Tenda

User Guide

XPON ONT
HG1

www.tendacn.com

Document version: V1.0

Copyright Statement

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.

Document version: V1.0

Preface

Thank you for choosing Tenda! This user guide walks you through all functions of the XPON ONT.

Conventions

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: *XX:XX:XX:XX:XX:XX*
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
NOTE	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.
TIP	This format is used to highlight a procedure that will save time or resources.

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
V1.0	2023-08-24	Original publication.

Contents

1 Typical application scenarios

1.1 Overview

The ONT type is divided into two main classes, including Single Family Unit (SFU) and Home Gateway Unit (HGU).

The ONT can work under the following modes:

- **HGU**

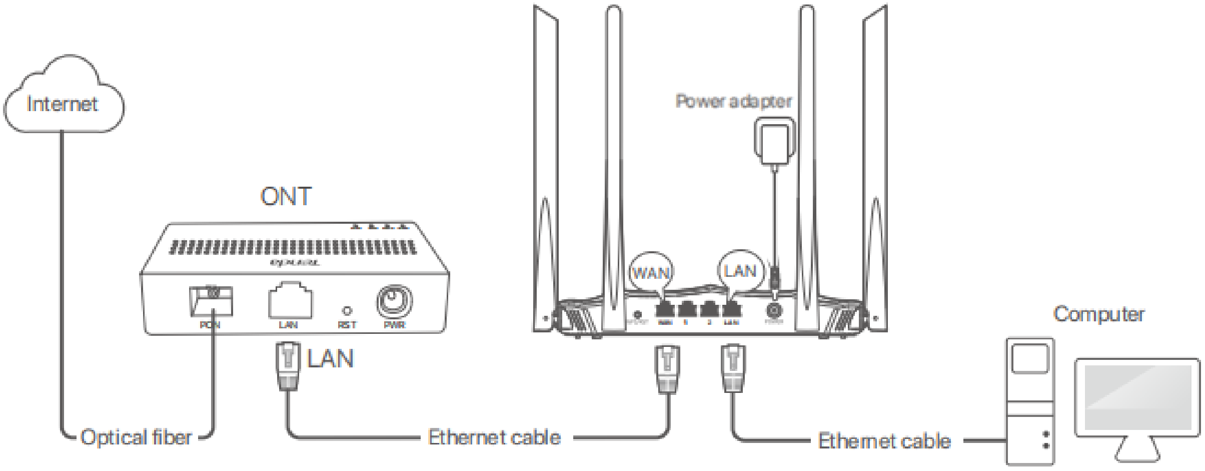
When the ONT type is HGU, the access modes include bridge mode and router mode.

  - Bridge mode: The channel mode 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 channel mode is set to **IPoE** or **PPPoE**. To access the internet, you can set up WAN connections on the ONT.

- **SFU**

When the ONT type is SFU, it is recommended to keep the default configurations of the ONT.

The network topology is shown as follows.



TIP

If you use the Ethernet cable to connect the LAN port of the ONT to the WAN of the router, determine whether to configure the router according to the actual ONT type.

- HGU: You can access the internet without configuring the router.
- SFU: You can configure the router to dial-up with the related parameters provided by your ISP.

1.2 Scenario 1: HGU ONT

1.2.1 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.

TIP

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

– If you use the Ethernet cable to connect the LAN port of the ONT to the computer without the router, you can access the internet without configuring the computer.

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

Configure the ONT

TIP

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.

Step 1 Log in to the web UI of the ONT.

Step 2 Navigate to **WAN** > **WAN** > **PON WAN.**

Step 3 Tick **Enable VLAN**.

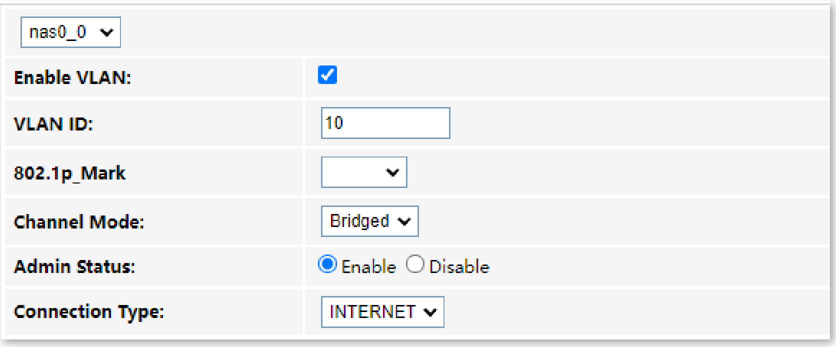
Step 4 Enter the **VLAN ID** provided by your ISP.

Step 5 Set **Channel Mode** to **Bridged.**

Step 6 Set **Connection Type** to **INTERNET**.

Step 7 Set other parameters according to your ISP and your own need.

Step 8 Click **Apply Changes**.



nas0_0	
Enable VLAN:	☑
VLAN ID:	10
802.1p_Mark	
Channel Mode:	Bridged
Admin Status:	● Enable ○ Disable
Connection Type:	INTERNET

---End

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

Configure internet access on a computer or a router

Configure internet access on a computer

TIP

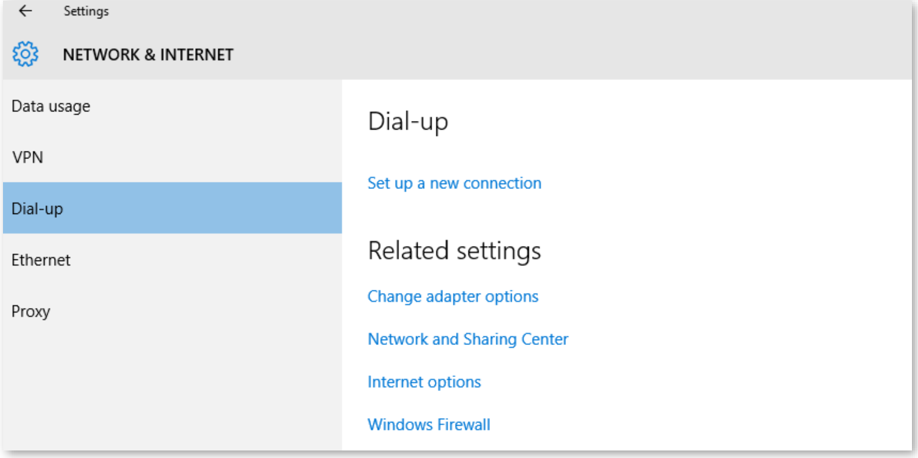
Configure your computer to access the internet according to the parameters provided by your ISP. PPPoE is used for illustration here.

Step 1 Configure the ONT.

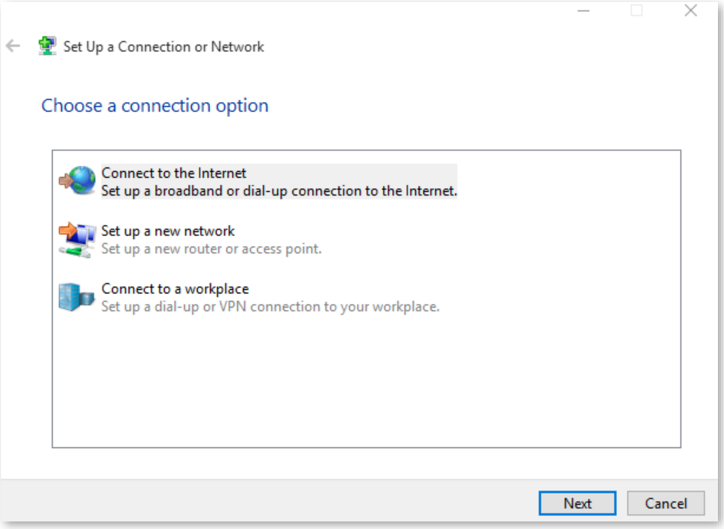
Step 2 Connect your computer to a LAN port of the ONT.

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**.



Set Up a Connection or Network

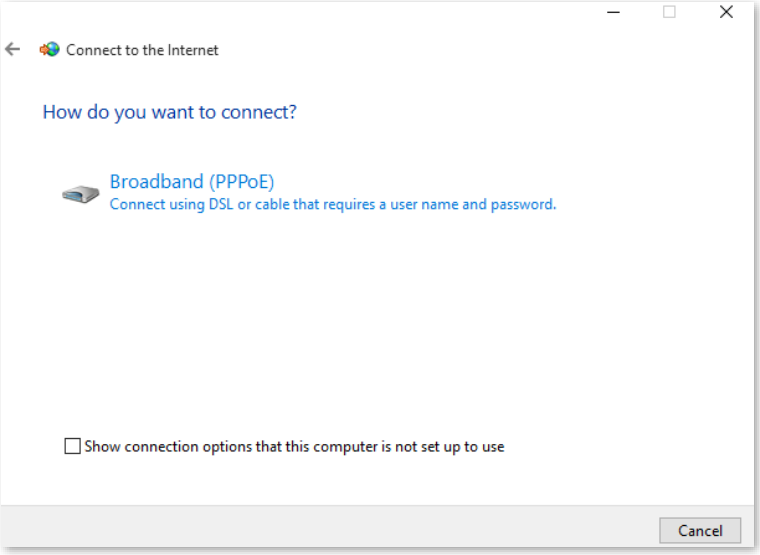
Choose a connection option

Connect to the Internet
Set up a broadband or dial-up connection to the Internet.

Set up a new network
Set up a new router or access point.

Connect to a workplace
Set up a dial-up or VPN connection to your workplace.

Step 6 Click **Broadband (PPPoE)**.



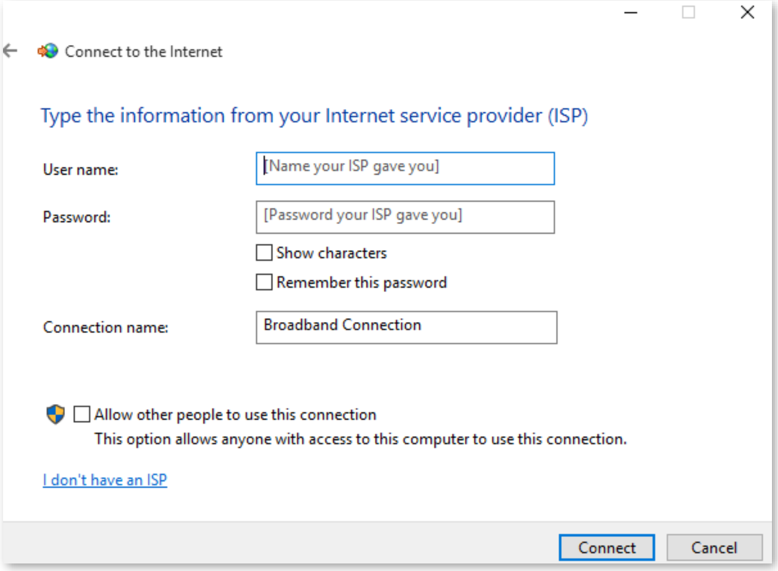
Connect to the Internet

How do you want to connect?

Broadband (PPPoE)
Connect using DSL or cable that requires a user name and password.

□ Show connection options that this computer is not set up to use

Step 7 Enter the PPPoE **User name** and **Password** provided by your ISP and click **Connect**.



Connect to the Internet

Type the information from your Internet service provider (ISP)

User name: [Name your ISP gave you]

Password: [Password your ISP gave you]

□ Show characters

□ Remember this password

Connection name: Broadband Connection

□ Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

I don't have an ISP

---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.

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.

1.2.2 Router mode

If you want to set up WAN connections for one or multiple services on the ONT, and access the WAN connection through the LAN port of the ONT, 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.

Set up a fixed IP connection

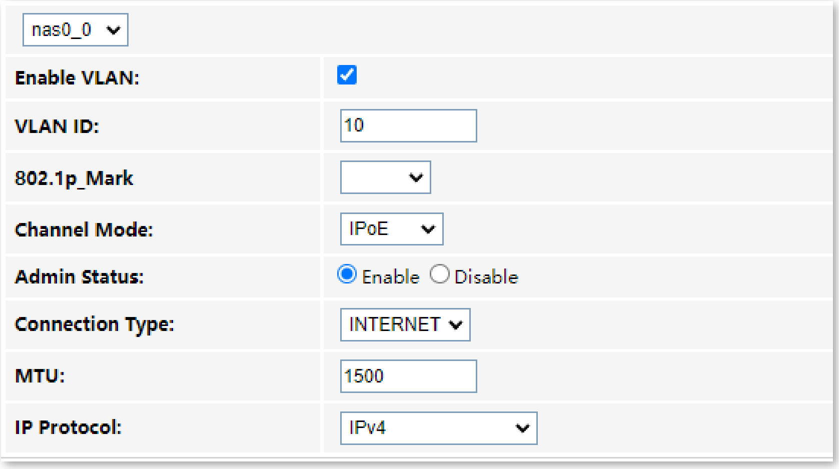
When your ISP provides fixed IP address (IPv4 or IPv6, or both) information, which may include the IP address, subnet mask and DNS server, you can set up a fixed IP connection.

Step 1 Log in to the web UI of the ONT.

Step 2 Navigate to **WAN** > **WAN** > **PON WAN**.

Step 3 Set **Channel Mode** to **IPoE**.

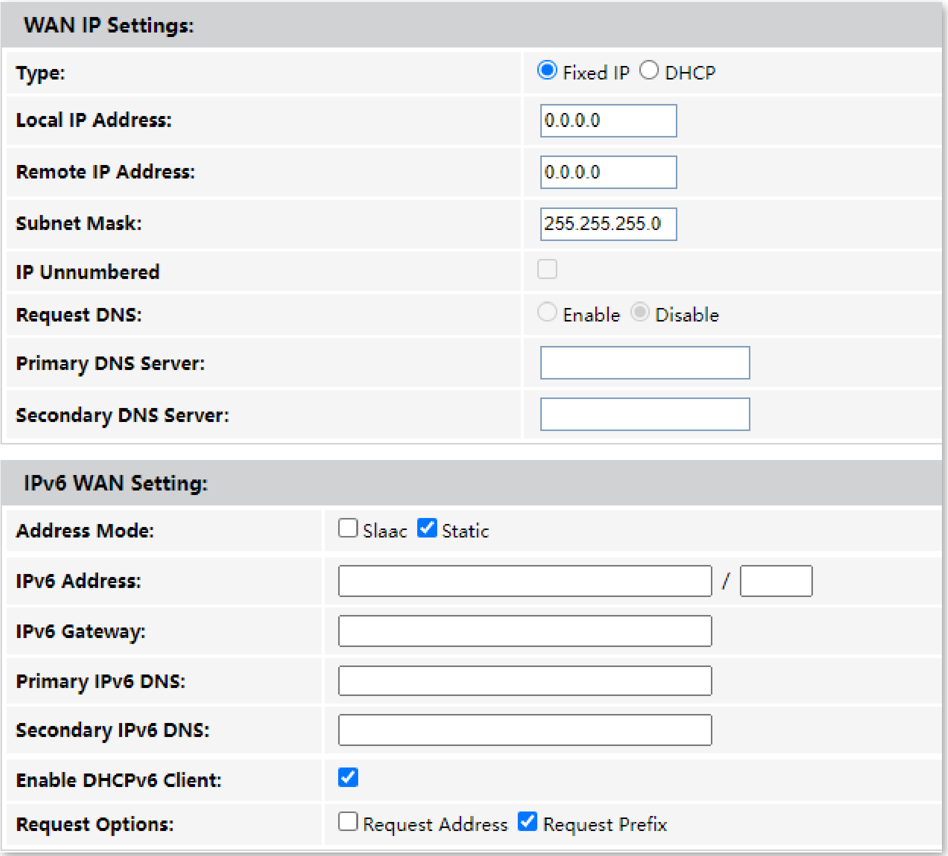
Step 4 Set other common WAN parameters as required by your ISP.



nas0_0	
Enable VLAN:	☑
VLAN ID:	10
802.1p_Mark	
Channel Mode:	IPoE
Admin Status:	● Enable ○ Disable
Connection Type:	INTERNET
MTU:	1500
IP Protocol:	IPv4

Step 5 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:	● Fixed IP ○ DHCP
Local IP Address:	0.0.0.0
Remote IP Address:	0.0.0.0
Subnet Mask:	255.255.255.0
IP Unnumbered	□
Request DNS:	○ Enable ● Disable
Primary DNS Server:	
Secondary DNS Server:	
IPv6 WAN Setting:	
Address Mode:	□ Slaac ☑ Static
IPv6 Address:	/
IPv6 Gateway:	
Primary IPv6 DNS:	
Secondary IPv6 DNS:	
Enable DHCPv6 Client:	☑
Request Options:	□ Request Address ☑ Request Prefix

Step 6 Click **Apply Changes**.

---End

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

Set up a dynamic IP connection

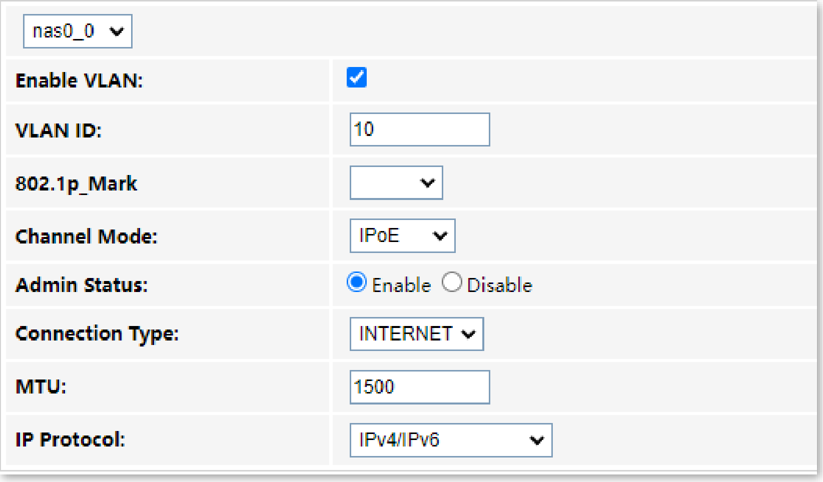
If your ISP does not provide any parameters, you can try to set up a DHCP connection.

Step 1 Log in to the web UI of the ONT.

Step 2 Navigate to **WAN** > **WAN** > **PON WAN**.

Step 3 Set **Channel Mode** to **IPoE**.

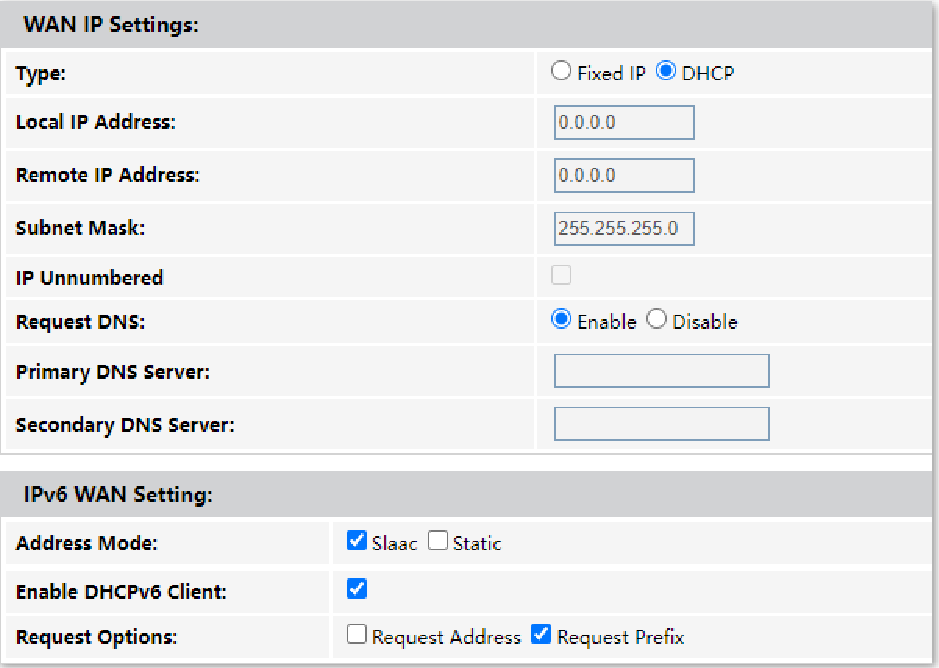
Step 4 Set other common WAN parameters as required by your ISP.



nas0_0	
Enable VLAN:	☑
VLAN ID:	10
802.1p_Mark	
Channel Mode:	IPoE
Admin Status:	● Enable ○ Disable
Connection Type:	INTERNET
MTU:	1500
IP Protocol:	IPv4/IPv6

Step 5 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 **Slaac** and configure other parameters as required.



WAN IP Settings:	
Type:	○ Fixed IP ● DHCP
Local IP Address:	0.0.0.0
Remote IP Address:	0.0.0.0
Subnet Mask:	255.255.255.0
IP Unnumbered	□
Request DNS:	● Enable ○ Disable
Primary DNS Server:	
Secondary DNS Server:	
IPv6 WAN Setting:	
Address Mode:	☑ Slaac □ Static
Enable DHCPv6 Client:	☑
Request Options:	□ Request Address ☑ Request Prefix

=

Step 6 Click **Apply Changes**.

