Huawei OptiXstar K562e-10 V500R022C00

Web Page Reference

Issue	01
Date	2023-04-28

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Notice

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

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

Symbol Conventions

Symbol Conventions

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

Symbol	Description
DANGER	Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
WARNING	Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
CAUTION	Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury.
NOTICE	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.
NOTE	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	2023-04-30	This is the first official release.

Contents

Symbol Conventions ii
Change History iii
1 Locally Logging in to the Web Interface 1
2 Internet Guide 6
3 Web Page Reference (Route mode) 14
3.1 Homepage 14
3.2 Internet Access 15
3.3 My Wi-Fi 16
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 WLAN Information 20
3.5.1.3 Home Network Information 22
3.5.2 WLAN 23
3.5.2.1 Wi-Fi Advanced Configuration 23
3.5.2.2 Wi-Fi Coverage Management 25
3.5.2.3 Automatic Wi-Fi Shutdown 29
3.5.3 Network Configuration 30
3.5.3.1 LAN Settings 30
3.5.3.2 IPv6 32
3.5.3.3 DDNS Function 33
3.5.3.4 UPnP Function 35
3.5.4 Security Configuration 36
3.5.4.1 Wi-Fi MAC Address Filtering 36
3.5.4.2 Firewall Configuration 38
3.5.4.3 Parental Control 38
3.5.4.4 DMZ Function 40
3.5.4.5 IPv4 Port Mapping 41
3.5.4.6 Port Trigger Configuration 44
3.5.4.7 Device Access Control 46
3.5.5 System Management 47

3.5.5.1 Upstream Network Port Settings 47
3.5.5.2 TR-069 47
3.5.5.3 Software Upgrade 51
3.5.5.4 Account Management 52
3.5.5.5 Time Setting 52
3.5.5.6 Backup and Recovery 54
3.5.5.7 Open Source Software Notice 54
3.5.5.8 Indicator Status Management 55
3.5.5.9 Security Self-Check 56
3.5.6 Maintenance Diagnosis 56
3.5.6.1 Maintenance 56
3.5.6.2 User Log 58
3.5.6.3 AP Log 59
3.5.6.4 Firewall Log 59
3.5.6.5 Debug Log 60
3.5.6.6 Fault Info Collect 61
3.5.6.7 Remote Mirror 62

4 Web Page Reference (Bridge mode) 65

4.1 Homepage 65
4.2 My Wi-Fi 66
4.3 More 67
4.3.1 System Information 67
4.3.1.1 Device Information 67
4.3.1.2 WLAN Information 68
4.3.2 WLAN 70
4.3.2.1 Wi-Fi Advanced Configuration 70
4.3.2.2 Smart Network Connection 72
4.3.2.3 Wi-Fi Repeater 72
4.3.3 Security Configuration 73
4.3.3.1 Device Access Control 73
4.3.4 System Management 74
4.3.4.1 Upstream Network Port Settings 74
4.3.4.2 TR-069 75
4.3.4.3 Software Upgrade 80
4.3.4.4 Account Management 80
4.3.4.5 Time Setting 81
4.3.4.6 Backup and Recovery 83
4.3.4.7 Open Source Software Notice 83
4.3.4.8 Security Self-Check 84
4.3.5 Maintenance Diagnosis 85
4.3.5.1 Maintenance 85
4.3.5.2 User Log 85

4.3.5.3 AP Log 86
4.3.5.4 Debug Log 87
4.3.5.5 Fault Info Collect 88
4.3.5.6 Indicator Status Management 89

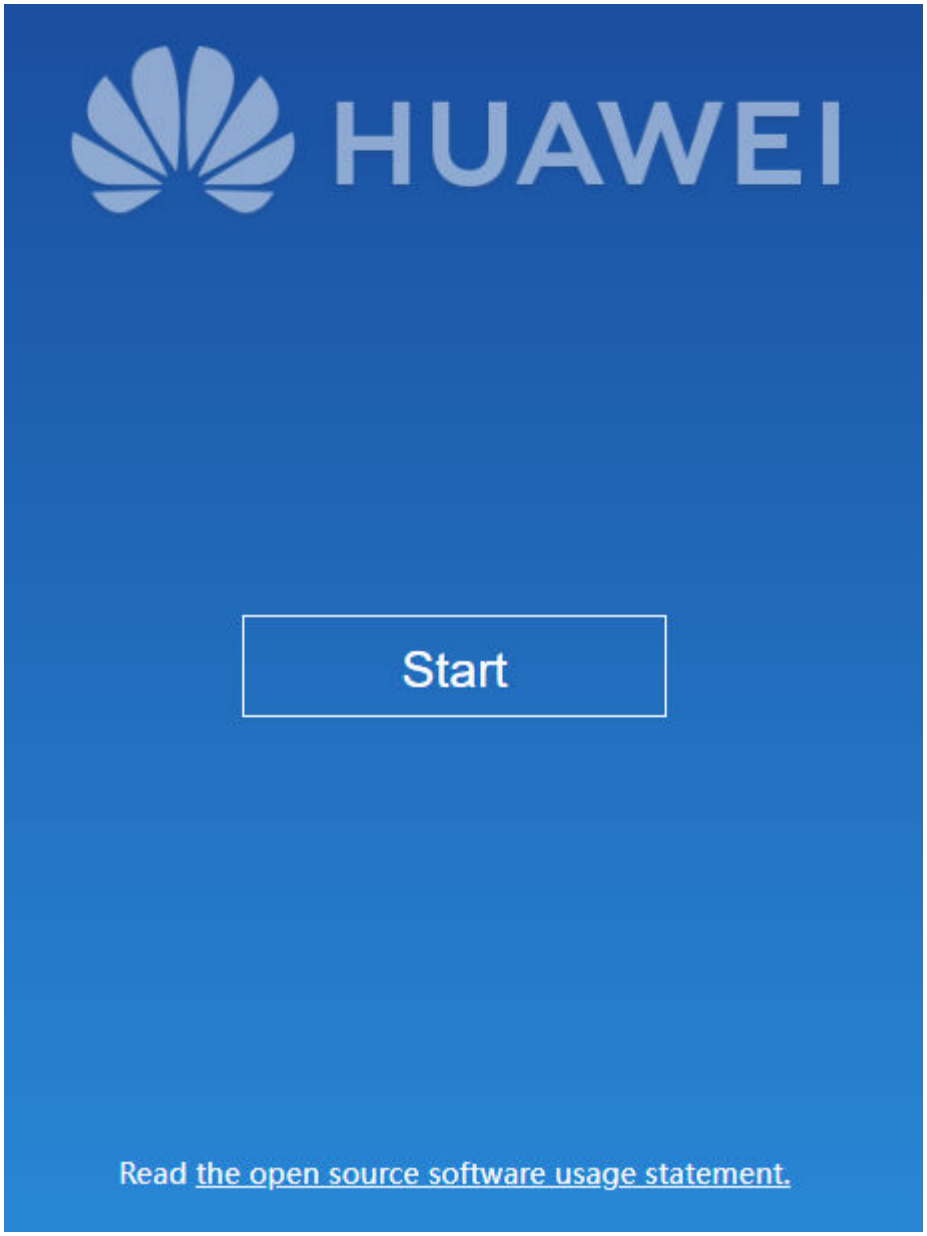
1 Locally Logging in to the Web Interface

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 (no password). For the Wi-Fi name, see the SSID on the device nameplate.
2. Open the browser. The configuration page is automatically displayed.

Figure 1-1 Web configuration interface-K562e-10



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.)
- No password is required for the first login. The password is required to log in to the interface after you configure Internet access.
- 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.

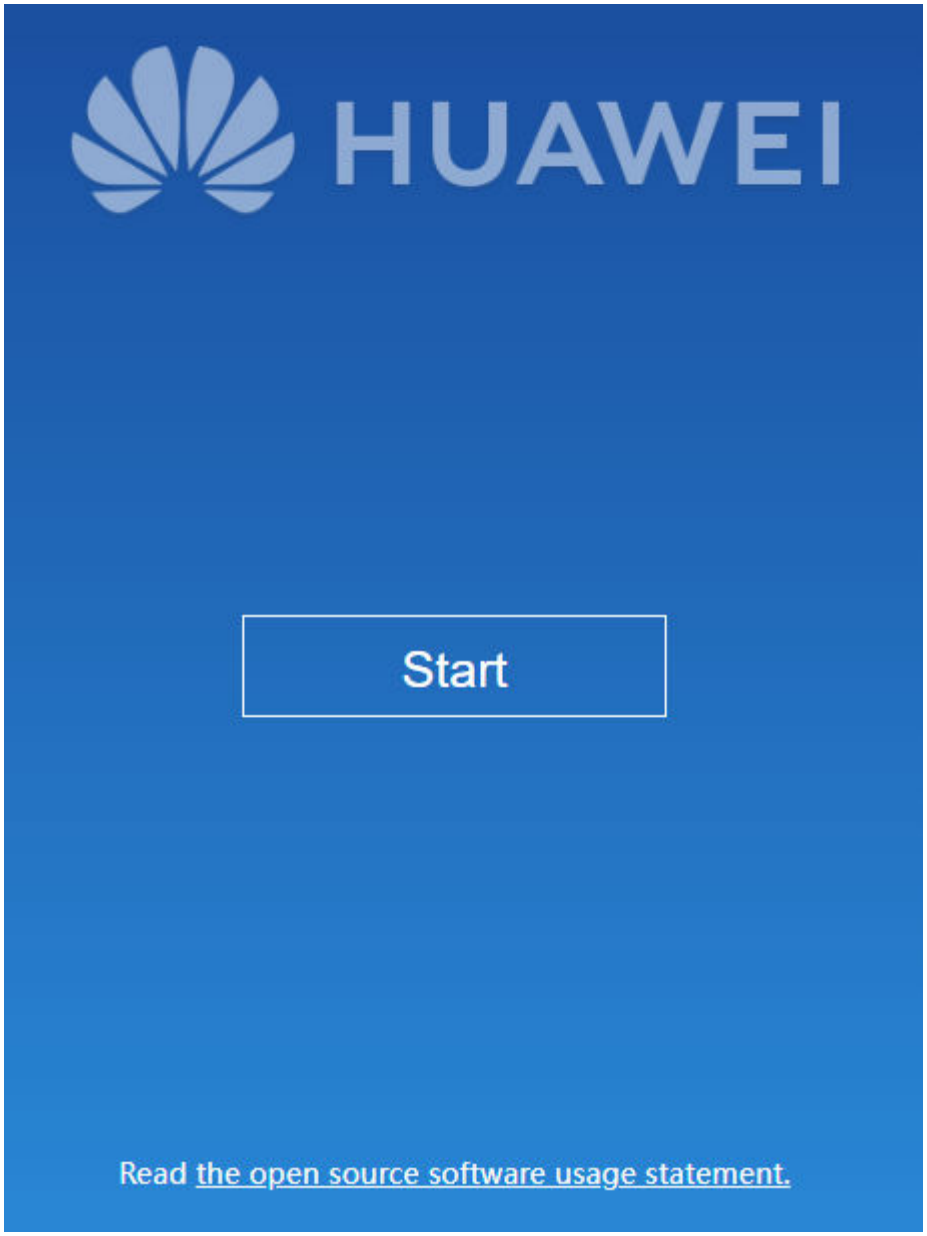
Table 1-1 Data plan

Item	Description
LAN IP address and subnet mask of the edge ONT	Default settings: • IP address: 192.168.101.1 • Subnet mask: 255.255.255.0
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: • IP address: 192.168.101.100 • Subnet mask: 255.255.255.0

- **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 IE (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-K562e-10

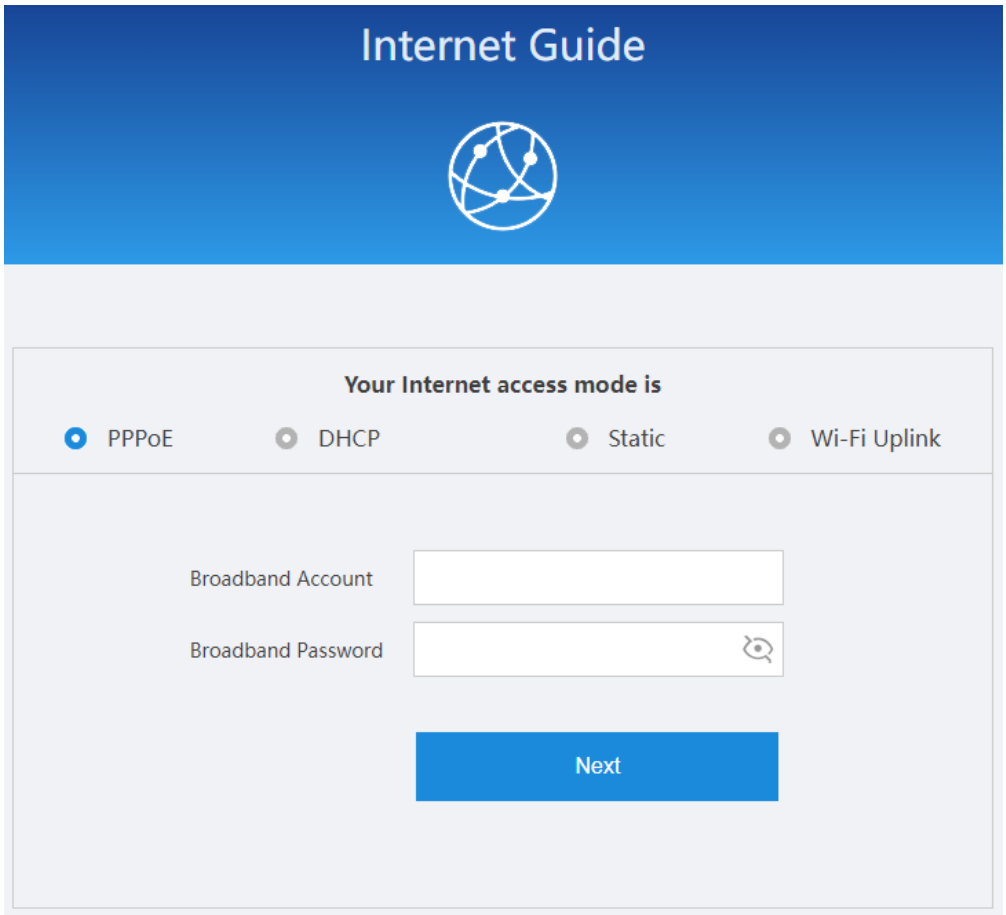


NOTE

- 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.
- No password is required for the first login. The password is required to log in to the interface after you configure Internet access.
- 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. Click **Start**, 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.



NOTE

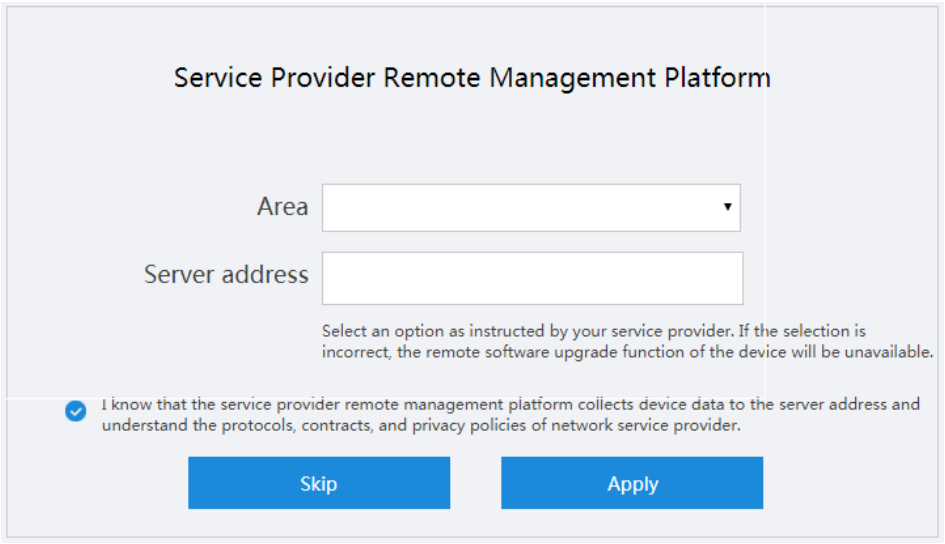
- If you forget the broadband account and password, contact your ISP to retrieve the account and password.
- To enhance system security, change the password to a password that meets security requirements after the first successful login. It is recommended that you change the password periodically.

– No drop cable is detected.

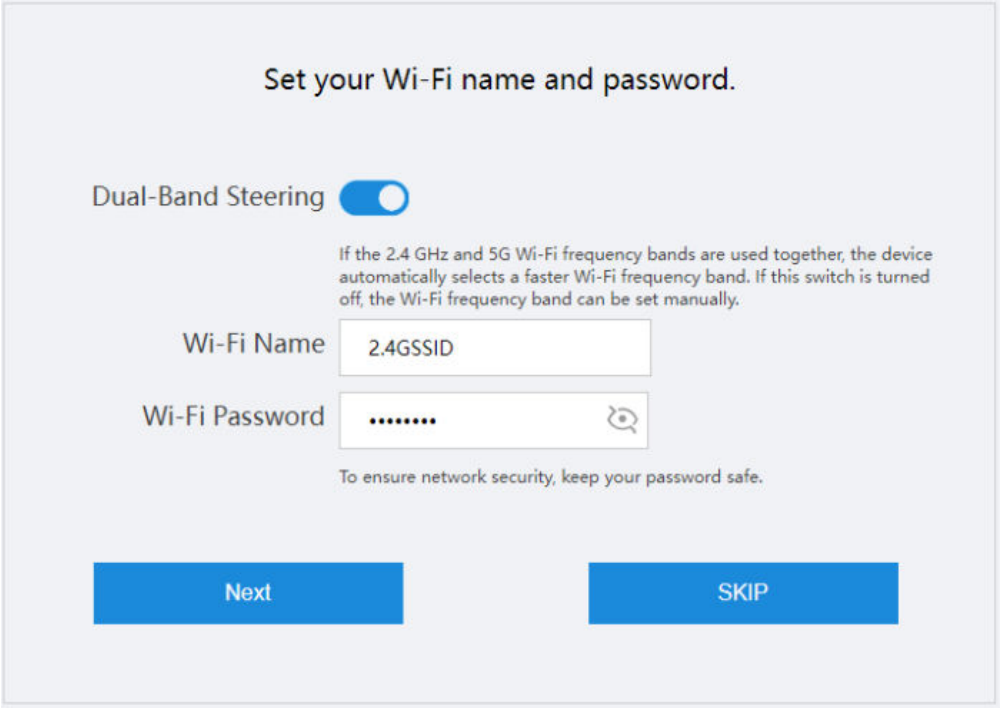
– If you click **Re-check**, the device checks the Internet access mode again.
– If you click **Wi-Fi Uplink**, the Internet access mode is set to Wi-Fi uplink, and the operation in step 4 is required.
– If you click **continue the configuration without inserting the network cable**, you need to manually 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.

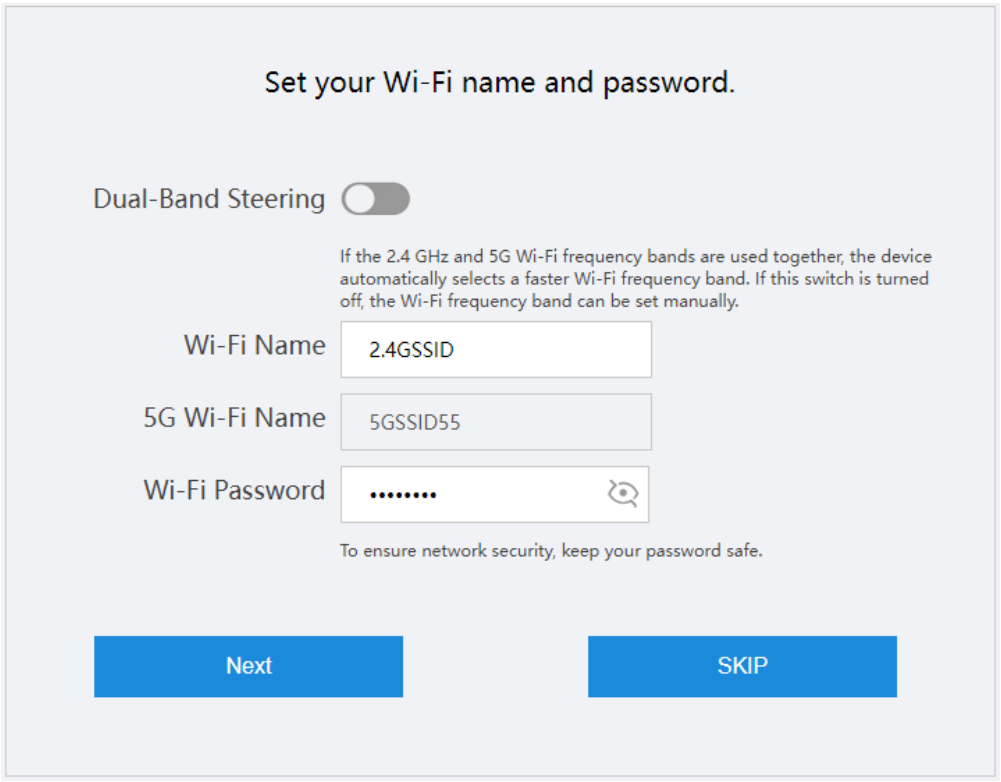
Figure 2-1 Service Provider Remote Management Platform



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



   - Disable Dual-Band Steering

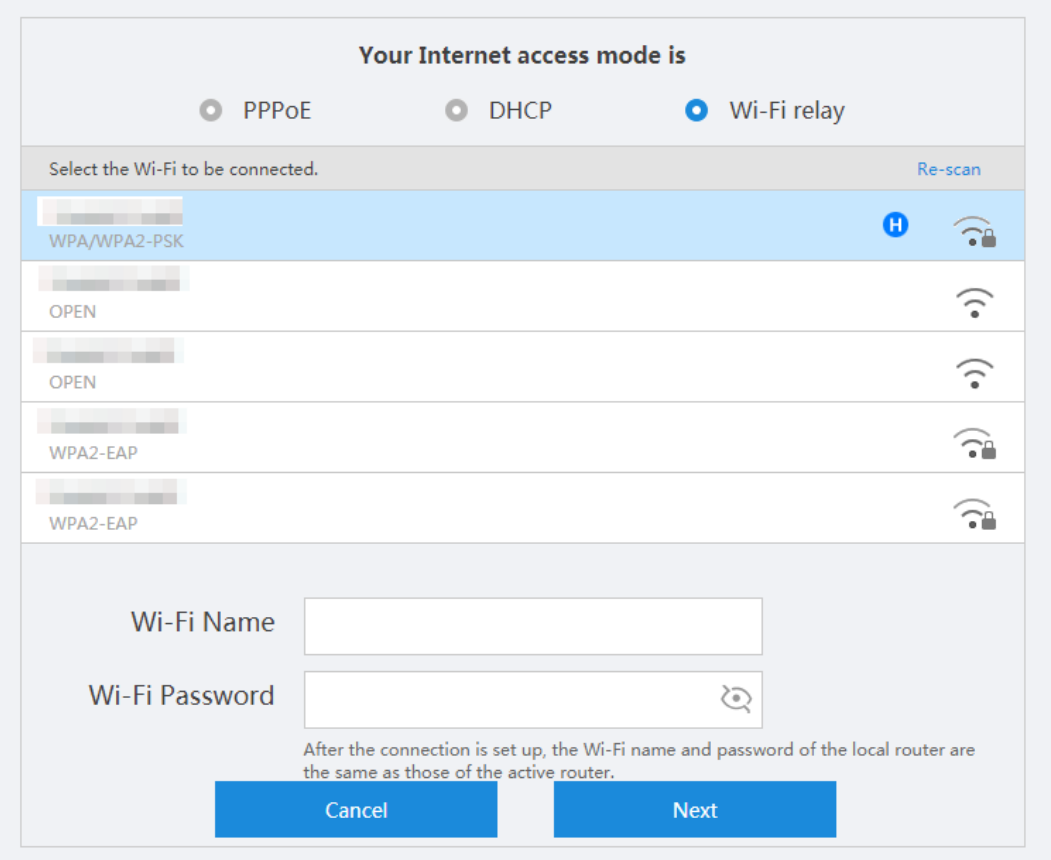


NOTICE

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.

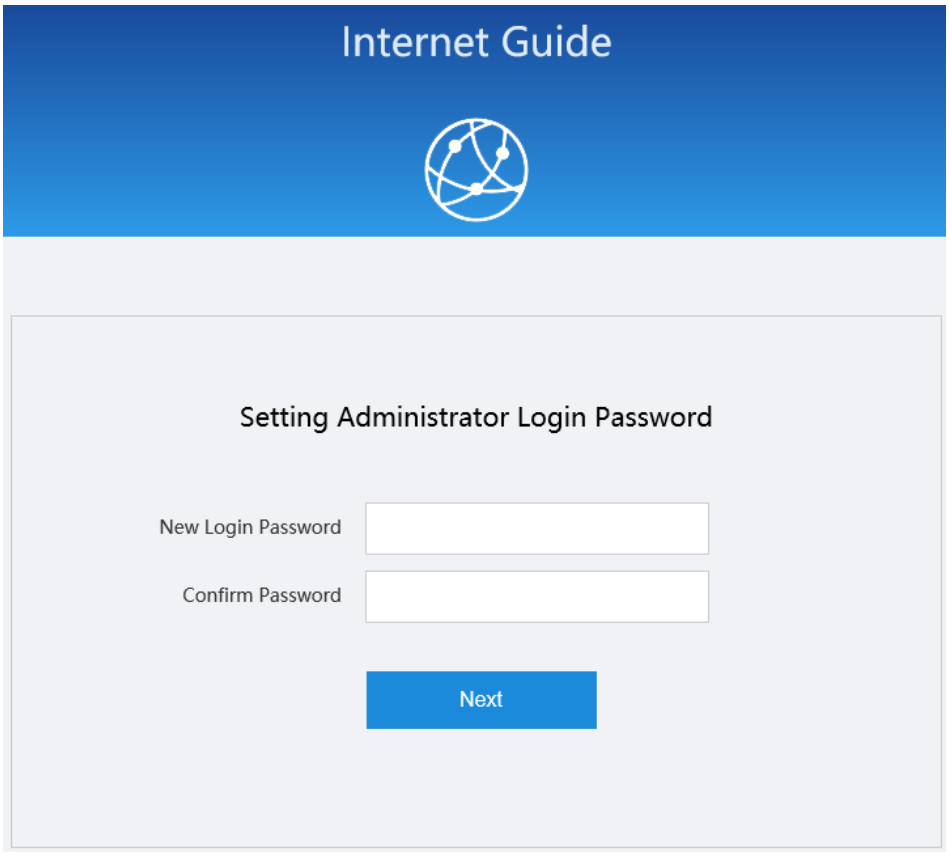
5. Select the Wi-Fi name to be connected, enter the Wi-Fi password, and click **Next.**



NOTE

Indicates that the Wi-Fi of the gateway supports the one-click pairing.

