of the open packet.
End Open Port	Indicates the destination end port of the open packet.

### 3.5.4.7 Device Access Control

1. In the navigation tree on the left, choose **Security Configuration > Device Access Control**. In the pane on the right, configure the rule of edge ONT access control, as shown in **Figure 3-24**.



Complete network security planning before enabling remote access control to ensure that edge ONTs are logged in to in secure network conditions. After the edge ONT login operations are complete, disable remote access control in a timely manner. If you do not complete network security planning or do not disable remote access control in a timely manner, the network may become faulty or be attacked, and Huawei will not be responsible for any related subsequences.

**Figure 3-24** Device Access Control

#### Device Access Control

On this page, you can enable or disable permissions to access the device.

##### LAN Service

Enable the LAN-side PC to access the device using Telnet:

Enable the LAN-side PC to access the device using SSH:

##### Wi-Fi Service

Enable devices on the Wi-Fi side to access web pages:

Enable the PC on the Wi-Fi side to access the device using Telnet:

Apply

Cancel

2. Click **Apply**.

### 3.5.4.8 PSK Crack Defense

1. In the navigation tree on the left, choose **Security Configuration > PSK Crack Defense**. In the pane on the right, you can enable or disable WLAN PSK Crack Defense, as shown in [Figure 3-25](#).

**Figure 3-25** WLAN PSK Crack Defense

#### WLAN PSK Crack Defense

On this page, you can enable or disable WLAN PSK crack defense.

WLAN PSK Crack Defense

Save

Cancel

2. Click **Save**.

## 3.5.5 System Management

This topic describes how to configure the System Management through the web page.

### 3.5.5.1 Upstream Network Port Settings

1. In the navigation tree on the left, choose **System Management > Upstream Network Port Settings**. In the pane on the right, set a fixed upstream network port or enable automatic selection of the upstream network port, as shown in [Figure 3-26](#).

**Figure 3-26** Upstream Network Port Settings

### Upstream Network Port Settings

On this page, you can set a fixed upstream network port or enable automatic selection of the upstream network port.

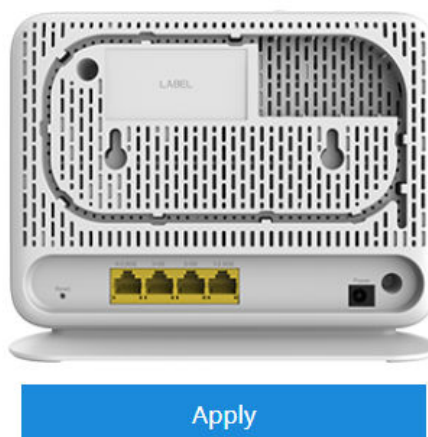
Upstream Network Port  
Settings

Select an upstream network port automatically

Fixed upstream network port

In this mode, LAN4 is the fixed WAN port.

Please manually set the WAN connection based on the networking configuration provided by your ISP.



2. Click **Apply**.

### 3.5.5.2 TR-069

1. In the navigation tree on the left, choose **System Management > TR-069**. In the pane on the right, set the parameters related to the interconnection between the ONT and the TR-069 server, as shown in [Figure 3-27](#).



### Figure 3-27 TR-069 ACS Configuration

On this page, you can set the ACS parameters, port mapping function of the primary gateway, set the authentication password of the SSL certificate, and import the corresponding SSL certificate.

#### ACS Parameter Settings

Enable ACS Management:

Enable Periodic Informing:

Informing Interval:  \*[1-2147483647](s)

Informing Time:  yyyy-mm-ddThh:mm:ss (for example, 2009-12-20T12:23:34)

ACS URL:  \*

ACS User Name:

ACS Password:

Connection Request User Name:

Connection Request Password:

DSCP:  (0-63)

#### Automatic configuration of the primary gateway portMapping port

Enable:

External Port: --

### STUN Server Management

Enable STUN:

Minimum STUN Keep-alive Period:  \*(s)

Maximum STUN Keep-alive Period:  \*(s)

STUN Server Address:  \*

STUN Server Port:  \*

STUN Username:  \*

STUN Password:  \*

2. Click **Apply**.

**Table 3-11** describes the TR-069 parameters.

**Table 3-11** TR-069 parameters

Parameter	Description
ACS Parameter Settings	
Enable ACS Management	Indicates whether to enable the <b>ACS Management</b> .
Enable Periodic Informing	Indicates whether to enable the notification function. <ul style="list-style-type: none"> <li>If the notification function is enabled, the ONT actively sends a connection request to the TR-069 server.</li> <li>If the notification function is disabled, the ONT does not actively send a connection request to the TR-069 server.</li> </ul> When the notification function is enabled, the <b>Informing Interval</b> and <b>Informing Time</b> parameters can be set.
Informing Interval	Indicates the interval for the ONT to send a connection request to the TR-069 server.
Informing Time	Indicates the time for the ONT to send a connection request to the TR-069 server.
ACS URL	Indicates the address of the TR-069 server to which the ONT sends a connection request.
ACS User Name	Indicates the user name for the ONT to register with the TR-069 server.

Parameter	Description
ACS Password	Indicates the password for the ONT to register with the TR-069 server.
Connection Request User Name	Indicates the user name to be carried when the TR-069 server initiates a connection request to the ONT.
Connection Request Password	Indicates the password to be carried when the TR-069 server initiates a connection request to the ONT.
DSCP	Defined by RFC2474 "Definition of the Differentiated Services Field". Differentiated Services Code Point (DSCP) uses code values for priority marking. DSCP can be customized for carriers based on service requirements so that devices on a network perform QoS based on the DSCP value.
Automatic configuration of the primary gateway portMapping port	
Enable	Indicates whether to enable the port mapping function of the primary gateway.
External port	Indicates an external port.
STUN Server Management	
Enable STUN	Enables or disables the use of STUN by the device. This applies only to the use of STUN in association with the ACS to allow UDP Connection Requests.
Minimum STUN Keep-alive Period	If STUN Is enabled, the minimum period, in seconds, that STUN Binding Requests can be sent by the device for the purpose of maintaining the binding in the Gateway. This limit applies only to Binding Requests sent from the UDP Connection Request address and port, and only those that do not contain the BINDING-CHANGE attribute. This limit does not apply to retransmissions following the procedures defined in [RFC3489].
Maximum STUN Keep-alive Period	If STUN Is enabled, the maximum period, in seconds, that STUN Binding Requests MUST be sent by the device for the purpose of maintaining the binding in the Gateway. This applies specifically to Binding Requests sent from the UDP Connection Request address and port. A value of -1 indicates that no maximum period is specified.

Parameter	Description
STUN Server Address	Host name or IP address of the STUN server for the CPE to send Binding Requests if STUN is enabled via <i>STUNEnable</i> . If an empty string and <i>STUNEnable</i> is <i>true</i> , the CPE MUST use the address of the ACS extracted from the host portion of the ACS URL.
STUN Server Port	Port number of the STUN server for the CPE to send Binding Requests if STUN is enabled via <i>STUNEnable</i> . By default, this SHOULD be the equal to the default STUN port, 3478.
STUN Username	If not an empty string, the value of the STUN USERNAME attribute to be used in Binding Requests (only if message integrity has been requested by the STUN server). If an empty string, the CPE MUST NOT send STUN Binding Requests with message integrity.
STUN Password	The value of the STUN Password to be used in computing the MESSAGE-INTEGRITY attribute to be used in Binding Requests (only if message integrity has been requested by the STUN server). When read, this parameter returns an empty string, regardless of the actual value.

### 3.5.5.3 SP Management Platform

In the navigation tree on the left, choose **System Management > SP Management Platform**. In the pane on the right, select an **Area** as instructed by your service provider, the **Management server address** field is automatically populated after you select an **Area**. Click **Apply** to enable the function of service provider remote management, as shown in [Figure Service Provider Remote Management Platform](#).

### Figure 3-28 Service Provider Remote Management Platform

#### Service Provider Remote Management Platform

On this page, you can set the address of the service provider remote management platform. Select an option as instructed by your service provider. If the selection is incorrect, the remote software upgrade function of the device will be unavailable.

Area

Management server address

I know that the service provider remote management platform collects device data to the server address and understand the protocols, contracts, and privacy policies of network service provider.

