DG8245V User Guide

Product Version: V100R019C00

Library Version: 01

Date: 2018-04-27

For any question, please contact us.

Web Page Reference (DG8245V)

Contents

1 Web Page Reference (DG8245V)

This topic describes the usage and meanings of the parameters on the web page.

Before configuring and viewing the parameters on the web page, log in to the web page. For details about how to log in to the web page, see Locally Logging in to the Web Page.

This topic uses figures of the DG8245V accessed by the administrator as examples. Different DSL home gateways may have different screen captures, actual screen captures prevail.

The configuration window for an administrator is different from that for a common user.

- Compared with a common user, an administrator has permissions to view and configure all parameters on the web page. A common user can configure and query some nodes and parameters and the queried information is less than that queried by an administrator. This topic lists different nodes queried by a common user. For details, see the web page for a common user.
- A common user does not have permissions to view the following parameters:
  - **DHCPv6 Information** under the **LAN Configuration** node
  - **Firewall Level Configuration**, **DoS Configuration** and **Precise Device Access Control** under the **Security Configuration** node
  - **Route** node
  - **Time Setting**, **ALG Configuration**, **IGMP Configuration**, **QoS Configuration** and **ARP Ping** under the **Application** node
  - **Voice** node
  - **TR-069** under the **System Management** node
  - **Software Upgrade**, **Debug Log**, **Fault Info Collect**, **Remote Mirror** and **Indicator Status Management** under the **Maintenance Diagnosis** node

Update History

Issue 01 (2018-04–23)

This is the first official release for the V100R019C00 version.

Locally Logging in to the Web Page

This topic describes the data plan and procedure for logging in to the web page.

Fast Setting

This topic describes how to quickly set a DSL home gateway.

Home Page

This topic describes the DSL home gateway common configurations, such as Wi-Fi configuration, home sharing, and network status query.

One-click Diagnosis

This topic describes how to quickly diagnose DSL home gateway network status.

System Info

This topic describes how to query the system information about the DSL home gateway such as the user device information through the web page.

Advanced Configuration

This topic describes how to configure functions through the web page, including LAN or WAN configuration, security configuration, and so on.

1.1 Locally Logging in to the Web Page

This topic describes the data plan and procedure for logging in to the web page.

Context

Before setting up the configuration environment, ensure that data information listed in Table 1 is available.

Table 1 Data plan

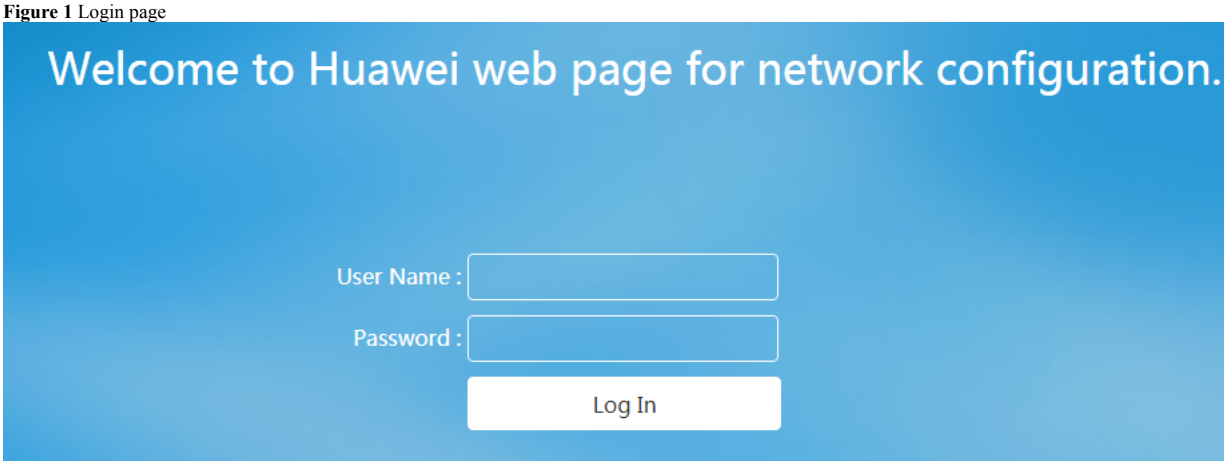
Item	Description
User name and password	Default settings: • **Administrator (installation and maintenance personnel):** ▪ User name: admin ▪ Password: @HuaweiHgw **NOTE:** ▪ If you do not perform any operations after logging in to the system for five minutes you will exit the system and the system automatically returns to the login interface. ▪ The system will be locked if you input incorrect user name or password three consecutive times. After one minute, it will be unlocked. ▪ Modify the password through the ACS or web page. **CAUTION:** ▪ Please change the initial password to ensure administrator account security. ▪ Do not provide terminal users with the password of the administrator account. The administrator account is used by the carrier for O&M. If a terminal user uses the administrator account, service parameters may be incorrectly modified and services may be affected. • **Common user (terminal user):** ▪ User name: user ▪ Password: HuaweiUser **NOTE:** ▪ The common user account can be used to query the service status. For DSL home gateways that support Wi-Fi and the USB storage function, the common user account can be used to configure services such as Wi-Fi and home sharing. ▪ If you do not perform any operations after logging in to the system for five minutes you will exit the system and the system automatically returns to the login interface. ▪ The system will be locked if you input incorrect user name or password three consecutive times. After one minute, it will be unlocked. ▪ Modify the password through the ACS or web page. **CAUTION:** Please change the initial password to ensure common user account security.
LAN IP address and subnet mask	Default settings: • IP address: 192.168.1.1 • 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 DSL home gateway. For example: • IP address: 192.168.1.100 • Subnet mask: 255.255.255.0

Procedure

1. Use a network cable to connect the LAN port of the DSL home gateway to a PC.
2. Ensure that the Internet Explorer (IE) of the PC does not use the proxy server. The following section considers IE8 as an example to describe how to check whether the IE uses the proxy server.
    a. Start the IE, and choose **Tools Internet Options** from the main menu of the IE window. Then, the **Internet Options** page is displayed.
    b. In the **Internet Options** page, 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.
4. Log in to the web page.

a. Enter **http://192.168.1.1** in the address bar of IE (**192.168.1.1** is the default IP address of the DSL home gateway), and then press **Enter** to display the login page, as shown in Figure 1.

Figure 1 Login page



NOTE:

The web page login supports TLS1.1 and TLS1.2. The TCP port 443 is used for listening for HTTPS packets. You need to type **https://192.168.1.1:443** in the address bar of IE and press **Enter** to log in to the DSL home gateway.

b. In the login page, enter the use name and password. For details about default settings of the user name and password, see Table 1. After the password authentication is passed, the web page is displayed.

Parent Topic: Web Page Reference (DG8245V)

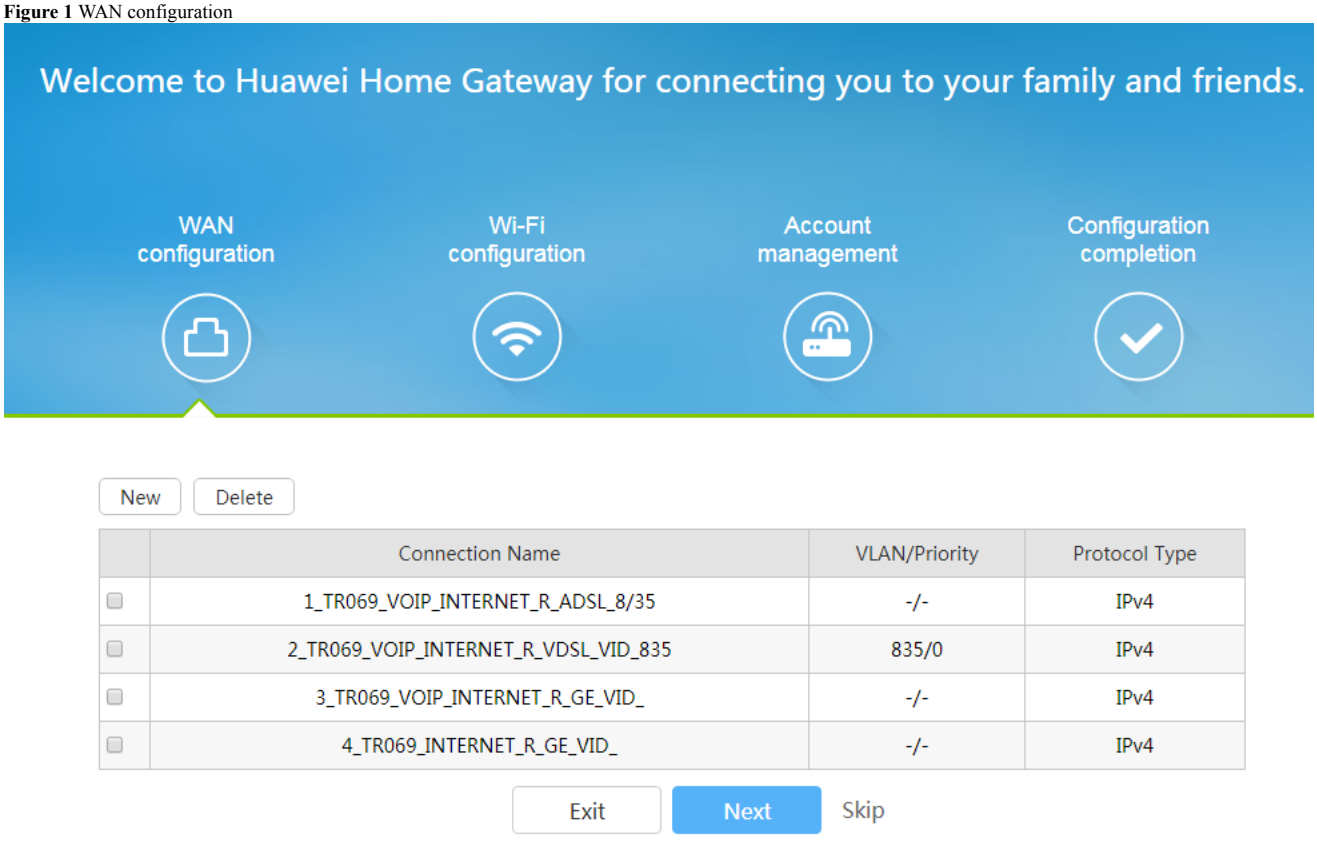
Next topic >

1.2 Fast Setting

This topic describes how to quickly set a DSL home gateway.

1. Log in to the web page. For details, see Locally Logging in to the Web Page.
2. In the displayed page, configure the WAN port parameters, as shown in Figure 1.

Figure 1 WAN configuration



NOTE:

- When the user logs in to the DSL home gateway web page for the first time, this page is displayed. In other cases, you need to click **Fast Setting** on the upper right corner of the page to go to this page.
- You can click **New** to new the WAN connection.
- You can click **Delete** to delete the related WAN connection.
- Only the DSL home gateway web page supports DSL home gateway WAN configurations. For methods of setting WAN configurations, see WAN Configuration.

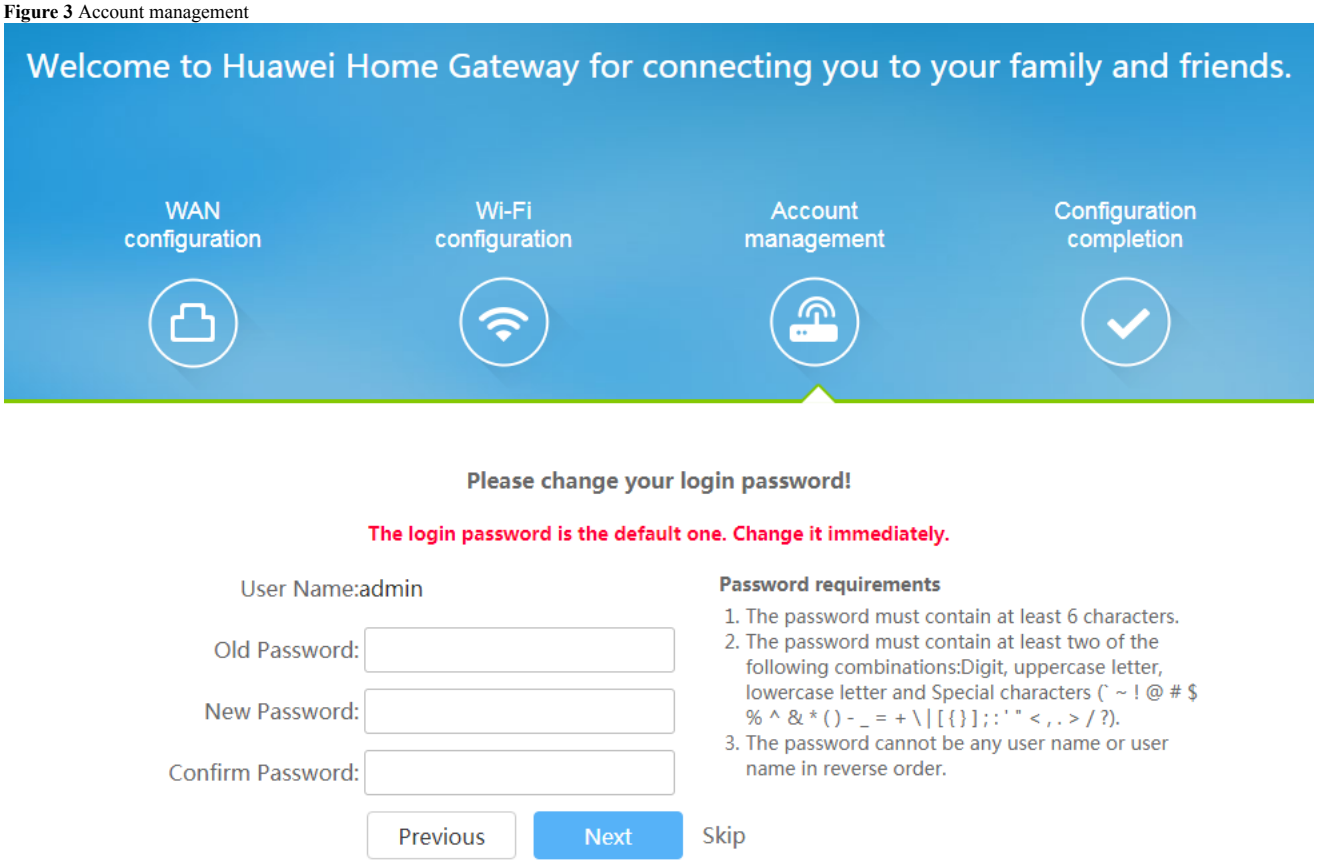
---

3. Click **Next**.
4. In the displayed page, change the Wi-Fi name and password, as shown in Figure 2.

Figure 2 Wi-Fi configuration

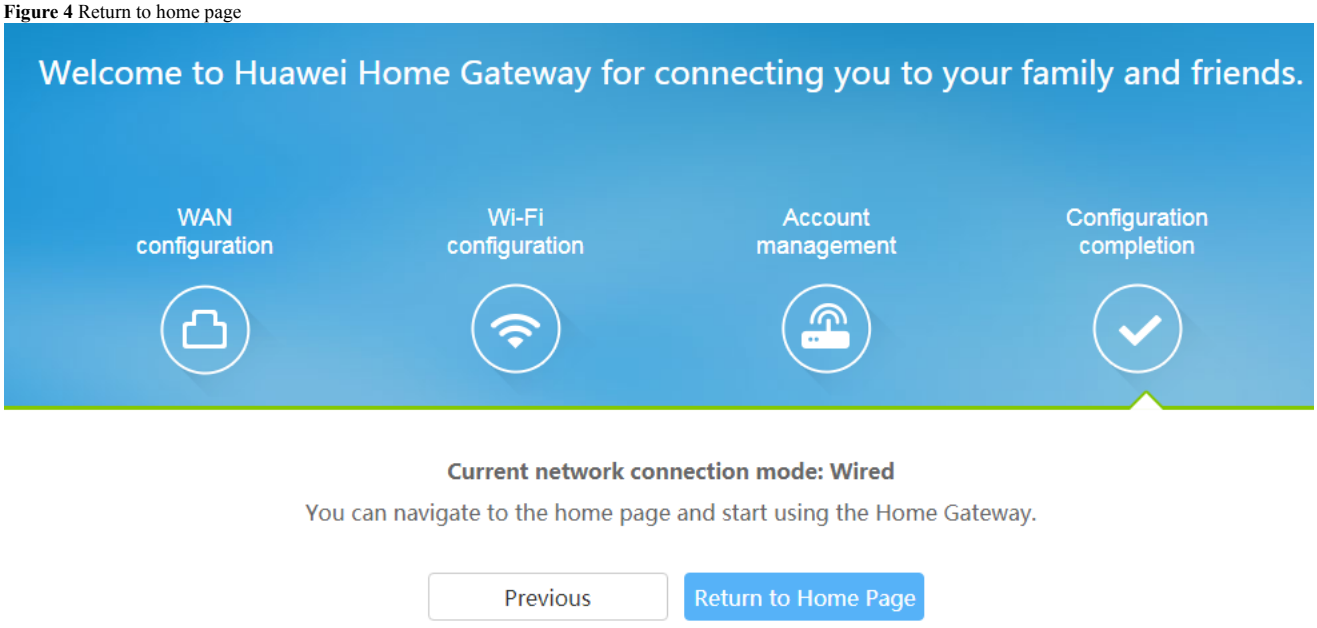
5. Click **Next**.
6. In the displayed page, change the login password, as shown in Figure 3.

Figure 3 Account management



7. Click **Next**.
8. In the displayed page, click **Return to Home page** to navigate to the home page, as shown in Figure 4.

Figure 4 Return to home page



Parent Topic: Web Page Reference (DG8245V)

< Previous topic Next topic >

1.3 Home Page

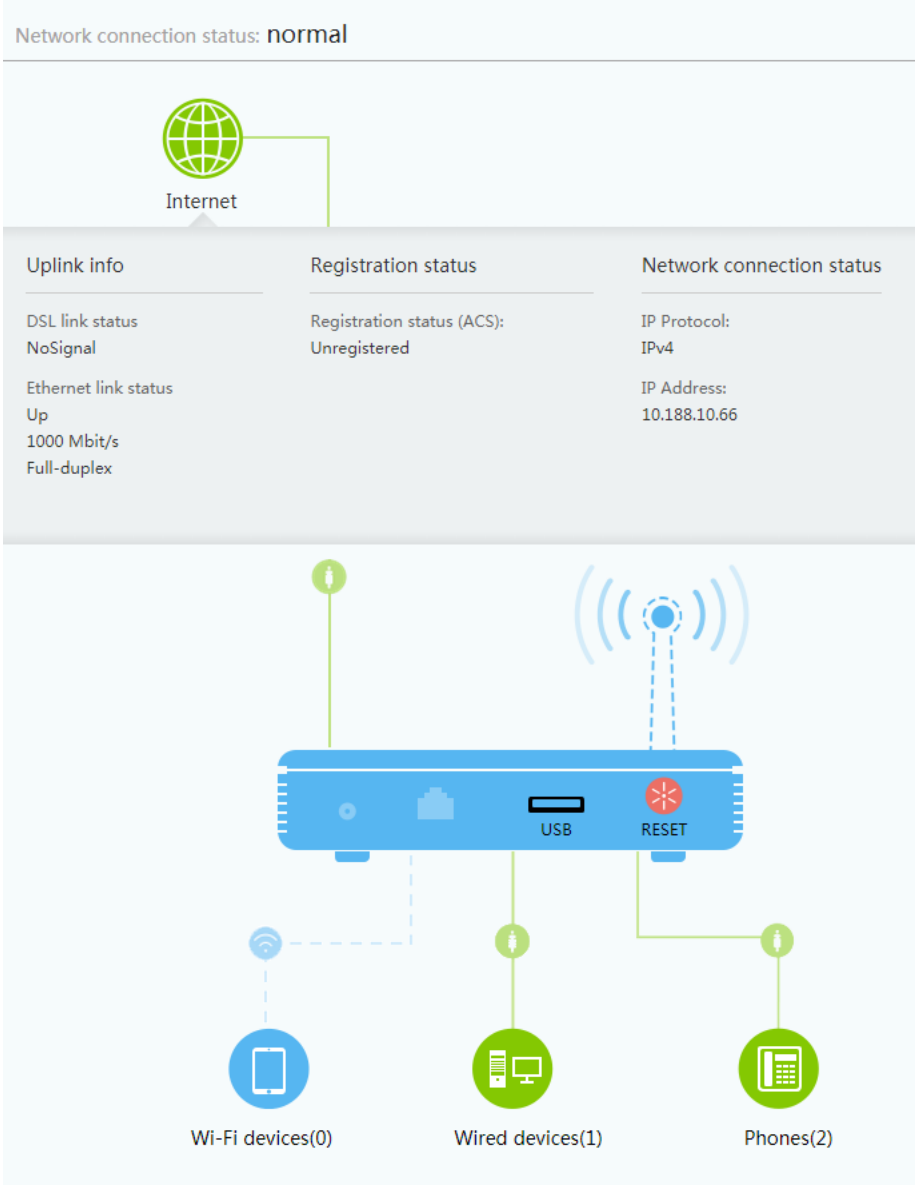
This topic describes the DSL home gateway common configurations, such as Wi-Fi configuration, home sharing, and network status query.

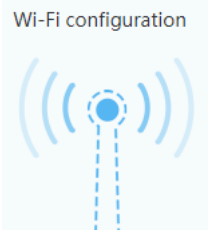
1. In the navigation tree on the left, choose **Home Page**.

2. In the pane on the right, you can click 

to query the network status, as shown in Figure 1.

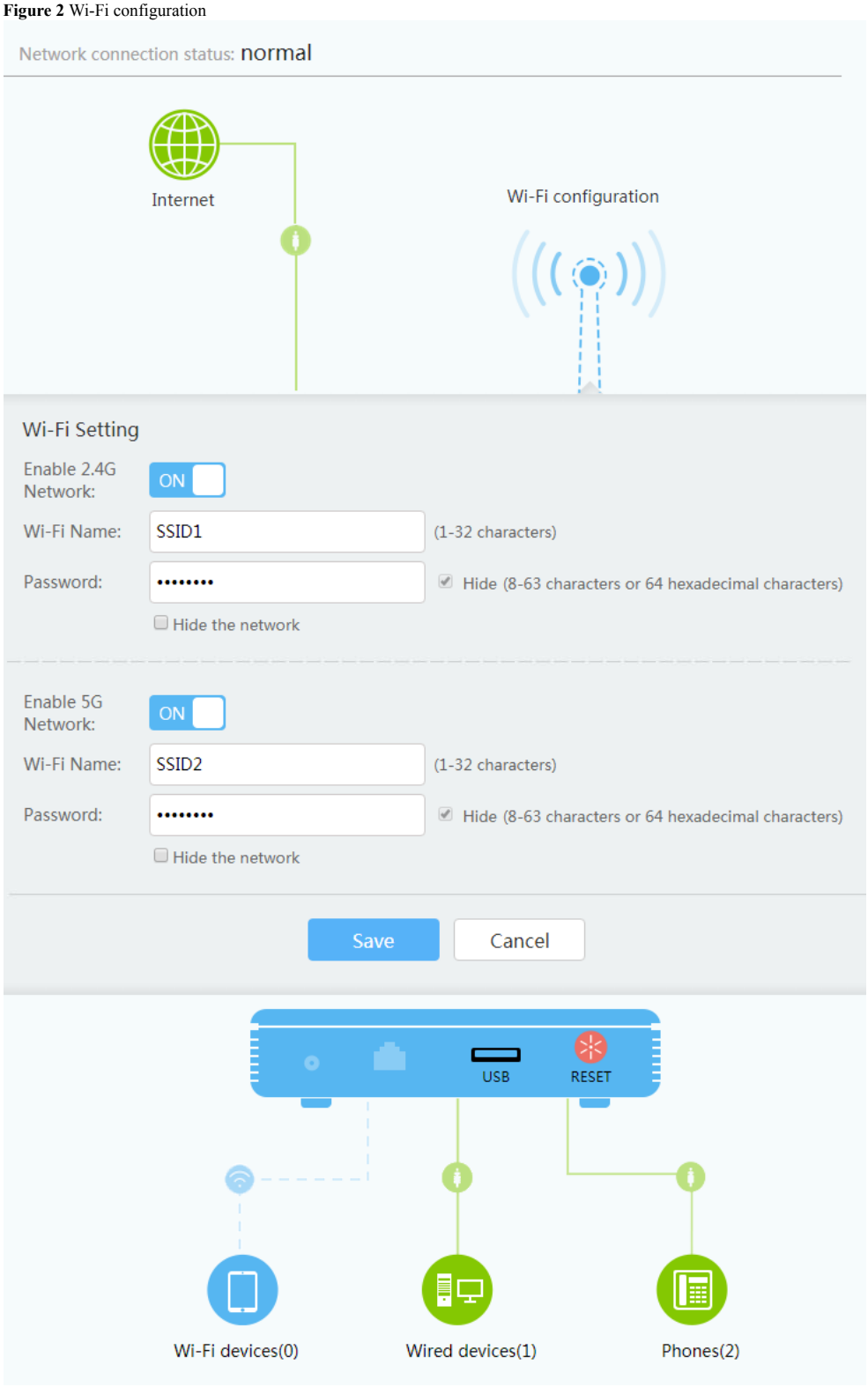
Figure 1 Internet



3. In the pane on the right, you can click 

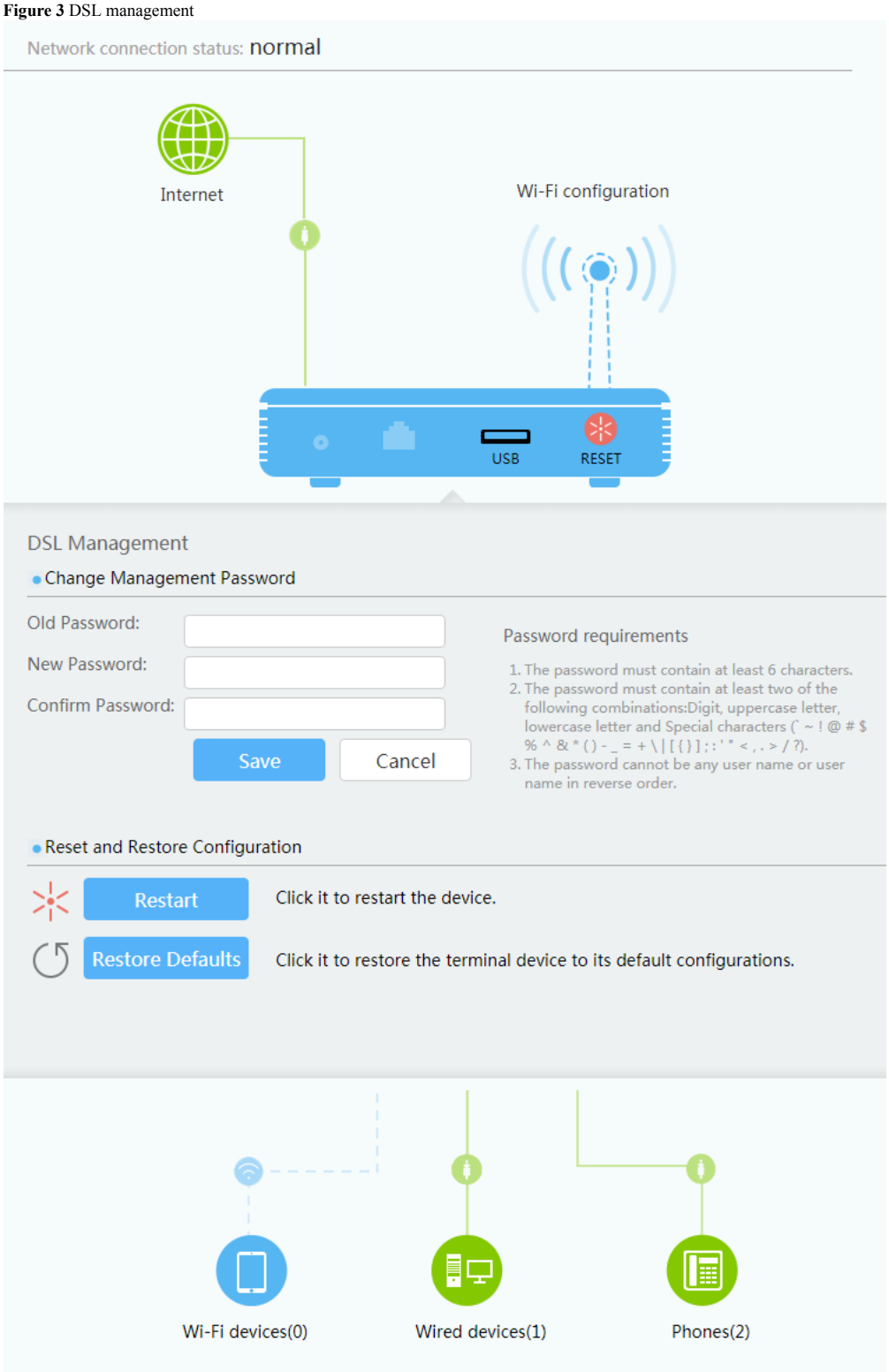
to configure the Wi-Fi parameters, as shown in Figure 2.

Figure 2 Wi-Fi configuration



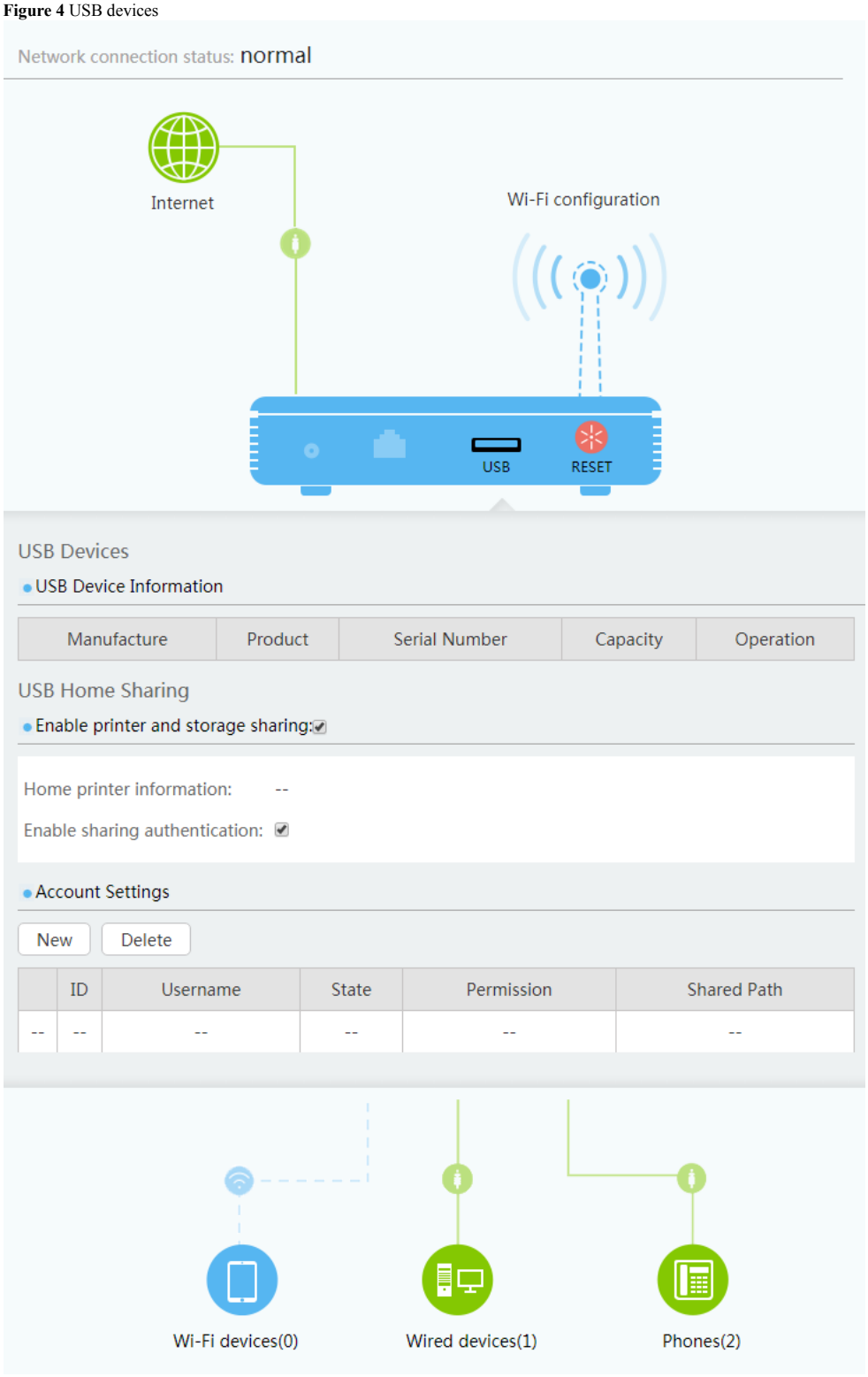
4. In the pane on the right, you can click the DSL home gateway device to manage accounts and passwords or reset the DSL home gateway, as shown in Figure 3.

Figure 3 DSL management

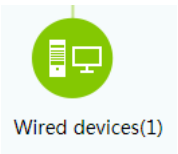


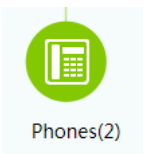
5. In the pane on the right, you can click  to start home sharing and set the sharing permission, as shown in Figure 4.

Figure 4 USB devices



6. In the pane on the right, you can click 

, 

and 

to manage devices connected to the DSL home gateway and query the connection status of these devices, as shown in Figure 5, Figure 6 and Figure 7.

