# 300Mbps Wireless N VDSL2 Modem Router

# User Guide

## Copyright Statement



## Disclaimer

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

# Preface

Thank you for choosing Tenda! Please read this user guide before you start with V300.

# Conventions

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

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

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

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

# Acronyms and Abbreviations

| Acronym or Abbreviation | Full Spelling |
| --- | --- |
| ADSL | Asymmetric Digital Subscriber Loop |
| ARP | Address Resolution Protocol |
| ATM | Asynchronous Transfer Mode |
| DDNS | Dynamic Domain Name System |
| DHCP | Dynamic Host Configuration Protocol |
| DSL | Digital Subscriber Loop |
| DLNA | Digital Living Network Alliance |
| DMZ | Demilitarized Zone |
| DNS | Domain Name System |

| Acronym or Abbreviation | Full Spelling |
|---|---|
| IEEE | Institute of Electrical and Electronics Engineers |
| IP | Internet Protocol |
| IPTV | Internet Protocol Television |
| ISP | Internet Service Provider |
| LAN | Local Area Network |
| L2TP | Layer 2 Tunneling Protocol |
| MPPE | Microsoft Point-to-Point Encryption |
| PPP | Point To Point Protocol |
| PPPoE | Point-to-Point Protocol over Ethernet |
| PPTP | Point to Point Tunneling Protocol |
| RIP | Routing Information Protocol |
| SIP | Session Initiation Protocol |
| SSID | Service Set Identifier |
| STB | Set Top Box |
| URL | Uniform Resource Locator |
| VDSL2 | Very-high-bit-rate Digital Subscriber Loop |
| VLAN | Virtual Local Area Network |
| VoIP | Voice over Internet Protocol |
| VPN | Virtual Private Network |
| WPS | WiFi Protected Setup |

## Additional Information

For more information, search this product model on our website at http://www.tendacn.com.

## Technical Support

If you need more help, contact us by any of the following means. We will be glad to assist you as soon as possible.

| | | | |
|---|---|---|---|
|  | Global: (86) 755-27657180<br>Canada: 1-888-998-8966 |  | support@tenda.cn |

| | | | |
|---|---|---|---|
| Hotline | Hong Kong: 00852-81931998 | Email | |
| Website | http://www.tendacn.com | Skype | tendasz |

# Contents

# 1 Get to Know the Device

## 1.1 Overview

V300 can serve as a VDSL2 modem with high downstream speed of 100 Mbps, a 300 Mbps wireless router, or a 4-port switch which can meet various demands. With 2 external high gain omni-directional antennas, V300 can provide wide wireless coverage. It can support multiple internet connection types, including phone cables, Ethernet cables as well as 3G/4G dongle backup. User-friendly web UI allows you to configure the modem router easily.

## 1.2 Features

- All-in-one device combines a VDSL2 modem, wired router, wireless router and switch
- Ethernet and VDSL uplinks: Access the internet via DSL port or WAN port (RJ45 port)
- Multiple internet connection types: Bridging, PPPoE, IPoE, PPPoA, and IPoA
- Tenda Quick Setup Wizard for easy installation and configuration
- Up to 300 Mbps wireless transmission speed for excellent HD video streaming and online gaming
- Compatible with 802.11b/g/n Wireless devices
- One-key WPS ensures quick and secure wireless network connection
- USB port lets you access and share files through an attached USB storage device
- Port 1 can function either as a LAN or a WAN port
- Port 4 can function either as a LAN or an IPTV port
- QoS feature helps prioritize media streaming and gaming applications for best entertainment experience
- Parental Control controls internet access of children using flexible and customizable filter settings
- 6 kV lightning—proof design fits into lightning-intensive environment
- Advanced Features: IPv6, DDNS, virtual server, DMZ, port triggering, IP filter, MAC filter, UPnP, and so on.

# 1.3 Packing List

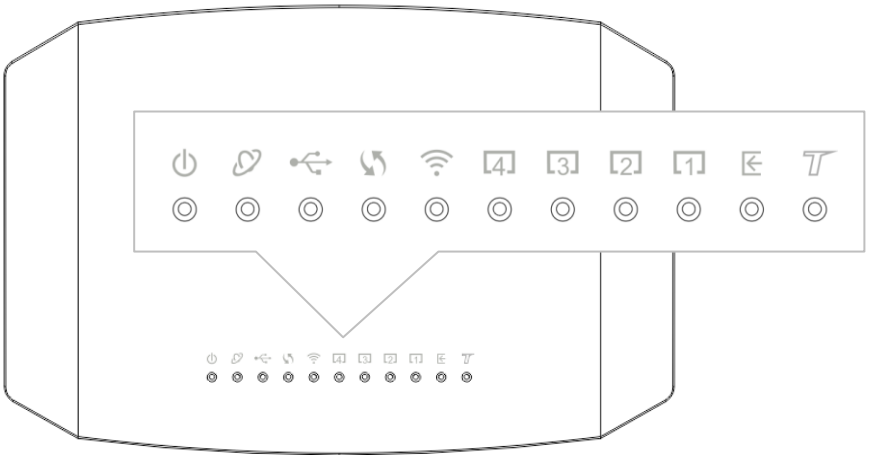
The package should contain the following items:

- Wireless Modem Router * 1
- Phone cable * 2
- Ethernet cable * 1
- Splitter * 1
- Installation Guide * 1
- Power adapter * 1

If any item is incorrect, missing or damaged, please keep the original package and contact the vendor.

# 1.4 Appearance

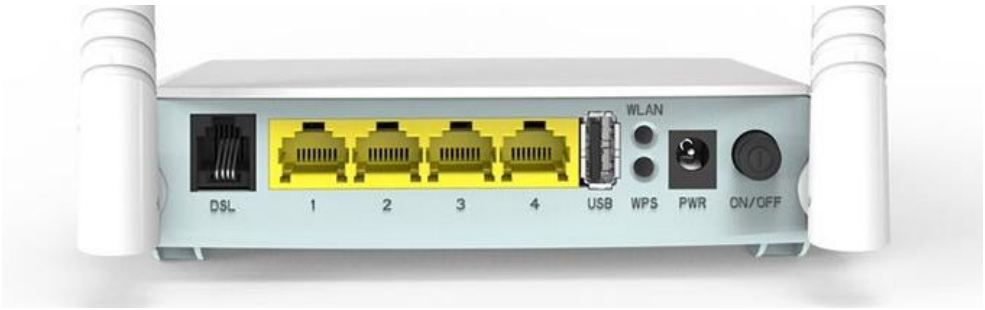
## 1.4.1 Front Panel



| LED Indicator | Color | Status | Description |
|---|---|---|---|
| PWR | Red | Solid on | The device is starting. |
| | | Blinking | The device is upgrading. |
| | Green | Solid on | The device is working properly. |
| INTERNET | Red | Solid on | No internet access. |
| | Green | Solid on | The device is connected to the internet successfully. |
| | | Blinking | Data is being transmitted. |

| | | | |
|---|---|---|---|
| USB | Green | Solid on | A USB device is properly connected and ready. |
| | | Blinking | Data is being transmitted. |
| | | Off | No USB device is detected, or the USB device is ejected. |
| WPS | Green | Solid on for 2 mins->Off | A WPS connection is established. |
| | | Blinking | The device is performing WPS negotiation. |
| | | Off | The WPS feature is disabled, or the WPS feature is enabled but the device does not perform WPS negotiation. |
| WLAN | Green | Solid on | The wireless feature is enabled. |
| | | Blinking | Data is being transmitted wirelessly. |
| | | Off | The wireless feature is disabled. |
| 1-4 | Green | Solid on | This port is properly connected. |
| | | Blinking | This port is transmitting data. |
| | | Off | No connection is detected on this port. |
| DSL | Green | Solid on | DSL negotiation is completed. |
| | | Blinking | The device is doing DSL negotiation. |
| | | Off | No connection is detected on the DSL port. |
| | | | This LED is reserved. |

## 1.4.2 Rear panel

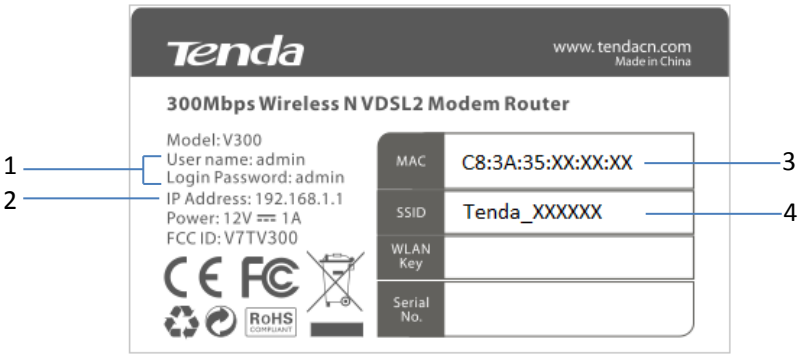



| Button/Port | Description |
|---|---|
| ON/OFF | This button is used to turn on/off the modem router. |
| PWR | The power jack is used to connect to the included power adapter for power supply. |
| WLAN | This button is used to enable or disable the wireless feature. |
| WPS | Enable the WPS function on the web UI of the modem router. Press this button for 3 seconds and then release it to perform the WPS negotiation process. Within 2 minutes after pressing the button, enable the wireless device's WPS feature to establish WPS connection. |
| 1 | This port serves as a LAN port by default. But if your link type is Ethernet, it serves as a WAN port. |
| 2/3 | LAN Ports. Used to connect to computers, switches, and so on. |
| 4 | If you enable IPTV feature of the modem router, this port serves as an IPTV port. Otherwise, it is a LAN port. |
| DSL | RJ11 port. Used to connect the modem router to the internet via a phone cable. |
| RST<br>*On the bottom panel of the modem router | Press this button for about 6 seconds and then release it to restore factory settings. |

NOTE

Please use the included power adapter for power supply to prevent device damage.

## 1.4.3 Product Label




1: Default login user name and password: When you log in to the web UI of the modem router, this information is required.

2: Default login IP address of the modem router.

3: MAC address of the modem router

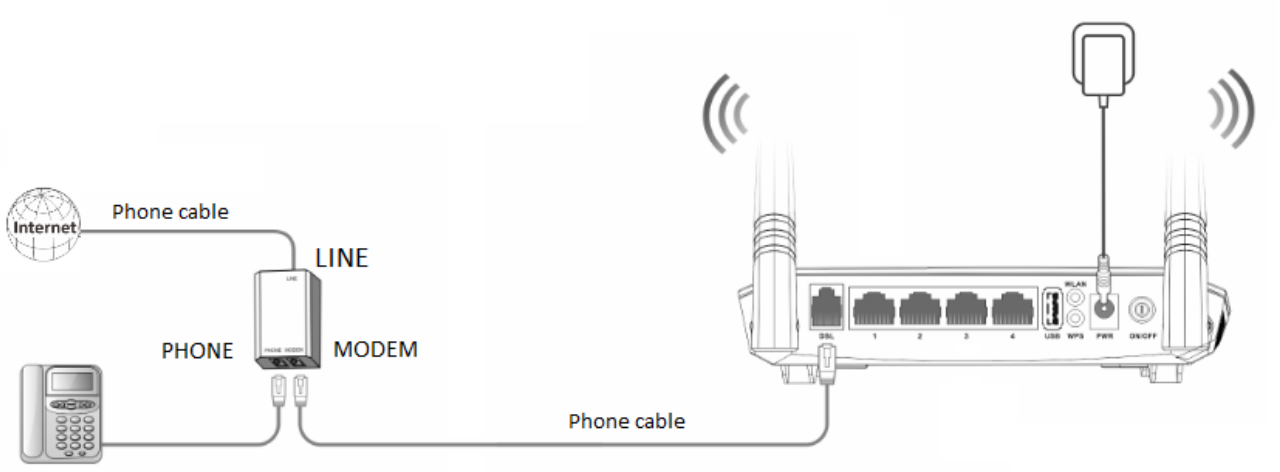
4: Default wireless network name of the modem router

# 2 Quick Setup

## 2.1 Connecting the Device to the Internet

### 2.1.1 Phone Cable Connection

If you want to use phone service and internet service concurrently, connect the modem router as follows:




**Step 1** Connect the LINE port of the included splitter to the cable connected to your ISP.

**Step 2** Connect the PHONE port of the splitter to your telephone.

**Step 3** Connect the MODEM port of the splitter to the **DSL** port of the modem router.

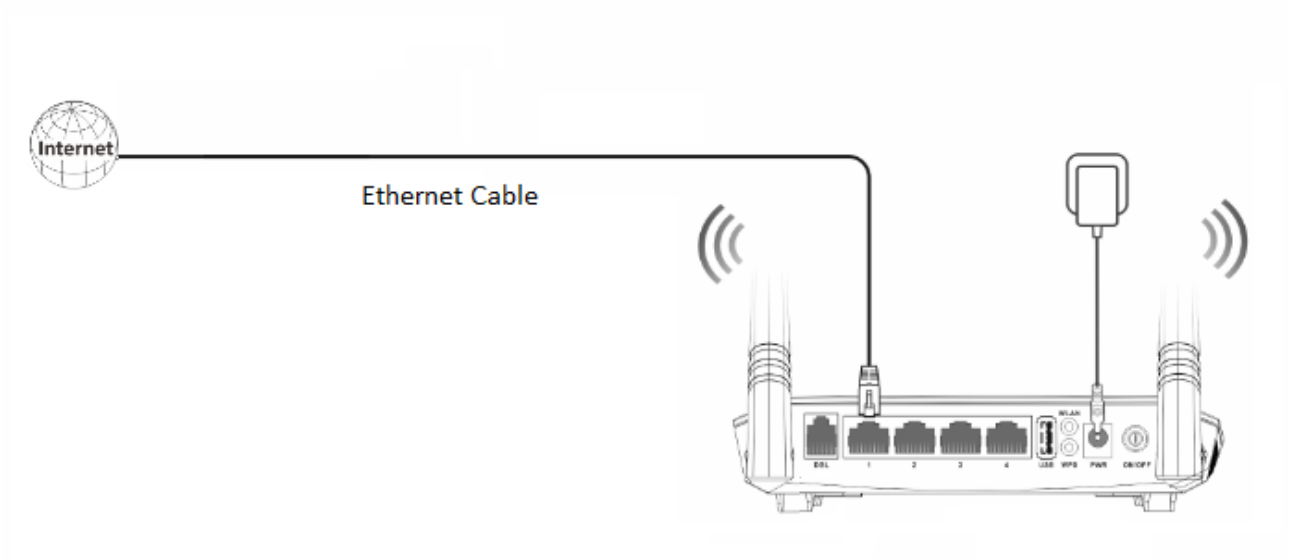
**Step 4** Power on the modem router.

**--End**

If you do not need to use the phone service, directly connect the phone cable to the **DSL** port of the modem router.

### 2.1.2 Ethernet Cable Connection

When the modem router only functions as a wireless router, connect the modem router as follows:




Connect the port 1 of the modem router to the internet.

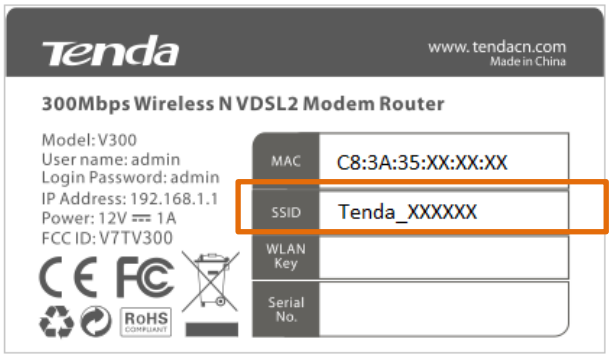
### 2.1.3 3G/4G Dongle

Insert a 3G/4G dongle provided by your ISP into USB port of the modem router for internet access.

## 2.2 Connecting the Device to a Client

### 2.2.1 Wireless Connection

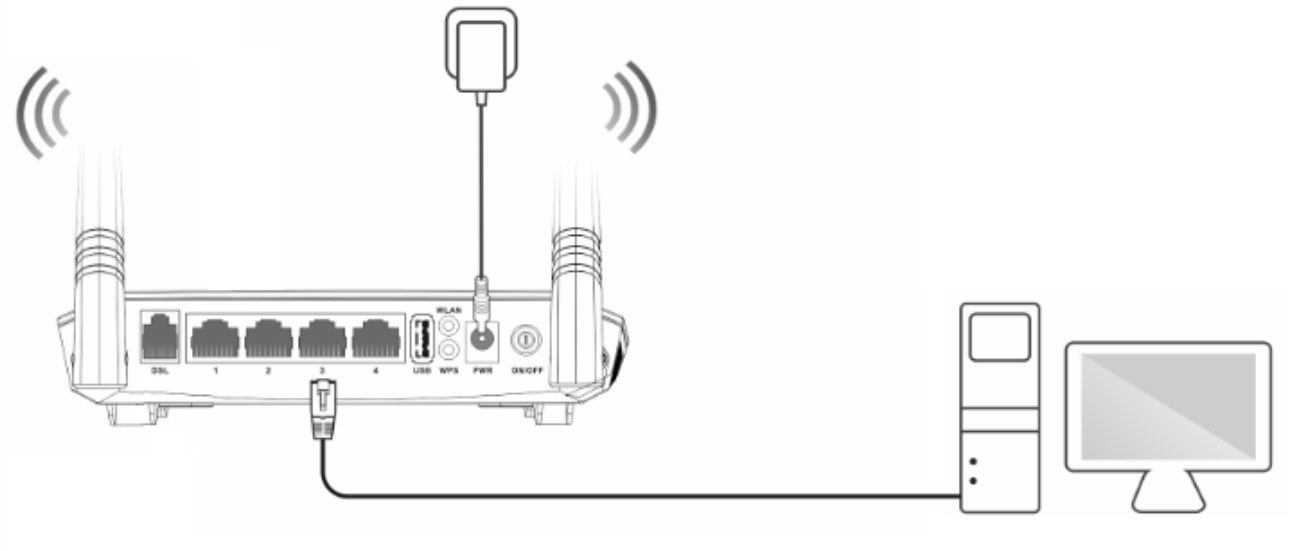
This label is on the bottom of the modem router.




Use your smart device to search and connect to the default SSID (WiFi name) of the modem router. There is no WLAN Key (WiFi password) by default.

If either the SSID or WLAN key is changed, the wireless device is required to connect to the modem router again.

## 2.2.2 Wired Connection



Connect your computer to an available LAN port (port 1, 2, 3, or 4) of the modem router.

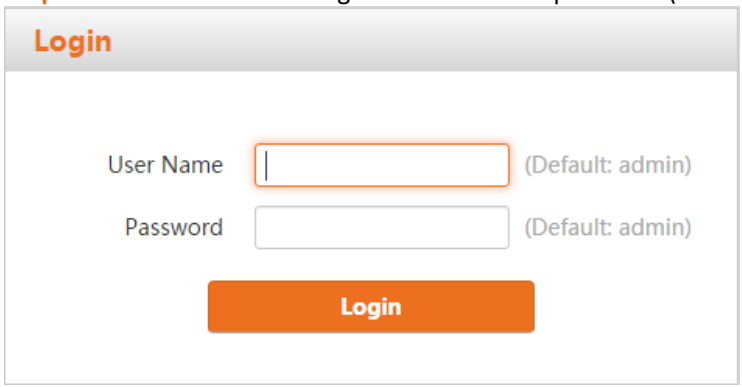
# 2.3 Login

**Step 1** Start a web browser on the computer connected to the modem router, enter **192.168.1.1** in the address bar and press **Enter** on the keyboard.

TIP

You'd better configure the modem router on a computer that connected to the modem router via an Ethernet cable.


**Step 2** Enter the default login user name and password (both are **admin**), and click **Login**.

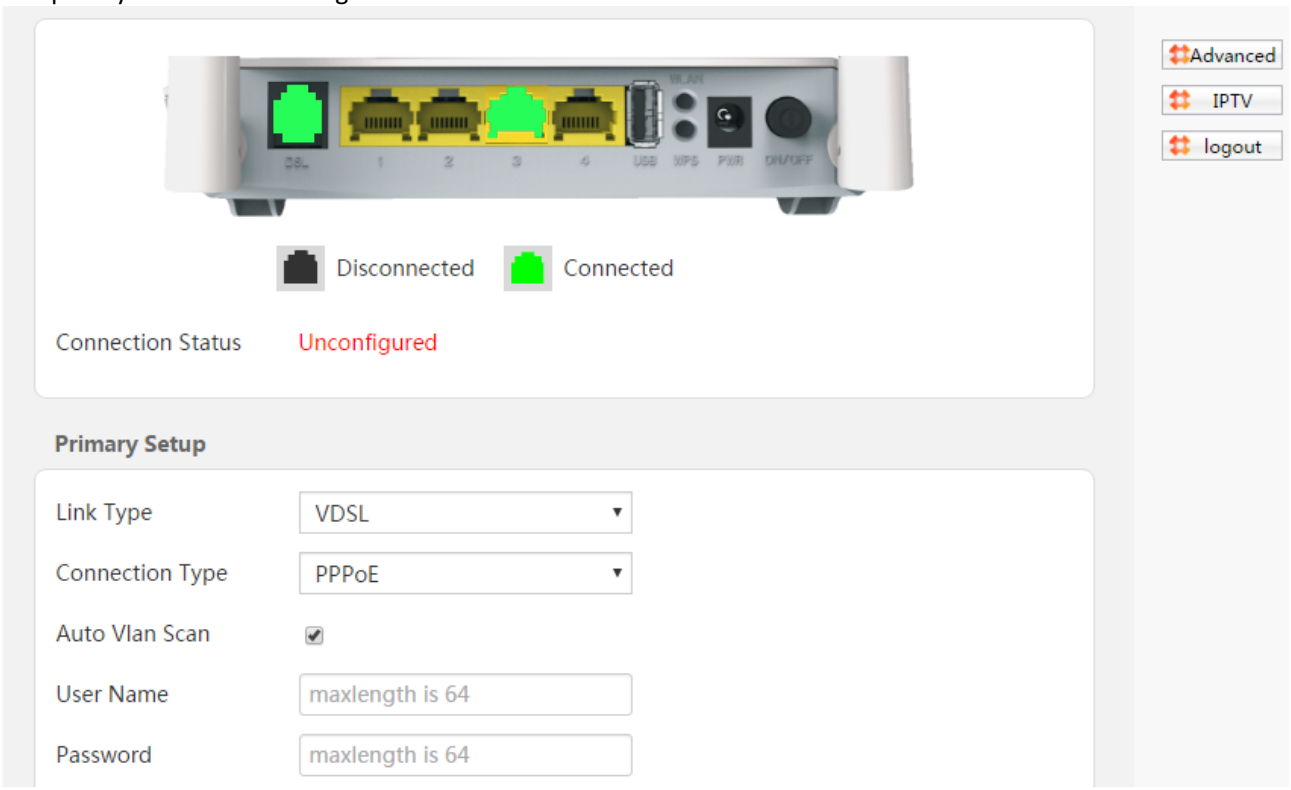



**--End**

# 2.4 Setting Up an Internet Connection

## 2.4.1 Phone Cable Connection

If you connect the modem router to the internet via a phone cable, refer to the configuration in this part to complete your internet settings.




### VDSL

If the link type your internet service provider (ISP) provided to you is **VDSL**, follow the procedure below:

**Step 1** Log in to the web UI and enter the **Home** page.

**Step 2** Link Type: Select VDSL.

**Step 3** **Connection Type**: Select a connection type according to the instructions in the table below, and set the related internet parameters.

| Connection Type | | Description |
|---|---|---|
| PPPoE | | Select this type if your ISP provides a user name and password to you for internet access. |
| IPoE | Dynamic IP | Select this type if your ISP does not provide any parameters to you for internet access. |
| | Static IP | Select this type if your ISP provides a static IP address and other related information to you for internet access. |
| Bridge | | Select this type when this device only serves as a modem, and you want to set up a dial-up connection or enter other internet parameters directly on your computer for internet access. |

**Step 4** Click **OK** on the bottom of the page to apply the settings.

**--End**

## ADSL

If the link type your ISP provided to you is **ADSL**, follow the procedures below:

**Step 1** Log in to the web UI and enter the **Home** page.

**Step 2** Link Type: Select ADSL.

**Step 3** **Connection Type**: Select a connection type according to the instructions in the table below, and complete the related internet parameters.

| Connection Type | | Description |
|---|---|---|
| PPPoE | | If your ISP provides a user name and password to you for internet access, your connection type may be PPPoE or PPPoA. Contact your ISP for details. |
| PPPoA | | |
| IPoE (IP over Ethernet) | Dynamic IP | Select this type if your ISP does not provide any parameters to you for internet access. |
| | Static IP | If your ISP provides a static IP address and other related information to you for internet access, your connection type may be IPoE or IPoA, contact your ISP for details. |
| IPoA (IP over ATM) | Static IP | |
| Bridge | | Select this type when this device only serves as a modem, and you want to set up a dial-up connection or enter other internet parameters directly on your computer for internet access. |

**Step 4** **Country/Region**: Select your country or region.

**Step 5** **ISP**: Select your ISP.

**Step 6** Enter the related internet parameters provided by your ISP.

**Step 7** Click **OK** on the bottom of the page to apply the settings.

**--End**

TIP

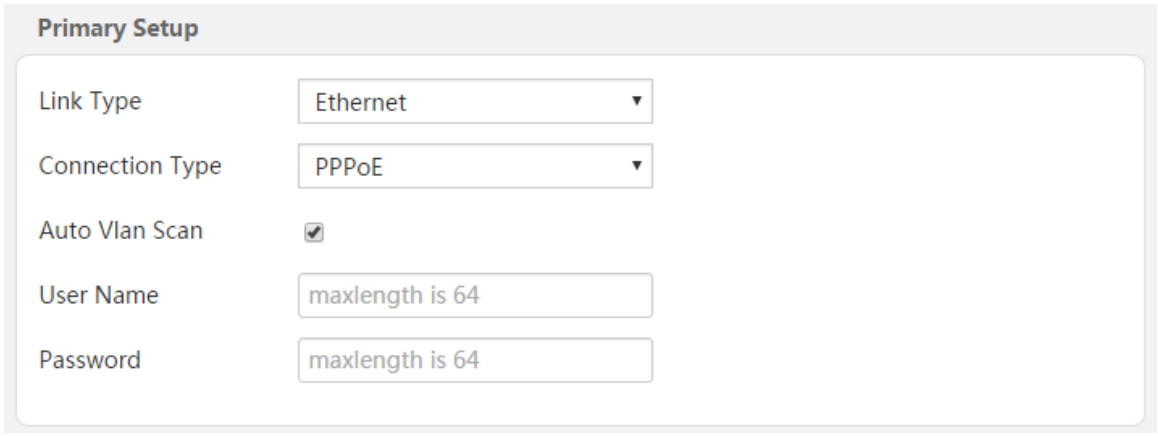
If your country/region and ISP are not available in the drop-down list, select **Other**, and enter the VPI and VCI manually. If you do not know the VPI and VCI, contact your ISP for help.

# 2.4.2 Ethernet Cable Connection

If you connect the modem router to the internet via an Ethernet cable, refer to the configuration in this part to complete your internet settings. In this case, this device only serves as a wireless router.


## PPPoE

Use this type if you can access the internet only after setting up a dial-up connection on the computer using a user name and password provided by your ISP.




**Step 1** Log in to the web UI and enter the **Home** page.

**Step 2** Link Type: Select Ethernet.

**Step 3** Connection Type: Select PPPoE.

**Step 4** Enter the user name and password.

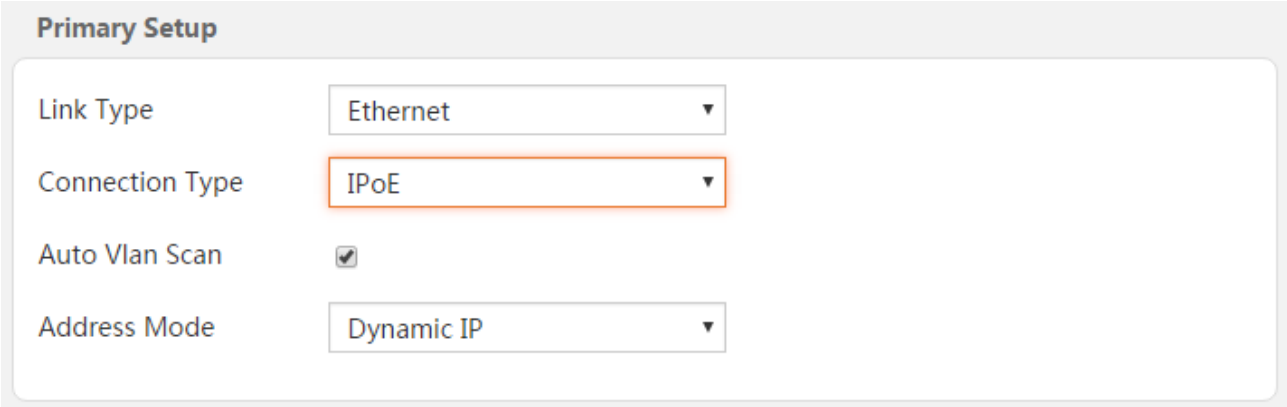
**Step 5** Click **OK** on the bottom of the page to apply the settings.

**--End**

## IPoE

### Dynamic IP

Use this type if you can access the internet without setting any information on your computer.




**Step 1** Log in to the web UI and enter the **Home** page.

**Step 2** Link Type: Select Ethernet.

**Step 3** Connection Type: Select IPoE.

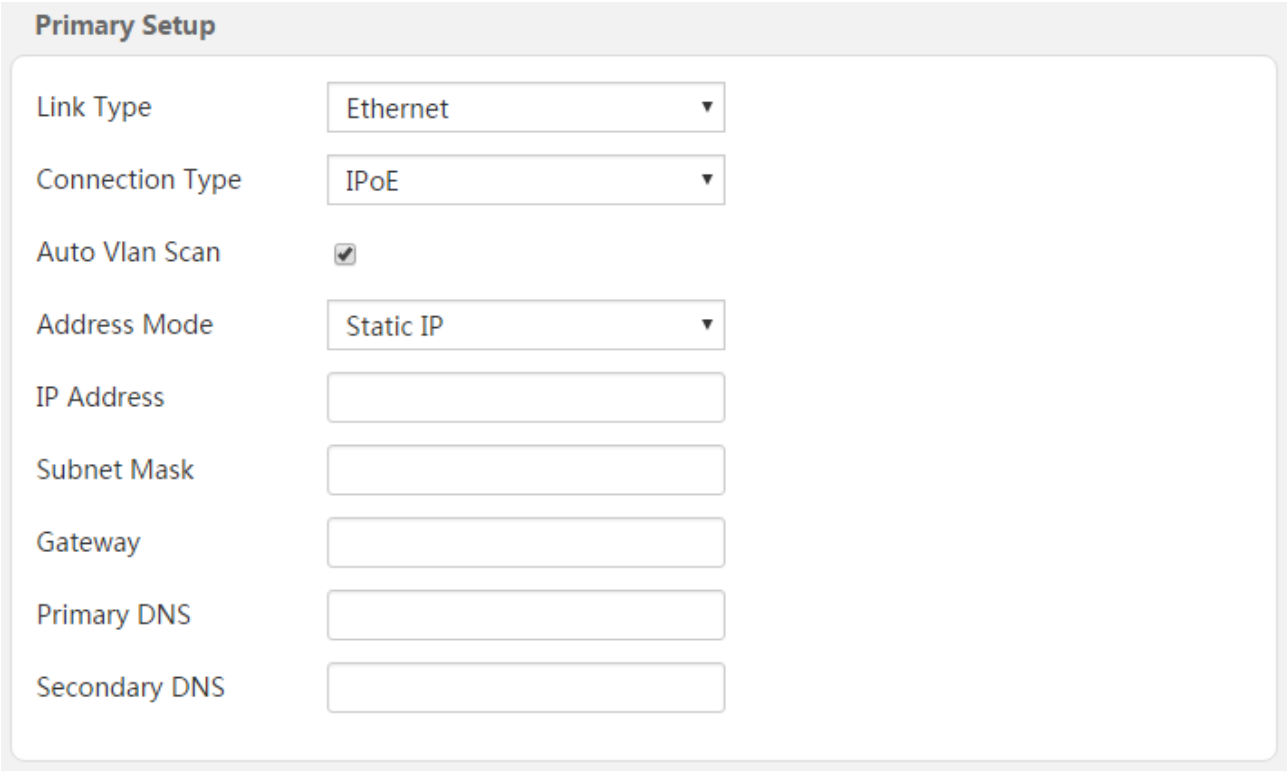
**Step 4** Address Mode: Select Dynamic IP.

**Step 5** Click **OK** on the bottom of the page to apply the settings.

**--End**

### Static IP

Use this type if you can access the internet only after setting a static IP address and other related information on your computer.




**Step 1** Log in to the web UI and enter the **Home** page.

**Step 2** Link Type: Select Ethernet.

**Step 3** Connection Type: Select IPoE.

**Step 4** Address Mode: Select Static IP.

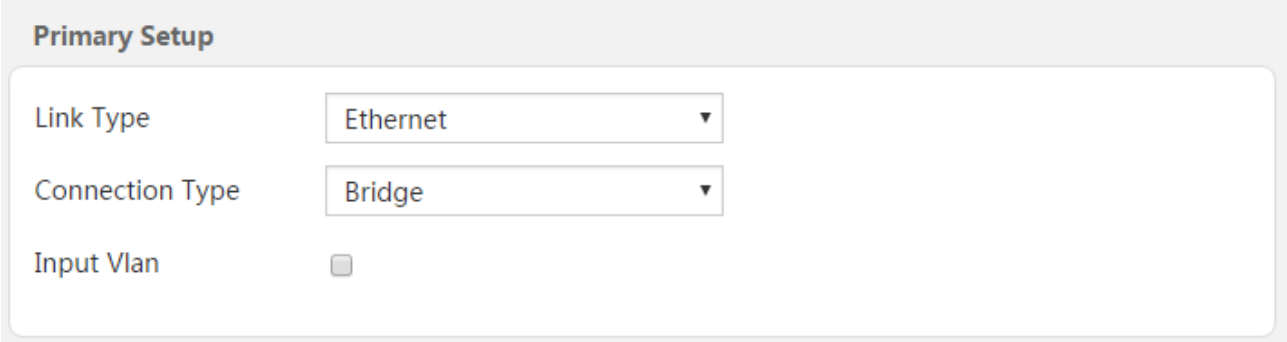
**Step 5** Enter the static IP address, and other related parameters.

**Step 6** Click **OK** on the bottom of the page to apply the settings.

**--End**

### Bridge

Select this type when this device only serves as a switch, and you want to set up a dial-up connection or enter other internet parameters directly on your computer for internet access.




**Step 1** Log in to the web UI and enter the **Home** page.

**Step 2** Link Type: Select Ethernet.

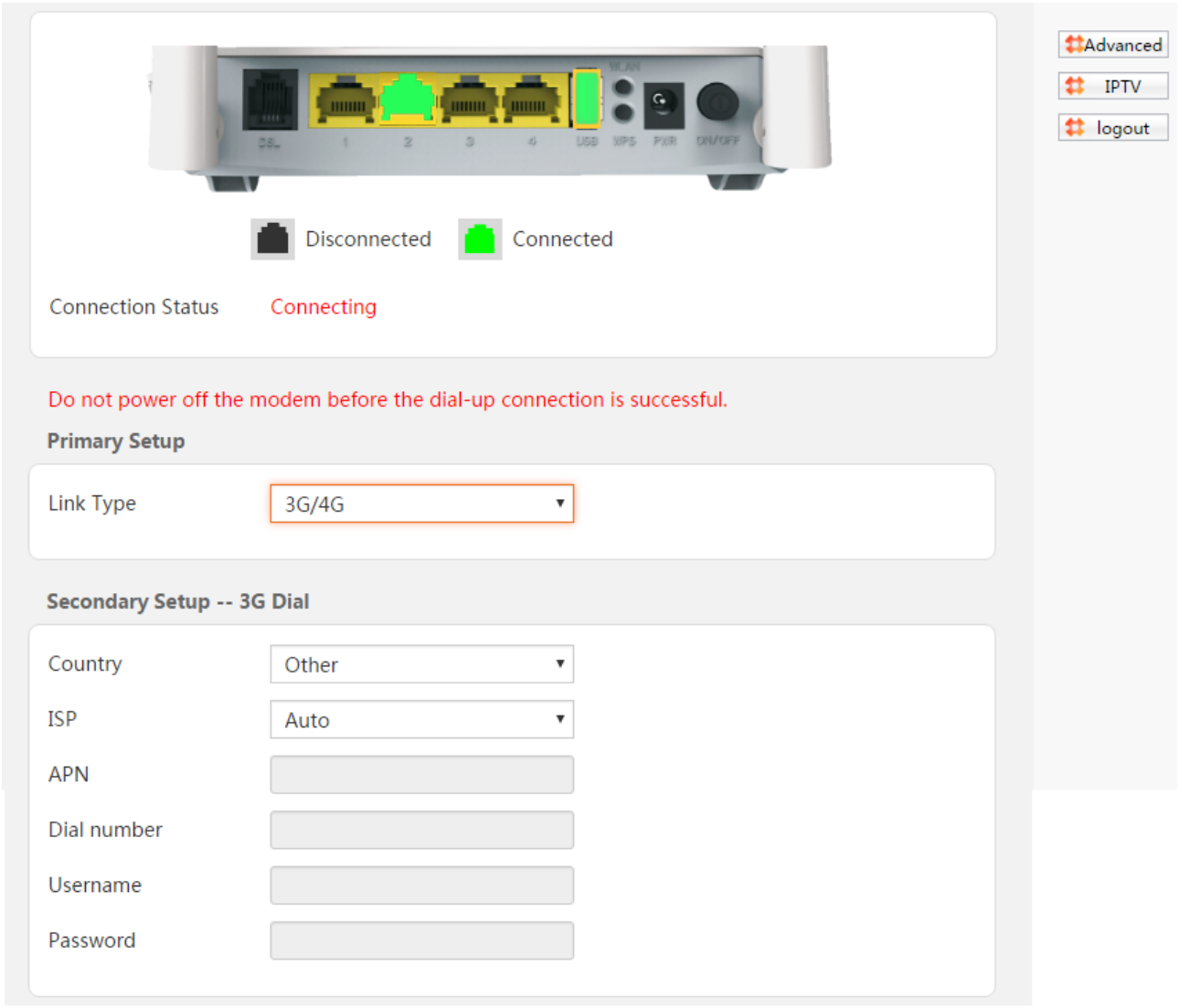
**Step 3** Connection Type: Select Bridge.

**Step 4** Click **OK** on the bottom of the page to apply the settings.

**--End**

## 2.4.3 3G/4G Dongle

If you connect the modem router to the internet via a 3G/4G dongle, refer to the configuration in this part to complete your internet settings.




**Step 1** Log in to the web UI and enter the **Home** page.

**Step 2** Link Type: Select 3G/4G.

**Step 3** **Country**: Select your country.

**Step 4** **ISP**: Select your ISP.

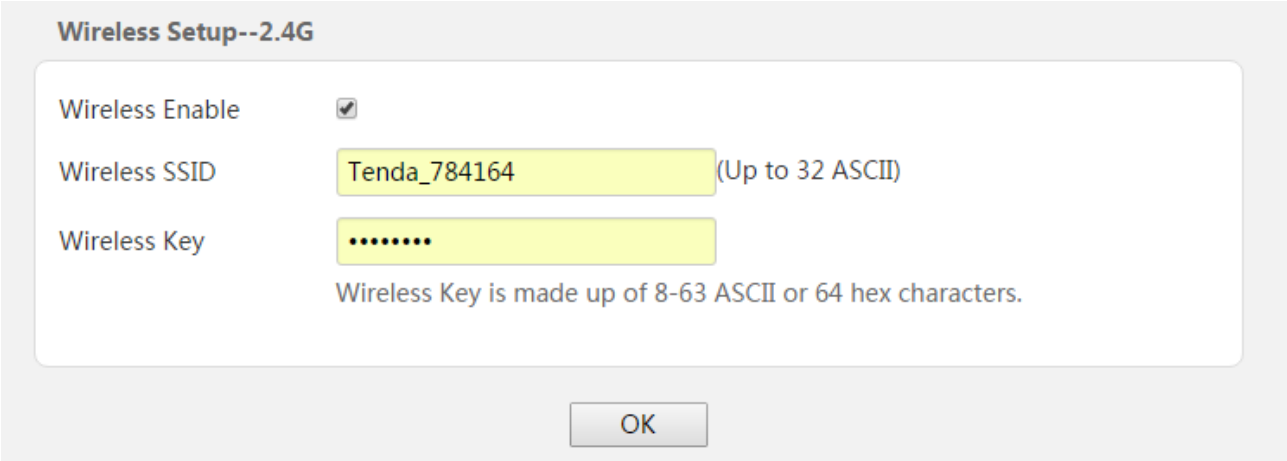
**Step 5** **(Optional) APN/Dial number/Username/Password**: Generally, if you select a correct country and ISP, the necessary parameters can be automatically filled in. If not, enter them manually according to the internet parameters your ISP provided.

**Step 6** Click **OK** on the bottom of the page to apply the settings.

**--End**

# 2.5 Wireless Setup

The wireless feature is enabled by default. The default SSID of the modem router is Tenda_*XXXXXX*, where XXXXXX is the last six characters of the MAC address of the modem router. There is no Wireless Key (WiFi password) by default. But there is a preset WiFi password 12345678 in the **Wireless Key** box. It takes effects when the **OK** button on the bottom of the page is clicked.




**To customize a WiFi name and password:**

**Step 1** Log in to the web UI and enter the **Home** page.

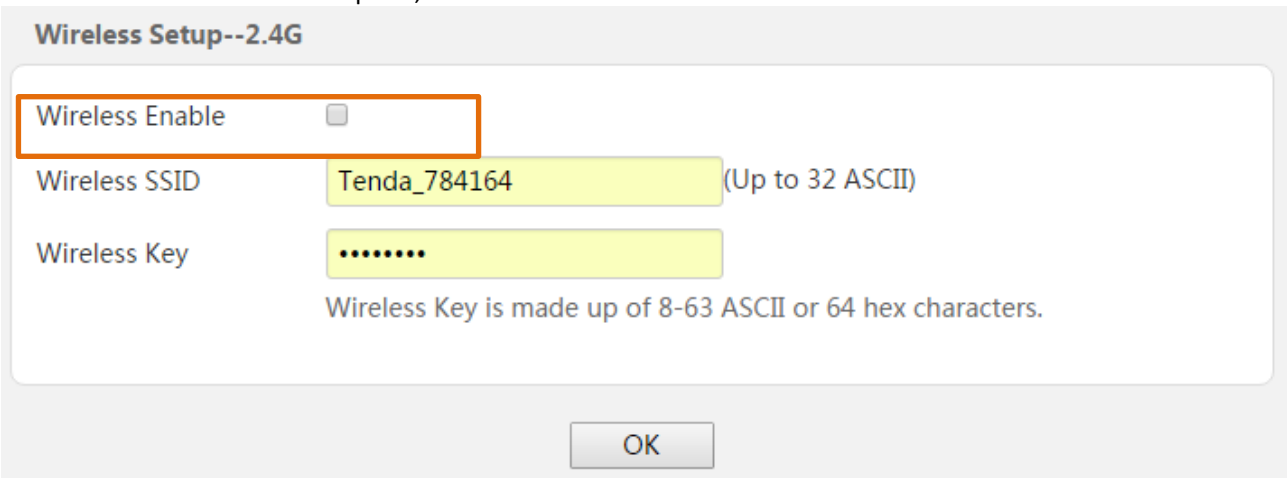
**Step 2** Enter a new WiFi name in the **Wireless SSID** box.

**Step 3** Enter a new WiFi password in the **Wireless Key** box.

**Step 4** Click **OK** to apply the settings.

**--End**

To disable wireless feature:
Deselect the **Wireless Enable** option, and click **OK**.

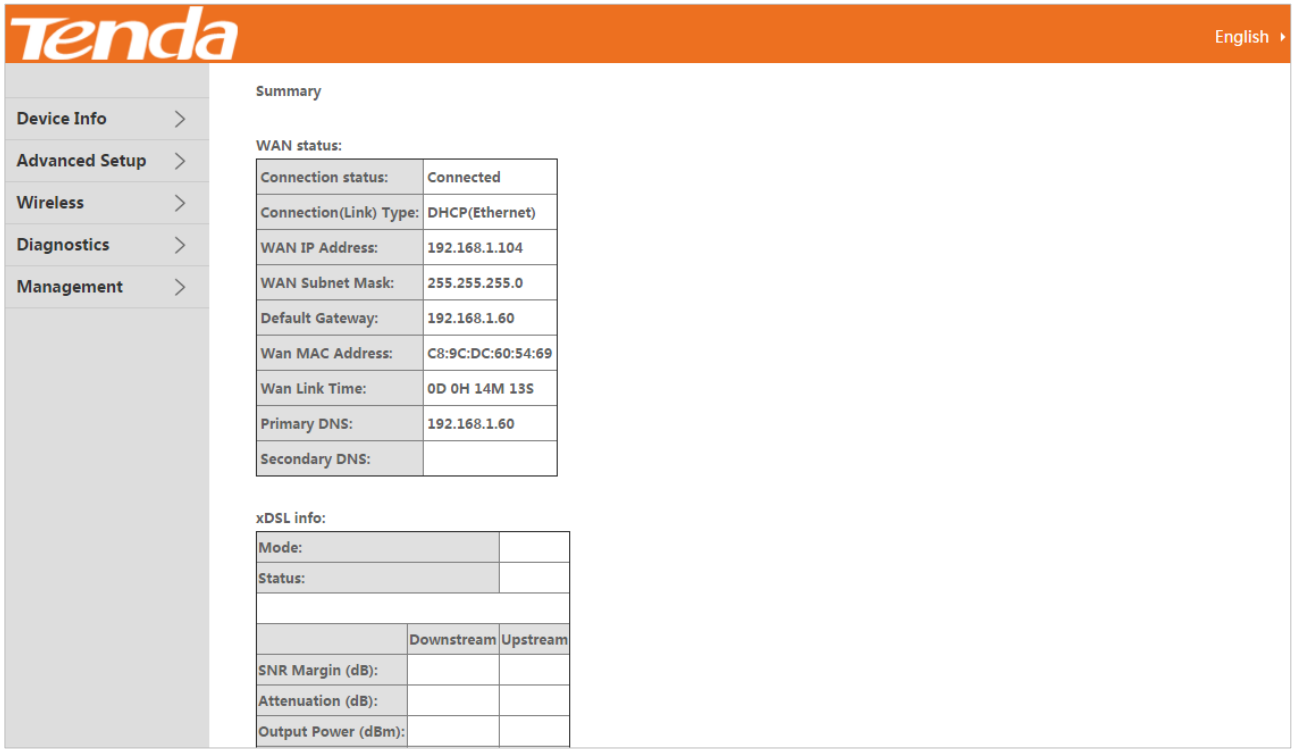



When the wireless feature is disabled, wireless device cannot connect to the modem router wirelessly.

# 3 Device Info

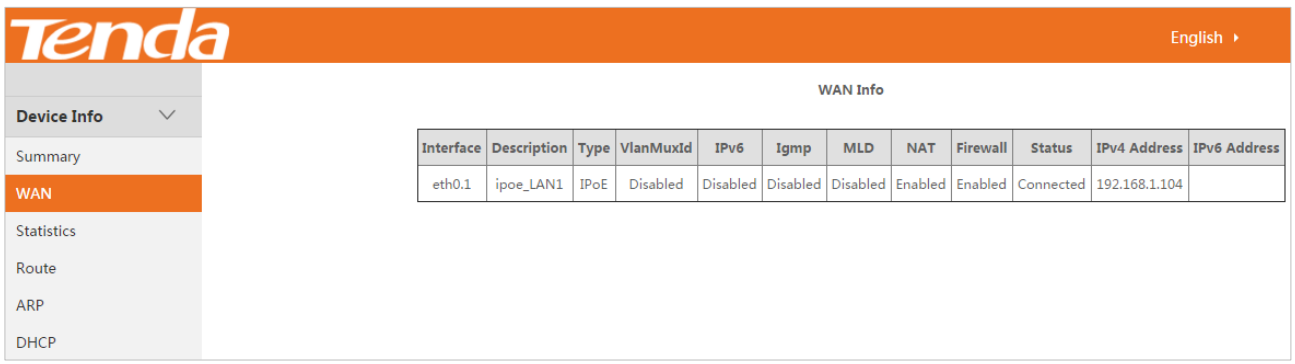
## 3.1 Summary

Here you can view WAN status, xDSL information, and the device information



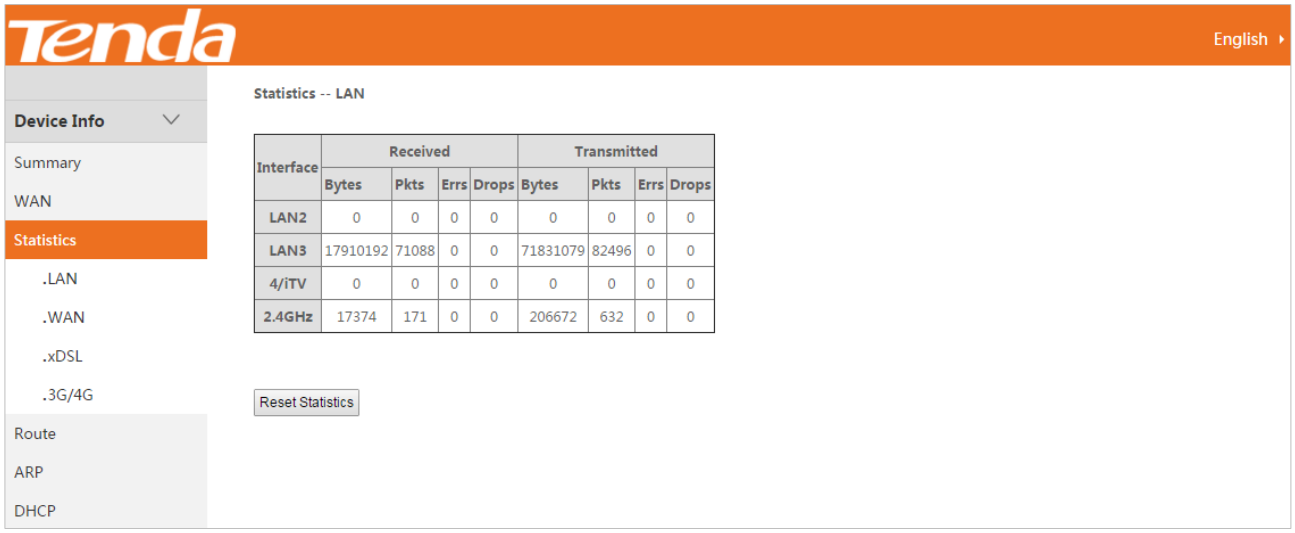

## 3.2 WAN

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

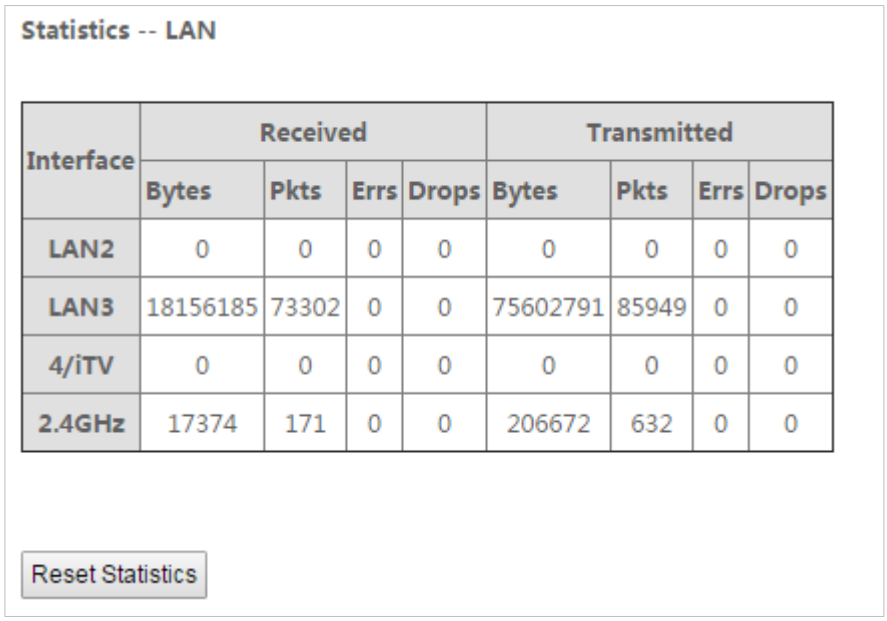


# 3.3 Statistics

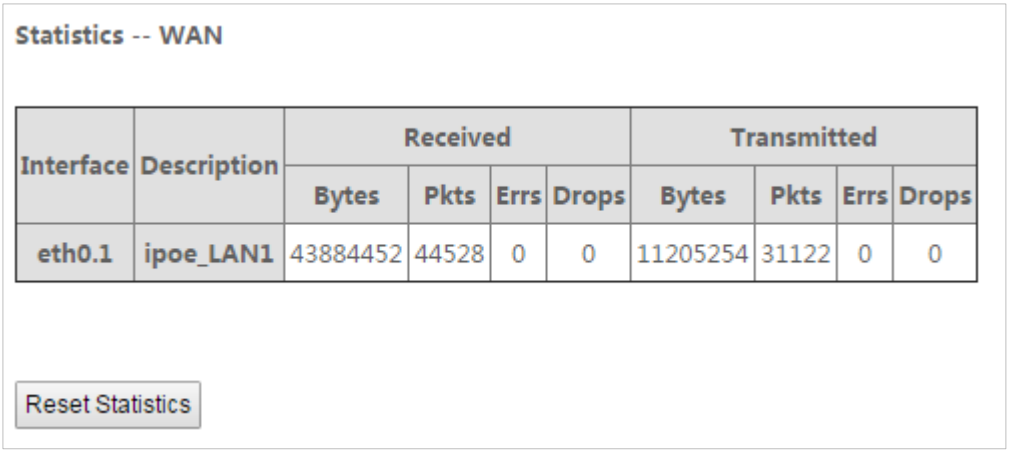
Here you can view the packets received and transmitted on LAN port, WAN port, DSL port, and USB port.




**Statistics--LAN**: Displays the packets received and transmitted on the LAN ports. Click **Reset Statistics** to clear the current statistics.




**Statistics--WAN**: Displays the packets received and transmitted on the WAN port. Click **Reset Statistics** to clear the current statistics.



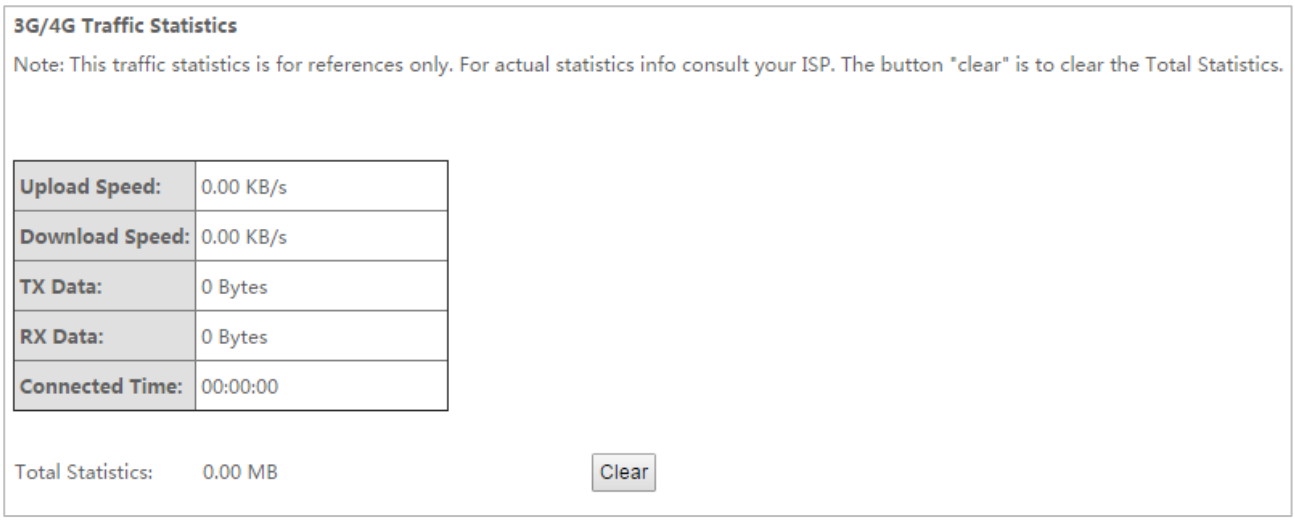

**Statistics--xDSL**: Displays the packets received and transmitted on the DSL port. Click **Reset Statistics** to clear the current statistics.

**Statistics -- xDSL**

| | | |
|---|---|---|
| **Mode:** | | |
| **Traffic Type:** | | |
| **Status:** | | Disabled |
| **Link Power State:** | | L3 |
| | | |
| | **Downstream** | **Upstream** |
| **Line Coding(Trellis):** | | |
| **SNR Margin (dB):** | | |
| **Attenuation (dB):** | | |
| **Output Power (dBm):** | | |
| **Attainable Rate (Kbps):** | | |
| **Rate (Kbps):** | | |
| | | |
| **Super Frames:** | | |
| **Super Frame Errors:** | | |
| **RS Words:** | | |
| **RS Correctable Errors:** | | |
| **RS Uncorrectable Errors:** | | |
| | | |
| **HEC Errors:** | | |
| **OCD Errors:** | | |
| **LCD Errors:** | | |
| **Total Cells:** | | |
| **Data Cells:** | | |
| **Bit Errors:** | | |
| | | |
| **Total ES:** | | |
| **Total SES:** | | |
| **Total UAS:** | | |

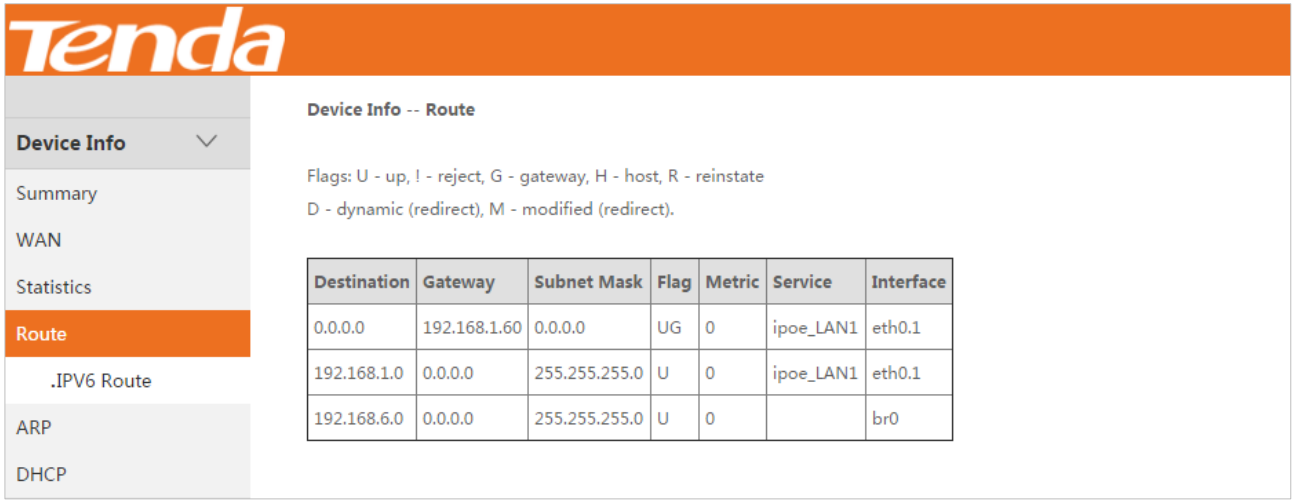
Reset Statistics

**Statistics—3G/4G**: Displays the packets received and transmitted on the USB port. Click **Clear** to clear the current statistics.



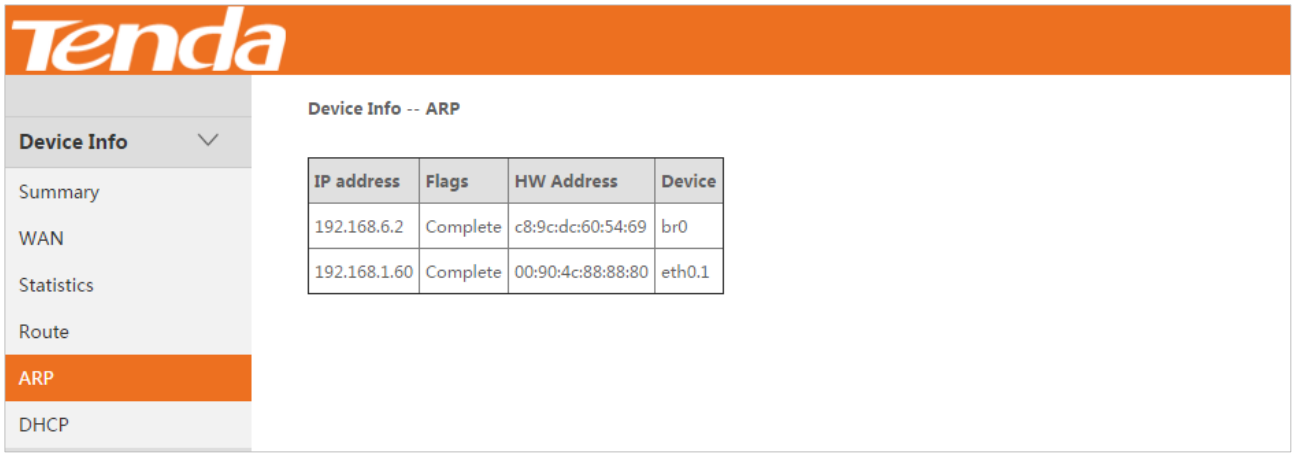

## 3.4 Route

Here you can view the route table。



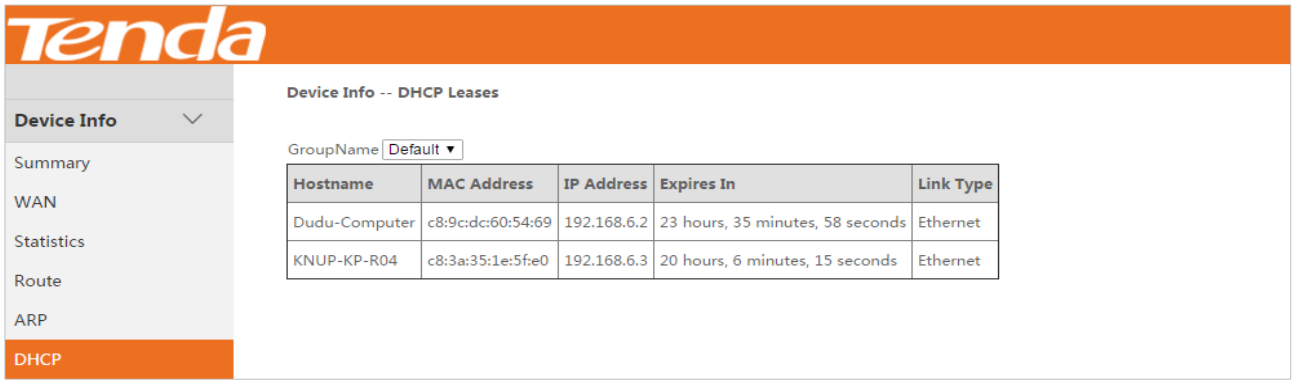

## 3.5 ARP

Here you can view the IP and MAC addresses of the devices connected to the modem router either in wired manner or in wireless manner.




## 3.6 DHCP

Here you can view the DHCP leases, including IP and MAC addresses of the devices, hostnames and remaining lease time.



# 4 Advanced Setup

## 4.1 Layer2 Interface

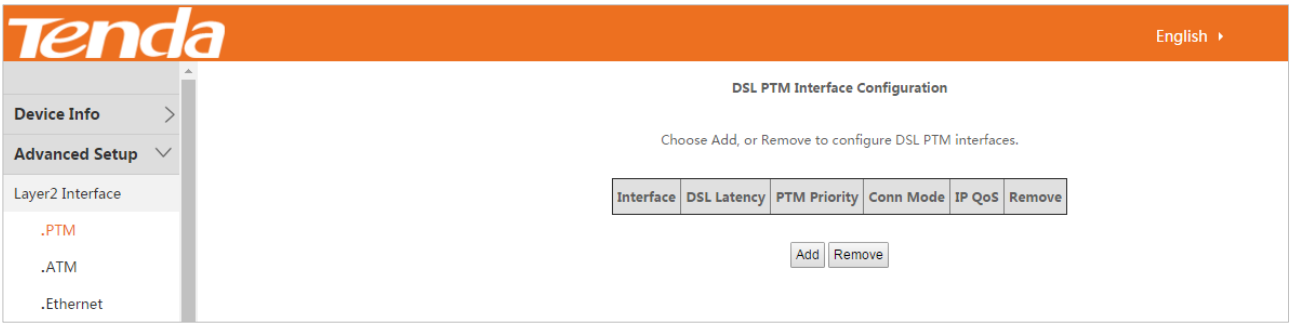
Choose **Advanced** > **Advanced Setup** > **Layer2 Interface** to enter the Layer2 Interface page.

This router provides three Layer2 Interfaces:

- PTM interface for accessing VDSL broadband internet service
- ATM interface for accessing ADSL broadband internet service
- ETH interface for connecting to the Internet via an Ethernet cable

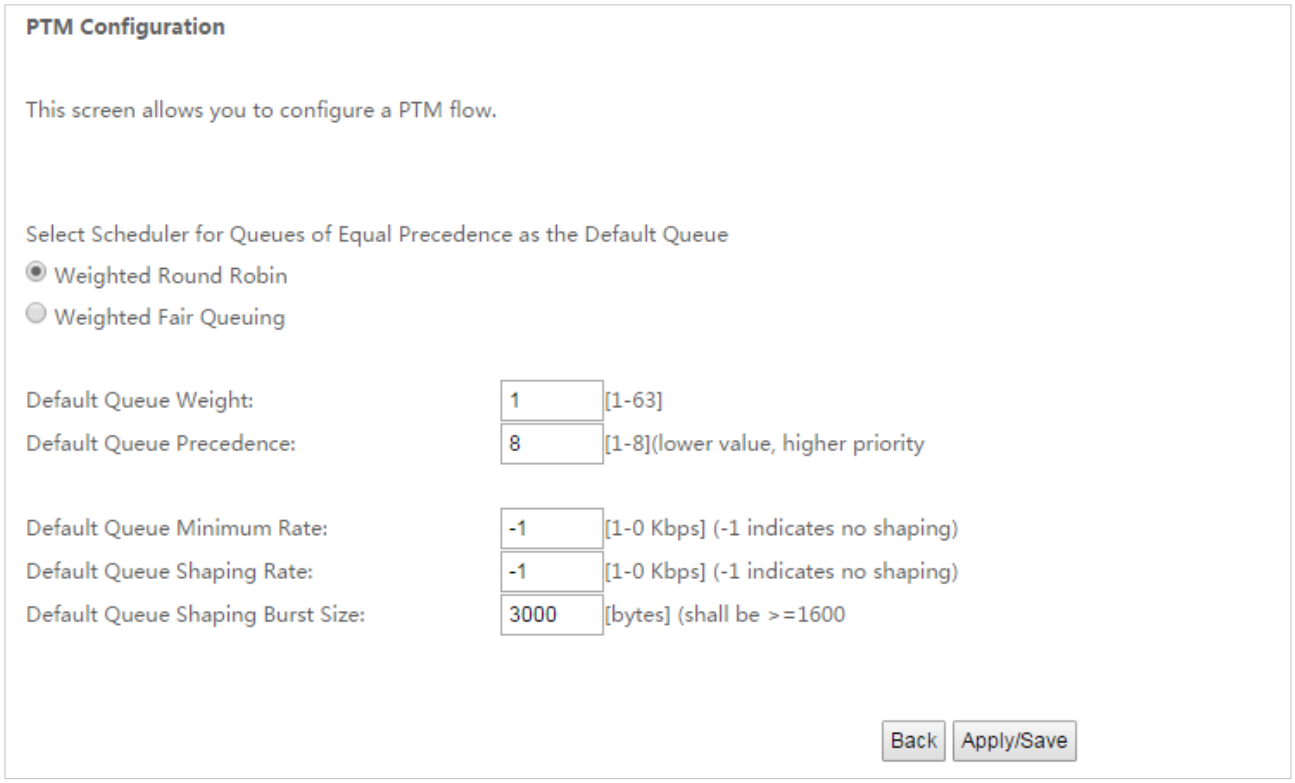
### 4.1.1 Setting the PTM Interface

Log in to the web UI, choose **Advanced** > **Advanced Setup** > **Layer2 Interface** > **PTM** to enter the following page.




**Step 1** Click **Add**.

**Step 2** Leave the parameters for queue parameters unchanged, and click **Apply/Save**.

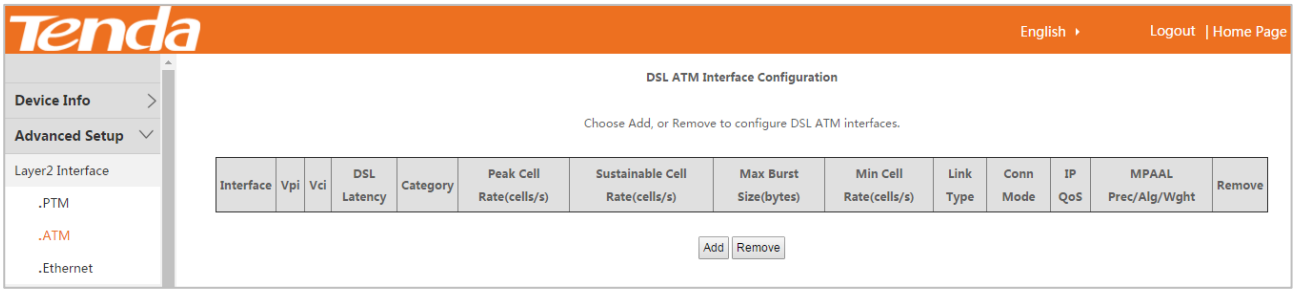



**Step 3** And then refer to Setting WAN Service for PTM Interface to configure the WAN service for internet access.

**--End**

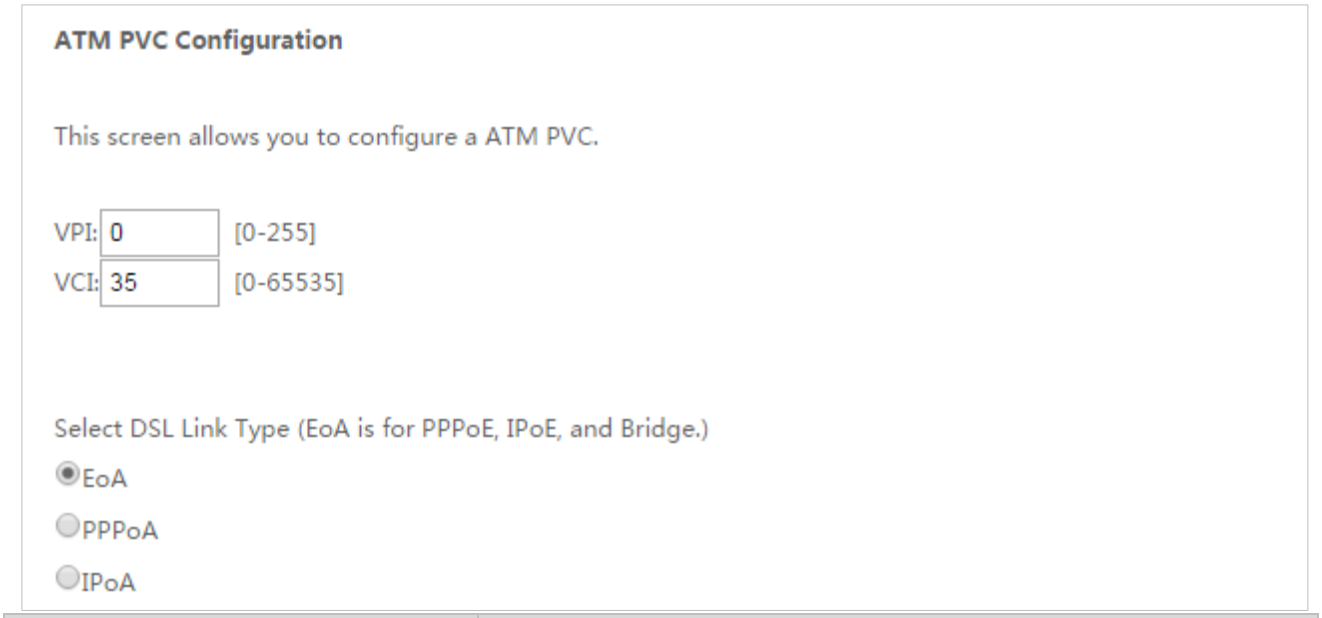
## 4.1.2 Setting the ATM Interface

Log in to the web UI, choose **Advanced** > **Advanced Setup** > **Layer2 Interface** > **ATM** to enter the following page.




