HG6145D2

GPON Optical Network Terminal

Product Manual

Version: 01

FiberHome Telecommunication Technologies Co., Ltd.

July 2022

Trademarks and Permissions


®and other FiberHome trademarks are trademarks of FiberHome Telecommunication Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Legal Notice

The purchased products, services or features shall be subject to the commercial contracts made between FiberHome and the customer. All or part of the products, services or features described in this document may not be within the purchase or usage scope.

Information in this document is subject to change without notice. All statements, information and recommendations in this document are believed to be accurate but do not constitute the warranty of any kind, express or implied.

FiberHome Telecommunication Technologies Co., Ltd.

Address: No.6, Gaoxinsilu, High-Tech Development Zone, Wuhan, Hubei Province, P. R. China

Postcode: 430205

Website: http://www.fiberhome.com

Tel: +86 800-8800787; +86 400-8890787

Safety Precautions

For your correct and safe operations on the equipment, please carefully read and strictly observe the following safety instructions:

- High optical power can cause bodily harm, especially to eyes. Never look directly into the end of the optical transmitter fiber jumper or the end of its active connector.
- Exercise care if you must bend fibers. If bends are necessary, the fiber bending radius should never be less than 38 mm.
- Overloaded power sockets or damaged cables and connectors may cause electric shock or fire. Regularly check electrical cables. If any of them is damaged, replace it immediately.
- Use the power supply adapter provided in the package only. Using other adapters may cause equipment damage or operation failures.
- Install the equipment in a well-ventilated environment without high temperature or direct sunlight to protect the equipment and its components from overheating, which may result in damage.
- Cut off the power supply for the equipment in lightning weather and disconnect all the wires and cables (such as the power cable, network cable and phone cable) from the equipment, so as to prevent the equipment from being damaged by lightning.
- Do not place the equipment in a wet or damp environment. Water seepage will lead to abnormal operation of the equipment and short circuit, which may cause dangers and should be prohibited.
- Do not lay this equipment on an unsteady base.

Contents

1 Preface

HG6145D2 Product Manual introduces the positioning, features, functions and technical specifications of the HG6145D2 as well as web configurations and handling of common problems, so that readers can have an overall idea about the product.

Intended readers for this manual are marketing personnel, commissioning engineers, and operation and maintenance engineers.

Version

Version	Description
01	Initial version.

Symbol Conventions

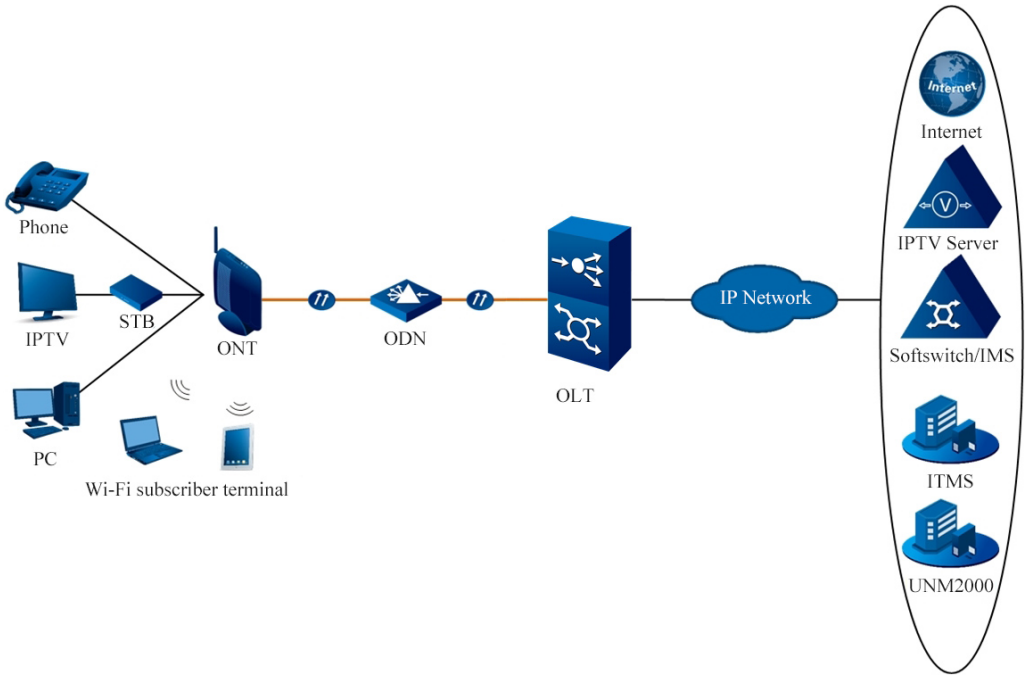
Symbol	Meaning	Description
	Note	Important features or operation guide.
	Caution	Possible injury to persons or systems, or cause traffic interruption or loss.
	Warning	May cause severe bodily injuries.

2 Product Introduction

2.1 Product Positioning

The HG6145D2 is an FTTH-type GPON optical network terminal. It provides users with communication and entertainment services in the form of data, voice, video and so on, to meet the integrated access demand of families and small-scaled enterprises.

The figure below shows the network positioning of the HG6145D2.



2.2 Product Specification

The tables below describe the interfaces and services supported by the HG6145D2, which can be referred to for ONT configuration.

Table 2-1 Interfaces Supported by the HG6145D2

ONT Type	Ethernet Interface Quantity	POTS Interface Quantity	Wi-Fi Interface Quantity	USB Interface Quantity	CATV interface Quantity
HG6145D2	4 (GE)	1	√ (2.4 GHz, 5 GHz)	2	-

Table 2-2 Service Types Supported by the HG6145D2

ONT Type	Internet Service	Multicast Service	Voice Service	Wi-Fi Service
HG6145D2	√	√	√	√
"√" indicates "supported"; "×" indicates "not supported".				

Service Reliability

The HG6145D2 supports MTBF up to 30 000 hours.

2.3 Interface Specifications

2.3.1 GPON Interface

Item	Specification
Standard compliance	ITU-T G.984, Class B+
Transmission rate	Rx: 2.5 Gbit/s; Tx: 1.25 Gbit/s
Interface mode	Single-mode
Interface type	SC/UPC
Maximum transmission distance	20 km
Central wavelength	Tx: 1310 nm; Rx: 1490 nm
Optical power	Tx.: 0.5 dBm to 5.0 dBm; Rx.: -8 dBm to -27 dBm
Extinction ratio	11 dB to 14 dB
Receiving sensitivity	-27 dBm
Maximum overload optical power	-8 dBm

2.3.2 LAN Interface

Item	Specification
Standard compliance	IEEE 802.3ab
Interface type	RJ-45
Interface rate	10 Mbit/s, 100 Mbit/s or 1000 Mbit/s
Maximum transmission distance	100 m

Item	Specification
Working mode	Supports full-duplex / half-duplex and auto negotiation to rates 10/100/1000 Mbit/s.
Specifications of the cable used	CAT-5 unshielded twisted pair

2.3.3 POTS Interface

Item	Specification
Interface type	RJ-11
Transmission rate	64 Kbit/s
Cable type	Twisted-pair cable
Line code	PCM

2.3.4 Wi-Fi Interface

Item	Specification
Standard compliance	IEEE 802.11 a/b/g/n/ac
Operating band	2.4GHz / 5GHz
Specifications	Four SSIDs and 13 working channels for the 2.4 GHz band; four SSIDs and 20 working channels for the 5 GHz band. Automatic rate adjustment and launched power adjustment for both the 2.4GHz and the 5 GHz bands.
Authentication mode	Open, WPA2-PSK and WPA-PSK/WPA2-PSK
Encryption mode	WEP, AES and TKIP / AES

2.3.5 USB Interface

Item	Specification
Standard compliance	2 × USB2.0
Transmission rate	20 MB/s

2.4 Introduction to the HG6145D2

2.4.1 Appearance

This section describes the appearance of the HG6145D2, including the overall look, interfaces, buttons, and indicator LEDs.

Note:

The pictures here are only for reference.

Appearance

The overall look of the HG6145D2 is shown in Figure 2-1.

Figure 2-1 Overall Look of the HG6145D2

Interfaces and Buttons

Interfaces and buttons of the HG6145D2 are located on the rear, side and bottom panels of the equipment. Figure 2-2, Figure 2-3 and Figure 2-4 show the rear panel, side panel and bottom panel respectively.

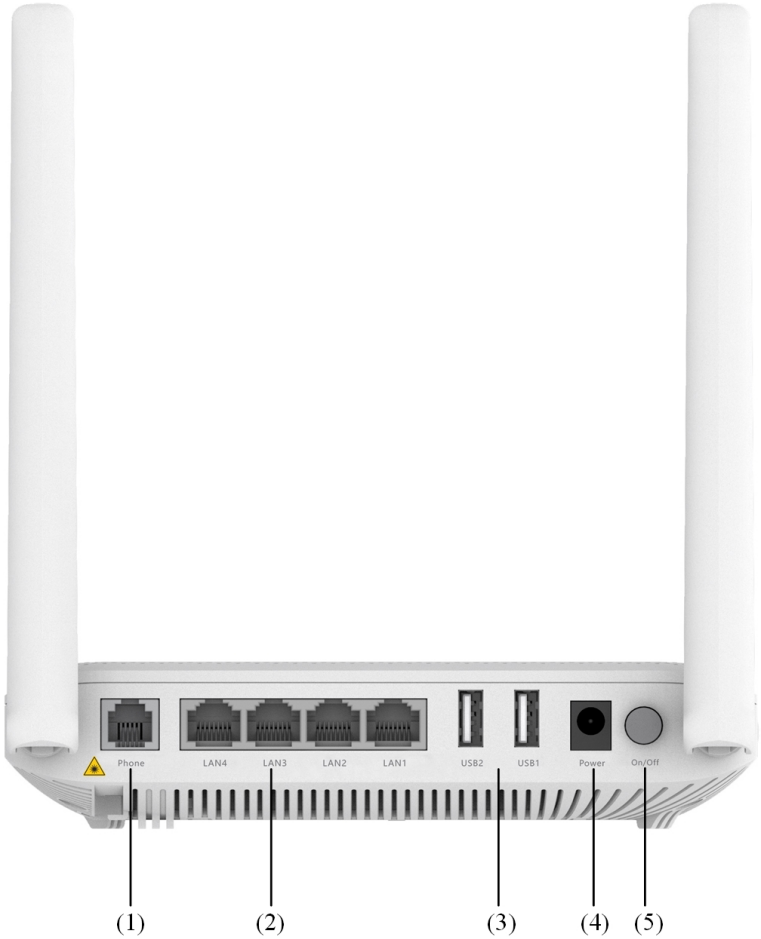


Figure 2-2 Rear Panel of the HG6145D2

Figure 2-3 Side Panel of the HG6145D2

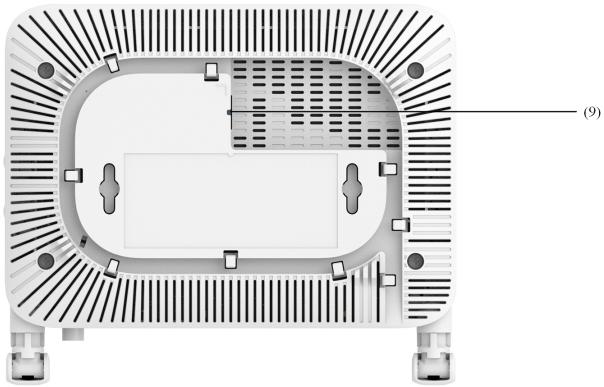


Figure 2-4 Bottom Panel of the HG6145D2

Table 2-3 describes the interfaces and buttons on the HG6145D2.

Table 2-3 Interfaces and Buttons on the HG6145D2

No.	Interface and Button	Description	Function
(1)	Phone	Telephone interface	Connects to the subscriber's telephone.
(2)	LAN1 to LAN4	Ethernet interface	Connects to the computer, IP router or IP set top box.
(3)	USB1, USB2	USB Host interface	Connects to the USB interface storage device.
(4)	Power	Power interface	Connects to the power adapter.
(5)	On/Off	Power switch	Turns on or off the power for the equipment.
(6)	Reset	Reboot hole	Insert a thin rod like a small needle or paper clip into the hole, and press the hole for no more than five seconds to restart the device, or press the hole for over 10 seconds to restore the factory settings and restart the device.
(7)	WLAN	WLAN function button	Enables / disables the WLAN function.
(8)	WPS	WPS function button	Enables / disables WLAN data encryption.
(9)	PON	Fiber interface	Connects with the optical fiber for uplink access.

Indicator LEDs

Indicator LEDs of the HG6145D2 are located on the front panel of the equipment.

Table 2-4 Indicator LEDs on the HG6145D2

Indicator LED	Meaning	Color	Status	Status Description
Power	Power status indicator LED	Green	ON	The device is powered on.
			OFF	The device is not powered on.
PON	Register status indicator LED	Green	ON	The ONT has been activated.
			Blinking	The ONT is being activated.
			OFF	Activation of the ONT is not yet started.
LOS	Optical signal status indicator LED	Red	Blinking	The device has not received the optical signal.
			OFF	The device has received the optical signal.
Internet	Broadband status indicator LED	Green	ON	Connection to the broadband network is normal.

Table 2-4 Indicator LEDs on the HG6145D2 (Continued)

Indicator LED	Meaning	Color	Status	Status Description
			Blinking	Connection to the broadband network is normal with data transmission.
			OFF	Not connected to the broadband network.
2.4G, 5G	2.4G/5G wireless signal status indicator LED	Green	ON	The 2.4G/5G wireless interface is enabled.
			Blinking	The 2.4G/5G wireless interface is transmitting / receiving data.
			OFF	The 2.4G/5G wireless interface is disabled.
WPS	WPS status indicator LED	Green	ON	WPS is enabled, and the Wi-Fi terminal has been connected to the ONT.
			Blinking	WPS is in use for relevant negotiation.
			OFF	WPS is not enabled, or the Wi-Fi terminal is not connected to the ONT.
USB1, USB2	USB indicator LED	Green	ON	The USB is connected.
			OFF	The USB is not connected.
LAN1 to LAN4	Ethernet interface status indicator LED	Green	ON	The interface is connected to the user terminal and no data is transmitted.
			Blinking	The interface is transmitting / receiving data.
			OFF	The interface is not connected to the user terminal.
Phone	Phone port status indicator LED	Green	ON	The port is registered in the softswitch system.
			Blinking	Service flow is found at the port.
			OFF	The port is not registered in the softswitch system.

2.4.2 Product Characteristics

The HG6145D2 can be used together with the OLT equipment to make up a GPON system and provide users with access to multiple services. The HG6145D2 has the following characteristics:

GPON Access Capability

- Conforms to ITU-T G.984 series of standards, with good interoperability.
- Provides large-capacity GPON transmission bandwidth: supports the downlink rate up to 2.5 Gbit/s and the uplink rate up to 1.25 Gbit/s.
- Supports the dynamic bandwidth allocation (DBA) algorithm.
- Supports long-haul transmission. The maximum transmission distance can reach 20 km.

Abundant Service Types

Provides abundant physical interfaces on the subscriber side to access multiple services such as Internet access, video, voice and home storage services.

Wi-Fi Wireless Access

- Provides Wi-Fi wireless access based on IEEE 802.11 a/b/g/n/ac to help you set up a safe and reliable wireless network.
- Compatible with IEEE 802.11 a/b/g/n/ac and authenticated by Wi-Fi Alliance, with good compatibility with other WLAN devices.
- Supports eight SSIDs (four for the 2.4 GHz band and another four for the 5 GHz band) so that users can set different wireless networks as needed.
- Supports multiple authentication and encryption modes to provide users with safe and reliable wireless access approaches.

Network Storage and File Sharing

- Provides a USB interface for connection with the USB interface storage device to provide convenient network storage and file sharing service.
- Supports plug-and-play and hot insertion of the USB interface.
- Supports configuration of the USB function based on the Web page to facilitate file sharing in the family network.
- Supports network storage based on FTP to provide the FTP client and server end functions. Users can download files from the FTP server in a public network to the USB interface storage device or access the USB interface storage device on the ONT via the FTP client end on the PC.

Gateway Functions

- Serves as home gateway and provides abundant and reliable gateway functions.
- Functions as the DHCP Server to cater for application demands in different scenarios.
- Supports configuring protection against DoS attacks, filtering of MAC addresses, IP addresses and URL addresses, firewall and ACL rules to guarantee safe operation of the equipment.

Remote Automatic Service Provisioning, Maintenance and Management

- Supports configuring the user-defined upgrade policies through the network management system so that the equipment can be upgraded automatically after being powered on.
- Supports collecting performance data of the ONT remotely via the network management system to enable real-time monitoring of the network performance.
- Supports remote fault isolation for the ONT via the network management system. Faults can be isolated remotely according to the alarms reported to reduce the maintenance cost.

2.4.3 Functions and Features

Item		Description
GPON	GPON interface specifications	Compliant with standards ITU-T G.984.1, G.984.2, G.984.3 and G.984.4.
		Supports GEM encapsulation (Ethernet over GEM is supported, but ATM encapsulation is not supported).
		The GPON system adopts the single-fiber bidirectional transmission mechanism, using the TDMA mode with the wavelength 1310 nm in the uplink direction, and the broadcast mode with the wavelength 1490 nm in the downlink direction.
		Supports embedded OAM messages, PLOAM messages and OMCI messages.
		Supports slicing of data messages and OMCI protocol messages in the uplink direction. Message slices with both adaptive length and fixed length are supported.
	GEM port	Supports bearing the downlink broadcast messages and unknown multicast messages via the broadcast GEM ports.
		Supports mapping from GEM ports to T-CONTs.

Item		Description
		Supports multiple flow mapping modes:
		Supports the GEM port loopback.
	T-CONT	Supports the T-CONTs of Type1 to Type 5.
		A T-CONT supports no less than 64 GEM ports.
		Supports eight T-CONTs.
	DBA	Supports DBA in the SR and NSR modes.
		Supports DBA Piggy-back DBRu Mode 0.
	FEC	Supports bi-directional FEC: downlink FEC decoding and uplink FEC encoding.
		Supports downlink FEC performance statistics.
	Encryption	Supports encryption for the downlink unicast data channel.
		Supports the AES-128 encryption algorithm.
		Supports generation of the key and response to the OLT's request for key.
		Supports OMCI channel encryption.
	Registration authentication	Supports the ONT registration process as specified in ITU-T. G.984.3.
		Supports four authentication modes: SN, Password, SN + Password and LOID.
		Supports performance statistics for the Ethernet interface.
		Supports performance statistics for the GEM ports.
Ethernet		Complies with the IEEE 802.3 standard.
		Supports configuring the Ethernet interface rate, working mode, and MDI/MDIX auto-negotiation mode.
		Supports manual configuration of the rate 10/100/1000 Mbit/s.
		Supports manual configuration of the half duplex or full duplex mode.
		Supports unlink / downlink rate control based on the Ethernet port, with the granularity of 64 kbit/s.
		Supports the PAUSE flow control.
		Supports the loopback detection at the subscriber side.
		Supports learning up to 1024 MAC addresses.
		Supports enabling / disabling the MAC address learning function globally.
		Supports remote configuration of the MAC address aging time. The value ranges between 0s and 300s. The default value is 80s.
Multicast		Supports the IGMP Snooping protocol.

Item	Description
	Supports IGMP v1/v2/v3.
	Supports filtering and forwarding of multicast MAC addresses.
	Supports controllable multicast and uncontrollable multicast.
	Supports fast leave.
	Supports translation, transparent transmission and stripping of the multicast VLAN tags.
	Supports VLAN translation for the uplink multicast protocol messages.
	Supports filtering the downlink multicast messages.
	Supports bearing downlink multicast service flows and IGMP signaling messages via different GEM ports.
	Supports configuration of the multicast GEM ports.
	Supports authentication of the GEM ports.
	Supports no less than 256 multicast groups.
	Supports the IPoE/PPPoE mode for multicast services.
	Supports the IPv6 Snooping multicast service; supports the MLDv1 message, MLDv2 query message and MLDv2 report message.
VLAN	Supports the IEEE 802.1Q VLAN standard.
	Supports adding the 802.1Q VLAN ID in the tag / untag mode.
	Supports up to 4095 VLANs.
Wire-speed forwarding	Supports Layer 2 / Layer 3 wire-speed forwarding.
Layer 3 features	Supports the IPv4/v6 dual stack.
	Supports obtaining network parameters such as the user IP address, subnet mask and DNS in the DHCP mode. Supports reporting the physical location of the Ethernet interface based on DHCP Option82.
	Supports obtaining user IP addresses in the PPPoE mode, and supports the PPPoE+ function for precise identification of users.
	Supports static routing and default routing.
	Supports DDNS, NAT, port forwarding and DMZ.
	Supports ARP, UPnP, ALG, Portal and QoS.
Voice	Supports the protocols H.248 and SIP.
	Supports the speech encoding modes such as G.711, G.729, G.723.1 and G.722.
	Provides a phone number for each connected telephone set.
	Supports simultaneous call and conversation of two POTS subscribers.

Item	Description
	Supports static and dynamic jitter buffer.
	Supports DTMF detection.
	Supports RFC 2833 for transmitting / receiving DTMF.
	Supports RTP/RTCP (RFC 3550).
WLAN	Supports 802.11b, 802.11g, 802.11n, 802.11b/g and the hybrid mode for the 2.4 GHz frequency band; supports 802.11a, 802.11n, 802.11ac and the hybrid mode for the 5 GHz frequency band.
	Supports the MIMO program for the 2.4 GHz and 5 GHz frequency bands.
	Supports eight SSIDs (four for the 2.4 GHz band and another four for the 5 GHz band) to differentiate networks.
	Supports 13 working channels in the 2.4 GHz frequency band and 20 working channels in the 5 GHz frequency band.
	Supports automatic selection and manual configuration of channels.
	Supports Open, WPA2-PSK and WPA-PSK/WPA2-PSK authentication.
	Supports the WEP, AES and AES/TKIP encryption.
	Supports the WPS negotiation encryption algorithm and key.
	Supports adjustment of the transmit power, which is configured in form of percentage. Five options are provided: 20%, 40%, 60%, 80%, 100%. Other values are not supported.
USB	Conforms to the USB 2.0 standard.
	Supports plug-and-play and hot insertion of the USB storage device.
	Supports storage devices such as the USB HUB and mass storage.
	Supports providing the FTP service on the USB.
Security	Supports the firewall.
	Supports packet filtering.
	Supports filtering MAC addresses.
	Supports filtering URL addresses.
	Supports protection against illegal message (such as DoS and ARP) attacks; supports suppression of broadcast storms.
	Supports configuring the HTTPS safe channel.
	Supports configuring ACL rules for the ONT.
	Supports remote control.
Management and maintenance	Supports local service configuration, query and software upgrade based on the Web page.
	Supports management of OMCI configurations and queries.

Item	Description
	Supports query of the ONT optical module information.
	Supports Type B protection.
QoS	Provides powerful QoS functions; supports global configuration of queue priorities and flexible mapping of 802.1p values of packets.
	Supports the ACL function to match traffics based on the ACL rules.
	Supports three queue scheduling modes (PQ, WRR and PQ+WRR); supports configuring the weight of scheduled queues to guarantee the quality of high-QoS services such as voice and video in multi-service scenarios.

