Tenda

User Guide

4 Antennas Wireless N300 ADSL2+ Modem Router

Shenzhen Tenda Technology Co.,ltd

Copyright Statement

© 2015 Shenzhen Tenda Technology Co., Ltd. All rights reserved.

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

Disclaimer

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

Contents

Shortcut to Common Function Setup ..... **v**

Chapter 1 Product Overview **1**

1.1 What It Does 1
1.2 Product Features 1
1.3 Package Contents 2
1.4 Front Panel 3
1.5 Back Panel 4

Chapter 2 Hardware Installation **5**

2.1 DSL Access 5
2.2 Ethernet Access 7

Chapter 3 Internet Setup **9**

3.1 Log in to UI (User Interface) 9
3.2 Set up Internet 10
About Link Type 10
About Connection Type 10
Internet Setup Instruction 11
3.3 Quick Wireless Security Setup 18

Chapter 4 Advanced Settings **19**

4.1 Device Info 19
4.2 Advanced Setup 22
4.2.1 Layer2 Interface 23
4.2.2 WAN Service 25
4.2.3 LAN Setup 79
4.2.4 NAT 82
4.2.5 Security 87
4.2.6 Parental Control 90
4.2.7 Bandwidth Control 93
4.2.8 Routing 94
4.2.9 DNS 96
4.2.10 DSL 99
4.2.11 Storage Service 100
4.2.12 Interface Grouping 103
4.2.13 IP Tunnel 105
4.2.14 Certificate 106
4.2.15 Multicast 109
4.2.16 IPTV 111
4.3 Wireless 112
4.3.1 Basic 112
4.3.2 Security 113
4.3.3 MAC Filter 116
4.3.4 Wireless Bridge 117
4.3.5 Station Info 125
4.4 Diagnostics 125

4.4.1 Diagnostics....126
4.4.2 Ping test....126
4.5 Management....127
4.5.1 Settings....127
4.5.2 System Logs....128
4.5.3 SNMP Agent....129
4.5.4 TR-069 Client....130
4.5.5 Internet Time....131
4.5.6 Access Control....132
4.5.7 Update Software....133
4.5.8 Reboot....136

Appendix 1 Applications....137

Application 1: How to change SSID and wireless password?....137
Application 2: How to reset the modem router?....138
Method 1: WPS/RST button....138
Method 2: Restore Default Settings from User Interface....138

Appendix 2 Configure Your PC....139

Windows 8....139
Windows 7....141
MAC....143

Appendix 3 Join Your Wireless Network....144

Windows 8....144
Windows 7....145
MAC....146
iPhone/iPad....147

Appendix 4 FAQs....148

Appendix 5 VPI/VCI List....149

Appendix 6 Regulatory Compliance Information....165

Shortcut to Common Function Setup

How to set up the Internet connection?	GO
How to change your SSID (WiFi name) and password?	GO
How to change your login username and password?	GO
How to make your kids surf the Internet safely?	GO
How to set bandwidth for a specified host or client?	GO
How to restrict a host to access your wireless network?	GO
How to access a USB storage?	GO
How to expand your wireless network coverage?	GO
How to make your set-top box available?	GO
How to reset the modem router to factory defaults?	GO

© 2015 Shenzhen Tenda Technology Co., Ltd. All rights reserved.

Technical Support: support@tenda.com.cn

Telephone: (86 755) 2765 7180

Email: sales@tenda.com.cn

Website: http://www.tendacn.com

Skype: tendasz

YouTube: Tendasz1999

Chapter 1 Product Overview

Get to know your modem router overall. This part includes the following:

1.1 What It Does

1.2 Product Features

1.3 Package Contents

1.4 Front Panel

1.5 Back Panel

1.1 What It Does

The Wireless ADSL2+ Modem Router, integrated with functions of ADSL2+ modem and wireless router, is especially designed for ordinary home users. So it supports telephone cable access and Ethernet cable access. Up to 300M wireless speed (fluently play file transfers, streaming HD video, and multiplayer gaming) can match the family requests perfectly. The auto-detecting link type and PVC make you set up the modem router quickly and easily. More advanced features, like Parental Control, USB Storage Service, Bandwidth Control, Interface Grouping, IPTV, IP Tunnel and Connection Diagnostics, etc., create a diverse network world for you.

1.2 Product Features

Wireless N: Speeds up to 300 Mbps for streaming HD videos and online gaming in addition to basic Internet applications

All-in-one device combines a built-in ADSL2+ modem, wired router, wireless router and switch

Sharable USB lets you access and share files on an attached USB storage

Bandwidth Control helps prioritize media streaming and gaming applications for best entertainment experience

Parental Control keeps your kids Internet experience safe using flexible and customizable filter settings

One-touch WPS ensures a quick and secure network connection

WEP and WPA/WPA2 are supported for advanced encryptions

Compatibility: Works with all major ADSL Internet service providers (ISPs); backward compatible with 802.11b/g WiFi devices

Interchangeable LAN/WAN ports to schedule the Ethernet port to function either as a LAN or a WAN port

Interchangeable LAN/IPTV to schedule the Ethernet port to function either as a LAN or an IPTV port

Optional Ethernet and ADSL Uplinks: Access the Internet via ADSL2+ Broadband Internet Service or an interchangeable LAN/WAN RJ45 port

Multiple Internet Connection Types: PPPoE, PPPoA, IPoA, Bridge, dynamic IP and static IP

IPTV Service lets your surf the Internet while watching online TV

6000V lightning-proof design fits into lightning-intensive environment

Strong driving capability up to 6.5Km transmission distance

High speed ADSL speed up to 24Mbps downstream 1Mbps upstream

Built-in firewall prevents hacker attacks

Channel auto-select for optimum performance

FDM technology enables telephoning, faxing and surfing activities to proceed simultaneously without mutual interference

Other Advanced Features: IPv6, DDNS, virtual server, DMZ, port triggering, IP filter, MAC filter and UPnP, etc.

Tenda Green: Equipped with hardware buttons Power On/Off and WiFi On/Off. You can conveniently turn on or off power and WiFi to save energy when not in use

1.3 Package Contents

Your box should contain the following items:

- 4 Antennas Wireless N300 ADSL2+ Modem Router
- Ethernet Cable
- Phone Cables (2)
- ADSL Splitter
- Install Guide
- Power Adapter

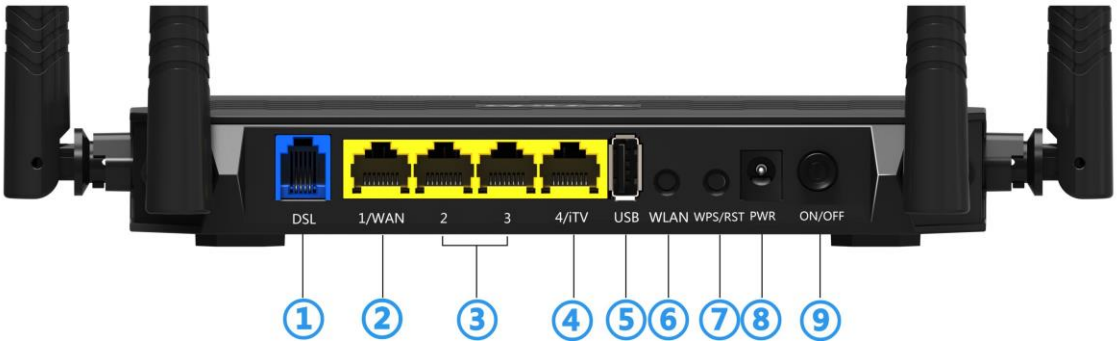
If any of the parts are incorrect, missing, or damaged, keep the carton, including the original packing materials and contact your Tenda dealer for immediate replacement.

1.4 Front Panel

The LEDs on the device are described below:

Item	Name	Status	Description
①	PWR	Solid	Power electricity is provided to the device properly.
		Off	Power is off.
②	SYS	Solid/Off	The system is malfunctioning.
		Blinking	The system works properly.
③	INTERNET	Solid	The device is connected to the Internet properly.
		Blinking	Transmitting Internet data…
		Off	The device is not connected to the Internet.
④	USB	Solid	A USB device is connected to the device.
		Blinking	A USB device is connected and is working.
		Off	No USB device is connected to the device.
⑤	WPS	Solid	A wireless device is connected to the device via WPS successfully. It will be off in 5 minutes.
		Blinking	It is waiting for a wireless device to join in.
		Off	Wireless device has finished WPS negotiation or WPS is disabled.
⑥	WLAN	Solid	The wireless is enabled.
		Blinking	The wireless is enabled and data is being transmitted via wireless.
		Off	The wireless is disabled.
⑦	4/iTV, 3, 2, 1/WAN	Solid	The port is connected.
		Blinking	The port is connected and data is being transmitted.
		Off	The port is not connected.
⑧	DSL	Solid	DSL link is connected.
		Blinking	DSL link is negotiating.
		Off	DSL link is disconnected.

1.5 Back Panel



Item	Name	Description
①	DSL	RJ11 port. Connect the telephone line from ISP to this port for DSL service connection.
②	1/WAN	LAN port or WAN port. When you access the Internet via the DSL, this port works as a LAN port which can be used to connect to a PC, switch, or a router; when you access the Internet via an Ethernet cable from your ISP directly, this port works as a WAN port. **Note**: It works as a LAN port by default.
③	2/3	LAN port. Connect your devices like computer to this port.
④	4/iTV	LAN port or IPTV port. When IPTV feature is disabled, it works as a LAN port which can be used to connect to a PC, switch or a router; when IPTV feature is enabled, it works as an IPTV port, and it can only be connected to a Set-Top Box. **Note**: IPTV feature is disabled by default.
⑤	USB	Used to connect a USB storage service for LAN sharing.
⑥	WLAN	Press this button for 3 seconds to enable/ disable WiFi.
⑦	WPS/RST	Press it for 1-3 seconds to do WPS negotiation. (Make sure WPS is enabled on Wireless > Security screen ahead.) Press it for 8 seconds to restore all configurations to factory defaults.
⑧	PWR	Connect the modem router to power supply via this port.
⑨	ON/OFF	Turn ON or OFF the modem router.

Chapter 2 Hardware Installation

Before you start to cable the modem router, you should figure out your Internet access type. Cable you modem router correctly, and make sure it works well. It supports two types of access, **DSL access** and **Ethernet access**. Choose your access type and cable your device and modem router.

This part includes the following:

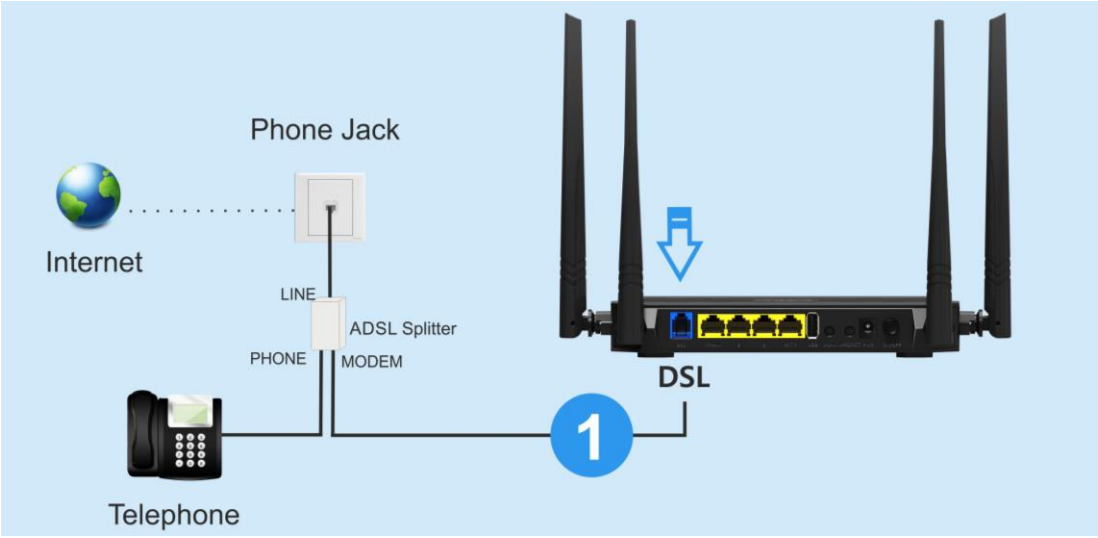
2.1 DSL Access

2.2 Ethernet Access

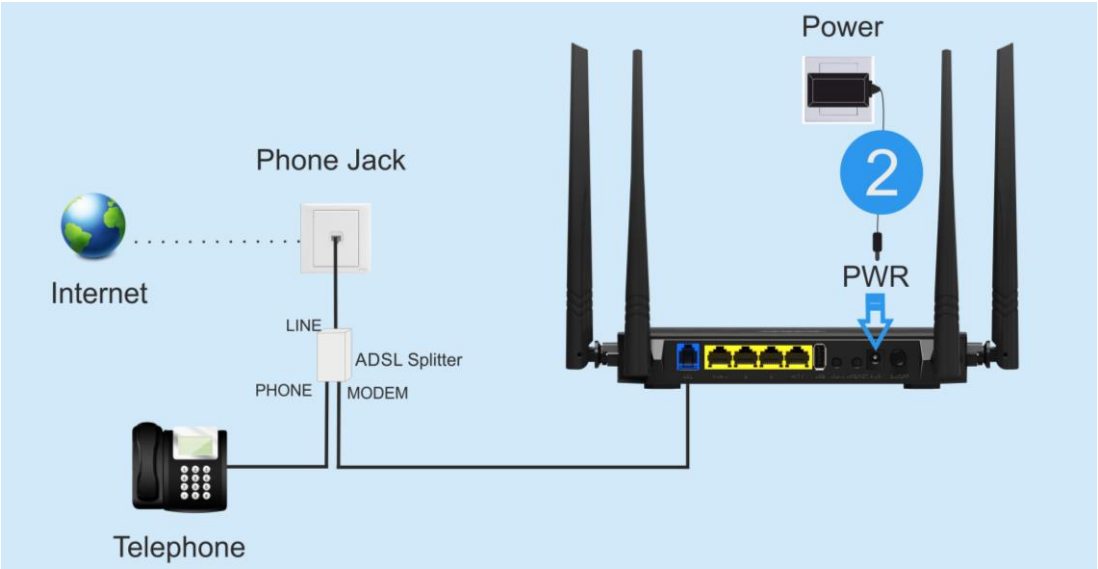
2.1 DSL Access

▪ **DSL access** cabling is detailed below. Cable the modem router and your computer following the steps ① →②→③.

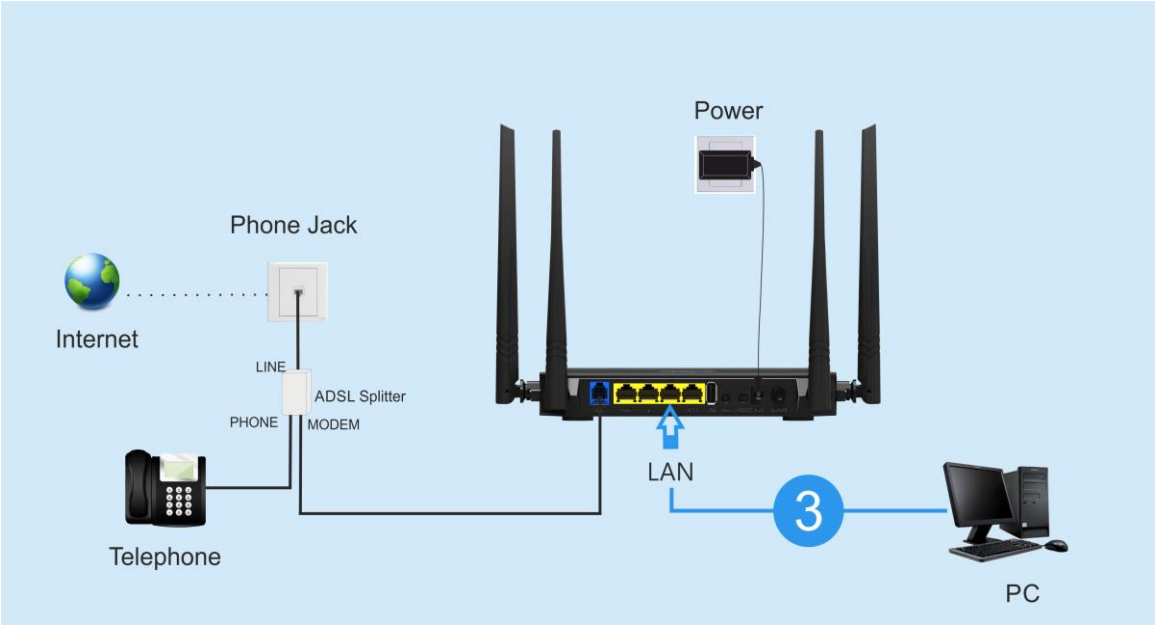
① Insert the telephone line provided by your ISP into the DSL port of the modem router. (If you are using telephone service and Internet service simultaneously, cable the ADSL spillter as the diagram below shows.)



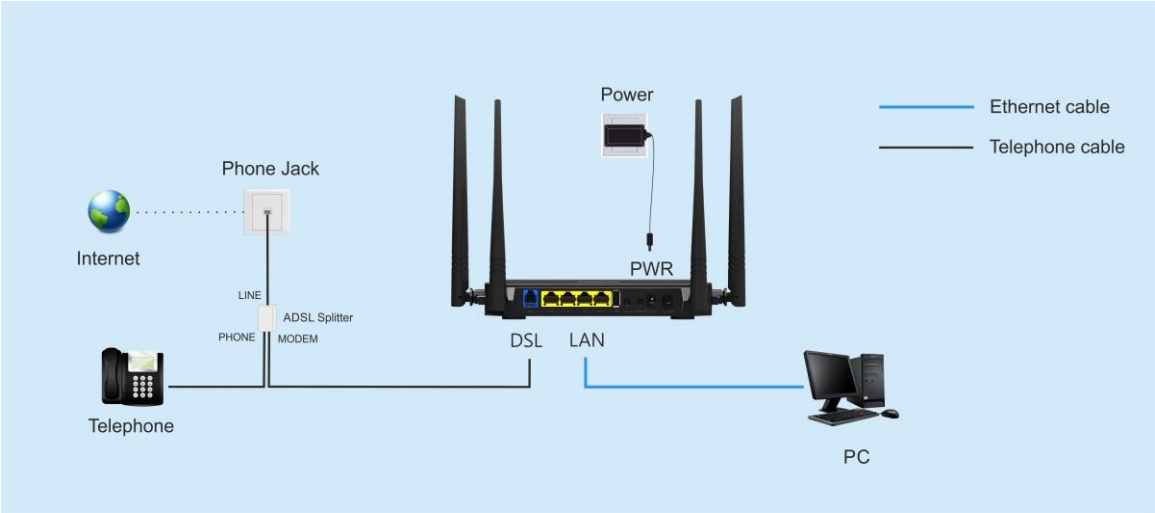
② Connect the modem router to the power supply with the attached power adapter.



③ Connect your computer to the LAN port of the modem router.



The overall diagram of DSL Access is shown below:



TIP

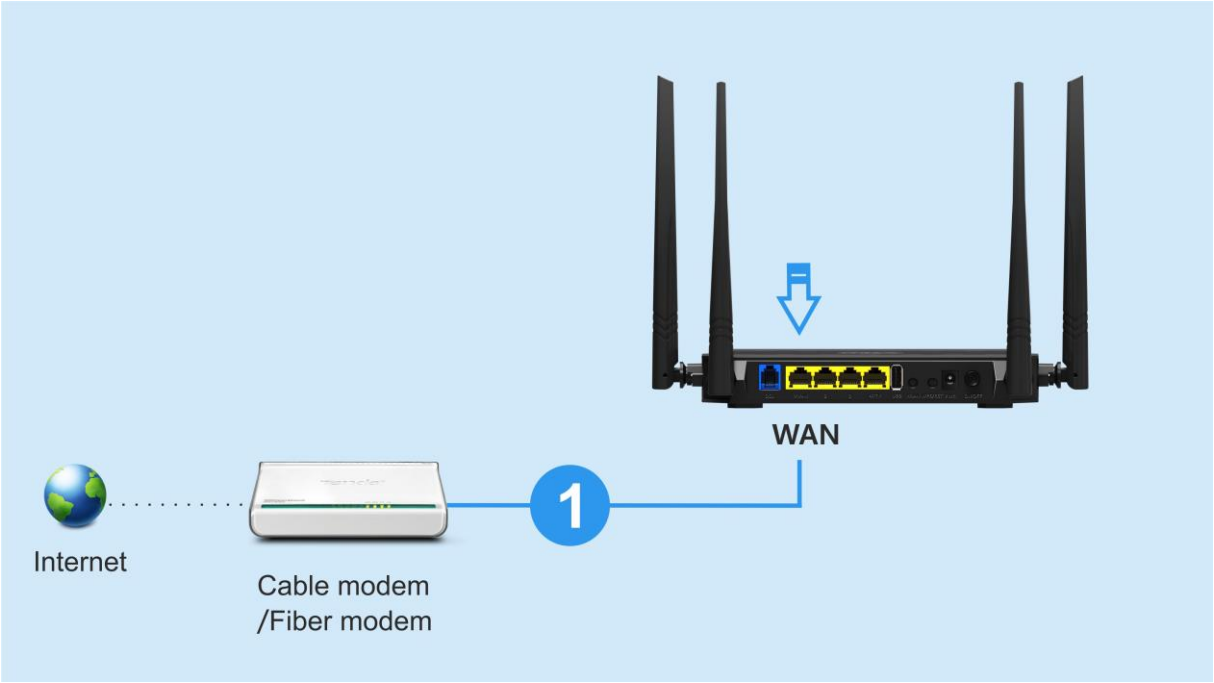
1. Before connecting, make sure the Internet service is available.
2. ADSL splitter is used to make you active in phone service and Internet service simultaneously. If you don't need the telephone service, just connect the telephone line from your ISP to the DSL port.
3. Make sure that the DSL LED indicator is on and then configure the modem router.
4. Please use the included power adapter. Use of a power adapter with different voltage rating may damage the device.

2.2 Ethernet Access

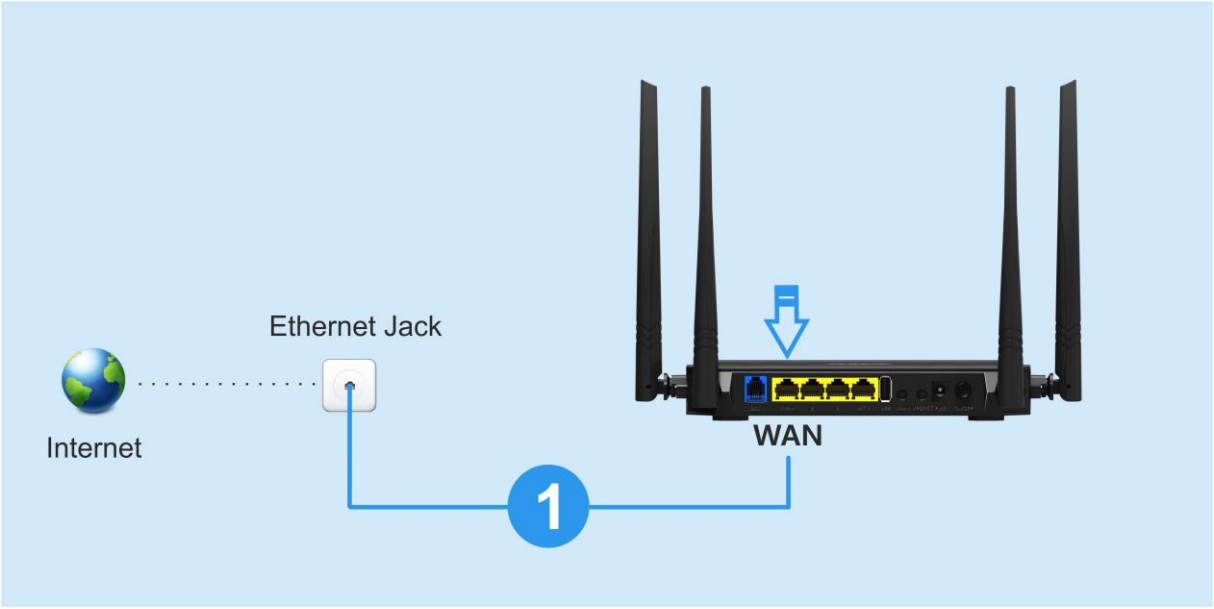
▪ **Ethernet access** cabling is detailed below. Cable the modem router and your computer following the steps ①→②→③.

Note that you may get to the Internet via a modem or an Ethernet cable directly, choose your access type correctly and follow the diagram.

a1. If you get to the Internet via a **modem** (cable modem or fiber modem), follow this one.

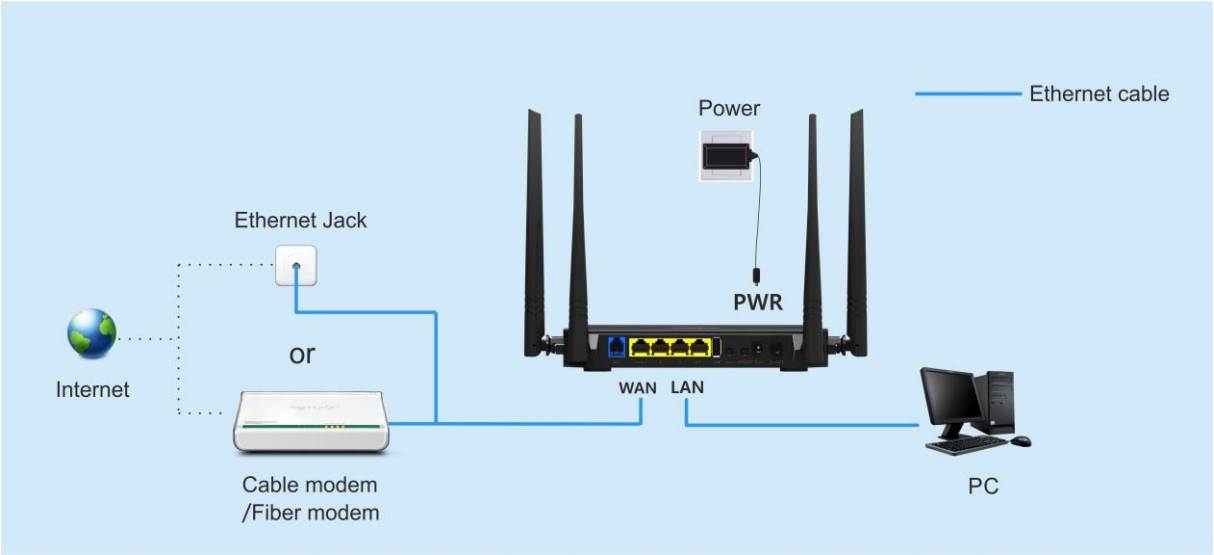


b1. If you get to the Internet via **Ethernet cable** directly, follow this one.



Steps 2 and 3 are same with that of DSL access. Click here to check.

The overall diagram of Ethernet Access is shown below:



TIP

1. Before connecting, make sure the Internet service is available.
2. Disconnect the modem router from WAN or DSL connection, and unplug it from the power when it is thunderstorm.

Chapter 3 Internet Setup

Internet setups are detailed in this part, which include connection types, link types and wireless security setup, etc.

This part includes the following:

3.1 Log in to UI

3.2 Set up Internet

3.3 Quick Wireless Security Setup

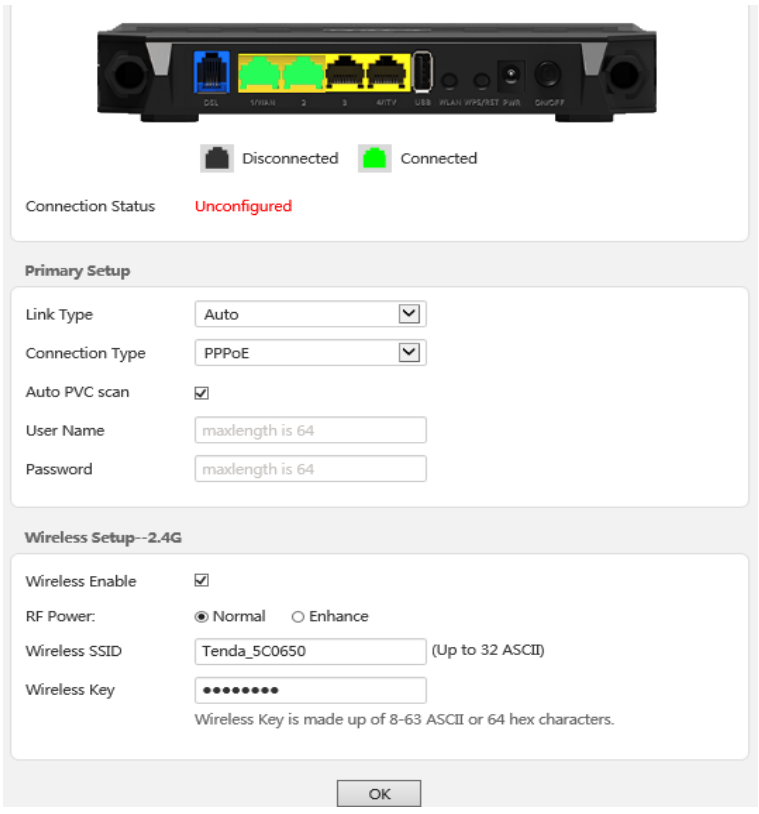
3.1 Log in to UI (User Interface)

To configure the parameters of the modem router, you should log in to its UI (User Interface) first.

① Set your PC to Obtain an IP address automatically. For more information, see Appendix 2 Configure Your PC.

② Launch a web browser and enter **192.168.1.1** to display the login window.

③ Enter **admin** in both the login User Name and Password fields if you access the router for the first time and then click **Login** to enter the home page.



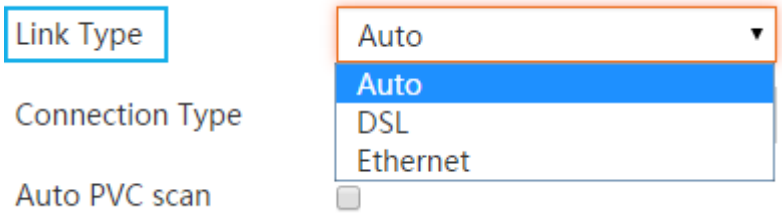
TIP

If you forgot your login user name and password, press the WPS/RST button on the device for about 8 seconds to reset the router, and then re-log in with the default user name and password “admin”.

3.2 Set up Internet

The device supports auto-detecting link type and PVC, which can help you configure the device easily and quickly. If you do want to configure the details, take below for references.

About Link Type



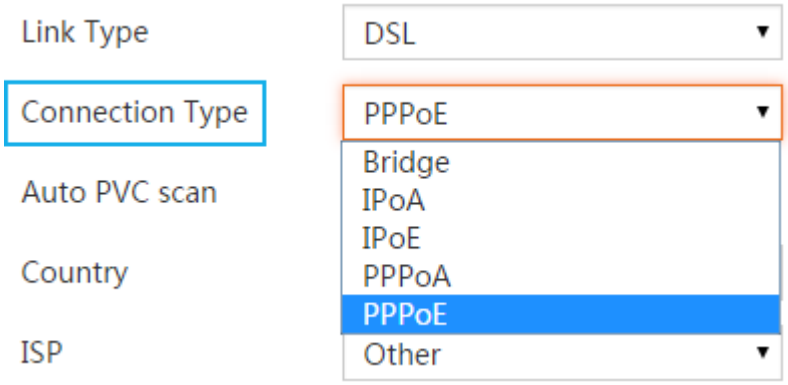
Link type includes three options: **Auto, DSL and Ethernet**.

Auto is recommended to you if you cannot figure out which type your Internet access is.

DSL is for a telephone line access, which means you access Internet service with a telephone line.

Ethernet is for an Ethernet cable access. If you are using this modem router with cable modem or fiber modem; or you get an Ethernet cable access directly, select Ethernet.

About Connection Type



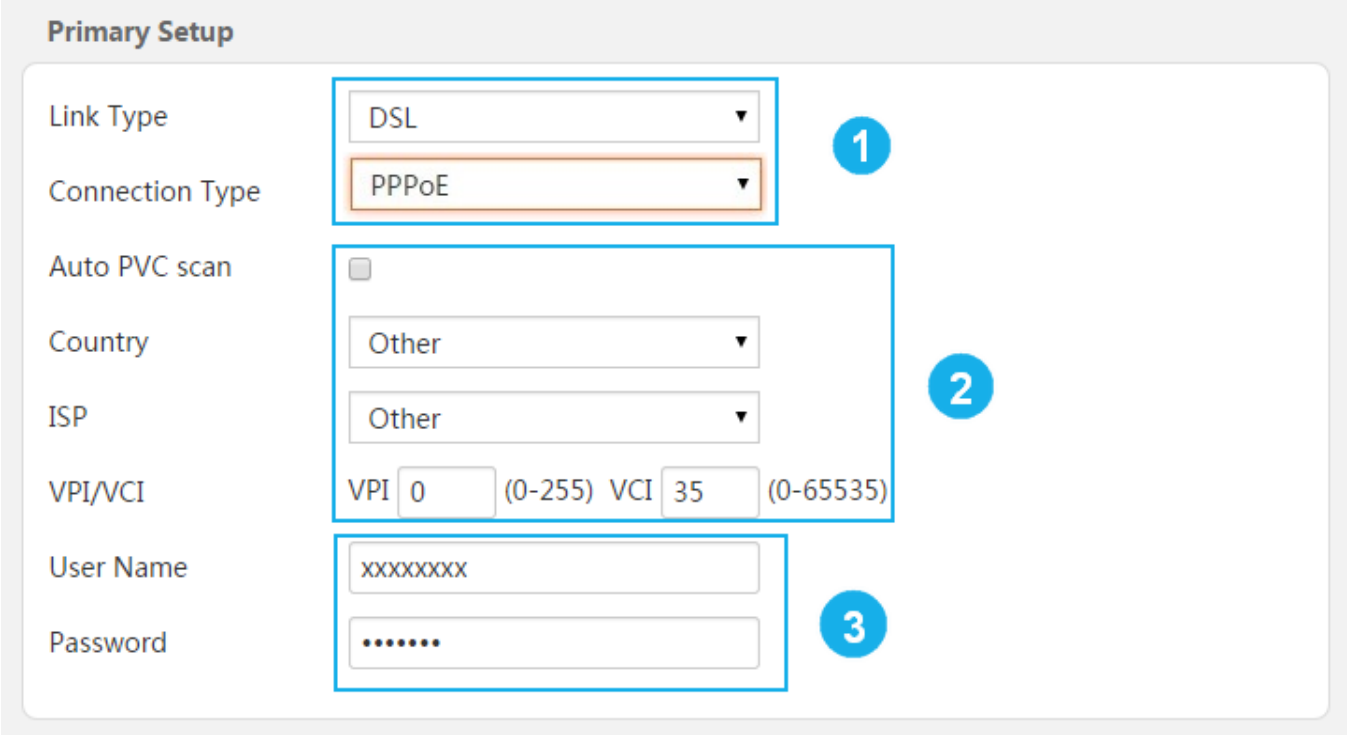
The device supports the following connection types, IPoE (Dynamic IP or Static IP), PPPoE, IPoA, PPPoA and Bridge.

You can set up Internet quickly on the Home page or click Advanced icon for more info about advanced settings.

Internet Setup Instruction

For DSL access

- **PPPoE**



① Select **Auto** or **DSL** link type and select **PPPoE** connection type. (Note that Auto mode only supports two connection types: PPPoE and IPoE.)

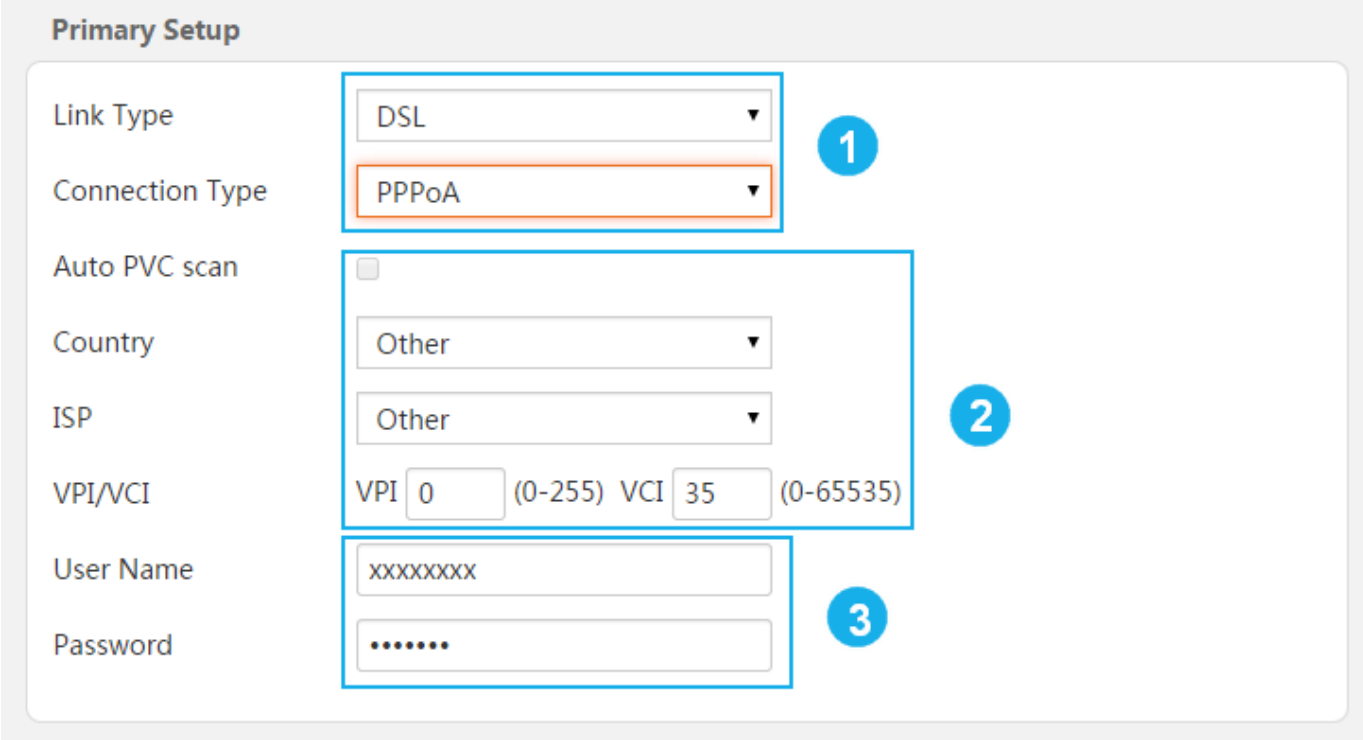
② Check **Auto PVC scan**. If the scan failed, uncheck this option and configure the PVC and country settings manually. Click here to check PVC value or consult your ISP if you cannot locate this info.

③ Type the user name and password of PPPoE provided by your ISP.

④ Finish the wireless setup. (Recommended)

⑤ Click **OK**.

- **PPPoA**



① Select **Auto** or **DSL** link type and select **PPPoA** connection type. (Note that Auto mode only supports two connection types: PPPoE and IPoE.)

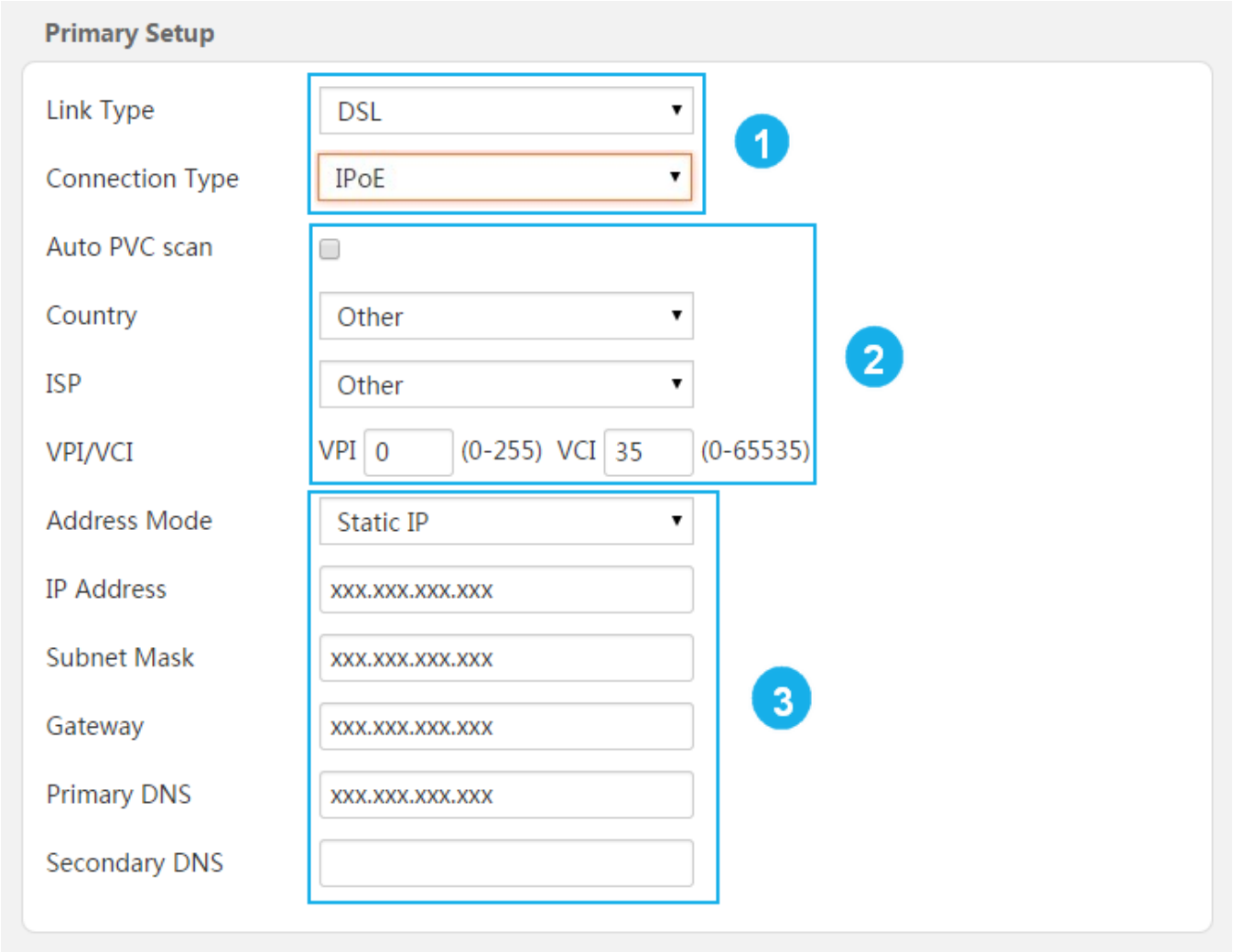
② Configure the PVC, ISP and country settings manually. Click here to check PVC value or consult your ISP if you cannot locate this info. (Note that Auto PVC scan is not available for PPPoA.)

③ Type the user name and password of PPPoA provided by your ISP.

④ Finish the wireless setup. (Recommended)

⑤ Click **OK**.

- **IPoE**



① Select **Auto** or **DSL** link type and select **IPoE** connection type.

② Check **Auto PVC scan**. If the scan failed, uncheck this option and configure the PVC and country settings manually. Click here to check PVC value or consult your ISP if you cannot locate this info.

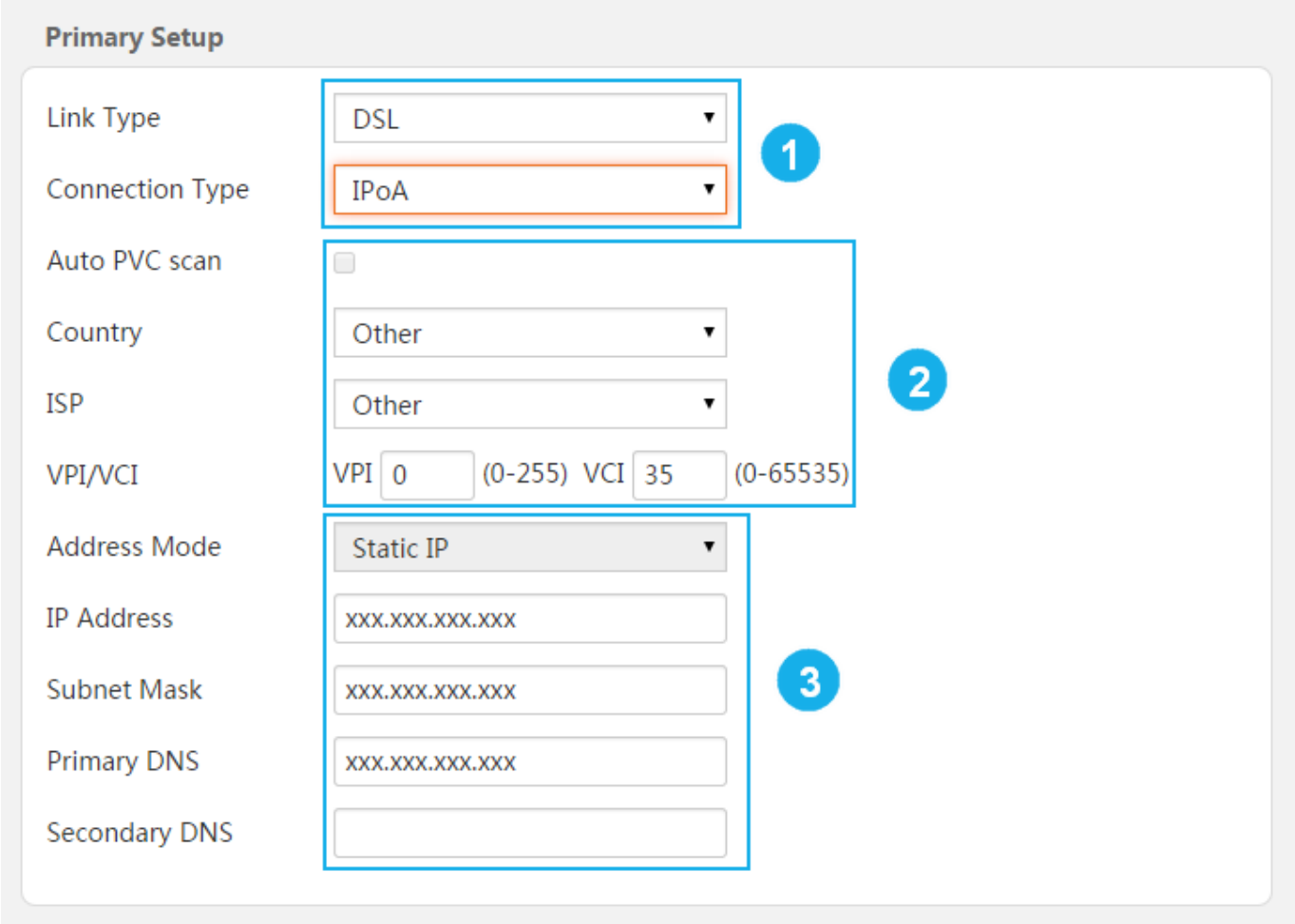
③ Select your address mode (**Dynamic IP** or **Static IP**). This is depending on your ISP.

- **Dynamic IP** mode requires nothing.
- **Static IP** requires a group of IP info provided by your ISP. Type them in the corresponding field.

④ Finish the wireless setup. (Recommended)

⑤ Click **OK**.

- **IPoA**



① Select **Auto** or **DSL** link type and select **IPoA** connection type.

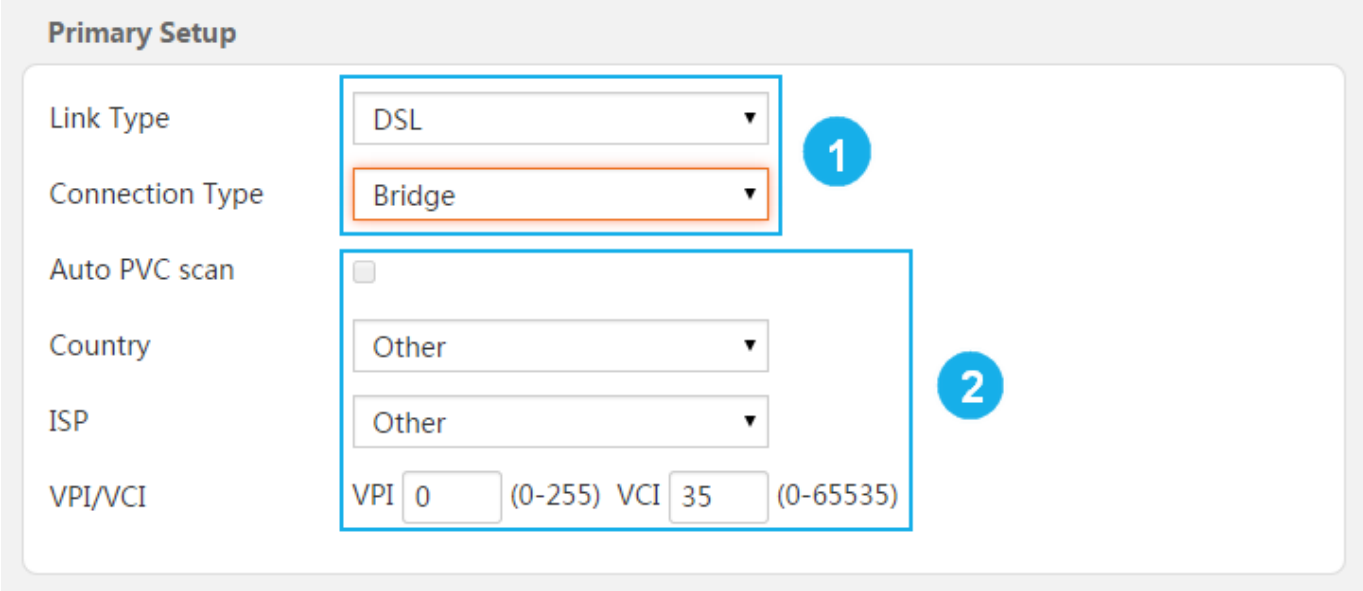
② Configure the PVC, ISP and country settings manually. Click here to check PVC value or consult your ISP if you cannot locate this info. (Note that Auto PVC scan is not available for IPoA.)

③ Select your address mode **Static IP**. And type the IP info provided by your ISP in the corresponding field.

④ Finish the wireless setup. (Recommended)

⑤ Click **OK**.

- **Bridge**



① Select **Auto** or **DSL** link type and select **Bridge** connection type.

② Configure the PVC, ISP and country settings manually. Click here to check PVC value or consult your ISP if you cannot locate this info. (Note that Auto PVC scan is not available for Bridge.)

③ Finish the wireless setup. (Recommended)

④ Click **OK**.

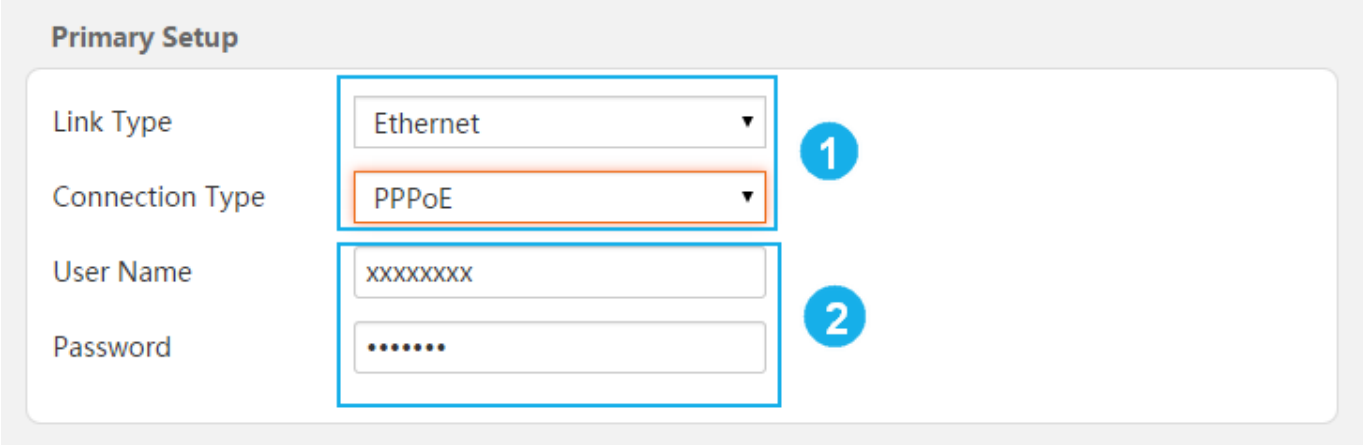
When Bridge mode in DSL access is enabled, dial up from the local PC with the account provided by your ISP for Internet service.

NOTE

If your country and/or your ISP are not covered on the Home page, select "Other" from the country list and configure the VPI and VCI value manually. If you cannot locate this information, refer to Appendix 5 VPI/VCI List or ask your ISP to provide it. For more information, see To Set up the ATM interface and To Set up WAN Service for ATM Interface.

For Ethernet access

- **PPPoE**



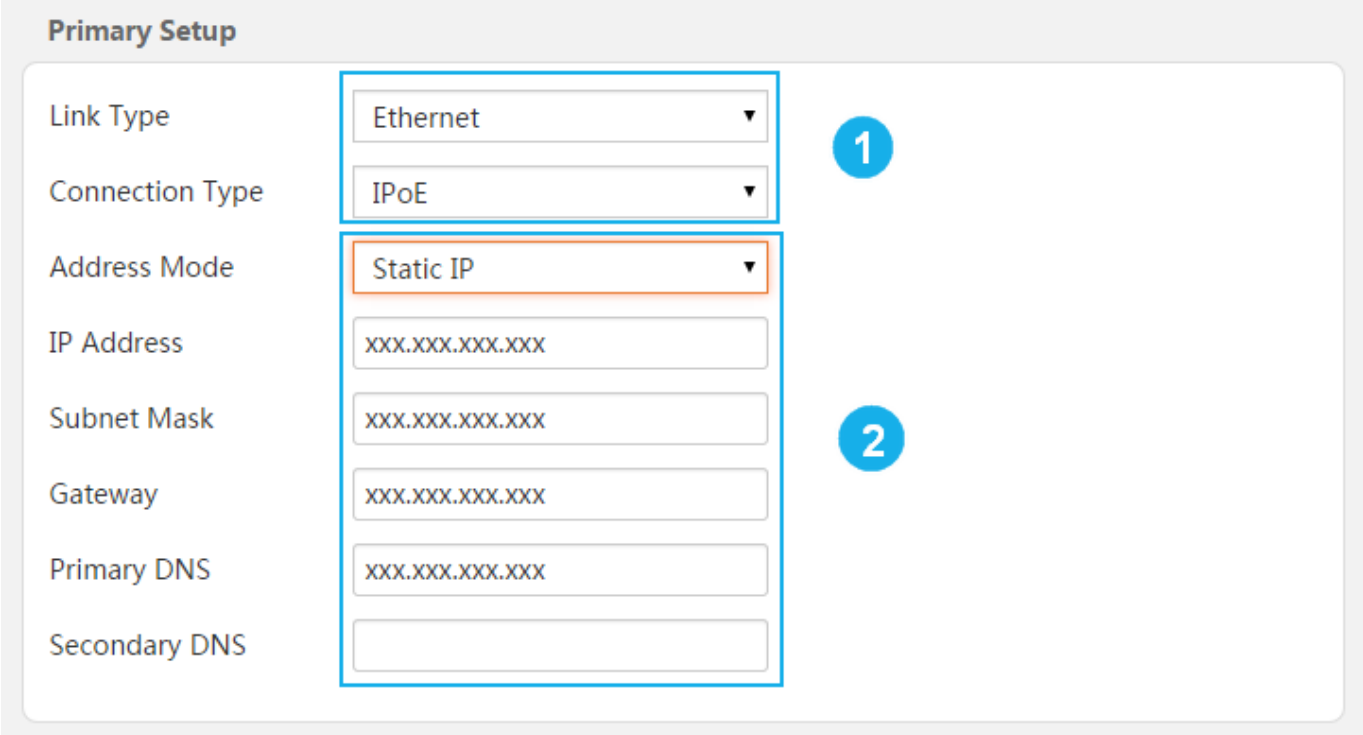
① Select **Auto** or **Ethernet** link type and select **PPPoE** connection type.

② Type the user name and password of PPPoE provided by your ISP.

③ Finish the wireless setup. (Recommended)

④ Click **OK**.

- **IPoE**



① Select **Auto** or **Ethernet** link type and select **IPoE** connection type.

② Select your address mode (**Dynamic IP** or **Static IP**). This is depending on your ISP.

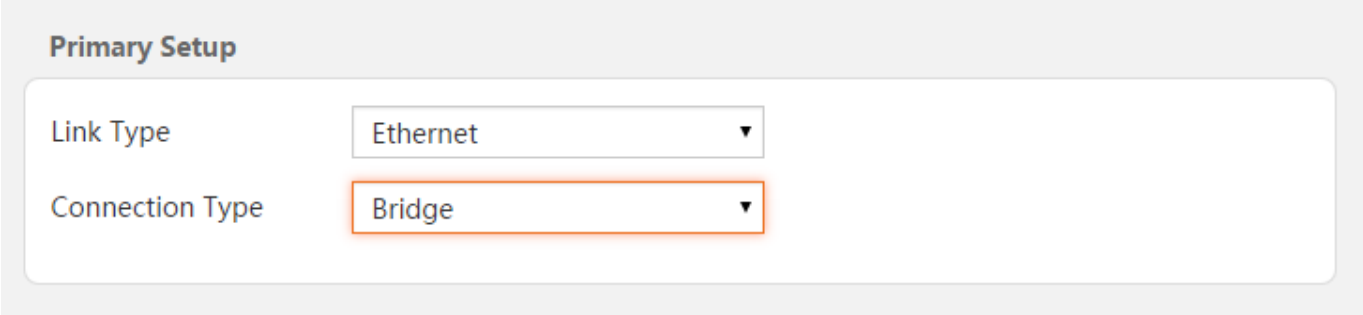
- **Dynamic IP** mode requires nothing.

- **Static IP** requires a group of IP info provided by your ISP. Type them in the corresponding field.

③ Finish the wireless setup. (Recommended)

④ Click **OK**.

- **Bridge**



① Link Type: Select **Auto** or **Ethernet**.

② Select **Bridge** connection type.

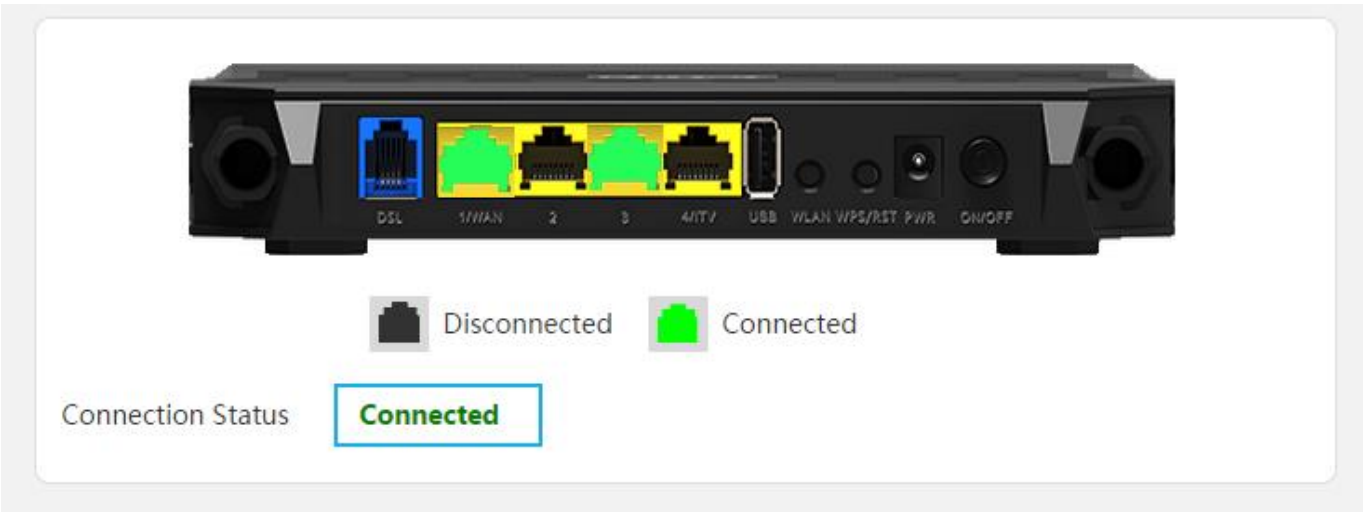
③ Finish the wireless setup. (Recommended)

④ Click **OK**.

When Bridge mode in Ethernet access is enabled, dial up from the local PC with the account provided by your ISP for Internet service.

Test Internet Connectivity

After the device is correctly set, it may get to the Internet. (Connection Status: **Connected**)

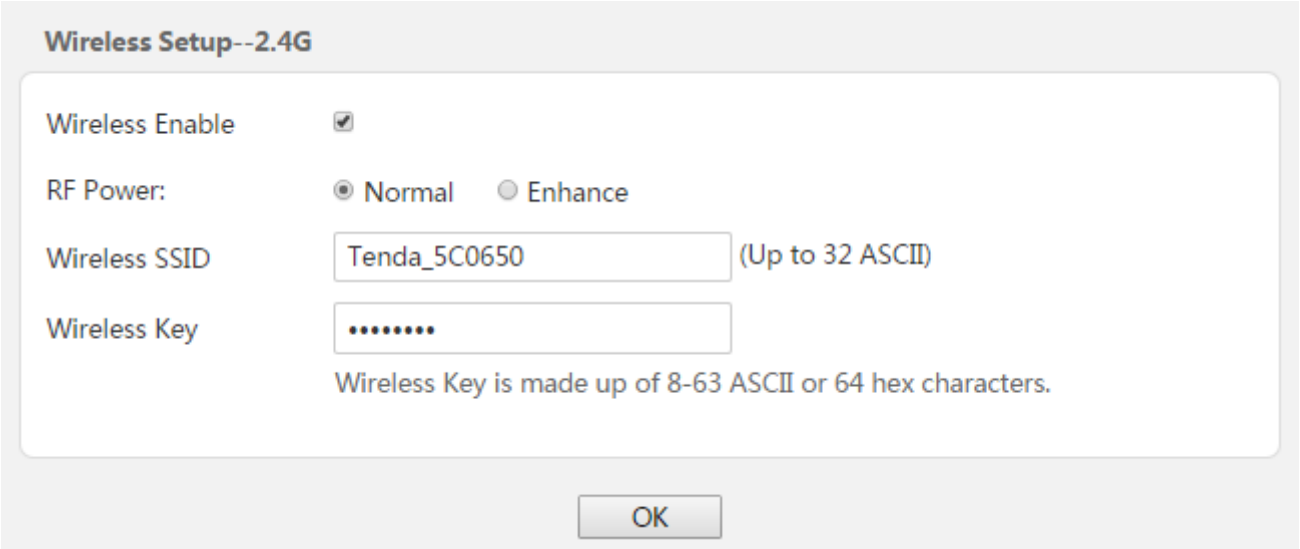


You can launch a web browser and search www.tendacn.com. If the webpage displays, you are able to enjoy the Internet service.

3.3 Quick Wireless Security Setup

On Home Page, you can set up the basic wireless parameters, like wireless SSID, wireless key and RF Power (namely signal strength). Also, you can disable or enable wireless feature here.

After you have finished settings, click OK to save and apply them.



Wireless Enable: Check it to enable wireless feature.

RF Power: Namely signal strength. It includes **Normal** and **Enhance** options. Enhance means stronger signal.

Wireless SSID: It is the name of your WiFi. Set it as you like.

Wireless Key: It is the key of your WiFi. The WiFi is unencrypted by default, but there is a preset key in the wireless key field. The preset key will work after you click OK.

NOTE

1. If you change a new wireless key, the current WiFi connection will be stopped. You may try to connect the WiFi with the new wireless key.
2. To join your wireless network, see Appendix 3 Join Your Wireless Network.

Chapter 4 Advanced Settings

This chapter describes the advanced features of your modem router. The information is for users with a solid understanding of networking concepts who want to configure the router for unique situations.

This part includes the following:

4.1 Device Info

4.2 Advanced Setup

4.3 Wireless

4.4 Diagnostics

4.5 Management

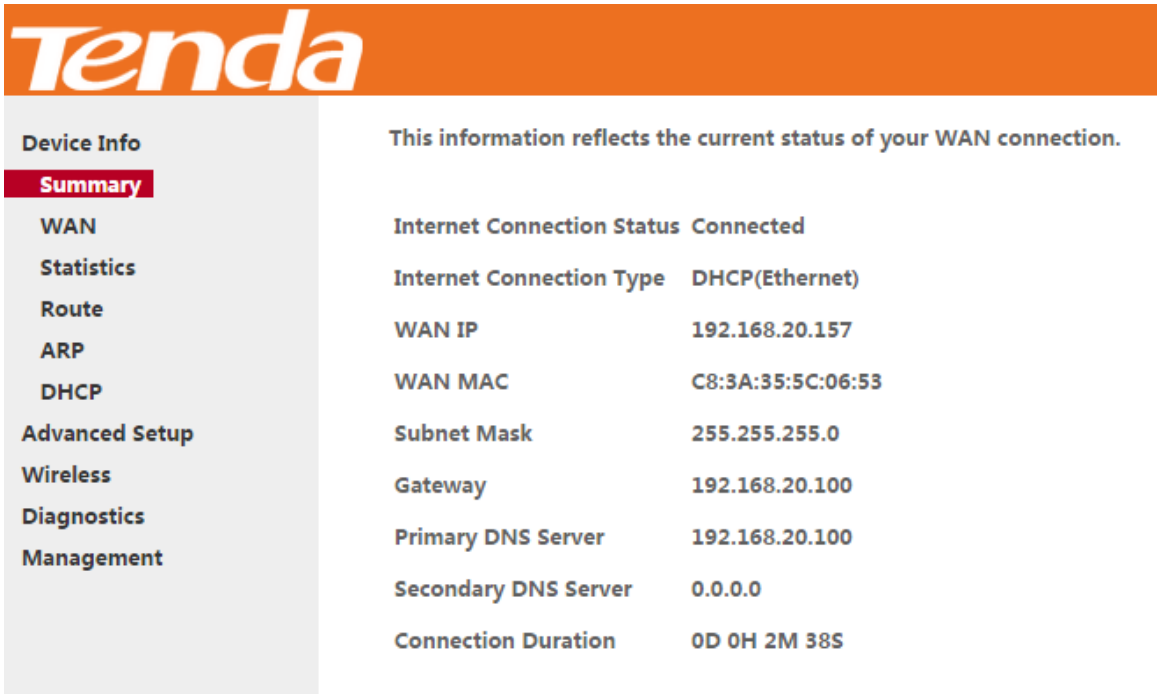
4.1 Device Info

This section includes the following information:

- *Summary*
- *WAN*
- *Statistics*
- *Route*
- *ARP*
- *DHCP*

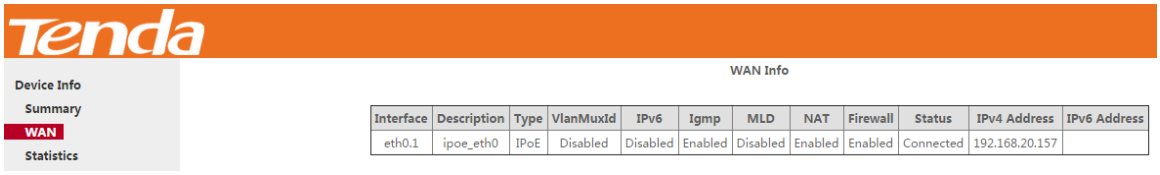
Summary

Here you can view system information and current status of your WAN connection as seen in the screenshot.



WAN

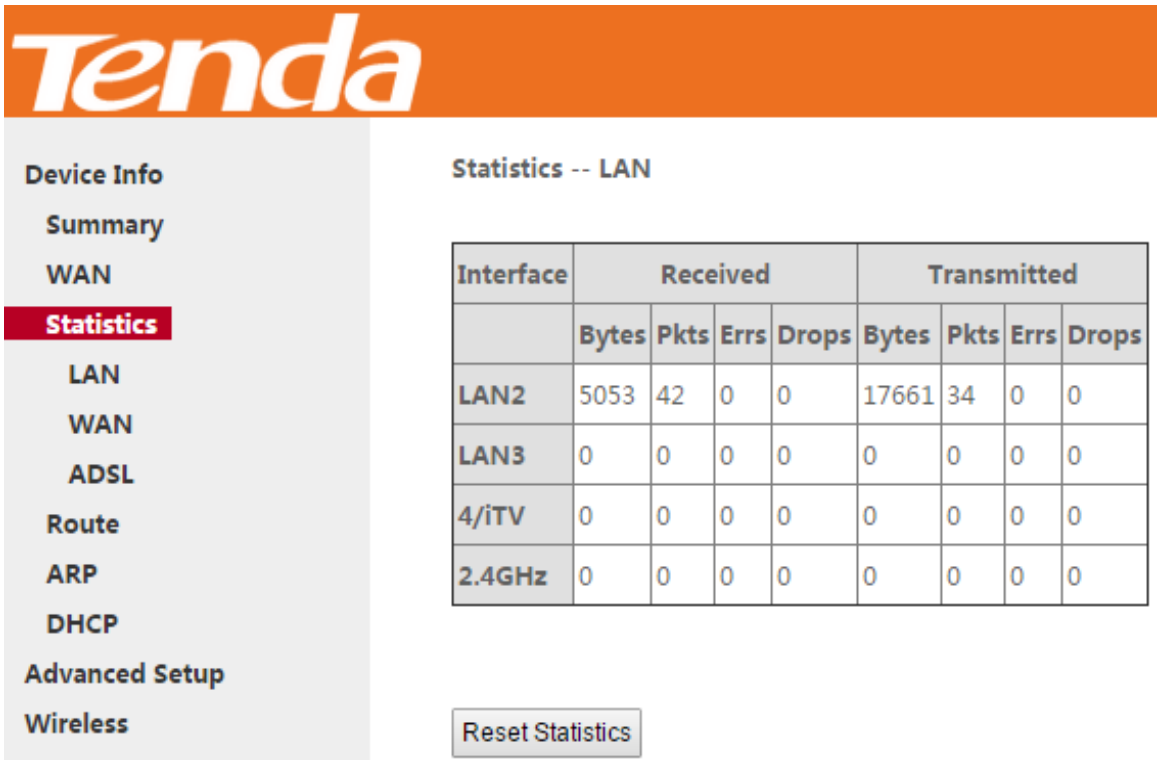
Here you can view the WAN Information including Interface, Description, Type, IGMP, NAT, Firewall, Status, IPv4 Address and VLAN ID as seen in the screenshot.



Statistics

Here you can view the packets received and transmitted on LAN/WAN ports.

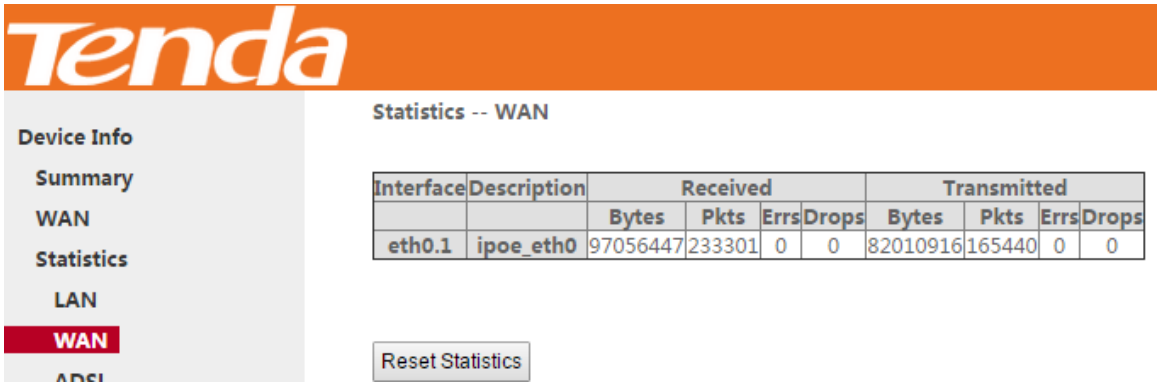
Statistics--LAN: Displays the packets received and transmitted on the LAN ports as seen in the screenshot below.



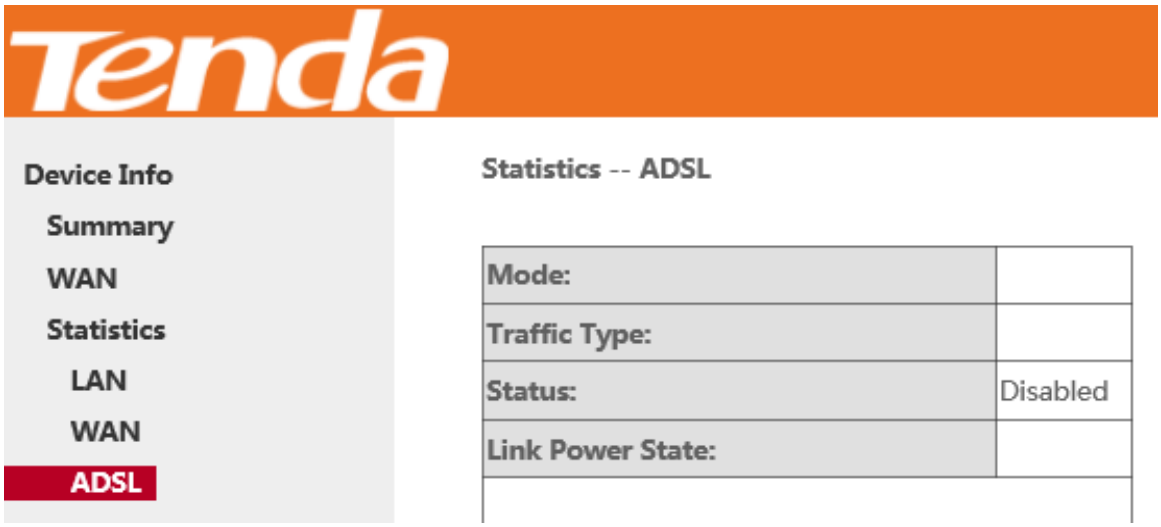
TIP

2.4GHz interface represents data transmitted and received via wireless.

Statistics--WAN: Displays the packets received and transmitted on the WAN ports as seen in the screenshot below.

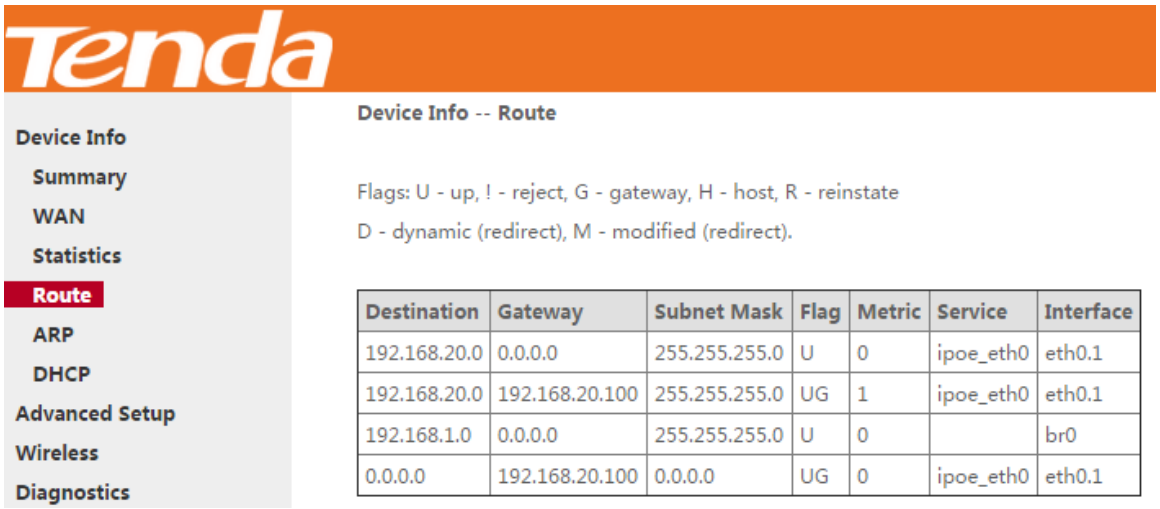


Statistics-ADSL: Displays the DSL port status e.g., packets received and transmitted on the DSL port.



Route

Here you can view the route table as seen in the screenshot:

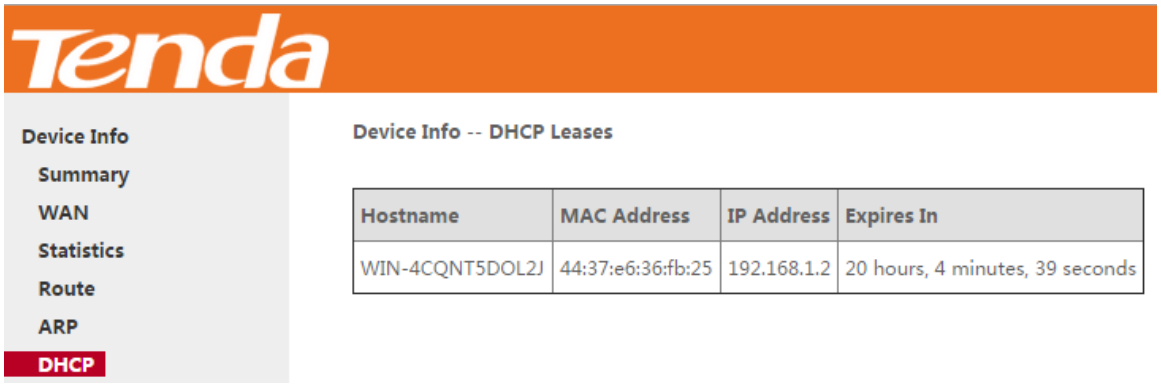


ARP

Here you can view the IP and MAC addresses of the PCs that attach to the device either via a wired or wireless connection as seen in the screenshot:

DHCP

Here you can view the DHCP leases, including IP and MAC addresses of the PCs, hostnames and remaining lease time as seen in the screenshot. Note that if the DHCP server is disabled, this info will be hidden.



4.2 Advanced Setup

This section explains the following information:

- *Layer2 Interface*
- *WAN Service*
- *LAN*
- *NAT*
- *Routing*
- *DSL*
- *DNS*
- *Bandwidth Control*
- *Security*
- *Parental Control*
- *IPTV*
- *Storage Service*
- *Interface Grouping*
- *Certificate*
- *Multicast*
- *IP Tunnel*

4.2.1 Layer2 Interface

Click **Advanced Setup > Layer2 Interface** to enter the Layer2 Interface screen.

This router provides two kinds of Layer2 Interface:

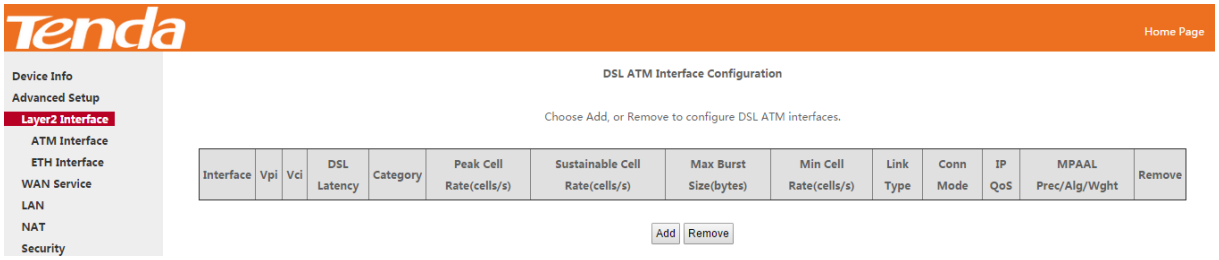
- ATM Interface for ADSL broadband Internet service

- ETH Interface for connecting to the Internet via an Ethernet cable.

By default, system applies the ATM Interface (ADSL uplink).

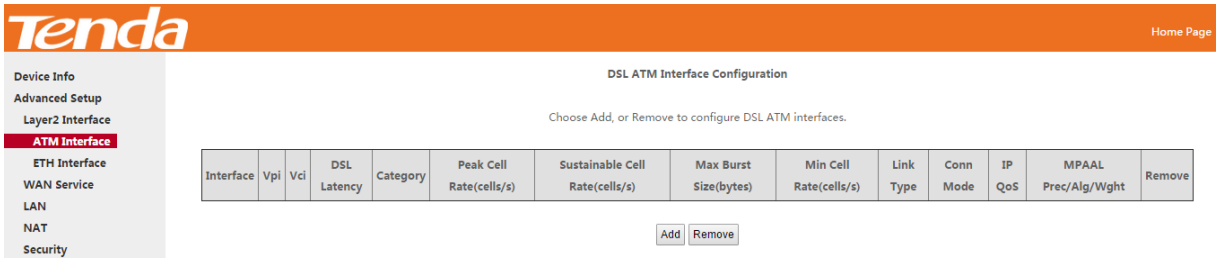
If you directly connect to the ADSL line via a phone cable, first refer to **To Set up the ATM interface** and then skip to **To Set up WAN Service for ATM Interface**.

