Tenda

User Guide

www.tendacn.com

Wireless AC1200 ADSL2+ Dual Band Modem Router

Copyright Statement

Disclaimer

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

Technical Support

Website: http://www.tendacn.com

Telephone: (86 755) 2765 7180

E-mail: support@tenda.com.cn

Contents

Chapter 1 Get to Know Your Router

1. What it does

The Wireless AC1200 ADSL2+ Dual Band Modem Router provides you with an easy and secure way to set up a wireless home network with fast access to the Internet over a high-speed digital subscriber line (DSL). Complete with a built-in ADSL modem, it is compatible with all major ADSL Internet service providers. It offers wireless speed of up to 1200Mbps (2.4G: 300Mbps; 5G: 900Mbps) needed for demanding applications, such as large file transfers, streaming HD video, and multiplayer gaming. The unit comes with a wide range of premium features and applications such as IPv6, SNMP, Multicast, IP tunnel, ready share USB, IPTV service and parental controls, etc. Plus, with the router, you can access the Internet via the ATM interface or Ethernet interface.

2. Product Features

Wireless AC speeds up to 1200 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 hard drive

Sharable Printer lets you print from your Windows computer to a connected USB printer

Advanced QoS 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: Bridging, PPPoE, IPoE, PPPoA, IPoA, 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 Setup Wizard for easy and fast installation and configuration

Tenda Green: Use hardware Power On/Off and software WiFi On/Off buttons to turn on and off power and WiFi to save energy when not in use

3. Package Contents

Your box should contain the following items:

- Wireless AC1200 ADSL2+ Dual Band Modem Router
- Phone Cable
- Ethernet Cable
- 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 the dealer for immediate replacement.

Chapter 2 Hardware Install

You can also set up your new router instead of using the Install Guide that comes in the box. This chapter walks you through the hardware install.

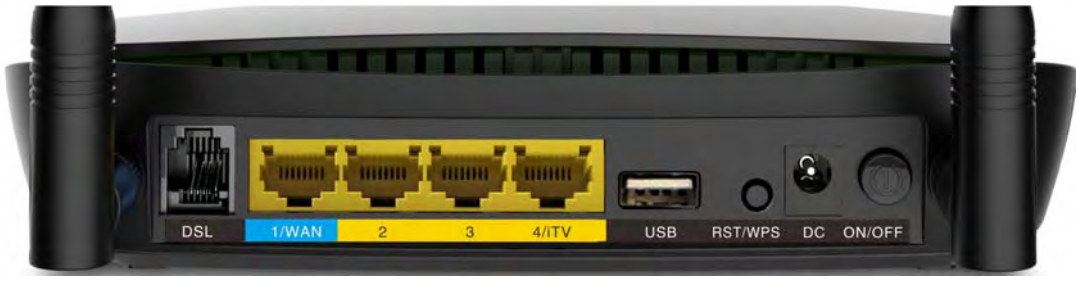
1. LED Indicators, Buttons and Interfaces

Front Panel

LED	Status	Description
PWR	Solid	Power is supplied to the device.
	Off	Power is not supplied to the device.
SYS	Blinking	System is functioning correctly.
	Solid/Off	System is functioning incorrectly.
WLAN	Blinking	Transmitting data wirelessly
	Off	Wireless is disabled.
	Solid	Wireless is enabled.
DSL	Slow Blinking	Physical connection failure.
	Fast Blinking	Synchronizing...
	Solid	ADSL connection is established.
LAN 1/2/3/4	Off	No connection established
	Blinking	Transmitting data
	Solid	Connection is established.

WPS	Solid	Client connected successfully.
	Blinking	WPS LED starts blinking if you press the WPS button on the device or interface.
	Off	No wireless clients are connected. WPS LED turns off after blinking for 2 minutes.
USB	Solid	Connection is successfully established on the USB port.
	Off	Connection is not established on the USB port.
INTERNET	Solid	Current client is connecting to the Internet; no data is transmitted via the Internet.
	Blinking	Current client is connecting to the Internet; data is transmitted via the Internet.
	Off	Current Internet client is not connecting to the Internet.

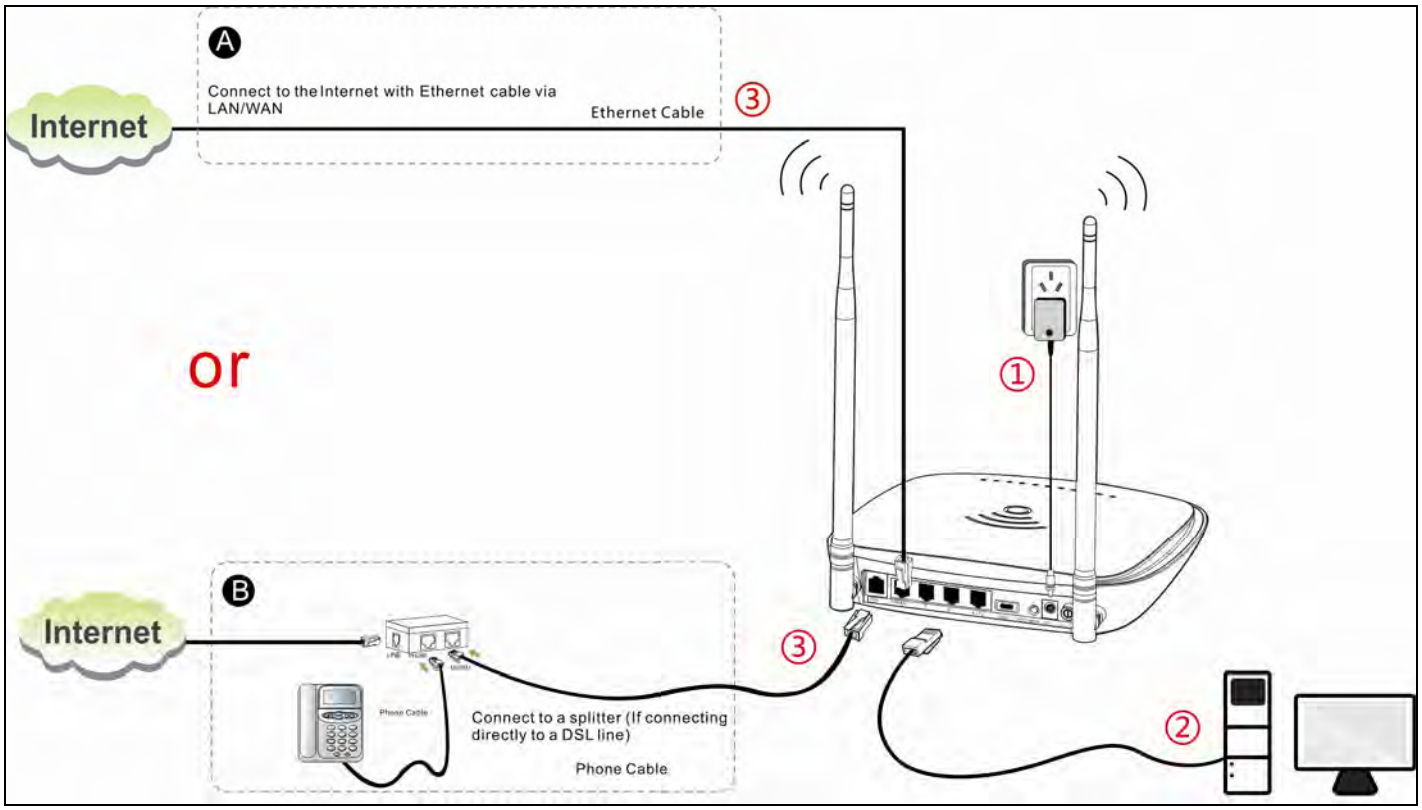
Back Panel



Button & Interface	Description
DSL	For connecting the router to the Internet via a phone cable provided by your ISP.
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, a switch, or a router; when you access the Internet via an Ethernet cable from your ISP directly, this port works as a WAN port, but this port works as a LAN port by default, you need to go to the Management webpage to select Ethernet type (namely, stimulate this port to function as a WAN port).
2/3	LAN port, used to cable the device to the local network devices such as computers.
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.
USB	Used to connect a USB device, such as a 3G USB modem, USB print server or storage service.

RST/WPS	Press it for 1-3 seconds to enable WPS-PBC feature; Press it for 8 seconds to restore all configurations to factory defaults.
DC	Used to connect to the power adapter, which is included in the package.
ON/OFF	Power switch to turn the router on or off.

2. Install the device



❶ Connect the included power adapter to your router and turn on the router.

❷ Connect your computer to your router. (You can also wirelessly connect the router to one wireless device by connecting to its SSID—wireless network name, and then enter the default username and password admin/admin, for entering the management web to configure the router. SSID and default username/password, see the bottom label of the router.)

❸ Connect your router to the Internet. Choose **ADSL Mode** or **Ethernet Mode** according to your actual Internet service type.

ADSL Mode	If your ISP provides you a DSL line	With a telephone	Simply connect the DSL line to the DSL port of your router.
		Without a telephone	Use the splitter as a medium: 1) Connect the DSL line from the Internet side to the LINE port of the splitter; 2) Connect the telephone with a phone cable to the PHONE port of the splitter; 3) Connect the MODEM port of the splitter and DSL port of your router via another phone cable.
Ethernet Mode	If your ISP provides you an Ethernet cable	Do not go to ❸ (connect the Ethernet cable to the 1/WAN port) until you finish the Primary Setup of Internet connection type on the Web Management Homepage, i.e., finish settings in **Ethernet Mode** in Chapter 3 Quick Internet Setup >3.2 Internet Setup.	

Chapter 3 Quick Internet Setup

This chapter instructs you to quickly set up your Internet connection.

1. Log in to Web Manager

Preparation for logging in to web manager:

■ **Method 1: Using Resource CD**

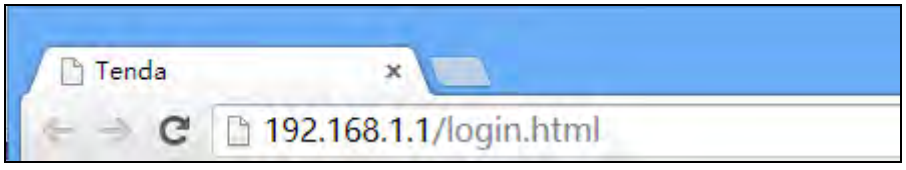
❶ Insert the included resource CD into your computer's driver and the CD automatically runs. If it does not, double click , and you will see the screen below.

❷ Click **Run** and it will automatically configure your PC's TCP/IP properties. If your PC is successfully configured, the login window will display.

■ **Method 2: Using a Web Browser**

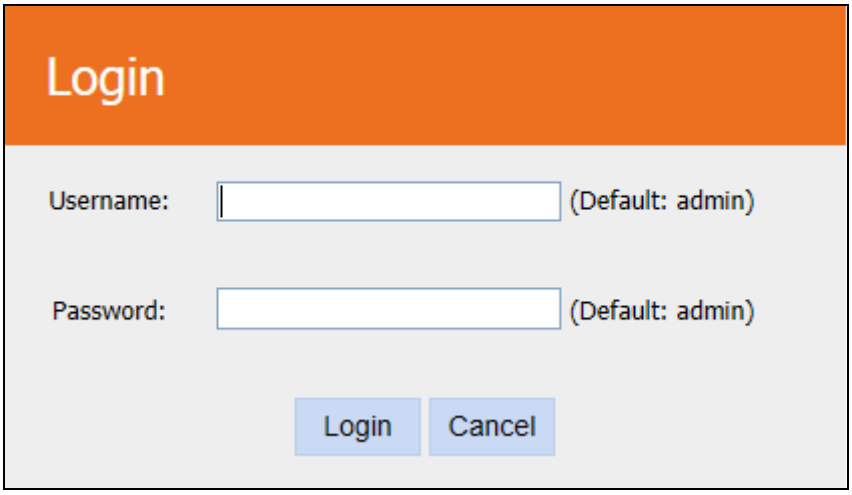
❶ Set your PC to **Obtain an IP address automatically**. For more information, see Appendix 1 Configure Your PC.

❷ Launch a web browser and enter **192.168.1.1** in the address bar.



Login:

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



Tip

If you change the login username and password and forget them, press the RST/WPS button on the device for at least 8 seconds to reset the router, and then enter the home page with the default name and password “admin” to reconfigure all settings you need.

2. Internet Setup

2.1 ADSL Mode

❶ **Connection Mode:** Select **ADSL** mode.

❷ **Country:** Select your country.

❸ **ISP:** Select your ISP.

❹ **VPI/VCI:** This two fields will be populated automatically if you select a correct country and ISP.

❺ **Connection Type:** Select your Connection Type, and fill the relevant Internet information. If you are not clear about this info, contact and consult your ISP.

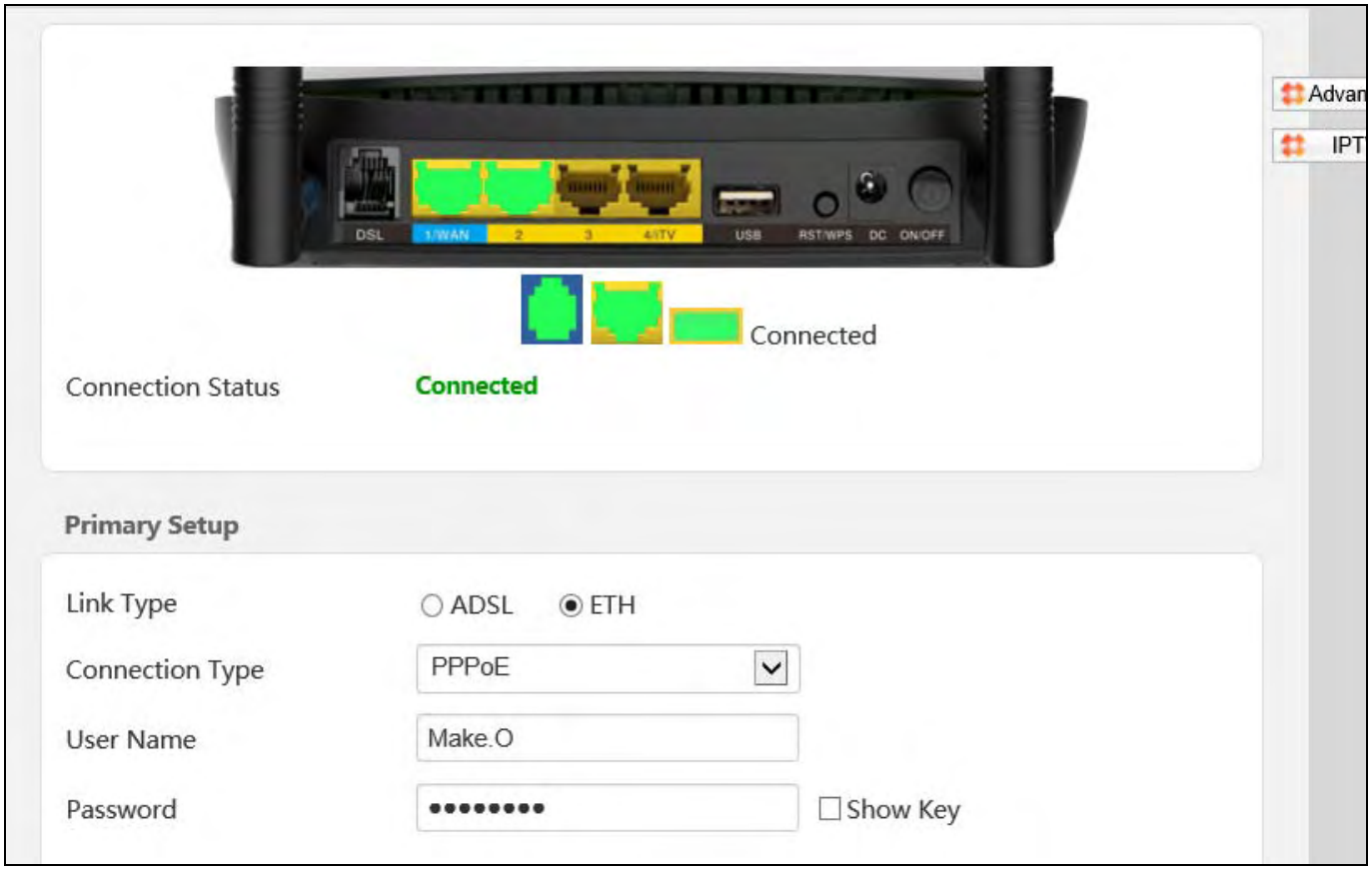
Connection Type		ISP Information
PPPoE/ PPPoA		Enter the ISP user name and password. If you are not clear about this information, ask your ISP to provide it.
IPoE	Dynamic IP	No entries are needed.
	Static IP	Enter the assigned IP address, subnet mask, and the IP address of your ISP's primary

		DNS server. This information should have been provided to you by your ISP. If a secondary DNS server address is available, enter it also.
IPoA	Static IP	Enter the assigned IP address, subnet mask, and the IP address of your ISP's primary DNS server. This information should have been provided to you by your ISP. If a secondary DNS server address is available, enter it also.
Bridge		When Bridge mode is enabled, the router works as a modem. If you wish to initiate a dialup directly from your PC for Internet access or enjoy the entire Internet connection by yourself (instead of sharing it with others), you can select **Bridge**.

Note

If your country and/or your ISP are not covered on the home page, select **Other** and configure the VPI and VCI value manually. If you do not know this information, ask your ISP to provide it. Also you can refer to Appendix 4 VPI/VCI List.

2.2 Ethernet Mode



❶ **Connection Mode:** Select **ETH** mode.

❷ **Connection Type:** Select your Connection Type, and fill the relevant Internet information. If you are not clear about this info, contact and consult your ISP.

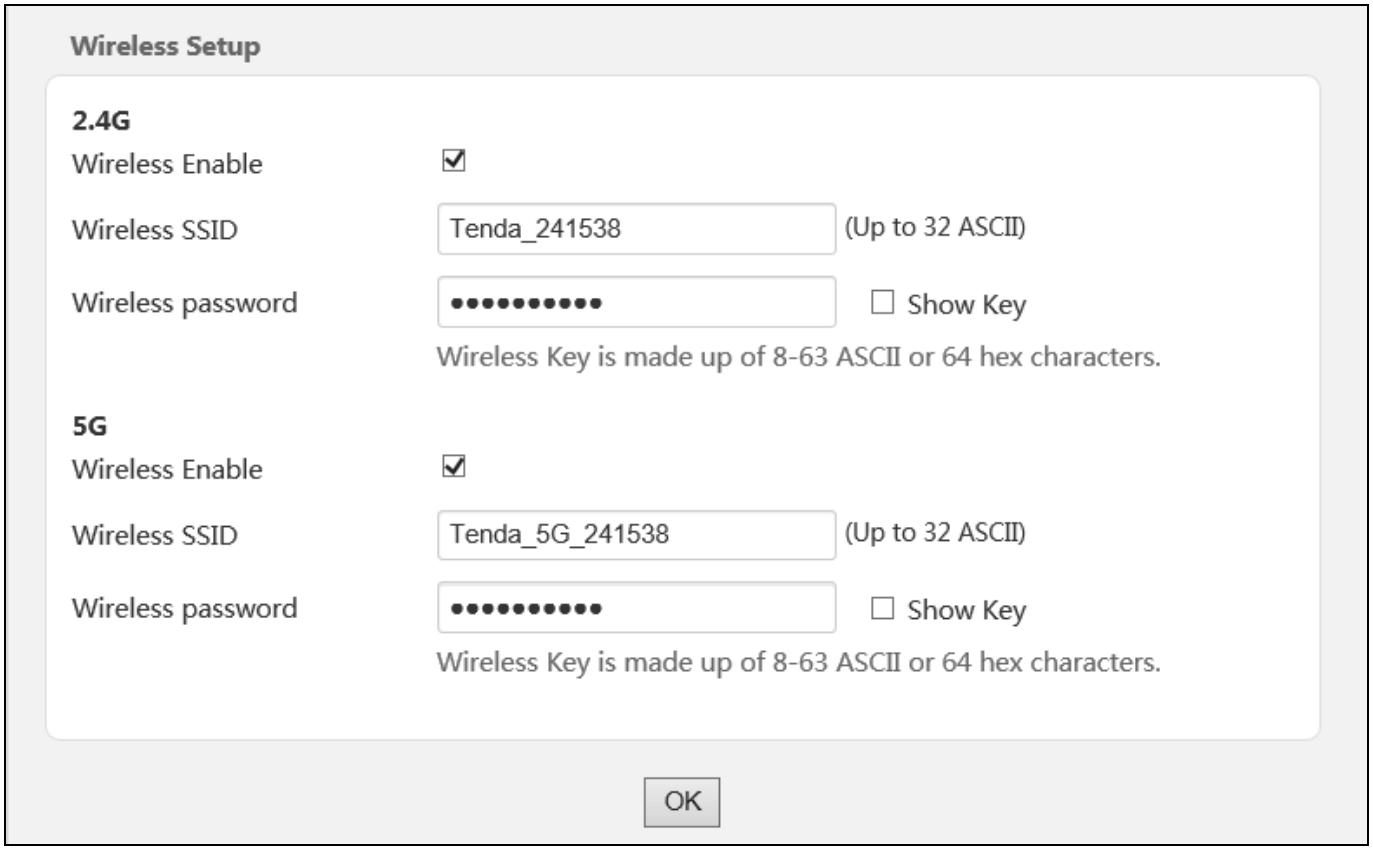
Connection Type		ISP Information
IPoE	Dynamic IP	No entries are needed.
	Static IP	Enter the Internet info (IP address, subnet mask, gateway and DNS server address) provided by your ISP.
PPPoE		Enter the username and password provided by your ISP.
Bridge		When Bridge mode is enabled, the router works as a modem. If you wish to initiate a dialup directly from your PC for Internet access or enjoy the entire Internet connection by yourself (instead of sharing it with others), you can select **Bridge**.

Note

After saving the Ethernet mode settings, you will see a note prompt to tell you the connection status Disconnected and asks you to insert the Ethernet cable to 1/WAN port.

And then you need to connect the Ethernet cable from the Internet side provided by your ISP to the 1/WAN port, i.e. to finish ❸ there in Ethernet Mode in Chapter 2 Hardware Install-> 2.2 Install the Device.

For your network security, please finish this part of settings. (Recommended)



Quick Wireless Setup:

Set wireless SSID

Set the wireless password.

Click **OK** to apply all the configurations on this page (including **Primary Setup**)

2.3 Test Internet Connectivity

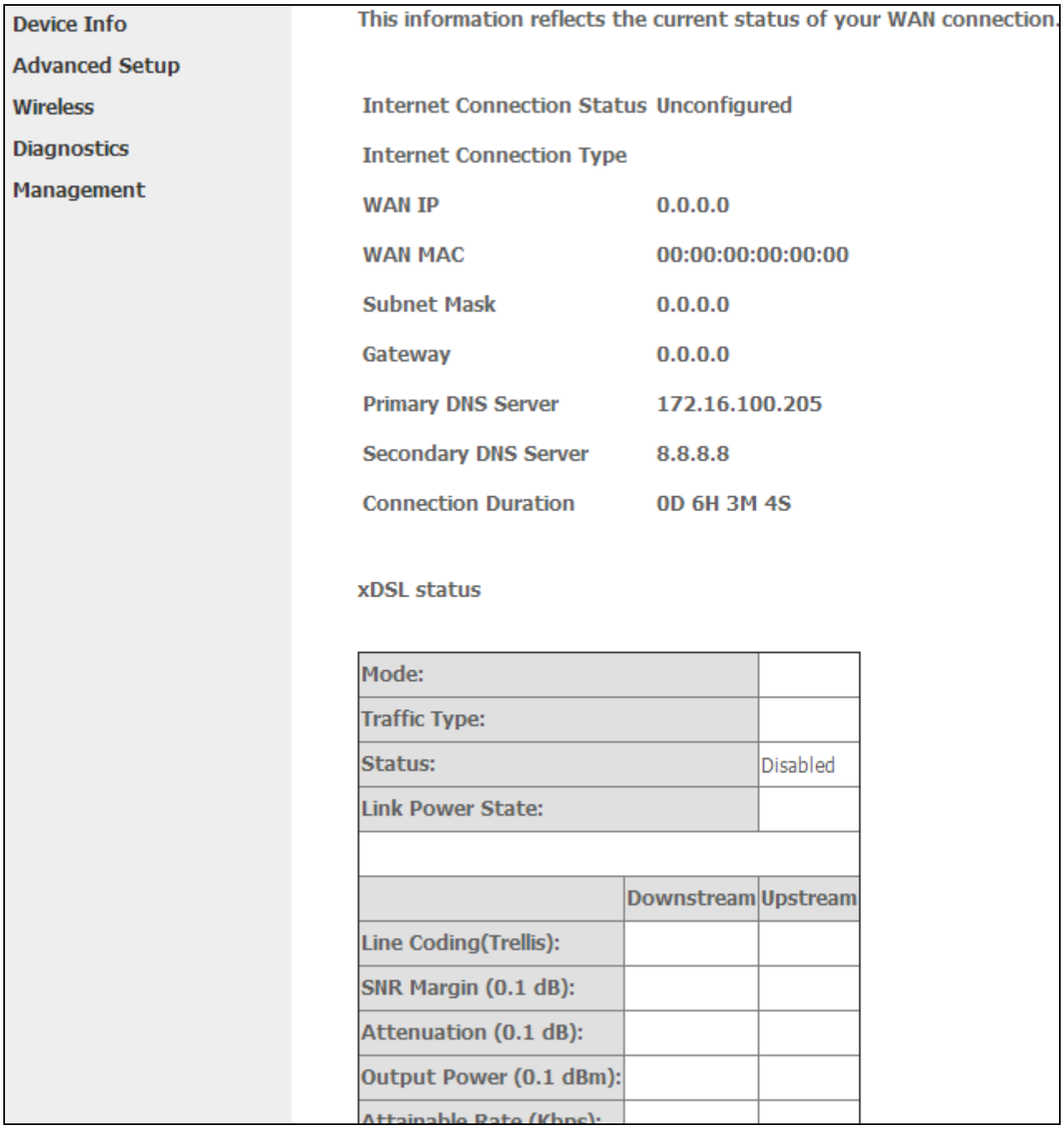
If **Connection Status** shows **Connected** shown as below, you access the Internet now.

Try to launch a web browser and enter www.tendacn.com. If the webpage displays properly, you are successfully connected to the Internet.

Chapter 4 Advanced Settings

If you prefer configuring your modem router for unique situations, consult this chapter to know advanced features.

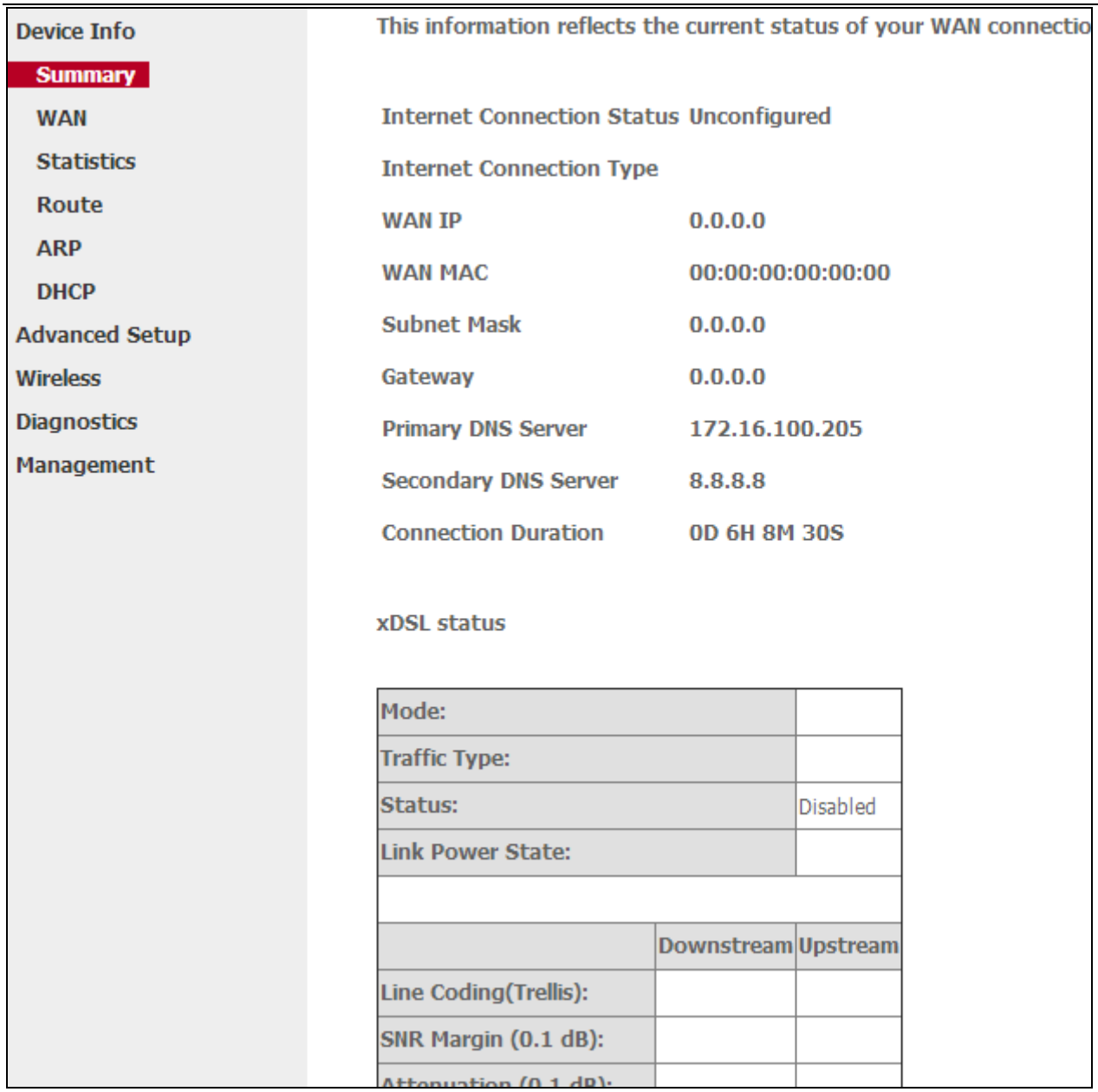
Click Advanced on the home page to enter the screen below.



1. Device Info

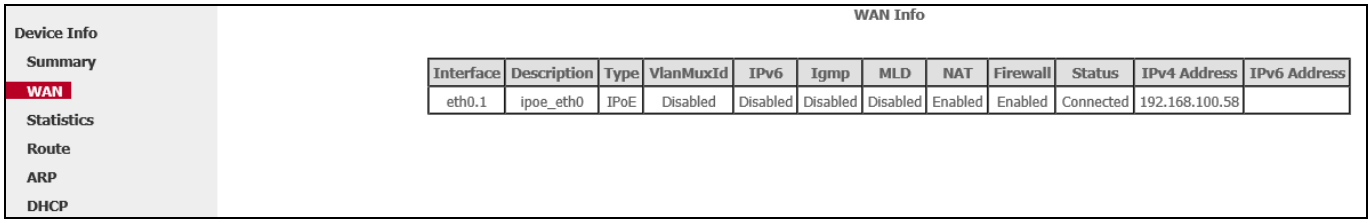
1.1 Summary

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



1.2 WAN

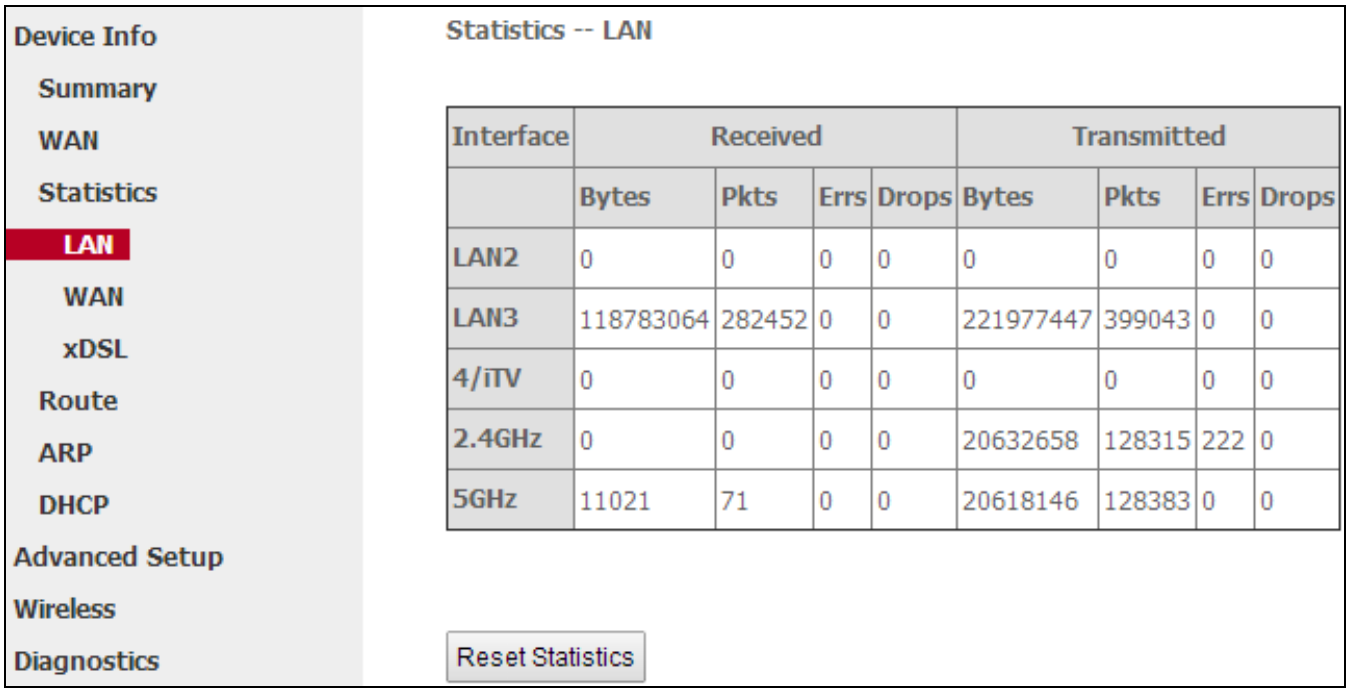
Here you can view the WAN Information including Interface, Description, Type, IGMP, NAT, Firewall, Status, IPv4 Address as seen in the screenshot.



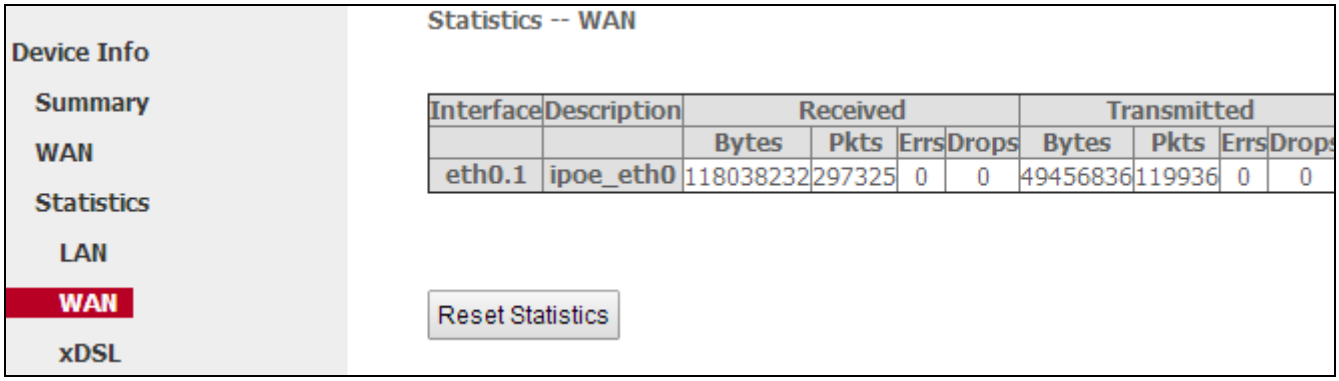
1.3 Statistics

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

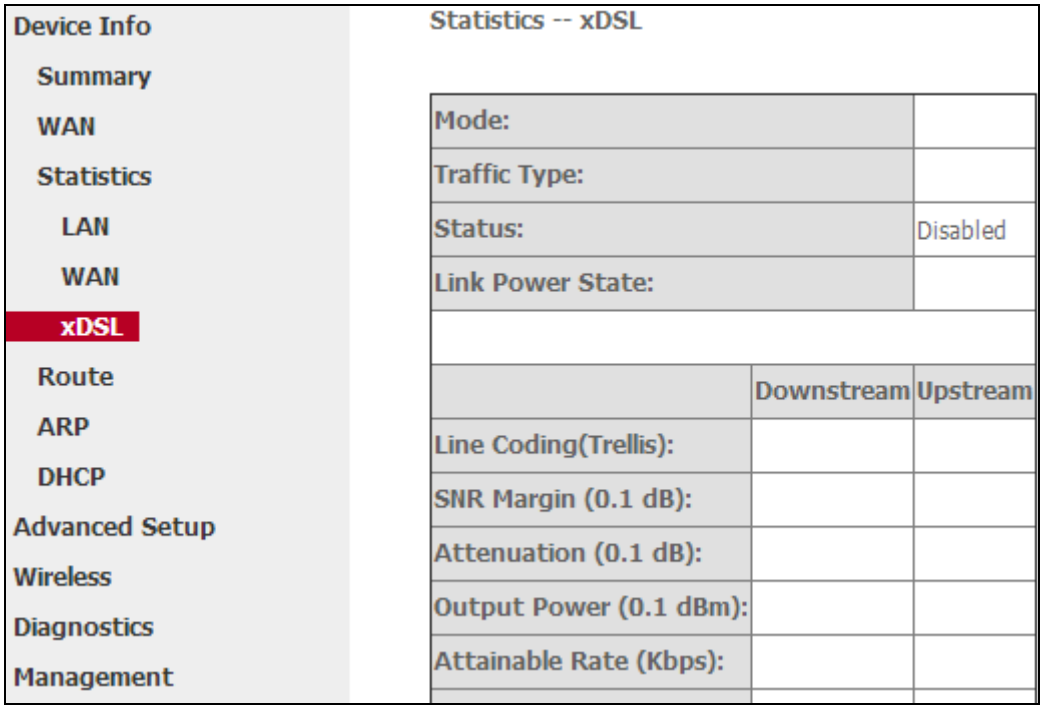
Statistics--LAN: Displays the packets received and transmitted on the LAN ports as seen in the screenshot below.



Statistics--WAN: Displays the packets received and transmitted on the WAN (eth0.1) port as seen in the screenshot below.

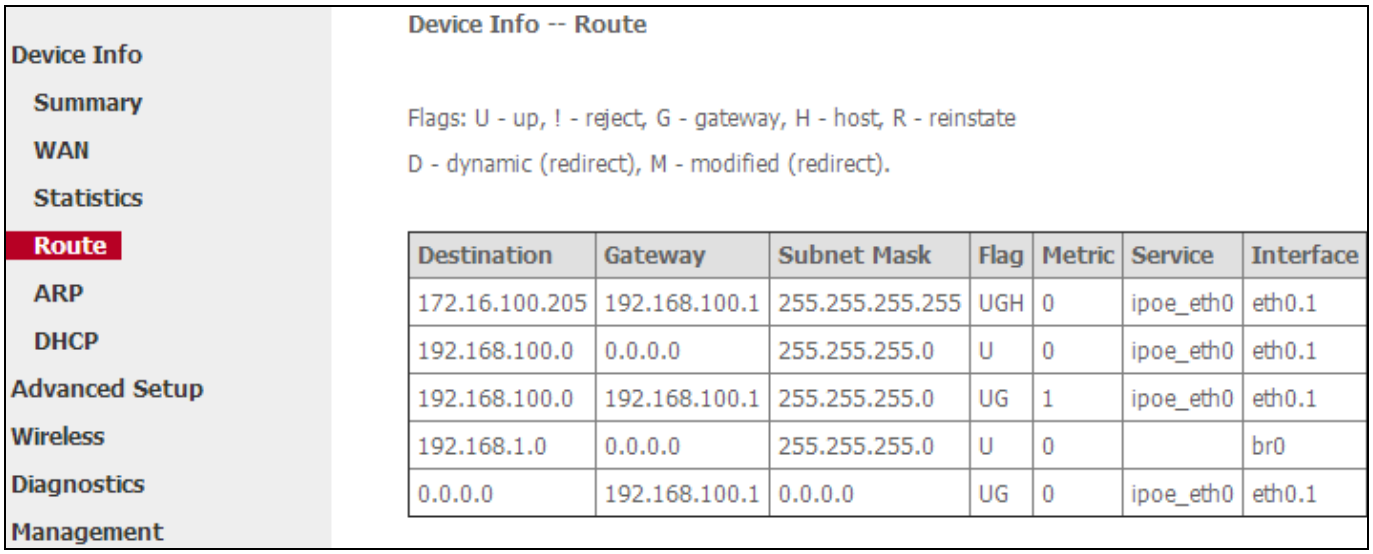


Statistics-xDSL: Displays the packets received and transmitted on the DSL port.



1.4 Route

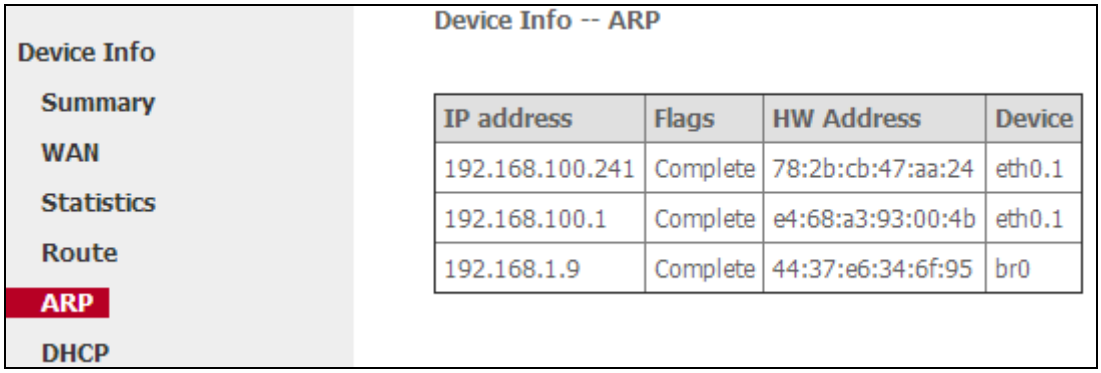
Here you can view the route table as seen in the screenshot:



Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
172.16.100.205	192.168.100.1	255.255.255.255	UGH	0	ipoe_eth0	eth0.1
192.168.100.0	0.0.0.0	255.255.255.0	U	0	ipoe_eth0	eth0.1
192.168.100.0	192.168.100.1	255.255.255.0	UG	1	ipoe_eth0	eth0.1
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0
0.0.0.0	192.168.100.1	0.0.0.0	UG	0	ipoe_eth0	eth0.1

1.5 ARP

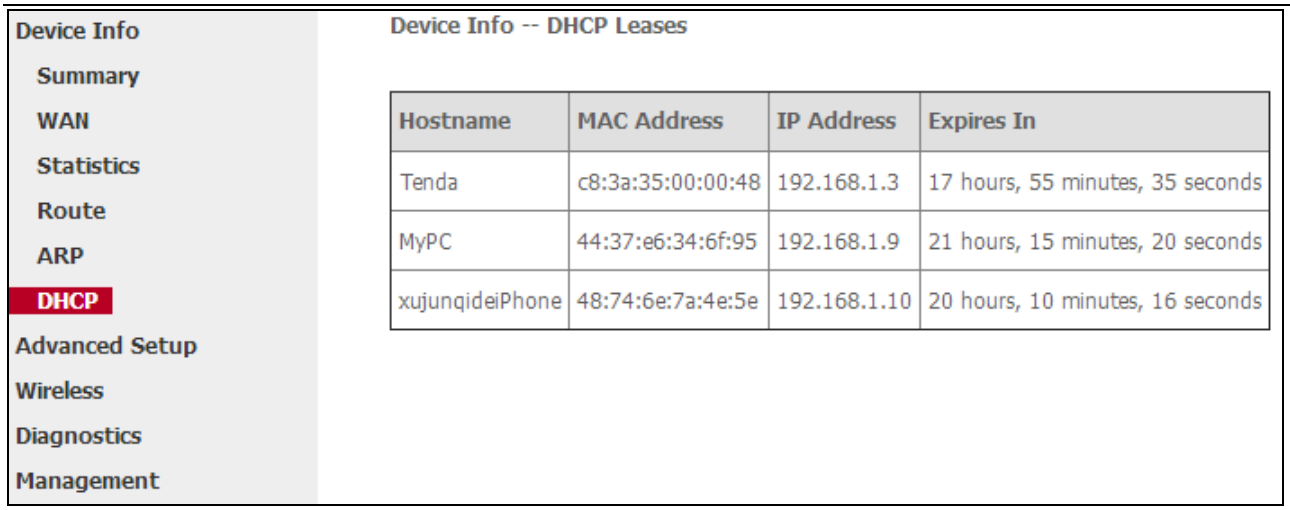
Here you can view the IP and MAC addresses of the PCs that attach to the device either via a wired or wireless connection as seen in the screenshot.



IP address	Flags	HW Address	Device
192.168.100.241	Complete	78:2b:cb:47:aa:24	eth0.1
192.168.100.1	Complete	e4:68:a3:93:00:4b	eth0.1
192.168.1.9	Complete	44:37:e6:34:6f:95	br0

1.6 DHCP

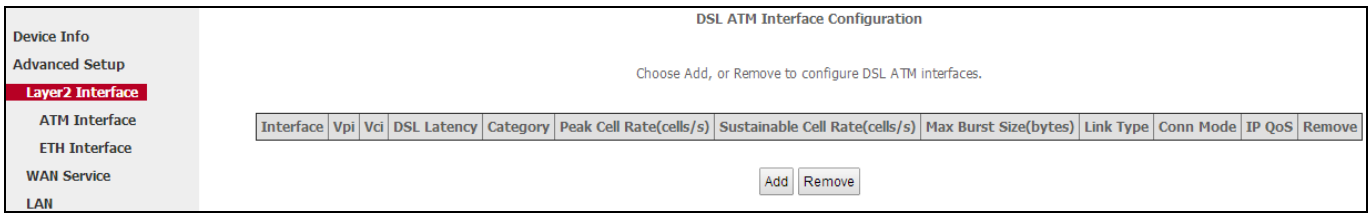
Here you can view the DHCP leases, including IP and MAC addresses of the PCs, hostnames and remaining lease time as seen in the screenshot:



2. Advanced Setup

2.1 Layer2 Interface

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



This modem router provides two Layer2 Interfaces:

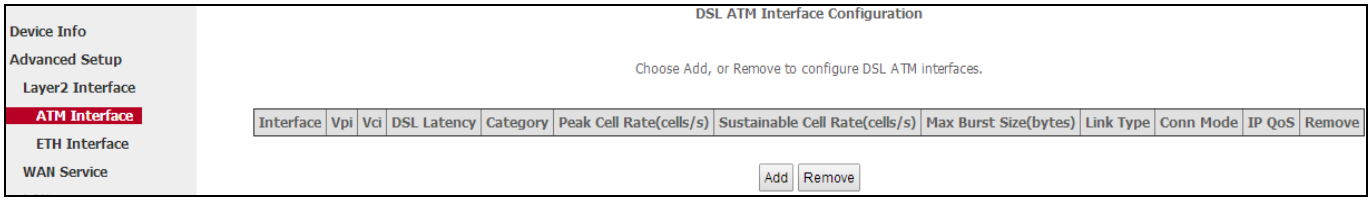
- ATM Interface for ADSL broadband Internet service. (By default, system applies the ATM Interface (ADSL uplink).)

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

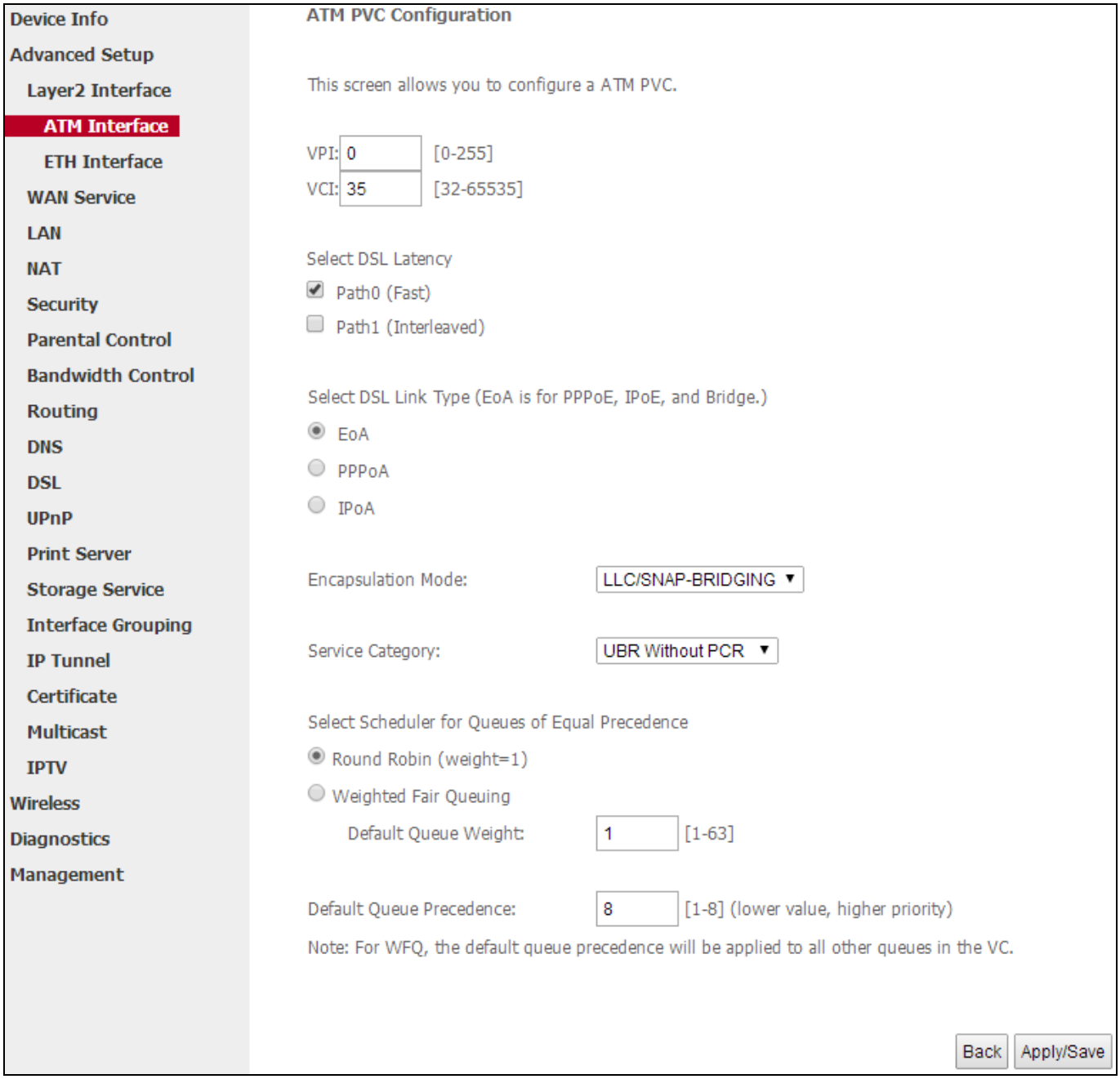
- If you directly connect to the ADSL line via a phone cable, first refer to 2.1.1 To set up the ATM interface and then skip to 2.2.1 For ATM Interface
- If you connect to the Internet via a fiber/cable modem using an Ethernet cable, first refer to 2.1.2 To set up the ETH interface and then skip to 2.2.2 For ETH Interface.

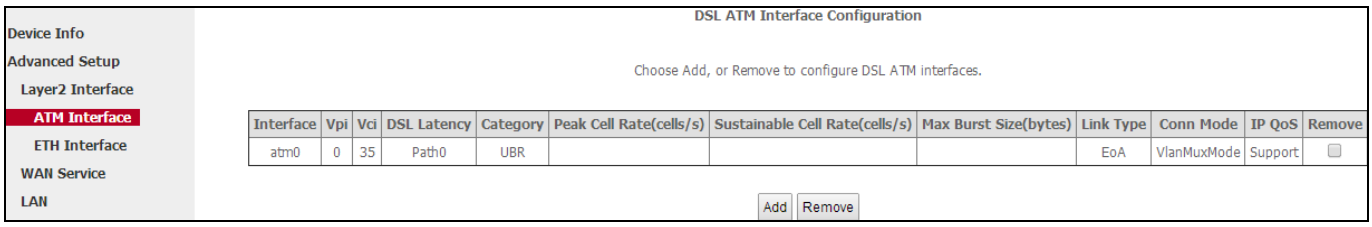
2.1.1 To set up the ATM interface

❶ Select **ATM Interface** and click **Add** to configure it.



❷ Enter the **VPI and VCI values**. Select a **DSL Link Type** (Internet connection type): EoA, PPPoA or IPoA. Leave other options unchanged from factory defaults. Click **Apply/Save**.





Go to 2.2.1 For ATM Interface to configure the WAN service for Internet access.

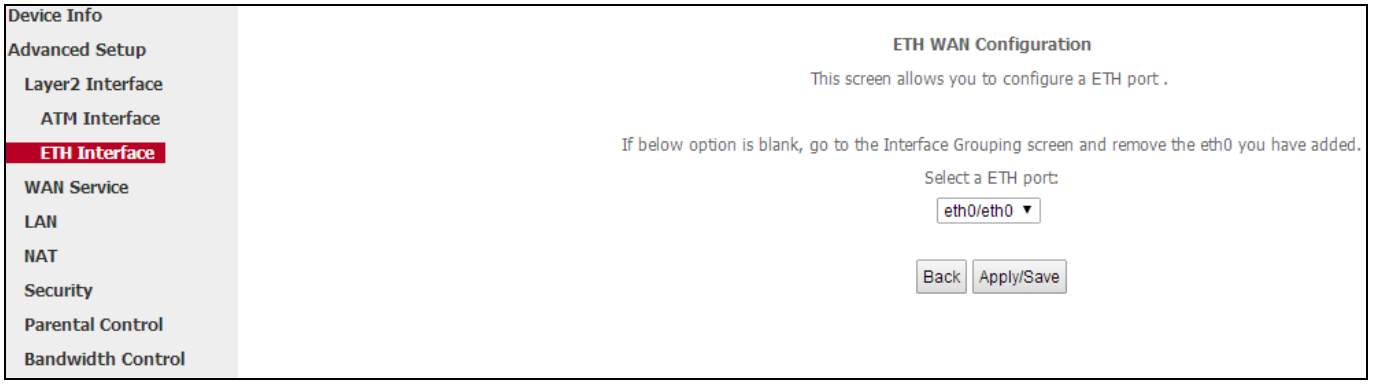
Tip

If you are unsure about the VPI/VCI parameters, see Appendix 4 VPI/VCI List, or ask your ISP to provide it.

2.1.2 To set up the ETH interface

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

❷ Select **eth0/eth0** in the box to function as a WAN port. Only one LAN port can be configured as the WAN port at a time. Click **Apply/Save** to take the settings into effect.



Go to 2.2.2 For ETH Interface to configure the WAN service for Internet access.

2.2 WAN Service

This modem router provides two WAN services:

- WAN Service for ATM Interface (ADSL uplink)

- WAN Service for ETH Interface (Ethernet uplink)

2.2.1 For ATM Interface

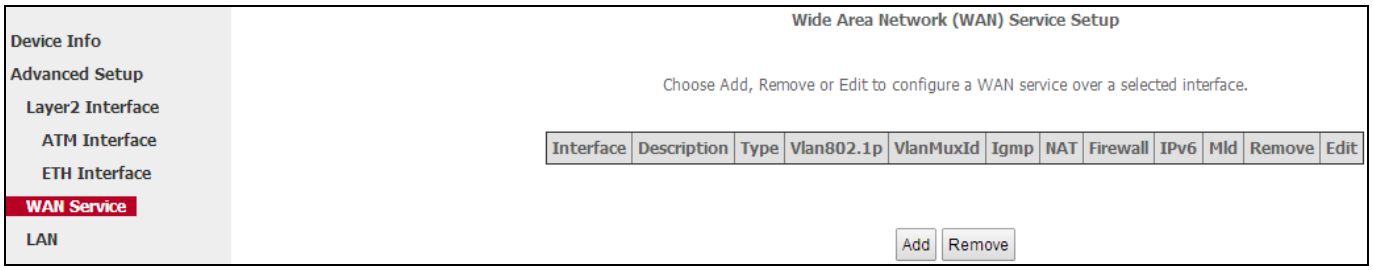
Following 11 modes are for you to choose according to your actual Internet service.

EoA	PPPoE	1) IPv4 Only	2) IPv4&IPv6(Dual Stack)	3) IPv6 Only
	IPoE	4) IPv4 Only	5) IPv4&IPv6(Dual Stack)	6) IPv6 Only
	7) Bridging			
PPPoA	PPPoA	8) IPv4 Only	9) IPv4&IPv6(Dual Stack)	10) IPv6 Only
IPoA	11) IPoA			

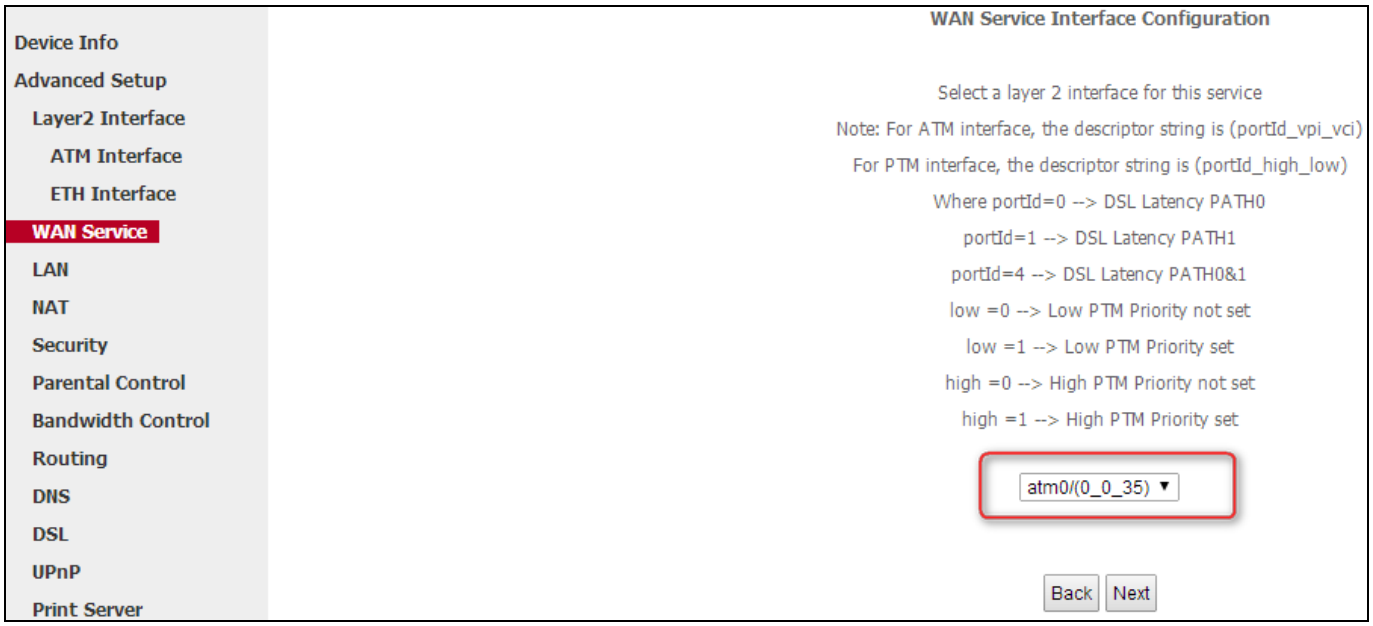
1) PPPoE IPv4 Only Users

If you configure the **ATM Interface** (ADSL uplink) and select **EoA** as the DSL link type, then you can start to set up WAN service for accessing the Internet.

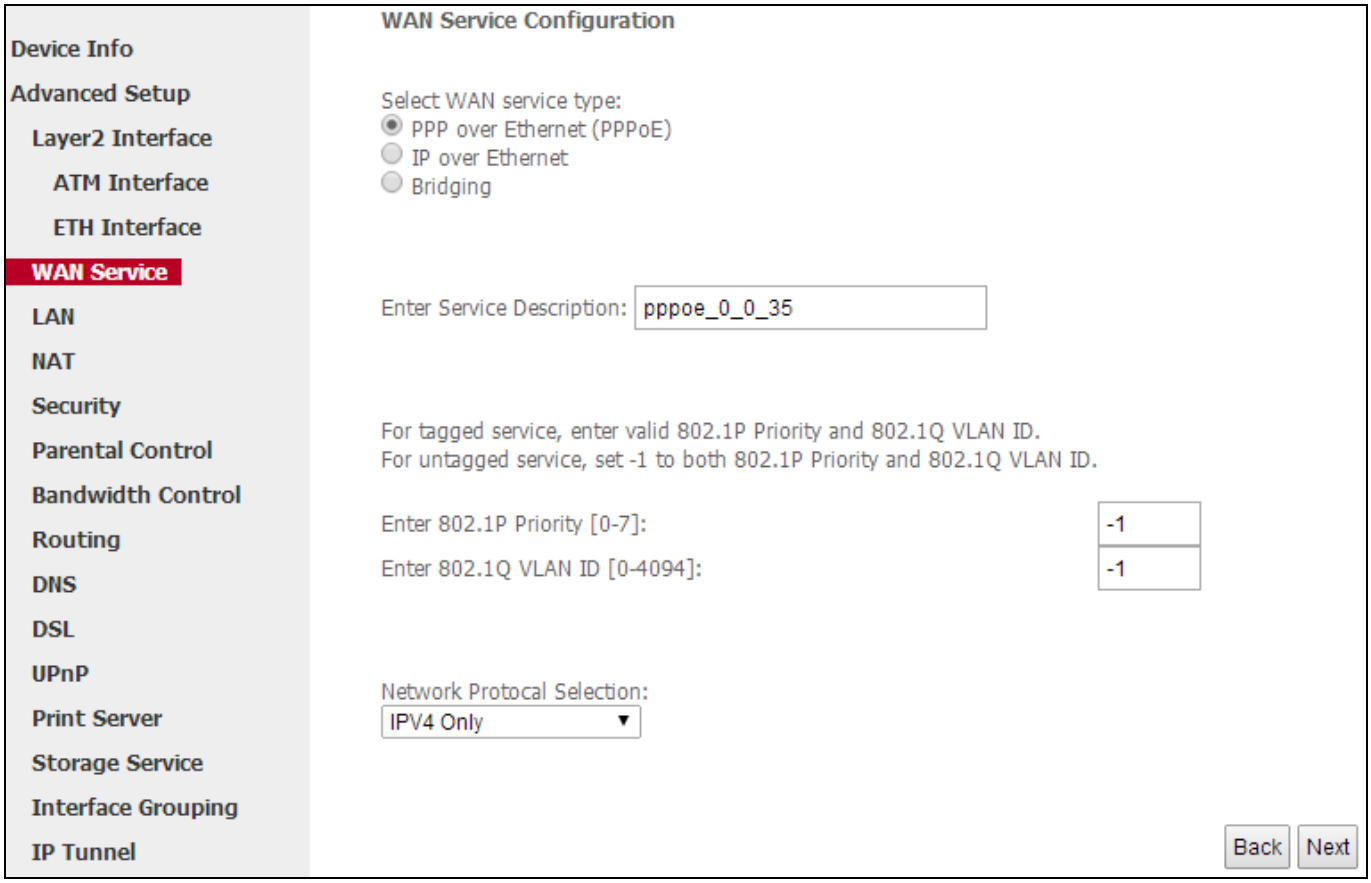
❶ Click **Advanced Setup > WAN Service** and then click the **Add** button.



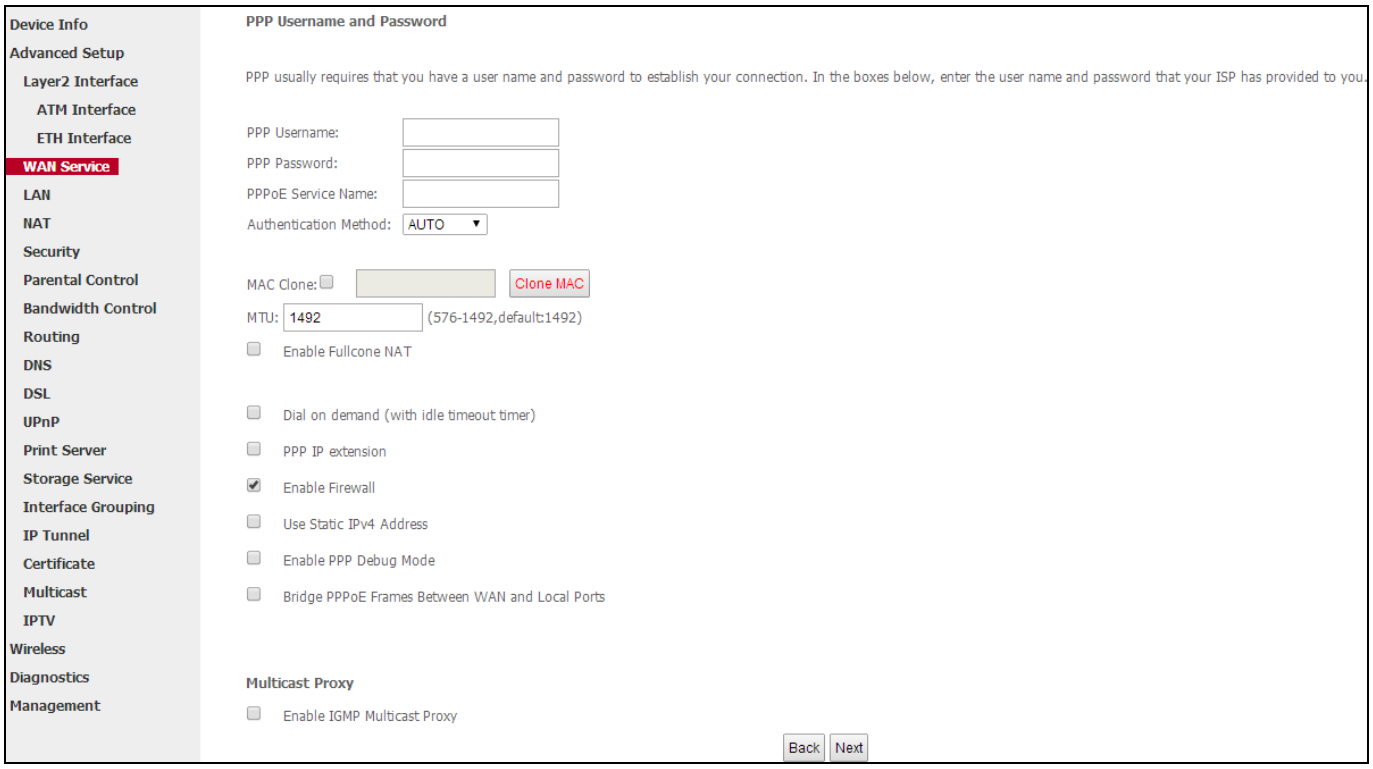
❷ Select the ATM interface you added just now from the pull-down menu in the figure below. Click **Next**.



❸ 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.**



❹ Finish PPP Username and Password and other settings on the figure below. Click **Next**.



PPP Username/ Password: Enter your PPP username and password. 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 modem 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 modem router will use multicast proxy.

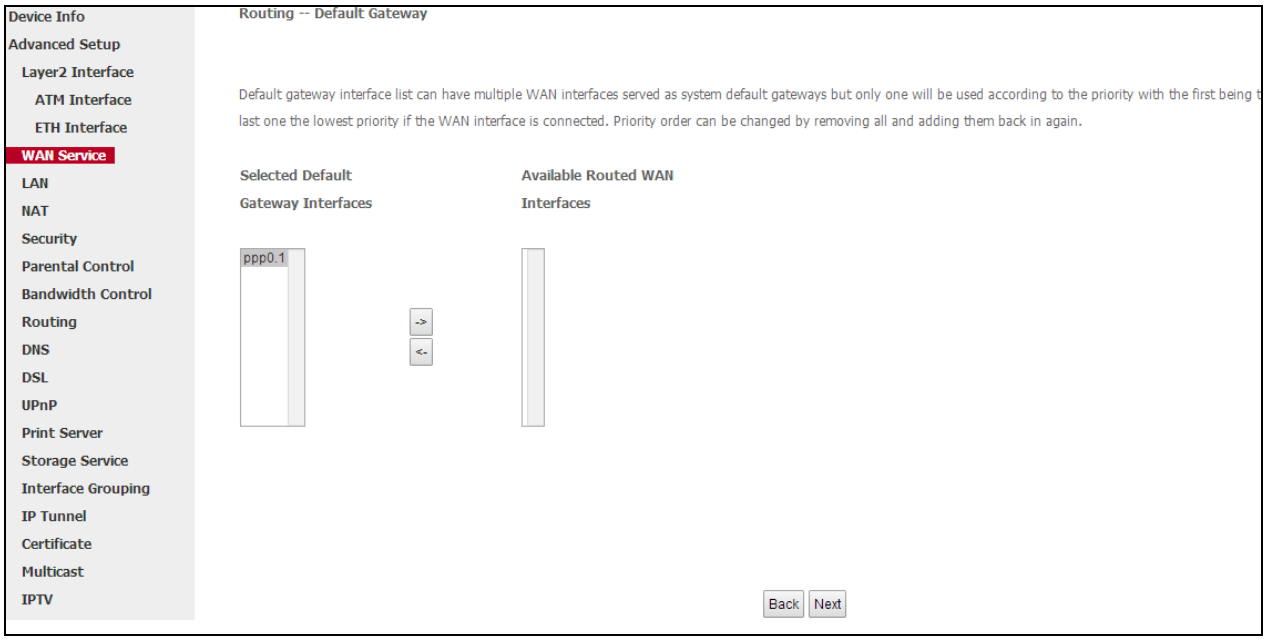
Knowledge Expansion

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 modem router.

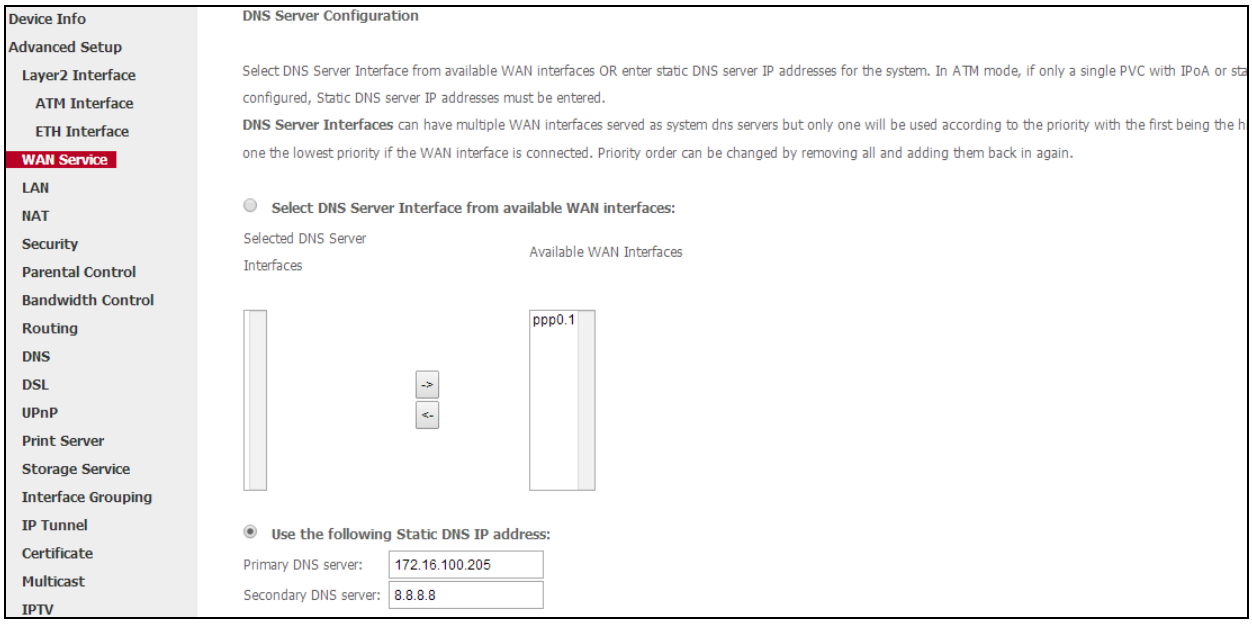
2. **MTU**: Short for ***M**aximum **T**ransmission **U**nit*, the largest physical packet size, measured in bytes, which a network can transmit. Any messages larger than the MTU are divided into smaller packets before being sent. The default MTU is 1492 bytes. For some ISPs, you might need to change the MTU. This is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.

---

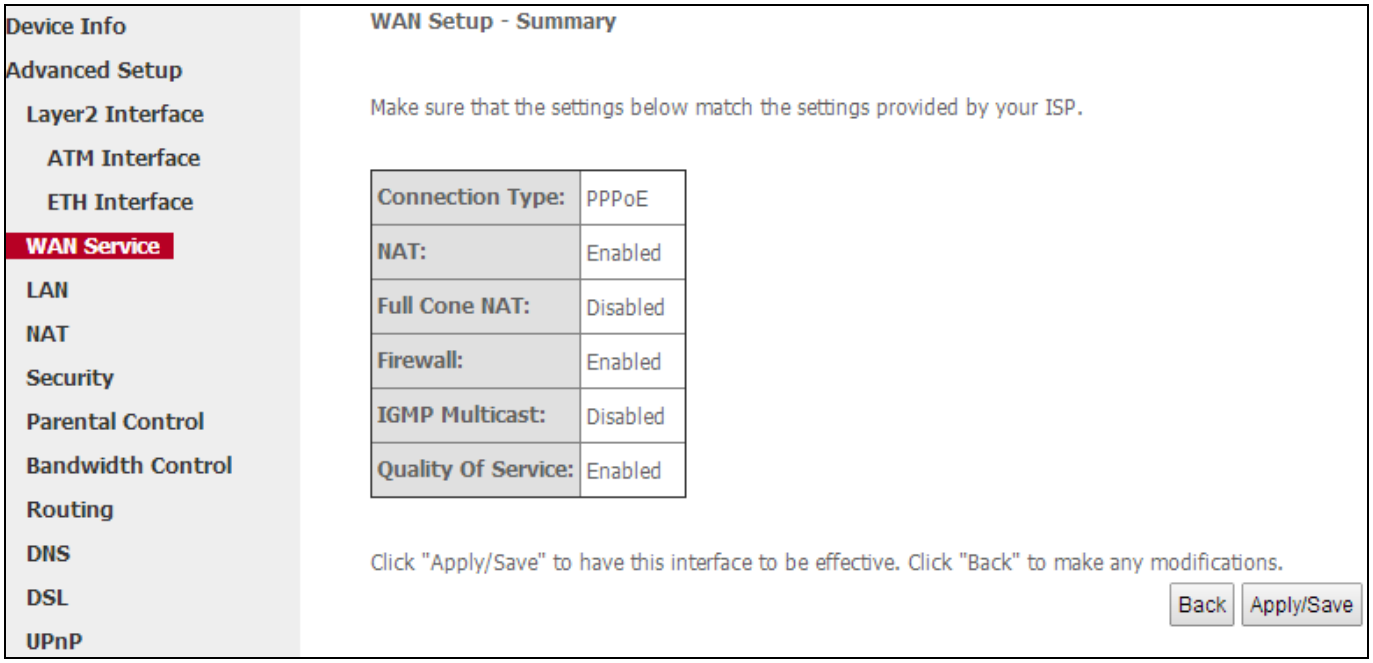
❺ To configure the Default Gateway interface, select the interface that you want to configure with the WAN gateway address in **Available Routed WAN Interfaces** box and move it into **Selected Default Gateway Interfaces** box. The default setting is recommended. Then click **Next**.



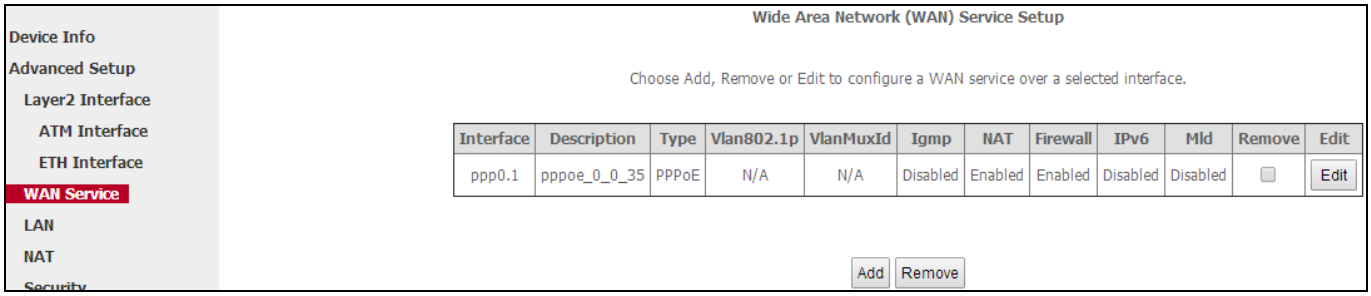
❻ To configure the WAN DNS address, click the **Select DNS Server Interface from available WAN interfaces** option, or select the **Use the following Static DNS IP address** option and enter the static DNS server IP addresses provided by your ISP. At last, click **Next**.



Click **Apply/Save** to save your settings if everything is correctly set.



Here you can view your configurations. When the PPPoE connection is successful, you can access the Internet.

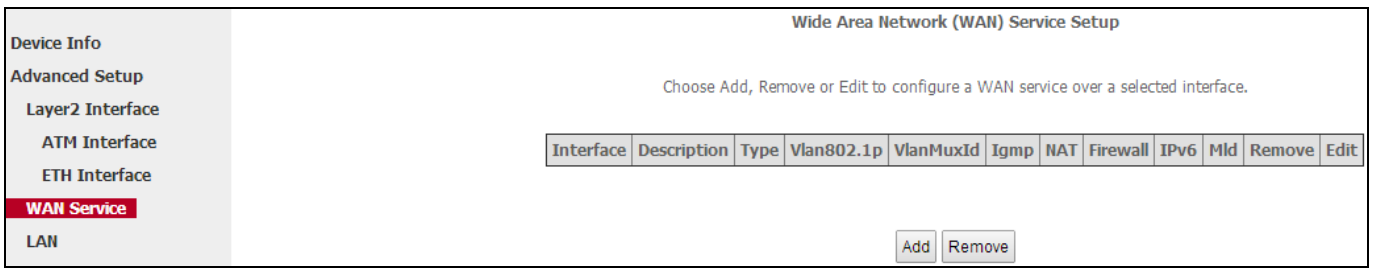


↗ Steps 1~6 above for **PPPoE and IPv4 Only** users

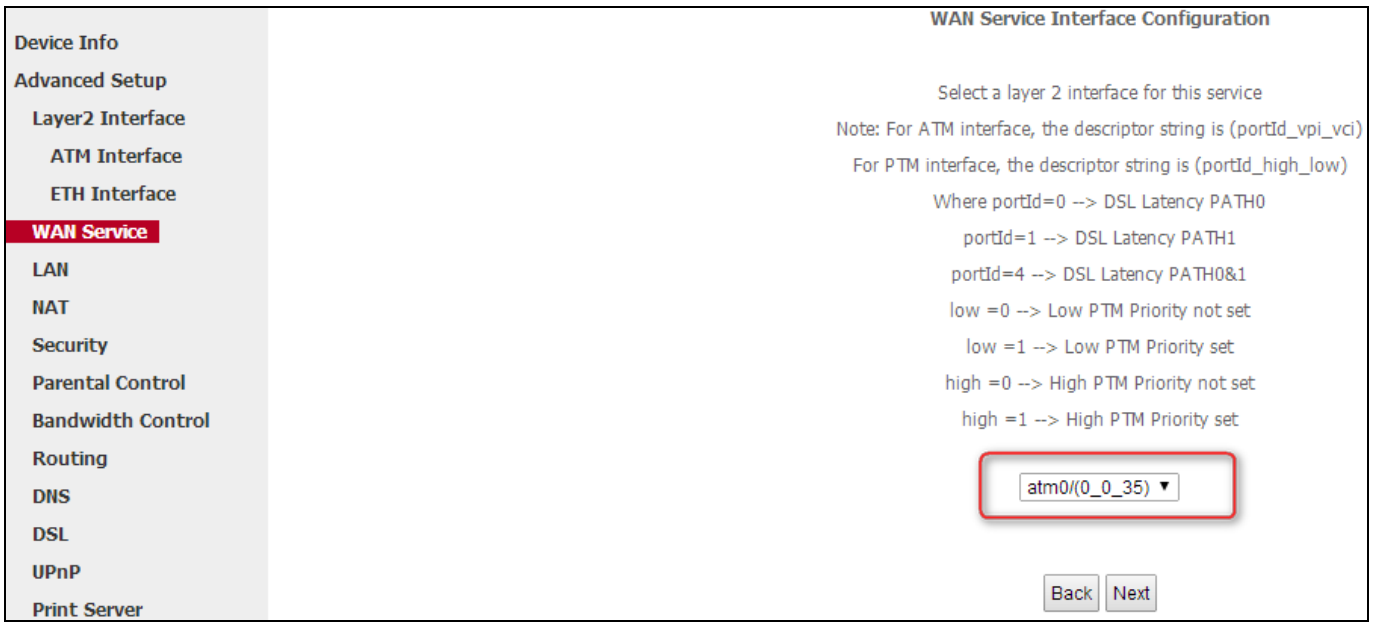
2) PPPoE IPv4&IPv6 (Dual Stack) Users

If you configure the **ATM Interface** (ADSL uplink) and select **EoA** as the DSL link type, then you can start to set up WAN service for accessing the Internet.

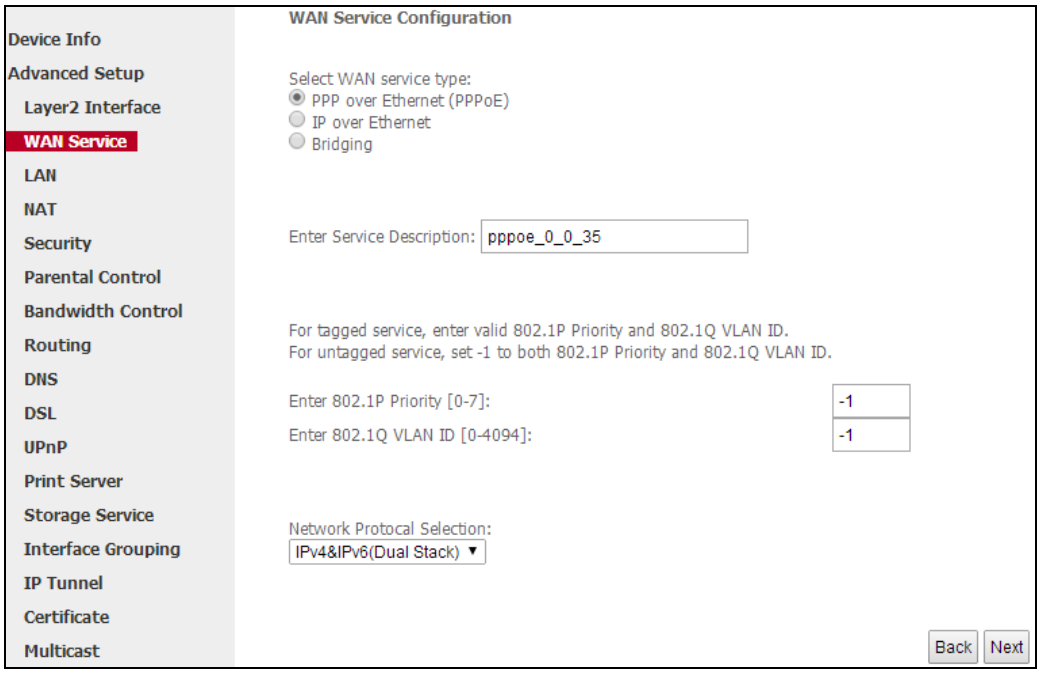
❶ Click **Advanced Setup > WAN Service** and then click the **Add** button.



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



❸ 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: **IPv4&IPv6 (Dual Stack)**. Click **Next**.

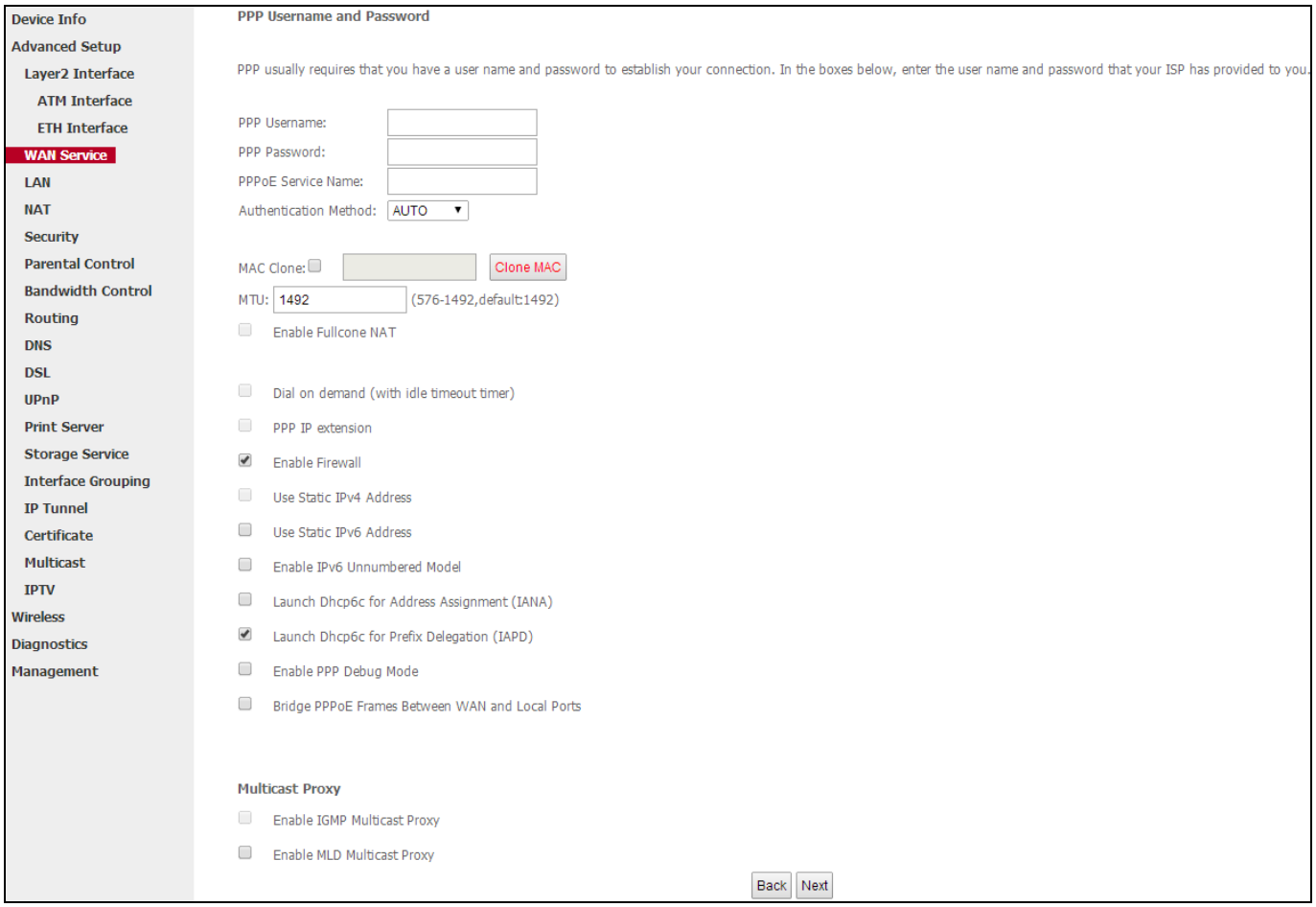


❹ Configure PPP Username and Password and other settings on the figure below. Each field with its indication is mentioned above in **PPPoE and IPv4 users-❹** section.

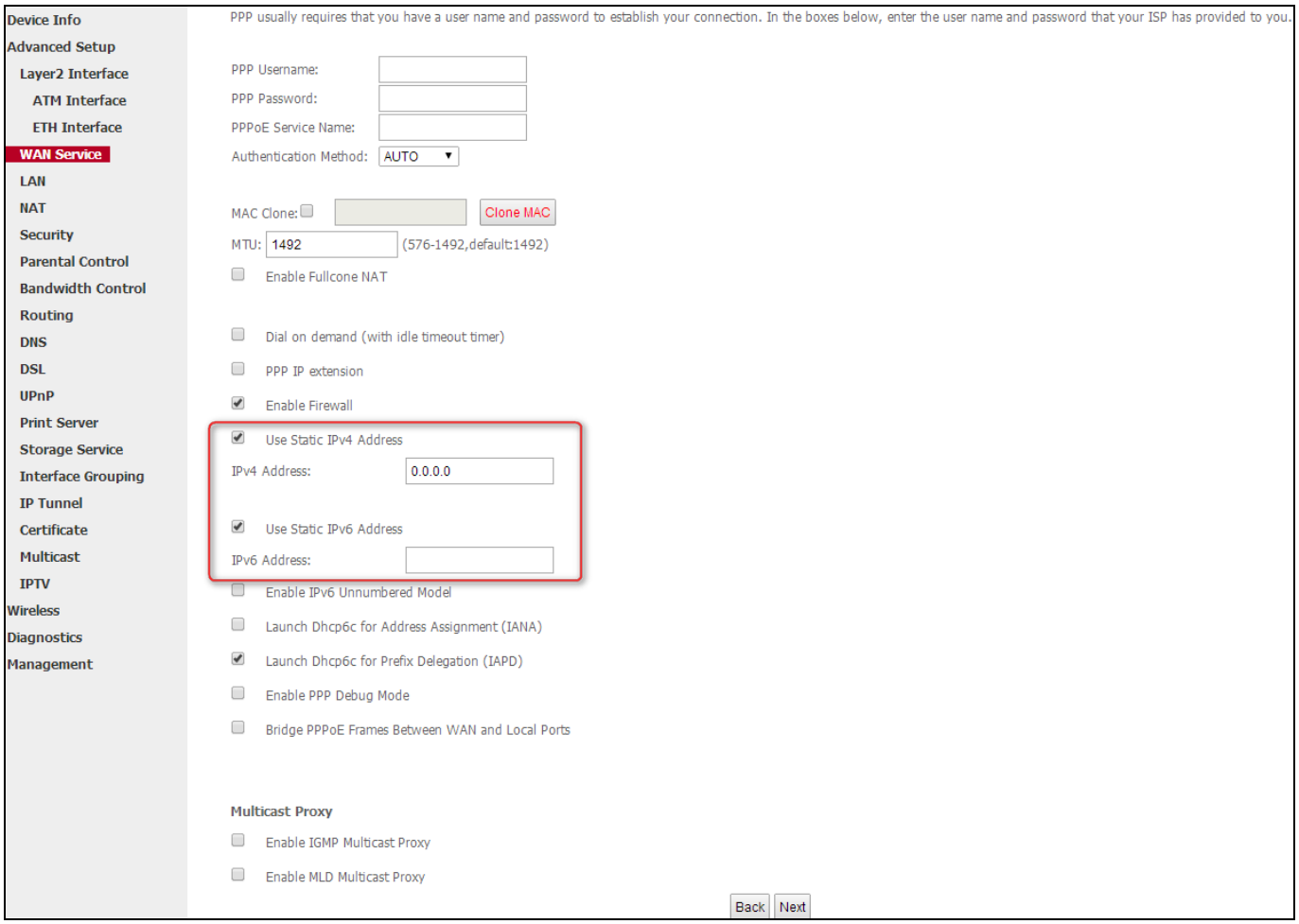
If ISP provides you no static IPv4 or IPv6 address, you just keep the default settings DHCP mode.