2.4.4 Technical Specifications

Classification	Item	Specification
Mechanical parameters	Dimensions	36 mm × 171 mm × 123 mm (H × W × D)
	Wall mounting hole distance	92 mm
	Weight	About 280 g
Power supply parameters	DC	DC 12 V/1.5 A
Power consumption parameter	Typical power consumption	9 W
	Maximum power consumption	16 W
Environment parameters	Working temperature	-5°C to 45°C
	Storage temperature	-20°C to 70°C
	Environmental humidity	10% to 95% (no condensation)

3 Web Configuration Guide

This chapter introduces the Web page for the HG6145D2 administrator, including the parameter meanings and operation methods.

Note:

Configure the ONT on the OLT via the access network management system. For details, please refer to the relevant OLT configuration guide.

3.1 Local Login to the Web Configuration GUI

This section introduces the local login to the ONT's web page and the layout of the configuration page.

Prerequisites

- The ONT has been connected to the computer correctly.
- The user computer is started normally.
- The ONT is started normally.

  Press down the ONT's power button. If the power indicator LED is illuminated, the ONT is powered on normally.

Planning Data

Before setting up the configuration environment, prepare the data as shown in Table 3-1.

Table 3-1 Planning Data for Local Login to the Web Page

Item	Description
Username and password	Factory default value: ◆ Administrator ▶ Username: admin ▶ Password: %0|F?H@f!berhO3e ◆ Common user ▶ Username: user ▶ Password: user1234 **Note: Some operators require customized username and password, so that the default username and password may be different from the ones mentioned above. In this case, please ask the local operator (if you are an administrator user) or refer to the User Guide attached to the device or the label at the bottom of the device (if you are a common user) for detailed information.** **Note: The password is case sensitive.**
Management IP address and subnet mask of the ONT	Factory default value: ◆ IP address: 192.168.1.1 ◆ Subnet mask: 255.255.255.0 **Note: Some operators require customized management IP address, so that the default management IP address may be different from the one mentioned above. In this case, please refer to the User Guide attached to the device or the label at the bottom of the device.**
IP address and subnet mask of the user computer	◆ Set this item to obtaining IP address automatically based on DHCP (recommended). ◆ Set this item to static IP address, which should be in the same network segment with the management IP address of the ONT. ▶ IP address: 192.168.1.X (X is a decimal integer between 2 and 253) ▶ Subnet mask: 255.255.255.0

Operation Procedure

1. Set the IP address and the subnet mask of the computer.
2. Enter **http://192.168.1.1** (default management IP address of the ONT) in the browser address bar of the computer, and press the Enter key to bring up the user login dialog box.

3. Enter the administrator username and password in the login dialog box. Access the Web page after the password is authenticated.

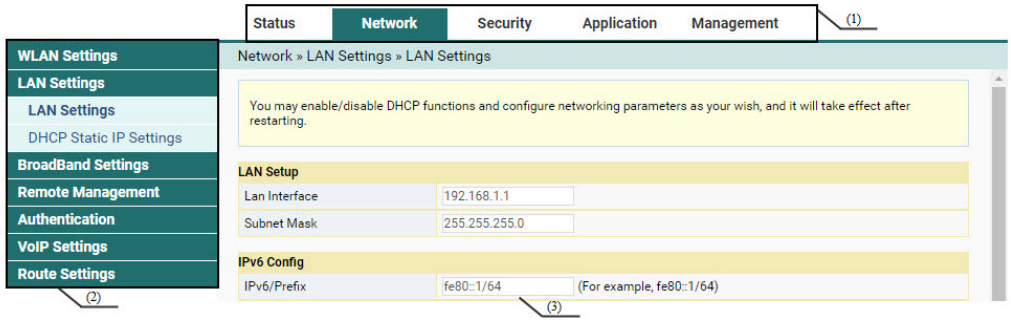
Caution:

The system will log out automatically if no user operation is detected in five minutes.

Layout of the Web Configuration Page

The web configuration page comprises three parts, as shown in Figure 3-1.

- Navigation bar. Click the link to access the corresponding configuration management page.
- Link bar. Click the link to access the sub-page for corresponding configuration management.
- Configuration management area. Displays the items selected in the navigation bar and link bar.



(1) Navigation bar (2) Link bar (3) Configuration management area

Figure 3-1 Web Configuration Page

Note:

The screenshots provided here are for reference only, and the actual web pages for the equipment shall prevail.

The configuration pages for the administrator are different from those for common users:

- The administrator can view and configure all the node items on the web page.
- The common users can view and configure only part of the node items. The following lists the key nodes available for common users. For details of the configuration items, please refer to the practical pages.
  - The **Status** tab.
  - **WLAN Settings** in the **Network** tab.
  - **User Account** and **Device Reboot** in the **Management** tab.

3.2 Status

This section introduces how to view basic information about the ONT, including the device information, wireless network status, WAN side status, LAN side status, optical power status and voice status, etc.

3.2.1 Device Information

Select **Status** in the navigation bar, and then select **Device Information→Device Information** in the left link bar to view the information such as the software version, hardware version, device model and device description, as shown in Figure 3-2.

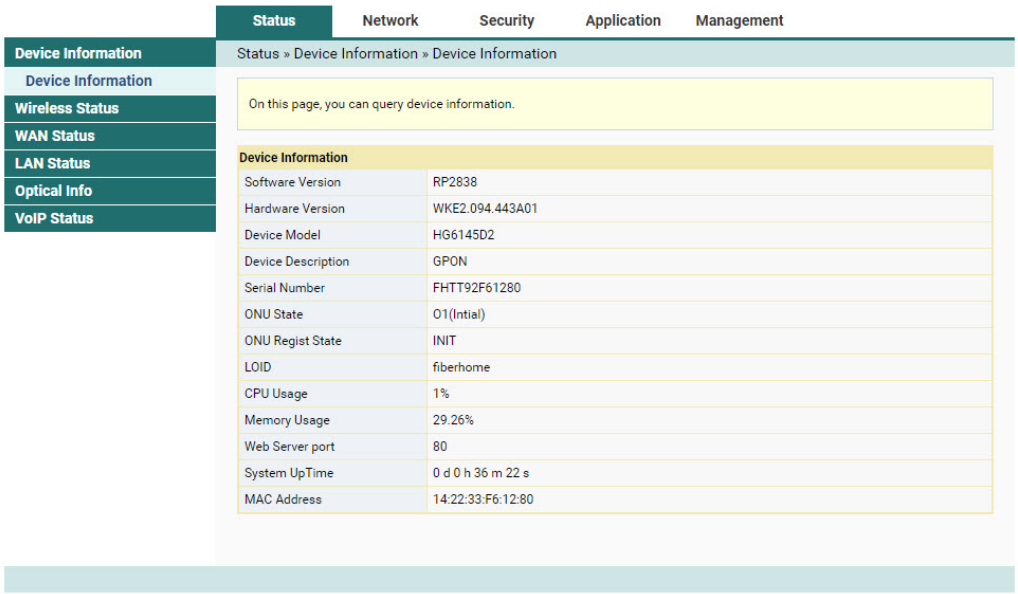


Figure 3-2 Device Information

3.2.2 Wireless Network Status

View the information about the wireless network, such as network mode, frequency channel, SSID, count of wireless packets, and list of Wi-Fi clients.

3.2.2.1 Wireless Network Status

Select **Status** in the navigation bar, and then select **Wireless Status→Wireless Status** in the left link bar to view the information of the wireless network, such as network mode, band, SSID and wireless packet statistics, as shown in Figure 3-3.

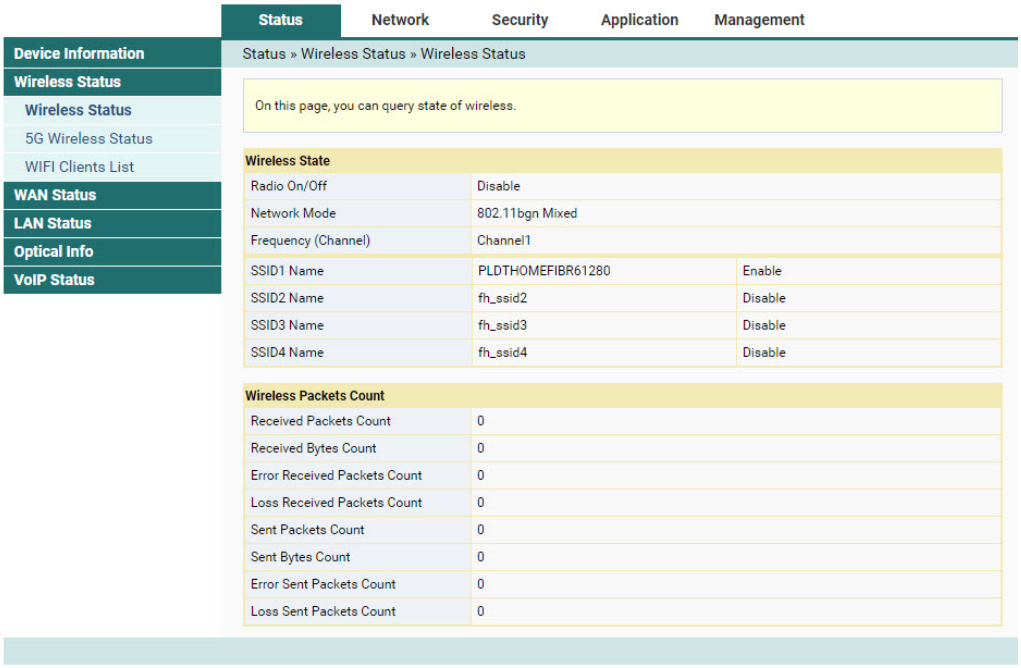


Figure 3-3 Wireless Network Status

3.2.2.2 Status of the 5G Wireless Network

Select **Status** in the navigation bar, and then select **Wireless Status→5G Wireless Status** in the left link bar to view the information of the 5G wireless network, such as network mode, band, SSID and wireless packet statistics, as shown in Figure 3-4.

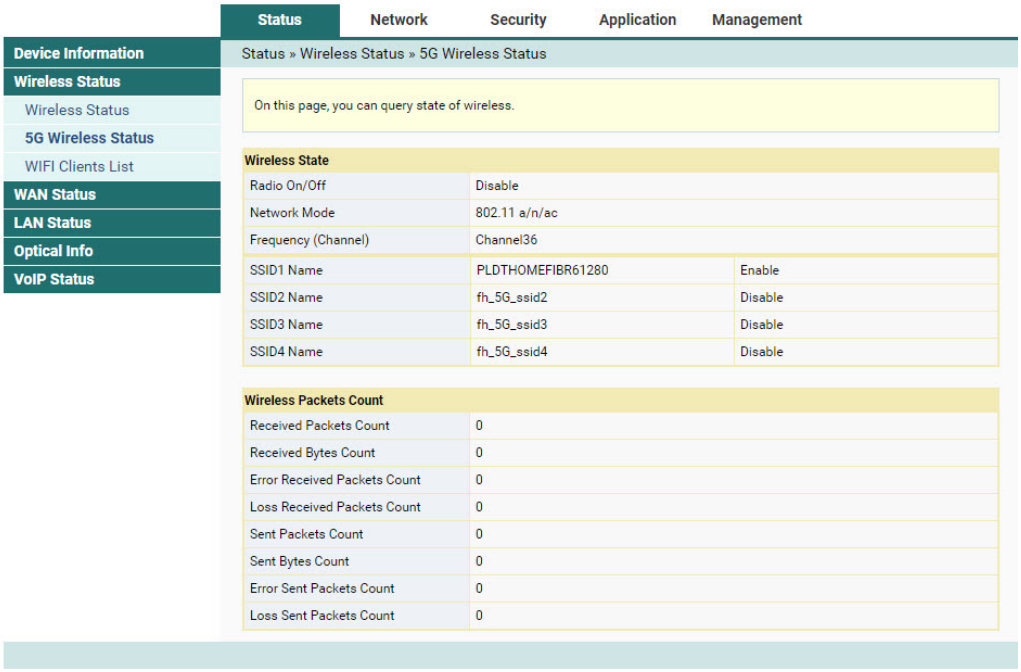


Figure 3-4 Status of the 5G Wireless Network

3.2.2.3 Wi-Fi User List

Select **Status** in the navigation bar, and then select **Wireless Status→WIFI Clients List** in the left link bar to view the list of client ends connected to the ONT wireless network, as shown in Figure 3-5.

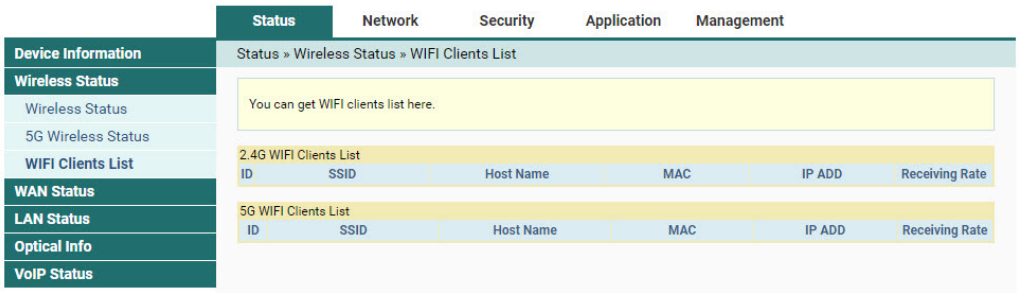


Figure 3-5 WIFI User List

3.2.3 WAN Side Status

Select **Status** in the navigation bar, and then select **WAN Status→WAN Status** in the left link bar to view the information such as the status, IP obtaining mode, IP address and subnet mask of the WAN interface, as shown in Figure 3-6.

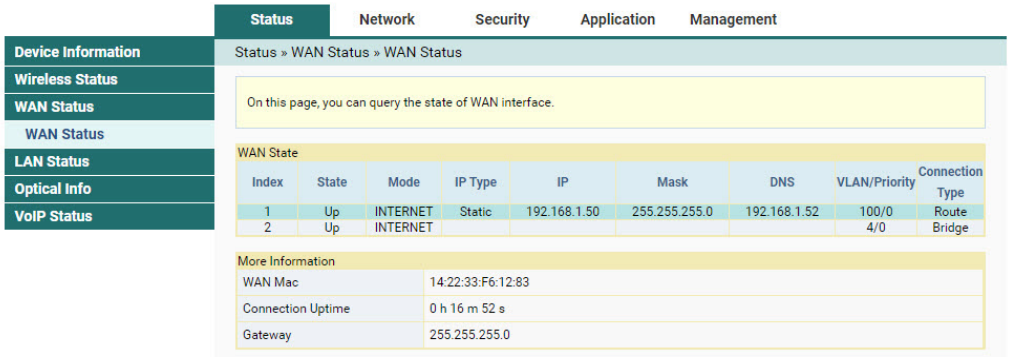


Figure 3-6 WAN Side Status

3.2.4 LAN Side Status

Check the state information about the LAN interface, Ethernet Ports and the DHCP client end.

3.2.4.1 LAN Side Status

Select **Status** in the navigation bar and select **LAN Status→LAN Status** in the left link bar to view the information such as the IP address and subnet mask of the LAN side, as shown in Figure 3-7.

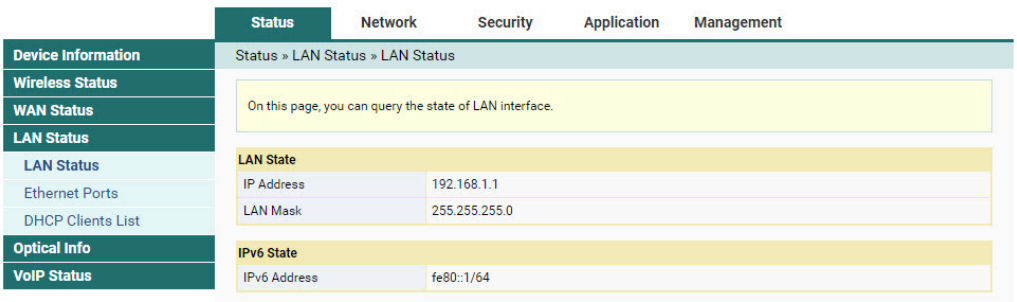


Figure 3-7 LAN Side Status

3.2.4.2 Ethernet Ports

Select **Status** in the navigation bar and select **LAN Status→Ethernet Ports** in the left link bar to view the information such as the LAN port, LAN mode, LAN speed, LAN state, transmit bytes, etc. See Figure 3-8.

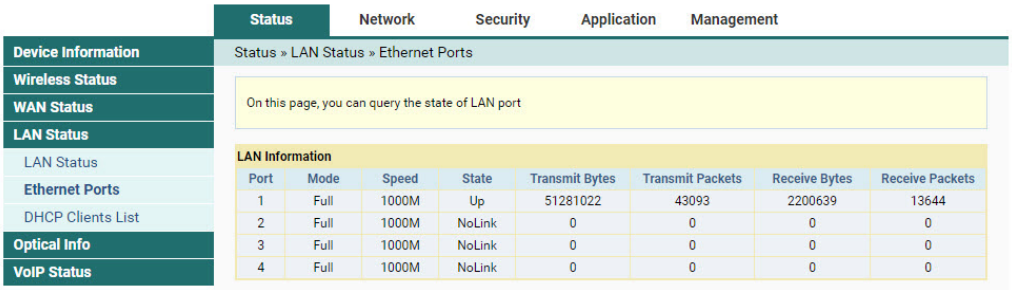


Figure 3-8 Ethernet Ports

3.2.4.3 DHCP User List

Select **Status** in the navigation bar and select **LAN Status→DHCP Clients List** in the left link bar to view the information about the DHCP client end such as the IP address, MAC address and leased time, as shown in Figure 3-9.

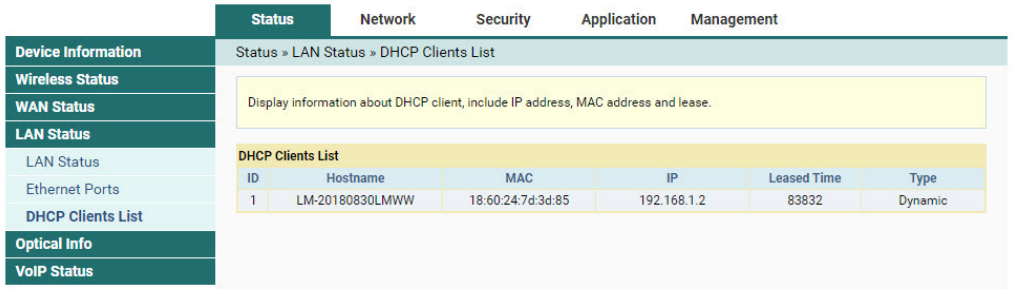


Figure 3-9 DHCP User List

3.2.5 Optical Power Status

Select **Status** in the navigation bar and select **Optical Info→Optical Info** in the left link bar to view the optical module information such as the Tx optical power, Rx optical power and operating temperature, as shown in Figure 3-10.

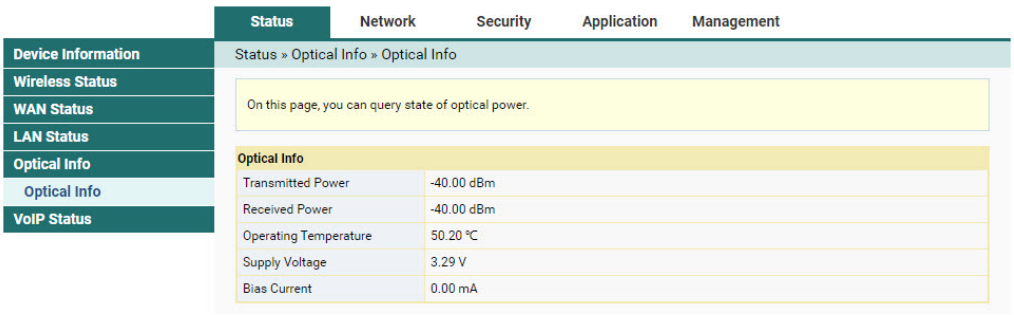


Figure 3-10 Optical Power Status

3.2.6 Voice Status

Select **Status** in the navigation bar and select **VoIP Status→VoIP Status** in the left link bar to view the information such as the port status and telephone number, as shown in Figure 3-11.

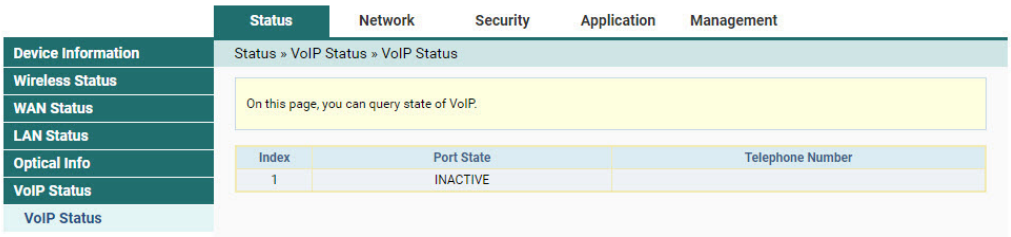


Figure 3-11 Voice Status

3.3 Network

This section introduces how to make the WLAN, LAN, broadband, remote management, authentication, voice and route configurations on the web page.

3.3.1 WLAN Settings

This section introduces how to configure Wi-Fi control and WPS as well as basic and advanced parameters of the wireless network on the Web page.

3.3.1.1 Band Steering

Configure the parameters relevant to the band steering. Setting up the wireless security and encryption can prevent any unauthorized access and monitoring.

1. Select **Network** in the navigation bar and select **WLAN Settings→BandSteering** in the left link bar to open the band steering page, as shown in Figure 3-12.

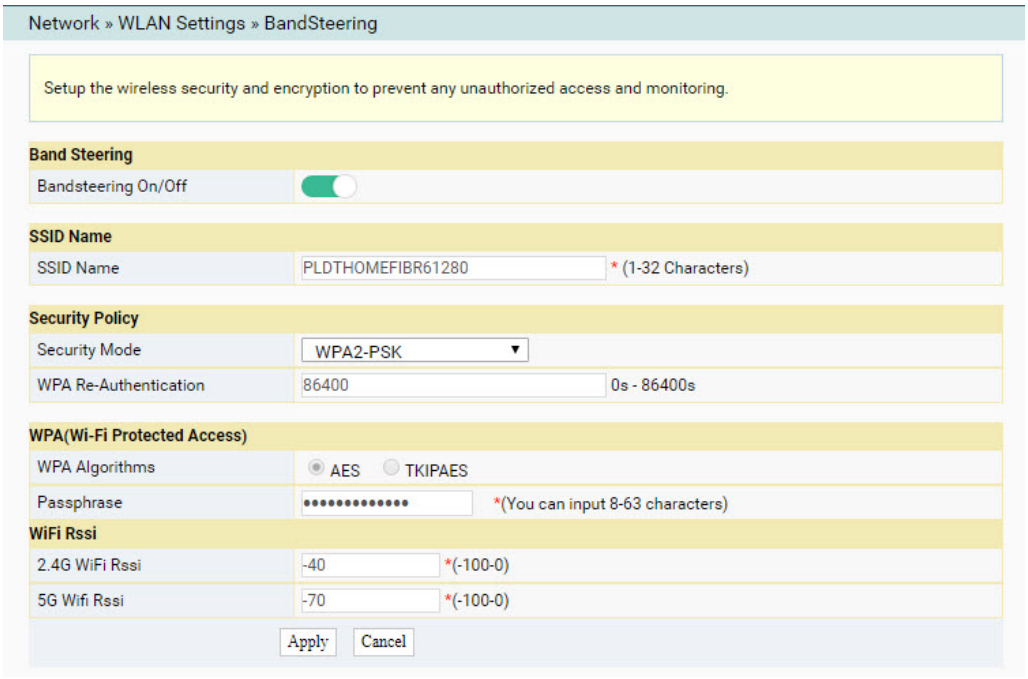


Figure 3-12 Band Steering

2. Configure the parameters as required. See Table 3-2 for the parameter description.
3. Click **Apply** to save and apply the configuration.