**Step 1** Click **Add**.

1. Enter the **VPI** and **VCI** values.
2. Select a DSL Link Type according to the instructions in the table below, and leave other options unchanged. Select **EoA** when your link type is PPPoE, IPoE, or Bridge.
3. Click **Apply/Save** on the bottom of the page.




| Connection Type | | Description |
|---|---|---|
| PPPoE (PPP over Ethernet) | | If your ISP (ISP) provides a user name and password to you for internet access, your connection type may be PPPoE or PPPoA, contact your ISP for details. |
| PPPoA (PPP over ATM) | | |
| IPoE (IP over Ethernet) | Dynamic IP | Select this type if your ISP does not provide any parameters to you for internet access. |
| | Static IP | If your ISP provides a static IP address and other related information to you for internet access, your connection type may be IPoE or IPoA, contact your ISP for details. |
| IPoA (IP over ATM) | Static IP | |
| Bridge | | Select this type when this device only serves as a modem, and you want to set up a dial-up connection or enter other internet parameters directly on your computer for internet access. |

**Step 2** And then refer to Setting WAN Service for ATM Interface to configure the WAN service for internet access.

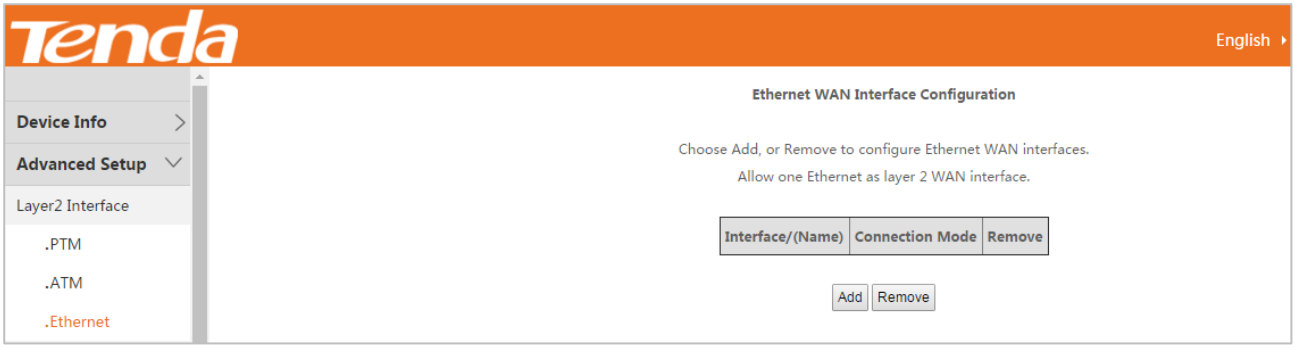
**--End**

TIP

If you are unsure about the VPI/VCI parameters, refer to Appendix 8.4 VPI/VCI List. If the ISP and the VPI/VCI information are not available here, ask your ISP to provide it.

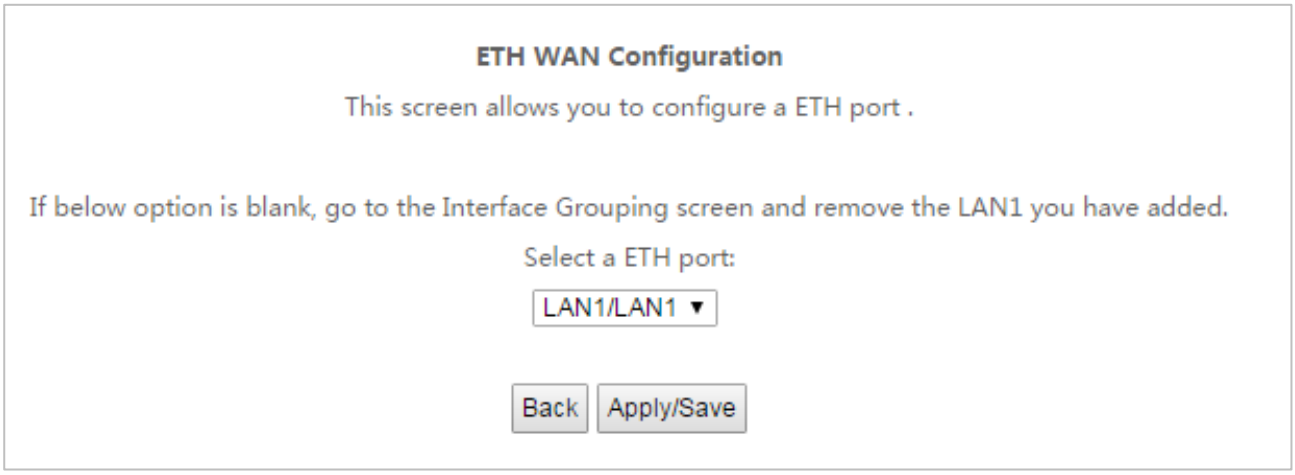
## 4.1.3 Setting the Ethernet Interface

Log in to the web UI, choose **Advanced** > **Advanced Setup** > **Layer2 Interface** > **Ethernet** to enter the following page.




**Step 1** Click **Add**.

**Step 2** Click Apply/Save.




**Step 3** And then refer to Setting WAN Service for Ethernet Interface to configure the WAN service for internet access.

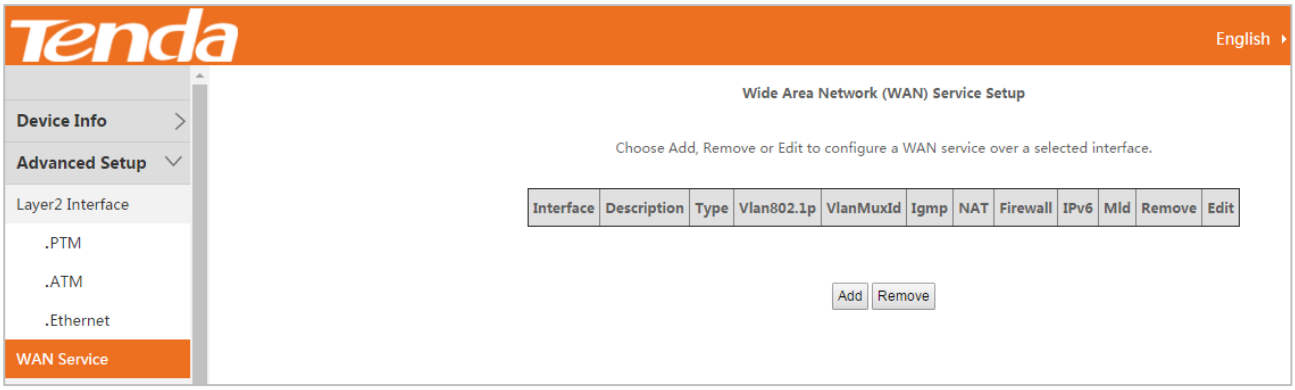
**--End**

# 4.2 WAN Service

Choose **Advanced** > **Advanced Setup** > **WAN Service** to enter the WAN Service page.

## 4.2.1 Setting WAN Service for PTM Interface

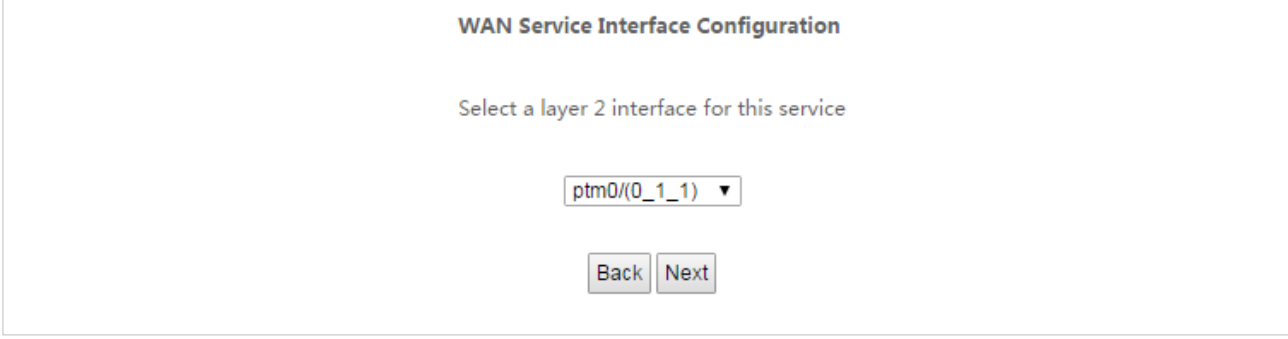
Log in to the web UI, choose **Advanced** > **Advanced Setup** > **WAN Service** to enter the following page.




**Step 1** Click **Add**.

**Step 2** Select the interface you create in Layer2 Interface which is **ptm0/(0_1_1)** in this example.

**Step 3** Click **Next**.




**Step 4** Select a WAN service type according to the instructions in the table below. Here take **PPPoE** as an example.

| Connection Type | | Description |
|---|---|---|
| PPP over Ethernet (PPPoE) | | Select this type if your ISP (ISP) provides a user name and password to you for internet access. |
| IP over Ethernet | Dynamic IP | Select this type if your ISP does not provide any parameters to you for internet access. |
| | Static IP | Select this type if your ISP provides a static IP address and other related information to you for internet access. |
| Bridging | | Select this type when this device only serves as a modem, and you want to set up a dial-up connection or enter other internet parameters directly on your computer for internet access. |

**Step 5** Select PPP over Ethernet.

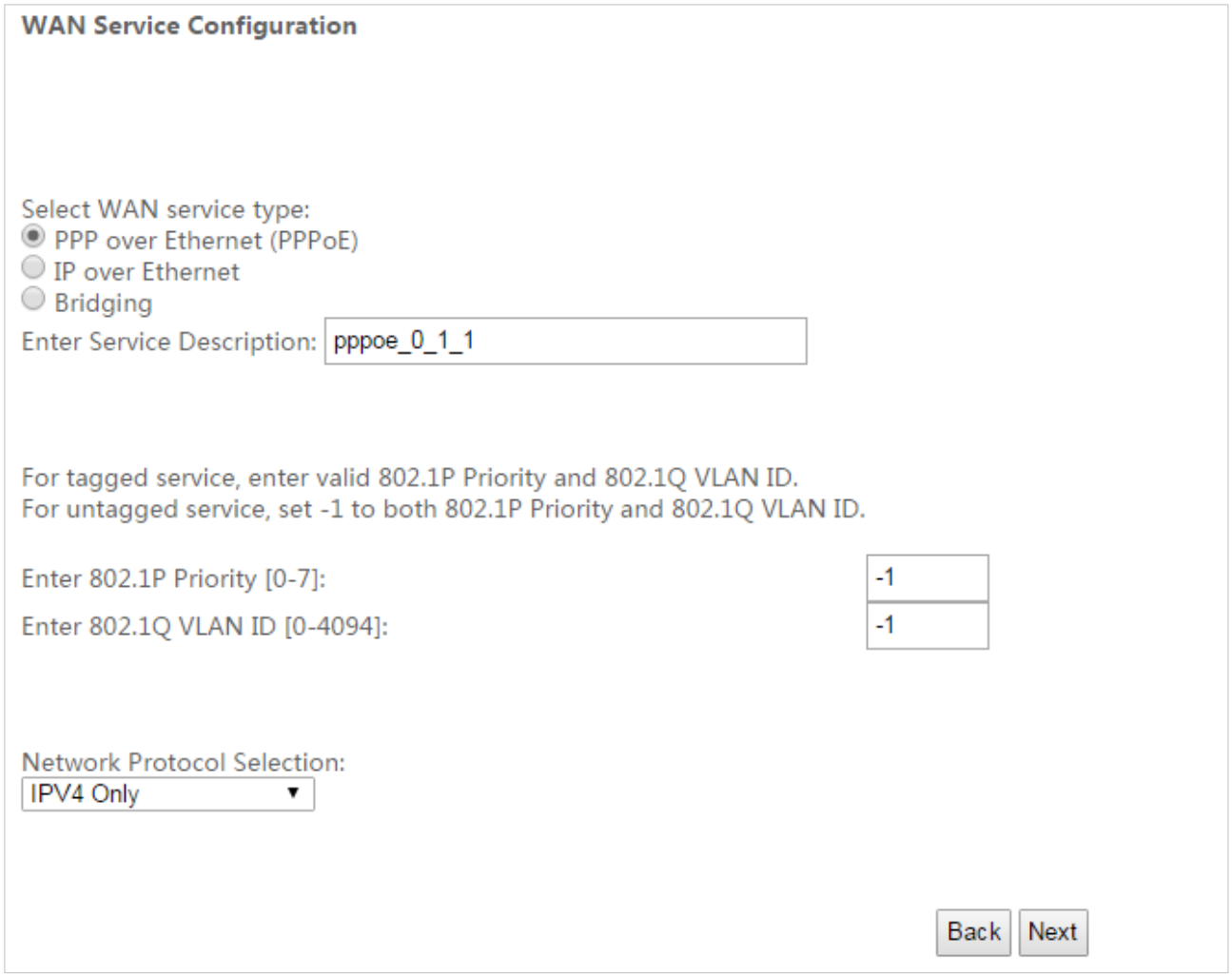
**Step 6** Specify the 802.1P priority and 802.1Q VLAN ID parameters.

TIP

If you are unsure about the 802.1P priority and 802.1Q VLAN ID parameters, refer to Appendix 8.5 VLAN List. If the parameters are not available, ask your ISP to provide it.

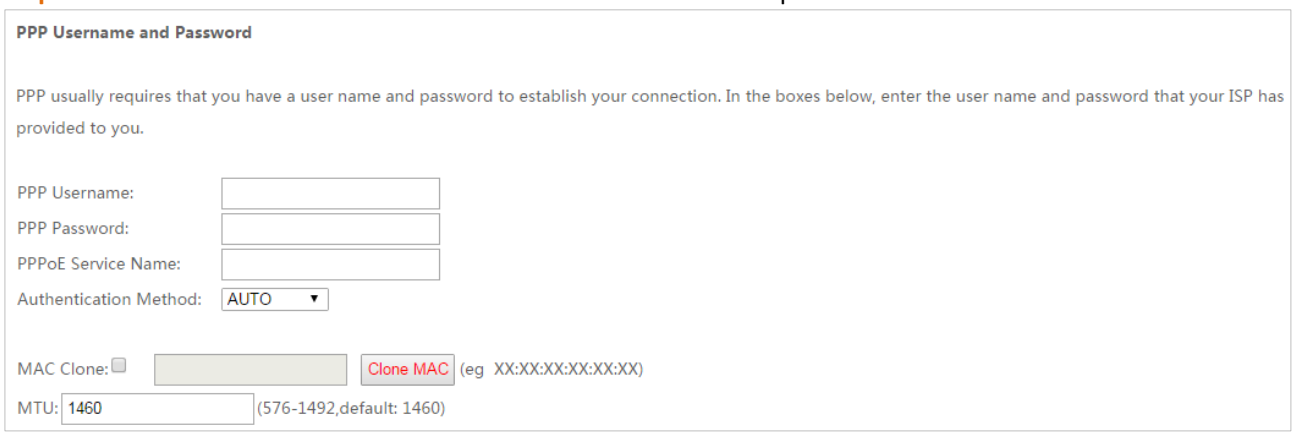
**Step 7** **Network Protocol Selection**: Select your network protocol type. The modem router supports three types of network protocol: IPv4 Only, IPv4&IPv6, and IPv6 Only. Here take IPv4 Only as an example.

**Step 8** Click **Next**.




**Step 9** **PPP Username/PPP Password/**: Enter the PPPoE user name and password provided by your ISP.

**Step 10** **PPPoE Service Name**: Enter the PPPoE service name if it is provided.



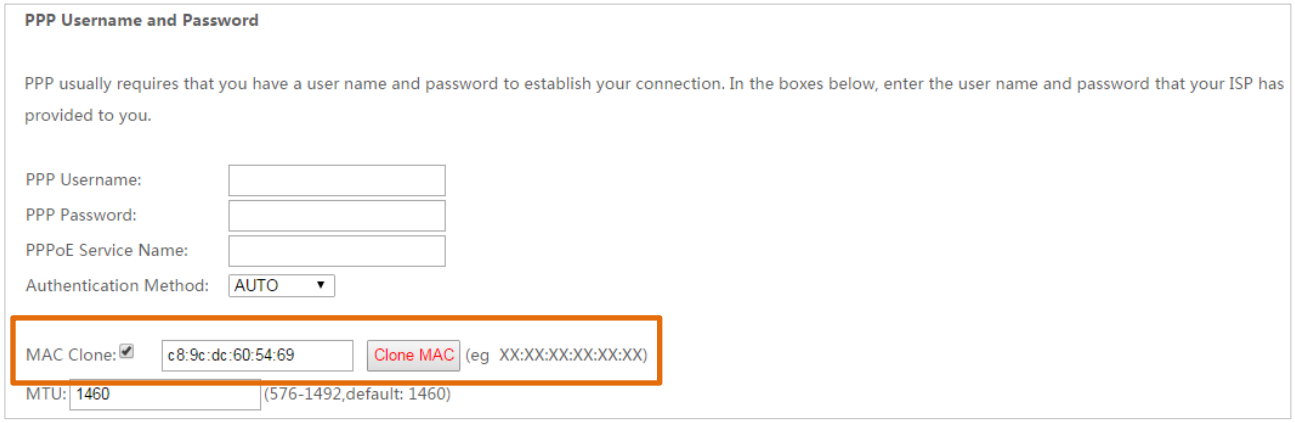

**Step 11** MAC Clone

If you can only access the internet via a specified computer, it may indicate that your ISP binds the internet service to the MAC address of the computer to restrict access. In this case, you need to clone the MAC address of this computer to the modem router for internet access.

**Procedure**

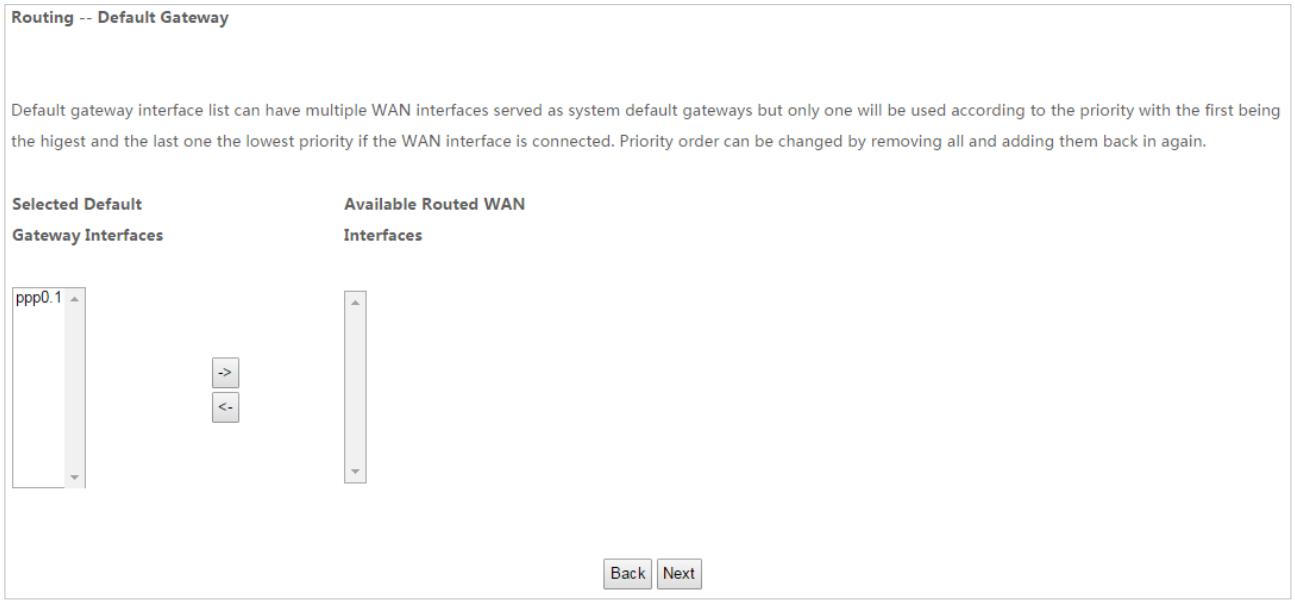
1 Select the MAC address box.

2 Enter the MAC address of the computer. If you use this computer to configure the modem router, you can directly click **Clone MAC** to copy the MAC address to the modem router.



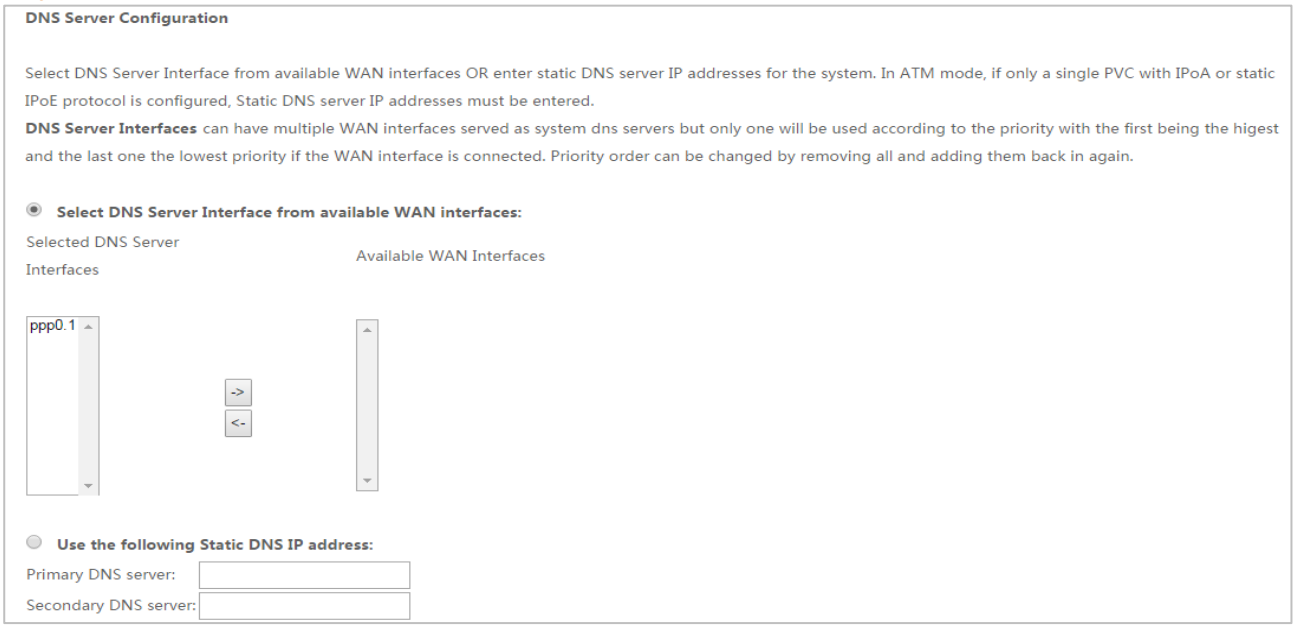

**Step 12** Click **Next**.

**Step 13** Leave the configuration unchanged, and click **Next**.

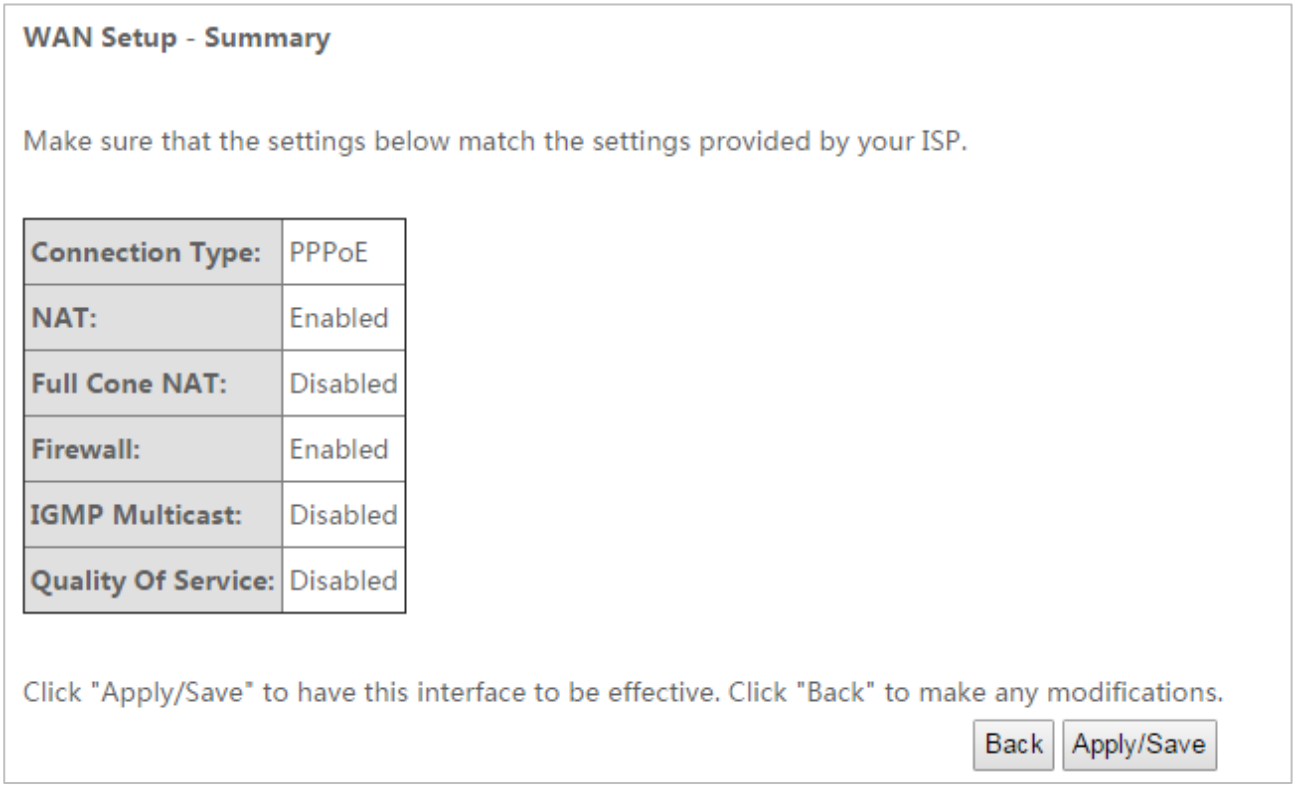



**Step 14** Enter the DNS IP addresses information if it is provided by your ISP. If not, leave then blank.

**Step 15** Click **Next**.

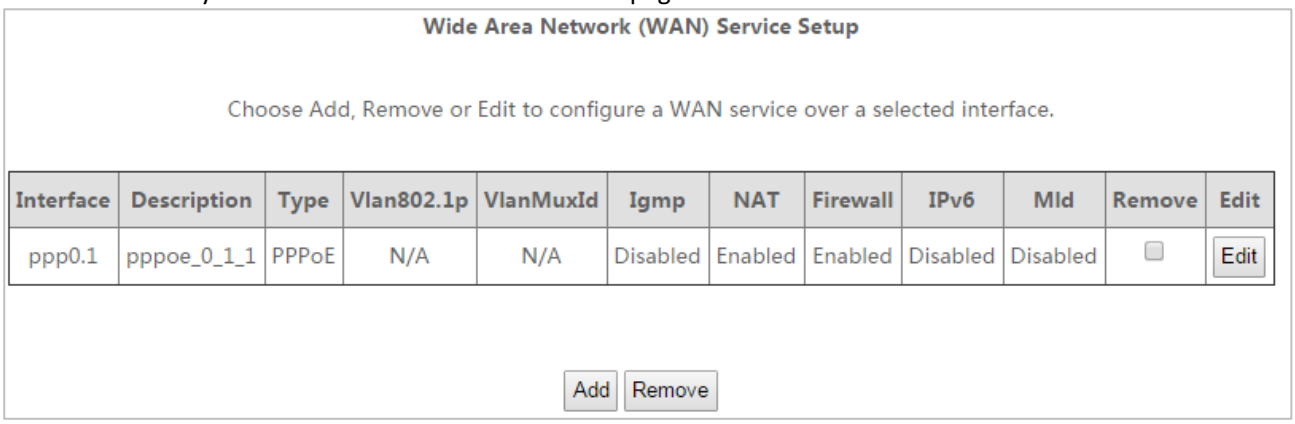


**Step 16** Check the parameters you select or set, and click **Apply/Save**.



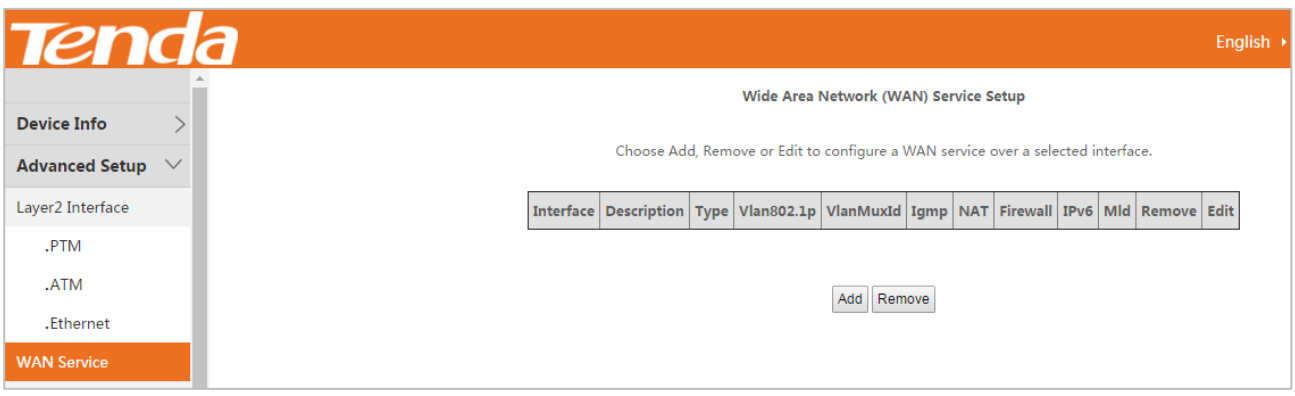

**--End**

The WAN service you set is shown on the **WAN Service** page.




## 4.2.2 Setting WAN Service for ATM Interface

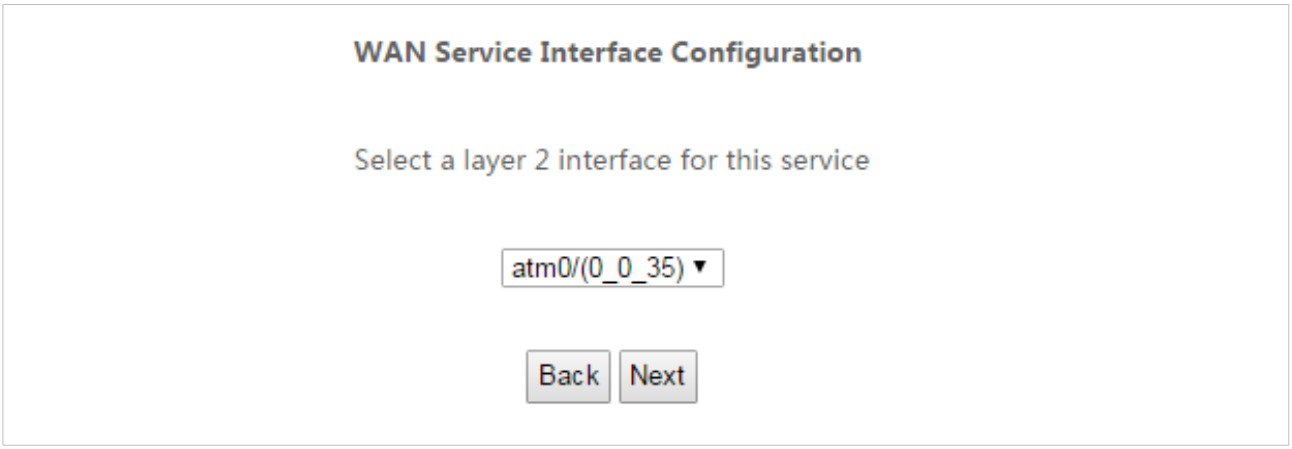
Log in to the web UI, choose **Advanced** > **Advanced Setup** > **WAN Service** to enter the following page.



**Step 1** Click **Add**.

**Step 2** Select ATM interface you create on the Layer2 Interface page which is **atm0/(0_0_35)** in this example.

**Step 3** Click **Next**.



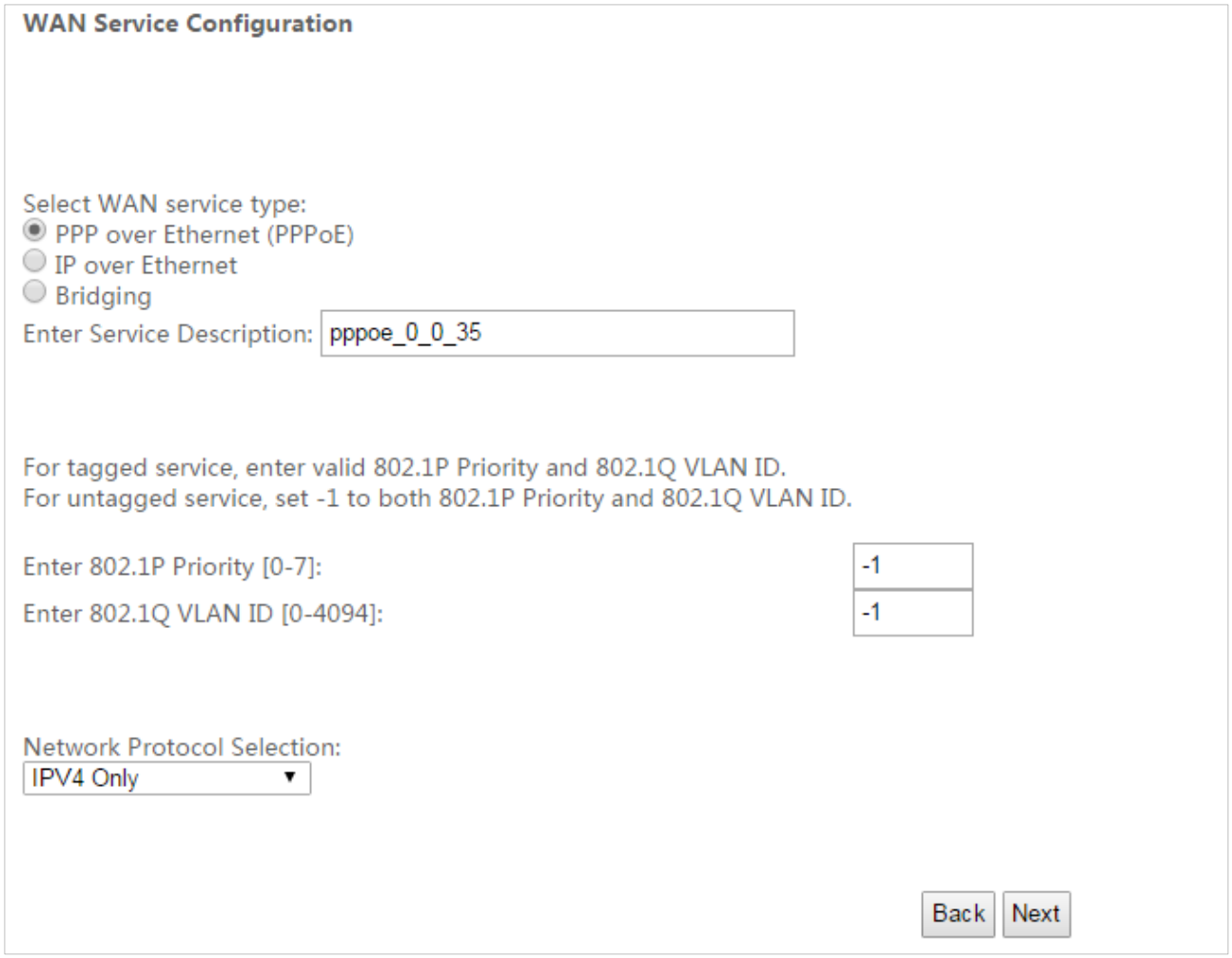

**Step 4** Select a WAN service type according to the instructions in the table below. Here take **PPPoE** as an example.

| **Connection Type** | | **Description** |
|---|---|---|
| PPP over Ethernet (PPPoE) | | Select this type if your ISP provides a user name and password to you for internet access. |
| IP over Ethernet | Dynamic IP | Select this type if your ISP does not provide any parameters to you for internet access. |
| | Static IP | Select this type if your ISP provides a static IP address and other related information to you for internet access. |
| Bridging | | Select this type when this device only serves as a modem, and you want to set up a dial-up connection or enter other internet parameters directly on your computer for internet access. |

**Step 5** Select PPP over Ethernet.

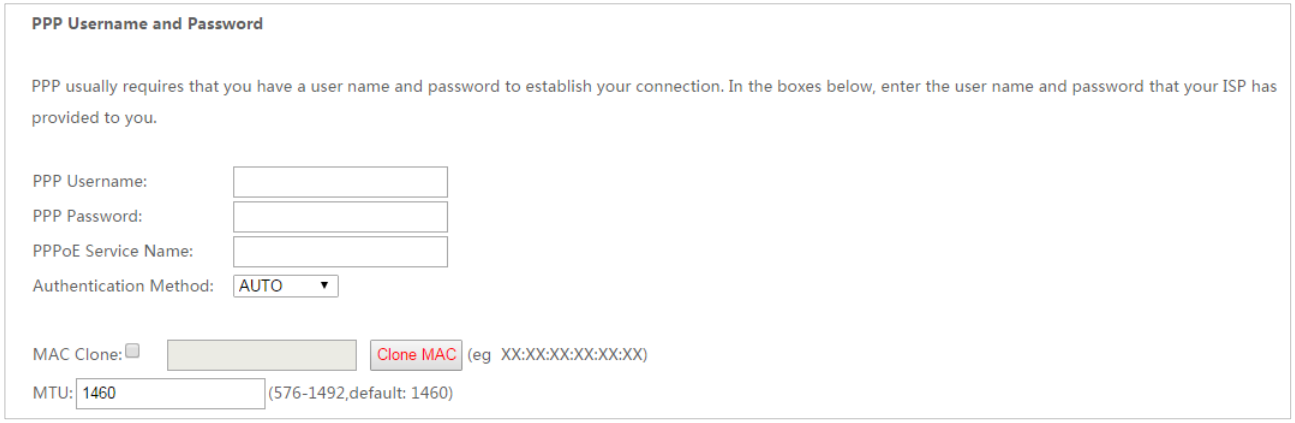
**Step 6** **Network Protocol Selection**: Select your network protocol type. The modem router provides three types of network protocol: IPv4 Only, IPv4&IPv6, and IPv6 Only. Here take IPv4 Only as an example.

**Step 7** Click **Next**.




**Step 8** **PPP Username/PPP Password/**: Enter the PPPoE user name and password provided by your ISP.

**Step 9** **PPPoE Service Name**: Enter the PPPoE service name if it is provided.



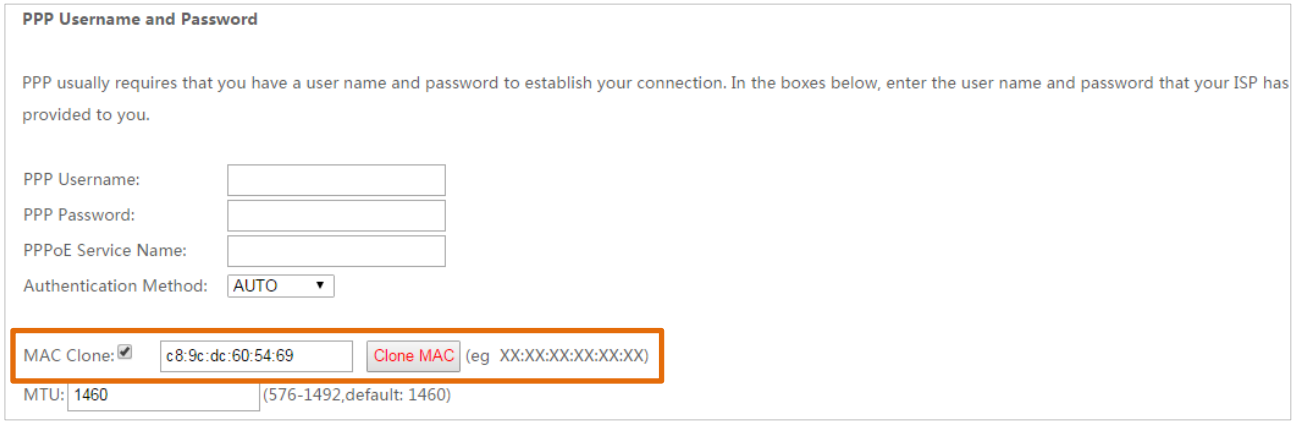

**Step 10** MAC Clone

If you can only access the internet via a specified computer, it may indicate that your ISP binds the internet service to the MAC address of the computer to restrict access. In this case, you need to clone the MAC address of this computer to the modem router for internet access.

**Procedure**

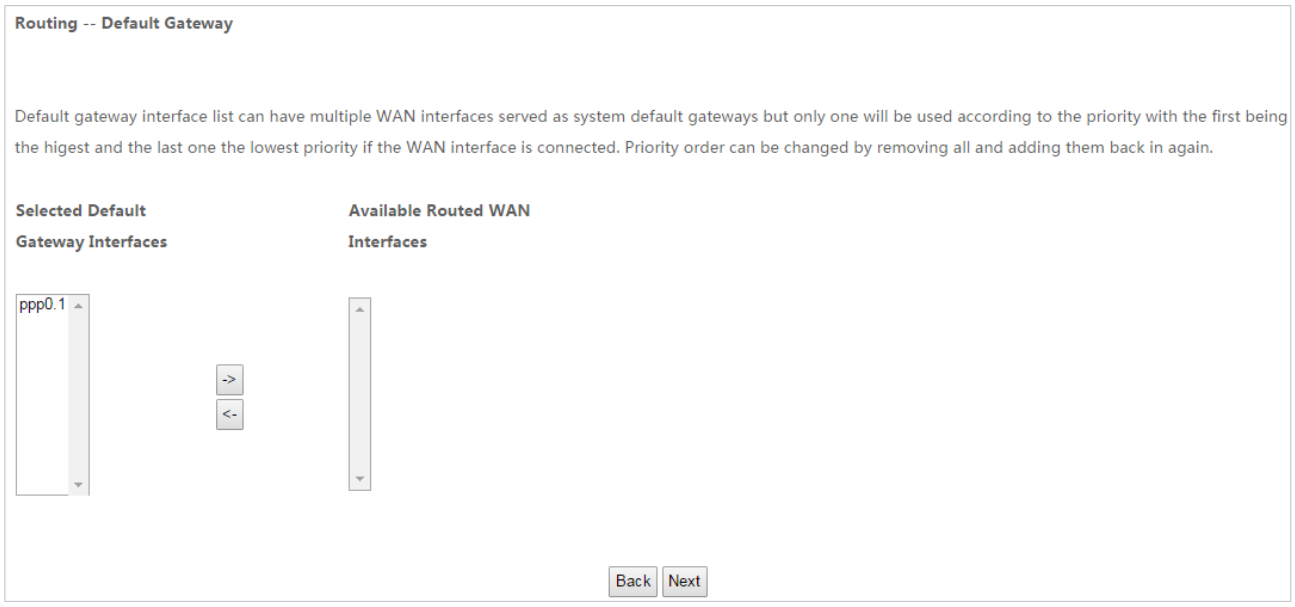
1 Select the MAC address box.

2 Enter the MAC address of the computer. If you use this computer to configure the modem router, you can directly click **Clone MAC** to copy the MAC address to the modem router.



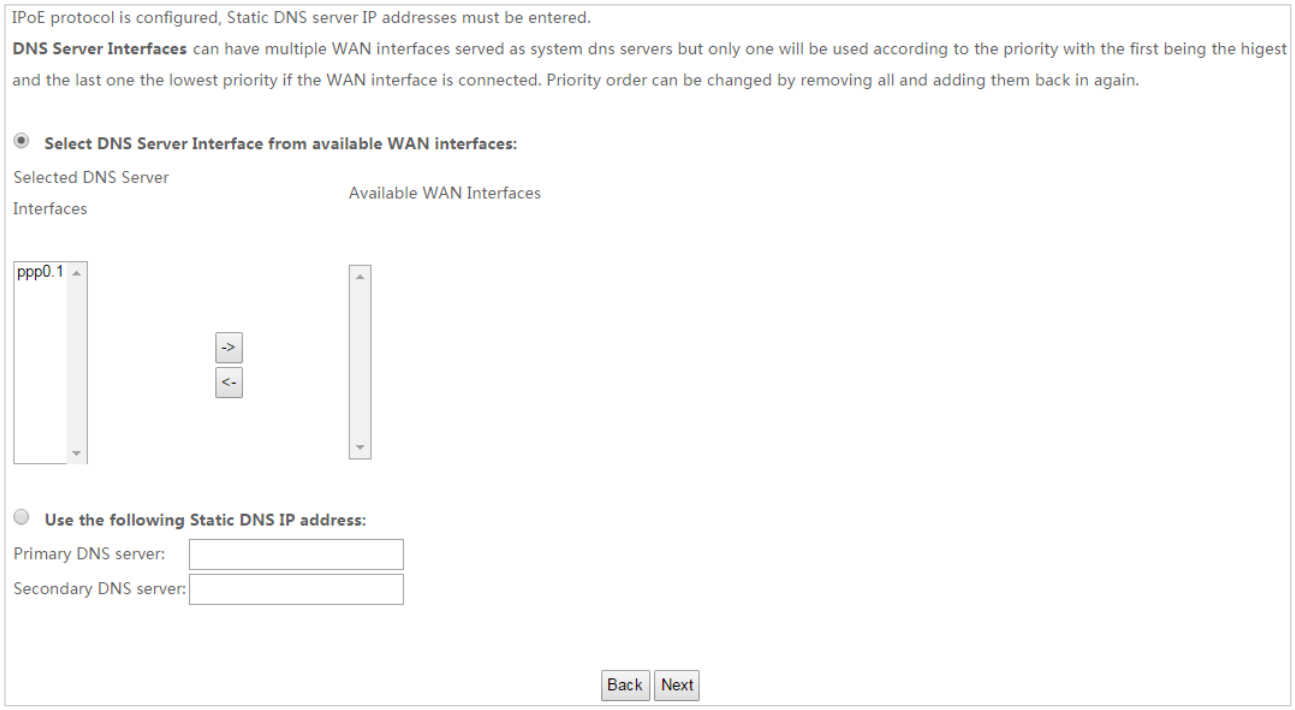

**Step 11** Click **Next**.

**Step 12** Leave the configuration unchanged, and click **Next**.

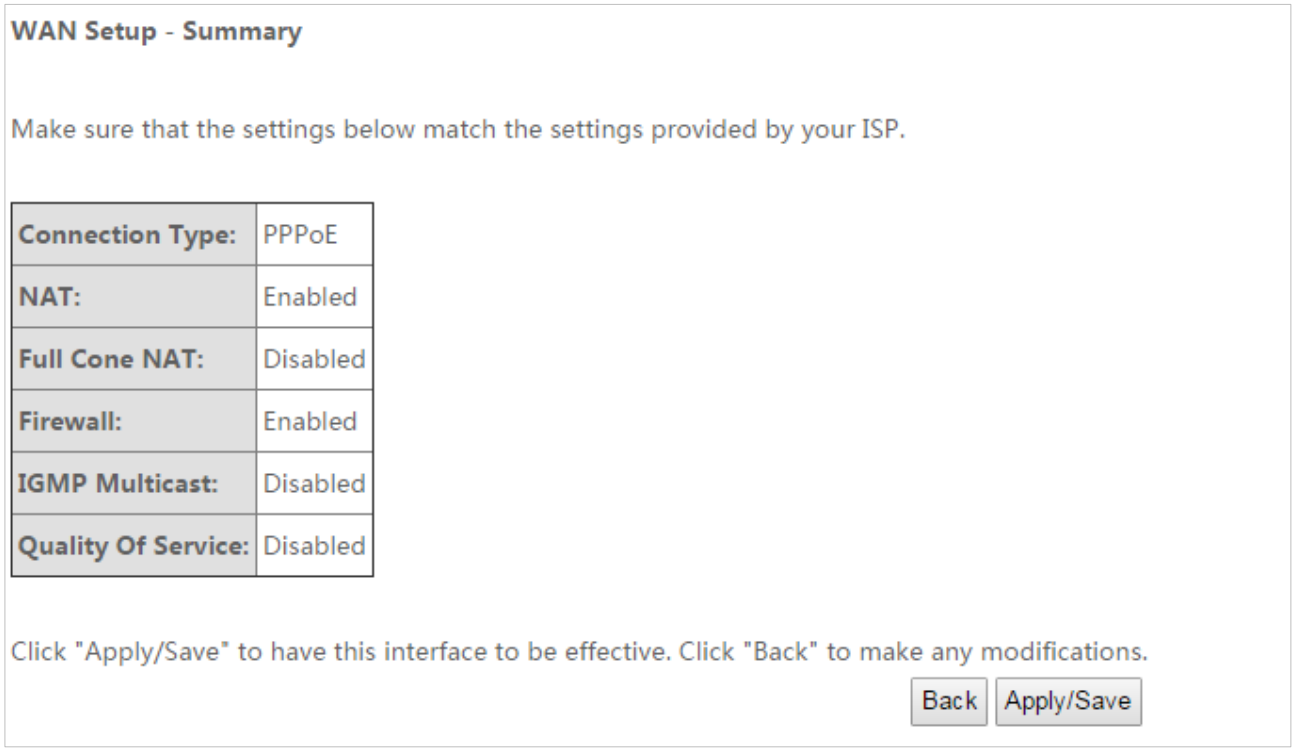



**Step 13** Enter the DNS IP addresses information if they are provided by your ISP. If not, leave then blank.

**Step 14** Click **Next**.

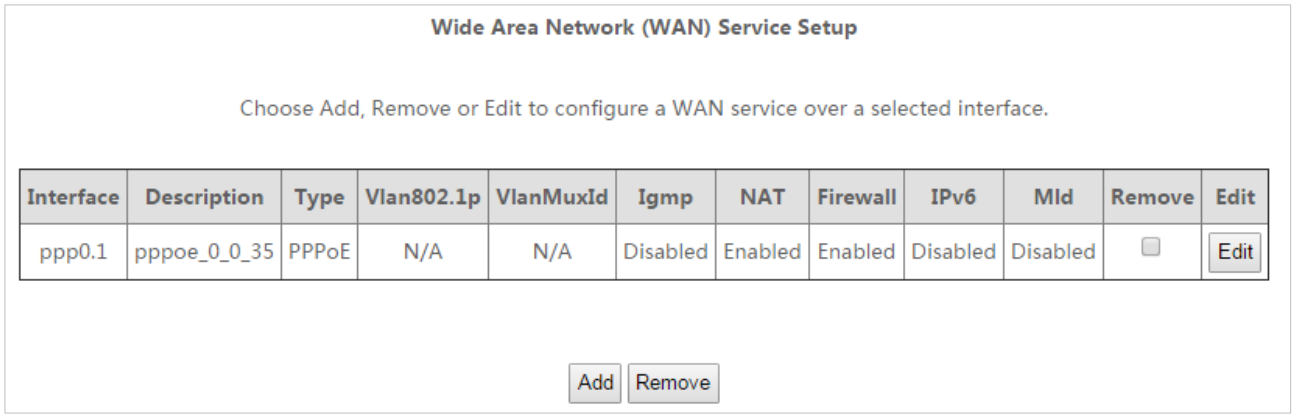



**Step 15** Check the parameters you select or set, and click **Apply/Save**.




**--End**

The WAN service you set is shown on the **WAN Service** page.



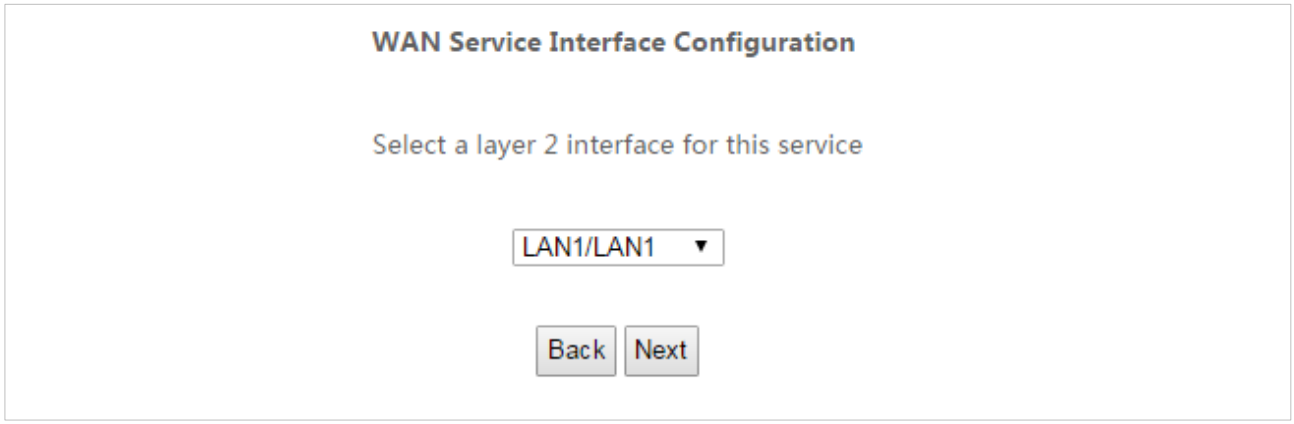

## 4.2.3 Setting WAN Service for Ethernet Interface

Log in to the web UI, choose **Advanced** > **Advanced Setup** > **WAN Service** to enter the following page.


**Step 1** Click **Add**.

**Step 2** Select the interface you create in Layer2 Interface which is **LAN1/LAN1** in this example.

**Step 3** Click **Next**.




**Step 4** Select a WAN service type according to the instructions in the table below. Here take **PPPoE** as an example.

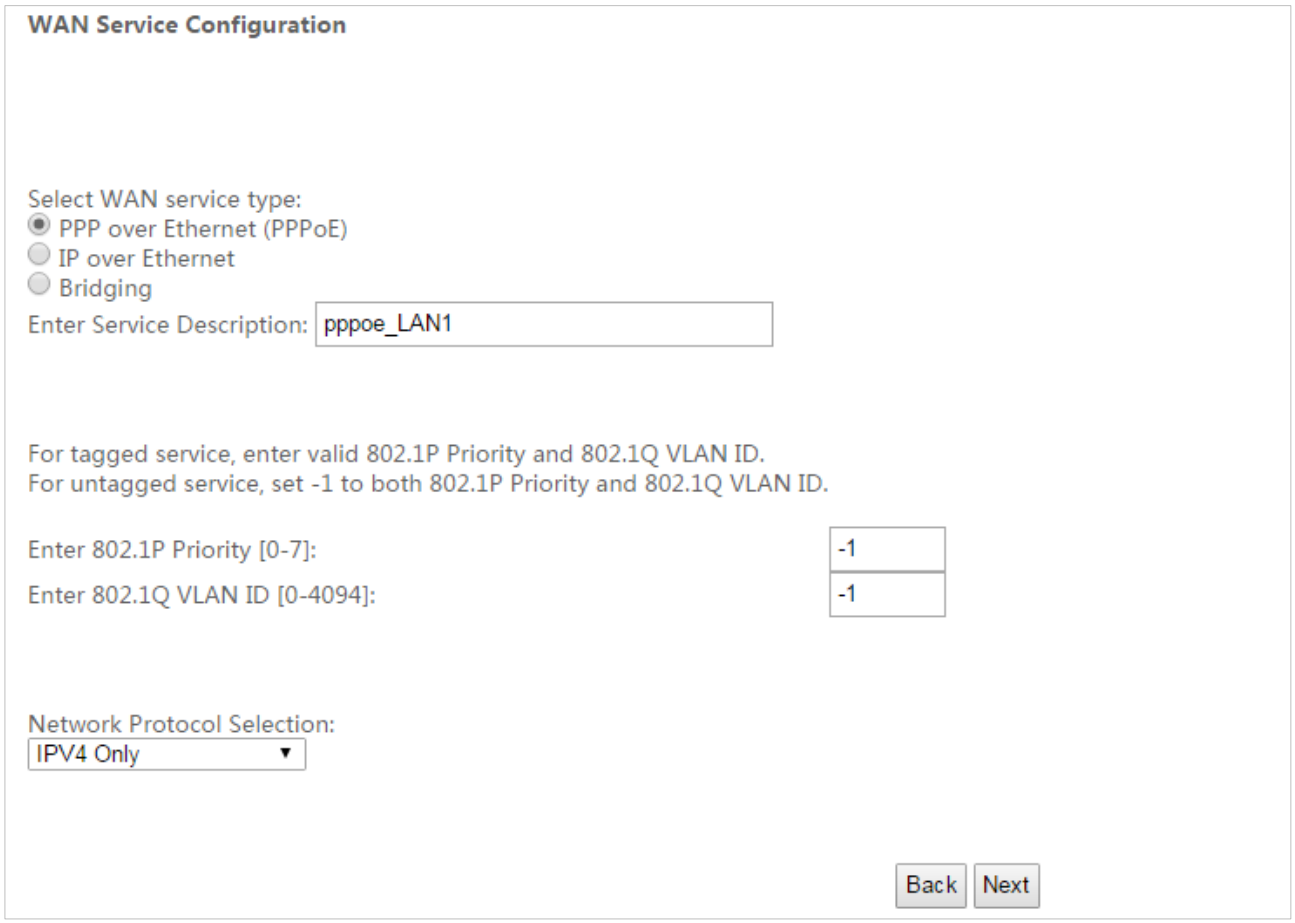
| Connection Type | | Description |
|---|---|---|
| PPP over Ethernet (PPPoE) | | Select this type if your ISP provides a user name and password to you for internet access. |
| IP over Ethernet | Dynamic IP | Select this type if your ISP does not provide any parameters to you for internet access. |

| | | |
|---|---|---|
| | Static IP | Select this type if your ISP provides a static IP address and other related information to you for internet access. |
| Bridging | | Select this type when this device only serves as a modem, and you want to set up a dial-up connection or enter other internet parameters directly on your computer for internet access. |

**Step 5** Select PPP over Ethernet.

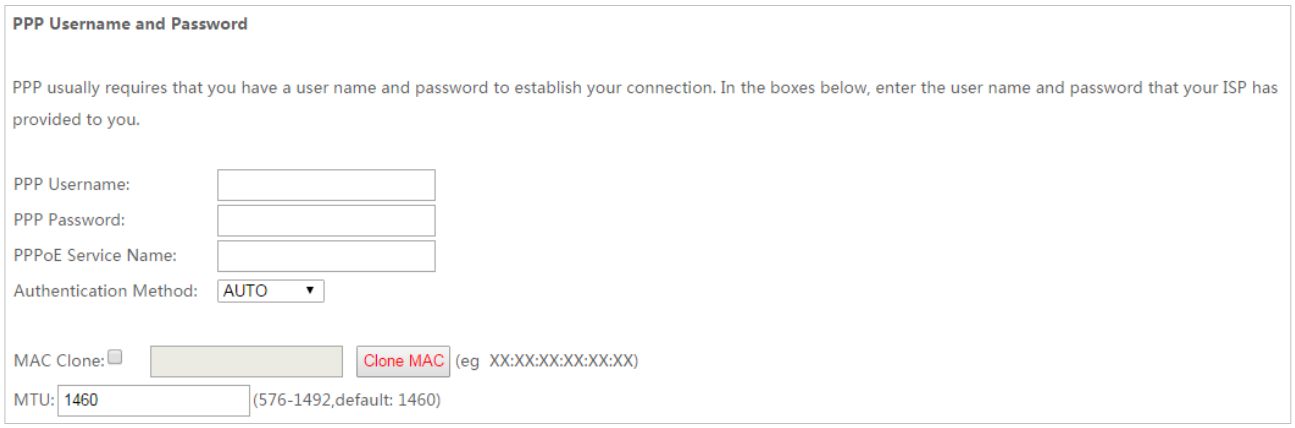
**Step 6** **Network Protocol Selection**: Select your network protocol type. The modem router provides three types of network protocol: IPv4 Only, IPv4&IPv6, and IPv6 Only. Here take IPv4 Only as an example.

**Step 7** Click **Next**.




**Step 8** **PPP Username/PPP Password/**: Enter the PPPoE user name and password provided by your ISP.

**Step 9** **(Optional) PPPoE Service**: Enter the PPPoE service name if it is provided.

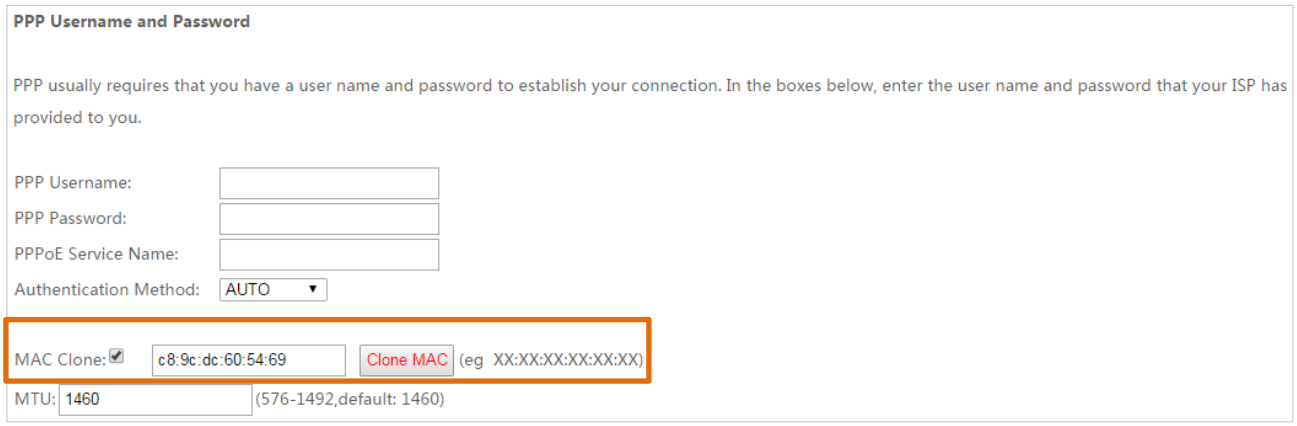


**Step 10** MAC Clone

If you can only access the internet via a specified computer, it may indicate that your ISP binds the internet service with the MAC address of the computer to restrict access. In this case, you need to clone the MAC address of this computer to the modem router for internet access.

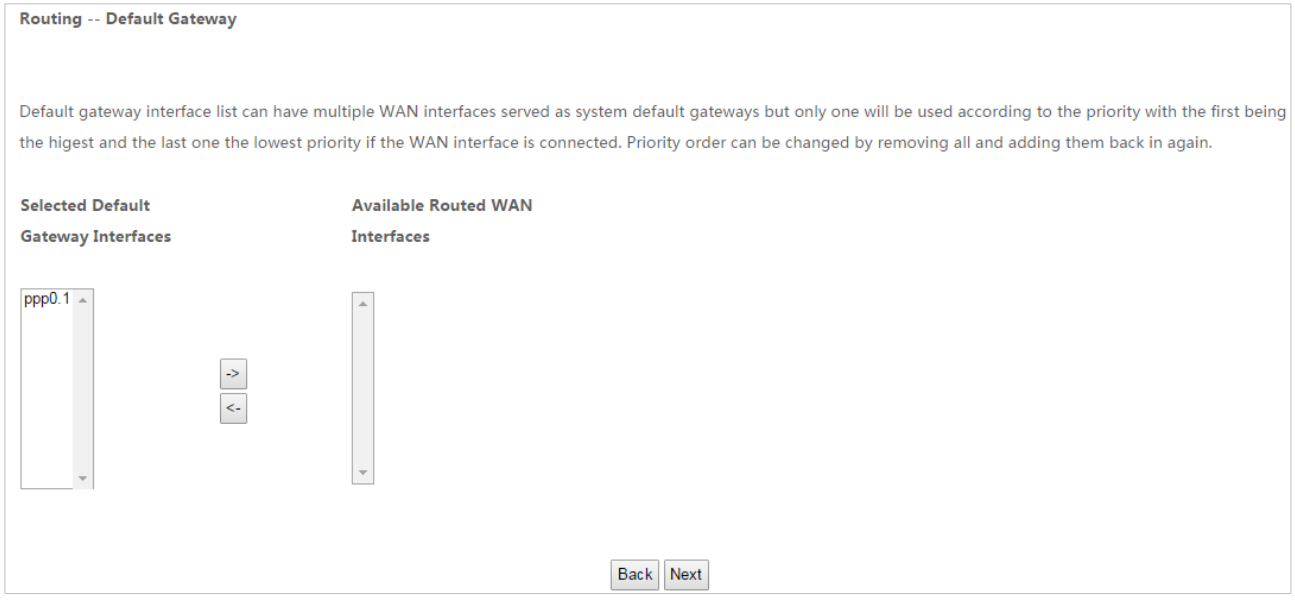
**Procedure**

1. Select the MAC address box.
2. Enter the MAC address of the computer. If you use this computer to configure the modem router, you can directly click **Clone MAC** to copy the MAC address to the modem router.



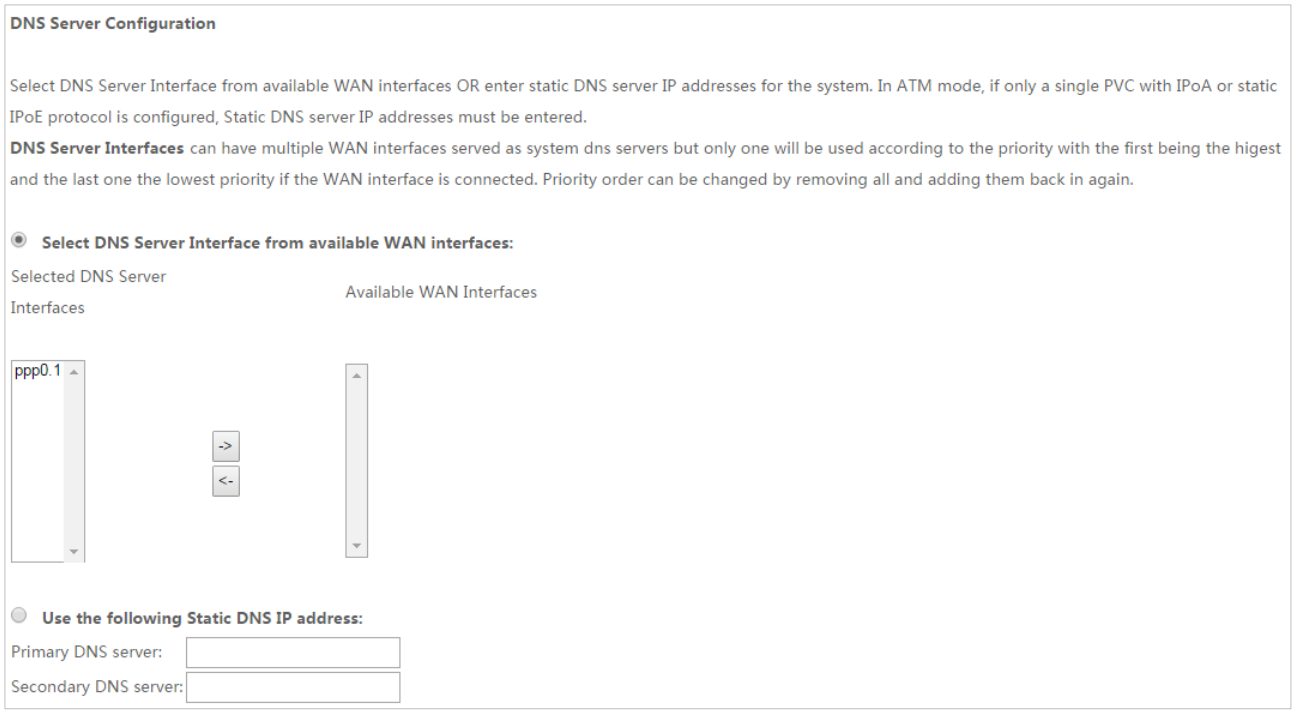

**Step 11** Click **Next**.

**Step 12** Leave the configuration unchanged, and click **Next**.

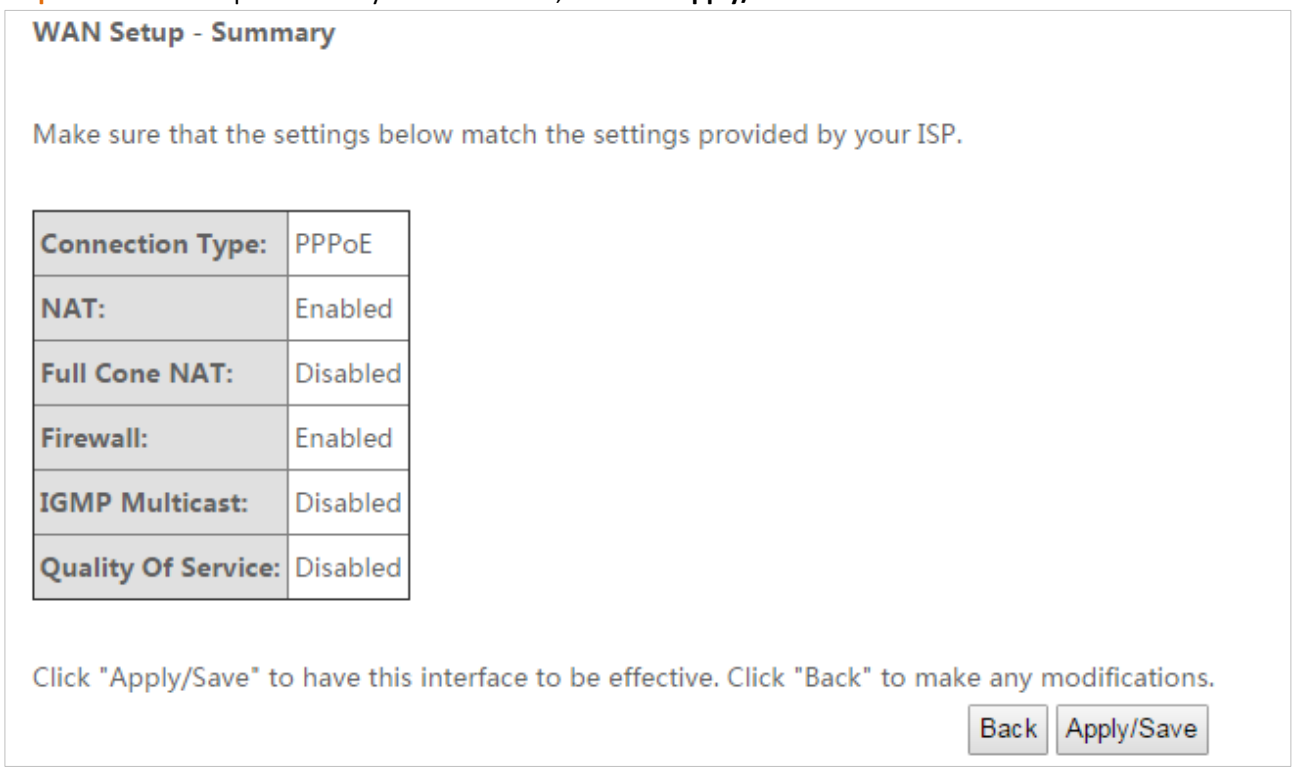



**Step 13** Enter the DNS IP addresses information if they are provided by your ISP. If not, leave then blank.

**Step 14** Click **Next**.

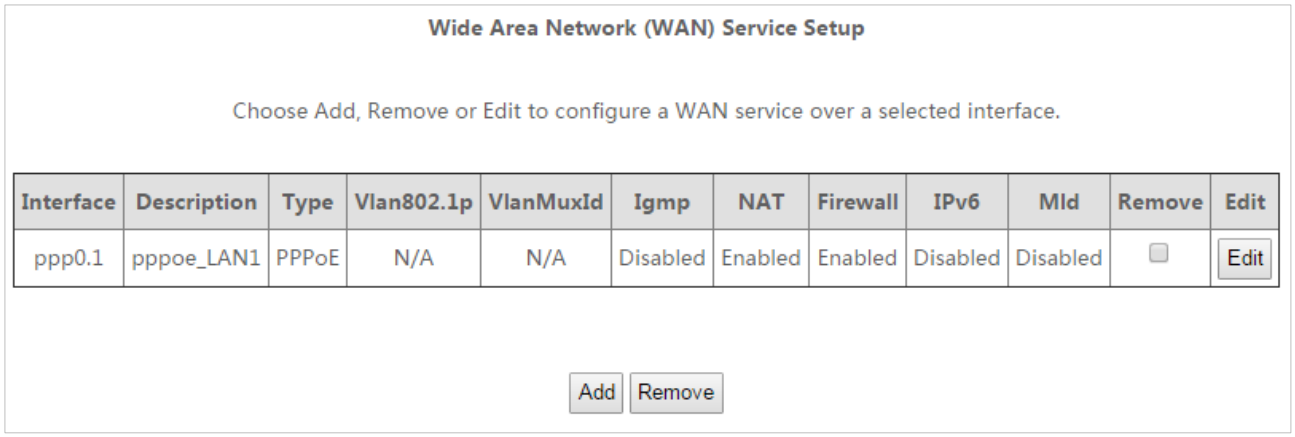



**Step 15** Check the parameters you select or set, and click **Apply/Save**.




**--End**

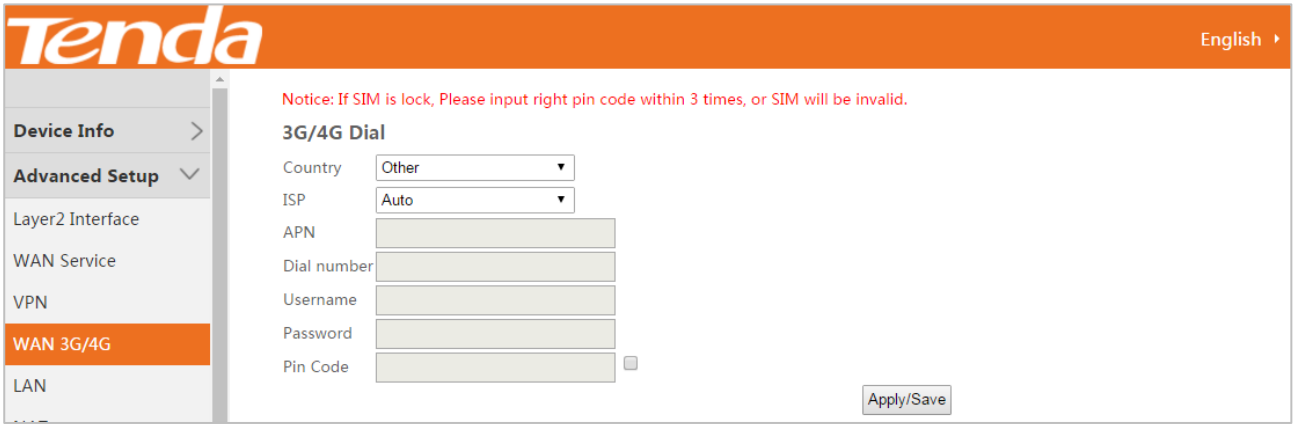
The WAN service you set is shown on the **WAN Service** page.