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

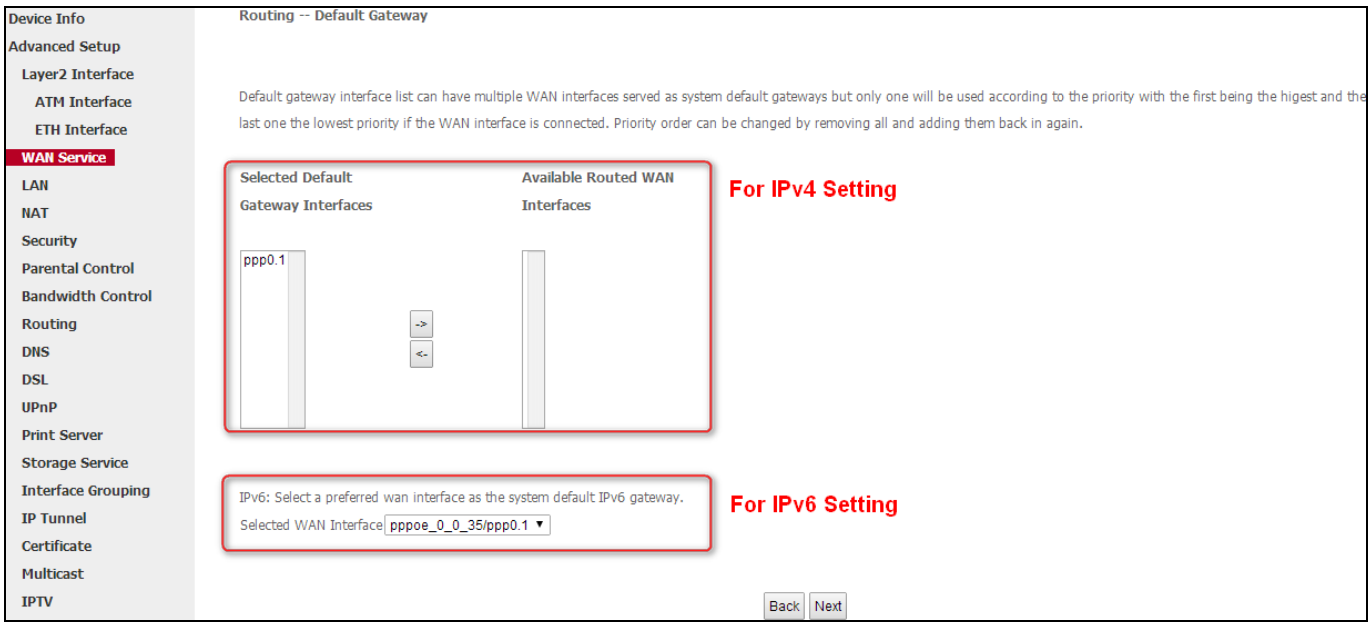
If your ISP is using stateful DHCPv6, check **Launch Dhcp6c for Address Assignment (IANA)** also. Click **Next.**



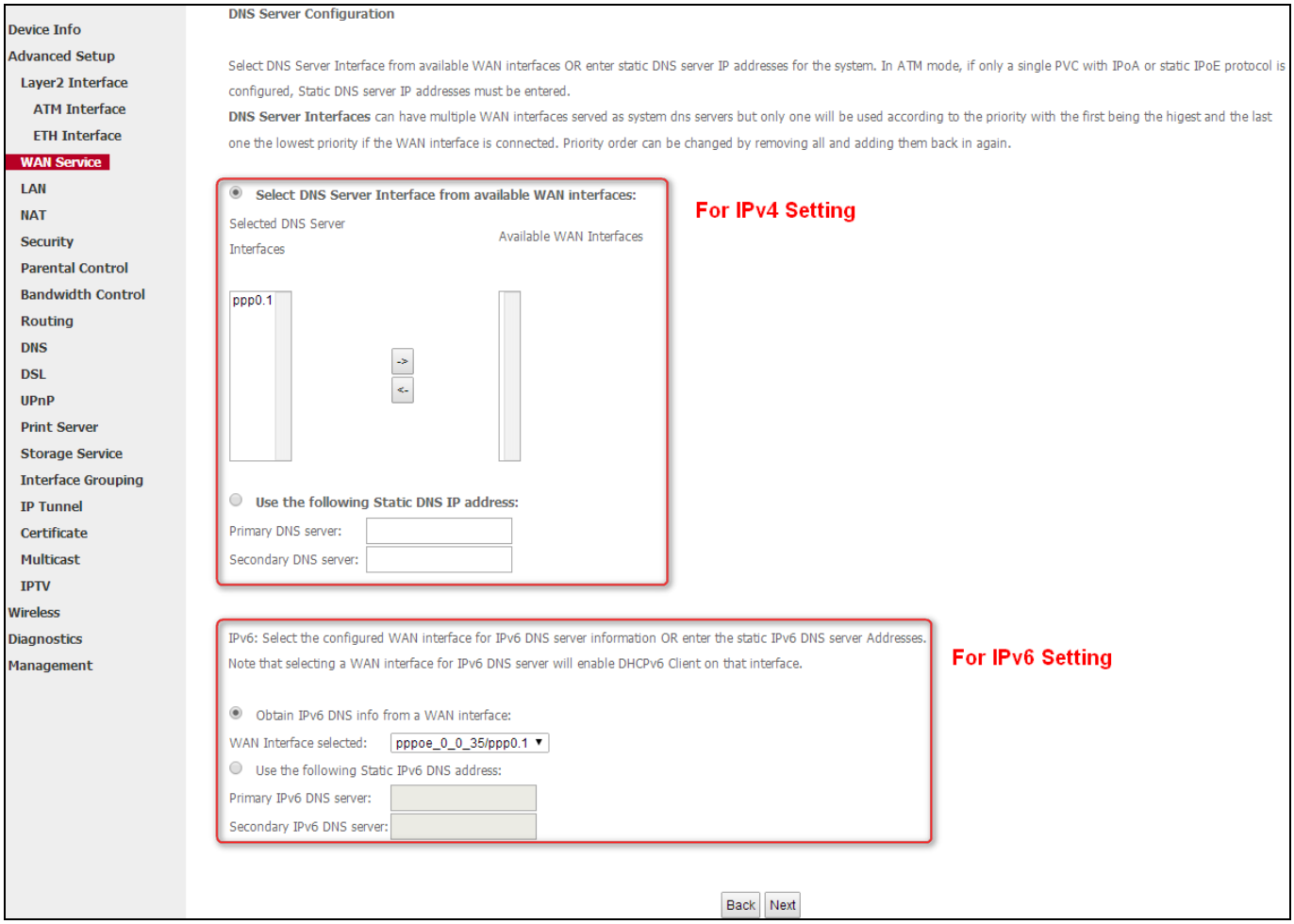
If ISP provides you with the static IPv4 and IPv6 address, configure the static IP addresses by checking **Use Static IPv4 Address** and **Use Static IPv6 Address** and enter the static IPv4 and IPv6 address.



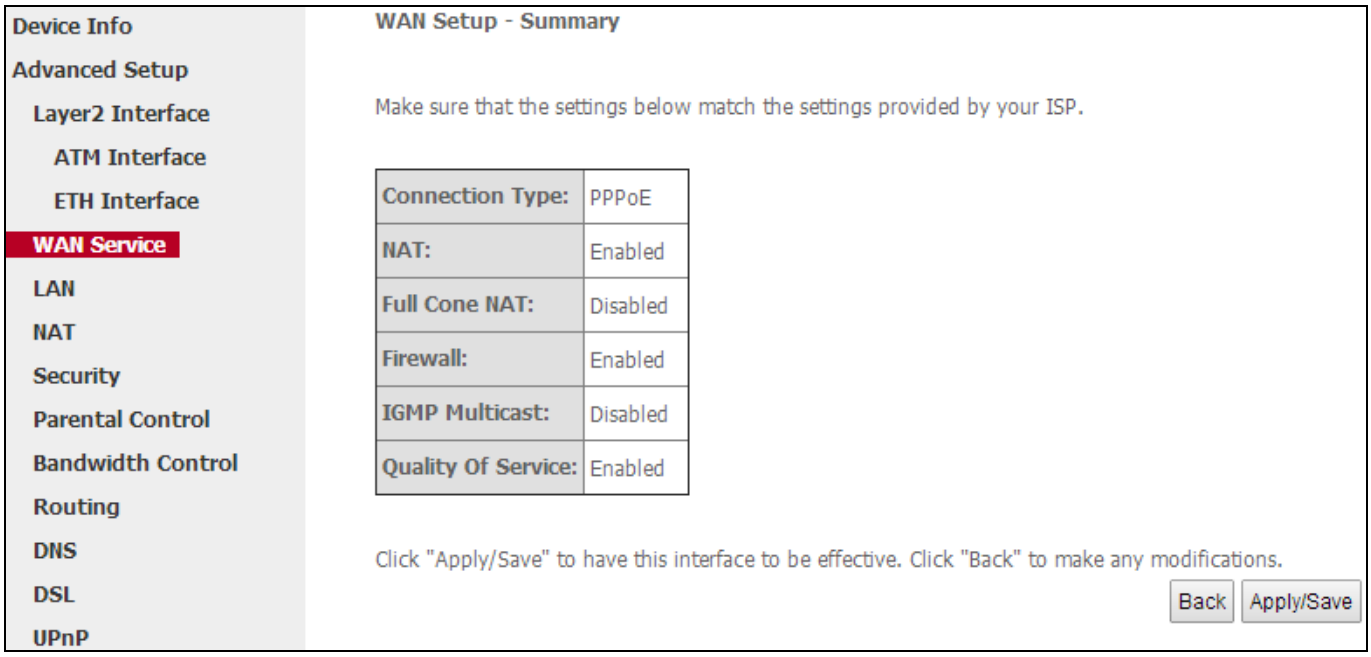
❺ To configure the Default Gateway interface, select the interface that you want to configure with the WAN gateway address. Then click **Next**.



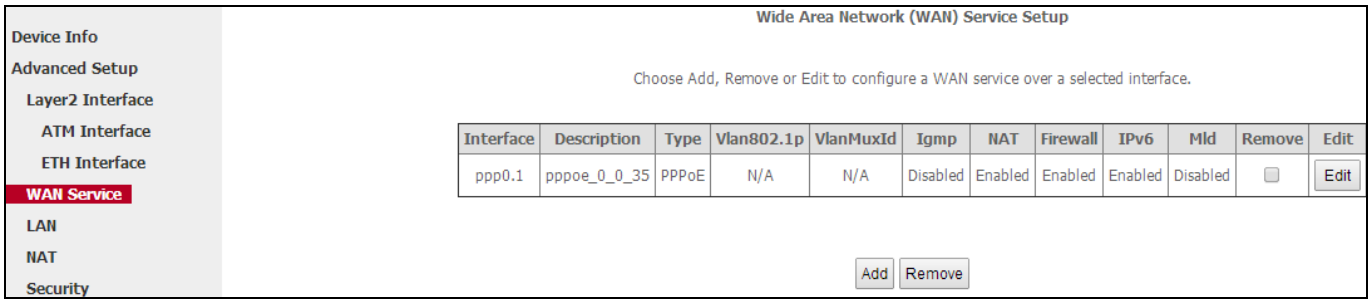
❻ To configure the WAN DNS address, finish both the IPv4 setting and IPv6 setting. Click **Next**.



Click **Apply/Save** to save your settings if everything is correctly set.



Here you can view your configurations. When the PPPoE connection is successful, you can access the Internet.

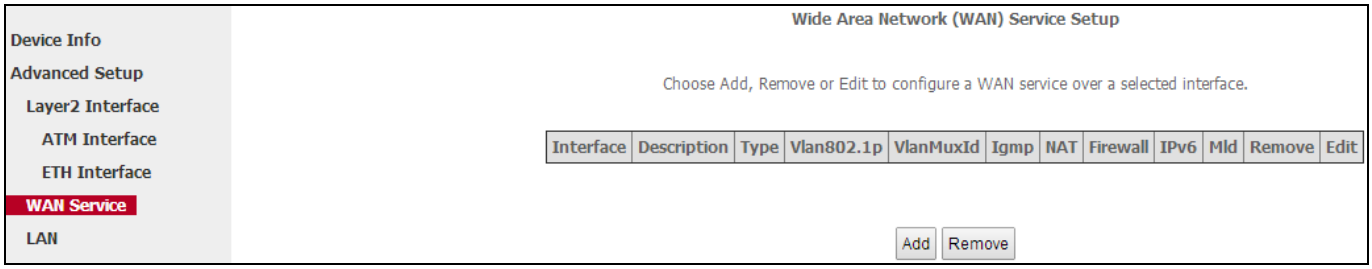


↗ Steps 1~6 above for **PPPoE and IPv4&IPv6 (Dual Stack)** users

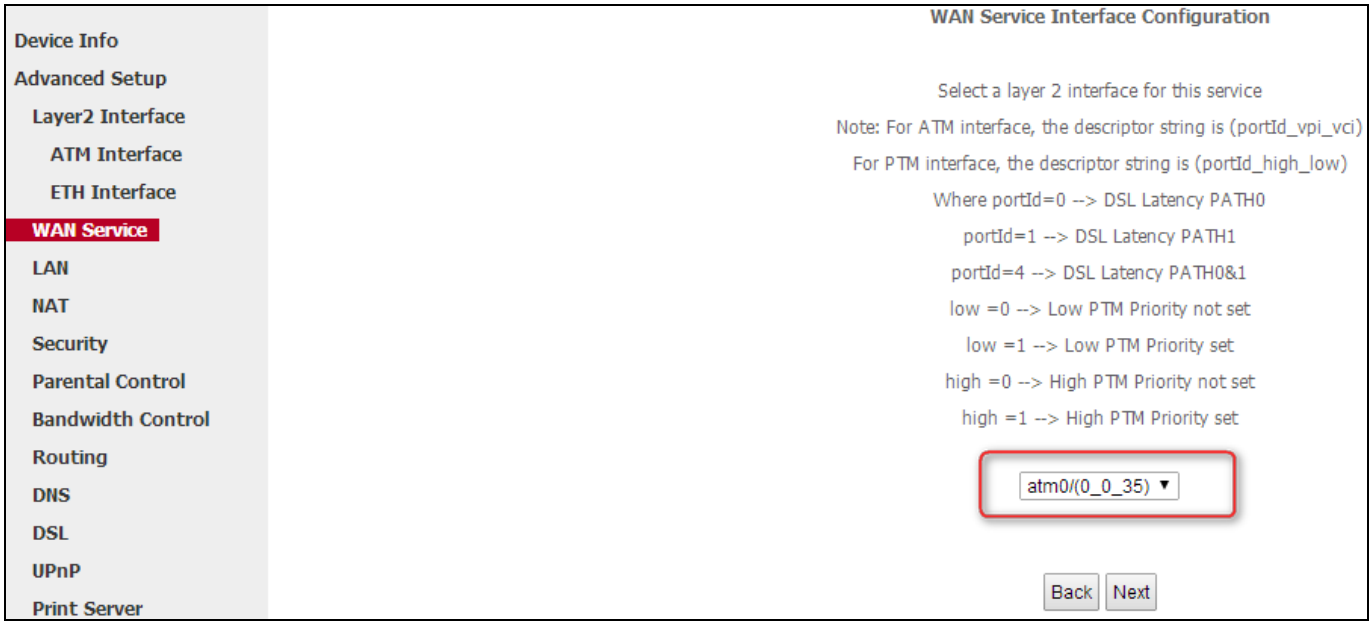
3) PPPoE IPv6 Only Users

If you configure the **ATM Interface** (ADSL uplink) and select **EoA** as the DSL link type, then you can start to set up WAN service for accessing the Internet.

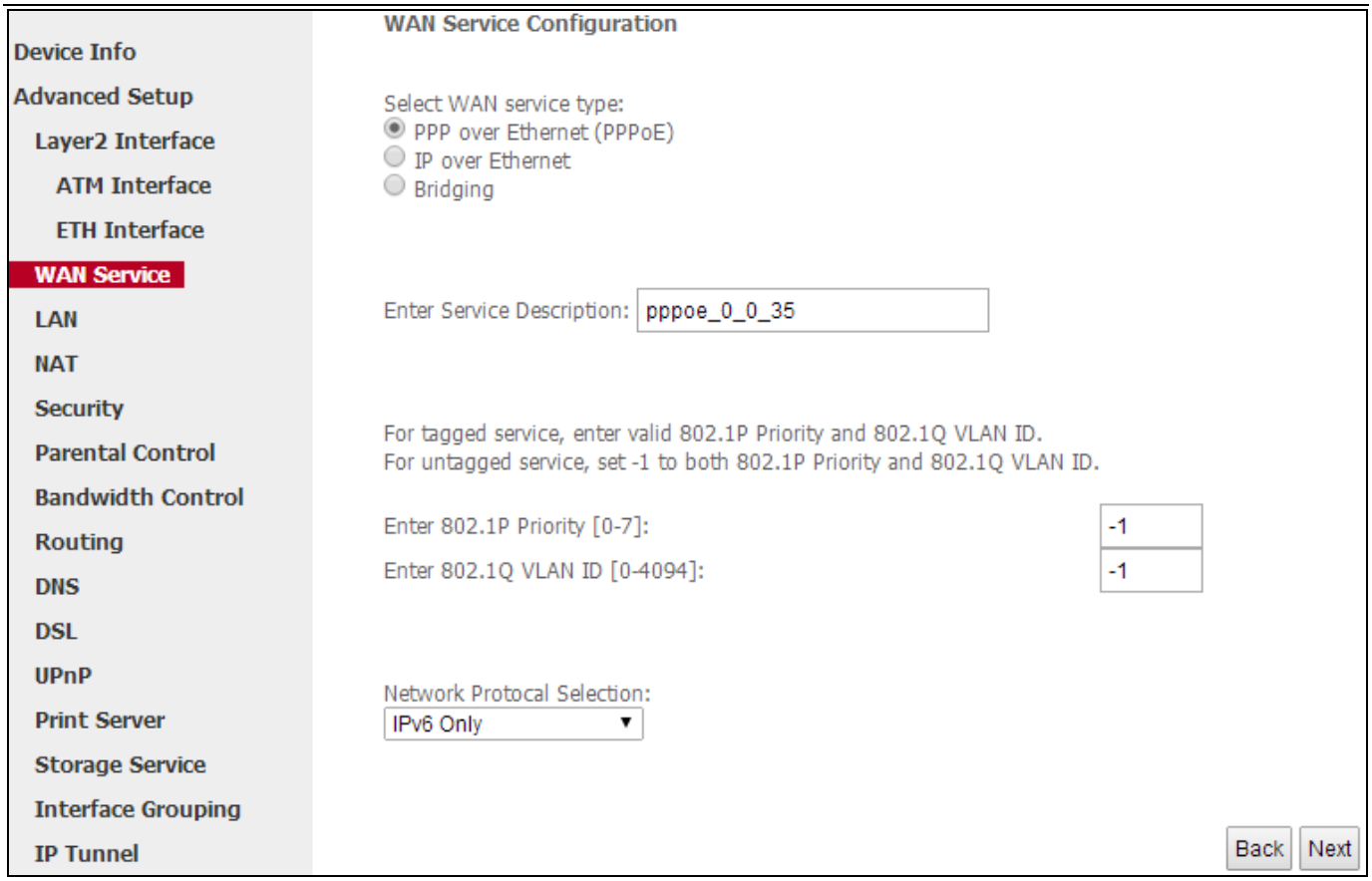
❶ Click **Advanced Setup > WAN Service** and then click the **Add** button.



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



❸ 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.**

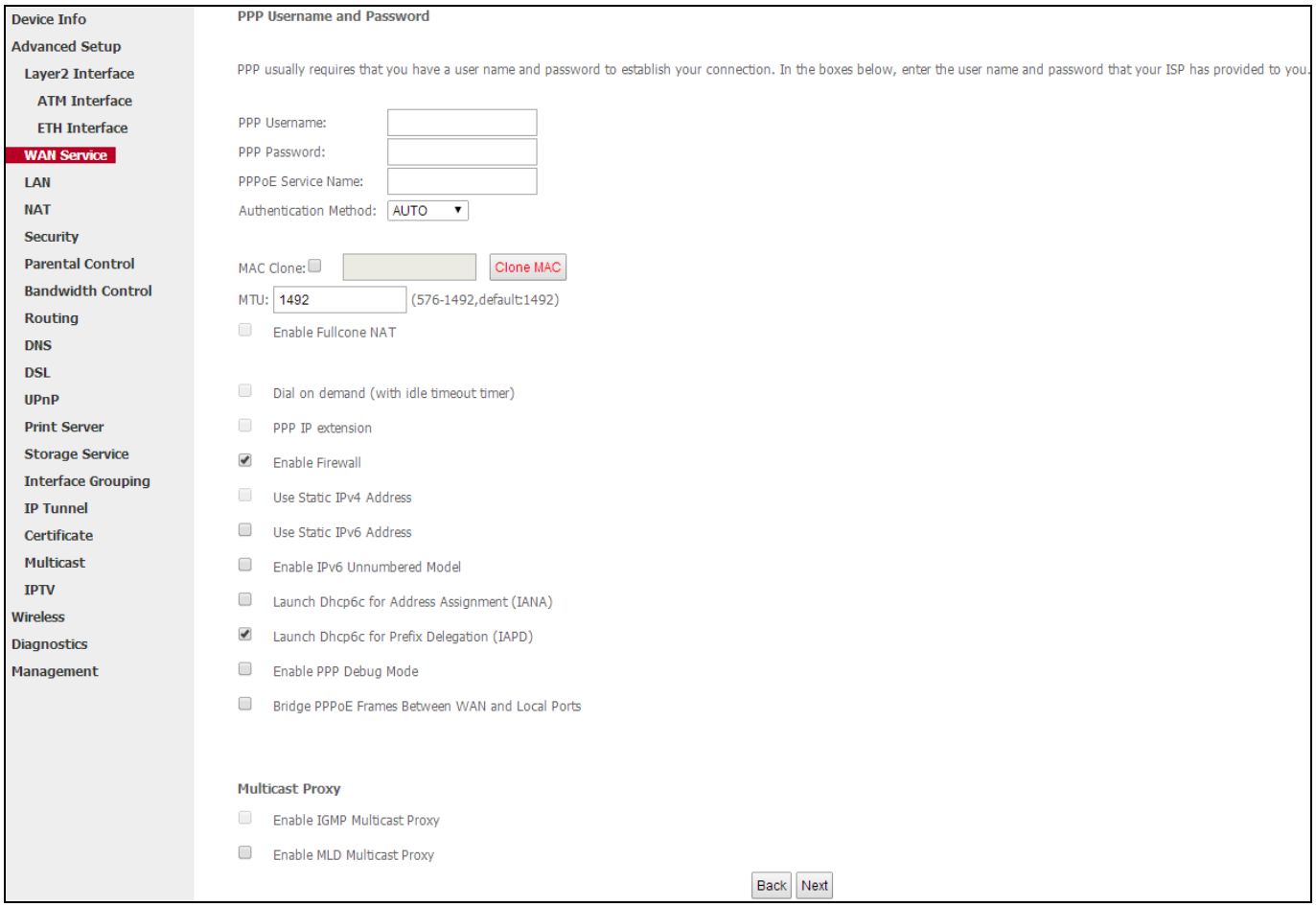


❹ Configure PPP Username and Password and other settings on the figure below. Each field with its indication is mentioned above in **PPPoE and IPv4 users** section.

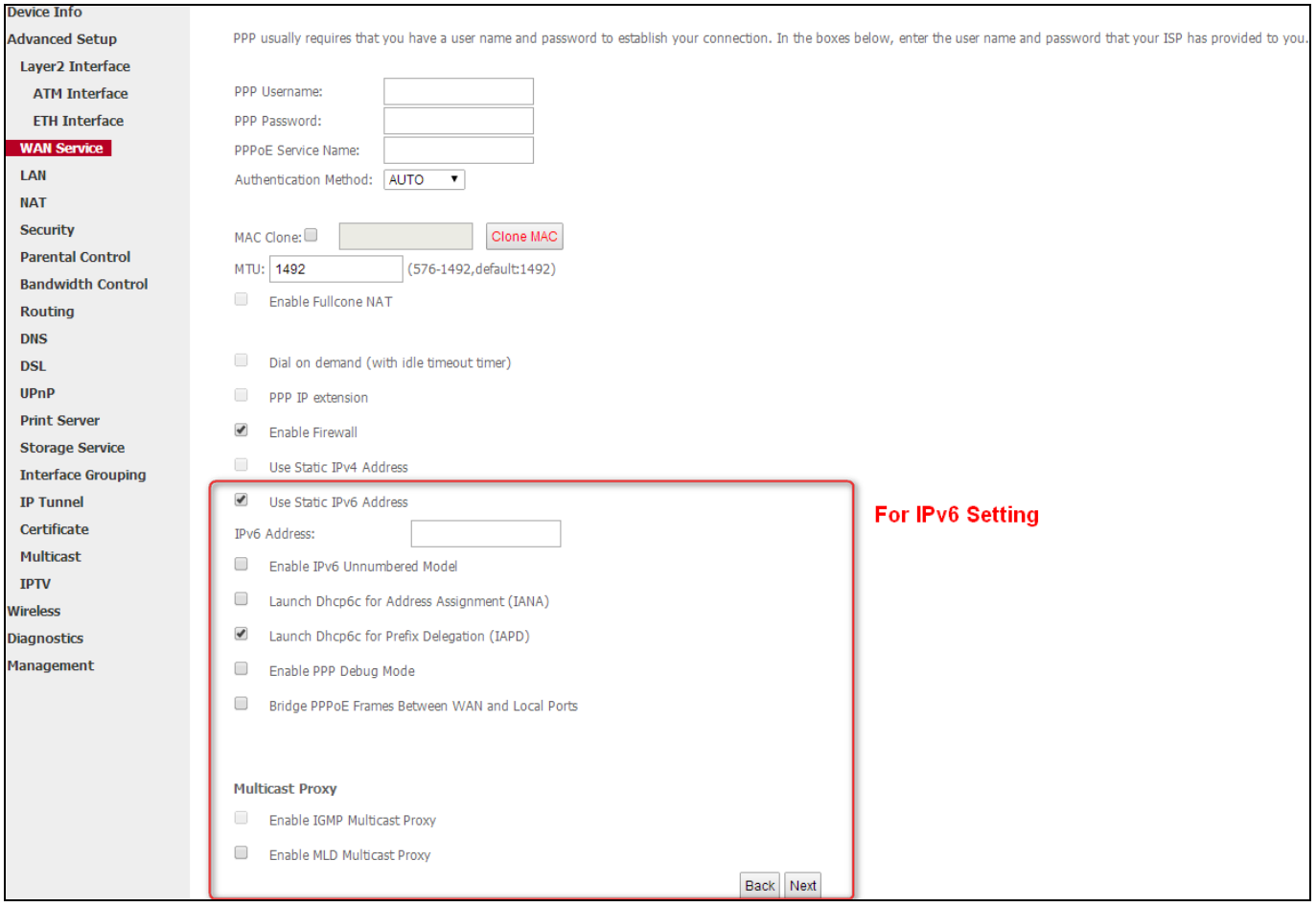
If ISP provides you no static IPv6 address, you just keep the default settings DHCP mode.

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

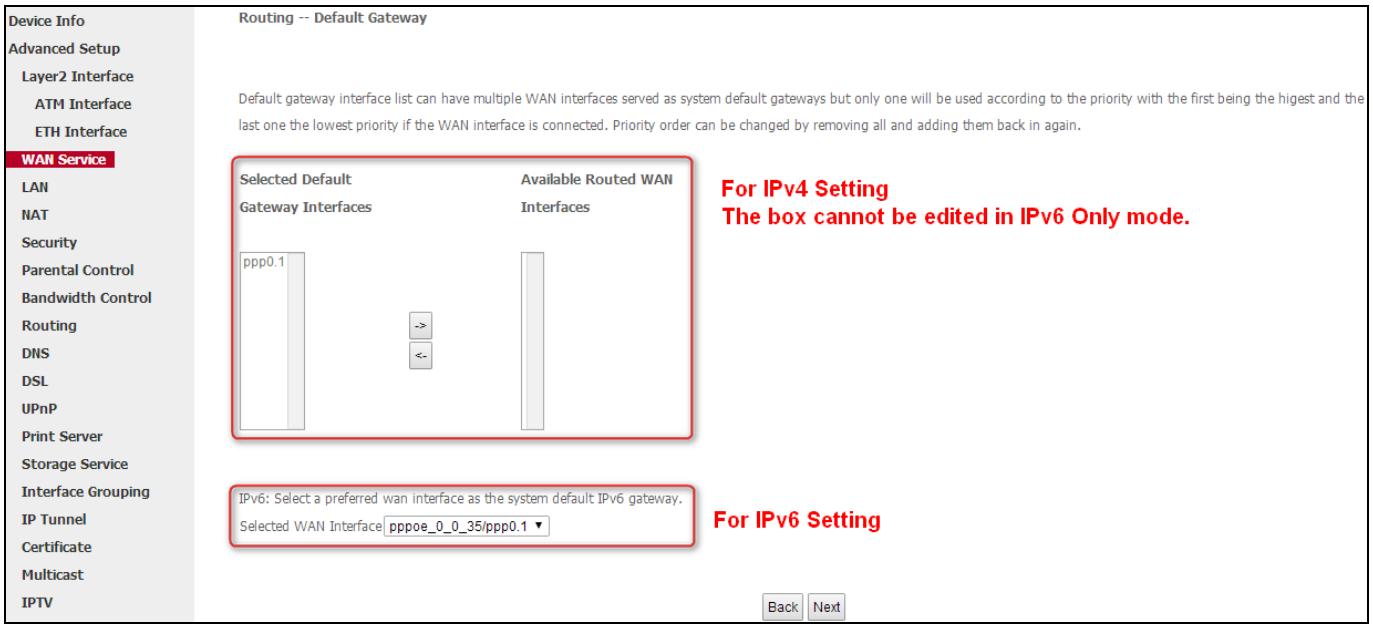
If your ISP is using stateful DHCPv6, check **Launch Dhcp6c for Address Assignment (IANA)** also. Click **Next.**



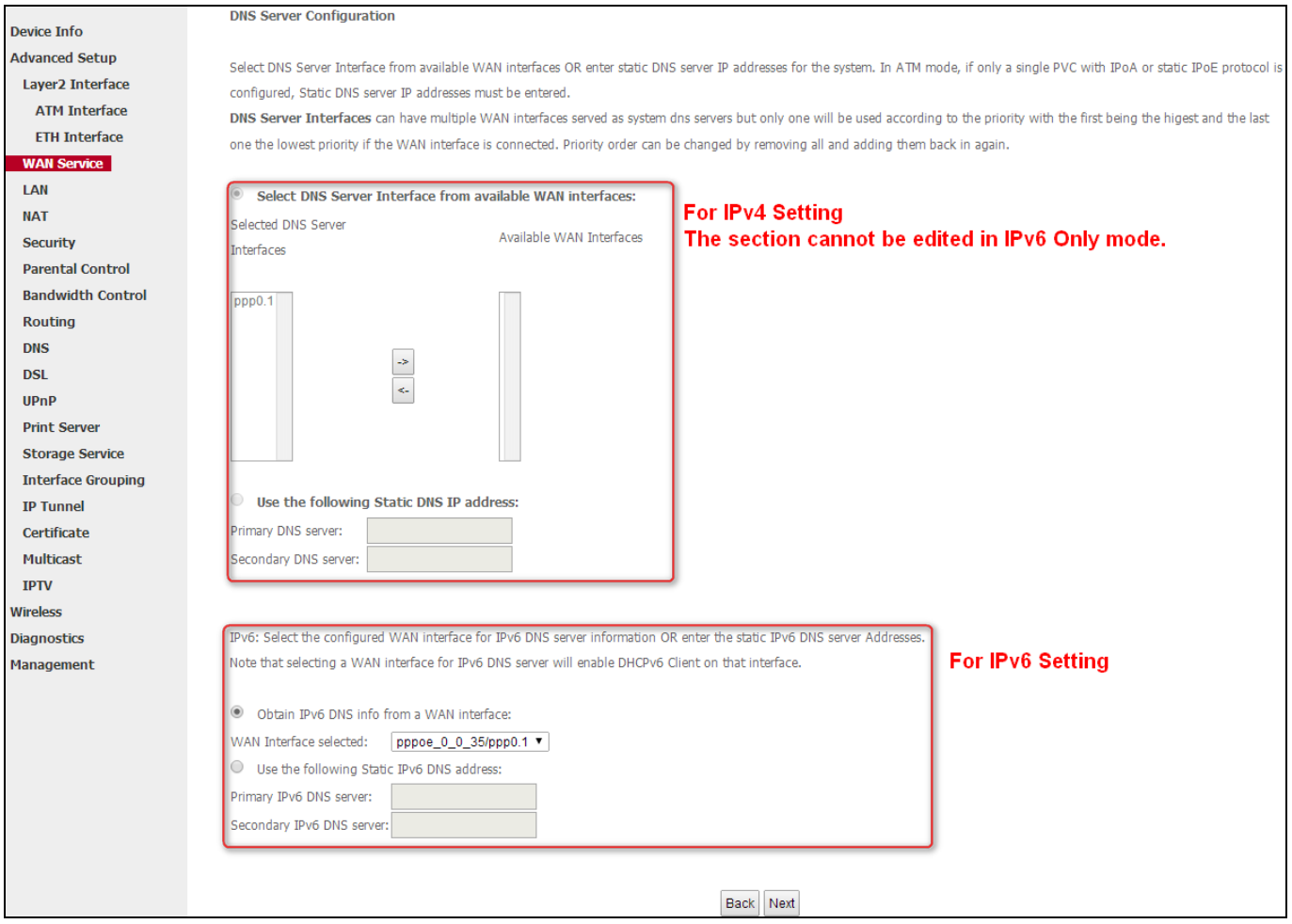
If ISP provides you with the static IPv6 address, configure a static IP address by checking **Use Static IPv6 Address** and enter the static IPv6 address.



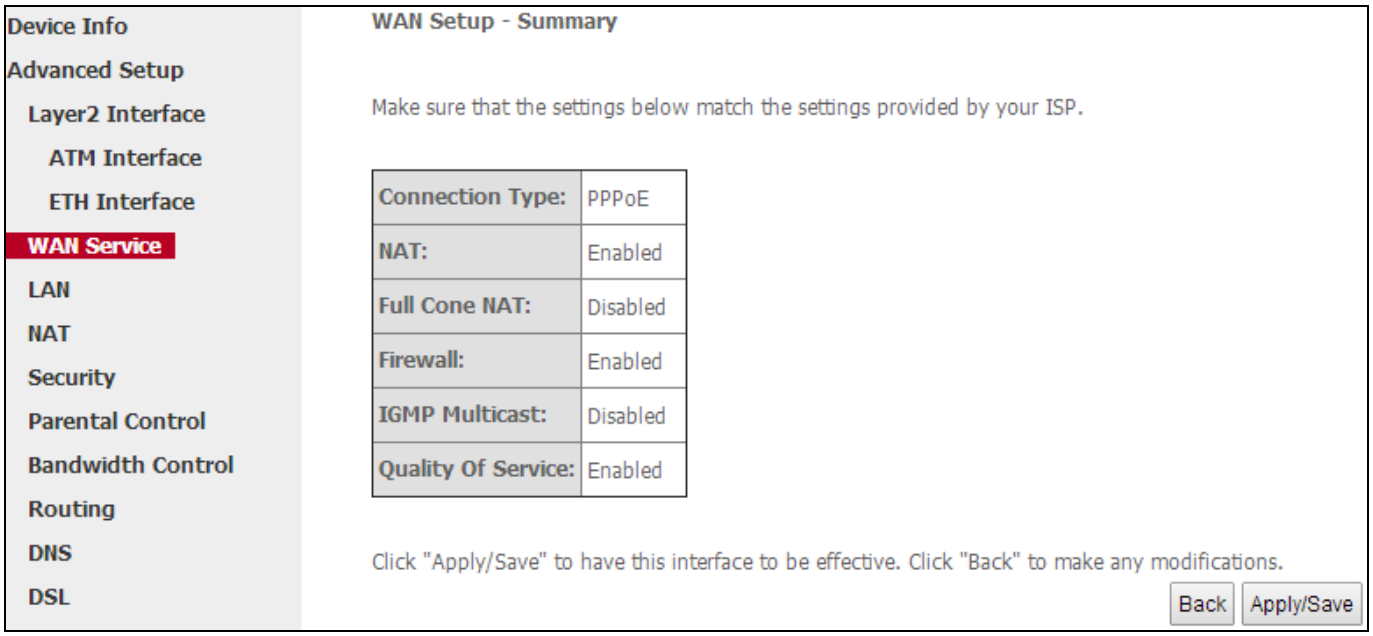
❺ To configure the Default Gateway interface when using IPv6, select the interface that you want to configure with the WAN gateway address in **Selected WAN Interface** box. Then click **Next**.



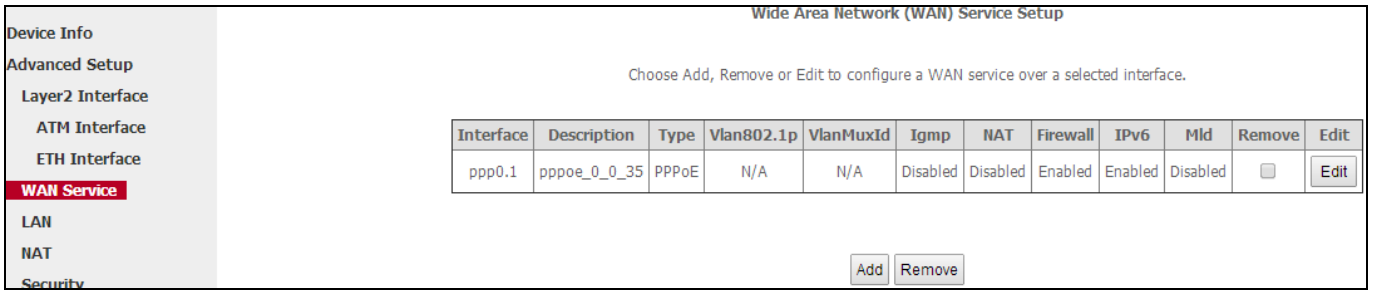
❻ To configure the WAN DNS address, check the **Obtain IPv6 DNS info from a WAN interface** option, or select the **Use the following Static IPv6 DNS address** option to enter the static DNS server IPv6 addresses provided by your ISP. At last, click **Next**.



Click **Apply/Save** to save your settings if everything is correctly set.



Here you can view your configurations. When the PPPoE connection is successful, you can access the Internet.



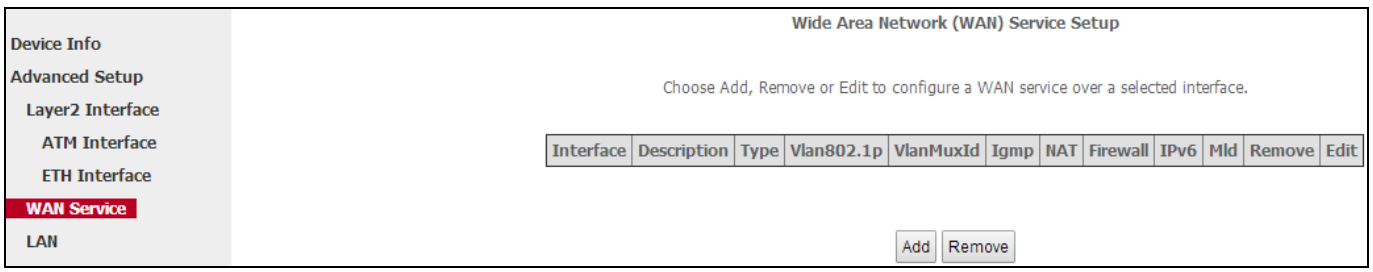
↗ Steps 1~6 above for **PPPoE and IPv6 Only** users

4) IPoE IPv4 Only Users

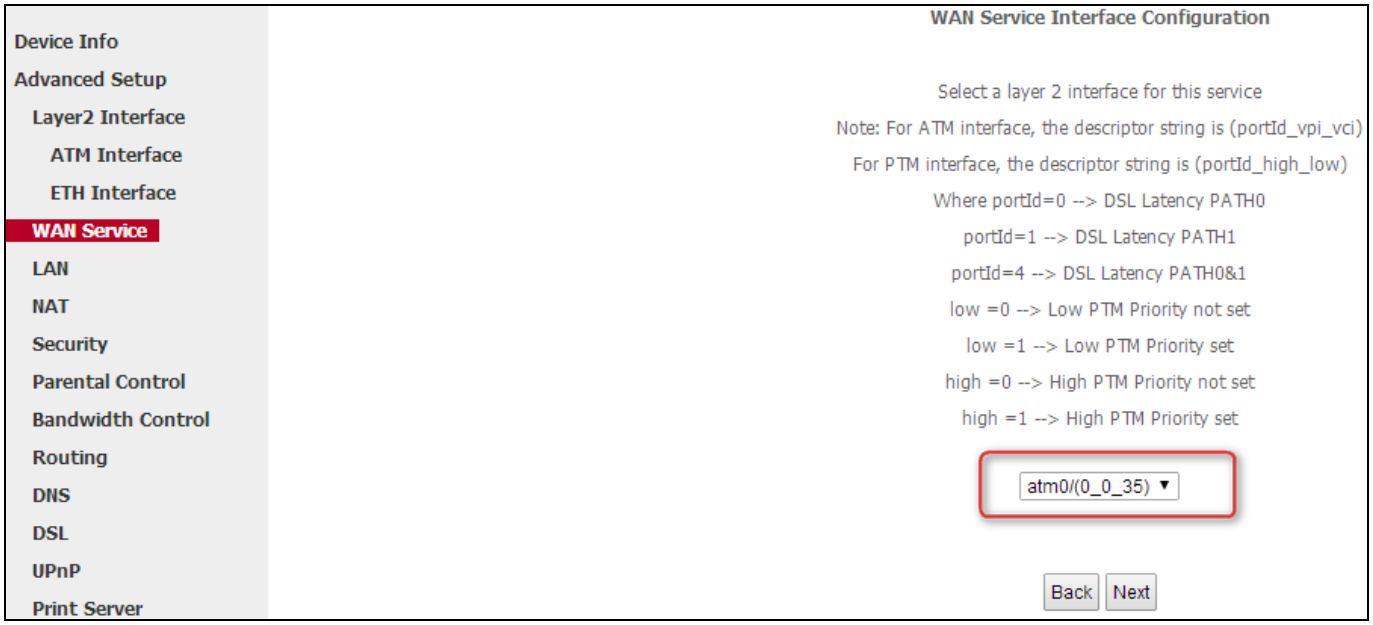
If your ISP uses DHCP to assign your IP address or if your ISP assigns you a static (fixed) IP address, IP subnet mask and the gateway IP address, you need to select the IP over Ethernet (IPoE).

After you configure the **ATM Interface** (ADSL uplink) and select **EoA** as the DSL link type, you can start to set up WAN service for accessing the Internet.

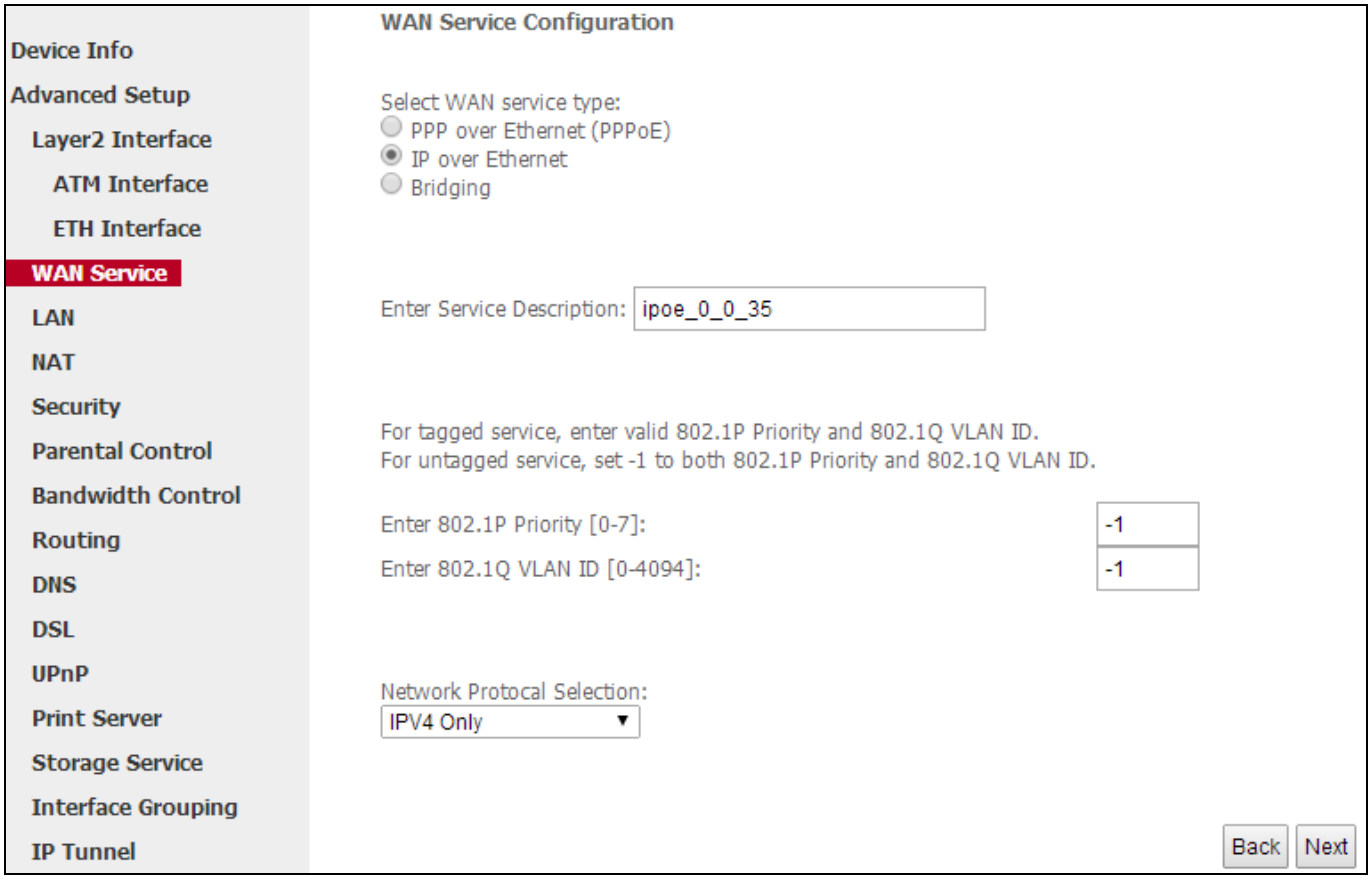
❶ Click **Advanced Setup** > **WAN Service** and then click the **Add** button.



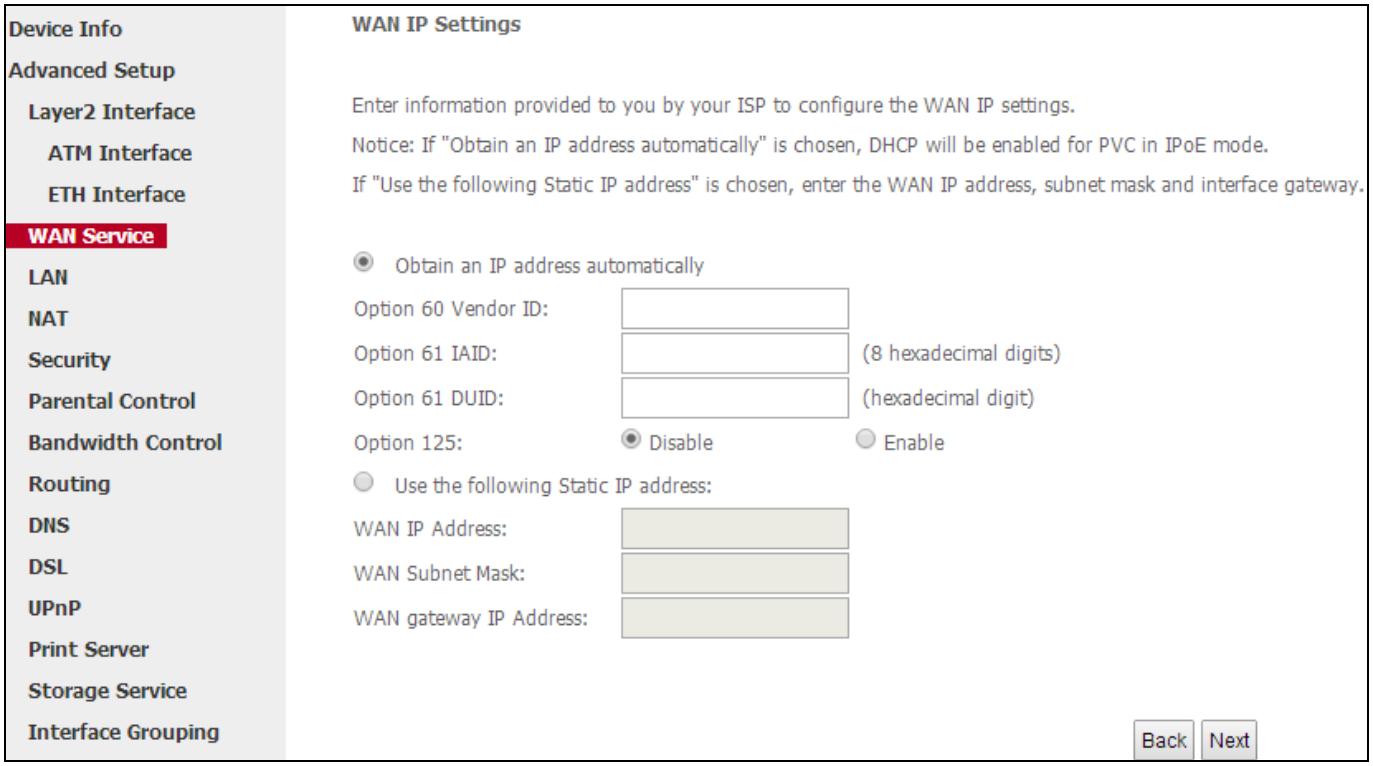
❷ Select the ATM interface you added just now from the pull-down menu in the figure below. Click **Next**.



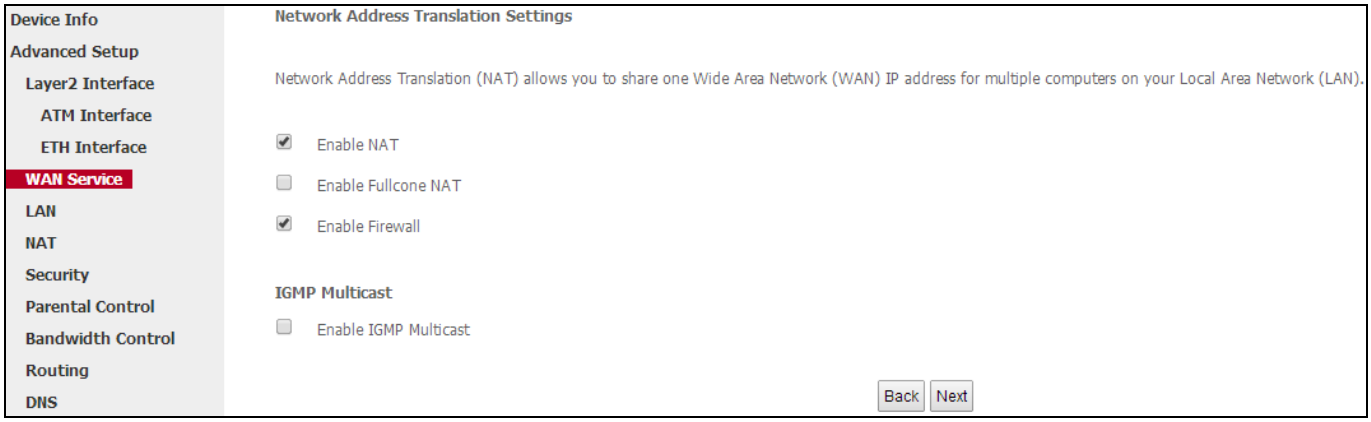
❸ Select **IP over Ethernet**. Edit the **Enter Service Description** which is optional. Suggest you keep the default. Select a network protocol: **IPv4 Only**. Click **Next**.



❹ Finish **WAN IP Settings** on the figure below. Click **Next**.

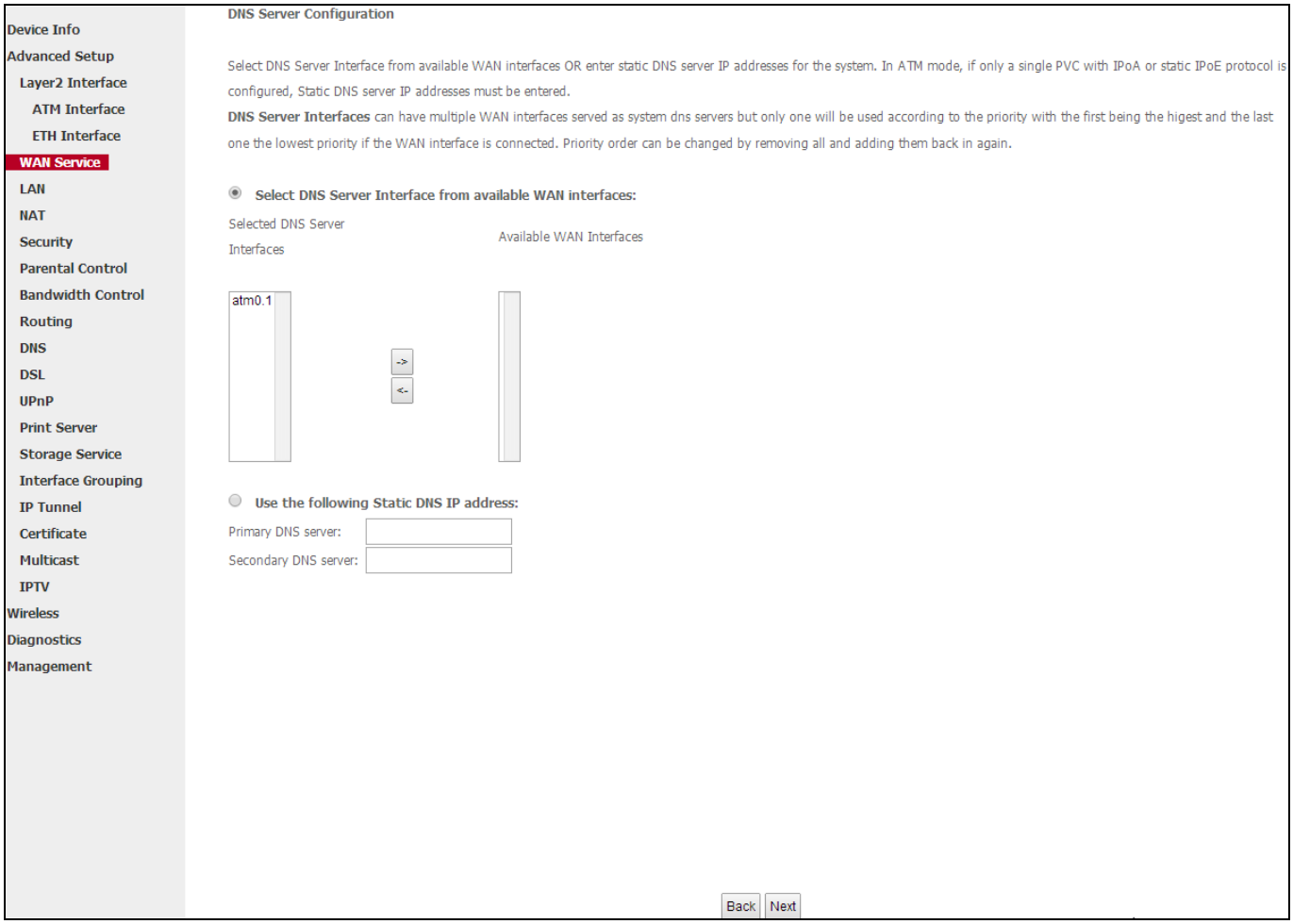


❺ Finish **Network Address Translation Settings**. Suggest keeping the default settings. Click **Next**.

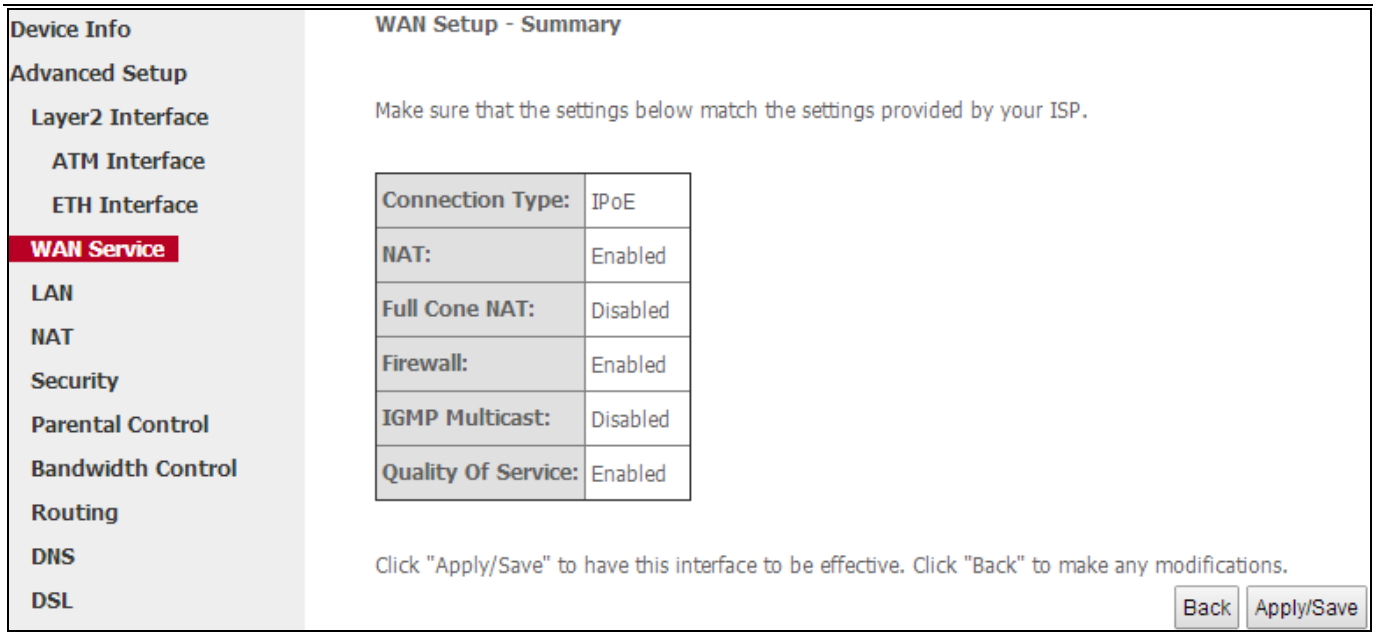


❻ To configure the Default Gateway interface, select the interface that you want to configure with the WAN gateway address in **Available Routed WAN Interfaces** box and move it into **Selected Default Gateway Interfaces** box. The default setting is recommended. Then click **Next**.

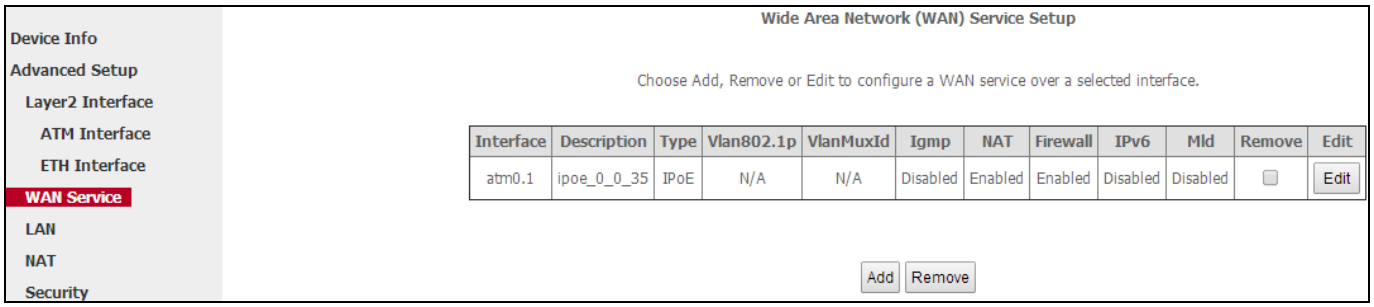
❼ To finish DNS Server Configuration, click the **Select DNS Server Interface from available WAN interfaces** option, or select the **Use the following Static DNS IP address** option and enter the static DNS server IP addresses provided by your ISP. At last, click **Next**.



Click **Apply/Save** to save your settings if everything is correctly set.



Here you can view your configurations. When the IPoE connection is successful, you can access the Internet.



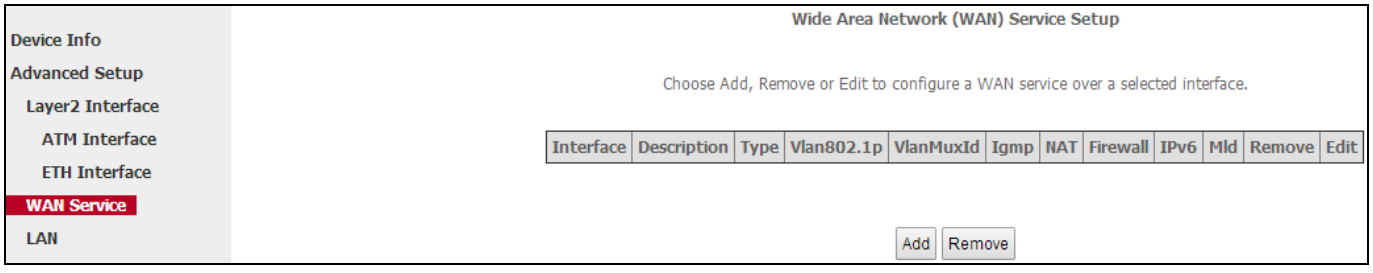
↗ Steps 1~7 above for **IPoE and IPv4 Only** users

5) IPoE IPv4&IPv6 (Dual Stack) Users

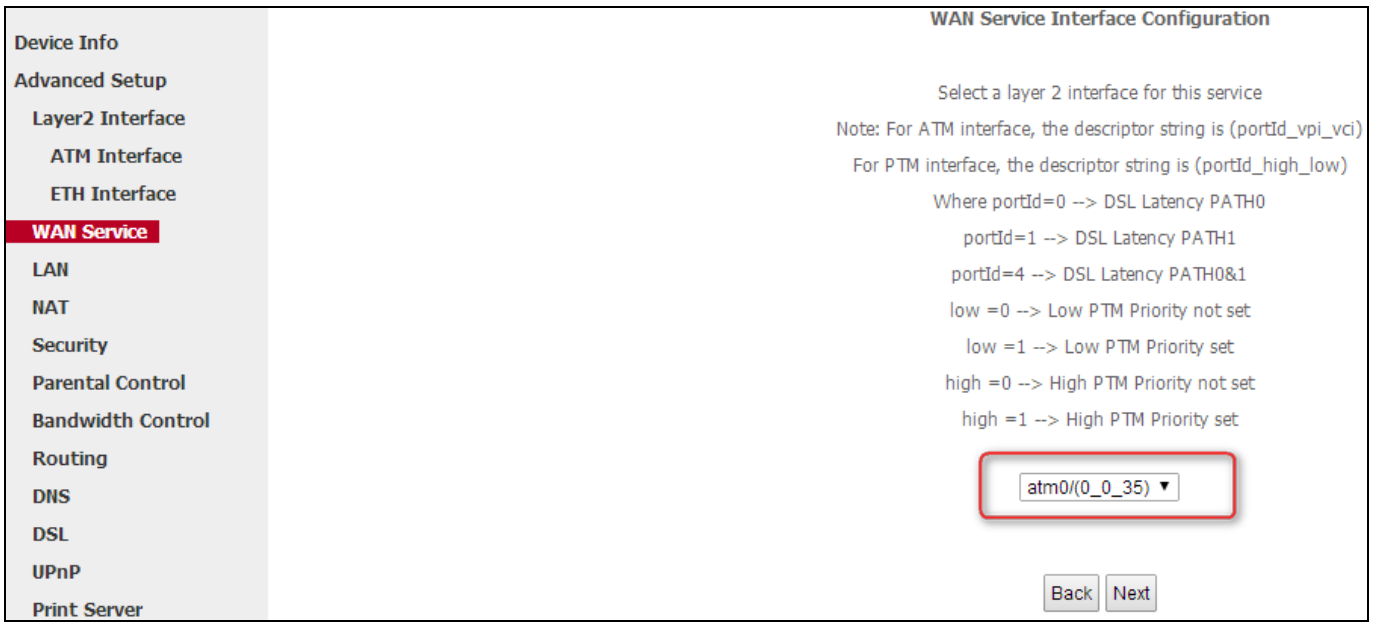
If your ISP uses DHCP to assign your IP address or if your ISP assigns you a static (fixed) IP address, IP subnet mask and the gateway IP address, you need to select the IP over Ethernet (IPoE).

After you configure the **ATM Interface** (ADSL uplink) and select **EoA** as the DSL link type, you can start to set up WAN service for accessing the Internet.

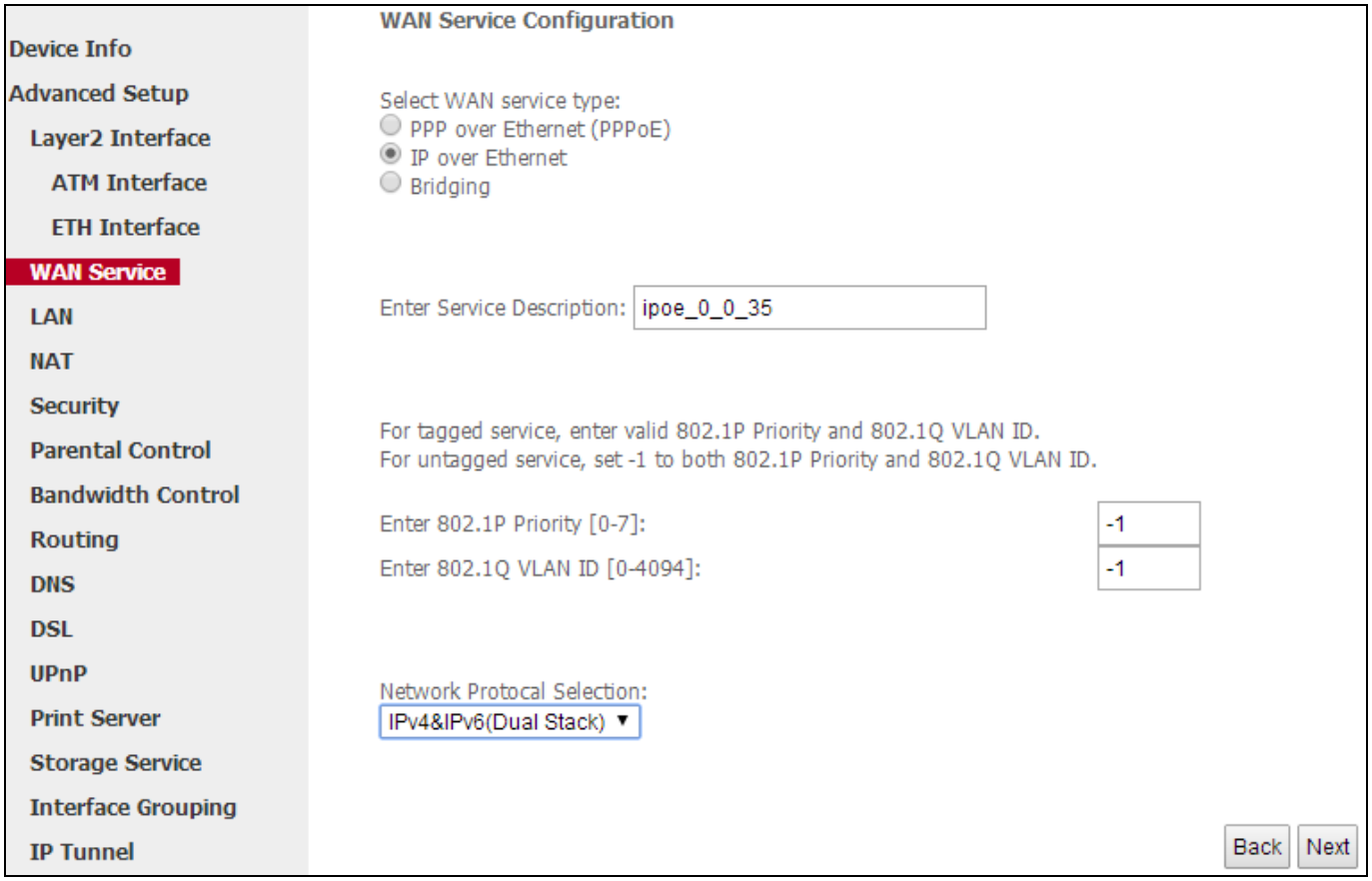
❶ Click **Advanced Setup > WAN Service** and then click the **Add** button.



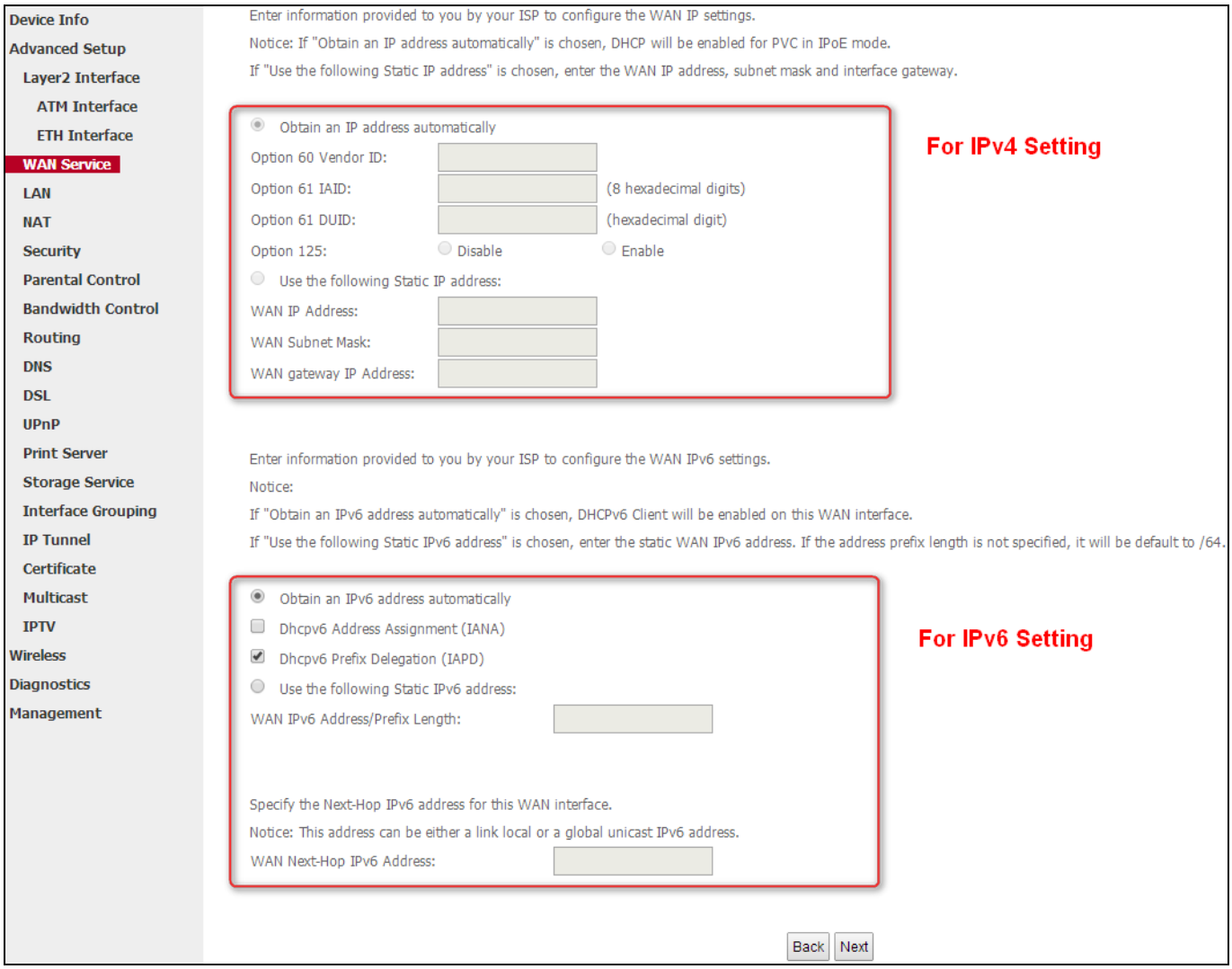
❷ Select the ATM interface you added just now from the pull-down menu in the figure below. Click **Next**.



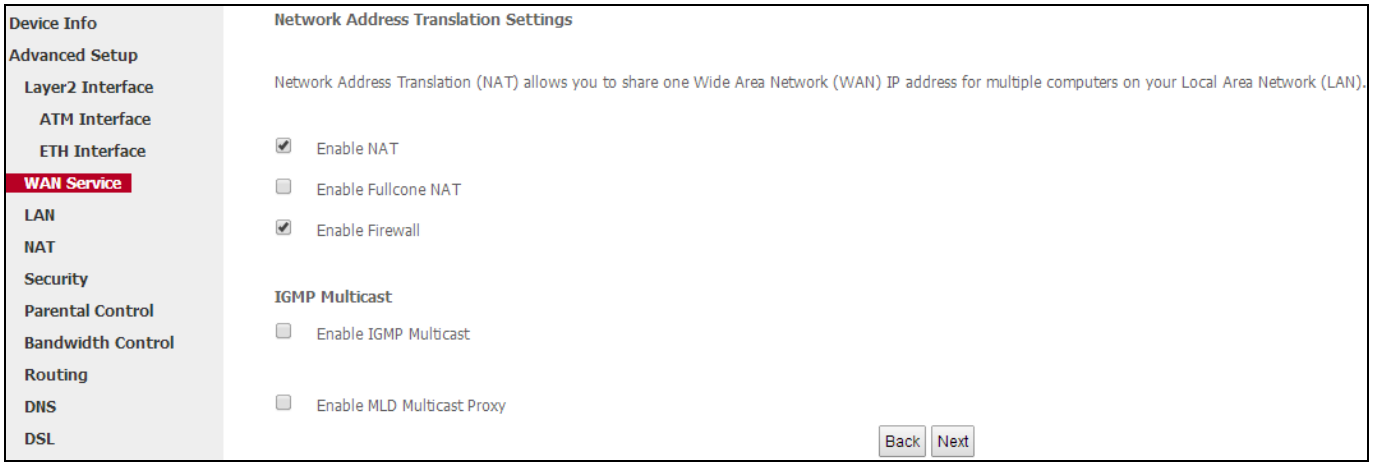
❸ Select **IP over Ethernet**. Edit the **Enter Service Description** which is optional. Suggest you keep the default. Select a network protocol you need: **IPv4&IPv6 (Dual Stack)**. Click **Next**.



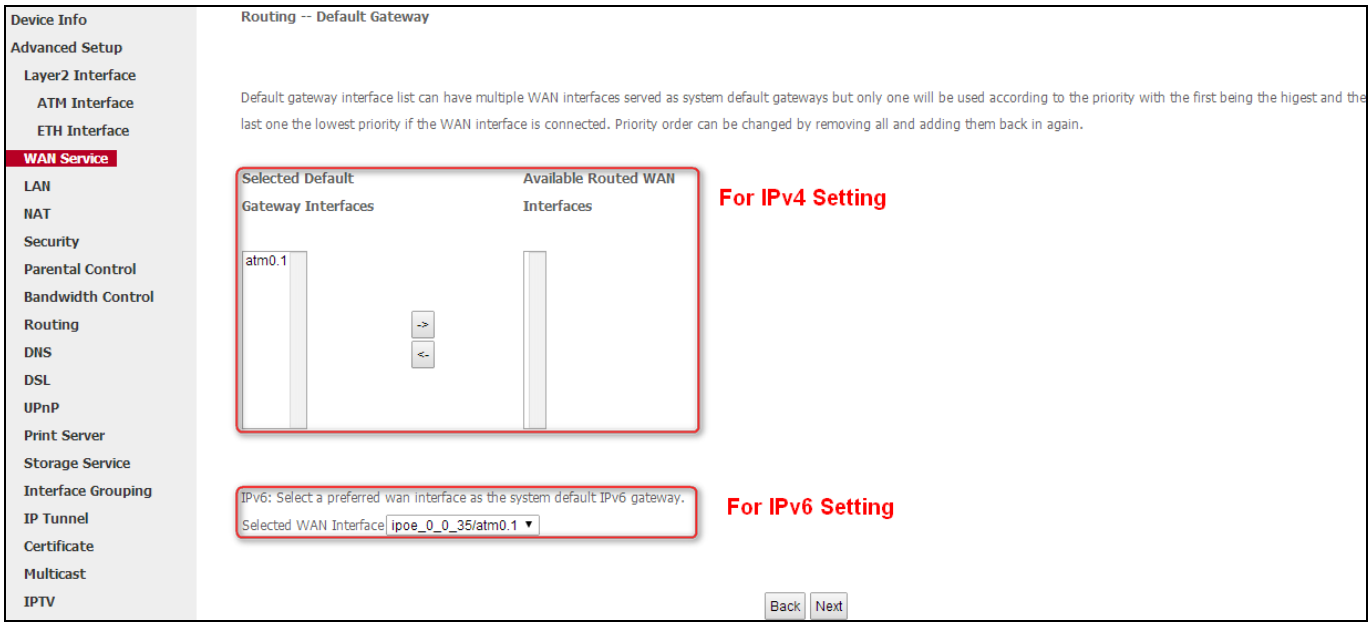
❹ To finish WAN IP Settings, select **Obtain an IP/IPv6 address automatically**, check **Dhcpv6 Prefix Delegation (IAPD)**. If your ISP is using stateful DHCPv6, check **Dhcpv6 Address Assignment (IANA)** also. Or select **Use the following Static IP/IPv6 address** if your ISP provide you with an IPv6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



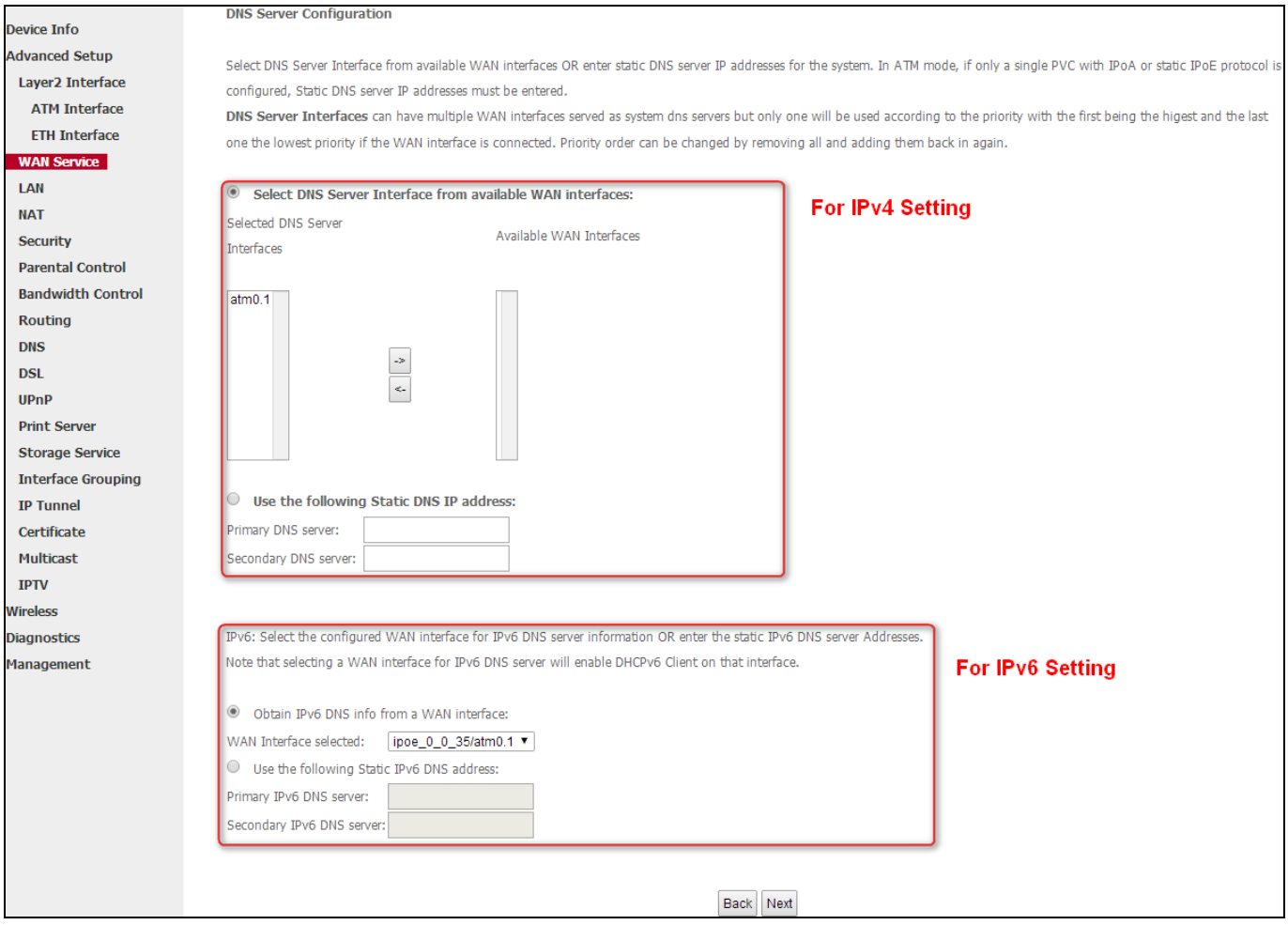
❺ Finish Network Address Translation Settings. Suggest keeping the default settings. Click **Next**.



❻ To configure the Default Gateway interface, select the interface that you want to configure with the WAN gateway address. Then click **Next**.



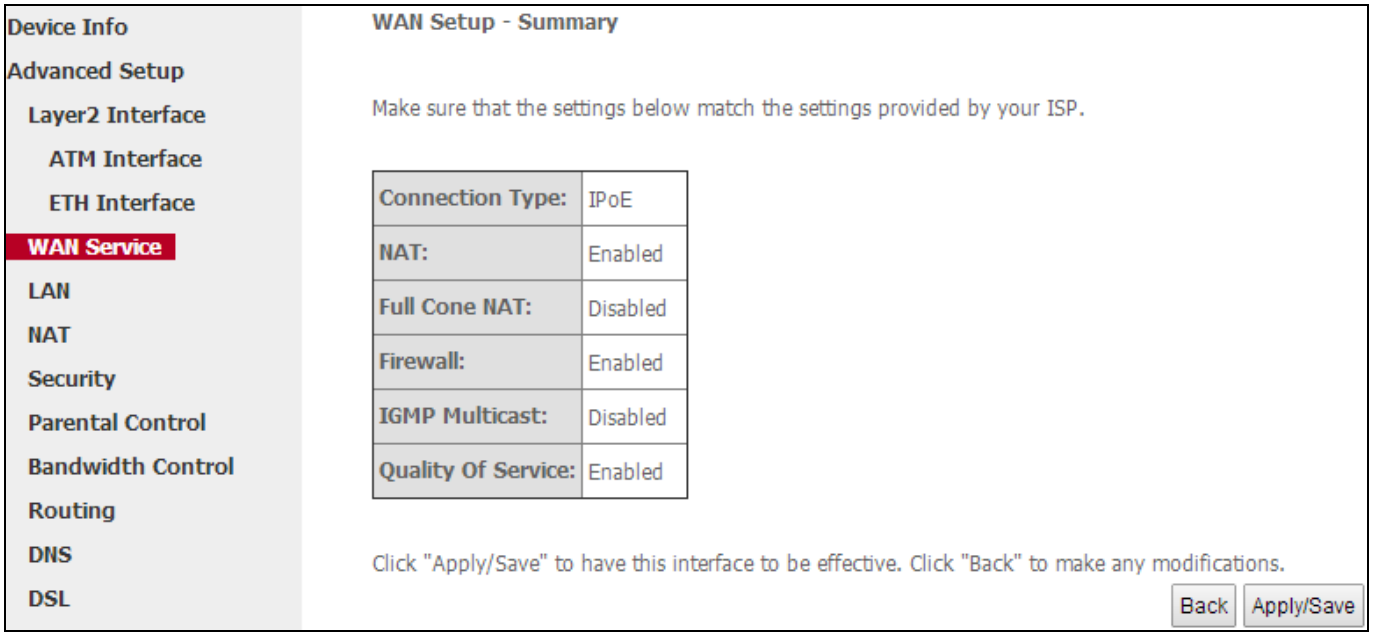
❼ To configure the WAN DNS address, finish both the IPv4 setting and IPv6 setting. Click **Next**.



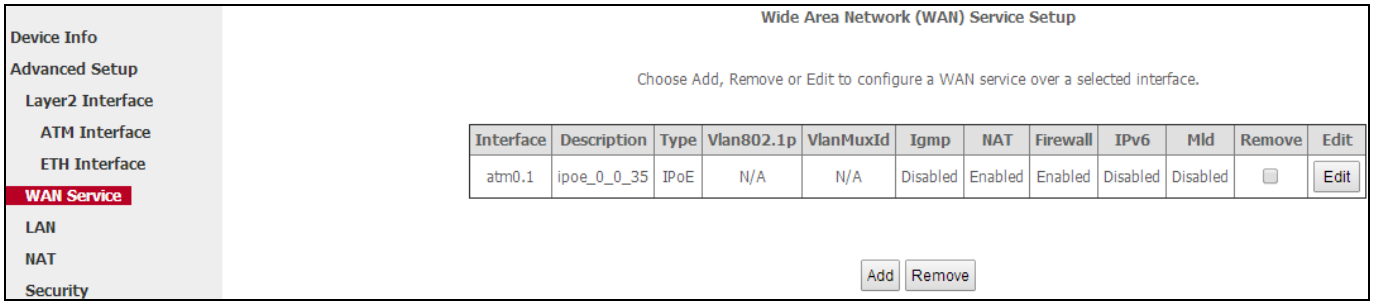
Note

If **Obtain an IP address automatically** is chosen, DHCP will be enabled for PVC in IPoE mode.

Click **Apply/Save** to save your settings if everything is correctly set.



Here you can view your configurations. When the IPoE connection is successful, you can access the Internet.



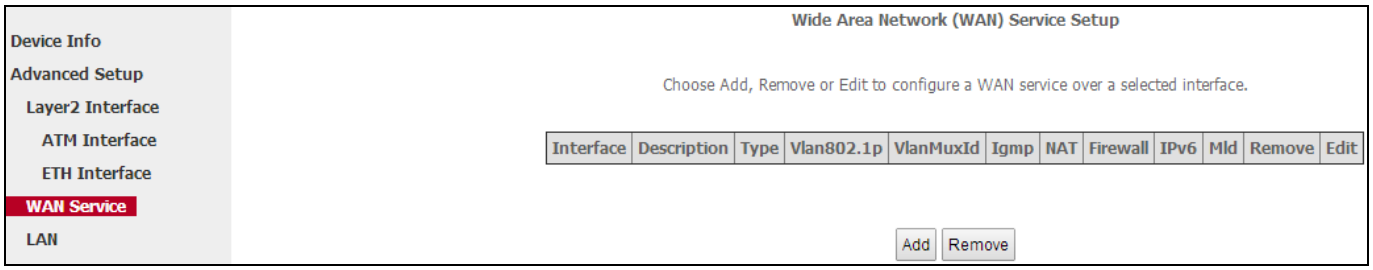
↗ Steps 1~7 above for **IPoE and IPv4&IPv6 (Dual Stack)** Users

6) IPoE IPv6 Only Users

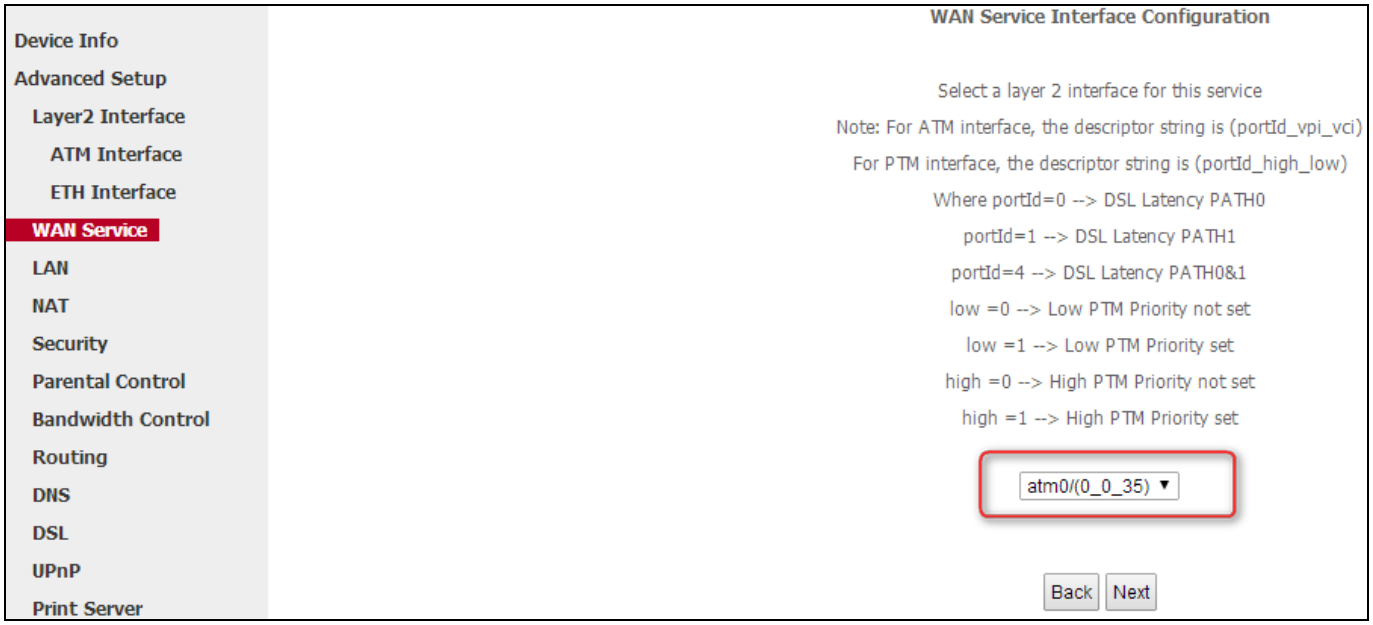
If your ISP uses DHCP to assign your IP address or if your ISP assigns you a static (fixed) IP address, IP subnet mask and the gateway IP address, you need to select the IP over Ethernet (IPoE).

After you configure the **ATM Interface** (ADSL uplink) and select **EoA** as the DSL link type, you can start to set up WAN service for accessing the Internet.

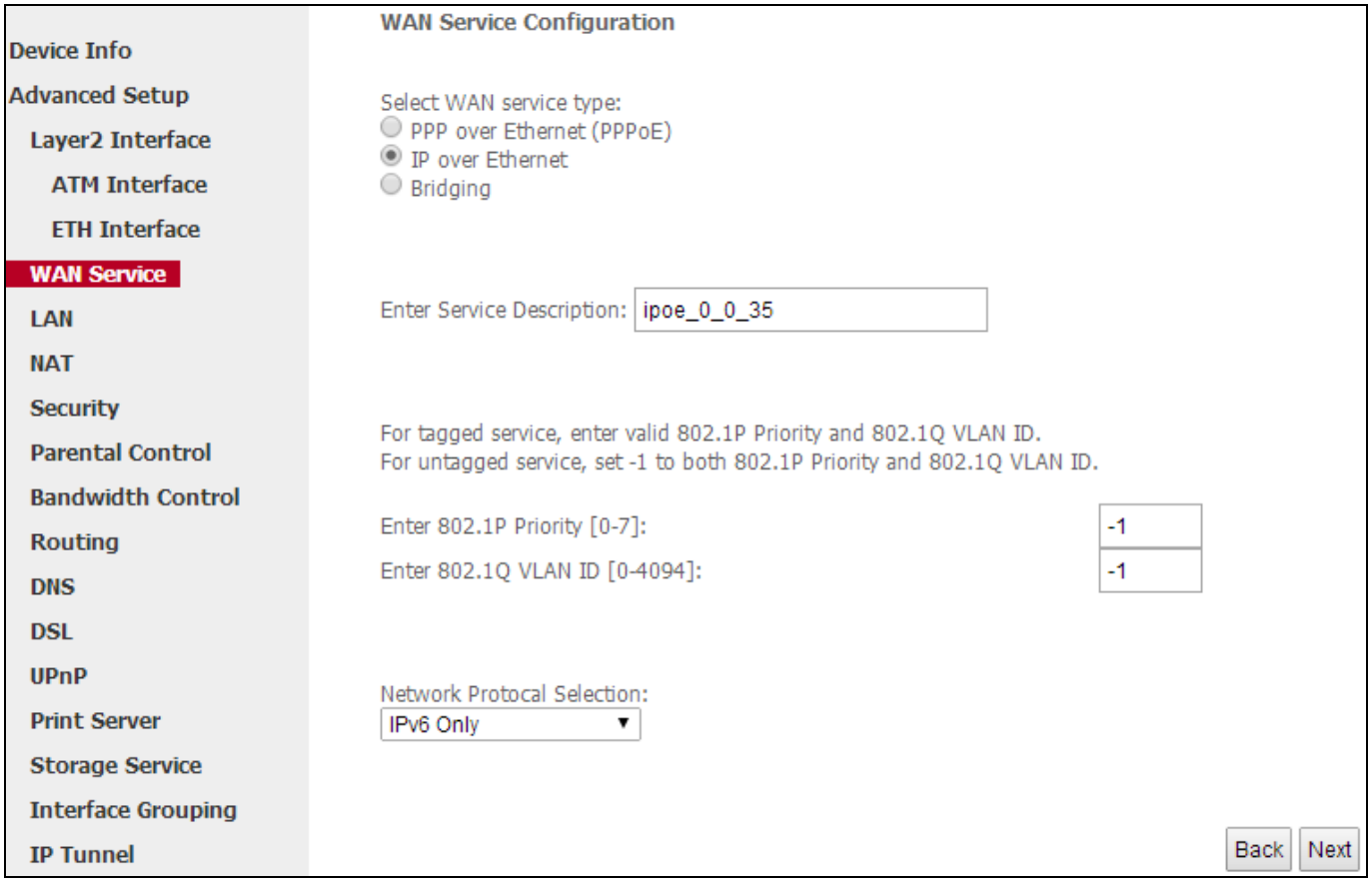
❶ Click **Advanced Setup > WAN Service** and then click the **Add** button.



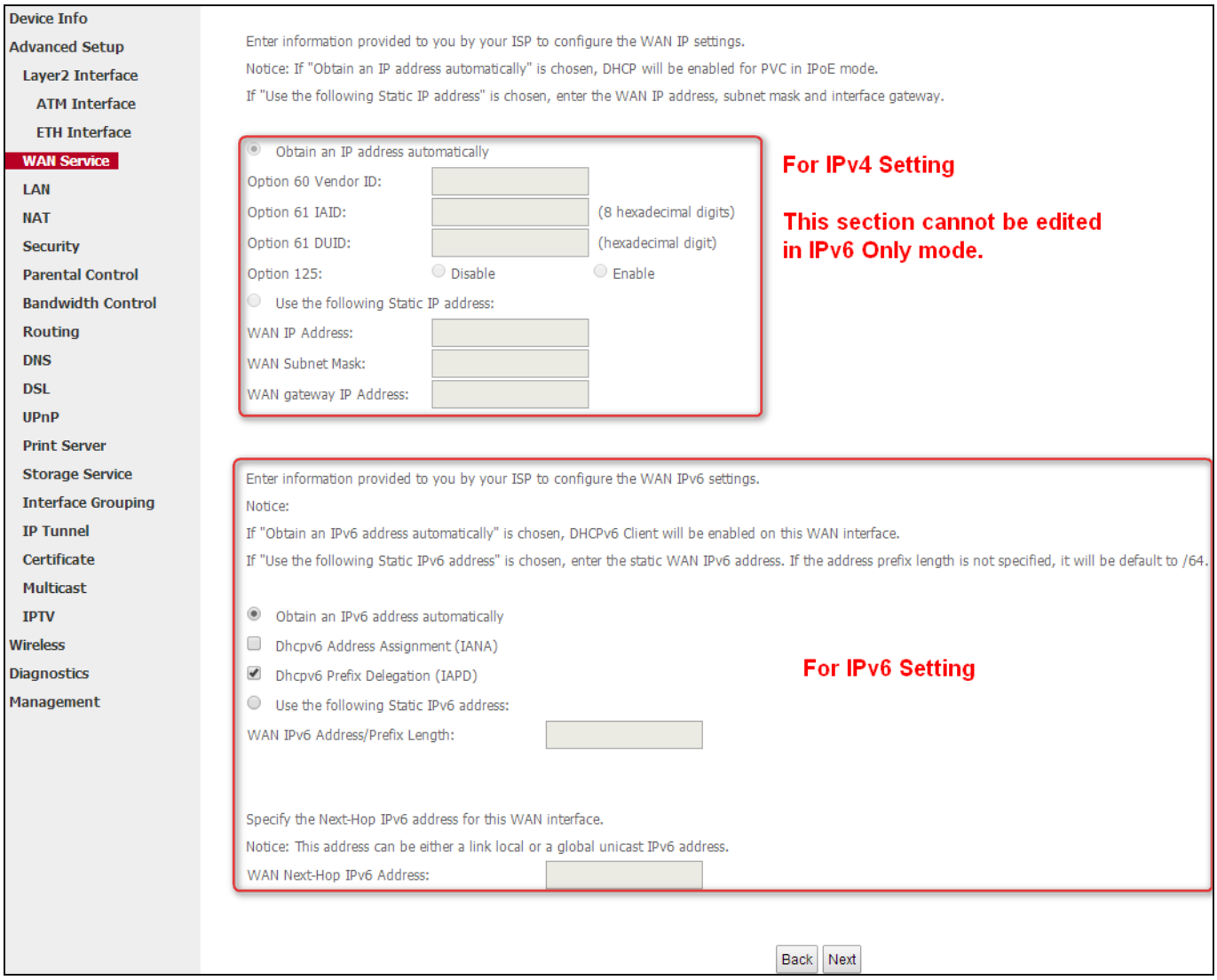
❷ Select the IPoA interface you added just now from the pull-down menu in the figure below. Click **Next**.