Table 3-2 Parameters for Band Steering Configuration

Item	Description
Bandsteering On/Off	Enables or disables the WLAN service. ◆ Radio On: the wireless network is enabled. ◆ Radio Off: the wireless network is disabled.
SSID Name	The wireless network name, used to identify different wireless networks.

Table 3-2 Parameters for Band Steering Configuration (Continued)

Item	Description	
Security Mode	The authentication mode of the wireless terminal requesting to access the wireless network. The options include OpenSystem, WPA2-PSK and WPA-PSK/WPA2-PSK. ◆ OpenSystem: Unencrypted. Any terminal can access to the wireless network, so that the security cannot be guaranteed. This mode is not advisable. ◆ WPA2-PSK: WPA2 is the second edition of WPA. ◆ WPA-PSK/WPA2-PSK: the authentication mode combining WPA and WPA2.	
WPA Re-Authentication	Set the WPA re-authentication times. The value ranges from 0 to 86400 (s).	This item should be set if the authentication mode is WPA-PSK/WPA2-PSK or WPA2-PSK.
WPA Algorithms	The encryption algorithms include AES and TKIPAES.	
Passphrase	Enter the SSID key.	
Encrypt Type	Option: None. This item is available only when **Security Mode** is set to **OpenSystem**.	
2.4G WiFi Rssi	Set the 2.4G WiFi Rssi. The value ranges from -100 to 0. The default setting is -40.	
5G WiFi Rssi	Set the 5G WiFi Rssi. The value ranges from -100 to 0. The default setting is -70.	

3.3.1.2 2.4G Basic Parameters

Configure the parameters of the 2.4G wireless network such as the switch, network mode, domain, frequency bandwidth and frequency channel.

1. Select **Network** in the navigation bar and select **WLAN Settings→2.4G Basic** in the left link bar to open the basic setting page for the 2.4G wireless access service, as shown in Figure 3-13.

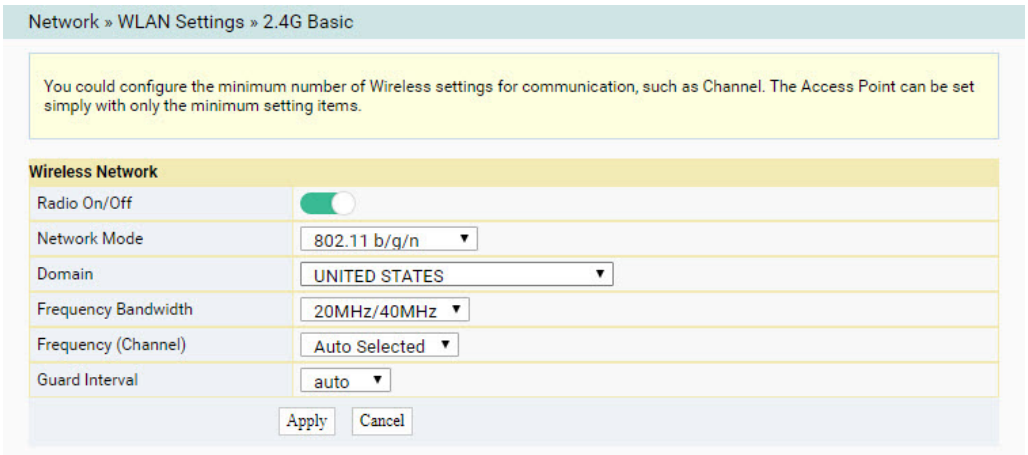


Figure 3-13 Basic Parameters of the Wireless Network

2. Configure the basic parameters of the 2.4G wireless network. For details of the parameters, see Table 3-3.

3. Click **Apply** to save and apply the configuration.

Table 3-3 Basic Parameters of the 2.4G Wireless Network

Item	Description
Radio ON/OFF	Enables or disables the WLAN service. ◆ RADIO ON: the wireless network is enabled. ◆ RADIO OFF: the wireless network is disabled.
Network Mode	The mode supported by the wireless network. The options include 802.11b, 802.11g, 802.11b/g, 802.11n and 802.11b/g/n. The default setting is 802.11b/g/n.
Domain	Select your region.
Frequency Bandwidth	The width of wireless band. The options include 20MHz/40MHz, 20MHz and 40MHz.
Frequency (Channel)	The channel used for communication between the wireless access point and the wireless station. The options includes **Auto Selectd** and **Channel1** to **Channel11**. The default setting is **Auto Selectd**.
Guard Interval	The wireless protection interval. The options include **0.4us**, **0.8us** and **auto**. The default setting is **auto**.

3.3.1.3 2.4G Advanced Configuration

Configure the parameters of the 2.4G wireless network, such as the SSID, password, security mode and algorithm.

1. Select **Network** in the navigation bar, and then select **WLAN Settings→2.4G Advanced** in the left link bar to open the advanced setting page for the 2.4G wireless access service, as shown in Figure 3-14.

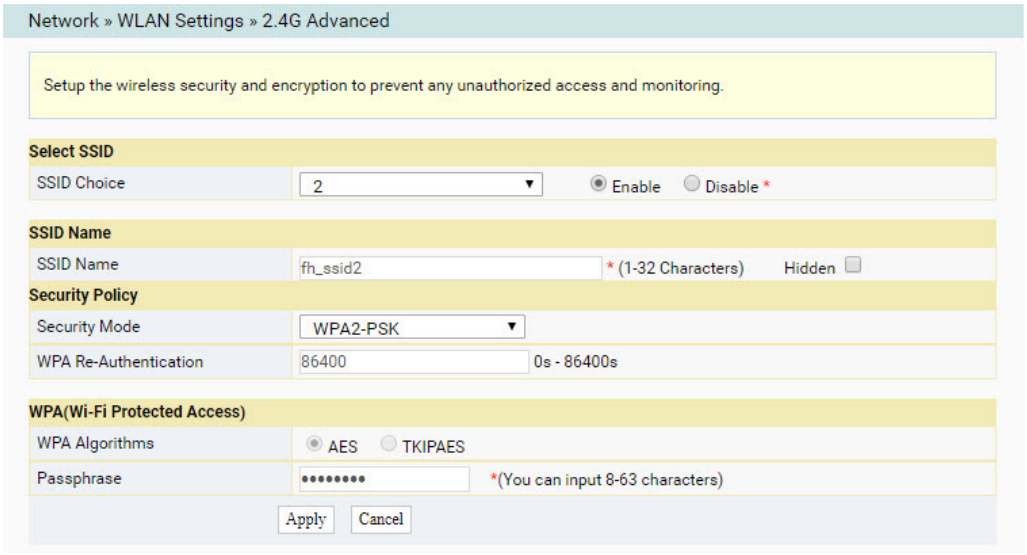


Figure 3-14 Advanced Settings of the Wireless Network

2. Configure the parameters of the 2.4G wireless network, such as the SSID, password, security mode and algorithm. For details of the parameters, see Table 3-4.

3. Click **Apply** to save and apply the configuration.

Table 3-4 Advanced Setting Parameters of Wireless Network

Item	Description
SSID Choice	Select the SSID. The value range is 1 to 4.
Enable / Disable	Enables or disables the corresponding SSID.
SSID Name	The wireless network name, used to identify different wireless networks.
Hidden	Select whether to hide the SSID. When the SSID is hidden, the wireless terminal cannot detect the wireless signals unless the SSID is entered.
Security Mode	The authentication mode of the wireless terminal requesting to access the wireless network. The options include OpenSystem, WPA2-PSK and WPA-PSK/WPA2-PSK. ◆ OpenSystem: Unencrypted. Any terminal can access to the wireless network, so that the security cannot be guaranteed. This mode is not advisable. ◆ WPA2-PSK: WPA2 is the second edition of WPA. ◆ WPA-PSK/WPA2-PSK: the authentication mode combining WPA and WPA2.

Table 3-4 Advanced Setting Parameters of Wireless Network (Continued)

Item	Description	
WPA Re-Authentication	Set the WPA re-authentication times. The value ranges from 0 to 86400 (s).	This item should be configured if the authentication mode is WPA2-PSK or WPA-PSK/WPA2-PSK.
WPA Algorithms	The encryption algorithms include AES and TKIPAES.	
Passphrase	Enter the SSID key.	
Encrypt Type	Option: None. This item is available only when **Security Mode** is set to **OpenSystem**.	

Note:

Pressing the **Apply** button will validate a single **SSID choice** configuration item. If you do not click **Apply** after modifying the SSID 1 setting, the modification will not take effect.

If the SSID1 setting is modified, the factory default wireless network account will be invalid.

If you forget the customized wireless network account, restore the factory default account by pressing down the Reset button for more than 5 seconds.

3.3.1.4 2.4G Wi-Fi Control

Configure parameters of the 2.4G wireless network, such as Wi-Fi power and number of WIFI connections.

1. Select **Network** in the navigation bar, and then select **WLAN Settings→2.4G WIFI Control** in the left link bar to open the WIFI control setting page for the 2.4G wireless access service, as shown in Figure 3-15.

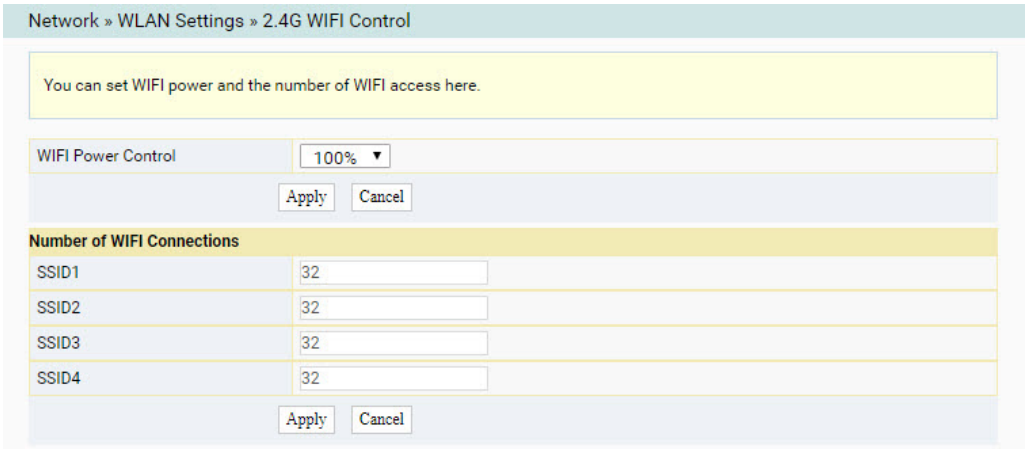


Figure 3-15 WIFI Control

2. Configure parameters of the 2.4G wireless network, such as WIFI power and number of WIFI connections. For details of the parameters, see Table 3-5.

3. Click **Apply** to save and apply the configuration.

Table 3-5 Parameters of WIFI Control

Item	Description
WIFI Power Control	The transmit power of the wireless signal. A larger value indicates a wider signal coverage.
Number of WIFI Connections	The maximum number of client ends supported by the SSIDs.

3.3.1.5 5G Basic Parameters

Configure the parameters of the 5G wireless network such as the switch, network mode, domain, frequency bandwidth and frequency channel.

1. Select **Network** in the navigation bar and select **WLAN Settings→5G Basic** in the left link bar to open the basic setting page for the 5G wireless access service, as shown in Figure 3-16.

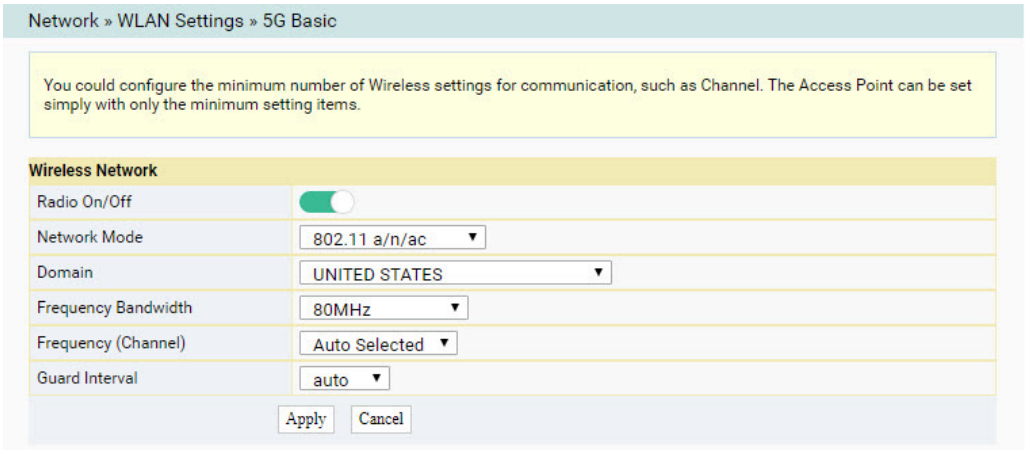


Figure 3-16 Basic Parameters of the 5G Wireless Network

2. Configure the basic parameters of the 5G wireless network. For details of the parameters, see Table 3-6.

3. Click **Apply** to save and apply the configuration.

Table 3-6 Basic Parameters of the 5G Wireless Network

Item	Description
Radio ON/OFF	Enables or disables the WLAN service. ◆ RADIO ON: the wireless network is enabled. ◆ RADIO OFF: the wireless network is disabled.
Network Mode	The mode supported by the wireless network. The options include 802.11a, 802.11a/n and 802.11a/n/ac. The default setting is 802.11a/n/ac.
Domain	Select your region.
Frequency Bandwidth	The width of wireless band. The options include 20MHz/40MHz, 20MHz, 40MHz and 80MHz. The default setting is 80MHz.
Frequency (Channel)	The channel used for communication between the wireless access point and the wireless station. The default setting is **Auto Selectd**.
Guard Interval	The wireless protection interval. The options include **0.4us**, **0.8us** and **auto**. The default setting is **auto**.

3.3.1.6 5G Advanced Configuration

Configure the parameters of the 5G wireless network, such as the SSID, password, security mode and algorithm.

1. Select **Network** in the navigation bar and select **WLAN Settings→5G Advanced** in the left link bar to open the advanced setting page for the 5G wireless access service, as shown in Figure 3-17.

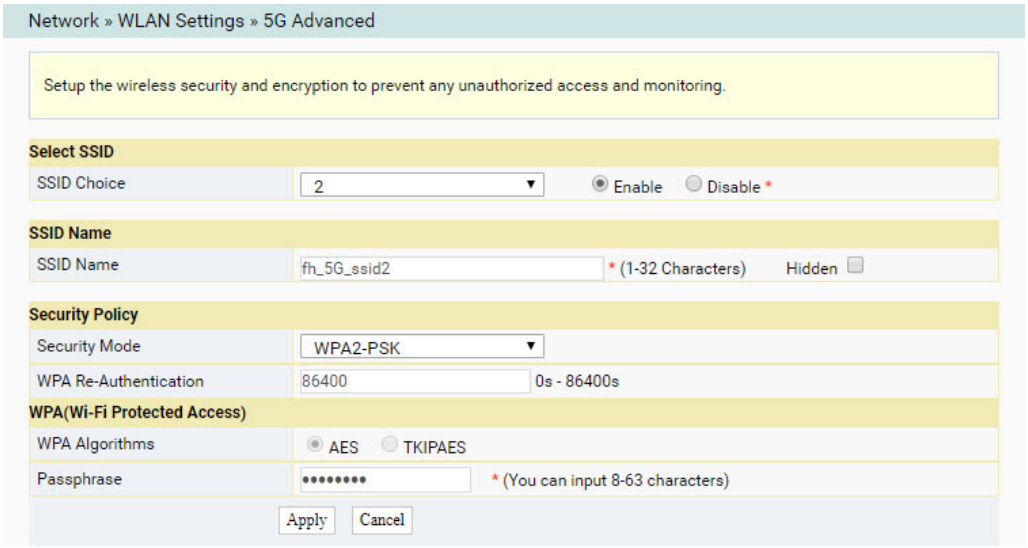


Figure 3-17 Advanced Settings of the 5G Wireless Network

2. Configure the parameters of the 5G wireless network, such as the SSID, password, security mode and algorithm. For details of the parameters, see Table 3-4.
3. Click **Apply** to save and apply the configuration.

Note:

Pressing the **Apply** button will validate a single **SSID choice** configuration item. If you do not click **Apply** after modifying the SSID 1 setting, the modification will not take effect.

If the SSID1 setting is modified, the factory default wireless network account will be invalid.

If you forget the customized wireless network account, restore the factory default account by pressing down the Reset button for more than 5 seconds.

3.3.1.7 5G Wi-Fi Control

Configure parameters of the 5G wireless network, such as Wi-Fi power and number of WIFI connections.

1. Select **Network** in the navigation bar and select **WLAN Settings→5G WIFI Control** in the left link bar to open the WIFI control setting page for the 5G wireless access service, as shown in Figure 3-18.

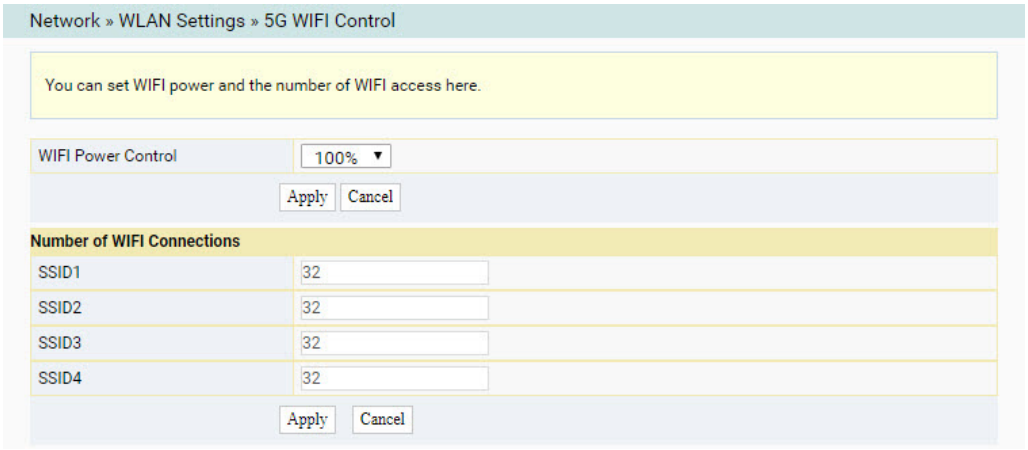


Figure 3-18 5G Wi-Fi Control

2. Configure the parameters of the 5G wireless network, such as WIFI power and quantity of connected client ends. For details of the parameters, see Table 3-5.
3. Click **Apply** to save and apply the configuration.

3.3.1.8 WPS Configuration

WPS can automatically set the wireless network name (SSID) and wireless encryption key for the HG6145D2 and client end supporting the Wi-Fi service. You need only to press down the WPS button or enter the PIN to achieve safe connection. Since you need not remember the long encryption key, you are free of the trouble caused by forgetting the password.

1. Select **Network** in the navigation bar and select **WLAN Settings→WPS** in the left link bar to open the WPS settings page, as shown in Figure 3-19.

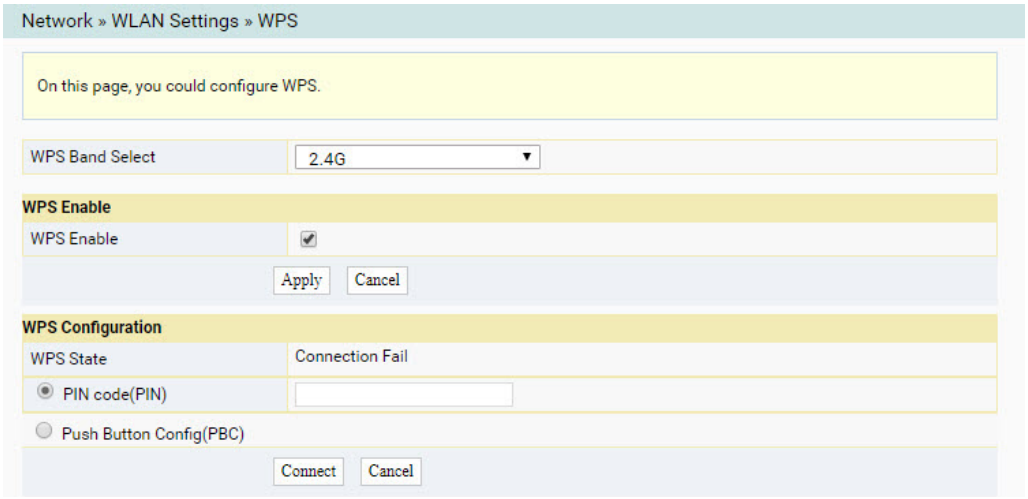


Figure 3-19 WPS Configuration

2. Select 2.4G/5G WPS Band.
3. Select whether to enable the WPS function. The options include **Enable** and **Disable**.
4. Select the WPS connection mode as required.
   - Select **PIN code(PIN)**, and enter the PIN code of the client end in the text box. Then click **Connect**.
   - Select **Push Button Config(PBC)** and click **Connect**.
5. Wait until the connection is completed.

3.3.2 LAN Settings

This section introduces how to configure the LAN settings and DHCP static IP settings in the Web page.

3.3.2.1 LAN Settings

Configure the management IP address and subnet mask at the LAN side.

1. Select **Network** in the navigation bar and select **LAN Settings→LAN Settings** in the left link bar to open the LAN settings page, as shown in Figure 3-20.

