

User Guide

HG series HGU products



This guide is for reference only and does not imply that the product supports all functions in the guide. The functions may differ with different product models or different versions of the same model. The actual product prevails.

Copyright statement

© 2022-2024 Shenzhen Tenda Technology Co., Ltd. All rights reserved.

Tenda is a registered trademark legally held by Shenzhen Tenda Technology Co., Ltd. Other brand and product names mentioned herein are trademarks or registered trademarks of their respective holders. Copyright of the whole product as integration, including its accessories and software, belongs to Shenzhen Tenda Technology Co., Ltd. No part of this publication can be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the prior written permission of Shenzhen Tenda Technology Co., Ltd.

Disclaimer

Pictures, images and product specifications herein are for references only. To improve internal design, operational function, and/or reliability, Tenda reserves the right to make changes to the products without obligation to notify any person or organization of such revisions or changes. Tenda does not assume any liability that may occur due to the use or application of the product described herein. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information and recommendations in this document do not constitute a warranty of any kind, express or implied.

Preface

Thank you for choosing Tenda! This guide is a complement to Quick Installation Guide. The Quick Installation Guide provides instructions for quick internet setup, while this guide contains details of each function and demonstrates how to configure them.

Applicable product

This user guide walks you through all functions of the HGU products. All the screenshots herein, unless otherwise specified, are taken from HG15V2.0.

Conventions

This guide is for reference only and does not imply that the product supports all functions in the guide. The functions supported by different models or different versions of the same model may differ. The actual product prevails.



The product figures and screenshots in this guide are for examples only. They may be different from the actual products you purchased, but do not affect the normal use.

If the function or parameter is displayed in gray on the product web interface, the product model is not supported or cannot be modified.

The typographical elements that may be found in this document are defined as follows.

Item	Presentation	Example
Cascading menus	>	System > Live Users
Parameter and value	Bold	Set User Name to Tom .
Variable	Italic	Format: <i>XX:XX:XX:XX:XX:XX</i>
UI control	Bold	On the Policy page, click the OK button.
Message	“ ”	The “Success” message appears.

The symbols that may be found in this document are defined as follows.

Symbol	Meaning
	This format is used to highlight information of importance or special interest. Ignoring this type of note may result in ineffective configuration, loss of data or damage to devices.
	This format is used to highlight a procedure that will save time or resources.

For more documents

If you want to get more documents about the device, visit www.tendacn.com and search for the corresponding product model.

Technical support

Contact us if you need more help. We will be glad to assist you as soon as possible.

Email address: support@tenda.cn

Website: www.tendacn.com

Revision history

Tenda is constantly searching for ways to improve its products and documentation. The following table indicates any changes that might have been made since this guide was first published.

Version	Date	Description
V1.2	2024-10-30	1. Added the description of the ICMP packets limit , energy saving configuration , WAN user and auto system maintenance .
		2. Optimized the description of getting to know your device , configuring INTERNET settings , view PON status , PPP settings , port forwarding , setting a hotline , and obtaining an IPv4/IPv6 address automatically .
		3. Optimized sentence expression.
V1.1	2023-12-08	1. Added the description of the View VoIP port status , Band steering and Inform report function.
		2. Optimized the description of Get to know your device , Basic settings of WLAN , WAN and Obtain an IPv4/IPv6 address automatically with computer .
		3. Optimized sentence expression.
V1.0	2023-03-23	Original publication.

Contents

Get to know your device	1
Web UI	4
2.1 Login	4
2.2 Logout	6
2.3 Web UI layout	6
2.4 Common buttons	7
Quick registration	8
3.1 Configure GPON or EPON settings	8
3.2 Configure INTERNET settings	9
3.3 Configure Wi-Fi settings	10
Status	11
4.1 ONT status	11
4.2 Device list	15
LAN	17
5.1 LAN interface settings	17
5.2 DHCP	18
WLAN	21
6.1 Band steering	21
6.2 Basic settings	22
6.3 Access control	28
6.4 WPS	30
6.5 Status	39
6.6 Mesh	40
WAN	45
7.1 Overview	45
7.2 Bridge mode	53
7.3 Router mode	58
7.4 NAT	64
Services	65
8.1 Service	65
8.2 Firewall	70
VoIP	88
9.1 Set VoIP proxy	88

9.2 Change advanced SIP settings	90
9.3 Set the forward mode	92
9.4 Set speed dial rules	93
9.5 Abbreviated dial	94
9.6 Set a dial plan	94
9.7 Set coding type	95
9.8 Set a hotline	96
9.9 Set the Don't Disturb mode	97
9.10 Set an alarm	97
9.11 Set fax protocol	98
Advance	99
10.1 Advanced settings	99
10.2 IP QoS settings	105
10.3 IPv6 settings	112
10.4 Energy saving configuration	118
Diagnostics	119
11.1 Ping and Tracert	119
11.2 Execute Ping to test connectivity	120
11.3 Execute Traceroute to test routing	121
11.4 Inform report	121
Admin	122
12.1 GPON/EPON settings	122
12.2 OMCI information	122
12.3 Commit/Reboot	123
12.4 Backup/Restore	123
12.5 WAN user	125
12.6 System log	126
12.7 Password	128
12.8 Auto logout time	129
12.9 Firmware upgrade	129
12.10 ACL	130
12.11 Time zone	132
12.12 Auto system maintenance	133
12.13 TR-069	134
12.14 Logout	135
Statistics	136
13.1 Interface statistics	136
13.2 PON statistics	137
Appendixes	138
A.1 Obtain an IPv4/IPv6 address automatically	138
A.2 Acronyms and abbreviations	143

1 Get to know your device

The ONTs are Fiber to the Home (FTTH) devices that provide internet access and other services with a fiber cord connected.

1.1.1 Indicators, ports and buttons

■ LED indicators

The LED indicators may vary with models. The actual product prevails.

LED indicator	Color	Status	Description
PWR	Green	Solid on	The ONT is powered on.
		Off	The ONT is powered off.
INET	Green	Solid on	The internet access is available through the ONT.
		Blinking	Data is being transmitted through the ONT.
		Off	No internet access is available through the ONT.
PON	Green	Solid on	The ONT is registered successfully.
		Blinking	The ONT is registering.
		Off	The ONT is unregistered.
LOS	Red	Blinking	The received optical power is lower than the optical receiver sensitivity.
		Off	The received optical power is at a proper value.
LAN	Green	Solid on	The LAN port is connected. No data is being transmitted.
		Blinking	The LAN port is transmitting data.
		Off	The LAN port is disconnected.
TEL	Green	Solid on	The ONT is registered with IMS. No data is being transmitted.
		Blinking	The ONT is registered with IMS and is transmitting data.
		Off	The ONT is not registered with IMS.
WLAN/2.4G/5G	Green	Solid on	The Wi-Fi network is enabled.
		Blinking	Data is being transmitted wirelessly.
		Blinking	For the device without the WPS LED indicator: If the WPS function is activated on the device, the WLAN/2.4G/5G LED indicator blinking means that the device is performing WPS negotiation.
		Off	The Wi-Fi network is disabled.
		Off	

LED indicator	Color	Status	Description
WPS	Green	Solid on for 2 minutes	A WPS connection is established.
		Blinking	The WPS negotiation is ongoing.
		Off	The WPS function is not activated.
USB	Green	Solid on	The USB port is connected. No data is being transmitted.
		Blinking	The USB port is transmitting data.
		Off	The USB port is disconnected.

■ Ports & Buttons

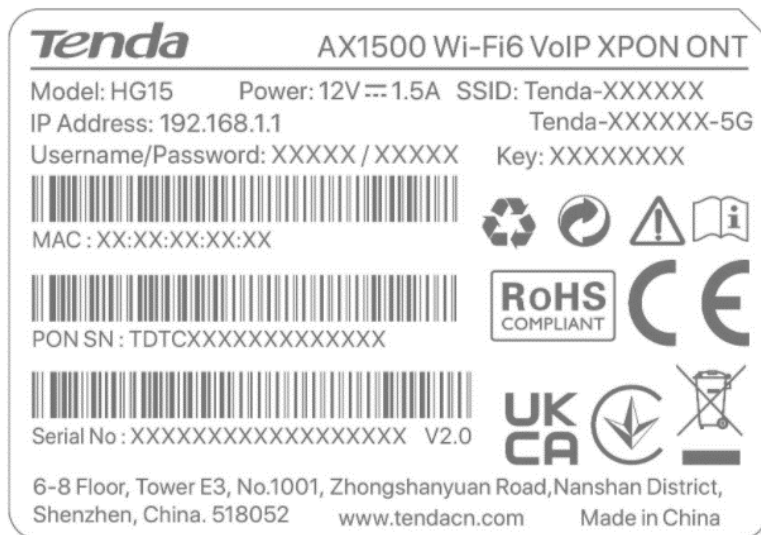
The ports and buttons may vary with models. The actual product prevails.

Port/Button	Description
ON/OFF	Press the button to turn on or turn off the ONT.
PON	Optical fiber port. Used to connect to optical network through an optical fiber cable.
PWR	Used to connect the ONT to a power source using the included power adapter.
USB	USB 2.0 port. Used to connect to a USB storage for resource sharing.
WLAN	Wi-Fi on/off button. Press the button to enable or disable the Wi-Fi function of the ONT.
TEL	Telephone port. Used to connect to a telephone for voice service using a telephone cable.
LAN1-4	Gigabit LAN ports. Used to connect to such devices as routers, switches, computers or IPTV set-top boxes.
WPS/RST	WPS/Reset button. <ul style="list-style-type: none"> WPS: WPS-supported devices can connect to the Wi-Fi networks of the ONT without entering the password through WPS negotiation. Press the button for about 1-3 seconds to start the WPS negotiation process of the ONT. The WPS (marked WLAN/2.4G/5G/WPS) LED indicator blinks quickly. Within 2 minutes, enable the WPS function to establish a WPS connection on a WPS-supported device. For details, see WPS.
	<ul style="list-style-type: none"> Reset: Restore the ONT to the preset configurations or restore the ONT to factory settings. <ul style="list-style-type: none"> For the ONT with the preset configurations: After the ONT completes startup, press the reset button (WPS/RST) for 8 to 20 seconds, and the ONT is restored to the preset configurations. Press the reset button (WPS/RST) for more than 20 seconds, and the ONT is restored to the factory settings. For the ONT without the preset configurations: After the ONT completes startup, press the reset (WPS/RST) button for more than 8 seconds, and the ONT is restored to the factory settings.

Port/Button	Description
LED	LED indicator on/off button. Press the button to turn on or off the LED indicators of the ONT.

1.1.2 Label

The label is located on the body of the ONT. See the following figure for details.



Example: HG15

- **Model:** Model of the ONT
- **Power:** Power supply for the ONT
- **IP Address:** Default IP address used to log in to the web UI of the ONT
- **SSID & Key:** Default Wi-Fi name and password of the ONT
- **Username & Password:** Default user name and password used to log in to the web UI of the ONT
- **MAC:** MAC address of the ONT
- **PON SN:** PON serial number of the ONT
- **Serial No:** Product serial number

2 Web UI

2.1 Login



TIP

A maximum of three users can log in to the web UI at the same time.

Procedure:

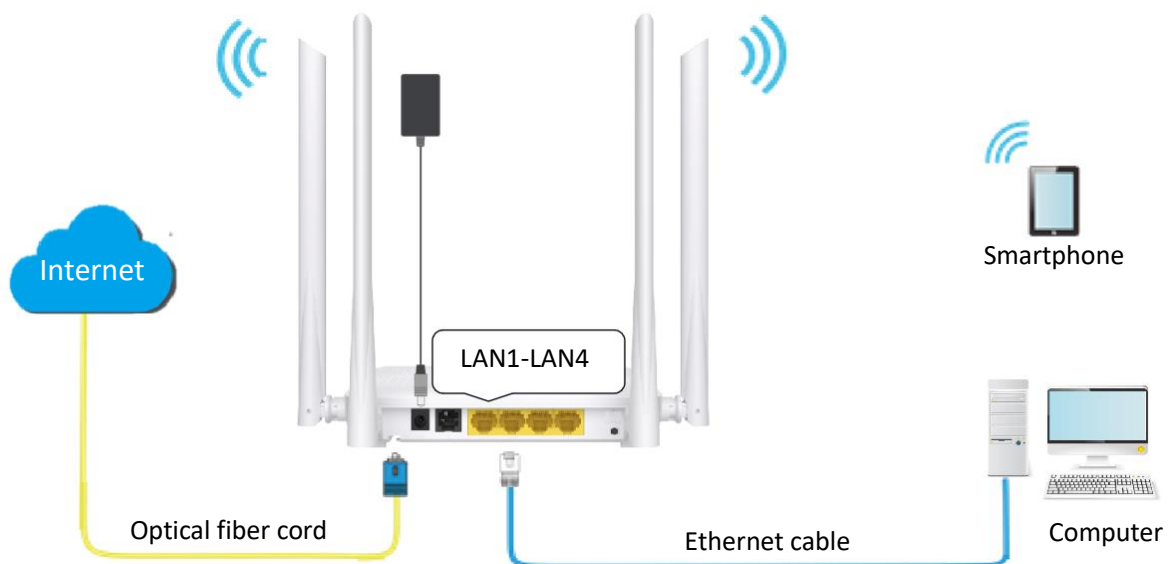
Step 1 Power on the ONT using the included power adapter.



TIP

Some models support **ON/OFF** button. Press **ON/OFF** button (if any) to turn on the ONT.

Step 2 Connect a computer to a LAN port of the ONT using an Ethernet cable, or connect your smartphone to the Wi-Fi network of the ONT.



Step 3 Start a web browser on a connected device and visit the IP address of the ONT (192.168.1.1 by default). Enter your **User Name** and **Password**, and click **Login**.



TIP

You can log in to the web UI of the ONT with user permissions or administrator permissions. Administrator permissions are for the installation and maintenance personnel only. Some functions are available only when you use the administrator permissions to log in to the web UI of the ONT.

- **User Permissions:** Able to view and modify partial configurations of the ONT. The default login user name is **admin**. You can get the password from the bottom label on the ONT.
- **Administrator Permissions:** Able to view and modify all configurations of the ONT. Some configurations changed by the installation and maintenance personnel will affect the normal operation of the ONT. Therefore, use the administrator permissions with caution. The default login user name and password are both **admin** (or **root**).



----End



TIP

If the above page does not appear, try the following solutions:

- Ensure that the ONT is powered on properly.
- If a wired device, such as a computer, is used for configuration, ensure that the wired device is connected to a LAN port of the router properly, and is set to **Obtain an IP address automatically** and **Obtain DNS server address automatically**.
- If a wireless device, such as a smartphone, is used for configuration, ensure that the wireless device is connected to the Wi-Fi network of the ONT and the cellular network (mobile data) of the client is disabled.
- [Restore the ONT to factory settings](#) and try again.

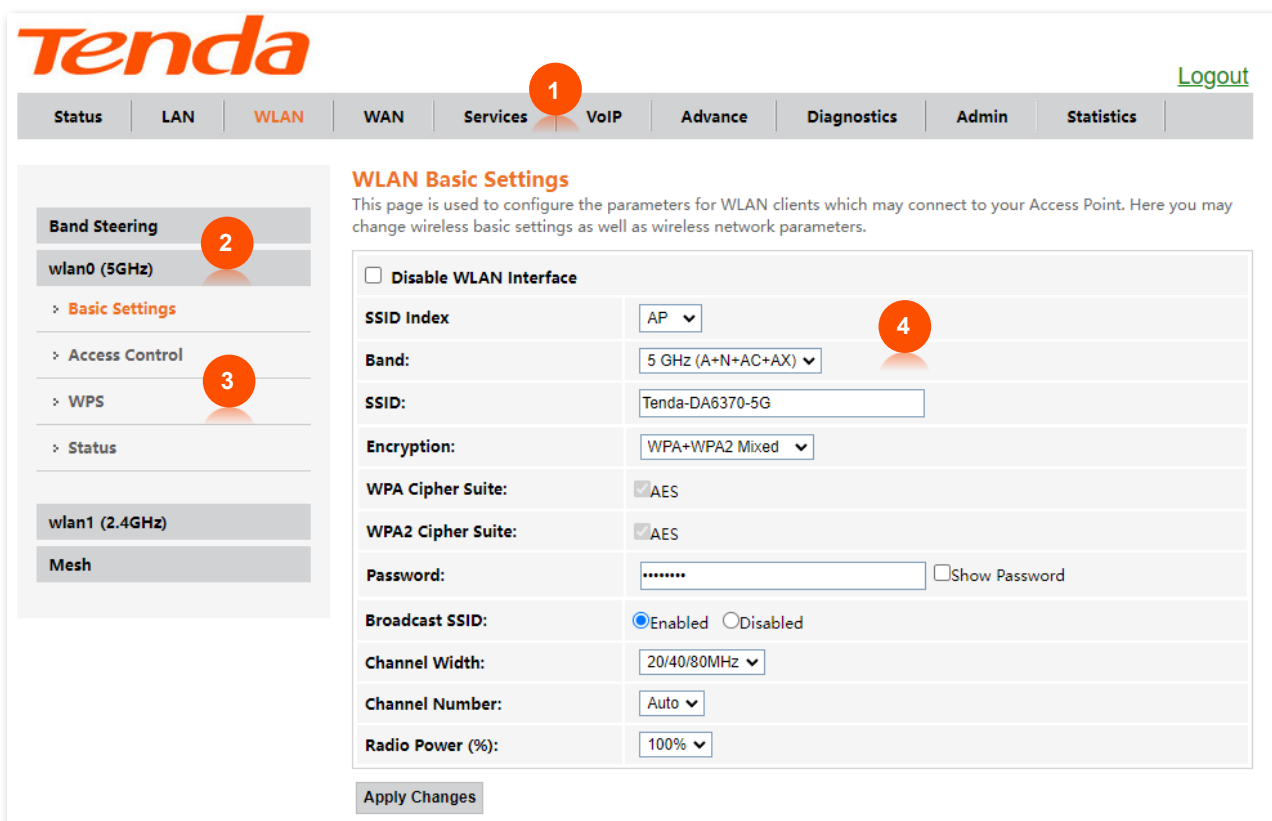
2.2 Logout

The ONT logs you out when you:

- Click the **Logout** button on the upper-right corner of the web UI, or click **Logout** in **Admin > Logout**.
- Perform no operation within the [Auto Logout Time](#).

2.3 Web UI layout

The web UI of the ONT is composed of 4 parts, including the level-1 navigation tree, level-2 navigation tree, level-3 navigation tree and configuration area. See the following figure.



No.	Name	Description
①	Level-1 navigation tree	The navigation trees display the function menu of the ONT. When you select a function in the navigation tree, the configuration of the function appears in the configuration area.
②	Level-2 navigation tree	
③	Level-3 navigation tree	
④	Configuration area	Used to view and modify the configuration.

2.4 Common buttons

Some buttons are commonly used in the web UI of the ONT, and their functions are listed as follows.

Button	Description
Refresh	Used to refresh the statistics shown on the page.
Add	Used to add the rule configured on the page.
Reset	Used to restore the configuration on the page.
Delete	
Delete Selected	Used to delete the rule or configuration on the page.
Delete All	
Modify	Used to modify the configuration on the page.
Remove	Used to remove the rule configured on the page.
Apply	
Apply Changes	Used to apply the settings configured on the page.

3 Quick registration

This guide is for reference only and does not imply that the product supports all functions in the guide. The functions may differ with different product models or different versions of the same model. The actual product prevails.



For initial registration of the ONT, you can register the ONT through the quick registration function with administrator permissions. When all settings are completed, you must click **Apply Changes** for the configurations to take effect. After the ONT is registered successfully, you will be automatically redirected to the web UI of the ONT when the network is detected by the ONT. You can click **Advance** on the upper-right corner of the page to complete related configurations.

3.1 Configure GPON or EPON settings

On this page, you can register your ONT for internet access with the quick registration function.

The ONT may register itself automatically after you connect a fiber cord to it and power it on. If ISP provides any parameters for registration, you can use them manually register the ONT with the quick registration function on this page.

To access the page, [log in to the web UI](#) of the ONT. In the **GPON Settings** (or **EPON Settings**) module, you can enter the parameters provided by your ISP to register the ONT.

GPON Settings	
LOID:	<input type="text"/>
LOID Password:	<input type="password"/>
PLOAM Password:	<input type="password"/>
Serial Number:	<input type="text"/>
OMCI OLT Mode:	Default Mode ▼

You can view the registration status of the ONT on the [PON status](#) page.

Parameter description

Parameter	Description
LOID	Specifies the unique identifier assigned to an ONT by the ISP. LOID is abbreviated for Line Operation Identification, which can be used to identify the ONT.
LOID Password	Specifies the ONT password assigned by the ISP for managing the ONT and authorizing users to access the device.
PLOAM Password	Specifies the password used for authentication between the ONT and the OLT.
Serial Number	Specifies the PON serial number of the ONT.
OMCI OLT Mode	Specifies the OLT manufacturer with which the settings are compatible with. The default mode is recommended.

3.2 Configure INTERNET settings

On this page, you can set up a WAN connection with the quick registration function.

To access the page, [log in to the web UI](#) of the ONT. In the **INTERNET Settings** module, you can set the parameters according to your ISP and your own need.



You can set up WAN connections to access different types of services or a combination of them, including internet, TR069, voice and others. For more information about setting up WAN connections, see [WAN](#).

INTERNET Settings	
VLAN ID:	<input type="text"/>
Service Type:	PPPoE ▼
UserName:	<input type="text"/>
Password:	<input type="password"/> <input type="checkbox"/> Show Password

Parameter description

Parameter	Description
VLAN ID	Specifies the VLAN ID of the WAN connection.

Parameter	Description
Service Type	<p>Specifies the type that you used to set up the WAN connection.</p> <ul style="list-style-type: none"> – IPoE: Select this type when the ONT automatically obtains the IP address from the upstream device or ISP through DHCP without entering the user name and password. – Bridge: Select this type when this device only serves as a modem, and you want to set up a dial-up connection or enter other internet parameters directly on your computer for internet access. – PPPoE: Select this type when your ISP provides a user name and password to you for internet access.
UserName	Specify the PPPoE user name and password provided by your ISP for settings up the WAN connection.
Password	

3.3 Configure Wi-Fi settings

On this page, you can change the Wi-Fi name and the Wi-Fi password with the quick registration function.

To access the page, [log in to the web UI](#) of the ONT. In the **WIFI Settings** module, you can set the parameters as required.

WIFI Settings	
SSID:	<input type="text" value="Tenda-DA6370"/> (2.4GHz and 5GHz will be modified at the same time.)
Pre-Shared Key:	<input type="password" value="*****"/> <input type="checkbox"/> Show Password

Parameter description

Parameter	Description
SSID	Specifies the Wi-Fi name of the Wi-Fi network.
Pre-Shared Key	Specifies the password for connecting to the Wi-Fi network.

4 Status

This guide is for reference only and does not imply that the product supports all functions in the guide. The functions may differ with different product models or different versions of the same model. The actual product prevails.

4.1 ONT status

4.1.1 View device status

On this page, you can view the basic system information, LAN configuration and WAN configuration of the ONT.

To access the page, [log in to the web UI](#) of the ONT and navigate to **Status > Status > Device**.

System									
Device Name			HG15						
Uptime			8 min						
Software Version			v2.0.0						
Hardware Version			v2.0						
Magic Number			300000698						
CPU Usage			1%						
Memory Usage			49%						
DNS Servers									
IPv4 Default Gateway									
IPv6 Default Gateway									
LAN Configuration									
IP Address			192.168.1.1						
Subnet Mask			255.255.255.0						
DHCP Server			Enabled						
MAC Address			<div></div>						
WAN Configuration									
WAN Name	Interface	VLAN ID	MAC	WAN Type	Protocol	IP Address	Gateway	Status	
---	nas0_0	0	<div></div>	INTERNET	Bridged			down	

Parameter description

Parameter		Description
System		Specifies the basic system information of the ONT, including the device name, uptime, software version, hardware version, magic number, CPU usage, memory usage, DNS servers, IPv4 default gateway and IPv6 default gateway.
	IP Address	Specifies the LAN IP address of the ONT, which is also the IP address used to log in to the web UI of the ONT.
LAN Configuration	Subnet Mask	Specifies the LAN subnet mask of the ONT.
	DHCP Server	Specifies whether to enable the DHCP server of the ONT.
	MAC Address	Specifies the MAC address of the ONT's LAN port.
WAN Configuration	WAN Name	Specifies the name of the WAN connection.
	Interface	Specifies the name of the interface or WAN connection when IPv4 is enabled.
	VLAN ID	Specifies the VLAN ID of the WAN connection.
	MAC	Specifies the MAC address automatically generated when WAN connection is created.
	WAN Type	Specifies the WAN connection type.
	Protocol	Specifies the channel mode used by the WAN port.
	IP Address	Specify the IP address and gateway address that the ONT obtains after you set up a WAN connection successfully.
	Gateway	
	Status	Specifies the connection status of the WAN connection.
		<ul style="list-style-type: none"> up: The WAN connection is successful. down: The WAN connection failed and is currently unavailable.

4.1.2 View IPv6 status

On this page, you can view the IPv6 connection status of the ONT.

To access the page, [log in to the web UI](#) of the ONT and navigate to **Status > Status > IPv6**.

LAN Configuration						
IPv6 Address						
IPv6 Link-Local Address		fe80::1/64				
Prefix Delegation						
Prefix						
WAN Configuration						
Interface	VLAN ID	MAC	WAN Type	Protocol	IP Address	Status

Parameter description

Parameter		Description
LAN Configuration	IPv6 Address	Specifies the LAN IPv6 address of the ONT.
	IPv6 Link-Local Address	Specifies the IPv6 link-local address of the ONT. A link-local address is an IPv6 unicast address that is automatically configured on any interface and is valid only for communications within the network segment.
Prefix Delegation	Prefix	Specifies the IPv6 prefix of the LAN port of ONT.
WAN Configuration	Interface	Specifies the name of the interface or WAN when IPv6 is enabled.
	VLAN ID	Specifies the VLAN ID of the WAN connection.
	MAC	Specifies the MAC address automatically generated when WAN connection is created.
	WAN Type	Specifies the WAN connection type.
	Protocol	Specifies the channel mode used by the WAN port.
	IP Address	Specifies the IP address that the ONT obtains after you set up a WAN connection successfully.

Parameter	Description
Status	<p>Specifies the connection status of the WAN connection.</p> <ul style="list-style-type: none"> – up: The WAN connection is successful. – down: The WAN connection failed and is currently unavailable.

4.1.3 View PON status

On this page, you can view the PON status and GPON or EPON connection status of the ONT.

To access the page, [log in to the web UI](#) of the ONT and navigate to **Status > Status > PON**.

PON Status	
Vendor Name	
Temperature	24.886719 C
Voltage	3.244800 V
Tx Power	No signal
Rx Power	No signal
Bias Current	0.000000 mA
GPON Status	
ONU State	O1

Parameter description

Parameter	Description
PON Status	Vendor Name Specifies the vendor name of the ONT.
	Temperature Specifies the current chip temperature of the ONT.
	Voltage Specifies the current voltage of the optical module of the ONT.
	Tx Power Specify the transmitted and received optical power of the ONT over the PON port.
	Rx Power
	Bias Current Specifies the current bias current of the optical module of the ONT.
GPON Status	<p>Specifies the state of the ONT, ranging from O1 to O7.</p> <p>ONU State</p> <ul style="list-style-type: none"> – O1 to O4: The ONT is registering. – O5: The ONT is registered successfully and is under normal operation. – O6/O7: The ONT is in the abnormal state and stops transmitting signals.

Parameter		Description
EPON Status	Auth state	Specifies the state of the ONT, including Unregistered and unauthorized , Registered and certified and Registered and unauthorized .

4.1.4 View LAN port status

On this page, you can view the LAN port status of the ONT.

To access the page, [log in to the web UI](#) of the ONT and navigate to **Status > Status > LAN Port**.

LAN Port Status	
LAN1	not-connected
LAN2	Up, 100Mb, Full
LAN3	not-connected
LAN4	not-connected

4.1.5 View VoIP port status

On this page, you can view the VoIP port status of the ONT.

To access the page, [log in to the web UI](#) of the ONT and navigate to **Status > Status > VOIP Port**.

VoIP Port Status		
Port	Number	Status
1		Disabled

4.2 Device list

4.2.1 View LAN device list

On this page, you can view the LAN device list of the ONT.

To access the page, [log in to the web UI](#) of the ONT and navigate to **Status > Device List > LAN Device List**.

Device Name	MAC Address	IPv4 Address	IPv6 Address
DESKTOP-2K2MLGI		192.168.1.10	fe80::3dc0:354c:3624:b6db

Parameter description

Parameter	Description
Device Name	Specifies the name of device connected to the LAN port of the ONT.
MAC Address	Specifies the MAC address connected to the LAN port of the ONT.
IPv4 Address	Specifies the LAN IPv4 address of the device.
IPv6 Address	Specifies the LAN IPv6 address of the device.

4.2.2 View WLAN device list

On this page, you can view the WLAN device list of the ONT.

To access the page, [log in to the web UI](#) of the ONT and navigate to **Status > Device List > WLAN Device List**.

Device Name	MAC Address	IPv4 Address	IPv6 Address
iQOO-10		192.168.1.2	fe80::309d:2cff:fe07:b582

Parameter description

Parameter	Description
Device Name	Specifies the name of wireless device connected to the ONT.
MAC Address	Specifies the MAC address of the wireless device connected to the ONT.
IPv4 Address	Specifies the IPv4 address of the wireless device connected to the ONT.
IPv6 Address	Specifies the IPv6 address of the wireless device connected to the ONT.

5 LAN

This guide is for reference only and does not imply that the product supports all functions in the guide. The functions may differ with different product models or different versions of the same model. The actual product prevails.

5.1 LAN interface settings

In this module, you can configure the LAN IPv4, IGMP Snooping and MLD Snooping settings of the ONT.

To access the page, [log in to the web UI](#) and navigate to **LAN > LAN > LAN Interface Settings**.

Interface Name:	br0
IP Address:	<input type="text" value="192.168.1.1"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
IGMP Snooping:	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
MLD Snooping:	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled

Parameter description

Parameter	Description
Interface Name	Specifies the LAN interface name of the ONT.
IP Address	Specifies the IPv4 LAN address of the ONT, which is also the IPv4 address for logging in to the web UI of the ONT.
Subnet Mask	Specifies the IPv4 LAN subnet mask of the ONT.
IGMP Snooping	When Internet Group Management Protocol (IGMP) snooping is enabled, multicast data from known IPv4 multicast groups are multicast to the specified LAN ports only, instead of all LAN ports, thus saving link bandwidth. The IGMP Snooping function is enabled by default and cannot be disabled.