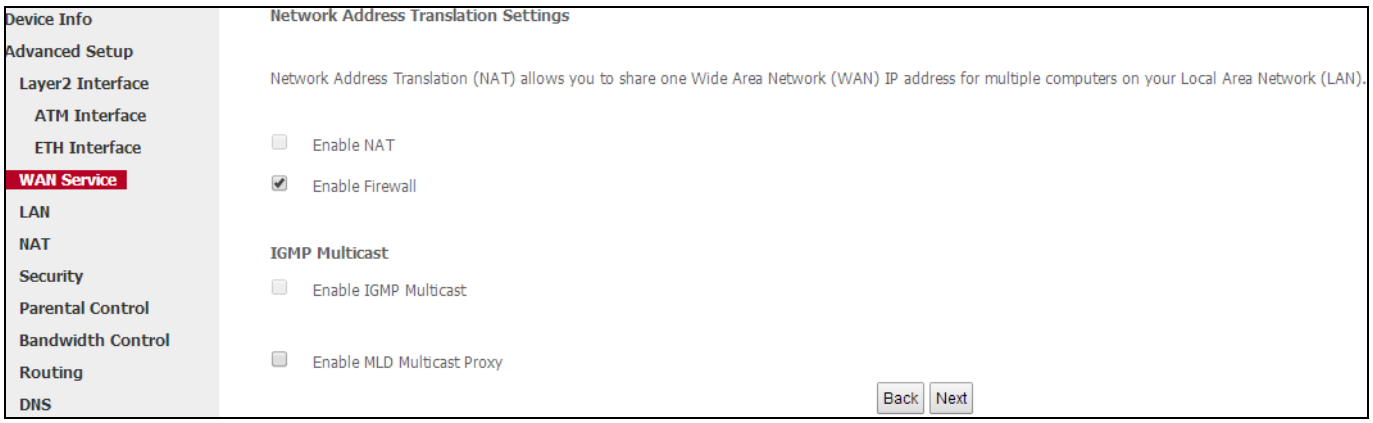
❸ Select **IP over Ethernet (IPoE)**. Edit the **Enter Service Description** field which is optional. Suggest you keep the default. Select a network protocol you need: **IPv6 Only**. Click **Next.**



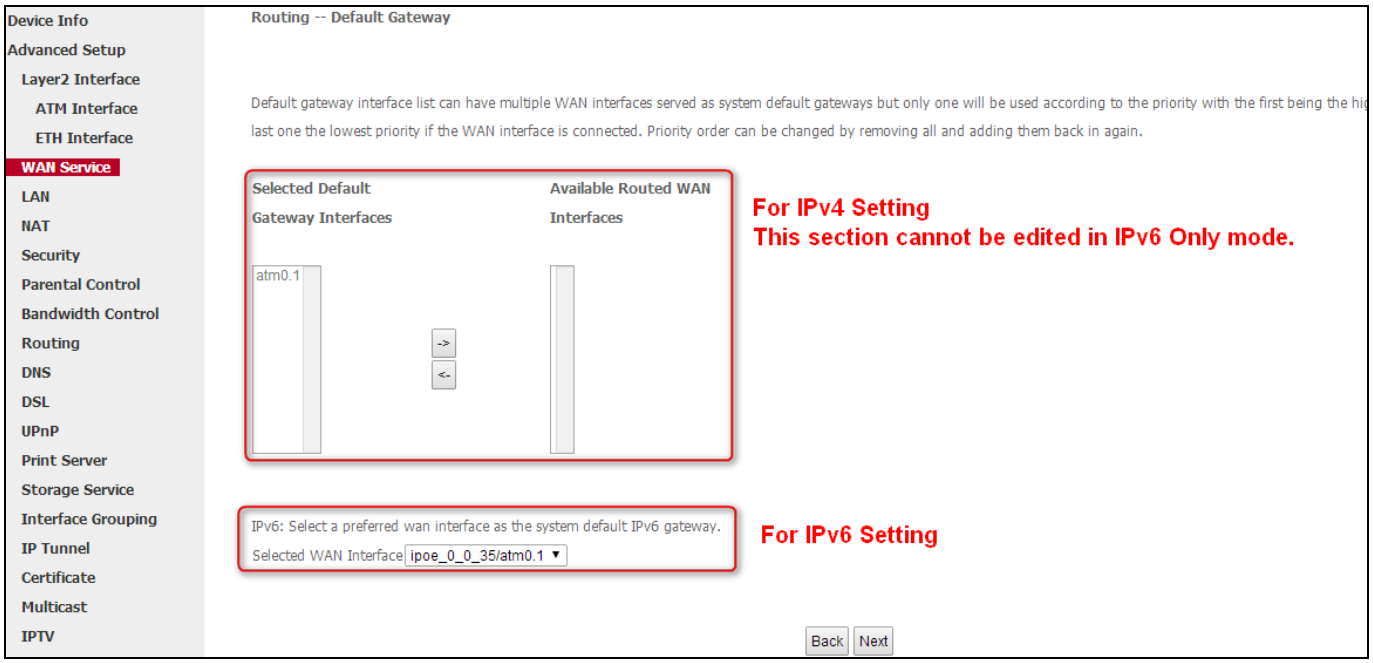
❹ Finish **WAN IP Settings** on the figure below. Click **Next**.



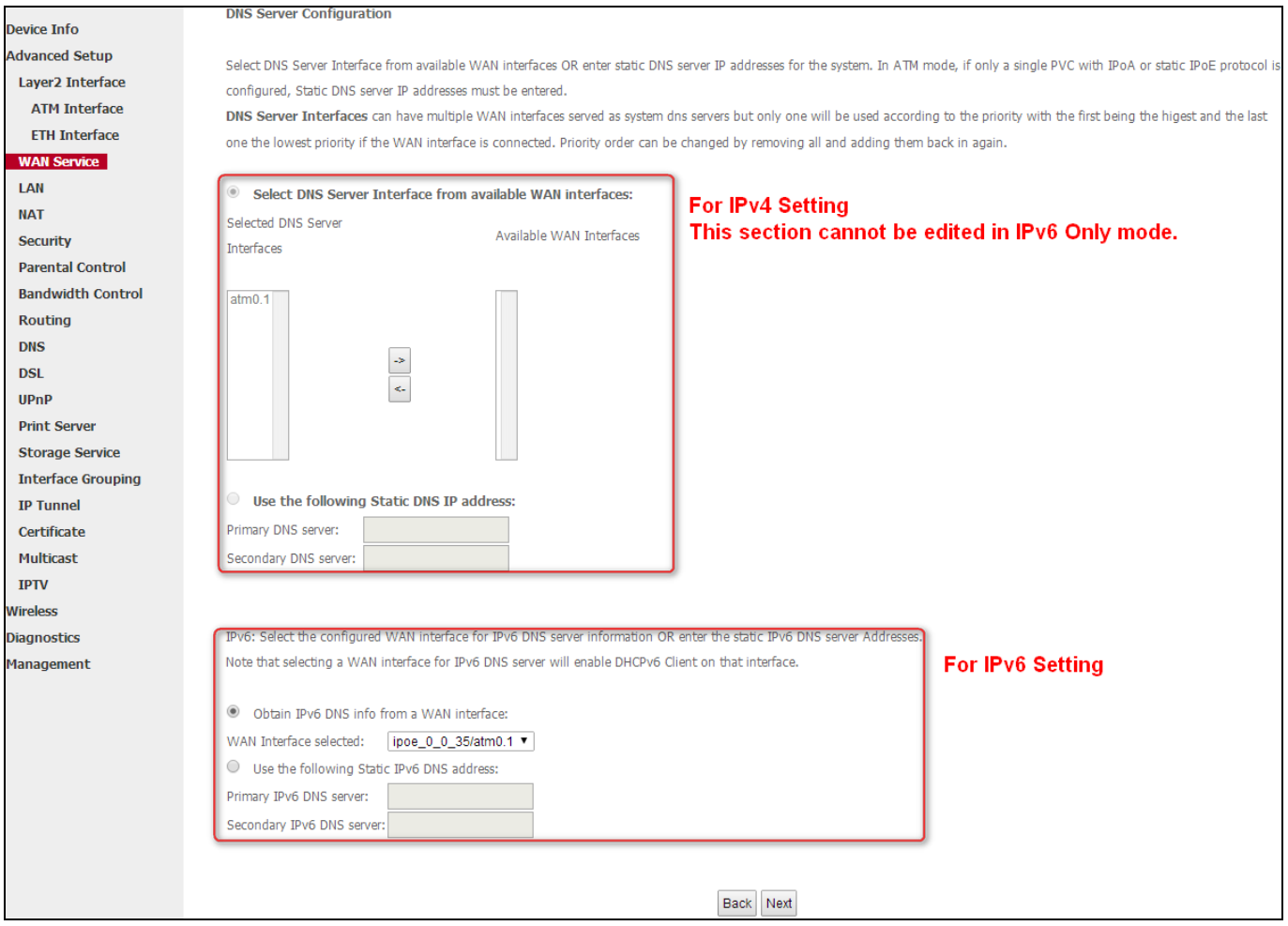
❺ Finish Network Address Translation Settings. Suggest keeping the default settings. Click **Next**.



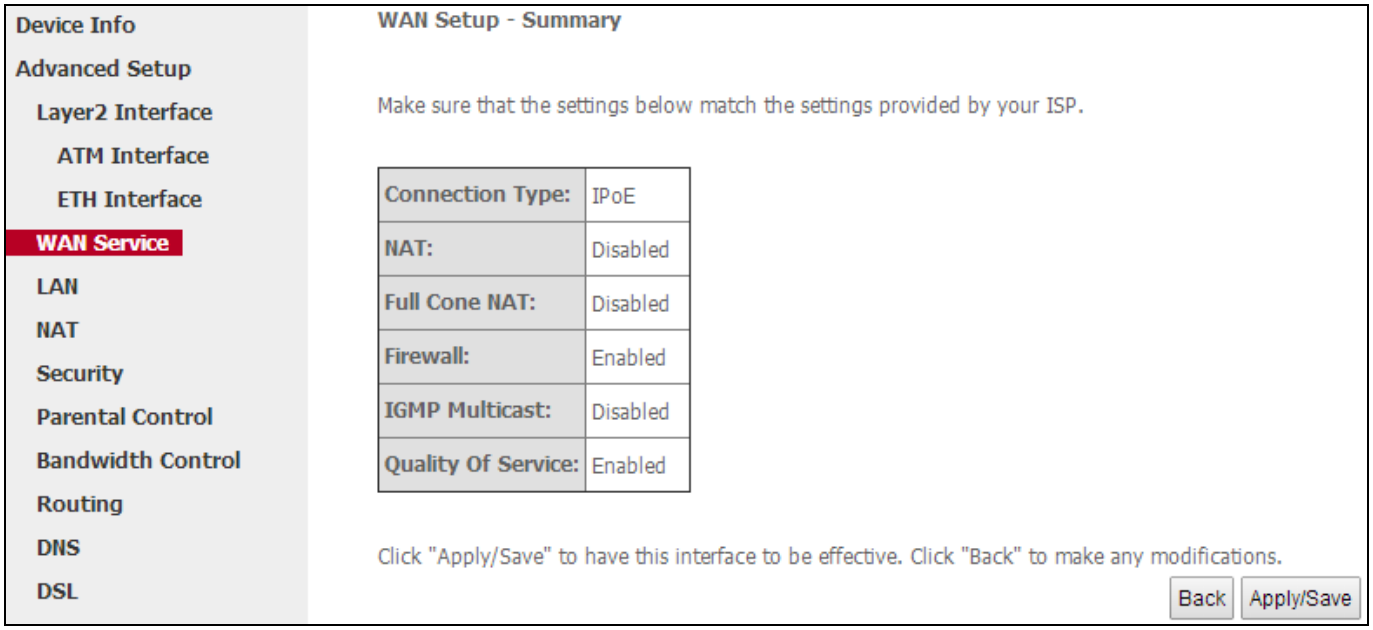
❻ To configure the Default Gateway interface when using IPv6, select the interface that you want to configure with the WAN gateway address in **Selected WAN Interface** box. Then click **Next**.



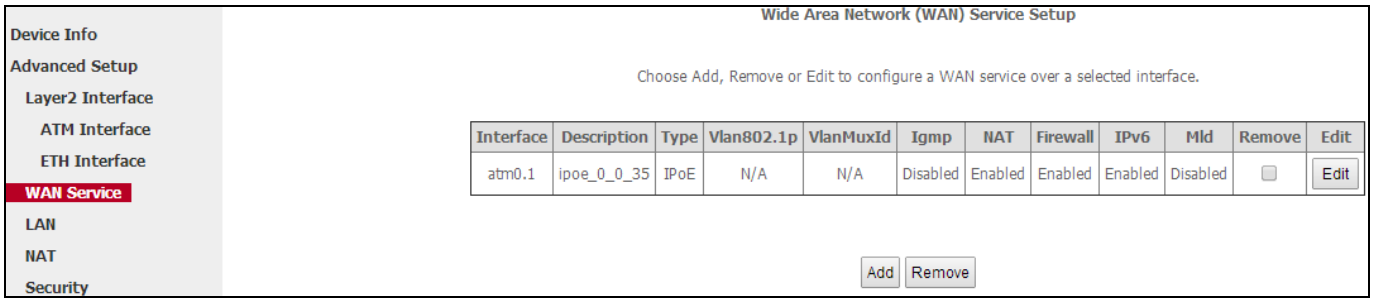
❼ To configure the WAN DNS address, check the **Obtain IPv6 DNS info from a WAN interface** option, or select the **Use the following Static IPv6 DNS address** option to enter the static DNS server IPv6 addresses provided by your ISP. At last, click **Next**.



Click **Apply/Save** to save your settings if everything is correctly set.



Here you can view your configurations. When the IPoE connection is successful, you can access the Internet.



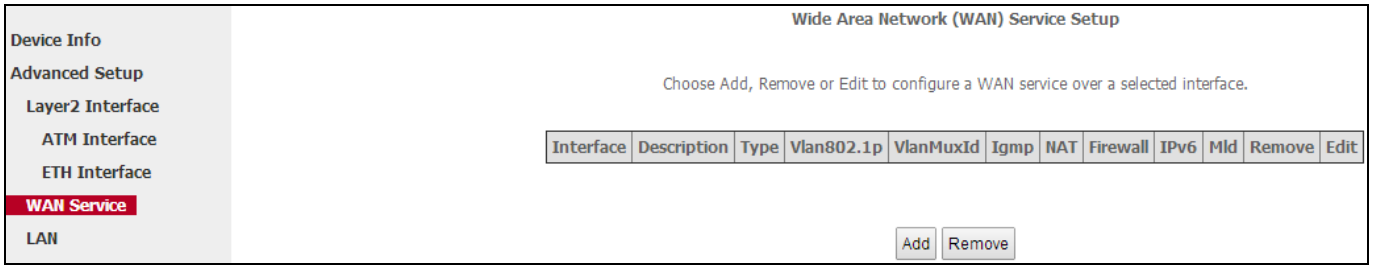
↗ Steps 1~7 above for **IPoE and IPv6 Only** Users

7) Bridging

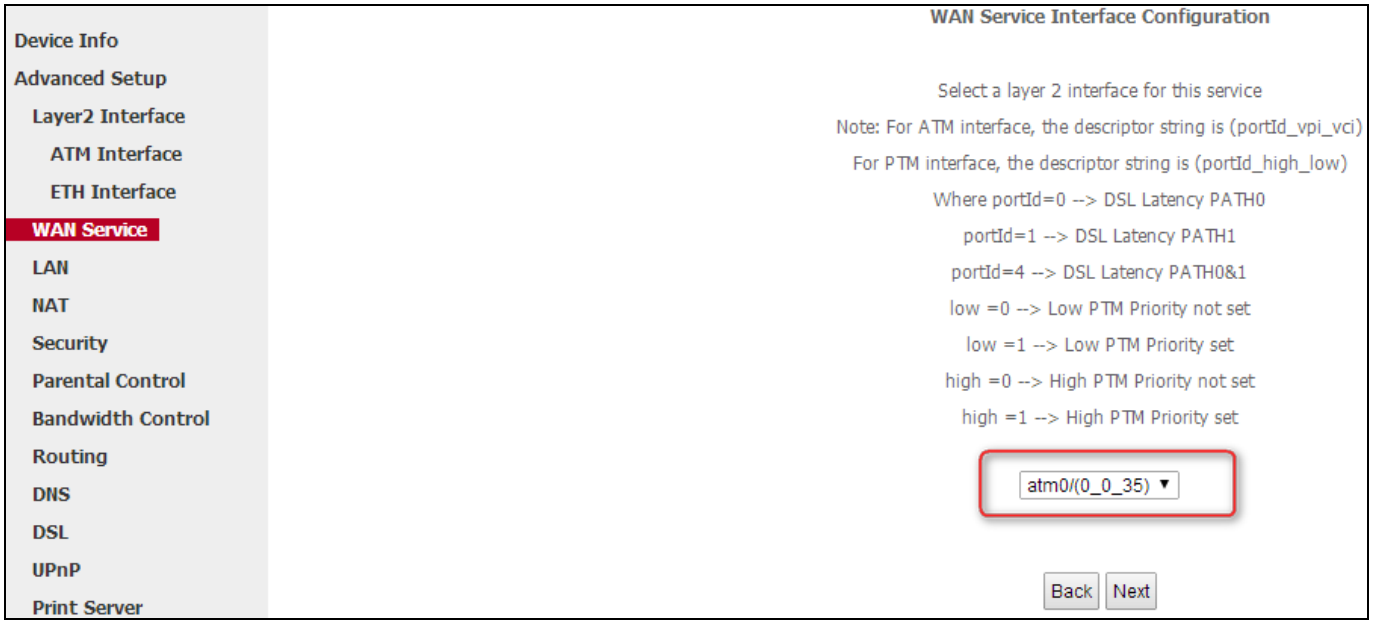
If you wish to initiate a dialup directly from your PC for Internet access or enjoy the entire Internet connection (instead of sharing it with others), you can use the Bridging DSL link type and create a dialup program on your PC.

After you configure the **ATM Interface** (ADSL uplink) and select **EoA** as the DSL link type, you can start to set up WAN service for accessing the Internet.

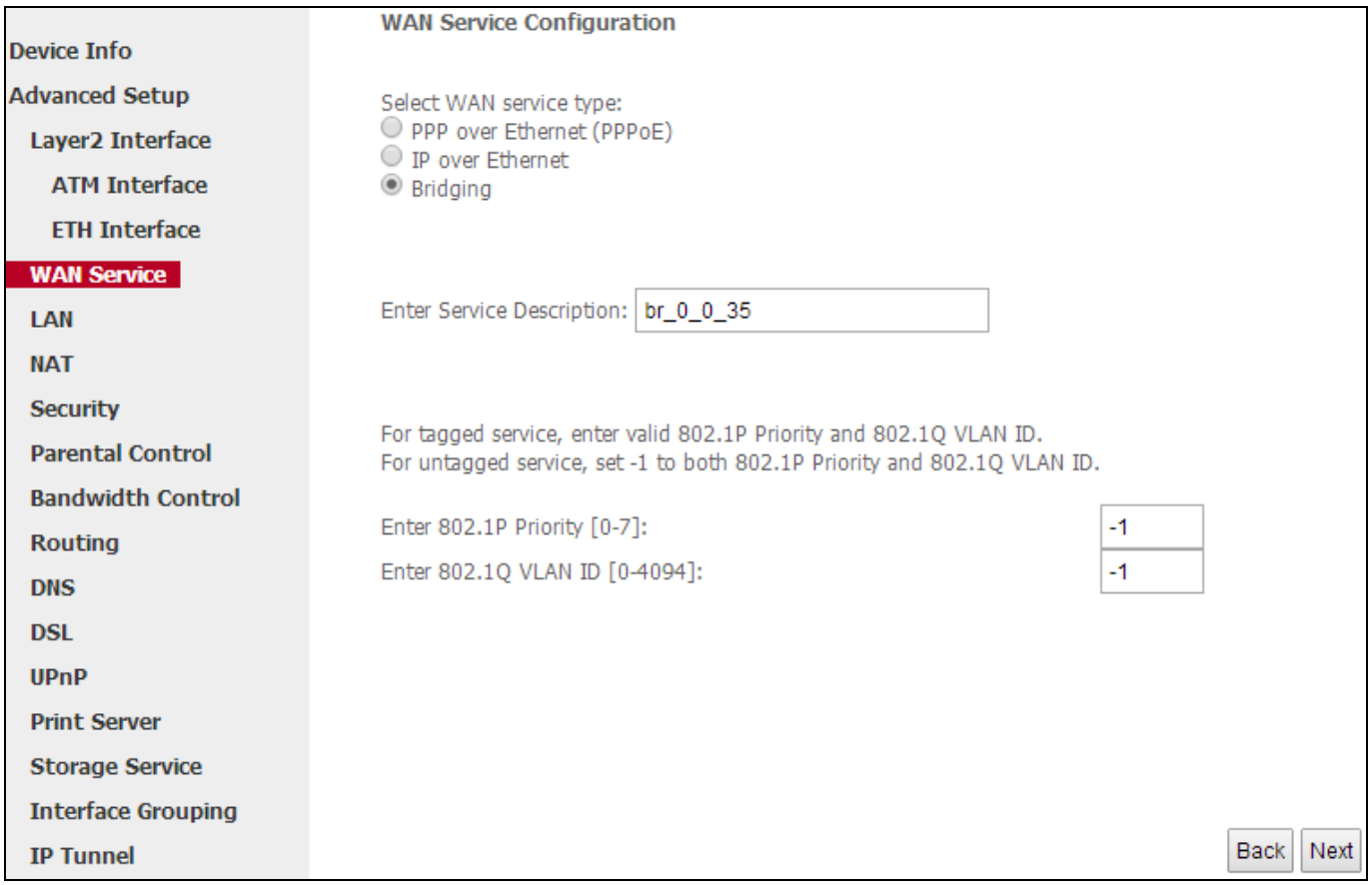
❶ Click **Advanced Setup** > **WAN Service** and then click the **Add** button.



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

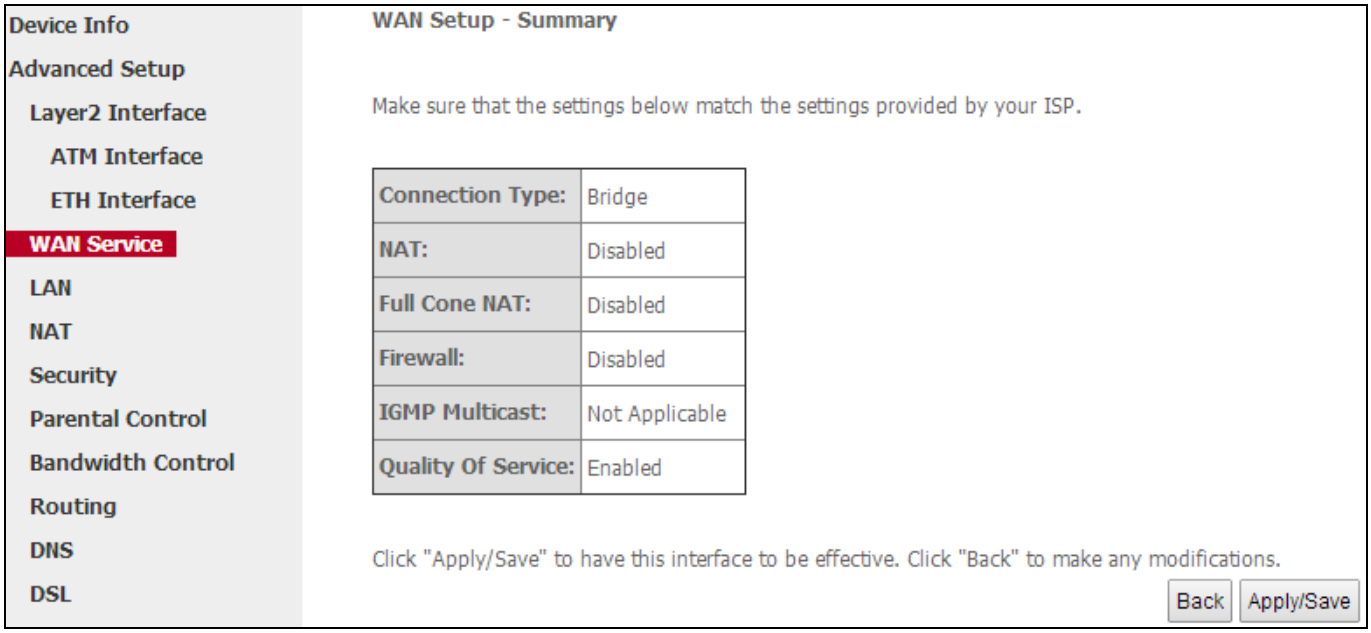


❸ Select **Bridging**. Edit the **Enter Service Description** field which is optional. Suggest you keep the default. Click **Next.**

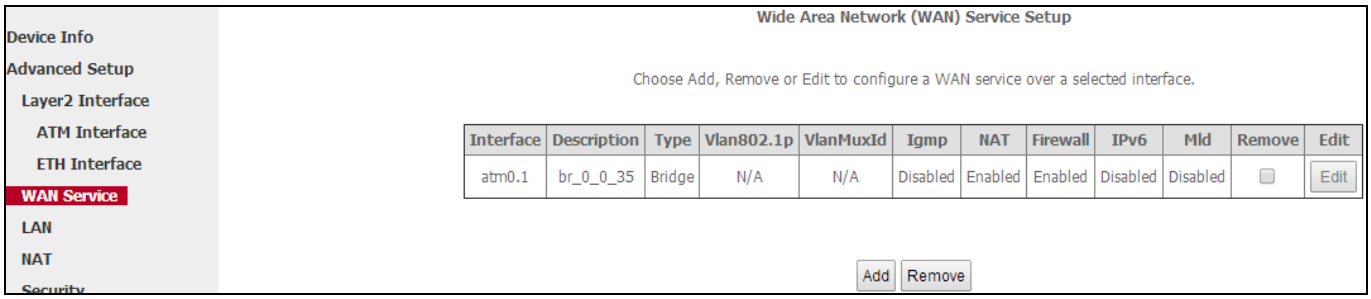


⇩

Click **Apply/Save** to save your settings if everything is correctly set.



Here you can view your configurations. When the Bridge connection is successful, you can access the Internet.

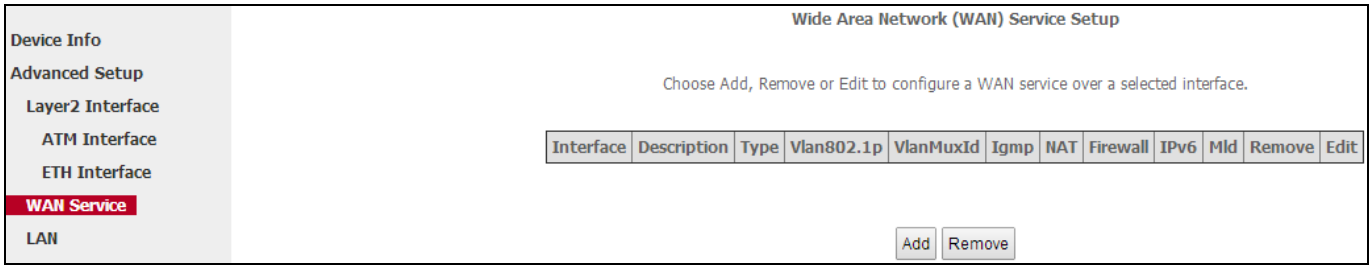


↗ Steps 1~3 above for **Bridging** Users

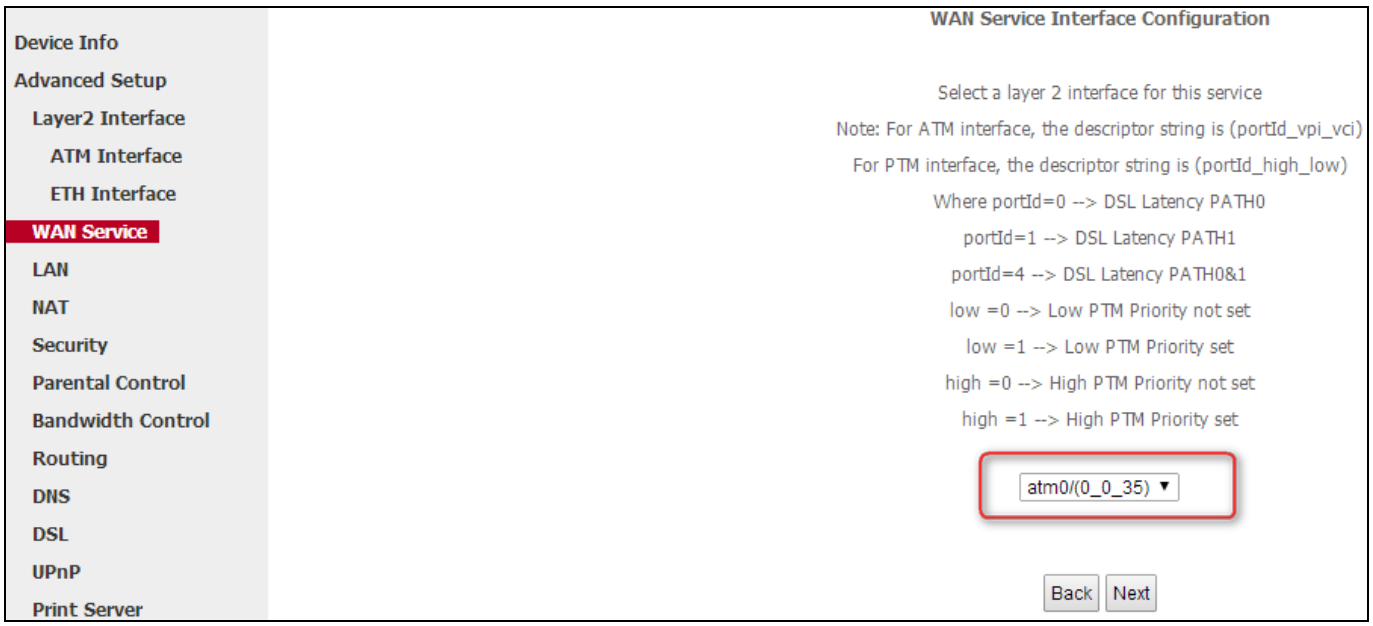
8) PPPoA IPv4 Only Users

After you configure the **ATM Interface** (ADSL uplink) and select **PPPoA** as the DSL link type, you can start to set up WAN service for accessing the Internet.

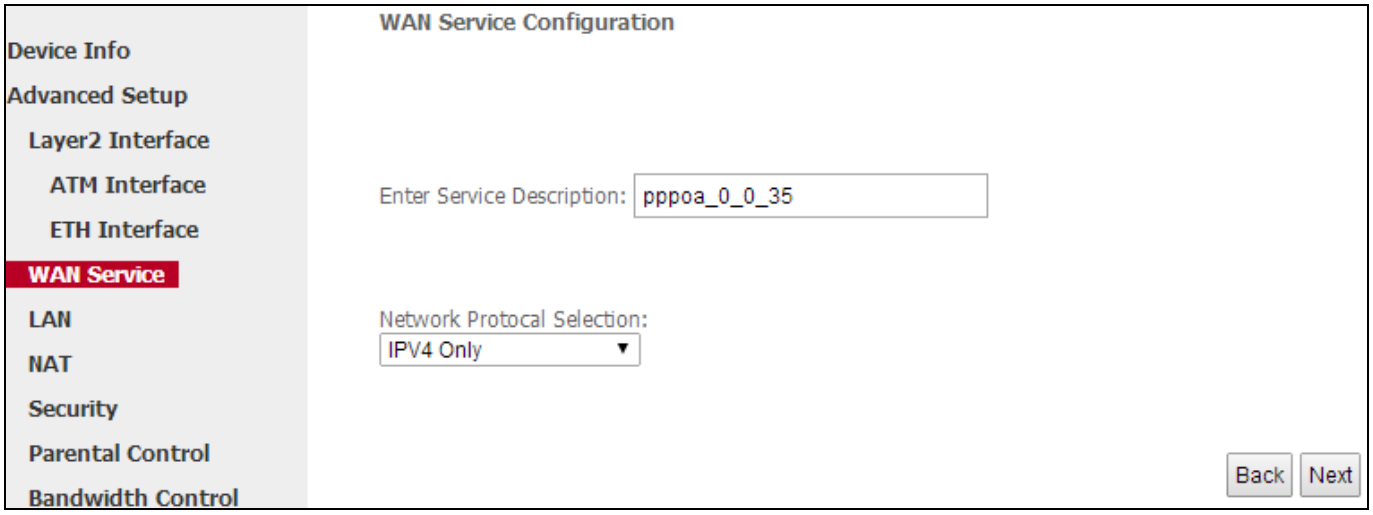
❶ Click **Advanced Setup > WAN Service** and then click the **Add** button.



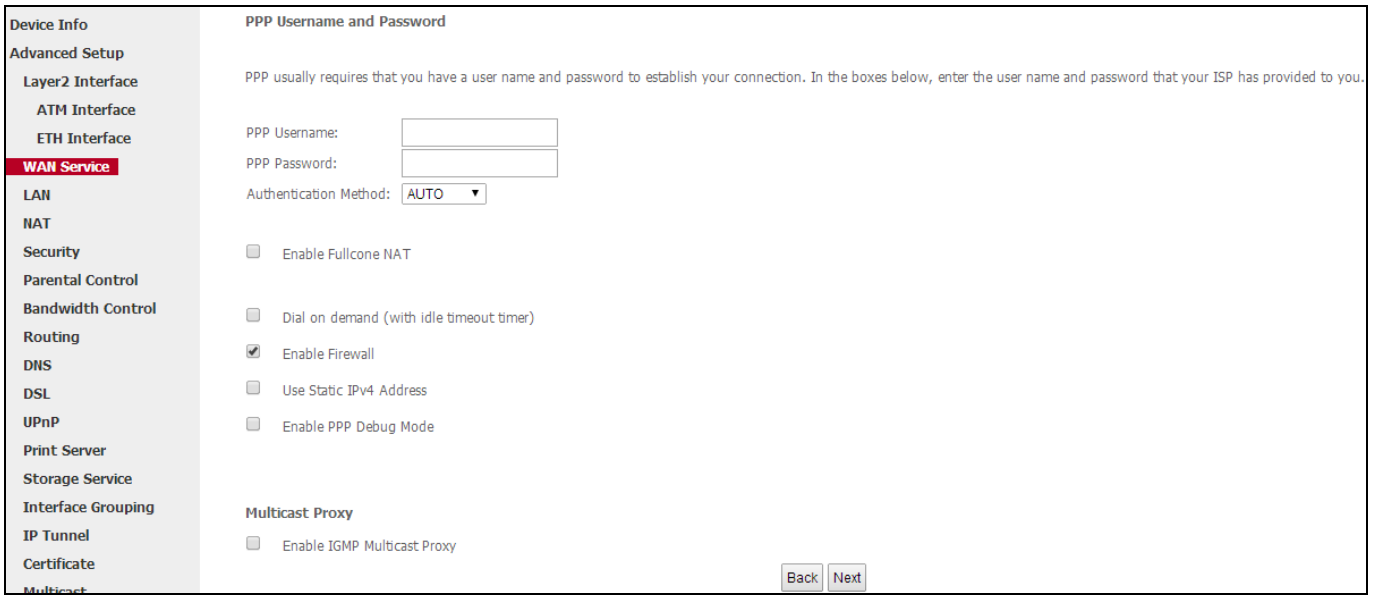
❷ Select the ATM interface you added just now from the pull-down menu in the figure below. Click **Next**.



❸ Edit the **Enter Service Description** field which is optional. Suggest you keep the default. Select a network protocol you need: **IPv4 Only**. Click **Next.**

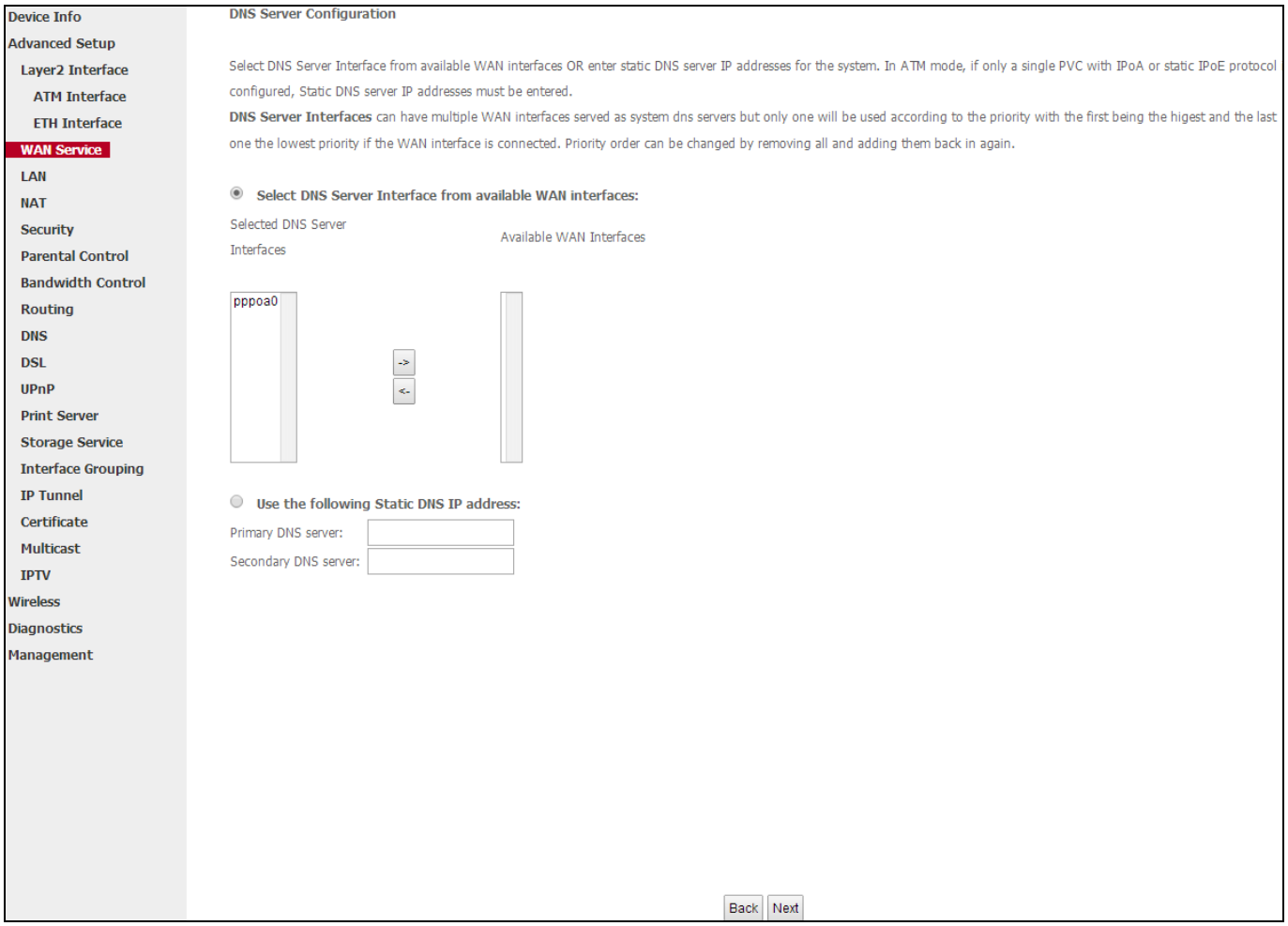


❹ Set PPP Username and Password on the figure below. Suggest keeping other options default. Click **Next**.

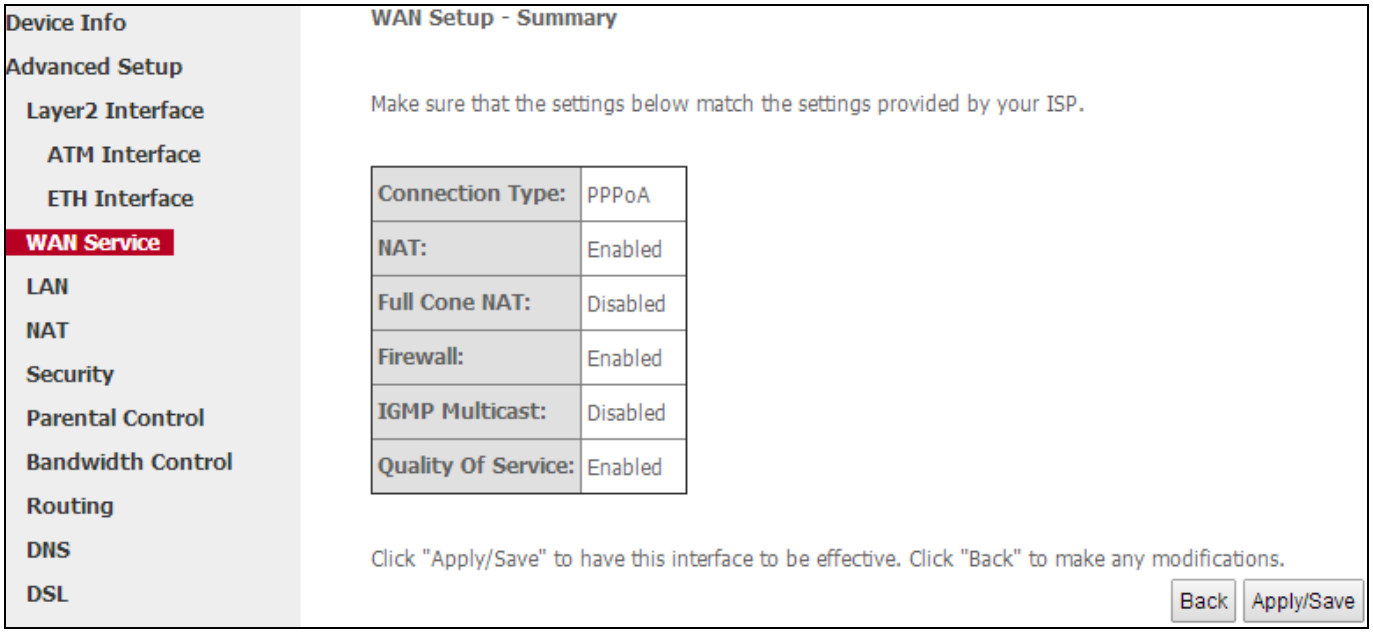


❺ To configure the Default Gateway interface, select the interface that you want to configure with the WAN gateway address in **Available Routed WAN Interfaces** box and move it into **Selected Default Gateway Interfaces** box. The default setting is recommended. Then click **Next**.

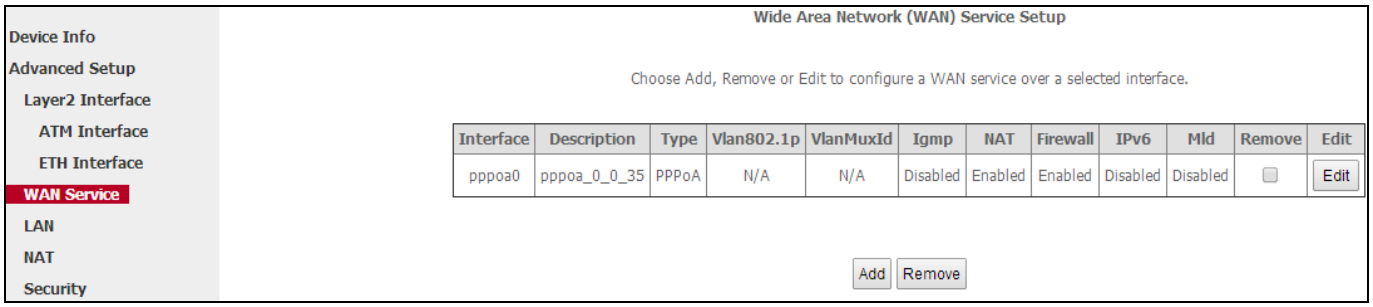
❻ To configure the WAN DNS address, click the **Select DNS Server Interface from available WAN interfaces** option, or select the **Use the following Static DNS IP address** option and enter the static DNS server IP addresses provided by your ISP. At last, click **Next**.



Click **Apply/Save** to save your settings if everything is correctly set.



Here you can view your configurations. When the PPPoA connection is successful, you can access the Internet.

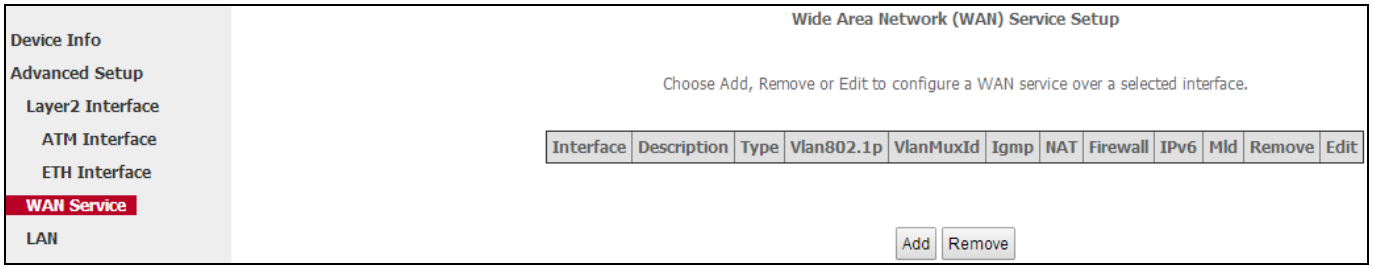


↗ Steps 1~6 above for **PPPoA and IPv4 Only** Users

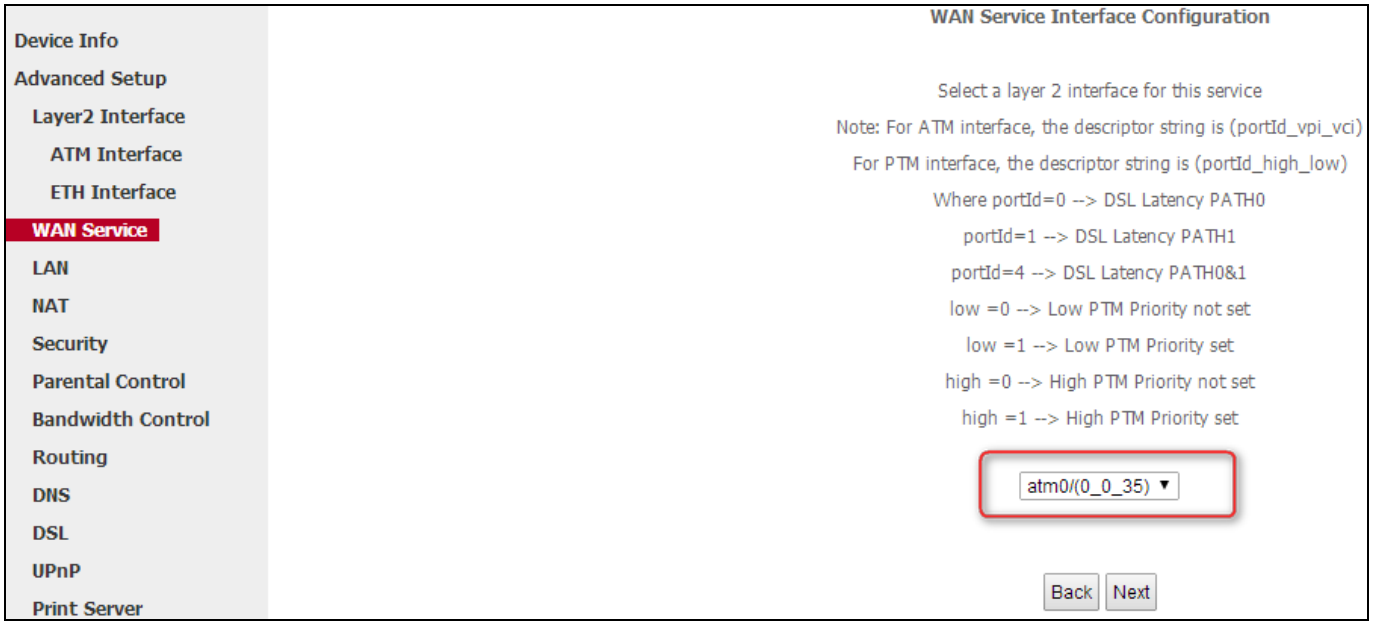
9) PPPoA IPv4&IPv6 (Dual Stack) Users

After you configure the **ATM Interface** (ADSL uplink) and select **PPPoA** as the DSL link type, you can start to set up WAN service for accessing the Internet.

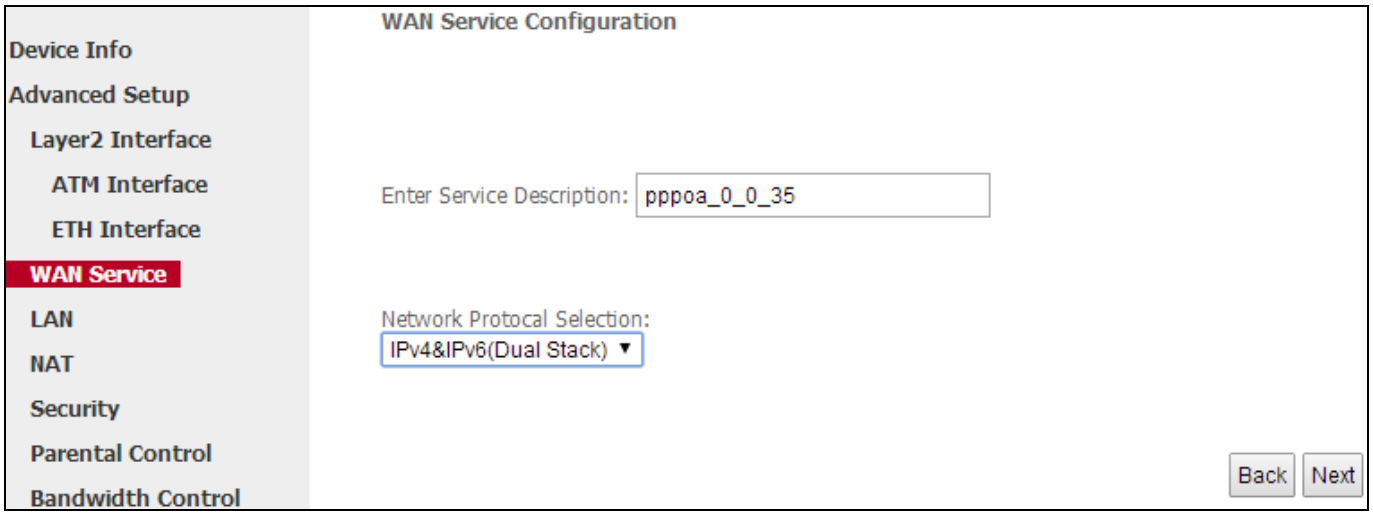
❶ Click **Advanced Setup > WAN Service** and then click the **Add** button.



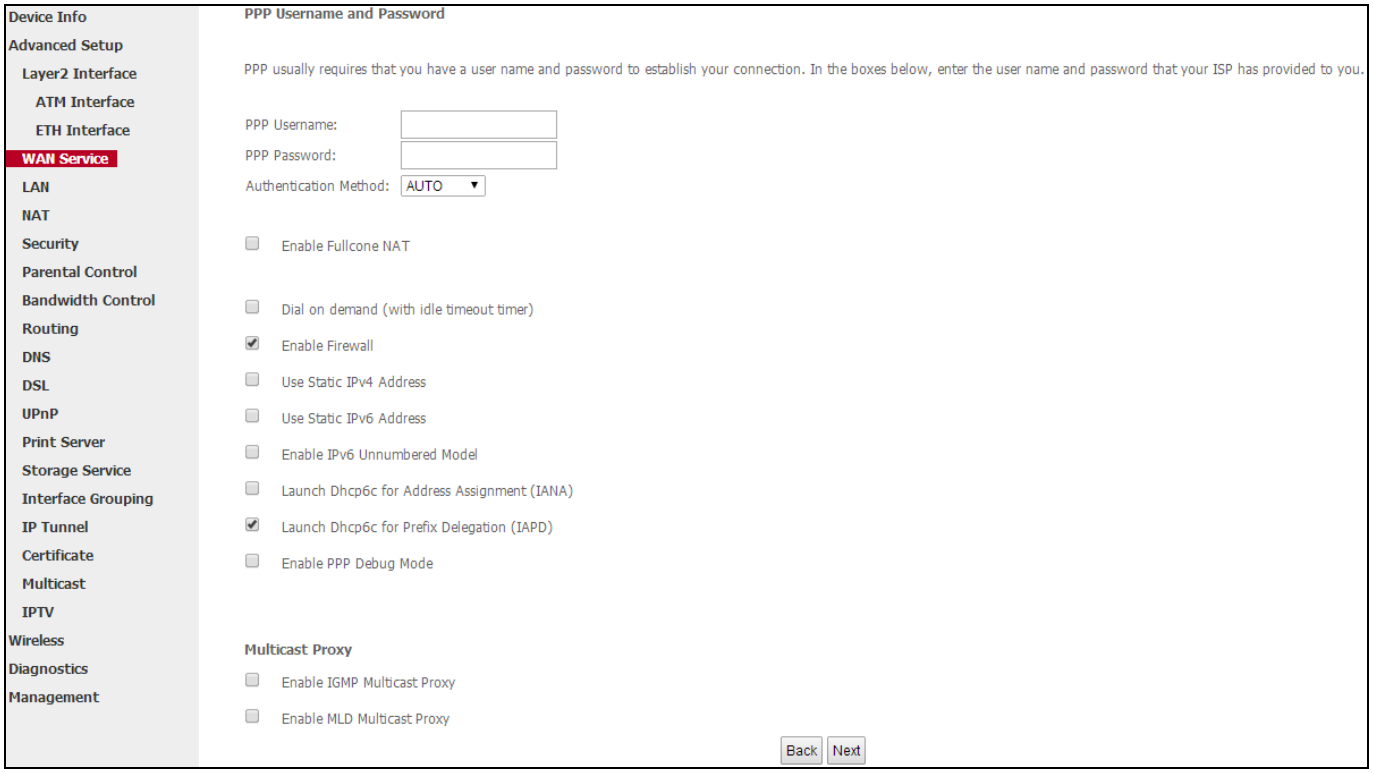
❷ Select the ATM interface you added just now from the pull-down menu in the figure below. Click **Next**.

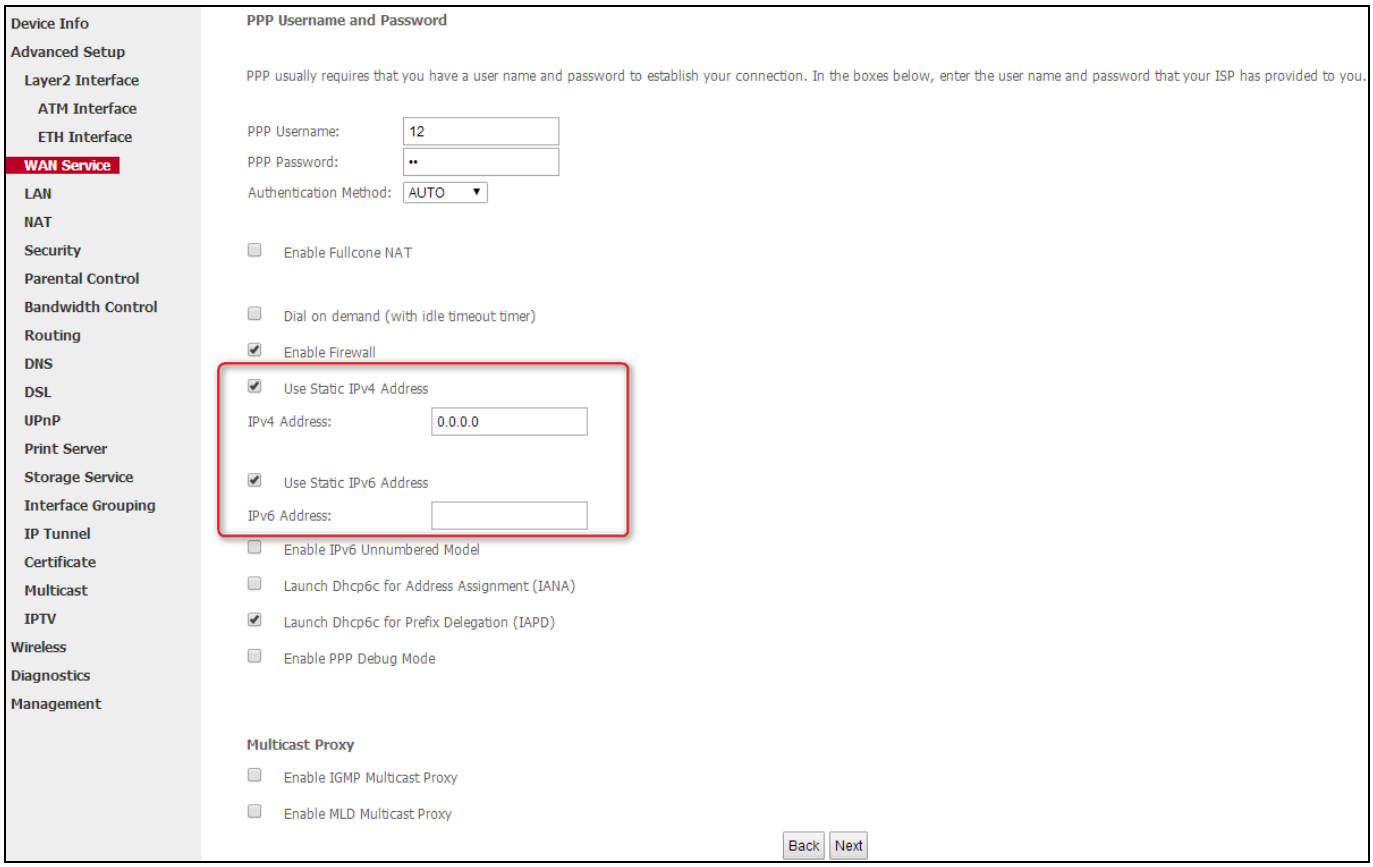


❸ Edit the **Enter Service Description** which is optional. Suggest you keep the default. Select a network protocol you need: **IPv4&IPv6 (Dual Stack)**. Click **Next**.

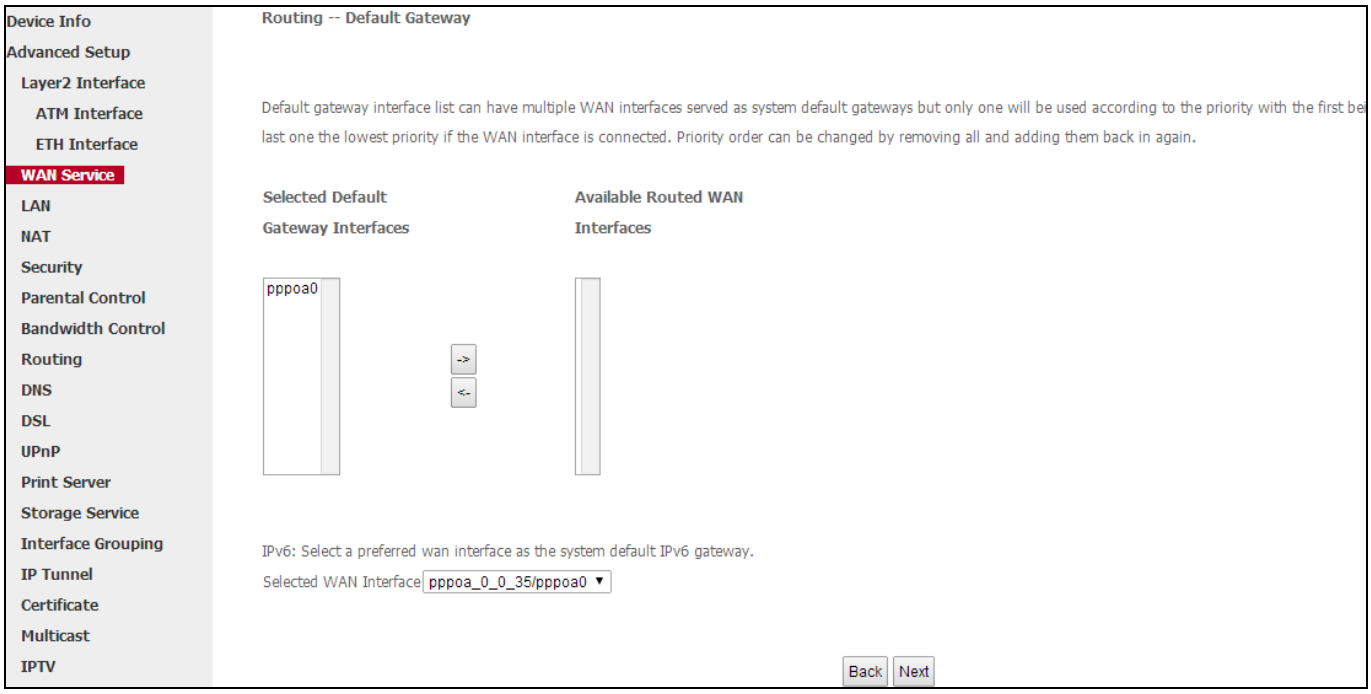


❹ Set PPP Username and Password on the figure below. Suggest keeping other options default. Click **Next**.

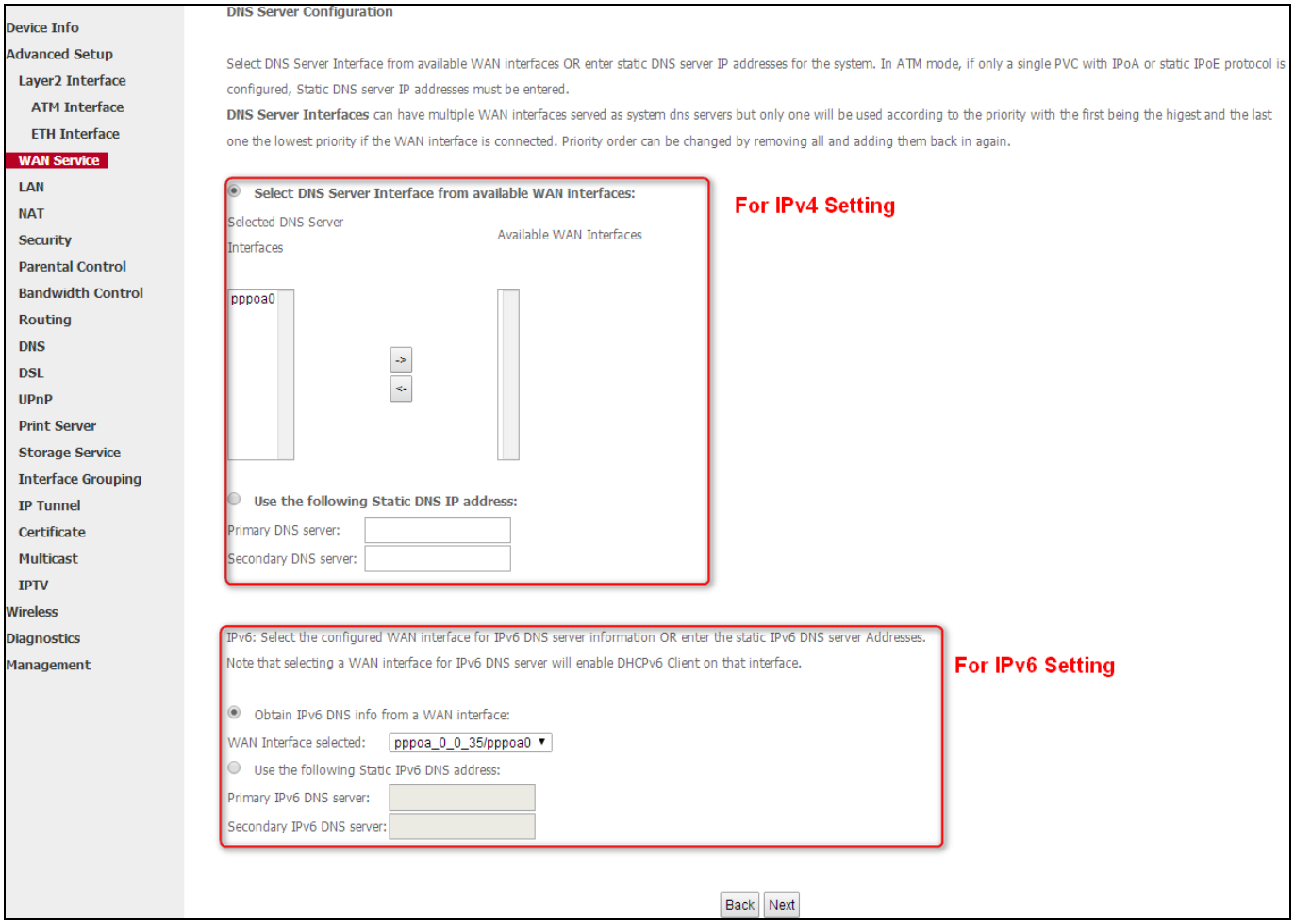




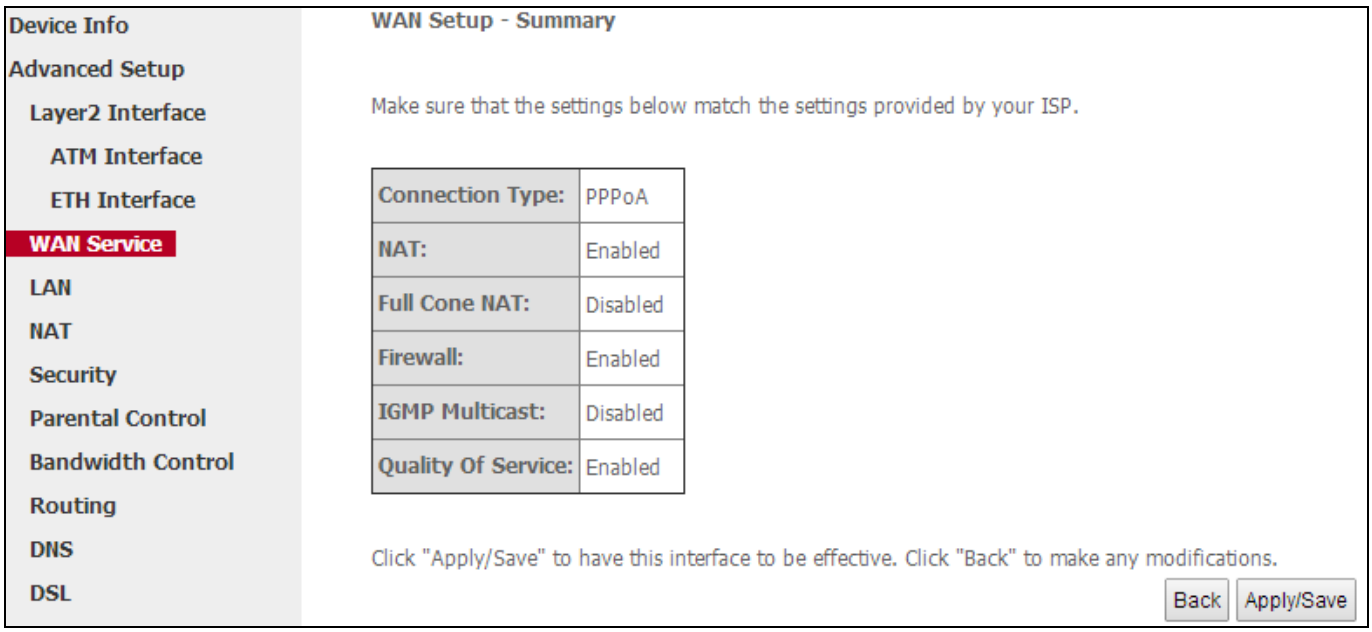
❺ To configure the Default Gateway interface, select the interface that you want to configure with the WAN gateway address. Then click **Next**.



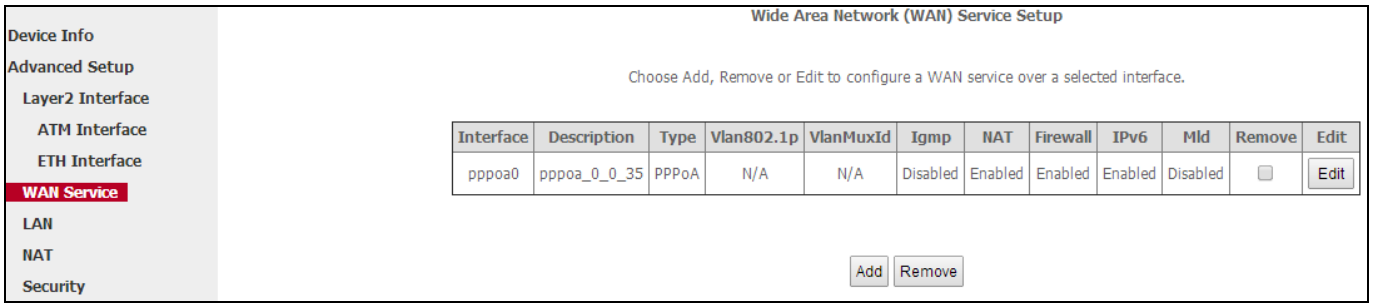
❻ To configure the WAN DNS address, finish both the IPv4 setting and IPv6 setting. Click **Next**.



Click **Apply/Save** to save your settings if everything is correctly set.



Here you can view your configurations. When the PPPoA connection is successful, you can access the Internet.

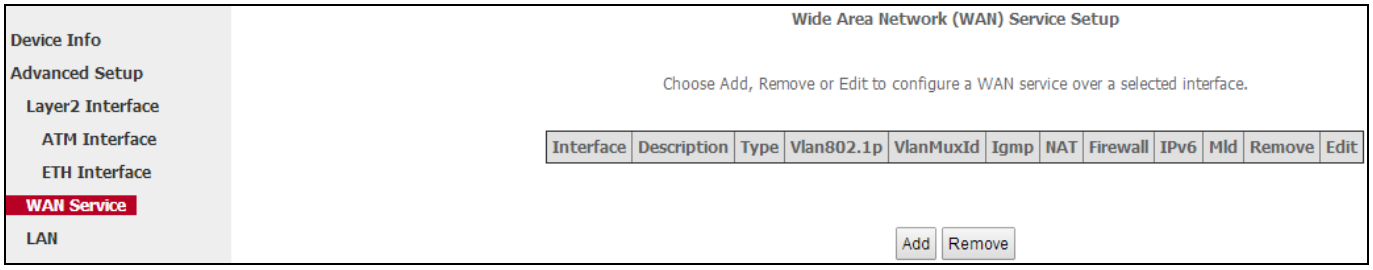


↗ Steps 1~6 above for **PPPoA and IPv4&IPv6 (Dual Stack)** Users

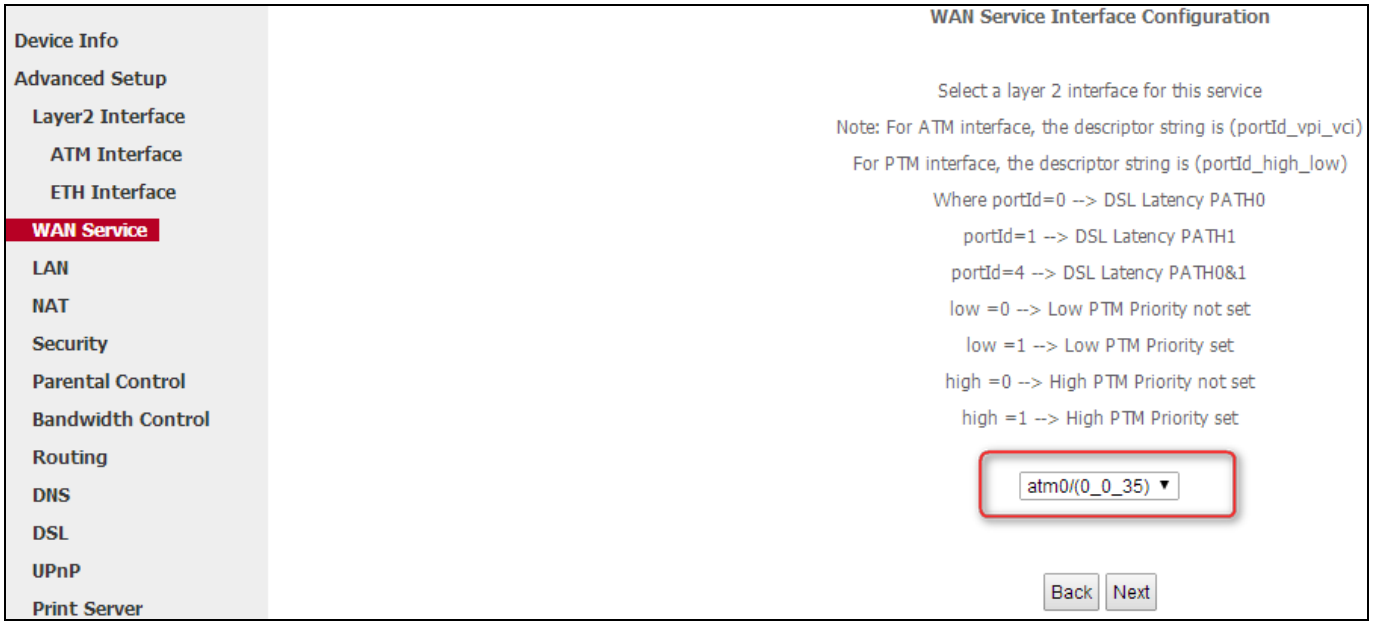
10) PPPoA IPv6 Only Users

After you configure the **ATM Interface** (ADSL uplink) and select **PPPoA** as the DSL link type, you can start to set up WAN service for accessing the Internet.

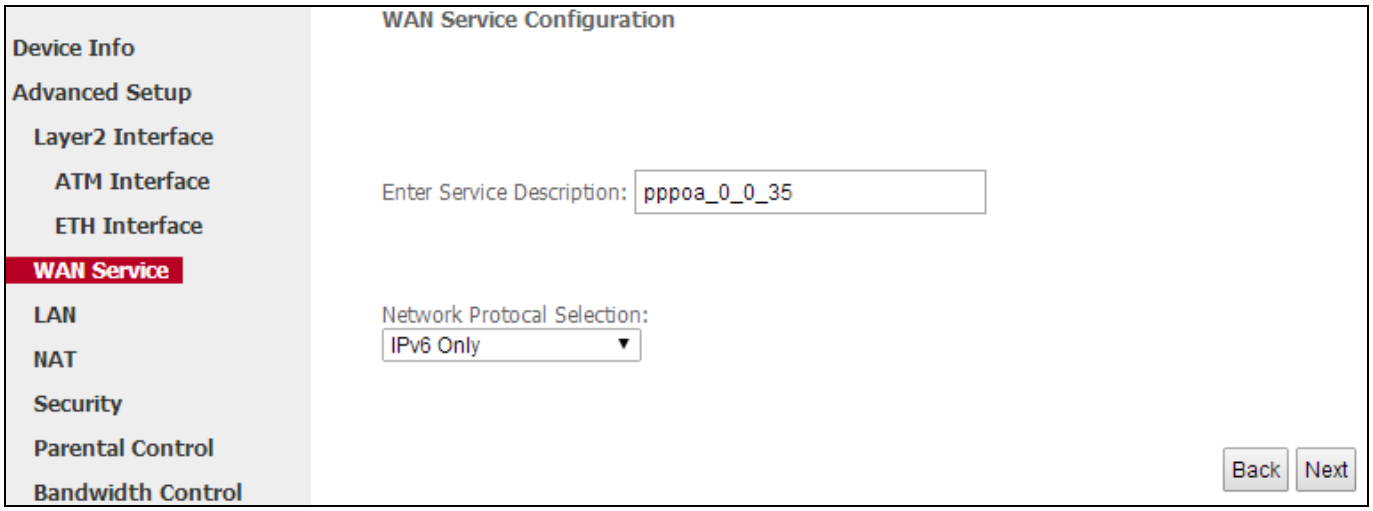
❶ Click **Advanced Setup > WAN Service** and then click the **Add** button.



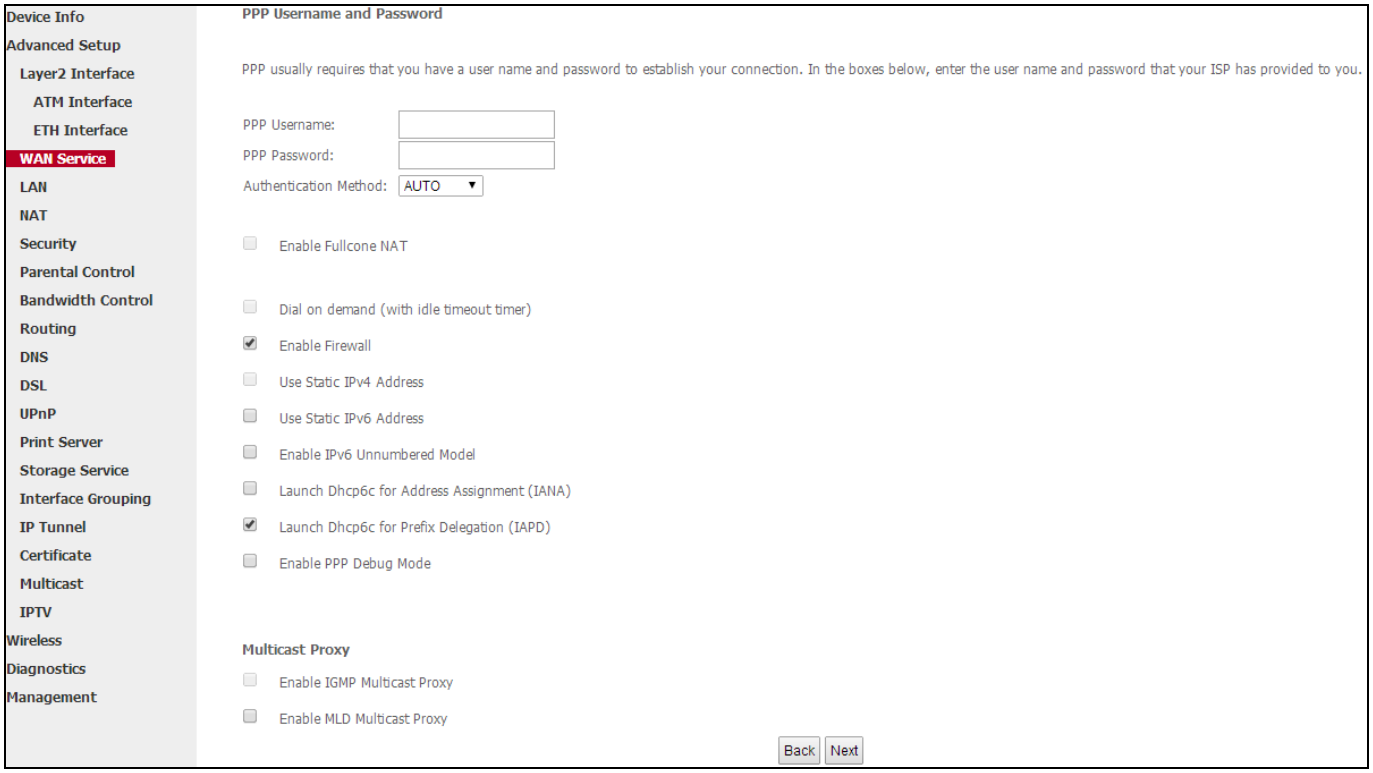
❷ Select the ATM interface you added just now from the pull-down menu in the figure below. Click **Next**.



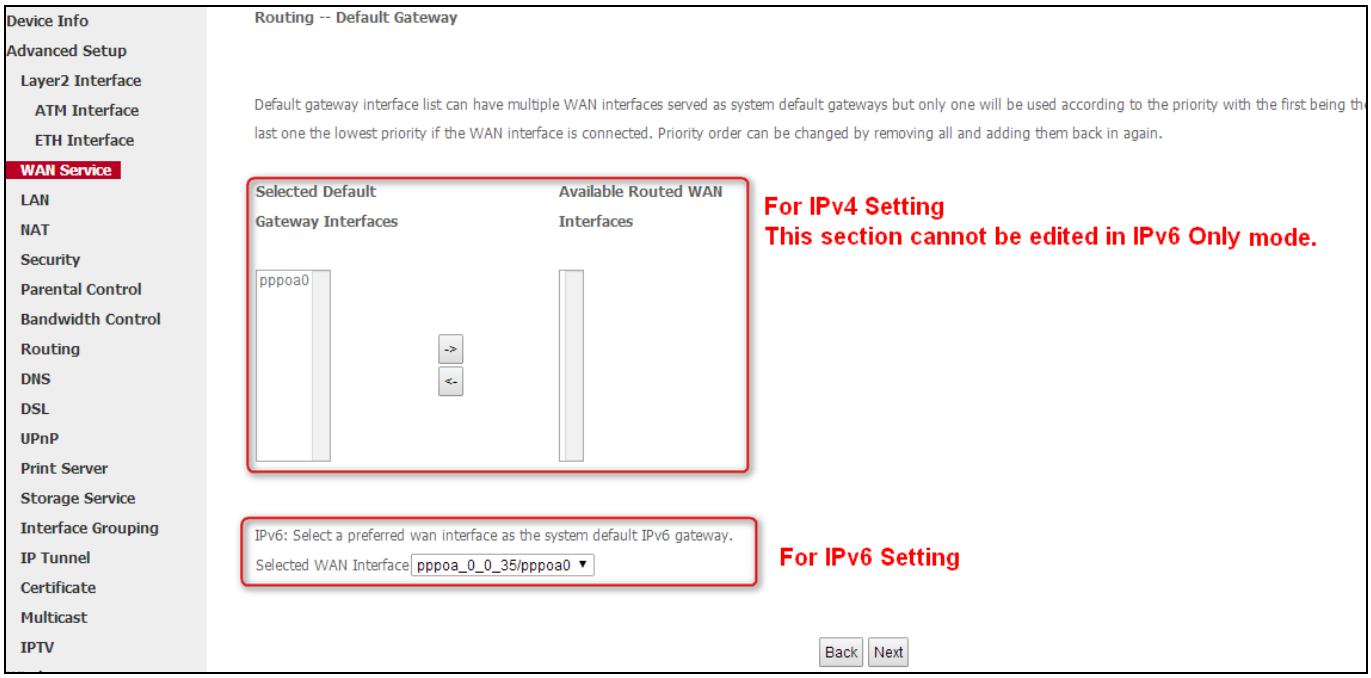
❸ Edit the **Enter Service Description** which is optional. Suggest you keep the default. Select a network protocol you need: **IPv6 Only**. Click **Next**.



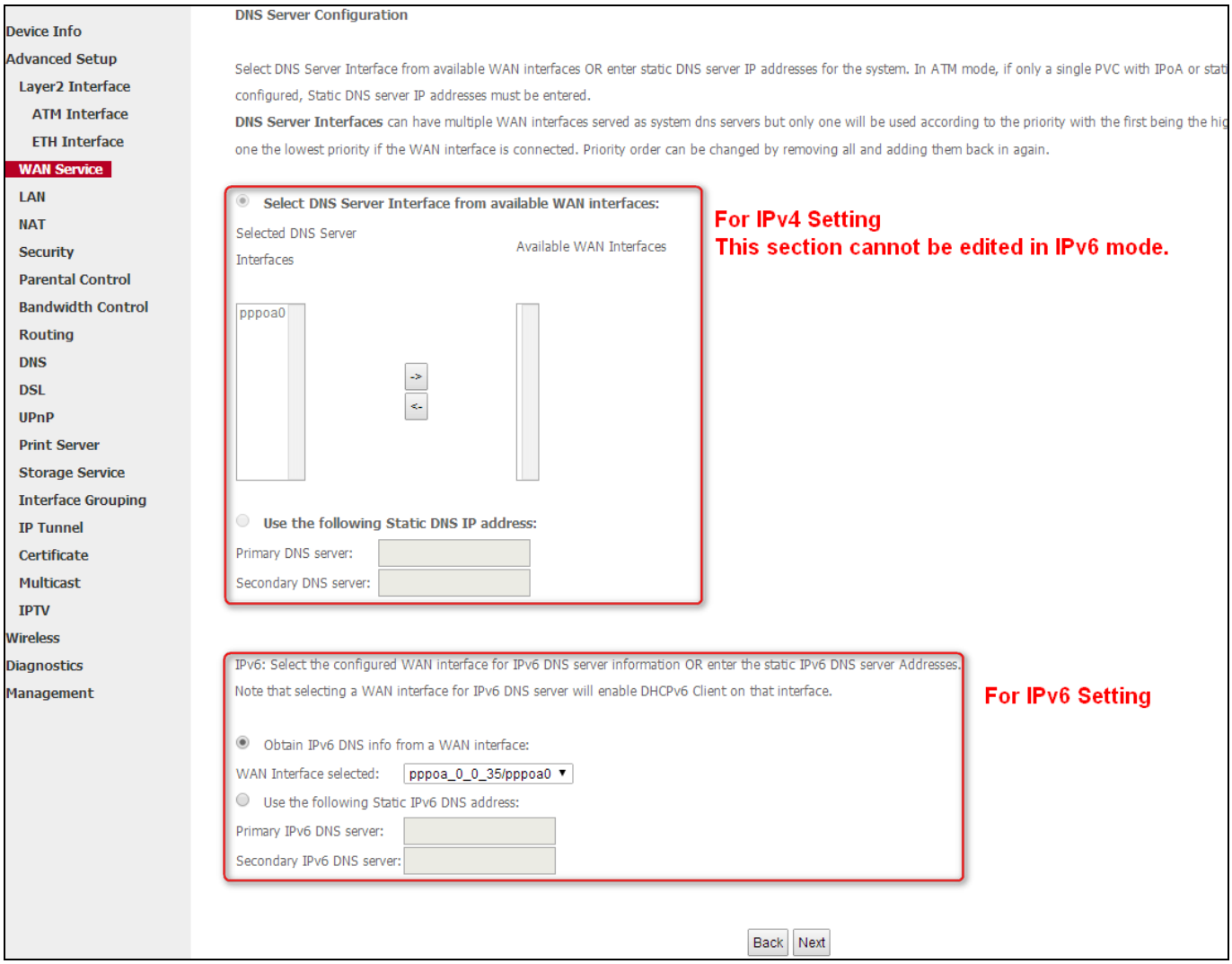
❹ Set PPP Username and Password on the figure below. Suggest keeping other options default. Click **Next**.



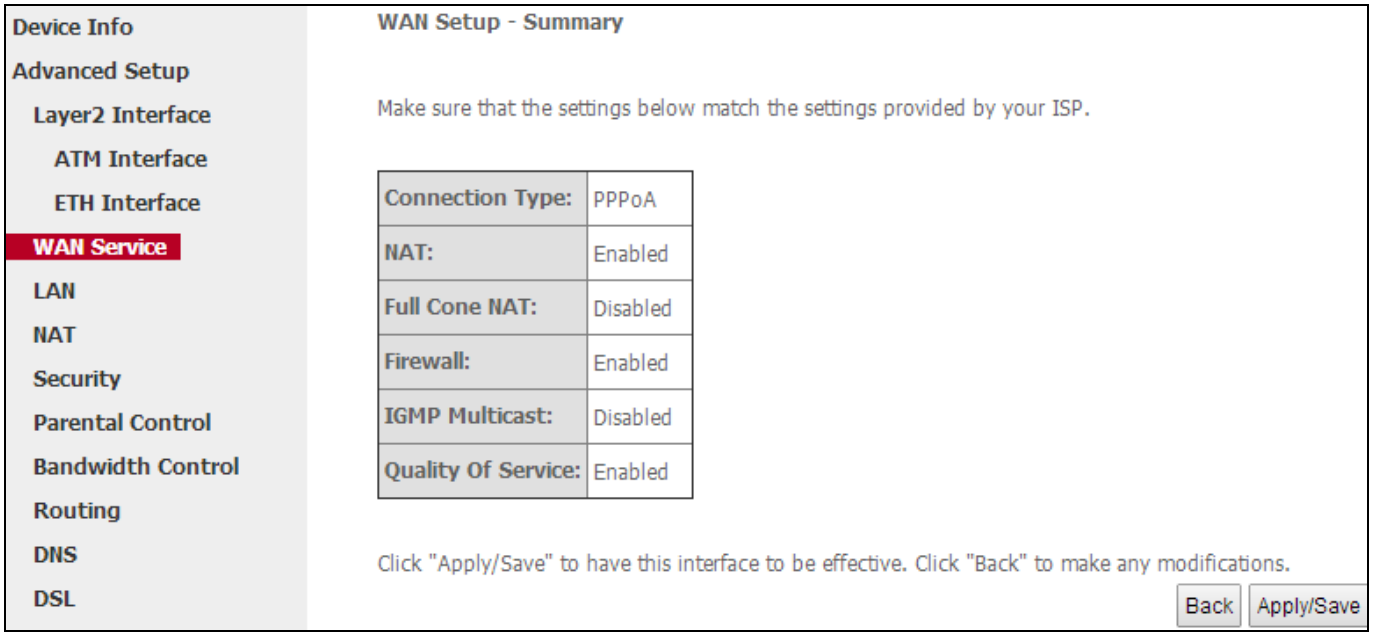
❺ To configure the Default Gateway interface, select the interface that you want to configure with the WAN gateway address. Then click **Next**.



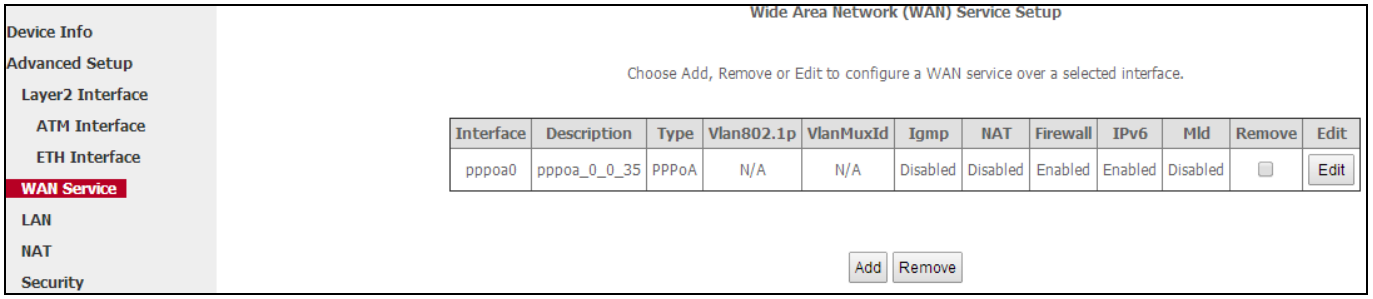
❻ To configure the WAN DNS address, finish both the IPv4 setting and IPv6 setting. Click **Next**.



Click **Apply/Save** to save your settings if everything is correctly set.



Here you can view your configurations. When the PPPoA connection is successful, you can access the Internet.

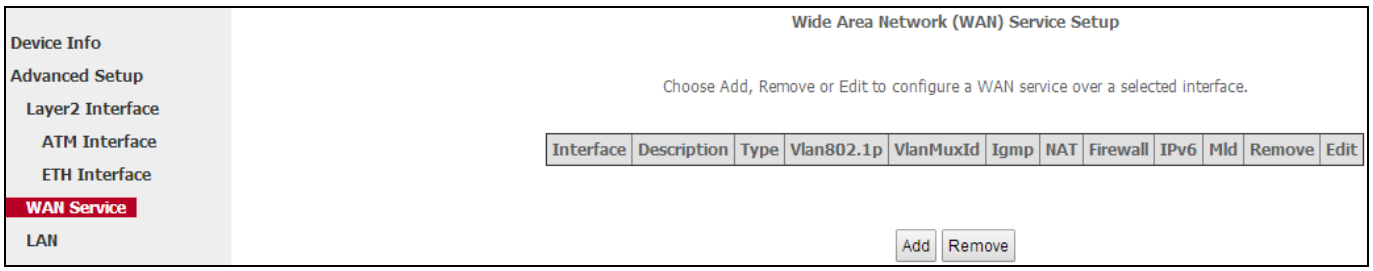


↗ Steps 1~6 above for **PPPoA and IPv6 Only** Users

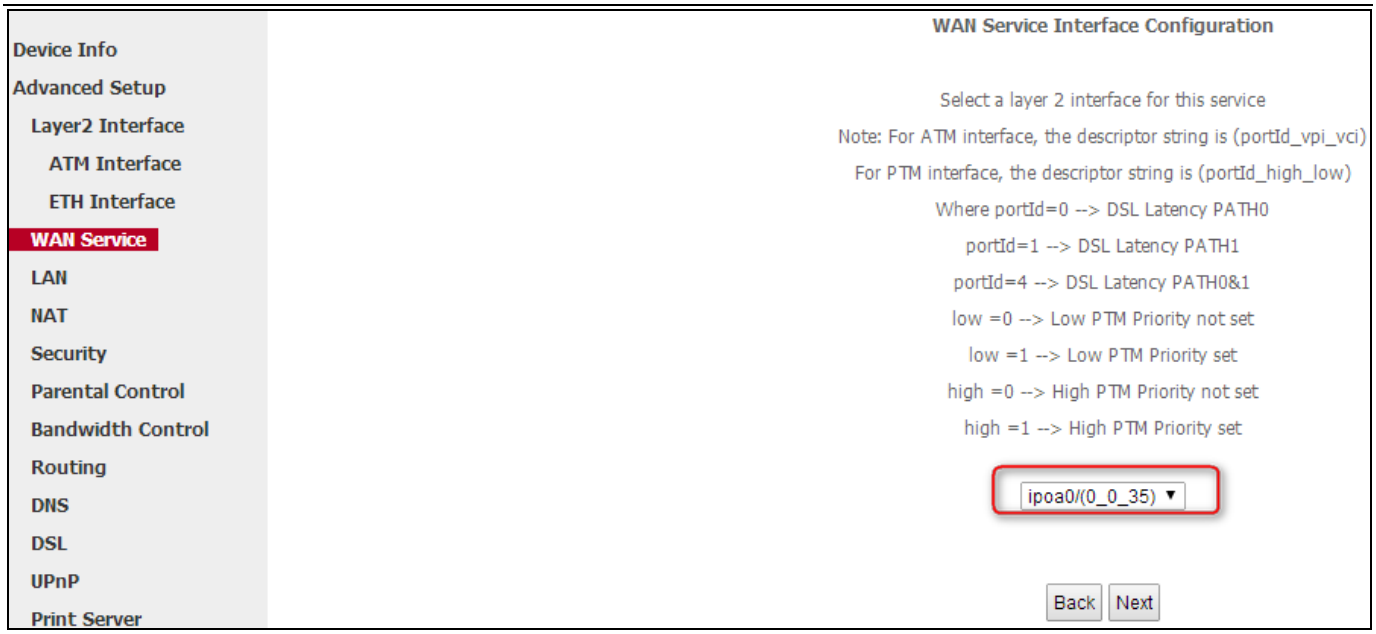
11) IPoA Users

After you configure the **ATM Interface** (ADSL uplink) and select **IPoA** as the DSL link type, you can start to set up WAN service for accessing the Internet.

