ONT User Guide

Product Version: V300R019C00&V500R019C00

Library Version: 04

Date: 2019-06-25

For any question, please contact us.

Web Page Reference (HG8145V5/HG8245H5/HG8247H5/HG8240T5/HG8141A5)

Contents

1 Web Page Reference (HG8145V5/HG8245H5/HG8247H5/HG8240T5/HG8141A5)

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 Interface.

The web page of the HG8145V5/HG8245H5/HG8247H5/HG8240T5/HG8141A5 varies according to ONT capability sets. For bridging-type ONTs, GUIs for Layer 3 and voice configurations are not supported. For ONTs without Wi-Fi interfaces, GUIs for wireless network configurations are not supported. For details on ONT capability sets, refer to Reference of GPON ONT Capability Sets. This topic uses figures of the HG8245H5 accessed by the administrator (telecomadmin) as examples. Different ONTs may have different screencaptures, actual screencaptures prevail.

Because different voice protocols, the **Voice** node contains different parameters. Only one of the SIP and H.248 protocols can be supported at a time. Which protocol is supported depends on the ONT used.

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.

Parent Topic: Maintenance and Troubleshooting

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.1 Locally Logging in to the Web Interface

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

Context

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

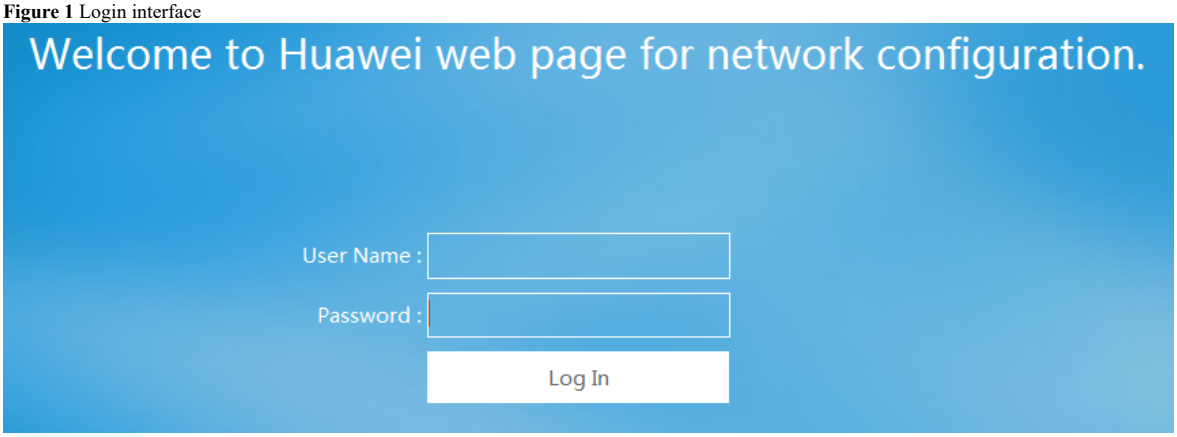
Table 1 Data plan

Item	Description
User name and password	Default settings: • Administrator (installation and maintenance personnel): ▪ User name: telecomadmin ▪ Password: admintelecom **NOTE:** • After logging in to the web page, if you do not perform any operations within five minute, you will be locked out and return back to the login interface. Then, You can unlock the account by entering the login user name and password. • Three times within five minutes the user name and password input error, the system is locked and unlocked automatically after one minute. • Modify the password through the BMS. • Certain carriers may customize accounts and passwords, which are different from the default accounts and passwords listed in the preceding. For details, contact the corresponding carrier. **NOTE:** • 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: root ▪ Password: adminHW **NOTE:** • The common user account can be used to query the service status. For ONTs 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. • After logging in to the web page, if you do not perform any operations within five minute, you will be locked out and return back to the login interface. Then, You can unlock the account by entering the login user name and password. • Three times the user name and password input error, the system is locked and unlocked automatically after one minute. • Modify the password through the Web. • Certain carriers may customize accounts and passwords, which are different from the default accounts and passwords listed in the preceding. For details, contact the corresponding carrier. **NOTE:** Change the initial password after common users log in to the web page.
LAN IP address and subnet mask	Default settings: • IP address: 192.168.100.1 • 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 ONT. For example: • IP address: 192.168.100.100 • Subnet mask: 255.255.255.0

Procedure

1. Use a network cable to connect the LAN port of the ONT to a PC.
2. Ensure that the Internet Explorer (IE) of the PC does not use the proxy server. The following section considers IE 6.0 as an example to describe how to check whether the IE uses the proxy server.
   a. Start the IE, and choose **ToolsInternet Options** from the main menu of the IE window. Then, the **Internet Options** interface is displayed.
   b. In the **Internet Options** interface, click the **Connections** tab, and then click **LAN settings**.
   c. In the **Proxy server** area, ensure that the **Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).** check box is not selected (that is, without the "√" sign). If the check box is selected, deselect it, and then click **OK**.
3. Set the IP address and subnet mask of the PC. For details, see Table 1.
4. Log in to the Web configuration interface.
   a. Enter **http://192.168.100.1** in the address bar of IE (192.168.100.1 is the default IP address of the ONT), and then press **Enter** to display the login interface, as shown in Figure 1.

Figure 1 Login interface



NOTE:

The web page login supports SSL3.0, TLS1.0, TLS1.1, and TLS1.2. It is recommended that you use high-security TLS1.1 or TLS1.2 if you log in to the ONT using https. The TCP port 80 is used for listening for HTTPS packets. You need to type "https://192.168.100.1:80" in the address bar of IE and press **Enter** to log in to the ONT.

b. In the login interface, 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 configuration interface is displayed.

Parent Topic: Web Page Reference (HG8145V5/HG8245H5/HG8247H5/HG8240T5/HG8141A5)

Copyright © Huawei Technologies Co., Ltd.
Next topic >

1.2 Fast Setting

This topic describes how to quickly set an ONT.

Administrator

NOTE:

- Only the ONT web page supports ONT WAN configurations.
- For methods of setting **ONT Authentication** and **WAN Configuration**, see ONT Authentication and WAN Configuration.

Common User

NOTE:

- When the root user logs in to the ONT 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 Home Page to go to this page.
- For detailed account management operations, see Account Management.

Parent Topic: Web Page Reference (HG8145V5/HG8245H5/HG8247H5/HG8240T5/HG8141A5)

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.3 Home Page

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

Auxiliary buttons (such as **Fast Setting**, and **admin**) on the upper right corner of the page can guide you to different pages.

Parent Topic: Web Page Reference (HG8145V5/HG8245H5/HG8247H5/HG8240T5/HG8141A5)

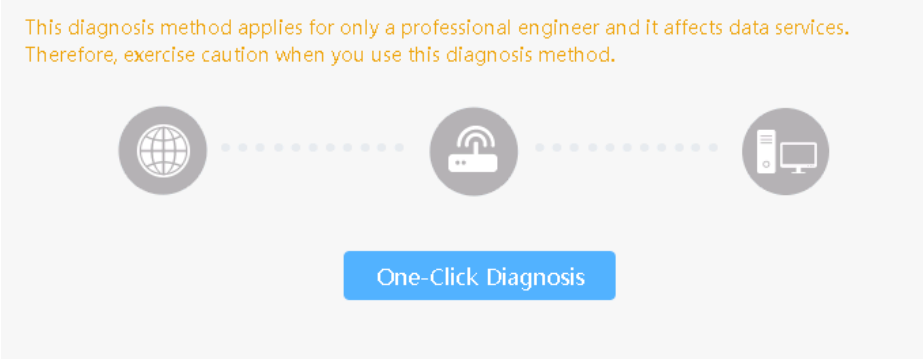
Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.4 One-click Diagnosis

This topic describes how to quickly diagnose ONT network faults.

1. Choose **One-click Diagnose** from the navigation tree on the left panel. Then click **One-click Diagnose** on the right panel 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 result

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 (HG8145V5/HG8245H5/HG8247H5/HG8240T5/HG8141A5)

Copyright © Huawei Technologies Co., Ltd.

< Previous topic Next topic >

1.5 System Information

This topic describes how to query the information about the ONT, including ETH port information, optical information, and user device information through the Web page.

- Device Information
- WAN Information
- Optical Information
- Service Provisioning Status
- VoIP Information

Eth Port Information

WLAN Information

Home Network Information

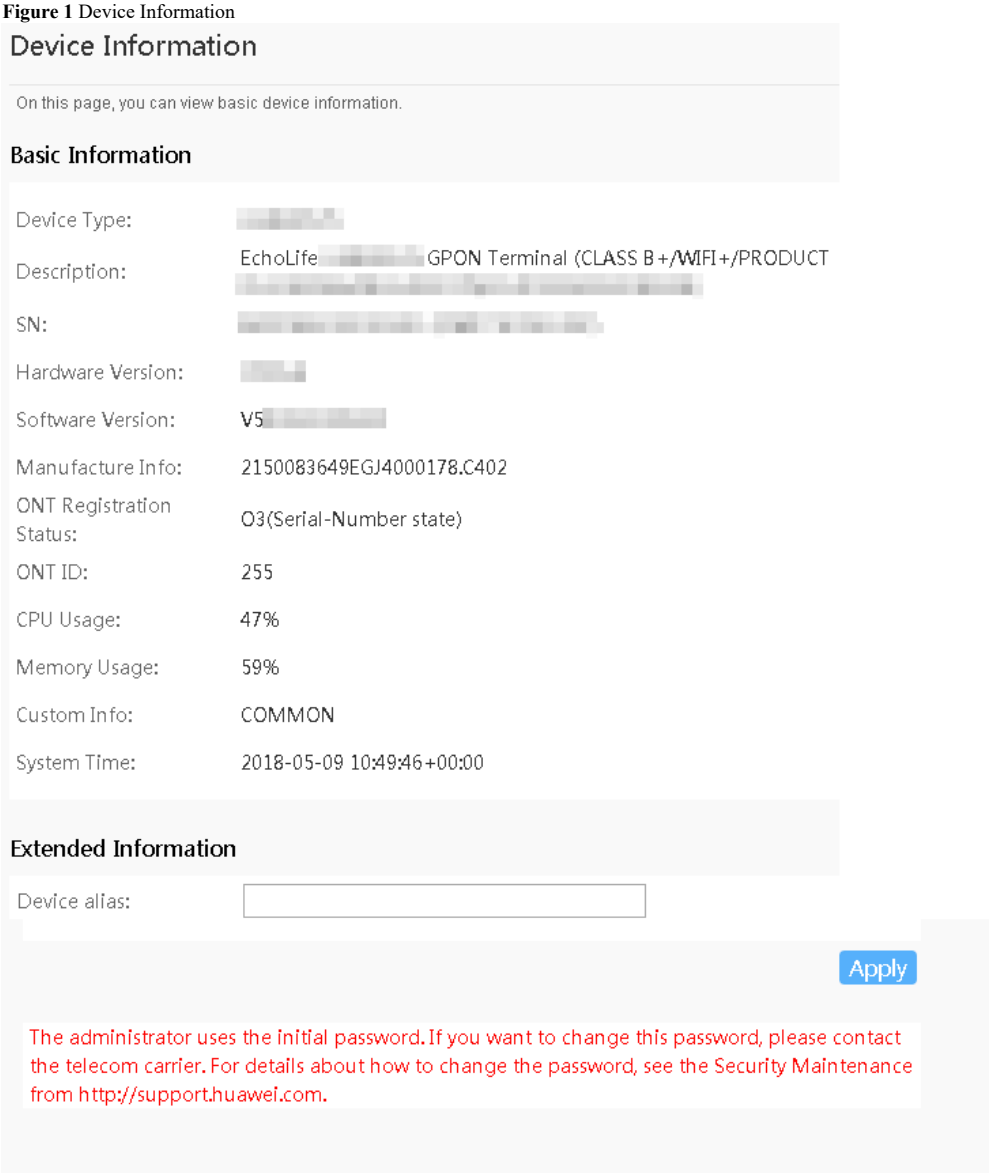
Parent Topic: Web Page Reference (HG8145V5/HG8245H5/HG8247H5/HG8240T5/HG8141A5)

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.5.1 Device Information

In the navigation tree on the left, choose **System Information** > **Device Information**. In the pane on the right, you can view the product name, hardware version, and software version, as shown in Figure 1.

Figure 1 Device Information



Parent Topic: System Information

Copyright © Huawei Technologies Co., Ltd.
Next topic >

1.5.2 WAN Information

In the navigation tree on the left, choose **System Information** > **WAN Information**. In the pane on the right, you can view the status of the WAN interface, mode of obtaining an IP address, IP address, and subnet mask, as shown in Figure 1

Figure 1 WAN Information

WAN Information

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

IPv4 Information(Click the form for details)

WAN Name	Status	IP Address	VLAN/Priority	Connect
2_TR069_INTERNET_R_VID_10	Disconnected	--	10/0	AlwaysOn

WAN Information

MAC Address:	00:E0:FC:00:
VLAN:	10
Policy:	Use the specified value
Priority:	0
NAT:	Enable
IP Acquisition Mode:	DHCP
IP Address/Subnet Mask:	--
Gateway:	--
DNS Servers:	--
Lease Time:	--
Remain Lease:	--
NTP Servers:	--
Time Zone Info:	--
SIP Servers:	--
Static Route:	--
Vendor Info:	--
Online Duration (dd:hh:mm:ss):	--

NOTE:

Click a record in the WAN list, 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** WebPage, you can click **Connected** link to connect the current WAN port, click **disconnected** link to disconnect the current WAN port.

Parent Topic: System Information

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.5.3 Optical Information

In the navigation tree on the left, choose **System Information** > **Optical Information**. In the pane on the right, you can view the optical status, transmit optical power, receive optical power of the optical module, as shown in Figure 1.

Figure 1 Optical Information

Optical Information

On this page, you can query the status of the optical module.

ONT Information

	Current Value	Reference Value
Optical Signal Sending Status:	--	Auto
TX Optical Power:	-- dBm	0.5 to 5 dBm
RX Optical Power:	-- dBm	-27 to -8 dBm
Working Voltage:	3369 mV	3100 to 3500 mV
Bias Current:	0 mA	0 to 90 mA
Working Temperature:	43 ℃	-10 to +85 ℃

OLT Information

	Current Value	Reference Value
Optical module type:	--	--
Transmit optical power:	-- dBm	--
PON port identifier:	--	--

Parent Topic: System Information

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.5.4 Service Provisioning Status

Click the **System Information** tab, and choose **Service Provisioning Status** from the navigation tree on the left. In the right pane, the ONT service provisioning status is displayed, as shown in Figure 1.

Figure 1 Service Provisioning Status

Service Provisioning Status

On this page, you can query the service provisioning status.

ONT Registration Status: Obtaining the status. Please wait.
OLT Service Configuration Status: --
EMS Configuration Status: --
ACS Registration Status: --

Refresh

Parent Topic: System Information

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.5.5 VoIP Information

In the navigation tree on the left, choose **System Information** > **VoIP Information**. Then, in the pane on the right, you can query the information such as user status and call status. The SIP configuration page is slightly different from the H.248 configuration page, as shown in Figure 1 and Figure 2.

Figure 1 VoIP Information - SIP

VoIP Information

On this page, you can query status information of voice users and reset the voice function.

No.	URI	User Name (Phone Number)	Associated POTS Port	User Status	Call Status	Registry Error	Error Code
1	--	77730020	2	Registering	Idle	The ONU is offline	--
2	--	+8675577730010	2	Registering	Idle	The ONU is offline	--

Restart VoIP

Figure 2 VoIP Information - H.248

VoIP Information

On this page, you can query status information of voice users and reset the voice function.

No.	Physical TID	Phone Number	Associated POTS Port	User Status	Call Status	Interface Status	Registry Error
1	A0	--	1	Registering	Idle	Closed	The ONU is offline
2	--	--	2	Initializing	Idle	Closed	The ONU is offline

Restart VoIP

If the VoIP service needs to be restarted, click **Restart VoIP** in the pane on the right.

Parent Topic: System Information

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.5.6 Eth Port Information

In the navigation tree on the left, choose **System Information** > **Eth Port Information**. In the pane on the right, you can view the duplex mode, speed, and status of the ETH port, as shown in Figure 1.

Figure 1 Eth Port Information

Eth Port Information

On this page, you can query the user-side Ethernet port information.

Ethernet Port Status

Port	Status			Receive (RX)		Transmit (TX)	
	Mode	Speed	Link	Bytes	Packets	Bytes	Packets
1	--	--	Down	0	0	193250	1690
2	Full-duplex	1000 Mbit/s	Up	2401372	16064	29226429	27902
3	--	--	Down	0	0	193250	1690
4	--	--	Down	0	0	193250	1690

Parent Topic: System Information

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.5.7 WLAN Information

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

Figure 1 WLAN Information

WLAN Information

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

One-Click Diagnosis

WLAN Info

WLAN Status:	Enabled
WLAN Channel:	6

WLAN Packet Statistics

SSID Index	SSID Name	Receive (RX)				Transmit (TX)			
		Bytes	Packets	Error	Discarded	Bytes	Packets	Error	Discarded
1	WirelessNet	0	0	0	0	862114	5094	0	5094

SSID Information

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

STA Information

Query

Number of STAs : 0

MAC Address	SSID Name	Connection Duration (s)	Sending Rate (Mbit/s)	Receiving Rate (Mbit/s)	Signal Strength (dBm)	Noise (dBm)	Signal-to-Noise Ratio (dB)	Signal Quality (dBm)

Neighboring AP Information

Query Note: querying the neighboring AP information may disconnect all STA connections.

SSID Name	MAC Address	Network Type	Channel	Signal Strength (dBm)	Noise (dBm)	DTIM Interval	Beacon Period (ms)	Authentication Mode	Working Mode	Max. Rate (Mbit/s)

STA Event Log

Download Log File

```
1981-01-01 00:00:47 [2.4G] [vap0] {dmac_config_down_vap:: WLAN DOWN success.}
1981-01-01 00:00:49 [2.4G] [vap0] {dmac_config_start_vap:: WLAN UP success.}
1981-01-01 00:00:49 [2.4G] [vap0] {wal_chan_switch_report::pre_chan=0 new_chan=5 reason=1 chip_inde
```

Parent Topic: System Information

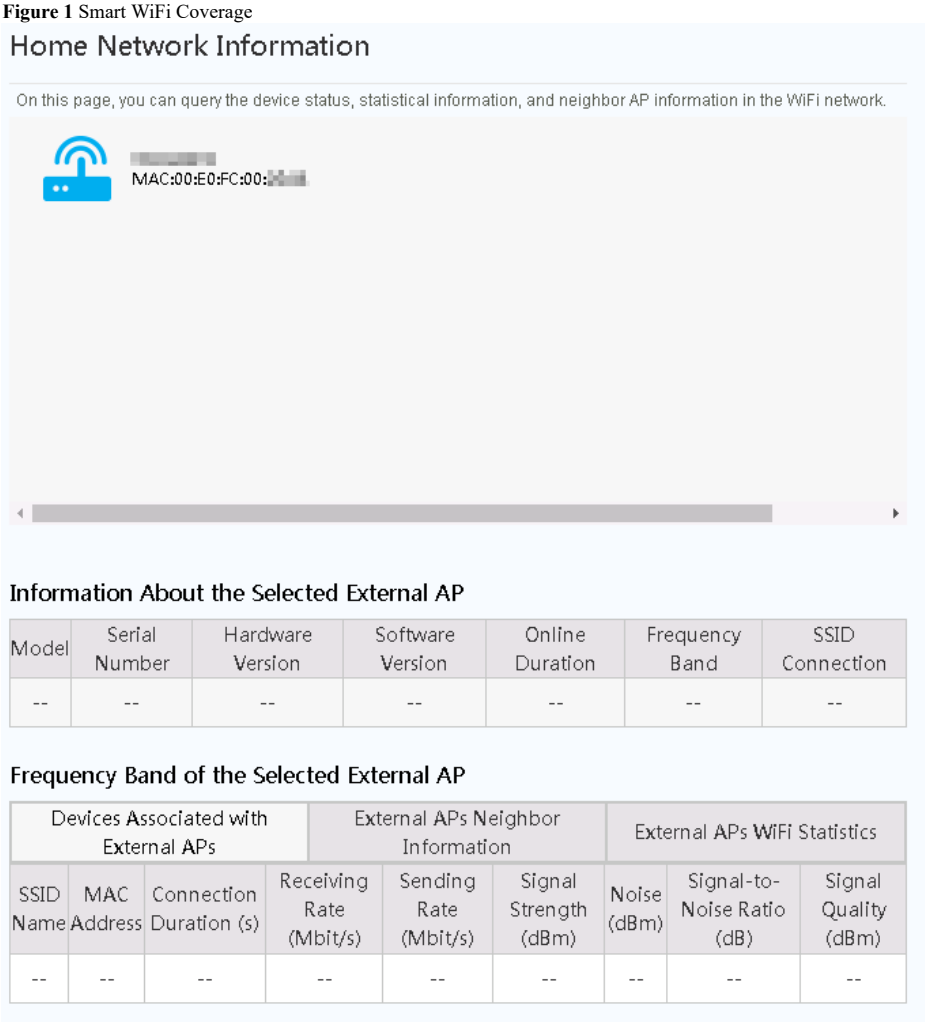
Copyright © Huawei Technologies Co., Ltd.

< Previous topic Next topic >

1.5.8 Home Network Information

Click the **System Information** tab, and choose **Home Network Information** from the navigation tree on the left. In the right pane, check the device status, statistical information, and neighbor AP information of external APs in the WiFi network, as shown in the figure below.

Figure 1 Smart WiFi Coverage



Parent Topic: System Information

Copyright © Huawei Technologies Co., Ltd.
< 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.

Parent Topic: Web Page Reference (HG8145V5/HG8245H5/HG8247H5/HG8240T5/HG8141A5)

Copyright © Huawei Technologies Co., Ltd.
< Previous topic

1.6.1 WAN Configuration

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

Parent Topic: Advanced Configuration

Copyright © Huawei Technologies Co., Ltd.
Next topic >

1.6.1.1 WAN Configuration

- WAN Configuration - route

1. In the navigation tree on the left, choose **Advanced Configuration** > **WAN Configuration**. In the pane on the right, click **New**. In the dialog box that is displayed, set **Mode** to **Route WAN**, as shown in Figure 1 and Figure 2.

Figure 1 WAN Configuration - route(IPv4)

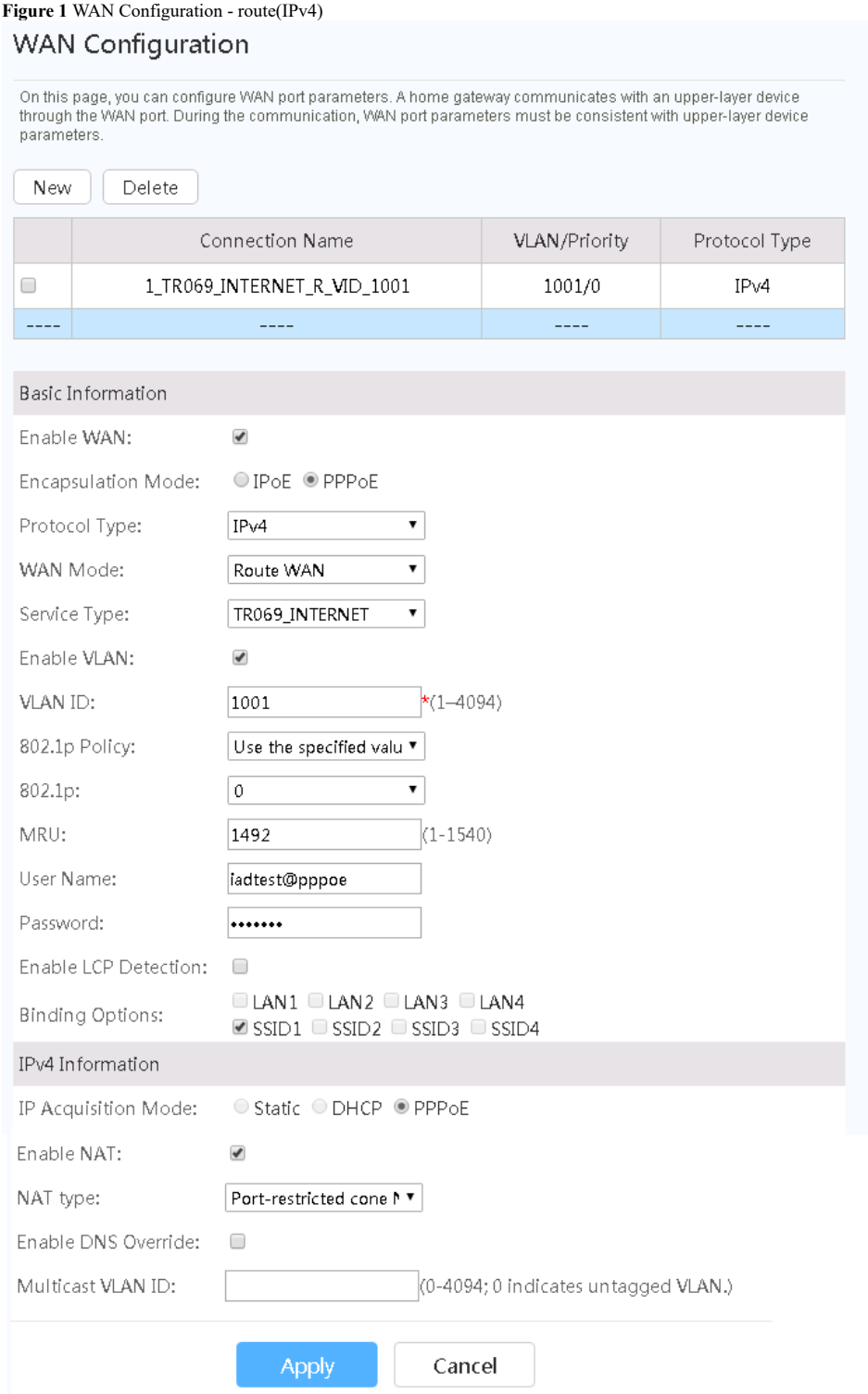
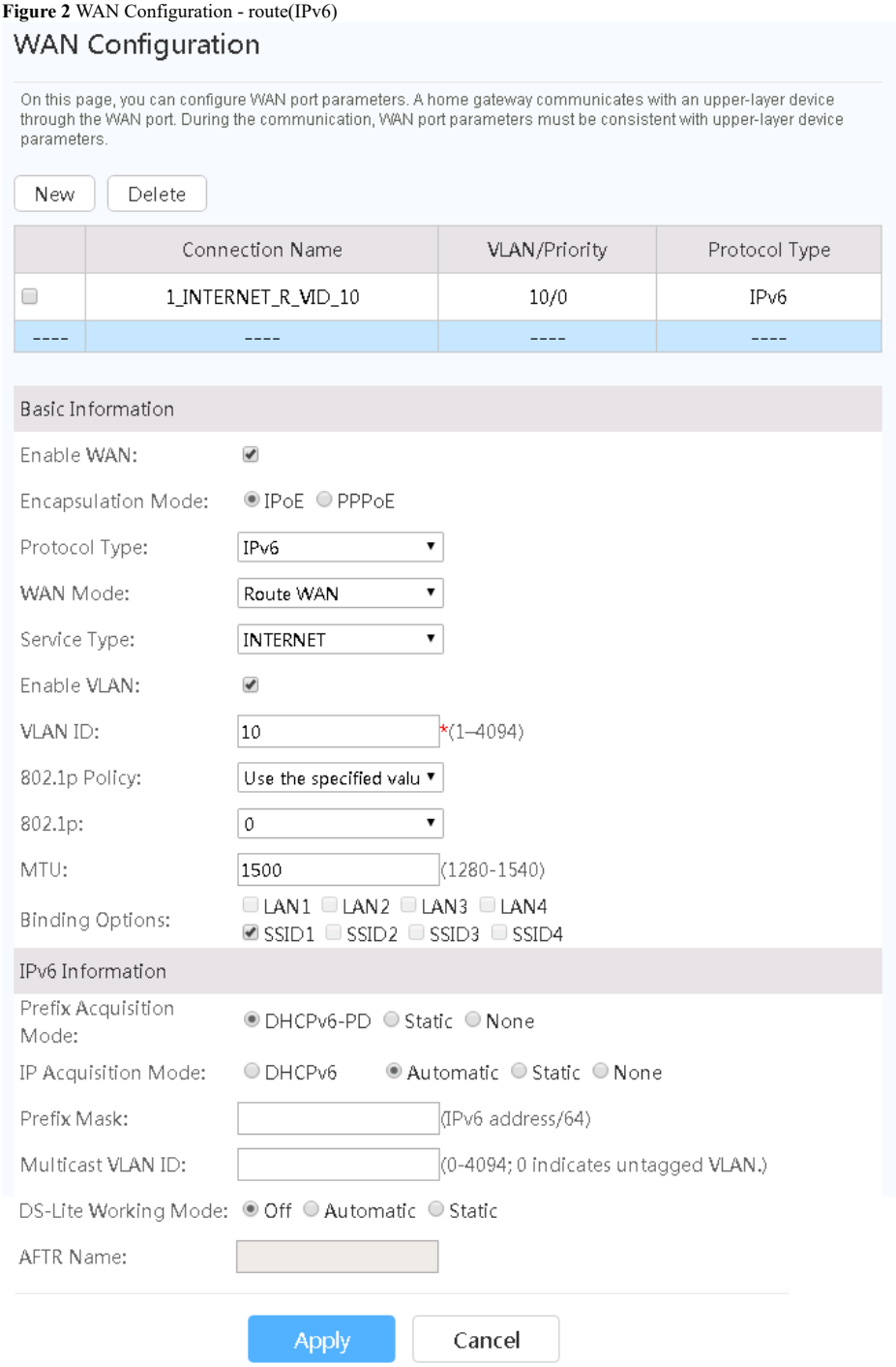


Figure 2 WAN Configuration - route(IPv6)



2. Click **Apply**.

NOTICE

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 in route mode.

Table 1 Parameters related to the WAN in route mode

Parameter	Description
Enable WAN Connection	Indicates whether to enable the WAN connection.
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 dual stack**.
Mode	Indicates the WAN interface mode. It can be set to **Bridge WAN** or **Route WAN**.
Service List	Indicates the service type of the WAN interface. It can be set to **TR069**, **INTERNET**, **TR069_INTERNET**, **VOIP**, **TR069_VOIP**, **VOIP_INTERNET**, **TR069_VOIP_INTERNET**, **IPTV**, **OTHER**, **VOIP_IPTV**, **TR069_IPTV** or **TR069_VOIP_IPTV**.
Enable VLAN	Selects this check box to set VLAN ID and 802.1p priority.
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 OLT.

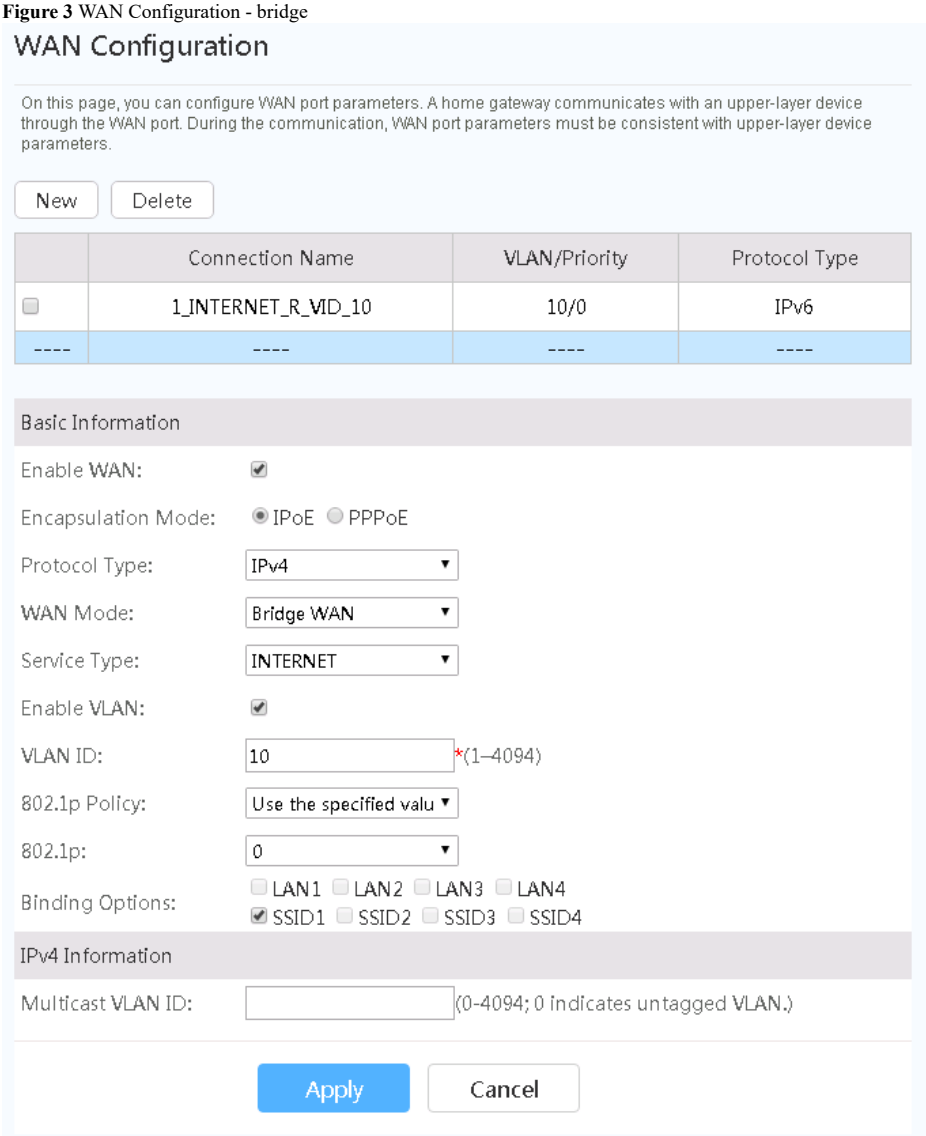
Parameter	Description
802.1p policy	Indicates the 802.1p priority policy. • Use specified value: indicates that a specified priority value is used. If you select this option, you need to set the **802.1p** parameter. • Copy from IP precedence: indicates that the priority is copied from the ToS field 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. • Dscp Pbit Mapping: indicates the priority displayed in the DSCP to 802.1p mapping table. The DSCP field is 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.
MTU	Indicates the maximum transmission unit (MTU) of IPoE packets. This parameter needs to be set only when **Encapsulation Mode** is set to **IPoE**.
MRU	Indicates the maximum receive unit (MRU) of PPPoE packets. This parameter needs to be set only when **Encapsulation Mode** is set to **PPPoE**.
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**.
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**.
Enable LCP detection	This parameter needs to be set only when **Encapsulation Mode** is set to **PPPoE**. • 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 Layer 2/3 Port Configuration, 2.4G Basic Network Settings and 5G Basic Network Settings.
IPv4 Information	
IP Acquisition Mode	Indicates the mode of obtaining an IPv4 address on the ONT. 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.
Dial Method	Indicates the PPPoE dialup method. It can be set to **Auto**, **Manual**, or **On Demand**.
Multicast VLAN ID	Indicates the multicast VLAN ID, ranging from 1 to 4094. The multicast VLAN ID must be the same as the multicast VLAN ID on the OLT.
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	
Prefix Acquisition Mode	Indicates the prefix acquisition mode. It can be set to **DHCP-PD**, **Static**, or **None**. • DHCPv6-PD: When the parameter is set to **DHCPv6-PD**, the BRAS assigns a prefix to the ONT 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. • If this parameter is set to **RA** or **Auto** in an earlier version, its value will be automatically changed to **DHCPv6-PD** automatically after the version is upgraded to V300R019C00&V500R019C00.