Parameter	Description
MLD Snooping	Multicast Listener Discovery (MLD) is a Layer 2 multicast protocol running on IPv6 networks. With MLD snooping enabled, the ONT listens to the multicast conversations and maintains a map of the relationship between links and IP multicast which the link needs. Multicasts may be filtered from the links which do not need them, conserving bandwidth on those links. The MLD Snooping function is enabled by default and cannot be disabled.

5.2 DHCP

5.2.1 Overview

The DHCP server can automatically assign IP addresses, subnet masks, gateway addresses and DNS to LAN clients. When it is disabled, you need to manually configure the IP address information on the LAN device to access the internet. Disable it only when necessary.

To access the page, [log in to the web UI](#) of the ONT and navigate to **LAN > LAN > DHCP**.

DHCP Mode:
☐ NONE
 ☒ DHCP Server

Enable the DHCP Server if you are using this device as a DHCP server. This page lists the IP address pools available to hosts on your LAN. The device distributes numbers in the pool to hosts on your network as they request Internet access.

LAN IP Address: 192.168.1.1 Subnet Mask: 255.255.255.0

IP Pool Range:
 -


Subnet Mask:

Max Lease Time:
 seconds

DNS option:
☒ Use DNS Proxy
 ☐ Set Manually

Parameter description

Parameter	Description
DHCP Mode	Specifies the status of the DHCP server. <ul style="list-style-type: none"> NONE: The DHCP server is disabled. DHCP Server: The DHCP server is enabled.
LAN IP Address	Specifies the current LAN IP address of the ONT, which is also the IP address used to log in to the web UI of the ONT.

Parameter	Description
Subnet Mask	Specifies the current subnet mask of the LAN.
IP Pool Range	Specifies the range of IP addresses that a DHCP server can assign to LAN clients.
Show Client	<p>Specifies the information of the active DHCP clients, including:</p> <ul style="list-style-type: none"> – IP Address: It specifies the IP address assigned to the DHCP leased client. – MAC Address: It specifies the MAC address of the DHCP leased client. – Expired Time (sec): It specifies the time expired for the DHCP leased client.
Subnet Mask	Specifies the subnet mask of the DHCP clients.
Max Lease Time	Specifies the valid time of the IP addresses assigned by the DHCP server of the ONT to the DHCP clients.
DNS option	<p>Specifies how the ONT assigns DNS server addresses to LAN clients.</p> <ul style="list-style-type: none"> – Use DNS Proxy: The ONT forwards the DNS query packets from LAN clients to an external DNS server. – Set Manually: You need to set the DNS server address manually. You can set three DNS servers at most, and at least one is required.
Port-Based Filter	Used to configure the Port-Based Filtering. When the port is selected, it means that the address assigned by the gateway cannot be obtained through DHCP.
MAC-Based Assignment	<p>Used to assign fixed IP addresses to certain LAN clients based on their MAC addresses. Devices with the MAC address connected to the ONT get the same IP address every time.</p> <p> TIP</p> <p>Note the format of the MAC address. Use “-” to separate every two characters in the MAC address.</p>

5.2.2 Reserve IP addresses for certain devices

Scenario: You have an FTP server at home under the LAN of the ONT.

Requirement: You want to visit resources on the FTP server when you are not at home and avoid instability of services resulting from the dynamic IP address assigned by the ONT.

Solution: You can reserve a fixed IP address for the FTP server to reach the requirement.

Assume that:

- Fixed IP address reserved for the FTP server: 192.168.1.136
- MAC address of the FTP server host: D4:61:DA:1B:CD:89

Procedure:

- Step 1** [Log in to the web UI](#) of the ONT.
- Step 2** Navigate to **LAN > LAN > DHCP**.
- Step 3** Click **MAC-Based Assignment**.
- Step 4** Set **MAC Address** in the format of **D4-61-DA-1B-CD-89**.
- Step 5** Enter **192.168.1.136** in **Assigned IP Address**.
- Step 6** Click **Assign IP**.

MAC-Based Assignment

This page is used to configure the static IP base on MAC Address. You can assign/delete the static IP. The Host MAC Address, please input a string with hex number. Such as 00-d0-59-c6-12-43. The Assigned IP Address, please input a string with digit. Such as 192.168.1.100 .

MAC Address (xx-xx-xx-xx-xx-xx):	<input type="text" value="D4-61-DA-1B-CD-89"/>
Assigned IP Address (xxx.xxx.xxx.xxx):	<input type="text" value="192.168.1.136"/>

MAC-Based Assignment Table		
Select	MAC Address	Assigned IP Address

----End

Now you can access resources on the FTP server free from the influence of the dynamic IP address.

6 WLAN

This guide is for reference only and does not imply that the product supports all functions in the guide. The functions may differ with different product models or different versions of the same model. The actual product prevails.

6.1 Band steering

On this page, you can configure the RSSI of the ONT's Wi-Fi network for the band steering.

When this function is enabled, the 2.4 GHz and 5 GHz Wi-Fi networks keep the same SSID and password. Wi-Fi-enabled clients connected to it will use the frequency according to the surrounding environment.

To access the page, [log in to the web UI](#) of the ONT and navigate to **WLAN > Band Steering**.

Band Steering:	<input type="radio"/> Disabled <input checked="" type="radio"/> Enable	
SSID Name:	<input type="text" value="Tenda-DA6370"/>	
Password:	<input type="password" value="....."/>	<input type="checkbox"/> Show Password
2.4GHz to 5GHz WiFi RSSI:	<input type="text" value="-55"/>	(-100-0)
5GHz to 2.4GHz WiFi RSSI:	<input type="text" value="-72"/>	(-100-0)

Parameter description

Parameter	Description
Band Steering	Specifies whether to enable the band steering function.
SSID Name	Specifies the Wi-Fi name (SSID) of the Wi-Fi network.
Password	Specifies the password for connecting to the Wi-Fi network.
2.4GHz to 5GHz WiFi RSSI	Specifies the signal strength of switching 2.4 GHz to 5 GHz Wi-Fi networks.
5GHz to 2.4GHz WiFi RSSI	Specifies the signal strength of switching 5 GHz to 2.4 GHz Wi-Fi networks.

6.2 Basic settings

6.2.1 Overview



- WLAN settings are only available on ONTs with the wireless function. The dual-band ONT supports both 2.4 GHz and 5 GHz, and the single-band ONT supports 2.4 GHz.
- WLAN (2.4 GHz) and WLAN (5 GHz) configurations are similar. WLAN (2.4 GHz) is used for illustration in this part.

On this page, you can set basic parameters of the Wi-Fi network of the ONT, such as enabling or disabling the Wi-Fi network, setting band and SSID (Wi-Fi name). You can also set password to secure your Wi-Fi network.

To access the page, [log in to the web UI](#) of the ONT and navigate to **WLAN > wlan1 (2.4 GHz) > Basic Settings**.


<input type="checkbox"/> Disable WLAN Interface	
SSID Index	AP ▼
Band:	2.4 GHz (B+G+N) ▼
SSID:	Tenda-DA6370
Encryption:	WPA+WPA2 Mixed ▼
WPA Cipher Suite:	<input checked="" type="checkbox"/> AES
WPA2 Cipher Suite:	<input checked="" type="checkbox"/> AES
Password: <input type="checkbox"/> Show Password
Broadcast SSID:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Channel Width:	40MHz ▼
Channel Number:	Auto ▼
Radio Power (%):	100% ▼

Parameter description

Parameter	Description
Disable WLAN Interface	Specifies whether to disable the Wi-Fi network.
SSID Index	Used to select the corresponding SSID to configure the parameters. AP is the primary SSID.

Parameter	Description
Band	Specifies the wireless band and protocol of the Wi-Fi network.
	<ul style="list-style-type: none"> - 2.4 GHz (B): In this mode, the 2.4 GHz wireless devices compliant with IEEE 802.11b protocol can connect to the 2.4 GHz wireless network of the ONT. The maximum wireless rate is 11 Mbps.
	<ul style="list-style-type: none"> - 2.4 GHz (G): In this mode, the 2.4 GHz wireless devices compliant with IEEE 802.11g protocol can connect to the 2.4 GHz wireless network of the ONT. The maximum wireless rate is 54 Mbps.
	<ul style="list-style-type: none"> - 2.4 GHz (B+G): In this mode, the 2.4 GHz wireless devices compliant with IEEE 802.11b or IEEE 802.11g protocol can connect to the 2.4 GHz wireless network of the ONT.
	<ul style="list-style-type: none"> - 2.4 GHz (N): In this mode, the 2.4 GHz wireless devices compliant with IEEE 802.11n protocol can connect to the 2.4 GHz wireless network of the ONT. The maximum wireless rate is 300 Mbps.
	<ul style="list-style-type: none"> - 2.4 GHz (G+N): In this mode, the 2.4 GHz wireless devices compliant with IEEE 802.11g or IEEE 802.11n protocol can connect to the 2.4 GHz wireless network of the ONT.
	<ul style="list-style-type: none"> - 2.4 GHz (B+G+N): In this mode, the 2.4 GHz wireless devices compliant with IEEE 802.11b, IEEE 802.11g or IEEE 802.11n protocol can connect to the 2.4 GHz wireless network of the ONT.
	<ul style="list-style-type: none"> - 5 GHz (A): In this mode, the 5 GHz wireless devices compliant with IEEE 802.11a protocol can connect to the 5 GHz wireless network of the ONT. The maximum wireless rate is 54 Mbps.
	<ul style="list-style-type: none"> - 5 GHz (N): In this mode, the 5 GHz wireless devices compliant with IEEE 802.11n protocol can connect to the 5 GHz wireless network of the ONT. The maximum wireless rate is 300 Mbps.
	<ul style="list-style-type: none"> - 5 GHz (A+N): In this mode, the 5 GHz wireless devices compliant with IEEE 802.11a or IEEE 802.11n protocol can connect to the 5 GHz wireless network of the ONT.
	<ul style="list-style-type: none"> - 5 GHz (AC): In this mode, the 5 GHz wireless devices compliant with IEEE 802.11ac protocol can connect to the 5 GHz wireless network of the ONT. The maximum wireless rate is 867 Mbps.
	<ul style="list-style-type: none"> - 5 GHz (N+AC): In this mode, the 5 GHz wireless devices compliant with IEEE 802.11n or IEEE 802.11ac protocol can connect to the 5 GHz wireless network of the ONT.
	<ul style="list-style-type: none"> - 5 GHz (A+N+AC): In this mode, the 5 GHz wireless devices compliant with IEEE 802.11a, IEEE 802.11n or IEEE 802.11ac protocol can connect to the 5 GHz wireless network of the ONT.
	<ul style="list-style-type: none"> - 5 GHz (AX): In this mode, the 5 GHz wireless devices compliant with IEEE 802.11ax protocol can connect to the 5 GHz wireless network of the ONT.
	<ul style="list-style-type: none"> - 5 GHz (AC+AX): In this mode, the 5 GHz wireless devices compliant with IEEE 802.11ac or IEEE 802.11ax protocol can connect to the 5 GHz wireless network of the ONT.
	<ul style="list-style-type: none"> - 5 GHz (N+AC+AX): In this mode, the 5 GHz wireless devices compliant with IEEE 802.11n, IEEE 802.11ac or IEEE 802.11ax protocol can connect to the 5 GHz wireless network of the ONT.
	<ul style="list-style-type: none"> - 5 GHz (A+N+AC+AX): In this mode, the 5 GHz wireless devices compliant with IEEE 802.11a, IEEE 802.11n, IEEE 802.11ac or IEEE 802.11ax protocol can connect to the 5 GHz wireless network of the ONT.

Parameter	Description
SSID	Specifies the Wi-Fi name of the Wi-Fi network.
Encryption	<p>Specifies the encryption mode of the Wi-Fi network.</p> <ul style="list-style-type: none"> – NONE: It specifies that the Wi-Fi network is not encrypted and clients can connect to it without password. – WPA: The wireless network adopts the WPA security mode, which has better compatibility. – WPA2: The wireless network adopts the WPA2 security mode, which has a higher security level. – WPA+WPA2 Mixed: Compatible with WPA and WPA2. At this time, wireless devices can connect to the corresponding wireless network using both WPA and WPA2. – WPA3: The wireless network adopts the WPA3 security mode, which is an upgraded version of WPA2. – WPA2+WPA3 Mixed: Compatible with WPA2 and WPA3. At this time, wireless devices can connect to the corresponding wireless network using both WPA2 and WPA3.
WPA Cipher Suite	Specify the encryption algorithm used for WPA. Advanced Encryption Standard (AES) is selected by default. When selected, clients adopting the corresponding encryption algorithm can connect to the Wi-Fi network.
WPA2 Cipher Suite	
Password	Specifies the password for connecting to the Wi-Fi network.
Broadcast SSID	<p>Specifies whether to hide the SSID of the Wi-Fi network.</p> <ul style="list-style-type: none"> – Enabled means that the SSID is displayed. – Disabled means that the SSID is hidden, and you need to enter the SSID of the Wi-Fi network manually to connect to it.
Channel Width	<p>Specifies the bandwidth of the wireless channel of the Wi-Fi network.</p> <ul style="list-style-type: none"> – 20MHz: It specifies that the channel bandwidth used by the ONT is 20 MHz. – 40MHz: It specifies that the channel bandwidth used by the ONT is 40 MHz. – 20/40MHz: It specifies that the ONT can switch its channel bandwidth between 20 MHz and 40 MHz based on the ambient environment. – 80MHz: It specifies that the channel bandwidth used by the ONT is 80 MHz. This option is available only at 5 GHz. – 20/40/80MHz: It specifies that the ONT can switch its channel bandwidth among 20 MHz, 40 MHz and 80 MHz based on the ambient environment. This option is available only at 5 GHz.

Parameter	Description
Channel Number	Specifies the channel in which the Wi-Fi network works.
	You are recommended to choose a channel with less interference for better wireless transmission efficiency. You can use a third-party tool to scan the Wi-Fi signals nearby to understand the channel usage situations.
	Auto: It specifies that the ONT automatically adjusts its operating channel according to the ambient environment.
	 TIP Some models support Auto (DFS) . With this function enabled, the ONT will automatically detect the frequency of the radar system. When the ONT detects radar signals in the same frequency as the ONT itself, the ONT will automatically switch to another frequency to avoid interference with the radar system.
Radio Power (%)	You can set the intensity of the radio power of the ONT. A higher radio power brings a wider coverage of Wi-Fi coverage.

6.2.2 Customize the SSID (Wi-Fi name)

- Step 1** [Log in to the web UI](#) of the ONT.
- Step 2** Navigate to **WLAN > wlan1 (2.4 GHz) > Basic Settings**.
- Step 3** Select SSID (Wi-Fi name) for which you want to customize the Wi-Fi name in **SSID Index**.
- Step 4** Set **SSID**.
- Step 5** Click **Apply Changes**.

☐ **Disable WLAN Interface**

SSID Index *	AP ▼
Band:	2.4 GHz (B+G+N) ▼
SSID: *	Tenda-DA6370
Encryption:	WPA+WPA2 Mixed ▼
WPA Cipher Suite:	<input checked="" type="checkbox"/> AES
WPA2 Cipher Suite:	<input checked="" type="checkbox"/> AES
Password:	<input type="password" value="....."/> <input type="checkbox"/> Show Password
Broadcast SSID:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Channel Width:	40MHz ▼
Channel Number:	Auto ▼
Radio Power (%):	100% ▼

---End

After completing the configuration, you can search the SSID on your Wi-Fi-enabled devices and connect to it to access the internet.

6.2.3 Hide the SSID (Wi-Fi name)



TIP

If the Broadcast SSID function is disabled, the WPS function is also disabled.

- Step 1** [Log in to the web UI](#) of the ONT.
- Step 2** Navigate to **WLAN > wlan1 (2.4 GHz) > Basic Settings**.
- Step 3** Select SSID (Wi-Fi name) for which you want to hide the Wi-Fi name in **SSID Index**.
- Step 4** Select **Disabled** for **Broadcast SSID**.

<input type="checkbox"/> Disable WLAN Interface	
SSID Index *	AP ▼
Band:	2.4 GHz (B+G+N) ▼
SSID:	Tenda-DA6370
Encryption:	WPA+WPA2 Mixed ▼
WPA Cipher Suite:	<input checked="" type="checkbox"/> AES
WPA2 Cipher Suite:	<input checked="" type="checkbox"/> AES
Password: <input type="checkbox"/> Show Password
Broadcast SSID: *	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Channel Width:	40MHz ▼
Channel Number:	Auto ▼
Radio Power (%):	100% ▼

- Step 5** Click **Apply Changes**.

---End

After the configuration is completed, the SSID (Wi-Fi name) of the 2.4 GHz network is hidden, but you can connect to the Wi-Fi network by entering its SSID and other required parameters.

6.2.4 Customize the Wi-Fi password

- Step 1** [Log in to the web UI](#) of the ONT.
- Step 2** Navigate to **WLAN > wlan1 (2.4 GHz) > Basic Settings**.
- Step 3** Select SSID (Wi-Fi name) for which you want to customize the password in **SSID Index**.
- Step 4** Set **Encryption** as required.
- Step 5** Set the other parameters related to password as required.
- Step 6** Enter the Wi-Fi password in **Password**.

<input type="checkbox"/> Disable WLAN Interface	
SSID Index	AP ▼
Band:	2.4 GHz (B+G+N) ▼
SSID:	Tenda-DA6370
Encryption:	WPA+WPA2 Mixed ▼
WPA Cipher Suite:	<input checked="" type="checkbox"/> AES
WPA2 Cipher Suite:	<input checked="" type="checkbox"/> AES
Password: <input type="checkbox"/> Show Password
Broadcast SSID:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Channel Width:	40MHz ▼
Channel Number:	Auto ▼
Radio Power (%):	100% ▼

- Step 7** (Optional) Repeat **Step 2** to **Step 6** to set the Wi-Fi password for other SSIDs.
- Step 8** Click **Apply Changes**.

---End

After the configuration is completed, you can connect the Wi-Fi networks using the Wi-Fi password you set.

6.3 Access control

6.3.1 Overview

On this page, you can add and delete access control rules to decide which clients can connect to all the Wi-Fi networks in the frequency band.

To access the page, [log in to the web UI](#) of the ONT and navigate to **WLAN > wlan1 (2.4 GHz) > Access Control**. Rules added are shown in **Current Access Control List**.

Mode:	Allow List ▼	Apply Changes
MAC Address:	<input type="text"/>	(ex. 00E086710502)
Add	Reset	
Current Access Control List		
MAC Address		Select

Parameter description

Parameter	Description
Mode	<p>Specifies the control mode of the client.</p> <ul style="list-style-type: none"> – Disabled: It specifies that the access control function is disabled. – Allow List: It specifies that only clients with the MAC addresses added to the list can connect to the Wi-Fi network. – Deny List: It specifies that clients with the MAC addresses added to the list cannot connect to the Wi-Fi network.
MAC Address	Specifies the MAC address of the client to be controlled.

6.3.2 Allow certain clients to access the Wi-Fi network

Assume that you only want to enable a smartphone and a tablet to access your Wi-Fi network and prevent misuse by others. The MAC addresses of smartphone and tablet are:

- Smartphone: 8E:5B:54:F6:E1:00
- Tablet: 8C:EC:4B:B3:04:92

Procedure:

Step 1 [Log in to the web UI](#) of the ONT.

Step 2 Navigate to **WLAN > wlan1 (2.4 GHz) > Access Control**.

Step 3 Select **Allow List** for **Mode**, and click **Apply Changes**.

Step 4 Enter **8E5B54F6E100** in **MAC Address**, and click **Add**.

Mode:	Allow List ▼	Apply Changes
MAC Address:	8E5B54F6E100 (ex. 00E086710502)	
Add	Reset	

Step 5 Repeat **Step 4** to add the MAC Address of the tablet.

---End

After the configuration is completed, the added devices are listed in **Current Access Control List**, and only the smartphone and tablet can connect to the Wi-Fi network.

Current Access Control List	
MAC Address	Select
8e:5b:54:f6:e1:00	<input type="checkbox"/>
8c:ec:4b:b3:04:92	<input type="checkbox"/>



If the MAC address of a device is added in the **Deny List** mode, the device will fail to access the Wi-Fi network and a message indicating incorrect password will be displayed on the device.

6.4 WPS

6.4.1 Overview

The Wi-Fi Protected Setup (WPS) function enables wireless clients that support WPS, such as smartphones, to connect to the Wi-Fi network of the ONT quickly and easily.

There are four methods to connect to the Wi-Fi network of the ONT through WPS.

- [Connect to the Wi-Fi network using the WPS/RST button](#)
- [Connect to the Wi-Fi network using PBC on the web UI](#)
- [Connect to the Wi-Fi network by entering PIN code of clients on the ONT](#)
- [Connect to the Wi-Fi network by entering PIN code of the ONT on clients](#)


The WPS function can also be used to network the ONT with devices that support the standard Mesh function using the following two methods:

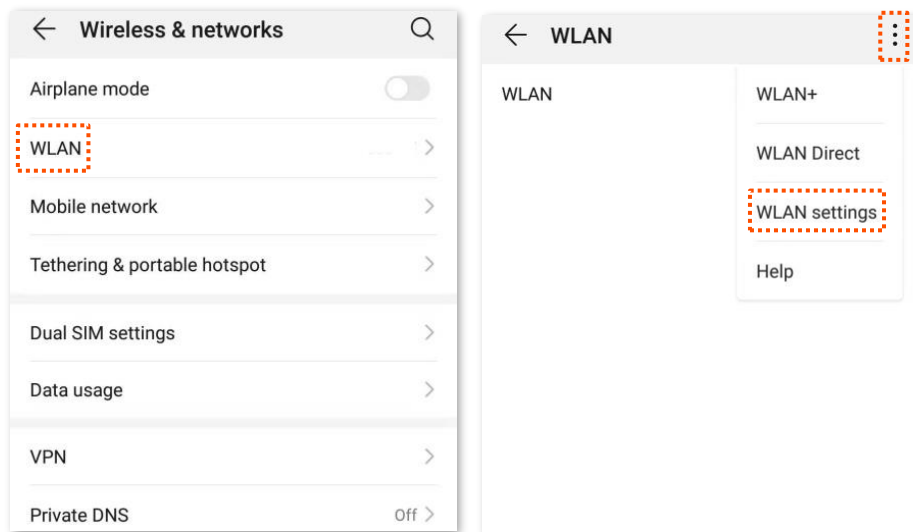
- [Network Mesh devices using the WPS/RST button](#)
- [Network Mesh devices using PBC on the web UI](#)

6.4.2 Connect to the Wi-Fi network

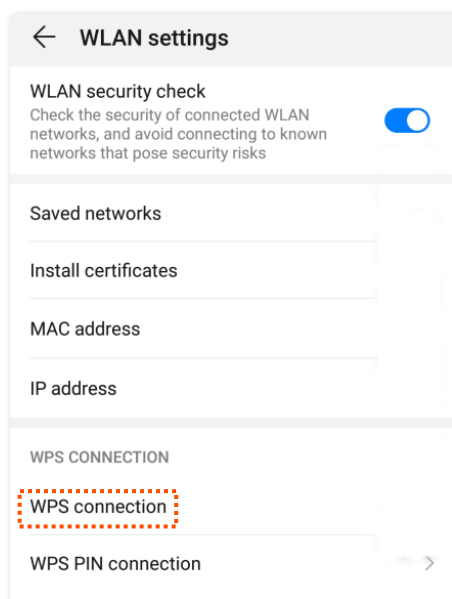
Connect to the Wi-Fi network using the WPS/RST button

- Step 1** Find the **WPS/RST** button on the ONT. Press it for 1 to 3 seconds and you can see the WPS (marked **WLAN/2.4G/5G/WPS**) LED indicator blinks.
- Step 2** Configure the WPS function on your wireless devices **within 2 minutes**. Configuration on various devices may differ (Example: HUAWEI P10 smartphone).
1. Find **Settings** on the smartphone.
 2. Choose **WLAN**.

3. Tap , and choose **WLAN settings**.



4. Choose **WPS connection**.



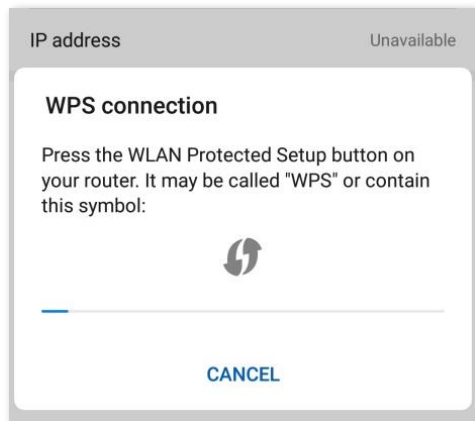
---End

Wait a moment until the WPS negotiation is completed, and the smartphone is connected to the Wi-Fi network.



TIP

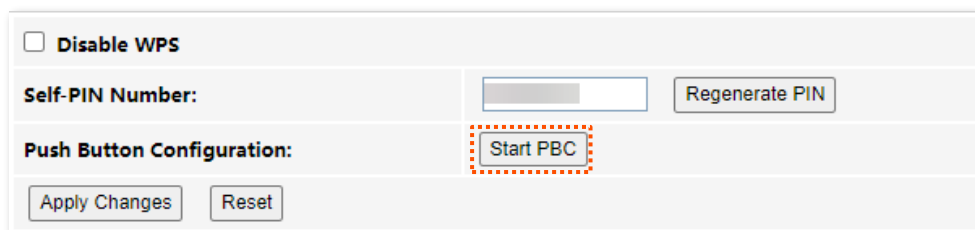
- If multiple wireless networks are enabled in a frequency band, the main network is connected by default.
- To use the WPS function, the encryption mode of the wireless network must be not encrypted, WAP2 or encryption contains WPA2.



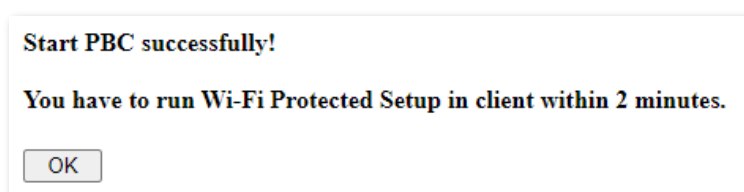
Connect to the Wi-Fi network using PBC on the web UI

Step 1 Get the ONT ready for WPS negotiation.

1. [Log in to the web UI](#) of the ONT.
2. Navigate to **WLAN > wlan1 (2.4GHz) > WPS**.
3. Click **Start PBC**.




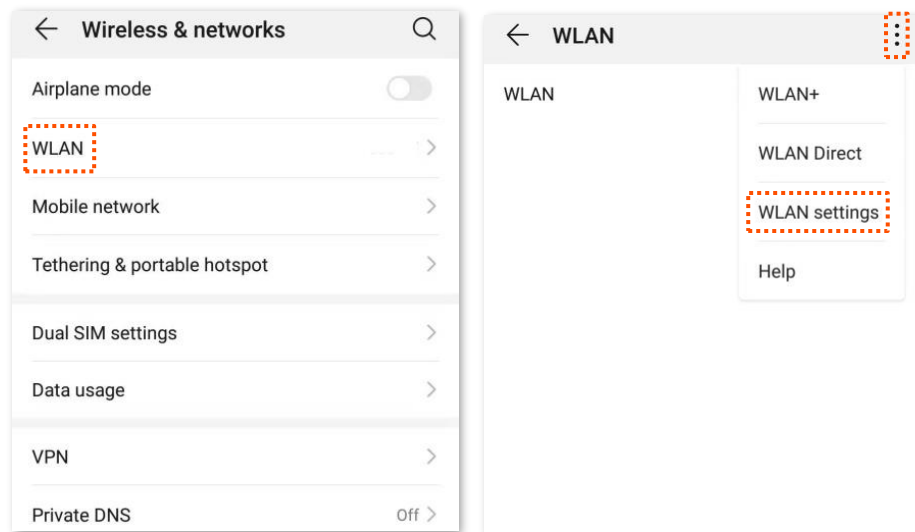
If the following message is displayed, the PBC is started successfully.



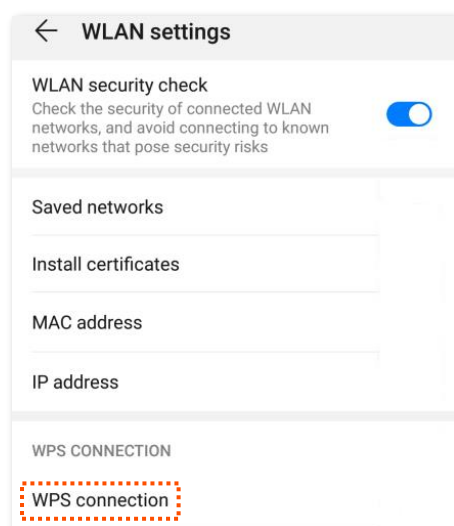
Step 2 Configure the WPS function on your wireless devices **within 2 minutes**. Configuration on various devices may differ (Example: HUAWEI P10 smartphone).

1. Find **Settings** on the smartphone.
2. Choose **WLAN**.

3. Tap , and choose **WLAN settings**.



4. Choose **WPS connection**.



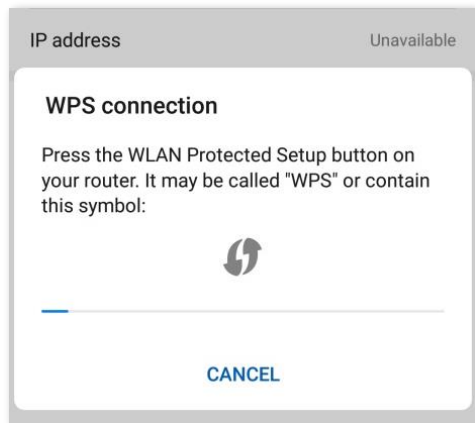
---End

Wait a moment until the WPS negotiation is completed, and the smartphone is connected to the Wi-Fi network.



TIP

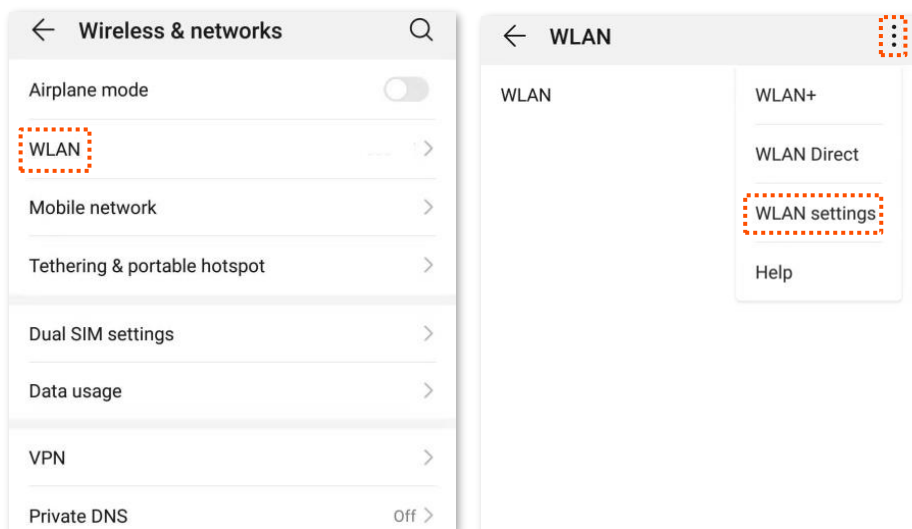
- If multiple wireless networks are enabled in a frequency band, the main network is connected by default.
- To use the WPS function, the encryption mode of the wireless network must be not encrypted, WAP2 or encryption contains WPA2.