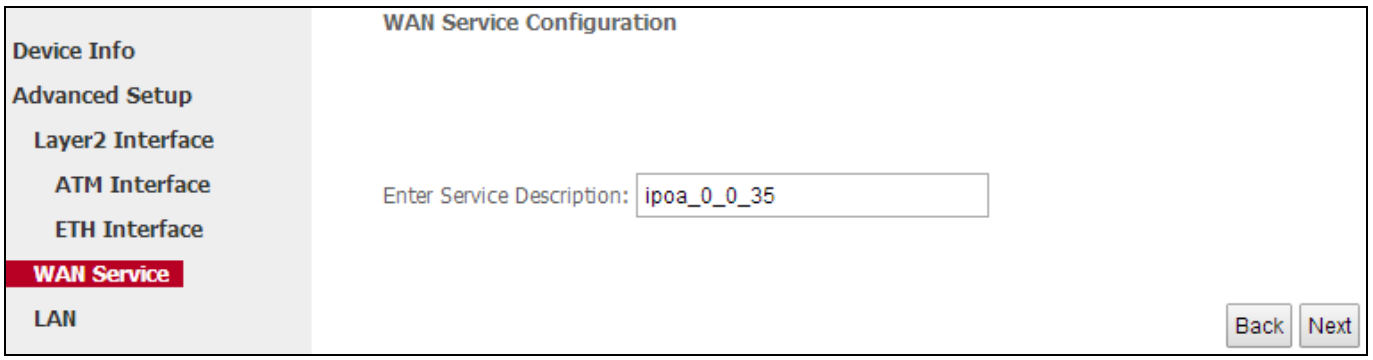
❶ Click **Advanced Setup** > **WAN Service** and then click the **Add** button.



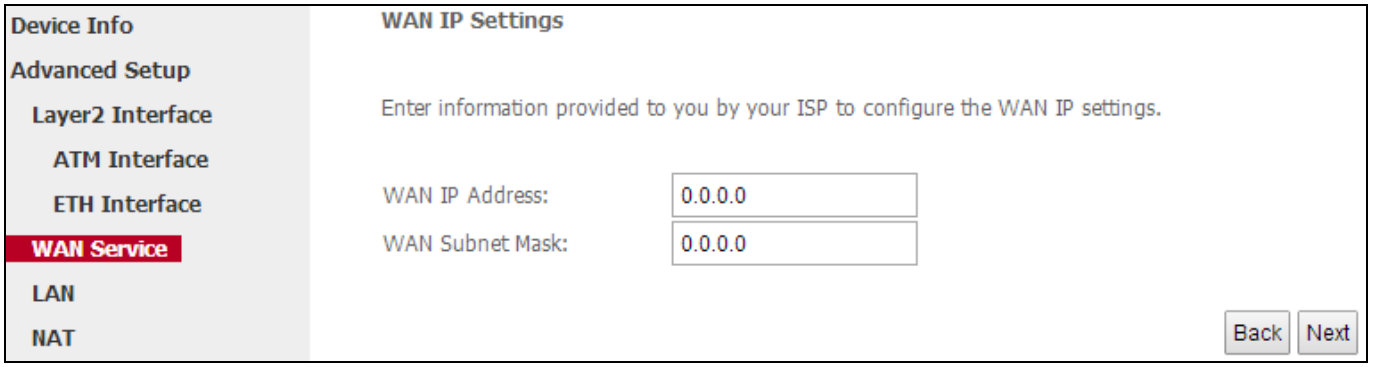
❷ Select the ATM interface you added just now from the pull-down menu in the figure below. Click **Next**.



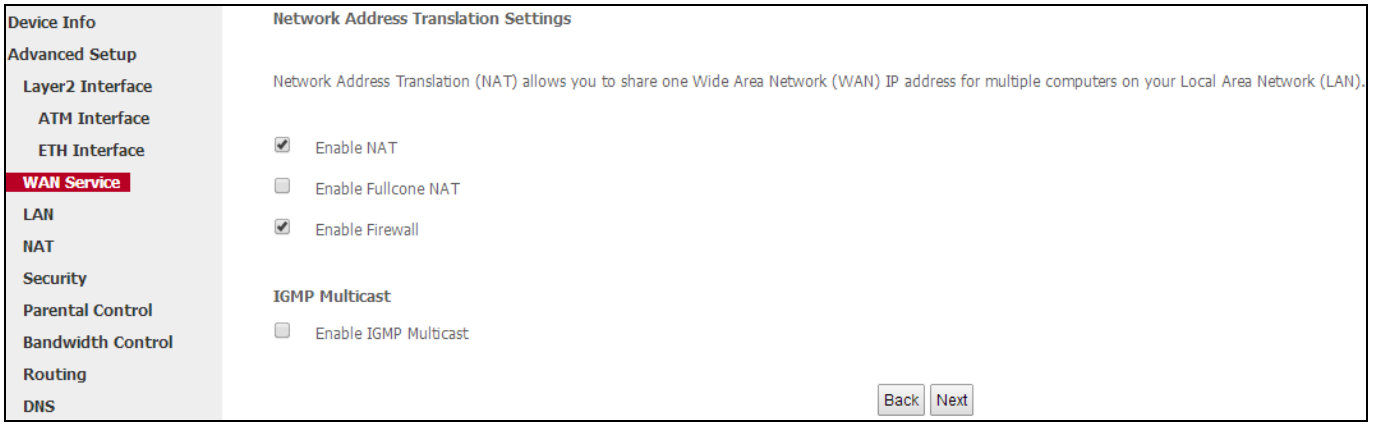
❸ Edit the **Enter Service Description**. This field is optional. Suggest to keep the default name. Click **Next.**



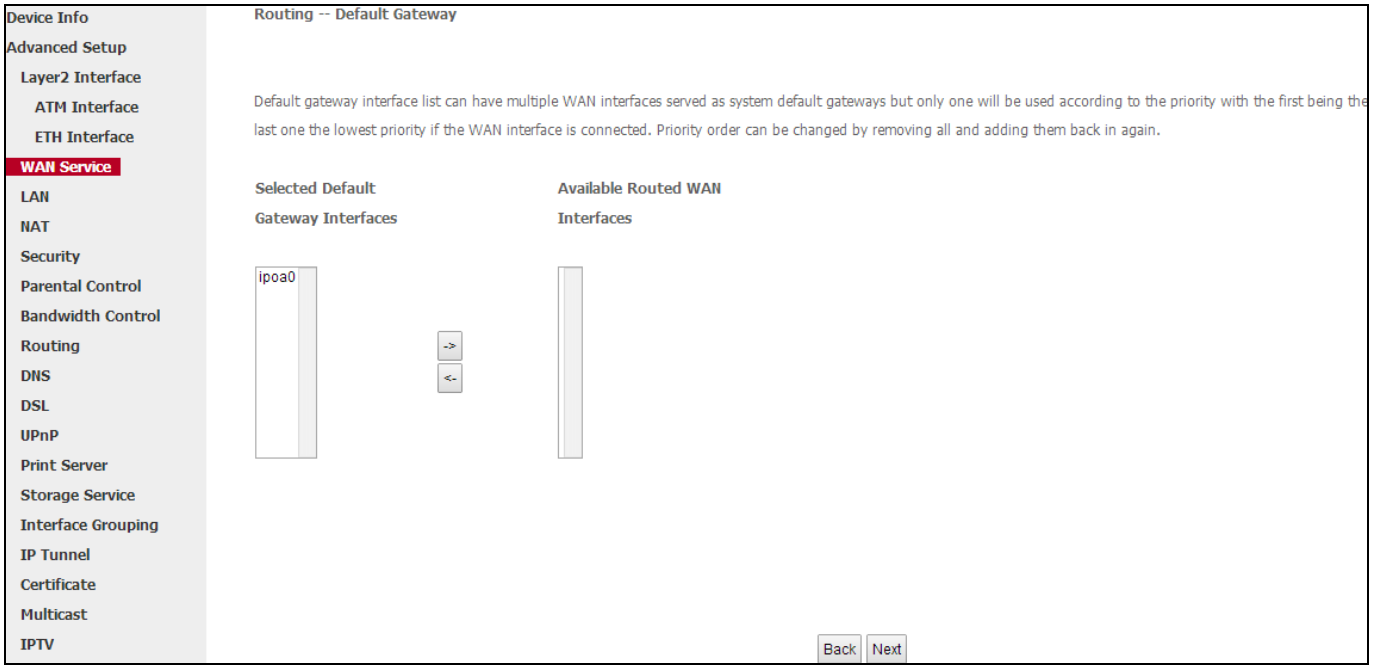
❹ Set the WAN IP address and subnet mask provided by your ISP.



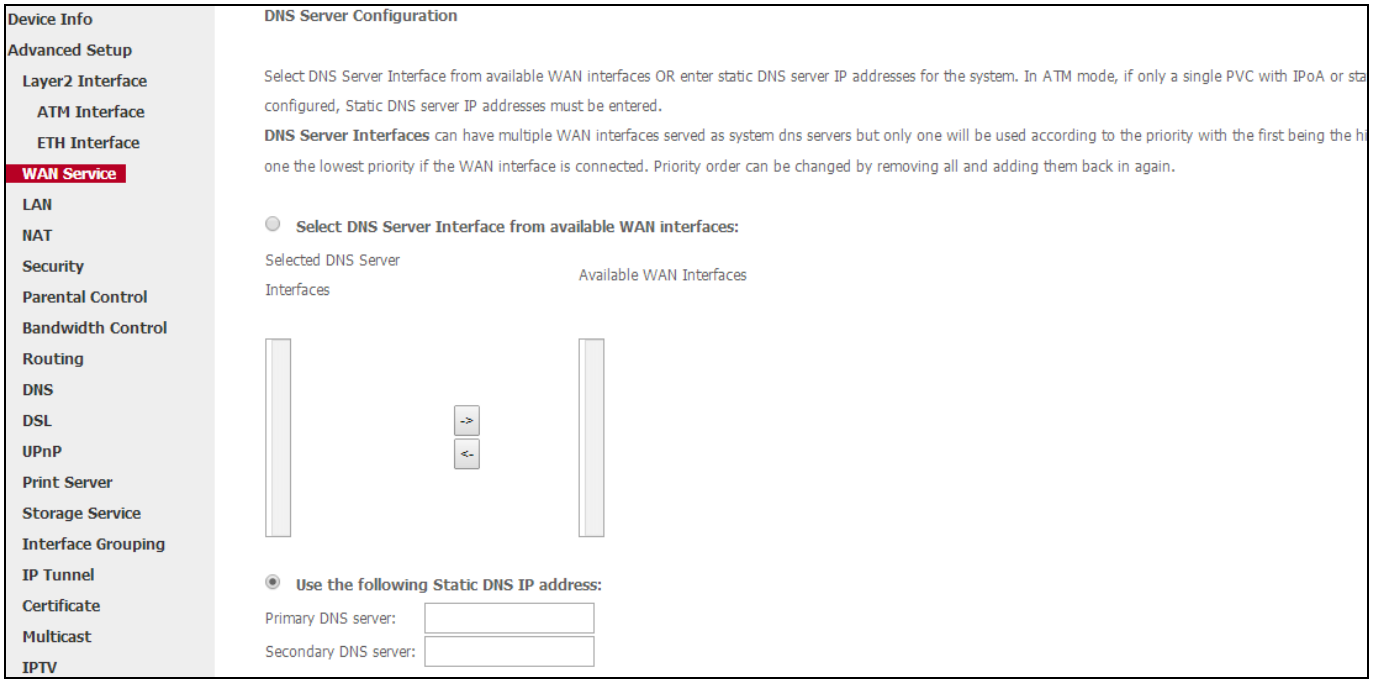
❺ Finish Network address translation settings. Suggest keeping the default settings if you're not sure how to set them. Click **Next**.



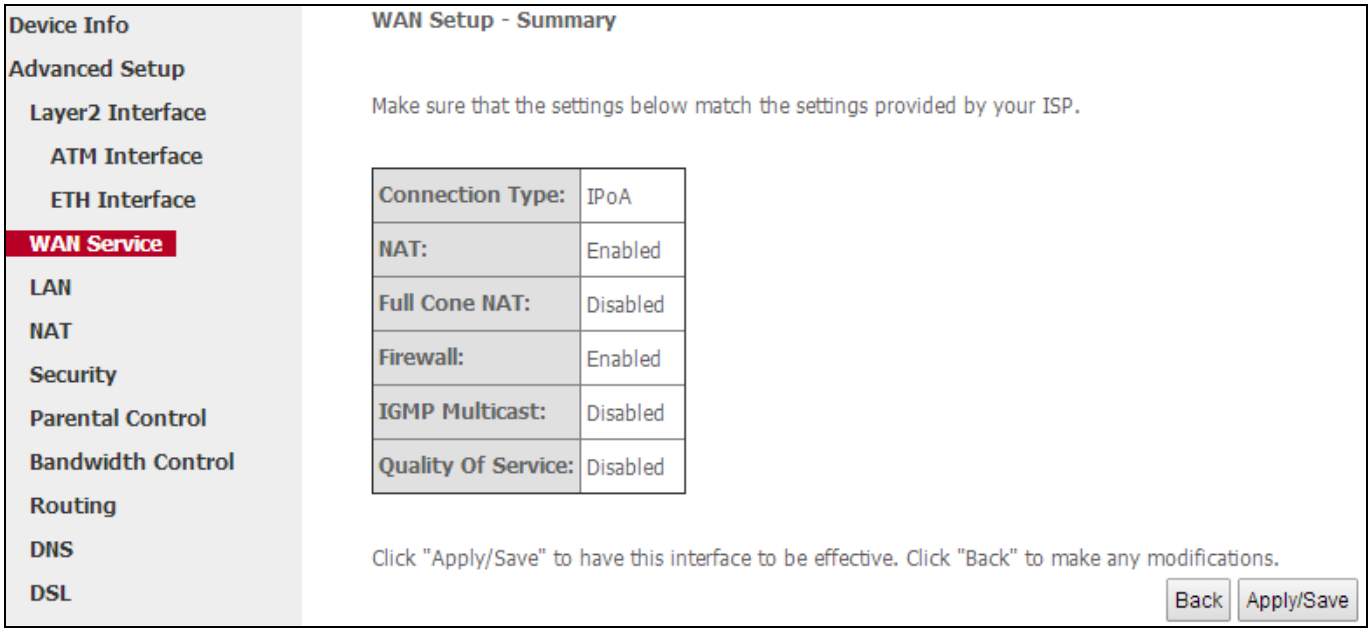
❻ Finish the default settings on the following screen. To configure one interface with the default gateway, select and move the interface from **Available Routed WAN Interfaces** into **Selected Default Gateway Interfaces**. To cancel the interface as the selected default gateway interface, select and move the interface from the **Selected Default Gateway Interfaces** into **Available Routed WAN Interfaces**. Click **Next**.



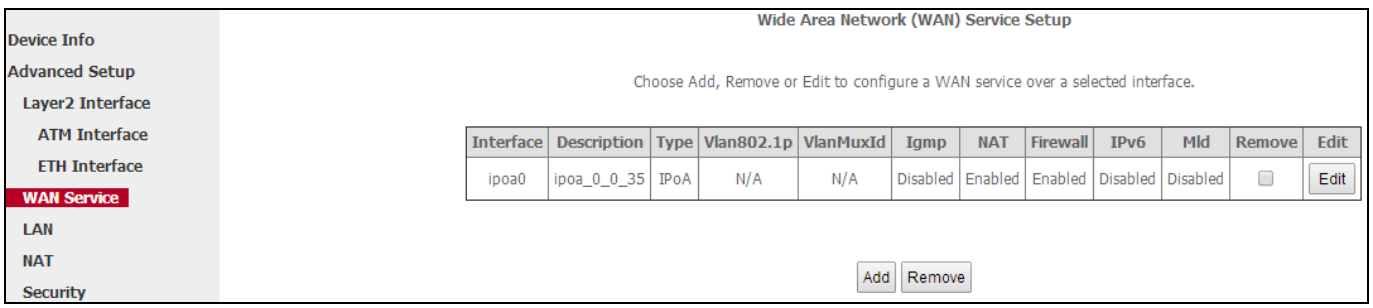
❼ Configure the DNS server of the interface you select. If you use static DNS IP address, select **Use the following Static DNS IP address** and then enter the DNS addresses provided by your ISP. Click **Next**.



Click **Apply/Save** to save your settings if everything is correctly set.



Here you can view your configurations. When the IPoA connection is successful, you can access the Internet.



↗ Steps 1~7 above for **IPoA** Users

2.2.2 For ETH Interface

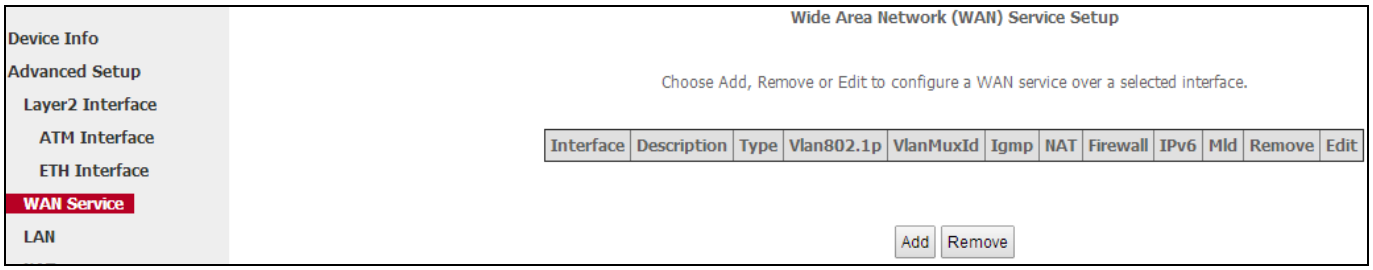
Following 7 modes are for you to choose according to your actual Internet service.

ETH	PPPoE	1) IPv4 Only	2) IPv4&IPv6 (Dual Stack)	3) IPv6 Only
	IPoE	4) IPv4 Only	5) IPv4&IPv6 (Dual Stack)	6) IPv6 Only
	7) Bridging			

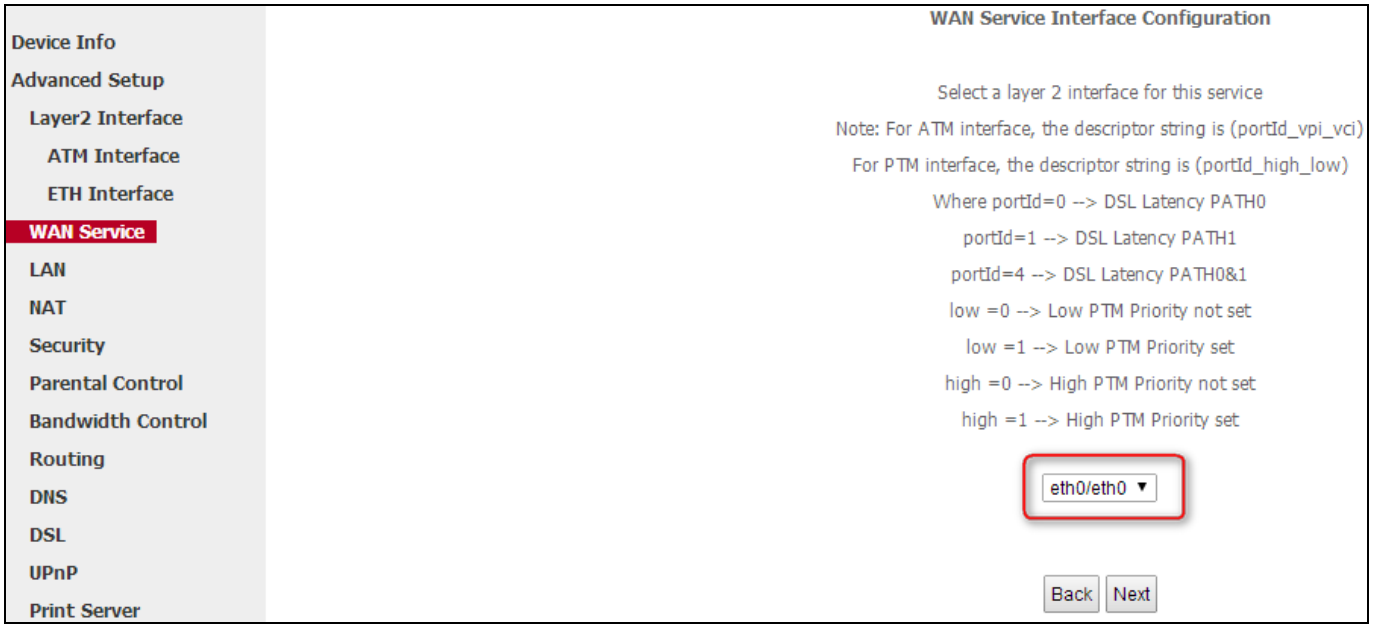
1) PPPoE IPv4 Only Users

If you configure the **ETH Interface** (Ethernet uplink) and select **eth0/eth0** as the ETH WAN interface, then you can start to set up WAN service for accessing the Internet.

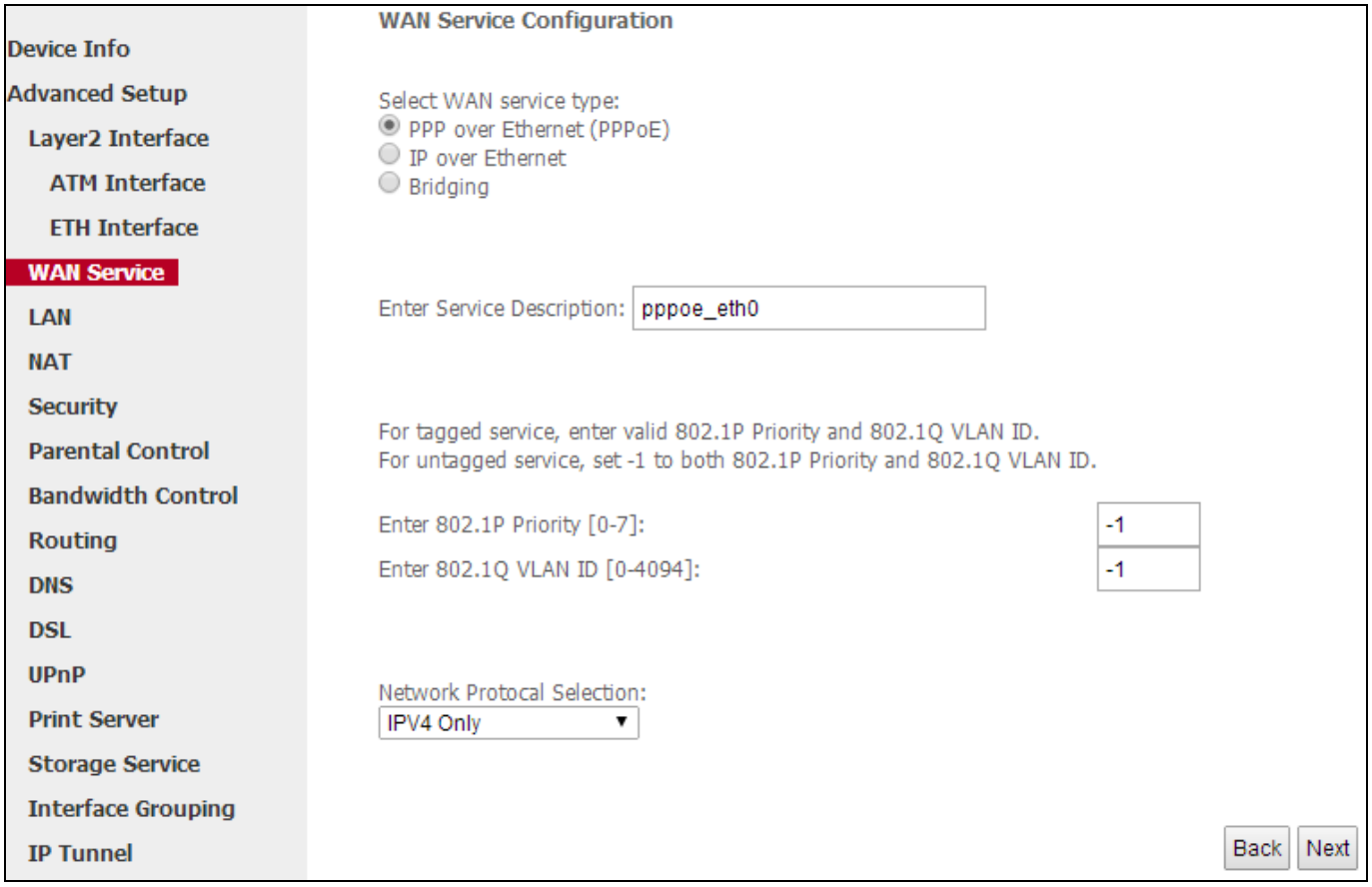
❶ Click **Advanced Setup > WAN Service** and then click the **Add** button.



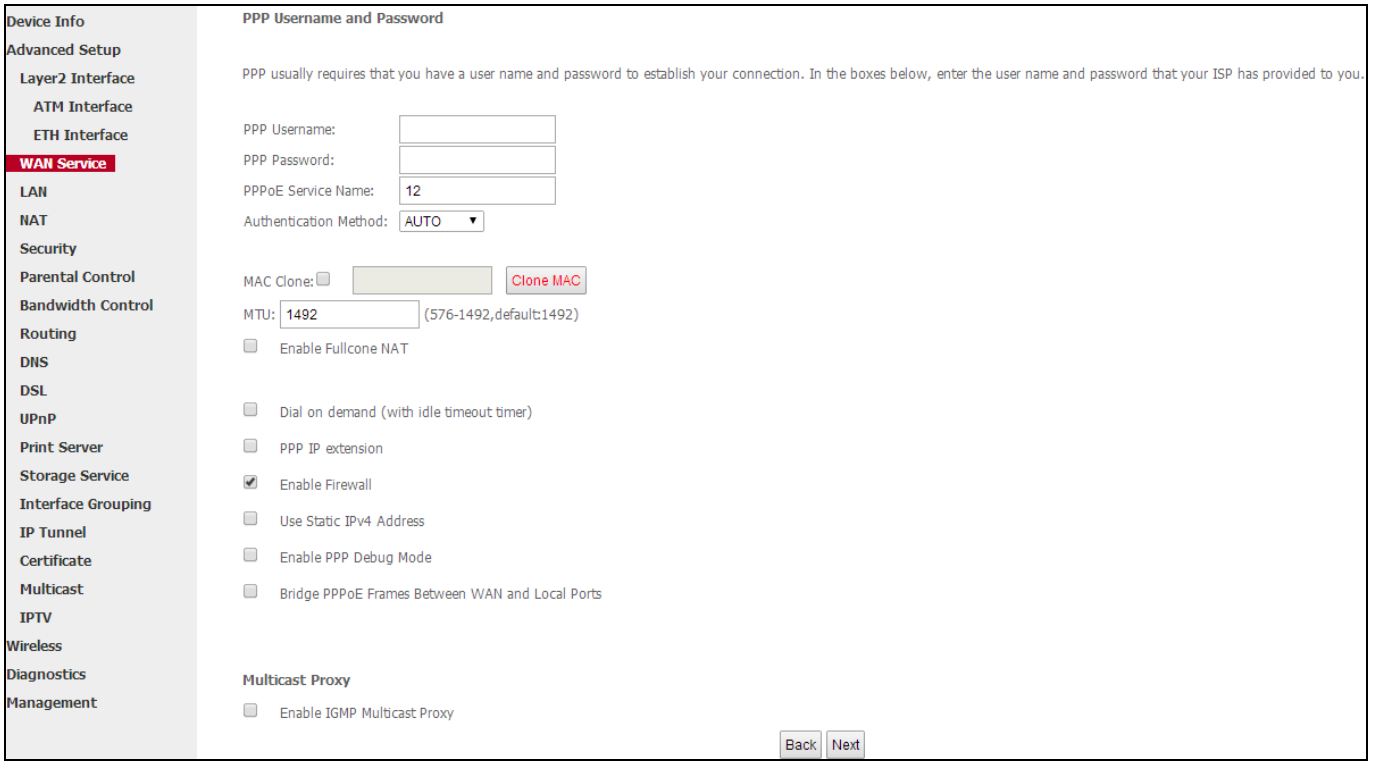
❷ Select the ETH interface you added just now from the pull-down menu in the figure below. Click **Next**.



❸ 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.**

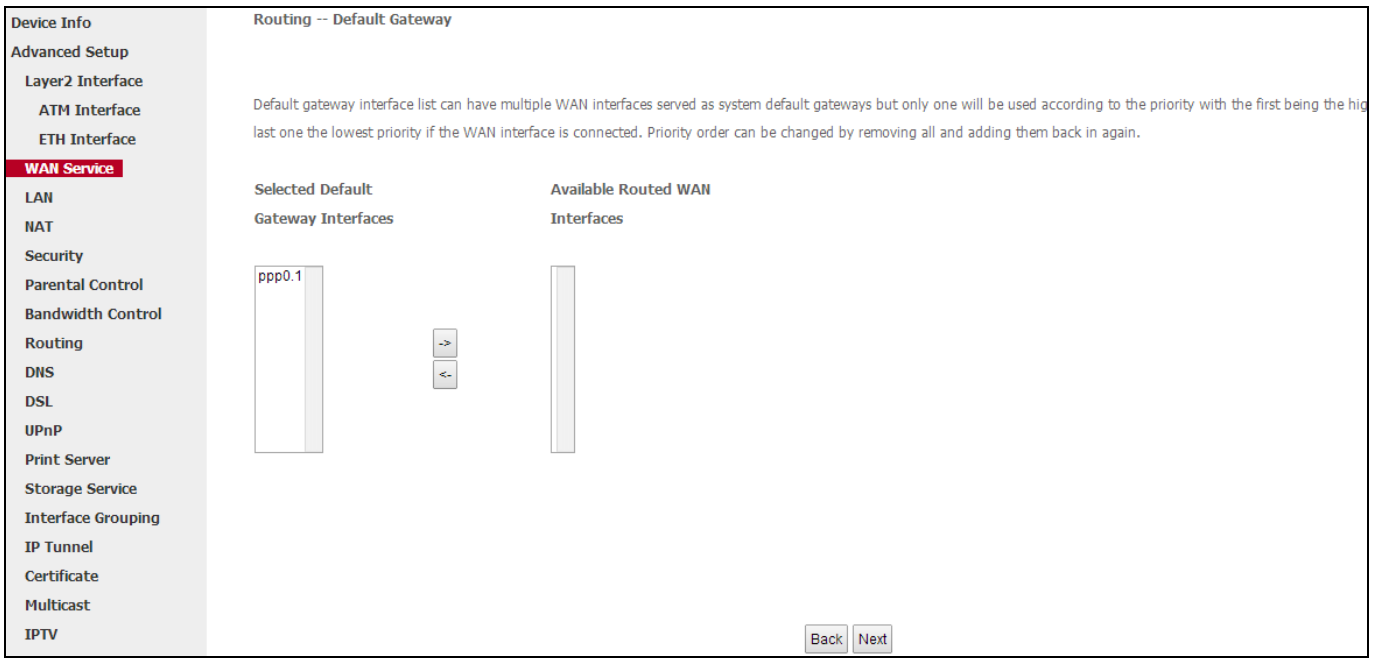


❹ Finish PPP Username and Password and other settings on the figure below. Click **Next**.

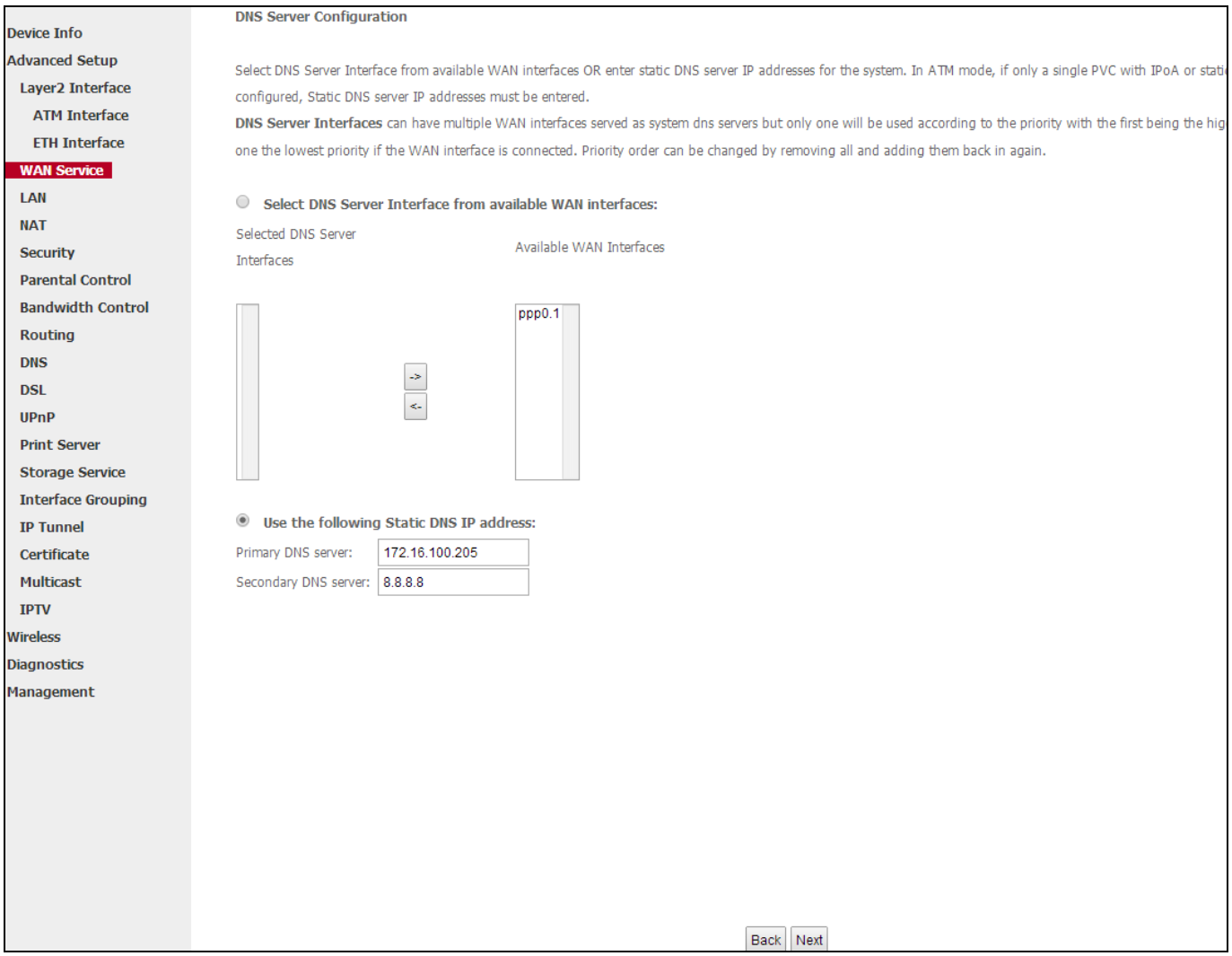


❺ To configure the Default Gateway interface, select the interface that you want to configure with the WAN gateway address in **Available Routed WAN Interfaces** box and move it into **Selected Default Gateway Interfaces** box. The

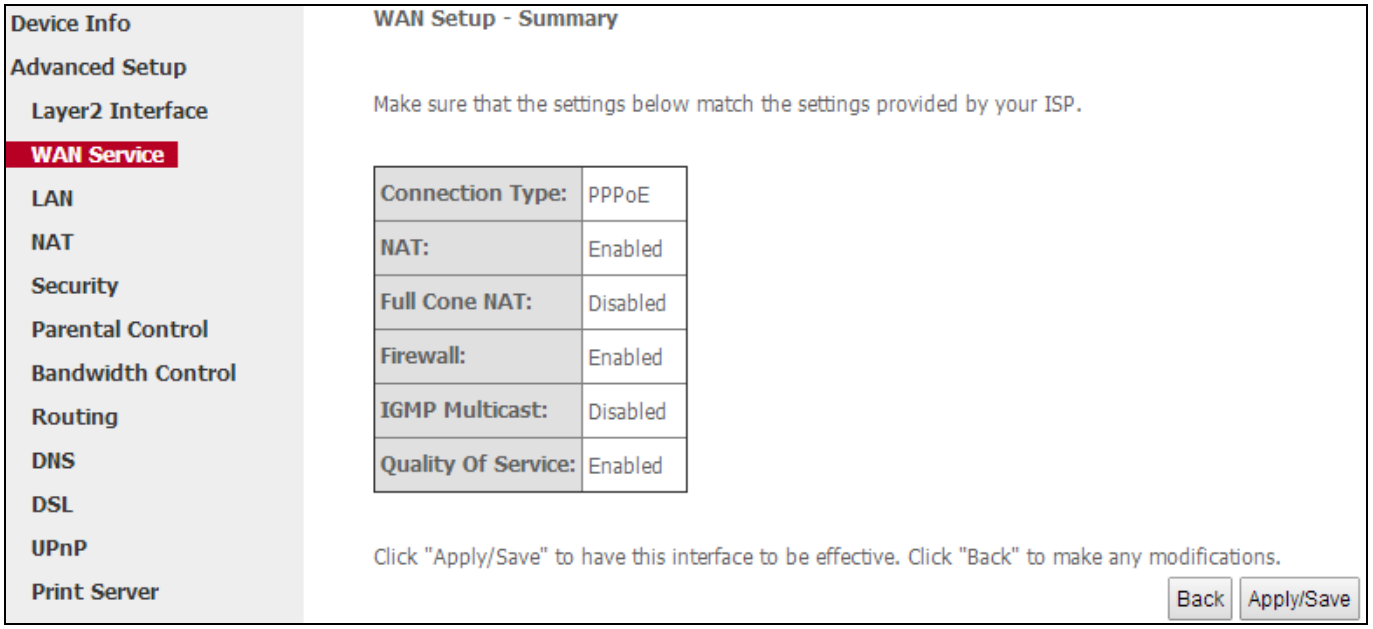
default setting is recommended. Then click **Next**.



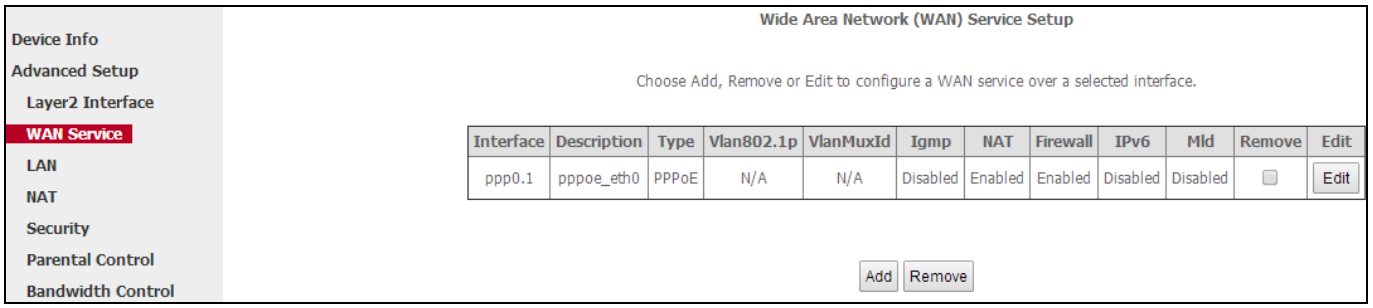
❻ To configure the WAN DNS address, click the **Select DNS Server Interface from available WAN interfaces** option, or select the **Use the following Static DNS IP address** option and enter the static DNS server IP addresses provided by your ISP. At last, click **Next**.



Click **Apply/Save** to save your settings if everything is correctly set.



Here you can view your configurations. When the PPPoE connection is successful, you can access the Internet.

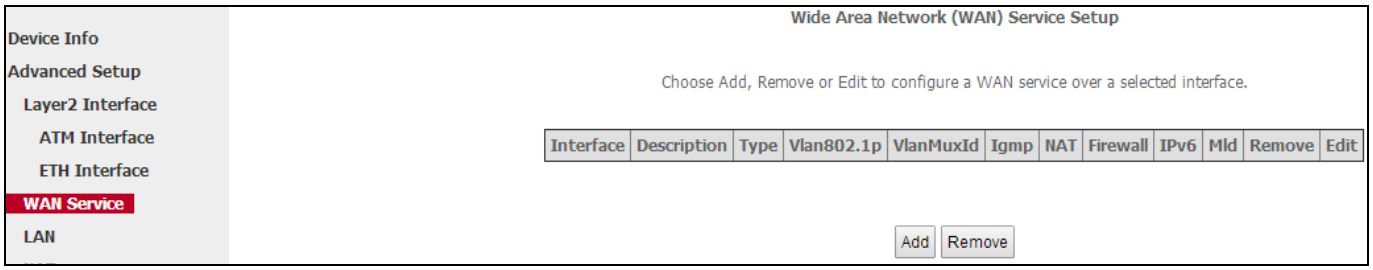


↗ Steps 1~6 above for **PPPoE and IPv4 Only** users

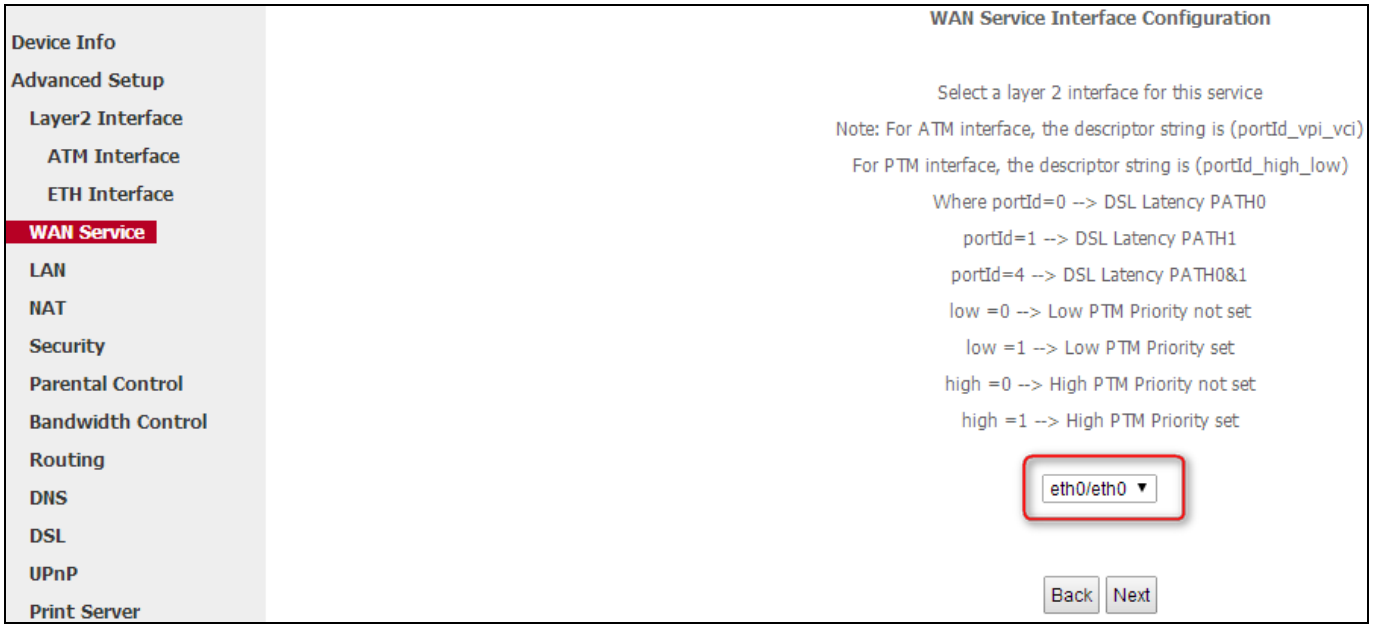
2) PPPoE IPv4&IPv6 (Dual Stack) Users

If you configure the **ETH Interface** (Ethernet uplink) and select **eth0/eth0** as the ETH WAN interface, then you can start to set up WAN service for accessing the Internet.

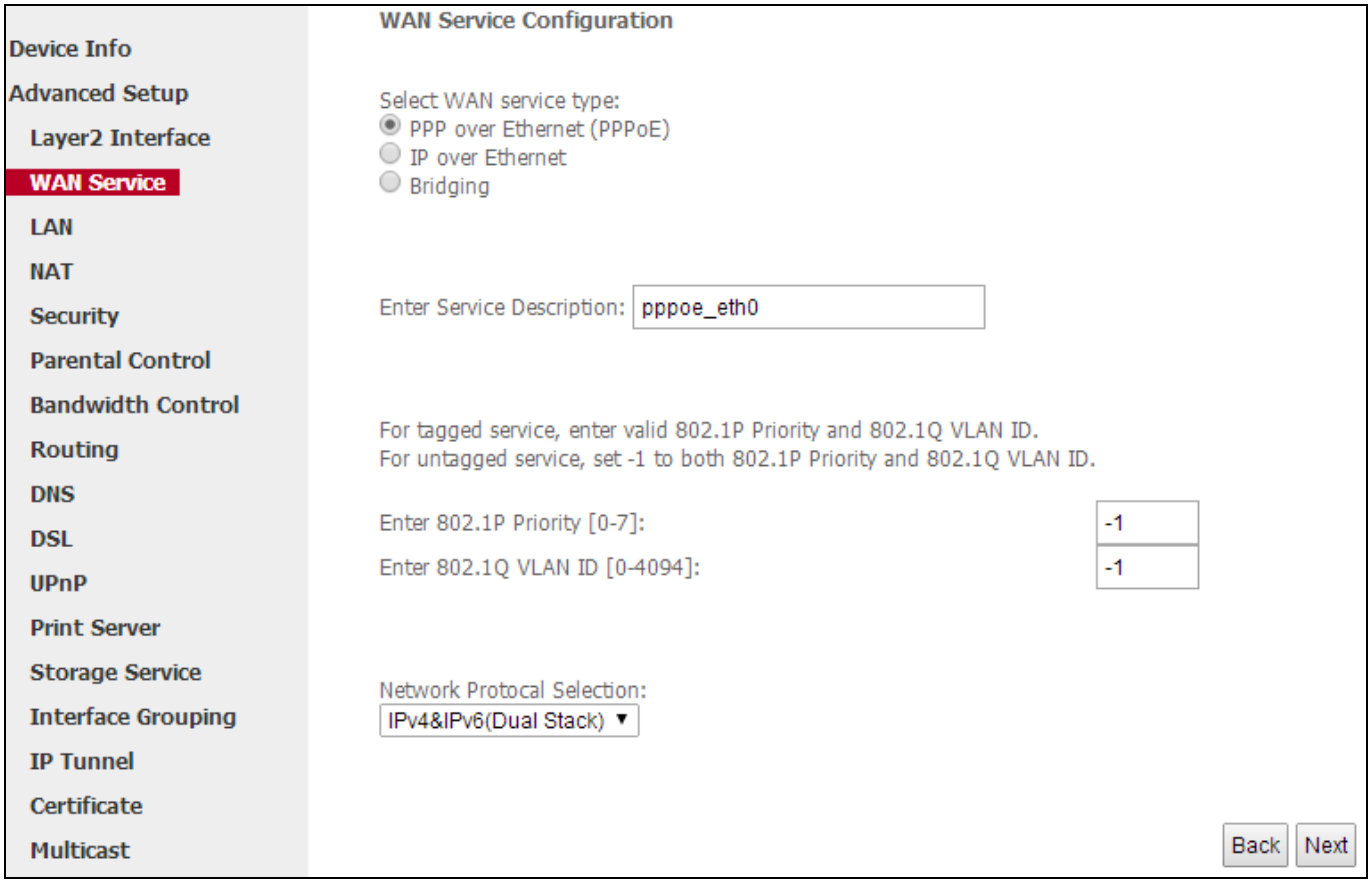
❶ Click **Advanced Setup > WAN Service** and then click the **Add** button.



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



❸ 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: **IPv4&IPv6 (Dual Stack)**. Click **Next**.

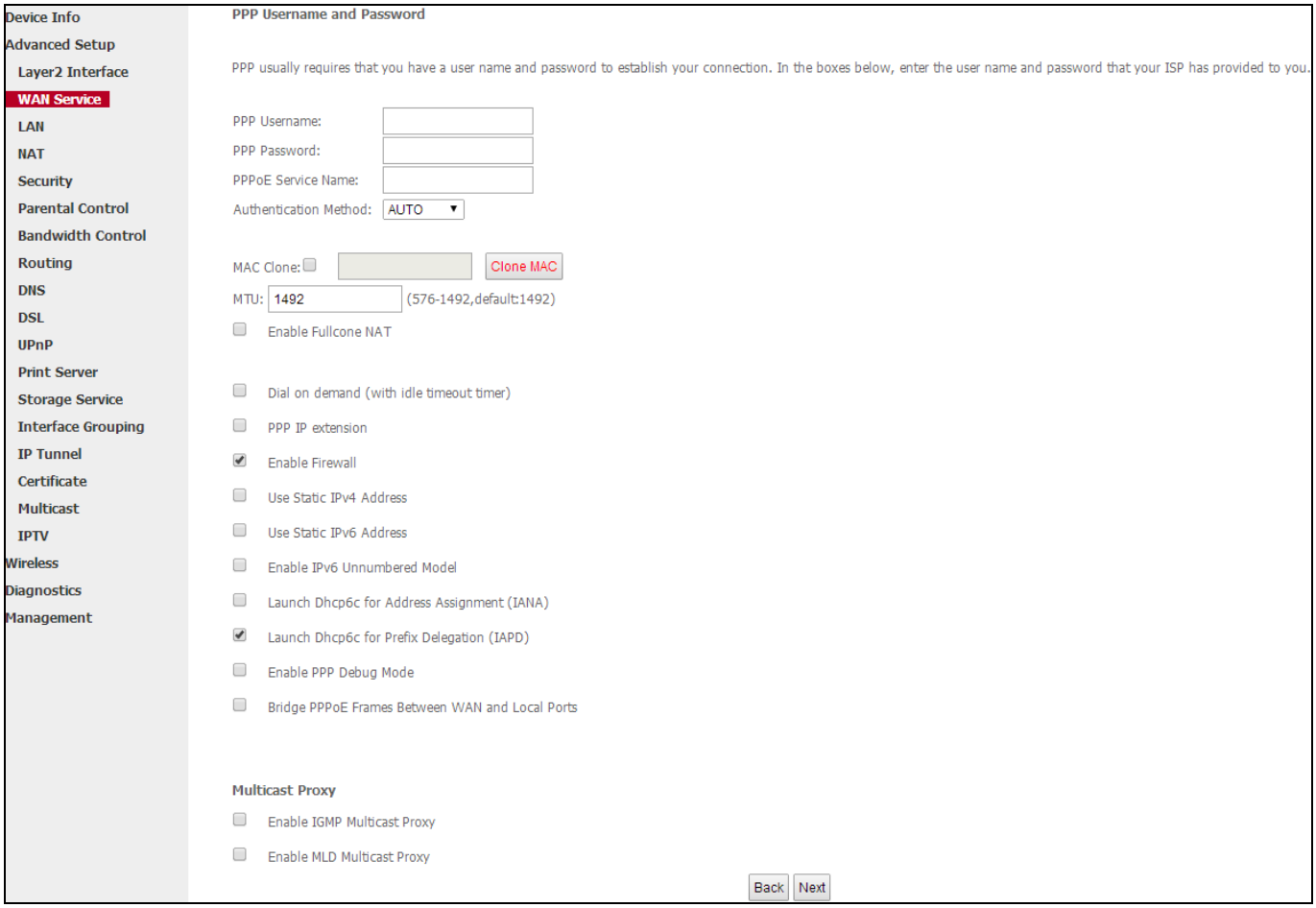


❹ Configure PPP Username and Password and other settings on the figure below. Each field with its indication is mentioned above in **PPPoE and IPv4 users-**❹ section.

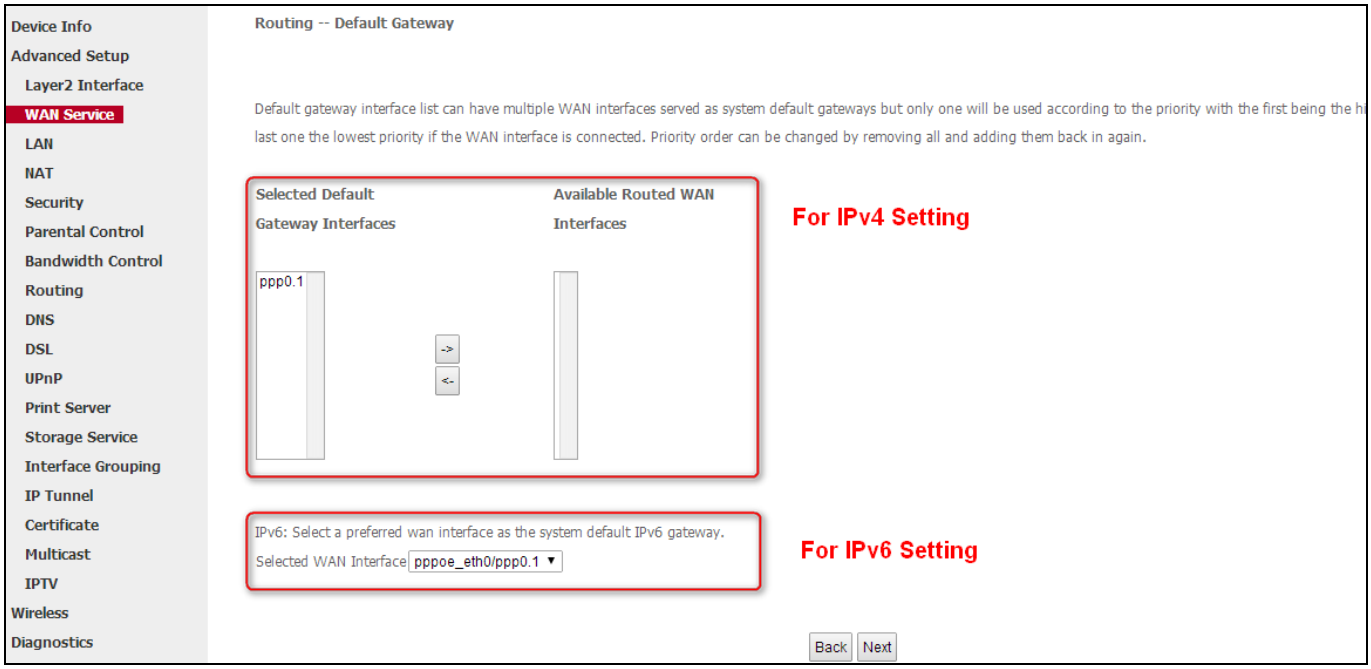
If ISP provides you no static IPv4 or IPv6 address, you just keep the default settings for it's by default the DHCP mode.

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

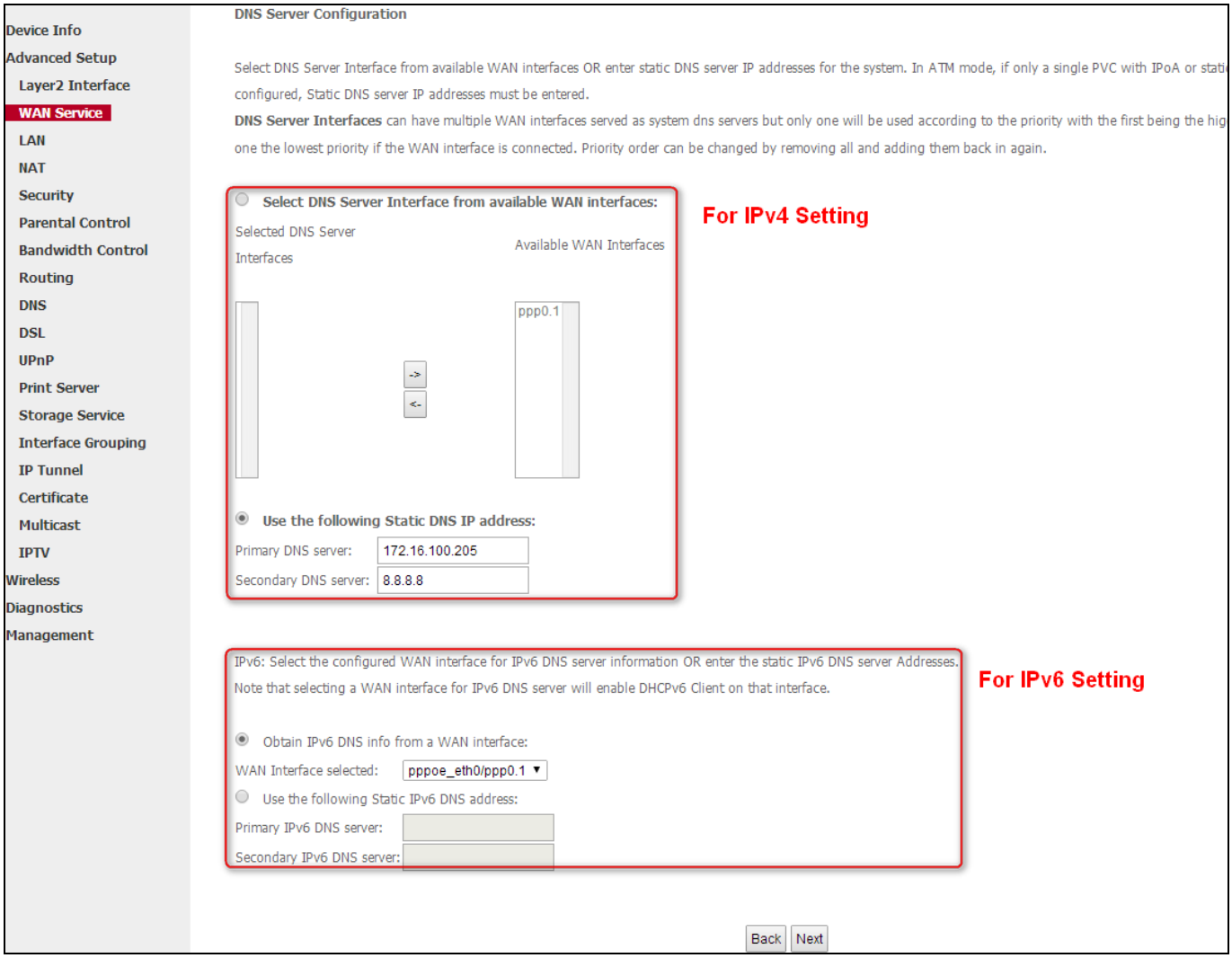
If your ISP is using stateful DHCPv6, check **Launch Dhcp6c for Address Assignment (IANA)** also. Click **Next.**



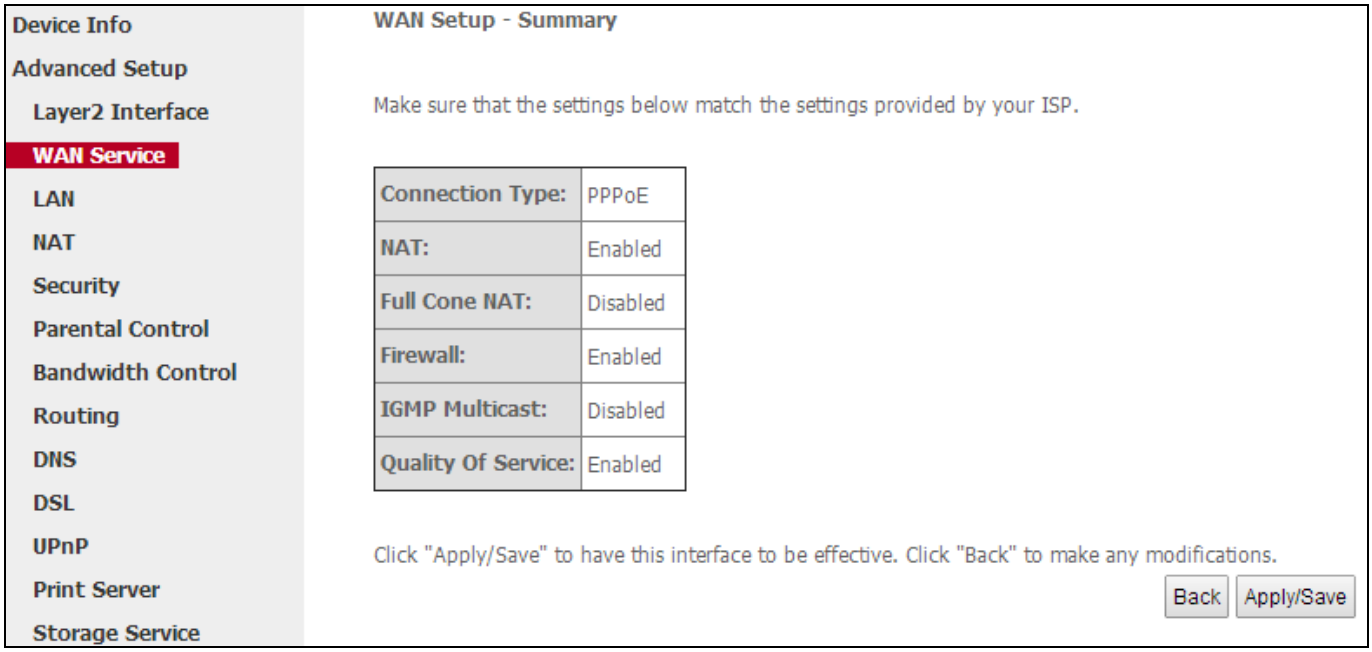
❺ To configure the Default Gateway interface, select the interface that you want to configure with the WAN gateway address. Then click **Next**.



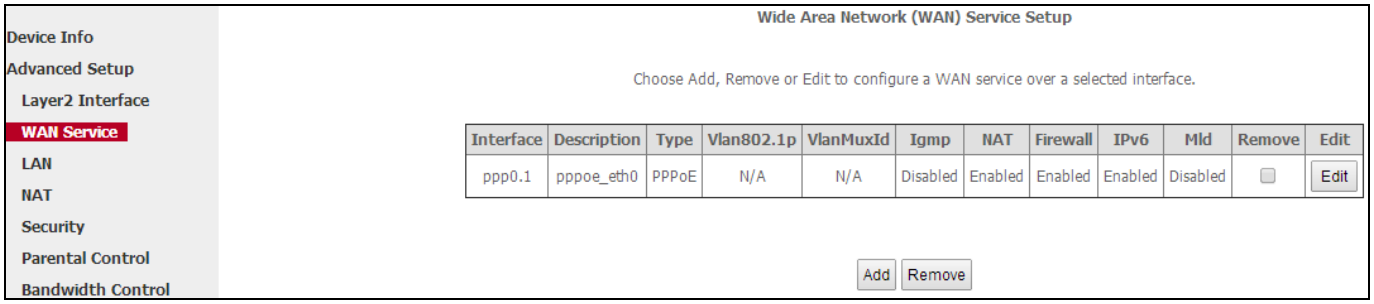
❻ To configure the WAN DNS address, finish both the IPv4 setting and IPv6 setting. Click **Next**.



Click **Apply/Save** to save your settings if everything is correctly set.



Here you can view your configurations. When the PPPoE connection is successful, you can access the Internet.

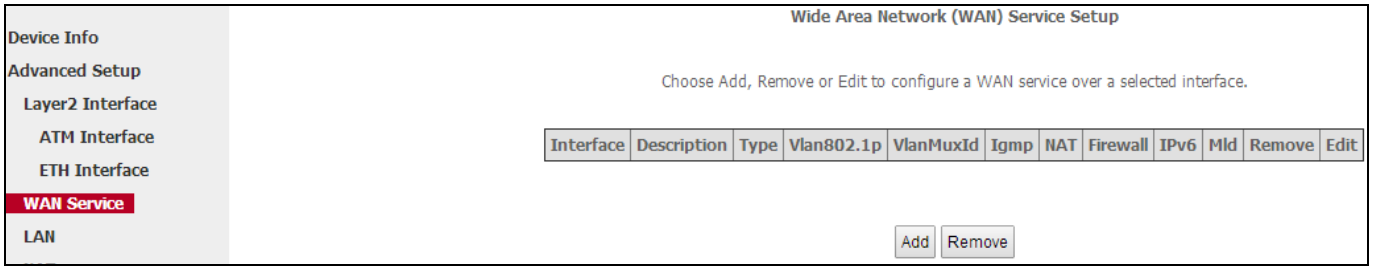


↗ Steps 1~6 above for **PPPoE and IPv4&IPv6 (Dual Stack)** users

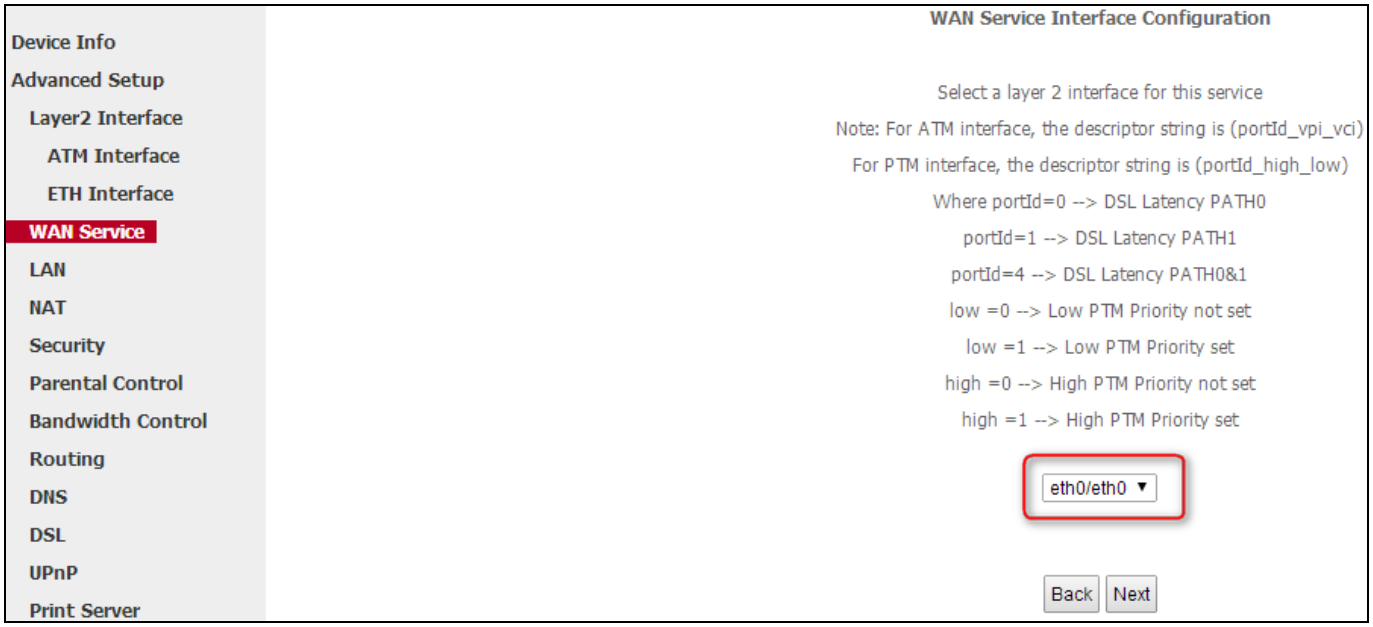
3) PPPoE IPv6 Only Users

If you configure the **ETH Interface** (Ethernet uplink) and select **eth0/eth0** as the ETH WAN interface, then you can start to set up WAN service for accessing the Internet.

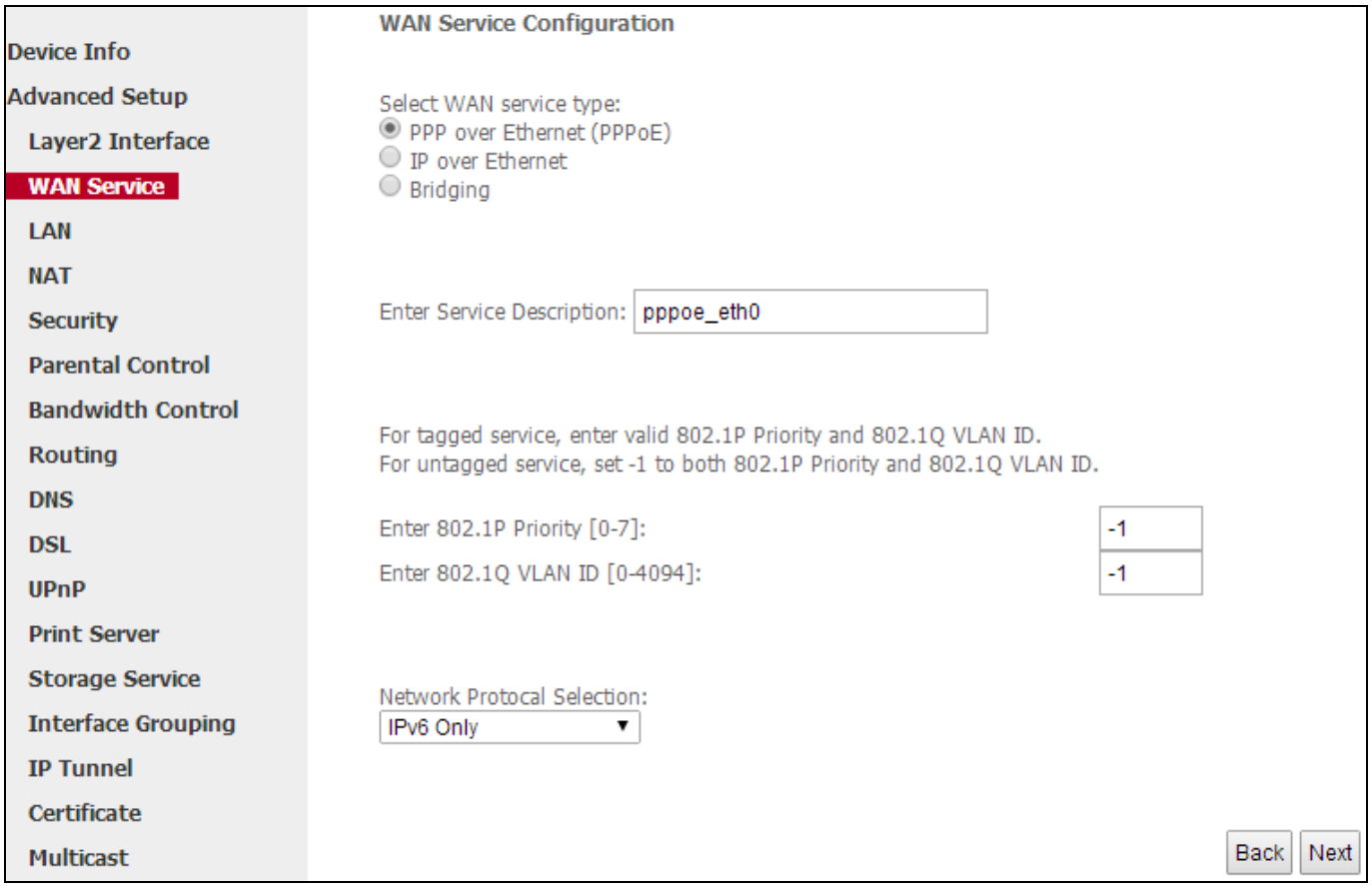
❶ Click **Advanced Setup > WAN Service** and then click the **Add** button.



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



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

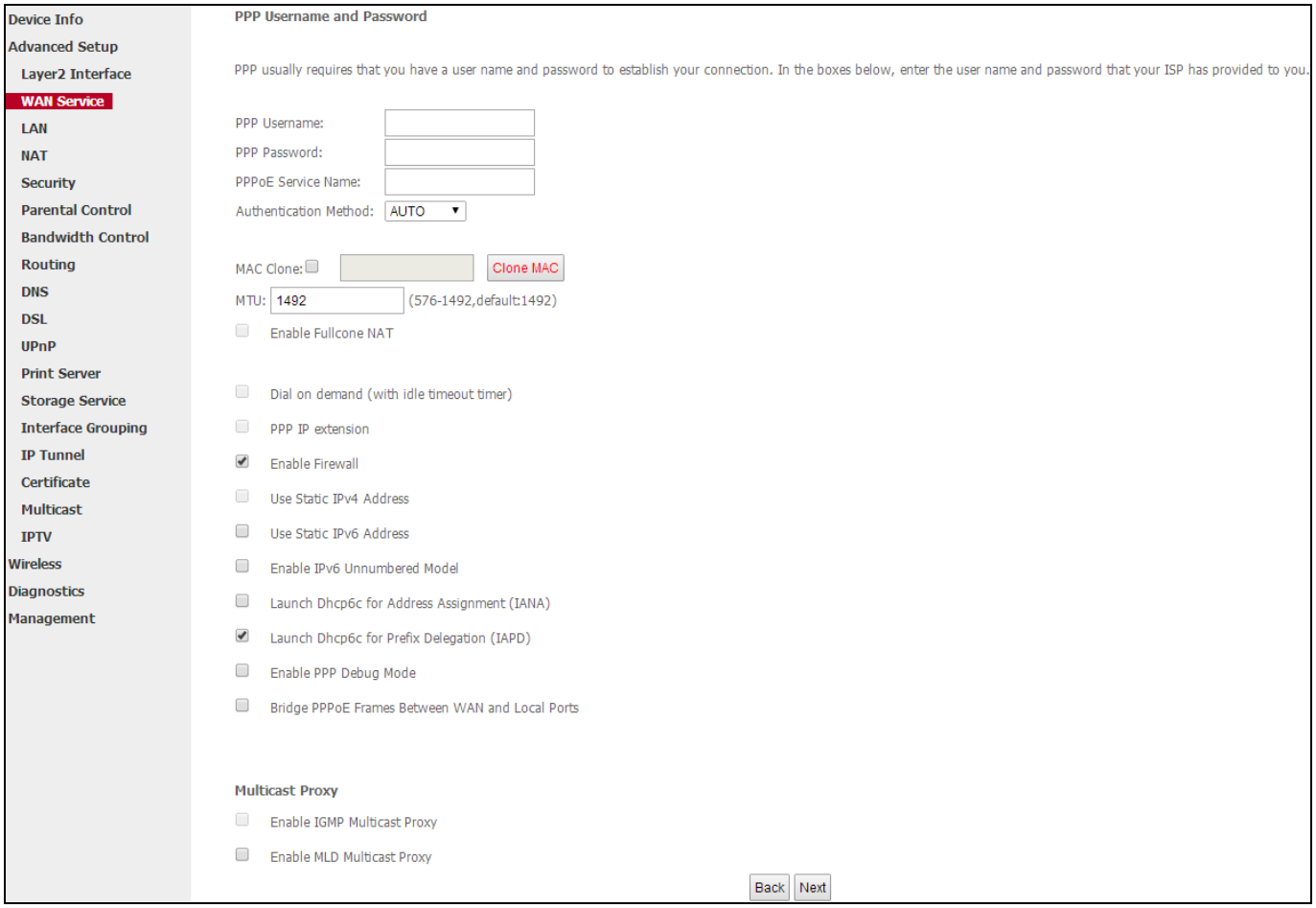


❹ Configure PPP Username and Password and other settings on the figure below. Each field with its indication is mentioned above in **PPPoE and IPv4 users** section.

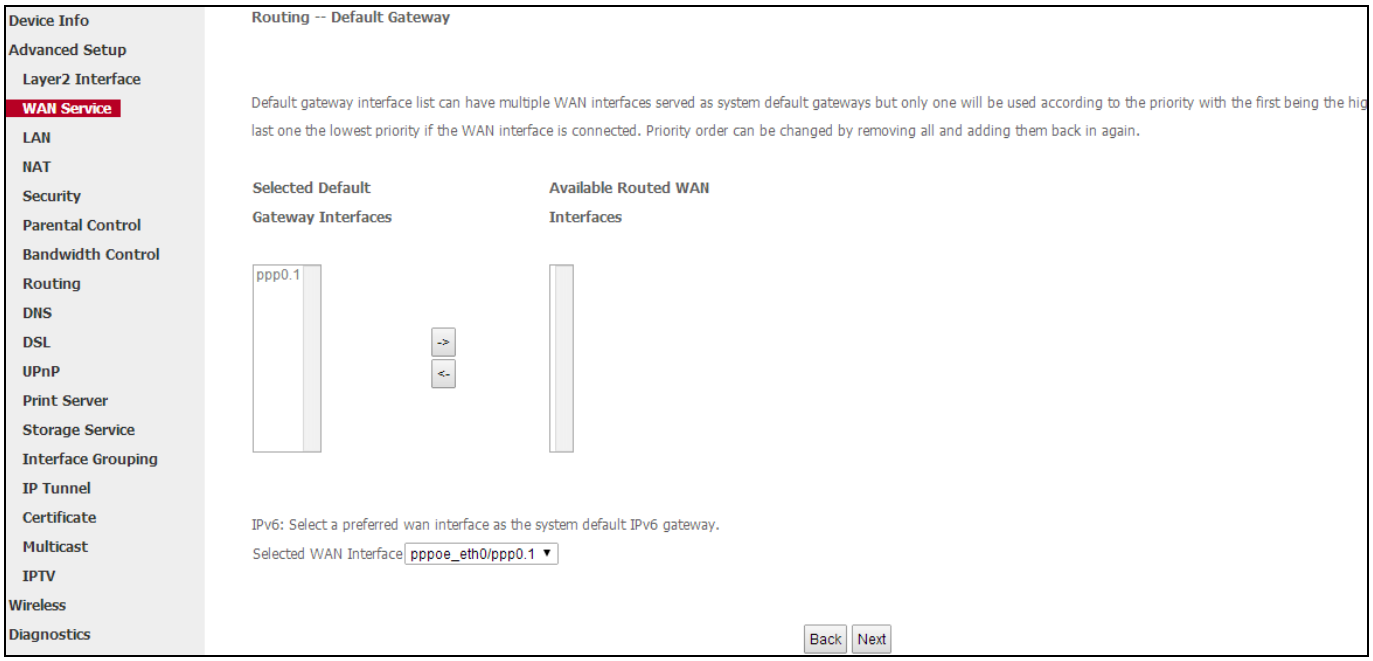
If ISP provides you no static IPv6 address, you just keep the default settings for it's by default the DHCP mode.

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

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

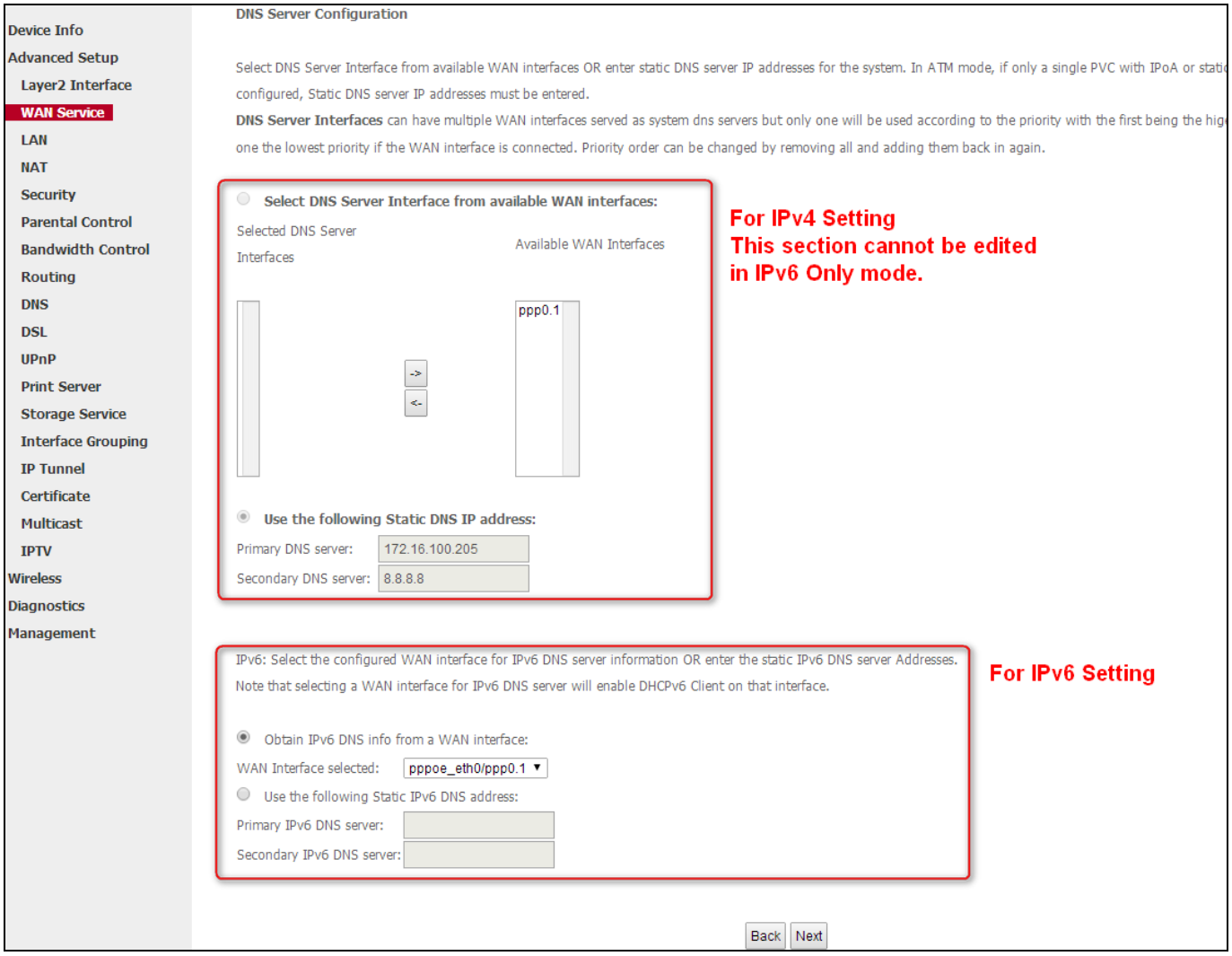


❺ To configure the Default Gateway interface when using IPv6, select the interface that you want to configure with the WAN gateway address in **Selected WAN Interface** box. Then click **Next**.

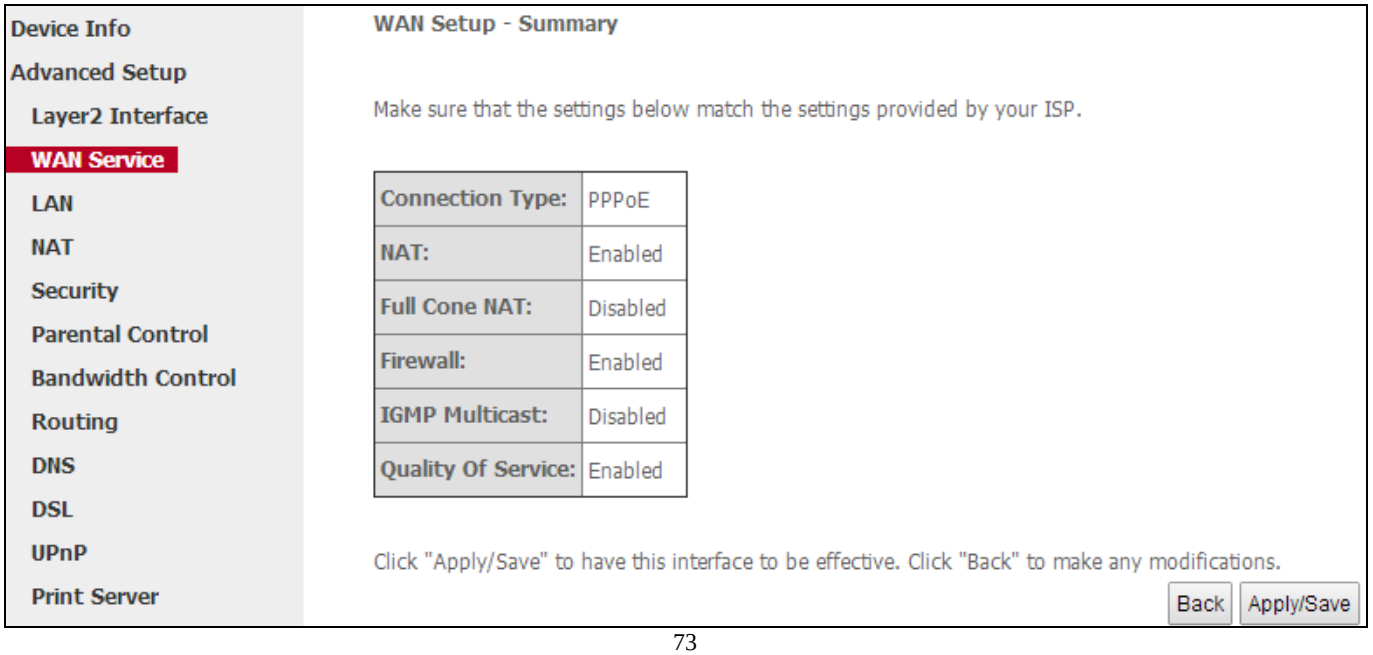


❻ To configure the WAN DNS address, check the **Obtain IPv6 DNS info from a WAN interface** option, or select the **Use the following Static IPv6 DNS address** option to enter the static DNS server IPv6 addresses provided by your ISP.

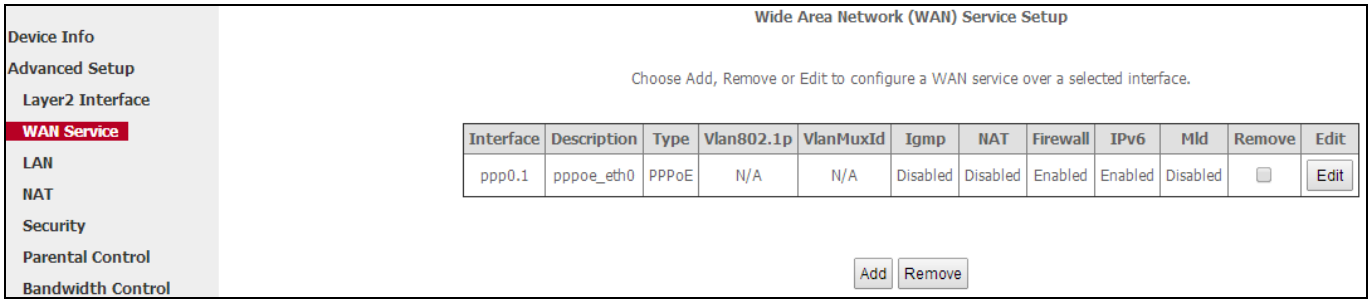
At last, click **Next**.



Click **Apply/Save** to save your settings if everything is correctly set.



Here you can view your configurations. When the PPPoE connection is successful, you can access the Internet.

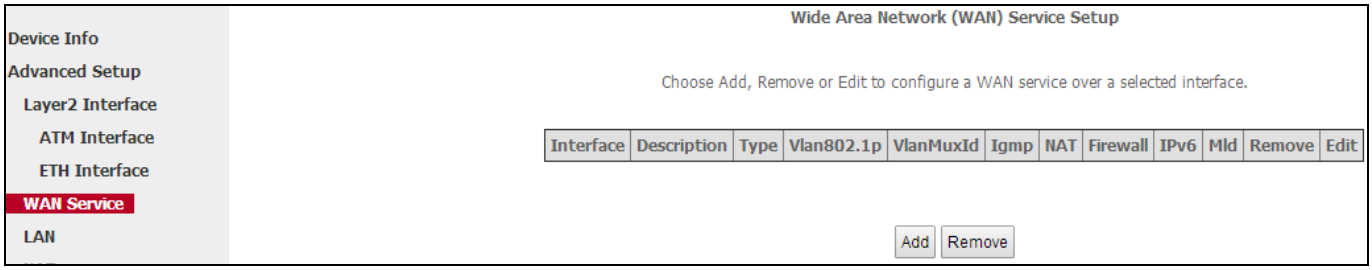


↗ Steps 1~6 above for **PPPoE and IPv6 Only** users

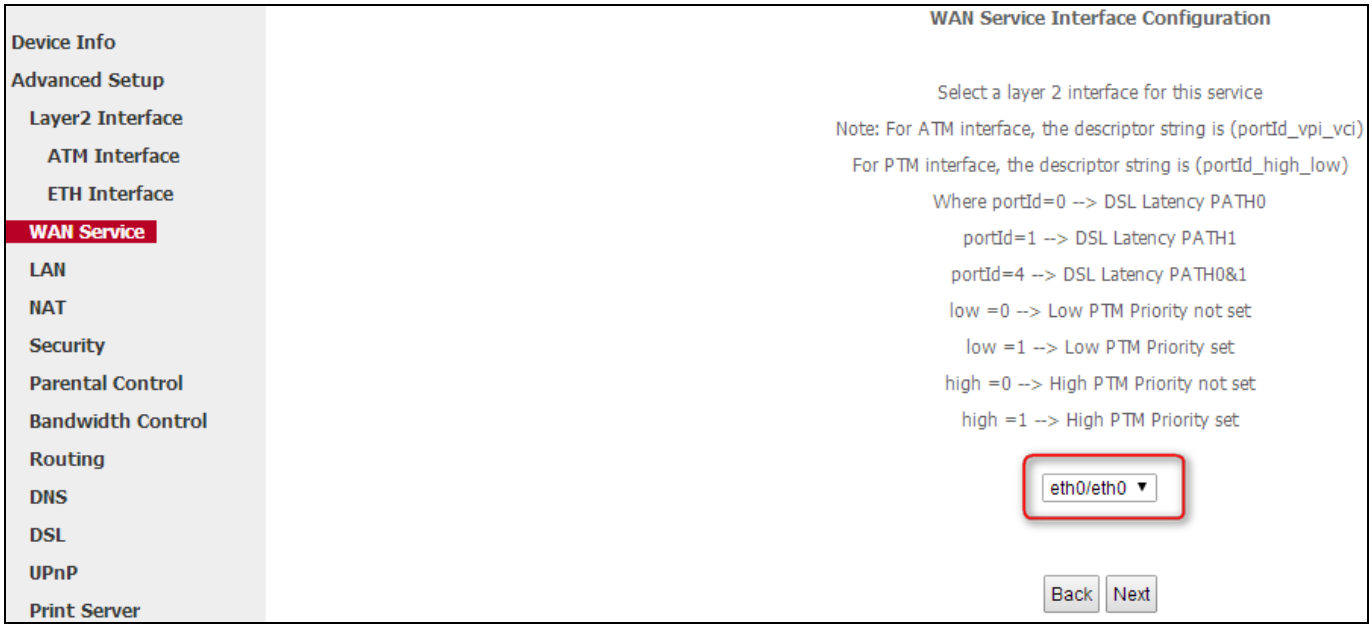
4) IPoE IPv4 Only Users

If you configure the **ETH Interface** (Ethernet uplink) and select **eth0/eth0** as the ETH WAN interface, then you can start to set up WAN service for accessing the Internet.

❶ Click **Advanced Setup** > **WAN Service** and then click the **Add** button.

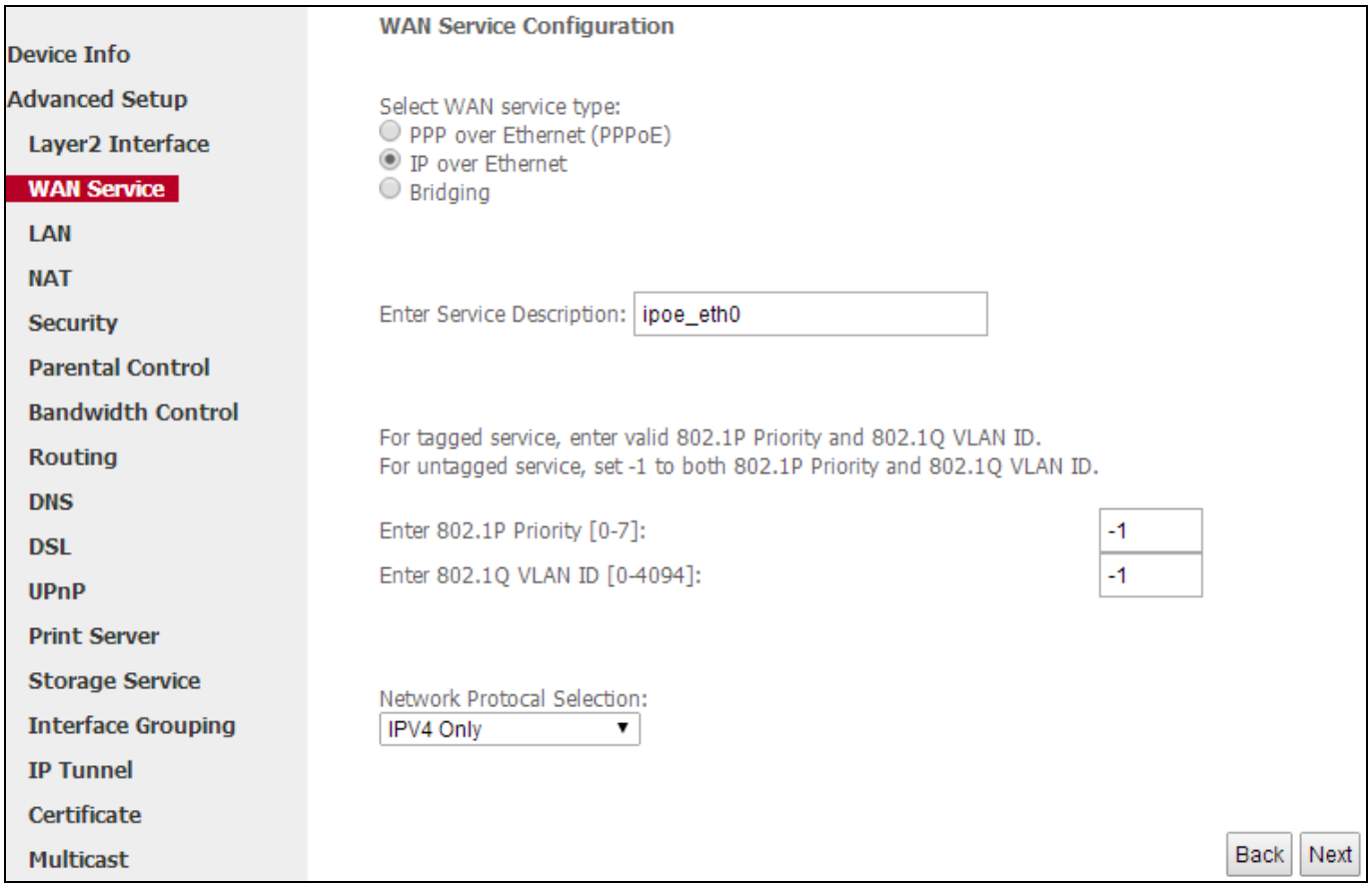


❷ Select the ETH interface you added just now from the pull-down menu in the figure below. Click **Next**.