6. Set the administrator login password. Click **Next**.



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

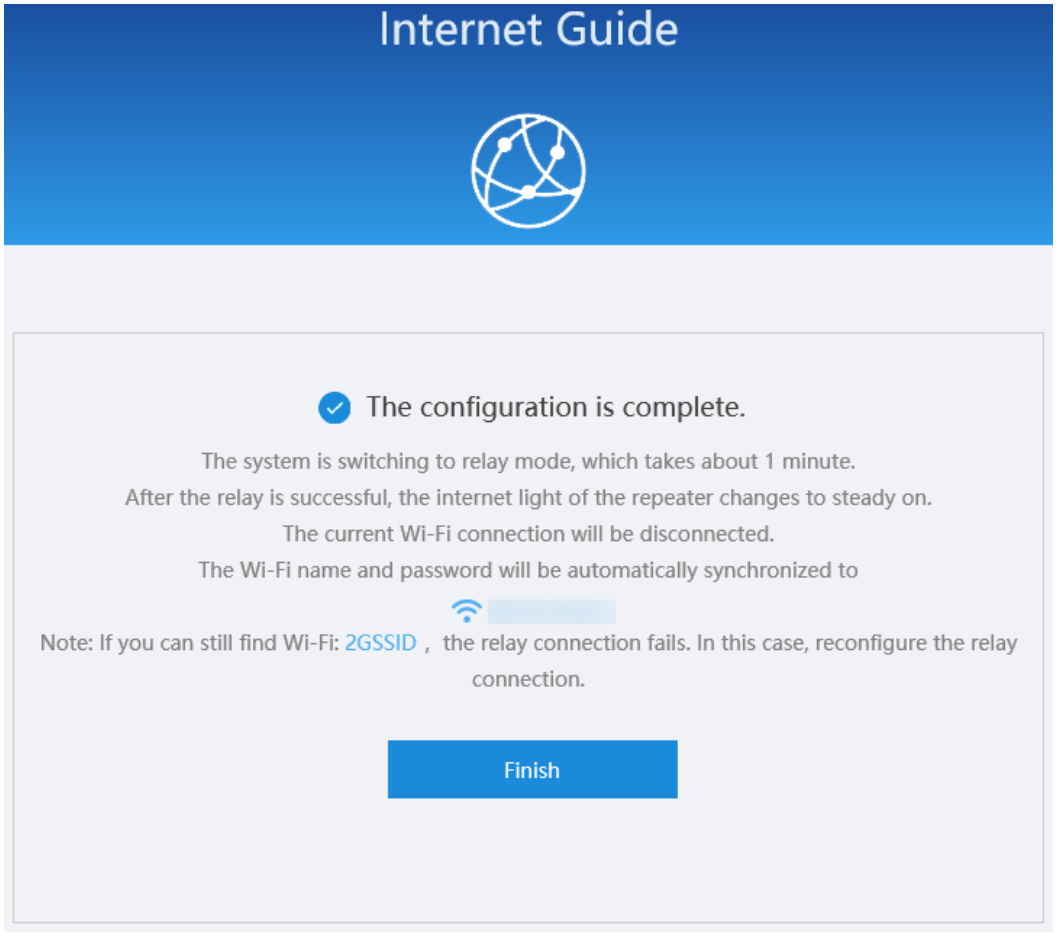
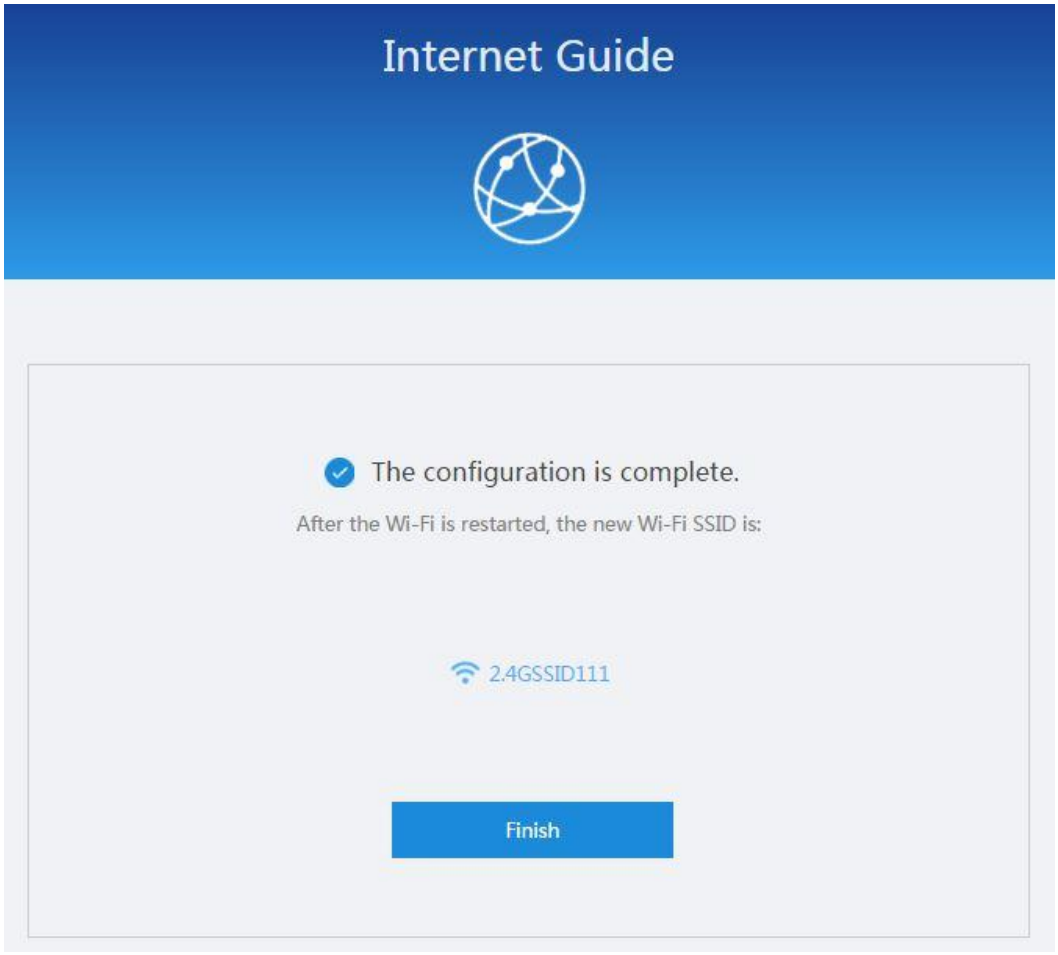


Figure 2-3 The configuration is complete-route mode

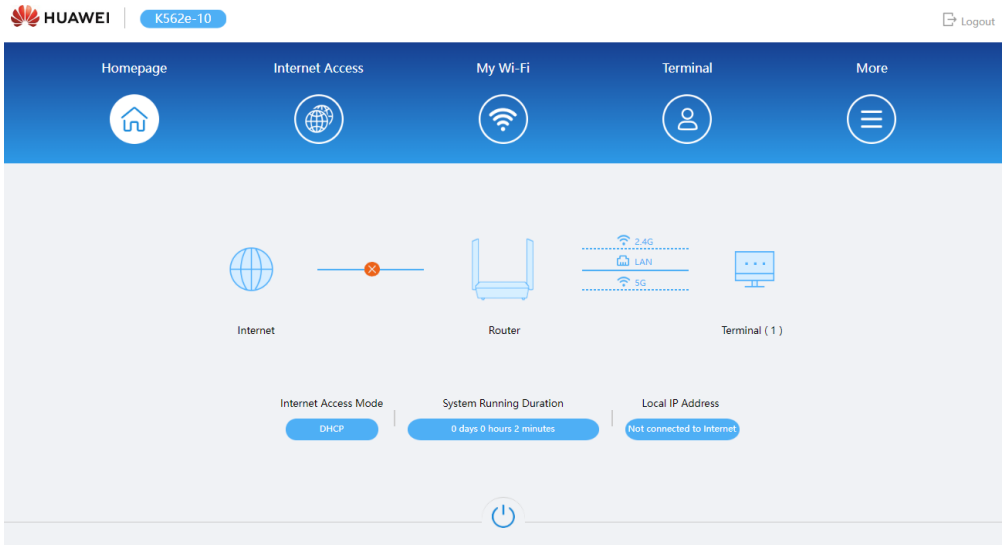


3 Web Page Reference (Route mode)

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.

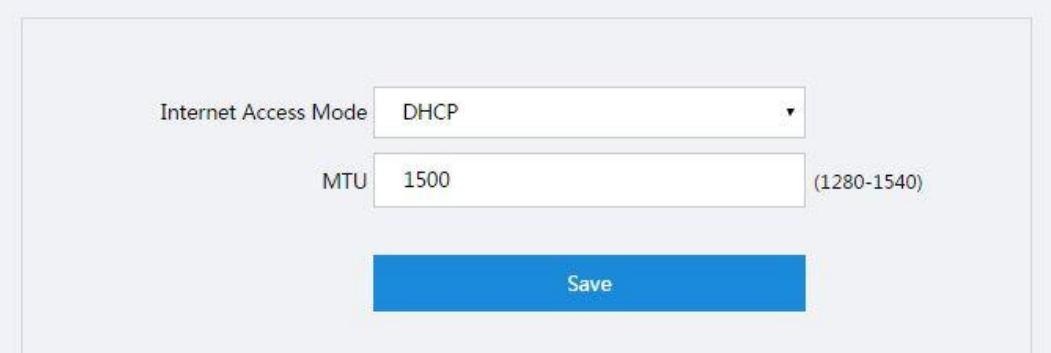
Figure 3-1 Homepage



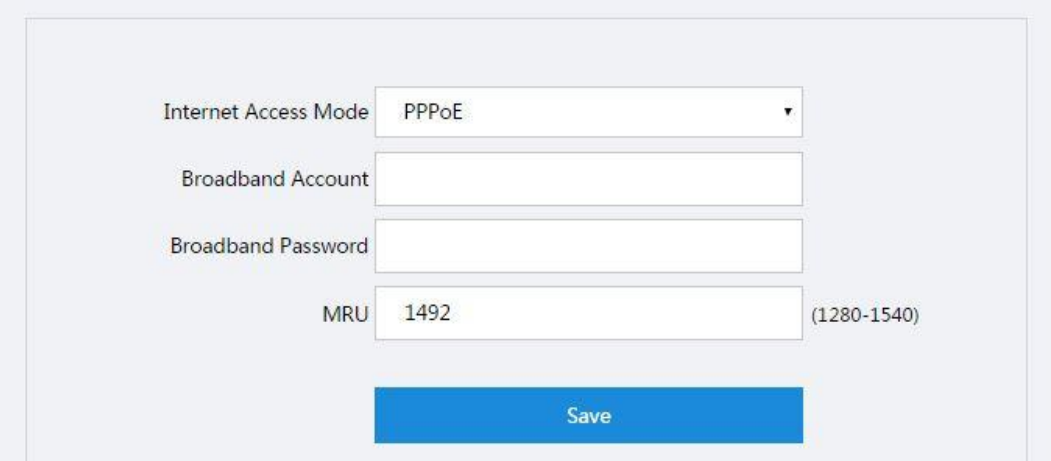
3.2 Internet Access

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)



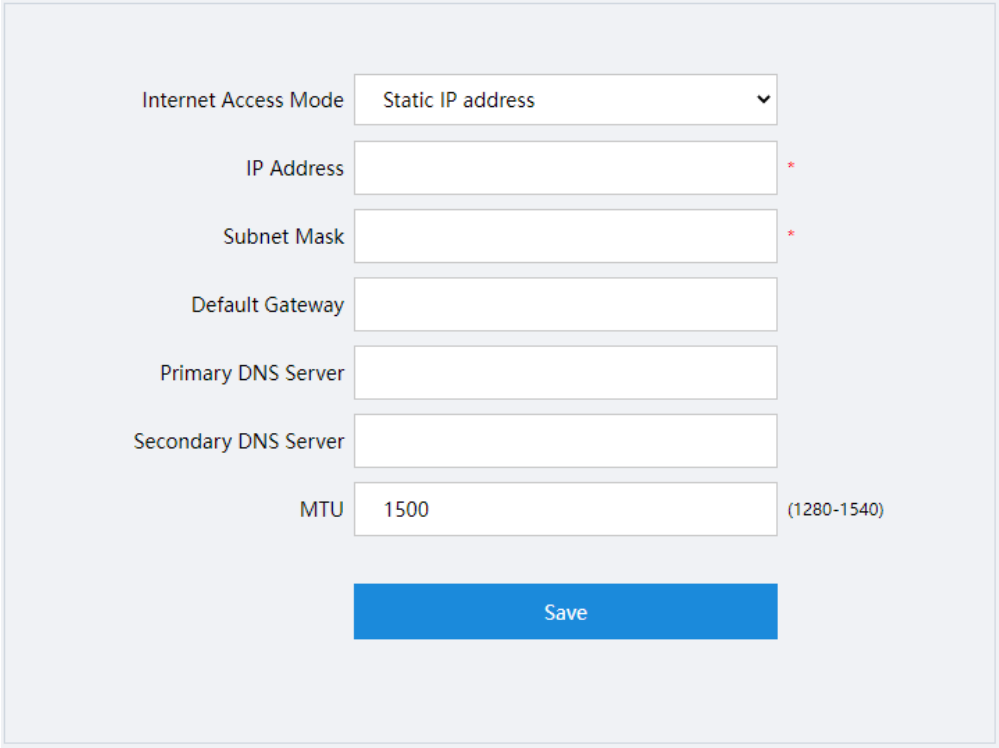
- PPPoE



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.

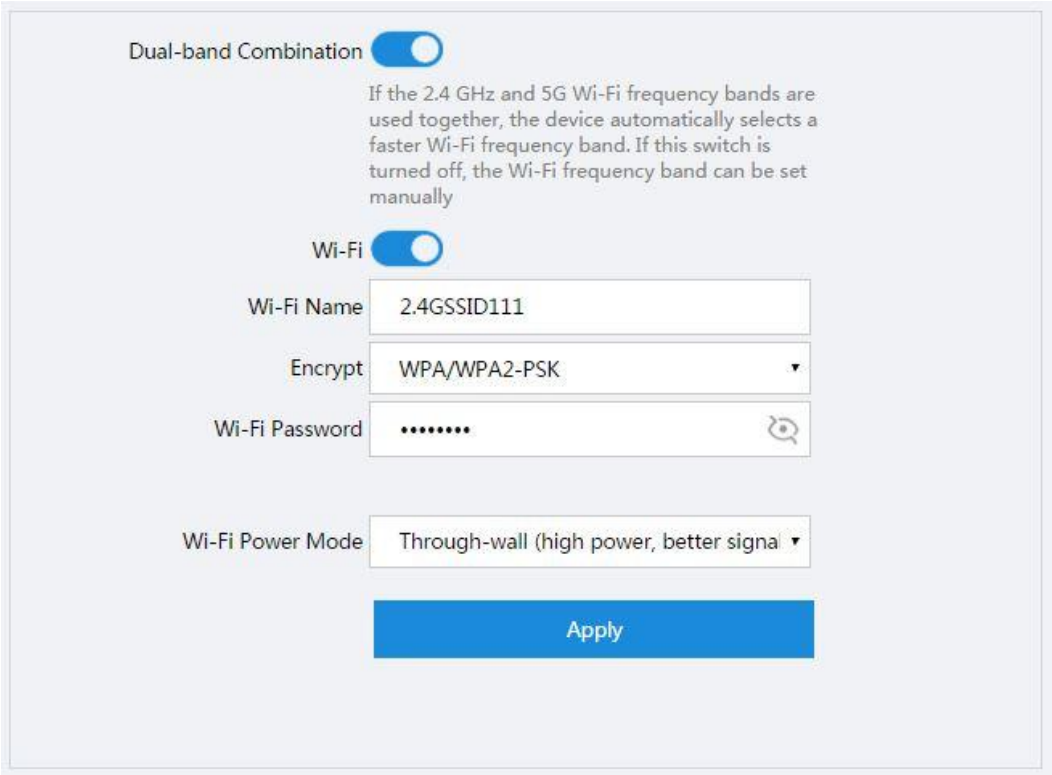
- Manual IP address input (static IP address): Enter the information provided by the operator during the subscription to the broadband service, including the fixed IP address, subnet mask, default gateway, primary DNS server IP address, and secondary DNS server IP address.



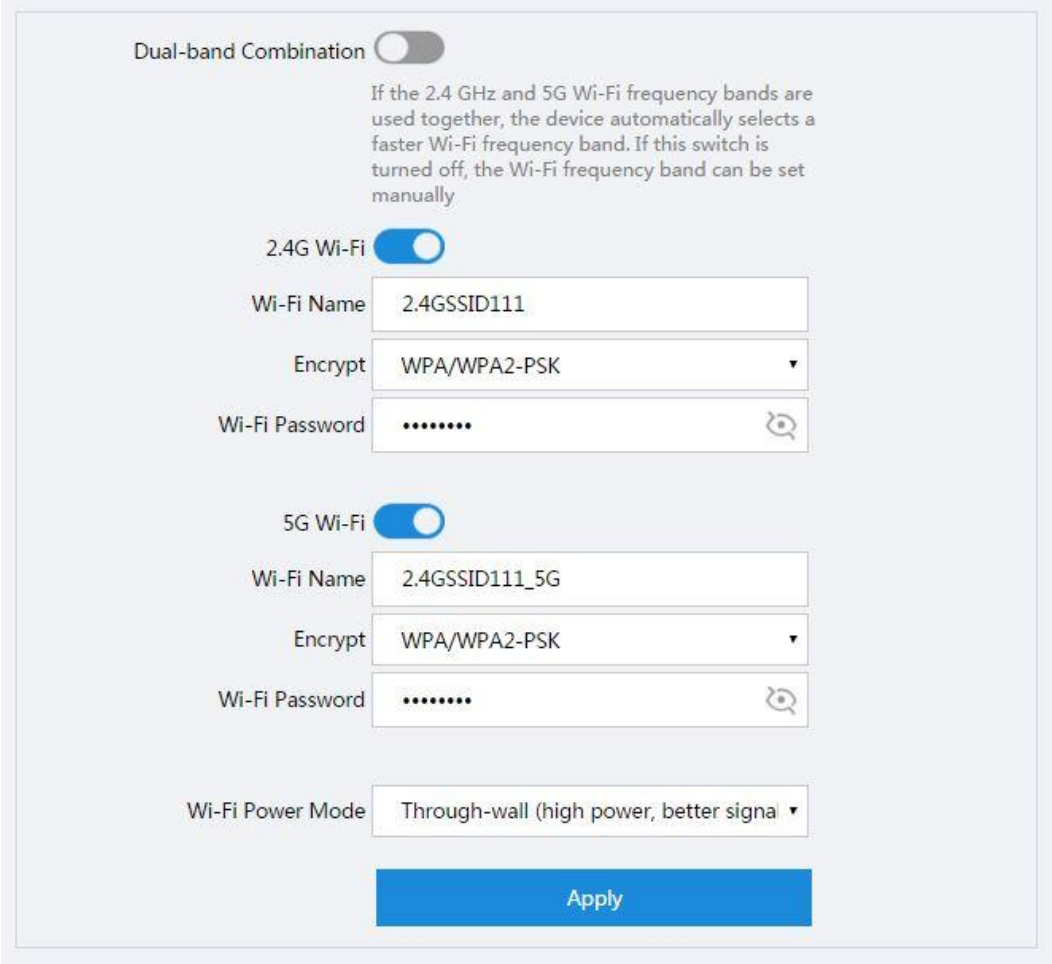
3.3 My Wi-Fi

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

- Enable Dual-Band Combination



- Disable Dual-Band Combination



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 Combination	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.

Parameter	Description
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: • Through-wall (high power, better signal) • Standard (standard power, common signal) • Sleep (low power, weak signal)

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

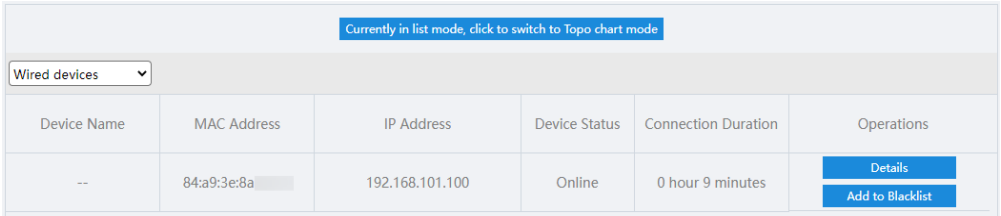
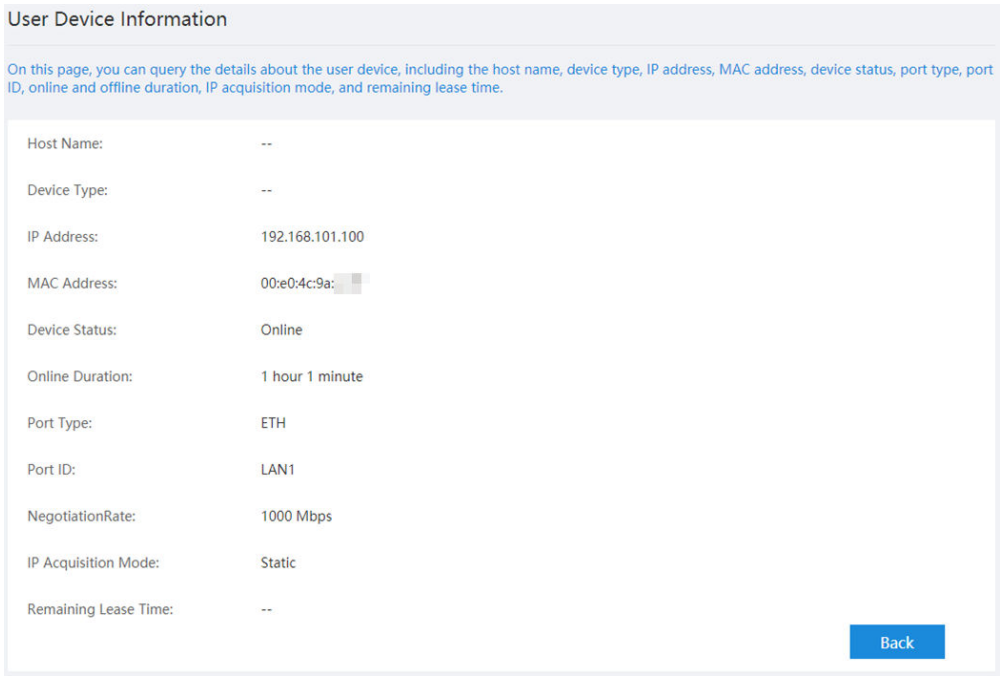


Figure 3-3 User Device Information



3.5 More

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

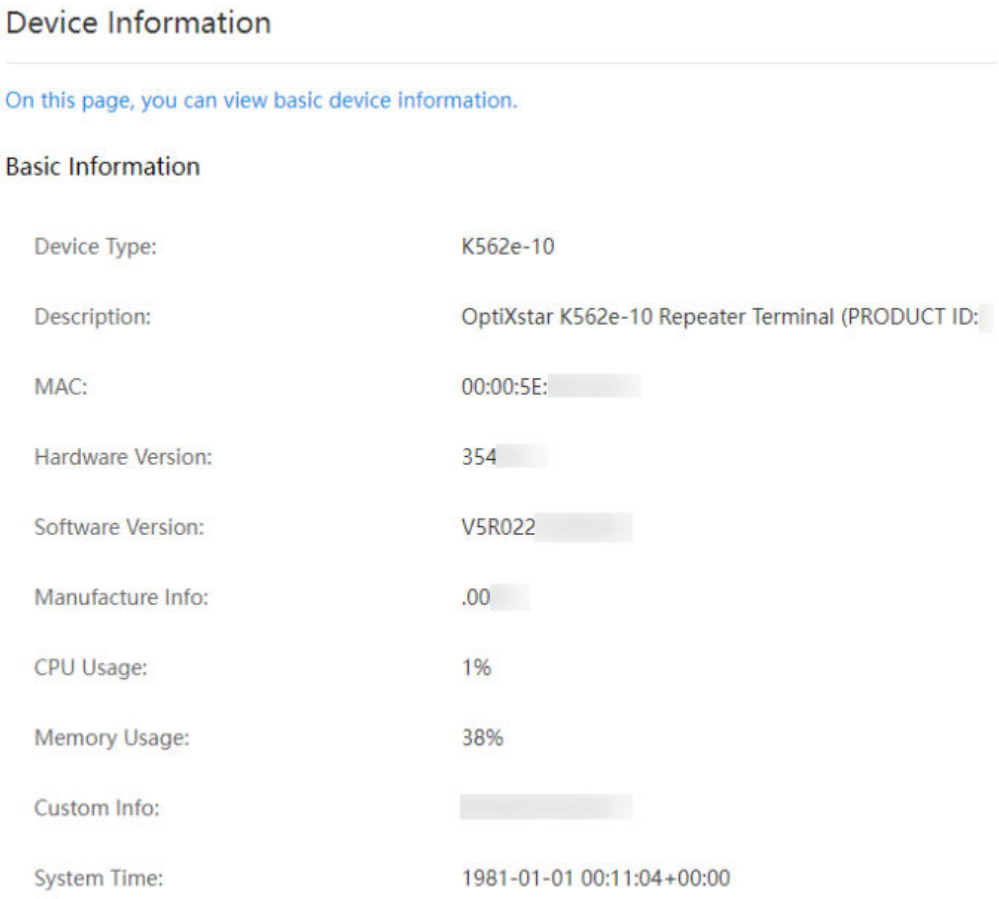
3.5.1 System Information

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**.