# 4.3 WAN 3G/4G

If you connect the modem router to the internet via a 3G/4G dongle, and do not complete the internet settings in **Quick Setup** > **3G/4G Dongle**, you can refer to the configuration in this part.

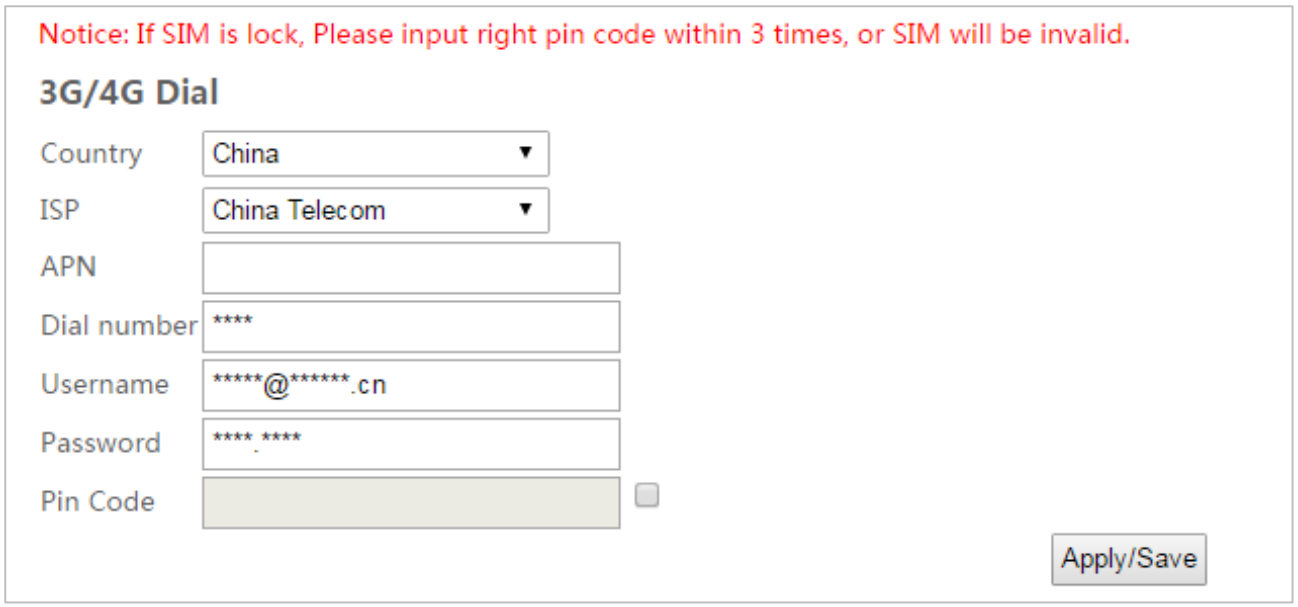
Choose **Advanced** > **Advanced Setup** > **WAN 3G/4G** to enter the configuration page.




**Step 1** Select your country and ISP.

**Step 2** **APN/Dial number/Username/Password/PIN Code**: Generally, if you select correct country and ISP, the necessary parameters can be automatically filled in. If not, set them manually based on the internet parameters provided by your ISP.

**Step 3** Click Apply/Save.



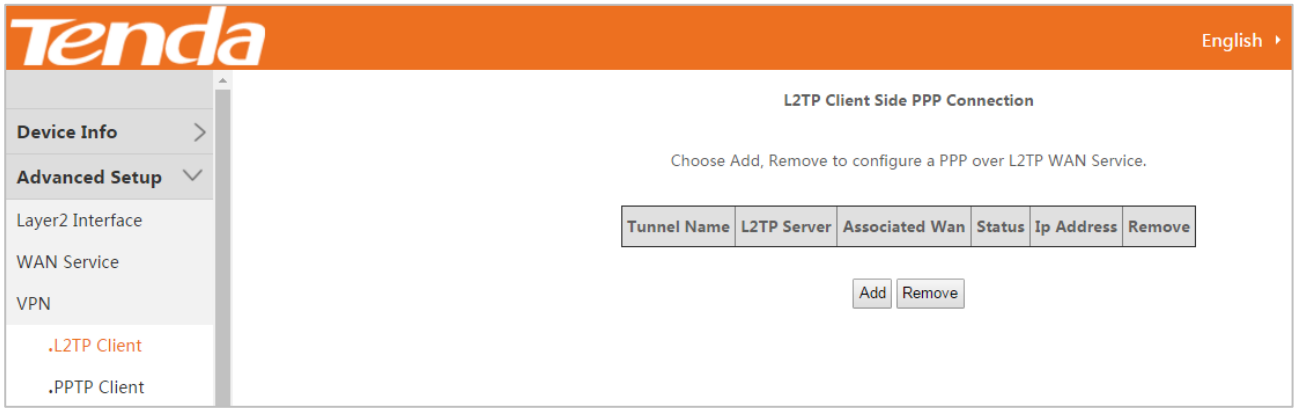

**--End**

# 4.4 VPN

A VPN is a virtual private network set up over a public network (usually the internet).
This modem router can function as a PPTP/L2TP client. The following section describes how to configure the router as a PPTP/L2TP client. If you set up a PPTP/L2TP server, you can enable PPTP/L2TP client function to help you visit the PPTP/L2TP server.

## 4.4.1 L2TP Client

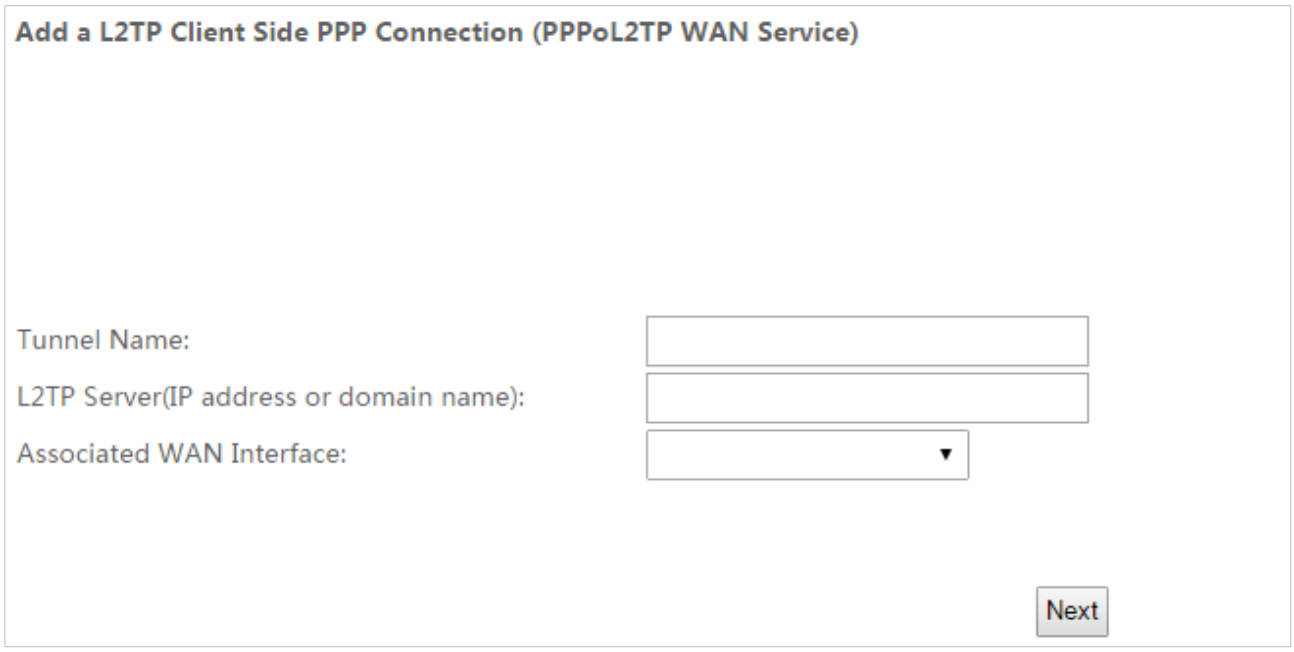
Choose **Advanced** > **Advanced Setup** > **VPN** > **L2TP Client** to enter the configuration page.




**Step 1** Click **Add**.

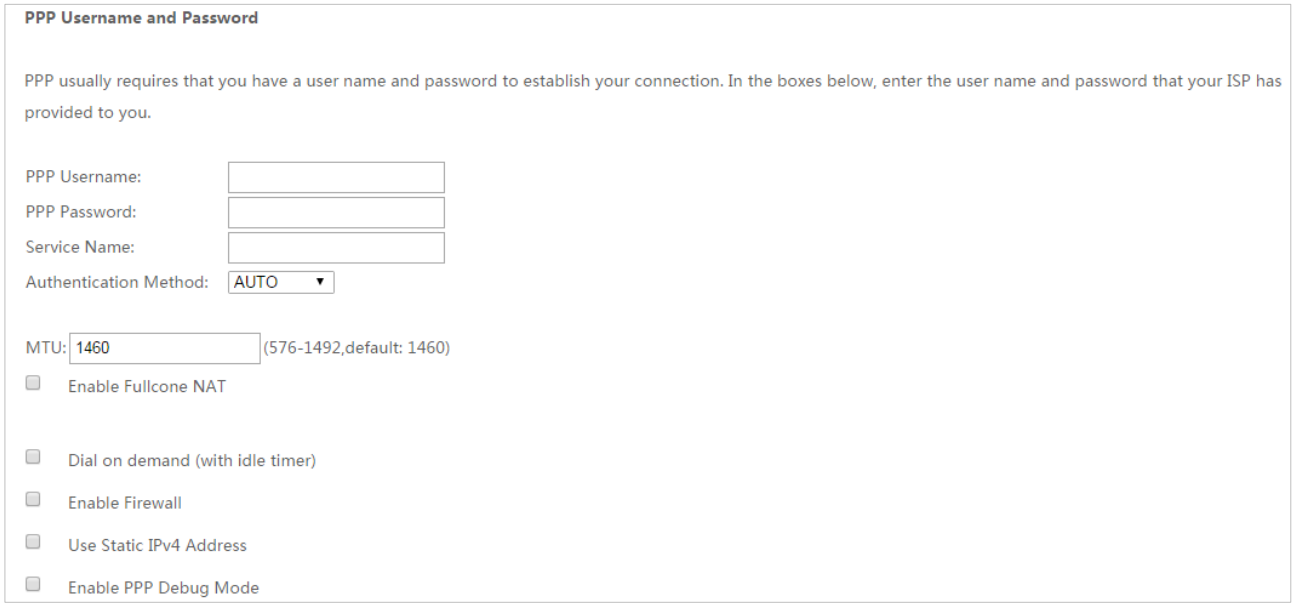

**Step 2** Set **Tunnel Name** and **L2TP Server IP address/domain name** based on the information set on the L2TP server, and select an **Associated WAN Interface**.

**Step 3** Click **Next**.



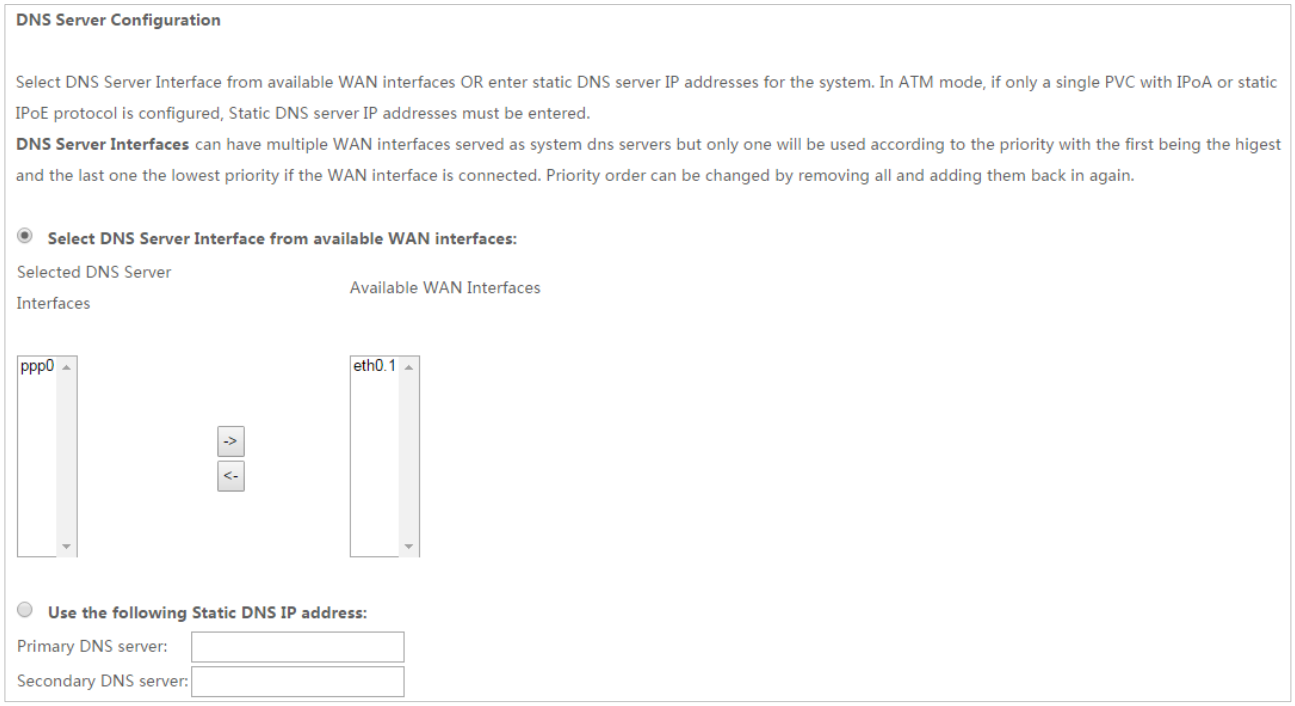

**Step 4** Set **PPP Username**, **PPP Password**, and **Service Name** based on the information set on the L2TP server.

**Step 5** Click **Next**.

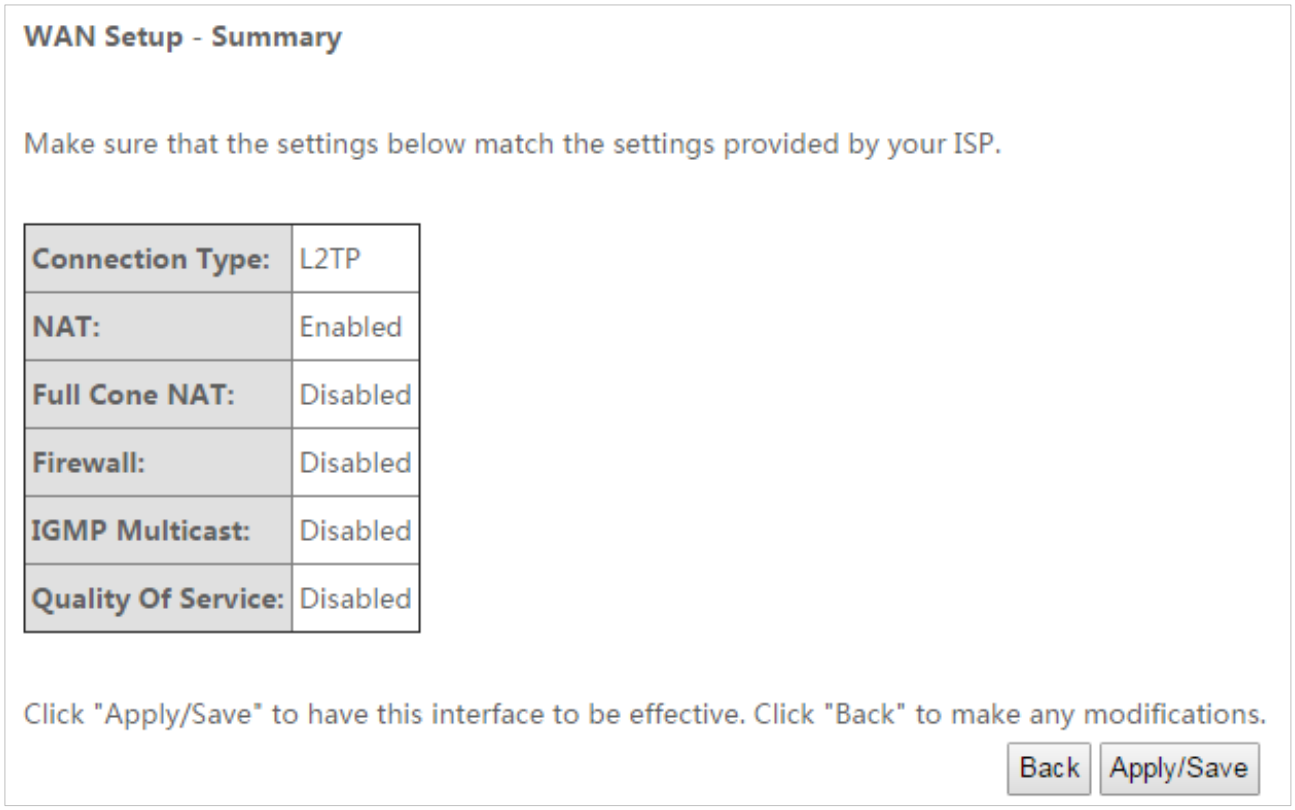


**Step 6** Click **Next**.


**Step 7** Enter the DNS IP addresses information if there is. If not, leave them blank.

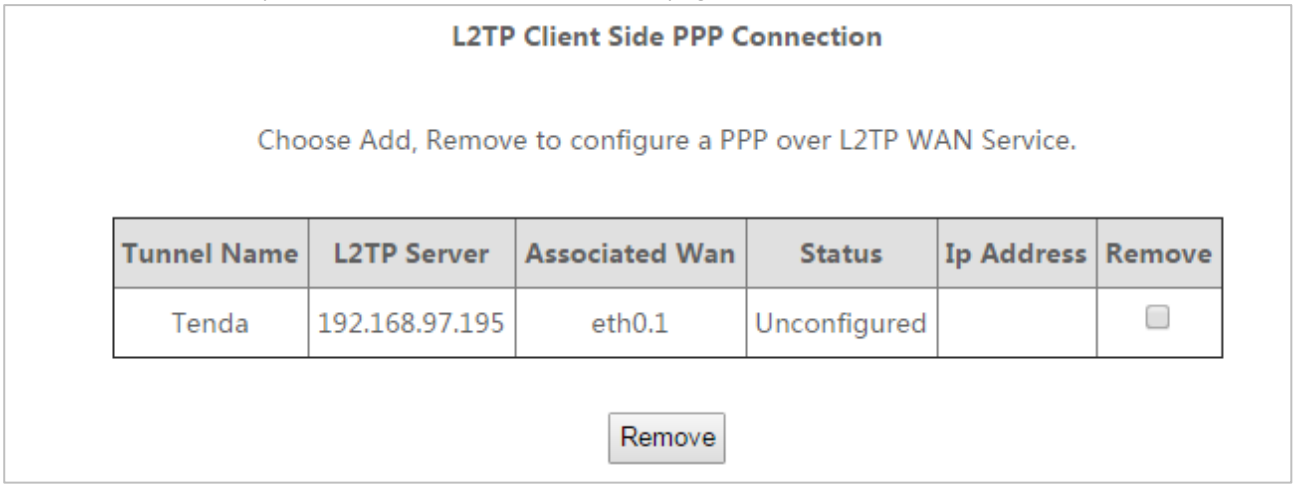



**Step 8** Check the parameters you select or set, and click **Apply/Save**.




**--End**

The L2TP WAN service you set is shown on the L2TP Client page.



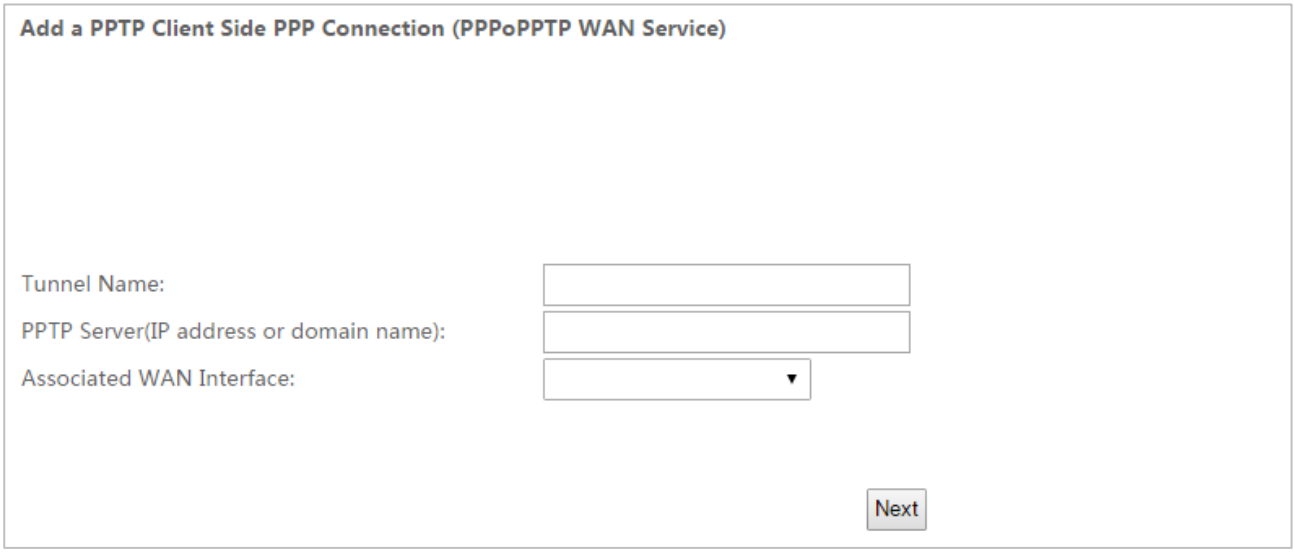

## 4.4.2 PPTP Client

Choose **Advanced** > **Advanced Setup** > **VPN** > **PPTP Client** to enter the configuration page.


**Step 1** Click **Add**.

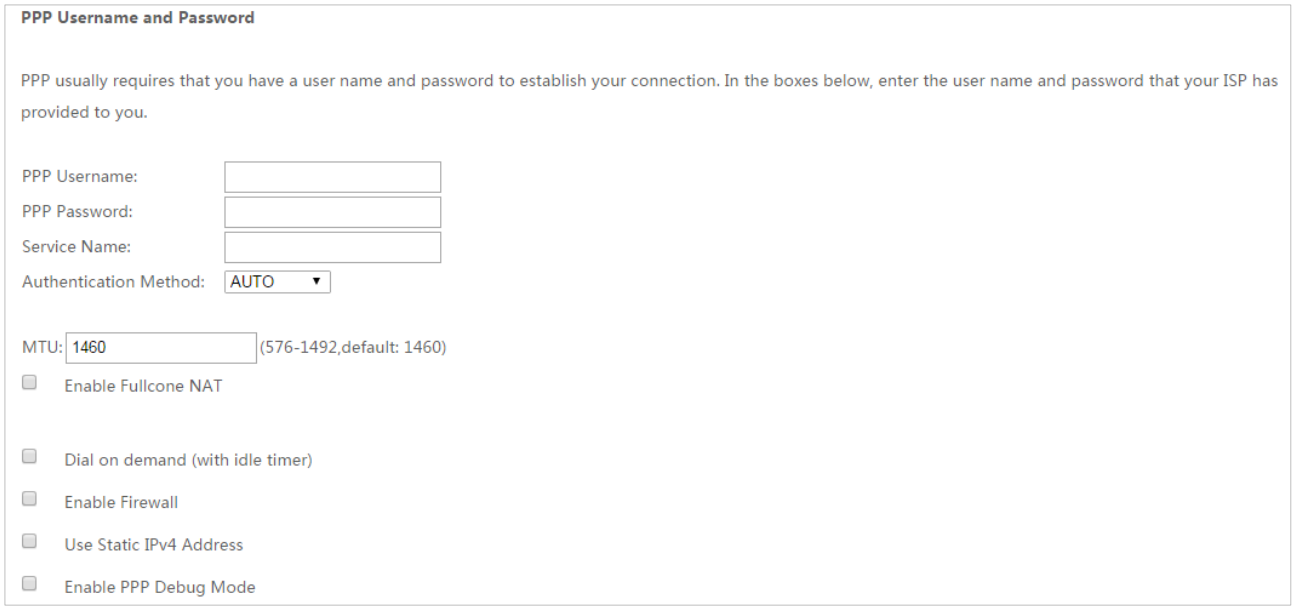

**Step 2** Set **Tunnel Name** and **L2TP Server IP address/domain name** based on the information set on the PPTP server, and select an **Associated WAN Interface**.

**Step 3** Click **Next**.

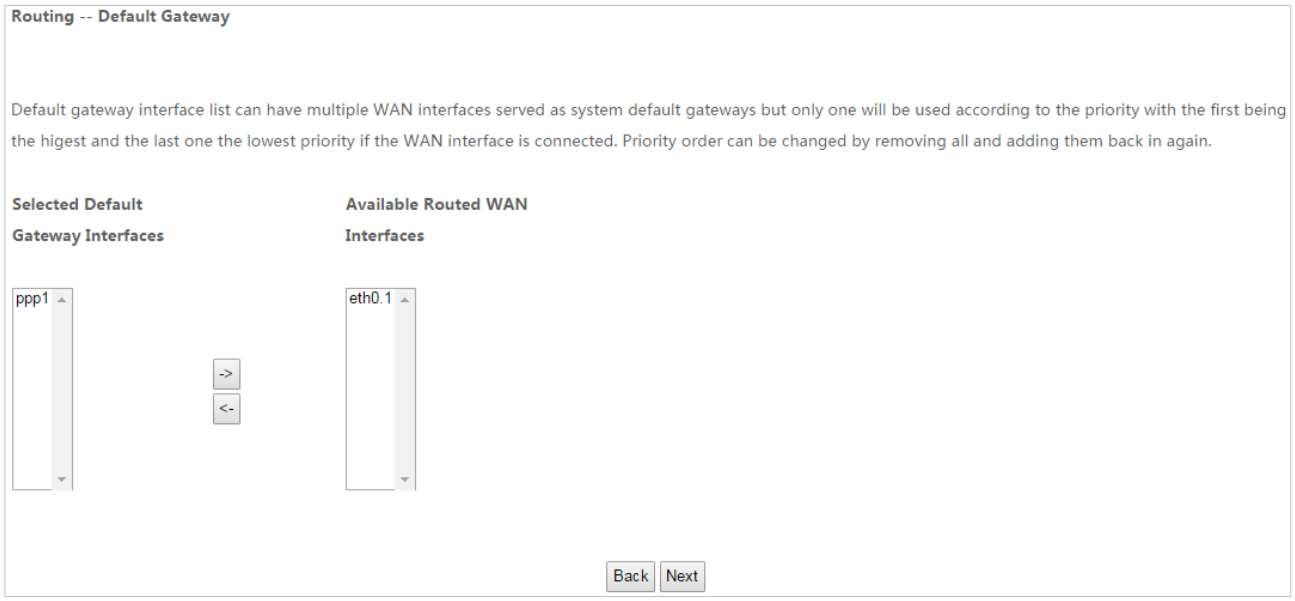



**Step 4** Set **PPP Username**, **PPP Password**, and **Service Name** based on the information set on the PPTP server.

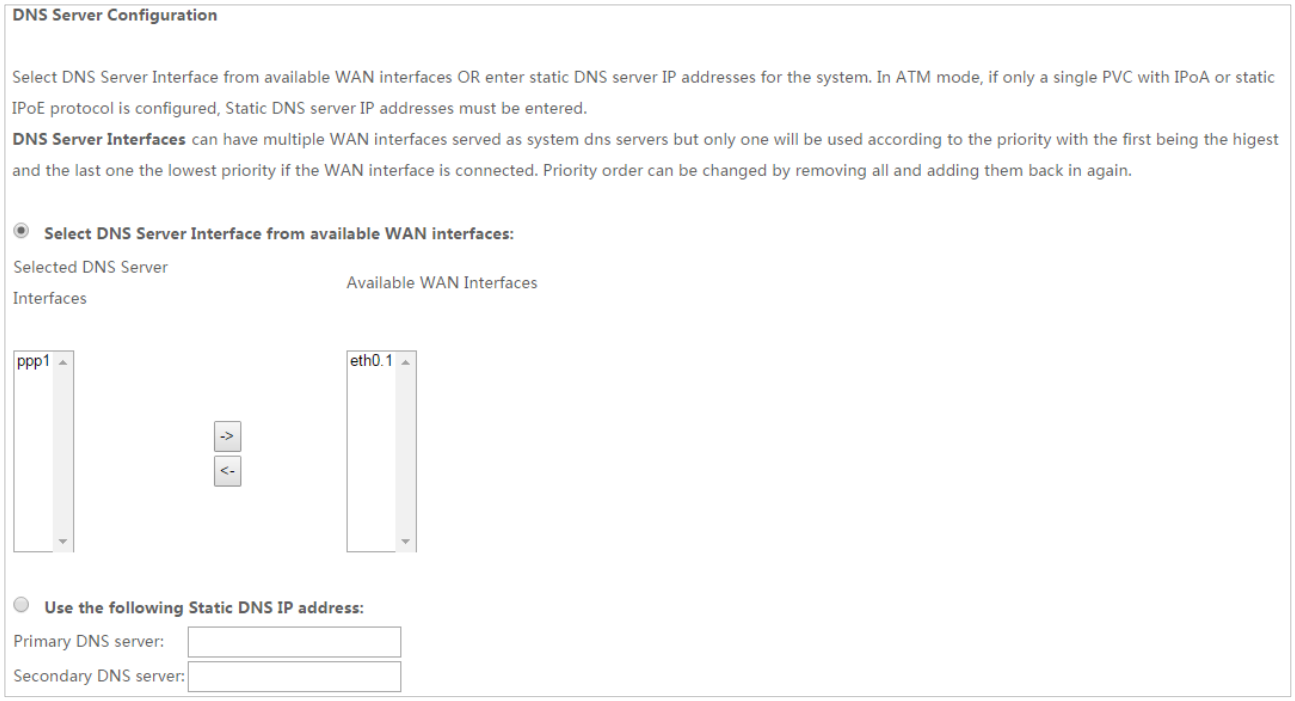
**Step 5** Click **Next**.



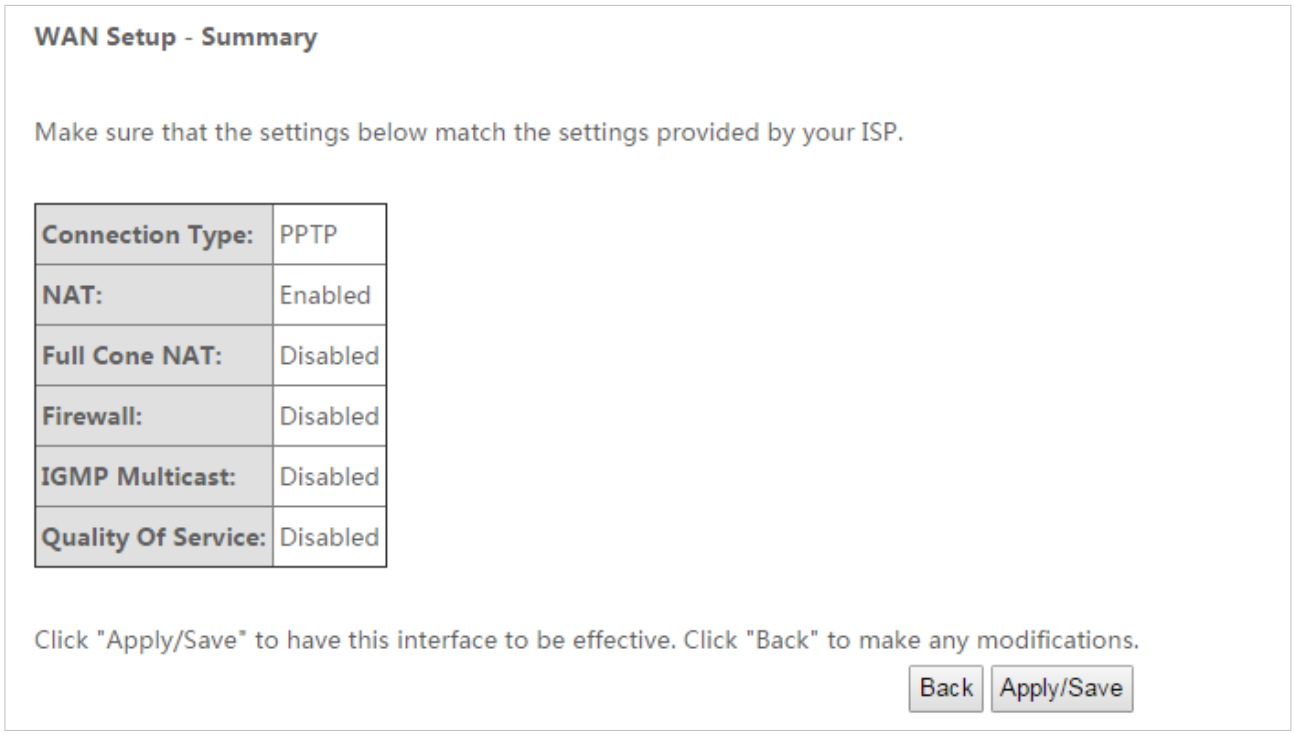

**Step 6** Click **Next**.




**Step 7** Enter the DNS IP addresses information if there is. If not, leave then blank.

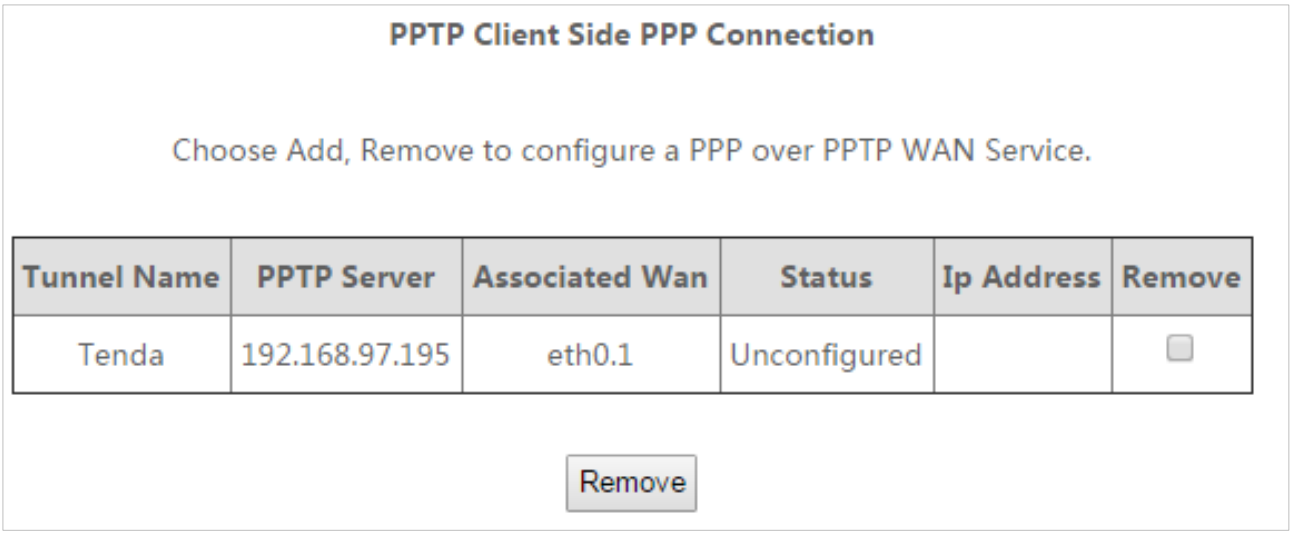



**Step 8** Check the parameters you select or set, and click **Apply/Save**.




**--End**

The PPTP WAN service you set is shown in the PPTP Client page.

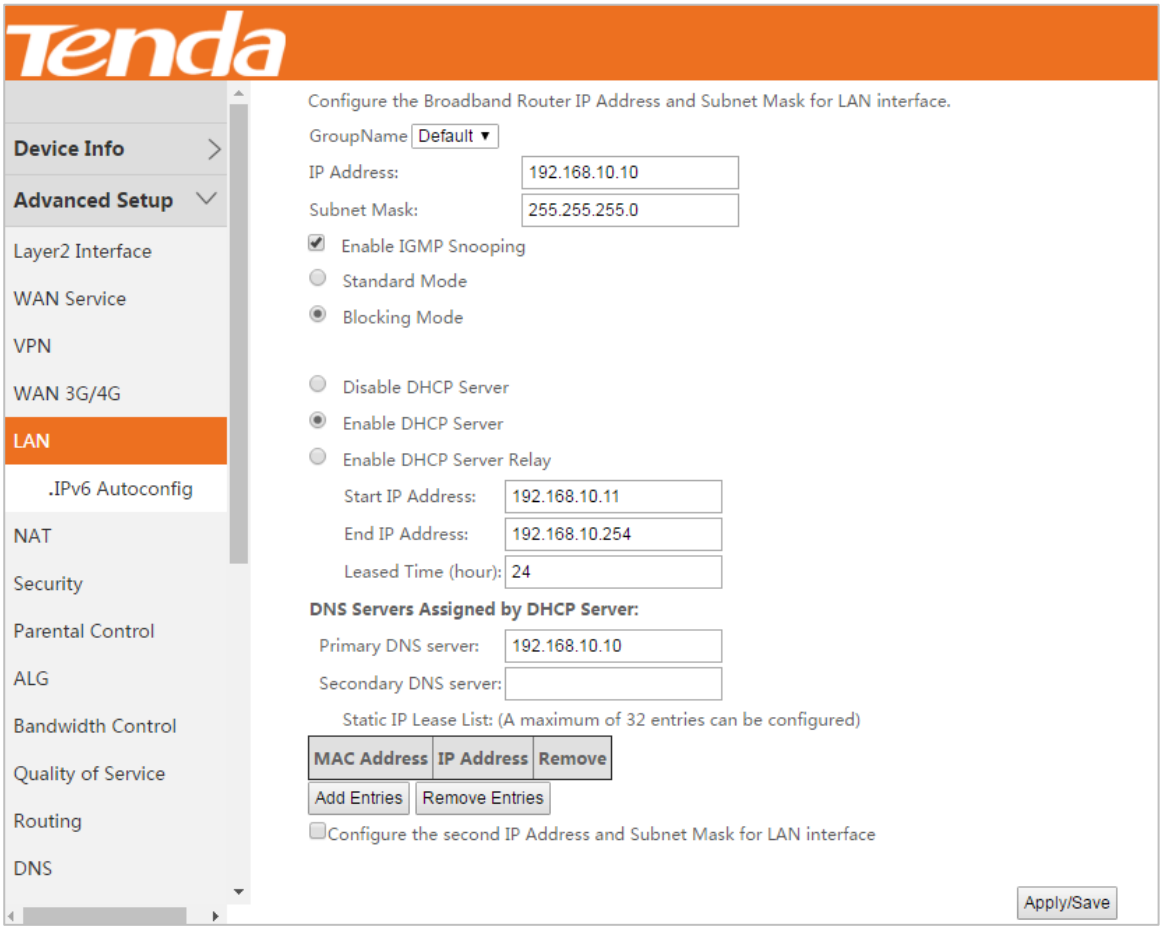



# 4.5 LAN

Here you can configure the LAN IP Address settings. This IP address is to be used to log in to the web UI of the modem router.

## 4.5.1 IPv4

Choose **Advanced** > **Advanced Setup** > **LAN** to enter the configuration page.

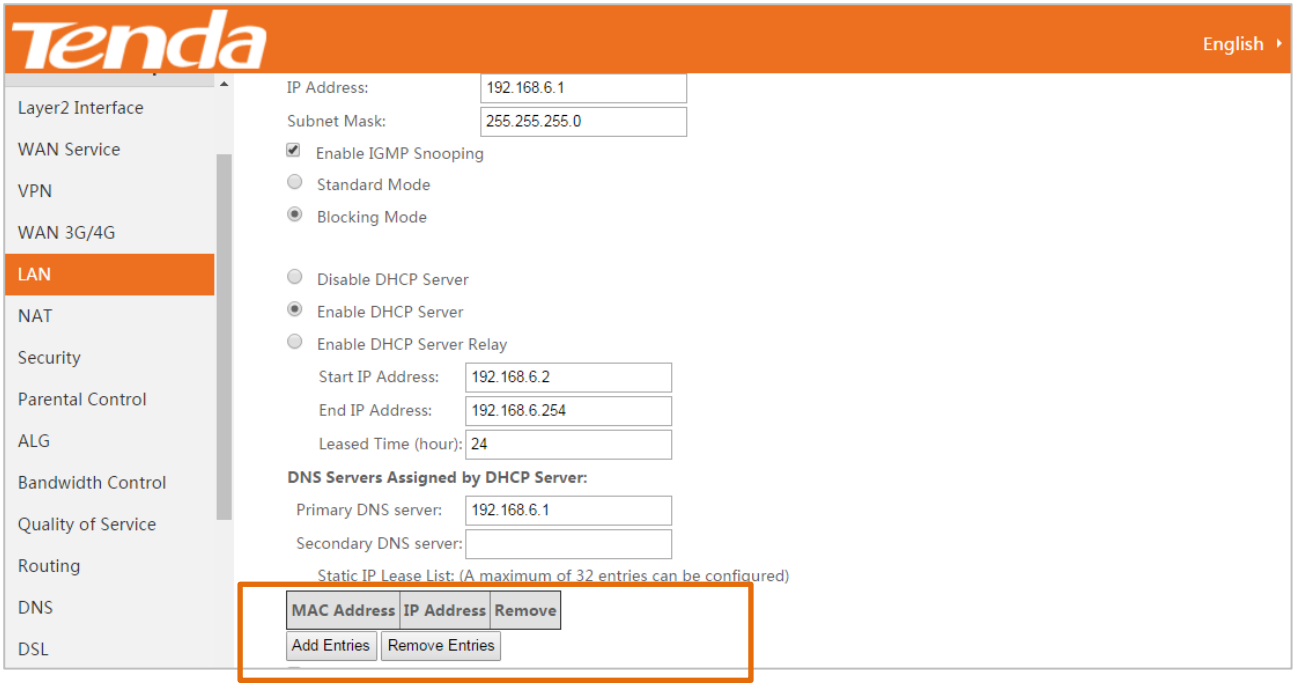


| Parameter | Description |
| --- | --- |
| IP Address | It specifies the LAN IP address of the modem router, that is, the login address of the web UI of the modem router. |
| Subnet Mask | The LAN subnet mask of the modem router. It specifies the network segment of the LAN. |
| Enable IGMP Snooping | Check to enable the IGMP Snooping feature and select either of the following two modes: Standard Mode and Blocking Mode. |
| Disable DHCP Server | It indicates that the modem router won't assign IP addresses to its clients. These devices can access the internet only after IP addresses are manually set on them. Manual IP address setting is complicated and may easily cause IP conflicts. Generally, it is recommended that you enable the DHCP server. |
| Enable DHCP Server | It indicates that the modem router can assign IP addresses to connected devices.<br>Start IP Address: Specify the start IP address of the IP address pool of the DHCP server.<br>End IP Address: Specify the end IP address of the range for the IP address pool of the DHCP server. |
| Primary/Secondary DNS Server | It specifies the primary/secondary DNS IP addresses assigned to connected devices. |
| Leased Time | It specifies the validity period of one IP address assigned to a device by the router. |
| Static IP Lease List | Displays a list of devices with reserved static IP addresses. |
| Add Entries | Click to add a static IP lease entry. A maximum 32 entries can be configured. |
| Remove Entries | Click to remove a static IP lease entry. |
| Configure the second IP Address and Subnet Mask for LAN interface | If you want to configure two IP addresses for the LAN interface, you can check this option and enter the second IP Address and Subnet Mask manually. |
| Apply/Save | After you configure all the needed settings, click this button to apply and save them. |

## DHCP Reservation

Generally, IP addresses assigned by the modem router to devices are changeable. Some functions, such as DMZ Host and virtual server, require static device IP addresses. In this case, you can use the DHCP reservation function to bind IP addresses with the devices involved in the functions.

To configure the DHCP reservation function, choose **Advanced** > **Advanced Setup** > **LAN**. Configure the function as follows.




**Step 1** Click Add Entries.

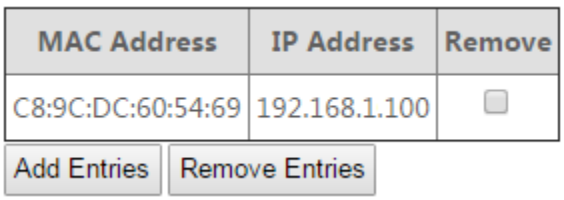
**Step 2** Set **MAC address** to the MAC address of the device.

**Step 3** Set **IP Address** to an IP address in the same segment as the LAN IP address of the modem router, such as any IP address in 192.168.1.3~192.168.1.254. It cannot be the same as the LAN IP address of the modem router. (The default LAN IP address of the modem router is 192.168.1.1.)

**Step 4** Click Apply/Save.

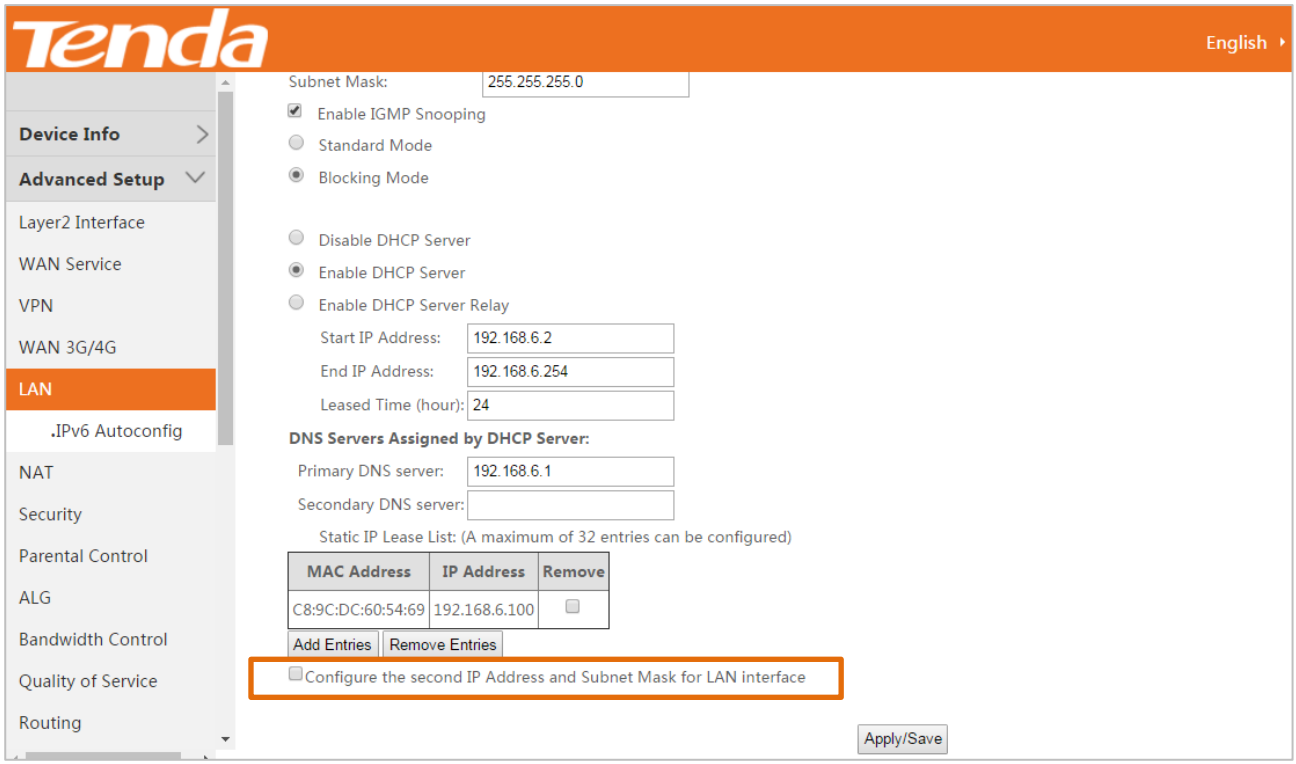

**--End**

The added entry appears in the table.



## To Configure a Second IP Address for LAN Interface

Choose **Advanced** > **Advanced Setup** > **LAN** to enter the configuration page.

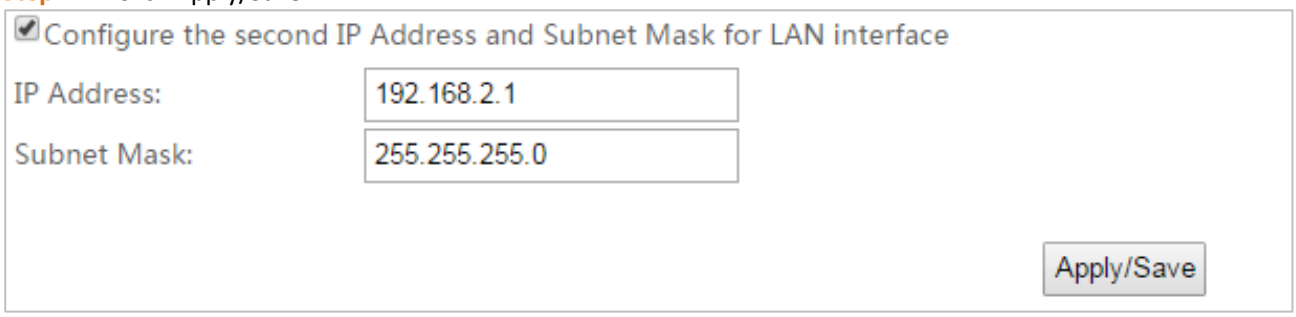



**Step 1** Select the Configure the second IP Address and Subnet Mask for LAN interface option.

**Step 2** Set **IP Address** to another IP address that belongs to another network segment, like **192.168.2.1**.

**Step 3** Set **Subnet Mask** to a subnet mask that fit the network segment, like **255.255.255.0**.

**Step 4** Click Apply/Save.




**--End**

TIP

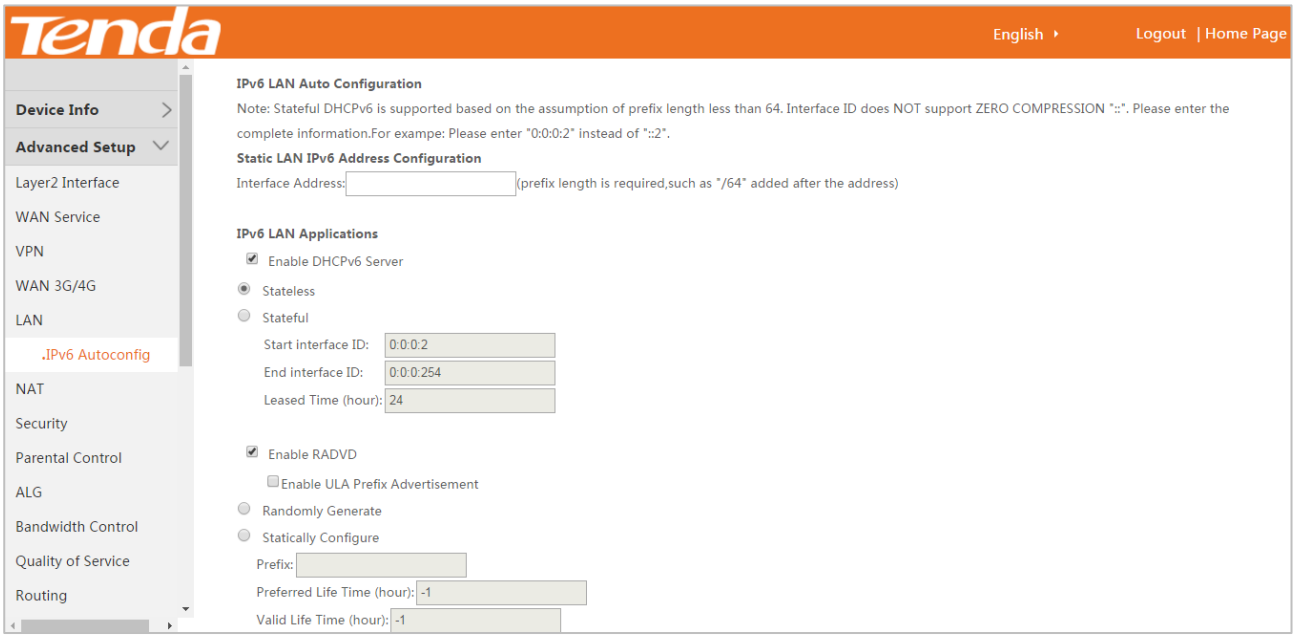
The second LAN IP address can also be used to log in to the web UI of the modem router.

## 4.5.2 IPv6

Choose **Advanced** > **Advanced Setup** > **LAN** > **IPv6config** to enter the configuration page.

NOTE

- IPv6 address can only be Aggregate Global Unicast Address and Unique Local Address. Link-Local Unicast Addresses and Multicast Addresses are not permitted.
- A prefix length must be specified for an IPv6 address.




| Parameter | Description |
|---|---|
| Enable DHCPv6 Server | Check to enable the DHCPv6 Server. |
| Stateless | If selected, IPv6 clients 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 lease time. The router will automatically assign IPv6 addresses to IPv6 clients. |
| 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". |
| Leased Time (hour) | The lease time is the validity period of an IP address assigned to a client. |
| Enable RADVD | The RADVD (Router Advertisement Daemon) implements link-local advertisements of IPv6 router addresses and IPv6 routing prefixes using the Neighbor Discovery Protocol (NDP) and is used by system administrators for stateless auto configuration of network hosts on Internet Protocol version 6 networks. Select the checkbox to enable the RADVD. |
| Enable ULA Prefix Advertisement | If enabled, the router will advertise ULA prefix periodically. |
| Randomly Generate | If selected, address prefix can be automatically generated. |
| Statically Configure | If you select this option, you need to manually configure the address prefix and validity period. |

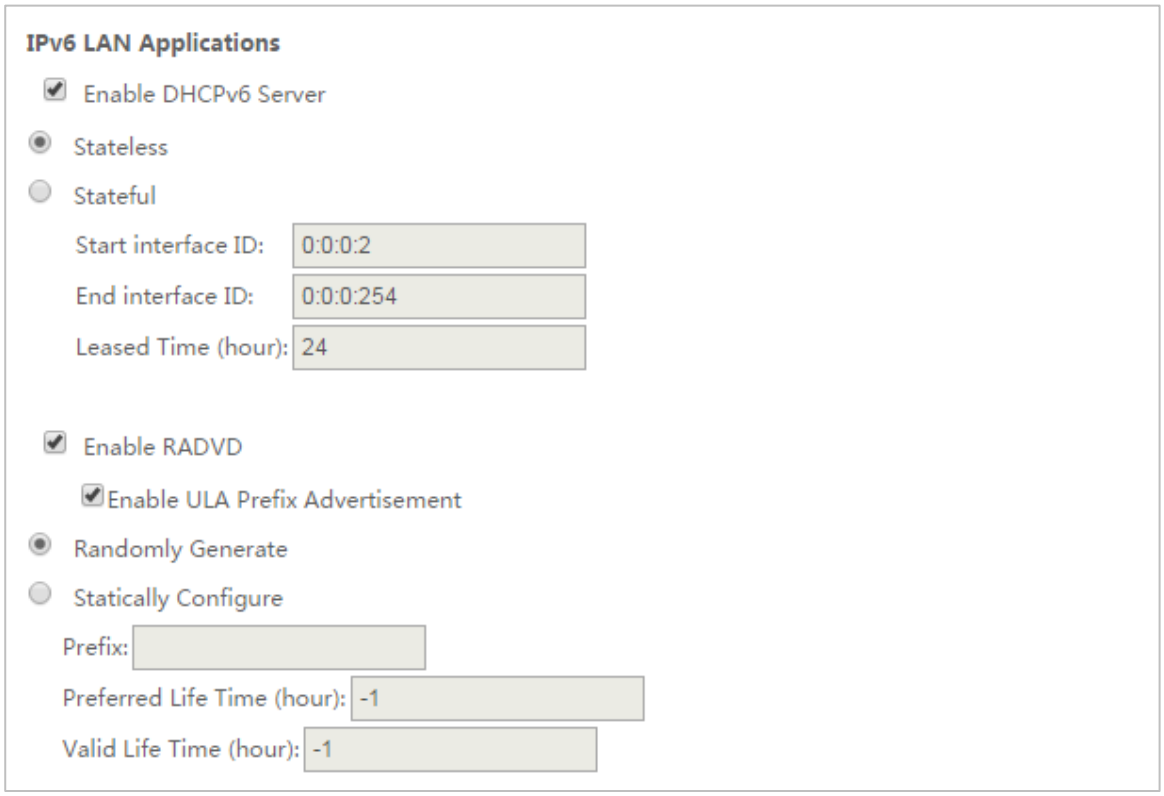
| | |
|---|---|
| Prefix | Specify the prefix. |
| Preferred Life Time (hour) | Specify the preferred life time in hour. When the time is out, the computer can continue to use the address in initiated communications, but cannot use it in new initiated communications. |
| Valid Life Time (hour) | Specify the valid life time in hour. When the time is out, the address is invalid. |
| 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. |

## IPv6 Address Auto Configuration

The Modem router supports two kinds of IPv6 address auto configuration: Stateless Address Auto Configuration and Stateful Address Auto Configuration. Select one to follow according to your needs.

### Stateless Address Auto Configuration

The computers in LAN only obtain prefix and DNS information from the modem router. The interface ID is generated based on its MAC address automatically.




**Procedure**

**Step 1** Select Enable DHCPv6 Server.

**Step 2** Select Stateless.

**Step 3** Select Enable RADVD.

**Step 4** Click Save/Apply.

**--End**

**Parameters Description you may need**:

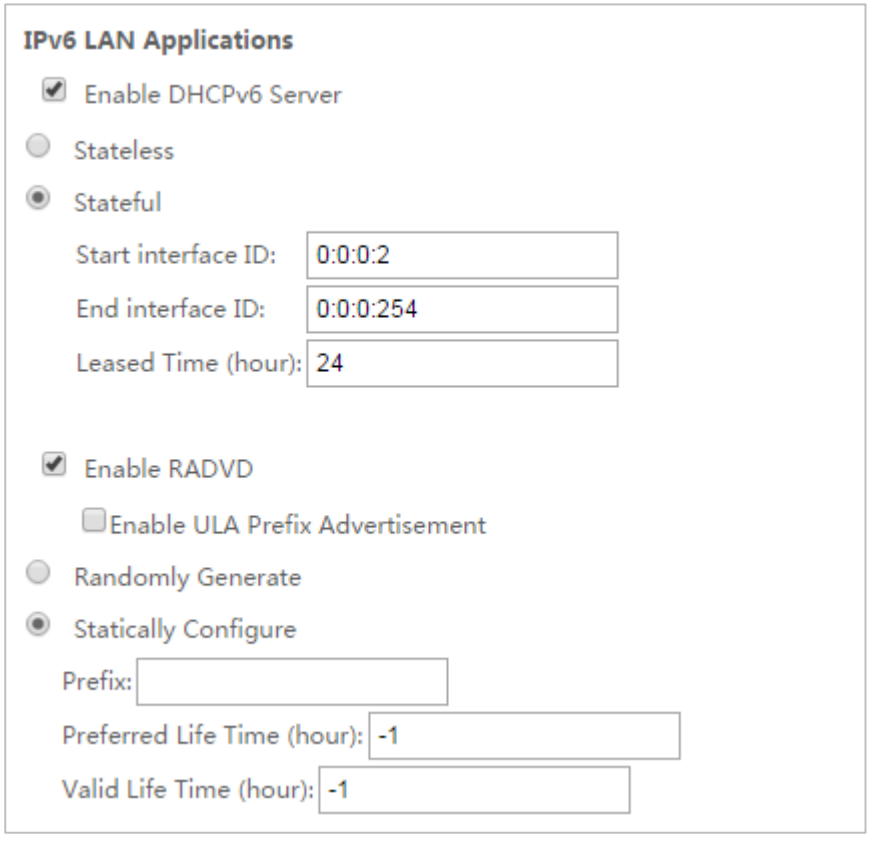
- **Interface ID**: It is equivalent to the host number (host ID) in IPv4 IP address.
- **Prefix**: It is equivalent to the network number in IPv4 IP address.
- **RADVD**:

  **Function 1**: Notice the routes in the network. Let the computers in LAN know that it is a router. When the computer receives the message, it can take it as an alternative route. And then the IP address can be the next hop address when the computer transfers data.

  **Function 2**: Broadcast prefix address. The computers in LAN can generate IPv6 address based on the prefix address.
- **Enable ULA Prefix Advertisement**: If you want the LAN port to distribute the ULA prefix, you can select this option. It is disabled by default. ULA prefix can be generated by the modem router randomly, or be set manually.
- **Prefix Life Time**: The computer retain the obtained prefix, but the retained time based on the following rule:
- **Preferred Life Time (hour)**: When the time is out, the computer can continue to use the address in initiated communications, but cannot use it in new initiated communications.
- **Valid Life Time (hour)**: When the time is out, the address is invalid.

### Stateful Address Auto Configuration

The computers in LAN obtain all IPv6 address information from the modem router.




**Procedure**

**Step 1** Select Enable DHCPv6 Server.

**Step 2** Select **Stateful**.

**Step 3** Start/End interface ID: Specify a start/end interface ID.

**Step 4** Lease Time: Specify the expired time of IPv6 address.

**Step 5** Select Enable RADVD.

**Step 6** Click Save/Apply.

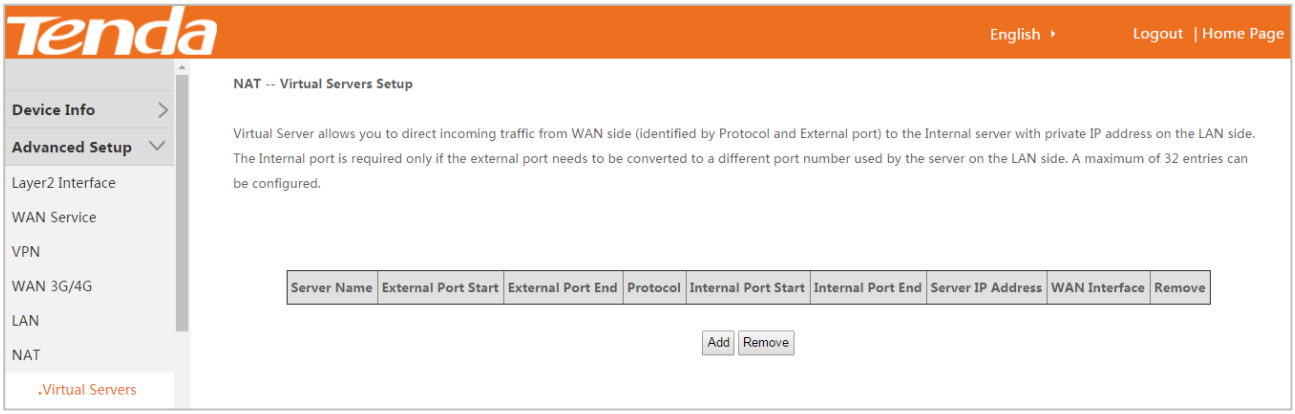
**--End**

# 4.6 NAT

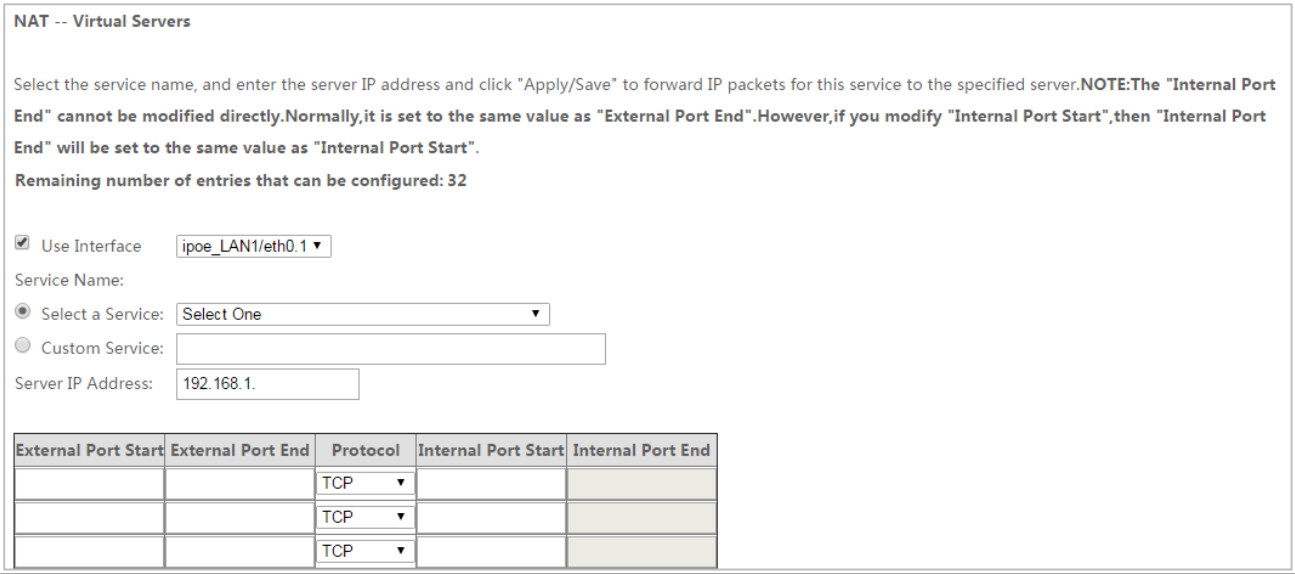
## 4.6.1 Virtual Server

If computers are connected to the modem router to form a LAN and access the internet through the modem router, internet users cannot access the hosts on the LAN. Therefore, the servers, such as web servers, email servers, and FTP servers, on the LAN are inaccessible to internet users. To enable internet users to access a LAN server, enable the virtual server function of the modem router, and map one service port of the virtual server to the IP address of the LAN server. This enables the modem router to forward the requests arriving at the port from the internet to the LAN server.

Choose **Advanced**> **Advanced Setup** > **NAT** > **Virtual Server** to enter the configuration page.




Click **Add** to configure the function.




| Parameter | Description |
|---|---|
| Use Interface | Select a WAN connection to which you wish to apply the rules. When there is only one WAN connection available, the rules will be automatically applied to it. |
| Service Name | Select a Service: Allows you to select an existing service from the drop-down list.<br>Custom Service: Allows you to customize a service. |
| Server IP Address | Enter the IP address of your local computer that will provide this service. |
| External Port Start and External Port End | These are the start number and end number for the public ports at the internet interface. |
| Protocol | Select a protocol from the Protocol drop-down list. If you are unsure, select TCP/UDP. |
| Internal Port Start and Internal Port End | These are the start number and end number for the ports of a computer on the LAN of the router. |

**Application Example**

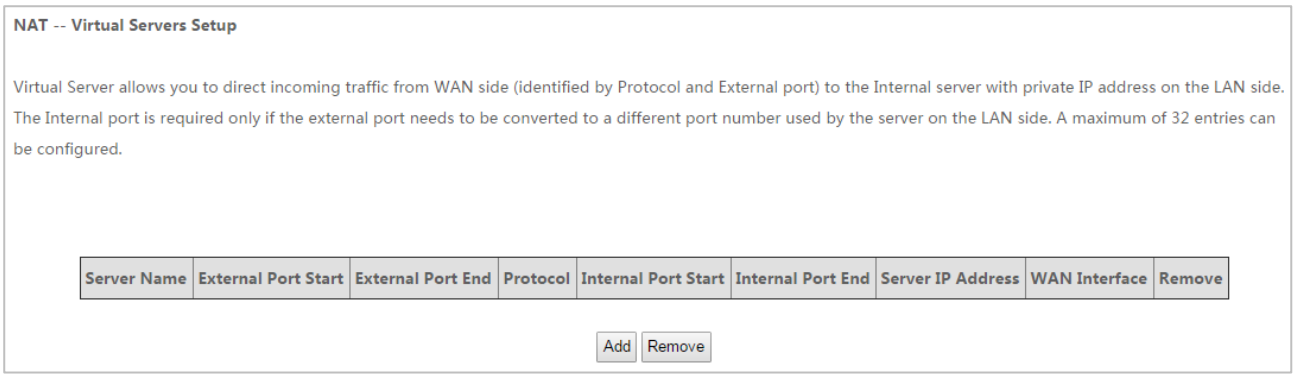
You have set up an FTP server on your LAN:

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

And want your friends to access the FTP server on default port over the internet. To access your FTP server from the Internet, a remote user has to know the Internet IP address or domain name of the modem router, such as *www.tendacn.com*. In this example, we assume the internet IP address of your router is *183.37.227.201*. Follow instructions below:

**To configure the router to make your local FTP server accessible over the internet**:

Choose **Advanced** > **Advanced Setup** > **NAT** > **Virtual Server** to enter the configuration page.