---End

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

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.

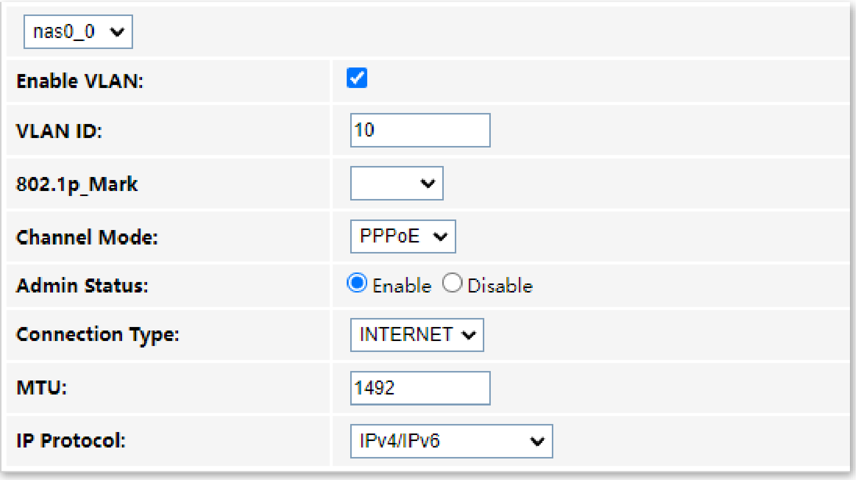
Step 1 Log in to the web UI of the ONT.

Step 2 Navigate to **WAN** > **WAN** > **PON WAN**.

Step 3 Set **Channel Mode** to **PPPoE**.

Step 4 Choose an **IP Protocol** in the drop-down list.

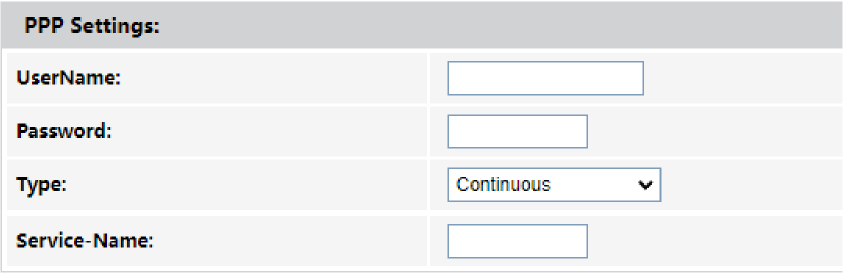
Step 5 Set other common WAN parameters as required by your ISP.



nas0_0

Enable VLAN:	☑
VLAN ID:	10
802.1p_Mark	
Channel Mode:	PPPoE
Admin Status:	● Enable ○ Disable
Connection Type:	INTERNET
MTU:	1492
IP Protocol:	IPv4/IPv6

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



PPP Settings:

UserName:	
Password:	
Type:	Continuous
Service-Name:	

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

Step 8 Click **Apply Changes**.

---End

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

1.3 Scenario 2: SFU ONT

When the device type is SFU, you can keep the default configurations of the ONT.

Procedure:

Step 1 Connect the WAN port of the router to a LAN port of the ONT using an Ethernet cable and connect the PON port of the ONT to the optical fiber.

Step 2 Register the ONT on the OLT.

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.

TIP

If you use the Ethernet cable to connect the LAN port of the ONT to the computer without the router, you can refer to configure internet access on a computer (Skip step 1) to configure the computer to dial-up.

2 Get to know your device

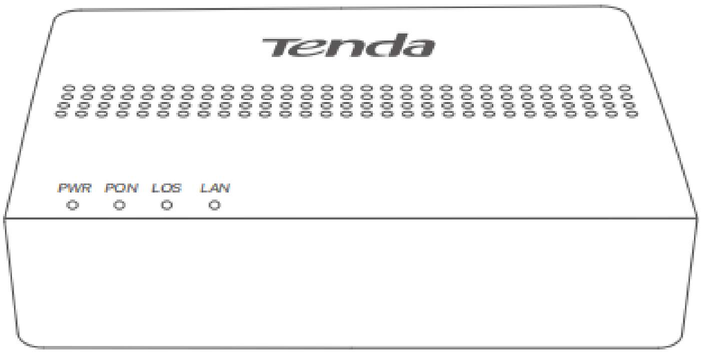
2.1 Overview

The XPON ONT is Fiber to the Home (FTTH) devices that provide internet access and other services with a fiber cord connected. You can enjoy internet access by connecting your devices to the ONT. HG1 provides a perfect terminal solution and service supporting capabilities for FTTH deployment.

2.2 Appearance

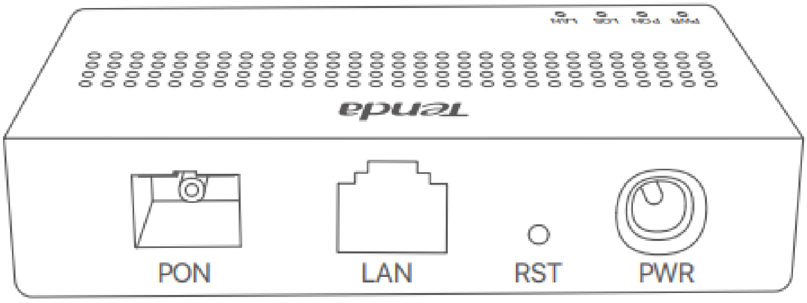
2.2.1 Indicators, ports, button and jack

- **LED indicators**



LED indicator	Color	Status	Description
PWR	Green	Solid on	Powered on
		Off	Powered off
PON	Green	Solid on	Registered successfully
		Blinking	Registering
		Off	Unregistered
LOS	Red	Blinking	Received optical power lower than optical receiver sensitivity
		Off	Received optical power at a proper value
LAN	Green	Solid on	LAN port connected properly without data transmitting
		Blinking	LAN port connected properly with data transmitting
		Off	No Ethernet device connected

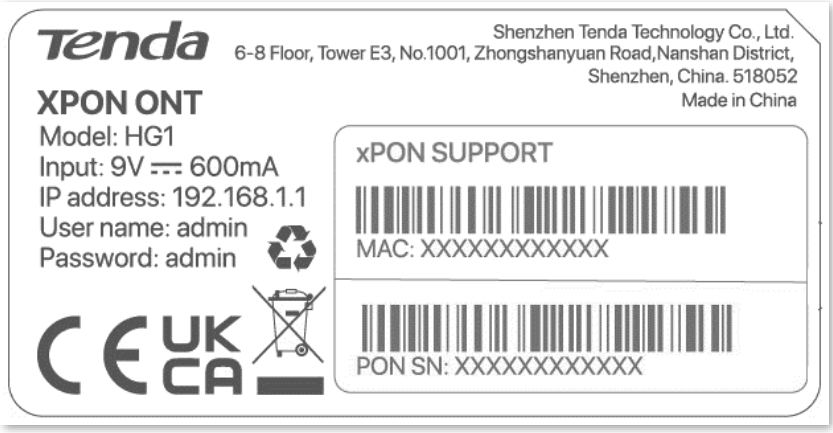
Ports, button and jack



Port/Button/Jack	Description
PON	Optical fiber port Used to connect to optical network through a fiber cord.
LAN	LAN port Used to connect to a router, switch or computer.
RST	Reset button When the **PWR** LED indicator lights solid on, use an object with a spike to hold the button down for longer than 10 seconds and release it. All LED indicators light off several seconds later. When the **PWR** LED indicator lights solid on again, the ONT is reset.
PWR	Power jack. Use the included power adapter to connect the device to a power source.
Wall-mounting hole	Used to mount the device onto the wall. Wall-mounting materials are self-prepared. Recommended specifications of the expansion bolts and screws you may use are as follows: [Expansion bolt] Inner diameter: 2.4 mm; Length: 26.4 mm. [Screws] Quantity: 2; Thread diameter: 3 mm; Length: 14 mm; Head diameter: 5.2 mm.

2.2.2 Label

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



Tenda

Shenzhen Tenda Technology Co., Ltd.
6-8 Floor, Tower E3, No.1001, Zhongshanyuan Road,Nanshan District,
Shenzhen, China. 518052
Made in China

XPON ONT
Model: HG1
Input: 9V ⎓ 600mA
IP address: 192.168.1.1
User name: admin
Password: admin

xPON SUPPORT

MAC: XXXXXXXXXXXX

PON SN: XXXXXXXXXXXX

- **Model:** Model of the ONT
- **Input:** Power supply for the ONT
- **IP address:** Default IP address used to log in to the web UI of the ONT
- **User name & 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

3 Web UI

3.1 Login

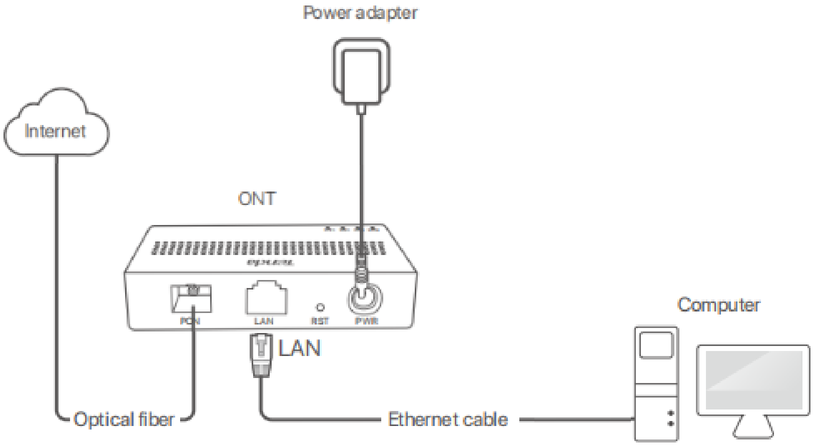
TIP

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

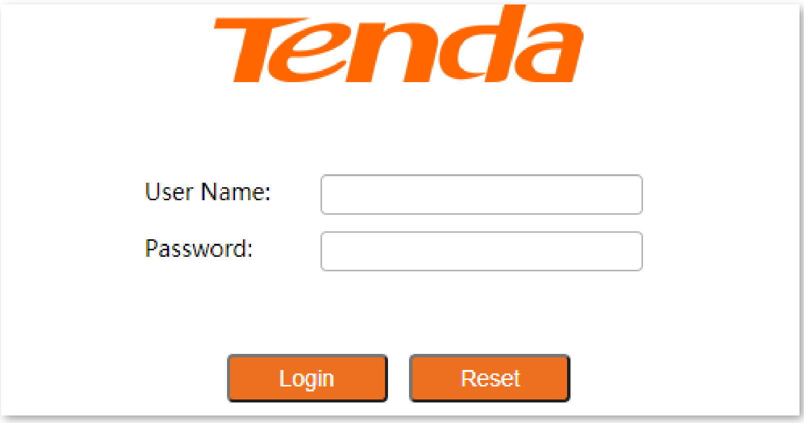
Procedure:

Step 4 Power on the ONT using the included power adapter.

Step 5 Connect a computer to a LAN port of the ONT using an Ethernet cable.



Step 6 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**.



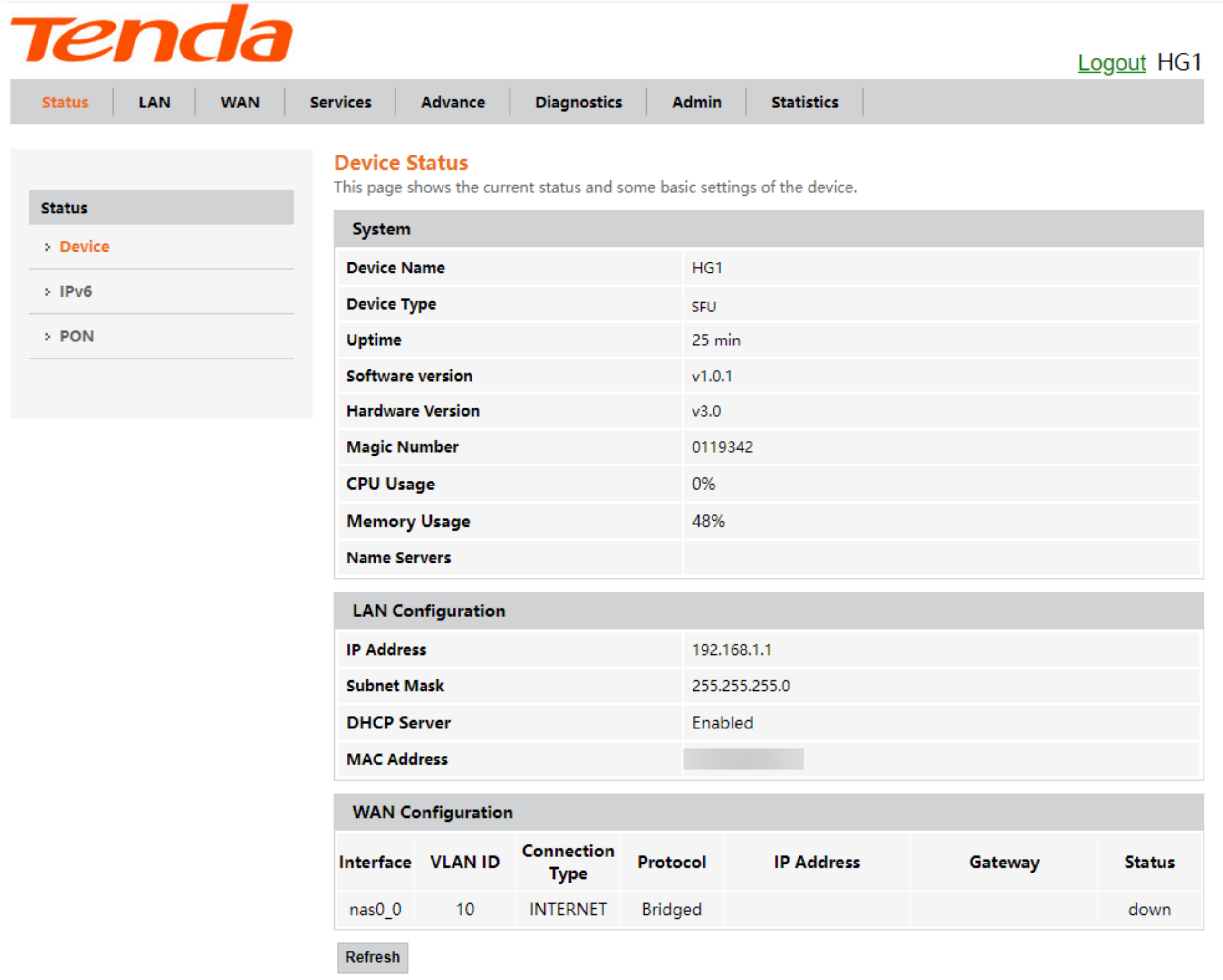
----End

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**.
- Restore the ONT to factory settings and try again.

The following page appears.



Device Status

This page shows the current status and some basic settings of the device.

System	
Device Name	HG1
Device Type	SFU
Uptime	25 min
Software version	v1.0.1
Hardware Version	v3.0
Magic Number	0119342
CPU Usage	0%
Memory Usage	48%
Name Servers	

LAN Configuration	
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
DHCP Server	Enabled
MAC Address	[redacted]

WAN Configuration

Interface	VLAN ID	Connection Type	Protocol	IP Address	Gateway	Status
nas0_0	10	INTERNET	Bridged			down

3.2 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 20 minutes.

3.3 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 information that you entered.
Reset	Used to restore the information that you entered on the page.
Delete	Used to delete the information that you selected.
Delete Selected	
Delete All	
Modify	Used to modify the information that you selected.
Remove	Used to remove the information that you selected.
Apply Changes	Used to apply the settings configured on the page.

4 Status

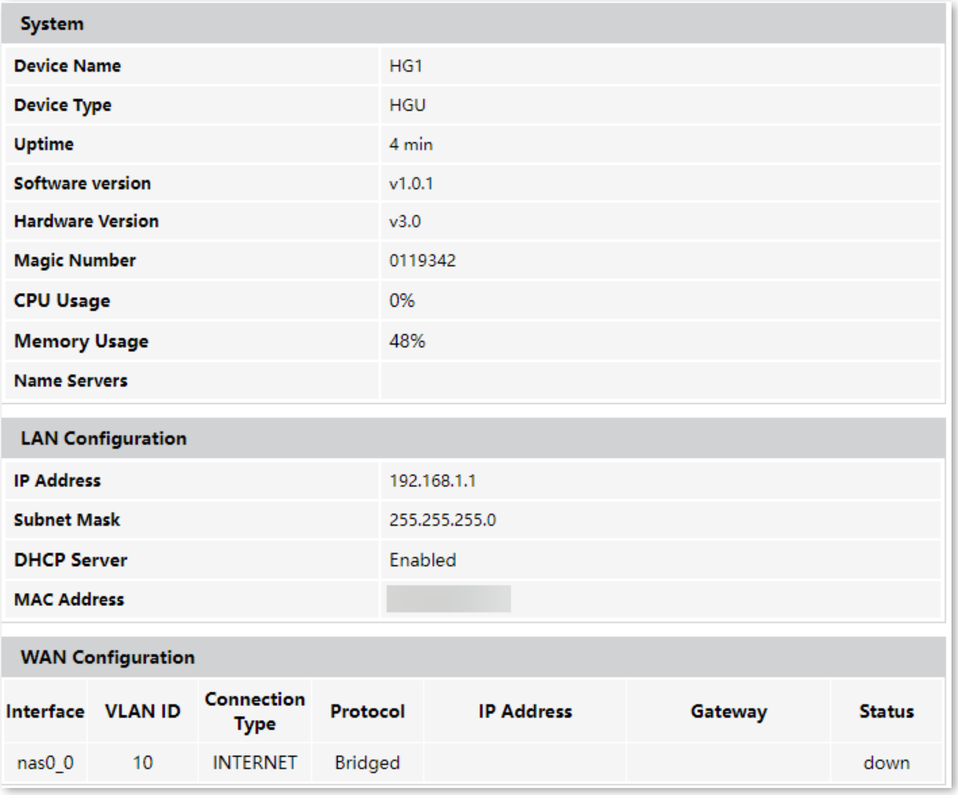
In this module, you can:

- View device status of the ONT.
- View IPv6 status of the ONT.
- View PON status of the ONT.

4.1 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	HG1
Device Type	HGU
Uptime	4 min
Software version	v1.0.1
Hardware Version	v3.0
Magic Number	0119342
CPU Usage	0%
Memory Usage	48%
Name Servers	

LAN Configuration	
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
DHCP Server	Enabled
MAC Address	[redacted]

WAN Configuration

Interface	VLAN ID	Connection Type	Protocol	IP Address	Gateway	Status
nas0_0	10	INTERNET	Bridged			down

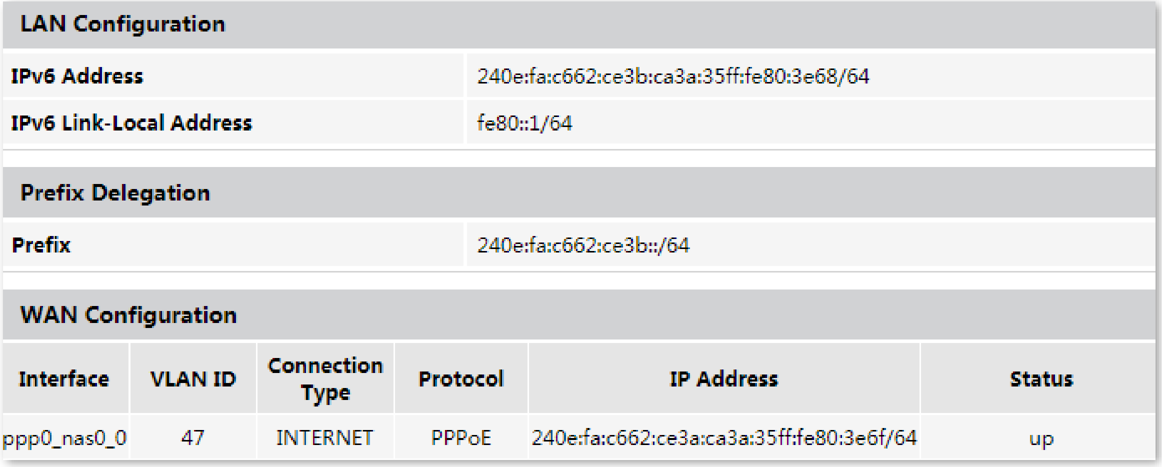
Parameter description

Parameter		Description
System		Specifies the basic system information of the ONT, including the device name, device type, uptime, software version, hardware version, magic number, CPU usage, memory usage, and name servers.
LAN Configuration	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.
	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	Interface	Specifies the name of the interface/WAN connection when IPv4 is enabled.
	VLAN ID	Specifies the VLAN ID of the WAN connection.
	Connection 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. ● **up**: The WAN connection is successful. ● **down**: The WAN connection failed and is currently unavailable.