Parameter	Description
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. The ONT address mode can be **Numbered** or **Unnumbered**. When the address mode is **Numbered**, the ONT WAN port has its own IPv6 GUA address. When the address mode is **Unnumbered**, the ONT WAN port has an LLA address but no GUA address, which is not good for network management and fault location. Therefore, the **Numbered** mode is recommended. • When the **Numbered** mode is used, the setting of **IP Acquisition Mode** is as follows: ▪ When M=1 is set for the RA packet on the BRAS, IP addresses are obtained in DHCPv6 mode on the WAN side. Then, **IP acquisition mode** can be set to **DHCPv6** or **Automatic**. **Automatic** is recommended. ▪ When M=0 is set for the RA packet on the BRAS, IP addresses are obtained in ND (stateless address allocation) mode on the WAN side. Then, **IP acquisition mode** can be set to **Automatic**. • When the **Unnumbered** mode is used, **IP acquisition mode** is set to **None**.
Multicast VLAN ID	The multicast VLAN ID ranges from 1 to 4094. The multicast VLAN ID must be the same as the multicast VLAN ID on the OLT.
DSLite work 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. • Off: Indicates the DSLite work mode is disabled. • Auto: 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.

- WAN Configuration - bridge

1. In the navigation tree on the left, choose **Advanced Configuration** > **WAN Configuration**. In the pane on the right, click **New**. In the dialog box that is displayed, set **Mode** to **Bridge WAN**, as shown in Figure 3.

Figure 3 WAN Configuration - bridge



2. Click **Apply**.

Table 2 describes the parameters related to the WAN in bridge mode.

Table 2 Parameters related to the WAN in bridge mode

Parameter	Description
Enable WAN Connection	Indicates whether to enable the WAN connection.
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 dual stack**.
Mode	Indicates the WAN interface mode. It can be set to **Bridge WAN** or **Route WAN**.
Service List	Indicates the service type of the WAN interface. It is always set to **INTERNET**.
Enable VLAN	Selects this check box to set VLAN ID and 802.1p priority.
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 OLT.
802.1p policy	Indicates the 802.1p priority policy. • Use 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. • Dscp Pbit Mapping: indicates the priority displayed in the DSCP to 802.1p mapping table. The DSCP field is 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.
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 Layer 2/3 Port Configuration, 2.4G Basic Network Settings and 5G Basic Network Settings.

Parameter	Description
Multicast VLAN ID	The multicast VLAN ID ranges from 1 to 4094. The multicast VLAN ID must be the same as the multicast VLAN ID on the OLT.

NOTE:

- WAN in route mode: The ONT functions as a gateway. The IP address of the ONT can be obtained through DHCP, Static, or PPPoE. The IP address of the PC connected to the ONT can be obtained from the DHCP address pool of the ONT or can be set manually.
- WAN in bridge mode: The ONT functions as a relay and does not process data. The ONT 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 ONT 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

Copyright © Huawei Technologies Co., Ltd.

1.6.2 LAN Configuration

This topic describes how to configure the LAN port or DHCP Parameters through the Web page.

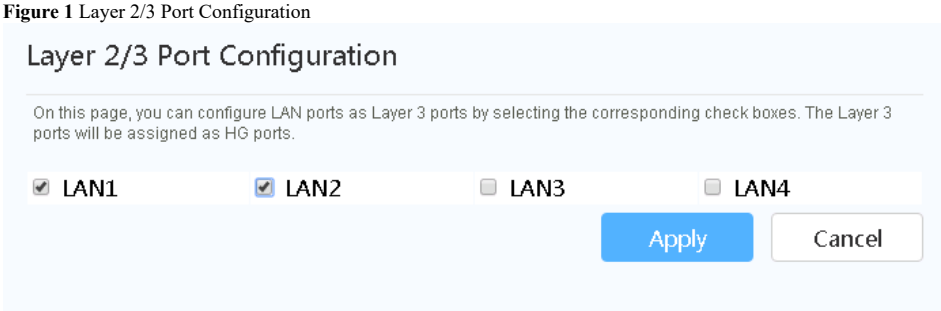
Parent Topic: Advanced Configuration

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.6.2.1 Layer 2/3 Port Configuration

1. In the navigation tree on the left, choose **Advanced Configuration** > **LAN Configuration** > **Layer 2/3 Port Configuration**. In the pane on the right, determine whether the LAN port works in layer 3 mode, as shown in Figure 1.

   Figure 1 Layer 2/3 Port Configuration

   NOTE:

   If the check box corresponding to the LAN port is selected, it indicates that the LAN port works in layer 3 mode, that is, the gateway mode; if the check box corresponding to the LAN port is deselected, it indicates that the LAN port works in layer 2 mode, that is, the bridge mode.

   By default, the check boxes corresponding to all LAN ports are deselected, that is, all LAN ports work in layer 2 mode.

2. Click **Apply**.

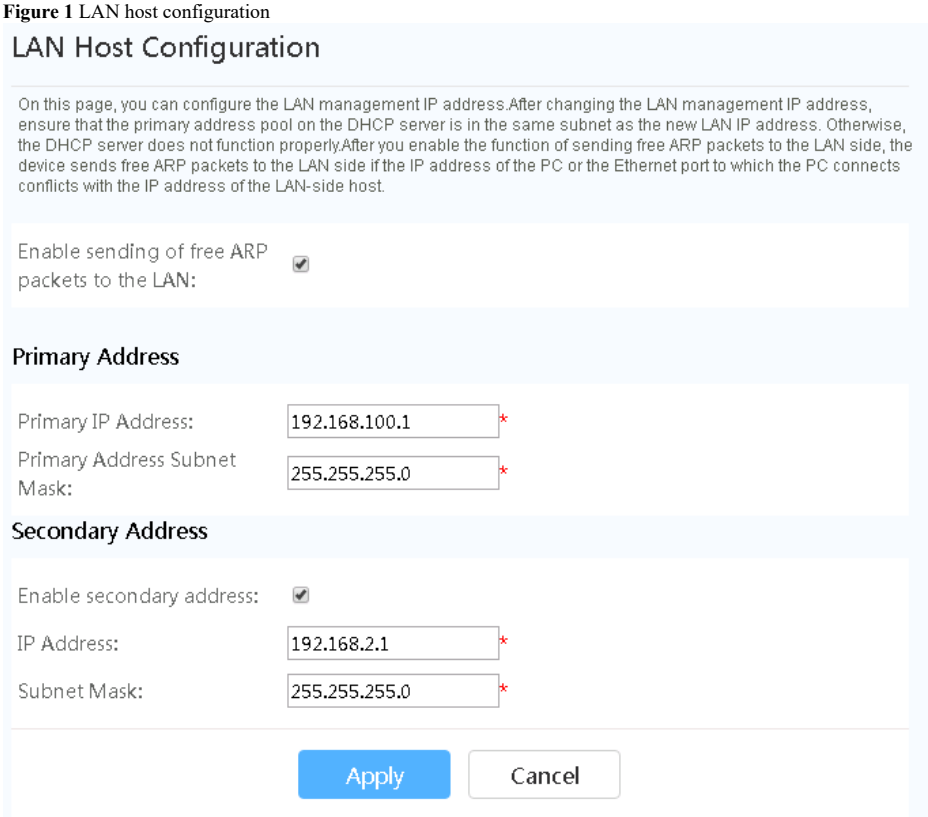
Parent Topic: LAN Configuration

Copyright © Huawei Technologies Co., Ltd.
Next topic >

1.6.2.2 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, set the management IP address of Primmary 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 an ONT through the Web page and perform the query and management.

2. Click **Apply**.

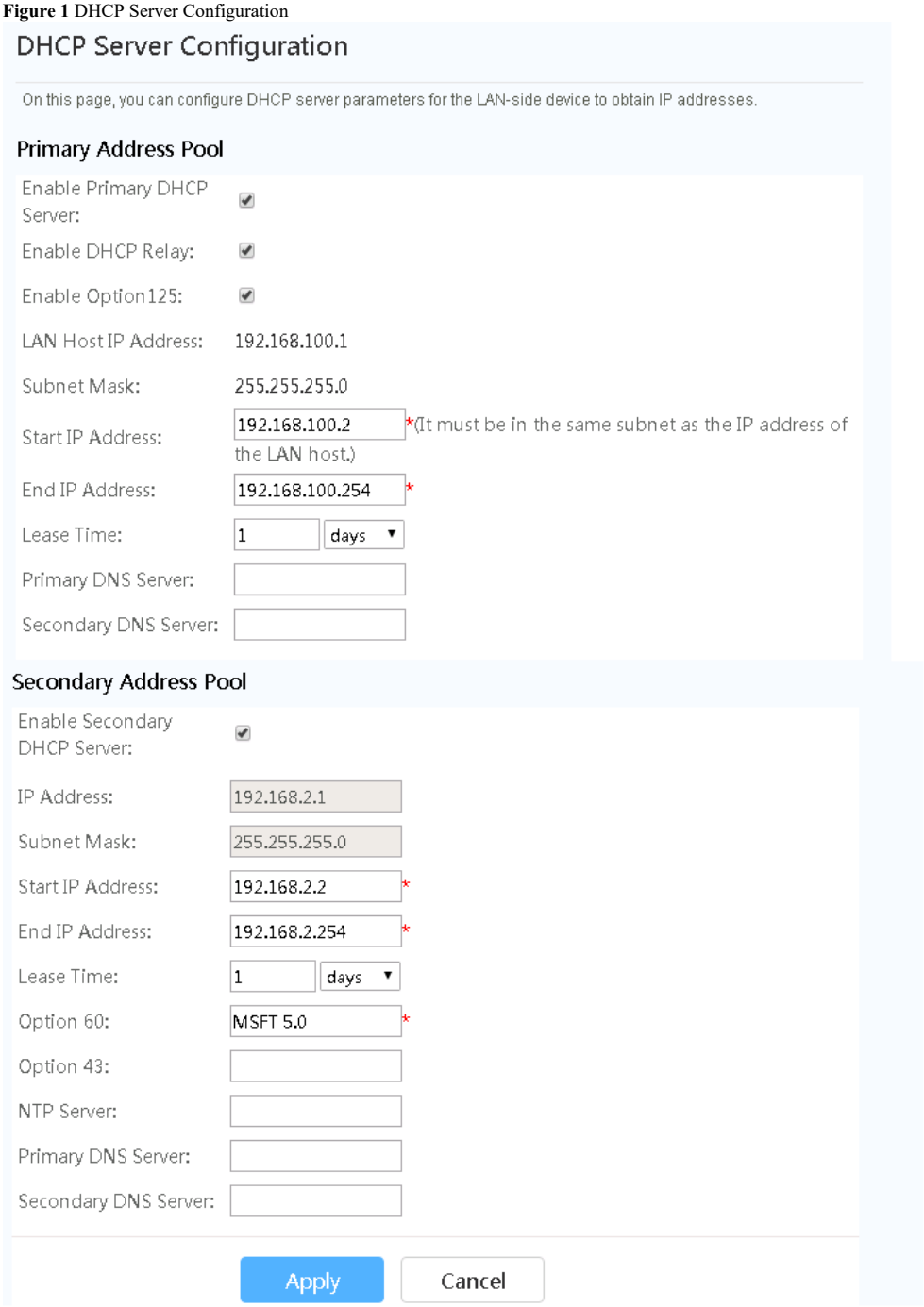
Parent Topic: LAN Configuration

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.6.2.3 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 ONT 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
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 L2 Relay	Indicates whether to enable the DHCP L2 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 **Mode** of the WAN port is **Route**, the IP address of the ONT 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 ONT. • If **Mode** of the WAN port is **Bridge**, the ONT functions as a bridge. In this way, the ONT does not have an IP address. The user-side IP addresses are obtained from upper-layer DHCP servers in different subnets.
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.

Parameter	Description
Leased Time	Indicates the lease time of the IP address pool on the active DHCP server. Options: minute, hour, day, and week.
Enable secondary DHCP 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.
Leased Time	Indicates the lease time of the IP address pool on the secondary DHCP server. Options: minute, hour, day, and week.
Option60	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.
Option43	Indicates the option 43 field of the secondary DHCP server, identifying a TFTP server.
NTP Server	Inputs the IP address of the NTP server.
Primary DNS Server	Inputs the IP address of the primary DNS server.
Secondary DNS Server	Inputs the IP address of the secondary DNS server.

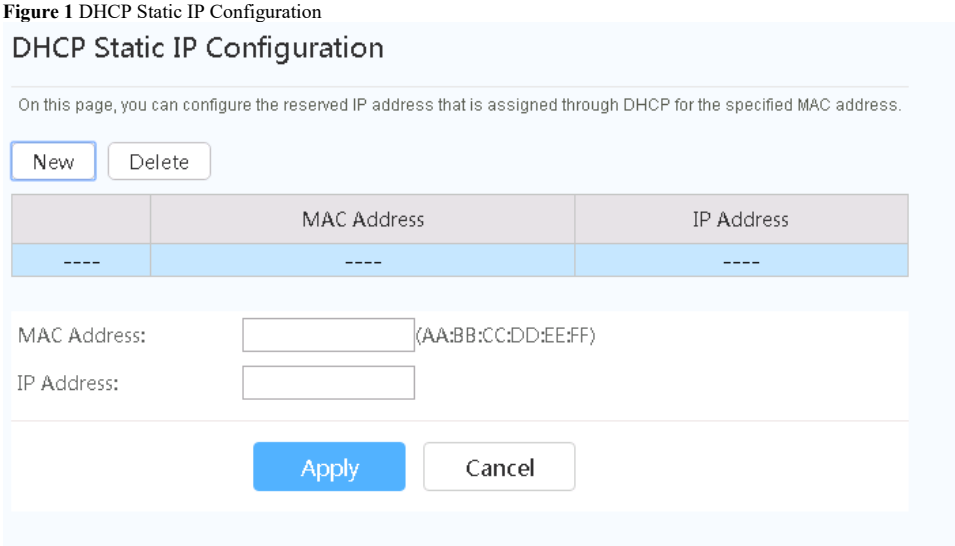
Parent Topic: LAN Configuration

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.6.2.4 DHCP Static IP Configuration

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

Figure 1 DHCP Static IP Configuration



2. Click **Apply**.

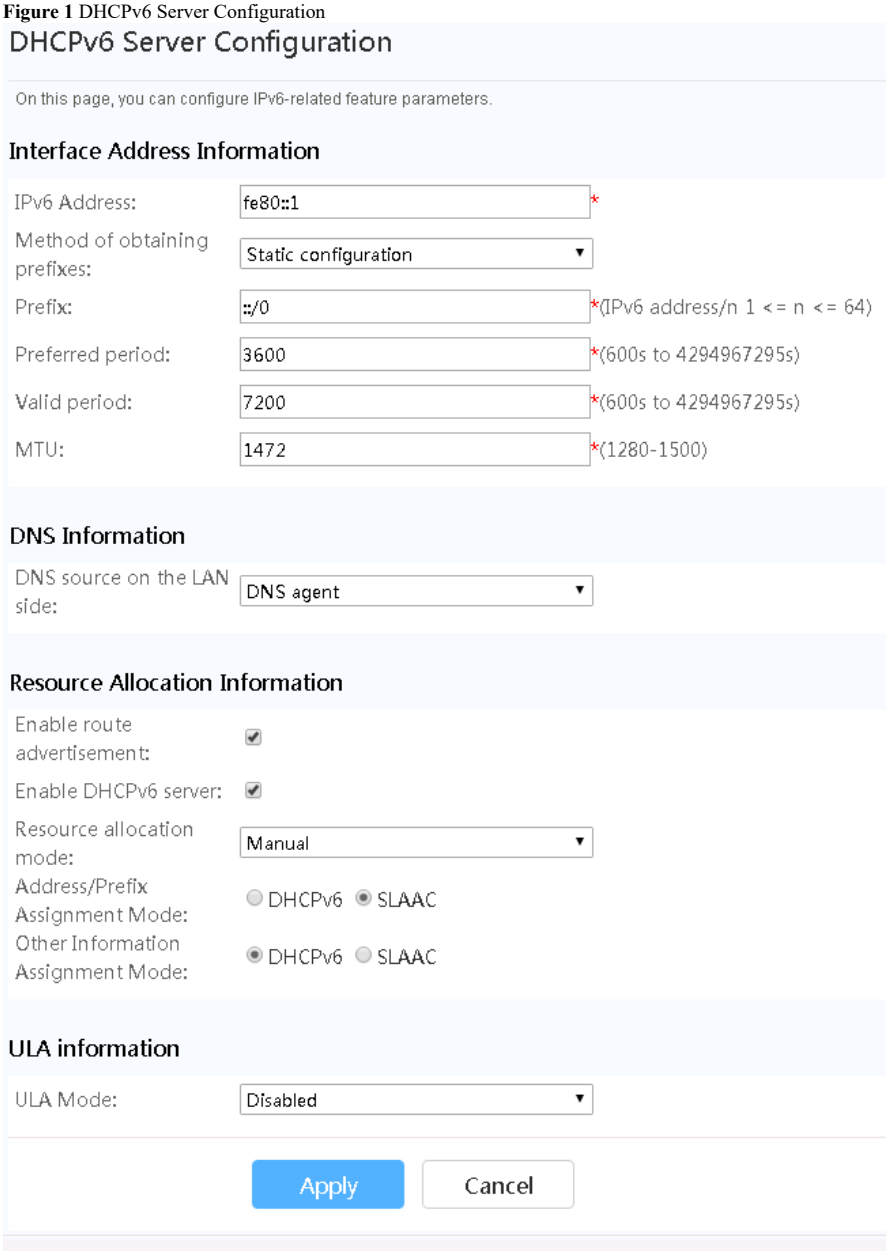
Parent Topic: LAN Configuration

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.6.2.5 DHCPv6 Server Configuration

1. In the navigation tree on the left, choose **Advanced Configuration** > **LAN Configuration** tab, and choose **DHCPv6 Server Configuration** from the navigation tree on the left. In the pane on the right, you can configure the LAN side address pool for the ONT that functions as a gateway, 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

Parameters	Description
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** > **LAN Host Configuration**.
Parent prefix	Indicates the parent prefix source. Usually an Internet-type WAN port is used as the parent prefix source. By default, the first created IPv6 Internet WAN port is used as the parent prefix source. If the value is left empty, no prefix will be obtained, which may result in service unavailability.
Child prefix mask	Used for LAN IP address allocation. This parameter needs to be configured when the obtained prefix is shorter than 64 bits. For example, if the obtained prefix is 2001:db8:2222::/48, and the child prefix mask value is set to 2001:db8:1:3333::/64, the generated IPv6 address prefix is2001:db8:2222:3333::/64.
Address/Prefix assignment mode	Indicates the address/prefix assignment mode. It can be set to DHCPv6 or stateless address autoconfiguration (SLAAC). 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. • DHCPv6: indicates that the address is obtained in DHCPv6 mode. • SLAAC: indicates that the address is obtained in ND mode.

Parameters	Description
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 **Prohibit**. **Prohibit** is recommended. • Prohibit: 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:db8: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:db8: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.

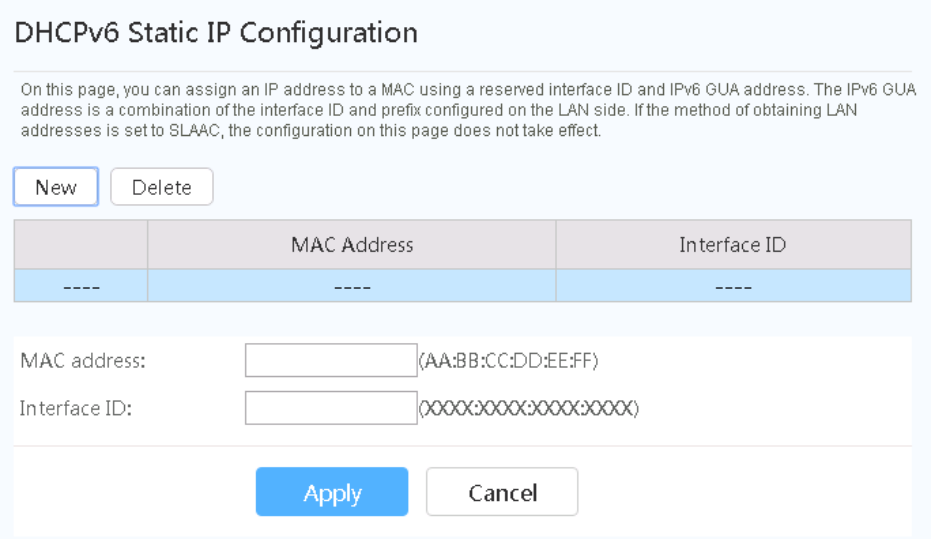
Parent Topic: LAN Configuration

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.6.2.6 DHCPv6 Static IP Configuration

Click **Advanced Configuration** > **LAN Configuration**tab, and choose **DHCPv6 Static IP Configuration** from the navigation tree on the left. In the pane on the right, 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



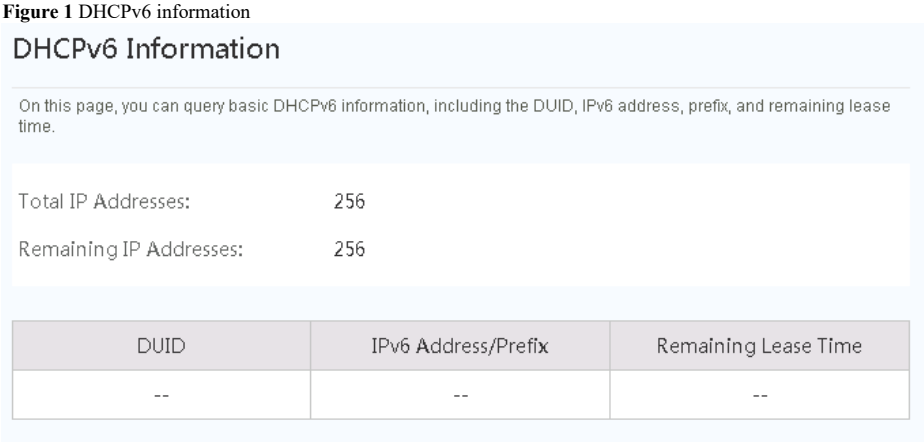
Parent Topic: LAN Configuration

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.6.2.7 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, and IPv6 address/prefix, as shown in Figure 1.

Figure 1 DHCPv6 information



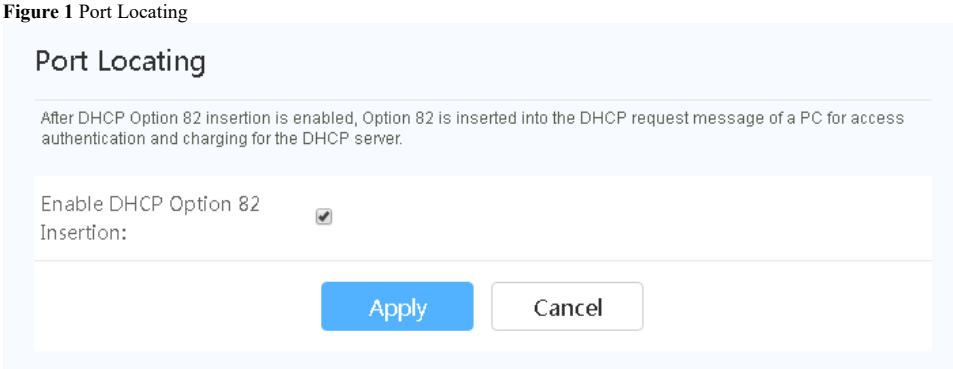
Parent Topic: LAN Configuration

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.6.2.8 Port Locating

1. Click **Advanced Configuration** > **LAN Configuration** tab, and choose **Port Locating** in the navigation tree on the left. In the pane on the right, determine whether to enable the **DHCP Option 82 Insertion** function, as shown in Figure 1.

   Figure 1 Port Locating

2. Click **Apply**.

Parent Topic: LAN Configuration

Copyright © Huawei Technologies Co., Ltd.
< Previous topic

1.6.3 Security Configuration

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

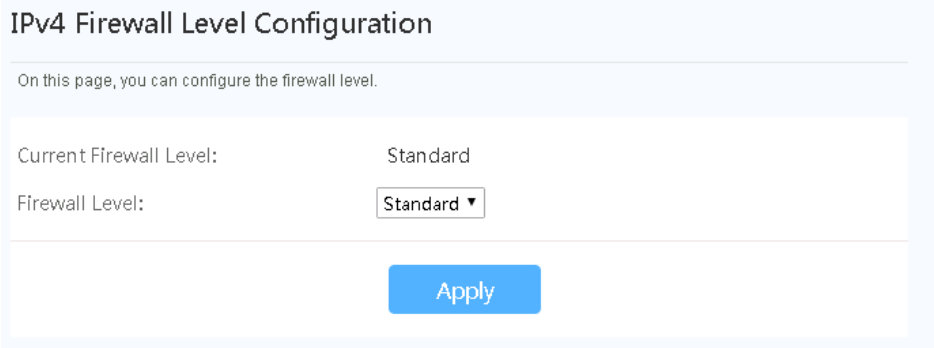
Parent Topic: Advanced Configuration

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.6.3.1 IPv4 Firewall Level Configuration

1. Click the **Advanced Configuration** > **Security Configuration** tab, and choose **IPv4 Firewall Level Configuration** from the navigation tree on the left. In the right pane, set the firewall level, as shown in Figure 1.

Figure 1 IPv4 Firewall level configuration



2. Click **Apply**.

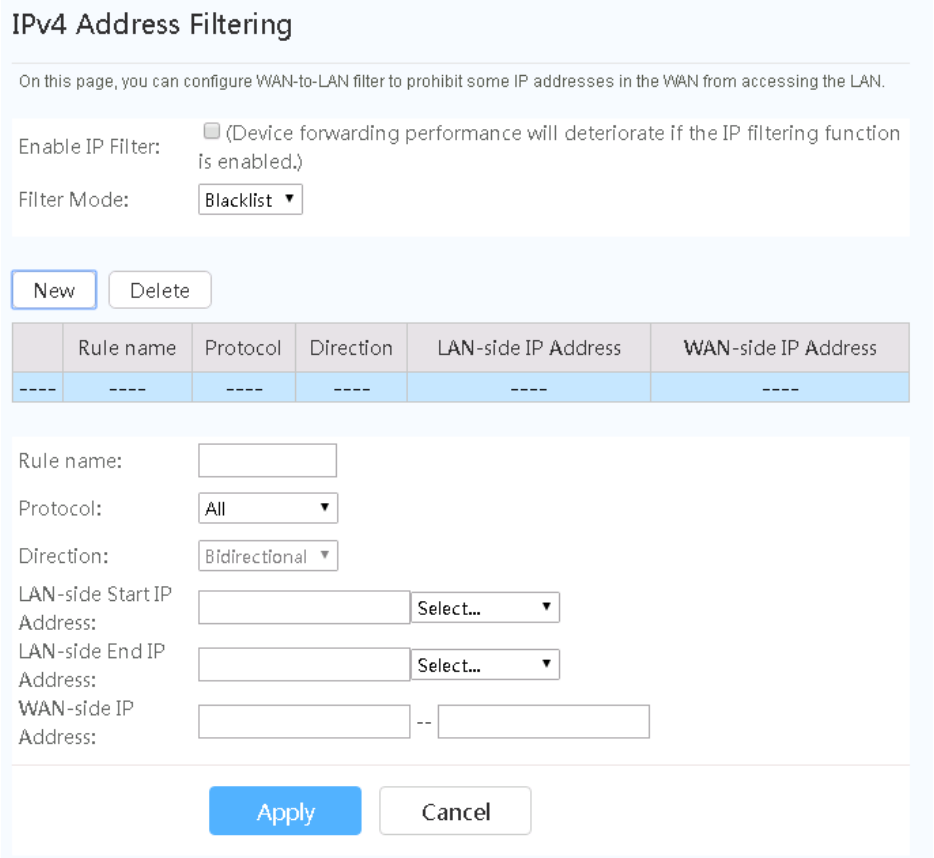
Parent Topic: Security Configuration

Copyright © Huawei Technologies Co., Ltd.
Next topic >

1.6.3.2 IPv4 Address Filtering

1. Click **Advanced Configuration** > **Security Configuration** tab, and choose **IPv4 Address Filtering** in the navigation tree on the left. In the pane on the right, enable the IP address filter function. After selecting the filter mode, click **New**. Then, in the dialog box that is displayed, 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**.

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.

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.

Parameter	Description
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.
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.
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 IP Address	Indicates the IP address on the WAN side.
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**.
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.

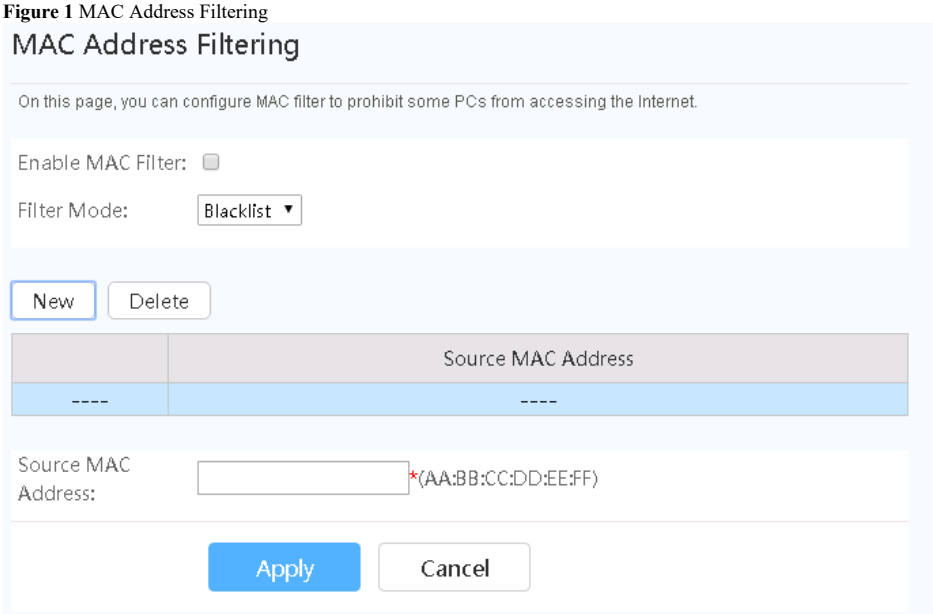
Parent Topic: Security Configuration

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.6.3.3 MAC Address Filtering

1. Click **Advanced Configuration** > **Security Configuration** tab, and choose **MAC Address Filtering** in the navigation tree on the left. In the pane on the right, after enabling MAC filter and selecting the filter mode, click **New**. On the dialog box that is displayed, 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**.

The MAC address lists of PCs in the network are saved on the ONT. 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.

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 rule of the blacklist or whitelist. • Blacklist: indicates that the data meeting the rule in the filter rule list is not allowed to pass. • Whitelist: indicates that the data meeting the rule in the filter rule list is allowed to pass. The filter mode is global config mode. Thus, the blacklist and whitelist mode cannot be used at the same time.
Source MAC Address	Indicates the source MAC address in the MAC address filter rule.