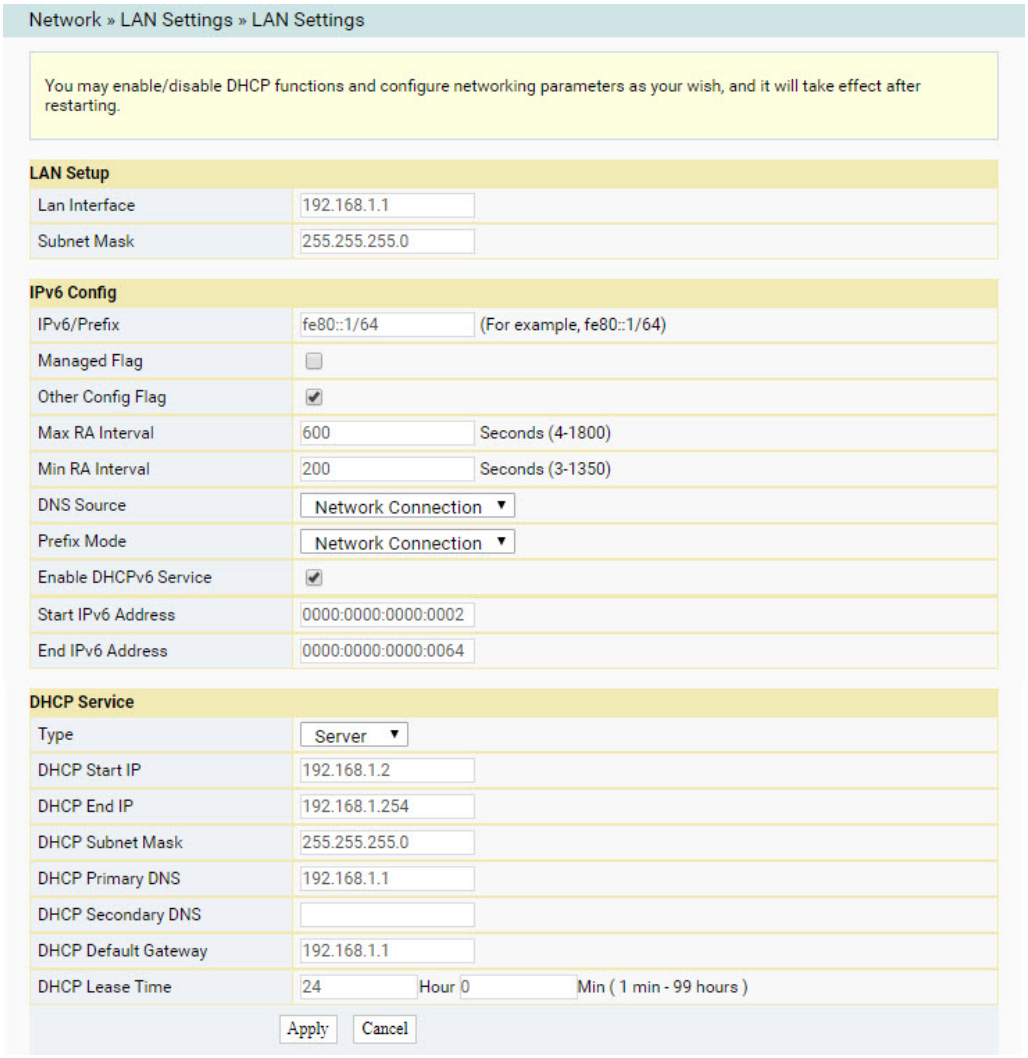


Figure 3-20 LAN Settings

2. Configure the management IP address and subnet mask at the LAN side. For details of the parameters, see Table 3-7.

3. Click **Apply** to save and apply the configuration.

Table 3-7 Parameters of LAN Settings

Item		Description
LAN Setup	Lan Interface	The management IP address at the LAN side of the ONT. The default value is 192.168.1.1.
	Subnet Mask	The subnet mask of the ONT for the LAN. The default value is 255. 255.255.0.

Table 3-7 Parameters of LAN Settings (Continued)

Item		Description	
IPv6 Config	IPv6/Prefix	The IPv6 gateway address, including a prefix of 64 bits. The default value is fe80::1/64.	
	Managed Flag	Select whether to distribute the IPv6 address based on DHCP. The default value is Disable.	
	Other Config Flag	Select whether to distribute the IPv6 DNS information based on DHCP. The default value is Enable.	
	Max RA interval	The maximum interval for announcing the gateway information. The default value is 600.	
	Min RA interval	The minimum interval for announcing the gateway information. The default value is 200.	
	DNS source	The source of the DNS distributed to PC, including **Network Connection**, **Static Setting** and **Proxy**. The default value is **Network Connection**.	
	Primary DNS Server	The IPv6 gateway address of the active DNS server.	**Note: This item should be configured if the DNS source is set to Static Setting.**
	Secondary DNS Server	The IPv6 gateway address of the standby DNS server.	
	Prefix mode	The source of the prefix information distributed to PC, including **Network Connection** and **Static Setting**. The default value is **Network Connection**.	
	Enable DHCPv6 Service	Sets whether to enable the DHCPv6 server.	
	Start IPv6 Address	The starting address ID of the address pool for distribution of DHCPv6 IP addresses.	
	End IPv6 Address	The ending address ID of the address pool for distribution of DHCPv6 IP addresses.	
DHCP Service	Type	Enables or disables the DHCP server. ◆ Server: Enables the DHCP server. The ONT can dynamically distribute IP addresses to user terminals. ◆ Disable: The user terminals connected to the ONT cannot obtain the private network IP address using the DHCP.	
	DHCP Start IP	The starting IP address of the IP address pool for the active DHCP server.	**Note: The IP address set here should be in the same network segment with the IP address set in LAN Setup; otherwise, the DHCP server will not operate normally.**
	DHCP End IP	The ending IP address of the IP address pool for the DHCP server.	

Table 3-7 Parameters of LAN Settings (Continued)

Item		Description
	DHCP Subnet Mask	The mask of the active DHCP server.
	DHCP Primary DNS	The IP address of the active DNS server.
	DHCP Secondary DNS	The IP address of the standby DNS server.
	DHCP Default Gateway	The default gateway of the active DHCP server.
	DHCP Lease Time	The lease time of the IP address pool of the DHCP server.

3.3.2.2 DHCP Static IP Settings

Configure the MAC address and IP address at the DHCP side.

1. Select **Network** in the navigation bar and select **LAN Settings→DHCP Static IP Settings** in the left link bar. Click **Add** to open the DHCP static IP settings page, as shown in Figure 3-21.

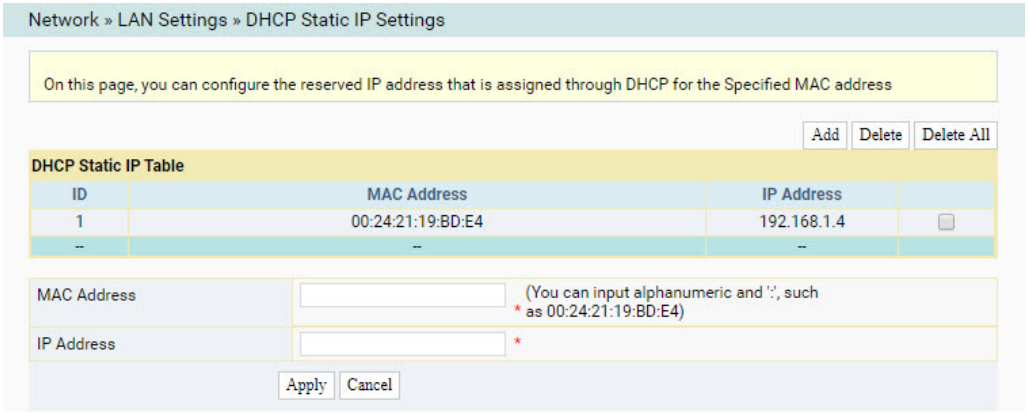


Figure 3-21 DHCP Static IP Settings

2. Configure the MAC address and IP address at the DHCP side. See Table 3-8 for the parameter description.
3. Click **Apply** to save and apply the configuration.

Table 3-8 Parameters of DHCP Static IP Settings

Item	Description
MAC Address	The MAC address of the user device subject to the DHCP filtering rule.
IP Address	The IP address for the DHCP server.

3.3.3 Broadband Settings

This section introduces how to configure the Internet settings and IPTV settings in the Web page.

3.3.3.1 Broadband Settings

Select the WAN connection suitable for the network environment, or configure the parameters concerned for the selected WAN connection.

1. Select **Network** in the navigation bar and select **BroadBand Settings→Internet Settings** in the left link bar to open the Internet settings page, as shown in Figure 3-22.

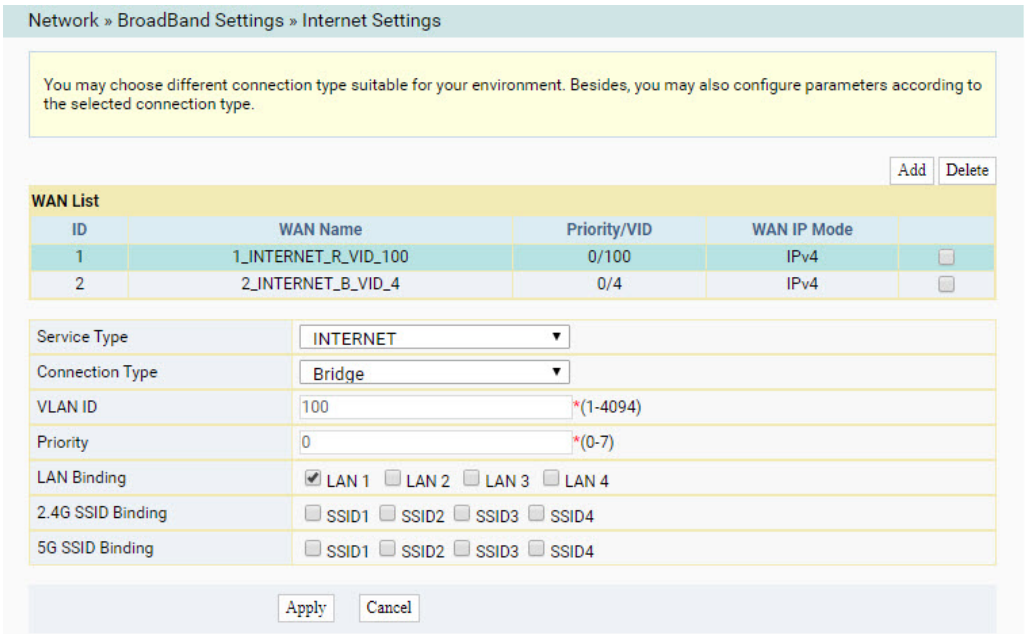


Figure 3-22 Internet Settings

2. Configure parameters relevant to the Internet at the WAN side. For details of the parameters, see Table 3-9.

3. Click **Apply** to save and apply the configuration.

Table 3-9 Parameters for Internet Settings

Item	Description	
Service Type	Select the WAN port service type. ◆ TR069: This connection is only applicable for TR069 service. ◆ VOIP: This connection is only applicable for voice service. ◆ TR069_VOIP: This connection is applicable for both TR069 and voice services. ◆ INTERNET: This connection is only applicable for Internet access service. ◆ TR069_INTERNET: This connection is applicable for both TR069 and Internet access services. ◆ VOIP_INTERNET: This connection is applicable for voice and Internet access services. ◆ TR069_VOIP_INTERNET: This connection is applicable for TR069, voice and Internet access services. ◆ MUTICAST: This connection is only applicable for multicast service. ◆ IPTV: This connection is only applicable for IPTV service. ◆ OTHER: other connections.	
Connection Type	Select the connection type of the WAN port. ◆ Bridge: the Layer 2 bridge connection mode. This connection mode can be used when the service type is set to **INTERNET**, **MULTICAST** or **OTHER**. ◆ Route: the Layer 3 router connection mode. This connection mode can be used in all service type.	
Packaging Type	The options include **IPoE** and **PPPoE**.	This item should be set if the connection type is **Route**.
VLAN ID	Sets the VLAN ID of the WAN connection. The value range is 1 to 4094. The VLAN ID value here should be consistent with that on the user side of the OLT.	
Priority	Sets the priority of the VLAN. The value range is 0 to 7.	
NAT	Enables or disables the NAT function.	Users need to configure this item when the service type is set to **INTERNET**, **TR069_INTERNET**, **VOIP_INTERNET**, or **TR069_VOIP_INTERNET** and the connection type is set to **Route**.
MTU	Enter the maximum transmission unit. It is advised to use the default value.	
LAN Binding	Select the LAN port to be bound with the WAN port.	
2.4G SSID Binding	Select the wireless 2.4G SSID to be bound with the WAN port.	

Table 3-9 Parameters for Internet Settings (Continued)

Item	Description	
5G SSID Binding	Select the wireless 5G SSID to be bound with the WAN port.	
IP Mode	The options include IPv4&IPv6, IPv4 and IPv6.	Users need to configure this item when the service type is set to **INTERNET**, **TR069_INTERNET**, **VOIP_INTERNET**, or **TR069_VOIP_INTERNET** and the connection type is set to **Route**.
WAN IP Mode	Sets the IP address obtaining mode at the WAN side of the ONT. The options include **DHCP**, **Static** and **PPPoE**. ◆ DHCP: Obtaining the IP address dynamically. ◆ Static: Setting the IP address in a static mode. ◆ PPPoE: PPPoE dialing mode.	This item should be set if the connection type is **Route**.
User Name	Enter the username provided by the ISP.	This item should be set if the WAN IP Mode is set to **PPPoE**.
Password	Enter the password provided by the ISP.	
Connection Trigger	Sets the PPPoE connection mode. The options include **AlwaysOn**, **OnDemand** and **Manual**.	
IP Address	Enter the static IP address at the WAN side provided by the ISP.	This item should be set when the IP Mode is set to **IPv4&IPv6** or **IPv4** and the WAN IP Mode is set to **Static**.
Subnet Mask	Enter the subnet mask provided by the ISP.	
Default Gateway	Enter the default gateway provided by the ISP.	
Primary DNS Server	Enter the IP address of the active DNS server provided by the ISP.	
Secondary DNS Server	Enter the IP address of the standby DNS server provided by the ISP.	
IPv6 Address	Enter the static IPv6 address at the WAN side provided by the ISP.	This item should be set when the IP Mode is set to **IPv4&IPv6** or **IPv6** and the **WAN IP Mode** is set to **Static**.
Default IPv6 Gateway	Enter the default gateway provided by the ISP.	
Primary DNS Server	Enter the IP address of the active DNS server provided by the ISP.	
Secondary DNS Server	Enter the IP address of the standby DNS server provided by the ISP.	
IPv6 Prefix	The destination IP address prefix to be accessed by the host.	

Table 3-9 Parameters for Internet Settings (Continued)

Item	Description	
Prefix Obtainment	Sets whether to enable the prefix obtainment function.	This item should be set when the IP Mode is set to **IPv4&IPv6** or **IPv6**.
Address Obtainment Method	Select the IPv6 address obtaining method.	
IPv6 Prefix Mode	Select the IPv6 prefix obtaining mode.	
Vendor ID	Sets the vendor ID.	This item should be set when the IP Mode is set to **IPv4&IPv6** or **IPv6** and the **WAN IP Mode** is set to **DHCP**.
Enable DS-lite	Enables or disables DS-lite.	This item should be set when the IP Mode is set to **IPv6**.

3.3.3.2 IPTV Settings

Configure the parameter **Multicast VLAN** for IPTV services.

1. Select **Network** in the navigation bar and select **BroadBand Settings→IPTV Settings** in the left link bar to open the IPTV settings page, as shown in Figure 3-23.

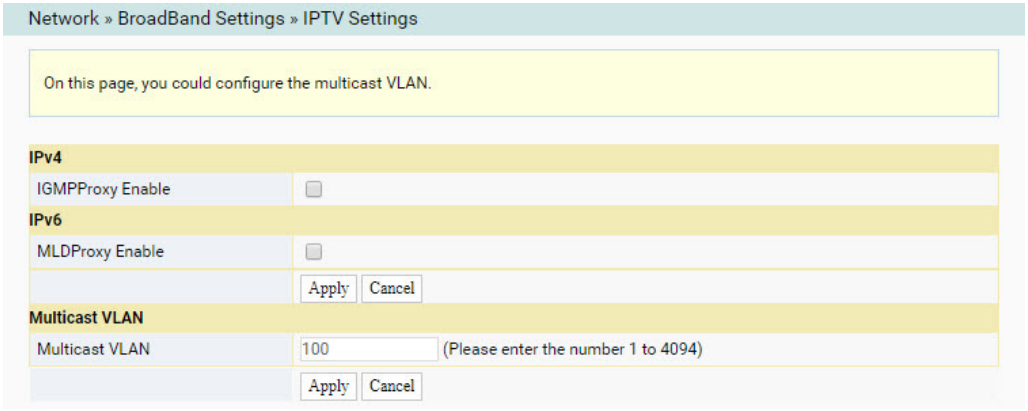


Figure 3-23 IPTV Settings

2. Select or clear the check boxes for **IGMPProxy Enable** and **MLDProxy Enable** as required.
3. Configure the **Multicast VLAN** parameter as required.

4. Click **Apply** to save and apply the configuration.

3.3.4 Remote Management

Configure the parameters relevant to the ACS server.

1. Select **Network** in the navigation bar and select **Remote Management→ACS Server** in the left link bar to open the ACS server page, as shown in Figure 3-24.

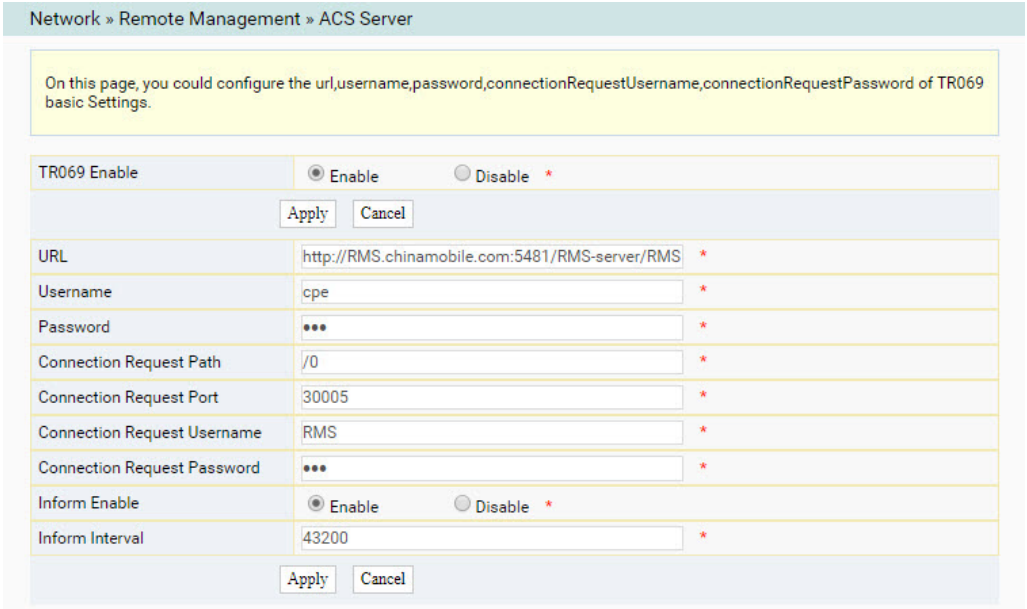


Figure 3-24 ACS Server

2. Configure the parameters as required. Table 3-10 describes the parameters.
3. Click **Apply** to save and apply the configuration.

Table 3-10 Parameters for ACS Server

Item	Description
TR069 Enable	Enables or disables the TR069 server. After setting, click **Apply** below so that the setting can take effect.
URL	Enter the URL provided by ISP.
Username	Enter the username provided by ISP.
Password	Enter the password provided by ISP.
Connection Request Path	Enter the requested connection path.
Connection Request Port	Enter the requested connection port.
Connection Request Username	Enter the requested connection username.

Table 3-10 Parameters for ACS Server (Continued)

Item	Description
Connection Request Password	Enter the requested connection password.
Inform Enable	Enables or disables the inform function. When enabled, the device periodically communicates with the ACS server, automatic reporting inform information.
Inform Interval	Set the inform interval, the default value is 43200.

3.3.5 Authentication Settings

Configure the parameters relevant to the ONT authentication mode, so that the ONT can pass the OLT authentication.

1. Select **Network** in the navigation bar and select **Authentication→OLT Authentication** in the left link bar to open the OLT authentication configuration page, as shown in Figure 3-25.

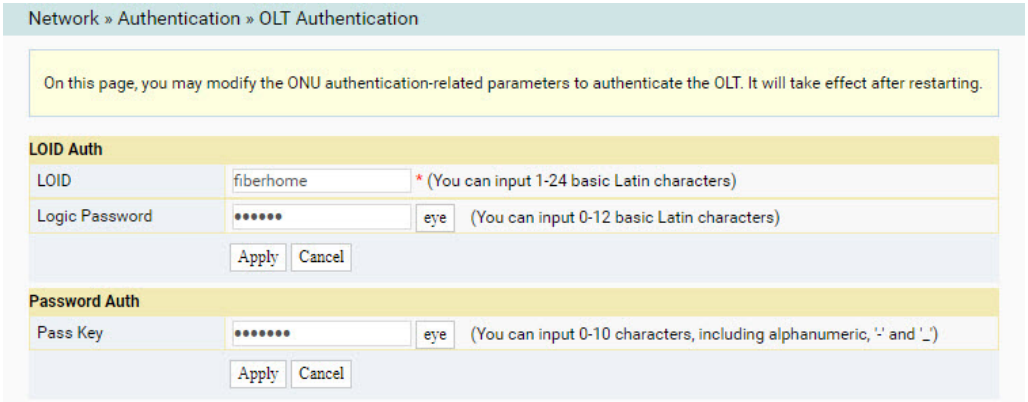


Figure 3-25 OLT Authentication

2. Configure the parameters as required. For details of the parameters, see Table 3-11.
3. Click **Apply** to save the configuration information. The configuration will take effect after the ONT is rebooted.

Table 3-11 Parameters for OLT Authentication

Item	Description	
LOID	Sets the LOID user name.	This item is configurable when the ONT uses the LOID authentication mode.
Logic Password	Sets the LOID password.	
Password Auth	Sets the authentication password when the ONT is authenticated by password.	

3.3.6 Voice Configuration

This section introduces how to configure the key parameters, basic parameters, advanced settings, digitmap and time length, and coding mode for voice services in the Web page.

3.3.6.1 Key Parameters

Configure the parameters such as VoIP protocol type and VoIP port.

1. Select **Network** in the navigation bar and select **VoIP Settings→Key Parameters** from the link bar on the left side to open the VoIP key parameter page, as shown in Figure 3-26.

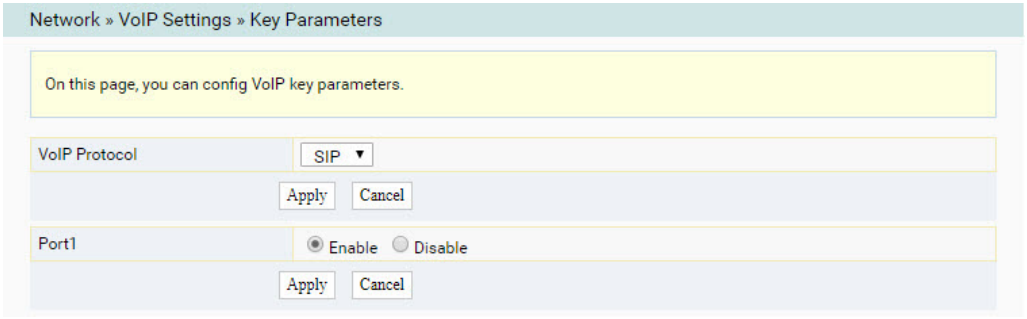


Figure 3-26 Key Parameters for Voice Configuration

2. Configure the key VoIP parameters as required. For details of the parameters, see Table 3-12.
3. Click **Apply** to save and apply the configuration.

Table 3-12 Key Parameters for Voice Service

Item	Description
VoIP Protocol	The voice protocol type. The default setting is SIP.
Port1	Enable or disable the VoIP port.

3.3.6.2 Basic Parameters

Configure basic voice parameters.

1. Select **Network** in the navigation bar and select **VoIP Settings→Basic** from the link bar on the left side to open the VoIP basic parameter configuration page, as shown in Figure 3-27.