4.2 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	240e:fa:c662:ce3b:ca3a:35ff:fe80:3e68/64
IPv6 Link-Local Address	fe80::1/64

Prefix Delegation

Prefix	240e:fa:c662:ce3b::/64

WAN Configuration

Interface	VLAN ID	Connection Type	Protocol	IP Address	Status
ppp0_nas0_0	47	INTERNET	PPPoE	240e:fa:c662:ce3a:ca3a:35ff:fe80:3e6f/64	up

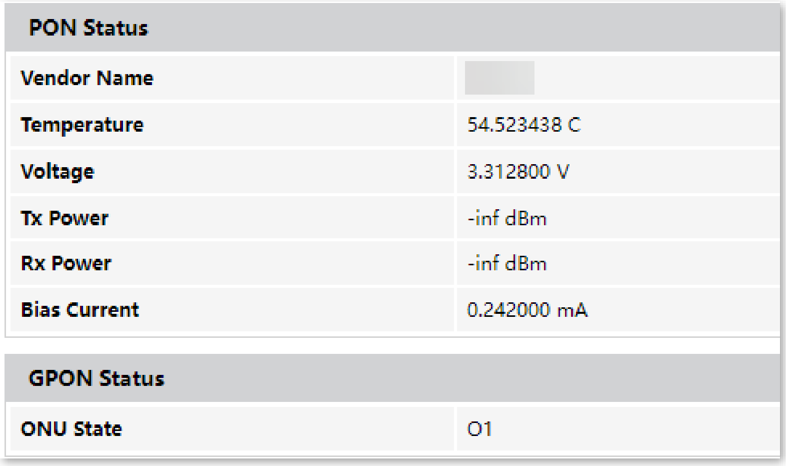
Parameter description

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/WAN when IPv6 is enabled.
	VLAN ID	Specifies the VLAN ID of the WAN connection.
	Connection 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.
	Status	Specifies the connection status of the WAN connection. • **up**: The WAN connection is successful. • **down**: The WAN connection failed and is currently unavailable.

4.3 View PON status

On this page, you can view the PON status and GPON/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	54.523438 C
Voltage	3.312800 V
Tx Power	-inf dBm
Rx Power	-inf dBm
Bias Current	0.242000 mA

GPON Status	
ONU State	O1

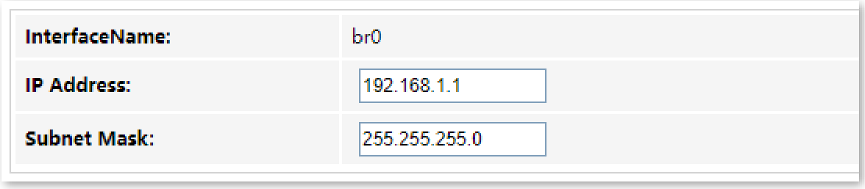
Parameter description

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	ONU State	Specifies the state of the ONT, ranging from O1 to O7. • **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.

5 LAN

In this module, you can configure the LAN IPv4 settings of the ONT.

To access the page, log in to the web UI and navigate to **LAN** > **LAN** > **LAN Interface Settings**.



InterfaceName:	br0
IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0

Parameter description

Parameter	Description
InterfaceName	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.

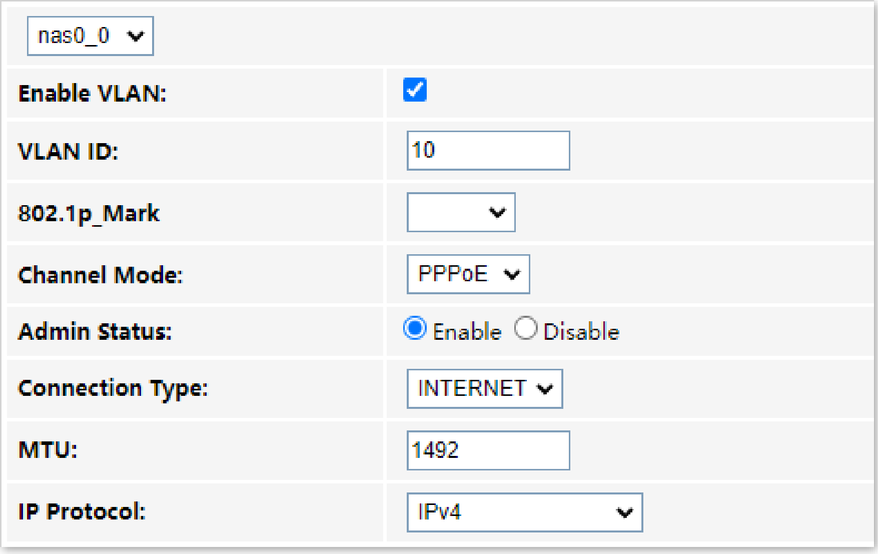
6 WAN

After you have registered the ONT successfully, you can set up the WAN connection.

To access the configuration 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 channel modes, connection types and IP protocols that you choose.

6.1 Common WAN settings

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



nas0_0	
Enable VLAN:	☑
VLAN ID:	10
802.1p_Mark	
Channel Mode:	PPPoE
Admin Status:	● Enable ○ Disable
Connection Type:	INTERNET
MTU:	1492
IP Protocol:	IPv4

Parameter description

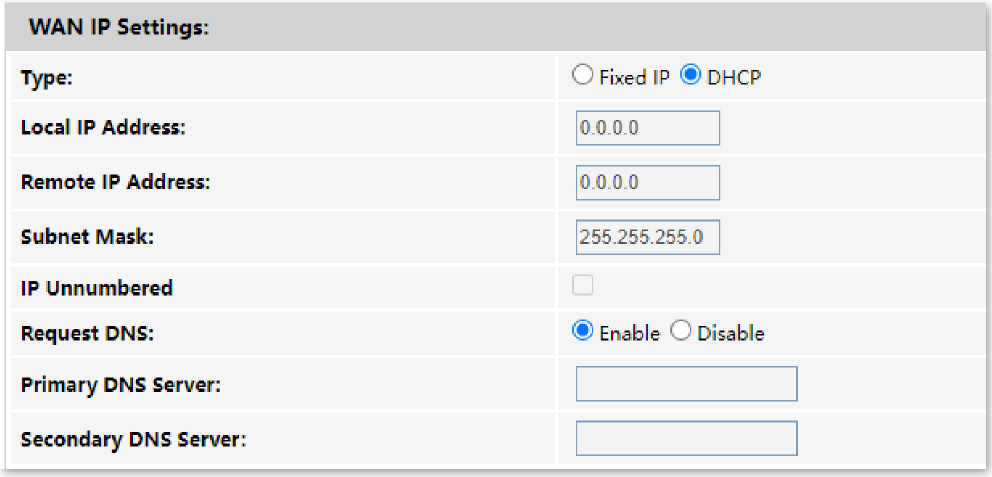
Parameter	Description
nas0_0	Specifies the WAN connection name which you set up. You can add multiple WAN connections by clicking the drop-down list and choose **new link**. After configuring required parameters, you can click **Apply Changes** to save the connections. This parameter is generated automatically after you create a new link and cannot be customized. A maximum of eight links can be created here.
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	

Parameter	Description
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.
Channel Mode	Specifies the mode that you used to set up the WAN connection, including **Bridged**, **IPoE** and **PPPoE**. • **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.
Admin Status	Specifies whether to enable this WAN connection.
Connection Type	Specifies the WAN connection type. It is **INTERNET** by default.
MTU	Maximum Transmission Unit (MTU) is the largest data packet transmitted by a network device. When the channel mode is PPPoE, the default MTU value is 1492. When the channel mode is IPoE, the default MTU value is 1500. Do not change the value unless necessary.
IP Protocol	Specifies the adopted IP protocol version. • **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.

6.2 WAN IP settings

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

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



WAN IP Settings:

Type:	○ Fixed IP ● DHCP
Local IP Address:	0.0.0.0
Remote IP Address:	0.0.0.0
Subnet Mask:	255.255.255.0
IP Unnumbered	□
Request DNS:	● Enable ○ Disable
Primary DNS Server:	
Secondary DNS Server:	

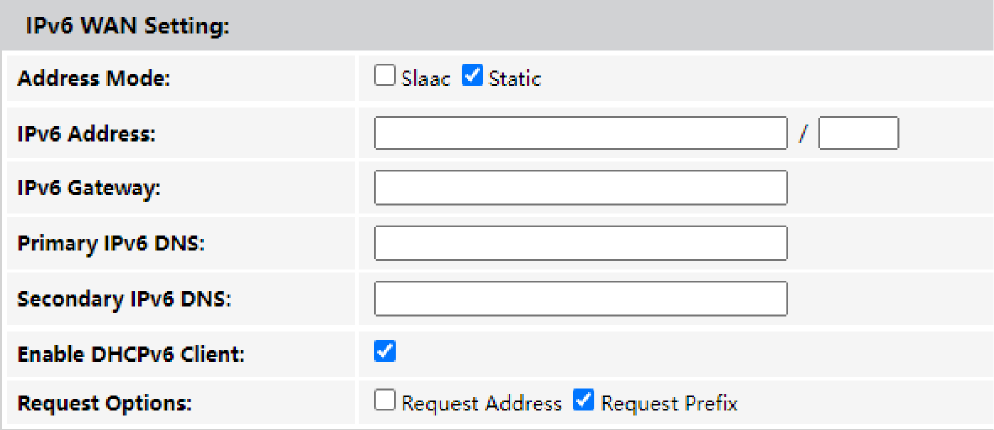
Parameter description

Parameter	Description
Type	Specifies the method used by the ONT to obtain WAN IP address information. - **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	If you select **Fixed IP** for **Type**, you should manually enter the IP address and related information provided by your ISP.
Remote IP Address	
Subnet Mask	
IP Unnumbered	Used to make multiple ports to share one IP address.
Request DNS	If the IP address is obtained through **DHCP**, you can select **Request DNS** to obtain the DNS server address automatically.
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. TIP If the ISP only provides one DNS server address, you can leave the secondary DNS blank.
Secondary DNS Server	

6.3 IPv6 WAN settings

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

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



IPv6 WAN Setting:

Address Mode:	☐ Slaac ☑ Static
IPv6 Address:	____ / ____
IPv6 Gateway:	
Primary IPv6 DNS:	
Secondary IPv6 DNS:	
Enable DHCPv6 Client:	☑
Request Options:	☐ Request Address ☑ Request Prefix

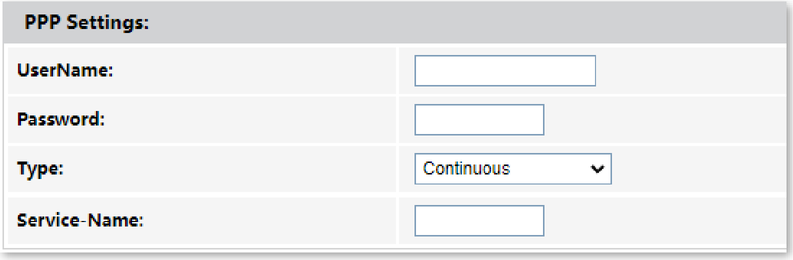
Parameter description

Parameter	Description
Address Mode	Specifies how the WAN IPv6 address of the ONT is obtained, including **Slaac** and **Static.** - **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.
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**.
Primary IPv6 DNS	Specify the primary and secondary DNS server addresses of the ONT.
Secondary IPv6 DNS	
Enable DHCPv6 Client	Specifies whether to enable the DHCPv6 client function.
Request Options	You can enable the ONT to obtain the address or prefix as a DHCPv6 client.

6.4 PPP settings

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

When **Channel Mode** is set to **PPPoE**, these parameters are required.



PPP Settings:

UserName:	
Password:	
Type:	Continuous
Service-Name:	

Parameter description

Parameter	Description
UserName	Specify the PPPoE user name and password for settings up the WAN connection.
Password	
Type	Specifies the PPPoE connection type. • **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.
Service-Name	Specifies the PPPoE service name used by the PPPoE server to verify the legitimacy of the ONT. TIP If your ISP did not provide a service name, leave this field blank. Otherwise, a dial failure may occur.

7 Services

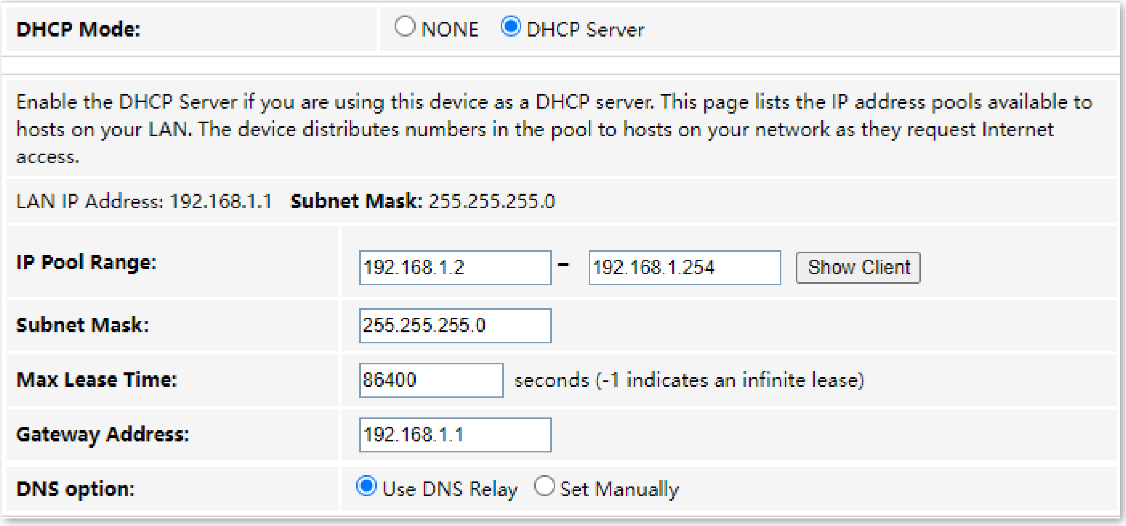
7.1 Service

7.1.1 DHCP

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 configuration page, log in to the web UI of the ONT and navigate to **Services** > **Service** > **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:	192.168.1.2 - 192.168.1.254 Show Client
Subnet Mask:	255.255.255.0
Max Lease Time:	86400 seconds (-1 indicates an infinite lease)
Gateway Address:	192.168.1.1
DNS option:	● Use DNS Relay ○ Set Manually

Parameter description

Parameter	Description
DHCP Mode	Specifies the status of the DHCP server. • **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.
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.

Parameter	Description
Show Client	Specifies the information of the active DHCP clients, including: ● **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.
Gateway Address	Specifies the gateway IP address of DHCP clients.
DNS option	Specifies how the ONT assigns DNS server addresses to LAN clients. ● **Use DNS Relay**: 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.
MAC-Based Assignment	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. TIP Please note the format of the MAC address. Use "-" to separate every two characters in the MAC address.

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 goal.

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.

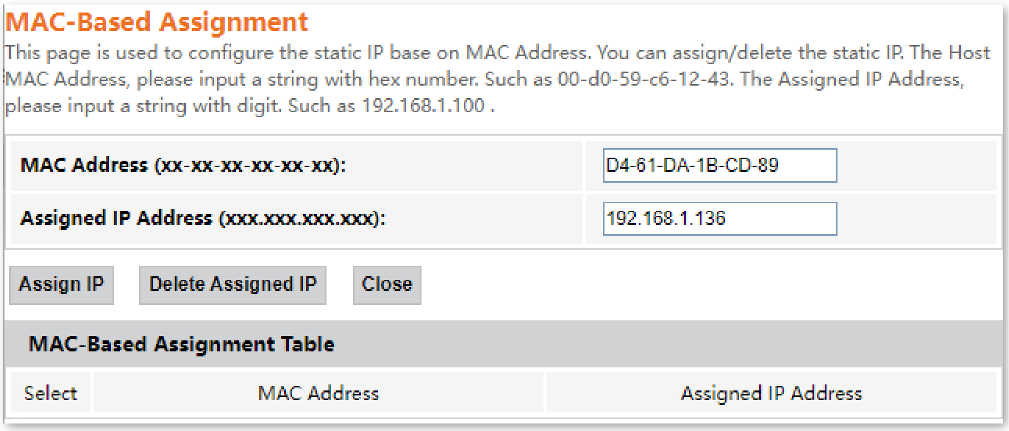
Step 2 Navigate to **Services** > **Service** > **DHCP**.

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

MAC-Based Assignment Table

Select	MAC Address	Assigned IP Address

----End

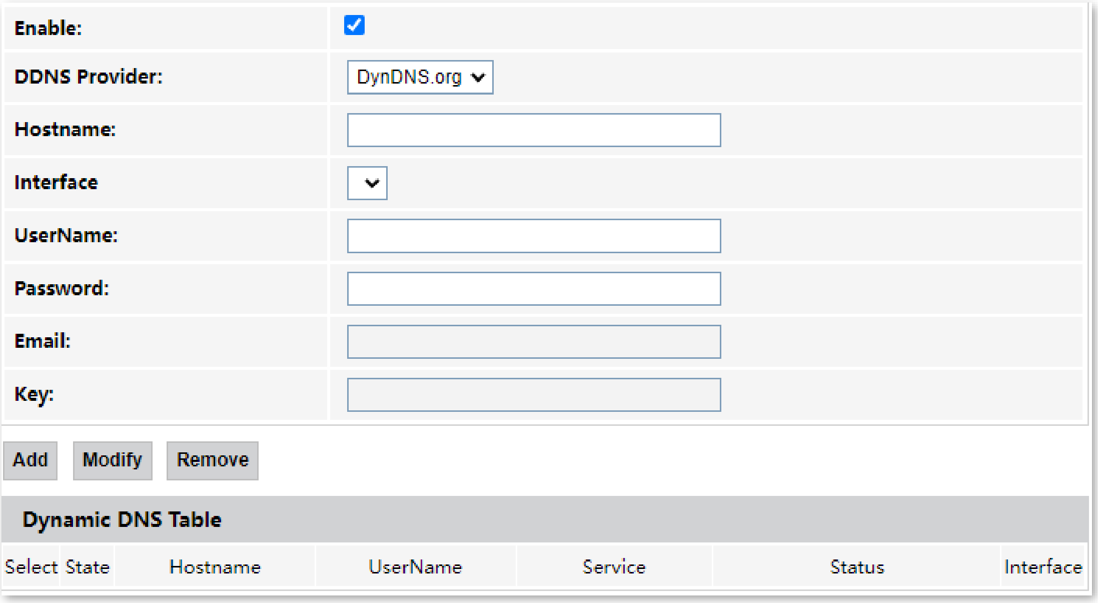
Now you can access resources on the FTP server free from the influence of the dynamic IP address.

7.1.2 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 configuration page, log in to the web UI of the ONT and navigate to **Services** > **Service** > **Dynamic DNS**.



Enable:	☑
DDNS Provider:	DynDNS.org
Hostname:	
Interface	
UserName:	
Password:	
Email:	
Key:	

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**, **TZO** 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. These fields are only available when the service provider is set to **DynDNS.org** and **NO-IP**.
Password	
Email	Specify the Email and key you registered with the DDNS service provider. These fields are only available when the service provider is set to **TZO**.
Key	
Operation	• **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.
Select	Used to 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 connection status of the DDNS, including **Successfully updated**, **Connection error** and **Authentication failure**.

Enable internet users to access LAN resources using a domain name

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

Goal: 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 goal.

Assume that the information of the FTP server includes:

- IP address: 192.168.1.136
- Service port: 21

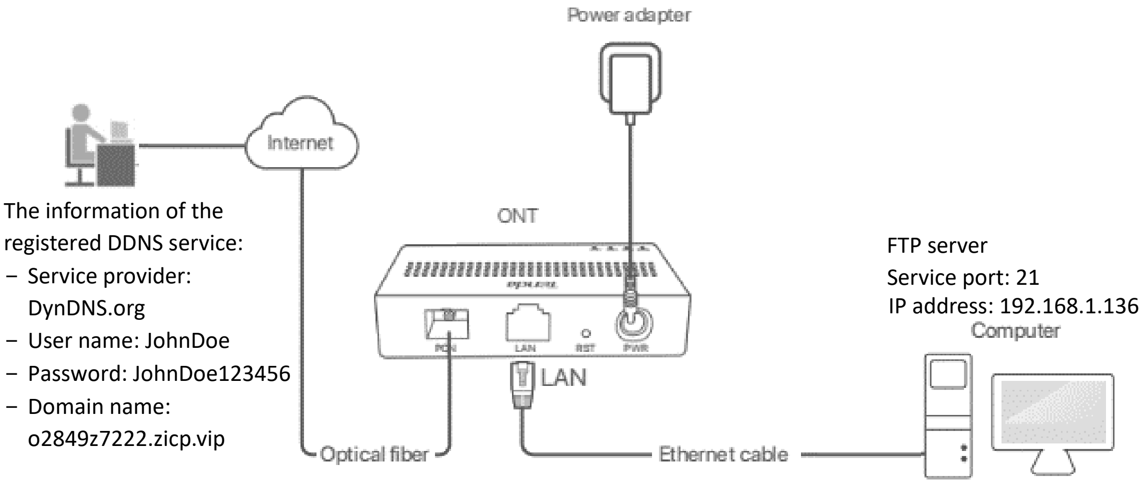
The information of the registered DDNS service:

- Service provider: DynDNS.org
- User name: JohnDoe

- Password: JohnDoe123456
- Domain name: o2849z7222.zicp.vip

TIP

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.