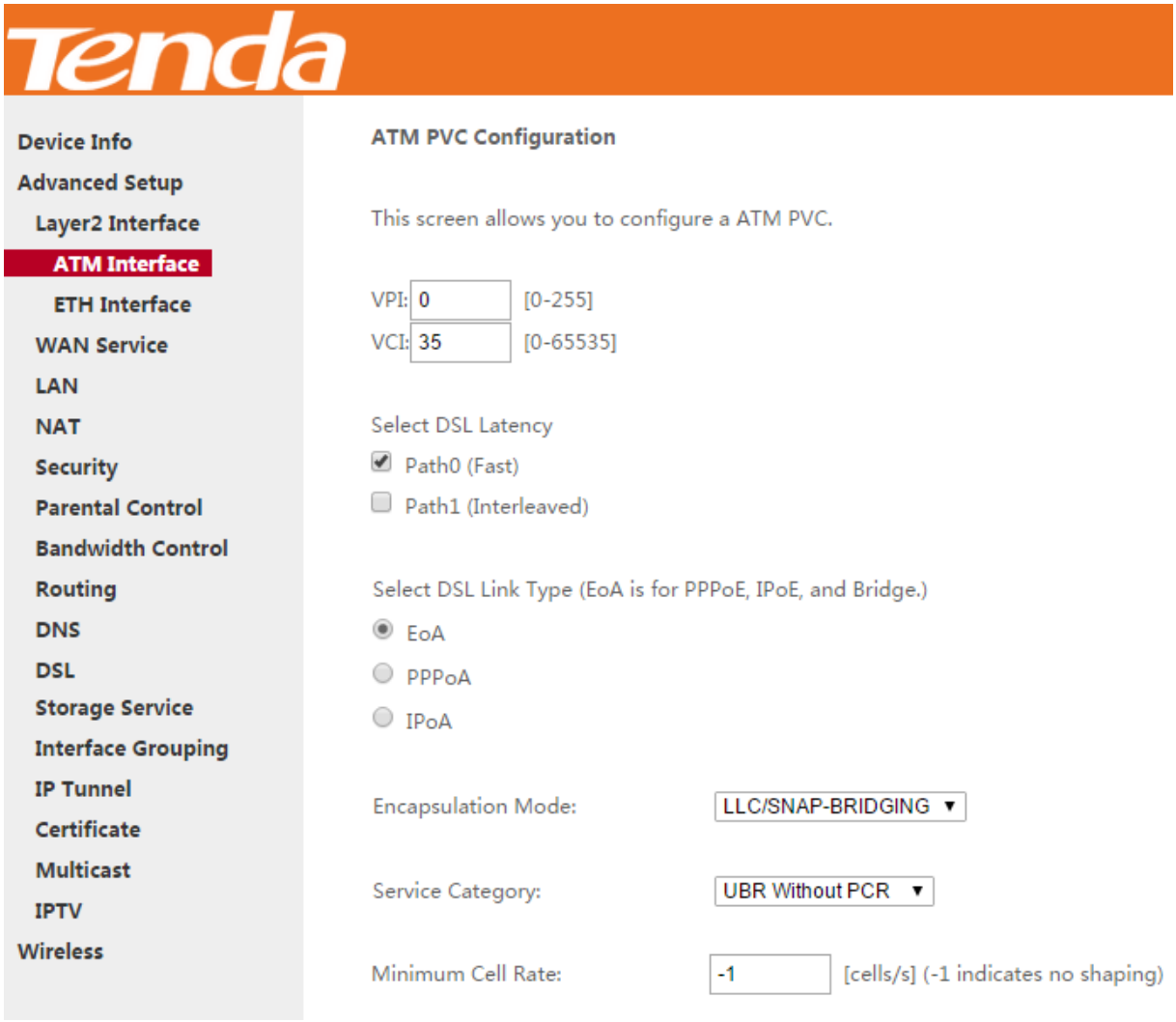
Or if you connect to the Internet via a fiber/cable modem using an Ethernet cable, first refer to **To Set up the ETH interface** and then skip to **To Set up WAN Service for ETH Interface**.



To Set Up the ATM Interface

Select **ATM Interface** and click **Add**.





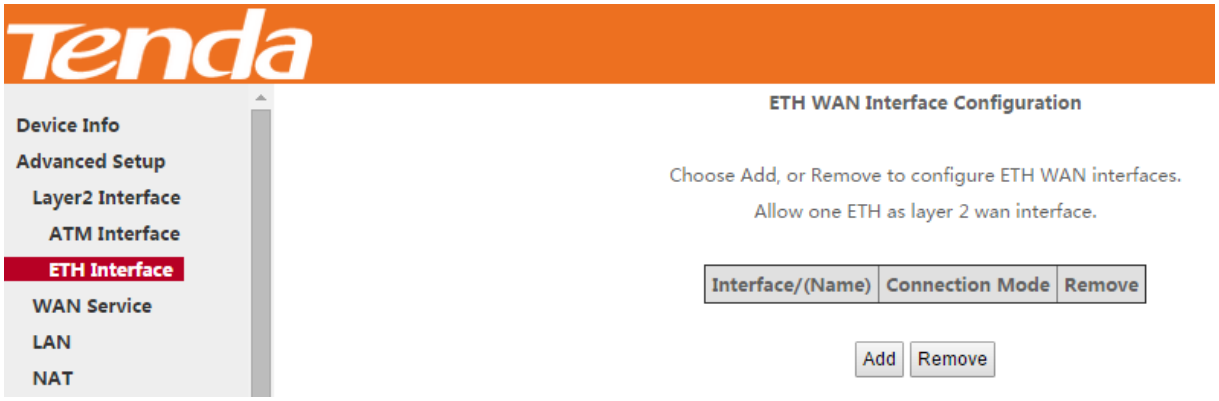
Enter the VPI and VCI values, select a DSL Link Type (Internet connection type): EoA (EoA is for PPPoE, IPoE, and Bridge.), PPPoA or IPoA. Leave other options unchanged from factory defaults and click Apply/Save and then refer to **To Set up WAN Service for ATM Interface** to configure the WAN service for Internet access.

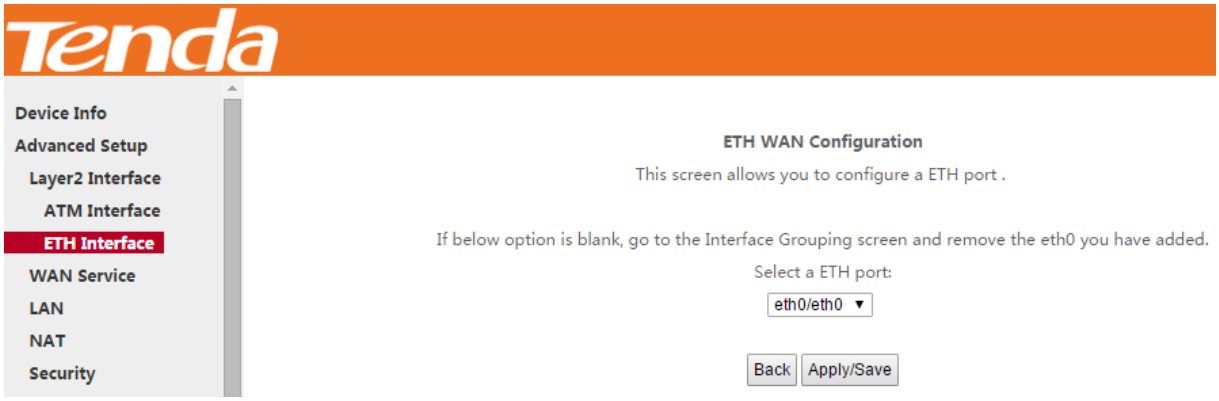
TIP

If you are unsure about the VPI/VCI parameters, see **Appendix 5 VPI/VCI List**. Or if your ISP and the VPI/VCI information is not covered there, ask your ISP to provide it.

To Set Up the ETH Interface

Select **ETH Interface** and click **Add**.





Eth0 is 1/WAN port on the back of the device. It is to function as a WAN port here. After you finish your settings, click Apply/Save and then refer to **To Set up WAN Service for ETH Interface** to configure the WAN service for Internet access.

4.2.2 WAN Service

This router provides two WAN services:

- WAN Service for ATM Interface (ADSL uplink)

- WAN Service for ETH Interface (Ethernet uplink)

To Set up WAN Service for ATM Interface

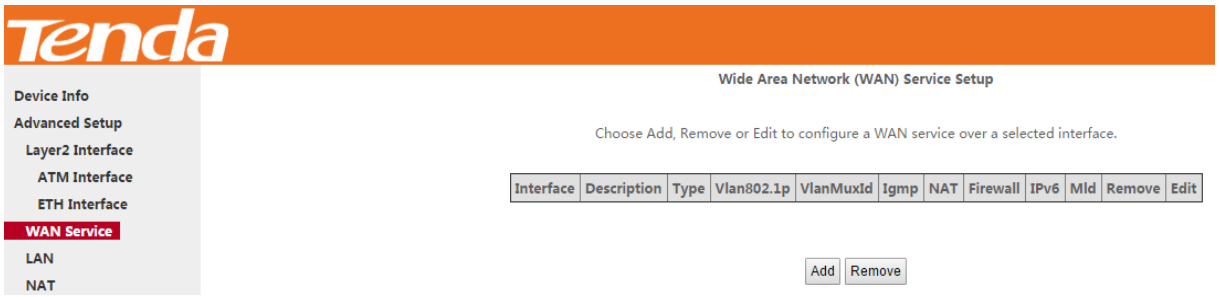
- **EoA (PPPoE, IPoE and Bridge)**

If you configured the **ATM Interface** (ADSL uplink) and select **EoA** as the DSL link type, follow below steps to configure the WAN service:

PPPoE

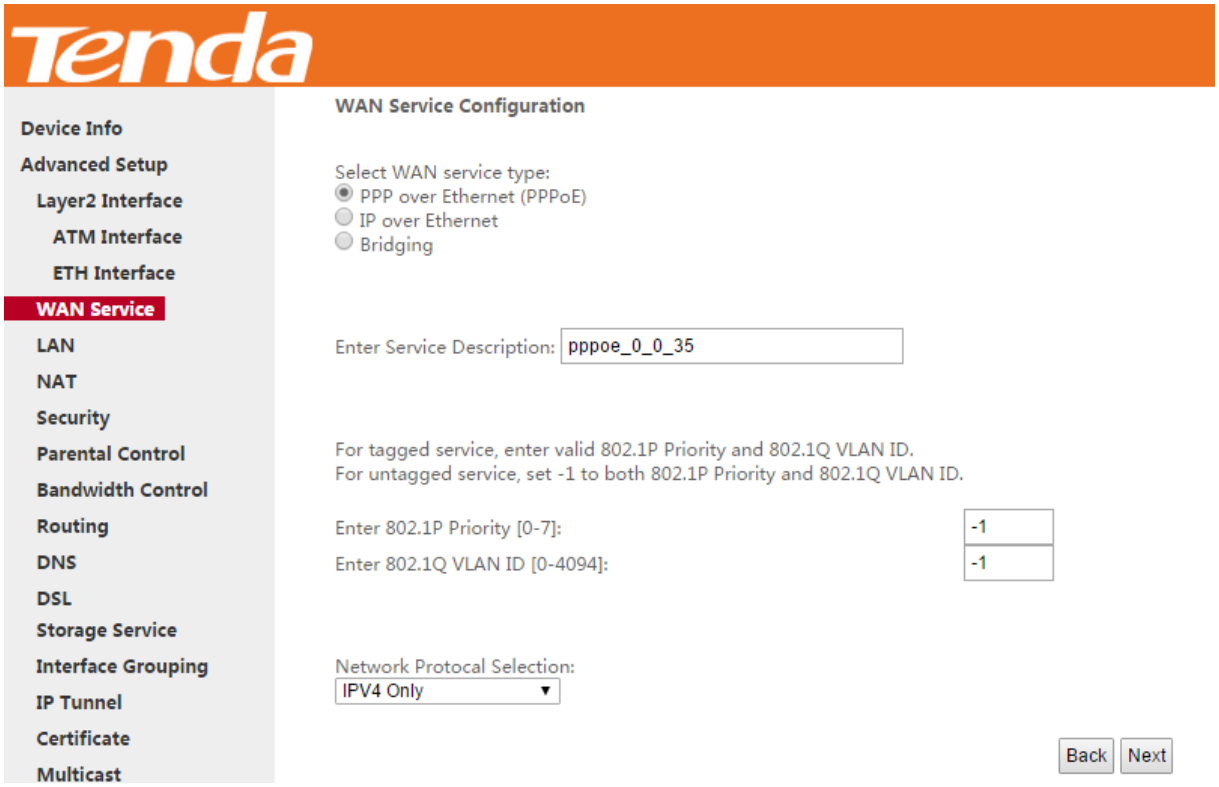
IPv4 Only

Step 1: Click **Advanced Setup > WAN Service** and then click the **Add** button.

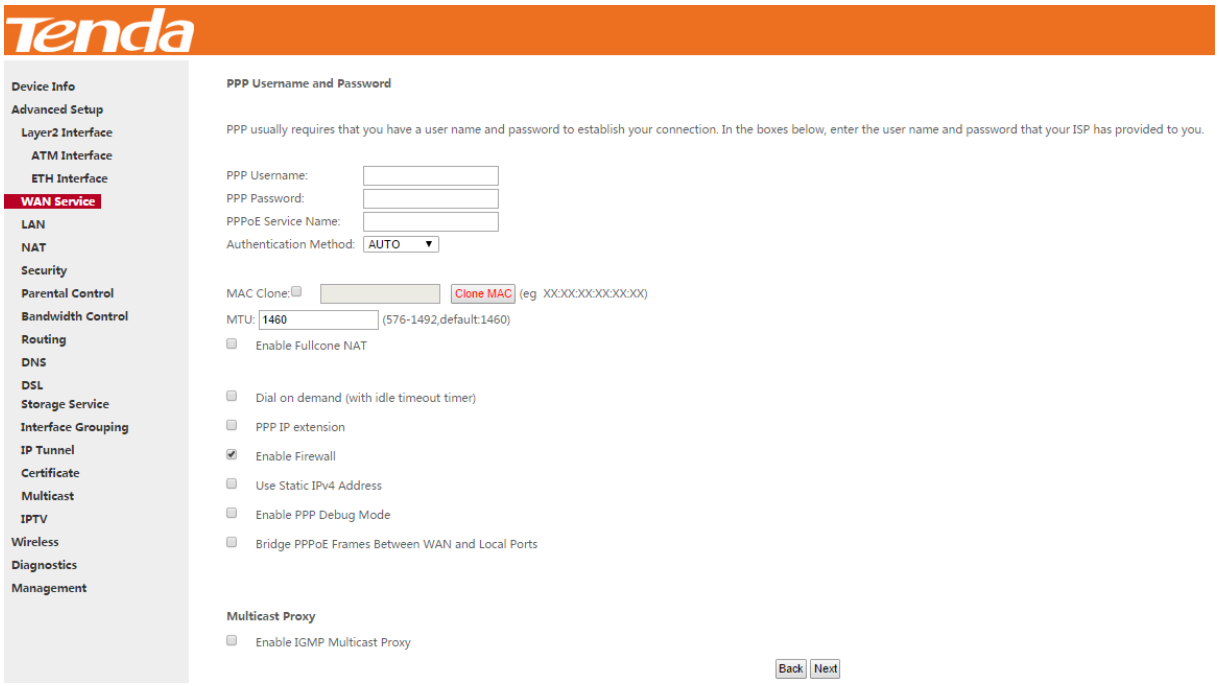


Step 2: Select the ATM interface you added just now from the pull-down menu in the figure below. Click **Next**.

Step 3: Select **PPP over Ethernet (PPPoE)**. Edit the **Enter Service Description** field which is optional. Suggest you keep the default. Select a network protocol: **IPv4 Only**. Click **Next.**



Step 4: Finish PPP Username and Password and other settings on the figure below. Click **Next**.



PPP Username/Password: For logging in to your ISP. If you cannot locate this information, ask your ISP to provide it.

PPPoE Service Name: Provided by your ISP. Only enter it if instructed by your ISP.

Authentication Method: Used by ISP to authenticate the client that attempts to connect. If you are not sure, consult your ISP or select **AUTO**.

MAC Clone: When you cannot access the Internet after finishing other settings here except this option, consider whether it's the matter of the MAC address of your computer. Clicking **Clone MAC** button copies the MAC address of your computer to the router.

MTU: Keep the default value unless you are sure it is necessary for your ISP connection.

Dial on demand: Connect to ISP only when there is traffic transmission. This saves your broadband Internet service bill.

PPP IP extension: If enabled, all the IP addresses in outgoing packets including management packets on the WAN port will be changed to the device's WAN IP address. Only change the default settings if necessary.

Enable PPP Debug Mode: Only enable this feature if supported by your ISP.

Bridge PPPoE Frames Between WAN and Local Ports: If enabled, PPPoE dialup frame from LAN side will directly egress the WAN port without modification.

Multicast Proxy: If enabled, the router will use multicast proxy.

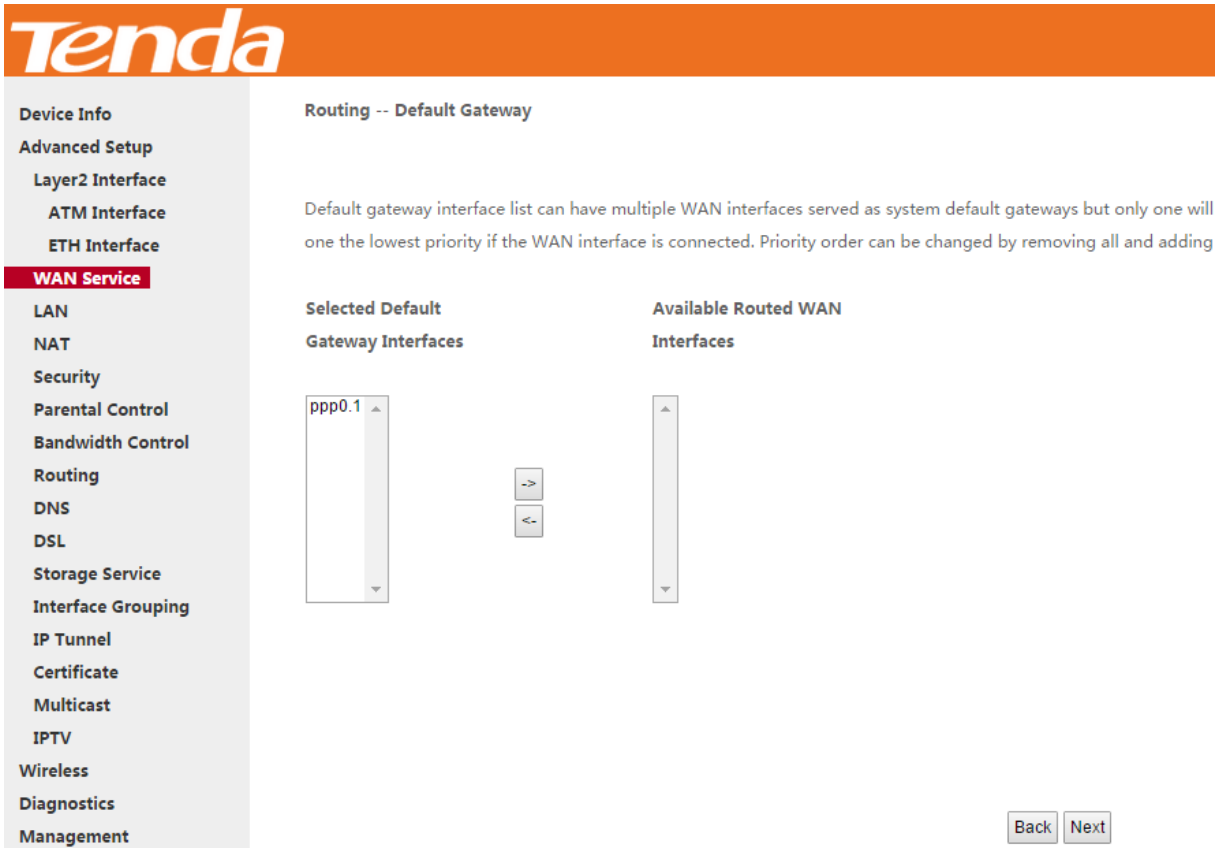
KNOWLEDGE EXPANSION

1. **MAC Clone:** Many broadband ISPs restrict access by allowing traffic only from the MAC address of your broadband modem, but some ISPs additionally register the MAC address of your computer when your account is first opened. If so, only by cloning the MAC address of your computer can you access the Internet through the router.

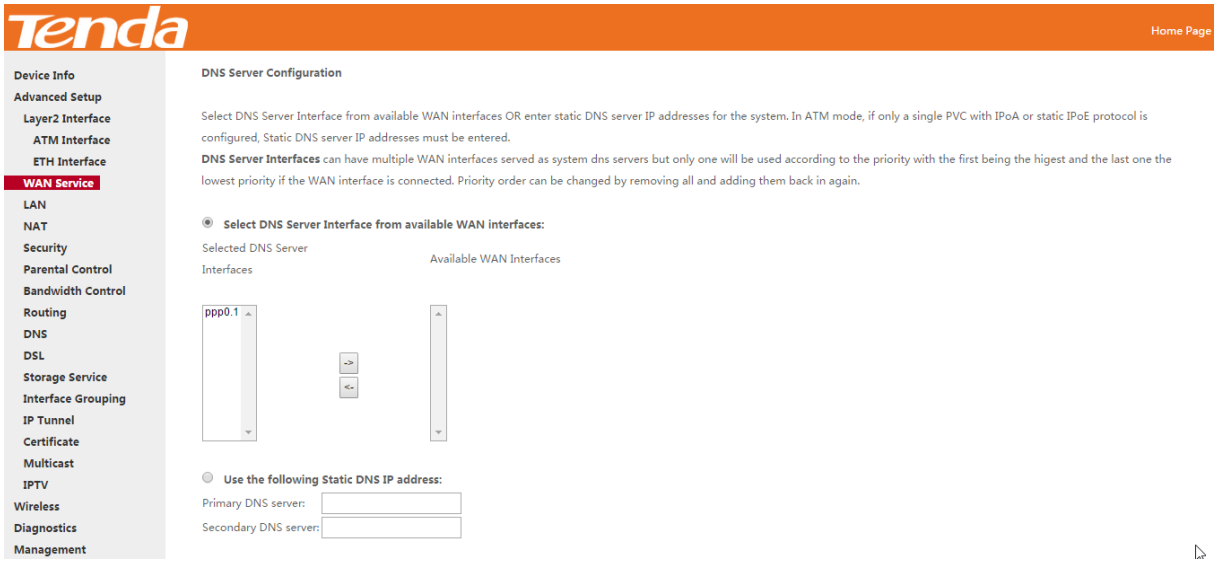
2. **MTU**: Short for ***Maximum Transmission Unit***, the largest physical packet size, measured in bytes, which

a network can transmit. Any messages larger than the MTU are divided into smaller packets before being sent. The default MTU is 1460 bytes. For some ISPs, you might need to change the MTU. This is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.

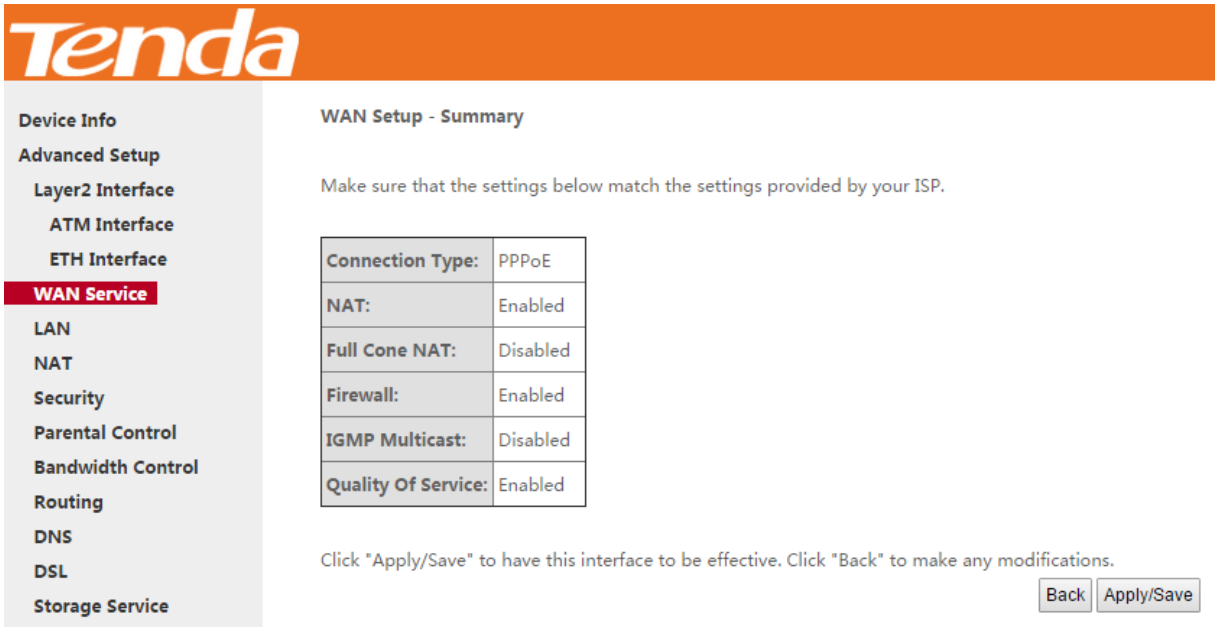
Step 5: To configure the Default Gateway interface, select the interface that you want to configure with the WAN gateway address in **Available Routed WAN Interfaces** box and move it into **Selected Default Gateway Interfaces** box. The default setting is recommended. Then click **Next**.



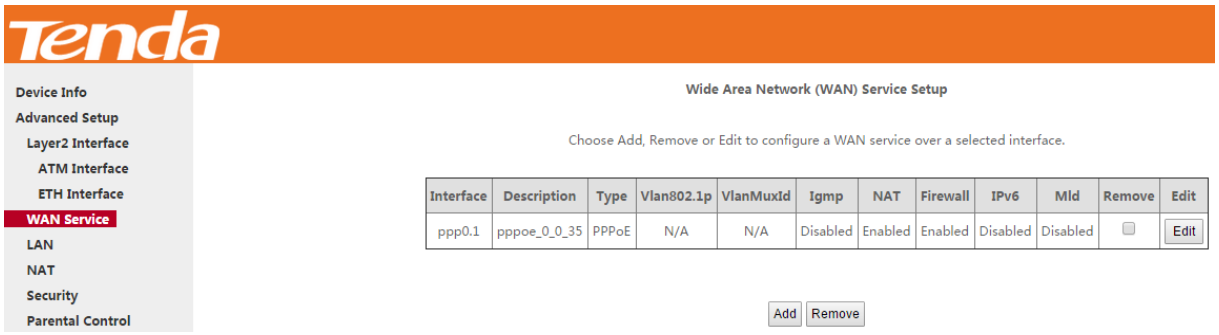
Step 6: To configure the WAN DNS address, click the **Select DNS Server Interface from available WAN interfaces** option, or select the **Use the following Static DNS IP address** option and enter the static DNS server IP addresses provided by your ISP. At last, click **Next**.



Step 7: Here you can view your configurations. Click **Apply/Save** to save your settings if everything is correctly set.

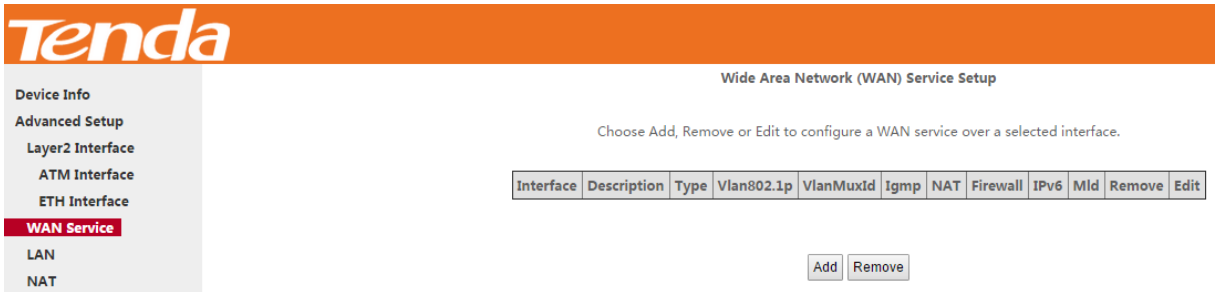


When the PPPoE connection is successful, you can access the Internet.



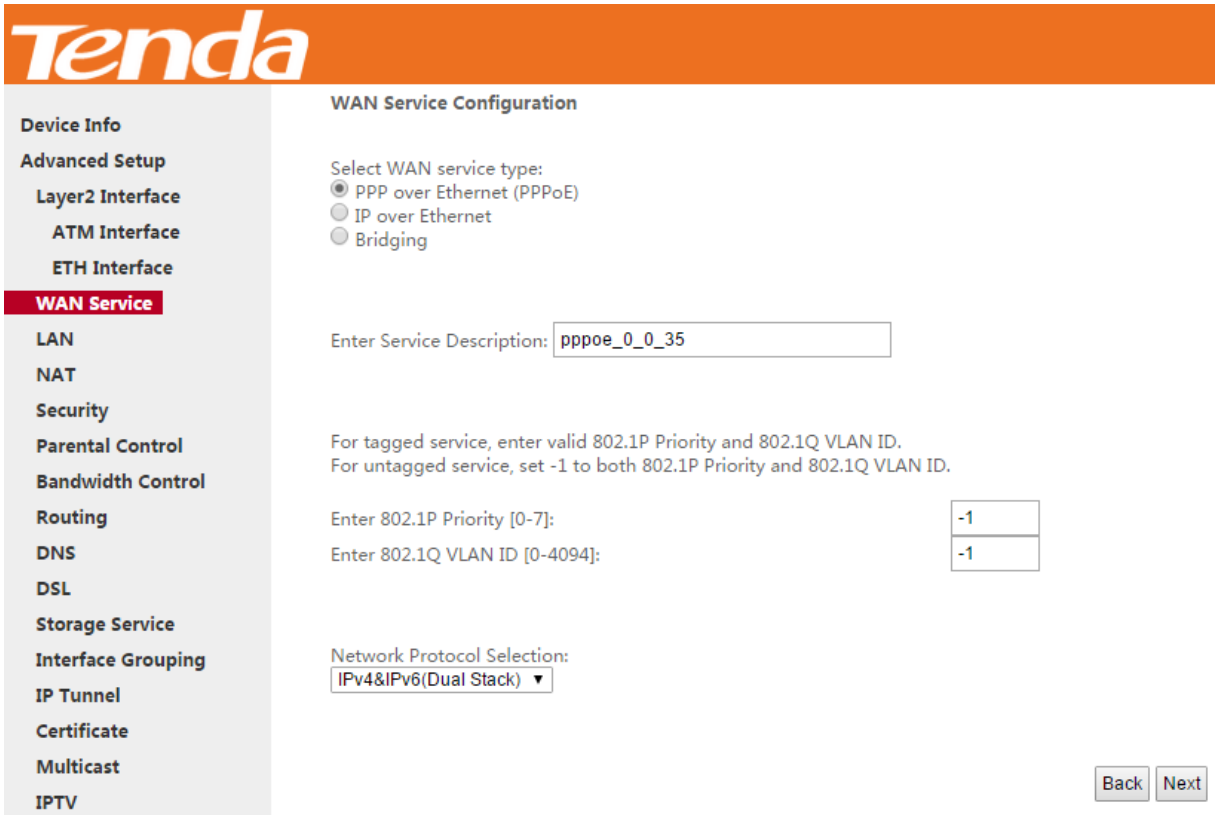
IPv4 & IPv6 (Dual Stack)

Step 1: Click **Advanced Setup** > **WAN Service** and then click the **Add** button.

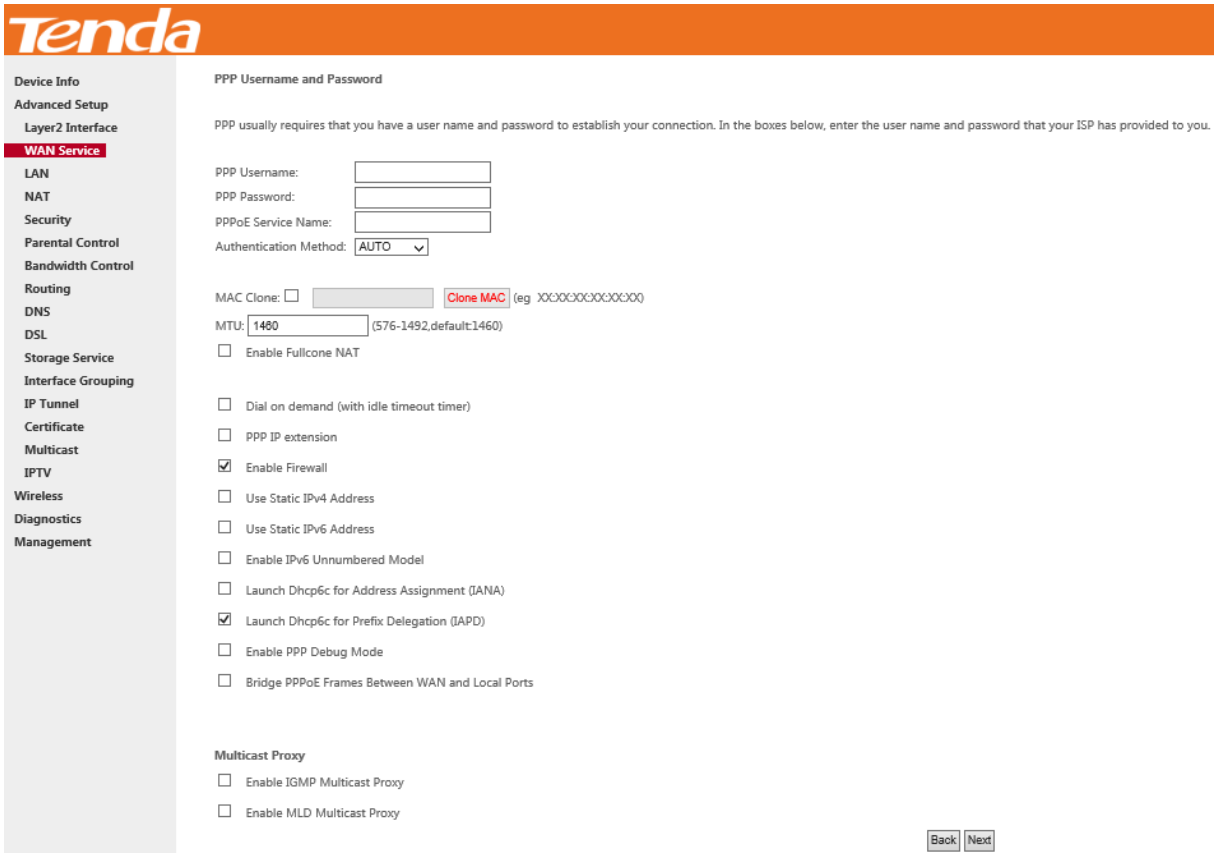


Step 2: Select the ATM interface you added just now from the pull-down menu in the figure below. Click **Next**.

Step 3: Select **PPP over Ethernet (PPPoE)**. Edit the **Enter Service Description** field which is optional. Suggest you keep the default. Select a network protocol: **IPv4&IPv6 (Dual Stack)**. Click **Next**.



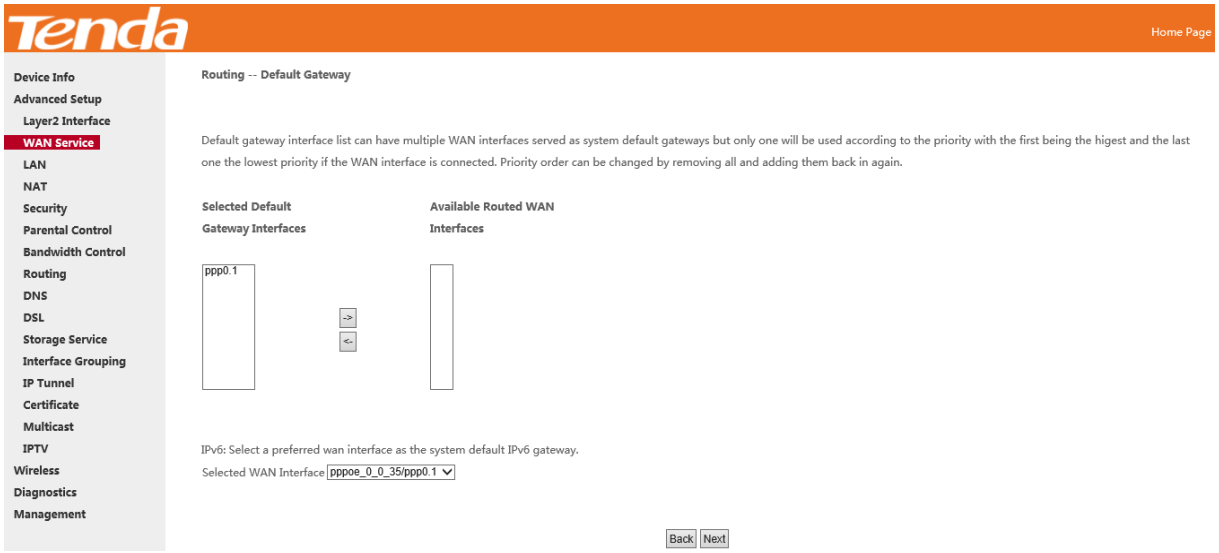
Step 4: Configure PPP Username and Password and other settings on the figure below. Each field with its indication is mentioned above in **IPv4 Only (PPPoE)** section. Check **Launch Dhcp6c for Prefix Delegation (IAPD)**. Click **Next**.



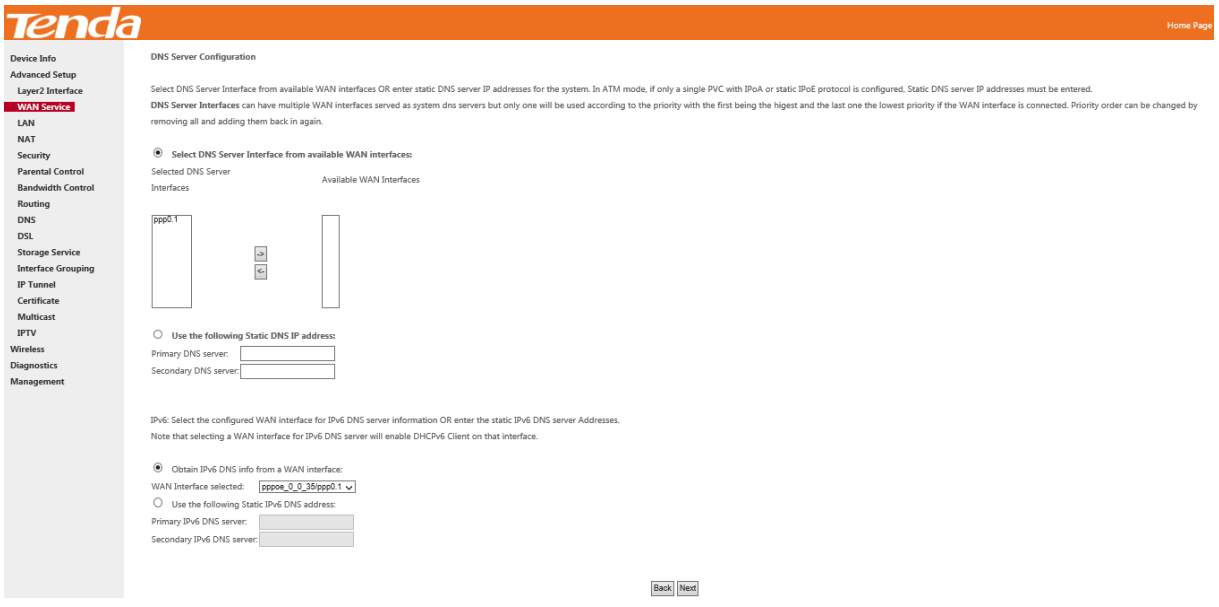
If your ISP is using static DHCPv6, check **Launch Dhcp6c for Address Assignment (IANA)** also, or configure a static

IP address by checking **Use Static IPv6 Address** and enter the static IPv6 address.

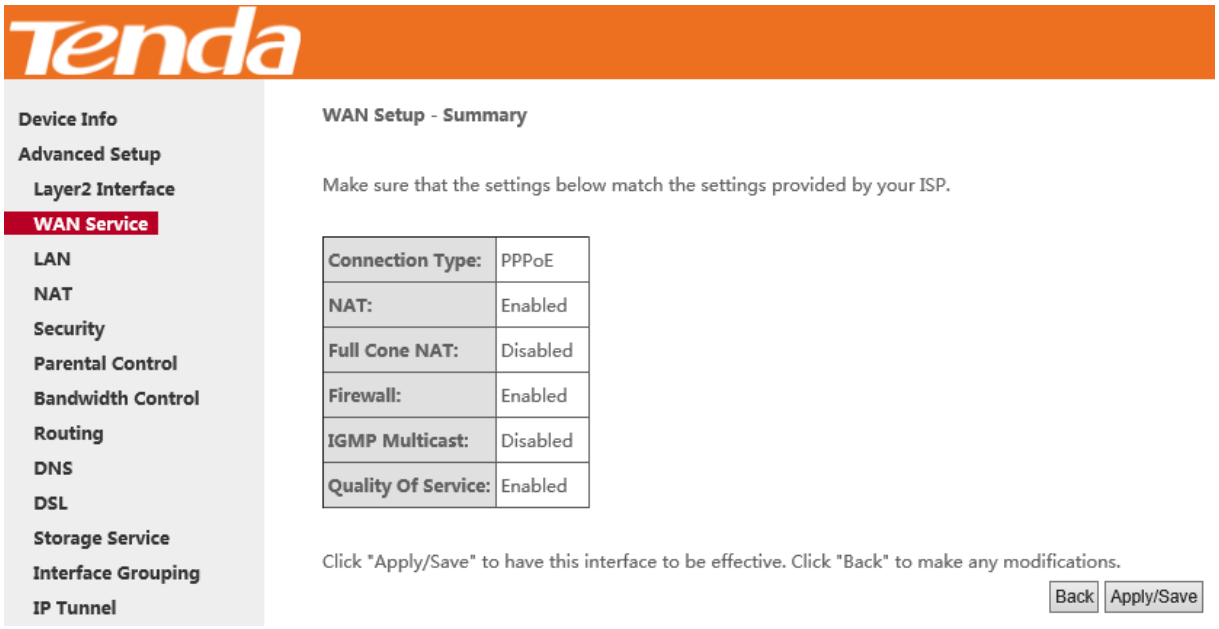
Step 5: To configure the Default Gateway interface when using IPv6, select the interface that you want to configure with the WAN gateway address in **Selected WAN Interface** box. Then click **Next**.



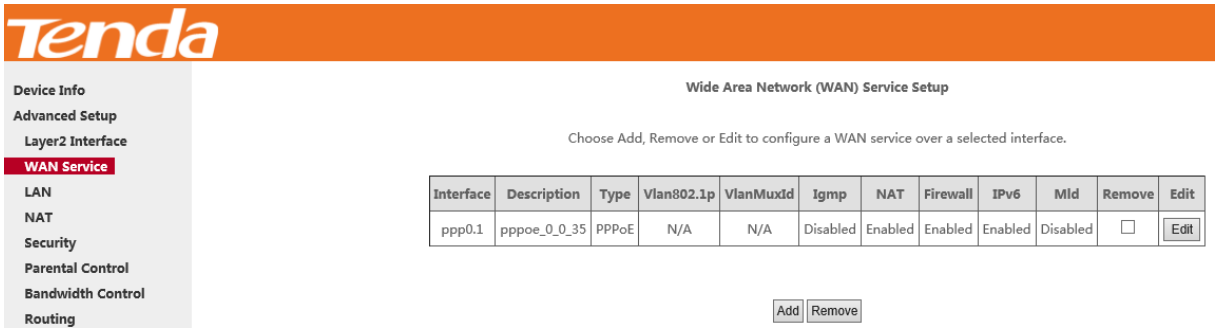
Step 6: To configure the WAN DNS address, check the **Obtain IPv6 DNS info from a WAN interface** option, or select the **Use the following Static IPv6 DNS address** option to enter the static DNS server IPv6 addresses provided by your ISP. At last, click **Next**.



Step 7: Here you can view your configurations. Click **Apply/Save** to save your settings if everything is correctly set.

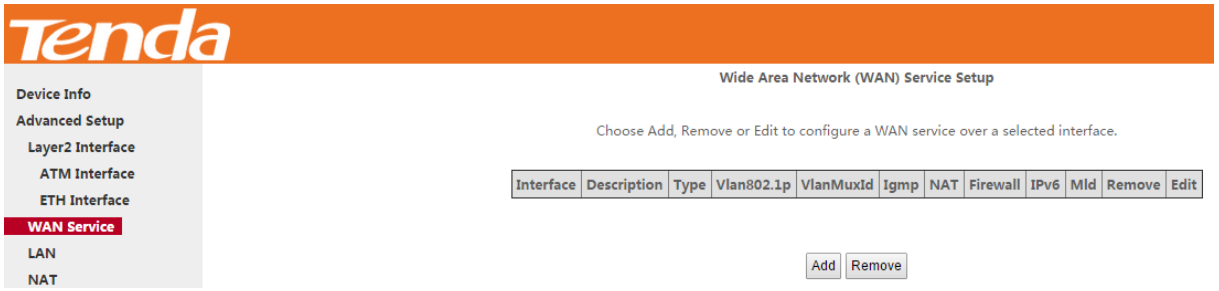


When the PPPoE connection is successful, you can access the Internet.



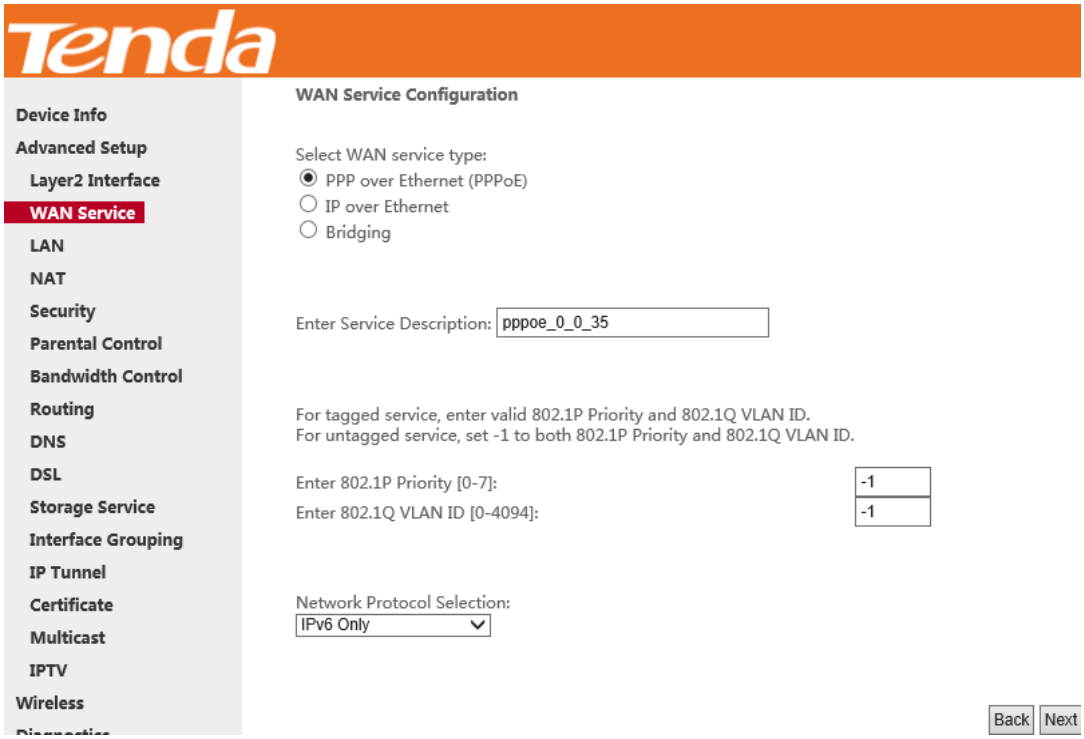
IPv6 Only

Step 1: Click **Advanced Setup** > **WAN Service** and then click the **Add** button.



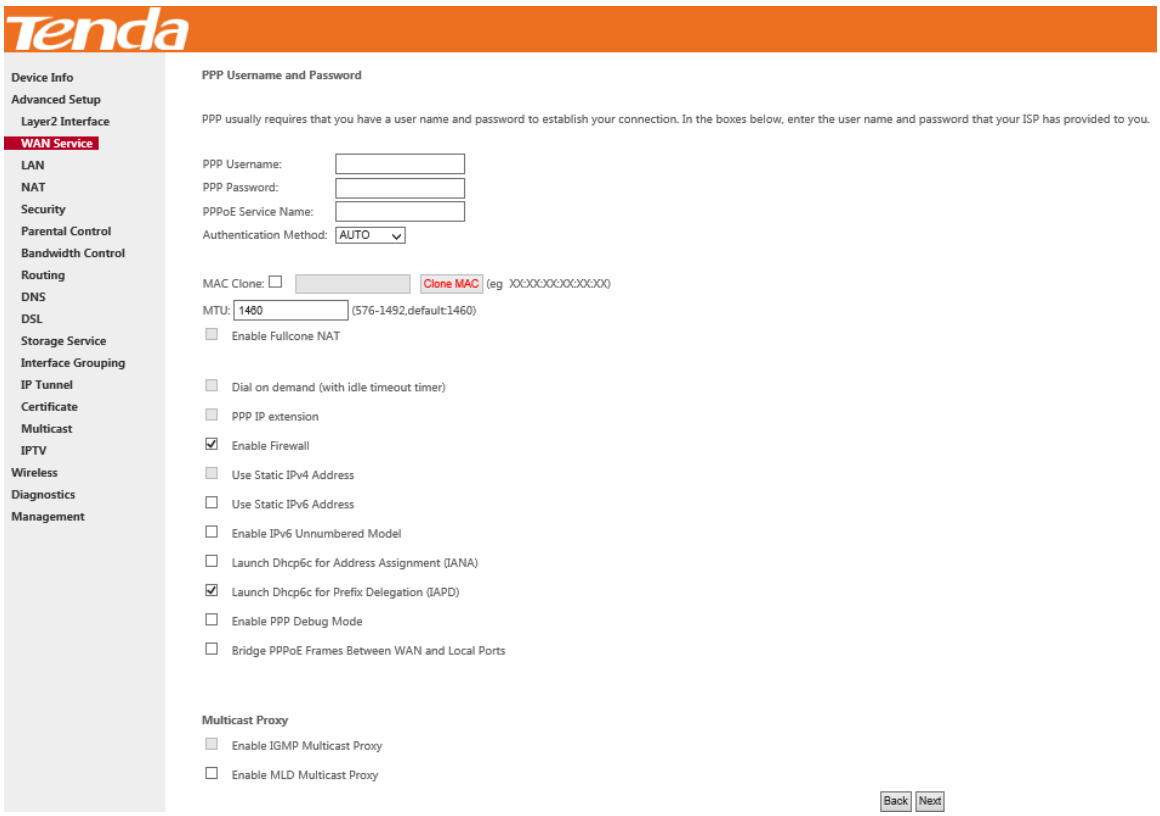
Step 2: Select the ATM interface you added just now from the pull-down menu in the figure below. Click **Next**.

Step 3: Select **PPP over Ethernet (PPPoE)**. Edit the **Enter Service Description** field which is optional. Suggest you keep the default. Select a network protocol you need: **IPv6 Only**. Click **Next.**



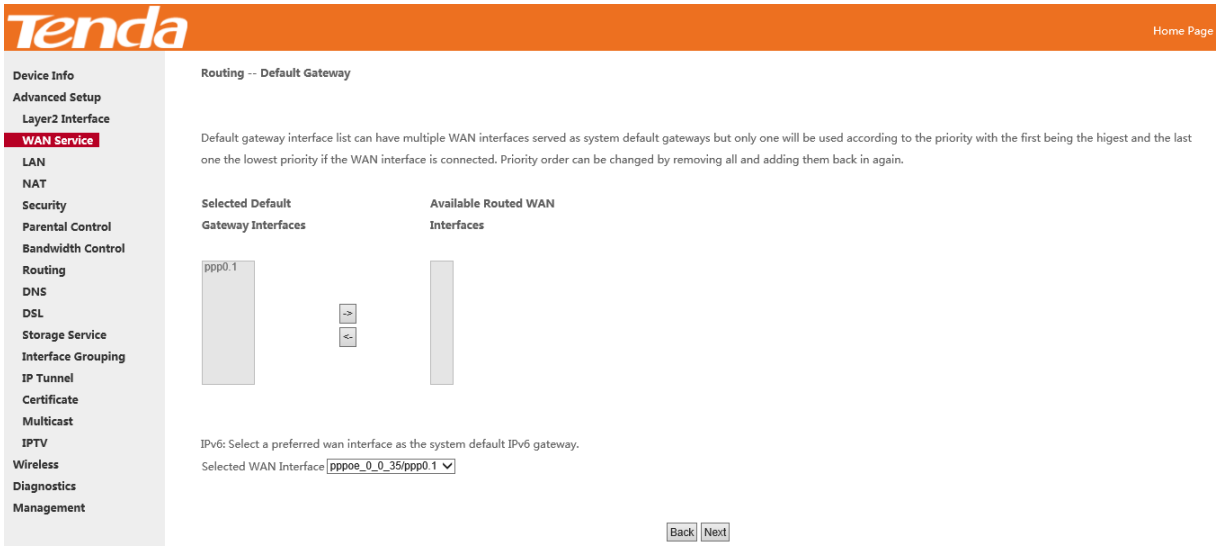
Step 4: Configure PPP Username and Password and other settings on the figure below. Each field with its indication is mentioned above in **IPv4 Only (PPPoE)** section.

If ISP provides you no static IPv6 address, you just keep the default settings for it's by default the DHCP mode. Check **Launch Dhcp6c for Prefix Delegation (IAPD)**. If your ISP is using stateful DHCPv6, check **Launch Dhcp6c for Address Assignment (IANA)** also. Click **Next**.

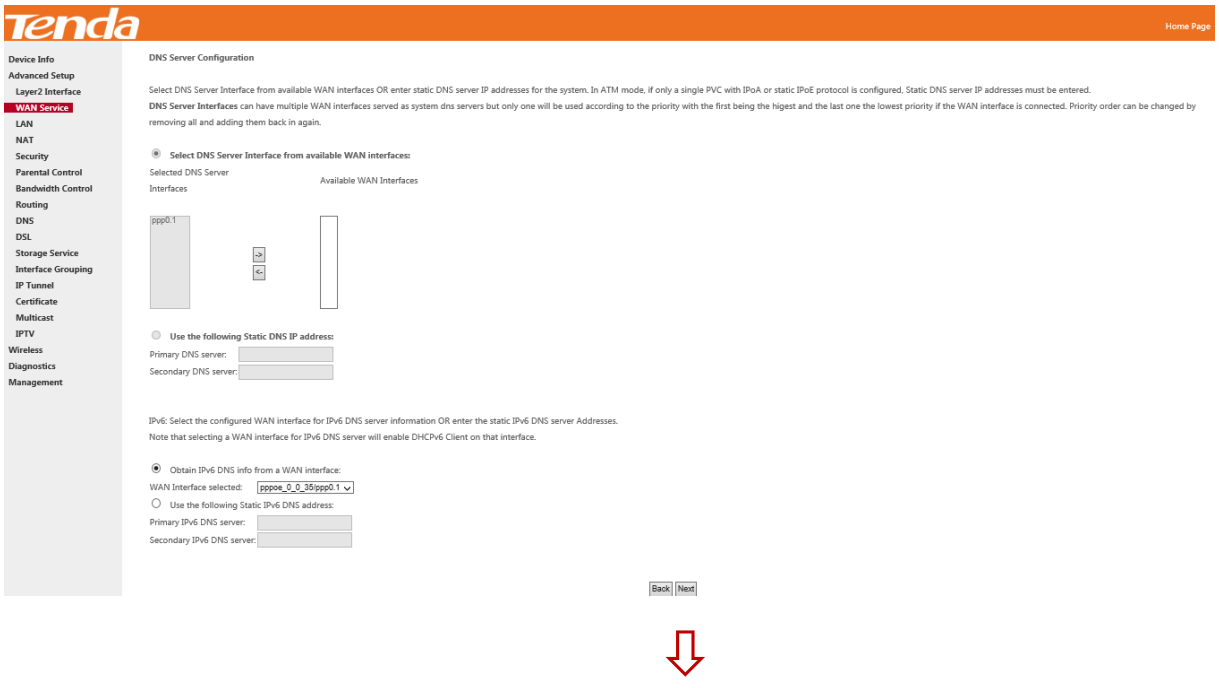


If ISP provides you with the static IPv6 address, configure a static IP address by checking **Use Static IPv6 Address** and enter the static IPv6 address.

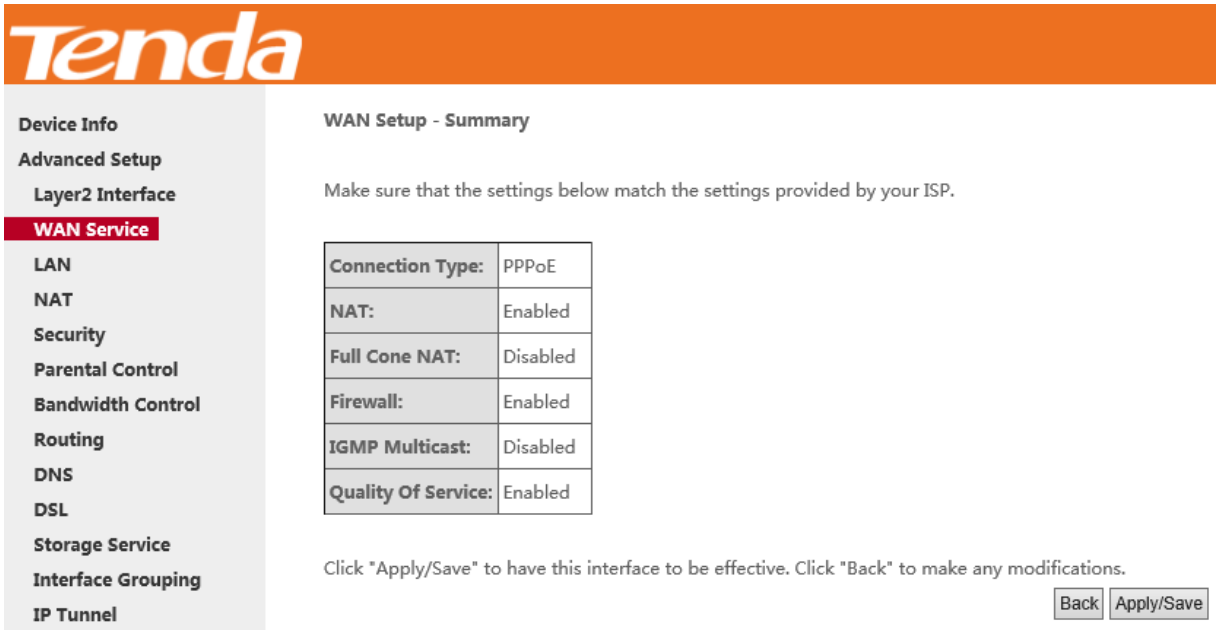
Step 5: To configure the Default Gateway interface when using IPv6, select the interface that you want to configure with the WAN gateway address in **Selected WAN Interface** box. Then click **Next**.



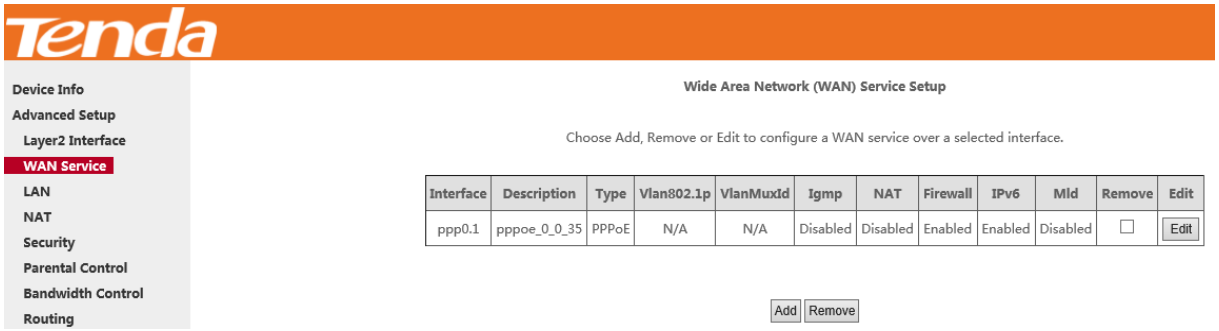
Step 6: To configure the WAN DNS address, check the **Obtain IPv6 DNS info from a WAN interface** option, or select the **Use the following Static IPv6 DNS address** option to enter the static DNS server IPv6 addresses provided by your ISP. At last, click **Next**.



Step 7: Here you can view your configurations. Click **Apply/Save** to take this interface into effect.



When the PPPoE connection is successful, you can access the Internet.

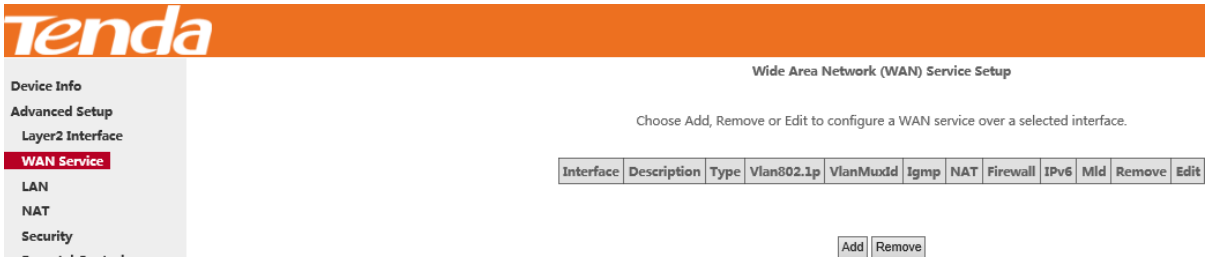


IPoE

IPv4 Only

If you get an IP address from your ISP automatically or if your ISP assigns you a static (fixed) IP address, subnet mask and gateway, you need to select the IP over Ethernet (IPoE).

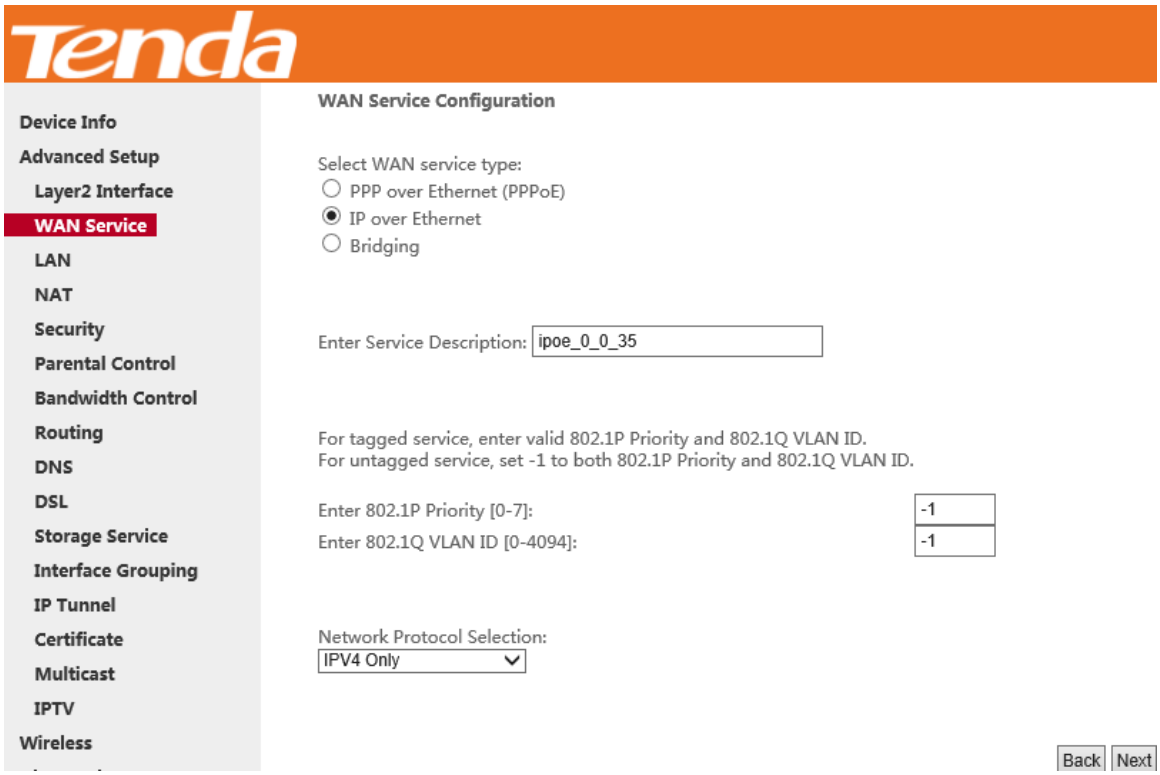
Step 1: Click **Advanced Setup** > **WAN Service** and then click the **Add** button.



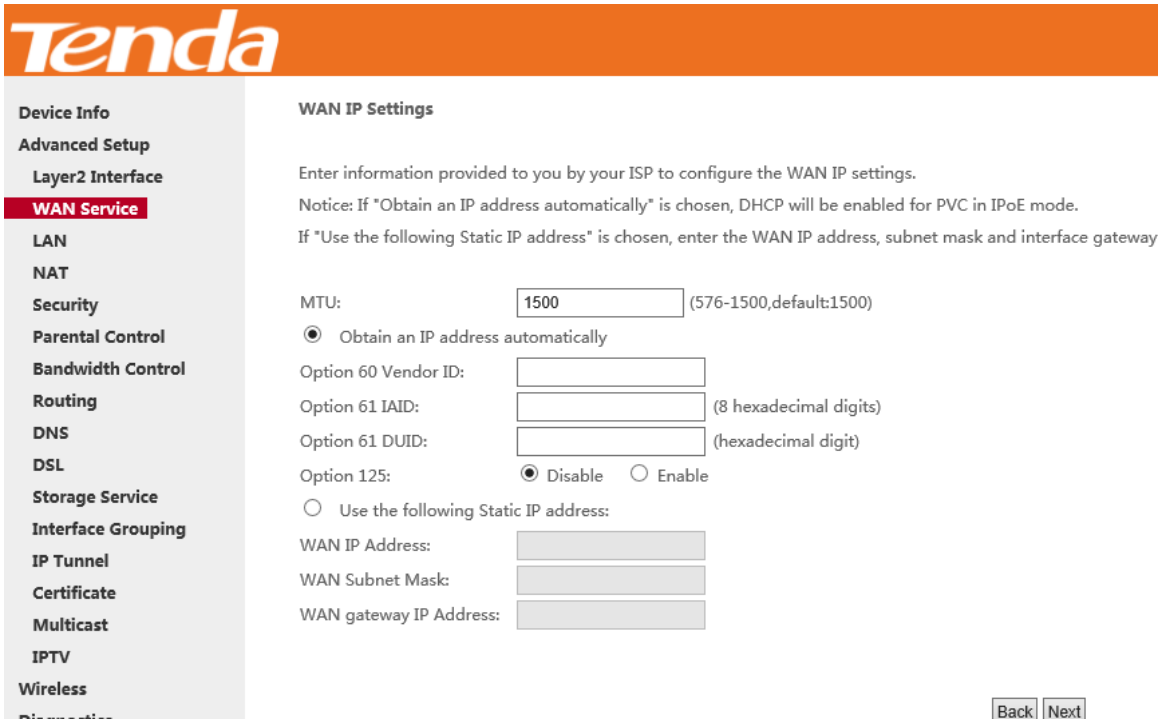
Step 2: Select the ATM interface you added just now from the pull-down menu in the figure below. Click **Next**.

Step 3: Select **IP over Ethernet**. Edit the **Enter Service Description** which is optional. Suggest you keep the default.

Select a network protocol: **IPv4 Only**. Click **Next**.



Step 4: Finish **WAN IP Settings** on the figure below. Click **Next**.



Obtain an IP address automatically: This allows the router to automatically acquire IP information from your ISP or your existing networking equipment.

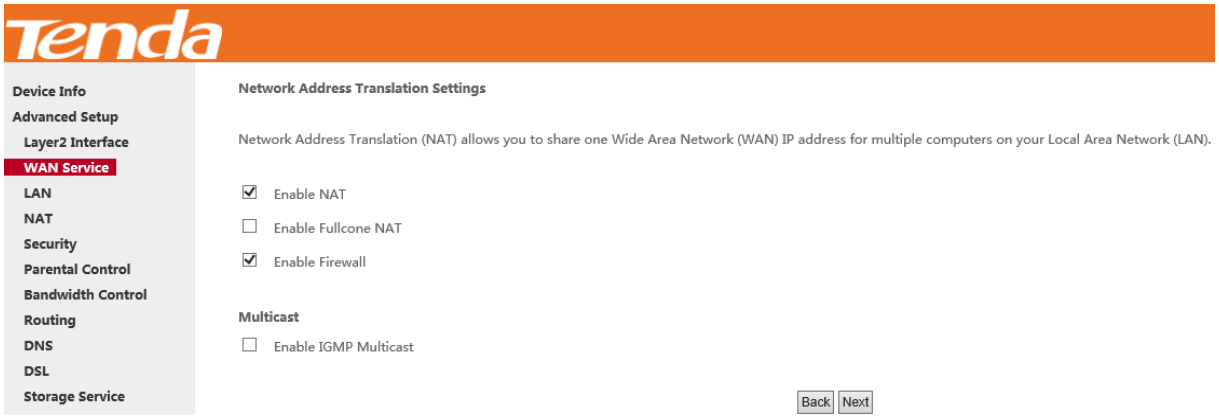
Use the following Static IP address: This allows you to specify the Static IP information provided by your ISP or that corresponds with your existing networking equipment.

WAN IP Address: The Internet IP address provided by your ISP for accessing the Internet.

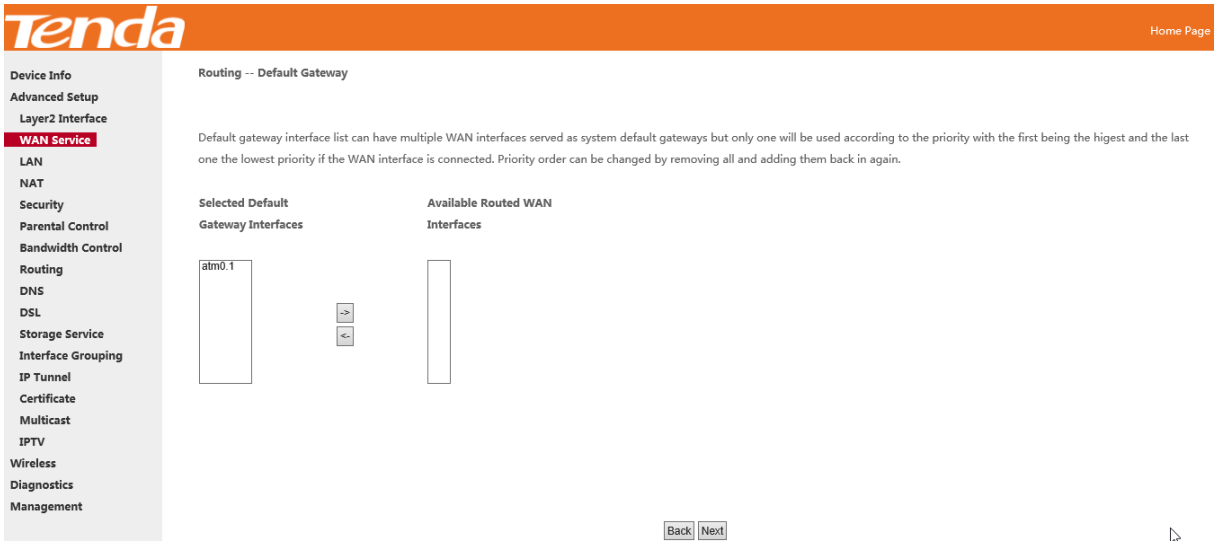
WAN Subnet Mask: The subnet mask address provided by your ISP for accessing the Internet.

WAN gateway IP Address: The gateway IP address provided by your ISP for accessing the Internet.

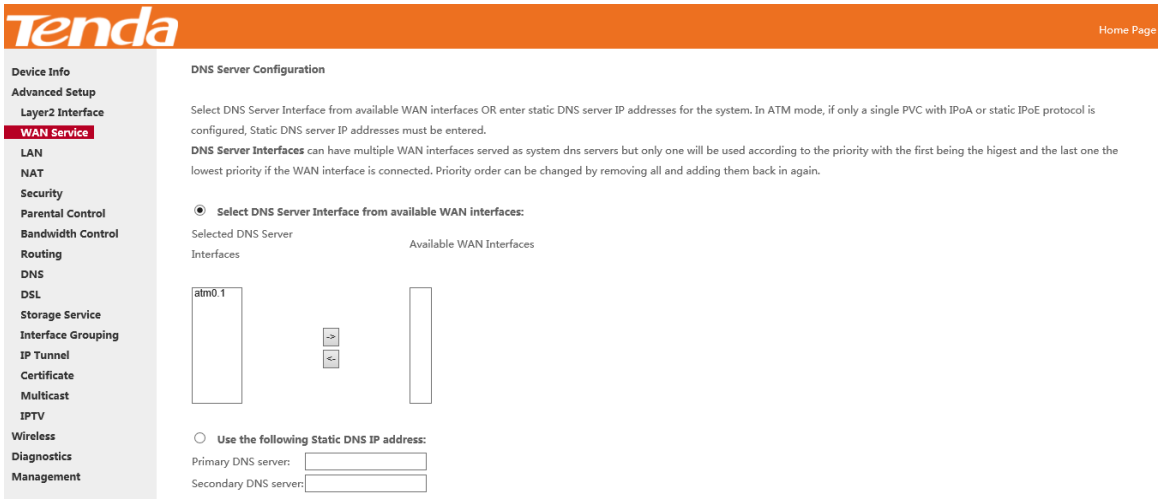
Step 5: Finish Network Address Translation Settings. Suggest keep the default settings. Click **Next**.



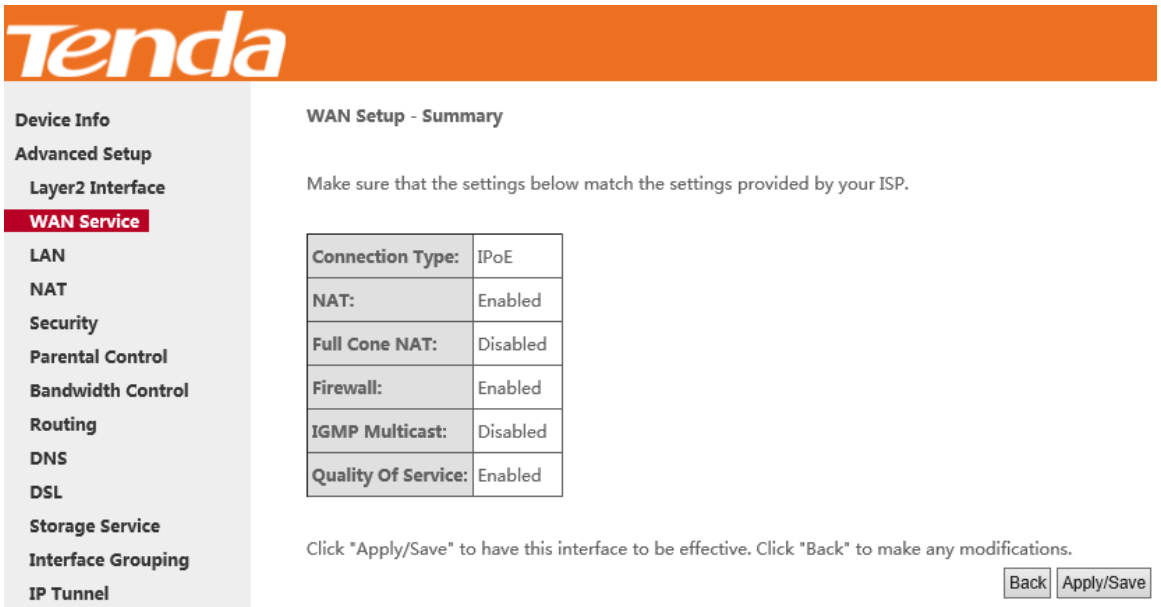
Step 6: To configure the Default Gateway interface, select the interface that you want to configure with the WAN gateway address in **Available Routed WAN Interfaces** box and move it into **Selected Default Gateway Interfaces** box. The default setting is recommended. Then click **Next**.



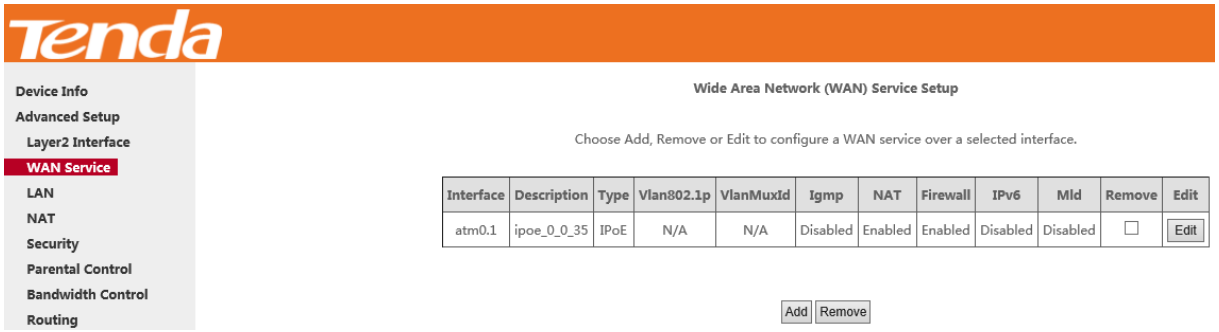
Step 7: To finish DNS Server Configuration, click the **Select DNS Server Interface from available WAN interfaces** option, or select the **Use the following Static DNS IP address** option and enter the static DNS server IP addresses provided by your ISP. At last, click **Next**.



Step 8: Here you can view your configurations. Click **Apply/Save** to save your settings if everything is correctly set.

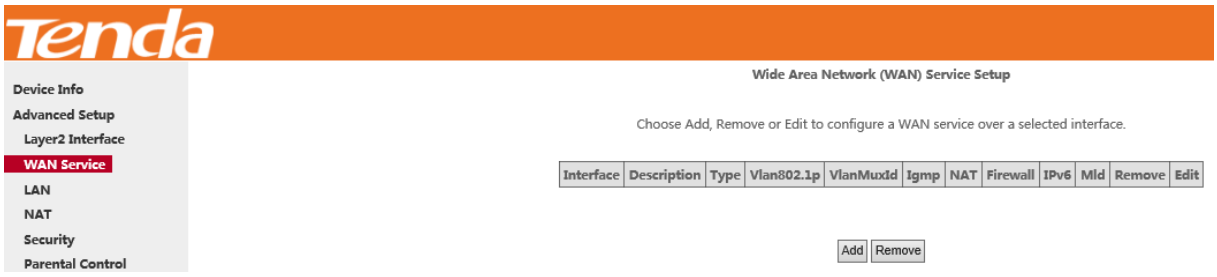


When the IPoE connection is successful, you can access the Internet.



IPv4 & IPv6 (Dual Stack)

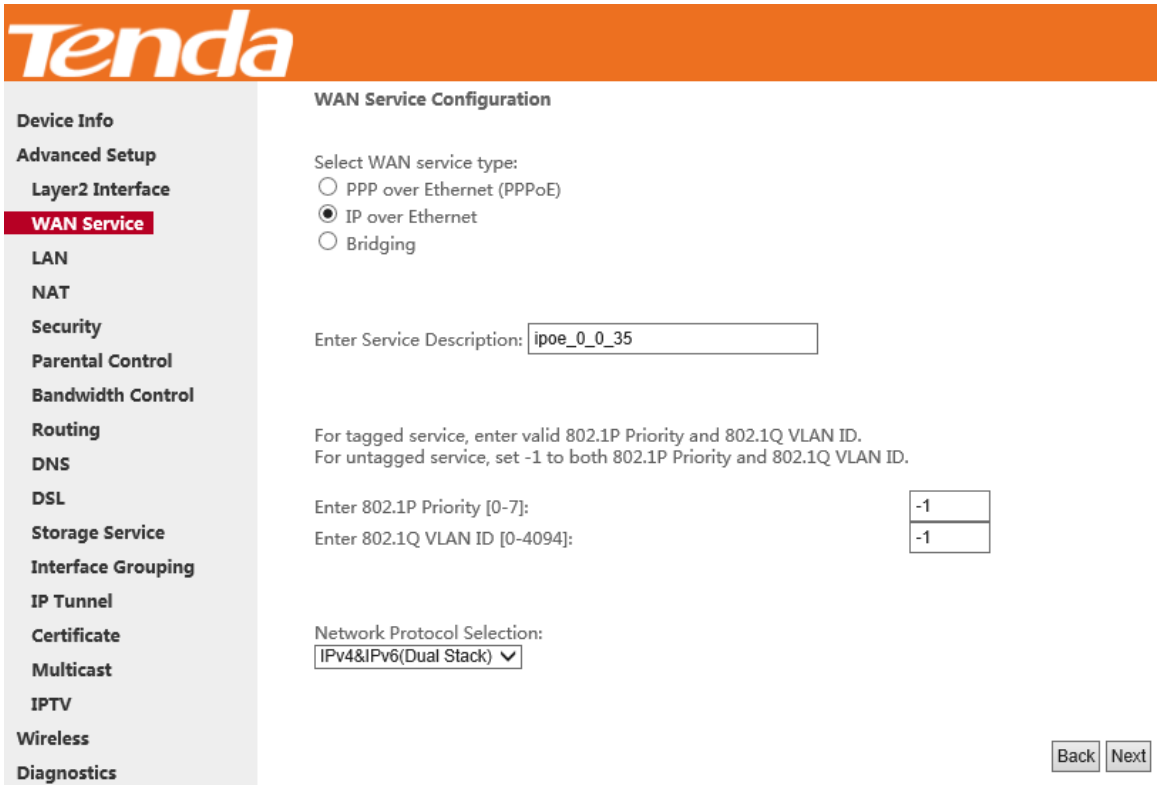
Step 1: Click **Advanced Setup** > **WAN Service** and then click the **Add** button.