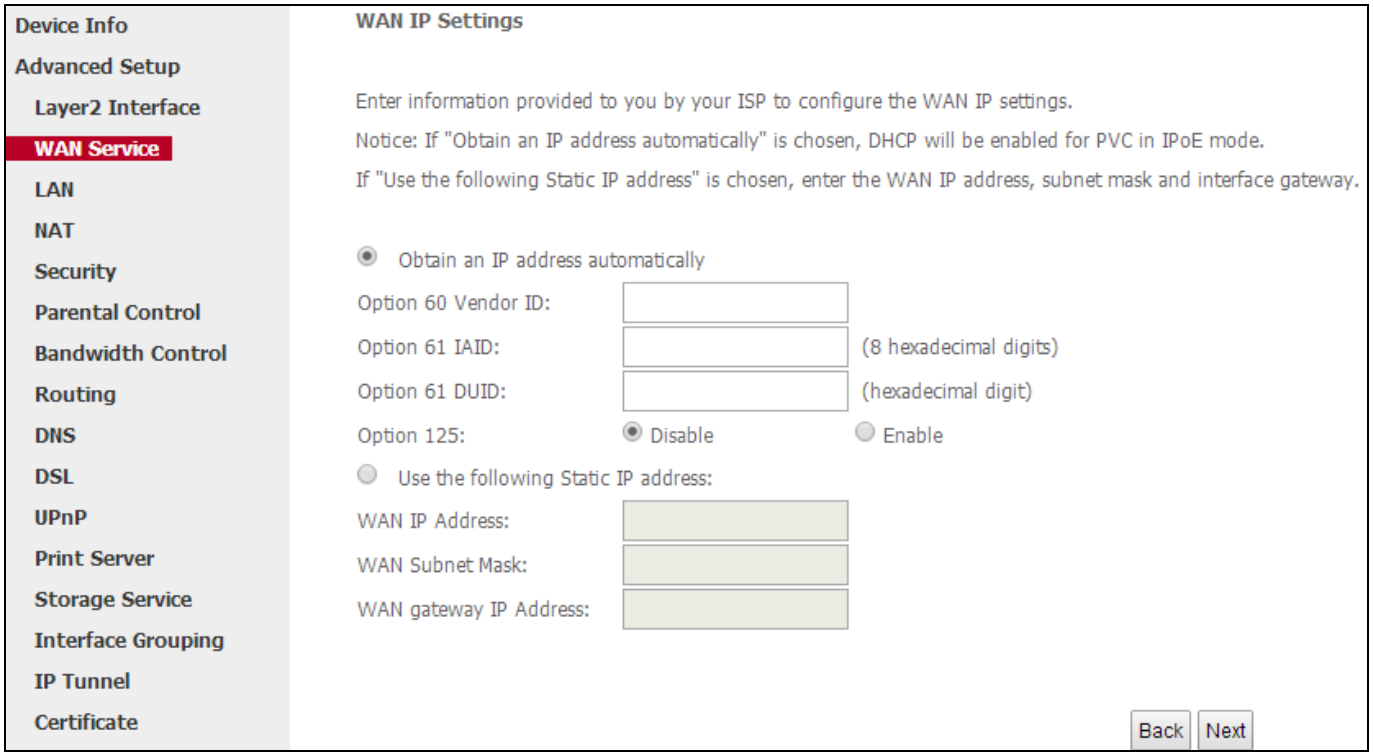


❸ Select **IP over Ethernet (IPoE)**. Edit the **Enter Service Description** field which is optional. Suggest you keep the

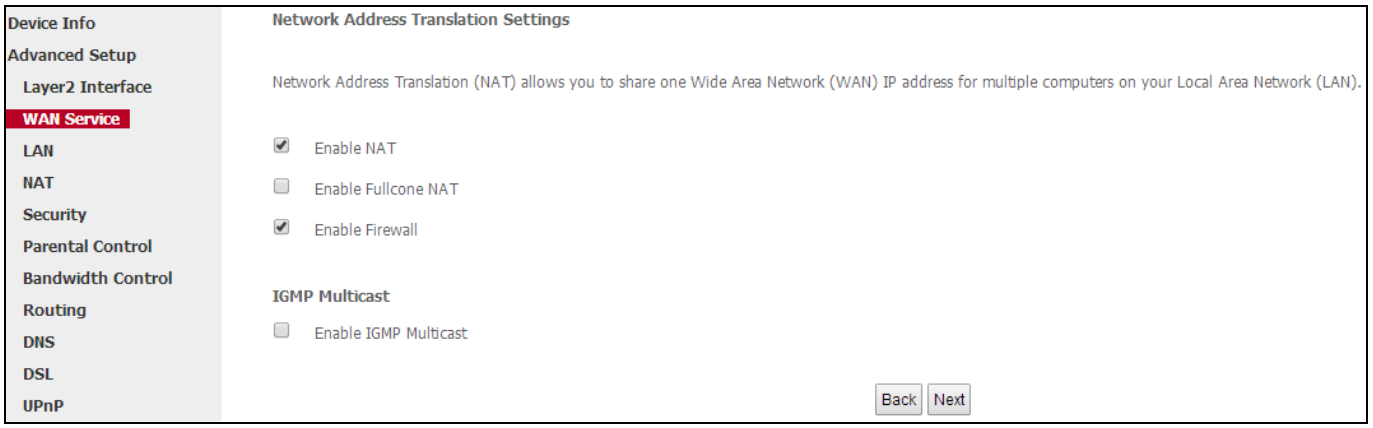
default. Select a network protocol: **IPv4 Only**. Click **Next.**



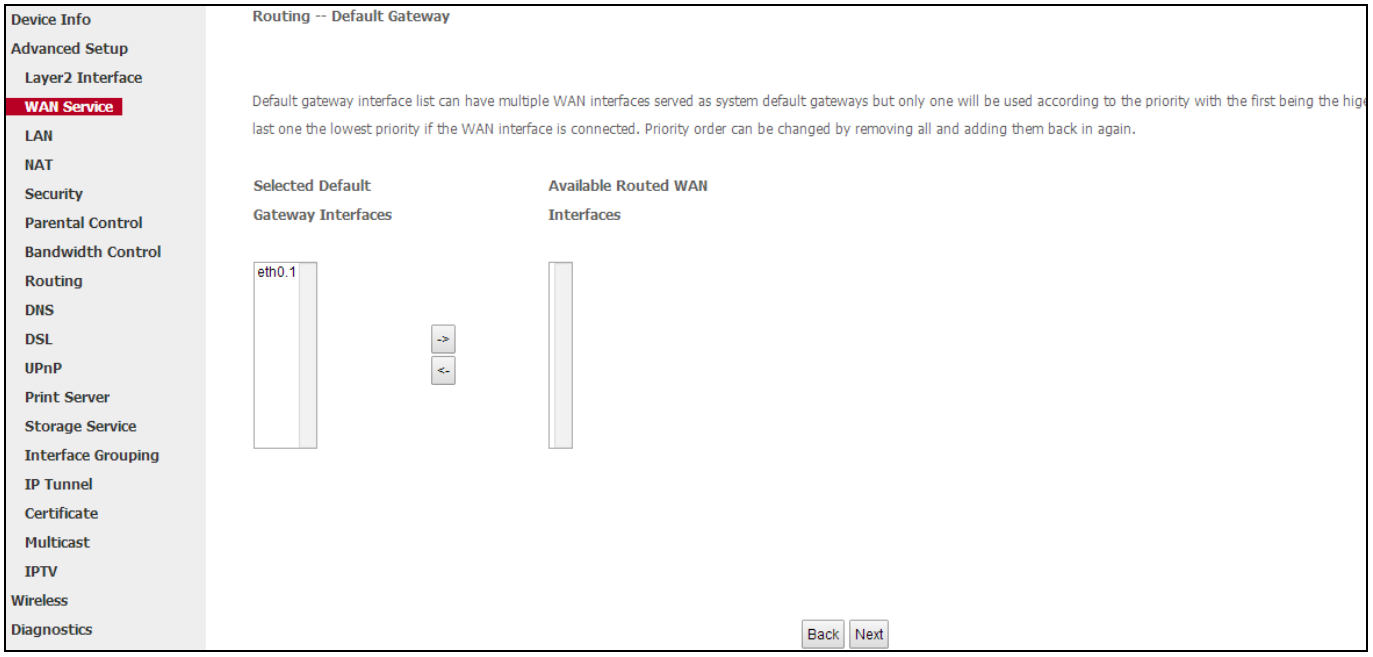
❹ Finish **WAN IP Settings** on the figure below. Click **Next**.



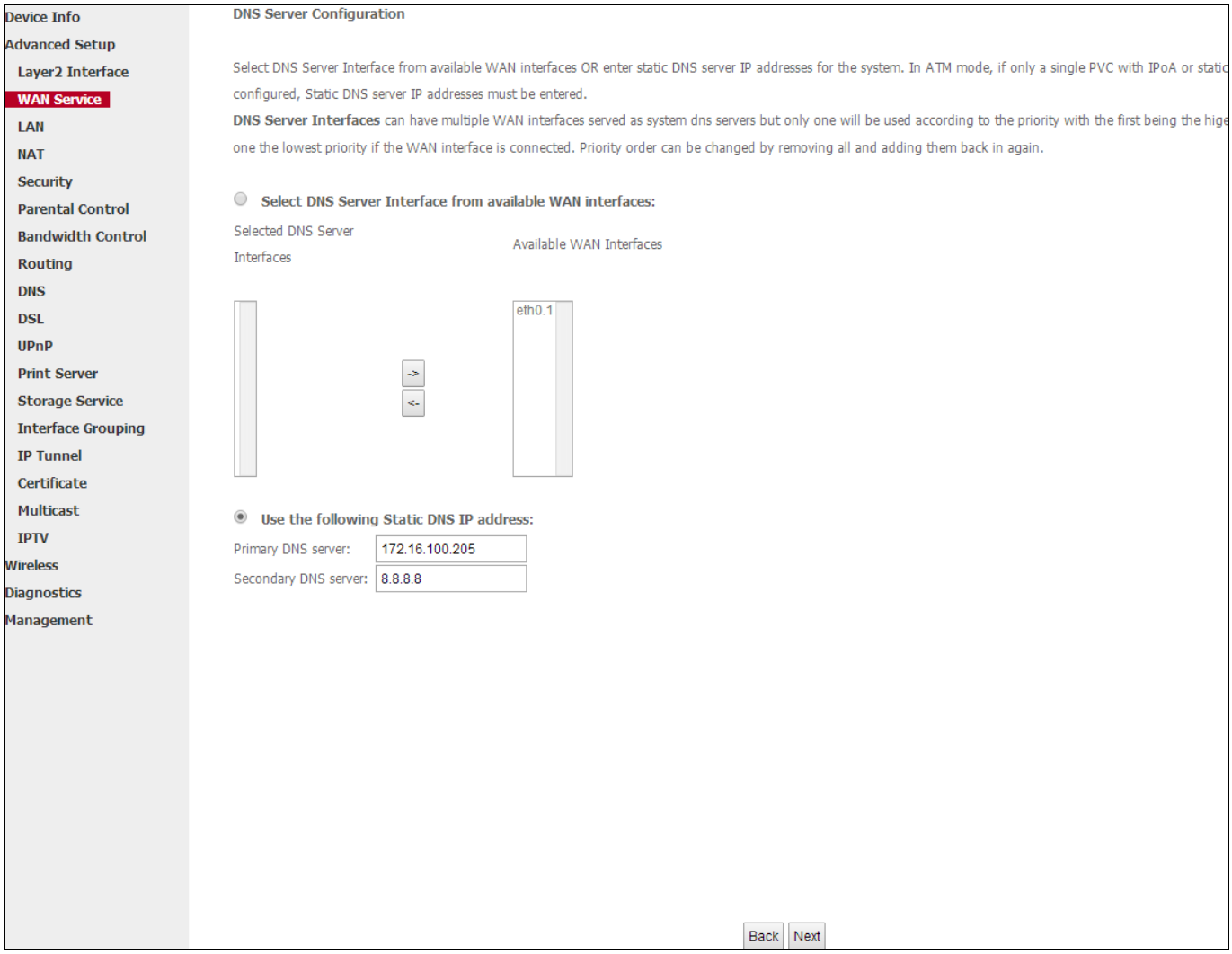
❺ Finish **Network Address Translation Settings**. Suggest to keep the default settings. Click **Next**.



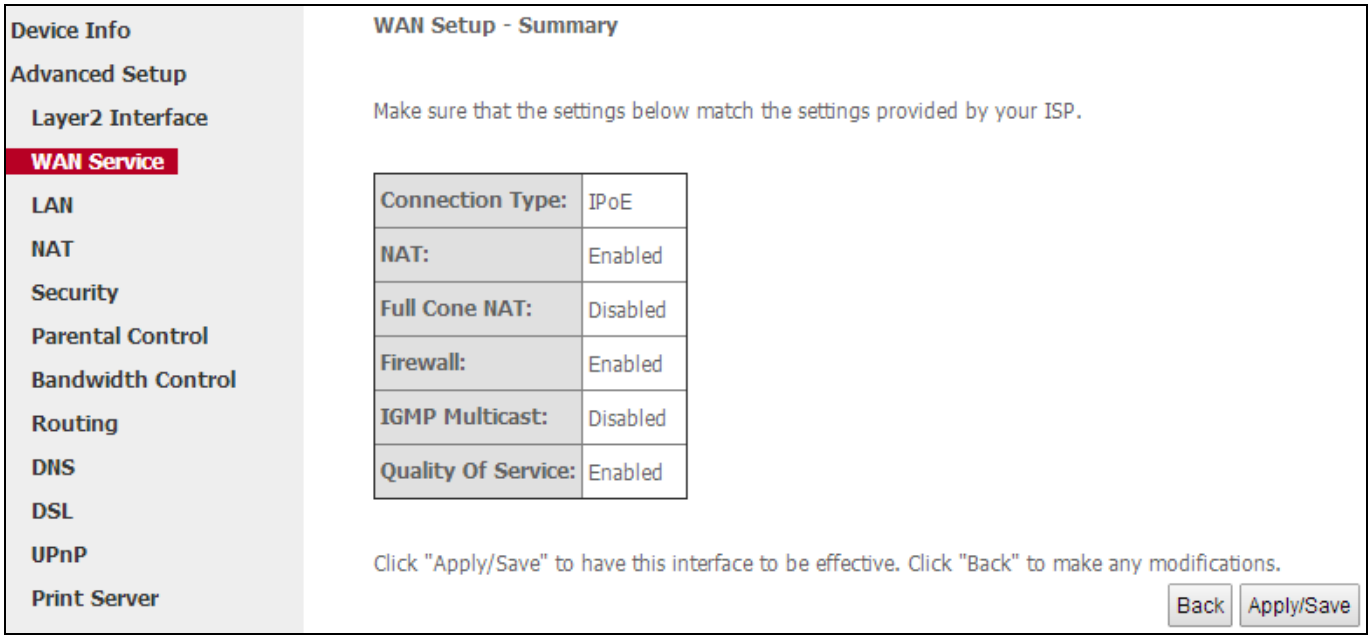
❻ To configure the Default Gateway interface, select the interface that you want to configure with the WAN gateway address in **Available Routed WAN Interfaces** box and move it into **Selected Default Gateway Interfaces** box. The default setting is recommended. Then click **Next**.



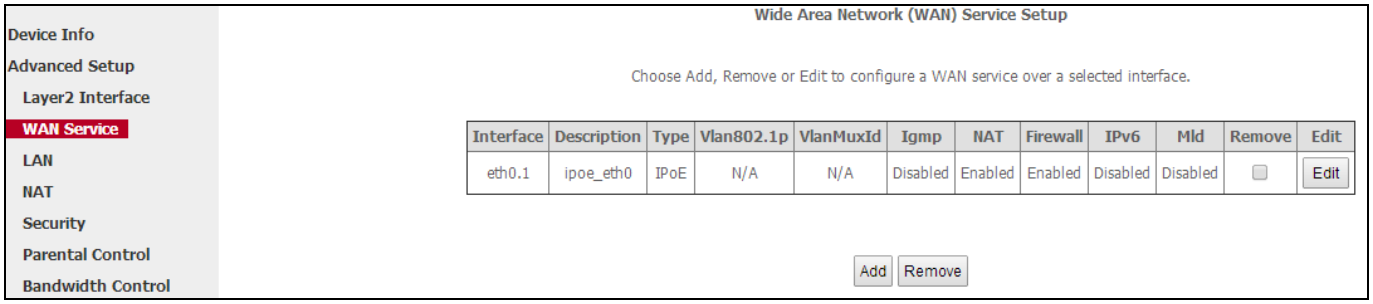
❼ To finish DNS Server Configuration, click the **Select DNS Server Interface from available WAN interfaces** option, or select the **Use the following Static DNS IP address** option and enter the static DNS server IP addresses provided by your ISP. At last, click **Next**.



Click **Apply/Save** to save your settings if everything is correctly set.



Here you can view your configurations. When the IPoE connection is successful, you can access the Internet.

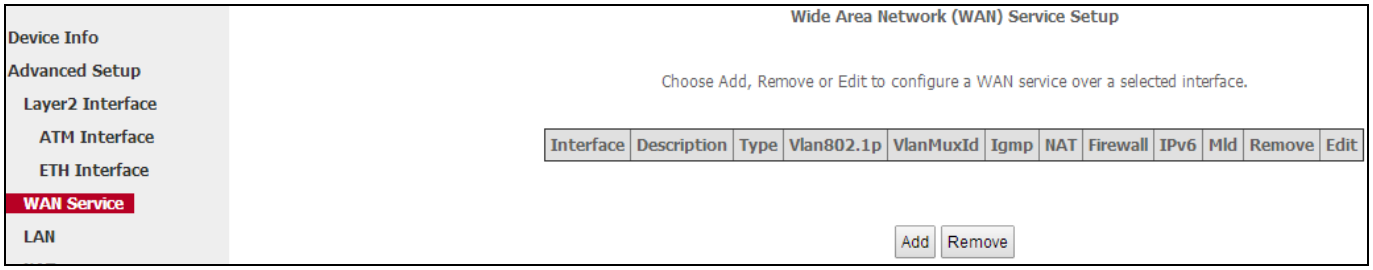


↗ Steps 1~7 above for **IPoE and IPv4 Only** users

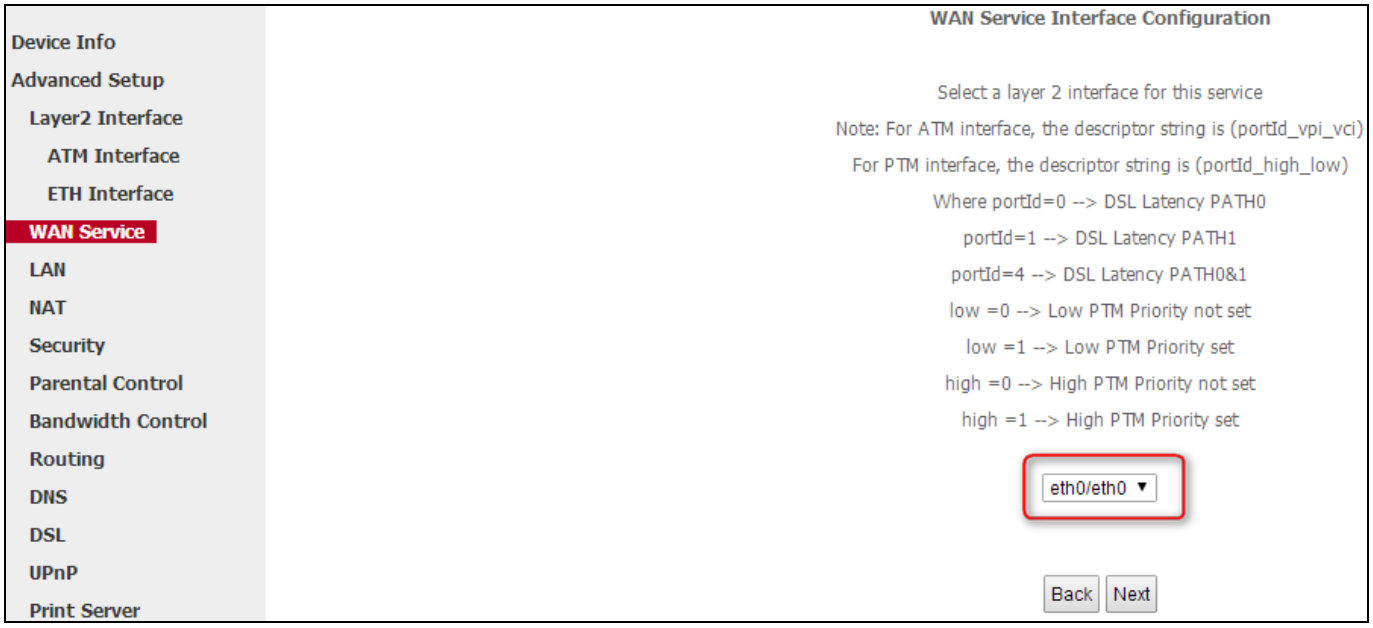
5) IPoE IPv4&IPv6 (Dual Stack) Users

If you configure the **ETH Interface** (Ethernet uplink) and select **eth0/eth0** as the ETH WAN interface, then you can start to set up WAN service for accessing the Internet.

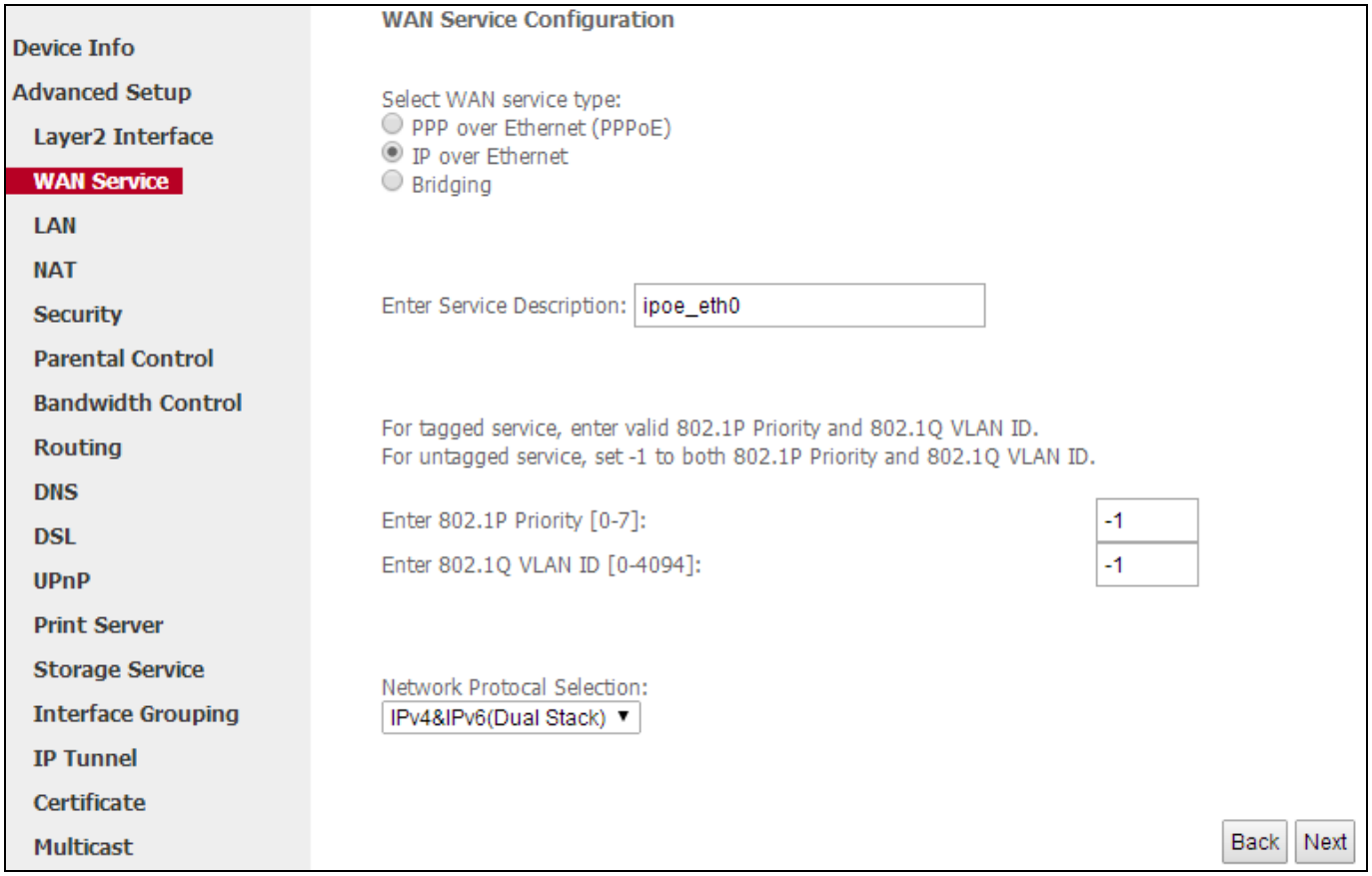
❶ Click **Advanced Setup** > **WAN Service** and then click the **Add** button.



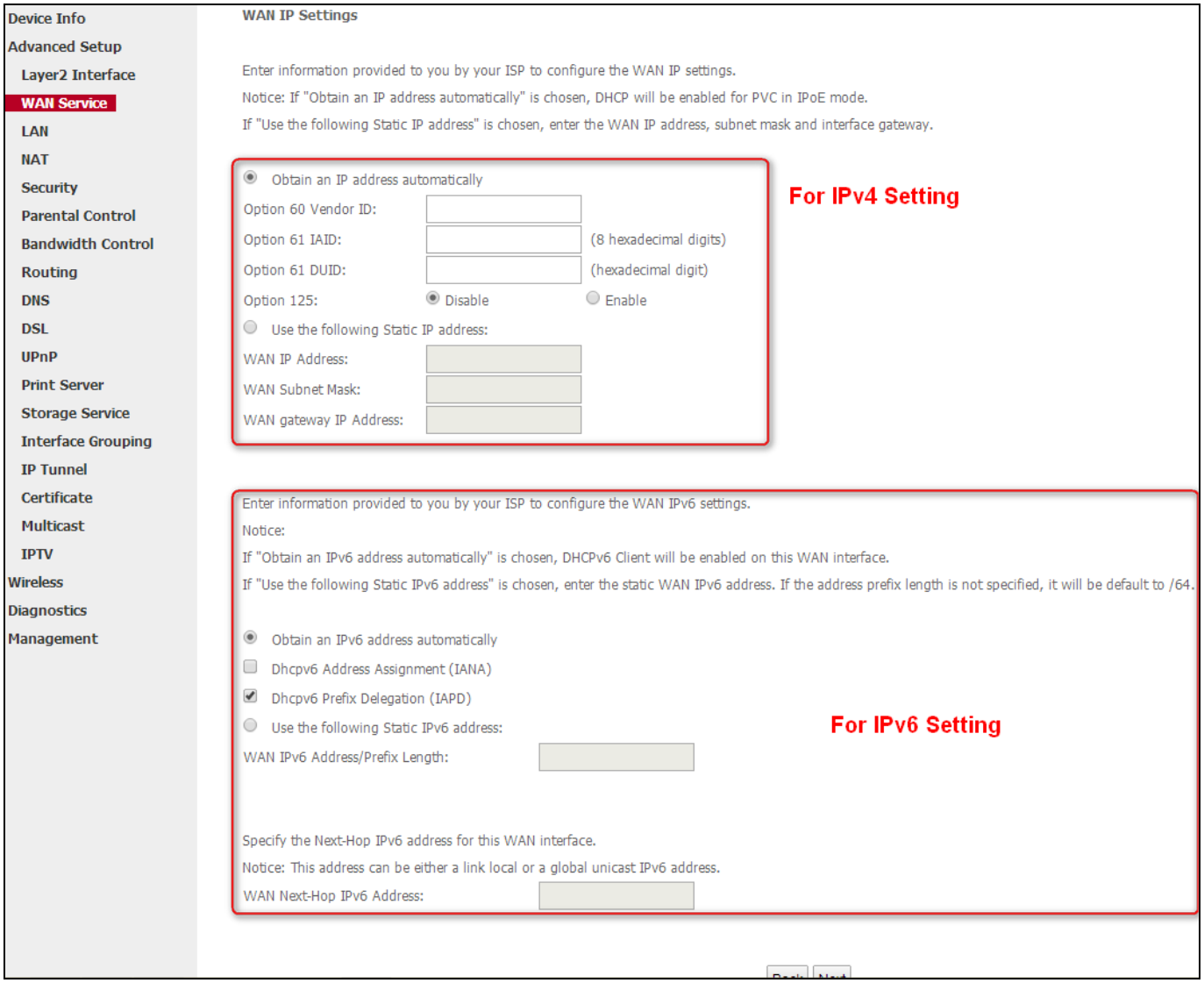
❷ Select the ATM interface you added just now from the pull-down menu in the figure below. Click **Next**.



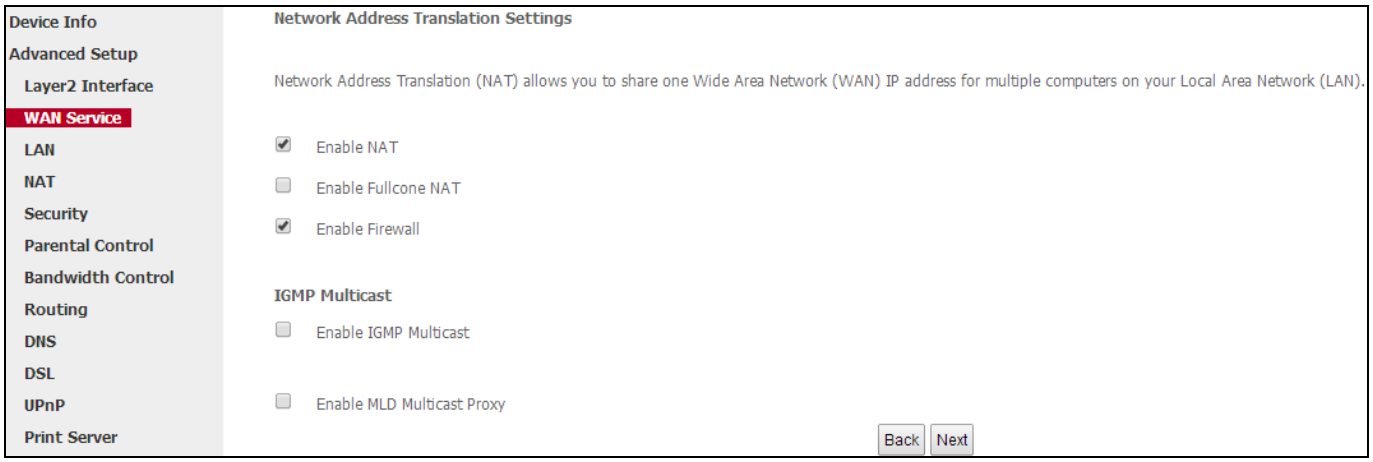
❸ Select **IP over Ethernet (IPoE)**.. Edit the **Enter Service Description** field which is optional. Suggest you keep the default. Select a network protocol you need: **IPv4&IPv6 (Dual Stack)**. Click **Next**.



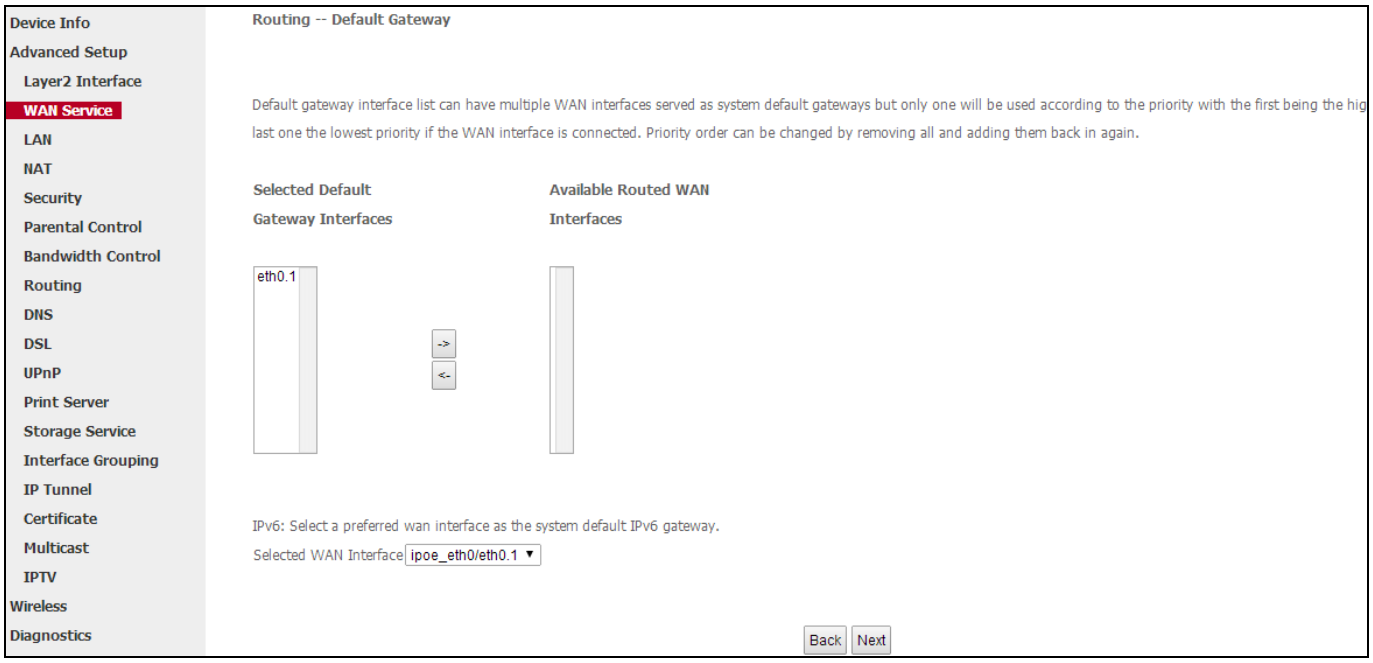
❹ To finish WAN IP Settings, select **Obtain an IP/IPv6 address automatically**, check **Dhcpv6 Prefix Delegation (IAPD)**. If your ISP is using stateful DHCPv6, check **Dhcpv6 Address Assignment (IANA)** also. Or select **Use the following Static IP/IPv6 address** if your ISP provide you with an IPv6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



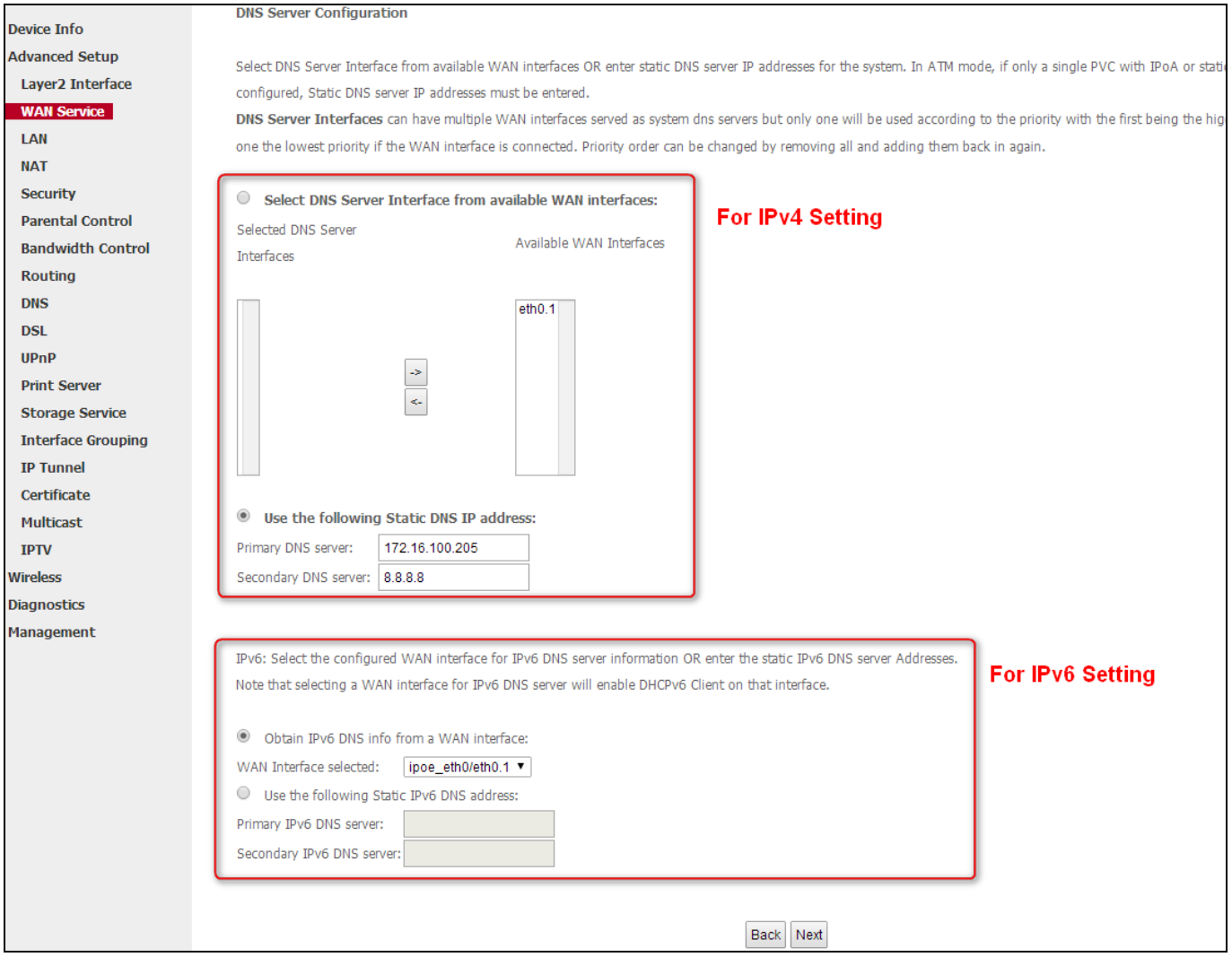
❺ Finish Network Address Translation Settings. Suggest to keep the default settings. Click **Next**.



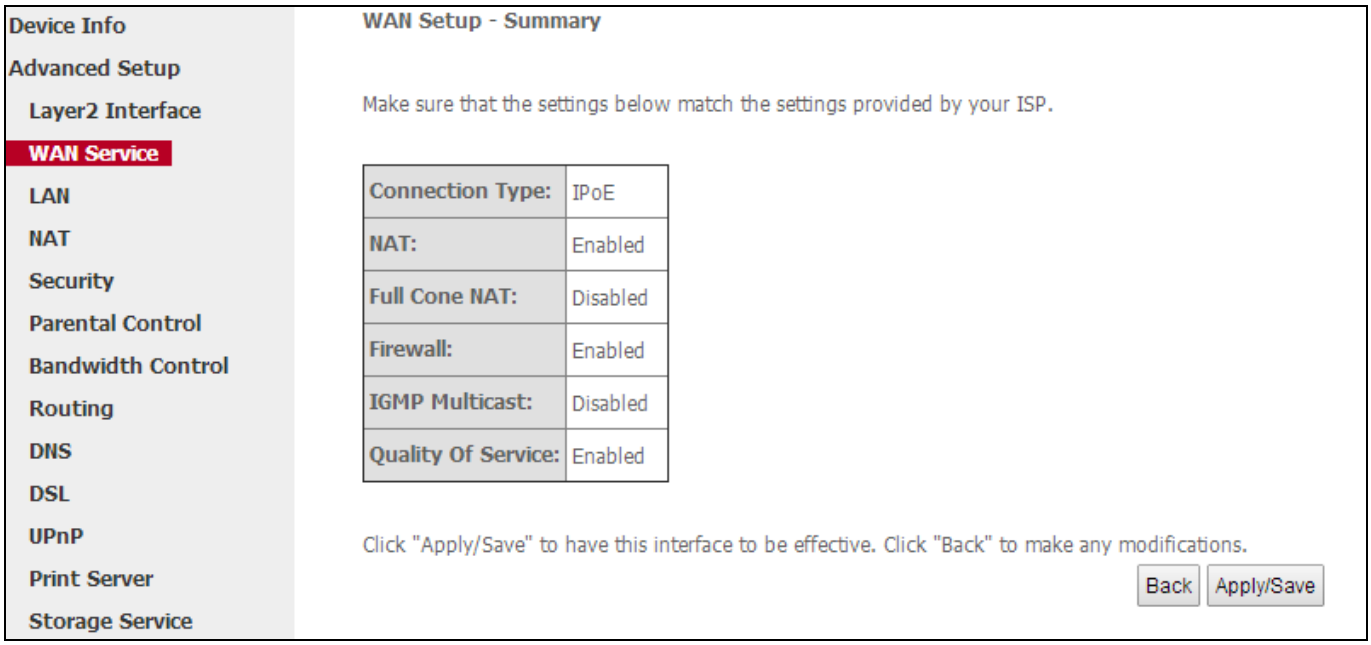
❻ To configure the Default Gateway interface, select the interface that you want to configure with the WAN gateway address. Then click **Next**.



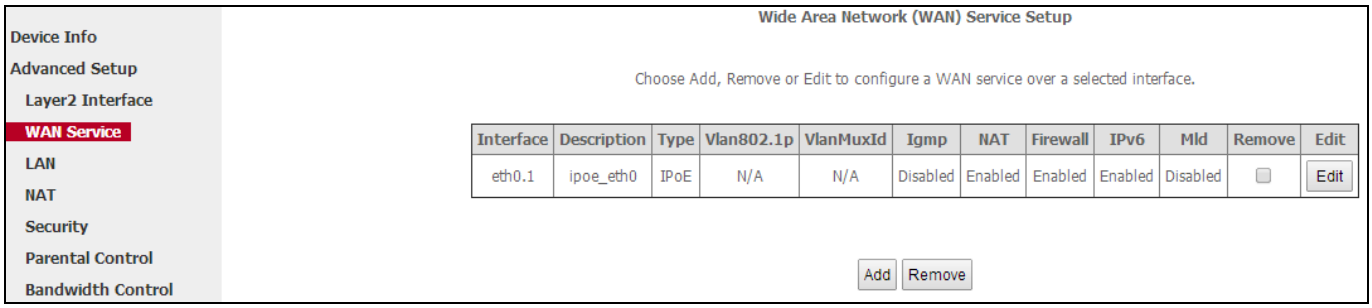
❼ To configure the WAN DNS address, finish both the IPv4 setting and IPv6 setting. Click **Next**.



Click **Apply/Save** to save your settings if everything is correctly set.



Here you can view your configurations. When the IPoE connection is successful, you can access the Internet.

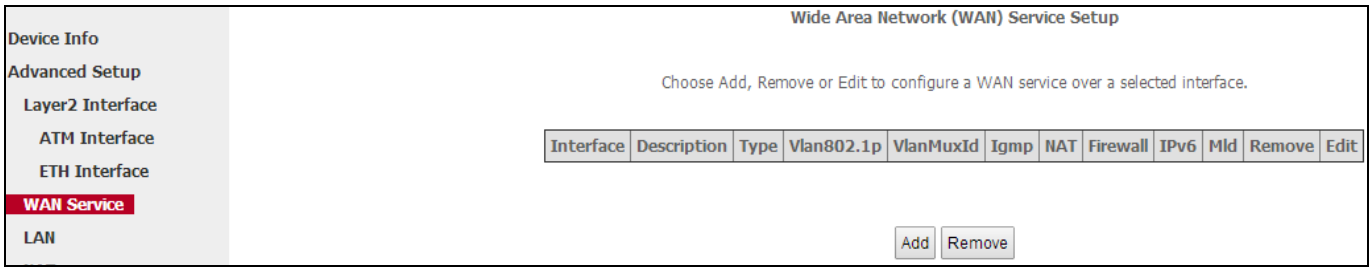


↗ Steps 1~7 above for **IPoE and IPv4&IPv6 (Dual Stack)** Users

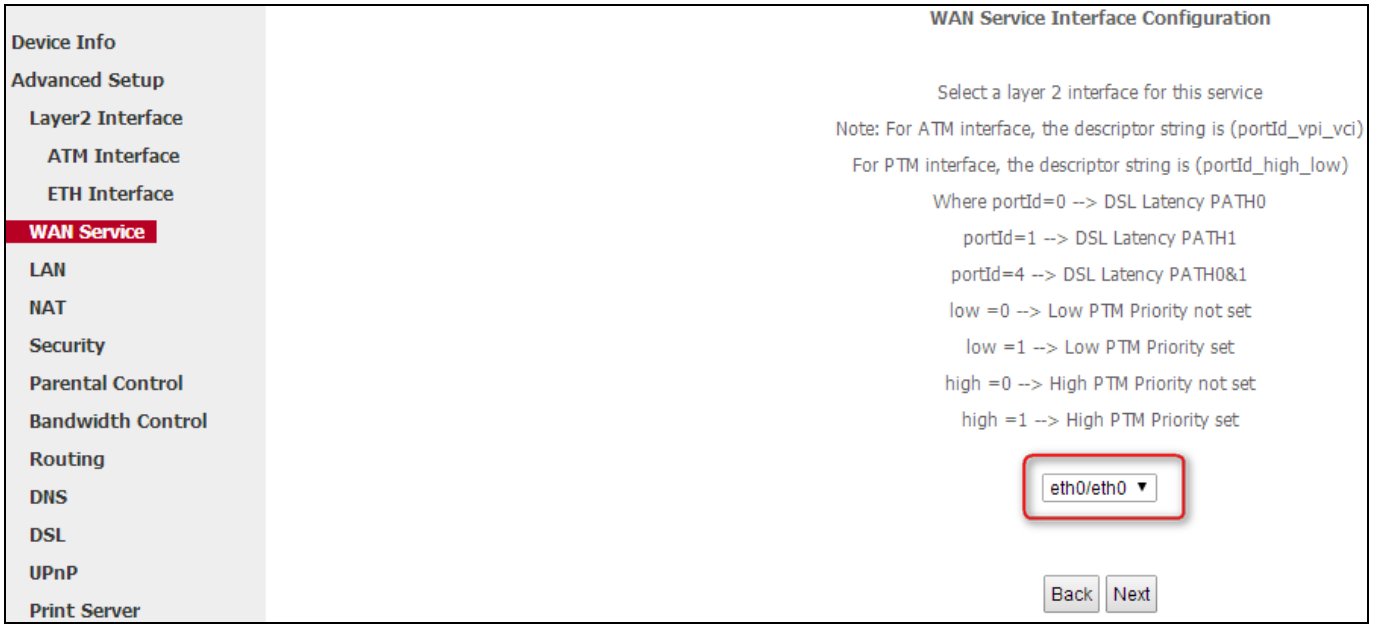
6) IPoE IPv6 Only Users

If you configure the **ETH Interface** (Ethernet uplink) and select **eth0/eth0** as the ETH WAN interface, then you can start to set up WAN service for accessing the Internet.

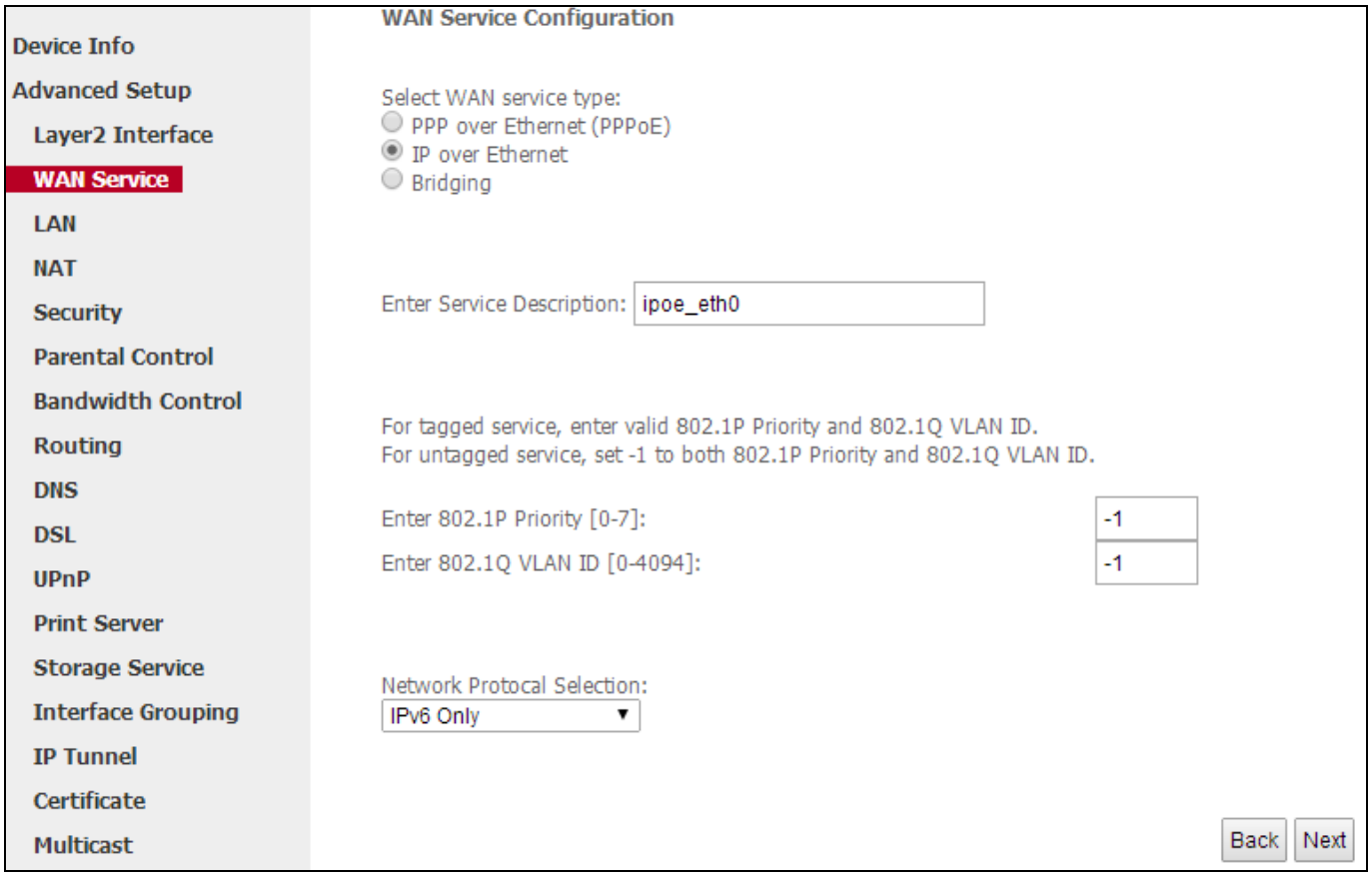
❶ Click **Advanced Setup > WAN Service** and then click the **Add** button.



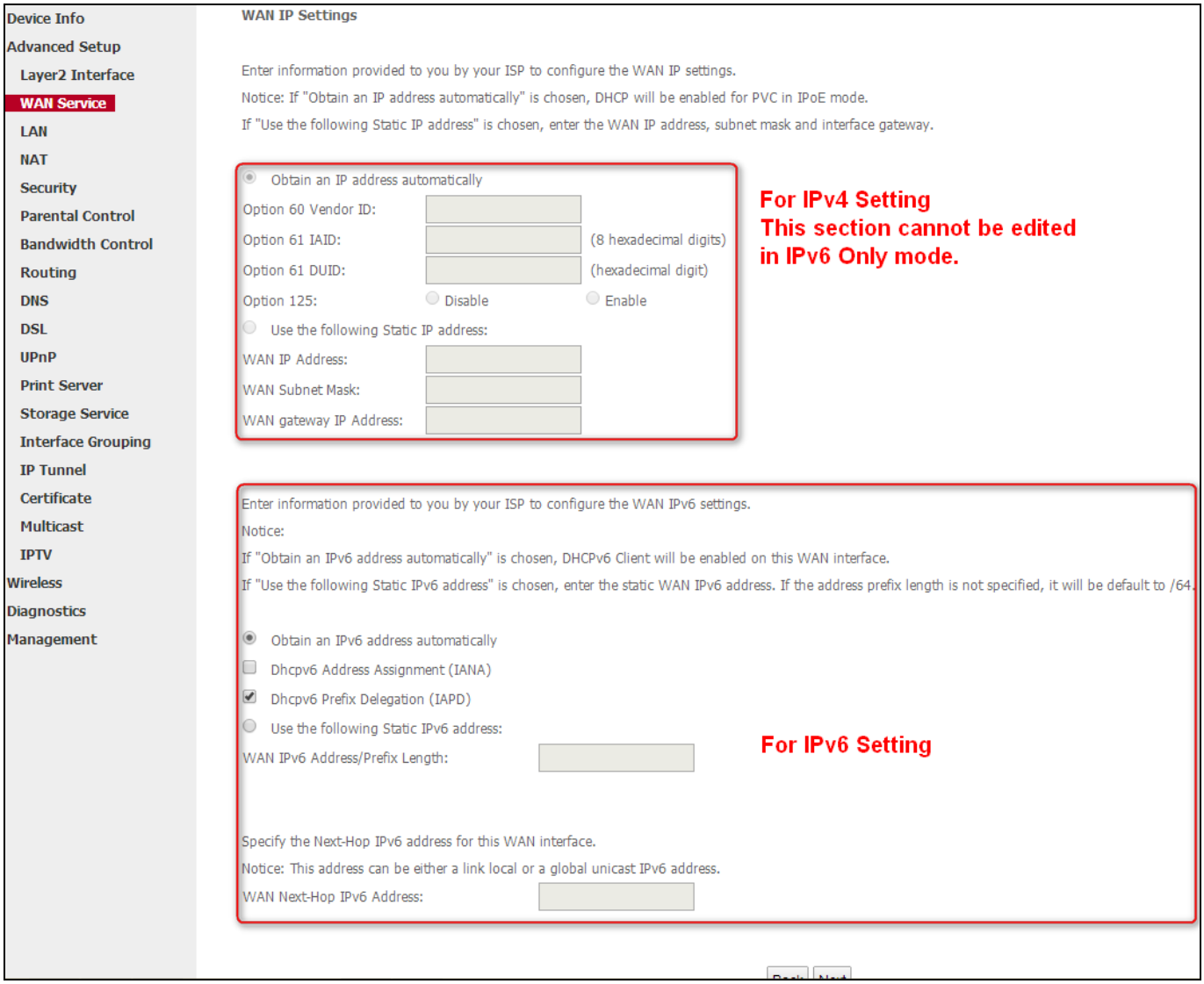
❷ Select the ETH interface you added just now from the pull-down menu in the figure below. Click **Next**.



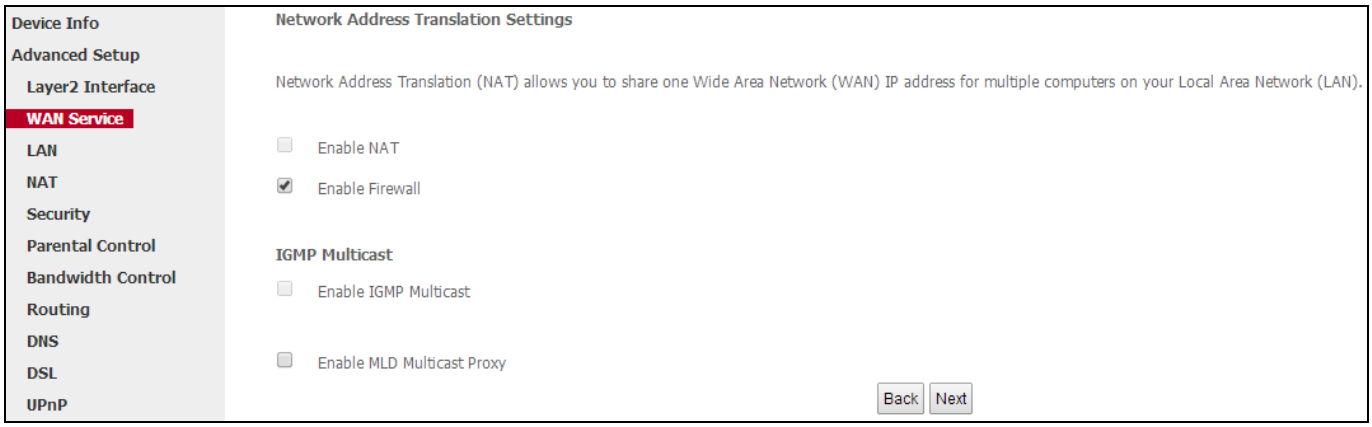
❸ Select **IP over Ethernet (IPoE)**. Edit the **Enter Service Description** field which is optional. Suggest you keep the default. Select a network protocol: **IPv6 Only**. Click **Next**.



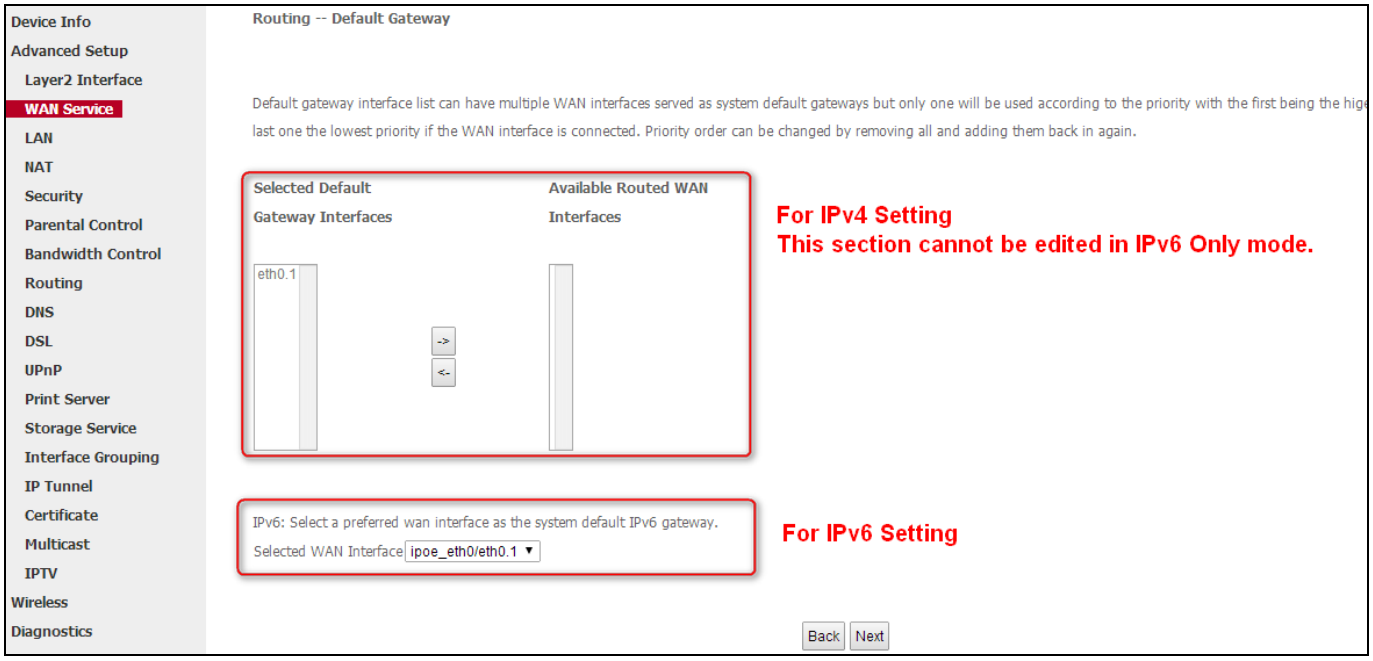
❹ Finish **WAN IP Settings** on the figure below. Click **Next**.



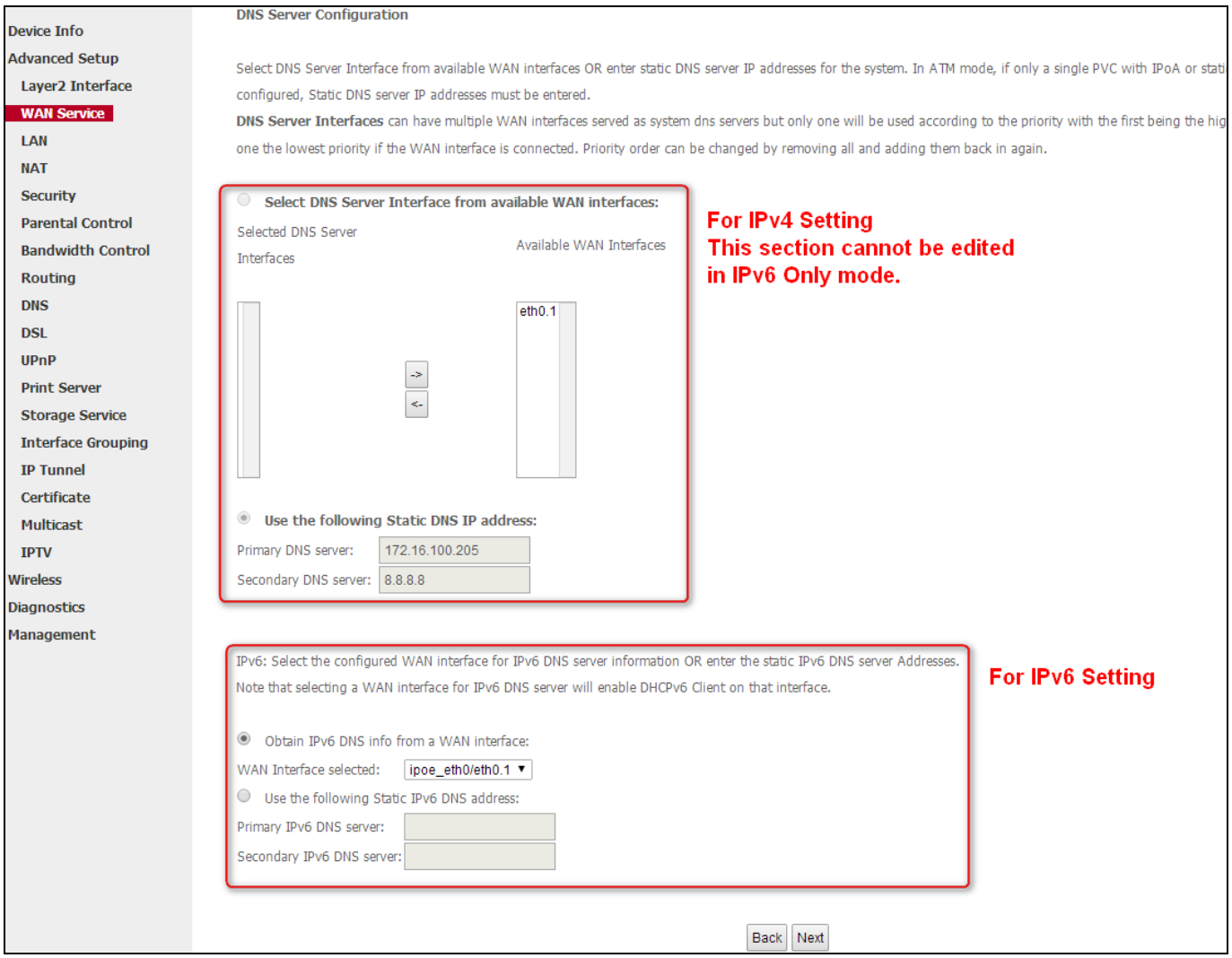
❺ Finish Network Address Translation Settings. Suggest to keep the default settings. Click **Next**.



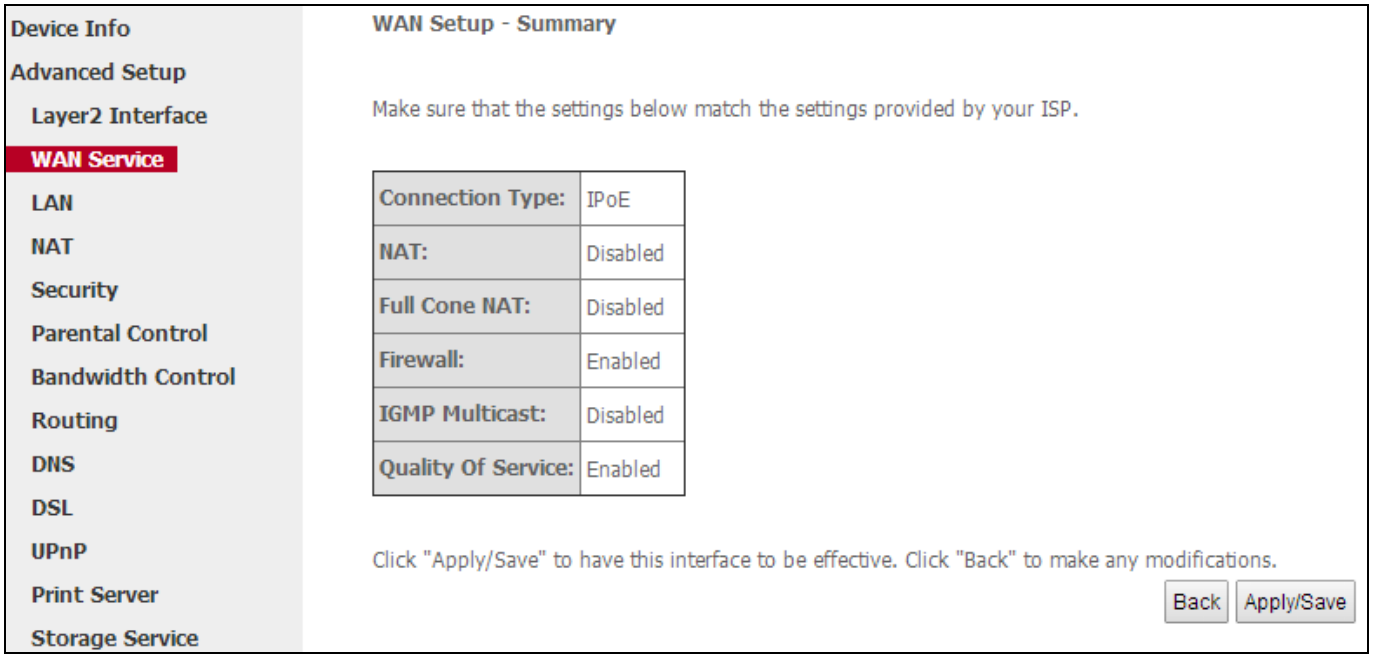
❻ To configure the Default Gateway interface when using IPv6, select the interface that you want to configure with the WAN gateway address in **Selected WAN Interface** box. Then click **Next**.



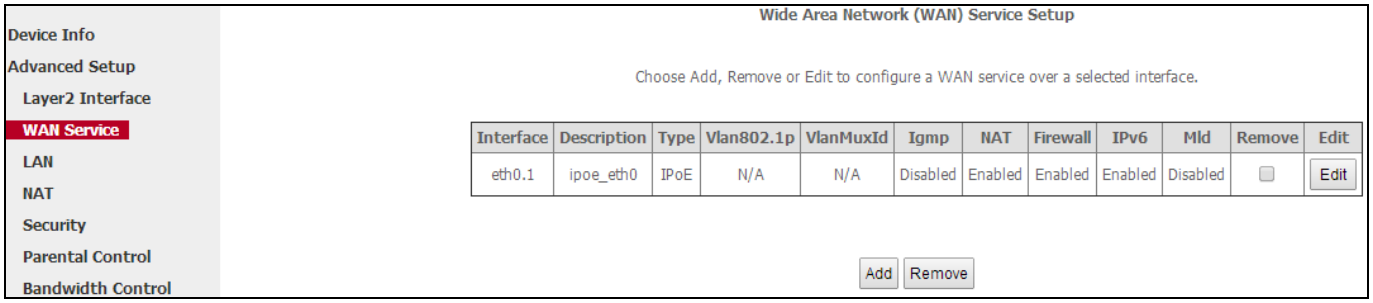
❼ To configure the WAN DNS address, check the **Obtain IPv6 DNS info from a WAN interface** option, or select the **Use the following Static IPv6 DNS address** option to enter the static DNS server IPv6 addresses provided by your ISP. At last, click **Next**.



Click **Apply/Save** to save your settings if everything is correctly set.



Here you can view your configurations. When the IPoE connection is successful, you can access the Internet.



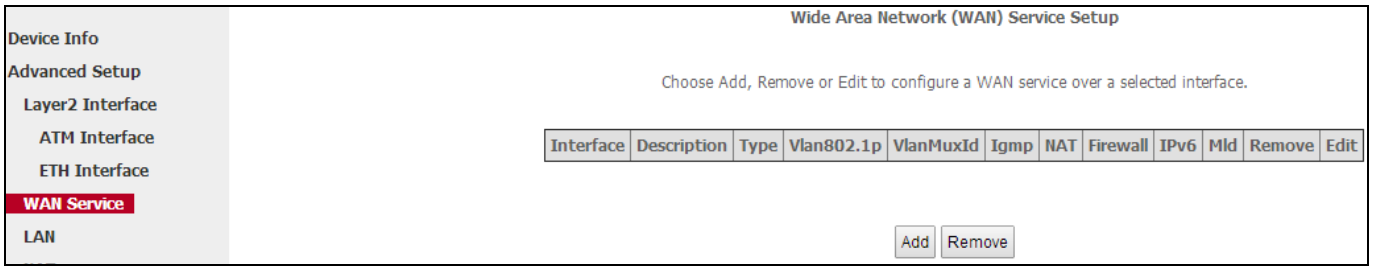
↗ Steps 1~7 above for **IPoE and IPv6 Only** Users

7) Bridging

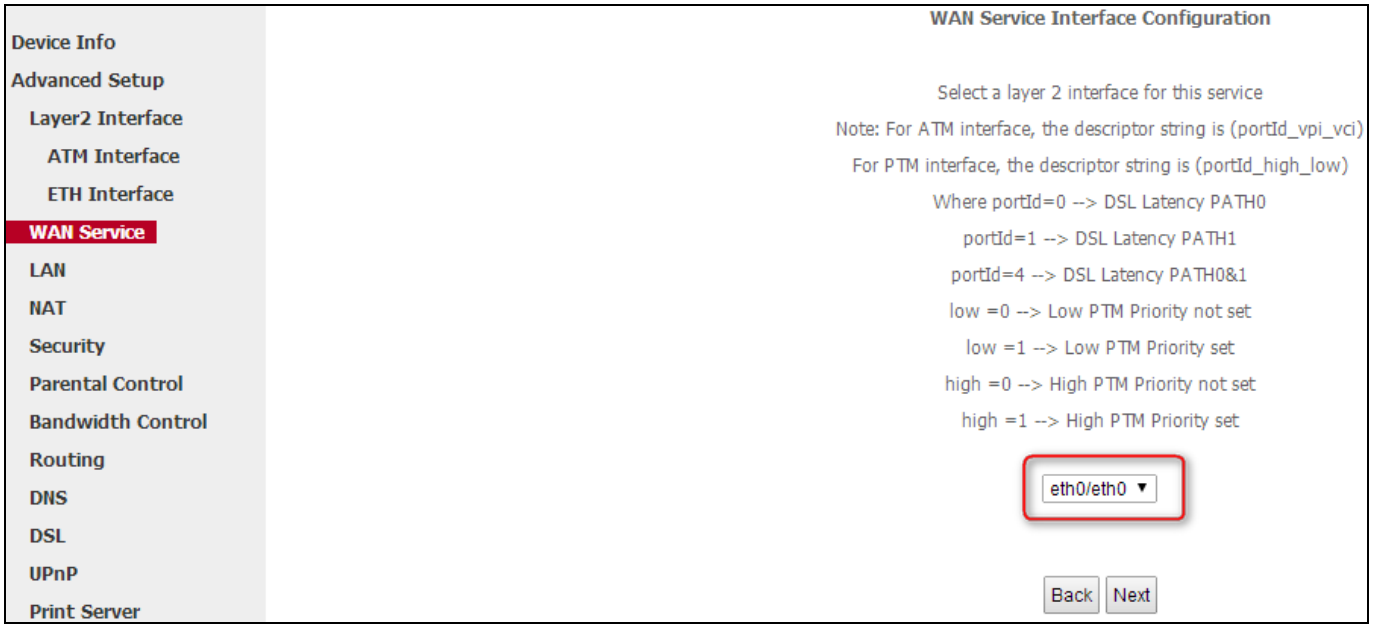
If you wish to initiate a dialup directly from your PC for Internet access or enjoy the entire Internet connection (instead of sharing it with others), you can use the Bridging DSL link type and create a dialup program on your PC.

After you configure the **ETH Interface** (Ethernet uplink) and select **eth0/eth0** as the ETH WAN interface, then you can start to set up WAN service for accessing the Internet.

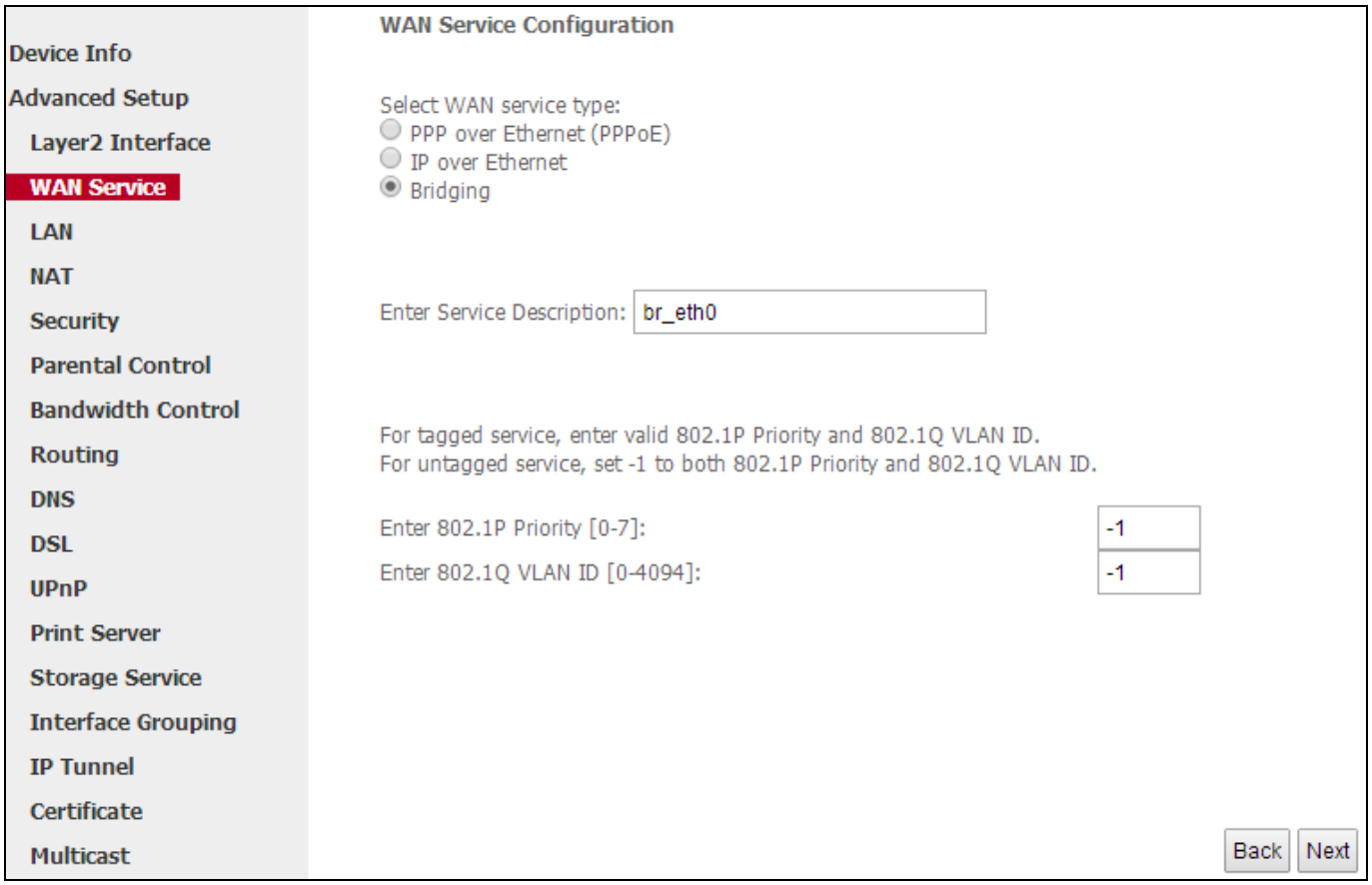
❶ Click **Advanced Setup > WAN Service** and then click the **Add** button.



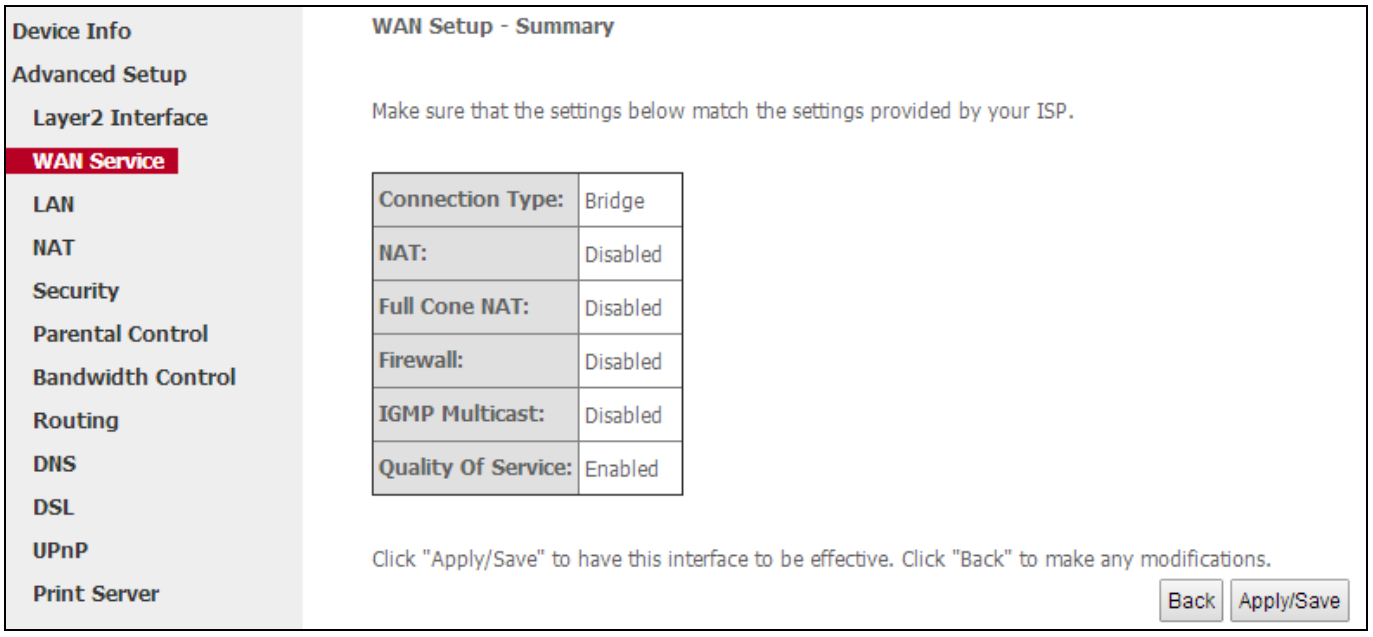
❷ Select the ETH interface you added just now from the pull-down menu in the figure below. Click **Next**.



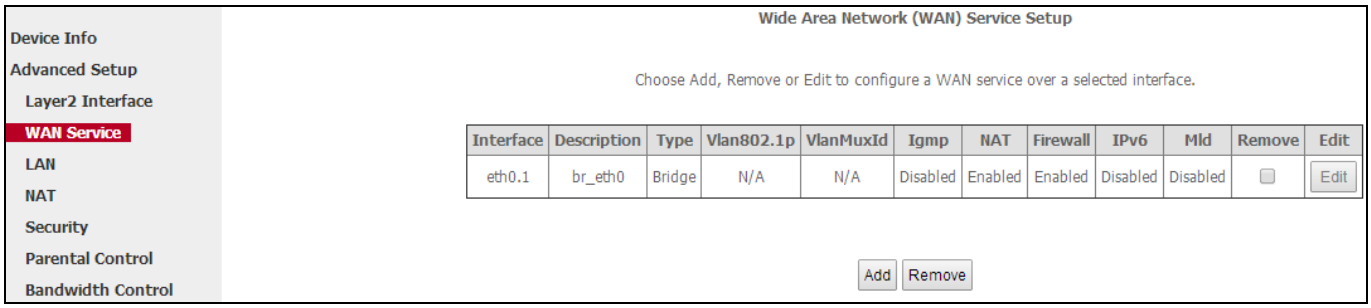
❸ Select **PPP over Ethernet (PPPoE)**. Edit the **Enter Service Description** field which is optional. Suggest you keep the default. Select a network protocol: **IPv4 Only**. Click **Next.**



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



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



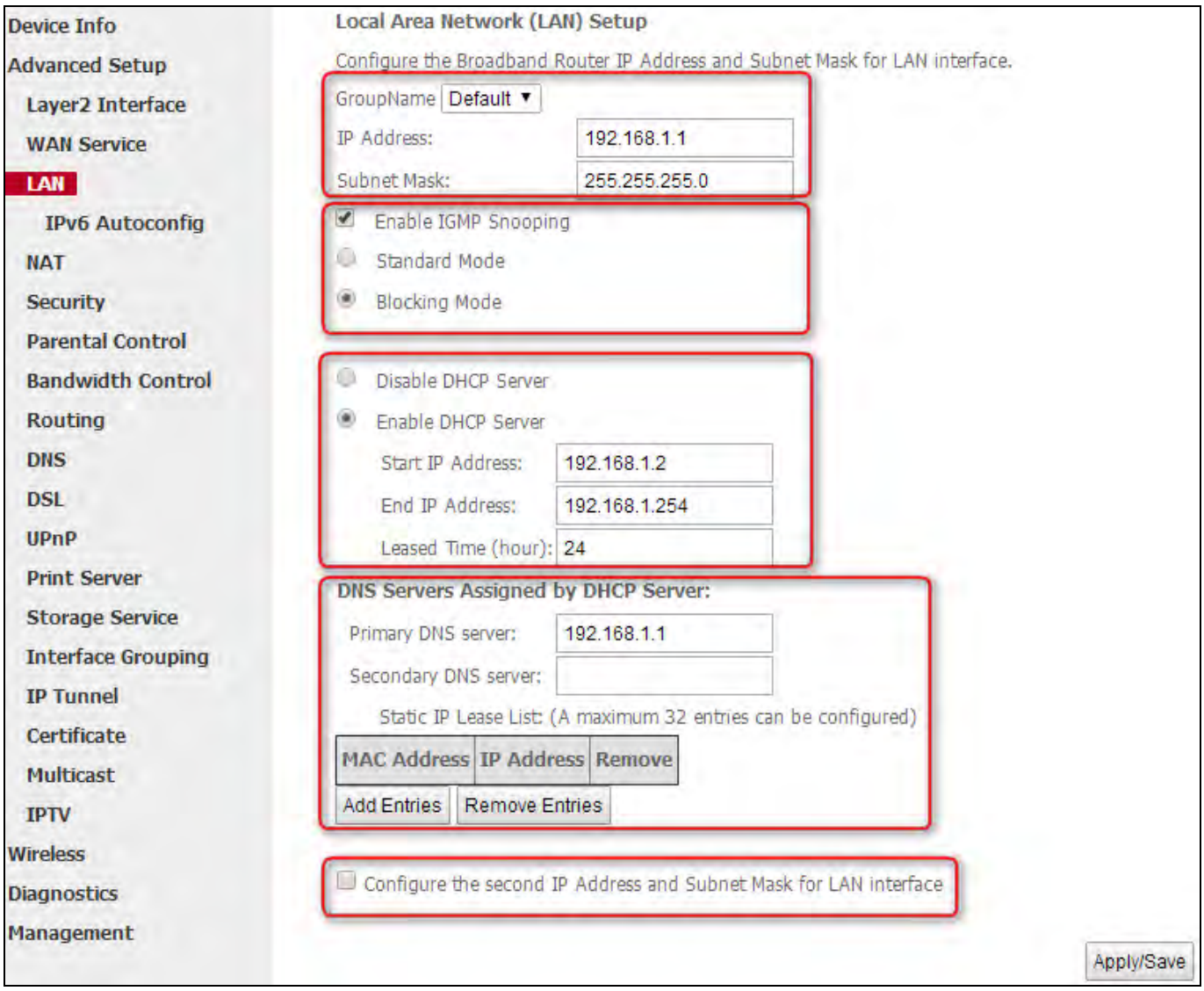
↗ Steps 1~3 above for **Bridging** Users

2.3 LAN

Click **Advanced** > **LAN** to 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. Suggest to take a note of the IP address or subnet mask you input here.

2.3.1 IPv4

Click **Advanced** > **LAN** to enter the IPv4 address setting interface.



❶ Keep the Group Name **Default** in the pull-down menu.

❷ **IP Address/Subnet Mask:** The device's LAN IP address and subnet mask that both you can change to fit your network. The default IP address is 192.168.1.1. Once you change the LAN IP address, you need to use the new address to login to the Management page to configure the modem router.

❸ **Enable IGMP Snooping**: Check to enable the IGMP Snooping feature. IGMP Snooping is to restrain broadcast on Layer 2. Enabling IGMP snooping is good for managing and controlling IPv4 broadcasts. Suggest to select **Blocking Mode**.

- **Standard Mode:** If no members join in one broadcast group, packets of this group will be broadcasted; if there're members joining in the group, packets will be only forwarded to the LAN port where the group members exist.
- **Blocking Mode:** If no members join in one broadcast group, packets of this group will be dropped; if there's members joining in the broadcast group, packets will be only forwarded to the LAN port where the group members exist.

❹ **Enable DHCP Server:** Check to enable the DHCP Server so that every upstream device connected to your router can obtain the IP address to access the Internet. If you would like to configure every upstream device with static IP address to access the Internet, you can check **Disable DHCP Server**.

❺ **Start/End IP Address:** Specify the start/end of the range for the IP address pool in the same subnet as the router. Only enabling DHCP server can this section can be edited.

❻ **Leased Time:** A time length that the IP address is assigned to each device before it is refreshed.

❼ **Static IP Lease List:** A list of devices with reserved static IP addresses. If you prefer to configure each upstream device of your router with a static IP address for better management, you can add static IP addresses to the list.

- **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.

❽ **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. The second IP address and subnet mask have the same function as the first ones.

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

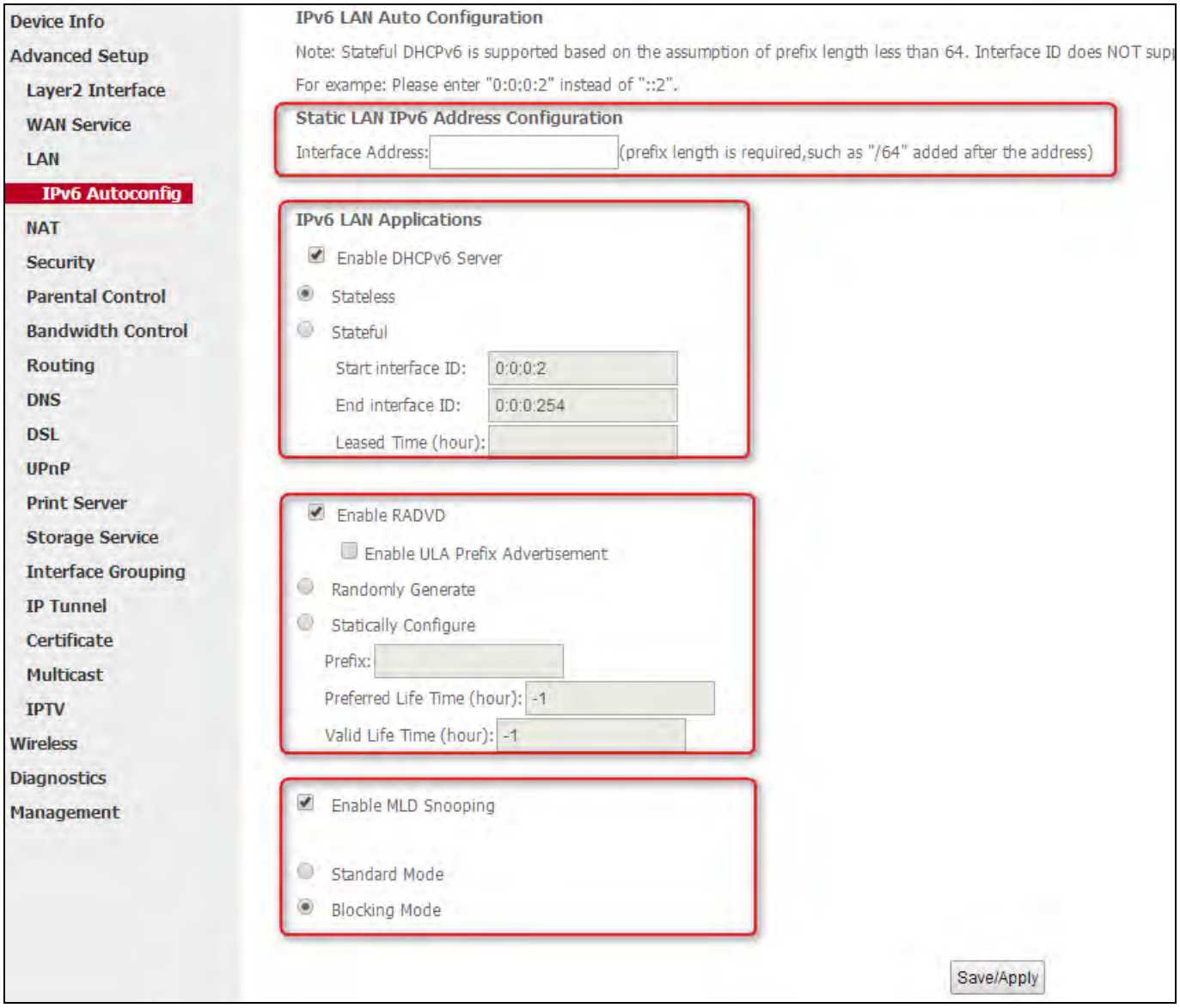
Tip

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, the router functions as a DHCP server.

2.3.2 IPv6 Autoconfig

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

Click **Advanced** > **LAN** > **IPv6 Autoconfig** to enter the IPv6 address setting page.



❶ **Interface Address**: Enter the interface address with prefix length. E.g., the interface address is “2000::1/64”, then you need to input “http://[2000::1]”.

❷ **Enable DHCPv6 Server:** Check to enable the DHCPv6 Server.

❸ Check **Stateless** or **Stateful** as you need.

- **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.

❹ **Enable RADVD:** Check it to enable the RADVD for informing computers in the LAN of your router’s existence.

When computers get the message, they will take the router's IP address as the secondary route for easy use. In addition, checking RADVD can also broadcast the prefix address generated from the computer in the LAN.

❺ **Enable IGMP Snooping**: Check to enable the IGMP Snooping feature. IGMP Snooping is to restrain broadcast on Layer 2. Enabling IGMP snooping is good for managing and controlling IPv6 broadcasts. Suggest to select **Blocking Mode**.

- **Standard Mode:** If no members join in one broadcast group, packets of this group will be broadcasted; if there're members joining in the group, packets will be only forwarded to the LAN port where the group members exist.
- **Blocking Mode:** If no members join in one broadcast group, packets of this group will be dropped; if there's members joining in the broadcast group, packets will be only forwarded to the LAN port where the group members exist.

❻ Click **Save/Apply**.

Other fields' introduction that may help:

- **Enable ULA Prefix Advertisement:** If enabled, the router will advertise ULA prefix periodically.
- **Leased Time (hour):** 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".
- **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.

2.4 NAT

2.4.1 Virtual Server

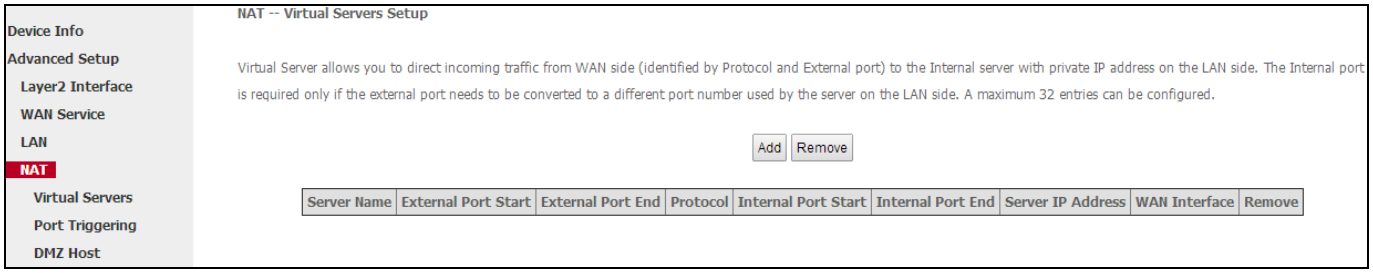
The Virtual Server is useful for web servers, ftp servers, e-mail servers, gaming and other specialized Internet applications.

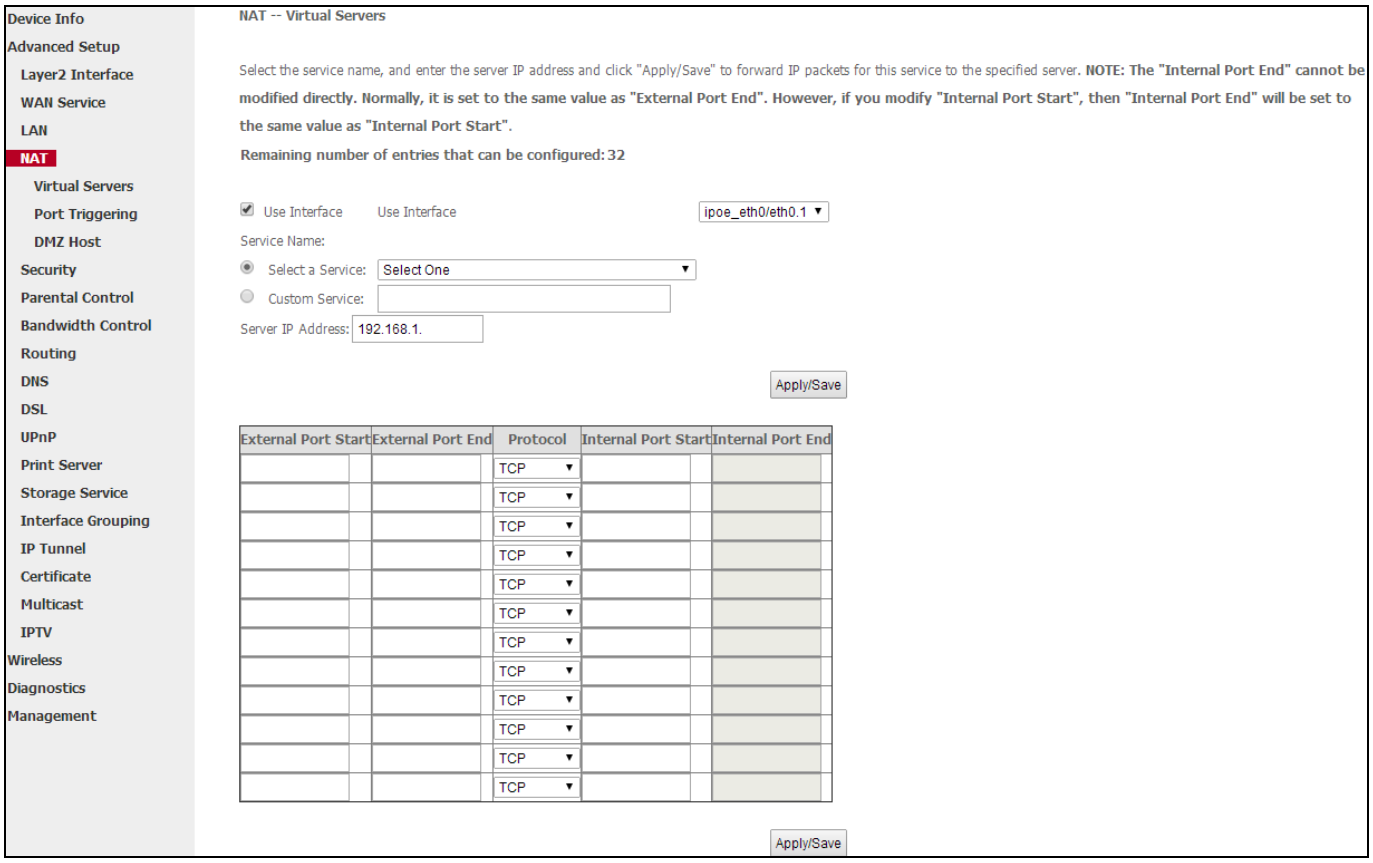
Scenario: If you have a server in the LAN, such as a website, FTP server or game server, you want e-friends to visit the

server, but the firewall and NAT function of your router stop visitors from accessing computers in the LAN.

Solution: Set virtual server rules to allow visitors to access the server via WAN IP address of your router.

Click **Advanced Setup > NAT > Virtual Servers** to enter the virtual server setup page. Click **Add** to add rules.