**Step 1** Click **Add**.

**Step 2** Select **FTP Server** from the **Select a Service** drop-down list. The port number (21) used by this service will then be automatically populated.

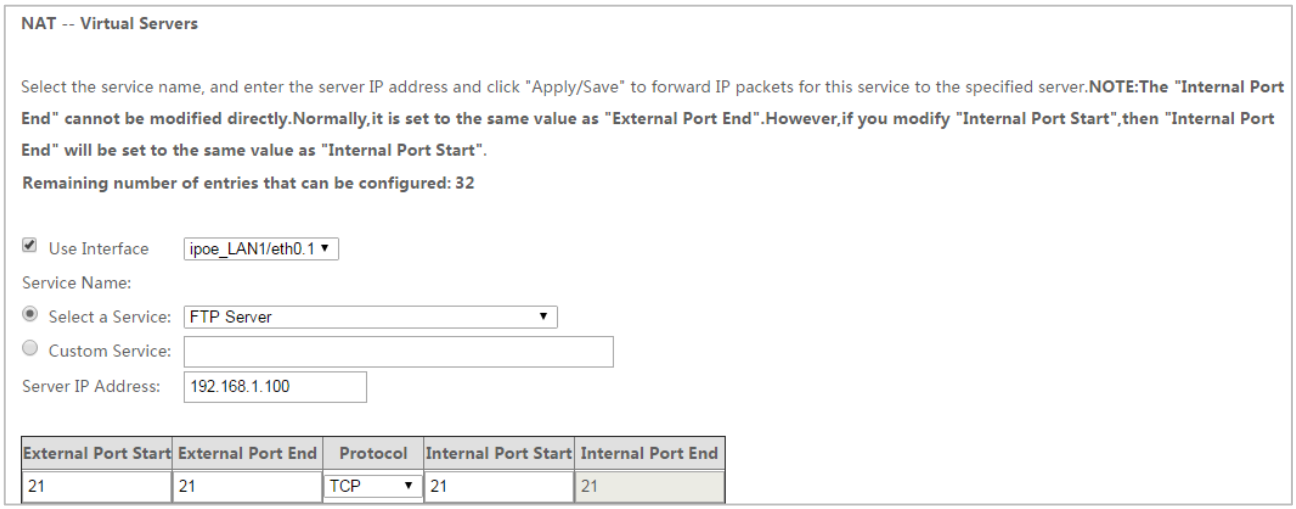
**Step 3** If you want to define the service yourself, enter a descriptive name in the Custom Service, such as My FTP, and then manually set the port number (21) used by this service in the **Internal Port Start**, **Internal Port End**, **External Port Start** and **External Port End**.

**Step 4** Select a protocol from the **Protocol** drop-down list. If you are unsure about which protocol is required, select **TCP/UDP**.

**Step 5** In the **Server IP Address** field, enter the IP address of your local computer that offers this service. Here in this example, we enter *192.168.1.100*.

**Step 6** Click the **Apply/Save**.

**Step 7**




**--End**

**Remote Access**:

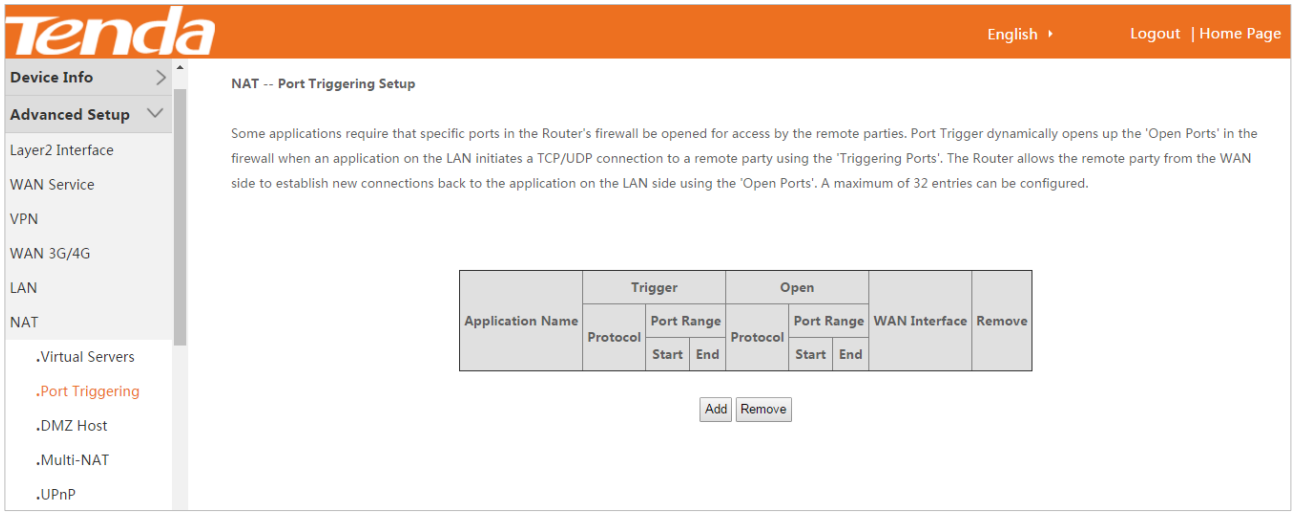
Your friends can access your FTP server by entering "*ftp://183.37.227.201:21*" in the address bar of a web browser.

## 4.6.2 Port Triggering

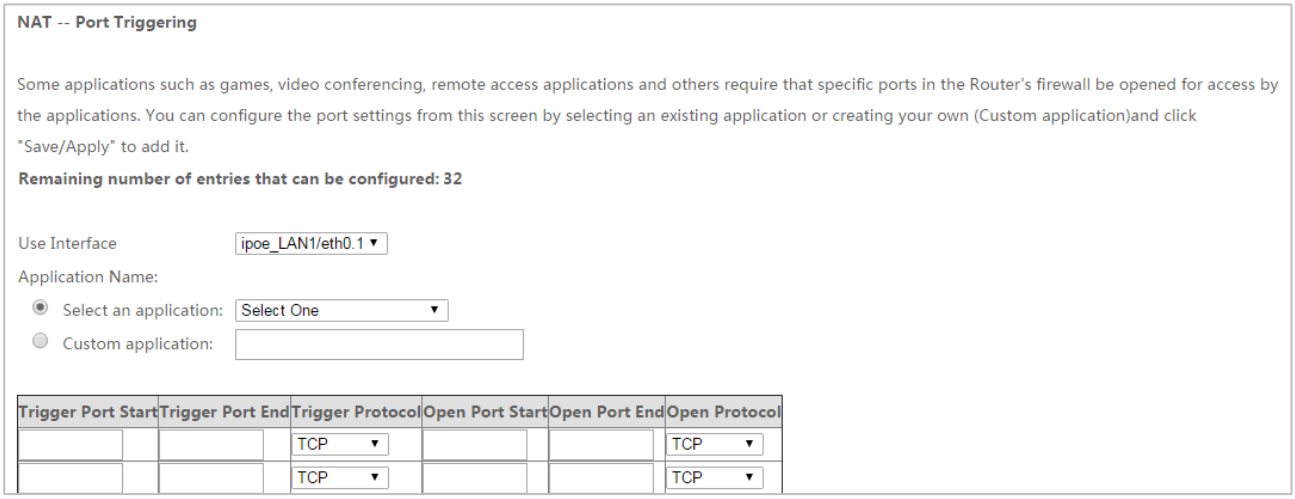
Some applications, such as games, video conferencing, and remote access, require that specific ports in the router's firewall be opened for access by the applications. Port triggering opens an incoming port when the user's computer is using a specified outgoing port for specific traffic. This allows computers behind a NAT-enabled router on a local network to provide services. Port triggering triggers can open an incoming port

when a client on the local network makes an outgoing connection on a predetermined port or range of ports.

Choose **Advanced**> **Advanced Setup** > **NAT** > **Port Triggering** to enter the configuration page.




Click **Add** and configure the function.

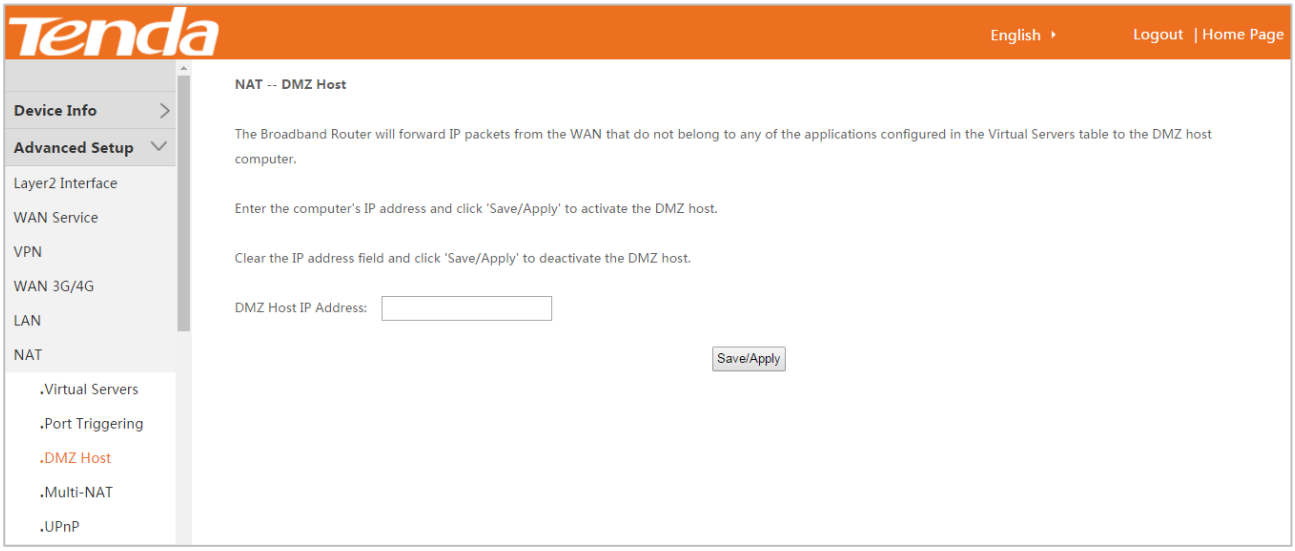



| Parameter | Description |
|---|---|
| Use Interface | Select a WAN connection to which you wish to apply the rules. When there is only one WAN connection available, the rules will be automatically applied to it. |
| Application Name | Select an application: Allows you to select an existing service from the drop-down list.<br>Custom application: Allows you to customize a service. |
| Trigger Port Start/Trigger Port End | The port range for an application to initiate connections. |
| Trigger Protocol | Select the protocol from the drop-down list. If you are unsure, select TCP/UDP. |
| Open Port Start/ Open Port End | These are the starting number and ending number for the ports that will be automatically opened by the built-in firewall when connections initiated by an application are established. |

## 4.6.3 DMZ Host

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

Choose **Advanced**> **Advanced Setup** > **NAT** > **DMZ Host** to enter the configuration page.




**DMZ Host IP Address**: The IP Address of the device for which the firewall of the modem router is disabled. Ensure that the IP address is a static IP address. The DMZ host should be connected to a LAN port of the modem router.

NOTE

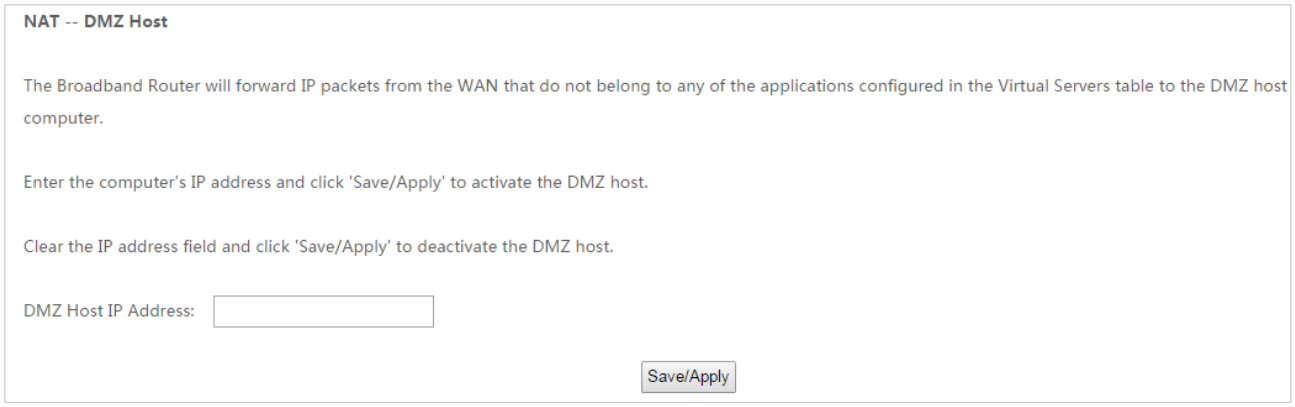
- A DMZ host is not protected by the firewall of the router. A hacker may leverage the DMZ host to attack your LAN. Therefore, enable the DMZ function only when necessary.
- Manually set the IP address of the LAN computer that functions as a DMZ host, to prevent IP address changes, which lead to DMZ function failures.
- Security software, antivirus software, and the built-in OS firewall of the computer may cause DMZ function failures. Disable them when using the DMZ function. If the DMZ function is not required, it is recommended that you disable it and enable your firewall, security, and antivirus software.

To configure the DMZ function, perform the following procedure:

**Step 1** Click **Add**.

**Step 2** Set **DMZ Host IP Address** to the IP address of the DMZ host.

**Step 3** Click **Save/Apply**.



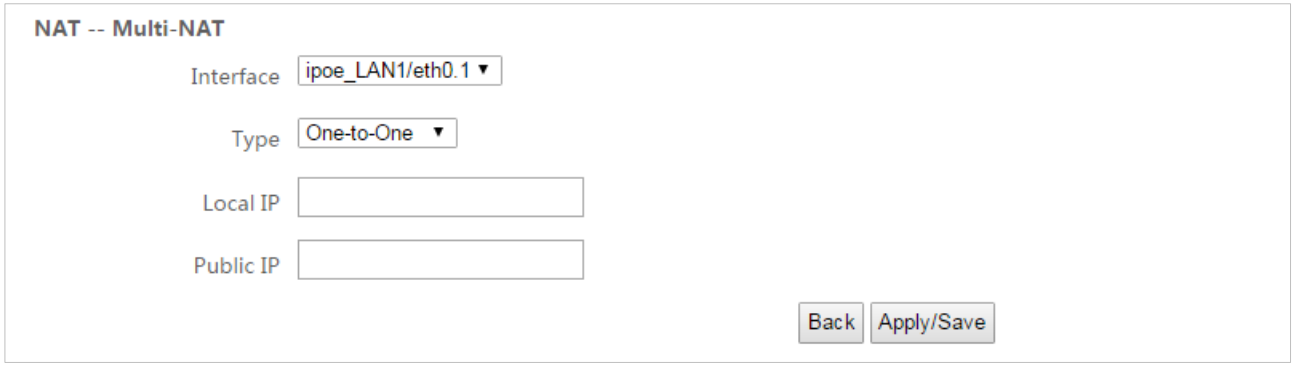

**--End**

## 4.6.4 Multi-NAT

Multi-NAT is a network function whereby one network address is rewritten (translated) to another address: Network Address Translation is frequently used to allow multiple network nodes (computers or inter-networked devices) to share a single public (or local network) IP address. Multi-NAT can work in one-to-one or many-to-one mode.

Choose **Advanced**> **Advanced Setup** > **NAT** > **Multi-NAT** to enter the configuration page.


Click **Add** to configure the function.



| Parameter | Description |
| --- | --- |
| Interface | Select a WAN interface that the function uses. |
| Type | One-to-One: Set a route from a local IP address to a public IP address<br>Many-to-One: Set a route from many local IP addresses to a public IP address |
| Local IP | Specify a local IP address |
| Local Start/End IP | Specify a local IP address range |
| Public IP | Specify a public IP address |

To configure the Multi-NAT function, perform the following procedure:

**Step 1** Click **Add**.

**Step 2** Select an interface from the drop-down list.

**Step 3** Select a type. If you only need to set a route for a local IP address, select **One-to-One**. Otherwise, select **Many-to-One**.

**Step 4** Set **Local IP** to a local IP address.

**Step 5** Set **Public IP** to a public IP address.

**Step 6** Click Apply/Save.

**--End**

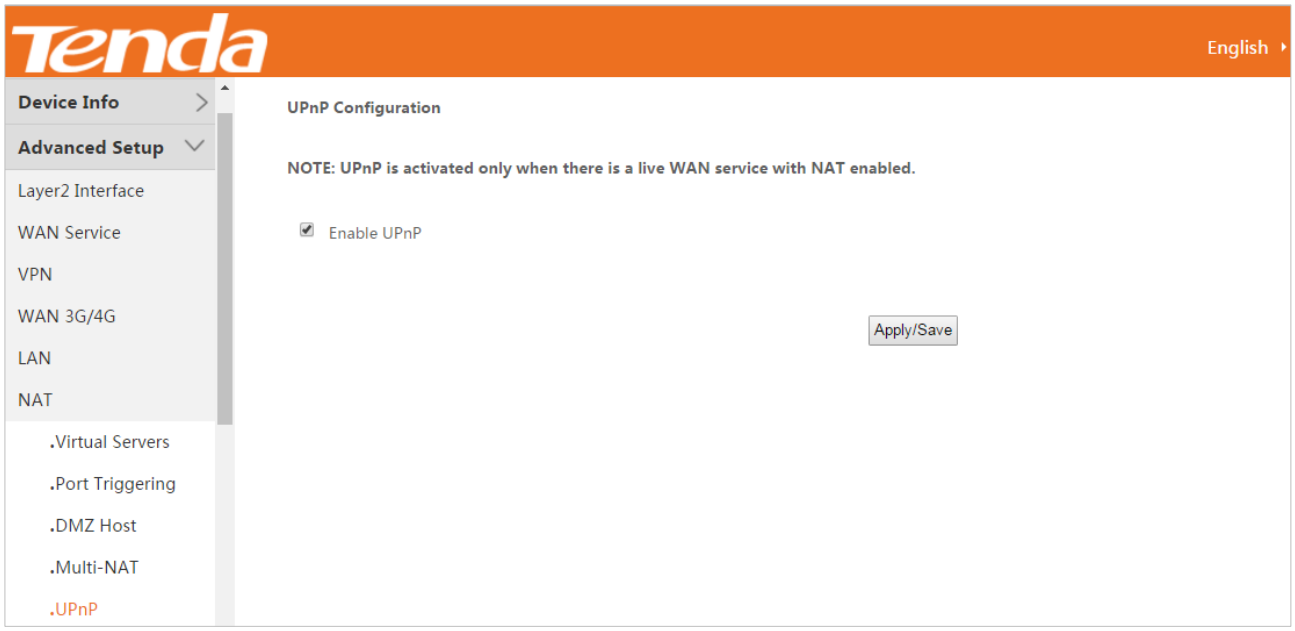
TIP

The local IP and Public IP you set should be static IP addresses.

## 4.6.5 UPnP

This function enables the modem router to map ports. It can enhance user experience especially during online gaming and P2P download.

Choose **Advanced**> **Advanced Setup** > **NAT** > **UPnP** to enter the configuration page.

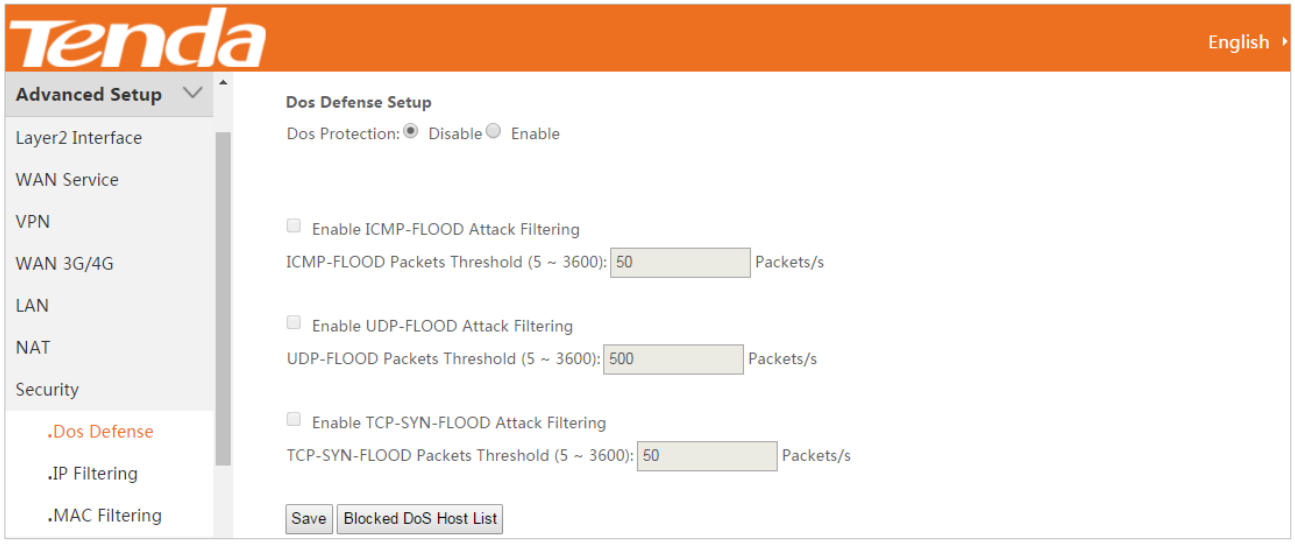



# 4.7 Security

## 4.7.1 DoS Defence

This function allows you to enable ICMP-FLOOD Attack Filtering, UDP-FLOOD Attack Filtering, and TCP-SYN-FLOOD Attack Filtering to defend the modem router against ICMP-FLOOD attack, UDP-FLOOD attack, and TCP-SYN-FLOOD attacks.

Choose **Advanced**> **Advanced Setup** > **Security** > **Dos Defense** to enter the configuration page.




To enable the Dos Defense function, perform the following procedure:

**Step 1** Select the **Enable** option of Dos Protection.

**Step 2** Select the corresponding attack filtering.

**Step 3** Click **Save**.

**--End**

Clicking **Blocked DoS Host List** can check the attacks the modem router blocks.

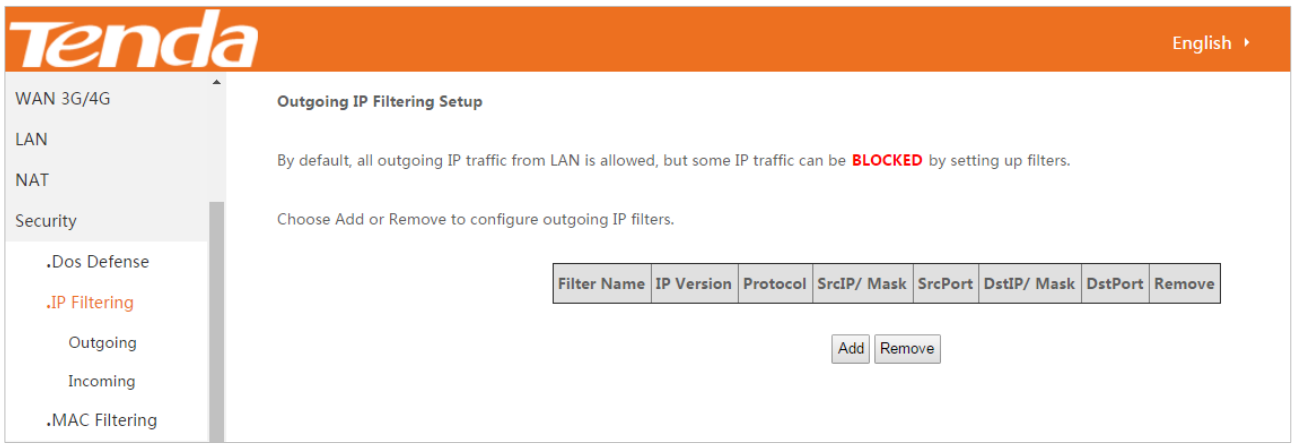
## 4.7.2 IP Filtering

This function can forbid the LAN devices to access the internet or allow WAN devices to visit the LAN devices.

### Outgoing

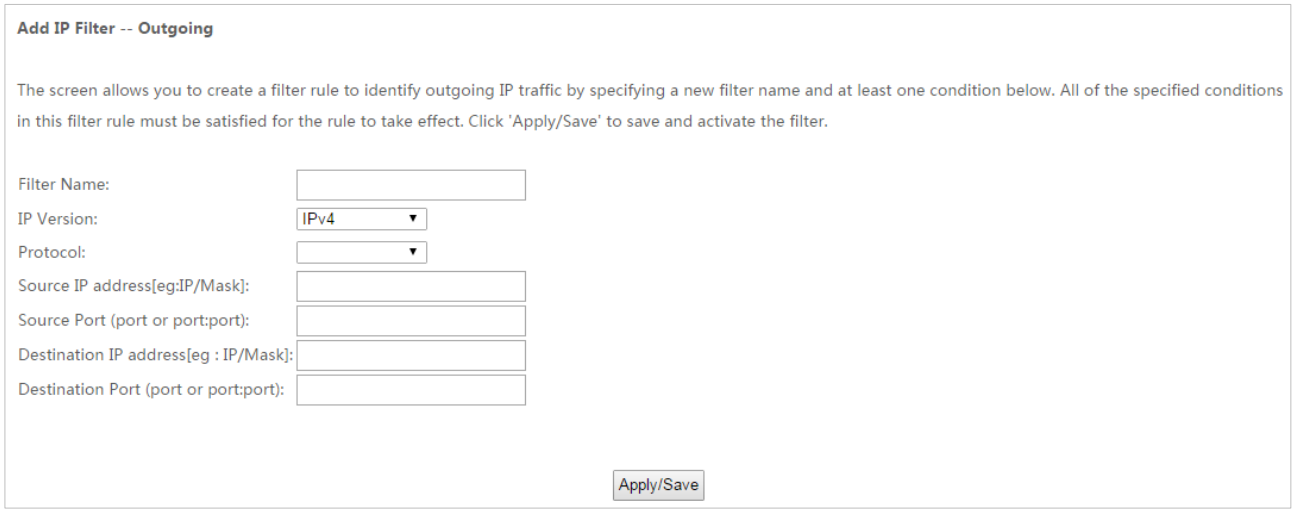
By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be BLOCKED by setting up filters. Outgoing IP Filtering function allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition.

Choose **Advanced**> **Advanced Setup** > **Security** > **IP Filtering** > **Outgoing** to enter the configuration page.




To configure the Outgoing IP Filtering function, perform the following procedure:

**Step 1** Click **Add**.




**Step 2** **Filter Name:** Enter a descriptive filtering name.

**Step 3** **IP Version:** Select your IP protocol which can be IPv4 or IPv6.

**Step 4** **Protocol:** Select a protocol for the filter rule.

**Step 5** **Source IP address [eg: IP/Mask]:** Enter the LAN IP address to be filtered.

**Step 6** **Source Port (port or port: port):** Specify a port number or a port range used by LAN PCs to access the internet. If you are not sure, leave it blank.

**Step 7** **Destination IP address [eg: IP/Mask]:** Specify the external network IP address to be accessed by specified LAN PCs.

**Step 8** **Destination Port** (port or port:port)**:** Specify a port number or a port range that the internet service you restrict uses.

**Step 9** Click Apply/Save.

**--End**

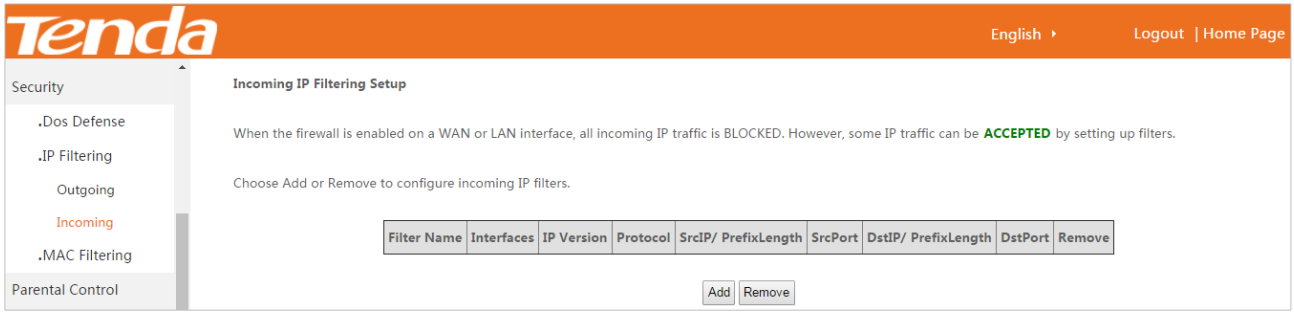
TIP

Source/destination port is for TCP/UDP protocol. If protocol ICMP is selected, do not need to enter the port information. Since the source port of the data packet is changeable, you'd better set the port to "1:65535" or leave them blank.

## Incoming

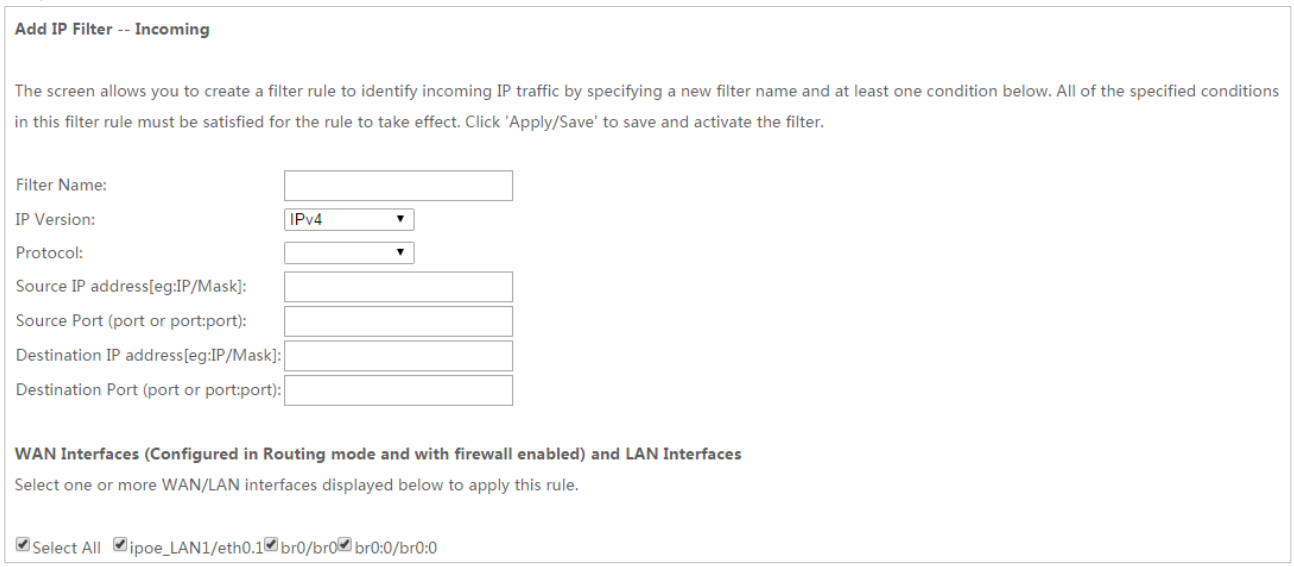
When the firewall is enabled on a WAN or LAN interface, all incoming IP traffic is BLOCKED. However, some IP traffic can be ACCEPTED by setting up filters. The Incoming IP Filtering function allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition.

Choose **Advanced**> **Advanced Setup** > **Security** > **IP Filtering** > **Incoming** to enter the configuration page.




To configure the Ingoing IP Filtering function, perform the following procedure:

**Step 1** Click **Add**.




**Step 2** **Filter Name:** Enter a descriptive filtering name.

**Step 3** **IP Version:** Select your IP protocol which can be IPv4 or IPv6.

**Step 4** **Protocol:** Select a protocol for the filter rule.

**Step 5** **Source IP address [eg: IP/Mask]:** Enter the internal IP address [eg: IP/Mask] to be filtered.

**Step 6** **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.

**Step 7** **Destination IP address [eg: IP/Mask]:** Specify the internal network IP address [eg: IP/Mask] to be accessed by the specified PCs from external network.

**Step 8** **Destination Port** (port or port:port)**:** Specify a port number or a port range that the internet service you restrict uses..

**Step 9** Click Apply/Save.

**--End**

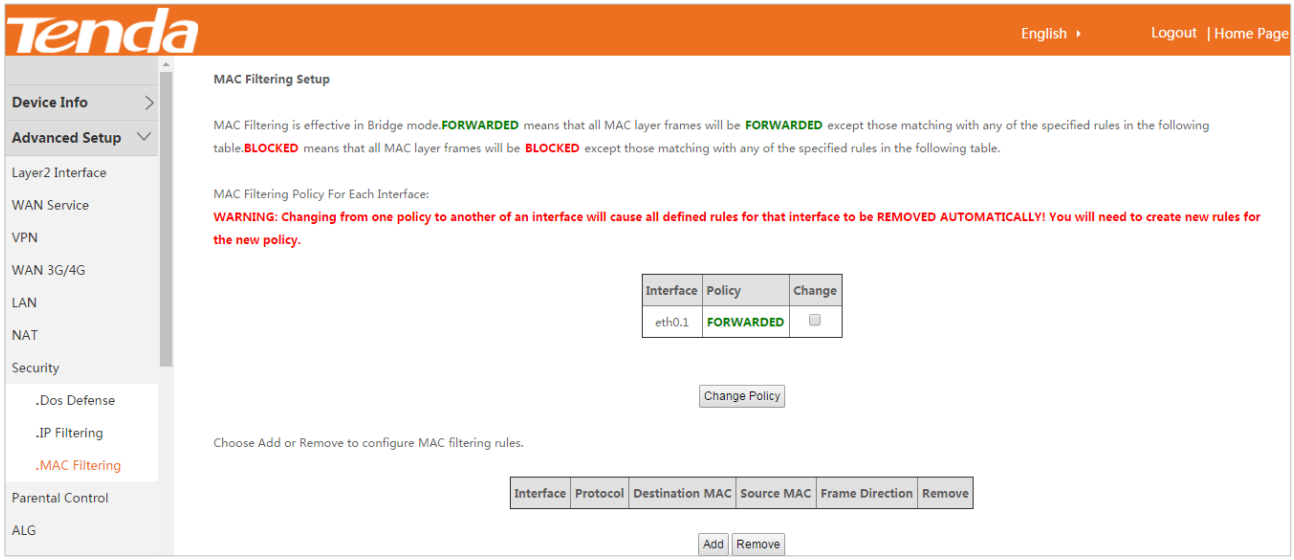
## 4.7.3 MAC Filtering

The MAC filtering is effective only when you set the WAN service to bridging. There are two policies of the function:

FORWARDED indicates that all MAC layer frames will be FORWARDED except those matching the rules you specify.

BLOCKED indicates that all MAC layer frames will be BLOCKED except those matching the rules you specify.

Choose **Advanced**> **Advanced Setup** > **Security** > **MAC Filtering** to enter the configuration page.




To add a frame forwarding rule, perform the following procedure:

**Step 1** Click **Add**.

**Step 2** **Protocol Type:** Select a protocol type from the drop-down list.

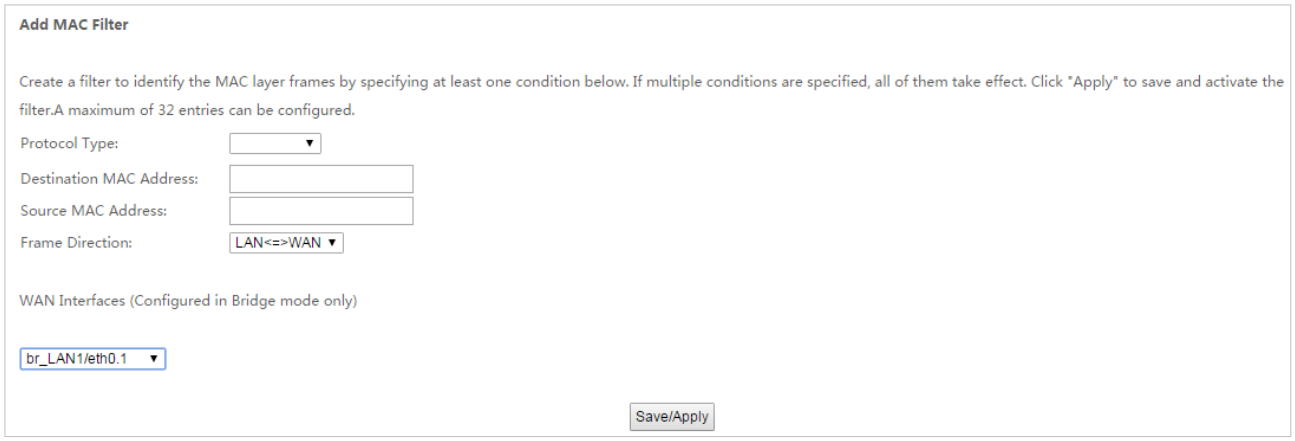
**Step 3** **Destination MAC Address:** Enter the destination MAC address to which you want to apply the MAC filtering rule.

**Step 4** **Source MAC Address:** Enter the source MAC address to which you want to apply the MAC filtering rule.

**Step 5** **Frame Direction:** Select a frame direction from the drop-down list.

**Step 6** **WAN Interfaces:** Select a WAN interface from the drop-down list.

**Step 7** Click Save/Apply.

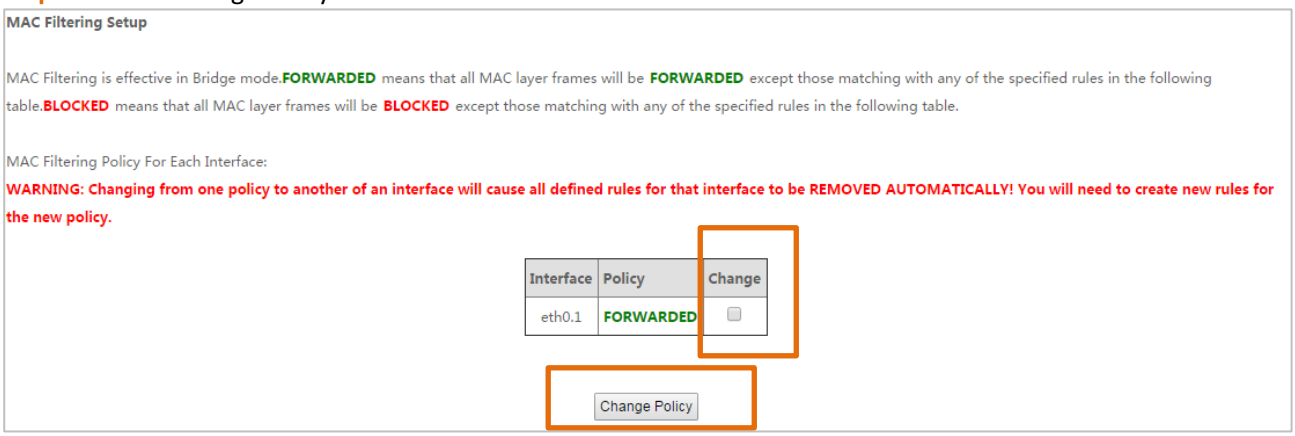



**--End**

To change the policy from FORWARDED to BLOCKED, perform the following procedure:

**Step 1** Select **Change** checkbox.

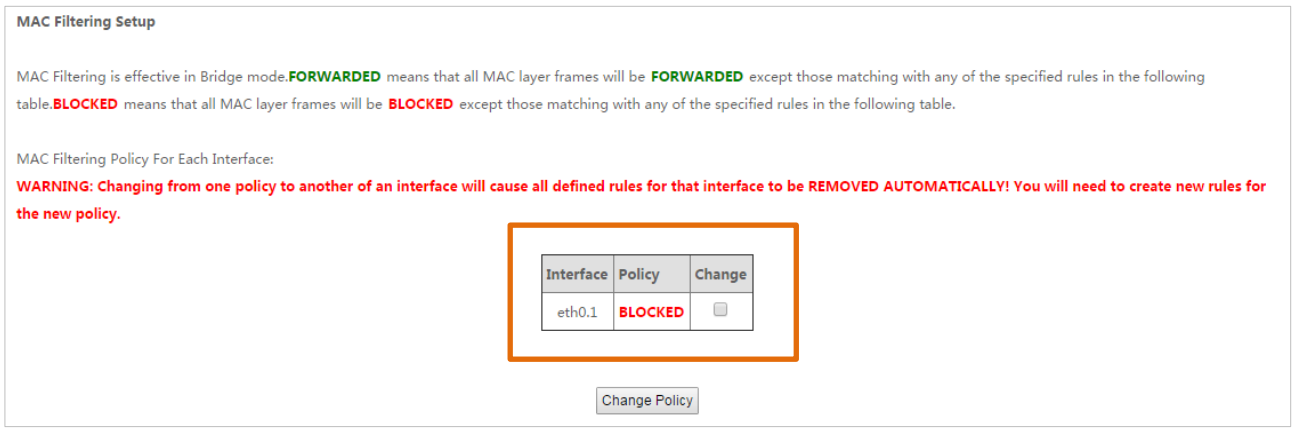
**Step 2** Click Change Policy.




**--End**

**Verification**

The policy is change to **BLOCKED**.



To add a frame blocking rule, perform the following procedure:

**Step 1** Change the policy to **BLOCKED**. Refer to "To change the policy from FORWARDED to BLOCKED".

**Step 2** Click **Add**.

**Step 3** **Protocol Type:** Select a protocol type from the drop-down list.

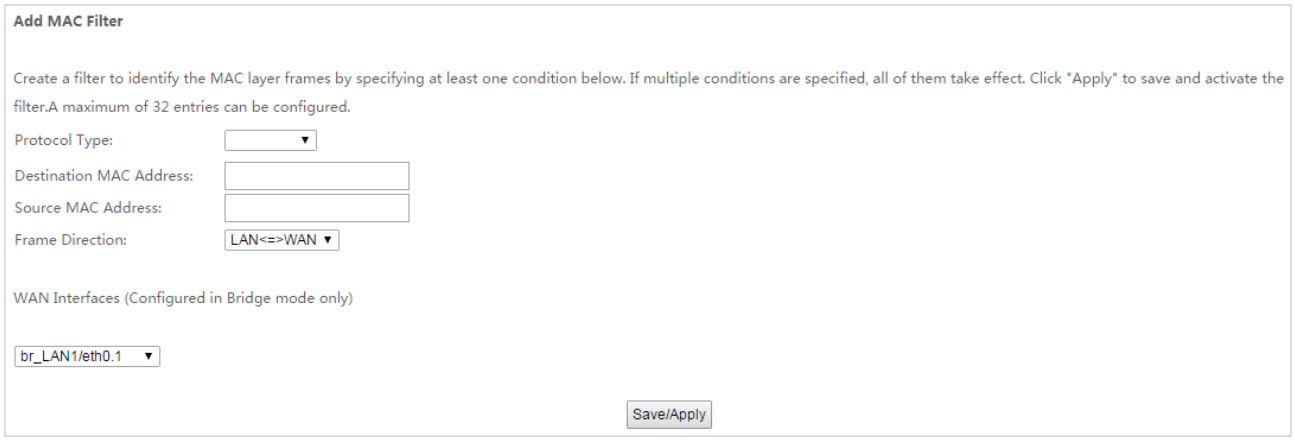
**Step 4** **Destination MAC Address:** Enter the destination MAC address apply the MAC filtering rule to which you want to apply the MAC filtering rule.

**Step 5** **Source MAC Address:** Enter the source MAC address to which you want to apply the MAC filtering rule.

**Step 6** **Frame Direction:** Select a frame direction from the drop-down list.

**Step 7** **WAN Interfaces:** Select a WAN interface from the drop-down list.

**Step 8** Click Save/Apply.




**--End**

# 4.8 Parental Control

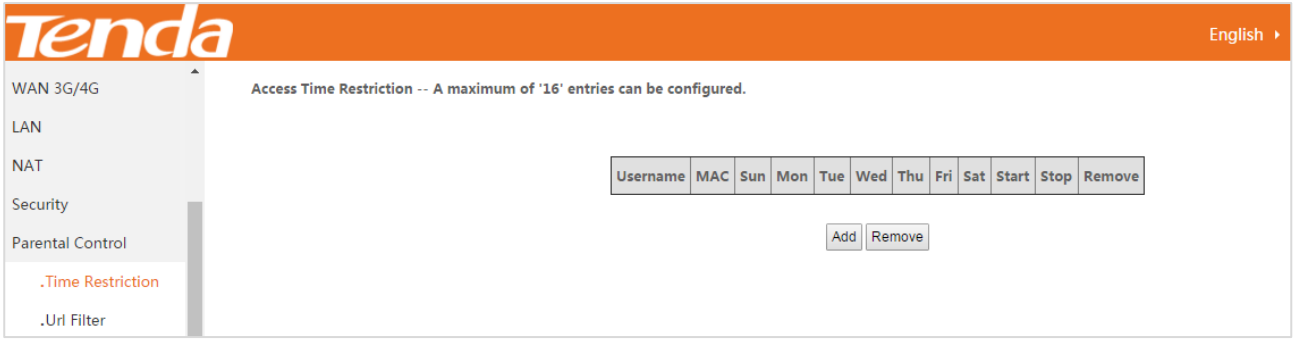
This function enables you to control internet connectivity availability and content accessibility for devices connected to the router.

## 4.8.1 Time Restriction

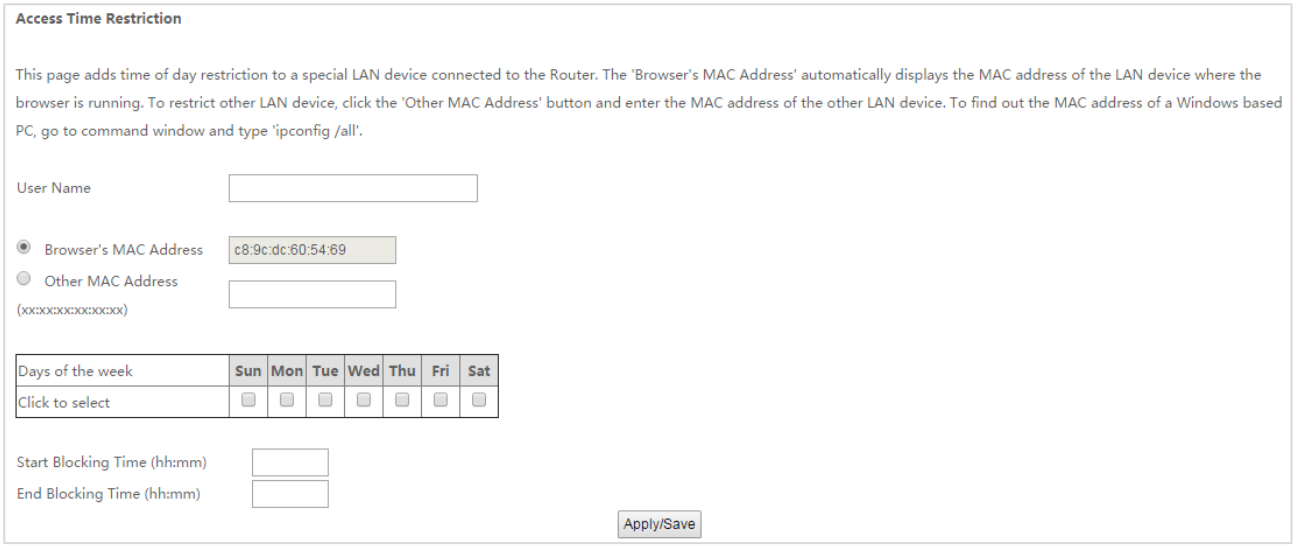
Time Restriction allows you to forbid a LAN device to access the internet during the specified time.

To add a time restriction rule, perform the following procedure:

Choose **Advanced** >**Advanced Setup** > **Parental Control** >**Time Restriction** to enter the configuration page.




**Step 1** Click **Add**.




**Step 2** **User Name**: Specify a user name for this rule. It must be 1-32 characters, and space is not allowed.

**Step 3** Select **Browser's MAC Address** if the rule is applied to the computer where the browser is running. If not, select Other MAC Address, and enter the MAC address of a computer to which the rule is applied.

**Step 4** **Days of week**: Click to select the days of week during which the rule takes effect.

**Step 5** **Start Blocking Time/End Blocking Time**: Specify time of day restriction for the rule. Within this specified period of the day, this LAN device cannot access the internet. For example, if you set **start Blocking Time** to *23:00*, and **End Blocking Time** to *06:00*, the device to which this rule is applied cannot access the internet during 23:00~06:00.

**Step 6** Click Apply/Save.

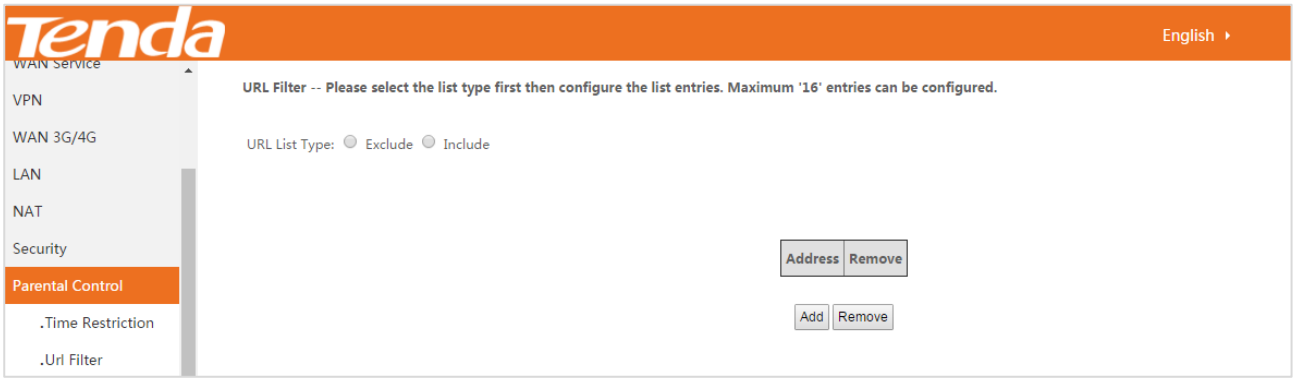
**--End**

## 4.8.2 URL Filter

URL Filter allows you to specify URLs can or cannot be accessed.

To add a URL Filter rule, perform the following procedure:

Choose **Advanced** >**Advanced Setup** > **Parental Control** >**URL Filter** to enter the configuration page.



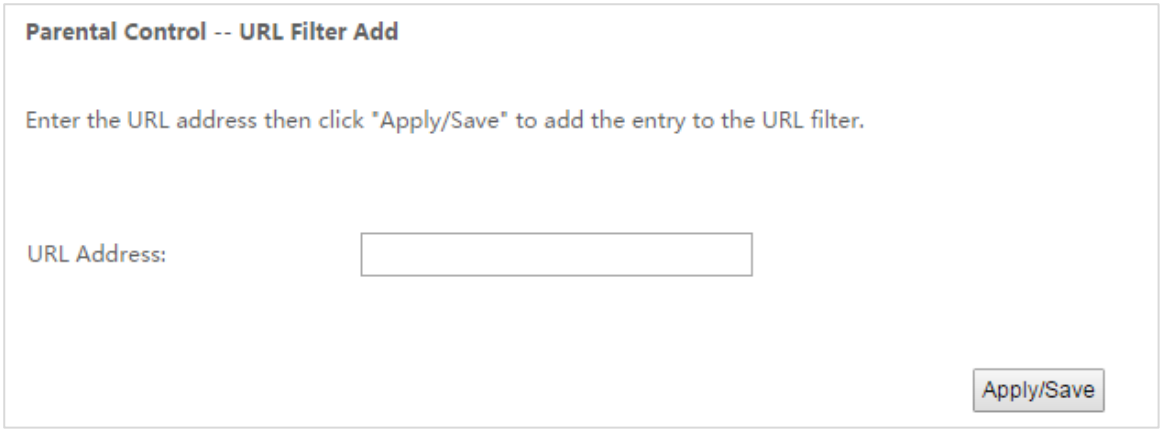

**Step 1** Select Exclude or Include.

- **Exclude** indicates that the URLs added to the list cannot be accessed.
- **Include** indicates that only the URLs added to the list can be accessed.

**Step 2** Click **Add**.

**Step 3** Enter a URL. For example, Set **URL Address** to ***www.google.com***.

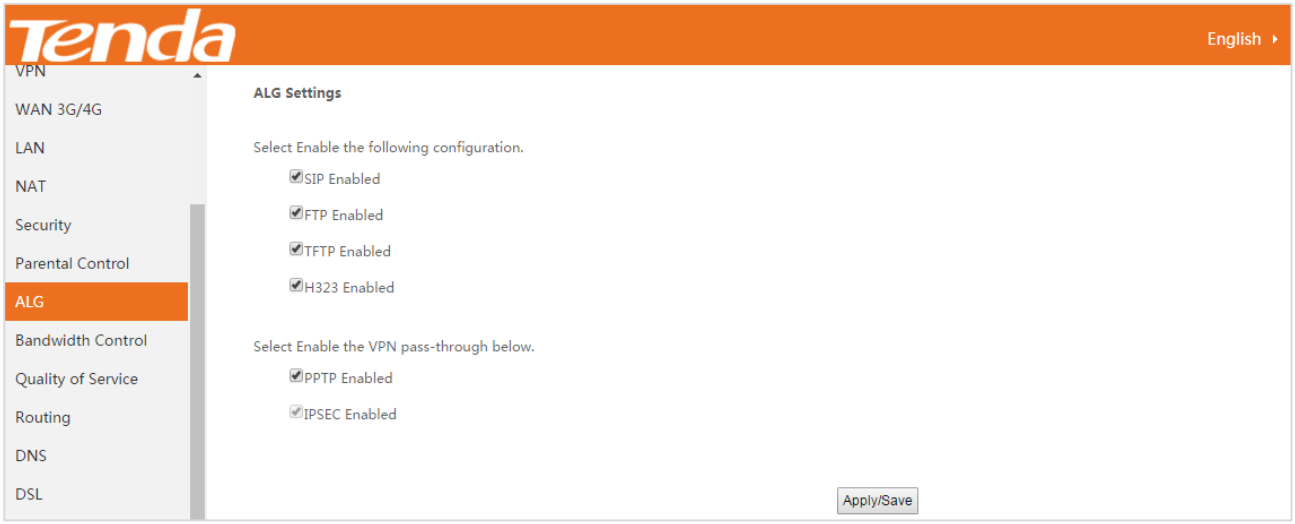
**Step 4** Click Apply/Save.




**--End**

# 4.9 ALG

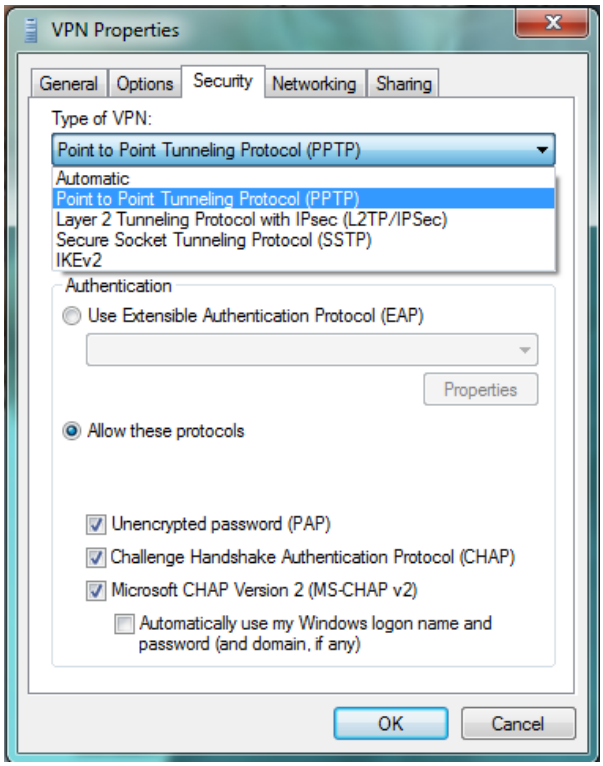
ALG allows you to enable SIP, FTP, TFTP, H323 functions, and VPN pass through.




| Parameter | Description |
|---|---|
| SIP Enabled | The IP phone function can be used on the computers connected to the modem router only when the checkbox is selected. |
| FTP Enabled | The users on LAN can share resources on the FTP server on WAN only when the checkbox is selected. |
| TFTP Enabled | The users on LAN can share resources on the TFTP server on WAN only when the checkbox is selected. |
| H323 Enabled | The IP phone and network conference function can be used on the computers connected to the modem router only when the checkbox is selected. |

**VPN pass-through**

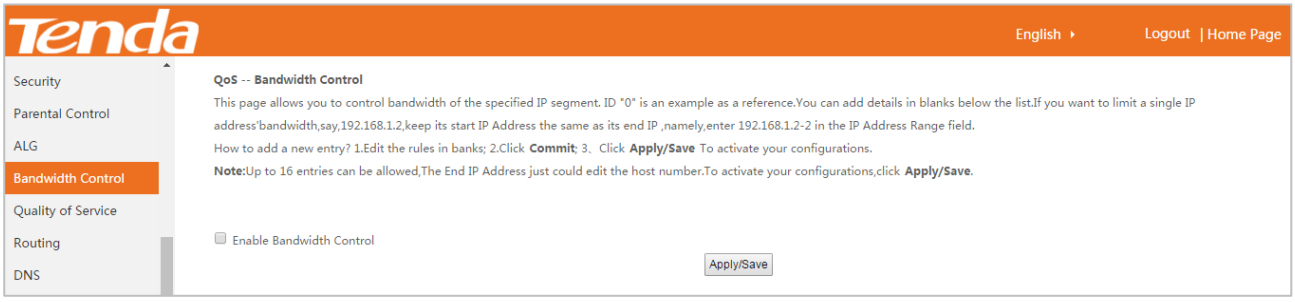
- **PPTP Enabled**: If you select PPTP protocol when you create a VPN connection on your computer, it takes effect only when this checkbox is selected.
- **IPSEC Enabled**: If you select IPSEC protocol when you create a VPN connection on your computer, it takes effect only when this checkbox is selected.




# 4.10 Bandwidth Conrtol

If multiple devices access the internet through the modem router, bandwidth control is recommended, so that high-speed file download by a device does not reduce the internet access speed of the other devices.

Choose **Advanced** > **Advanced Setup** > **Bandwidth Control** to enter the configuration page.




To add a bandwidth control rule, perform the following procedure:

**Step 1** Select Enable Bandwidth Control.

**Step 2** Specify a name for the rule.

**Step 3** Specify an IP address, or an IP address range.

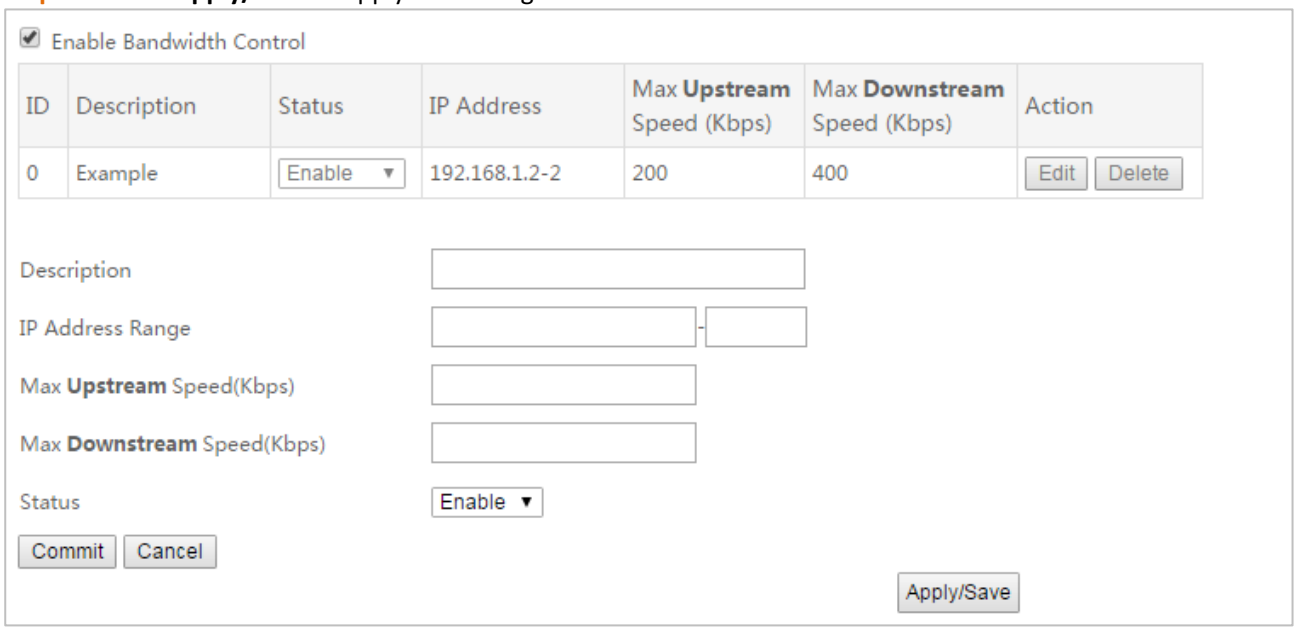
**Step 4** Specify a maximum upstream and downstream speed.

**Step 5** Select the status for the rule.

- **Enable**: When **Enable** is selected, the rule takes effect.
- **Disable**: When **Disable** is selected, the rule does not take effect.

**Step 6** Click **Commit** to add the rule to the list.

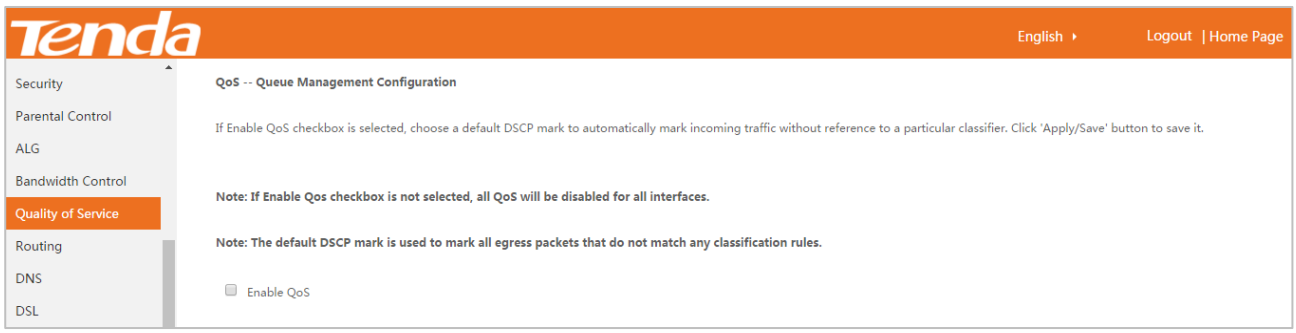
**Step 7** Click **Apply/Save** to apply the settings.




**--End**

# 4.11 Quality of Service

Choose **Advanced** > **Advanced Setup** > **Quality of Service** to enter the configuration page.




If **Enable QoS** checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier.

- **Enable QoS**: Select it to enable the QoS feature of the modem feature.
- **Select Default DSCP Mark**: Select a DSCP mark for the packets not matching the created QoS classification rules.
- **No Change (-1)**: Do not add DSCP mark, and keep the original packets.
- **Auto Marking (-2)**: Randomly select a mark from the following mark list to tag the packets.
- **Default (000000)**: Default PHB (Per-Hop Behaviors). It specifies the best-effort internet service.
- **EF (101110)**: EF (Expedited Forwarding PHB). It specifies the highest priority of the internet service.
- **Class-Selector PHB**: It specifies that the DSCP mark is "XXX000" where X can be "0" or "1". The class of service of Class-Selector PHB is the same as that of IP Precedence used in the current internet. When the XXX are all "0", it is the default PHB.
- **Assured Forwarding PHB**: RFC2597. It is applicable to video service, VPN service, and so on. AF PHB has four service classes which require the corresponding bandwidths and caches. Each service class has three packet-loss priorities.

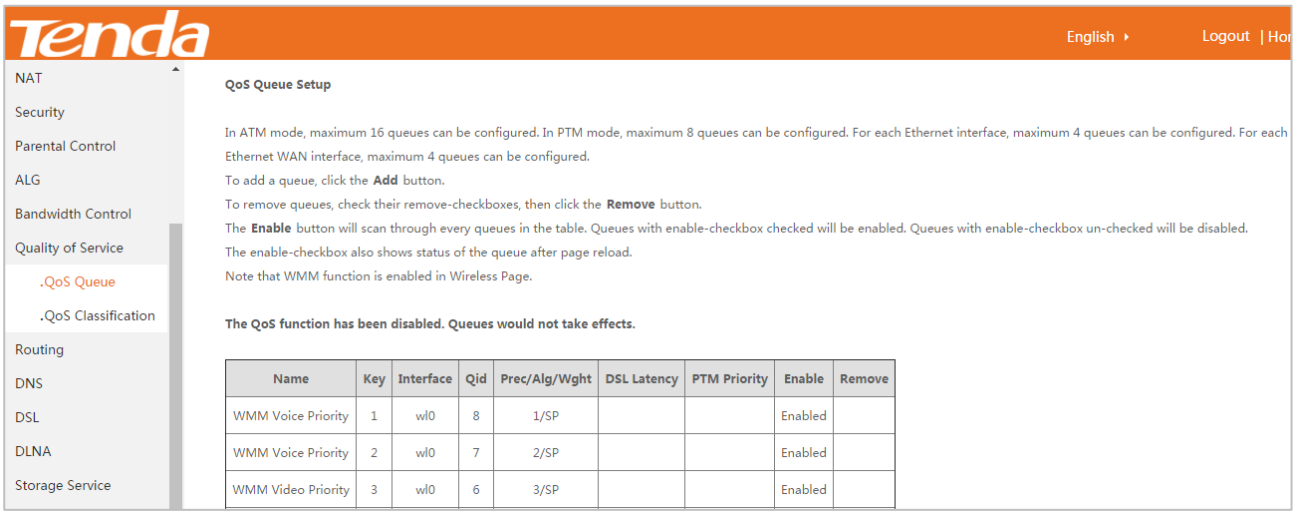
| Packet-loss Priority | AF1 | AF2 | AF3 | AF4 |
|---|---|---|---|---|
| Low (1) | 001010 | 010010 | 011010 | 100010 |
| Medium (2) | 001100 | 010100 | 011100 | 100100 |
| High (3) | 001110 | 010110 | 011110 | 100110 |

NOTE

- If **Enable QoS** checkbox is not selected, the QoS Queue and QoS Classification are not available.
- The default DSCP mark is used to mark all egress packets that do not match any classification rules.

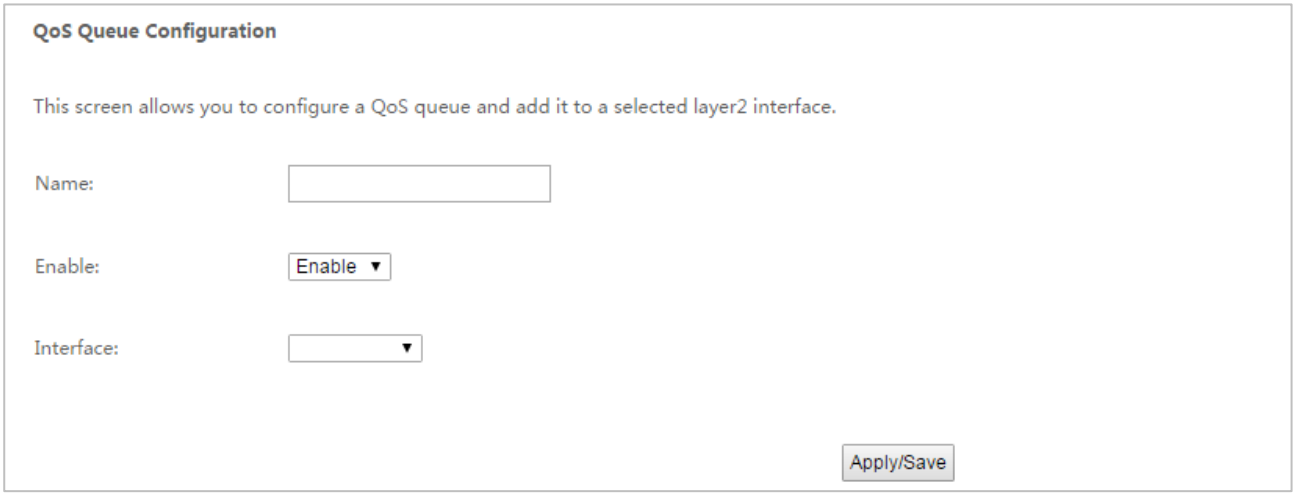
## 4.11.1 QoS Queue

Choose **Advanced** > **Advanced Setup** > **Quality of Service** > **QoS Queue** to enter the configuration page.




To add a queue, perform the following procedure:

**Step 1** Click **Add** to enter the configuration page.




**Step 2** **Name**: Specify a name for the queue.

**Step 3** **Enable**: Select it to enable or disable the queue.

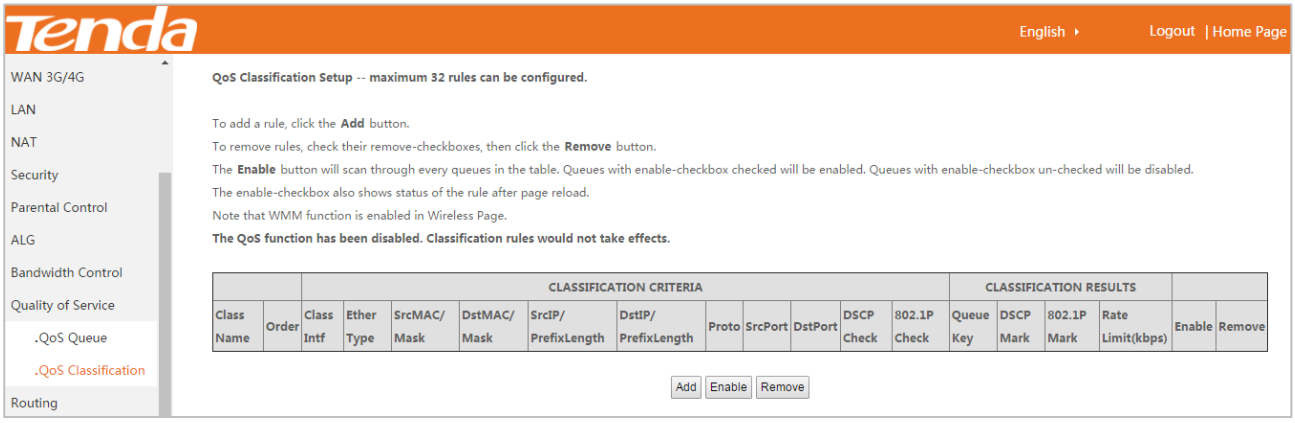
**Step 4** **Interface**: Set an interface for the queue.