### 3.5.5.4 Software Upgrade

1. In the navigation tree on the left, choose **System Management > Software Upgrade**. In the pane on the right, select the target software version of the device. Click **Upgrade** to upgrade the software of the device, you can also use online upgrade function to automatically upgrade the software of the device, as shown in [Figure 3-29](#).

### Figure 3-29 Software Upgrade

#### Software Upgrade

On this page, you can use the firmware upgrade function to upgrade the software of the terminal to the target version.

Firmware File:

2. After the upgrade is successful, a message is displayed indicating that the device needs to be reset. Click **Restart**. The configuration data takes effect after the device is reset.

### 3.5.5.5 Account Management

1. In the navigation tree on the left, choose **System Management > Account Management**. In the pane on the right, change the password of the current login user, as shown in [Figure 3-30](#).

**Figure 3-30** Account Management  
Account Management

On this page, you can change the password of the current login user to ensure security and make it easy to remember.

Change Password

Old Password:	<input type="text"/>	1. The password must contain at least 8 characters. 2. The password must contain at least two of the following combinations: digits, uppercase letters, lowercase letters, and special characters. Special characters can be the following: ` ~ ! @ # \$ % ^ & * ( ) - _ = + \   [ { } ] ; : ' " < , . > / ? .
New Password:	<input type="text"/>	
Confirm Password:	<input type="text"/>	

Apply

Cancel

**NOTICE**

To enhance system security, change the password to a password that meets security requirements after the first successful login. It is recommended that you change the password periodically.

2. Click **Apply**.

### 3.5.5.6 Time Setting

1. In the navigation tree on the left, choose **System Management > Time Setting**. In the pane on the right, set the parameters related to the system time, including the SNTP server, time zone, and daylight saving time (DST), as shown in [Figure 3-31](#).

**Figure 3-31** Time Setting

### Time Setting

On this page, you can configure the SNTP protocol, time zone, and DST to obtain the accurate time.

Automatically Synchronize The Network Time Server

Primary SNTP Server:

Secondary SNTP Server:

Time Zone:

Time Synchronization Period:  (s)

WAN Name:

Enable DST

DST Start Time:

Hour:  Minute:  Second:

DST End Time:

Hour:  Minute:  Second:

2. Click **Apply**.

**Table 3-12** describes the parameters related to the system time.

**Table 3-12** Parameters related to the system time

Parameter	Description
Automatically Synchronize The Network Time Server	Indicates whether to enable the auto synchronization network time server, that is, SNTP server.
Primary SNTP Server	Indicates the primary SNTP server.
Secondary SNTP Server	Indicates the secondary SNTP server.
Time Zone	Indicates the time zone.
Time Synchronization Period	Indicates the interval for the edge ONT to synchronize time with the SNTP server.

Parameter	Description
WAN Name	Indicates the name of the WAN port for network time synchronization.
Enable DST	Indicates whether to enable the DST.
DST Start Time	Indicates the DST start time.
DST End Time	Indicates the DST end time.

### 3.5.5.7 Backup and Recovery

In the navigation tree on the left, choose **System Management > Backup And Recovery**. In the pane on the right, you can export, import, and restore factory configuration operations.

**Figure 3-32** Backup and recovery

#### Backup And Recovery

On this page, you can export, import, and restore factory configuration operations.

Export Configuration File

Export Configuration File

Import Configuration File

Configuration File:

Browse...

Import Configuration File

Restoring Factory Settings

Restoring Factory Settings

### 3.5.5.8 Open Source Software Notice

In the navigation tree on the left, choose **System Management > Open Source Software Notice**. In the pane on the right, you can view the open source software notice for the product, as shown in **Figure 3-33**.



### Figure 3-33 Open Source Software Notice

#### OPEN SOURCE SOFTWARE NOTICE

This part contains an open source software notice for this product. The open source software licenses are granted by the respective right holders. The open source licenses prevail all other license information with regard to the respective open source software contained in the product.

#### Warranty Disclaimer

**THE OPEN SOURCE SOFTWARE IN THIS PRODUCT IS DISTRIBUTED IN THE HOPE THAT IT WILL BE USEFUL, BUT WITHOUT ANY WARRANTY, WITHOUT EVEN THE IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SEE THE APPLICABLE LICENSES FOR MORE DETAILS.**

#### Copyright Notice and License Texts

##### **License: Apache License V2.0**

Apache License

Version 2.0, January 2004

<http://www.apache.org/licenses/>

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

### 3.5.5.9 Indicator Status Management

In the navigation tree on the left, choose **System Management > Indicator Status Management**. In the pane on the right, you can set the indicator switch of a device, and specify a time period during which all indicators are always off, as shown in [Figure 3-34](#).

**Figure 3-34** Indicator status management

### Indicator Status Management

On this page, you can set the indicator switch of a device. You can configure an indicator off period if you set Indicator switch to Off. An indicator is always off if you do not specify an indicator off period.

#### Indicator Switch Configuration

Indicator Switch  On  Off

#### Indicator Off Period Configuration

New Delete

	Start time	End time
<input type="checkbox"/>	21:00	23:00
----	----	----

Indicator Off Period Start time  :  End time  :  (00:00-23:59)

Apply Cancel

## 3.5.5.10 Security Self-Check

In the navigation tree on the left, choose **System Management > Security Self-Check**. In the pane on the right, you can check insecure configuration items in the system. Click **Start** to start the check, as shown in [Figure 3-35](#).

**Figure 3-35** Security self-check

### Security Self-Check

On this page, you can check for insecure configuration items in the system. Click Start to start the check. The previous check results are displayed by default.

Start

Check Item	Conclusion	Description
------------	------------	-------------

## 3.5.6 Maintenance Diagnosis

This topic describes how to configure the Maintenance Diagnosis through the web page.

### 3.5.6.1 Maintenance

In the navigation tree on the left, choose **Maintenance Diagnosis > Maintenance**.

1. In the pane on the right, enter the target IP address or host name in Target and WAN name, and then click Start, as shown in [Figure 3-36](#).

**Figure 3-36** Ping test

### Maintenance

On this page, you can use the maintenance and diagnosis function to check LAN or Internet connectivity and the basic functions of main chips.

Note: Hardware fault detection may not find out all hardware faults. This operation is intended only for maintenance engineers and must be performed with caution. Data services are interrupted during hardware fault detection.

#### Ping Test

Target:	<input type="text"/>	*
Port Name:	<input type="text"/>	▼
Data Block Size:	<input type="text" value="56"/>	(32-65500; default without inputting: 56)
Repetitions:	<input type="text" value="4"/>	(1-3600; default without inputting: 4)
Maximum Timeout Time:	<input type="text" value="10"/>	(1-4294967s; default without inputting: 10)
DSCP Value:	<input type="text" value="0"/>	(0-63; default without inputting: 0)

Start

Stop

#### Traceroute Test

Target:	<input type="text"/>	*
Port Name:	<input type="text"/>	▼
Data Block Size:	<input type="text" value="38"/>	(38-32768; default without inputting: 38)
Protocol Type:	<input type="text" value="AUTO"/>	▼

Start

Stop

- If the ping test is successful, The result is displayed as **PASS**, that is, the edge ONT can interwork with the device with the destination IP address.
  - If the ping test fails, The result is displayed as **FAIL**, that is, the edge ONT cannot interwork with the device with the destination IP address.
2. In the pane on the right, click **Start Hardware Fault Detection** to start hardware fault detection, as shown in [Figure 3-37](#).

**Figure 3-37** Hardware fault detection

### Hardware Fault Detection

Start Hardware Fault Detection

### 3.5.6.2 User Log

In the navigation tree on the left, choose **Maintenance Diagnosis > User Log**. In the pane on the right, click **Download Log File**. In the dialog box that is displayed, click **Save**, specify the path of saving the log file, and save the file to the local disk, as shown in **Figure 3-38**.

**Figure 3-38** User Log

#### User Log

On this page, you can download and query user logs.