Figure 5 Wi-Fi devices

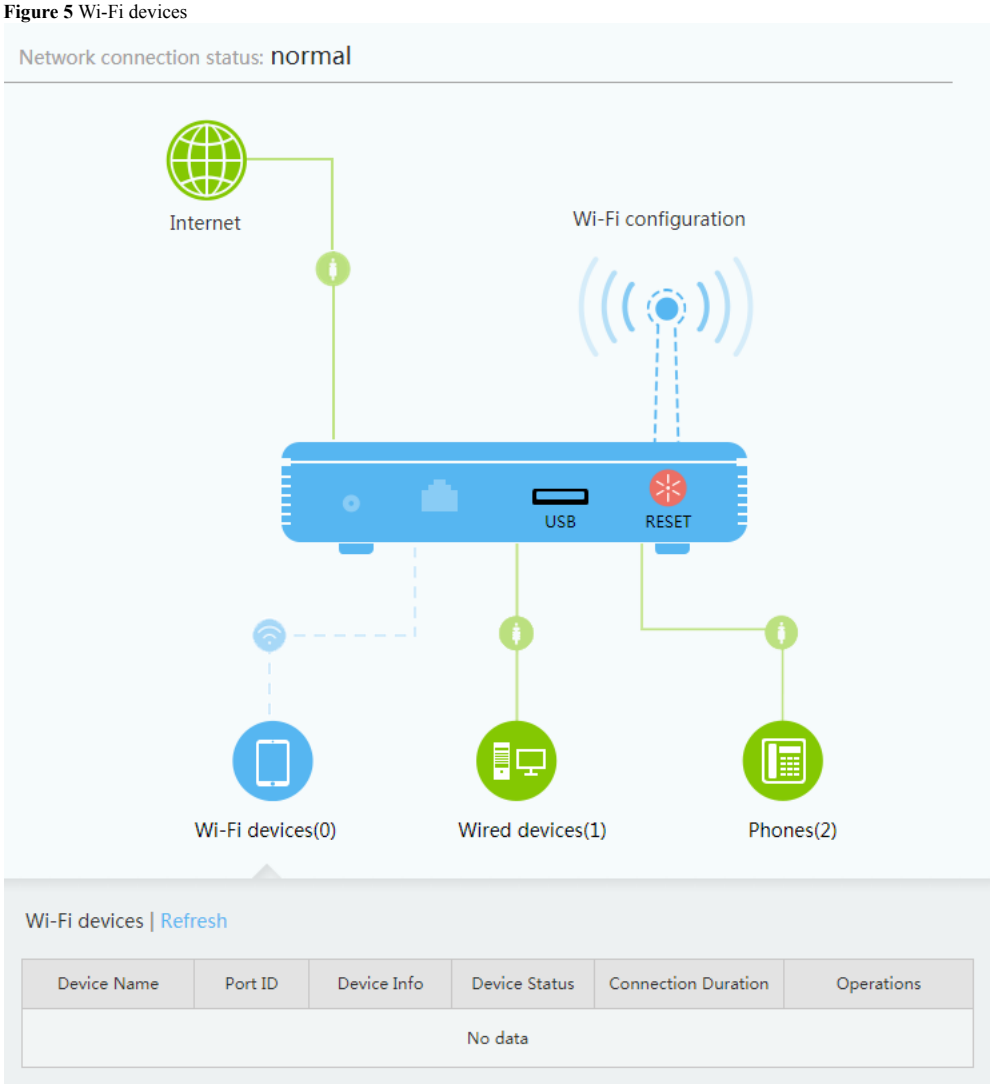


Figure 6 Wired devices

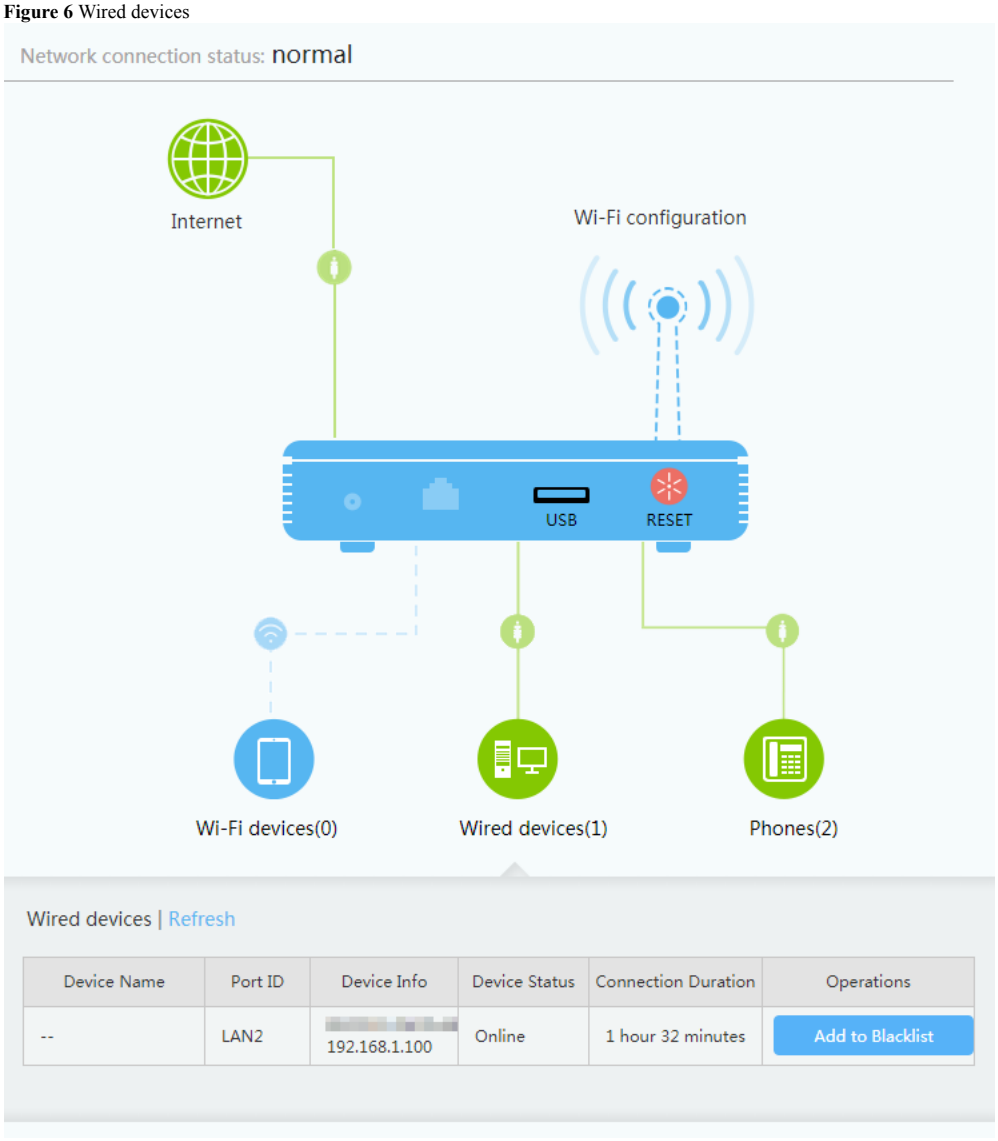
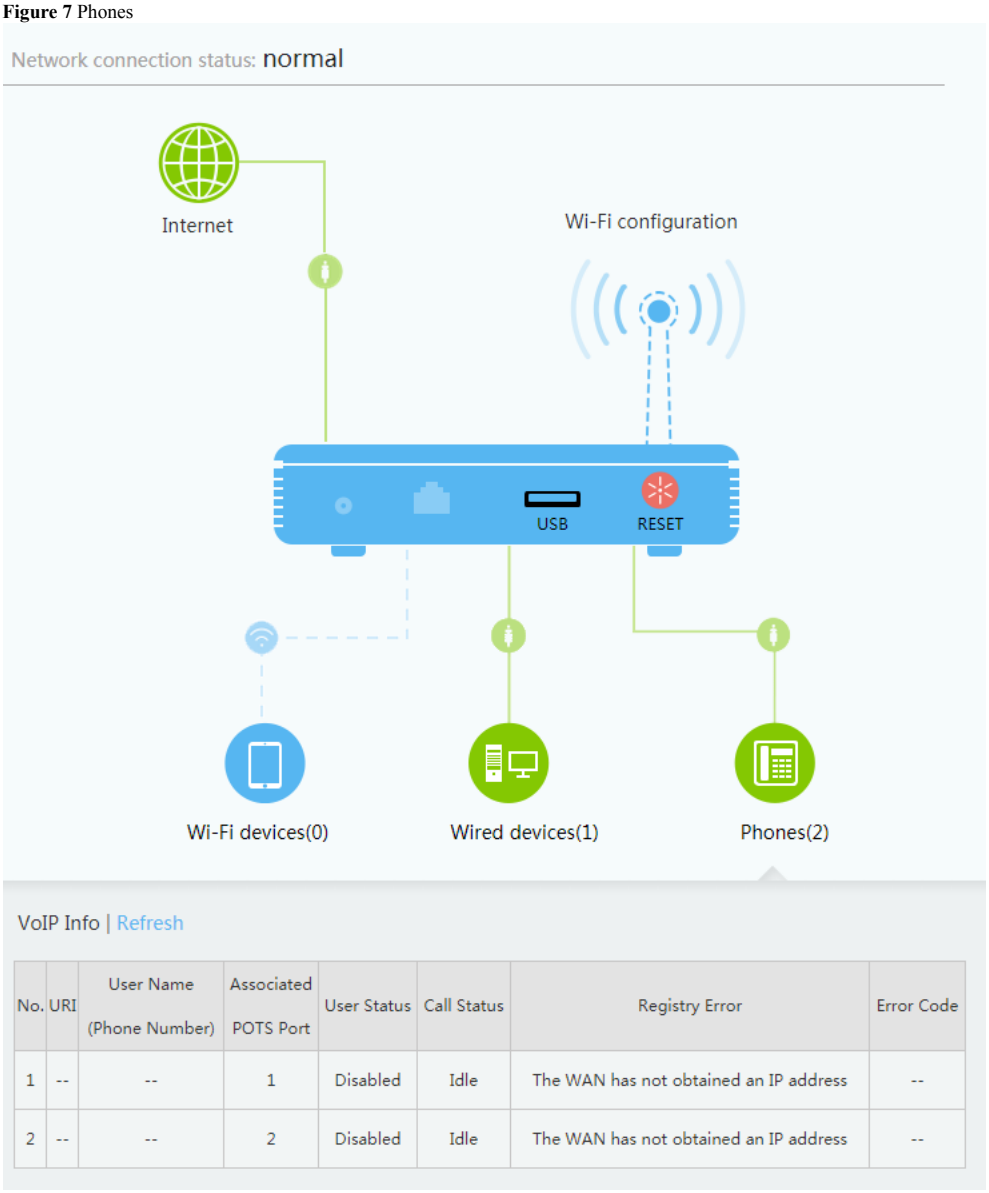


Figure 7 Phones



No.	URI	User Name (Phone Number)	Associated POTS Port	User Status	Call Status	Registry Error	Error Code
1	--	--	1	Disabled	Idle	The WAN has not obtained an IP address	--
2	--	--	2	Disabled	Idle	The WAN has not obtained an IP address	--

Parent Topic: Web Page Reference (DG8245V)

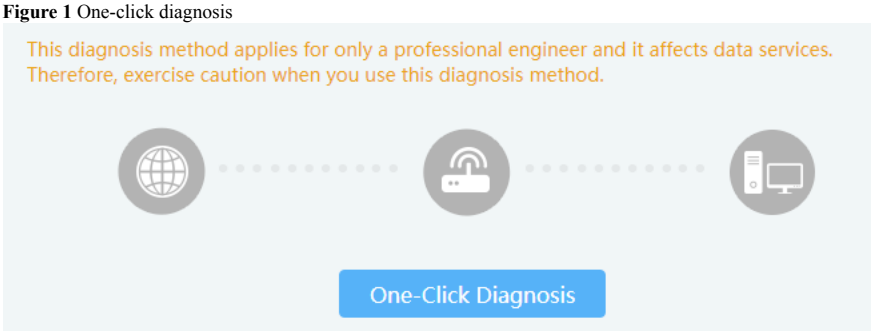
< Previous topic Next topic >

1.4 One-click Diagnosis

This topic describes how to quickly diagnose DSL home gateway network status.

1. In the navigation tree on the left, choose **One-Click Diagnosis**. In the pane on the right, you can click **One-Click Diagnosis** to diagnose the network status, as shown in Figure 1.

Figure 1 One-click diagnosis



2. Figure 2 shows the diagnosis results.

Figure 2 Diagnosis results

NOTE:

- This diagnosis method applies for only a professional engineer and it affects data services. Therefore, exercise caution when you use this diagnosis method.
- If you need to re-diagnose the faults, click **Diagnose again**.

Parent Topic: Web Page Reference (DG8245V)

< Previous topic Next topic >

1.5 System Info

This topic describes how to query the system information about the DSL home gateway such as the user device information through the web page.

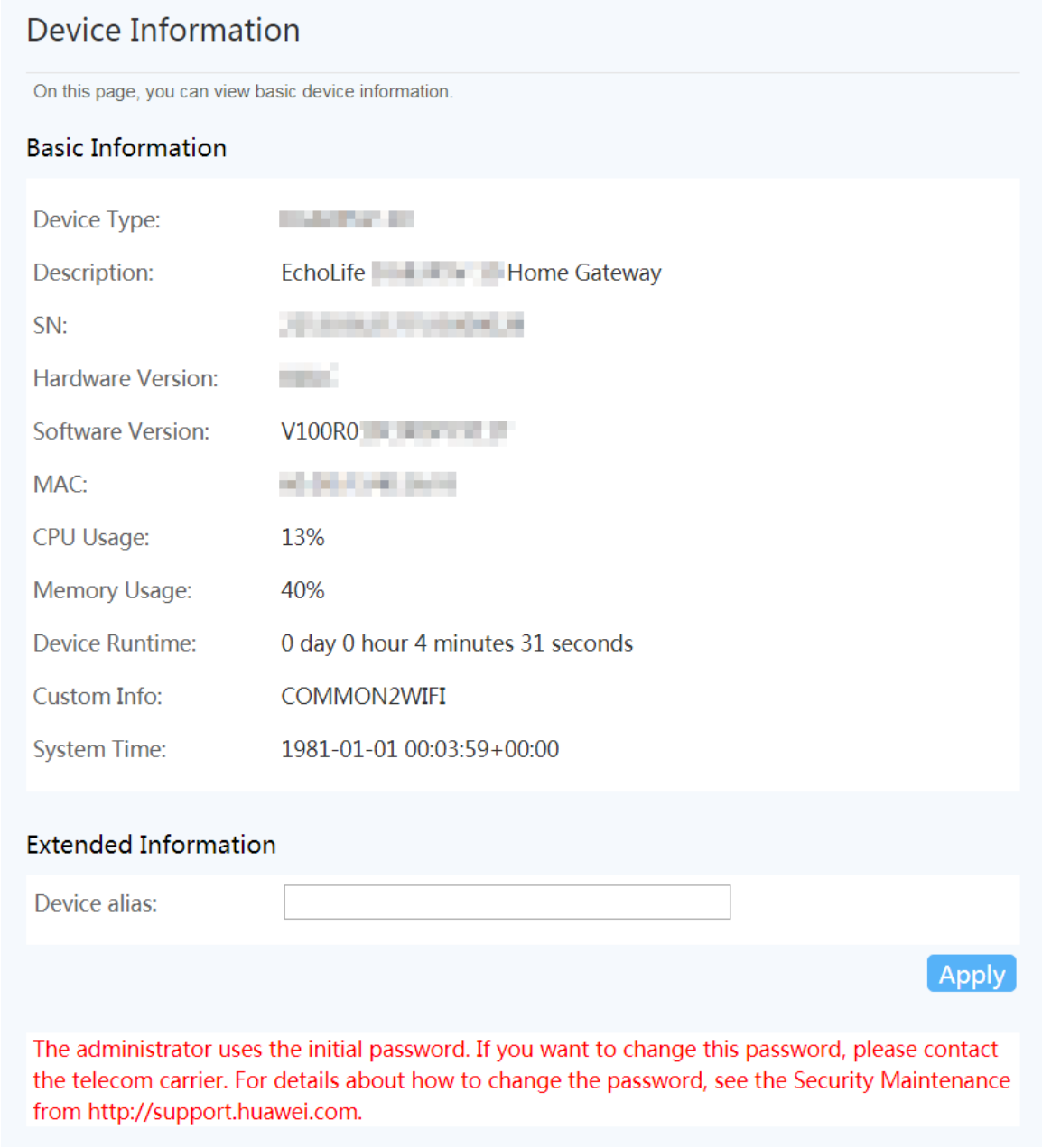
Parent Topic: Web Page Reference (DG8245V)

< Previous topic Next topic >

1.5.1 Device Information

In the navigation tree on the left, choose **System Info** > **Device Information**. In the pane on the right, you can view the device information such as the software version, as shown in Figure 1.

Figure 1 Device information



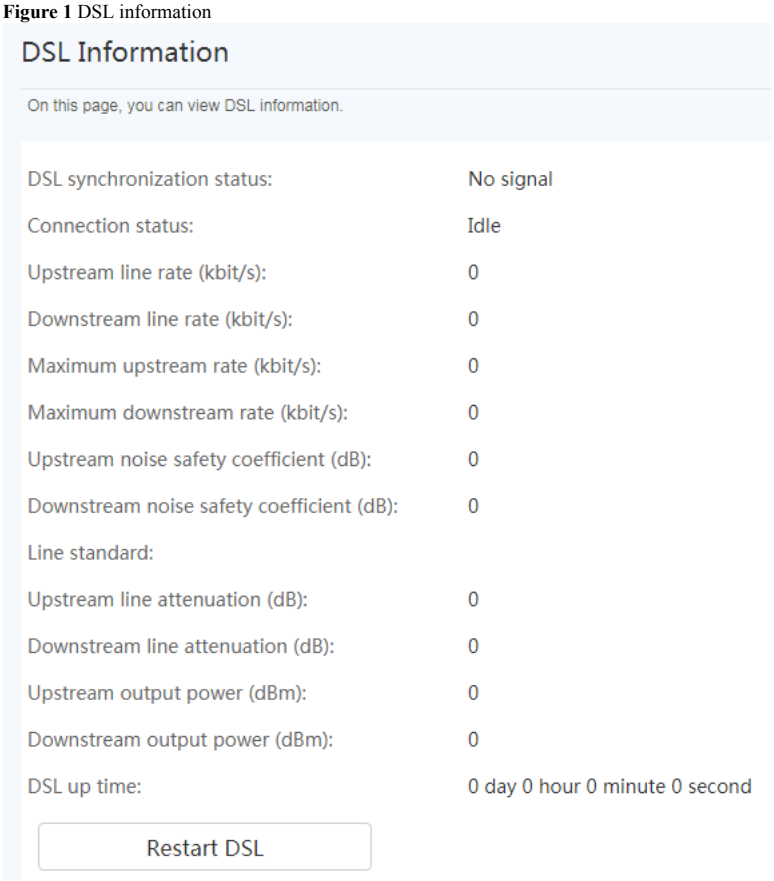
Parent Topic: System Info

Next topic >

1.5.2 DSL Information

In the navigation tree on the left, choose **System Info** > **DSL Information**. In the pane on the right, you can view the DSL information such as the connection status, as shown in Figure 1.

Figure 1 DSL information



NOTE:

If you need to renegotiate the DSL line paramters, click **Restart DSL**.

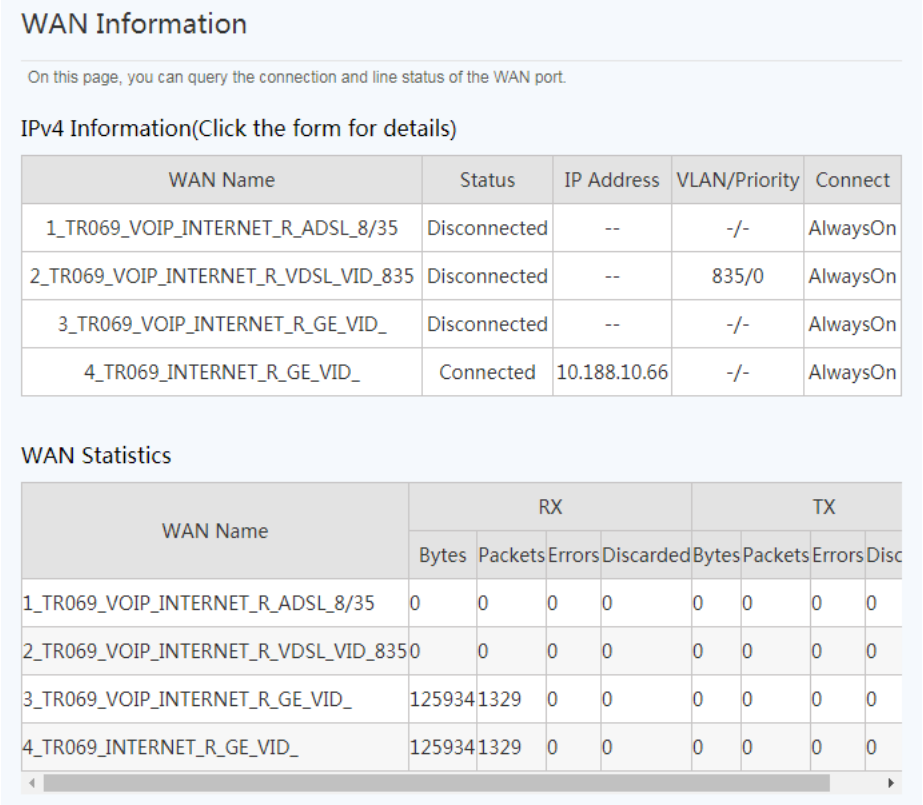
Parent Topic: System Info

< Previous topic Next topic >

1.5.3 WAN Information

In the navigation tree on the left, choose **System Info** > **WAN Information**. In the pane on the right, you can view the WAN information such as the status of the WAN interface, as shown in Figure 1

Figure 1 WAN information



NOTE:

- You can view more detailed information by clicking a record in the WAN list.
- If **Encapsulation Mode** is set to **PPPoE** and **Dialing Method** is selected as **Manual** on the **WAN Configuration** page, you can click **Connected** link to connect the current WAN port, click **disconnected** link to disconnect the current WAN port.

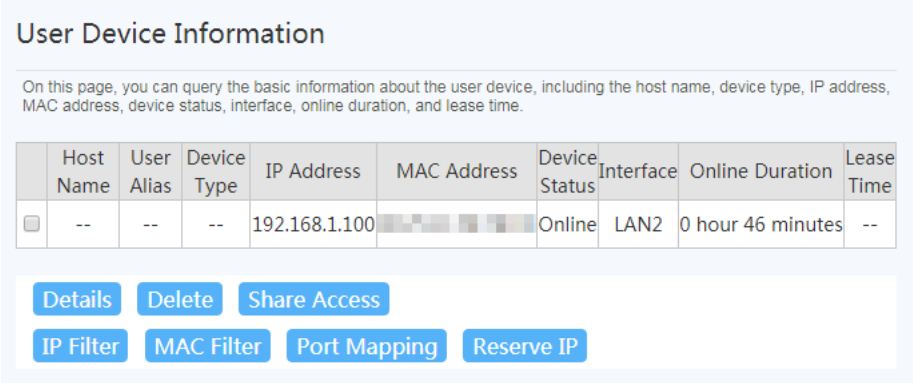
Parent Topic: System Info

< Previous topic Next topic >

1.5.4 User Device Information

In the navigation tree on the left, choose **System Info** > **User Device Information**. In the pane on the right, you can view the user device information such as the IP address, as shown in Figure 1.

Figure 1 User device information



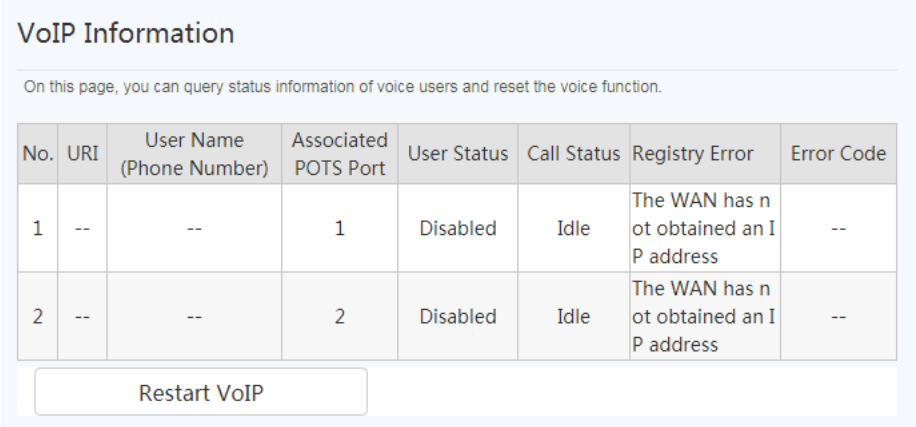
Parent Topic: System Info

< Previous topic Next topic >

1.5.5 VoIP Information

In the navigation tree on the left, choose **System Info** > **VoIP Information**. In the pane on the right, you can view the VoIP information such as the user status, as shown in Figure 1.

Figure 1 VoIP information



NOTE:
If you need to restart the VoIP service, click **Restart VoIP**.

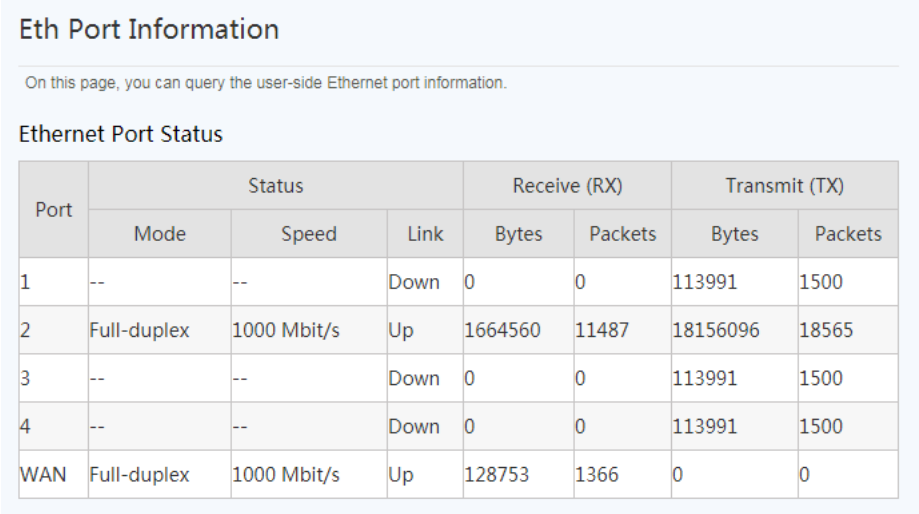
Parent Topic: System Info

< Previous topic Next topic >

1.5.6 Eth Port Information

In the navigation tree on the left, choose **System Info** > **Eth Port Information**. In the pane on the right, you can view the Ethernet port information such as the speed, as shown in Figure 1.

Figure 1 Eth port information



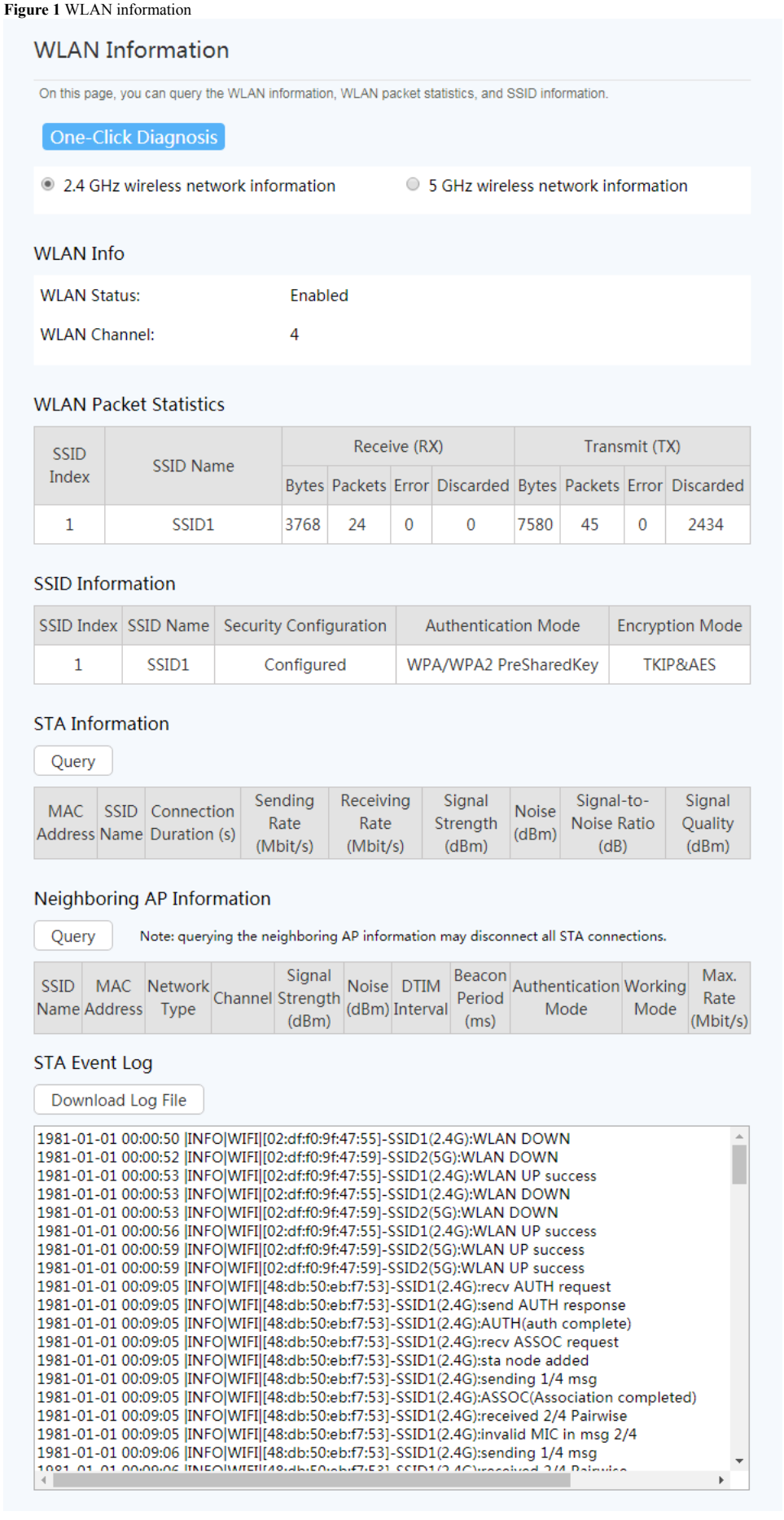
Parent Topic: System Info

< Previous topic Next topic >

1.5.7 WLAN Information

In the navigation tree on the left, choose **System Info** > **WLAN Information**. In the pane on the right, you can query the WLAN information such as the Wi-Fi port status, as shown in Figure 1.

Figure 1 WLAN information



NOTE:

Choose **2.4 GHz wireless network information** or **5 GHz wireless network information** to query 2.4G or 5G WLAN information.

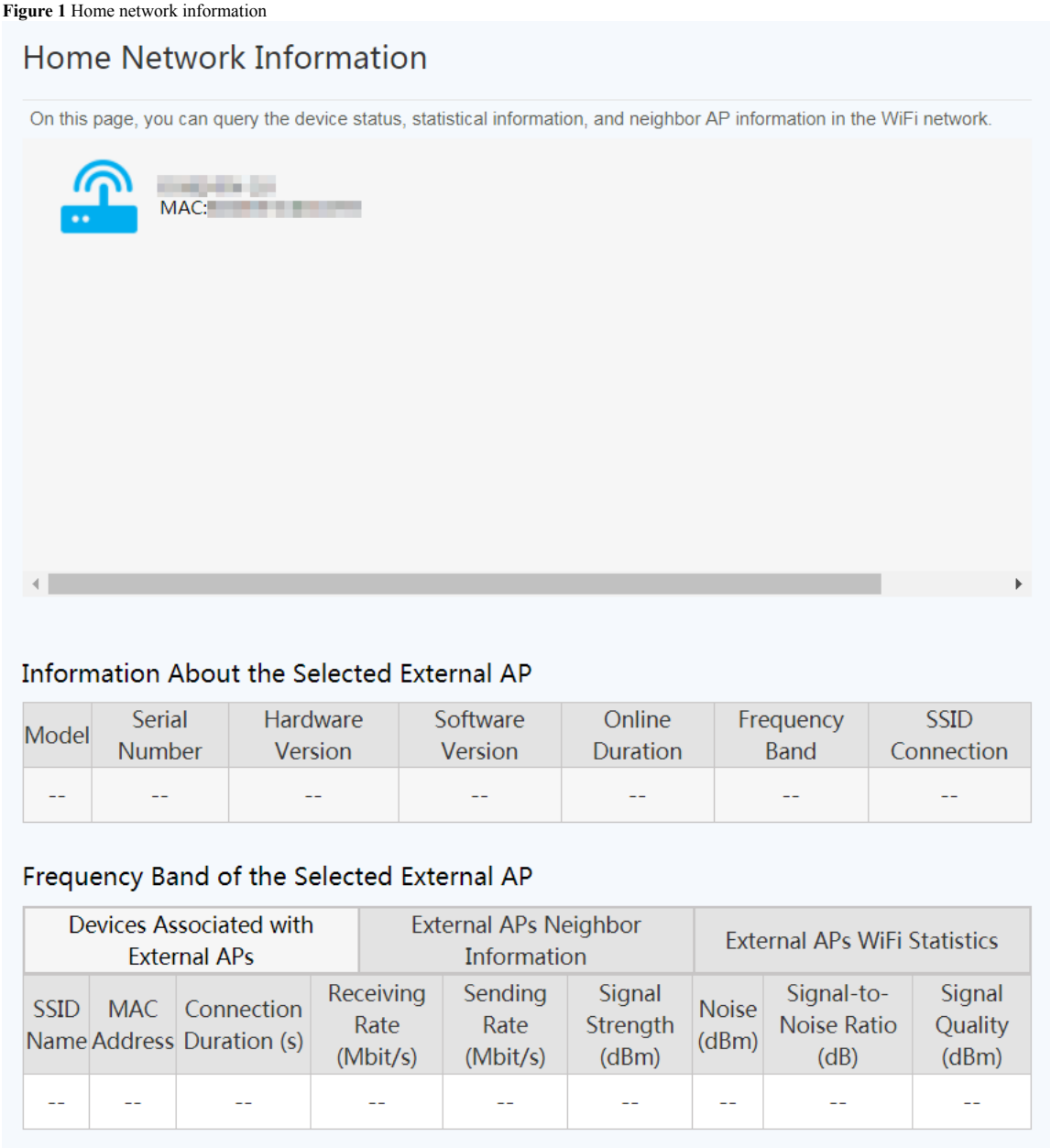
Parent Topic: System Info

< Previous topic Next topic >

1.5.8 Home Network Information

In the navigation tree on the left, choose **System Info** > **Home Network Information**. In the pane on the right, you can view the home network information, as shown in Figure 1.

Figure 1 Home network information



Parent Topic: System Info

< Previous topic

1.6 Advanced Configuration

This topic describes how to configure functions through the web page, including LAN or WAN configuration, security configuration, and so on.

WAN Configuration

This topic describes how to configure the WAN interface through the web page.

LAN Configuration

This topic describes how to configure the LAN port or DHCP parameters through the web page.

Security Configuration

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

Route

This topic describes how to configure the default route and static route through the web page.

Forward Rules

This topic describes how to configure the DMZ, port mapping, and port trigger through the web page.

Application

This topic describes how to configure functions such as time setting through the web page.

WLAN

This topic describes how to perform 2.4G&5G basic and advanced configurations of the WLAN through the web page.

Voice

This topic describes how to configure the voice service through the web page.

System Management

This topic describes how to manage the system on the web page, including the configuration of TR-069, account management, and so on.

Maintenance Diagnose

This topic describes how to maintain the system on the web page, including the method to restart the device, diagnose the fault, upgrade software version, and so on.

Parent Topic: Web Page Reference (DG8245V)

< Previous topic

1.6.1 WAN Configuration

This topic describes how to configure the WAN interface through the web page.