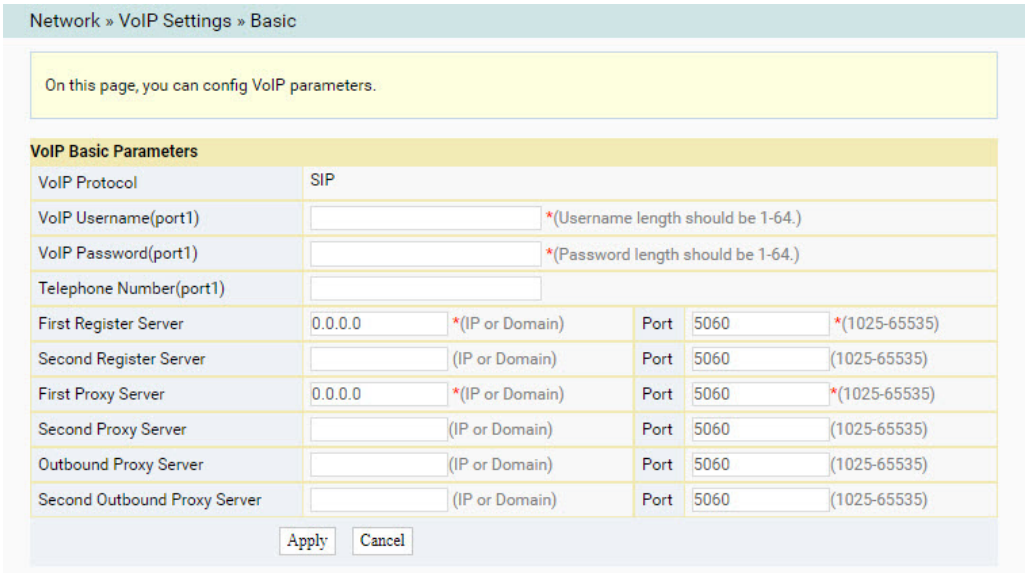


Figure 3-27 Basic Parameters for Voice Configuration

2. Configure the basic VoIP parameters as required. For details of the parameters, see Table 3-13.

3. Click **Apply** to save and apply the configuration.

Table 3-13 Basic Parameters for Voice Service

Item	Description
VoIP Protocol	The VoIP protocol type, configured in **Key Parameters**.
VoIP Username	The VoIP username.
VoIP Password	The VoIP password.
Telephone Number	The telephone number for the voice port.
First Register Server	The IP address or domain name of the active register server. The port number range is 1025 to 65535, and the default setting is 5060.
Second Register Server	The IP address or domain name of the standby register server. The port number range is 1025 to 65535, and the default setting is 5060.
First Proxy Server	The IP address or domain name of the active proxy server. The port number range is 1025 to 65535, and the default setting is 5060.

Table 3-13 Basic Parameters for Voice Service (Continued)

Item	Description
Second Proxy Server	The IP address or domain name of the standby proxy server. The port number range is 1025 to 65535, and the default setting is 5060.
Outbound Proxy Server	The IP address or the domain name of the outbound proxy server. The value ranges from 1025 to 65535. The default value is 5060.
Second Outbound Proxy Server	The IP address or the domain name of the standby outbound proxy server. The value ranges from 1025 to 65535. The default value is 5060.

3.3.6.3 Advanced Configuration

Configure advanced VoIP parameters.

1. Select **Network** in the navigation bar and select **VoIP Settings→Advanced** in the left link bar to open the advanced VoIP setting page, as shown in Figure 3-28.

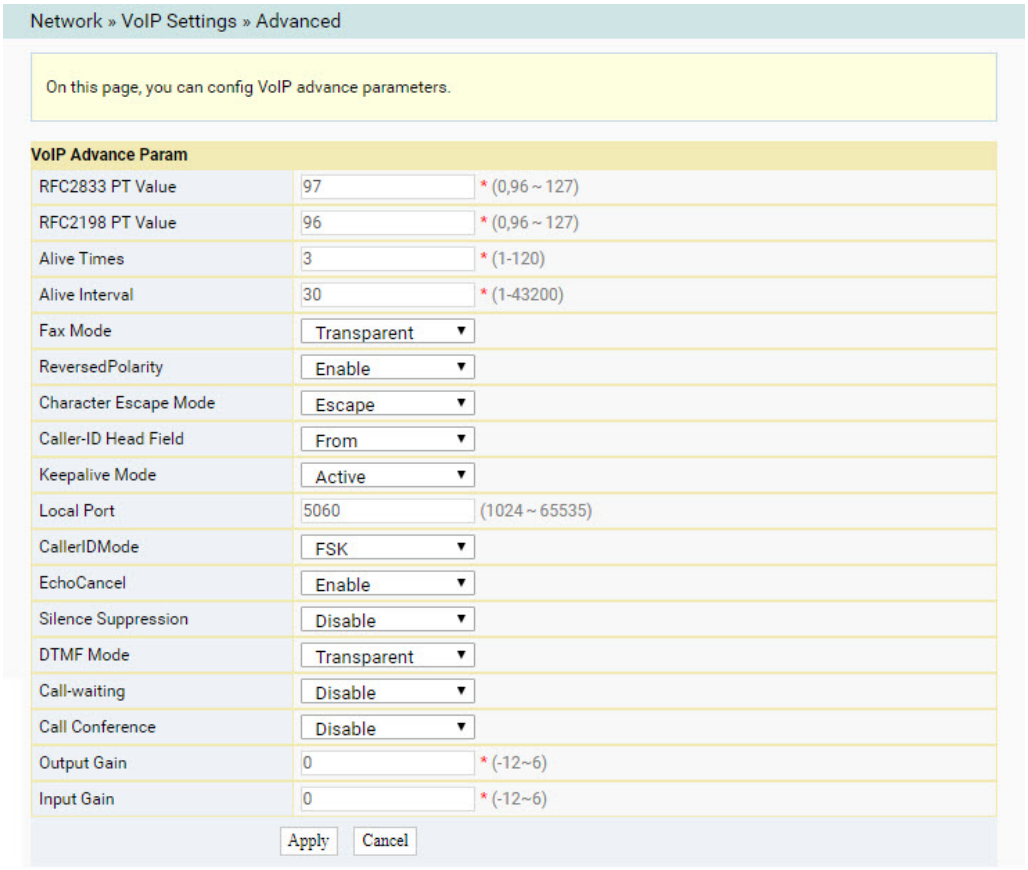


Figure 3-28 Advanced Voice Configuration

2. Configure the advanced VoIP parameters as required. For details of the parameters, see Table 3-14.

3. Click **Apply** to save and apply the configuration.

Table 3-14 Advanced Parameters for Voice Service

Item	Description
RFC2833 PT Value	Default PT value in RFC2833. The values include 0 and 96 to 127.
RFC2198 PT Value	Default PT value in RFC2198. The values include 0 and 96 to 127.
Alive Times	Heartbeat timeout times. The value ranges from 1 to 120.
Alive Interval	Heartbeat time length. The value ranges from 1 to 43200.
Fax Mode	The fax mode. The options include **Transparent** and **T38**. The default setting is **Transparent**.
Reversed Polarity	Enable or disable the reversed polarity signal. The default value is **Enable**.
Character Escape Mode	The options include **Escape** and **Not Escape**. The default value is **Escape**.
Caller-ID Head Field	The Caller ID display mode. The options include **From** and **P-Asserted-id**. The default setting is **From**.
Keepalive Mode	Enable or Disable the heartbeat mode. The default setting is **Active**.
Local Port	The number of the local port. Value range: 1024 to 65535. The default setting is 5060.
Caller ID Mode	The options include **FSK**, **DTMF** and **Disable**. The default setting is **FSK**.
Echo Cancel	Enable or disable the echo suppression. The default value is **Enable**.
Silence Suppression	Enable or disable the silence suppression. The default setting is **Disable**.
DTMF Mode	The DTMF mode. The options include **Transparent** and **RFC2833**. The default setting is **Transparent**.
Call-waiting	Enable or disable the call-waiting function. The default setting is **Disable**.
Call Conference	Enable or disable the call conference. The default setting is **Disable**.
Output Gain	Output gain. The value ranges from -12 to 6.
Input gain	Input gain. The value ranges from -12 to 6.

3.3.6.4 Digitmap and Time Length

Configure the VoIP time length and digitmap parameters including digitmap matching mode, SIP registration cycle, short timer, long timer, starting timer and long call time, etc.

1. Select **Network** in the navigation bar and select **VoIP Settings→Dial and Timeout** from the link bar on the left side to open the dial and timeout configuration page, as shown in Figure 3-29.

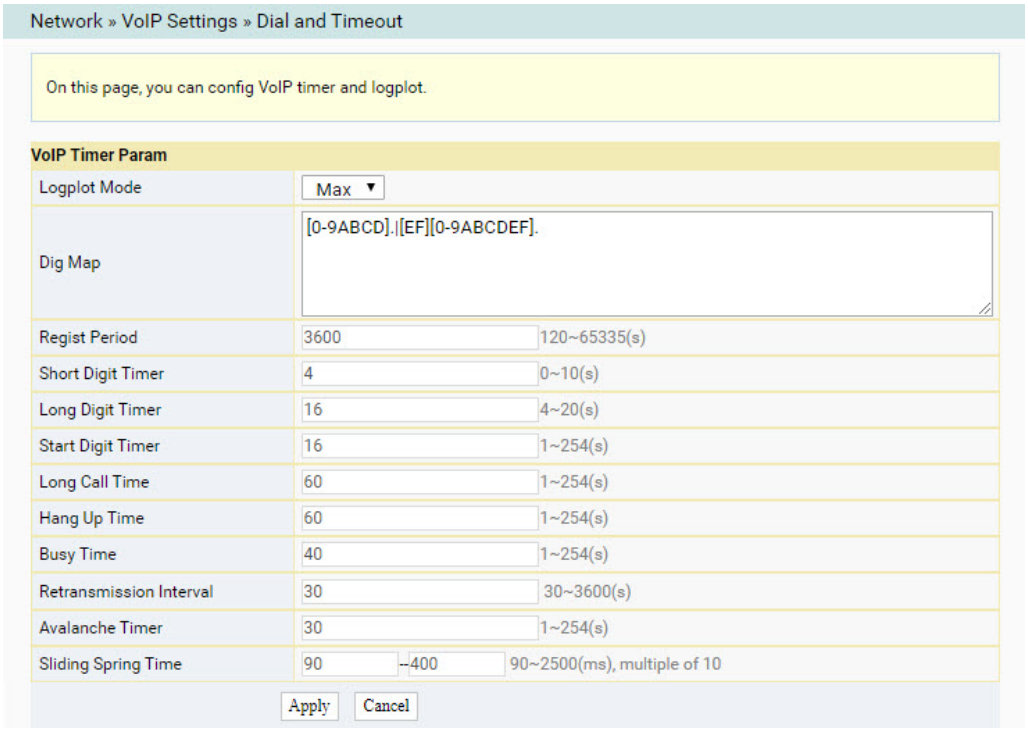


Figure 3-29 Digitmap and Time Length

2. Configure VoIP time length parameters. For details of the parameters, see Table 3-15.
3. Click **Apply** to save and apply the configuration.

Table 3-15 Parameters of Digitmap and Time Length

Item	Description
Logplot Mode	The digitmap matching mode. The options include **Max** and **Min**. The default setting is **Max**.
Regist Period	The SIP registration period. The value range is 120 to 65535 (s), and the default setting is 3600.
Short Digit Timer	The timeout period set for the short timer. The value range is 0 to 10 (s), and the default setting is 4.
Long Digit Timer	The timeout period set for the long timer. The value range is 4 to 20 (s), and the default setting is 16.
Start Digit Timer	The timeout period set for the starting timer. The value range is 1 to 254 (s), and the default setting is 16.

Table 3-15 Parameters of Digitmap and Time Length (Continued)

Item	Description
Long Call Time	The time for long call without response. The value range is 1 to 254 (s), and the default setting is 60.
Hang Up Time	The howler tone time. The value range is 1 to 254 (s), and the default setting is 60.
Busy Time	The busy tone time. The value range is 1 to 254 (s), and the default setting is 40.
Retransmission Interval	The interval for retransmission of registration information. The value range is 30 to 3600 (s), and the default setting is 30.
Avalanche Timer	The timeout period set for the avalanche timer. The value range is 1 to 254 (s), and the default setting is 30.
Sliding Spring Time	The sliding spring time. The value ranges from 90 to 2500 (ms) and should be multiples of 10. The default value range is 90 to 400.

3.3.6.5 Coding

Configure coding priority for voice ports. The parameters include priority, coding mode, RTP packetization period, and so on.

1. Select **Network** in the navigation bar and select **VoIP Settings→Coding** from the link bar on the left side to open the coding configuration page, as shown in Figure 3-30.

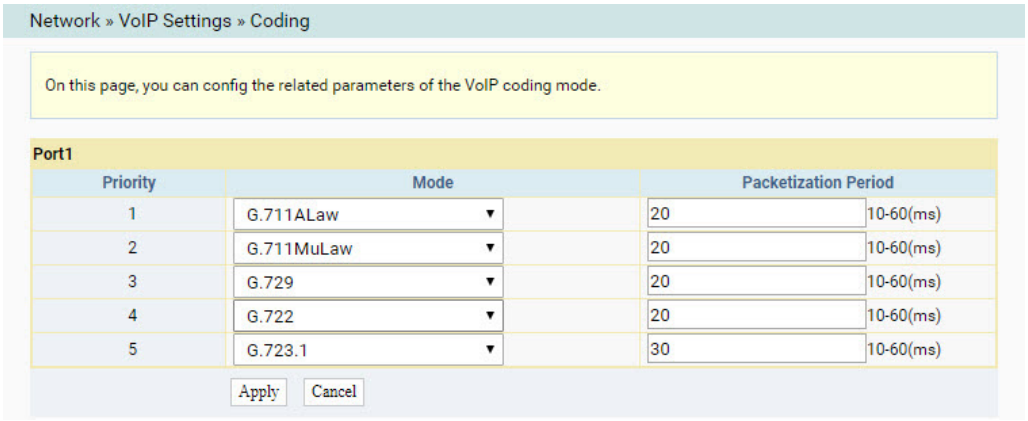


Figure 3-30 Coding

2. Configure parameters of voice ports, including priority, coding mode and RTP packetization period, as shown in Table 3-16.
3. Click **Apply** to save and apply the configuration.

Table 3-16 Coding Parameters

Item	Description
Mode	The coding mode. The options include G.711MuLaw, G.711ALaw, G.723.1, G.729 and G.722.
Packetization Period	The RTP packetization period. The value range is 10 to 60 (ms).

3.3.7 Route Settings

The following introduces how to configure the IPv4 default route and IPv4 static route.

3.3.7.1 IPv4 Default Route

Configure the IPv4 default route.

1. Select **Network** in the navigation bar and select **Route Settings→Default Route** in the left link bar to open the IPv4 Default Route configuration page, as shown in Figure 3-31.

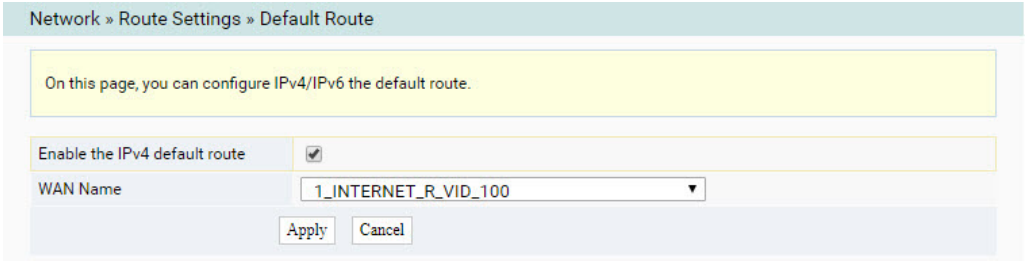


Figure 3-31 IPv4 Default Route

2. Select **Enable the IPv4 default route** and the corresponding WAN name as needed.
3. Click **Apply** to save and apply the configuration.

3.3.7.2 IPv4 Static Route

Configure the IPv4 static route.

1. Select **Network** in the navigation bar and select **Route Settings→IPv4 Static Route** in the left link bar to open the IPv4 static route configuration page, as shown in Figure 3-32.

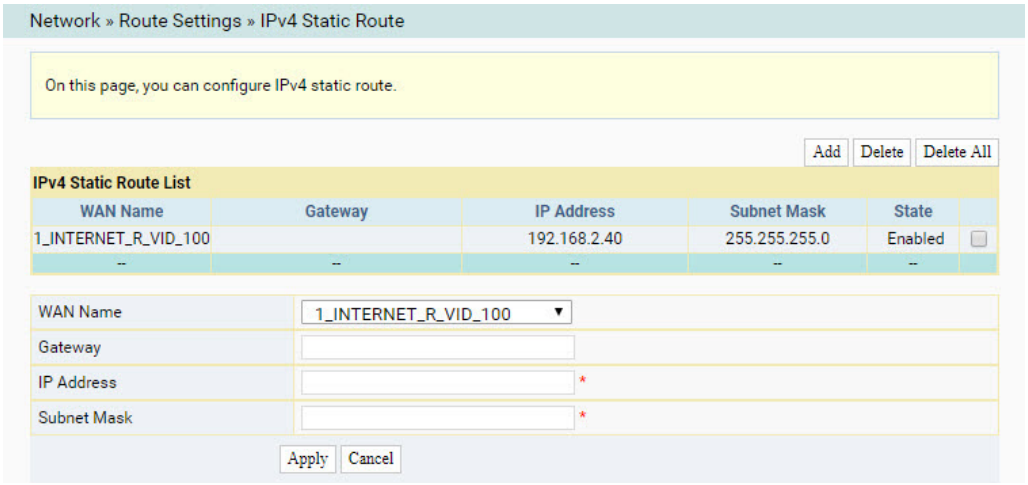


Figure 3-32 IPv4 Static Route

2. Configure relevant parameters according to the requirement.Table 3-17 describes the parameters.
3. Click **Apply** to save and apply the configuration.

Table 3-17 Parameters for IPv4 Static Route Configuration

Item	Description	
WAN Name	WAN name.	
Gateway	The gateway corresponding to the IP address.	
IP Address	The destination IP address.	Note: Make sure this IP address is not in the same network segment with that of the **LAN Interface** set on the **LAN Settings** page.
Subnet Mask	Subnet mask.	

3.4 Security

This section introduces how to configure the firewall, dynamic DoS and HTTPS on the web page.

3.4.1 Firewall

The firewall configuration includes

- Firewall Control
- IPv4 Filtering
- IPv6 Filtering
- DHCP Filtering
- URL Filtering
- Anti Port Scan
- MAC Filtering
- IPv6 MAC Filtering
- ACL Settings
- IPv6 ACL Settings

3.4.1.1 Firewall Control

Enabling the firewall can prevent malicious access to the WAN port of the ONT.

1. Select **Security** in the navigation bar and select **Firewall→Firewall Control** in the left link bar to open the firewall enabling page, as shown in Figure 3-33.

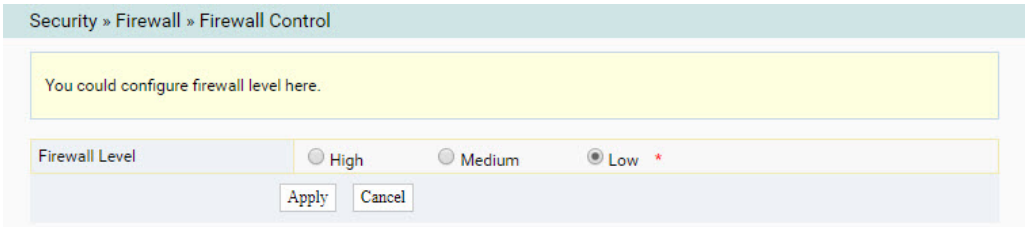


Figure 3-33 Firewall Control

2. Set the **Firewall Level** to **High**, **Medium** or **Low** as required.
3. Click **Apply** to save and apply the configuration.

3.4.1.2 IPv4 Filtering

Allow or forbid the incoming or outgoing flow of the IP packets meeting the filtering criteria. After the firewall is enabled, the pre-set rules will take effect.

1. Select **Security** in the navigation bar and select **Firewall→IPv4 Filtering** in the left link bar. Then click **Add** to open the filtering rule list configuration page, as shown in Figure 3-34.

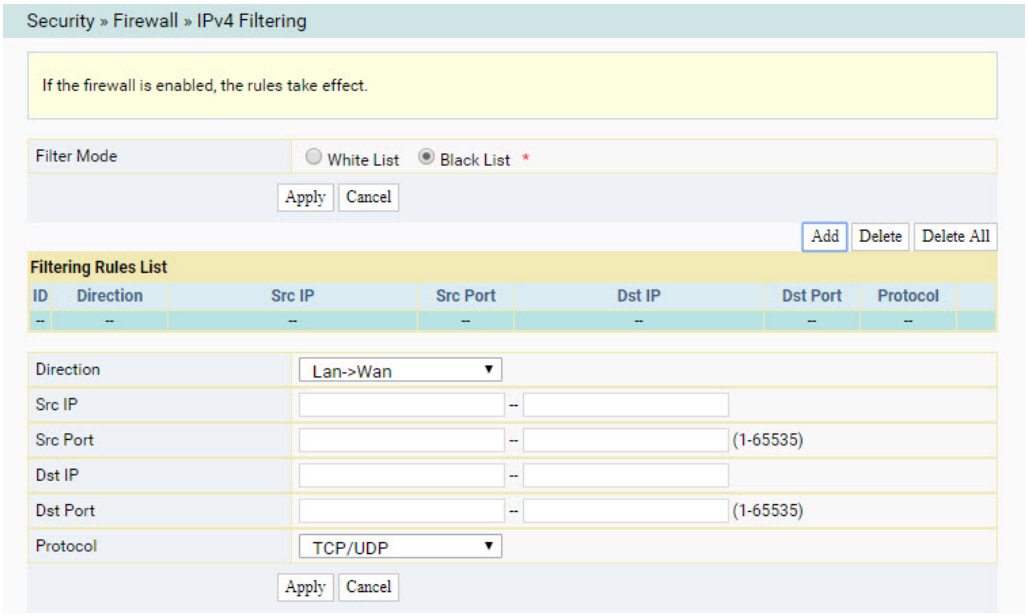


Figure 3-34 IPv4 Filtering

2. Configure the parameters relevant to filtering as required. For details of the parameters, see Table 3-18.
3. Click **Apply** to save and apply the configuration.

Table 3-18 Parameters for IP Address Filtering

Item	Description	
Filter Mode	Select the filtering mode. ◆ **White List** indicates that the data complying with the rules in the filtering rule table will be allowed to pass. ◆ **Black List** indicates that the data complying with the rules in the filtering rule table will not be allowed to pass.	Click the **Apply** button below to apply the settings.
Direction	Sets the direction of the filtering rule. ◆ LAN->WAN: uplink direction. ◆ WAN->LAN: downlink direction.	
Src IP	Enter the IP address at the LAN side if the direction is LAN->WAN. Enter the IP address at the WAN side if the direction is WAN->LAN.	
Src Port	The port range of the source IP address.	
Dst IP	Enter the IP address at the WAN side if the direction is LAN->WAN. Enter the IP address at the LAN side if the direction is WAN->LAN.	
Dst Port	The port range of the destination IP address.	
Protocol	The protocol type, including **TCP**, **UDP**, **TCP/UDP**, **ICMP** and **ALL**.	

3.4.1.3 IPv6 Filtering

Allow or forbid the IPv6 packets meeting the filtering criteria to be transmitted from the LAN or transmitted into the WAN. After the firewall is enabled, the pre-set rules will take effect.

1. Select **Security** in the navigation bar and select **Firewall→IPv6 Filtering** in the left link bar. Then click **Add** to open the IPv6 filtering rule list configuration page, as shown in Figure 3-35.