#### Download and View Logs

**Download Log File**

Log Type:

```
Manufacturer:Huawei Technologies Co., Ltd;
ProductClass:K572;
SerialNumber:
IP:192.168.101.1;
HWVer:
SWVer:V5R024
[Error][Alarm-Log] AlarmID:104001,AlarmLevel:Error,Device reset. Cause: System re
[Notice][Run-Log] SourceId[691] : Delete Cert Instance, inst[3], path[/mnt/jffs2/cert
[Notice][Event-Log] portisolate:ctp1 change to layer3 port,enable isolate
[Notice][Event-Log] portisolate:ctp2 change to layer3 port,enable isolate
[Notice][Event-Log] portisolate:ctp3 change to layer3 port,enable isolate
[Notice][Event-Log] portisolate:ctp4 change to layer3 port,enable isolate
[Notice][Event-Log] portisolate:rcv_pkttype:1,ctp3 disable isolate,pkt smac:2c:58:b
[Critical][Alarm-Log] Integrity check ok
[Critical][Run-Log] [cplugin] open install dir err
[Critical][Run-Log] [kernelapp.cpk] install ret [0]
[Error][Alarm-Log] AlarmID:104509,AlarmLevel:Error,Software upgrading.Terminal:C
[Critical][Config-Log] Terminal:CEC TOOL (/) Result:Fail Type:Set Internet Gateway De
```

- Save Log is enabled by default, It can not be configured on the Web page.
- You cannot configure Log Level, which indicates the level of the saved log. The log whose level is equal to or higher than the debug-level log is saved.
- Click **Download Log File**. In the dialog box that is displayed, click Save, specify the path for saving the log file, and save the log file to the local disk.
- Select a type from the Log Type drop-down list box to view different types of logs. Options are **All-Log**, **Config-Log**, **Shell-Log**, and **Alarm-Log**.

#### NOTICE

When IE8 is used for log file downloading and you click the save button 10s-over later after downloading, the downloaded log file is incomplete.

### 3.5.6.3 AP Log

In the navigation tree on the left, choose **Maintenance Diagnosis > AP Log**. In the pane on the right, click **Download Log File**. In the dialog box that is displayed, click **Save**, specify the path of saving the log file, and save the file to the local disk, as shown in **Figure 3-39**.

**Figure 3-39** AP Log

#### AP Log

If the AP device is connected, you will be able to query and download the AP's logs on this page.

Download And View Logs

[Download Log File](#)

```
Manufacturer:Huawei Technologies Co., Ltd;
ProductClass:K572;
SerialNumber:
IP:192.168.101.1;
HWVer:
SWVer:V5R024
[Notice] BBSP Set PortIndex:1 LinkMode Nego:1 Speed:5 Duplex:2
[Notice] BBSP Set PortIndex:2 LinkMode Nego:1 Speed:5 Duplex:2
[Notice] BBSP Set PortIndex:3 LinkMode Nego:1 Speed:5 Duplex:2
[Notice] BBSP Set PortIndex:4 LinkMode Nego:1 Speed:5 Duplex:2
[Notice] ACCESS Set PortIndex:1 Enable:1
[Notice] ACCESS Set PortIndex:2 Enable:1
[Notice] ACCESS Set PortIndex:3 Enable:1
[Notice] ACCESS Set PortIndex:4 Enable:1
[Notice] BBSP Set PortIndex:1 LinkMode Nego:1 Speed:5 Duplex:2
[Notice] BBSP Set PortIndex:2 LinkMode Nego:1 Speed:5 Duplex:2
[Notice] BBSP Set PortIndex:3 LinkMode Nego:1 Speed:5 Duplex:2
[Notice] BBSP Set PortIndex:4 LinkMode Nego:1 Speed:5 Duplex:2
[Notice] BBSP Set PortIndex:1 LinkMode Nego:1 Speed:5 Duplex:2
```

#### NOTICE

When IE8 is used for log file downloading and you click the save button 10s-over later after downloading, the downloaded log file is incomplete.

### 3.5.6.4 Firewall Log

In the navigation tree on the left, choose **Maintenance Diagnosis > Firewall Log**. In the pane on the right, you can view logs and download log files, as shown in **Figure 3-40**.

### Figure 3-40 Firewall Log Firewall Log

On this page, you can configure, download, and query a firewall log.

Enable Firewall Log  (If enabled, device forwarding performance will be deteriorated.)

	Log Rule Status	Log Access Direction	Log Rule Action
--	--	--	--

Download and View Logs

```
Manufacturer:Huawei Technologies Co., Ltd;  
ProductClass:K572;  
SerialNumber:*****;  
IP:192.168.101.1;  
HWVer:*****;  
SWVer:V5R024*****;
```

- Click **Enable Firewall Log** to enable or disable the function. If enabled, device forwarding performance will be deteriorated.
- Click **New** to configure the firewall rules.
- Click **Download Log File**. In the dialog box that is displayed, click **Save**, specify the path for saving the log file, and save the log file to the local disk.

#### NOTICE

When IE8 is used for log file downloading and you click the save button 15s-over later after downloading, the downloaded log file is incomplete.

### 3.5.6.5 Debug Log

In the navigation tree on the left, choose **Maintenance Diagnosis > Debug Log**. In the pane on the right, click **Download Log File**. In the dialog box that is displayed, click **Save**, specify the path of saving the log file, and save the file to the local disk, as shown in [Figure 3-41](#).

**Figure 3-41** Debug Log  
Debug Log

On this page, you can download and query debug logs.

Download And View Logs

[Download Log File](#)

Log Type:

```
Manufacturer:Huawei Technologies Co., Ltd;
ProductClass:K572;
SerialNumber:
IP:192.168.101.1;
HWVer:
SWVer:V5R024

[Debug][Debug-Log] static:[dhcpd]receive Discover, xid[24540a8e], mac[f4-30-8b-2
[Critical][Debug-Log] static:[dhcpd]xid[24540a8e] choose [main] address pool
[Debug][Debug-Log] static:[dhcpd]send Offer, xid[24540a8e], mac[f4-30-8b-26-*.
[Debug][Debug-Log] static:[dhcpd]receive Request, xid[24540a8e], mac[f4-30-8b-2
[Debug][Debug-Log] static:[dhcpd]send Ack, xid[24540a8e], mac[f4-30-8b-26-*.
[Debug][Debug-Log] static:[dhcpd]send Ack, xid[24540a8e], mac[f4-30-8b-26-*.
[Debug][Debug-Log] static:[dhcpd]receive Discover, xid[f9719441], mac[f6-d5-b4-0
[Critical][Debug-Log] static:[dhcpd]xid[f9719441] choose [main] address pool
[Debug][Debug-Log] static:[dhcpd]send Offer, xid[f9719441], mac[f6-d5-b4-00-*.
[Debug][Debug-Log] static:[dhcpd]receive Discover, xid[f9719441], mac[f6-d5-b4-0
[Critical][Debug-Log] static:[dhcpd]xid[f9719441] choose [main] address pool
[Debug][Debug-Log] static:[dhcpd]receive Request, xid[f9719441], mac[f6-d5-b4-0
```

Click **Download Log File**. In the dialog box that is displayed, click **Save**, specify the path for saving the log file, and save the log file to the local disk.

#### NOTICE

When IE8 is used for log file downloading and you click the save button 10s-over later after downloading, the downloaded log file is incomplete.

### 3.5.6.6 Intrusion Detect Log

In the navigation tree on the left, choose **Maintenance Diagnosis > Intrusion Detect Log**. In the pane on the right, you can download and query intrusion detect logs, as shown in [Figure 3-42](#).

### Figure 3-42 Intrusion Detect Log

#### Intrusion Detect Log

On this page, you can download and query intrusion detect logs.

Download And View Logs

[Download Log File](#)

```
Manufacturer:Huawei Technologies Co., Ltd;  
ProductClass:K572;  
SerialNumber: ;  
IP:192.168.101.1;  
HWVer: ;  
SWVer:V5R024 ;
```

Click **Download Log File**. In the dialog box that is displayed, click **Save**, specify the path for saving the log file, and save the log file to the local disk.

#### NOTICE

When IE8 is used for log file downloading and you click the save button 10s-over later after downloading, the downloaded log file is incomplete.

### 3.5.6.7 Fault Info Collect

In the navigation tree on the left, choose **Maintenance Diagnosis > Fault Info Collect**. In the pane on the right, click **Start** to collect edge ONT fault information, and click **Show Wi-Fi Diagnosis** to view edge ONT fault information, as shown in [Figure 3-43](#).

Figure 3-43 Fault Info Collect

#### Enable Collect Fault Information

On this page, you can collect and download fault information.