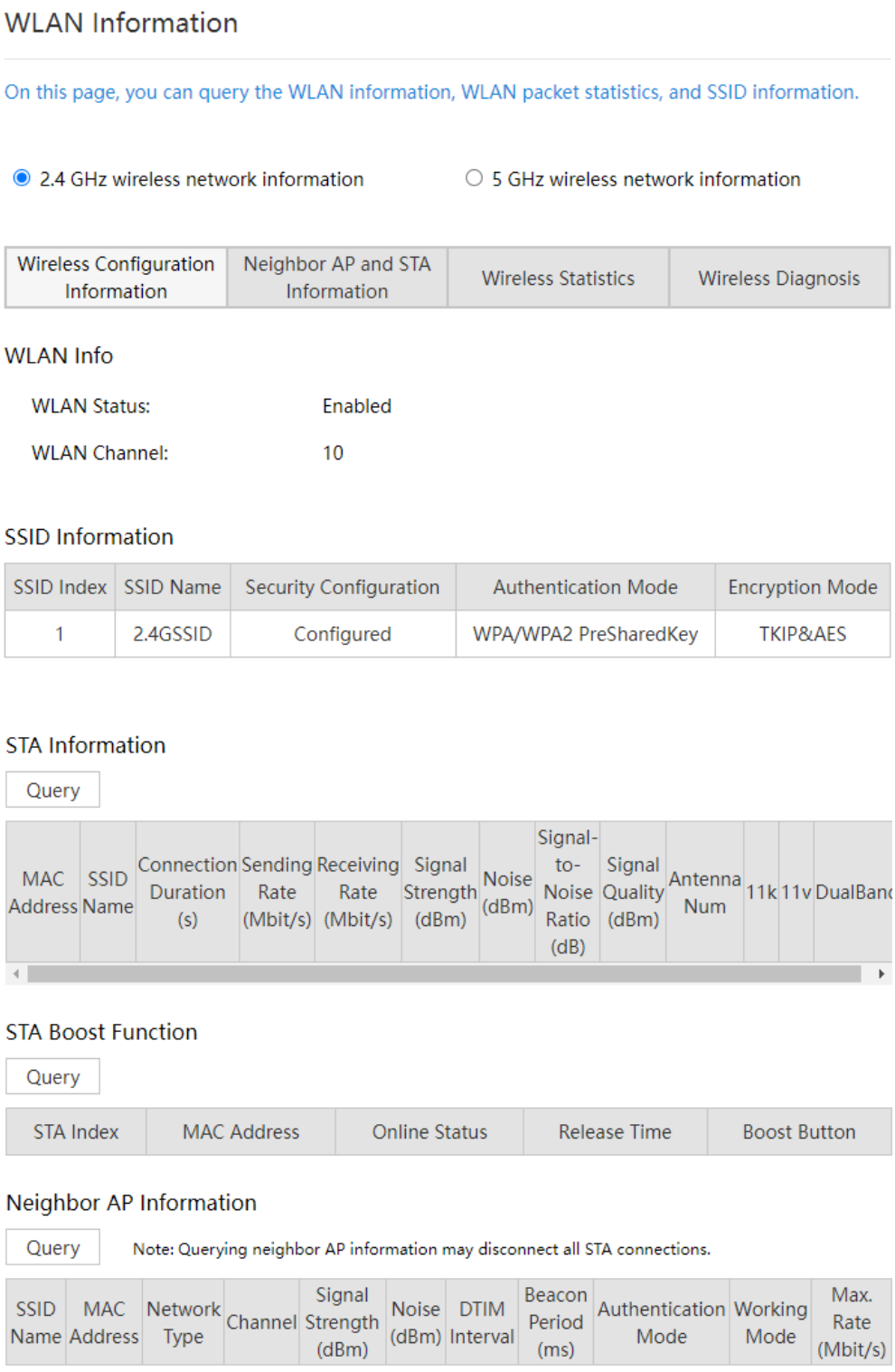
Figure 3-4 Device Information



3.5.1.2 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 3-5**.

Figure 3-5 WLAN Information

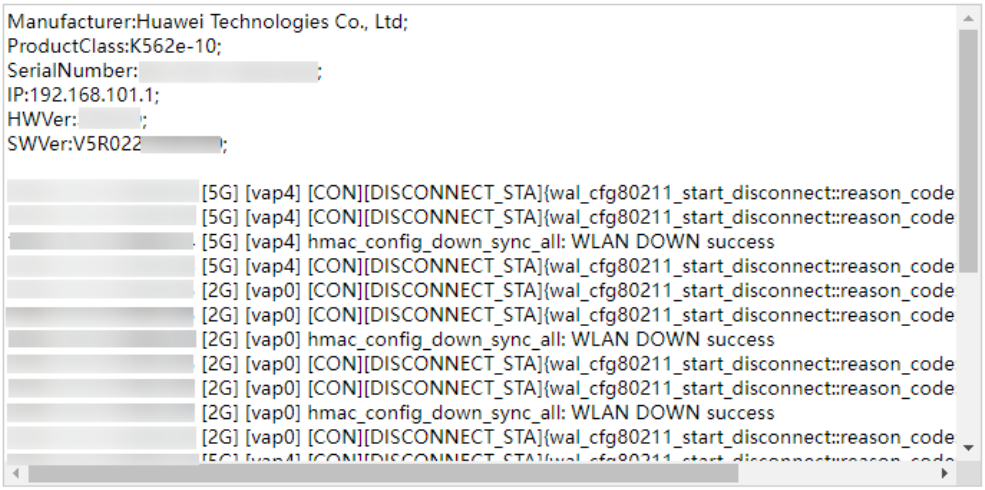


WLAN Packet Statistics

SSID Index	SSID Name	Receive (RX)				Transmit (TX)			
		Bytes	Packets	Error	Discarded	Bytes	Packets	Error	Discarded
1	2.4GSSID	0	0	0	0	18498	118	0	0

STA Event Log

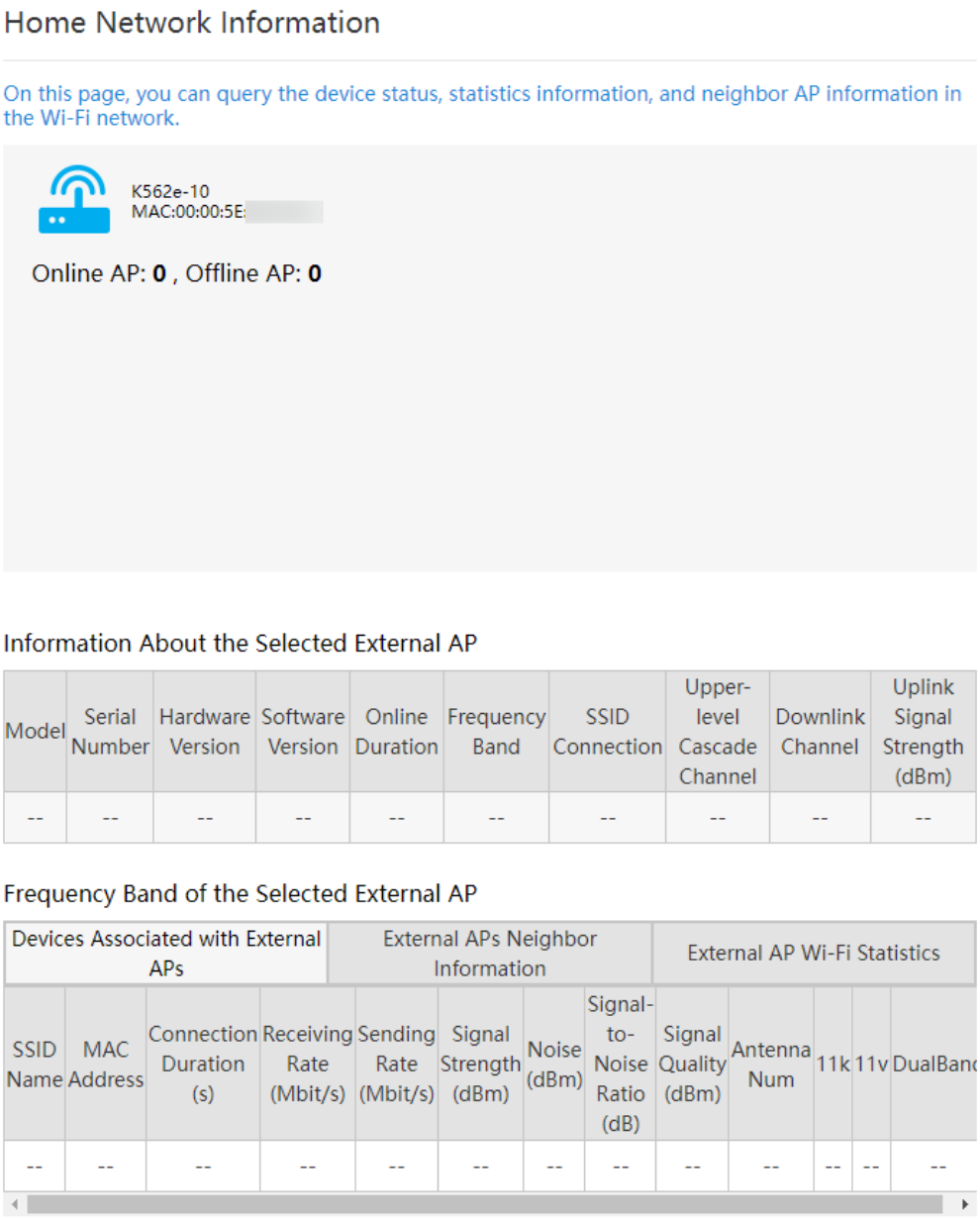
Download Log File



3.5.1.3 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 3-6**.

Figure 3-6 Home Network Information



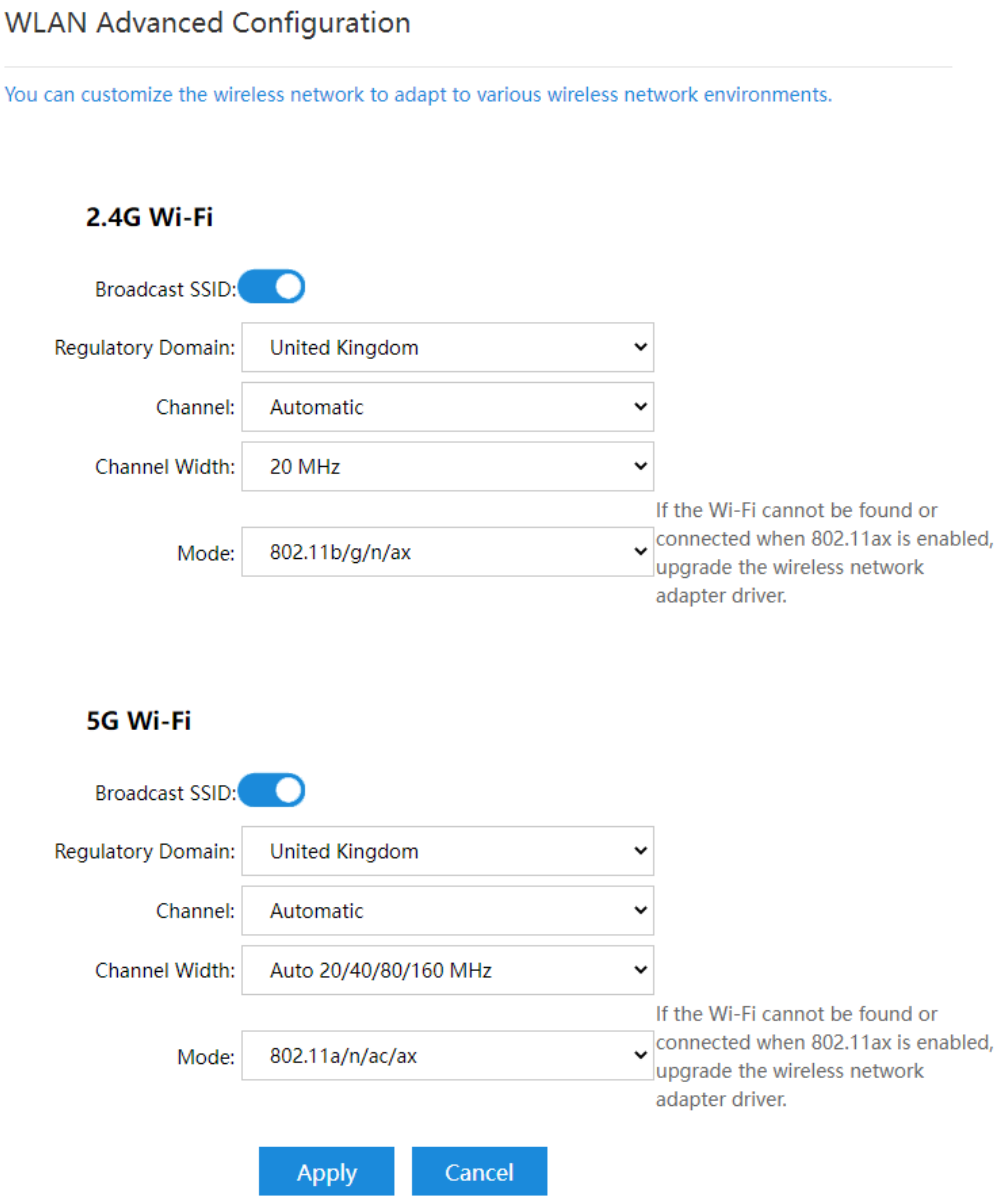
3.5.2 WLAN

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 3-7**.

Figure 3-7 WLAN Advanced Configuration



2. Click **Apply**.

Table 3-2 describes the WLAN advanced parameters.

Table 3-2 WLAN advanced parameters

Parameter	Description
Broadcast SSID	Indicates whether to enable or hide broadcast. • 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. • 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.
Regulatory Domain	Indicates the country code of the wireless network.
Channel	Indicates the channel of the wireless network. The channel varies with the value of Regulatory Domain.
Channel Width	Indicates the wireless channel width. • 2.4G Wi-Fi can be set to **Auto 20/40 MHz**, **20 MHz** or **40 MHz**. • 5G Wi-Fi can be set to **Auto 20/40 MHz**, **20 MHz** , **40 MHz**, **Auto 20/40/80 MHz** or **Auto 20/40/80/160 MHz.**
Mode	Indicates the supported wireless network mode. • 2.4G Wi-Fi can be set to **802.11b**, **802.11g**, **802.11b/g**, **802.11b/g/n** or **802.11b/g/n/ax**. • 5G Wi-Fi can be set to **802.11a**, **802.11a/n**, **802.11a/n/ac** or **802.11a/n/ac/ax**.

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 3-8** and **Figure 3-9**.

Figure 3-8 Wi-Fi Parameter Configuration

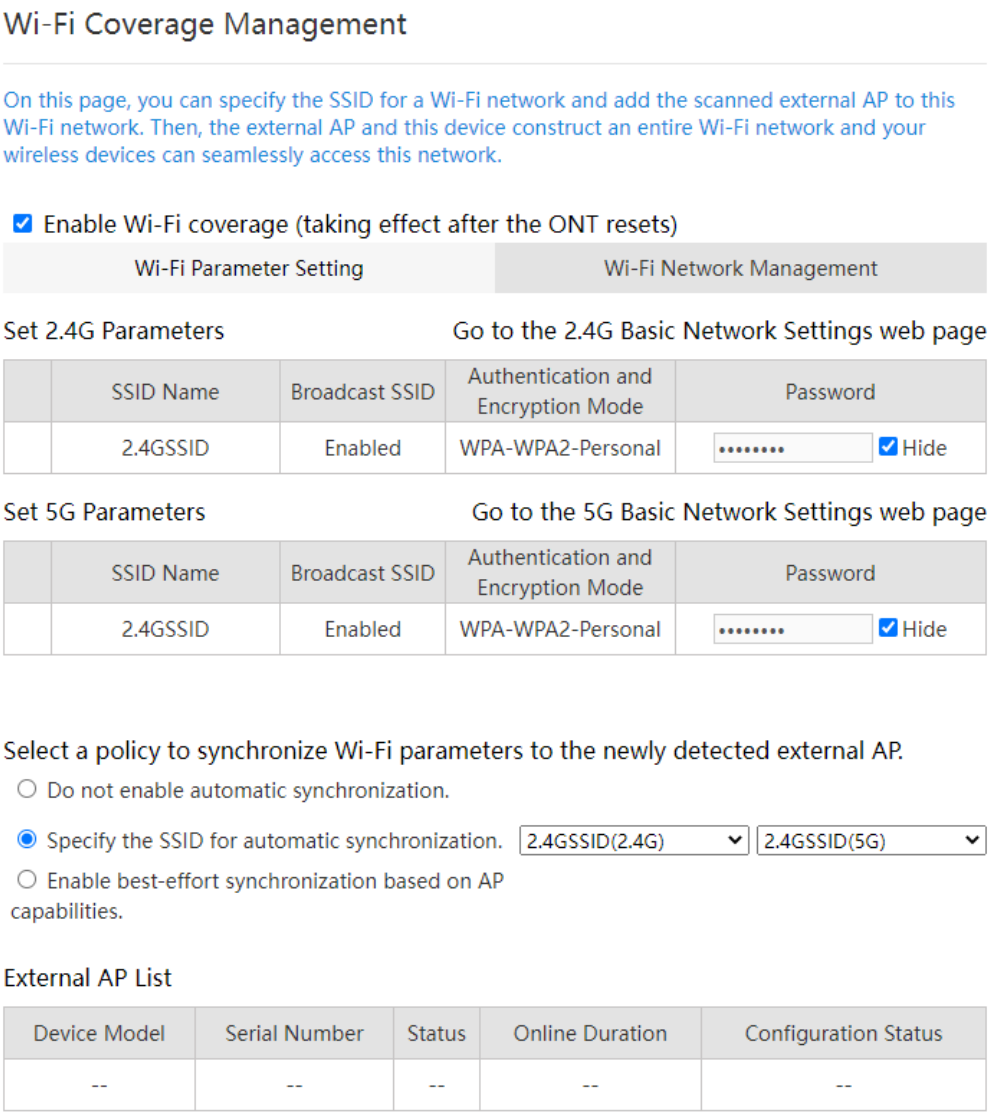


Figure 3-9 Wi-Fi Network Management

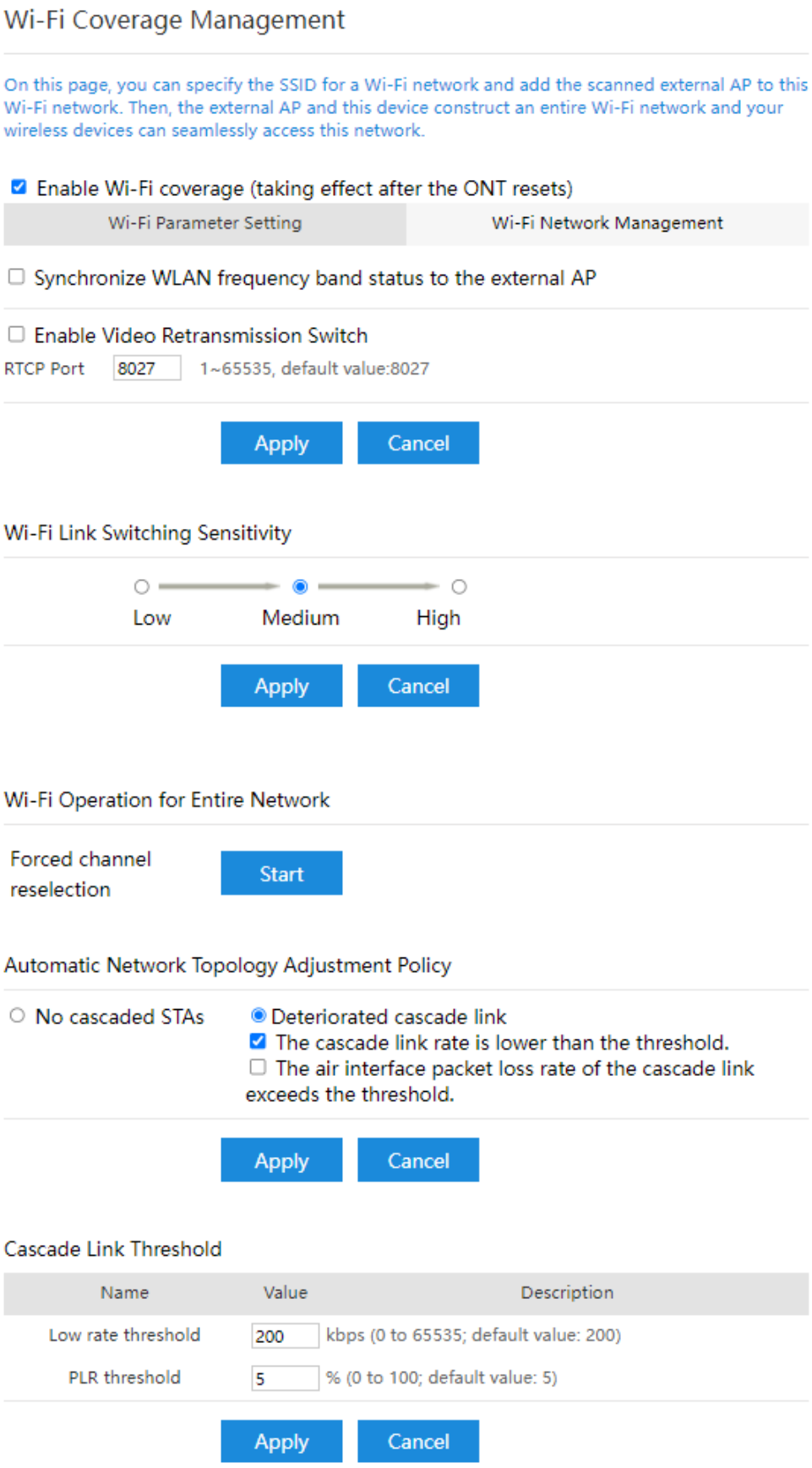


Table 3-3 describes the Wi-Fi coverage management parameters.

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.
Wi-Fi Parameters Configuration	
Set 2.4G Parameters	Displays 2.4G Wi-Fi parameter settings configured on **My Wi-Fi** and **WLAN Advanced Configuration** pages.
Set 5G Parameters	Displays 5G Wi-Fi parameter settings configured on **My Wi-Fi** and **WLAN Advanced Configuration** pages.
Select a policy to synchronize Wi-Fi parameters to the newly detected external AP	Selects either of the following policies: • **Do not enable automatic synchronization.** • **Specify the SSID for automatic synchronization.** (If the device has multiple SSIDs, specify one of the SSIDs to be synchronized to an external AP.) • **Enable best-effort synchronization according to AP capabilities.**
Wi-Fi Network Management	
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 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.
Wi-Fi Link Switching Sensitivity	Sets the Wi-Fi sensitivity applied during Wi-Fi roaming. Sensitivity options are as follows: • **Low** (no active switching) • **Medium** (default value) • **High** (active switching)
Forced channel reselection	Re-assess network-wide Wi-Fi channels and re-selects a channel after you click **Start**.

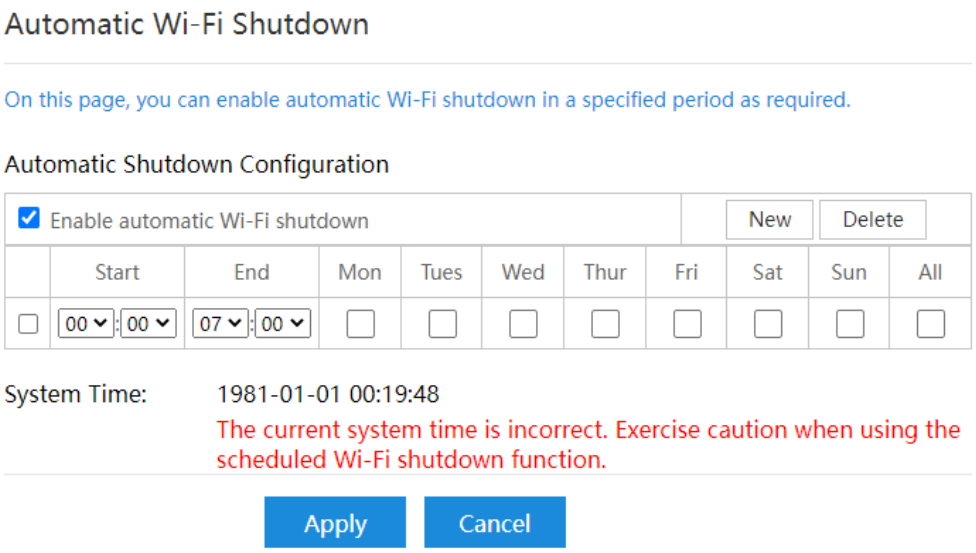
Parameter	Description
Automatic Network Topology Adjustment Policy	• **No cascaded STAs:** After this option is selected, automatic network topology adjustment is implemented only when no STA is connected to the network. • **Deteriorated cascade link**: Automatic network topology adjustment is implemented when the quality of cascading links deteriorates. You can set the link quality deterioration criteria to **The cascade link rate is lower than the threshold** or **The air interface packet loss rate of the cascade link exceeds the threshold**. The threshold refers to the settings in the **Cascading Link Threshold** field.
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 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 3-10**.

Figure 3-10 Automatic Wi-Fi Shutdown



2. Click **Apply**.

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

Table 3-4 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.
End	Indicates the end time to shut down the Wi-Fi network automatically which can be set after **Enable automatic Wi-Fi shutdown** is selected.
Start	Indicates the start time to shut down the Wi-Fi network automatically which can be set after **Enable automatic Wi-Fi shutdown** is selected.