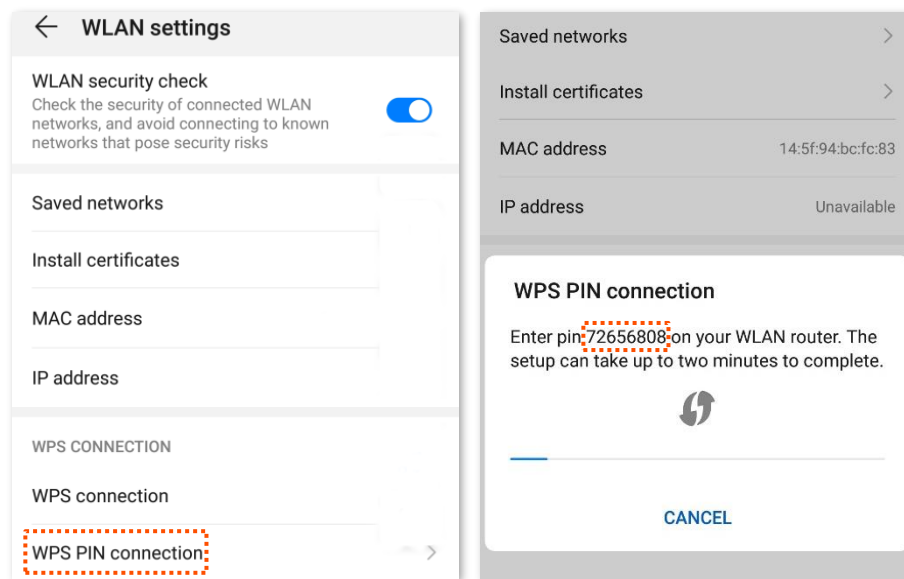
Connect to the Wi-Fi network by entering PIN code of clients on the ONT

Step 1 Find the PIN code of the client. (The method differs with devices. HUAWEI P10 smartphone is used for illustration here.)

1. Find **Settings** on the smartphone.
2. Choose **WLAN**.
3. Tap **:**, and choose **WLAN settings**.



4. Choose **WPS PIN connection**, and record the PIN code of the client.



Step 2 Start WPS connection on the ONT.

1. [Log in to the web UI](#) of the ONT.
2. Navigate to **WLAN > wlan1 (2.4 GHz) > WPS**.
3. Enter the PIN code in **Client PIN Number** and click **Start PIN**.

---End

After the ONT and the client finish WPS negotiation, the client connects to the Wi-Fi network of the ONT successfully.



- If multiple wireless networks are enabled in a frequency band, the main network is connected by default.
- To use the WPS function, the encryption mode of the wireless network must be not encrypted, WAP2 or encryption contains WPA2.

Connect to the Wi-Fi network by entering PIN code of the ONT on clients



TIP

This method is usually used on Wi-Fi network adapters. Refer to the user guide of the Wi-Fi network adapter for configuration details.

Step 1 [Log in to the web UI](#) of the ONT.

Step 2 Navigate to **WLAN > wlan1 (2.4GHz) > WPS**. Find and record the **Self-PIN Number** of the ONT.

<input type="checkbox"/> Disable WPS	
Self-PIN Number:	<input type="text"/> Regenerate PIN
Push Button Configuration:	Start PBC

Step 3 Enter the PIN code on the wireless device that supports WPS connection using PIN code.

---End

Wait a moment until the WPS negotiation is completed, and the wireless device is connected to the Wi-Fi network.



TIP

- If multiple wireless networks are enabled in a frequency band, the main network is connected by default.
- To use the WPS function, the encryption mode of the wireless network must be not encrypted, WAP2 or encryption contains WPA2.

6.4.3 Network Mesh devices



- The ONT with the [Mesh function enabled](#) can work only as the primary node (controller) to network with devices that support the Mesh protocol. Mesh protocol includes [EasyMesh](#) and [Xmesh](#). EasyMesh function and Xmesh function cannot be configured at the same time.
- Do not disable the Wi-Fi function after the Mesh networking is completed successfully. Otherwise, the Mesh networking will fail.
- A maximum of eight secondary nodes (Mesh devices) can be connected to the Mesh network.
- If you want to network multiple devices, network them one by one.

Network Mesh devices using the WPS/RST button

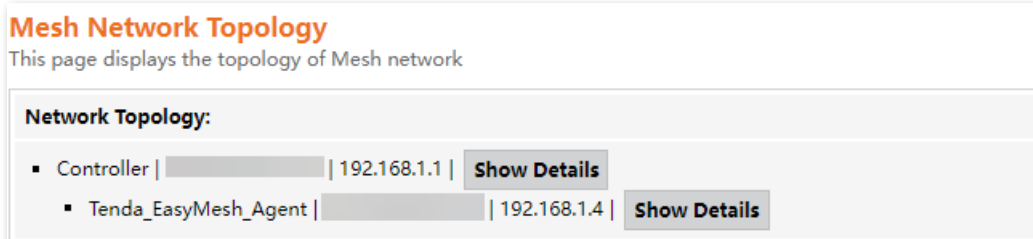
Step 1 Hold down the **WPS/RST** button of the ONT using a needle-like item (such as a pin) for about 1-3 seconds, and you can see the WPS (marked **WLAN/2.4G/5G/WPS**) LED indicator blinks.

The Mesh networking function of the ONT is enabled, which can connect to other Mesh devices for networking.

Step 2 **Within 2 minutes**, hold down the Mesh button of the Mesh device (as a secondary node) to be networked, and the Mesh device will negotiate with the ONT for Mesh networking. For more details, refer to the user guide of the corresponding Mesh device.

---End

Wait a moment and navigate to **WLAN > Mesh > Topology**. If the corresponding Mesh agent is displayed on the page, the Mesh device is networked successfully. For details, see [Mesh](#).



Network Mesh devices using PBC on the web UI

Step 1 Get the ONT ready for Mesh networking.

1. [Log in to the web UI](#) of the ONT.
2. Navigate to **WLAN > wlan1 (2.4GHz) > WPS**.

3. Click **Start PBC**.

☐ **Disable WPS**

Self-PIN Number: **Regenerate PIN**

Push Button Configuration: **Start PBC**

Apply Changes **Reset**

If the following message is displayed, the PBC is started successfully.

Start PBC successfully!

You have to run Wi-Fi Protected Setup in client within 2 minutes.

OK

Step 2 **Within 2 minutes**, hold down the Mesh button of the Mesh device (as a secondary node) to be networked, and the Mesh device will negotiate with the ONT for Mesh networking. For more details, refer to the user guide of the corresponding Mesh device.

---End

Wait a moment and navigate to **WLAN > Mesh > Topology**. If the corresponding Mesh agent is displayed on the page, the Mesh device is networked successfully. For details, see [Mesh](#).

Mesh Network Topology
This page displays the topology of Mesh network

Network Topology:

- Controller | 192.168.1.1 | **Show Details**
- Tenda_EasyMesh_Agent | 192.168.1.4 | **Show Details**


6.5 Status

On this page, you can check the information and status of the Wi-Fi network you set up, including those virtual AP Wi-Fi networks.

To access the page, [log in to the web UI](#) of the ONT and navigate to **WLAN > wlan1 (2.4 GHz) > Status**.

WLAN Configuration	
Mode	AP
Band	2.4 GHz (B+G+N)
SSID	Tenda-DA6370
Channel Number	1
Encryption	WPA2 Mixed
BSSID	c8:3a:35:da:63:77
Associated Clients	1 show client

Parameter description

Parameter	Description
Mode	Specifies the mode of the Wi-Fi network.
Band	Specifies the wireless band and protocol of the Wi-Fi network.
SSID	<p>Specifies the Wi-Fi name of the Wi-Fi network.</p> <p> TIP</p> <p>The SSID of Virtual AP1 (used for Mesh networking) is hidden.</p>
Channel Number	Specifies the channel in which the Wi-Fi network works.
Encryption	Specifies the encryption mode of the Wi-Fi network.
BSSID	Basic Service Set Identifier (BSSID) is used to describe sections of a wireless local area network. This service set is the MAC address of the AP's radio for clients to identify and connect to.
Associated Clients	Specifies the number of connected clients.

Parameter	Description
You can view the clients that connect to the Wi-Fi network by clicking show clients .	
show client	– MAC Address: It specifies the MAC address of the client connected to the Wi-Fi network.
	– Tx Packets: It specifies the number of transmitted packets of the client through the Wi-Fi network.
	– Rx Packets: It specifies the number of received packets of the client through the Wi-Fi network.
	– Tx Rate (Mbps): It specifies the transmitting rate of the Wi-Fi network.
	– RSSI: It specifies the signal strength of the client received by the AP.

6.6 Mesh

6.6.1 Mesh Interface Setup



- The ONT with the Mesh function enabled can work only as the primary node (controller) to network with devices that support the standard Mesh protocol. Mesh protocol includes [EasyMesh](#) and [Xmesh](#). EasyMesh and Xmesh function cannot be configured at the same time.
- Do not disable the Wi-Fi function after the Mesh networking is completed successfully. Otherwise, the Mesh networking will fail.
- A maximum of eight secondary nodes (Mesh devices) can be connected in the Mesh network.
- If you want to network multiple devices, network them one by one.

On this page, you can enable or disable the Mesh function, and set the Mesh mode and device name when the Mesh function is enabled. By default, the Mesh function is enabled and the role of the ONT is fixed to controller. For details, see [Network Mesh devices using the WPS/RST button](#) and [Network Mesh devices using PBC on the web UI](#).

To access the page, [log in to the web UI](#) of the ONT and navigate to **WLAN > Mesh > Mesh Interface Setup**.

<input type="checkbox"/> Disable Mesh	
Mesh Mode:	EasyMesh ▼
Device Name:	Controller
Role:	<input checked="" type="radio"/> Controller

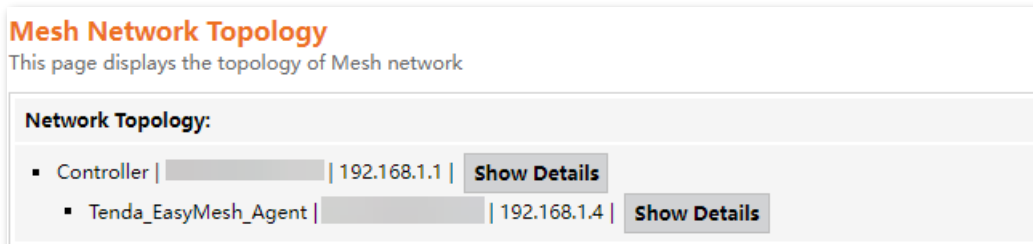
Parameter description

Parameter	Description
Disable Mesh	Specifies whether the Mesh function is enabled. It is enabled by default.
Mesh Mode	<p>Specifies the Mesh mode of the ONT, including EasyMesh and Xmesh.</p> <ul style="list-style-type: none"> • EasyMesh: It indicates a public authentication protocol. If the EasyMesh standard followed by the router and ONT is consistent, networking can be performed. • Xmesh: It is defined by Tenda, and can only be used with specific Tenda routers for networking. The actual Tenda routers prevail.
Device Name	Specifies the name of the controller, that is, the ONT.
Role	Specifies the role of the ONT in the Mesh network. It is fixed to Controller and cannot be modified.
Steerd	Specifies whether the frequency band roaming function is enabled when Xmesh is selected. After the function is enabled, the ONT will automatically connect to the better frequency band roaming to realize the conversion between 2.4G roaming and 5G roaming. It is disabled by default.

6.6.2 Topology

On this page, you can see the information of all nodes in the Mesh network, including the node role, MAC address and IP address.

To access the page, [log in to the web UI](#) of the ONT and navigate to **WLAN > Mesh > Topology**.



For more details, click **Show Details**. The following page is displayed.

Mesh Device Details Table

This table shows the details of individual Mesh device in the network, child neighbor list and associated station list.

Neighbor RSSI (excluding parent AP):

MAC Address	Name	RSSI	Connected Band
	Tenda_EasyMesh_Agent	-10 dBm	5G

Station Info:

MAC Address	RSSI	Connected Band	Downlink	Uplink
	-35 dBm	2.4G	81	1

Parameter description

Parameter		Description
Neighbor RSSI (excluding parent AP)	MAC Address	Specifies the MAC address of the Mesh device networked with the current node.
	Name	Specifies the name of the Mesh device networked with the current node.
	RSSI	Specifies the signal strength of the Mesh device networked with the current node.
	Connected Band	Specifies the band used for networking between the Mesh device and the current node.
Station Info	MAC Address	Specifies the MAC address of the station (such as a smartphone) connected to the current node.
	RSSI	Specifies the signal strength of the station (such as a smartphone) connected to the current node.
	Connected Band	Specifies the band used for networking between the client (such as a smartphone) and the current node.
	Downlink	Specifies the current download speed of the client (such as a smartphone) connected to the current node.
	Uplink	Specifies the current upload speed of the client (such as a smartphone) connected to the current node.

6.6.3 Xmesh blacklist

On this page, you can set access control rules to blacklist clients in the 2.4 GHz and 5 GHz frequency band when the Xmesh function is enabled.

To access the page, [log in to the web UI](#) of the ONT and navigate to **WLAN > Mesh > Access Control**.

Current Access Control List		
Mode	MAC Address	Select

Parameter description

Parameter	Description
MAC Address	Specifies the MAC address of the client to be blacklisted.
Mode	Specifies the control mode of the client. It is Deny by default, which means that clients with the MAC addresses added to the list cannot connect to the Wi-Fi network.

Add Xmesh blacklist

Assume that you want to add the wireless client (smartphone as example) to the blacklist in the 2.4 GHz and 5 GHz frequency bands when the Xmesh function is enabled. The MAC address of smartphone is 8E:5B:54:F6:E1:00.

Procedure:

Step 1 [Log in to the web UI](#) of the ONT.

Step 2 Navigate to **WLAN > Mesh > Access Control**.

Step 3 Enter **8E5B54F6E100** in **MAC Address**, and click **Add**.

Step 4 Confirm the prompt information, and click **OK**.

---End

After the configuration is completed, the added devices are listed in **Current Access Control List**, and the smartphone cannot connect to the Wi-Fi network.

Current Access Control List		
Mode	MAC Address	Select
Deny	8e:5b:54:f6:e1:00	<input type="checkbox"/>

Delete Xmesh blacklist

Assume that you want to remove the wireless client (smartphone as example) from the blacklist in the 2.4 GHz and 5 GHz frequency band when the Xmesh function is enabled. The MAC address of smartphone is 8E:5B:54:F6:E1:00.

Procedure:

- Step 1** [Log in to the web UI](#) of the ONT.
- Step 2** Navigate to **WLAN > Mesh > Access Control**.
- Step 3** Select the added device to remove from the blacklist as required, and click **Delete Selected**.

Current Access Control List		
Mode	MAC Address	Select
Deny	8e:5b:54:f6:e1:00	<input checked="" type="checkbox"/>
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/>		

- Step 4** Confirm the prompt information, and click **OK**.

192.168.1.1 says

Do you really want to delete the selected entry?

---End

After the configuration is completed, the smartphone can connect to the Wi-Fi network again.



If you want to remove all added devices from the blacklist, you can click **Delete All**.

7 WAN

This guide is for reference only and does not imply that the product supports all functions in the guide. The functions may differ with different product models or different versions of the same model. The actual product prevails.

7.1 Overview

After you have [registered the ONT](#) successfully, you can set up the WAN connection.



TIP

Internet is used for illustration in this chapter unless specified.

The ONT can work under the following two modes:

- [Bridge mode](#): The service type is set to **Bridged**. To access the internet, you can set up an internet connection (PPPoE, DHCP or static IP) on a computer or router connected to the ONT.
- [Router mode](#): The service type is set to **IPoE** or **PPPoE**. To access the internet, you can set up WAN connections on the ONT.



TIP

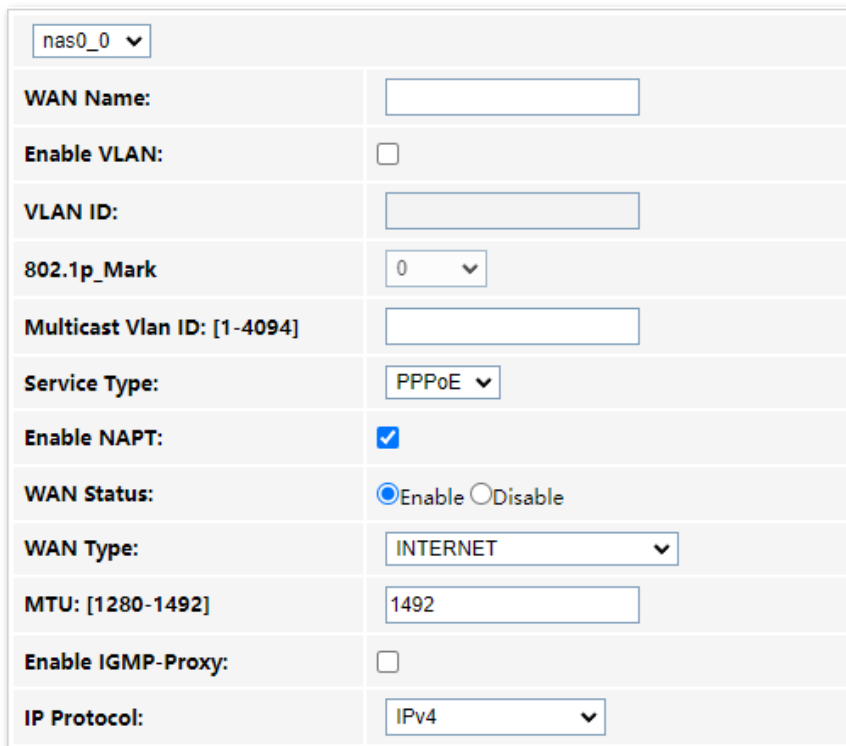
- The actual service type and web UI of the product prevail.
- Under the bridge mode, you can only access the internet through the LAN ports of the ONT.
- Under the router mode, you can access the internet through both the LAN ports and Wi-Fi networks of the ONT.

To access the page, [log in to the web UI](#) of the ONT and navigate to **WAN > WAN > PON WAN**. Required settings for WAN connections differ with the service types, connection types and IP protocols that you choose.

7.1.1 Common WAN settings



To access the page, [log in to the web UI](#) of the ONT and navigate to **WAN > WAN > PON WAN**.

This part shows the common settings in all types of WAN connections.



Parameter description

Parameter	Description
nas0_0	<p>Specifies the WAN interface name which you set up.</p> <p>You can add multiple WAN connections by clicking the drop-down list and choose new link. After configuring required parameters, you can click Apply Change to save the connections.</p> <p>This parameter is generated automatically after you create a new link and cannot be customized. A maximum of eight links can be created here.</p>
WAN Name	Specifies the name of the WAN connection.
Enable VLAN	If the WAN connection you want to set up includes VLAN information, you can select Enable VLAN and set the VLAN ID as required.
VLAN ID	
802.1p_Mark	This parameter is available only when the Enable VLAN function is enabled. It specifies the 802.1P priority. Data with a larger priority value takes a higher priority to be processed.

Parameter	Description
Multicast Vlan ID: [1-4094]	The VLAN ID should meet the VLAN range specified by 802.1Q. The ONT can only forward multicast packets of this VLAN.
Service Type	<p>Specifies the type that you used to set up the WAN connection.</p> <ul style="list-style-type: none"> – Bridged: Select this type when this device only serves as a modem, and you want to set up a dial-up connection or enter other internet parameters directly on your computer for internet access. – IPoE: Select DHCP if your ISP does not provide any parameters to you for internet access, and select Fixed IP if your ISP provides a static IP address and other related information to you for internet access. – PPPoE: Select this type if your ISP provides a user name and password to you for internet access. <p> TIP</p> <p>The actual service type and web UI of the product prevail.</p>
WAN Status	Specifies whether to enable this WAN connection.
WAN Type	<p>Specifies the WAN connection type. Choose the proper connection type as required by your ISP, including Other, TR069, INTERNET, INTERNET_TR069, VOICE, VOICE_TR069, VOICE_INTERNET, and VOICE_INTERNET_TR069.</p> <p> TIP</p> <p>If Other is selected, certain interfaces in Port Mapping must be for the WAN connection to forward packets. If INTERNET is selected, when certain interfaces in Port Mapping are not selected, the packets will be forwarded according to the route table.</p>
MTU: [1280-1492]	Maximum Transmission Unit (MTU) is the largest data packet transmitted by a network device. When the service type is PPPoE, the default MTU value is 1492. When the service type is IPoE, the default MTU value is 1500. Do not change the value unless necessary.
Enable IGMP-Proxy	<p>Specifies whether to enable the Internet Group Management Protocol (IGMP) Proxy. If you are not sure, keep the default setting or consult your ISP.</p> <p>IGMP Proxy is used to manage multicast data and reduce traffic replication. IGMP proxy enables a device to issue IGMP host messages on behalf of its users, reducing IGMP messages and the load for the uplink device.</p>
IP Protocol	<p>Specifies the adopted IP protocol version.</p> <ul style="list-style-type: none"> – IPv4: Select this option if IPv4 is used for communication. – IPv6: Select this option if IPv6 is used for communication. – IPv4/IPv6: Select this option if both IPv4 and IPv6 are used for communication.

7.1.2 WAN IP settings

To access the page, [log in to the web UI](#) of the ONT and navigate to **WAN > WAN > PON WAN**.

You can configure the WAN IPv4 address information in this part.

This part needs to be configured only when **Service Type** is set to **IPoE** and **IP Protocol** is set to **IPv4** or **IPv4/IPv6**.




The actual service type and web UI of the product prevail.

WAN IP Settings:	
Type:	<input checked="" type="radio"/> Fixed IP <input type="radio"/> DHCP
Local IP Address:	<input type="text"/>
Gateway:	<input type="text"/>
Subnet Mask:	<input type="text"/>
Request DNS:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Primary DNS Server:	<input type="text"/>
Secondary DNS Server :	<input type="text"/>

Parameter description

Parameter	Description
Type	<p>Specifies the method used by the ONT to obtain WAN IP address information.</p> <ul style="list-style-type: none"> Fixed IP: You need to configure the local IP address, remote IP address (gateway address) and other related information manually. DHCP: The ONT obtains WAN IP address information automatically. Choose this type if your ISP does not provide related parameters.
Local IP Address	
Gateway	If you select Fixed IP for Type , you should manually enter the IP address and related information provided by your ISP.
Subnet Mask	
Request DNS	If the IP address is obtained through DHCP , you can select Request DNS to obtain the DNS server address automatically.

Parameter	Description
Primary DNS Server	If the IP address obtaining type is Fixed IP or Request DNS function is disabled when the IP address obtaining type is DHCP , you should enter the DNS server address provided by your ISP.
Secondary DNS Server	 TIP If the ISP only provides one DNS server address, you can leave the secondary DNS blank.

7.1.3 IPv6 WAN settings

To access the page, [log in to the web UI](#) of the ONT and navigate to **WAN > WAN > PON WAN**.

You can configure the WAN IPv6 address information in this part.

When **IP Protocol** is set to **IPv6** or **IPv4/IPv6**, and **Service Type** is set to **IPoE** or **PPPoE**, these parameters are required.



TIP

The actual service type and web UI of the product prevail.

IPv6 WAN Setting:	
Address Mode:	Static ▼
IPv6 Address:	<input type="text"/> / <input type="text"/>
IPv6 Gateway:	<input type="text"/>
Request DNS :	<input checked="" type="radio"/> on <input type="radio"/> off
Primary IPv6 DNS:	<input type="text"/>
Secondary IPv6 DNS:	<input type="text"/>

Parameter description

Parameter	Description
Address Mode	<p>Specifies how the WAN IPv6 address of the ONT is obtained, including Stateless DHCPv6(SLAAC), Static, Stateful DHCPv6 and Auto Detect Mode.</p> <ul style="list-style-type: none"> – Stateless DHCPv6(SLAAC): Stateless Address Autoconfiguration (SLAAC) is a dynamic allocation method of IPv6 address, which enables the ONT to auto-generate IPv6 addresses with local information and those from the router advertisement. – Static: You need to enter parameters related to IPv6 address manually. – Stateful DHCPv6: The DHCPv6 server assigns IPv6 addresses to all DHCPv6 clients while keeping track of what IPv6 address has been assigned to what client. In IPv6, only routers sending router advertisement messages can provide a default gateway address dynamically. – Auto Detect Mode: Network hosts get configured with IPv6 addresses automatically.
IPv6 Address	Specifies the IPv6 address and prefix length provided by your ISP when you select Static for Address Mode .
IPv6 Gateway	Specifies the IPv6 gateway address of the ONT when you select Static for Address Mode .
Request Options	You can enable the ONT to obtain the prefix as a DHCPv6 client.
Request DNS	When Request DNS is set to on , the ONT obtains the IPv6 DNS server address from the DHCPv6 server.
Primary IPv6 DNS	When Request DNS is set to off , you need to set the primary and secondary DNS server addresses manually.
Secondary IPv6 DNS	

7.1.4 PPP settings

To access the page, [log in to the web UI](#) of the ONT and navigate to **WAN > WAN > PON WAN**.

You can configure the PPPoE parameters to access the internet in this part.



When **Service Type** is set to **PPPoE**, these parameters are required.



The actual service type and web UI of the product prevail.

PPP Settings:	
UserName:	<input type="text"/>
Password:	<input type="password"/> <input type="checkbox"/> Show Password
Type:	Continuous ▼
AC-Name:	<input type="text"/>
Service-Name:	<input type="text"/>

Parameter description

Parameter	Description
UserName	Specify the PPPoE user name and password for settings up the WAN connection.
Password	
Type	<p>Specifies the PPPoE connection type.</p> <ul style="list-style-type: none"> - Continuous: The ONT keeps connected to the internet. - Connect on Demand: The ONT disconnects from the internet after a certain period and establishes the connection as soon as you attempt to access the internet. - Manual: Users should manually connect and disconnect the network connection.
AC-Name	<p>Specifies the PPPoE server name used by the PPPoE server to verify the legitimacy of the ONT.</p> <p> TIP</p> <p>If your ISP did not provide the AC name, leave this field blank. Otherwise, a dial failure may occur.</p>
Service-Name	<p>Specifies the PPPoE service name used by the PPPoE server to verify the legitimacy of the ONT.</p> <p> TIP</p> <p>If your ISP did not provide a service name, leave this field blank. Otherwise, a dial failure may occur.</p>

7.1.5 Port mapping

To access the page, [log in to the web UI](#) of the ONT and navigate to **WAN > WAN > PON WAN**.

You can configure the port mapping options in this part. When certain interfaces are selected for the WAN connection, devices connected to these interfaces use the WAN connection to access the internet preferentially.



TIP

- If the **Service Type** is set to **Bridged** and the **Connection Type** is set to **Other**, the corresponding LAN port is required to be selected.
- If the **Service Type** is set to **IPoE** or **PPPoE**, you can leave this field blank.
- The actual service type and web UI of the product prevail

Port Mapping:	
<input type="checkbox"/> LAN_1	<input type="checkbox"/> LAN_2
<input type="checkbox"/> LAN_3	<input type="checkbox"/> LAN_4
<input type="checkbox"/> WLAN0	
<input type="checkbox"/> WLAN0-AP1	<input type="checkbox"/> WLAN0-AP2
<input type="checkbox"/> WLAN0-AP3	<input type="checkbox"/> WLAN0-AP4
<input type="checkbox"/> WLAN1	
<input type="checkbox"/> WLAN1-AP1	<input type="checkbox"/> WLAN1-AP2
<input type="checkbox"/> WLAN1-AP3	<input type="checkbox"/> WLAN1-AP4

7.2 Bridge mode

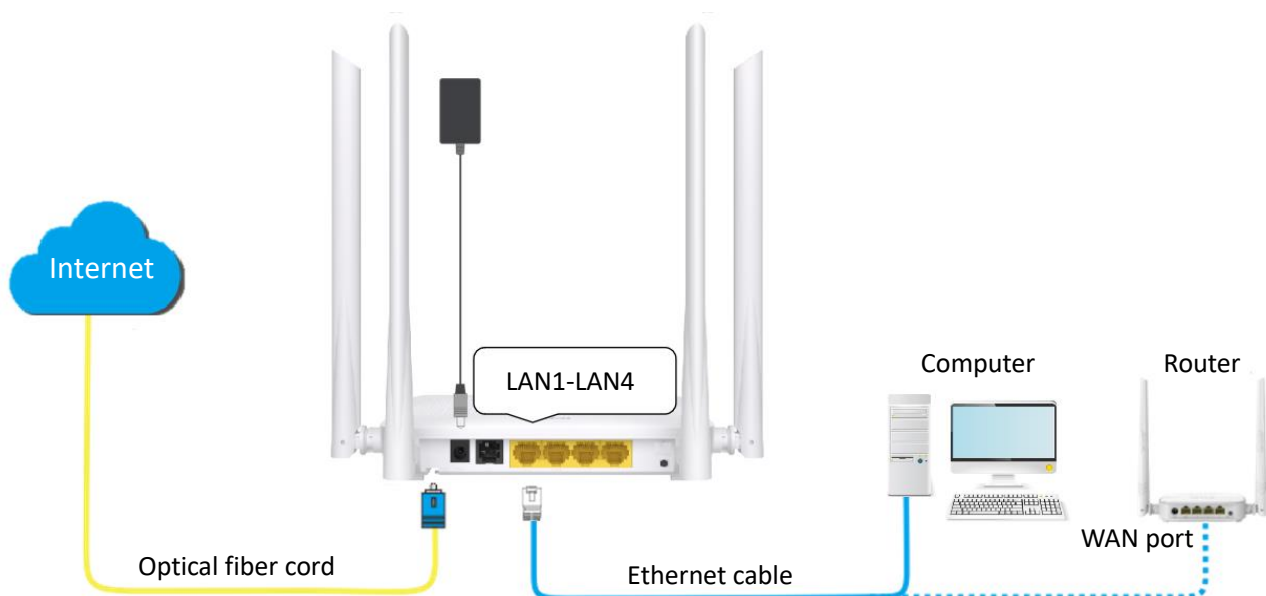
If you have a router and want to set up internet access on it, or you only want to access the internet on a certain computer, you can use the ONT under bridge mode.



When the ONT is under bridge mode, you can only access the internet through the downstream device used for setting up internet access.