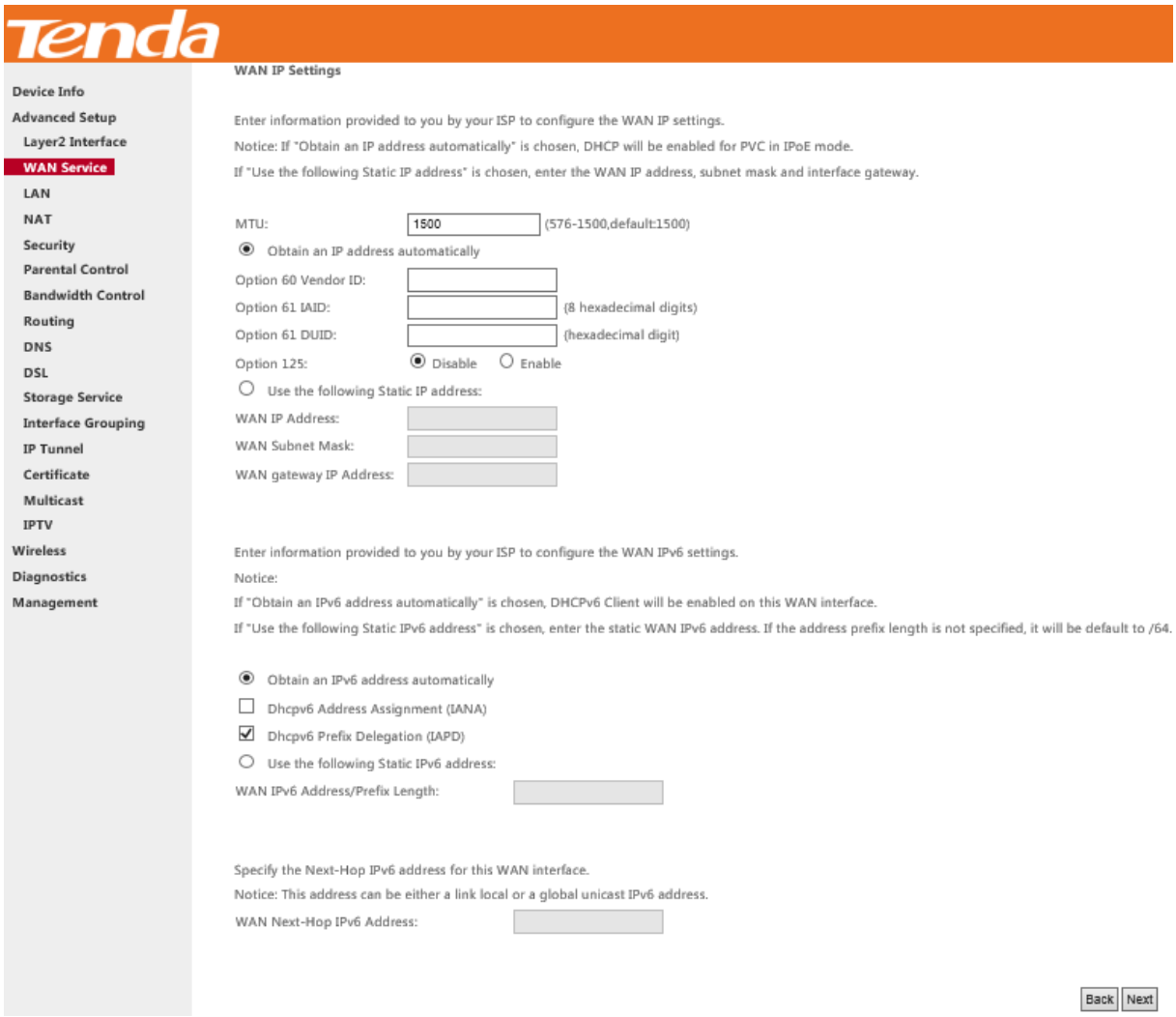
Step 2: Select the ATM interface you added just now from the pull-down menu in the figure below. Click **Next**.

Step 3: Select **IP over Ethernet**. Edit the **Enter Service Description** which is optional. Suggest you keep the default.

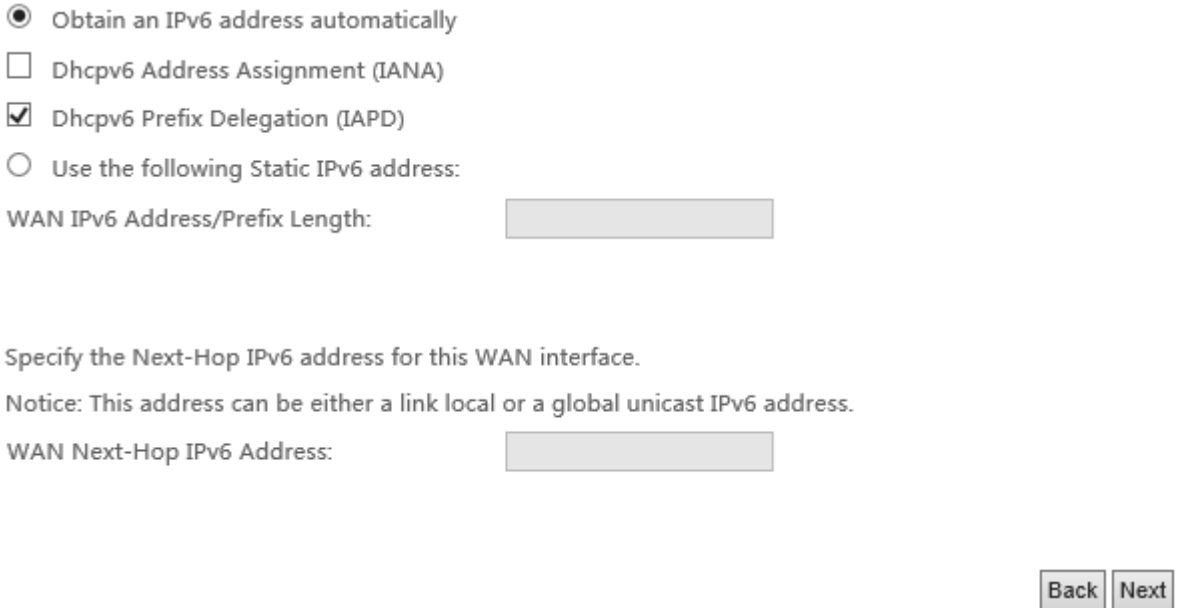
Select a network protocol: **IPv4&IPv6 (Dual Stack)**. Click **Next**.



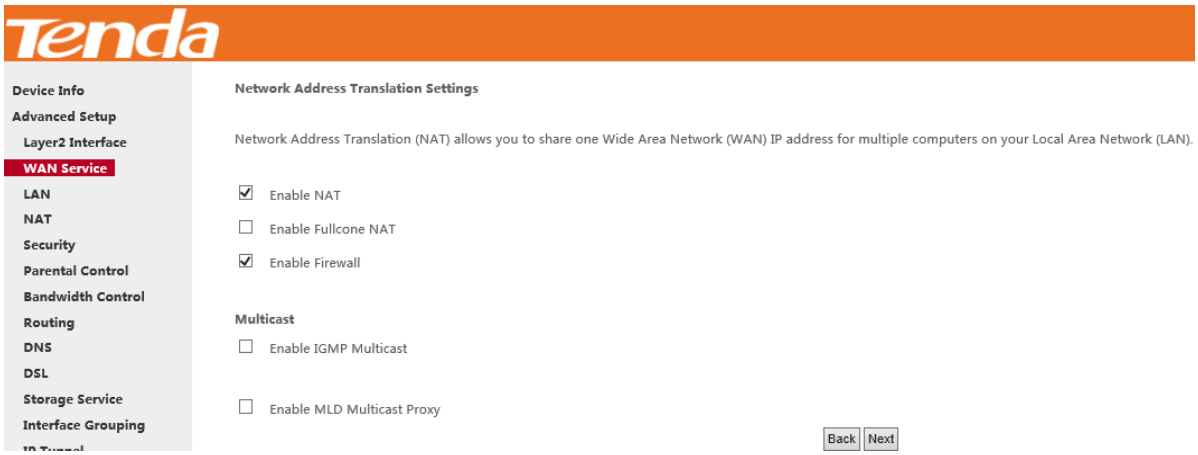
Step 4: To finish WAN IP Settings, select **Obtain an IPv6 address automatically**, check **Dhcpv6 Prefix Delegation (IAPD)**. If your ISP is using stateful DHCPv6, check **Dhcpv6 Address Assignment (IANA)** also. Or select **Use the following Static IP address** if your ISP provides you with an IPv6 address. Click **Next**.



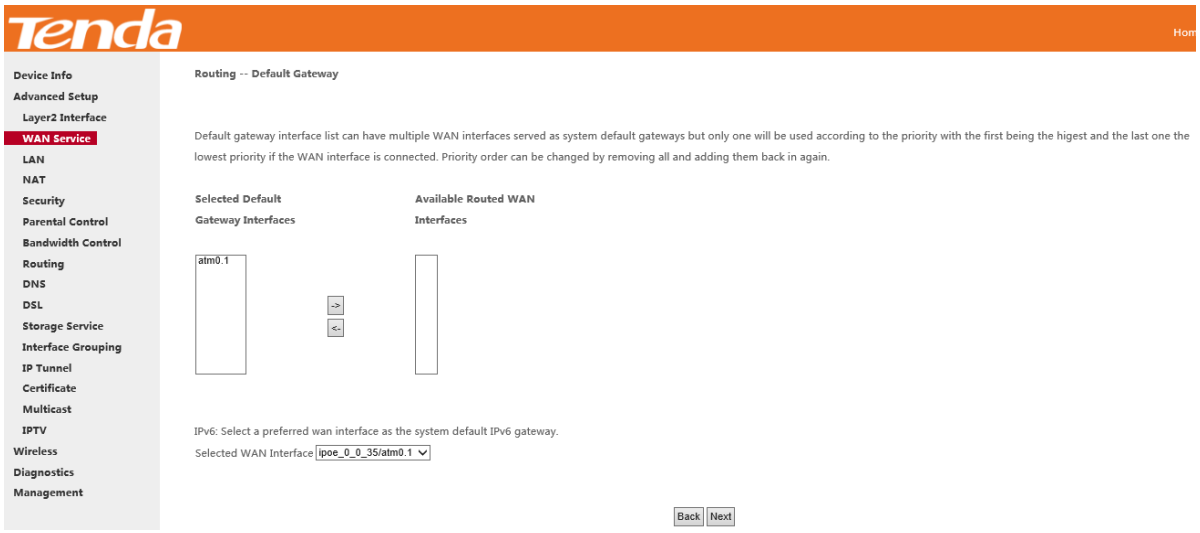
If ISP provides you with the static IPv6 address, configure a static IP address by checking **Use the following Static IPv6 address** and enter the static IPv6 address.



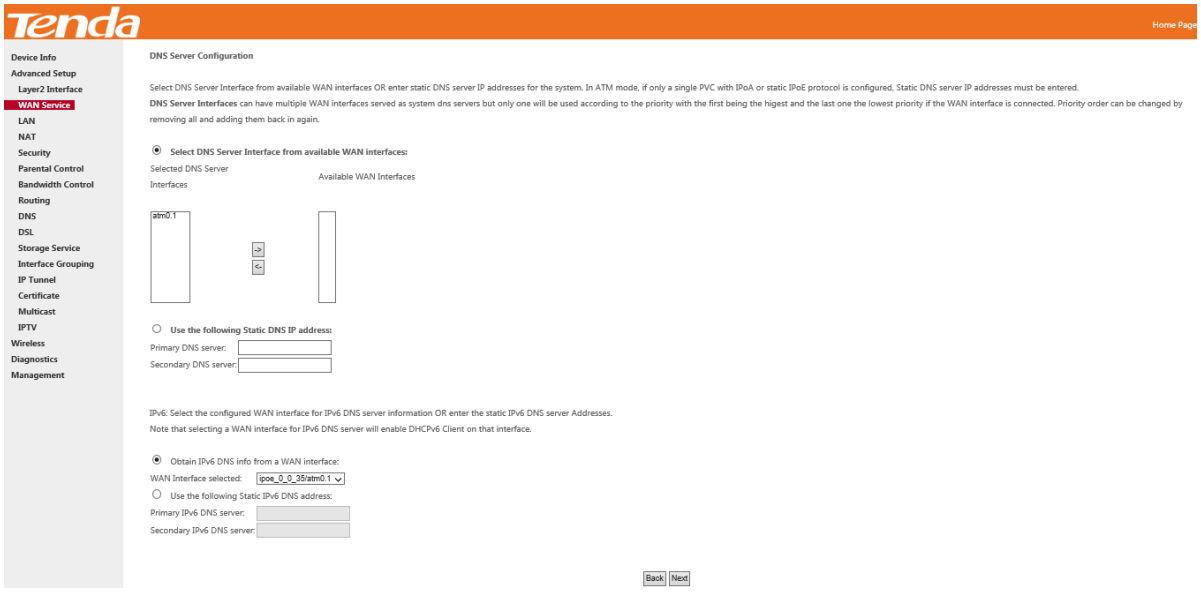
Step 5: Configure NAT settings. If you are unsure about the options, please keep the default settings and then click **Next**.



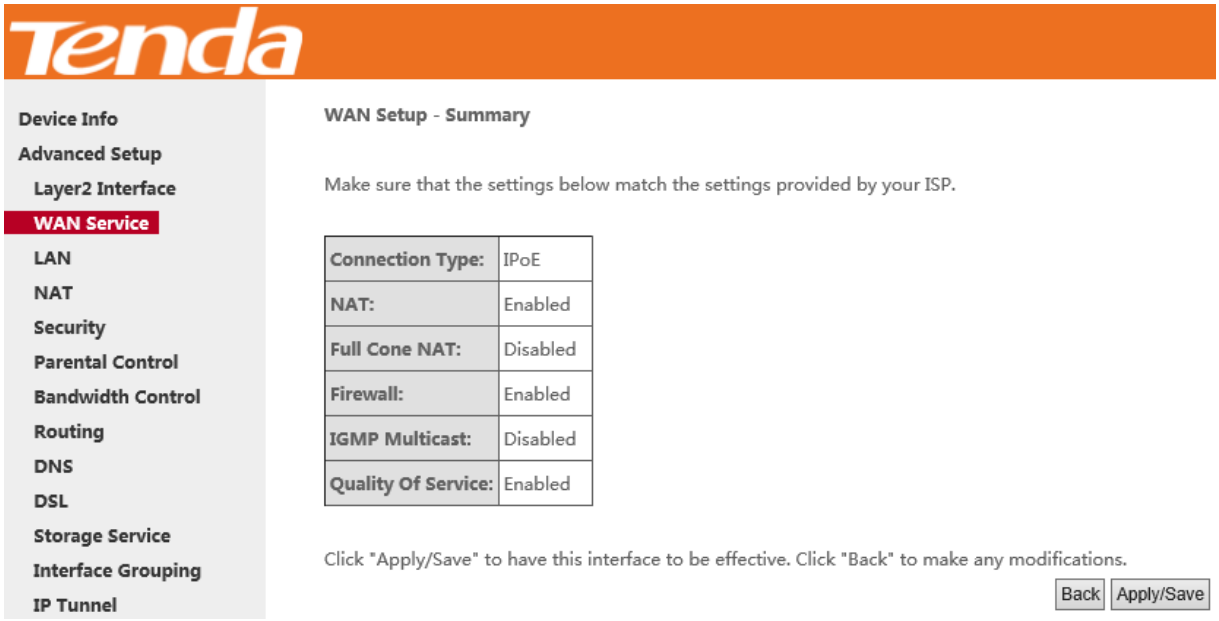
Step 6: To configure the Default Gateway interface, select the interface that you want to configure with the WAN gateway address in **Available Routed WAN Interfaces** box and move it into **Selected Default Gateway Interfaces** box. Then click **Next**.



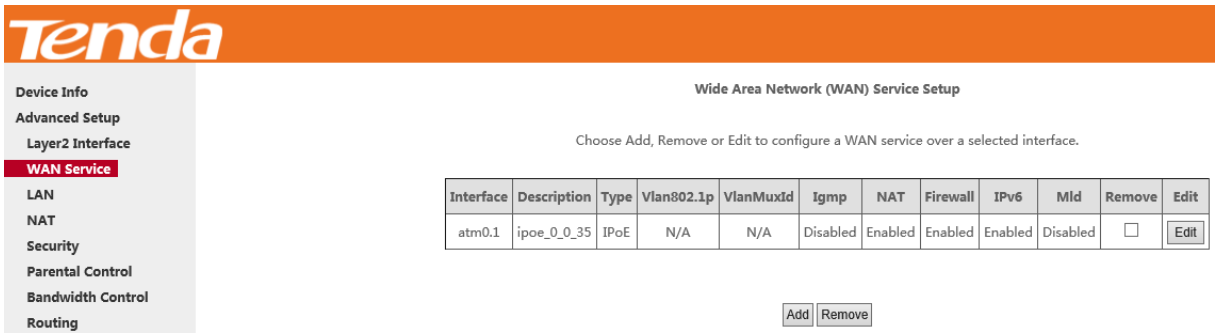
Step 7: To configure the WAN DNS address, check the **Obtain IPv6 DNS info from a WAN interface** option, or select the **Use the following Static IPv6 DNS address** option to enter the static DNS server IPv6 addresses provided by your ISP. At last, click **Next**.



Step 8: Here you can view your configurations. Click **Apply/Save** to save your settings if everything is correctly set.



When the IPoE connection is successful, you can access the Internet.

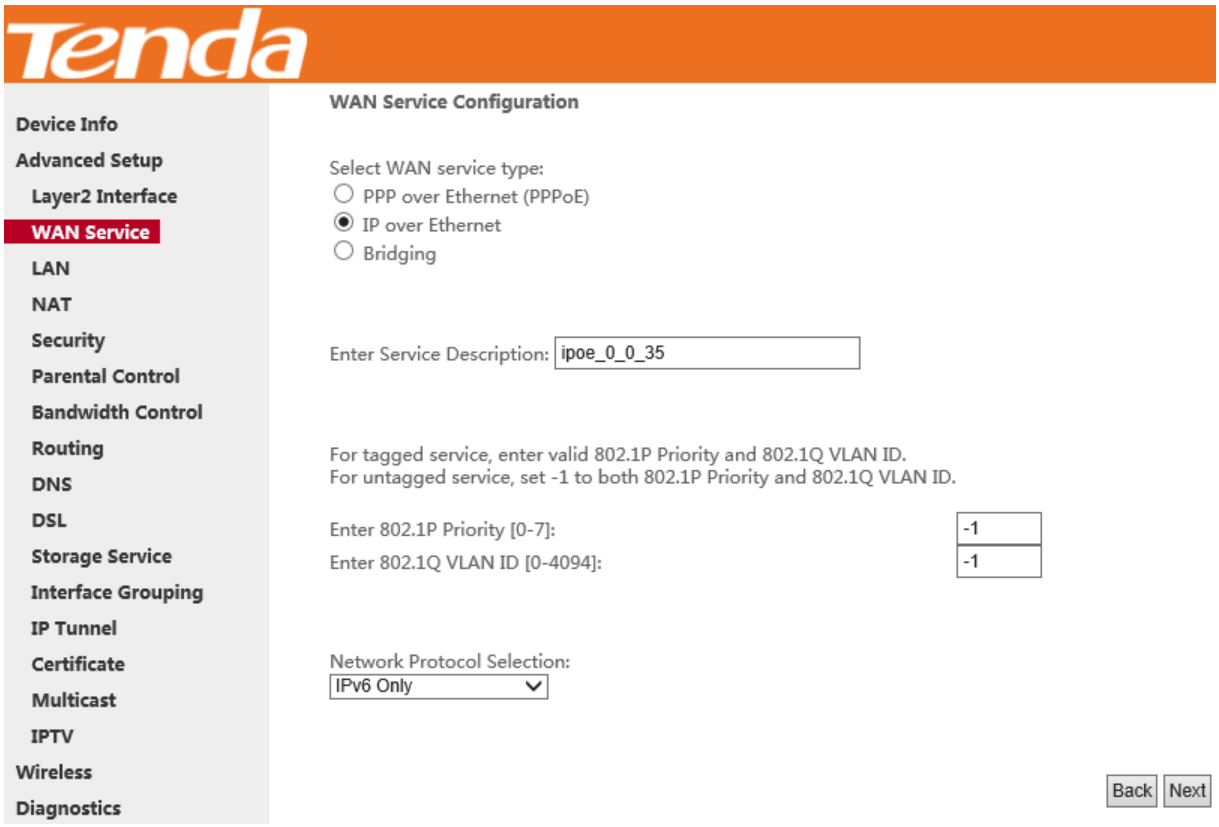


IPv6 Only

Step 1: Click **Advanced Setup** > **WAN Service** and then click the **Add** button.

Step 2: Select the ATM interface you added just now from the pull-down menu in the figure below. Click **Next**.

Step 3: Select **IP over Ethernet (IPoE)**. Edit the **Enter Service Description** field which is optional. Suggest you keep the default. Select a network protocol you need: **IPv6 Only**. Click **Next**.



Step 4: Enter the WAN information provided by your ISP to configure the WAN IPv6 settings.

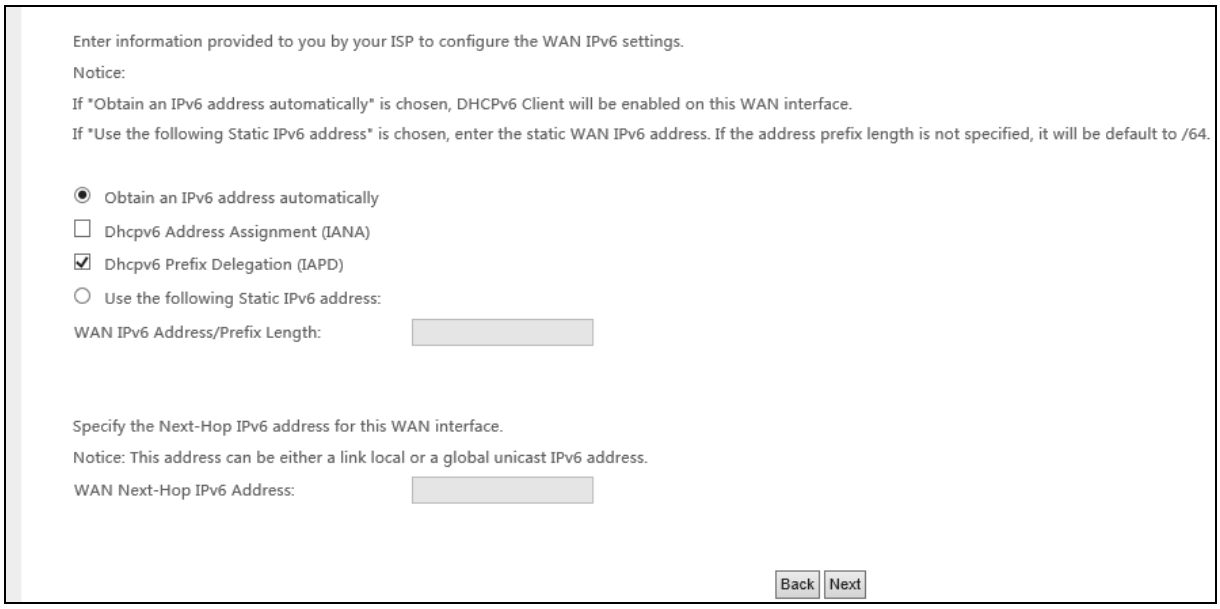
To obtain an IP address automatically:

Select **Obtain an IPv6 address automatically**.

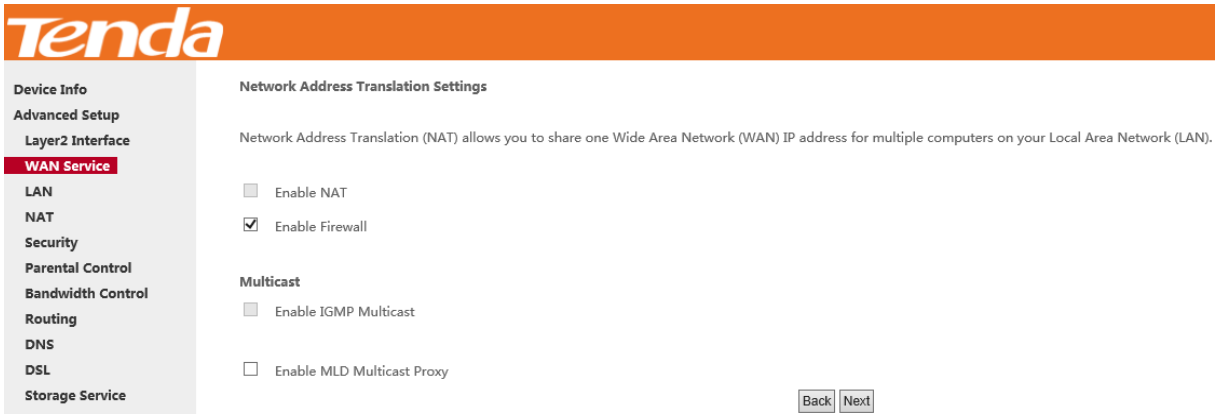
Check **Dhcp6c Prefix Delegation (IAPD)**.

If your ISP is using stateful DHCPv6, check **Dhcp6c Address Assignment (IANA)** also.

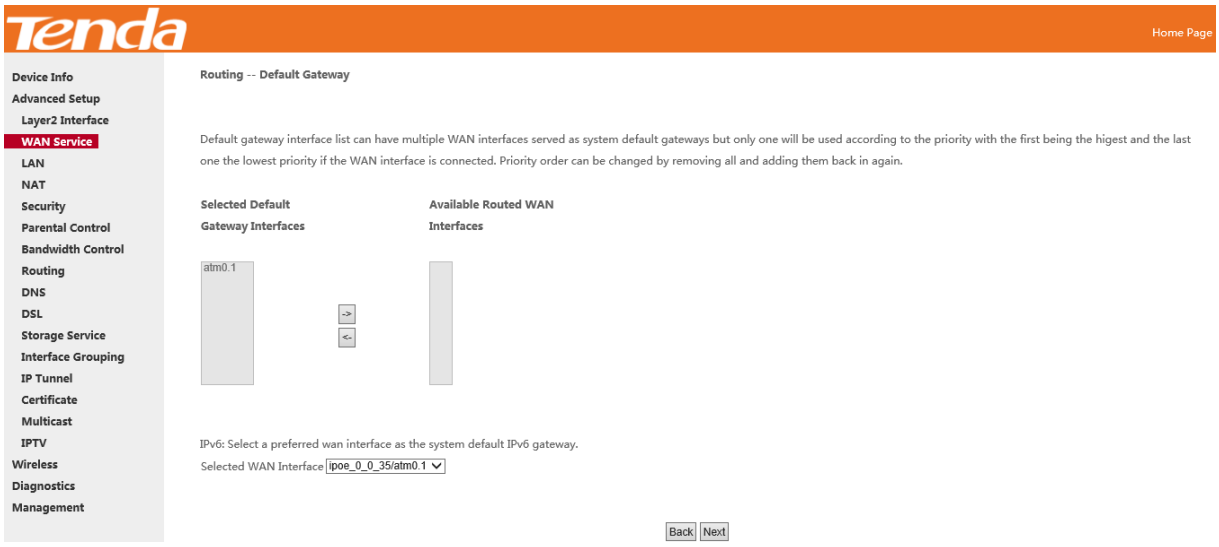
Click **Next** to go forwards.



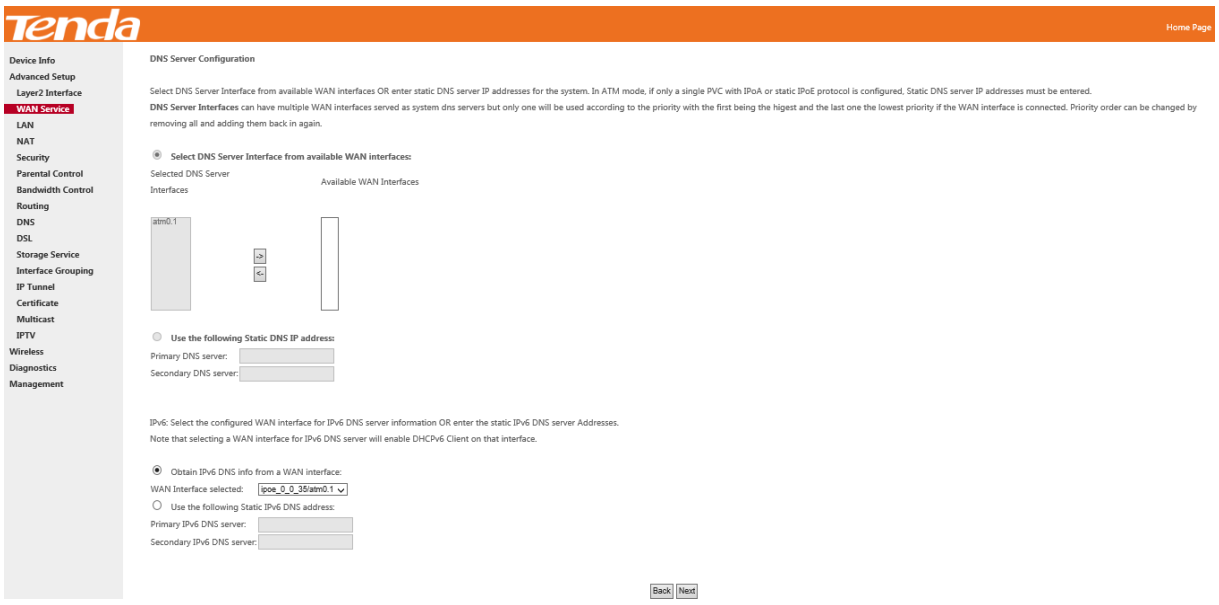
Step 5: Finish Network Address Translation Settings. Suggest keep the default settings. Click **Next**.



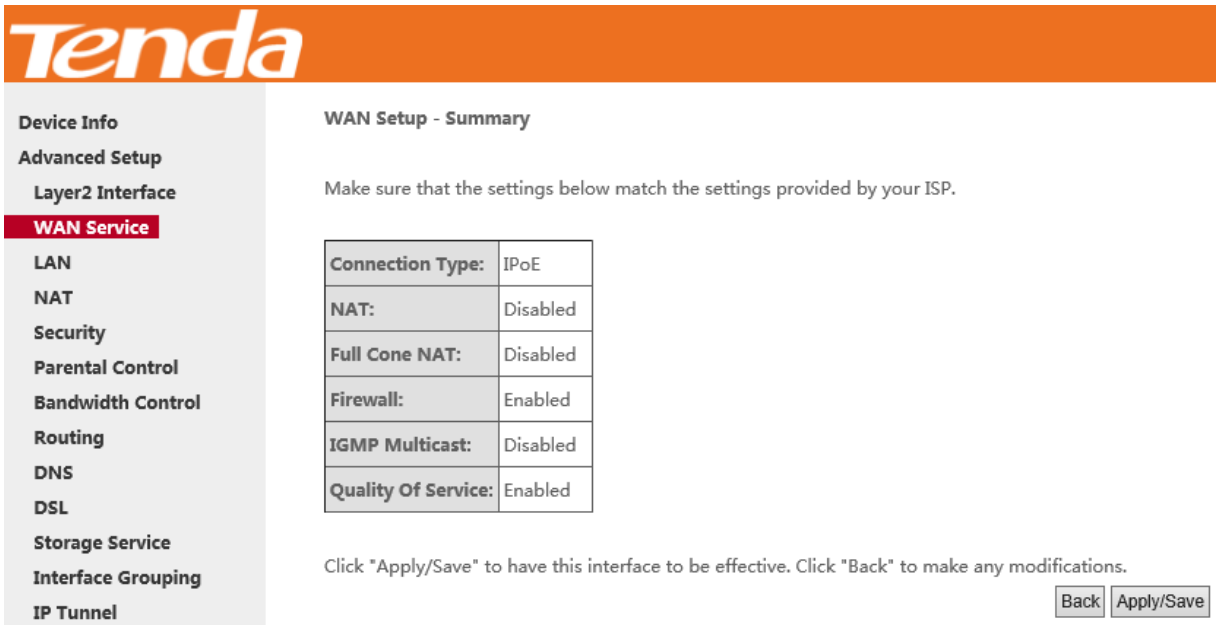
Step 6: To configure the Default Gateway interface when using IPv6, select the interface that you want to configure with the WAN gateway address in **Selected WAN Interface** box. Then click **Next**.



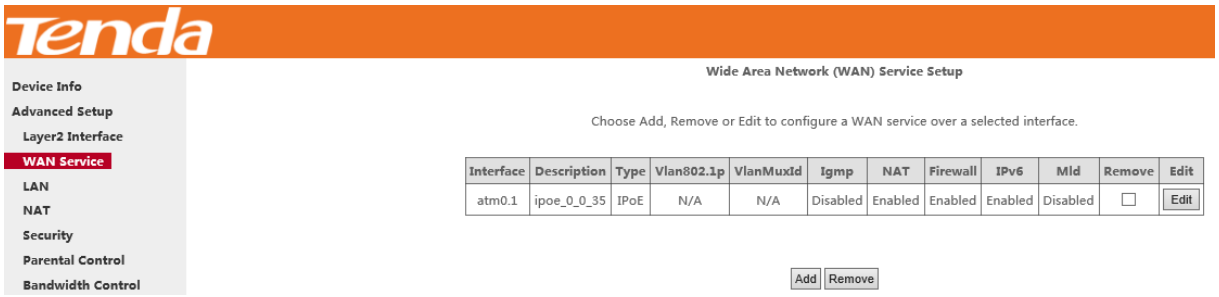
Step 7: To configure the WAN DNS address, check the **Obtain IPv6 DNS info from a WAN interface** option, or select the **Use the following Static IPv6 DNS address** option to enter the static DNS server IPv6 addresses provided by your ISP. At last, click **Next**.



Step 8: Here you can view your configurations. Click **Apply/Save** to have this interface to be effective.



When the IPoE connection is successful, you can access the Internet.



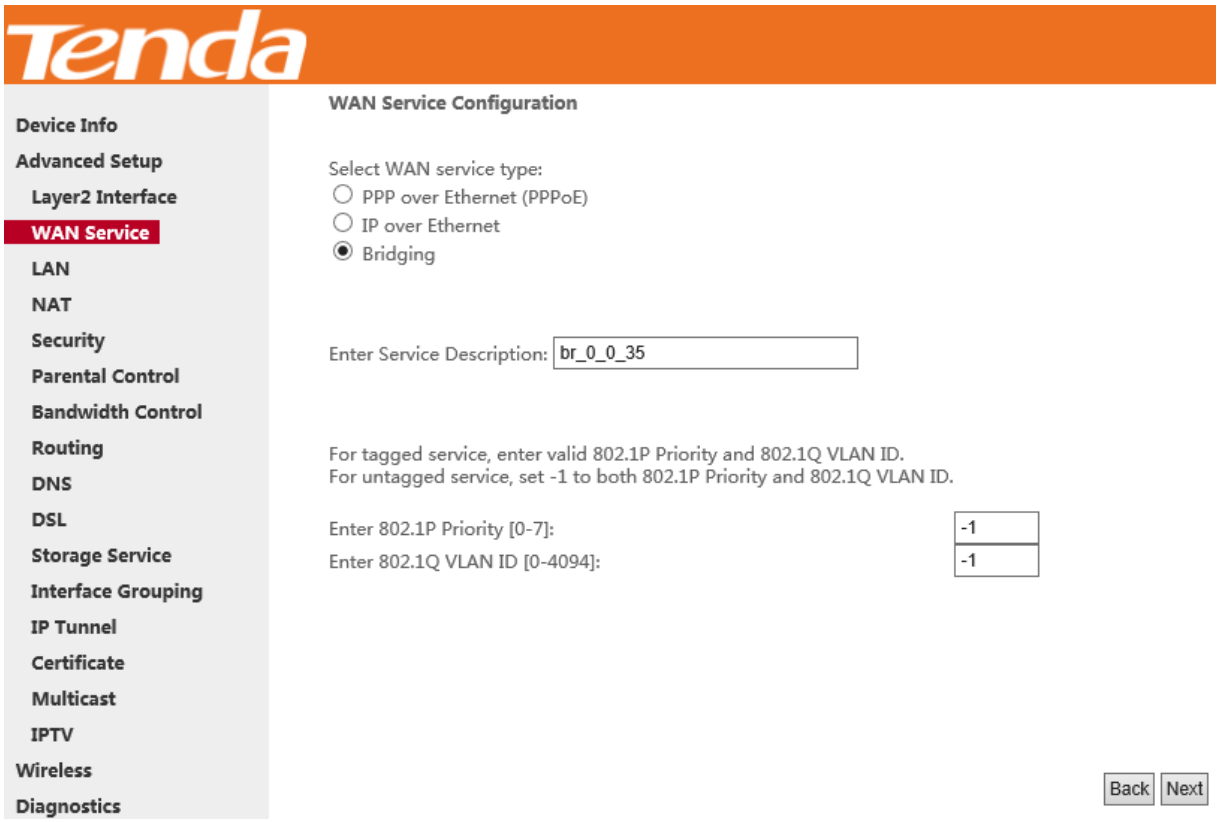
Bridge

If you wish to initiate a dialup directly from your PC for Internet access or enjoy the entire Internet connection (instead of sharing it with others), you can use the Bridging DSL link type and create a dialup program on your PC.

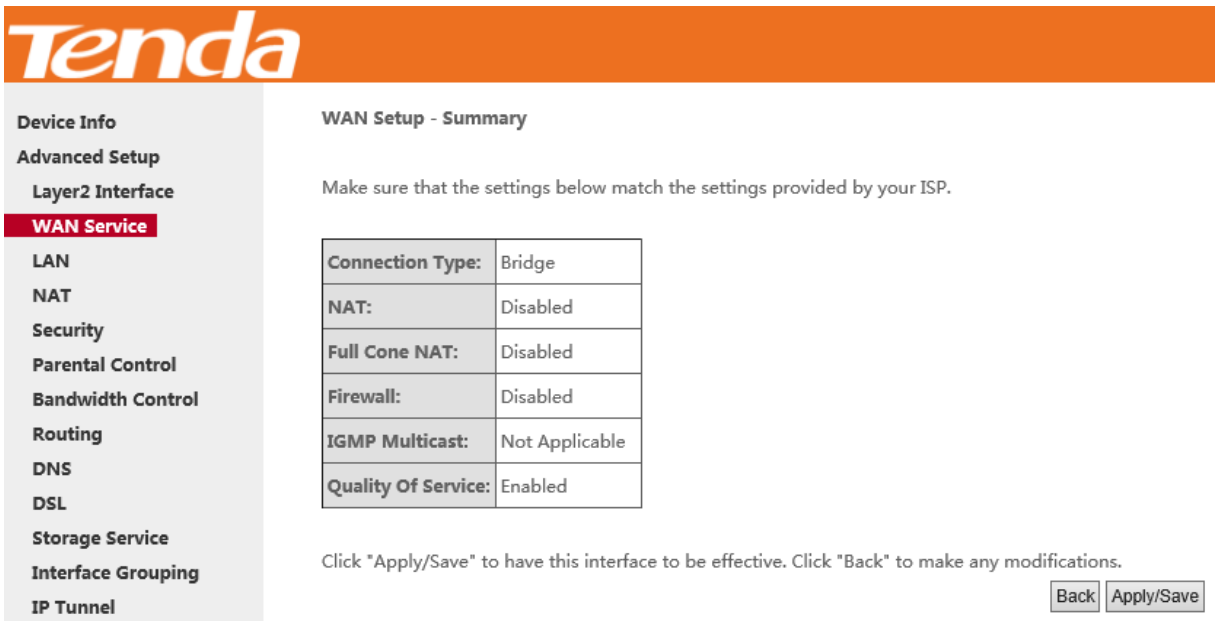
Step 1: Click **Advanced Setup > WAN Service** and then click the **Add** button.

Step 2: Select the ATM interface you added just now from the pull-down menu in the figure below. Click **Next**.

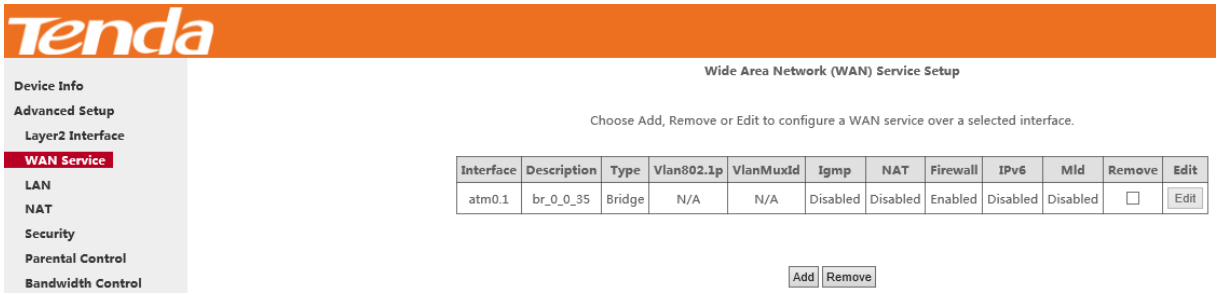
Step 3: Select **Bridging**. Edit the **Enter Service Description** which is optional. Suggest you keep the default. Click **Next**.



Step 4: Here you can view your configurations. Click **Apply/Save** to activate your settings..



After the bridging connection is successful, initiate a dialup directly from your PC for Internet access.



NOTE

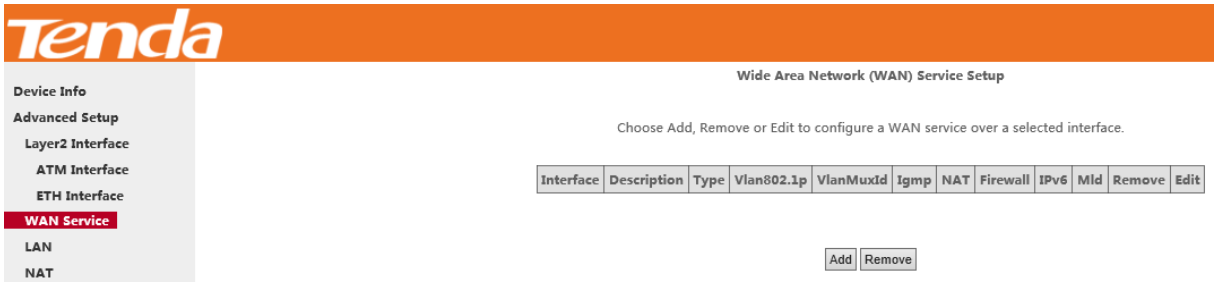
To configure multiple WAN connections, simply configure multiple ATM interfaces and then follow the instructions above.

- **PPPoA**

If you have selected the **PPPoA** from the **ATM Interface** screen in **Layer2 Interface**, you will see the screen below when you click the **WAN Service** tab, select the configured interface and click **Next**.

IPv4 Only

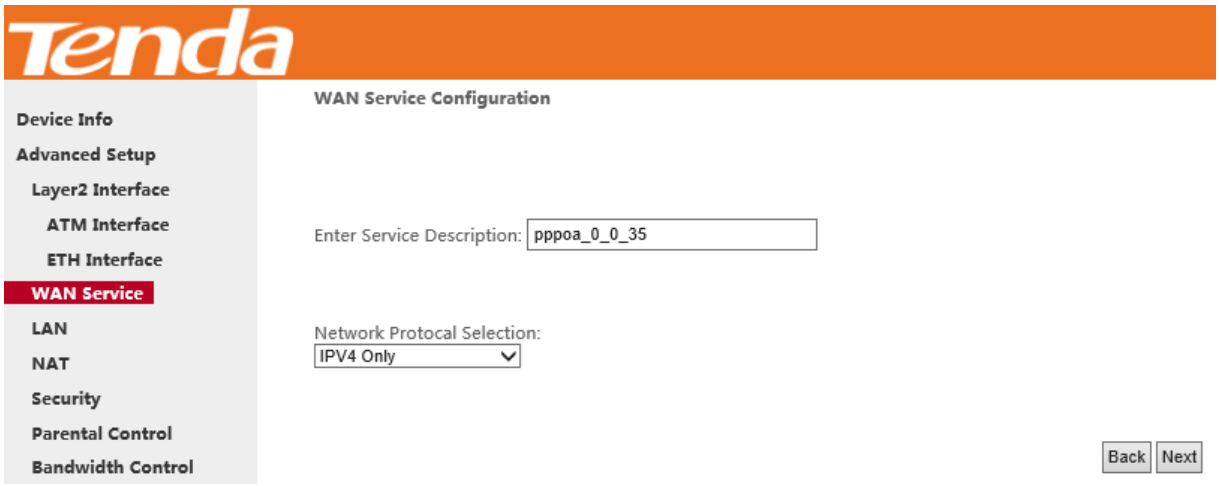
Step 1: Click **Advanced Setup** > **WAN Service** and then click the **Add** button.



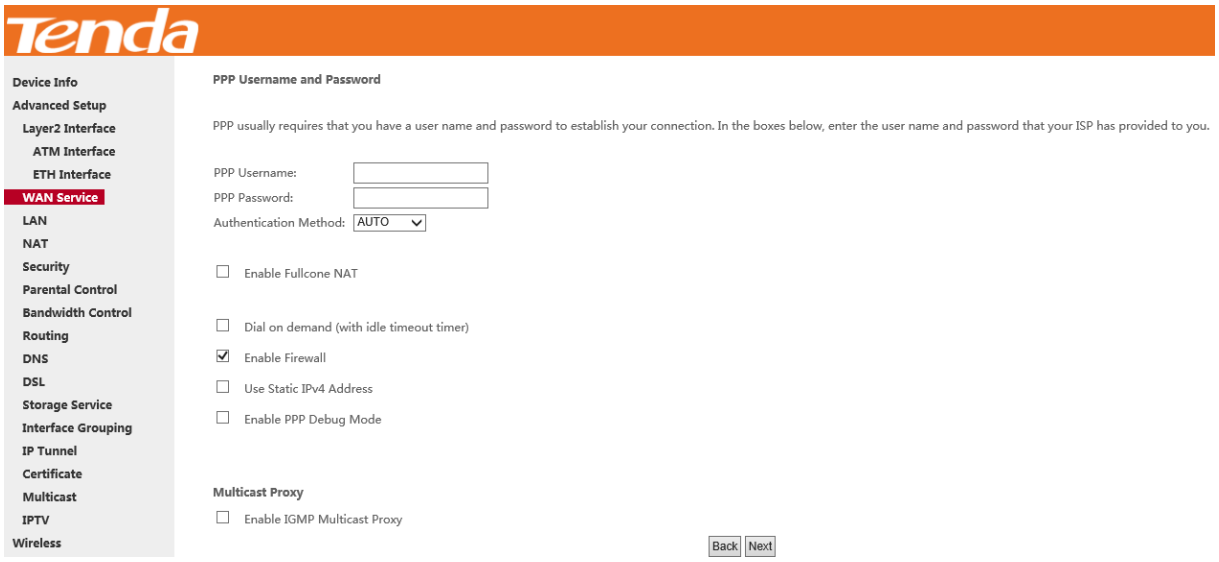
Step 2: Select the ATM interface you added just now from the pull-down menu in the figure below. Click **Next**.

Step 3: Edit the **Enter Service Description.** This field is optional. We recommend that you keep the default.

Select a network protocol: **IPv4 Only** and click **Next**.



Step 4: Enter PPP username and its password provided by your ISP. Click **Next**.



PPP Username: This is for logging in to your ISP. If you cannot locate this information, ask your ISP to provide it.

PPP Password: This is for logging in to your ISP. If you cannot locate this information, ask your ISP to provide it.

Authentication Method: This is used by ISP to authenticate the client that attempts to connect. If you are not sure, consult your ISP or select **AUTO**.

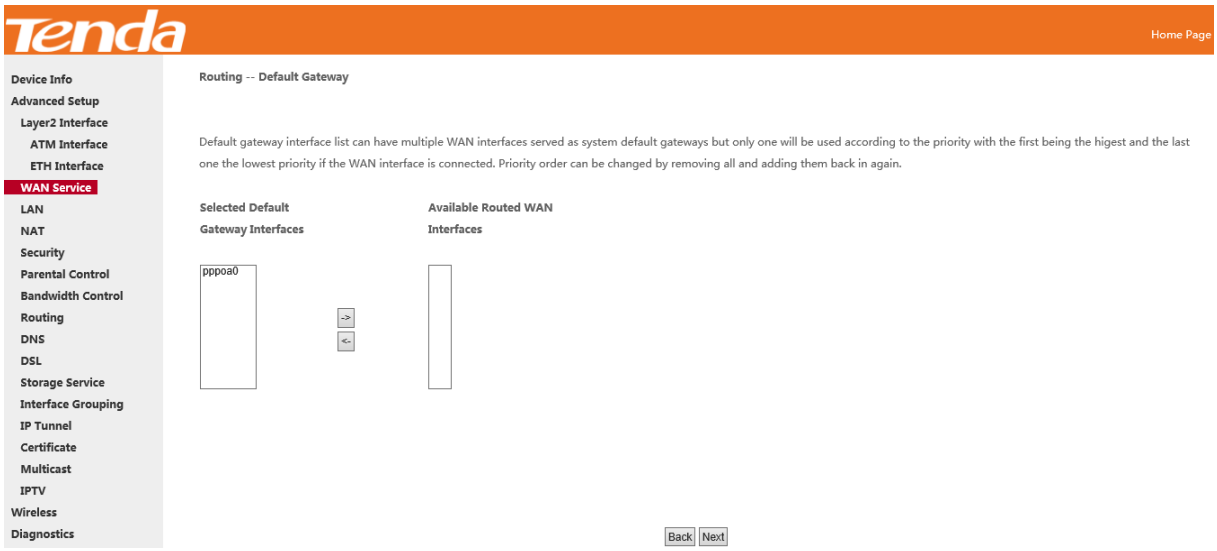
Dial on demand: Connect to ISP only when there is traffic transmission. This saves your broadband Internet service bill.

Enable PPP Debug Mode: Only enable this feature if supported by your ISP.

Multicast Proxy: If enabled, the router will use multicast proxy.

If you are not sure about the options on this screen, simply enter your ISP user name and password and leave the other options unchanged from defaults. Click **Next** to enter the following screen.

Step 5: To configure the WAN gateway address. After you configure it click **Next**. The default setting is recommended.

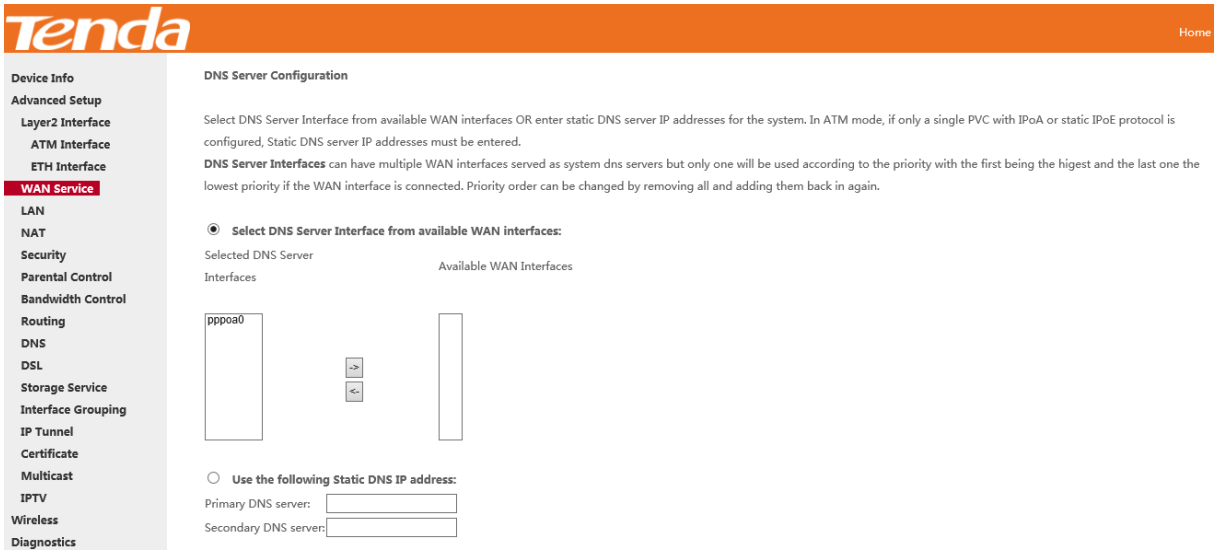


Step 6: To configure the WAN DNS address. Choose a way to get DNS server according to what your ISP has provided.

-Click the Select DNS Server Interface from available WAN interfaces option.

-Select the **Use the following Static DNS IP address** option and enter static DNS server IP addresses for the system.

And then click **Next**.

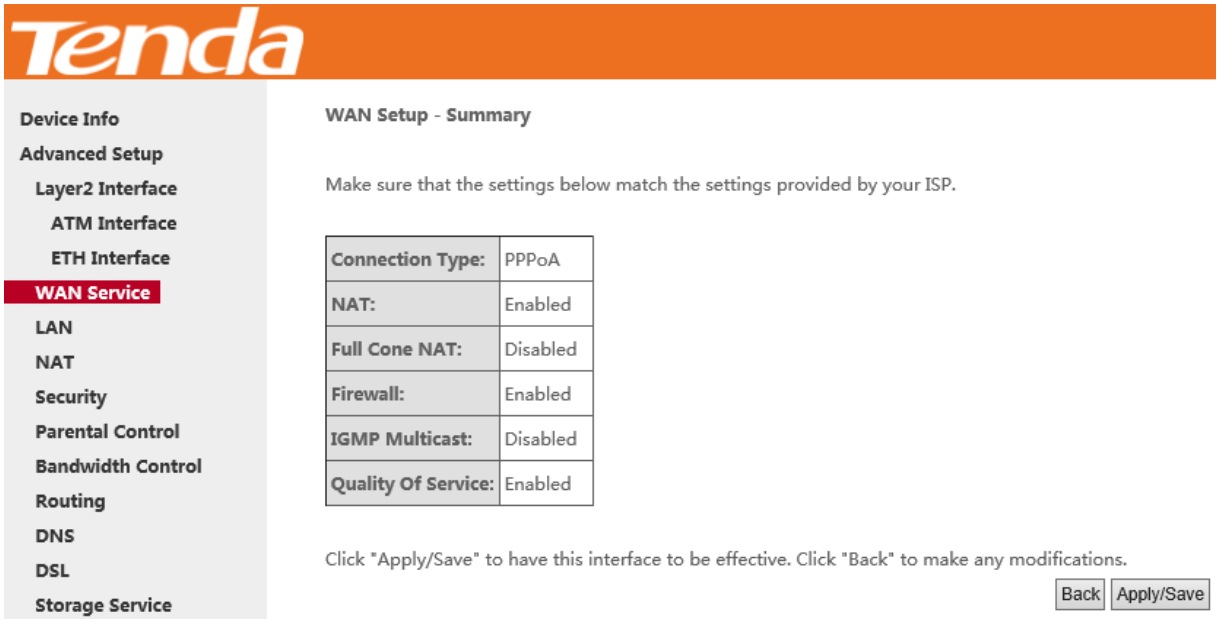


NOTE

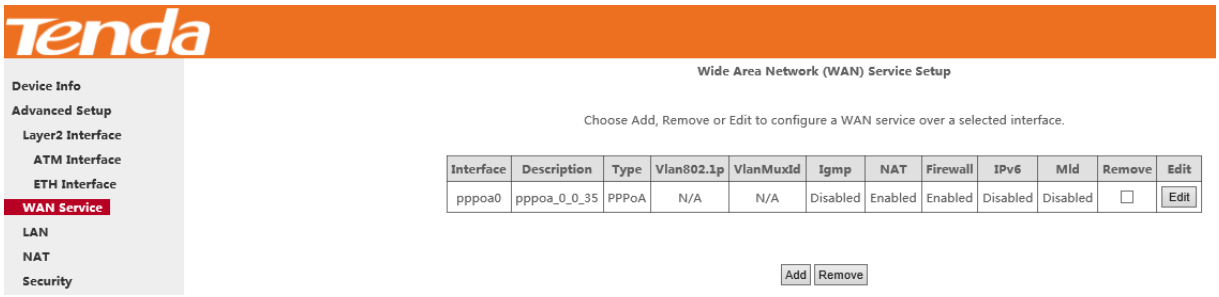
1. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

2. If you cannot locate the static DNS server IP information, ask your ISP to provide it.

Step 7: Here you can view your configurations. Click **Apply/Save** to have this interface to be effective.



Step 8: When the PPPoA connection is successful, you can access the Internet.



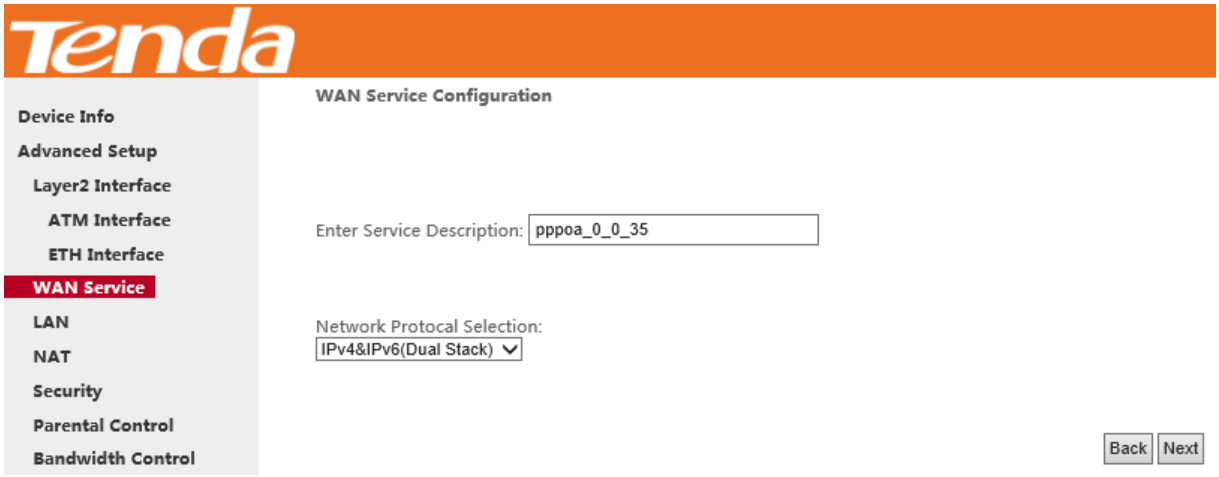
IPv4 & IPv6 (Dual Stack)

Step 1: Click **Advanced Setup** > **WAN Service** and then click the **Add** button.

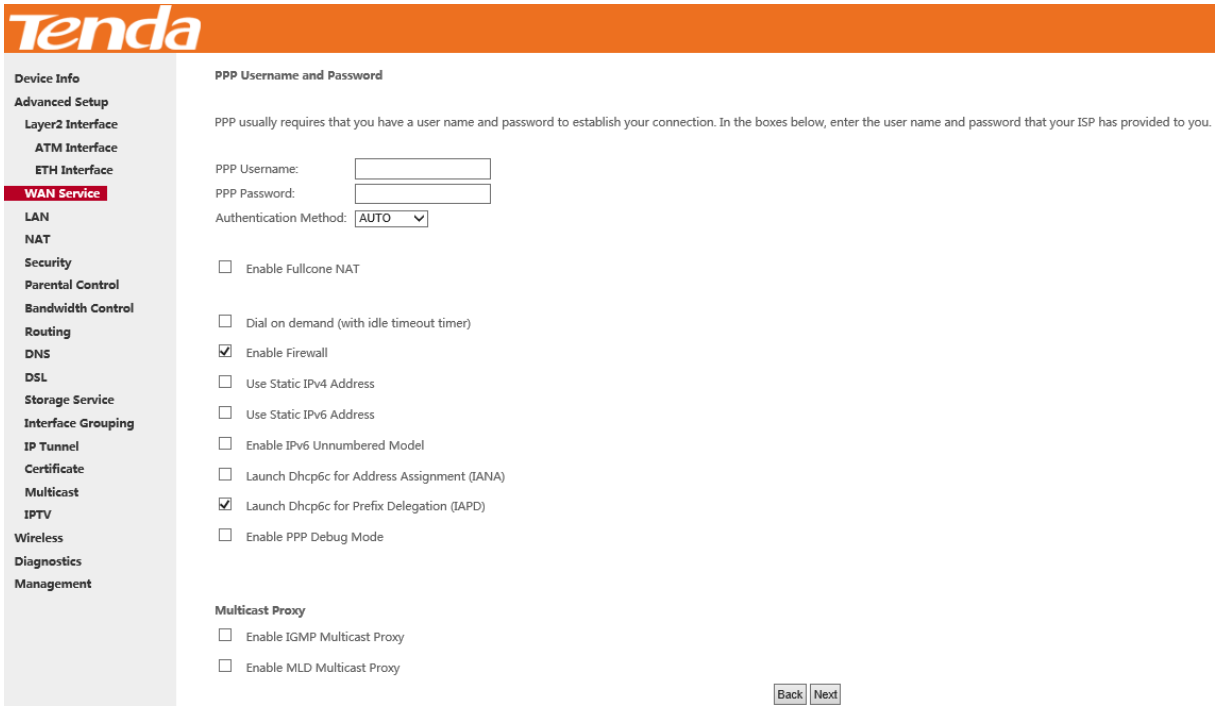
Step 2: Select the ATM interface you added just now from the pull-down menu in the figure below. Click **Next**.

Step 3: Edit the **Enter Service Description.** This field is optional. We recommend that you keep the default.

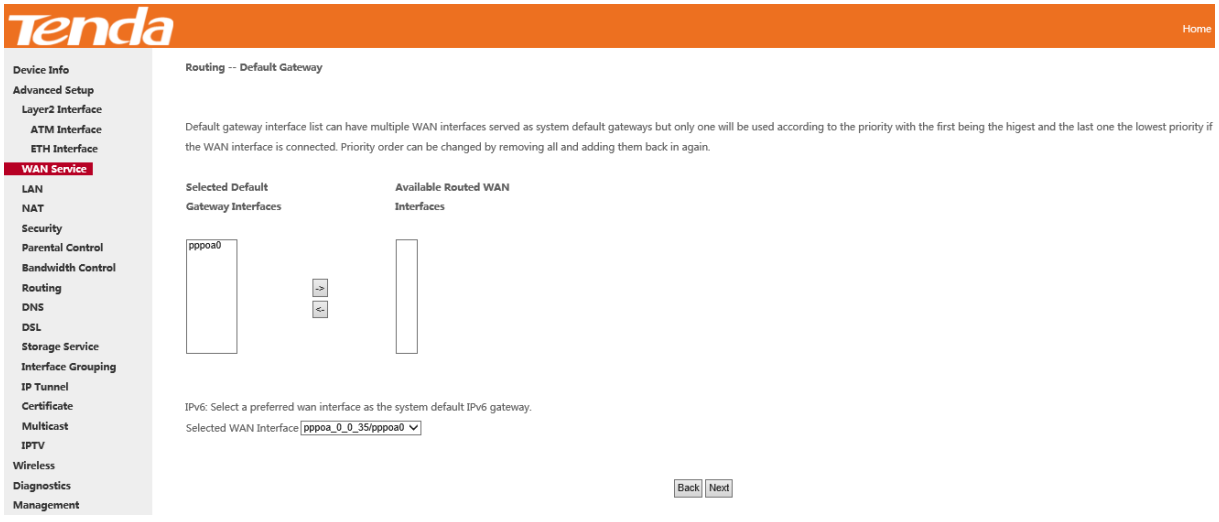
Select a network protocol: **IPv4 & IPv6 (Dual Stack)**. Click **Next**.



Step 4: Enter PPP username and its password provided by your ISP. Click **Next**.



Step 5: To configure the WAN gateway address. After you configure it click **Next**. The default setting is recommended.

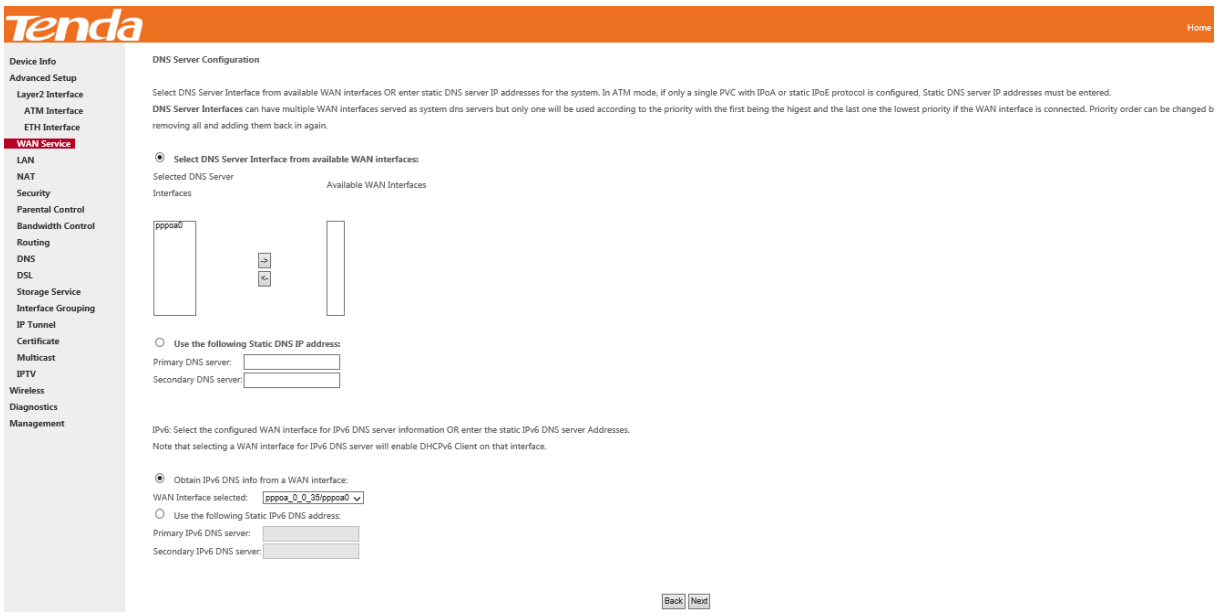


NOTE

Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Step 6: To configure the WAN DNS address

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. And then click **Next**.



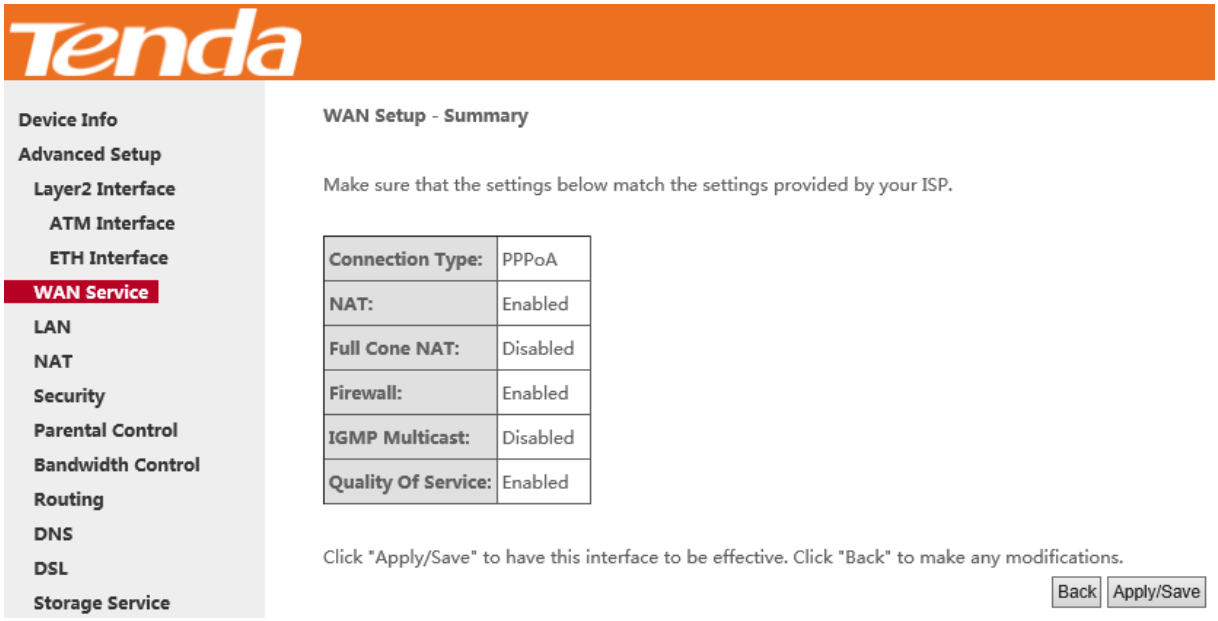
NOTE

1. DNS Server Interfaces can have multiple WAN interfaces served as system DNS servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

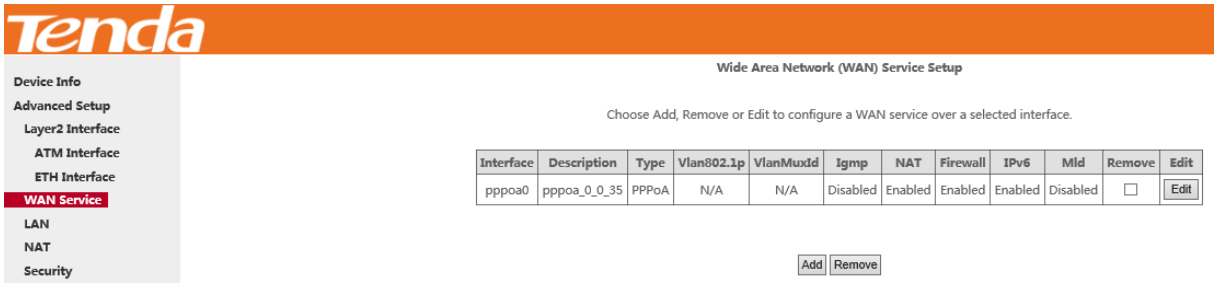
2. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

3. If you cannot locate the static DNS server IP information, ask your ISP to provide it.

Step 7: Here you can view your configurations. Click **Apply/Save** to save your settings if everything is correctly set.

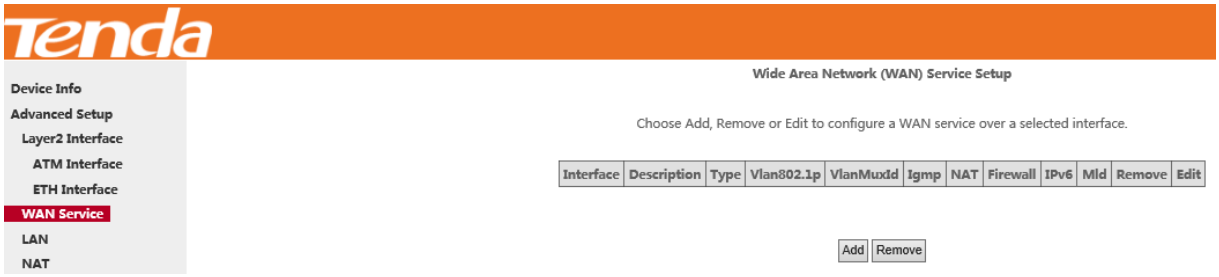


Step 8: When the PPPoA connection is successful, you can access the Internet.



IPv6 Only

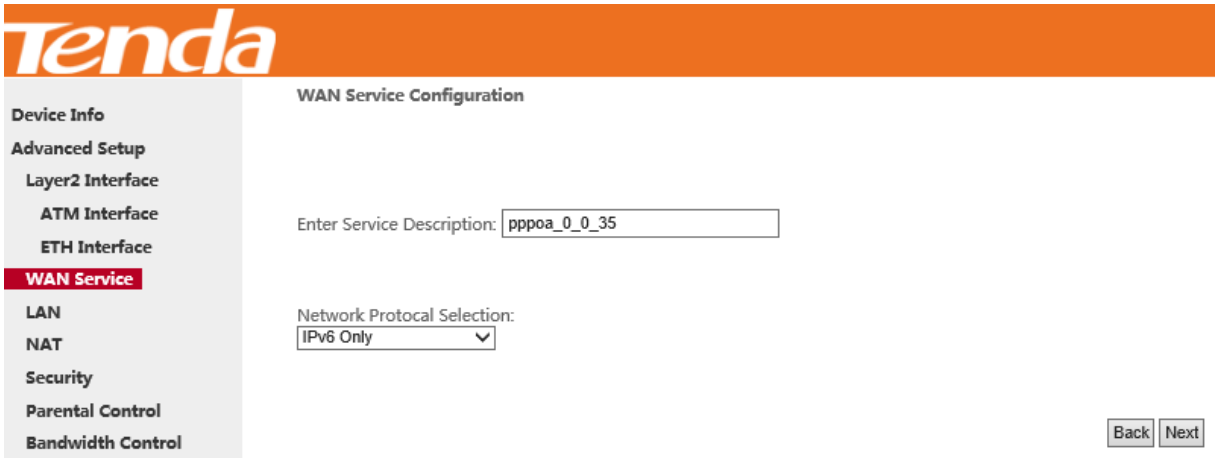
Step 1: Click **Advanced Setup** > **WAN Service** and then click the **Add** button.



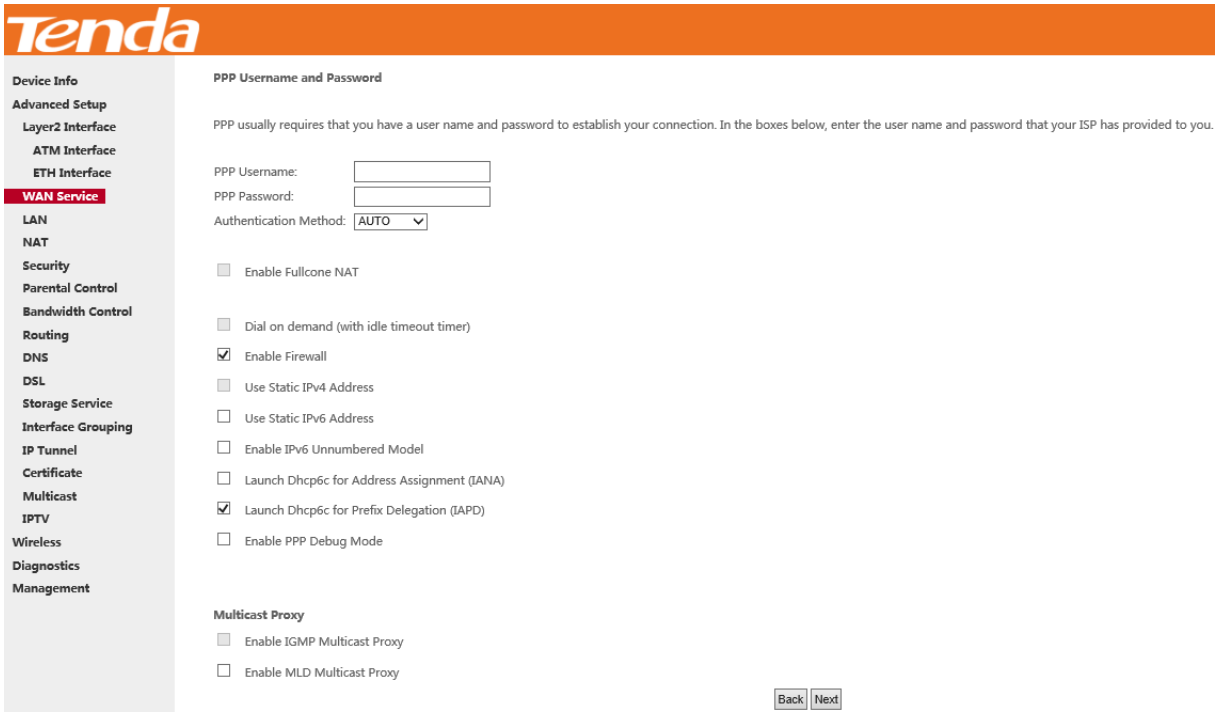
Step 2: Select the ATM interface you added just now from the pull-down menu in the figure below. Click **Next**.

Step 3: Edit the **Enter Service Description.** This field is optional. We recommend that you keep the default.

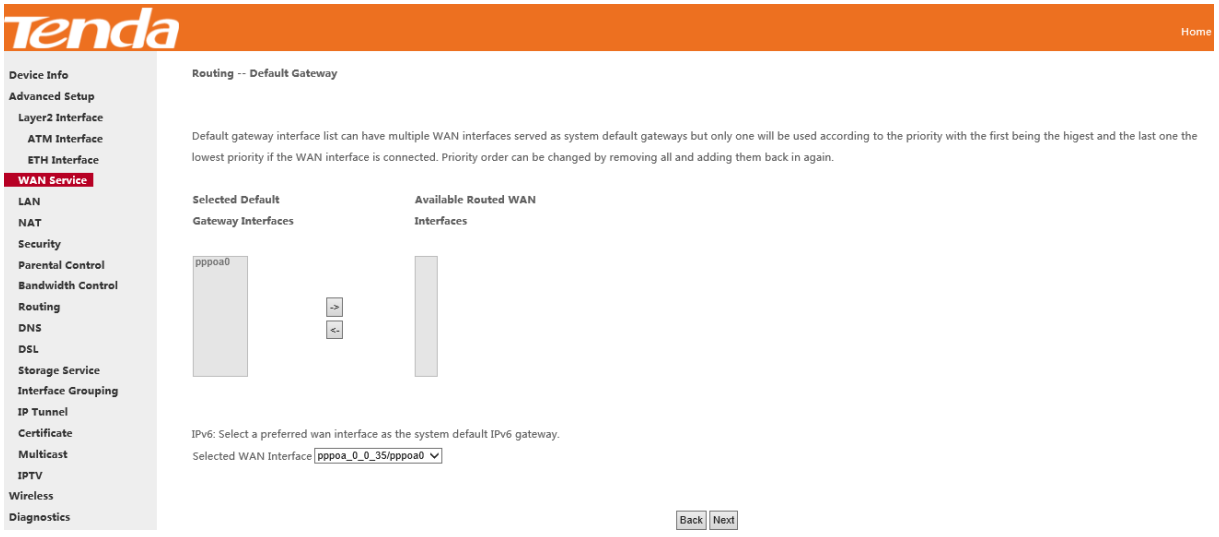
Select a network protocol: **IPv6 Only**. Click **Next**.



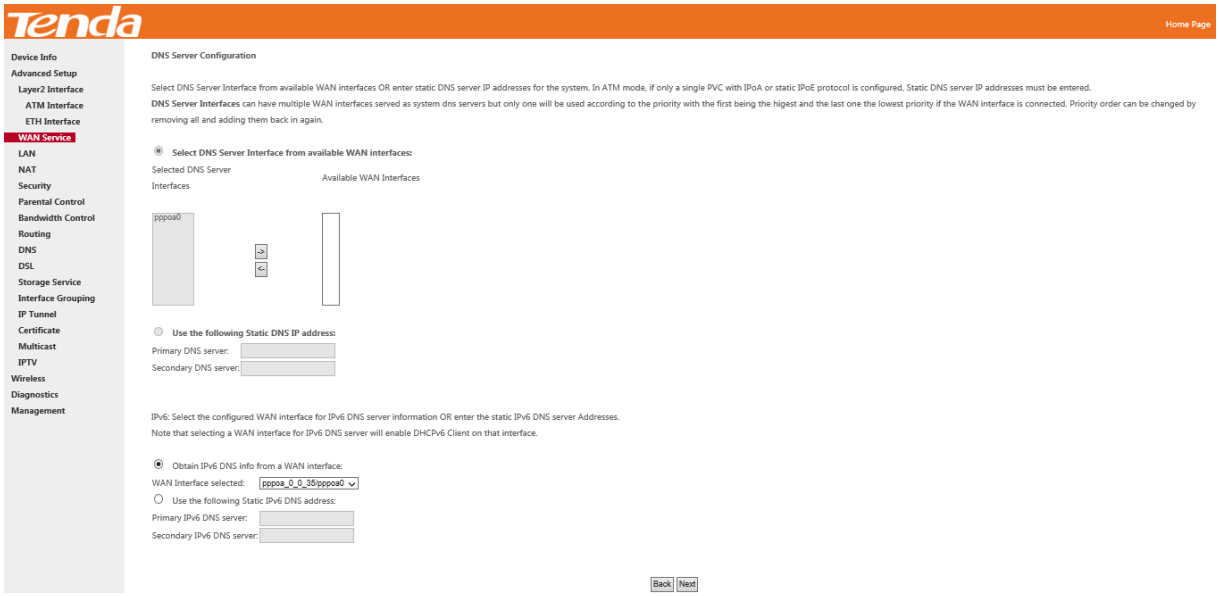
Step 4: Enter PPP username and its password provided by your ISP. Click **Next**.



Step 5: Select a preferred wan interface as the system default IPv6 gateway. Click **Next**.