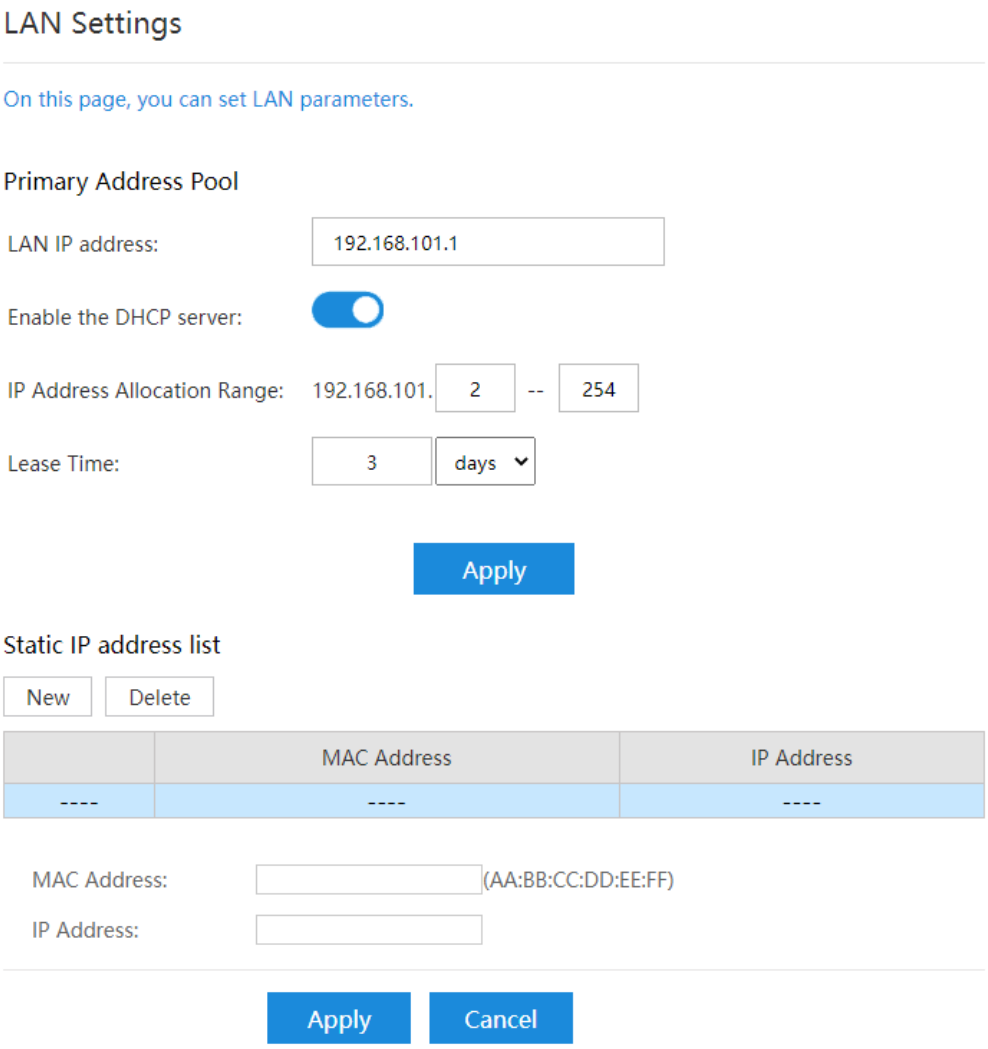
3.5.3 Network Configuration

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 3-11**.

Figure 3-11 LAN Settings



2. Click **Apply**.

The following table describes the LAN parameters.

Table 3-5 LAN parameters

Parameter	Description
LAN IP address	Indicates the management IP address of the local LAN of the device. **NOTE** 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. • You can set the IP address of the LAN-side device to be in the same network segment as the management IP address. • 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.
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 3-12**.

   Figure 3-12 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.

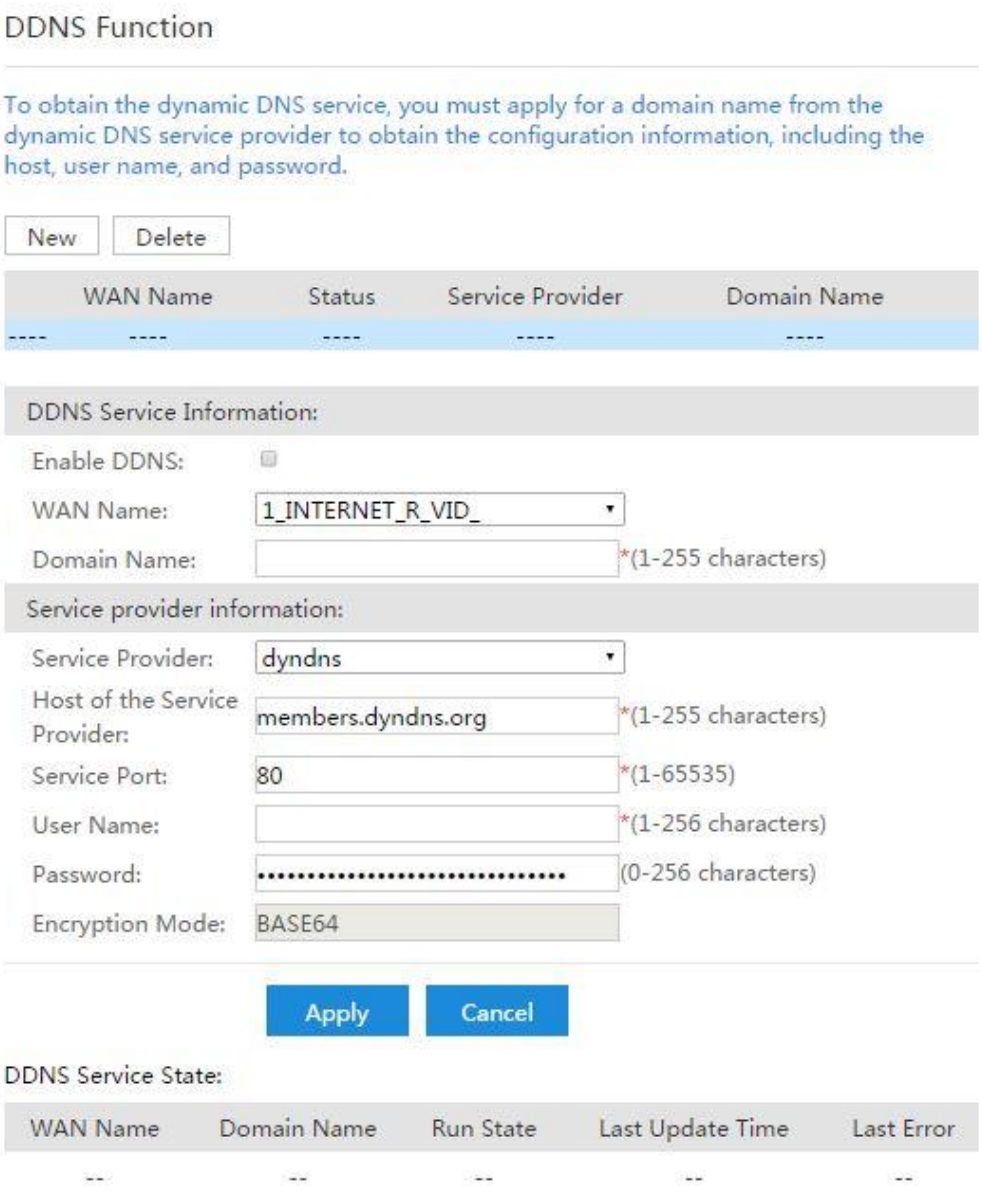
Assume that server A provides HTTP or FTP service and it is connected to the Internet using routers. If server A obtains an IP address through DHCP, or server A is connected to the Internet through PPPoE, PPTP, or L2TP, the IP address is an dynamic IP address. That is, its IP address may change each 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 3-13**.

Figure 3-13 DDNS Function



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.
Service provider information	

Parameter	Description
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	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. **NOTICE** MD5/BASE64 is an insecure encryption algorithm, and can be used only in a secure environment.

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 3-14**.

Figure 3-14 UPnP Function

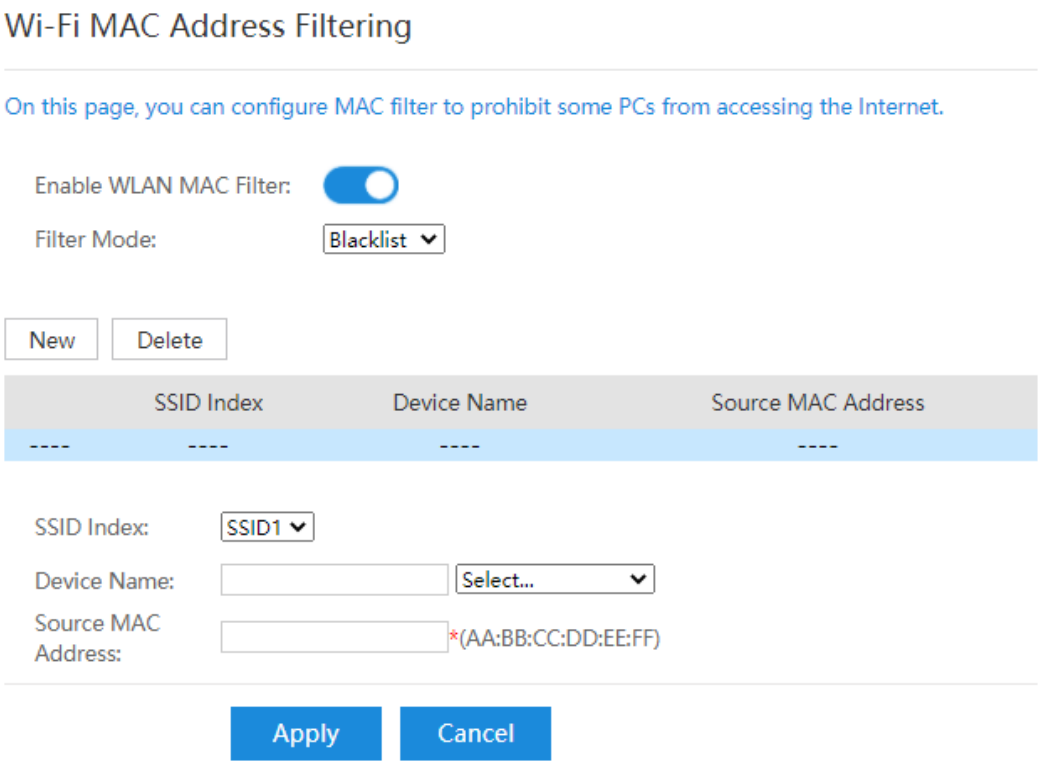
3.5.4 Security Configuration

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

3.5.4.1 Wi-Fi MAC Address Filtering

1. In the navigation tree on the left, choose **Security Configuration** > **Wi-Fi MAC Address Filtering**. In the right pane, select **Enable WAN MAC Filter**, set the filter mode, and click **New**. In the dialog box that is displayed, configure the SSID-based MAC address filter rule, as shown in **Figure 3-15**.

Figure 3-15 Wi-Fi MAC Address Filtering



2. Click **Apply**.

NOTE

The edge ONT stores the MAC address list of terminal devices on the network. The function of MAC address filtering only allows devices that meet a specific rule to normally access the Internet. A terminal may have multiple IP addresses but its MAC address is unique. Therefore, MAC address filtering can effectively control the Internet access permission of PCs in a LAN.

Table 3-6 describes the configuration parameters for wireless network MAC filtering.

Table 3-6 Parameters for wireless network MAC filtering

Parameter	Description
Enable WLAN MAC Filter	Enables or disables the WLAN MAC filter function.
Filter Mode	Indicates the MAC address filter rule of the blacklist or whitelist. • Blacklist: indicates that the data meeting the rule in the filter rule list is not allowed to pass. • Whitelist: indicates that the data meeting the rule in the filter rule list is allowed to pass. The filter mode is global config mode. Thus, the blacklist and whitelist mode cannot be used at the same time.

Parameter	Description
SSID index	Indicates the SSID index of the WLAN for which MAC address filtering is configured.
Device Name	Indicates the device name to be filtered.
Source MAC address	Indicates the source MAC address in the MAC filter rules.

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 3-16**.

Figure 3-16 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 3-17**.

Figure 3-17 Parental Control

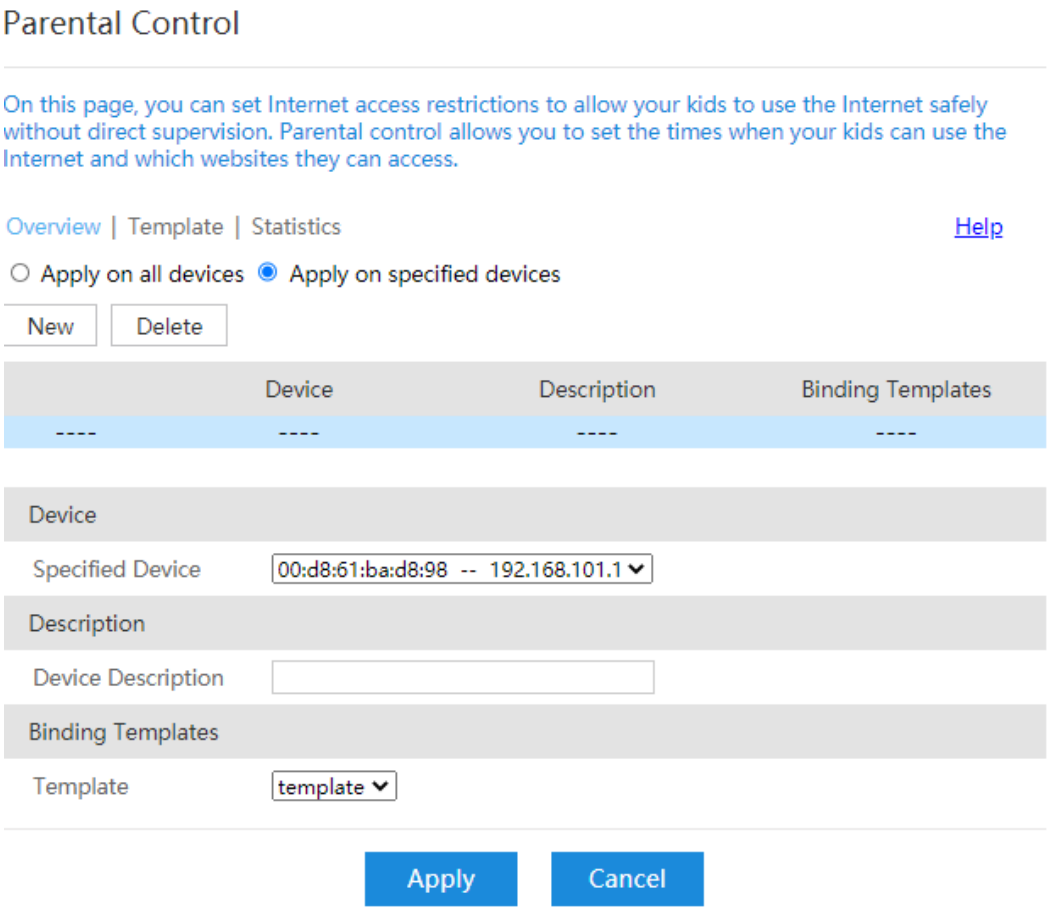


Table 3-7 describes the parameters related to the Parental Control.

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 **Apply on specified devices** 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.

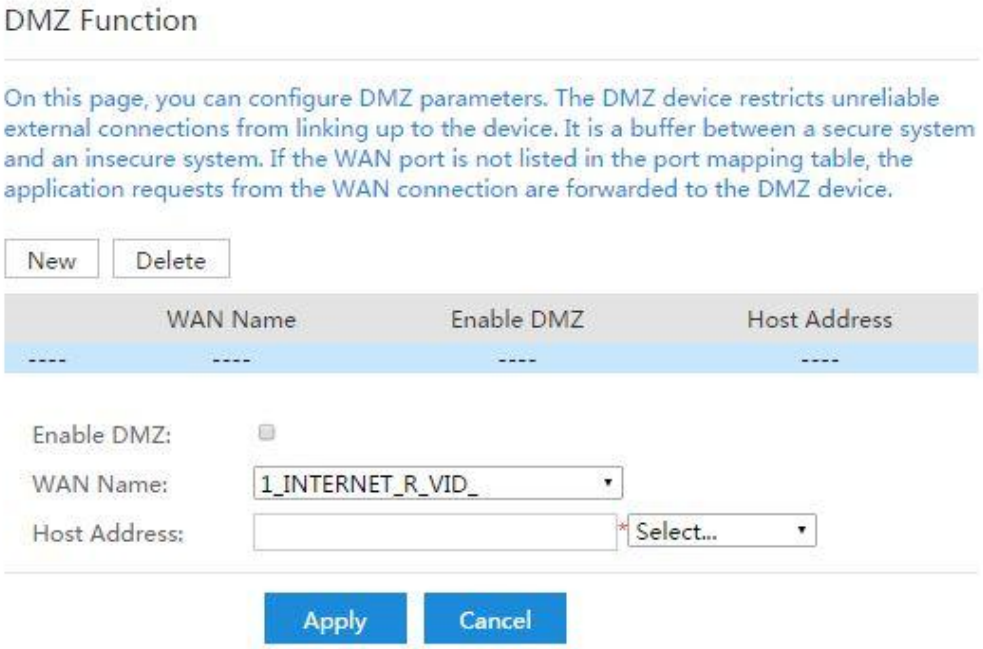
NOTE

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 3-18**.

   Figure 3-18 DMZ Function

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.

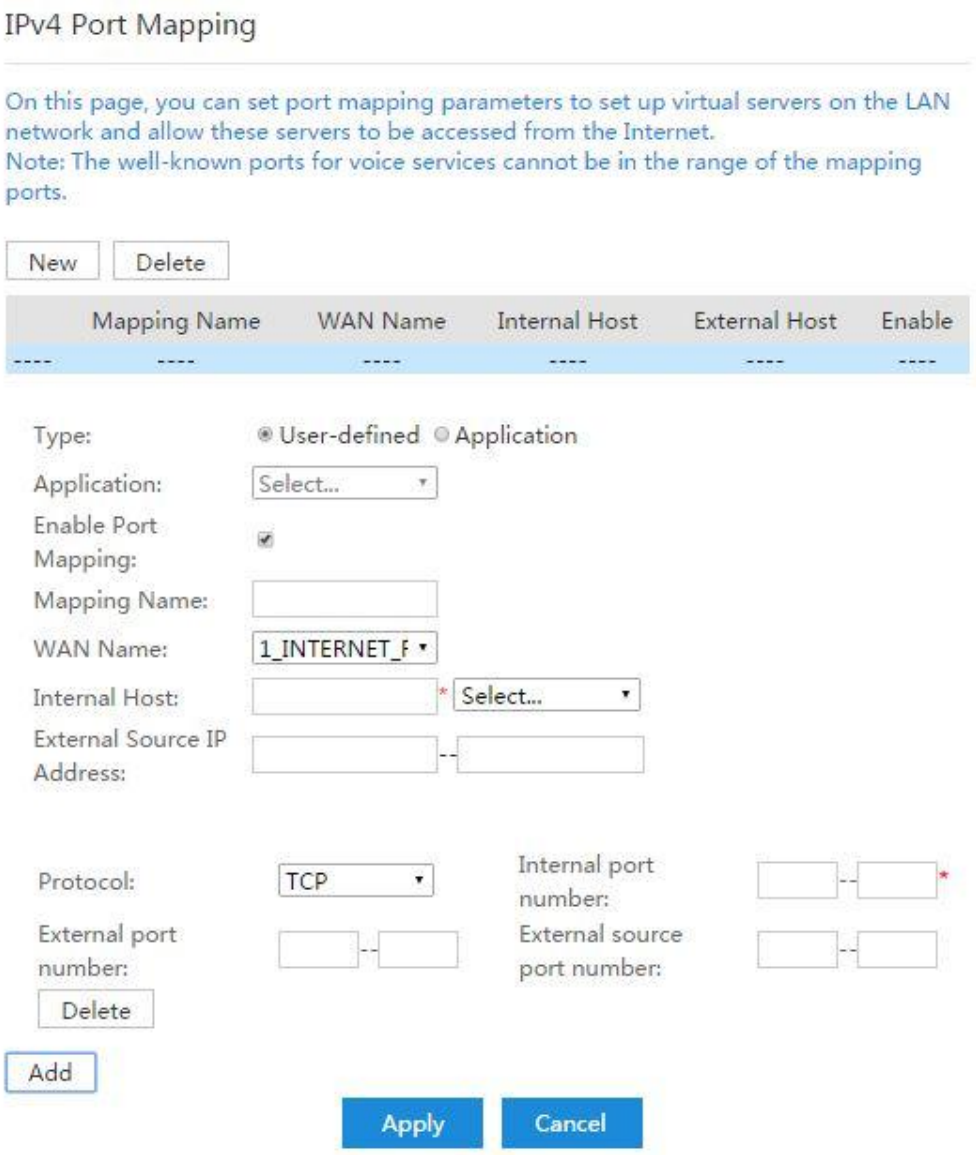
3.5.4.5 IPv4 Port Mapping

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 3-19**.

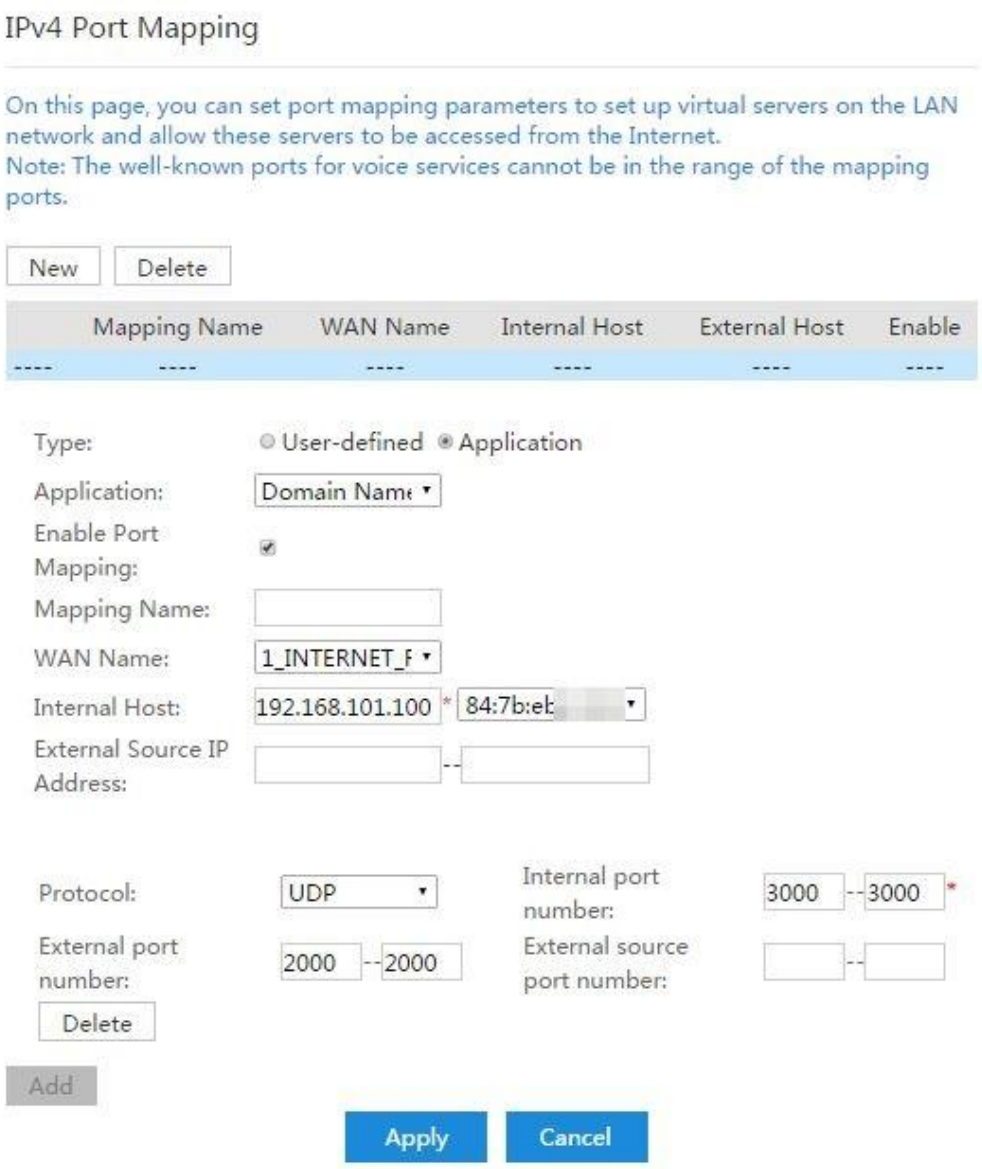
Figure 3-19 IPv4 Port Mapping



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.



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 **User-defined** or **Application**. If the type is set to **Application**, you can select a server from the **Application** drop-down list box.
Enable Port Mapping	Indicates whether to enable port mapping.
Mapping Name	Indicates the name of the port mapping rule.