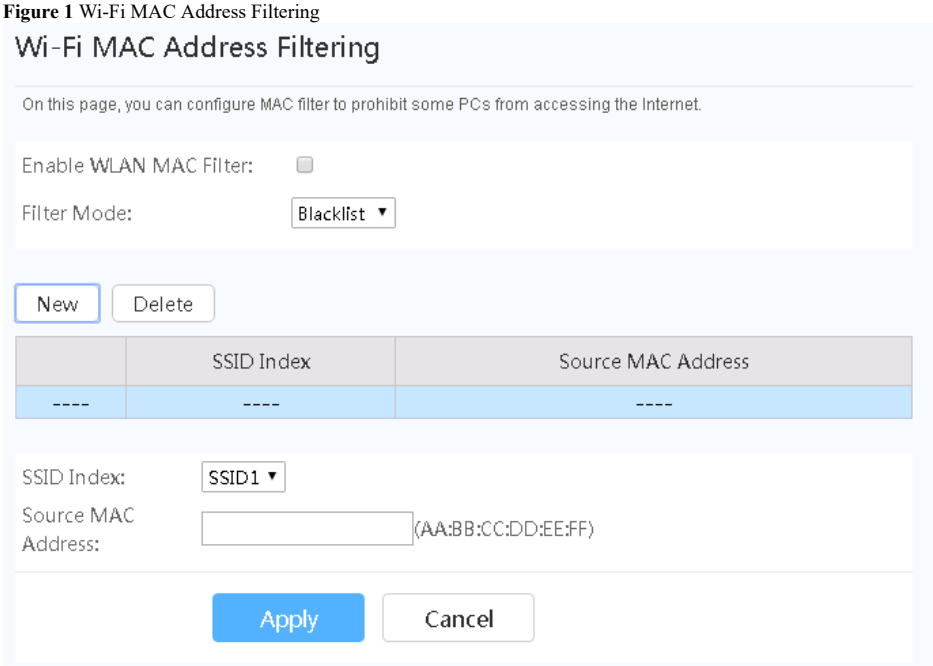
Parent Topic: Security Configuration

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.6.3.4 Wi-Fi MAC Address Filtering

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

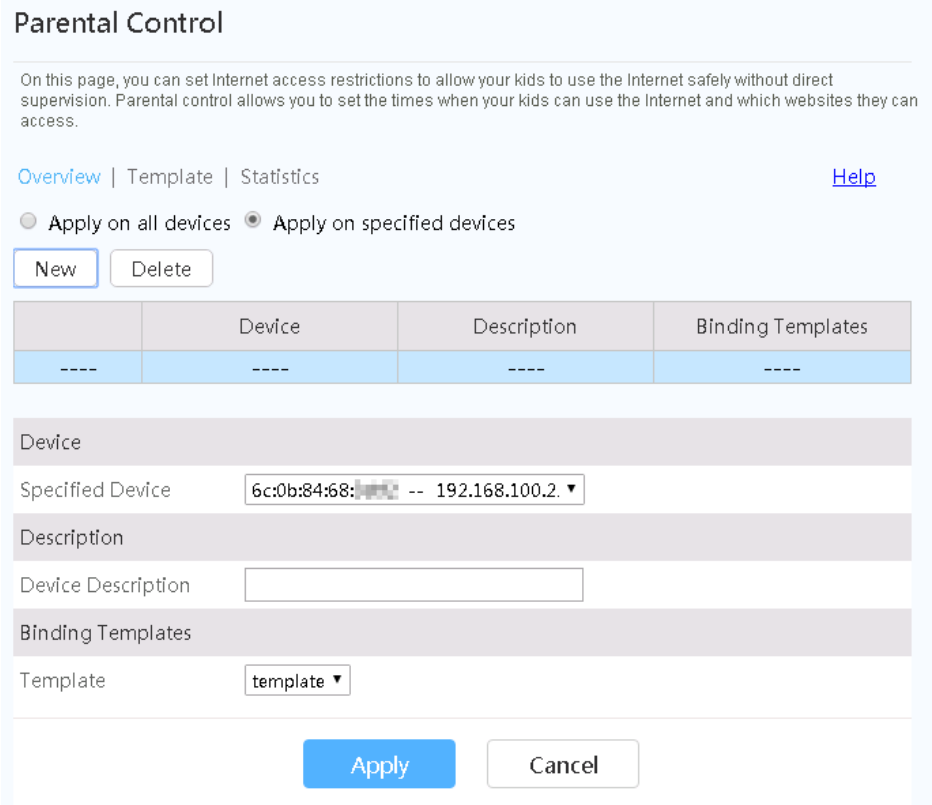
Parent Topic: Security Configuration

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.6.3.5 Parental Control

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

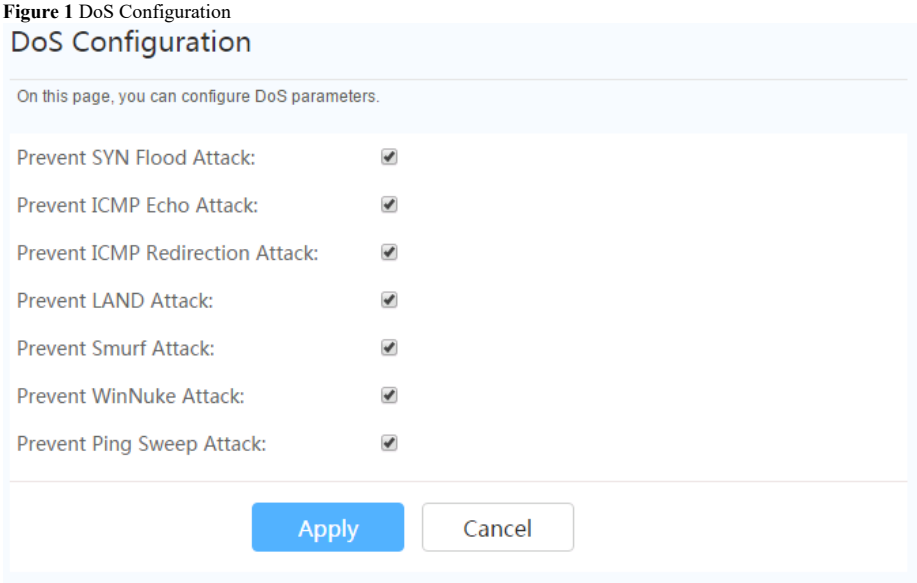
Parent Topic: Security Configuration

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.6.3.6 DoS Configuration

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

Figure 1 DoS Configuration



2. Click **Apply**.

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.

Table 1 describes the parameters related to the DoS.

Table 1 Parameters related to the DoS

Parameter	Description
Prevent SYN Flooding Attack	Indicates whether to enable the prevent SYN flooding attack. In the attack, several source hosts send SYN packets to a destination host. After receiving the SYN ACK packets from the destination host, the source hosts do not respond. In this case, the destination host establishes many connection queues for the source hosts and maintains these queues all the time because no ACK response is received. As a result, many resources are used and the destination host fails to provide normal services for normal connections.
Prevent ICMP Echo Attack	Indicates whether to enable the prevent ICMP echo attack. In the attack, many ICMP echo packets are sent to a destination host within a short time. As a result, the network is congested or the resources of the host are exhausted.
Prevent ICMP Redirect Attack	Indicates whether to enable the prevent ICMP redirect attack. In the attack, many ICMP redirect packets are sent to a destination host within a short time. As a result, the network is congested or the resources of the host are exhausted.

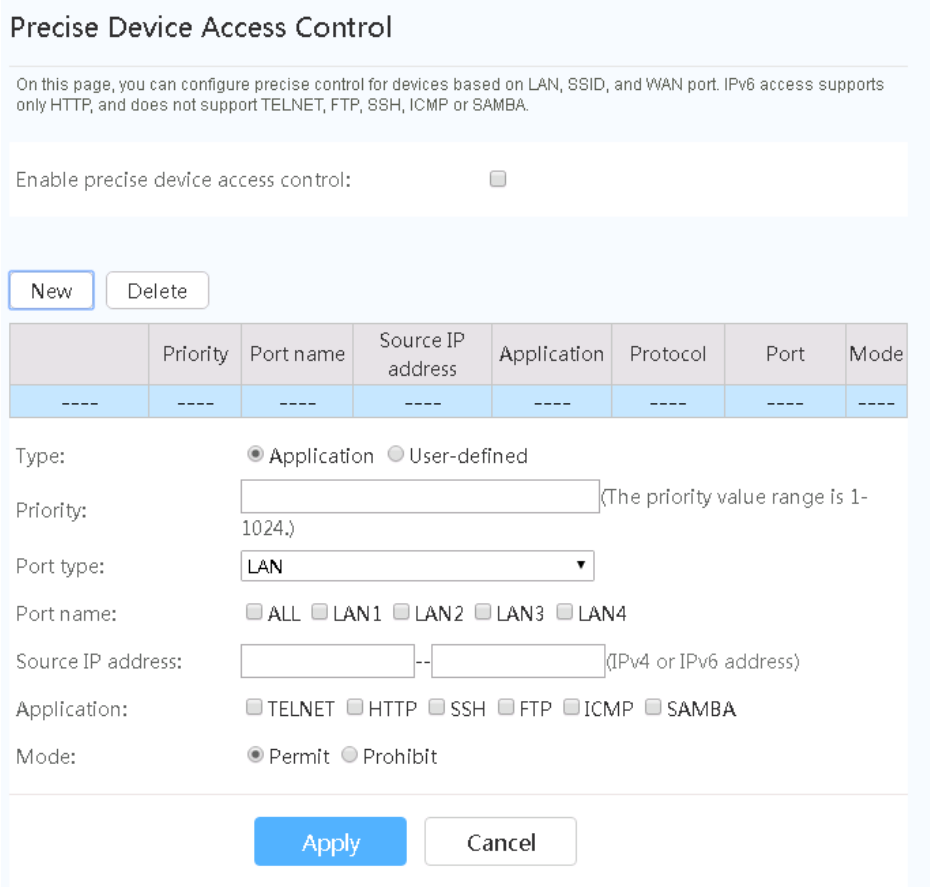
Parent Topic: Security Configuration

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.6.3.7 Precise Device Access Control

Click **Advanced Configuration** > **Security Configuration** tab, and choose **Precise Device Access Control** in the navigation tree on the left. Click **New**. In the displayed window, set LAN port, SSID or WAN port information, including **Priority**, **Protocol** and **Mode**,as shown in Figure 1.

Figure 1 Parental Control



Parent Topic: Security Configuration

Copyright © Huawei Technologies Co., Ltd.

< Previous topic Next topic >

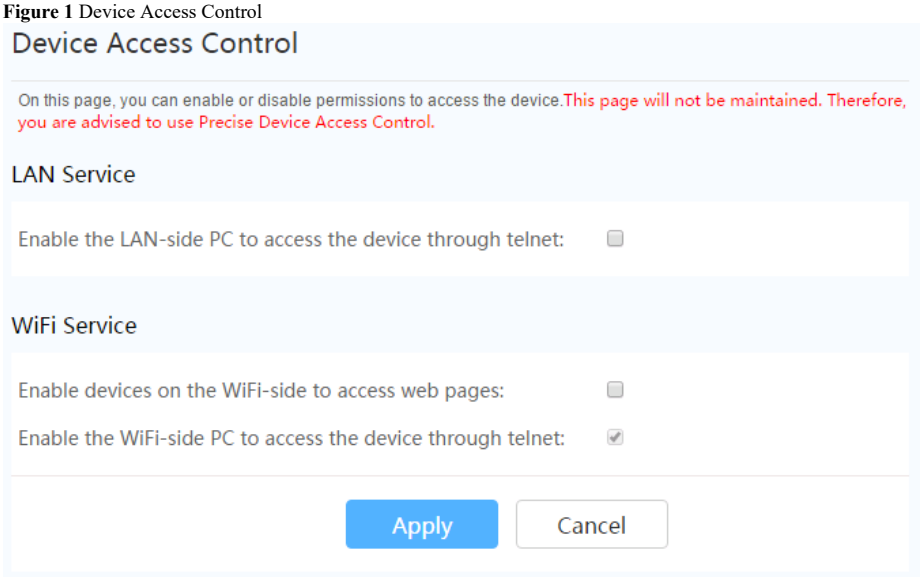
1.6.3.8 Device Access Control

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

DANGER

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

Figure 1 Device Access Control



2. Click **Apply**.

Parent Topic: Security Configuration

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

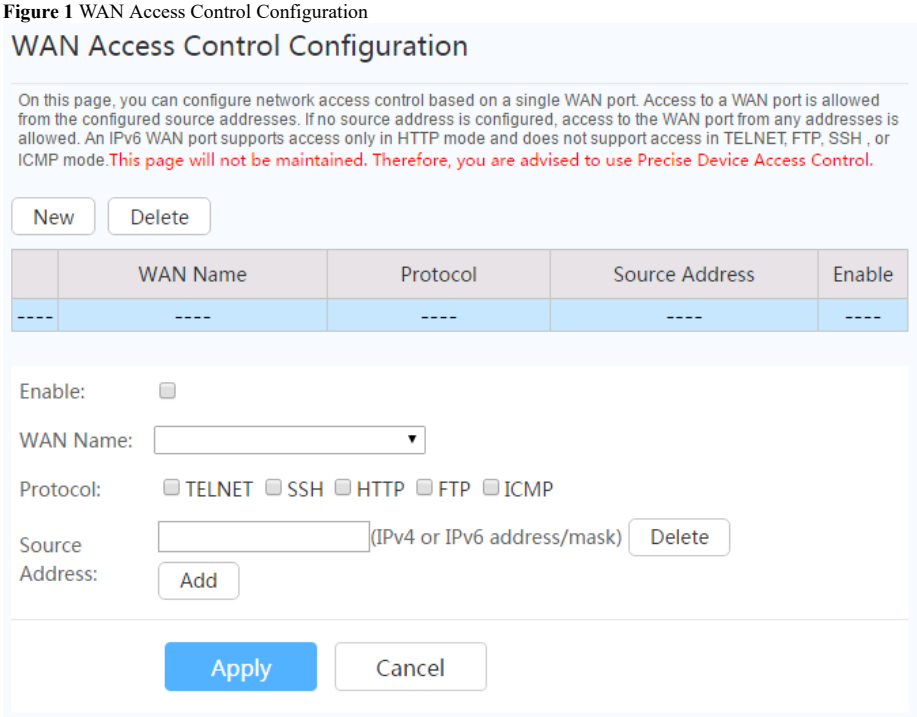
1.6.3.9 WAN Access Control Configuration

1. In the navigation tree on the left, choose **Security Configuration** > **WAN Access Control Configuration**. In the pane on the right, click **New**. In the dialog box that is displayed, set the parameters of the WAN access control, as shown in Figure 1

DANGER

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

Figure 1 WAN Access Control Configuration



2. Click **Apply**.

Parent Topic: Security Configuration

Copyright © Huawei Technologies Co., Ltd.
< Previous topic

1.6.4 Route

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

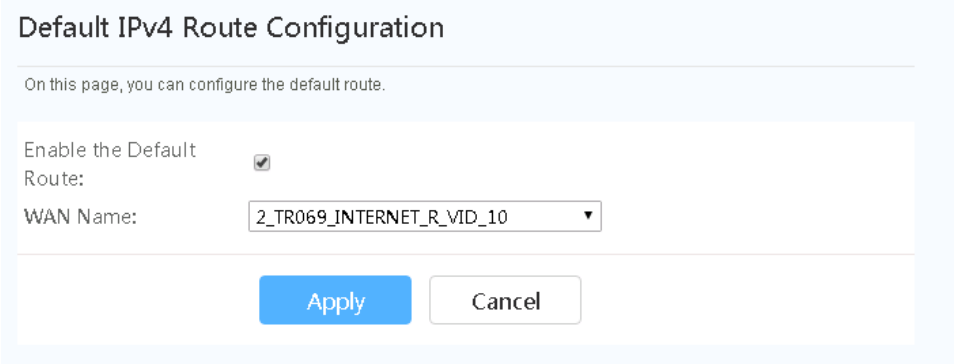
Parent Topic: Advanced Configuration

Copyright © Huawei Technologies Co., Ltd.
< 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, select or deselect 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 an ONT 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**.

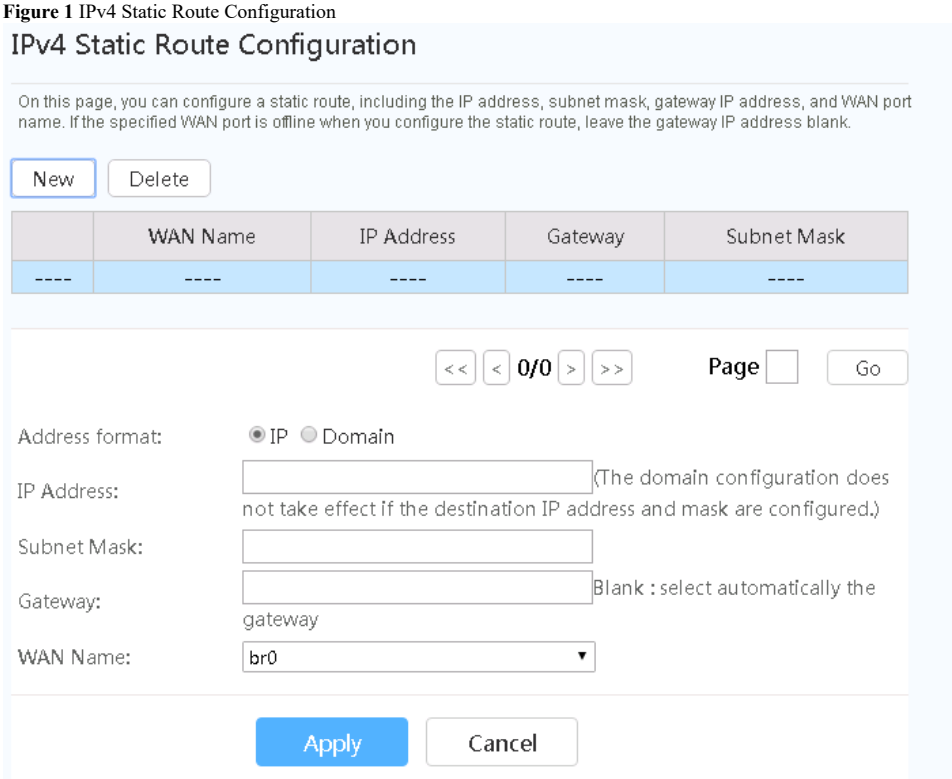
Parent Topic: Route

Copyright © Huawei Technologies Co., Ltd.
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, 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**.
Domain name	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.

Parameter	Description
Subnet Mask	Indicates the subnet mask of the static route.
Gateway	Indicates the gateway IP address of the static route.
WAN Name	Indicates the WAN interface that the route travels through.

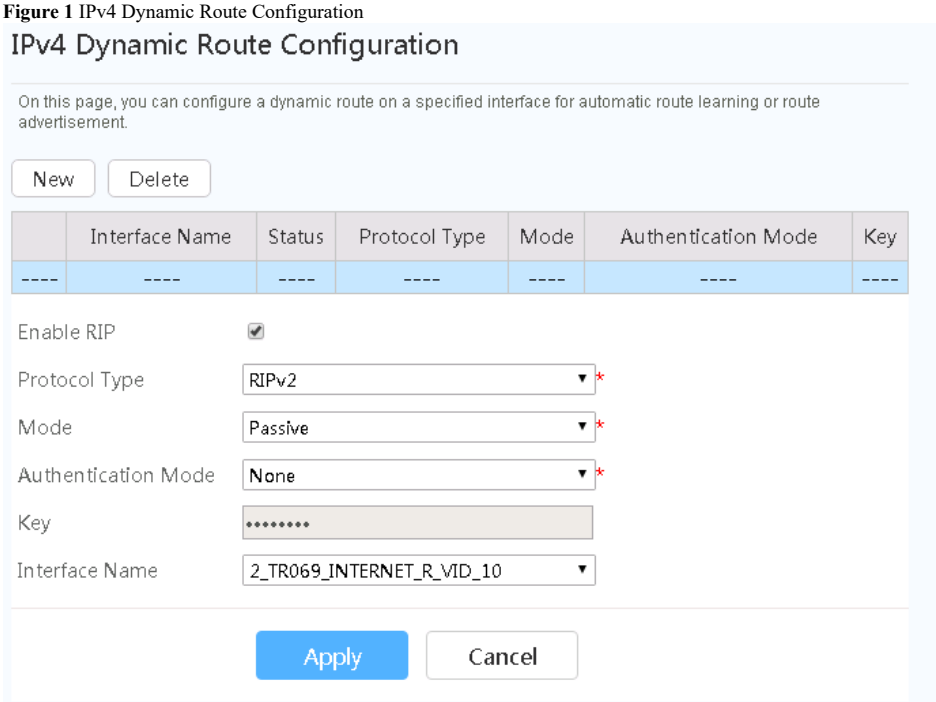
Parent Topic: Route

Copyright © Huawei Technologies Co., Ltd.
< 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, 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**. **NOTE:** When the authentication mode is **Plaintext**, the input plaintext is displayed as asterisks (*).
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.

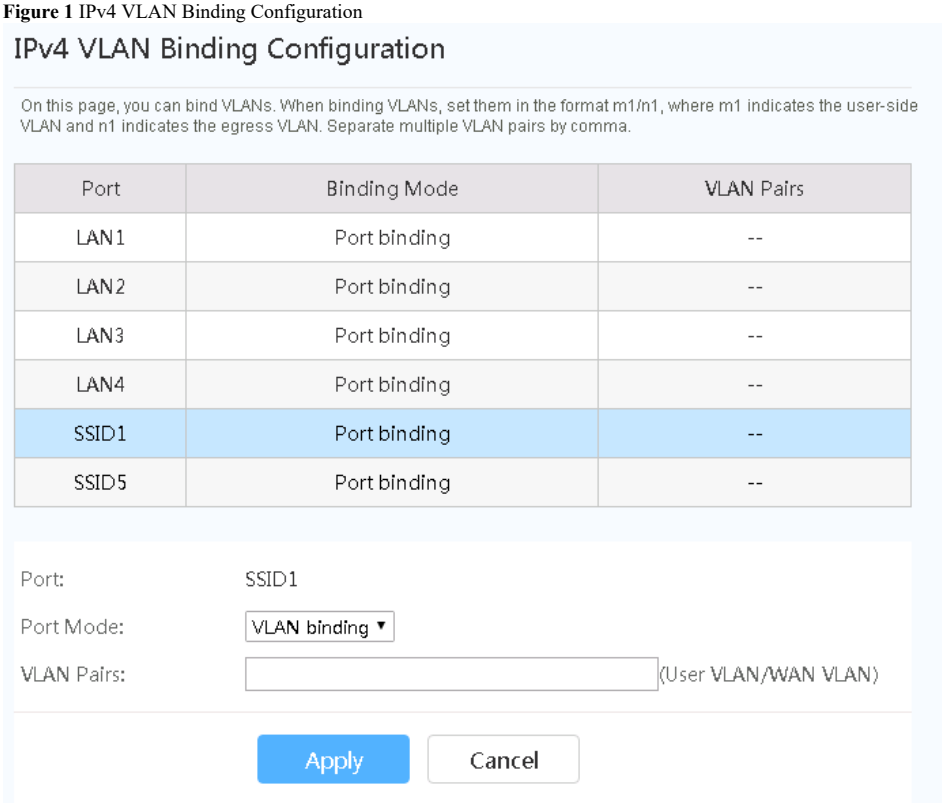
Parent Topic: Route

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.6.4.4 IPv4 VLAN Binding Configuration

1. Click the **Advanced Configuration** > **Route** tab and then choose **IPv4 VLAN Binding Configuration** from the navigation tree. In the right pane, Click to need to configure the port VLAN binding column in the tab to set the port VLAN binding relationship, as shown in Figure 1.

Figure 1 IPv4 VLAN Binding Configuration



2. Click **Apply**.

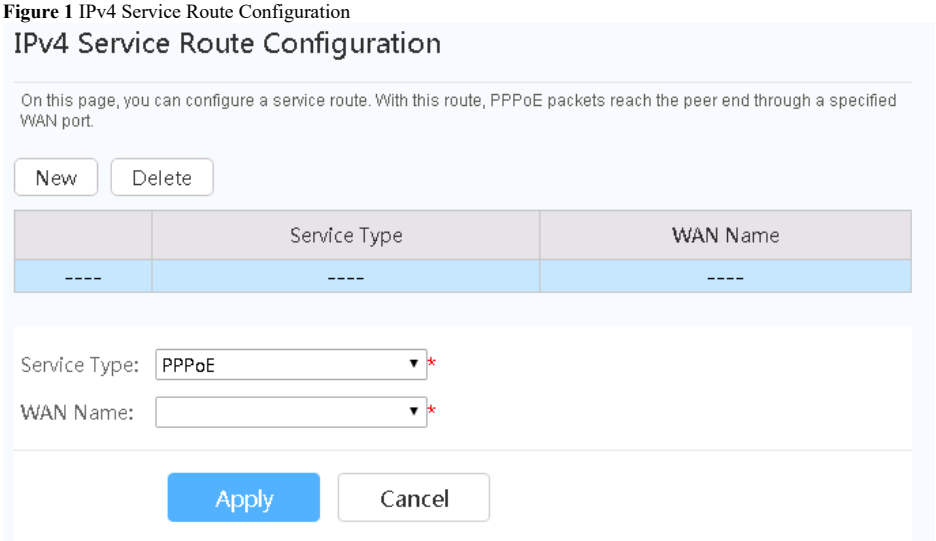
Parent Topic: Route

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.6.4.5 IPv4 Service Route Configuration

1. Click the **Advanced Configuration** > **Route** tab. In the navigation tree on the left, choose **IPv4 Service Route Configuration**. In the right pane, click **New**. In the dialog box that is displayed, set related service route parameters, as shown in Figure 1.

Figure 1 IPv4 Service Route Configuration



NOTE:

The configuration takes effect when the device works in the bridge mode, and the corresponding WAN must be bridging-type WAN.

2. Click **Apply**.

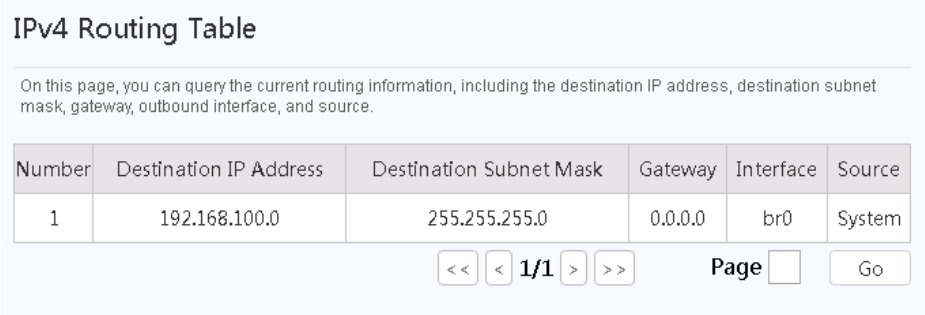
Parent Topic: Route

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.6.4.6 IPv4 Routing Table

Click the **Advanced Configuration** > **Route** tab, and choose **IPv4 Routing Table** from the navigation tree on the left. In the right pane, 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



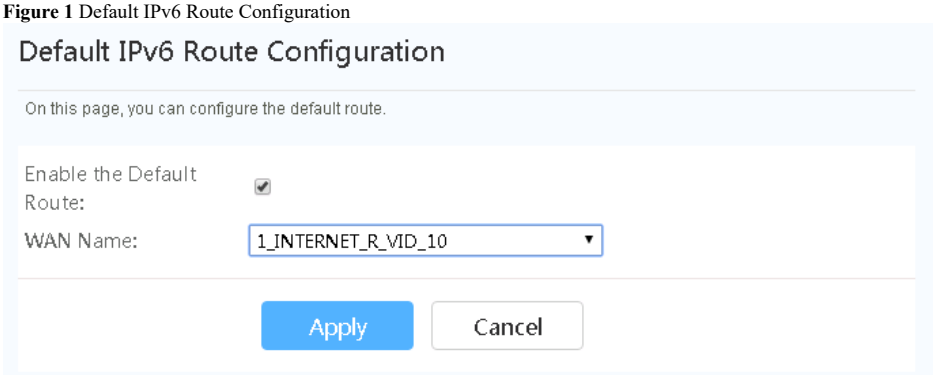
Parent Topic: Route

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.6.4.7 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, 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 an ONT 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**.

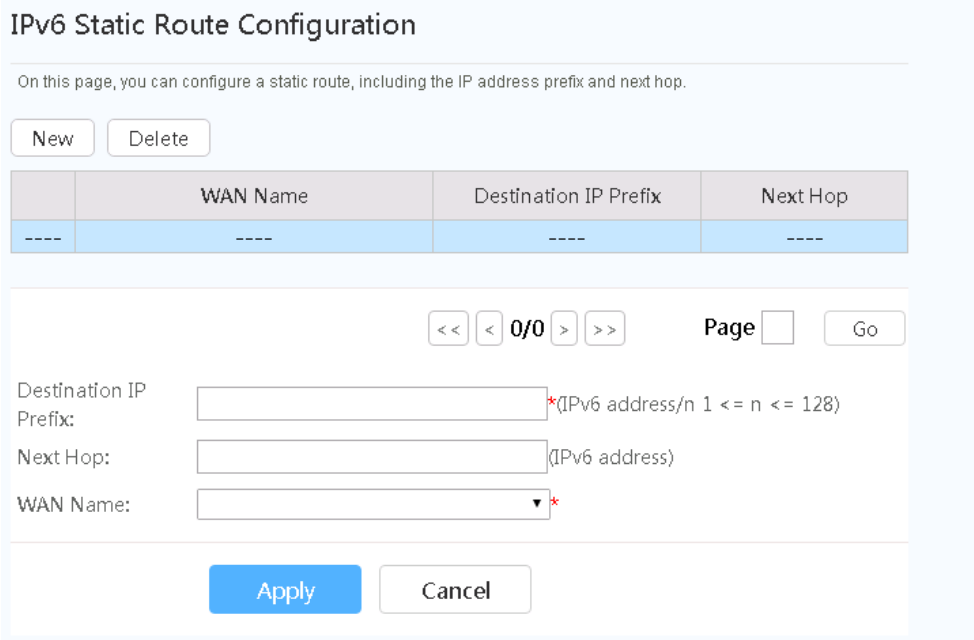
Parent Topic: Route

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.6.4.8 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, 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

Copyright © Huawei Technologies Co., Ltd.
< Previous topic

1.6.5 Forward Rules

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

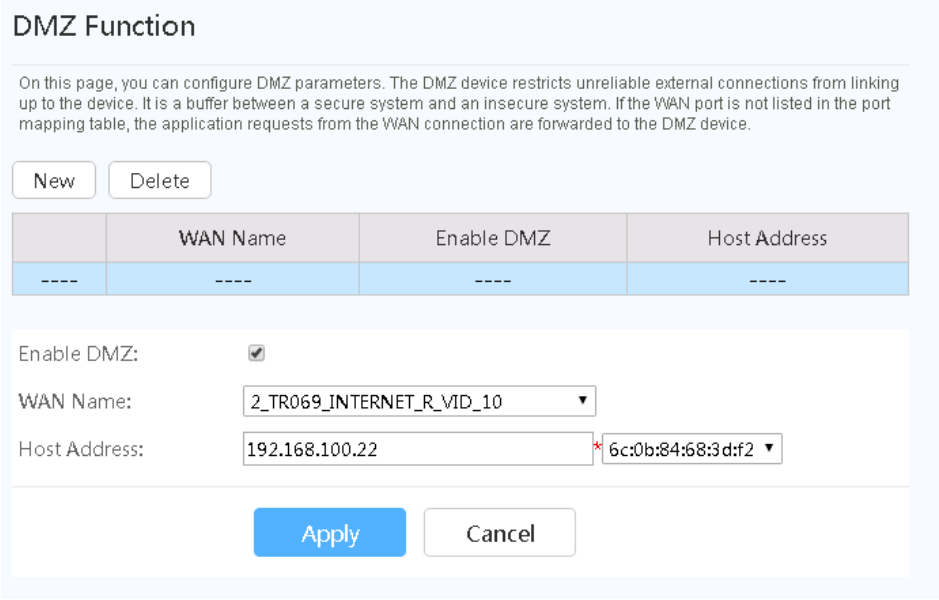
Parent Topic: Advanced Configuration

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.6.5.1 DMZ Function

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

Figure 1 DMZ Function



2. Click **Apply**.

The demilitarized zone (DMZ) is a technology that enables the ONT 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.

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

Copyright © Huawei Technologies Co., Ltd.
Next topic >

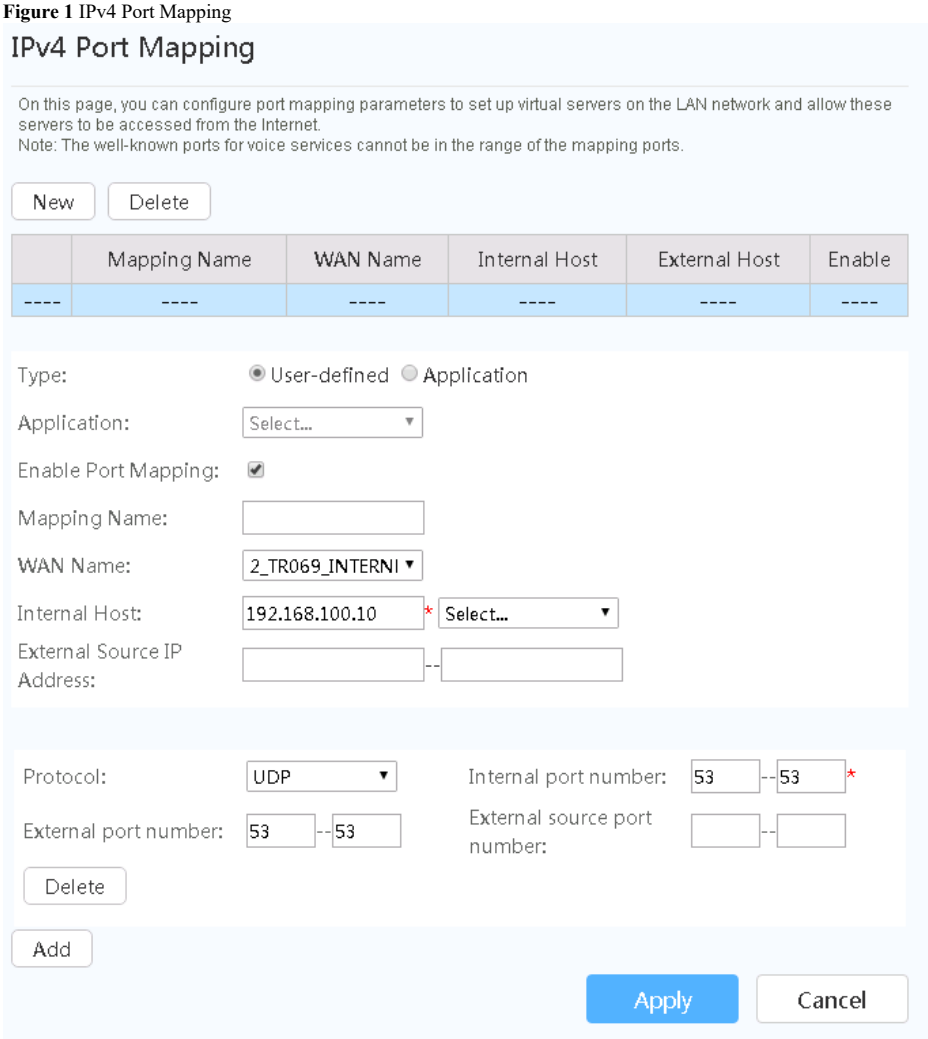
1.6.5.2 IPv4 Port Mapping

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.