❶ **User Interface:** Select the WAN interface you will use to visit the server in your LAN.

❷ Configure the **Service Name > Select a Service option** to select an existing service (**Select One** here is only an express to tell you select one service.) from the drop-down list. And then the corresponding external/internal start/end port will prompt automatically. Or configure **Service Name** > **Custom Service** to customize a service manually.

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

❹ Click **Apply/Save** next to the **Server IP Address** or click **Apply/Save** next to the port number table.

Other fields' introduction that may help:

External Port Start/External Port End: Server ports provided for Internet users accessing the LAN.

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

Internal Port Start/Internal Port End: The ports used by the server in the LAN.

After all the configurations, visitors on the Internet can access your server by simply using “Protocol Name://WAN IP address: External Port”.

Note

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

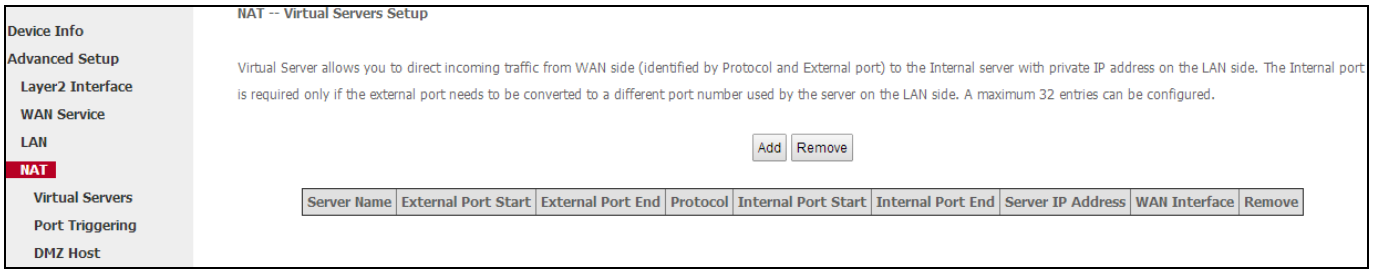
Application Scenario:

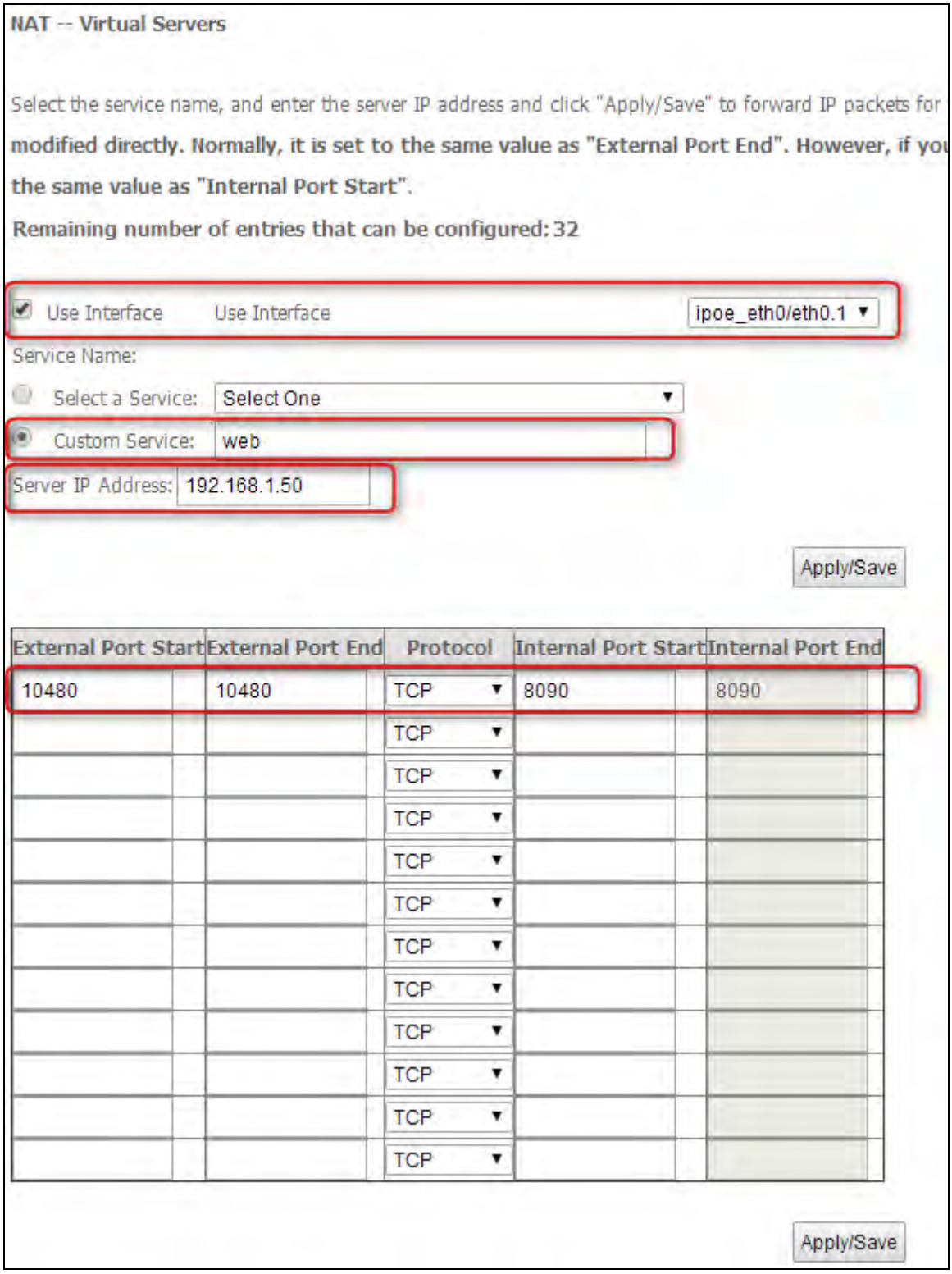
You have set up one web server on the LAN. Web server——IP: 192.168.1.50, TCP port: 8090.

Now you hope friends on the Internet can access your web by **Port 10480** through WAN port. WAN port——ipoe_eth1, IP: 1.2.3.4

Configuration Steps:

Click **Advanced Setup** > **NAT** > **Virtual Server** to enter it and then click the **Add** button.





❶ Select the WAN interface **ipoe_eth/eth0.1** here.

❷ Input the word **web** in the **Custom Service** field. Then manually enter the port number 10480 in the **External Port Start** and **External Port End** fields, and enter the port number 8090 in the **Internal Port Start** and **Internal Port End** fields. Actually port in the **Internal Port End** filed follows the port number in the **Internal Port Start** field automatically.

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

❹ In the **Server IP Address** field, enter the IP address of the web server: **192.168.1.50**.

❺ Click **Apply/Save** next to the **Server IP Address** or click **Apply/Save** next to the port number table.

Result:

Your friend on the Internet will be able to access your web server simply by entering “http://1.2.3.4:10480” in browser.

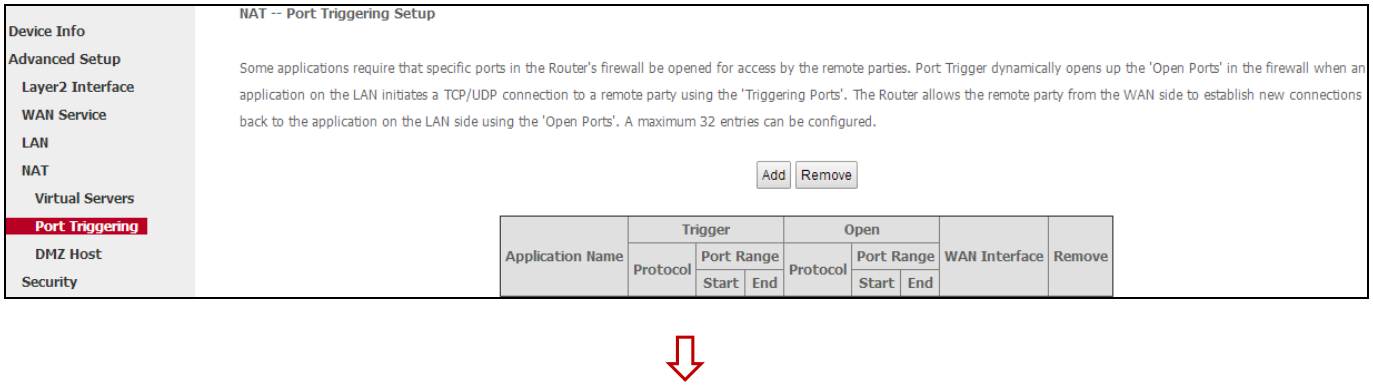
Actually if you set the DNS in 2.9, your friend can also enter http://admin name:10480 to access your web server.

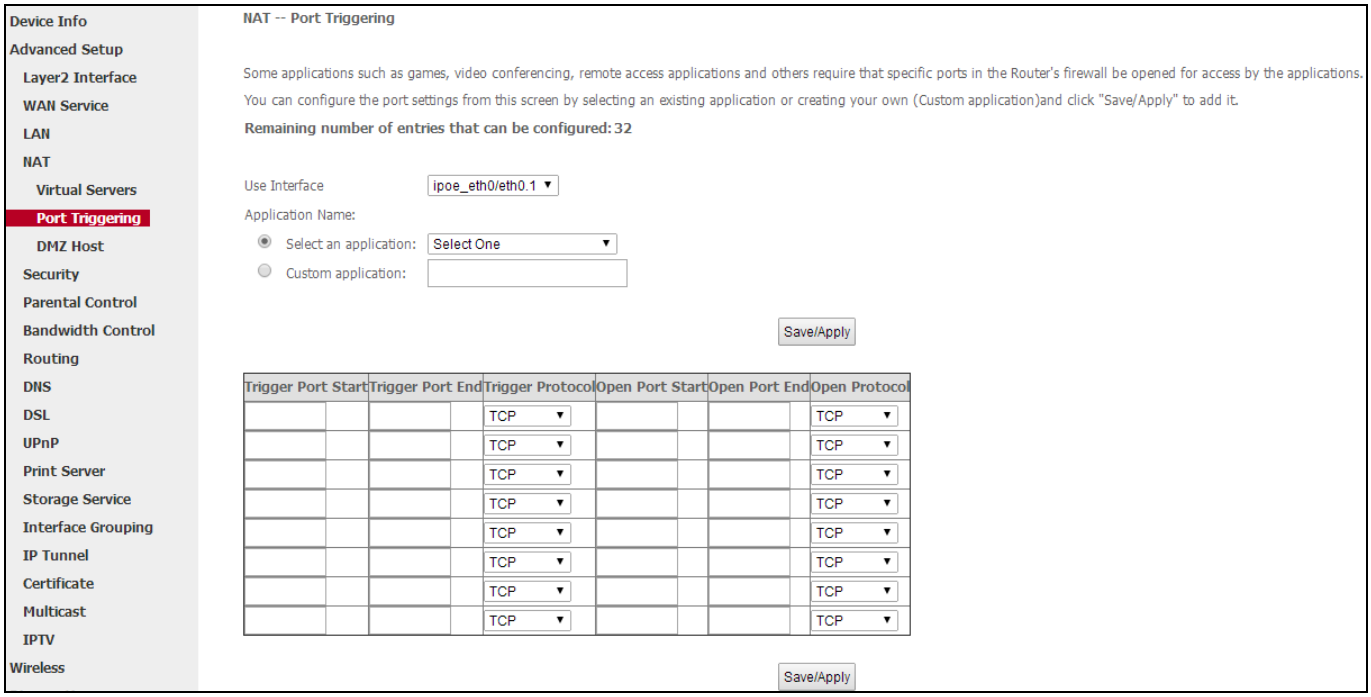
2.4.2 Port Triggering

Ports of some applications such as games, video conferencing and instant messenger, etc., are specified and meanwhile, your router’s firewall will stop messages to/from such ports, so for those applications, you cannot use them properly. However, **Port Triggering** is provided to help your play such games, or use this kind of instant messenger normally.

Some safety system applications (like, safe guard and firewall) in the computer on the LAN may interfere with the Port triggering function. When using Port triggering, you can disable such applications.

Click **Advanced Setup > NAT > Port Triggering** and then click the **Add** button to add rules.





Here in the **Port Triggering** interface, you can configure the port settings by selecting an existing application or creating your own (Custom application).

❶ **User Interface:** Select the WAN interface you will use to visit the server in your LAN.

❷ Configure the **Application Name > Select an application** to select an existing application (**Select One** here is only an express to tell you select one application.) from the drop-down list. And then the corresponding trigger start/end port will prompt automatically. Or configure **Application Name** > **Custom application** to customize an application manually.

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

❹ Click **Save/ Apply** next to the **Custom application** or click **Save/ Apply** next to the port number table.

Other fields' introduction that may help:

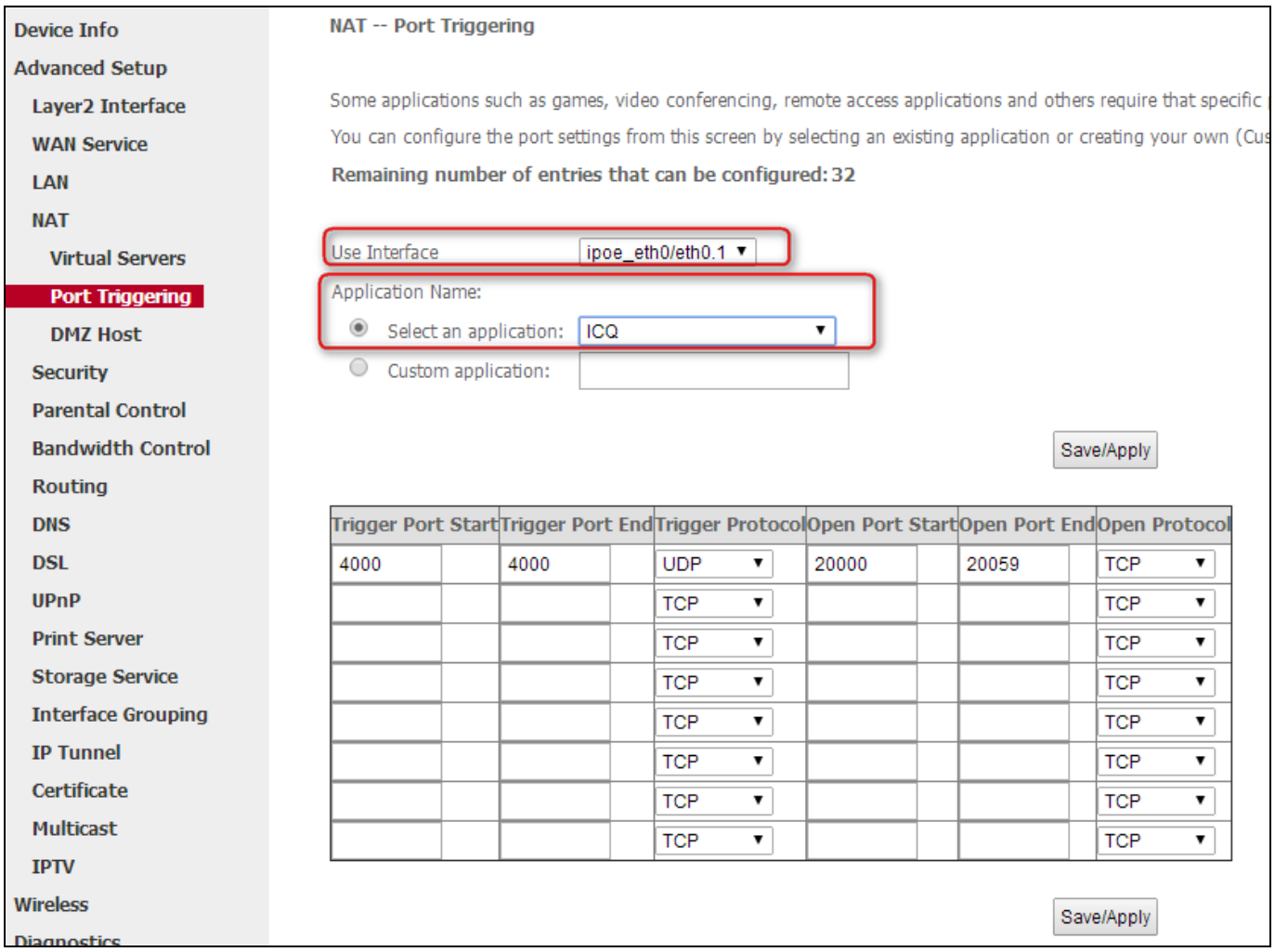
Trigger Port Start/End: The port range for an application to initiate connections.

Open Port Start/End: After the application connection is established, the built-in firewall of the router will open ports between the start port number and end port number automatically.

Application Scenario:

You always use ICQ to communicate with computers on the Internet. You hope your LAN is secure and your instant communication with other computers can be smoother. The WAN port now is ipoe_eth1.

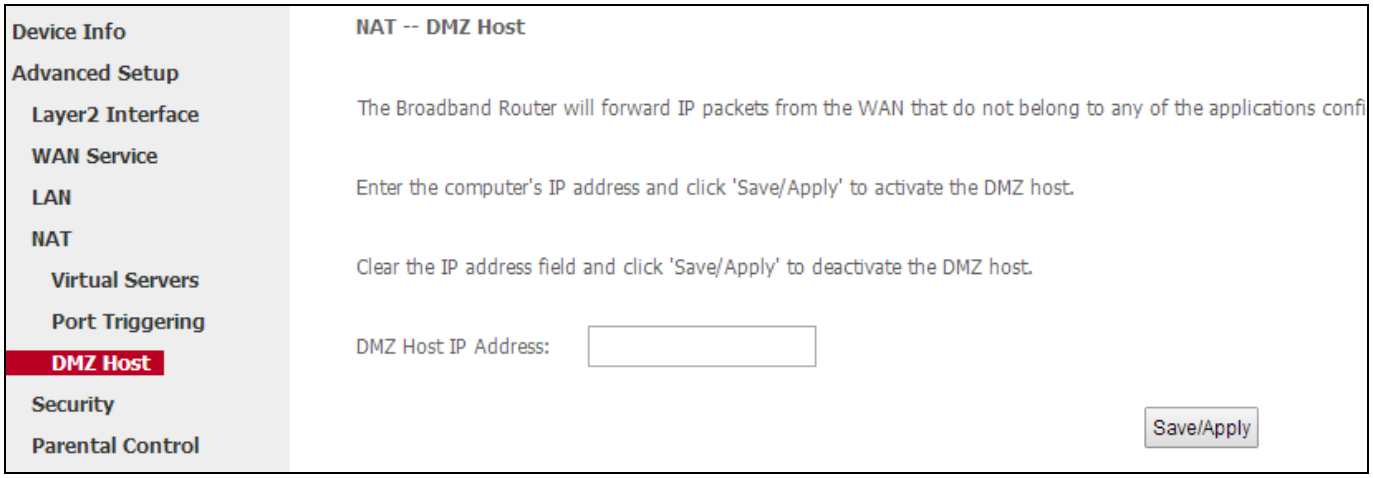
Solution:



2.4.3 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). Note that enabling DMZ host means the built-in firewall of your router takes no effect, and your computer that's set as the DMZ host will totally expose itself to the Internet. In this case, hacker may easily attack the DMZ host. Strongly recommend you to disable DMZ host and clear all the DMZ host settings as soon as possible when you do not use it.

Click **Advanced Setup** > **NAT** > **DMZ Host**, input the IP address of the computer that you want to configure as the DMZ host into the **DMZ Host IP Address** field. At last, click **Save/Apply**.



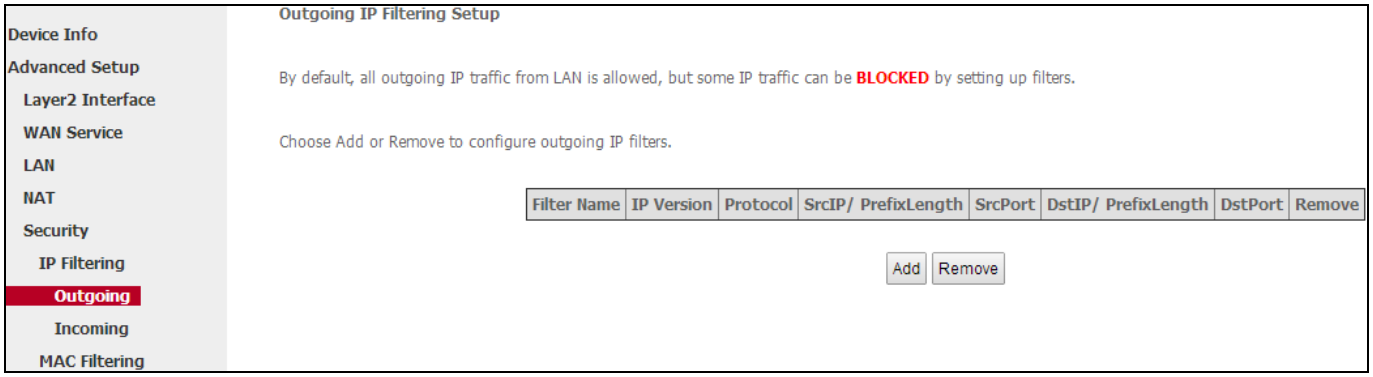
2.5 Security

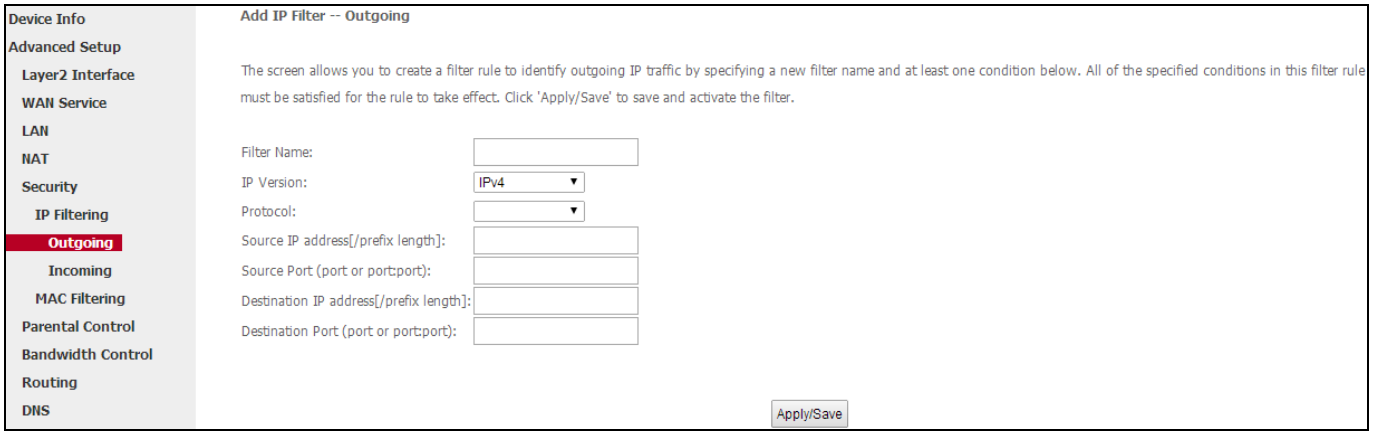
2.5.1 IP Filtering

✧ **Outgoing IP Filtering Setup**

If you want to limit computers in the LAN to access the Internet, go to **Outgoing** section to set the router.

Click **Advance Setup** > **Security** > **IP Filtering** > **Outgoing**, and then click **Add** to configure outgoing IP filters.





❶ **Filter Name:** Enter a descriptive filtering name.

❷ **IP Version:** Select IPv4.

❸ **Protocol:** TCP/UDP, TCP, UDP and ICMP are available for your option.

❹ **Source IP address [/prefix length]:** Enter the LAN IP address to be filtered.

❺ **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.

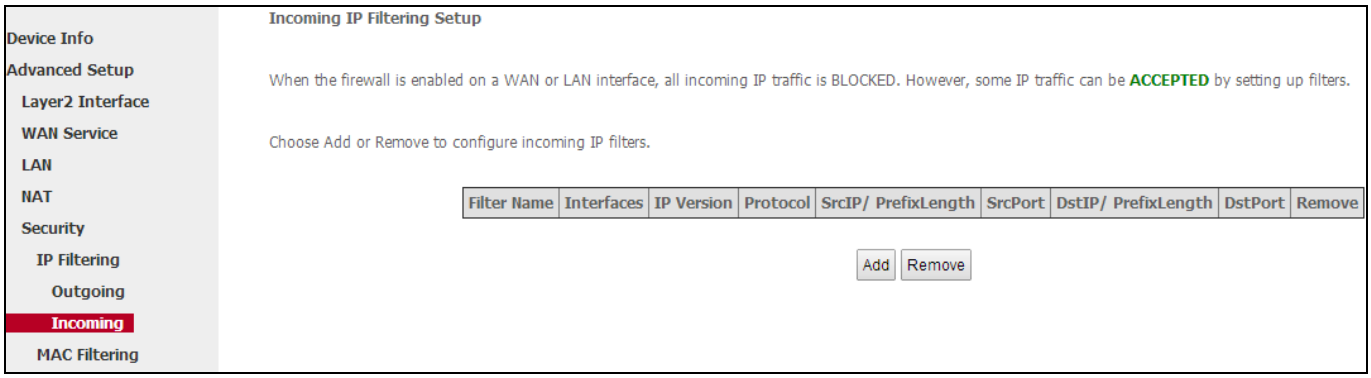
❻ **Destination IP address [/prefix length]:** Specify the external network IP address to be accessed by specified LAN PCs.

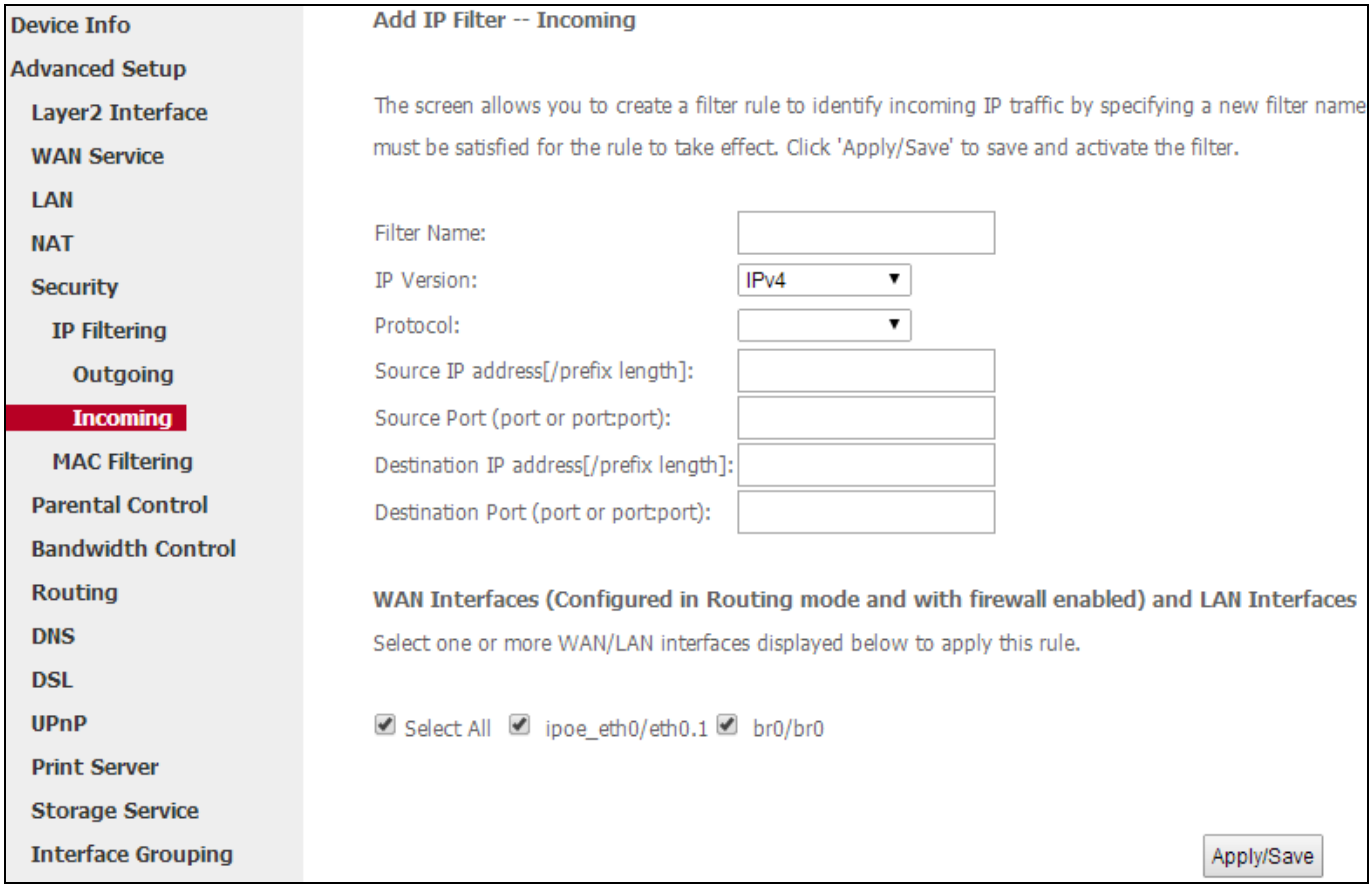
❼ **Destination Port** (port or port:port)**:** Specify a port number or a range of ports used by LAN PCs to access external network.

❽ Click **Apply/Save** to save and activate the filter.

✧ Incoming IP Filtering Setup

Click **Advance Setup** > **Security** > **IP Filtering** > **Incoming**, and then click **Add** to configure incoming IP filters.





❶ **Filter Name:** Specify a new filter name for identifying the incoming IP traffic.

❷ **IP Version:** Select either IPv4.

❸ **Protocol:** TCP/UDP, TCP, UDP and ICMP are available for your option.

❹ **Source IP address [/prefix length]:** Enter the Internal IP address [/prefix length] to be filtered.

❺ **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.

❻ **Destination IP address [/prefix length]:** Specify the internal network IP address [/prefix length] to be accessed by the specified PCs from external network.

❼ **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.

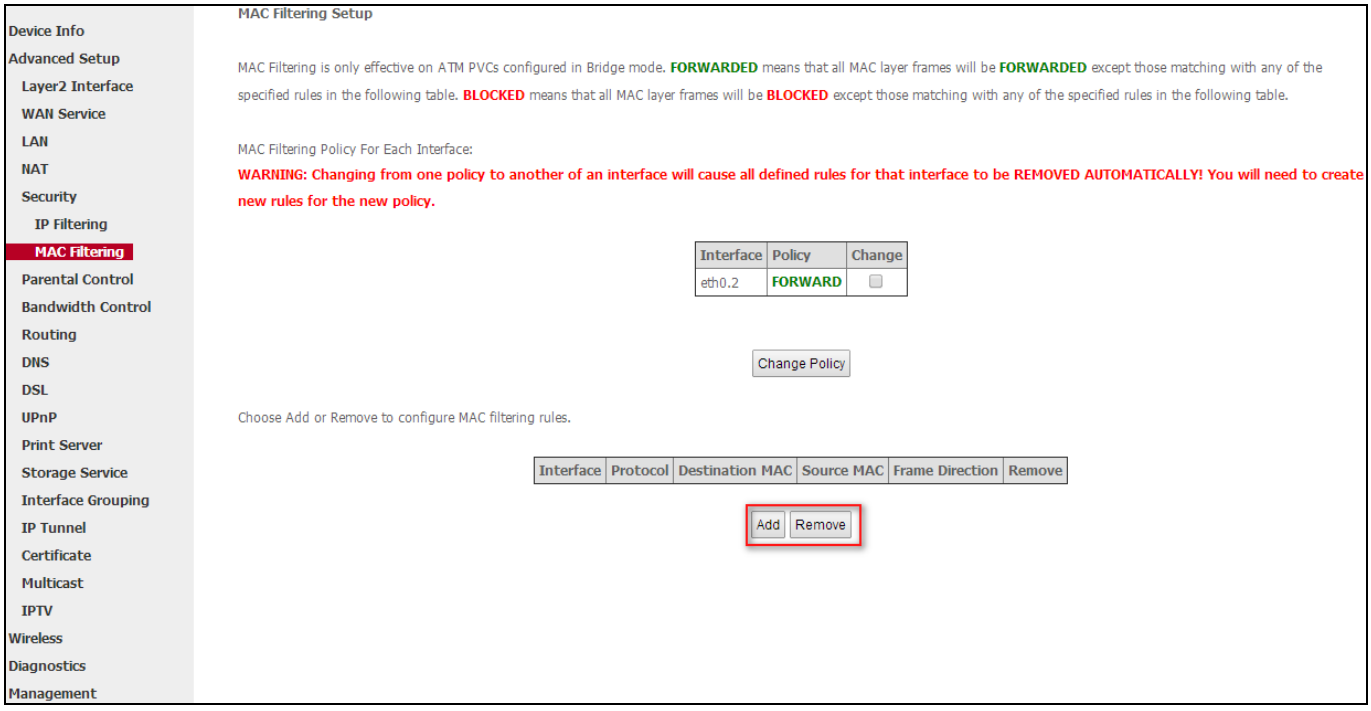
❽ Click **Apply/Save** to save and activate the filter.

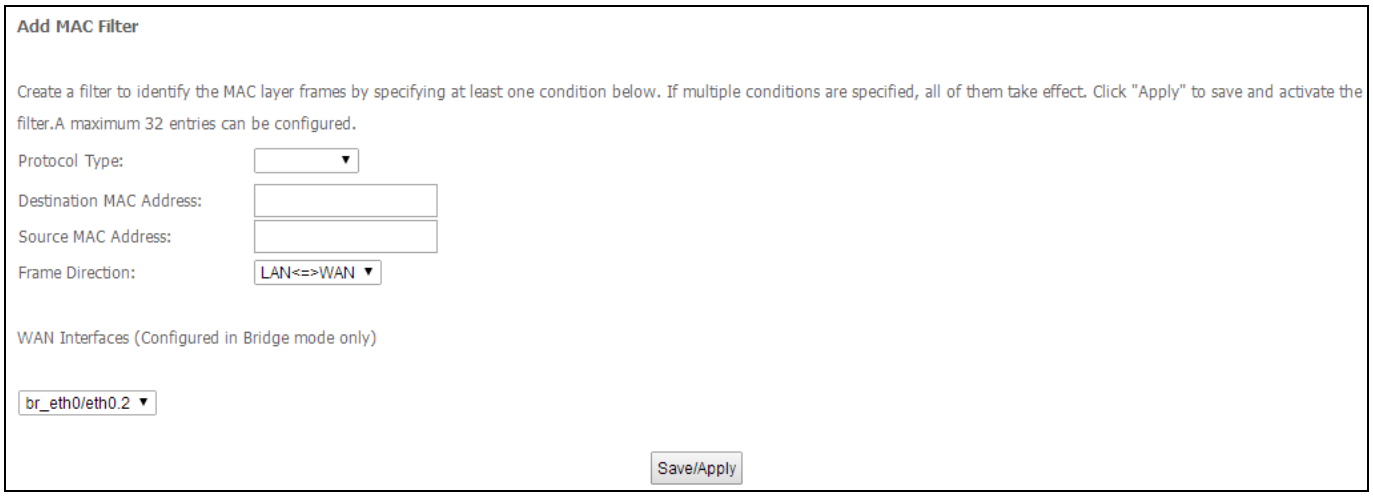
2.5.2 MAC Filtering

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** enter the following screen. (Note that 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.)





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.

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

❷ **Destination MAC Address:** Enter the destination MAC address to which you wish to apply the MAC filtering rule.

❸ **Source MAC Address:** Enter the source MAC address to which you wish to apply the MAC filtering rule.

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

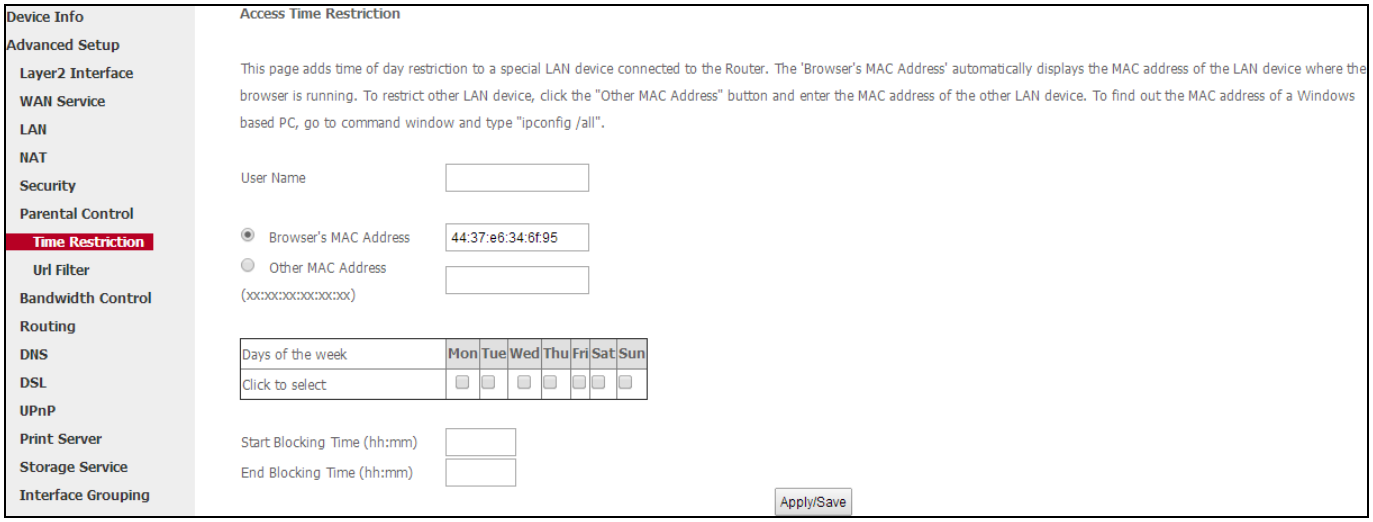
❺ **WAN Interfaces:** Select a WAN interface from the drop-down list.

❻ Click **Apply/Save** to save and activate the filter.

2.6 Parental Control

2.6.1 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.

❶ **User Name:** Enter a user name.

❷ **Browser's MAC Address:** This section will automatically add the MAC address of the attached LAN device where the browser is running.

❸ **Other MAC Address:** Specify MAC address of the computer which you want to apply Internet access restriction to.

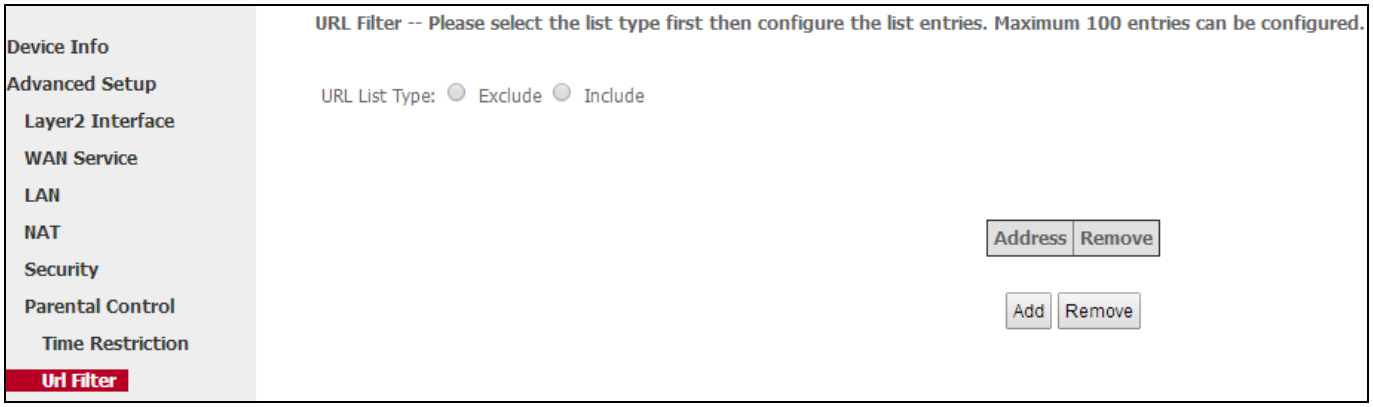
❹ **Days of the week:** Click to select the days of the week during which you wish to restrict Internet access.

❺ **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.

❻ **Apply/Save:** Click to **Apply/Save** your settings.

2.6.2 URL Filter

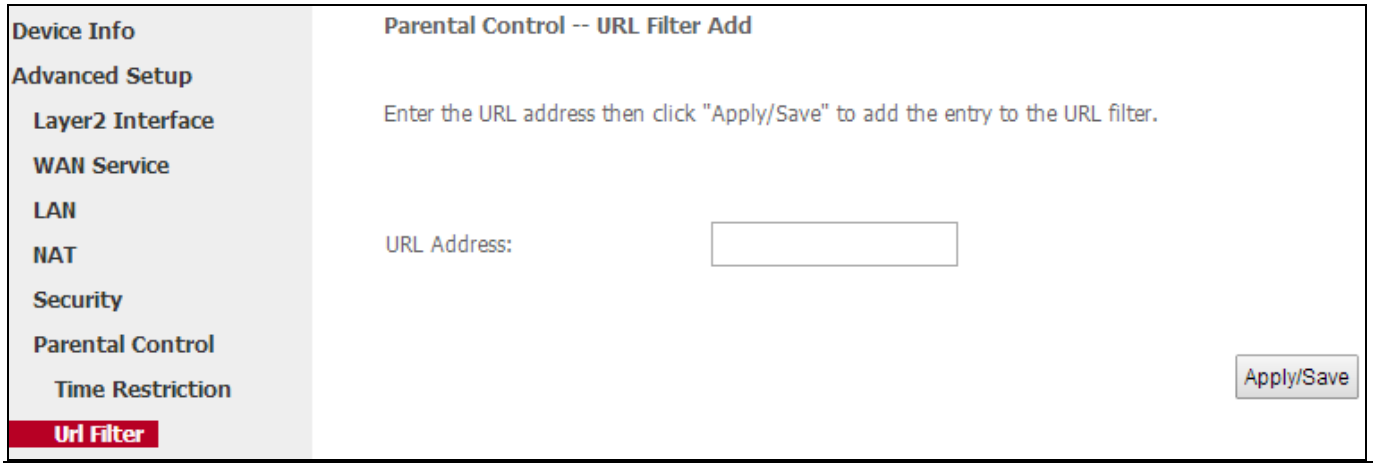
Click **Parental Control > Url Filter** to enter the following screen.



❶ Select the **URL List Type**, Exclude or Include as you need.

- Exclude: Devices on the LAN side of your router are not allowed to access the URLs specified on the list.
- Include: Devices on the LAN side of your router are only allowed to access the URLs specified on the list.

❷ Click **Add** to add the URLs that all PCs in the device network can(not) access. Up to 100 entries can be configured.

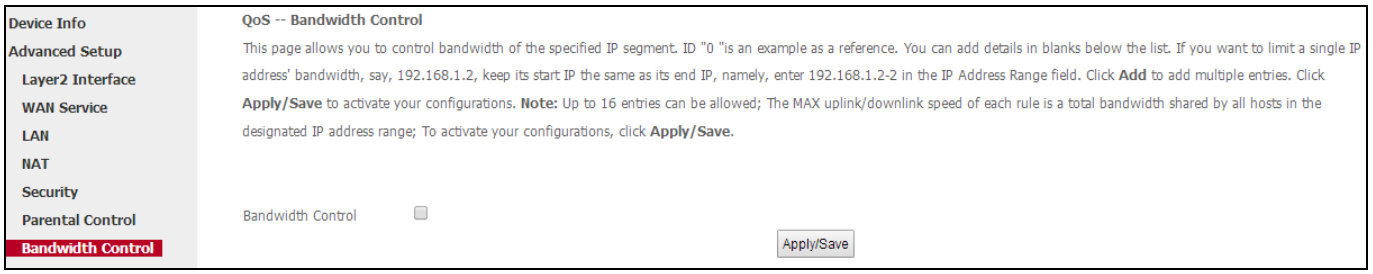


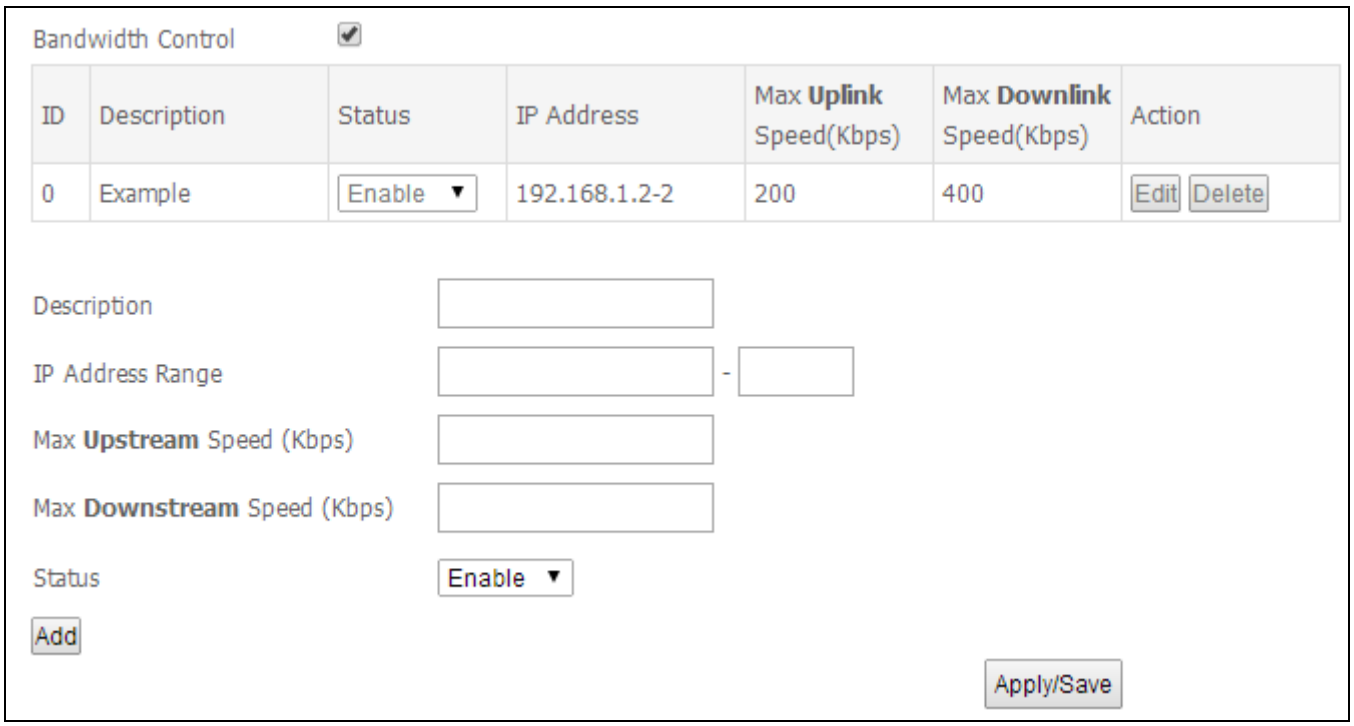
Note

If you have accessed the URL before you include it in a URL filter rule, you must reboot the modem router and erase it from your PC to activate this URL filter rule. To erase the domain name from your PC, click **Start > Run** (Windows XP for references), enter **cmd** and then type **ipconfig /flushdns**.

2.7 Bandwidth Control

Click **Advanced Setup** > **Bandwidth Control**, and check **Bandwidth Control** to enable this feature on the screen.





Up to 16 entries can be allowed.

❶ **Description:** Enter the description of the controlled host.

❷ **IP Address Range:** Enter the IP address of the host you want to control. It can be a single host or hosts. If you want to limit a single IP address's bandwidth, just keep the start IP same with the end IP. Like, 192.168.100.2-2

❸ **Max Upstream Speed (Kbps)**: Set the max upstream speed.

❹ **Max downstream Speed (Kbps)**: Set the max downstream speed.

❺ **Status:** You can change the current status of the controlled hosts, or you can select **Enable/Disable** from the drop-down list to enable/disable the current control rule.

❻ **Action:** Here display the actions you can do about the corresponding rule. There are tow actions: **Edit** and **Delete**.

- **Edit:** Click the **Edit** button corresponding to the ID to eidt its control rule. Click **OK** to apply the modification.
- **Delete:** Click the **Delete** button corresponding to the ID to delete its control rule.

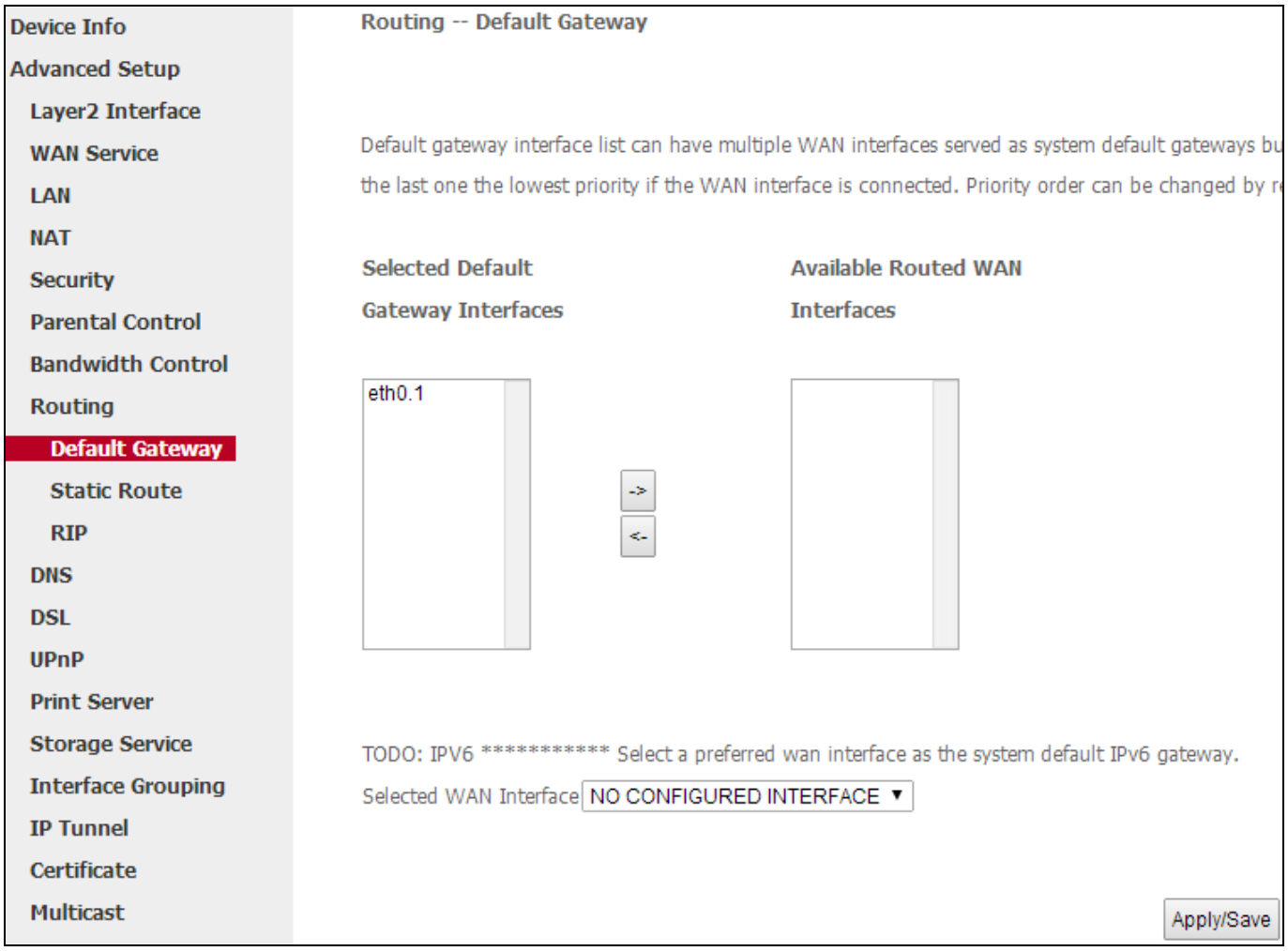
❼ **Add:** Aftre finishing the bandwidth control settings, click **Add** to generate the control rule.

❽ **Apply/Save:** Click this button to activate your configurations.

2.8 Routing

2.8.1 Default Gateway

This section is to set the default forwarding interface of the data in the same network segment of the WAN IP or LAN IP of your modem router. Click **Advanced Setup** > **Routing** > **Default Gateway** to enter this section.



❶ **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.

❷ **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.

❸ **Selected WAN Interface:** Select the current effective default IPv6 gateway interface from the pull-down menu if you use IPv6 connection.

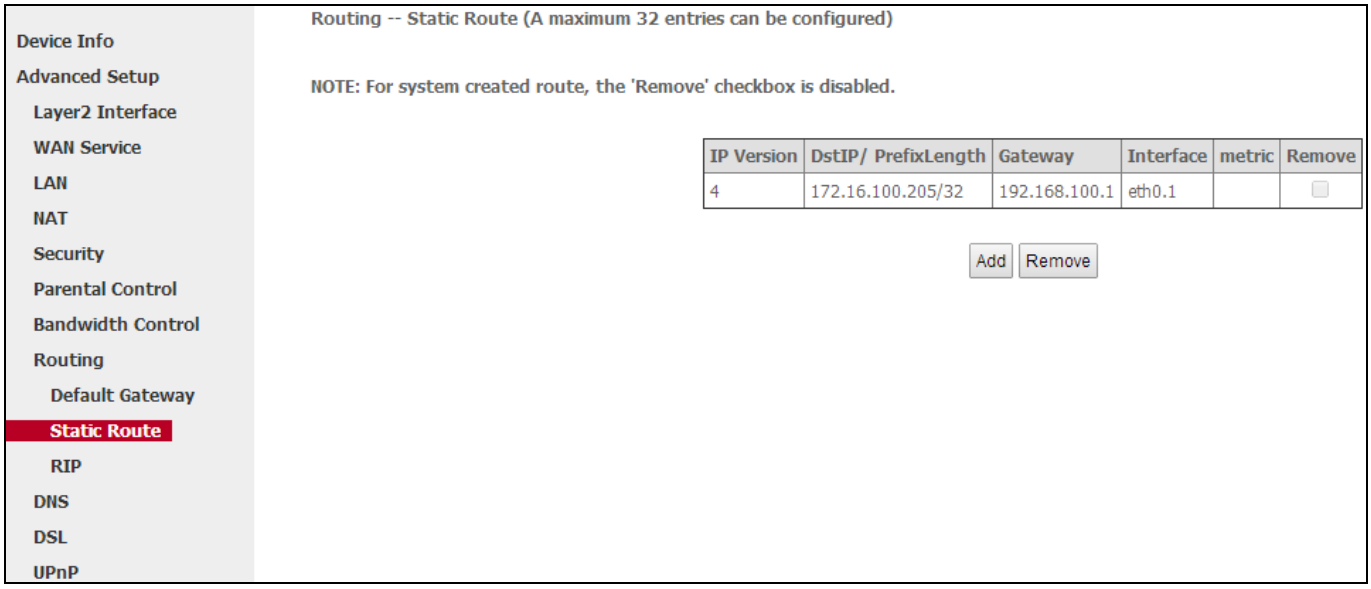
❹ **Apply/Save:** Click to save and activate your settings.

2.8.2 Static Route

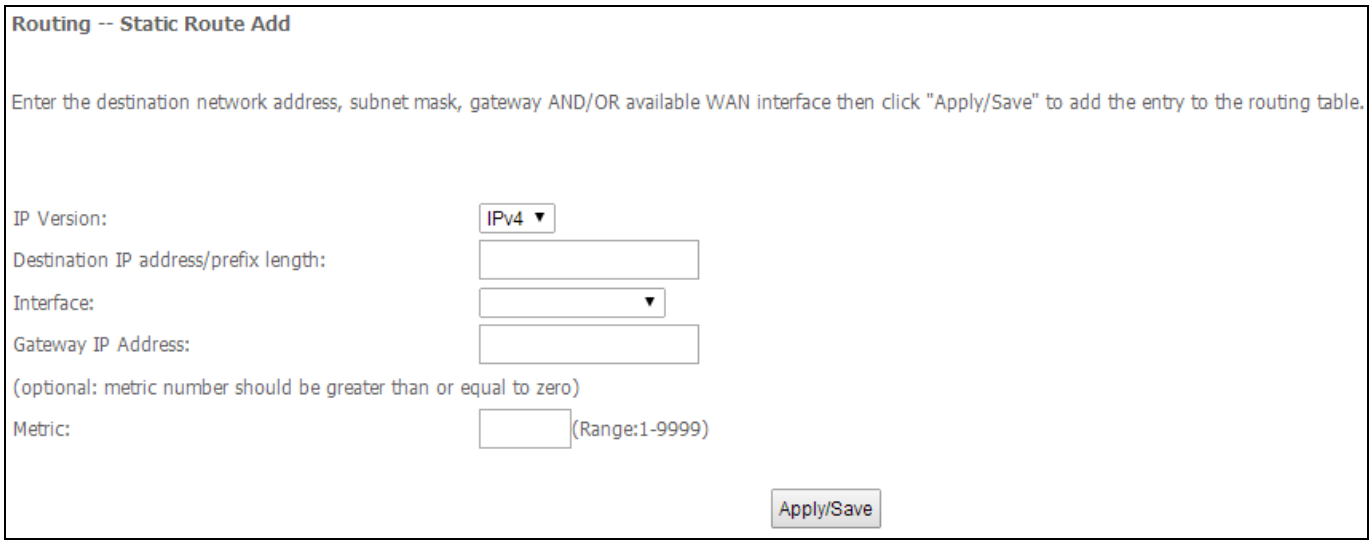
It is not recommended to use this setting unless you are familiar with static routing.

In most cases, dynamic routing is recommended, because this feature allows the router to detect the physical changes of the network layout automatically. If you want to use static routing, make sure the router's DHCP function is disabled.

Static routes provide additional routing information to your router. 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.



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



❶ **IP Version:** Select either IPv4 or IPv6.

❷ **Destination IP address/prefix length:** Enter the destination IP address and prefix length of the final destination.

- If the destination host is one specified host, its prefix is 32. E.g., the specified host 1.2.3.4 can be expressed as "1.2.3.4/32".
- If the destination host is one specified network, the IP address is the network number of destination host. E.g.,

the specified network 2.2.3.3, 255.255.0.0 can be expressed as “2.2.0.0/16” indicating all hosts that starts with “2.2”.

❸ **Interface:** Select an interface from the drop-down list according to your need. This interface can be the one on the LAN side or WAN side that data will forwarded out by.

❹ **Gateway IP address:** Input the ingress IP address of the next hop which packets are forwarded to from your modem router.

❺ **Metric:** Set the metric of this static route rule. It’s optional. The lower the value is, the higher the priority will be. When this two static routes’ destination address are the same, packets will be forwarded by following the higher priority route rule.

❻ **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.

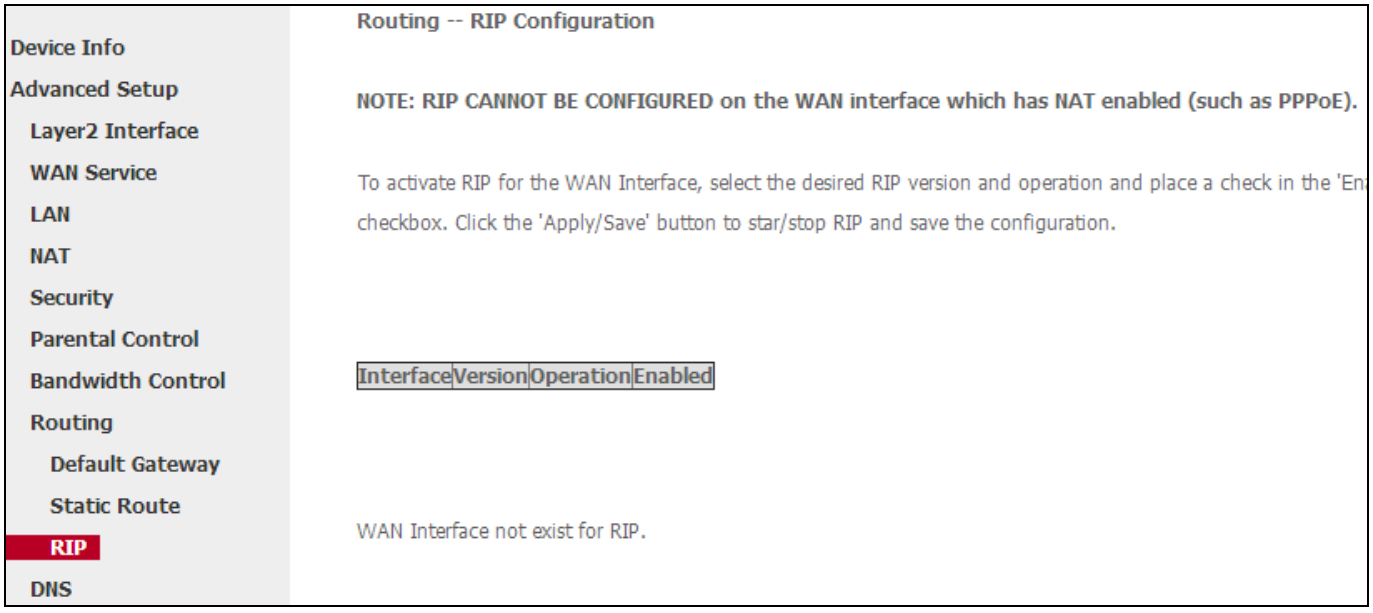
2. Only configure additional static routes for unusual cases such as multiple routers or multiple IP subnets located on your network. Wrong static routes may lead to network failure.

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

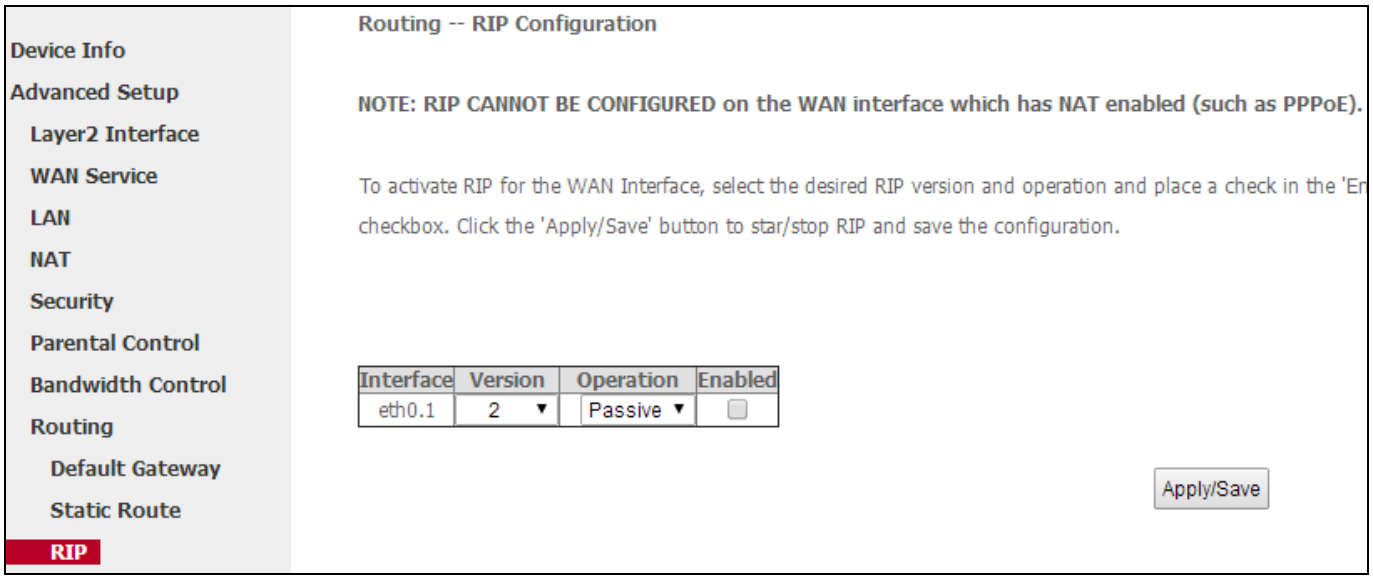
2.8.3 RIP

RIP is an advanced protocol used in the ISP environment to maintain the backbone network, for dynamically refreshing and generating the route table within each router that supports RIP. If all these route tables are managed by human beings, it will be a lot of work. RIP here helps automatically learn the router table and share the refreshment with RIP-based routers.

Click **Advanced Setup** > **Routing** > **RIP**. If the following figure shows, it means NAT feature on the WAN interface is enabled and RIP cannot be configured.



In this case, you should go to **Advanced Setup > WAN Service > Network Address Translation Settings** to disable NAT. Then go back here. You should be displayed with the following figure.



Operation-Passive indicates the RIP-enabled router will automatically tell other surrounding RIP-enabled routers the newest route table and share the newest route table with them.

Operation-Active indicates the RIP-enabled router will receive and share messages sent by another RIP-enabled router and then refresh its own route table.

Click **Apply/Save** to take the current settings into effect.

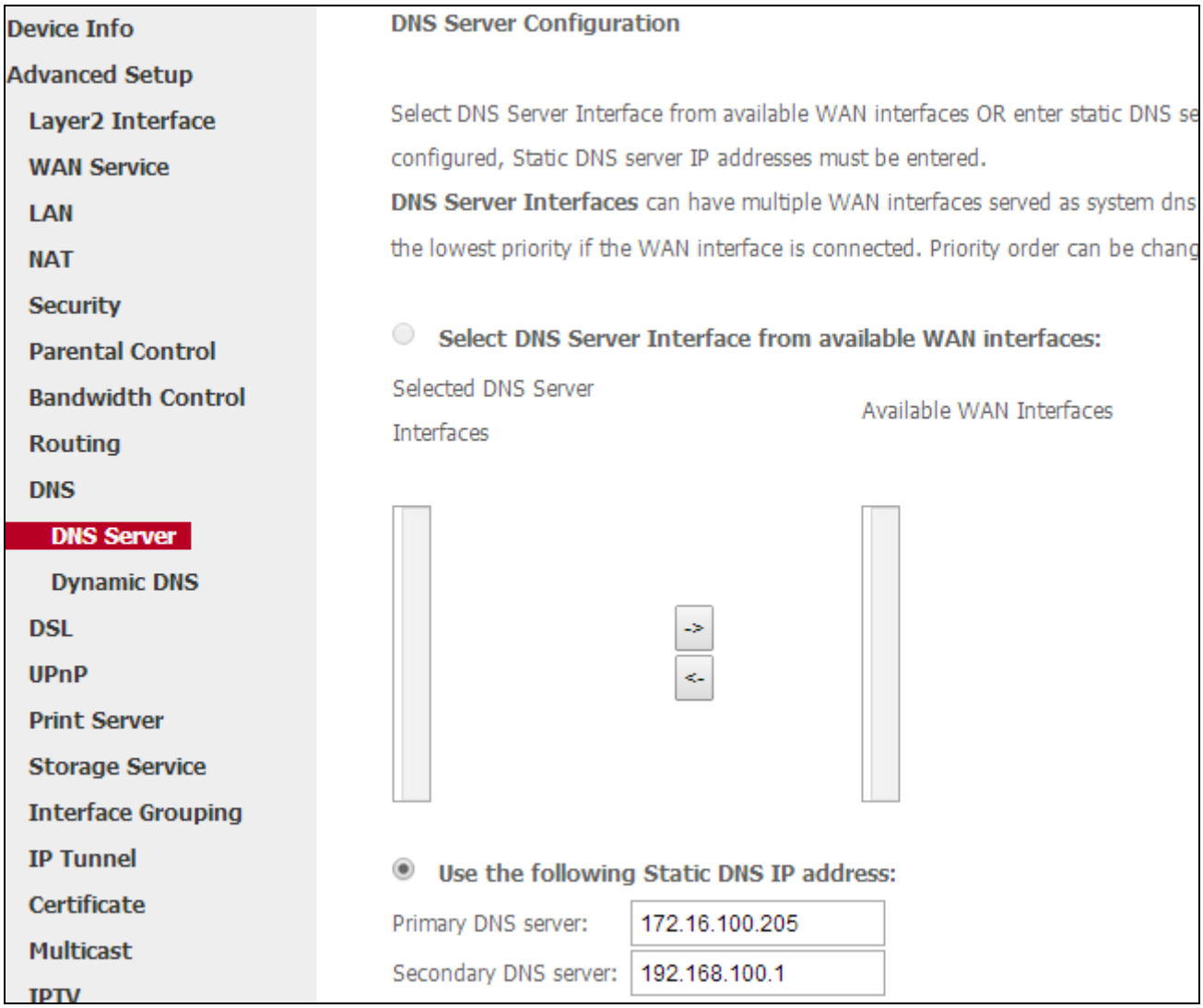
2.9 DNS

2.9.1 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. Here you can configure the WAN DNS address:

For IPv4

❶ Click **Advanced Setup** > **DNS** > **DNS Server**, and enter the screen below. See the upper part for IPv4 setting.

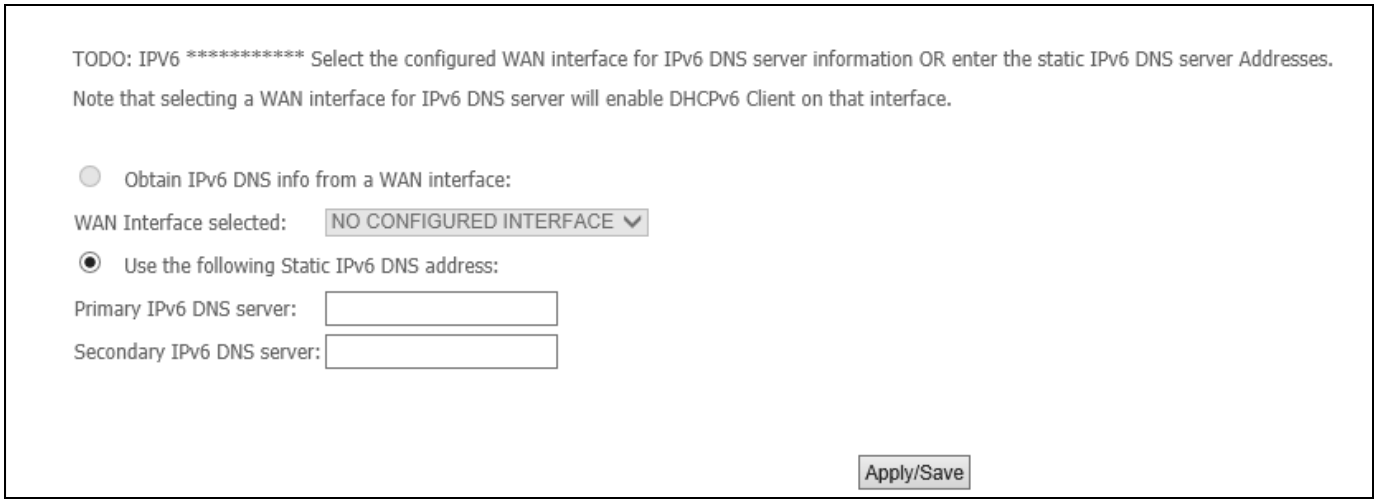


❷ Check the **Select DNS Server Interface from available WAN interfaces** option. OR select the **Use the following Static DNS IP address** option and enter static DNS server IP addresses for the system.

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

For IPv6

❶ Click **Advanced Setup** > **DNS** > **DNS Server**, and enter the screen below. See the lower part for IPv6 setting.



❷ Select the **Obtain IPv6 DNS info from a WAN interface** option, 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 Addresses.

❸ Click **Apply/Save**.

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 are not clear about the static DNS server IP information, ask your ISP to provide it.

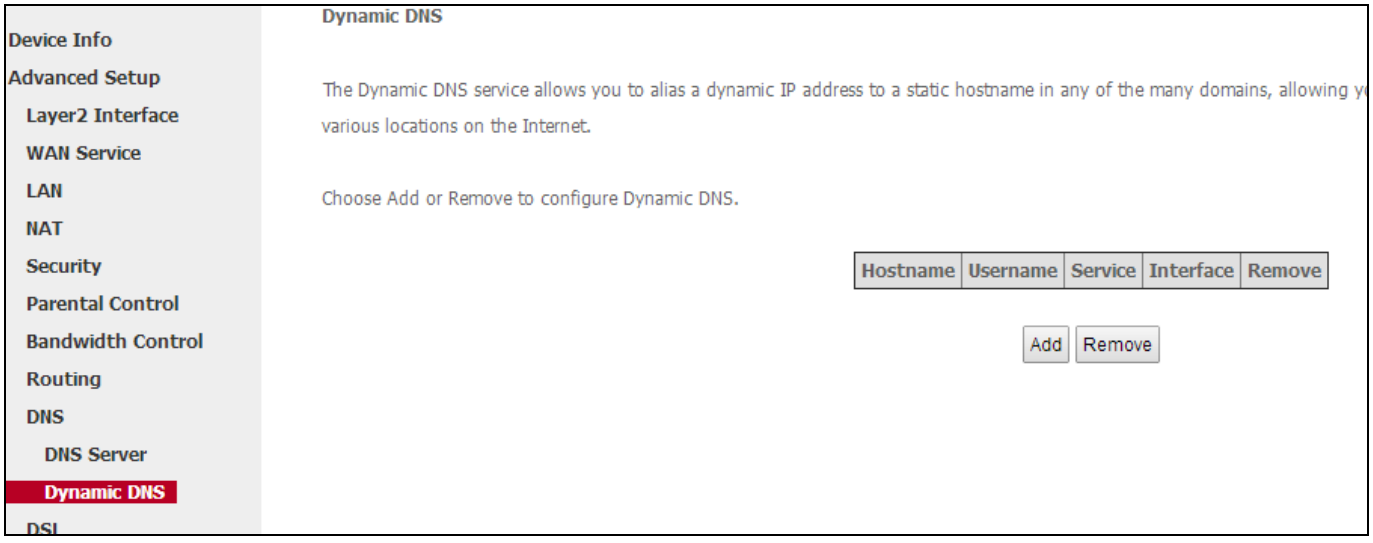
4. The default settings are recommended if you are unsure about the DNS server addresses. If a wrong DNS server address is configured, webpages may not be open.

2.9.2 Dynamic DNS (DDNS)

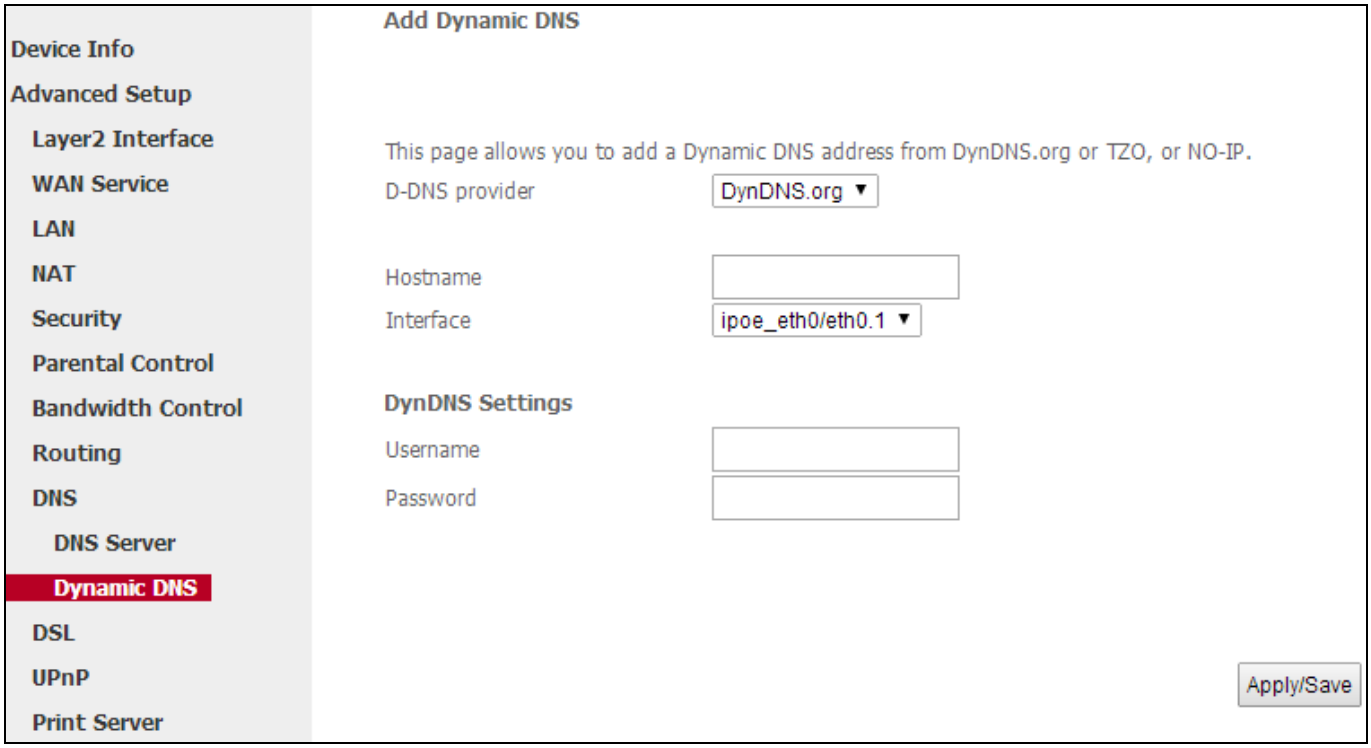
If your Internet service provider (ISP) gave you a static (fixed) public IP address, you can register a domain name and have that name associated with your IP address by public Domain Name Servers (DNS).

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 lets you register your domain to the IP address and forwards 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 the **Add** button to configure the DDNS settings.



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

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

❸ **Interface:** Specify a WAN connection interface.

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

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

❻ Click **Apply/Save** to take the setting into effect.

Example:

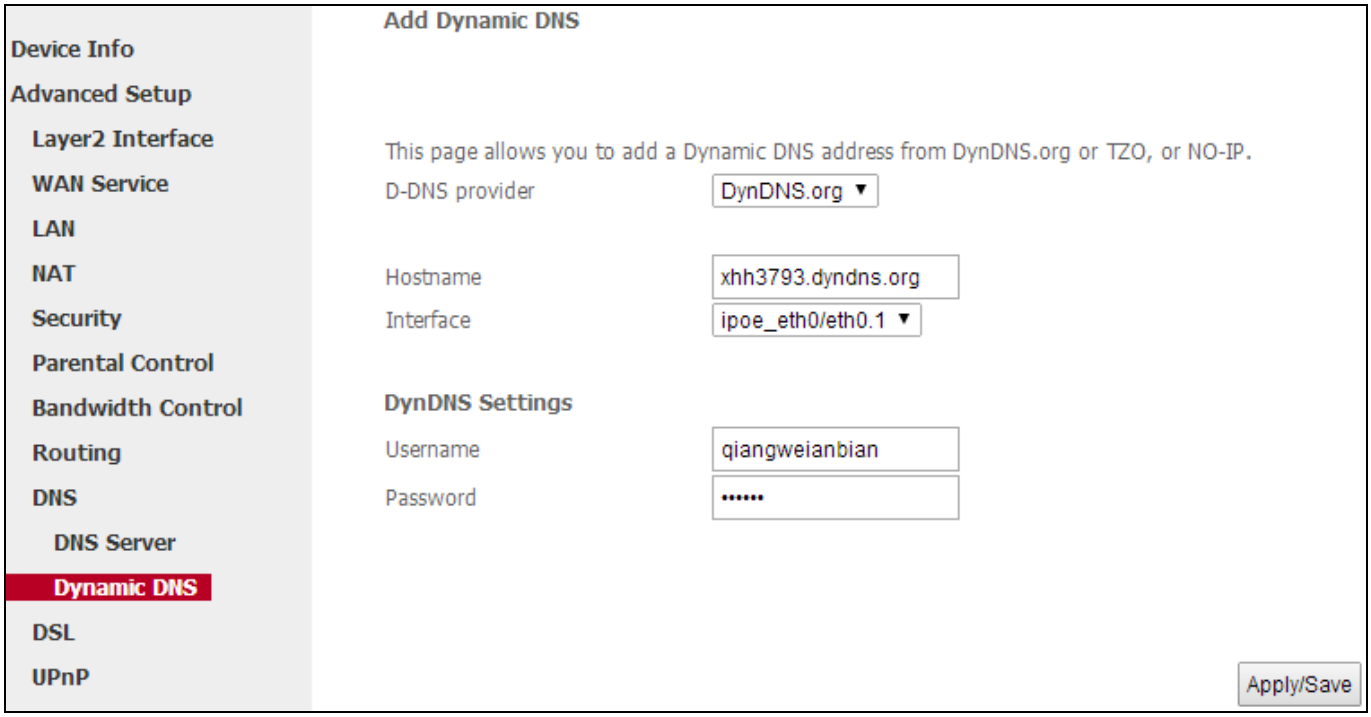
D-DNS provider: Dyndns.org

Username: qiangweianbian

Password: 414637

Hostname: xhh3793.dyndns.org

Configuration Steps:



❶ Select **DynDNS.org** from the **D-DNS provider** drop-down menu.

❷ Enter the Dyndns hostname, **xhh3793.dyndns.org**.

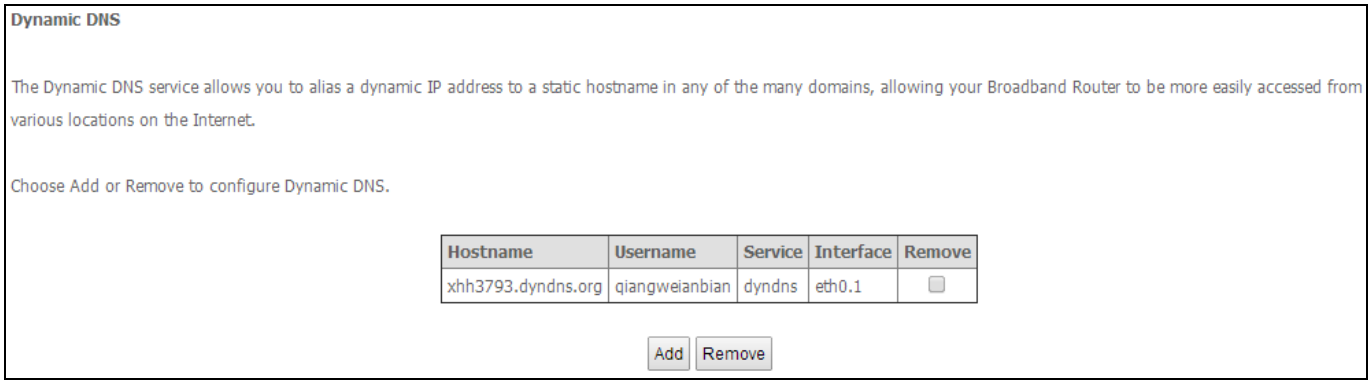
❸ Specify the WAN connection interface, **ipoe_eth0/eth0.1**.

❹ Enter the DynDNS username, **qiangweianbian**.

❺ Enter the password of your DynDNS.org account, **414637**.

❻ Click **Apply/Save** to save your configurations.

At last you will see the table below.



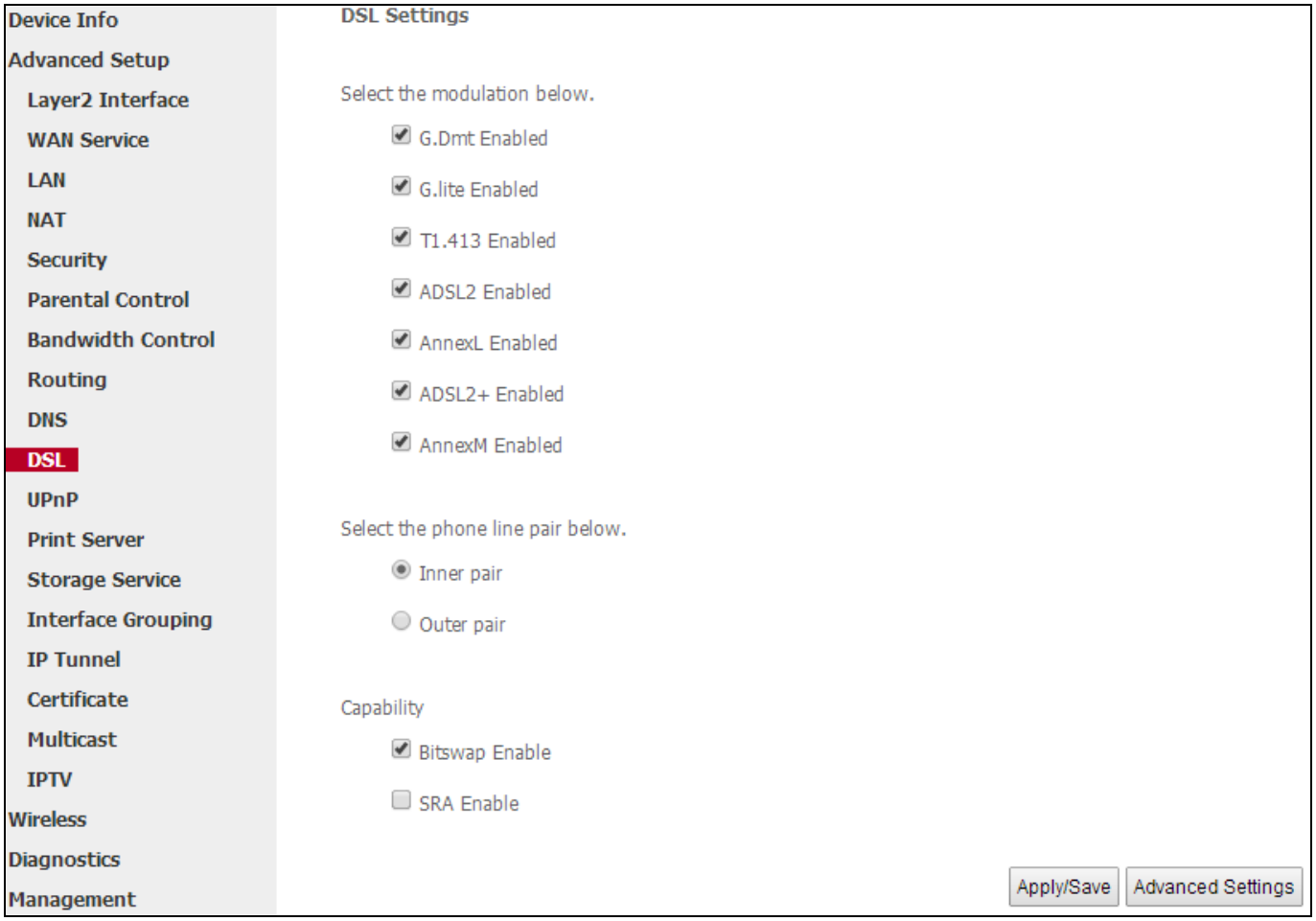
2.10 DSL

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-xDSL**) resulted from the negotiation between your router and ISP. Wrong configurations may fail your Internet access.

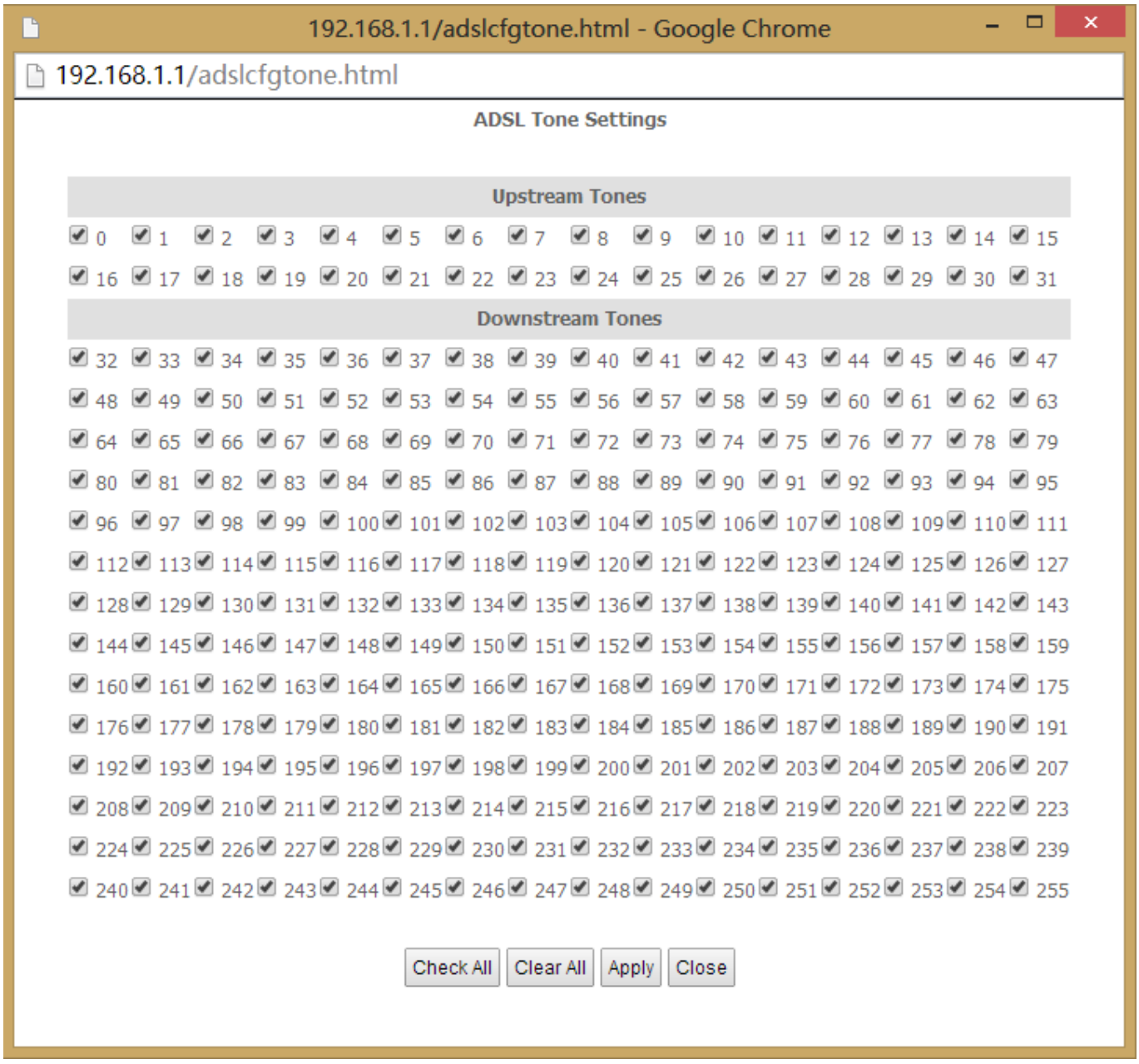
The best DSL configurations are the factory defaults. Only change them if you are instructed by your ISP or our technical staff when your router fails to negotiate with ISP in DSL (ATM) mode. Usually, this failure can be identified and confirmed if the ADSL LED on the device keeps displaying a slow or quick blinking light.

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.

Click Tone Selection to enter the prompt window below.



Tip

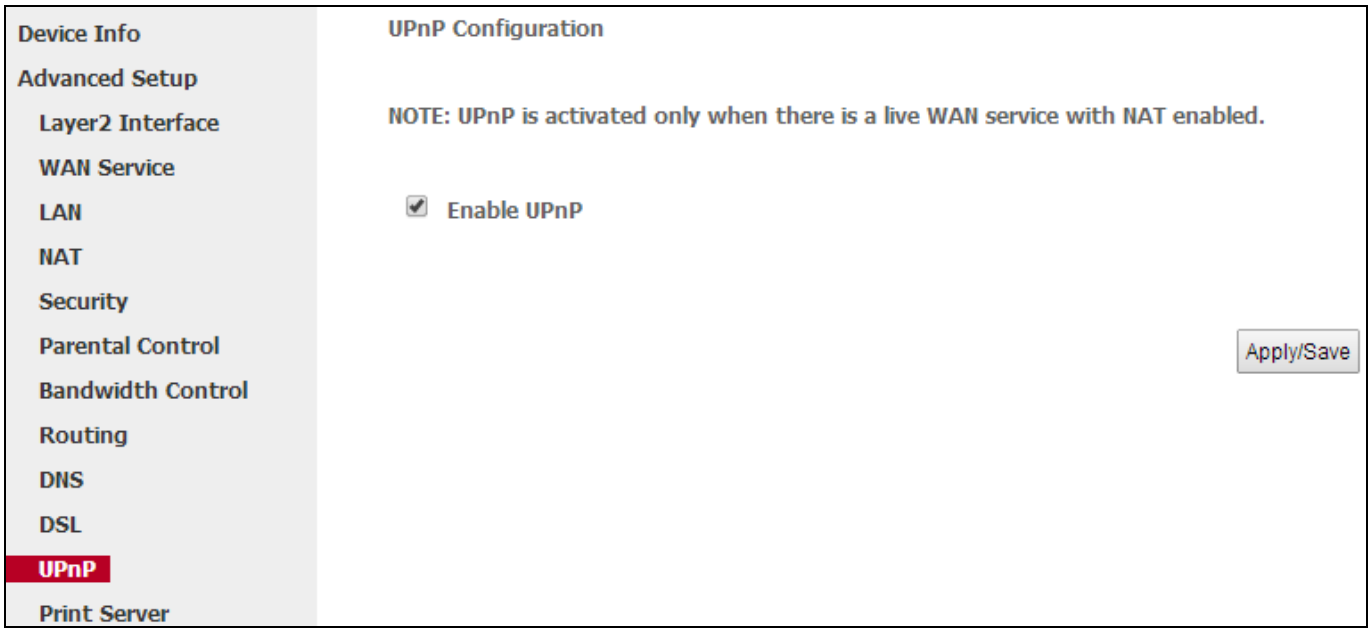
If you are unsure about the ADSL parameters, please apply the factory default settings. Wrong configurations may fail your Internet access.

2.11 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.

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

❷ Click **Apply/Save**.