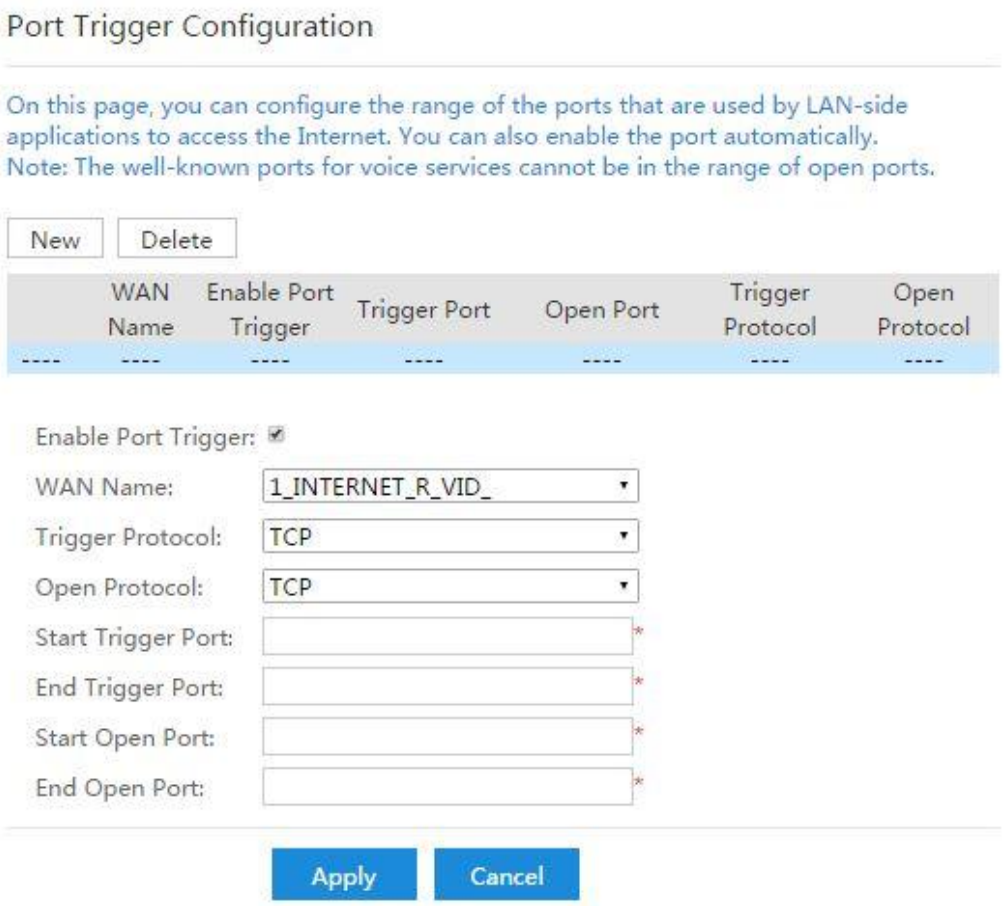
Parameter	Description
WAN Name	Indicates the name of the WAN interface where port mapping is enabled.
Internal Host	Indicates the IP address of the host to which the port is mapped.
External Source IP Address	Indicates the source IP address of the external data packet.
Protocol	Indicates the protocol 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 3-20**.

Figure 3-20 Port Trigger Configuration



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.

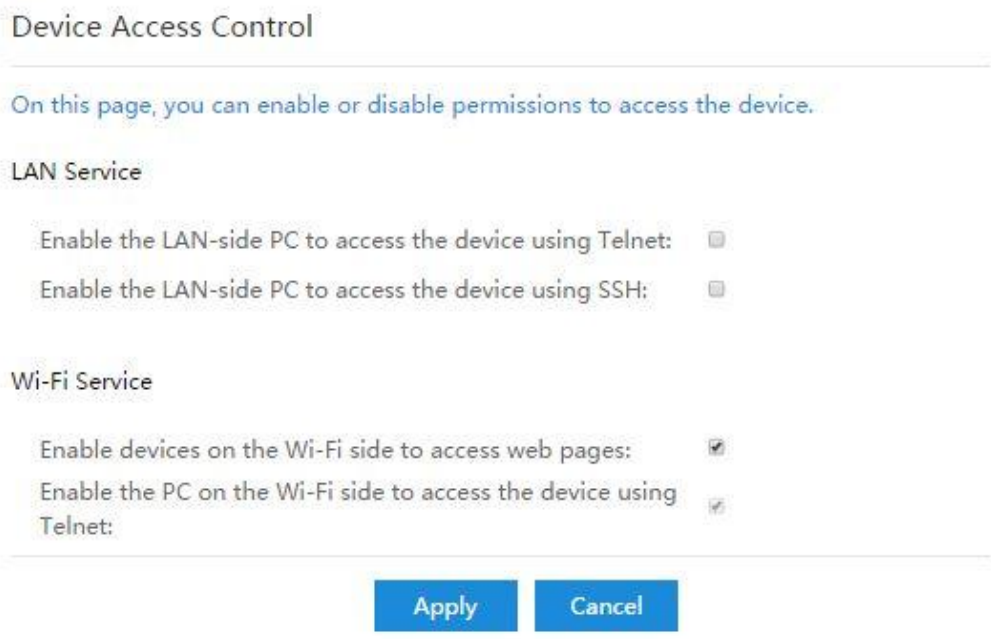
3.5.4.7 Device Access Control

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 3-21**.

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 3-21 Device Access Control



2. Click **Apply**.

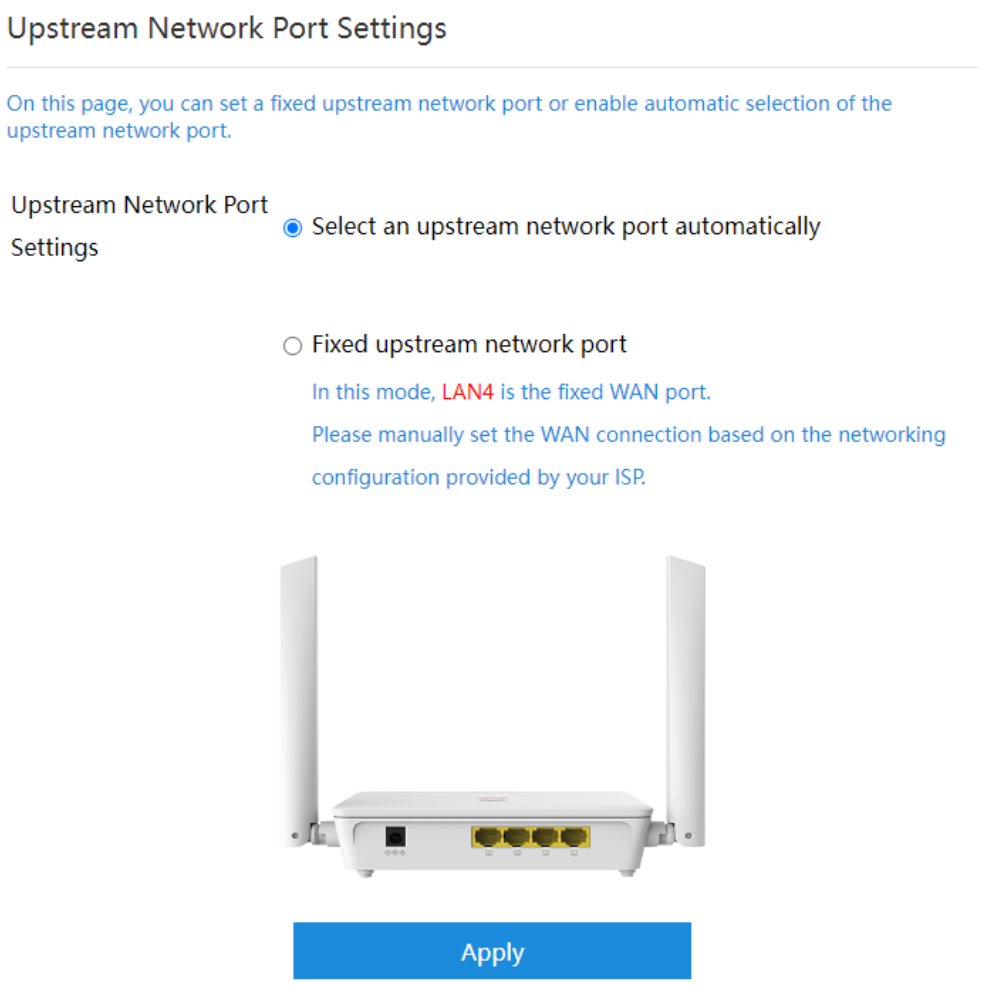
3.5.5 System Management

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 3-22**.

Figure 3-22 Upstream Network Port Settings

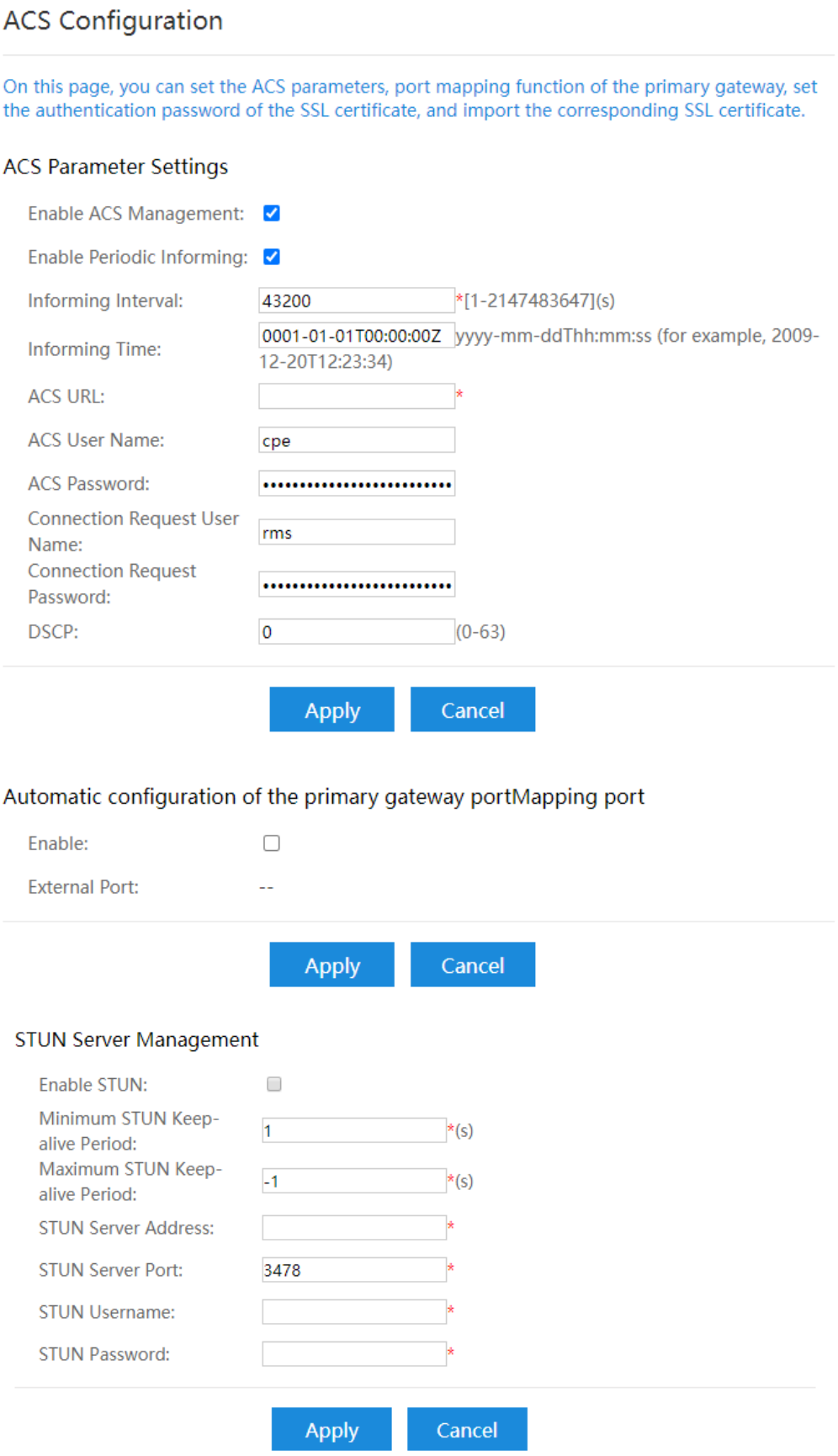


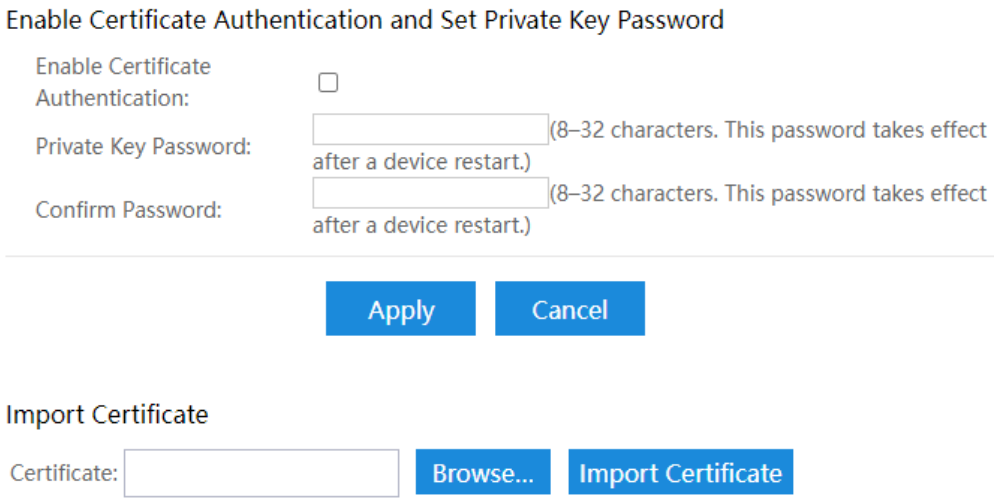
2. Click **Apply**.

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 3-23**.

Figure 3-23 TR-069





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 **ACS Management**.
Enable Periodic Informing	Indicates whether to enable the notification function. • If the notification function is enabled, the ONT actively sends a connection request to the TR-069 server. • If the notification function is disabled, the ONT does not actively send a connection request to the TR-069 server. When the notification function is enabled, the **Informing Interval** and **Informing Time** 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.

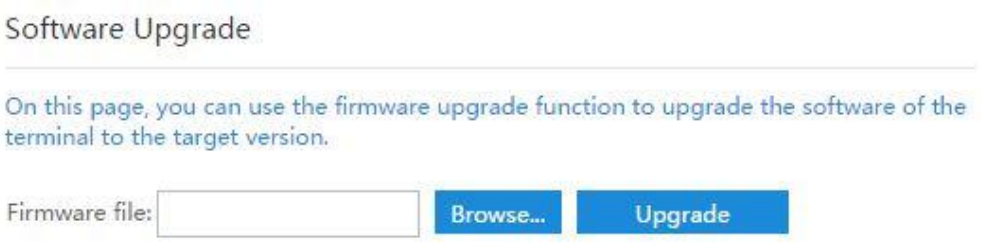
Parameter	Description
Connection Request User Name	Indicates the user name to be carried when the TR-069 server initiates a connection request to the ONT.
Connection Request Password	Indicates the password to be carried when the TR-069 server initiates a connection request to the ONT.
DSCP	Defined by 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 *STUNEnable*. If an empty string and *STUNEnable* is *true*, 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 *STUNEnable*. 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.
Enable Certificate Authentication and Set Private Key Password	
Enable Certificate Authentication	Enable the certificate if the ACS is connected through SSL.
Private Key Password	Sets the private key password after the certificate is enabled.
Confirm Password	Confirms the password and ensures that it is the same as **Private Key Password**.
Import Certificate	
Certificate	Indicates the certificate file provided by the carrier.

3.5.5.3 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 3-24**.

Figure 3-24 Software Upgrade

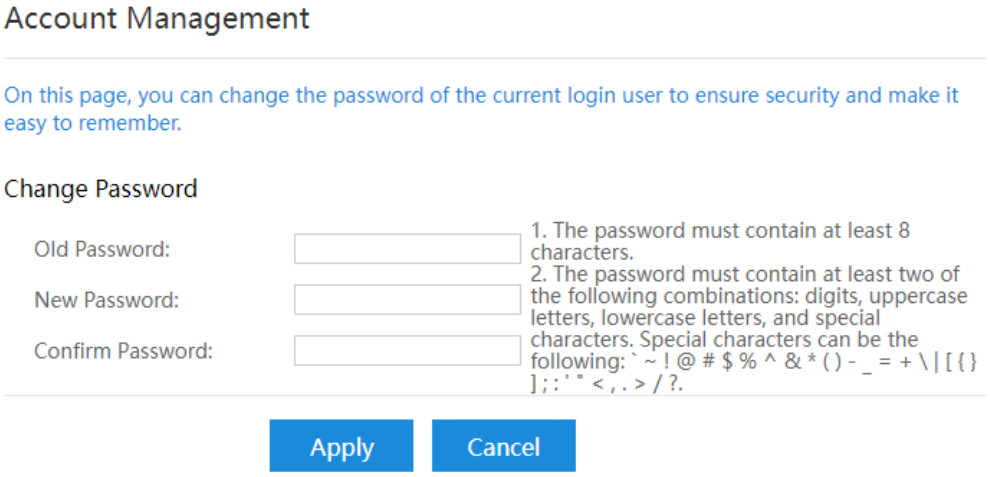


2. After the upgrade is successful, a message is displayed indicating that the device needs to be reset. Click **Restart**. The configuration data takes effect after the device is reset.

3.5.5.4 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 3-25**.

Figure 3-25 Account Management



NOTICE

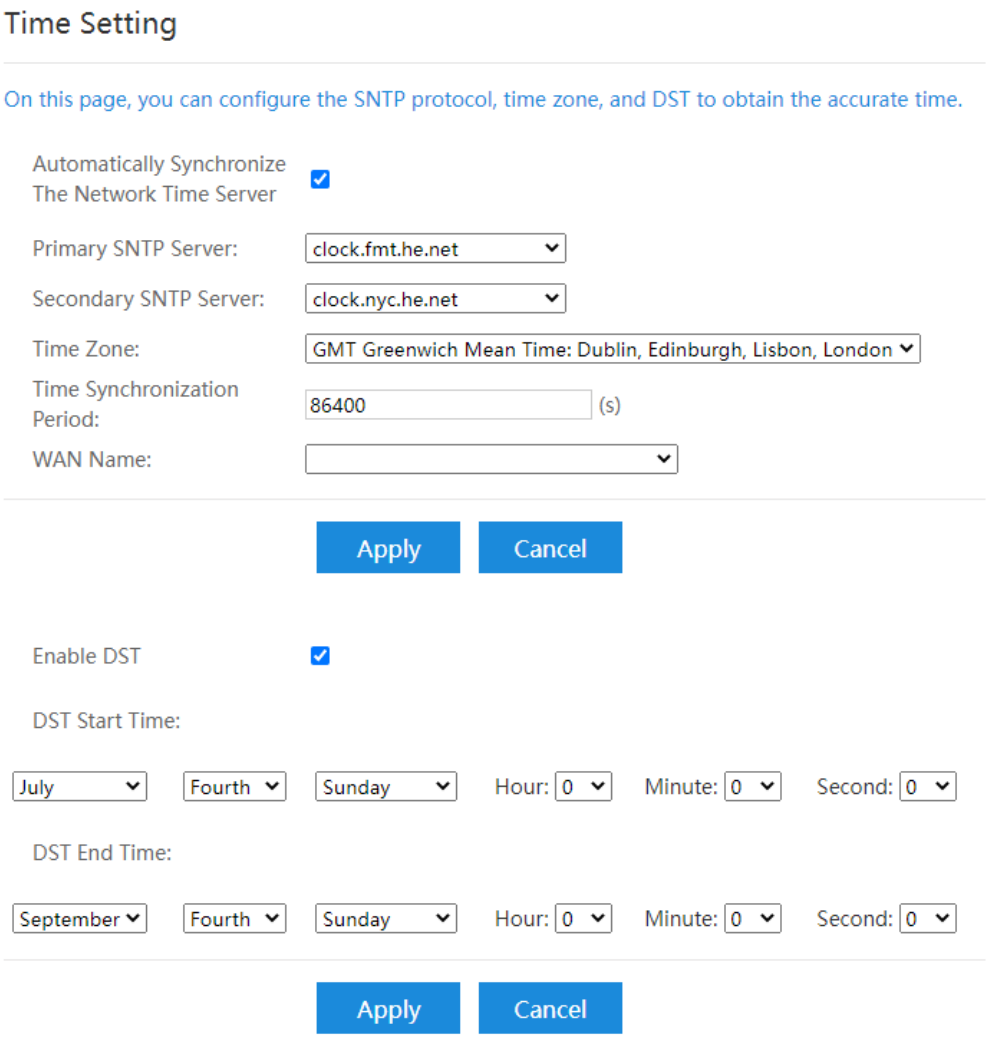
To enhance system security, change the password to a password that meets security requirements after the first successful login. It is recommended that you change the password periodically.

2. Click **Apply**.

3.5.5.5 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 3-26**.

Figure 3-26 Time Setting



2. Click **Apply**.

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

Table 3-12 Parameters related to the system time

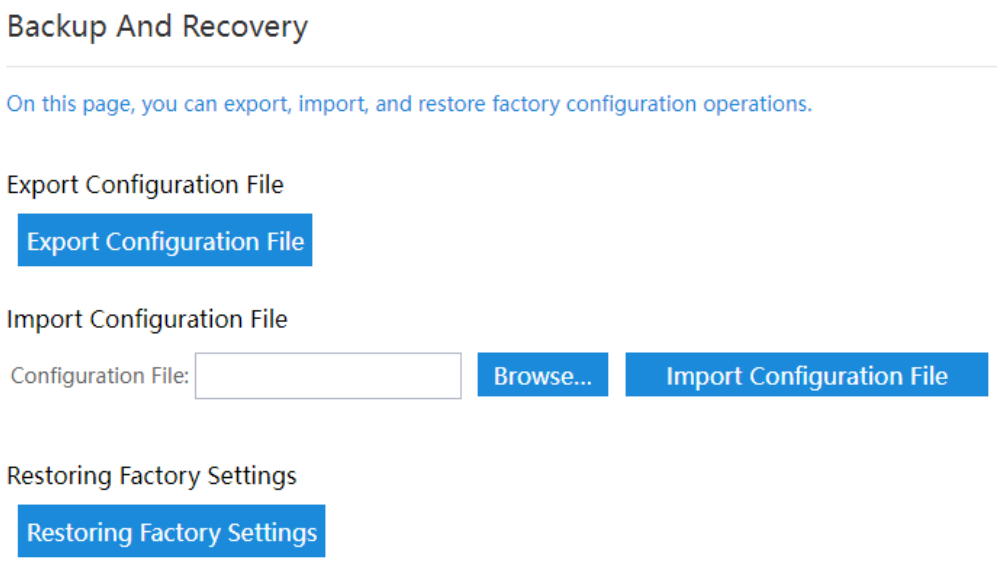
Parameter	Description
Automatically Synchronize The Network Time Server	Indicates whether to enable the auto synchronization network time server, that is, SNTP server.
Primary SNTP Server	Indicates the primary SNTP server.
Secondary SNTP Server	Indicates the secondary SNTP server.
Time Zone	Indicates 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.

3.5.5.6 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 facory configuration operations.

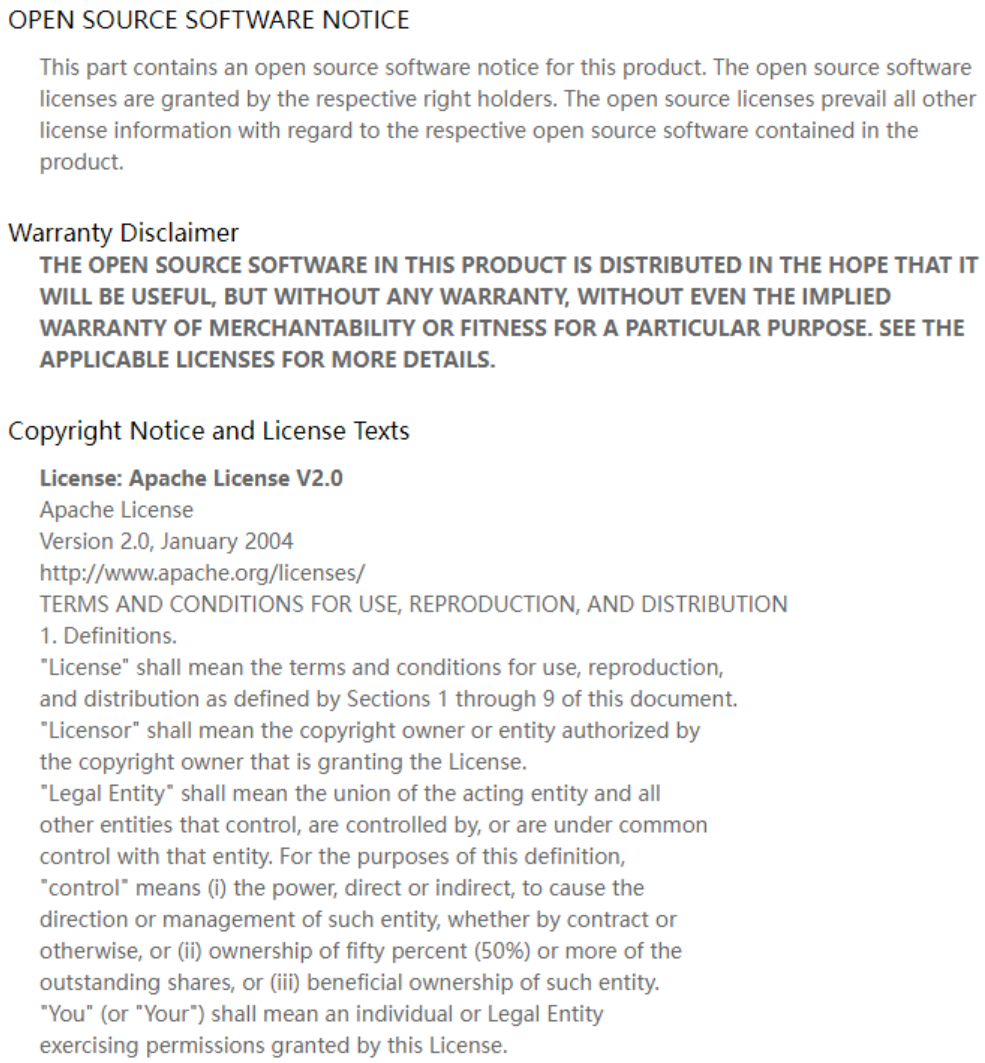
Figure 3-27 Backup and recovery



3.5.5.7 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 3-28**.

Figure 3-28 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.