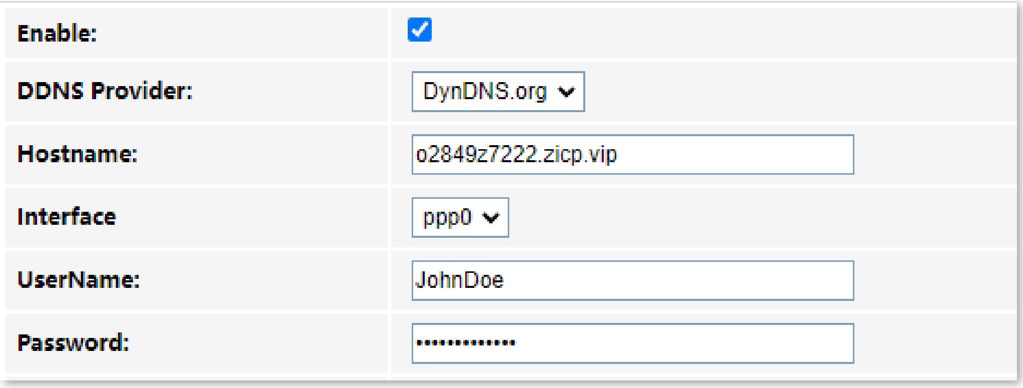

Power adapter
Internet
The information of the registered DDNS service:
– Service provider: DynDNS.org
– User name: JohnDoe
– Password: JohnDoe123456
– Domain name: o2849z7222.zicp.vip
ONT
PON
LAN
RST
PWR
LAN
FTP server
Service port: 21
IP address: 192.168.1.136
Computer
Optical fiber
Ethernet cable

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:	☑
DDNS Provider:	DynDNS.org
Hostname:	o2849z7222.zicp.vip
Interface	ppp0
UserName:	JohnDoe
Password:	•••••••••••••

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

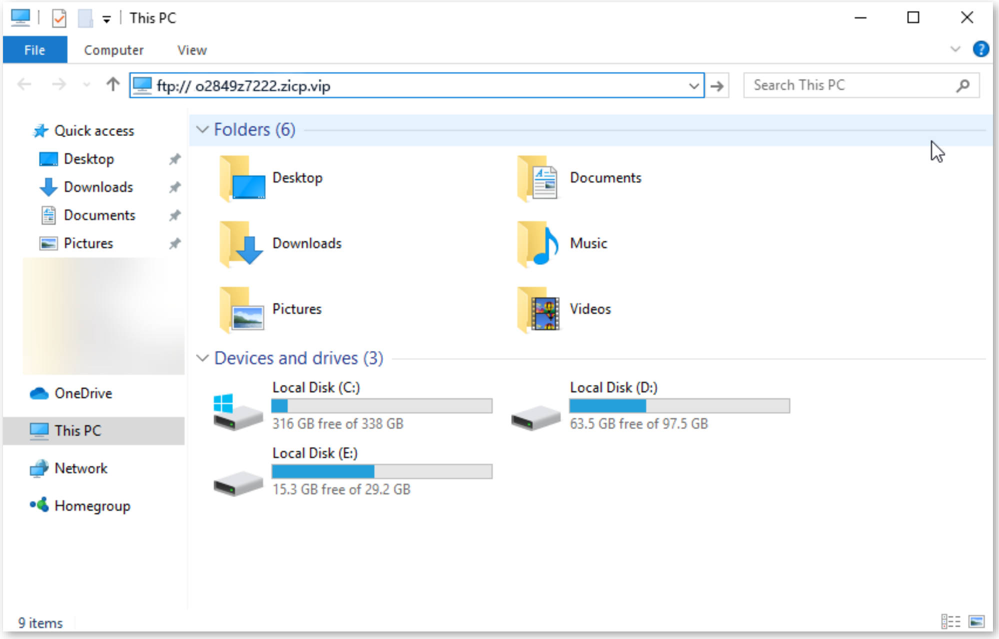
---End

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**.

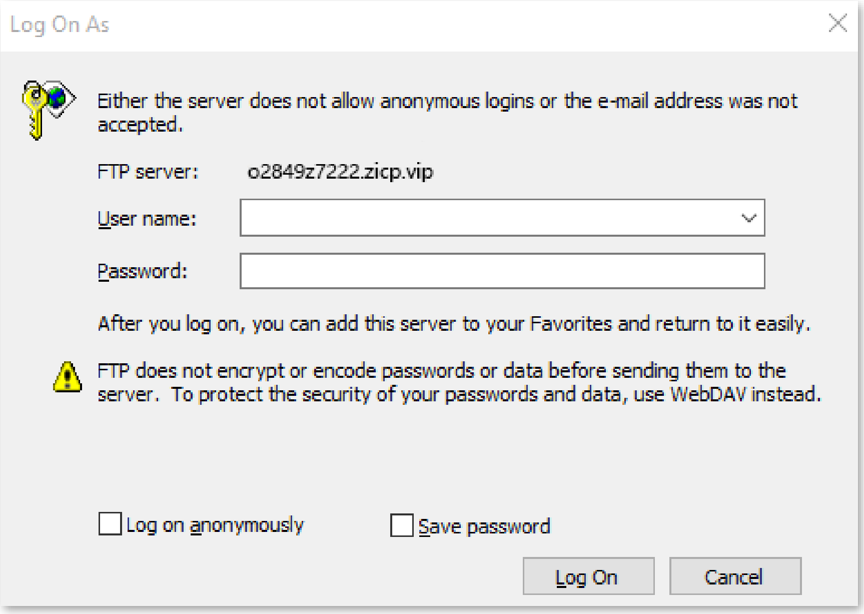
To access the FTP server from the internet with a domain name:

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



ftp:// o2849z7222.zicp.vip

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



Log On As

Either the server does not allow anonymous logins or the e-mail address was not accepted.

FTP server: o2849z7222.zicp.vip

User name:

Password:

After you log on, you can add this server to your Favorites and return to it easily.

FTP does not encrypt or encode passwords or data before sending them to the server. To protect the security of your passwords and data, use WebDAV instead.

□ Log on anonymously □ Save password

TIP

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

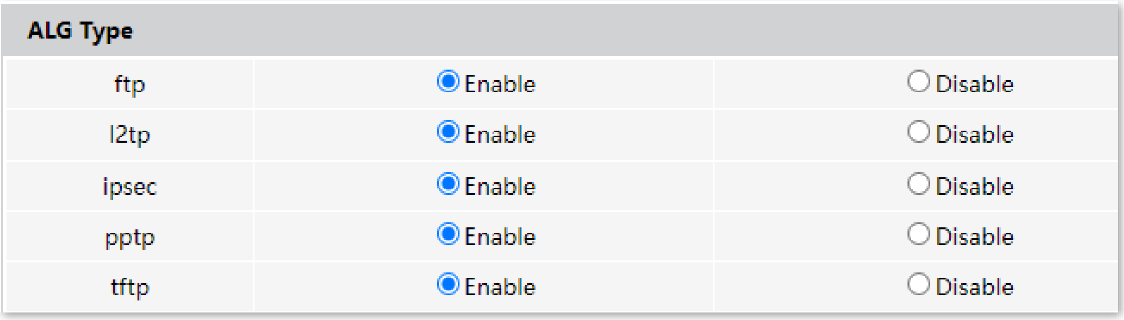
- Ensure that the local port number configured in the port forwarding function is the same as the intranet service port number set on the server.
- Close the firewall, antivirus software and security guards on the host of the FTP server and try again.

7.2 Firewall

7.2.1 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 configuration page, log in to the web UI of the ONT and navigate to **Services** > **Firewall** > **ALG**.



ALG Type		
ftp	● Enable	○ Disable
l2tp	● Enable	○ Disable
ipsec	● Enable	○ Disable
pptp	● Enable	○ Disable
tftp	● Enable	○ Disable

Parameter description

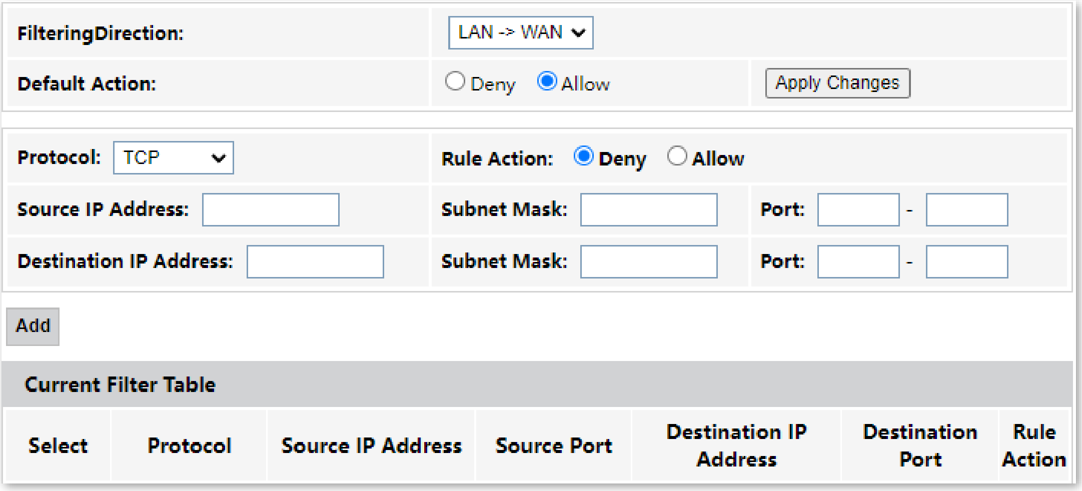
Parameter	Description
ftp	The File Transfer Protocol (FTP) is a standard network protocol used for the transfer of computer files between a client and server on a computer network. The users on LAN can share resources on the FTP server on WAN only when it is selected.
l2tp	The Layer Two Tunneling Protocol (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. 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.
ipsec	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). 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.
pptp	The Point-to-Point Tunneling Protocol (PPTP) is an obsolete method for implementing virtual private networks. PPTP has many well-known security issues. 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.
tftp	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.

7.2.2 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 configuration 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**.



FilteringDirection:	LAN -> WAN	
Default Action:	○ Deny ● Allow	Apply Changes

Protocol: TCP	**Rule Action:** ● Deny ○ Allow	
Source IP Address:	**Subnet Mask:**	**Port:** -
Destination IP Address:	**Subnet Mask:**	**Port:** -

Add

Current Filter Table

Select	Protocol	Source IP Address	Source Port	Destination IP Address	Destination Port	Rule Action

Parameter description

Parameter	Description
FilteringDirection	Specifies the forwarding direction of data to be filtered.
Default Action	Specify the default action for the outgoing (LAN -> WAN) or incoming (WAN -> LAN) data. • **Deny**: 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. • **Allow**: 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.
Protocol	Specifies the protocol adopted by data to be filtered. • **TCP**: TCP protocol. • **UDP**: UDP protocol. • **ICMP**: ICMP protocol. • **TCP/UDP**: TCP protocol and UDP protocol. • **ANY**: Any protocol.

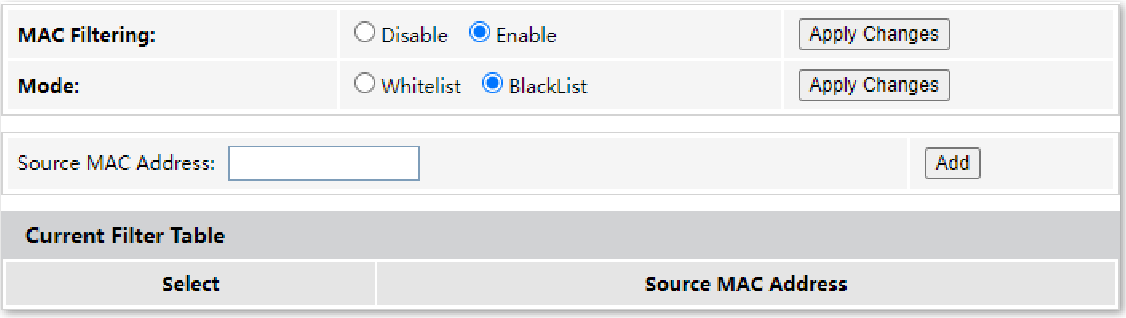
Parameter	Description
Rule Action	Specifies whether to deny or allow the data to pass through. - **Deny**: Packets that comply with the rule are denied, while others are perform the default action. - **Allow**: Only packets that comply with the rule are allowed, while others perform the default action.
Source IP Address	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. - When **Filtering Direction** is set to **LAN→WAN**, this parameter specifies the LAN computer's IP address to be affected. - When **Filtering Direction** is set to **WAN→LAN**, 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	Specifies the source port of the packets. The source port is only available for the TCP/UDP protocol. If **ICMP** or **ANY** is selected for **Protocol**, this field is not required. TIP 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.
Destination IP Address	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. - When **Filtering Direction** is set to **LAN→WAN**, this parameter specifies the internet server's IP address to be affected. - When **Filtering Direction** is set to **WAN→LAN**, 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	Specifies the destination port of the packets. Its setting determines which services are affected by this rule. The destination port is only for TCP and UDP protocol.

7.2.3 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 configuration 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**.



MAC Filtering: ○ Disable ● Enable

Mode: ○ Whitelist ● BlackList

Source MAC Address:

Current Filter Table

Select	Source MAC Address

Parameter description

Parameter	Description
MAC Filtering	Specifies whether to enable the MAC filtering function.
Mode	Specifies the mode of the MAC filtering function. • **Whitelist**: Only data packets whose source or destination MAC addresses are added in the current filter table can access the internet. • **BlackList**: Data packets from the LAN whose source or destination MAC addresses are added in the current filter table cannot pass through the ONT.
Source MAC Address	Specifies the source MAC address of data packets. You can only enter one source MAC address in one MAC filtering rule. TIP The MAC address cannot contain any special characters. An example in the correct format is cc3a61711b6e.

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.

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

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

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

Procedure:

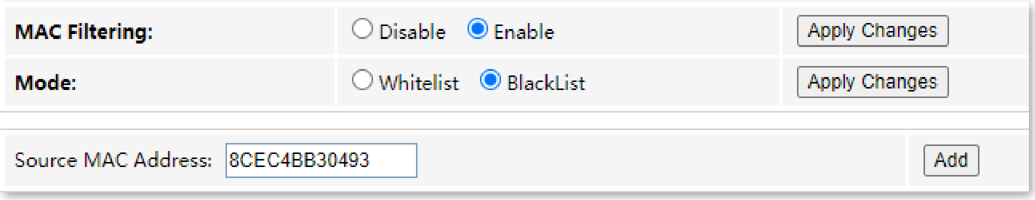
Step 1 Log in to the web UI of the ONT.

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

Step 3 Set **MAC Filtering** to **Enable**, and click **Apply Changes**.

Step 4 Set **Mode** to **BlackList**, and click **Apply Changes**.

Step 5 Set **Source MAC Address** to **8CEC4BB30493**, and click **Add**.

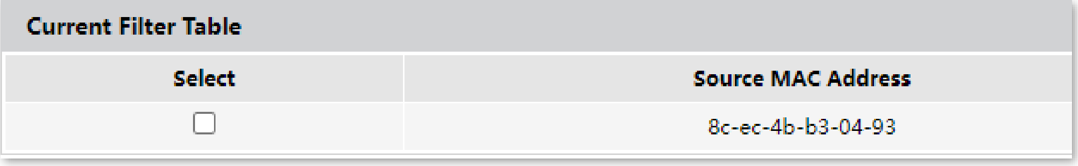


MAC Filtering:	○ Disable ● Enable	Apply Changes
Mode:	○ Whitelist ● BlackList	Apply Changes

Source MAC Address: 8CEC4BB30493 Add

---End

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



Current Filter Table

Select	Source MAC Address
□	8c-ec-4b-b3-04-93

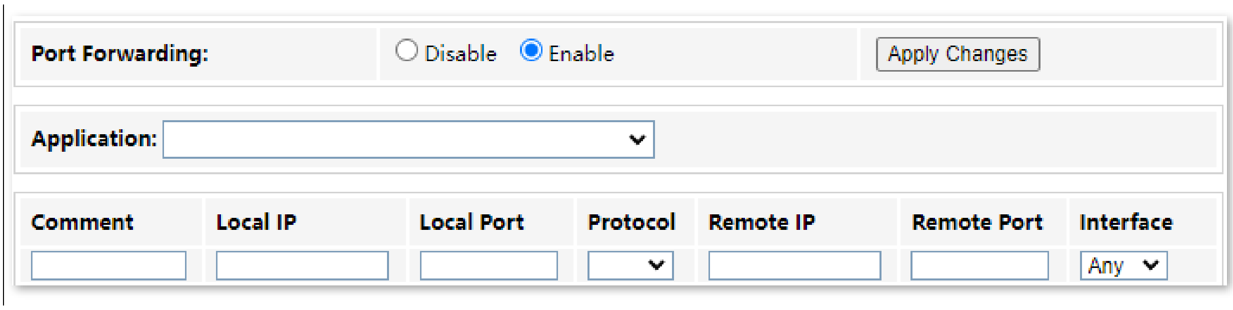
In this example, after the configuration is completed, the device added cannot access the internet through the ONT.

7.2.4 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 configuration 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: ○ Disable ● Enable

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.

Goal: 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.

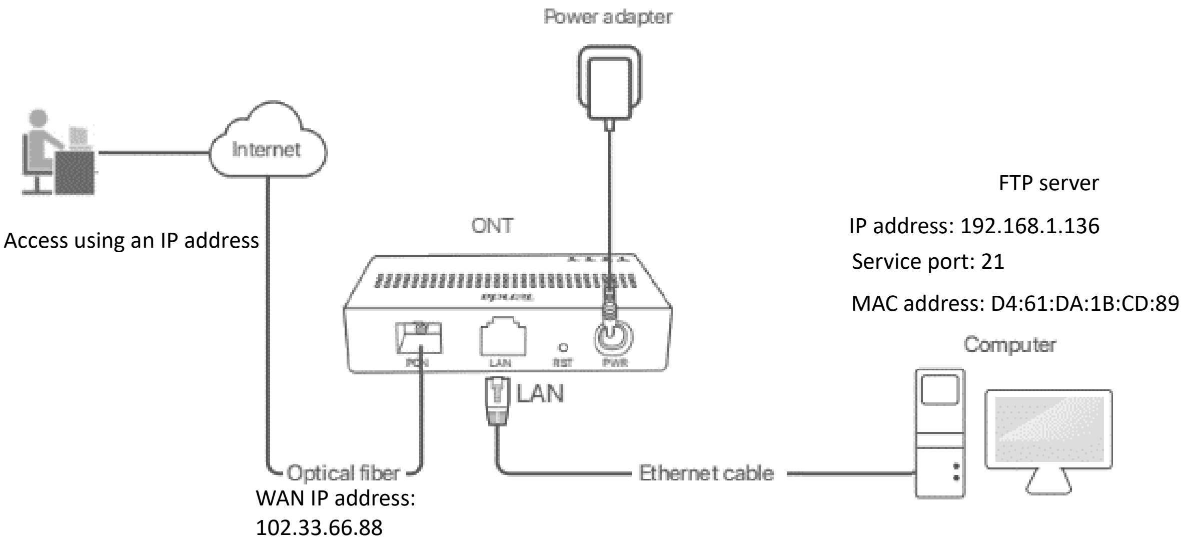
Solution: You can configure the port forwarding function to reach the goal.

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
- The WAN IP address of the router: 102.33.66.88

TIP

- 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.

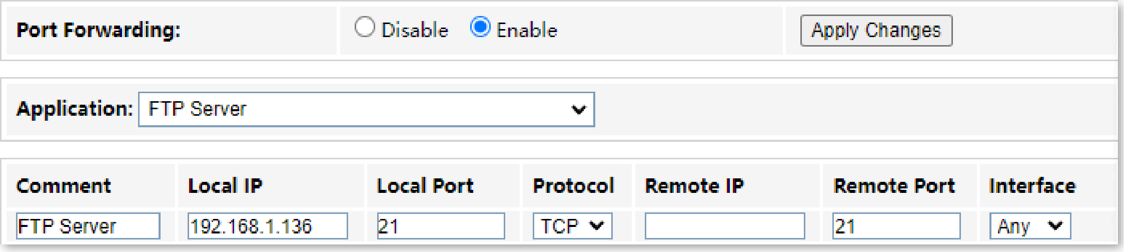


Procedure:

Step 1 Log in to the web UI of the ONT.

Step 2 Add a port forwarding rule.