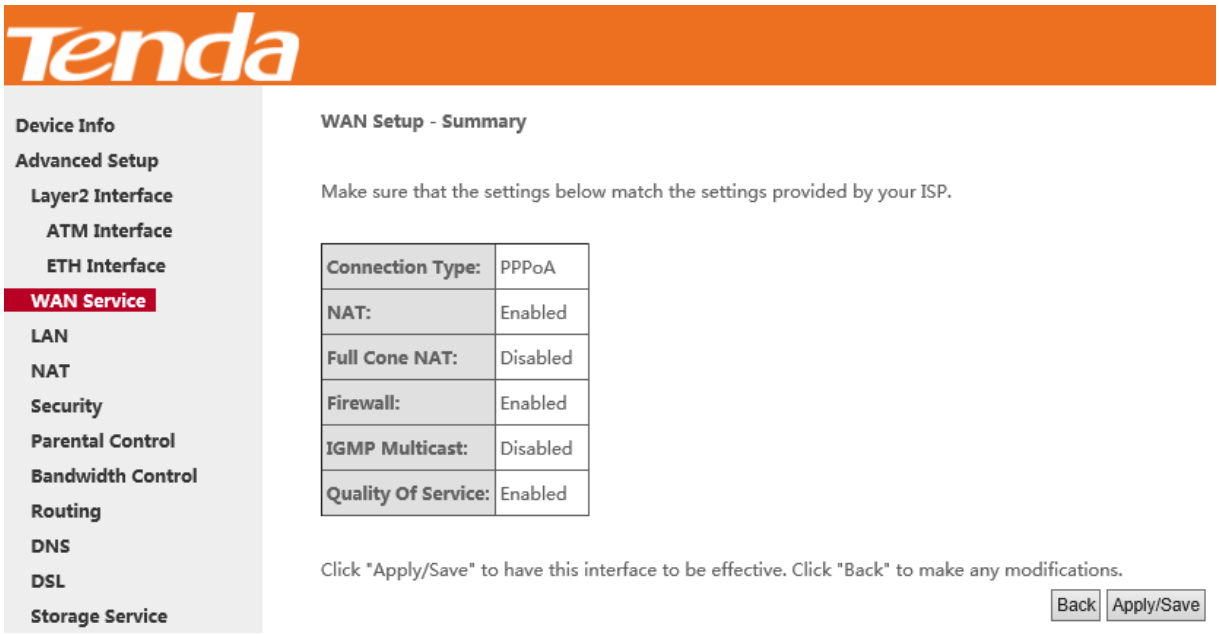
Step 6: To configure the WAN DNS address, select the configured WAN interface for IPv6 DNS server information or enter the static IPv6 DNS server addresses. And then click **Next**.



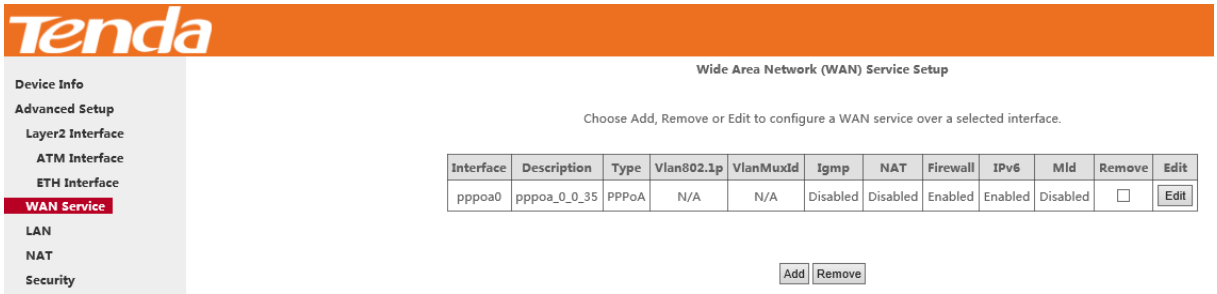
NOTE

Selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Client on that interface.

Step 7: Here you can view your configurations. Click **Apply/Save** to save your settings if everything is correctly set.

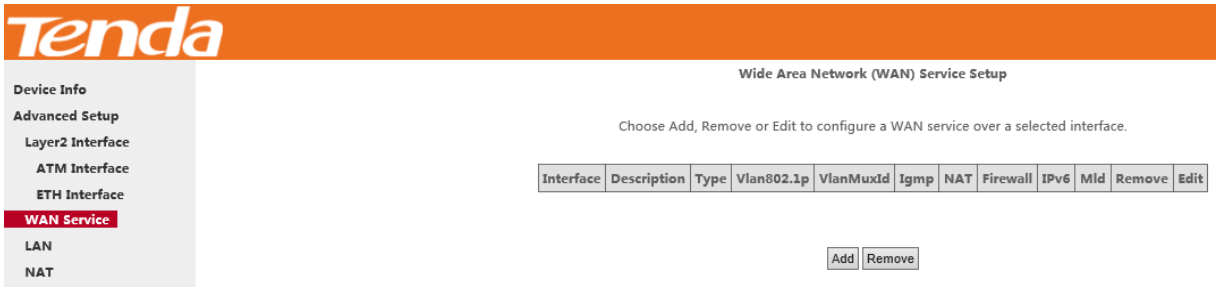


Step 8: When the PPPoA connection is successful, you can access the Internet.



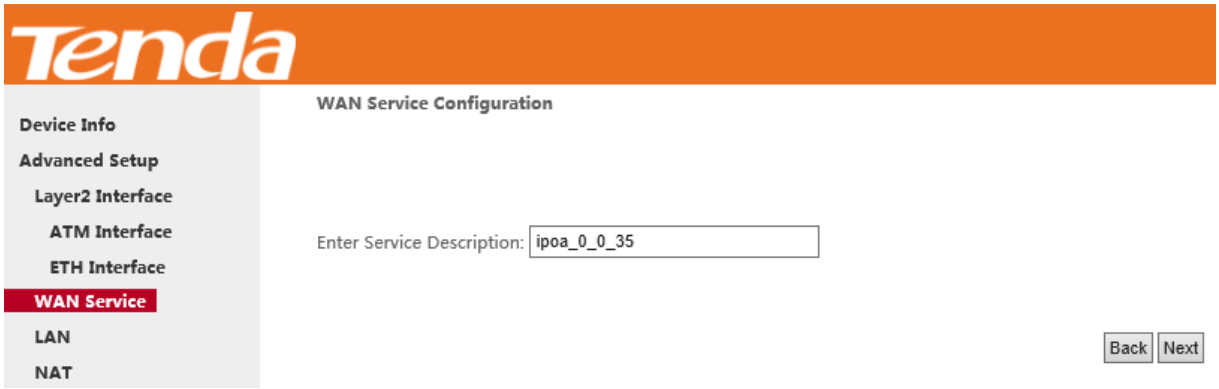
- **IPoA**

Step 1: Click **Advanced Setup** > **WAN Service** and then click the **Add** button.



Step 2: Select the ATM interface you added just now from the pull-down menu in the figure below. Click **Next**.

Step 3: Edit the Enter Service Description. This field is optional. It is recommended that you keep the default. Click **Next**.

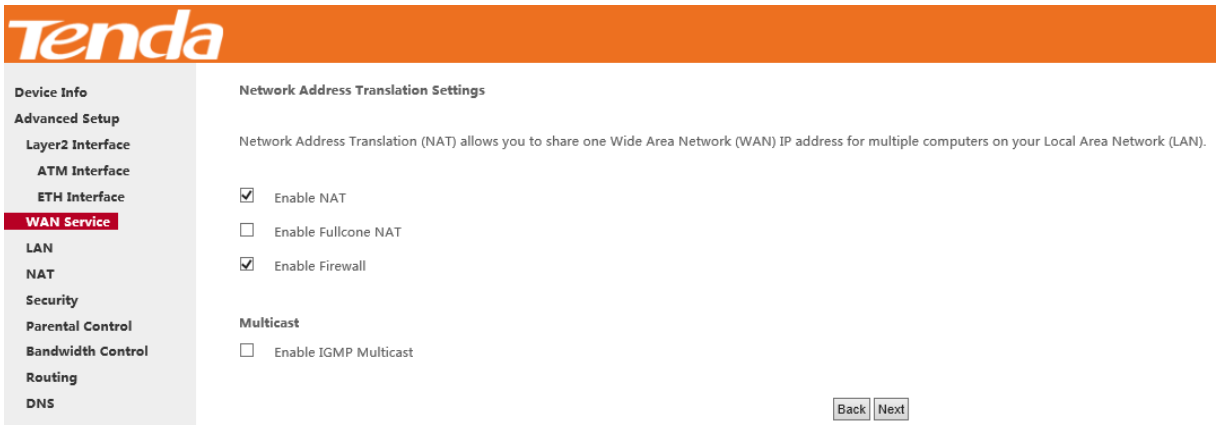


Step 4: Enter the WAN IP address and subnet mask which should have been provided to you by your ISP. If you cannot locate this information, ask your ISP to provide it. And then click **Next**.

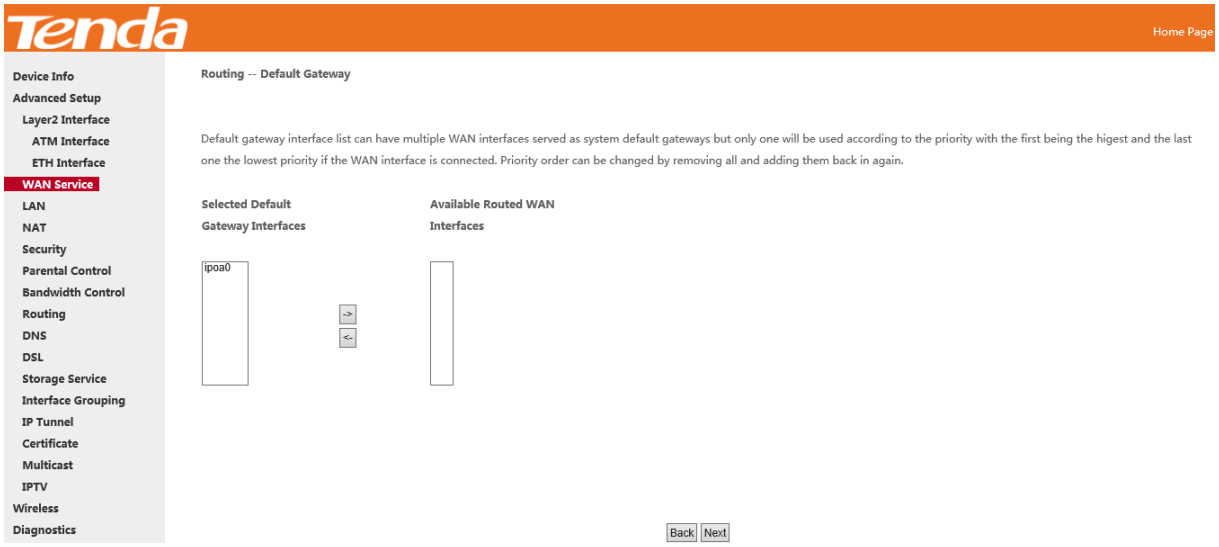
WAN IP Address: The Internet IP address provided by your ISP for accessing the Internet.

WAN Subnet Mask: The subnet mask address provided by your ISP for accessing the Internet.

Step 5: Keep the defaults if you are unsure about the options on the screen below and click **Next**.



Step 6: To configure the WAN gateway address. After you configure it click **Next**. The default setting is recommended.



NOTE

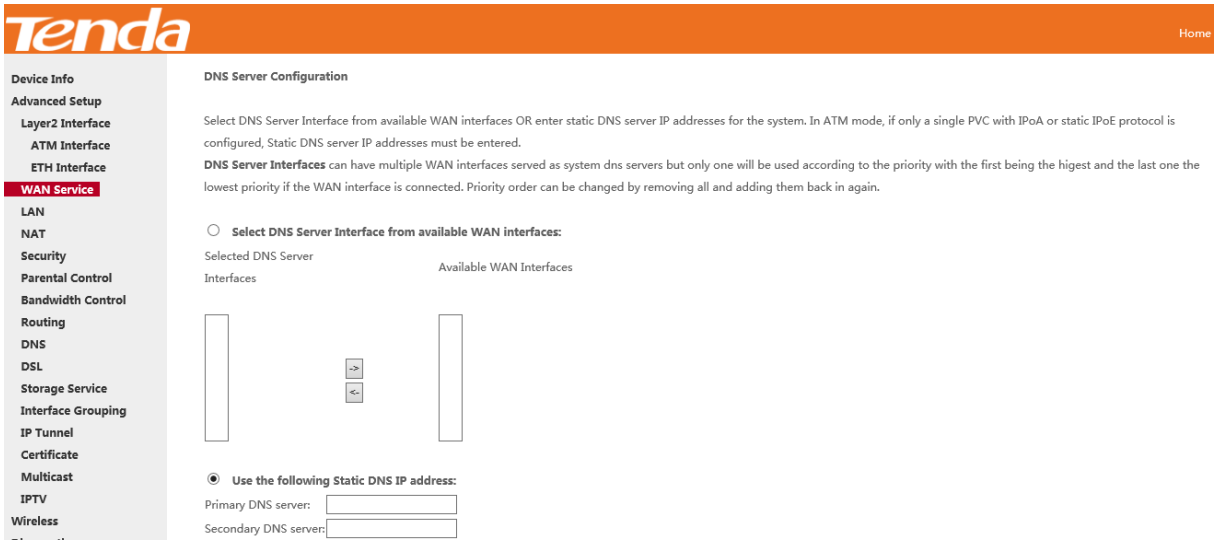
Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Step 7: Configure the WAN DNS Server configuration according to your ISP.

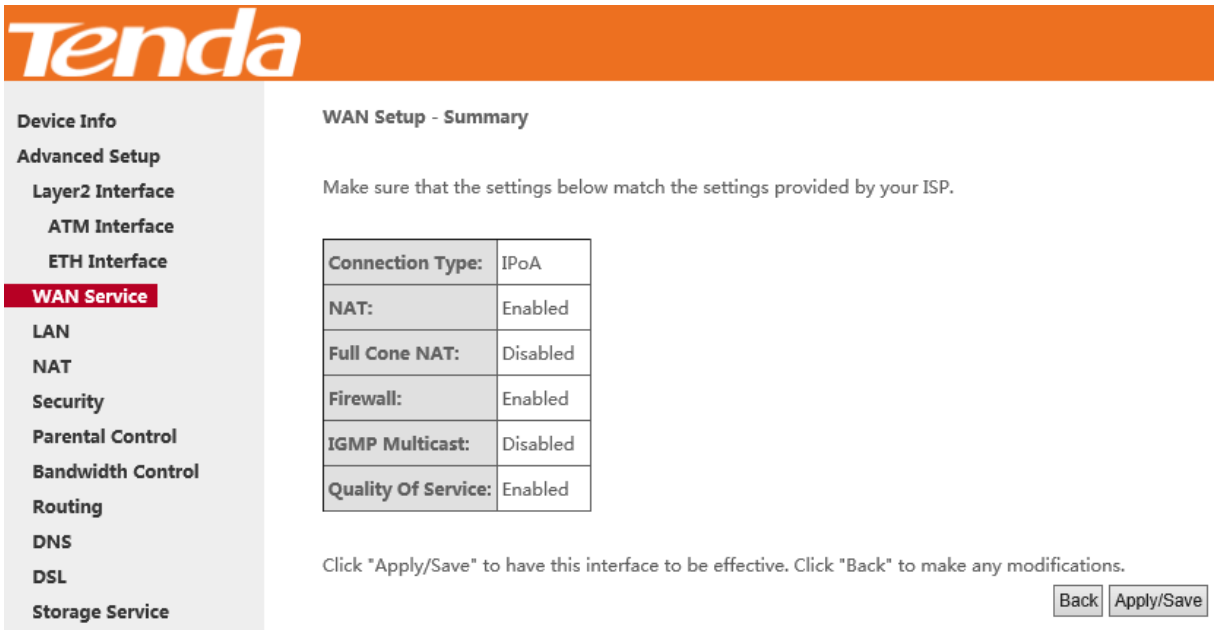
-Click the **Select DNS Server Interface** from available WAN interfaces option;

-Or select the **Use the following Static DNS IP address** option and enter static DNS server IP addresses for the system.

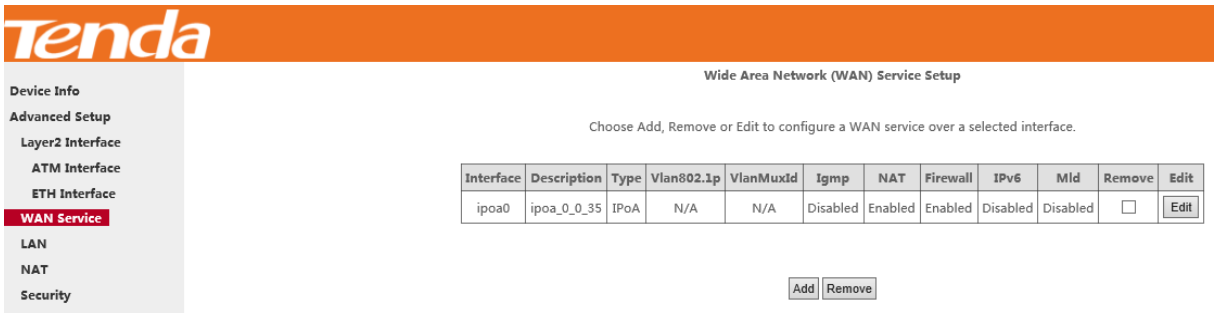
And then click **Next**.



Step 8: Here you can view your configurations. Click **Apply/Save** to save your settings if everything is correctly set.



Step 9: IPoA WAN service setup parameter is shown as below.



To Set up WAN Service for ETH Interface

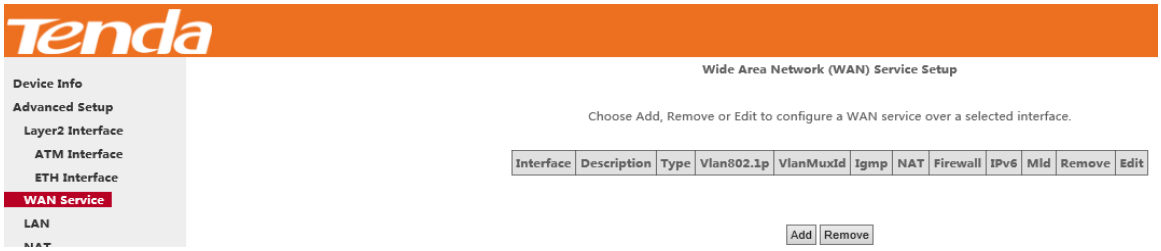
Three Internet connections: PPP over Ethernet (PPPoE), IP over Ethernet (IPoE) and Bridging are available in the Ethernet uplink mode.

If you selected and configured the **ETH Interface** (Ethernet uplink), follow steps below to configure the WAN service:

- **PPP over Ethernet (PPPoE)**

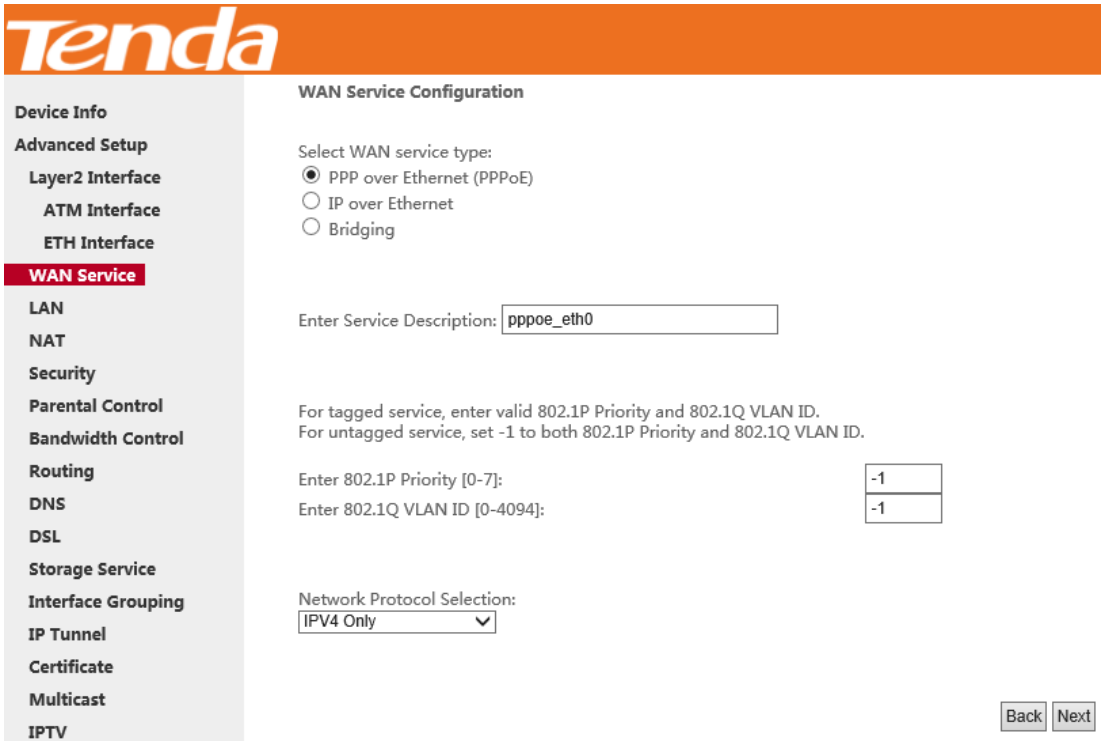
IPv4

Step 1: Click **Advanced Setup** > **WAN Service** and then click the **Add** button.

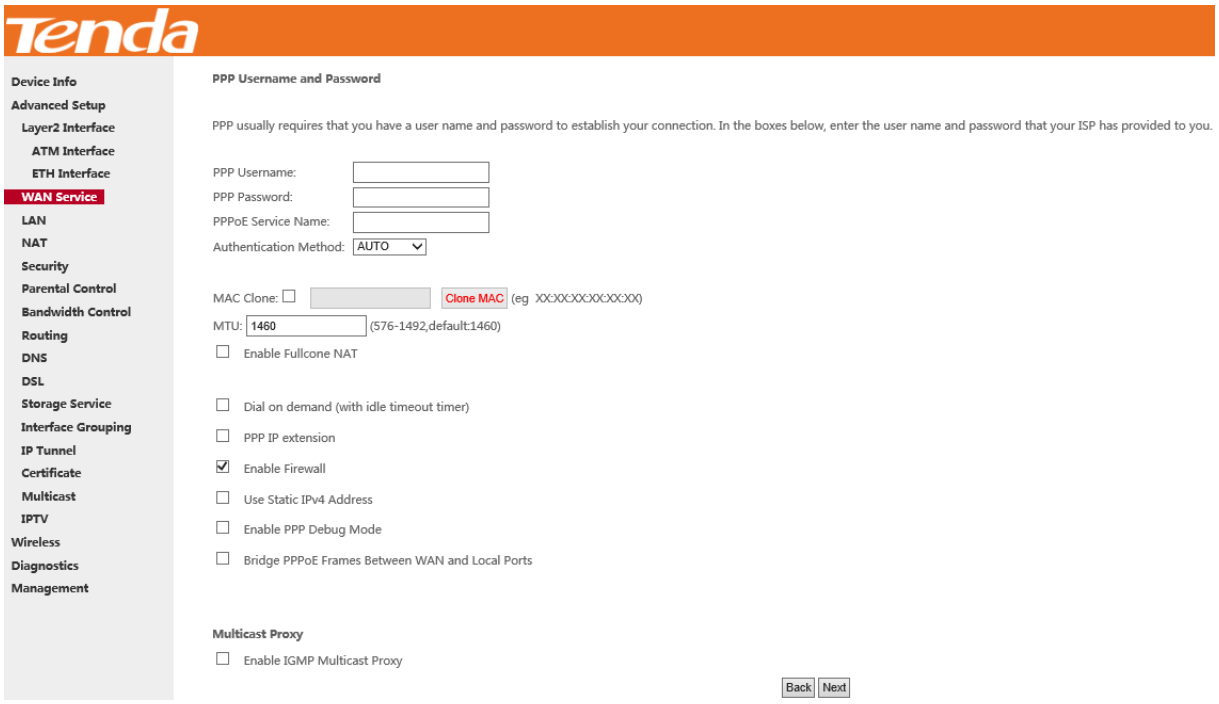


Step 2: Select the ETH interface you added just now from the pull-down menu in the figure below. Click **Next**.

Step 3: Select **PPP over Ethernet**. Edit the **Enter Service Description**. This field is optional. It is recommended that you keep the default. Select a network protocol: **IPv4 Only**. And click **Next**.



Step 4: Enter the PPP username and password provided by your ISP. If you are not sure about other options, just leave them unchanged from defaults. And click **Next**.



PPP Username: This is for logging in to your ISP. If you cannot locate this information, ask your ISP to provide it.

PPP Password: This is for logging in to your ISP. If you cannot locate this information, ask your ISP to provide it.

PPPoE Service Name: This information is provided by your ISP. Only enter it if instructed by your ISP.

Authentication Method: This is used by ISP to authenticate the client that attempts to connect. If you are not sure, consult your ISP or select **Auto**.

MAC Clone: Clicking **Clone MAC** button copies the MAC address of your PC to the router. Many broadband ISPs restrict access by allowing traffic only from the MAC address of your broadband modem, but some ISPs additionally register the MAC address of the network interface card in your computer when your account is first opened. They then accept traffic only from the MAC address of that computer. If so, configure your router to "clone" the MAC address from the authorized computer.

MTU: Short for ***Maximum Transmission Unit***, the largest physical packet size, measured in bytes, which a network can transmit. Any messages larger than the MTU are divided into smaller packets before being sent. The default MTU is 1460 bytes. For some ISPs, you might need to change the MTU. This is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.

Dial on demand: Connect to ISP only when there is traffic transmission. This saves your broadband Internet service bill.

PPP IP extension: If enabled, all the IP addresses in outgoing packets including management packets on the WAN port will be changed to the device's WAN IP address. Only change the default settings if necessary.

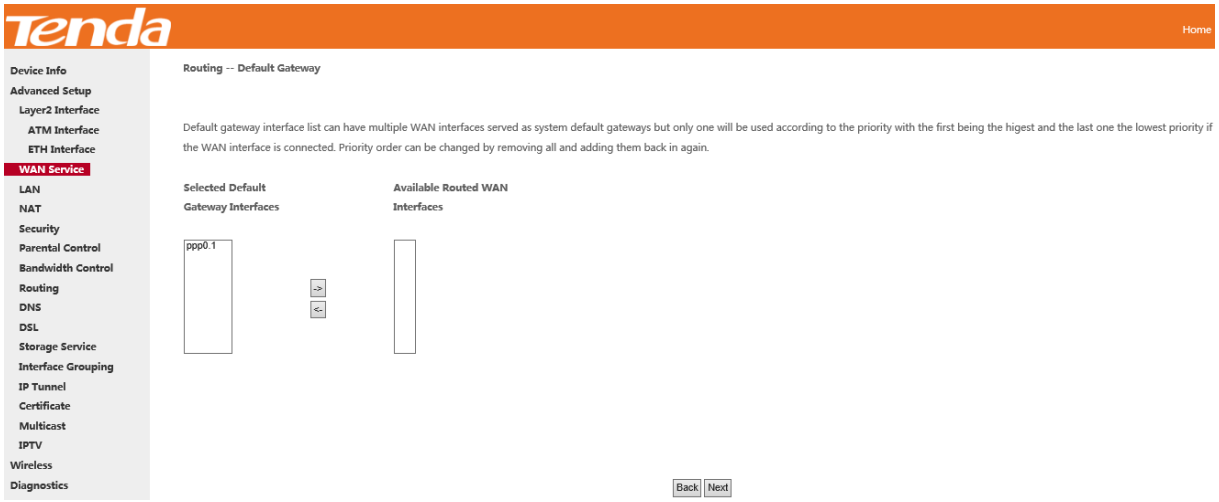
Enable PPP Debug Mode: Only enable this feature if supported by your ISP.

Bridge PPPoE Frames Between WAN and Local Ports: If enabled, PPPoE dialup frame from LAN side will directly

egress the WAN port without modification.

Multicast Proxy: If enabled, the router will use multicast proxy.

Step 5: Configure the WAN gateway address. After you configure it click **Next**. The default setting is recommended.



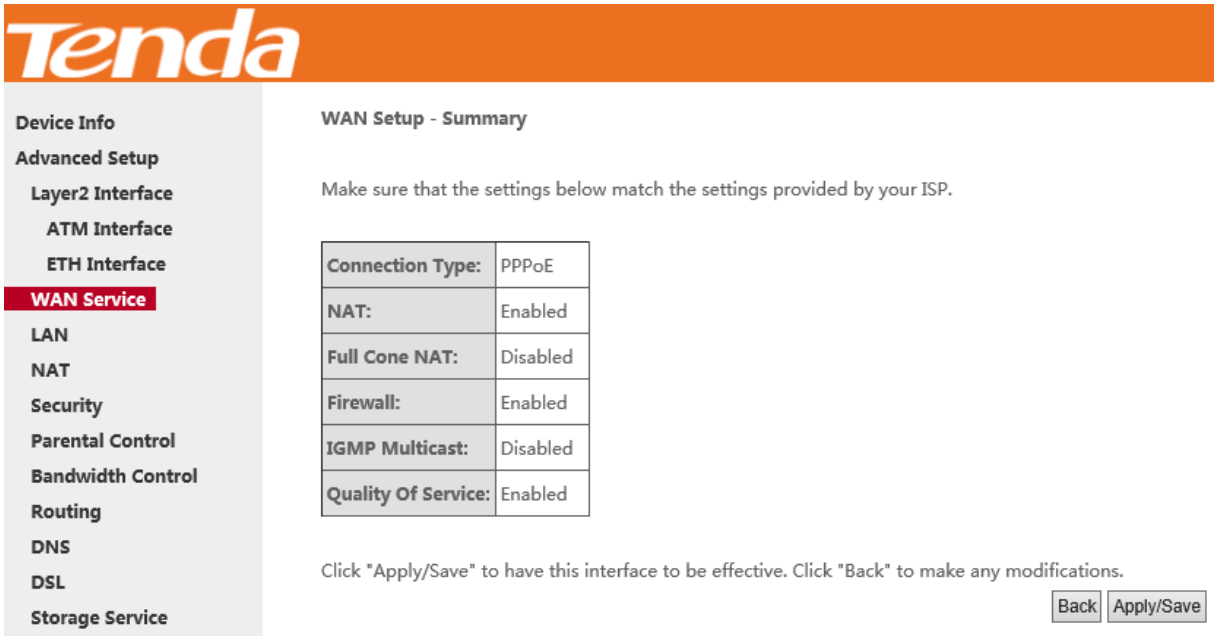
Step 6: Configure the WAN DNS address according to your ISP.

-Click the **Select DNS Server Interface** from available WAN interfaces option;

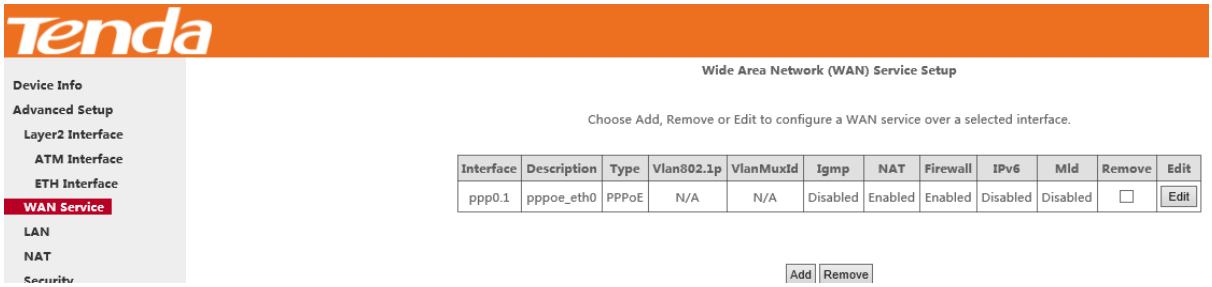
-Or select the **Use the following Static DNS IP address** option and enter static DNS server IP addresses for the system.

And then click **Next**.

Step 7: Here you can view your configurations. Click **Apply/Save** to save your settings if everything is correctly set.



When the PPPoE connection is successful, you can access the Internet.

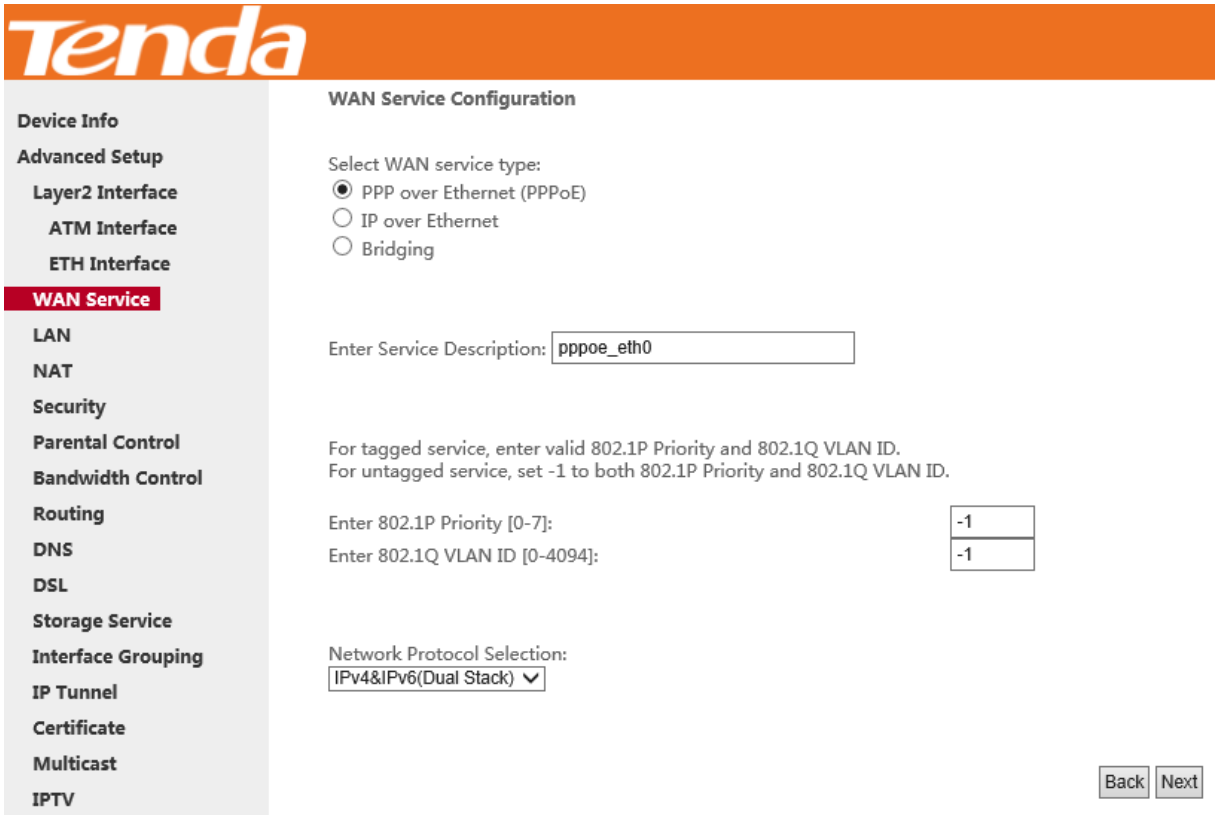


IPv4 & IPv6 (Dual Stack)

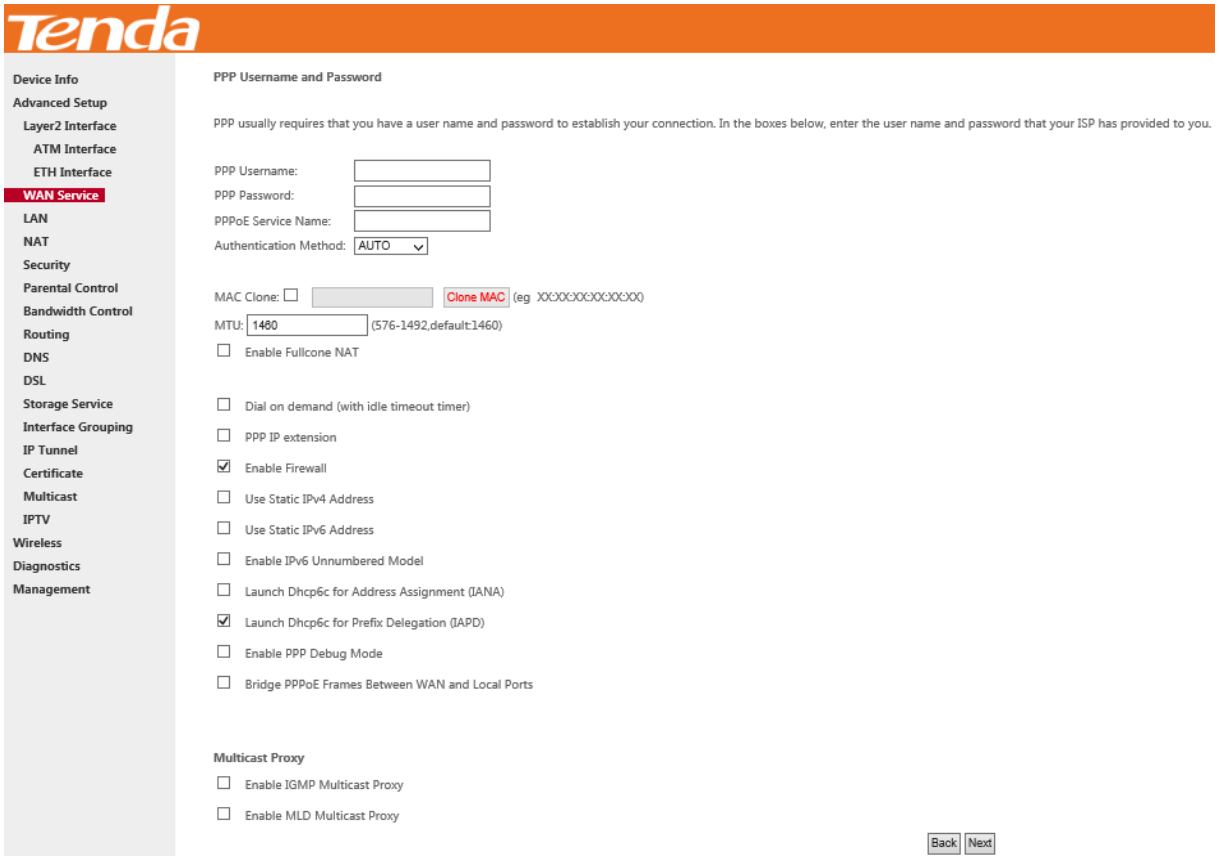
Step 1: Click **Advanced Setup** > **WAN Service** and then click the **Add** button.

Step 2: Select the ETH interface you added just now from the pull-down menu in the figure below. Click **Next**.

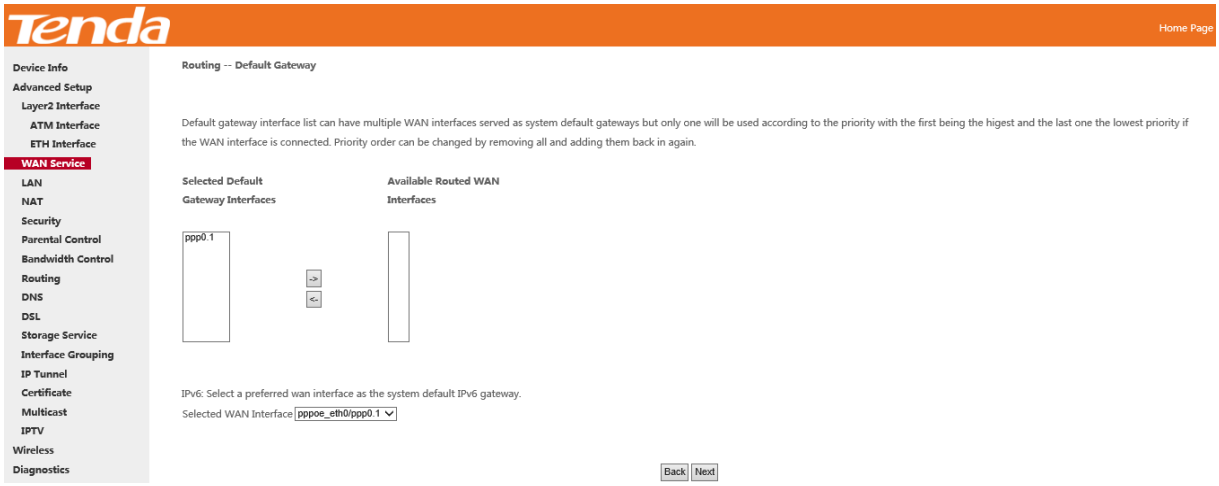
Step 3: Select **PPP over Ethernet**. Edit the **Enter Service Description**. This field is optional. It is recommended that you keep the default. Select a network protocol: **IPv4&IPv6 (Dual Stack)**. And click **Next**.



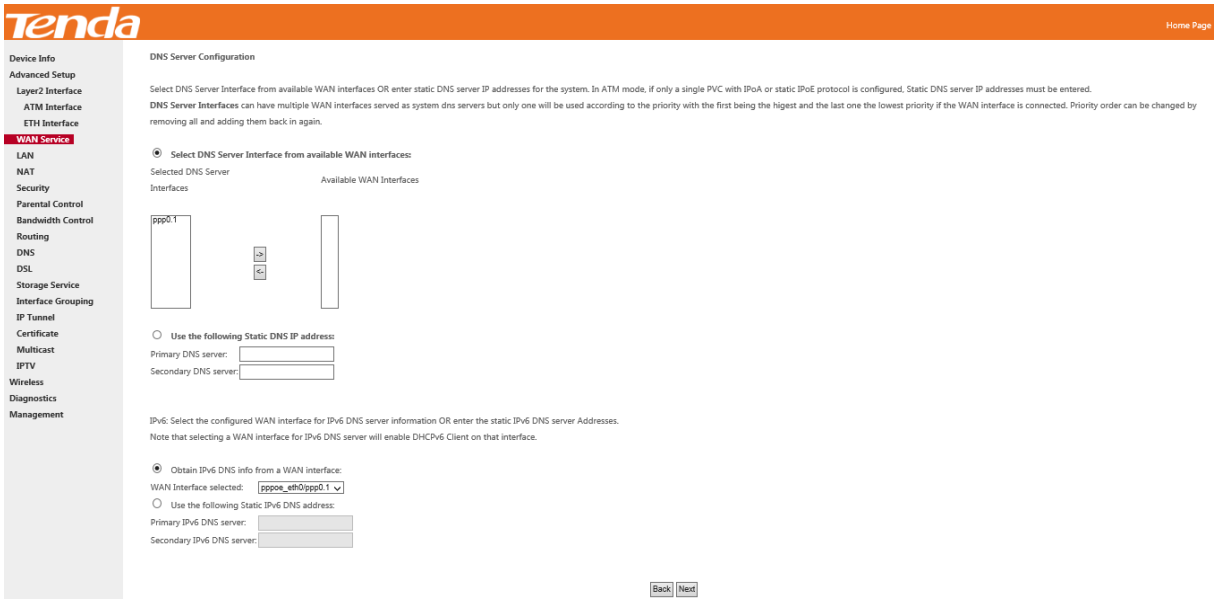
Step 4: Enter PPP username and PPP password provided by your ISP. Check **Launch Dhcp6c for Prefix Delegation (IAPD)**. If your ISP is using stateful DHCPv6, check **Launch Dhcp6c for Address Assignment (IANA)** also. Or configure a static IP address.



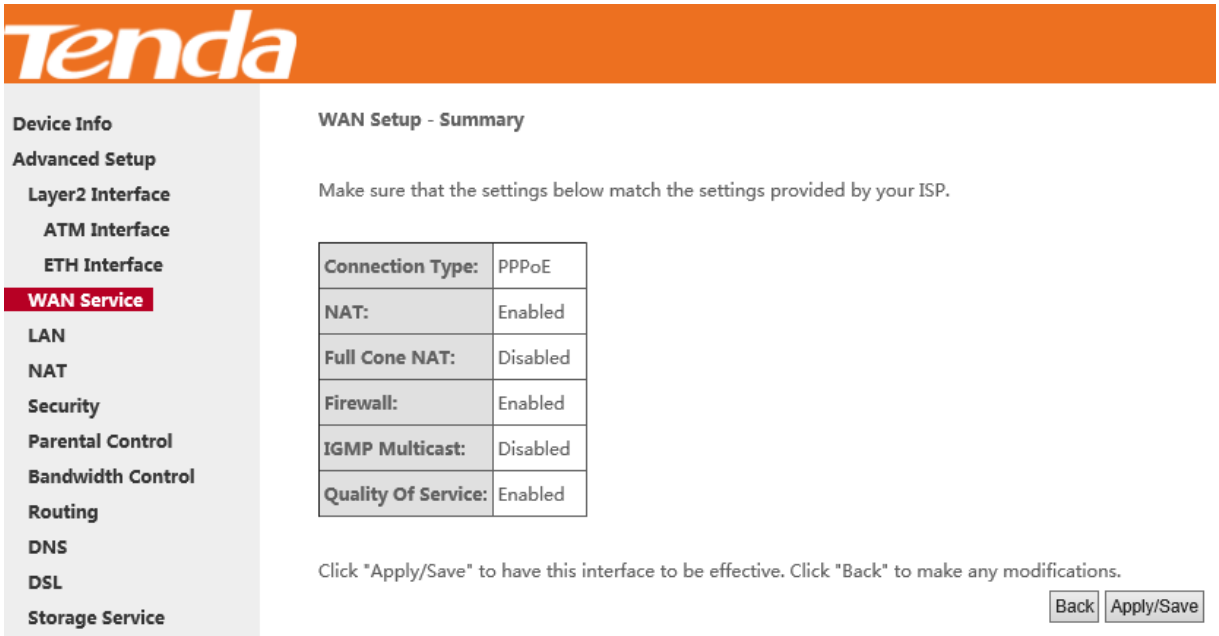
Step 5: Select an available WAN interface as the system default gateway. Then click **Next**.



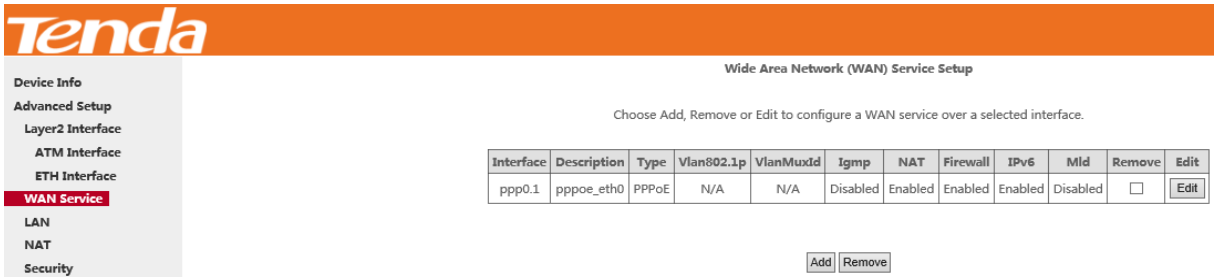
Step 6: Configure DNS server (Select an available DNS server interface or use a specified DNS server); configure IPv6 DNS server (Obtain IPv6 DNS info from a WAN interface or use a specified DNS server), and then click **Next**.



Step 7: Here you can view your configurations. Click **Apply/Save** to save your settings if everything is correctly set.

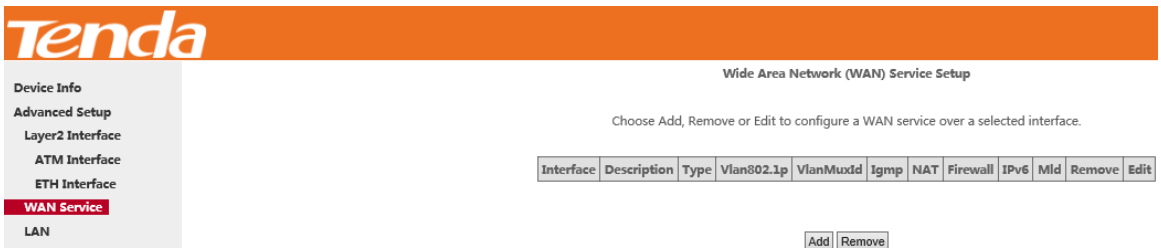


When the PPPoE connection is successful, you can access the Internet.



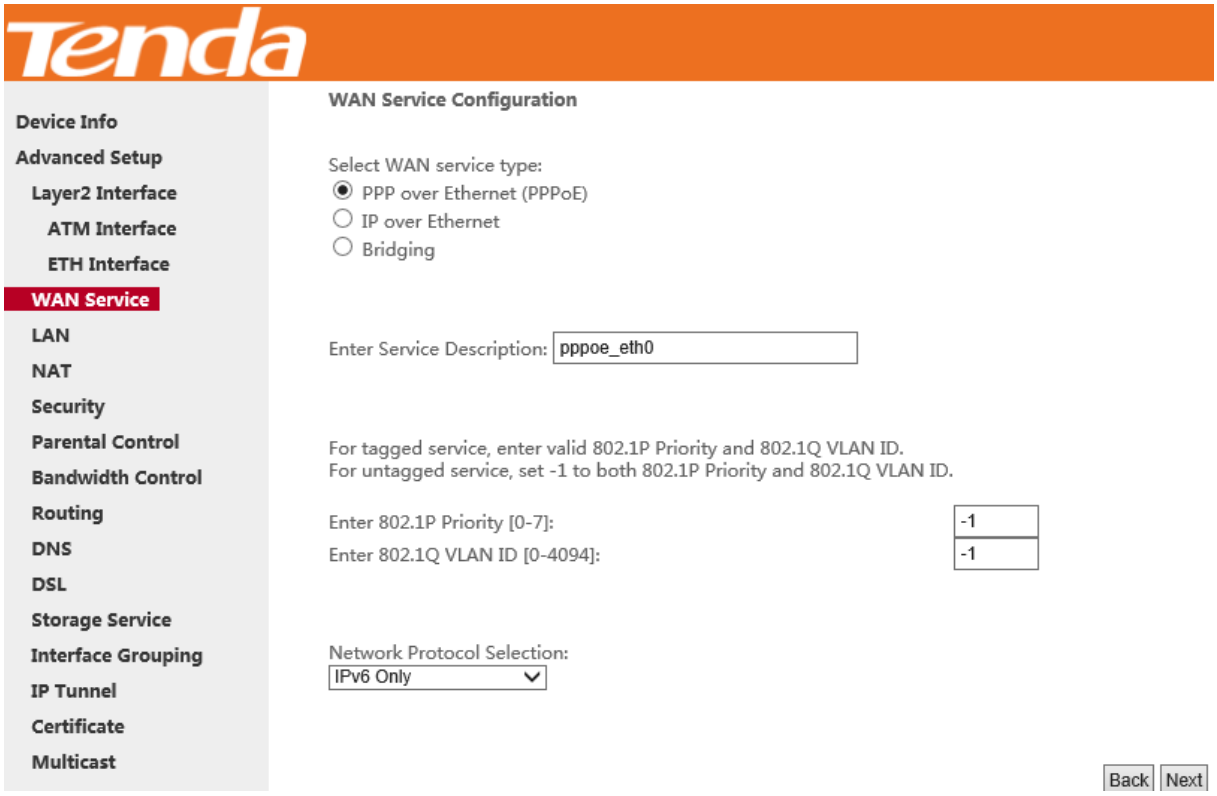
IPv6

Step 1: Click **Advanced Setup** > **WAN Service** and then click the **Add** button.

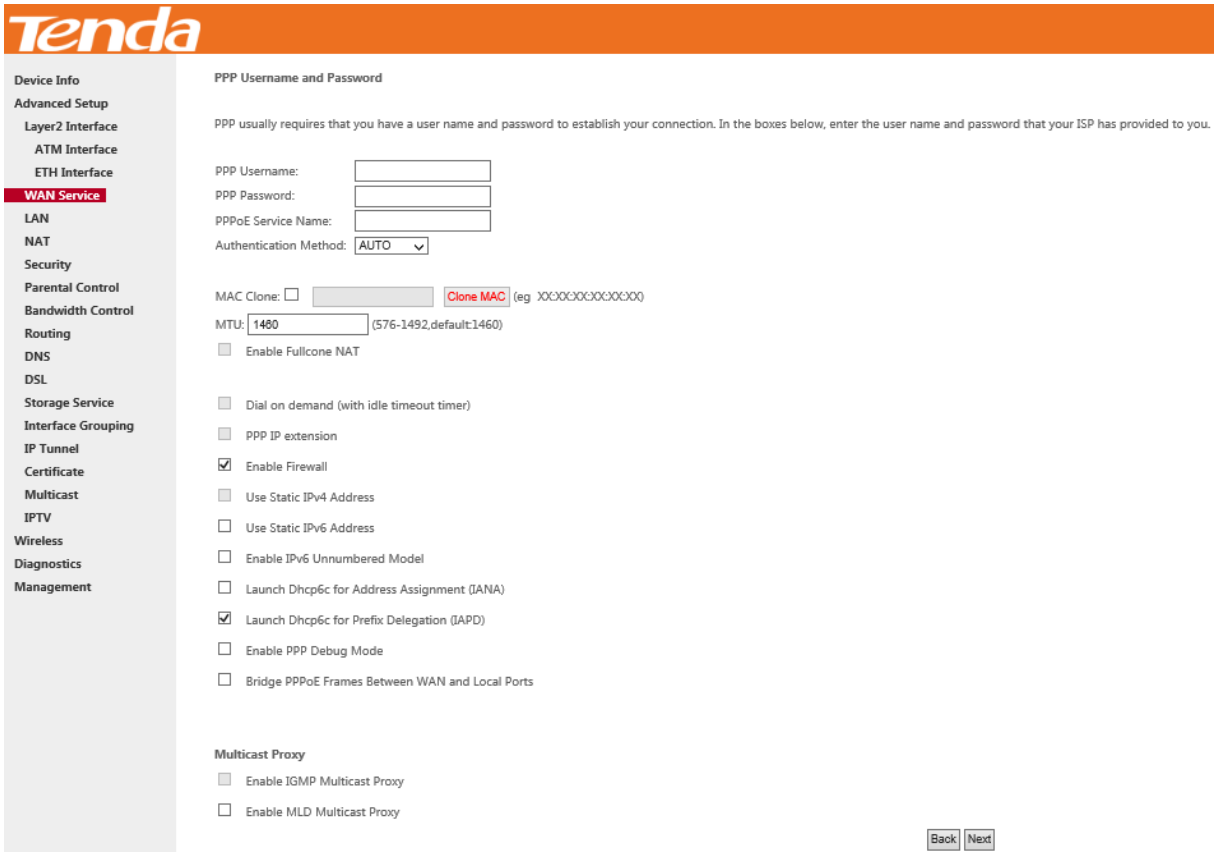


Step 2: Select the ETH interface you added just now from the pull-down menu in the figure below. Click **Next**.

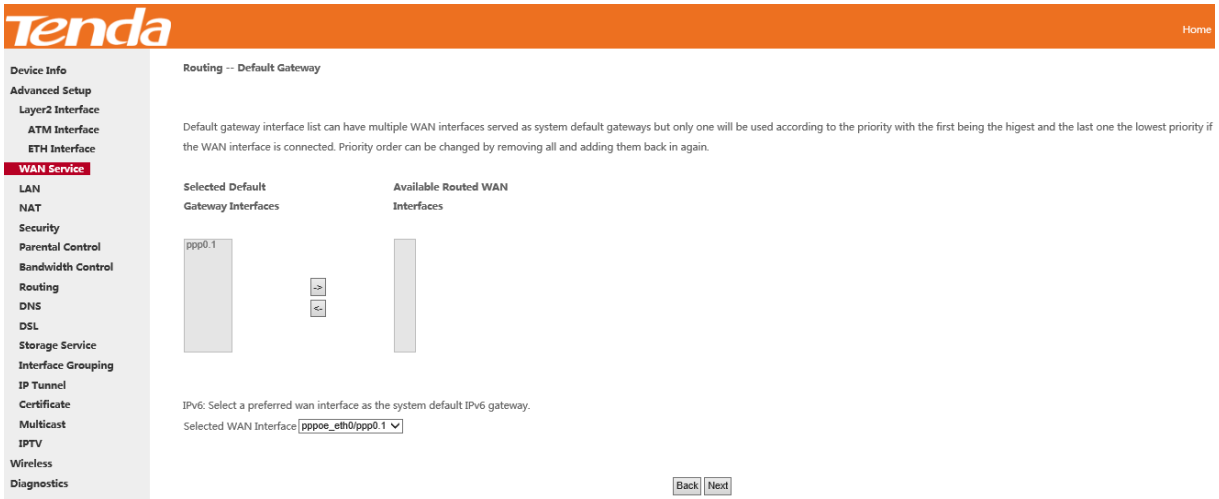
Step 3: Select **PPP over Ethernet**. Edit the **Enter Service Description**. This field is optional. It is recommended that you keep the default. Select a network protocol: **IPv6 Only**. And click **Next**.



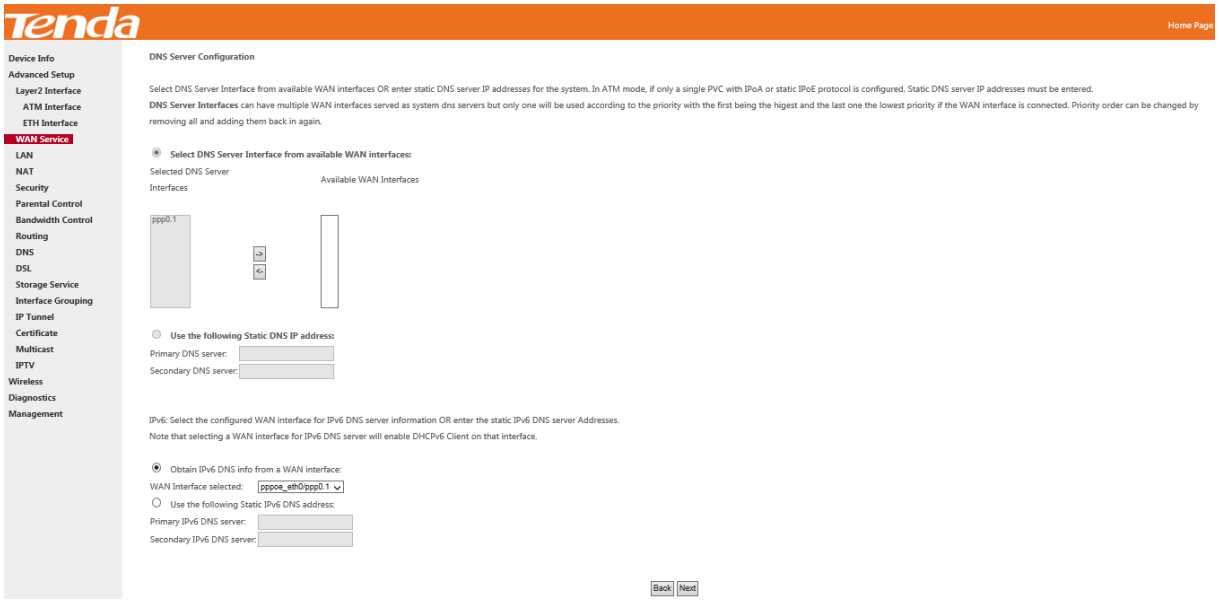
Step 4: Enter PPP username and PPP password provided by your ISP. Check **Launch Dhcp6c for Prefix Delegation (IAPD)**. If your ISP is using stateful DHCPv6, check **Launch Dhcp6c for Address Assignment (IANA)** also. Or configure a static IP address.



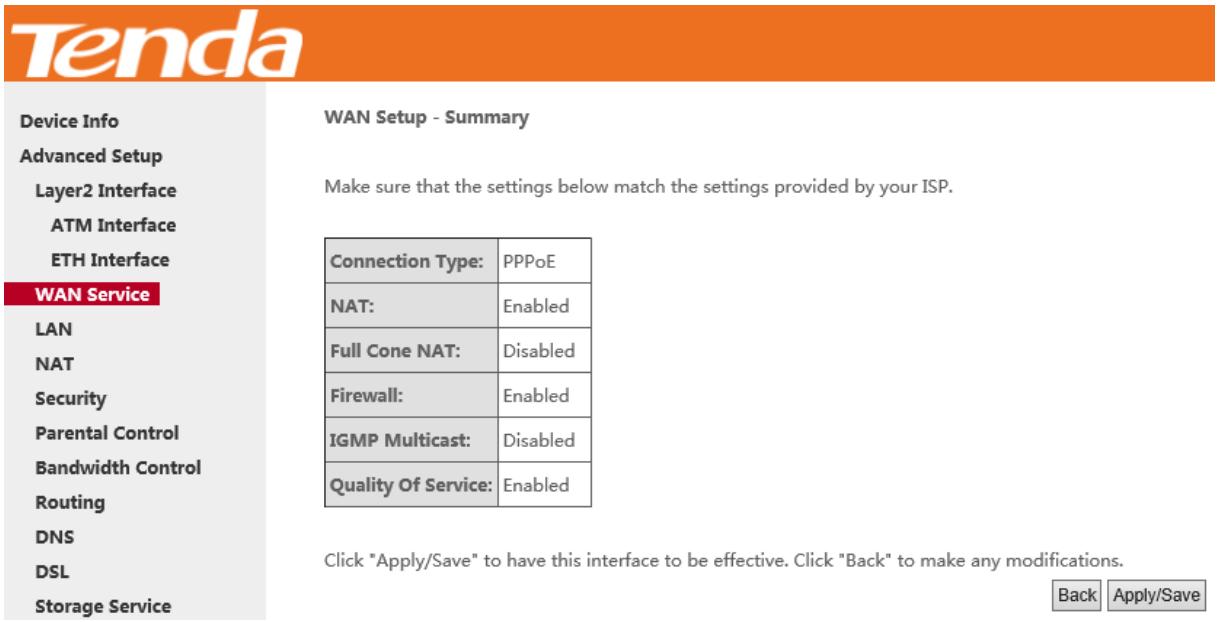
Step 5: Select a preferred WAN interface from the WAN interface list as the system default IPv6 gateway. Click **Next**.



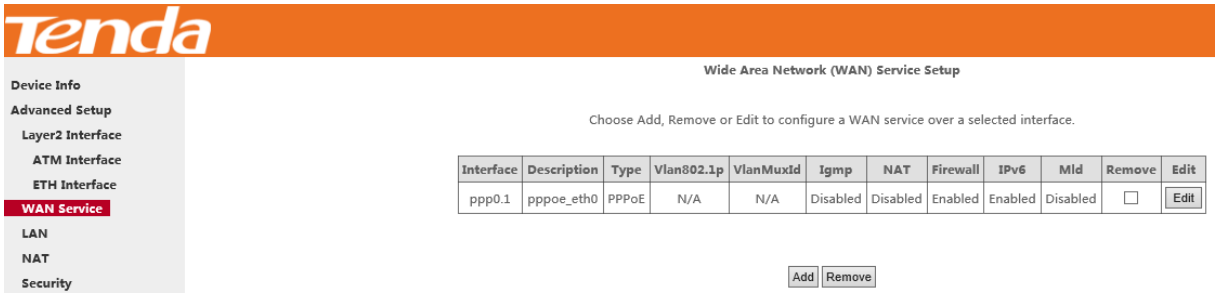
Step 6: Select the configured WAN interface for IPv6 DNS server information or use a static IPv6 DNS server address. Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Client on that interface. And then click **Next**.



Step 7: Here you can view your configurations. Click **Apply/Save** to save your settings if everything is correctly set.



When the PPPoE connection is successful, you can access the Internet.

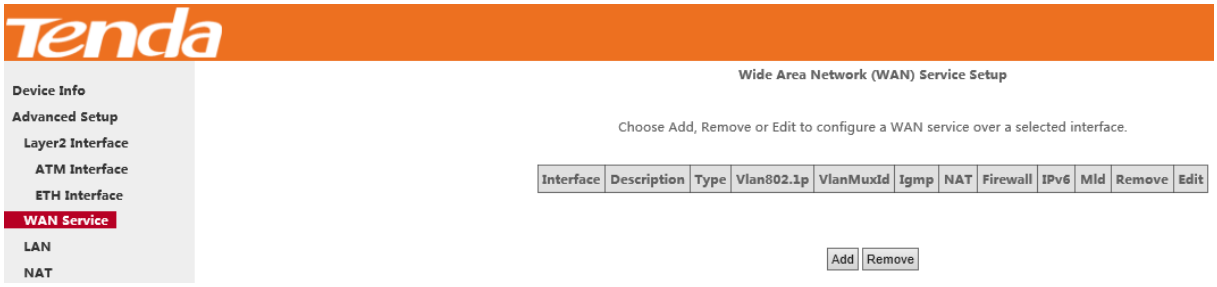


- **IP over Ethernet (IPoE)**

If you get an IP address from your ISP automatically or if your ISP assigns you a static (fixed) IP address, subnet mask and gateway, you need to select the IP over Ethernet (IPoE).

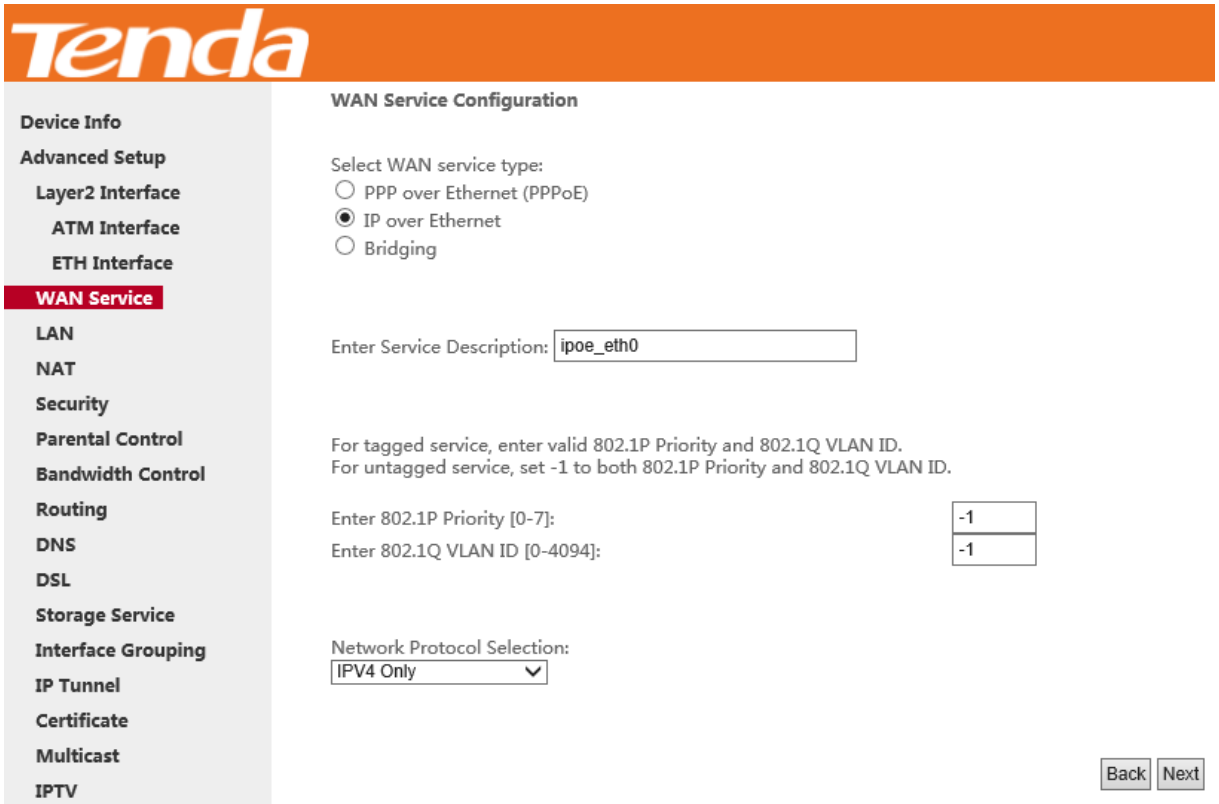
IPv4

Step 1: Click **Advanced Setup > WAN Service** and then click the **Add** button.

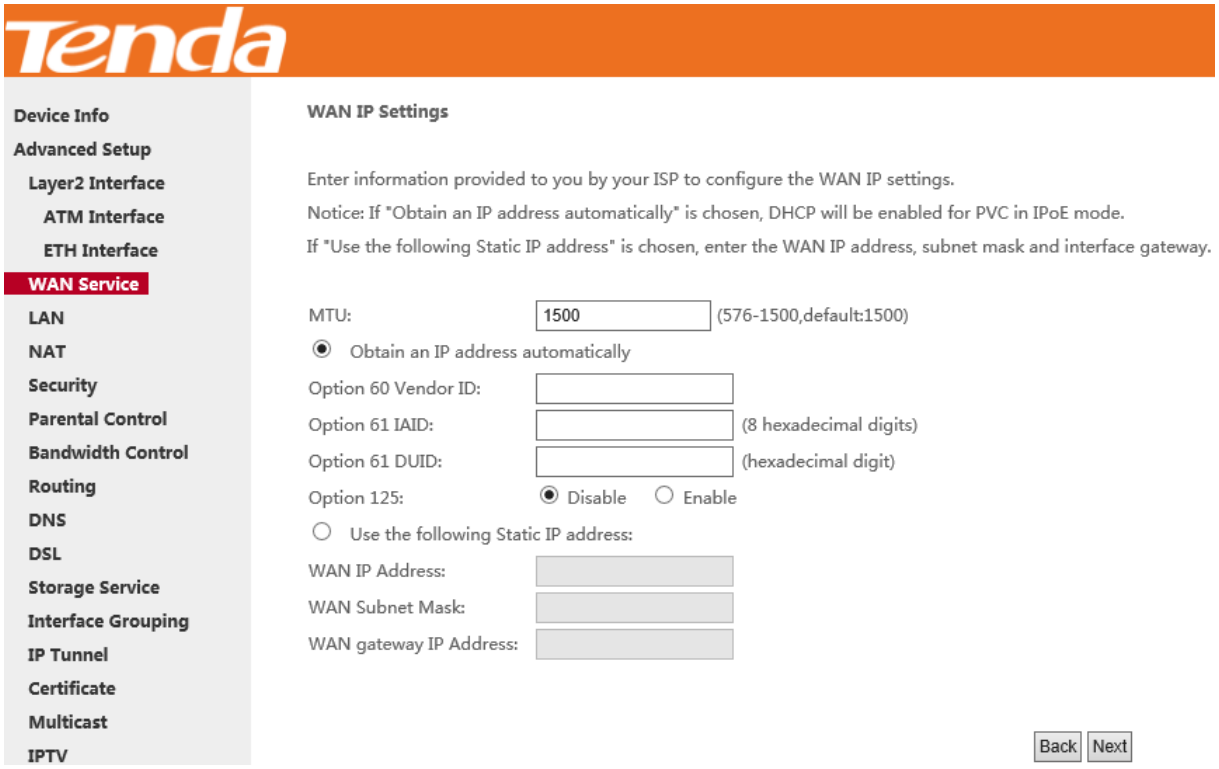


Step 2: Select the ETH interface you added just now from the pull-down menu in the figure below. Click **Next**.

Step 3: Select **IP over Ethernet** as WAN service type. Edit the **Enter Service Description.** This field is optional. It is recommended that you keep the default. Select a network protocol: **IPv4 Only**. And then click **Next**.



Step 4: Enter the IP address/subnet mask/gateway IP address provided by your ISP or select **Obtain an IP address automatically** and then click the **Next** button.



Obtain an IP address automatically: This allows the router to automatically acquire IP information from your ISP or your existing networking equipment.

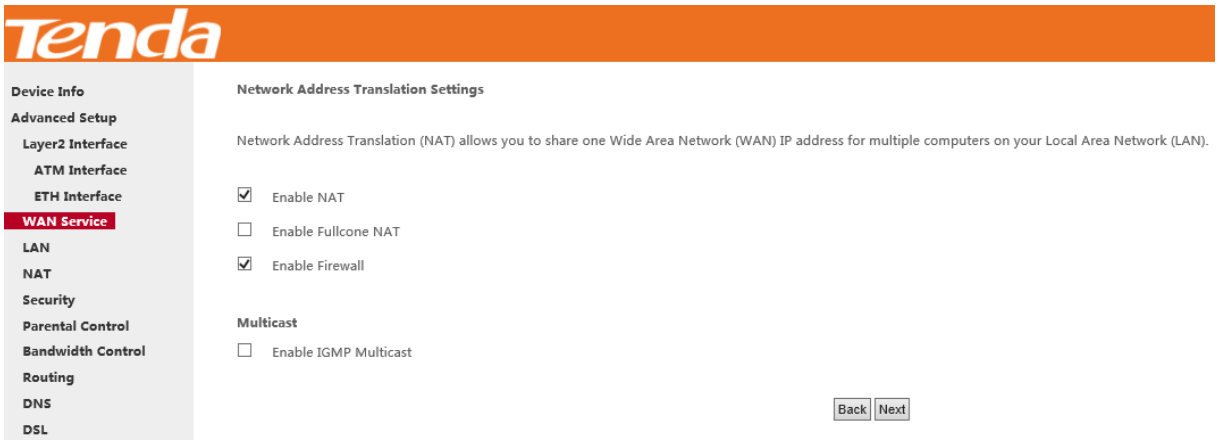
Use the following Static IP address: This allows you to specify the Static IP information provided by your ISP or that corresponds with your existing networking equipment.

WAN IP Address: The Internet IP address provided by your ISP for accessing the Internet.

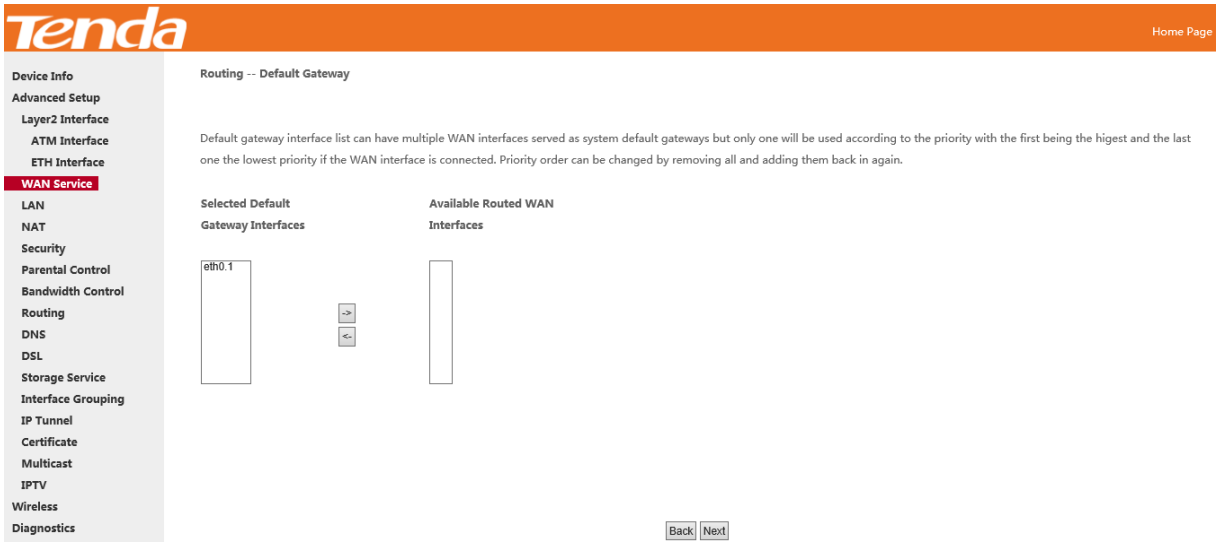
WAN Subnet Mask: The subnet mask address provided by your ISP for accessing the Internet.

WAN gateway IP Address: The gateway IP address provided by your ISP for accessing the Internet.

Step 5: Here you can configure the NAT. If you are not an advanced user, the default settings are recommended and then click **Next**.



Step 6: Here you can configure the WAN gateway address. After you configure it click **Next**. The default setting is recommended.

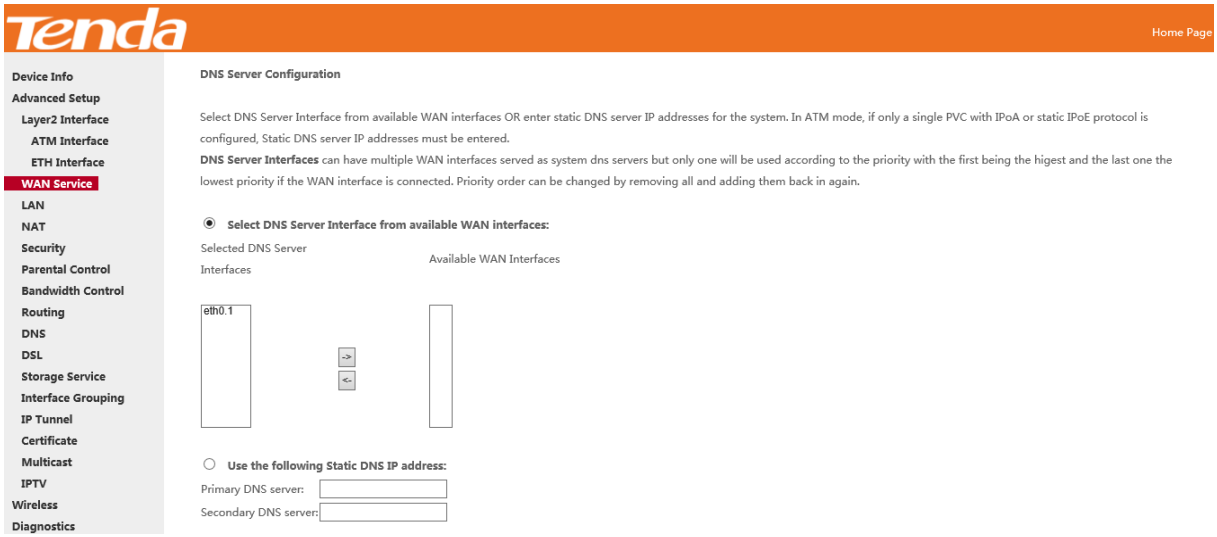


Step 7: Here you can configure the WAN DNS address.

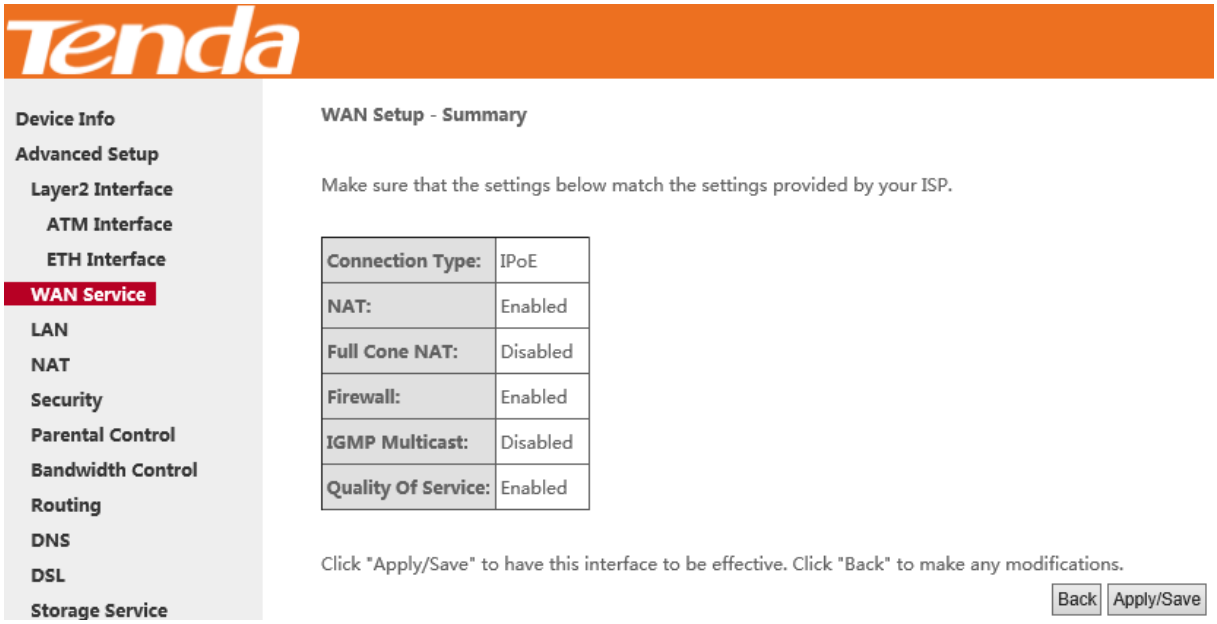
-Click the **Select DNS Server Interface** from available WAN interfaces option;

-Or select the **Use the following Static DNS IP address** option and enter static DNS server IP addresses for the system.

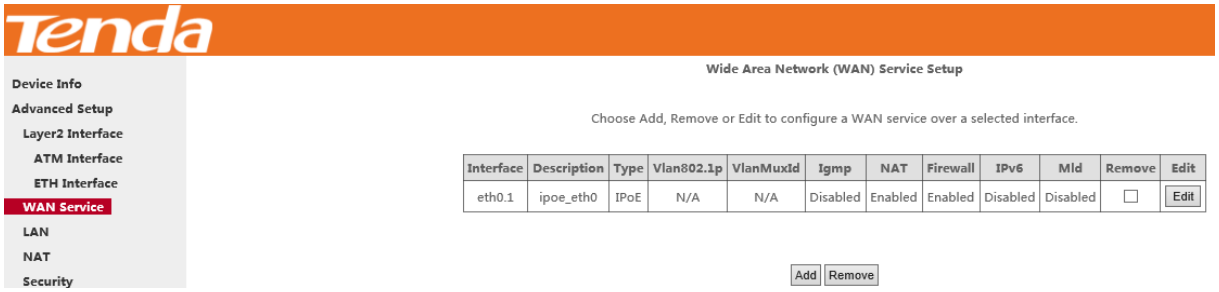
And then click **Next**.



Step 8: Here you can view your configurations. Click **Apply/Save** to save your settings if everything is correctly set.