Under bridge mode, the ONT acts as a bridging device between your LAN and your ISP. The ONT works under bridge mode by default.

The network topology is shown as follows.



7.2.1 Configure the ONT



When the ONT is set to the bridge mode, you can configure the related parameters of the ONT according to your ISP and your own need.

Procedure:

- Step 1** [Log in to the web UI](#) of the ONT, and navigate to **WAN > WAN > PON WAN**.
- Step 2** Set **WAN Name**.
- Step 3** Tick **Enable VLAN**.
- Step 4** Enter the **VLAN ID** provided by your ISP.

- Step 5** Set **Service Type** to **Bridged**.
- Step 6** Set **Connection Type** to **INTERNET**.
- Step 7** Select the interface for the WAN connection, which is **LAN_1** in this example.
- Step 8** Set other parameters according to your ISP and your own need.
- Step 9** Click **Apply Changes**.

nas0_0 ▾	
WAN Name:	<input type="text"/>
Enable VLAN:	<input checked="" type="checkbox"/>
VLAN ID:	<input type="text"/>
802.1p_Mark	0 ▾
Multicast Vlan ID: [1-4094]	<input type="text"/>
Service Type:	Bridged ▾
Enable NAPT:	<input type="checkbox"/>
WAN Status:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
WAN Type:	INTERNET ▾

Port Mapping:	
<input checked="" type="checkbox"/> LAN_1	<input type="checkbox"/> LAN_2
<input type="checkbox"/> LAN_3	<input type="checkbox"/> LAN_4
<input type="checkbox"/> WLAN0	
<input type="checkbox"/> WLAN0-AP1	<input type="checkbox"/> WLAN0-AP2
<input type="checkbox"/> WLAN0-AP3	<input type="checkbox"/> WLAN0-AP4
<input type="checkbox"/> WLAN1	
<input type="checkbox"/> WLAN1-AP1	<input type="checkbox"/> WLAN1-AP2
<input type="checkbox"/> WLAN1-AP3	<input type="checkbox"/> WLAN1-AP4

---End

After the configuration is completed, you can configure a computer or a router to dial-up.

7.2.2 Configure internet access on a computer or a router

Configure internet access on a computer



Configure your computer to access the internet according to the parameters provided by your ISP. PPPoE is used for illustration here.

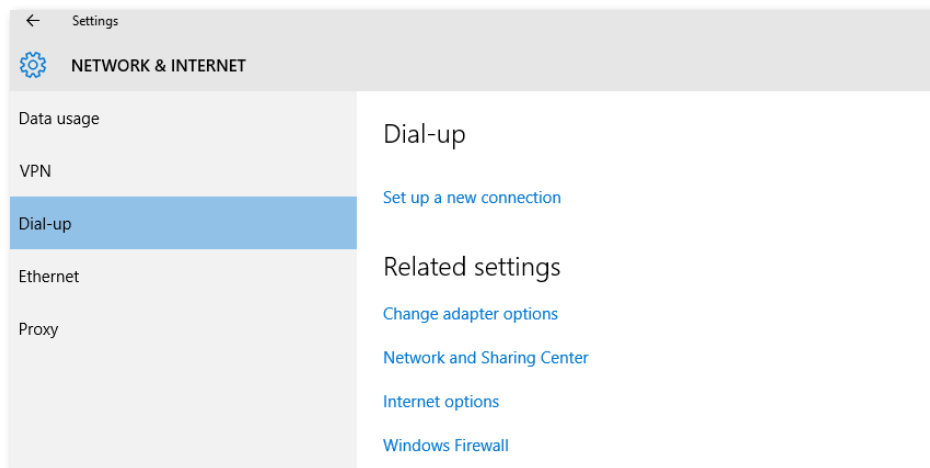
Procedure:

Step 1 [Configure the ONT.](#)

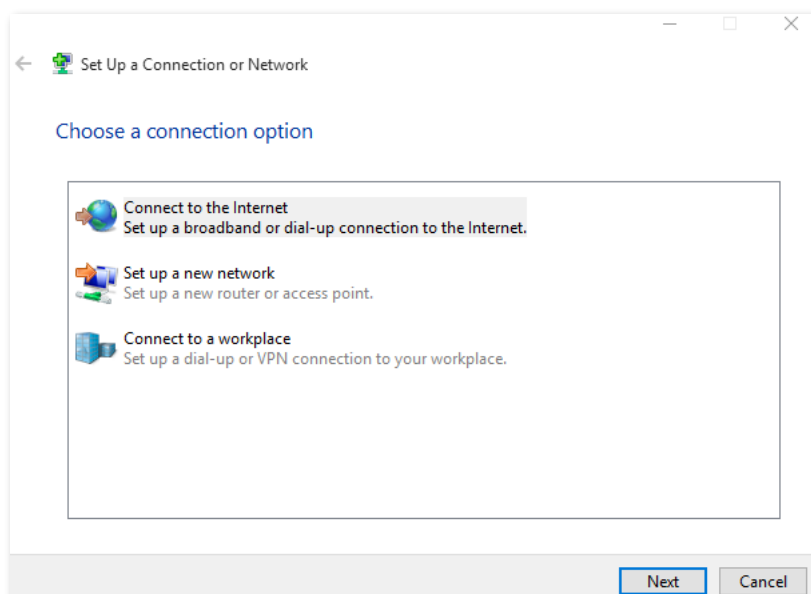
Step 2 Connect your computer to a LAN port of the ONT.

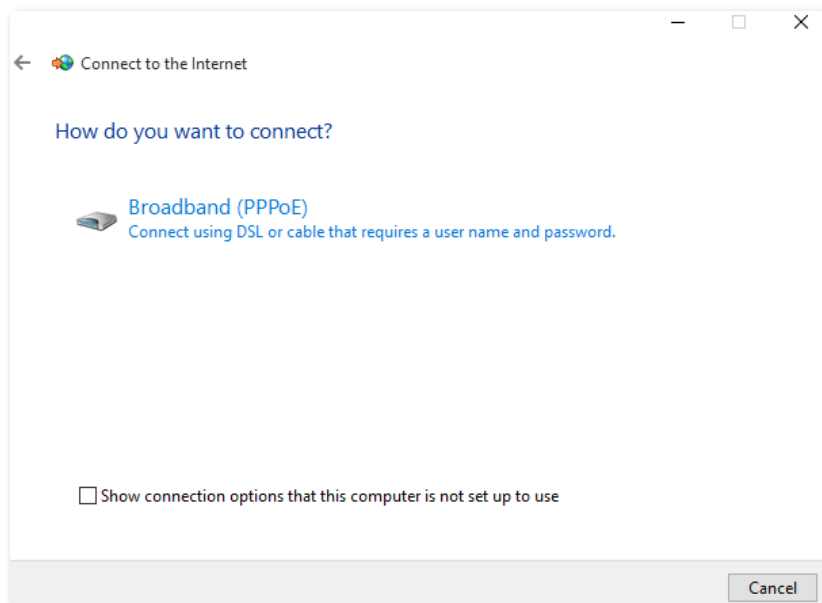
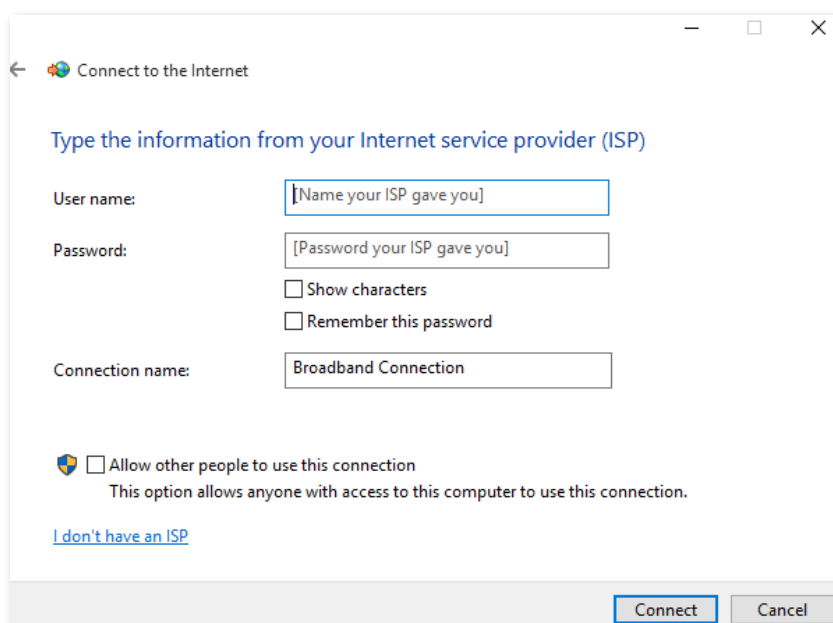
Step 3 Right-click  on the desktop and choose **Network Connections**.

Step 4 Choose **Dial-up** and click **Set up a new connection**.



Step 5 Click **Connect to the Internet** and click **Next**.



Step 6 Click **Broadband (PPPoE)**.**Step 7** Enter the PPPoE **User name** and **Password** provided by your ISP and click **Connect**.**---End**

After the configuration is completed, you can access the internet on the computer.

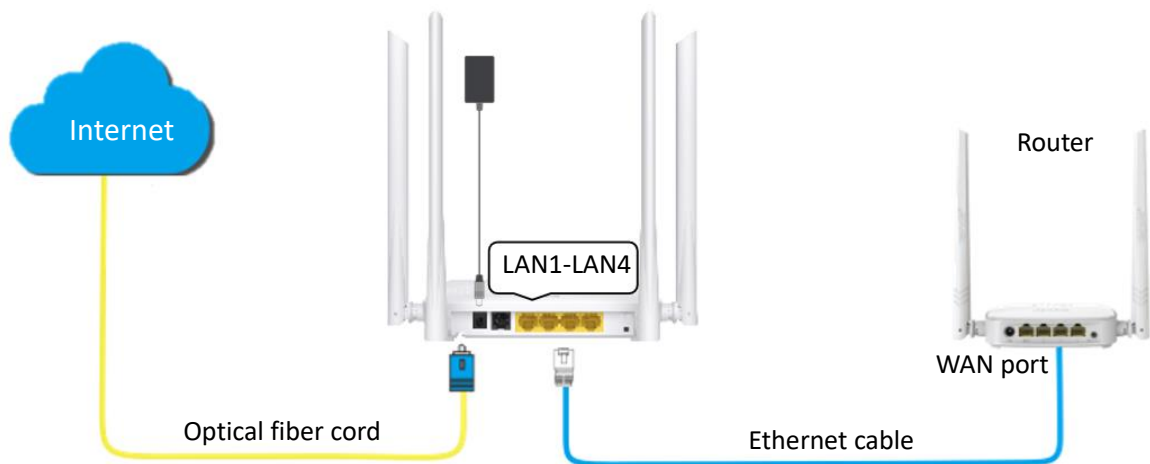
Configure internet access on a router

Assume that your ISP provides you with the PPPoE user name and password.

Procedure:

Step 1 [Configure the ONT.](#)

Step 2 Connect the WAN port of router to a LAN port of the ONT using an Ethernet cable.



Step 3 Refer to the quick installation guide or user guide of your router to configure the internet access.

---End

After the configuration is completed, you can access the internet through the router.

7.3 Router mode

If you want to set up WAN connections for one or multiple services on the ONT, and access the WAN connection through both the Wi-Fi networks of the ONT and LAN ports, you can set the ONT to router mode. Based on the information provided by your ISP, you need to complete different configurations on the web UI.

7.3.1 Set up a fixed IP connection

When your ISP provides fixed IP address (IPv4 or IPv6, or both) information, which may include the IP address, subnet mask and DNS server, you can set up a fixed IP connection.

Procedure:

- Step 1** [Log in to the web UI](#) of the ONT.
- Step 2** Navigate to **WAN > WAN > PON WAN**.
- Step 3** Set **WAN Name**.
- Step 4** Set **Service Type** to **IPoE**.
- Step 5** Set other common WAN parameters as required by your ISP.

nas0_0 ▼	
WAN Name:	<input type="text"/>
Enable VLAN:	<input type="checkbox"/>
VLAN ID:	<input type="text"/>
802.1p_Mark	0 ▼
Multicast Vlan ID: [1-4094]	<input type="text"/>
Service Type:	IPoE ▼
Enable NAT:	<input checked="" type="checkbox"/>
WAN Status:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
WAN Type:	INTERNET ▼
MTU: [1280-1500]	1500
Enable IGMP-Proxy:	<input type="checkbox"/>
IP Protocol:	IPv4 ▼

- Step 6** Configure **WAN IP Settings** or (and) **IPv6 WAN Setting** based on the IP protocol you choose.
 - In the **WAN IP Settings** part, set **Type** to **Fixed IP** and configure other parameters as required.

- In the **IPv6 WAN Setting** part, set **Address Mode** to **Static** and configure other parameters as required.

WAN IP Settings:	
Type:	<input checked="" type="radio"/> Fixed IP <input type="radio"/> DHCP
Local IP Address:	<input type="text"/>
Gateway:	<input type="text"/>
Subnet Mask:	<input type="text"/>
Request DNS:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Primary DNS Server:	<input type="text"/>
Secondary DNS Server :	<input type="text"/>

IPv6 WAN Setting:	
Address Mode:	Static <input type="button" value="v"/>
IPv6 Address:	<input type="text"/> / <input type="text"/>
IPv6 Gateway:	<input type="text"/>
Request DNS :	<input checked="" type="radio"/> on <input type="radio"/> off
Primary IPv6 DNS:	<input type="text"/>
Secondary IPv6 DNS:	<input type="text"/>

Step 7 (Optional) Configure **Port Mapping** as required.

Port Mapping:	
<input type="checkbox"/> LAN_1	<input type="checkbox"/> LAN_2
<input type="checkbox"/> LAN_3	<input type="checkbox"/> LAN_4
<input type="checkbox"/> WLAN0	
<input type="checkbox"/> WLAN0-AP1	<input type="checkbox"/> WLAN0-AP2
<input type="checkbox"/> WLAN0-AP3	<input type="checkbox"/> WLAN0-AP4
<input type="checkbox"/> WLAN1	
<input type="checkbox"/> WLAN1-AP1	<input type="checkbox"/> WLAN1-AP2
<input type="checkbox"/> WLAN1-AP3	<input type="checkbox"/> WLAN1-AP4

Step 8 Click **Apply Changes**.

---End

After the configuration is completed, you can access the internet through the LAN ports or Wi-Fi networks of the ONT, or by connecting a router (connection type: DHCP or dynamic IP) to a LAN port of the ONT.

7.3.2 Set up a dynamic IP connection

If your ISP does not provide any parameters, you can try to set up a DHCP connection.

Procedure:

- Step 1** [Log in to the web UI](#) of the ONT.
- Step 2** Navigate to **WAN > WAN > PON WAN**.
- Step 3** Set **WAN Name**.
- Step 4** Set **Service Type** to **IPoE**.
- Step 5** Set other common WAN parameters as required by your ISP.

nas0_0 ▼	
WAN Name:	<input type="text"/>
Enable VLAN:	<input type="checkbox"/>
VLAN ID:	<input type="text"/>
802.1p_Mark	0 ▼
Multicast Vlan ID: [1-4094]	<input type="text"/>
Service Type:	IPoE ▼
Enable NAPT:	<input checked="" type="checkbox"/>
WAN Status:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
WAN Type:	INTERNET ▼
MTU: [1280-1500]	1500
Enable IGMP-Proxy:	<input type="checkbox"/>
IP Protocol:	IPv4 ▼

- Step 6** Configure **WAN IP Settings** or (and) **IPv6 WAN Setting** based on the IP protocol you choose.
 - In the **WAN IP Settings** part, set **Type** to **DHCP** and configure other parameters as required.
 - In the **IPv6 WAN Setting** part, set **Type** to **Stateless DHCPv6(SLAAC)** and configure other parameters as required.

WAN IP Settings:	
Type:	<input type="radio"/> Fixed IP <input checked="" type="radio"/> DHCP
Request DNS:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

IPv6 WAN Setting:	
Address Mode:	Stateless DHCPv6(SLAAC) ▼
Request Options:	<input checked="" type="checkbox"/> Request Prefix
Request DNS :	<input checked="" type="radio"/> on <input type="radio"/> off
Primary IPv6 DNS:	<input type="text"/>
Secondary IPv6 DNS:	<input type="text"/>

Step 7 (Optional) Configure **Port Mapping** as required.

Port Mapping:	
<input type="checkbox"/> LAN_1	<input type="checkbox"/> LAN_2
<input type="checkbox"/> LAN_3	<input type="checkbox"/> LAN_4
<input type="checkbox"/> WLAN0	
<input type="checkbox"/> WLAN0-AP1	<input type="checkbox"/> WLAN0-AP2
<input type="checkbox"/> WLAN0-AP3	<input type="checkbox"/> WLAN0-AP4
<input type="checkbox"/> WLAN1	
<input type="checkbox"/> WLAN1-AP1	<input type="checkbox"/> WLAN1-AP2
<input type="checkbox"/> WLAN1-AP3	<input type="checkbox"/> WLAN1-AP4

Step 8 Click **Apply Changes**.

---End

After the configuration is completed, you can access the internet through the LAN ports or Wi-Fi networks of the ONT, or by connecting a router (connection type: DHCP or dynamic IP) to a LAN port of the ONT.

7.3.3 Set up a PPPoE connection

If your ISP provides the PPPoE user name, password, and other related parameters (if any), you can set up a PPPoE connection.

Procedure:

- Step 1** [Log in to the web UI](#) of the ONT, and navigate to **WAN > WAN > PON WAN**.
- Step 2** Set **WAN Name**.
- Step 3** Set **Service Type** to **PPPoE**.
- Step 4** Choose an **IP Protocol** in the drop-down list.
- Step 5** Set other common WAN parameters as required by your ISP.

nas0_0 ▼	
WAN Name:	<input type="text"/>
Enable VLAN:	<input type="checkbox"/>
VLAN ID:	<input type="text"/>
802.1p_Mark	0 ▼
Multicast Vlan ID: [1-4094]	<input type="text"/>
Service Type:	PPPoE ▼
Enable NAPT:	<input checked="" type="checkbox"/>
WAN Status:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
WAN Type:	INTERNET ▼
MTU: [1280-1492]	1492
Enable IGMP-Proxy:	<input type="checkbox"/>
Enable MLD-Proxy:	<input type="checkbox"/>
IP Protocol:	IPv4/IPv6 ▼

- Step 6** Enter the PPPoE **UserName** and **Password** provided by your ISP in **PPP Settings**.

PPP Settings:	
UserName:	<input type="text"/>
Password:	<input type="password"/> <input type="checkbox"/> Show Password
Type:	Continuous ▼
AC-Name:	<input type="text"/>
Service-Name:	<input type="text"/>

Step 7 (Optional) If you set **IP Protocol** to **IPv6** or **IPv4/IPv6**, enter required parameters in **IPv6 WAN Setting**.

Step 8 (Optional) Configure **Port Mapping** as required.

Port Mapping:	
<input type="checkbox"/> LAN_1	<input type="checkbox"/> LAN_2
<input type="checkbox"/> LAN_3	<input type="checkbox"/> LAN_4
<input type="checkbox"/> WLAN0	
<input type="checkbox"/> WLAN0-AP1	<input type="checkbox"/> WLAN0-AP2
<input type="checkbox"/> WLAN0-AP3	<input type="checkbox"/> WLAN0-AP4
<input type="checkbox"/> WLAN1	
<input type="checkbox"/> WLAN1-AP1	<input type="checkbox"/> WLAN1-AP2
<input type="checkbox"/> WLAN1-AP3	<input type="checkbox"/> WLAN1-AP4

Step 9 Click **Apply Changes**.

---End

After the configuration is completed, you can access the internet through the LAN ports or Wi-Fi networks of the ONT, or by connecting a router (connection type: DHCP or dynamic IP) to a LAN port of the ONT.

7.4 NAT

NAT is abbreviated for Network Address Translation, which enables multiple devices in the LAN to share one or more public IP addresses to access the internet and hide the LAN devices, so that the internet cannot directly access the LAN devices, providing certain security for the LAN.

The NAT function is suitable for scenarios where there are few public network addresses but many private network users need to access the internet. You can select the NAT type according to the actual security level requirements. The security level is as follows: NAT4 > NAT2 > NAT1.

To access the page, [log in to the web UI](#) of the ONT and navigate to **WAN > WAN > NAT**.

NAT
 This page is used to configure the nat type. NAT1: Full Cone NAT, NAT2: Address-Restricted Cone NAT, NAT4: Symmetric NAT.

Nat Type
 ☐ NAT1
 ☒ NAT2
 ☐ NAT4

Parameter description

Parameter	Description
NAT1	Specifies the full cone NAT, which maps all requests from the IP address and port of the private network to the same IP address and port of the public network. Any host of the public network can communicate with the host of the private network by sending the message to the mapped IP address and port of the public network.
NAT2	Specifies the restricted cone NAT, which maps all requests from the IP address and port of the private network to the same IP address and port of the public network. The host of the public network can send the message to the host of the private network only if the host of the private network has sent the message to the host of the public network before. Compared with NAT1, NAT2 has the address restrictions. IP address is restricted, but port is not restricted.
NAT4	Specifies the symmetric NAT. All requests sent from the IP address and port of the same private network to the specific destination IP address and port will be mapped to the same IP address and port. The host of the public network can send the message to the host of the private network only if the host of the private network has sent the message to the host of the public network before.

8 Services

This guide is for reference only and does not imply that the product supports all functions in the guide. The functions may differ with different product models or different versions of the same model. The actual product prevails.

8.1 Service

8.1.1 Dynamic DNS

Overview

The Dynamic DNS (DDNS) maps the WAN IP address (changeable public IP address) of the ONT to a domain name for dynamic domain name resolution. This ensures proper operation of functions that involve the WAN IP address of the ONT, such as port forwarding and Demilitarized Zone (DMZ).

To access the page, [log in to the web UI](#) of the ONT and navigate to **Services > Service > Dynamic DNS**.

Enable:	<input checked="" type="checkbox"/>
DDNS Provider:	<input type="text" value="DynDNS.org"/>
Hostname:	<input type="text"/>
Interface	<input type="text" value="v"/>
UserName:	<input type="text"/>
Password:	<input type="text"/> <input type="checkbox"/> Show Password

Dynamic DNS Table						
Select	State	Hostname	Username	Service	Status	Interface

Parameter description

Parameter	Description
Enable	Specifies whether the rule takes effect after being added.
DDNS Provider	Specifies the DDNS service provider. The ONT supports DynDNS.org and No-IP . You need to register and purchase services from one of these service providers and use the parameters provided by the service provider to configure the function on the ONT.
Hostname	Specifies the hostname registered with the DDNS service.
Interface	Specifies the WAN interface on which the dynamic DNS rule takes effect.
UserName	Specify the user name and password registered on a DDNS service provider for logging in to the DDNS service.
Password	These fields are only available when the service provider is set to DynDNS.org and No-IP .
Add/Modify/Remove/Update	<ul style="list-style-type: none"> – Add: It is used to add a new dynamic DNS rule. – Modify: It is used to modify existing dynamic DNS rules. – Remove: It is used to delete existing dynamic DNS rules. – Update: It is used to update existing dynamic DNS rules.
Select	Select existing rules to modify or remove them.
State	Specifies the status of a rule, including Enable and Disable .
Service	Specifies the DDNS service of the ONT.
Status	Specifies the description information about the rule.

Enable internet users to access LAN resources using a domain name

Scenario: You have set up an FTP server within your LAN.

Requirement: Open the FTP server to internet users and enable yourself to access the resources of the FTP server from the internet using a domain name when you are not at home.

Solution: You can configure the DDNS plus port forwarding functions to reach the requirement.

Assume that the information of the FTP server includes:

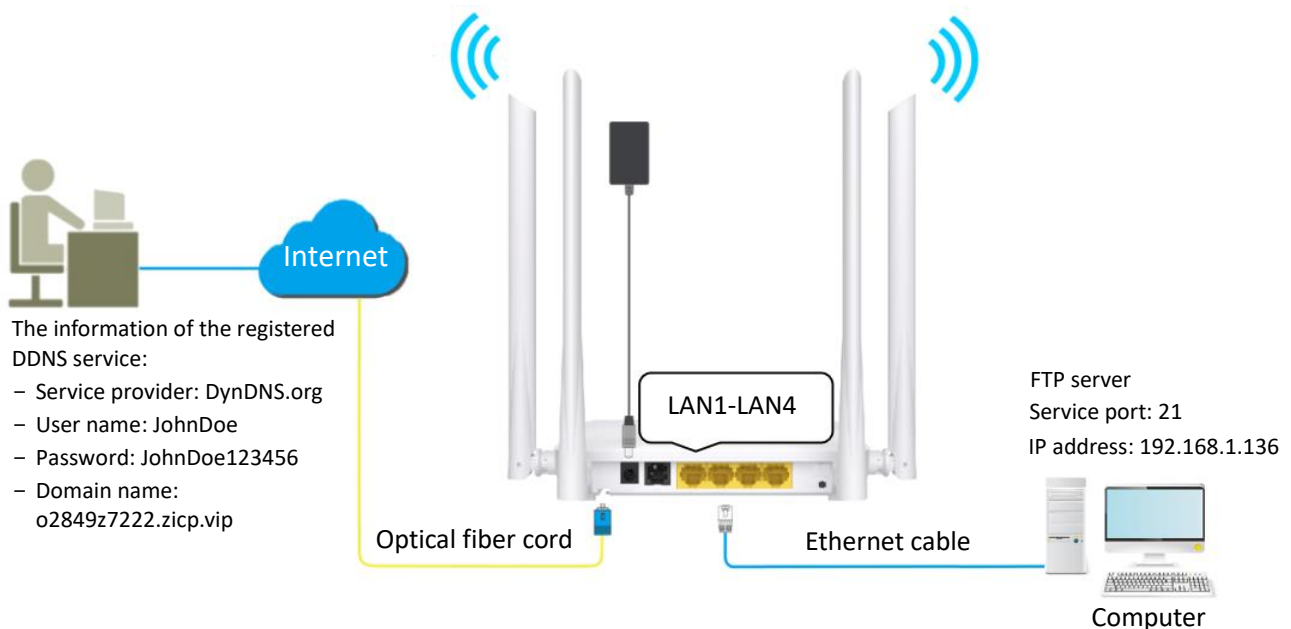
- IP address: 192.168.1.136
- Service port: 21

The information of the registered DDNS service:

- Service provider: DynDNS.org
- User name: JohnDoe
- Password: JohnDoe123456
- Domain name: o2849z7222.zicp.vip



Please ensure that the ONT obtains a public IP address. This function may not work on a host with an IP address of a private network or an intranet IP address assigned by ISPs that start with 100. Common IPv4 addresses are classified into class A, class B and class C. Private IP addresses of class A range from 10.0.0.0 to 10.255.255.255. Private IP addresses of class B range from 172.16.0.0 to 172.31.255.255. Private IP addresses of class C range from 192.168.0.0 to 192.168.255.255.



Procedure:

Step 1 [Log in to the web UI](#) of the ONT.

Step 2 Add a Dynamic DNS rule.

1. Navigate to **Services > Service > Dynamic DNS**.
2. Select **Enable**.
3. Choose a service provider in **DDNS Provider**, which is **DynDNS.org** in this example.
4. Enter the **Hostname**, which is **o2849z7222.zicp.vip** in this example.
5. Select the WAN interface that the port forwarding rule applies to, which is **ppp0** in this example.
6. Enter the user name and password, which are **JohnDoe** and **JohnDoe123456** in this example.

7. Click **Add**.

Enable:	<input checked="" type="checkbox"/>
DDNS Provider:	DynDNS.org ▼
Hostname:	o2849z7222.zicp.vip
Interface	ppp0 ▼
UserName:	JohnDoe
Password: <input type="checkbox"/> Show Password

Step 3 Configure the port forwarding function (refer to [port forwarding](#)).

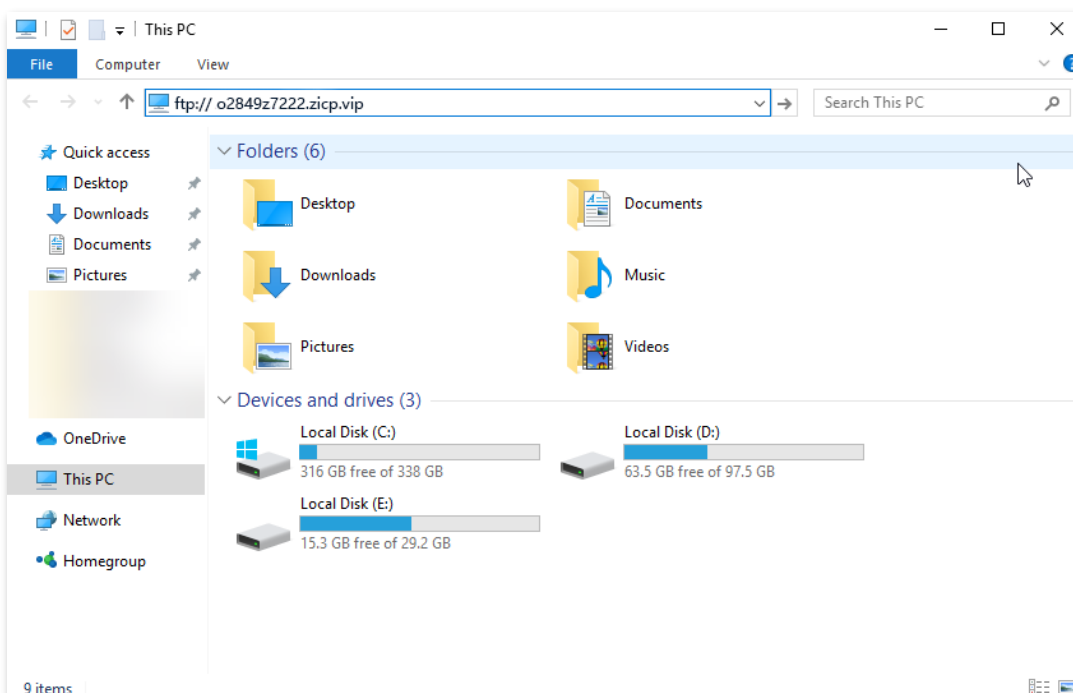
---End

After the configuration is completed, users from the internet can access the FTP server by visiting *"Intranet service application layer protocol name://Domain name"*. If the remote port number is not the same as the default intranet service port number, the accessing address should be: *"Intranet service application layer protocol name://Domain name:Remote port number"*.