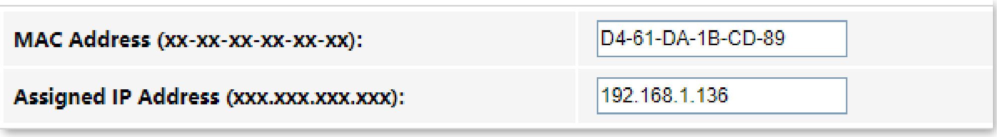
1. Navigate to **Services** > **Firewall** > **Port Forwarding**.
2. Set **Port Forwarding** to **Enable**, and click **Apply Changes**.
3. Select **FTP Server** from the **Application** drop-down list.
4. (Optional) Modify **Comment** for the rule, which is **FTP Server** in this example.
5. Set **Local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



Port Forwarding:	○ Disable ● Enable		Apply Changes			
Application:	FTP Server					
Comment	Local IP	Local Port	Protocol	Remote IP	Remote Port	Interface
FTP Server	192.168.1.136	21	TCP		21	Any

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

1. Navigate to **Services** > **Service** > **DHCP**.
2. Click **MAC-Based Management**.
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

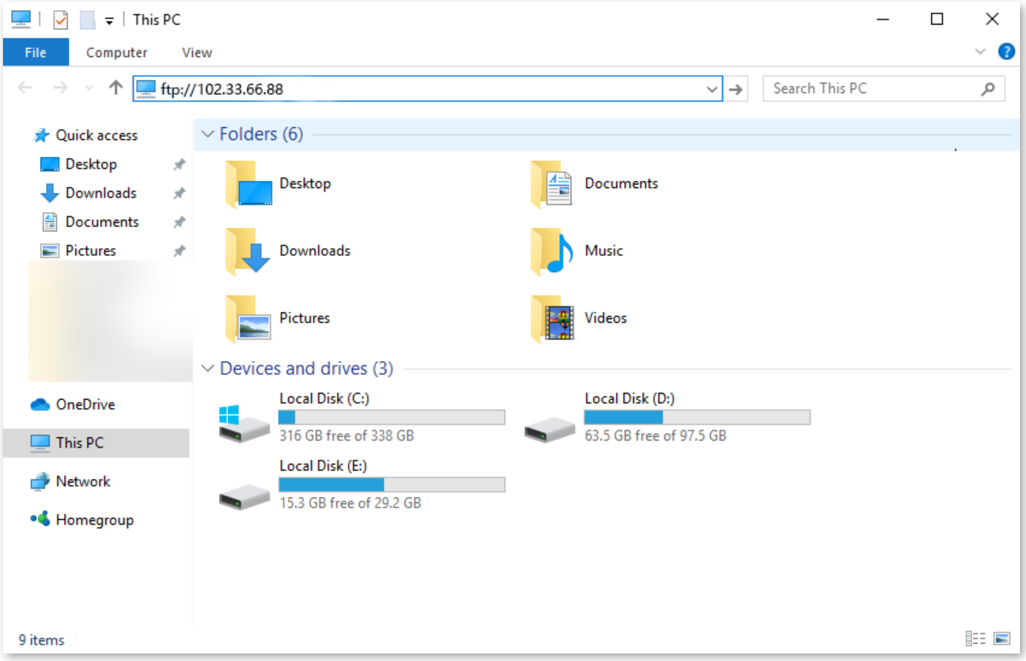
5. Click **Assign IP**.

---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:

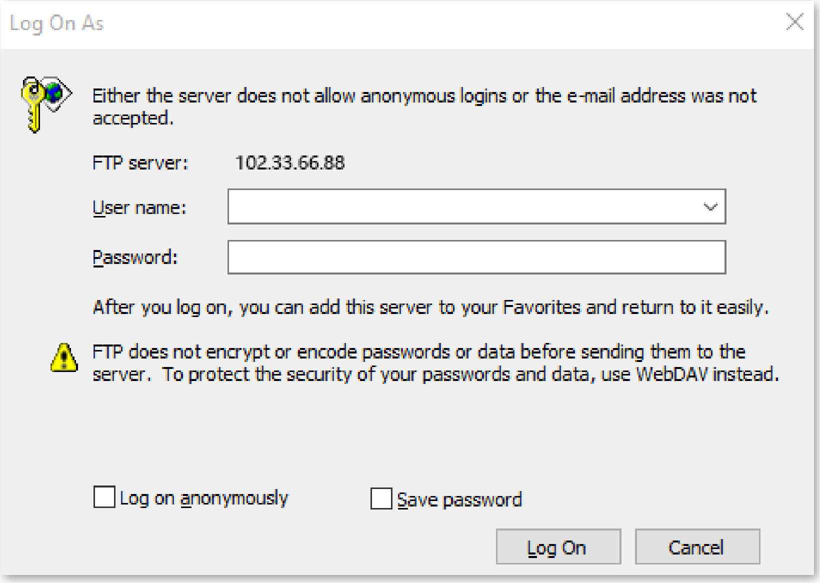
Open the file explorer on a computer that can access the internet, and visit **ftp://102.33.66.88**.



This PC

ftp://102.33.66.88

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



Log On As

Either the server does not allow anonymous logins or the e-mail address was not accepted.

FTP server: 102.33.66.88

User name:

Password:

After you log on, you can add this server to your Favorites and return to it easily.

FTP does not encrypt or encode passwords or data before sending them to the server. To protect the security of your passwords and data, use WebDAV instead.

□ Log on anonymously

□ Save password

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

TIP

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

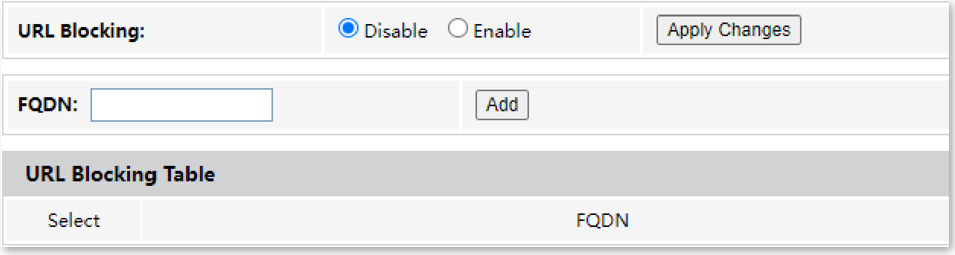
- Ensure that the LAN port number configured in the port forwarding function is the same as the service port number set on the server.
- Close the firewall, antivirus software and security guards on the host of the FTP server and try again.

7.2.5 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 configuration 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: ● Disable ○ Enable [Apply Changes]

FQDN: [ ] [Add]

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 goal.

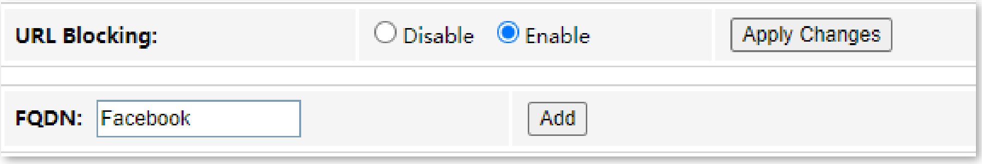
Procedure:

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: ○ Disable ● Enable [Apply Changes]

FQDN: Facebook [Add]

---End

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

7.2.6 DMZ

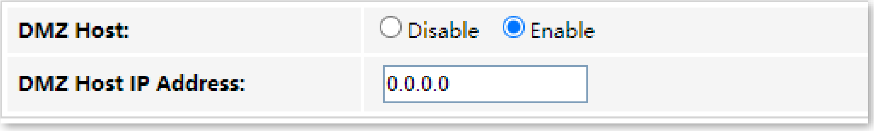
Overview

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.

NOTE

- 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 configuration page, log in to the web UI of the ONT and navigate to **Services** > **Firewall** > **DMZ**.



DMZ Host:	○ Disable ● Enable
DMZ Host IP Address:	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.

Goal: 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 goal.

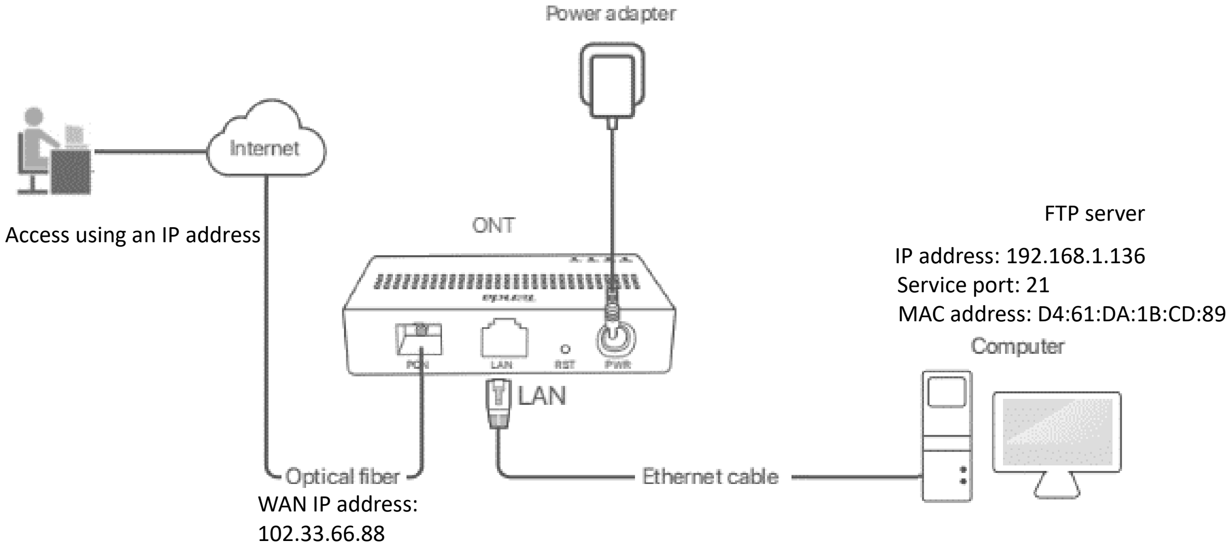
Assume that the information of the FTP server includes:

- 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.

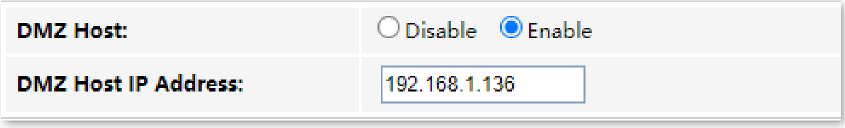


Procedure:

Step 1 Log in to the web UI of the ONT.

Step 2 Set the server host as the DMZ host.

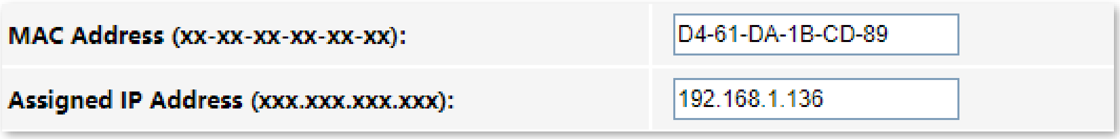
1. Navigate to **Services** > **Firewall** > **DMZ**.
2. Select **Enable** for **DMZ Host**.
3. Enter the IP address of the server host, which is **192.168.1.136** in this example.
4. Click **Apply Changes**.



DMZ Host:	○ Disable ● Enable
DMZ Host IP Address:	192.168.1.136

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

1. Navigate to **Services** > **Service** > **DHCP**.
2. Click **MAC-Based Management**.
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):	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 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*".

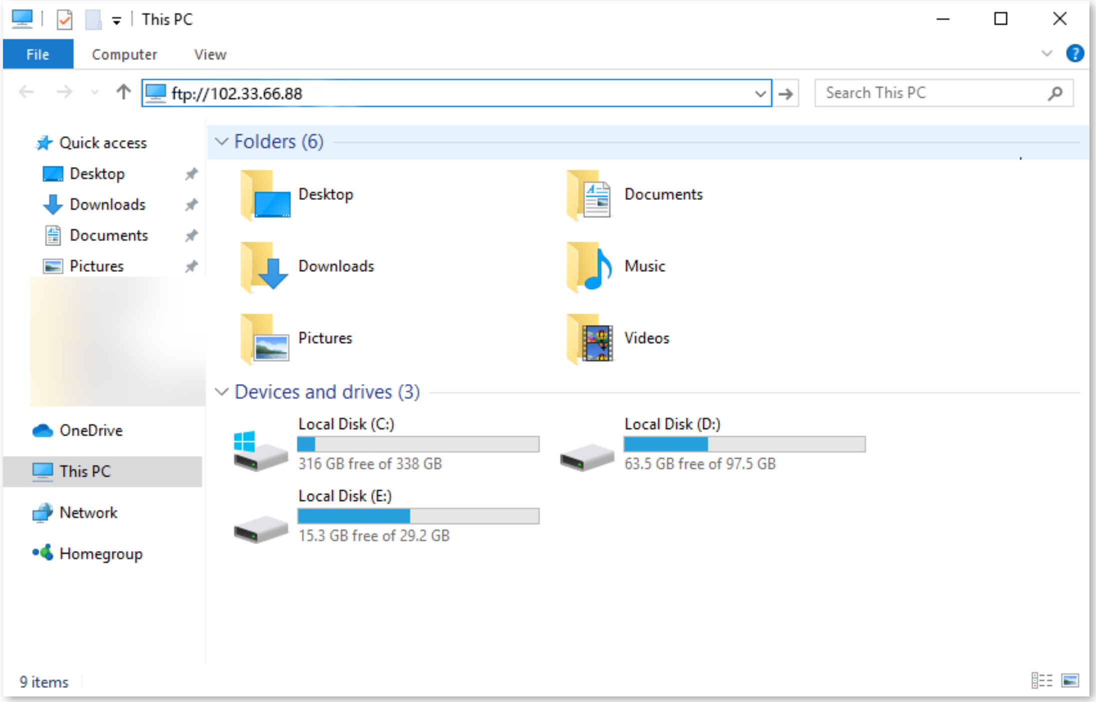
TIP

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.

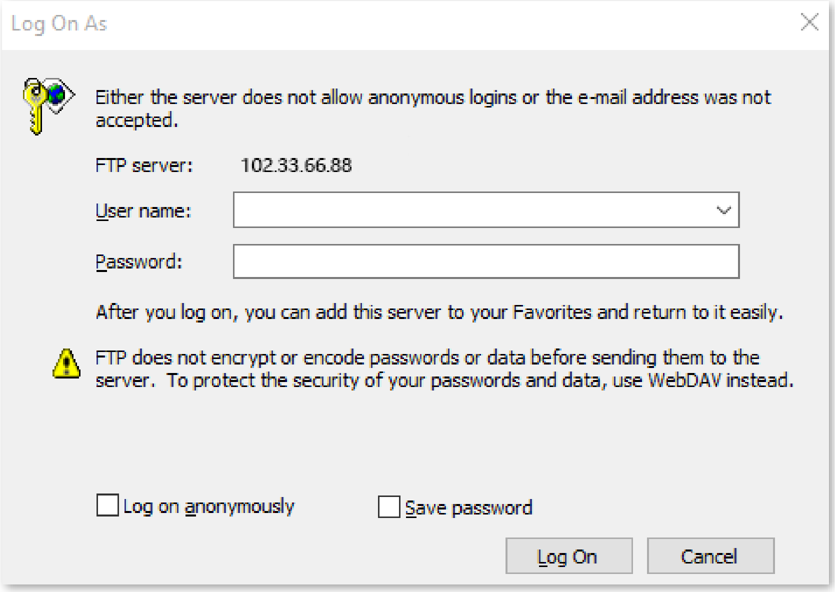
To access the FTP server from the internet:

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



ftp://102.33.66.88

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



Log On As

Either the server does not allow anonymous logins or the e-mail address was not accepted.

FTP server: 102.33.66.88

User name:

Password:

After you log on, you can add this server to your Favorites and return to it easily.

FTP does not encrypt or encode passwords or data before sending them to the server. To protect the security of your passwords and data, use WebDAV instead.

□ Log on anonymously □ Save password

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

TIP

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.

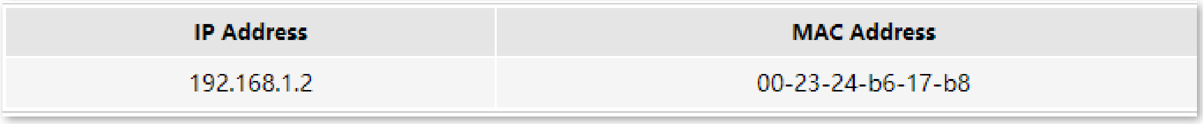
8 Advance

8.1 Advanced settings

8.1.1 ARP table

On this page, you can view the IP address and MAC address of devices connected to the ONT in a wired manner.

To access the page, log in to the web UI of the ONT and choose **Advance** > **Advance** > **ARP Table**.



IP Address	MAC Address
192.168.1.2	00-23-24-b6-17-b8

8.1.2 Routing

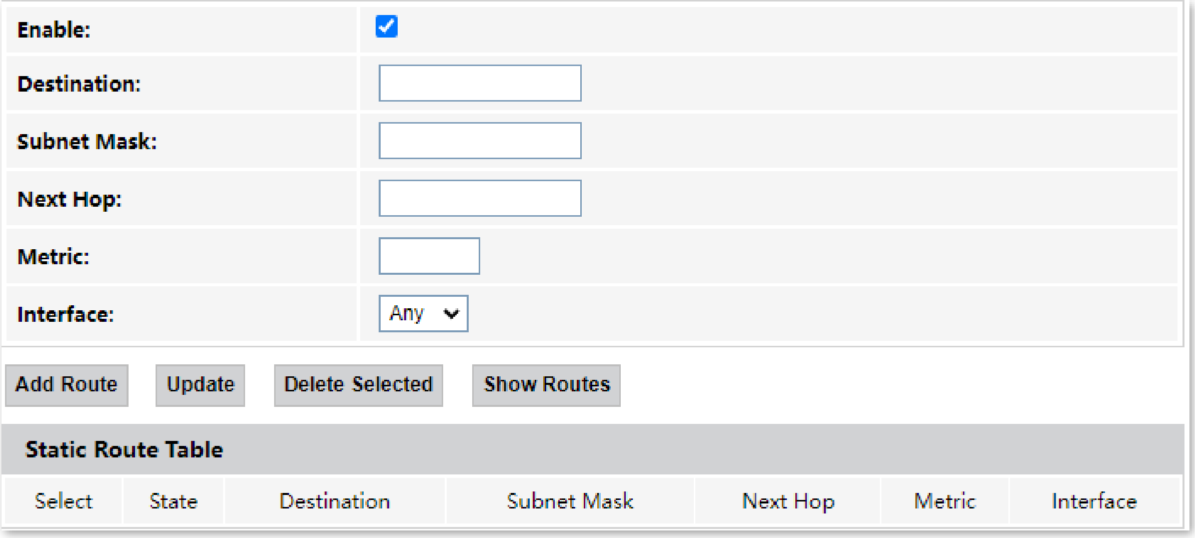
Overview

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:	☑
Destination:	
Subnet Mask:	
Next Hop:	
Metric:	
Interface:	Any

Static Route Table

Select	State	Destination	Subnet Mask	Next Hop	Metric	Interface

Parameter description

Parameter	Description
Enable	Specifies whether to enable the static route function.
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 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**.

Add a new static route rule

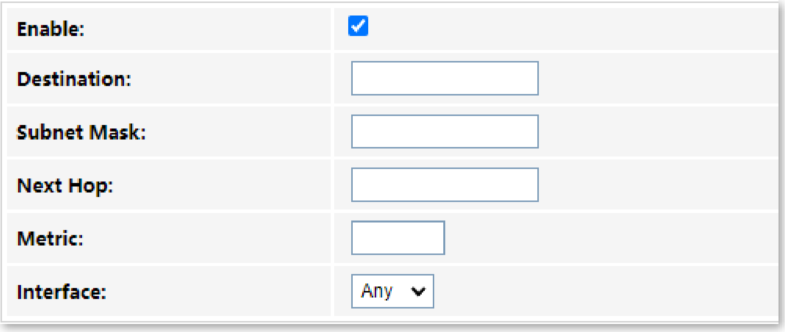
Step 1 Log in to the web UI of the ONT.

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:	☑
Destination:	
Subnet Mask:	
Next Hop:	
Metric:	
Interface:	Any

---End

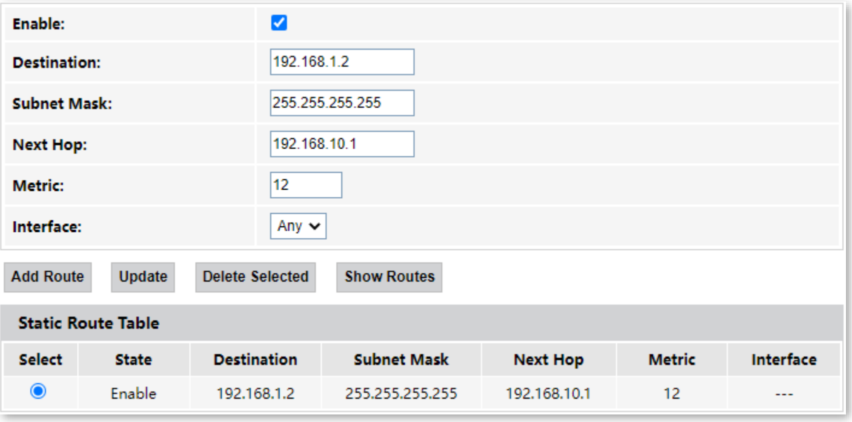
After the configuration is completed, the static rule will be displayed in **Static Route Table**.