WAN Configuration

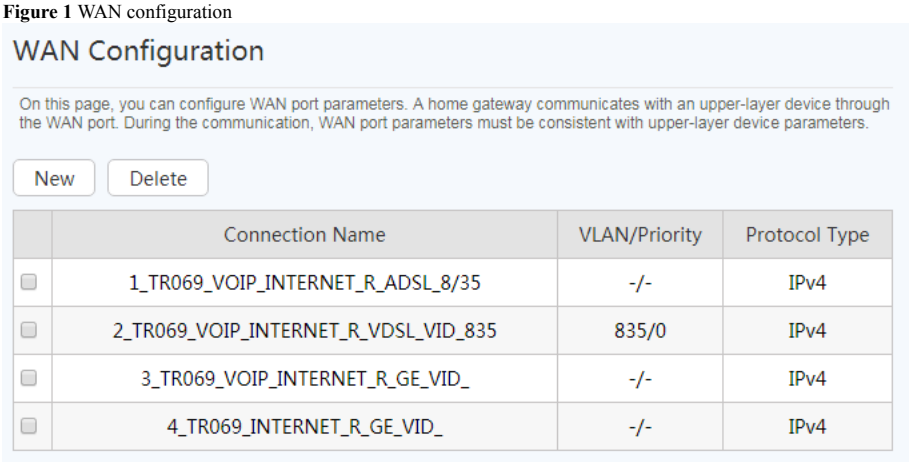
Parent Topic: Advanced Configuration

Next topic >

1.6.1.1 WAN Configuration

In the navigation tree on the left, choose **Advanced Configuration** > **WAN Configuration**. In the pane on the right, you can configure the WAN parameters, as shown in Figure 1.

Figure 1 WAN configuration



NOTE:

- You can select the WAN connection to edit the WAN information.
- You can click **New** to new the WAN connection.
- You can click **Delete** to delete the related WAN connection. All data associated with the WAN will be deleted after you delete the WAN port configuration. Exercise caution when you perform this operation.

Table 1 describes the parameters related to the WAN configuration.

Table 1 Parameters related to the WAN configuration

Parameter	Description
Basic Information	
Enable WAN	Indicates whether to enable the WAN connection.

Parameter	Description
Access Type	Indicates the access type of the WAN port. It can be set to **ATM uplink**, **PTM uplink**, or **GE uplink**.
Encapsulation Mode	Indicates the encapsulation mode of a WAN interface. It can be set to **IPoE** or **PPPoE**.
Protocol Type	Indicates the protocol type of a WAN interface. It can be set to **IPv4**, **IPv6**, or **IPv4/IPv6**.
WAN Mode	Indicates the WAN interface mode. It can be set to **Bridge WAN** or **Route WAN**.
Service Type	Indicates the service type of the WAN interface.
Enable VLAN	Selects this check box to set **VLAN ID** and **802.1p Policy**.
VLAN ID	Indicates the VLAN ID. It ranges from 1 to 4094. The VLAN ID must be the same as the C-VLAN ID on the DSLAM.
802.1p Policy	Indicates the 802.1p priority policy. • Use the specified value: indicates that a specified priority value is used. If you select this option, you need to set the **802.1p** parameter. • Copy from IP precedence: indicates that the priority is copied from the ToS field in the IP header of the user-side packets. If the received packet is not an IP packet or the packet does not carry the 802.1p priority, the default 802.1p priority is used. If you select this option, you need to set the **Default 802.1p** parameter.
802.1p	Indicates the packet 802.1p priority.
Default 802.1p	Indicates the default packet 802.1p priority.
MTU	Indicates the maximum transmission unit (MTU) of IPoE packets. This parameter needs to be set only when **Encapsulation Mode** is set to **IPoE** and **WAN Mode** is set to **Route WAN**.
MRU	Indicates the maximum receive unit (MRU) of PPPoE packets. This parameter needs to be set only when **Encapsulation Mode** is set to **PPPoE** and **WAN Mode** is set to **Route WAN**.
User Name	Indicates the user name that is used for PPPoE dialup. This user name must be the same as that configured on the BRAS. This parameter needs to be set only when **Encapsulation Mode** is set to **PPPoE** and **WAN Mode** is set to **Route WAN**.
Password	Indicates the password that is used for PPPoE dialup. This password must be the same as that configured on the BRAS. This parameter needs to be set only when **Encapsulation Mode** is set to **PPPoE** and **WAN Mode** is set to **Route WAN**.
Enable LCP Detection	This parameter needs to be set only when **Encapsulation Mode** is set to **PPPoE** and **WAN Mode** is set to **Route WAN**. • If you select this option, the LCP detection function is enabled. When the local LCP request times out and no response is received, the system will detect LCP requests from the peer and considers the link normal if the LCP request is detected. • If you do not select this option, the LCP detection function is disabled. When the local LCP request times out and no response is received, the system does not detect LCP requests from the peer and considers the link abnormal.
Binding Options	Used to bind the WAN interface to the LAN port or to the wireless SSID. **NOTE:** Before setting the binding options, set the work mode of the LAN port to route or set the wireless SSID. The binding options can be set only after the work mode or wireless SSID is successfully set. For details, see 2.4G Basic Network Settings and 5G Basic Network Settings.
Link Information **NOTE:** This parameter can be configured when **Access Type** is set to **ATM uplink**.	
VPI/VCI	Indicates the virtual path identifier (VPI) or virtual channel identifier (VCI) provided by the carrier. • VPI value range: 0–255 • VCI value range: 32–65535
Link Mode	Indicates the packet encapsulation mode of a WAN port. It can be set to **EoA**, **PPPoA**, or **IPoA**.
Service Type	Indicates the ATM QoS type. It can be set to **UBR without PCR**, **UBR with PCR**, **CBR**, **Non real-time VBR**, or **Real-time VBR**.
Encapsulation Mode	Indicates the encapsulation mode of ATM frames. It can be set to **LLC** or **VCMUX**.
IPv4 Information **NOTE:** This parameter can be configured when **Protocol Type** is set to **IPv4** or **IPv4/IPv6** and **WAN Mode** is set to **Route WAN**.	

Parameter	Description
IP Acquisition Mode	Indicates the mode of obtaining an IPv4 address on the DSL home gateway. It can be set to **DHCP**, **Static**, or **PPPoE**. If the encapsulation mode is set to **IPoE**, this parameter can be set to **DHCP** or **Static**. If the encapsulation mode is set to **PPPoE**, this parameter can be set to only **PPPoE**. • In DHCP mode, the IP address is dynamically obtained. • In static mode, the IP address is set statically. You need to enter the IP address, subnet mask, IP addresses of the active and standby DNS servers, and default gateway. • In PPPoE mode, you need to enter the user name and password.
Enable NAT	Indicates whether to enable the NAT function.
NAT type	Specifies the NAT type. It can be set to **Port-restricted cone NAT** or **Full-cone NAT**. This parameter is configurable only if the NAT function is enabled. • Port-restricted cone NAT: After an internal address A is mapped to an external address B, an external host can send packets to A by sending packets to B only if A has previously sent a packet to the host. The source IP and port number in the message sent by the host must be the same as the destination IP and port number in the previous message sent by A. • Full-cone NAT: After an internal address A is mapped to an external address B, any external host can send packets to A by sending packets to B.
Dialing Method	Indicates the PPPoE dialup method. It can be set to **Automatic**, **Manual**, or **Packet trigger**. When **IP Acquisition Mode** is set to **PPPoE**, this parameter is configurable.
Vendor ID	Sets the option 60 field on the DHCP client. The IP address can be obtained from the DHCP server only when the option 60 field is the same as the setting on the upper-layer DHCP server. When **IP Acquisition Mode** is set to **DHCP**, this parameter is configurable.
User ID	Adds the Option 61 information to the DHCP packet for a WAN port request. This parameter is used to identify a WAN port uniquely in a customer's network management domain. This parameter is configurable when **IP Acquisition Mode** is set to **DHCP**.
IPv6 Information **NOTE:** This parameter can be configured when **Protocol Type** is set to **IPv6** or **IPv4/IPv6** and **WAN Mode** is set to **Route WAN**.	
Prefix Acquisition Mode	Indicates the prefix acquisition mode. It can be set to **DHCPv6-PD**, **Static**, or **None**. • DHCPv6-PD: When the parameter is set to **DHCPv6-PD**, the BRAS assigns a prefix to the DSL home gateway in DHCPv6 mode. • Static: When the parameter is set to **Static**, you need to manually enter a prefix. • None: When the parameter is set to **None**, no prefix is obtained.
IP Acquisition Mode	Indicates the IP acquisition mode. It can be set to **DHCPv6**, **Automatic**, **Static**, or **None**. • If this parameter is set to **Automatic**, you need to make the prefix mask 64-bit long. The prefix mask length of the IPv6 address is similar to the subnet mask of the IPv4 address. • If this parameter is set to **Static**, you need to enter the IP address, primary DNS server, and secondary DNS server.
Prefix Mask	Indicates the prefix mask.
DS-Lite Working Mode	Indicates that the IPv4 packet is encapsulated into the IPv6 packet and transmitted through IPv6 tunnel. This work mode is only enabled for the DS-Lite solution. This parameter can be configured when **Protocol Type** is set to **IPv6**. • Off: Indicates the DS-Lite work mode is disabled. • Automatic: Indicates that the IP address and domain name of the peer device at the tunnel are automatically obtained using RA or DHCP protocol. • Static: Indicates that the IP address and domain name information of the peer device at the tunnel are manually entered. When this mode is used, you need to enter the AFTR domain name which must be consistent with that on the BRAS.
AFTR Name	Indicates the IP address or domain name of the peer device at the tunnel. AFTR is short for address family transition router. This parameter can be configured when **Protocol Type** is set to **IPv6**.

NOTE:

- WAN in route mode: The DSL home gateway functions as a gateway. The IP address of the DSL home gateway can be obtained through DHCP, static, or PPPoE. The IP address of the PC connected to the DSL home gateway can be obtained from the DHCP address pool of the DSL home gateway or can be set manually.
- WAN in bridge mode: The DSL home gateway functions as a relay and does not process data. The DSL home gateway does not obtain the IP address allocated by the upper-layer device and it does not allow manual configuration of a static IP address. The IP address of the device connected to the DSL home gateway can be obtained through DHCP, PPPoE, or static.
    - In the case of the DHCP mode, you need to set the DHCP relay. After configuration is complete, the user-side IP address is obtained from the upper-layer device. For the detailed procedure, see DHCP Server Configuration.
    - In the case of the PPPoE mode, the user-side IP address is obtained through PPPoE authentication of the upper-layer device.

Parent Topic: WAN Configuration

1.6.2 LAN Configuration

This topic describes how to configure the LAN port or DHCP parameters through the web page.

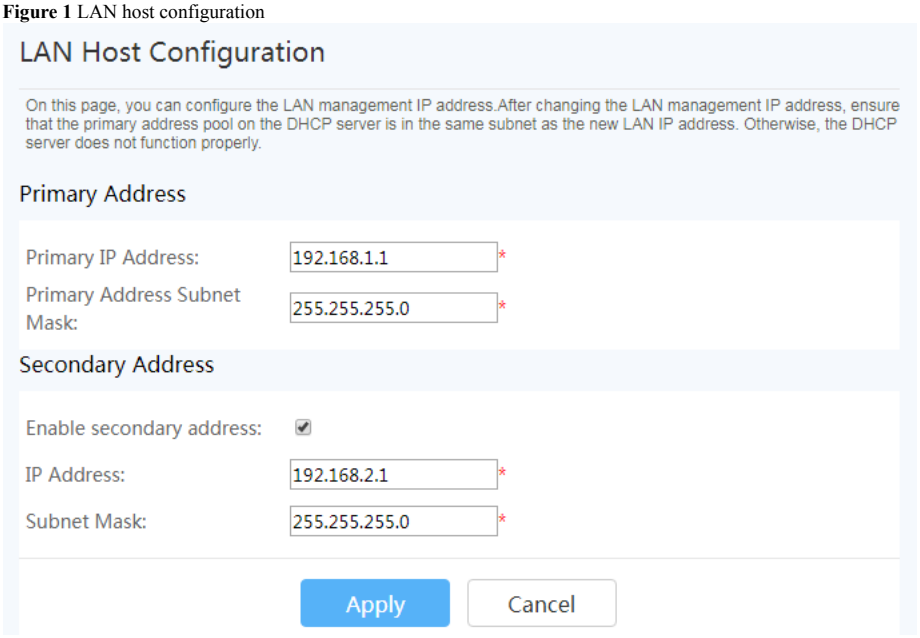
Parent Topic: Advanced Configuration

< Previous topic Next topic >

1.6.2.1 LAN Host Configuration

1. In the navigation tree on the left, choose **Advanced Configuration** > **LAN Configuration** > **LAN Host Configuration**. In the pane on the right, you can configure the LAN management IP address of the primary address and secondary address, as shown in Figure 1.

Figure 1 LAN host configuration



NOTE:

The IP address of the device connected to the LAN port must be in the same subnet as the management IP address. In this way, you can access a DSL home gateway through the web page and perform the query and management.

2. Click **Apply**.

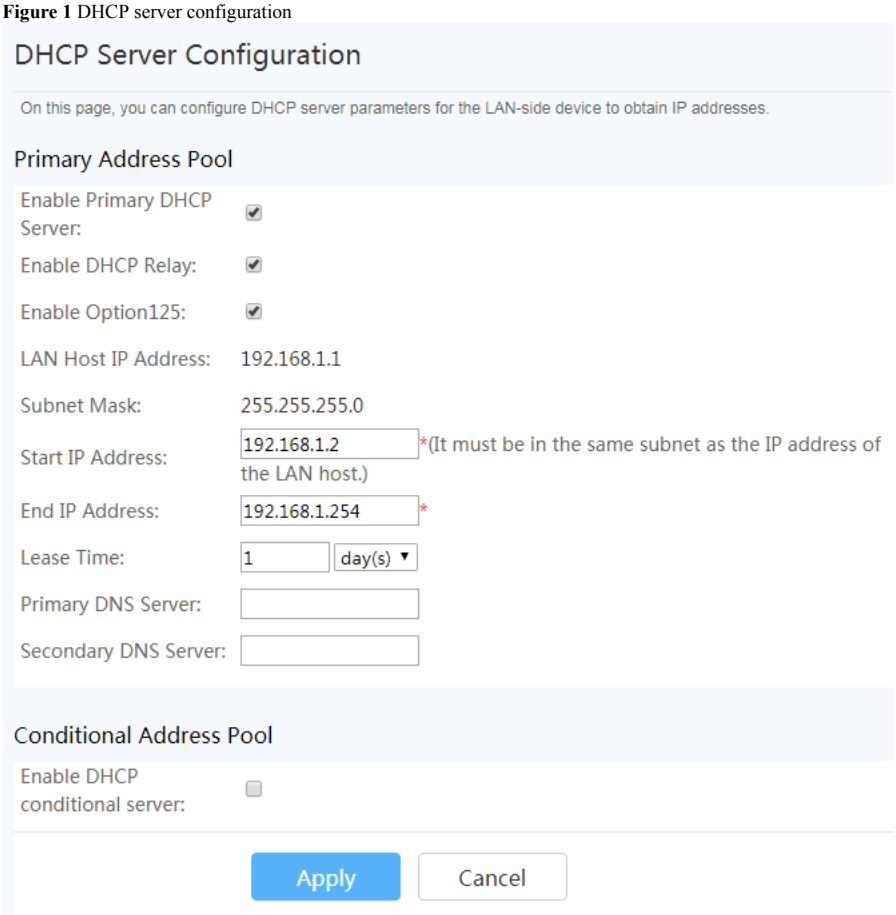
Parent Topic: LAN Configuration

Next topic >

1.6.2.2 DHCP Server Configuration

1. In the navigation tree on the left, choose **Advanced Configuration** > **LAN Configuration** > **DHCP Server Configuration**. In the pane on the right, you can configure the LAN side DHCP address pool for the DSL home gateway that functions as a gateway. After the configuration, the PC connected to the LAN port can automatically obtain an IP address from the address pool, as shown in Figure 1.

Figure 1 DHCP server configuration



2. Click **Apply**.

Table 1 describes the parameters related to the DHCP server.

Table 1 Parameters related to the DHCP server

Parameter	Description
Primary Address Pool	
Enable Primary DHCP Server	Indicates whether to enable the primary DHCP server. If the check box is selected, you can set the primary DHCP server.
Enable DHCP Relay	Indicates whether to enable the DHCP relay. The DHCP relay is a process in which cross-subnet forwarding of DHCP broadcast packets is implemented between the DHCP client and the DHCP server. In this manner, the DHCP clients in different physical subnets can obtain IP addresses which are dynamically allocated from the same DHCP server. • If **WAN Mode** of the WAN port is **Route WAN**, the IP address of the DSL home gateway is obtained from upper-layer DHCP servers in different subnets and the user-side IP addresses are obtained from the DHCP address pool of the DSL home gateway. • If **WAN Mode** of the WAN port is **Bridge WAN**, the DSL home gateway functions as a bridge. In this way, the DSL home gateway does not have an IP address. The user-side IP addresses are obtained from upper-layer DHCP servers in different subnets.
Enable Option125	Enables or disables option125.
LAN Host IP Address	Indicates the IP address of the primary DHCP server.
Subnet Mask	Indicates the mask of the primary DHCP server.
Start IP Address	Indicates the start IP address in the IP address pool on the primary DHCP server.
End IP Address	Indicates the end IP address in the IP address pool on the active DHCP server.
Lease Time	Indicates the lease time of the IP address pool on the active DHCP server. Options: minute, hour, day, and week.
Primary DNS Server	Inputs the IP address of the primary DNS server.
Secondary DNS Server	Inputs the IP address of the secondary DNS server.
Conditioanl Address Pool	

Parameter	Description
Enable DHCP conditional server	Indicates whether to enable the secondary DHCP server. If the check box is selected, you can set the secondary DHCP server.
IP Address	Indicates the IP address of the secondary DHCP server.
Subnet Mask	Indicates the subnet mask of the secondary DHCP server.
Start IP Address	Indicates the start IP address in the IP address pool on the secondary DHCP server.
End IP Address	Indicates the end IP address in the IP address pool on the secondary DHCP server.
Lease Time	Indicates the lease time of the IP address pool on the secondary DHCP server. Options: minute, hour, day, and week.
Option 60	Indicates the option 60 field of the secondary DHCP server. A user-side DHCP client can obtain an IP address from the IP address pool on the secondary DHCP server only when the option 60 field carried by the user-side DHCP client is the same as this setting.
Option60 matching mode	Indicates the option60 matching mode. It can be set to **Exact match**, **Prefix-based match**, **Suffix-based match**, or **String-based match**.
Primary DNS Server	Inputs the IP address of the primary DNS server.
Secondary DNS Server	Inputs the IP address of the secondary DNS server.

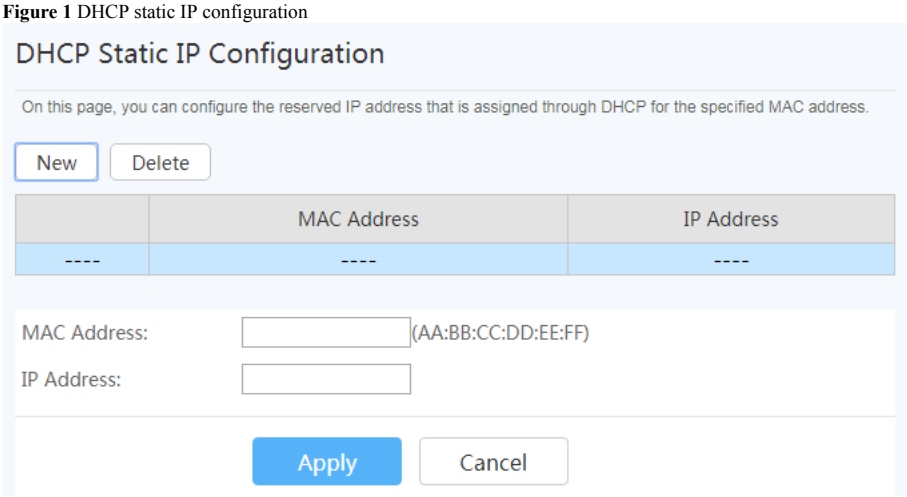
Parent Topic: LAN Configuration

< Previous topic Next topic >

1.6.2.3 DHCP Static IP Configuration

1. In the navigation tree on the left, choose **Advanced Configuration** > **LAN Configuration** > **DHCP Static IP Configuration**. In the pane on the right, click **New**. In the dialog box that is displayed, you can set **MAC Address** and **IP Address**, as shown in Figure 1.

Figure 1 DHCP static IP configuration



2. Click **Apply**.

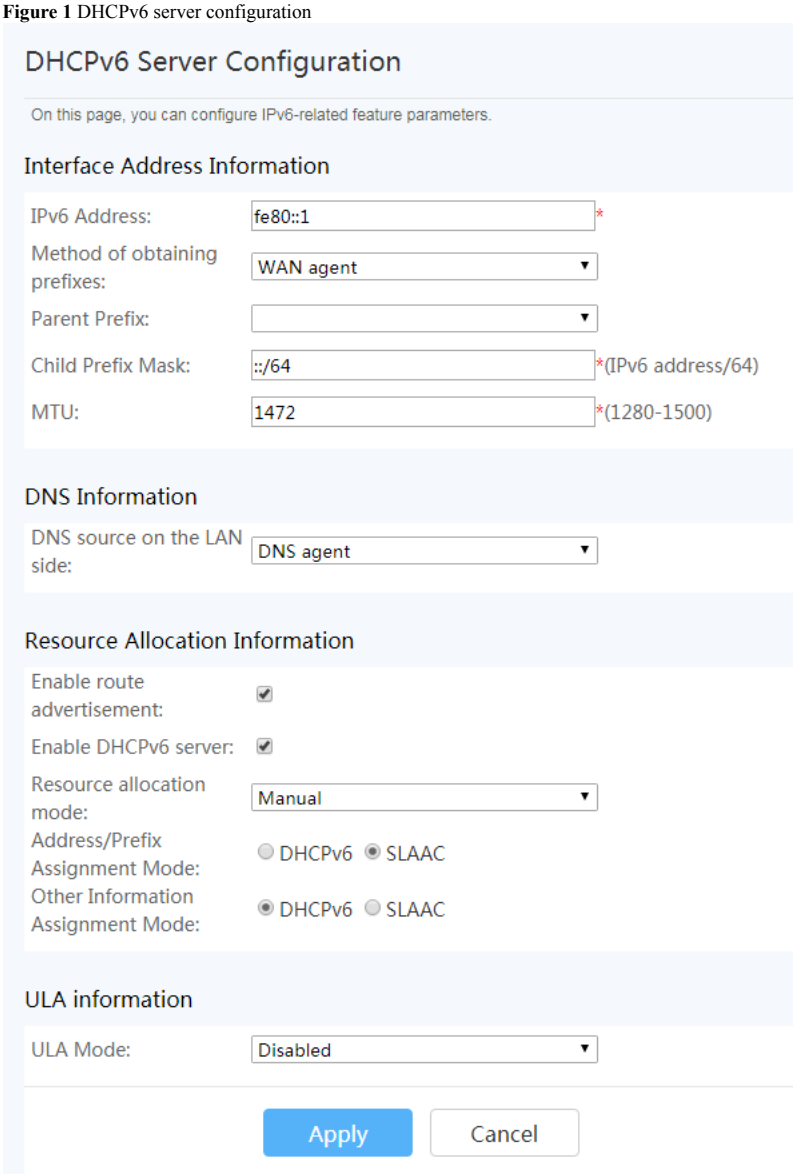
Parent Topic: LAN Configuration

< Previous topic Next topic >

1.6.2.4 DHCPv6 Server Configuration

1. In the navigation tree on the left, choose **Advanced Configuration** > **LAN Configuration** > **DHCPv6 Server Configuration**. In the pane on the right, you can configure the IPv6–related feature parameters, as shown in Figure 1.

Figure 1 DHCPv6 server configuration



2. Click **Apply**.

Table 1 lists the DHCPv6 server configuration parameters.

Table 1 DHCPv6 server configuration parameters

Parameter	Description
Interface Address Information	
IPv6 Address	Indicates the management IP address of IPv6. The default value is **fe80::1**. To configure the management IP address for IPv4, choose **LAN Configuration** > **LAN Host Configuration**.
Method of obtaining prefixes	Indicates the method of obtaining prefixes. It can be set to **WAN agent** or **Static configuration**.
Parent Prefix	Indicates the parent prefix. This parameter can be configured when the **Method of obtaining prefixes** parameter is set to **WAN agent**.
Child Prefix Mask	Indicates the child prefix mask. This parameter can be configured when the **Method of obtaining prefixes** parameter is set to **WAN agent**.
Prefix	Indicates the prefix. This parameter can be configured when the **Method of obtaining prefixes** parameter is set to **Static configuration**.
Preferred period	Indicates the preferred period. This parameter can be configured when the **Method of obtaining prefixes** parameter is set to **Static configuration**.
Valid period	Indicates the valid period. This parameter can be configured when the **Method of obtaining prefixes** parameter is set to **Static configuration**.
MTU	Indicates the maximum transmission unit (MTU) of packets.
DNS Information	
DNS source on the LAN side	Indicates the DNS source on the LAN side. It can be set to **DNS agent**, **WAN port**, or **Static configuration**.

Parameter	Description
WAN name	Indicates the WAN name. This parameter can be configured when the **DNS source on the LAN side** parameter is set to **WAN port**.
Preferred DNS	Indicates the preferred DNS. This parameter can be configured when the **DNS source on the LAN side** parameter is set to **Static configuration**.
Spare DNS	Indicates the spare DNS. This parameter can be configured when the **DNS source on the LAN side** parameter is set to **Static configuration**.
Resource Allocation Information	
Enable route advertisement	Indicates whether to enable the route advertisement.
Enable DHCPv6 server	Indicates whether to enable the DHCPv6 server.
Resource allocation mode	Indicates the mode in which the DSL home gateway allocates prefixes and addresses to the connected PCs. It can be set to **Manual**, **Manual(strict)** or **Automatic**.
Address/Prefix Assignment Mode	Indicates the address/prefix assignment mode. It can be set to DHCPv6 or stateless address autoconfiguration (SLAAC). This parameter can be configured when the **Resource allocation mode** parameter is set to **Manual** or **Manual(strict)**. When it is set to **SLAAC**, **ULA Mode** must be set. • DHCPv6: indicates that the LAN-side host obtains addresses in DHCPv6 mode. • SLAAC: indicates that the LAN-side host obtains addresses in ND mode. In SLAAC mode, the host automatically configures addresses. The address information contains the prefix advertised by the local router and the interface identifier of the host. If there is no router on the link, the host has to automatically configure the link local address to communicate with local nodes.
Other Information Assignment Mode	Indicates the assignment mode of other information. Other information refers to the IPv6 address in payloads of packets such as DNS packets. This parameter can be configured when the **Resource allocation mode** parameter is set to **Manual** or **Manual(strict)**. • DHCPv6: indicates that the address is obtained in DHCPv6 mode. • SLAAC: indicates that the address is obtained in ND mode.
ULA Information	
ULA Mode	Indicates the unique local IPv6 address (ULA) mode. A ULA address starts with a prefix **fd**. Similar to a reserved IPv4 address, the reserved IPv6 address is used for private purpose. This is to ensure protocol consistency. This parameter can be set to **Manual**, **Automatic**, or **Disabled**. **Disabled** is recommended. • Disabled: This function is disabled. • Automatic: The system automatically assigns addresses. • Manual: The address needs to be entered. If this option is selected, **Prefix**, **Prefix Length**, **Preferred Lifetime**, and **Valid Lifetime** also need to be set.
Prefix	Indicates the network address space. IPv6 uses a prefix to indicate the network address space. For example, 2001:251:e000::/48 indicates an address space with a 48-bit prefix.
Prefix Length	Indicates the prefix length, which is a decimal value. It specifies the number of left-most bits used to form a prefix in an address. The address prefix is expressed in the "IPv6 address/prefix length" format. For example, 2001:251:e000::/48 indicates an address space with a 48-bit prefix.
Preferred Lifetime	Indicates the period of time for which a valid address is in the preferred state. When the preferred lifetime expires, the address becomes out of date.
Valid Lifetime	Indicates the period of time for which an address is valid. The valid lifetime must be longer than the preferred lifetime. When the valid lifetime expires, the address becomes invalid.

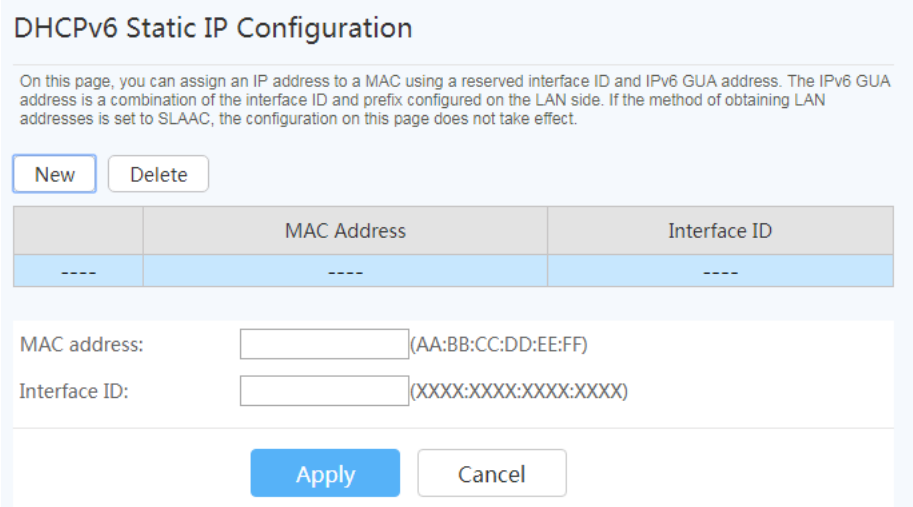
Parent Topic: LAN Configuration

< Previous topic Next topic >

1.6.2.5 DHCPv6 Static IP Configuration

In the navigation tree on the left, choose **Advanced Configuration** > **LAN Configuration** > **DHCPv6 Static IP Configuration**. In the pane on the right, click **New**. In the dialog box that is displayed, you can assign an IP address to a MAC address using the interface ID and IPv6 GUA address. The IPv6 GUA address is a combination of the interface ID and prefix configured on the LAN side, as shown in Figure 1.

Figure 1 DHCPv6 static IP configuration



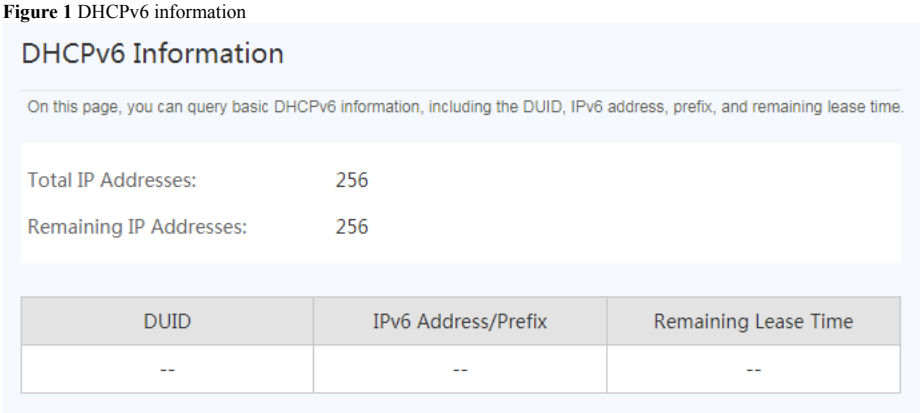
Parent Topic: LAN Configuration

< Previous topic Next topic >

1.6.2.6 DHCPv6 Information

In the navigation tree on the left, choose **Advanced Configuration** > **LAN Configuration** > **DHCPv6 Information**. In the pane on the right, you can view the total number of addresses, the remaining number of IP addresses, the DUID, IPv6 address/prefix, and remaining lease time, as shown in Figure 1.

Figure 1 DHCPv6 information



Parent Topic: LAN Configuration

< Previous topic

1.6.3 Security Configuration

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

- Firewall Level Configuration
- DoS Configuration
- IPv4 Address Filtering
- MAC Address Filtering
- Wi-Fi MAC Address Filtering
- Parental Control
- Precise Device Access Control

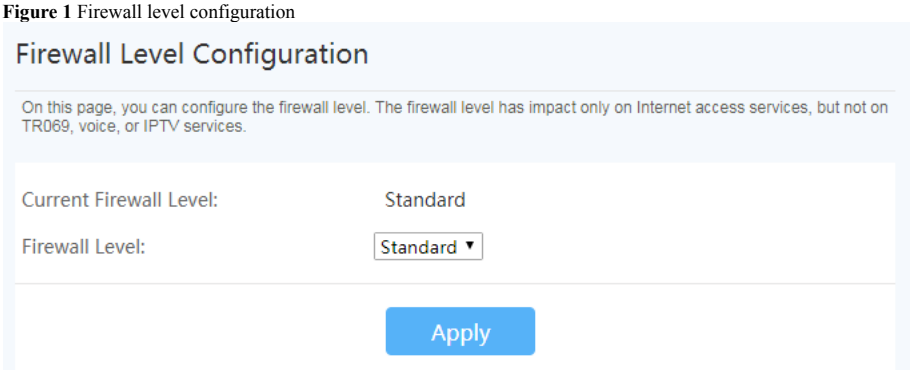
Parent Topic: Advanced Configuration

< Previous topic Next topic >

1.6.3.1 Firewall Level Configuration

1. In the navigation tree on the left, choose **Advanced Configuration** > **Security Configuration** > **Firewall Level Configuration**. In the pane on the right, you can set the firewall level, as shown in Figure 1.

Figure 1 Firewall level configuration



2. Click **Apply**.

Parent Topic: Security Configuration

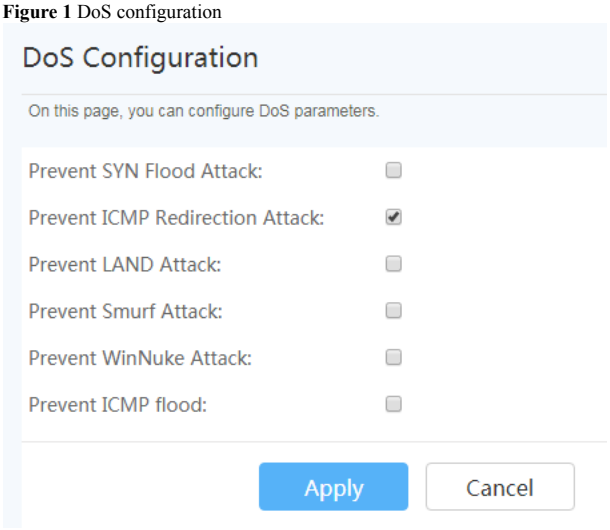
Next topic >

1.6.3.2 DoS Configuration

Denial of service (DoS) attack is a network-based attack that denies users from accessing the Internet. The DoS attack initiates a large number of network connections, making the server or the program running on the server break down or server resources exhaust or denying users to access the Internet service. As a result, the network service fails.

1. In the navigation tree on the left, choose **Advanced Configuration** > **Security Configuration** > **DoS Configuration**. In the pane on the right, you can determine whether to enable the DoS attack-preventive configuration, as shown in Figure 1.