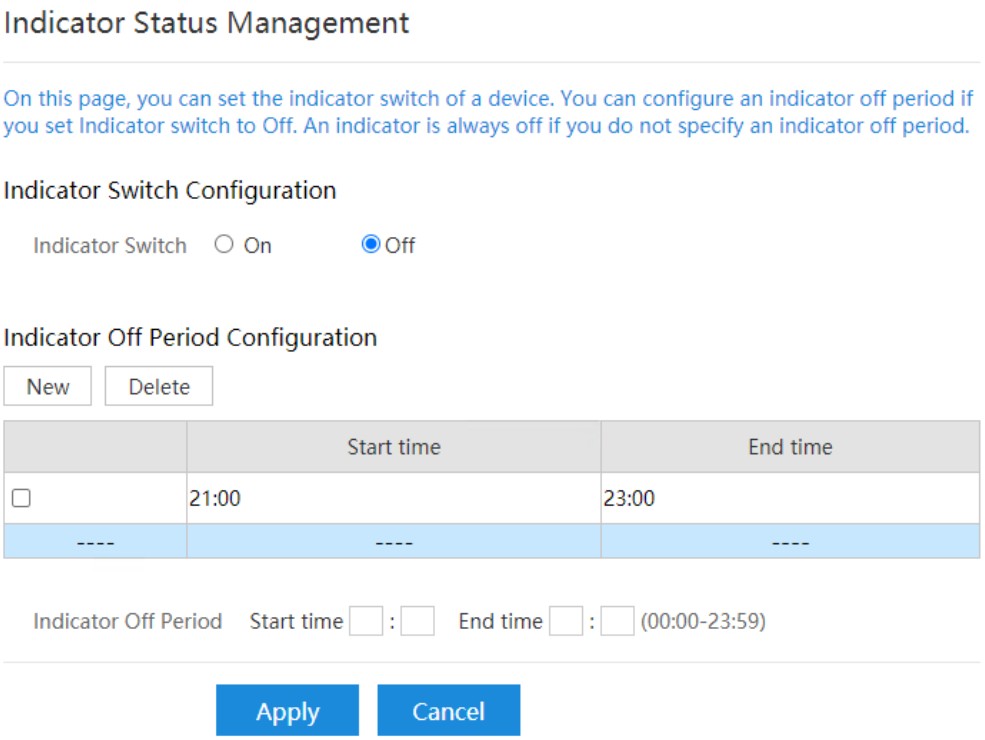
Copyright Notice and License Texts

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.

3.5.5.8 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 3-29**.

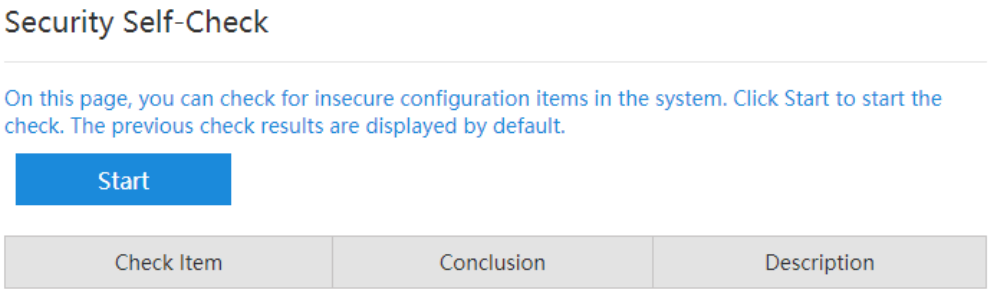
Figure 3-29 Indicator status management



3.5.5.9 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 incecure configuration items in the system. Click **Start** to start the check, as shown in **Figure 3-30**.

Figure 3-30 Security self-check



3.5.6 Maintenance Diagnosis

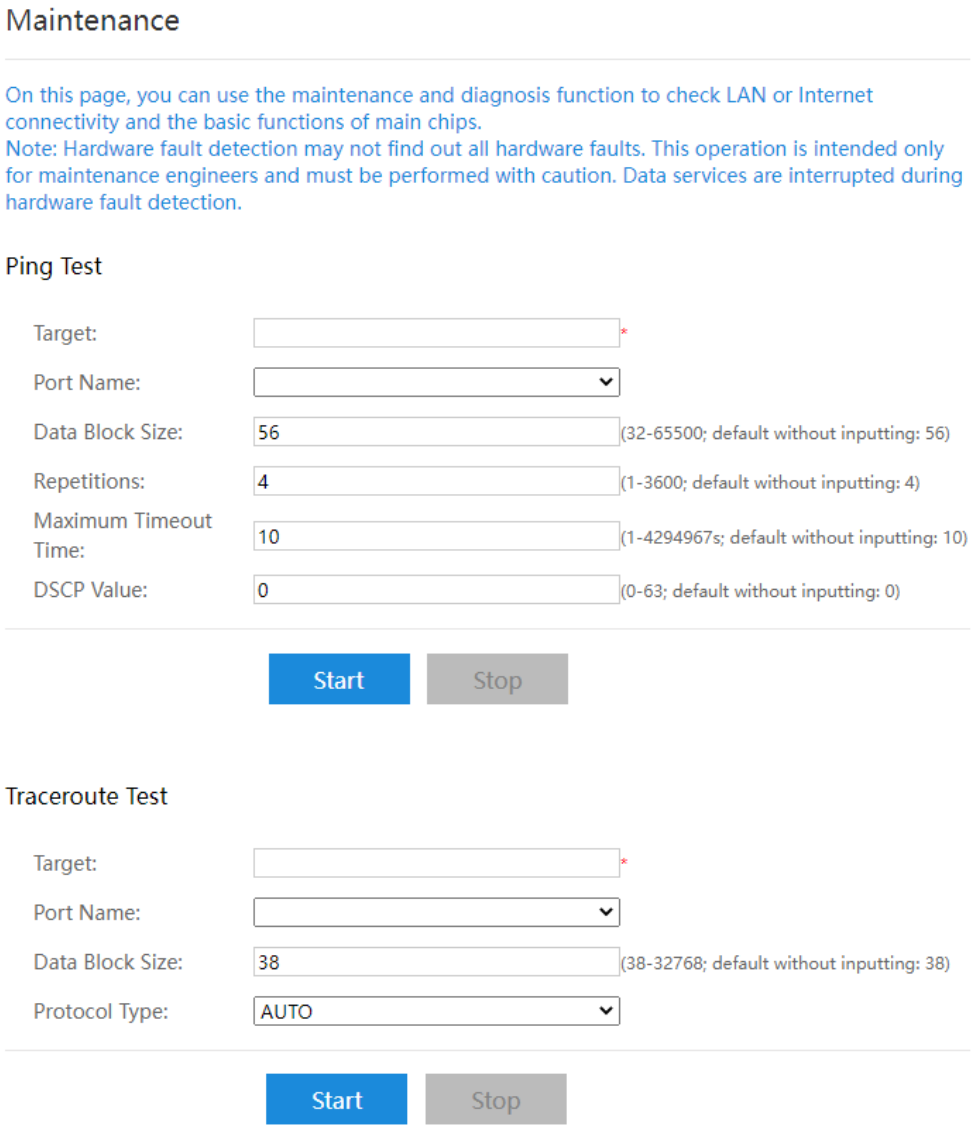
This topic describes how to configure the Maintenance Diagnosis through the web page.

3.5.6.1 Maintenance

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

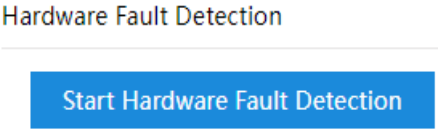
1. In the pane on the right, enter the target IP address or host name in Target and WAN name, and then click Start, as shown in **Figure 3-31**.

Figure 3-31 Ping test



   - 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 3-32**.

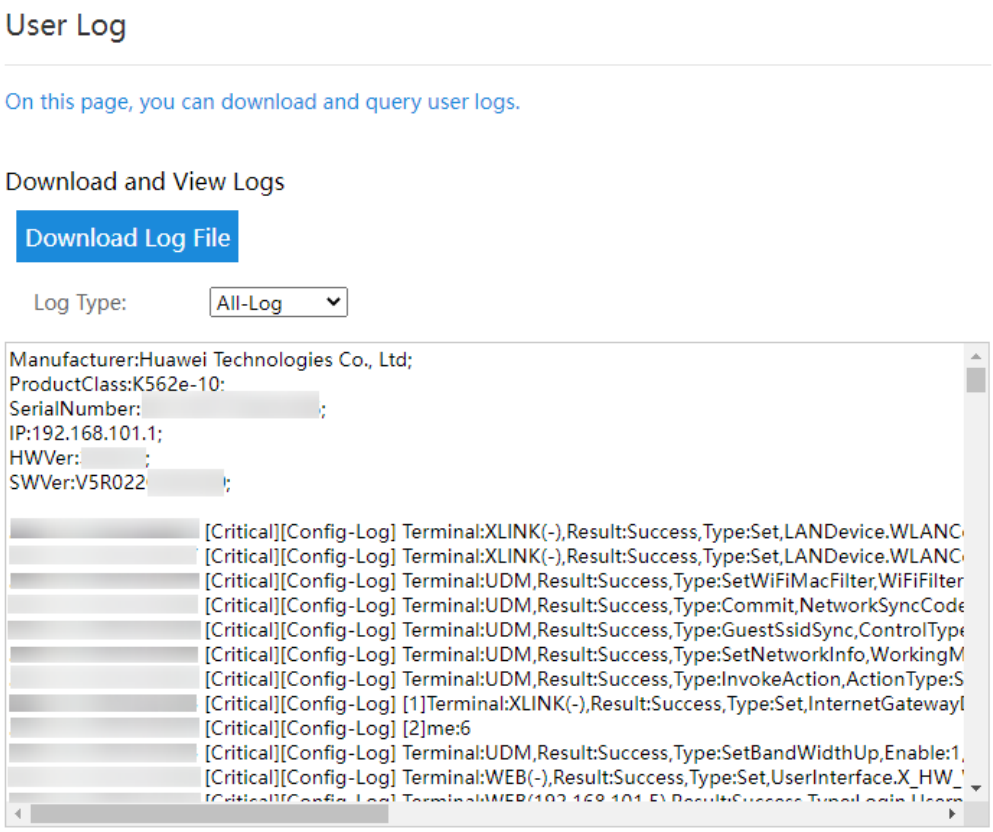
Figure 3-32 Hardware fault detection



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 3-33**.

Figure 3-33 User Log



- 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**.

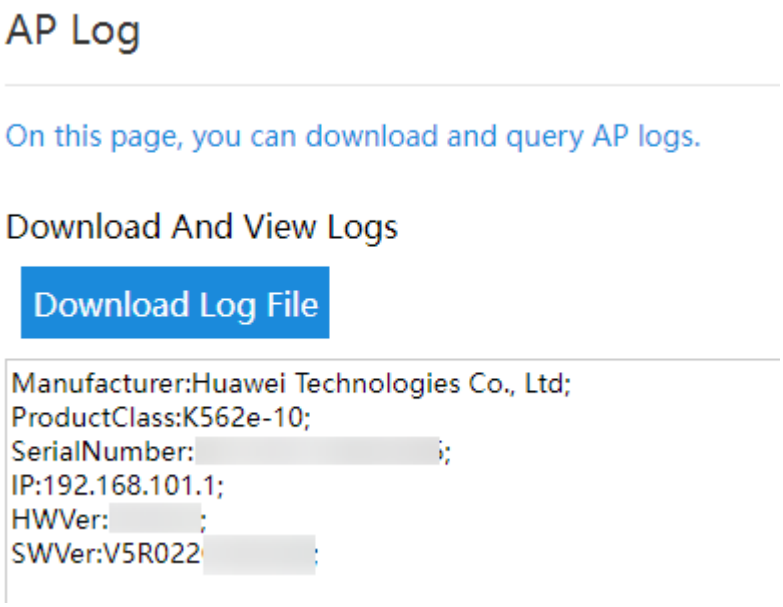
NOTICE

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 3-34**.

Figure 3-34 AP Log



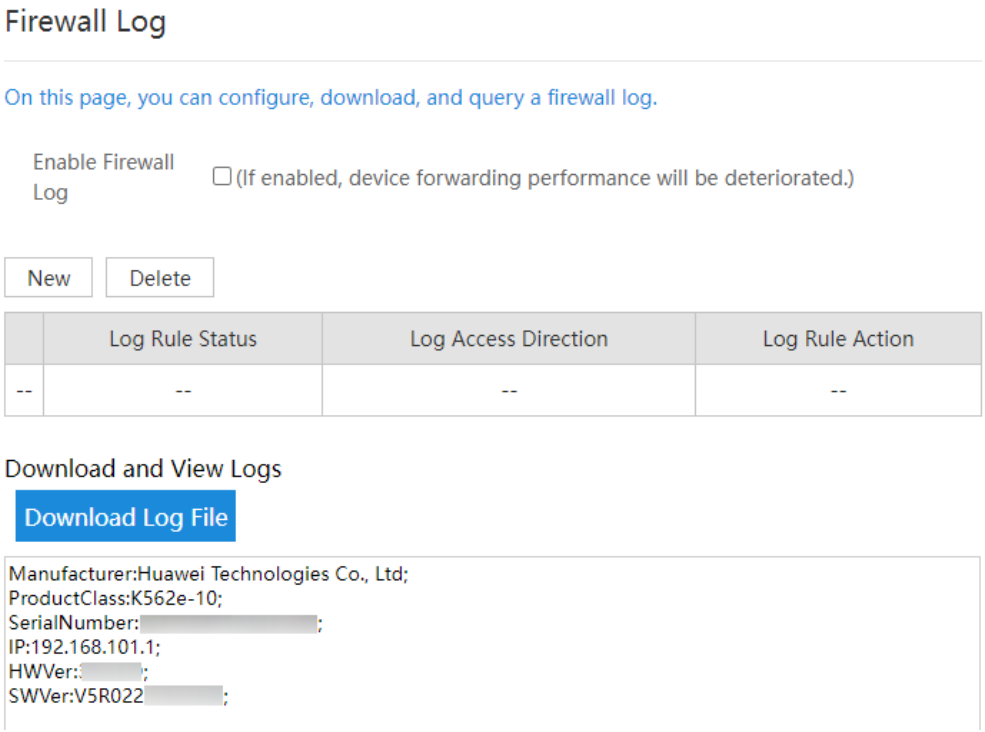
NOTICE

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.

3.5.6.4 Firewall Log

In the navigation tree on the left, choose **Maintenance Diagnosis** > **Firewall Log**. In the pane on the right, you can viewl logs and download log files, as shown in **Figure 3-35**.

Figure 3-35 Firewall Log



- 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.

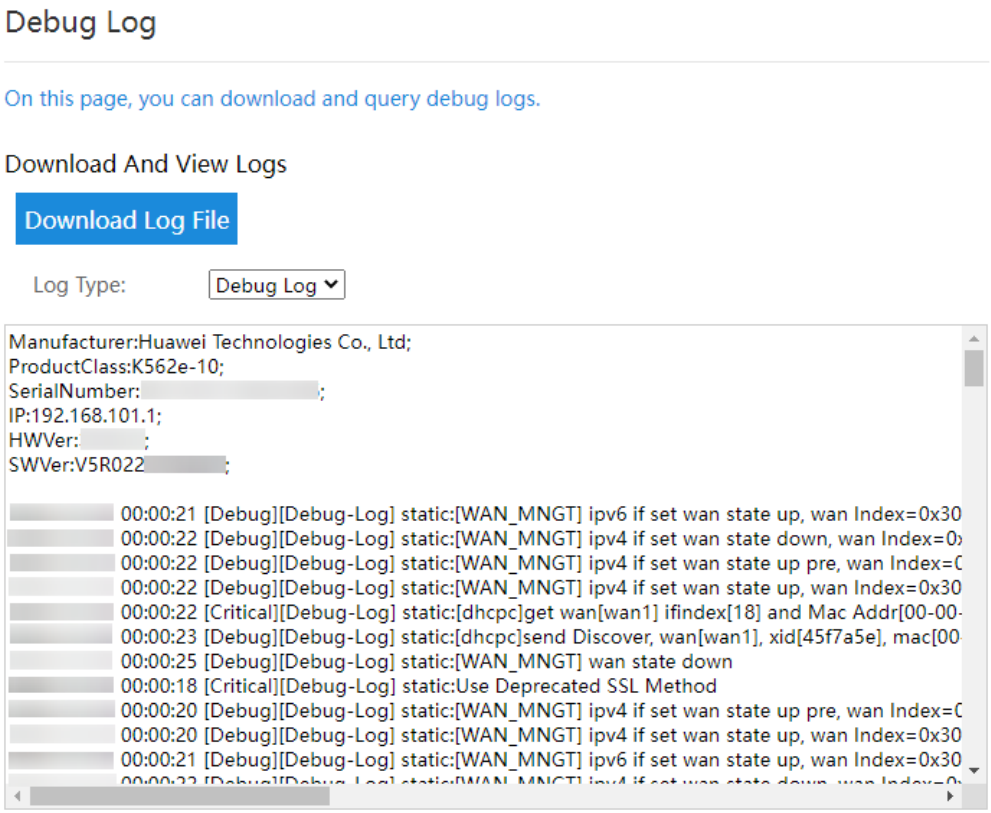
NOTICE

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 3-36**.

Figure 3-36 Debug Log



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.

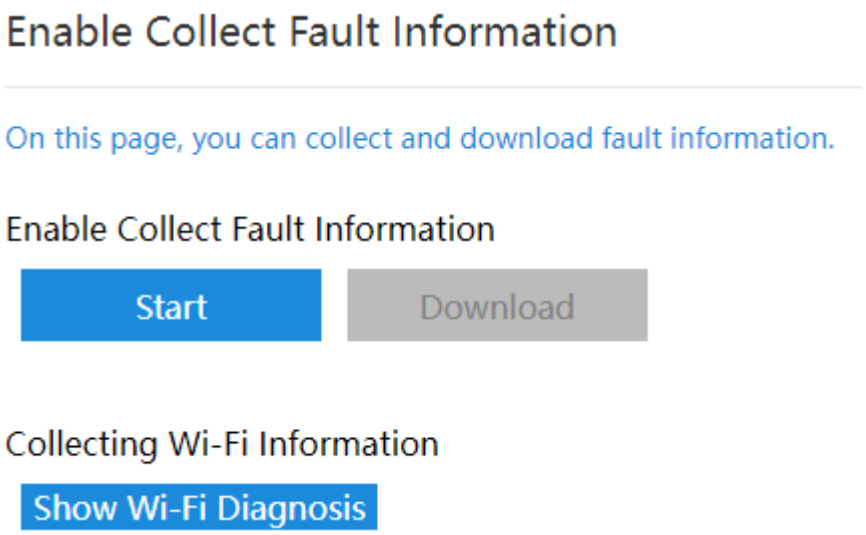
NOTICE

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 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 3-37**.

Figure 3-37 Fault Info Collect



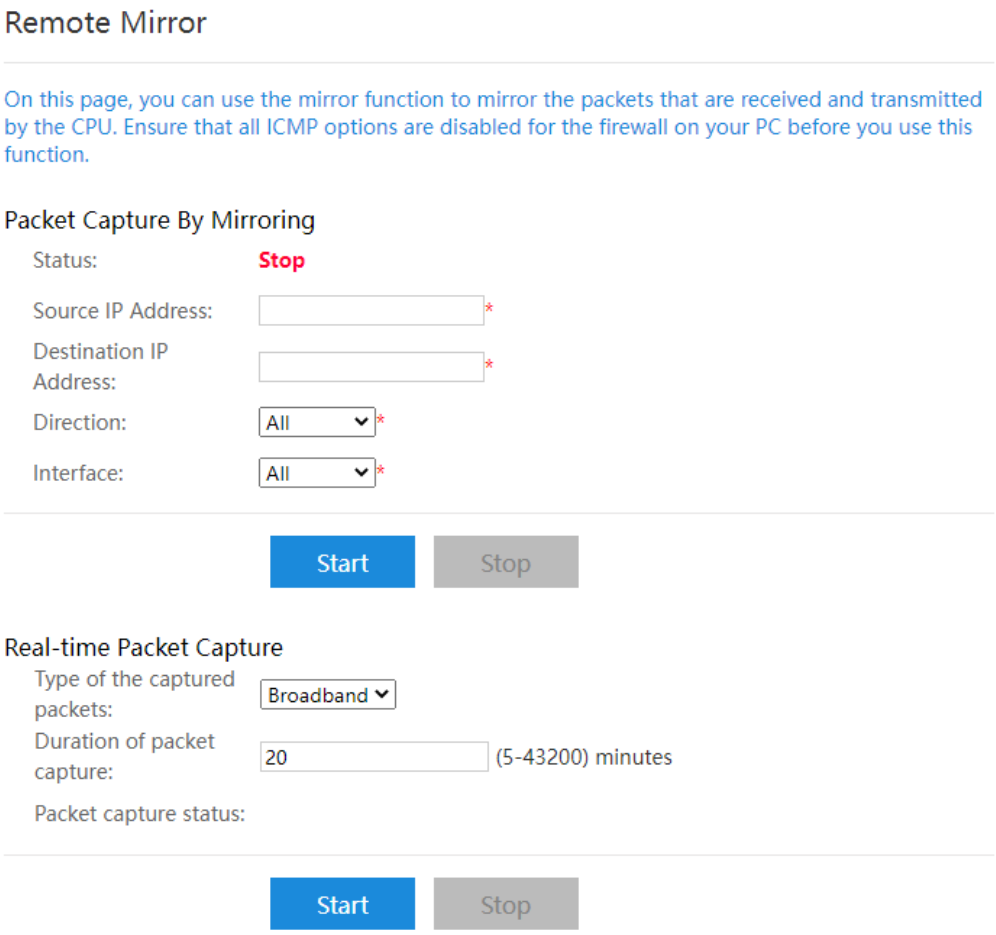
NOTE

- 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.

3.5.6.7 Remote Mirror

1. In the navigation tree on the left, choose **Maintenance Diagnosis** > **Remote Mirror**, as shown in **Figure 3-38**.

Figure 3-38 Remote Mirror



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

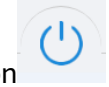
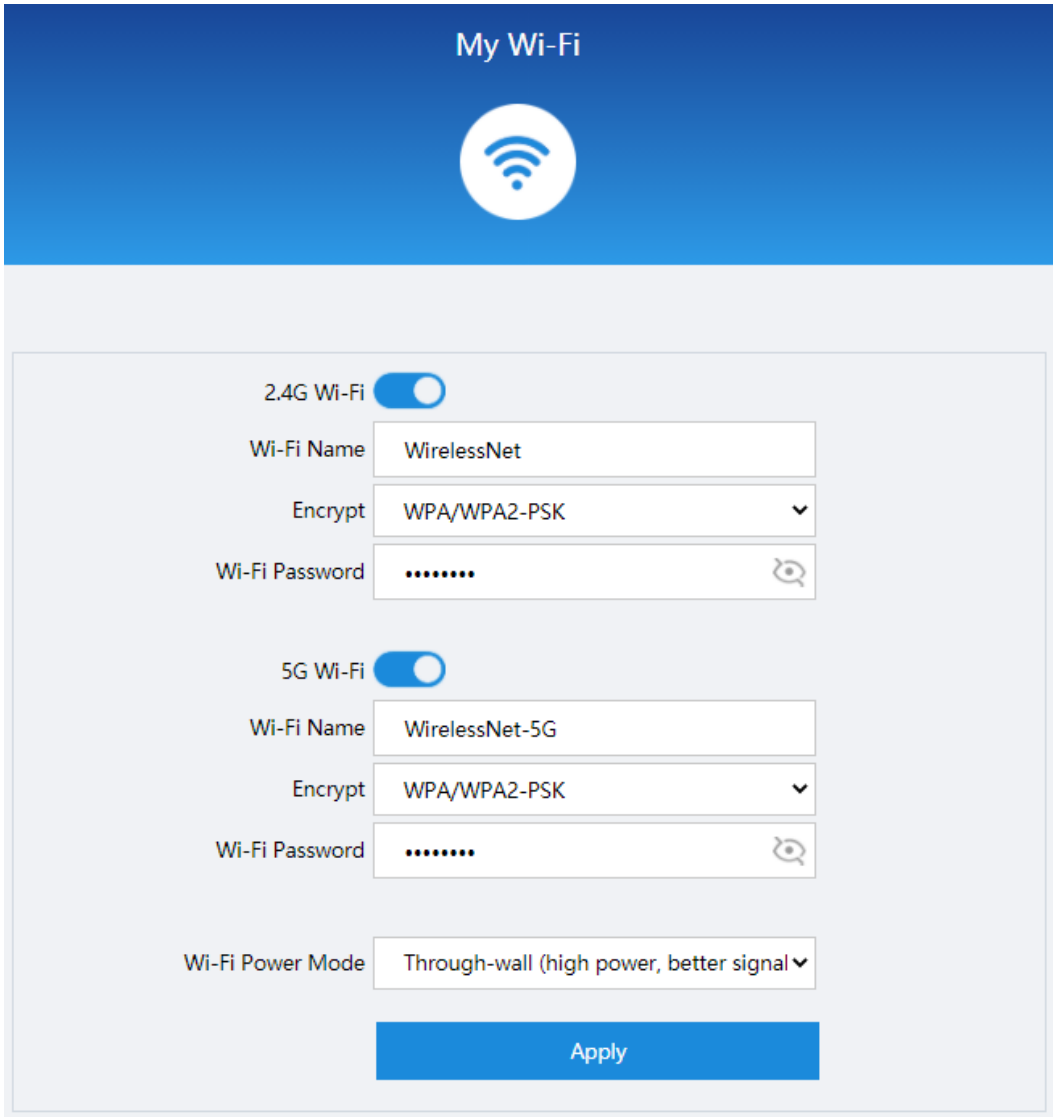
On the homepage, you can view the current home network topology, Internet access mode, system running duration, and local IP address. A click on  in the lower part of the page restarts the device.