Enable Collect Fault Information

[Start](#)

[Download](#)

Collecting Wi-Fi Information

[Show Wi-Fi Diagnosis](#)



 NOTE

- After the information is collected, click **Download** to download the collected information to a local directory.
- When IE8 is used for fault info collect and you click the save button 10s-over later after downloading, the downloaded fault info collect is incomplete.

### 3.5.6.8 Remote Mirror

1. In the navigation tree on the left, choose **Maintenance Diagnosis > Remote Mirror**, as shown in [Figure 3-44](#).

**Figure 3-44** Remote Mirror

#### Remote Mirror

On this page, you can use the mirror function to mirror the packets that are received and transmitted by the CPU. Ensure that all ICMP options are disabled for the firewall on your PC before you use this function.

#### Packet Capture By Mirroring

Status: **Stop**

Source IP Address: \*

Destination IP Address: \*

Direction: \*

Interface: \*

#### Real-time Packet Capture

Type of the captured packets: \*

Duration of packet capture:  (5-43200) minutes

Packet capture status:

Packets sent to and transmitted from the CPU can be remotely Obtained for analysis based on the configuration.

- Source IP Address: indicates the IP address of the WAN port where remote mirroring is performed.
- Destination IP Address: indicates the IP address of the host where the result is located.
- Type of the captured packets: indicates the type of the captured packets. It can be set to **Broadband** and **Wi-Fi**.

2. click **Start**.

 **NOTE**

Some third-party plug-ins, such as Google Chrome Frame, may lead to downloading failure. If such a failure occurs, disable the plug-in.

Based on industry experience, the mirroring feature may involve obtaining personal data of users and the content of users' communications (the product does not save, parse, or process such information) for the purpose of safeguarding network operation and protecting services. Huawei alone is unable to collect or save the personal data of users and the content of users' communications. It is suggested that you activate the interception-related functions based on the applicable laws and regulations in terms of purpose and scope of usage. You are obligated to take considerable measures to ensure that the personal data of users and the content of users' communications are fully protected when the personal data and the content are being used and saved.

The command execution may involve obtaining the personal data of users or the content of users' communications for the purpose of safeguarding network operation and protecting services. Huawei alone is unable to collect or save the personal data of users and the content of users' communications. It is suggested that you activate the interception-related functions based on the applicable laws and regulations in terms of purpose and scope of usage. You are obligated to take considerable measures to ensure that the personal data of users and the content of users' communications are fully protected when the personal data and the content are being used and saved.

# 4 Web Page Reference (Bridge mode)

## 4.1 Homepage

On the homepage, you can view the current home network topology, Internet


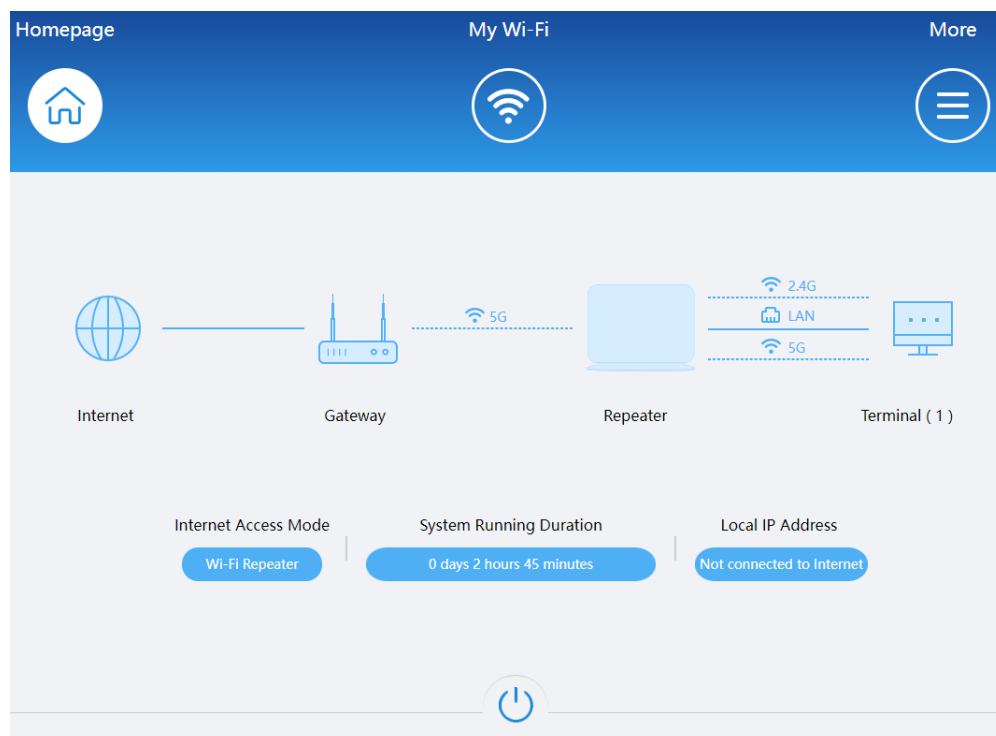
access mode, system running duration, and local IP address. A click on  in the lower part of the page restarts the device.

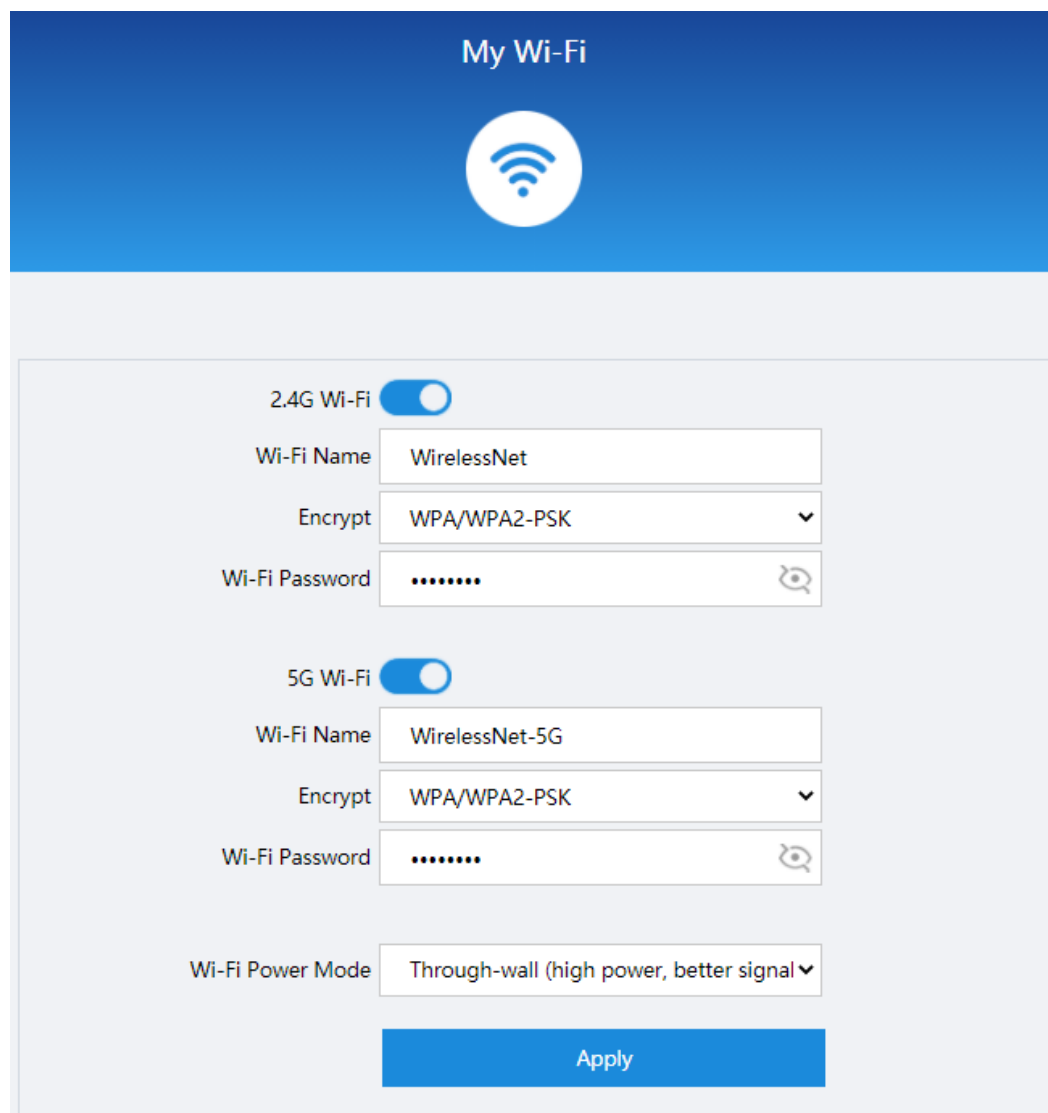
Figure 4-1 Homepage



## 4.2 My Wi-Fi

On this page, you can configure Wi-Fi parameters.