Navigation Path

1. Click **Advanced Configuration** > **Forward Rules** tab, and choose **IPv4 Port Mapping**. In the dialog box that is displayed, set the parameters related to port mapping, as shown in Figure 1.

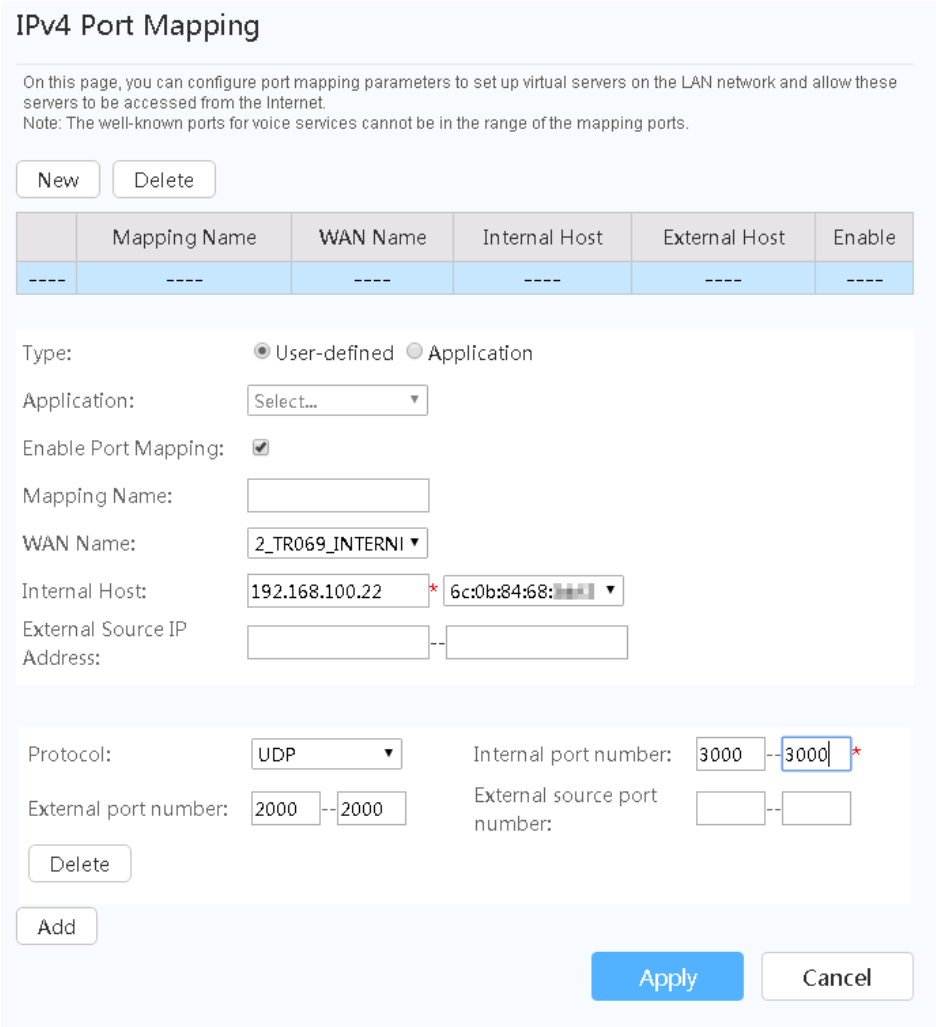
Figure 1 IPv4 Port Mapping



2. Click **Apply**.

Configuration Example

Enable the packets sent from the WAN side to the ONT whose the destination WAN port number is 2000 to be forwarded to the LAN-side PC whose IP address is 192.168.100.20, and the port number is changed to 3000.



Parameter Description

Table 1 describes the parameters related to IPv4 port mapping.

Table 1 Parameters related to IPv4 port mapping

Parameter	Description
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.
Protocol	Indicates the protocol type of port mapping packet, which may be TCP, UDP, or TCP/UDP.
Start External Port	Indicates the destination start port of the external data packet.
End External Port:	Indicates the destination end port of the external data packet.
Start Internal Port	Indicates the internal destination start port of the port mapping packet.
End Internal Port	Indicates the internal destination end port of the port mapping packet.
Start External Source Port	Indicates the source start port of the external data packet.
End External Source Port	Indicates the source end port of the external data packet.
External Source IP Address	Indicates the source IP address of the external data packet.

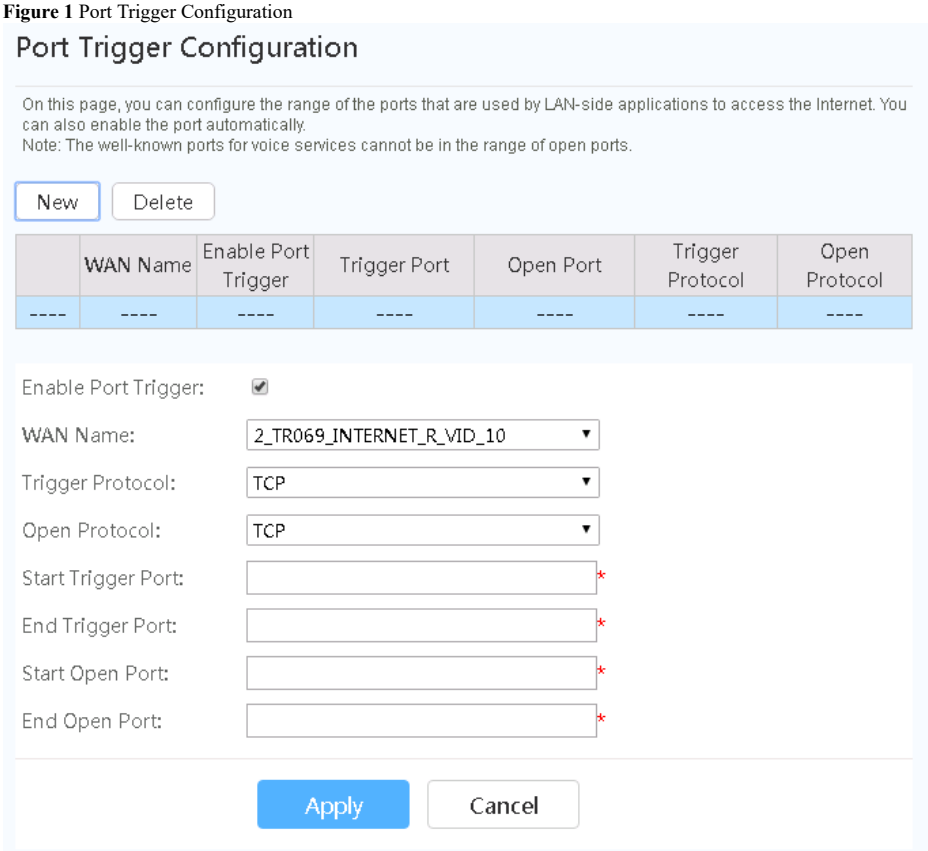
Parent Topic: Forward Rules

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.6.5.3 Port Trigger Configuration

1. Click **Advanced Configuration** > **Forward Rules** tab, and choose **Port Trigger Configuration**. In the pane on the right, click **New**. In the dialog box that is displayed, set the parameters related to the port trigger, as shown in Figure 1.

Figure 1 Port Trigger Configuration



2. Click **Apply**.

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 ONT through the Intranet so that specific packets of the Extranet can be mapped to the corresponding host. A specified port on the gateway firewall is open to some applications for remote access. The port trigger can dynamically enable the open port of the firewall.

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.
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

Copyright © Huawei Technologies Co., Ltd.
< Previous topic

1.6.6 Application

This topic describes how to configure functions such as Time Setting through the Web page.

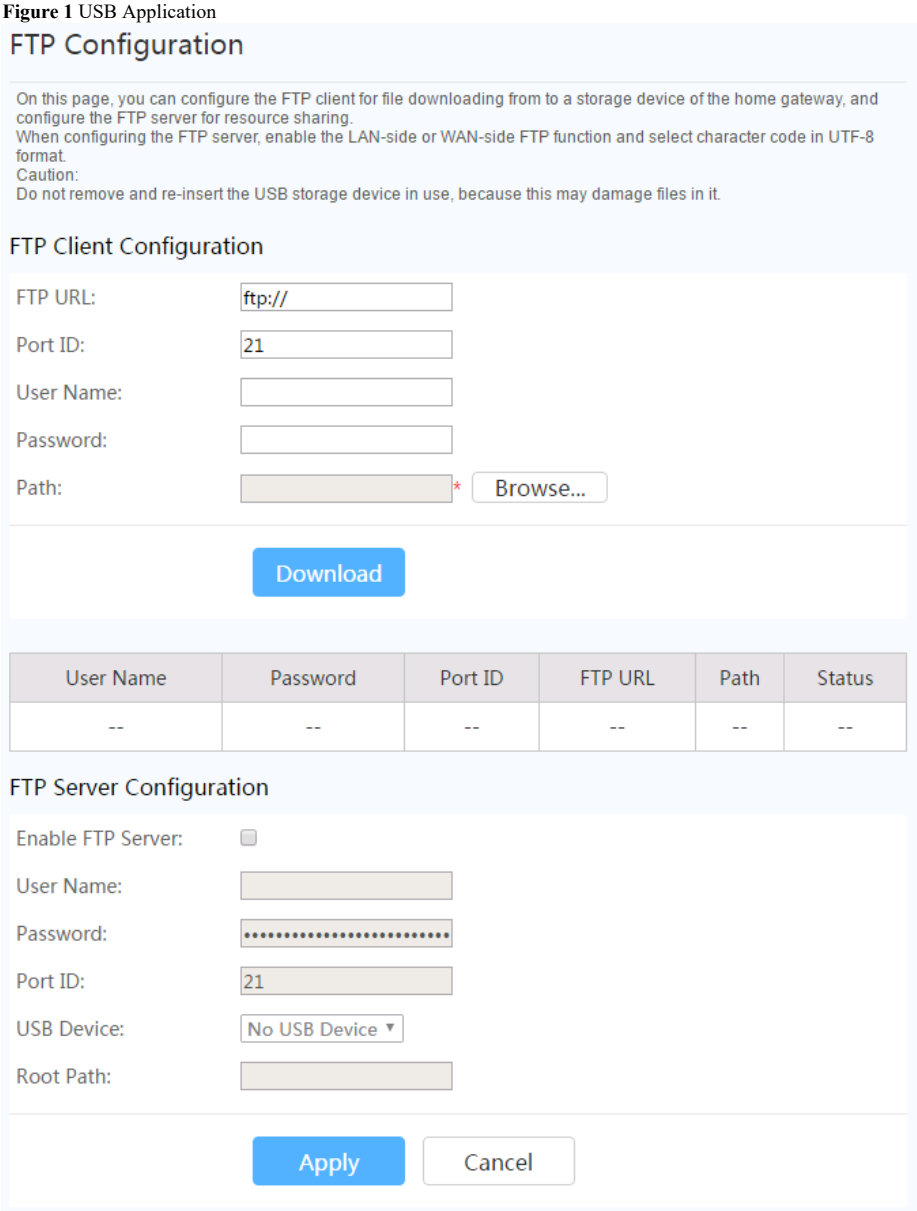
Parent Topic: Advanced Configuration

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.6.6.1 USB Application

1. Click **Advanced Configuration** > **Application** tab, and choose **USB Application** in the navigation tree on the left. In the pane on the right, set the parameters related to FTP downloading to share the FTP file of the ONT, as shown in Figure 1.

Figure 1 USB Application



NOTE:

FTP server configuration supports only English.

The file time of an ONT is in the UNIX format. In Windows OS, the file time displayed may be different from the actual time for FTP access.

Parameter Description

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 path of the file downloaded through FTP.

Parameter	Description
Port ID	Indicates the FTP port number. It is set to 21 by default. Generally, the setting is not required.
User Name	Indicates the user name for connecting to the FTP server. If the FTP server supports anonymous login, the setting is not required.
Password	Indicates the password for connecting to the FTP server. If the FTP server supports anonymous login, the setting is not required.
USB Device	Indicates the drive of the external USB device for saving the file downloaded through FTP. When the USB storage device is connected to the USB port, the drop-down list is available.
Path	Indicates the path for saving the FTP-downloaded file to the external USB device. If the path is not entered, the path specified in Download URL is used by default.
FTP Server Configuration	
Enable FTP Server	Enables the FTP server when the ONT 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.
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 ONT serves as a server.

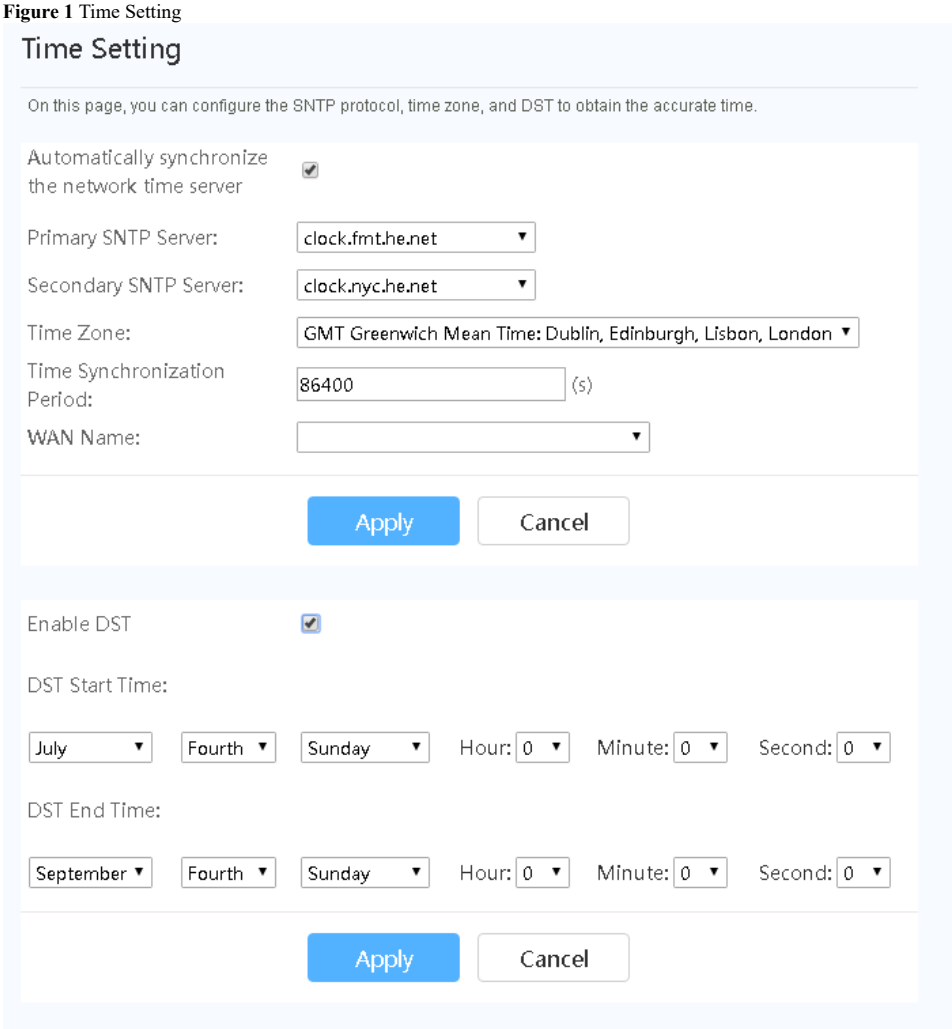
Parent Topic: Application

Copyright © Huawei Technologies Co., Ltd.
Next topic >

1.6.6.2 Time Setting

1. Click **Advanced Configuration** > **Application** tab, and choose **Time Setting** in the navigation tree on the left. In the pane on the right, set the parameters related to the system time, including the SNTP server, time zone, and daylight saving time (DST), as shown in Figure 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
Auto Synchronization 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 Cycle	Indicates whether to enable the DST.
DST Start Time	Indicates the DST start time.
DST End Time	Indicates the DST end time.

NOTE:

If the SNTP server is configured based on domain name format, a static route or a default route must be configured. If the static route or default route is not configured, the ONT will fail to obtain time from the SNTP sever.

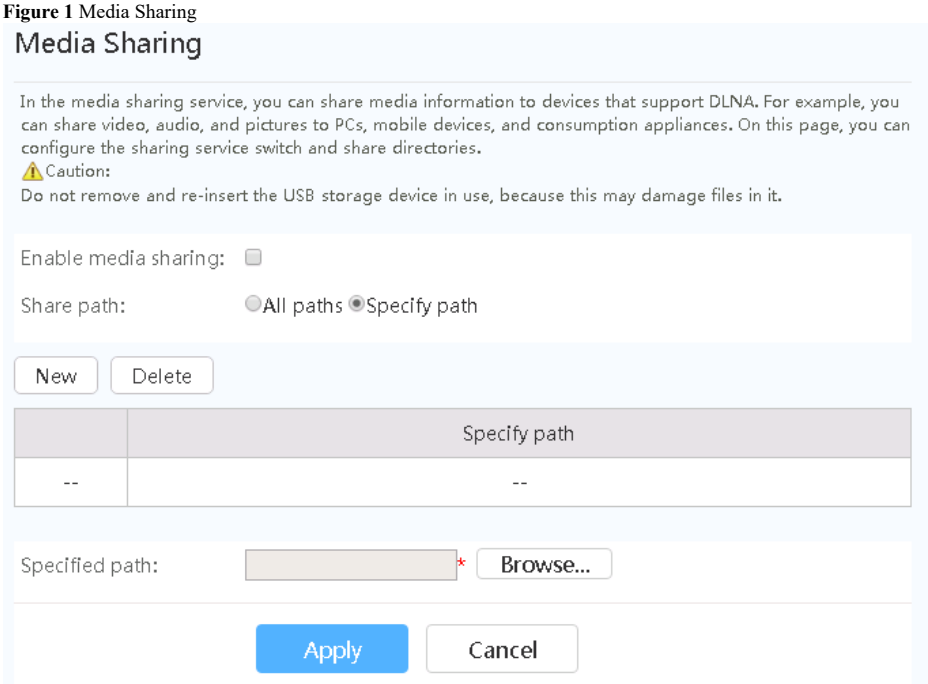
Parent Topic: Application

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.6.6.3 Media Sharing

1. Click **Advanced Configuration** > **Application** tab, and choose **Media Sharing** in the navigation tree on the left. In the right pane, configure the media sharing settings, as shown in Figure 1.

Figure 1 Media Sharing



2. Click **Apply**.

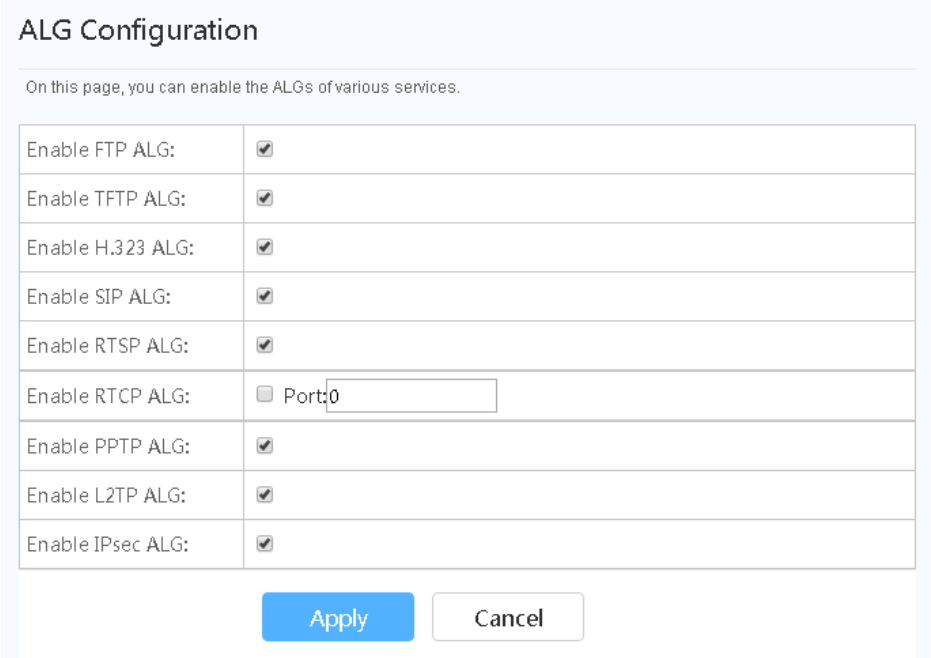
Parent Topic: Application

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.6.6.4 ALG Configuration

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

Figure 1 ALG Configuration



2. Click **Apply**.

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.

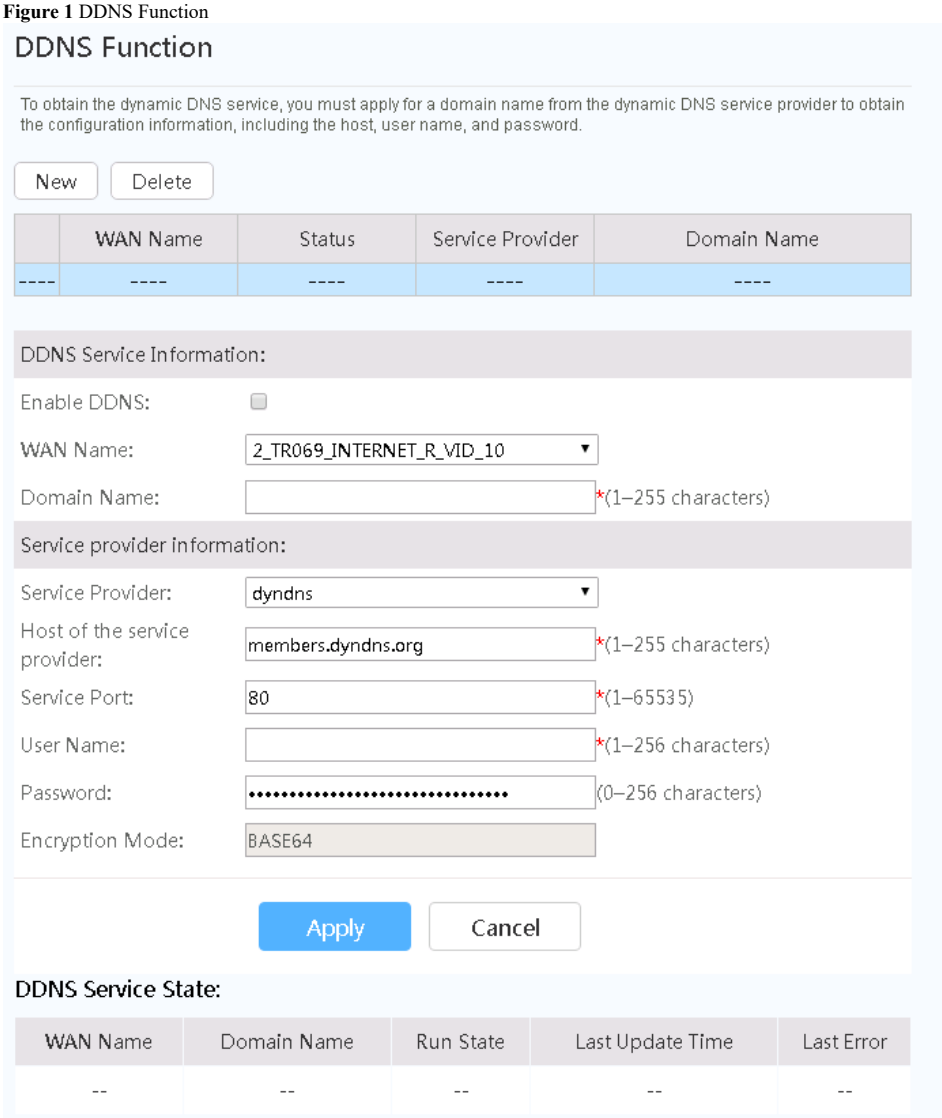
Parent Topic: Application

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.6.6.5 DDNS Function

1. Click the **Advanced Configuration** > **Application** tab and then choose **DDNS Function** from the navigation tree. In the right pane, configure DDNS parameters, including **Service Provider**, **Host Name**, **Service Port**, **Domain Name**, **Username**, and **Password**, as shown in Figure 1.

Figure 1 DDNS Function



2. Click **Apply**.

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

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

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

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

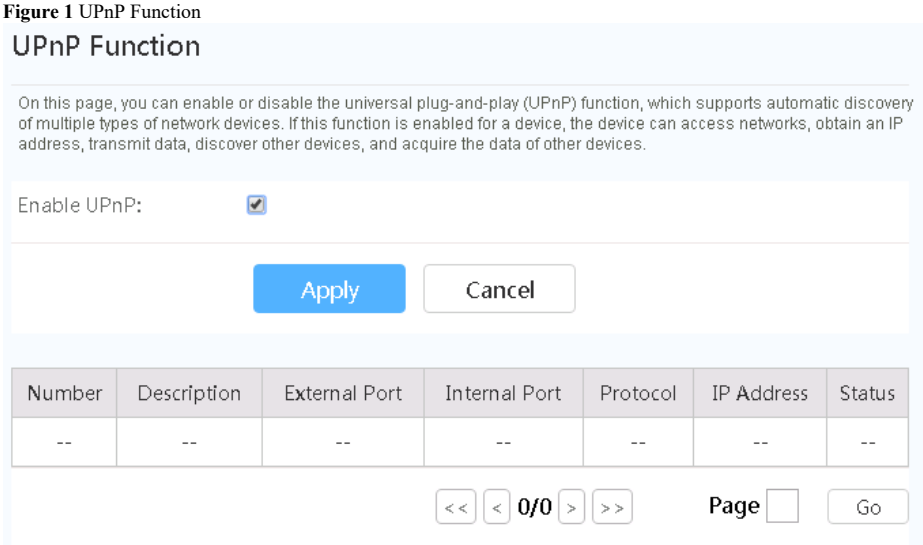
Parent Topic: Application

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.6.6.6 UPnP Function

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

Figure 1 UPnP Function



2. Click **Apply**.

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

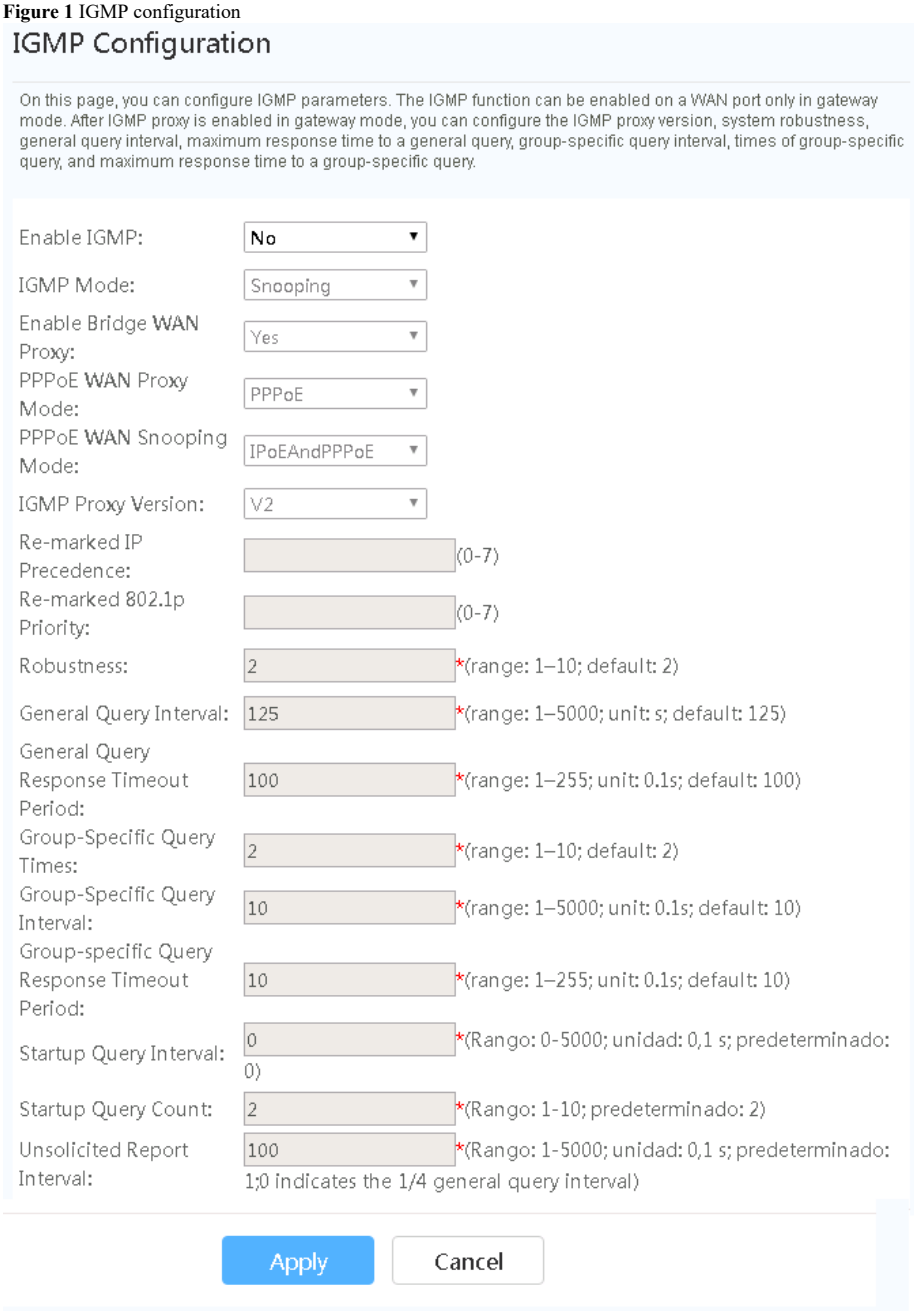
Parent Topic: Application

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.6.6.7 IGMP Configuration

1. Click the **Advanced Configuration** > **Application** tab and then choose **IGMP Configuration** from the navigation tree. In the right pane, configure the IGMP parameters, as shown in Figure 1.

Figure 1 IGMP configuration



2. Click **Apply**.

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 time**, **Specific query number**, **Specific query interval**, and **Specific query response time**.