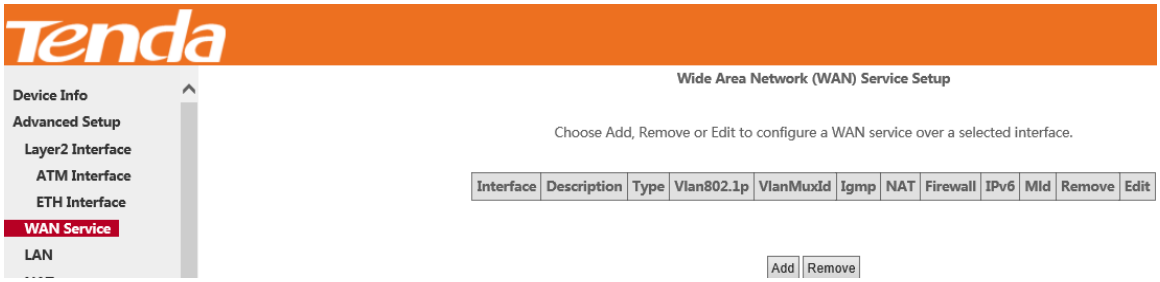


When the IPoE connection is successful, you can access the Internet.



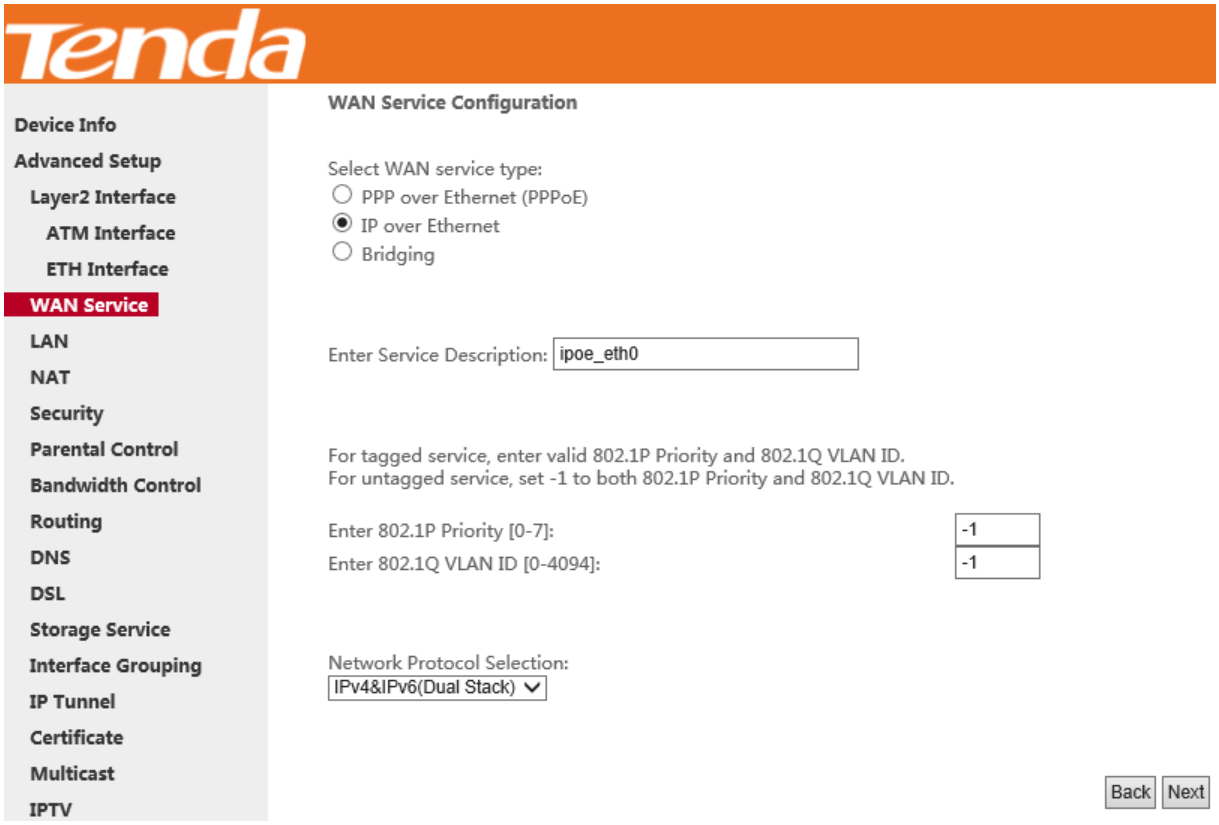
IPv4 & IPv6 (Dual Stack)

Step 1: Click **Advanced Setup > WAN Service** and then click the **Add** button.

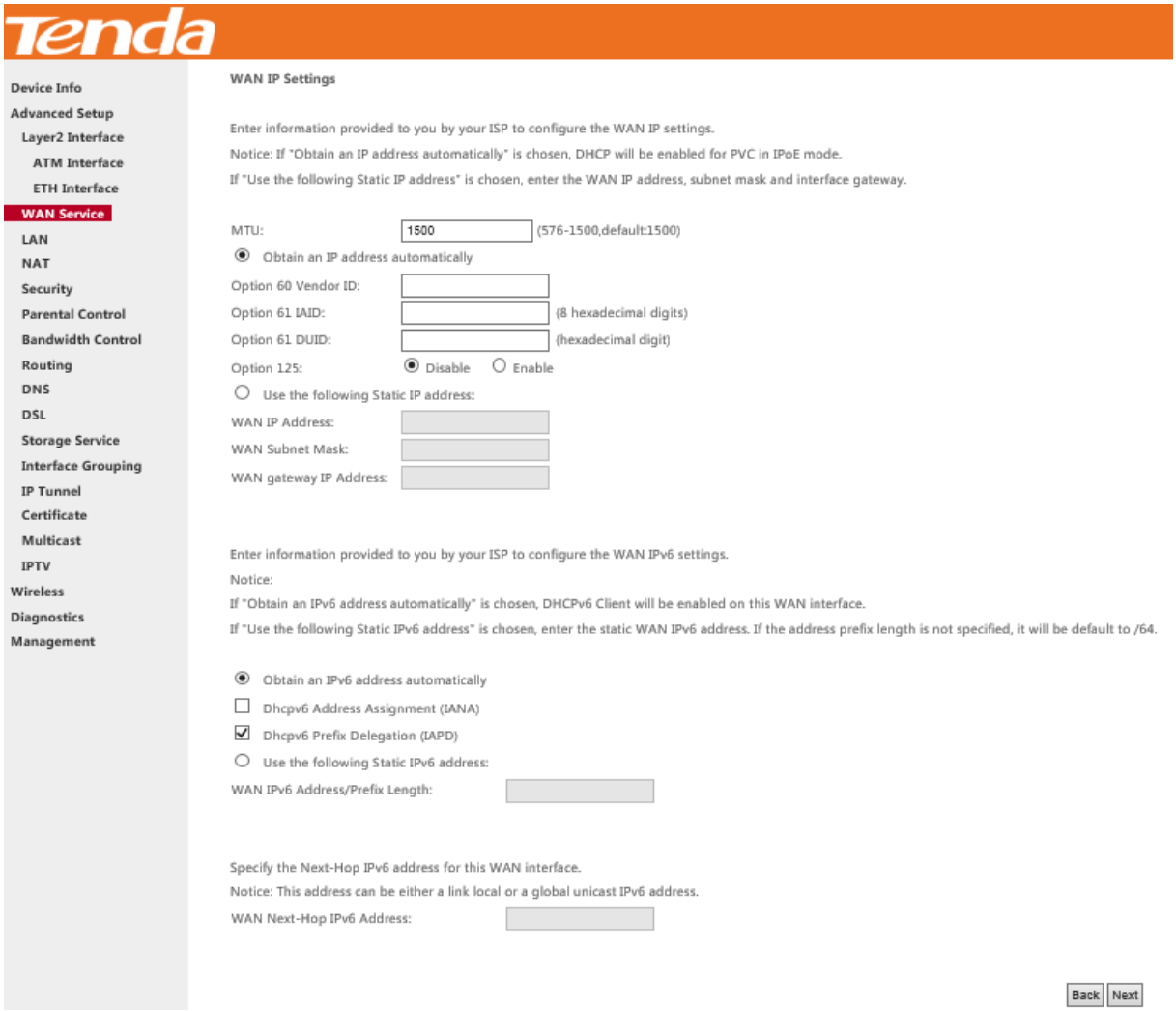


Step 2: Select the ETH interface you added just now from the pull-down menu in the figure below. Click **Next**.

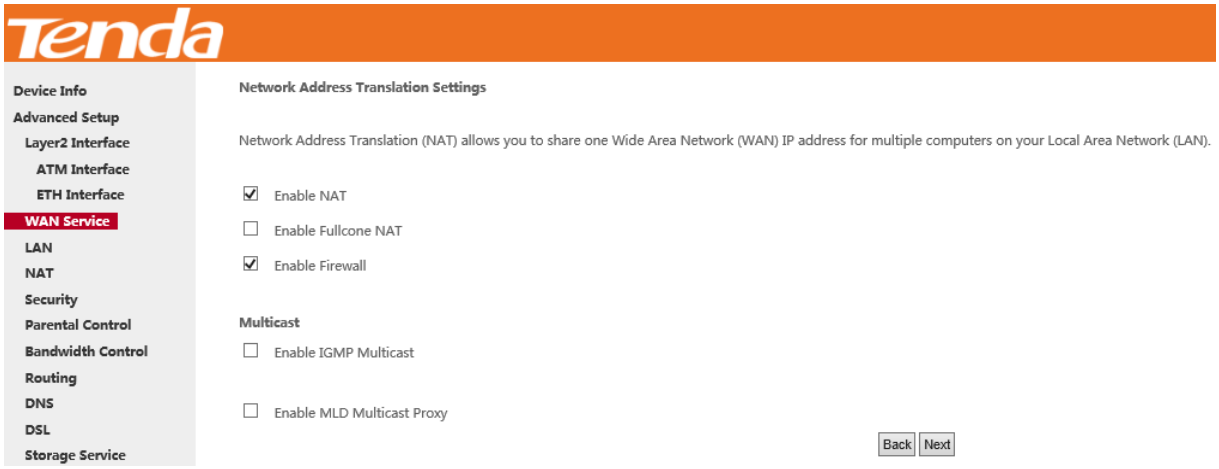
Step 3: Select **IP over Ethernet** as WAN service type. Edit the **Enter Service Description.** This field is optional. It is recommended that you keep the default. Select a network protocol: **IPv4&IPv6 (Dual Stack)**. And then click **Next**.



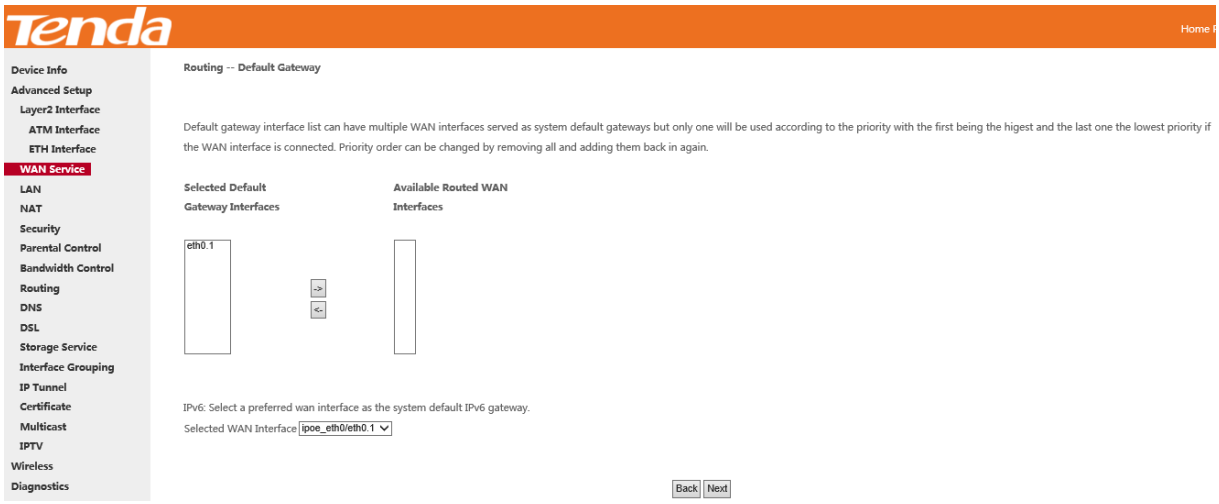
Step 4: Enter information provided by your ISP to configure the WAN IP settings.



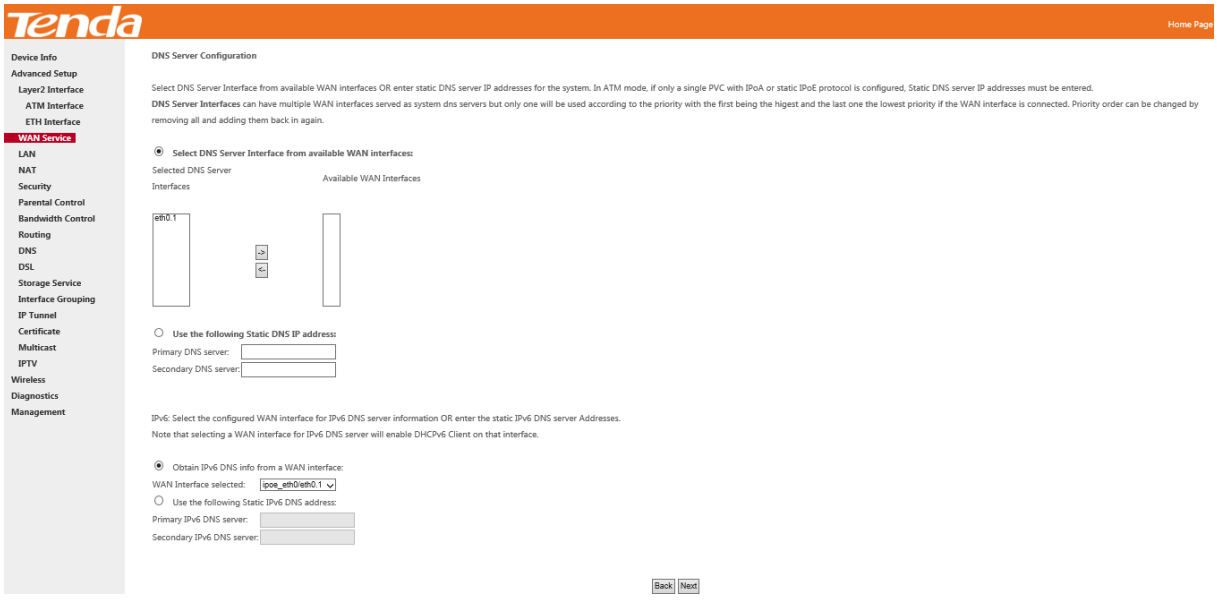
Step 5: Here you can configure the NAT. If you are not an advanced user, the default settings are recommended and then click **Next**.



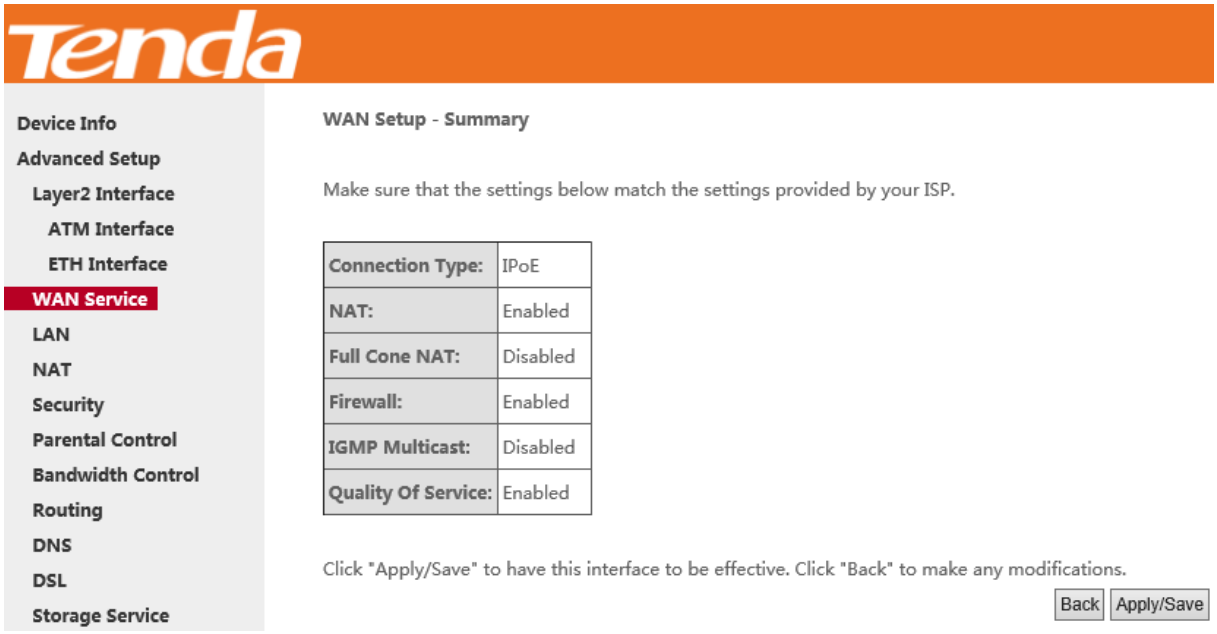
Step 6: Configure a WAN interface as the default gateway.



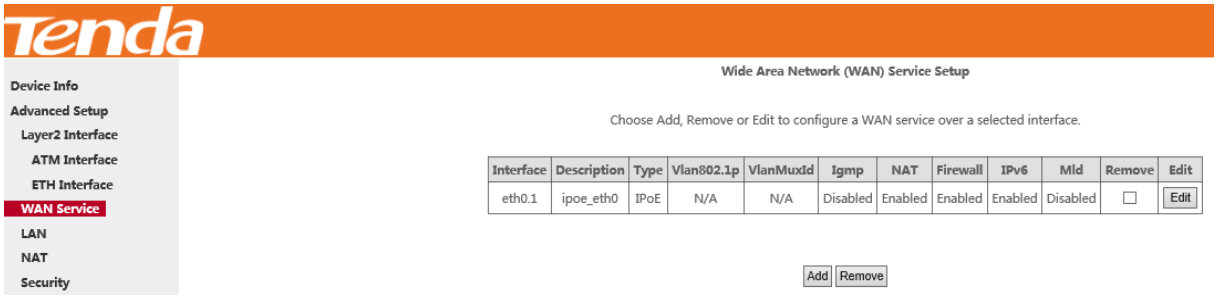
Step 7: Configure DNS server (Select an available DNS server interface or use a specified DNS server); configure IPv6 DNS server (Obtain IPv6 DNS info from a WAN interface or use a specified DNS server), and then click **Next**.



Step 8: Here you can view your configurations. Click **Apply/Save** to save your settings if everything is correctly set.

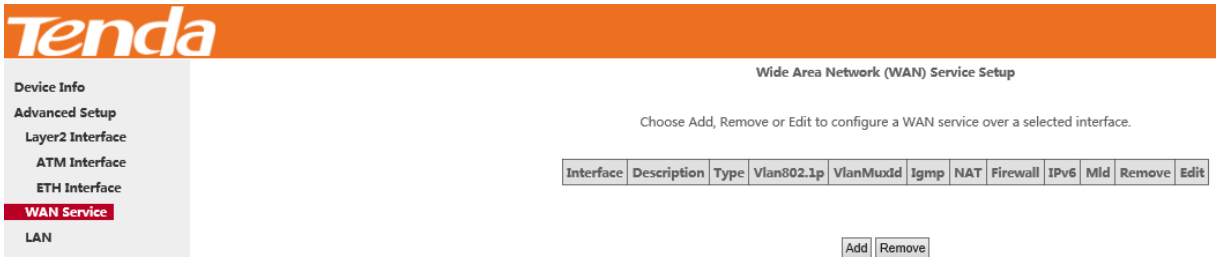


When the IPoE connection is successful, you can access the Internet.



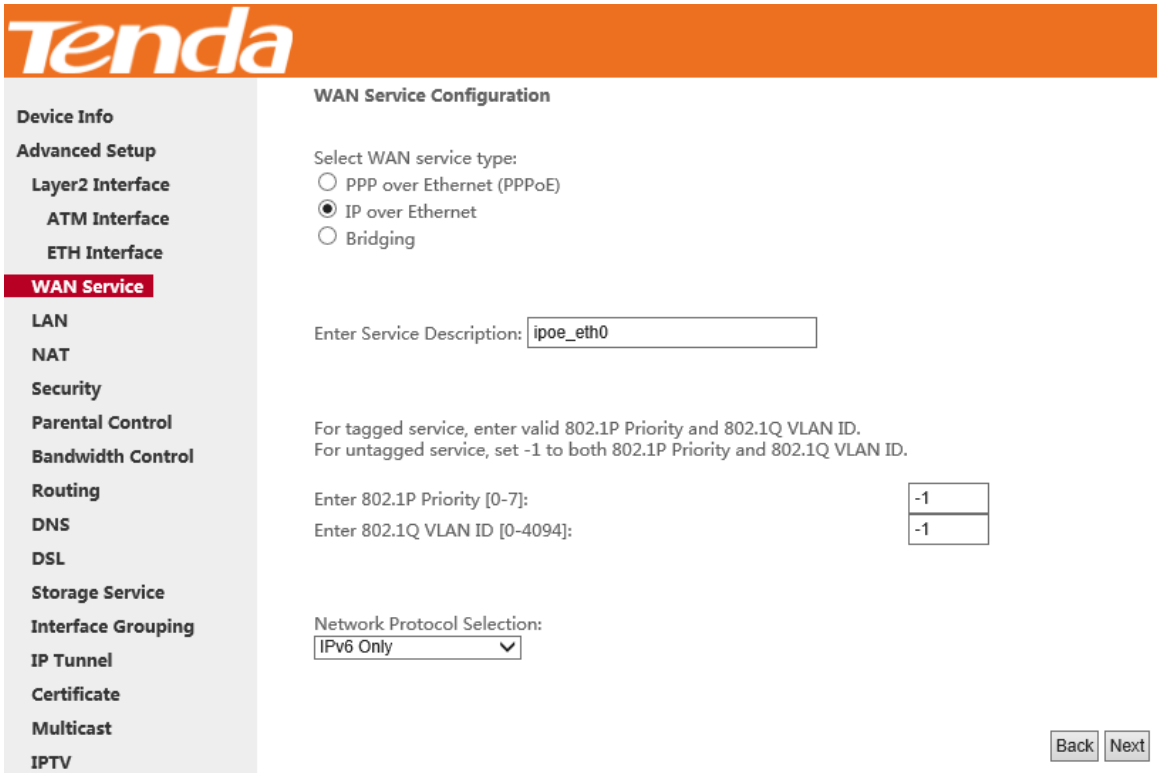
IPv6

Step 1: Click **Advanced Setup > WAN Service** and then click the **Add** button.



Step 2: Select the ETH interface you added just now from the pull-down menu in the figure below. Click **Next**.

Step 3: Select **IP over Ethernet** as WAN service type. Edit the **Enter Service Description.** This field is optional. We recommend that you keep the default. Select a network protocol: **IPv6 Only**. And then click **Next**.

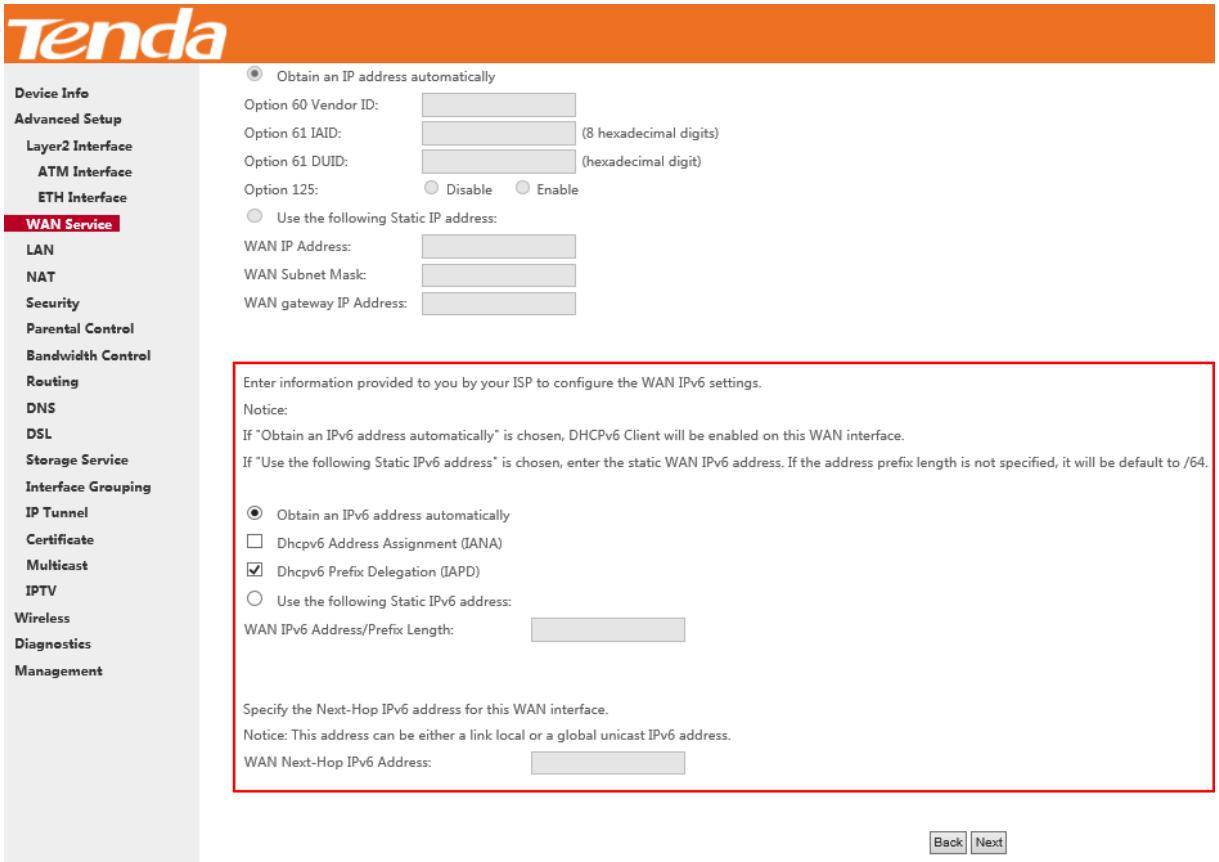


Step 4: Enter the WAN information provided by your ISP to configure the WAN IPv6 settings.

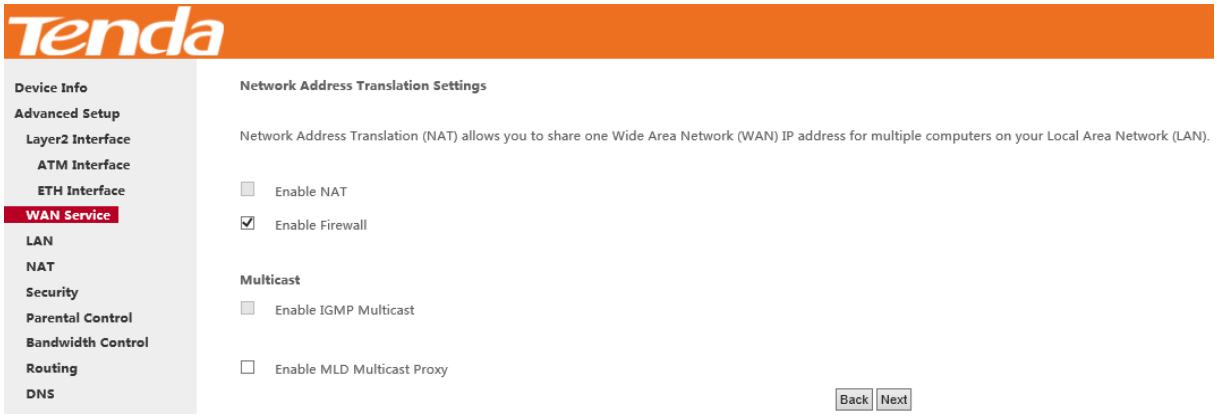
To obtain an IP address automatically:

Select **Obtain an IPv6 address automatically** and Check **Dhcp6c Prefix Delegation (IAPD)**.

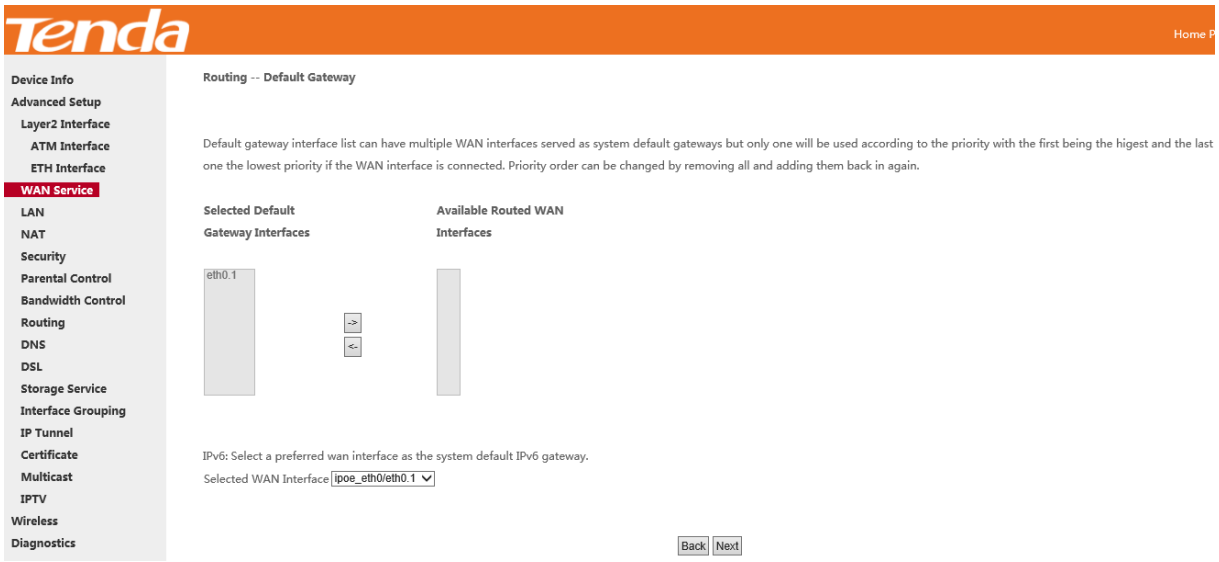
If your ISP is using stateful DHCPv6, check **Dhcp6c Address Assignment (IANA)** also. Click **Next** to go forwards.



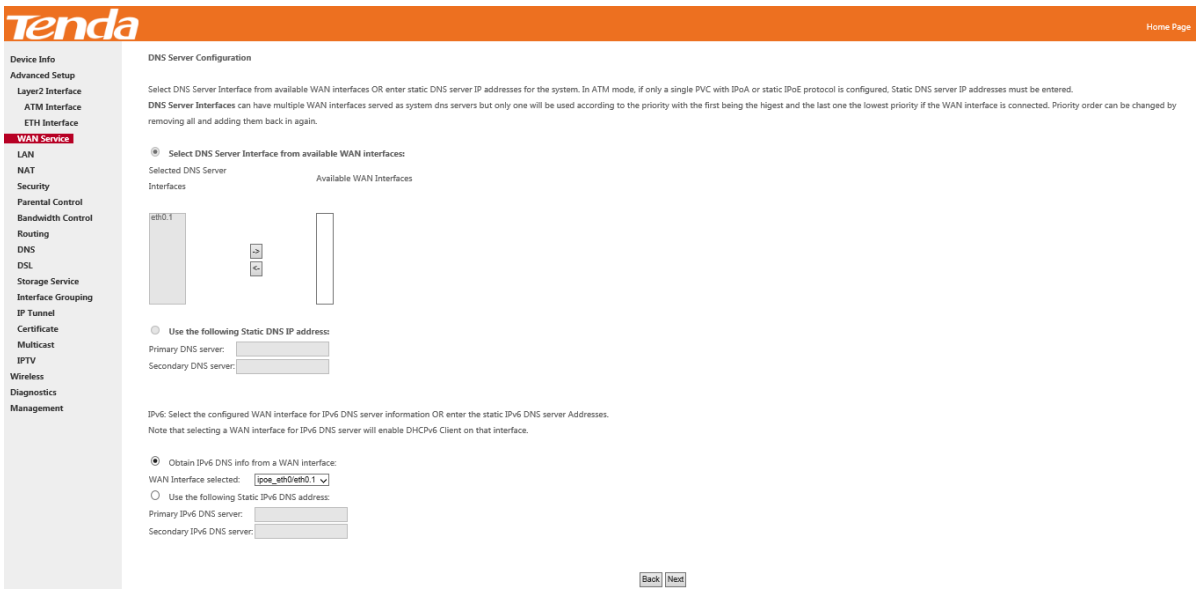
Step 5: Here you can configure the NAT. If you are not an advanced user, the default settings are recommended and then click **Next**.



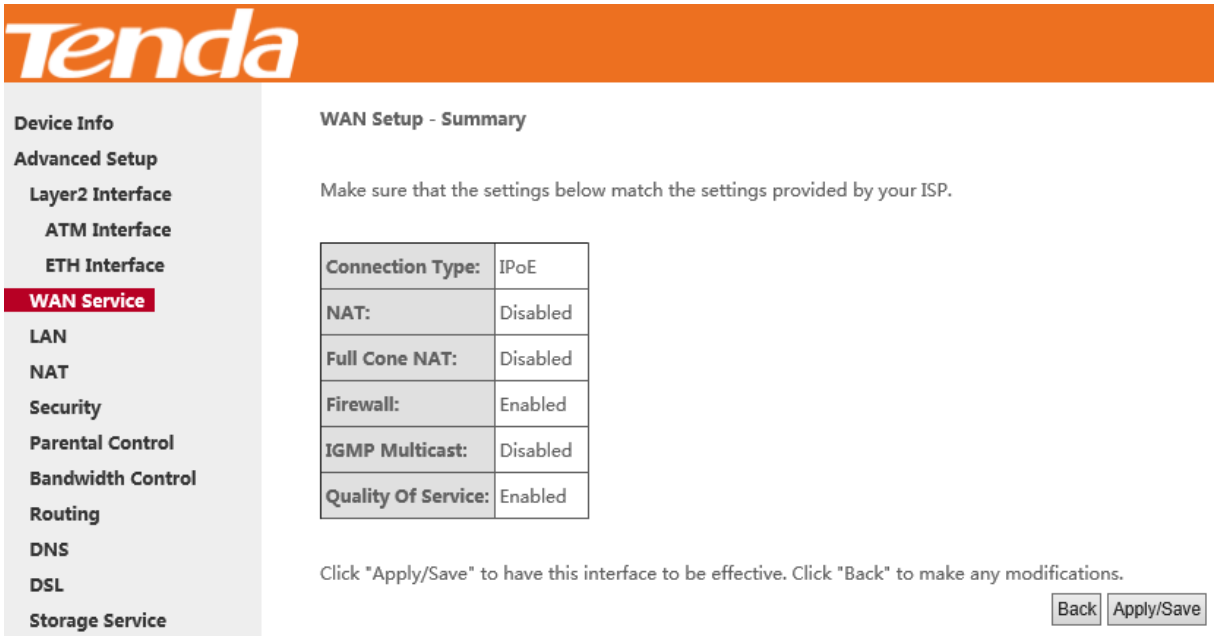
Step 6: To configure the Default Gateway interface when using IPv6, select the interface that you want to configure with the WAN gateway address in **Selected WAN Interface** box. Then click **Next**.



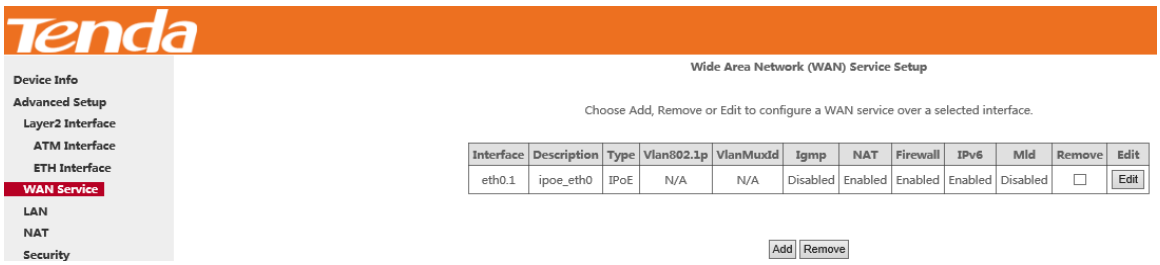
Step 7: To configure the WAN DNS address, check the **Obtain IPv6 DNS info from a WAN interface** option, or select the **Use the following Static IPv6 DNS address** option to enter the static DNS server IPv6 addresses provided by your ISP. At last, click **Next**.



Step 8: Here you can view your configurations. Click **Apply/Save** to save your settings if everything is correctly set.



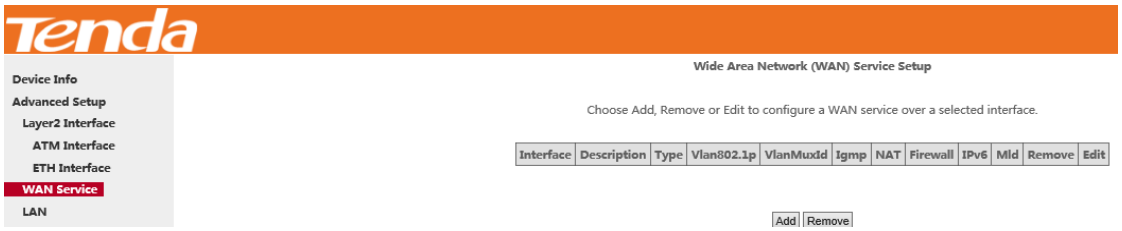
When the IPoE connection is successful, you can access the Internet.



▪ Bridging

If you wish to initiate a dialup directly from your PC for Internet access or enjoy the entire Internet connection (instead of sharing it with others), you can select the Bridging and create a dialup program from your PC.

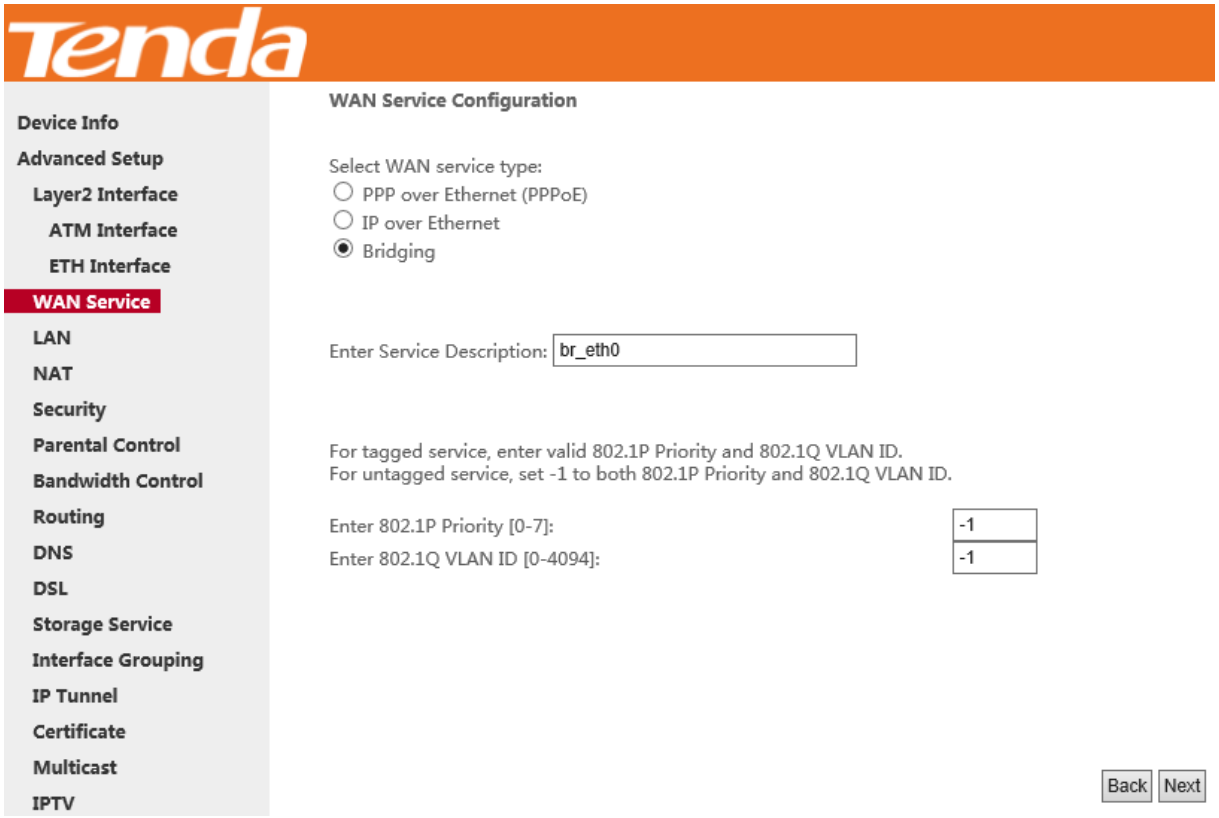
Step 1: Click **Advanced Setup** > **WAN Service** and then click the **Add** button.



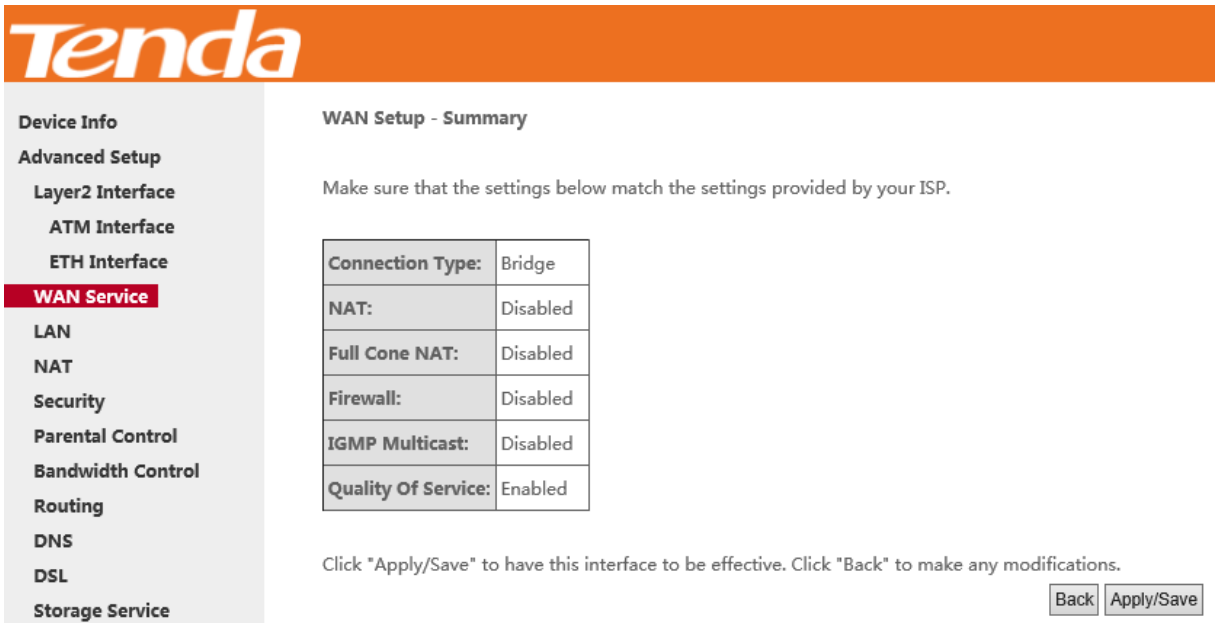
Step 2: Select the ETH interface you added just now from the pull-down menu in the figure below. Click **Next**.

Step 3: Select **Bridging**. Edit the **Enter Service Description**. This field is optional. It is recommended that you keep the

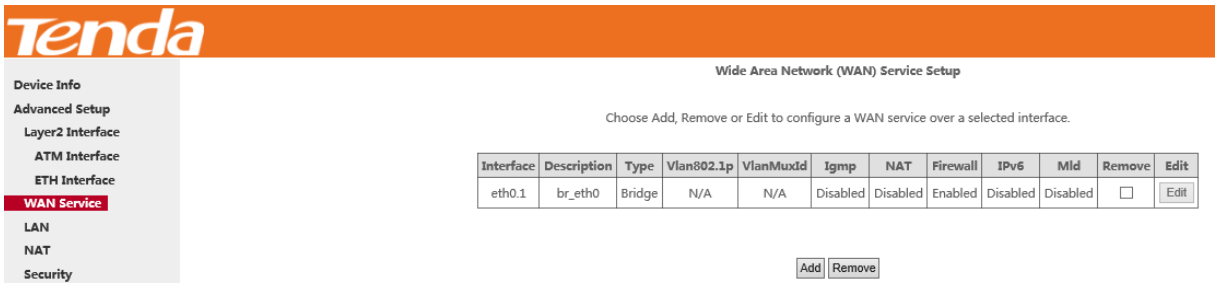
default. And click **Next**.



Step 4: Here you can view your configurations. Click **Apply/Save** to save your settings if everything is correctly set.



After the bridging connection is successful, initiate a dialup directly from your PC for Internet access.



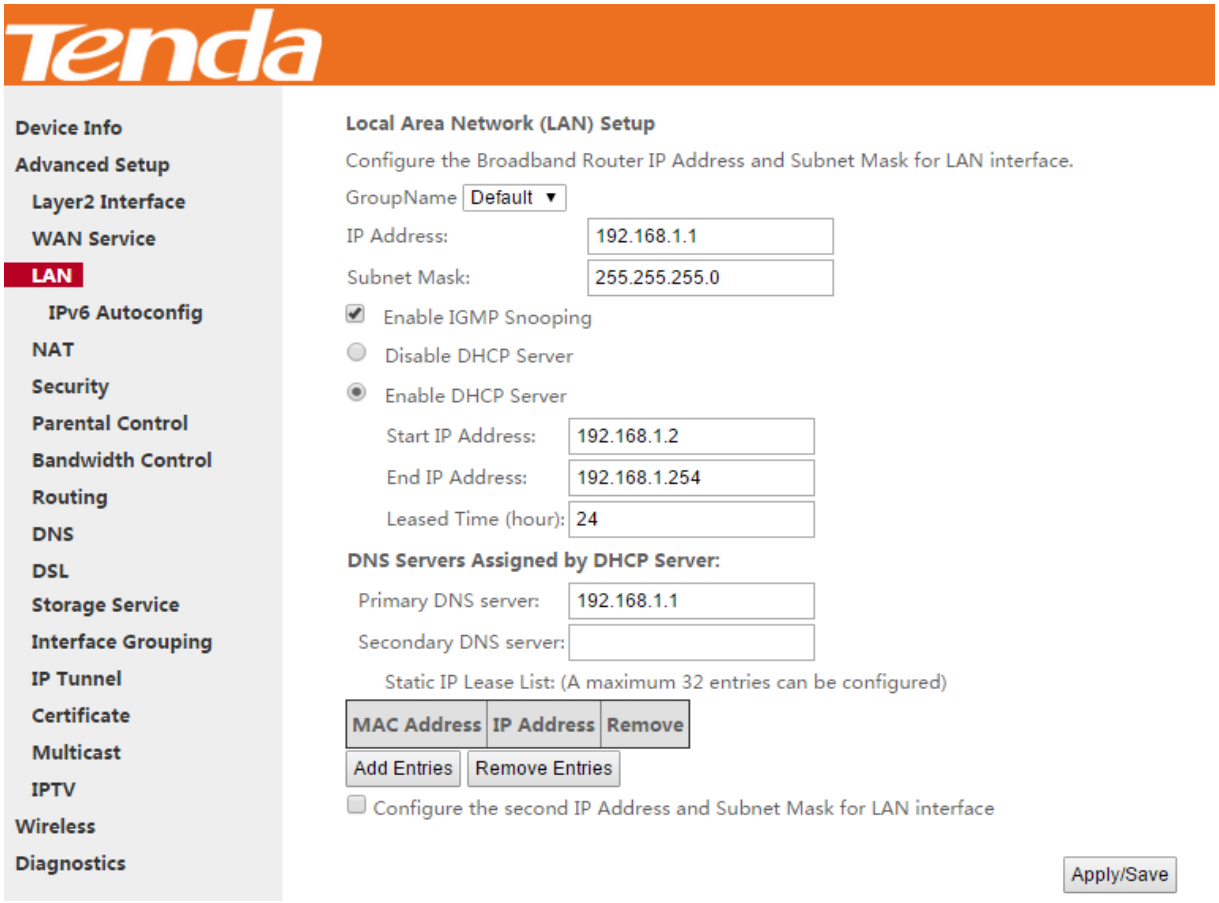
4.2.3 LAN Setup

Here you can configure the LAN IP Address and subnet mask. This IP address is to be used to access the device's settings through a web browser. Be sure to make a note of any changes you apply to this page.

This part includes the following information:

- *IPv4*
- *IPv6 Autoconfig*

IPv4



IP Address: The device's LAN IP address. The default setting is 192.168.1.1.

Subnet Mask: The LAN subnet mask of the device. Combined with the IP address, the IP Subnet Mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or modem router. You can change the subnet mask to fit your network.

Enable IGMP Snooping: Check to enable the IGMP Snooping. It is recommended to keep the default settings.

Disable DHCP Server: Click to disable the DHCP Server.

Enable DHCP Server: Click to enable the DHCP Server.

Start IP Address: Specify the start of the range for the pool of IP addresses in the same subnet as the router.

End IP Address: Specify the end of the range for the pool of IP addresses in the same subnet as the router.

Leased Time: The lease time is a time length that the IP address is assigned to each device before it is refreshed.

Static IP Lease List: Displays a list of devices with reserved static IP addresses.

Add Entries: Click to add a static IP lease entry. A maximum 32 entries can be configured.

Remove Entries: Click to remove a static IP lease entry.

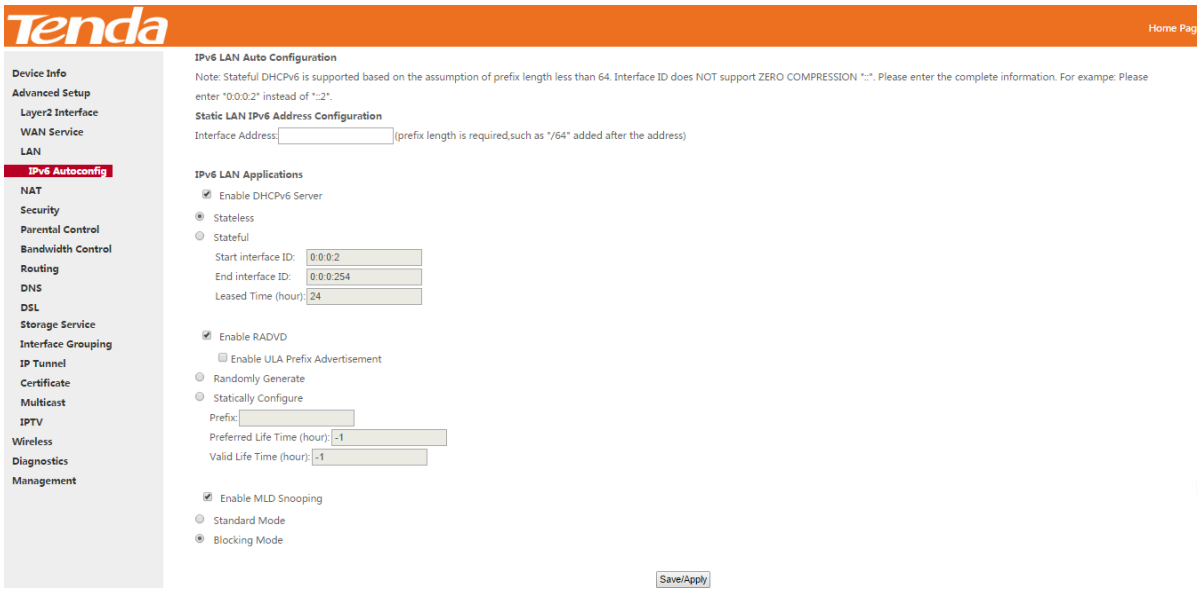
Configure the second IP Address and Subnet Mask for LAN interface: If you want to configure two IP addresses for the LAN interface, you can check this option and enter the second IP Address and Subnet Mask manually.

Apply/Save: After you configure all the needed settings, click this button to apply and save them.

TIP

DHCP (Dynamic Host Configuration Protocol) assigns an IP address to each device on the LAN/private network. When you enable the DHCP Server, the DHCP Server will automatically allocate an unused IP address from the IP address pool specified in this screen to the requesting device as long as the device is set to "Obtain an IP Address Automatically". By default, DHCP is enabled.

IPv6 Autoconfig



- **Static LAN IPv6 Address Configuration**

Interface Address (prefix length is required): Enter the interface address.

NOTE

1. IPv6 address can only be Aggregatable Global Unicast Addresses and Unique Local Address. Link-Local Unicast Addresses and Multicast Addresses are not permitted.

2. The IPv6 address must be entered with a prefix length.

▪ IPv6 LAN Applications

Enable DHCPv6 Server： Check to enable the DHCPv6 Server.

Stateless: If selected, IPv6 clients will generate IPv6 addresses automatically based on the Prefix Delegation's IPv6 prefix and their own MAC addresses.

Stateful: Stateful DHCPv6 is supported based on the assumption of prefix length less than 64. Select this option and configure the start/end interface ID and leased time. The router will automatically assign IPv6 addresses to IPv6 clients.

Leased Time (hour): The lease time is a time length that the IP address is assigned to each device before it is refreshed.

Start interface ID/End interface ID: Specify the start/end interface ID Interface ID does NOT support ZERO COMPRESSION "::". Please enter the complete information. For example: Please enter "0:0:0:2" instead of "::2".

Enable RADVD: The RADVD (Router Advertisement Daemon) implements link-local advertisements of IPv6 router addresses and IPv6 routing prefixes using the Neighbor Discovery Protocol (NDP) and is used by system administrators in stateless autoconfiguration methods of network hosts on Internet Protocol version 6 networks. Check the checkbox to enable the RADVD.

Enable ULA Prefix Advertisement: If enabled, the router will advertise ULA prefix periodically

Randomly Generate: If selected, address prefix can be automatically generated.

Statically Configure: If you select this option, you need to manually configure the address prefix and life time.

Prefix: Specify the prefix.

Preferred Life Time (hour): Specify the preferred life time in hour.

Valid Life Time (hour): Specify the valid life time in hour.

Enable MLD Snooping: MLD is used by IPv6 routers for discovering multicast listeners on a directly attached link. If disabled on layer2 devices, IPv6 multicast data packets will be broadcast on the entire layer2; if enabled, these packets will be multicast to only specified recipient instead of being broadcast on the entire layer2.

TIP

If you change the LAN IP address of the device, the current connection to the device will be stopped. You must use the new IP address to log in to the device. Be sure to write the new address on a sticky label and attach it to the bottom of the unit. You will need the new address to log in to the device in the future.

4.2.4 NAT

This section explains the following:

• *Virtual Server*

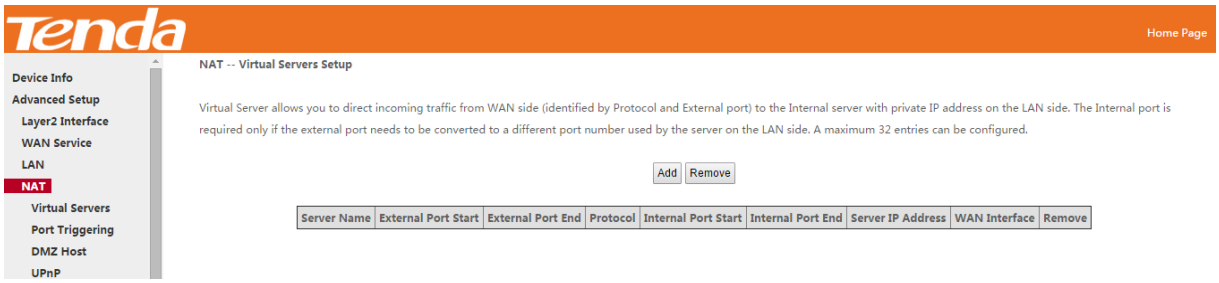
• *Port Triggering*

• *DMZ Host*

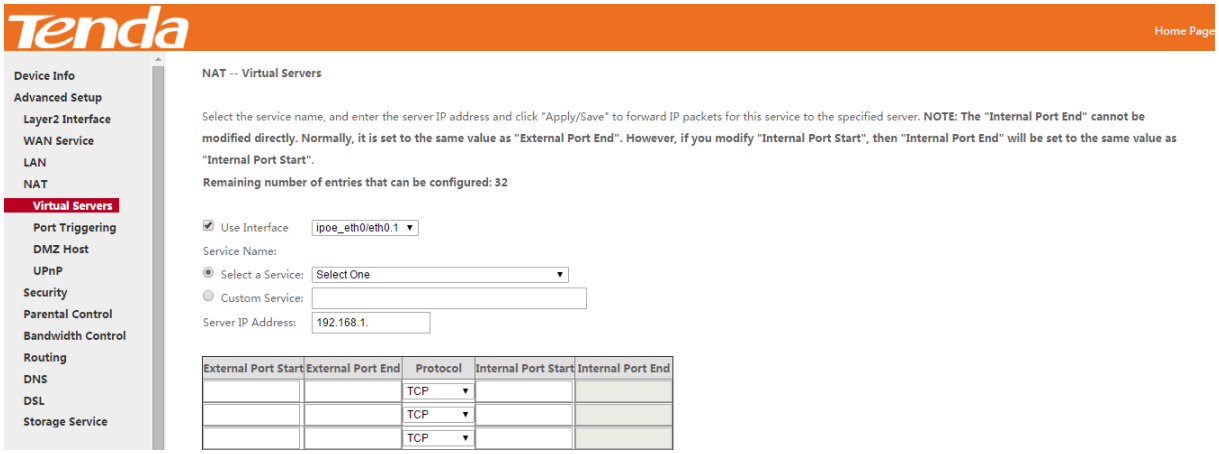
• *UPnP*

Virtual Server

The Virtual Server is useful for web servers, ftp servers, e-mail servers, gaming and other specialized Internet applications. When you enable the Virtual Server, the communication requests from the Internet to your router's WAN port will be forwarded to the specified LAN IP address.



To enter the virtual server screen, click **NAT > Virtual Server** and then click the **Add** button to add rules.



Use Interface: Select a WAN connection to which you wish to apply the rules. When there is only one WAN connection available, the rules will be automatically applied to it.

Service Name:

- Select a Service: Allows you to select an existing service from the drop-down list.

- Custom Service: Allows you to customize a service.

Server IP Address: Enter the IP address of your local computer that will provide this service.

External Starting Port and External Ending Port: These are the starting number and ending number for the public

ports at the Internet interface.

Protocol: Select the protocol from the Protocol drop-down list. If you are unsure, select TCP/UDP.

Internal Starting Port and Internal Ending Port: These are the starting number and ending number for the ports of a computer on the router's local area network (LAN).

NOTE

If you have enabled the UPnP functionality on both the router and your PC that is attached to one of the LAN port of the router, you will be prompted on the Virtual Server page that the UPnP interface is being used.

Instance

You have set up two servers on your LAN side:

- An FTP server (using the default port number of 21) at the IP address of 192.168.1.100

- A web server (using the default port number of 8080) at the IP address of 192.168.1.110

And want your friends on the Internet to access the FTP server and web server via default ports. To access your FTP or web server from the Internet, a remote user has to know the WAN IP address of your router. In this example, we assume the WAN IP address of your router is 183.37.227.201. Then follow instructions below:

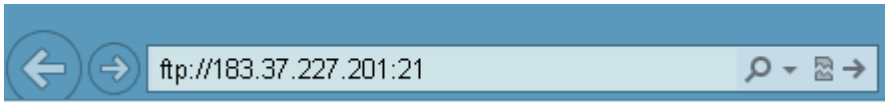
To configure the router to make your local FTP server public:

Procedure

1. Click **NAT > Virtual Server** to enter it and then click the **Add** button.
2. Select **FTP Server** that you wish to host on your network from the **Select a Service** drop-down list. The port number (21) used by this service will then be automatically populated.

   - Or if you wish to define the service yourself, enter a descriptive name in the **Custom Service,** say My FTP, and then manually enter the port number (21) used by this service in the **Internal Starting Port, Internal Ending Port, External Starting Port and External Ending Port fields**.
3. Select a protocol from the **Protocol** drop-down list. If you are unsure, select **TCP/UDP**.
4. In the **Server IP Address** field, enter the last digit of the IP address of your local computer that offers this service. Here in this example, we enter 100.
5. Click Apply/Save.

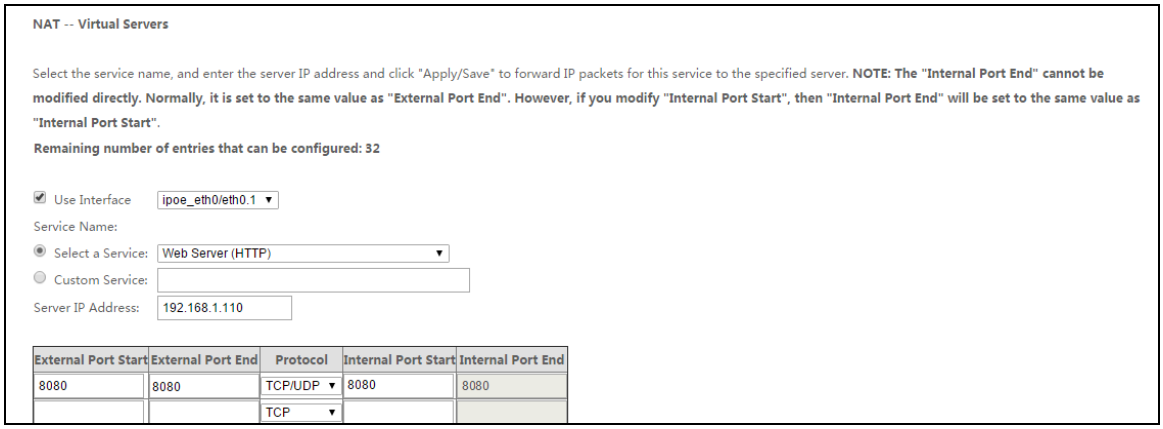
Your friends on the Internet will then be able to access your FTP server simply by "ftp://183.37.227.201:21".



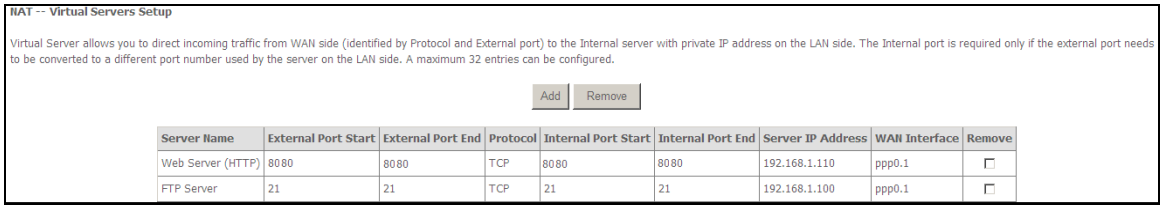
To configure your router to make your local web server public:

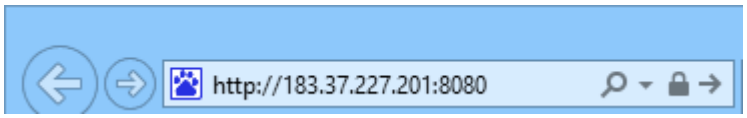
Procedure

1. Click **NAT > Virtual Server** to enter it and then click the **Add** button.
2. Select **Web Server (HTTP)** that you wish to host on your network from the **Select a Service** drop-down list. The port number (8080) used by this service will then be automatically populated.
   - Or if you wish to define the service yourself, enter a descriptive name in the **Custom Service,** say My Web Server (HTTP), and then manually enter the port number (8080) used by this service in the **Internal Starting Port, Internal Ending Port, External Starting Port and External Ending Port fields**.
3. Select a protocol from the **Protocol** drop-down list. If you are unsure, select **TCP/UDP**.
4. In the **Server IP Address** field, enter the last digit of the IP address of your local computer that offers this service. Here in this example, we enter 110.
5. Click Apply/Save.



Now you can view your configurations as seen in the screenshot below. Your friends on the Internet will then be able to access the web server simply by entering "http://183.37.227.201:8080" in his browser.





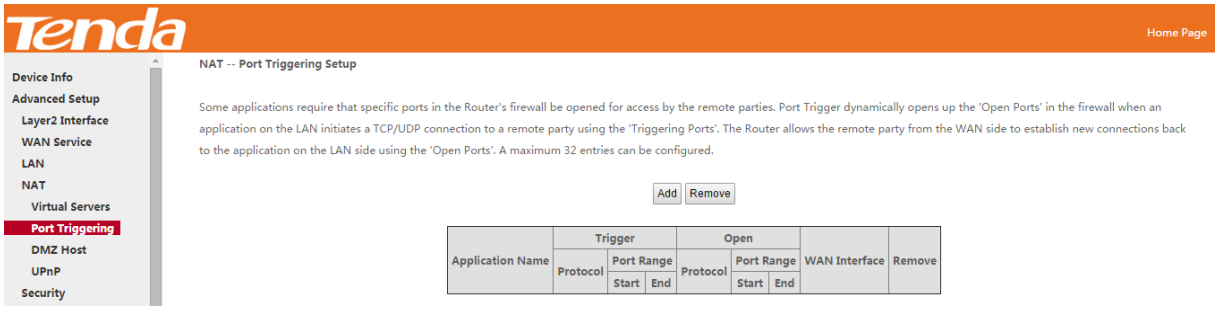
NOTE

1. The "Internal Port End" cannot be modified directly. Normally, it is set to the same value as "External Port End". However, if you modify "Internal Port Start", then "Internal Port End" will be set to the same value as "Internal Port Start".

2. If the service or game you wish to host on your network is not included in the list, manually add it in the Custom Service field and then add the port number used by it to the **Internal Starting Port, Internal Ending Port, External Starting Port and External Ending Port fields**.

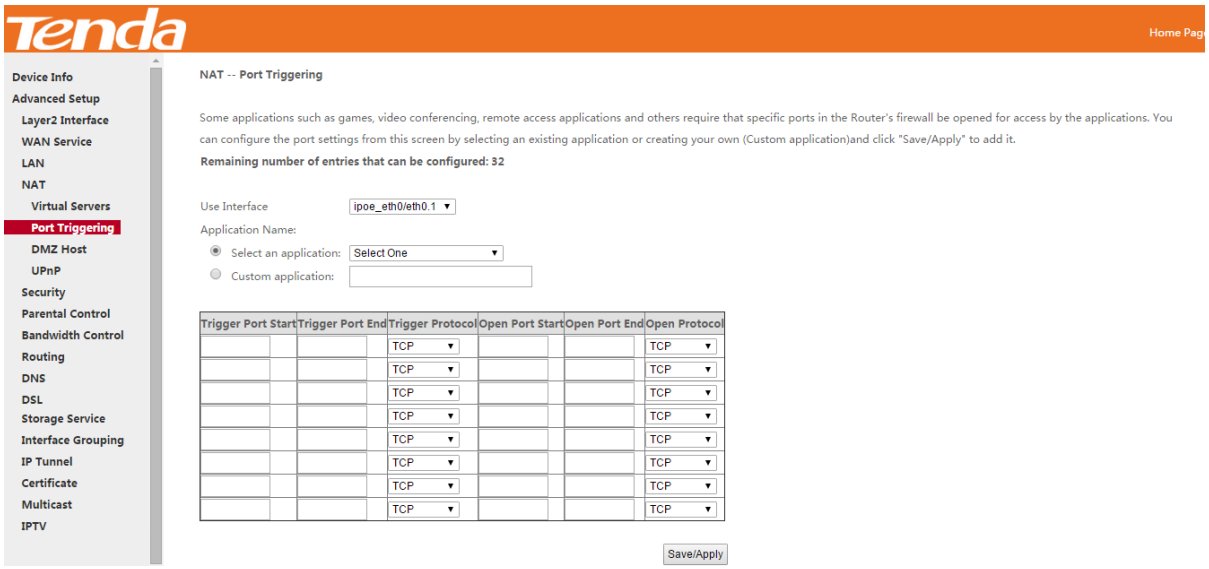
Port Triggering

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'.



To enter the Port Triggering screen, click **NAT > Port Triggering** and then click the **Add** button to add rules.

You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application) and click **Save/Apply** to add it.



Use Interface: Select a WAN connection to which you wish to apply the rules. When there is only one WAN connection available, the rules will be automatically applied to it.

Application Name: Two options are available:

Select an application: Select one from the drop-down list directly.

- Custom application: Custom application by yourself.

Trigger Port Start/Trigger Port End: The port range for an application to initiate connections.

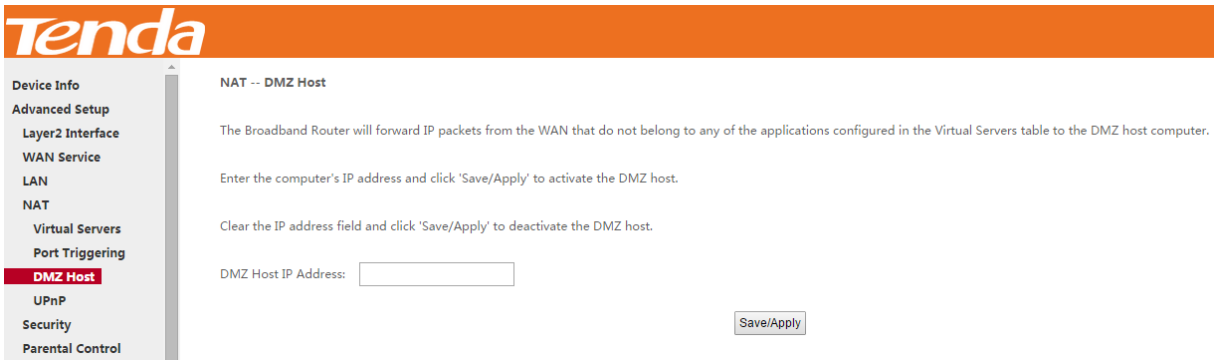
Trigger Protocol: Select the protocol from the drop-down list. If you are unsure, select TCP/UDP.

Open Port Start/ Open Port End: These are the starting number and ending number for the ports that will be

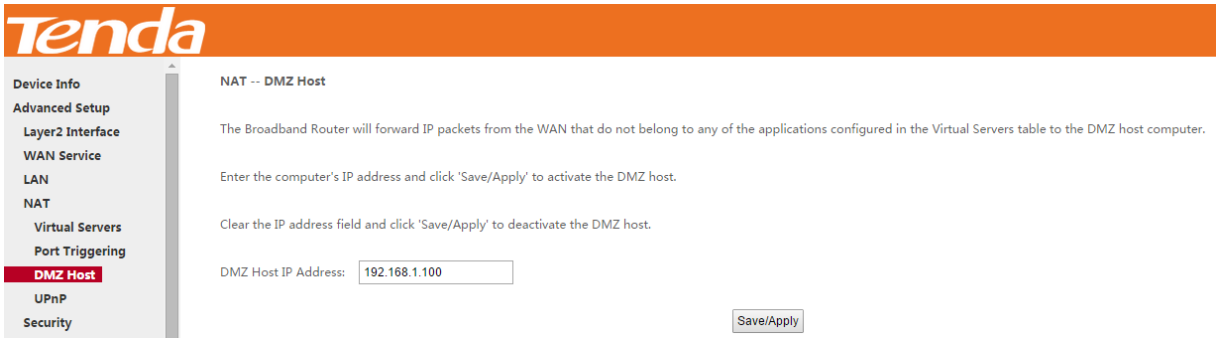
automatically opened by the built-in firewall when connections initiated by an application are established.

DMZ Host

The default DMZ (De-Militarized Zone) host feature is helpful when you are using some online games and videoconferencing applications that are not compatible with NAT (Network Address Translation).



DMZ Host IP Address: The IP Address of the device for which the router's firewall will be disabled. Be sure to assign a static IP Address to that device. The DMZ host should be connected to a LAN port of the device. Be sure to assign a static IP address to that DMZ host.

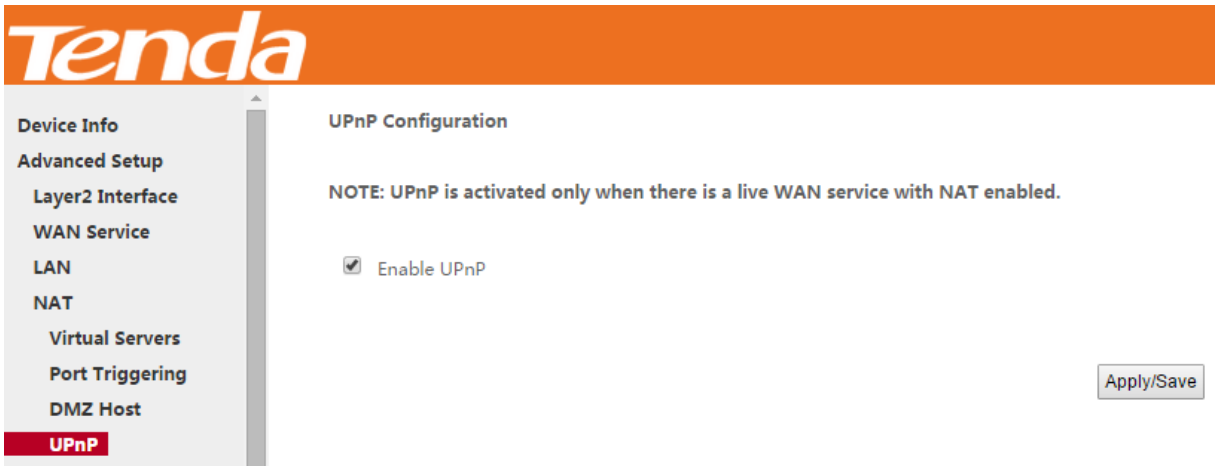


Warning!

DMZ servers pose a security risk. A computer designated as the DMZ server loses much of the protection of the firewall and is exposed to exploits from the Internet.

UPnP

UPnP (Universal Plug and Play) allows Windows based systems to configure the device for various Internet applications automatically. UPnP devices can automatically discover the services from other registered UPnP devices on the network. If you use applications such as multiplayer gaming, peer-to-peer connections, or real-time communications, like instant messaging or remote assistance (a feature in Windows XP), you should enable UPnP.



Enable UPnP: Check/uncheck to enable/disable the UPnP feature.

NOTE

UPnP is activated only when there is a live WAN service with NAT enabled.

4.2.5 Security

This section explains the following information:

• *IP Filtering*

• *MAC Filtering*

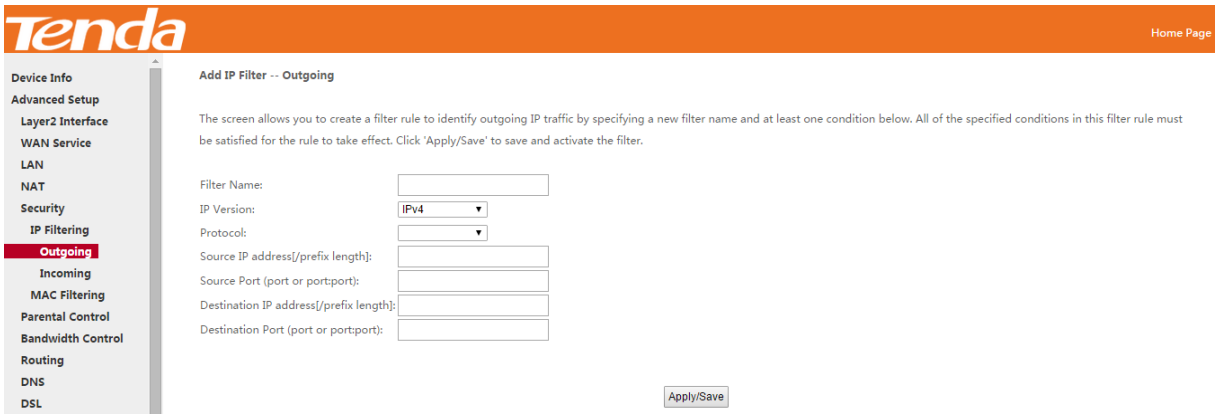
IP Filtering

Outgoing IP Filtering Setup

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be BLOCKED by setting up filters.

Choose **Add** or **Remove** to configure outgoing IP filters.

Choose **Add** to enter the following screen:



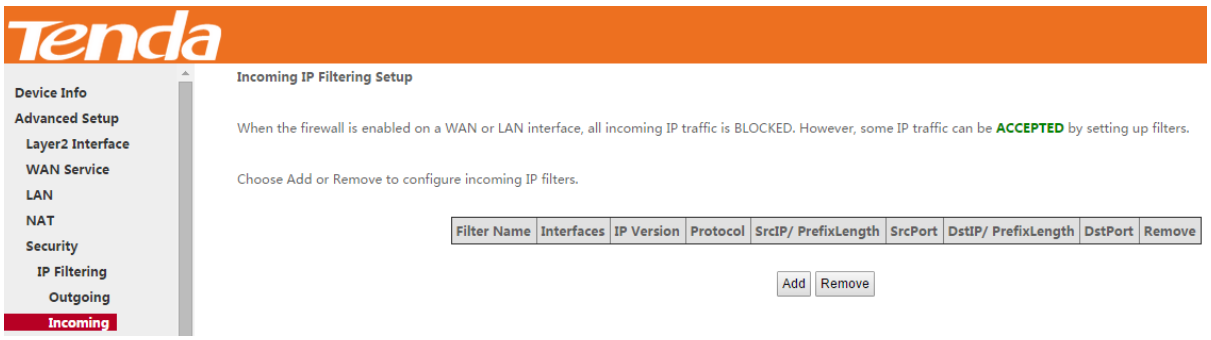
This screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click Apply/Save to save and activate the filter.

- **Filter Name:** Enter a descriptive filtering name.
- **IP Version:** Support IPv4.
- **Protocol:** TCP/UDP, TCP, UDP and ICMP are available for your option.
- **Source IP address [/prefix length]:** Enter the LAN IP address to be filtered.
- **Source Port (port or port: port):** Specify a port number or a range of ports used by LAN PCs to access the Internet. If you are unsure, leave it blank.
- **Destination IP address [/prefix length]:** Specify the external network IP address to be accessed by specified LAN PCs.
- **Destination Port** (port or port:port)**:** Specify a port number or a range of ports used by LAN PCs to access external network.

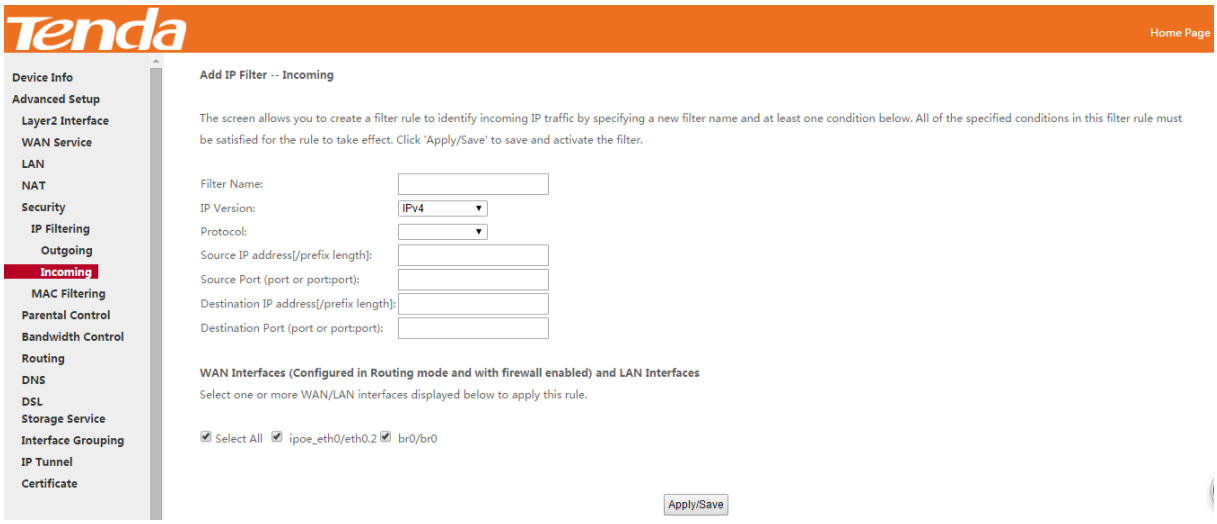
Incoming IP Filtering Setup

When the firewall is enabled on a WAN or LAN interface, all incoming IP traffic is BLOCKED. However, some IP traffic can be **ACCEPTED** by setting up filters.

Choose **Add** or **Remove** to configure incoming IP filters.



Click **Add** to enter the following screen:



This screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click Apply/Save to save and activate the filter.