Figure 1 DoS configuration



2. Click **Apply**.

Parent Topic: Security Configuration

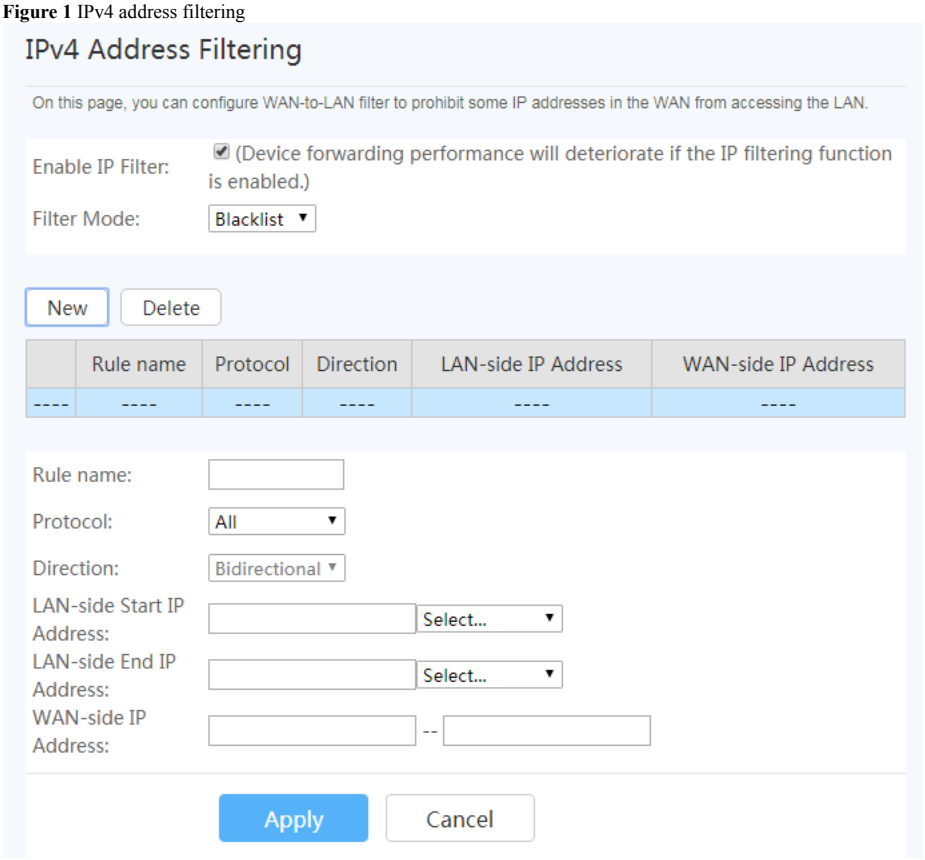
< Previous topic Next topic >

1.6.3.3 IPv4 Address Filtering

The IP address filter function is a security mechanism configured on the residential gateway. It enables or disables all or partial ports in an Intranet IP address segment to communicate with all or partial ports in an Extranet IP address segment. The IP address filter configuration is used to limit communication between an Intranet device and an Extranet device.

1. In the navigation tree on the left, choose **Advanced Configuration** > **Security Configuration** > **IPv4 Address Filtering**. In the pane on the right, select **Enable IP Filter**, set the filter mode, and click **New**. In the dialog box that is displayed, you can configure the rule for filtering IP addresses from the WAN interface to the LAN port, as shown in Figure 1.

Figure 1 IPv4 address filtering



2. Click **Apply**.

Table 1 describes the parameters related to the IPv4 address filter.

Table 1 Parameters related to the IPv4 address filter

Parameter	Description
Enable IP Filter	Indicates whether to enable the IP address filter function.
Filter Mode	Indicates the IP 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. • Hybrid: indicates that packets are filtered based on the upstream or downstream direction. Certain IP packets in the upstream or downstream direction are (not) allowed to pass through. Only one of the preceding modes can be selected.
Rule name	Indicates the name of the rule for filtering IP addresses.
Protocol	Indicates the type of the protocol, which may be **TCP/UDP**, **TCP**, **UDP**, **ICMP**, or **All**.
Priority	Indicates the priority of the IP address. When **Filter Mode** is selected in the hybrid mode, this parameter can be configured. • Range:0–255.
Direction	Indicates the direction to which the filter rule applies. • Bidirectional: This value is available only when **Filter Mode** is **Blacklist** or **Whitelist**. The value cannot be changed. • Upstream: When this value is selected in the hybrid mode, the filter rule applies to the upstream direction. In the hybrid filter mode, only **Upstream** or **Downstream** can be selected. • Downstream: When this value is selected in the hybrid mode, the filter rule applies to the downstream direction.
LAN-side Start IP Address	Indicates the start IP address on the LAN side.
LAN-side End IP Address	Indicates the end IP address on the LAN side.
WAN-side IP Address	Indicates the IP address on the WAN side.
LAN-side TCP Port	Indicates the port ID on the LAN side. This parameter can be configured when **Protocol** is set to **TCP/UDP** or **TCP**.
LAN-side UDP Port	Indicates the port ID on the LAN side. This parameter can be configured when **Protocol** is set to **TCP/UDP** or **UDP**.
WAN-side TCP Port	Indicates the ID of the WAN side port. This parameter can be configured when **Protocol** is set to **TCP/UDP** or **TCP**.
WAN-side UDP Port	Indicates the ID of the WAN side port. This parameter can be configured when **Protocol** is set to **TCP/UDP** or **UDP**.

Parameter	Description
Action	Indicates the IP filter action. When **Filter Mode** is selected in the hybrid mode, this parameter can be configured. • Accept: accepts packets that meet the IP filter rule. • Drop: drops packet that meet the IP filter rule.

Parent Topic: Security Configuration

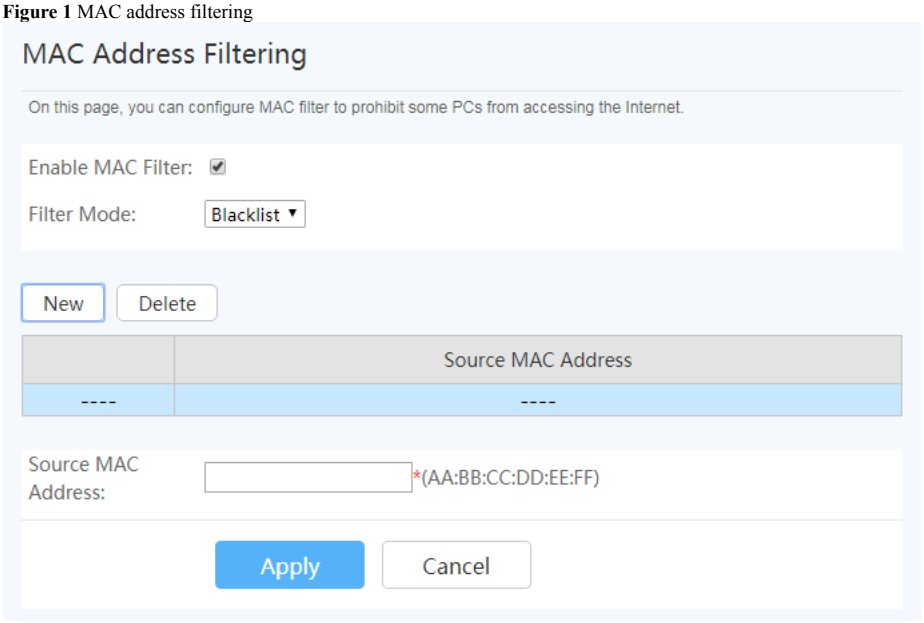
< Previous topic Next topic >

1.6.3.4 MAC Address Filtering

The MAC address lists of PCs in the network are saved on the DSL home gateway. Configuring MAC filter rules enables the PCs that conform to the rules to access the Internet service or disables the PCs that do not conform to the rules to access the Internet service. A PC may have more than one IP addresses but a unique MAC address. Therefore, configuring MAC filter rules effectively controls the Internet service access rights of PCs in a LAN.

1. In the navigation tree on the left, choose **Advanced Configuration** > **Security Configuration** > **MAC Address Filtering**. In the pane on the right, select **Enable MAC Filter**, set the filter mode, and click **New**. In the dialog box that is displayed, you can configure the MAC filter rule for the PC to access the Internet, as shown in Figure 1.

Figure 1 MAC address filtering



2. Click **Apply**.

Table 1 describes the parameters related to the MAC filter.

Table 1 Parameters related to the MAC address filter

Parameter	Description
Enable MAC Filter	Indicates whether to enable the MAC address filter function.
Filter Mode	Indicates the MAC address filter mode.
Source MAC Address	Indicates the source MAC address in the MAC address filter rule.

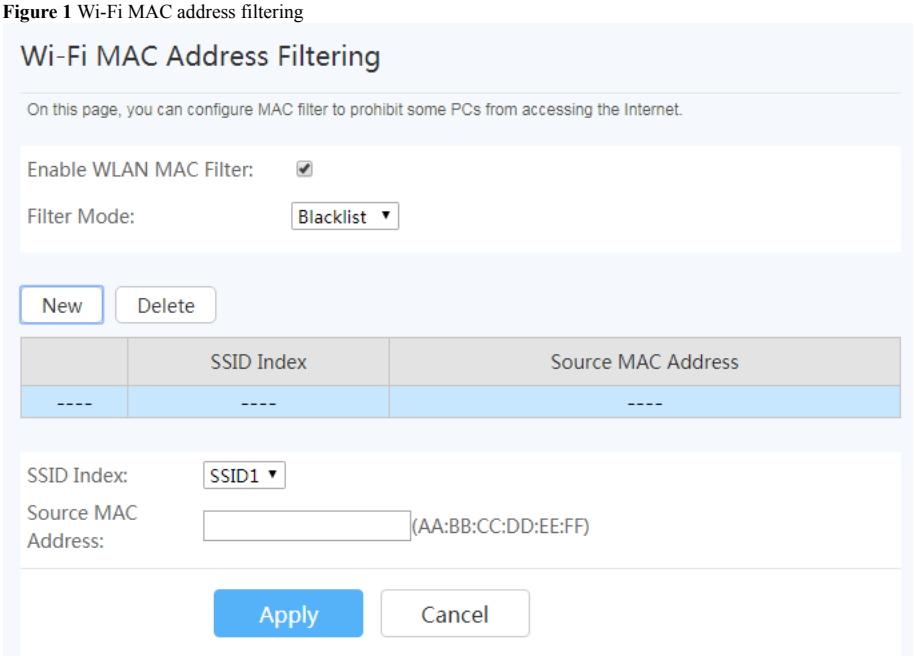
Parent Topic: Security Configuration

< Previous topic Next topic >

1.6.3.5 Wi-Fi MAC Address Filtering

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

Figure 1 Wi-Fi MAC address filtering



2. Click **Apply**.

Table 1 describes the configuration parameters for wireless network MAC filtering.

Table 1 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 filter mode. It can be set to **Blacklist** or **Whitelist**. • Blacklist: forbids data packets that match rules in the blacklist to pass through. • Whitelist: allows data packets that match rules in the whitelist to pass through. The blacklist or whitelist mode is a global configuration. The two modes cannot be used at the same time.
SSID Index	Indicates the SSID index of the WLAN for which MAC address filtering is configured.
Source MAC Address	Indicates the source MAC address in the MAC filter rules.

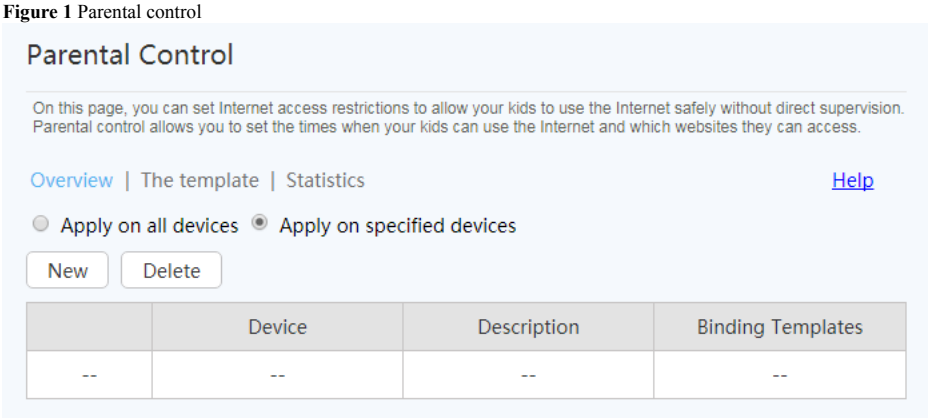
Parent Topic: Security Configuration

< Previous topic Next topic >

1.6.3.6 Parental Control

In the navigation tree on the left, choose **Advanced Configuration** > **Security Configuration** > **Parental Control**. In the pane on the right, you can configure different constraints for the network surfing time and website access on working days and holidays. In this way, the children are allowed to access networks in specified time segments and free from age inappropriate contents, as shown in Figure 1.

Figure 1 Parental control



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.

Parent Topic: Security Configuration

< Previous topic Next topic >

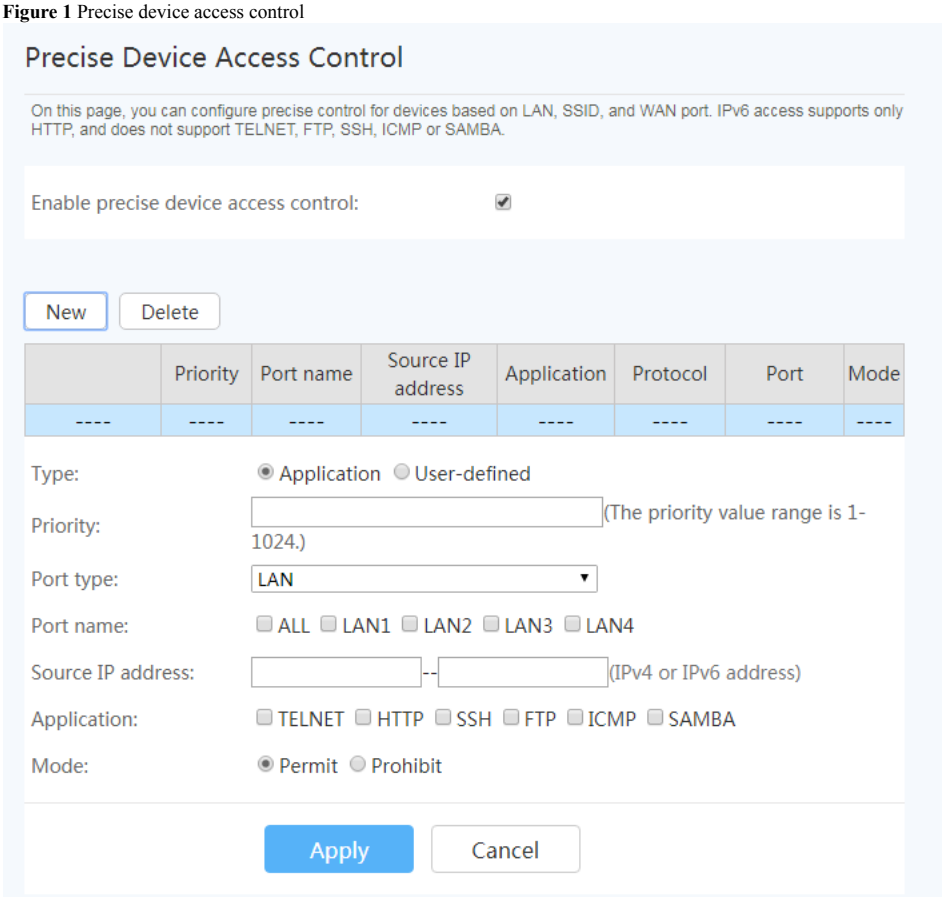
1.6.3.7 Precise Device Access Control

1. In the navigation tree on the left, choose **Advanced Configuration** > **Security Configuration** > **Precise Device Access Control**. In the pane on the right, select **Enable precise device access control** and click **New**. In the dialog box that is displayed, you can configure the rule of DSL home gateway access control, as shown in Figure 1.

DANGER:

Complete network security planning before enabling remote access control to ensure that DSL home gateways are logged in to in secure network conditions. After the DSL home gateway 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 1 Precise device access control



2. Click **Apply**.

Table 1 describes the parameters related to the precise device access control.

Table 1 Parameters related to the precise device access control

Parameter	Description
Enable precise device access control	Indicates whether to enable the precise device access control.
Type	Indicates the type. It can be set to **Application** or **User-defined**.
Priority	Indicates the priority.
Port type	Indicates the port type.
Port name	Indicates the port name.
Source IP address	Indicates the source IP address.
Application	Indicates the application. This parameter needs to be set only when **Type** is set to **Application**.

Parameter	Description
Protocol	Indicates the protocol. This parameter needs to be set only when **Type** is set to **User-defined**.
Port	Indicates the port. This parameter needs to be set only when **Type** is set to **User-defined**.
Mode	Indicates the mode.

Parent Topic: Security Configuration

< Previous topic

1.6.4 Route

This topic describes how to configure the default route and static route through the web page.

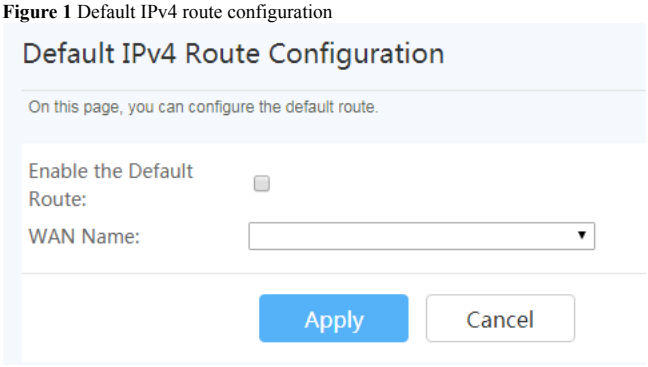
Parent Topic: Advanced Configuration

< Previous topic Next topic >

1.6.4.1 Default IPv4 Route Configuration

1. In the navigation tree on the left, choose **Advanced Configuration** > **Route** > **Default IPv4 Route Configuration**. In the pane on the right, you can select or deselect the **Enable the Default Route** option button to enable or disable the default route of the system, as shown in Figure 1.

   Figure 1 Default IPv4 route configuration

   NOTE:
   If a DSL home gateway fails to find a matching routing entry after receiving a packet, the WAN interface specified by the default route configuration sends the packet to a network device. Before the default route of the system is enabled, the WAN interface must obtain the IP address. Therefore, the parameters of the WAN interface must be correctly set. For details, see WAN Configuration.

2. Click **Apply**.

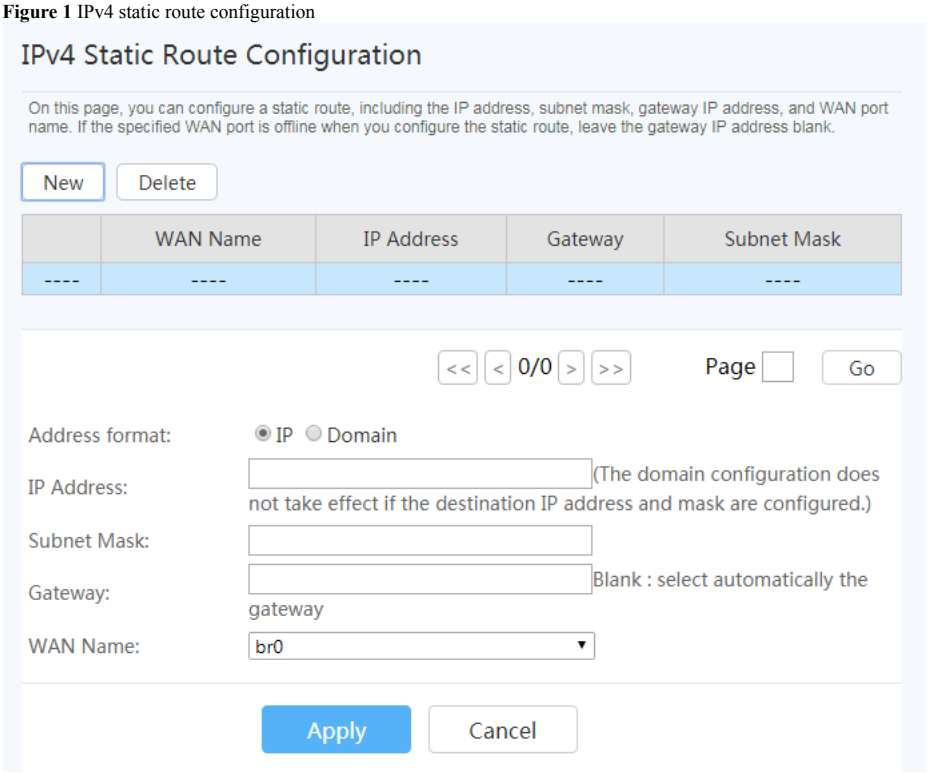
Parent Topic: Route

Next topic >

1.6.4.2 IPv4 Static Route Configuration

1. In the navigation tree on the left, choose **Advanced Configuration** > **Route** > **IPv4 Static Route Configuration**. In the pane on the right, click **New**. In the dialog box that is displayed, you can set the parameters related to the static route, as shown in Figure 1.

Figure 1 IPv4 static route configuration



2. Click **Apply**.

Table 1 describes the parameters related to the static route.

Table 1 Parameters related to the static route

Parameter	Description
Address format	Indicates the format of an address, which can be in IP address or domain name format. When both the destination IP address and the domain name are configured, only the destination IP address takes effect.
IP Address	Indicates the destination IP address of the static route. This parameter must be configured when the IP address format is specified for **Address format**.
Subnet Mask	Indicates the subnet mask of the static route. This parameter must be configured when the IP address format is specified for **Address format**.
Domain	Indicates the domain name of the static route. This parameter must be configured when the domain name formats is specified for **Address format**. The wildcard domain names in the following formats are supported: *.abc.com, abc.com.*, and abc.*.com. The wildcard domain names in the following format are not supported: *abc.com, abc*.com, and a*c.com.
Gateway	Indicates the gateway IP address of the static route.
WAN Name	Indicates the WAN interface that the route travels through.

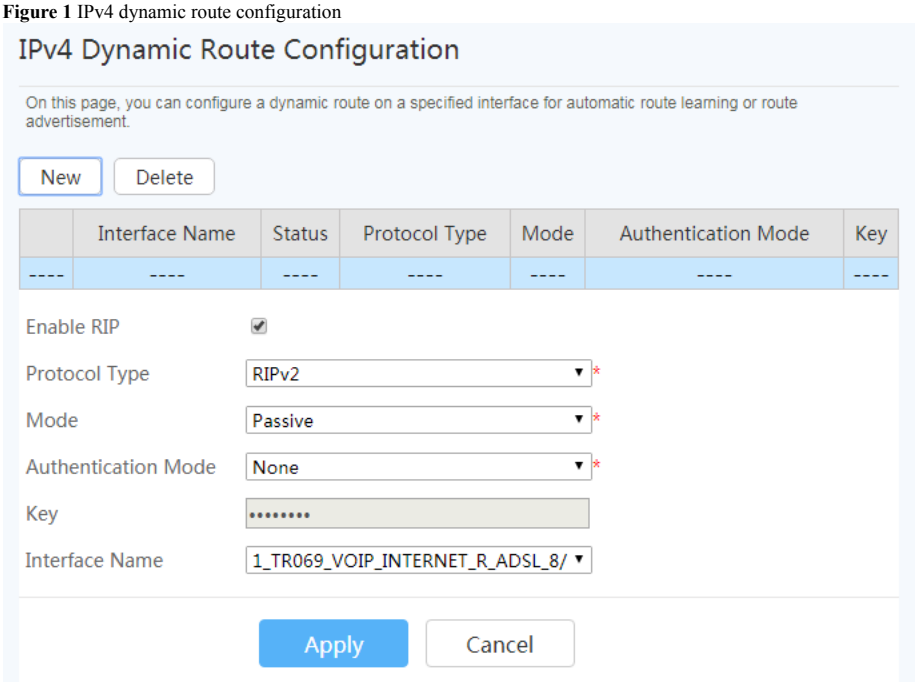
Parent Topic: Route

< Previous topic Next topic >

1.6.4.3 IPv4 Dynamic Route Configuration

1. In the navigation tree on the left, choose **Advanced Configuration** > **Route** > **IPv4 Dynamic Route Configuration**. In the pane on the right, click **New**. In the dialog box that is displayed, you can set the parameters related to the dynamic route, as shown in Figure 1.

Figure 1 IPv4 dynamic route configuration



2. Click **Apply**.

Table 1 describes the parameters related to the dynamic route.

Table 1 Parameters related to the dynamic route

Parameter	Description
Enable RIP	Controls whether the RIP function configured on the WAN port takes effect.
Protocol Type	Indicates the RIP protocol type. It is used for dynamic route learning and route advertisement. • RIPv1: does not support packet authentication. When this protocol type is selected, the authentication mode automatically changes to **None**. • RIPv2: supports packet authentication. • RIPv1_v2: supports both RIPv1 and RIPv2.
Mode	Indicates the RIP protocol working mode. Its values are **Active** and **Passive**. • Active: advertises and automatically learns routes. • Passive: only automatically learns routes but does not advertise routes.
Authentication Mode	Indicates the packet authentication mode. It is used for authentication on route learning and advertisement packets. • When RIPv1 is selected, the authentication mode cannot be edited and is set to **None**. • When RIPv1_v2 is selected, the authentication mode works for only RIPv2 and RIPv1 packets are not authenticated.
Key	Indicates the key required for packet authentication. • It cannot be set if the authentication mode is **None**. • It is mandatory if the authentication mode is **Plaintext**, **MD5**, or **HMAC-SHA256**.
Interface Name	Indicates the name of a WAN port, which is used to associate a port configured using a dynamic route. By default, it is the name of every WAN port.

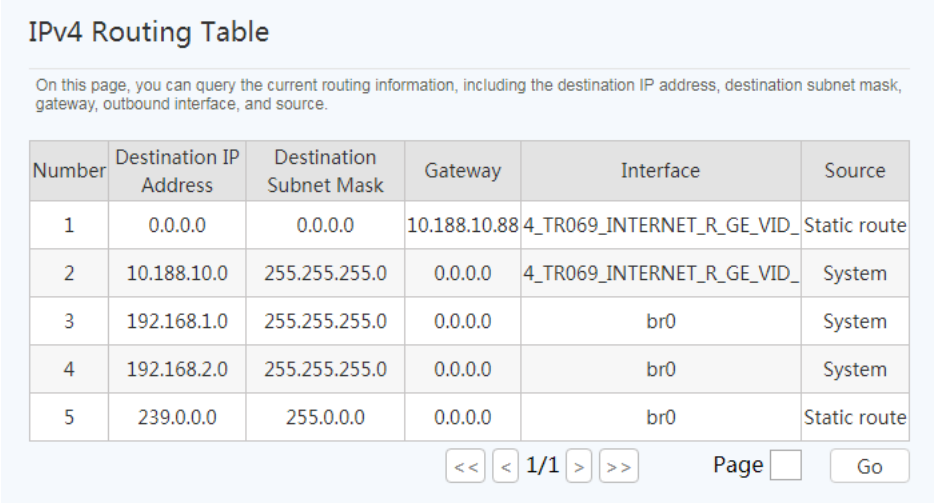
Parent Topic: Route

< Previous topic Next topic >

1.6.4.4 IPv4 Routing Table

In the navigation tree on the left, choose **Advanced Configuration** > **Route** > **IPv4 Routing Table**. In the pane on the right, routing information of the device is displayed, including the destination IP address, destination subnet mask, gateway, and outgoing interface, as shown in Figure 1.

Figure 1 IPv4 routing table



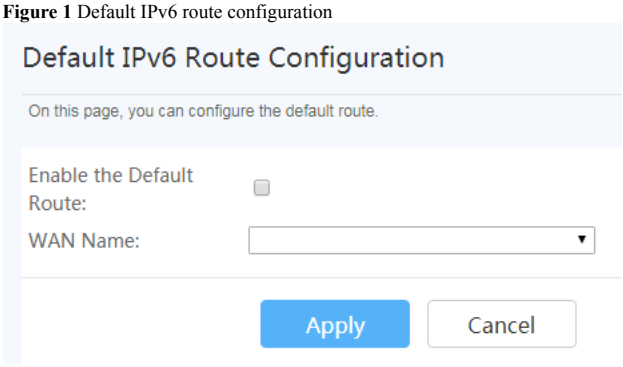
Parent Topic: Route

< Previous topic Next topic >

1.6.4.5 Default IPv6 Route Configuration

1. In the navigation tree on the left, choose **Advanced Configuration** > **Route** > **Default IPv6 Route Configuration**. In the pane on the right, you can select or deselect the **Enable the Default Route** option button to enable or disable the default route of the system, as shown in Figure 1.

   Figure 1 Default IPv6 route configuration

   NOTE:
   If a DSL home gateway fails to find a matching routing entry after receiving a packet, the WAN interface specified by the default route configuration sends the packet to a network device. Before the default route of the system is enabled, the WAN interface must obtain the IP address. Therefore, the parameters of the WAN interface must be correctly set. For details, see WAN Configuration.

2. Click **Apply**.

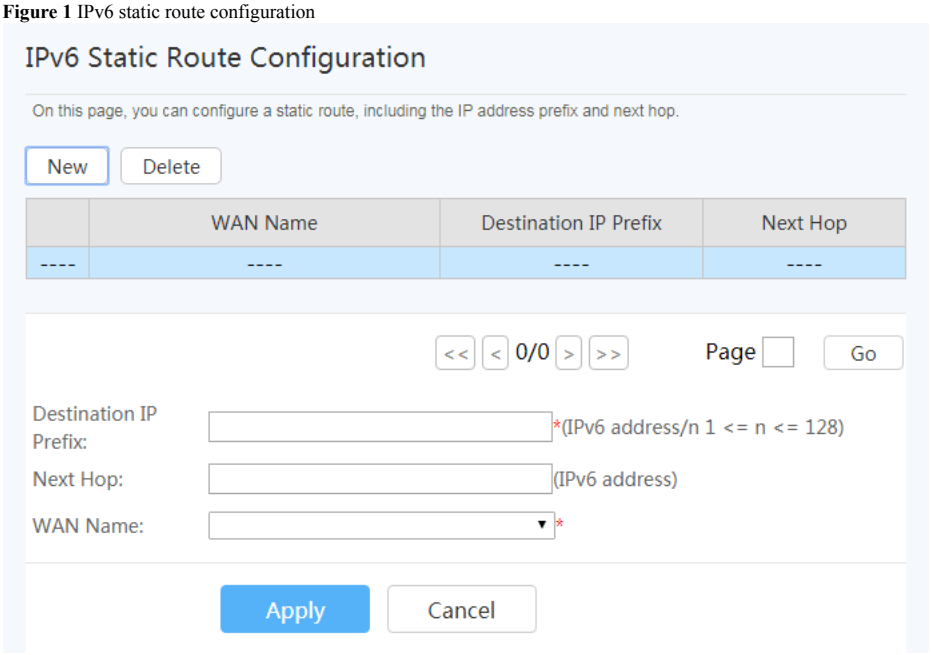
Parent Topic: Route

< Previous topic Next topic >

1.6.4.6 IPv6 Static Route Configuration

1. In the navigation tree on the left, choose **Advanced Configuration** > **Route** > **IPv6 Static Route Configuration**. In the pane on the right, click **New**. In the dialog box that is displayed, you can set the parameters related to the static route, as shown in Figure 1.

Figure 1 IPv6 static route configuration



2. Click **Apply**.

Table 1 lists the configuration parameters for a static route.

Table 1 Static route parameters

Parameter	Description
Destination IP Prefix	This parameter needs to be set when the obtained prefix is shorter than 64 bits. It is used for LAN IP address allocation.
Next Hop	Indicates the destination IP address of the static route.
WAN Name	Indicates the WAN interface that the static route traverses.

Parent Topic: Route

< Previous topic

1.6.5 Forward Rules

This topic describes how to configure the DMZ, port mapping, and port trigger through the web page.

Parent Topic: Advanced Configuration

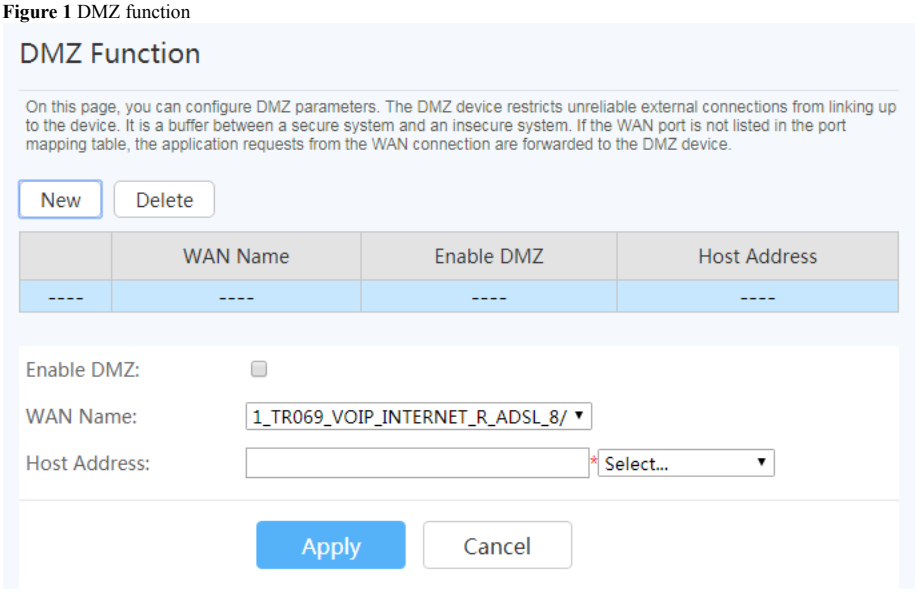
< Previous topic Next topic >

1.6.5.1 DMZ Function

The demilitarized zone (DMZ) is a technology that enables the DSL home gateway to forward all received packets through a specified internal server. The technology enables a computer in the LAN to be completely exposed to all users on the Internet or enables the mutual communication without restrictions between a host with a specified IP address and other users or other servers on the Internet. In this way, many applications can run on the host with the specified IP address. The host with the specified IP address receives all connections and files that can be identified.

1. In the navigation tree on the left, choose **Advanced Configuration** > **Forward Rules** > **DMZ Function**. In the pane on the right, click **New**. In the dialog box that is displayed, you can set the parameters related to the DMZ, as shown in Figure 1.

Figure 1 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.

Table 1 describes the parameters related to the DMZ.

Table 1 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.