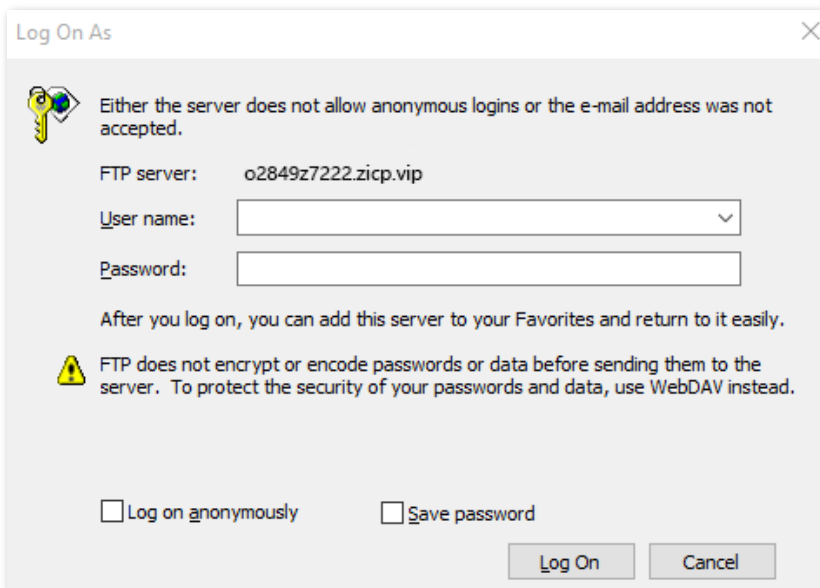
In this example, the address is **ftp://o2849z7222.zicp.vip**.

To access the FTP server from the internet with a domain name:

Open the file explorer on a computer that can access the internet, and visit **ftp://o2849z7222.zicp.vip**.



Enter the user name and password to access the resources on the FTP server.



TIP

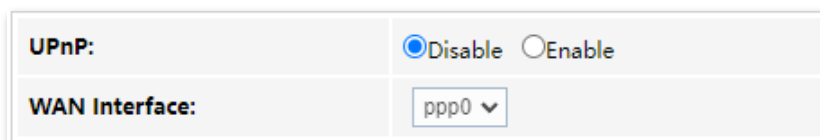
After the configuration is completed, if internet users still cannot access the FTP server, try the following methods:

- Ensure that the local port number configured in the port forwarding function is the same as the intranet service port number set on the server.
- Close the firewall, antivirus software and security guards on the host of the FTP server and try again.

8.1.2 UPnP

UPnP is short for Universal Plug and Play. This function enables the ONT to open port automatically for UPnP-based programs. It is generally used for P2P programs, such as BitComet and AnyChat, and helps increase the download speed.

To access the page, [log in to the web UI](#) of the ONT and navigate to **Services > Service > UPnP**.



8.2 Firewall

8.2.1 ALG

Application Layer Gateway (ALG) is a software component that manages specific application protocols such as Session Initiation Protocol (SIP) and File Transfer Protocol (FTP). The ALG acts as an intermediary between the internet and an application server and allows or denies traffic of certain types to the application server. It does this by intercepting and analyzing the specified traffic, allocating resources, and defining dynamic policies to allow traffic to pass through.

To access the page, [log in to the web UI](#) of the ONT and navigate to **Services > Firewall > ALG**.

ALG Type		
FTP		<input checked="" type="radio"/> Enable <input type="radio"/> Disable
TFTP		<input checked="" type="radio"/> Enable <input type="radio"/> Disable
H323		<input checked="" type="radio"/> Enable <input type="radio"/> Disable
RTSP		<input checked="" type="radio"/> Enable <input type="radio"/> Disable
L2TP		<input checked="" type="radio"/> Enable <input type="radio"/> Disable
IPSec		<input checked="" type="radio"/> Enable <input type="radio"/> Disable
SIP		<input checked="" type="radio"/> Enable <input type="radio"/> Disable
PPTP		<input checked="" type="radio"/> Enable <input type="radio"/> Disable

Parameter description

Parameter	Description
FTP	<p>The File Transfer Protocol (FTP) is a standard network protocol used for the transfer of computer files between a client and server on a computer network.</p> <p>The users on LAN can share resources on the FTP server on WAN only when it is selected.</p>
TFTP	<p>The Trivial File Transfer Protocol (TFTP) is a simple file transfer protocol that allows a client to get a file from or put a file onto a remote host.</p>
H323	<p>H.323 is a recommendation from the ITU Telecommunication Standardization Sector (ITU-T) that defines the protocols to provide audio-visual communication sessions on any packet network. The H.323 standard addresses call signaling and control, multimedia transport and control, and bandwidth control for point-to-point and multi-point conferences.</p> <p>The IP phone and network conference function can be used on the computers connected to the ONT only when this function is enabled.</p>

Parameter	Description
RTSP	<p>The Real Time Streaming Protocol (RTSP) is a network control protocol designed for use in entertainment and communications systems to control streaming media servers. The protocol is used for establishing and controlling media sessions between end points.</p> <p>The users on LAN can view videos on demand when this function is enabled.</p>
L2TP	<p>The Layer Two Tunneling Protocol (L2TP) is an extension of the Point-to-Point Tunneling Protocol (PPTP) used by an Internet Service Provider (ISP) to enable the operation of a Virtual Private Network (VPN) over the Internet.</p> <p>If you select L2TP protocol when you create a VPN connection on your computer in the LAN of the ONT, it takes effect only when this function is enabled.</p>
IPSec	<p>The Internet Protocol Security (IPsec) is a secure network protocol suite that authenticates and encrypts the packets of data to provide secure encrypted communication between two computers over an IP network. It is used in Virtual Private Networks (VPNs).</p> <p>If you select IPsec protocol when you create a VPN connection on your computer in the LAN of the ONT, it takes effect only when this function is enabled.</p>
SIP	<p>The Session Initiation Protocol (SIP) is a signaling protocol used for signaling and controlling multimedia communication sessions in applications of internet telephony for voice and video calls, in private IP telephone systems, in instant messaging over IP networks as well as smartphone calling over LTE (VoLTE).</p> <p>The IP phone function can be used on the computers connected to the ONT only when this function is enabled.</p>
PPTP	<p>The Point-to-Point Tunneling Protocol (PPTP) is an obsolete method for implementing virtual private networks. PPTP has many well-known security issues.</p> <p>If you select the PPTP protocol when you create a VPN connection on your computer in the LAN of the ONT, it takes effect only when this function is enabled.</p>

8.2.2 IP/Port filtering

In this section, you can configure filtering rules to restrict certain types of data packets from passing through the ONT. The use of such filters can help secure or restrict your local network.


- LAN→WAN: By default, all outgoing traffic from LAN is allowed, but some can be blocked by specific filtering rules. Outgoing filtering rules can block outgoing traffic under some conditions.
- WAN→LAN: By default, all incoming traffic is blocked. However, some traffic can access by specific filtering rules. The incoming filtering rules allow traffic to pass in some conditions.

To access the page, [log in to the web UI](#) of the ONT and navigate to **Services > Firewall > IP/Port Filtering**. The rules added are shown in the **Current Filter Table**.

Outgoing Default Action:	<input type="radio"/> WhiteList <input checked="" type="radio"/> BlackList						
Incoming Default Action:	<input checked="" type="radio"/> WhiteList <input type="radio"/> BlackList						
Apply Changes							
Direction: <input type="text" value="Outgoing"/>	Protocol: <input type="text" value="TCP"/>	Rule Action: <input checked="" type="radio"/> Deny <input type="radio"/> Allow					
Source IP Address: <input type="text"/>	Subnet Mask: <input type="text"/>	Port: <input type="text"/> - <input type="text"/>					
Destination IP Address: <input type="text"/>	Subnet Mask: <input type="text"/>	Port: <input type="text"/> - <input type="text"/>					
Add							
Current Filter Table							
Select	Direction	Protocol	Source IP Address	Source Port	Destination IP Address	Destination Port	Rule Action

Parameter description

Parameter	Description
Outgoing Default Action	<p>Specify the default action for the outgoing (LAN -> WAN) or incoming (WAN -> LAN) data.</p> <ul style="list-style-type: none"> BlackList: By default, all incoming traffic is blocked. However, some traffic can access by specific filtering rules. The incoming filtering rules allow traffic to pass in some conditions.
Incoming Default Action	<ul style="list-style-type: none"> WhiteList: By default, all outgoing traffic from LAN is allowed, but some can be blocked by specific filtering rules. Outgoing filtering rules can block outgoing traffic under some conditions.
Direction	Specifies the forwarding direction of data to be filtered.
Protocol	<p>Specifies the protocol adopted by data to be filtered.</p> <ul style="list-style-type: none"> TCP: TCP protocol. UDP: UDP protocol. ICMP: ICMP protocol. TCP/UDP: TCP protocol and UDP protocol. ANY: Any protocol.
Rule Action	<p>Specifies whether to deny or allow the data to pass through.</p> <ul style="list-style-type: none"> Deny: Packets that comply with the rule are denied, while others are perform the default action. Allow: Only packets that comply with the rule are allowed, while others perform the default action.

Parameter	Description
Source IP Address	<p>Specifies the source IP address of the packets. The settings of Source IP Address and Subnet Mask determine which computers are affected by this rule.</p> <ul style="list-style-type: none"> When Direction is set to Outgoing, this parameter specifies the LAN computer's IP address to be affected. When Direction is set to Incoming, this parameter specifies the internet computer's IP address to be affected. When this parameter is left blank, all IP addresses are covered.
Subnet Mask	Specifies the subnet mask of the source IP address.
Port	<p>Specifies the source port of the packets.</p> <p>The source port is only available for the TCP/UDP protocol. If ICMP or ANY is selected for Protocol, this field is not required.</p> <p> TIP</p> <p>Since the source port of the data packet is changeable, it is recommended that the port be set to 1 to 65535 or left blank.</p>
Destination IP Address	<p>Specifies the destination IP address of the packets. The settings of Destination IP Address and Subnet Mask determine which servers are affected by this rule.</p> <ul style="list-style-type: none"> When Direction is set to Outgoing, this parameter specifies the internet server's IP address to be affected. When Direction is set to Incoming, this parameter specifies the LAN server's IP address to be affected. When this parameter is left blank, all IP addresses are covered.
Subnet Mask	Specifies the subnet mask of the destination IP address. The settings of Destination IP Address and Subnet Mask determine which servers are affected by this rule.
Port	<p>Specifies the destination port of the packets. Its setting determines which services are affected by this rule.</p> <p>The destination port is only for TCP and UDP protocol.</p>

8.2.3 MAC filtering

Overview


The MAC filtering function enables you to filter data packets from your local network to the internet to disallow clients with certain MAC addresses to access the internet and helps you to manage your network.

To access the page, [log in to the web UI](#) of the ONT and navigate to **Services > Firewall > MAC Filtering**. The rule added is shown in **Current Filter Table**.

Outgoing Default Action:	<input type="radio"/> WhiteList <input checked="" type="radio"/> BlackList			
Incoming Default Action:	<input type="radio"/> WhiteList <input checked="" type="radio"/> BlackList			
<button>Apply Changes</button>				
Direction:	<input type="text" value="Outgoing"/>			
Source MAC Address:	<input type="text"/>			
Destination MAC Address:	<input type="text"/>			
Rule Action:	<input checked="" type="radio"/> Deny <input type="radio"/> Allow			
<button>Add</button>				
Current Filter Table				
Select	Direction	Source MAC Address	Destination MAC Address	Rule Action

Parameter description

Parameter	Description
Outgoing Default Action	Specify the default action for the outgoing (LAN -> WAN) or incoming (WAN -> LAN) data. <ul style="list-style-type: none"> BlackList: By default, all incoming traffic is blocked. However, some traffic can access by specific filtering rules. The incoming filtering rules allow traffic to pass in some conditions.
Incoming Default Action	<ul style="list-style-type: none"> WhiteList: By default, all outgoing traffic from LAN is allowed, but some can be blocked by specific filtering rules. Outgoing filtering rules can block outgoing traffic under some conditions.
Direction	Specifies the forwarding direction of data to be filtered.
Source MAC Address	Specify the source and destination MAC addresses of data packets.

Parameter	Description
Destination MAC Address	<p>You can only enter one source MAC address and destination MAC address in one MAC filtering rule.</p> <p> TIP</p> <p>The MAC address cannot contain any special characters. An example in the correct format is cc3a61711b6e.</p>
Rule Action	<p>Specifies whether to deny or allow the data to pass through.</p> <ul style="list-style-type: none"> - Deny: Packets that comply with the rule are denied, while others perform the default action. - Allow: Only packets that comply with the rule are allowed, while others perform the default action.

Deny the specified device to access the internet

Scenario: The final exam for your kid is approaching and you want to ban your kid from accessing the internet on the smartphone.

Requirement: Deny certain device of family member to access the internet.

Solution: You can configure the MAC address filter function to reach the requirement.

Assume that the MAC address of your kid's smartphone is 8CEC4BB30493.

Procedure:

Step 1 [Log in to the web UI](#) of the ONT.

Step 2 Navigate to **Services > Firewall > MAC Filtering**.

Step 3 Set **Outgoing Default Action** and **Incoming Default Action**, which are **WhiteList** in this example.

Step 4 Set **Direction**, which is **Outgoing** in this example.

Step 5 Set **Source MAC Address** to **8CEC4BB30493**.

Step 6 Set **Rule Action** to **Deny**, and click **Add**.

Outgoing Default Action:	<input checked="" type="radio"/> WhiteList <input type="radio"/> BlackList
Incoming Default Action:	<input checked="" type="radio"/> WhiteList <input type="radio"/> BlackList
Apply Changes	
Direction:	Outgoing ▼
Source MAC Address:	8CEC4BB30493
Destination MAC Address:	
Rule Action:	<input checked="" type="radio"/> Deny <input type="radio"/> Allow

---End

After the MAC address is added, it is displayed in **Current Filter Table**.

Current Filter Table				
Select	Direction	Source MAC Address	Destination MAC Address	Rule Action
<input type="checkbox"/>	Outgoing	8c-ec-4b-b3-04-93	-----	Deny

In this example, after the configuration is completed, the device added cannot access the internet through the ONT.

8.2.4 Port forwarding

Overview

By default, internet users cannot access any service on any of their local hosts. The port forwarding function enables you to open certain ports of a local host to internet users and allow them to access the corresponding services. This function can allow access and prevent the local network from being attacked at the same time.

To access the page, [log in to the web UI](#) of the ONT and navigate to **Services > Firewall > Port Forwarding**. The rules added are shown in **Current Port Forwarding Table**.

Port Forwarding:	<input type="radio"/> Disable <input checked="" type="radio"/> Enable	Apply Changes				
Application:	▼					
Comment	Local IP	Local Port	Protocol	Remote IP	Remote Port	Interface
			▼			Any ▼

Parameter description

Parameter	Description
Port Forwarding	Specifies whether to enable the port forwarding function.
Application	Includes some common services. When you choose a service from the list, some parameters of the rule are filled automatically, including Comment , Local Port , Protocol and Remote Port .
Comment	You can specify a comment for the rule for easy retrieval.
Local IP	Specifies the IP address of the LAN host which runs the service to be accessed.
Local Port	Specifies the port used for the LAN service.
Protocol	Specifies the service protocol. Select Both if you are uncertain about the service type.
Remote IP	Specifies the IP address of the host which needs to access the local service. When it is left blank, users with any IP address can access the local server.
Remote Port	Specifies the port that internet users use to access the local service.
Interface	Specifies the WAN interface through which internet users access the local service.

Enable internet users to access local services

Scenario: You have set up an FTP server within your LAN.

Requirement: Open the FTP server to internet users and enable family members who are not at home to access the resources of the FTP server from the internet.

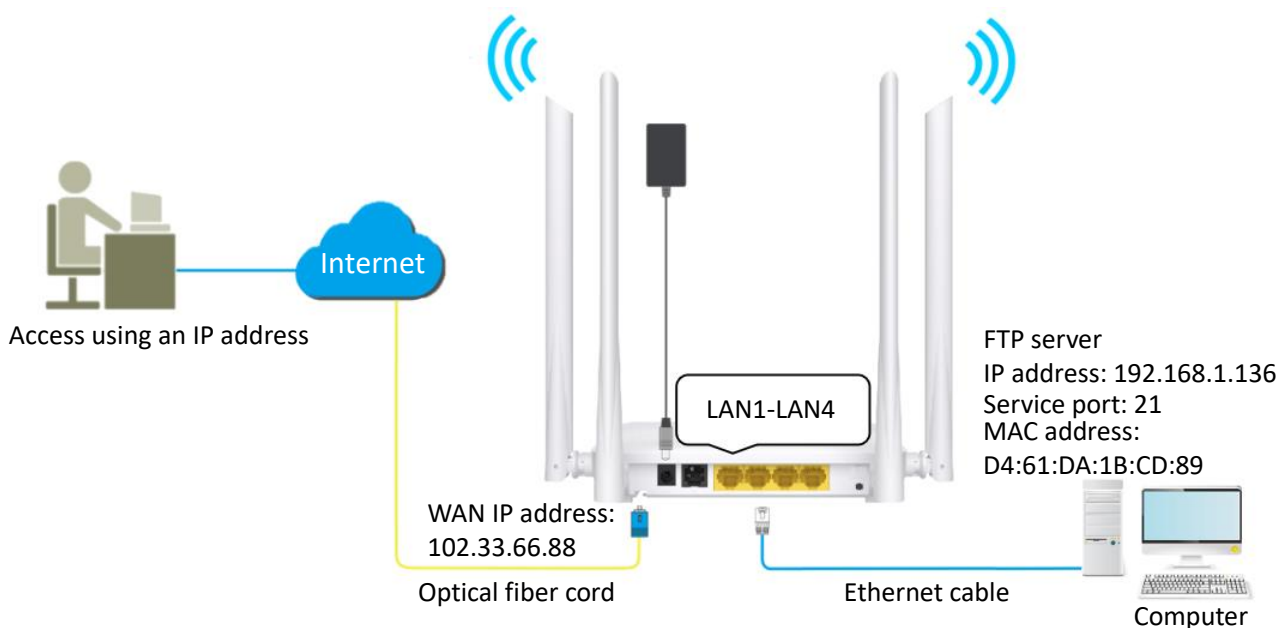
Solution: You can configure the port forwarding function to reach the requirement.

Assume that the information of the FTP server includes:

- Local IP address: 192.168.1.136
- Remote IP address: 192.168.2.100
- MAC address: D4:61:DA:1B:CD:89
- Service port: 21
- The WAN IP address of the router: 102.33.66.88



- Please ensure that the router obtains an IP address from the public network. This function may not work on a host with an IP address of a private network or an intranet IP address assigned by ISPs that start with 100. Common IPv4 addresses are classified into class A, class B and class C. Private IP addresses of class A range from 10.0.0.0 to 10.255.255.255. Private IP addresses of class B range from 172.16.0.0 to 172.31.255.255. Private IP addresses of class C range from 192.168.0.0 to 192.168.255.255.
- ISPs may block unreported web services to be accessed with the default port number 80. Therefore, when the default LAN port number is 80, please manually change it to an uncommon port number (1024–65535), such as 9999.
- The LAN port number can be different from the WAN port number.



Procedure:

Step 1 [Log in to the web UI](#) of the ONT.

Step 2 Add a port forwarding rule.

1. Navigate to **Services > Firewall > Port Forwarding**.
2. Set **Port Forwarding** to **Enable**, and click **Apply Changes**.
3. Select **FTP Server** from the **Application** drop-down list.
4. (Optional) Modify **Comment** for the rule, which is **FTP Server** in this example.
5. Set **Local IP**, which is **192.168.1.136** in this example.
6. Set **Remote IP**, which is **192.168.2.100** in this example.
7. Click **Add**.

Port Forwarding:		<input type="radio"/> Disable <input checked="" type="radio"/> Enable		<button>Apply Changes</button>		
Application: FTP Server ▼						
Comment	Local IP	Local Port	Protocol	Remote IP	Remote Port	Interface
FTP Server	192.168.1.136	21	TCP ▼	192.168.2.100	21	Any ▼

Step 3 Assign a fixed IP address to the host where the server locates.

1. Navigate to **LAN > LAN > DHCP**.
2. Click **MAC-Based Assignment**.
3. Set **MAC Address** of the host of the server, which is **D4-61-DA-1B-CD-89** in this example.
4. Set **Assigned IP Address** for the server host, which is **192.168.1.136** in this example.

MAC Address (xx-xx-xx-xx-xx-xx):	D4-61-DA-1B-CD-89
Assigned IP Address (xxx.xxx.xxx.xxx):	192.168.1.136

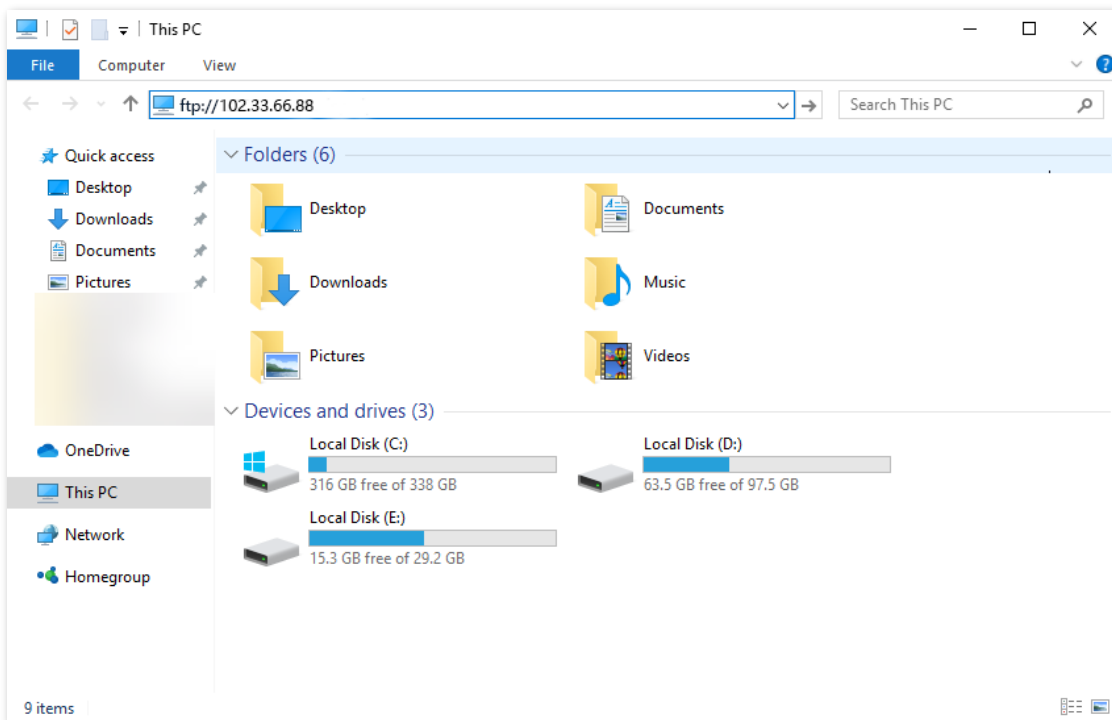
5. Click **Assign IP**.

---End

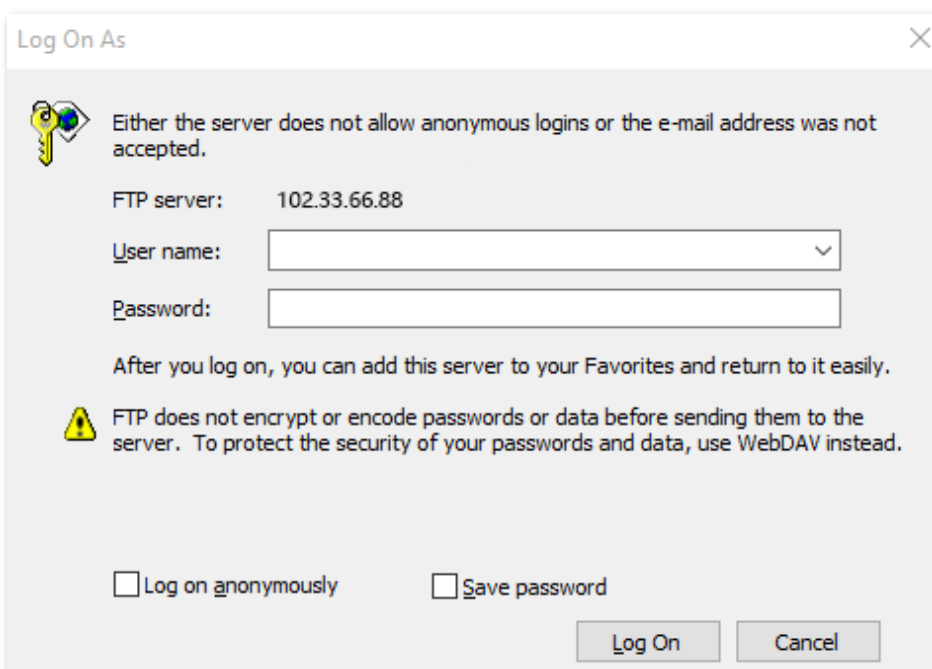
After the configuration is completed, users from the internet can access the FTP server by visiting *"Intranet service application layer protocol name://WAN IP address of the ONT"*. If the remote port number is different from the default intranet service port number, the visiting address should be: *"Intranet service application layer protocol name://WAN IP address of the ONT:Remote port number"*. In this example, the address is **"ftp://102.33.66.88"**. You can find the WAN IP address of the ONT in [Device status](#).

To access the FTP server from the internet:

Open the file explorer on a computer that can access the internet, and visit **ftp://102.33.66.88**.



Enter the user name and password to access the resources on the FTP server.



If you want to access the server within a LAN using a domain name, refer to the solution [Dynamic DNS](#) + [Port Forwarding](#).



After the configuration is completed, if internet users cannot access the FTP server, try the following methods:

- Ensure that the LAN port number configured in the port forwarding function is the same as the service port number set on the server.
- Close the firewall, antivirus software and security guards on the host of the FTP server and try again.

8.2.5 URL blocking

Overview

The URL blocking function enables you to block LAN clients from accessing certain websites by specifying a Fully Qualified Domain Name (FQDN) or keyword.

To access the page, [log in to the web UI](#) of the ONT and navigate to **Services > Firewall > URL Blocking**. The rule added is shown in the **URL Blocking Table**.

URL Blocking	
<input checked="" type="radio"/> Disable <input type="radio"/> Enable	<button>Apply Changes</button>
FQDN: <input type="text"/>	<button>Add</button>
URL Blocking Table	
Select	FQDN

Parameter description

Parameter	Description
URL Blocking	Specifies whether to enable the URL blocking function.
FQDN	Specifies the domain name that you want to block LAN clients from accessing. An FQDN, sometimes also referred to as an absolute domain name, is a domain name that specifies its exact location in the tree hierarchy of the Domain Name System (DNS). It specifies all domain levels, including the top-level domain and the root zone.

Block clients from accessing certain websites

Assume that you use the ONT to provide internet access at your home. You want your children to focus on studying rather than social media, such as Facebook, Twitter or Instagram. You can use URL blocking to reach the requirement.

Procedure:

Step 1 [Log in to the web UI](#) of the ONT.

Step 2 Navigate to **Services > Firewall > URL Blocking**.

Step 3 Select **Enable** for **URL Blocking**, and click **Apply Changes**.

Step 4 Enter **Facebook** in **FQDN** and click **Add**. Repeat this step for blocking **Twitter** and **Instagram**.

URL Blocking:	<input type="radio"/> Disable <input checked="" type="radio"/> Enable	<button>Apply Changes</button>
FQDN:	<input type="text" value="Facebook"/>	<button>Add</button>

---End

After the configuration is completed, Facebook, Twitter and Instagram are not accessible through the ONT.

8.2.6 DMZ

Overview

A DMZ host on a LAN is free from restrictions in communicating with the internet. It is useful for getting better and smoother experiences in video conferences and online games. You can also set the host of a server within the LAN as a DMZ host when in need of accessing the server from the internet.



- A DMZ host is not protected by the firewall of the router. Hackers may leverage the DMZ host to attack your LAN. Therefore, enable the DMZ function only when necessary.
- Hackers may leverage the DMZ host to attack the local network. Do not use the DMZ host function randomly.
- Security software, antivirus software and the built-in OS firewall of the computer may cause DMZ function failures. Disable them when using the DMZ function. If the DMZ function is not required, you are recommended to disable it and enable your firewall, security and antivirus software.

To access the page, [log in to the web UI](#) of the ONT and navigate to **Services > Firewall > DMZ**.

DMZ Host:	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
DMZ Host IP Address:	<input type="text" value="0.0.0.0"/>

Parameter description

Parameter	Description
DMZ Host	Specifies whether to enable the DMZ host function.
DMZ Host IP Address	Specifies the IP address of the LAN host to be set as the DMZ host.

Enable internet users to access LAN resources

Scenario: You have set up an FTP server within your LAN.

Requirement: Open the FTP server to internet users and enable family members who are not at home to access the resources of the FTP server from the internet.

Solution: You can configure the DMZ host function to reach the requirement.

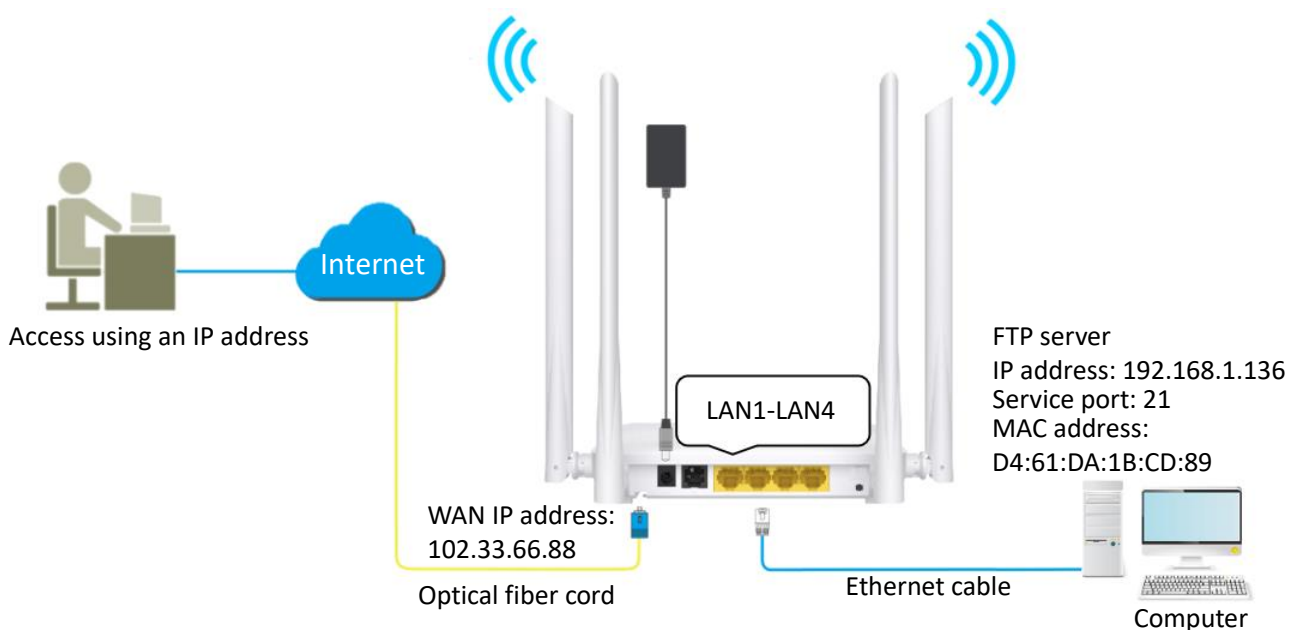
Assume that the information of the FTP server includes:

- IP address: 192.168.1.136
- MAC address: D4:61:DA:1B:CD:89
- Service port: 21
- WAN IP address of the router: 102.33.66.88



TIP

Please ensure that the router obtains a public IP address public. This function may not work on a host with an IP address of a private network or an intranet IP address assigned by ISPs that start with 100. Common IPv4 addresses are classified into class A, class B and class C. Private IP addresses of class A range from 10.0.0.0 to 10.255.255.255. Private IP addresses of class B range from 172.16.0.0 to 172.31.255.255. Private IP addresses of class C range from 192.168.0.0 to 192.168.255.255.