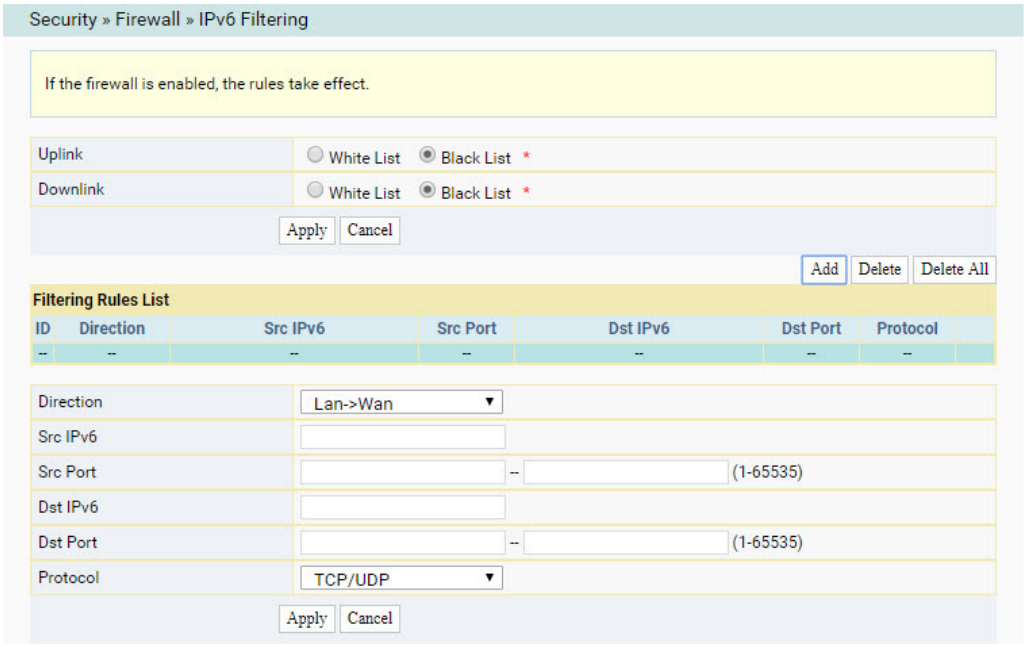


Figure 3-35 IPv6 Filtering

2. Configure the parameters relevant to filtering as required. For details of the parameters, see Table 3-19.

3. Click **Apply** to save and apply the configuration.

Table 3-19 Parameters of IPv6 Filtering

Item	Description	
Uplink	Select the uplink filtering mode. ◆ **White List** indicates that the data complying with the rules in the filtering rule table will be allowed to pass. ◆ **Black List** indicates that the data complying with the rules in the filtering rule table will not be allowed to pass.	Click the **Apply** button below to apply the settings.
Downlink	Select the downlink filtering mode. ◆ **White List** indicates that the data complying with the rules in the filtering rule table will be allowed to pass. ◆ **Black List** indicates that the data complying with the rules in the filtering rule table will not be allowed to pass.	
Direction	Sets the direction of the filtering rule. ◆ LAN->WAN: uplink direction. ◆ WAN->LAN: downlink direction.	

Table 3-19 Parameters of IPv6 Filtering (Continued)

Item	Description
Src IPv6	Enter the IPv6 address at the LAN side if the direction is set to LAN->WAN. Enter the IPv6 address at the WAN side if the direction is set to WAN->LAN.
Src Port	The port range of the source IP address.
Dst IPv6	Enter the IPv6 address at the WAN side if the direction is set to LAN->WAN. Enter the IPv6 address at the LAN side if the direction is set to WAN->LAN.
Dst Port	The port range of the destination IP address.
Protocol	The protocol type, including **TCP**, **UDP**, **TCP/UDP**, **ICMP** and **ALL**.

3.4.1.4 DHCP Filtering

Forbid or allow the user device configured with the MAC address to obtain an IP address in the DHCP mode to prevent DoS attacks. After the firewall is enabled, the pre-set rules will take effect.

1. Select **Security** in the navigation bar and select **Firewall→DHCP Filtering** in the left link bar. Then click **Add** to open the DHCP Filtering Table configuration page, as shown in Figure 3-36.

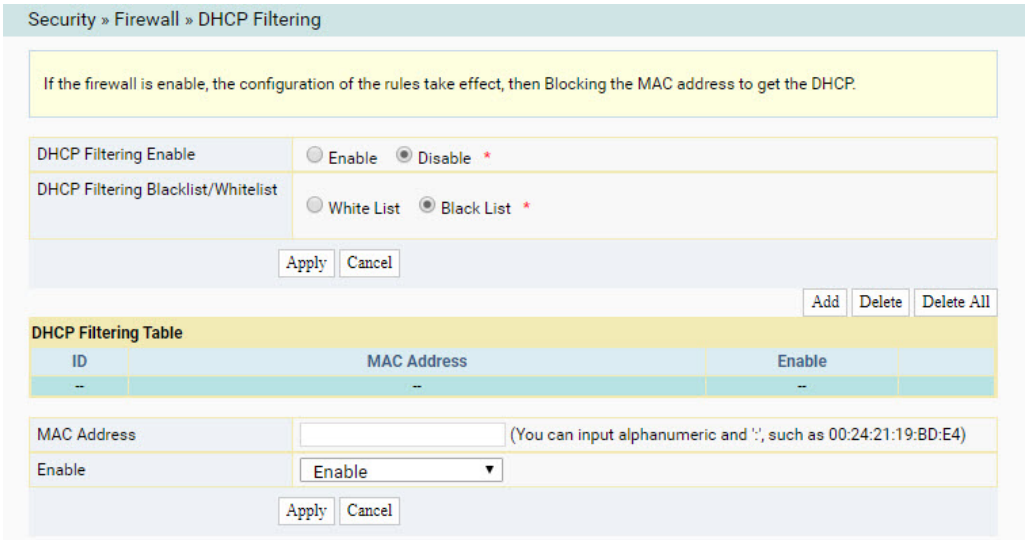


Figure 3-36 DHCP Filtering

2. Configure the parameters relevant to filtering as required. For details of the parameters, see Table 3-20.
3. Click **Apply** to save and apply the configuration.

Table 3-20 Parameters for DHCP Filtering

Item	Description	
DHCP Filtering Enable	Enables or disables the DHCP filtering.	Click the **Apply** button below to apply the settings.
DHCP Filtering Blacklist / Whitelist	Select the filtering mode. The white list and black list modes are configured globally and cannot be enabled simultaneously. ◆ **White List** indicates allowing the device configured with the MAC address to obtain an IP address through the DHCP. ◆ **Black List** indicates forbidding the device configured with the MAC address to obtain an IP address through the DHCP.	
MAC Address	The MAC address of the user device subject to the DHCP filtering rule.	
Enable	Enables or disables this filtering rule. The options include **Disable** and **Enable**.	

3.4.1.5 URL Filtering

By setting the URL filtering rules, users can forbid or allow all the data packets sent to or received from a certain IP address. After the firewall is enabled, the pre-set URL filtering rule will take effect, and the domain names that meet the filtering criteria will be filtered.

1. Select **Security** in the navigation bar and select **Firewall→URL Filtering** in the left link bar. Then click **Add** to open the URL filtering table configuration page, as shown in Figure 3-37.

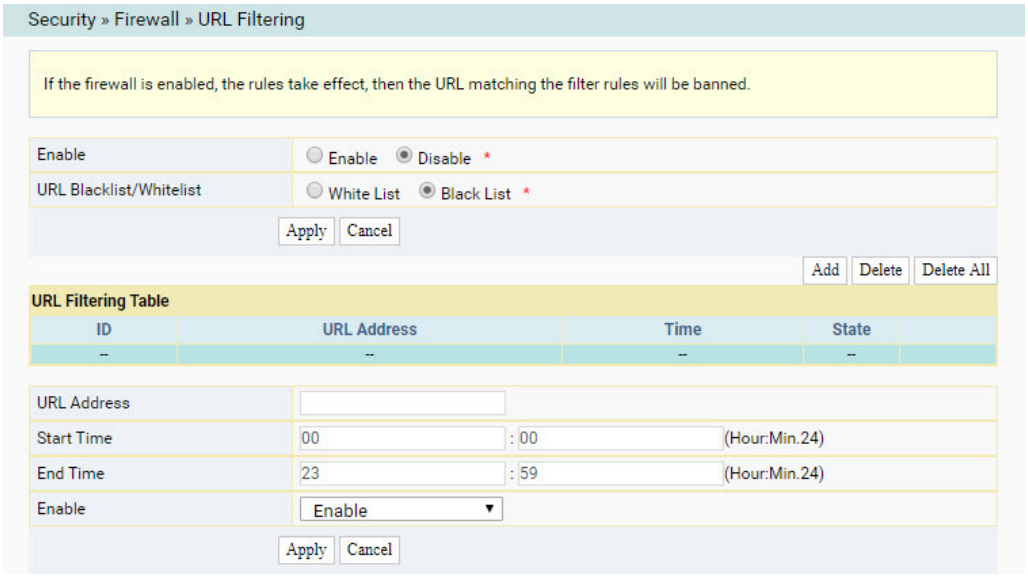


Figure 3-37 URL Filtering

2. Configure the parameters relevant to filtering as required. For details of the parameters, see Table 3-21.

3. Click **Apply** to save and apply the configuration.

Table 3-21 Parameters for URL Filtering Parameters

Item	Description	
Enable	Enables or disables the URL filtering function.	Click the **Apply** button below to apply the settings.
URL Blacklist / Whitelist	Select the filtering mode. The white list and black list modes are configured globally and cannot be enabled simultaneously. ◆ **White List** indicates that the data complying with the rules defined in the filtering table will be allowed to pass. ◆ **Black List** indicates that the data complying with the rules defined in the filtering table will not be allowed to pass.	
URL Address	The URL address accessed by users.	
Start Time	The starting time of the filtering rule.	
End Time	The ending time of the filtering rule.	
Enable	Enables or disables this filtering rule. The options include **Disable** and **Enable**.	

3.4.1.6 Anti Port Scan

Enable or disable the anti port scan function.

1. Select **Security** in the navigation bar and select **Firewall→Anti Port Scan** in the left link bar to open the anti port scan page, as shown in Figure 3-38.

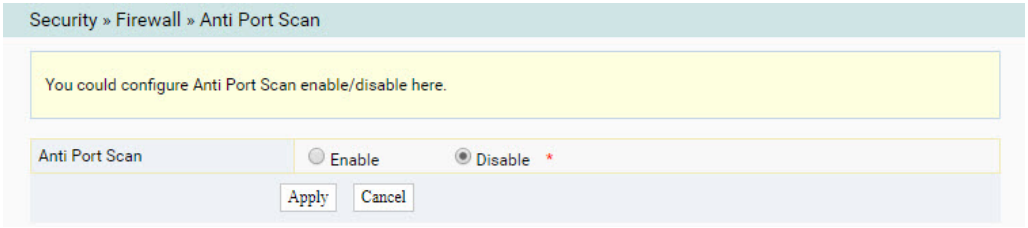


Figure 3-38 Anti-port Scan

2. Select to **Enable** or **Disable** the anti port scan function as required.
3. Click **Apply** to save and apply the configuration.

3.4.1.7 MAC Address Filtering

One user device may have multiple IP addresses but only one MAC address. The user device access authority in the LAN can be controlled effectively by setting the MAC address filtering. After the firewall is enabled, the pre-set rules will take effect, and the MAC addresses that meet the filtering criteria will be filtered.

1. Select **Security** in the navigation bar and select **Firewall→MAC Filtering** in the left link bar. Then click **Add** to open the MAC address filtering table configuration page, as shown in Figure 3-39.

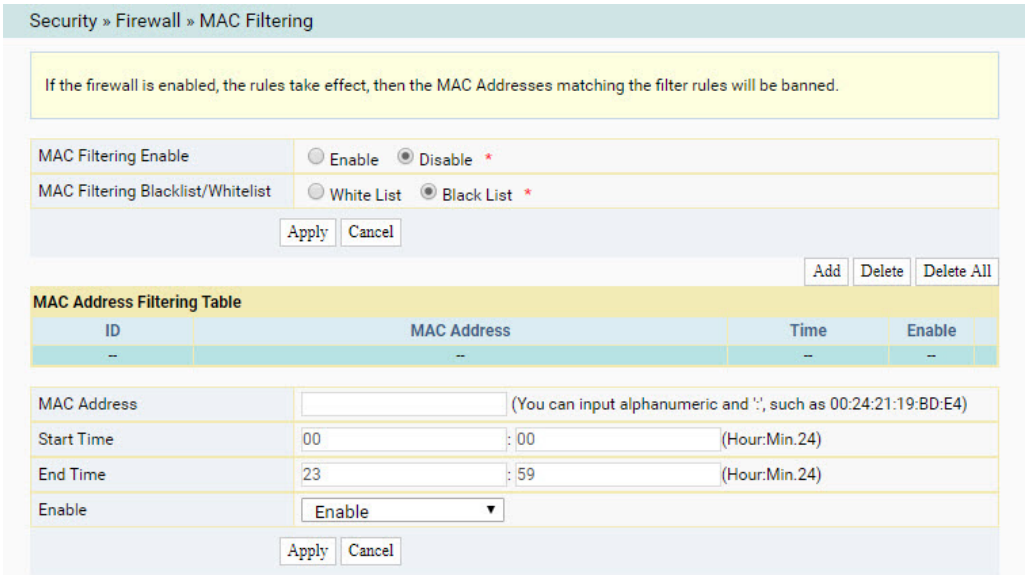


Figure 3-39 MAC Address Filtering

2. Configure parameters relevant to filtering as required. For details of the parameters, see Table 3-22.

3. Click **Apply** to save and apply the configuration.

Table 3-22 Parameters for MAC Address Filtering

Item	Description	
MAC Filtering Enable	Enables or disables the MAC address filtering function.	Click the **Apply** button below to apply the settings.
MAC Filtering Blacklist / Whitelist	Select the filtering mode. The white list and black list modes are configured globally and cannot be enabled simultaneously. ◆ **White List** indicates that the data complying with the rules defined in the filtering table will be allowed to pass. ◆ **Black List** indicates that the data complying with the rules defined in the filtering table will not be allowed to pass.	
MAC Address	The MAC address in the MAC address filtering rule.	
Start Time	The starting time of the filtering rule.	
End Time	The ending time of the filtering rule.	
Enable	Enables or disables this filtering rule. The options include **Disable** and **Enable**.	

3.4.1.8 IPv6 MAC Filtering

One user device may have multiple IPv6 addresses but only one MAC address. The user device access authority in the LAN can be controlled effectively by setting the MAC address filtering. After the firewall is enabled, the pre-set rules will take effect, and the MAC addresses that meet the filtering criteria will be filtered.

1. Select **Security** in the navigation bar and select **Firewall→IPv6 MAC Filtering** in the left link bar. Then click **Add** to open the configuration page for the MAC address filtering table, as shown in Figure 3-40.

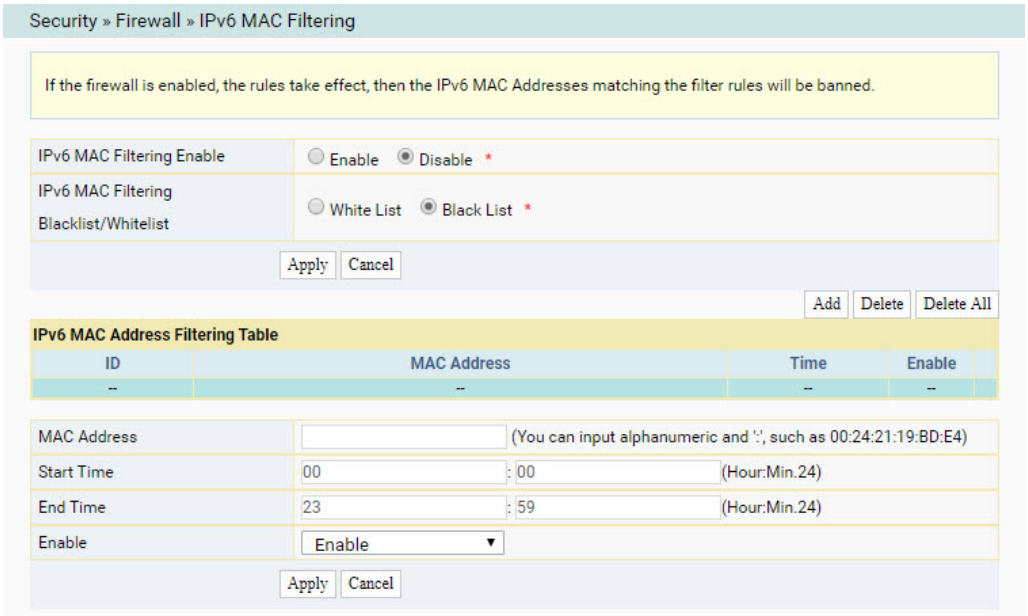


Figure 3-40 IPv6 MAC Filtering

2. Configure the parameters relevant to filtering as required. For details of the parameters, see Table 3-23.
3. Click **Apply** to save and apply the configuration.

Table 3-23 Parameters for IPv6 MAC Address Filtering

Item	Description	
IPv6 MAC Filtering Enable	Enables or disables the IPv6 MAC address filtering function.	Click the **Apply** button below to apply the settings.

Table 3-23 Parameters for IPv6 MAC Address Filtering (Continued)

Item	Description	
IPv6 MAC Filtering Blacklist / Whitelist	Select the filtering mode. The white list and black list modes are configured globally and cannot be enabled simultaneously. ◆ **White List** indicates that the data complying with the rules defined in the filtering table will be allowed to pass. ◆ **Black List** indicates that the data complying with the rules defined in the filtering table will not be allowed to pass.	
MAC Address	The IPv6 MAC address in the IPv6 MAC address filtering rule.	
Start Time	The starting time of the filtering rule.	
End Time	The ending time of the filtering rule.	
Enable	Enables or disables this filtering rule. The options include **Disable** and **Enable**.	

3.4.1.9 ACL Settings

The ONT provides ACL function. After the ACL rule is enabled, the corresponding port will filter the packets as per the configured ACL rules.

1. Select **Security** in the navigation bar and select **Firewall→ACL Settings** in the left link bar. Then click **Add** to open the ACL configuring page, as shown in Figure 3-41.

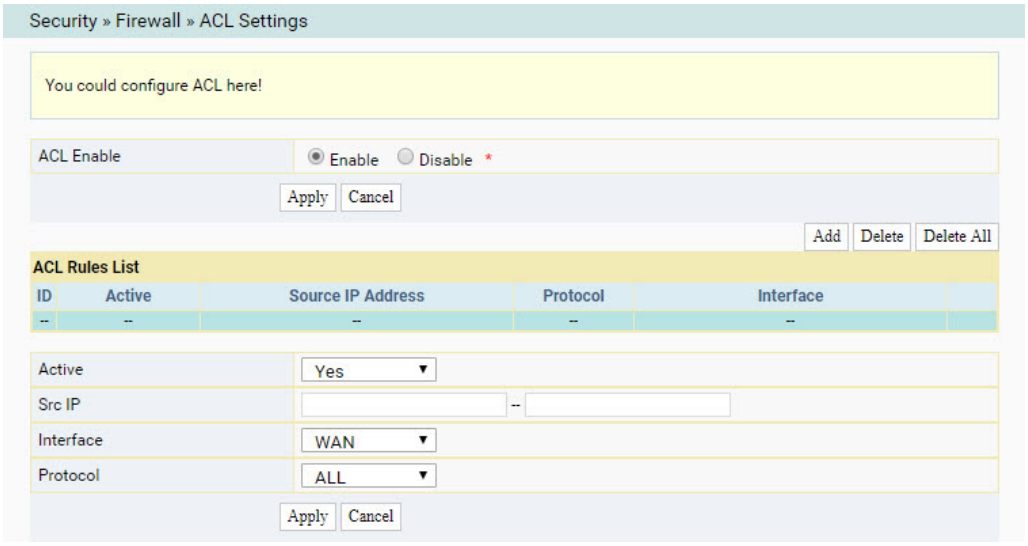


Figure 3-41 ACL Settings

2. Configure the parameters relevant to ACL as required. Table 3-24 describes the parameters.

3. Click **Apply** to save and apply the configuration.

Table 3-24 Parameters for ACL Settings

Item	Description
ACL Enable	Enables or disables the ACL function. After setting, click **Apply** below so that the setting can take effect.
Active	Activates or deactivates this filtering rule. The option includes **Yes** and **No**.
Src IP	Enter the IP address.
Interface	Set the interface to **WAN** or **LAN**.
Protocol	Protocol type, including **HTTP**, **Telnet**, **ICMP**, **SNMP**, **FTP**, **SSH** and **ALL**.

3.4.1.10 IPv6 ACL Settings

The ONT provides IPv6 ACL function. After the IPv6 ACL rule is enabled, the corresponding port will filter the packets as per the configured ACL rules.

1. Select **Security** in the navigation bar and select **Firewall→IPv6 ACL Settings** in the left link bar. Then click **Add** to open the IPv6 ACL configuring page, as shown in Figure 3-42.

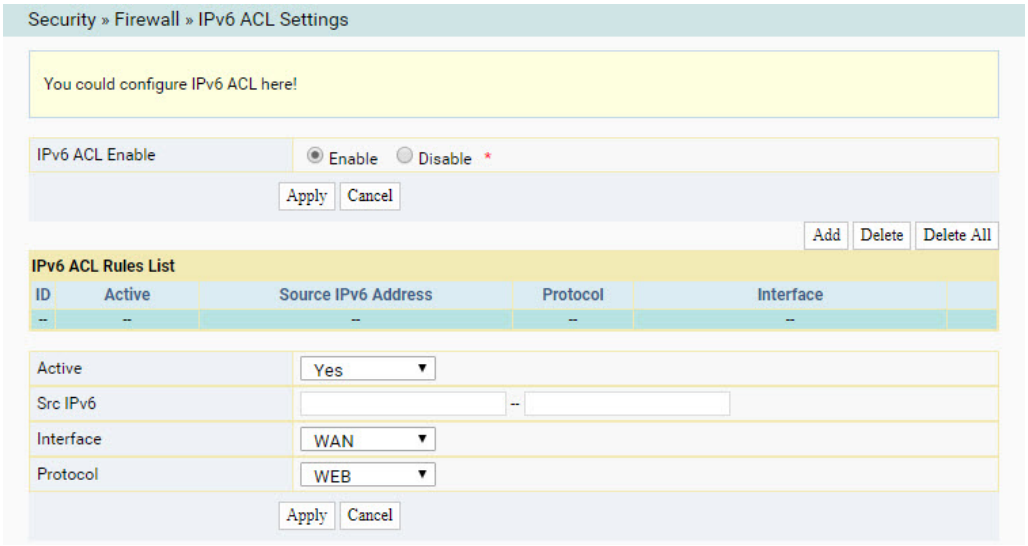


Figure 3-42 IPv6 ACL Settings

2. Configure the parameters relevant to IPv6 ACL as required. Table 3-25 describes the parameters.

3. Click **Apply** to save and apply the configuration.

Table 3-25 Parameters for IPv6 ACL Settings

Item	Description
IPv6 ACL Enable	Enables or disables the IPv6 ACL function. After setting, click **Apply** below so that the setting can take effect.
Active	Activates or deactivates this filtering rule. The option includes **Yes** and **No**.
Src IPv6	Enter the IP address.
Interface	Set the interface to **WAN** or **LAN**.
Protocol	Protocol type, including **WEB** and **PING**.

3.4.2 Dynamic DoS

The DoS attack exhausts the resource of target computer using massive virtual information flow, so that the attacked computer has to handle the virtual information with all strength, which influences the handling of normal information flow. The ONT provides the protection against the DoS attack.

1. Select **Security** in the navigation bar and select **DDOS→DDOS** in the left link bar to open the anti-DoS attack configuration page, as shown in Figure 3-43.