Parent Topic: Forward Rules

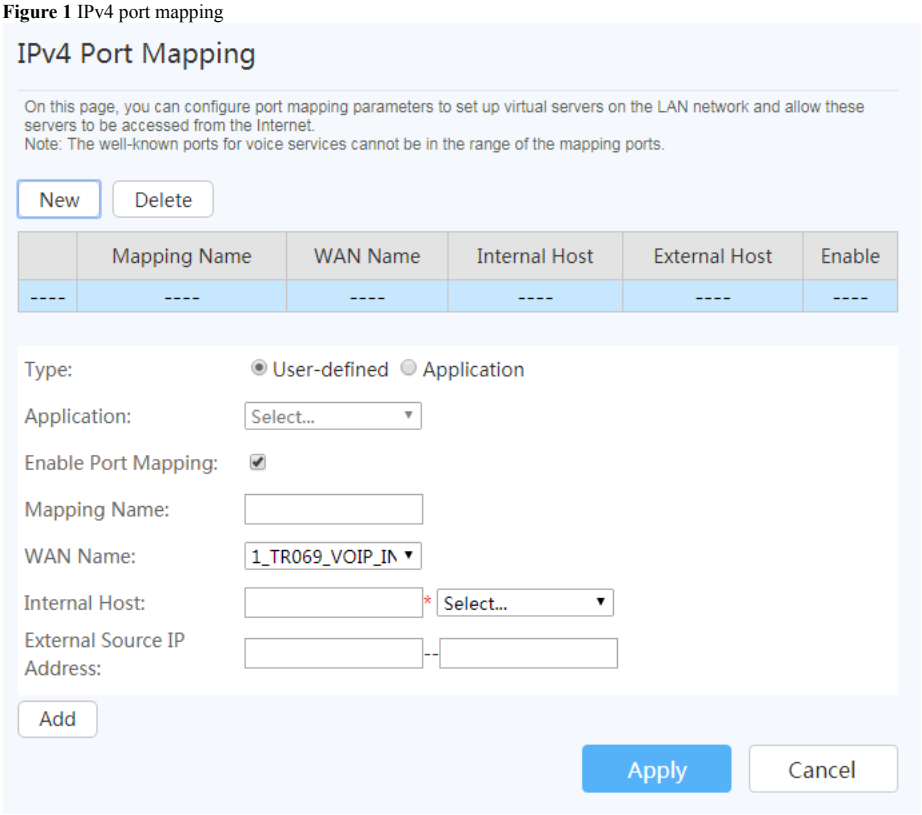
Next topic >

1.6.5.2 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.

1. In the navigation tree on the left, choose **Advanced Configuration** > **Forward Rules** > **IPv4 Port Mapping**. In the pane on the right, click **New**. In the dialog box that is displayed, you can set the parameters related to port mapping, as shown in Figure 1.

Figure 1 IPv4 port mapping



2. Click **Apply**.

Table 1 describes the parameters related to IPv4 port mapping.

Table 1 Parameters related to IPv4 port mapping

Parameter	Description
Type	Indicates the port mapping type. It can be set to **User-defined** or **Application**. • After **User-defined** is selected, **Protocol**, **Internal port number**, and **External port number** need to be manually configured. • After **Application** is selected, the default values of **Protocol**, **Internal port number**, and **External port number** are displayed.
Application	Indicates the application type of port mapping. This parameter can be configured only when the **Type** parameter is set to **Application**.
Enable Port Mapping	Indicates whether to enable port mapping.
Mapping Name	Indicates the name of the port mapping rule.
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**.
Internal port number	Indicates the internal destination start and end ports of the port mapping.
External port number	Indicates the external destination start and end ports of the port mapping.
External source port number	Indicates the external source start and end ports of the port mapping.

Parent Topic: Forward Rules

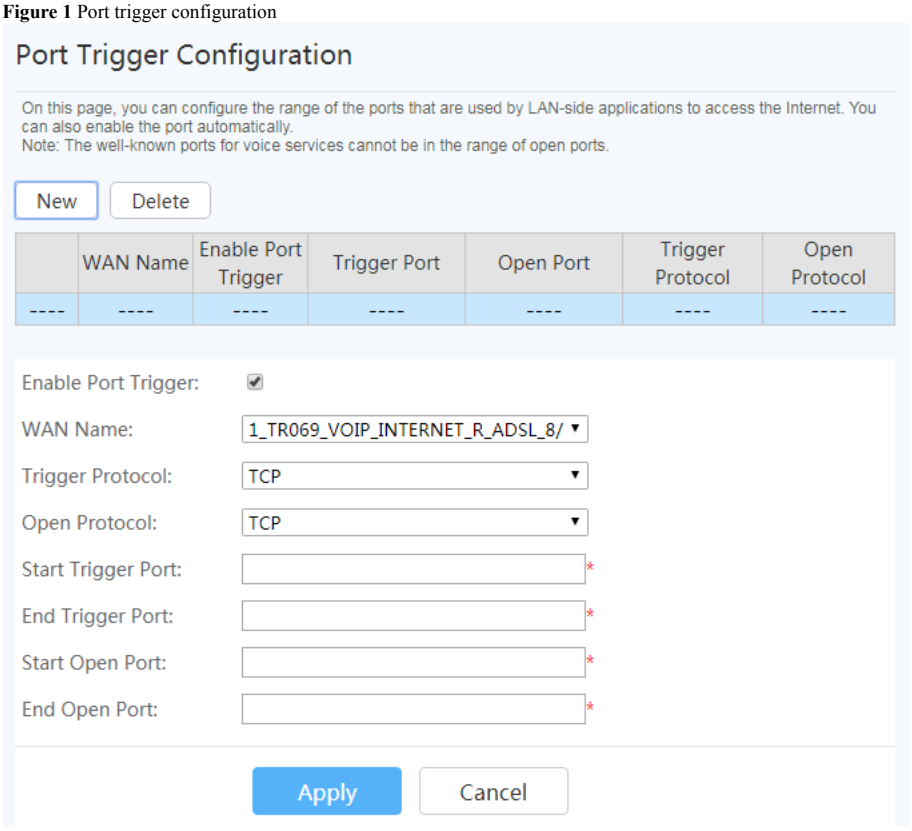
< Previous topic Next topic >

1.6.5.3 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 DSL home gateway 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 **Advanced Configuration** > **Forward Rules** > **Port Trigger Configuration**. In the pane on the right, click **New**. In the dialog box that is displayed, you can set the parameters related to the port trigger, as shown in Figure 1.

Figure 1 Port trigger configuration



2. Click **Apply**.

Table 1 describes the parameters related to the port trigger.

Table 1 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, which may be **TCP**, **UDP**, or **TCP/UDP**.
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.
Start Open Port	Indicates the destination start port of the open packet.
End Open Port	Indicates the destination end port of the open packet.

Parent Topic: Forward Rules

< Previous topic

1.6.6 Application

This topic describes how to configure functions such as time setting through the web page.

QoS Configuration

ARP Ping

Static DNS

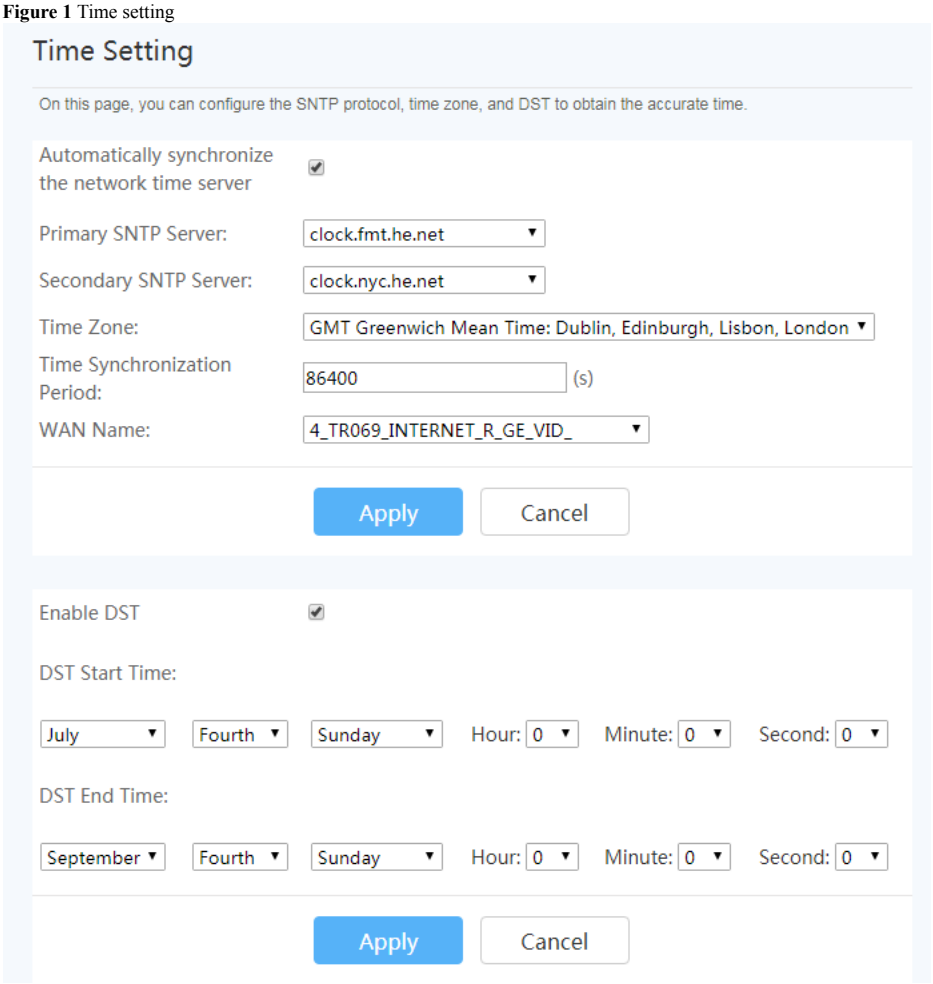
Parent Topic: Advanced Configuration

< Previous topic Next topic >

1.6.6.1 Time Setting

1. In the navigation tree on the left, choose **Advanced Configuration** > **Application** > **Time Setting**. In the pane on the right, select **Automatically synchronize the network time server** and **Enable DST**. In the dialog box that is displayed, you can set the parameters related to the system time, including the SNTP server, time zone, and daylight saving time (DST), as shown in Figure 1.

Figure 1 Time setting



2. Click **Apply**.

Table 1 describes the parameters related to the system time.

Table 1 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 time synchronization period.
WAN Name	Indicates the name of the WAN for time synchronization.
Enable DST	Indicates whether to enable the DST.
DST Start Time	Indicates the DST start time.

Parameter	Description
DST End Time	Indicates the DST end time.

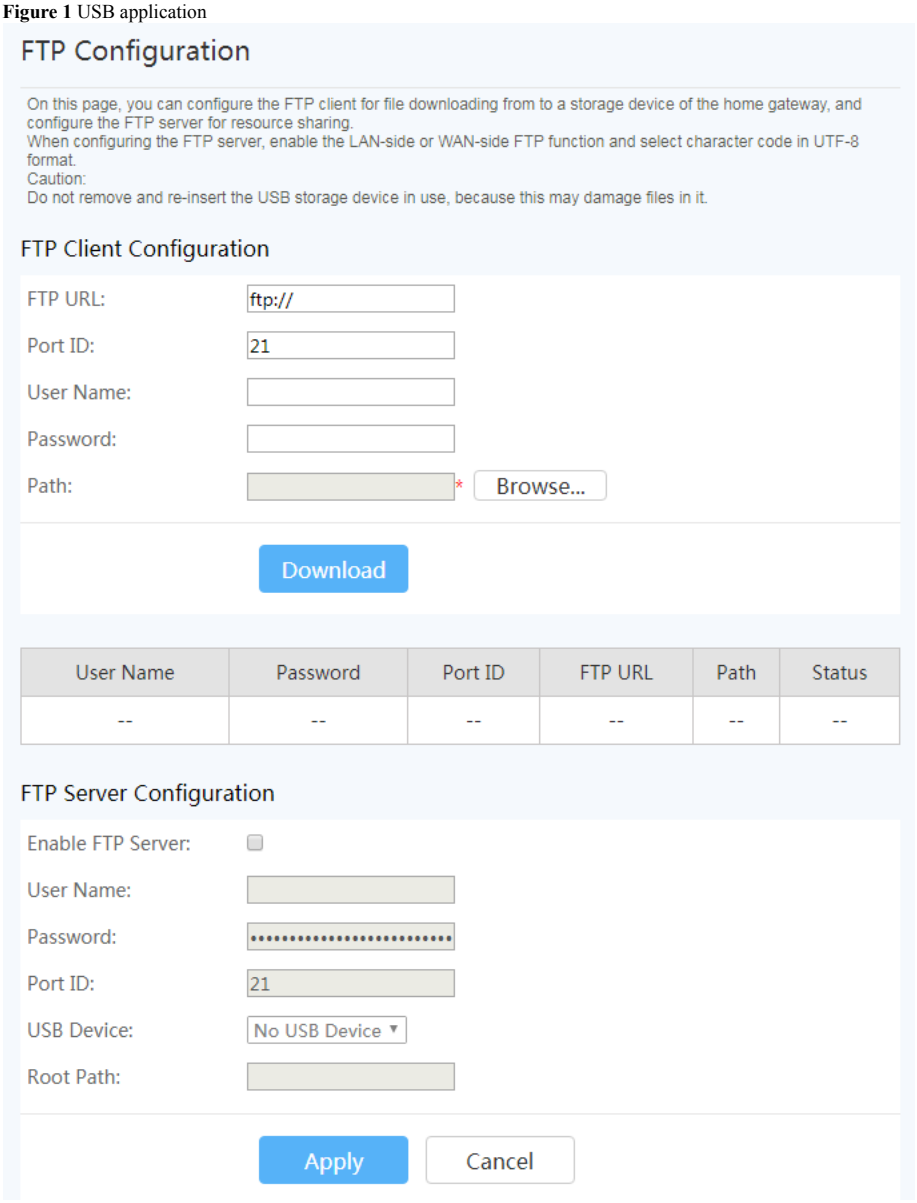
Parent Topic: Application

Next topic >

1.6.6.2 USB Application

1. In the navigation tree on the left, choose **Advanced Configuration** > **Application** > **USB Application**. In the pane on the right, you can set the parameters to share the FTP file of the DSL home gateway, as shown in Figure 1.

Figure 1 USB application



2. Click **Apply**.

NOTE:

- FTP server configuration supports only English.
- The file time of a DSL home gateway is in the UNIX format. In Windows OS, the file time displayed may be different from the actual time for FTP access.

Table 1 describes the parameters related to the USB.

Table 1 Parameters related to the USB

Parameter	Description
FTP Client Configuration	
FTP URL	Indicates the FTP URL of the FTP client.

Parameter	Description
Port ID	Indicates the port ID of the FTP client.
User Name	Sets the user name of the FTP client.
Password	Sets the password of the FTP client.
Path	Indicates the path of the FTP client.
FTP Server Configuration	
Enable FTP Server	Enables the FTP server when the DSL home gateway serves as an FTP server.
User Name	Sets the user name of the FTP server. This user name is required when another FTP client logs in to the FTP server.
Password	Sets the password of the FTP server. This password is required when another FTP client logs in to the FTP server.
Port ID	Indicates the port ID.
USB Device	Indicates the drive of the external USB device for saving the file downloaded through FTP.
Root Path	Indicates the path for saving shared files when the DSL home gateway serves as a server.

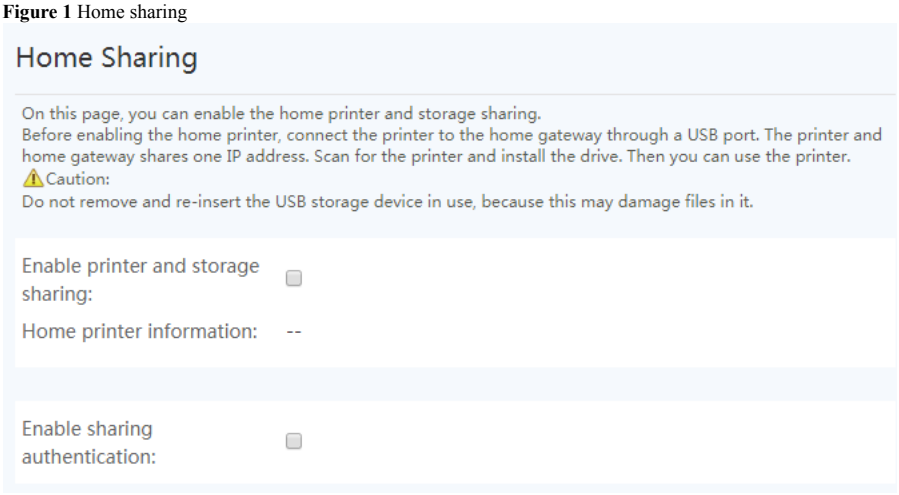
Parent Topic: Application

< Previous topic Next topic >

1.6.6.3 Home Sharing

1. In the navigation tree on the left, choose **Advanced Configuration** > **Application** > **Home Sharing**. In the pane on the right, you can configure the home sharing parameters, as shown in Figure 1.

   Figure 1 Home sharing

2. Click **Apply**.

NOTE:

- To enable a home printer, connect it to the USB port of the home gateway (DSL home gateway). The IP address of this printer is the IP address of the DSL home gateway. This printer can be used after it is searched out and its driver is installed.

  Do not remove and re-insert the USB storage device in use, because this may damage files in it.

  A file (such as PDF) may fail to be printed in the Windows OS in any of the following cases:

  - The Windows domain is used and user domain fails to be authenticated.
  - An alias is used to access the printer.
  - No authentication mode is used for a printer.

  This issue occurs because of application program incompatibility. If this issue occurs, check your Windows or printer settings.
- If the security software is installed on the PC, which leads to Samba user name authentication failure for the first login attempt, authenticate the user name again or use the Samba function in anonymity.

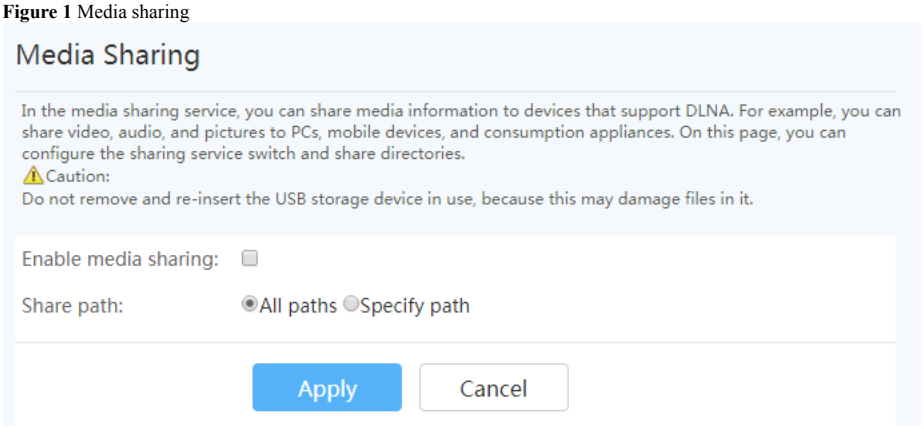
Parent Topic: Application

< Previous topic Next topic >

1.6.6.4 Media Sharing

1. In the navigation tree on the left, choose **Advanced Configuration** > **Application** > **Media Sharing**. In the pane on the right, you can configure the media sharing parameters, as shown in Figure 1.

Figure 1 Media sharing



2. Click **Apply**.

Parent Topic: Application

< Previous topic Next topic >

1.6.6.5 DDNS Function

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

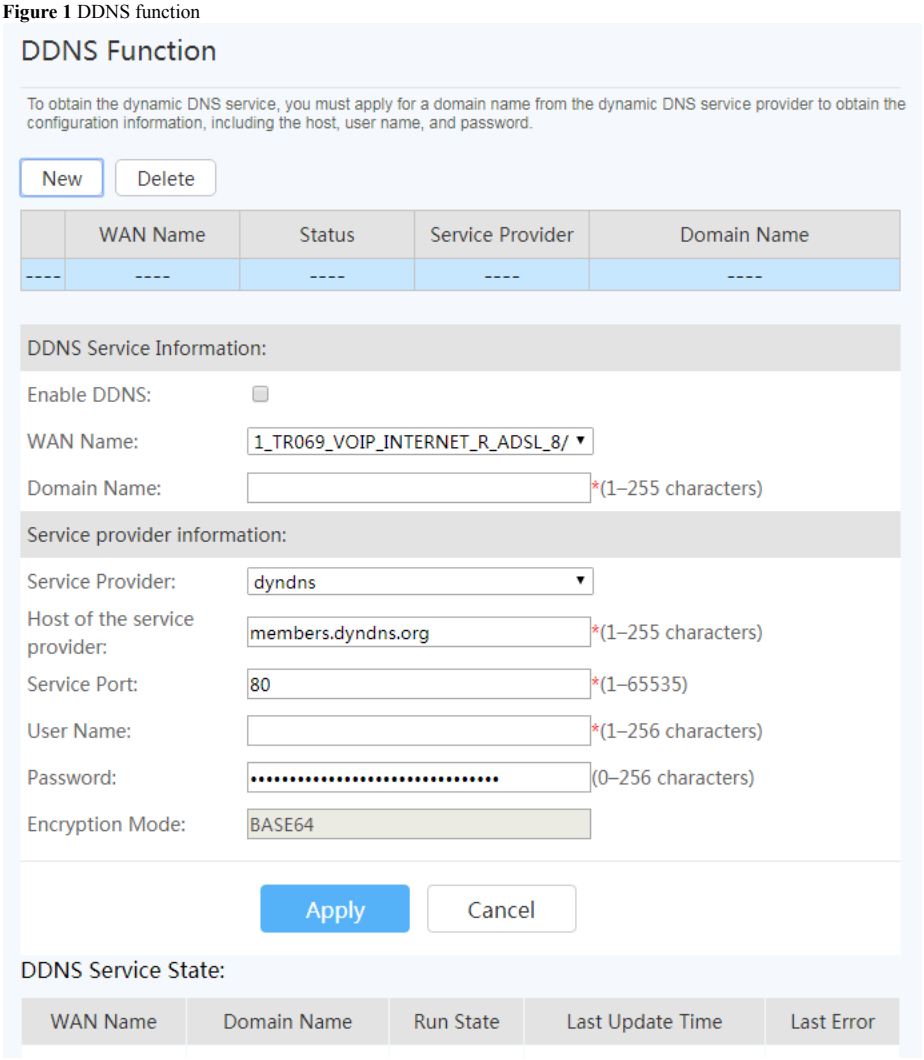
Assume that server A provides HTTP or FTP service and it is connected to the Internet using routers. If server A obtains an IP address through DHCP, or server A is connected to the Internet through PPPoE, PPTP, or L2TP, the IP address is a dynamic IP address. That is, its IP address may change each time 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 **Advanced Configuration** > **Application** > **DDNS Function**. In the pane on the right, click **New**. In the dialog box that is displayed, you can configure the DDNS parameters, as shown in Figure 1.

Figure 1 DDNS function



2. Click **Apply**.

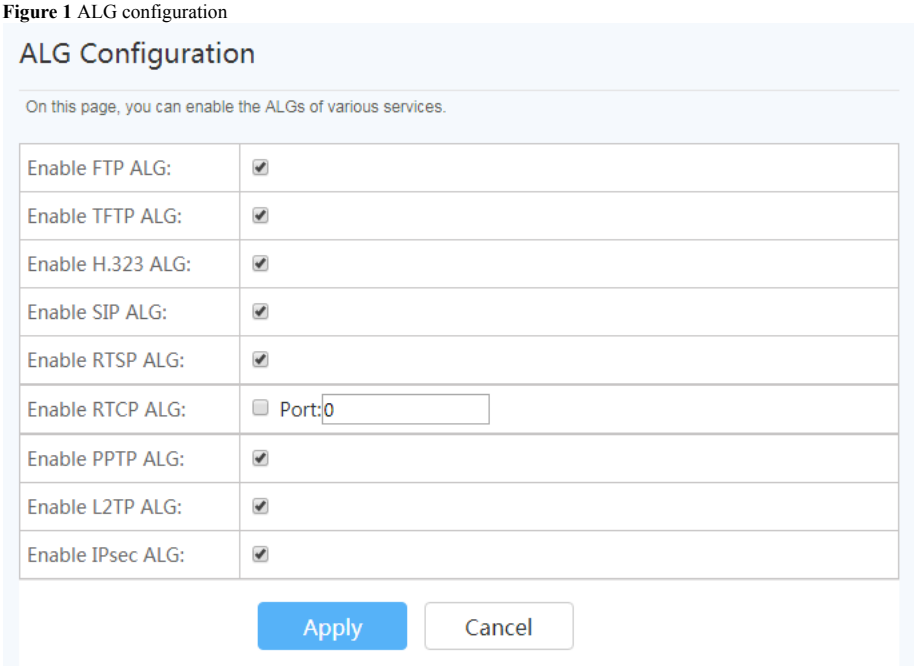
Parent Topic: Application

< Previous topic Next topic >

1.6.6.6 ALG Configuration

1. In the navigation tree on the left, choose **Advanced Configuration** > **Application** > **ALG Configuration**. In the pane on the right, you can determine whether to enable the FTP or TFTP, as shown in Figure 1.

Figure 1 ALG configuration



2. Click **Apply**.

NOTE:
When the NAT function is enabled, the application level gateway (ALG) function needs to be enabled to ensure that some application software and hardware can be normally used.

Parent Topic: Application

< Previous topic Next topic >

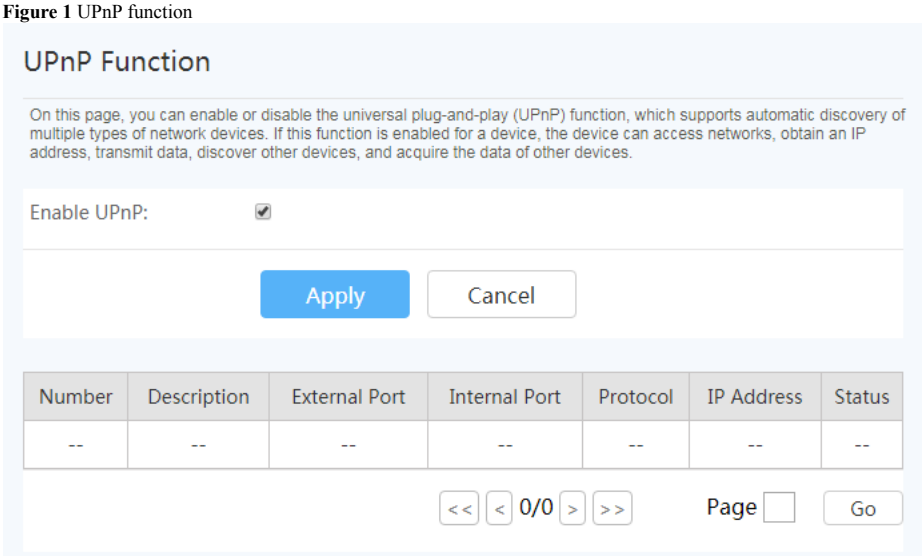
1.6.6.7 UPnP Function

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 DSL home gateway, 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 DSL home gateway through the UPnP protocol, thus improving the running speed.

1. In the navigation tree on the left, choose **Advanced Configuration** > **Application** > **UPnP Function**. In the pane on the right, you can determine whether to enable the UPnP, as shown in Figure 1.

Figure 1 UPnP function



2. Click **Apply**.

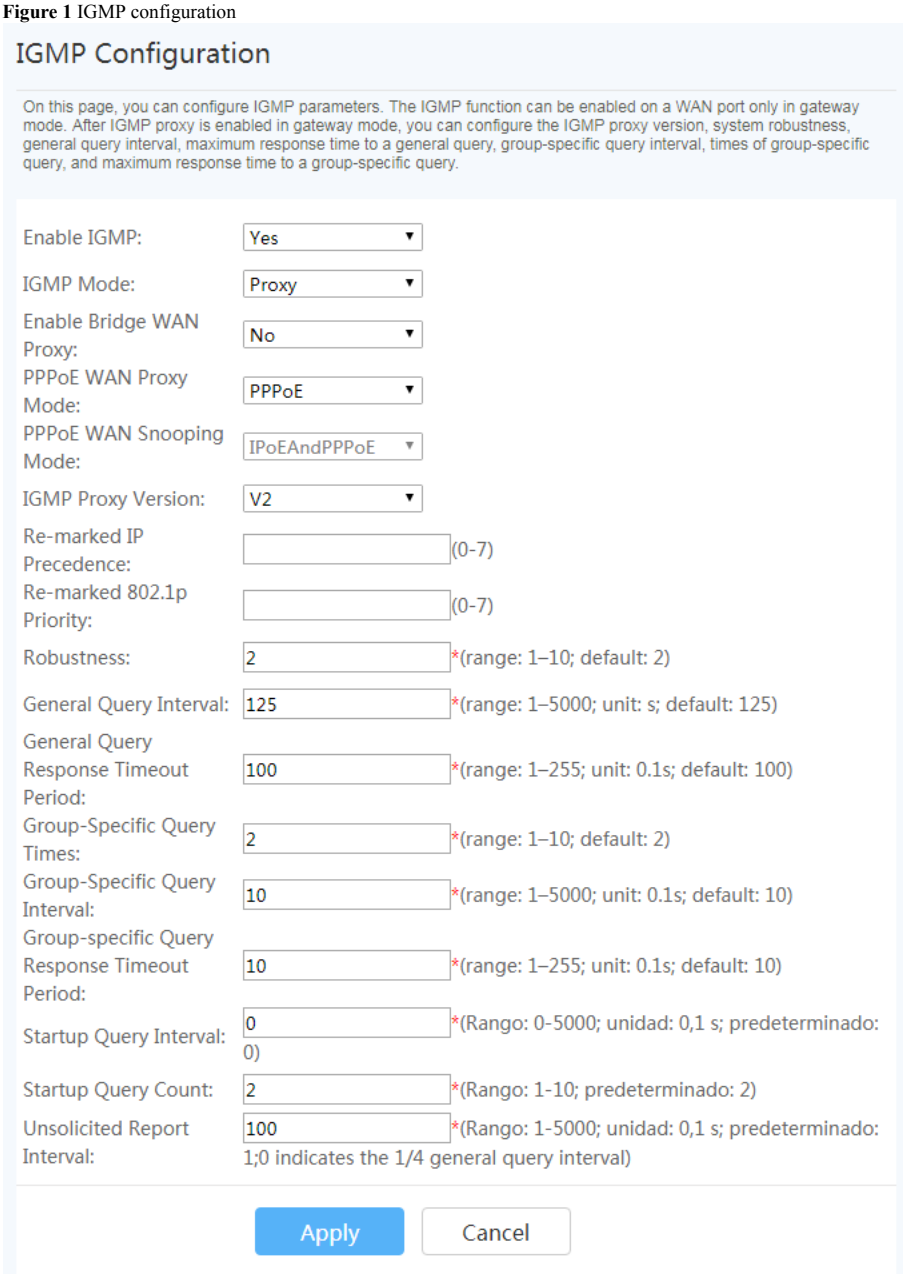
Parent Topic: Application

< Previous topic Next topic >

1.6.6.8 IGMP Configuration

1. In the navigation tree on the left, choose **Advanced Configuration** > **Application** > **IGMP Configuration**. In the pane on the right, you can configure the IGMP parameters, as shown in Figure 1.

Figure 1 IGMP configuration



2. Click **Apply**.

NOTE:
The IGMP function of WAN ports can be enabled only when IGMP works in the gateway mode. Only when **IGMP Mode** is **Proxy**, parameters such as **Robustness**, **General Query Interval**, **General Query Response Timeout Period**, **Group-Specific Query Times**, **Group-Specific Query Interval**, and **Group-specific Query Response Timeout Period** can be configured.