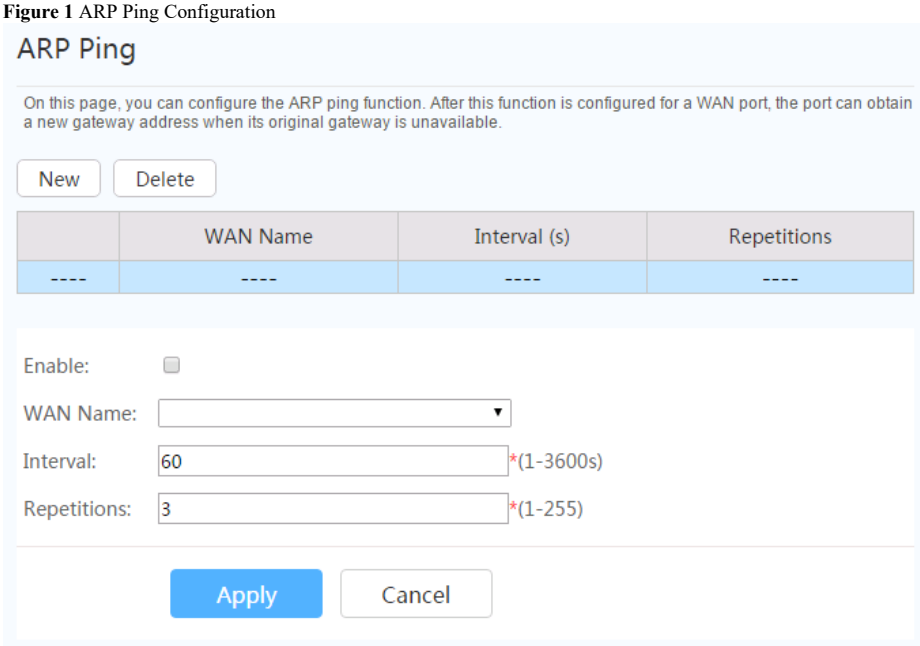
Parent Topic: Application

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.6.6.8 ARP Ping

1. Click **Advanced Configuration** > **Application** tab, and choose **ARP Ping** in the navigation tree on the left. In the pane on the right, configure ARP Ping parameters, including **WAN Name**, **Interval**, and **Repetitions**, as shown in Figure 1

Figure 1 ARP Ping Configuration



2. Click **Apply**.

Parent Topic: Application

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

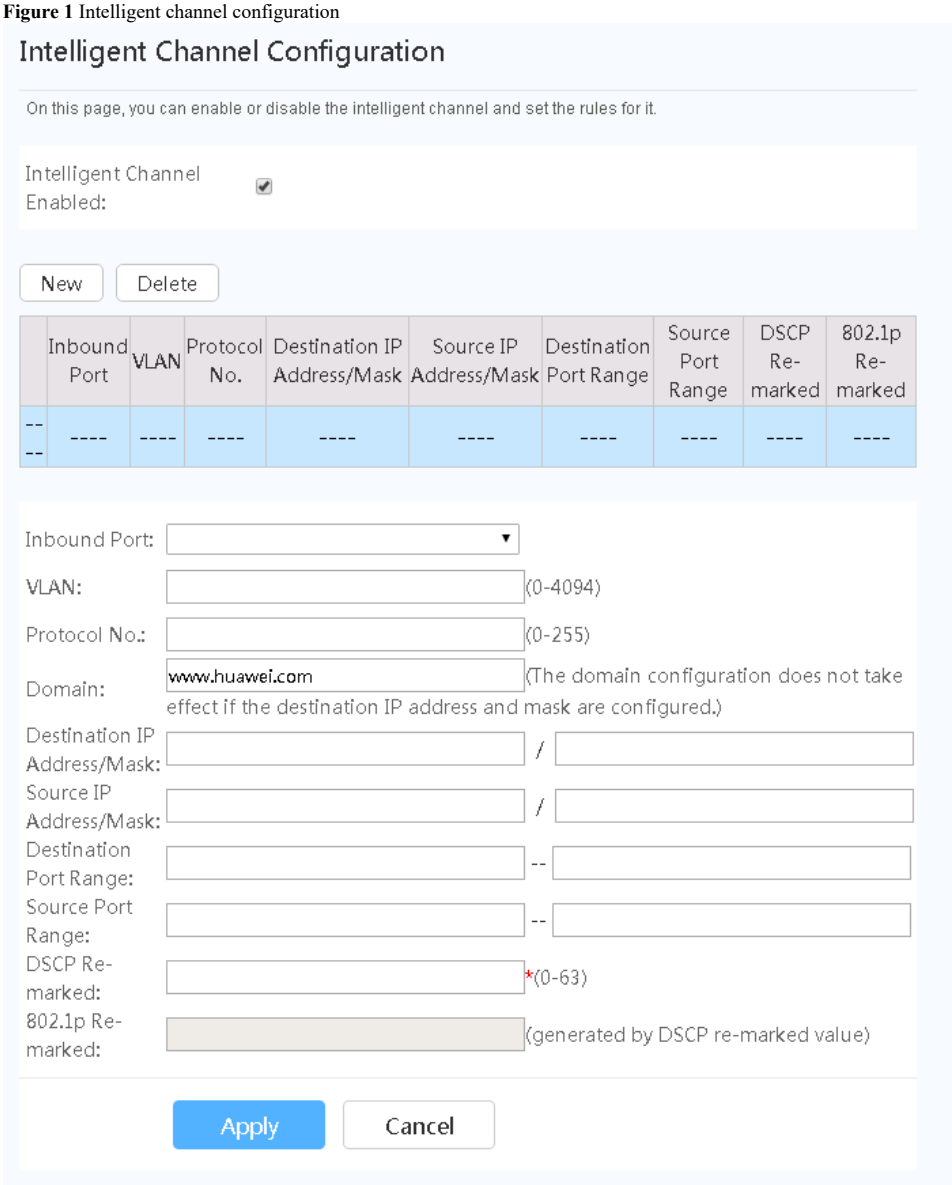
1.6.6.9 Intelligent Channel Configuration

NOTE:

After over-the-top (OTT) service flows are configured and services become normal, you can configure the intelligent channel according to the following description to ensure the OTT service bandwidth and thereby improve service experience.

1. Click the **Advanced Configuration** > **Application** tab, and choose **Intelligent Channel Configuration** from the navigation tree on the left. In the right pane, select **Intelligent Channel Enabled**, and click **New**. In the dialog box that is displayed, configure the intelligent channel, as shown in Figure 1.

Figure 1 Intelligent channel configuration



2. Click **Apply**.

Table 1 describes the intelligent channel parameters.

Table 1 Intelligent channel parameters

Parameter	Description
Intelligent Channel Enabled	Enables or disables the intelligent channel function.
Inbound Port	Indicates the port through which packets come in the ONT. The port must be the same as the LAN port that is bound to the WAN port of the intelligent channel service.
VLAN	Indicates the VLAN carried by packets when packets reach the inbound port. This parameter is not used for live-network services and thereby does not need to be configured.
Protocol No.	Indicates the Layer 3 protocol type of packets. Indicates the Layer 3 protocol type of packets. The following lists the numbers of common protocols: • TCP: 6 • UDP: 17 • IGMP: 2 • ICMP: 1
Domain	Indicates the domain name of the intelligent channel. When both the destination IP address and the domain name are configured, the destination IP address takes precedence over the domain name (that is, the domain name does not take effect.) The wildcard domain names in the following format 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.
Destination IP Address/Mask	Indicates the destination IP address and mask of packets related to the intelligent channel service. The IP address can be an address or an address segment. Generally, only the destination IP address and mask need to be configured.

Parameter	Description
Source IP Address/Mask	Indicates the source IP address and mask of packets related to the intelligent channel service. The IP address can be an address or an address segment.
Destination Port Range	Indicates the destination TCP/IP port of packets. It can be a consecutive port range.
Source Port Range	Indicates the source TCP/IP port of packets. It can be a consecutive port range.
DSCP Re-marked	Indicates the DSCP value to be remarked. A greater DSCP value indicates a higher 802.1p priority.
802.1p Re-marked	Indicates the 802.1p value to be remarked, which is generated through association with the DSCP value. The 802.1p value is calculated based on the most significant 3 bits of the DSCP value.

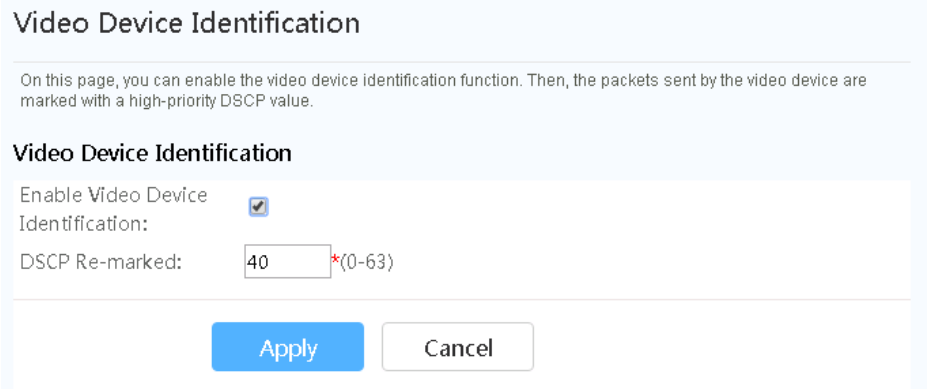
Parent Topic: Application

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.6.6.10 Video Device Identification

1. Click **Advanced Configuration** > **Application** tab, and choose **Video Device Identification** in the navigation tree on the left. In the pane on the right, determine whether to enable the **Video Device Identification** function,and enter the **DSCP Re-marked** value.as shown in Figure 1.

   Figure 1 Video Device Identification

2. Click **Apply**.

Parent Topic: Application

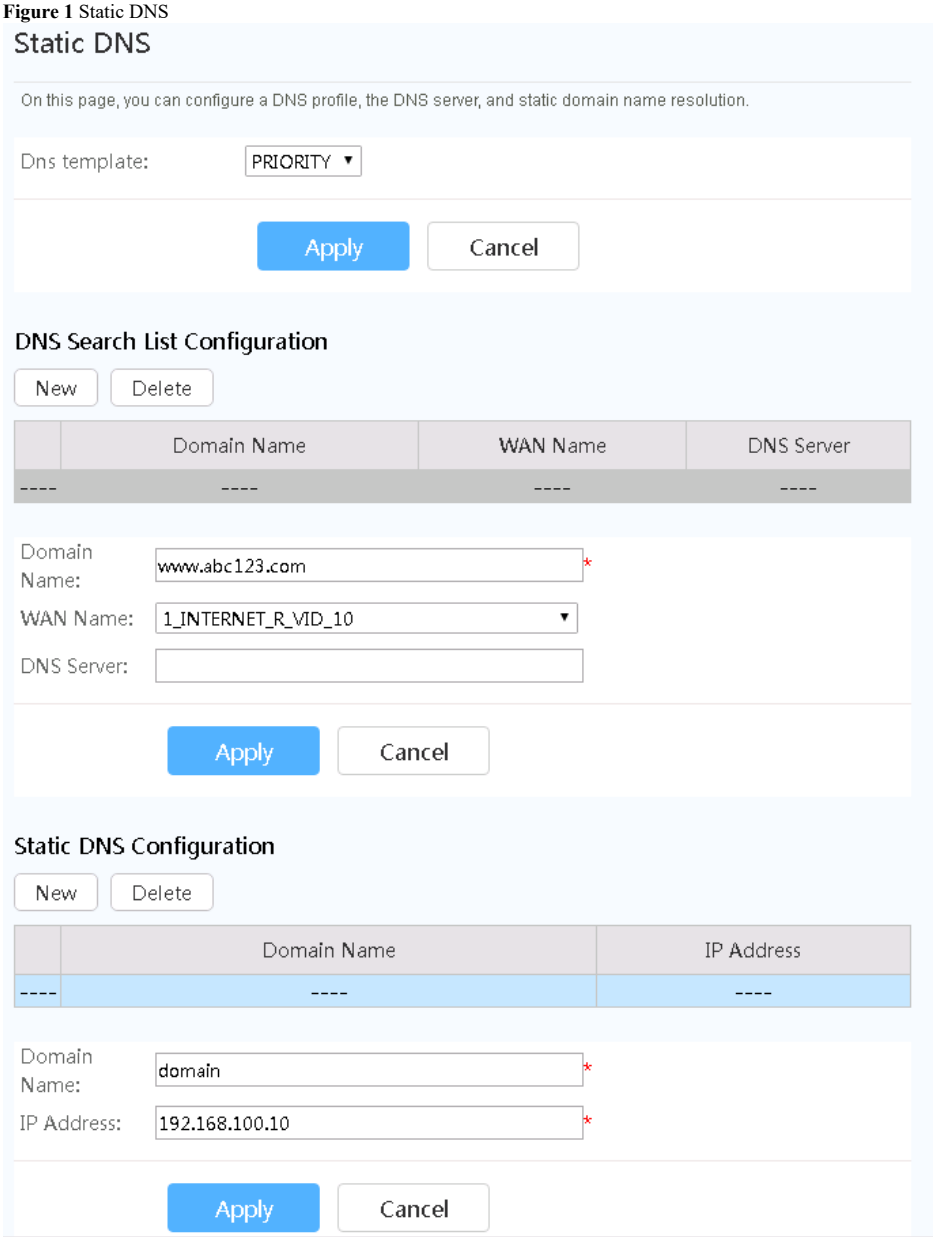
Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.6.6.11 Static DNS

1. Click the **Advanced Configuration** > **Application** tab and then choose **Static DNS** from the navigation tree.

   In the right pane, configure DNS parameters, and you can also configure static DNS domain name resolution, as shown in Figure 1.

Figure 1 Static DNS



2. Click **Apply**.

Parent Topic: Application

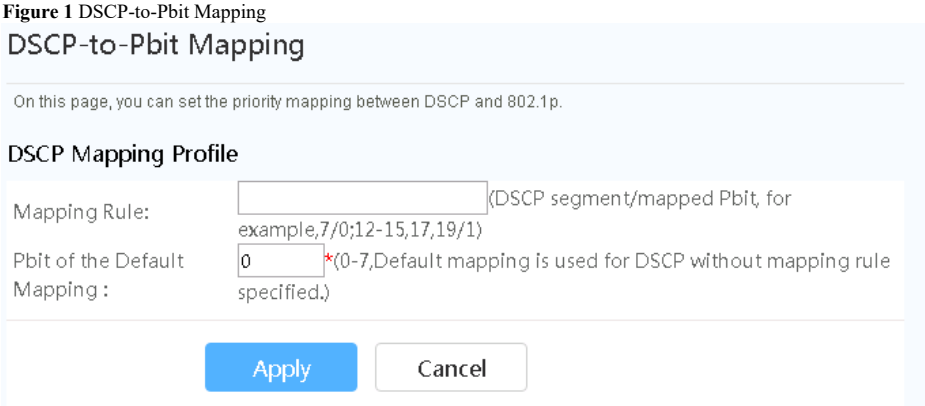
Copyright © Huawei Technologies Co., Ltd.

< Previous topic Next topic >

1.6.6.12 DSCP-to-Pbit Mapping

Click **Advanced Configuration** > **Application** tab, and choose **DSCP-to-Pbit Mapping** in the navigation tree on the left. on the left.On the right pane, set can set the mapping rule and Pbit of the Default Mapping, as shown inFigure 1.

Figure 1 DSCP-to-Pbit Mapping



A mapping rule indicates a newly added DSCP mapping profile. In the example, profile 1 is set and DSCP value is 7, the mapped Pbit is 0; DSCP values 12, 13, 14, 15, 17, and 19, the mapped Pbit is 1. Different priorities are separated by semicolon (;). Field **Pbit of the Default Mapping** indicates

the priority to which a DSCP value maps. In this field, values 0-7 are permitted. If no DSCP value is specified in Mapping Rule, the value set in **Pbit of the Default Mapping** takes effect.

Parent Topic: Application

Copyright © Huawei Technologies Co., Ltd.
< 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.

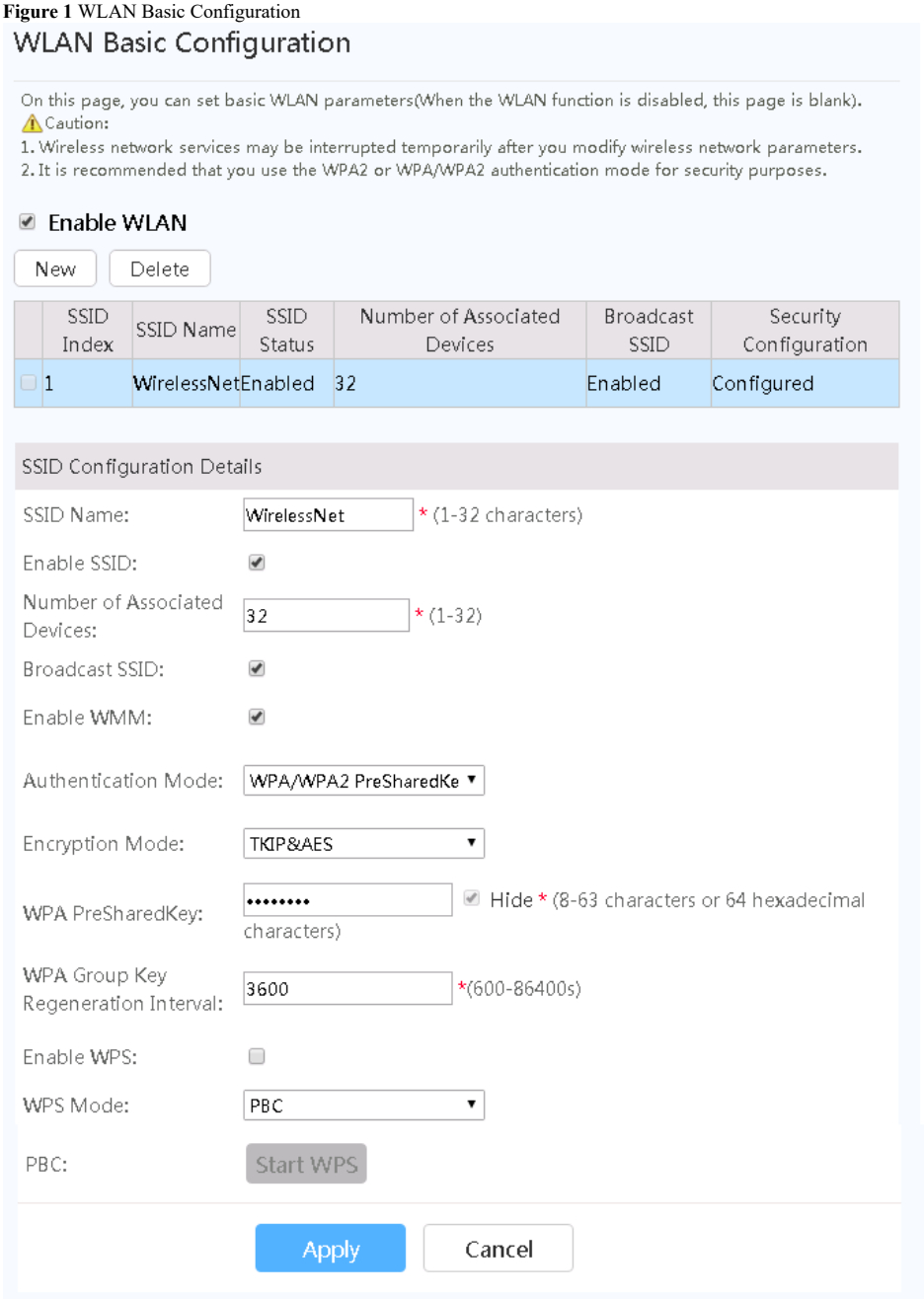
Parent Topic: Advanced Configuration

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.6.7.1 WLAN Basic Configuration

1. Click the **Advanced Configuration** > **WLAN** tab, and choose **WLAN Basic Configuration** from the navigation tree on the left. In the right pane, configure the basic parameters of the Wi-Fi network, as shown in Figure 1.

Figure 1 WLAN Basic Configuration



2. Click **Apply**.

Table 1 describes the basic parameters of the 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, named **WirelessNet** is created after the creation of an ONT. The system can configure up to four SSIDs at a time and cannot assign IP addresses to Wi-Fi terminals by SSID.
Enable SSID	Specifies whether to enable the connection.
Associated Device Number	Specifies the number of STAs. It ranges from 1 to 32.
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 ONT periodically broadcasts the SSID, that is, the name of the wireless network. In this way, any STA can search for the wireless network. • If the option box is not selected, it indicates that the SSID broadcast function is disabled. The SSID is hidden, and the STA cannot search for the wireless network. The SSID can be obtained only through a request.
WMM Enable	Specifies whether to enable Wi-Fi multimedia.

Parameter	Description
Authentication Mode	Indicates the authentication mode for the STA to request access to the wireless network. The mode can be Open, Shared, WPA Pre-Shared Key, WPA2 Pre-Shared Key, WPA/WPA2 Pre-Shared Key, WPA Enterprise, WPA2 Enterprise, or PA/WPA2 Enterprise. It is set to open by default, that is, the STA can access the 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 Pre-Shared Key**, **WPA2 Pre-Shared Key**, **WPA/WPA2 Pre-Shared Key**, **WPA Enterprise**, **WPA2 Enterprise** or **WPA/WPA2 Enterprise**, the encryption mode can be set to **AES**, **TKIP**, or **TKIP&AES**.

NOTE:

- The security mode and encryption configured on a Wi-Fi terminal must be the same as those of an ONT. 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.
- The WPS function can be used on SSID1 for only one band. In addition, do not enable WPS for multiple SSIDs in the same band. Otherwise, a Wi-Fi connection abnormality may occur.

Parent Topic: WLAN

Copyright © Huawei Technologies Co., Ltd.
Next topic >

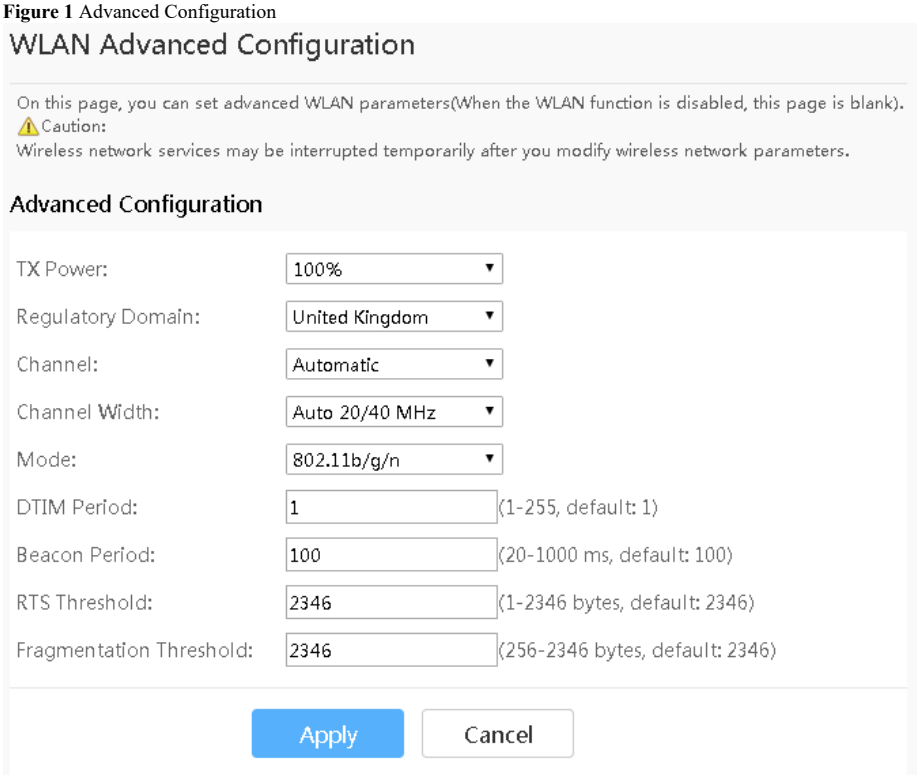
1.6.7.2 WLAN Advanced Configuration

1. Click the **Advanced Configuration** > **WLAN** tab, and choose **WLAN Advanced Configuration** from the navigation tree on the left. In the right pane, configure the basic parameters of the Wi-Fi network, as shown in Figure 1.

NOTE:

This page is empty if **Enable WLAN** is not selected in **Advanced Configuration**.

Figure 1 Advanced Configuration



2. Click **Apply**.

Table 1 describes the Wi-Fi parameters of the 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 country code of the wireless network.
Channel	Indicates the channel of the wireless network. The channel varies with the value of **Regulatory Domain**.

Parameter	Description
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

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

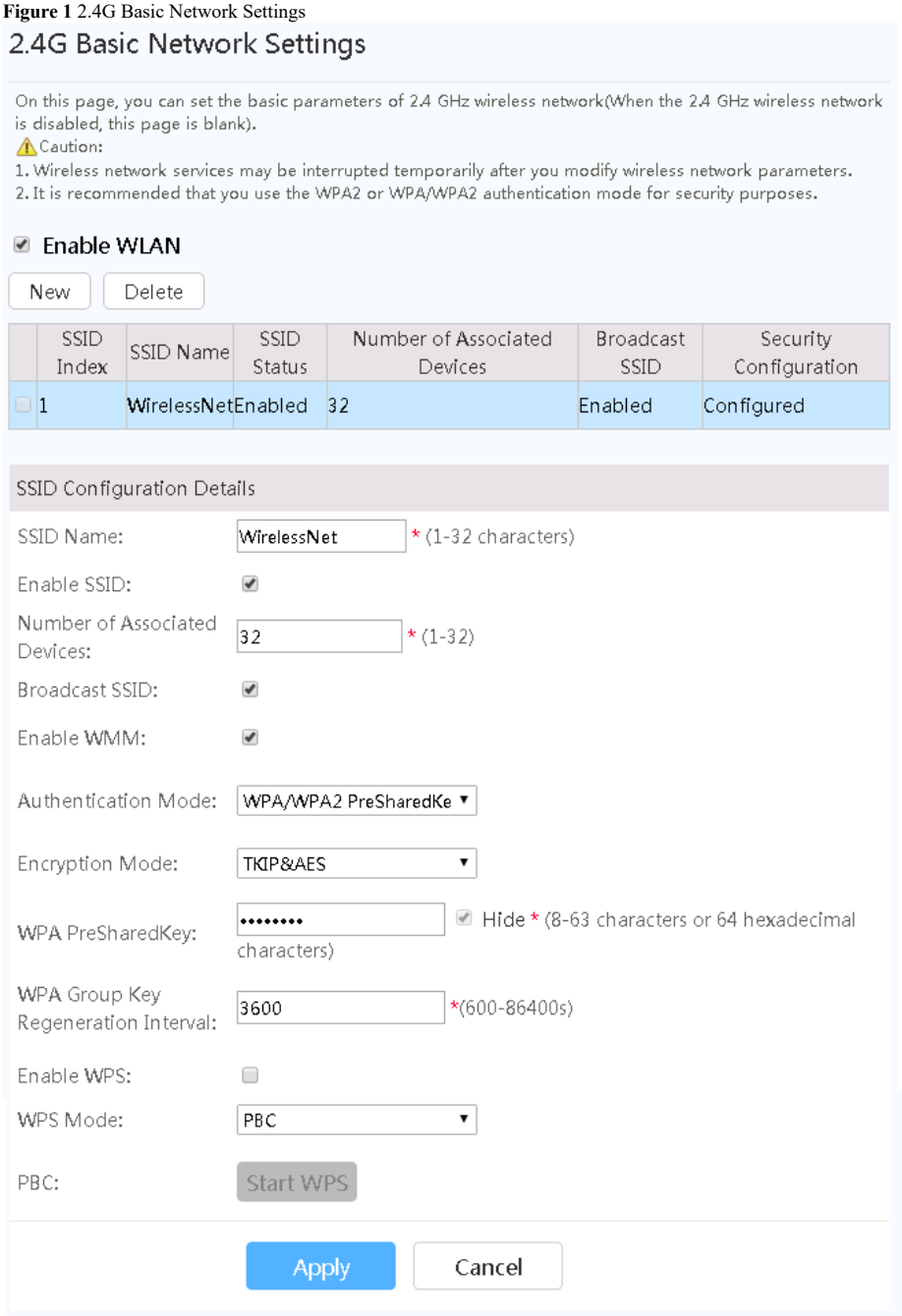
1.6.7.3 2.4G Basic Network Settings

NOTE:

Only dual-band products support this page

1. Click the **Advanced Configuration** > **WLAN** tab, and choose **2.4G Basic Network Settings** from the navigation tree on the left. In the right pane, configure the basic parameters of the 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 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, named **WirelessNet** is created after the creation of an ONT. The system can configure up to four SSIDs at a time and cannot assign IP addresses to Wi-Fi terminals by SSID.
Enable SSID	Specifies whether to enable the connection.
Associated Device Number	Specifies the number of STAs. It ranges from 1 to 32.
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 ONT periodically broadcasts the SSID, that is, the name of the wireless network. In this way, any STA can search for the wireless network. • If the option box is not selected, it indicates that the SSID broadcast function is disabled. The SSID is hidden, and the STA cannot search for the wireless network. The SSID can be obtained only through a request.
WMM Enable	Specifies whether to enable Wi-Fi multimedia.

Parameter	Description
Authentication Mode	Indicates the authentication mode for the STA to request access to the wireless network. The mode can be Open, Shared, WPA Pre-Shared Key, WPA2 Pre-Shared Key, WPA/WPA2 Pre-Shared Key, WPA Enterprise, WPA2 Enterprise, or PA/WPA2 Enterprise. It is set to open by default, that is, the STA can access the 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 Pre-Shared Key**, **WPA2 Pre-Shared Key**, **WPA/WPA2 Pre-Shared Key**, **WPA Enterprise**, **WPA2 Enterprise** or **WPA/WPA2 Enterprise**, the encryption mode can be set to **AES**, **TKIP**, or **TKIP&AES**.

NOTE:

- The security mode and encryption configured on a Wi-Fi terminal must be the same as those of an ONT. 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.
- The WPS function can be used on SSID1 for only one band. In addition, do not enable WPS for multiple SSIDs in the same band. Otherwise, a Wi-Fi connection abnormality may occur.

Parent Topic: WLAN

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.6.7.4 2.4G Advanced Network Settings

NOTE:

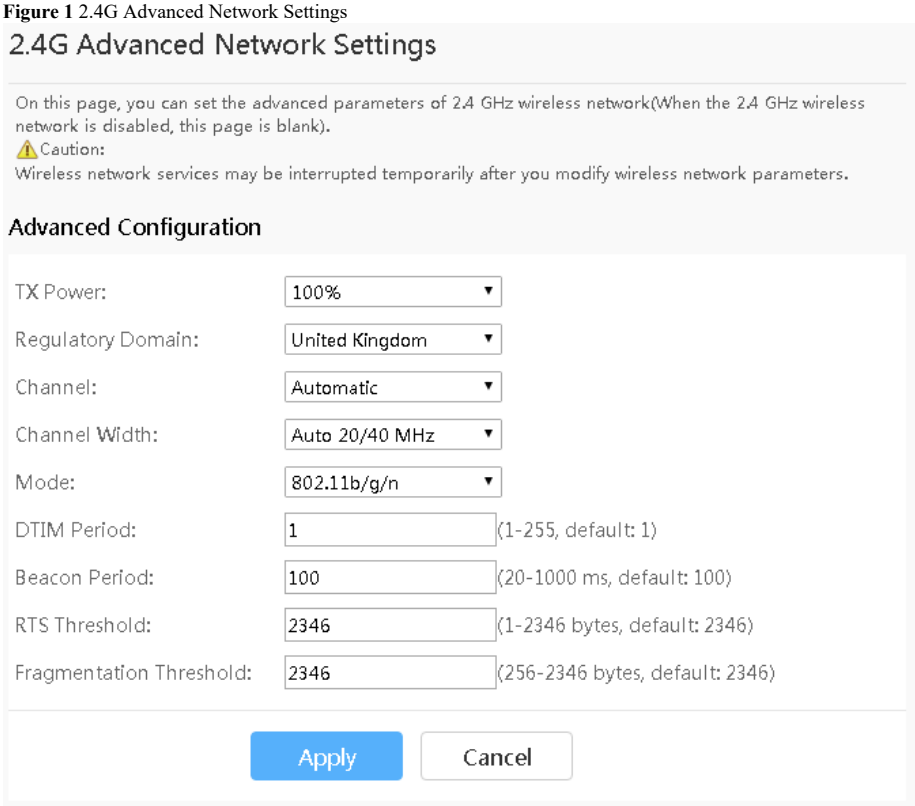
Only dual-band products support this page

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

   NOTE:

   This page is empty if **Enable WLAN** is not selected in **Advanced Configuration**.

   Figure 1 2.4G Advanced Network Settings



2. Click **Apply**.

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

Table 1 Wireless network advance parameters

Parameter	Description

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 country code of the wireless network.
Channel	Indicates the channel of the wireless network. The channel varies with the value of **Regulatory Domain**.
Channel Width	Indicates the wireless channel width. 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

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

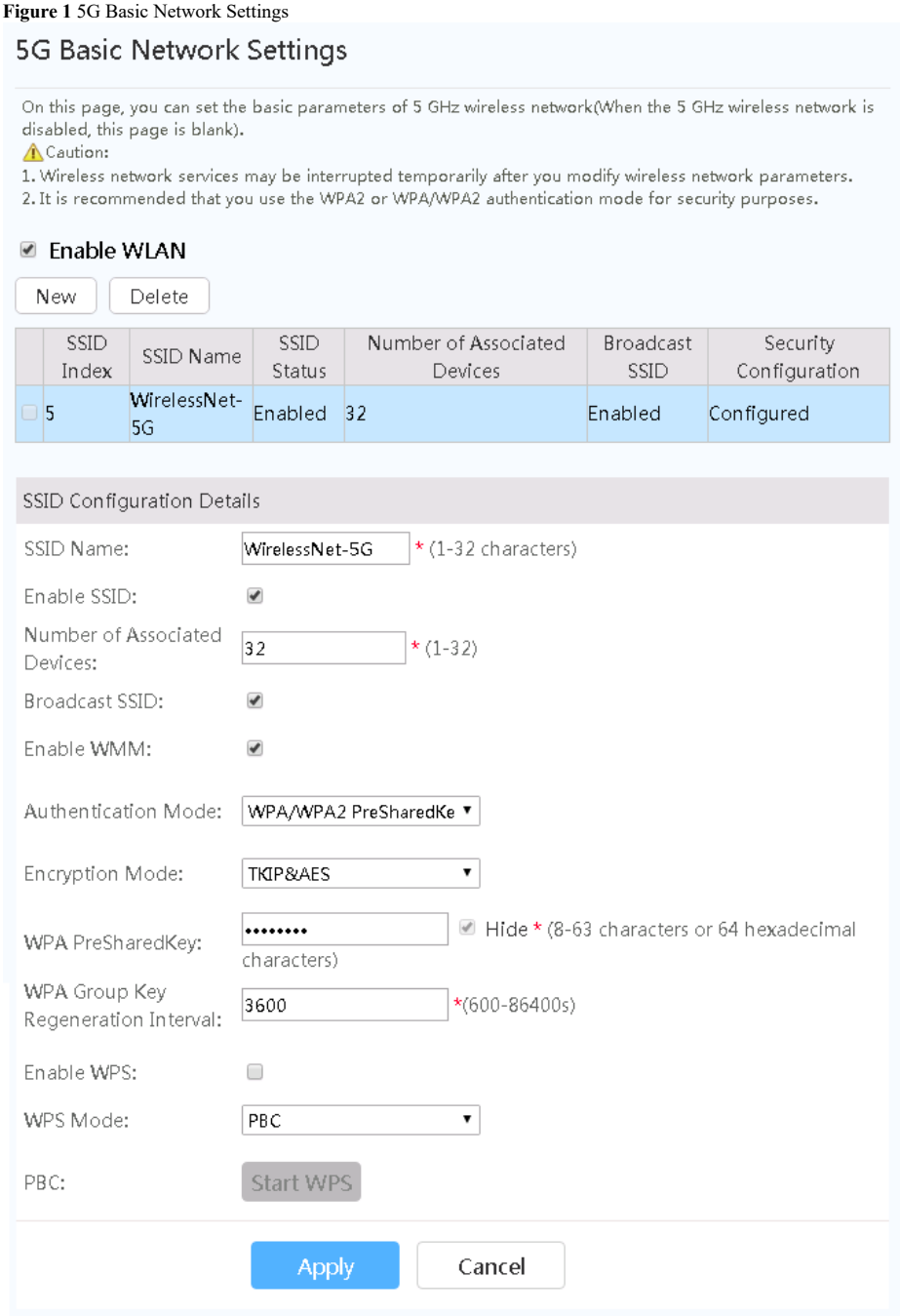
1.6.7.5 5G Basic Network Settings

NOTE:

Only dual-band products support this page.