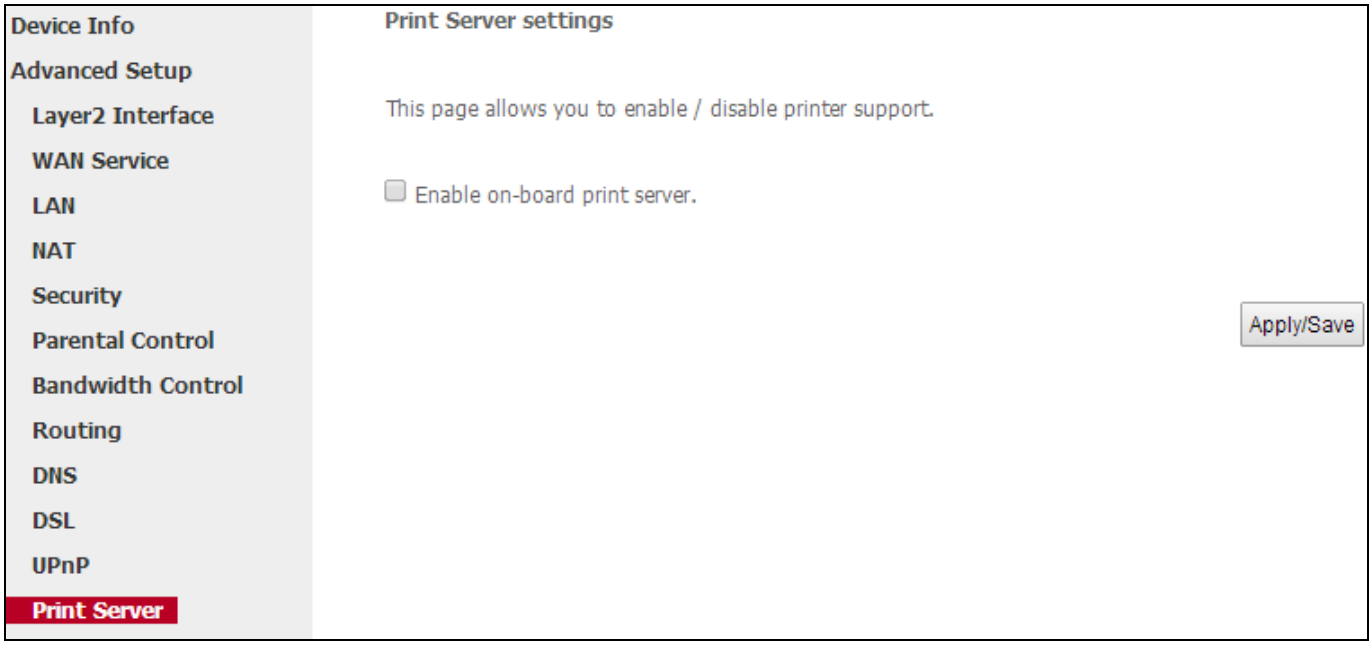


Note

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

2.12 Print Server

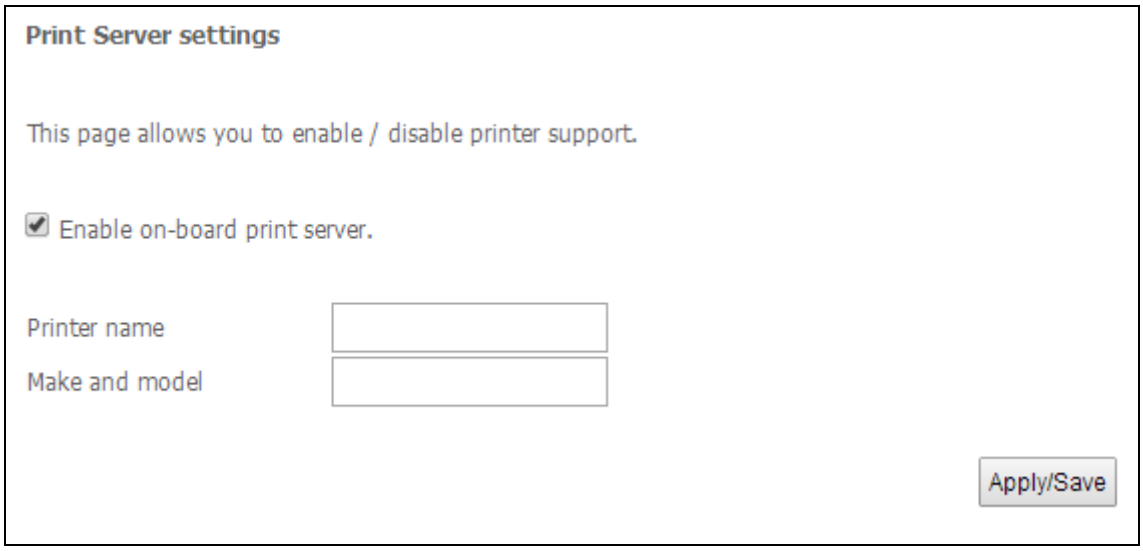
Enabling **Print Server** makes all PCs on the LAN have an access to the USB printer which has been connected to this router. Click **Advanced Setup > Printer Server** to enter screen below:



USB printing config:

❶ Connect the USB printer to the USB port of the device.

❷ Enable USB printing service of the device (the router).



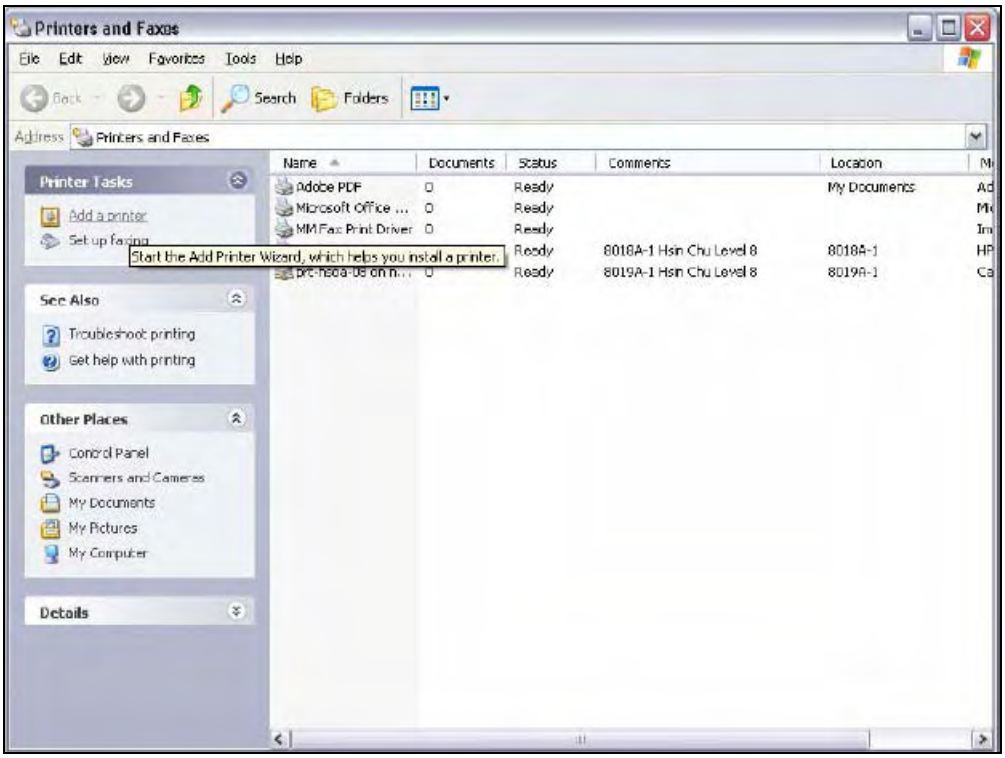
First, enter the name of the USB printer in **Printer name** box.

Then, enter the manufacturer and model of the USB printer in the **Make and model** box.

At last, click **Apply/Save**.

❸ Add the printer from your local PC (In Windows XP OS).

Step 1: Click **Start > Control Panel > Printers and Faxes > Add a printer**;

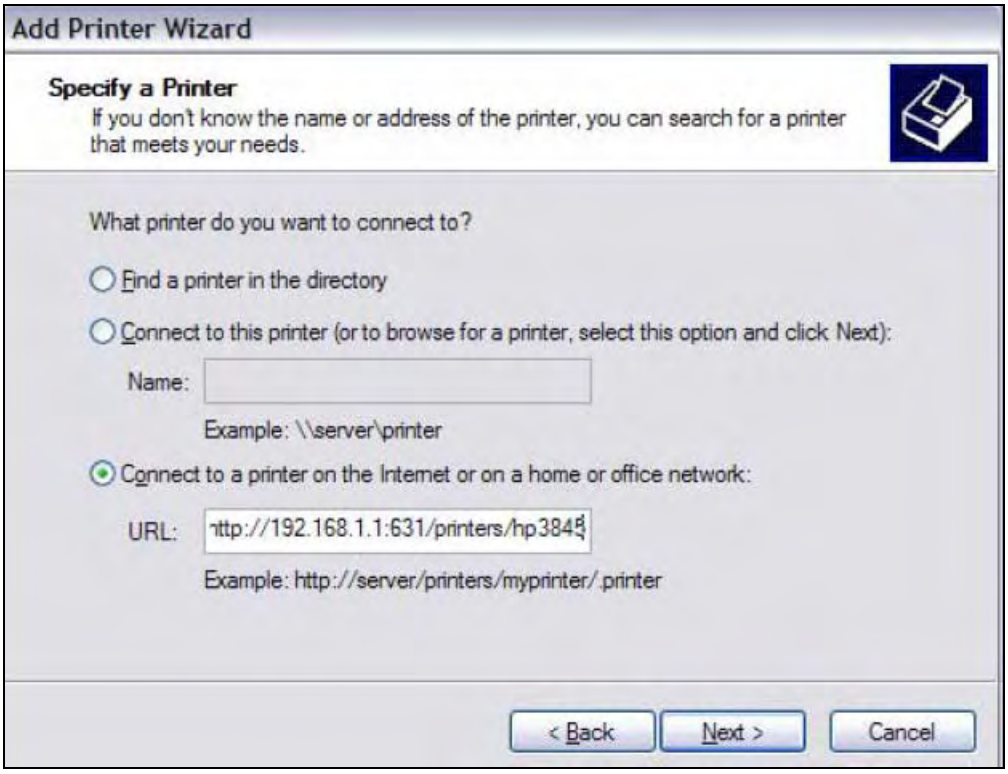


Step 2: Click **Next**;

Step 3: Select **A network printer, or a printer attached to another computer** and click **Next**;

Step 4: Select **Connect to a printer on the Internet or on a home or office network**;

Type in “http://192.168.1.1:631/printers/hp3845” in the URL field and click **Next**;



Note

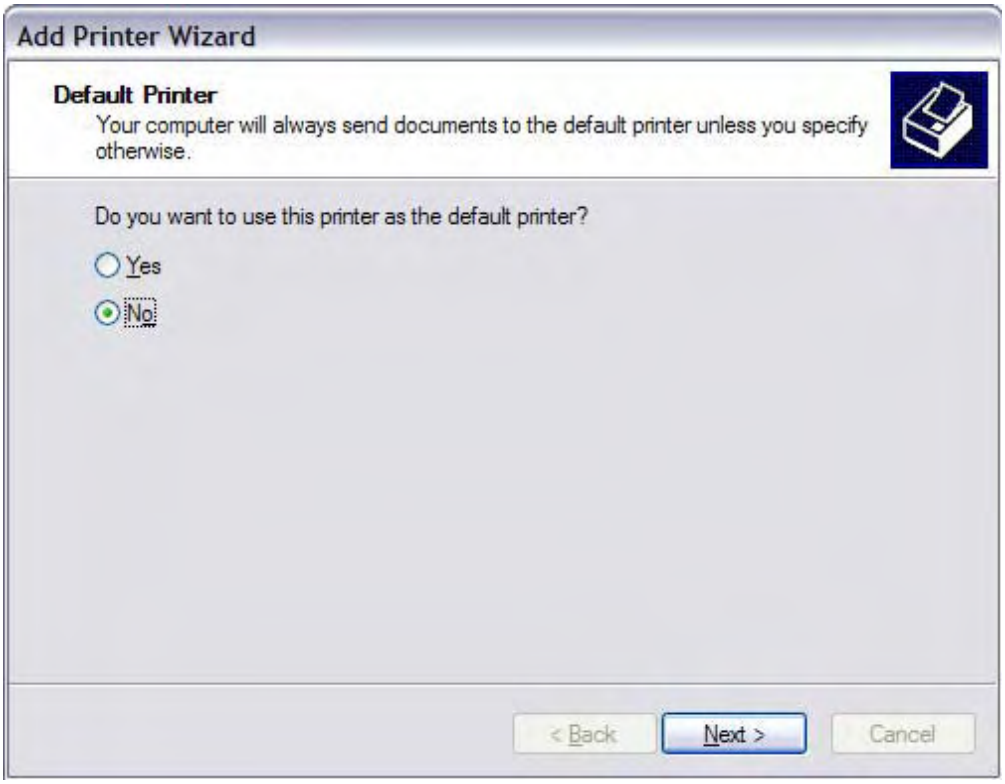
Here “192.168.1.1” refers to this router’s LAN IP address and “hp3845” refers to the USB printer name you’ve filled in on the Print Server Settings page.

Step 5: Insert the printer driver CD into your computer and click **Have Disk…**;

Step 6: Click **Browse**, select driver file directory on CD-ROM and click **OK**;

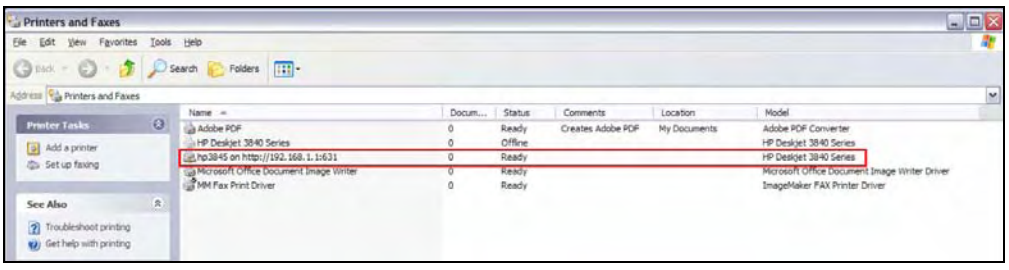
Step 7: Select the manufacturer and the model of your printer. And click **OK**.

Step 8: Choose “Yes” or “No” for default printer setting and click **Next**.



Step 9: Click **Finish**.

Check the status of printer from Windows “Control Panel”, printer window. Status should be shown “ready”.



2.13 Storage Service

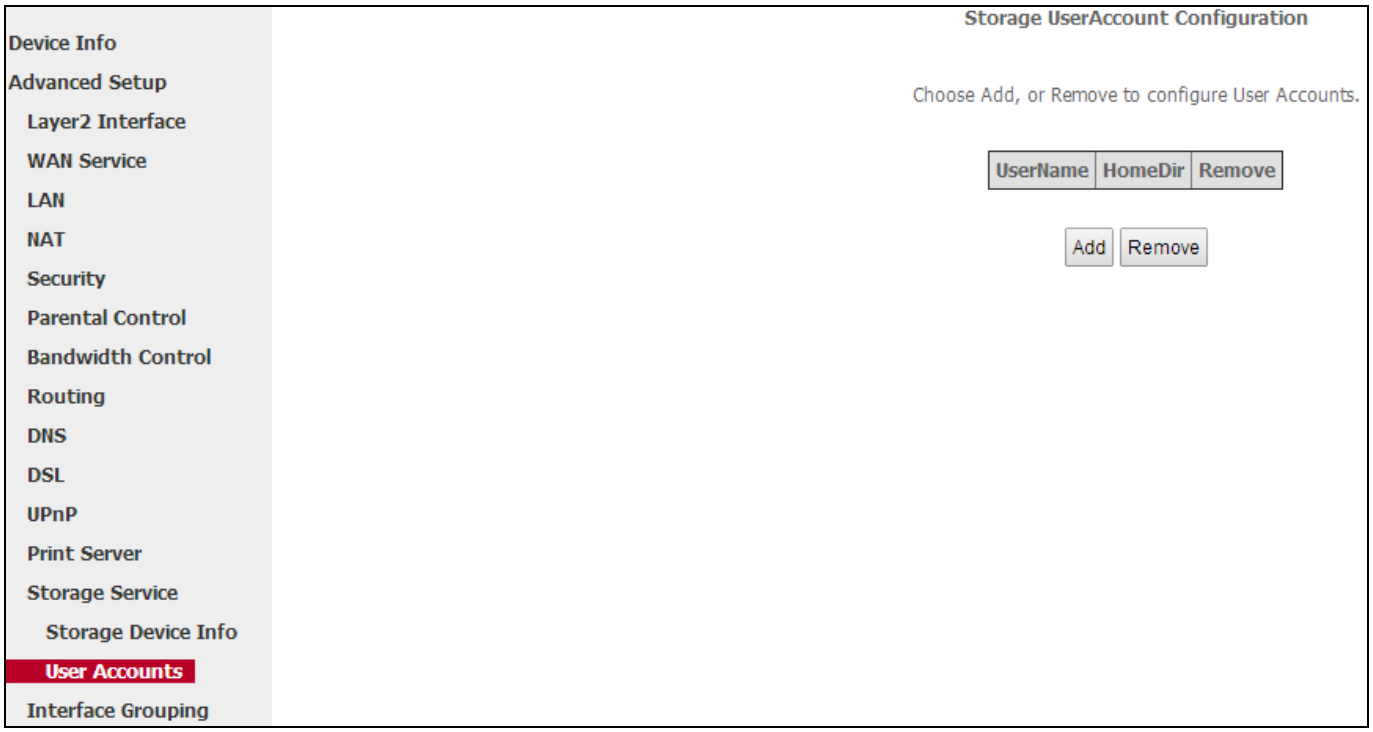
This section helps you to use USB Storage devices in your modem router, including the following parts:

• **User Account:** You can control the LAN users' accessing to the USB storage device information, namely, some of them can access the USB device info but others cannot.

• **Storage Device Info**: When you plug the USB storage device into the USB interface of your modem router, the router can recognize that's the USB storage device and then read the storage device's information.

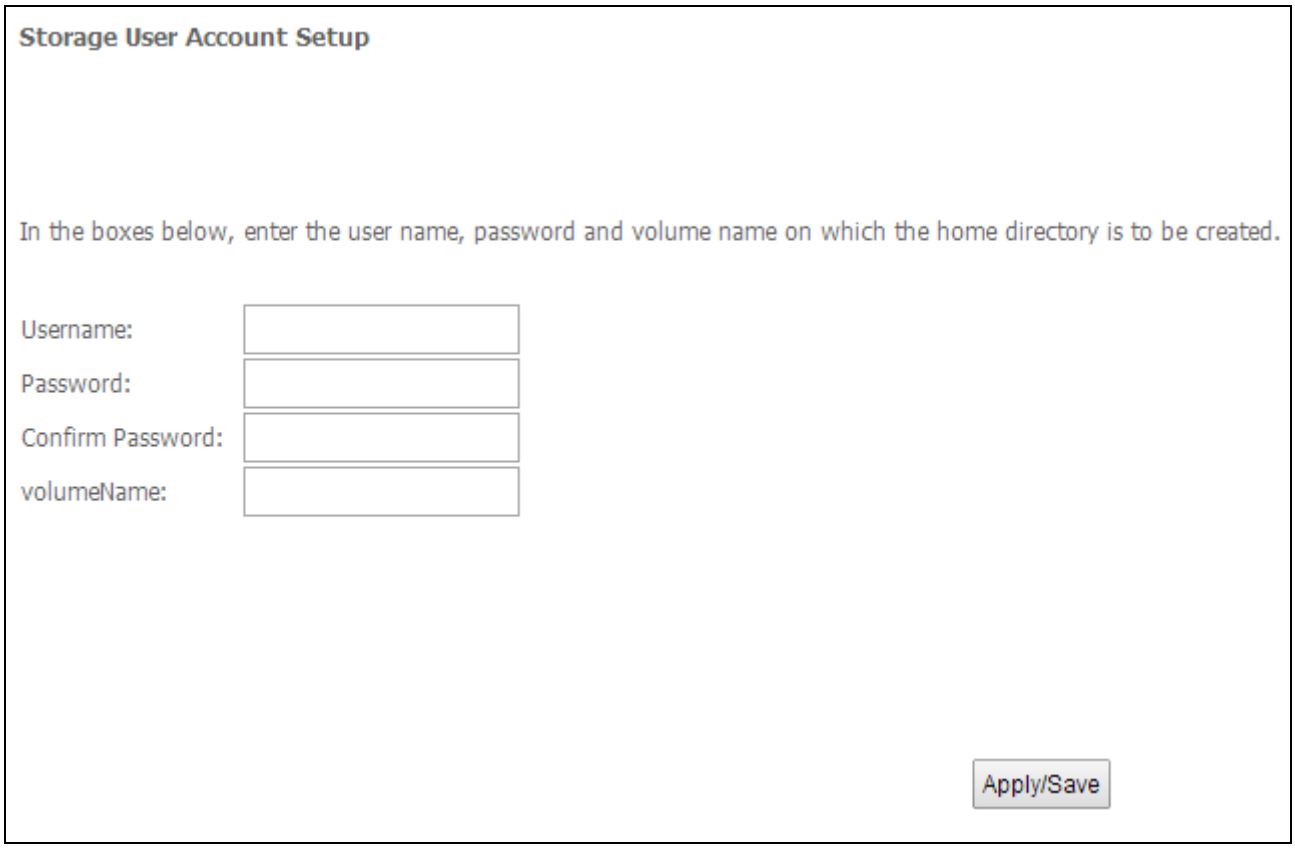
2.13.1 User Account

Before you share your USB storage on the internet, you need to add a storage user account. And only the users on the user account list can visit the USB storage device plugged in the modem router. Thus, before you access the USB storage device, set the user account information first.



To add a new account:

❶ Click **Add** to enter the user account configuration page.



❷ **Username**: Name your USB storage account.

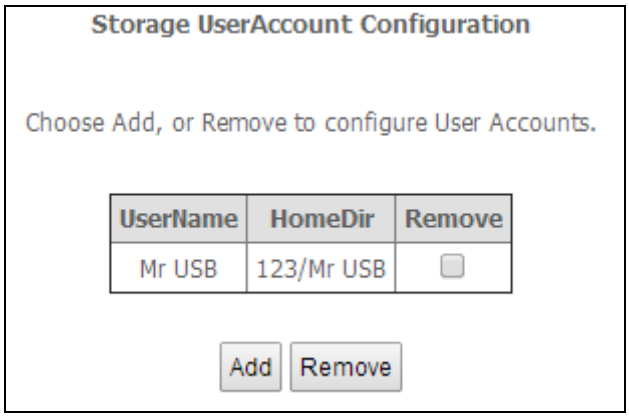
❸ **Password:** Specify a password to secure your USB storage account.

❹ **Confirm Password:** Enter your password again for a confirmation.

❺ **VolumeName:** Enter the volume name of the USB storage, which is displayed in the **Storage Device Info** page.

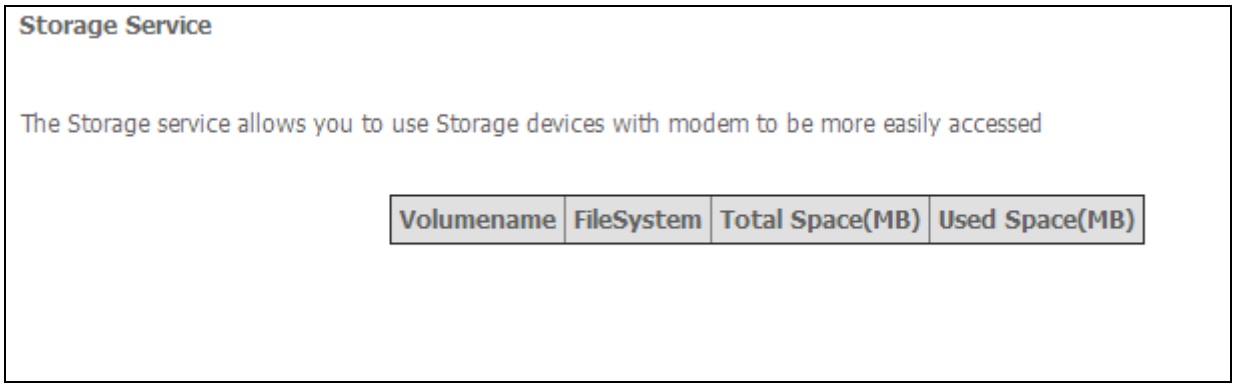
❻ Click **Apply/Save** to save your configurations.

At last, you will see the table shown as below. Here's an example.



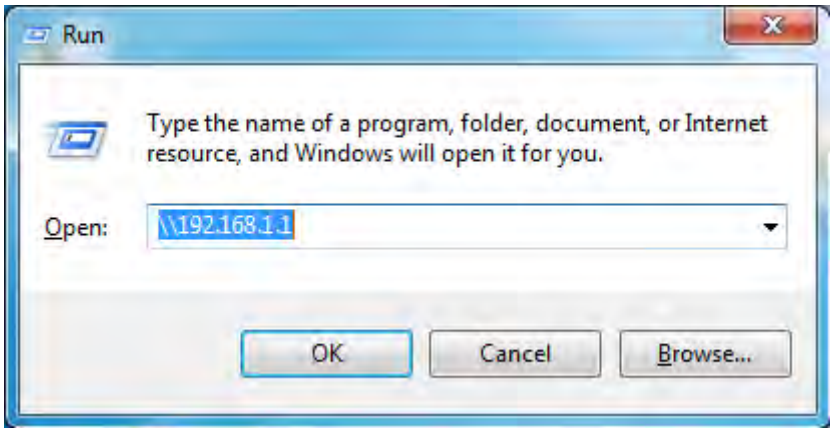
2.13.2 Storage Device Info

Your modem router can automatically recognize the USB storage device and the **Storage Device Info** screen will show the information such as the label, file system type, total disk space, used disk space.

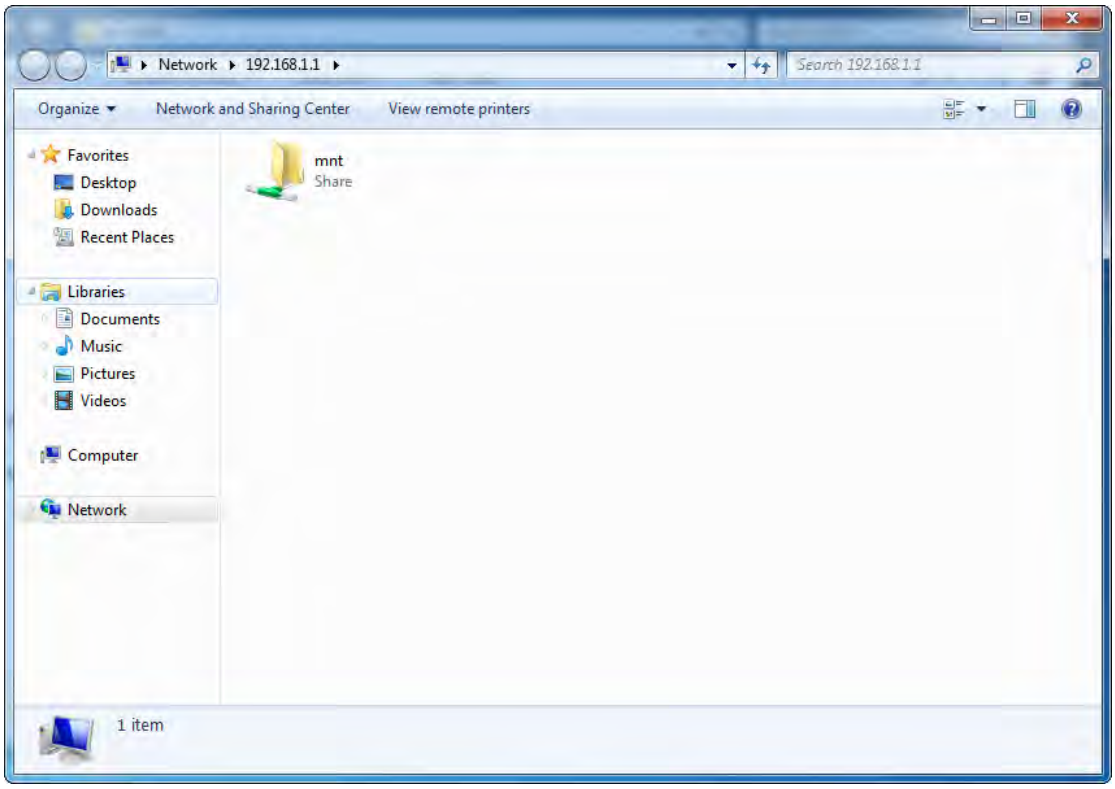


After your modem router recognizes the USB storage device, follow guidelines below for visiting the storage info via the computer on the LAN. Here takes **Windows 7** as an example to explain the guidelines which are similar in other operation systems.

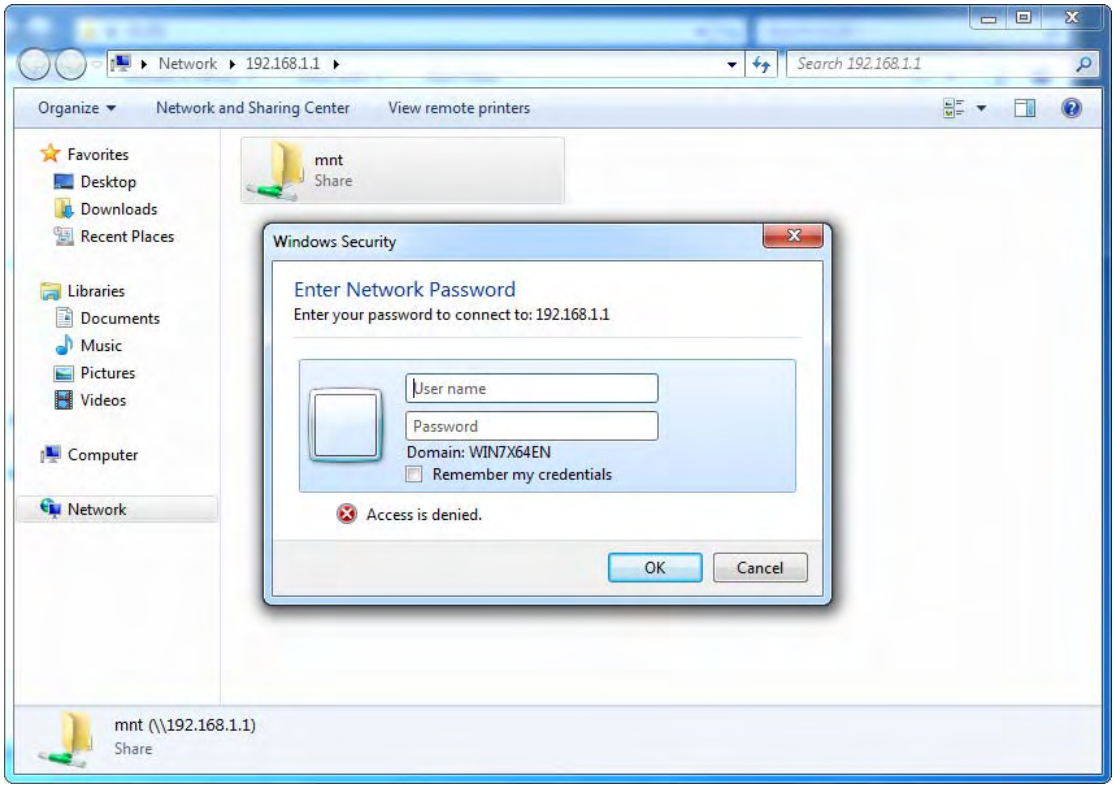
❶ Press **Win+R** buttons. On the **Run** window, input \\192.168.1.1 (\\+ LAN IP address of the router), and then click **OK**.



❷ Double click the USB storage device icon (“mnt”).



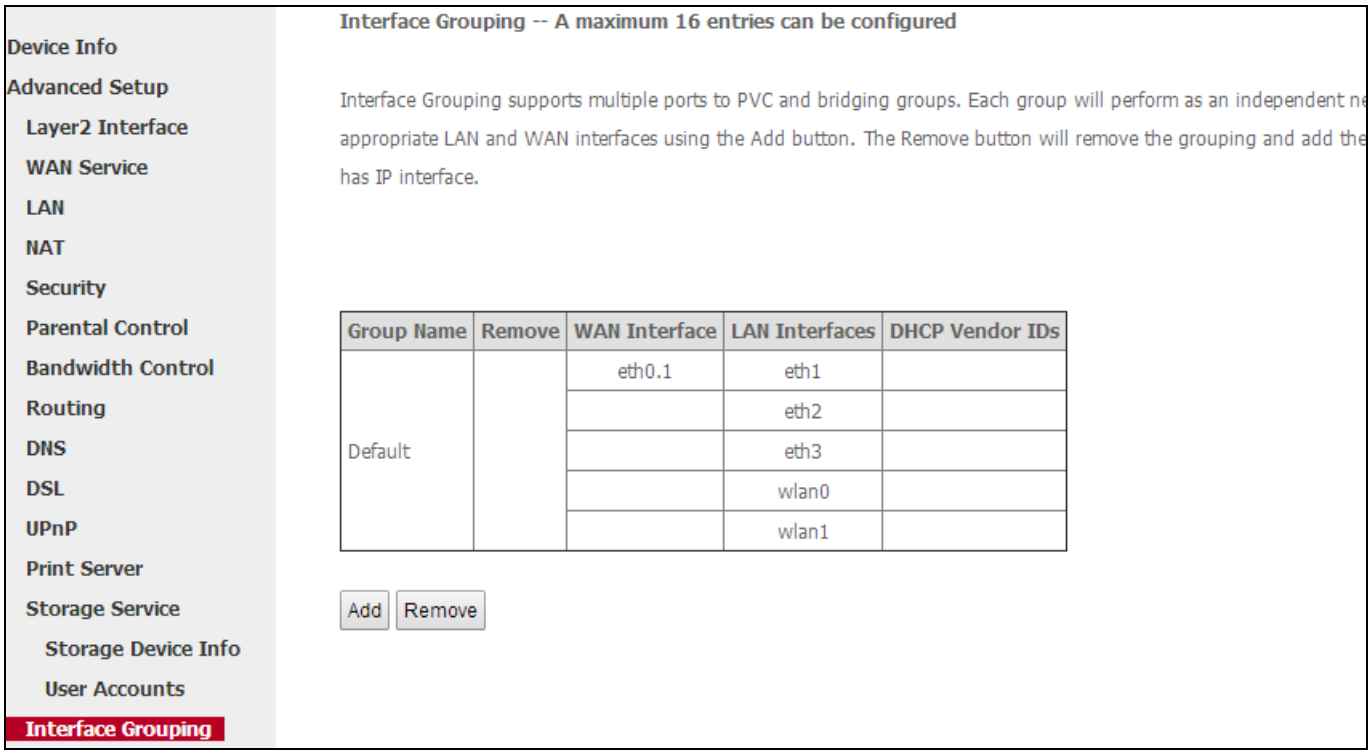
❸ **Account authentication:** Enter your user account name and password which were configured in **User Account** part in the corresponding box, and click **OK**. Then you can see the detailed info within the USB device.



2.14 Interface Grouping

Interface Grouping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. Only the default group has IP interface.

Click **Advanced Setup** > **Interface Grouping** to enter the following figure.



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

Group Name: The name of a configured rule.

WAN Interface used in the grouping: WAN connection to which the interface grouping rules apply.

Available LAN Interfaces: LAN interfaces that can be used for interface grouping.

Grouped LAN Interfaces: LAN interfaces that use specified WAN interface.

To create a new interface group:

❶ Enter the Group name which should be unique.

❷ Select the WAN interface that's shared by the LAN interfaces in the interface group.

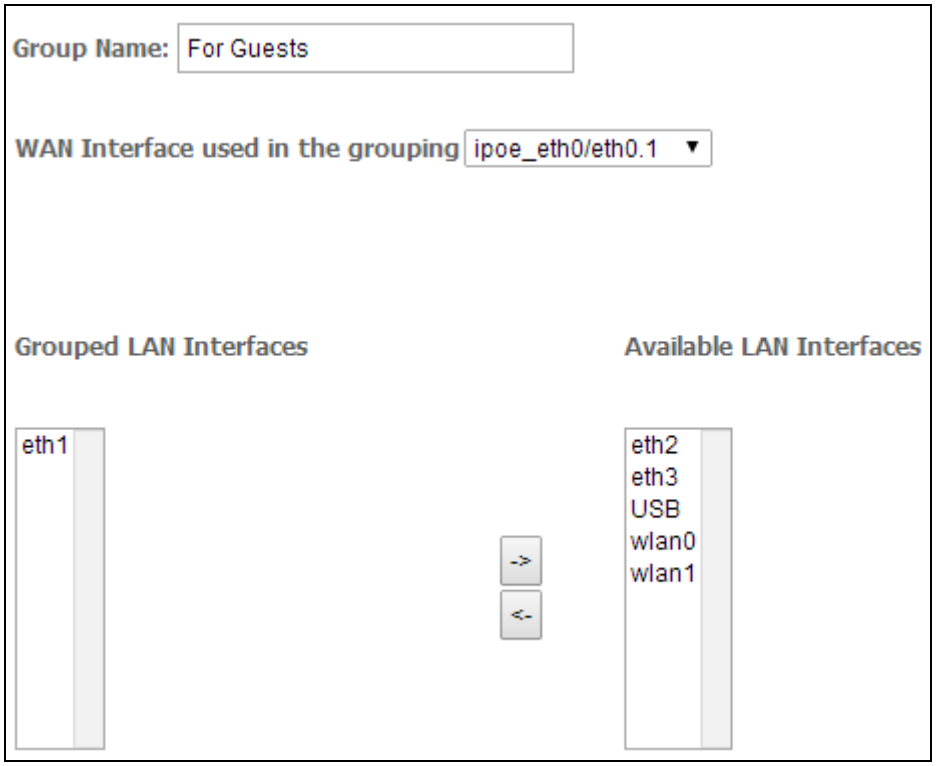
❸ Select interfaces that will be connected to the specified WAN you will use. Note that these clients may obtain public IP addresses.

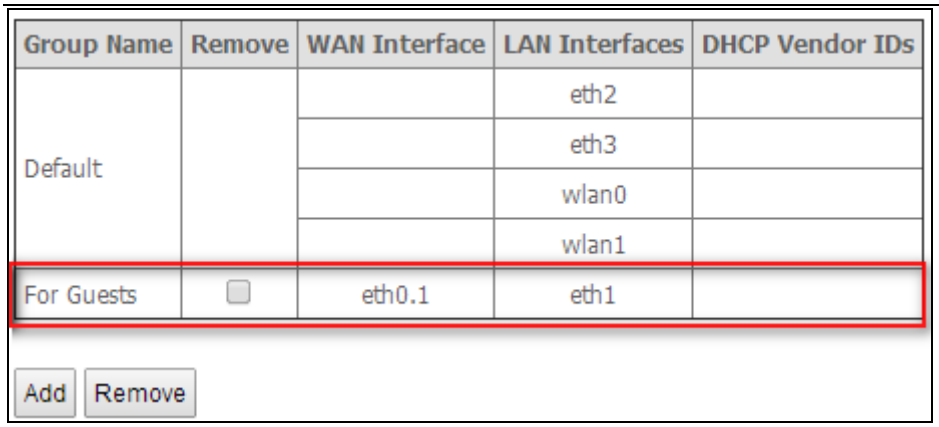
❹ Click **Apply/Save** button to make the changes effective immediately.

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.

Application:

Your ADSL line support 2 PVC groups: ppp0.1 used for home users to access the Internet; atm.1.1 used for guests to access the Internet. You hope that eth3 (Interface 4 on the modem router) can be used for guests to visit the Internet, and meanwhile data of the guest won't be forwarded to other interfaces. Configurations are as below in the figure.





Note

1. After the settings above, you need to reboot the modem router to take the settings into effect.

2. After the settings above, the LAN IP address used by the Default group member is 192.168.1.1, the LAN IP of the second group member is 192.168.2.1. LAN IPs of the following groups follows the same rule.

3. After you set the IPTV function, the modem router will automatically add one interface group named IPTV, which should be saved. If it's deleted, the IPTV function takes no effect.

2.15 IP Tunnel

This section explains the following information:

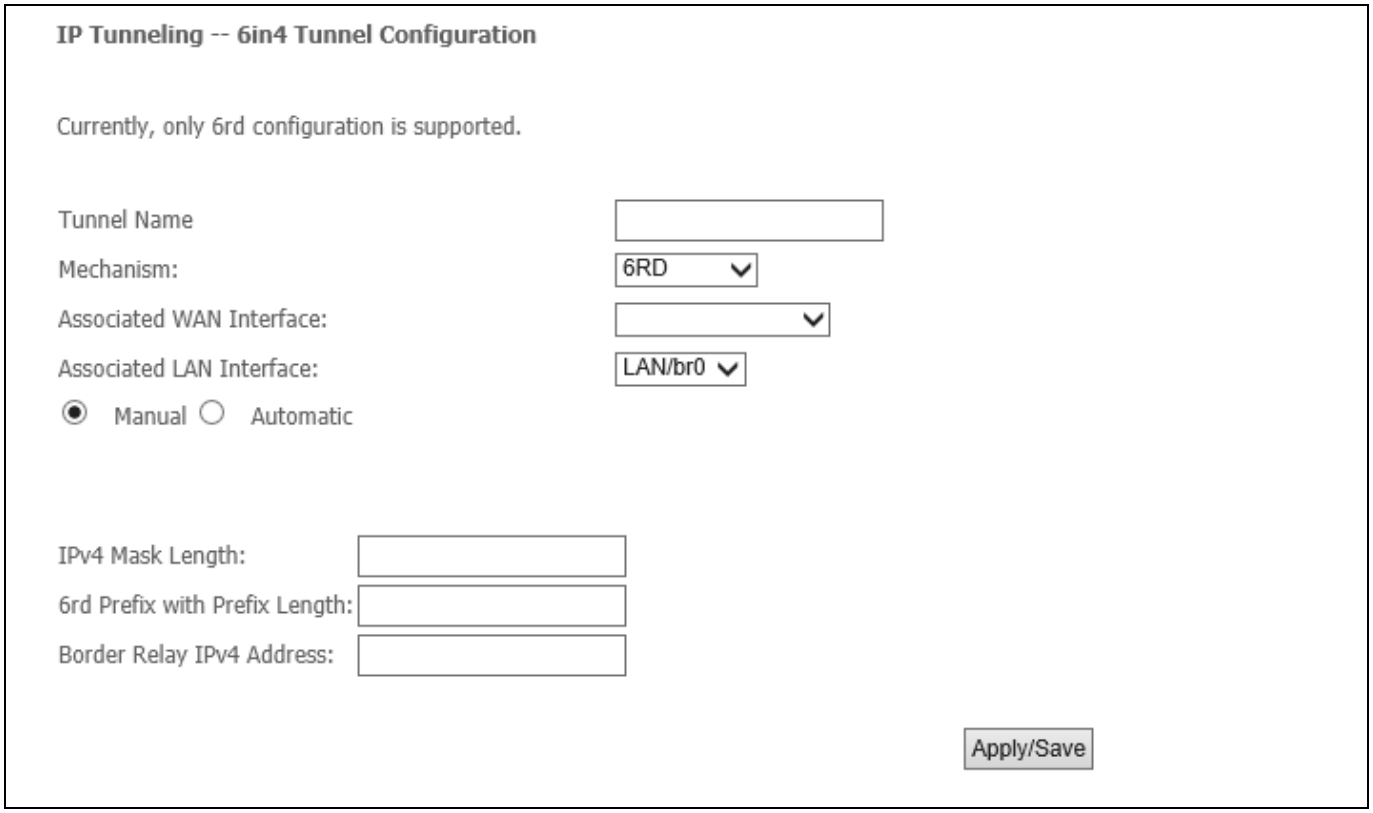
• IPv6inIPv4

• IPv4inIPv6

2.15.1 IPv6inIPv4

Keeping the current IPv4 network frame, IPv6 in IPv4 accomplishes support to IPv6, for solving problems of communications between IPv6 stations or hosts, which is commonly used during IPv6 initially imported period.

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



❶ **Tunnel Name:** Specify the name of the tunnel.

❷ **Mechanism:** Currently, only 6RD configuration is supported.

❸ **Associated WAN Interface:** Specify the WAN interface of the tunnel.

❹ **Associated LAN Interface:** Specify the LAN interface of the tunnel.

❺ **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 other configurations are required.

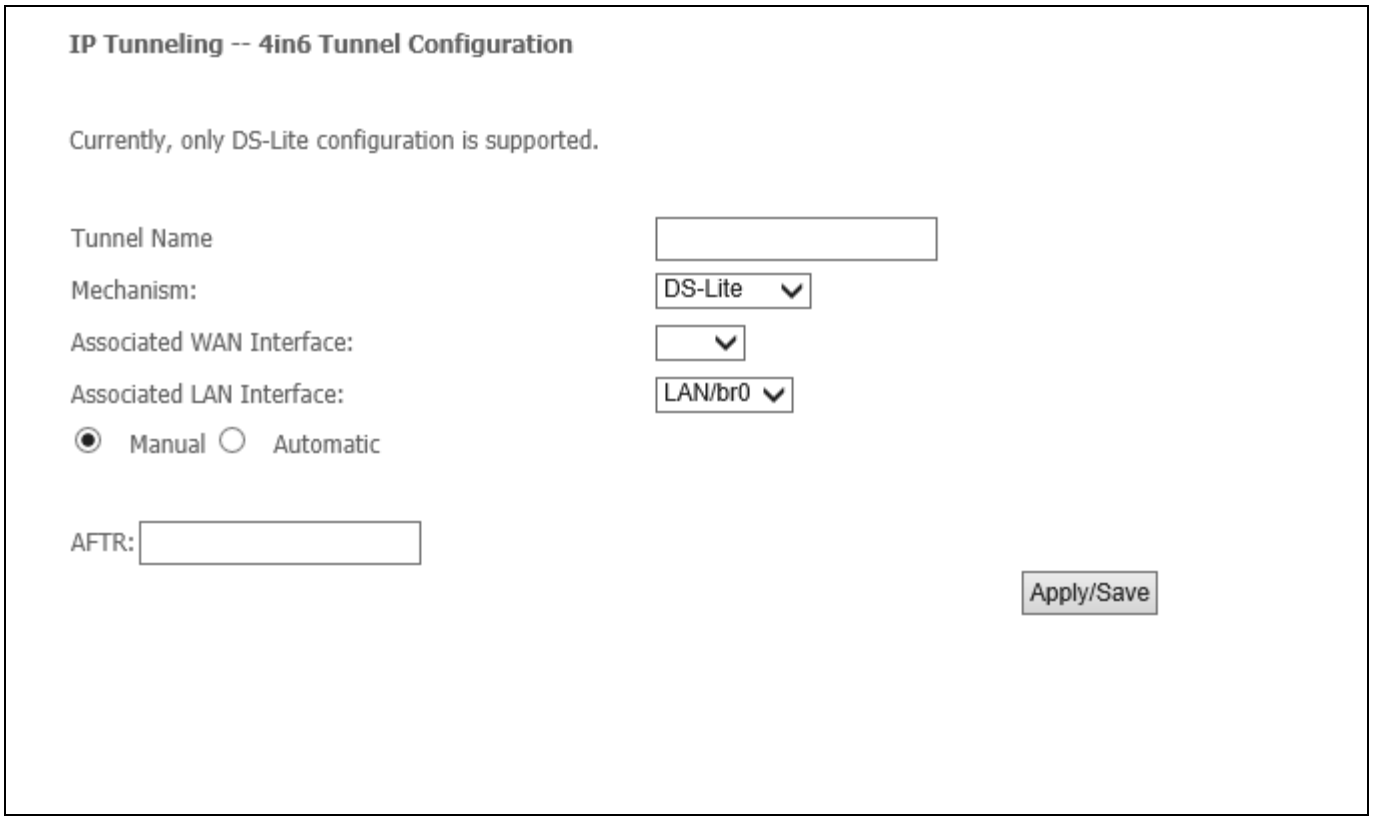
❻ **Apply/Save:** Click to apply and save your settings.

2.15.2 IPv4inIPv6

Via network devices, IPv4 in IPv6 support IPv6 to establish the network fundamental network frame, so as to systematically import IPv6.

As for the current IPv4, IPv4 in IPv6 accomplishes the inheritance of usage of IPv4, namely regarding IPv4 as one of IPv6' business. This IPv4 in IPv6 function mainly refers to IPv6, as well as the newly created IPv4 business or the network that won't adopt dual stack.

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



❶ **Tunnel Name:** Specify the name of the tunnel.

❷ **Mechanism:** Currently, only DS-Lite configuration is supported.

❸ **Associated WAN Interface:** Specify the WAN interface of the tunnel.

❹ **Associated LAN Interface:** Specify the LAN interface of the tunnel.

❺ **Manual:** If you select Manual, enter the AFTR information also:

Automatic: If Automatic is selected, no other configurations are required.

❻ **Apply/Save:** Click to apply and save your settings.

2.16 Certificate

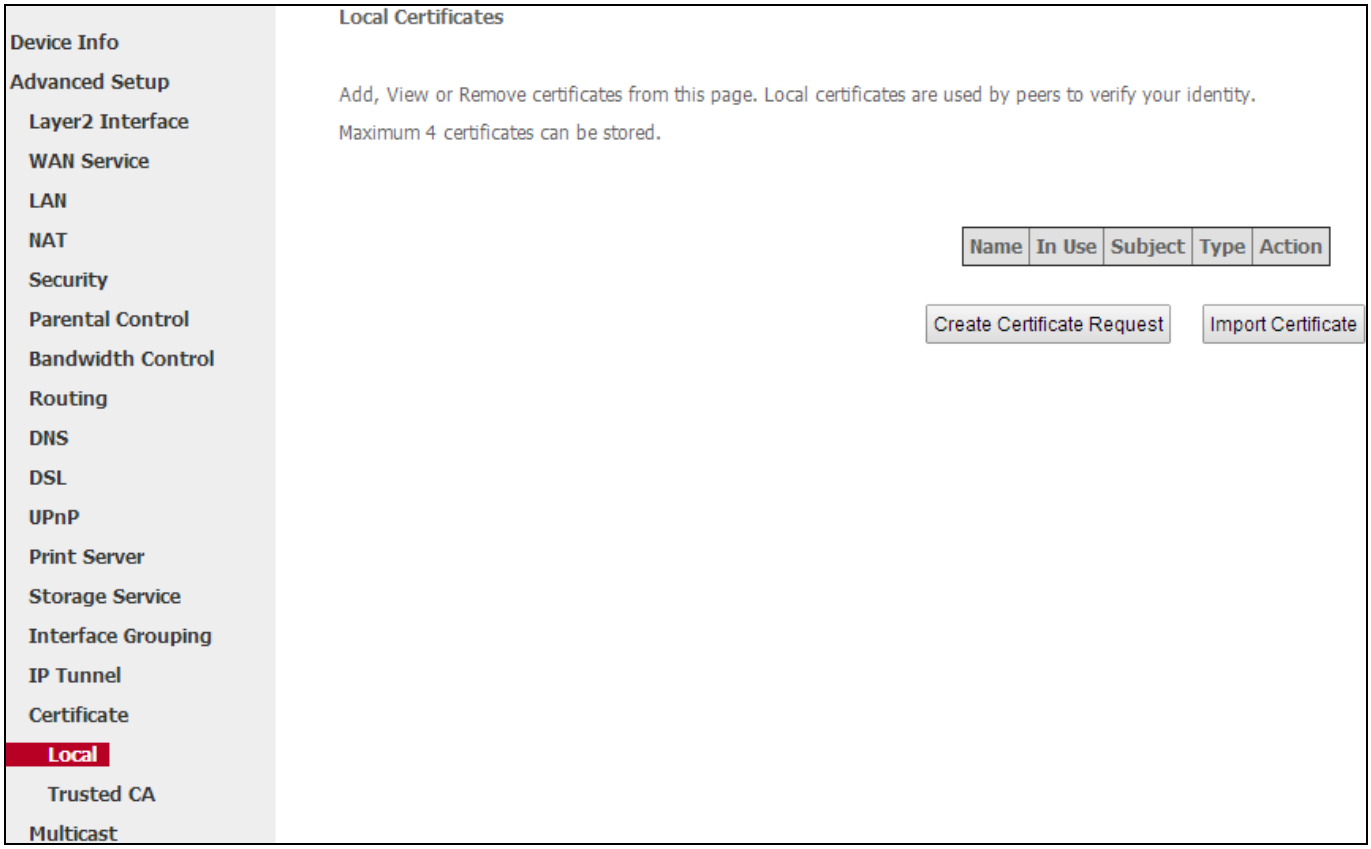
This section explains the following information:

• Local Certificates

• Trusted CA (Certificate Authority) Certificates

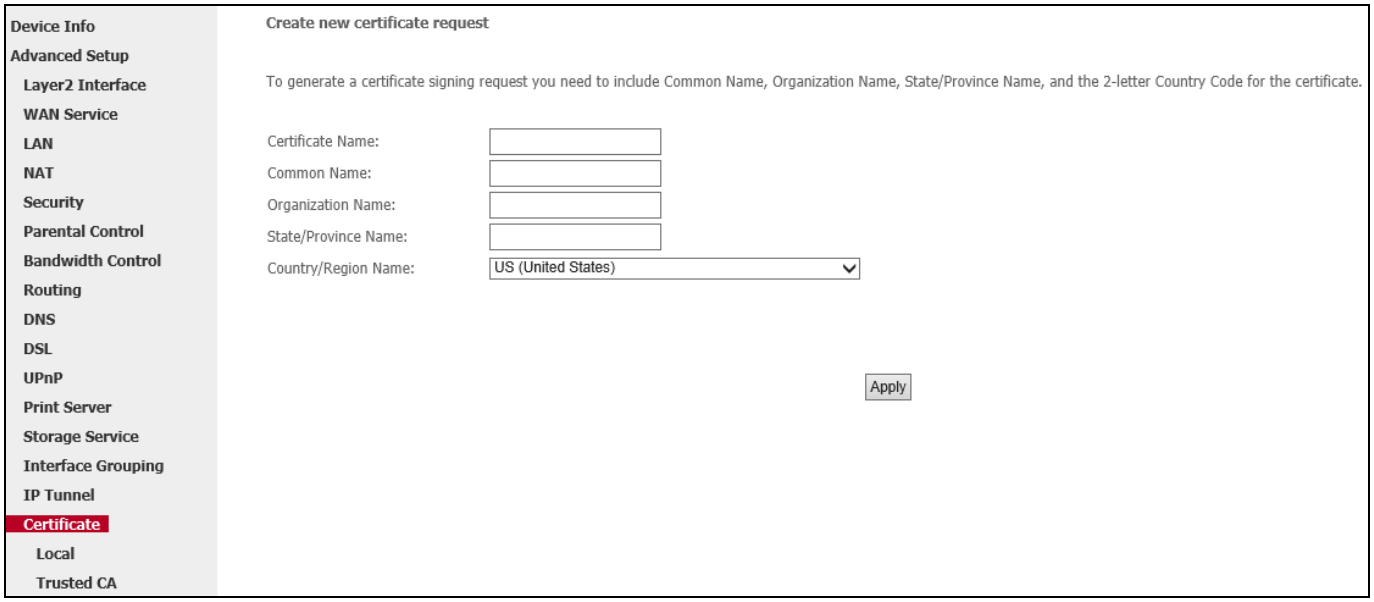
2.16.1 Local Certificates

This section is to apply a CA certificate, or import the CA certificate you applied before, for other network devices to verify your modem router’s identification.



To create a certificate signing request:

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



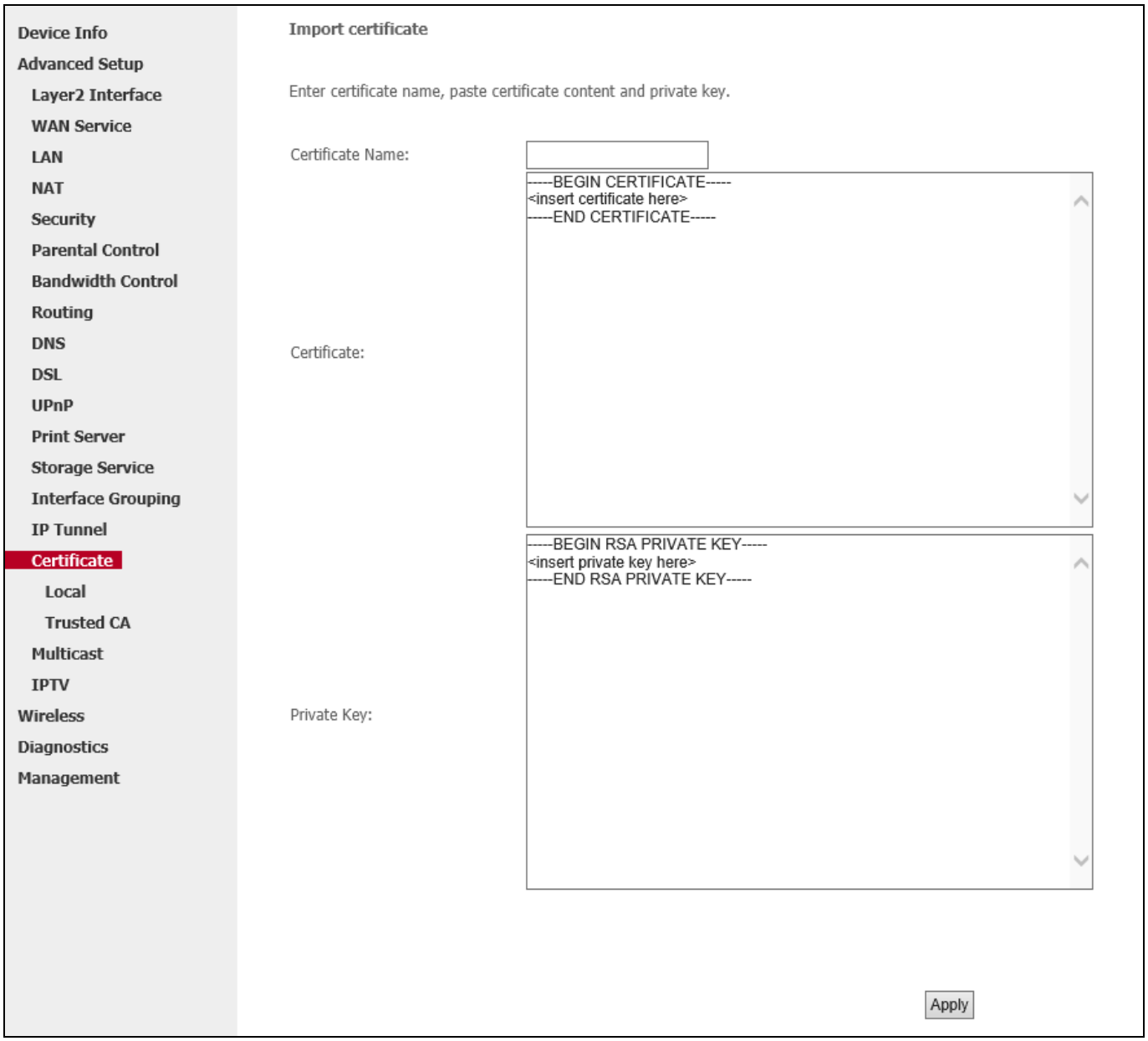
❷ Specify the Common Name, Organization Name and State/Province Name

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

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

To Import certificate:

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



❷ Enter the certificate name.

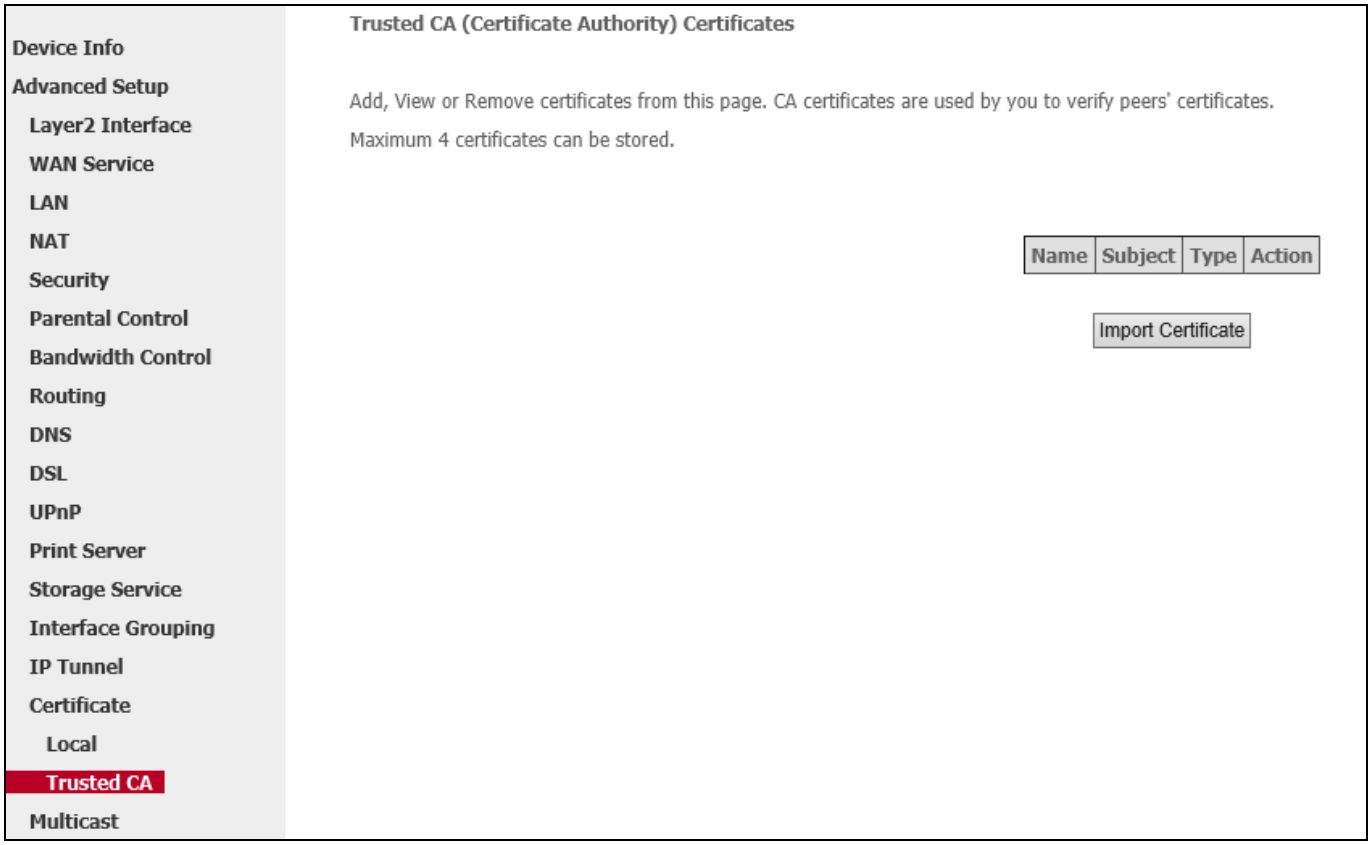
❸ Paste the certificate content and private key.

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

2.16.2 Trusted CA (Certificate Authority) Certificates

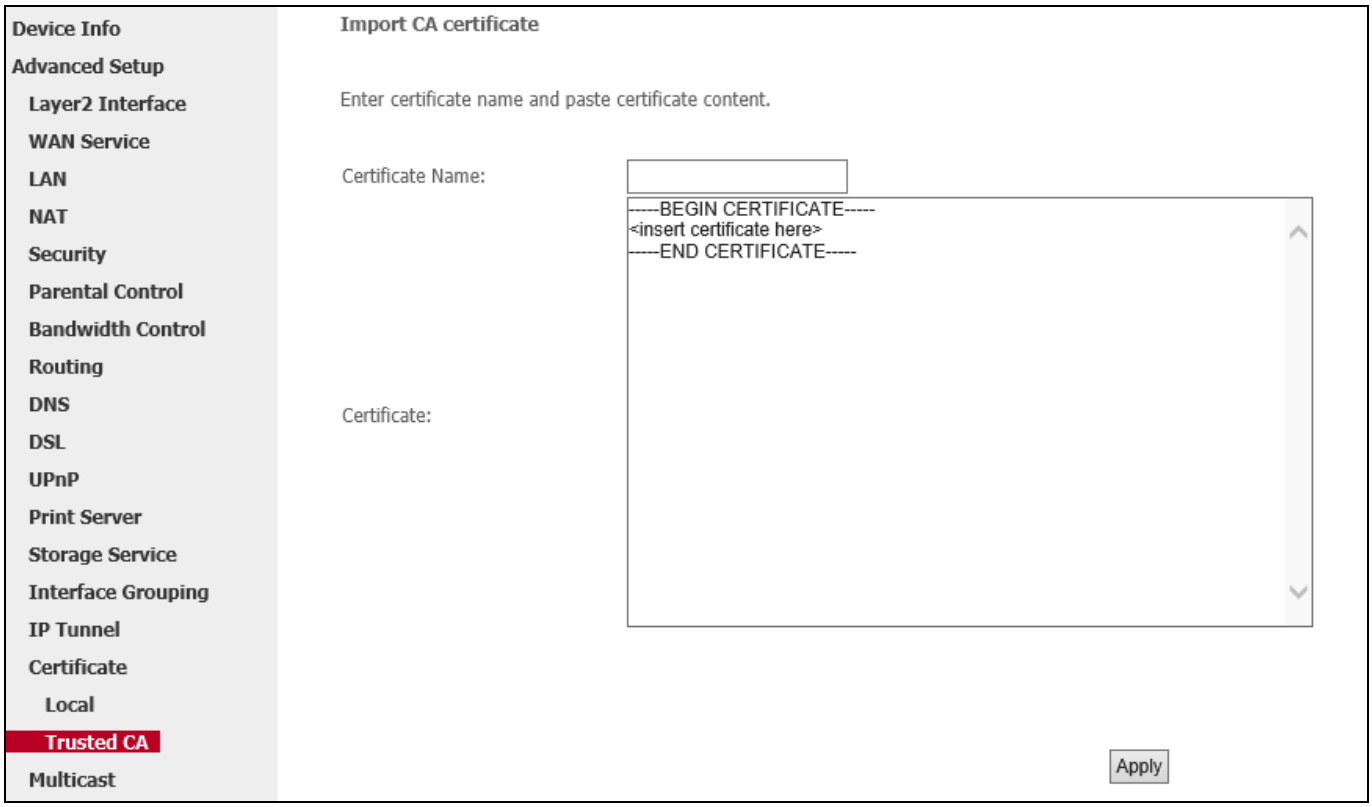
The CA certificate added to other network devices here is used for verifying the identification of other network devices.

E.g., in TR-069, you can import the correct ACS server's CA certificate, to verify the ACS server's identification.



To Import certificate：

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



❷ Enter the certificate name.

❸ Paste the certificate content.

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

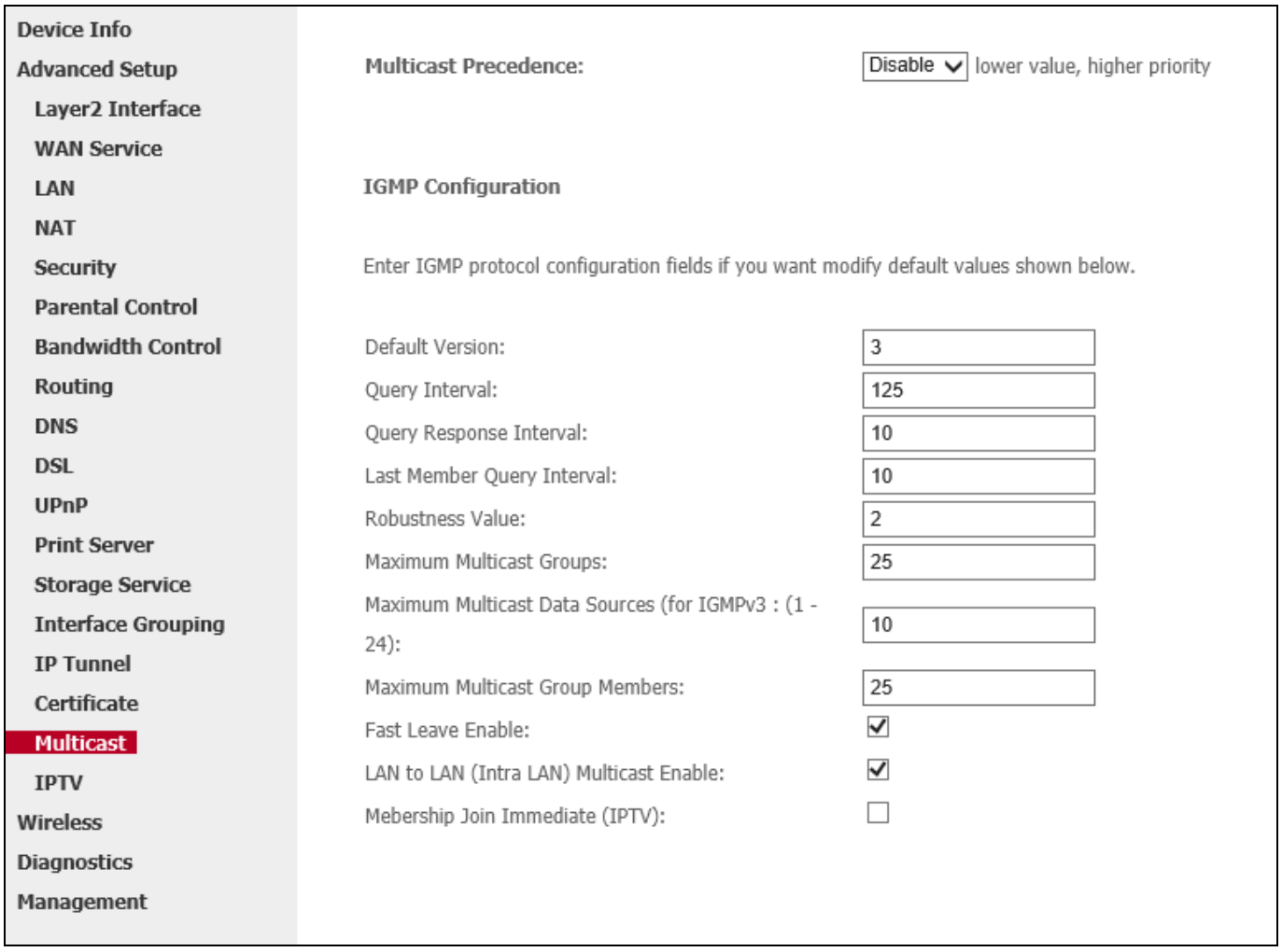
2.17 Multicast

To configure IGMP for IPv4

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

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

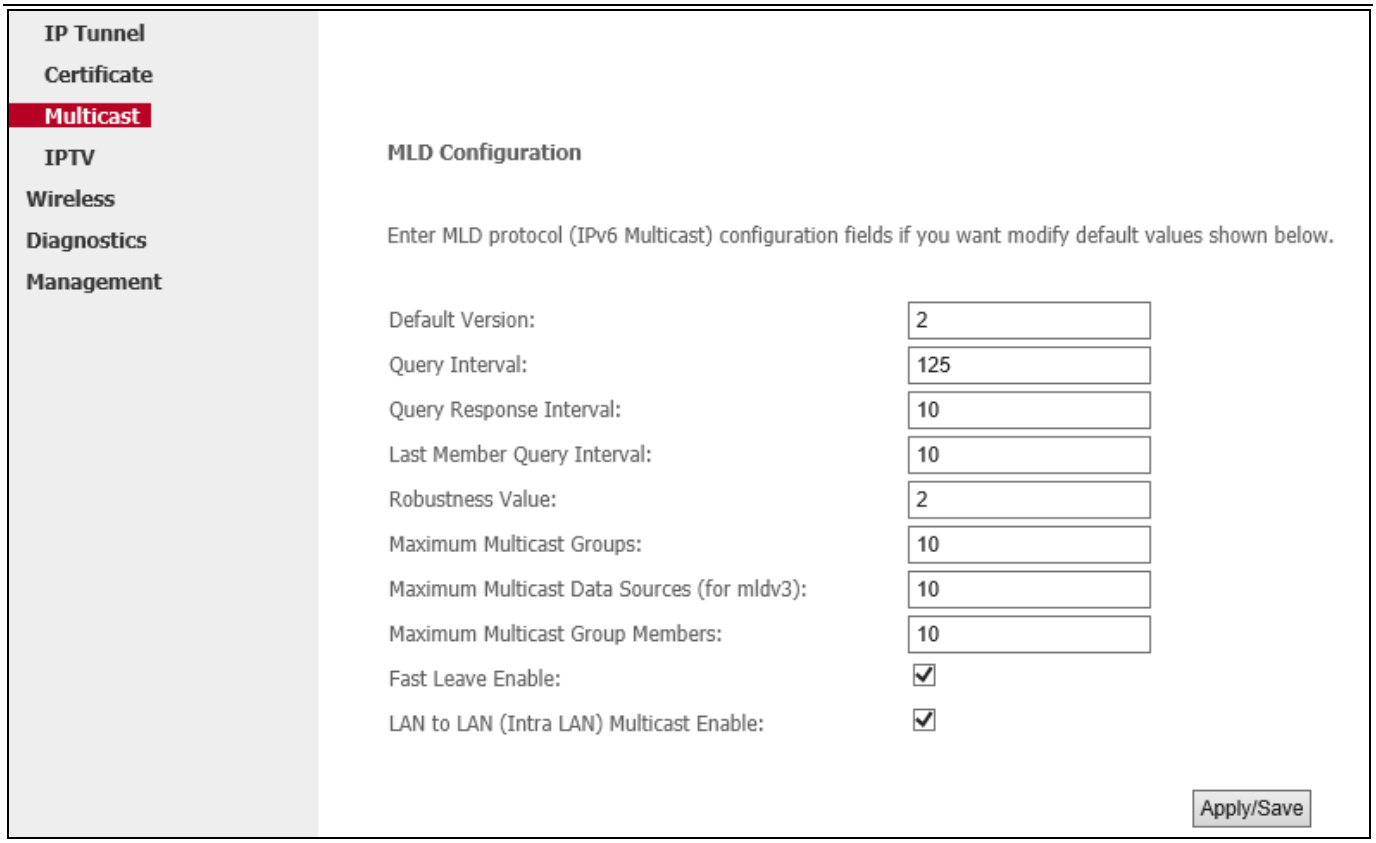
❸ Keep other options unchanged from factory defaults if you are not an advanced user. This is strongly recommended.



To configure IGMP for IPv6

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

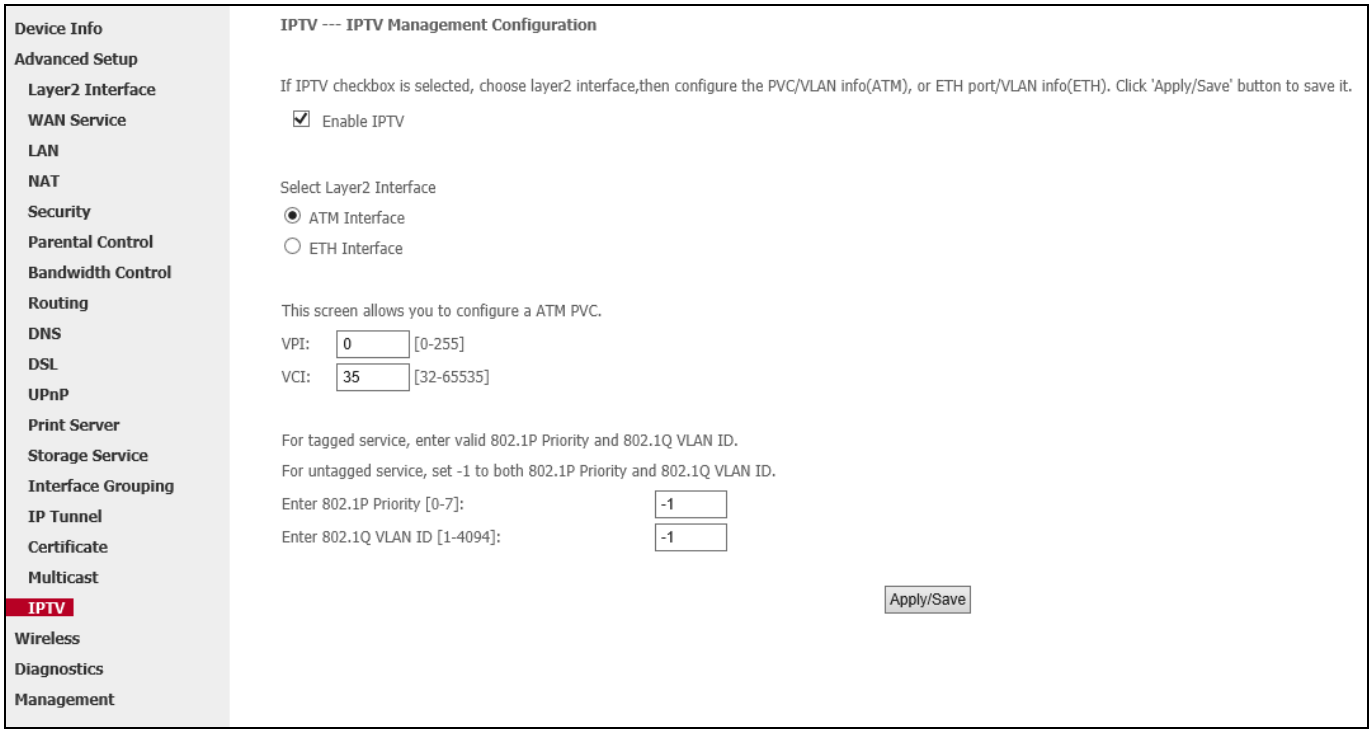
❷ Keep other options unchanged from factory defaults if you are not an advanced user. This is strongly recommended.



2.18 IPTV

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

Enable IPTV: Check/uncheck to enable/disable the IPTV service.



IPTV configuration for Phone Cable Access user:

1) Enable **IPTV**.

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

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

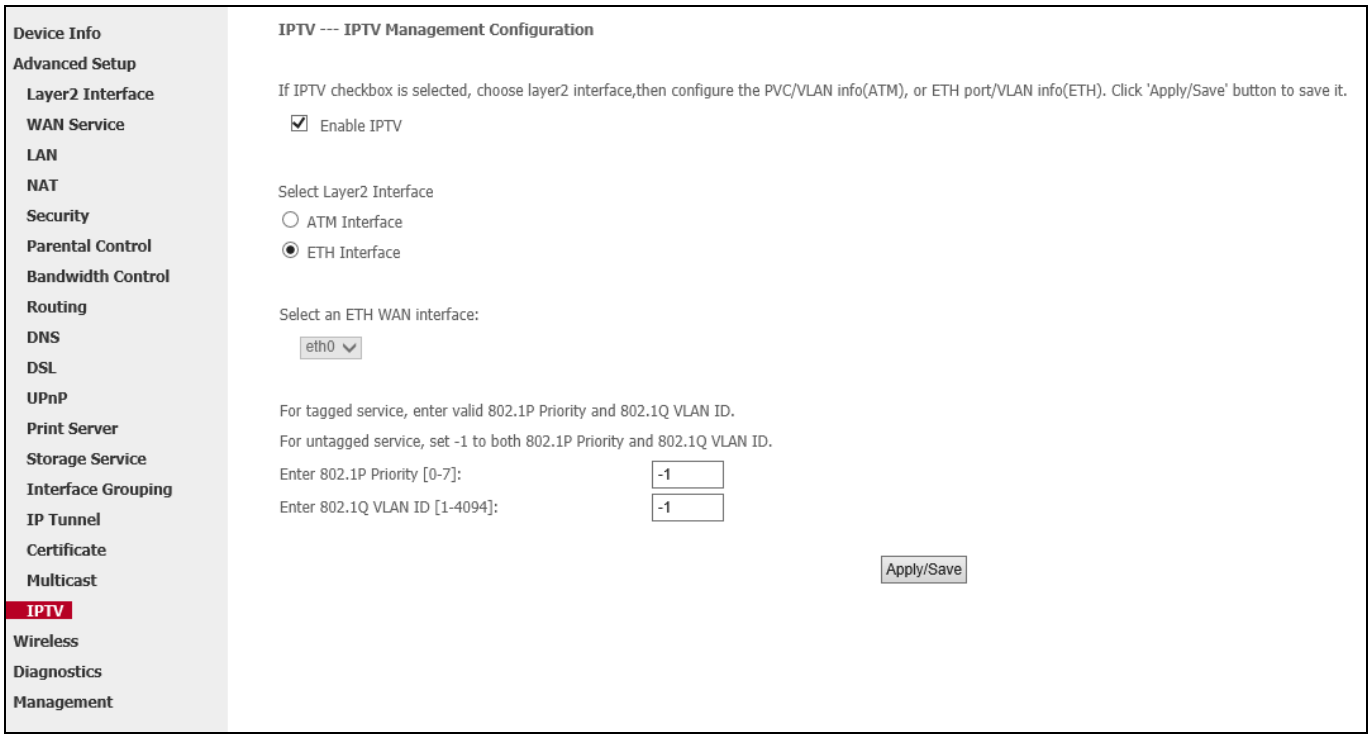
4) Click **Apply/Save**.

IPTV configuration for Ethernet Cable Access user:

1) Enable **IPTV**.

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

3) Click **Apply/Save**.



After successful IPTV configuration, Port 4 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.

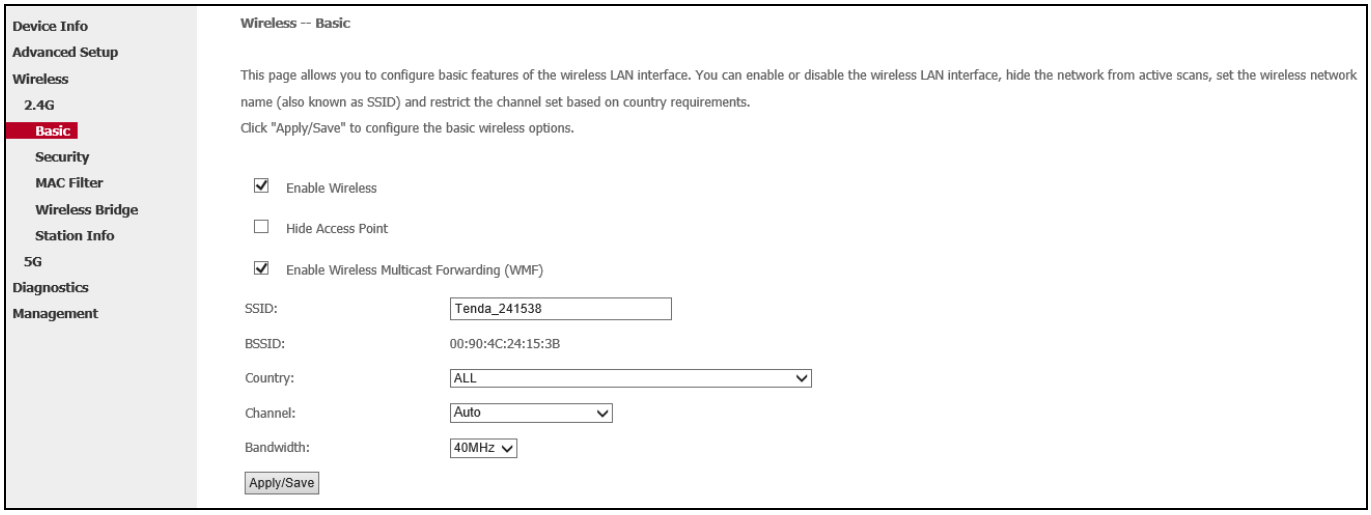
3. Wireless

3.1 2.4G

There are five submenus under the Wireless menu **Wireless**: **Basic**, **Security**, **MAC Filter**, **Wireless Bridge and Station Info**. Click any of them, and you will be able to configure the corresponding functions.

3.1.1 Basic

Click **Wireless > 2.4G** > **Basic** to enter the page where you can configure the basic settings of the wireless network of 2.4GHz.



Enable Wireless: check/uncheck to enable/disable the wireless network of 2.4GHz.

Hide Access Point: This option allows you to have your wireless network names (SSID) publicly broadcast or if you choose to enable it, the SSID will be hidden.

SSID: Service Set Identifier. This is the name of your wireless network.

Country: Select your country from the drop-down list.

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 neighboring networks. The default selection is **Auto**.

Bandwidth: Select the bandwidth from the drop-down list. There are two selections provided, 20MHz and 40MHz. The default setting is 40MHz.

Apply/Save: Click it to apply your current configurations.

3.1.2 Security

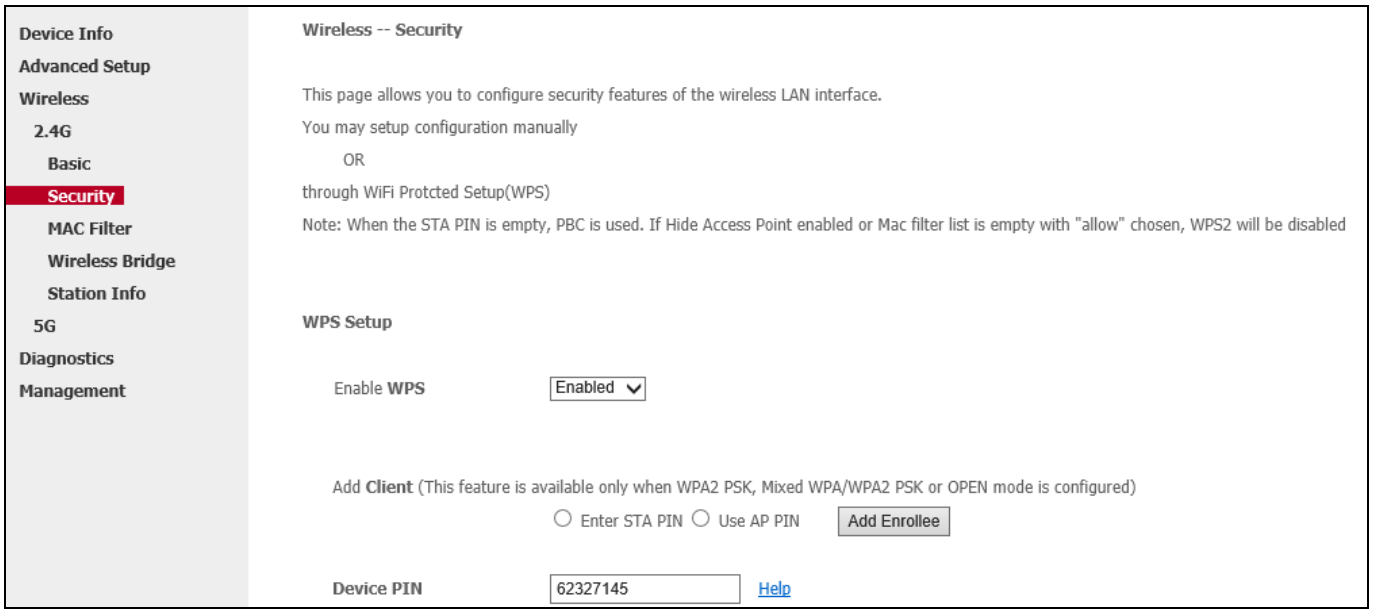
Click **Wireless > 2.4G** > **Security** to enter the page where you can configure the security settings of wireless network of 2.4GHz.

Note

1. To use the WPS security, the wireless client must be also WPS-capable.

2. When both STA PIN and Authorized MAC are empty, PBC is used. If Hide Access Point is enabled or Mac filter list is empty with "allow" chosen, WPS2 will be disabled.

3. WPS only supports WPA2, which means only when you select “WPA2” encryption or “Open”, you can change WPS status.



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. Simply enter a PIN code on the device web interface or press hardware WPS button (on the back panel of the device) and a secure wireless connection is established.

WPS (hardware button): Press the hardware WPS button on the device for 1 second and the WPS LED will keep blinking for about 2 minutes. Within the 2 minutes, press the WPS button on your wireless computer or other device. When the WPS displays a solid light, the device has joined your wireless network.

Device PIN: To use this option, you must know the PIN code from the wireless client and enter it in the corresponding field on your device while using the same PIN code on client side for such connection.

Enable WPS: Check/uncheck to enable/disable the WPS function. It is disabled by default.

Manual Setup AP

You can manually set the network authentication method:

Select data encryption;

Specify whether a network key is required to authenticate to this wireless network;

Specify the encryption strength;

Click **Apply/Save** when done.

Network Authentication: Select Open, Shared, 802.1X, 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.

Apply/Save: Click it to apply the current configurations.

3.1.3 MAC Filter

Click **Wireless > 2.4G > MAC Filter** to enter the page where you can configure the MAC filter of wireless network of 2.4GHz. The MAC-based Wireless Access Control feature can be used to allow or disallow clients to connect to your wireless network on the base of device’s MAC address.

MAC Restrict Mode：Disabled, Allow and Deny

- **Allow:** Allow only 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.
- **Disabled:** Disable MAC filter feature.

Add: Click to add a MAC address.

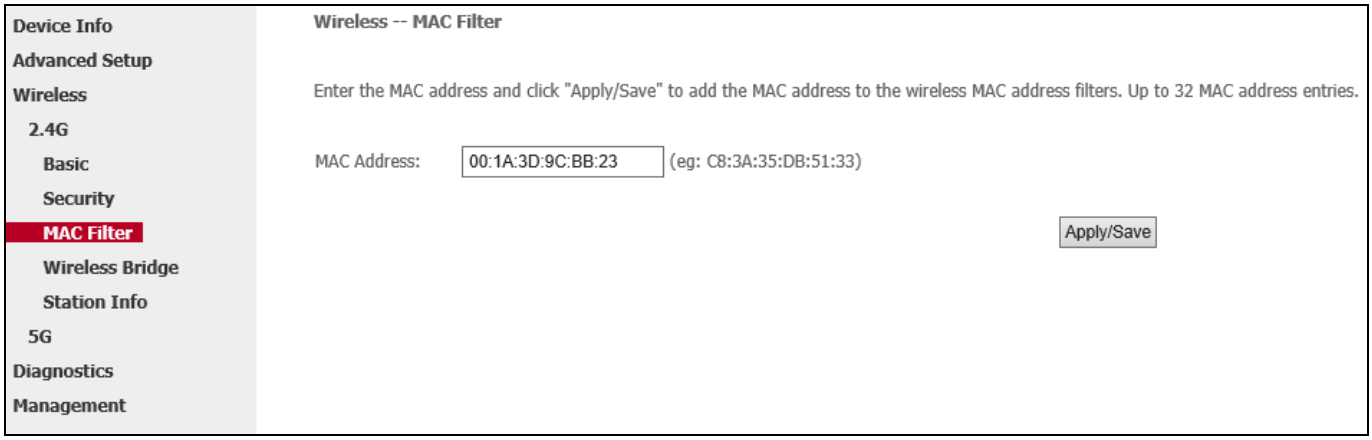
Remove: To delete an existing MAC address, first check the **Remove** box next to the MAC address in list and then click this button.

Example: 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:

❶ Select **Allow**.

❷ Click the **Apply/Save** button.

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



Note

1. If you select “Allow” MAC restrict mode and directly click **Apply/Save** instead of adding any MAC address to be filtered, WPS will be disabled (You can go to **Wireless > Security** to check WPS status).

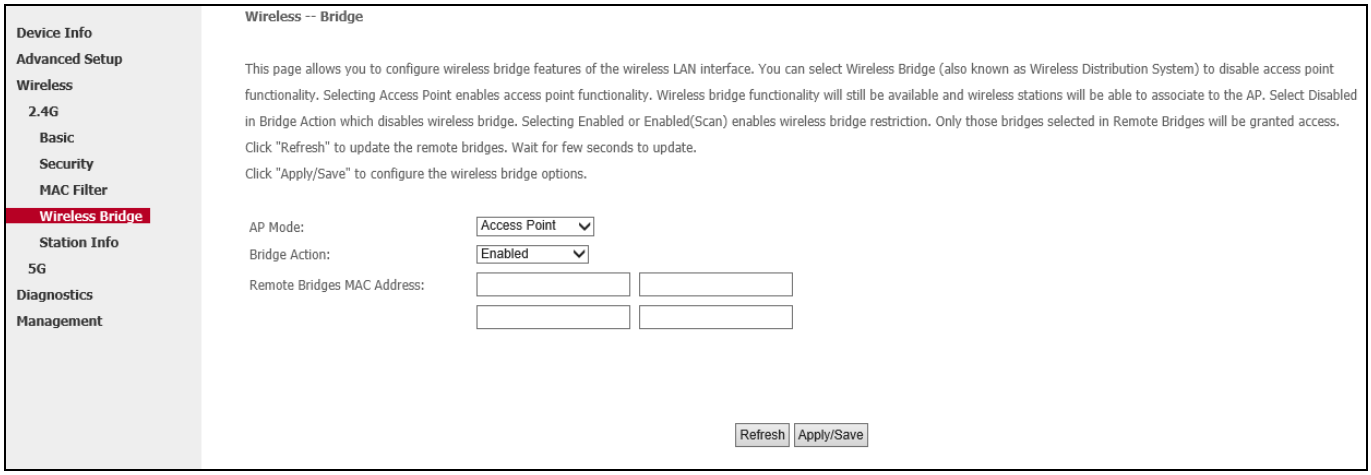
2. If you want to change the MAC filter mode above from “Allow” to “Deny”, just select **Deny** and click **Apply/Save**.

3.1.4 Wireless Bridge

Click **Wireless > 2.4G > Wireless Bridge** to enter the page where you can configure bridge settings.

This page allows you to configure wireless bridge (also known as Wireless Distribution System) features of the wireless LAN 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**. Select **Disabled** in **Bridge Action** which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting **Enabled** or **Enabled (Scan)** enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access. The Enabled (Scan) enables wireless bridge restriction and automatically scans the remote bridges.

Remote Bridges MAC Address: Specify the MAC address of the remote bridge. If you select the **Enabled (Scan)** option in Bridge Restrict, system automatically scans the remote bridges and you only need to select those bridges and their MAC addresses will be added to automatically.

Refresh: Click it to update the remote bridges. Wait for few seconds to update.

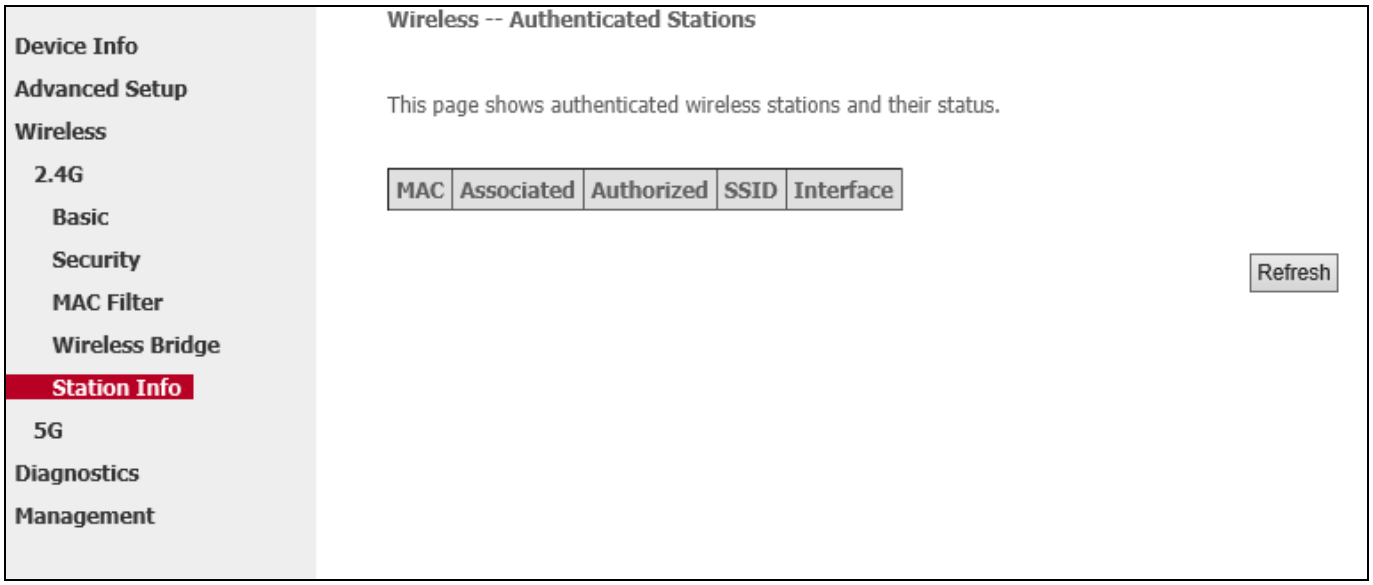
Apply/Save: Click it to apply and save the settings.

Note

The WDS feature (aka. 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.