**Step 5** Click **Apply/Save**.

**--End**

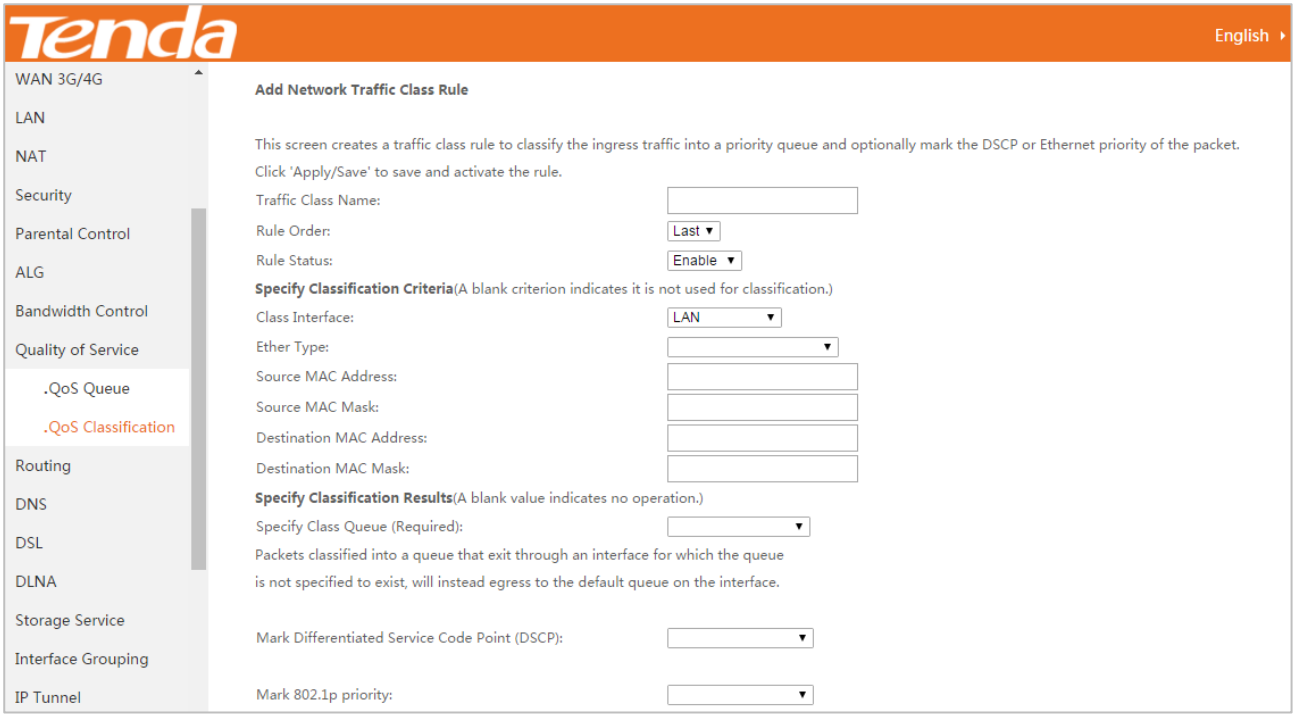
## 4.11.2 QoS Classification

Choose **Advanced** > **Advanced Setup** > **Quality of Service** > **QoS Classification** to enter the configuration page.




To add a QoS classification rule, perform the following procedure:

**Step 1** Click **Add** to enter the configuration page.




**Step 2** **Traffic Class Name**: Specify a name for the rule.

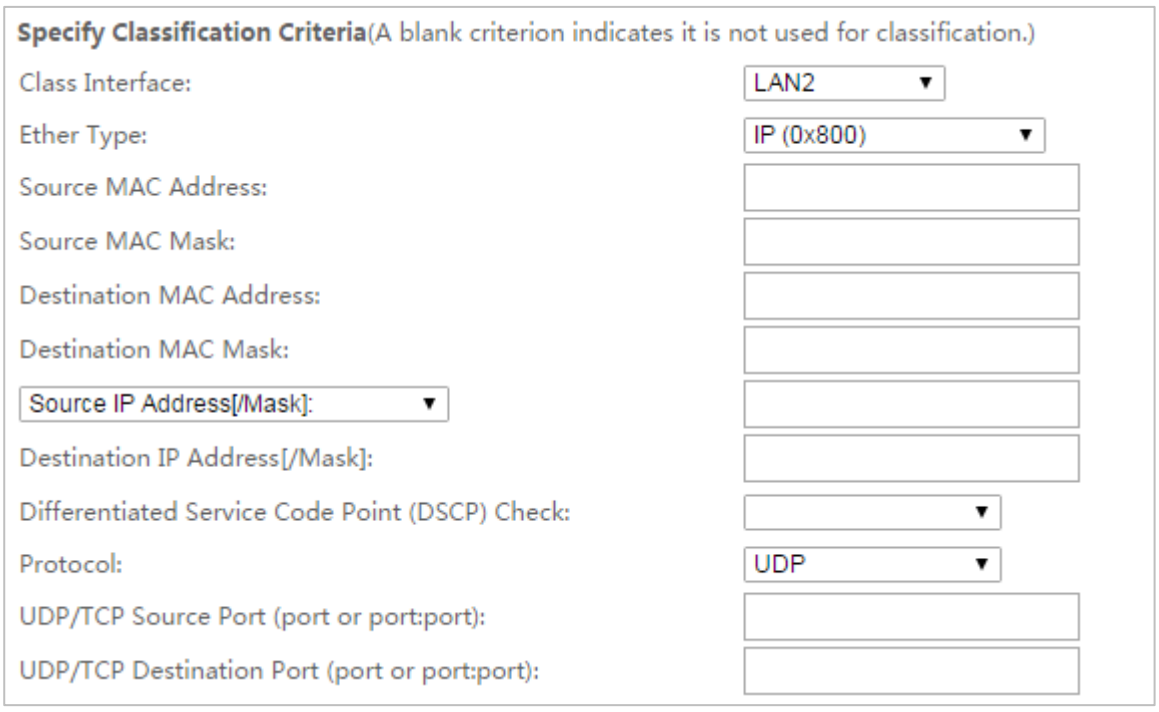
**Step 3** **Rule Order**: Keep the default value ”Last”.

**Step 4** **Rule Status**: Select **Enable** to enable the rule.

**Step 5** Specify the classification criteria.

- **Class Interface**: Specify an interface from which the data traffic comes.
- **Ether Type**: Specify an Ether type for the packets of the rule.
- **Source/Destination MAC Address**: Specifies the source/destination MAC addresses.
- **Source/Destination MAC Mask:** Leave them blank.

When the **Ether Type** is set to **IP (0x800)** or **IPv6 (0x86DD)**, the following parameters need to be specified.




- **Source/Destination IP Address**: If you do not specify the source/destination MAC address, you need to

specify the source/destination IP Address for the classification.

- **Differentiated Service Code Point (DSCP) Check**: Specify a DSCP mark for the data streaming.
- **Protocol**: Select a protocol.
- **UDP/TCP Source/Destination Port**: Specify the port information for the data streaming.

**Step 6** Specify the classification results.

- **Specify Class Queue (Required)**: Specifies a queue to which packets are distributed (The queue should be set in **Advanced** > **Advanced Setup** >**QoS** > **QoS Classification** in advance.)
- **Mark Differentiated Service Code Point (DSCP)**: Specify a mark for the queue when the queue exits.
- **Mark 802.1p priority**: Tag an 802.1p priority mark for the data stream.
- **Set Rate Limit**: Specify the maximum transmission speed of the queue.

**Step 7** Click **Apply/Save**.

**--End**

**Application Scenario**

Company A has three kinds of network service: video conference, IP phone and online video business, and FTP/Web/Email service. To ensure the quality of these services, the QoS function is required.

Assume that:

- The company accesses the internet through phone cable.
- UDP ports for video conference: 1718, 1719, and 1720
- UDP port for IP phone: 65060
- Online video uses PPlive. UDP port for PPlive: 7100 and 7101

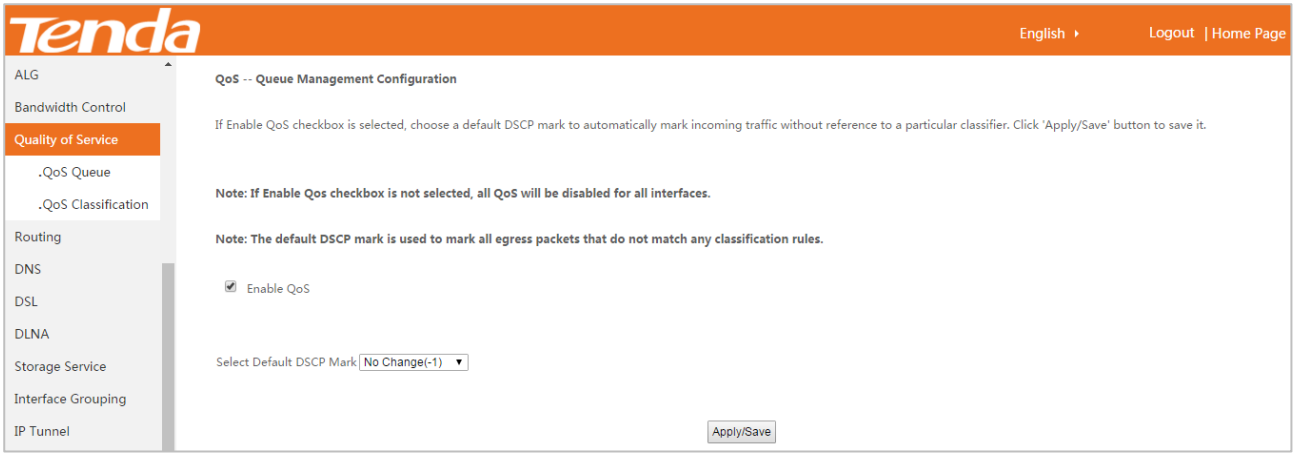
**Solution:**

- Video Conference: High priority is required. We set the priority to 1.
- IP Phone and Online Video: Average priority is required. We set the priority to 2. The queue weight of IP phone (weight 20) should be higher than that of online video (weight 10).
- FTP/Web/Email Service: The priority is not required. We set the priority to 3. The queue weight of web service (weight 20) should be higher than that of FTP and Email service (weight 10).
- These services all use WFQ algorithm.

**Procedure**

**Step 1** Enable QoS function.

1. Choose **Advanced** > **Advanced Setup** > **Quality of Service** to enter the configuration page.



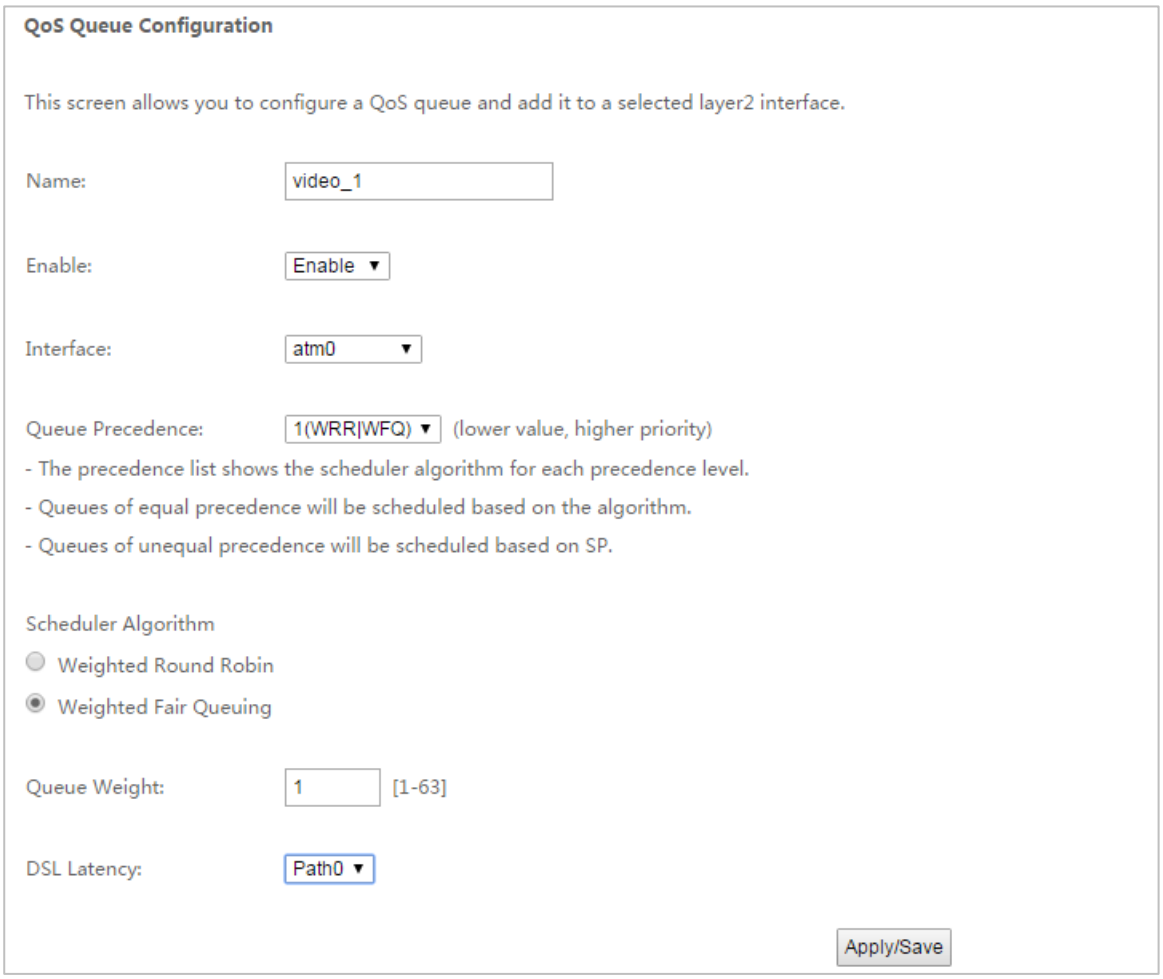

2. Select **Enable QoS**.
3. Click **Apply/Save**.

**Step 2** Configure QoS Queues.

1. Choose **Advanced** > **Advanced Setup** > **Quality of Service > QoS Queue** to enter the configuration page.
2. Add a Video Conference queue.

(1) Click **Add**.


(2) **Name**: Specify a name for the queue.
(3) **Enable**: Select **Enable**.
(4) **Interface**: Select **atm0**.
(5) **Queue Precedence**: Select **1 (WRR/WFQ)**.
(6) Select **Weighted Fair Queuing**.
(7) Set **Queue Weight** to 1.
(8) Click **Apply/Save**.



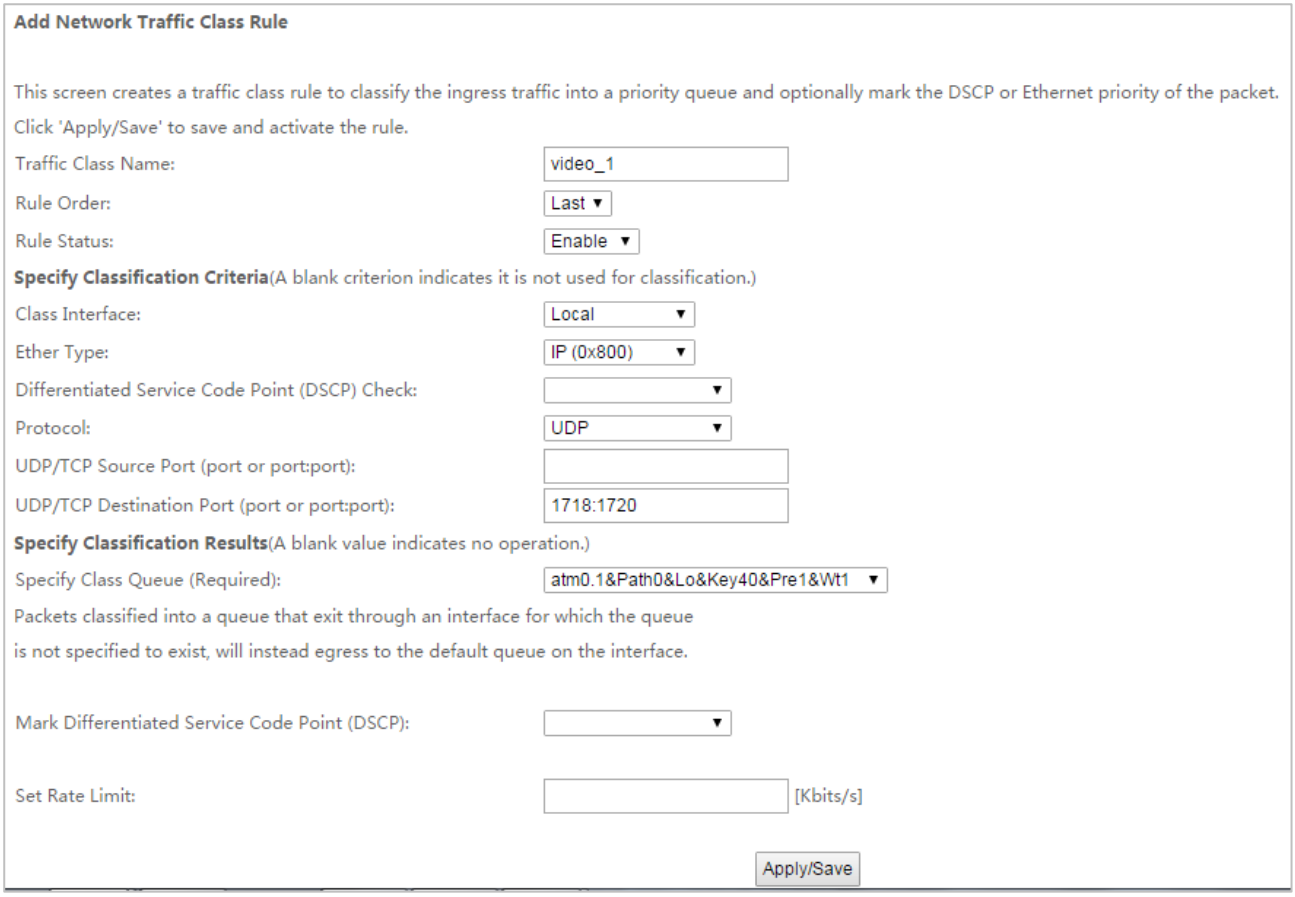

3. Perform the steps in step "2" to add IP phone, online video, web, FTP and Email queues.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Default Queue | 33 | atm0 | 1 | 8/WRR/1 | Path0 | | ☑ | |
| video_1 | 40 | atm0 | 2 | 1/WFQ/1 | Path0 | Low | ☑ | ☐ |
| IP-Phone | 42 | atm0 | 3 | 2/WFQ/20 | Path0 | Low | ☑ | ☐ |
| Online_Video | 43 | atm0 | 4 | 2/WFQ/10 | Path0 | Low | ☑ | ☐ |
| Web | 44 | atm0 | 5 | 3/WFQ/20 | Path0 | Low | ☑ | ☐ |
| FTP_Email | 46 | atm0 | 6 | 3/WFQ/10 | Path0 | Low | ☑ | ☐ |

**Step 3** Configure QoS classification.

1. Choose **Advanced** > **Advanced Setup** > **Quality of Service** > **QoS Classification** to enter the configuration page.
2. Click **Add**.
3. Traffic Class Name: Specify a name for the classification.
4. Rule Order: Keep the default.
5. Rule Status: Set it to **Enable**.
6. Class Interface: Select **Local**.
7. Ether Type: Select **IP (0x800)**.

8. Protocol: Select **UDP**.
9. UDP/TCP Destination Port: Enter **1718:1720**.
10. Specify Class Queue (Required): Select the **video_1** queue you add.
11. Click **Apply/Save**.




**Step 4** Perform the steps in "step 3" to add classifications for IP phone, online video, web, FTP and Email services.

| | | CLASSIFICATION CRITERIA | | | | | | | | | | | CLASSIFICATION RESULTS | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Class Name | Order | Class Intf | Ether Type | SrcMAC/ Mask | DstMAC/ Mask | SrcIP/ PrefixLength | DstIP/ PrefixLength | Proto | SrcPort | DstPort | DSCP Check | 802.1P Check | Queue Key | DSCP Mark | 802.1P Mark | Rate Limit(kbps) | Enable | Remove |
| video_1 | 1 | Local | IP | | | | | UDP | | 1718:1720 | | | 40 | | | | ☑ | ☐ |
| IP-Phone | 2 | Local | IP | | | | | UDP | | 65060 | | | 42 | | | | ☑ | ☐ |
| Online_Video | 3 | Local | IP | | | | | UDP | | 7100:7101 | | | 43 | | | | ☑ | ☐ |
| Web | 4 | Local | IP | | | | | TCP | | 80 | | | 44 | | | | ☑ | ☐ |
| FTP | 5 | Local | IP | | | | | TCP | | 20:21 | | | 46 | | | | ☑ | ☐ |
| Email | 6 | Local | IP | | | | | TCP | | 25 | | | 46 | | | | ☑ | ☐ |

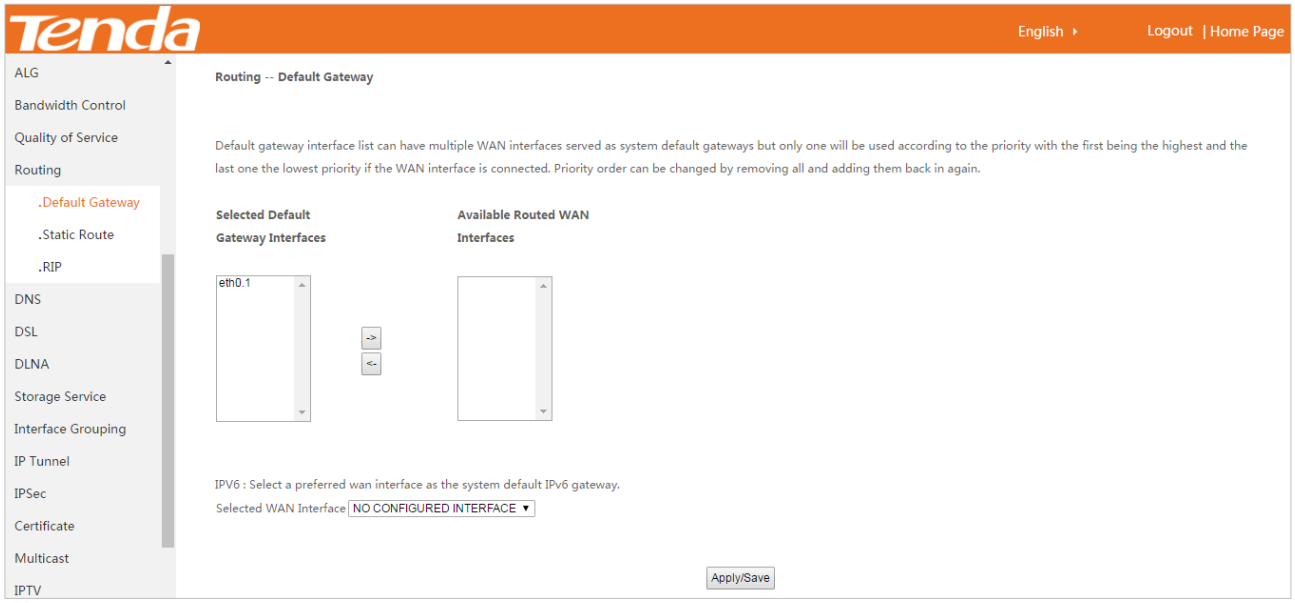
**--End**

# 4.12 Routing

## 4.12.1 Default Gateway

Default gateway interface list can contain multiple WAN interfaces serving as system default gateways. The first WAN interface has the highest priority.

Choose **Advanced** > **Advanced Setup** > **Routing** > **Default Gateway** to enter the configuration page.




**Selected Default Gateway Interfaces**: It specifies the current effective default IPv4 gateway interface. If there are many interfaces in the list, the first one always takes effect.

Select a WAN interface and click the  button to move it to the Available Routed WAN Interfaces box.

**Available Routed WAN Interfaces**: It Specifies the current alternative default IPv4 gateway interface. Select a WAN interface and click the  button to add it to the **Selected Default Gateway Interfaces** box.

**IPV6 Selected WAN Interface**: Select the current IPv6 gateway interface in effect from the drop-down list.

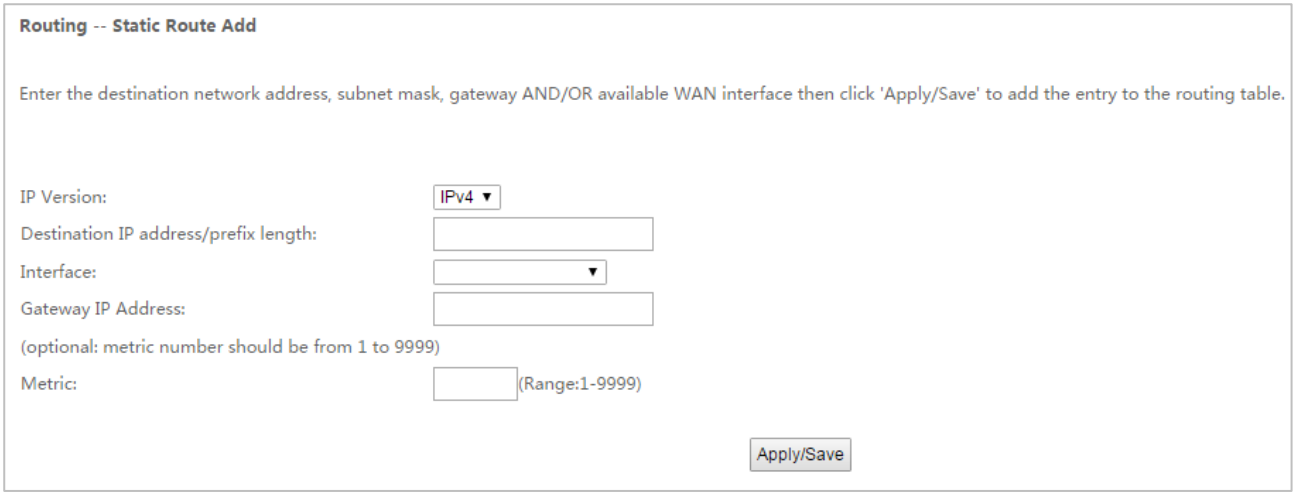
## 4.12.2 Static Route

Static Route is used to select the best route for delivering data from a source address to a destination address. A static route is a manually configured route, which is simple, efficient, and reliable. Appropriate static routes help reduce the number of route selection problems and reduce route selection load, increasing the packet forwarding speed.

Choose **Advanced** > **Advanced Setup** > **Routing** > **Static Route** to enter the configuration page.


To add a static route, perform the following procedure:

**Step 1** Click **Add**.




**Step 2** **IP Version**: Specify an IP protocol version for the static route: IPv4 or IPv6.

**Step 3** **Destination IP address/prefix length**: Set an IP address of a specified host or a network number of a specified network.

For example, if you want to set the **Destination IP address/prefix length** to a specified host, assume that the IP of the host is "**1.2.3.4**", you can set it to "**1.2.3.4/32**". If you want to set the **Destination IP address/prefix length** to all hosts in a specified network, assume that the network is "**2.2.3.3/255.255.0.0**", you can set it to "**2.2.0.0/16**" which represents all hosts whose IP address start with "2.2".

**Step 4** **Interface**: Specify an interface for the outgoing data.

**Step 5** **Gateway IP Address**: set the gateway IP address to the IP address of the next-hop router.

**Step 6** (**Optional**) **Metric**: Specify a metric value for the static route. A smaller number indicates a higher priority.

**--End**

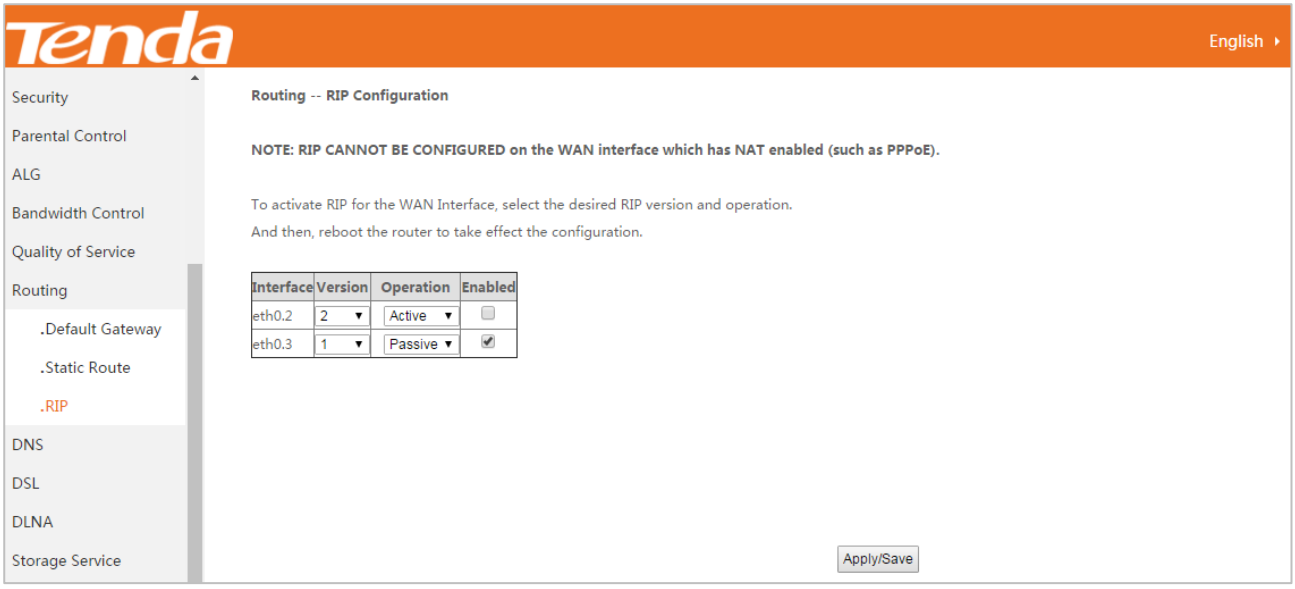
TIP

- Destination IP address cannot be in the same IP network segment as that of WAN or LAN IP address of the modem router.
- When the interface is set to a WAN interface, the gateway IP address should be in the same network segment as that of that of WAN port. When the interface is set to a LAN interface, the gateway IP address should be in the same network segment as that of the LAN port.
- If you are not familiar with static IP, you'd better not configure this function. Inappropriate static routes may cause fault to the network.

## 4.12.3 RIP

RIP (Routing Information Protocol) is one of the oldest distance-vector routing protocols which employ the hop count as a routing metric. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from source to destination. The maximum number of hops allowed for RIP is 15, which limits the size of networks that RIP can support. A hop count of 16 is considered an infinite distance and the route is considered unreachable.

Choose **Advanced** > **Advanced Setup** > **Routing** > **RIP** to enter the configuration page.




| Parameter | Description |
|---|---|
| Interface | It specifies the WAN interfaces you add in a WAN service with NAT disabled. |
| Version | It specifies two RIP versions the modem router supports: RIPv1 and RIPv2.<br>RIP 1: The periodic routing updates do not carry subnet information.<br>RIP 2: The periodic routing updates carry subnet information. |
| Operation | Active: The WAN interface sends and receives RIP packets.<br>Passive: The WAN interface only receives RIP packets. |
| Enable | Select to enable the RIP function of this WAN interface. |
| Apply/Save | Click this button to apply the settings. |

NOTE

- Only the WAN service with NAT disabled is displayed in the list.
- After configuration, reboot the modem router for the settings to take effect.

# 4.13 DNS

## 4.13.1 DNS Server

The DNS server translates domain names to numeric IP addresses. It is used to look up site addresses based on their names.

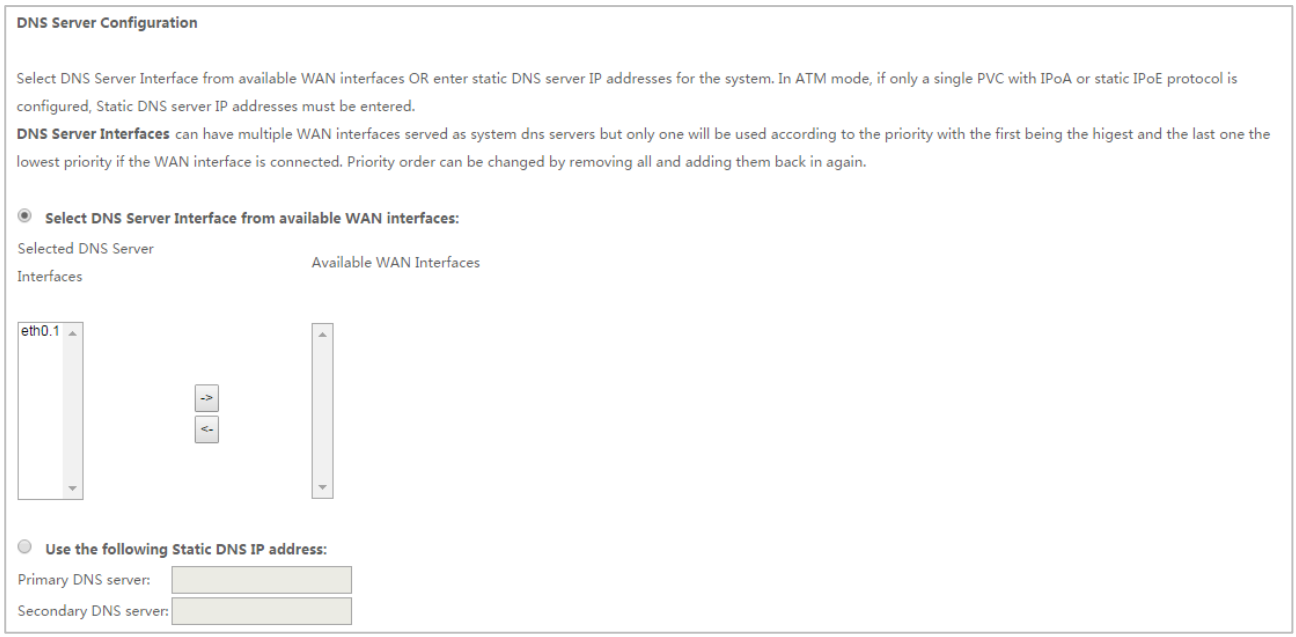
Choose **Advanced** > **Advanced Setup** > **DNS** > **DNS Server** to enter the configuration page.

**For IPv4, perform either of the following procedures:**

-Select a WAN interface from **Available WAN interfaces** box, and click <- to add it to **Select DNS Server Interface** box**.**

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

And then click **Apply/Save**.

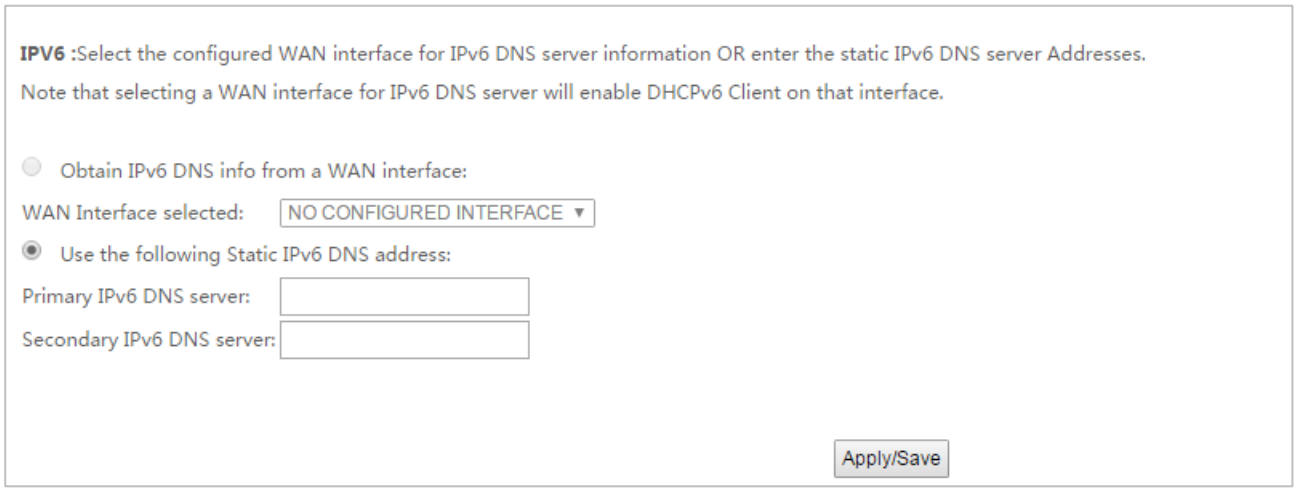



**For IPv6:**

-Select **Obtain IPv6 DNS info from a WAN interface** and select a configured WAN interface for the IPv6 DNS server information.

-Select **Use the following Static IPv6 DNS address** and enter the static IPv6 DNS server Addresses.

And then click **Apply/Save**.




NOTE

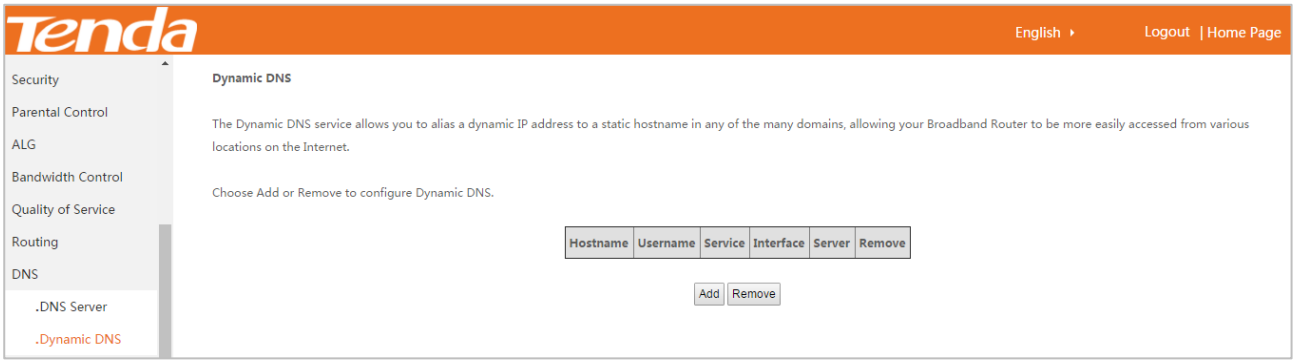
- Default gateway interface list can contain multiple WAN interfaces serving as system default gateways. The first WAN interface has the highest priority.

- In ATM mode, static DNS server IP addresses must be entered if only single PVC with IPoA or static IPoE protocol is configured.
- If you do not know the static DNS server IP information, consult your ISP.
- 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 accessible.

## 4.13.2 Dynamic DNS

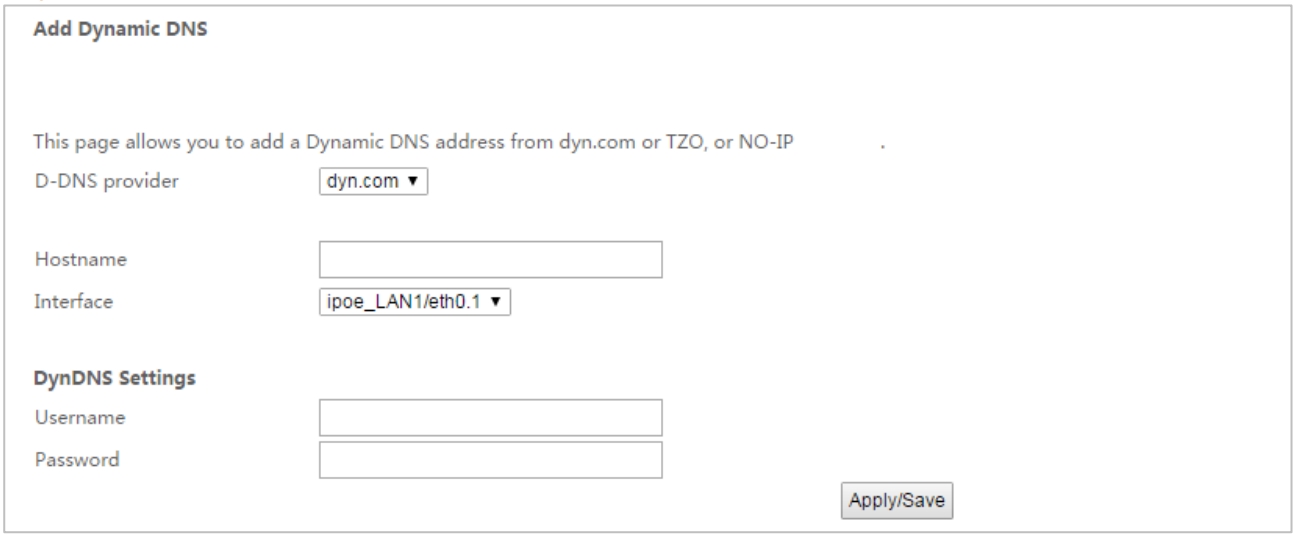
DDNS maps the WAN IP address (changeable public IP address) of the router to a domain name for dynamic domain name resolution. This ensures proper operation of functions that involve the WAN IP address of the modem router, such as the remote management and virtual server functions.

Choose **Advanced** > **Advanced Setup** > **DNS** > **Dynamic DNS** to enter the configuration page.




To configure the DDNS function, perform the following procedure:

**Step 1** Click **Add**.




**Step 2** **D-DNS provider**: Specify a DDNS service provider. The supported service providers include dyn.com, TZO, and NO-IP.

**Step 3** **Hostname**: Specify the DDNS domain name registered on a DDNS service provider's website.

**Step 4** **Interface**: Specify a WAN service.

**Step 5** **Username/Password**: Specify the user name and password registered on a DDNS service provider's website for logging in to the DDNS service.

**Step 6** Click Apply/Save.

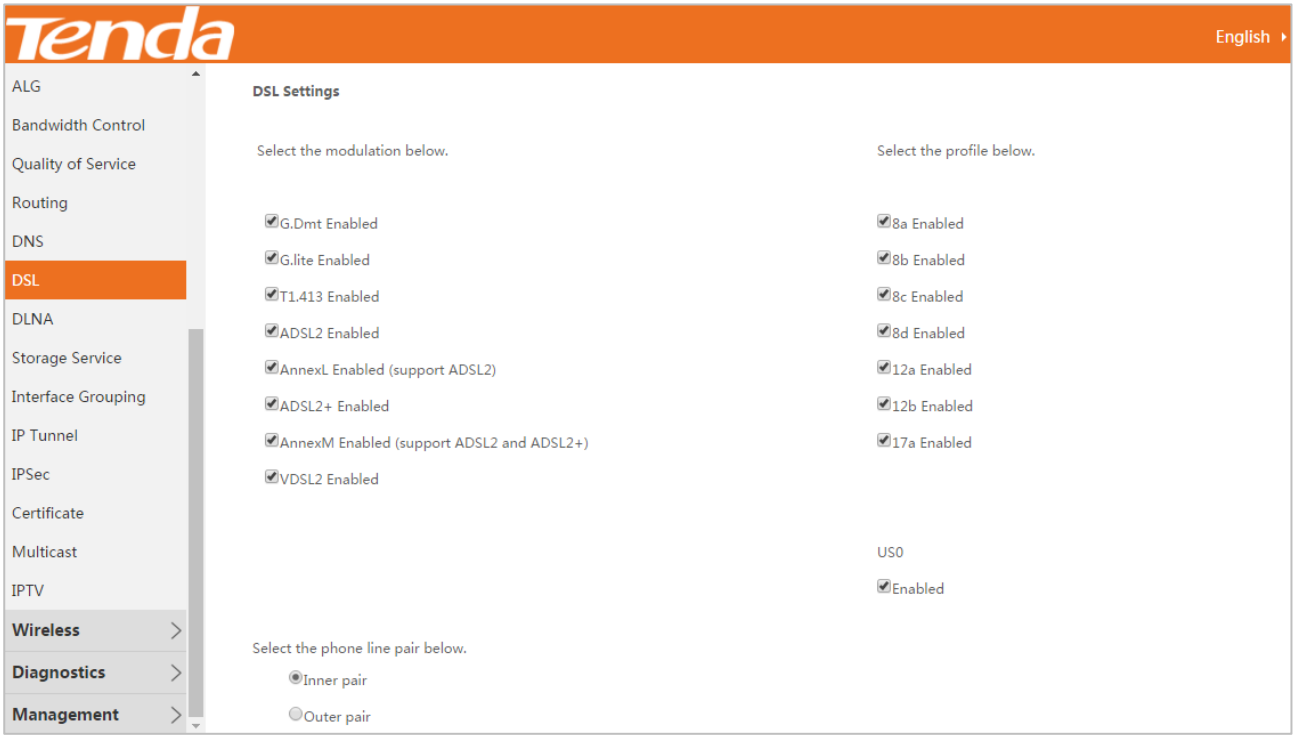
**--End**

# 4.14 DSL

This page allows you to configure DSL parameters. DSL parameters configuration should be based on the parameters of the upstream device. Final parameters can be checked on Statistics-xDSL page. Wrong configurations may fail your Internet access.

Change them only when you are instructed by your ISP or our technical staff when your modem router fails to negotiate with ISP in DSL (ATM) mode. If the ADSL LED of the device blinks, DSL negotiation may fail.

Choose **Advanced** > **Advanced Setup** > **DSL** to enter the configuration page.



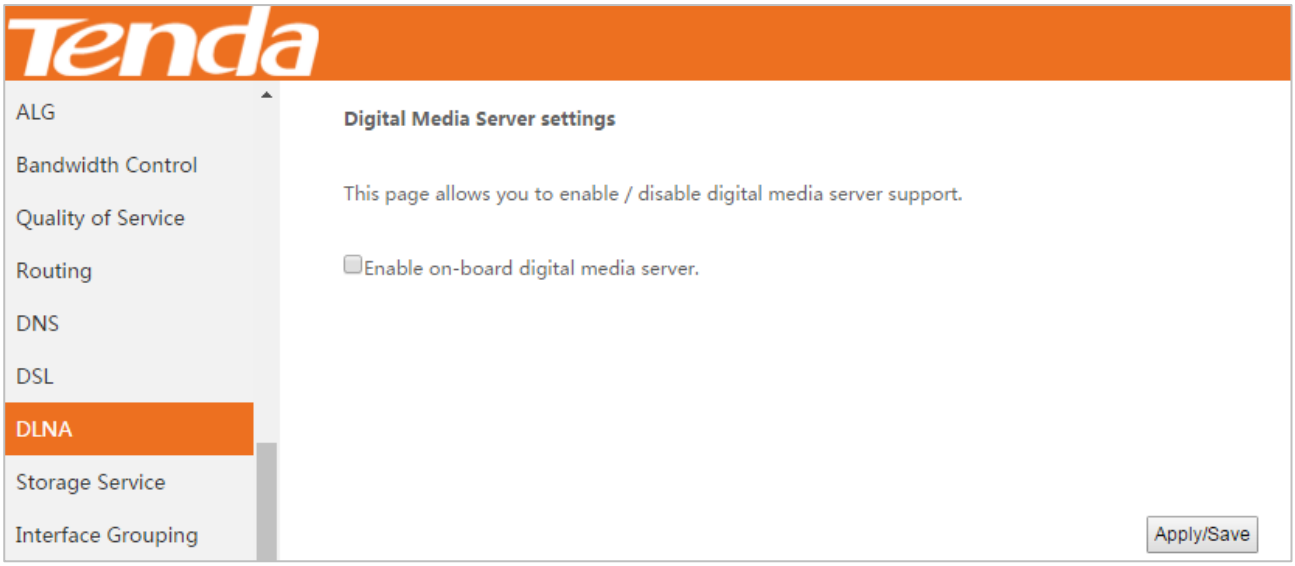

| Parameter | Description |
|---|---|
| G.Dmt | It specifies G992.1. The maximum upload/download rates are 1.3 Mbps and 8 Mbps. When it is used, POTS splitter is required for client. |
| G.lite | It specifies G992.2. The maximum uploading/downloading rate is 512 Kbps/1.5 Mbps. When it is used, POTS splitter is NOT required for client. |
| T1.413 | It specifies ANSI_T1.413. Based on DMT standard, the maximum uploading/downloading rate is 1.5 Mbps/15 Mbps. When it is used, POTS splitter is required for client. |
| ADSL2 | It specifies G992.3. The maximum uploading/downloading rate is 1 Mbps/12 Mbps. |
| AnnexL | It specifies reach Extended ADSL2. When the clients are far away from the modem router, this mode can improve the coverage. The maximum uploading/downloading rate is 1.5 Mbps/15 Mbps. |
| ADSL2+ | It specifies G992.5. The maximum uploading/downloading rate is 1 Mbps/24 Mbps. |
| AnnexM | This mode is compatible with the upstreaming bandwidth extension mode and implemented based on G992.3 ADSL2 and G992.5 ADSL2+. In this mode, the upload |

| | |
|---|---|
| | rate of ADSL2+ is increased from 1 Mbps to 2.5 Mbps. AnnexM takes effect only when ADSL2, AnnexL or ADSL2+ is selected. |

# 4.15 DLNA

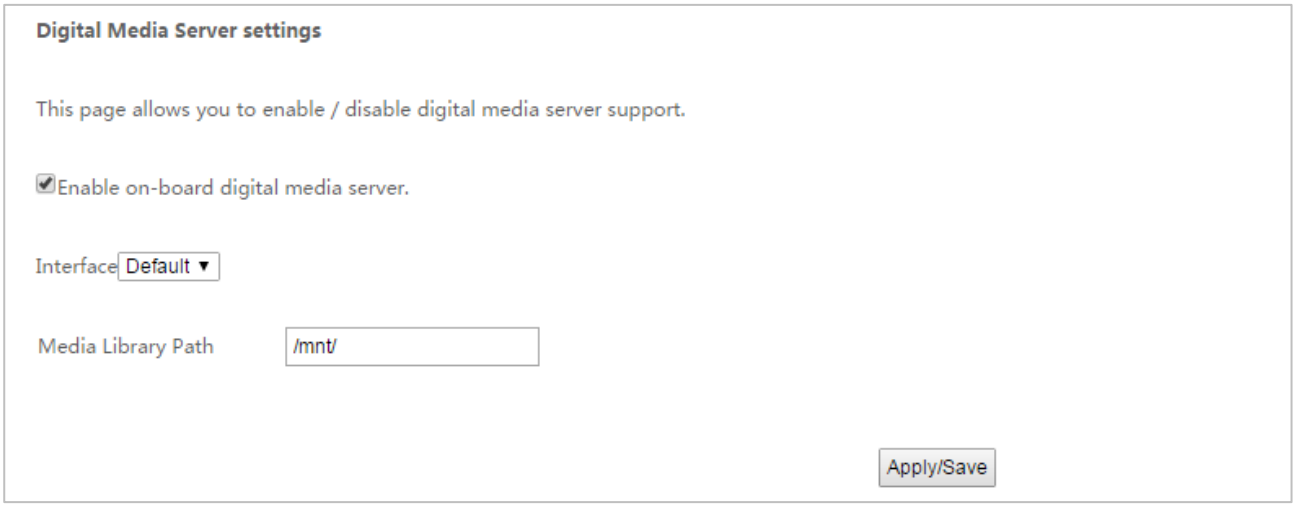
DLNA is a solution to share multimedia resources among digital devices by wired or wireless means. Connect a USB storage device to the USB port of the modem router, enable DLNA function, and computers or smart phones connected to the router can play the resources in the USB storage device.

Choose **Advanced** > **Advanced Setup** >**DLNA** to enter the configuration page.




To configure the DLNA function, perform the following procedure:

**Step 1** Select Enable on-board digital media server.




**Step 2** **Interface**: Keep the default value.

**Step 3** **Media Library Path**: Enter the path of the media library you want to share. The default path "/mnt" indicates that all resources in the USB storage device attached to the modem router can be played.

**Step 4** Click Apply/Save.

--End

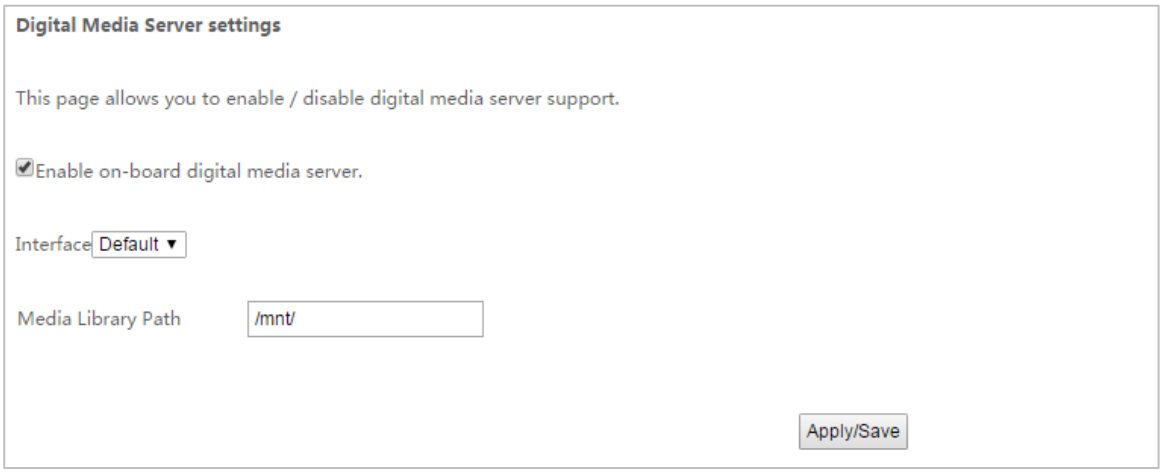
**Application Scenario**

User A uses V300 to set up a LAN in his apartment. His desktop PC, smart phone, and tablet access the internet through this modem router. He connects a USB storage device to the USB port of the modem router and stores lots of movies, TV series, images, and audio clips in the device.

**Configuration Procedure**

**Step 1** Enable the **DLNA** function of the modem router.

1. Choose **Advanced** > **Advanced Setup** >**DLNA** to enter the configuration page.




2 Select Enable on-board digital media server.

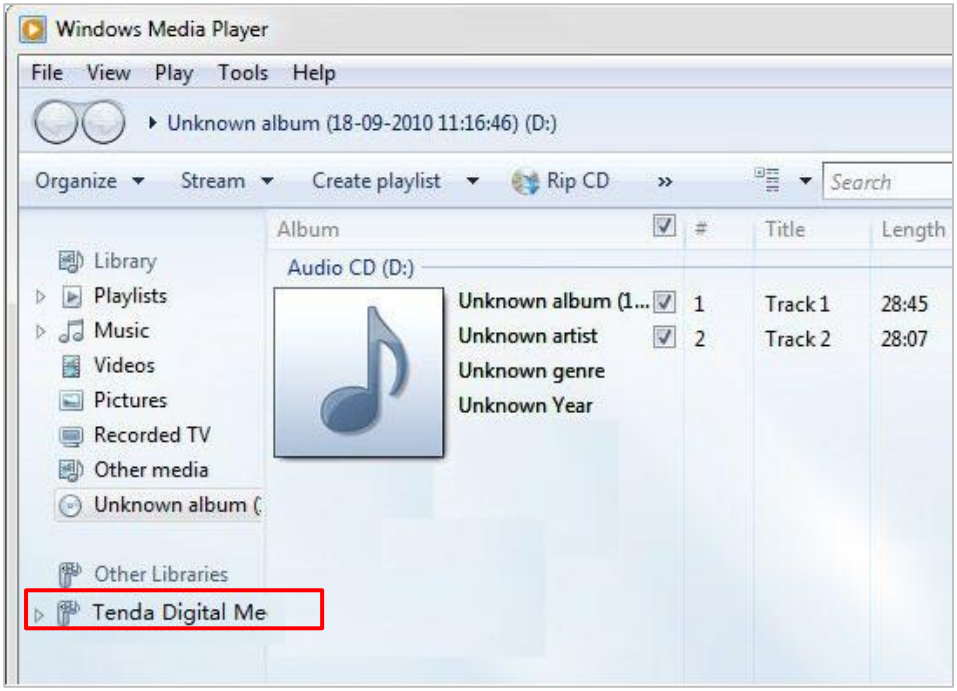
3 Click **Apply/Save**.

**Step 2** On the computer, browse the video, audio, and image files in the USB storage device attached to the modem router. A computer running Windows 7 is taken as an example to describe the procedure.

1 Run **Windows Media Player**. The USB storage device is displayed in the **Other Libraries** of the left pane.

2 Click the name of USB storage device which is **Tenda Digital Media Server** in this example.

The video, audio, and image files in the USB storage device appear. Then you can select the items you want to play.




**--End**

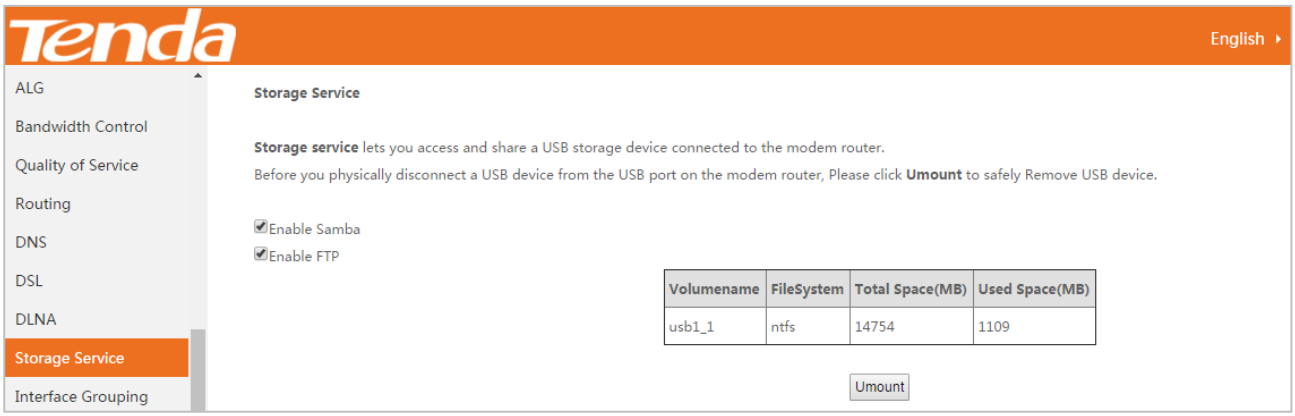
TIP

If you want to play the resources in the USB storage device on your smart phone, it needs to be equipped with DLNA client.

# 4.16 Storage Service

The modem router can automatically recognize a USB storage device connected to the USB port of the modem router. The device can be accessed over the LAN through FTP or Samba.

Choose **Advanced** > **Advanced Setup** > **Storage Service** to enter the configuration page.




To enable the Samba and FTP servers, perform the following procedure:

**Step 1** Select Enable Samba.

**Step 2** Select Enable FTP.

**--End**

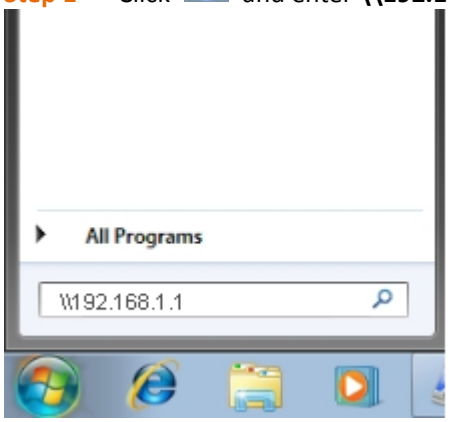
**Accessing the USB Storage Device Connected to the Modem Router over the LAN**

A V300 modem router is used to set up a LAN in an apartment. A USB storage device is connected to the USB port of the modem router and functions as a file server. Users can download resource from the server. Assume that:

The server address is **192.168.1.1** (the LAN IP address of the modem router).

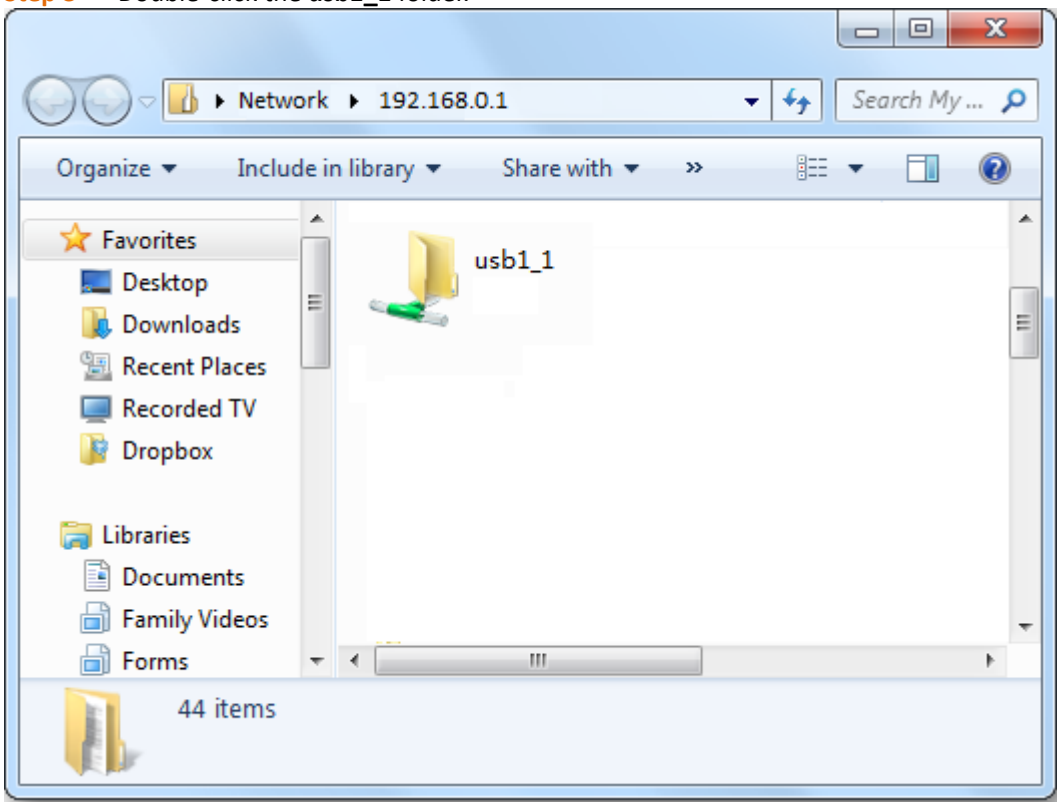
To access the USB storage device, perform the following procedure: (Windows 7 is used as an example for description.)

**Step 1** Click and enter **\\192.168.1.1**.



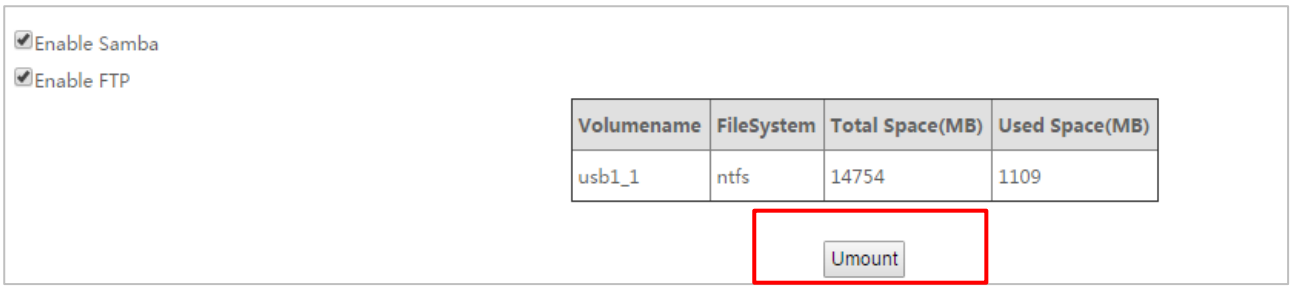

**Step 2** Press **Enter** on the keyboard.

**Step 3** Double-click the **usb1_1** folder.




**--End**

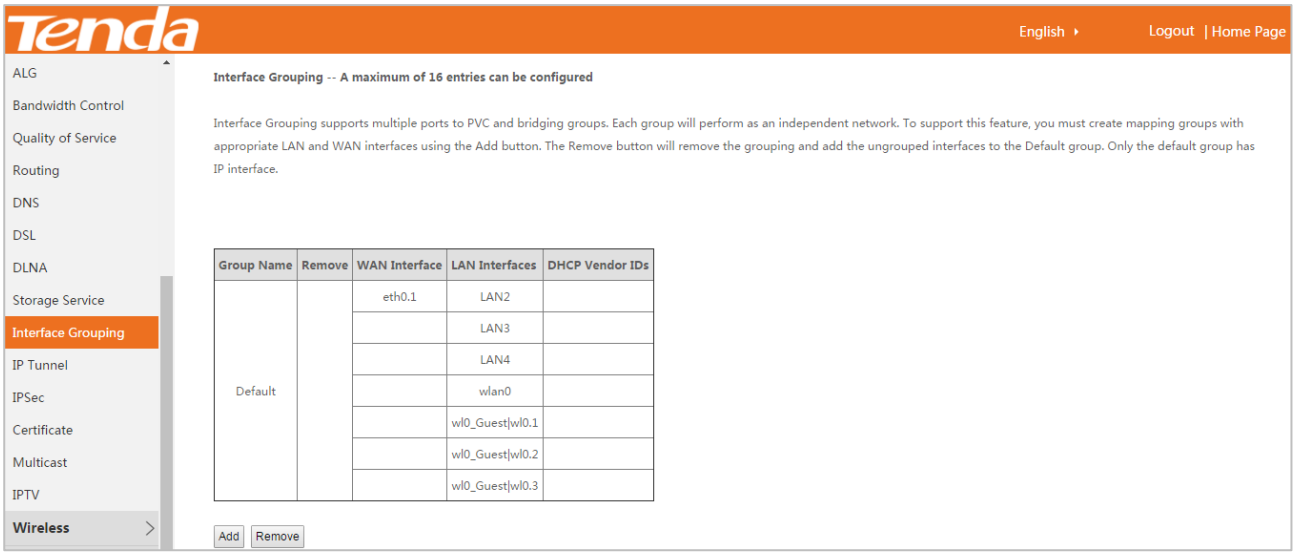
Before you physically disconnect a USB device from the USB port on the modem router, Please click **Umount** to safely Remove USB device.




# 4.17 Interface Grouping

If you create multiple WAN services (PPPoE and other WAN service types), and want a LAN or WLAN to use a WAN service exclusively, you can use this function to map the LAN or WLAN onto the WAN service. Each group forms an independent network.

Choose **Advanced** > **Advanced Setup** > **Interface Grouping** to enter the configuration page.




Assume that:

- The modem router accesses the internet through port 1 using an Ethernet cable.
- You create two WAN services: Including one service whose WAN service type and WAN IP settings are set to **IP over Ethernet** and **Obtain an IP address automatically** and the other service whose WAN service type is set to **Bridging**.
- You want all wireless devices to use **IP over Ethernet** WAN service, and all wired device use **bridging** WAN service.

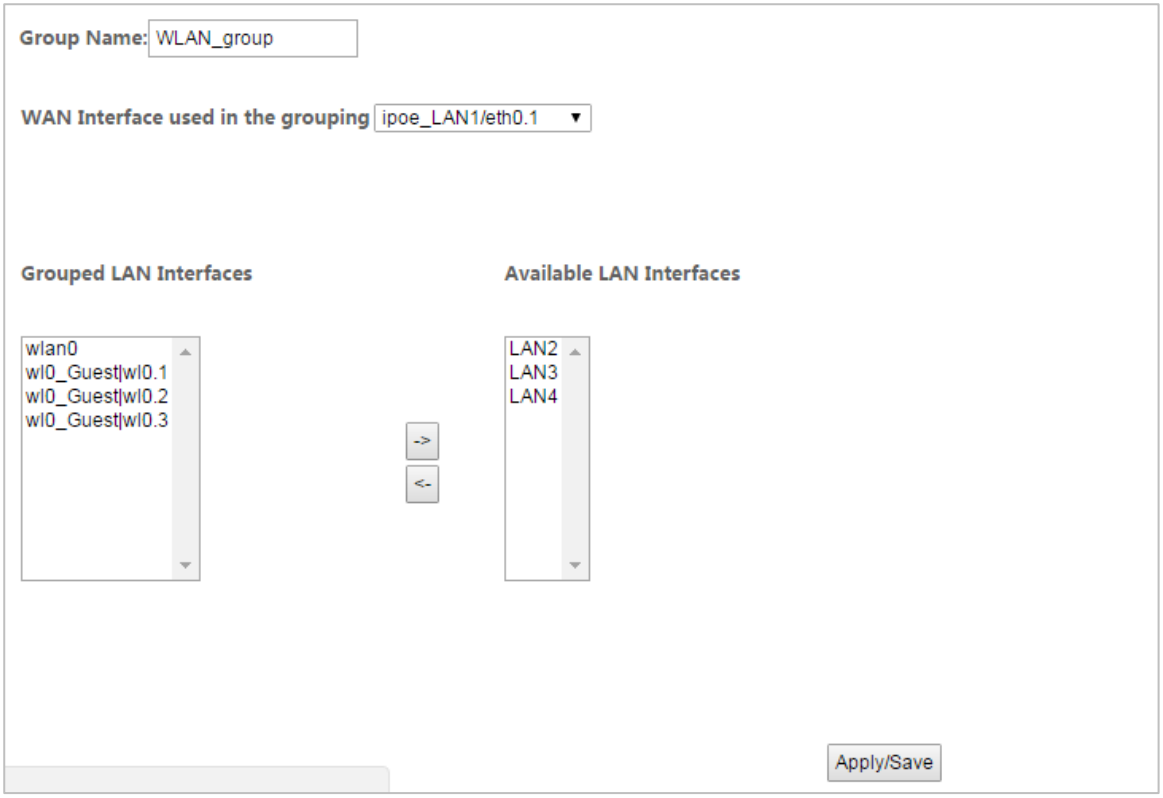
To create an interface group, perform the following procedure:

**Step 1** Click **Add**.

**Step 2** Specify a group name.

**Step 3** Select a WAN service you create, which is **ipoe_LAN1/eth0.1** in this example.

**Step 4** Select an interface in **Available LAN Interfaces** list and click <- button to move it to **Grouped LAN Interfaces** list. In this example, all wireless interfaces are moved to **Grouped LAN Interfaces** list.




**Step 5** Click Apply/Save.

**--End**

After the configuration takes effect, all wireless interfaces belong to **WLAN_group**, and use the WAN service **IP over Ethernet** (eth0.1). All wired interfaces (port 1, 2, and 3) belong to the default group, and use the WAN service **Bridging** (eth0.2).

| Group Name | Remove | WAN Interface | LAN Interfaces | DHCP Vendor IDs |
|---|---|---|---|---|
| Default | | eth0.2 | LAN2 | |
| | | | LAN3 | |
| | | | LAN4 | |
| WLAN_group | ☐ | eth0.1 | wlan0 | |
| | | | wl0_Guest\|wl0.1 | |
| | | | wl0_Guest\|wl0.2 | |
| | | | wl0_Guest\|wl0.3 | |

TIP

- If you create many groups, the LAN IP address used by the Default group members is 192.168.1.1, the LAN IP address of the second group member is 192.168.2.1, and so on.
- If the IPTV function is enabled, the modem router automatically creates one interface group named IPTV. If it is deleted, the IPTV function is not available.

# 4.18 IP Tunnel

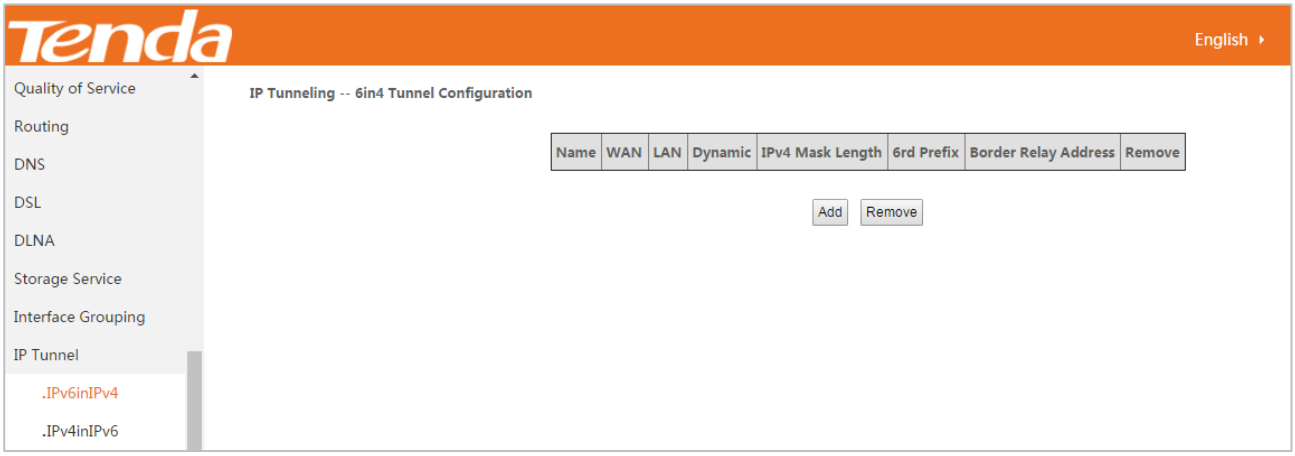
An IP tunnel is an Internet Protocol (IP) network communications channel between two networks. It is used to transport another network protocol by encapsulating one IP packet in another IP packet. To encapsulate an IP packet in another IP packet, an outer header is added with source IP, the entry point of the tunnel and the destination point, the exit point of the tunnel. While doing this, the inner packet is unmodified.