1. Click the **Advanced Configuration** > **WLAN** tab, and choose **5G Basic Network Settings** from the navigation tree on the left. In the right pane, 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 5G basic Wi-Fi network settings.

Table 1 5G basic network settings

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 space or Tab character. A default SSID1, named **WirelessNet** is created after the creation of an ONT. The system can configure up to four SSIDs at a time and cannot assign IP addresses to Wi-Fi terminals by SSID.
Enable SSID	Specifies whether to enable the connection.
Associated Device Number	Specifies the number of STAs. It ranges from 1 to 32.
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 ONT periodically broadcasts the SSID, that is, the name of the wireless network. In this way, any STA can search for the wireless network. • If the option box is not selected, it indicates that the SSID broadcast function is disabled. The SSID is hidden, and the STA cannot search for the wireless network. The SSID can be obtained only through a request.
WMM Enable	Specifies whether to enable Wi-Fi multimedia.

Parameter	Description
Authentication Mode	Indicates the authentication mode for the STA to request access to the wireless network. The mode can be Open, Shared, WPA Pre-Shared Key, WPA2 Pre-Shared Key, WPA/WPA2 Pre-Shared Key, WPA Enterprise, WPA2 Enterprise, or PA/WPA2 Enterprise. It is set to open by default, that is, the STA can access the 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 Pre-Shared Key**, **WPA2 Pre-Shared Key**, **WPA/WPA2 Pre-Shared Key**, **WPA Enterprise**, **WPA2 Enterprise** or **WPA/WPA2 Enterprise**, the encryption mode can be set to **AES**, **TKIP**, or **TKIP&AES**.

NOTE:

- The security mode and encryption configured on a Wi-Fi terminal must be the same as those of an ONT. 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.
- The WPS function can be used on SSID1 for only one band. In addition, do not enable WPS for multiple SSIDs in the same band. Otherwise, a Wi-Fi connection abnormality may occur.

Parent Topic: WLAN

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.6.7.6 5G Advanced Network Settings

NOTE:

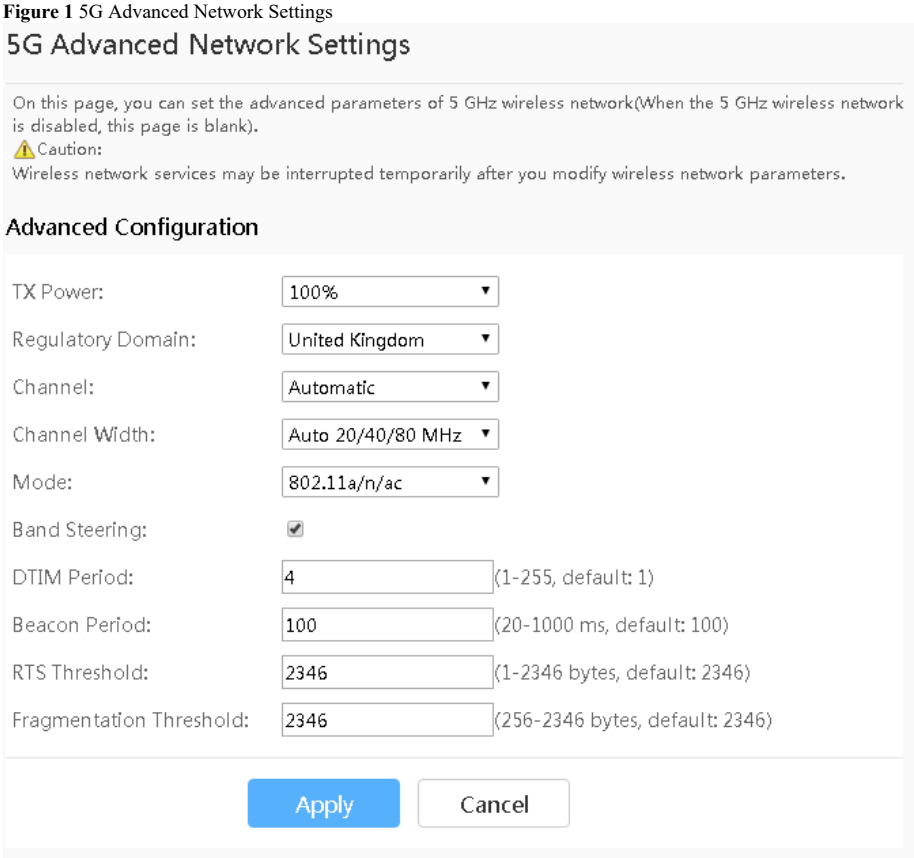
Only dual-band products support this page.

1. Click the **Advanced Configuration** > **WLAN** tab, and choose **5G Advanced Network Settings** from the navigation tree on the left. In the right pane, 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 country code of the wireless network.
Channel	Indicates the channel of the wireless network. The channel varies with the value of **Regulatory Domain**.
Channel Width	Indicates the wireless channel width. 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 **802.11b**, **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.

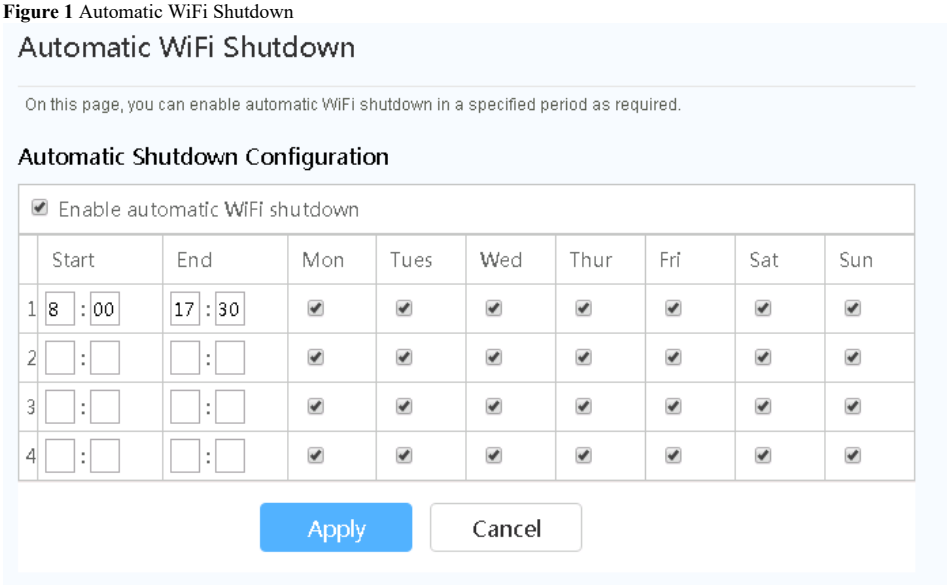
Parent Topic: WLAN

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.6.7.7 Automatic WiFi Shutdown

1. Click the **Advanced Configuration** > **WLAN** tab, and choose **Automatic WiFi Shutdown** from the navigation tree on the left. In the right pane, configure the scheduled WiFi shutdown time segment, to enable the WiFi network to be automatically shut down when the WiFi network is not in use, as shown in Figure 1.

Figure 1 Automatic WiFi Shutdown



2. Click **Apply**.

Parent Topic: WLAN

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.6.7.8 WiFi Coverage Management

1. Click the **Advanced Configuration** > **WLAN** tab, and choose **WiFi Coverage Management** from the navigation tree on the left. In the right pane, specify the SSID used for smart WiFi coverage and add the identified external AP devices to the WiFi network, as shown in Figure 1 and Figure 2.

Figure 1 Wi-Fi Parameter Configuration

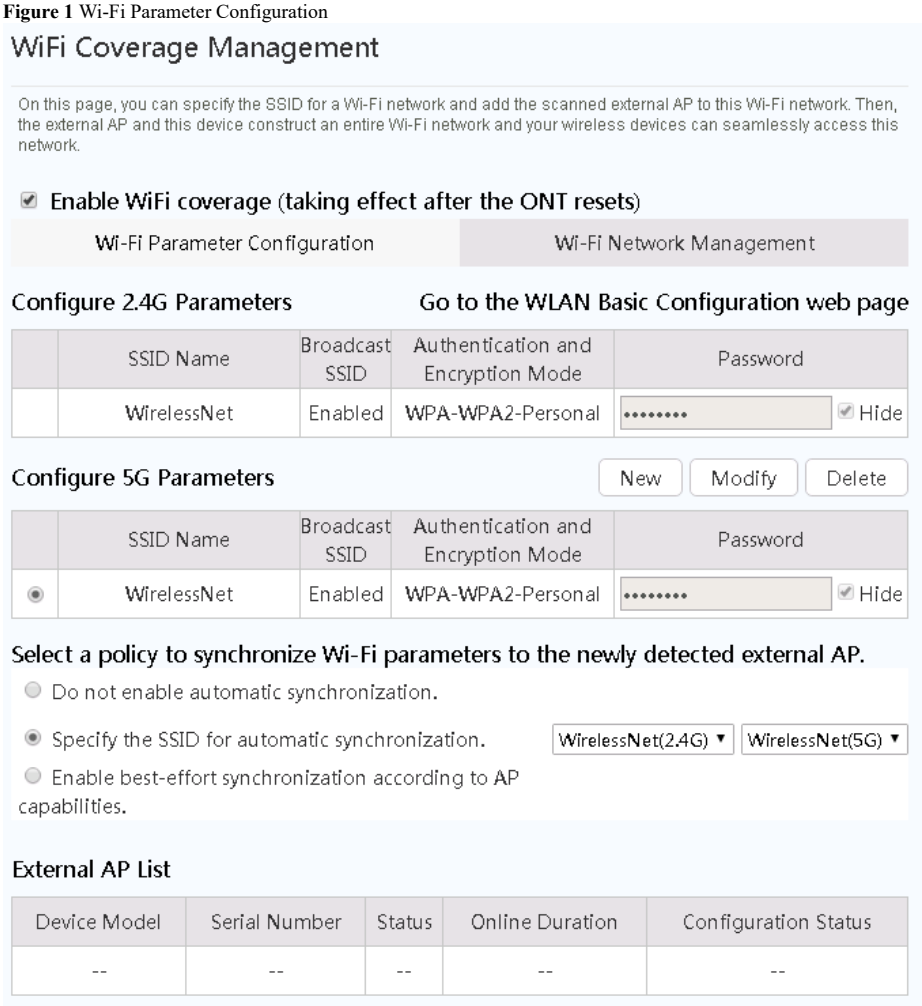
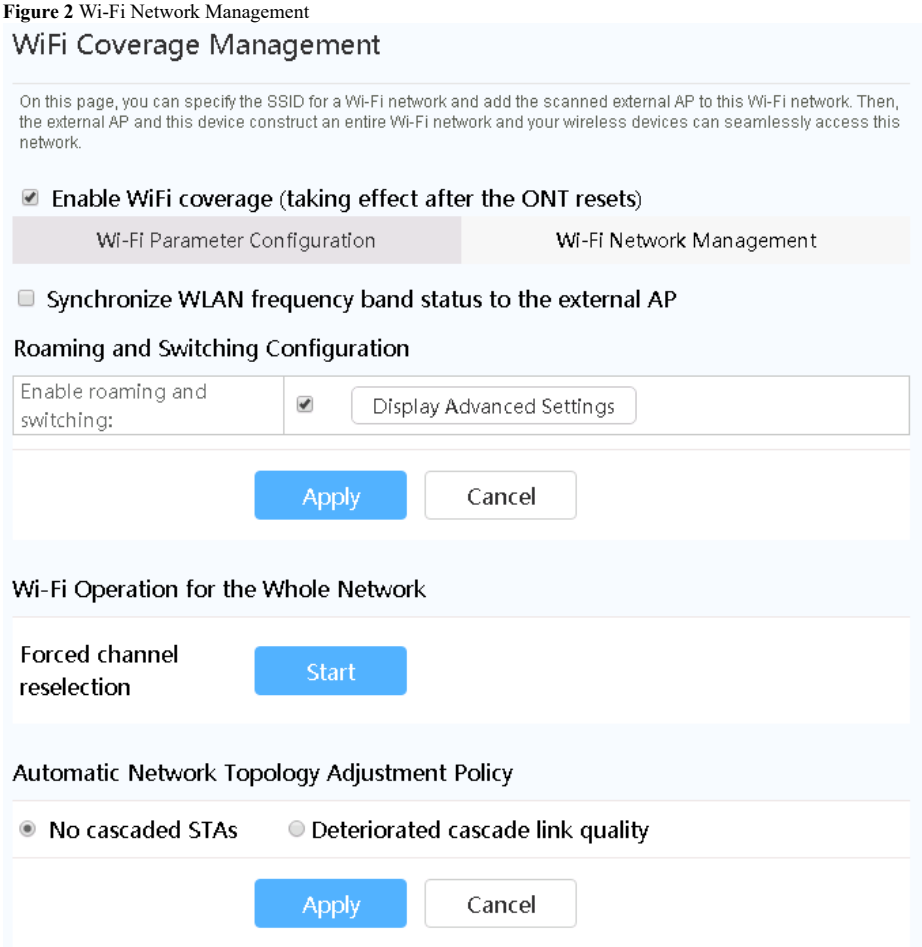


Figure 2 Wi-Fi Network Management



2. Click **Apply**.

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 pages after the H.248 protocol and the SIP protocol are loaded.

Parent Topic: Advanced Configuration

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

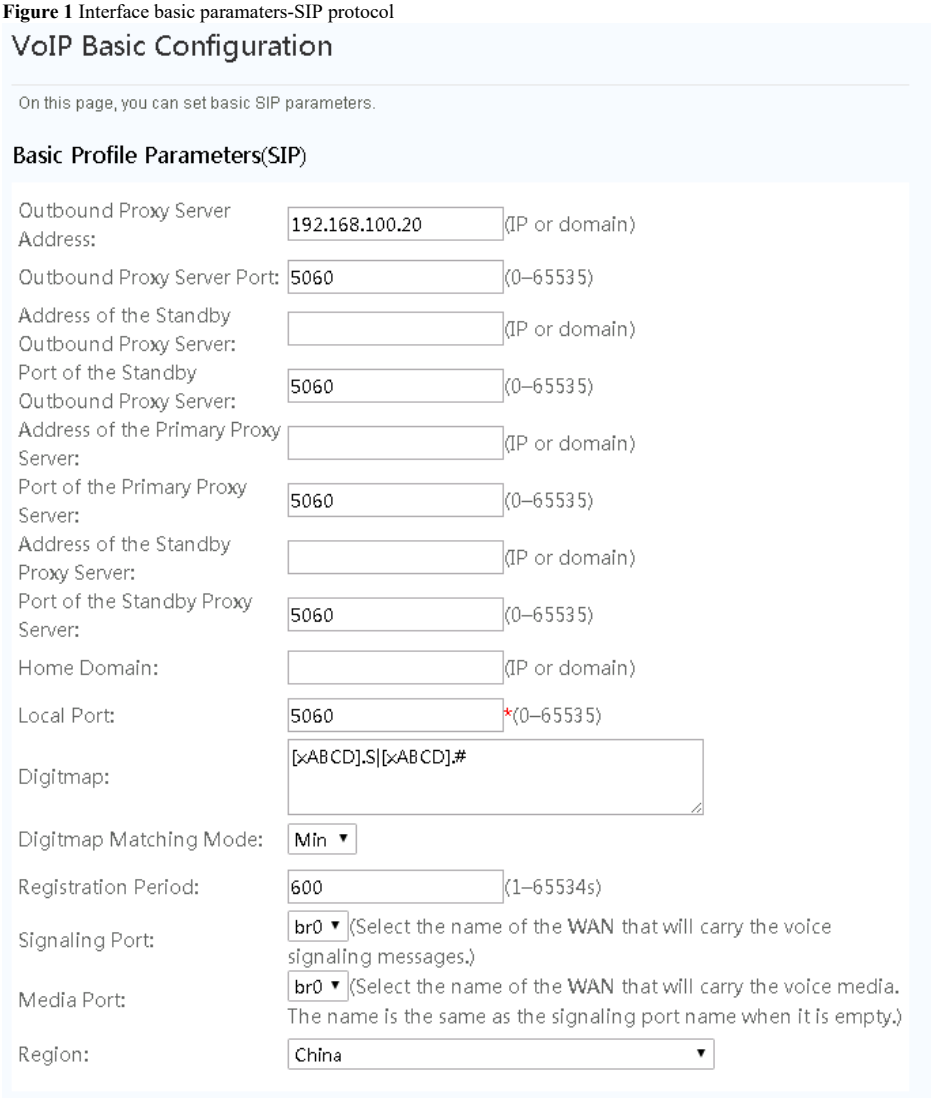
1.6.8.1 VoIP Basic Configuration

- **VoIP Basic Configuration - SIP protocol**

  1. In the navigation tree on the left, choose **Advanced Configuration** > **Voice** > **VoIP Basic Configuration**. In the pane on the right, parameters of a VoIP interface can be configured, including the IP addresses of the primary server and secondary server, and digitmap.

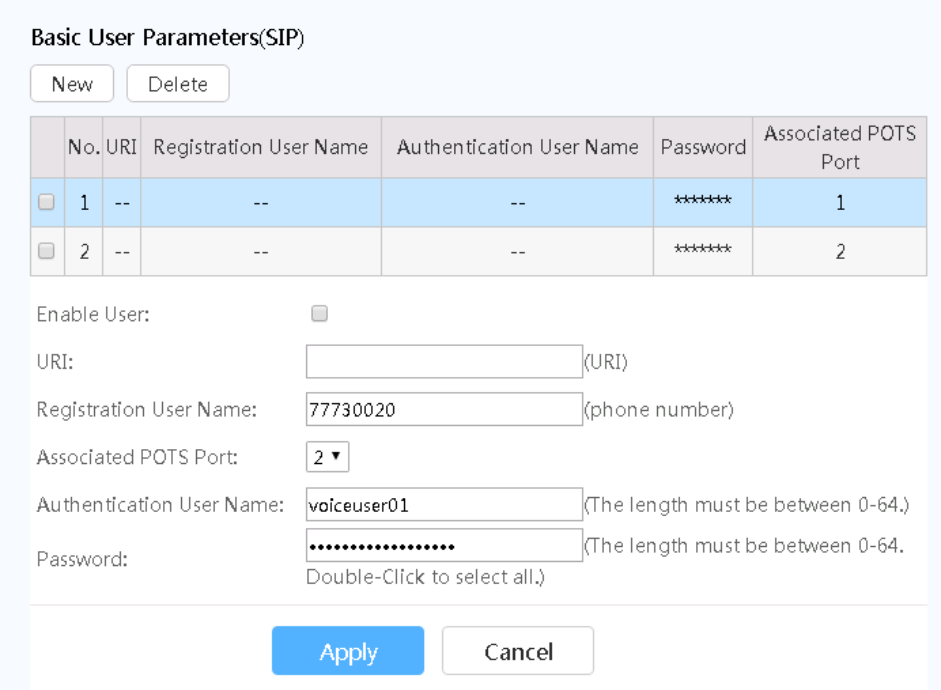
     a. Configure the basic parameters for a voice interface.

Figure 1 Interface basic paramaters-SIP protocol



     b. Configure basic parameters for a SIP voice user.

Figure 2 User basic parameters-SIP protocol



2. Click **Apply**.

Table 1 describes the parameters used for configuring a VoIP interface based on the SIP protocol.

Table 1 Parameters used for configuring a VoIP interface based on the SIP protocol

Parameter	Description
Basic Interface 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 1 to 65535 and the default ID is 5060.
Outbound Proxy Server Port	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 1 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 1 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 1 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 ONT. The ID ranges from 1 to 65535 and the default ID is 5060.
Digitmap	Indicates the voice digitmap.
Digitmap Match 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.

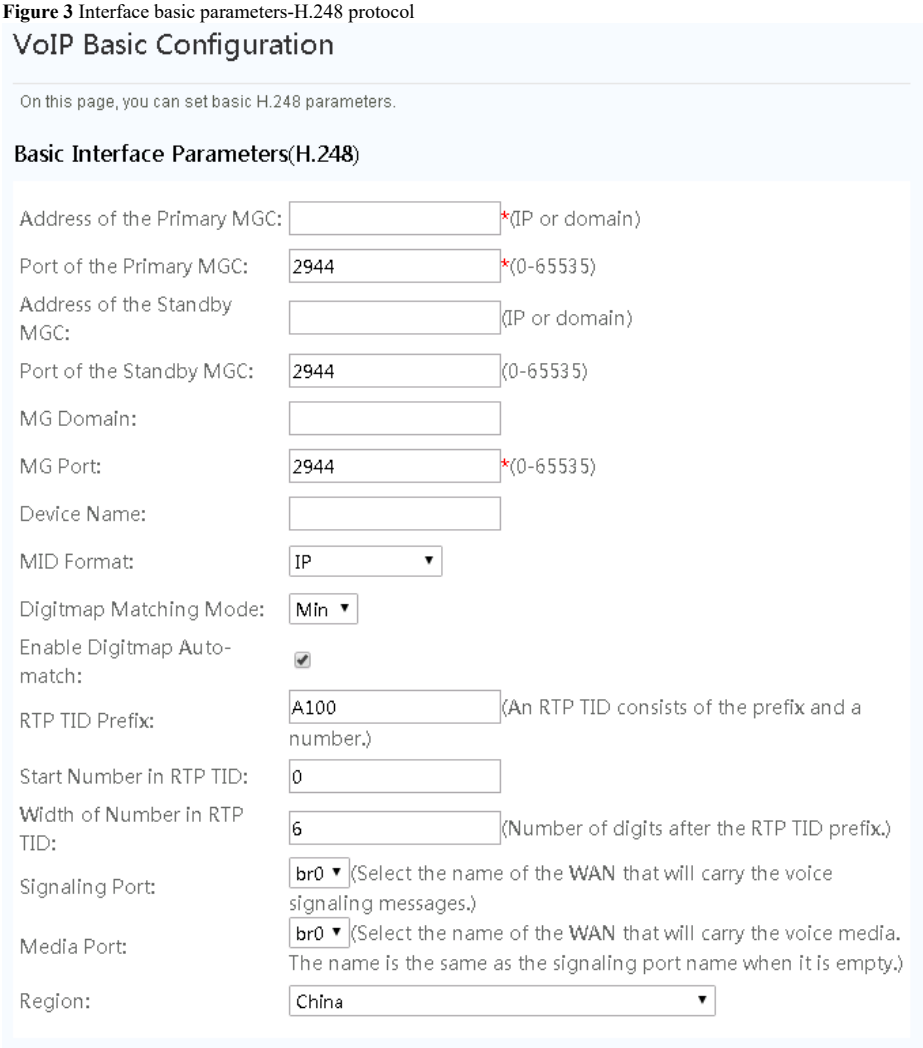
Parameter	Description
Basic User Parameters(SIP)	
Enable User	Enables or disables a SIP user. The SIP user starts the registration only after being enabled.
URI	Indicates the SIP user identifier. It uniquely identifies a SIP user and the value must be the same as the configuration on the IMS.
Registration 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.

- **VoIP Interface Configuration - H.248 Protocol**

1. In the navigation tree on the left, choose **Advanced Configuration** > **Voice** > **VoIP basic Configuration**. In the pane on the right, parameters of a VoIP interface can be configured, including the address of the primary MGC, device name, and region, as shown in Figure 3 and Figure 4.

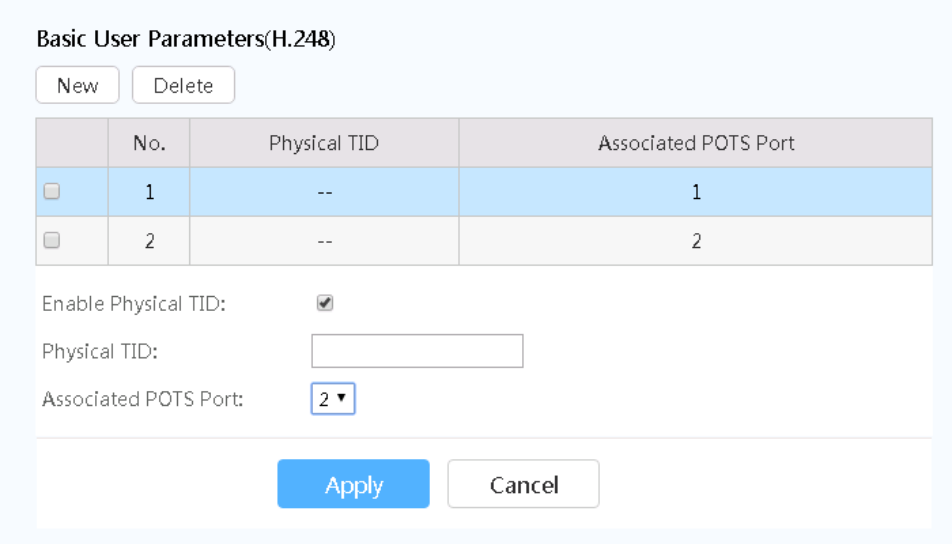
   a. Configure the basic parameters for a voice interface.

   Figure 3 Interface basic parameters-H.248 protocol



   b. Configure basic parameters for an H.248–based voice user.

Figure 4 User basic parameters-H.248 protocol



2. Click **Apply**.

Table 2 describes parameters used for configuring a VoIP interface based on the H.248 protocol.

Table 2 Parameters used for configuring a VoIP interface based on the H.248 protocol

Parameter	Description
Basic Interface Parameters(H.248)	
Address of the Primary MGC	Indicates the IP address (provided by the ISP) of the primary MGC server.
Port of the Primary MGC	Indicates the ID (provided by the ISP) of the port used for communication between the primary MGC server and the VoIP terminal. The ID ranges from 1 to 65535 and the default ID is 2944.
Address of the Standby MGC	Indicates the IP address (provided by the ISP) of the secondary MGC server.
Port of the Standby MGC	Indicates the ID (provided by the ISP) of the port used for communication between the secondary MGC server and the VoIP terminal. The ID ranges from 1 to 65535 and the default ID is 2944.
MG Domain	Fill the domain name when MID Format is set to **Domain Name**, such as user.huawei.com.
MG Port	Indicates the ID of the local port on the ONT. The ID ranges from 1 to 65535 and the default ID is 2944.
Device Name	Fill the device name when MID Format is set to **Device Name**.
MID Format	Indicates the MG registration format. It can be the MG domain name, IP address, or device name. The MG register format must be the same as the register format provided by the ISP.
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 softswitches. • Max: If the dialed character string matches a digitmap scheme, the system does not immediately report the number to the softswitches but starts the short timer. If a user does not continue dialing digits, the system reports the number to the softswitches 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 softswitches.
Enable Digitmap Auto-match	Enables or disables the function of digitmap auto match.
RTP TID Prefix	Indicates the index of the ephemeral termination. The default prefix on Huawei softswitches is A100.
Start Number of RTP TID	Indicates the start number of RTP TID. The default start number is 0.
Width of RTP TID Number	Indicates the width of RTP TID. The default number is 6.
Signaling Port	Indicates the signaling WAN port used for connecting the VoIP terminal to the MGC server.
Media Port	Indicates the WAN port of the voice media streams. When the name of the media port is empty, it indicates that the name of the media port is the same as that of the signaling port.
Region	Indicates the country code.
Basic User Parameters(H.248)	
Enable Physical TID	Enables or disables an ONT POTS port.
Physical TID	Indicates the POTS port identifier.
Associated POTS Port	Indicates the binding of a POTS port and a physical terminal.

Parent Topic: Voice

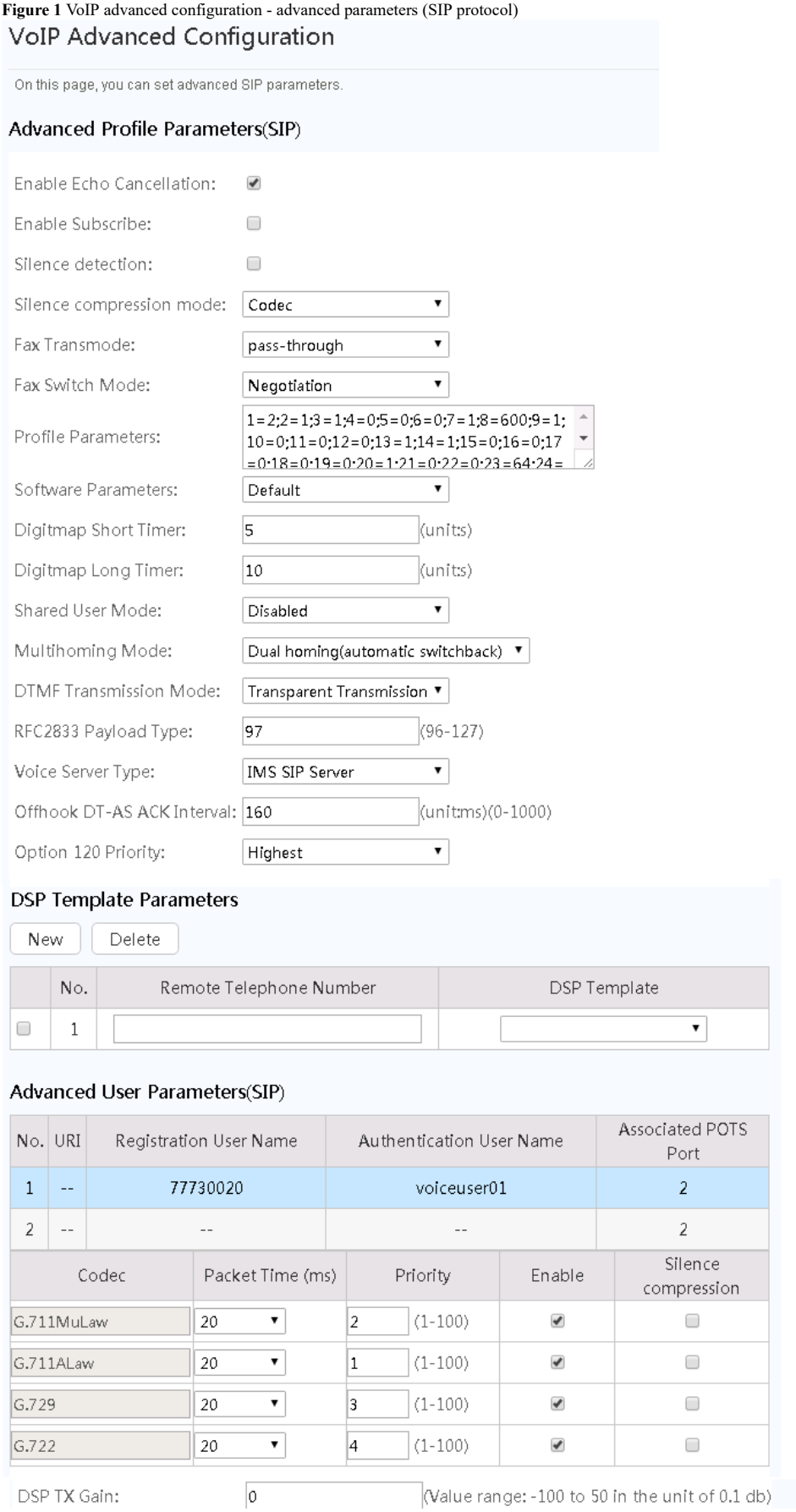
Copyright © Huawei Technologies Co., Ltd.
Next topic >

1.6.8.2 VoIP Advanced Configuration

- **VoIP Advanced Configuration - SIP protocol**

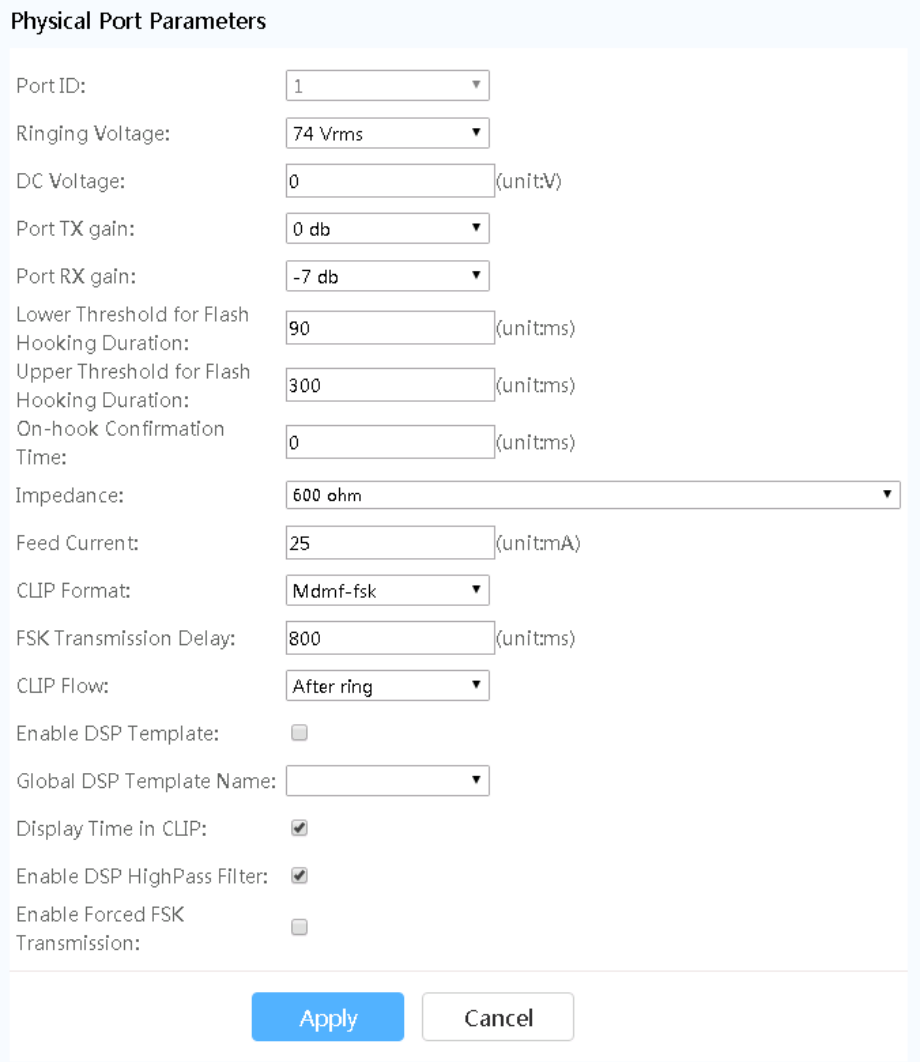
1. IIn the navigation tree on the left, choose **Advanced Configuration** > **Voice** > **VoIP Advanced Configuration**. In the pane on the right, you can configure parameters of a VoIP user, including the register user name, authentication user name, password, and associated POTS, as shown in Figure 1 and Figure 2.