Procedure:

Step 1 [Log in to the web UI](#) of the ONT.

Step 2 Set the server host as the DMZ host.

1. Navigate to **Services > Firewall > DMZ**.
2. Select **Enable** for **DMZ Host**.
3. Enter the IP address of the server host, which is **192.168.1.136** in this example.
4. Click **Apply Changes**.

DMZ Host:	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
DMZ Host IP Address:	<input type="text" value="192.168.1.136"/>

Step 3 Assign a fixed IP address to the host where the server locates.

1. Navigate to **LAN > LAN > DHCP**.
2. Click **MAC-Based Assignment**.
3. Enter the **MAC Address** of the host of the server, which is **D4-61-DA-1B-CD-89** in this example.
4. Enter the assigned IP Address for the server host, which is **192.168.1.136** in this example.

MAC Address (xx-xx-xx-xx-xx-xx):	<input type="text" value="D4-61-DA-1B-CD-89"/>
Assigned IP Address (xxx.xxx.xxx.xxx):	<input type="text" value="192.168.1.136"/>

5. Click **Assign IP**.

---End

After the configuration is completed, users from the internet can access the FTP server by visiting "*Intranet service application layer protocol name://WAN IP address of the ONT*". If the intranet service port number is not the default number, the accessing address should be: "*Intranet service application layer protocol name://WAN IP address of the ONT:Intranet service port number*".

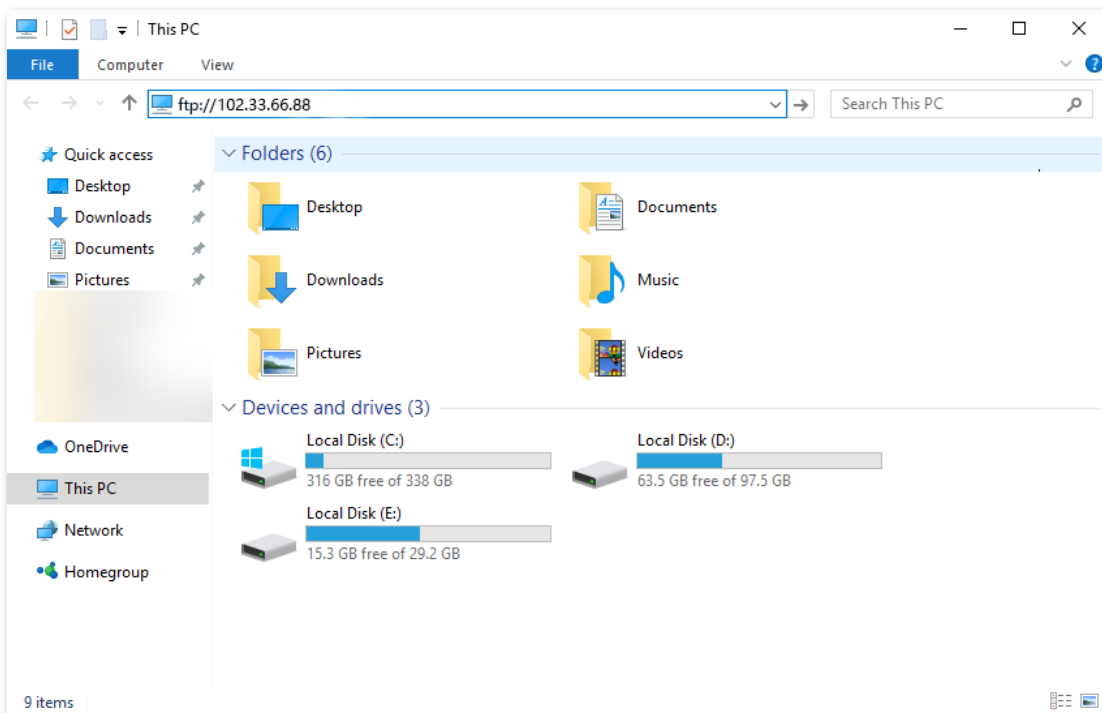


If the default intranet service port number is 80, please change the service port number to an uncommon one (1024–65535), such as 9999.

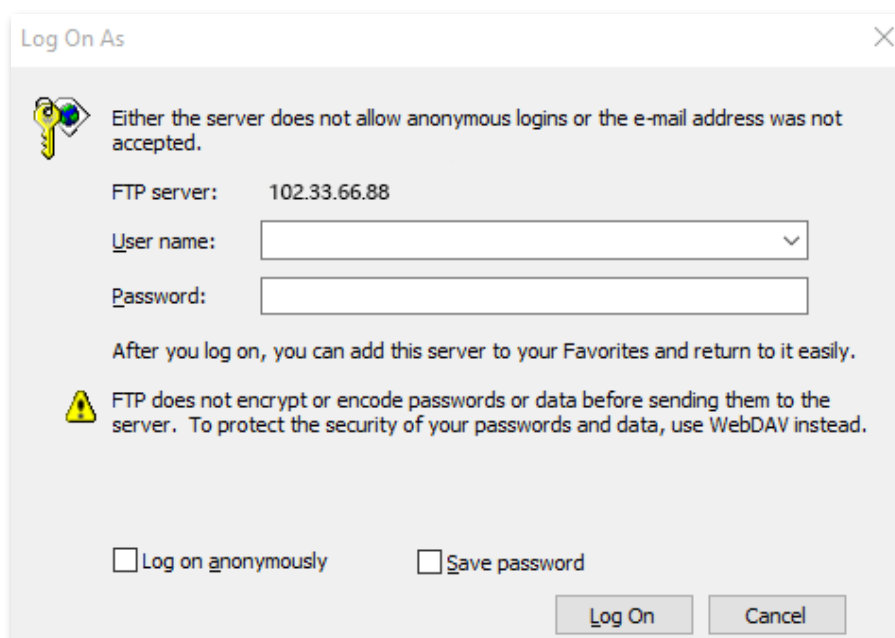
In this example, the address is "**ftp://102.33.66.88**". You can find the WAN IP address of the ONT in [Device status](#).

To access the FTP server from the internet:

Open the file explorer on a computer that can access the internet, and visit **ftp://102.33.66.88**.



Enter the user name and password to access the resources on the FTP server.



If you want to access the server within a LAN using a domain name, refer to the solution [DMZ](#) + [Dynamic DNS](#).



After the configuration is completed, if internet users still cannot access the FTP server, close the firewall, antivirus software and security guards on the host of the FTP server and try again.

8.2.7 ICMP packets limit

On this page, you can set the threshold to limit the Internet Control Message Protocol (ICMP) packets rate. The greater the value, the better the protection against ICMP flood attack. The value range is 1 to 100.

To access the page, [log in to the web UI](#) of the ONT and navigate to **Services > Firewall > ICMP Packets Limit**.

ICMP Packets Limit:	<input type="text" value="20"/>	pps
---------------------	---------------------------------	-----

8.2.8 DDoS

DDoS is short for Distributed Denial of Service. DDoS attack indicates the distributed denial of service attack. The attack allows an attacker to exhaust the resources of a system, making the system unable to properly provide services.

To access the page, [log in to the web UI](#) of the ONT and navigate to **Services > Firewall > DDOS**.

DDoS Protection	
DDoS Protection:	<input type="checkbox"/>
ICMP Flood Attack Filtering:	<input type="text" value="Low"/>
TCP Flood Attack Filtering:	<input type="text" value="Low"/>
ARP Flood Attack Filtering:	<input type="text" value="Low"/>

Parameter description

Parameter	Description
DDoS Protection	Specifies whether to enable the DDoS Protection function.
ICMP Flood Attack Filtering	Specifies the level of protection for the ICMP flood attack filtering to prevent the Internet Control Message Protocol (ICMP) flood attack, including Low , Middle and High . The higher the level, the less data packets that can pass through, which means the more ICMP packets will be filtered.
TCP Flood Attack Filtering	Specifies the level of protection for the TCP flood attack filtering to prevent the Transmission Control Protocol (TCP) flood attack, including Low , Middle and High . The higher the level, the less data packets that can pass through, which means the more SYN packets will be filtered.

Parameter	Description
ARP Flood Attack Filtering	Specifies the level of protection for the ARP flood attack filtering to prevent the Address Resolution Protocol (ARP) flood attack, including Low , Middle and High . The higher the level, the less data packets that can pass through, which means the more ARP packets will be filtered.

9 VoIP

This guide is for reference only and does not imply that the product supports all functions in the guide. The functions may differ with different product models or different versions of the same model. The actual product prevails.

The VoIP function enables telephone calls to be made and received over an IP network.

9.1 Set VoIP proxy

Before you can make phone calls on the phone connected to the ONT, you need to complete registration with the SIP server.

To access the page, [log in to the web UI](#) of the ONT and navigate to **VoIP > VoIP > Basic**.

In the **Main Proxy** and **Backup Proxy** modules, you can complete the registration. After the parameters are properly configured, click **Apply** on the bottom of the page to enable the settings to take effect.

Main Proxy	
Display Name	<input type="text"/>
Number	<input type="text"/>
Login ID	<input type="text"/>
Password	<input type="text"/>
Proxy	<input type="checkbox"/> Enable
Proxy Addr	<input type="text"/>
Proxy Port	<input type="text" value="5060"/>
SIP Subscribe	<input type="checkbox"/> Enable
SIP Domain	<input type="text"/>
Reg Expire (sec)	<input type="text" value="3600"/>
Outbound Proxy	<input type="checkbox"/> Enable
Outbound Proxy Addr	<input type="text"/>
Outbound Proxy Port	<input type="text" value="5060"/>
Enable Session timer	<input checked="" type="checkbox"/> Enable
Session Expire (sec)	<input type="text" value="1800"/>
Register Status	Disabled

Parameter description

Parameter	Description
Display Name	Specifies the caller name that will be displayed on the peer side.
Number	Specifies the phone number of your telephone.
Login ID	Specify the login ID and password to register with the SIP server.
Password	
Proxy	You can choose to enable the SIP proxy server function as required. When enabled, you need to enter the IP address and port of the SIP proxy server.
Proxy Addr	
Proxy Port	
SIP Subscribe	Used to create a subscription between the client application that wishes to obtain service information and the information provider.
SIP Domain	Specifies the domain name for SIP service registration.
Reg Expire (sec)	Specifies the period after which the SIP registration expires.
Outbound Proxy	When it is enabled, all outgoing requests will be sent to this outbound proxy server.
Outbound Proxy Addr	Specify the IP address and port number of the SIP Outbound Proxy server.
Outbound Proxy Port	
Enable Session timer	When it is enabled, the ONT periodically checks the status of a SIP session.
Session Expire (sec)	Specifies the interval at which the ONT checks the status of a SIP session.
Register Status	Specifies the SIP registration status.

9.2 Change advanced SIP settings

To access the page, [log in to the web UI](#) of the ONT and navigate to **VoIP > VoIP > Advanced**.

In the **SIP Advanced** module, you can change advanced SIP settings.

Change the parameters as required by your ISP, or keep the default value if you are not sure. After the parameters are properly configured, click **Apply** on the bottom of the page to enable the settings to take effect.

SIP Advanced	
SIP Port	<input type="text" value="5060"/>
Media Port	<input type="text" value="9000"/>
DTMF Relay	<input type="text" value="RFC2833"/>
DTMF RFC2833 Payload Type	<input type="text" value="96"/>
DTMF RFC2833 Packet Interval	<input type="text" value="10"/> (msec) (Must be multiple of 10msec)
Use DTMF RFC2833 PT as Fax/Modem RFC2833 PT	<input checked="" type="checkbox"/> Enable
Fax/Modem RFC2833 Payload Type	<input type="text" value="101"/>
Fax/Modem RFC2833 Packet Interval	<input type="text" value="10"/> (msec) (Must be multiple of 10msec)
SIP INFO Duration (ms)	<input type="text" value="250"/>
Call Waiting	<input checked="" type="checkbox"/> Enable
Call Waiting Caller ID	<input type="checkbox"/> Enable
Caller ID Mode	<input type="text" value="FSK_BELLCORE"/>
Reject Direct IP Call	<input type="checkbox"/> Enable
Send Caller ID hidden	<input type="checkbox"/> Enable
call transfer	<input checked="" type="checkbox"/> Enable
3 way conference	<input checked="" type="checkbox"/> Enable
conference on server/CPE	<input type="radio"/> server <input checked="" type="radio"/> CPE
conference-uri	<input type="text"/>

Parameter description

Parameter	Description
SIP Port	Specifies the port used for SIP calls.
Media Port	Specifies the port for voice streams using the Real-time Transport Protocol (RTP).
DTMF Relay	Dual-tone Multi-frequency (DTMF) Relay enables the ONT to send DTMF digits over IP. You can choose the DTMF relay type here, which includes RFC2833 , SIP INFO , Inband and DTMF_delete .

Parameter	Description
DTMF RFC2833 Payload Type	When DTMF Relay is set to RFC2833 , you need to specify these five parameters. If you are not sure, keep the default values.
DTMF RFC2833 Packet Interval	
Use DTMF RFC2833 PT as Fax/Modem RFC2833 PT	
Fax/Modem RFC2833 Payload Type	
Fax/Modem RFC2833 Packet Interval	
SIP INFO Duration (ms)	When DTMF Relay is set to SIP INFO , you need to specify the SIP INFO duration.
Call Waiting	Specifies whether to enable the call waiting function, which allows you to suspend a telephone call already in progress to accept a second call, or switch between calls.
Call Waiting Caller ID	Specifies whether to display the caller ID of the waiting call.
Caller ID Mode	Specifies how the caller ID is obtained. It is automatically set based on your country code. Do not modify it unless necessary.
Reject Direct IP Call	Specifies whether to reject or accept direct IP calls.
Send Caller ID hidden	Specifies whether to hide your caller ID when making phone calls.
call transfer	Specifies whether to enable the call transfer function, which allows you to relocate an existing telephone call to another phone.
3 way conference	Specifies whether to enable the 3-way conference function, which allows you to talk with 2 people at the same time using your telephone.
conference on server/CPE	Specifies the location of conferences.
conference-uri	Specifies the URI where the conference is made.

9.3 Set the forward mode

By setting the forward mode, incoming phone calls can be forwarded to another phone number under different circumstances.

To access the page, [log in to the web UI](#) of the ONT and navigate to **VoIP > VoIP > Advanced**.

In the **Forward Mode** module, you can configure the forward mode. After the parameters are properly configured, click **Apply** on the bottom of the page to enable the settings to take effect.

Forward Mode	
Immediate Forward to	<input checked="" type="radio"/> off <input type="radio"/> VoIP
Immediate Number	<input type="text"/>
Busy Forward to	<input checked="" type="radio"/> off <input type="radio"/> VoIP
Busy Number	<input type="text"/>
No Answer Forward to	<input checked="" type="radio"/> off <input type="radio"/> VoIP
No Answer Number	<input type="text"/>
No Answer Time (sec)	<input type="text" value="0"/>

Parameter description

Parameter	Description
Immediate Forward to	You can enable or disable Immediate Forward. Immediate Forward prevails Busy Forward and No Answer Forward.
Immediate Number	<ul style="list-style-type: none"> off: Immediate Forward is disabled. VoIP: Immediate Forward is enabled, and phone calls will be forwarded immediately to the phone number you specified in Immediate Number.
Busy Forward to	You can enable or disable Immediate forward. To enable Busy Forward, disable Immediate Forward first.
Busy Number	<ul style="list-style-type: none"> off: Busy Forward is disabled. VoIP: Busy Forward is enabled, and phone calls will be forwarded to the phone number you specified in Busy Number when the line is busy.
No Answer Forward to	You can enable or disable No Answer Forward. To enable No Answer Forward, disable Immediate Forward and Busy Forward first.
No Answer Number	<ul style="list-style-type: none"> off: No Answer Forward is disabled. VoIP: No Answer Forward is enabled, and phone calls will be forwarded to the phone number you specified in No Answer Number when the calls are not answered after the time set in No Answer Time (sec) is reached.
No Answer Time (sec)	

9.4 Set speed dial rules

By adding speed dial rules, you can make phone calls quickly by pressing the speed name plus # instead of the original numbers on the keypad of the telephone.

To access the page, [log in to the web UI](#) of the ONT and navigate to **VoIP > VoIP > Advanced**.

In the **Speed Dial** module, you can set speed dial rules. After the parameters are properly configured, click **Apply** on the bottom of the page to enable the settings to take effect.

Speed Dial			
Position	Speed Name	Phone Number	Select
0	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
9	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

Parameter description

Parameter	Description
Speed Name	You can set Speed Name for each commonly used number to facilitate making phone calls. You only need to press the speed name plus # on the telephone to dial a certain phone number that you specify in Phone Number .
Phone Number	

9.5 Abbreviated dial

By adding abbreviated dial rules, you can make phone calls by dialing the abbreviated number rather than the full number.

To access the page, [log in to the web UI](#) of the ONT and navigate to **VoIP > VoIP > Advanced**.

In the **Abbreviated Dial** module, you can set abbreviated dial rules. After the parameters are properly configured, click **Apply** on the bottom of the page to enable the settings to take effect.

Abbreviated Dial	
Abbreviated Name	Phone Number
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>

9.6 Set a dial plan

The dial plan function is used to analyze the number dialed by the call participant and decides which number should be dialed or which function should be selected. With the help of the dial plan, the telephone network, or the telephone system itself analyses and recognizes the dialed number and generates the proper connection request.

To access the page, [log in to the web UI](#) of the ONT and navigate to **VoIP > VoIP > Advanced**.

In the **Dial plan** module, you can set a dial plan. After the parameters are properly configured, click **Apply** on the bottom of the page to enable the settings to take effect.

Dial plan	
Enable Dialplan	<input type="radio"/> on <input checked="" type="radio"/> off
Dial plan	<input type="text"/>

Parameter description

Parameter	Description
Enable Dialplan	Specifies whether to enable a dial plan.

Parameter	Description
Dial plan	Specifies the name of dial plan.

9.7 Set coding type

Codecs enable the ONT to compress digital voice data to reduce bandwidth usage per call. Change the settings only when necessary.

To access the page, [log in to the web UI](#) of the ONT and navigate to **VoIP > VoIP > Advanced**.

In the **Codec** module, you can set the codec type. After the parameters are properly configured, click **Apply** on the bottom of the page to enable the settings to take effect.

Codec

RTP Redundant (First precedence)

Codec

Disabled ▾

Payload Type

121

Type	Packetization	Precedence									Disable
		1	2	3	4	5	6	7	8	9	
G711-ulaw	20 ms ▾	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G711-alaw	20 ms ▾	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G729	20 ms ▾	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G723	30 ms ▾	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
G726-16k	20 ms ▾	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G726-24k	20 ms ▾	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G726-32k	20 ms ▾	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G726-40k	20 ms ▾	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
G722	10 ms ▾	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Parameter description

Parameter	Description
Codec	Specifies the coding type used to compress digital voice data, which has higher priority over other coding types.
Payload Type	Specifies the payload type value for digital voice data coding.

Parameter	Description
Type	Specifies the coding type used to compress digital voice data.
Packetization	Specifies the packetization rate of digital voice data.
Disable	Used to disable the selected codec type.

9.8 Set a hotline

By setting a hotline for the telephone, the telephone dials the phone number you set if there is no dialing action within a period after you pick up the phone set.

To access the page, [log in to the web UI](#) of the ONT and navigate to **VoIP > VoIP > Advanced**.

In the **Hot Line** module, you can set a hotline. After the parameters are properly configured, click **Apply** on the bottom of the page to enable the settings to take effect.

Hot Line	
Use Hot Line	<input checked="" type="radio"/> Disable <input type="radio"/> Immediately <input type="radio"/> Delay
Hot Line Number	<input type="text"/>

Parameter description

Parameter	Description
	Specifies how to use the hotline.
Use Hot Line	<ul style="list-style-type: none"> – Disable: The hotline is disabled. – Immediately: When you pick up the phone set, the telephone immediately dials the phone number you set. – Delay: When you pick up the phone set, the telephone dials the phone number you set after 5 seconds.
Hot Line Number	Specifies the hotline number to be dialed when no dialing action is performed within a specific period after you pick up the phone set.

9.9 Set the Don't Disturb mode

If you enable the Don't Disturb (DND) mode, incoming calls will be denied during the specified period.

To access the page, [log in to the web UI](#) of the ONT and navigate to **VoIP > VoIP > Advanced**.

In the **DND (Don't Disturb)** module, you can set the Don't Disturb mode. After the parameters are properly configured, click **Apply** on the bottom of the page to enable the settings to take effect.

Choose the desired mode for your phone:

- **Always:** All phone calls are denied all the time.
- **Enable:** Phone calls are denied during the specified period.
- **Disable:** The DND mode is disabled, and all phone calls are accepted.

DND (Don't Disturb)	
DND Mode	<input type="radio"/> Always <input type="radio"/> Enable <input checked="" type="radio"/> Disable
From	<input type="text" value="00"/> : <input type="text" value="00"/> (hh:mm)
To	<input type="text" value="00"/> : <input type="text" value="00"/> (hh:mm)

Parameter description

Parameter	Description
DND Mode	Specifies whether the DND mode is enabled.
From	Specify the period during which the DND mode is enabled when Enable is selected for DND Mode .
To	

9.10 Set an alarm

To access the page, [log in to the web UI](#) of the ONT and navigate to **VoIP > VoIP > Advanced**.

In the **Alarm** module, you can set an alarm on and the telephone will ring at the specified time. After the parameters are properly configured, click **Apply** on the bottom of the page to enable the settings to take effect.

Alarm	
Enable	<input type="checkbox"/>
Time	<input type="text" value="0"/> : <input type="text" value="0"/> (hh:mm)

Parameter description

Parameter	Description
Enable	Specifies whether the alarm is enabled.
Time	Specifies the time at which the telephone rings.

9.11 Set fax protocol

To access the page, [log in to the web UI](#) of the ONT and navigate to **VoIP > VoIP > Advanced**.

In the **T.38(FAX)** module, you can send and receive faxes when the peer device also supports the T.38 fax protocol. After the function is enabled, click **Apply** on the bottom of the page to enable the settings to take effect.

T.38(FAX)	
T.38	<input type="checkbox"/> Enable

10 Advance

This guide is for reference only and does not imply that the product supports all functions in the guide. The functions may differ with different product models or different versions of the same model. The actual product prevails.

10.1 Advanced settings

10.1.1 Routing

Overview

On this page, you can add, modify and delete static route rules. In addition, you can view the route table of the ONT.

Routing is the act of choosing an optimal path to transfer data from a source address to a destination address. A static route is a special route that is manually configured and has the advantages of simplicity, efficiency and reliability. Proper static routing can reduce routing problems and overload of routing data flow, and improve the forwarding speed of data packets.

After the static route is established, all data whose destination address is the destination network of the static route are directly forwarded to the next hop through the static route interface.

To access the page, [log in to the web UI](#) of the ONT and navigate to **Advance > Advance > Routing**.

Enable:	<input checked="" type="checkbox"/>
Destination:	<input type="text"/>
Subnet Mask:	<input type="text"/>
Next Hop:	<input type="text"/>
Metric:	<input type="text"/>
Interface:	<input type="text" value="Any"/> ▼

Static Route Table						
Select	State	Destination	Subnet Mask	Next Hop	Metric	Interface

Parameter description

Parameter	Description
Add Route	Used to add a new static route rule.
Update	Used to update your modification to an existing rule.
Delete Selected	Used to delete the selected rule.
Show Routes	Used to display the commonly used routes of the ONT.
Select	Select existing rules to update or delete them.
State	Specifies the status of a rule, including Enable and Disable .
Destination	Specifies the IP address of the destination network.
Subnet Mask	Specifies the subnet mask of the destination network.
Next Hop	Specifies the ingress IP address of the next hop route after the data packet exits from the WAN interface of the ONT.
Metric	Specifies the priority of the routing rule. The smaller the number, the higher the priority. When the destination networks of two rules are the same, packets will be forwarded according to the rule with smaller metric.
Interface	Specifies the interface of the ONT that the packet exits from.

Add a new static route rule

- Step 1** [Log in to the web UI](#) of the ONT.
- Step 2** Navigate to **Advance > Advance > Routing**.
- Step 3** Select **Enable** as required.
- Step 4** Set **Destination**, **Subnet Mask**, **Next Hop**, **Metric** and **Interface** as required.

Step 5 Click **Add Route**.

Enable:	<input checked="" type="checkbox"/>
Destination:	<input type="text"/>
Subnet Mask:	<input type="text"/>
Next Hop:	<input type="text"/>
Metric:	<input type="text"/>
Interface:	Any ▾

---End

After the configuration is completed, the static rule will be displayed in **Static Route Table**.

Modify a static rule

Step 1 [Log in to the web UI](#) of the ONT.

Step 2 Navigate to **Advance > Advance > Routing**.

Step 3 Select a static route rule, and it will appear in the configuring part. The following figure is for reference only.

Enable:	<input checked="" type="checkbox"/>
Destination:	<input type="text" value="192.168.1.2"/>
Subnet Mask:	<input type="text" value="255.255.255.255"/>
Next Hop:	<input type="text" value="192.168.10.1"/>
Metric:	<input type="text" value="12"/>
Interface:	Any ▾

Add Route
Update
Delete Selected
Show Routes

Static Route Table						
Select	State	Destination	Subnet Mask	Next Hop	Metric	Interface
<input checked="" type="radio"/>	Enable	192.168.1.2	255.255.255.255	192.168.10.1	12	---

Step 4 Modify the parameters of the rule as required.

Enable:	<input checked="" type="checkbox"/>
Destination:	<input type="text" value="192.168.1.2"/>
Subnet Mask:	<input type="text" value="255.255.255.255"/>
Next Hop:	<input type="text" value="192.168.10.1"/>
Metric:	<input type="text" value="12"/>
Interface:	<input type="text" value="Any"/>

Step 5 Click **Update**.

---End

After the configuration is completed, the updated parameters of the static rule will be displayed in **Static Route Table**.

Delete an existing rule

To delete an existing rule, select the rule in **Static Route Table** and click **Delete Selected**. The following figure is for reference only.

Enable:	<input checked="" type="checkbox"/>
Destination:	<input type="text" value="192.168.1.2"/>
Subnet Mask:	<input type="text" value="255.255.255.255"/>
Next Hop:	<input type="text" value="192.168.10.1"/>
Metric:	<input type="text" value="12"/>
Interface:	<input type="text" value="Any"/>

Add Route
Update
Delete Selected
Show Routes

Static Route Table						
Select	State	Destination	Subnet Mask	Next Hop	Metric	Interface
<input checked="" type="radio"/>	Enable	192.168.1.2	255.255.255.255	192.168.10.1	12	---

Show commonly used routes

Click **Show Routes**, and you will find the commonly used routes in the prompt window. The following figure is for reference only.

Destination	Subnet Mask	Next Hop	Metric	Interface
0.0.0.0	0.0.0.0	*	0	ppp0
10.11.122.1	255.255.255.255	*	0	ppp0



- The route with 0.0.0.0 as both destination and subnet mask is the default route. When no perfectly matched route is found for a packet, the packet will be forwarded through the default route.
- 0.0.0.0 as the next hop indicates that the ONT is directly connected to the destination network.

10.1.2 SNMP

The Simple Network Management Protocol (SNMP) is the most widely used network management protocol in TCP or IP networks. SNMP enables you to remotely manage all your network devices compliant with this protocol, such as monitoring the network status, changing network device settings, and receiving network event alarms.

SNMP allows automatic management of devices from various vendors regardless of physical differences among the devices.

SNMP management framework

The SNMP management framework consists of the SNMP manager, SNMP agent and Management Information Base (MIB).

- **SNMP manager:** It is a system that controls and monitors network nodes using the SNMP protocol. The SNMP manager most widely used in network environments is Network Management System (NMS). An NMS can be a dedicated network management server, or an application that implements management functions in a network device.
- **SNMP agent:** It is a software module in a managed device. The module is used to manage data about the device and report the management data to an SNMP manager.
- **MIB:** It is a collection of managed objects. It defines a series of attributes of managed objects, including names, access permissions and data types of objects. Each SNMP agent has its MIB. An SNMP manager can read and/or write objects in the MIB based on the permissions assigned to the SNMP manager.

SNMP operations

There are mainly three operations based on SNMP:

- **Get:** The SNMP manager sends a request to retrieve the value of a variable or list of variables.
- **Set:** The SNMP manager sends a request to change the value of a variable or list of variables.
- **Trap:** The SNMP agent notifies the SNMP manager of significant events by an unsolicited SNMP message.

An SNMP manager manages SNMP agents in an SNMP network. The SNMP manager exchanges management information with the SNMP agents using the SNMP protocol. The ONT functions as an SNMP agent.

The ONT is compatible with SNMP V1 and SNMP V2C and adopts the community authentication mechanism.

To access the page, [log in to the web UI](#) of the ONT and navigate to **Advance > Advance > SNMP**.

SNMP:	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
System Description:	<input type="text" value="System Description"/>
System Contact:	<input type="text" value="System Contact"/>
SystemName:	<input type="text" value="HG15"/>
System Location:	<input type="text" value="System Location"/>
System Object ID:	<input type="text" value="1.3.6.1.4.1.16972"/>
Trap IP Address:	<input type="text" value="192.168.1.254"/>
Community name (read-only):	<input type="text" value="public"/>
Community name (write-only):	<input type="text" value="public"/>

Parameter description

Parameter	Description
SNMP	Specifies whether to enable the SNMP agent function.
System Description	Specifies a description of the ONT, which can be anything you like and is used for identification.
System Contact	Specifies the contact information of the ONT.
SystemName	Specifies the name of ONT.
System Location	Specifies the place where the ONT is located.
System Object ID	Specifies the object ID of the ONT in the MIB, which can be used by the SNMP manager to identify and manage the ONT.
Trap IP Address	Specifies the destination IP address of the SNMP trap. Make sure that the ONT and the SNMP manager are reachable to each other.
Community name (read-only)	Specify the community names which act as passwords for the interaction between the SNMP manager and SNMP agent.
Community name (write-only)	<ul style="list-style-type: none"> – Community name (read-only): It is used to authenticate the Get request. – Community name (write-only): It is used to authenticate the Set request.