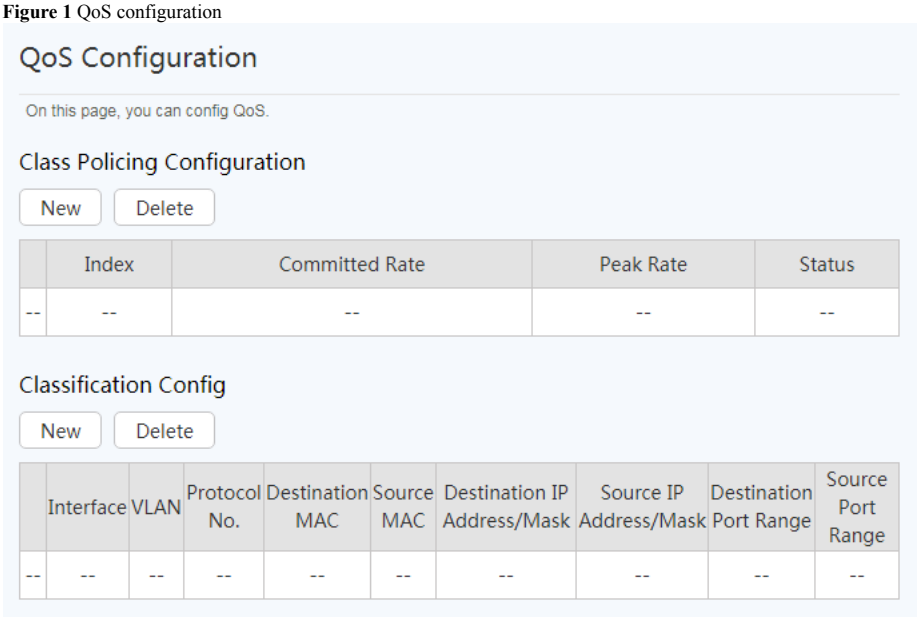
Parent Topic: Application

< Previous topic Next topic >

1.6.6.9 QoS Configuration

1. In the navigation tree on the left, choose **Advanced Configuration** > **Application** > **QoS Configuration**. In the pane on the right, you can configure the QoS parameters, as shown in Figure 1

Figure 1 QoS configuration



2. Click **Apply**.

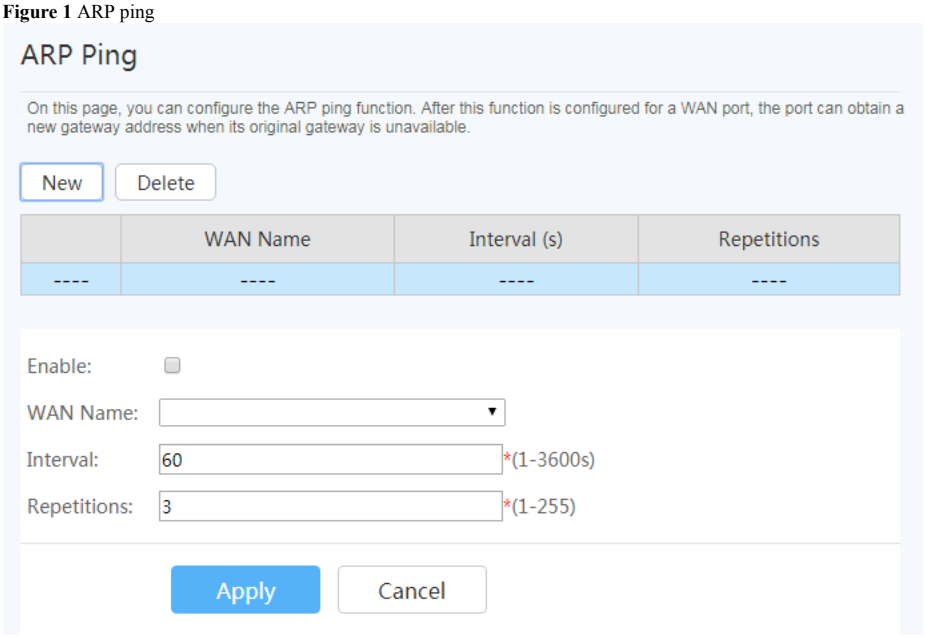
Parent Topic: Application

< Previous topic Next topic >

1.6.6.10 ARP Ping

1. In the navigation tree on the left, choose **Advanced Configuration** > **Application** > **ARP Ping**. In the pane on the right, click **New**. In the dialog box that is displayed, you can configure the ARP ping parameters, as shown in Figure 1

Figure 1 ARP ping



2. Click **Apply**.

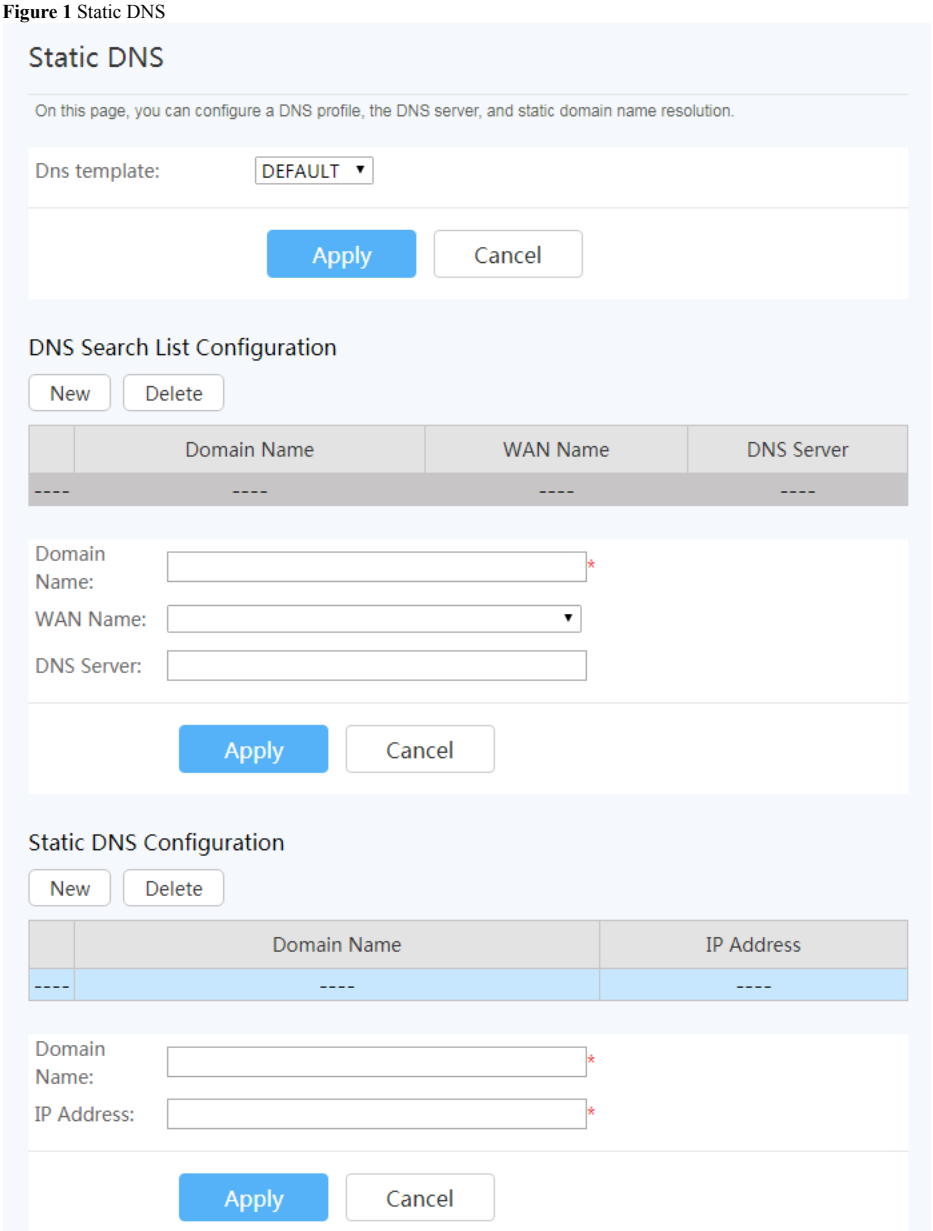
Parent Topic: Application

< Previous topic Next topic >

1.6.6.11 Static DNS

1. In the navigation tree on the left, choose **Advanced Configuration** > **Application** > **Static DNS**. In the pane on the right, click **New**. In the dialog box that is displayed, you can configure the DNS parameters, as shown in Figure 1.

Figure 1 Static DNS



2. Click **Apply**.

Parent Topic: Application

< Previous topic

1.6.7 WLAN

This topic describes how to perform 2.4G&5G basic and advanced configurations of the WLAN through the web page.

- 2.4G Basic Network Settings
- 2.4G Advanced Network Settings
- 5G Basic Network Settings
- 5G Advanced Network Settings
- Automatic WiFi Shutdown
- WiFi Coverage Management

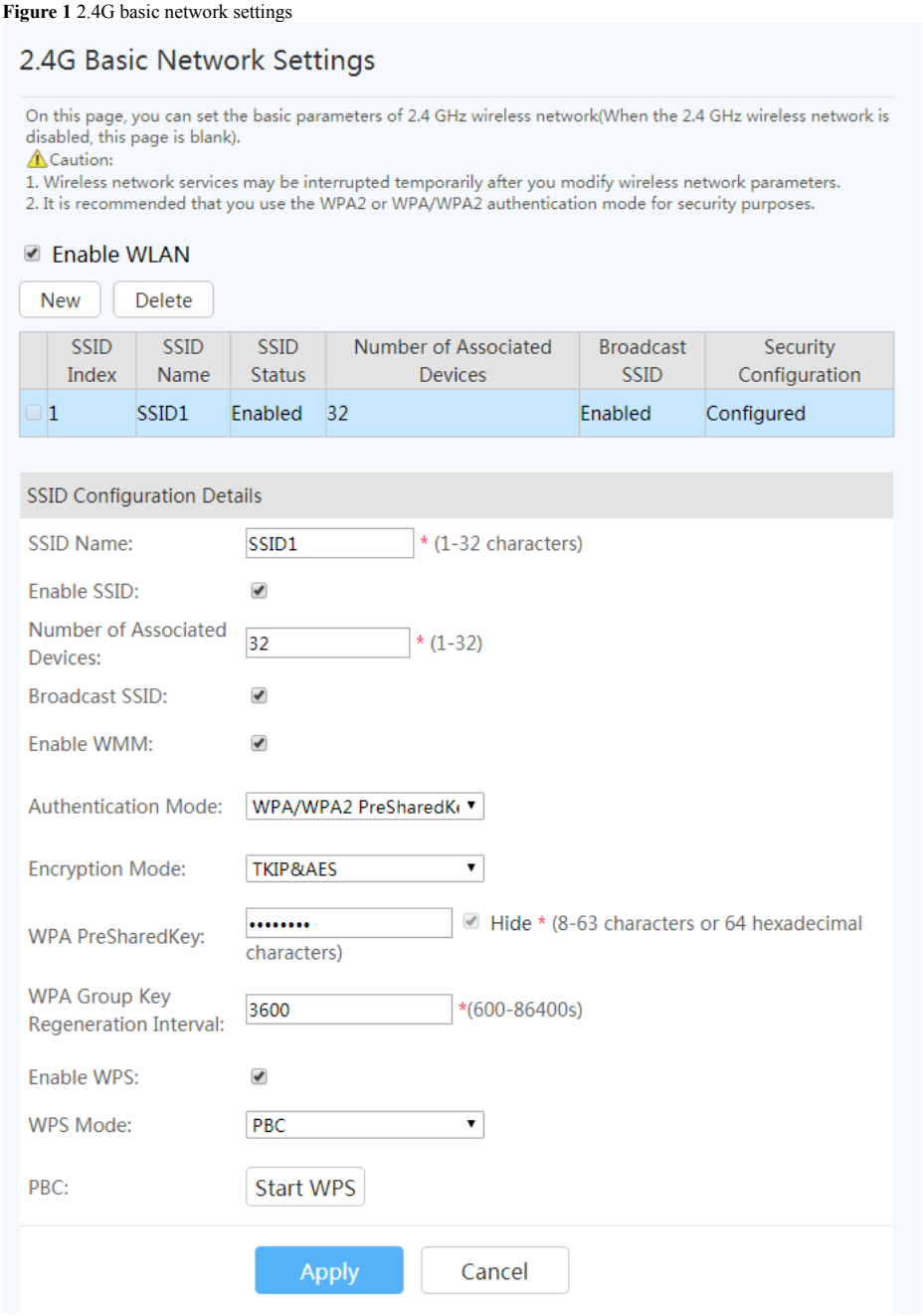
Parent Topic: Advanced Configuration

< Previous topic Next topic >

1.6.7.1 2.4G Basic Network Settings

1. In the navigation tree on the left, choose **Advanced Configuration** > **WLAN** > **2.4G Basic Network Settings**. In the pane on the right, you can configure the basic parameters of the 2.4G Wi-Fi network, as shown in Figure 1.

Figure 1 2.4G basic network settings



2. Click **Apply**.

Table 1 describes the basic parameters of the 2.4G Wi-Fi network.

Table 1 Basic wireless network configurations

Parameter	Description
Enable WLAN	Indicates whether to enable the wireless network. The following parameters can be set only when the wireless network is enabled.
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 Tab character. A default SSID1 is created after the creation of a DSL home gateway. The system cannot assign IP addresses to Wi-Fi terminals by SSID.
Enable SSID	Specifies whether to enable the connection.
Number of Associated Devices	Specifies the number of STAs. It ranges from 1 to 32.

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 DSL home gateway 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.
Enable WMM	Specifies whether to enable Wi-Fi multimedia.
Authentication Mode	Indicates the authentication mode for the STA to request access to the wireless network. It is set to **WPA/WPA2 PreSharedKey** for SSID1 by default. However, for the newly-created SSID, the default authentication mode is **Open**. That is, the wireless terminal can access the wireless network without authentication.
Encryption Mode	Indicates the encryption mode for the STA to request access to the wireless network. The encryption mode and encryption parameters vary with the authentication mode. • If the authentication mode is set to **Open**, the encryption mode can be set to **None** or **WEP**. • If the authentication mode is set to **Shared**, the encryption is **WEP**. • If the authentication mode is set to **WPA PreSharedKey**, **WPA2 PreSharedKey**, **WPA/WPA2 PreSharedKey**, **WPA Enterprise**, **WPA2 Enterprise** or **WPA/WPA2 Enterprise**, the encryption mode can be set to **AES**, **TKIP**, or **TKIP&AES**.
WPA PreSharedKey	Indicates the pre-shared key (that is, the key for the wireless connection).
WPA Group Key Regeneration Interval	Indicates the regeneration interval of group keys. Group keys are used for multicast and broadcast communication.
Enable WPS	Indicates whether to enable the WPS. This parameter needs to be set only when **Authentication Mode** is set to **WPA2 PreSharedKey** or **WPA/WPA2 PreSharedKey**.
WPS Mode	Indicates the WPS mode. It can be set to **PBC**, **PIN** or **AP-PIN**. This parameter needs to be set only when **Authentication Mode** is set to **WPA2 PreSharedKey** or **WPA/WPA2 PreSharedKey**.
PBC	You can click **Start WPS** to start the WPS. This parameter needs to be set only when **WPS Mode** is set to **PBC**.
PIN	Indicates the PIN. This parameter needs to be set only when **WPS Mode** is set to **PIN**.
AP-PIN	You can click **Regenerate PIN** or **Reset PIN** to get a PIN. This parameter needs to be set only when **WPS Mode** is set to **AP-PIN**.

NOTE:

- The security mode and encryption configured on a Wi-Fi terminal must be the same as those of a DSL home gateway. If the TKIP&AES, or AES encryption mode is not configured on the Wi-Fi terminal, the Wi-Fi terminal may have an old-version driver. If so, update the driver version.
- When two SSIDs are configured, if you modify the information of an SSID, the other SSID will re-choose a channel, causing the service to be interrupted for a few minutes.

Parent Topic: WLAN

Next topic >

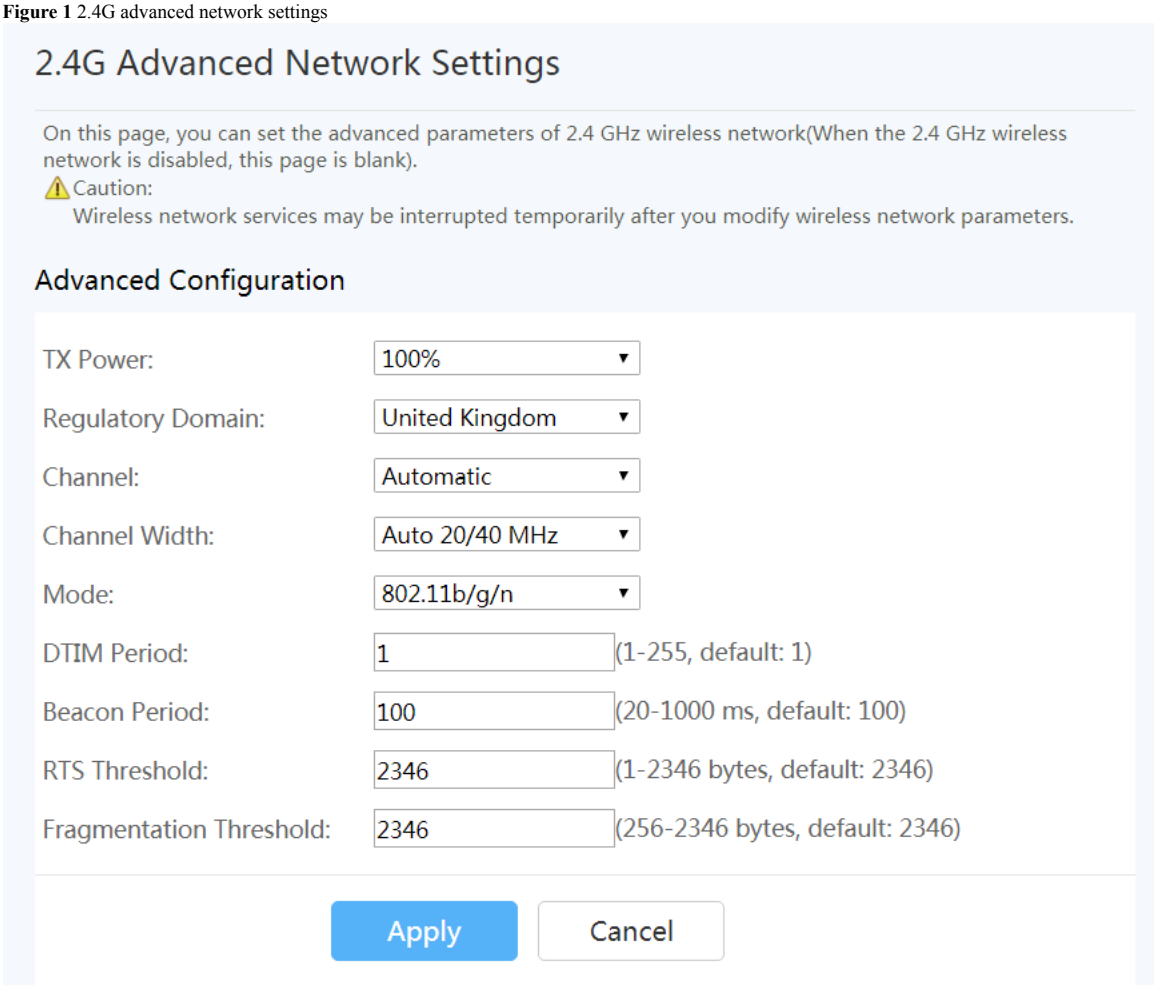
1.6.7.2 2.4G Advanced Network Settings

1. In the navigation tree on the left, choose **Advanced Configuration** > **WLAN** > **2.4G Advanced Network Settings**. In the pane on the right, you can configure the advanced parameters of the 2.4G Wi-Fi network, as shown in Figure 1.

   NOTE:

   This page is empty if **Enable WLAN** is not selected in **2.4G Basic Network Settings**.

Figure 1 2.4G advanced network settings



2. Click **Apply**.

Table 1 describes the Wi-Fi parameters of the 2.4G Wi-Fi network.

Table 1 Wireless network advanced parameters

Parameter	Description
TX Power	Indicates the transmit optical power of wireless signals. It can be set to **20%**, **40%**, **60%**, **80%**, or **100%**. The larger the value, the better the coverage of wireless signals.
Regulatory Domain	Indicates the regulatory domain.
Channel	Indicates the channel of the wireless network.
Channel Width	Indicates the wireless channel width. It can be set to **Auto 20/40 MHz**, **20 MHz** or **40 MHz**.
Mode	Indicates the supported wireless network mode. It can be set to **802.11b**, **802.11g**, **802.11b/g**, or **802.11b/g/n**.
DTIM Period	Indicates the delivery period of the delivery traffic indication map (DTIM). The value ranges from 1 to 255, and the default value is 1.
Beacon Period	Indicates the delivery period of the beacon. The beacon is used to contact other access point devices or network control devices. The value ranges from 20 ms to 1000 ms, and the default value is 100 ms.
RTS Threshold	Indicates the request to send (RTS) threshold. It is used to avoid conflicts in data transmission in the wireless LAN. The smaller the RTS threshold, the higher the transmission frequency of RTS packets, and the faster of the system recovers from an interruption or conflict. However, more bandwidths are used, which affects the throughput of other network data packets. The value ranges from 1 bytes to 2346 bytes, and the default value is 2346 bytes.
Fragmentation Threshold	Indicates the fragment threshold. When the size of a packet is greater than this threshold, the packet will be fragmented. If the transmission of fragments is interrupted, only the parts that are not successfully transmitted need to be retransmitted. The value ranges from 256 bytes to 2346 bytes, and the default value is 2346 bytes.

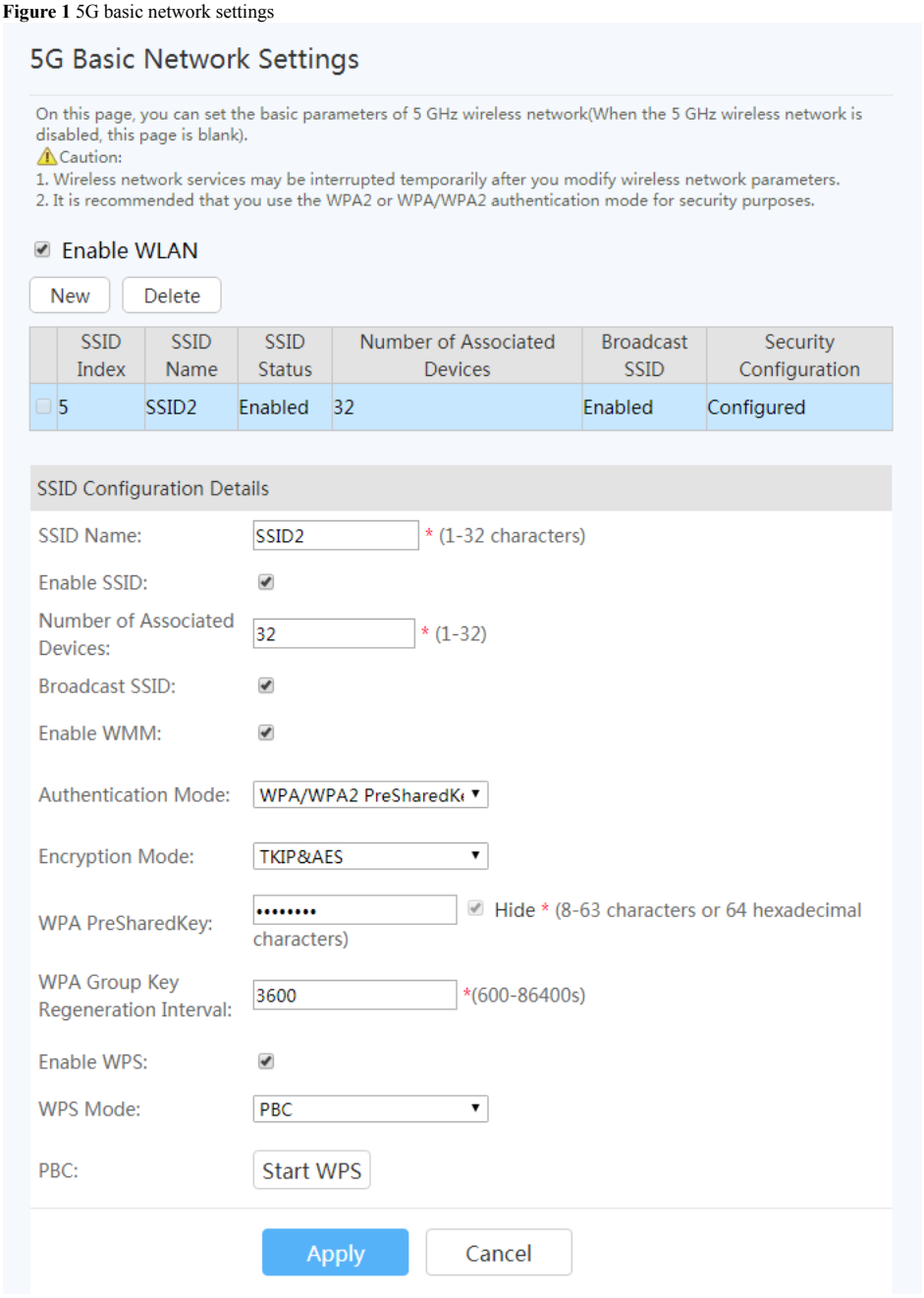
Parent Topic: WLAN

< Previous topic Next topic >

1.6.7.3 5G Basic Network Settings

1. In the navigation tree on the left, choose **Advanced Configuration** > **WLAN** > **5G Basic Network Settings**. In the pane on the right, you can configure the basic parameters of the 5G Wi-Fi network, as shown in Figure 1.

Figure 1 5G basic network settings



2. Click **Apply**.

Table 1 describes the basic parameters of the 5G Wi-Fi network.

Table 1 Basic wireless network configurations

Parameter	Description
Enable WLAN	Indicates whether to enable the wireless network. The following parameters can be set only when the wireless network is enabled.
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 Tab character. A default SSID5 is created after the creation of a DSL home gateway. The system cannot assign IP addresses to Wi-Fi terminals by SSID.
Enable SSID	Specifies whether to enable the connection.
Number of Associated Devices	Specifies the number of STAs. It ranges from 1 to 32.

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 DSL home gateway 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.
Enable WMM	Specifies whether to enable Wi-Fi multimedia.
Authentication Mode	Indicates the authentication mode for the STA to request access to the wireless network. It is set to **WPA/WPA2 PreSharedKey** for SSID5 by default. However, for the newly-created SSID, the default authentication mode is **Open**. That is, the wireless terminal can access the wireless network without authentication.
Encryption Mode	Indicates the encryption mode for the STA to request access to the wireless network. The encryption mode and encryption parameters vary with the authentication mode. • If the authentication mode is set to **Open**, the encryption mode can be set to **None**. • If the authentication mode is set to **WPA PreSharedKey**, **WPA2 PreSharedKey**, **WPA/WPA2 PreSharedKey**, **WPA Enterprise**, **WPA2 Enterprise** or **WPA/WPA2 Enterprise**, the encryption mode can be set to **AES**, **TKIP**, or **TKIP&AES**.
WPA PreSharedKey	Indicates the pre-shared key (that is, the key for the wireless connection).
WPA Group Key Regeneration Interval	Indicates the regeneration interval of group keys. Group keys are used for multicast and broadcast communication.
Enable WPS	Indicates whether to enable the WPS. This parameter needs to be set only when **Authentication Mode** is set to **WPA2 PreSharedKey** or **WPA/WPA2 PreSharedKey**.
WPS Mode	Indicates the WPS mode. It can be set to **PBC**, **PIN** or **AP-PIN**. This parameter needs to be set only when **Authentication Mode** is set to **WPA2 PreSharedKey** or **WPA/WPA2 PreSharedKey**.
PBC	You can click **Start WPS** to start the WPS. This parameter needs to be set only when **WPS Mode** is set to **PBC**.
PIN	Indicates the PIN. This parameter needs to be set only when **WPS Mode** is set to **PIN**.
AP-PIN	You can click **Regenerate PIN** or **Reset PIN** to get a PIN. This parameter needs to be set only when **WPS Mode** is set to **AP-PIN**.

NOTE:

- The security mode and encryption configured on a Wi-Fi terminal must be the same as those of a DSL home gateway. If the TKIP&AES, or AES encryption mode is not configured on the Wi-Fi terminal, the Wi-Fi terminal may have an old-version driver. If so, update the driver version.
- When two SSIDs are configured, if you modify the information of an SSID, the other SSID will re-choose a channel, causing the service to be interrupted for a few minutes.

Parent Topic: WLAN

< Previous topic Next topic >

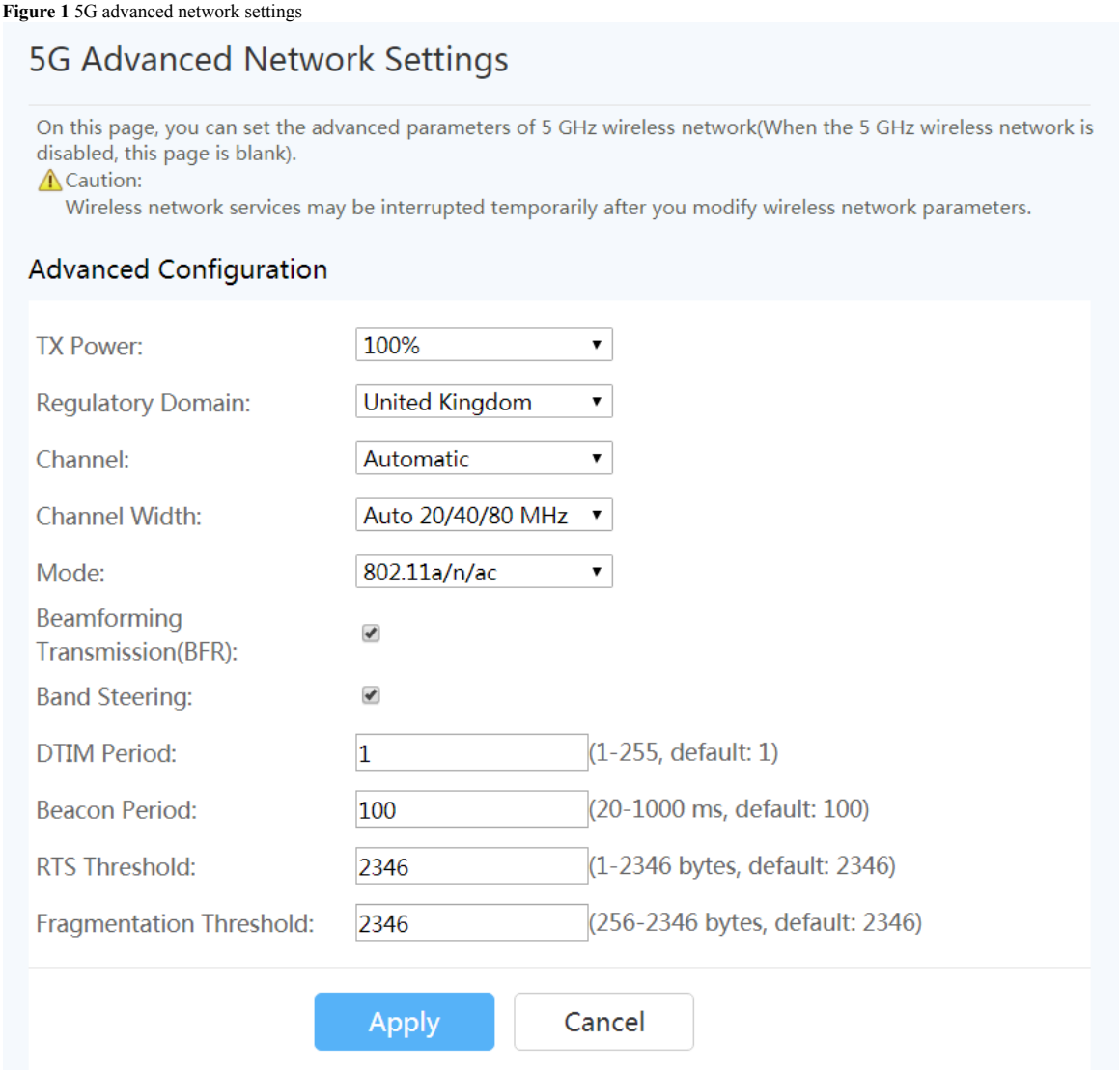
1.6.7.4 5G Advanced Network Settings

1. In the navigation tree on the left, choose **Advanced Configuration** > **WLAN** > **5G Advanced Network Settings**. In the pane on the right, you can configure the basic parameters of the 5G Wi-Fi network, as shown in Figure 1.

NOTE:

This page is empty if **Enable WLAN** is not selected in **5G Basic Network Settings**.

Figure 1 5G advanced network settings



2. Click **Apply**.

Table 1 describes the Wi-Fi parameters of the 5G Wi-Fi network.

Table 1 Wireless network advance parameters

Parameter	Description
TX Power	Indicates the transmit optical power of wireless signals. It can be set to **20%**, **40%**, **60%**, **80%**, or **100%**. The larger the value, the better the coverage of wireless signals.
Regulatory Domain	Indicates the regulatory domain.
Channel	Indicates the channel of the wireless network.
Channel Width	Indicates the wireless channel width. It can be set to **Auto 20/40/80 MHz**, **Auto 20/40 MHz**, **20 MHz** or **40 MHz**.
Mode	Indicates the supported wireless network mode. It can be set to **802.11a**, **802.11a/n**, or **802.11a/n/ac**.
Beamingforming Transmission(BFR)	Specifies whether to enable the beamingforming transmission(BFR).
Band Steering	Specifies whether to enable the band steering.
MU-MIMO	Specifies whether to enable multi-user multiple-input multiple-output.
DTIM Period	Indicates the delivery period of the delivery traffic indication map (DTIM). The value ranges from 1 to 255, and the default value is 1.
Beacon Period	Indicates the delivery period of the beacon. The beacon is used to contact other access point devices or network control devices. The value ranges from 20 ms to 1000 ms, and the default value is 100 ms.
RTS Threshold	Indicates the request to send (RTS) threshold. It is used to avoid conflicts in data transmission in the wireless LAN. The smaller the RTS threshold, the higher the transmission frequency of RTS packets, and the faster of the system recovers from an interruption or conflict. However, more bandwidths are used, which affects the throughput of other network data packets. The value ranges from 1 bytes to 2346 bytes, and the default value is 2346 bytes.

Parameter	Description
Fragmentation Threshold	Indicates the fragment threshold. When the size of a packet is greater than this threshold, the packet will be fragmented. If the transmission of fragments is interrupted, only the parts that are not successfully transmitted need to be retransmitted. The value ranges from 256 bytes to 2346 bytes, and the default value is 2346 bytes.

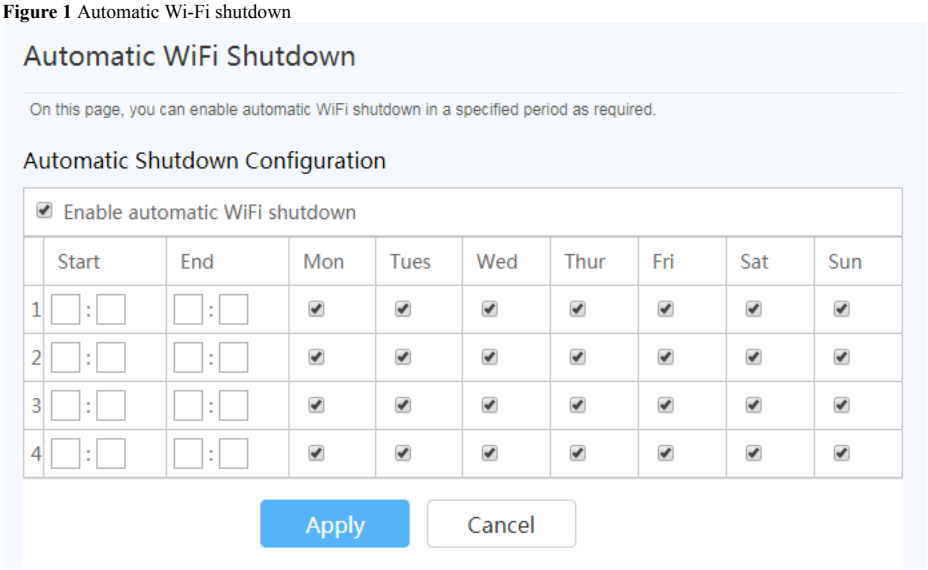
Parent Topic: WLAN

< Previous topic Next topic >

1.6.7.5 Automatic WiFi Shutdown

1. In the navigation tree on the left, choose **Advanced Configuration** > **WLAN** > **Automatic WiFi Shutdown**. In the pane on the right, select **Enable automatic WiFi shutdown**. In the dialog box that is displayed, you can configure the scheduled Wi-Fi shutdown time segment, to enable the WiFi network to be automatically shut down when the Wi-Fi network is not in use, as shown in Figure 1.

Figure 1 Automatic Wi-Fi shutdown



2. Click **Apply**.

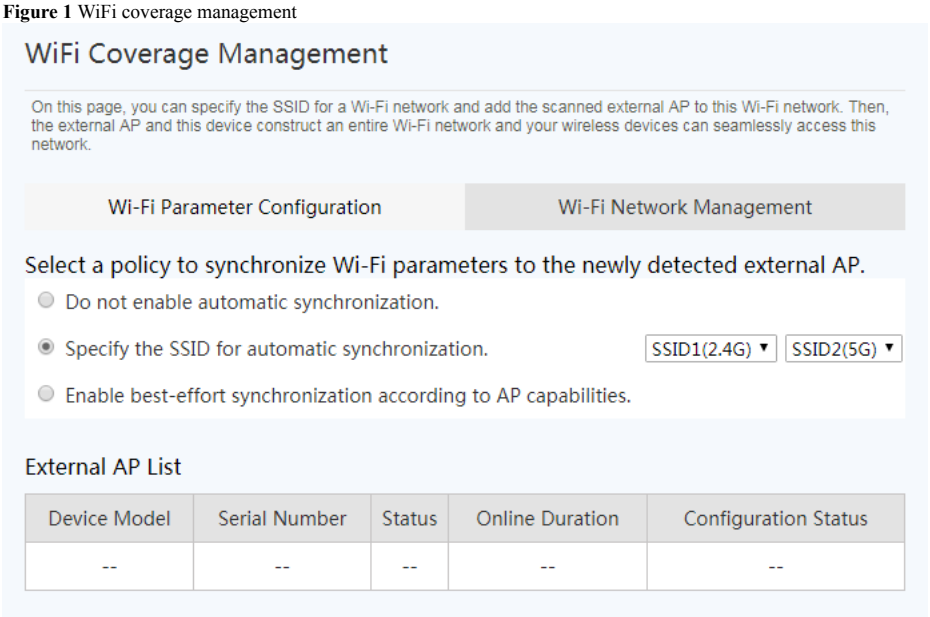
Parent Topic: WLAN

< Previous topic Next topic >

1.6.7.6 WiFi Coverage Management

In the navigation tree on the left, choose **Advanced Configuration** > **WLAN** > **WiFi Coverage Management**. In the pane on the right, you can configure the WiFi coverage, as shown in Figure 1.