Figure 1 VoIP advanced configuration - advanced parameters (SIP protocol)



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)
Enable Call Forwarding on No Reply:	☐	
Call Forwarding on No Reply Number:		(0-32)
Call Waiting	☑	
Message Waiting Indicator	☑	
Three-party Call	☑	
Call Holding	☑	
Malicious Call Identification	☐	
Caller ID Display	☑	
Call Transfer	☐	
Anonymous Call	☐	
Activate Anonymous Call	☐	

Figure 2 VoIP advanced configuration - physical Port parameters (SIP protocol)



2. Click **Apply**.

Table 1 describes the advanced parameters used for configuring a VoIP interface based on the SIP protocol.

Table 1 Advanced parameters used for configuring a VoIP interface based on the SIP protocol

Parameter	Description
Advanced Profile Parameters(SIP)	
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	Indicates a silence detection method for a network call. This method is used to detect silence in full-duplex and half-duplex modes, isolates voice from background noise, and filters out redundant audio data. Silence detection function controls the global mode in silence compression mode.
Silence compression mode	Supports 2 modes: • Codec mode: In **Advanced User Parameters**(SIP), select **Silence compression** . Then, you can set G.711MuLaw, G.711ALaw, G.729 and G.722. • Global mode: Select **Silence detection**, and you can configure all coding/decoding modes.
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.

Parameter	Description
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 ONT 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 ONT 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 ONT switches back to the active softswitch when detecting that the active softswitch recovers and is reachable. • Loading sharing: The ONT 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 or in 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. • Softswitch: softswitch NGN service type based on the SIP protocol. • H.248 Server: H.248 service type.
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.
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; and supports silence compression.
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.
Enabled	Indicates whether the user carries the codec (enable: carry; disable: not carry).
DSP TX Gain	Indicates the direction in which gain takes effect: from the local POTS side to the remote IP side.
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.

Parameter	Description
Caller ID Display	A called party-side service allows the number of the calling party to be presented to the called party.
Anonymous Call	This service does not allow the number of the calling party who registers this service to be presented to the called party.
Call Transfer	Enables or disables the call transfer function.
Physical Port Parameters (SIP)	
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 of the connected device.
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 **Mdmf-FSK**, **Sdmf-FSK**, **Dtmf**, **R1.5**, and **Etsi**.
FSK Transmission Delay	Indicates the delay before FSK signals are issued.
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.
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	Enables or disables time synchronization on a phone. After this function is enabled, the ONT issues time to the phone.
Enable DSP HighPass Filter	Enables this function to mask the low frequency (lower than 50 Hz) interference on the phone.
Enable Forced FSK Transmission	Enables or disables forced FSK transmission.

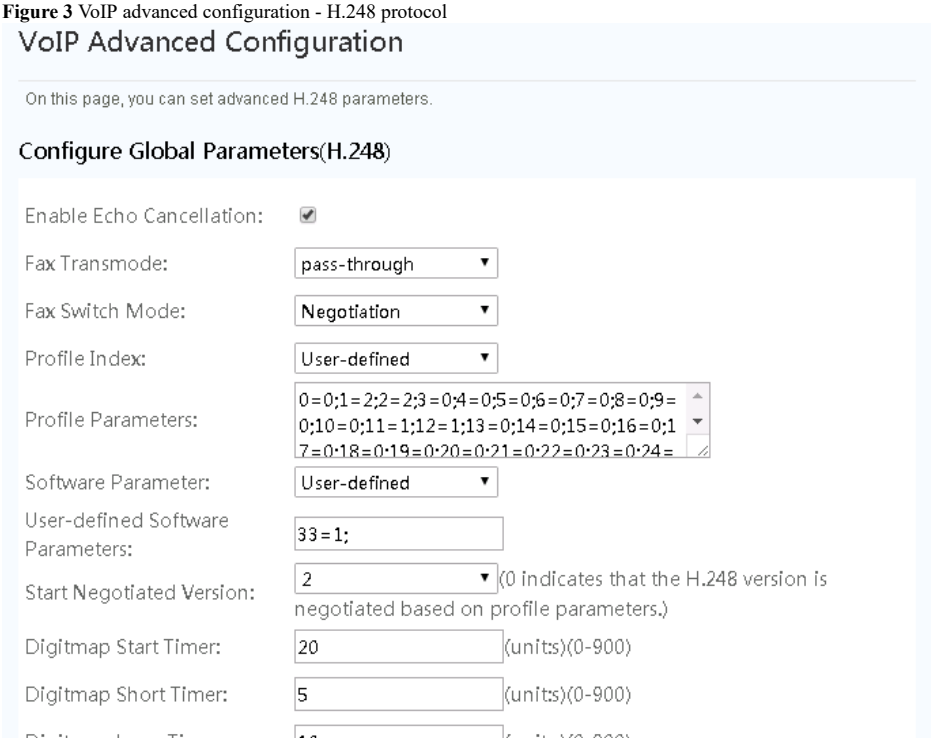
NOTE:

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

- **VoIP Advanced Configuration - H.248 Protocol**

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 line name and associated POTS, as shown in Figure 3.

Figure 3 VoIP advanced configuration - H.248 protocol



Digitmap Long Timer: 10 (unit:s)(0-900)

Enable Heartbeat: ☑

Heartbeat Message Interval: 600 (unit:s)

Heartbeat Message Retransmission Interval: 60 (unit:s)

Heartbeat Message Retransmission Count: 3

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

DSP Template Parameters

New Delete

	No.	Remote Telephone Number	DSP Template
☐	1		

User Advanced Parameters(H.248)

NO.	Line Name	Associated POTS
1	--	1
2	--	2

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)

Physical Port Parameters

Port ID: 1

Ringing Voltage: 74 Vrms

DC Voltage: 0 (unit:V)

Port TX gain: 0 db

Port RX gain: -7 db

Lower Threshold for Flash Hooking Duration: 90 (unit:ms)

Upper Threshold for Flash Hooking Duration: 300 (unit:ms)

On-hook Confirmation Time: 0 (unit:ms)

Impedance: 600 ohm

Feed Current: 25 (unit:mA)

CLIP Format: Mdmf-fsk

FSK Transmission Delay: 800 (unit:ms)

CLIP Flow: After ring

Enable DSP Template: ☐

Global DSP Template Name:

Display Time in CLIP: ☑

Enable DSP HighPass Filter: ☑

Enable Forced FSK Transmission: ☐

Apply Cancel

2. Click **Apply**.

Table 2 describes the advanced parameters used for configuring a VoIP interface based on the H.248 protocol.

Table 2 Advanced parameters used for configuring a VoIP interface based on the H.248 protocol

Parameter	Description

Parameter	Description
Enable Echo Cancellation	Echo is mainly produced in the PSTN user, the echo of user port allows remote users feel the affects call quality and.
Fax Transmode	The fax can be divided into fax pass through (G.711), T.38 fax (T.38 encoding).
Fax Switch Mode	Whether to participate in the SIP signaling, fax type can be divided into consultations fax, since switching the fax.
Profile Index	The system has built-in universal profile index, if does not meet the demand, according to the actual specific configuration Profile index.
Profile Parameters	If the profile index is **User-defined**, configure the profile parameter according to actual configurations.
Soft Parameter	Select the default software parameters.
Start Negotiate Version	H.248 version of the negotiations based on the profile parameter.
Digitmap Start Timer	Indicates the start timer of the digitmap. This timer starts up when a user picks up the phone and hears the dialing tone. If the user does not dial digits within the time specified by the timer, the call is released.
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.

NOTE:

Physical Interface Parameters and **Advanced User 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

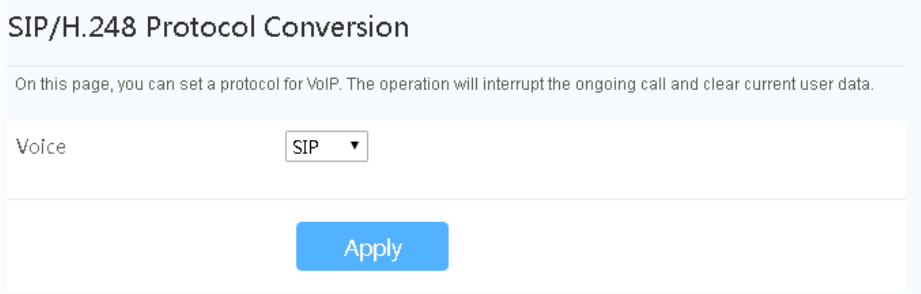
Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.6.8.3 SIP/H.248 Protocol Conversion

Click the **Advanced Configuration** > **Voice** tab, and choose **SIP/H.248 Protocol Conversion** from the navigation tree on the left.

1. In the right pane, you can change the VoIP protocol (SIP or H.248) by changing the value of the **Voice** parameter, as shown in Figure 1.

   Figure 1 SIP/H.248 Protocol Conversion

   NOTE:

   Exercise caution when performing this operation because it will interrupt the ongoing call and delete current data.

2. Click **Apply**.

Parent Topic: Voice

Copyright © Huawei Technologies Co., Ltd.
< 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 ONT Authentication.

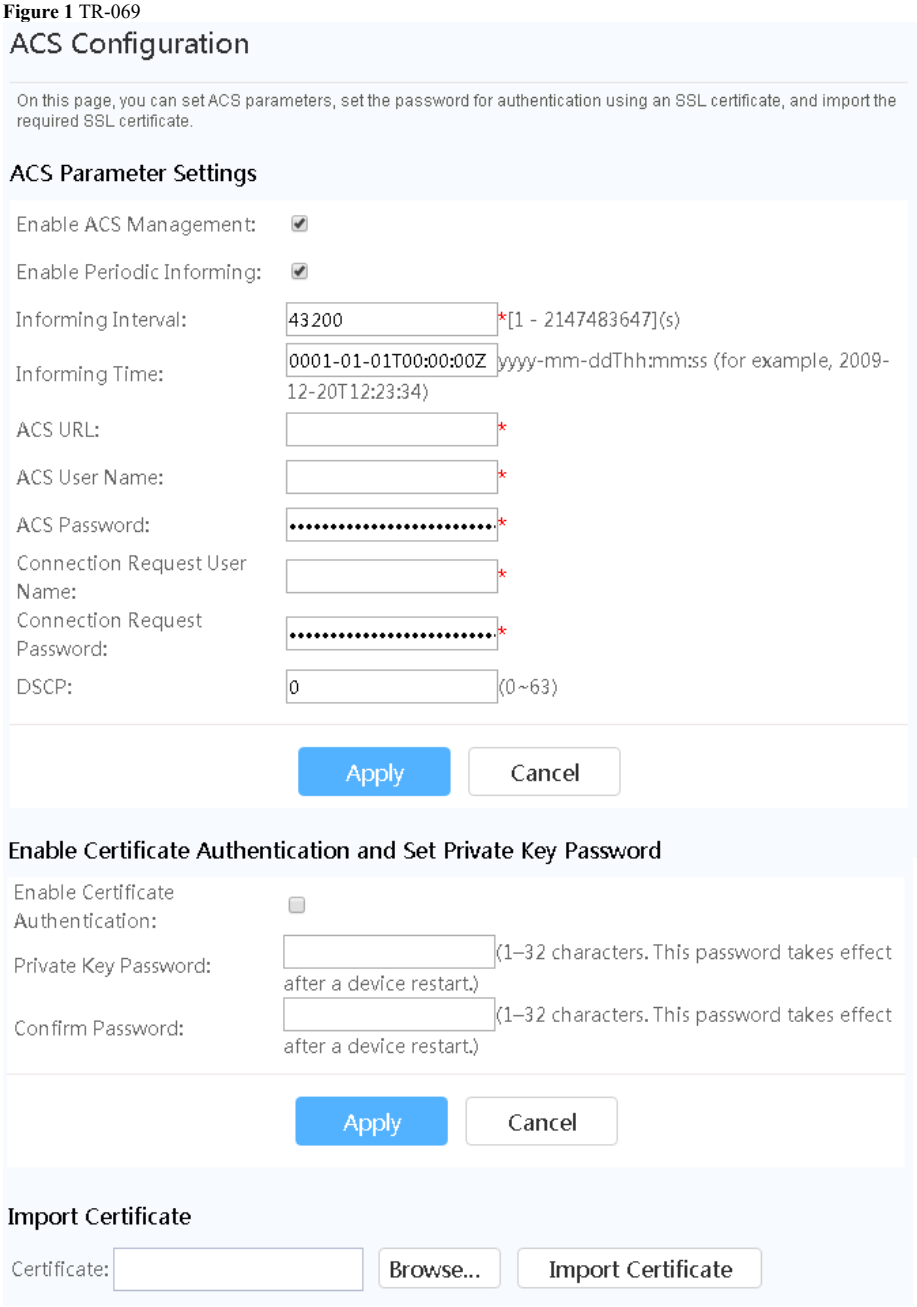
Parent Topic: Advanced Configuration

< 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, set the parameters related to the interconnection between the ONT and the TR-069 server, as shown in Figure 1.

Figure 1 TR-069



NOTE:

Configuring the interconnection between the ONT and the TR-069 requires creating a WAN interface. In addition, **Service List** 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	
Enable Periodic Informing	Indicates whether to enable the notification function. • If the notification function is enabled, the ONT actively sends a connection request to the TR-069 server. • If the notification function is disabled, the ONT does not actively send a connection request to the TR-069 server. When the notification function is enabled, the **Period Inform Interval** and **Period Inform Time** parameters can be set.

Parameter	Description
Informing Interval	Indicates the interval for the ONT to send a connection request to the TR-069 server.
Informing Time	Indicates the time for the ONT to send a connection request to the TR-069 server.
ACS URL	Indicates the address of the TR-069 server to which the ONT sends a connection request.
ACS User Name	Indicates the user name for the ONT to register with the TR-069 server.
ACS Password	Indicates the password for the ONT to register with the TR-069 server.
Connection Request User Name	Indicates the user name to be carried when the TR-069 server initiates a connection request to the ONT.
Connection Request Password	Indicates the password to be carried when the TR-069 server initiates a connection request to the ONT.
DSCP	Defined by RFC2474 "Definition of the Differentiated Services Field". Differentiated Services Code Point (DSCP) uses code values for priority marking. DSCP can be customized for carriers based on service requirements so that devices on a network perform QoS based on the DSCP value.
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.

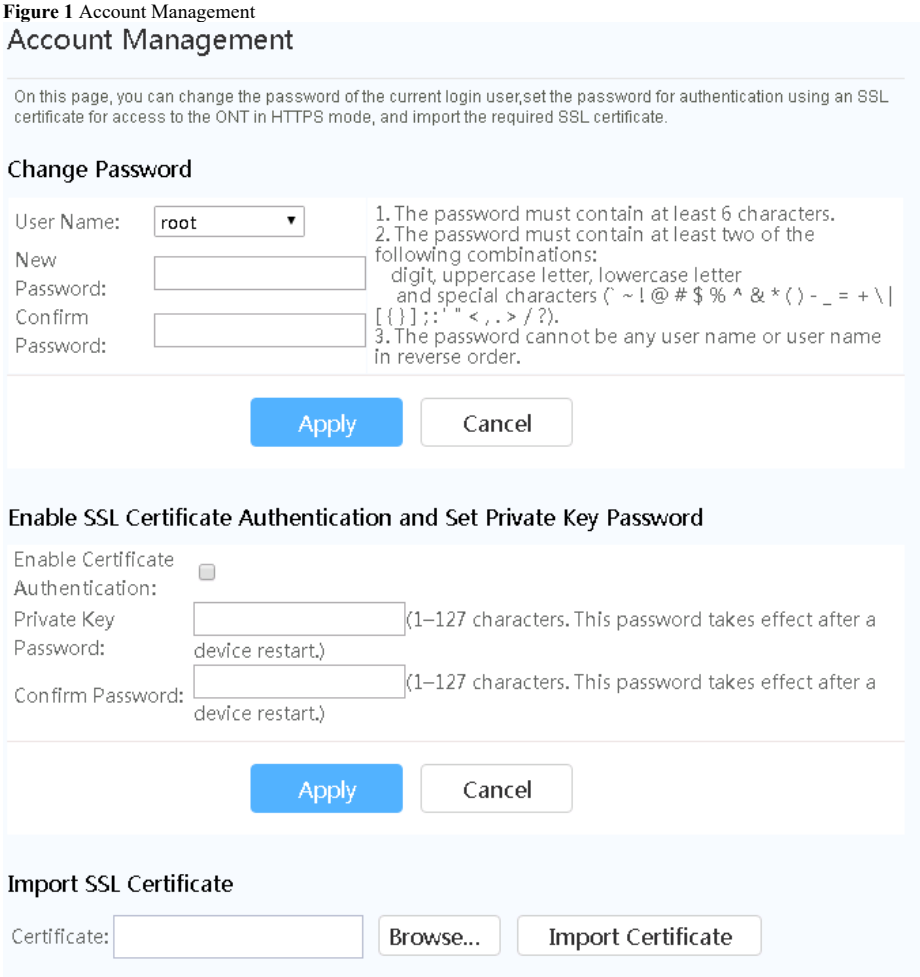
Parent Topic: System Management

Copyright © Huawei Technologies Co., Ltd.
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 right pane, change the password of the **root** user, as shown in Figure 1.

Figure 1 Account Management



NOTE:

- After the user logs in to the ONT Web interface using the default common user name and password, the **Account Management** interface is automatically displayed, prompting the user to change the initial password. After the user successfully changes the password, the **Account Management** interface is no

longer displayed in the following logins.

- Change the initial user name and password after logging in to the web page.

2. Click **Apply**.

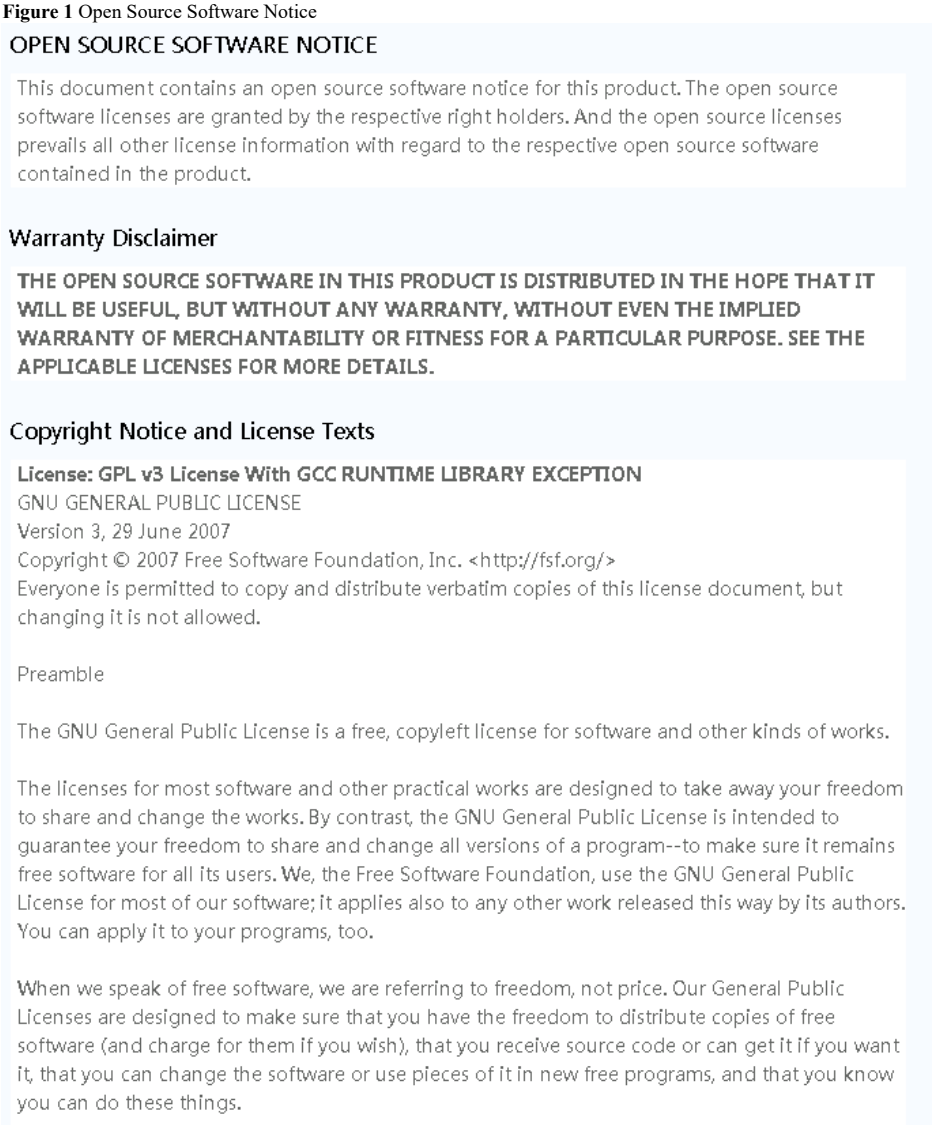
Parent Topic: System Management

Copyright © Huawei Technologies Co., Ltd.
< 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



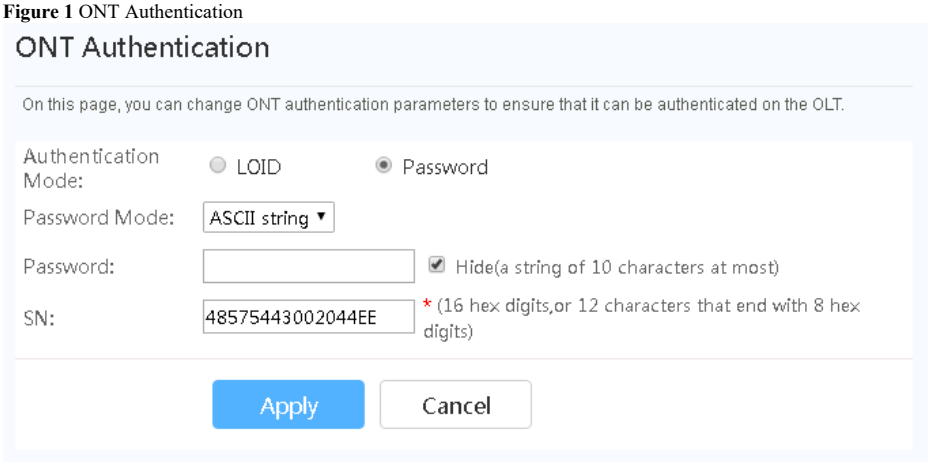
Parent Topic: System Management

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.6.9.4 ONT Authentication

1. In the navigation tree on the left, choose **Advanced Configuration** > **System Management** > **ONT Authentication**. In the pane on the right, you can view or change the authentication mode for the registration of the ONT on the OLT, as shown in Figure 1.

Figure 1 ONT Authentication



2. Click **Apply**.

NOTE:

The user can modify the ONT SN or password by using the phone on condition that the ONT is offline. The modification is performed as follows:

Connect the phone to the POTS port on an ONT, dial "**SN**SN#" or "**password**password#" , and then restart the ONT.

Parent Topic: System Management

Copyright © Huawei Technologies Co., Ltd.
< 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 and upgrade software version.

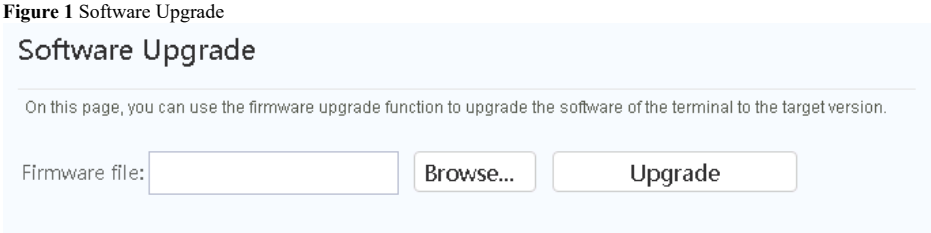
Parent Topic: Advanced Configuration

Copyright © Huawei Technologies Co., Ltd.
< Previous topic

1.6.10.1 Software Upgrade

1. Click **Advanced Configuration** > **Maintenance diagnose** tab, and choose **Software Upgrade**. In the dialog box that is displayed, select the target software version of the device. Click **Update** 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.

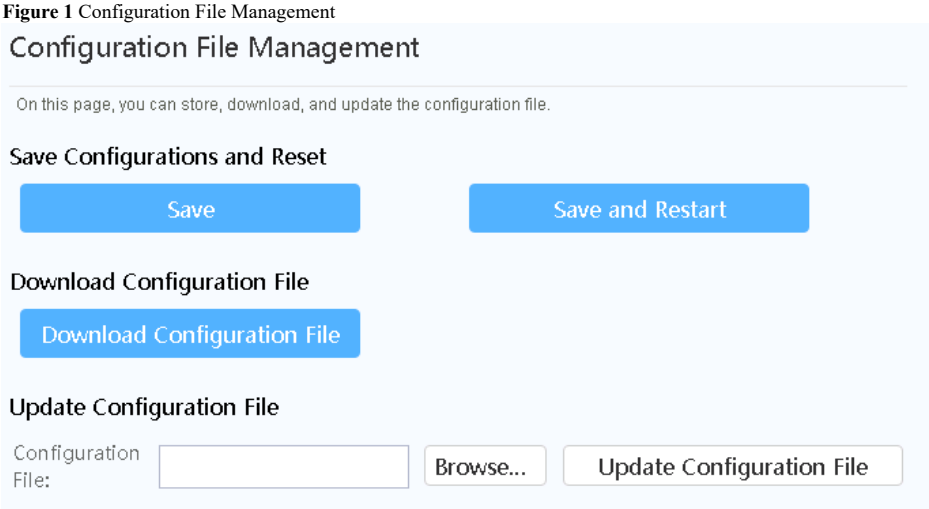
Parent Topic: Maintenance Diagnose

Copyright © Huawei Technologies Co., Ltd.
Next topic >

1.6.10.2 Configuration File Management

Click **Advanced Configuration** > **Maintenance diagnose** tab, and choose **Configuration File Management**. in the navigation tree on the left. 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 ONT.
- 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.

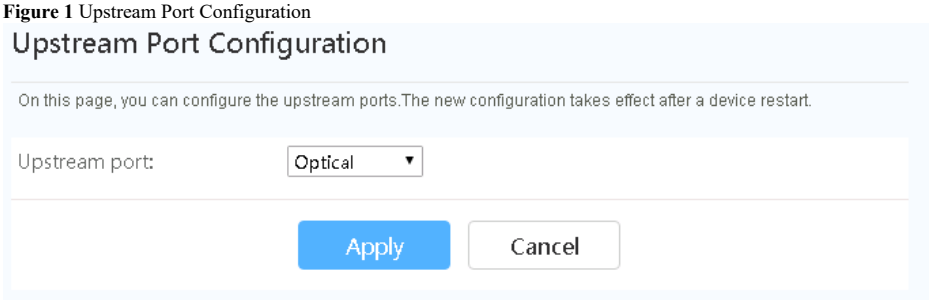
Parent Topic: Maintenance Diagnose

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.6.10.3 Upstream Port Configuration

1. Click the **Advanced Configuration** > **Maintenance diagnose** tab, and choose **Upstream Port Configuration** from the navigation tree on the left. In the right pane, set the **Upstream port** type, as shown in Figure 1.

   Figure 1 Upstream Port Configuration



2. Click **Apply**.

Parent Topic: Maintenance Diagnose

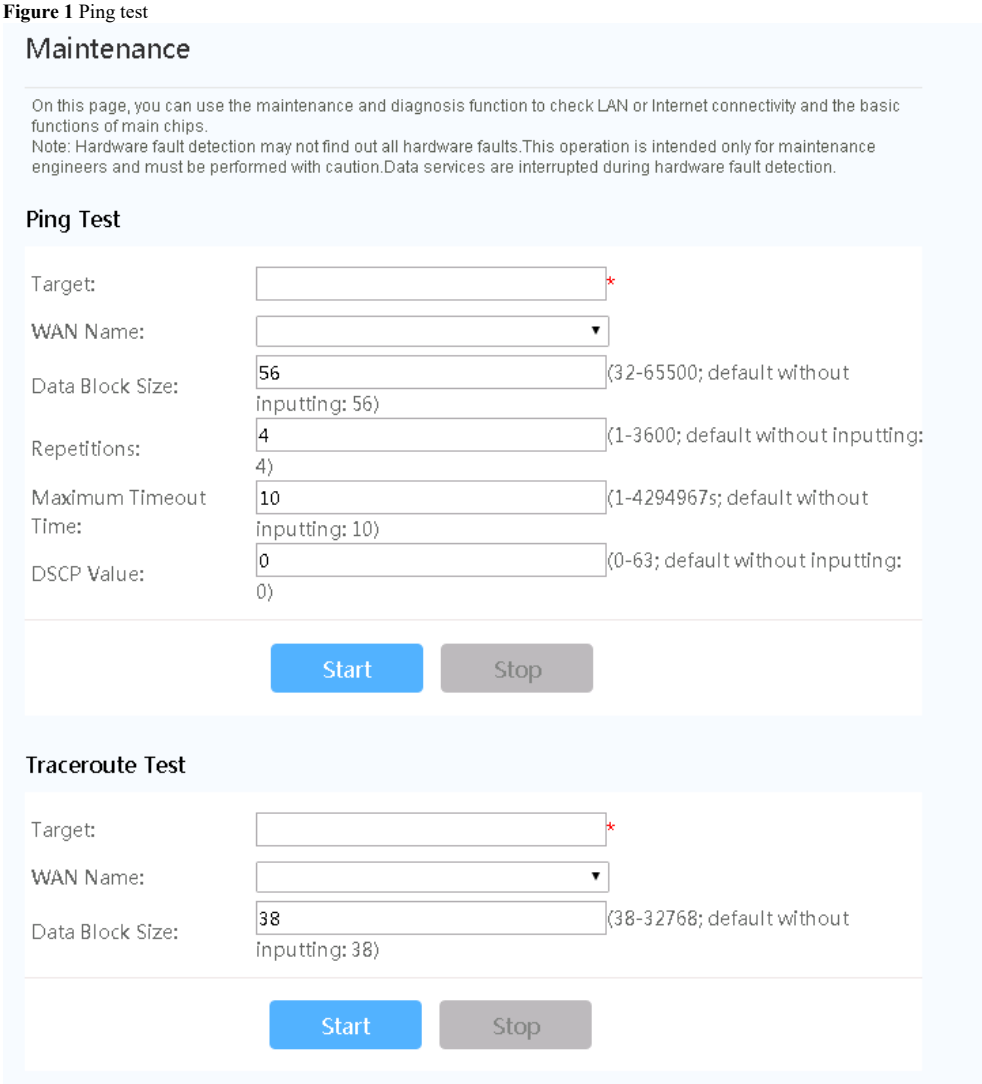
Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.6.10.4 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** and **WAN name**, and then click **Start**, as shown in Figure 1.

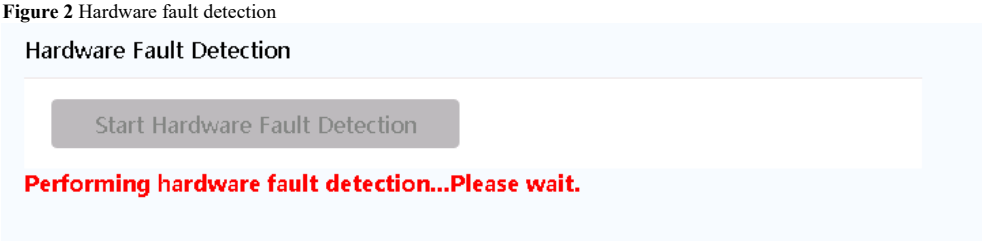
Figure 1 Ping test



- If the ping test is successful, **The result** is displayed as **PASS**, that is, the ONT can interwork with the device with the destination IP address.
- If the ping test fails, **The result** is displayed as **FAIL**, that is, the ONT cannot interwork with the device with the destination IP address.