Figure 4-2 My Wi-Fi



The screenshot shows the 'My Wi-Fi' configuration interface. It features a blue header with the title 'My Wi-Fi' and a Wi-Fi icon. Below the header, there are two sections for configuring 2.4G and 5G Wi-Fi. Each section has a toggle switch, a text input for the Wi-Fi Name, a dropdown for the encryption type, and a password input field with a visibility toggle. At the bottom, there is a 'Wi-Fi Power Mode' dropdown and an 'Apply' button.

Band	Wi-Fi Name	Encrypt	Wi-Fi Password
2.4G Wi-Fi	WirelessNet	WPA/WPA2-PSK	.....
5G Wi-Fi	WirelessNet-5G	WPA/WPA2-PSK	.....

Wi-Fi Power Mode: Through-wall (high power, better signal)

Apply

### NOTICE

To enhance system security, change the password to a password that meets security requirements after the first successful login. It is recommended that you change the password periodically.

**Table 4-1** Wi-Fi parameters

Parameter	Description
2.4G Wi-Fi/5G Wi-Fi	Enable or disable Wi-Fi.
Wi-Fi Name	Wi-Fi name.
Encrypt	Indicates the authentication mode for the STA to request access to the wireless network. The mode can be OPEN, WPA2-PSK, WPA/WPA2-PSK. It is set to WPA/WPA2-PSK by default.
Wi-Fi Password	Wi-Fi password. This parameter is available when <b>Encrypt</b> is set to <b>WPA2-PSK, WPA/WPA2-PSK, WPA3-SAE, WPA2/WPA3-PSK and SAE</b> .
Wi-Fi Power Mode	The mode can be set to the following as required: <ul style="list-style-type: none"><li>• Through-wall (high power, better signal)</li><li>• Standard (standard power, common signal)</li><li>• Sleep (low power, weak signal)</li></ul>

## 4.3 More

A click on **More** displays the page for configuring more functions.

### 4.3.1 System Information

This topic describes the basic information about an edge ONT on the web page, including the device, WLAN information.

#### 4.3.1.1 Device Information

In the navigation tree on the left, choose **System Info > Device Information**. In the pane on the right, you can view the product name, hardware version, and software version, as shown in [Figure 4-3](#).

**Figure 4-3** Device Information

## Device Information

[On this page, you can view basic device information.](#)

### Basic Information

Device Type:	K572
Description:	OptiXstar K572 Repeater Terminal (PRODUCT ID: ██████████)
MAC:	00:25:9E:87: ████████
Hardware Version:	██████
Software Version:	V5R024 ████████
Manufacture Info:	██
CPU Usage:	9%
Memory Usage:	63%
Custom Info:	████████████████████
System Time:	██████████ 02:46:27+00:00

[Refresh](#)

### Secure Boot Settings

Secure Boot:	Enable
Hash Value of Level-1 BIOS:	██
Hash Value of Level-2 BIOS:	██
Firmware Package Signature Result:	<a href="#">Download</a>

## 4.3.1.2 WLAN Information

In the navigation tree on the left, choose **System Info > WLAN Information**. Then, in the pane on the right, you can query the information such as WLAN status, Wi-Fi packet statistics, and STA information, as shown in [Figure 4-4](#).

### Figure 4-4 WLAN Information

#### WLAN Information

On this page, you can query the WLAN information, WLAN packet statistics, and SSID information.

- 2.4 GHz wireless network information
  5 GHz wireless network information

Wireless Configuration Information	Neighbor AP and STA Information	Wireless Statistics	Wireless Diagnosis
------------------------------------	---------------------------------	---------------------	--------------------

#### WLAN Info

WLAN Status: Enabled

WLAN Channel: 5

#### SSID Information

SSID Index	SSID Name	Security Configuration	Authentication Mode	Encryption Mode
1	2.4GSSID111	Configured	WPA/WPA2 PreSharedKey	TKIP&AES

Wireless Configuration Information	Neighbor AP and STA Information	Wireless Statistics	Wireless Diagnosis
------------------------------------	---------------------------------	---------------------	--------------------

#### STA Information

Query

MAC Address	SSID Name	Connection Duration (s)	Sending Rate (Mbps)	Receiving Rate (Mbps)	Signal Strength (dBm)	Noise (dBm)	Signal-to-Noise Ratio (dB)	Signal Quality (dBm)	Antenna Num	11k	11v	DualBand
<div style="border: 1px solid gray; height: 15px; width: 100%;"></div>												

#### STA Boost Function

Query

STA Index	MAC Address	Online Status	Release Time
<div style="border: 1px solid gray; height: 15px; width: 100%;"></div>			

#### Neighbor AP Information

Query

Note: Querying neighbor AP information may disconnect all STA connections.

SSID Name	MAC Address	Network Type	Channel	Signal Strength (dBm)	Noise (dBm)	DTIM Interval	Beacon Period (ms)	Authentication Mode	Working Mode	Max. Rate (Mbps)	Multi-Link
<div style="border: 1px solid gray; height: 15px; width: 100%;"></div>											

Wireless Configuration Information	Neighbor AP and STA Information	Wireless Statistics	Wireless Diagnosis
------------------------------------	---------------------------------	---------------------	--------------------

WLAN Packet Statistics

SSID Index	SSID Name	Receive (RX)				Transmit (TX)			
		Bytes	Packets	Error	Discarded	Bytes	Packets	Error	Discarded
1	2.4GSSID111	0	0	0	0	0	0	0	0

STA Event Log

[Download Log File](#)

```

Manufacturer:Huawei Technologies Co., Ltd;
ProductClass:K572;
SerialNumber:
IP:192.168.101.1;
HWVer:
SWVer:V5R024;

693883 [5G] [vap4] hmac_config_down_sync_all: WLAN DOWN success
063053 [2G] [vap0] hmac_config_down_sync_all: WLAN DOWN success
252654 [2G] [vap0] hmac_config_down_sync_all: WLAN DOWN success
842610 [5G] [vap4] hmac_config_down_sync_all: WLAN DOWN success
474212 [5G_STA] [vap9] hmac_config_down_sync_all: WLAN DOWN success
101281 [5G_STA] [vap9] hmac_config_connect_check:check pass, BSSID[AC:B3:B5:44
101311 [5G_STA] [vap9] hmac_mgmt_encap_auth_req:Send Auth to ROOT AP, BSSID
605610 [5G_STA] [vap9] hmac_mgmt_encap_auth_req:Send Auth to ROOT AP, BSSID
760962 [5G_STA] [vap9] hmac_mgmt_encap_asoc_req_sta:send assoc req to ROOT /
772643 [5G_STA] [vap9] hmac_assoc_rsp_check::rcv assoc response, status code:0
776354 [5G_STA] [vap9] hmac_mgmt_rx_addba_req_process:: uc_tid[0], uc_status[0]
050010 [2G] [vap0] hmac_config_down_sync_all: WLAN DOWN success
    
```



Wireless Configuration Information	Neighbor AP and STA Information	Wireless Statistics	Wireless Diagnosis
------------------------------------	---------------------------------	---------------------	--------------------

### WLAN Health Diagnosis Report

#### WLAN Information

2.4G WLAN Status:	Enabled
Working Mode:	802.11b/g/n/ax/be
Channel check:	6(Auto)
Frequency bandwidth mode:	20 MHz
Current working frequency bandwidth:	20 MHz
Whitelist/Blacklist filtering:	Off
MAC address check:	OK
Difference of antenna signal strength:	RSSI difference between antennas is less than or equal to 10.
Interference:	335
Calibration parameter:	Normal

## 4.3.2 WLAN

This topic describes how to configure WLAN through the Web page.