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.

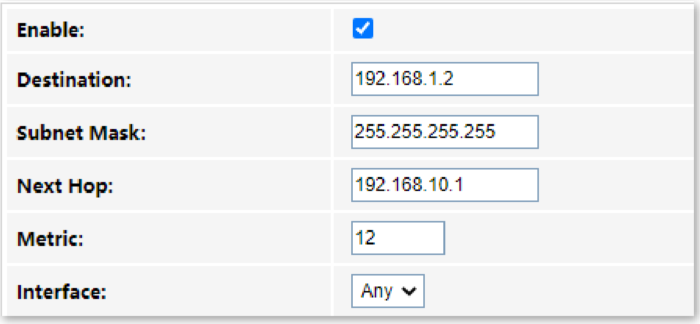


Enable:	☑
Destination:	192.168.1.2
Subnet Mask:	255.255.255.255
Next Hop:	192.168.10.1
Metric:	12
Interface:	Any

Static Route Table

Select	State	Destination	Subnet Mask	Next Hop	Metric	Interface
●	Enable	192.168.1.2	255.255.255.255	192.168.10.1	12	---

Step 4 Modify the parameters of the rule as required.

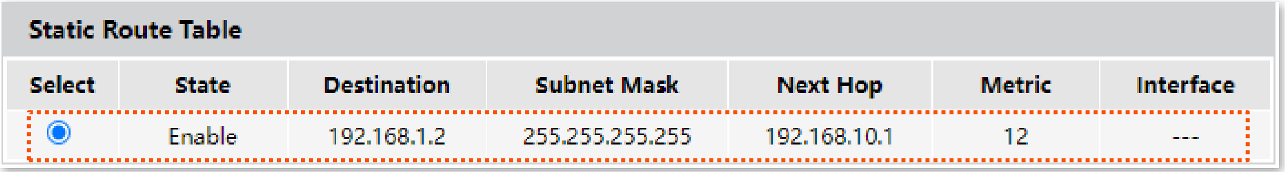


Enable:	☑
Destination:	192.168.1.2
Subnet Mask:	255.255.255.255
Next Hop:	192.168.10.1
Metric:	12
Interface:	Any

Step 5 Click **Update**.

---End

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

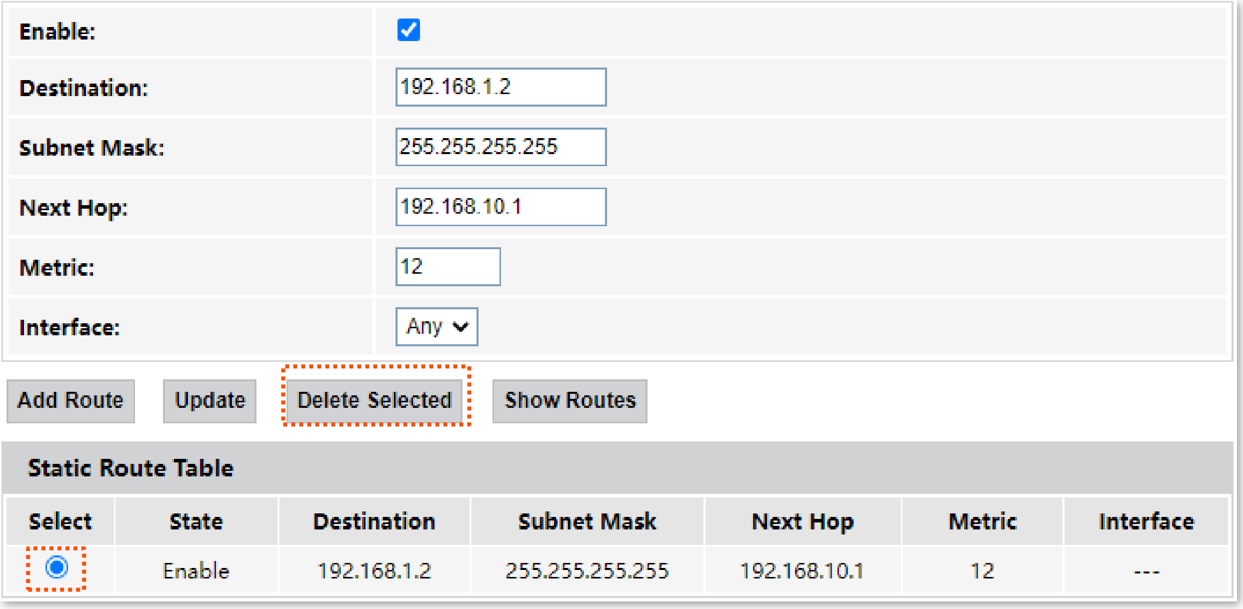


Static Route Table

Select	State	Destination	Subnet Mask	Next Hop	Metric	Interface
●	Enable	192.168.1.2	255.255.255.255	192.168.10.1	12	---

Delete an existing rule

To delete an existing rule, select the rule in **Static Route Table** and click **Delete Selected**.



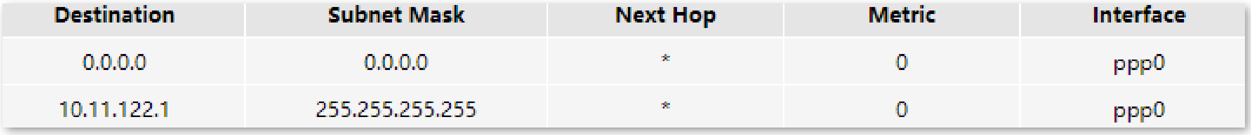
Enable:	☑
Destination:	192.168.1.2
Subnet Mask:	255.255.255.255
Next Hop:	192.168.10.1
Metric:	12
Interface:	Any

Static Route Table

Select	State	Destination	Subnet Mask	Next Hop	Metric	Interface
●	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.



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

TIP

- 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.

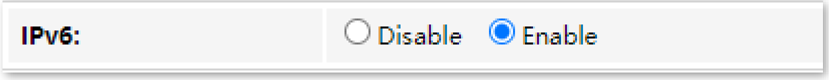
8.2 IPv6 settings

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.

8.2.1 IPv6 status

On this page, you can enable or disable the IPv6 function of the ONT.

To access the page, log in to the web UI of the ONT and navigate to **Advance** > **IPv6** > **IPv6 Enable/Disable**. Select **Enable** or **Disable** and click **Apply Changes**.



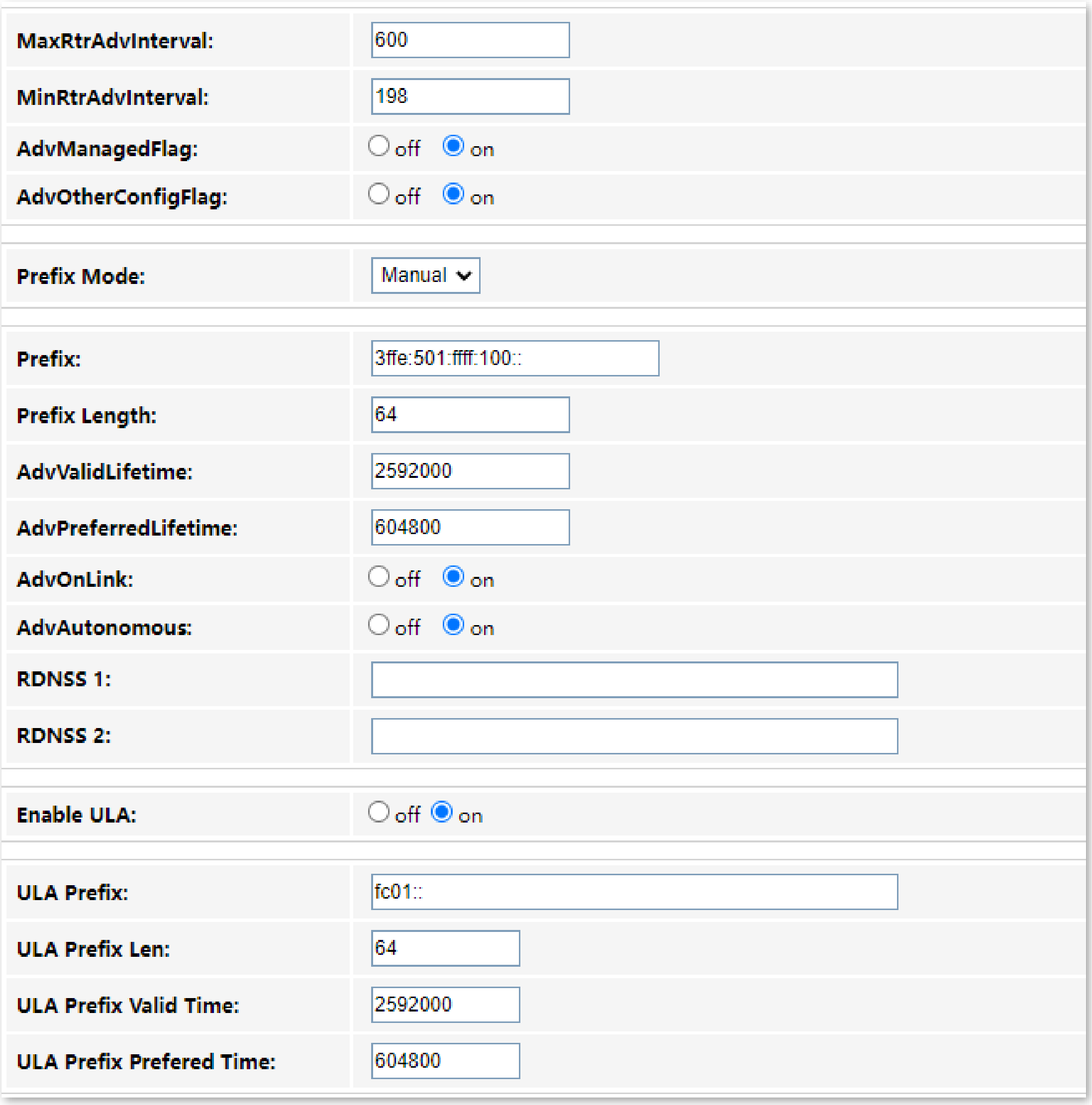
IPv6: ○ Disable ● Enable

8.2.2 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**.



MaxRtrAdvInterval:	600
MinRtrAdvInterval:	198
AdvManagedFlag:	○ off ● on
AdvOtherConfigFlag:	○ off ● on
Prefix Mode:	Manual
Prefix:	3ffe:501:ffff:100::
Prefix Length:	64
AdvValidLifetime:	2592000
AdvPreferredLifetime:	604800
AdvOnLink:	○ off ● on
AdvAutonomous:	○ off ● on
RDNSS 1:	
RDNSS 2:	
Enable ULA:	○ off ● on
ULA Prefix:	fc01::
ULA Prefix Len:	64
ULA Prefix Valid Time:	2592000
ULA Prefix Prefered Time:	604800

Parameter description

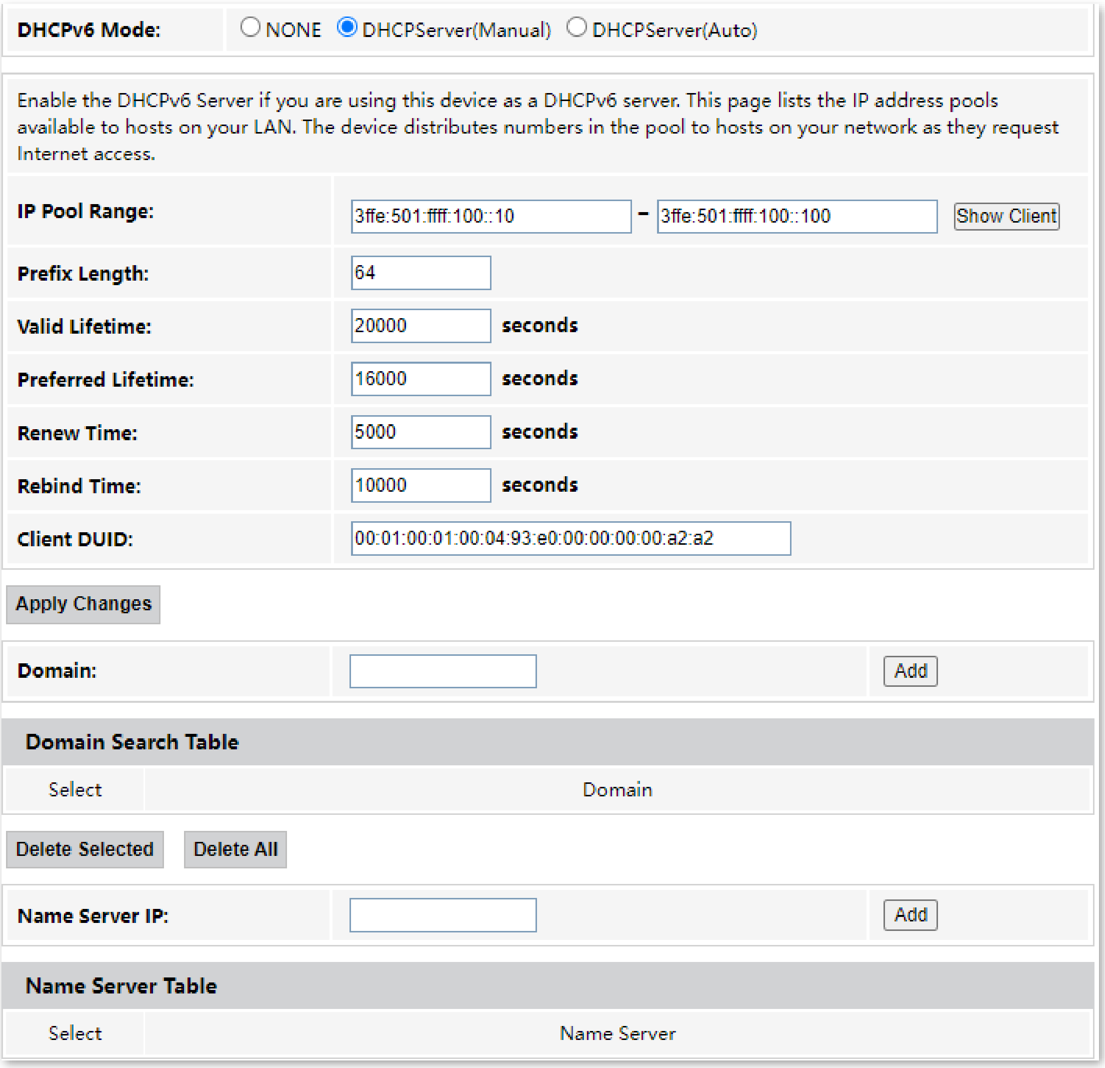
Parameter	Description
MaxRtrAdvInterval MinRtrAdvInterval	Specify the Maximum and Minimum Router Advertisement Intervals. They are the intervals between each router advertisement message. The router sends these messages periodically. The actual interval used is randomly selected from a value between the minimum and maximum values.
AdvManagedFlag AdvOtherConfigFlag	Specify the Advertisement Managed Flag and Advertisement Other Configuration Flag. • **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	Specifies the configuring mode of the prefix which is assigned to the IPv6 host, including **Auto** and **Manual**. • **Auto**: The ONT automatically assigns a prefix to the IPv6 host.

Parameter	Description
	- **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. 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. TIP The valid lifetime must be greater than or equal to the preferred lifetime.
AdvPreferredLifetime	
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	Specifies whether to enable the Unique Local Address (ULA). 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.
ULA Prefix	Specify the ULA prefix information advertised by the ONT to hosts for generating unique local addresses. They are available only when **Enable ULA** is set to **on**.
ULA Prefix Len	
ULA Prefix Valid Time	Specify the valid lifetime and preferred lifetime of ULA prefix. They are available only when **Enable ULA** is set to **on**. 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**. TIP The valid time must be greater than or equal to the preferred time.
ULA Prefix Preferred Time	

8.2.3 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: ○ NONE ● DHCPServer(Manual) ○ DHCPServer(Auto)

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.

IP Pool Range:	3ffe:501:ffff:100::10 - 3ffe:501:ffff:100::100
Prefix Length:	64
Valid Lifetime:	20000 seconds
Preferred Lifetime:	16000 seconds
Renew Time:	5000 seconds
Rebind Time:	10000 seconds
Client DUID:	00:01:00:01:00:04:93:e0:00:00:00:00:a2:a2

Domain Search Table

Select	Domain

Name Server Table

Select	Name Server

Parameter description

Parameter	Description
DHCPv6 Mode	You can select a DHCPv6 server mode or disable it. - **NONE**: The DHCPv6 server of the ONT is disabled. - **DHCPServer(Manual)**: The DHCPv6 server of the ONT is enabled. You need to define the IP address pool, prefix length and other required parameters for IPv6 addresses to be assigned to IPv6 hosts. - **DHCPServer(Auto):** The ONT defines the IPv6 addresses to be assigned to the IPv6 host automatically.
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. 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.
Preferred Lifetime	

Parameter	Description
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	Specifies the DHCP Unique Identifier (DUID) assigned to clients. 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.
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	

9 Diagnostics

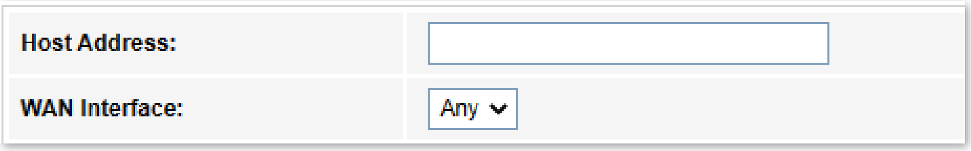
9.1 Ping and Tracert

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

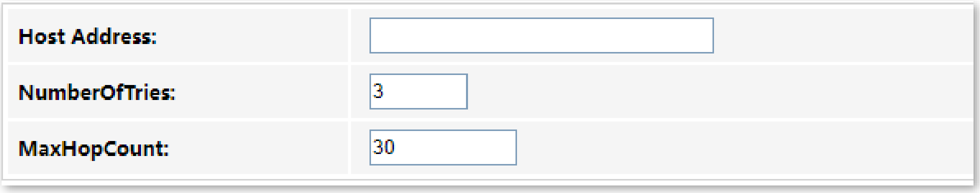


Host Address:	
WAN Interface:	Any

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:	
NumberOfTries:	3
MaxHopCount:	30

Parameter description

Parameter	Description
Host Address	Specifies the IP address or domain name of the tracert target.
NumberOfTries	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.

9.2 Execute Ping to test connectivity

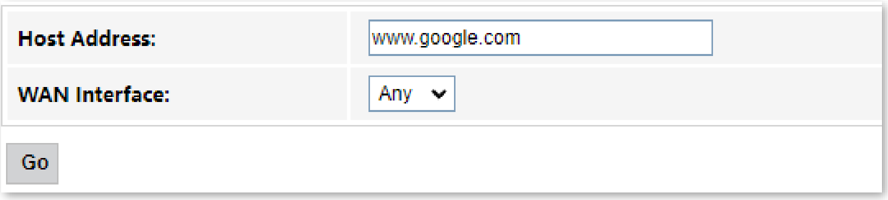
Step 1 Log in to the web UI of the ONT.

Step 2 Navigate to **Diagnostics** > **Diagnostics** > **Ping**.

Step 3 Enter the IP address or domain name in **Host Address**, which is **www.google.com** in this example.

Step 4 Select **Any** in **WAN Interface**.

Step 5 Click **Go**.



Host Address:	www.google.com
WAN Interface:	Any

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

---End

9.3 Execute Traceroute to test routing

Step 1 Log in to the web UI of the ONT.

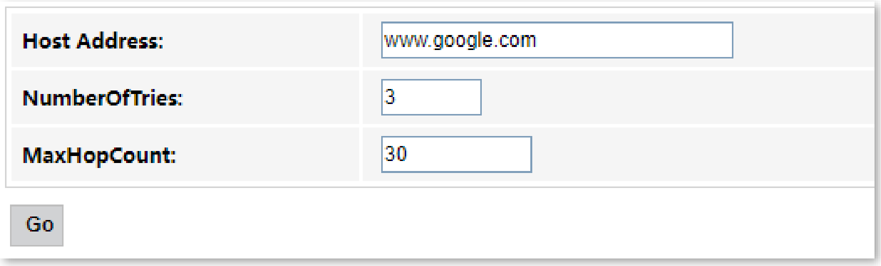
Step 2 Navigate to **Diagnostics** > **Diagnostics** > **Tracert**.

Step 3 Enter the IP address or domain name in **Host Address**, which is **www.google.com** in this example.