10.2 IP QoS settings

The IP quality-of-service (IP QoS) feature enables you to prioritize, control and gather accounting statistics. IP QoS is a security mechanism of the network and a technology to solve problems such as network delay and congestion. When the network is overloaded and congested, reasonable IP QoS settings can ensure that important traffic is not delayed or discarded and the network runs efficiently.

10.2.1 Configuration guidance

Configure the IP QoS policy

Step	Task	Description
1	Configure the QoS rule template	Used to configure the rule template. If the WAN configuration is configured, the rule template should be reconfigured.
2	Configure the QoS queue	Used to configure the QoS policy and queue.
3	Configure the QoS bandwidth	Used to configure the bandwidth of different type of WAN.

Configure the IP QoS classification rules

Step	Task	Description
1	Assign IP precedence/DSCP/802.1p	Used to configure the mapping relationship between the DSCP priority and queues, and the mapping relationship between the 802.1p priority and queues.
2	Specify traffic classification rules	When the uplink bandwidth is limited, based on the port, Ethernet type, IP/protocol and MAC address classification, some data is preferentially forwarded to different queues.

Configure the IP QoS traffic shaping rules

Task	Description
Configure IP QoS traffic shaping rules	Used to configure the speed limit of uplink traffic.

10.2.2 Configure the QoS rule template

To access the page, [log in to the web UI](#) of the ONT and navigate to **Advance > IP QoS > QoS Policy**.

On this page, you can configure the QoS rule template to preferentially forward some data to different queues according to different service types when the uplink bandwidth is limited. The IP QoS function is disabled by default. You must enable the IP QoS function before configuration.

IP QoS	<input type="radio"/> Disable	<input checked="" type="radio"/> Enable
QoS Rule Template Config		
This page is used to configure the Rule Template.If the WAN configuration is configured, the rule template should be reconfigured.		
Rule Template:	<input type="text" value="TR069,INTERNET"/>	

Parameter description

Parameter		Description
IP QoS		Specifies whether to enable the IP QoS function.
QoS Rule Template Config	Rule Template	Used to configure the rule template of the IP QoS. Choose the proper rule template as required.
		– TR069, INTERNET
		– TR069, VOIP, INTERNET
		– TR069, OTHER, INTERNET
		– TR069, VOIP, OTHER, INTERNET
		– NONE

10.2.3 Configure the QoS queue

To access the page, [log in to the web UI](#) of the ONT and navigate to **Advance > IP QoS > QoS Policy**.

On this page, you can set the queue mode including **PRIO** and **WRR**. The IP QoS function is disabled by default. You must enable the IP QoS function before configuration.

QoS Queue Config				
This page is used to configure the QoS policy and Queue. If select PRIO of policy, the lower numbers imply greater precedence. If select WRR of policy, please input the weight of this queue. Default is 40:30:20:10. After configuration, please click 'Apply Changes'				
Policy:		<input checked="" type="radio"/> PRIO	<input type="radio"/> WRR	
Queue	Policy	Priority	Weight	Enable
Q1	PRIO	1	--	<input checked="" type="checkbox"/>
Q2	PRIO	2	--	<input checked="" type="checkbox"/>
Q3	PRIO	3	--	<input checked="" type="checkbox"/>
Q4	PRIO	4	--	<input checked="" type="checkbox"/>

Parameter description

Parameter	Description
QoS Queue Config	Specifies the policy of the QoS queue including PRIO and WRR . <ul style="list-style-type: none"> PRIO: A unique priority is set for each queue with this policy. The queues are serviced by priority from high to low. The advantage of this policy is that high-priority services are always processed before low-priority services. WRR: The Weighted Round Robin (WRR) algorithm schedules the queues in a polling manner based on the weights, ensuring that all queues can be serviced with certain time.
	Queue Specifies the QoS queue.
	Priority Specifies the QoS priority. It is available only when Policy is set to PRIO .
	Weight Specifies the weighted value which means the resource proportion for each queue. It is available only when Policy is set to WRR .
	Enable Specifies whether to apply the queue information.

10.2.4 Configure the QoS bandwidth

To access the page, [log in to the web UI](#) of the ONT and navigate to **Advance > IP QoS > QoS Policy**.

On this page, you can configure the total uplink bandwidth rate limit. The IP QoS function is disabled by default. You must enable the IP QoS function before configuration.

QoS Bandwidth Config	
This part is used to configure the bandwidth of different type of WAN. If select Disable, CPE will select the appropriate bandwidth based on WAN. If select Enable, User is allowed to configure specific bandwidth of WAN.	
User Defined Bandwidth:	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Total Bandwidth Limit:	<input type="text" value="100000"/> Kb

Parameter description

Parameter		Description
QoS Bandwidth Config	User Defined Bandwidth	Specifies whether to allow the user to configure the specific bandwidth of WAN. It is disabled by default. It is recommended to keep the default settings.
	Total Bandwidth Limit	Specifies the rate of the total uplink bandwidth. The value range is 64 to 1000000.

10.2.5 QoS classification

On this page, you can add, modify and delete QoS classification rules.

To access the page, [log in to the web UI](#) of the ONT and navigate to **Advance > IP QoS > QoS Classification**.

		Mark		Classification Rules				
ID	Name	DSCP Mark	802.1p	Queue	WanIf	Rule Detail	Delete	Edit

You can click **Add** to customize the QoS classification rule.

Assign IP precedence/DSCP/802.1p

To access the page, [log in to the web UI](#) of the ONT and navigate to **Advance > IP QoS > QoS Classification**.

On this page, you can configure the mapping relationship between the DSCP priority and queues, and the mapping relationship between the 802.1p priority and queues. The IP QoS function is disabled by default. You must enable the IP QoS function before configuration.

RuleName:	<input type="text" value="rule_"/>
Assign IP Precedence/DSCP/802.1p	
Precedence:	<input type="text" value="Queue 1"/>
DSCP Remarking:	<input type="text"/>
802.1p:	<input type="text"/>

Parameter description

Parameter	Description
RuleName	Specifies the rule name of the QoS classification.
Precedence	Specifies the QoS queue.
DSCP Remarking	Specifies the mechanism used for classifying network traffic on IP networks. DSCP is abbreviated for Differentiated Services Code Point.
802.1p	Specifies the 802.1P priority. Data with a larger priority value takes a higher priority to be processed.

Specify traffic classification rules

To access the page, [log in to the web UI](#) of the ONT and navigate to **Advance > IP QoS > QoS Classification**.

On this page, you can configure the traffic classification rules to preferentially forwarded some data to different queues when the uplink bandwidth is limited. The IP QoS function is disabled by default. You must enable the IP QoS function before configuration.

Specify Traffic Classification Rules			
IP QoS Rule by type:	<input type="radio"/> Port	<input type="radio"/> Ethery Type	<input checked="" type="radio"/> IP/Protocol
IP Version:	<input type="text" value="IPv4"/>		
Protocol:	<input type="text"/>		
DSCP Pattern:	<input type="text"/>		
Source IP:	<input type="text"/>		
Source Mask:	<input type="text"/>		
Destination IP:	<input type="text"/>		
Destination Mask:	<input type="text"/>		
Source Port:	<input type="text"/>	:	<input type="text"/>
Destination Port:	<input type="text"/>	:	<input type="text"/>

Parameter description

Parameter		Description
IP QoS Rule by type		Specifies the type to perform QoS flow control.
Port	Physical Port	Specifies the LAN port connected to the ONT.
Ether Type	Ethernet Type	Specifies the Ethernet type of the ONT.
IP/Protocol	IP Version	Specifies the IP version including IPv4 , IPv6 and IPv4/IPv6 .
	Protocol	Specifies the protocol type of data.
		<ul style="list-style-type: none"> – TCP: Abbreviated for Transmission Control Protocol. The connection is established through the three-way handshaking. When the communication is completed, the connection should be removed. It can only be used for end-to-end communication, such as Telnet and FTP.
		<ul style="list-style-type: none"> – UDP: Abbreviated for User Datagram Protocol. UDP data includes destination port and source port information. The communication does not require connection, and the broadcast transmission can be realized. Services using UDP include DNS and SNMP.
		<ul style="list-style-type: none"> – ICMP: Abbreviated for Internet Control Message Protocol. It is used to transmit control messages between IP hosts and ONTs, including whether the network or the host is reachable, and whether the route is available.
	DSCP Pattern	Specifies the patterns of the Differentiated Services Code Point.
	Source IP	Specify the source IP address, source subnet mask, destination IP address, destination subnet mask, source port and destination port.
	Source Mask	
	Destination IP	
	Destination Mask	
	Source Port	
	Destination Port	
MAC Address	Source MAC	Specify the source MAC address and destination MAC address.
	Destination MAC	

10.2.6 Configure traffic shaping rules

On this page, you can add and delete traffic shaping rules of IP QoS.

To access the page, [log in to the web UI](#) of the ONT and navigate to **Advance > IP QoS > Traffic Shaping**.

ID	Protocol	Source Port	Destination Port	Source IP	Destination IP	Rate(kb/s)	Delete	Edit	IP Version	Direction	WAN Interface
----	----------	-------------	------------------	-----------	----------------	------------	--------	------	------------	-----------	---------------

You can click **Add** to customize the traffic shaping rule.

IP Version:	IPv4 ▼
Interface:	ppp0 ▼
Protocol:	NONE ▼
Source IP:	<input type="text"/>
Source Mask:	<input type="text"/>
Destination IP:	<input type="text"/>
Destination Mask:	<input type="text"/>
Rate Limit:	<input type="text"/> kb/s

Parameter description

Parameter	Description
IP Version	Specifies the IP version, including IPv4 and IPv6 .
Interface	Specifies the WAN interface on which the traffic shaping rule takes effect.
Protocol	<p>Specifies the protocol type of data.</p> <ul style="list-style-type: none"> – NONE: It specifies that ICMP, TCP and UDP are all included. – TCP: Abbreviated for Transmission Control Protocol. The connection is established through the three-way handshaking. When the communication is completed, the connection should be removed. It can only be used for end-to-end communication, such as Telnet and FTP. – UDP: Abbreviated for User Datagram Protocol. UDP data includes destination port and source port information. The communication does not require connection, and the broadcast transmission can be realized. Services using UDP include DNS and SNMP. – ICMP: Abbreviated for Internet Control Message Protocol. It is used to transmit control messages between IP hosts and ONTs, including whether the network or the host is reachable, and whether the route is available.

Parameter	Description
Source IP	Specify the source IP address, source subnet mask, destination IP address, destination subnet mask, source port, destination port, source prefix length and destination prefix length.
Source Mask	
Destination IP	
Destination Mask	
Source Port	
Destination Port	
Source Prefix Length	
Destination Prefix Length	
Rate Limit	Specifies the traffic rate limit.

10.3 IPv6 settings

The ONT supports both IPv4 and IPv6 for internet access. In this module, you can enable and disable IPv6 of the ONT, and perform other IPv6-related configurations on the ONT.

10.3.1 RADVD

The Router Advertisement Daemon (RADVD) is used by system administrators in stateless auto-configuration methods of network hosts on IPV6 networks.


When IPv6 hosts configure their network interfaces, they broadcast Router Solicitation (RS) requests onto the network to discover available devices. The RADVD software answers requests with Router Advertisement (RA) messages. In addition, RADVD periodically broadcasts RA packets to the attached link to update network hosts.


To access the page, [log in to the web UI](#) of the ONT and navigate to **Advance > IPv6 > RADVD**.

RADVDEnabled:	<input type="radio"/> off <input checked="" type="radio"/> on
MaxRtrAdvInterval:	<input type="text" value="600"/>
MinRtrAdvInterval:	<input type="text" value="198"/>
AdvManagedFlag:	<input type="radio"/> off <input checked="" type="radio"/> on
AdvOtherConfigFlag:	<input type="radio"/> off <input checked="" type="radio"/> on
Prefix Mode:	<input type="text" value="Manual"/>
Prefix:	<input type="text" value="3ffe:501:ffff:100::"/>
Prefix Length:	<input type="text" value="64"/>
AdvValidLifetime:	<input type="text" value="2592000"/>
AdvPreferredLifetime:	<input type="text" value="604800"/>
AdvOnLink:	<input type="radio"/> off <input checked="" type="radio"/> on
AdvAutonomous:	<input checked="" type="radio"/> off <input type="radio"/> on
RDNSS 1:	<input type="text"/>
RDNSS 2:	<input type="text"/>
Enable ULA:	<input type="radio"/> off <input checked="" type="radio"/> on
ULA Prefix Random:	<input checked="" type="checkbox"/>
ULA Prefix:	<input type="text"/>
ULA Prefix Len:	<input type="text" value="64"/>
ULA Prefix Valid Time:	<input type="text" value="2592000"/>
ULA Prefix Preferred Time:	<input type="text" value="604800"/>

Parameter description

Parameter	Description
RADVDEnabled	Specifies whether to enable the RADVD function.
MaxRtrAdvInterval	Specify the Maximum and Minimum Router Advertisement Intervals.
MinRtrAdvInterval	They are the intervals between each router advertisement message. The router sends these messages periodically. The actual interval used is randomly selected from a value between the minimum and maximum values.

Parameter	Description
AdvManagedFlag	Specify the Advertisement Managed Flag and Advertisement Other Configuration Flag.
AdvOtherConfigFlag	<ul style="list-style-type: none"> - Advertisement Managed Flag: This flag indicates that hosts retrieve managed IPv6 addresses from a DHCPv6 server for their interfaces. - Advertisement Other Configuration Flag: This flag indicates that hosts use SLAAC to generate their IPv6 address and obtain other configuration information using DHCPv6, such as DNS information.
Prefix Mode	<p>Specifies the configuring mode of the prefix which is assigned to the IPv6 host, including Auto and Manual.</p> <ul style="list-style-type: none"> - Auto: The ONT automatically assigns a prefix to the IPv6 host. - Manual: You need to set the prefix manually.
Prefix	Specify the prefix information included in the RA message to hosts for generating their IPv6 address.
Prefix Length	
AdvValidLifetime	Specify the Advertisement Valid Lifetime and Advertisement Preferred Lifetime.
AdvPreferredLifetime	<p>When the preferred lifetime expires, the use of the prefix is not encouraged, but not prohibited. When the valid lifetime expires, the prefix becomes invalid.</p> <p> TIP</p> <p>The valid lifetime must be greater than or equal to the preferred lifetime.</p>
AdvOnLink	Specifies whether the router advertisement is on the link.
AdvAutonomous	Specifies whether the prefix in the router advertisement can be used to generate IPv6 address.
RDNSS 1/2	Specify the Recursive DNS Server (RDNSS) addresses assigned to IPv6 hosts for DNS information configuration.
Enable ULA	<p>Specifies whether to enable the Unique Local Address (ULA).</p> <p>The purpose of ULA resembles that of the private network address in IPv4. It is only used within the private network and increases stability for the IPv6 host and its use of services.</p>
ULA Prefix Random	Specifies whether to enable the ULA prefix. It is available only when Enable ULA is set to on . When ULA Prefix Random is selected, ULA Prefix cannot be set.
ULA Prefix	Specify the ULA prefix information advertised by the ONT to hosts for generating unique local addresses. ULA Prefix is available only when Enable ULA is set to on and ULA Prefix Random is deselected. ULA Prefix Len is available only when Enable ULA is set to on .
ULA Prefix Len	

Parameter	Description
ULA Prefix Valid Time	<p>Specify the valid time and preferred time of ULA prefix. It is available only when Enable ULA is set to on.</p> <p>When the preferred time expires, the use of the ULA prefix is not encouraged, but not prohibited. When the valid time expires, the ULA prefix becomes invalid. It is available only when Enable ULA is set to on.</p>
ULA Prefix Preferred Time	<p> TIP</p> <p>The valid time must be greater than or equal to the preferred time.</p>

10.3.2 DHCPv6

IPv6 hosts may automatically generate IP addresses internally using Stateless Address Autoconfiguration (SLAAC), or they may be assigned configuration with Dynamic Host Configuration Protocol version 6 (DHCPv6). When the DHCPv6 server is enabled, the ONT can assign IPv6 hosts with IP addresses, IP prefixes and other configurations required for IPv6 internet access.

To access the page, [log in to the web UI](#) of the ONT and navigate to **Advance > IPv6 > DHCPv6**.

DHCPv6 Mode:	<input type="radio"/> NONE <input checked="" type="radio"/> DHCP Server	
DHCPv6 Server Type:	<input type="radio"/> Auto <input checked="" type="radio"/> Manual	
<p>Enable the DHCPv6 Server if you are using this device as a DHCPv6 server. This page lists the IP address pools available to hosts on your LAN. The device distributes numbers in the pool to hosts on your network as they request Internet access.</p>		
IP Pool Range:	<input type="text" value="3ffe:501:ffff:100::10"/> - <input type="text" value="3ffe:501:ffff:100::100"/>	
Prefix Length:	<input type="text" value="64"/>	
Valid Lifetime:	<input type="text" value="20000"/>	seconds
Preferred Lifetime:	<input type="text" value="16000"/>	seconds
Renew Time:	<input type="text" value="5000"/>	seconds
Rebind Time:	<input type="text" value="10000"/>	seconds
Client DUID:	<input type="text" value="00:01:00:01:00:04:93:e0:00:00:00:a2:a2"/>	
<input type="button" value="Apply Changes"/> <input type="button" value="Show Client"/>		
Domain:	<input type="text"/>	<input type="button" value="Add"/>
Domain Search Table		
Select	Domain	
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/>		
Name Server IP:	<input type="text"/>	<input type="button" value="Add"/>
Name Server Table		
Select	Name Server	

Parameter description

Parameter	Description
DHCPv6 Mode	<p>You can select a DHCPv6 server mode or disable it.</p> <ul style="list-style-type: none"> – NONE: The DHCPv6 server of the ONT is disabled. – DHCP Server: The DHCPv6 server of the ONT is enabled.
DHCPv6 Server Type	<p>Specifies the type of the DHCPv6 server.</p> <ul style="list-style-type: none"> – Auto: The ONT defines the IPv6 addresses to be assigned to the IPv6 host automatically. – Manual: You need to define the IP address pool, prefix length and other required parameters for IPv6 addresses to be assigned to IPv6 hosts.
IP Pool Range	Specifies the IP address range within which the ONT can assign IPv6 addresses to the IPv6 host.
Prefix Length	Specifies the length of IPv6 prefix.
Valid Lifetime	Specify the valid lifetime and preferred lifetime of the IPv6 address assigned to IPv6 hosts.
Preferred Lifetime	When the preferred lifetime expires, communication using the IPv6 address is not encouraged, but allowed. When the valid lifetime expires, the IPv6 address becomes invalid.
Renew Time	Specifies the time before expiration when the host is expected to contact the DHCPv6 server that did the assignment to renew the lifetimes of the addresses assigned to the client.
Rebind Time	Specifies the new valid time after the IPv6 address is renewed.
Client DUID	<p>Specifies the DHCP Unique Identifier (DUID) assigned to clients.</p> <p>The DUID is used by a client to get an IP address from a DHCPv6 server, and the server compares the DUID with its database and delivers configuration data (such as the address and DNS servers) to the client.</p>
Domain	Used to configure the domain.
Domain Search Table	Specifies all domain settings.
Name Server IP	You can add a DNS server address to obtain DNS information for address resolution.
Name Server Table	

10.4 Energy saving configuration

To access the page, [log in to the web UI](#) of the ONT and navigate to **Advance > Advance Power Manage > Advance Power Manage**.

After the energy saving configuration function is ticked, the transmission power of the wireless frequency band will be reduced to save the energy. The function is disabled by default.

Energy Saving Configuration	<input type="checkbox"/>
-----------------------------	--------------------------

11 Diagnostics

This guide is for reference only and does not imply that the product supports all functions in the guide. The functions may differ with different product models or different versions of the same model. The actual product prevails.

11.1 Ping and Tracert

The ONT provides connectivity diagnosis tools, which include Ping and Tracert. You can use these tools to test the connectivity to the internet, a certain IP address or domain name.

- **Ping:** It is a utility that helps to check if an IP address or domain name is accessible or not. Ping works by sending a packet to the specified address and waits for the reply. It also measures round trip time and reports errors.
- **Tracert:** It is a utility that traces a packet from your computer to the host, and will also show the number of steps (hops) required to reach there, along with the time by each step.

To access the page, [log in to the web UI](#) of the ONT and click **Diagnostics**. Both tools include IPv4 (**Ping/Tracert**) and IPv6 (**Ping6/Tracert6**) versions. The IPv4 version is used for illustration.

Ping

Host Address:	<input type="text"/>
WAN Interface:	<input type="text" value="Any"/> ▼

Parameter description

Parameter	Description
Host Address	Specifies the IP address or domain name whose connectivity with the ONT is to be diagnosed.
WAN Interface	Specifies the WAN interface through which the packet for diagnosis is forwarded.

Tracert

Host Address:	<input type="text"/>
Number Of Tries:	<input type="text" value="3"/>
Max Hop Count:	<input type="text" value="30"/>
WAN Interface:	<input type="text" value="Any"/>

Parameter description

Parameter	Description
Host Address	Specifies the IP address or domain name of the tracert target.
Number Of Tries	Specifies the maximum number of times that the host tries to reach the host address. If all the attempts fail, it denotes network congestion and a reason for slow loading web pages and dropped connections.
Max Hop Count	Specifies the hops of the packet for diagnosis. When a packet cannot reach the destination and expires at an intermediate step, that node returns the packet and identifies itself. It denotes network congestion and a reason for slow loading web pages and dropped connections.
WAN Interface	Specifies the WAN interface through which the packet for diagnosis is forwarded.

11.2 Execute Ping to test connectivity

- Step 1** [Log in to the web UI](#) of the ONT.
- Step 2** Navigate to **Diagnostics > Diagnostics > Ping**.
- Step 3** Enter the IP address or domain name in **Host Address**, such as **www.google.com**.
- Step 4** Choose any interface from **WAN Interface**.
- Step 5** Click **Start**.

Host Address:	<input type="text" value="www.google.com"/>
WAN Interface:	<input type="text" value="Any"/>

Wait a moment. The result appears when the diagnosis finishes.

---End

11.3 Execute Traceroute to test routing

- Step 1** [Log in to the web UI](#) of the ONT.
- Step 2** Navigate to **Diagnostics > Diagnostics > Tracert**.
- Step 3** Enter the IP address or domain name in **Host Address**, such as **www.google.com**.
- Step 4** Specify the number of attempts in **Number Of Tries**.
- Step 5** Specify the number of hops in **Max Hop Count**.
- Step 6** Choose any interface from **WAN Interface**.
- Step 7** Click **Start**.

Host Address:	<input type="text" value="www.google.com"/>
Number Of Tries:	<input type="text" value="3"/>
Max Hop Count:	<input type="text" value="30"/>
WAN Interface:	<input type="text" value="Any"/> ▼

Wait a moment. The result appears when the diagnosis finishes.

---End

11.4 Inform report

On this page, you can manually inform reports to the Auto-Configuration Server (ACS).

To access this page, [log in to the web UI](#) of the ONT and navigate to **Diagnostics > Diagnostics > Inform report**.

Inform report Diagnostics

This page is used to manual inform report to acs server. The diagnostic result will then be displayed.

Inform report status:	<input type="text" value="Not Report"/>
------------------------------	---

12 Admin

This guide is for reference only and does not imply that the product supports all functions in the guide. The functions may differ with different product models or different versions of the same model. The actual product prevails.

12.1 GPON/EPON settings

On this page, you can register your ONT for internet access.

To access the page, [log in to the web UI](#) of the ONT and navigate to **Admin > Admin > GPON Settings** (or **EPON Settings**). Enter the parameters provided by your ISP and click **Apply Changes** to register the ONT.

You can view the registration status of the ONT on the [PON status](#) page.

LOID:	<input type="text"/>
LOID Password:	<input type="password"/>
PLOAM Password:	<input type="password"/>
Serial Number:	TZAN35DA6370
OMCI OLT Mode:	Default Mode <input type="button" value="v"/>

12.2 OMCI information

ONU Management Control Interface (OMCI) defines a mechanism and message format that is used by the Optical Line Termination (OLT) to configure, manage and monitor ONTs.

To access the page, [log in to the web UI](#) of the ONT and navigate to **Admin > Admin > OMCI Information**. You can click **Refresh** to update the information.

OMCI software version 1:	v2.0.0
OMCI software version 2:	v2.0.0
OMCC version:	0x80
Traffic Management option:	2
CWMP Product Class:	HG15
HW version:	V2.0

12.3 Commit/Reboot

This page is used to commit any configuration changes you have made and reboot the ONT to put the changes into effect. Click **Commit and Reboot** to save settings and reboot the ONT.

To access the page, [log in to the web UI](#) of the ONT and navigate to **Admin > Admin > Commit/Reboot**.

Commit and Reboot:	<input type="button" value="Commit and Reboot"/>
---------------------------	--

12.4 Backup/Restore

On this page, you can back up the configuration of the ONT, restore the configuration from a backup file, and reset the ONT.

To access the page, [log in to the web UI](#) of the ONT and navigate to **Admin > Admin > Backup/Restore**.

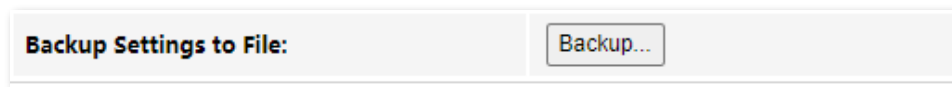
Backup Settings to File:	<input type="button" value="Backup..."/>
Restore Settings from File:	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Restore"/>
Reset Settings to Default:	<input type="button" value="Reset"/>

12.4.1 Back up the configuration of the ONT

You can back up the configuration of the ONT at a certain time for future restoration after you change the settings or reset the ONT.

Procedure:

- Step 1** [Log in to the web UI](#) of the ONT.
- Step 2** Navigate to **Admin > Admin > Backup/Restore**.
- Step 3** Click **Backup....**



The configuration file (**config.xml**) is automatically downloaded to the local host.

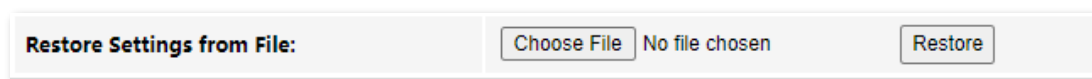
---End

12.4.2 Restore previous configuration of the ONT

You can restore the previous configuration of the ONT using the backup file that you have downloaded.

Procedure:

- Step 1** [Log in to the web UI](#) of the ONT.
- Step 2** Navigate to **Admin > Admin > Backup/Restore**.
- Step 3** Click **Choose File**, and select the configuration file.
- Step 4** Click **Restore**.



The ONT reboots to enable the configuration to take effect.

---End

12.4.3 Reset the ONT

When the ONT malfunctions and you cannot find a solution, you can try to reset the ONT. If your ISP has preset the ONT, the ONT will be restored to the configurations preset by the ISP. Otherwise, the ONT will be restored to factory settings.



Resetting the ONT will clear all previous personalized configurations. It is recommended to back up the configuration of the ONT in advance.

Procedure:

- Step 1** [Log in to the web UI](#) of the ONT.

Step 2 Navigate to **Admin > Admin > Backup/Restore**.

Step 3 Click **Reset**.

Reset Settings to Default:	Reset
----------------------------	-------

The ONT starts rebooting. Wait until it finishes rebooting, and then you can log in to the ONT again and perform settings.

---End

12.5 WAN user

On this page, after the WAN connection is set up, you can set the account to access the web server of the ONT through the WAN interface. The default user name is **tendaxpon** and the password is **XPON#TDWLD**.

To access the page, [log in to the web UI](#) of the ONT and navigate to **Admin > Admin > WAN User**.



For network security, you should change the user name and the password of the WAN user function after the WAN connection is set up.

User Name:	<input type="text" value="tendaxpon"/>
Old Password:	<input type="text"/>
New Password:	<input type="text"/>
Confirmed Password:	<input type="text"/>

Procedure:

Step 1 [Log in to the web UI](#) of the ONT.

Step 2 Navigate to **Admin > Admin > WAN User**.

Step 3 Set **User Name** as required.

Step 4 Enter the original password in **Old Password**.

Step 5 Enter your new password in **New Password** and **Confirmed Password**.

Step 6 Click **Apply Changes**.

User Name:	<input type="text" value="tendaxpon"/>
Old Password:	<input type="password"/>
New Password:	<input type="password"/>
Confirmed Password:	<input type="password"/>

---End

The following message is displayed, indicating that the modification is successfully.

192.168.1.1 says

Change setting successfully! Please login with new setting.

OK

12.6 System log

On this page, you can view the log information recorded by the ONT. In case of a system fault, you can refer to the logs during troubleshooting.

The time of the logs depends on the system time of the ONT. To make sure the time of the logs is correct, set correctly [Time zone](#) of the ONT first.

To access the page, [log in to the web UI](#) of the ONT and navigate to **Admin > Admin > System Log**.

System Log:	<input type="radio"/> Disable <input checked="" type="radio"/> Enable		
Log Level:	<input type="text" value="Notice"/>		
Display Level:	<input type="text" value="Notice"/>		
Mode:	<input type="text" value="Local"/>		
Server IP Address:	<input type="text"/>		
Server UDP Port:	<input type="text"/>		
<input type="button" value="Apply Changes"/>			
Save Log to File:	<input type="button" value="Save..."/>		
Clear Log:	<input type="button" value="Reset"/>		
System Log			
Date/Time	Facility	Level	Message

Parameter description

Parameter	Description
System Log	Specifies whether to enable the System Log function of the ONT.
Log Level	Specify the lowest severity of the log level and which level you want to display. <ul style="list-style-type: none"> – Emergency: The system has become unstable. – Alert: Immediate action is required. – Critical: Functionality is affected. – Error: An error condition exists and functionality could be affected. – Warning: Functionality might be affected. – Notice: Information about normal events. – Informational: General information about system operations. – Debugging: Detailed information about the system that can be used to troubleshoot unexpected behavior.
Display Level	
Mode	Specifies the mode of the system log. <ul style="list-style-type: none"> – Local: Logs will be saved in the log buffer and log file. – Remote: Logs will be saved in remote log servers. Remote logs facilitate you to remotely monitor the running status of the network. – Both: Logs will be saved in both the log buffer, log file and the remote log server.
Server IP Address	Specifies the IP address of the log server.
Server UDP Port	Specifies the UDP port used by the server to receive the log messages. It should be the same port as the port configured by the log server.
Save Log to File	Click it to save the log information to a file on your device.
Clear Log	Click Reset to clear all previous log information.
Date/Time	Specifies when the log is generated.
Facility	Specifies the device of the system log of the ONT.
Level	Specifies the log's severity level and you can decide whether to check the network or not.
Message	Specifies the description of the system log of the ONT.