### 4.3.2.1 Wi-Fi Advanced Configuration

1. In the navigation tree on the left, choose **WLAN > Wi-Fi Advanced Network Settings**. In the right pane, configure the advanced parameters of 2.4G and 5G Wi-Fi, as shown in [Figure 4-5](#).

**Figure 4-5** WLAN Advanced Configuration  
WLAN Advanced Configuration

You can customize the wireless network to adapt to various wireless network environments.

### 2.4G Wi-Fi

Broadcast SSID:

Channel: Automatic

Channel Width: 20 MHz

Mode: 802.11b/g/n/ax/be

If the Wi-Fi cannot be found or connected when 802.11be is enabled, upgrade the wireless network adapter driver.

### 5G Wi-Fi

Broadcast SSID:

Channel: Automatic

Channel Width: Auto 20/40/80/160 MHz

Mode: 802.11a/n/ac/ax/be

If the Wi-Fi cannot be found or connected when 802.11be is enabled, upgrade the wireless network adapter driver.

Apply

Cancel

2. Click **Apply**.

**Table 4-2** describes the WLAN advanced parameters.

**Table 4-2** WLAN advanced parameters

Parameter	Description
Broadcast SSID	<p>Indicates whether to enable or hide broadcast.</p> <ul style="list-style-type: none"> <li>• If the option box is selected, it indicates that the SSID broadcast function is enabled. The edge ONT periodically broadcasts the SSID, that is, the name of the wireless network. In this way, any STA can search for the wireless network.</li> <li>• If the option box is not selected, it indicates that the SSID broadcast function is disabled. The SSID is hidden, and the STA cannot search for the wireless network. The SSID can be obtained only through a request.</li> </ul>
Channel	Indicates the channel of the wireless network.
Channel Width	Indicates the wireless channel width.
Mode	Indicates the supported wireless network mode.

### 4.3.2.2 Smart Network Connection

In the navigation tree on the left, choose **WLAN > Smart Network Connection**. In the right pane, set whether parameter configurations are synchronized from the primary gateway, as shown in [Figure 4-6](#).

**Figure 4-6** Smart Network Connection

#### Smart Network Connection

On this page, you can set whether parameter settings are synchronized from the primary gateway.

- Enable wireless configuration synchronization with the smart gateway
- Enable synchronous repeat parameters to Access WLAN
- Enable to synchronize with the gateway smartlink to force the use of https connection

#### WiFi Cascading Frequency Option

- 2.4G (wide coverage, applicable to the scenario where the upstream device is far away)
- 5G (high rate, applicable to the scenario where the upstream device is nearby)
- Auto (automatically select the cascading frequency band)

### 4.3.2.3 Wi-Fi Repeater

1. In the navigation tree on the left, choose **WLAN > Wi-Fi Repeater**. In the right pane, click **Modify Configuration** and select the desire Wi-Fi network and enter the correct Wi-Fi password if required as shown in [Figure 4-7](#).

**Figure 4-7** Wi-Fi Repeater

### Wi-Fi Repeater

The Wi-Fi Repeater mode allows you to connect to another router over Wi-Fi. The two routers work at the same time to provide better coverage for a large area.

Select the wireless network to be connected

Select the Wi-Fi to be connected. [Re-scan](#)

WPA2-EAP	
WPA2-EAP	
OPEN	
WPA2-PSK	
WPA/WPA2-PSK	

Add other networks

Wi-Fi Name

Wi-Fi Password

After the connection is set up, the Wi-Fi name and password of the local router are the same as those of the active router.

[Cancel](#) [Connect](#)

2. Click **Connect**.

#### 4.3.2.4 Multi-AP

1. In the navigation tree on the left, choose **WLAN > Multi-AP**. In the right pane, set the mesh device role to controller or agent, as shown in [Figure 4-8](#).

**Figure 4-8** Multi-AP  
Multi-AP

On this page, you can set EasyMesh device role to Controller, Agent.

Enable EasyMesh	<input checked="" type="checkbox"/> (Need to restart to take effect)
Role Settings	
Role Setting	<input checked="" type="radio"/> Controller <input type="radio"/> Agent
Current Role	Controller
<input type="button" value="Apply"/>	

2. Click **Apply**.

## 4.3.3 Security Configuration

This topic describes how to configure the security through the web page.

### 4.3.3.1 Device Access Control

1. In the navigation tree on the left, choose **Security Configuration > Device Access Control**. In the pane on the right, configure the rule of edge ONT access control, as shown in [Figure 4-9](#).

---

 **DANGER**

Complete network security planning before enabling remote access control to ensure that edge ONTs are logged in to in secure network conditions. After the edge ONT login operations are complete, disable remote access control in a timely manner. If you do not complete network security planning or do not disable remote access control in a timely manner, the network may become faulty or be attacked, and Huawei will not be responsible for any related subsequences.

---

**Figure 4-9** Device Access Control  
Device Access Control

On this page, you can enable or disable permissions to access the device.

#### LAN Service

Enable the LAN-side PC to access the device using Telnet:

Enable the LAN-side PC to access the device using SSH:

#### Wi-Fi Service

Enable devices on the Wi-Fi side to access web pages:

Enable the PC on the Wi-Fi side to access the device using Telnet:

Apply

Cancel

2. Click **Apply**.

## 4.3.4 System Management

This topic describes how to configure the System Management through the web page.

### 4.3.4.1 Upstream Network Port Settings

1. In the navigation tree on the left, choose **System Management > Upstream Network Port Settings**. In the pane on the right, set a fixed upstream network port or enable automatic selection of the upstream network port, as shown in [Figure 4-10](#).

**Figure 4-10** Upstream Network Port Settings

### Upstream Network Port Settings

On this page, you can set a fixed upstream network port or enable automatic selection of the upstream network port.

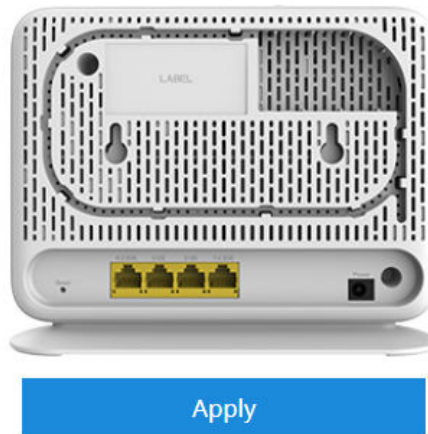
Upstream Network Port  
Settings

Select an upstream network port automatically

Fixed upstream network port

In this mode, LAN4 is the fixed WAN port.

Please manually set the WAN connection based on the networking configuration provided by your ISP.



2. Click **Apply**.

#### 4.3.4.2 TR-069

1. In the navigation tree on the left, choose **System Management > TR-069**. In the pane on the right, set the parameters related to the interconnection between the ONT and the TR-069 server, as shown in **Figure 4-11**.

### Figure 4-11 TR-069 ACS Configuration

On this page, you can set the ACS parameters, port mapping function of the primary gateway, set the authentication password of the SSL certificate, and import the corresponding SSL certificate.

#### ACS Parameter Settings

Enable ACS Management:

Enable Periodic Informing:

Informing Interval:  \*[1-2147483647](s)

Informing Time:  yyyy-mm-ddThh:mm:ss (for example, 2009-12-20T12:23:34)

ACS URL:  \*

ACS User Name:

ACS Password:

Connection Request User Name:

Connection Request Password:

DSCP:  (0-63)

#### Automatic configuration of the primary gateway portMapping port

Enable:

External Port: --



### STUN Server Management

Enable STUN:

Minimum STUN Keep-alive Period:  \*(s)

Maximum STUN Keep-alive Period:  \*(s)

STUN Server Address:  \*

STUN Server Port:  \*

STUN Username:  \*

STUN Password:  \*

2. Click **Apply**.

**Table 4-3** describes the TR-069 parameters.

**Table 4-3** TR-069 parameters

Parameter	Description
ACS Parameter Settings	
Enable ACS Management	Indicates whether to enable the <b>ACS Management</b> .
Enable Periodic Informing	Indicates whether to enable the notification function. <ul style="list-style-type: none"> <li>If the notification function is enabled, the ONT actively sends a connection request to the TR-069 server.</li> <li>If the notification function is disabled, the ONT does not actively send a connection request to the TR-069 server.</li> </ul> When the notification function is enabled, the <b>Informing Interval</b> and <b>Informing Time</b> parameters can be set.
Informing Interval	Indicates the interval for the ONT to send a connection request to the TR-069 server.
Informing Time	Indicates the time for the ONT to send a connection request to the TR-069 server.
ACS URL	Indicates the address of the TR-069 server to which the ONT sends a connection request.
ACS User Name	Indicates the user name for the ONT to register with the TR-069 server.
ACS Password	Indicates the password for the ONT to register with the TR-069 server.