Figure 1 WiFi coverage management



Parent Topic: WLAN

< Previous topic

1.6.8 Voice

This topic describes how to configure the voice service through the web page.

NOTE:

The web page for configuring the voice service varies with the voice protocols. The following topics describe the web page after the SIP protocol is loaded.

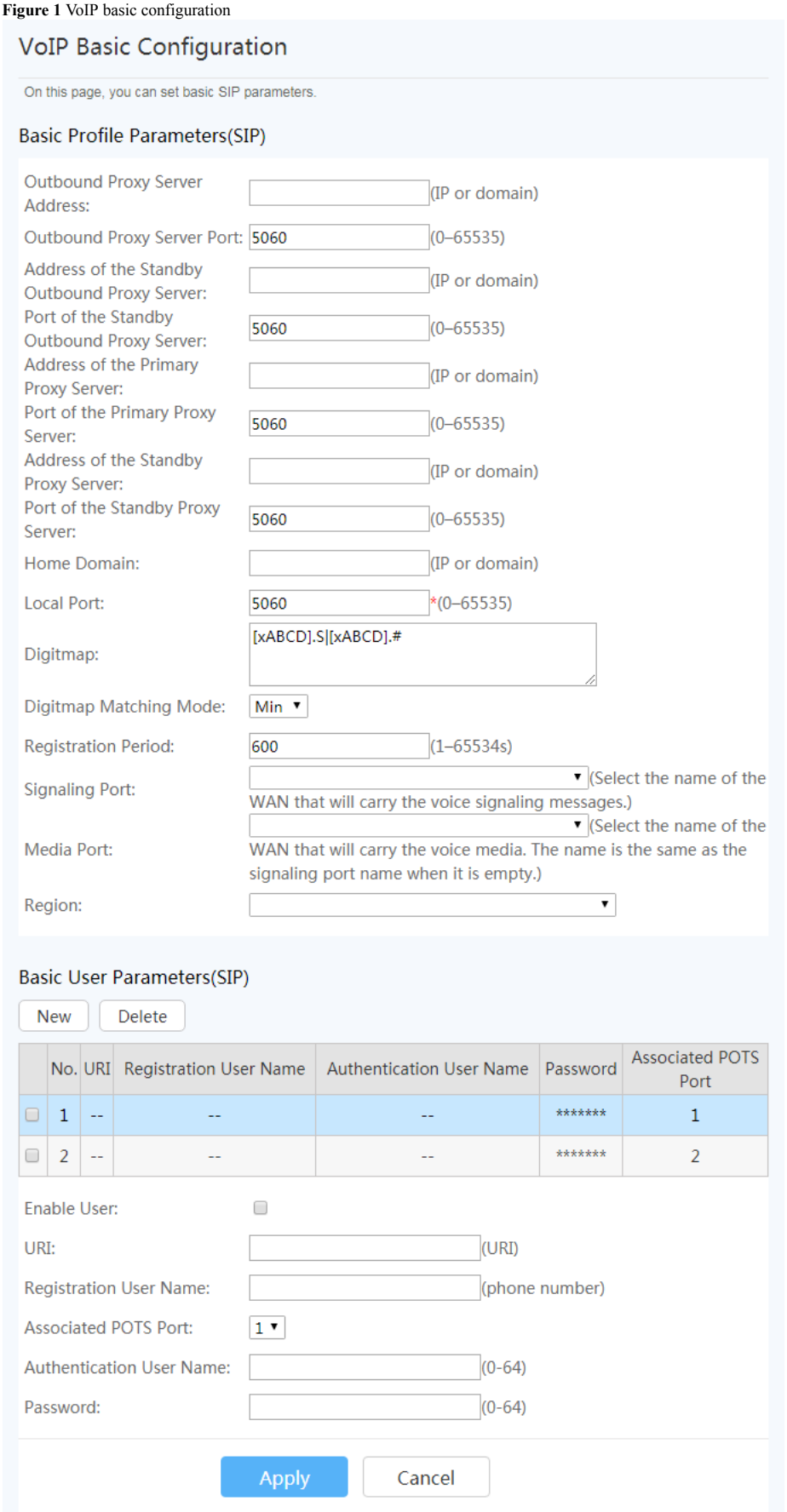
Parent Topic: Advanced Configuration

< Previous topic Next topic >

1.6.8.1 VoIP Basic Configuration

1. In the navigation tree on the left, choose **Advanced Configuration** > **Voice** > **VoIP Basic Configuration**. In the pane on the right, you can configure the VoIP basic parameters, as shown in Figure 1.

Figure 1 VoIP basic configuration



2. Click **Apply**.

Table 1 describes the basic parameters used for configuring a VoIP.

Table 1 Basic parameters used for configuring a VoIP

Parameter	Description

Parameter	Description
Basic Profile Parameters(SIP)	
Outbound Proxy Server Address	Indicates the IP address (provided by the ISP) of the primary SIP outbound server. This server IP address overrides the primary server IP address. Specifically, when IP addresses of both the primary outbound server and the primary server are configured, the primary server IP address does not take effect.
Outbound Proxy Server Port	Indicates the ID (provided by the ISP) of the port used for communication between the primary SIP outbound server and the VoIP terminal. The ID ranges from 0 to 65535 and the default ID is 5060.
Address of the Standby Outbound Proxy Server	Indicates the IP address (provided by the ISP) of the secondary SIP outbound server.
Port of the Standby Outbound Proxy Server	Indicates the ID (provided by the ISP) of the port used for communication between the secondary SIP outbound server and the VoIP terminal. The ID ranges from 0 to 65535 and the default ID is 5060.
Address of the Primary Proxy Server	Indicates the IP address (provided by the ISP) of the primary SIP proxy server.
Port of the Primary Proxy Server	Indicates the ID (provided by the ISP) of the port used for communication between the primary SIP proxy server and the VoIP terminal. The ID ranges from 0 to 65535 and the default ID is 5060.
Address of the Standby Proxy Server	Indicates the IP address (provided by the ISP) of the secondary SIP proxy server.
Port of the Standby Proxy Server	Indicates the ID (provided by the ISP) of the port used for communication between the secondary SIP proxy server and the VoIP terminal. The ID ranges from 0 to 65535 and the default ID is 5060.
Home Domain	Indicates the domain of the registration server of the VoIP terminal in network communications, such as softx3000.huawei.com.
Local Port	Indicates the ID of the local port on the DSL home gateway. The ID ranges from 0 to 65535 and the default ID is 5060.
Digitmap	Indicates the voice digitmap.
Digitmap Matching Mode	Indicates the digitmap matching mode, including Min and Max. • Min: If the dialed character string matches a digitmap scheme, the system immediately reports the number to the call proxy. • Max: If the dialed character string matches a digitmap scheme, the system does not immediately report the number to the call proxy but starts the short timer. If a user does not continue dialing digits, the system reports the number to the call proxy after the short timer times out; if the user continues dialing digits and the number matches the long digitmap, the system reports the number that matches the digitmap to the call proxy.
Registration Period	Indicates the valid registration period. When this period expires, the SIP user needs to register again. The value range is 1s to 65534s, and the default value is 600s.
Signaling Port	Indicates the signaling WAN port used for connecting the VoIP terminal to the SIP server.
Media Port	Indicates the media streams WAN port used for connecting the VoIP terminal to the SIP server.
Region	Indicates the country code.
Basic User Parameters(SIP)	
Enable User	Enables or disables a SIP user. The SIP user starts the registration only after being enabled.
URI	Indicates the SIP user identifier. It uniquely identifies a SIP user and the value must be the same as the configuration on the IMS.
Registration User Name	Indicates the name used for SIP user registration. It is generally the user phone number.
Associated POTS Port	Indicates the POTS port associated with the SIP user.
Authentication User Name	Indicates the user name used for authentication on the IMS. It must be the same as the configuration on the IMS.
Password	Indicates the password used for authentication on the IMS. It must be the same as the configuration on the IMS.

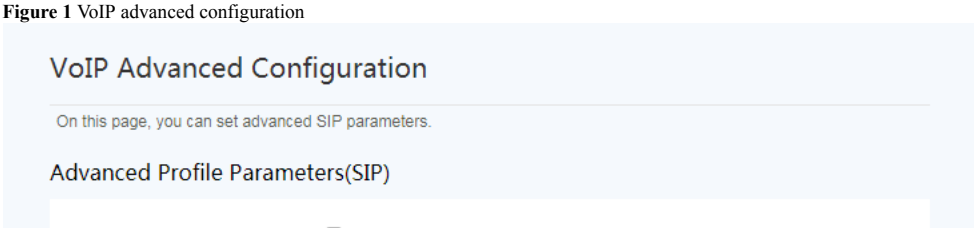
Parent Topic: Voice

Next topic >

1.6.8.2 VoIP Advanced Configuration

1. In the navigation tree on the left, choose **Advanced Configuration** > **Voice** > **VoIP Advanced Configuration**. In the pane on the right, you can configure the VoIP advanced parameters, as shown in Figure 1.

Figure 1 VoIP advanced configuration



Enable Echo Cancellation: ☑

Enable Subscribe: ☐

Silence detection: ☐

Silence compression mode: Codec

Fax Transmode: pass-through

Fax Switch Mode: Negotiation

Profile Parameters: 1=2;2=1;3=1;4=0;5=0;6=0;7=1;8=600;9=1;10=0;11=0;12=0;13=1;14=1;15=0;16=0;17=0;18=0;19=0;20=1;21=0;22=0;23=64;24=60;2

Software Parameters: Default

Digitmap Short Timer: 5 (unit:s)

Digitmap Long Timer: 10 (unit:s)

Shared User Mode: Disabled

Multihoming Mode: Dual homing(automatic switchback

DTMF Transmission Mode: Transparent Transmissio

RFC2833 Payload Type: 97 (96-127)

Voice Server Type: IMS SIP Server

Offhook DT-AS ACK Interval: 160 (unit:ms)(0-1000)

Option 120 Priority: Highest

DSP Template Parameters

New Delete

	No.	Remote Telephone Number	DSP Template
--	--	--	--

Advanced User Parameters(SIP)

No.	URI	Registration User Name	Authentication User Name	Associated POTS Port
1	--	--	--	1
2	--	--	--	2

Codec	Packet Time (ms)	Priority	Enable	Silence compression
G.711MuLaw	20	2 (1-100)	☑	☐
G.711ALaw	20	1 (1-100)	☑	☐
G.729	20	3 (1-100)	☑	☐
G.722	20	4 (1-100)	☑	☐

DSP TX Gain: 0 (Value range: -100 to 50 in the unit of 0.1 db)

DSP RX Gain: 0 (Value range: -100 to 100 in the unit of 0.1 db)

Enable Hotline: ☐

Hotline Number: (0-32)

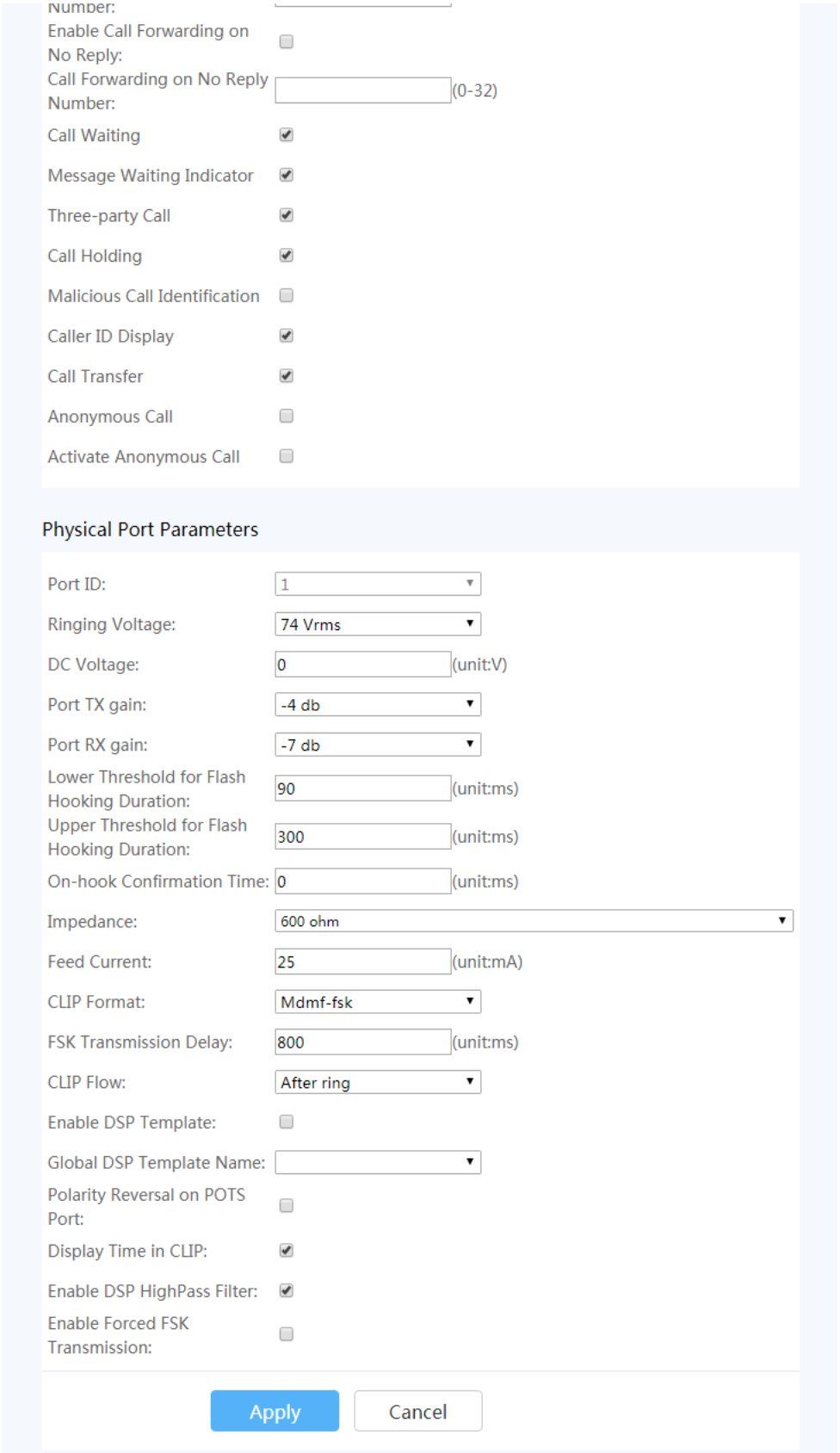
Hotline Delay: 5 (unit:s)(0-255)

Enable Call Forwarding Unconditional: ☐

Call Forwarding Unconditional Number: (0-32)

Enable Call Forwarding Busy: ☐

Call Forwarding Busy Number: (0-32)



2. Click **Apply**.

Table 1 describes the advanced parameters used for configuring a VoIP.

Table 1 Advanced parameters used for configuring a VoIP

Parameter	Description
Advanced Profile Parameters(SIP)	

Parameter	Description
Enable Echo Cancellation	Enables or disables echo cancellation. By default, echo cancellation is enabled.
Enable Subscribe	Enables or disables subscription of user rights. When the server type is NGN SIP, this function is disabled.
Silence detection	Enables or disables the silence detection.
Silence compression mode	Indicates the silence compression mode, including **Global** and **Codec**.
Fax Transmode	Indicates the fax mode, including **pass-through** and **T.38**. • pass-through: The MG encodes the fax signals transmitted by a fax machine according to the voice codec (G.711), and then coverts such signals into the RTP data packets for real-time transmission over an IP network. • T.38: The MG, through ITU-T T.38, converts the T.30-compliant fax signals transmitted by a fax machine into the T.38 packets for transmission over an IP bearer network.
Fax Switch Mode	Indicates the fax switching mode, including **Negotiation** and **Self-switch**. The fax switching mode is selected according to the customer requirements.
Profile Parameters	Indicates the control point parameters. Such parameters are selected according to the softswitch. Generally, the default settings are adopted.
Software Parameters	Indicates the software parameters. Such parameters are selected according to the softswitch. Generally, the default settings are adopted.
Digitmap Short Timer	Indicates the short timer of the digitmap. This timer starts up if a number that matches digitmap A is dialed and then matches digitmap B.
Digitmap Long Timer	Indicates the long timer of the digitmap. This timer starts up if the dialed digits comply with the dialing scheme but one more digit is required.
Shared User Mode	Specifies whether to bind telephone numbers to phone ports. • Disabled: The shared user mode is disabled. • Parallel ringing: If this option is selected, only one telephone number can be configured. That is, all phone ports on the DSL home gateway share a telephone number. All telephones ring together when an incoming call is made. If two telephone numbers are configured, this option is invalid.
Multihoming Mode	The multi-homing mode supports multiple IP addresses for one end point. That is, one end point can use multiple physical network ports. This improves the end point reliability. If this mode is enabled, two servers (active/standby) must be configured. • Disabled: The multi-homing mode is disabled. • Dual homing(not automatic switchback): Once an DSL home gateway is registered with a softswitch (no matter active or standby), the softswitch is always used as long as it works correctly. • Dual homing(automatic switchback): The DSL home gateway switches back to the active softswitch when detecting that the active softswitch recovers and is reachable. • Load sharing: The DSL home gateway is registered with one of the addresses resolved from the domain name to ensure that multiple softswitches process services in load sharing mode.
DTMF Transmission Mode	Specifies the DTMF signal transmission mode. DTMF signals can be transmitted transparently, in SIPInfo or RFC2833 packets.
RFC2833 Payload Type	Specifies the payload value used for transmit DTMF signals in RFC2833 packets. It ranges from 96 to 127.
Voice Server Type	Indicates the supported voice server type. • IMS SIP Server: core network service type based on the SIP protocol. • NGN SIP Server: NGN service type based on the SIP protocol.
Offhook DT-AS ACK Interval	Indicates the time during which the DT-AS signal (detects whether a phone supports offhook CLIP) waits for a response from the phone.
Option 120 Priority	Indicates the option 120 priority. It can be set to **Ignore**, **Highest**, or **Lowest**.
Advanced User Parameters(SIP)	
Codec	Indicates encoding/decoding. In encoding, the DSP encodes TDM voice data into packets and sends the packets to the IP network. In decoding, the DSP decodes the voice packets received from the network and sends the data to the TDM side. Four types of codec are supported: **G.711MuLaw**, **G.711ALaw**, **G.729**, and **G.722**; but the codec cannot be configured.
Packet Time	Indicates the interval at which the DSP assembles voice packets. Different encoding modes support different packetization periods. The period can be **10 ms**, **20 ms**, or **30 ms**, and the default period is **20 ms**.
Priority	Indicates the codec priority. Two users negotiate the priority in descending order. Currently, priorities 1-4 are supported, with 1 being the highest priority.
Enable	Indicates whether the user carries the codec (enable: carry; disable: not carry).
Silence compression	Enables or disables the silence compression.
DSP TX Gain	Indicates the direction in which gain takes effect: from the local POTS side to the remote IP side.

Parameter	Description
DSP RX Gain	Indicates the direction in which gain takes effect: from the remote IP side to the local POTS side.
Enabled Hotline	Enables or disables the hotline function.
Hotline Number	Indicates the hotline number. After the user specifies a number as the hotline number and also enables the hotline function, the number is automatically dialed if the user does not dial the number following a delay time expiration after offhook.
Hotline Delay	Indicates the period over which the user does not dial the number after offhook.
Enable Call Forwarding Unconditional	Enables the call forwarding unconditional (CFU) function. A called party-side service, with which, a user can unconditionally forward all incoming calls to a designated forwarded-to number or a voice mailbox.
Call Forwarding Unconditional Number	Indicates the forwarded-to number.
Enable Call Forwarding Busy	Enables the call forwarding busy (CFB) function. A called party-side service, with which, a user can forward all incoming calls to a designated forwarded-to number or a voice mailbox when the user is busy on another call.
Call Forwarding Busy Number	Indicates the forwarded-to number.
Enable Call Forwarding on No Reply	Enables the call forwarding on no reply (CFNR) function. A called party-side service, with which, a user can forward all incoming calls to a designated forwarded-to number or a voice mailbox if the calls are not answered within a preset period.
Call Forwarding on No Reply Number	Indicates the forwarded-to number.
Call Waiting	A called party-side service, with which, if user C calls user A when user A is talking with user B, user A hears a call waiting (CW) tone indicating that there is an incoming call.
Message Waiting Indicator	This indicator on the phone is on when receiving a new message for a user who is provisioned with the voice mailbox service.
Three-party Call	When user A is communicating with user B and user C wants to join the call, user A can call user C without disconnecting the call with user B. In this case, these 3 users can communicate with each other or two of three can communicate with each other.
Call Holding	A user in a call can hold this call.
Malicious Call Identification	A called party-side service, with which, a user can identify the calling number if the user receives a malicious call.
Caller ID Display	A called party-side service allows the number of the calling party to be presented to the called party.
Call Transfer	Indicates whether to enable the call transfer.
Anonymous Call	This service does not allow the number of the calling party who registers this service to be presented to the called party.
Activate Anonymous Call	Indicates whether to activate the Anonymous Call.
Physical Port Parameters	
Port ID	Indicates the phone port ID.
Ringing Voltage	Indicates the voltage when a phone rings.
DC Voltage	Indicates the DC voltage on a voice port.
Port TX gain	Indicates the Tx gain on a port.
Port RX gain	Indicates the Rx gain on a port.
Lower Threshold for Flash Hooking Duration	Indicates the lower threshold for flash hooking (press the flash button). This function is used for call transfer from an external call to an internal call.
Upper Threshold for Flash Hooking Duration	Indicates the upper threshold for flash hooking.
On-hook Confirmation Time	Indicates the onhook confirmation time.
Impedance	Indicates the impedance.
Feed Current	Feed current supplies power to speech circuits, which requires only current but no voltage.
CLIP Format	Specifies the CLIP format that is supported by the connected phone, including **Sdmf-fsk**, **Mdmf-fsk**, **Dtmf**, **R1.5**, and **Etsi**.
FSK Transmission Delay	Indicates the delay before FSK signals are issued.

Parameter	Description
CLIP Flow	• After ring: the number of the calling party is presented after ringing. • Before ring: the number of the calling party is presented before ringing.
Enable DSP Template	This function can only be used for maintenance and cannot be enabled.
Global DSP Template Name	Indicates the DSP template names, which are used to differentiate DSP templates.
Polarity Reversal on POTS Port	Enables or disables polarity reversal on a POTS port. This function is usually used for charging.
Display Time in CLIP	Indicates whether to display time in CLIP.
Enable DSP HighPass Filter	Indicates whether to enable the DSP highPass filter.
Enable Forced FSK Transmission	Indicates whether to enable the forced FSK transmission.

NOTE:

Physical Port Parameters specify the POTS port physical parameters and the parameter names use the standard terms, which are unnecessary to be described here.

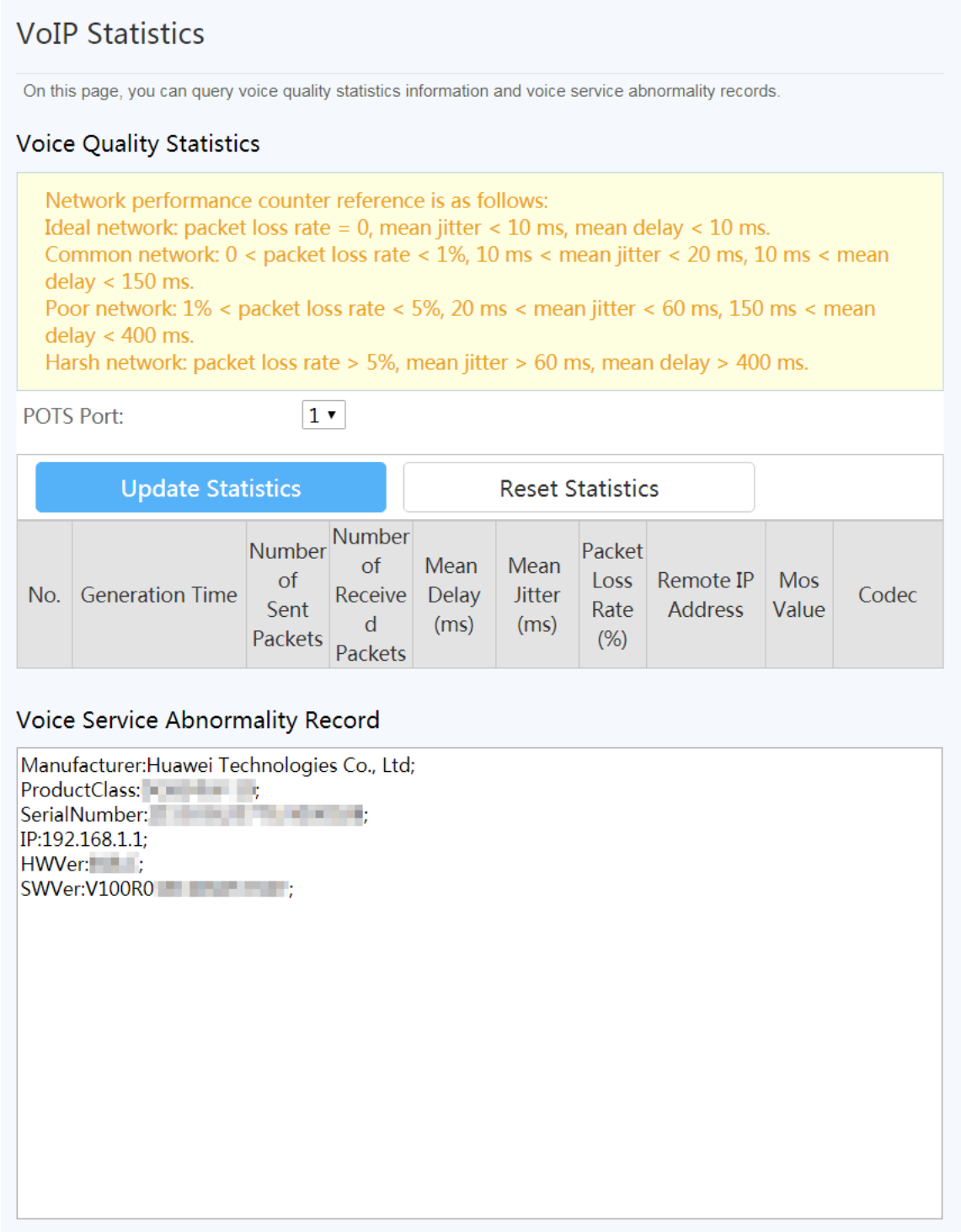
Parent Topic: Voice

< Previous topic Next topic >

1.6.8.3 VoIP Statistics

In the navigation tree on the left, choose **Advanced Configuration** > **Voice** > **VoIP Statistics**. In the pane on the right, you can query the voice quality statistics information and voice service abnormality records, as shown in Figure 1.

Figure 1 VoIP statistics



NOTE:

- If you need to update the statistics, click **Update Statistics**.
- If you need to reset the statistics, click **Reset Statistics**.

Parent Topic: Voice

< Previous topic

1.6.9 System Management

This topic describes how to manage the system on the web page, including the configuration of TR-069, account management, and so on.

TR-069

Account Management

Open Source Software Notice

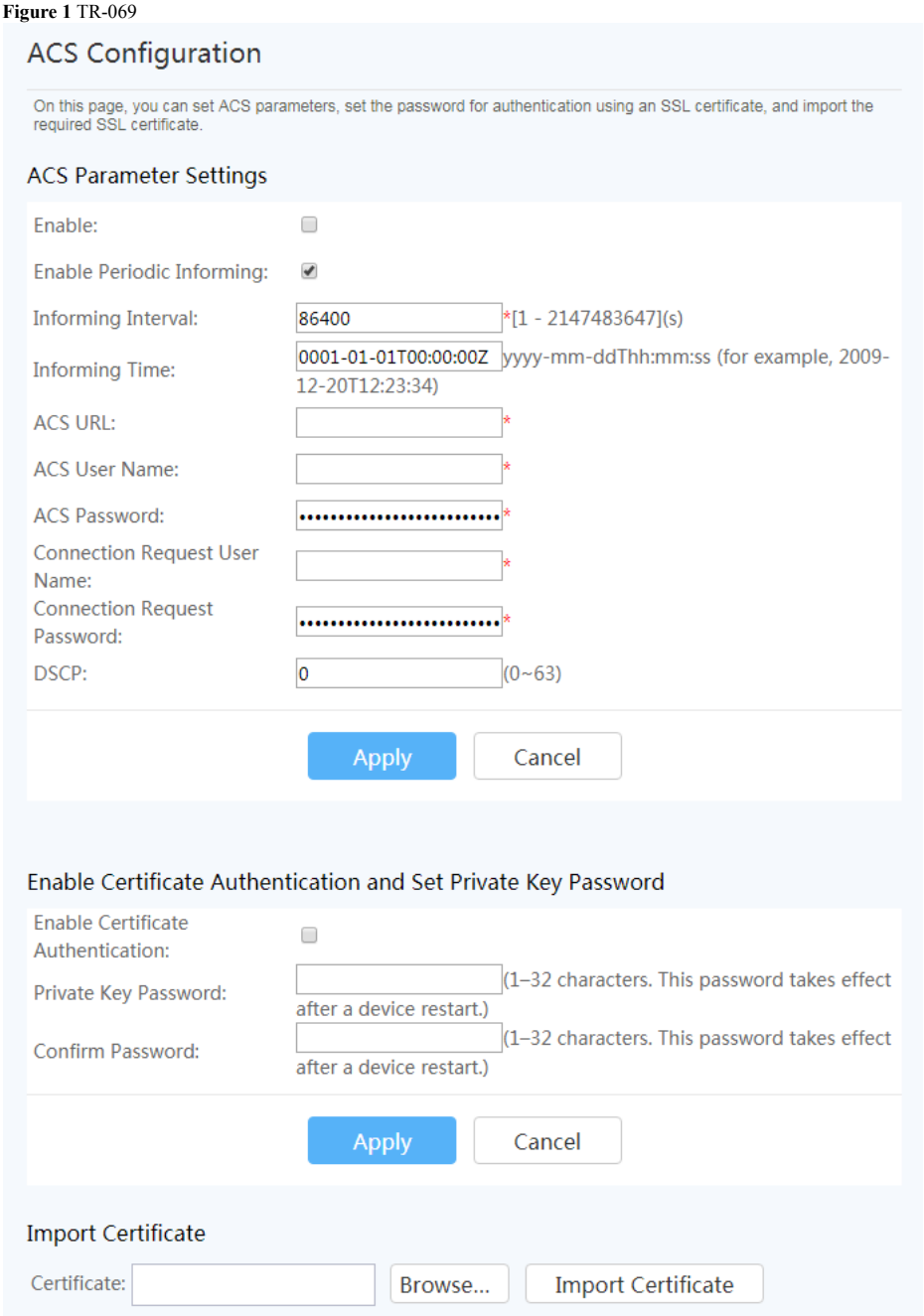
Parent Topic: Advanced Configuration

< Previous topic Next topic >

1.6.9.1 TR-069

1. In the navigation tree on the left, choose **Advanced Configuration** > **System Management** > **TR-069**. In the pane on the right, you can set the parameters related to the interconnection between the DSL home gateway and the TR-069 server, as shown in Figure 1.

Figure 1 TR-069



NOTE:
Configuring the interconnection between the DSL home gateway and the TR-069 requires creating a WAN interface. In addition, **Service Type** of the WAN interface must contain the TR069. For details, see WAN Configuration.

2. Click **Apply**.

Table 1 describes the TR-069 parameters.

Table 1 TR-069 parameters

Parameter	Description
ACS Parameter Settings	

Parameter	Description
Enable	Enables or disables the ACS function.
Enable Periodic Informing	Indicates whether to enable the notification function. • If the notification function is enabled, the DSL home gateway actively sends a connection request to the TR-069 server. • If the notification function is disabled, the DSL home gateway 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 DSL home gateway to send a connection request to the TR-069 server.
Informing Time	Indicates the time for the DSL home gateway to send a connection request to the TR-069 server.
ACS URL	Indicates the address of the TR-069 server to which the DSL home gateway sends a connection request.
ACS User Name	Indicates the user name for the DSL home gateway to register with the TR-069 server.
ACS Password	Indicates the password for the DSL home gateway 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 DSL home gateway.
Connection Request Password	Indicates the password to be carried when the TR-069 server initiates a connection request to the DSL home gateway.
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.
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.

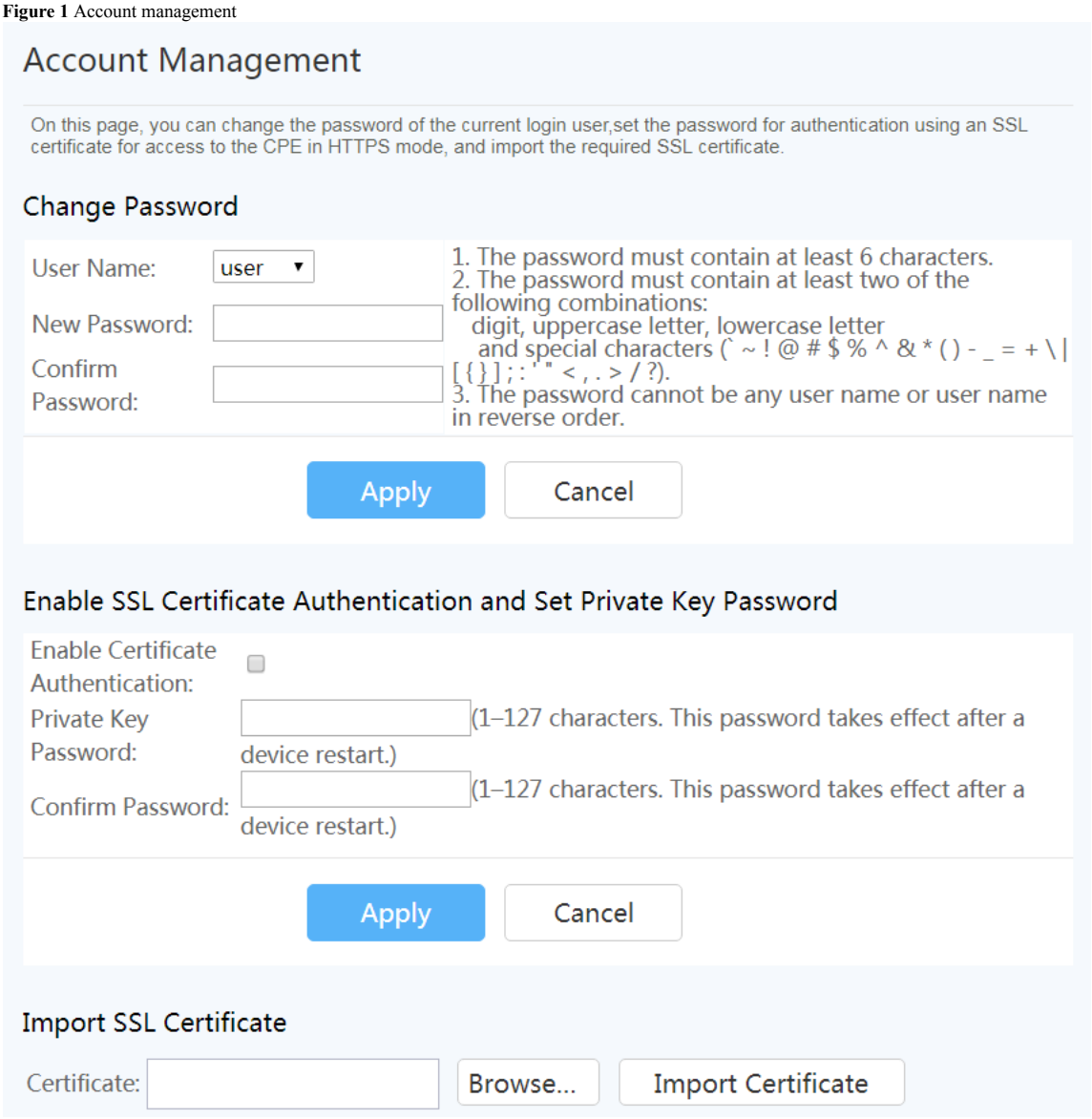
Parent Topic: System Management

Next topic >

1.6.9.2 Account Management

1. In the navigation tree on the left, choose **Advanced Configuration** > **System Management** > **Account Management**. In the pane on the right, you can change the password, as shown in Figure 1.