12.7 Password

On this page, you can change the login password for the ONT. You can only change the password, and the original password is required during the process.



TIP

You can log in to the web UI of the ONT with user permissions or administrator permissions. Administrator permissions are for the installation and maintenance personnel only.

- **User Permissions:** The default login user name is **admin**. You can get the password from the bottom label on the ONT.
- **Administrator Permissions:** The default login user name and password are both **admin** (or **root**).

Procedure:

- Step 1** [Log in to the web UI](#) of the ONT.
- Step 2** Navigate to **Admin > Admin > Password**.
- Step 3** Set **UserName** according to the actual permissions.
- Step 4** Enter the original password in **Old Password**.
- Step 5** Enter your new password in **New Password** and **Confirmed Password**.
- Step 6** Click **Apply Changes**.

UserName:	root ▼
Old Password:	<input type="password"/>
New Password:	<input type="password"/>
Confirmed Password:	<input type="password"/>

The following message is displayed, indicating that the password is changed successfully.

192.168.1.1 says

Change password successfully! Please login with new password.

OK

---End

12.8 Auto logout time

On this page, you can set the auto logout time for the ONT. After logging in to the web UI of the ONT, you will be automatically logged out when no operation is performed within the defined time period.

To access the page, [log in to the web UI](#) of the ONT and navigate to **Admin > Admin > Auto Logout Time**. Enter the parameters as required and click **Apply Changes** to configure the auto logout time.

Auto Logout Time:	<input type="text" value="1200"/>	seconds
--------------------------	-----------------------------------	---------

12.9 Firmware upgrade

To get new features and improve performance and operating stability, you can upgrade the firmware of the ONT when a new version is available.

Procedure:

- Step 1** Go to www.tendacn.com. Download an applicable firmware of the ONT to your local computer and unzip it.
- Step 2** [Log in to the web UI](#) of the ONT.
- Step 3** Navigate to **Admin > Admin > Firmware Upgrade**.
- Step 4** Click **Choose File**, and select the upgrade file.
- Step 5** Click **Upgrade**.

<input type="button" value="Choose File"/>	No file chosen
<input type="button" value="Upgrade"/>	<input type="button" value="Reset"/>

The ONT reboots automatically.

---End

12.10 ACL

Access Control List (ACL) is a collection of permitting and denying rules that ensure security by blocking unauthorized users from and allowing authorized users to access ONT.

To access the page, [log in to the web UI](#) of the ONT and navigate to **Admin > Admin > ACL**.

ACL Capability:	<input type="radio"/> Disable <input checked="" type="radio"/> Enable <button>Apply Changes</button>
Interface:	LAN ▼
Start IP Address:	<input type="text"/>
End IP Address:	<input type="text"/>

ServiceName	LAN
Any	<input type="checkbox"/>
TELNET	<input type="checkbox"/>
FTP	<input type="checkbox"/>
HTTP	<input type="checkbox"/>
HTTPS	<input type="checkbox"/>
SNMP	<input type="checkbox"/>
PING	<input checked="" type="checkbox"/>

Add

ACL Table				
Select	Interface	IP Address	Services	Port
<input type="checkbox"/>	LAN	0.0.0.0	ftp,web,https,snmp,ping	21,80,443,161,162
<input type="checkbox"/>	WAN	0.0.0.0	web,https,ping	80,443

Parameter description

Parameter	Description
ACL Capability	Specifies whether to enable the ACL function of the ONT.
Interface	<p>Specifies the interface that the access control rule applies to, including LAN and WAN.</p> <ul style="list-style-type: none"> LAN: The ONT checks traffic from the LAN side according to the rule and decides to pass it or discard it. WAN: The ONT checks traffic from the WAN side according to the rule and decides to pass it or discard it.
Start IP Address	Specify the IP address range or a certain IP address that is controlled by the rule.
End IP Address	

Parameter	Description
ServiceName	<p>Specifies the protocol adopted by the traffic, or the types of traffic.</p> <ul style="list-style-type: none"> - Any: It specifies that all types of traffic are under the control of this rule. - TELNET: Telnet is a protocol that provides a command line interface for communication with a remote device or server, sometimes employed for remote management but also for initial device setup like network hardware. - FTP: File Transfer Protocol (FTP) is a standard network protocol used for the transfer of computer files between a client and server on a computer network. - HTTP: Hypertext Transfer Protocol (HTTP) is an application protocol and the foundation of data communication for the World Wide Web, where hypertext documents include hyperlinks to other resources that the user can easily access. - HTTPS: Hypertext Transfer Protocol Secure (HTTPS) is an extension of HTTP. SNMP is used for secure communication over a computer network, and is widely used on the Internet. - SNMP: Simple Network Management Protocol (SNMP) is the most widely used network management protocol in TCP/IP networks, which enables you to remotely manage all your network devices compliant with this protocol. - PING: Ping is a computer network administration software utility used to test the reachability of a host on an IP network.
ACL Table	Specifies all the ACL rules that are added.
Select	Used to select multiple ACL rules.
State	Specifies the control mode of the rule. If you deselect Enable when setting an ACL rule, the State shows Disable .
Interface	Specifies the interface that the access control rule applies to, including LAN and WAN .
IP Address	Specifies the IP address range or a certain IP address that is controlled by the rule.
Services	Specifies the protocols adopted by the traffic, or the types of traffic.
Port	Specifies the default ports adopted by the corresponding services.

12.11 Time zone

On this page, you can change the system time of the ONT, or enable the ONT to update its system time with the Simple Network Time Protocol (SNTP) server.

To access the page, [log in to the web UI](#) of the ONT and navigate to **Admin > Admin > Time Zone**.

Current Time :	Year <input type="text" value="2024"/> Mon <input type="text" value="10"/> Day <input type="text" value="21"/> Hour <input type="text" value="17"/> Min <input type="text" value="10"/> Sec <input type="text" value="26"/>
Time Zone Select :	<input type="text" value="Beijing/Chongqing/Hong Kong/Urumqi/Taipei (UTC+08:00)"/> ▼
Enable Daylight Saving Time	<input type="checkbox"/>
Enable SNTP Client Update	<input checked="" type="checkbox"/>
WAN Interface:	<input type="text" value="Any"/> ▼
SNTP Server 1 :	<input checked="" type="radio"/> <input type="text" value="130.149.17.8"/> ▼ <input type="radio"/> <input type="text" value="220.130.158.52"/> (Manual Setting)

Parameter description

Parameter	Description
Current Time	Specifies the current system time of the ONT. You can change it manually.
Time Zone Select	Specifies the time zone where the ONT locates.
Enable Daylight Saving Time	<p>Daylight Saving Time (DST) is the practice of advancing clocks during warmer months so that darkness falls later each day according to the clock.</p> <p>With it is enabled, the ONT sets the time forward by one hour in the spring ("spring forward") and sets the time back by one hour in autumn ("fall back") to return to standard time. In other words, there is one 23-hour day in late winter or early spring and one 25-hour day in the autumn.</p>
Enable SNTP Client Update	<p>Specifies whether to enable automatic update of system time through synchronization with SNTP server.</p> <p>The SNTP is a time synchronization protocol of the TCP/IP protocol family. It is based on the connectionless User Datagram Protocol (UDP) and can be used on all supporting devices to synchronize system time in IP networks.</p>
WAN Interface	Specifies the interface through which the ONT updates its system time with the SNTP server.
SNTP Server 1	You can choose a preset SNTP server, or manually set the IP address for updating system time.

12.12 Auto system maintenance

On this page, by setting the ONT to reboot periodically during leisure time, you can prevent the decreasing of performance and instability of the ONT after running for a long period.

To access the page, [log in to the web UI](#) of the ONT and navigate to **Admin > Admin > Auto System Maintenance**.

Auto System Maintenance:	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Reboot at:	03 : 00
Repeat:	<input checked="" type="checkbox"/> Sun. <input checked="" type="checkbox"/> Mon. <input checked="" type="checkbox"/> Tue. <input checked="" type="checkbox"/> Wed. <input checked="" type="checkbox"/> Thu. <input checked="" type="checkbox"/> Fri. <input checked="" type="checkbox"/> Sat.
Delay Reboot:	<input checked="" type="checkbox"/> Delay the reboot if a client is connected and the traffic is higher than Delay Reboot Limit Traffic
Delay Reboot Limit Traffic:	100 (3 - 1000)KB/s

Automatic maintenance takes effect only if the system time is synchronized with the internet time.

Parameter description

Parameter	Description
Auto System Maintenance	Specifies whether to enable the auto system maintenance function of the ONT.
Reboot at	Specify the time when the ONT reboots automatically.
Repeat	Used to enable or disable the reboot delay function.
Delay Reboot	<ul style="list-style-type: none"> Ticked: The function is enabled. When the time for rebooting approaches, if there is any client connected to the ONT and the traffic exceeds the limit you set, the ONT will delay rebooting. Unticked: The function is disabled. The ONT reboots immediately when the specified time for rebooting approaches.
Delay Reboot Limit Traffic	Used to set the traffic limit for delayed reboot. It is available only when the delay reboot function is enabled.

12.13 TR-069

The Customer Premise Equipment (CPE) WAN Management Protocol (TR-069) allows an Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection and diagnostics to the ONT from the internet. Generally, it is used by the ISP to manage the ONT.

To access the page, [log in to the web UI](#) of the ONT and navigate to **Admin > Admin > TR-069**.

ACS	
URL:	<input type="text" value="http://"/>
UserName:	<input type="text" value="cpe"/>
Password:	<input type="text" value="cpe"/>
Periodic Inform:	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
Periodic Inform Interval:	<input type="text" value="43200"/>
Connection Request	
Authentication:	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
UserName:	<input type="text"/>
Password:	<input type="text"/>
Path:	<input type="text" value="/tr069"/>
Port:	<input type="text" value="7547"/>
<input type="button" value="Apply"/> <input type="button" value="Undo"/>	
Certificate Management	
CPE Certificate Password:	<input type="text" value="client"/> <input type="button" value="Apply"/> <input type="button" value="Undo"/>
CPE Certificate:	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Upload"/>
CA Certificate:	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Upload"/>

Parameter description

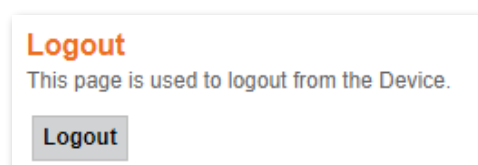
Parameter		Description
ACS	URL	Specifies the URL of the ACS.
	UserName	Specify the user name and password used to authenticate the ONT when the ONT connects to the ACS using the CPE WAN management protocol.
	Password	

Parameter	Description	
Connection Request	Periodic Inform	Used to enable or disable the ONT to periodically inform ACS.
	Periodic Inform Interval	Specifies the interval that the ONT to inform the ACS.
	Authentication	Specifies whether to authenticate the connection request sent by the ACS.
	UserName	Specify the user name and password used to authenticate the ACS when it sends the connection request to the CPE.
	Password	
Certificate Management	Path	Specifies the path used to receive the connection request sent by the ACS. Keep the default value if you are not sure.
	Port	Specifies the port used to receive the connection request sent by the ACS.
	CPE Certificate Password	Specifies an authentication password to ensure higher data security.
	CPE Certificate	Specifies an authentication of Customer Premise Equipment.
	CA Certificate	Specifies an authentication of a user's public key issued by a Certificate Authority (CA).

12.14 Logout

To access the page, [log in to the web UI](#) of the ONT and navigate to **Admin > Admin > Logout**.

You can log out of the web UI of the ONT by clicking **Logout** on this page, or click **Logout** at the upper-right corner of the web UI.



13 Statistics

This guide is for reference only and does not imply that the product supports all functions in the guide. The functions may differ with different product models or different versions of the same model. The actual product prevails.

In this part, you can view the packet statistics of the ports and interfaces of the ONT.

13.1 Interface statistics

This page displays the received and transmitted packets statistics, including the received packets (Rx pkt), received packets error (Rx err), dropped received packets (Rx drop), transmitted packets (Tx pkt), transmitted packets error (Tx err), dropped transmitted packets (Tx drop).

To access the page, [log in to the web UI](#) of the ONT and navigate to **Statistics > Statistics > Interface**.

Interface Statistics						
Interface	Rx pkt	Rx err	Rx drop	Tx pkt	Tx err	Tx drop
LAN1	0	0	0	0	0	0
LAN2	100118	0	0	107797	0	0
LAN3	0	0	0	0	0	0
LAN4	0	0	0	0	0	0
wlan0	2990	0	0	3984	0	0
wlan0-vap0	0	0	0	0	0	0
wlan1	41106	0	0	0	0	0
nas0_0	0	0	0	0	0	0
ppp0_nas0_1	0	0	0	0	0	0

13.2 PON statistics

The page displays the data statistics transmitted and received through the PON port.

To access the page, [log in to the web UI](#) of the ONT and navigate to **Statistics > Statistics > PON Statistics**.


Bytes Sent:	0
Bytes Received:	0
Packets Sent:	0
Packets Received:	0
Unicast Packets Sent:	0
Unicast Packets Received:	0
Multicast Packets Sent:	0
Multicast Packets Received:	0
Broadcast Packets Sent:	0
Broadcast Packets Received:	0
FEC Errors:	0
HEC Errors:	0
Packets Dropped:	0
Pause Packets Sent:	0
Pause Packets Received:	0

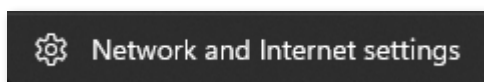
Appendixes

A.1 Obtain an IPv4/IPv6 address automatically

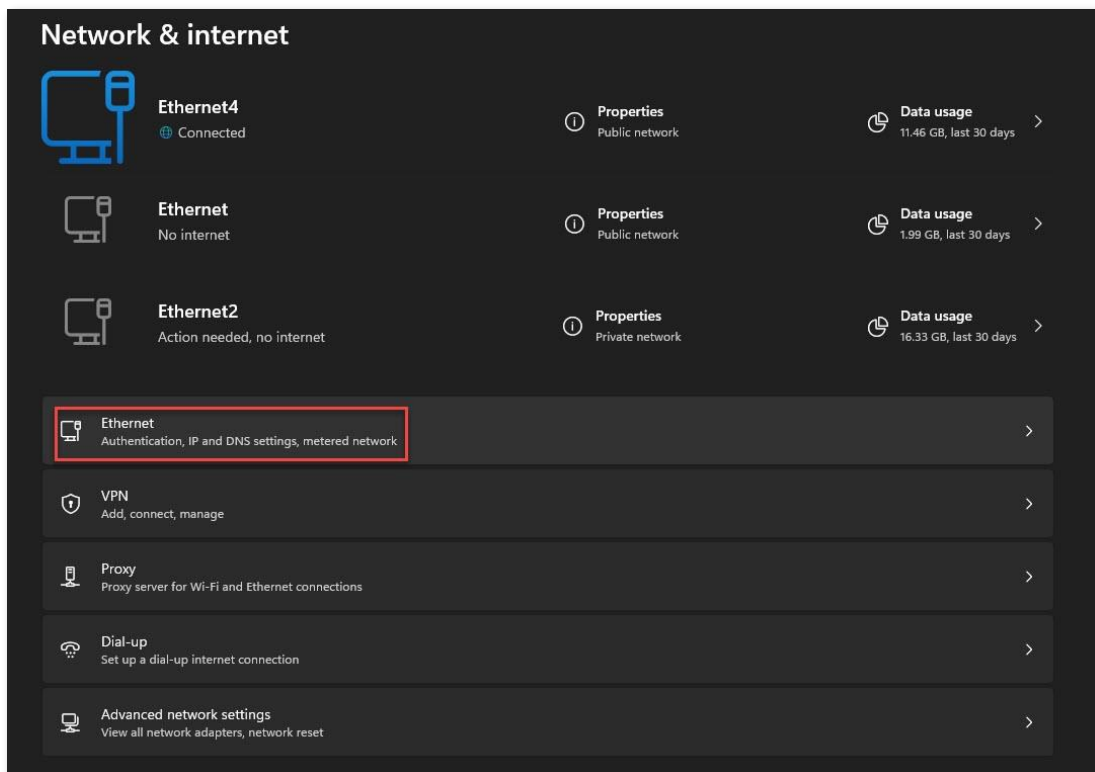
Perform the configuration procedure in [Windows 11](#) and [Windows 10](#) as required. A computer installed with a wired network adapter is used as an example to describe the procedure. The procedures for configuring computers installed with Wi-Fi network adapters are similar.

A.1.1 Windows 11

Step 1 Click  at the bottom right corner of the desktop and choose **Network and Internet settings**.



Step 2 Click **Ethernet**.



Step 3 Click **Edit**.

Network profile type

☒ **Public network (Recommended)**
Your device is not discoverable on the network. Use this in most cases—when connected to a network at home, work, or in a public place.

☐ **Private network**
Your device is discoverable on the network. Select this if you need file sharing or use apps that communicate over this network. You should know and trust the people and devices on the network.

[Configure firewall and security settings](#)

Authentication settings Edit

Metered connection Off ☐
Some apps might work differently to reduce data usage when you're connected to this network

[Set a data limit to help control data usage on this network](#)

IP assignment:	Automatic (DHCP)	Edit
DNS server assignment:	Automatic (DHCP)	Edit

Step 4 Select **Automatic (DHCP)**, and click **Save**.

Edit IP settings

Automatic (DHCP) ▼

Save Cancel

Step 5 Click **Edit**.

Network profile type

☒ **Public network (Recommended)**
Your device is not discoverable on the network. Use this in most cases—when connected to a network at home, work, or in a public place.

☐ **Private network**
Your device is discoverable on the network. Select this if you need file sharing or use apps that communicate over this network. You should know and trust the people and devices on the network.

[Configure firewall and security settings](#)

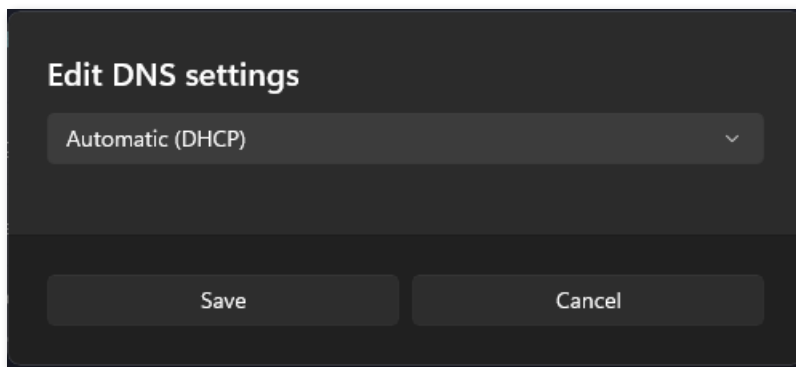
Authentication settings Edit

Metered connection Off ☐
Some apps might work differently to reduce data usage when you're connected to this network

[Set a data limit to help control data usage on this network](#)


IP assignment:	Automatic (DHCP)	Edit
DNS server assignment:	Automatic (DHCP)	Edit

Step 6 Select **Automatic (DHCP)**, and click **Save**.



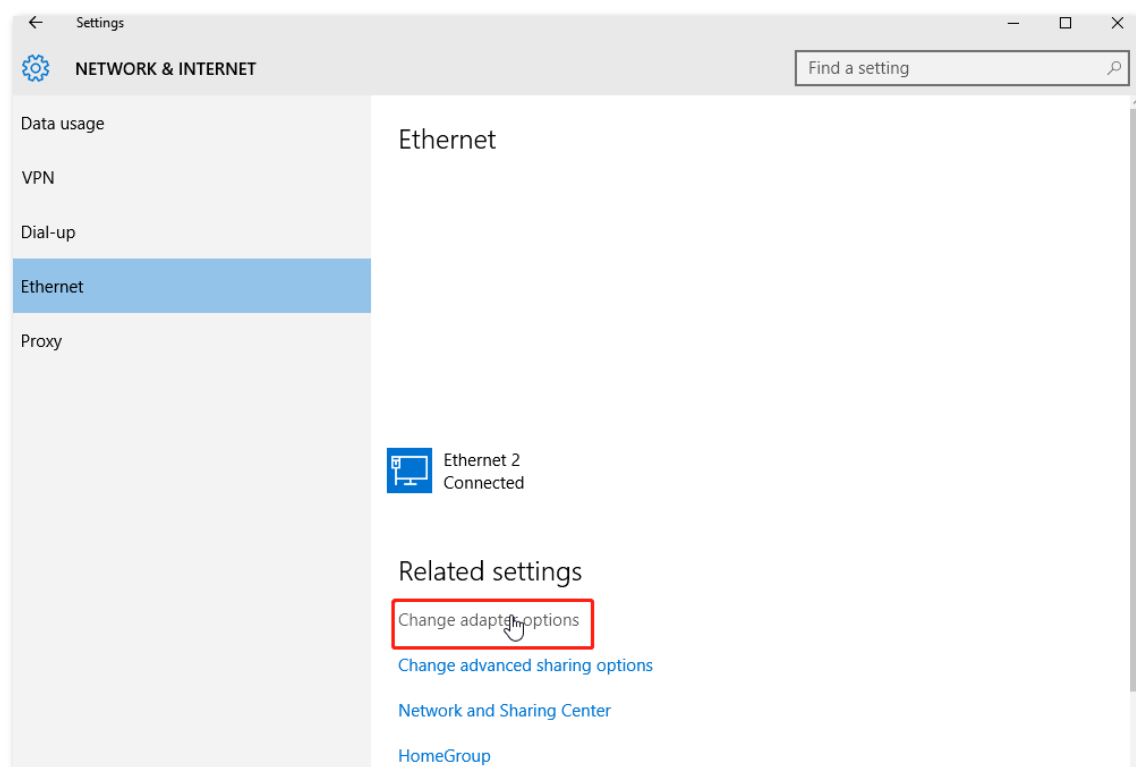
---End

A.1.2 Windows 10

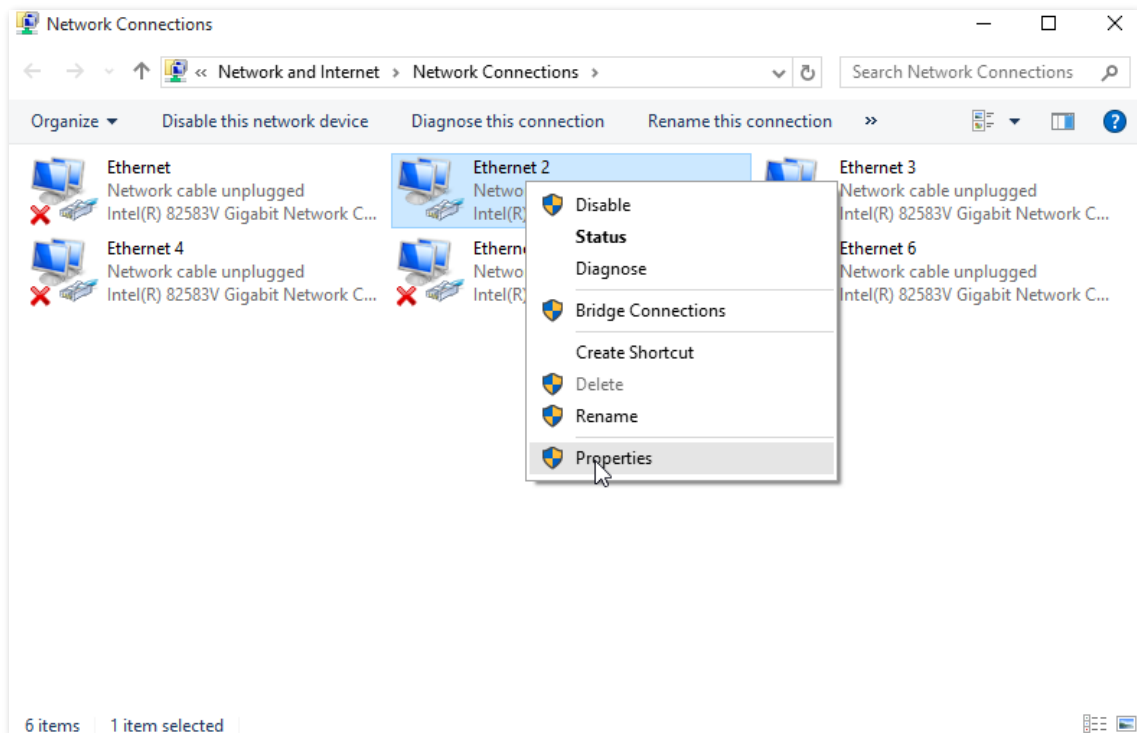
Step 1 Click  at the bottom right corner of the desktop and choose **Network settings**.



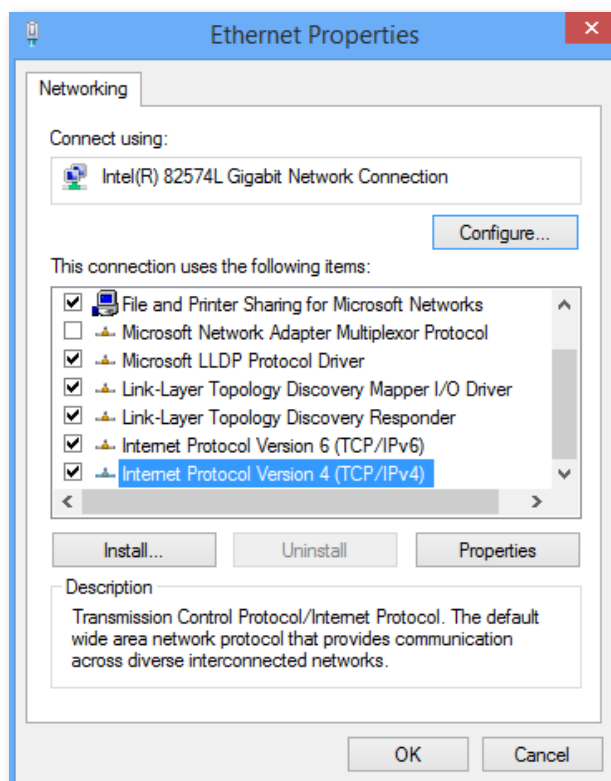
Step 2 Click **Change adapter options**.



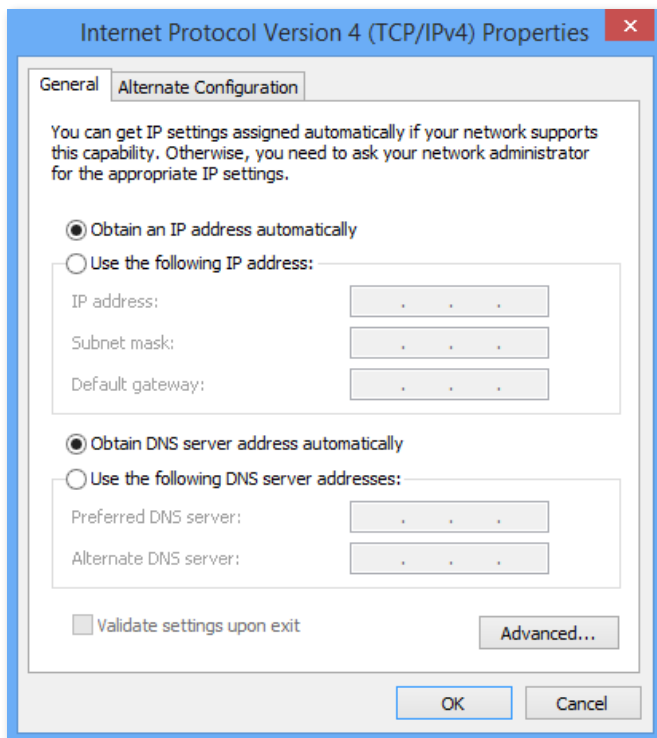
Step 3 Right-click on the connection in use, and then click **Properties**.



Step 4 Double-click **Internet Protocol Version 4 (TCP/IPv4)** or **Internet Protocol Version 6 (TCP/IPv6)**.



- Step 5** Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**, and click **OK**.



- Step 6** Click **OK** in the **Ethernet Properties** window.

---End

A.2 Acronyms and abbreviations

Acronym or Abbreviation	Full Spelling
ACL	Access control list
ACS	Auto-Configuration Server
AES	Advanced Encryption Standard
ALG	Application Layer Gateway
AP	Access Point
APC	Angled Physical Contact
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
BSSID	Basic Service Set Identifiers
CA	Certificate Authority
CPE	Customer Premise Equipment
CPU	Central processing unit
CTS	Clear To Send
CWMP	CPE WAN Management Protocol
DDNS	Dynamic Domain Name System
DDoS	Distributed Denial of Service
DFS	Dynamic Frequency Selection
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol version 6
DMZ	Demilitarized zone
DND	Don't Disturb

Acronym or Abbreviation	Full Spelling
DNS	Domain Name System
DTMF	Dual tone multi-frequency
DUID	DHCP unique identifier
FQDN	Fully qualified domain name
FTP	File Transfer Protocol
FTTH	Fiber to the Home
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPsec	Internet Protocol Security
IPTV	Internet Protocol television
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPoE	Internet Protocol over Ethernet
ISP	Internet service provider
ITU	International Telecommunication Union
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LOID	Line Operation Identification

Acronym or Abbreviation	Full Spelling
MAC	Medium access control
MIB	Management information base
MLD	Multicast Listener Discovery
MPPE	Microsoft Point-to-Point Encryption
MTU	Maximum Transmission Unit
NAPT	Network Address Port Translation
NAT	Network Address Translation
NMS	Network Management System
OLT	Optical line termination
OMCI	ONU Management Control Interface
ONT	Optical Network Terminal
ONU	Optical network unit
OS	Operating system
P2P	Peer-to-peer
PIN	Personal Identification Number
PON	Passive optical network
PPP	Point-to-Point Protocol
PPPoE	Point-to-Point Protocol over Ethernet
PPTP	Point-to-Point Tunneling Protocol
RA	Router Advertisement
RADVD	Router Advertisement Daemon
RDNSS	Recursive DNS Server
RS	Router Solicitation

Acronym or Abbreviation	Full Spelling
RSSI	Received Signal Strength Indicator
RTP	Real-time Transport Protocol
RTS	Request To Send
RTSP	Real Time Streaming Protocol
SC	Subscriber connector
SIP	Session Initiation Protocol
SLAAC	Stateless address autoconfiguration
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SSID	Service set identifier
STB	Set-top box
SYN	Synchronize Sequence Numbers
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TKIP	Temporal Key Integrity Protocol
TR-069	Technical Report - 069
UDP	User Datagram Protocol
UI	User interface
ULA	Unique Local Address
UPnP	Universal Plug and Play
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network

Acronym or Abbreviation	Full Spelling
VPN	Virtual Private Network
VoIP	Voice over IP
VoLTE	Voice over Long-Term Evolution
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WPA-PSK	WPA-Preshared Key
WPS	Wi-Fi Protected Setup
WRR	Weighted Round Robin