Step 4 Specify the number of attempts in **NumberOfTries**.

Step 5 Specify the number of hops in **Max Hop Count**.

Step 6 Click **Go**.



Host Address:	www.google.com
NumberOfTries:	3
MaxHopCount:	30

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

---End

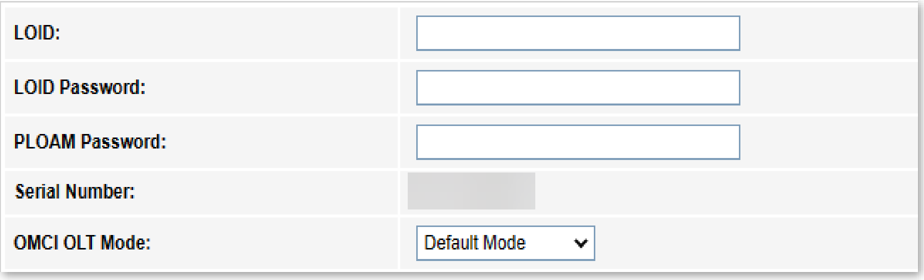
10 Admin

10.1 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.

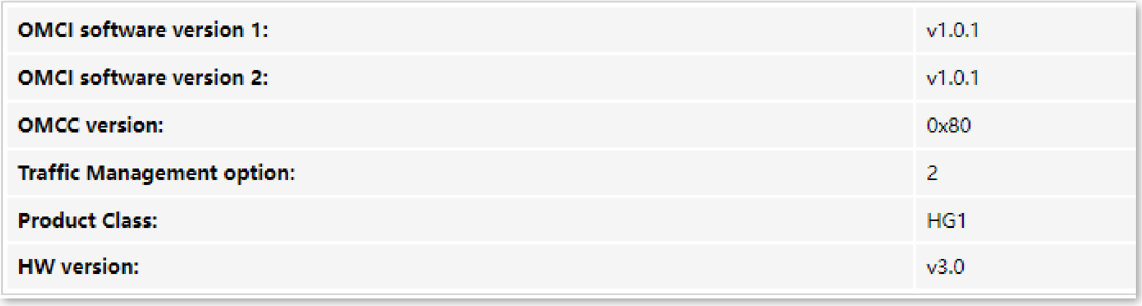


LOID:	
LOID Password:	
PLOAM Password:	
Serial Number:	
OMCI OLT Mode:	Default Mode

10.2 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.

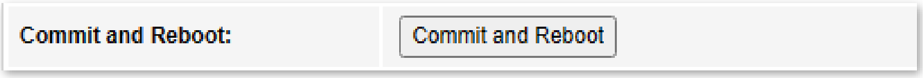


OMCI software version 1:	v1.0.1
OMCI software version 2:	v1.0.1
OMCC version:	0x80
Traffic Management option:	2
Product Class:	HG1
HW version:	v3.0

10.3 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**.

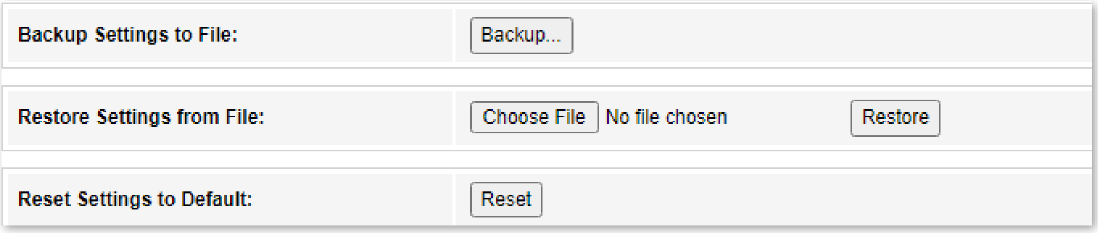


Commit and Reboot:

10.4 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:	Backup...
Restore Settings from File:	Choose File No file chosen Restore
Reset Settings to Default:	Reset

10.4.1 Back up the configuration of the ONT

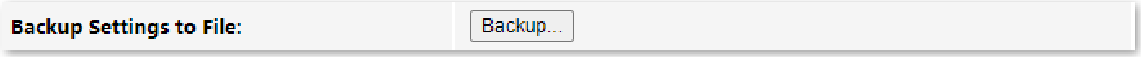
You can back up the configuration of the ONT at a certain time for future restoration after you change the settings or reset the ONT.

Procedure:

Step 1 Log in to the web UI of the ONT.

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

Step 3 Click **Backup...**.



Backup Settings to File:	Backup...

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

---End

10.4.2 Restore previous configuration of the ONT

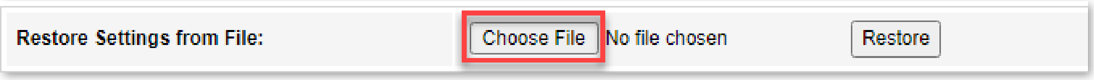
You can restore the previous configuration of the ONT using the backup file that you have downloaded.

Procedure:

Step 1 Log in to the web UI of the ONT.

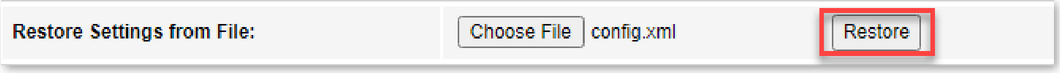
Step 2 Navigate to **Admin** > **Admin** > **Backup/Restore**.

Step 3 Click **Choose File**, and select the configuration file.



Restore Settings from File:	Choose File No file chosen Restore

Step 4 Click **Restore**.


Restore Settings from File: Choose File config.xml Restore

The ONT reboots to enable the configuration to take effect.

---End

10.4.3 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.

TIP

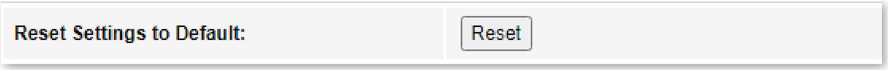
Resetting the ONT will clear all previous personalized configurations. It is recommended to back up the configuration of the ONT in advance.

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

10.5 Password

On this page, you can change the login password for the ONT. The default login user name and password are **admin**. You can only change the password, and the original password is required during the process.

Procedure:

Step 1 Log in to the web UI of the ONT.

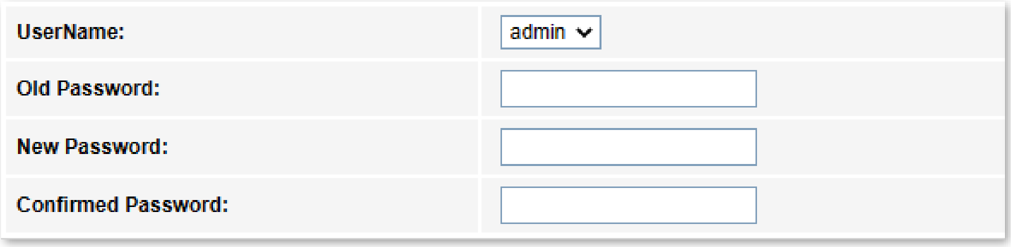
Step 2 Navigate to **Admin** > **Admin** > **Password**.

Step 3 Set **UserName** according to the actual permissions.

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

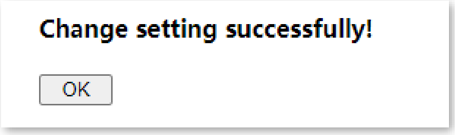
Step 5 Enter your new password in **New Password** and **Confirmed Password**.

Step 6 Click **Apply Changes**.



UserName:	admin
Old Password:	
New Password:	
Confirmed Password:	

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



Change setting successfully!

---End

10.6 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:

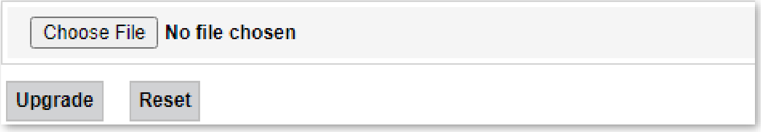
Step 1 Go to www.tendacn.com. Download an applicable firmware of the ONT to your local computer and unzip it.

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**.



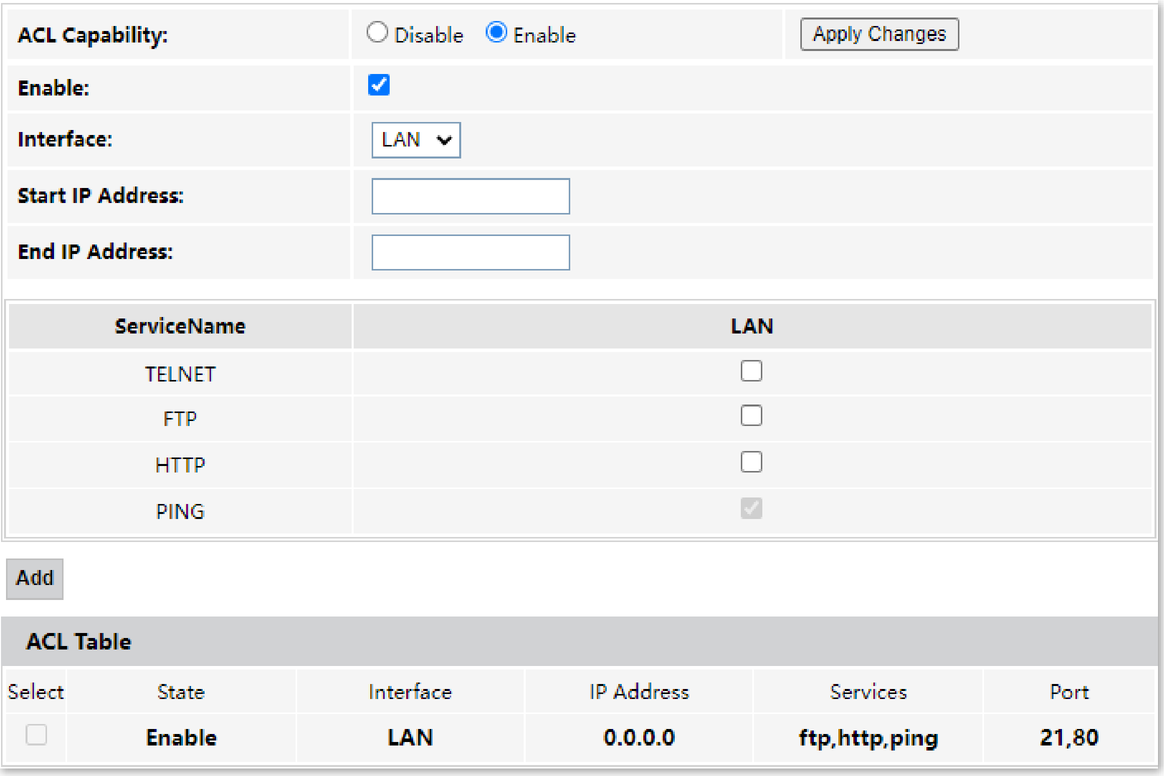
The ONT reboots automatically.

---End

10.7 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:	○ Disable ● Enable	Apply Changes
Enable:	☑	
Interface:	LAN	
Start IP Address:		
End IP Address:		

ServiceName	LAN
TELNET	□
FTP	□
HTTP	□
PING	☑

ACL Table

Select	State	Interface	IP Address	Services	Port
□	Enable	LAN	0.0.0.0	ftp,http,ping	21,80

Parameter description

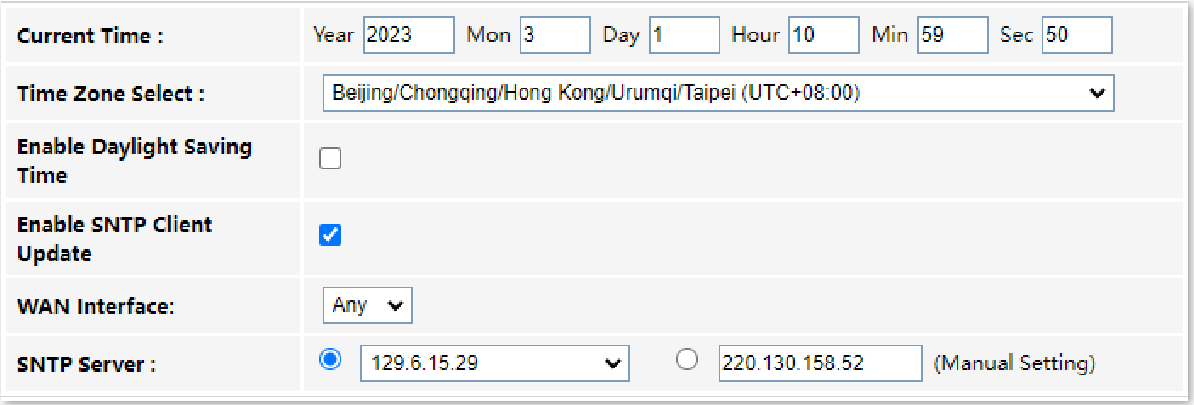
Parameter	Description
ACL Capability	Specifies whether to enable the ACL function of the ONT.
Enable	Specifies the control mode of the rule. • When **Enable** is selected, traffic that meets the criteria of the rule can pass through the specified port of the ONT. • When **Enable** is deselected, traffic that meets the criteria of the rule is discarded at the specified port of the ONT.
Interface	Specifies the interface that the access control rule applies to, including **LAN** and **WAN**. • **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	Specifies the protocol adopted by the traffic, or the types of traffic. - **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. - **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.

10.8 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 2023 Mon 3 Day 1 Hour 10 Min 59 Sec 50
Time Zone Select :	Beijing/Chongqing/Hong Kong/Urumqi/Taipei (UTC+08:00)
Enable Daylight Saving Time	□
Enable SNTP Client Update	☑
WAN Interface:	Any
SNTP Server :	● 129.6.15.29 ○ 220.130.158.52 (Manual Setting)

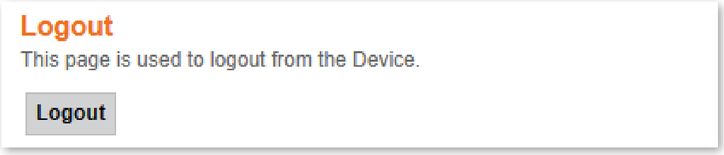
Parameter description

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	Daylight Saving Time (DST) is the practice of advancing clocks during warmer months so that darkness falls later each day according to the clock. 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.
Enable SNTP Client Update	Specifies whether to enable automatic update of system time through synchronization with SNTP server. 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.
WAN Interface	Specifies the interface through which the ONT updates its system time with the SNTP server.
SNTP Server	You can choose a preset SNTP server, or manually set the IP address for updating system time.

10.9 Logout

To access the page, 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.



Logout

This page is used to logout from the Device.

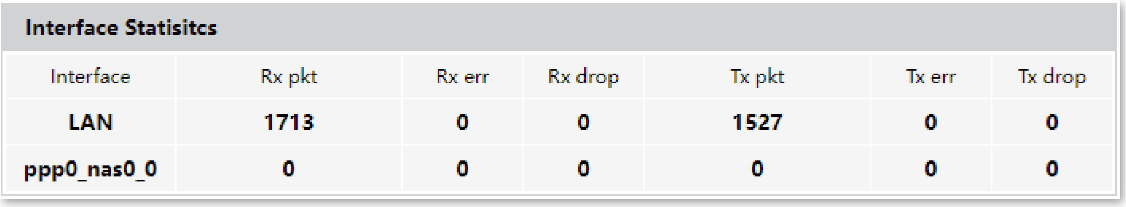
11 Statistics

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

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**.



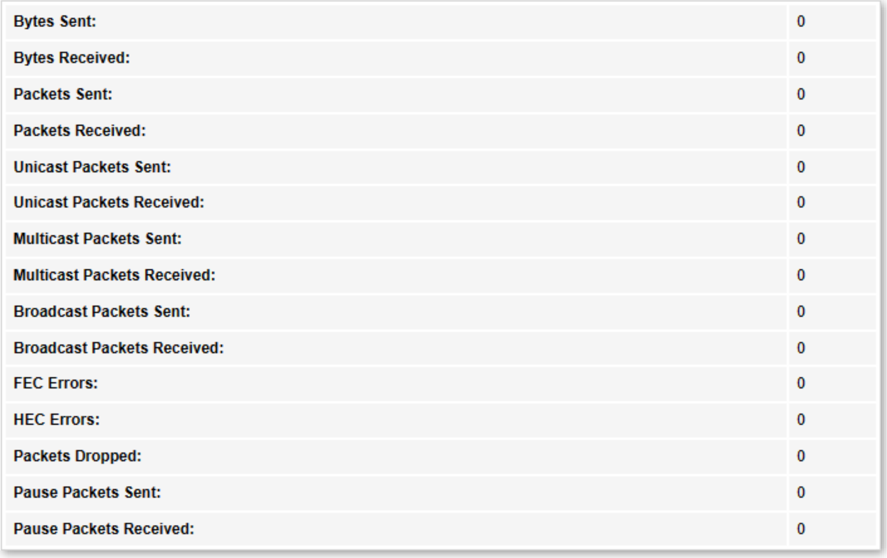
Interface Statisitcs

Interface	Rx pkt	Rx err	Rx drop	Tx pkt	Tx err	Tx drop
LAN	1713	0	0	1527	0	0
ppp0_nas0_0	0	0	0	0	0	0

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

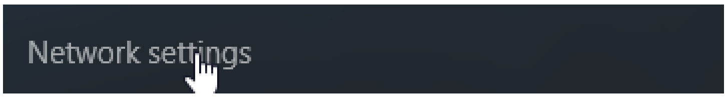
Appendixes

A.1 Configure the computer to obtain an IPv4/IPv6 address automatically

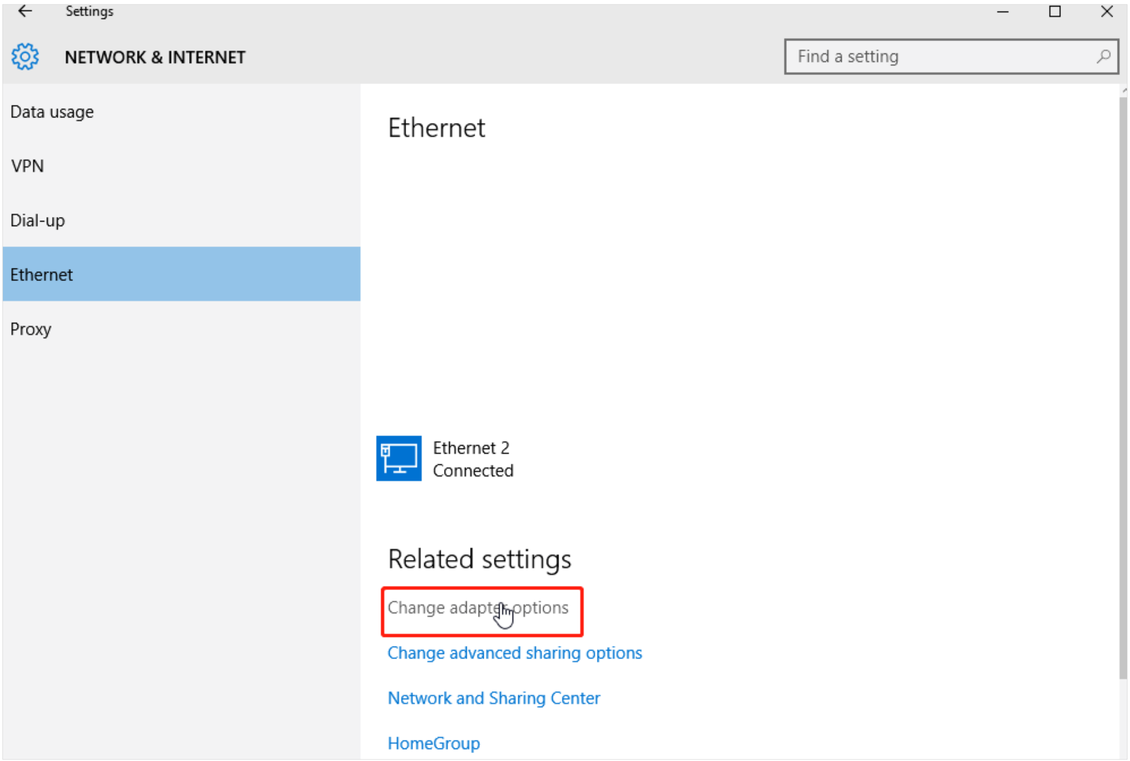
Perform the configuration procedure in Windows 10, Windows 8 and Windows 7 as required. A computer installed with a wired network adapter is used as an example to describe the procedure.