The modem router provides two IP tunnels: IPv6inIPv4 and IPv4inIPv6.

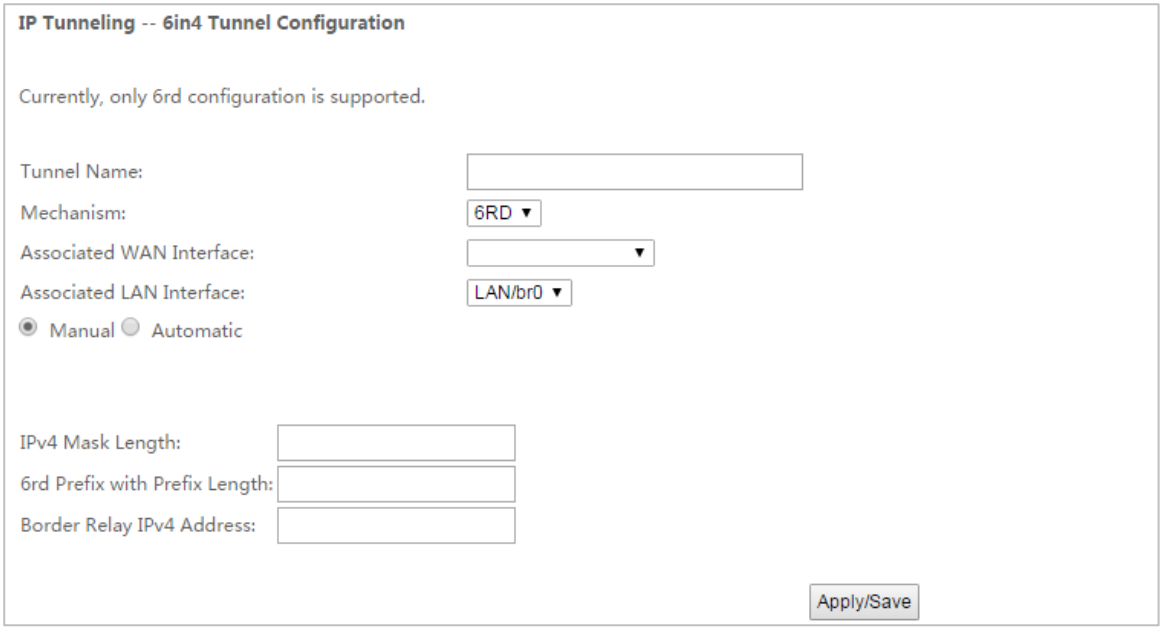
## 4.18.1 IPv6inIPv4

IPv6inIPv4 is an internet transition mechanism for migrating from Internet Protocol version 4 (IPv4) to IPv6. IPv6inIPv4 uses tunneling to encapsulate IPv6 traffic over explicitly-configured IPv4 links.

Choose **Advanced** > **Advanced Setup** > **IP Tunnel > IPv6inIPv4** to enter the configuration page.




To configure the IPv6inIPv4 tunnel, perform the following procedure:




**Step 1** Click **Add**.

**Step 2** **Tunnel Name**: It specifies a tunnel name.

**Step 3** **Mechanism**: It specifies the 6in4 tunnel implement mechanism. The modem router only supports 6RD.

**Step 4** **Associated WAN Interface**: It specifies an associated WAN interface for the 6in4 tunnel. The WAN interface is required to use IPv4 protocol only.

**Step 5** **Associated LAN Interface**: Specify an associated LAN interface for the 6in4 tunnel.

**Step 6** Select a type of obtaining border relay address.

- **Manual**: Manually set a 6RD-BR address.
- **Automatic**: Automatically obtain a 6RD-BR address from BR. If you select **Automatic**, skip step 7 - 9.

**Step 7** **IPv4 Mask Length**: Specify the IPv4 mask length.

**Step 8** **6rd Prefix with Prefix Length**: Specify the 6RD prefix with prefix length.

**Step 9** **Border Relay IPv4 Address**: Specify the border relay IPv4 address of WAN.

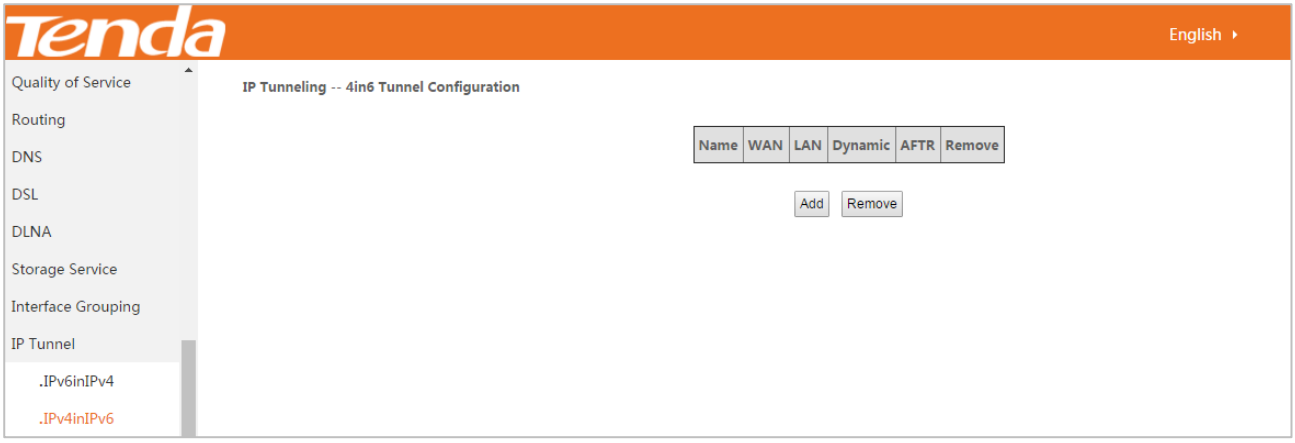
**Step 10** Click Apply/Save.

**--End**

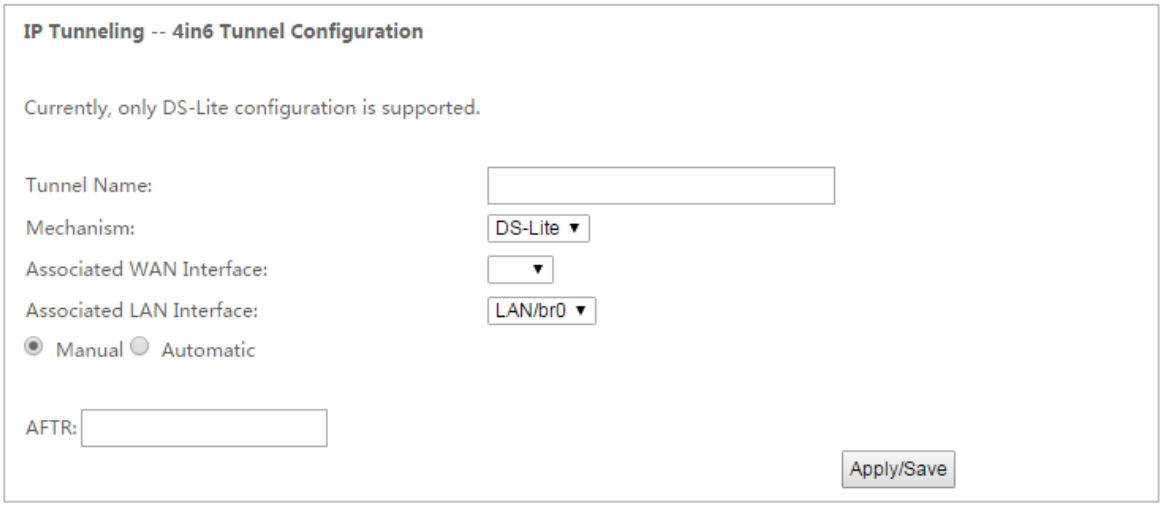
## 4.18.2 IPv4inIPv6

IPv4inIPv6 is an Internet interoperation mechanism allowing Internet Protocol version 4 (IPv4) to be used in an IPv6 only network. 4in6 uses tunneling to encapsulate IPv4 traffic over configured IPv6 tunnels.

Choose **Advanced** > **Advanced Setup** > **IP Tunnel > IPv4inIPv6** to enter the configuration page.




To configure the IPv4inIPv6 tunnel, perform the following procedure:




**Step 1** Click **Add**.

**Step 2** **Tunnel Name**: Tunnel Specify a tunnel name.

**Step 3** **Mechanism**: It specifies the 4in6 tunnel implement mechanism. The modem router only supports DS-Lite.

**Step 4** **Associated WAN Interface**: Specify an associated WAN interface for the 4in6 tunnel. The WAN interface is required to use IPv6 protocol only.

**Step 5** **Associated LAN Interface**: Specify an associated LAN interface for the 6in4 tunnel.

**Step 6** Select a type of obtaining AFTR IPv6 address.

- **Manual**: Manually set an AFTR IPv6 address.
- **Automatic**: The modem router obtains the AFTR name through DHCPv6 option, and translates the AFTR name to specific IPv6 IP address through DNS. If you select **Automatic**, skip step 7.

**Step 7** **AFTR**: Specify the IPv6 AFTR address.

**Step 8** Click **Apply/Save**.

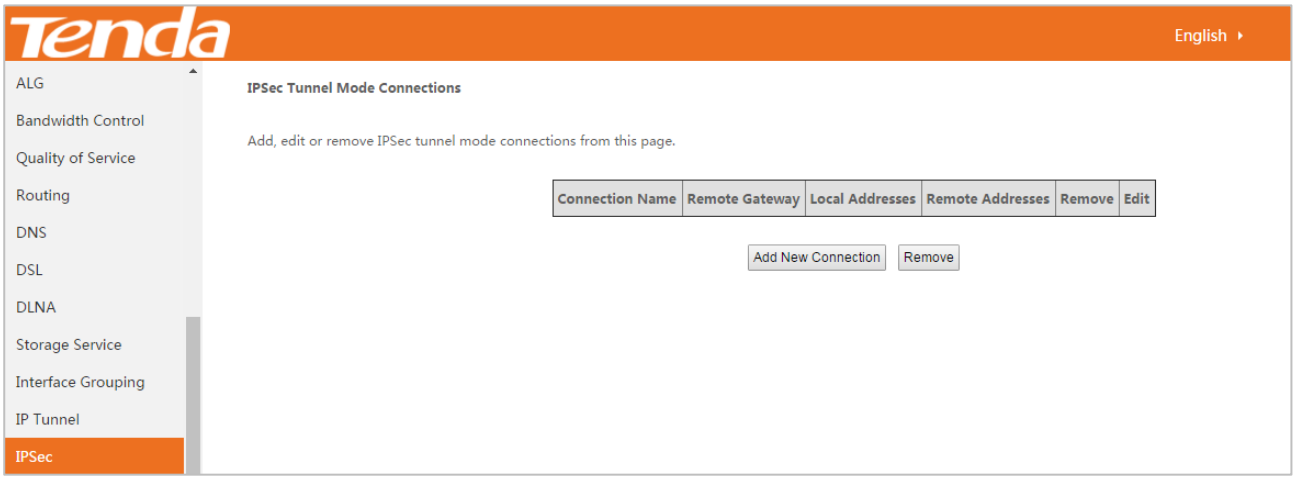
**--End**

# 4.19 IPSec

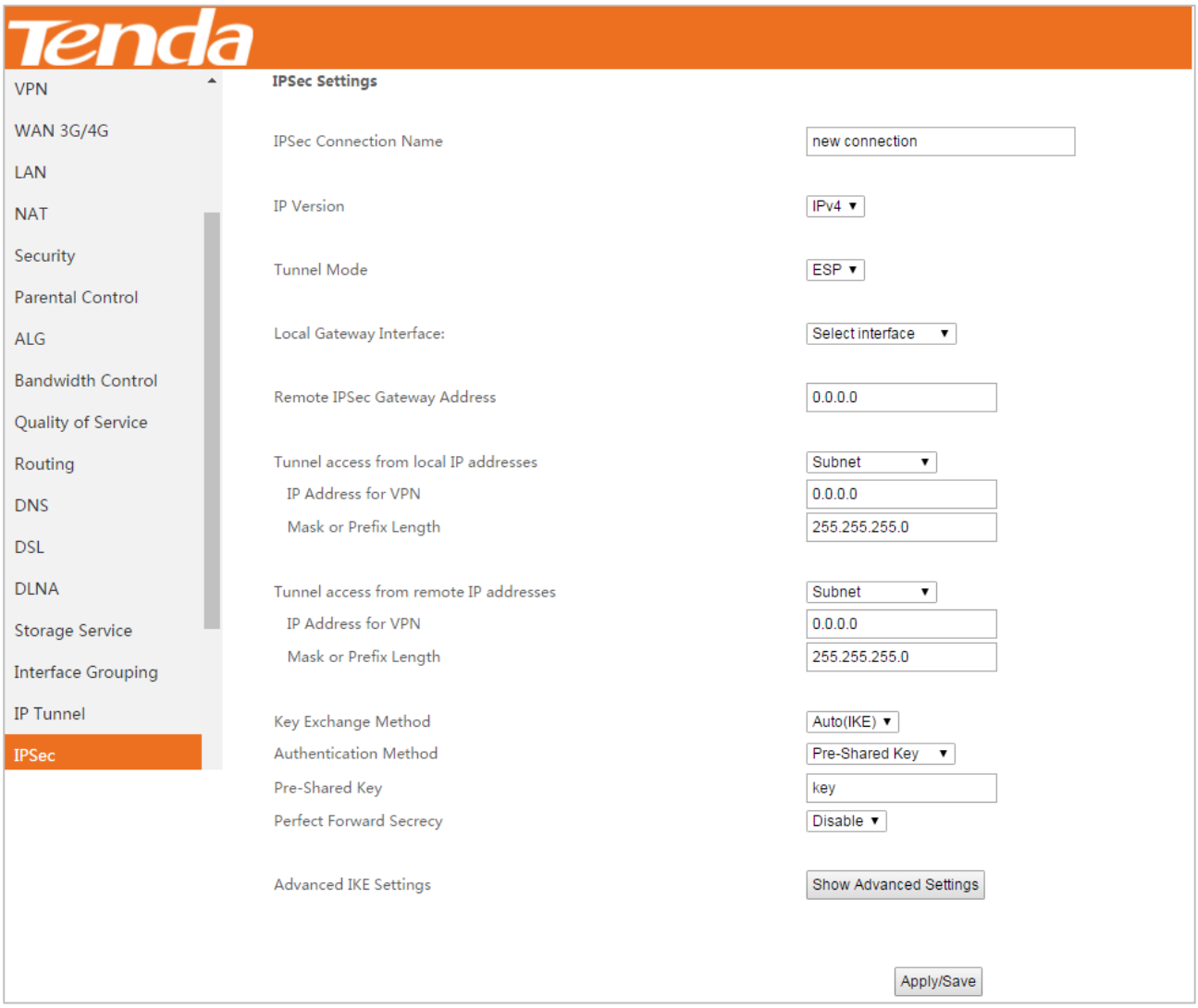
Internet Protocol Security (IPSec) is a network protocol suite that authenticates and encrypts the packets of data

sent over a network. IPsec can protect data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host). IPsec uses cryptographic security services to protect communications over Internet Protocol (IP) networks.

Choose **Advanced** > **Advanced Setup** > **IPSec** to enter the configuration page.



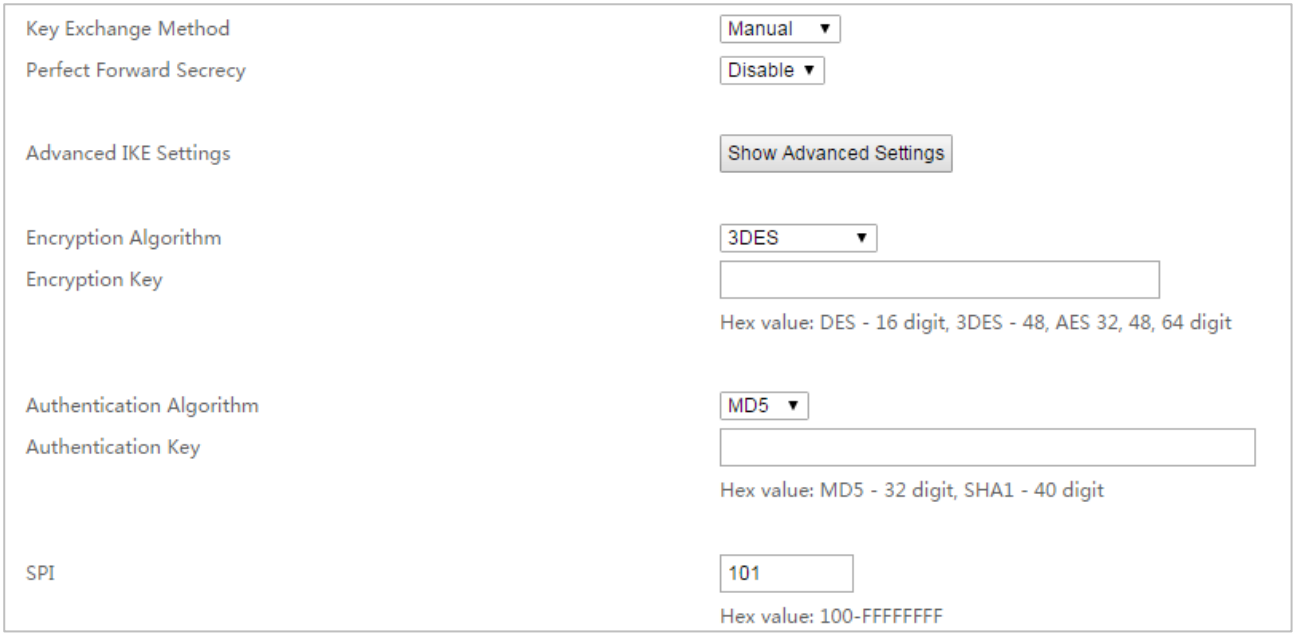

Click **Add New Connection**.



| Parameter | Description |
| --- | --- |
| IPSec Connection Name | Specify a name for the IPSec connection. |
| IP Version | Select an IP version to which the rule applies. |
| Tunnel Mode | It specifies tunnel protocol the rule uses.<br>• **ESP**: It specifies Encapsulating Security Payload. This protocol is used to test data integrity and encryption. Even the encrypted packet is intercepted, the third party also cannot obtain correct message.<br>• **AH**: It specifies Authentication Header. This protocol is used to test data integrity. If a packet is tampered during transmission, the receiver discards the packet when it performs data integrity test. |
| Local Gateway Interface | Select a WAN service for the rule. |
| Remote IPSec Gateway Address | It specifies WAN IP address or domain name of the peer device enabled IPSec function. |
| Tunnel access from local IP addresses | **Subnet**: When “Subnet” is selected, you can specify all hosts on LAN.<br>**Single Address**: When “Single Address” is selected, you can only specify one host on LAN. |
| IP Address for VPN | It specifies IP address of a local host. |
| Mask or Prefix Length | It specifies local IP network segment included all hosts on LAN. |
| Tunnel access from remote IP addresses | **Subnet**: When “Subnet” is selected, you can specify all hosts on the peer network.<br>**Single Address**: When “Single Address” is selected, you can only specify one host on the peer network. |
| IP Address for VPN | It specifies IP address of a host on peer network. |
| Mask or Prefix Length | It specifies LAN IP network segment of the peer router. |
| Key Exchange Method | It specifies key negotiation method.<br>**Auto(IKE)**: When “Auto(IKE)” is selected, the negotiation process is divided into two stages:<br>Stage 1: Both communication sides exchange verification algorithm, encryption algorithm and so on security protocols, and establish a ISAKMP (Internet Security Association and Key Management Protocol) SA (Security Association) which is used to exchange more information in stage 2.<br>Stage 2: Both communication sides take ISAKMP SA as IPSec security protocol parameters, and create IPSec SA which is used to secure data transmission.<br>IKE: It specifies internet key exchange.<br>**Manual**: Refer to Key Exchange Method-Manual. |

**Key Exchange Method-Manual**

When “Manual” is selected, the following parameters appear.

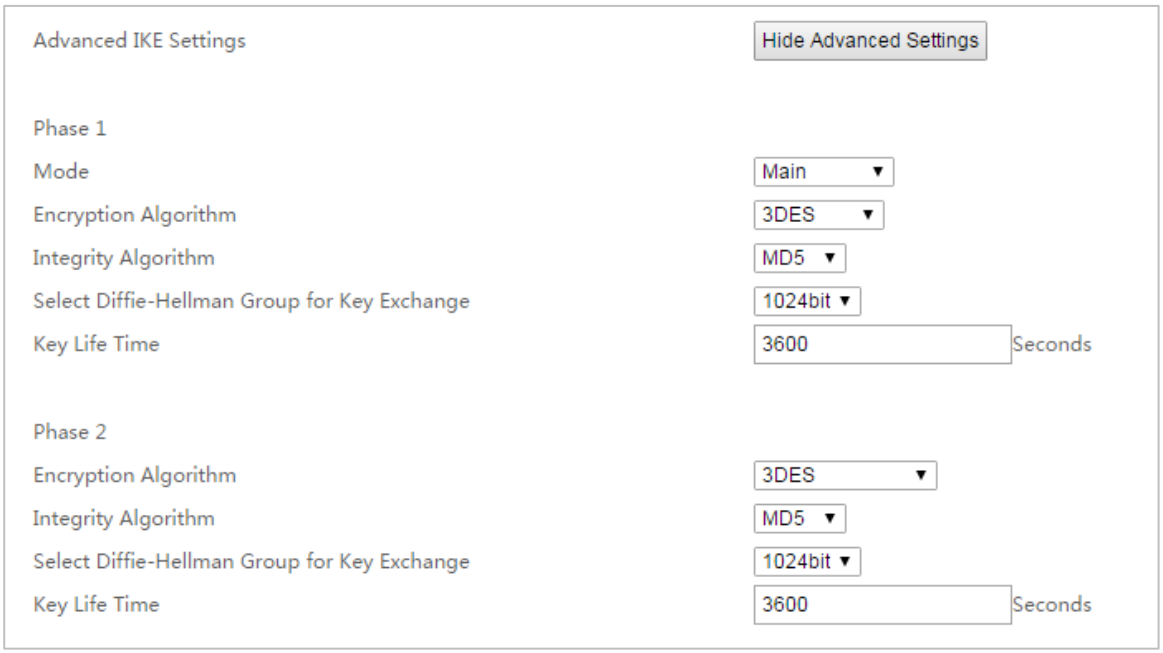



| Parameter | Description |
|---|---|
| Perfect Forward Secrecy | It specifies the property that ensures that a session key derived from a set of long-term public and private keys will not be compromised if one of the (long-term) private keys is compromised in the future.<br>Select Enable or Disable according to your needs. It is disabled by default. |
| Advanced IKE Settings | Refer to Advanced IKE Settings. |
| Encryption Algorithm | When the Tunnel Mode is set to ESP, you can configure ESP encryption algorithm.<br>The modem router supports the following encryption algorithm:<br>**DES**: It specifies Data Encryption Standard.<br>**3DES**: It specifies Triple DES.<br>**AES(aes-cbc)**: It specifies Advanced Encryption Standard. |
| Encryption Key | Specify a encryption key. Both communication sides should set it to the same one. |
| Authentication Algorithm | When the Tunnel Mode is set to AH, you can configure AH authentication algorithm.<br>The modem router supports the following authentication algorithm:<br>**MD5**: It specifies Message Digest Algorithm. The system generates a 128 bit message digest for a message.<br>**SHA1**: It specifies Secure Hash Algorithm. The system generates a 128 bit message digest for a message. |
| Authentication Key | Specify an authentication key. Both communication sides should set it to the same one. |
| SPI | It specifies Security Parameter Index. It is an identification tag added to the header while using IPsec for tunneling the IP traffic. This tag helps the kernel discern between two traffic streams where different encryption rules and algorithms may |

| | |
|---|---|
| | be in use. |

**Advanced IKE Settings**

When the Show Advanced Settings button is clicked, the following parameters appear.




| Parameter | Description |
|---|---|
| Mode | The mode should be set to the same one as that of the peer device.<br>**Main**: This mode provides identity protection, and is applicable to high requirement situation for identity protection.<br>**Aggressive**: This mode does not provide identity protection, and is applicable to not high requirement situation for identity protection. |
| Encryption Algorithm | **DES**: It specifies Data Encryption Standard.<br>**3DES**: It specifies Triple DES.<br>**AES**: It specifies Advanced Encryption Standard. AES - 128/192/256 indicates that the key length is 128/192/256 bit. |
| Integrity Algorithm | **MD5**: It specifies Message Digest Algorithm. The system generates a 128 bit message digest for a message.<br>**SHA1**: It specifies Secure Hash Algorithm. The system generates a 128 bit message digest for a message. |
| Select Diffie-Hellman Group for Key Exchange | It specifies the group information of Diffie-Hellman algorithm. It is used to generate session key encrypted IKE tunnel. |
| Key Life Time | It specifies the life time of IPSec SA. |

**Configure Procedure**

**Step 1** Choose **Advanced** > **Advanced Setup** > **IPSec** to enter the configuration page.

**Step 2** Click **Add New Connection**.

**Step 3** Specify an IPSec Connection Name which is IPSec_1 in this example.

**Step 4** Specify the IP version which is **IPv4** in this example.

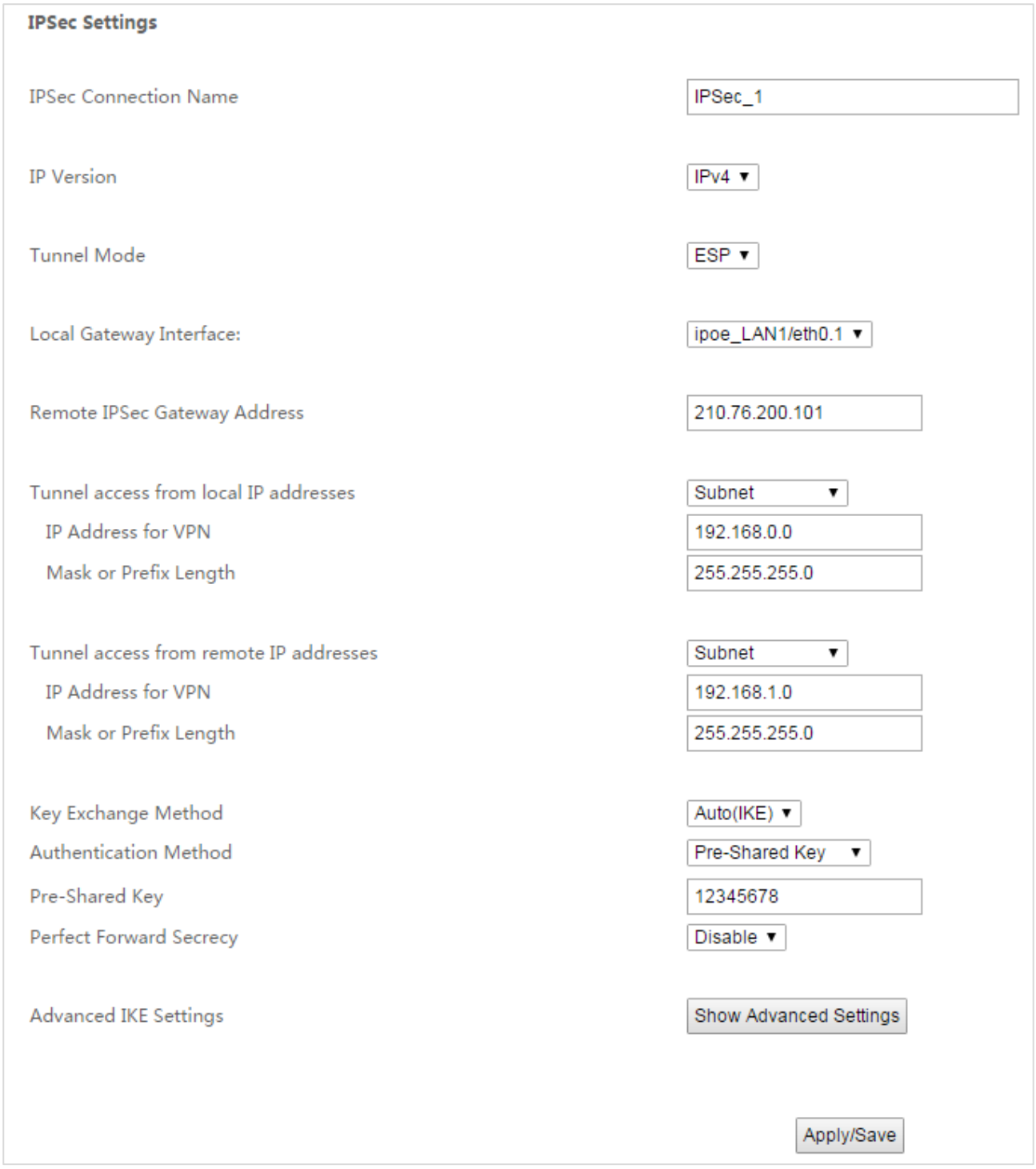
**Step 5** Specify a local gateway interface which is **ipoe_LAN1/eth0.1** in this example.

**Step 6** Enter a remote IPSec gateway address which is **210.76.200.101** in this example.

**Step 7** Set Tunnel access from local IP address to Subnet, and specify a local network segment which is **192.168.0.0** and **255.255.255.0** in this example.

**Step 8** Set Tunnel access from remote IP address to Subnet, and specify a local network segment of the peer router which is **192.168.1.0** and **255.255.255.0** in this example.

**Step 9** Specify a Pre-Shared key which is **12345678** in this example. And leave other parameters unchanged.



**Step 10** Click **Apply/Save**.

**--End**

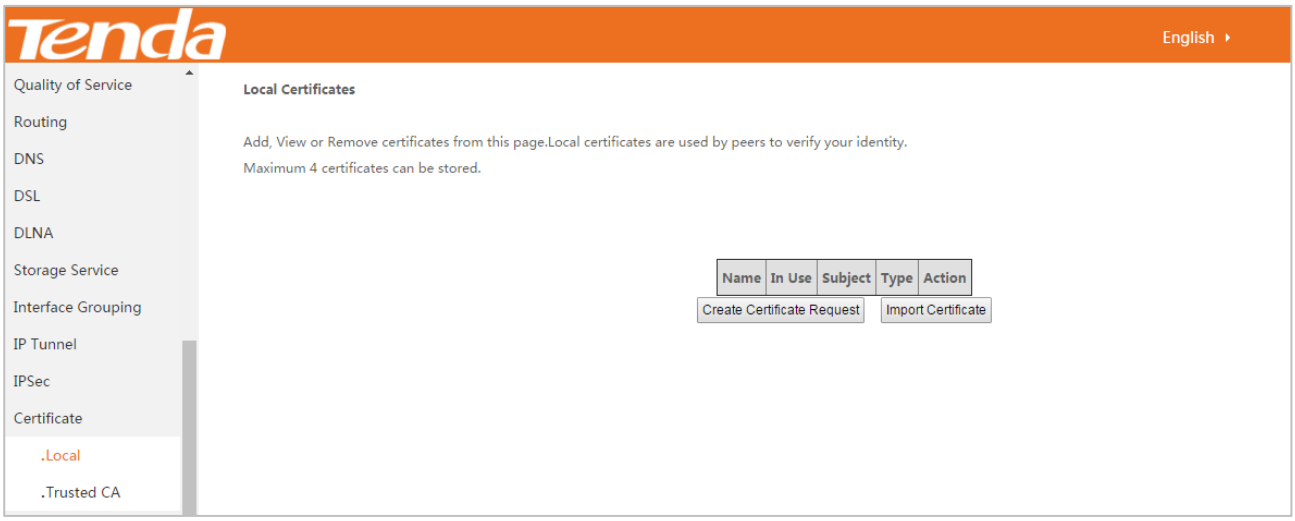
The rule is displayed in the list shown as below.


# 4.20 Certificate

## 4.20.1 Local

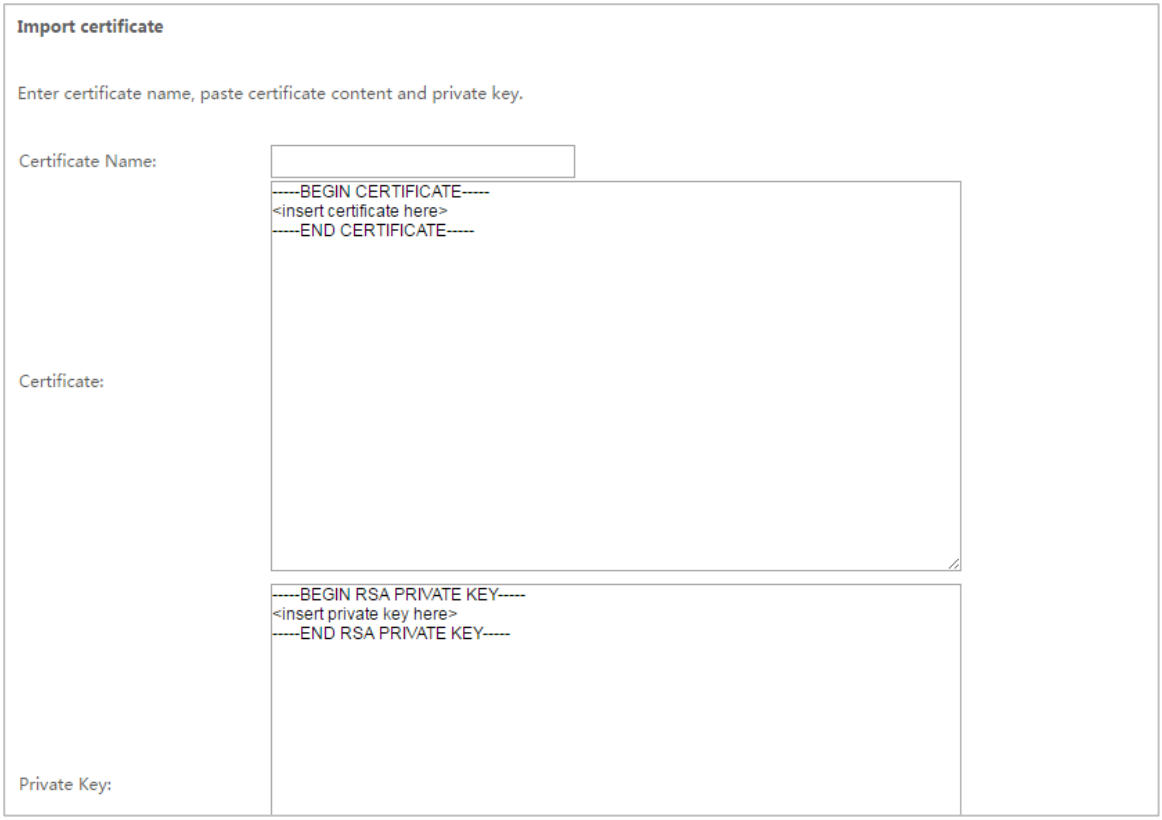
Apply or import a certificate for the modem router which is used to authenticate the identity of the modem router.

Choose **Advanced** > **Advanced Setup** > **Certificate > Local** to enter the configuration page.




To import a certificate, perform the following procedure:

**Step 1** Click **Import Certificate**.




**Step 2** **Certificate Name**: Enter the name of applied certificate.

**Step 3** **Certificate**: Open the certified certificate with notepad .exe, and copy the content to the text box.

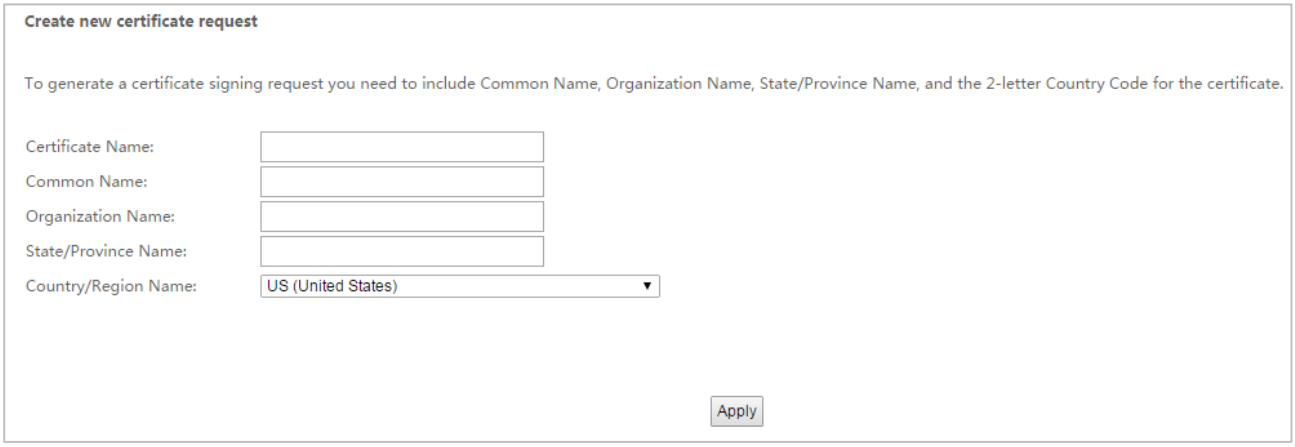
**Step 4** **Private Key**: Copy the private key information which is generated when you apply the certificate to the box.

**Step 5** Click **Apply**.

**--End**

To create a new certificate, perform the following procedure:

**Step 1** Click **Create Certificate Request**.




**Step 2** **Certificate Name**: Specify a name for the certificate, such as **mycertificate**.

**Step 3** **Common Name**: Enter the website domain name, company name or name of the applicant, such as **Tendacn.com**, **Tenda** or **Lucy**.

**Step 4** **Organization Name**: Enter the name of an organization/company, such as **Tenda**.

**Step 5** **State/Province Name**: Enter the state or province where the certificate is to be used.

**Step 6** **Country/Region Name**: Select the country where the certificate is to be used.

**Step 7** Click **Apply**.

**--End**

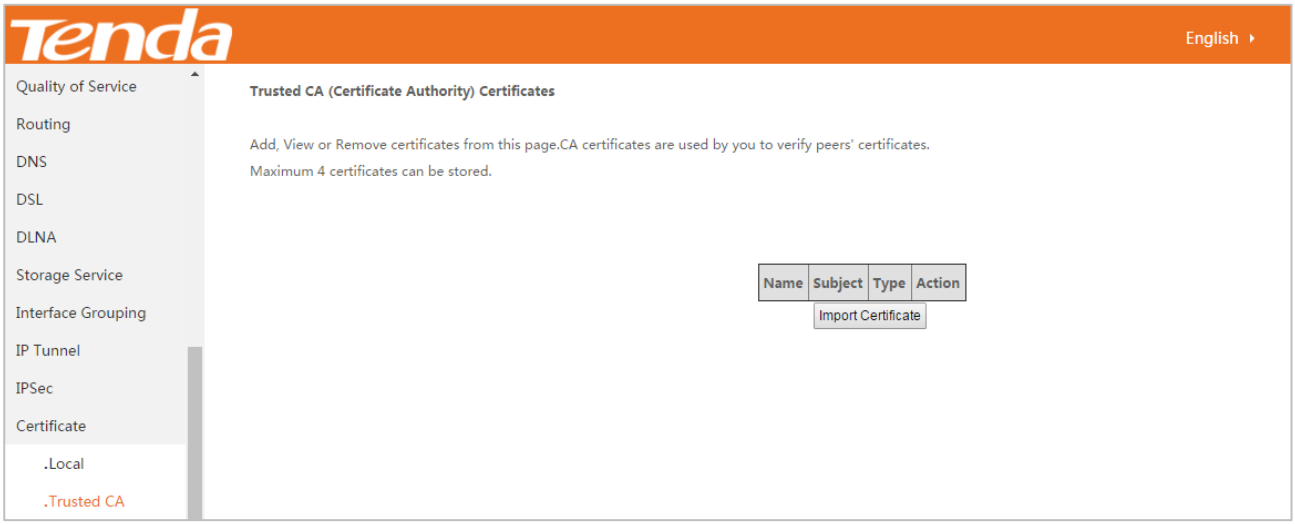
Then wait for the CA to deal with the application, sign and load the signature certificate to the modem router.


- **View:** Views the details of the certificate.
- **Load Signed**: To import and apply the certificate.
- **Remove**: To delete the certificate.

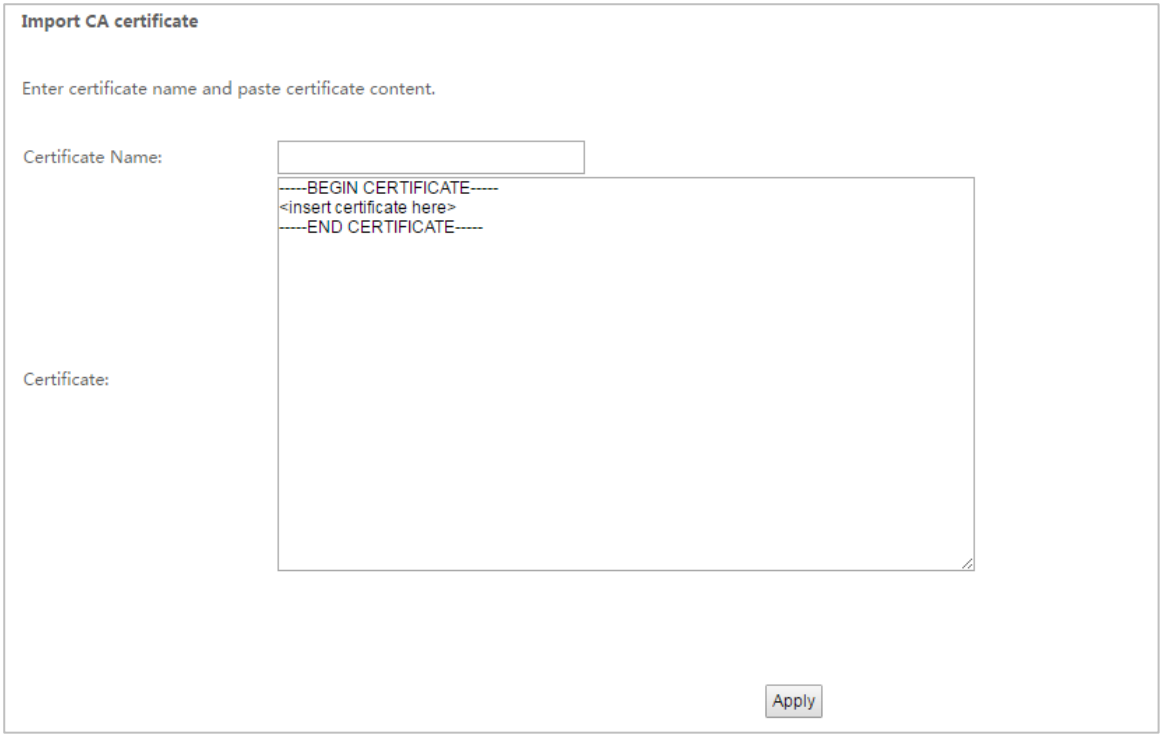
## 4.20.2 Trusted CA

This function is used to import certificates from trusted CAs to authenticate the identity of the modem router.

Choose **Advanced** > **Advanced Setup** > **Certificate > Trusted CA** to enter the configuration page.




To import a certificate, perform the following procedure:




**Step 1** Click Import Certificate.

**Step 2** **Certificate Name**: Enter the name of the certificate.

**Step 3** **Certificate:** Enter the content of the certificate.

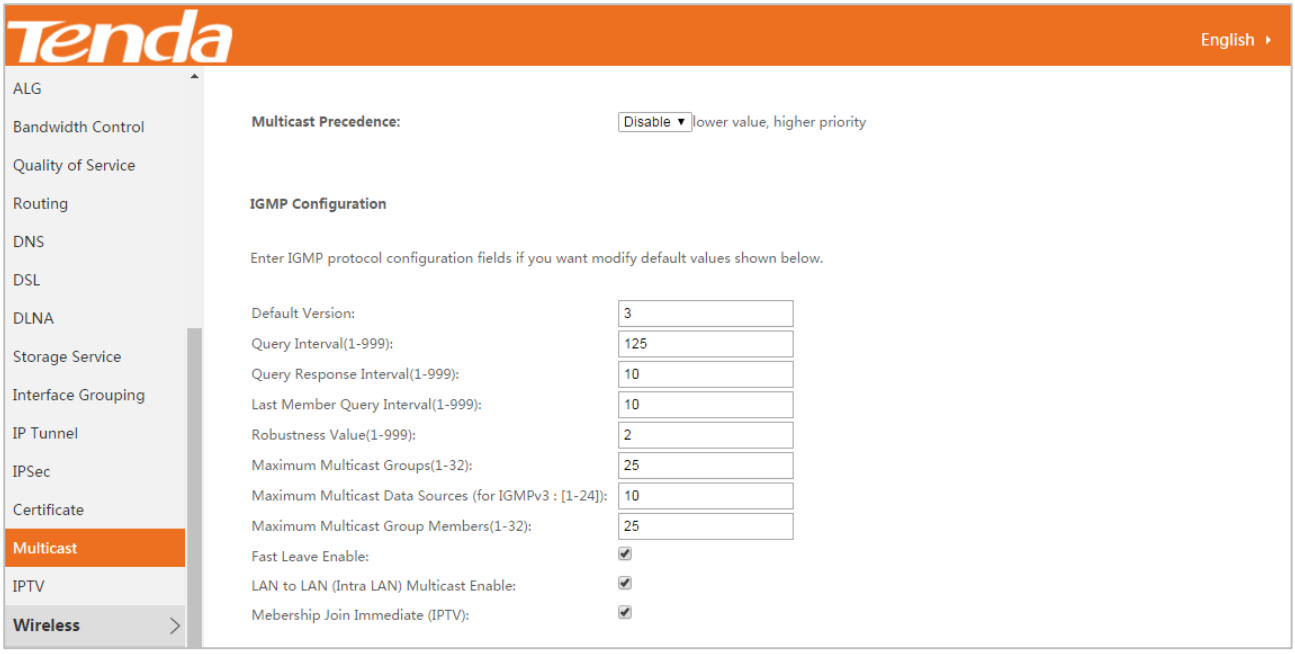
**Step 4** Click **Apply**.

**--End**

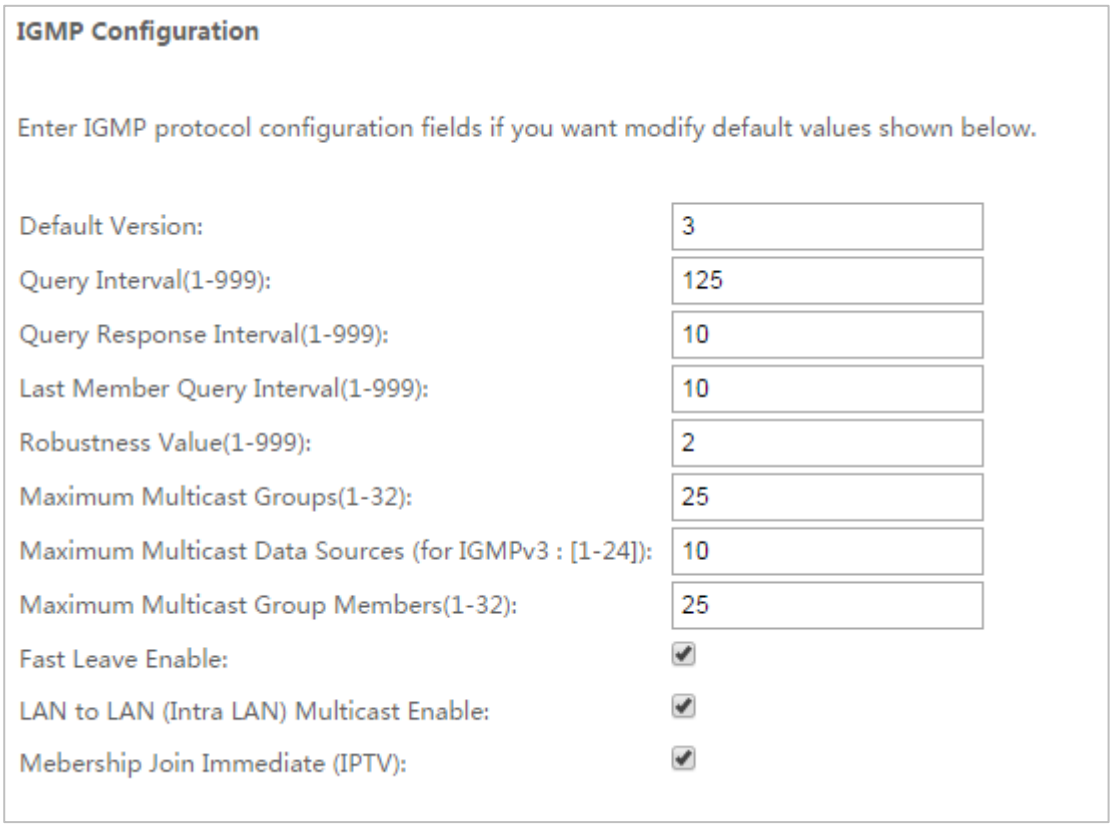
# 4.21 Multicast

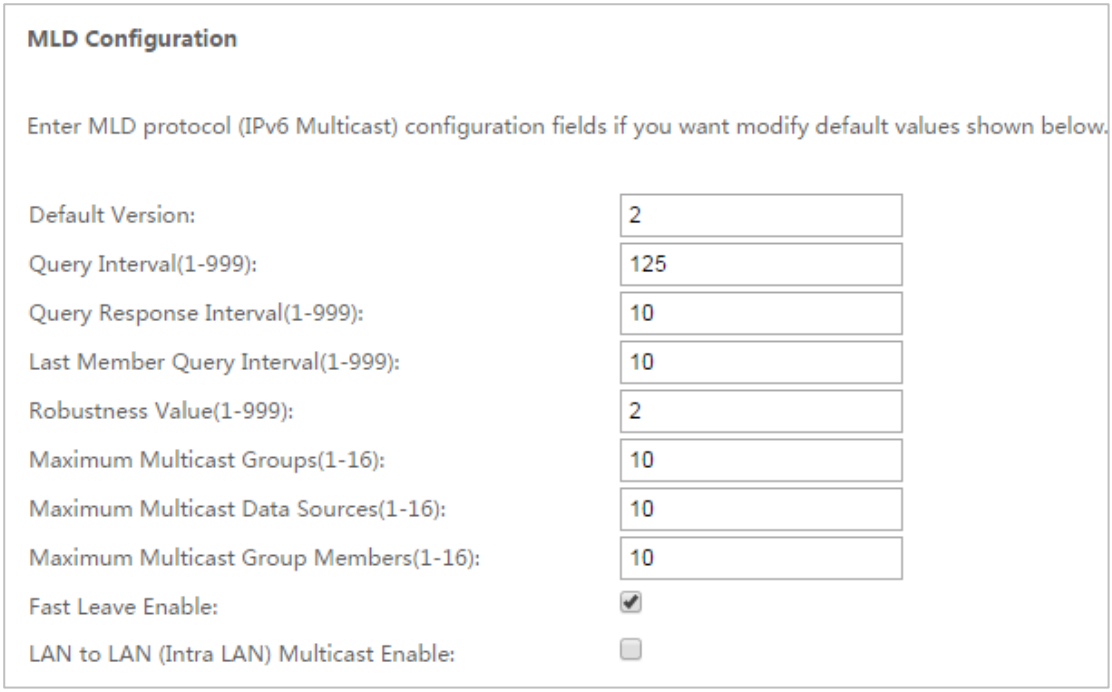
Multicast (one-to-many or many-to-many distribution) is group communication where information is addressed to a group of destination computers simultaneously. Multicast can be used for one-to-many networking applications such as online streaming video and gaming, and allows more efficient use of resources when supporting these types of applications.

To configure multicast function, choose **Advanced** > **Advanced Setup** > **Multicast**.




**Multicast Precedence**: Set the priority for the multicast data. A smaller value indicates a higher priority.

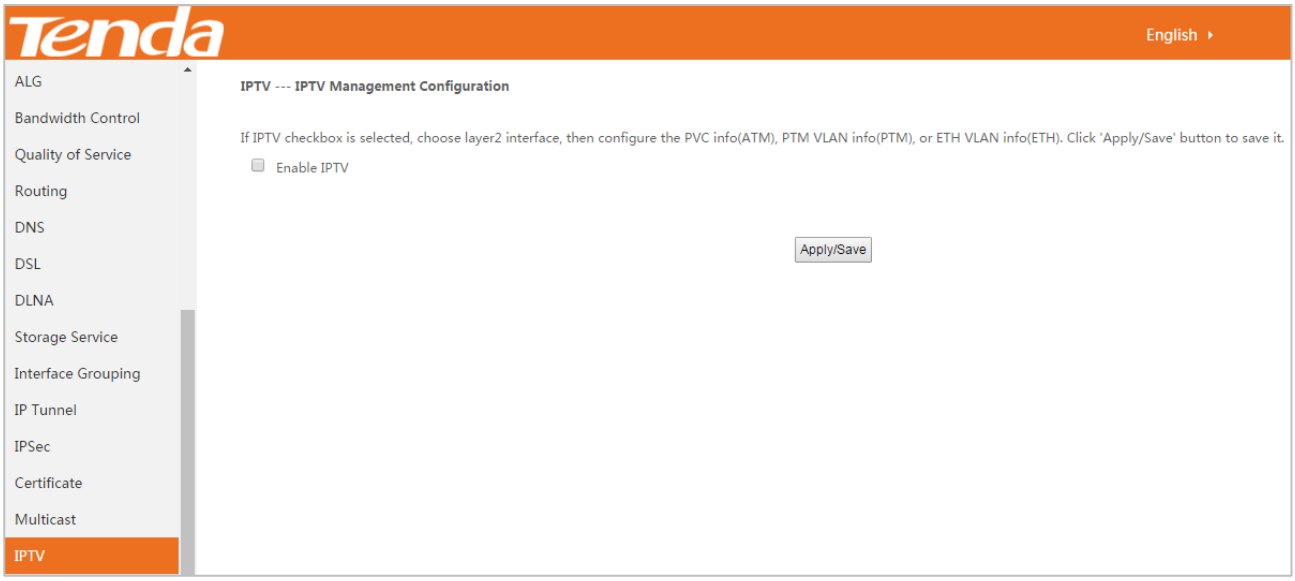





| Parameter | Description |
|---|---|
| Default Version | It specifies the IGMP (MLD) version for WAN. The default is IGMPv3 (MLDv2). |
| Query Interval (1-999) | It specifies the interval for sending IGMP (MLD) query message. The default is 125. The value range is 1 to 999. The unit is “0.1 second”. |
| Query Response Interval (1-999) | It specifies the response interval for the query message. The default is 10. The value range is 1 to 999. The unit is “second”. |
| Last Member Query Interval (1-999) | It specifies the interval for sending query message of specified group. The default is 10. The value range is 1 to 999. The unit is “second”. |
| Robustness Value (1-999) | It specifies the robustness value of IGMP (MLD) querier. The default is 2. The value range is 1 to 999. |
| Maximum Multicast Groups (1-32) | It specifies the maximum number of multicast groups for each interface. The default is 25. The value range is 1 to 32. |
| Maximum Multicast Data Sources (for IGMPv3: [1-24]) | It specifies the maximum number of multicast data sources. The default is 10. The value range is 1 to 24. |
| Maximum Multicast Group Members (1-32) | It specifies the maximum number of multicast group members. |
| Fast Leave Enable | If the function is enabled, the modem router does not send group specific-queries when it receives a leave message. |
| LAN to LAN (Intra LAN) Multicast Enable | This function is useful when you want to use multicast data source of LAN as well as IGMP (MLD) interception. |

# 4.22 IPTV

Choose **Advanced** > **Advanced Setup** > **IPTV** to enter the configuration page.

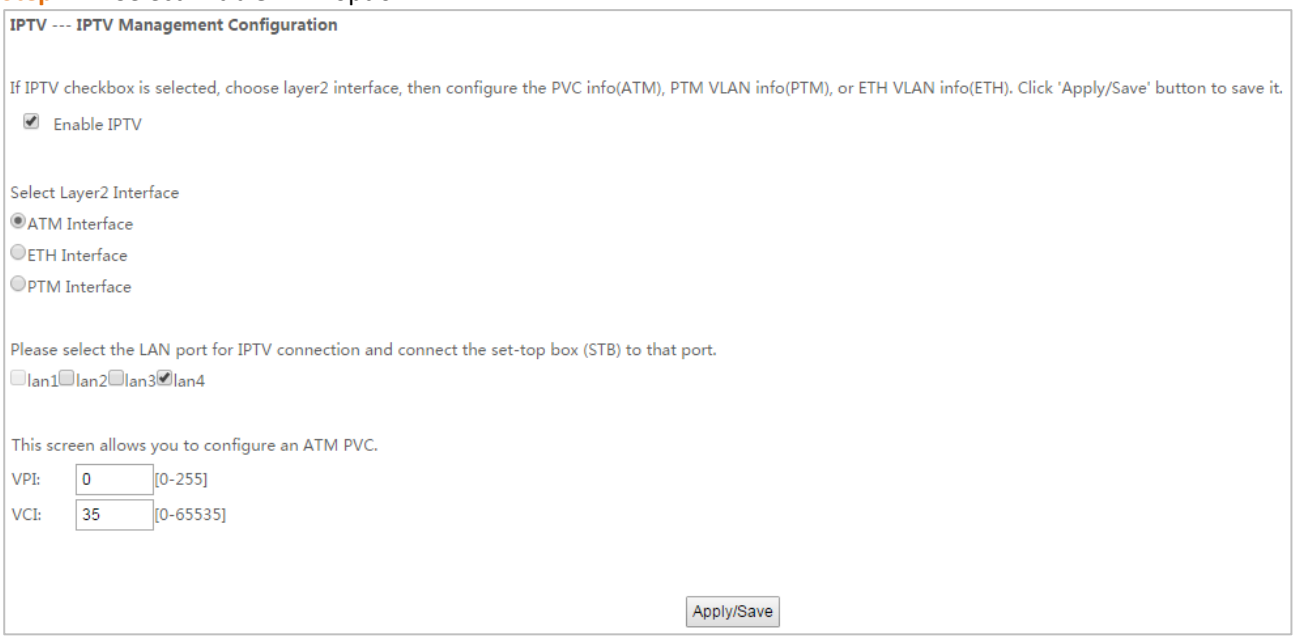



To configure the IPTV function, select one to follow according to the interface you create in Layer2 Interface.

## ATM Interface

If you create **ATM Interface**, perform the following procedure:

**Step 1** Select **Enable IPTV** option.




**Step 2** Select ATM Interface.

**Step 3** Select a LAN port to serves as an IPTV port for connecting to the set-top box. The default IPTV is port 4.

**Step 4** Enter valid VPI/VCI value provided by your ISP.

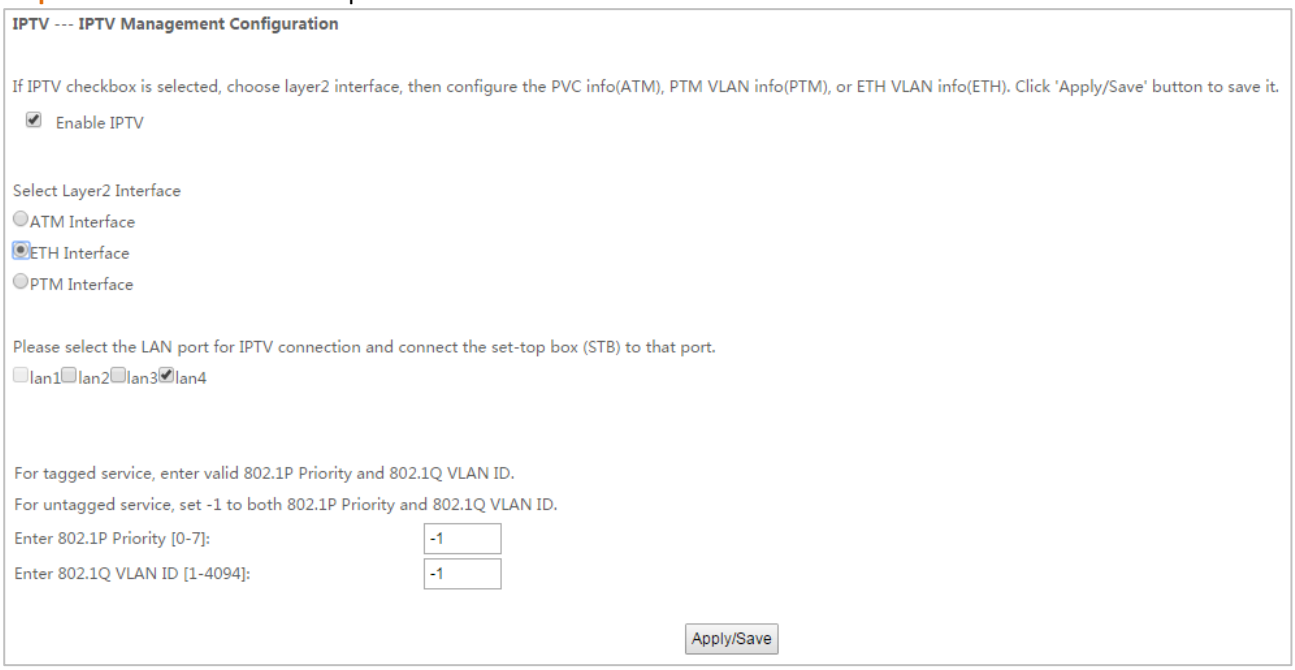
**Step 5** Click Apply/Save.

**--End**

# ETH Interface

If you create **Ethernet Interface**, perform the following procedure:

**Step 1** Select **Enable IPTV** option.




**Step 2** Select Ethernet Interface.

**Step 3** Select a LAN port to serves as an IPTV port for connecting to the set-top box. The default IPTV is port 4.

**Step 4** Enter 802.1P priority and 802.1Q VLAN ID values provided by your ISP.

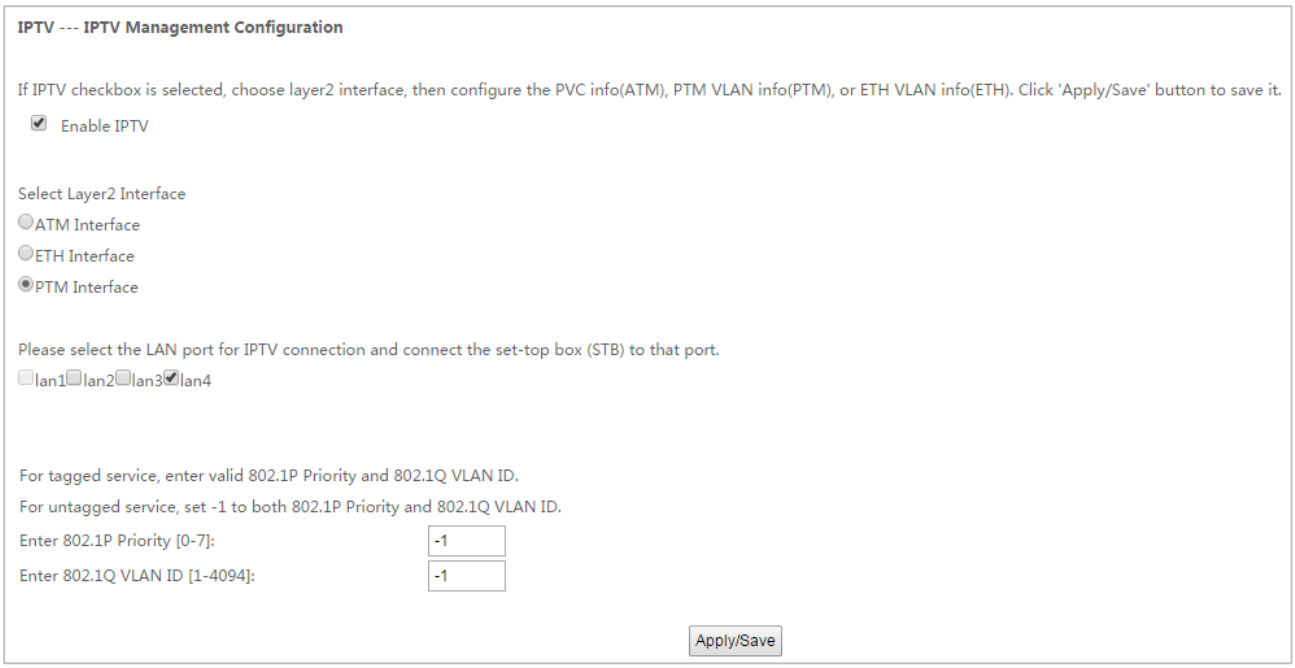
**Step 5** Click Apply/Save.

**--End**

# PTM Interface

If you create **PTM Interface**, perform the following procedure:

**Step 1** Select **Enable IPTV** option.




**Step 2** Select PTM Interface.

**Step 3** Select a LAN port to serves as an IPTV port for connecting to the set-top box. The default IPTV is port 4.

**Step 4** Enter the 802.1P priority and 802.1Q VLAN ID values provided by your ISP.

**Step 5** Click Apply/Save.

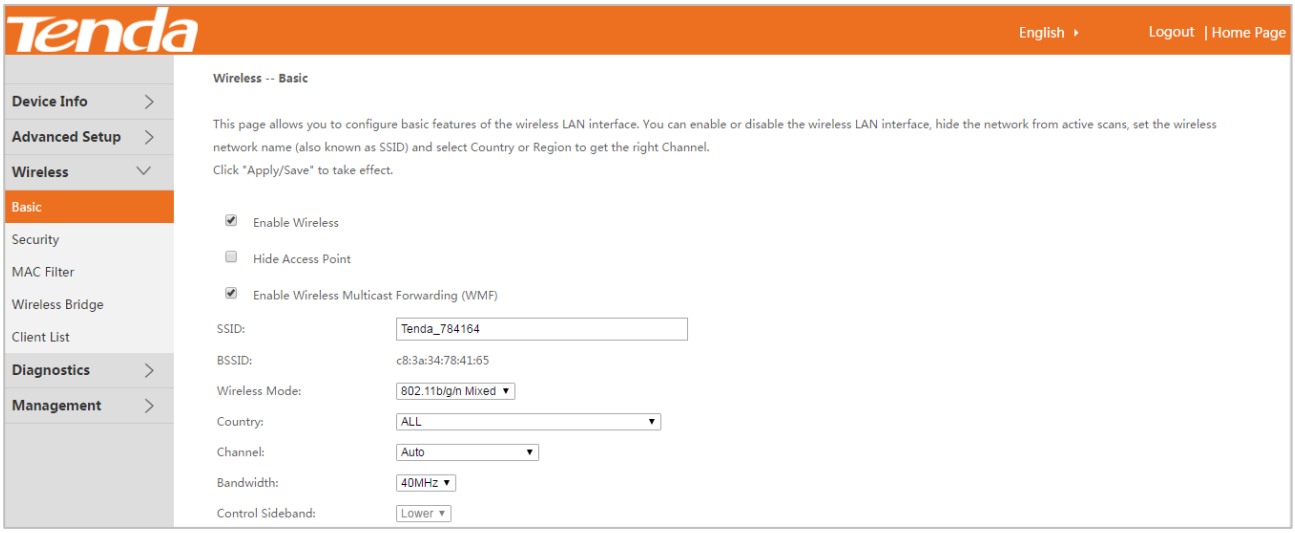
**--End**

# 5 Wireless

## 5.1 Basic

This section allows you to configure basic features of the wireless network.

Choose **Advanced** > **Wireless** > **Basic** to enter the configuration page.

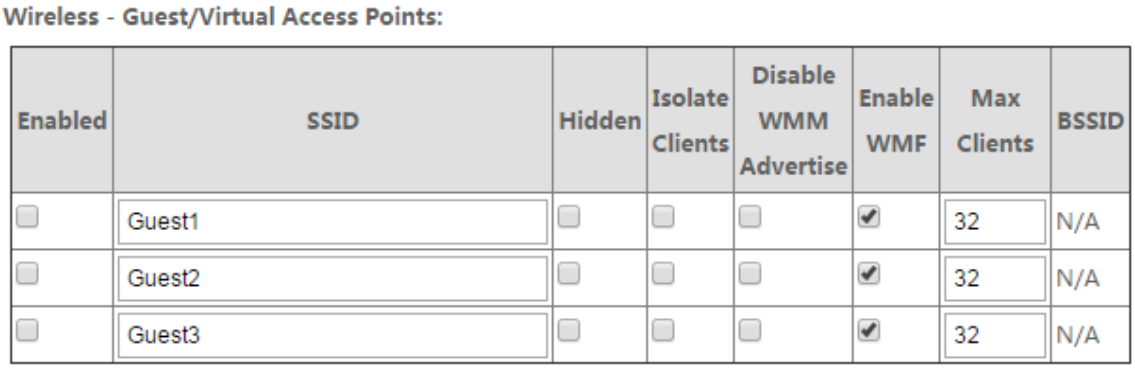



| Parameter | Description |
|---|---|
| Enable Wireless | Select the option to enable the wireless function. |
| Hide Access Point | Select the option to hide the SSID of the modem router. In this case, wireless clients cannot find the SSID (wireless network name) of the modem route. The SSID must be manually entered on the wireless clients for connecting the clients to the modem router. |
| SSID | Wireless network name of the modem router. |
| BSSID | MAC address of the wireless network. |
| Wireless Mode | • If 802.11b is selected, only 11b wireless devices can connect to the wireless network. The maximum wireless rate supported in this mode is 11 Mbps.<br>• If 802.11g is selected, only 11g wireless devices can connect to the wireless network. The maximum of 54 Mbps wireless rate is supported in this mode.<br>• If 802.11n is selected, only 11n wireless devices can connect to the wireless network. The maximum of 300 Mbps wireless rate is supported in this mode.<br>• If 802.11b/g Mixed is selected, only 11b or 11g wireless devices can connect to the wireless network. The maximum of 54 Mbps wireless rate is supported in this mode.<br>• If 802.11b/g/n Mixed is selected, 11b, 11g or 11n wireless devices can connect to the wireless network. The maximum of 300 Mbps wireless rate is supported in |

| | |
|---|---|
| | this mode. |
| Country | Select your country. |
| Channel | Select a channel in which the modem router works. Auto indicates that the modem router automatically changes to a channel rarely used in the ambient environment to prevent interference. |
| Bandwidth | Select a frequency band of the channel of the modem router. |

## Enabling multiple SSID

To enable multiple SSIDs, choose **Advanced** > **Wireless** > **Basic** to enter the configuration page.




**Step 1** Select **Enable** option to enable the corresponding SSID.

**Step 2** Specify a name for the SSID.

**Step 3** **Hidden:** It specifies whether to hide the SSID. If the option is selected, wireless devices cannot find the SSID.

**Step 4** **WMM:** WMM (Wi-Fi Multimedia) is a Wi-Fi Alliance interoperability certification based on the IEEE 802.11e standard. It provides basic quality of service (QoS) features to IEEE 802.11 networks.

**Step 5** **WMF:** It specifies whether to forward multicast packets through unicast tunnels. Generally, multicast packets are transmitted at the lowest rate, such as 1 Mbps, leading to poor transmission efficiency. WMF leverages the auto-negotiated high rate, reliable feedback mechanism, and other advantages of unicast packets to address multicast problems such as video playback stalls caused by packet loss and long delays over a wireless network.