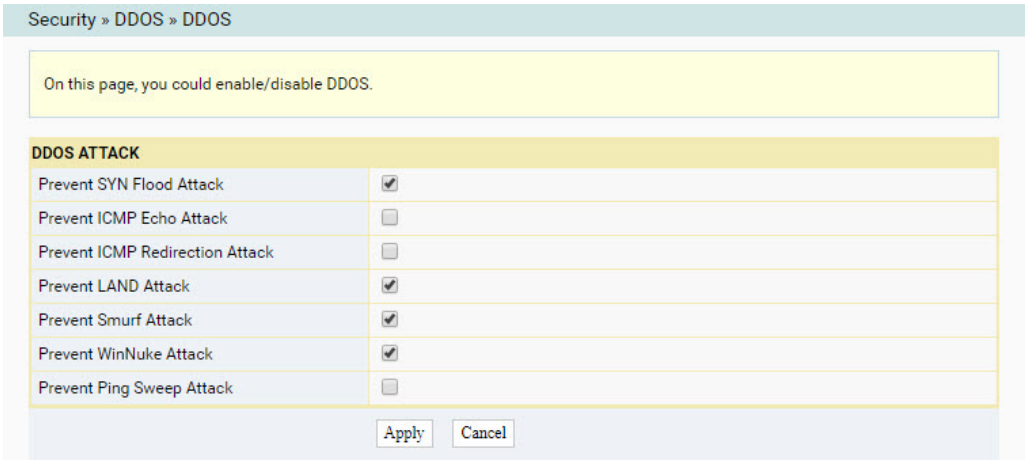


Figure 3-43 Dynamic DoS

2. Enable or disable protection against DDoS attacks as needed.

3. Click **Apply** to save and apply the configuration.

3.4.3 HTTPS

The ONT provides the HTTPS function. HTTPS is the HTTP channel for security purpose. It is built on the SSL+HTTP protocol, and can perform encryption transmission and identity authentication.

1. Select **Security** in the navigation bar and select **HTTPS→HTTPS** in the left link bar to open the HTTPS function configuration page, as shown in Figure 3-44.

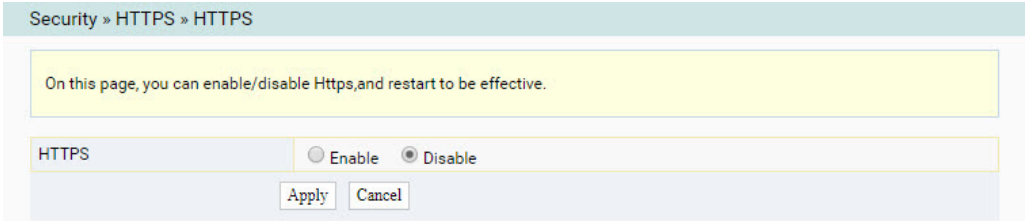


Figure 3-44 HTTPS

2. Select to **Enable** or **Disable** the HTTPS function as required.

Caution:

After enabling the HTTPS function, log into the web page. The protocol type in URL should be https, e.g. **https://192.168.1.1**.

3. Click **Apply** to save and apply the configuration.

3.5 Application

This section introduces how to configure the VPN, DDNS, port mapping, NAT, UPnP, DMZ, web port and network diagnosis on the web page.

3.5.1 VPN

Set whether to enable the VPN transparent transmission channel.

1. Select **Application** in the navigation bar and select **VPN→VPN Passthrough** in the left link bar to open the page for configuring the VPN transparent transmission, as shown in Figure 3-45.

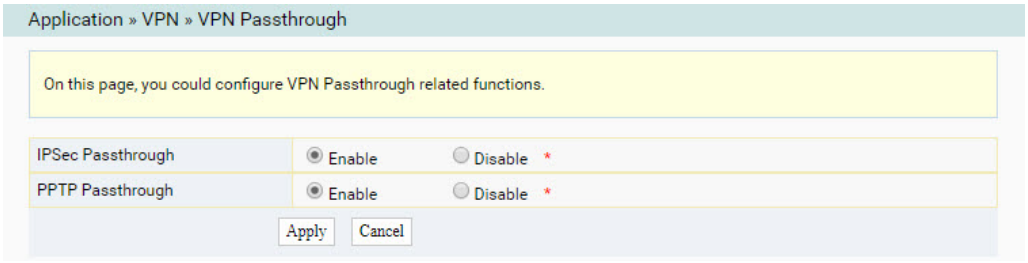


Figure 3-45 VPN Transparent Transmission

2. Configure the parameters **IPSec Passthrough** and **PPTP Passthrough** enabled or disabled as required.
3. Click **Apply** to save and apply the configuration.

3.5.2 DDNS

The DDNS server transforms the dynamic IP address at the WAN side of the ONT into a static domain name. Users from Internet can easily access the gateway using this domain name.

1. Select **Application** in the navigation bar and select **DDNS→DDNS** in the left link bar to open the DDNS configuration page, as shown in Figure 3-46.

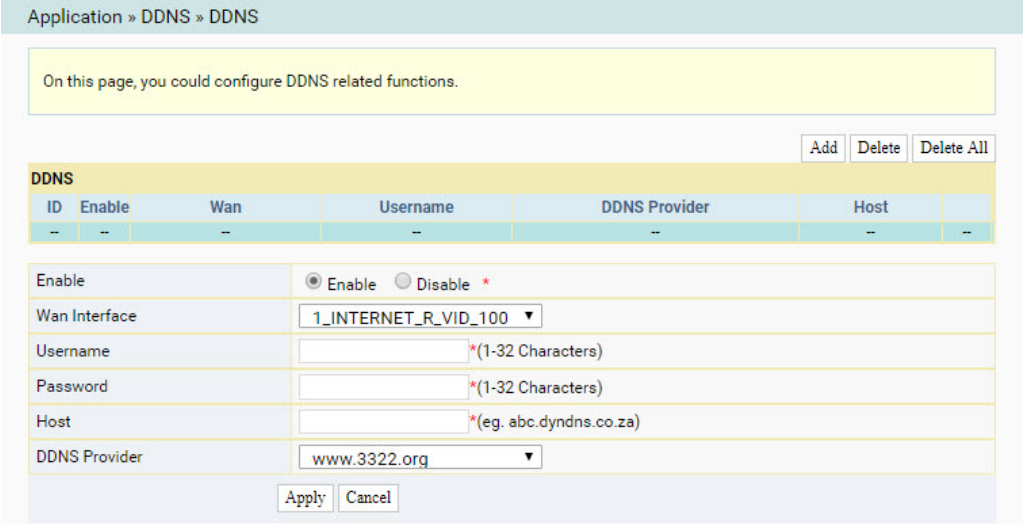


Figure 3-46 DDNS Settings

2. Configure parameters relevant to DDNS according to the requirement. For details of the parameters, see Table 3-26.

3. Click **Apply** to save and apply the configuration.

Table 3-26 Parameters for DDNS Settings

Item	Description
Enable	Enables or disables the rule.
Wan Interface	The name of the created WAN connection.
Username	The username allocated by the DDNS provider.
Password	The password allocated by the DDNS provider.
Host	The domain name allocated by the DDNS provider.
DDNS Provider	The DDNS service provider.

3.5.3 Port Mapping

Port mapping can generate the mapping between the WAN port IP address / common port number and the LAN server IP address / private port number. In this way, all the accesses to a certain service port at this WAN port will be re-directed to the corresponding port of the server in the designated LAN.

1. Select **Application** in the navigation bar and select **Port Mapping→Port Mapping** in the left link bar. Then click **Add** to open the port mapping configuration page, as shown in Figure 3-47.

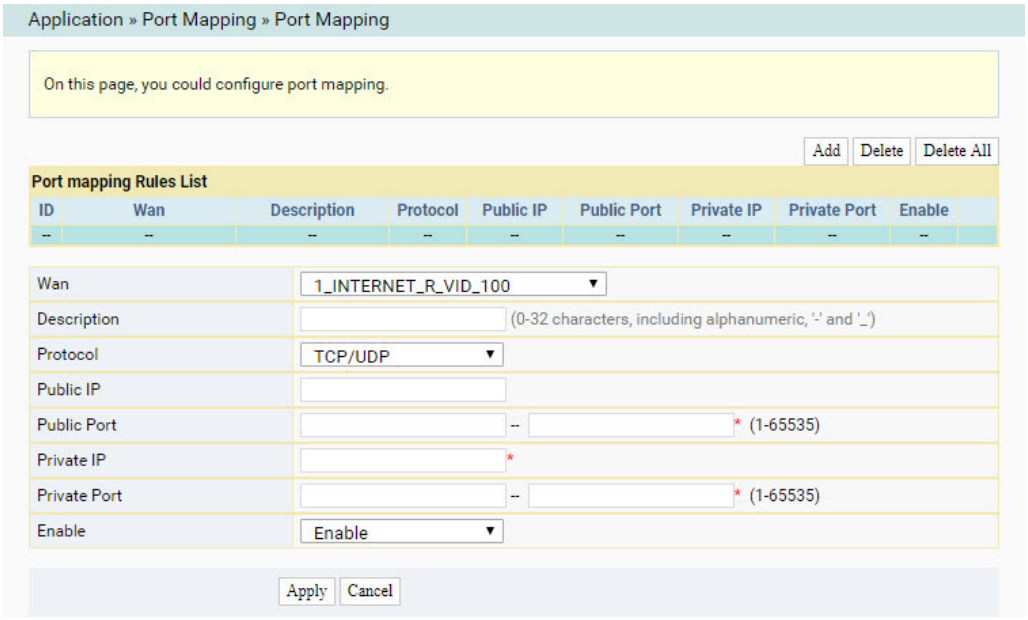


Figure 3-47 Port Mapping

2. Configure parameters relevant to port mapping according to the requirement. For details of the parameters, see Table 3-27.

3. Click **Apply** to save and apply the configuration.

Table 3-27 Parameters for Port Mapping

Item	Description
Wan	The WAN connection bound with the port mapping rule.
Description	The port mapping rule name.
Protocol	The protocol used for the port to forward data packets. The options include TCP/UDP, TCP and UDP.
Public IP	The IP address of the Extranet virtual server for port mapping.
Public Port	The range of ports for Extranet data packets. If only one port exists, enter the same port number.
Private IP	The IP address of the LAN virtual server for port mapping.
Private Port	The range of the LAN ports for mapping. If only one port exists, enter the same port number.
Enable	Enables or disables the rule.

3.5.4 NAT

NAT allows the conversion between intranet IP addresses and public network IP addresses. NAT converts a great number of intranet IP addresses into one or a small number of public network IP addresses, so as to save the resource of public network IP addresses.

Note:

The NAT configuration below can take effect only when the NAT function is enabled in **Network→BroadBand Settings→Internet Settings**.

1. Select **Application** in the navigation bar and select **NAT→NAT** in the left link bar. Then click **Add** to open the NAT rule list configuration page, as shown in Figure 3-48.

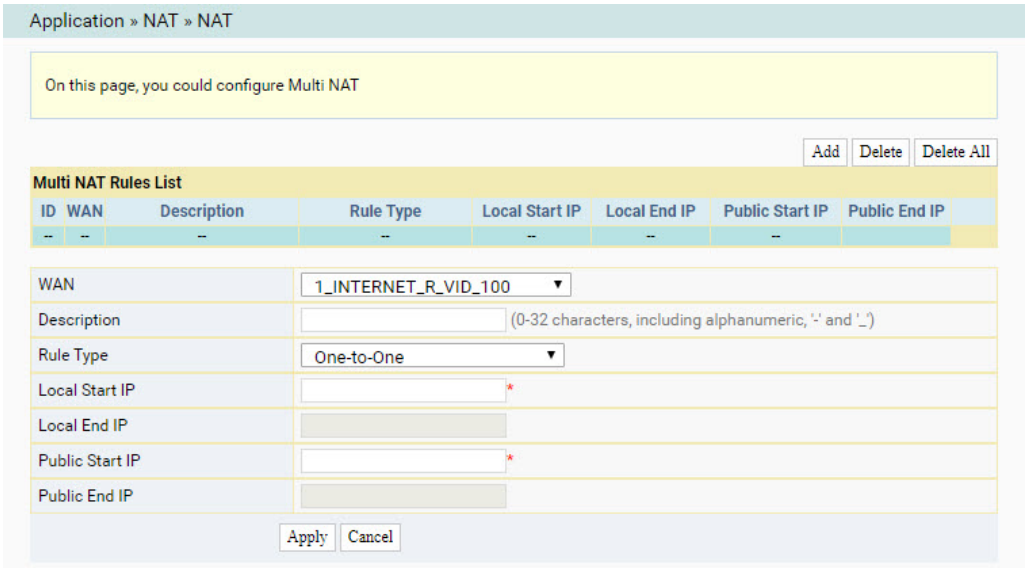


Figure 3-48 NAT

2. Configure relevant parameters according to the requirement. For details of the parameters, see Table 3-28.
3. Click **Apply** to save and apply the configuration.

Table 3-28 Parameters for NAT Configuration

Item	Description
WAN	The WAN connection bound with the NAT rule.
Description	The NAT rule name.

Table 3-28 Parameters for NAT Configuration (Continued)

Item	Description
Rule Type	Select the NAT conversion mode. It is advisable to select **One-to-One** or **Many-to-One**.
Local Start IP	The starting IP address of the intranet.
Local End IP	The ending IP address of the intranet.
Public Start IP	The starting IP address of the public network.
Public End IP	The ending IP address of the public network.

3.5.5 UPnP

The UPnP supports the plug and play function and the automatic discovery function of multiple network devices. When UPnP is enabled, the devices that supports UPnP can be added into the network dynamically. In this way, an external computer can access the resource on the internal computer when necessary. For example, when some application software are running on a PC, the port mapping table will be generated on the ONT automatically using the UPnP protocol, so that the operation can be sped up.

1. Select **Application** in the navigation bar and select **UPNP→UPNP** in the left link bar to open the UPnP configuration page, as shown in Figure 3-49.

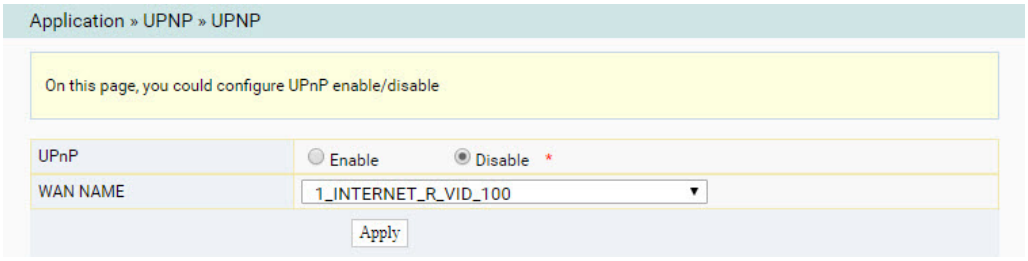


Figure 3-49 UPnP

2. Select to **Enable** or **Disable** the UPnP function as required.
3. Select name of the created WAN connection.
4. Click **Apply** to save and apply the configuration.

3.5.6 DMZ

When the ONT is working in the routing mode, enable the DMZ function if a host at the WAN side needs to access a certain host at the LAN side. The ONT will forward all the IP packets from the WAN to the designated DMZ host.

1. Select **Application** in the navigation bar and select **DMZ→DMZ** in the left link bar. Click **Add** to open the DMZ configuration page, as shown in Figure 3-50.

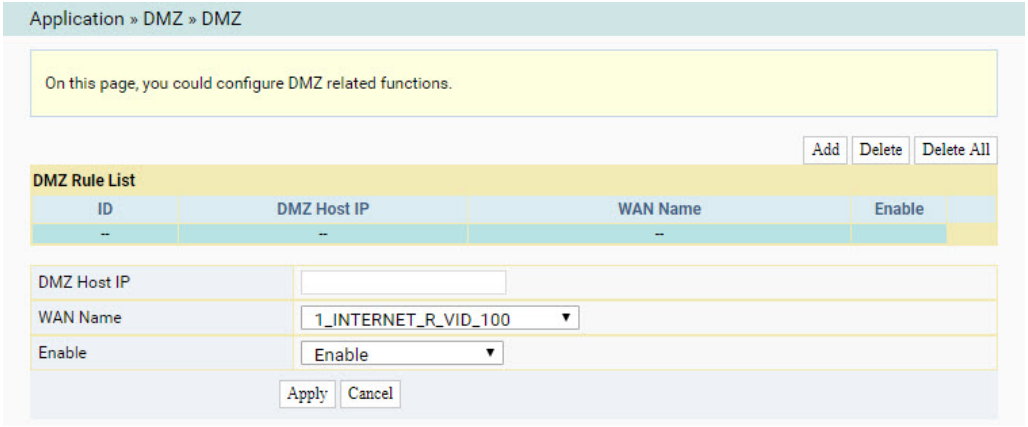


Figure 3-50 DMZ

2. Configure relevant parameters according to the requirement. For details of the parameters, see Table 3-29.
3. Click **Apply** to save and apply the configuration.

Table 3-29 Parameters for DMZ Configuration

Item	Description
DMZ Host IP	The host IP address of the DMZ.
WAN Name	Name of the created WAN connection.
Enable	Enables or disables the DMZ function.

3.5.7 Web Port

Configure the HTTP communication port for the web. The configuration becomes valid after the equipment is restarted.

1. Select **Application** in the navigation bar and select **Web Port→Web Port** in the left link bar to open the Web Port configuration page, as shown in Figure 3-51.

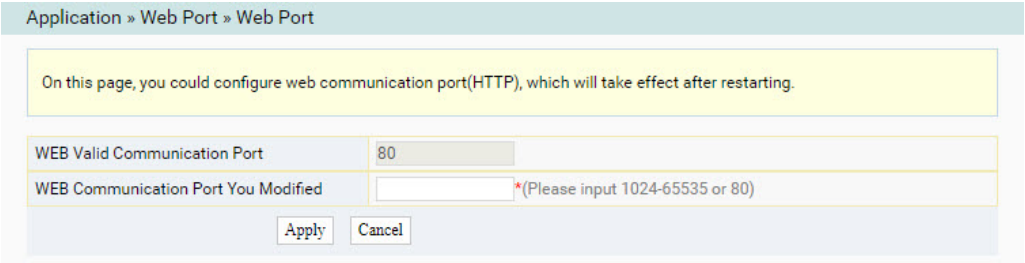


Figure 3-51 Web Port

2. Configure relevant parameters according to the requirement. Table 3-30 describes the parameters.

3. Click **Apply** to save and apply the configuration.

Table 3-30 Parameters for Web Port Configuration

Item	Description
WEB Valid Communication Port	The current valid web communication port.
WEB Communication Port You Modified	The modified web communication port. The value ranges from 1024 to 65535, and can also be set to 80.

3.5.8 Network Diagnosis

Network Diagnosis includes ping diagnosis and tracert diagnosis.

3.5.8.1 Ping Diagnosis

Test whether the router is normally connected with the target host or another device in the ping diagnosis page.

1. Select **Application** in the navigation bar and select **Diagnosis→Ping Diagnosis** in the left link bar to open the diagnosis page, as shown in Figure 3-52.

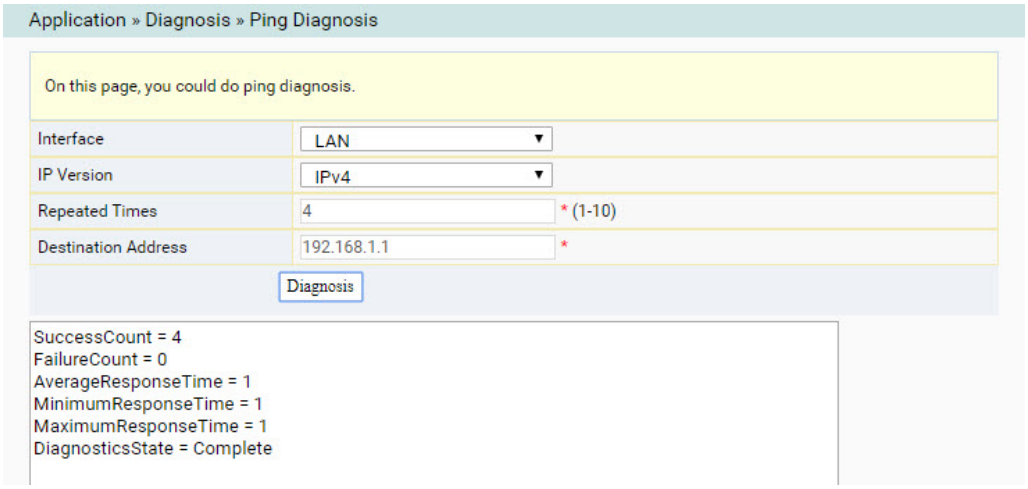


Figure 3-52 Ping Diagnosis

2. Configure relevant parameters according to the requirement. Table 3-31 describes the parameters.

3. Click **Diagnosis** to test. The test result will be displayed in the lower text box.

Table 3-31 Parameters for Ping Diagnosis Configuration

Item	Description
Interface	Name of the created WAN connection.
IP Version	The version of the destination IP address.
Repeated Times	The repeated times for diagnosis. The value ranges from 1 to 10.
Destination Address	The destination IP address to be tested.

3.5.8.2 Tracert Diagnosis

Check the routing condition from the router to the target host in the tracert diagnosis page.

1. Select **Application** in the navigation bar and select **Diagnosis→Tracert Diagnosis** in the left link bar to open the diagnosis page, as shown in Figure 3-53.

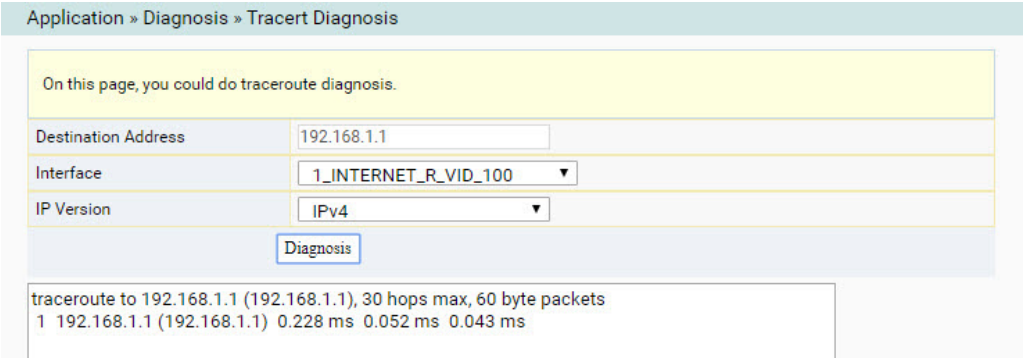


Figure 3-53 Tracert Diagnosis

2. Configure relevant parameters according to the requirement. Table 3-32 describes the parameters.

3. Click **Diagnosis** to test. The test result will be displayed in the lower text box.

Table 3-32 Parameters for Tracert Diagnosis Configuration

Item	Description
Destination Address	The destination IP address to be tested.
Interface	Name of the created WAN connection.
IP Version	The version of the destination IP address.

3.6 Management

This section introduces how to perform account management, device management and log management on the web page.

3.6.1 Account Management

Account management includes user account management and maintenance account management.

3.6.1.1 User Account Management

Users can modify the password of a common user account.

1. Select **Management** in the navigation bar. Select **Account Management→User Account** from the left link bar to open the user account management page, as shown in Figure 3-54.