A.1.1 Windows 10

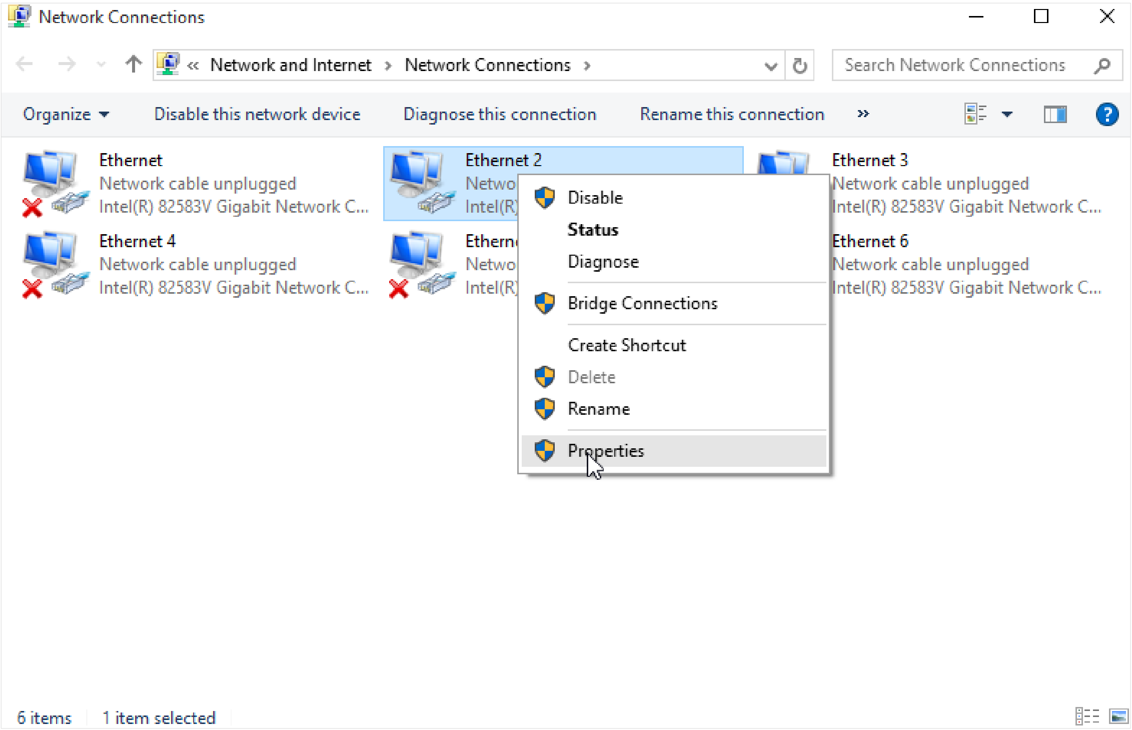
Step 1 Click 🖳 in the bottom right corner of the desktop and choose **Network settings**.



Step 2 Click **Change adapter options**.



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



Ethernet
Network cable unplugged
Intel(R) 82583V Gigabit Network C...

Ethernet 2
Netwo
Intel(R)

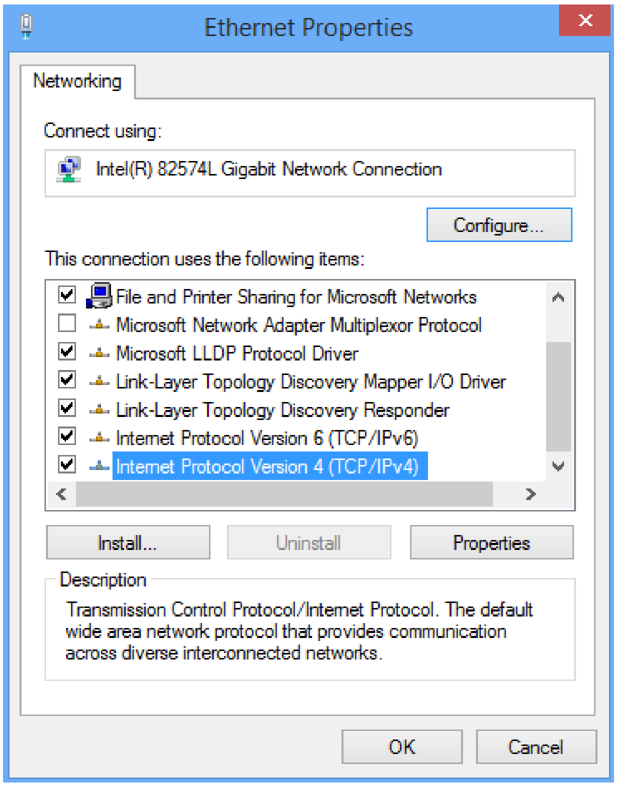
Ethernet 3
Network cable unplugged
Intel(R) 82583V Gigabit Network C...

Ethernet 4
Network cable unplugged
Intel(R) 82583V Gigabit Network C...

Ethern
Netwo
Intel(R)

Ethernet 6
Network cable unplugged
Intel(R) 82583V Gigabit Network C...

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



Connect using:

Intel(R) 82574L Gigabit Network Connection

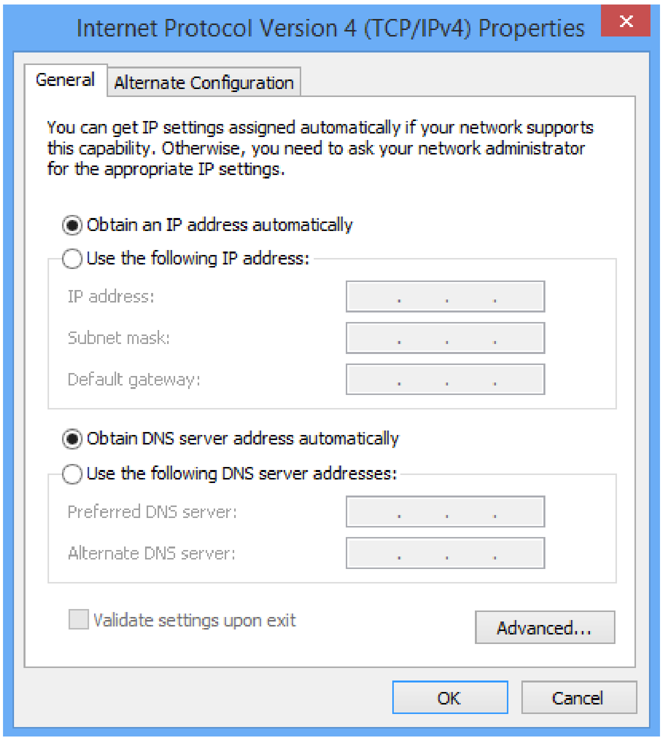
This connection uses the following items:

☑ File and Printer Sharing for Microsoft Networks
☐ Microsoft Network Adapter Multiplexor Protocol
☑ Microsoft LLDP Protocol Driver
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

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



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

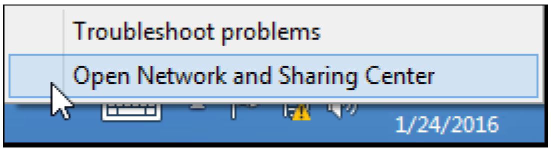
□ Validate settings upon exit

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

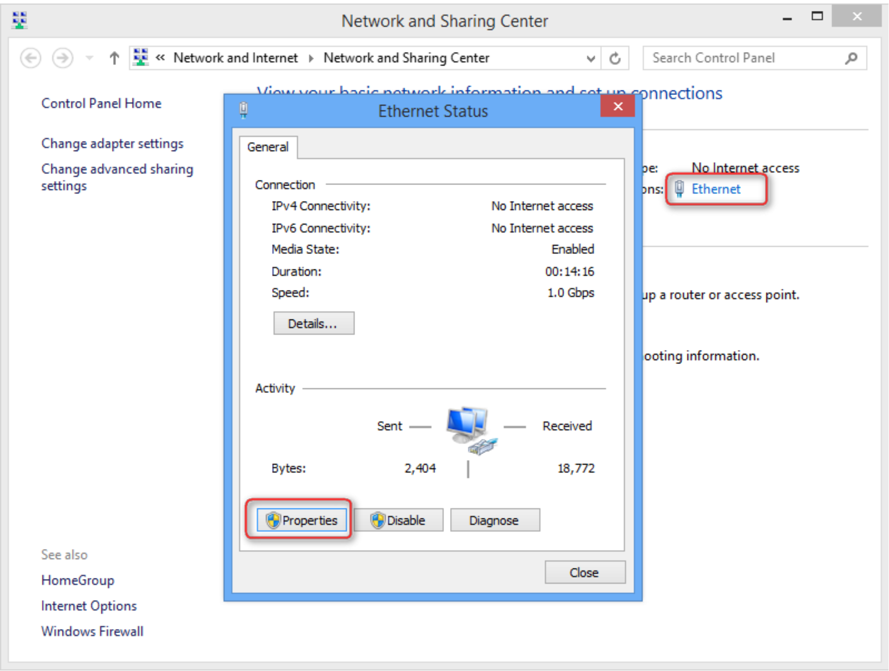
---End

A.1.2 Windows 8

Step 1 Right-click in the bottom right corner of the desktop and choose **Open Network and Sharing Center**.



Step 2 Click **Ethernet** and then **Properties**.



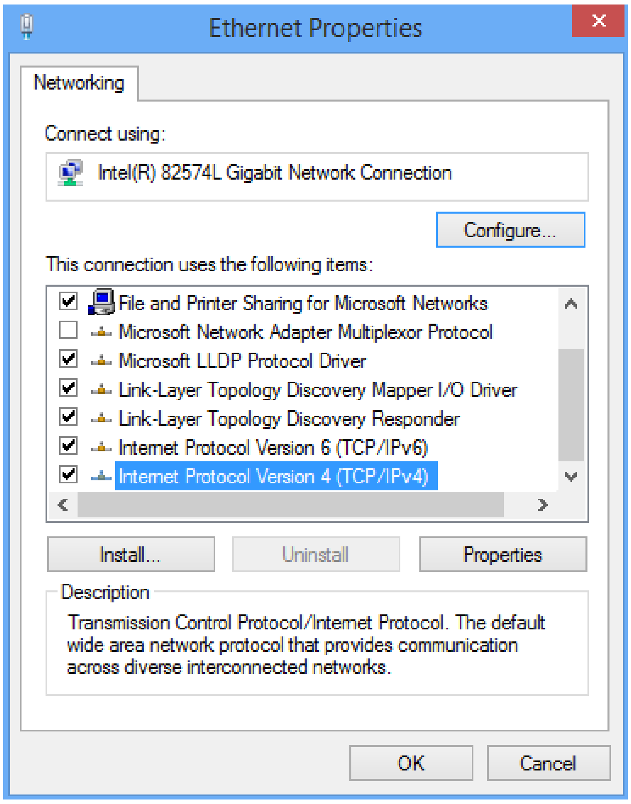
Connection

IPv4 Connectivity:	No Internet access
IPv6 Connectivity:	No Internet access
Media State:	Enabled
Duration:	00:14:16
Speed:	1.0 Gbps

Activity

	Sent	Received
Bytes:	2,404	18,772

Step 3 Double-click **Internet Protocol Version 4 (TCP/IPv4)** or **Internet Protocol Version 6 (TCP/IPv6)**.



Ethernet Properties

Networking

Connect using:

Intel(R) 82574L Gigabit Network Connection

Configure...

This connection uses the following items:

- ☑ File and Printer Sharing for Microsoft Networks
- □ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)

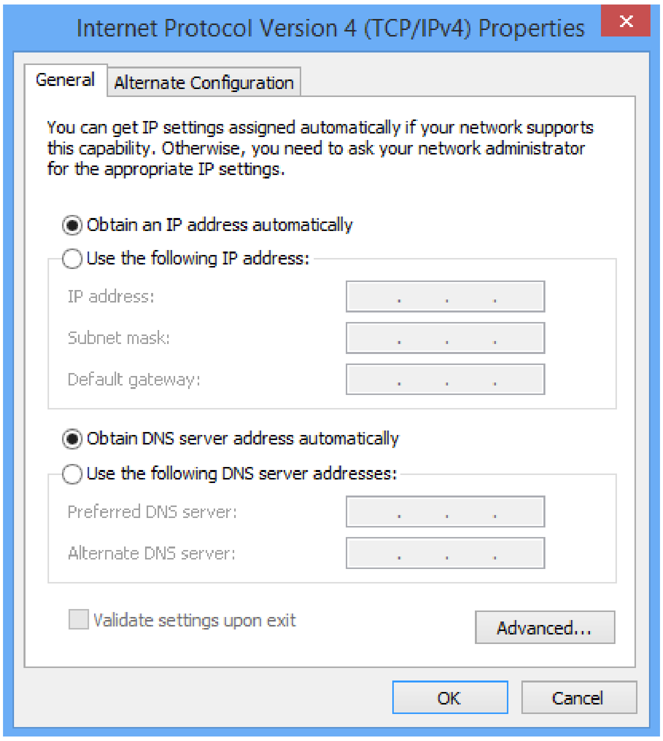
Install... Uninstall Properties

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

OK Cancel

Step 4 Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**, and click **OK**.



Internet Protocol Version 4 (TCP/IPv4) Properties

General Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

Advanced...

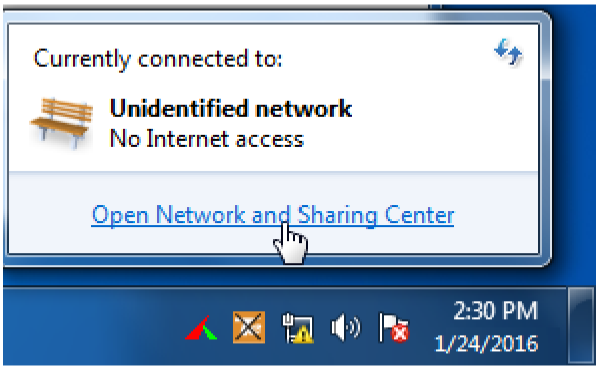
OK Cancel

Step 5 Click **OK** in the **Ethernet Properties** window.

---End

A.1.3 Windows 7

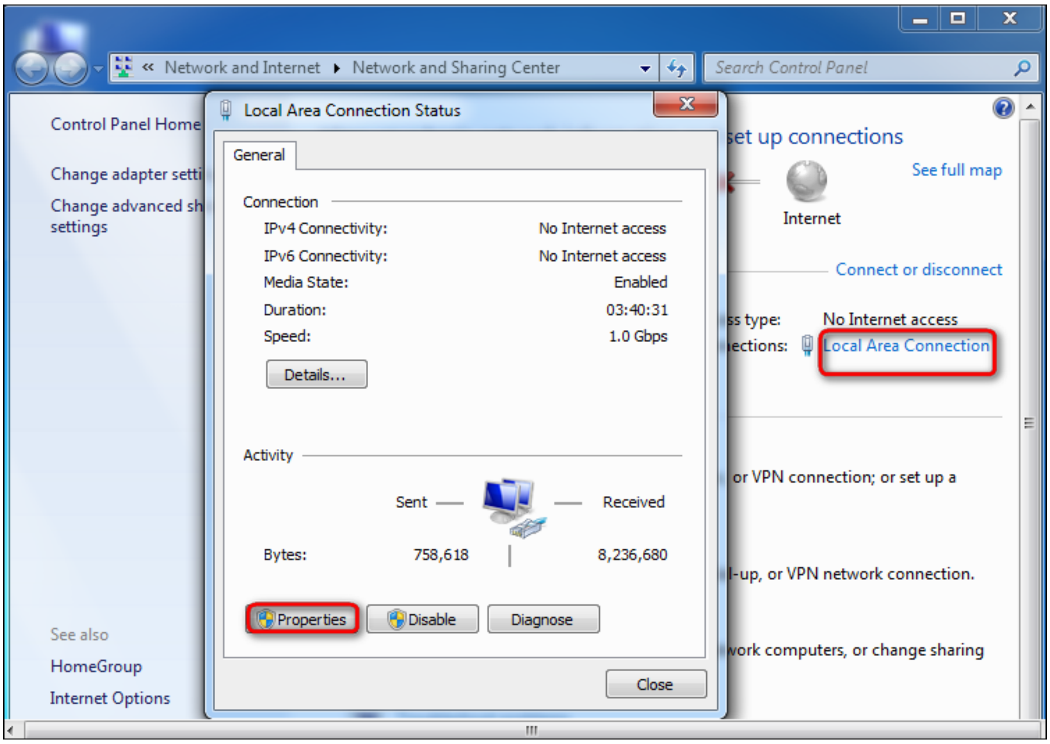
Step 1 Click in the bottom right corner of the desktop and choose **Open Network and Sharing Center**.



Currently connected to:

Unidentified network
No Internet access

Step 2 Click **Local Area Connection** and then click **Properties**.



Connection

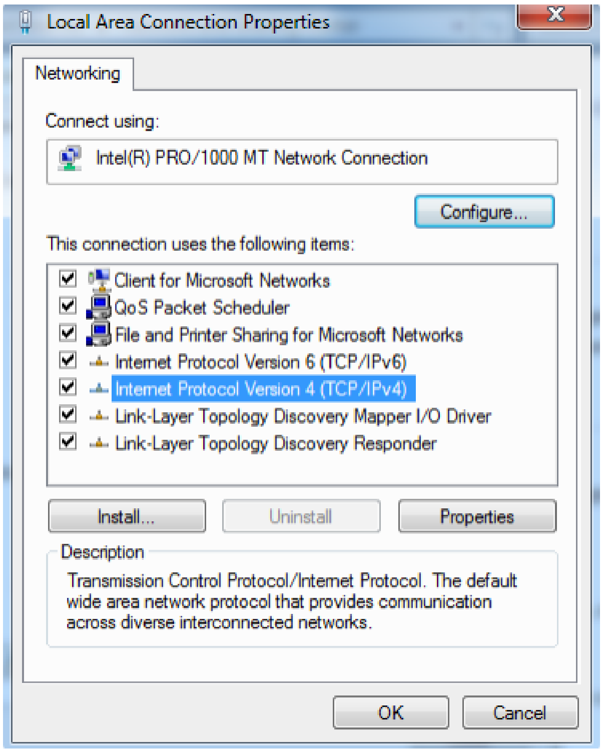
IPv4 Connectivity: No Internet access
IPv6 Connectivity: No Internet access
Media State: Enabled
Duration: 03:40:31
Speed: 1.0 Gbps

Activity

	Sent	Received
Bytes:	758,618	8,236,680

No Internet access

Step 3 Double-click **Internet Protocol Version 4 (TCP/IPv4)** or **Internet Protocol Version 6 (TCP/IPv6)**.



Local Area Connection Properties

Networking

Connect using:

Intel(R) PRO/1000 MT Network Connection

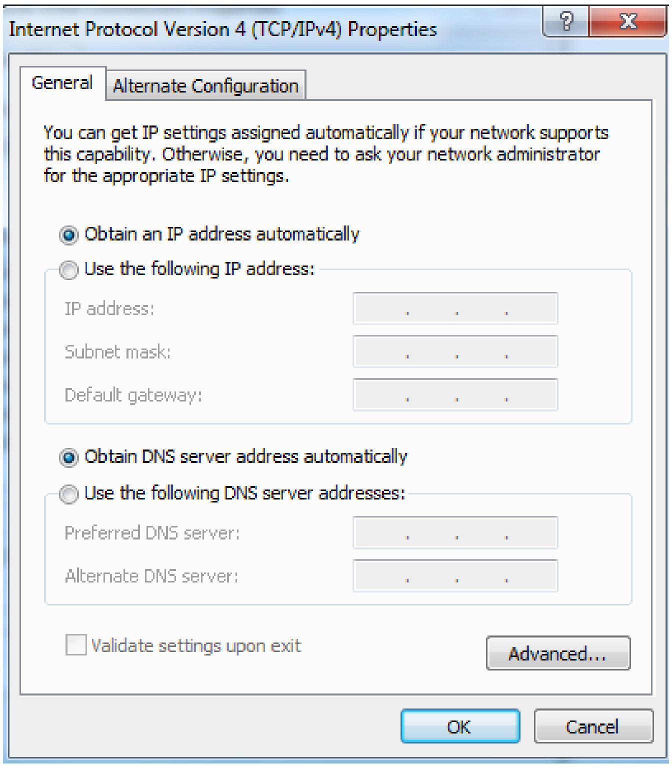
This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Step 4 Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**, and click **OK**.



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

Step 5 Click **OK** in the **Local Area Connection Properties** window.

---End

A.2 Acronyms and abbreviations

Acronym or Abbreviation	Full Spelling
ACL	Access control list
ALG	Application Layer Gateway
ARP	Address Resolution Protocol
CPU	Central processing unit
DDNS	Dynamic Domain Name System
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol version 6
DMZ	Demilitarized zone
DNS	Domain Name System
DST	Daylight Saving Time
DUID	DHCP unique identifier
FQDN	Fully qualified domain name
FTP	File Transfer Protocol
FTTH	Fiber to the Home
HGU	Home Gateway Unit
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IPsec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPoE	Internet Protocol over Ethernet
ISP	Internet service provider
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
MAC	Medium access control

Acronym or Abbreviation	Full Spelling
MTU	Maximum Transmission Unit
OLT	Optical line termination
OMCI	ONU Management Control Interface
ONT	Optical Network Terminal
ONU	Optical network unit
OS	Operating system
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
SFU	Single Family Unit
SIP	Session Initiation Protocol
SLAAC	Stateless address autoconfiguration
SNTP	Simple Network Time Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UI	User interface
ULA	Unique Local Address
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network