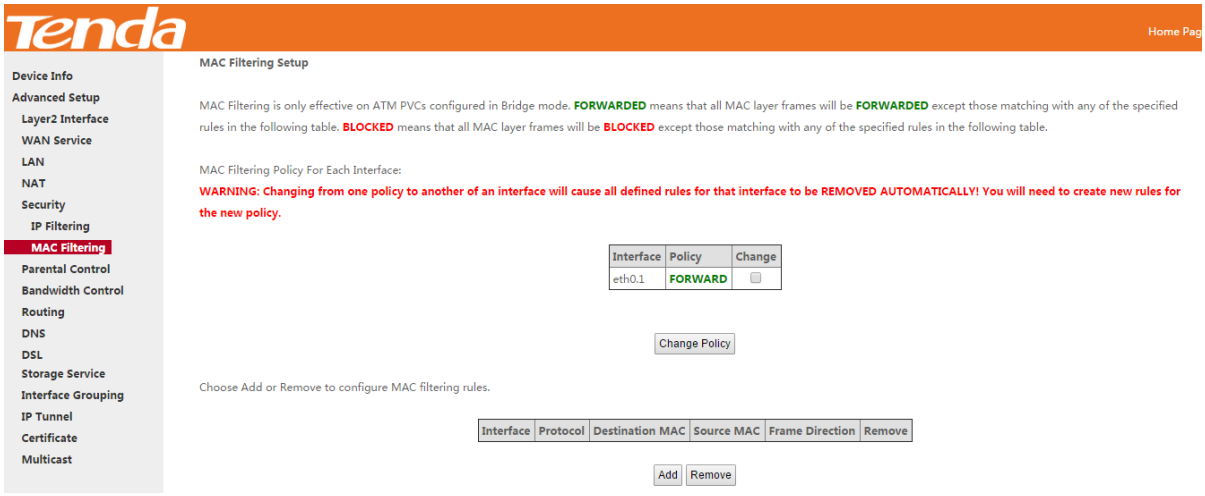
- **IP Version:** Select IP version.
- **Protocol:** TCP/UDP, TCP, UDP and ICMP are available for your option.
- **Source IP address [/prefix length]:** Enter the Internal IP address [/prefix length] to be filtered.
- **Source Port (port or port: port):** Specify a port number or a range of ports used by PCs from external network to access your internal network.
- **Destination IP address [/prefix length]:** Specify the internal network IP address [/prefix length] to be accessed by the specified PCs from external network.
- **Destination Port** (port or port:port)**:** Specify a port number or a range of ports used by PCs from external network to access your internal network.

MAC Filtering

A bridge WAN service is needed to configure this service.

MAC Filtering is only effective on ATM PVCs configured in Bridge mode. FORWARDED means that all MAC layer frames will be forwarded except those matching with any of the specified rules in the following table. BLOCKED means that all MAC layer frames will be blocked except those matching with any of the specified rules in the following table.

Choose **Add** or **Remove** to configure MAC filtering rules.



Warning!

Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.

Click **Add** to enter the following screen:

Here you can create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click **Save/Apply** to save and activate the filter.

Protocol Type: Select a protocol type from the drop-down list.

Destination MAC Address: Enter the MAC address of data frame being restricted to arrive.

Source MAC Address: Enter the MAC address of data frame being restricted to come.

Frame Direction: Select a frame direction from the drop-down list.

WAN Interfaces: Select a WAN interface from the drop-down list.

4.2.6 Parental Control

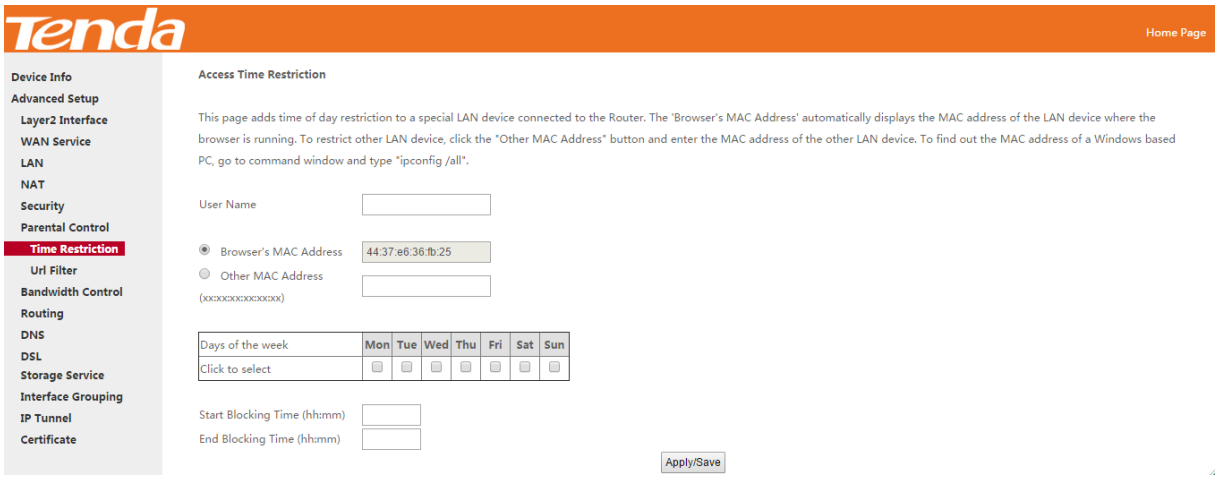
This section explains the following information:

• *Time Restriction*

• *URL Filter*

Time Restriction

Click **Parental Control > Time Restriction > Add** to enter the following screen.



Here you can add time of day restriction that an attached LAN device can access the Internet.

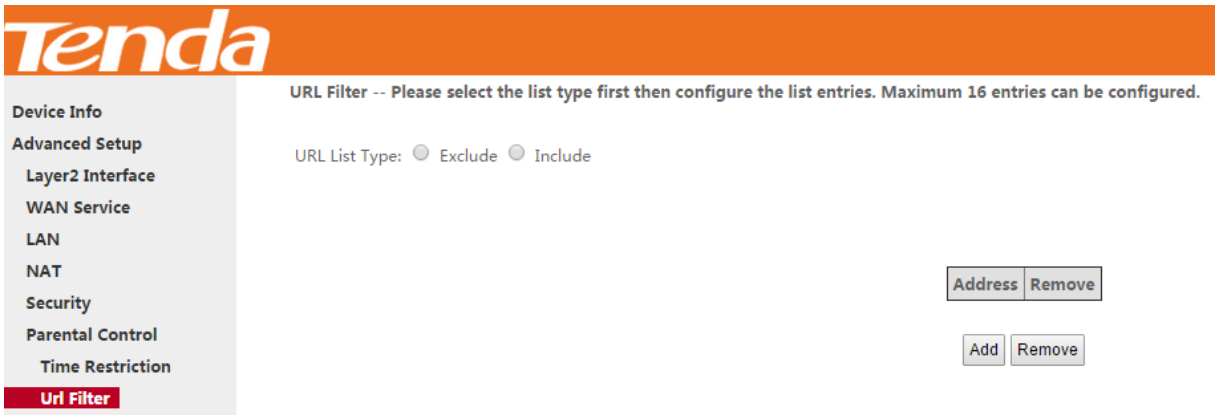
The Browser's MAC Address automatically displays the MAC address of the LAN device where the browser is running.

To restrict other LAN device, check the "Other MAC Address" option and enter its MAC address.

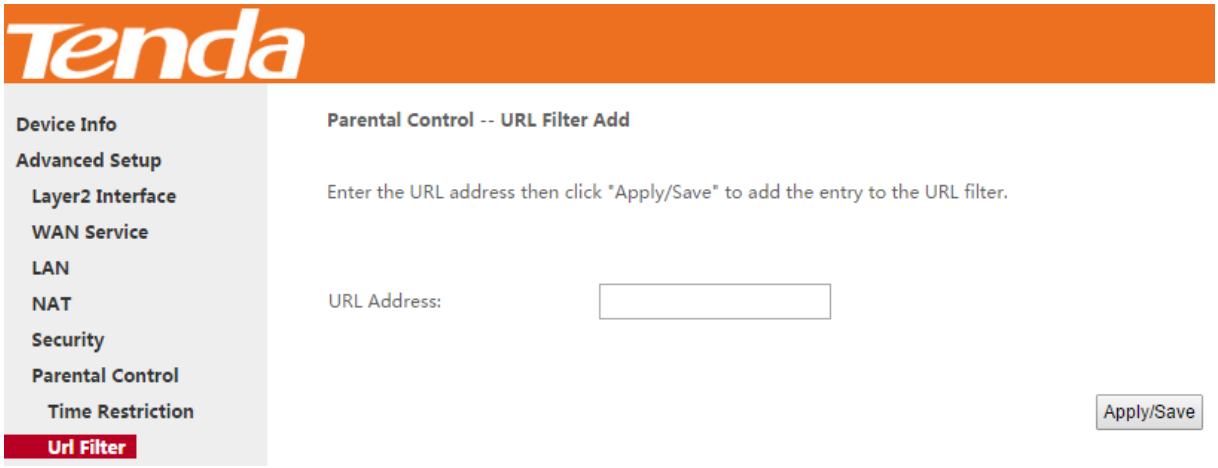
- **User Name:** Enter a user name.
- **Browser's MAC Address:** Automatically adds the MAC address of the attached LAN device where the browser is running.
- **Other MAC Address:** Specify the MAC address of the computer that you want to apply Internet access restriction.
- **Days of the week:** Click to select the days of the week during which you wish to restrict Internet access.
- **Start Blocking Time/ End Blocking Time:** Specify time of day restriction to an attached LAN device. Within this specified time length of the day, this LAN device will be blocked from the Internet.
- **Apply/Save:** Click to save and apply your settings.

URL Filter

Here you can add URL access restriction to specific LAN PCs.



Select the **URL List Type** (Exclude or Include) first and then click **Add** to enter the screen below for configuring the list entries.



URL Address: Enter a specific URL or a key word of domain name in this field.

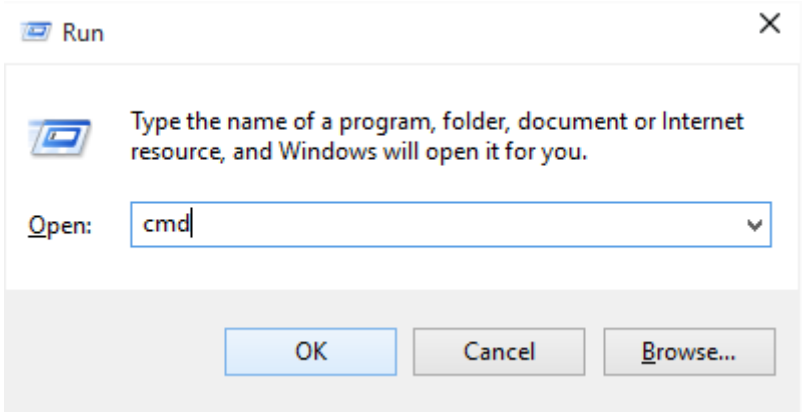
Click Apply/Save to apply and save the settings.

NOTE

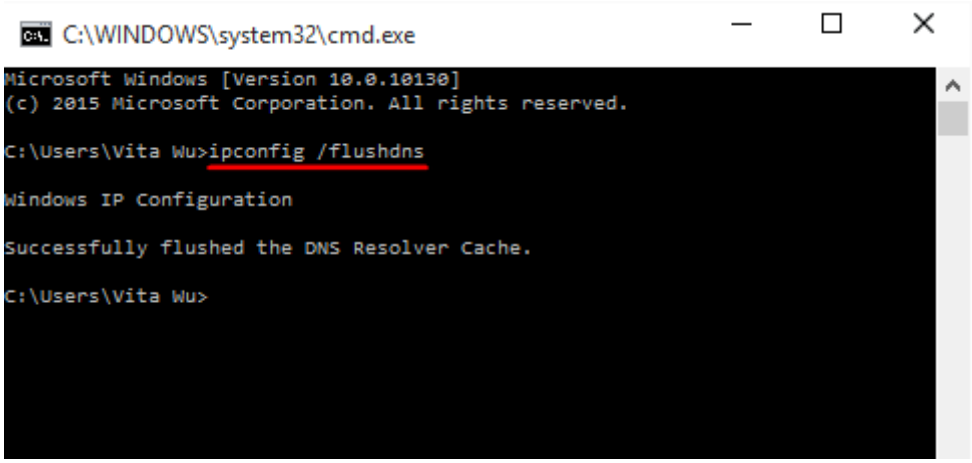
If you have accessed the URL before you include it in a URL filter rule, you must reboot the router and erase it from your PC to activate this URL filter rule. To erase the domain name from your PC:

1. Click the keys **+R** on the keyboard to enable "Run" dialog, and type **cmd** > click **OK**.

(**Note that** different operation systems may have different ways to enable "Run"; Windows is taken a guide here.)



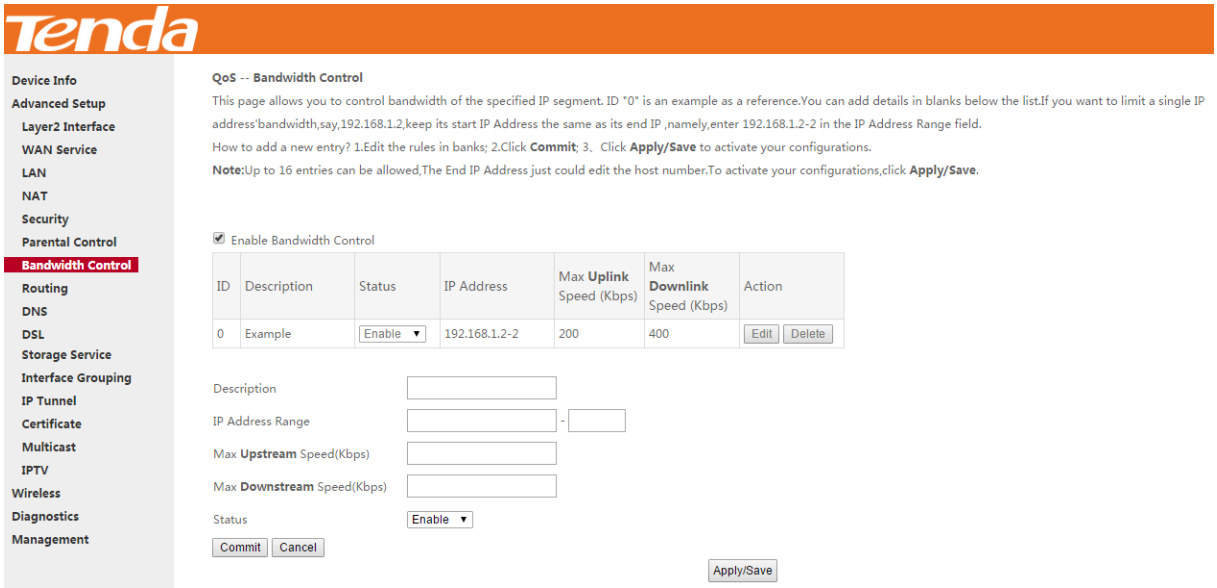
2. Then type **ipconfig /flushdns** and hit **Enter** on the keyboard.



4.2.7 Bandwidth Control

When multiple devices each of which requests a different bandwidth attach to the modem router, to ensure the attached devices obtaining a fair bandwidth and getting a fluent Internet experience, set a bandwidth control rule.

Check **Enable Bandwidth Control** to enable this feature.



Description: Name the bandwidth control rule as you like.

IP Address Range: Type the IP address range of target hosts. Follow the example 192.168.1.2 - 254.

If you want to set one host, follow the example 192.168.1.2 - 2.

Max Upstream Speed (Kbps): Set the upstream speed as your actual bandwidth need.

Max Downstream Speed (Kbps): Set the downstream speed as your actual bandwidth need.

Status: Enable or Disable.

After you have edited the details of the bandwidth control rule, click Commit first to save and then click Apply/Save to activate the settings.

4.2.8 Routing

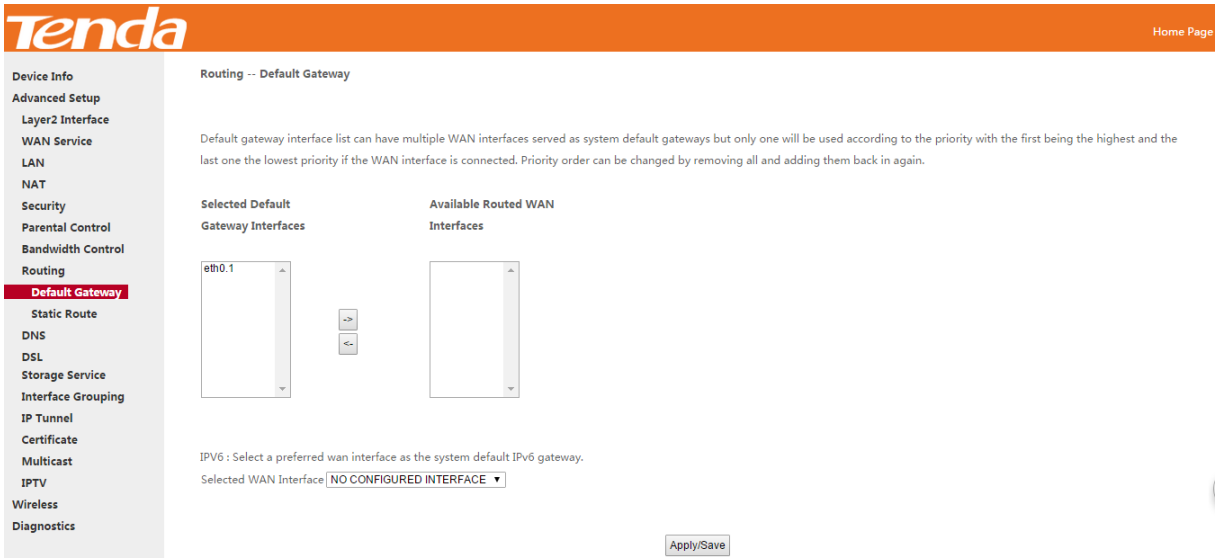
This section explains the following:

• *Default Gateway*

• *Static Route*

Default Gateway

Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

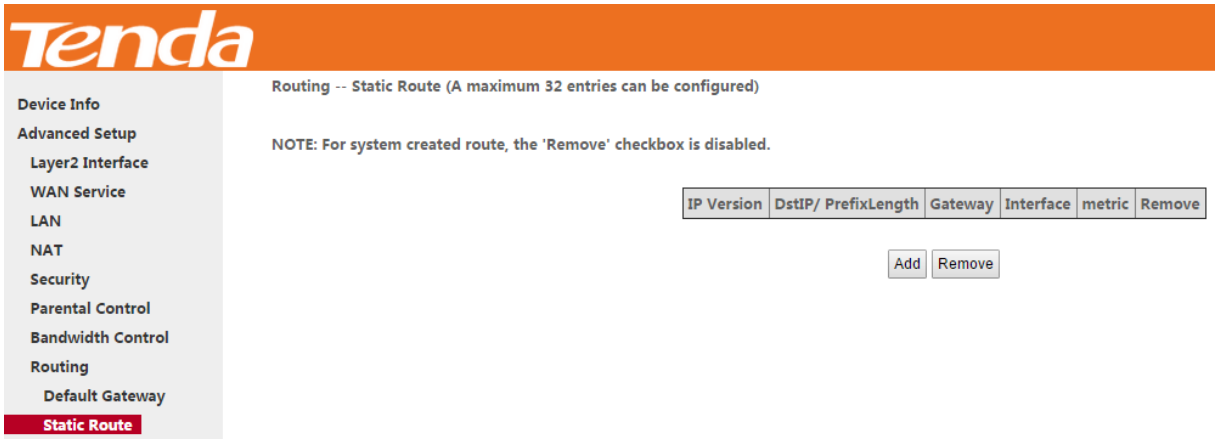


- **Selected Default Gateway Interfaces:** Displays the selected default gateway interfaces. Select a WAN interface and click the -> button to move it to the **Available Routed WAN Interfaces** box.

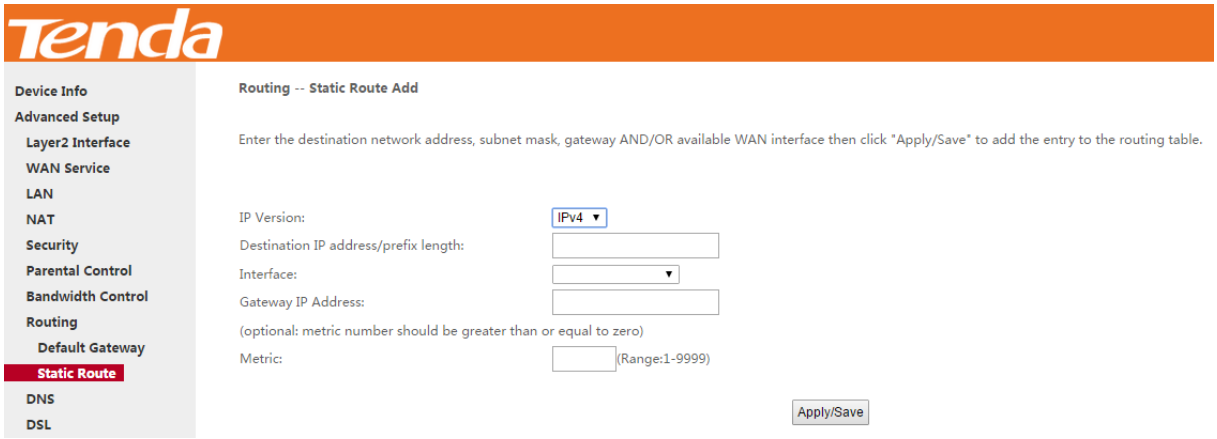
- **Available Routed WAN Interfaces:** Displays the available routed WAN interfaces. Select a WAN interface and click the <- button to add it to the **Selected Default Gateway Interfaces** box.
- **Apply/Save:** Click to save and activate your settings.

Static Route

Static routes provide additional routing information to your router. Typically, you do not need to add static routes. However, when there are several routers in the network, you may want to set up static routing. Static routing determines the path of the data in your network. You can use this feature to allow users on different IP domains to access the Internet via this device. It is not recommended to use this setting unless you are familiar with static routing. In most cases, dynamic routing is recommended, because this feature allows the router to detect the physical changes of the network layout automatically.



Click **Add** to enter the following screen:



- **IP Version:** Select IP version.
- **Destination IP address/prefix length:** Enter the destination IP address and prefix length of the final destination.
- **Interface:** Select an interface from the drop-down list.
- **Gateway IP address:** Enter the gateway IP address, which must be a router on the same LAN segment as the

router.

- **Metric:** Enter a number in the Metric field. This stands for the number of routers between your network and the destination.
- **Apply /Save:** Click to apply and save your settings.

NOTE

1. Destination IP address cannot be on the same IP segment as WAN or LAN segment as the router.

2. Only configure additional static routes for unusual cases such as multiple routers or multiple IP subnets located on your network. Wrong static routes may lead to network failure.

3. For system created route, the “Remove” checkbox is disabled.

4.2.9 DNS

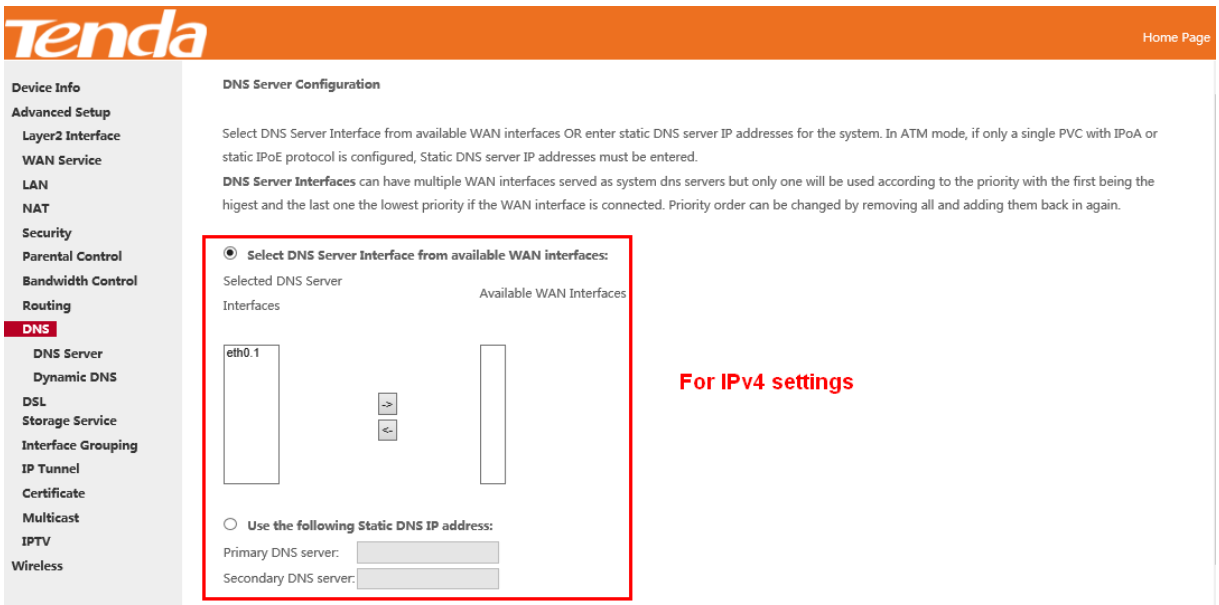
DNS Server (Static DNS)

The DNS server translates domain names to numeric IP addresses. It is used to look up site addresses based on their names. If the DNS server works incorrectly, Internet access will be blocked.

DNS server is configured when you are setting up your Internet connectivity. So, you do not have to finish DNS server setup here unless your network works false.

For IPv4

① Click **Advanced Setup** > **DNS** > **DNS Server**, and enter the screen below.

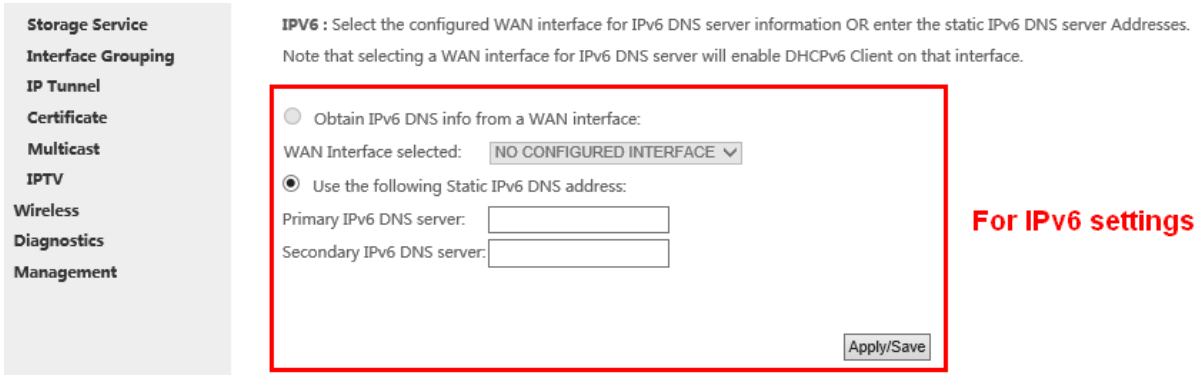


② Check the **Select DNS Server Interface from available WAN interfaces** option if the device gets a DNS address automatically from an upstream device. Or select the **Use the following Static DNS IP address** option and enter static DNS server address provided by your ISP.

③ Click **Apply/Save** at the bottom of the page.

For IPv6

① Click **Advanced Setup** > **DNS** > **DNS Server**, and enter the screen below.



② Select the **Obtain IPv6 DNS info from a WAN interface** option if the device gets a DNS server address from the upstream device automatically. And select a configured WAN interface for the IPv6 DNS server information. Or select the **Use the following Static IPv6 DNS address** option and enter the static IPv6 DNS server address provided by your ISP.

③ Click **Apply/Save**.

NOTE

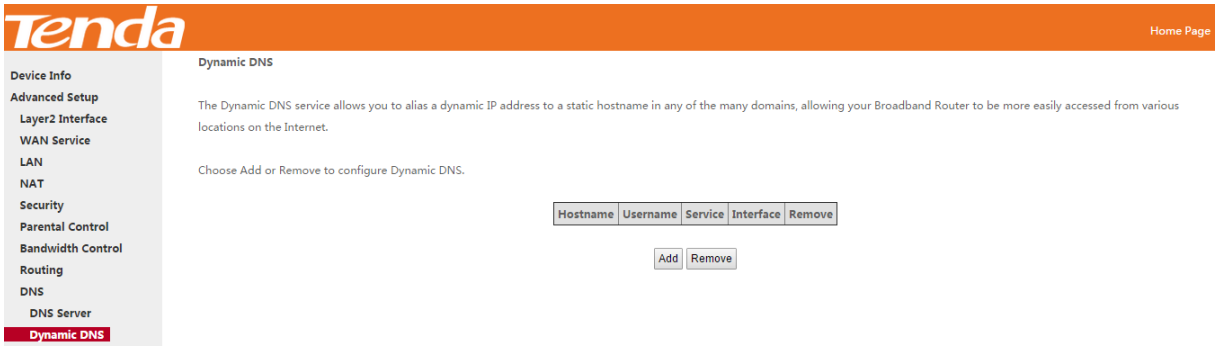
1. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.
2. If you are not clear about the static DNS server IP information, ask your ISP to provide it.
3. The default settings are recommended if you are unsure about the DNS server addresses. If a wrong DNS server address is configured, webpages may not be open.

Dynamic DNS (DDNS)

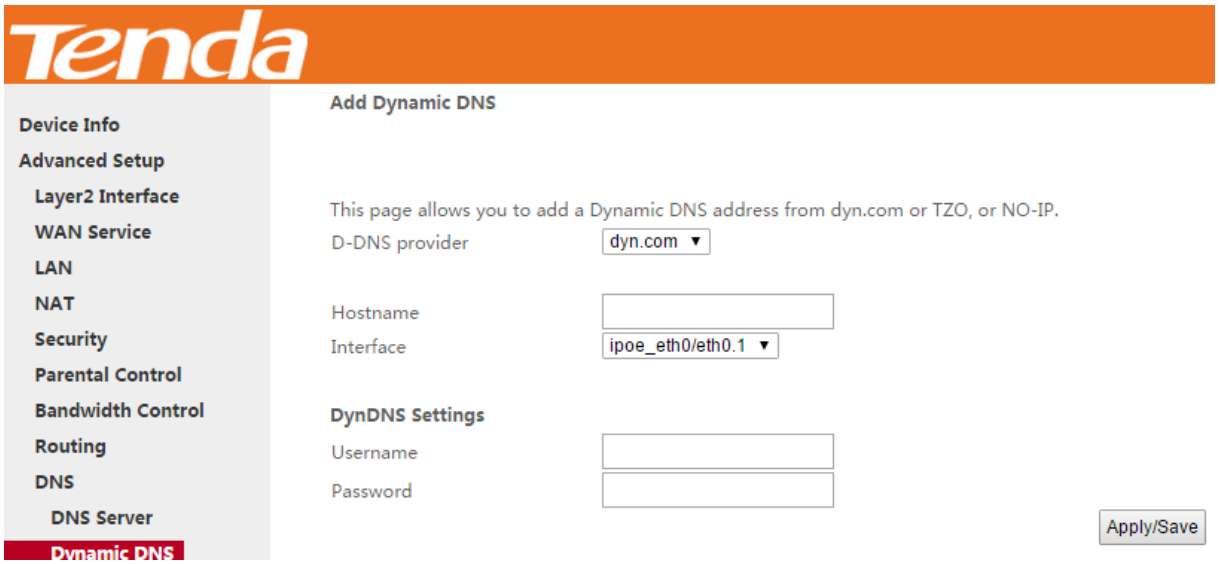
If your Internet service provider (ISP) gave you a static (fixed) public IP address, you can register a domain name and have that name associated with your IP address by public Domain Name Servers (DNS). However, if your ISP gave you a dynamic (changing) public IP address, you cannot predict what your IP address will be, and the address can change frequently. In this case, you can use a commercial Dynamic DNS service. It allows you to register your domain to their IP address and forward traffic directed at your domain to your frequently changing IP address. If your ISP assigns a private WAN IP address (such as 192.168.x.x or 10.x.x.x), the Dynamic DNS service does not work because private

addresses are not routed on the Internet.

Click **Advanced Setup** > **DNS** > **Dynamic DNS** to enter the Dynamic DNS screen.



Click Add to configure the DDNS settings.



D-DNS Provider: Select your DDNS service provider from the drop-down menu.

Hostname: Enter the DDNS domain name registered with your DDNS service provider.

Interface: Specify a WAN connection interface.

Username: Enter the DDNS user name registered with your DDNS service provider.

Password: Enter the DDNS Password registered with your DDNS service provider.

Click Apply/Save to save your settings.

Example: dyn.com

Hostname: tenda.dyndns.org

Username: tenda

Password: 123456789

Add Dynamic DNS

① Select **dyn.com** from the **D-DNS provider** drop-down menu.

② Enter the hostname. Here is “tenda.dyndns.org” for example.

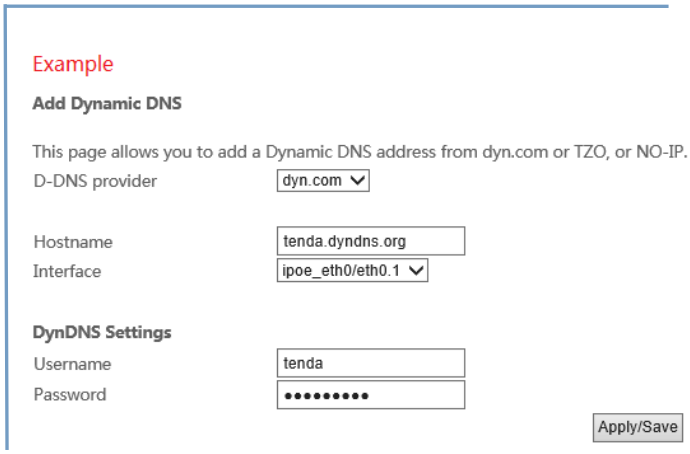
③ Specify a WAN connection interface.

DynDNS Settings

④ Enter your DynDNS username. Here is “tenda” for example.

⑤ Enter the password of DynDNS account. Here is “123456789” for example.

⑥ Click Apply/Save to save your configuration.

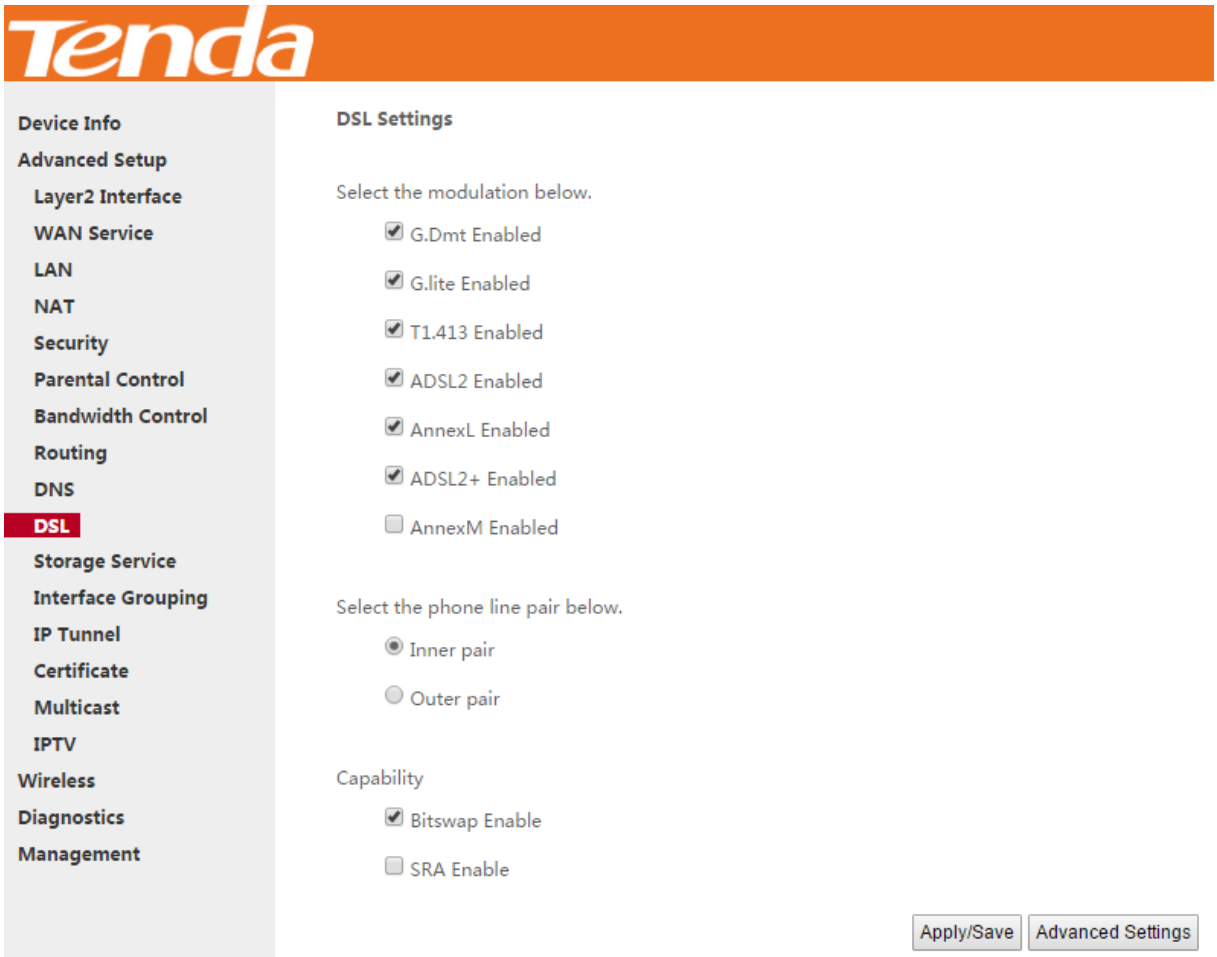


4.2.10 DSL

This screen provides multiple ASDL modulation modes to meet diversified environments. You can also select phone line pair and Capability.

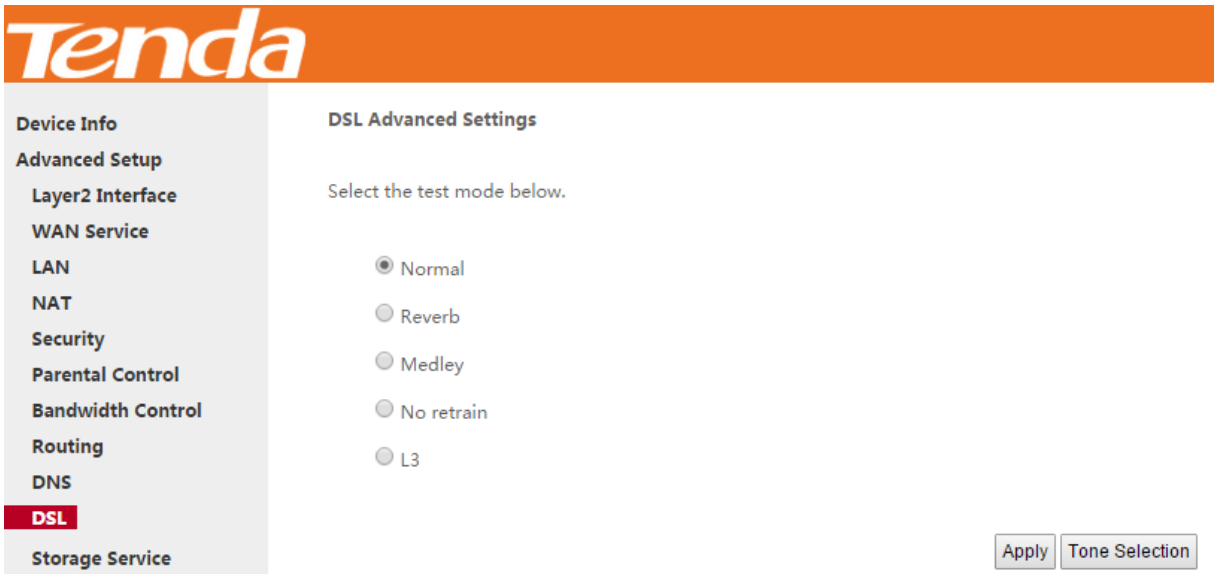
DSL parameter configurations must be supported by ISP to take effect. Actual parameters (see Statistics-DSL) resulted from the negotiation between your router and ISP. Wrong configurations may fail your Internet access.

The best DSL configurations are the factory defaults. Only change them with the support of your ISP or our technical staff when your router fails to negotiate with ISP in DSL (ATM) mode.



Check the checkbox next to a modulation to enable it and then click Apply/Save.

Advanced Settings: Click it to enter the Advanced Settings screen as below.



Here you can select the test mode and tone.

TIP

If you are unsure about the DSL parameters, please apply the factory default settings. Wrong configurations may fail your Internet access.

4.2.11 Storage Service

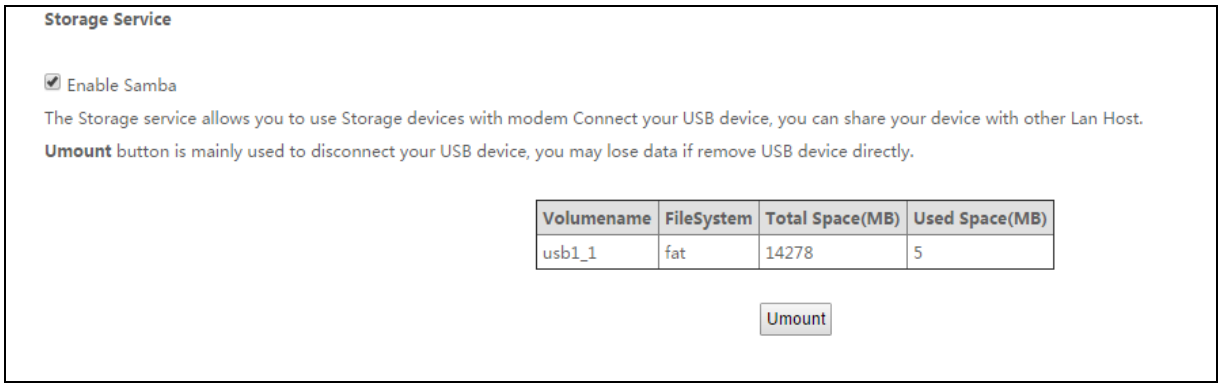
This section explains the following:

- *Storage Device Info*
- *User Account*

The modem router provides a USB port. You can attach a USB storage device to it and share your USB device with a user in the LAN.

Storage Device Info

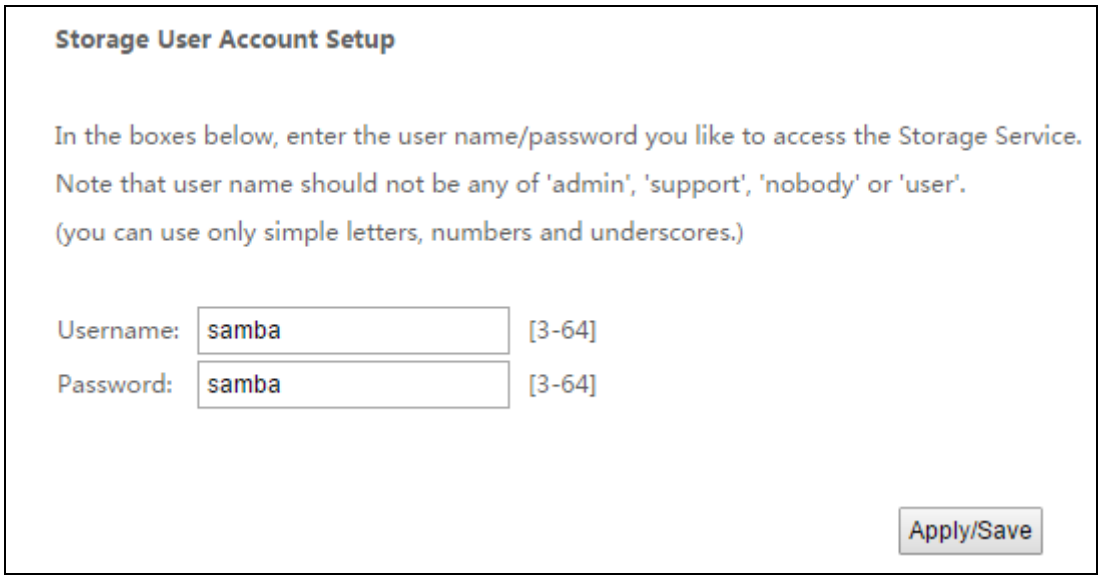
Once you plug your USB storage device into the USB port, the details about the USB storage will be recorded shown as below table.



Click Umount and then uplug your USB device. Removing directly may damage your USB storage device.

User Account

Accessing the USB storage device requires an account. You can click Apply/Save to use the default account or you can customize a new one. Pay attention to that your computer system will record the account you used at the first time.



Application: How to access the USB storage device attached to the modem router?

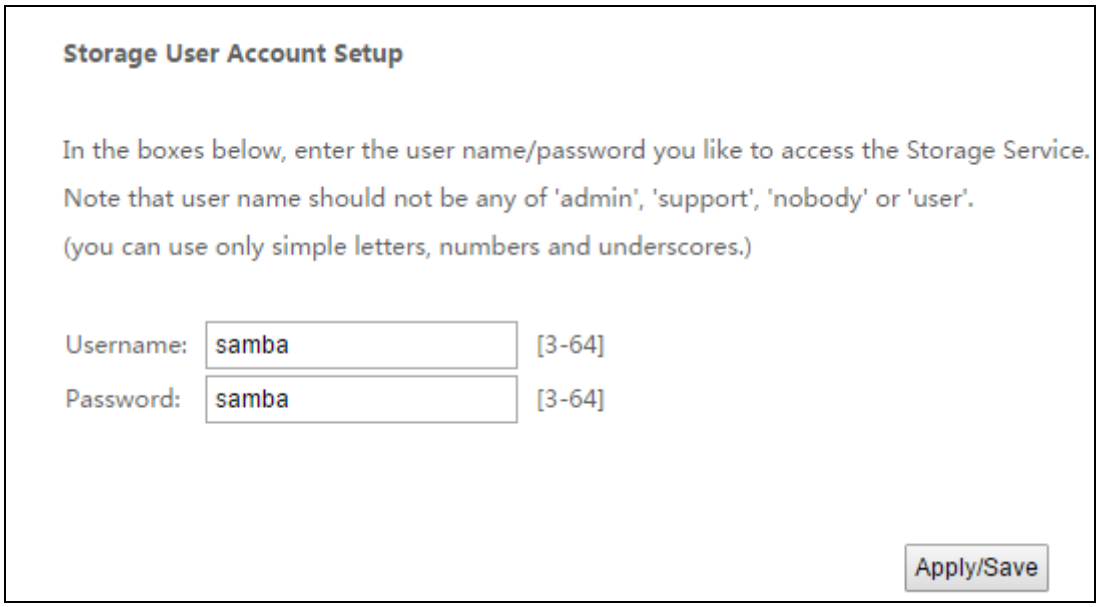
Step 1: Plug USB storage device.

Plug your USB storage device into the USB port, and make sure the USB LED indicator is on.

Step 2: Create an account.

Go to **User Account** interface, and set up your account. Here the default account “samba” is kept. And click Apply/Save

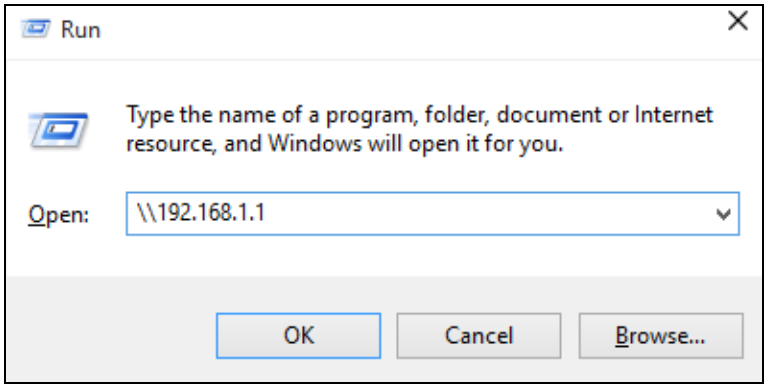
to save and apply.



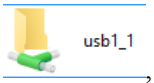
Step 3: Access the USB storage device from a computer.

Click **+R** on the keyboard to pop up the **Run** dialog, and type \\192.168.1.1 in the blank field.

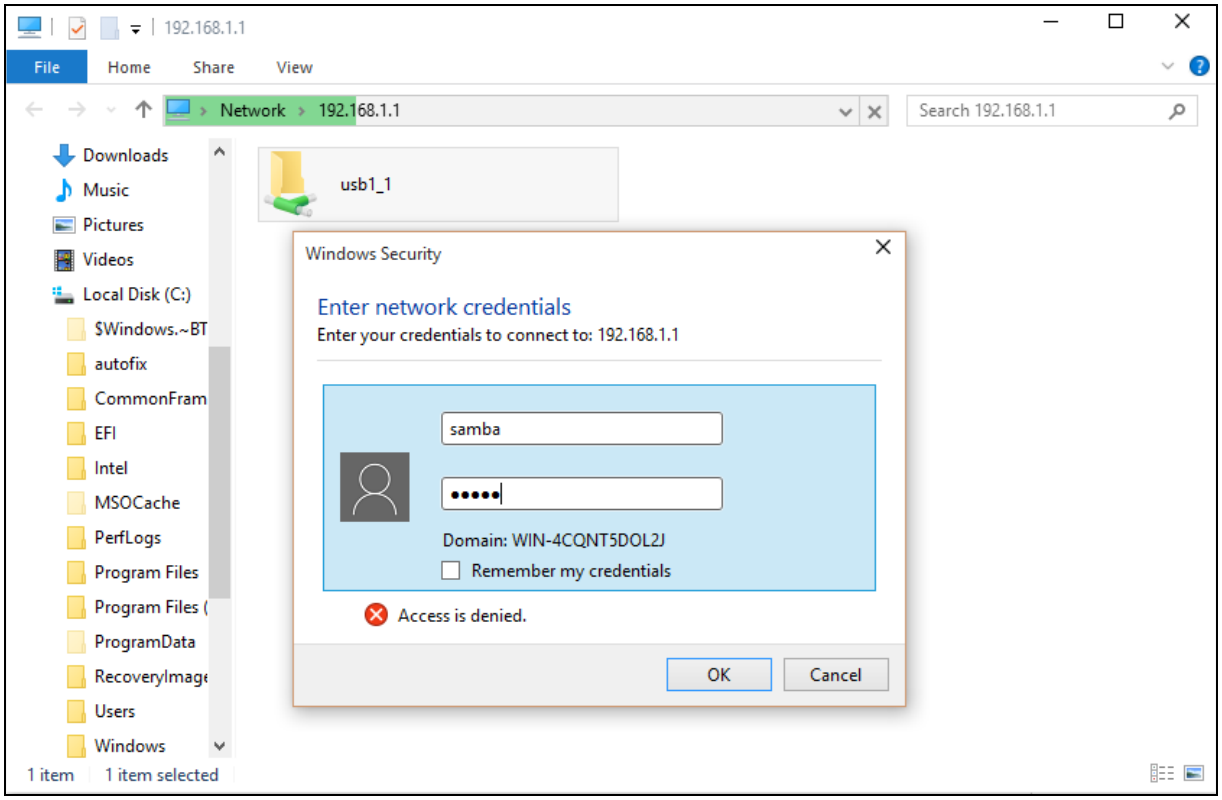
Click **OK**.



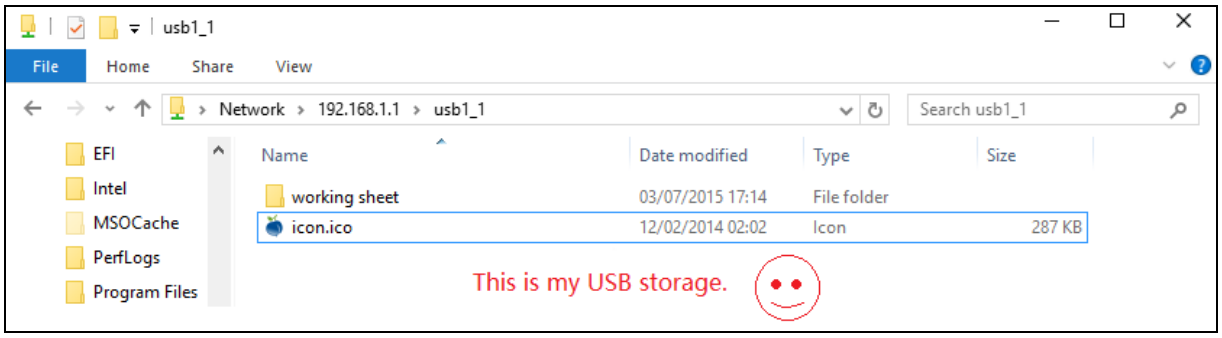
Step 4: Access the USB storage device with the account “samba”.

Double click 

, and enter your account “samba” and password to finish the credentials. Then, click **OK**.

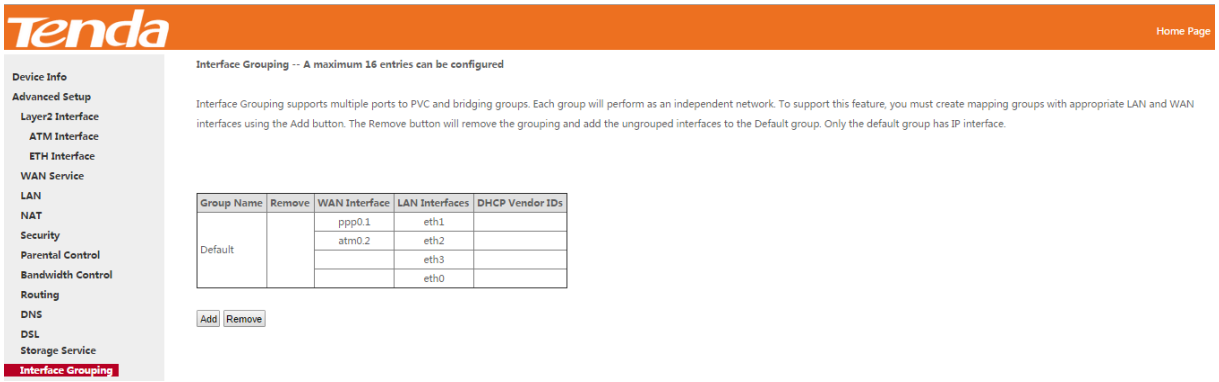


Access successfully!

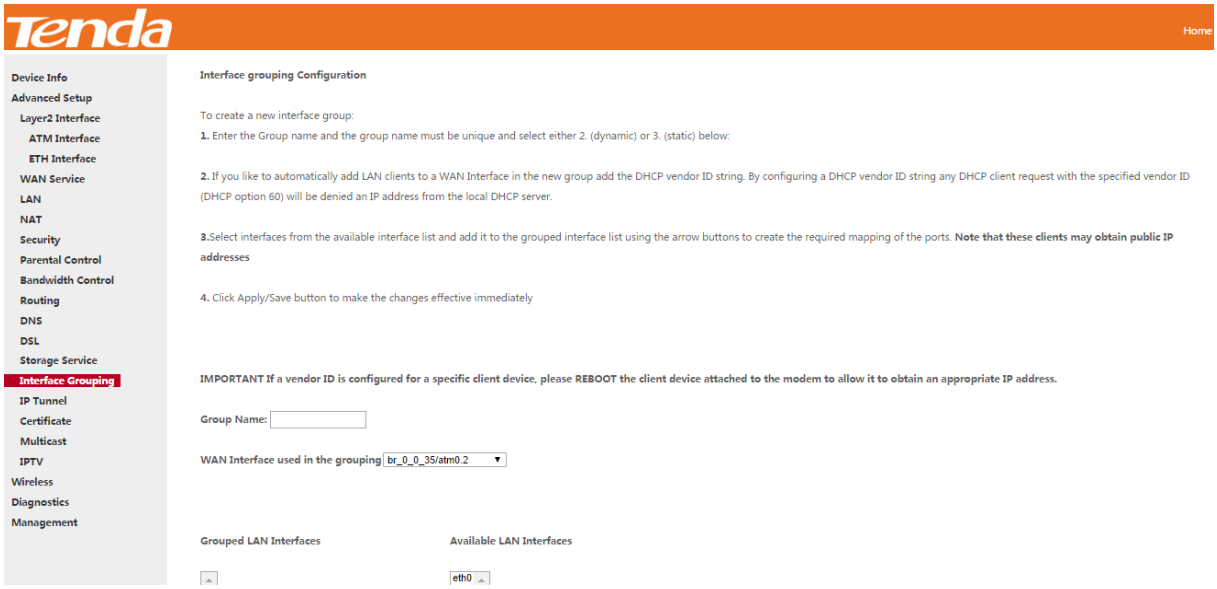


4.2.12 Interface Grouping

Interface Grouping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the **Add** button. The **Remove** button will remove the grouping and add the ungrouped interfaces to the Default group.



Click **Add** to enter the screen below:



- **Group Name:** Define a name for group.
- **WAN Interface used in the grouping:** WAN connection to which the interface grouping rules apply.
- **Available LAN Interfaces:** LAN interfaces which are available for interface grouping.
- **Grouped LAN Interfaces:** LAN interfaces which are classed into the specified WAN connection.

To create a new interface group:

① Enter the Group name and the group name must be unique.

② Select an available WAN interface for the LAN network proxy.

③ Define the available LAN interface to connect to the specified WAN interface. Select interfaces from the **Available LAN Interfaces** list and add it to the **Grouped LAN Interfaces** list using the arrow buttons to create the required mapping of the ports.

④ Click **Apply/Save** button to make the changes effective immediately.

If you want to bypass NAT via the router's interface and obtain the public IP address automatically, you need to add the DHCP vendor ID in the **Automatically Add Clients with the following DHCP Vendor IDs** section. After the ID takes effect, your router will automatically detect the DHCP request from computers on the LAN, and it will forward the DHCP vendor ID and the corresponding DHCP request to the WAN interface used in the interface rules.

NOTE

1. Eth0, eth1, eth2 and eth3 respectively represent 1/WAN, 2, 3 and 4/iTV port of the device. And wlan0 is the port for all wireless devices connecting to the modem router.
2. If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address.
3. No Interface/None indicates that there is no WAN port.

4.2.13 IP Tunnel

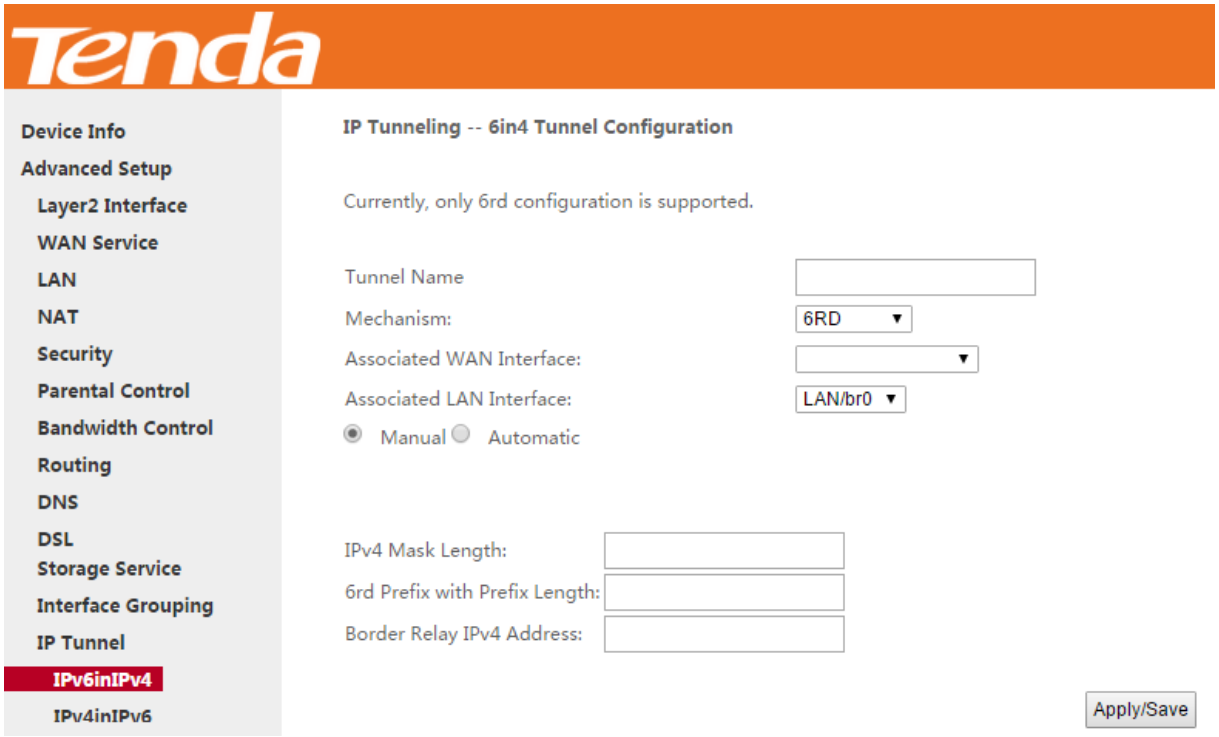
This section explains the following information:

• *IPv6inIPv4*

• *IPv4inIPv6*

IPv6inIPv4

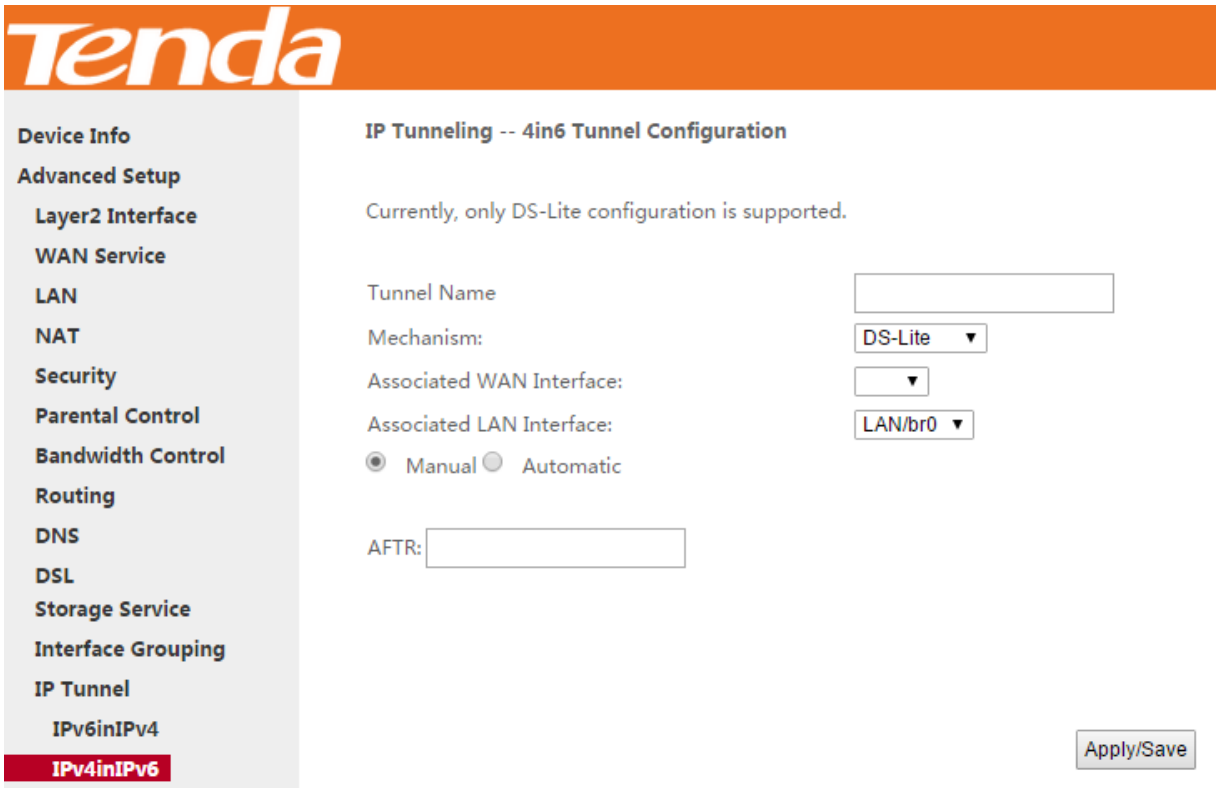
Click **IPv6inIPv4** and **Add** to enter the following screen:



- **Tunnel Name:** Specify the name of the tunnel.
- **Mechanism:** Currently, only 6RD configuration is supported.
- **Associated WAN Interface:** Specify the WAN interface of the tunnel.
- **Associated LAN Interface:** Specify the LAN interface of the tunnel.
- **Manual:** If you select Manual, configure the following settings also:
  - **IPv4 Mask Length:** Specify the IPv4 Mask Length.
  - **6rd Prefix with Prefix Length:** Specify the 6rd Prefix with Prefix Length.
  - **Border Relay IPv4 Address:** Specify the Border Relay IPv4 Address.
- **Automatic:** If Automatic is selected, no configurations are required.
- **Apply/Save:** Click to apply and save your settings.

IPv4inIPv6

Click **IPv4inIPv6** and **Add** to enter the following screen:



- **Tunnel Name:** Specify the name of the tunnel.
- **Mechanism:** Currently, only DS-Lite configuration is supported.
- **Associated WAN Interface:** Specify the WAN interface of the tunnel.
- **Associated LAN Interface:** Specify the LAN interface of the tunnel.
- **Manual:** If you select Manual, enter the AFTR information also:
- **Automatic:** If Automatic is selected, no configurations are required.
- **Apply/Save:** Click to apply and save your settings.

4.2.14 Certificate

This section explains the following information:

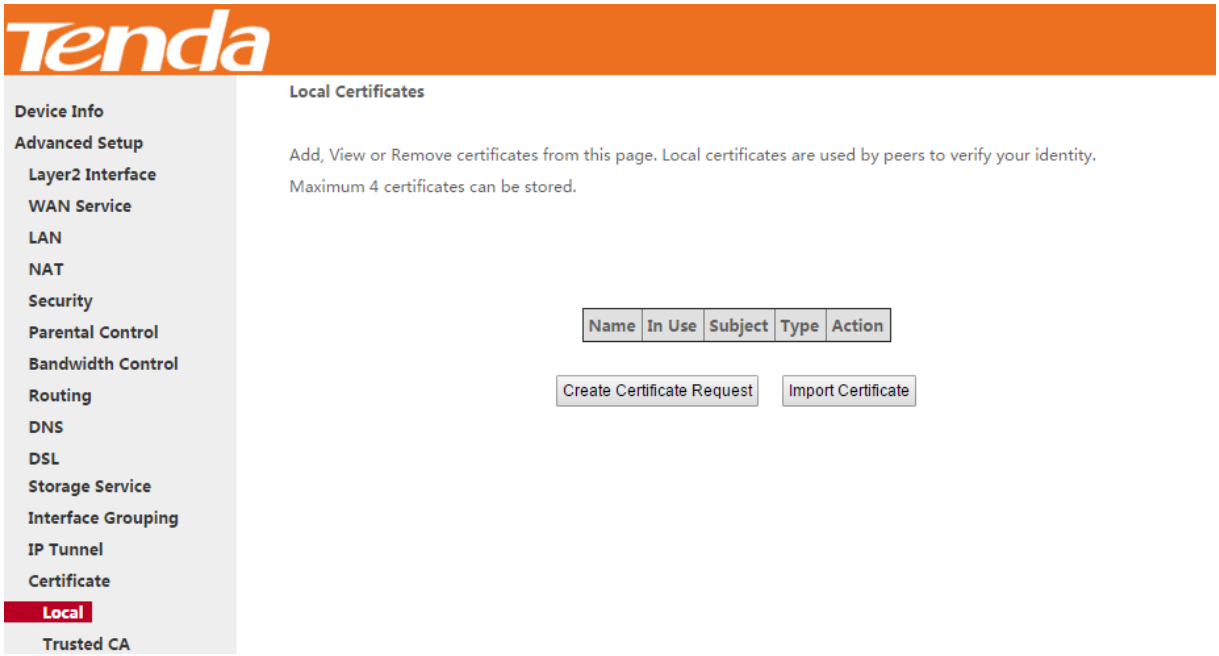
• *Local Certificates*

• *Trusted CA (Certificate Authority) Certificates*

Local Certificates

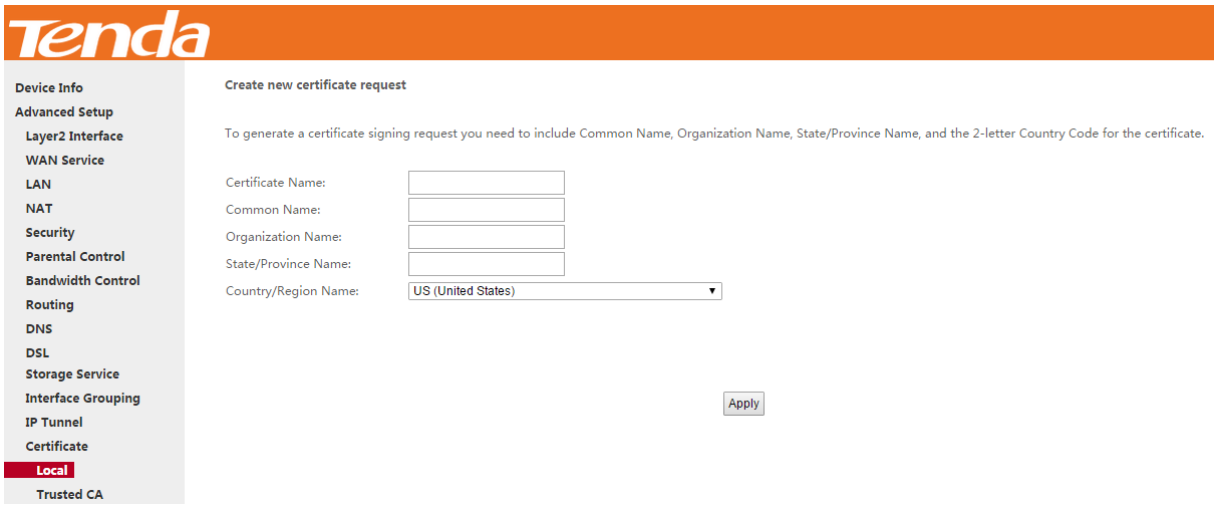
Here you can add, view or remove certificates. Local certificates are used by peers to verify your identity. Maximum 4

certificates can be stored.



To generate a certificate signing request:

① Click the **Create Certificate Request** button to enter the page below.



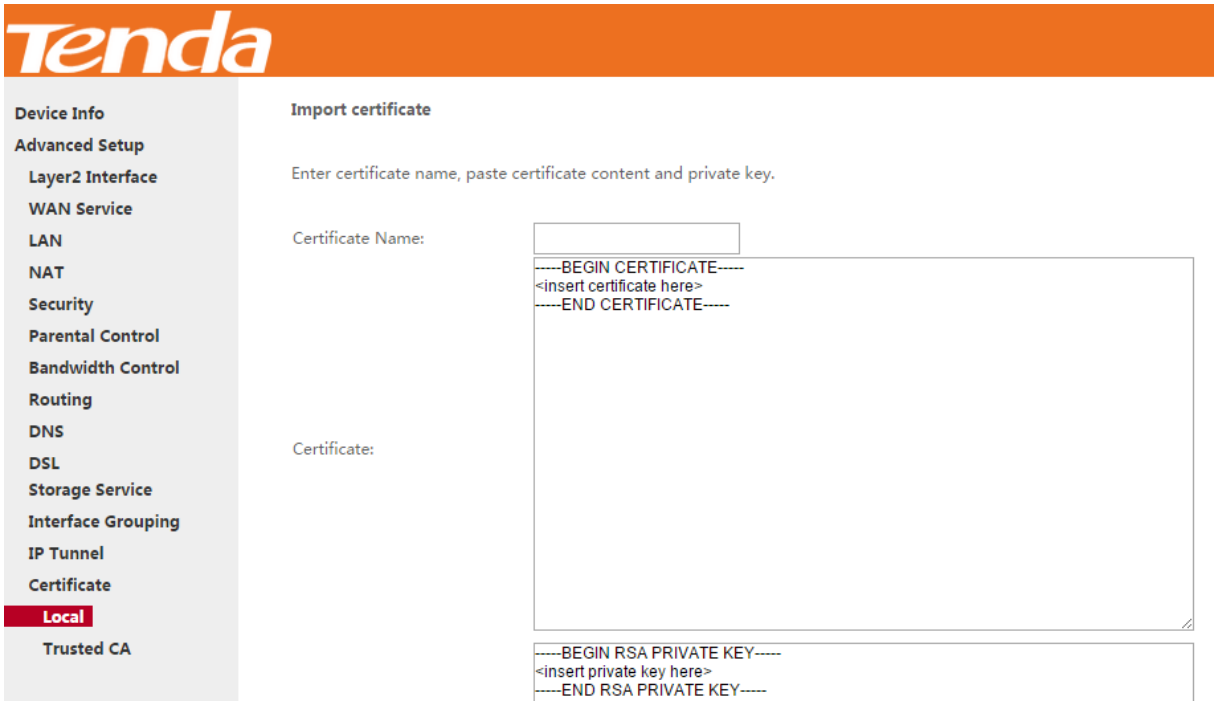
② Specify the Common Name, Organization Name and State/Province Name

③ Enter the 2-letter Country Code for the certificate.

④ Click **Apply** to apply your settings.

To Import certificate：

① Click the **Import Certificate** button on the local certificates page to enter the page below.



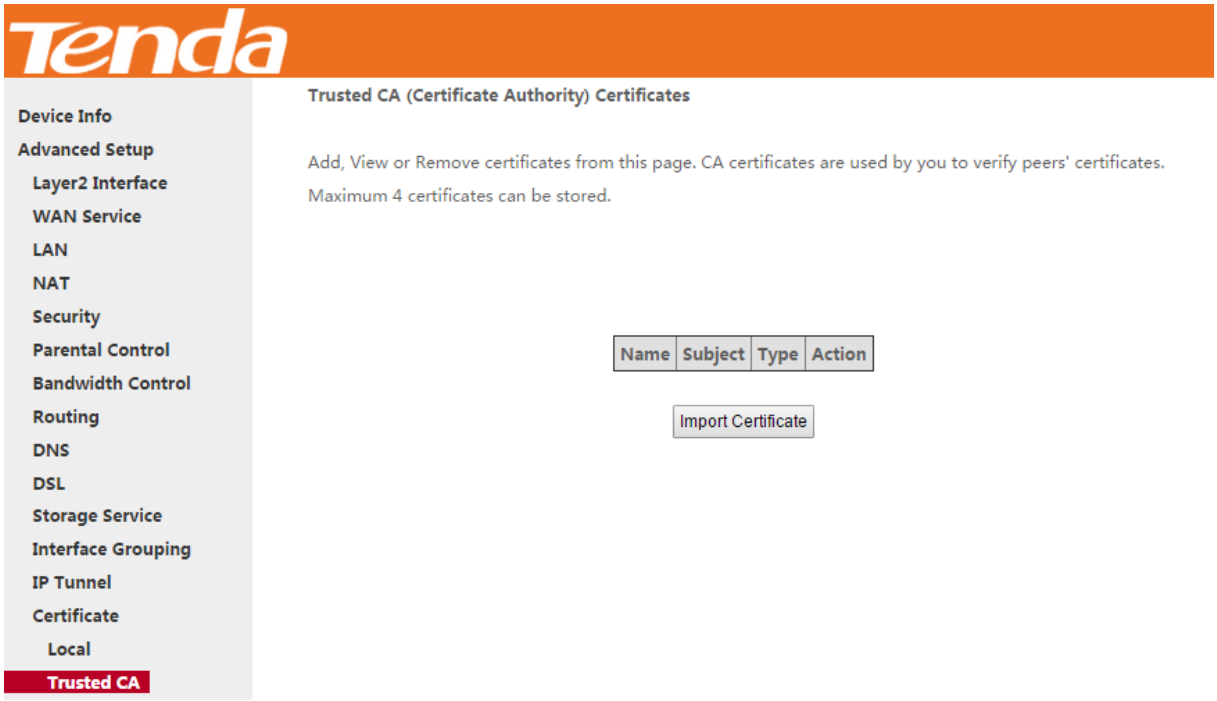
② Enter the certificate name.

③ Paste the certificate content and private key.

④ Click **Apply** to apply your settings.

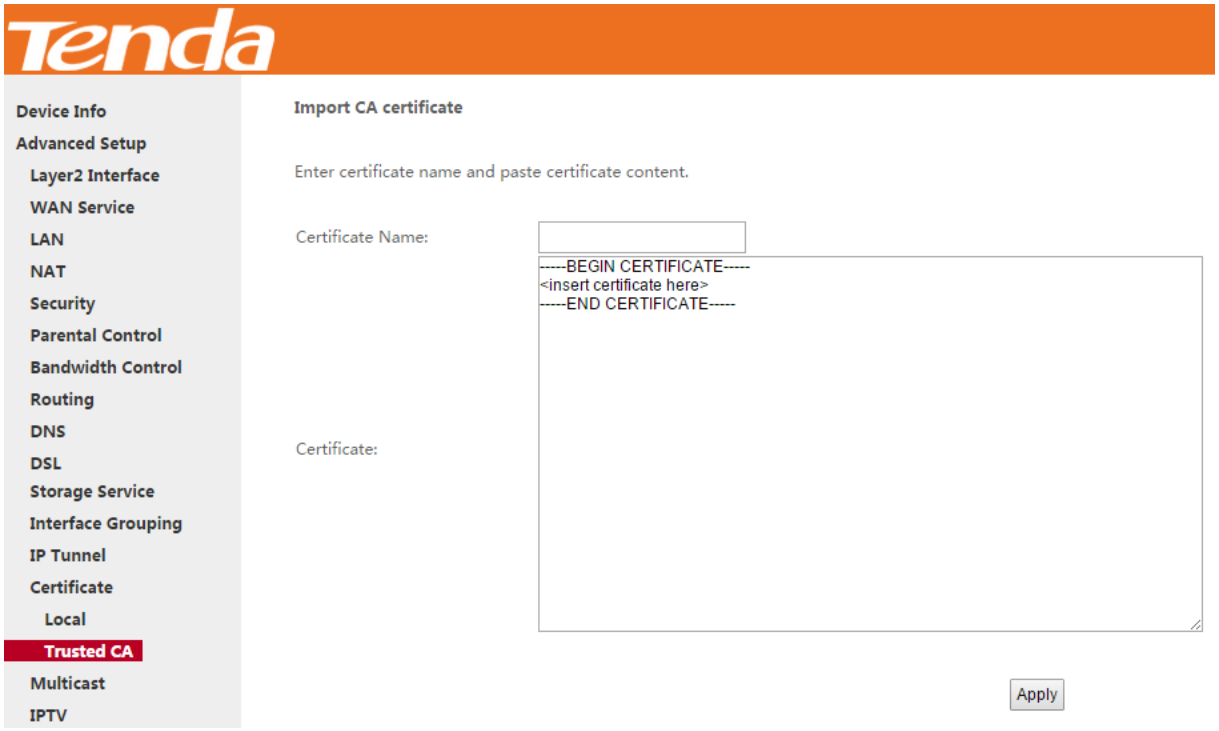
Trusted CA (Certificate Authority) Certificates

Here you can add, view or remove CA certificates. CA certificates are used by you to verify peers' certificates. Maximum 4 certificates can be stored.



To Import certificate:

① Click the **Import Certificate** button to enter the page below.



② Enter the certificate name.

③ Paste the certificate content.

④ Click **Apply** to apply your settings.

4.2.15 Multicast

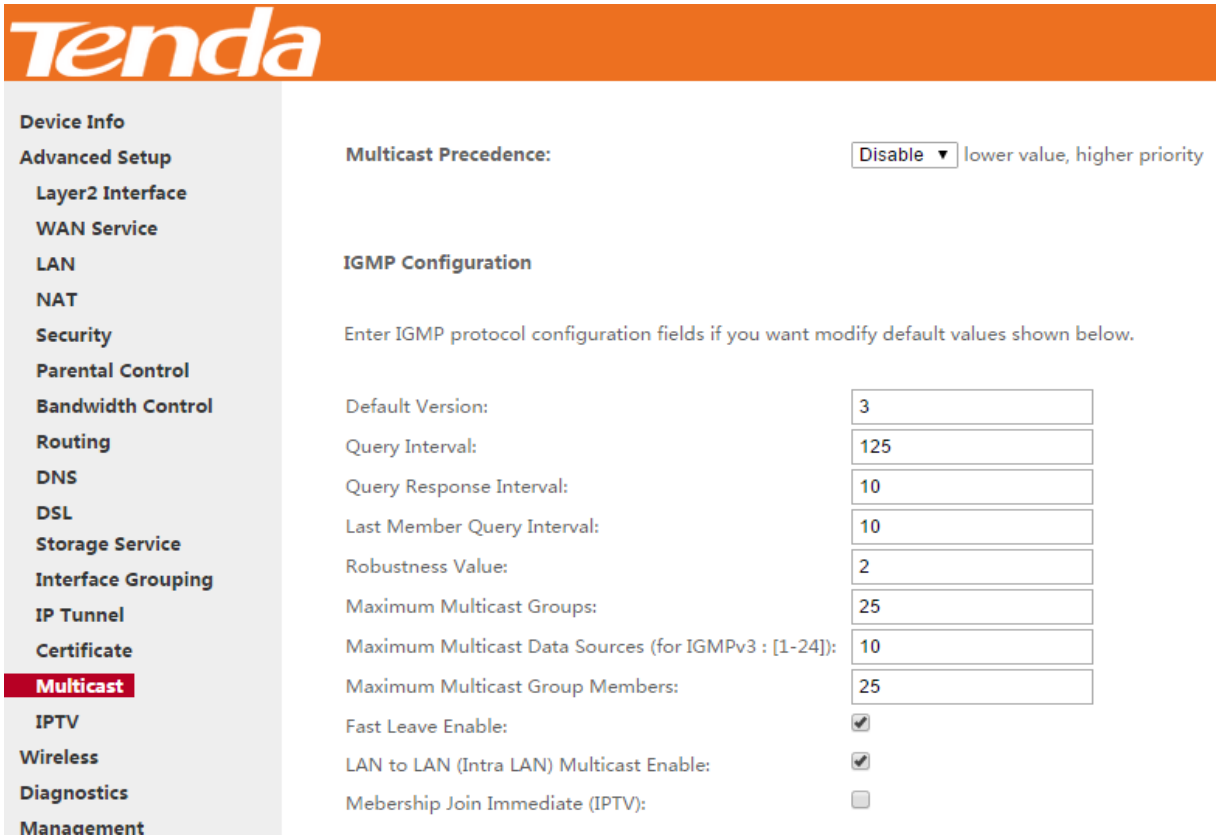
Here you can configure the multicast feature.