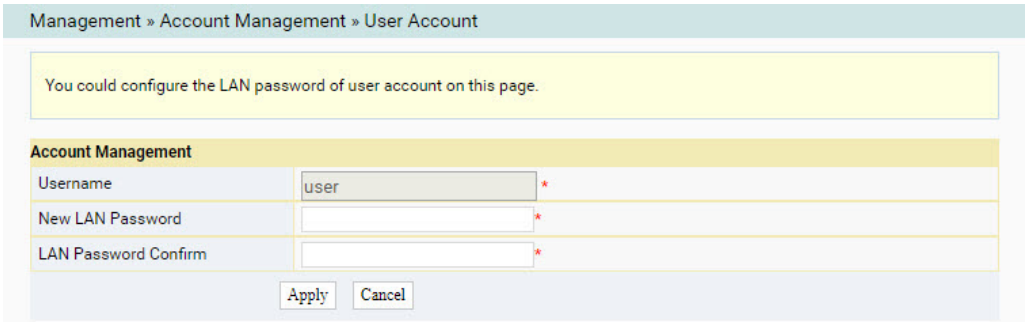


Figure 3-54 User Account Management

2. Modify the password of a common user account as required.
3. Click **Apply** to save and apply the configuration.

3.6.1.2 Maintenance Account Management

Users can modify the password of the maintenance account.

1. Select **Management** in the navigation bar. Select **Account Management→ Maintenance Account** from the left link bar to open the maintenance account management page, as shown in Figure 3-55.

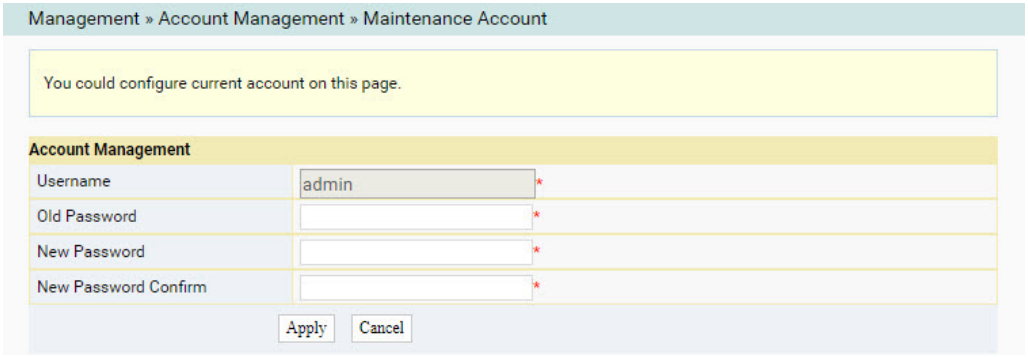


Figure 3-55 Maintenance Account Management

2. Modify the password of the maintenance account as required.
3. Click **Apply** to save and apply the configuration.

3.6.2 Device Management

The ONT provides multiple device management functions such as restoring some of the configuration data, local upgrade, configuration backup, device reboot, FTP server, and NTP time calibration.

3.6.2.1 Restoring the Configuration Data

Restore factory settings of the ONT, including user name and password for Web login, SSID and password for wireless network, etc.

1. Select **Management** in the navigation bar. Select **Device Management→Restore** from the left link bar to open the configuration restoring page, as shown in Figure 3-56.

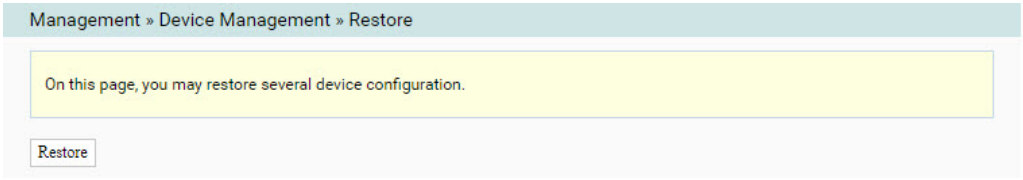


Figure 3-56 Restoring the Configuration Data

2. Click **Restore** and then click **OK** in the alert box that appears. Wait until the configuration data are completely restored.

3.6.2.2 Local Upgrade

Select the local file and upgrade the ONT software. During upgrade, do not power off the device or perform other operations to prevent damage to the device.

1. Select **Management** in the navigation bar. Select **Device Management→Local Upgrade** from the left link bar to open the local upgrade page, as shown in Figure 3-57.

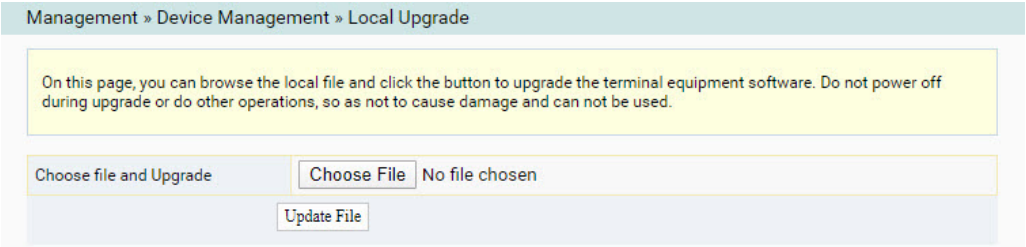


Figure 3-57 Local Upgrade

2. Click **Choose file**. In the dialog box that appears, select the device software version to be upgraded and click **Update File** to upgrade the ONT software.
3. When the upgrade succeeds, the page will prompt for device rebooting. Click **Reboot**. After rebooting, the device will be upgraded to the new version.

Note:

After the upgrade, you can view the **Software Version** in the device information page to check whether the current version is correct.

3.6.2.3 Configuration Backup

Back up and update the configuration files.

1. Select **Management** in the navigation bar. Select **Device Management→Config Backup** from the left link bar to open the configuration backup page, as shown in Figure 3-58.

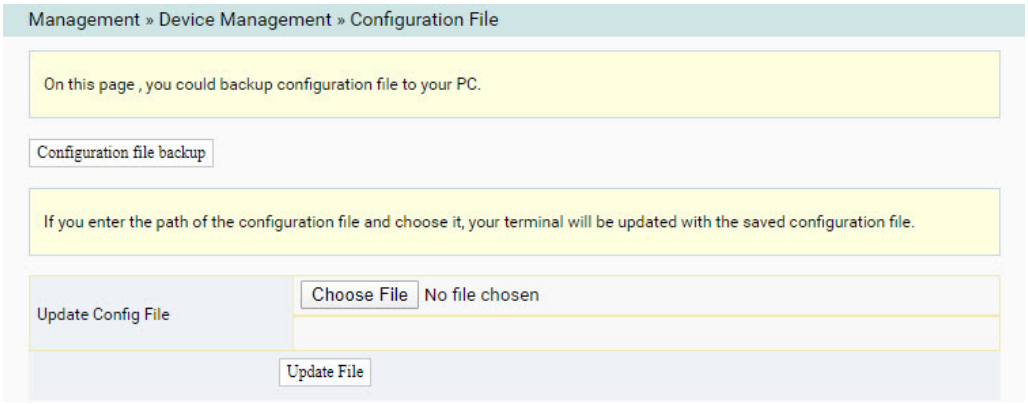


Figure 3-58 Configuration Backup

- Backup configuration file

  Click **Configuration file backup** to back up the ONT configuration file into computer.

- Update configuration file

  Click **Choose file**, in the dialog box that appears, select the configuration file to be updated and click **Update File**. The terminal will be updated with the saved configuration file.

3.6.2.4 Device Reboot

1. Select **Management** in the navigation bar. Select **Device Management→Device Reboot** from the left link bar to open the device reboot page, as shown in Figure 3-59.

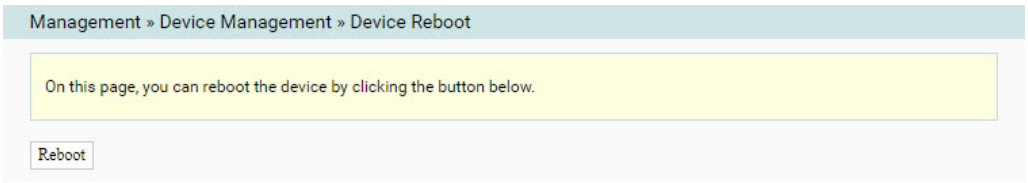


Figure 3-59 Device Reboot

2. Click **Reboot** and click **OK** in the alert box that appears and wait for the device to reboot.

Caution:

Save the configuration data before rebooting the device to prevent loss of the data.

After the device is rebooted, wait for about two minutes before next login to the web page of the device.

3.6.2.5 NTP Time Calibration

Users can obtain the precise time by connecting the ONT to an NTP server.

1. Select **Management** in the navigation bar. Select **Device Management→NTP Check Time** from the left link bar to open the NTP check time page, as shown in Figure 3-60.

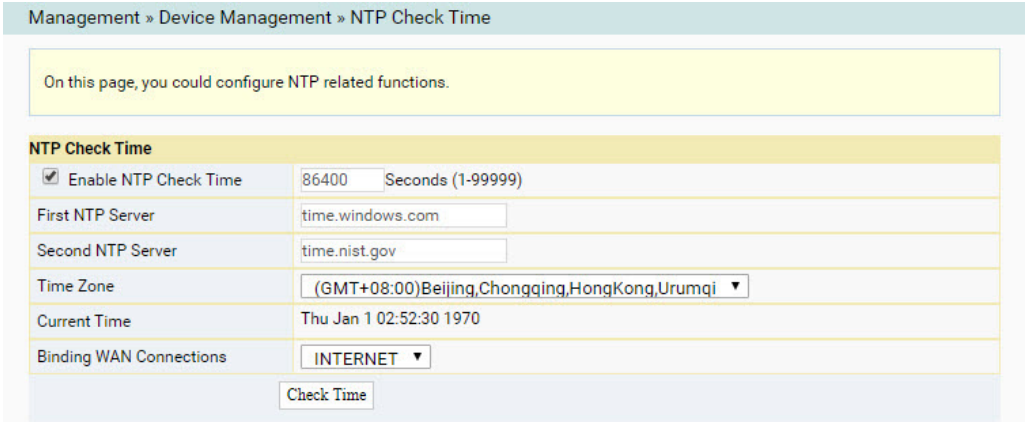


Figure 3-60 NTP Time Calibration

2. Configure parameters relevant to the NTP time calibration. For details of the parameters, see Table 3-33.
3. Click **Check Time** to save and apply the configuration.

Table 3-33 Parameters for NTP Time Calibration

Item	Description
Enable NTP Check Time	Select whether to enable the NTP time calibration function.
Seconds	Sets the time interval for synchronization with the time server.
First NTP Server	Enter the IP address of the active NTP server.

Table 3-33 Parameters for NTP Time Calibration (Continued)

Item	Description
Second NTP Server	Enter the IP address of the standby NTP server.
Time Zone	Select the time zone according to the location of the device.
Current Time	When NTP Check Time is enabled, time will be calibrated according to the location of the device, and the local time will be displayed. When NTP Check Time is disabled, the system initial time (1970-01-01) or the previous calibrated time will be displayed.
Binding WAN Connections	Select the WAN connection type for time calibration.

3.6.2.6 FTP Server

With the FTP server function of the ONT enabled, users can access the ONT resources via the FTP client end on the PC.

1. Select **Management** in the navigation bar. Select **Device Management→FTP Server** from the left link bar to open the FTP server configuration page, as shown in Figure 3-61.

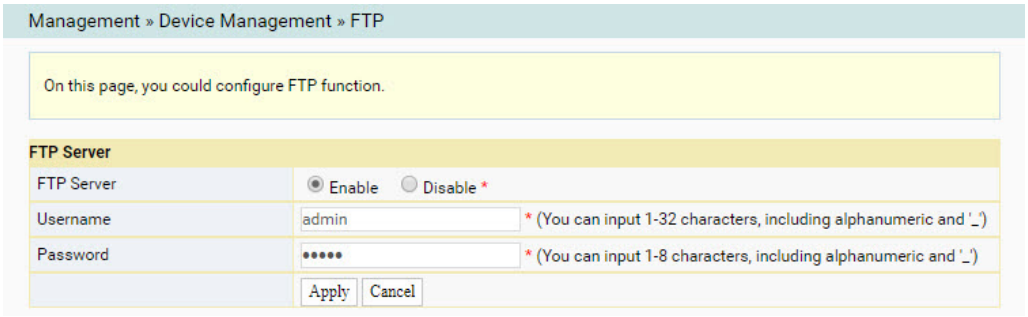


Figure 3-61 FTP Server

2. Enable or disable the FTP server function according to the requirement. Select **Enable** and then enter the **Username** and **Password** for connection with the FTP server.
3. Click **Apply** to save and apply the configuration.

3.6.3 Log Management

The log files record key operations and actions on the ONT. Users can view the information saved in the log as needed.

Select **Management** in the navigation bar. Select **Log→Log** from the left link bar to open the log information page, as shown in Figure 3-62.

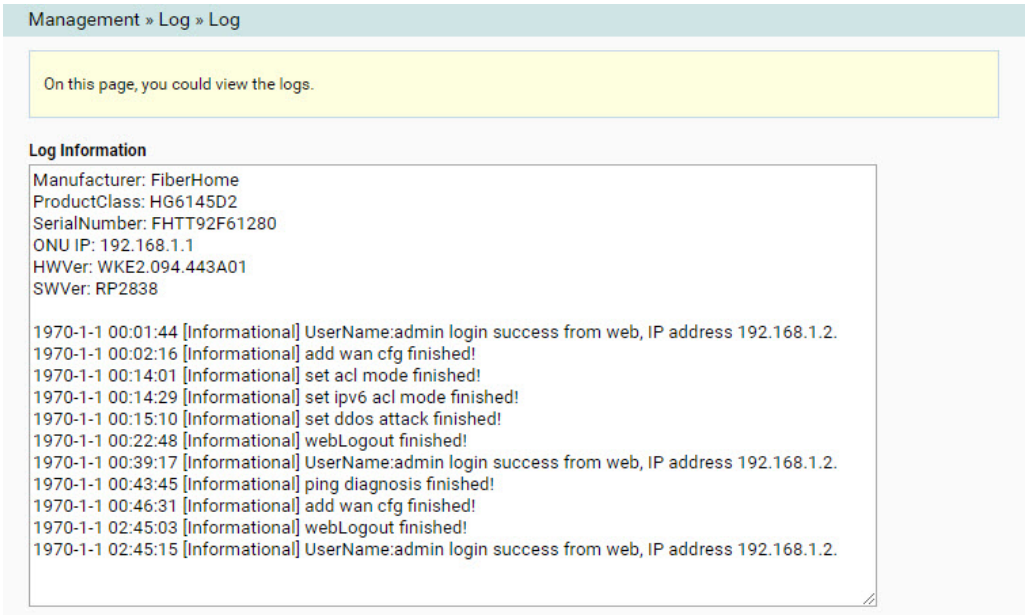


Figure 3-62 Log

4 Handling Common Problems

This chapter introduces how to handle common problems encountered in equipment operation and service test.

4.1 Power Status Indicator LED Extinguished

Handle the problem according to the procedures below.

1. Check whether the mains supply is normal.
2. Check whether the power adapter matches the device.
3. Check whether the power button is pressed down.
4. Check whether the power cable connection is normal.

4.2 Register Status Indicator LED Extinguished

Handle the problem according to the procedures below.

1. Check whether the device power supply is normal.
2. Check whether the optical fiber connection is normal.
3. Check whether the ONT has obtained the ISP authorization.
4. Check whether the optical interface is normal; if not, replace the device.

4.3 Optical Signal Status Indicator LED Blinking

Handle the problem according to the procedures below.

1. Check whether the optical fiber is damaged.
2. Check whether the optical fiber is connected to the correct interface.
3. Check whether the Rx optical power of the ONT (measured with the optical power meter) is below specifications.
4. Check whether the ONT optical module is aged or damaged.

5. Check whether the local device is faulty.

4.4 Ethernet Interface Status Indicator LED Extinguished

Handle the problem according to the procedures below.

1. Check whether the network cable is damaged or connected incorrectly.
2. Check whether the color-coding scheme of the network cable is incorrect; if so, replace it with a standard CAT-5 twisted pair network cable.
3. Check whether the network cable length exceeds the allowed range (100 m).

4.5 Failing to Detect the ONT Using Wi-Fi

Handle the problem according to the procedures below.

1. Check whether the wireless function is disabled for the ONT and whether the SSID is set to **Hidden** so that the network is invisible.
2. Check whether the network card drive of the computer is installed normally and whether the WLAN function of the wireless terminal (such as computer and telephone) is enabled.
3. Adjust the position of the ONT to reduce the barriers on the wireless channel (such as walls) and make sure the distance between the ONT and the wireless terminal is within the required range.

4.6 Failing to Access Local Web Login Page and Failing to Ping 192.168.1.1

Handle the problem according to the procedures below.

1. Check whether the LAN port indicator LED is solid ON; if not, replace the network cable.
2. Check whether the computer is set with a fixed IP address in the network segment of 192.168.1.x.

4.7 Failing to Access Internet Using the LAN Port

Handle the problem according to the procedures below.

1. Check whether the computer is set with a fixed IP address. If yes, modify the configuration so that the computer can obtain an IP address automatically. Then retry the connection.
2. If the computer obtains an IP address automatically, check whether the computer has obtained an IP address in the network segment of 192.168.x.x.
3. Contact the personnel in the network management center to check whether the WAN is connected correctly and bound with the LAN port.

4.8 Failing to Access Internet Using Wi-Fi

Handle the problem according to the procedures below.

1. Check whether the computer is connected to the ONT's Wi-Fi signal correctly and can obtain an IP address automatically.
2. Contact the personnel in the network management center to check whether the WAN connection is bound with the Wi-Fi port correctly.

4.9 Measured Internet Access Rate Out of Normal Range

Contact the personnel in the network management center to check whether the bandwidth profile is configured correctly and bound to the ONT.

4.10 Test of Voice Service Failed

Handle the problem according to the procedures below.

1. Check whether you can hear the current tone when you go off-hook; if no, check whether the phone cable is connected correctly.

2. Check whether you can hear the dial tone when you go off-hook; if no, contact the network management center to check whether the voice service work order has been delivered correctly and whether the uplink device has delivered the configuration data to the voice service port of the ONT.
3. Log into the ONT to check whether it has obtained an IP address for the voice service .
4. Contact the softswitch platform to check whether the voice node data have been configured.

5 Standards and Protocols

Classification	Standard Number	Title
GPON	ITU-T G.984.1	Gigabit-capable passive optical networks (GPON): General characteristics
	ITU-T G.984.2	Gigabit-capable Passive Optical Networks (GPON): Physical Media Dependent (PMD) layer specification
	ITU-T G.984.3	Gigabit-capable Passive Optical Networks (G-PON): Transmission convergence layer specification
	ITU-T G.984.4	Gigabit-capable passive optical networks (G-PON): ONT management and control interface specification
Ethernet	IEEE 802-2001	IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture
	IEEE 802.1D-2004	IEEE Standard for Local and metropolitan area networks: Media Access Control (MAC) Bridges
	IEEE 802.1Q-2005	IEEE Standard for Local and Metropolitan Area Networks - Virtual Bridged Local Area Networks - Amendment 4: Provider Bridges
	IEEE 802.1ad	IEEE Standard for Local and Metropolitan Area Networks - Virtual Bridged Local Area Networks - Amendment 4: Provider Bridges
	IEEE 802.1x-2004	IEEE Standard for Local and Metropolitan Area Networks Port- Based Network Access Control
	IEEE 802.1ag-2007	IEEE Standard for Local and Metropolitan Area Networks Virtual Bridged Local Area Networks Amendment 5: Connectivity Fault Management
	IEEE 802.3-2005	IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications
	IEEE 802.3z	Gigabit Ethernet Standard
	IEEE 802.1p	Traffic class expediting and dynamic multicast filtering. Describes important methods for providing QoS at MAC level
	TR-101	Migration to Ethernet-Based Broadband Aggregation
	TR-143	Enabling Network Throughput Performance Tests and Statistical Monitoring

Classification	Standard Number	Title
VoIP	ITU-T G.711	Pulse code modulation (PCM) of voice frequencies
	ITU-T G.711.1	Wideband embedded extension for G.711 pulse code modulation
	ITU-T G.722	7 kHz audio-coding within 64 kbit/s
	ITU-T G.723.1	Dual rate speech coder for multimedia communications transmitting at 5.3 and 6.3 kbit/s
	ITU-T G.729	Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP)
	ITU-T G.729.1	G.729 based Embedded Variable bit-rate coder: An 8-32 kbit/s scalable wideband coder bitstream interoperable with G.729
	ITU-T G.165	Echo Cancellers
	ITU-T G.168	Digital network echo cancellers
Multicast	IETF RFC 2236	Internet Group Management Protocol, Version 2
	IETF RFC 3376	Internet Group Management Protocol, Version 3
	IETF RFC 4541	Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches
Time	IETF RFC 1305	Network Time Protocol (Version 3) Specification, Implementation and Analysis
	IETF RFC 2030	Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI
EMC	EN 300 386	Electromagnetic compatibility and Radio spectrum Matters (ERM); Telecommunication network equipment; Electromagnetic Compatibility (EMC) requirements
	CISPR 22 (EN55022)	Information technology equipment - Radio disturbance characteristics - Limits and methods of measurement
	CISPR 24 (EN55024)	Information technology equipment - Immunity characteristics - Limits and methods of measurement

Appendix A Abbreviations

ONT	Optical Network Terminal
FTTH	Fiber To The Home
GPON	Gigabit-capable Passive Optical Network
ODN	Optical Distribution Network
OLT	Optical Line Termination
MTBF	Mean Time Between Failure
DBA	Dynamic Bandwidth Allocation
XML	Extensible Markup Language
GEM	GPON Encapsulation Mode
ATM	Asynchronous Transfer Mode
OAM	Operation, Administration And Maintenance
FEC	Forward Error Correction
TDMA	Time Division Multiple Access
PLOAM	Physical Layer Operations, Administration and Maintenance
OMCI	ONU Management and Control Interface
T-CONT	Transmission Container
NSR	Network Security Recorder
AES	Advanced Encryption Standard
MAC	Medium Access Control
IGMP	Internet Group Management Protocol
VLAN	Virtual Local Area Network
QoS	Quality of Service
ACL	Access Control List
WRR	Weighted Round Robin
DHCP	Dynamic Host Configuration Protocol
PPPoE	Point to Point Protocol over Ethernet
NAT	Network Address Translation
DMZ	Demilitarized Zone
ARP	Address Resolution Protocol

UPnP	Universal Plug and Play
DoS	Denial of Service
URL	Uniform Resource Locator
HTTPS	Hyper Text Transfer Protocol over Secure Socket Layer
CATV	Cable Antenna Television
SIP	Session Initiation Protocol
VoIP	Voice over Internet Protocol
RTP	Real-time Transport Protocol
SSID	Service Set Identifier
WAN	Wide Area Network
LAN	Local Area Network
WLAN	Wireless Local Area Networks
MTU	Maximum Transmission Unit
PPPoE	Point to Point Protocol over Ethernet
DTMF	Dual Tone Multi Frequency
VPN	Virtual Private Network
DDNS	Dynamic Domain Name Server
FTP	File Transfer Protocol
CPE	Customer Premise Equipment
EMC	Electro Magnetic Compatibility
GUI	Graphical User Interface
HG	Home Gateway
ICMP	Internet Control Message Protocol
IP	Internet Protocol
LAN	Local Area Network
MLD	Multicast Listener Discover
PON	Passive Optical Network
POTS	Plain Old Telephone Service
SP	Strict Priority
STB	Set Top Box
TCP	Transmission Control Protocol
UDP	User Datagram Protocol