Parameter	Description
Connection Request User Name	Indicates the user name to be carried when the TR-069 server initiates a connection request to the ONT.
Connection Request Password	Indicates the password to be carried when the TR-069 server initiates a connection request to the ONT.
DSCP	Defined by RFC2474 "Definition of the Differentiated Services Field". Differentiated Services Code Point (DSCP) uses code values for priority marking. DSCP can be customized for carriers based on service requirements so that devices on a network perform QoS based on the DSCP value.
Automatic configuration of the primary gateway portMapping port	
Enable	Indicates whether to enable the port mapping function of the primary gateway.
External Port	Indicates an external port.
STUN Server Management	
Enable STUN	Enables or disables the use of STUN by the device. This applies only to the use of STUN in association with the ACS to allow UDP Connection Requests.
Minimum STUN Keep-alive Period	If STUN Is enabled, the minimum period, in seconds, that STUN Binding Requests can be sent by the device for the purpose of maintaining the binding in the Gateway. This limit applies only to Binding Requests sent from the UDP Connection Request address and port, and only those that do not contain the BINDING-CHANGE attribute. This limit does not apply to retransmissions following the procedures defined in [RFC3489].
Maximum STUN Keep-alive Period	If STUN Is enabled, the maximum period, in seconds, that STUN Binding Requests MUST be sent by the device for the purpose of maintaining the binding in the Gateway. This applies specifically to Binding Requests sent from the UDP Connection Request address and port. A value of -1 indicates that no maximum period is specified.
STUN Server Address	Host name or IP address of the STUN server for the CPE to send Binding Requests if STUN is enabled via <i>STUNEnable</i> . If an empty string and <i>STUNEnable</i> is <i>true</i> , the CPE MUST use the address of the ACS extracted from the host portion of the ACS URL.

Parameter	Description
STUN Server Port	Port number of the STUN server for the CPE to send Binding Requests if STUN is enabled via <i>STUNEnable</i> . By default, this SHOULD be the equal to the default STUN port, 3478.
STUN Username	If not an empty string, the value of the STUN USERNAME attribute to be used in Binding Requests (only if message integrity has been requested by the STUN server). If an empty string, the CPE MUST NOT send STUN Binding Requests with message integrity.
STUN Password	The value of the STUN Password to be used in computing the MESSAGE-INTEGRITY attribute to be used in Binding Requests (only if message integrity has been requested by the STUN server). When read, this parameter returns an empty string, regardless of the actual value.

#### 4.3.4.3 Software Upgrade

1. In the navigation tree on the left, choose **System Management > Software Upgrade**. In the pane on the right, select the target software version of the device. Click **Upgrade** to upgrade the software of the device, as shown in [Figure 4-12](#).

**Figure 4-12** Software Upgrade

#### Software Upgrade

On this page, you can use the firmware upgrade function to upgrade the software of the terminal to the target version.

Firmware File:

2. After the upgrade is successful, a message is displayed indicating that the device needs to be reset. Click **Restart**. The configuration data takes effect after the device is reset.

#### 4.3.4.4 Account Management

1. In the navigation tree on the left, choose **System Management > Account Management**. In the pane on the right, change the password of the current login user, as shown in [Figure 4-13](#).

**Figure 4-13** Account Management

### Account Management

On this page, you can change the password of the current login user to ensure security and make it easy to remember.

#### Change Password

Old Password:	<input type="text"/>	1. The password must contain at least 8 characters.
New Password:	<input type="text"/>	2. The password must contain at least two of the following combinations: digits, uppercase letters, lowercase letters, and special characters. Special characters can be the following: ` ~ ! @ # \$ % ^ & * ( ) - _ = + \   [ { } ] ; : ' " < , . > / ? .
Confirm Password:	<input type="text"/>	

Apply

Cancel

#### NOTICE

To enhance system security, change the password to a password that meets security requirements after the first successful login. It is recommended that you change the password periodically.

2. Click **Apply**.

### 4.3.4.5 Time Setting

1. In the navigation tree on the left, choose **System Management > Time Setting**. In the pane on the right, set the parameters related to the system time, including the SNTP server, time zone, and daylight saving time (DST), as shown in [Figure 4-14](#).

**Figure 4-14** Time Setting

### Time Setting

On this page, you can configure the SNTP protocol, time zone, and DST to obtain the accurate time.

Automatically Synchronize The Network Time Server

Primary SNTP Server:

Secondary SNTP Server:

Time Zone:

Time Synchronization Period:  \* (s)

Enable DST

DST Start Time:

Hour:  Minute:  Second:

DST End Time:

Hour:  Minute:  Second:

2. Click **Apply**.

**Table 4-4** describes the parameters related to the system time.

**Table 4-4** Parameters related to the system time

Parameter	Description
Automatically Synchronization The Network Time Server	Indicates whether to enable the auto synchronization network time server, that is, SNTP server.
Primary SNTP Server	Indicates the primary SNTP server.
Secondary SNTP Server	Indicates the secondary SNTP server.
Time Zone	Indicates the time zone.
Time Synchronization Period	Indicates the interval for the edge ONT to synchronize time with the SNTP server.
Enable DST	Indicates whether to enable the DST.

Parameter	Description
DST Start Time	Indicates the DST start time.
DST End Time	Indicates the DST end time.

#### 4.3.4.6 Backup and Recovery

In the navigation tree on the left, choose **System Management > Backup And Recovery**. In the pane on the right, you can export, import, and restore factory configuration operations.

**Figure 4-15** Backup and recovery

##### Backup And Recovery

On this page, you can export, import, and restore factory configuration operations.

Export Configuration File

Export Configuration File

Import Configuration File

Configuration File:

Browse...

Import Configuration File

Restoring Factory Settings

Restoring Factory Settings

#### 4.3.4.7 Open Source Software Notice

In the navigation tree on the left, choose **System Management > Open Source Software Notice**. In the pane on the right, you can view the open source software notice for the product, as shown in **Figure 4-16**.

### Figure 4-16 Open Source Software Notice

#### OPEN SOURCE SOFTWARE NOTICE

This part contains an open source software notice for this product. The open source software licenses are granted by the respective right holders. The open source licenses prevail all other license information with regard to the respective open source software contained in the product.

#### Warranty Disclaimer

**THE OPEN SOURCE SOFTWARE IN THIS PRODUCT IS DISTRIBUTED IN THE HOPE THAT IT WILL BE USEFUL, BUT WITHOUT ANY WARRANTY, WITHOUT EVEN THE IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SEE THE APPLICABLE LICENSES FOR MORE DETAILS.**

#### Copyright Notice and License Texts

##### License: Apache License V2.0

Apache License

Version 2.0, January 2004

<http://www.apache.org/licenses/>

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition,

"control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

### 4.3.4.8 Indicator Status Management

In the navigation tree on the left, choose **System Management > Indicator Status Management**. In the pane on the right, you can set the indicator switch of a device, and specify a time period during which all indicators are always off, as shown in [Figure 4-17](#).

**Figure 4-17** Indicator status management  
Indicator Status Management

On this page, you can set the indicator switch of a device. You can configure an indicator off period if you set Indicator switch to Off. An indicator is always off if you do not specify an indicator off period.

Indicator Switch Configuration

Indicator Switch  On  Off

Indicator Off Period Configuration

	Start time	End time
<input type="checkbox"/>	21:00	23:00
----	----	----

Indicator Off Period Start time  :  End time  :  (00:00-23:59)

### 4.3.4.9 Security Self-Check

In the navigation tree on the left, choose **System Management > Security Self-Check**. In the pane on the right, you can check insecure configuration items in the system. Click **Start** to start the check, as shown in [Figure 4-18](#).