Figure 1 Account management



NOTE:
Change the initial password after logging in to the web page.

2. Click **Apply**.

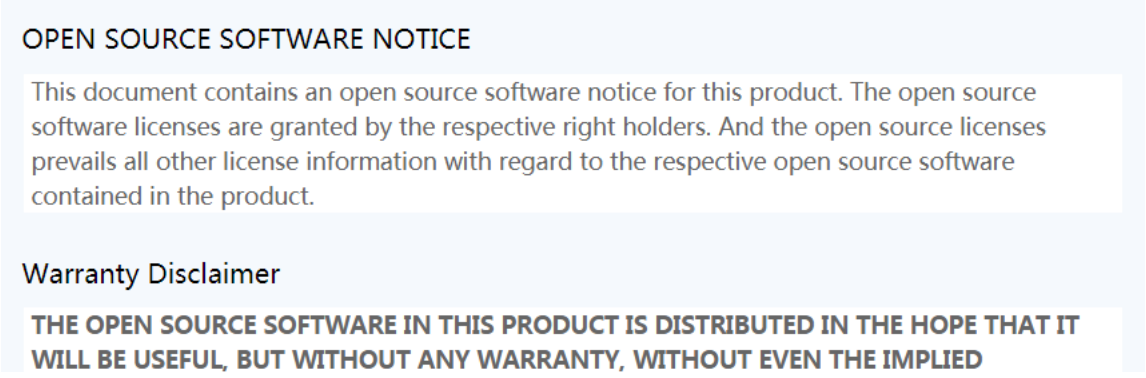
Parent Topic: System Management

< Previous topic Next topic >

1.6.9.3 Open Source Software Notice

In the navigation tree on the left, choose **Advanced Configuration** > **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 1.

Figure 1 Open source software notice



WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SEE THE APPLICABLE LICENSES FOR MORE DETAILS.

Copyright Notice and License Texts

Open Source Software Information

Software	Version	Copyright Notice	License	License Link
jQuery JavaScript Library	1.11.1	Copyright 2005, 2014 jQuery Foundation, Inc. and other contributors Copyright 2008, 2014 jQuery Foundation, Inc. and other contributors Copyright 2005, 2012 jQuery Foundation, Inc. and other contributors Copyright 2012 jQuery Foundation and other contributors Copyright 2005, 2014 jQuery Foundation, Inc. and other contributors Copyright 2008, 2014 jQuery Foundation, Inc. and other contributors Copyright 2014 jQuery Foundation and other contributors Copyright 2013 jQuery Foundation and other contributors Copyright 2013 jQuery Foundation and other contributors Copyright (c) 2010-2013 Christian Johansen Copyright 2005, 2012 jQuery Foundation, Inc. and other contributors Copyright 2012 jQuery Foundation and other contributors	MIT License V2	http://opensource.org/licenses/mit-license.php
thickbox	3.1	Copyright (c) 2007 cody lindley	MIT License	http://opensource.org/licenses/MIT-license.php
jquery_treeview	1.4.1	Copyright (c) 2007 Jörn Zaefferer. Copyright 2010, John Resig. Copyright 2010, The Dojo Foundation. Copyright (c) 2006 Klaus Hartl (stilbuero.de). Copyright (c) 2008 Paul Bakaus	MIT License	http://opensource.org/licenses/MIT-license.php
mtd-utils	1.5.0	Copyright (c) 2000-2007 by Nicolas Devillard.	GPL v2.0	http://www.gnu.org/licenses/gpl-2.0.html
uClibc - A C Library for Embedded Linux	0.9.32	Copyright(C)1989, 1991 Free Software Foundation, Inc. Copyright © Free Software Foundation, Inc.	LGPL v2.1	http://www.gnu.org/licenses/lgpl-2.1.html
			GPL v3.0 With GCC RU	http://www.gnu.or

gcc	4.6	Copyright (C) Free Software Foundation, Inc. http://fsf.org/	tH GCC RU NTIME LIBRARY EXCEPTION	http://www.gnu.org/licenses/gpl-3.0.html
Linux Kernel	3.4.11	Copyright (C) Patrick McHardy. Copyright (C) 1989, 1991 Free Software Foundation, Inc. Copyright (C) 1996,1997,1998 Ralph Metzler. Copyright (C) 1991,1992,1995 Linus Torvalds. Copyright (C) Christoph Hellwig. Copyright (C) Harald Welte. Copyright (C) 1992 Theodore Ts 'o. Copyright (C) 1995 - 2000 by Ralf Baechle. Copyright (C) 1998-2008 Novell/SUSE. Copyright (C) 2000 Russell King. Copyright (C) 2002,2006 Vojtech Pavlik. Copyright (C) 2000-2006 Tigran Aivazian <tigran@aivazian.fsnet.co.uk>. Copyright (C) 2000 - 2007 Jeff Dike (jdike@{addtoit,linux.intel}.com). Copyright (C) 2001 Dan Malek (dmalek@jlc.net). Copyright (C) 2000-2003 Patrick Mochel. Copyright (C) 2001 MandrakeSoft S.A. Copyright (C) 2001 Tim Waugh <twaugh@redhat.com>. Copyright (C) 2001 WireX Communications, Inc <chris@wirex.com>. Copyright (C) 2001-2002 Greg Kroah-Hartman <greg@kroah.com>. Copyright (C) 2001, 2002 Andy Grover <andrew.grover@intel.com>. Copyright (C) 2001 Networks Associates Technology, Inc <ssmalley@nai.com>. Copyright (C) 2001 - 2005 Tensilica Inc. Copyright (C) 2002-2005 Eric Biederman <ebiederm@xmission.com>. Copyright (C) 2003 Red Hat, Inc., James Morris <jmorris@redhat.com>. Copyright (C) 2003 - 2004, 2006 Tresys Technology, LLC. Copyright (C) 2003-2005 Nokia Corporation. Copyright (C) 2004 PathScale, Inc. Copyright (C) 2004-2006 Trusted Computer Solutions, Inc. Copyright (C) 2004-2007 Greg Kroah-Hartman <greg@kroah.com>. Copyright (C) 2004-2008 Red Hat, Inc. All Rights Reserved. Copyright (C) 2004-2010 Freescale Semiconductor, Inc. All Rights Reserved. Copyright (C) 2005 Venkatesh Pallipadi <venkatesh.pallipadi@intel.com>. Copyright (C) 2005-2007 Michael Buesch <mb	GPL v2.0	http://www.gnu.org/licenses/gpl-2.0.html

		uesch@freenet.de>. Copyright (C) 2006 International Business Machines Corp. Copyright (C) 2005-2010 IBM Corporation. Copyright (C) 2006-2008 Intel Corporation. Copyright (C) 2006 IBM Corporation, Timothy R. Chavez <tinytim@us.ibm.com>. Copyright (C) 2005-2011 NTT DATA CORPORATION. Copyright (C) 2007 Hewlett-Packard Development Company, L.P. Copyright (C) 2007 Novell Inc. Copyright (C) 2007-2010 Florian Fainelli <florian@openwrt.org>. Copyright (C) 2008-2009 Red Hat, Inc., Peter Zijlstra <pzijlstr@redhat.com>. Copyright (C) 2009 Wolfram Sang, Pengutronix. Copyright (C) 2009 Jason Baron <jbaron@redhat.com>. Copyright (C) 2009 Jaswinder Singh Rajput. Copyright (C) 2009 Advanced Micro Devices, Inc., Robert Richter. Copyright 2009-2010 Canonical Ltd. Copyright (C) 2010 NXP Semiconductors. Copyright (C) 2010 Nokia Corporation. Copyright (C) 2010 Politecnico di Torino, Italy. Copyright (C) 2011 John Crispin <blogic@openwrt.org>. Copyright (C) 2011 Linus Walleij <linus.walleij@linaro.org>. Copyright (C) 2001 Rusty Russell.		
linux kernel network stack - included in Linux kernel	3.4.11	Copyright (C) 1989, 1991Free Software Foundation, Inc. Copyright (C) Patrick McHardy.	GPL v2.0	http://www.gnu.org/licenses/gpl-2.0.html
netfilter	3.4.11	Copyright© Patrick McHardy. Copyright© Harald Welte.	GPL v2.0	http://www.gnu.org/licenses/gpl-2.0.html
		Copyright (C) 1989, 1991 Free Software Foundation, Inc. Copyright (C) 675 Mass Ave, Cambridge, MA02139, USA. Copyright (C) 2003, CyberTAN Corporation All Rights Reserved. Copyright (c) 2004, 2005 Metaparadigm Pte. Ltd. Michael Clark <michael@metaparadigm.com>. Copyright (c) 2009		

Parent Topic: System Management

< Previous topic

1.6.10 Maintenance Diagnose

This topic describes how to maintain the system on the web page, including the method to restart the device, diagnose the fault, upgrade software version, and so on.

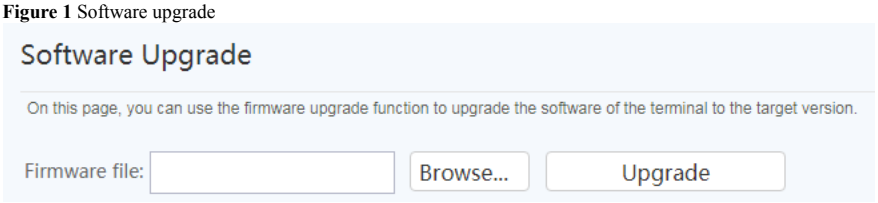
Parent Topic: Advanced Configuration

< Previous topic

1.6.10.1 Software Upgrade

1. In the navigation tree on the left, choose **Advanced Configuration** > **Maintenance Diagnose** > **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 1.

   Figure 1 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.

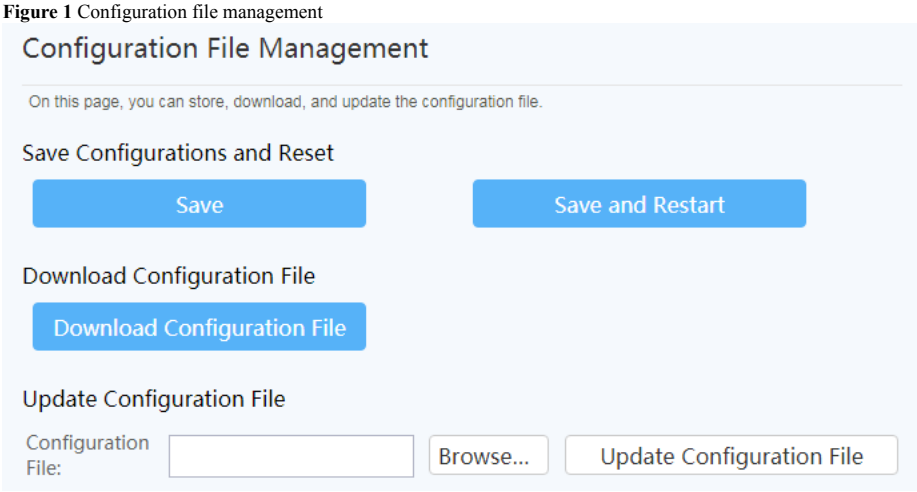
Parent Topic: Maintenance Diagnose

Next topic >

1.6.10.2 Configuration File Management

In the navigation tree on the left, choose **Advanced Configuration** > **Maintenance Diagnose** > **Configuration File Management**. In the pane on the right, click the button as required as shown in Figure 1.

Figure 1 Configuration file management



- Click **Save** to save the configuration file to the flash memory. This prevents data loss due to the restart of the device.
- Click **Save and Restart** to save the configuration file and reboot the DSL home gateway.
- Click **Download Configuration File**. In the dialog box that is displayed, click **Save**, specify the path of saving the configuration file, and then back up the file to the local disk.
- Click **Browse** following the **Configuration File** text box. In the dialog box that is displayed, select the configuration file to be uploaded. Click **Update Configuration File** to upload the configuration file that is saved in the local disk. After the configuration file is successfully uploaded, the device automatically restarts and then the new configuration takes effect.

⚠ **NOTICE:**

- Before uploading the configuration file, choose the configuration file with the correct type and the name of the selected configuration file must not be the same as that of any file saved in the device. Otherwise, the configuration file fails to be uploaded.
- When IE8 is used for configuration file downloading and you click the save button 10s-over later after downloading, the downloaded configuration file is incomplete.

Parent Topic: Maintenance Diagnose

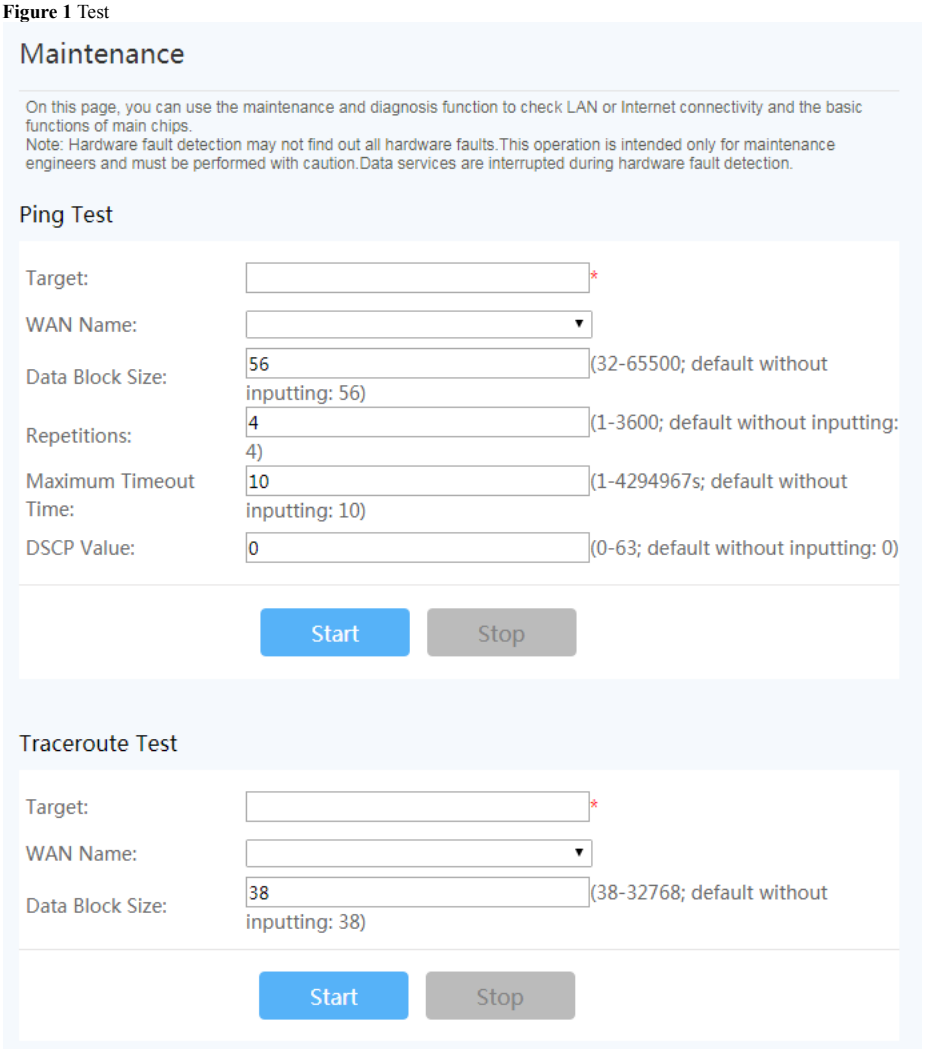
< Previous topic Next topic >

1.6.10.3 Maintenance

In the navigation tree on the left, choose **Advanced Configuration** > **Maintenance Diagnose** > **Maintenance**.

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

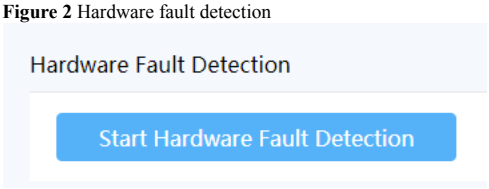
Figure 1 Test



After the test, the web page shows the test results.

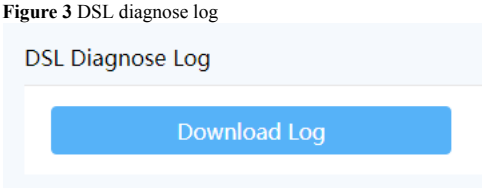
2. In the pane on the right, click **Start Hardware Fault Detection** to start hardware fault detection, as shown in Figure 2.

Figure 2 Hardware fault detection



3. In the pane on the right, click **Download Log** to download the DSL diagnose log, as shown in Figure 3.

Figure 3 DSL diagnose log



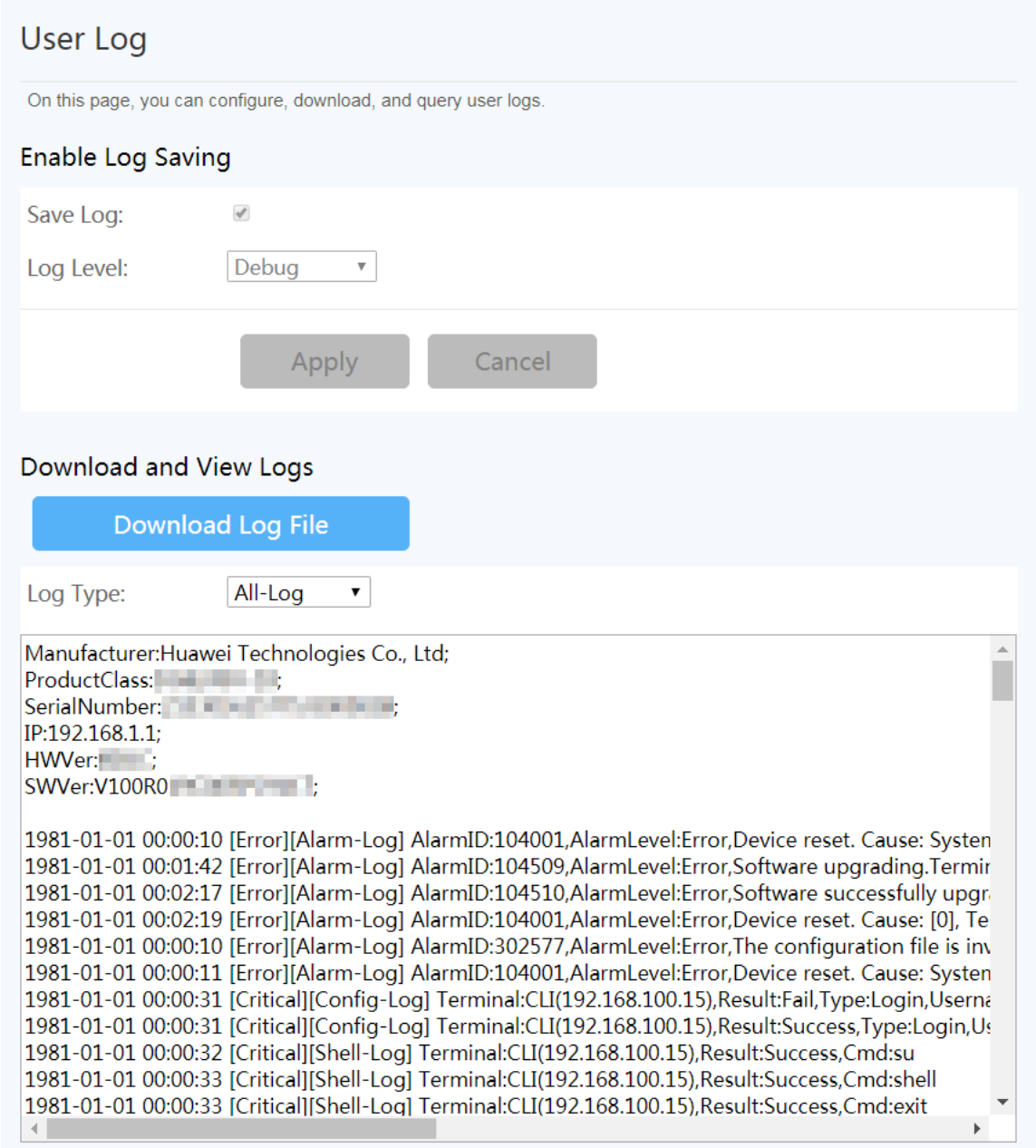
Parent Topic: Maintenance Diagnose

< Previous topic Next topic >

1.6.10.4 User Log

In the navigation tree on the left, choose **Advanced Configuration** > **System Management** > **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 1

Figure 1 User log



- **Save Log** is enabled by default, it cannot 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.

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.

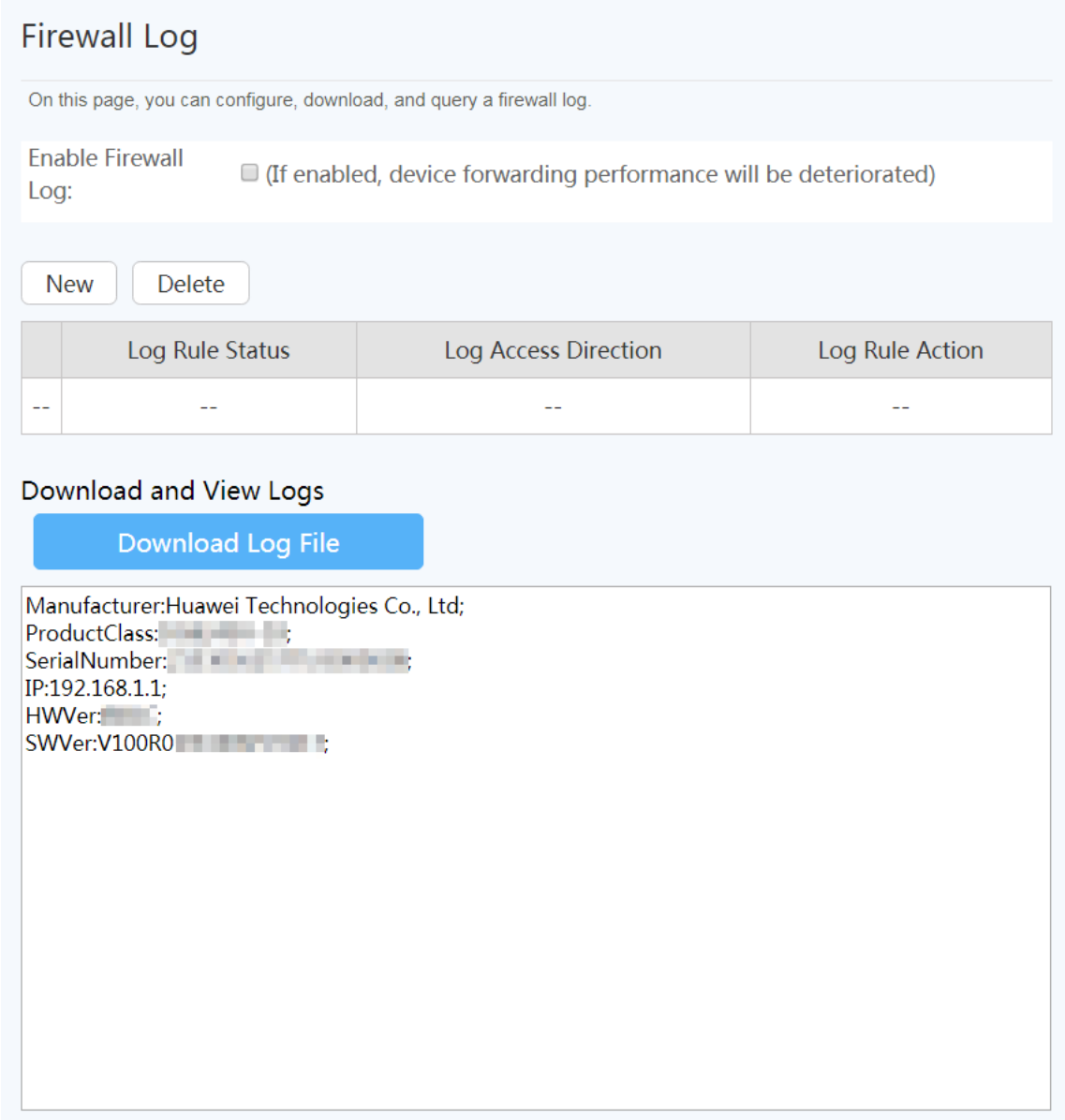
Parent Topic: Maintenance Diagnose

< Previous topic Next topic >

1.6.10.5 Firewall Log

In the navigation tree on the left, choose **Advanced Configuration** > **Maintenance Diagnose** > **Firewall Log**. In the pane on the right, you can view logs and download log files, as shown in Figure 1.

Figure 1 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 **Delete** to delete 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.

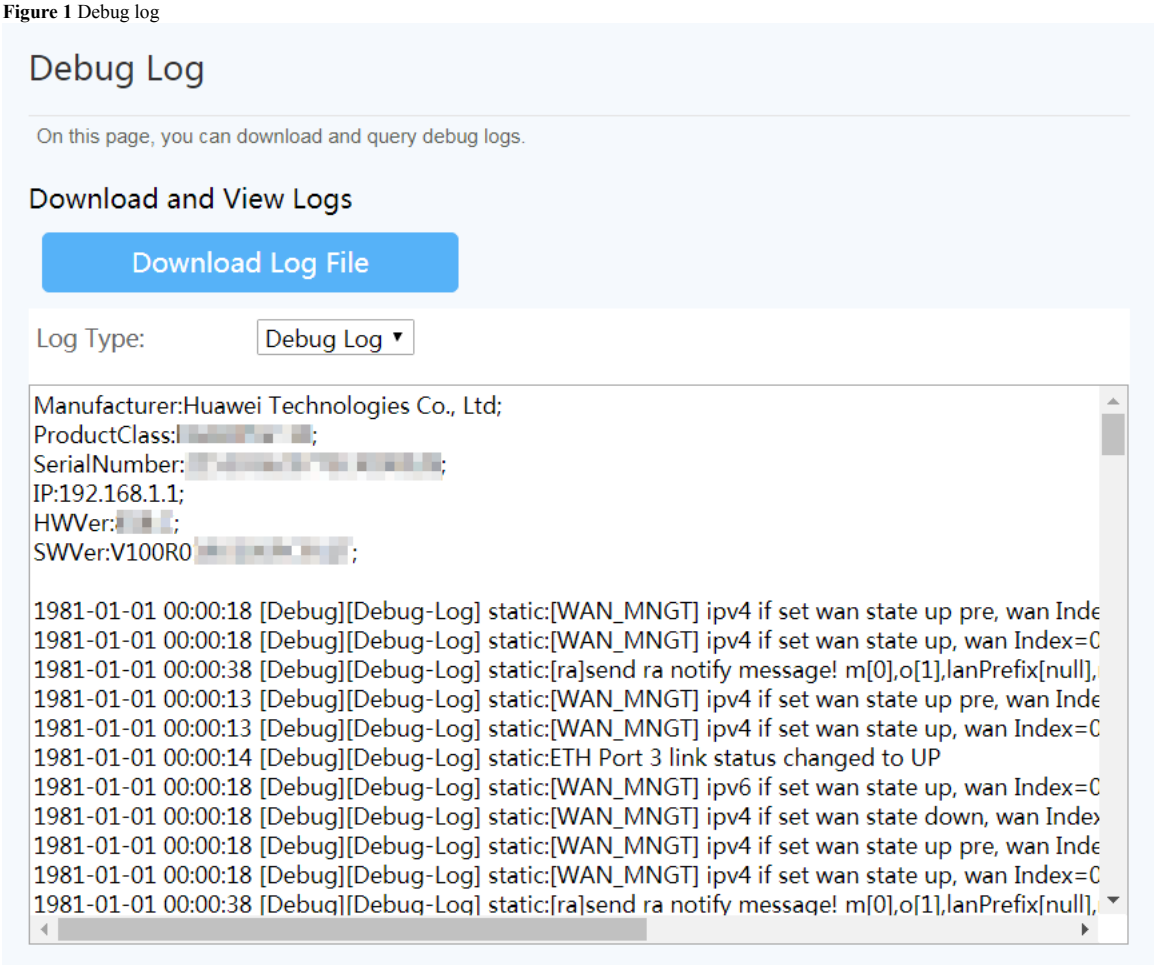
Parent Topic: Maintenance Diagnose

< Previous topic Next topic >

1.6.10.6 Debug Log

In the navigation tree on the left, choose **Advanced Configuration** > **Maintenance Diagnose** > **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 1.

Figure 1 Debug 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.

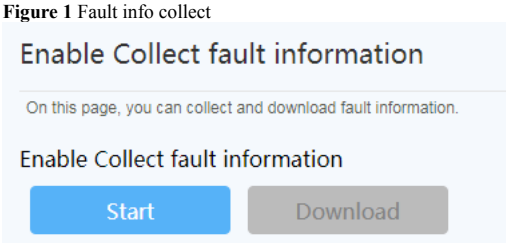
Parent Topic: Maintenance Diagnose

< Previous topic Next topic >

1.6.10.7 Fault Info Collect

In the navigation tree on the left, choose **Advanced Configuration** > **Maintenance Diagnose** > **Fault Info Collect**. In the pane on the right, click **Start** to collect DSL home gateway fault information, as shown in Figure 1.

Figure 1 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.

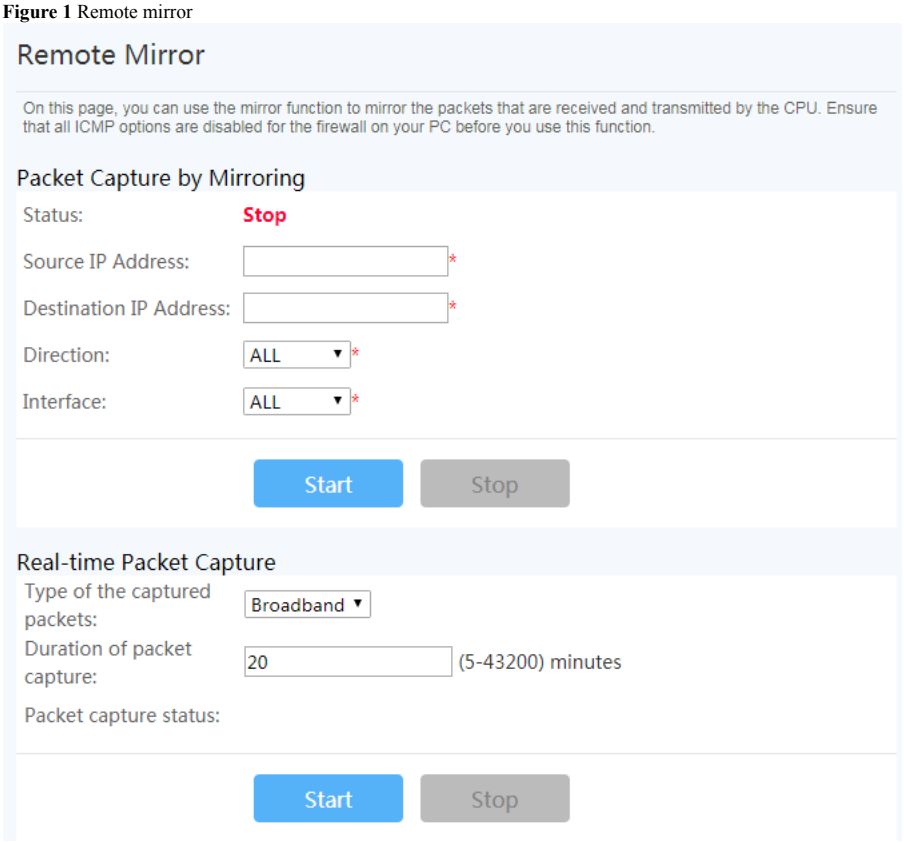
Parent Topic: Maintenance Diagnose

< Previous topic Next topic >

1.6.10.8 Remote Mirror

1. In the navigation tree on the left, choose **Advanced Configuration** > **Maintenance Diagnose** > **Remote Mirror**, as shown in Figure 1.

Figure 1 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.

2. Click **Start**.

NOTE:

Based on your requirements, this function may involve using, obtaining, or saving some information about users' communications for the purpose of safeguarding network operation and protecting services. Huawei alone is unable to collect or save 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 content of users' communications is fully protected when the content is being used and saved.

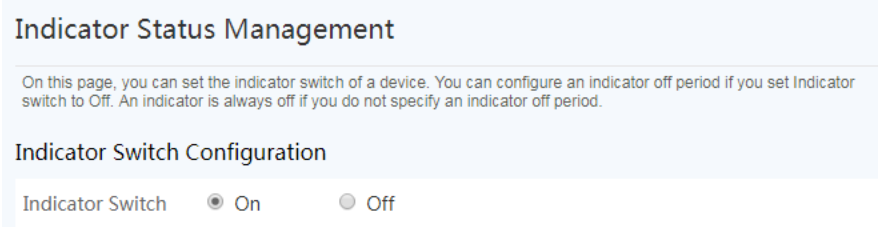
Parent Topic: Maintenance Diagnose

< Previous topic Next topic >

1.6.10.9 Indicator Status Management

1. In the navigation tree on the left, choose **Advanced Configuration** > **Maintenance Diagnose** > **Indicator Status Management**. In the pane on the right, you can set the indicator switch and disabling time segment, as shown in Figure 1.

Figure 1 Indicator status management



2. Click **Apply**.

Parent Topic: Maintenance Diagnose

< Previous topic