To configure IGMP for IPv4

① Check the LAN to LAN (Intra LAN) Multicast Enable box.

② Check the **Membership Join Immediate (IPTV)** box. This is only required for IPTV.

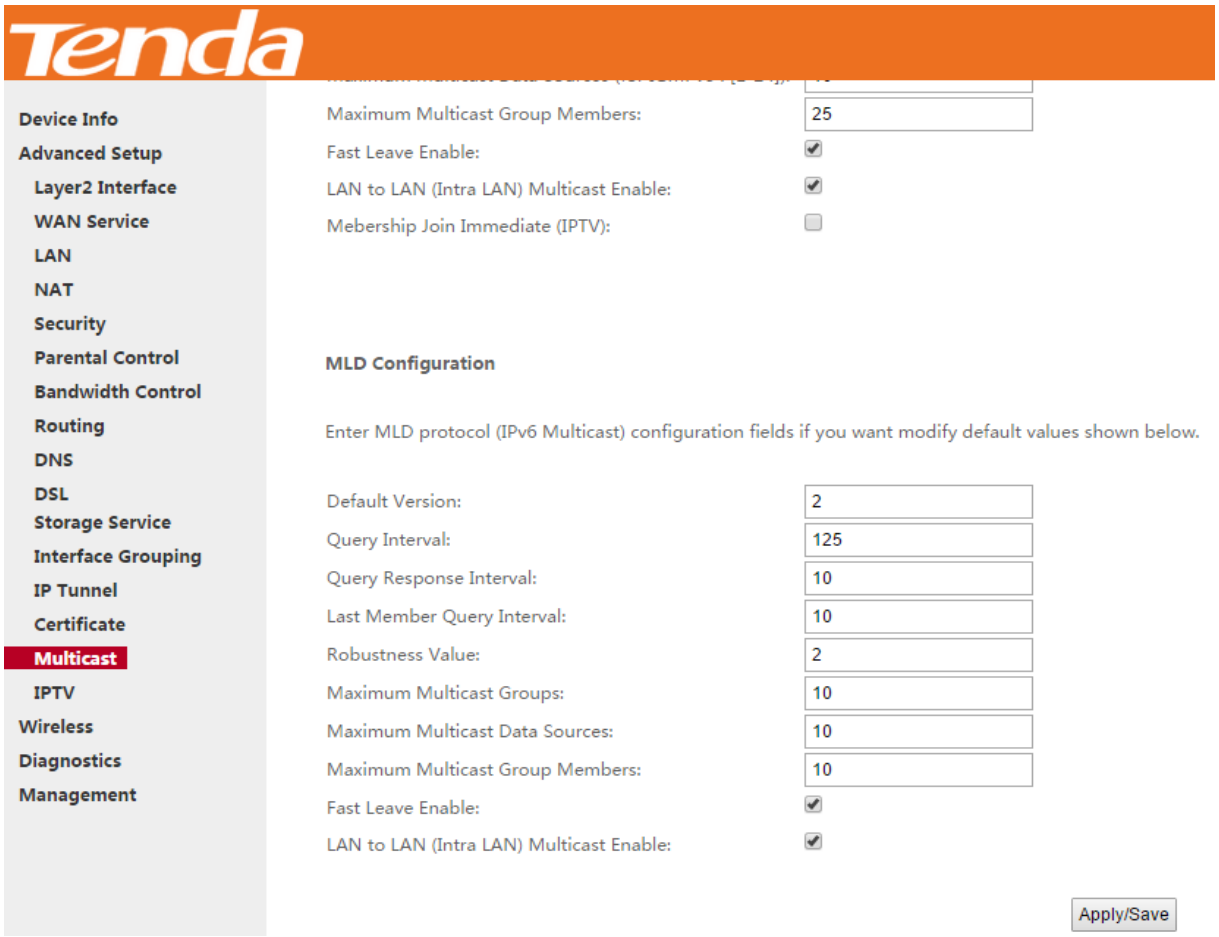
③ Keep other options unchanged from factory defaults if you are not an advanced user. This is strongly recommended.



To configure IGMP for IPv6

① Check the LAN to LAN (Intra LAN) Multicast Enable box.

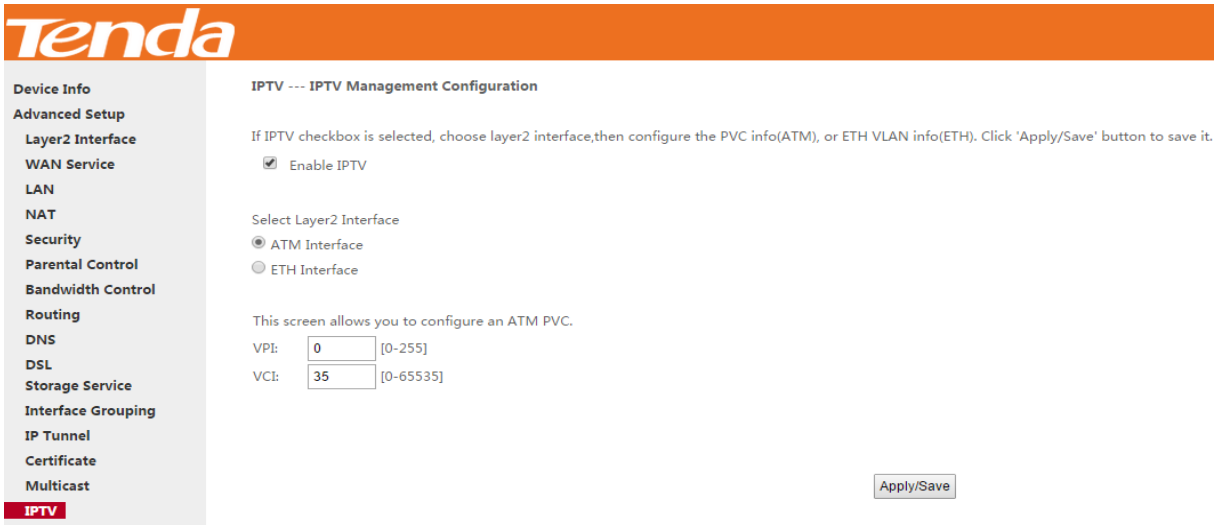
② Keep other options unchanged from factory defaults if you are not an advanced user. This is strongly recommended.



4.2.16 IPTV

If you check the **Enable IPTV** checkbox, you must choose a layer2 interface, and then configure the PVC info (ATM), or VLAN info (ETH). Click Apply/Save to save it.

Enable IPTV: Check to enable the IPTV service, or disable it.



IPTV configuration for DSL Internet Access user:

① Enable **IPTV**.

② Select Layer2 interface: **ATM Interface**.

③ Configure an available VPI/VCI value which should be provided by your ISP.

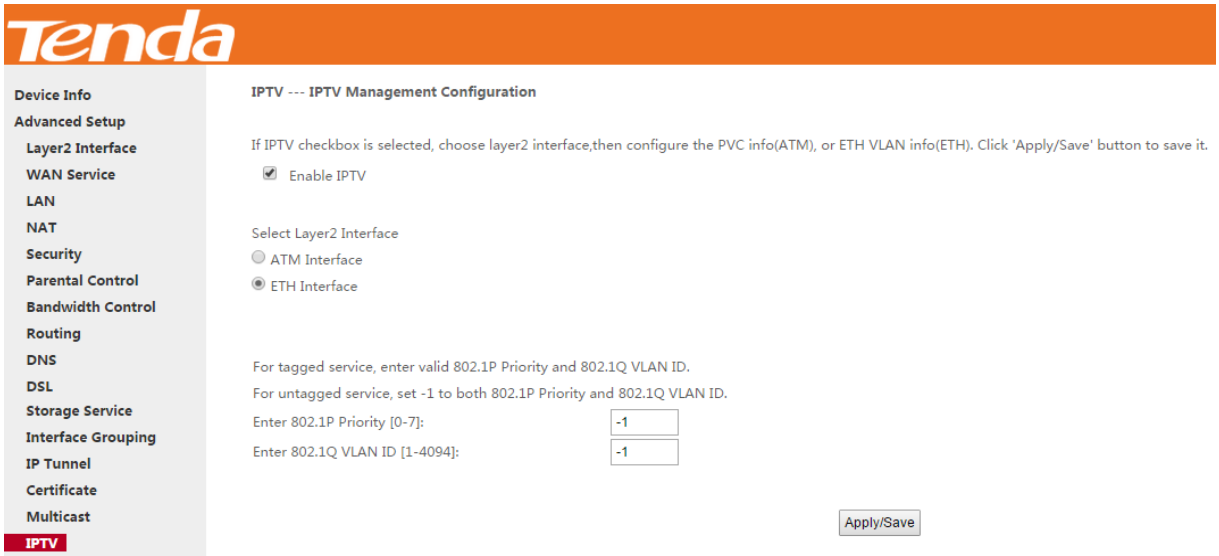
④ Click Apply/Save.

IPTV configuration for Ethernet Internet Access user:

① Enable **IPTV**.

② Select Layer2 Interface: **ETH Interface**.

③ Click Apply/Save.



After successful IPTV configurations, Port **4/iTV** on the back panel of the device can only be an IPTV port.

TIP

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.

For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

4.3 Wireless

This section explains the following information:

• *Basic*

• *Security*

• *MAC Filter*

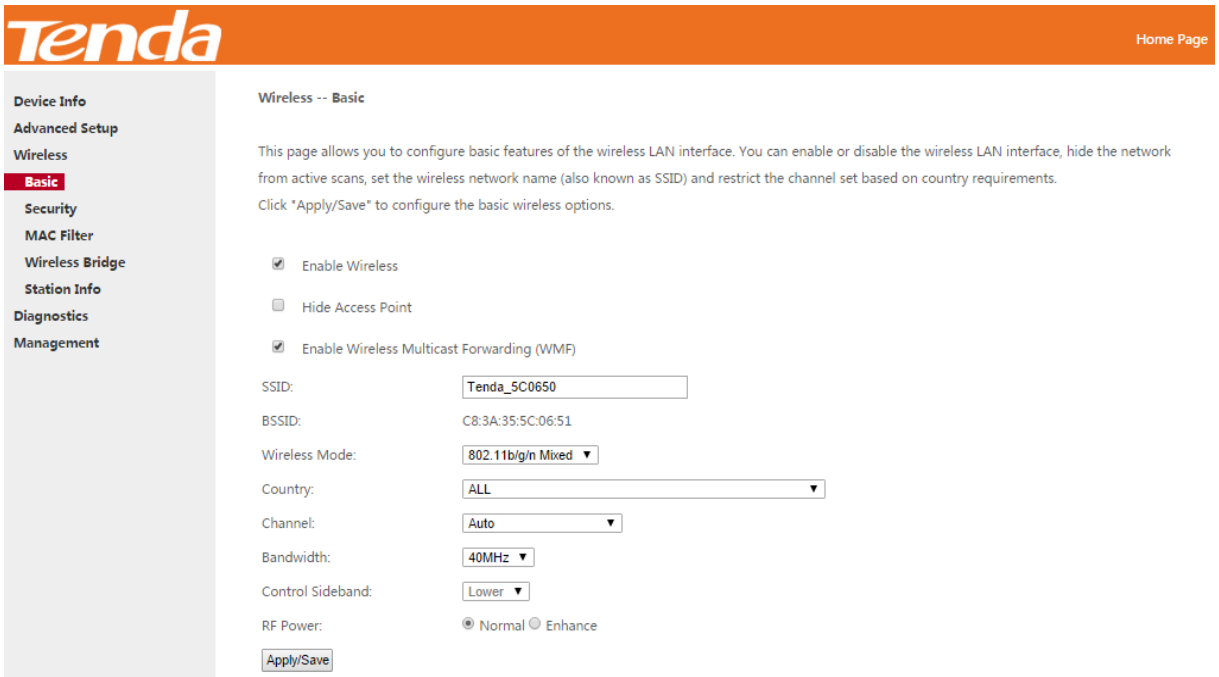
• *Wireless Bridge*

• *Station Info*

4.3.1 Basic

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements.

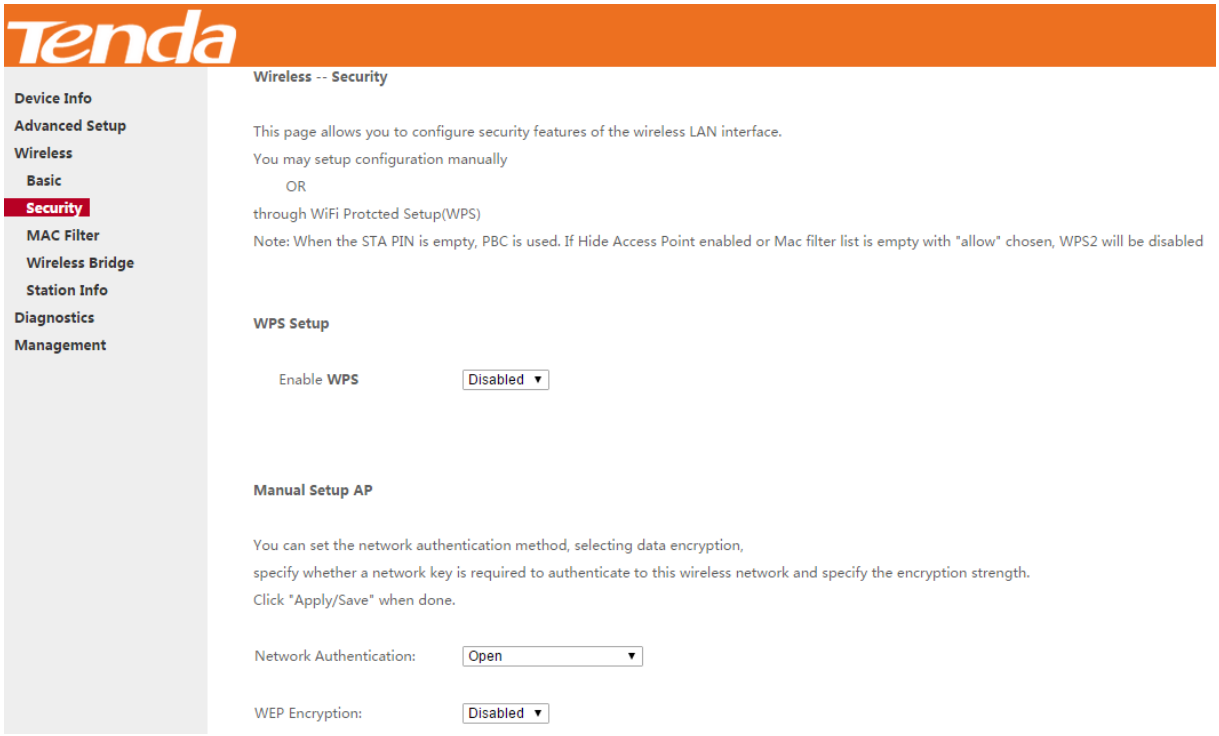
Click Apply/Save to configure the basic wireless options.



- **Enable Wireless:** check/uncheck to enable/disable the wireless feature.
- **Hide Access Point (Hide SSID):** This option allows you to have your network names (SSID) publicly broadcast. If you choose to enable it, the SSID will be hidden.
- **SSID:** This is the public name of your WiFi.
- **BSSID:** Display the MAC address of the wireless network.
- **Country:** Select your country.
- **Channel:** Select a channel, or select **Auto** to let system automatically select one for your wireless network to operate on if you are unsure. The best selection is a channel that is the least used by adjacent networks.
- **Bandwidth:** Configure the wireless bandwidth. The default is 40MHz.
- **RF Power:** Normal or Enhance. This option may adjust the wireless signal strength.

4.3.2 Security

This page allows you to configure security features of the wireless LAN interface. You may set up configuration manually or through WiFi Protected Setup (WPS).

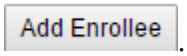


WPS Setup

Wi-Fi Protected Setup makes it easy for home users who know little of wireless security to establish a home network, as well as to add new devices to an existing network without entering long passphrases or configuring complicated settings.

Enable WPS: This is WPS ON/OFF turn. Click it to enable or disable WPS. WPS is disabled by default.

Device PIN: This is PIN code of the modem router for WPS PIN mode.

Enter SAT PIN: "SAT" means the remote wireless client requiring a connection. Enter its PIN code in the blank if you select this option, and then click 

.

Use AP PIN: "AP" means the modem router. Select this option if you copy the PIN code of the modem router to the remote wireless client.

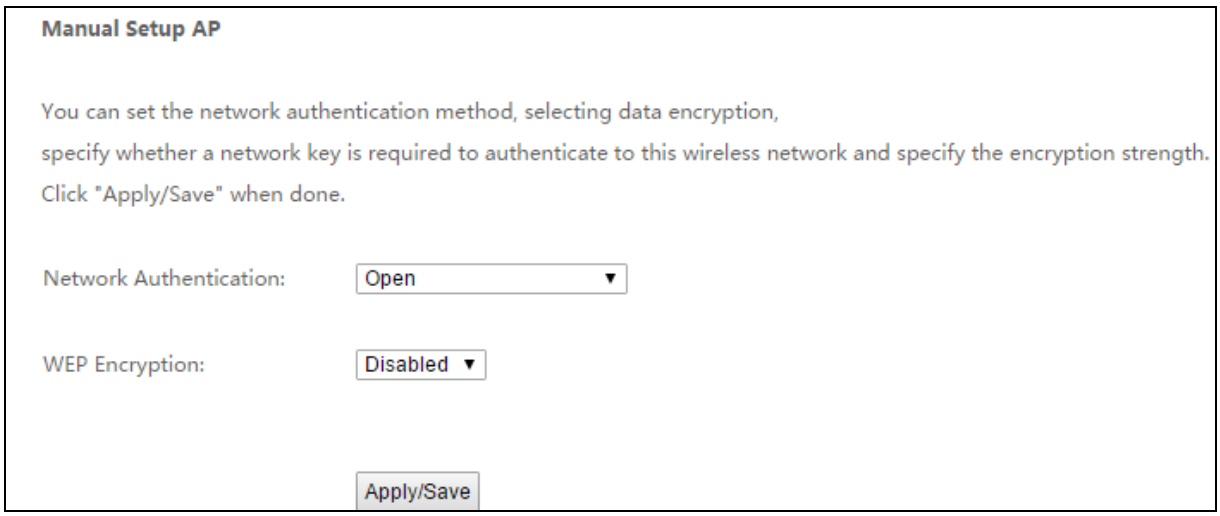
NOTE

1. **WPS/RST** button in the device back panel**:** When WPS feature is enabled, press this button on the device for 1~3 seconds and the WPS LED will keep blinking for about 2 minutes. Within the 2 minutes, press the WPS button on your wireless clients. When the WPS displays a solid light, the wireless client has joined in your wireless network.
2. To use the WPS security, the wireless client must be also WPS-capable.
3. WPS only supports WPA2, which means only when you select "WPA2" encryption or "Open" you can change WPS status.

Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.

Click Apply/Save when done.

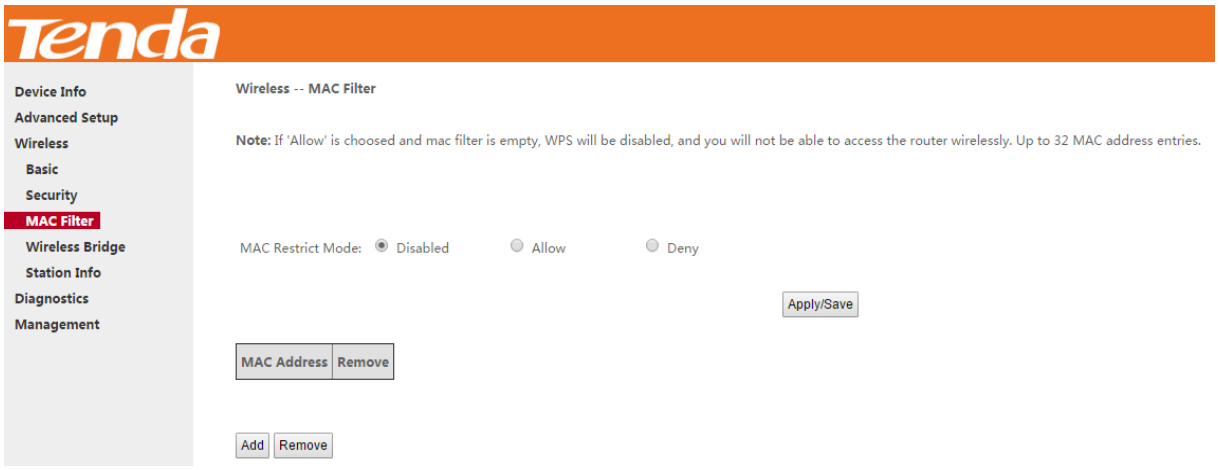


- **Network Authentication:** Select Open, Shared, WPA-PSK, WPA2-PSK or Mixed WPA/ WPA2-PSK from the drop-down list to encrypt your wireless network.

  Depending on the type of network authentication you select, you will be prompted to enter corresponding settings.
- **WEP Encryption:** Select Enabled or Disabled.
- **Encryption Strength:** Select 128-bit or 64-bit.
- **Current Network Key:** Select a network key to be active.
- **Network Key 1/2/3/4:** Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys; enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.
- **WPA/WAPI passphrase:** Enter a WPA/WAPI network key.
- **WPA Group Rekey Interval:** Specify a key update interval.
- **WPA/WAPI Encryption:** Select AES or TKIP+AES.

4.3.3 MAC Filter

The MAC-based Wireless Access Control feature can be used to allow or disallow clients to connect to your wireless network.



MAC Restrict Mode: Disabled, Allow and Deny

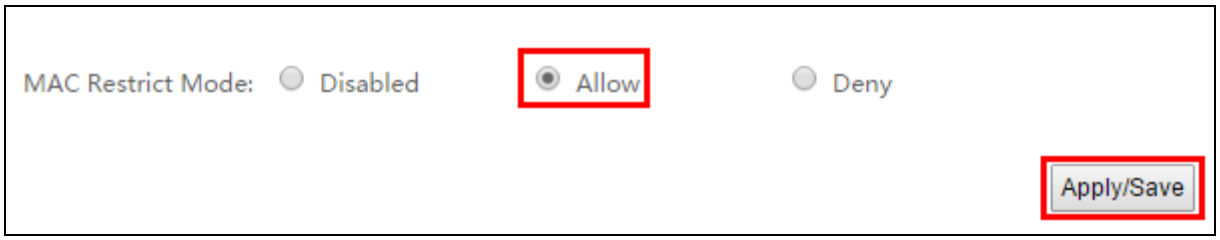
- **Allow:** Only allow PCs at specified MAC addresses (in the list) to connect to your wireless network.
- **Deny:** Block only PCs at specified MAC addresses from connecting to your wireless network.
- **Disable:** Disable this feature.

Add: Click it to add a MAC address.

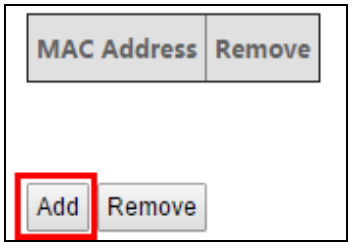
Remove: To delete an existing MAC address, first check the **Remove** box next to the MAC address in list and then click this button.

Example 1: To allow only the PC at the MAC address of 00:1A:3D:9C:BB:23 to connect to your wireless network, do as follows:

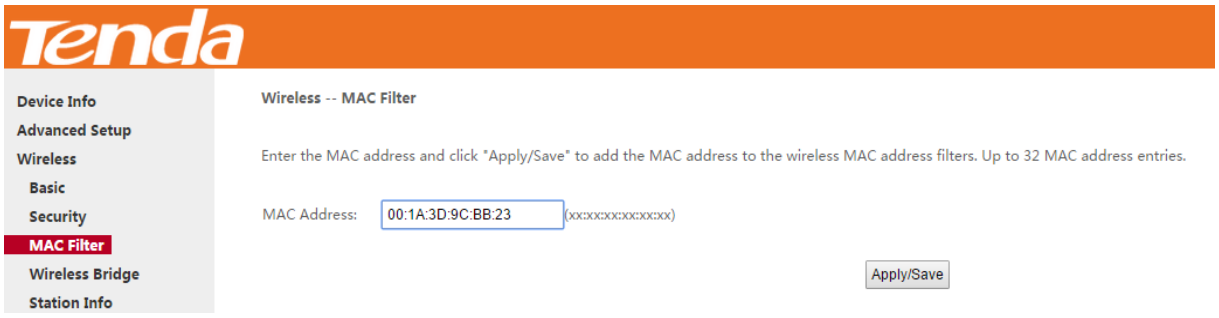
① Select **Allow**, and click Apply/Save.



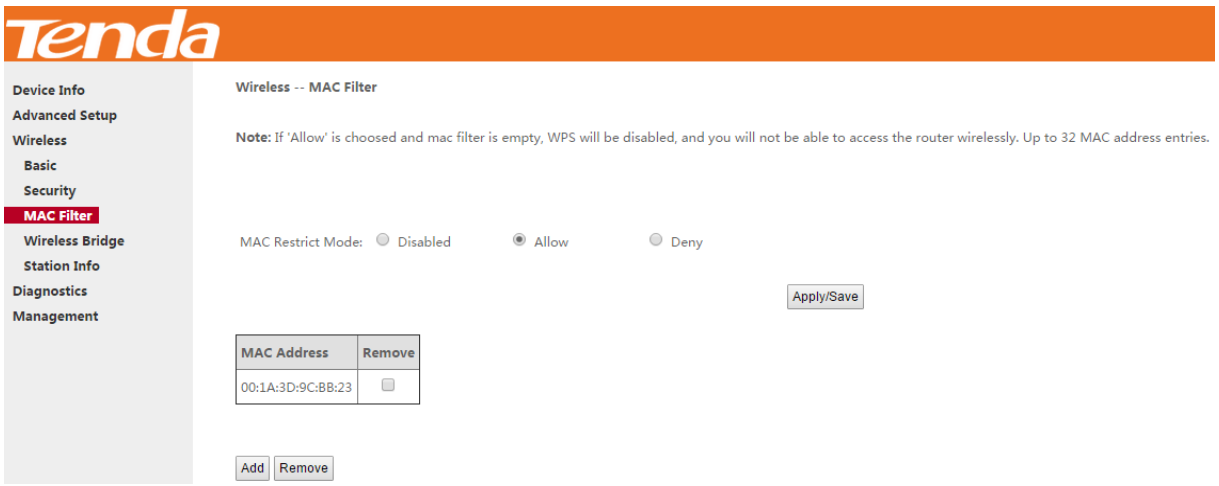
② Click the **Add** button.



③ Enter **00:1A:3D:9C:BB:23** in the MAC address box as shown in the figure below, and click Apply/Save



Set up successfully!



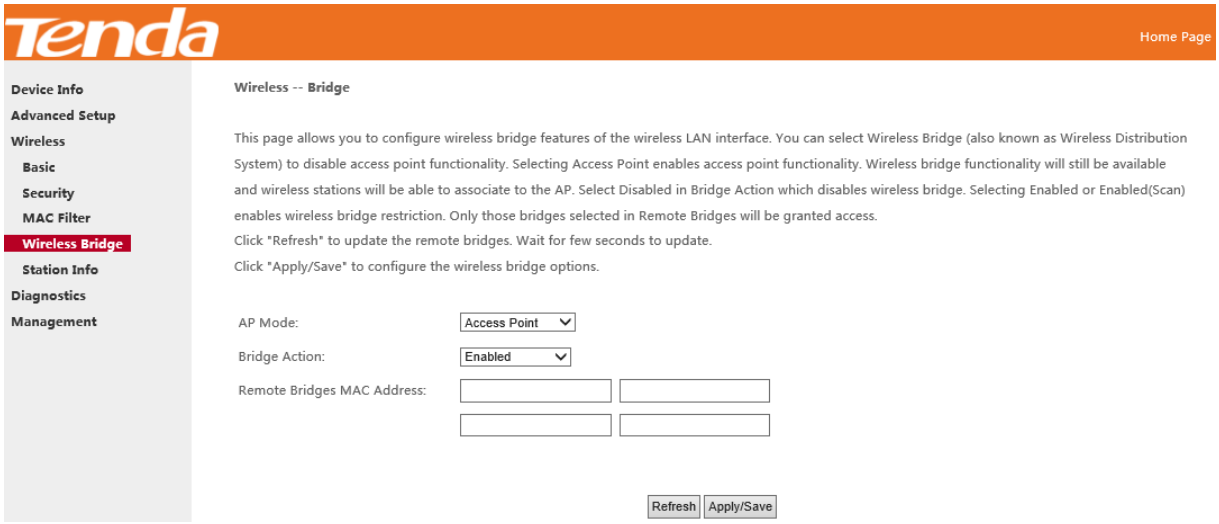
NOTE

If "Allow" mode is activated with no MAC address being limited, WPS feature will be disabled. Go to **Wireless > Security** to check WPS status).

4.3.4 Wireless Bridge

This page allows you to configure wireless bridge (also known as Wireless Distribution System) features of the wireless interface.

Wireless distribution system (WDS) is a system enabling the wireless interconnection of access points in an IEEE 802.11 network. It allows a wireless network to be expanded using multiple access points without the traditional requirement for a wired backbone to link them.



AP Mode: You can select **Wireless Bridge** (also known as Wireless Distribution System) to disable access point functionality. Selecting **Access Point** enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP.

Bridge Action: There are three options available: **Enabled**, **Enabled (Scan)** and **Disabled**. **Disabled** mode means disabling the wireless bridge function. If **Enabled** mode is selected, you need to enter the remote device MAC address manually. If **Enabled (Scan)** is selected, the system automatically scans the remote device MAC address and SSID.

Remote Bridges MAC Address: Here displays the remote device info, MAC address and SSID (if **Bridge Action** is **Enabled Scan**), or offers you field to enter the remote info, MAC address (if **Bridge Action** is **Enabled**).

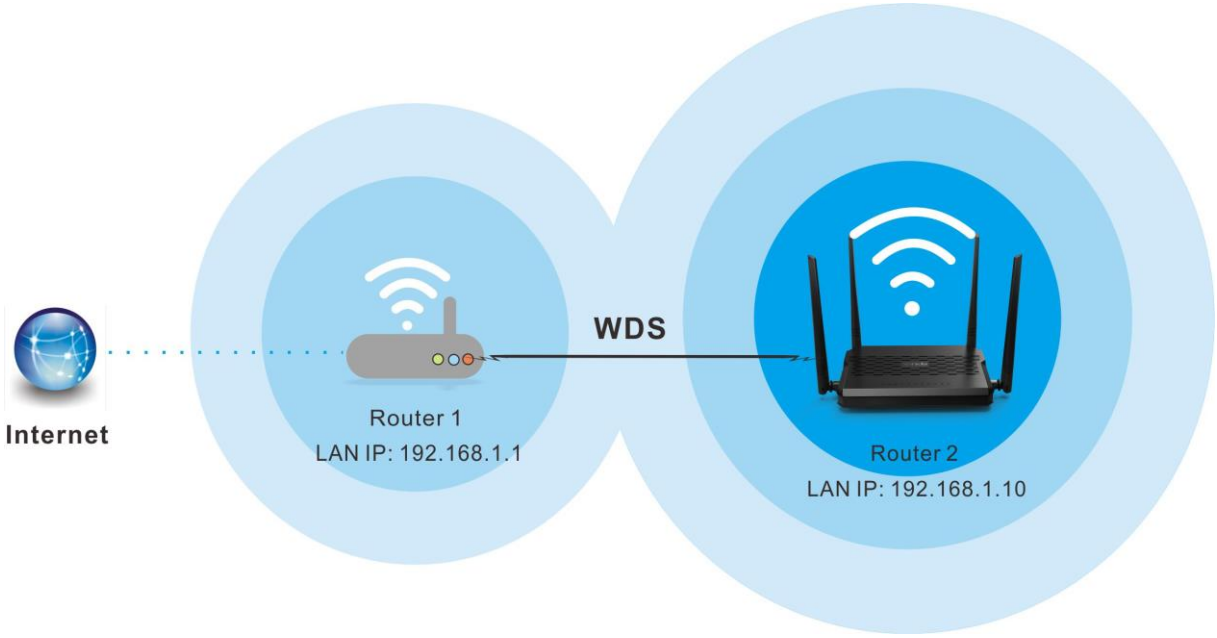
Refresh: Click to refresh the Wireless Name (SSID). Wait for few seconds to refresh.

Apply/Save: Click to apply and save the settings.

Instance

Assume that there is a wireless router in your living room, far away from your study room. Every time you join the WiFi in the study room, it seems hard for you to watch a high-quality live streaming video. To add another wireless router in the study room is an ideal choice to solve your problem. **Wireless Bridge** function of the modem router helps you to extend your wireless coverage, speed up downloading. Then your video will run smoother and faster.

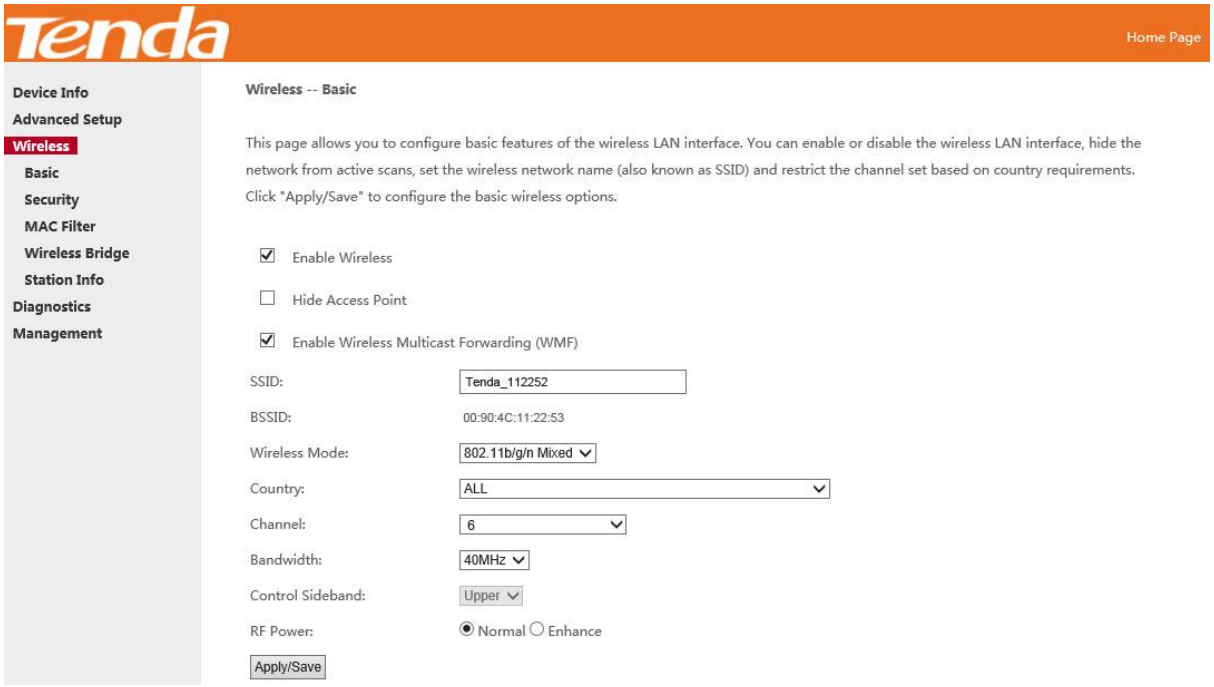
Assume that the router in your living room is **Router 1**, and the other one in study room is **Router 2**.



Before you get started:

① View and note down the security settings of Router 1: wireless name (SSID), channel, security mode, MAC address and wireless key.

a) Click **Advanced > Wireless > Basic** to check the **SSID**, **MAC address** (**BSSID**) and **Channel**.

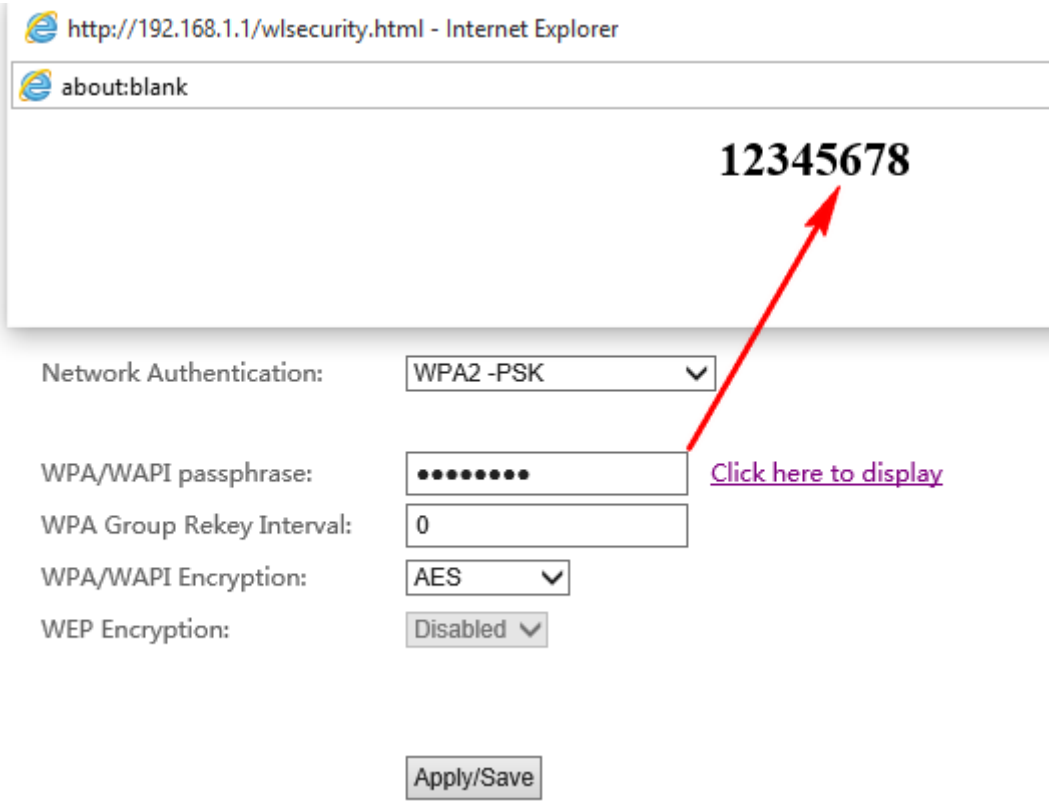


SSID: Tenda_112252

BSSID: 00:90:4C:11:22:53

Channel: 6

b) Click **Advanced** > **Wireless** > **Security** to check security mode and wireless key.



WPS: Disable

Security Mode: WPA2-PSK / AES

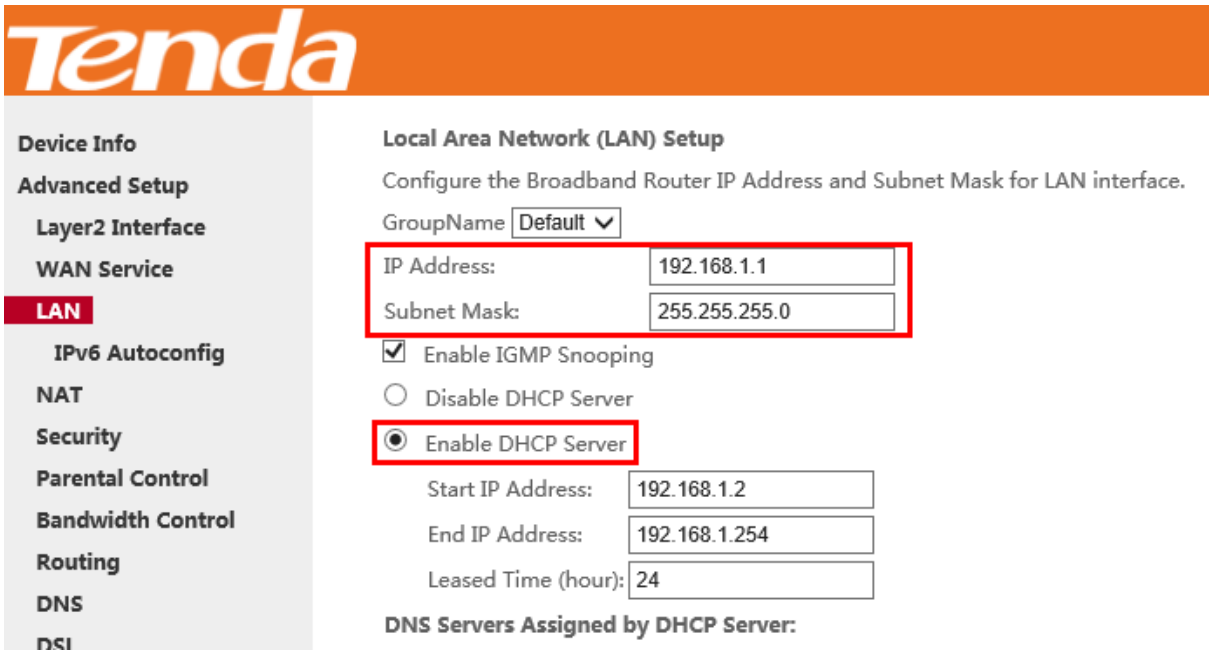
Wireless Key: 12345678

② **View the LAN settings of Router 1.**

Click **Advanced > Advanced Setup > LAN** to check LAN IP address and Subnet Mask, and verify that the DHCP Server is enabled.

LAN IP Address: 192.168.1.1;

Subnet Mask: 255.255.255.0

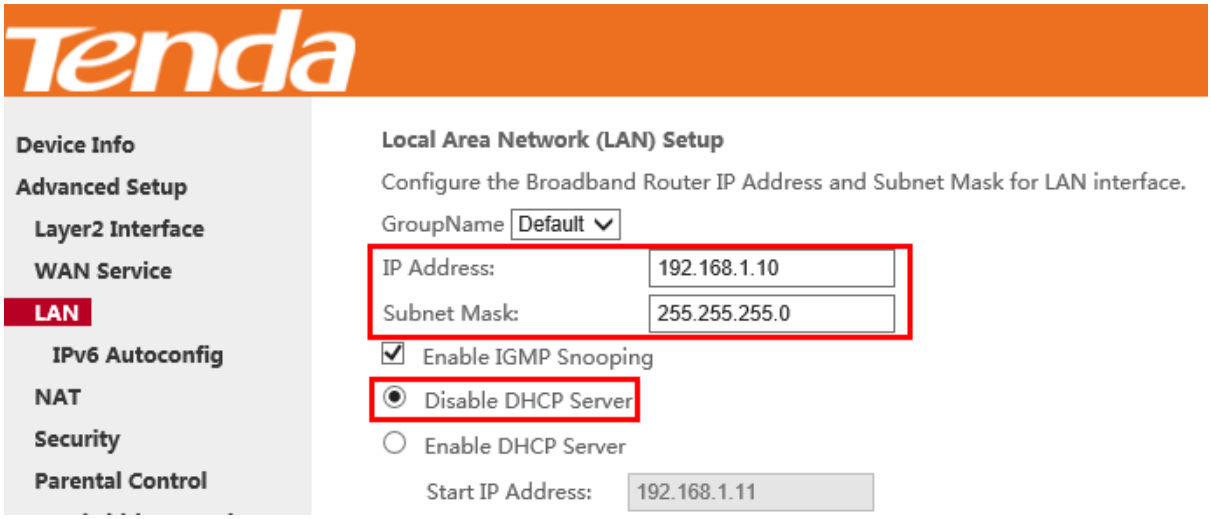


After you prepare two steps above, do as follows:

Configure Router 2:

① Set the LAN IP address of Router 2 to a different IP address yet on the same segment as Router 1.

- Click **Advanced > Advanced Setup > LAN** to change the LAN IP address into 192.168.1.10.
- Disable your DHCP server.



② Click **Advanced > Wireless > Basic** to check the SSID and Channel. They should be the same as Router 1's. If not, correct them manually. Click **Apply/Save** to save your settings.

③ Click **Advanced > Wireless > Security** to check the security mode and wireless key. Verify that they are the same as Router 1's. If not, correct them manually. Click **Apply/Save** to save your settings.

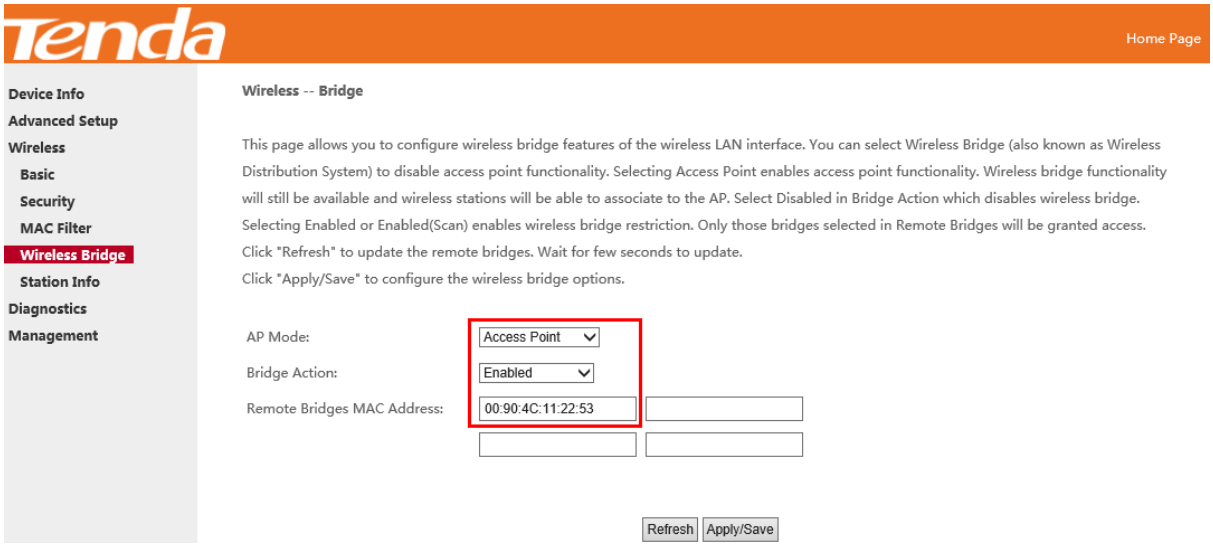
④ Click **Advanced > Wireless > Wireless Bridge** to configure wireless bridge.

➢ **Access Point (Recommended):**

Two ways to bridge Router 1 by using **Access Point**:

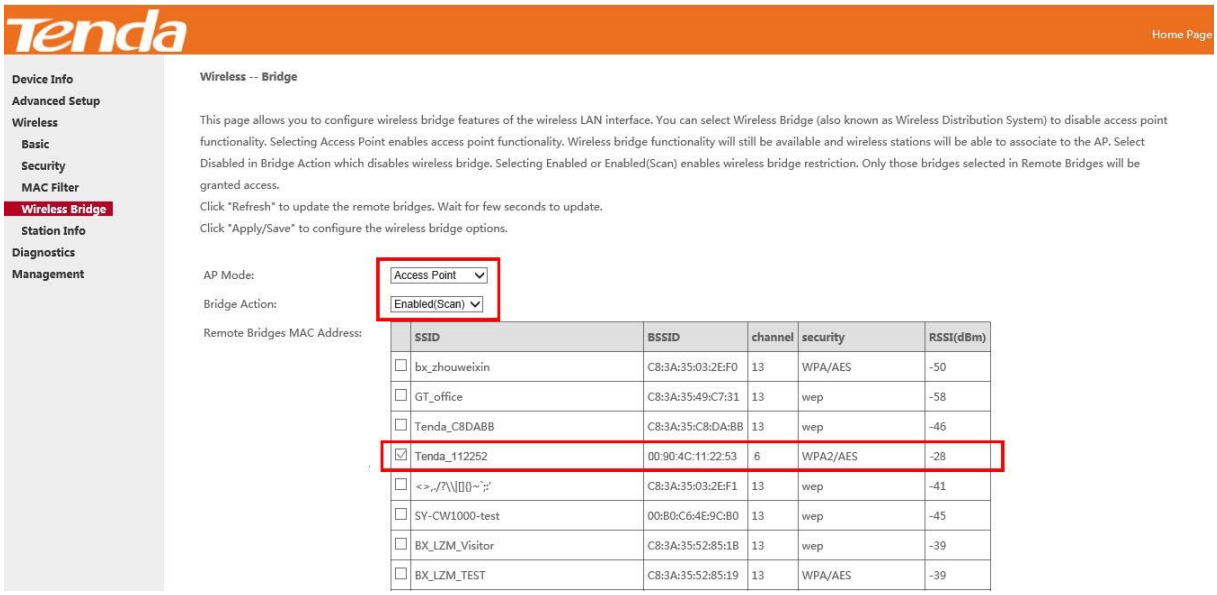
a. If you select **Enable** in Bridge Action field.

- Enter the MAC address of Router 1 which you have noted down (00:90:4C:11:22:53).
- Then click **Apply/Save** to save the settings.



b. If you select **Enable(Scan)** in Bridge Action field.

- Select the SSID of Router 1 (Tenda_112252) in **Remote Bridges MAC Address** field.
- If you cannot find the SSID on the list, click **Refresh** to refresh the list.
- Then click **Apply/Save** to save your settings.

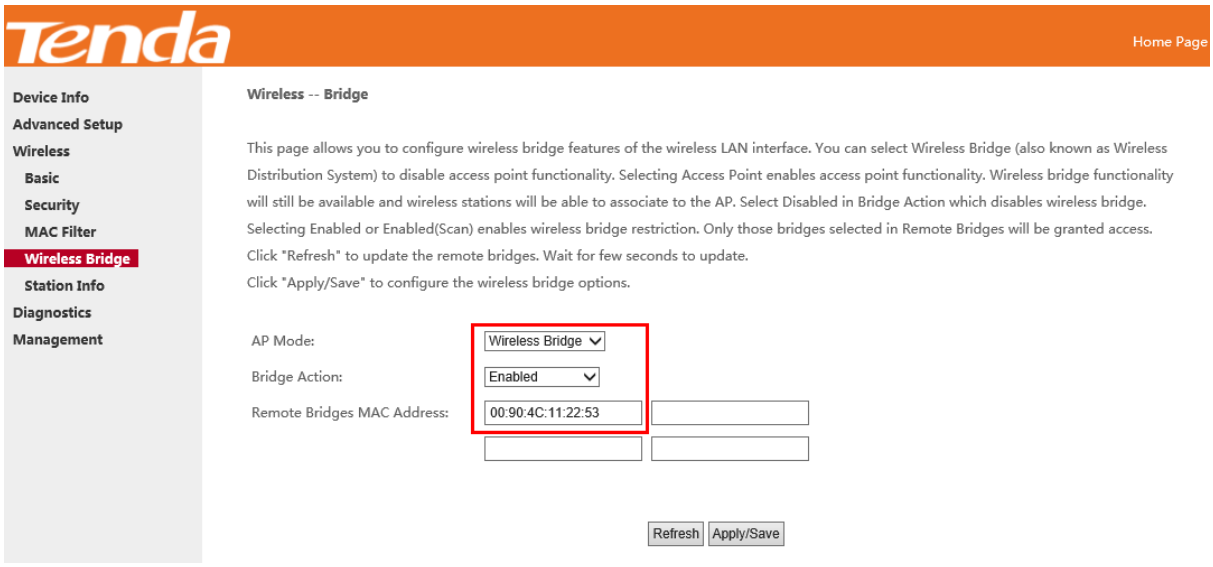


➢ Wireless Bridge

Two ways to bridge Router 1 by using **Wireless Bridge**:

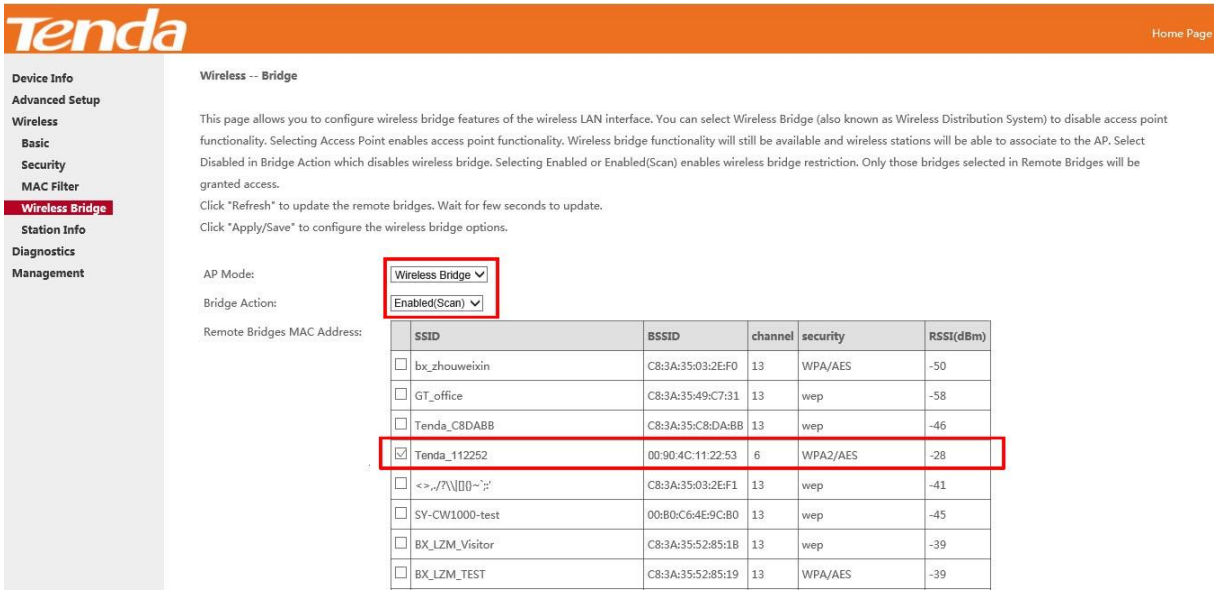
a. If you select **Enable** in Bridge Action field.

- Enter the MAC address of Router 1 which you have noted down (00:90:4C:11:22:53).
- Then click **Apply/Save** to save the settings.



b. If you select **Enable(Scan)** in Bridge Action field:

- Select the SSID of Router 1 (Tenda_112252) in **Remote Bridges MAC Address** field. If you cannot find the SSID on the list, click **Refresh** to refresh the list.
- Then click **Apply/Save** to save your settings.



After you fininsh the settings on Router 2 above, do as follows:

Configure Router 1:

① Click **Advanced > Wireless > Wireless Bridge**.

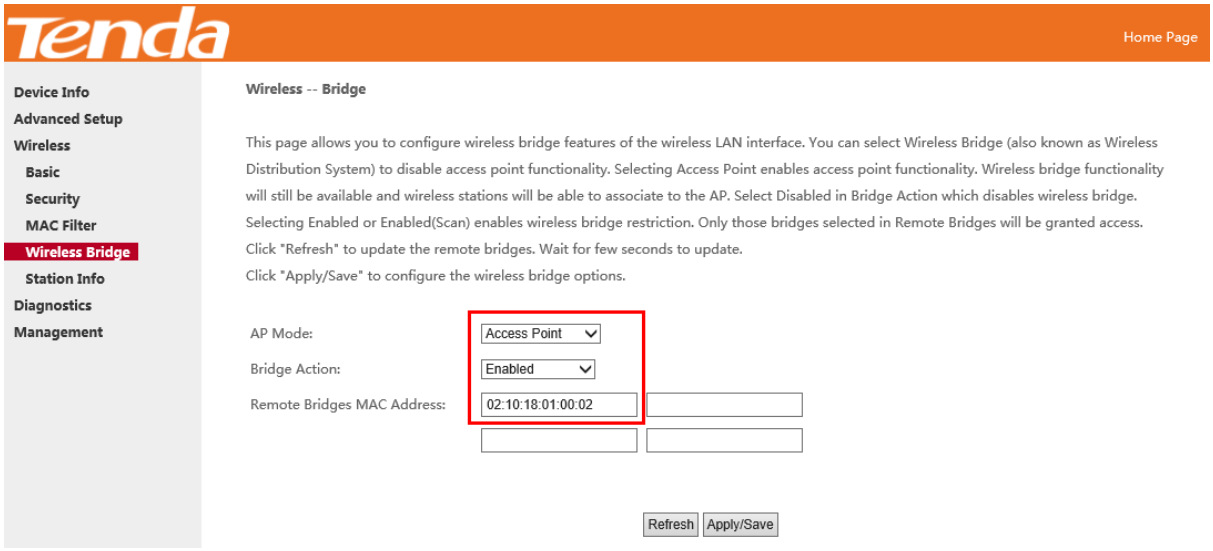
② Select **Access Point** in **AP Mode** field. (If you select **Wireless Bridge** here, the wireless devices will not be able to connect Router 1 wirelessly.)

If **AP Mode** of Router 2 is **Access Point**, there are two ways to bridge Router 2.

a. If you select **Enable** in Bridge Action field:

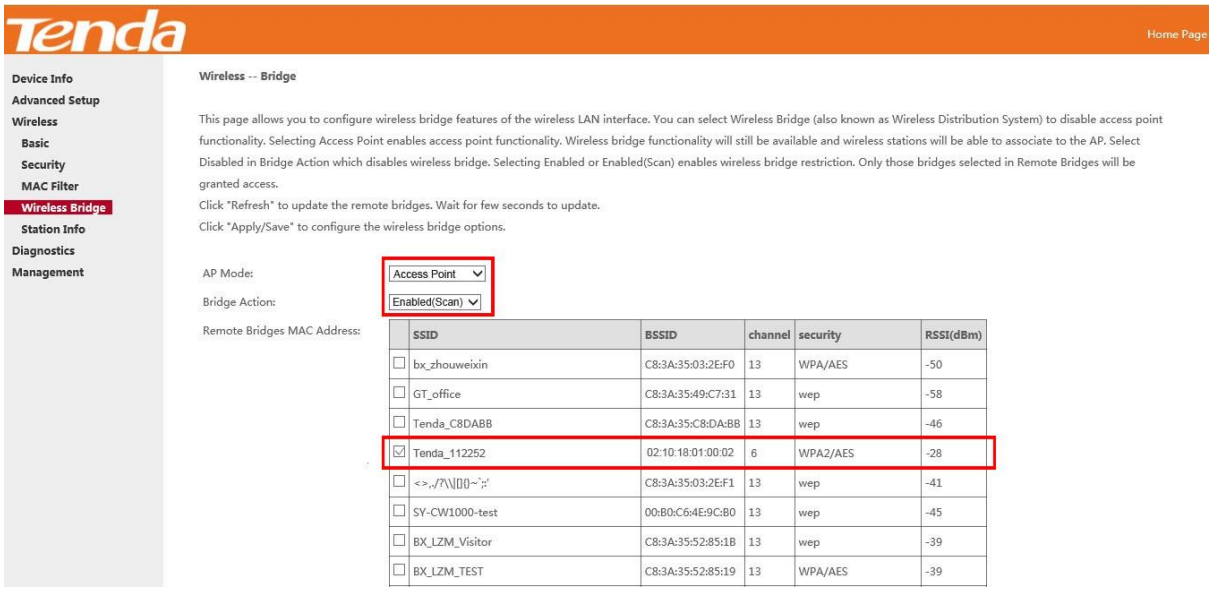
- Enter the MAC address of Router 2 which you can check on **Wireless > Basic** interface, say **BSSID** (02:10:18:01:00:02).

- Then click **Apply/Save** to save the settings.



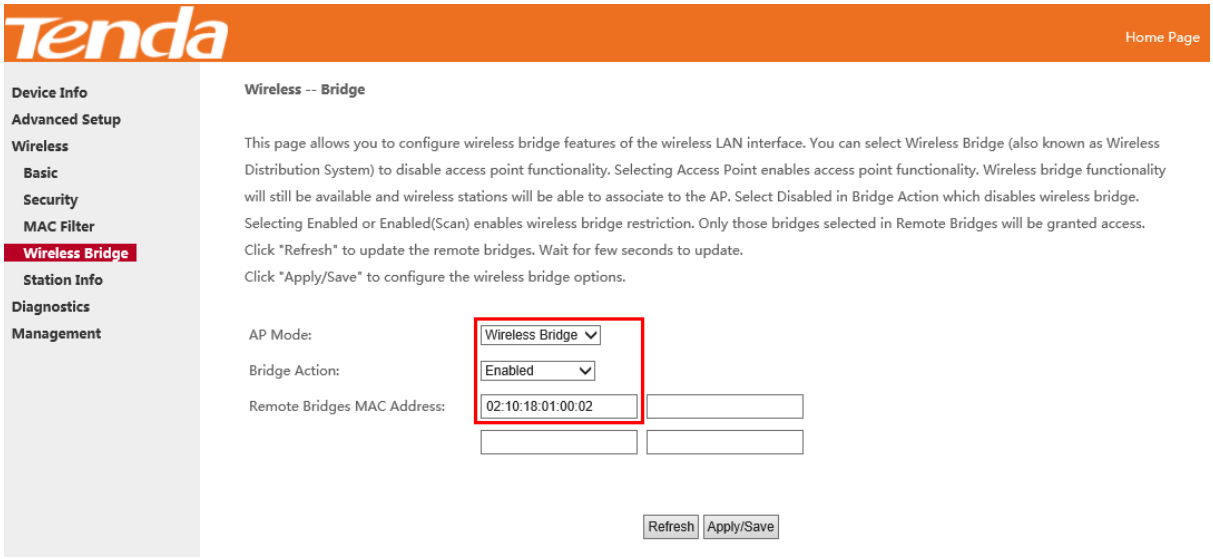
b. If you select **Enable(Scan)** in Bridge Action field:

- Select the SSID of Router 2 (Tenda_112252) in **Remote Bridges MAC Address** field.
- If you cannot find the SSID on the list, click **Refresh** to refresh the list.
- Then click **Apply/Save** to save your settings.



The configuration is finished. Then the devices can connect Router 2 wirelessly or via Ethernet cables.

If **AP Mode** of Router 2 is **Wireless Bridge**, you can only select **Enable** and enter the MAC address (02:10:18:01:00:02) to bridge Router 2.



The configuration is finished. Then the devices can only connect Router 2 via Ethernet cables.

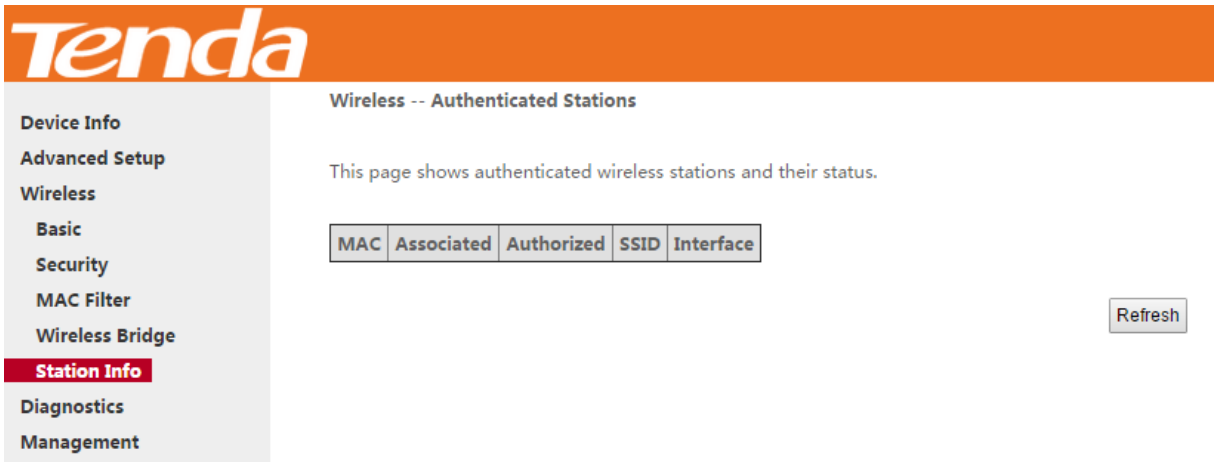
NOTE

The WDS feature (also known as Wireless Bridge) can only be implemented between 2 WDS-capable wireless devices.

Plus, SSID, channel, security settings and security key must be exactly the same on both such devices.

4.3.5 Station Info

This page shows authenticated wireless stations and their status.



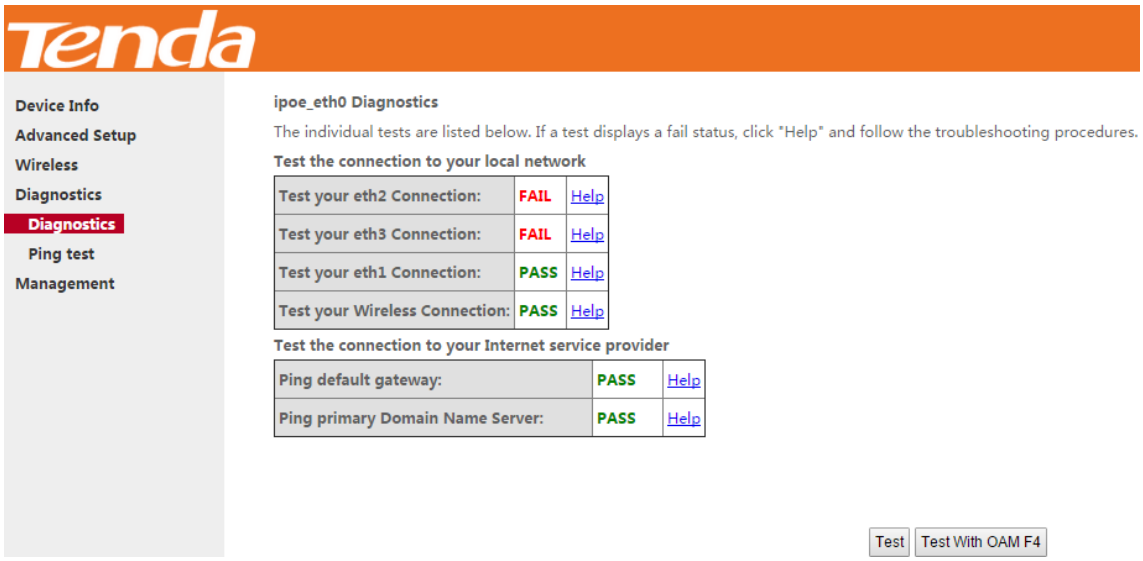
4.4 Diagnostics

this part includes the following information:

- *Diagnostics*
- *Ping test*

4.4.1 Diagnostics

The device is capable of testing the connection to your DSL service provider, the connection to your Internet service provider and the connection to your local network. If a test displays a fail status, click “Rerun Diagnostic Tests” at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click “Help” and follow the troubleshooting procedures.



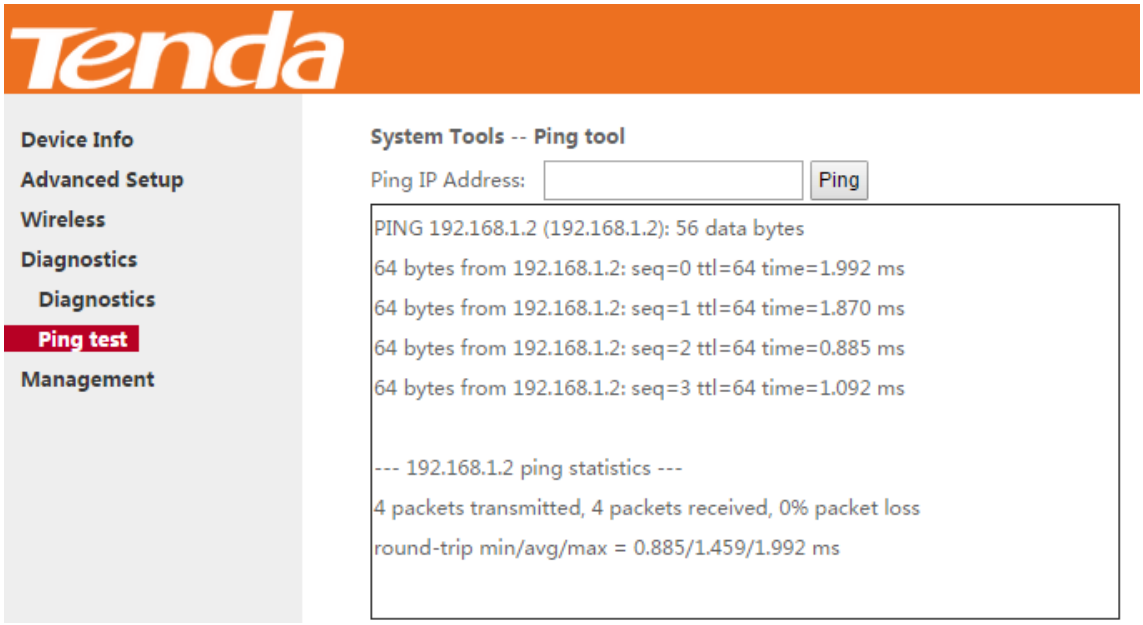
Pass: Indicates that the Ethernet interface from your computer is connected to the LAN port of the device.

Fail: Indicates that the device does not detect the Ethernet interface on your computer.

4.4.2 Ping test

Ping utility can help test whether the device has built a proper connection with your host.

Type in the IP address of your host in the Ping IP Address field, and click **Ping**. If you get a similar screen shown as below, it indicates the connection between the Ping object (Here is 192.168.1.2) and the device has been established.



4.5 Management

This section explains the following information:

• *Settings*

• *System Logs*

• *SNMP Agent*

• *TR-069 Client*

• *Internet Time*

• *Access Control*

• *Update Software*

• *Reboot*

4.5.1 Settings

This section explains the following information:

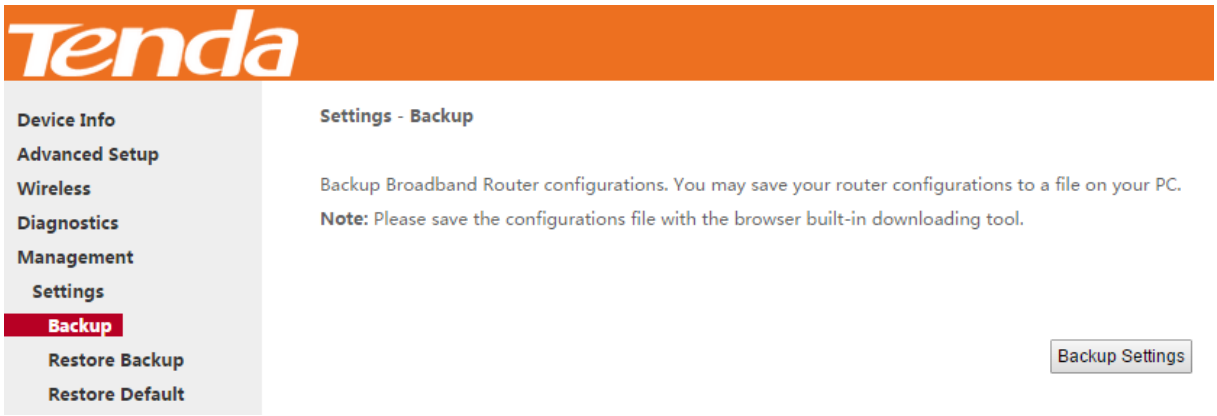
• *Backup*

• *Restore Backup*

• *Restore Default*

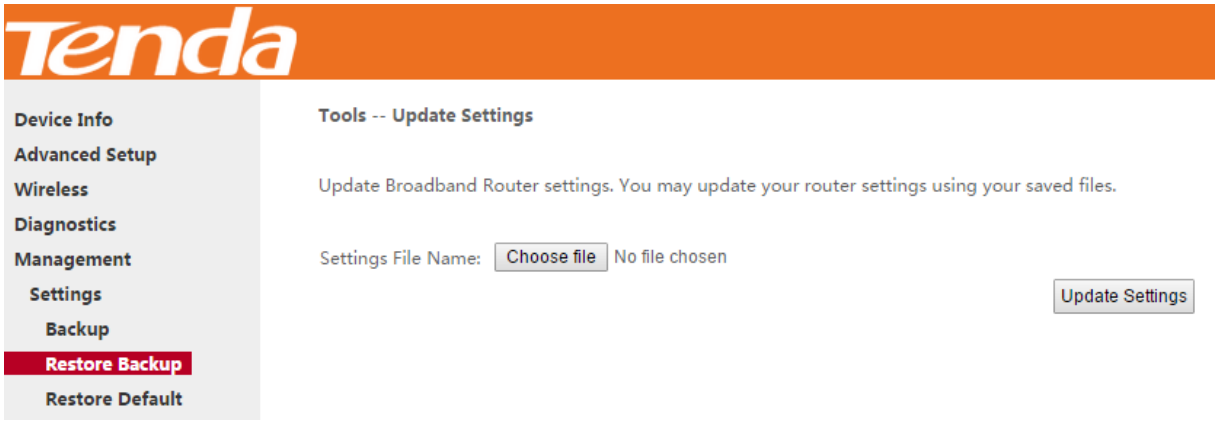
Backup

Here you can save a copy of your device's configurations to your computer. Once you have configured the device, you can save these settings to a configuration file on your local hard drive. The configuration file can later be imported to your device in case the device is reset to factory default settings.



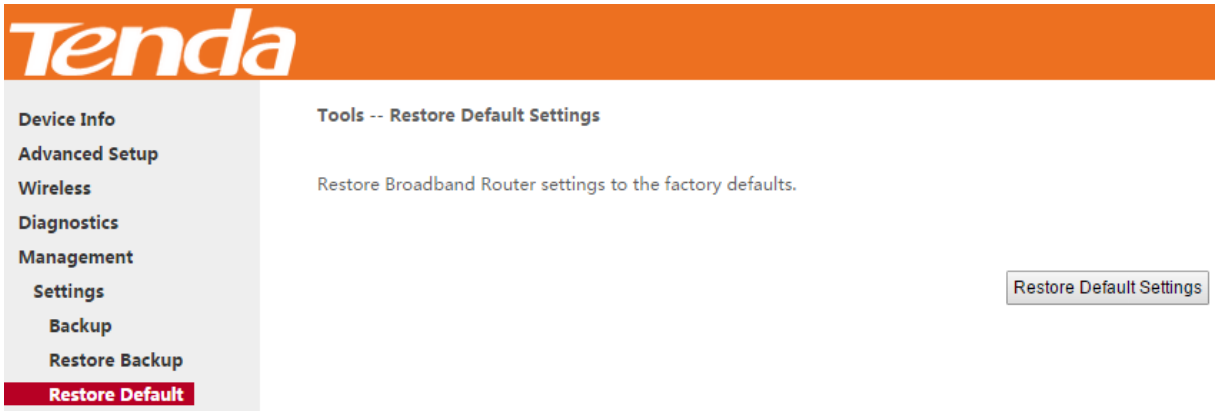
Restore Backup

Here you can restore the configurations of the modem router from a file saved on your PC.



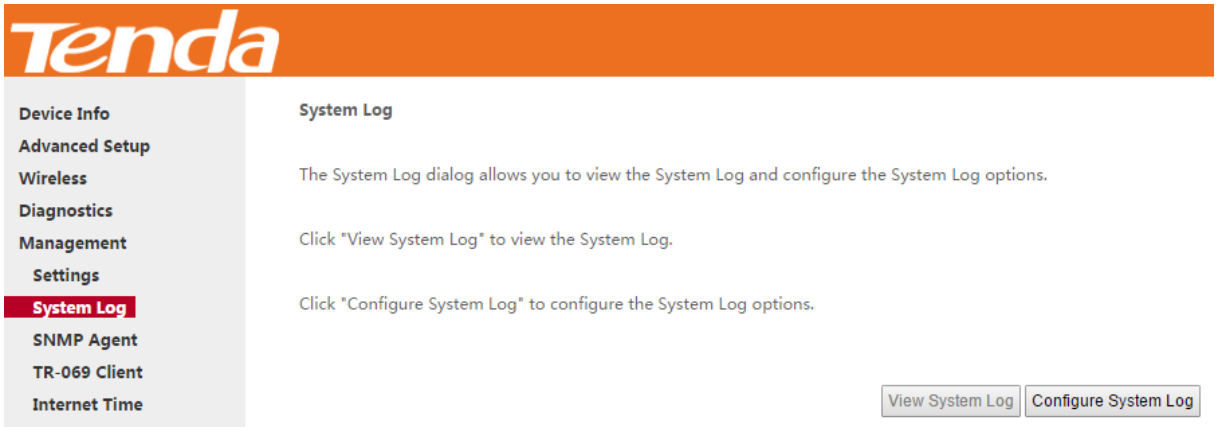
Restore Default

Under some circumstances (for example, join a different network or unfortunately forgetting the login password), you may need to remove the existing configuration and restore the factory default settings.

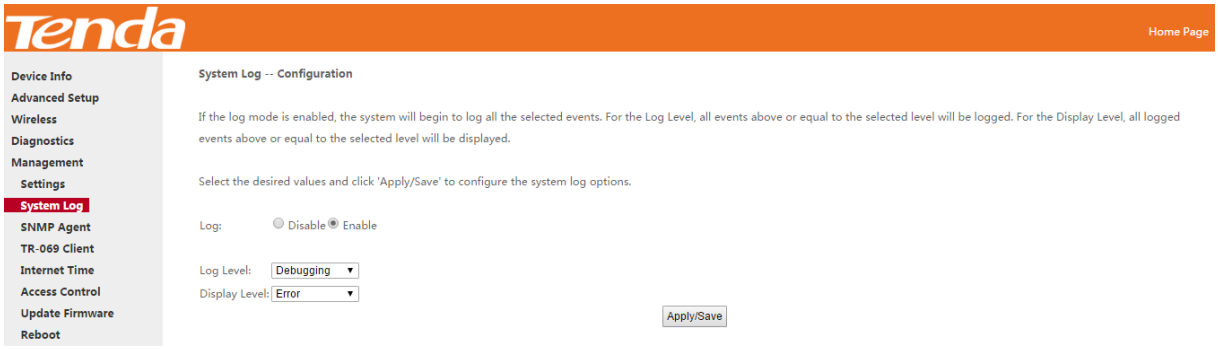


4.5.2 System Logs

The System Log dialog allows you to view the system log and configure the system log options.

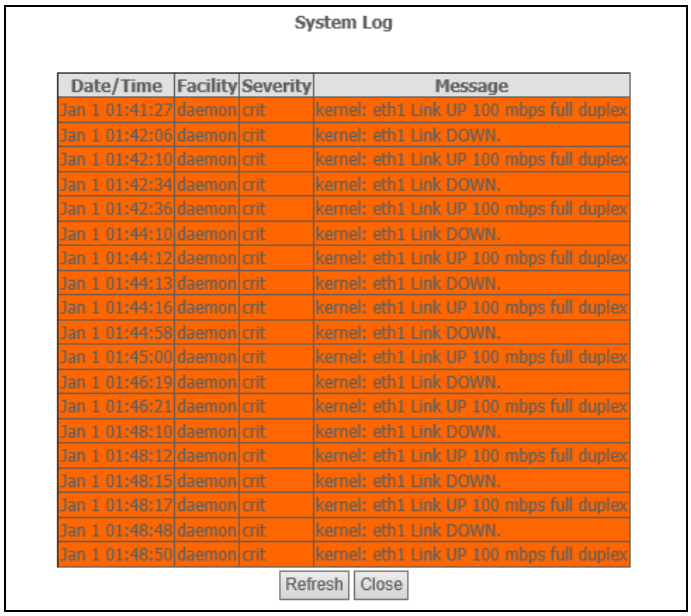


To configure the system log, click **Configure System Log**.



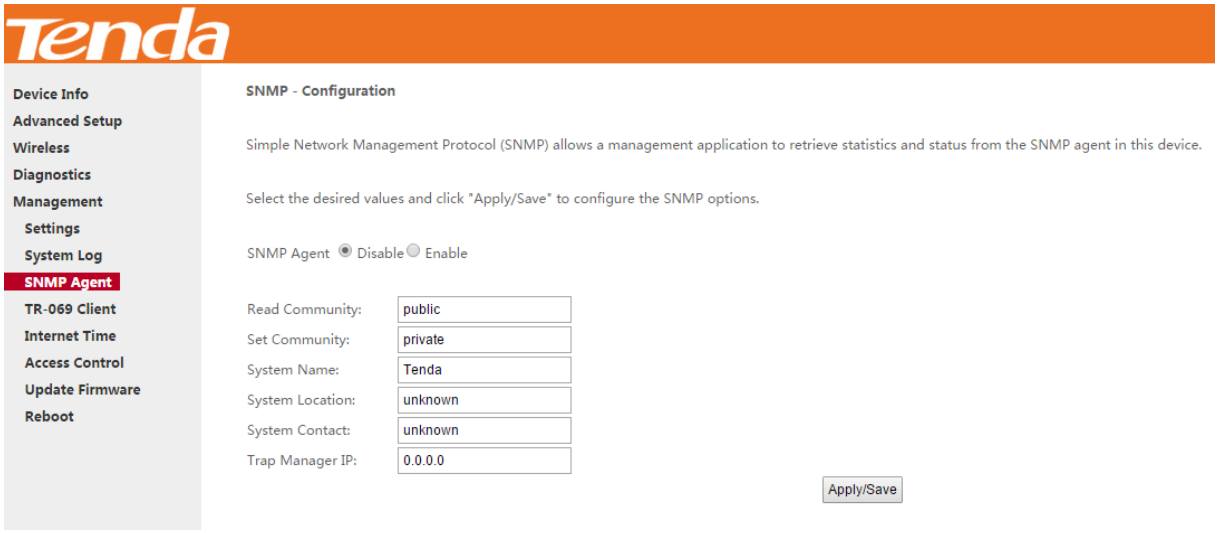
- **Log:** If Enable is selected, the system will begin to log all the selected events.
- **Log Level:** Set the log level. All events above or equal to the selected level will be logged.
- **Display Level:** Set the log display level. All logged events above or equal to the selected level will be displayed.
- **Apply/Save:** click to apply and save the system log settings.

To view the system log, firstly ensure log is enabled, otherwise you cannot read any log.



4.5.3 SNMP Agent

Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device.