**Figure 4-18** Security self-check  
Security Self-Check

On this page, you can check for insecure configuration items in the system. Click Start to start the check. The previous check results are displayed by default.

Check Item	Conclusion	Description
------------	------------	-------------

## 4.3.5 Maintenance Diagnosis

This topic describes how to configure the maintenance diagnosis through the web page.

### 4.3.5.1 Maintenance

In the navigation tree on the left, choose **Maintenance Diagnosis > Maintenance**. In the pane on the right, click **Start Hardware Fault Detection** to start hardware fault detection, as shown in [Figure 4-19](#).



**Figure 4-19 Maintenance**

### Maintenance

Note: Hardware fault detection may not find out all hardware faults. This operation is intended only for maintenance engineers and must be performed with caution. Data services are interrupted during hardware fault detection.

#### Hardware Fault Detection

Start Hardware Fault Detection

## 4.3.5.2 User Log

In the navigation tree on the left, choose **Maintenance Diagnosis > User Log**. In the pane on the right, click **Download log File**. In the dialog box that is displayed, click **Save**, specify the path of saving the log file, and save the file to the local disk, as shown in [Figure 4-20](#).

**Figure 4-20 User Log**

### User Log

On this page, you can download and query user logs.

#### Download and View Logs

Download Log File

Log Type:

```
Manufacturer:Huawei Technologies Co., Ltd;  
ProductClass:K572;  
SerialNumber: [REDACTED]  
IP:192.168.101.1;  
HWVer: [REDACTED]  
SWVer:V5R024 [REDACTED];  
[Critical][Config-Log] Terminal:XLINK(-),Result:Success,Type>Delete,WiFi.Radio.X_HV  
[Critical][Config-Log] Terminal:XLINK(-),Result:Success,Type>Delete,WiFi.Radio.X_HV  
[Critical][Alarm-Log] Integrity check ok  
[Error][Alarm-Log] AlarmID:104001,AlarmLevel:Error,Device reset. Cause: System re  
[Critical][Config-Log] Terminal:XLINK(-),Result:Success,Type>Delete,WiFi.Radio.X_HV  
[Critical][Config-Log] Terminal:XLINK(-),Result:Success,Type>Delete,WiFi.Radio.X_HV  
[Critical][Config-Log] Terminal:XLINK(-),Result:Success,Type>Delete,WiFi.Radio.X_HV  
[Critical][Config-Log] Terminal:XLINK(-),Result:Success,Type>Delete,WiFi.Radio.X_HV  
[Critical][Alarm-Log] Integrity check ok  
[Error][Alarm-Log] AlarmID:104001,AlarmLevel:Error,Device reset. Cause: System re  
[Critical][Config-Log] Terminal:XLINK(-),Result:Success,Type>Delete,WiFi.Radio.X_HV  
[Critical][Config-Log] Terminal:XLINK(-),Result:Success,Type>Delete,WiFi.Radio.X_HV
```

- Save Log is enabled by default, It can not be configured on the Web page.
- You cannot configure Log Level, which indicates the level of the saved log. The log whose level is equal to or higher than the debug-level log is saved.

- Click **Download Log File**. In the dialog box that is displayed, click Save, specify the path for saving the log file, and save the log file to the local disk.
- Select a type from the Log Type drop-down list box to view different types of logs. Options are **All-Log**, **Config-Log**, **Shell-Log**, and **Alarm-Log**.

#### NOTICE

When IE8 is used for log file downloading and you click the save button 10s-over later after downloading, the downloaded log file is incomplete.

### 4.3.5.3 AP Log

In the navigation tree on the left, choose **Maintenance Diagnosis > AP Log**. In the pane on the right, click **Download Log File**. In the dialog box that is displayed, click **Save**, specify the path of saving the log file, and save the file to the local disk, as shown in [Figure 4-21](#).

Figure 4-21 AP Log

#### AP Log

If the AP device is connected, you will be able to query and download the AP's logs on this page.

Download And View Logs

[Download Log File](#)

```
Manufacturer:Huawei Technologies Co., Ltd;
ProductClass:K572;
SerialNumber:
IP:192.168.101.1;
HWVer:
SWVer:V5R024

[Notice] BBSP Set PortIndex:1 LinkMode Nego:1 Speed:5 Duplex:2
[Notice] BBSP Set PortIndex:2 LinkMode Nego:1 Speed:5 Duplex:2
[Notice] BBSP Set PortIndex:3 LinkMode Nego:1 Speed:5 Duplex:2
[Notice] BBSP Set PortIndex:4 LinkMode Nego:1 Speed:5 Duplex:2
[Notice] ACCESS Set PortIndex:1 Enable:1
[Notice] ACCESS Set PortIndex:2 Enable:1
[Notice] ACCESS Set PortIndex:3 Enable:1
[Notice] ACCESS Set PortIndex:4 Enable:1
[Notice] BBSP Set PortIndex:1 LinkMode Nego:1 Speed:5 Duplex:2
[Notice] BBSP Set PortIndex:2 LinkMode Nego:1 Speed:5 Duplex:2
[Notice] BBSP Set PortIndex:3 LinkMode Nego:1 Speed:5 Duplex:2
[Notice] BBSP Set PortIndex:4 LinkMode Nego:1 Speed:5 Duplex:2
```

#### NOTICE

When IE8 is used for log file downloading and you click the save button 10s-over later after downloading, the downloaded log file is incomplete.

### 4.3.5.4 Debug Log

In the navigation tree on the left, choose **Maintenance Diagnosis > Debug Log**. In the pane on the right, click **Download Log File**. In the dialog box that is displayed, click **Save**, specify the path of saving the log file, and save the file to the local disk, as shown in [Figure 4-22](#).

**Figure 4-22** Debug Log

#### Debug Log

On this page, you can download and query debug logs.

Download And View Logs

[Download Log File](#)

Log Type:

```
Manufacturer:Huawei Technologies Co., Ltd;
ProductClass:K572;
SerialNumber:
IP:192.168.101.1;
HWVer:
SWVer:V5R024

[Debug][Debug-Log] static:ETH Port 2 link status changed to Up, Rate is 100 Mbit/
[Debug][Debug-Log] static:[L2M] eth state change rpc invoke
[Debug][Debug-Log] static:[L2M] eth state change rpc invoke portid:2, value:1
[Debug][Debug-Log] static:[dhcp]send Discover, wan[wan1], xid[b118bd50], mac[
[Debug][Debug-Log] static:[WAN_MNGT] ipv4 if set wan state up pre, wan Index=C
[Debug][Debug-Log] static:[WAN_MNGT] ipv4 if set wan state up, wan Index=0x30
[Debug][Debug-Log] static:[WAN_MNGT] ipv6 if set wan state up, wan Index=0x30
[Debug][Debug-Log] static:[WAN_MNGT] ipv4 if set wan state down, wan Index=0;
[Debug][Debug-Log] static:[WAN_MNGT] ipv4 if set wan state up pre, wan Index=C
[Debug][Debug-Log] static:[WAN_MNGT] ipv4 if set wan state up, wan Index=0x30
[Critical][Debug-Log] static:[dhcp]get wan[wan1] ifindex[12] and Mac Addr[00-25-
[Debug][Debug-Log] static:[dhcp]send Discover, wan[wan1], xid[b118bd50], mac[
```

Click **Download Log File**. In the dialog box that is displayed, click **Save**, specify the path for saving the log file, and save the log file to the local disk.

#### NOTICE

When IE8 is used for log file downloading and you click the save button 10s-over later after downloading, the downloaded log file is incomplete.

### 4.3.5.5 Fault Info Collect

In the navigation tree on the left, choose **Maintenance Diagnosis > Fault Info Collect**. In the pane on the right, click **Start** to collect edge ONT fault information, and click **Show Wi-Fi Diagnosis** to view edge ONT fault information, as shown in [Figure 4-23](#).

**Figure 4-23** Fault Info Collect

## Enable Collect Fault Information

---

On this page, you can collect and download fault information.

### Enable Collect Fault Information

Start

Download

### Collecting Wi-Fi Information

Show Wi-Fi Diagnosis

 **NOTE**

- After the information is collected, click **Download** to download the collected information to a local directory.
- When IE8 is used for fault info collect and you click the save button 10s-over later after downloading, the downloaded fault info collect is incomplete.