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

Figure 2 Hardware fault detection



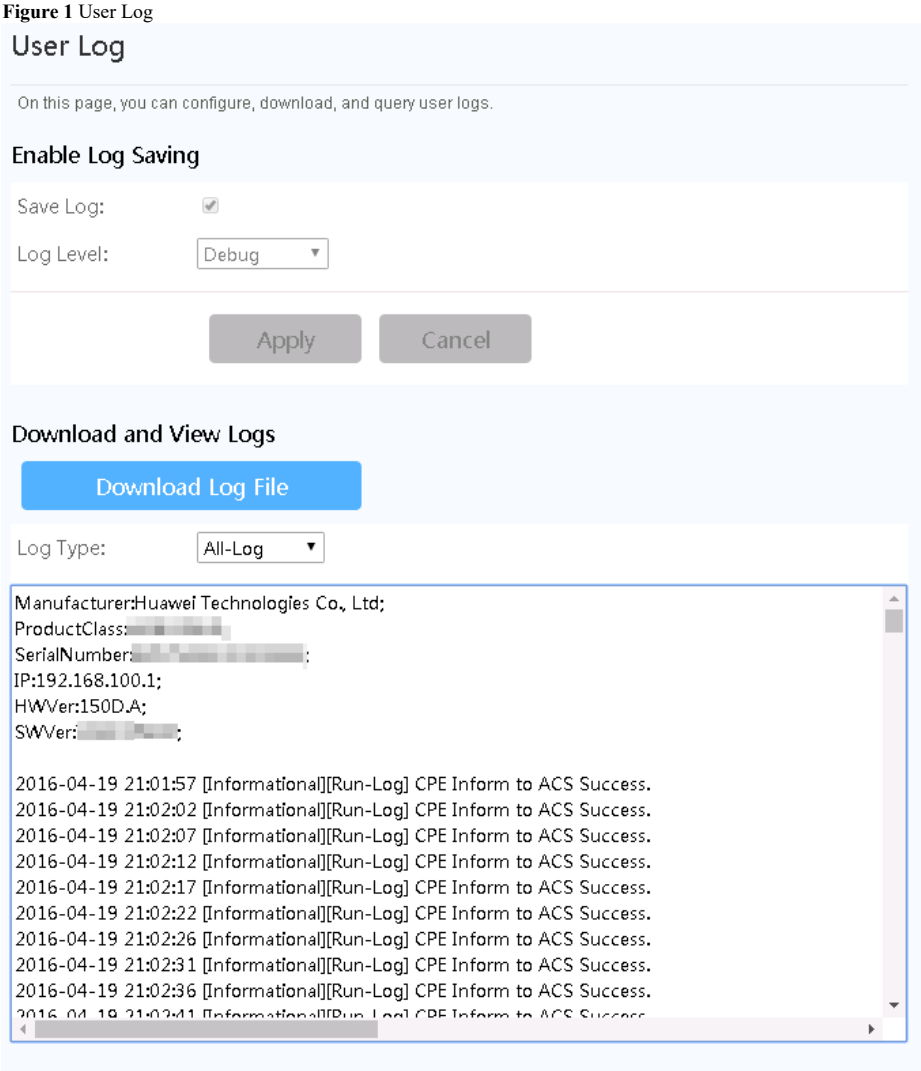
Parent Topic: Maintenance Diagnose

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.6.10.5 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 can not be configured on the Web page.
- You cannot configure **Log Level**, which indicates the level of the saved log. The log whose level is equal to or higher than the debug-level log is saved.
- Click **Download Log File**. In the dialog box that is displayed, click **Save**, specify the path for saving the log file, and save the log file to the local disk.

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.

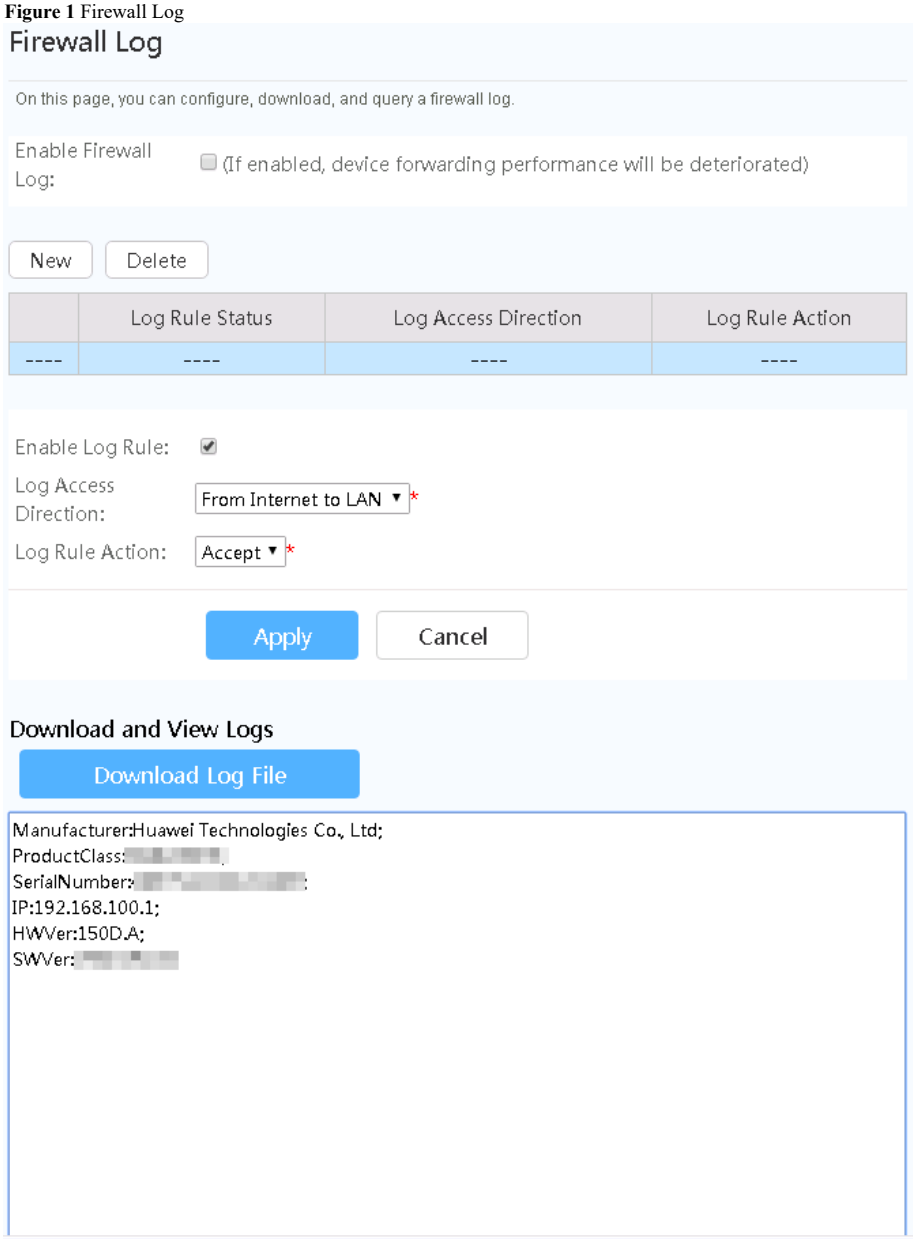
Parent Topic: Maintenance Diagnose

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.6.10.6 Firewall Log

Click the **Advanced Configuration** > **Maintenance Diagnose** tab, and choose **Firewall Log** from the navigation tree on the left. In the pane on the right, you can viewl 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 **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

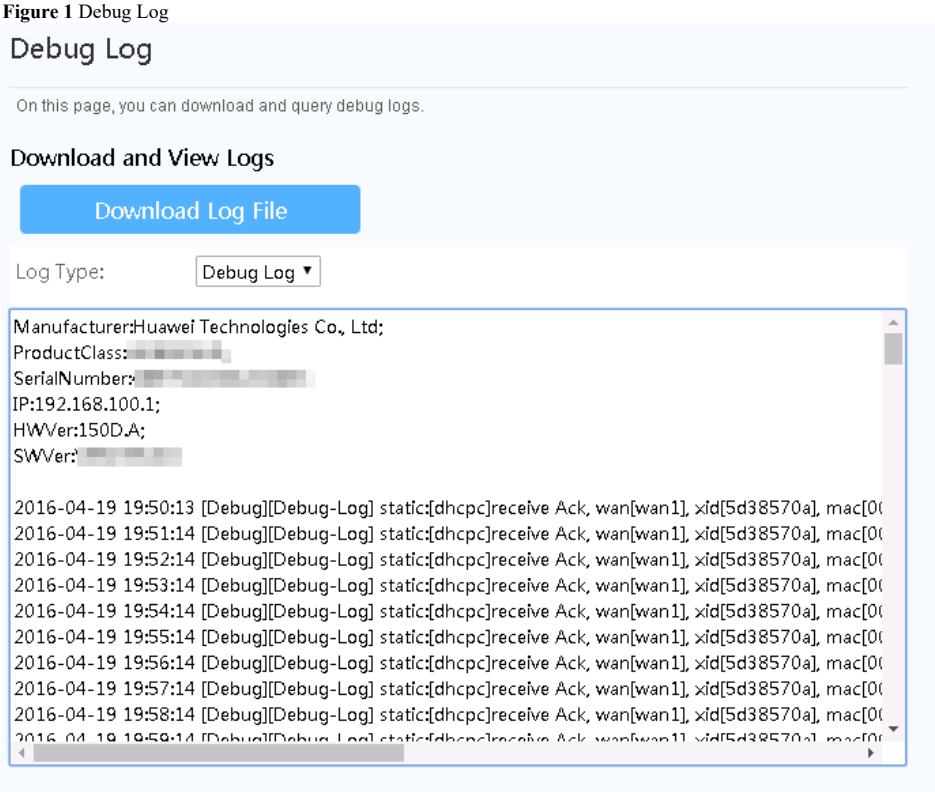
Copyright © Huawei Technologies Co., Ltd.

< Previous topic Next topic >

1.6.10.7 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.

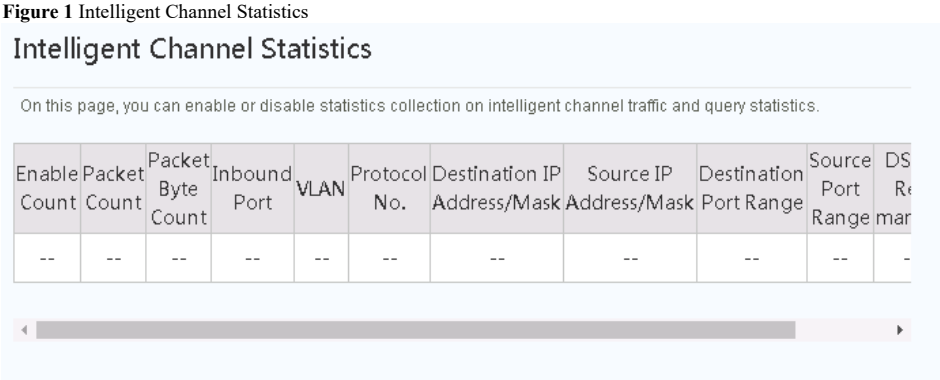
Parent Topic: Maintenance Diagnose

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.6.10.8 Intelligent Channel Statistics

1. Click the **Maintenance Diagnose** tab and choose **Intelligent Channel Statistics** from the navigation tree. In the right pane, select **Enable Count** to enable traffic statistics collection for intelligent channels, as shown in Figure 1.

Figure 1 Intelligent Channel Statistics



NOTE:

You can enable traffic statistics collection only when intelligent channels are configured and **Intelligent Channel Enabled** is selected on **Application** > **Intelligent Channel Configuration**.

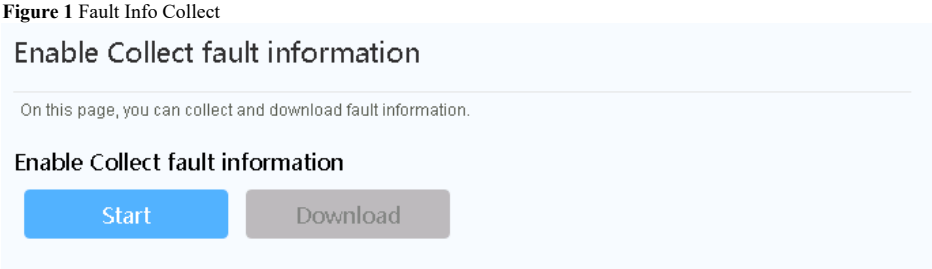
Parent Topic: Maintenance Diagnose

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.6.10.9 Fault Info Collect

Click the **Advanced Configuration** > **Maintenance Diagnose** tab, and choose **Fault Info Collect** from the navigation tree on the left. In the right pane, click **Start** to collect ONT 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

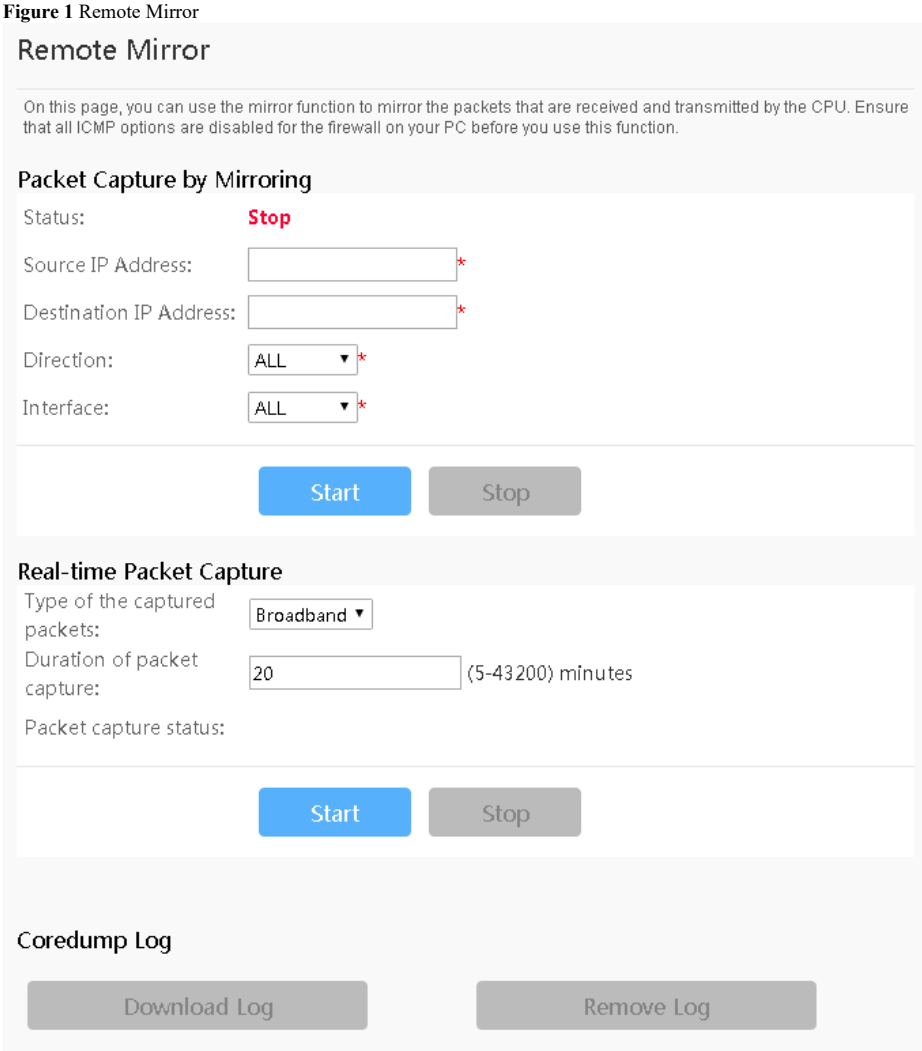
Copyright © Huawei Technologies Co., Ltd.

< Previous topic Next topic >

1.6.10.10 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.
- Type of the captured packets: indicates the type of the captured packets that are broadband, wifi and voice .

2. click **Start**.

NOTE:

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

Based on 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.

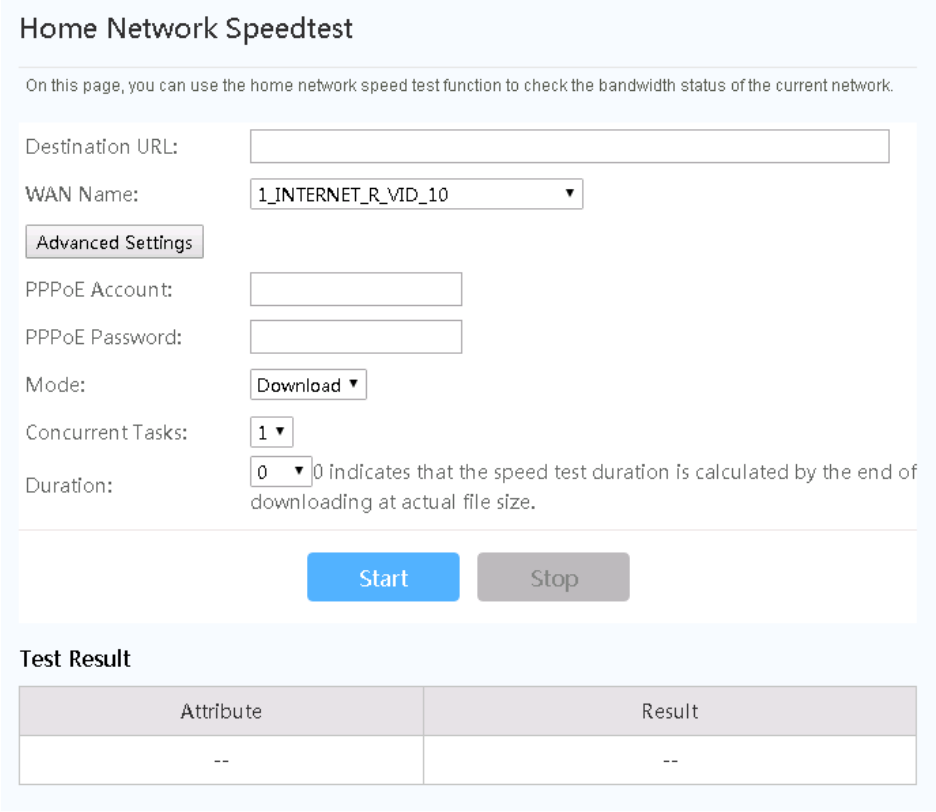
Parent Topic: Maintenance Diagnose

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.6.10.11 Home Network Speedtest

In the navigation tree on the left, choose **Advanced Configuration** > **Maintenance Diagnose** > **Home Network Speedtest**. In the pane on the right, enter the destination URL and select a WAN name from the drop-down box. Click **Start** to test the network speed, as shown in Figure 1.

Figure 1 Home Network Speedtest



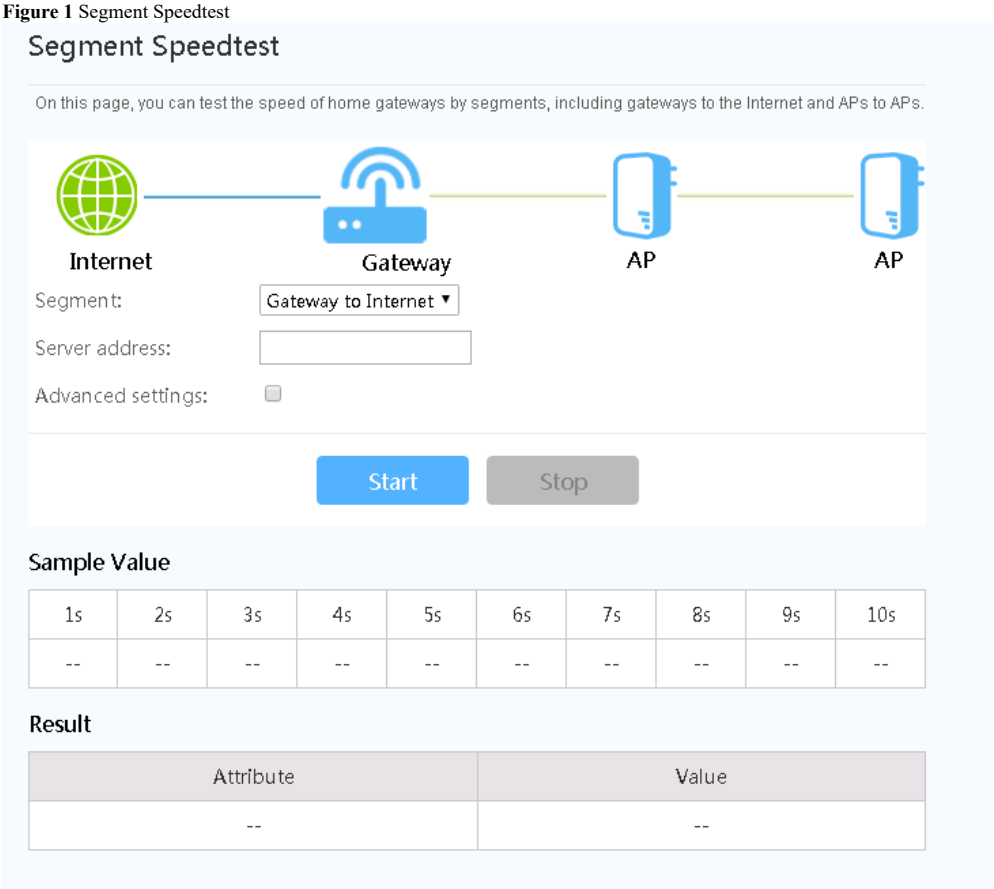
Parent Topic: Maintenance Diagnose

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.6.10.12 Segment Speedtest

In the navigation tree on the left, choose **Advanced Configuration** > **Maintenance Diagnose** > **Segment Speedtest**. In the pane on the right, select **Gateway to Internet** or **AP to AP**. Configure other settings according to the prompt. Click **Start** to start testing the home network speed by segment, as shown in Figure 1.

Figure 1 Segment Speedtest



Parent Topic: Maintenance Diagnose

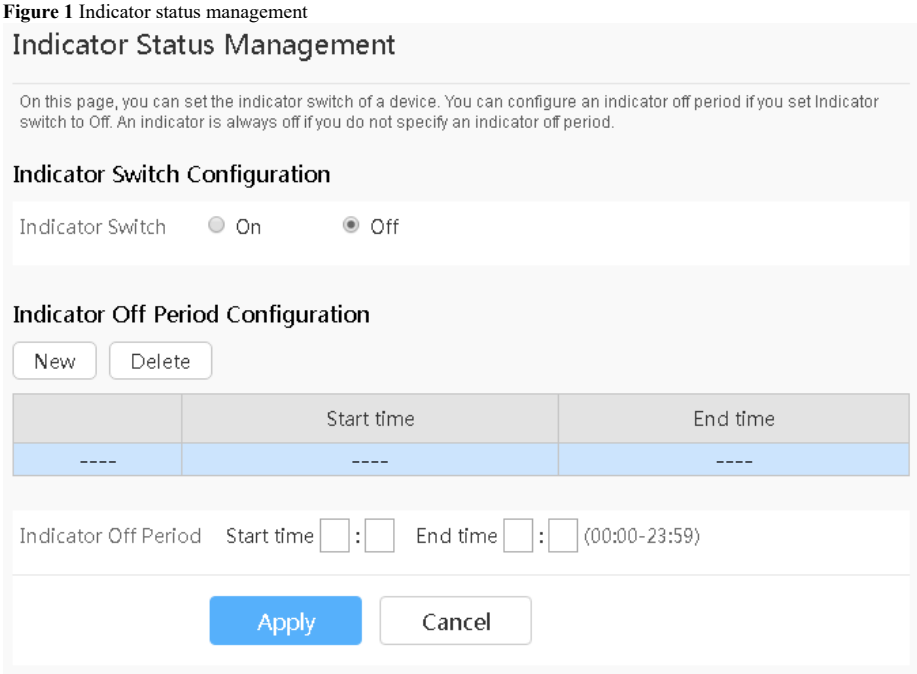
Copyright © Huawei Technologies Co., Ltd.

< Previous topic Next topic >

1.6.10.13 Indicator Status Management

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

   Figure 1 Indicator status management

   NOTE:

   If both **Global indicator disabling time segment** and **Customized indicator disabling time segment** are configured, **Customized indicator disabling time segment** takes effect if **Whether to Validate Customized Time Segments** is selected for **Customized indicator disabling time segment**, and **Global indicator disabling time segment** takes effect if **Whether to Validate Customized Time Segments** is not selected.

2. Click **Apply**.

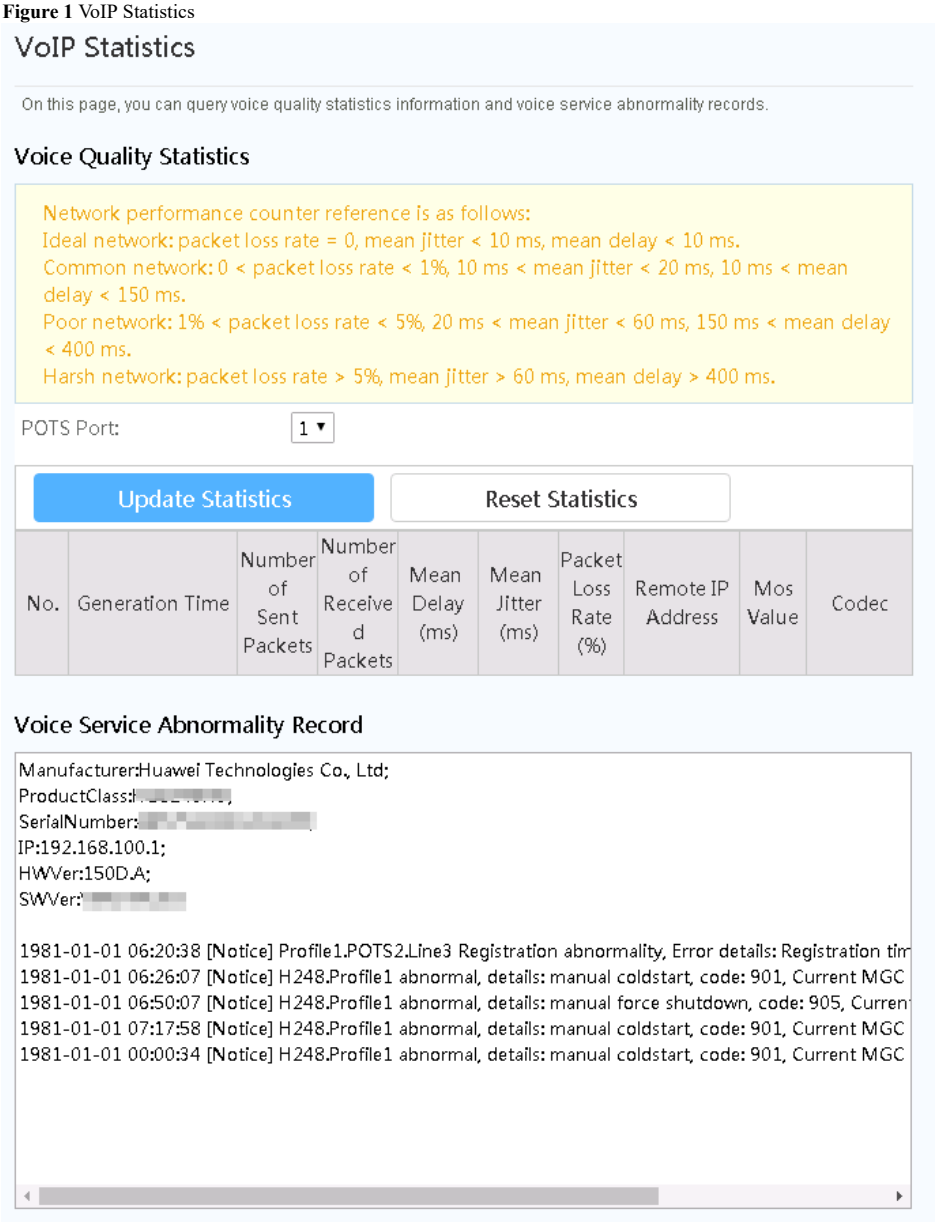
Parent Topic: Maintenance Diagnose

Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.6.10.14 VoIP Statistics

Click the **Advanced Configuration** > **Maintenance Diagnose** tab, and choose **VoIP Statistics** from the navigation tree on the left. In the right pane, query voice quality statistics information and voice service abnormality records, as shown in Figure 1.

Figure 1 VoIP Statistics



Parent Topic: Maintenance Diagnose

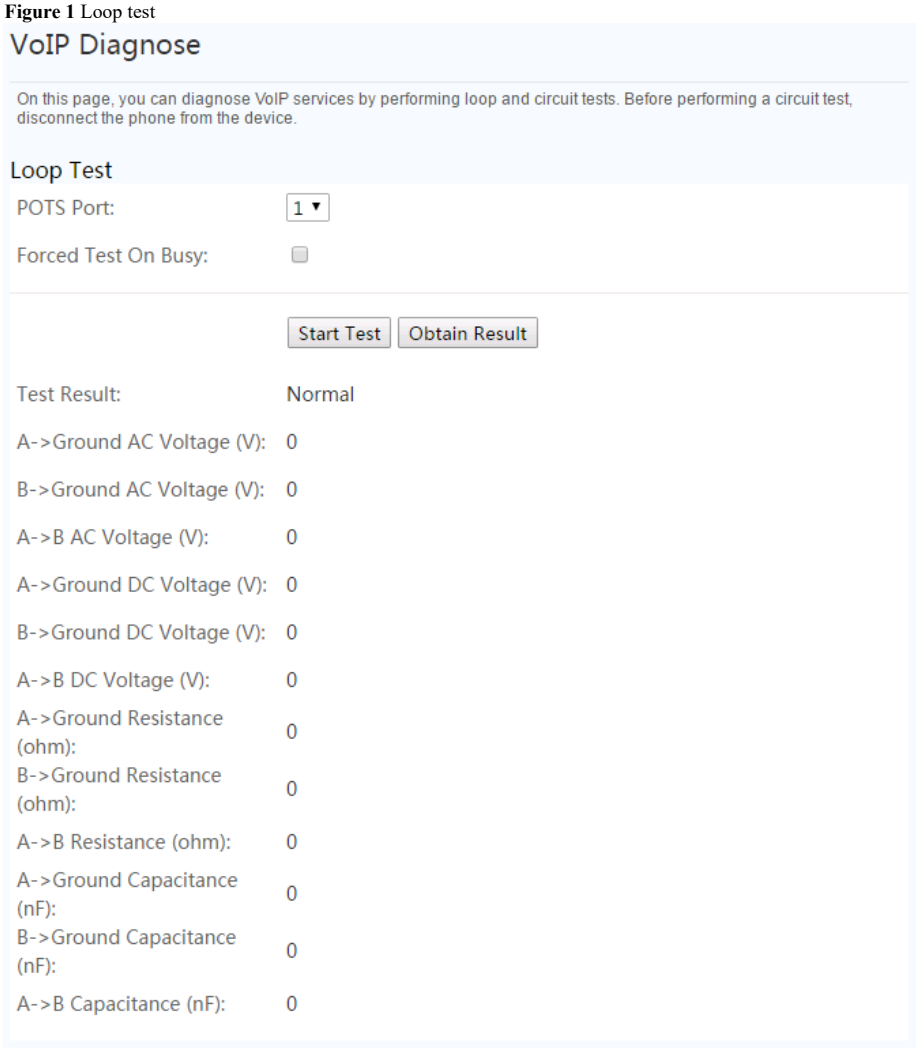
Copyright © Huawei Technologies Co., Ltd.
< Previous topic Next topic >

1.6.10.15 VoIP Diagnose

Click the **Advanced Configuration** > **Maintenance Diagnose** tab, and choose **VoIP Diagnose** from the navigation tree on the left. In the right pane, set **POTS Port** and click **Start Test** to start a voice loop line or circuit line test.

- Figure 1 shows the parameter settings for a loop line test.

Figure 1 Loop test

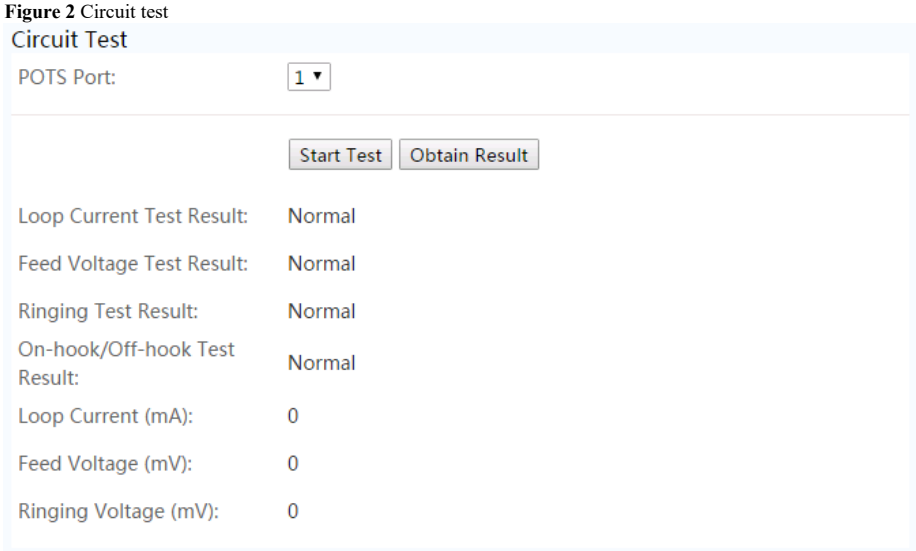


NOTE:

If you want to perform a loop line test during a call, select **Forced Test On Busy**.

- Figure 2 shows the parameter settings for a circuit line test.

Figure 2 Circuit test



Parent Topic: Maintenance Diagnose

Copyright © Huawei Technologies Co., Ltd.
< Previous topic