**Step 6** Specify the maximum number of wireless clients that can be connected to this SSID.

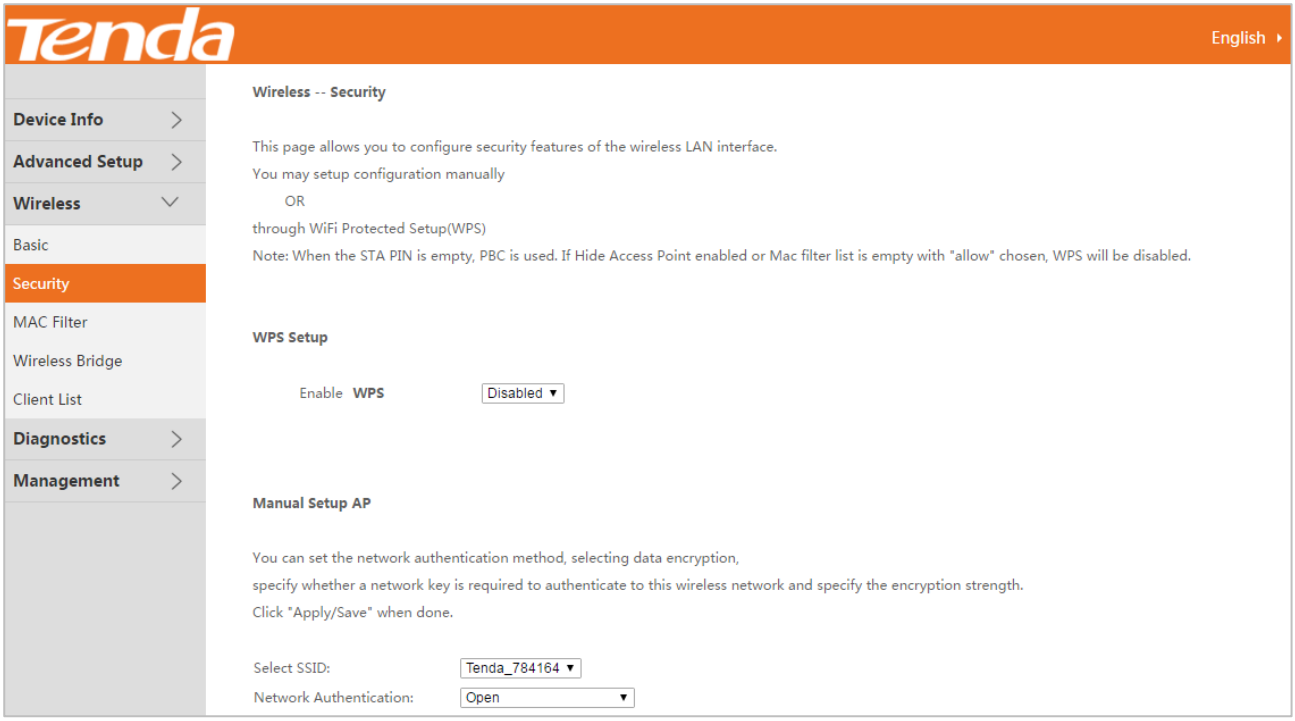
**Step 7** Click Apply/Save.

**--End**

# 5.2 Security

This section allows you to configure security features of the wireless network.

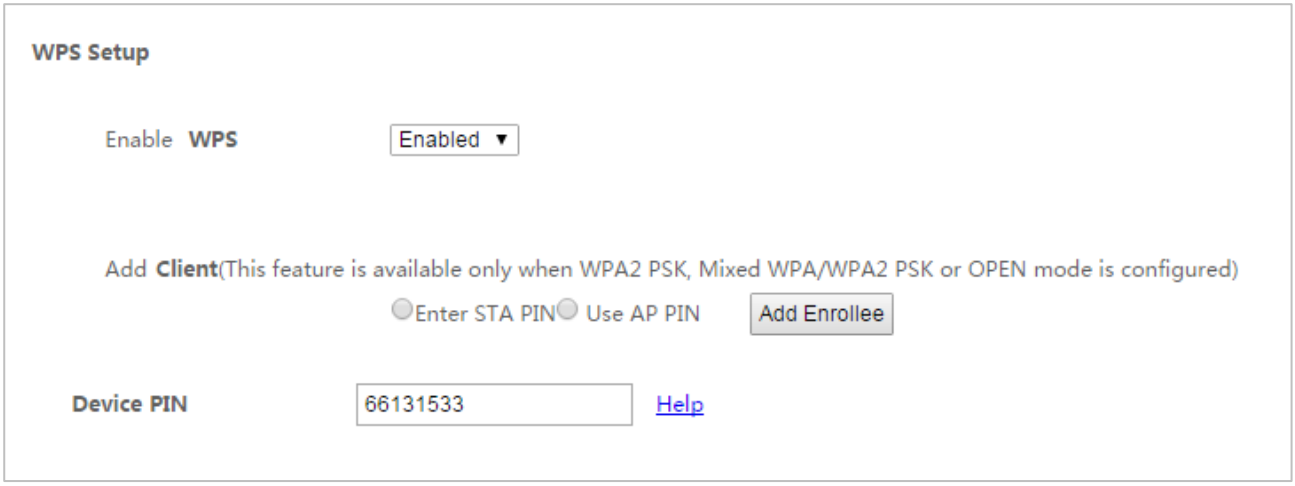
Choose **Advanced** > **Wireless** > **Security** to enter the configuration page.




## 5.2.1 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. They can set up network connections simply by entering a PIN code on the device web interface or pressing hardware WPS button (on the back panel of the device).

Select **Enabled** to enable the WPS function.




If the wireless network of the modem router is not encrypted, or the wireless network is encrypted but you forget or do not want to enter the complicated password, you can use WPS function to encrypt or connect clients to it quickly. There are three options for you:

### Option 1: PBC Negotiation

**Step 1** Choose **Advanced** > **Wireless** > **Security** to enter the configuration page.

**Step 2** Select **Enabled** to enable the function.

**Step 3** Click **Apply/Save** on the bottom of this page.


**Step 4** Press the WPS hardware button on the rear panel of the modem router for 3 seconds, and then release it. (The WPS LED indicator starts blinking)

**Step 5** Within 2 minutes, enable the WPS negotiation function on your wireless device.

**--End**

When the WPS LED turns to solid green, it indicates that the PBC negotiation is successful. The wireless device is connected to the modem router, and the wireless network is encrypted.

## Option 2 Using the WPS PIN Code of the Wireless Device

**Step 1** Log in to the web UI of the modem router, choose **Advanced** > **Wireless** > **Security** to enter the configuration page.

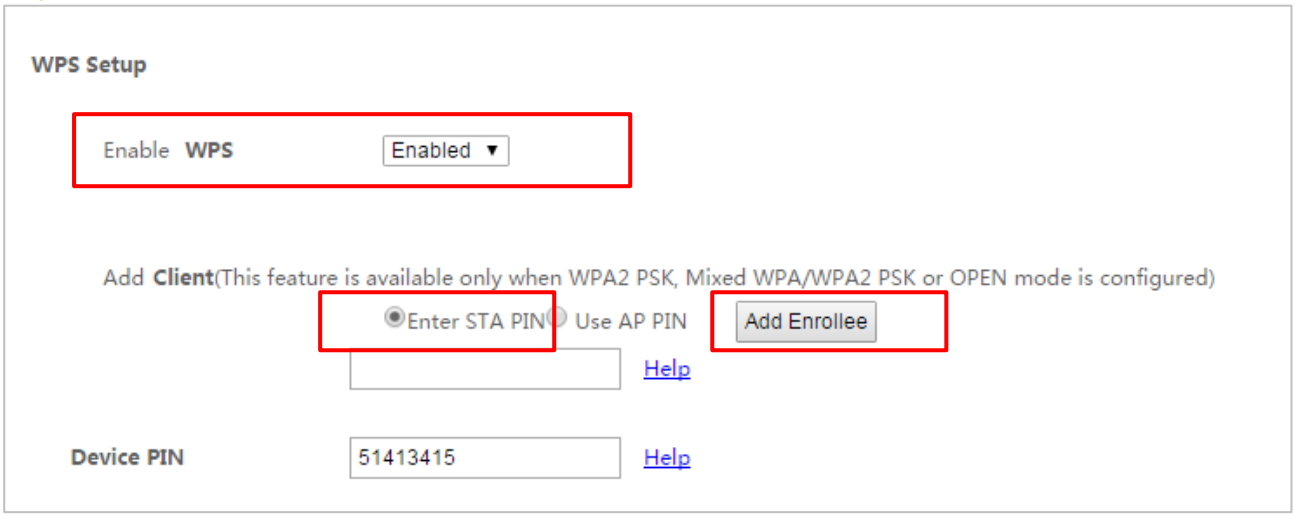
**Step 2** Select **Enabled** to enable the function.

**Step 3** Click **Apply/Save** on the bottom of this page.

**Step 4** Select Enter STA PIN.

**Step 5** Check the WPS PIN code of your wireless device and enter it to the blank box on the WPS Setup page of the web UI.

**Step 6** Click Add Enrollee.




**--End**

The WPS LED indicator blinks for about 2 minutes, and then turns to solid green. It indicates that the wireless

device is connected to the modem router, and the wireless network is encrypted.

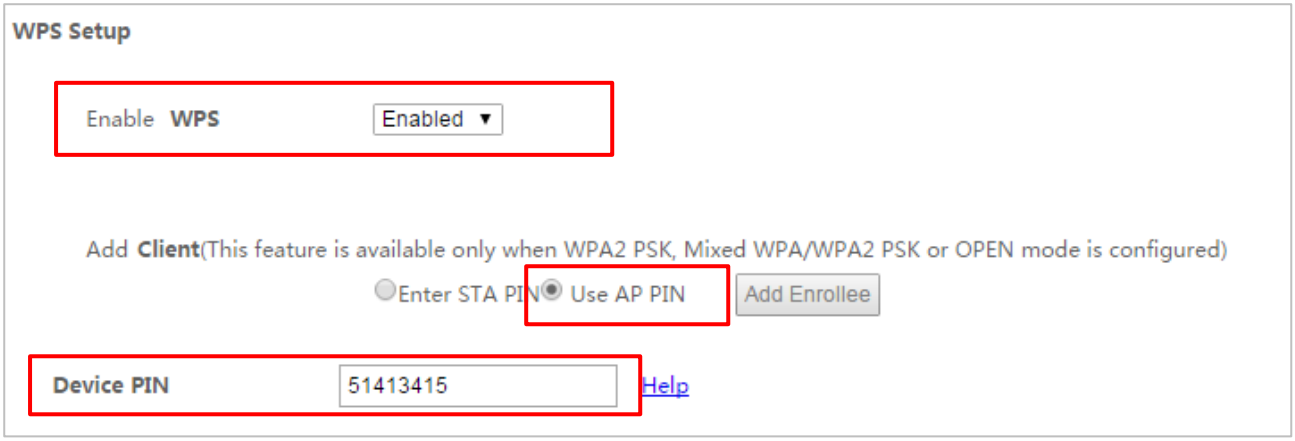
### Option 3 Using the WPS PIN Code of the Modem Router

**Step 1** Log in to the web UI of the modem router, choose **Advanced** > **Wireless** > **Security** to enter the configuration page.

**Step 2** Select **Enabled** to enable the function.

**Step 3** Click **Apply/Save** on the bottom of this page.

**Step 4** Select Use AP PIN.



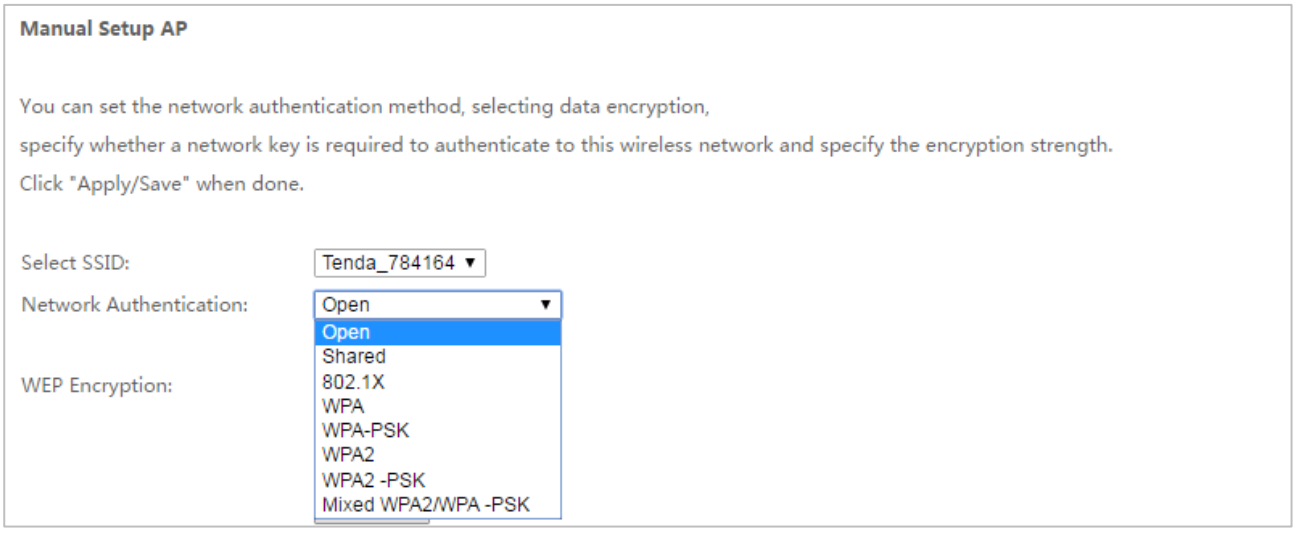

**Step 5** Enter the **Device PIN** on your wireless device.

**--End**

When the WPS LED turns to solid on, the negotiation process is successful and the SSID and password are changed to random ones.

## 5.2.2 Manual Setup AP

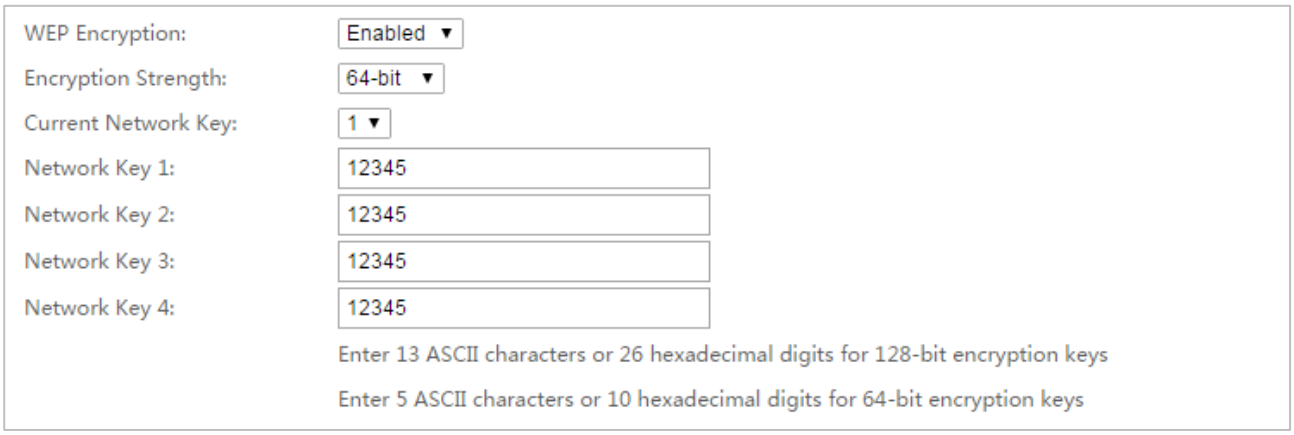
This part allows you to manually configure the encryption settings for the wireless network.




### Open/Shared/802.1X

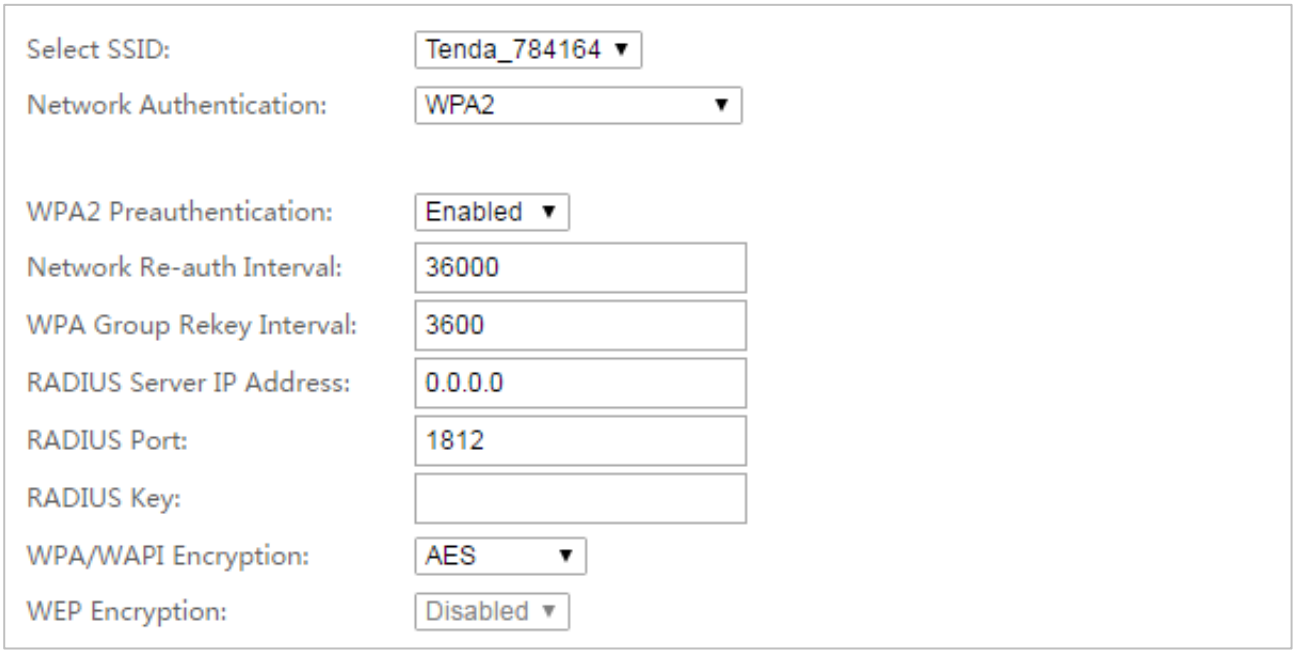
Open/Shared/802.1X supports WEP encryption.

WEP is a security mode for data exchange between two devices. Wireless speed can reach 54Mbps if WEP is used.



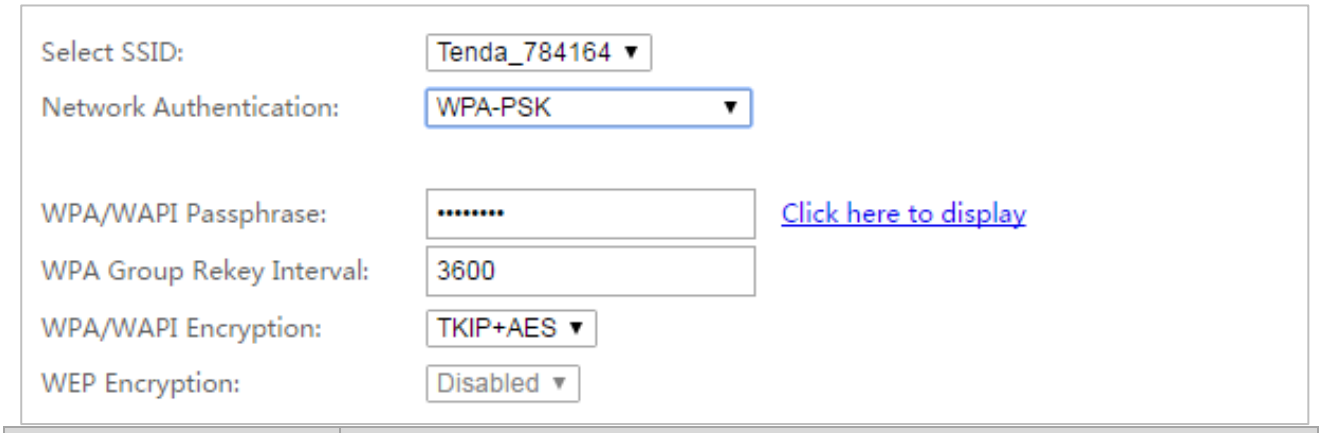

| Parameter | Description |
|---|---|
| WEP Encryption | When the **Open** option is selected, you can enable or disable WEP encryption. But if Shared or 802.1X option is selected, the WEP encryption is enabled by default.<br>For better network security, this kind of encryption is not suggested. |
| Encryption Strength | Select 128-bit or 64-bit according to your needs. |
| Current Network Key | Select a network key to be used. |
| Network Key 1/2/3/4 | Enter 13 ASCII characters or 26 hexadecimal digits as a 128-bit encryption key; enter 5 ASCII characters or 10 hexadecimal digits as a 64-bit encryption keys. |

## WPA/WPA2



| Parameter | Description |
| --- | --- |
| WPA/WPA2 | They specify the security modes implemented based on a shared key. |
| WPA Group Rekey Interval | It specifies an interval at which a WPA key is updated. A shorter interval leads to higher security. The value 0 indicates that no key update is performed. |
| RADIUS Server IP Address | It specifies the IP address of the RADIUS server for authentication. |
| RADIUS Port | It specifies the authentication port of the RADIUS server. The default port number is 1812. |
| RADIUS Key | It specifies a shared password of the RADIUS server, which consists of 1 to 64 ASCII characters. |
| WPA/WAPI Encryption | It specifies an algorithm for WPA encryption.<br>• AES: If selected, AES enabled wireless clients can join your wireless network.<br>• TKIP+AES: If selected, both AES and TKIP enabled wireless clients can join your wireless network. |

## WPA-PSK/WPA2-PSK/Mixed WPA-PSK/WPA2-PSK

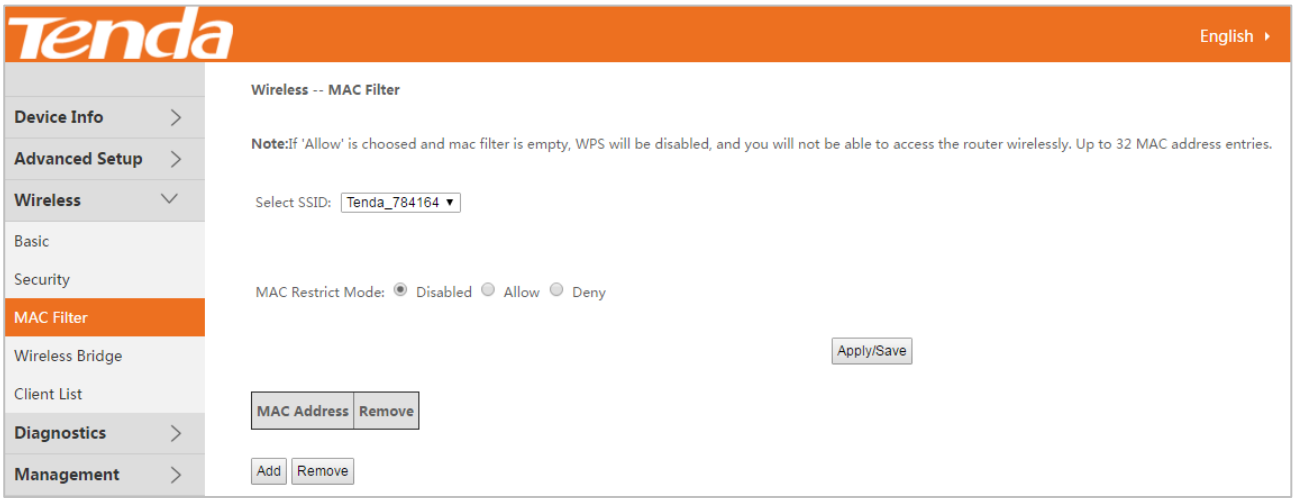



| Parameter | Description |
| --- | --- |
| WPA-PSK/WPA2PSK/ Mixed WPA-PSK/WPA2PSK | They specify the security modes implemented based on a shared key. |
| WPA/WAPI Passphrase | It specifies the password of the wireless network. |
| WPA Group Rekey Interval | It specifies an interval at which a WPA key is updated. A shorter interval leads to higher security. The value 0 indicates that no key update is performed. |
| WPA/WAPI Encryption | It specifies an algorithm for WPA encryption.<br>• AES: If selected, the maximum wireless speed can reach 300Mbps.<br>• TKIP+AES: If selected, both AES and TKIP enabled wireless clients can join your wireless network. |

# 5.3 MAC Filter

The MAC-based wireless access control feature can be used to allow or disallow clients to connect to your wireless network.

Choose **Advanced** > **Wireless** > **MAC Filter** to enter the configuration page.




| Parameter | Description |
|---|---|
| Select SSID | Select a SSID to which the rule is applied.<br>The rule is only applicable to the devices connected to the modem router wirelessly. |
| MAC Restrict Mode | **Disabled**: Disable this feature. |
| | **Allow**: To allow only devices with specified MAC addresses (in the list) to connect to your wireless network. |
| | **Deny**: To disallow only devices with specified MAC addresses (in the list) to connect to your wireless network. |
| MAC Address | The MAC address of a device to which a MAC filter rule is applied. |
| Add | Used to add a rule. |
| Remove | Used to remove the rule. |

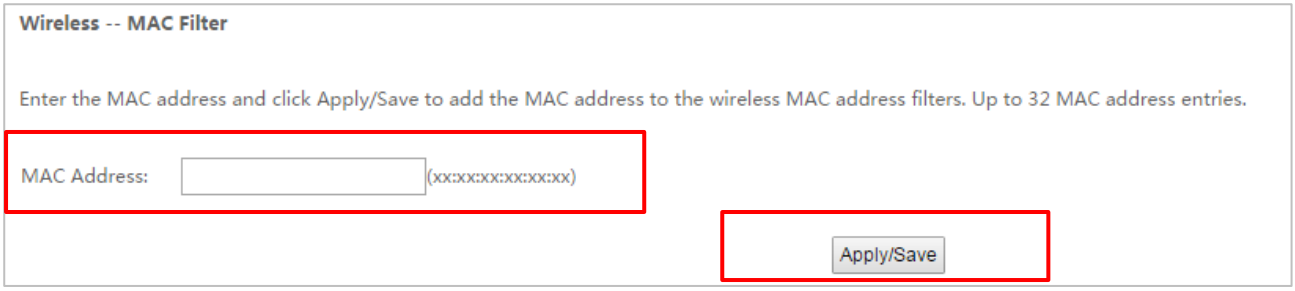
To add a MAC filter rule, perform the following procedure:

**Step 1** Select a SSID to apply the rule if you enable multiple SSIDs.

**Step 2** Click **Add**.

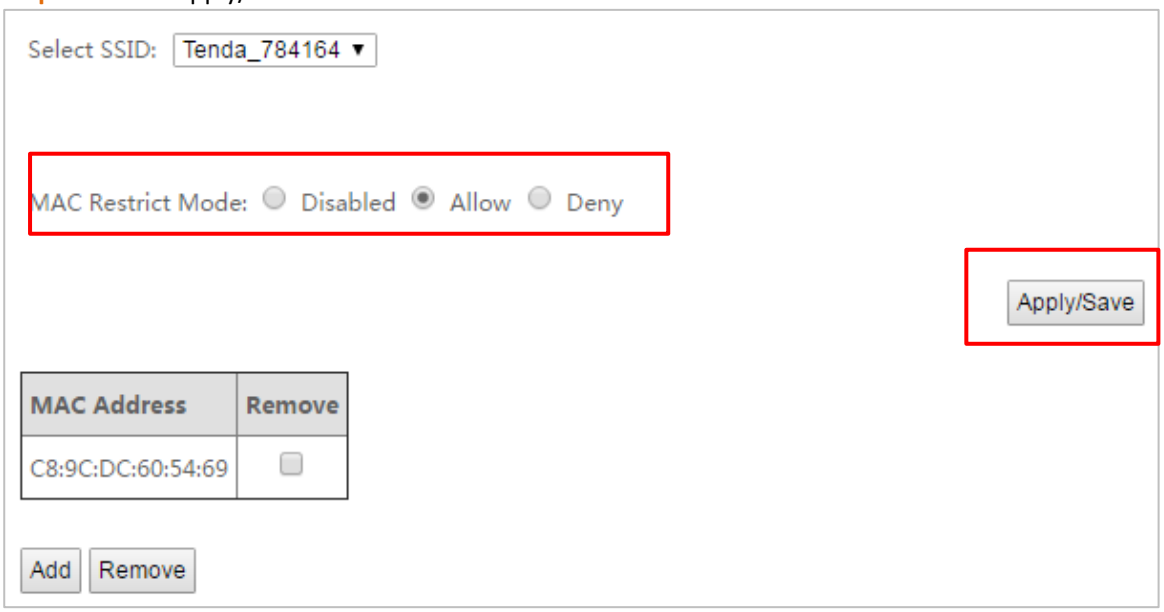
**Step 3** Enter the MAC address of the device to which the rule applies.

**Step 4** Click Apply/Save.




**Step 5** Select **Allow** or **Deny** according to your needs.

**Step 6** Click Apply/Save.

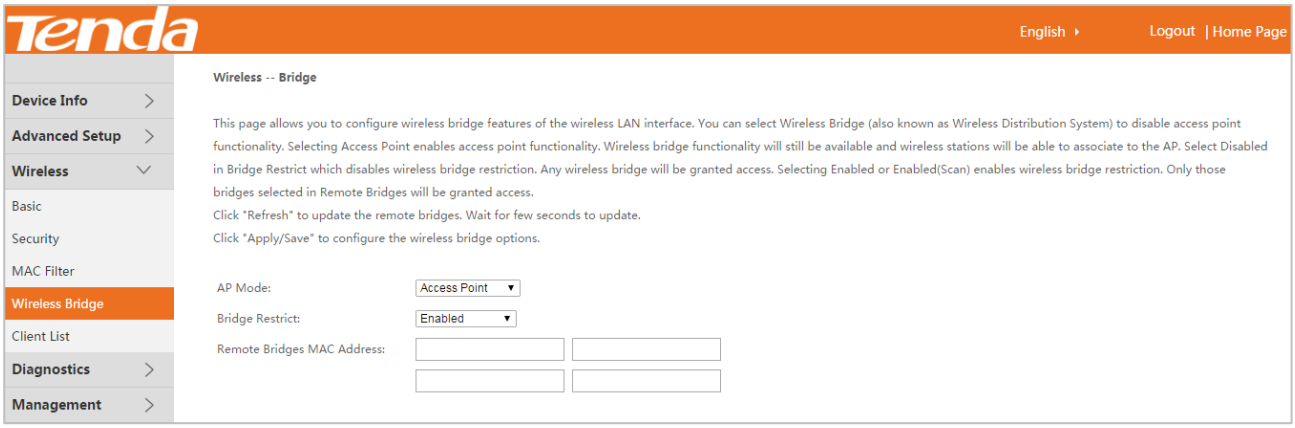



**--End**

# 5.4 Wireless Bridge

This section allows you to configure wireless bridge (also known as Wireless Distribution System) functions of the modem router. The function requires that the upstream wireless router supports WDS function as well.

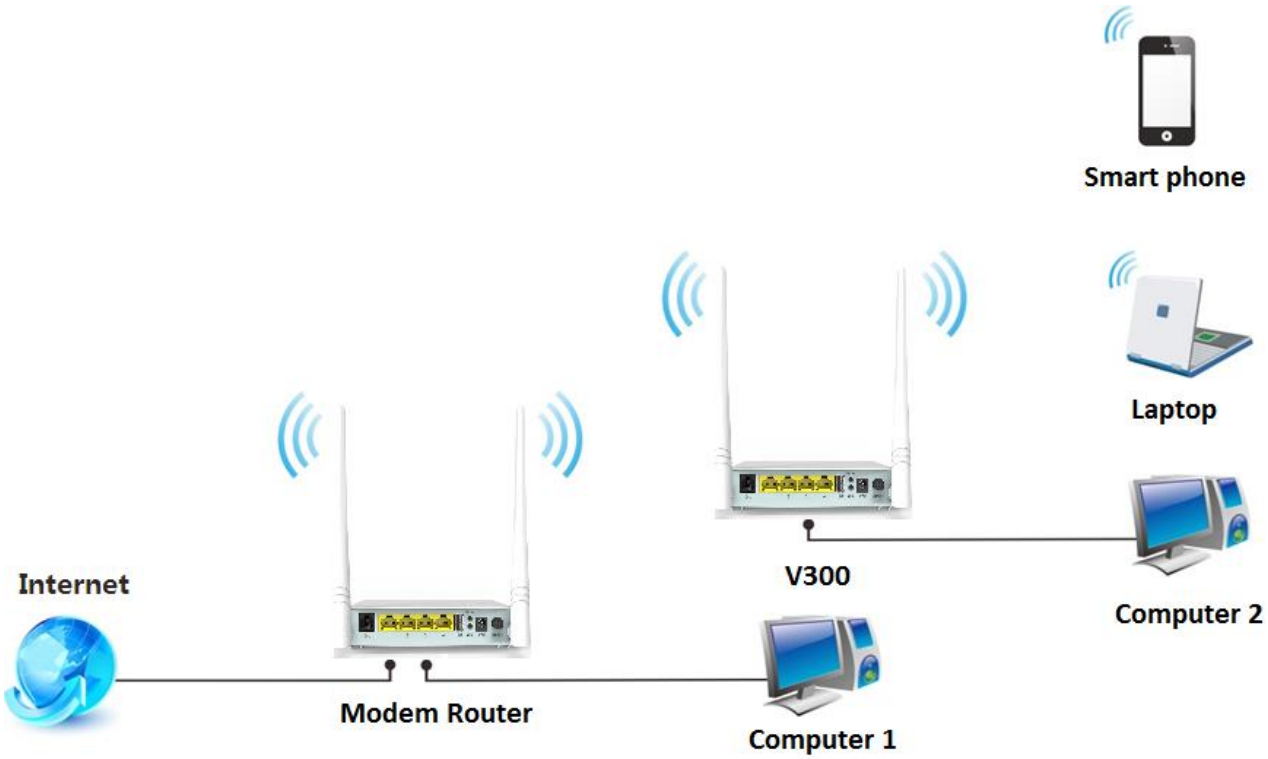
Choose **Advanced** > **Wireless** > **Wireless Bridge** to enter the configuration page.

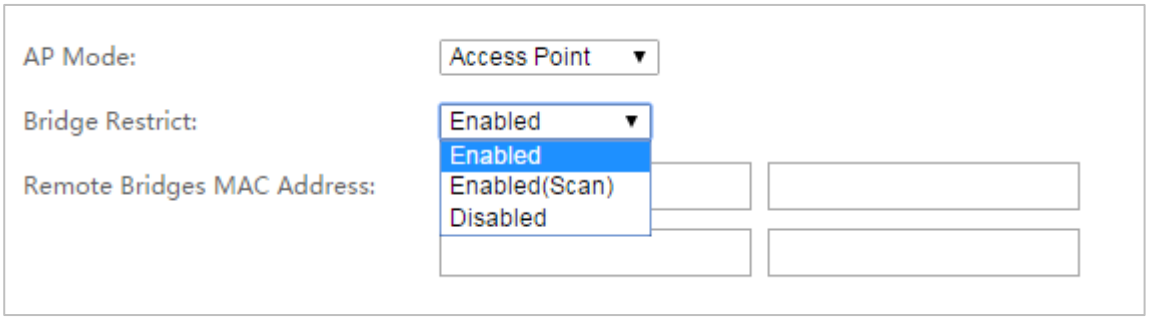


# Access Point

When the modem router enables access point function, it can extend the wireless network of the upstream wireless router to provide wireless coverage to wireless devices.

**Network Topology:**



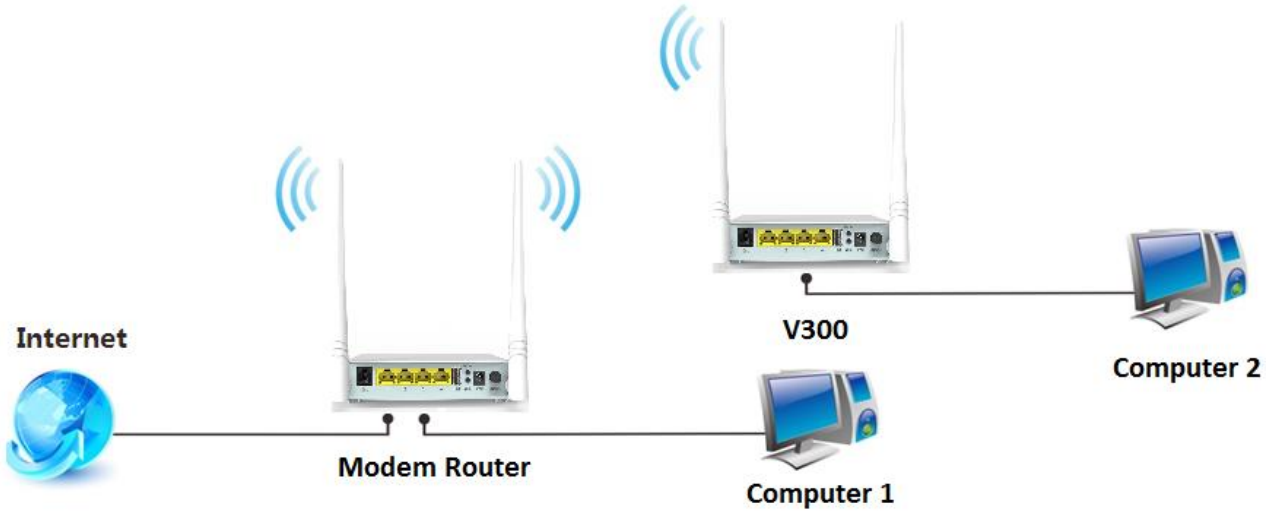

| Parameter | Description |
|---|---|
| AP Mode | It specifies the mode in which the modem router works. When the modem router works in this mode, it can extend the wireless network of the upstream wireless router to provide wireless coverage to wireless devices. |
| Bridge Restrict | Enabled: Enable the access point function, and you need to manually enter the MAC address of upstream wireless router. |
| | Enabled (Scan): Enable the access point function, and the modem router scans the wireless signals nearby. Then you can select the wireless network name from the list. |
| | Disabled: Disable the access point function. |

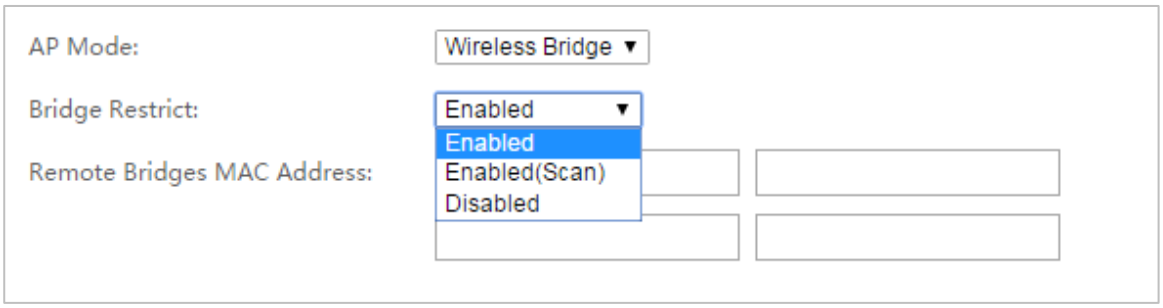
| | |
|---|---|
| Remote Bridges MAC Address | It specifies the MAC address of upstream wireless router. |

# Wireless Bridge

When the modem router enables wireless bridge function, it connects to the upstream wireless router wirelessly to provide internet connectivity to local wired clients.

**Network Topology:**




| Parameter | Description |
|---|---|
| AP Mode | It specifies the mode in which the modem router works. The modem router allows you to bridge a maximum of four wireless networks concurrently. |
| Bridge Restrict | Enabled: Enable the wireless bridge function, and you need to manually enter the MAC address of upstream wireless router. |
| | Enabled (Scan): Enable the wireless bridge function, and the modem router scans the wireless signals nearby. Then you can select the wireless network name from the list. |
| | Disabled: Disable the wireless bridge function. |
| Remote Bridges MAC Address | Enter the MAC address of upstream wireless router. |

NOTE

The WDS function (access point and wireless bridge) requires that the wireless channel, encryption type, and wireless password of the modem router must be the same as those of the upstream router.

**Application Scenario**

User A purchases a wireless router for wireless coverage in his apartment. The router (Router A) is placed in the living room. The WiFi signals are strong in the living room, but too weak in the bedroom and study room.

**Solution**

To improve internet connectivity in the bedroom, the user can add a V300 modem router and configure the wireless bridge function of the router to extend the WiFi network coverage. That will eliminate blind areas in the apartment, enabling the user to access the internet anywhere in the apartment.

Assume that:

- The modem router works in access point mode.
- The upstream wireless router uses the following wireless settings.

| Parameter | Description |
|---|---|
| Wireless Name | Tenda_XXXXXX |
| Wireless Password | 12345678 |
| Wireless Encryption | Mixed WPA2/WPA-PSK, AES |
| Wireless Channel | 6 |
| LAN IP | 192.168.1.1 |

**Procedure**:

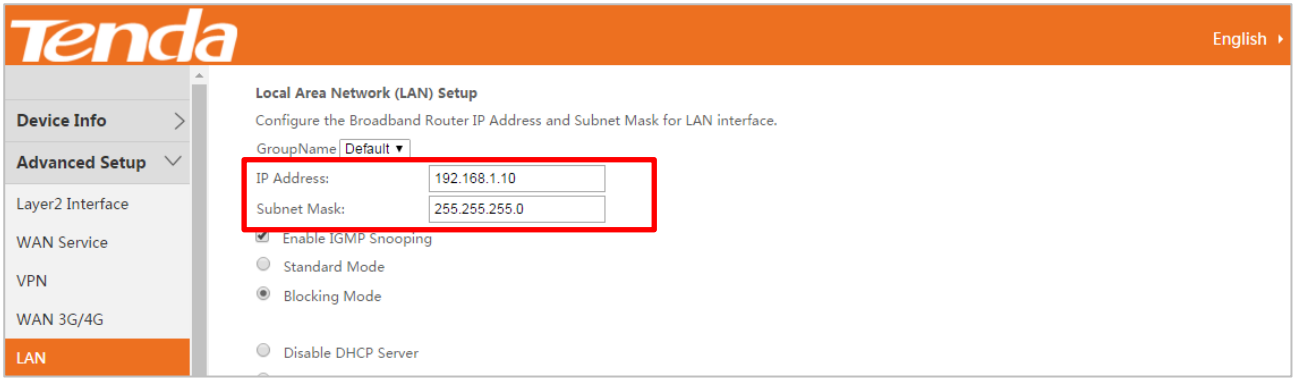
**Step 1** Configure the modem router.

1. Set the LAN IP of the modem router to one that is in the same network segment but different from the LAN IP address of the upstream wireless router. For example, if the LAN IP of the upstream wireless router is **192.168.1.1**, set the LAN IP of the modem router to **192.168.1.10**.

   (1) Choose **Advanced** > **Advanced Setup** > **LAN** to enter the configuration page.

   (2) Set **IP Address** to **192.168.1.10**, and **Subnet Mask** to **255.255.255.0**.

   (3) Click **Apply/Save**.



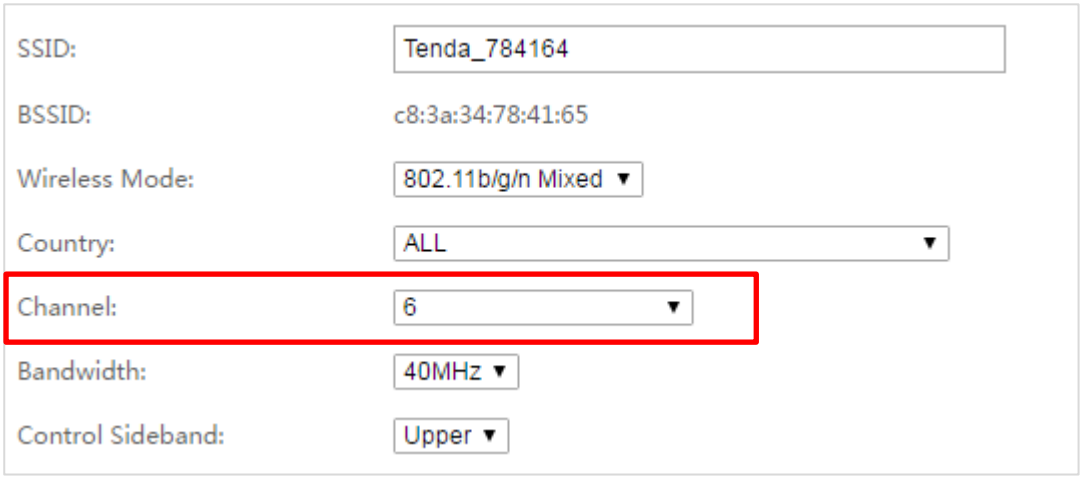

2 Change the wireless channel, encryption, and password to the same as those of the upstream router.

(1) Log in to the modem router using the new LAN IP address **192.168.1.10**. (If you cannot log in to the web UI of the modem router with the new LAN IP address, disable the adapter of your computer, and then enable it again to obtain an IP address again.)

(2) Choose **Advanced** > **Wireless** > **Basic** to enter the configuration page.

(3) Set **Channel** to **6**.

(4) Click **Apply/Save** on the bottom of this page.




(5) Choose **Advanced** > **Wireless** > **Security** to enter the configuration page.

(6) Set the **Network Authentication**, **WPA/WAPI Passphrase**, and **WPA/WAPI Encryption** to **Mixed WPA2/WPA-PSK**, **12345678**, and **AES** respectively.

(7) Click **Apply/Save** on the bottom of this page.


3 Configure the access point function.

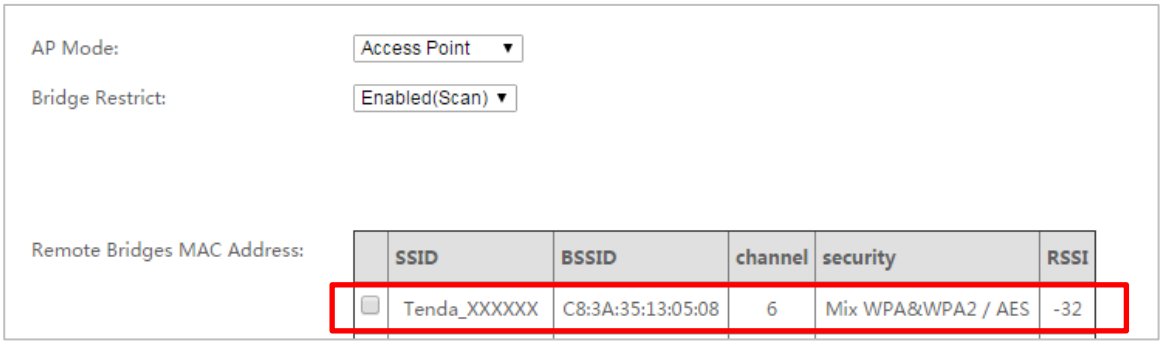
(1) Choose **Advanced** > **Wireless** > **Wireless Bridge** to enter the configuration page.

(2) Set the **AP Mode** to **Access Point**.

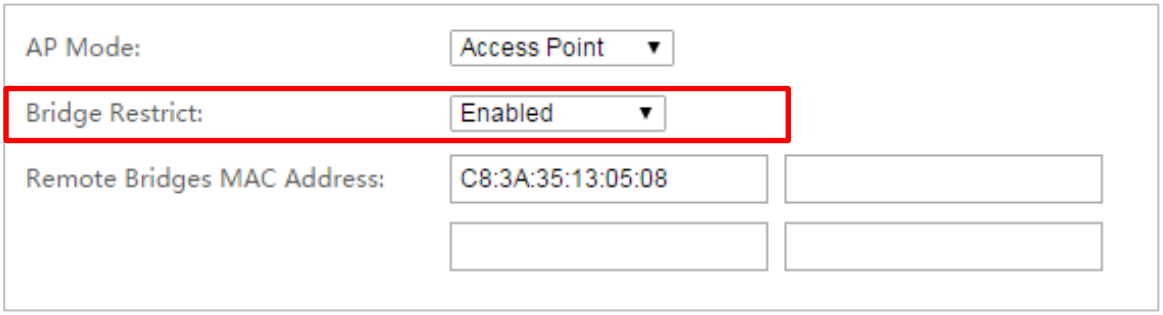
(3) Set the **Bridge Restrict** to **Enabled (Scan)**.

(4) Select the SSID (wireless network name) of the upstream router which is **Tenda_XXXXXX** in this example.

(5) Click **Apply/Save**.




(6) Set the **Bridge Restrict** to **Enabled**.




(7) Click **Apply/Save**.

**Step 2** Configure the upstream router. Perform the steps in step "3".

**--End**

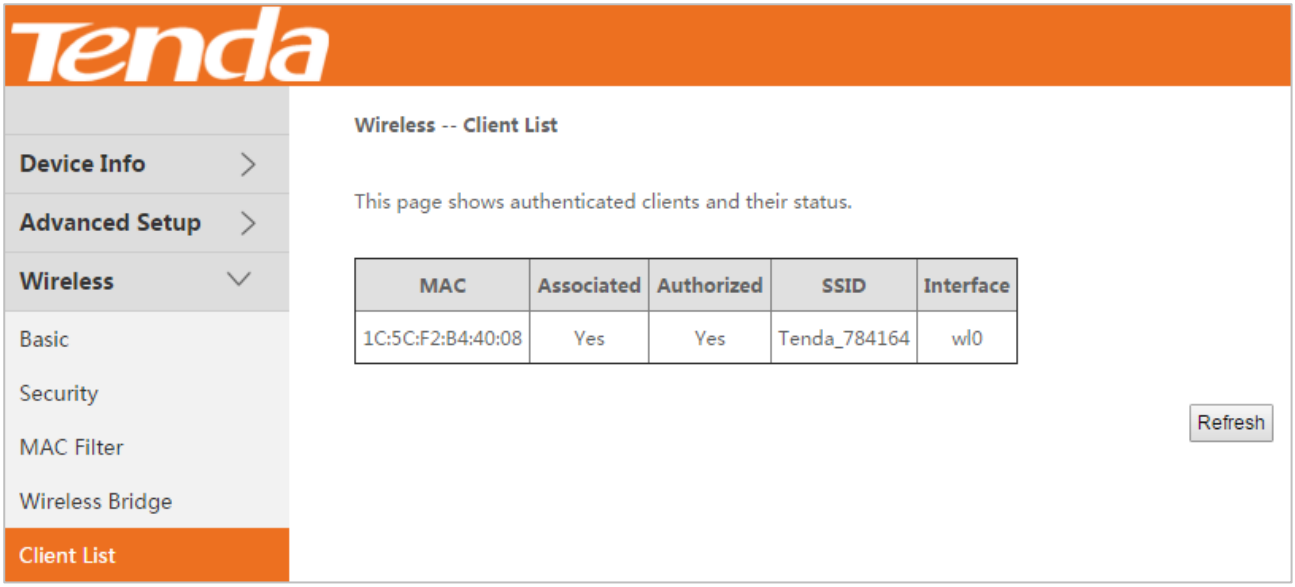
**Verification**

Try logging in to the web UI of the upstream router with **192.168.1.1** on a computer connected to the modem router.

# 5.5 Client List

This section allows you to check the information of wireless clients connected to the wireless networks of the modem router.

Choose **Advanced** > **Wireless** > **Client List** to enter this page.

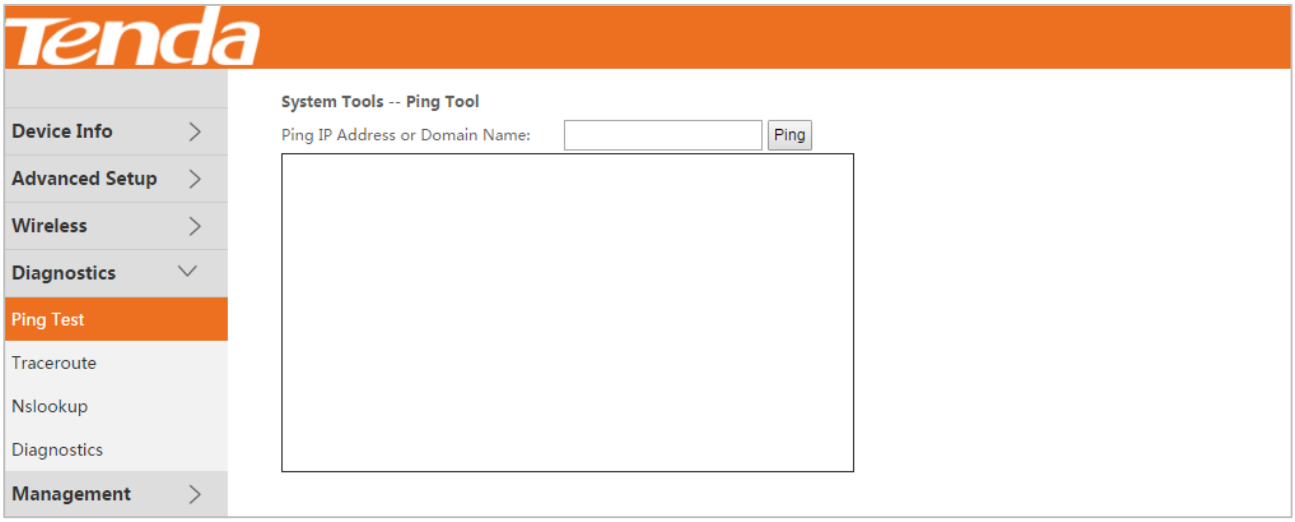

Tenda
Device Info
Advanced Setup
Wireless
Basic
Security
MAC Filter
Wireless Bridge
Client List
Wireless -- Client List
This page shows authenticated clients and their status.
MAC
Associated
Authorized
SSID
Interface
1C:5C:F2:B4:40:08
Yes
Yes
Tenda_784164
wl0
Refresh

# 6 Diagnostics

## 6.1 Ping Test

Ping test can help test whether a host or the internet is reachable.

Choose **Advanced** > **Diagnostics** > **Ping Test** to enter this page.



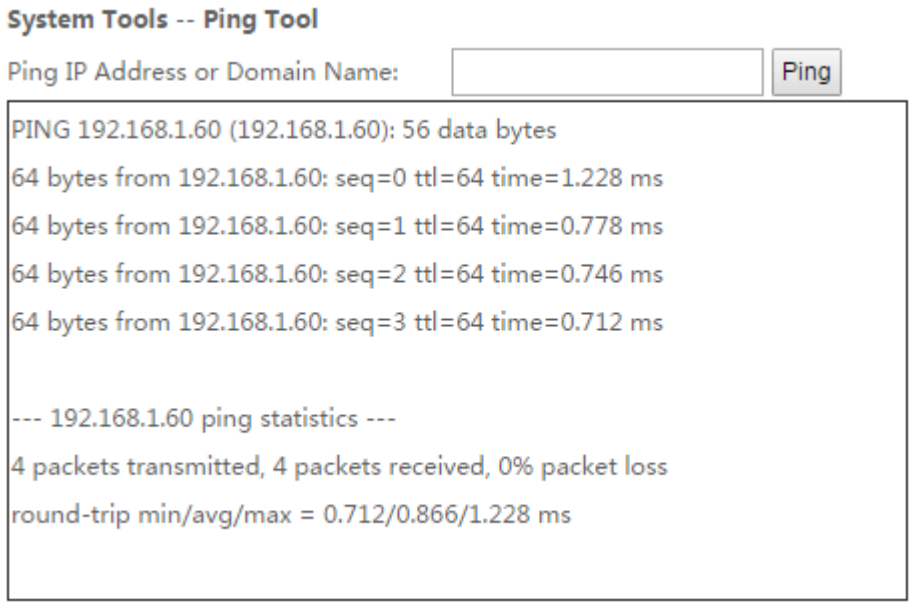

To perform the ping test:

**Step 1** Enter the IP address or domain name of the host in the **Ping IP Address or Domain Name** field.

**Step 2** Click **Ping**.

**--End**

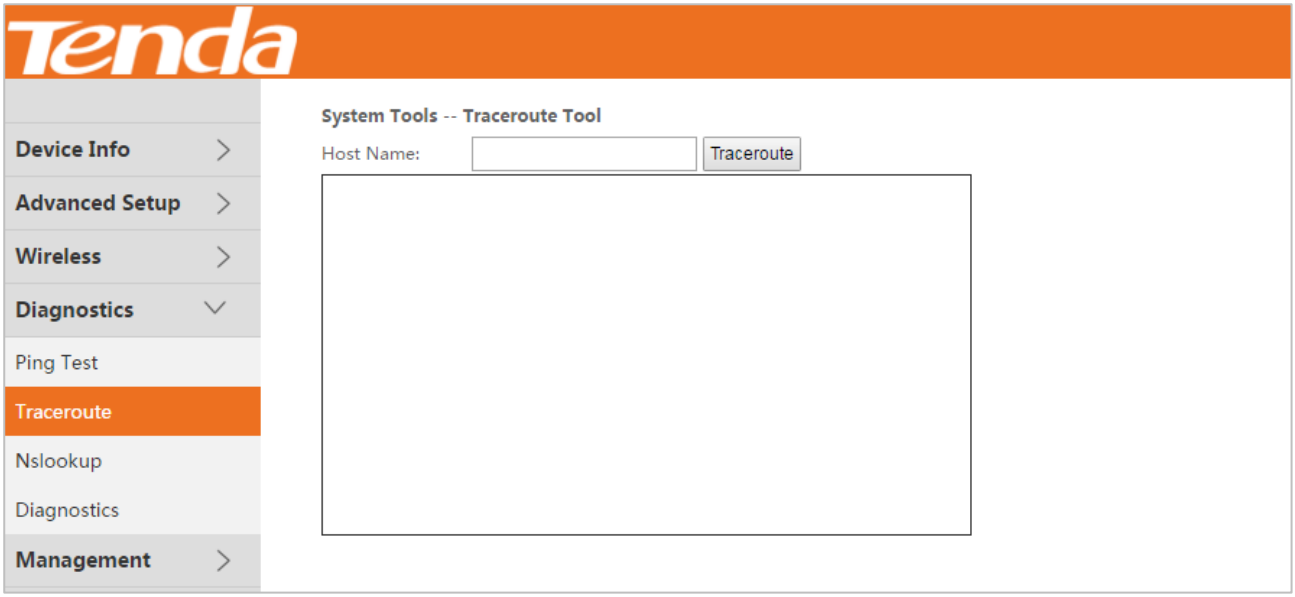
If you get a similar screenshot shown as below, it indicates that the host is reachable from the modem router.



# 6.2 Traceroute

Traceroute helps you check the specific routes to a host.

Choose **Advanced** > **Diagnostics** > **Traceroute** to enter this page.



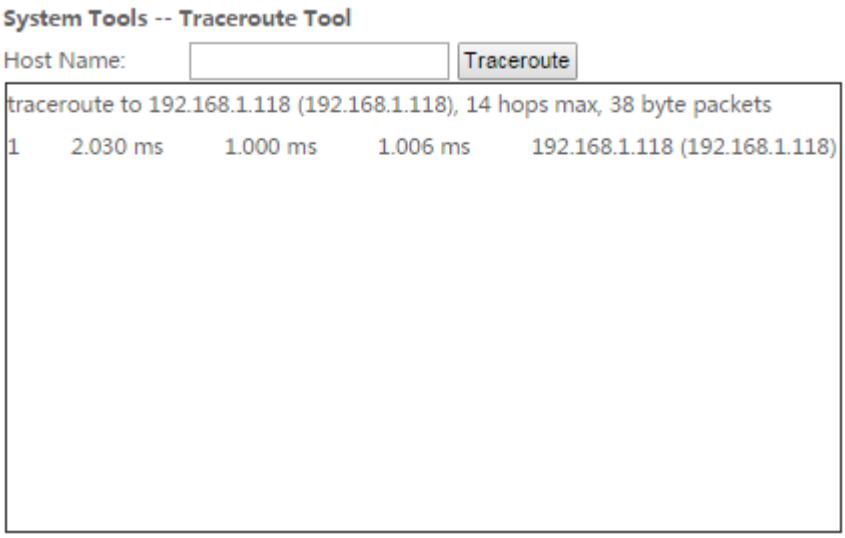

To perform the traceroute:

**Step 1** Enter the IP address or domain name of the host in the **Host Name** field.

**Step 2** Click Traceroute.

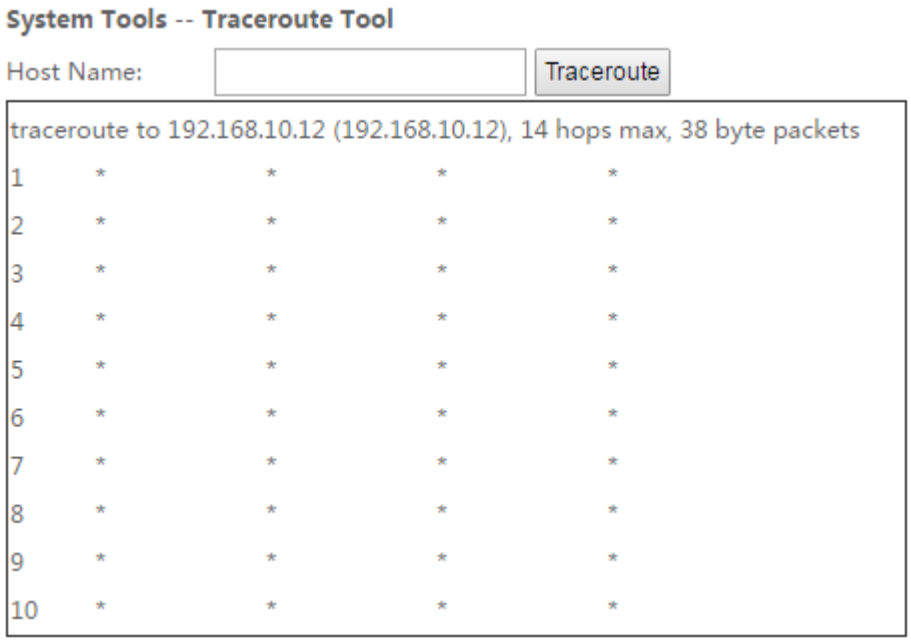
**--End**

Then you can check the result. The following route table displays the traceroute to the host whose IP address is **192.168.1.118**.



TIP

If the host is unreachable, the route table is blank.

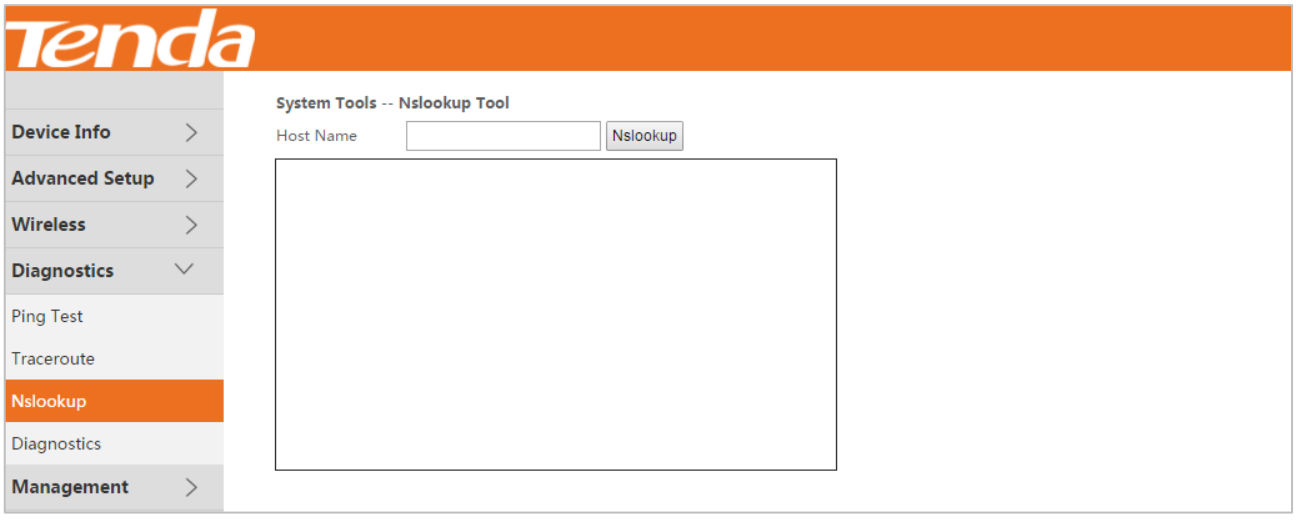



# 6.3 Nslookup

**Step 1** Nslookup helps you translate the domain name to specific IP address.

Choose **Advanced** > **Diagnostics** > **Nslookup** to enter this page.

**Step 2**



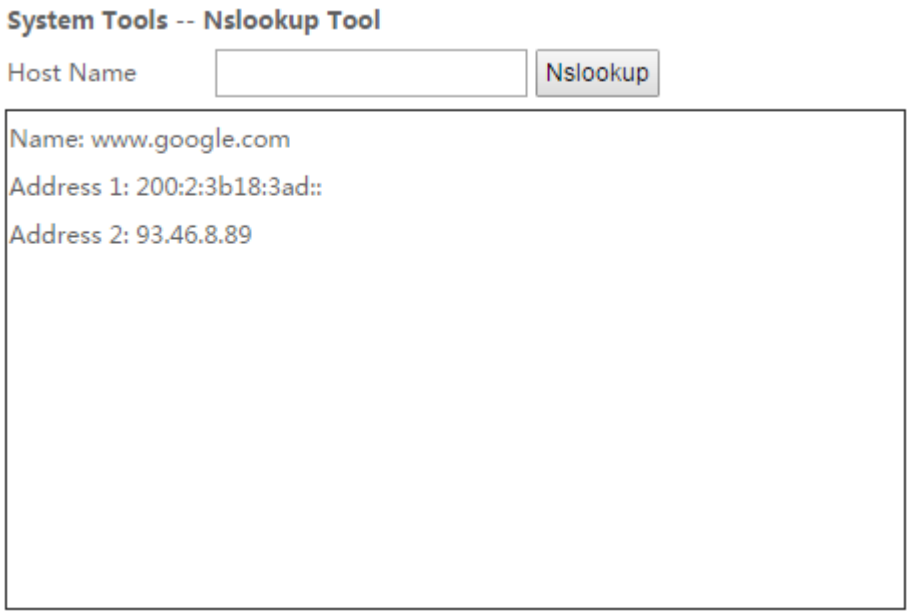

**Step 3** To translate a domain name, to perform the following procedure:

**Step 4** Enter a domain name in the **Host Name** field.

**Step 5** Click **Nslookup**.

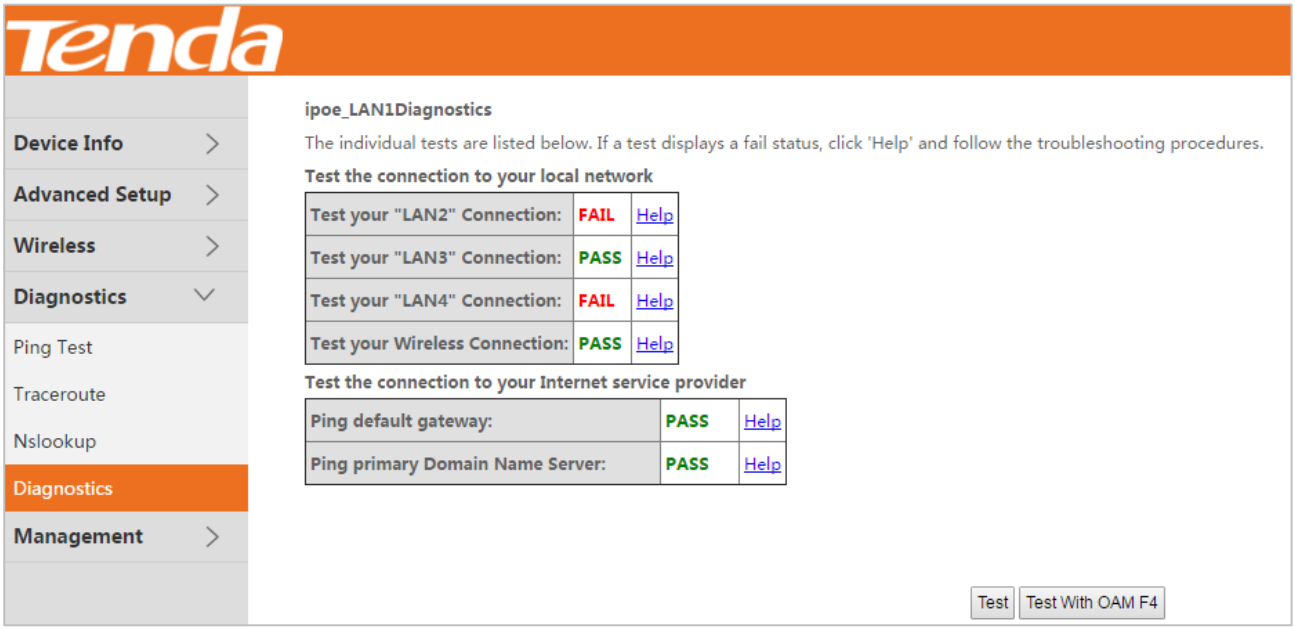
**--End**

Then you can check the result. The following screenshot displays the IP address of the domain name **www.google.com**.




## 6.4 Diagnostics

The device is capable of testing the connection to your DSL service provider, the connection to your ISP and the connection to your local network. If a test fails, click "Help" and follow the troubleshooting procedures.



# 7 Management

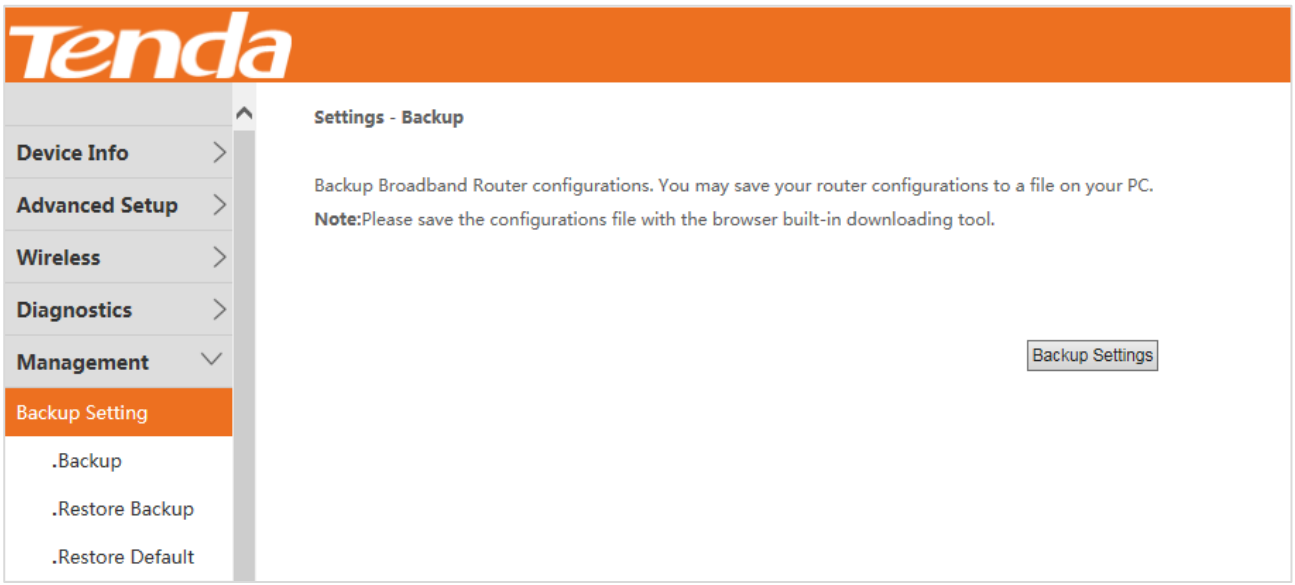
## 7.1 Backup Settings

Here you can back up the current settings, restore earlier settings, and restore the factory settings of the device.

### 7.1.1 Backup

This function allows you to save a copy of your device's settings 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.

Choose **Management** > **Backup Setting** > **Backup** to enter the configuration page.