Figure 4-1 Homepage

4.2 My Wi-Fi

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

Figure 4-2 My Wi-Fi



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 availabe when **Encrypt** is set to **WPA2-PSK**, **WPA/WPA2-PSK**, **WPA3-SAE**, **WPA2/WPA3-PSKandSAE**.
Wi-Fi Power Mode	The mode can be set to the following as required: • Through-wall (high power, better signal) • Standard (standard power, common signal) • Sleep (low power, weak signal)

4.3 More

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

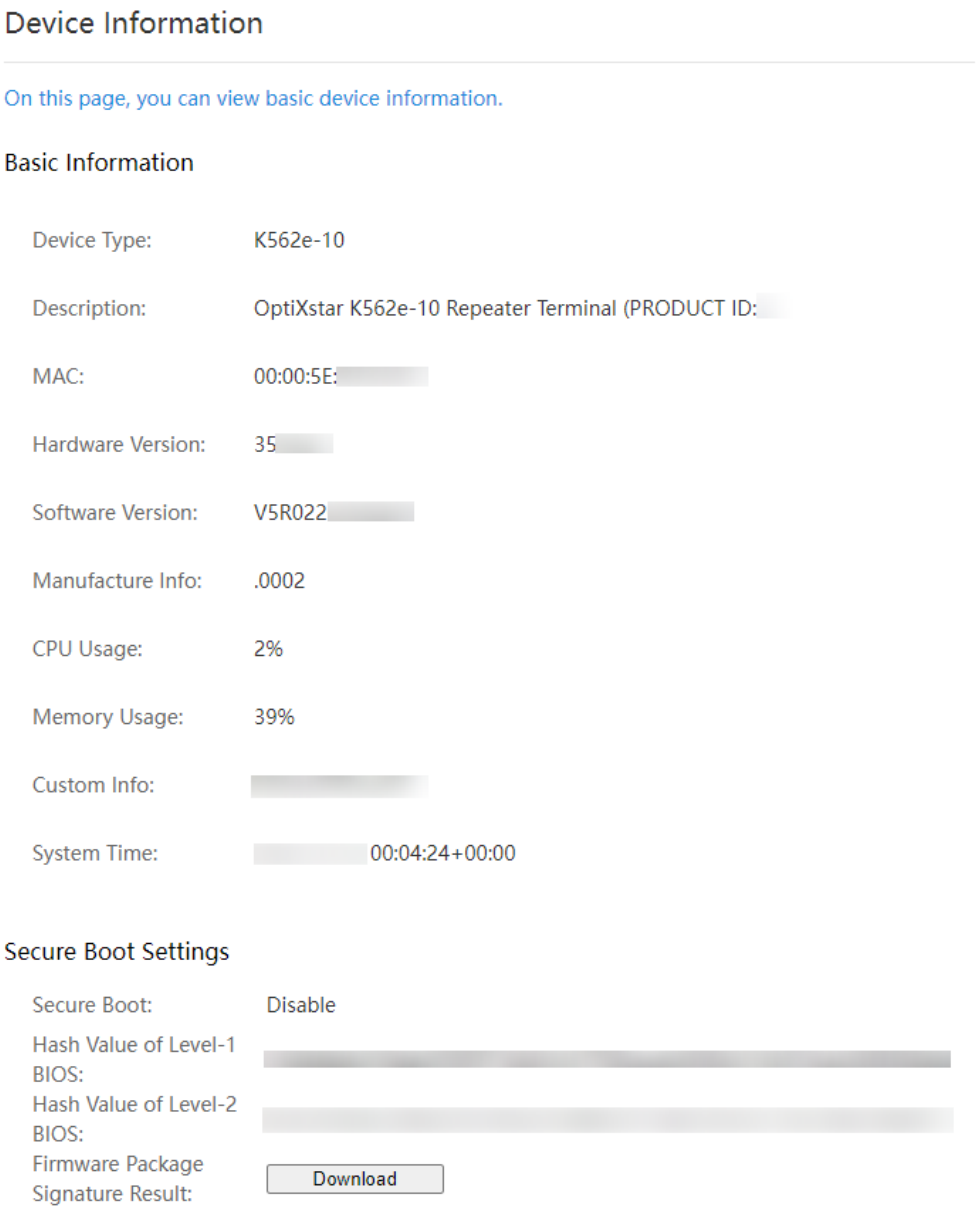
4.3.1 System Information

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**.

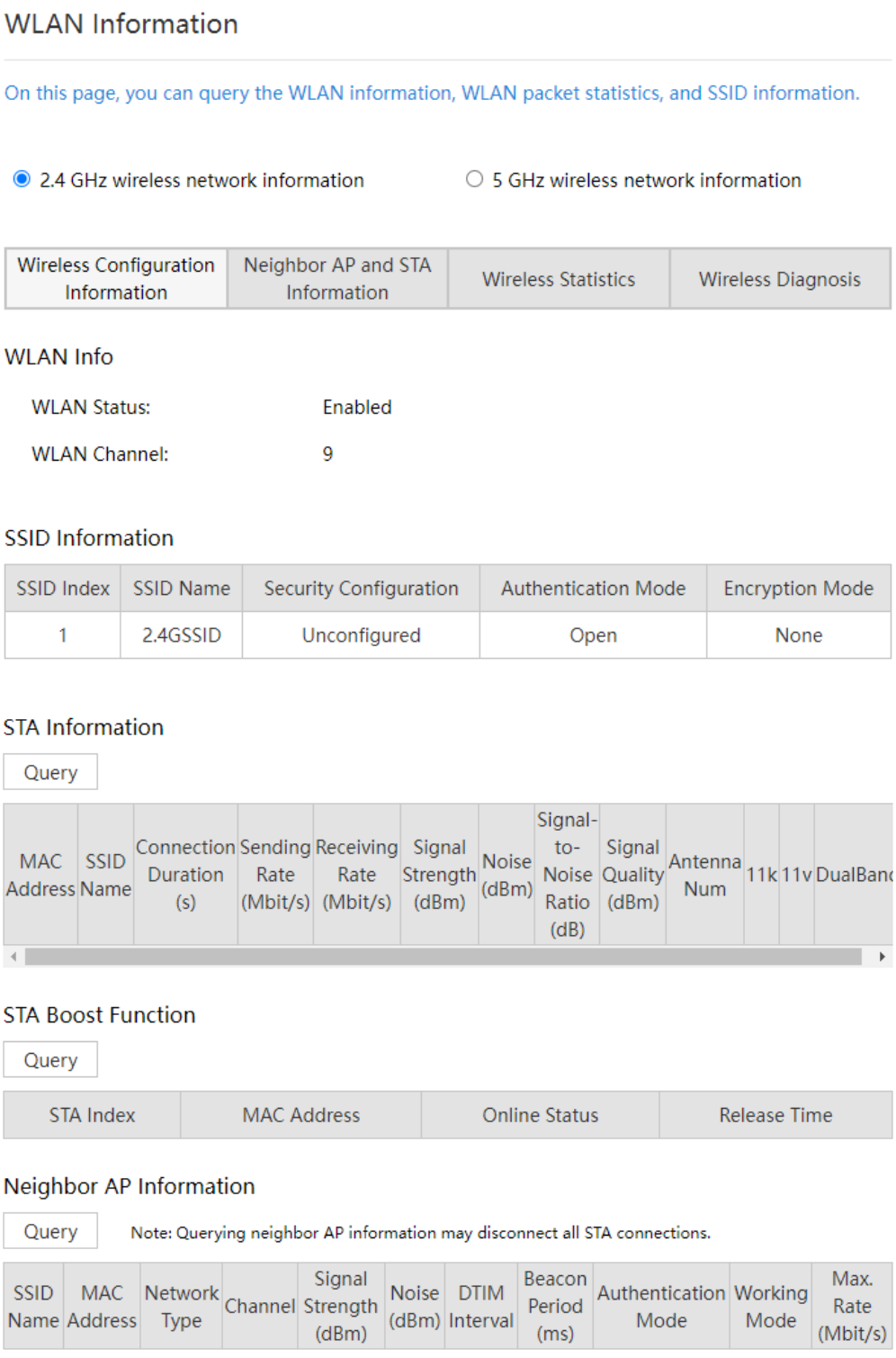
Figure 4-3 Device Information



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 Packet Statistics

SSID Index	SSID Name	Receive (RX)				Transmit (TX)			
		Bytes	Packets	Error	Discarded	Bytes	Packets	Error	Discarded
1	2.4GSSID	0	0	0	0	11328	114	0	0

STA Event Log

Download Log File

```
Manufacturer:Huawei Technologies Co., Ltd;
ProductClass:K562e-10;
SerialNumber:                ;
IP:192.168.101.1;
HWVer:35      ;
SWVer:V5R022          ;

          00:00:44 [5G] [vap4] [CON][DISCONNECT_STA]{wal_cfg80211_start_disconnect::reason_code
          00:00:44 [5G] [vap4] [CON][DISCONNECT_STA]{wal_cfg80211_start_disconnect::reason_code
          00:00:44 [5G] [vap4] hmac_config_down_sync_all: WLAN DOWN success
          00:00:44 [5G] [vap4] [CON][DISCONNECT_STA]{wal_cfg80211_start_disconnect::reason_code
          00:00:45 [2G] [vap0] [CON][DISCONNECT_STA]{wal_cfg80211_start_disconnect::reason_code
          00:00:45 [2G] [vap0] [CON][DISCONNECT_STA]{wal_cfg80211_start_disconnect::reason_code
          00:00:45 [2G] [vap0] hmac_config_down_sync_all: WLAN DOWN success
          00:00:45 [2G] [vap0] [CON][DISCONNECT_STA]{wal_cfg80211_start_disconnect::reason_code
          00:00:45 [2G] [vap0] [CON][DISCONNECT_STA]{wal_cfg80211_start_disconnect::reason_code
          00:00:45 [2G] [vap0] hmac_config_down_sync_all: WLAN DOWN success
          00:00:45 [2G] [vap0] [CON][DISCONNECT_STA]{wal_cfg80211_start_disconnect::reason_code
```

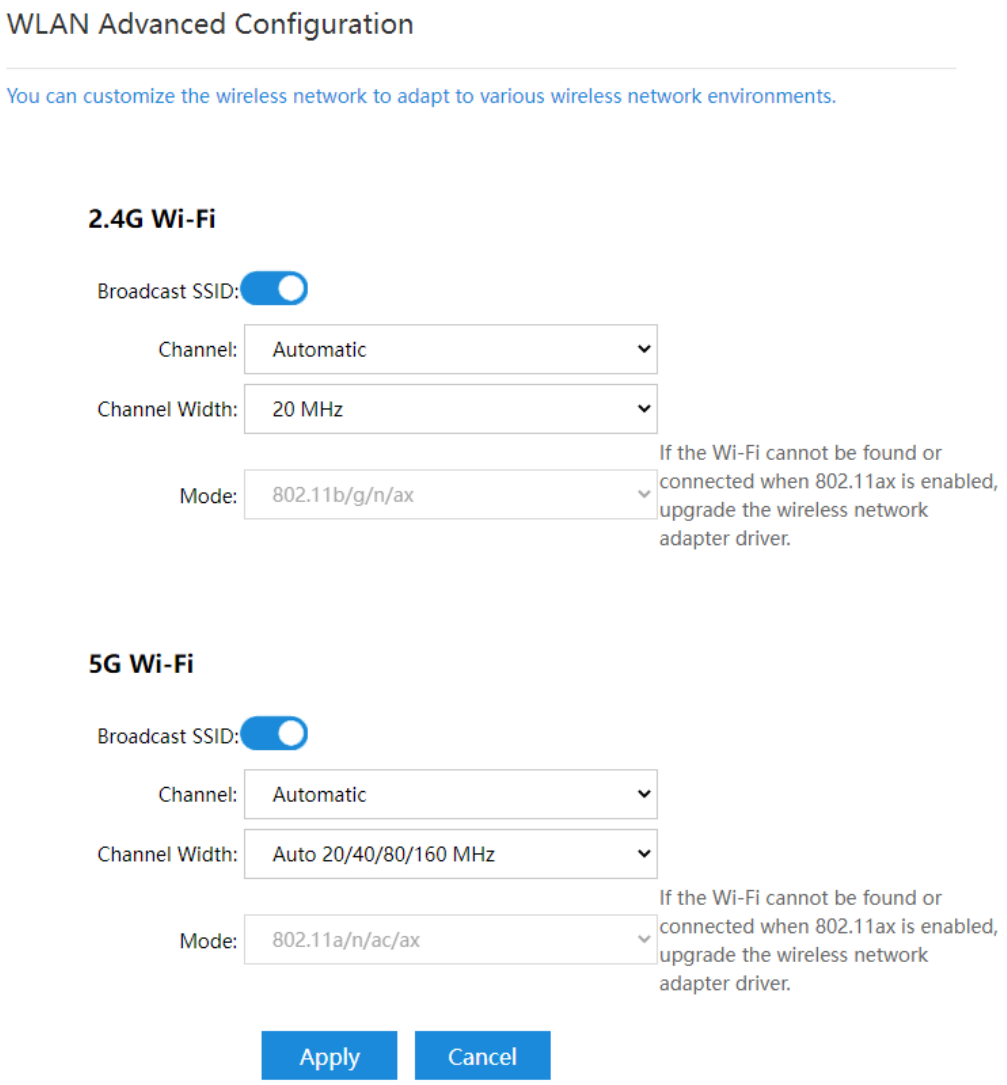
4.3.2 WLAN

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



2. Click **Apply**.

Table 4-2 describes the WLAN advanced parameters.

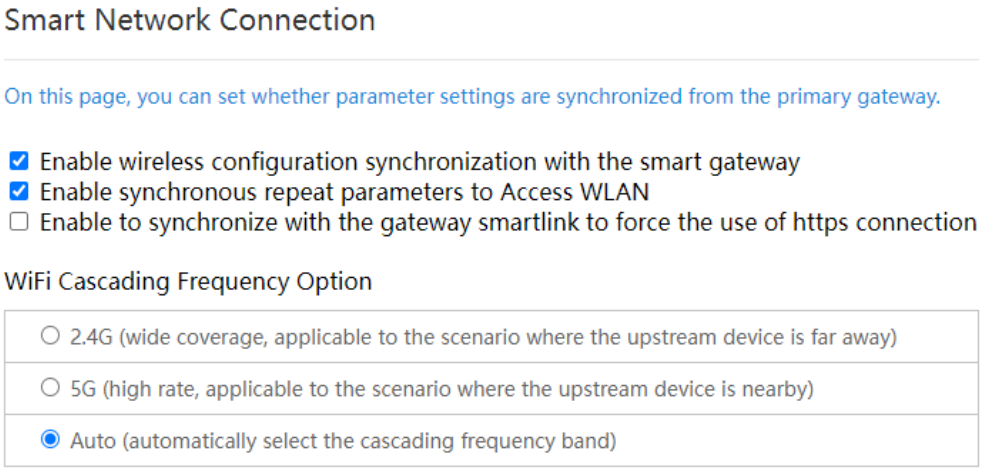
Table 4-2 WLAN advanced parameters

Parameter	Description
Broadcast SSID	Indicates whether to enable or hide broadcast. • 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. • 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.
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**.

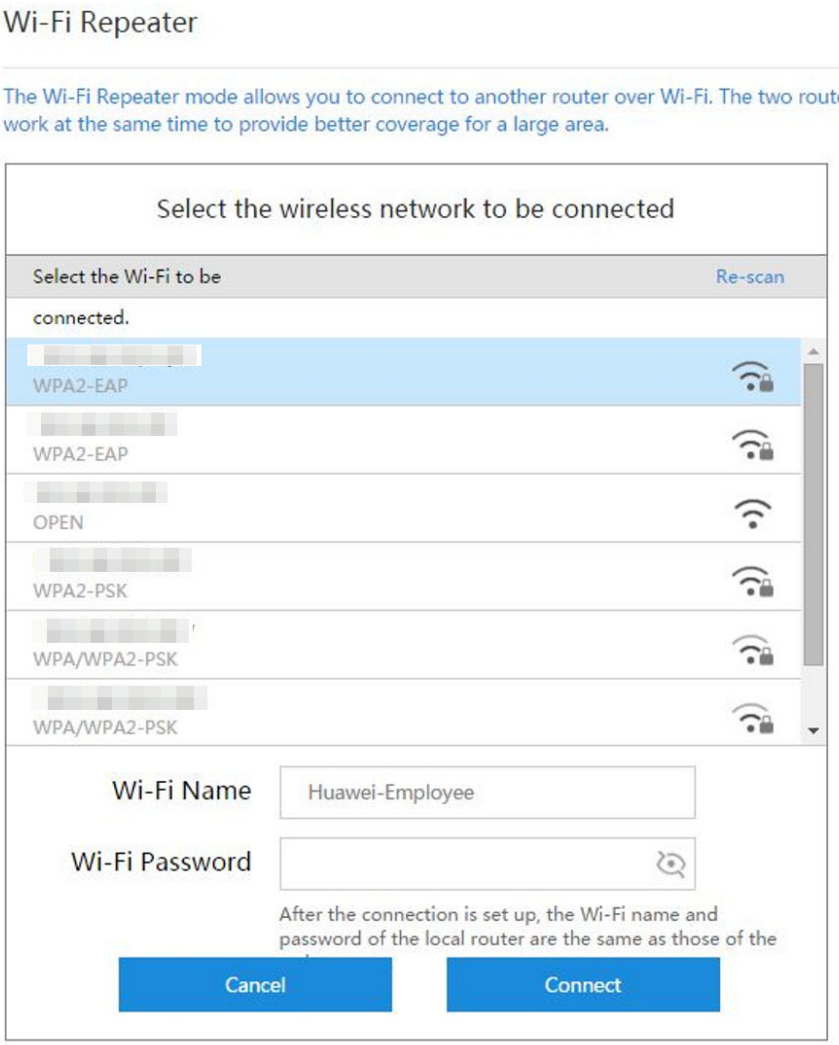
Figure 4-6 Smart Network Connection



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



2. Click **Connect**.

4.3.3 Security Configuration

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

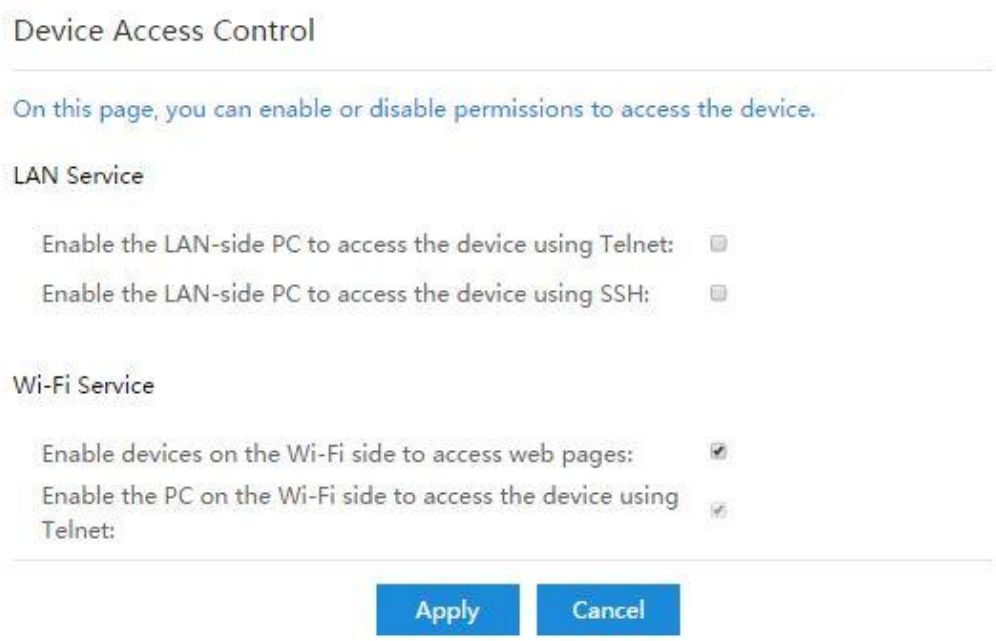
4.3.3.1 Device Access Control

1. In the navigation tree on the left, choose **Security Configutation** > **Device Access Control**. In the pane on the right, configure the rule of edge ONT access control, as shown in **Figure 4-8**.

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 4-8 Device Access Control



2. Click **Apply**.

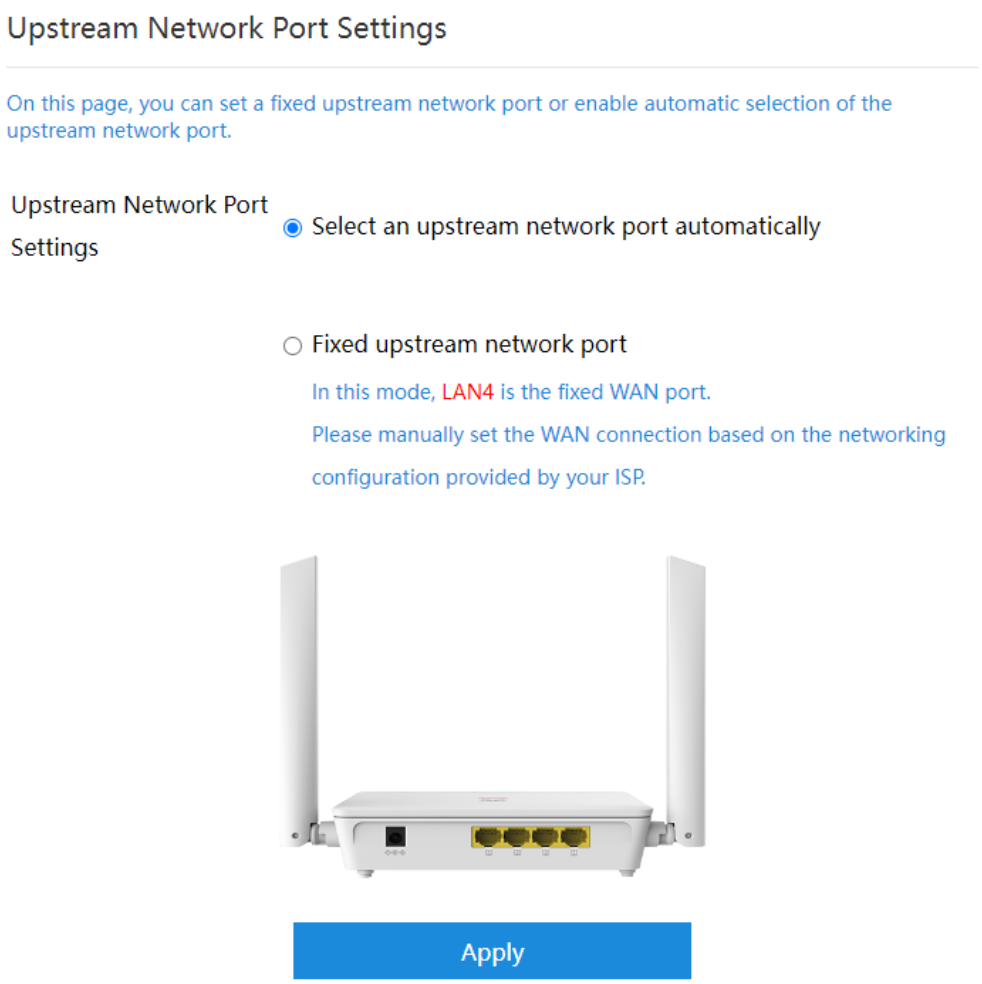
4.3.4 System Management

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 4-9**.

Figure 4-9 Upstream Network Port Settings

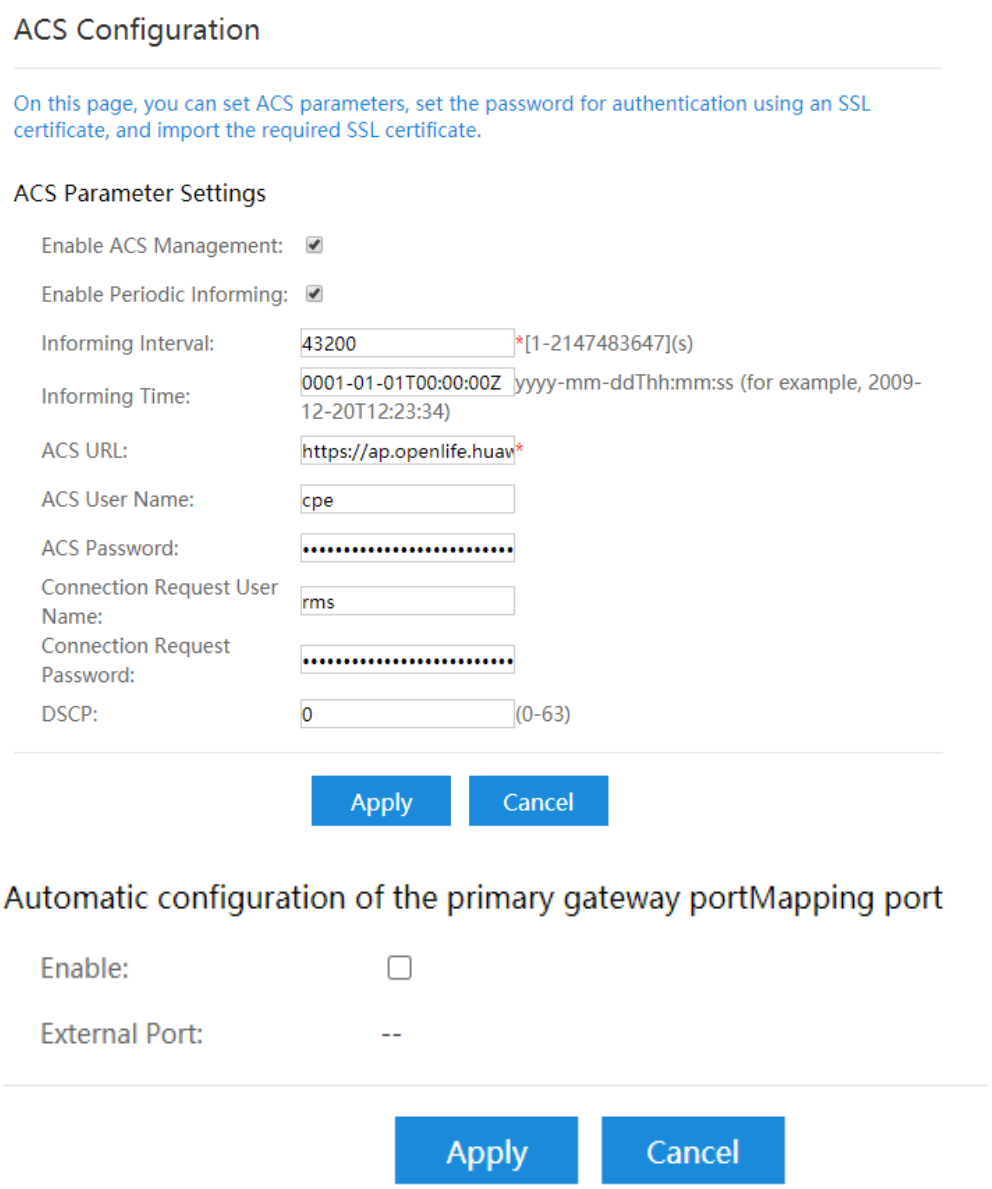


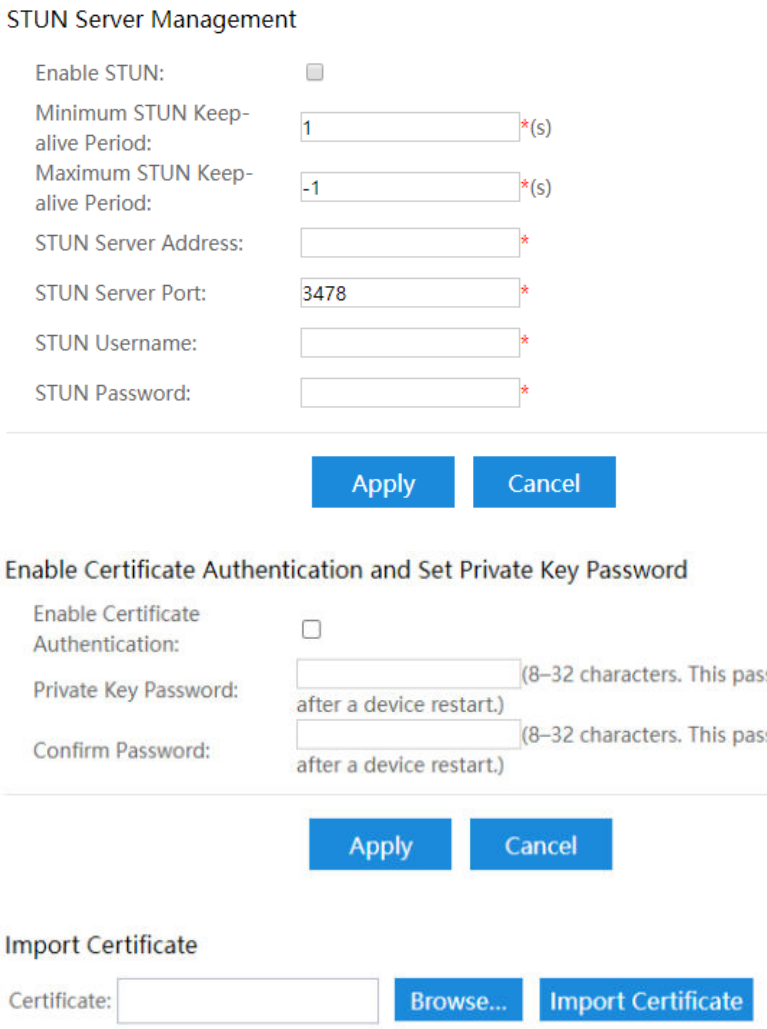
2. Click **Apply**.