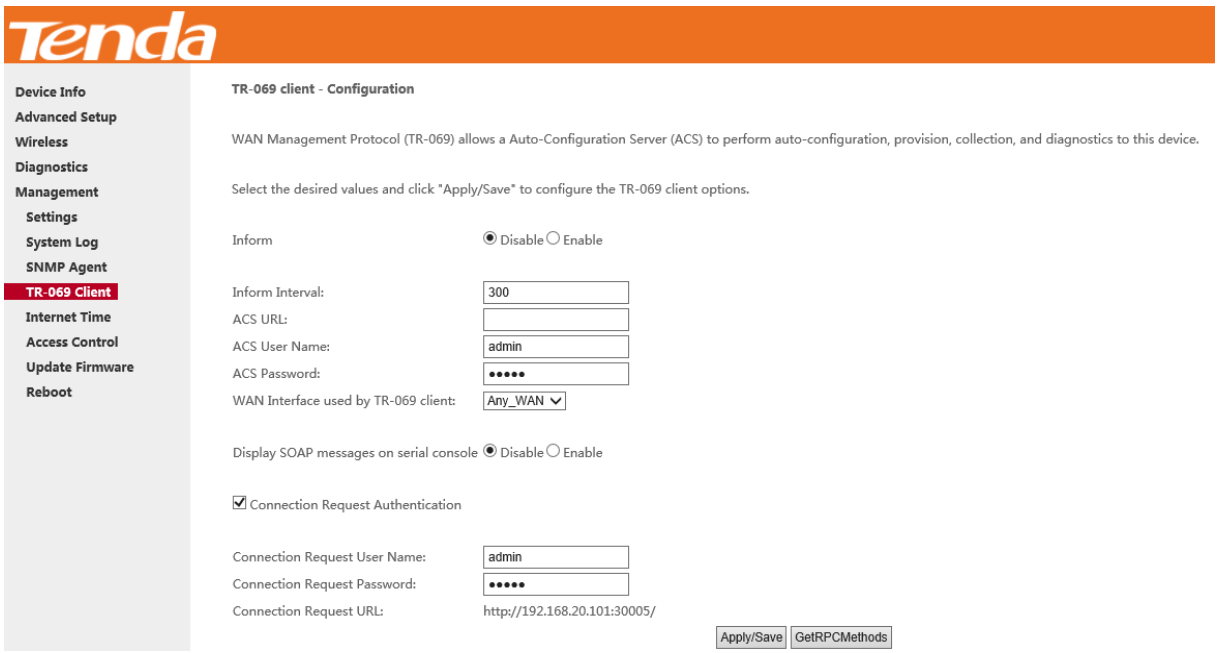


- **SNMP Agent：** Select “Enable” to activate the SNMP Agent feature or “Disable” to deactivate it.
- **Read Community:** Specify a Read Community string. The default is public.
- **Set Community:** Specify a Set Community string. The default is private.
- **System Name:** Specify a descriptive system name.
- **System Location:** Specify a system location.
- **System Contact:** Specify a system contact.
- **Trap Manager IP:** Specify the IP address of the Trap Manager.

4.5.4 TR-069 Client

WAN Management Protocol (TR-069) allows an Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

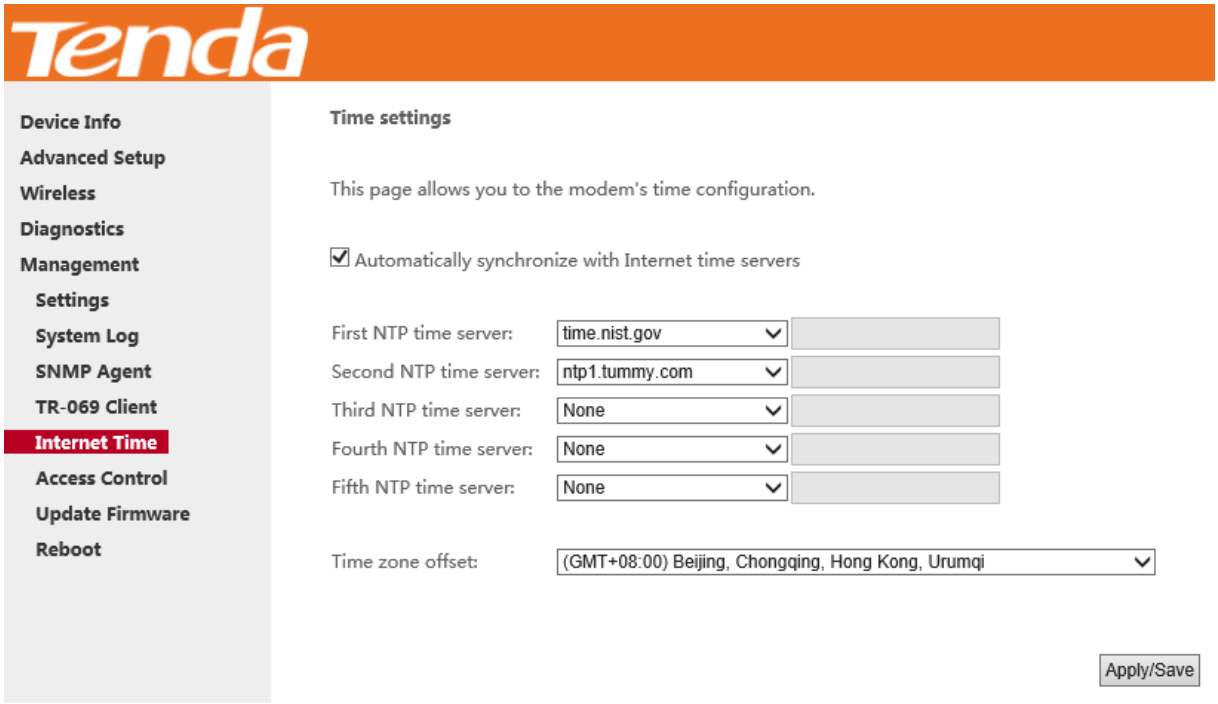
Click the **TR-069 Client** tab to enter the TR-069 Client configuration screen as seen below:



- Inform: Select **Enable/Disable** to enable/disable the **TR-069 Client** function. By default, it is disabled.
- **Inform Interval:** Specify the inform interval.
- **ACS URL:** Enter the ACS (Auto-Configuration Server) URL address.
- **ACS User Name:** Enter the ACS (Auto-Configuration Server) user name.
- **ACS Password:** Enter the ACS (Auto-Configuration Server) password.
- **WAN Interface used by TR-069 client:** Select the WAN interface used by the TR-069 client from the drop-down list.
- **Display SOAP messages on serial console:** If Enable is selected, SOAP messages will be displayed on serial console; if Disable is selected, SOAP messages will not be displayed on serial console.
- **Connection Request Authentication:** Check/uncheck to enable/disable the connection request authentication.
- **Connection Request User Name:** Enter the connection request user name.
- **Connection Request Password:** Enter the connection request password.
- **Connection Request URL:** Specify the connection request URL.

4.5.5 Internet Time

This page is used to set the router's system time. If **Automatically synchronize with Internet time servers** is checked, the system will automatically connect to NTP server to synchronize the time.



First/Second/Third/Fourth/Fifth NTP time server: Select a NTP time server from the drop-down list. If the NTP time server you are looking for is not included in the list, select "Other" and then enter it manually in the box.

Time zone offset: Select your time zone from the drop-down list.

4.5.6 Access Control

This section explains the following information:

• *Password*

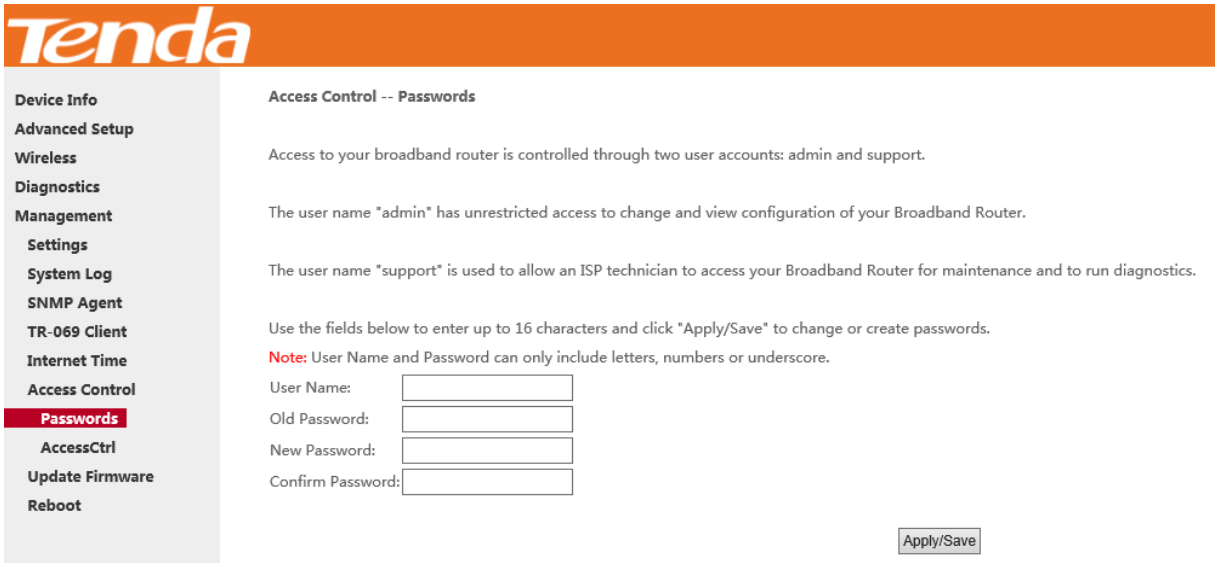
• *AccessControl - Service*

Password

Access to your broadband router is controlled through two user accounts: admin and support.

Admin has unrestricted access to change and view configuration of your Broadband Router.

Support is used to allow a professional technician to access your Broadband Router for maintenance and to run diagnostics.



User Name: Enter the user name of up to 16 characters. The default is “admin”.

Old Password: Enter the old password of up to 16 characters. The default is “admin”.

New Password: Enter a new password of up to 16 characters.

Confirm Password: Re-enter to confirm the new password.

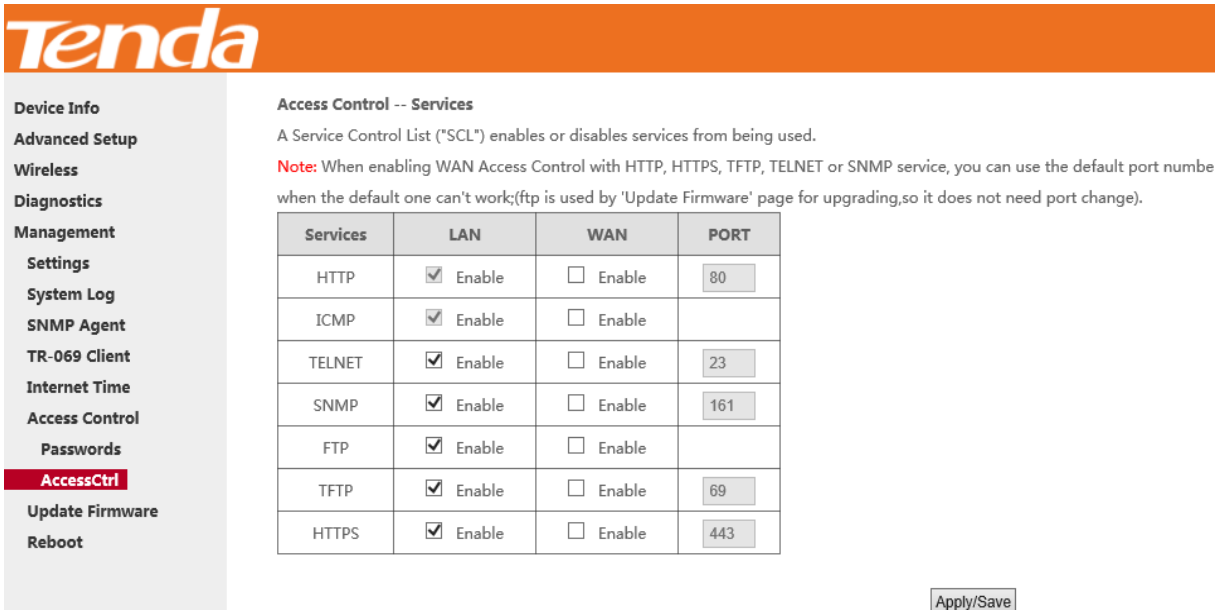
Apply/Save: Click to change or create passwords.

NOTE

Password cannot contain a space.

Access Control - Service

Here you can manage the device either from LAN or WAN side using HTTP, ICMP, TELNET, SNMP, FTP, TFTP and HTTPS.

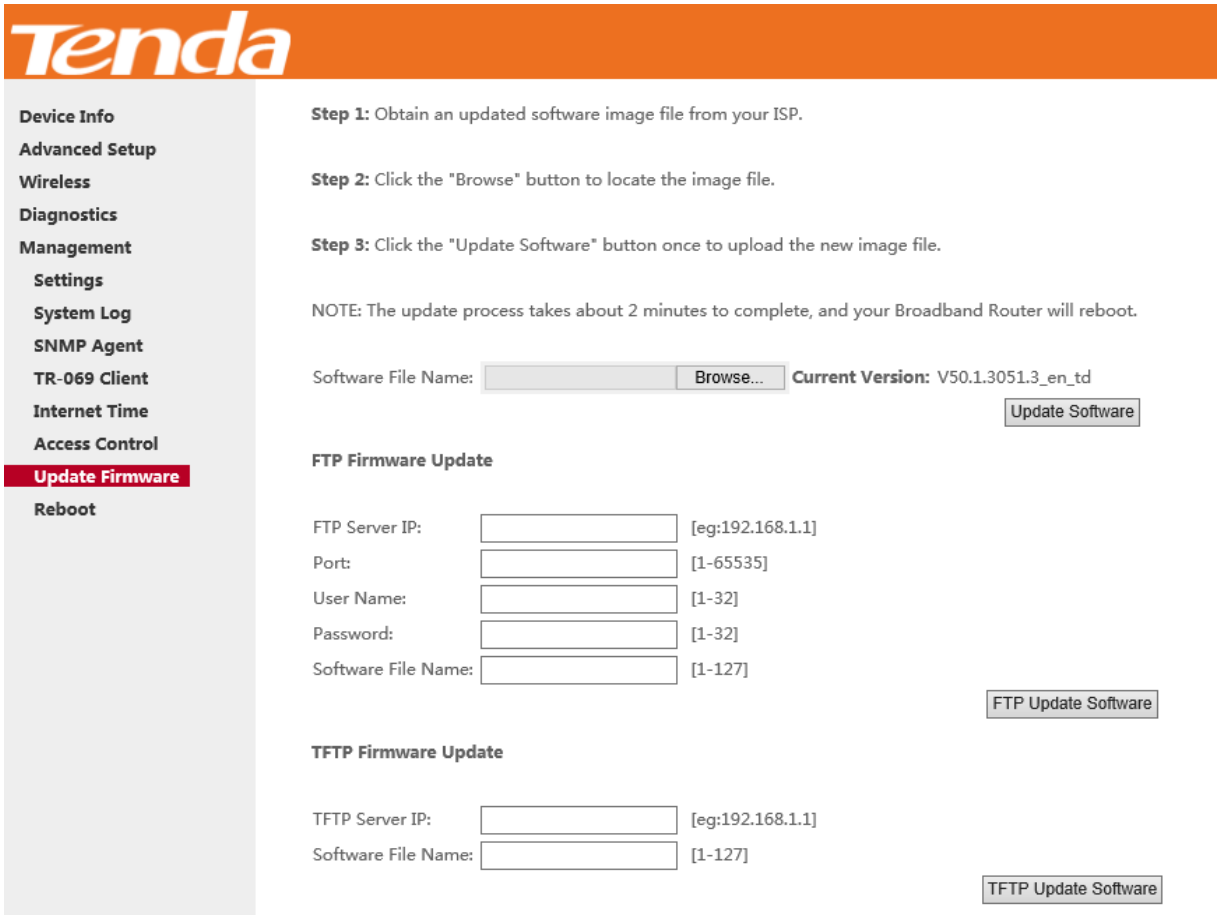


NOTE

If you are not an advanced user, it is recommended to keep the default settings.

4.5.7 Update Software

Firmware upgrade is released periodically to improve the functionality of your device and add any new features. If you run into a problem with a specific feature of the device you could log in to our website (www.tendacn.com) to download the latest firmware to update your device.

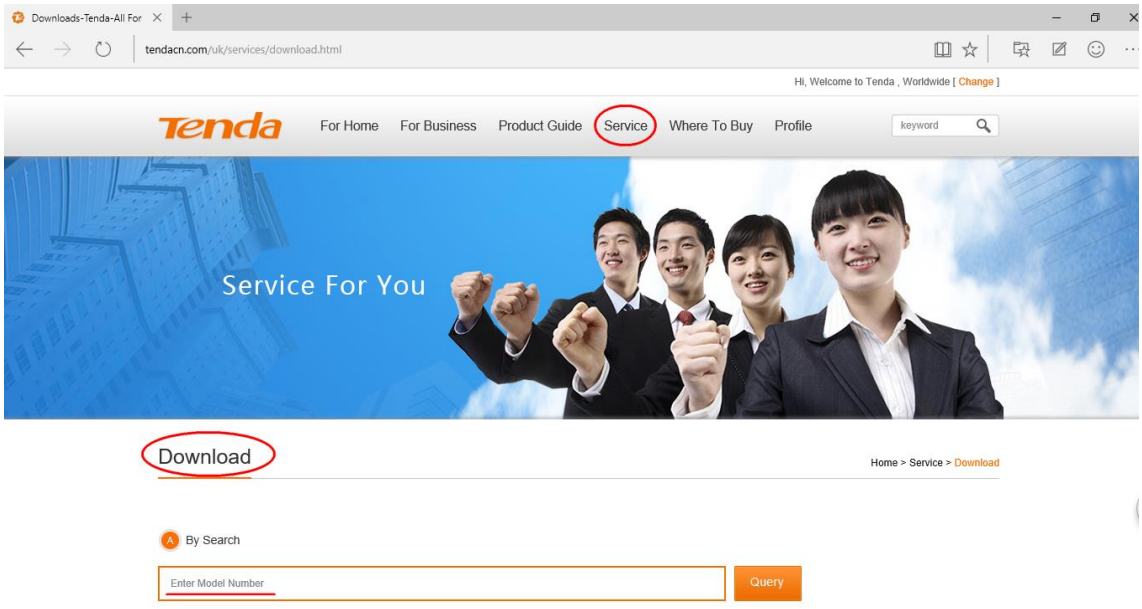


This modem router supports three types to update firmware.

Type 1: General Update

To update software, do as follows:

① Obtain an updated software image file from our website: www.tendacn.com.

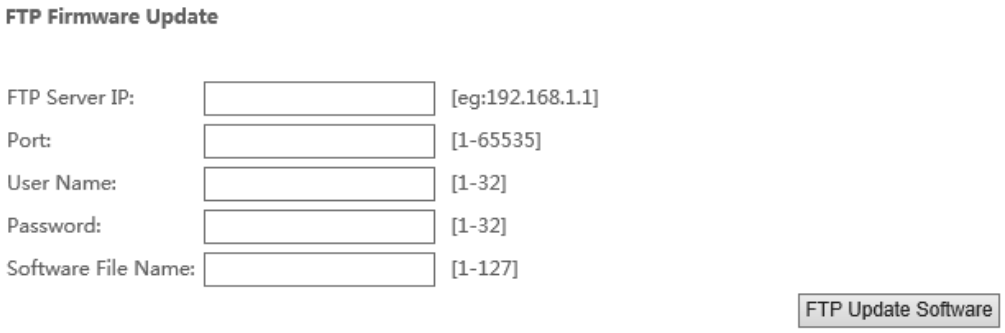


② Click the "Browse" button to locate the firmware file.

③ Click Update Software to start updating.

Type 2: Updating Via FTP Server

Updating via FTP server is supported. Make sure there is an available FTP server.



① Type the FTP Server IP address, like the right figure

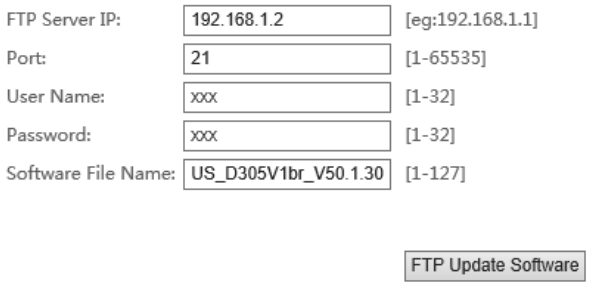
② Type the port the FTP server used.

③ Type the user name and password to access the FTP server.

④ Copy the name of the firmware.

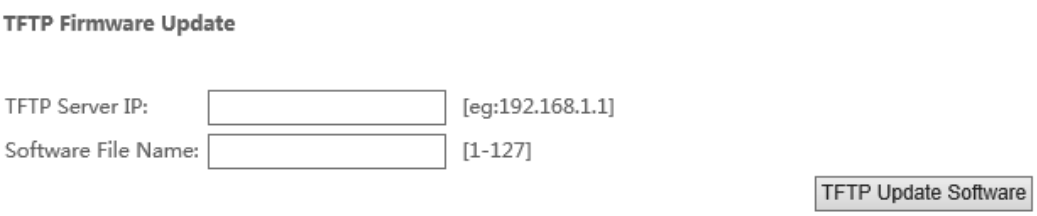
⑤ Click FTP Update Software to start updating.

Example



Type 3: Updating Via TFTP Server

Updating via TFTP server is supported. Make sure there is an available TFTP server.

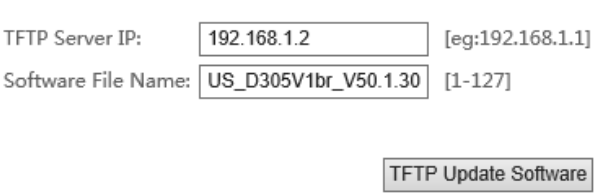


① Type the TFTP Server IP address in the field.

② Copy the name of the firmware.

③ Click TFTP Update Software to start updating.

Example

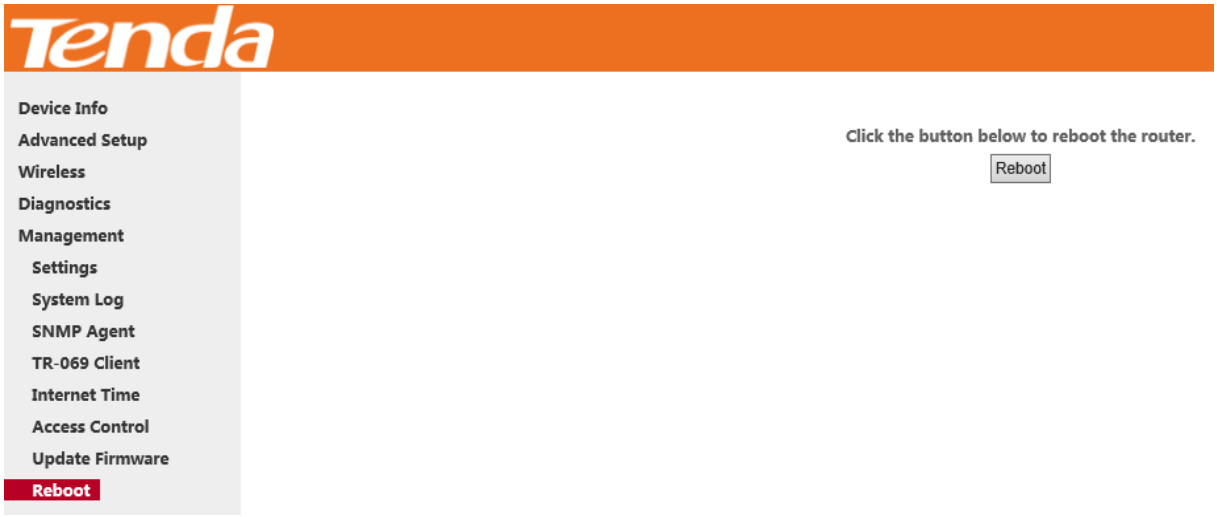


NOTE

The update process will cost 2 minutes, and the device will reboot.

4.5.8 Reboot

Click the **Reboot** button to reboot the router.



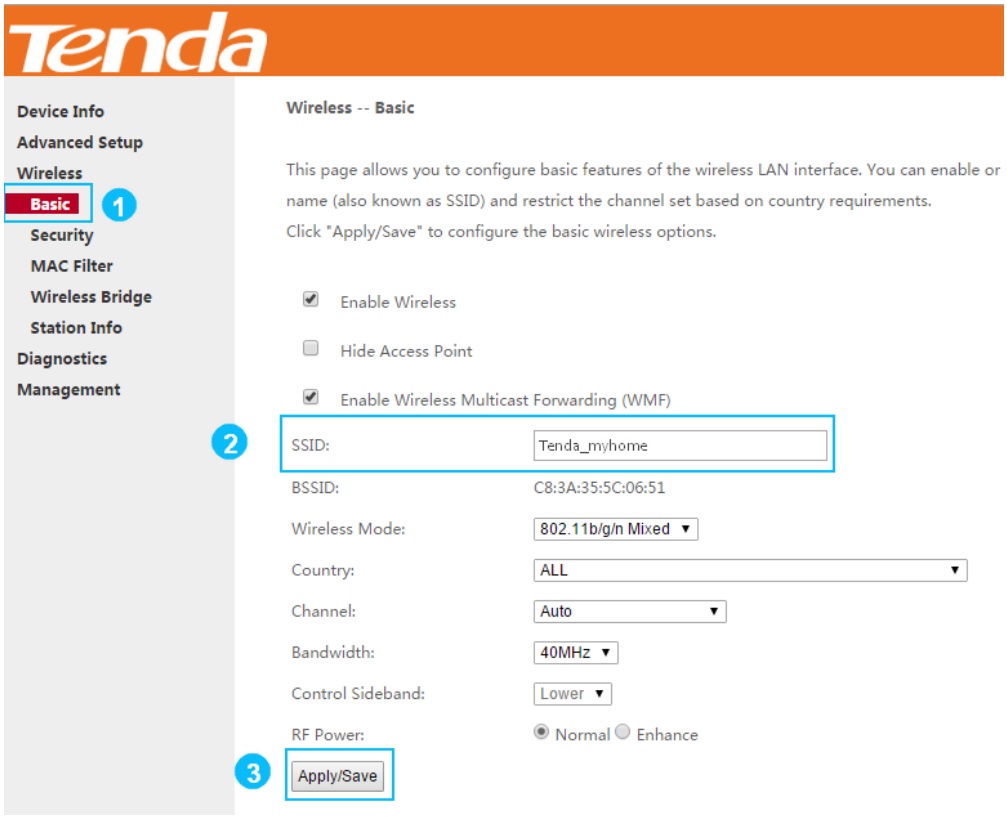
Appendix 1 Applications

Application 1: How to change SSID and wireless password?

① Go to **Wireless** > **Basic** interface.

② Specify a SSID as you like, like **Tenda_myhome**.

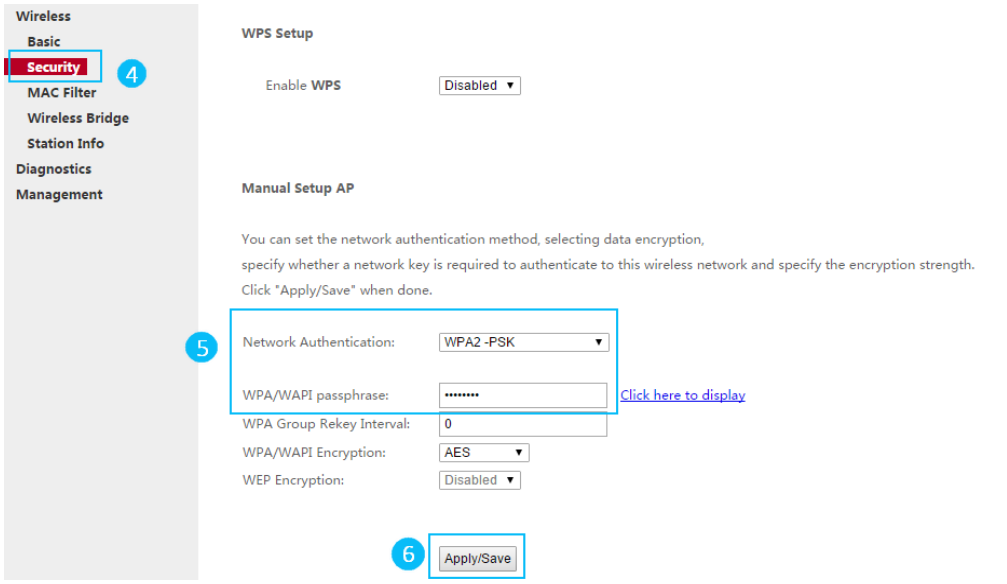
③ Click **Apply/Save** to save the settings.



④ Go to **Wireless** > **Security** interface.

⑤ Choose a network authentication (WPA2-PSK is recommended) and set a passphrase.

⑥ Click **Apply/Save** to save the settings.



Application 2: How to reset the modem router?

The device supports two methods to reset to factory defaults. Note that after you reset the device, you should reconfigure it for Internet service.

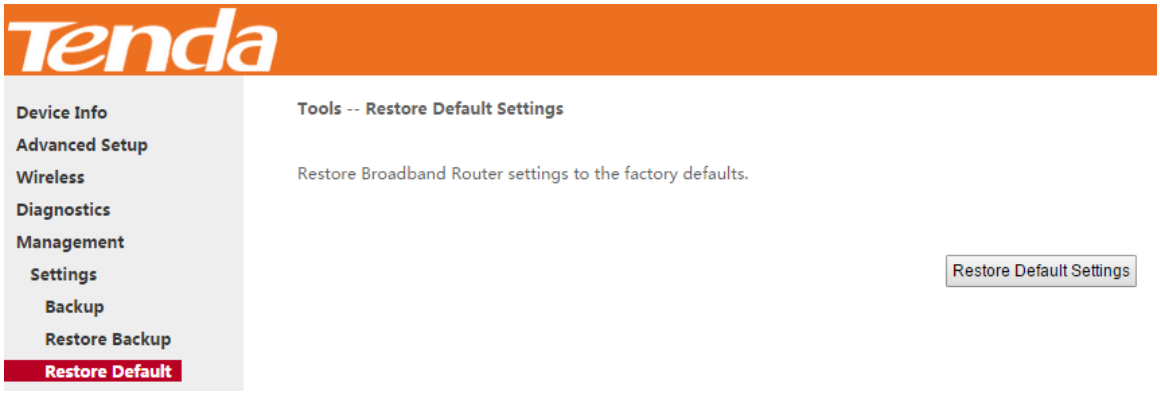
Method 1: WPS/RST button

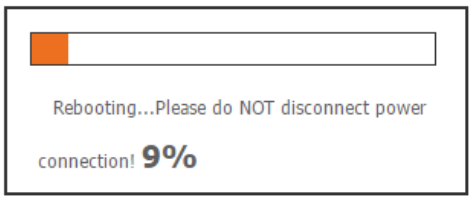
Press the WPS/RST button on the back of the modem router for about **8** seconds to reset it to factory defaults.

Method 2: Restore Default Settings from User Interface

① Go to **Management > Settings > Restore Default** to enter the interface below.

② Click Restore Default Settings icon to start resetting. And wait for the processing bar completing…





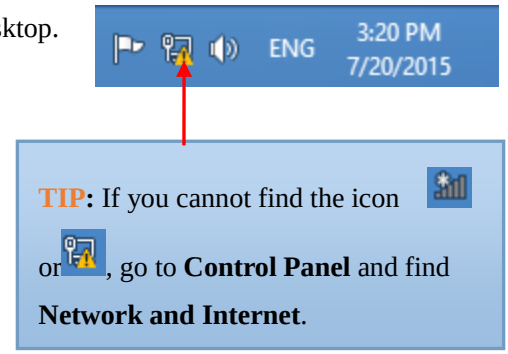
Appendix 2 Configure Your PC

This part is just for your references when your computer connecting to the modem router cannot get an IP address.

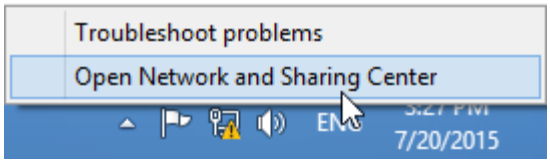
Screens to configure TCP/IP properties in other Operating Systems are similar to those below.

Windows 8

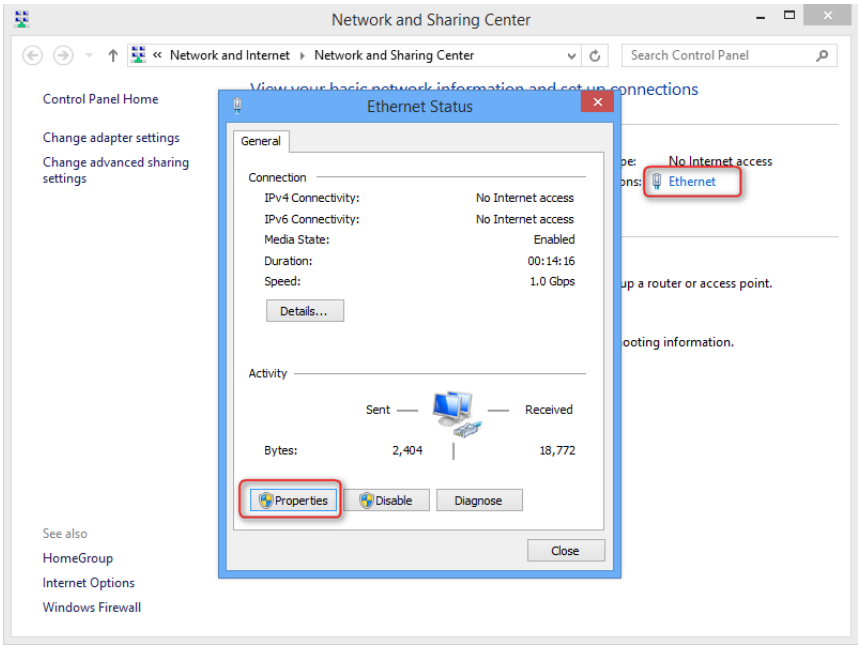
1. Right click the icon or on the bottom right corner of your desktop.



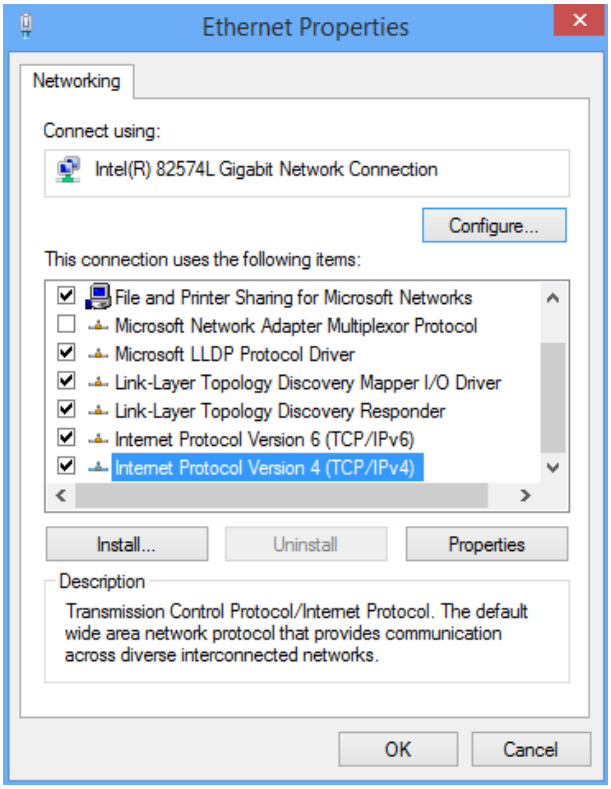
2. Click **Open Network and Sharing Center**.



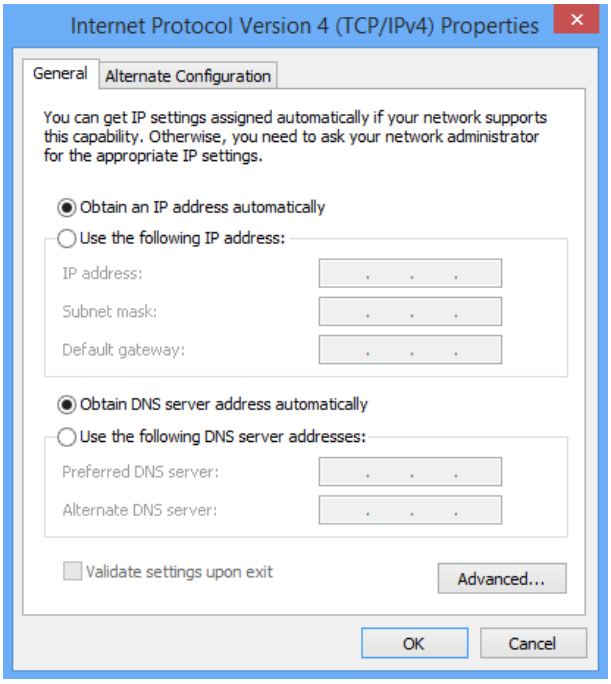
3. Click **Ethernet > Properties**.



4. Find and double click **Internet Protocol Version 4(TCP/IPv4)**.



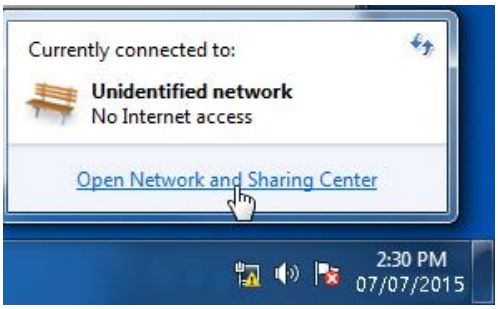
5. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically** and click **OK**.



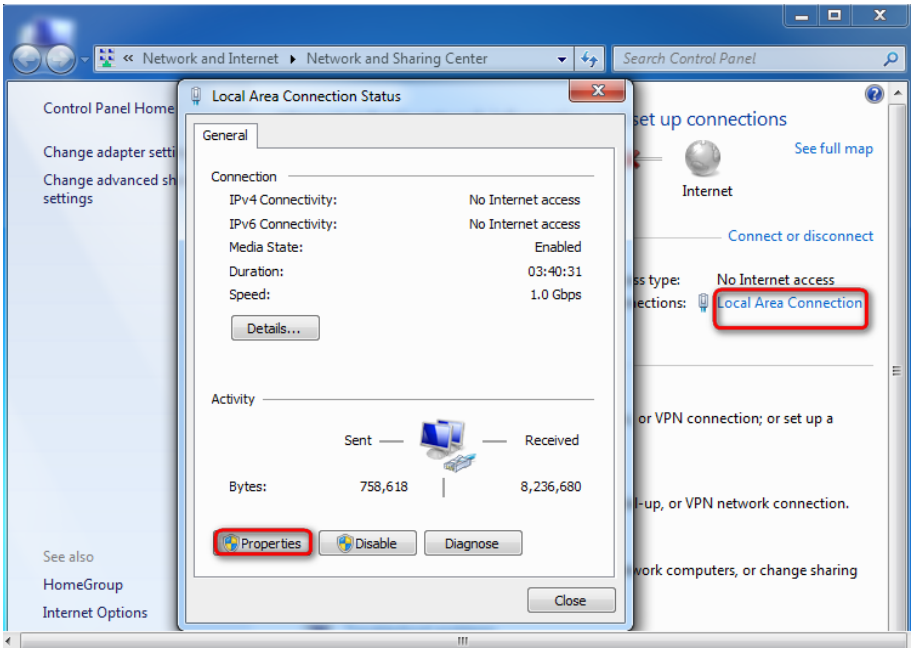
6. Click **OK** on the **Ethernet Properties** window (see **Step 4** for the screenshot).

Windows 7

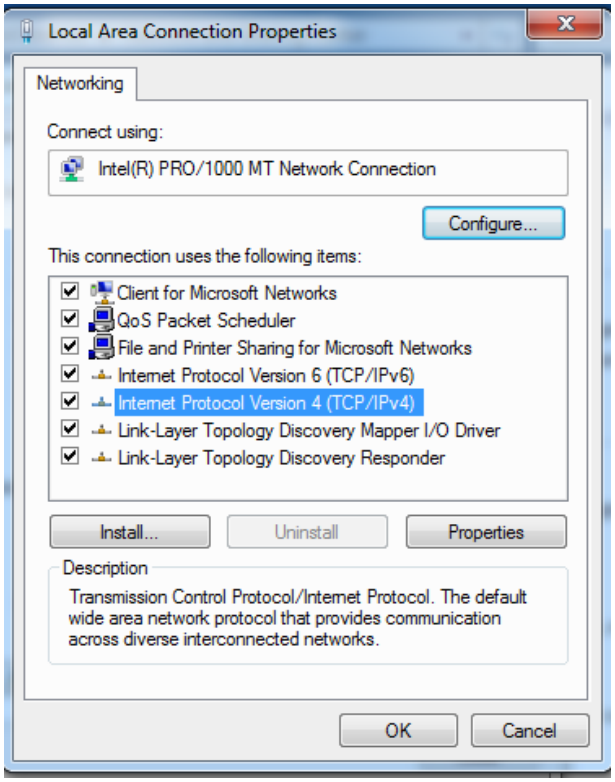
1. Click the icon on the bottom right corner of your desktop.
2. Click **Open Network and Sharing Center**.



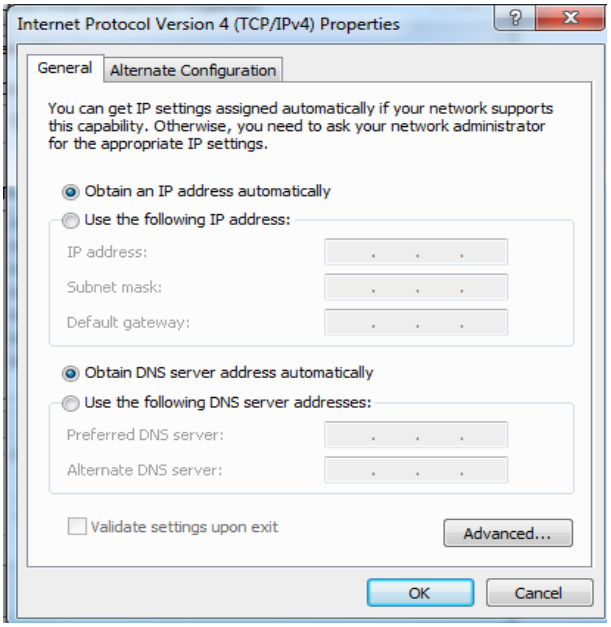
3. Click **Local Area Connection > Properties**.



4. Find and double click **Internet Protocol Version 4(TCP/IPv4)**.



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



6. Click **OK** on the **Local Area Connection Properties** window (see **Step 4** for the screenshot).

MAC

1. Click on the **Apple** icon from the top-left corner and select **System Preferences**.

2. Click **Network**.

3. Click on **Ethernet**.
4. Select **Using DHCP**.
5. Click **Apply**.

Appendix 3 Join Your Wireless Network

Windows 8

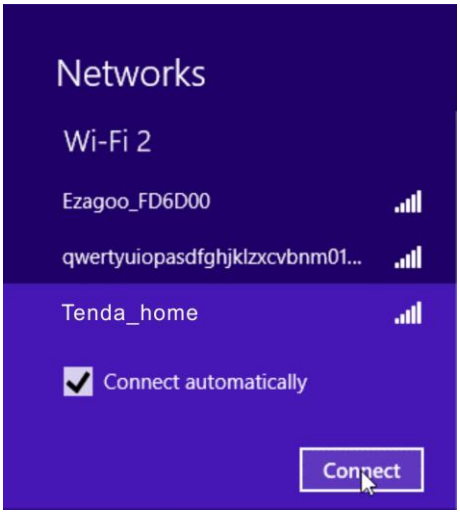
1. Click the icon on the bottom right corner of your desktop.

TIP:

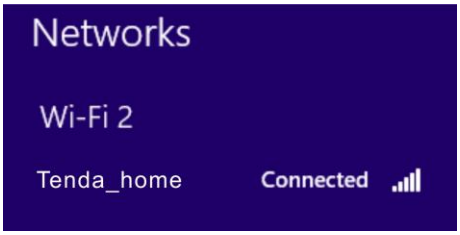
1. If you cannot find the icon, please move your mouse to the top right corner of your desktop, select **Settings > Control Panel > Network and Internet > Network and Sharing Center > Change adapter settings**, right click **Wi-Fi** and select **Connect/Disconnect**.

2. If you cannot find your wireless network from the list, ensure the Airplane Mode is not enabled on your PC.

2. Select your wireless network from the list, click **Connect** and then follow onscreen instructions.

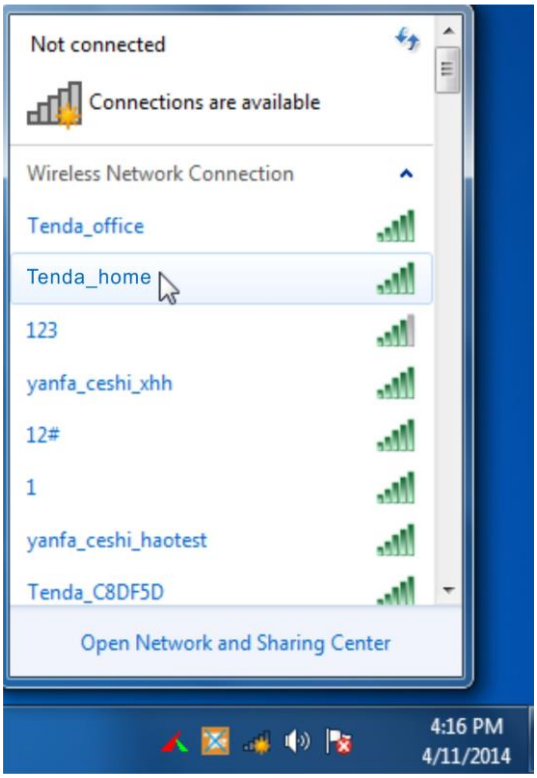


3. When your wireless network is connected successfully, the following screen will appear.

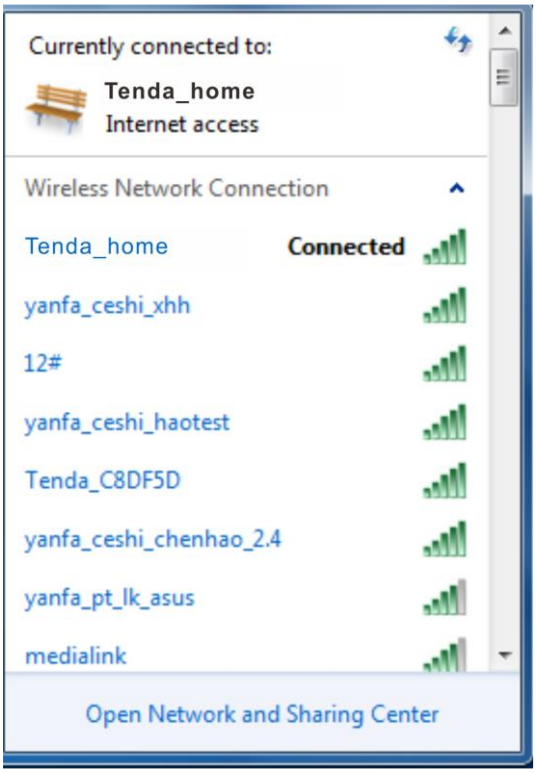


Windows 7

1. Click the icon on the bottom right corner of your desktop.
2. Double click your SSID (wireless network name) and then follow onscreen instructions.



3. When your SSID (wireless network name) displays **Connected** as shown below, you've connected to it for Internet access successfully.

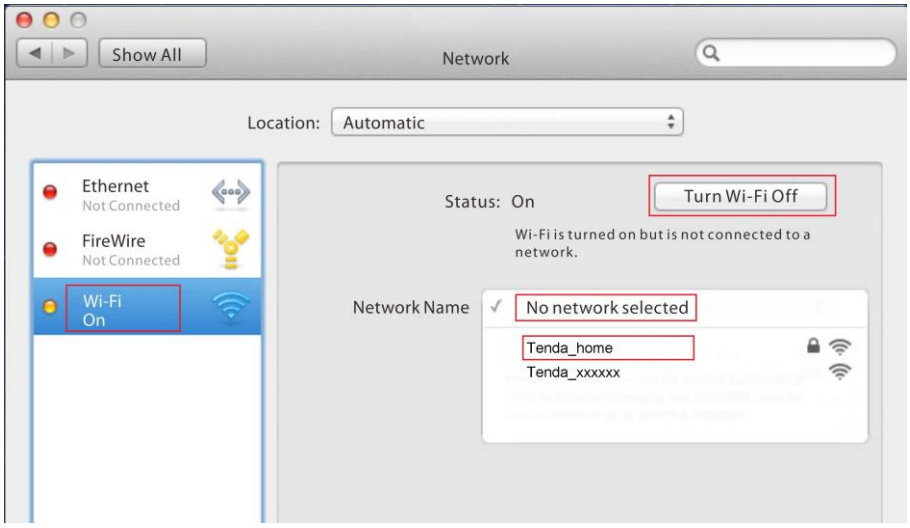


MAC

1. Click > **System Preferences**.

2. Select **Network** from **Internet & Network**.

3. Click **WiFi**.
4. Turn WiFi on.
5. Click **No network selected**.
6. Select the wireless network name of your router.



7. Enter the wireless password and click **Join**.

iPhone/iPad

1. Scroll screen to find the **Settings** icon and click it.

2. Click WiFi, and turn on WiFi.
3. Find the name of the wireless network you wish to connect, and click it.

4. Enter the wireless password and click **Join**.

Connected successfully!

Appendix 4 FAQs

1. What information should I have to access the Internet via the DSL uplink?

If you have DSL broadband service, you might need the following information to set up your modem router.

• Active Internet service provided by a DSL account

• The ISP configuration information for your DSL account

- ISP login name and password

- Fixed or static IP address

Depending on how your ISP set up your Internet account, you could need to know the Virtual path identifier (VPI) and virtual channel identifier (VCI) parameters for a manual setup.

2. I cannot access the device's User Interface (UI). What should I do?

1) Verify the physical connection (namely, the Ethernet cable) between your PC and the modem router. For details, see **Chapter 2 Hardware Installation** hereof.

2) Double check the TCP/IP settings on your PC. For details, see **Appendix 2 Configure Your PC** hereof.

3) Press the **WPS/RST** button on the device for about 8 seconds and then re-access the UI with the default login info "admin".

4) Change the Ethernet cable that connects your PC and the device.

5) Try accessing device management interface from other PCs, smart phones or iPads.

6) Connect your PC alone to one of the LAN ports on the device.

3. What can I do if I forget my password?

1) If you forgot your login password, restore the device to its factory default settings and then use the default User Name "admin" and Password "admin" to log in.

2) If you forgot your wireless network password, log in to the device User Interface, and go to **Wireless > Security** to check or change your password.

4. Why cannot I connect to the searched wireless network?

1) Verify that you entered a correct security key.

2) Log in to the device, select **Advanced** > **Wireless** and change the wireless network name (SSID). Then connect again.

3) Log in to the device, select **Advanced** > **Wireless** > **Security** and change the security settings. Then connect again.

Appendix 5 VPI/VCI List

The following table lists common ISPs and their VPI and VCI numbers. If you cannot locate your ISP and their VPI and VCI information here, ask your ISP to provide it.

Country	ISP	VPI	VCI	Encapsulation
Australia	Telstra	8	35	PPPoA LLC
Australia	GoldenIT	8	35	PPPOA_VCMUX
Australia	Telstra Bigpond	8	35	PPPOE_LLC
Australia	OptusNET	8	35	PPPOE_VCMUX
Australia	AAPT	8	35	PPPOE_VCMUX
Australia	ADSL Direct	8	35	PPPOE_LLC
Australia	Ausie Broadband	8	35	PPPOE_LLC
Australia	Australia On Line	8	35	PPPOA_VCMUX
Australia	Connexus	8	35	PPPOE_LLC
Australia	Dodo	8	35	PPPOE_LLC
Australia	Gotalk	8	35	PPPOE_VCMUX
Australia	Internode	8	35	PPPOE_VCMUX
Australia	iPrimus	8	35	PPPOA_VCMUX
Australia	Netspace	8	35	PPPOE_VCMUX
Australia	Southern Cross Telco	8	35	PPPOE_LLC
Australia	TPG Internet	8	35	PPPOE_LLC
Argentina	Telecom	0	33	PPPoE LLC
Argentina	Telefonica	8	35	PPPoE LLC
Argentina		1	33	PPPoA VC-MUX
Belgium	ADSL Office	8	35	1483 Routed IP LLC
Belgium	Turboline	8	35	PPPoA LLC
Belgium	Turboline	8	35	1483 Bridged IP LLC
Belgium	ADSL Office	8	35	1483 Bridged IP LLC
Bolivia		0	34	1483 Routed IP LLC
Brazil	Brasil Telcom	0	35	PPPoE LLC
Brazil	Telefonica	8	35	PPPoE LLC

Country	ISP	VPI	VCI	Encapsulation
Brazil	Telmar	0	33	PPPoE LLC
Brazil	South Region	1	32	PPPoE LLC
Canada	Primus Canada	0	35	PPPoE LLC
Canada	Rogers Canada (1)	0	35	PPPoE LLC
Canada	Rogers Canada (2)	8	35	1483 Bridged IP LLC
Canada	Rogers Canada (3)	0	35	1484 Bridged IP LLC
Canada	BellSouth(1) Canada	8	35	PPPoE LLC
Canada	BellSouth(2) Canada	0	35	PPPoE LLC
Canada	Sprint (1) Canada	0	35	PPPoA LLC
Canada	Sprint (2) Canada	8	35	PPPoE LLC
Canada	Verizon (1) Canada	0	35	PPPoE LLC
Canada	Verizon (2) Canada	0	35	1483 Bridged IP LLC
Colombia	EMCALI	0	33	PPPoA VC-MUX
Columbia	ETB	0	33	PPPoE LLC
Costa Rica	ICE	1	50	1483 Routed IP LLC
Czech Republic		8	48	1483 Bridged IP LLC
Denmark	Cybercity, Tiscali	0	35	PPPoA VC-MUX
Dominican Republic		0	33	1483 Bridged IP LLC
Dubai		0	50	1483 Bridged IP LLC
Egypt:	TE-data	0	35	1483 Bridged IP LLC
Egypt:	Linkdsl	0	35	1483 Bridged IP LLC
Egypt:	Vodafone	8	35	1483 Bridged IP LLC
Finland	Saunalahti	0	100	1483 Bridged IP LLC
Finland	Elisa	0	100	1483 Bridged IP LLC
Finland	DNA	0	100	1483 Bridged IP LLC
Finland	Sonera	0	35	1483 Bridged IP LLC
France	Free	8	36	LLC
France (1)	Orange	8	35	PPPoE LLC
France (2)		8	67	PPPoE LLC
France (3)	SFR	8	35	PPPoA VC-MUX
Germany		1	32	PPPoE LLC

Country	ISP	VPI	VCI	Encapsulation
Hungary	Sci-Network	0	35	PPPoE LLC
Iceland	Islandssimi	0	35	PPPoA VC-MUX
Iceland	Siminn	8	48	PPPoA VC-MUX
India	Airtel	1	32	1483 Bridged IP LLC
India	BSNL	0	35	1483 Bridged IP LLC
India	MTNL	0	35	1483 Bridged IP LLC
India	RELIANCE COMMUNICATION	0	35	PPPOE LLC
India	TATA INDICOM	0	32	PPPOE LLC
India	CONNECT	1	32	PPPOE LLC
Indonesia Speedy Telkomnet		8	81	PPPoE LLC
Iran	[Shatel] Aria-Rasaneh-Tadbir	0	35	PPPOE LLC
Iran	Asia-Tech	0	35	PPPOE LLC
Iran	Pars-Online (Tehran)	0	35	PPPOE LLC
Iran	Pars-Online (Provinces)	0	59	PPPOE LLC
Iran	[Saba-Net] Neda-Gostar-Saba	0	35	PPPOE LLC
Iran	Pishgaman-Tose	0	35	PPPOE LLC
Iran	Fan-Ava	8	35	PPPOE LLC
Iran	Datak	0	35	PPPOE LLC
Iran	Laser (General)	0	35	PPPOE LLC
Iran	Laser (Privates)	0	32	PPPOE LLC
Iran	Asr-Enteghal-Dadeha	8	35	PPPOE LLC
Iran	Kara-Amin-Ertebat	0	33	PPPOE LLC
Iran	ITC	0	35	PPPOE LLC
Iran (1)		0	35	PPPoE LLC
Iran (2)		8	81	PPPoE LLC
Iran	Dadegostar Asre Novin	0	33	PPPOE LLC
Israel		8	35	PPPoA VC-MUX

Country	ISP	VPI	VCI	Encapsulation
Israel(1)		8	48	PPPoA VC-MUX
Italy		8	35	1483 Bridged IP LLC
Italy		8	35	PPPoA VC-MUX
Jamaica (1)		8	35	PPPoA VC-MUX
Jamaica (2)		0	35	PPPoA VC-MUX
Jamaica (3)		8	35	1483 Bridged IP LLC SNAP
Jamaica (4)		0	35	1483 Bridged IP LLC SNAP
Kazakhstan	Kazakhtelecom «Megaline»	0	40	LLC/SNAP Bridging
Kazakhstan		0	33	PPPoA VC-MUX
kuwait unitednetwork		0	33	1483 Bridged IP LLC
Malaysia	Streamyx	0	35	PPPOE LLC
Malaysia		0	35	PPPoE LLC
Mexico	Telmex (1)	8	81	PPPoE LLC
Mexico	Telmex (2)	8	35	PPPoE LLC
Mexico	Telmex (3)	0	81	PPPoE LLC
Mexico	Telmex (4)	0	35	PPPoE LLC
morocco	IAM	8	35	PPPOE
Netherlands	BBNED	0	35	PPPoA VC-MUX
Netherlands	MXSTREAM	8	48	1483 Bridged IP LLC
Netherlands	BBNED	0	35	1483 Bridged IP LLC
Netherlands	MX Stream	8	48	PPPoA VC-MUX
New Zealand	Xtra	0	35	PPPoA VC-MUX
New Zealand	Slingshot	0	100	PPPoA VC-MUX
Orange Nyumbani (Kenya)		0	35	PPPoE LLC
Pakistan (PALESTINE)		8	35	1483 Bridged IP LLC
Pakistan for PTCL		0	103	1483 Bridged IP LLC
Pakistan (cyber net)		8	35	PPPoE LLC
Pakistan (linkDotnet)		0	35	PPPoA LLC
Pakistan(PTCL)		8	81	PPPoE LLc

Country	ISP	VPI	VCI	Encapsulation
Philippines(1)		0	35	1483 Bridged IP LLC
Philippines(2)		0	100	1483 Bridged IP LLC
Portugal		0	35	PPPoE LLC
Puerto Rico	Coqui.net	0	35	PPPoA LLC
RomTelecom Romania:		0	35	1483 Bridged IP LLC
Russia	Rostel	0	35	PPPoE LLC
Russia	Port telecom	0	35	PPPoE LLC
Russia	VNTC	8	35	PPPoE LLC
Saudi Arabia (1)		0	33	PPPoE LLC
Saudi Arabia (2)		0	35	PPPoE LLC
Saudi Arabia (3)		0	33	1483 Bridged IP LLC
Saudi Arabia (4)		0	33	1483 Routed IP LLC
Saudi Arabia (5)		0	35	1483 Bridged IP LLC
Saudi Arabia (6)		0	35	1483 Routed IP LLC
Spain	Arrakis	0	35	1483 Bridged IP VC-MUX
Spain	Auna	8	35	1483 Bridged IP VC-MUX
Spain	Comunitel	0	33	1483 Bridged IP VC-MUX
Spain	Eresmas	8	35	1483 Bridged IP VC-MUX
Spain	Jazztel	8	35	IPOE VC-MUX
Spain	Jazztel ADSL2+/ Desagregado	8	35	1483 Bridged IP LLC-BRIDGING
Spain	OpenforYou	8	32	1483 Bridged IP VC-MUX
Spain	Tele2	8	35	1483 Bridged IP VC-MUX
Spain	Telefónica (España)	8	32	1483 Bridged IP LLC/SNAP
Spain	Albura, Tiscali	1	32	PPPoA VC-MUX
Spain	Colt Telecom, Ola Internet	0	35	PPPoA VC-MUX
Spain	EresMas, Retevision	8	35	PPPoA VC-MUX
Spain	Telefonica (1)	8	32	PPPoE LLC
Spain	Telefonica (2), Terra	8	32	1483 Routed IP LLC
Spain	Wanadoo (1)	8	35	PPPoA VC-MUX

Country	ISP	VPI	VCI	Encapsulation
Spain	Wanadoo (2)	8	32	PPPoE LLC
Spain	Terra	8	32	1483 Bridged IP LLC/SNAP
Spain	Terra	8	32	1483 Bridged IP LLC/SNAP
Spain	Uni2	1	33	1483 Bridged IP VC-MUX
Spain	Orange	8	35	1483 Bridged IP VC-MUX
Spain	Orange 20 Megas	8	35	LLC-BRIDGING
Spain	Orange	8	32	1483 Bridged IP LLC/SNAP
Spain	Ya.com	8	32	1483 Bridged IP VC - MUX
Spain	Ya.com	8	32	1483 Bridged IP LLC/SNAP
Spain	Wanadoo (3)	8	32	1483 Routed IP LLC
SpainWanadoo		8	32	1483 Bridged IP LLC
Sri Lanka Telecom-(SLT)		8	35	PPPOE LLC
Sweden	Telenordia	8	35	PPPoE
Sweden	Telia	8	35	1483 Routed IP LLC
Switzerland		8	35	1483 Bridged IP LLC
Switzerland		8	35	PPPoE LLC
Telefónica (Argentina)		8	35	1483 Bridged IP LLC-based
Telefónica (Perú)		8	48	1483 Bridged IP VC-MUX
Thailand	TRUE	0	100	PPPoE LLC
Thailand	TOT	1	32	PPPoE LLC
Thailand	3BB	0	33	PPPoE LLC
Thailand	Cat Telecom	0	35	PPPoE LLC
Thailand	BuddyBB	0	35	PPPoE LLC
Trinidad & Tobago	TSTT	0	35	PPPoA VC-MUX
Turkey (1)		8	35	PPPoE LLC
Turkey (2)		8	35	PPPoA VC-MUX
UAE (Al sahmil)		0	50	1483 Bridged IP LLC
United States	4DV.Net	0	32	PPPoA VC-MUX
United States	All Tel (1)	0	35	PPPoE LLC
United States	All Tel (2)	0	35	1483 Bridged IP LLC

Country	ISP	VPI	VCI	Encapsulation
United States	Ameritech	8	35	PPPoA LLC
United States	AT&T (1)	0	35	PPPoE LLC
United States	AT&T (2)	8	35	1483 Bridged IP LLC
United States	AT&T (3)	0	35	1483 Bridged IP LLC
United States	August.net (1)	0	35	1483 Bridged IP LLC
United States	August.net (2)	8	35	1483 Bridged IP LLC
United States	BellSouth	8	35	PPPoE LLC
United States	Casstle.Net	0	96	1483 Bridged IP LLC
United States	CenturyTel (1)	8	35	PPPoE LLC
United States	CenturyTel (2)	8	35	1483 Bridged IP LLC
United States	Coqui.net	0	35	PPPoA LLC
United States	Covad	0	35	PPPoE LLC
United States	Earthlink (1)	0	35	PPPoE LLC
United States	Earthlink (2)	8	35	PPPoE LLC
United States	Earthlink (3)	8	35	PPPoE VC-MUX
United States	Earthlink (4)	0	32	PPPoA LLC
United States	Eastex	0	100	PPPoA LLC
United States	Embarq	8	35	1483 Bridged IP LLC
United States	Frontier	0	35	PPPoE LLC
United States	Grande ommunications	1	34	PPPoE LLC
United States	GWI	0	35	1483 Bridged IP LLC
United States	Hotwire	0	35	1483 Bridged IP LLC
United States	Internet Junction	0	35	1484 Bridged IP LLC
United States	PVT	0	35	1485 Bridged IP LLC
United States	QWest (1)	0	32	PPPoALLC
United States	QWest (2)	0	32	PPPoA VC-MUX
United States	QWest (3)	0	32	1483 Bridged IP LLC
United States	QWest (4)	0	32	PPPoE LLC
United States	SBC (1)	0	35	PPPoE LLC
United States	SBC (2)	0	35	1483 Bridged IP LLC
United States	SBC (3)	8	35	1483 Bridged IP LLC

Country	ISP	VPI	VCI	Encapsulation
United States	Sonic	0	35	1484 Bridged IP LLC
United States	SouthWestern Bell	0	35	1483 Bridged IP LLC
United States	Sprint (1)	0	35	PPPoALLC
United States	Sprint (2)	8	35	PPPoE LLC
United States	Sprint Territory	0	35	PPPoE LLC
United States	SureWest Communications(1)	0	34	1483 Bridged LLC Snap
United States	SureWest Communications(2)	0	32	PPPoE LLC
United States	SureWest Communications(3)	0	32	PPPoA LLC
United States	Toast.Net	0	35	PPPoE LLC
United States	Uniserv	0	33	1483 Bridged IP LLC
United States	US West	0	32	PPPoA VC-MUX
United States	Verizon (1)	0	35	PPPoE LLC
United States	Verizon (2)	0	35	1483 Bridged IP LLC
United States	Windstream	0	35	PPPoE LLC
United States	Verizon (2)	0	35	1483 Bridged IP LLC
United Kingdom (1)		0	38	PPPoA VC-MUX
United Kingdom (2)		0	38	PPPoE LLC
United Kingdom	AOL	0	38	PPPoE VC-MUX
United Kingdom	Karoo	1	50	PPPoA LLC
UK		0	38	1483 Bridged IP LLC
Uzbekistan	Sharq Stream	8	35	PPPoE LLC
Uzbekistan	Sarkor	0	33	PPPoE LLC
Uzbekistan	TShTT	0	35	PPPoE LLC
Venezuela	CANTV	0	33	1483 Routed IP LLC
Vietnam		0	35	PPPoE LLC
Vietnam	VDC	8	35	PPPoE LLC
Vietnam	Viettel	8	35	PPPoE LLC
Vietnam	FPT	0	33	PPPoE LLC

Country	ISP	VPI	VCI	Encapsulation
Australia	Telstra	8	35	PPPoA LLC
Australia	GoldenIT	8	35	_PPPOA_VCMUX
Australia	Telstra Bigpond	8	35	PPPOE_LLC
Australia	OptusNET	8	35	PPPOE_VCMUX
Australia	AAPT	8	35	PPPOE_VCMUX
Australia	ADSL Direct	8	35	PPPOE_LLC
Australia	Ausie Broadband	8	35	PPPOE_LLC
Australia	Australia On Line	8	35	PPPOA_VCMUX
Australia	Connexus	8	35	PPPOE_LLC
Australia	Dodo	8	35	PPPOE_LLC
Australia	Gotalk	8	35	PPPOE_VCMUX
Australia	Internode	8	35	PPPOE_VCMUX
Australia	iPrimus	8	35	PPPOA_VCMUX
Australia	Netspace	8	35	PPPOE_VCMUX
Australia	Southern Cross Telco	8	35	PPPOE_LLC
Australia	TPG Internet	8	35	PPPOE_LLC
Argentina	Telecom	0	33	PPPoE LLC
Argentina	Telefonica	8	35	PPPoE LLC
Argentina		1	33	PPPoA VC-MUX
Belgium	ADSL Office	8	35	1483 Routed IP LLC
Belgium	Turboline	8	35	PPPoA LLC
Belgium	Turboline	8	35	1483 Bridged IP LLC
Belgium	ADSL Office	8	35	1483 Bridged IP LLC
Bolivia		0	34	1483 Routed IP LLC
Brazil	Brasil Telcom	0	35	PPPoE LLC
Brazil	Telefonica	8	35	PPPoE LLC
Brazil	Telmar	0	33	PPPoE LLC
Brazil	South Region	1	32	PPPoE LLC
Canada	Primus Canada	0	35	PPPoE LLC
Canada	Rogers Canada (1)	0	35	PPPoE LLC
Canada	Rogers Canada (2)	8	35	1483 Bridged IP LLC

Country	ISP	VPI	VCI	Encapsulation
Canada	Rogers Canada (3)	0	35	1484 Bridged IP LLC
Canada	BellSouth(1) Canada	8	35	PPPoE LLC
Canada	BellSouth(2) Canada	0	35	PPPoE LLC
Canada	Sprint (1) Canada	0	35	PPPoA LLC
Canada	Sprint (2) Canada	8	35	PPPoE LLC
Canada	Verizon (1) Canada	0	35	PPPoE LLC
Canada	Verizon (2) Canada	0	35	1483 Bridged IP LLC
Colombia	EMCALI	0	33	PPPoA VC-MUX
Columbia	ETB	0	33	PPPoE LLC
Costa Rica	ICE	1	50	1483 Routed IP LLC
Czech Republic		8	48	1483 Bridged IP LLC
Denmark	Cybercity, Tiscali	0	35	PPPoA VC-MUX
Dominican Republic		0	33	1483 Bridged IP LLC
Dubai		0	50	1483 Bridged IP LLC
Egypt:	TE-data	0	35	1483 Bridged IP LLC
Egypt:	Linkdsl	0	35	1483 Bridged IP LLC
Egypt:	Vodafone	8	35	1483 Bridged IP LLC
Finland	Saunalahti	0	100	1483 Bridged IP LLC
Finland	Elisa	0	100	1483 Bridged IP LLC
Finland	DNA	0	100	1483 Bridged IP LLC
Finland	Sonera	0	35	1483 Bridged IP LLC
France	Free	8	36	LLC
France (1)	Orange	8	35	PPPoE LLC
France (2)		8	67	PPPoE LLC
France (3)	SFR	8	35	PPPoA VC-MUX
Germany		1	32	PPPoE LLC
Hungary	Sci-Network	0	35	PPPoE LLC
Iceland	Islandssimi	0	35	PPPoA VC-MUX
Iceland	Siminn	8	48	PPPoA VC-MUX
India	Airtel	1	32	1483 Bridged IP LLC
India	BSNL	0	35	1483 Bridged IP LLC

Country	ISP	VPI	VCI	Encapsulation
India	MTNL	0	35	1483 Bridged IP LLC
India	RELIANCE COMMUNICATION	0	35	PPPOE LLC
India	TATA INDICOM	0	32	PPPOE LLC
India	CONNECT	1	32	PPPOE LLC
Indonesia Speedy Telkomnet		8	81	PPPoE LLC
Iran	[Shatel] Aria-Rasaneh-Tadbir	0	35	PPPOE LLC
Iran	Asia-Tech	0	35	PPPOE LLC
Iran	Pars-Online (Tehran)	0	35	PPPOE LLC
Iran	Pars-Online (Provinces)	0	59	PPPOE LLC
Iran	[Saba-Net] Neda-Gostar-Saba	0	35	PPPOE LLC
Iran	Pishgaman-Tose	0	35	PPPOE LLC
Iran	Fan-Ava	8	35	PPPOE LLC
Iran	Datak	0	35	PPPOE LLC
Iran	Laser (General)	0	35	PPPOE LLC
Iran	Laser (Privates)	0	32	PPPOE LLC
Iran	Asr-Enteghal-Dadeha	8	35	PPPOE LLC
Iran	Kara-Amin-Ertebat	0	33	PPPOE LLC
Iran	ITC	0	35	PPPOE LLC
Iran (1)		0	35	PPPoE LLC
Iran (2)		8	81	PPPoE LLC
Iran	Dadegostar Asre Novin	0	33	PPPOE LLC
Israel		8	35	PPPoA VC-MUX
Israel(1)		8	48	PPPoA VC-MUX
Italy		8	35	1483 Bridged IP LLC
Italy		8	35	PPPoA VC-MUX
Jamaica (1)		8	35	PPPoA VC-MUX
Jamaica (2)		0	35	PPPoA VC-MUX

Country	ISP	VPI	VCI	Encapsulation
Jamaica (3)		8	35	1483 Bridged IP LLC SNAP
Jamaica (4)		0	35	1483 Bridged IP LLC SNAP
Kazakhstan	Kazakhtelecom «Megaline»	0	40	LLC/SNAP Bridging
Kazakhstan		0	33	PPPoA VC-MUX
kuwait unitednetwork		0	33	1483 Bridged IP LLC
Malaysia	Streamyx	0	35	PPPOE LLC
Malaysia		0	35	PPPoE LLC
Mexico	Telmex (1)	8	81	PPPoE LLC
Mexico	Telmex (2)	8	35	PPPoE LLC
Mexico	Telmex (3)	0	81	PPPoE LLC
Mexico	Telmex (4)	0	35	PPPoE LLC
morocco	IAM	8	35	PPPOE
Netherlands	BBNED	0	35	PPPoA VC-MUX
Netherlands	MXSTREAM	8	48	1483 Bridged IP LLC
Netherlands	BBNED	0	35	1483 Bridged IP LLC
Netherlands	MX Stream	8	48	PPPoA VC-MUX
New Zealand	Xtra	0	35	PPPoA VC-MUX
New Zealand	Slingshot	0	100	PPPoA VC-MUX
Orange Nyumbani (Kenya)		0	35	PPPoE LLC
Pakistan (PALESTINE)		8	35	1483 Bridged IP LLC
Pakistan for PTCL		0	103	1483 Bridged IP LLC
Pakistan (cyber net)		8	35	PPPoE LLC
Pakistan (linkDotnet)		0	35	PPPoA LLC
Pakistan(PTCL)		8	81	PPPoE LLc
Philippines(1)		0	35	1483 Bridged IP LLC
Philippines(2)		0	100	1483 Bridged IP LLC
Portugal		0	35	PPPoE LLC
Puerto Rico	Coqui.net	0	35	PPPoA LLC
RomTelecom Romania:		0	35	1483 Bridged IP LLC

Country	ISP	VPI	VCI	Encapsulation
Russia	Rostel	0	35	PPPoE LLC
Russia	Port telecom	0	35	PPPoE LLC
Russia	VNTC	8	35	PPPoE LLC
Saudi Arabia (1)		0	33	PPPoE LLC
Saudi Arabia (2)		0	35	PPPoE LLC
Saudi Arabia (3)		0	33	1483 Bridged IP LLC
Saudi Arabia (4)		0	33	1483 Routed IP LLC
Saudi Arabia (5)		0	35	1483 Bridged IP LLC
Saudi Arabia (6)		0	35	1483 Routed IP LLC
Spain	Arrakis	0	35	1483 Bridged IP VC-MUX
Spain	Auna	8	35	1483 Bridged IP VC-MUX
Spain	Comunitel	0	33	1483 Bridged IP VC-MUX
Spain	Eresmas	8	35	1483 Bridged IP VC-MUX
Spain	Jazztel	8	35	IPOE VC-MUX
Spain	Jazztel ADSL2+ / Desagregado	8	35	1483 Bridged IP LLC-BRIDGING
Spain	OpenforYou	8	32	1483 Bridged IP VC-MUX
Spain	Tele2	8	35	1483 Bridged IP VC-MUX
Spain	Telefónica (España)	8	32	1483 Bridged IP LLC/SNAP
Spain	Albura, Tiscali	1	32	PPPoA VC-MUX
Spain	Colt Telecom, Ola Internet	0	35	PPPoA VC-MUX
Spain	EresMas, Retevision	8	35	PPPoA VC-MUX
Spain	Telefonica (1)	8	32	PPPoE LLC
Spain	Telefonica (2), Terra	8	32	1483 Routed IP LLC
Spain	Wanadoo (1)	8	35	PPPoA VC-MUX
Spain	Wanadoo (2)	8	32	PPPoE LLC
Spain	Terra	8	32	1483 Bridged IP LLC/SNAP
Spain	Terra	8	32	1483 Bridged IP LLC/SNAP
Spain	Uni2	1	33	1483 Bridged IP VC-MUX
Spain	Orange	8	35	1483 Bridged IP VC-MUX

Country	ISP	VPI	VCI	Encapsulation
Spain	Orange 20 Megas	8	35	LLC-BRIDGING
Spain	Orange	8	32	1483 Bridged IP LLC/SNAP
Spain	Ya.com	8	32	1483 Bridged IP VC - MUX
Spain	Ya.com	8	32	1483 Bridged IP LLC/SNAP
Spain	Wanadoo (3)	8	32	1483 Routed IP LLC
SpainWanadoo		8	32	1483 Bridged IP LLC
Sri Lanka Telecom-(SLT)		8	35	PPPOE LLC
Sweden	Telenordia	8	35	PPPoE
Sweden	Telia	8	35	1483 Routed IP LLC
Switzerland		8	35	1483 Bridged IP LLC
Switzerland		8	35	PPPoE LLC
Telefónica (Argentina)		8	35	1483 Bridged IP LLC-based
Telefónica (Perú)		8	48	1483 Bridged IP VC-MUX
Thailand	TRUE	0	100	PPPoE LLC
Thailand	TOT	1	32	PPPoE LLC
Thailand	3BB	0	33	PPPoE LLC
Thailand	Cat Telecom	0	35	PPPoE LLC
Thailand	BuddyBB	0	35	PPPoE LLC
Trinidad & Tobago	TSTT	0	35	PPPoA VC-MUX
Turkey (1)		8	35	PPPoE LLC
Turkey (2)		8	35	PPPoA VC-MUX
UAE (Al sahmil)		0	50	1483 Bridged IP LLC
United States	4DV.Net	0	32	PPPoA VC-MUX
United States	All Tel (1)	0	35	PPPoE LLC
United States	All Tel (2)	0	35	1483 Bridged IP LLC
United States	Ameritech	8	35	PPPoA LLC
United States	AT&T (1)	0	35	PPPoE LLC
United States	AT&T (2)	8	35	1483 Bridged IP LLC
United States	AT&T (3)	0	35	1483 Bridged IP LLC
United States	August.net (1)	0	35	1483 Bridged IP LLC

Country	ISP	VPI	VCI	Encapsulation
United States	August.net (2)	8	35	1483 Bridged IP LLC
United States	BellSouth	8	35	PPPoE LLC
United States	Casstle.Net	0	96	1483 Bridged IP LLC
United States	CenturyTel (1)	8	35	PPPoE LLC
United States	CenturyTel (2)	8	35	1483 Bridged IP LLC
United States	Coqui.net	0	35	PPPoA LLC
United States	Covad	0	35	PPPoE LLC
United States	Earthlink (1)	0	35	PPPoE LLC
United States	Earthlink (2)	8	35	PPPoE LLC
United States	Earthlink (3)	8	35	PPPoE VC-MUX
United States	Earthlink (4)	0	32	PPPoA LLC
United States	Eastex	0	100	PPPoA LLC
United States	Embarq	8	35	1483 Bridged IP LLC
United States	Frontier	0	35	PPPoE LLC
United States	Grande ommunications	1	34	PPPoE LLC
United States	GWI	0	35	1483 Bridged IP LLC
United States	Hotwire	0	35	1483 Bridged IP LLC
United States	Internet Junction	0	35	1484 Bridged IP LLC
United States	PVT	0	35	1485 Bridged IP LLC
United States	QWest (1)	0	32	PPPoALLC
United States	QWest (2)	0	32	PPPoA VC-MUX
United States	QWest (3)	0	32	1483 Bridged IP LLC
United States	QWest (4)	0	32	PPPoE LLC
United States	SBC (1)	0	35	PPPoE LLC
United States	SBC (2)	0	35	1483 Bridged IP LLC
United States	SBC (3)	8	35	1483 Bridged IP LLC
United States	Sonic	0	35	1484 Bridged IP LLC
United States	SouthWestern Bell	0	35	1483 Bridged IP LLC
United States	Sprint (1)	0	35	PPPoALLC
United States	Sprint (2)	8	35	PPPoE LLC
United States	Sprint Territory	0	35	PPPoE LLC

Country	ISP	VPI	VCI	Encapsulation
United States	SureWest Communications(1)	0	34	1483 Bridged LLC Snap
United States	SureWest Communications(2)	0	32	PPPoE LLC
United States	SureWest Communications(3)	0	32	PPPoA LLC
United States	Toast.Net	0	35	PPPoE LLC
United States	Uniserv	0	33	1483 Bridged IP LLC
United States	US West	0	32	PPPoA VC-MUX
United States	Verizon (1)	0	35	PPPoE LLC
United States	Verizon (2)	0	35	1483 Bridged IP LLC
United States	Windstream	0	35	PPPoE LLC
United States	Verizon (2)	0	35	1483 Bridged IP LLC
United Kingdom (1)		0	38	PPPoA VC-MUX
United Kingdom (2)		0	38	PPPoE LLC
United Kingdom	AOL	0	38	PPPoE VC-MUX
United Kingdom	Karoo	1	50	PPPoA LLC
UK		0	38	1483 Bridged IP LLC
Uzbekistan	Sharq Stream	8	35	PPPoE LLC
Uzbekistan	Sarkor	0	33	PPPoE LLC
Uzbekistan	TShTT	0	35	PPPoE LLC
Venezuela	CANTV	0	33	1483 Routed IP LLC
Vietnam		0	35	PPPoE LLC
Vietnam	VDC	8	35	PPPoE LLC
Vietnam	Viettel	8	35	PPPoE LLC
Vietnam	FPT	0	33	PPPoE LLC

Appendix 6 Regulatory Compliance Information

CE Mark Warning

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

NOTE: (1) The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. (2) To avoid unnecessary radiation interference, it is recommended to use a shielded RJ45 cable.

FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with part 15 of the FCC Rules.

Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment.

NOTE: (1) The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. (2) To avoid unnecessary radiation interference, it is recommended to use a shielded RJ45 cable.