3.1.5 Station Info

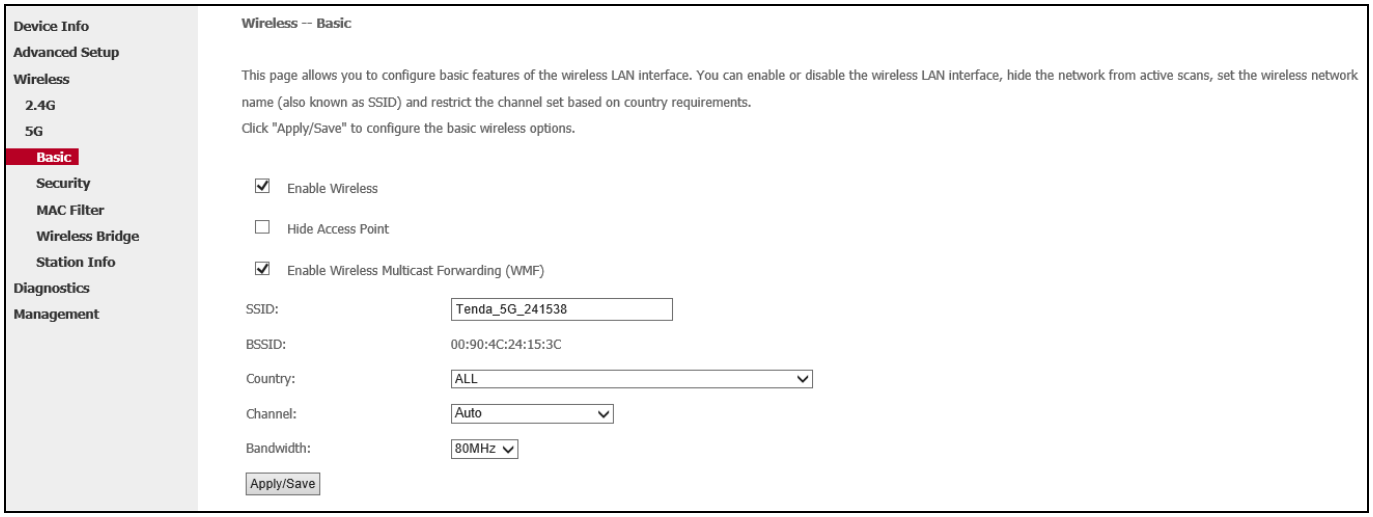
Click **Wireless > 2.4G > Station Info** to enter the page where displays authenticated wireless stations and their status.



3.2 5G

3.2.1 Basic

Click **Wireless > 5G** > **Basic** to enter the page where you can configure the basic settings of the wireless network of 5GHz.



Enable Wireless: check/uncheck to enable/disable the wireless network of 5GHz.

Hide Access Point: This option allows you to have your wireless network names (SSID) publicly broadcast or if you choose to enable it, the SSID will be hidden.

SSID: Service Set Identifier. This is the name of your wireless network.

Country: Select your country from the drop-down list.

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 neighboring networks. The default selection is **Auto**.

Bandwidth: Select the bandwidth from the drop-down list. There are three selections provided, 20MHz, 40MHz and 80MHz. The default is 80MHz.

Apply/Save: Click it to apply your current configurations.

3.2.2 Security

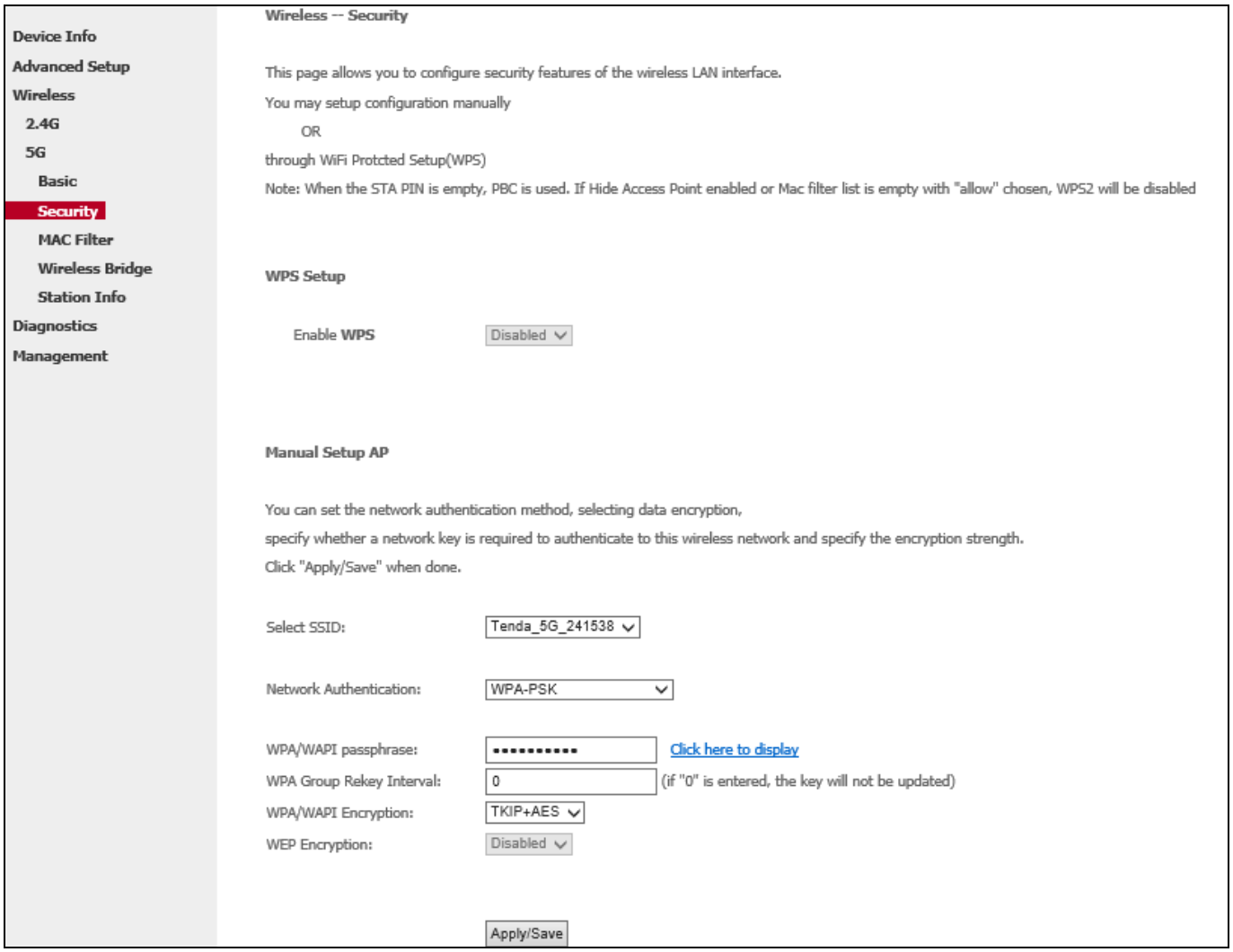
Click **Wireless > 5G** > **Security** to enter the page where you can configure the security settings of wireless network of 5GHz.

Note

1. To use the WPS security, the wireless client must be also WPS-capable.

2. When both STA PIN and Authorized MAC are empty, PBC is used. If Hide Access Point is enabled or Mac filter list is empty with "allow" chosen, WPS2 will be disabled.

3. WPS only supports WPA2, which means only when you select “WPA2” encryption or “Open”, you can change WPS status.



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. Simply enter a PIN code on the device web interface or press hardware WPS button (on the back panel of the device) and a secure wireless connection is established.

WPS (hardware button): Press the hardware WPS button on the device for 1 second and the WPS LED will keep blinking for about 2 minutes. Within the 2 minutes, press the WPS button on your wireless computer or other device. When the WPS displays a solid light, the device has joined your wireless network.

Device PIN: To use this option, you must know the PIN code from the wireless client and enter it in the corresponding field on your device while using the same PIN code on client side for such connection.

Enable WPS: Check/uncheck to enable/disable the WPS function. It is disabled by default.

Manual Setup AP

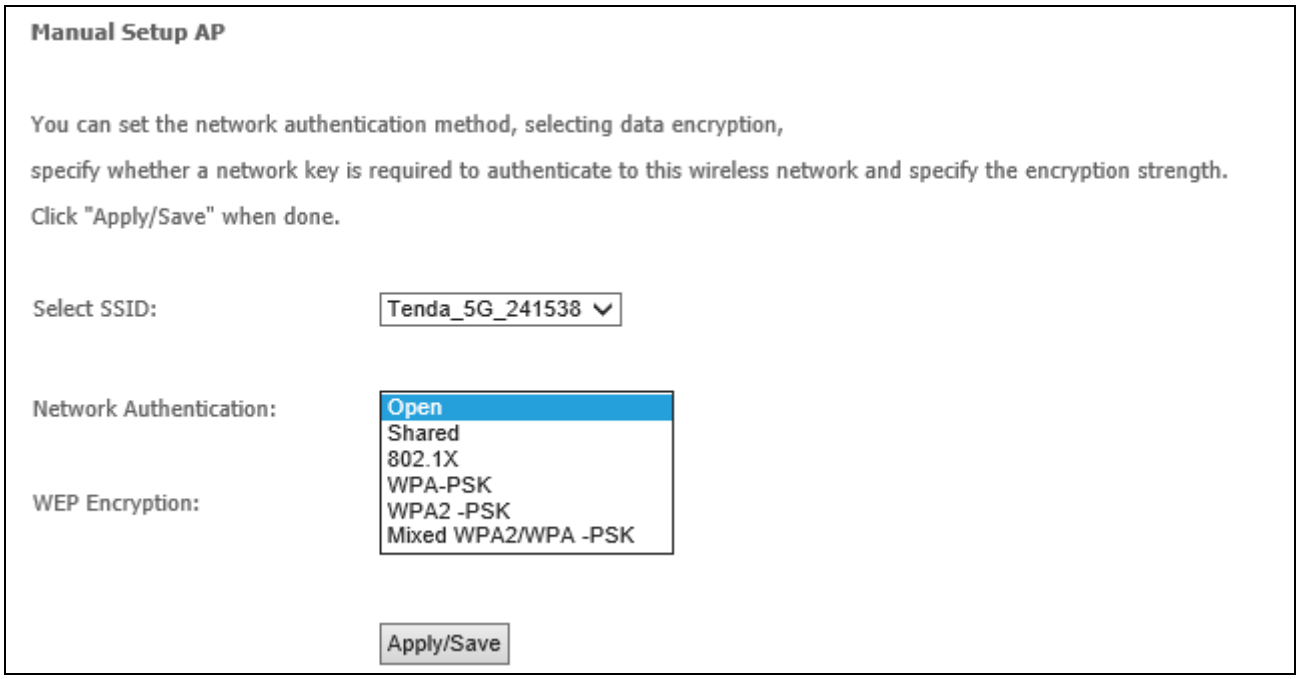
You can manually set the network authentication method:

Select data encryption;

Specify whether a network key is required to authenticate to this wireless network;

Specify the encryption strength;

Click **Apply/Save** when done.



Network Authentication: Select Open, Shared, 802.1X, 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 TKIP, AES, or TKIP+AES.

Apply/Save: Click it to apply the current configurations.

3.2.3 MAC Filter

Click **Wireless > 5G > MAC Filter** to enter the page where you can configure the MAC filter of wireless network of 5GHz. 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.
- **Disabled:** Disable MAC filter feature..

Add: Click 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.

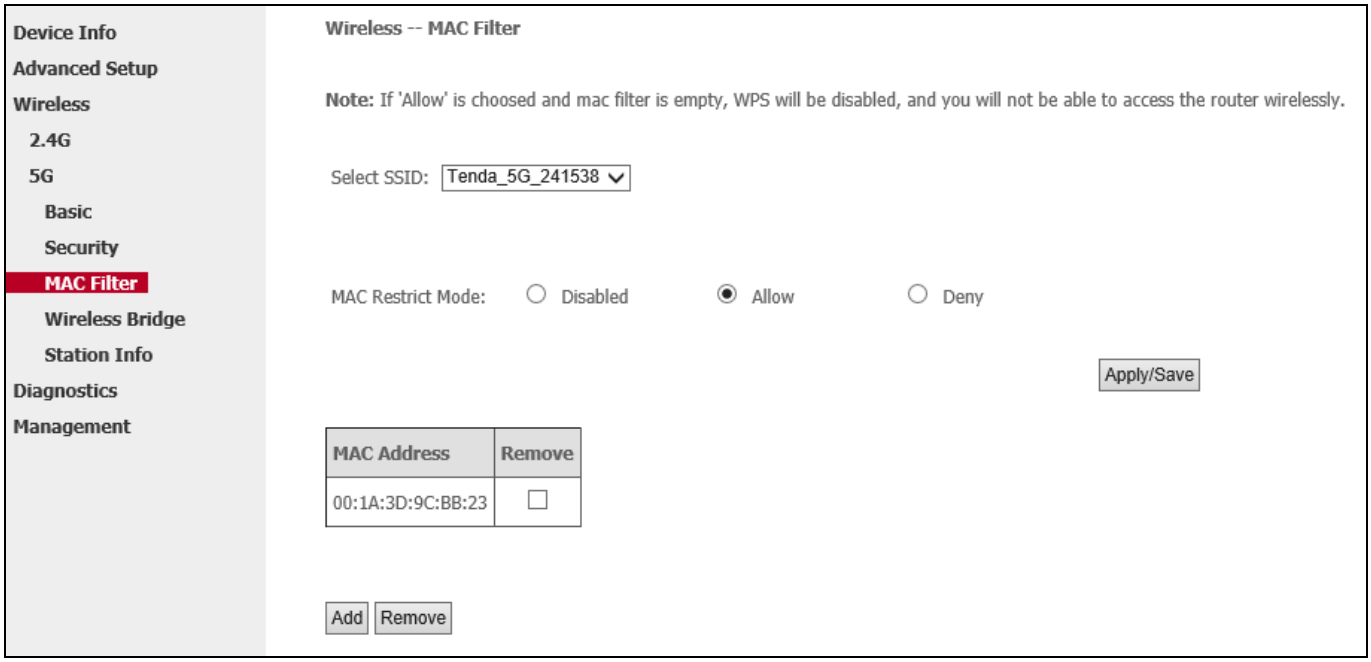
Example: To allow only the PC at the MAC address of 00:1A:3D:9C:BB:23 to connect to your wireless network, do as follows:

❶ Select **Allow**.

❷ Click the **Apply/Save** button.

❸ Enter 00:1A:3D:9C:BB:23 in the MAC address box as shown in the figure below.

❹ Click **Apply/Save**.



Note

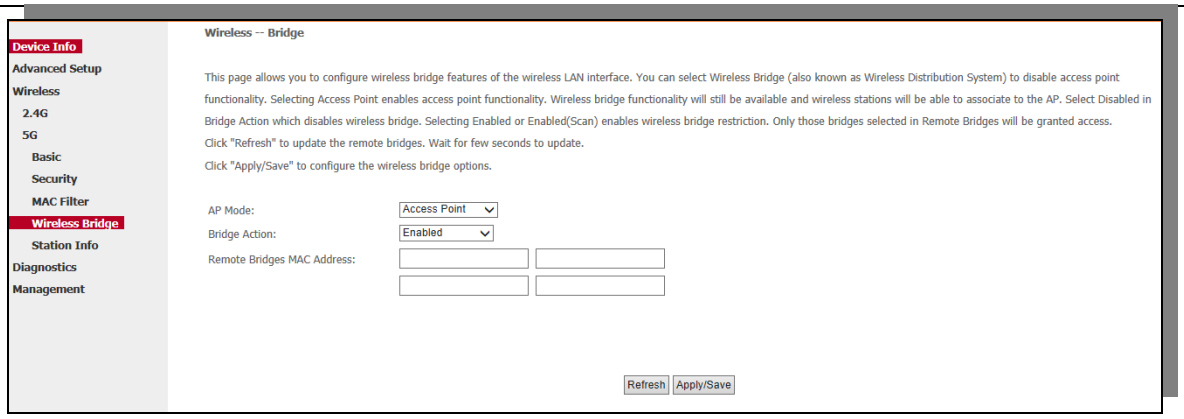
1. If you select “Allow” MAC restrict mode and directly click **Apply/Save** instead of adding any MAC address to be filtered, WPS will be disabled.

2. If you want to change the MAC filter mode above from “Allow” to “Deny”, just select **Deny** and click **Apply/Save**.

3.2.4 Wireless Bridge

Click **Wireless > 5G > Wireless Bridge** to enter the page where you can configure bridge settings. This page allows you to configure wireless bridge (also known as Wireless Distribution System) features of the wireless LAN 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**. Select **Disabled** in **Bridge Action** which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting **Enabled** or **Enabled (Scan)** enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access. The Enabled (Scan) enables wireless bridge restriction and automatically scans the remote bridges.

Remote Bridges MAC Address: Specify the MAC address of the remote bridge. If you select the **Enabled (Scan)** option in Bridge Restrict, system automatically scans the remote bridges and you only need to select those bridges and their MAC addresses will be added to automatically.

Refresh: Click it to update the remote bridges. Wait for few seconds to update.

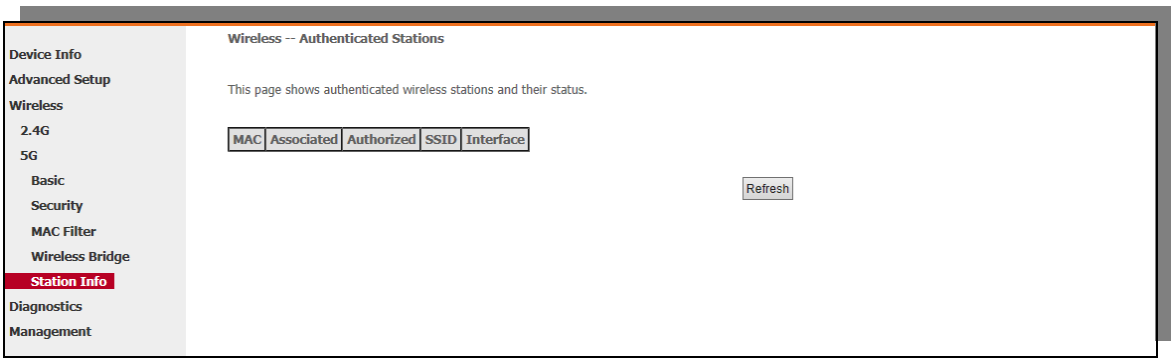
Apply/Save: Click it to apply and save the settings.

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.

3.2.5 Station Info

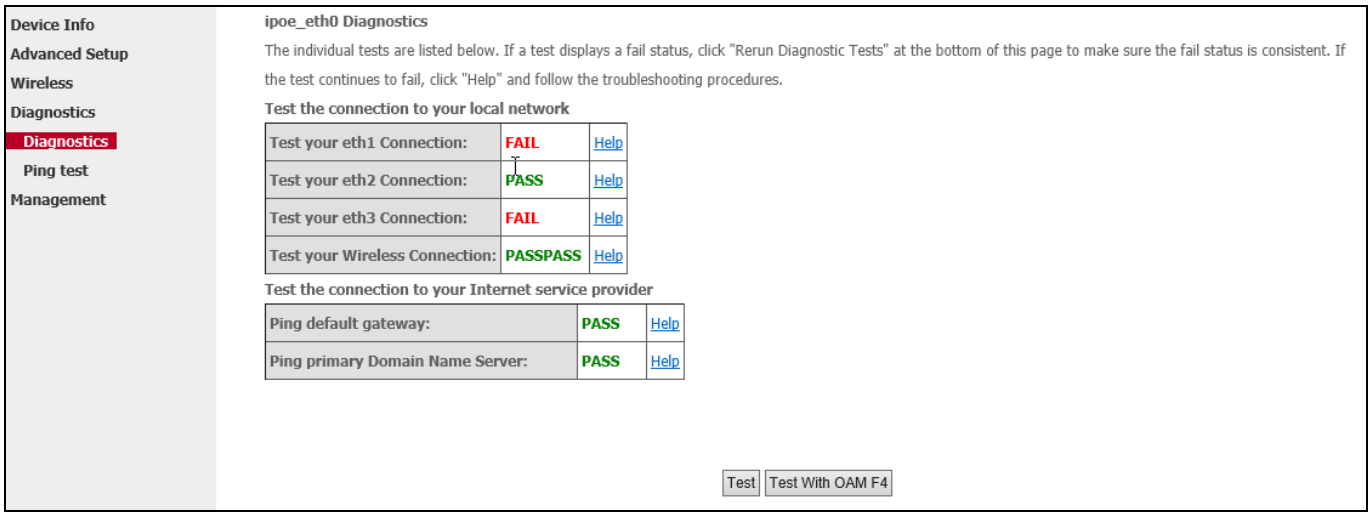
Click **Wireless > 5G > Station Info** to enter the page where displays authenticated wireless stations and their status.



4. Diagnostics

4.1 Diagnostics

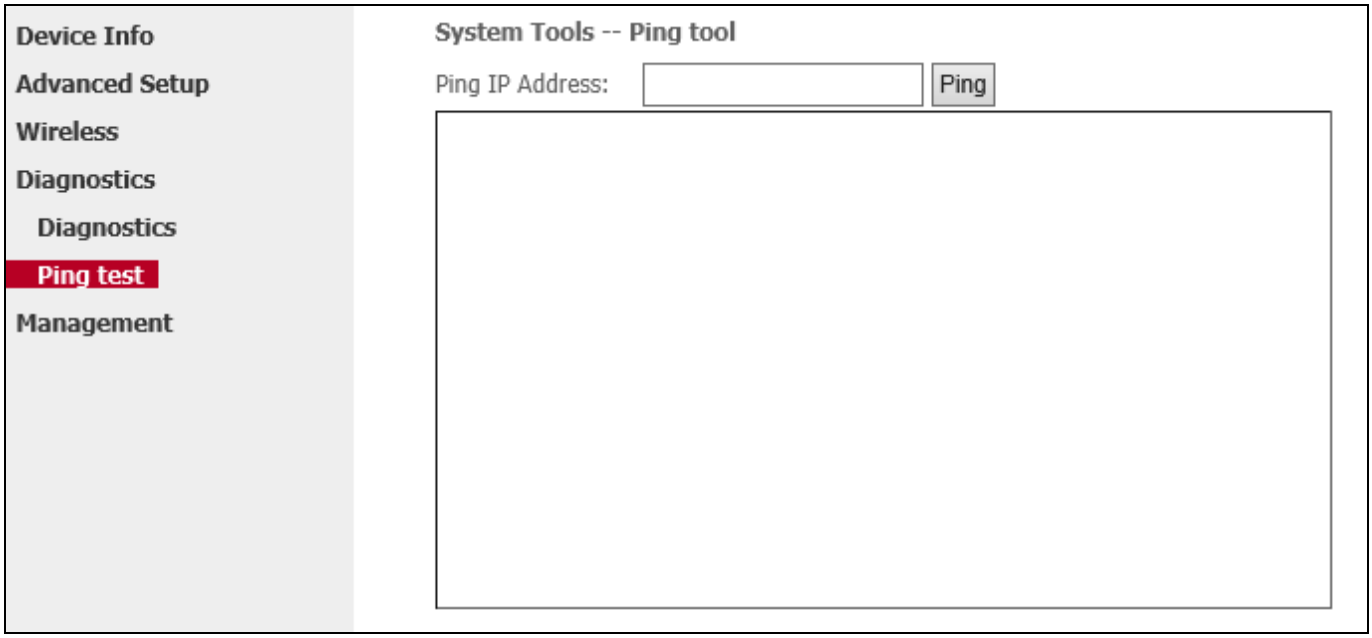
The modem router is capable of testing the connection to your DSL service provider, the connection to your Internet service provider and the connection to your local network. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent.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



4.2 Ping test

Ping utility can help test your network 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**.

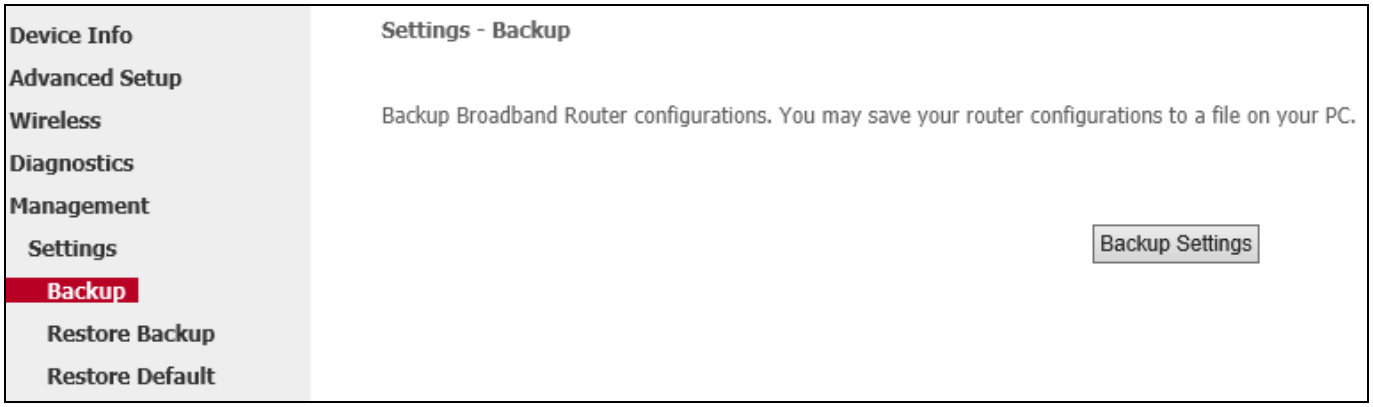


5. Management

5.1 Settings

5.1.1 Backup

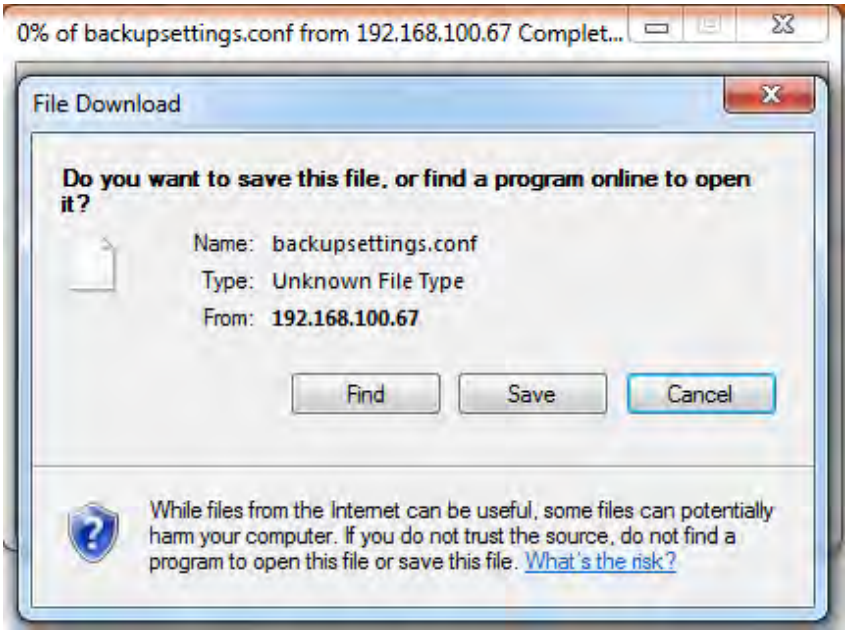
Here you can save a copy of your device's configurations to your computer. Once you have configured the device, you can save these settings to a configuration file on your local hard drive. The configuration file can later be imported to your device in case the device is reset to factory default settings.



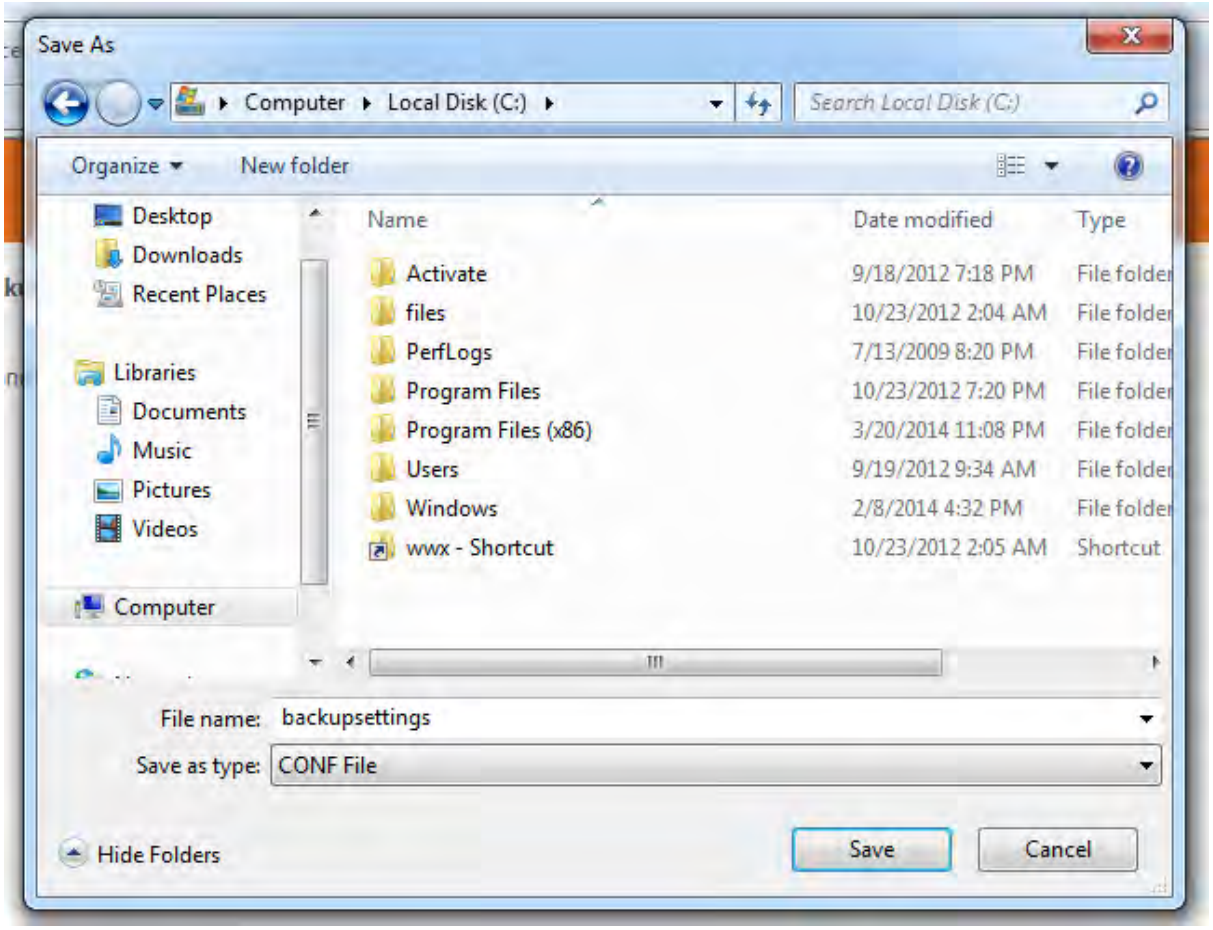
To backup settings:

❶ Click **Backup Settings** button.

❷ Click **Save** on the popup dialog shown as below.



❸ Specify a path to save the backup file, and then click **Save**.

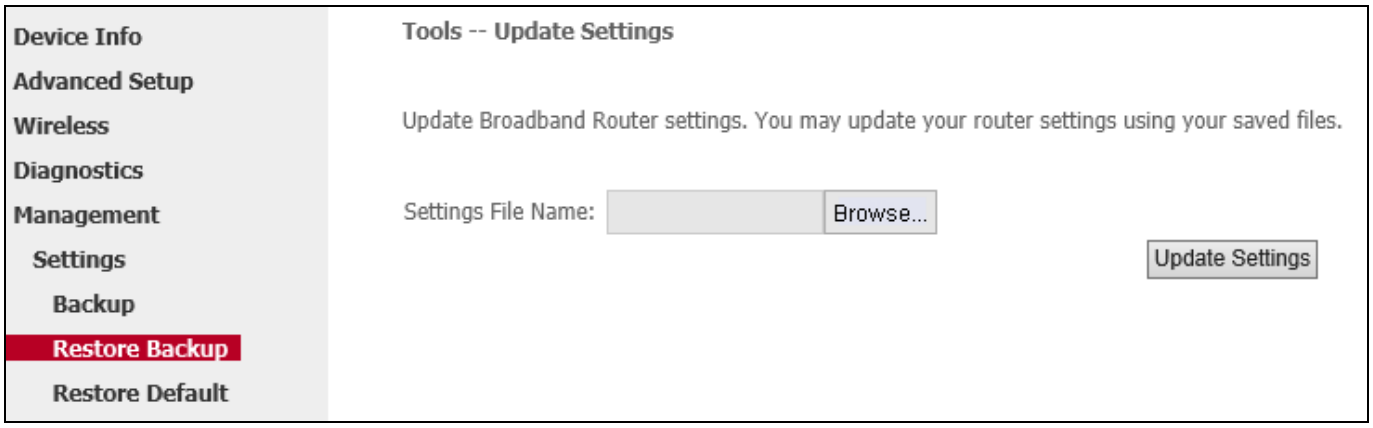


Note

The backup file is named as “backupsettings” and suffixed by .conf. For better memorizing, you can change the name, but do not change the file suffix.

5.1.2 Restore Backup

Here you can restore the configuration from a file saved on your PC.



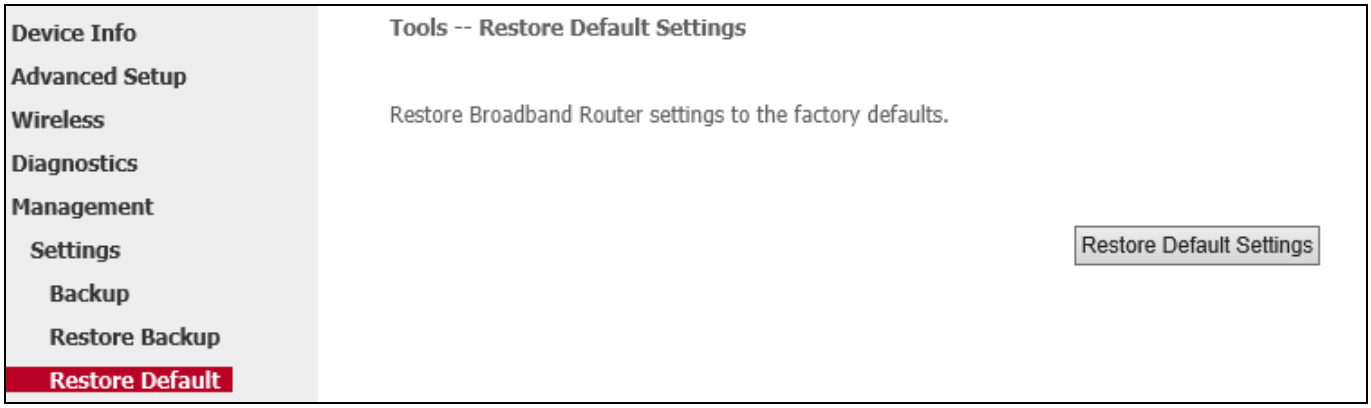
To update the firmware:

❶ Click **Browse** to locate and upload the updating firmware.

❷ Click **Update Settings**.

5.1.3 Restore Default

Under some circumstances (for example, you cannot visit a website or unfortunately forget the login password), you may need to remove the existing configuration and restore the factory default settings.



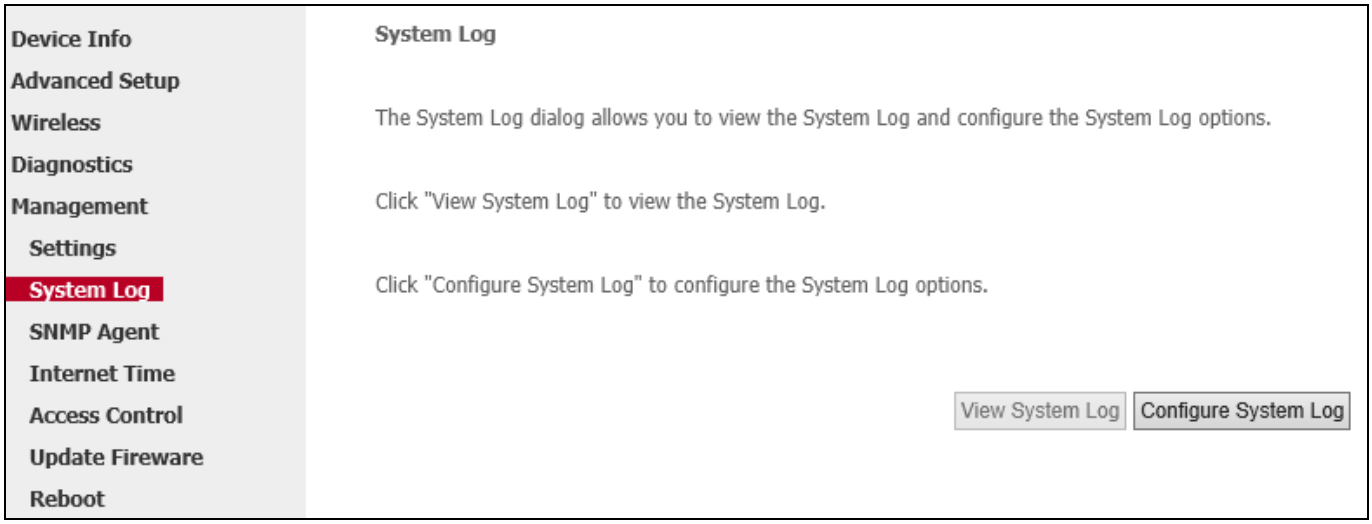
To restore the device to factory default:

Method 1: Click **Restore Default Settings** in above screen page.

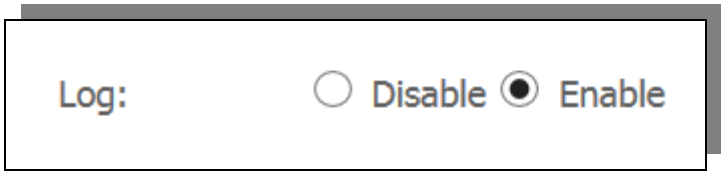
Method 2: Press the WPS/RST button on the back panel of the device for about 8 seconds when all LEDs light and then off. The device is reset.

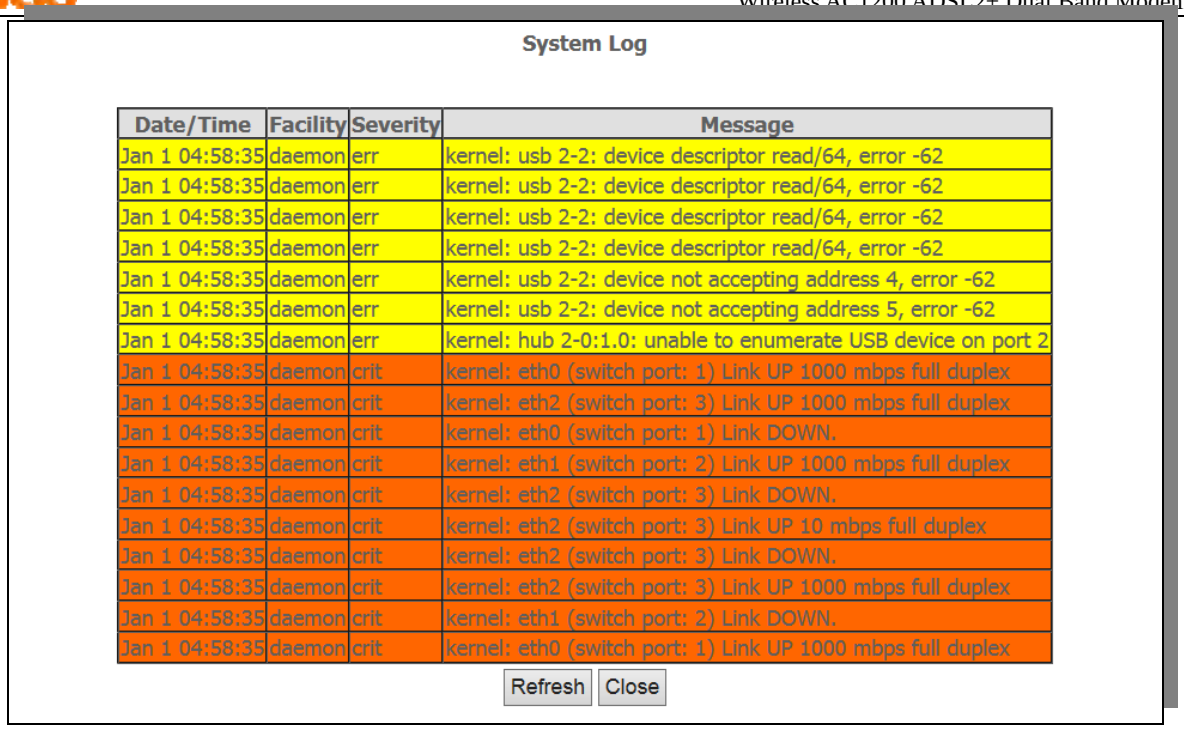
5.2 System Log

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

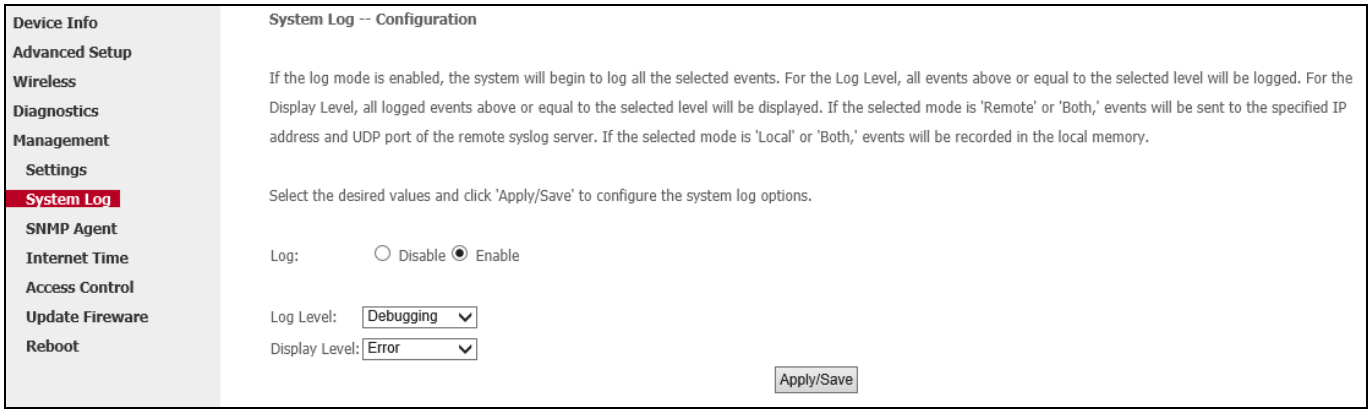


To view the System Log, firstly ensure log is enabled, otherwise you cannot view.





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



Log: If Enable is selected, the system will begin to log all the selected events.

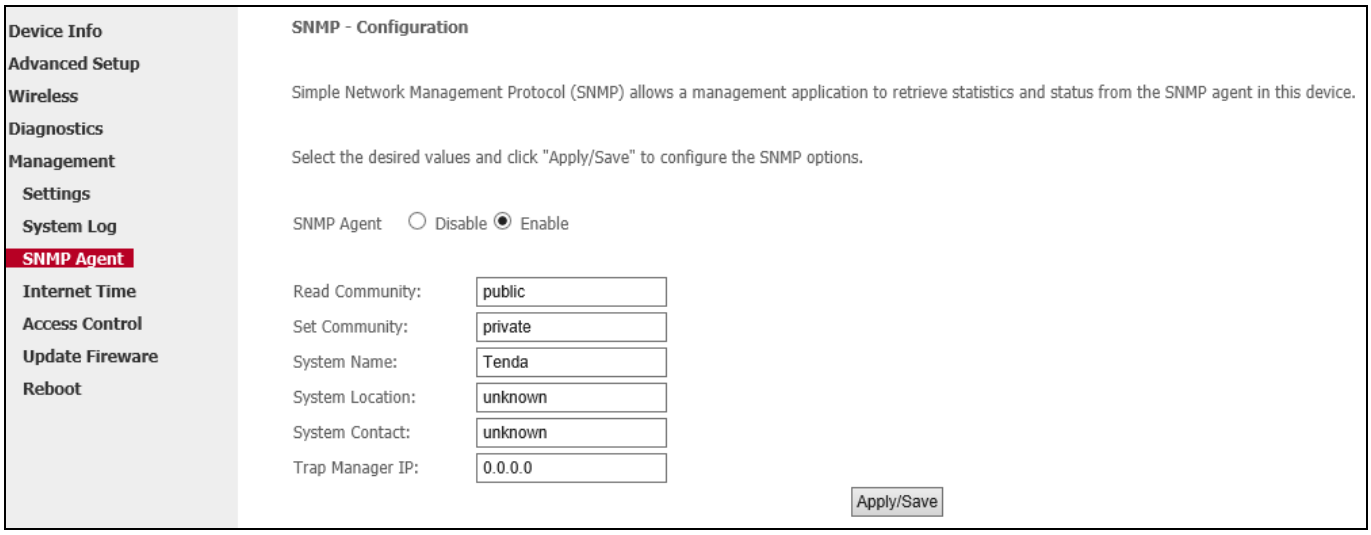
Log Level: All events above or equal to the selected level will be logged.

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.

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.



To configure SNMP Agent:

❶ Enable SNMP agent.

❷ Configure the read operation command between SNMP management and SNMP agent. Read Community-SNMP agent allows SNMP management to read variable in MIB with read community.

❸ Configure the read and write operation command between SNMP management and SNMP agent. Write Community-SNMP agent allows SNMP management to read and write variable in MIB with write community.

❹ Configure the device name, network location and admin contact to make the device be conveniently managed by SNMP management.

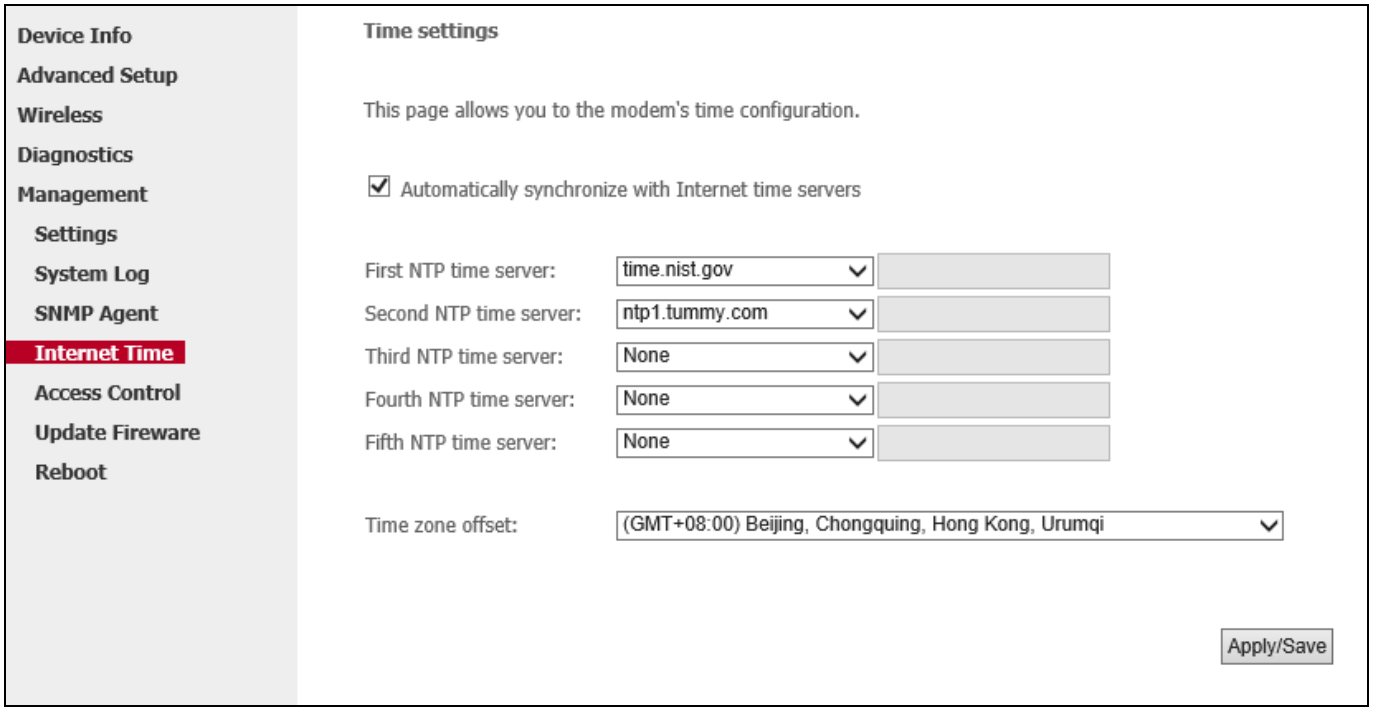
❺ Configure the IP address to which the SNMP agent sends a trap message.

❻ Click **Apply/Save**.

❼ After above configurations, click **Management > Access Control > Accessctrl** to enter the access control-service interface to enable SNMP service.

5.4 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.



Time Server: Internet time server domain.

To configure Internet time:

❶ Check **Automatically synchronize with Internet time servers** box.

❷ 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.

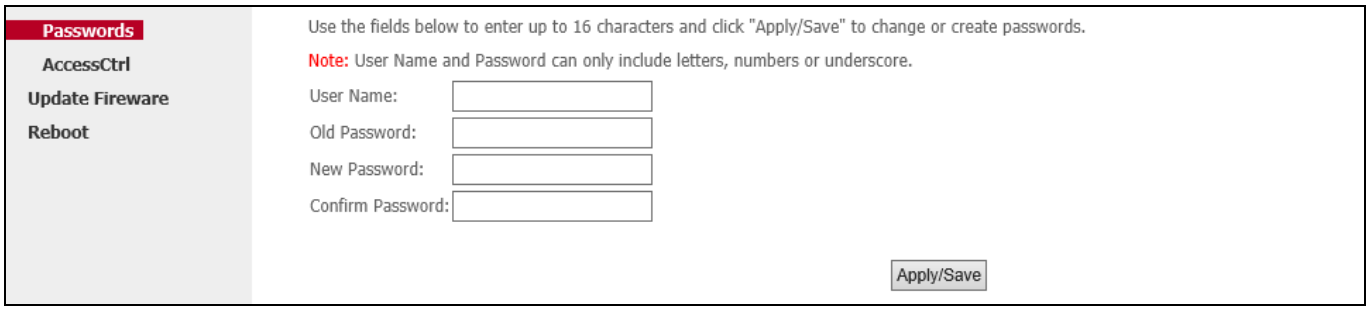
❸ Configure your time zone.

❹ Click **Apply/Save**.

5.5 Access Control

5.5.1 Password

The user name "admin" has unrestricted access to change and view configuration of your modem router.



User Name: Enter the user name.

Old Password: Enter the old password.

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

Confirm Password: Enter the new password again to confirm the new password.

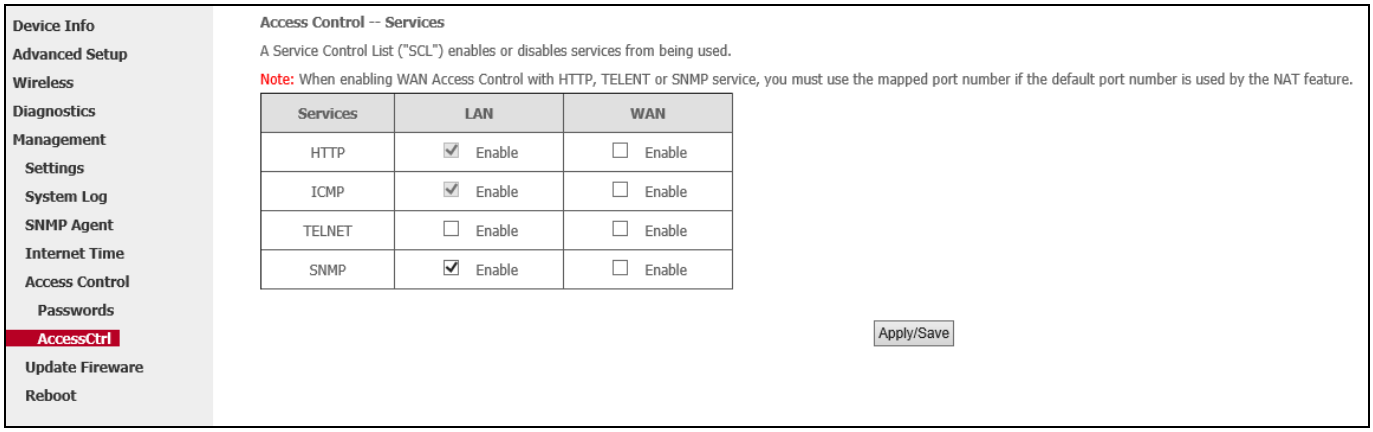
Apply/Save: Click this button to save configurations.

Note

Password cannot contain a space.

5.5.2 Access Control - Service

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



HTTP: Enabling the corresponding side (LAN/WAN) HTTP makes the device can be configured from the corresponding side (LAN/WAN) by a(n) admin/user/support.

ICMP: Enabling the corresponding side (LAN/WAN) ICMP makes the device's connection can be diagnosed via ping IP address from the corresponding side (LAN/WAN).

TELNET: Enabling the corresponding side (LAN/WAN) TELNET makes the user access the device via telnet from the corresponding side (LAN/WAN) and view the device details. Telnet is usually used to diagnose the device fault by users who know network knowledge.

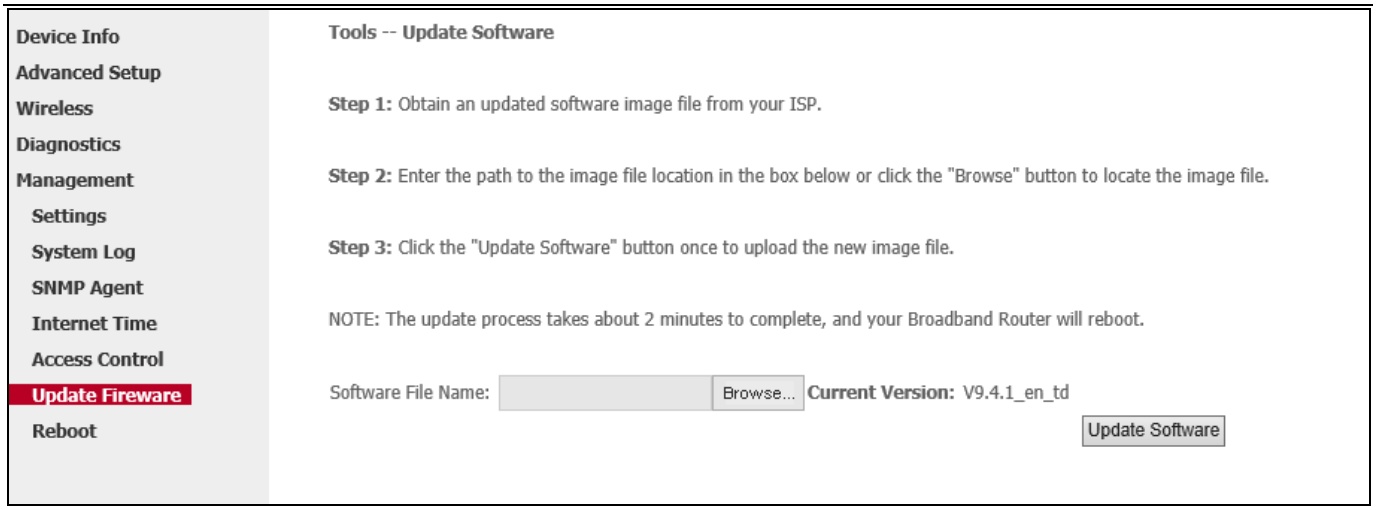
SNMP: Enabling the corresponding side (LAN/WAN) SNMP makes users manage the device via SNMP management client. This feature is usually used by network server or nerwork manager.

Note

1. If you are not an advanced user, we suggest you keep the default settings.
2. To access the device from the LAN side, log in the device with LAN IP address of the device as "admin" or "user"; to access the device from the WAN side, you must use the WAN IP address and log in as "support".

5.6 Update Firmware

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 go to our website (www.tendacn.com) to download the latest firmware to update your device.



To update software, do as follows:

❶ Download the latest firmware from our website: www.tendacn.com.

❷ Click the "Browse" button to locate and upload the firmware file.

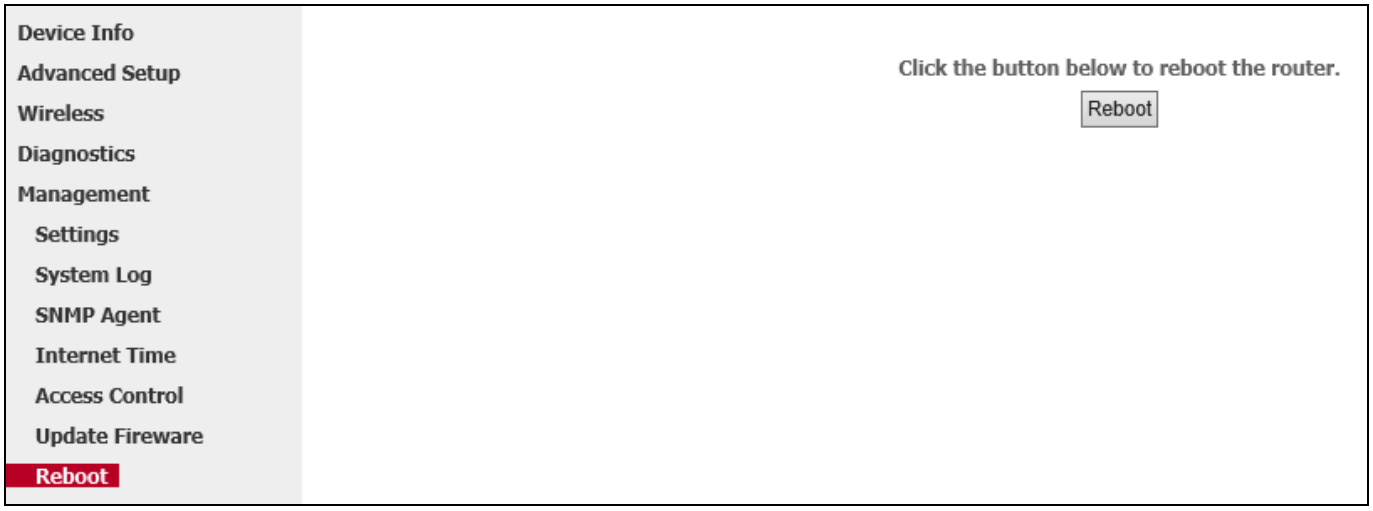
❸ Click the "Update Software" button to start updating.

Note

The update process takes about 2 minutes to complete, and after that your modem router will reboot.

5.7 Reboot

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

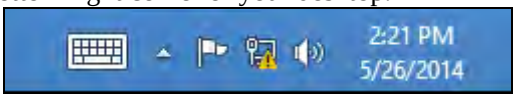


Appendix 1 Configure Your PC

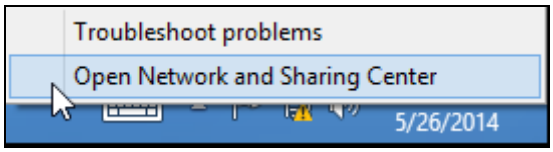
Screens to configure TCP/IP properties in other Operating Systems are similar to those below.

Windows 8

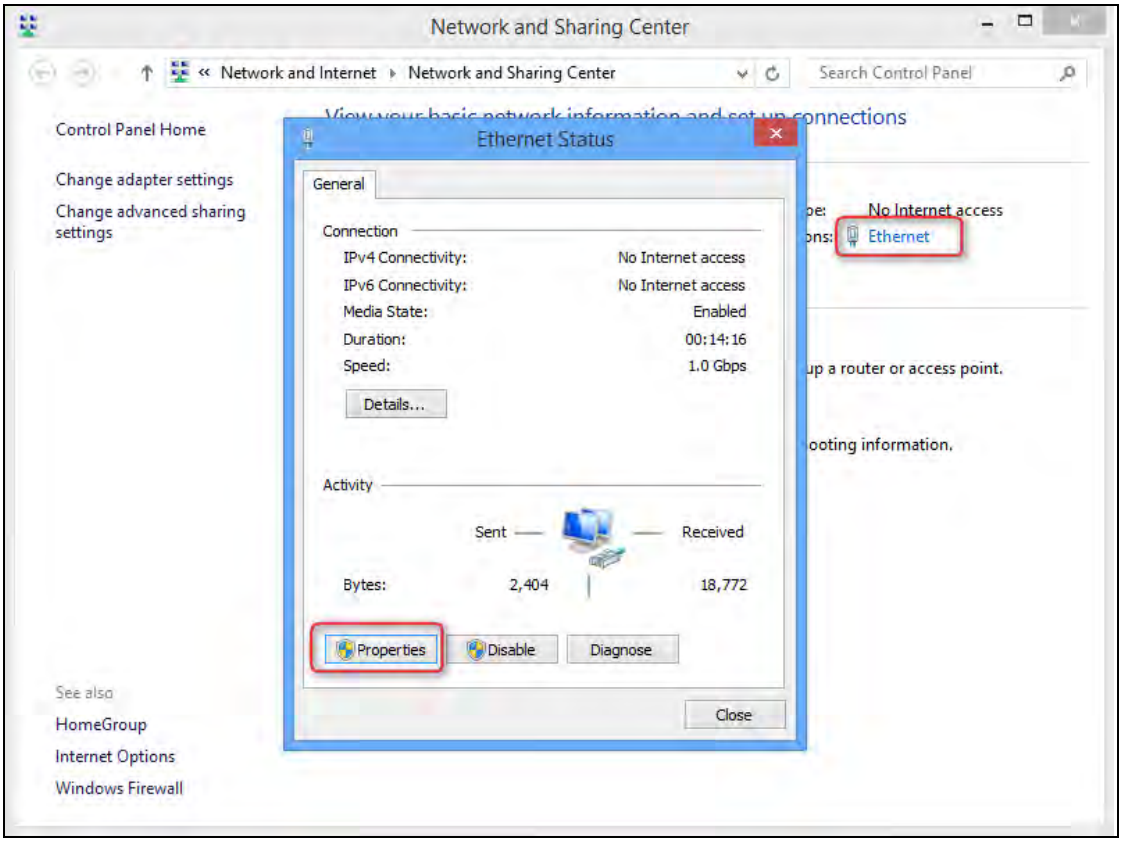
❶ Right click the icon on the bottom right corner of your desktop.



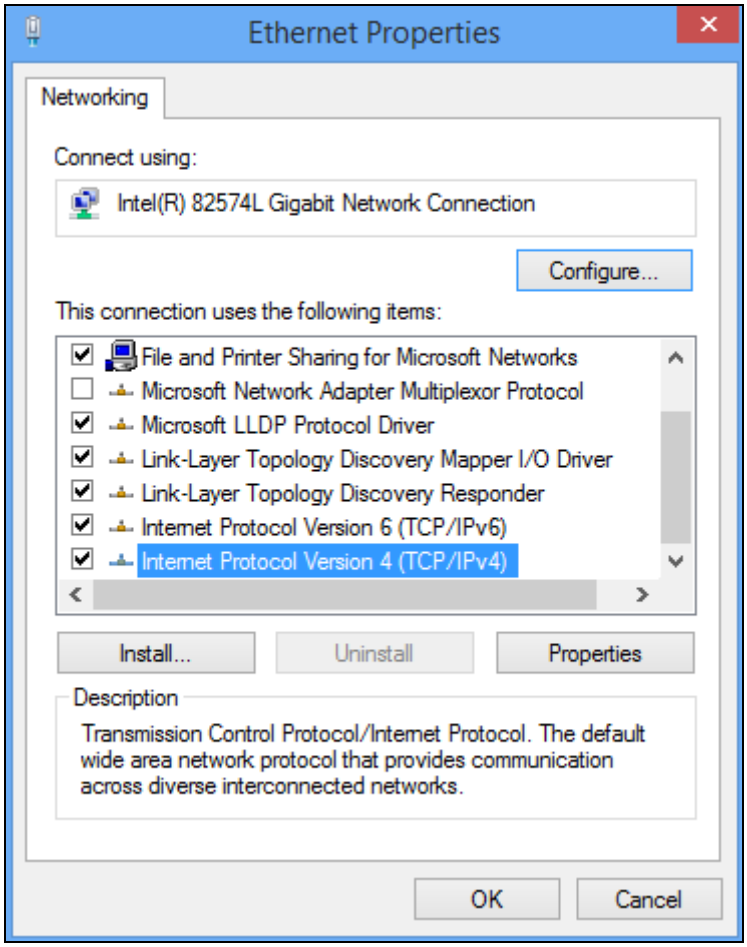
❷ Click **Open Network and Sharing Center**.



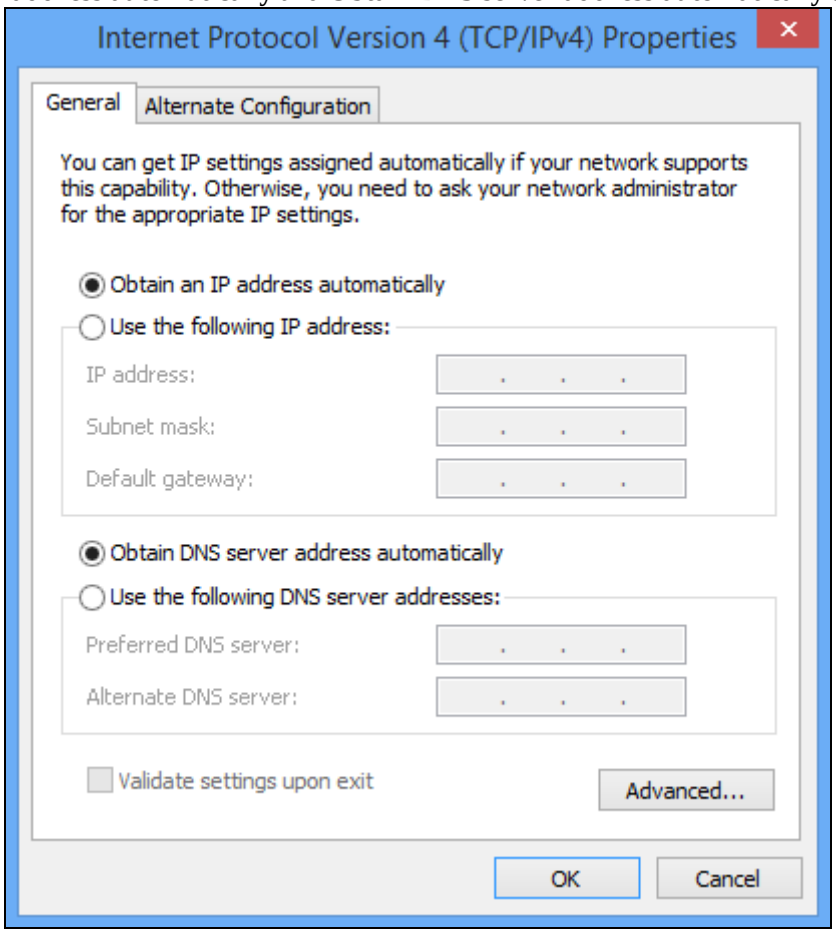
❸ Click **Ethernet -> Properties**.



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



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

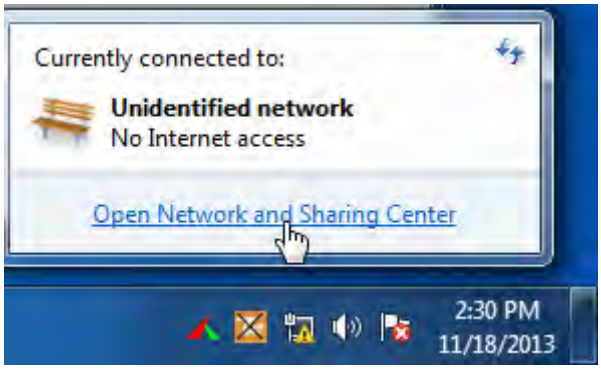


❻ Click **OK** on the **Ethernet Properties** window (see ❹ for the screenshot).

Windows 7

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

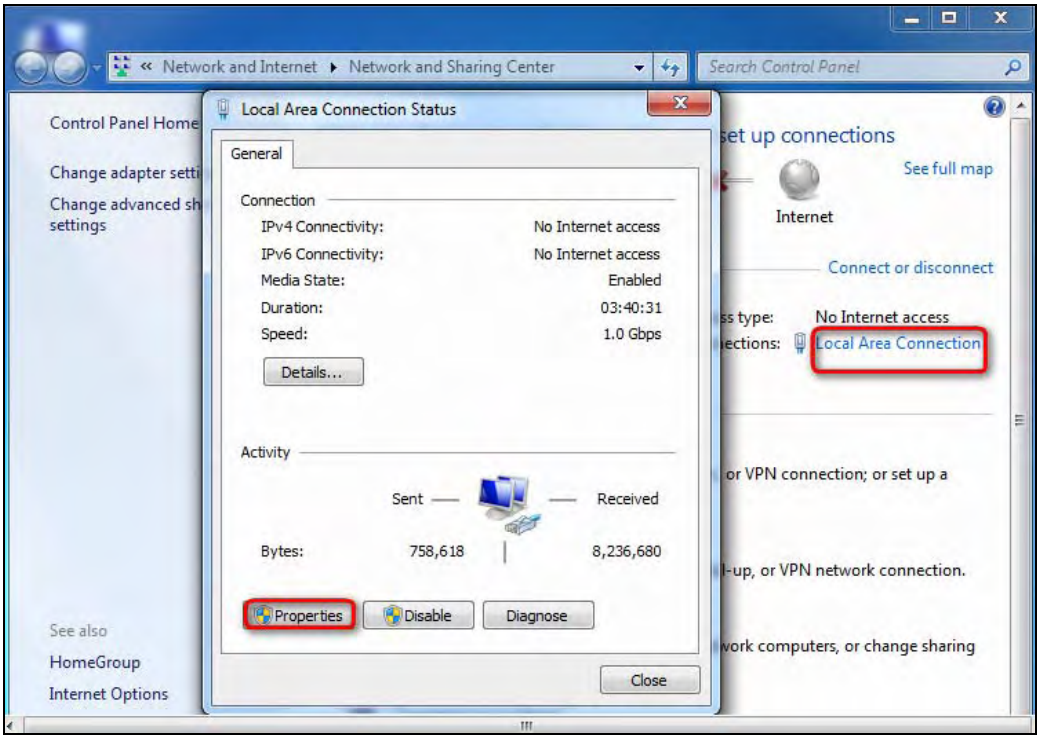
❷ Click **Open Network and Sharing Center**.



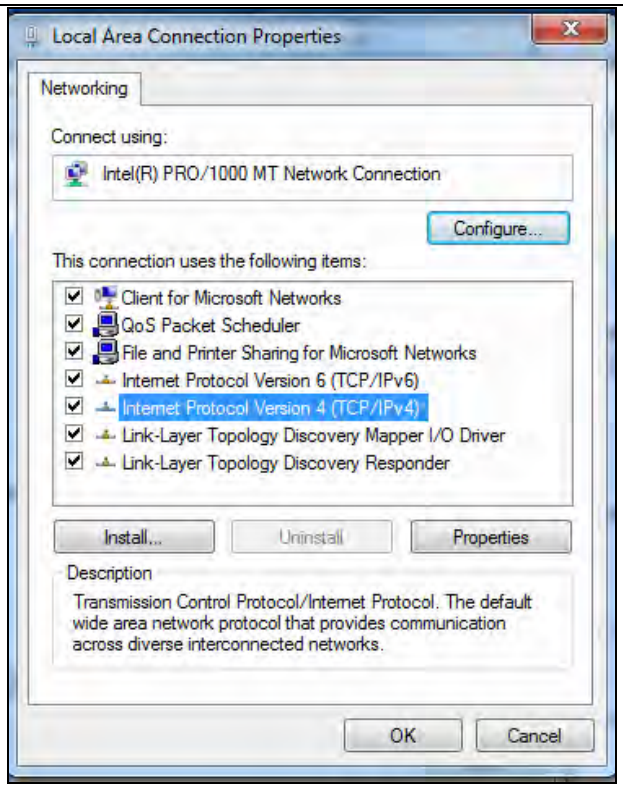
Tip

If you cannot find the icon  on the bottom right corner of your desktop, follow steps below: Click **Start -> Control Panel -> Network and Internet -> Network and Sharing Center**.

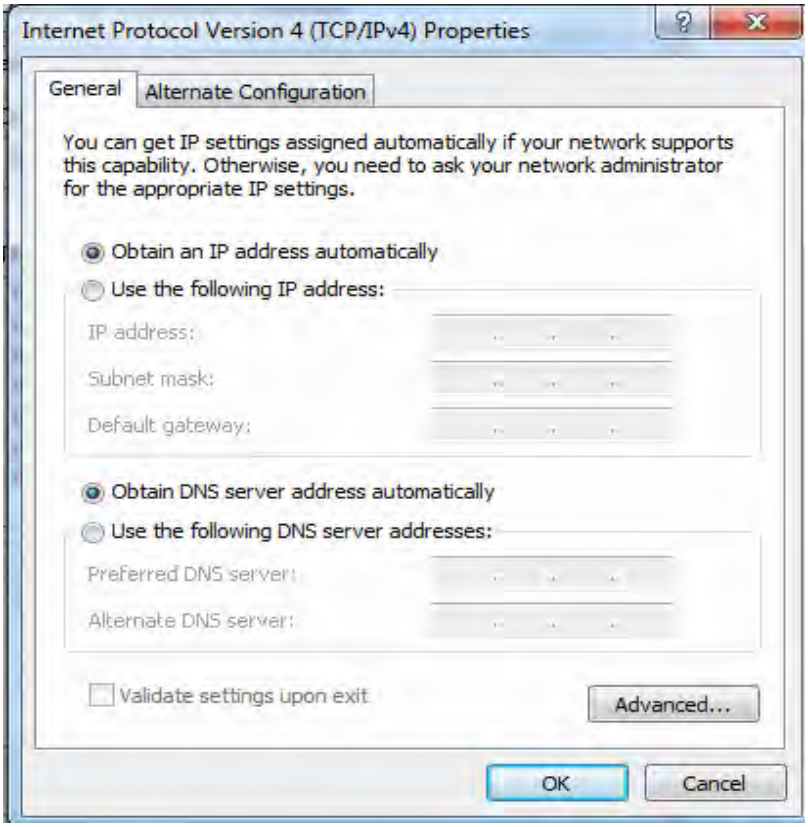
❸ Click **Local Area Connection -> Properties**.



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



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

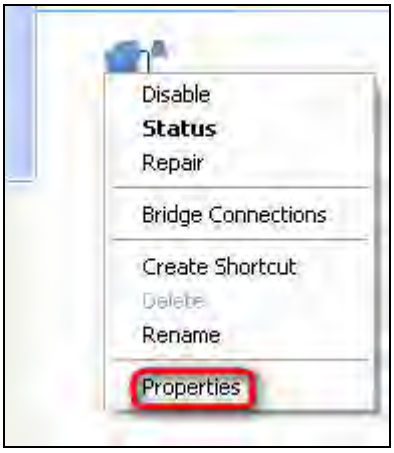


❻ Click **OK** on the **Local Area Connection Properties** window (see ❹ for the screenshot).

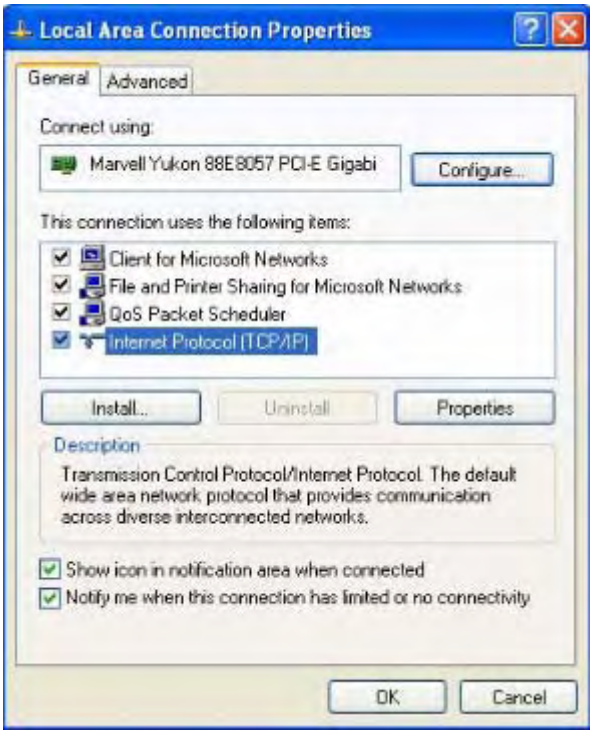
Windows XP

❶ Right click **My Network Places** on your desktop and select **Properties**.

❷ Right click **Local Area Connection** and select **Properties**.



❸ Scroll down to find and double click **Internet Protocol (TCP/IP)**.



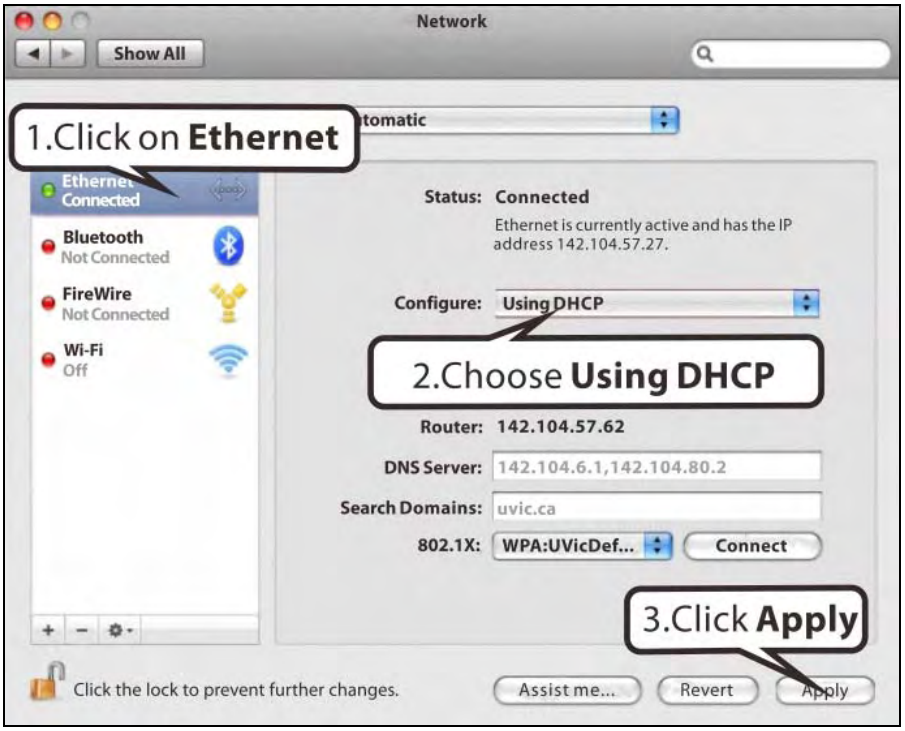
❹ Select **Obtain an IP address automatically** and **Obtain DNS server address automatically** and click **OK**.

❺ Click **OK** on the **Local Area Connection Properties** window (see ❸ for the screenshot).

MAC

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


Show All
Personal
Appearance
Desktop & Screen Saver
Dock
Expose & Spaces
Hardware
Bluetooth
CDs & DVDs
Displays
Energy Saver
Click Network
MobileMe
Network
QuickTime
Sharing
System
Accounts
Date & Time
Parental Controls
Software Update

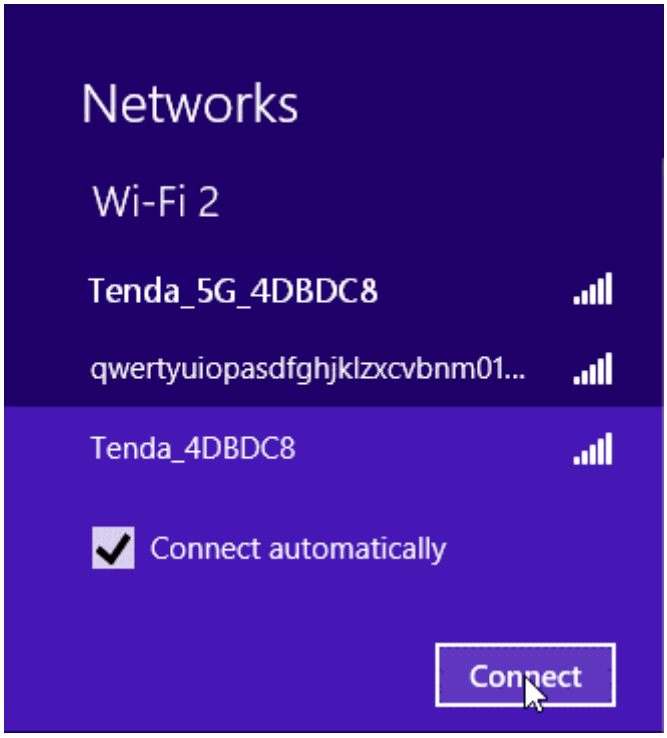

Network
Show All
1.Click on Ethernet
Connected
Bluetooth
Not Connected
FireWire
Not Connected
Wi-Fi
Off
Status: Connected
Ethernet is currently active and has the IP address 142.104.57.27.
Configure: Using DHCP
2.Choose Using DHCP
Router: 142.104.57.62
DNS Server: 142.104.6.1,142.104.80.2
Search Domains: uvic.ca
802.1X: WPA:UVicDef...
Connect
3.Click Apply
Click the lock to prevent further changes.
Assist me...
Revert
Apply

Appendix 2 WiFi Connection

Windows 8

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

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



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.

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

Windows 7

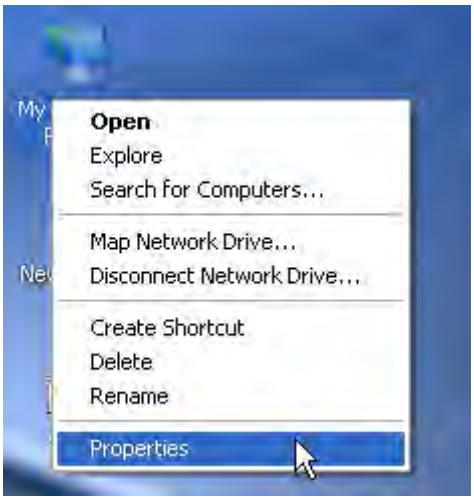
1. Click the icon on the bottom right corner of your desktop.

2. Double click your SSID (wireless network name) and then follow onscreen instructions.

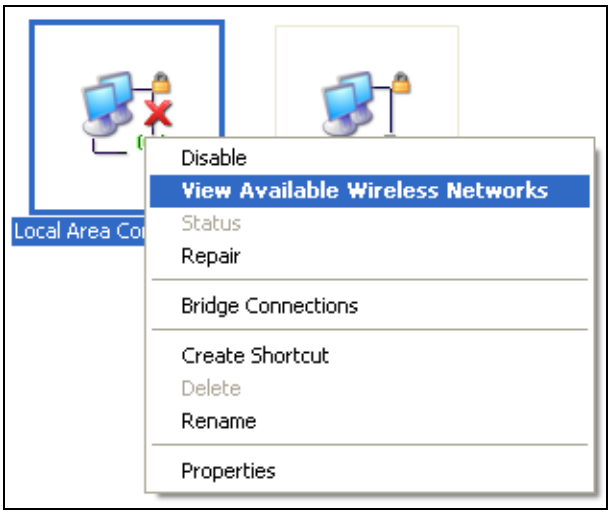
3. When your SSID (wireless network name) displays **Connected** as shown below, you've connected to it for Internet access successfully.

Windows XP

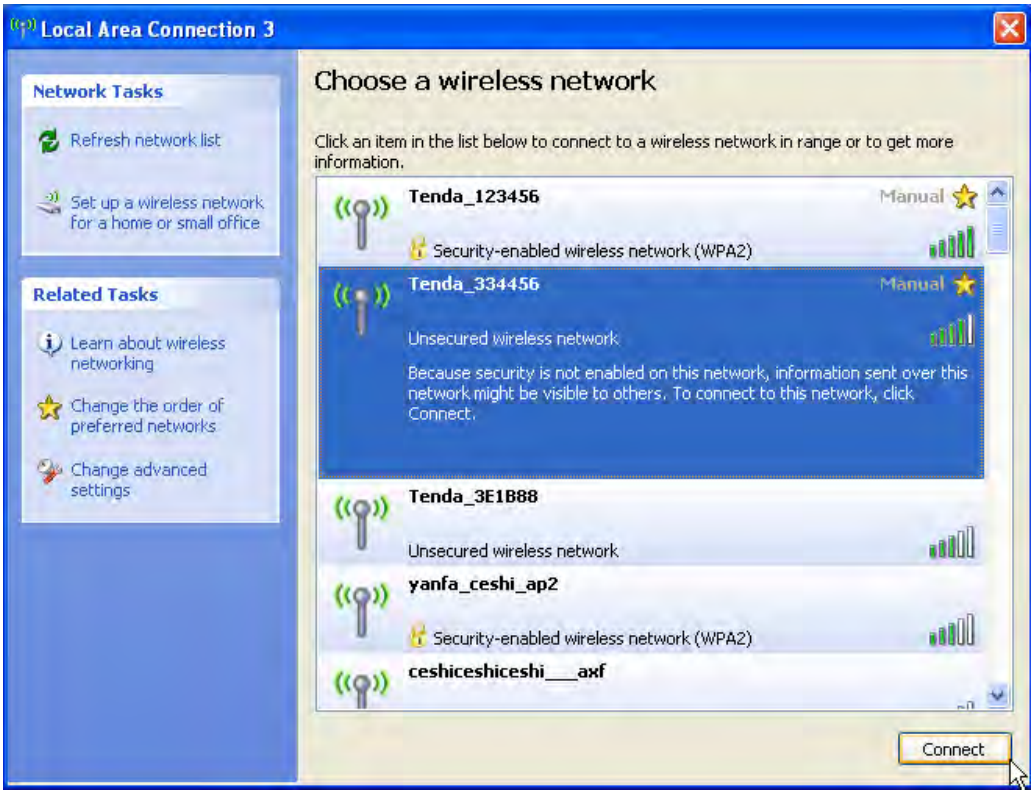
1. Right click **My Network Places**, and select **Properties**.



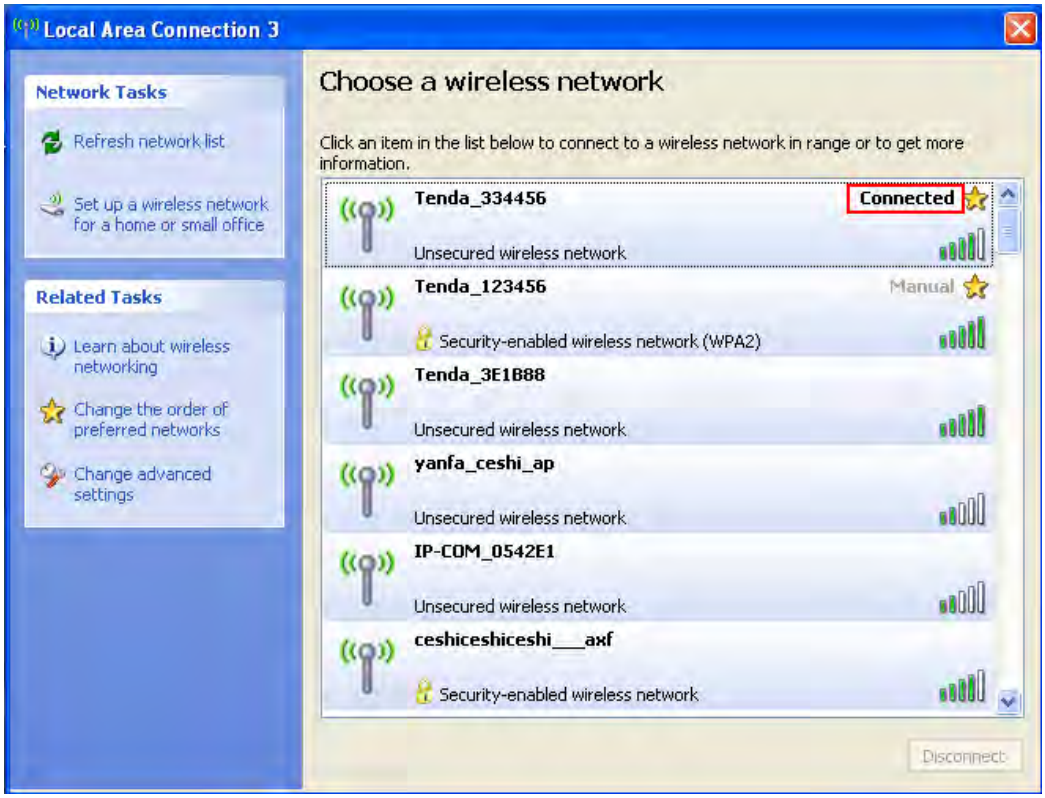
2. Right click **Local Area Connection**, and select **View Available Wireless Networks** from the pop-up submenu.



3. Select your wireless network from the list and then follow onscreen instructions.



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

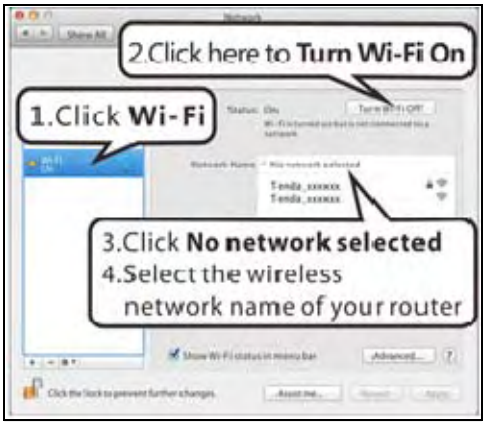


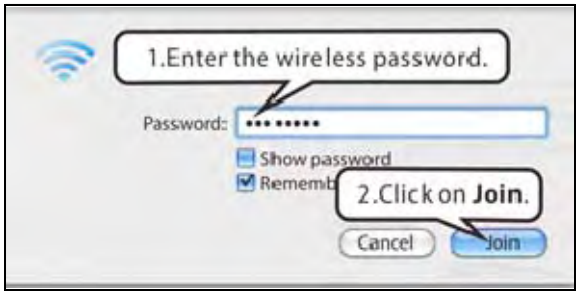
MAC

Click  > **System Preferences**.


Finder File Edit View
About This Mac
Software Update...
Mac OS X Software...
System Preferences...
Dock
Location
Recent Items
Force Quit Finder
Sleep
Restart...
Shut Down...
Log Out helpdesk...


Show All
Personal
Appearance
Desktop & Screen Saver
Dock
Expose & Spaces
Select Network from Internet & Network.
Internet & Network
MobileMe
Network
QuickTime
Sharing
System
Accounts
Date & Time
Parental Controls
Software Update


2.Click here to Turn Wi-Fi On
1.Click Wi-Fi
3.Click No network selected
4.Select the wireless network name of your router


1.Enter the wireless password.
Password:
Show password
2.Click on Join.
Cancel
Join

iPhone/iPad


1.Scroll screen to find the Settings icon.
2.Click the icon.
Settings


1.Click Wi-Fi.
2.Click here to open Wi-Fi
Airplane Mode OFF
Wi-Fi
Bluetooth Off
Do Not Disturb OFF
Notifications
General
Sounds
Brightness & Wallpaper
Picture Frame
Privacy
iCloud
Mail, Contacts, Calendars
Notes
Reminders
Wi-Fi ON
Choose a Network...
Tenda_xxxxxx
Tenda_xxxxxx
3.Find the name of the wireless network you wish to connect
4.Click on it.
Other...
Ask to Join Networks ON
Known networks will be joined automatically. If no known networks are available, you will be asked before joining a new network.


2.Click here to join the wireless network.
Enter the password for "dianshang"
Cancel
Enter Password
Join
Password
1.Enter a security key.


Settings
Airplane Mode OFF
Wi-Fi
Bluetooth Off
Do Not Disturb OFF
Notifications
General
Sounds
Brightness & Wallpaper
Picture Frame
Privacy
iCloud
Mail, Contacts, Calendars
Notes
Reminders
Wi-Fi
Wi-Fi ON
Choose a Network...
ChinaNet-YJ3M
Tenda_xxxxxx
dianshang
Connected successfully
Other...
Ask to Join Networks ON
Known networks will be joined automatically. If no known networks are available, you will be asked before joining a new network.

Appendix 3 FAQs

1. I cannot access the device's management interface. What should I do?

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

2) Double check the TCP/IP settings on your PC. For details, see Appendix 1 Configure Your PC hereof.

3) Press the **RST/WPS** button on the device and then re-access the management interface.

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.

2. I forget the wireless security key. What should I do? (How do I configure or change the security key?)

Try the default security key, which can be seen from the label attached to the device bottom.

- If the above works, access the device web manager and customize a new security key.
- If the above does not work, press the **RST/WPS** button on the device to restore factory default settings. And then log in to the device web manager to customize a new security key.

3. My notebook is unable to search wireless networks, what should I do?

1) Verify that wireless service is enabled on your notebook by checking the wireless hardware or software button on your notebook. The hardware button is usually located on the side of your notebook. Note that some notebooks may not have such hardware button. Software button can be implemented by pressing Fn+  . **Fn** is situated on the bottom left corner of your keyboard,  may be any key between **F1-F12** depending on what type of keyboard you are using.

2) Log in to the device, select **Wireless** > **2.4G/5G** > **Basic** and change the wireless network name (SSID). Then search again.

Follow below steps to verify that wireless service is enabled on your notebook (for Windows XP OS only).

From the desktop, right click on the **My Computer** icon and select **Manage**. Select **Services and Applications**, double click **Services** and view the status of **Wireless Zero Configuration**. If **Status** dose not display **Started**, right click the **Wireless Zero Configuration** and select **Start**; if **Startup Type** displays **Disabled**, right click the **Wireless Zero Configuration**, select **Properties**; from the **Startup Type** drop-down list box, select **Automatic** and then click **Star**t in **Service Status**.

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 **Wireless** > **2.4G/5G > Basic** and change the wireless network name (SSID). Then connect again.

3) Log in to the device, select **Wireless** > **2.4G/5G > Security** and change the security settings. Then connect again.

5. Where should I place the wireless device for optimum performance?

1) Know that multiple floors and walls will reduce the signal strength of Wi-Fi equipment, and that metal framing, ultraviolet-resistant window film and even metallic paint also reduce the signal strength.

2) Position the device in a central location within the area to be used for wireless communications.

3) Position the wireless router away from other radio equipment that operates at a frequency of 2.4GHz such as cordless phones, remote control receivers for R/C hobbyist, wireless cameras, and microwave ovens, cordless telephones and microwave ovens which are also considered to be electromagnetic devices.

Appendix 4 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

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

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
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
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
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
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
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

Appendix 5 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. This device complies with EU 1999/5/EC.

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 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.

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 in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

— Reorient or relocate the receiving antenna.
— Increase the separation between the equipment and receiver.
— Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
— Consult the dealer or an experienced radio/TV technician for help.

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 transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment.

Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

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.

***Note:** The country code selection is for non-US model only and is not available to all US model. Per FCC regulation, all WiFi product marketed in US must fixed to US operation channels only.