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 4-10**.

Figure 4-10 TR-069





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 **ACS Management**.

Parameter	Description
Enable Periodic Informing	Indicates whether to enable the notification function. • If the notification function is enabled, the ONT actively sends a connection request to the TR-069 server. • If the notification function is disabled, the ONT does not actively send a connection request to the TR-069 server. When the notification function is enabled, the **Informing Interval** and **Informing Time** 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.
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.

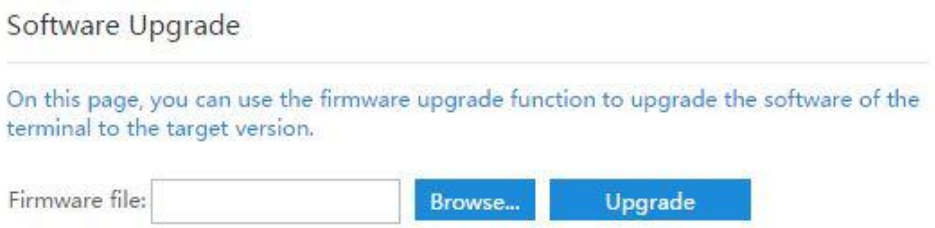
Parameter	Description
Minimum STUN Keep-alive Period	If STUN Is enabled, the minimum period, in seconds, that STUN Binding Requests can be sent by the device for the purpose of maintaining the binding in the Gateway. This limit applies only to Binding Requests sent from the UDP Connection Request address 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 *STUNEnable*. If an empty string and *STUNEnable* is *true*, 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 *STUNEnable*. 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.
Enable Certificate Authentication and Set Private Key Password	
Enable Certificate Authentication	Enable the certificate if the ACS is connected through SSL.

Parameter	Description
Private Key Password	Sets the private key password after the certificate is enabled.
Confirm Password	Confirms the password and ensures that it is the same as **Private Key Password**.
Import Certificate	
Certificate	Indicates the certificate file provided by the carrier.

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 4-11**.

   Figure 4-11 Software Upgrade

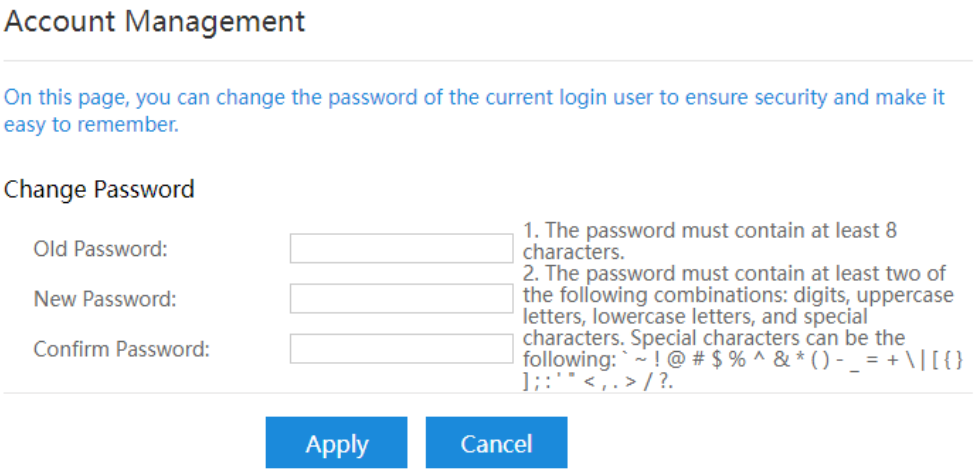
   

2. After the upgrade is successful, a message is displayed indicating that the device needs to be reset. Click **Restart**. The configuration data takes effect after the device is reset.

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 4-12**.

Figure 4-12 Account Management



NOTICE

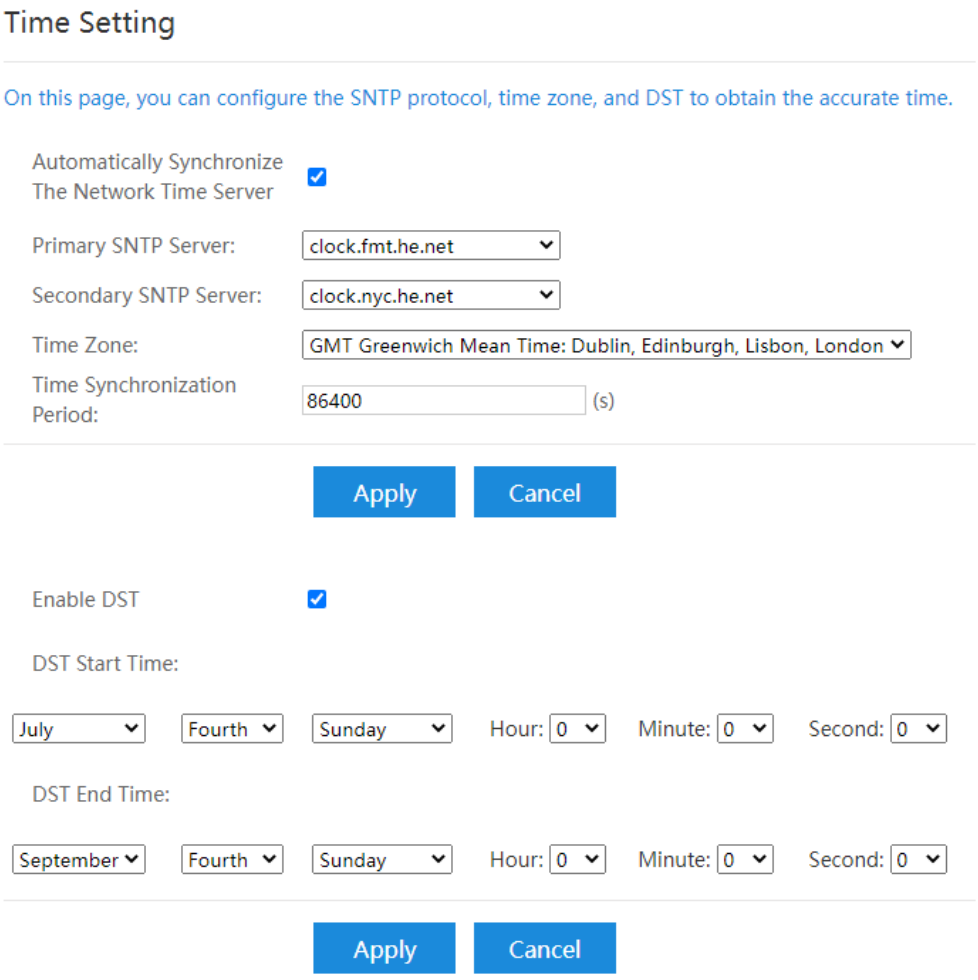
To enhance system security, change the password to a password that meets security requirements after the first successful login. It is recommended that you change the password periodically.

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 4-13**.

Figure 4-13 Time Setting



2. Click **Apply**.

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

Table 4-4 Parameters related to the system time

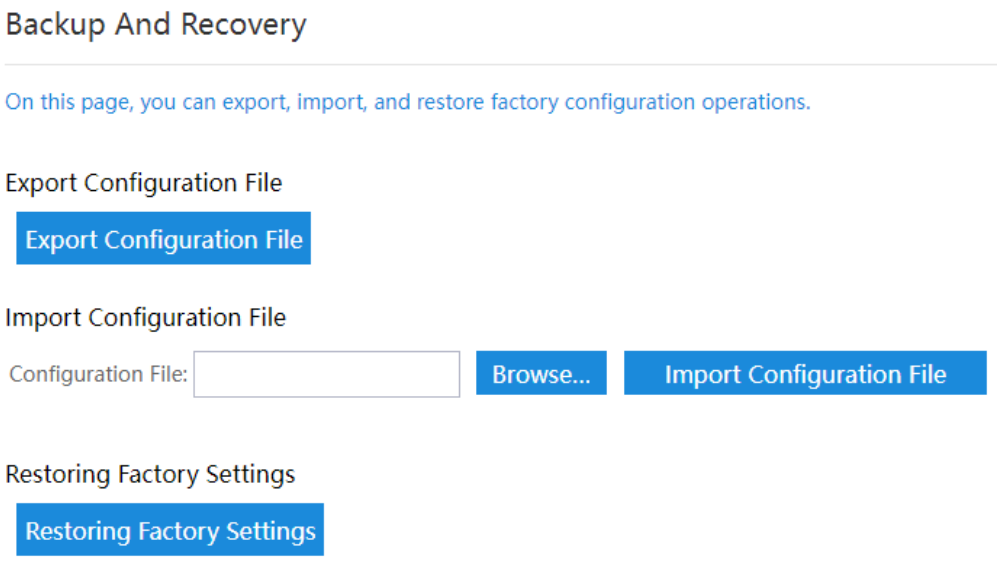
Parameter	Description
Automatically Synchronization The Network Time Server	Indicates whether to enable the auto synchronization network time server, that is, SNTP server.
Primary SNTP Server	Indicates the primary SNTP server.
Secondary SNTP Server	Indicates the secondary SNTP server.
Time Zone	Indicates 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 facory configuration operations.

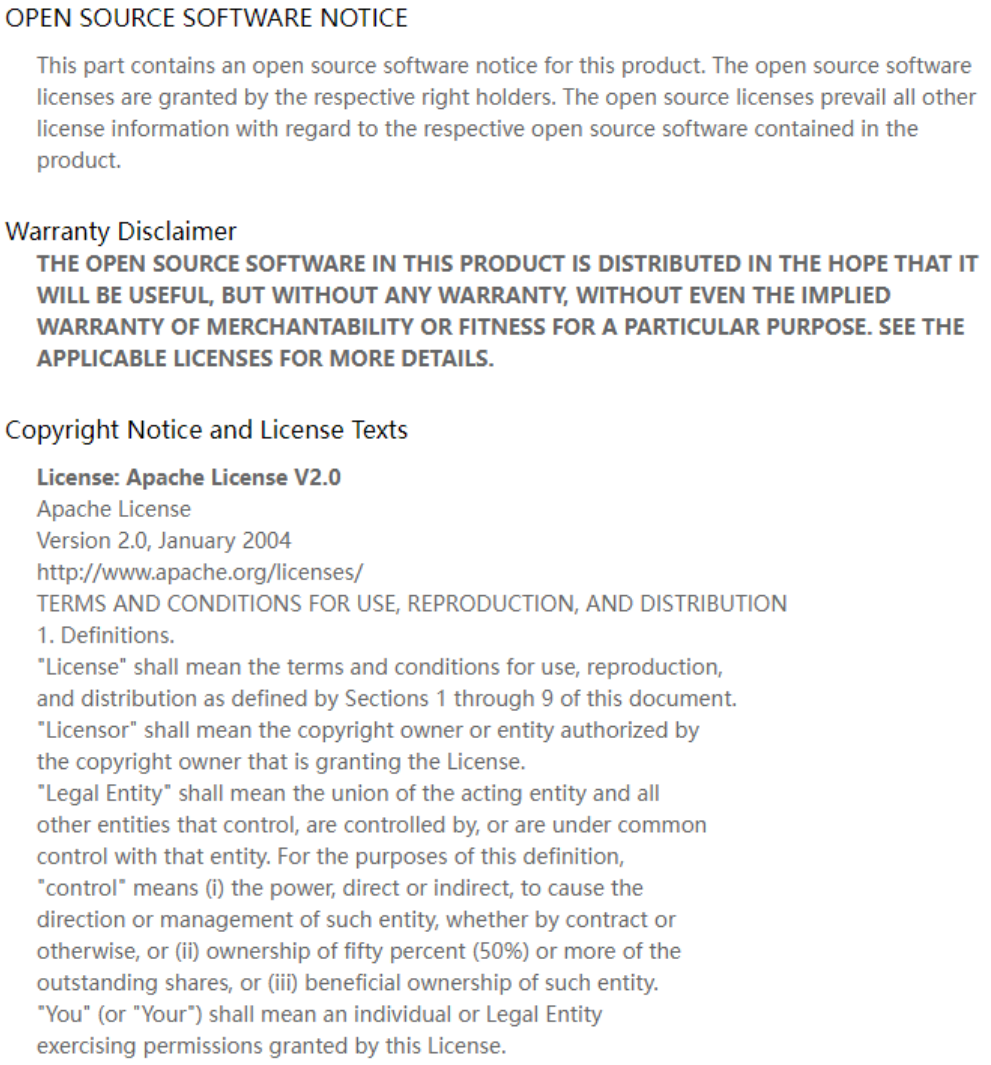
Figure 4-14 Backup and recovery



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 4-15**.

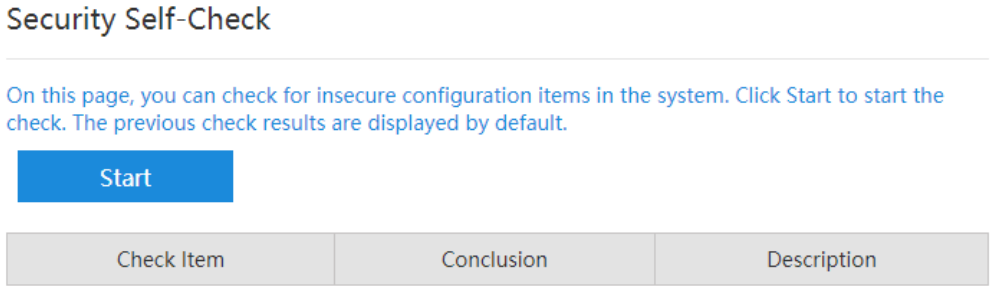
Figure 4-15 Open Source Software Notice



4.3.4.8 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 incecure configuration items in the system. Click **Start** to start the check, as shown in **Figure 4-16**.

Figure 4-16 Security self-check



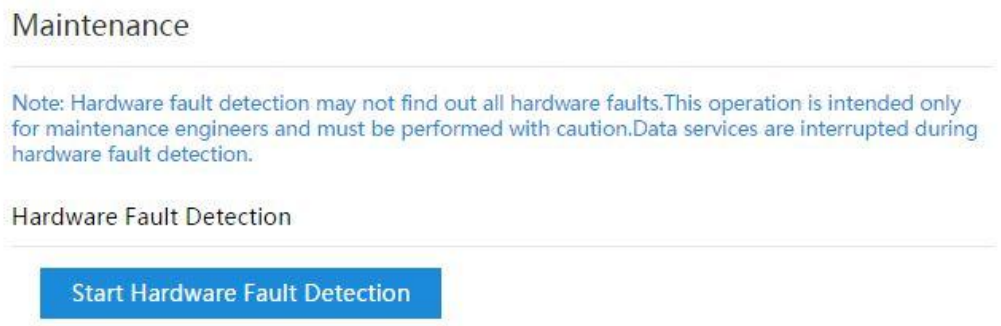
4.3.5 Maintenance Diagnosis

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 4-17**.

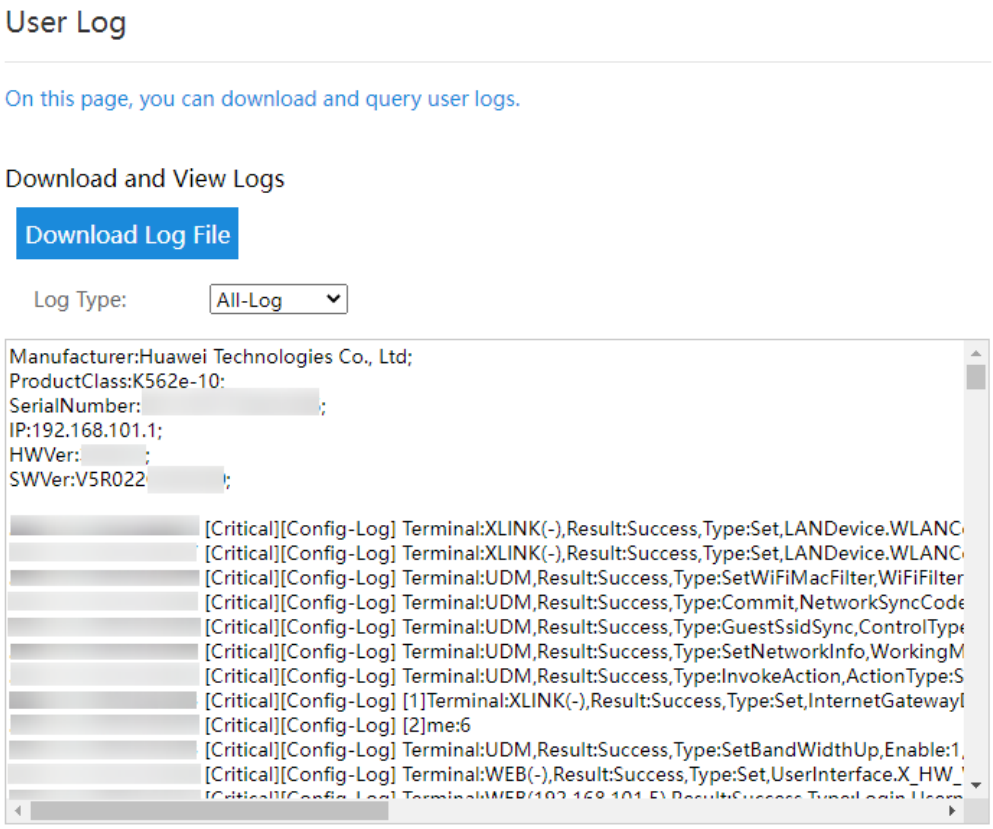
Figure 4-17 Maintenance



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 4-18**.

Figure 4-18 User Log



- 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**.

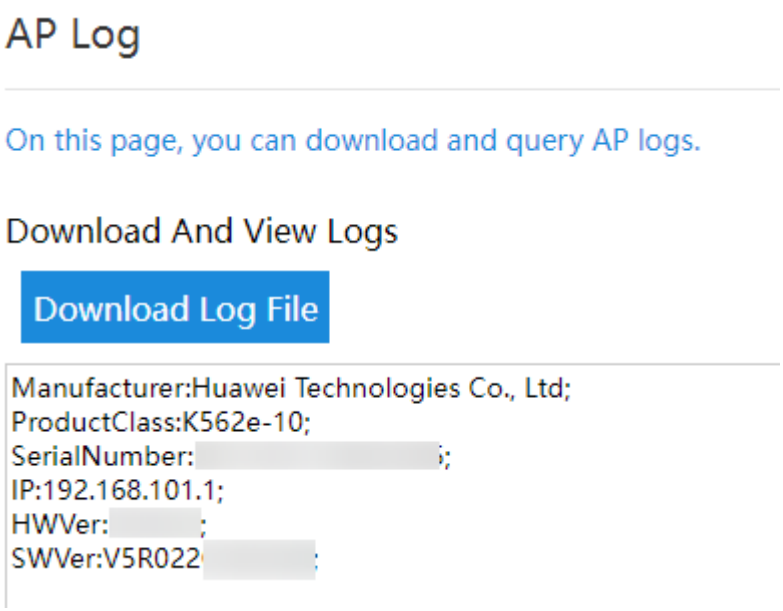
NOTICE

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 4-19**.

Figure 4-19 AP Log



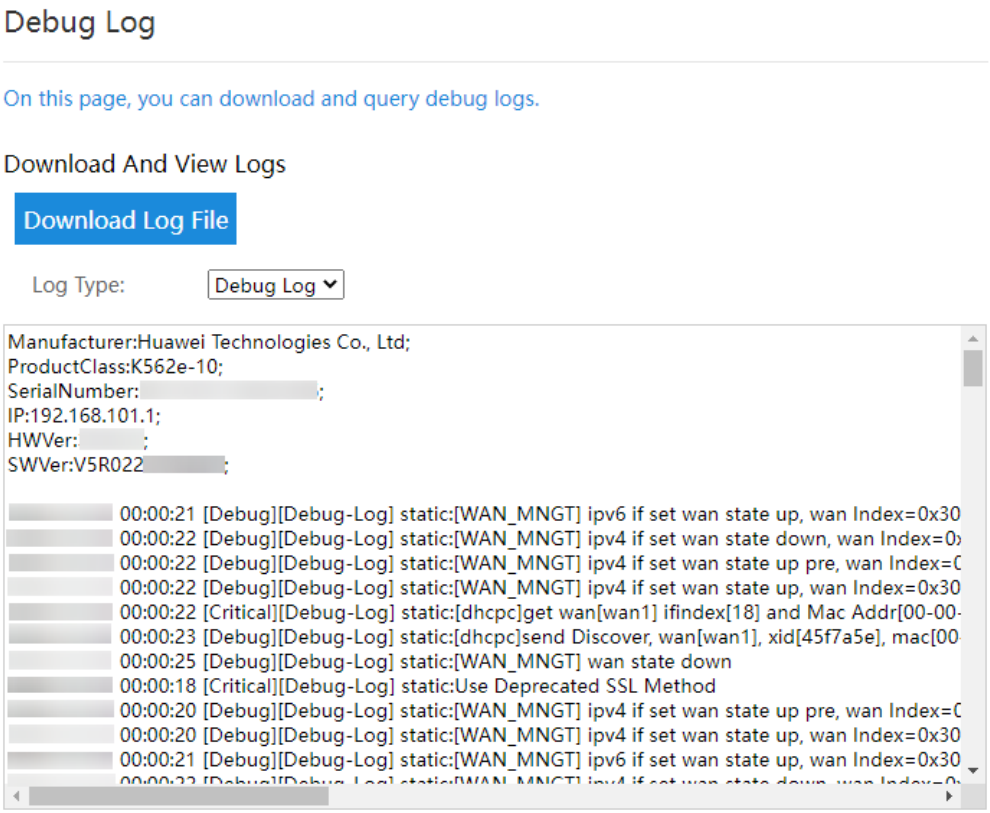
NOTICE

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.

4.3.5.4 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 4-20**.

Figure 4-20 Debug Log



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.

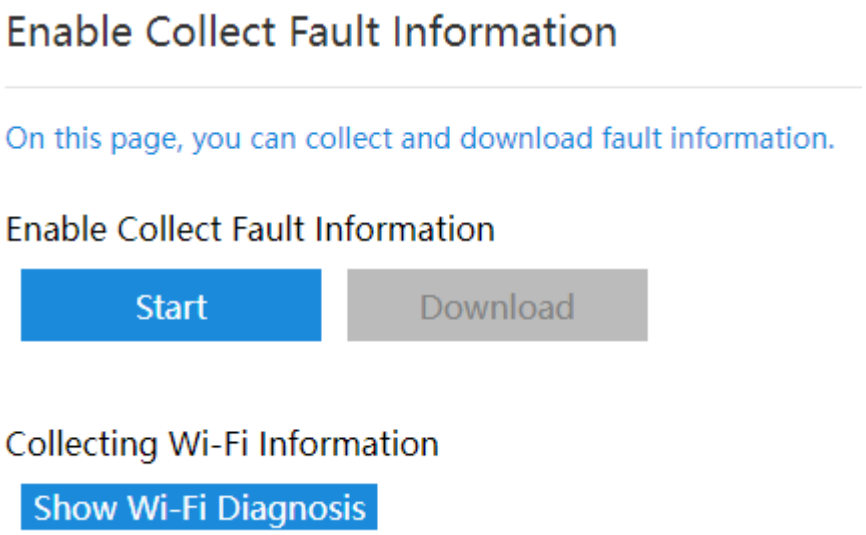
NOTICE

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 4-21**.

Figure 4-21 Fault Info Collect



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.

4.3.5.6 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 4-22**.

Figure 4-22 Indicator status management