To back up the settings, perform the following procedure:

**Step 1** Click **Backup Settings**.

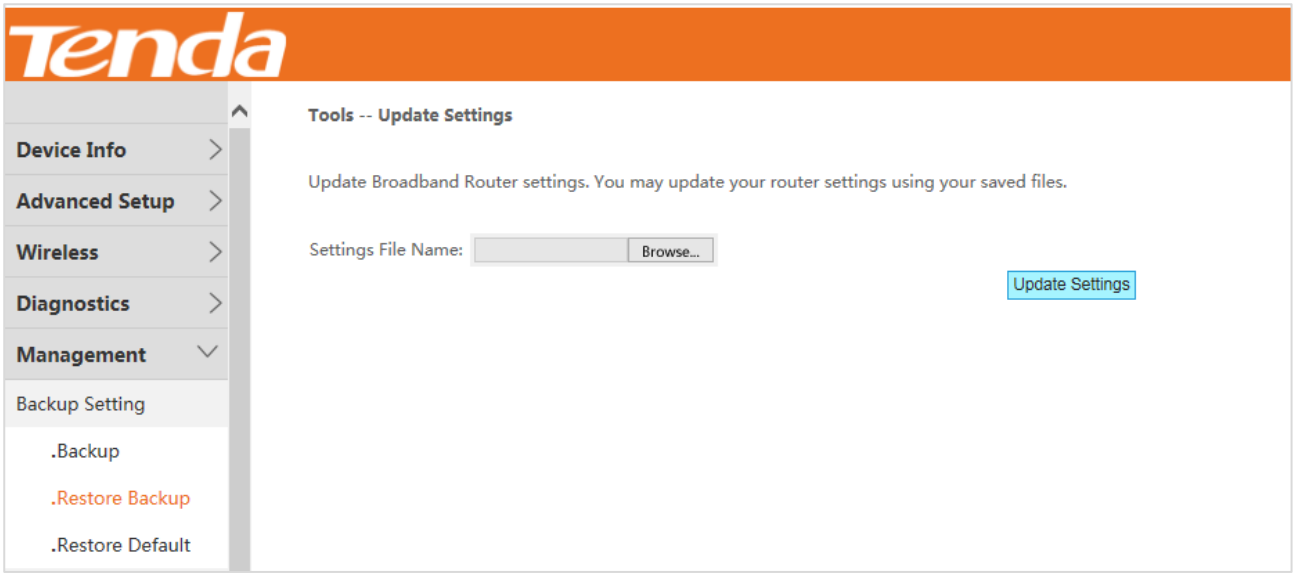
**Step 2** Follow the on-screen instructions to save the file to a local path.

**---End**

### 7.1.2 Restore Backup

This function allows you to restore the settings saved in a configuration file on your PC.

Choose **Management** > **Backup Setting** > **Restore Backup** to enter the configuration page.




To restore the settings, perform the following procedure:

**Step 1** Click **Browse**.

**Step 2** Select a configuration file on your PC.

**Step 3** Click Update Settings.

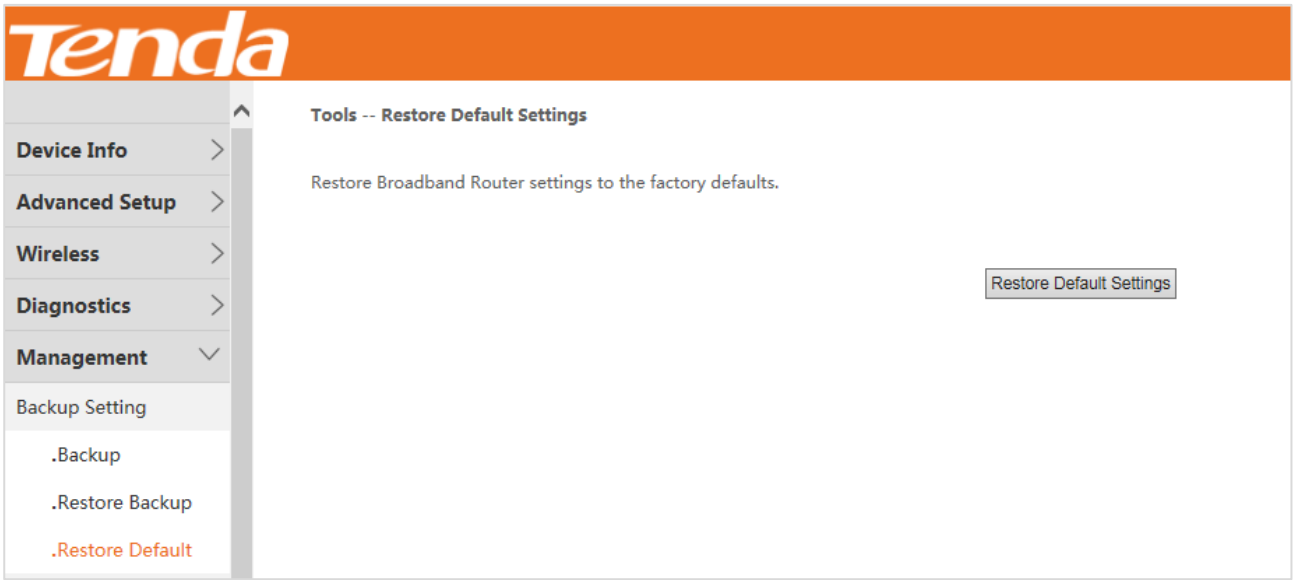
**Step 4** Click **OK**.

**---End**

## 7.1.3 Restore Default

This function allows you to restore the factory settings of the device.

Choose **Management** > **Backup Setting** > **Restore Default** to enter the configuration page.




To restore the settings, perform the following procedure:

**Step 1** Click **Restore Default Settings**.

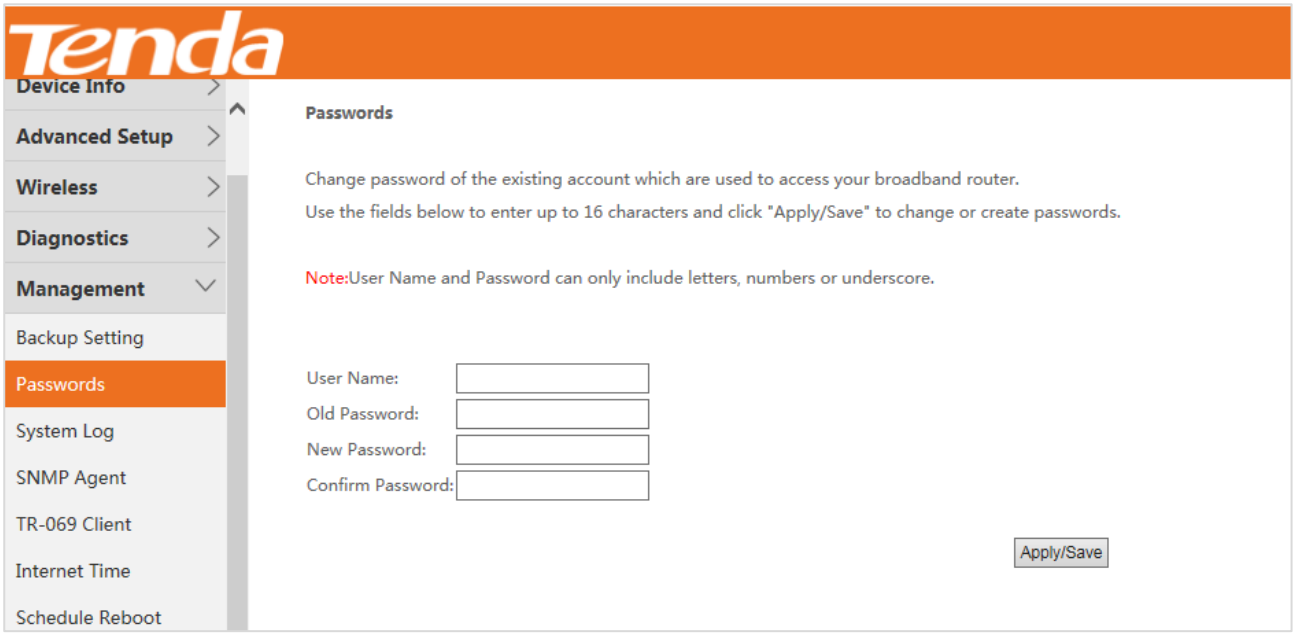
**Step 2** Click **OK**.

**---End**

# 7.2 Passwords

This function allows you to change the login password of the device.

Choose **Management** > **Passwords** to enter the configuration page.




To change the login password, perform the following procedure:

**Step 1** Set **User Name** to the current user name, such as the default user name **admin**.

**Step 2** Set **Old Password** to the current password, such as the default password **admin**.

**Step 3** Set **New Password** to the new password consisting of 1 to 16 letters, digits, or underscores, such as **admin1**.

**Step 4** Set Confirm Password to the same value as New Password.

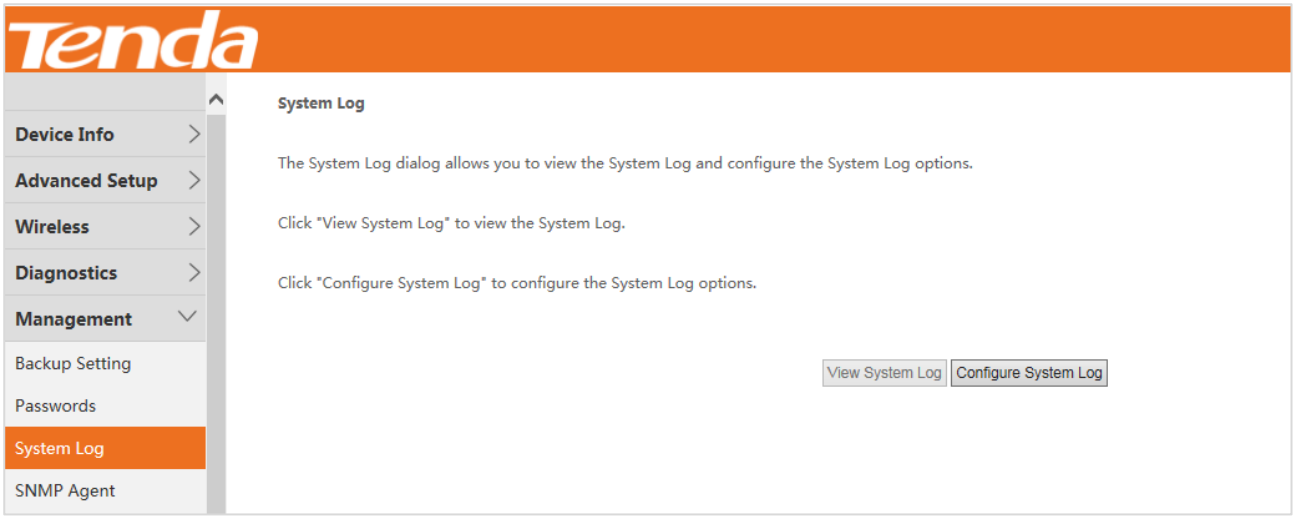
**Step 5** Click **Apply/Save**.

**---End**

# 7.3 System Log

This function allows you to configure, view, and export system logs, which helps you understand the operating conditions of the device.

Choose **Management** > **System Log** to enter the configuration page.

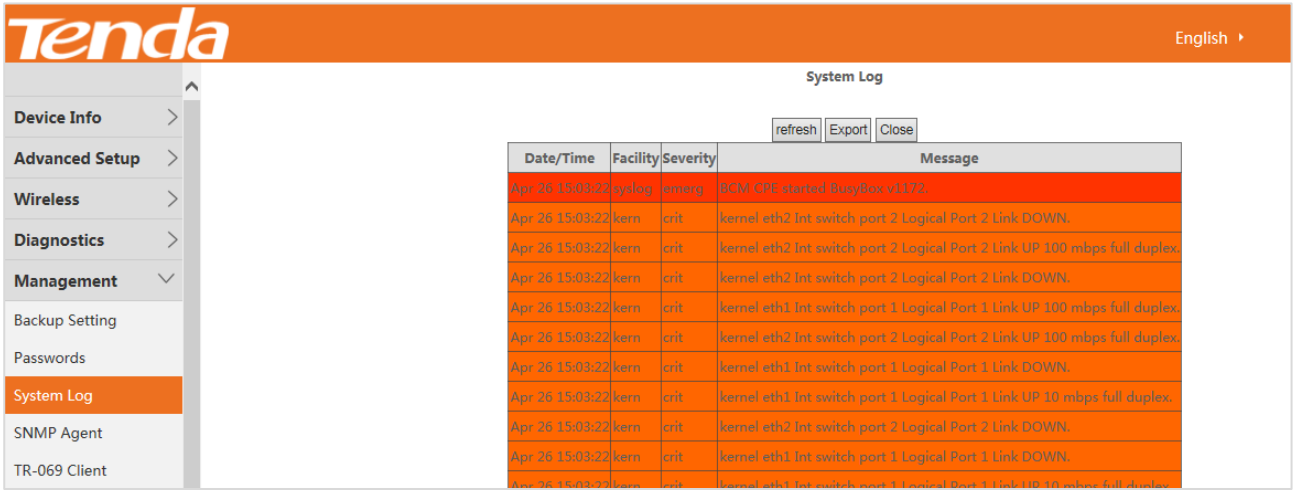



## 7.3.1 Viewing System Logs

NOTE

You can view system logs only after enabling the logging function. For details, see section 7.3.2 Configuring System Logs.

To view the system logs, click **View System Log**.

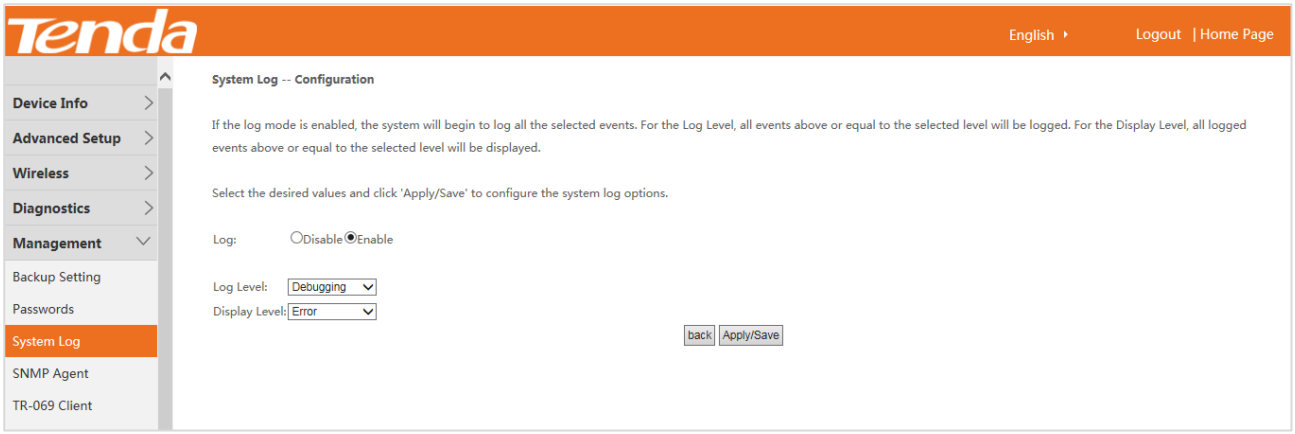



On the page that appears:

- To update the system logs, click **Refresh**.
- To export the system logs, click **Export** and follow the onscreen instructions to save the system logs to a file on your PC.

## 7.3.2 Configuring System Logs

Click **Configure System Log** to enter the configuration page.




To configure system logs, perform the following procedure:

**Step 1** Set Log to **Enable**.

**Step 2** Select a logging level from the Log Level drop-down list box. All the system events at or above the selected level are logged.

**Step 3** Select a log display level from the **Display Level** drop-down list box. Only the logs at or above the selected level can be viewed.

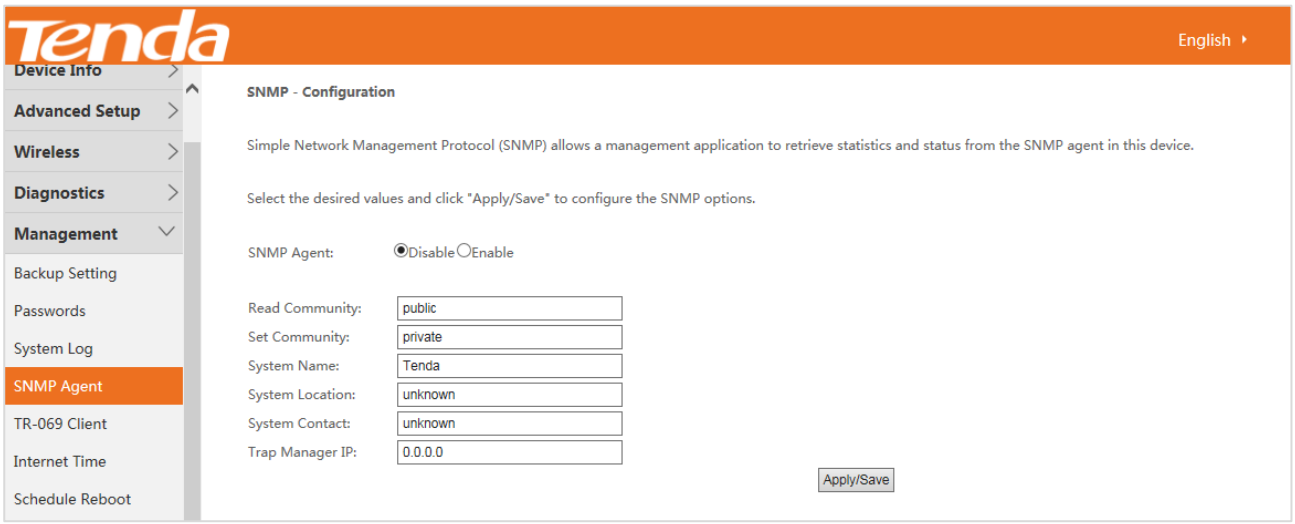
**Step 4** Click **Apply/Save**.

**---End**

# 7.4 SNMP Agent

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

Choose **Management** > **SNMP Agent** to enter the configuration page.




To configure the SNMP agent, perform the following procedure:

**Step 1** Set SNMP Agent to **Enable**.

**Step 2** Set **Read Community** to the password for reading data. The default value is public.

**Step 3** Set **Set Community** to the password for writing data. The default value is private.

**Step 4** Set **System Name** to the name of the system.

**Step 5** Set **System Location** to the location of the system.

**Step 6** Set **System Contact** to the contact information of the system.

**Step 7** Set **Trap Manager IP** to the IP address of the Trap Manager.

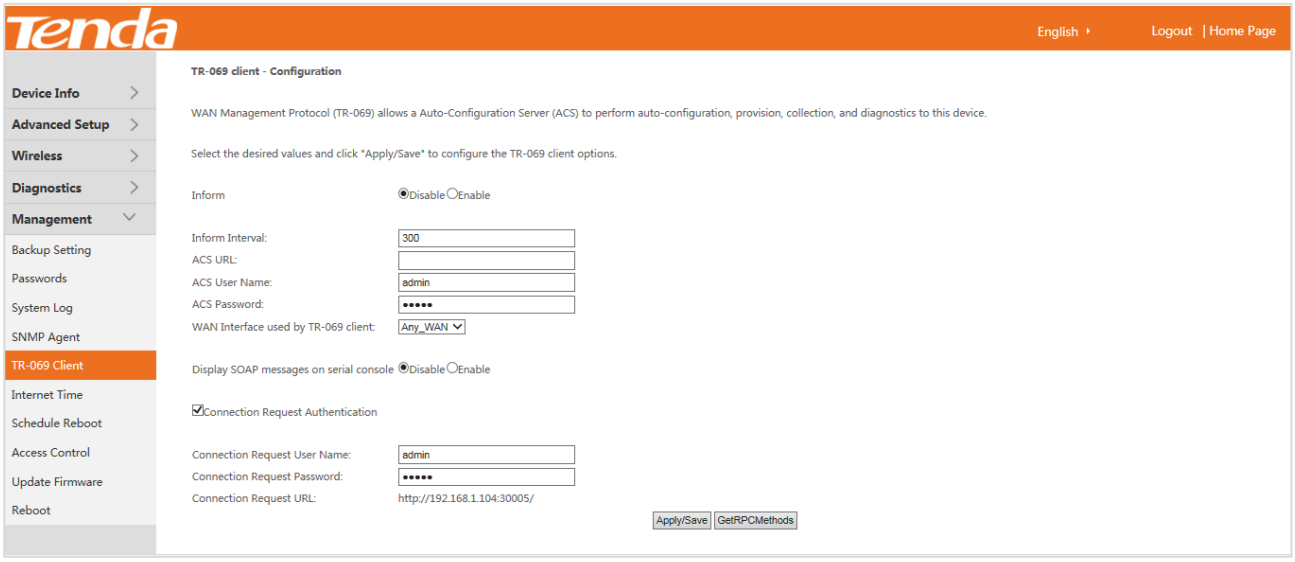
**Step 8** Click **Apply/Save**.

**---End**

# 7.5 TR-069 Client

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

Choose **Management** > **TR-069 Client** to enter the configuration page.




To configure the TR-069 Client function, perform the following procedure:

**Step 1** Set **Inform** to **Enable**. By default, it is disabled.

**Step 2** Set **Inform Interval** to the interval at which inform packets are sent.

**Step 3** Set **ACS URL** to the URL of the ACS.

**Step 4** Set **ACS User Name** to the user name of the ACS.

**Step 5** Set **ACS Password** to the password of the ACS.

**Step 6** Select the WAN port used by the TR-069 client from the **WAN Interface used by TR-069 client** drop-down list box.

**Step 7** Set **Display SOAP messages on serial console** to **Enable** if SOAP messages must be displayed on the serial console, or to disabled if SOAP messages do not need to be displayed on the serial console.

**Step 8** Select **Connection Request Authentication** if connection request authentication is required.
If it is selected, perform the following steps:

1. Set **Connection Request User Name** to the user name for connection request authentication.
2. Set **Connection Request Password** to the password for connection request authentication.
3. Set **Connection Request URL** to the URL for connection request authentication.

**Step 9** Click **Apply/Save**.

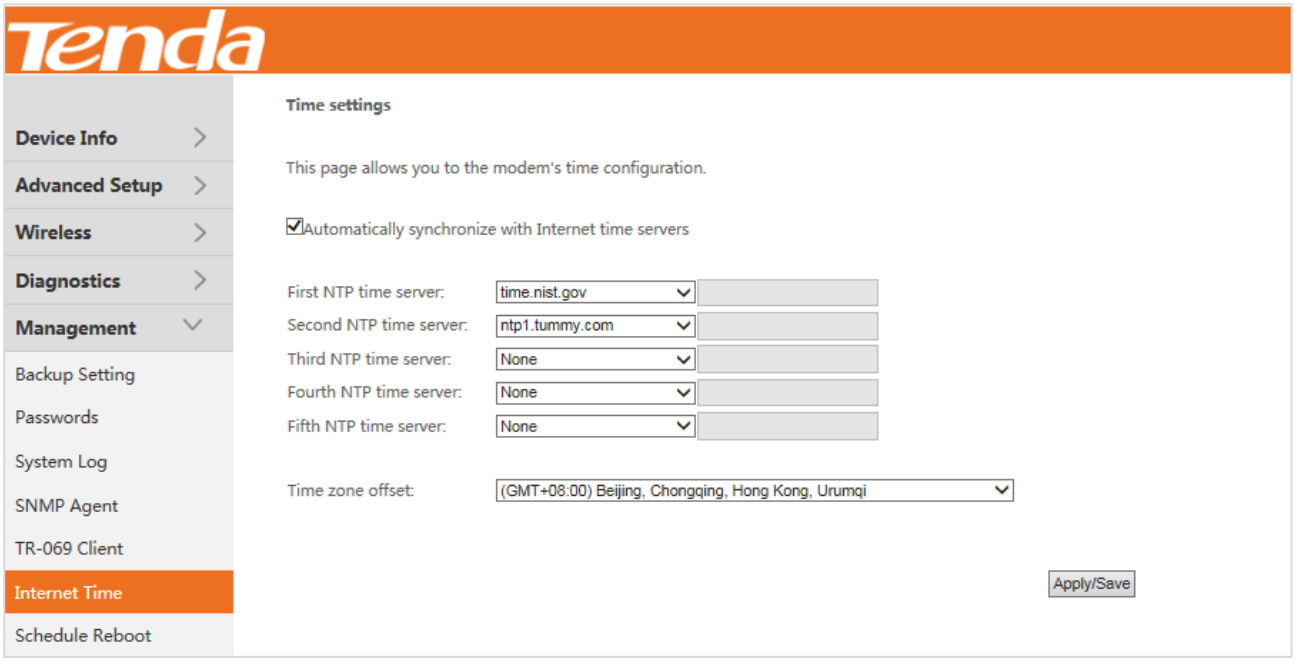
**---End**

NOTE

To learn about the methods supported by the ACS, click **GetRPCMethods**.

# 7.6 Internet Time

This function allows you to synchronize the time of the device with the internet time.
Choose **Management** > **Internet Time** to enter the configuration page.




To synchronize the time of the device with the internet time, perform the following procedure:

**Step 1** Select Automatically synchronize with Internet time servers.

**Step 2** Set **First NTP time server** to the first time server with which the device time is synchronized.

**Step 3** Set **Second NTP time server** to the second time server with which the device time is synchronized.

**Step 4** Set **Third NTP time server** to the third time server with which the device time is synchronized.

**Step 5** Set **Fourth NTP time server** to the fourth time server with which the device time is synchronized.

**Step 6** Set **Fifth NTP time server** to the fifth time server with which the device time is synchronized.

**Step 7** Select your time zone from the **Time zone offset** drop-down list box.

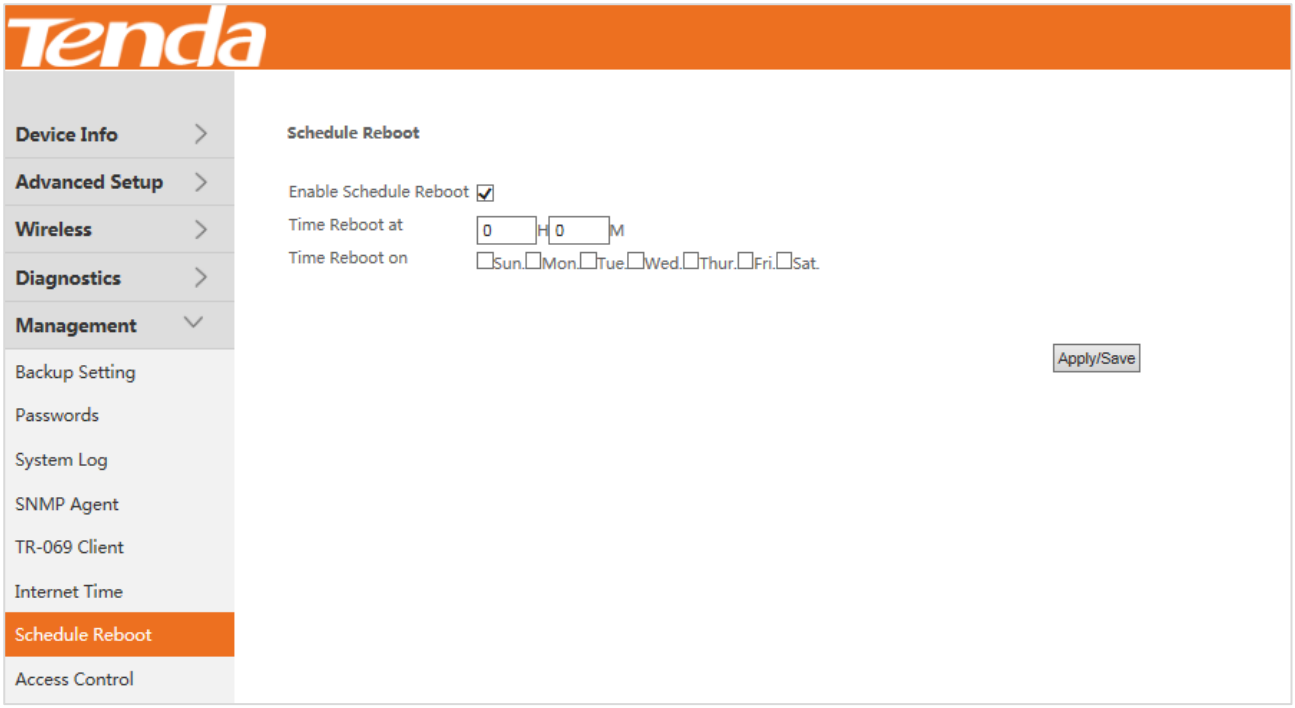
**Step 8** Click **Apply/Save**.

**---End**

# 7.7 Schedule Reboot

This function allows you to specify device reboot schedule.

Choose **Management** > **Schedule Reboot** to enter the configuration page.




To specify the schedule, perform the following procedure:

**Step 1** Select Enable Schedule Reboot.

**Step 2** Set **Time Reboot At** to the time when you want the device to reboot.

**Step 3** Set **Time Reboot On** to the days when you want the device to reboot.

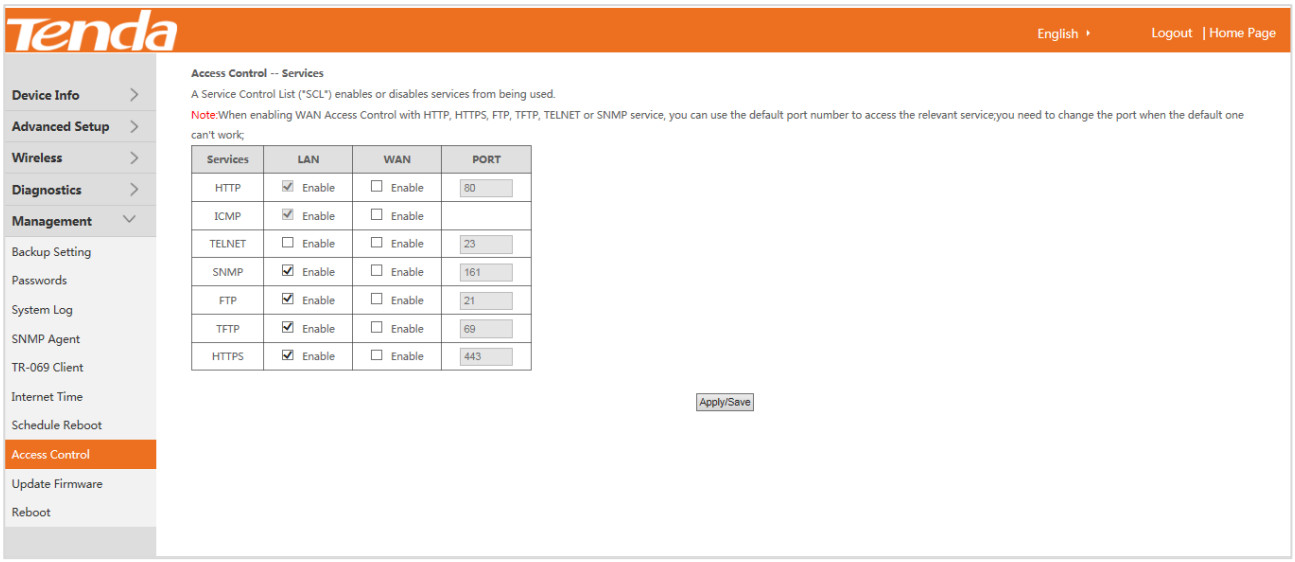
**Step 4** Click **Apply/Save**.

**---End**

# 7.8 Access Control

This function allows you to control service accessibility by protocol and port type.

Choose **Management** > **Access Control** to enter the configuration page.




To control service accessibility, perform the following procedure:

**Step 1** Select the check boxes by protocol and port type to enable the required services.

**Step 2** Change the default ports if they are being used.

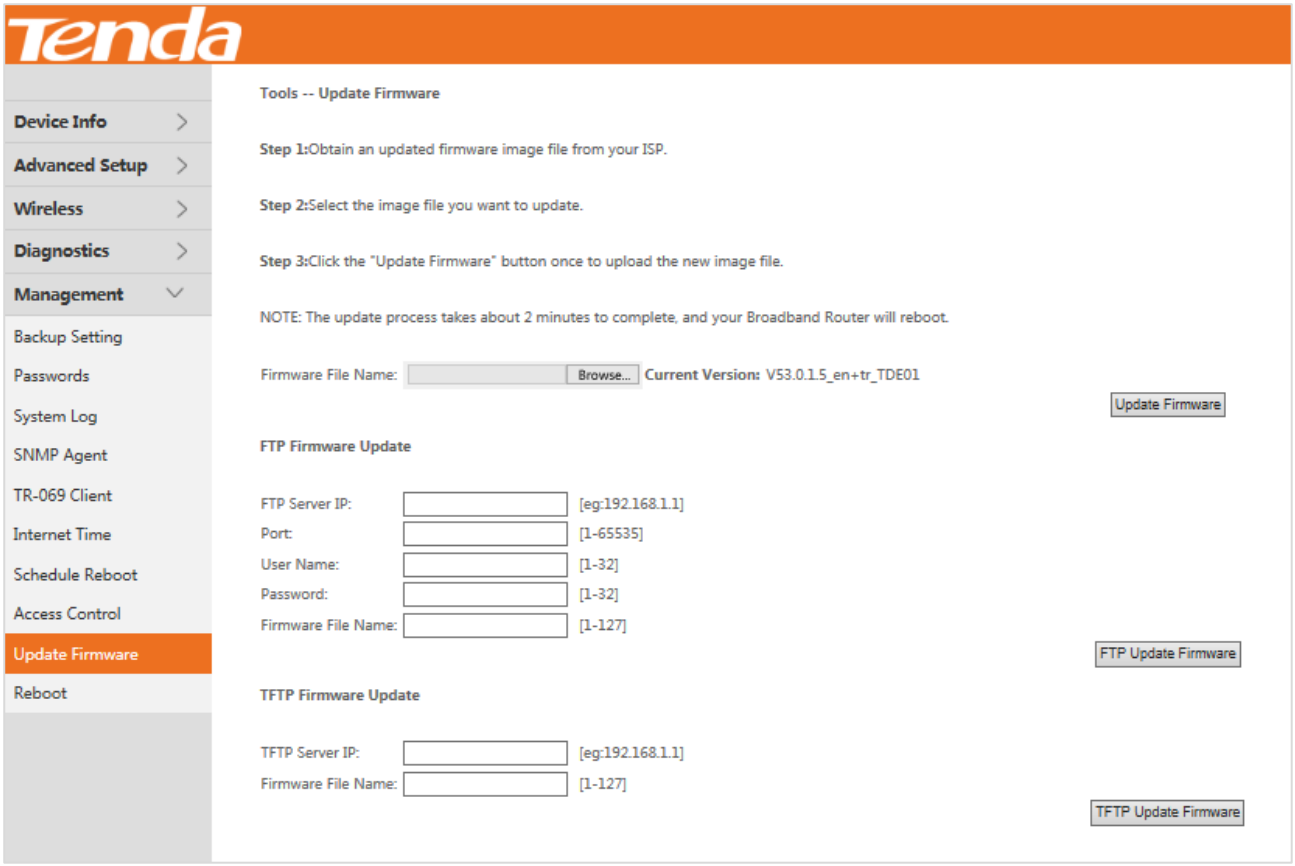
**Step 3** Click **Apply/Save**.

**---End**

# 7.9 Update Firmware

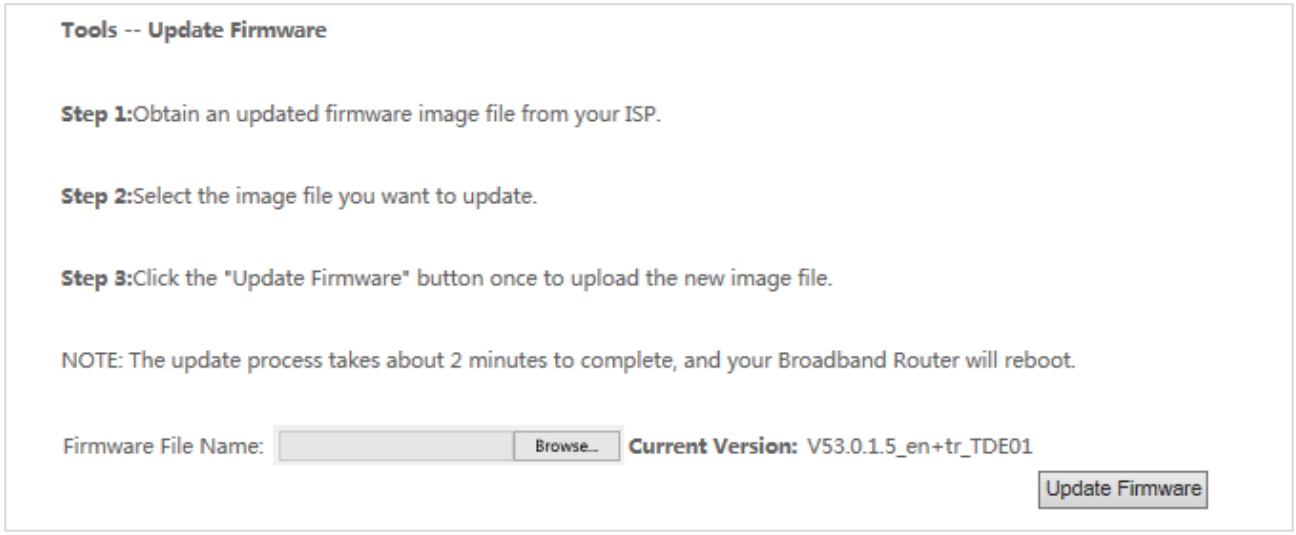
This function allows you to upgrade the firmware of the device locally, using FTP, or using TFTP.

Choose **Management** > **Update Firmware** to enter the configuration page.




## 7.9.1 Upgrading the Firmware Locally

The **Tools -- Update Firmware** module is used to upgrade the firmware locally.




To upgrade the firmware locally, perform the following procedure:

**Step 1** Click **Browse**.

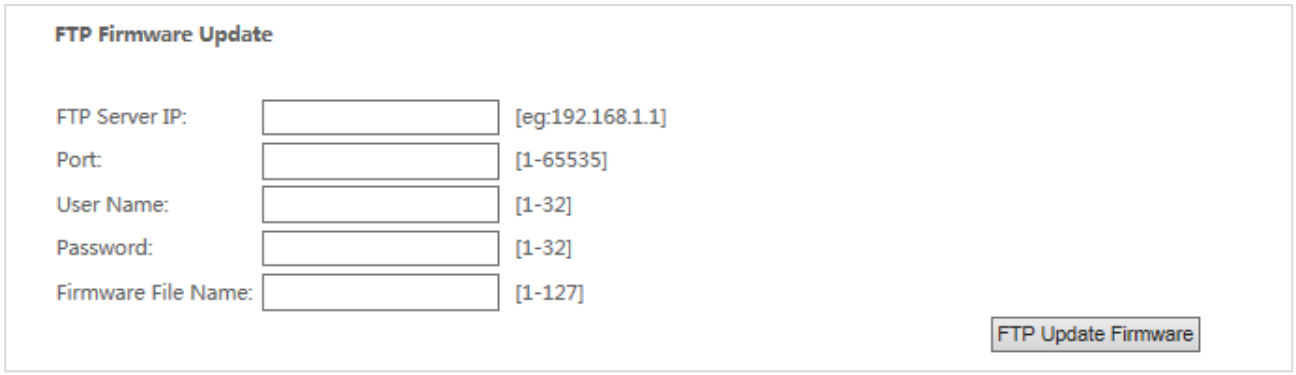
**Step 2** Select the firmware downloaded to your PC.

**Step 3** Click **Update Firmware**.

**---End**

## 7.9.2 Upgrading the Firmware Using FTP

The **FTP Firmware Update** module is used to upgrade the firmware using FTP.




To upgrade the firmware using FTP, perform the following procedure:

**Step 1** Set **FTP Server IP** to the IP address of the FTP server where the target firmware resides.

**Step 2** Set **Port** to the port number of the FTP server.

**Step 3** Set **User Name** to the user name for logging in to the FTP server.

**Step 4** Set **Password** to the password for logging in to the FTP server.

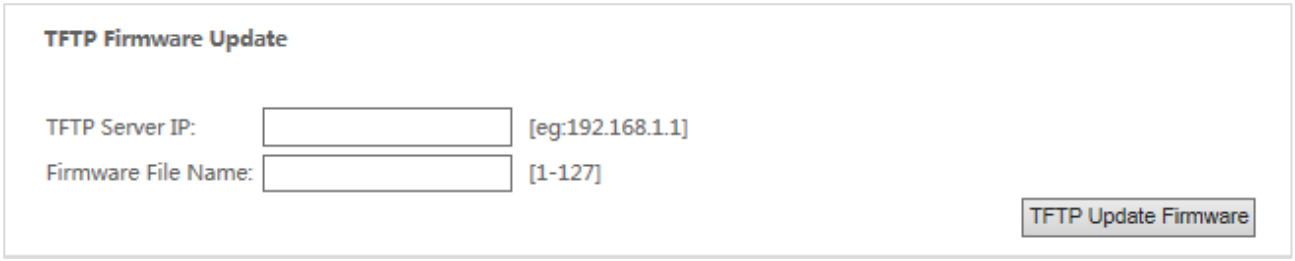
**Step 5** Set **Firmware File Name** to the file name of the target firmware.

**Step 6** Click **FTP Update Firmware**.

**---End**

## 7.9.3 Upgrading the Firmware Using TFTP

The **TFTP Firmware Update** module is used to upgrade the firmware using TFTP.




To upgrade the firmware using TFTP, perform the following procedure:

**Step 1** Set T**FTP Server IP** to the IP address of the TFTP server where the target firmware resides.

**Step 2** Set **Firmware File Name** to the file name of the target firmware.

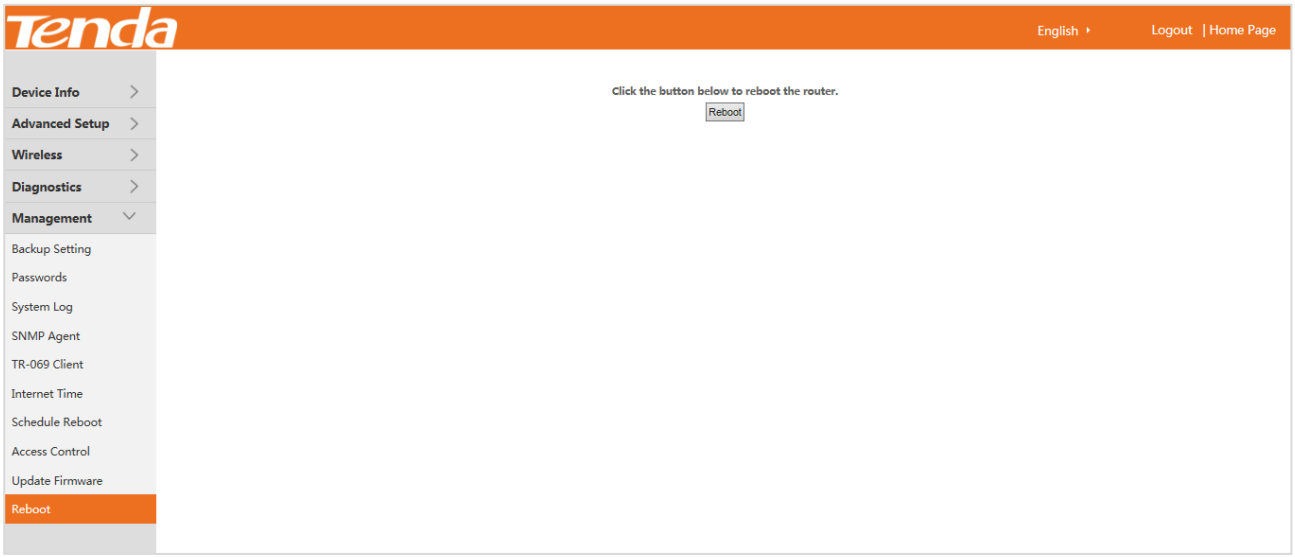
**Step 3** Click **TFTP Update Firmware**.

**---End**

# 7.10 Reboot

This function allows you to manually reboot the device.

Choose **Management** > **Reboot** to enter the configuration page.




To manually reboot the device, click **Reboot**.

# 8 Appendix

## 8.1 Connecting a Computer to the WiFi Network

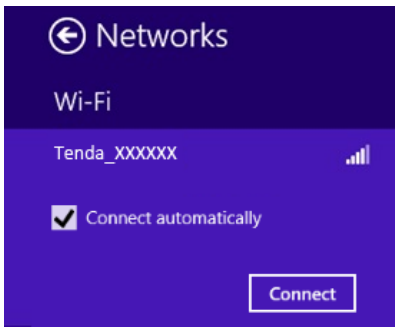
A computer can connect to the WiFi network of the router only if it has a wireless network adapter.

### Windows 8

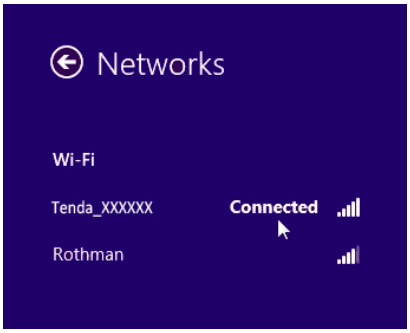
**Step 1** Right-click  in the lower-right corner of the desktop.

**Step 2** Select the WiFi network of the router from the network list that appears.

**Step 3** Follow the onscreen instruction to perform operation.








**--End**

NOTE

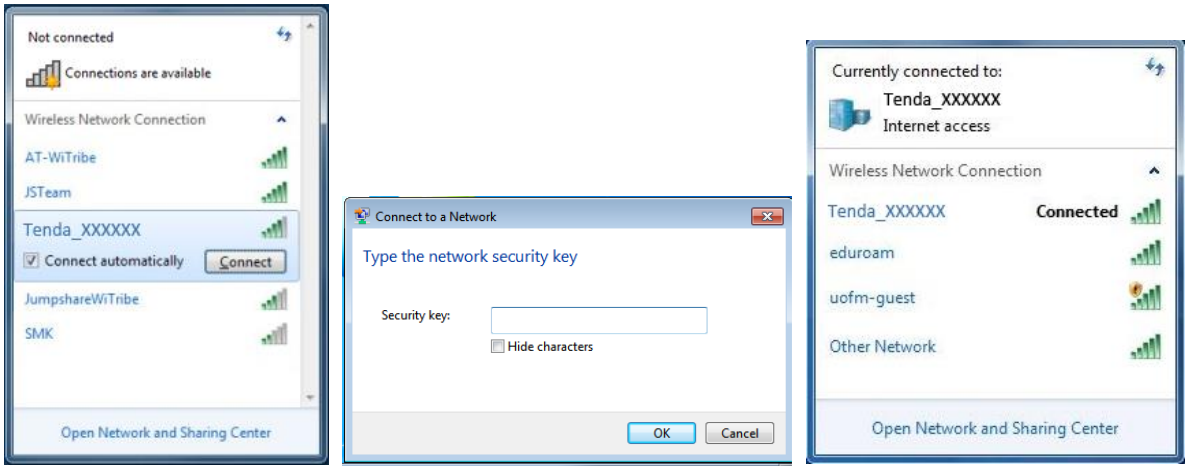
- If you cannot find the  icon, move the cursor to the upper-right corner of the desktop, choose **Settings** > **Control Panel** > **Network and Internet** > **Network and Sharing Center**, click **Change adapter settings**, right-click **WiFi**, and choose **Disable**. Then, right-click **WiFi**, and choose **Enable**.
- If the WiFi network is not detected, check whether the Airplane mode is enabled.

### Windows 7

**Step 1** Right-click  in the lower-right corner of the desktop.

**Step 2** Select the WiFi network of the router from the network list that appears.

**Step 3** Follow the onscreen instruction to perform operation.




**--End**

NOTE

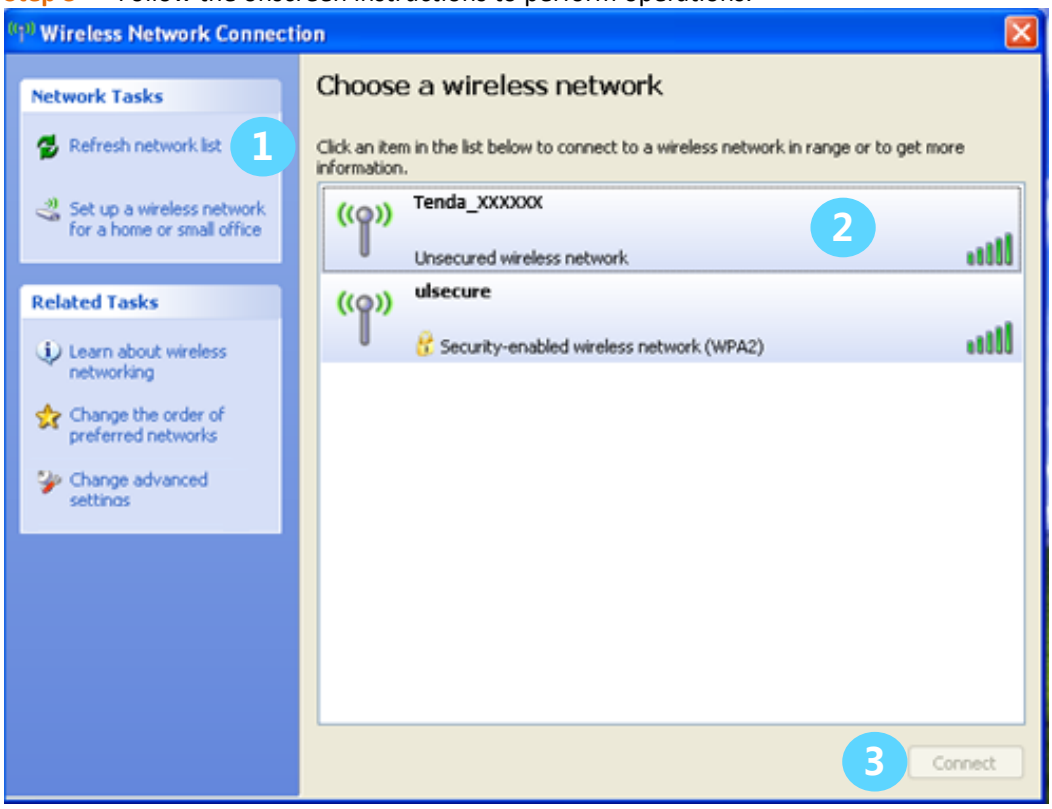
- If you cannot find the icon, choose **Start** > **Control Panel** > **Network and Internet** > **Network and Sharing Center**, click **Change adapter settings**, right-click **Wireless Network Connection**, and choose **Disable**. Then, right-click **Wireless Network Connection**, and choose **Enable**.
- If the wireless network is not detected, click in the upper-right corner to refresh the list of wireless networks.

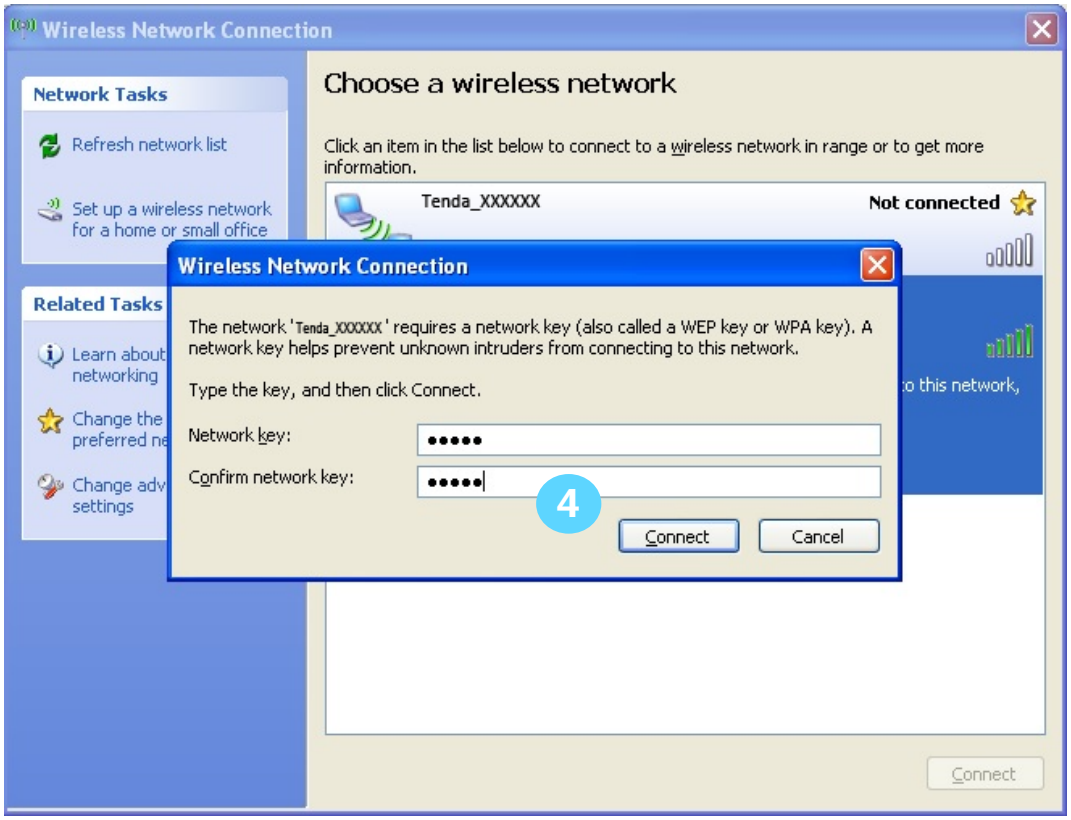
# Windows XP

**Step 1** Click in the lower-right corner of the desktop.

**Step 2** Select the WiFi network from the list that appears.

**Step 3** Follow the onscreen instructions to perform operations.






**--End**

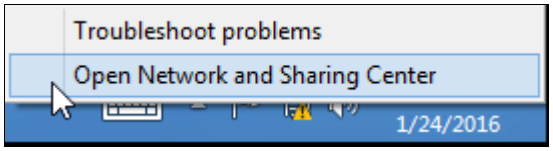
If the computer is connected to the network, **Connected** appears.

# 8.2 Configuring the Computer

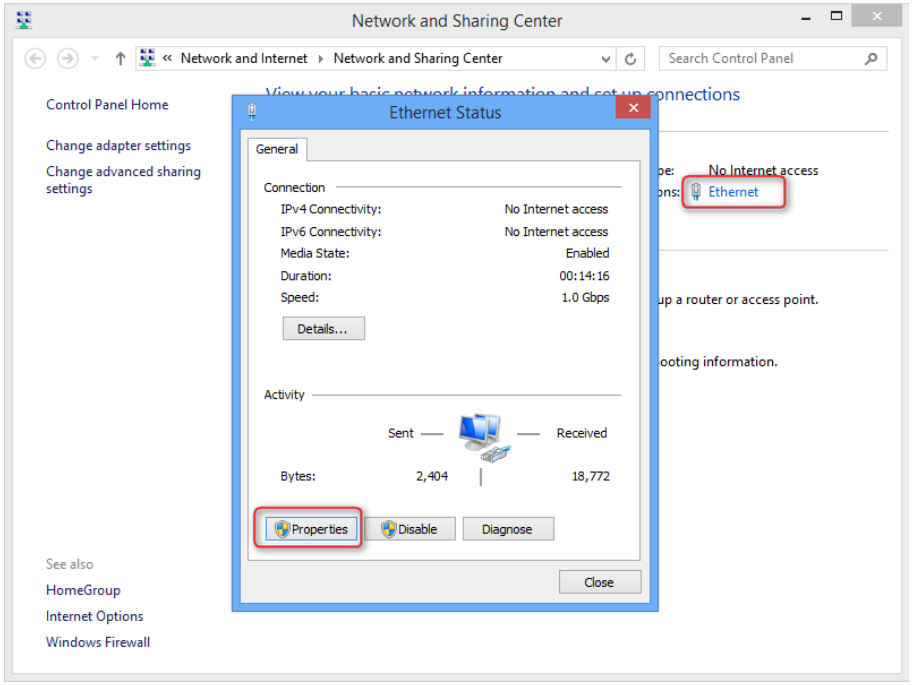
Perform the configuration procedure corresponding to Windows 8, Windows 7, or Windows XP, depending on your OS. A computer installed with a wired network adapter is used as an example to describe the procedures. The procedures for configuring computers installed with a wireless network adapter are similar to these procedures.

## Windows 8

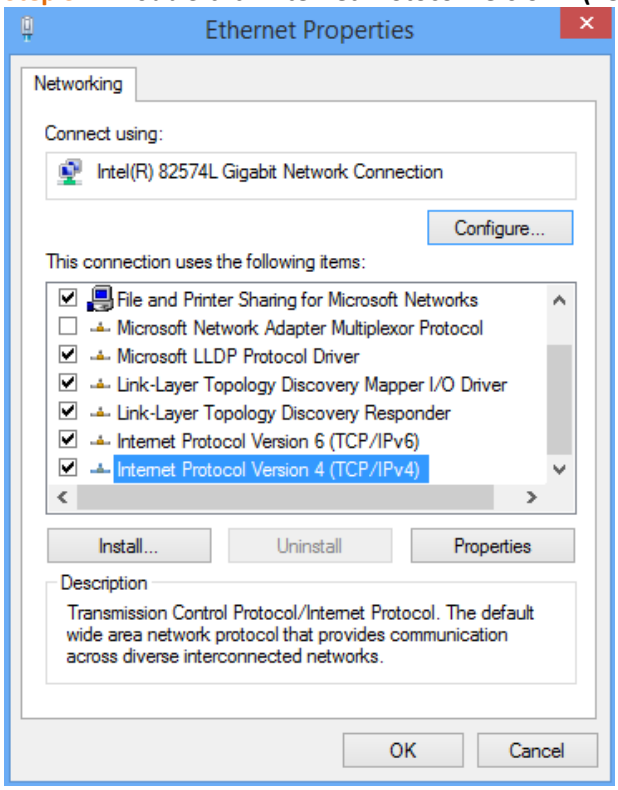
**Step 1** Right-click in the lower-right corner of the desktop and choose **Open Network and Sharing Center**.



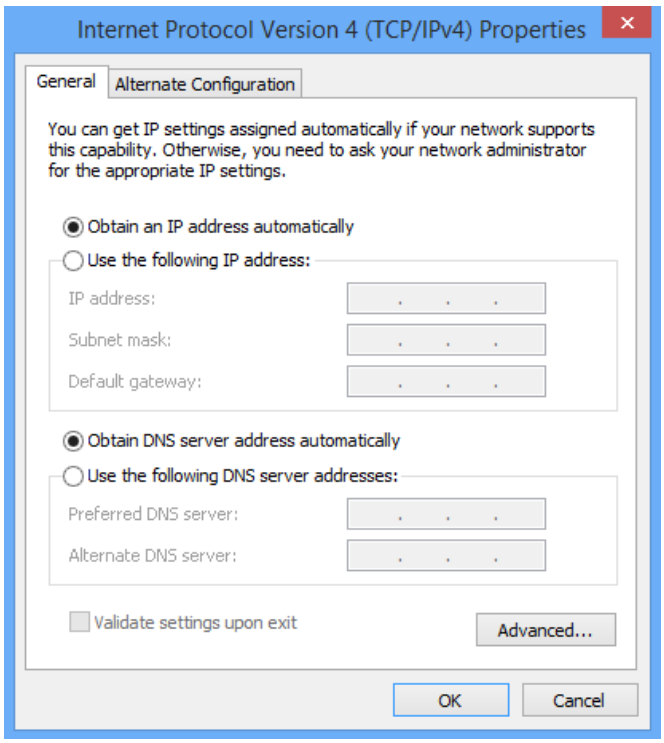

**Step 2** Click **Ethernet and then Properties**.




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




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

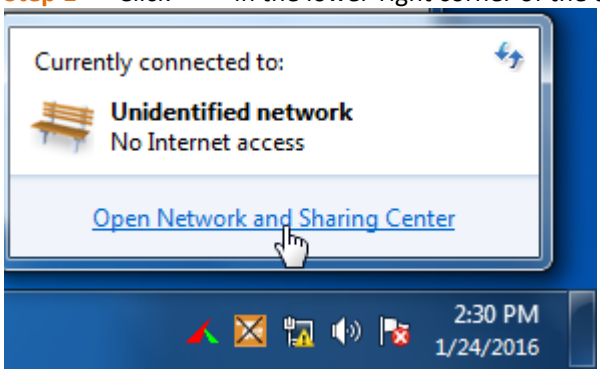



**Step 5** Click **OK** in the **Ethernet Properties** window.

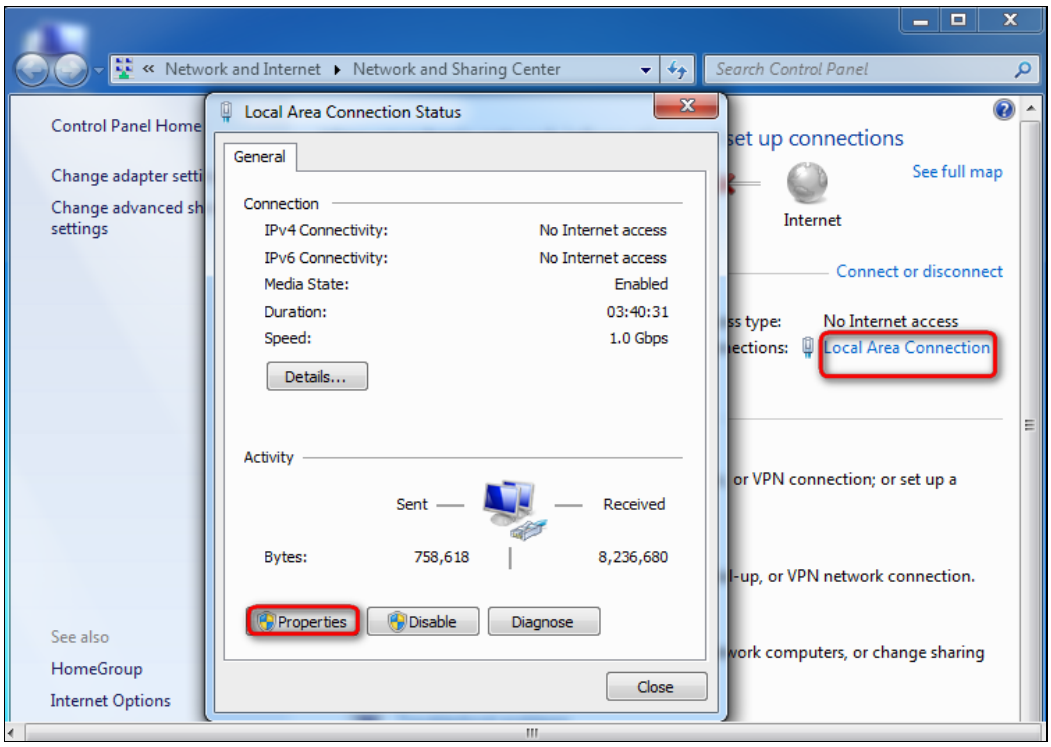
**---End**

# Windows 7

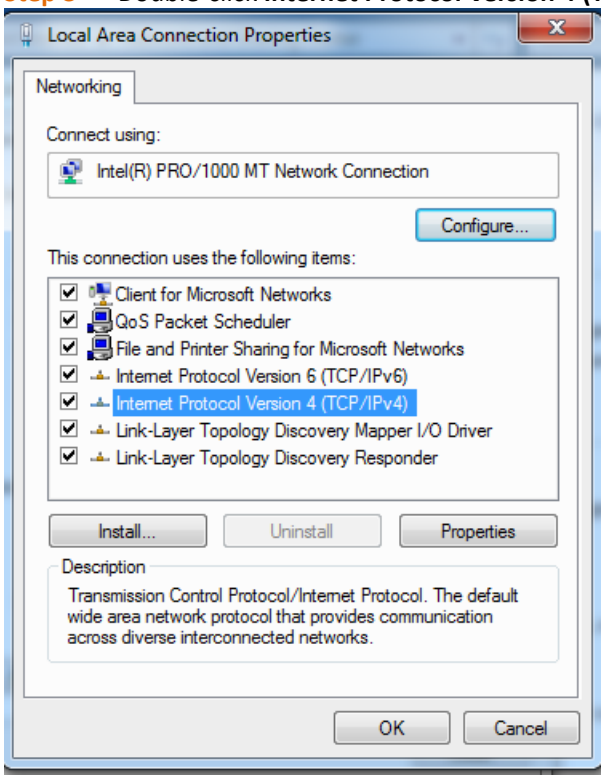
**Step 1** Click in the lower-right corner of the desktop and choose **Open Network and Sharing Center**.



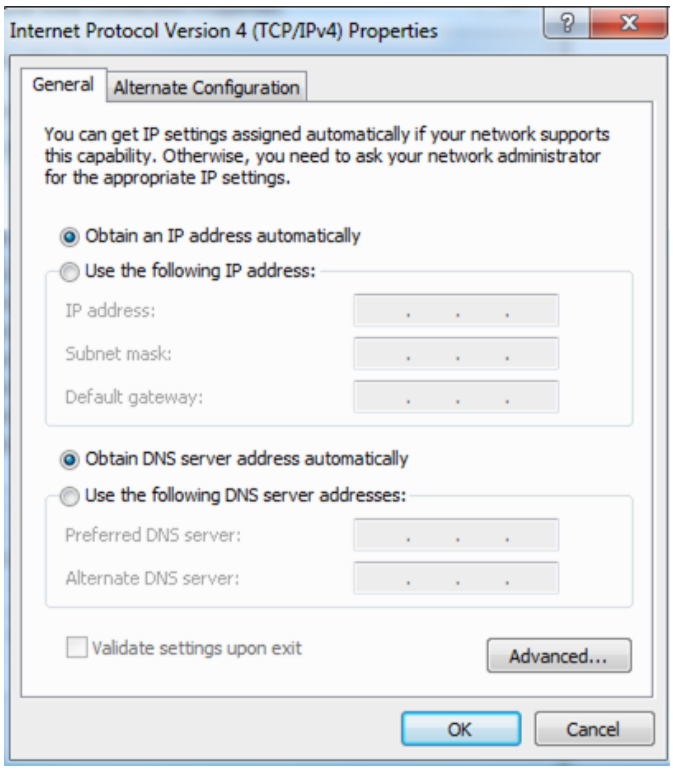

**Step 2** Click **Local Area Connection and then Properties**.




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




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



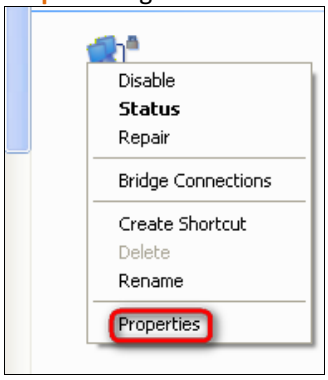

**Step 5** Click **OK** in the **Local Area Connection Properties** window.

**---End**

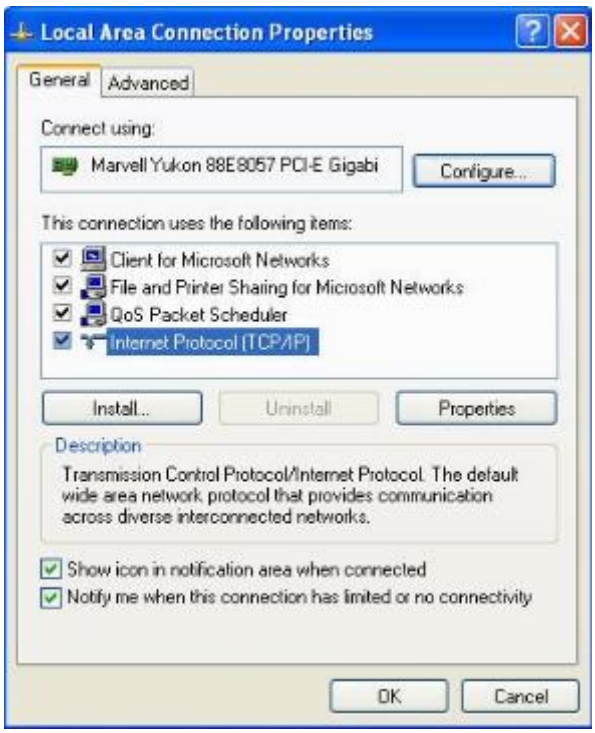
# Windows XP

**Step 1** Right-click **My Network Places** on the desktop and choose **Properties**.


**Step 2** Right-click **Local Area Connection and choose Properties**.




**Step 3** Double-click **Internet Protocol (TCP/IP)**.




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


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

**---End**

# 8.3 FAQ

**Q1: I cannot log in to the modem router's web UI. What should I do?**

**A1: Use the following method to troubleshoot the fault.**

- Verify that the Ethernet cable between your computer and the modem router is intact and well-connected.
- Verify that you type the correct login IP address in the browser's address bar.

- Verify that the IP address of your computer is 192.168.1.X (X is a number between 2 and 254).
- Use another computer, smartphone or iPad to login.
- Clear cache of your browser, or change another browser.
- Press the **RST** button for about 6 seconds to reset the modem router to factory default settings, and then try to login again.

**Q2: I cannot access to internet, what should I do?**

**A2: Use the following method to troubleshoot the fault.**

- Verify that the INTERNET LED is green and solid on.
- Verify that the modem router is connected to the internet through phone cable, Ethernet cable or 3G/4G dongle.
- Verify that the internet parameters you entered are correct (The screen instruction helps you confirm that).
- Uncheck the Auto Vlan Scan option, and configure it manually.
- Reboot the modem router.
- Reset the modem router to factory default settings and configure it again.
- Contact your ISP for help.

**Q3: I forget my WiFi password, what should I do?**

**A3: Use the following method to troubleshoot the fault.**

- If you do not change the WiFi password, it should be 12345678.
- If you change it, you can check it on the web UI of the modem router.
- If you forget the login password of the web UI as well, reset the wireless router to factory default settings. By default, there is no WiFi password and login name and password are both “admin”. Restore Method: Press the **RST** button for about 6 seconds and then release it.

## 8.4 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 | Sauna Lahti | 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]<br>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]<br>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<br>«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 communications | 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 |
| **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 communications | 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 | PPPoA LLC |
| 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 | South Western Bell | 0 | 35 | 1483 Bridged IP LLC |
| United States | Sprint (1) | 0 | 35 | PPPoA LLC |
| United States | Sprint (2) | 8 | 35 | PPPoE LLC |
| United States | Sprint Territory | 0 | 35 | PPPoE LLC |
| United States | Sure West Communications(1) | 0 | 34 | 1483 Bridged LLC Snap |
| United States | Sure West Communications(2) | 0 | 32 | PPPoE LLC |
| United States | Sure West 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 |

## 8.5 VLAN List

| Country | ISP | VLANID | Protocol |
|---|---|---|---|
| Albania | VDSL | 101 | PPPoE |
| | Other | | |
| Algeria | VDSL | Disabled | PPPoE |
| | Other | | |
| Argentina | Telecom | 150 | PPPoE |
| | Telefonica | 20 | PPPoE |
| | Other | | |
| Australia | TransAct | 10 | PPPoE |
| | NetSpeed | 10 | PPPoE |
| | CBIT Internet | 10 | PPPoE |
| | EveryNet | 10 | PPPoE |
| | IINET | 10 | PPPoE |
| | Infinite | 10 | PPPoE |
| | Officelink | 10 | PPPoE |
| | Velocitynet | 10 | PPPoE |

| | | | |
|---|---|---|---|
| | Other | | |
| Austria | Telekom | 7 | PPPoE |
| | Other | | |
| Bahrain | VDSL | Disabled | PPPoE |
| | Other | | |
| Balize | VDSL | Disabled | PPPoE |
| | Other | | |
| Belgium | VDSL | Disabled | PPPoE |
| | Other | | |
| Bengal | VDSL | Disabled | PPPoE |
| | Other | | |
| Bolivia | VDSL | Disabled | PPPoE |
| | Other | | |
| Brazil | VDSL | Disabled | PPPoE |
| | Other | | |
| Cameroon | VDSL | Disabled | PPPoE |
| | Other | | |
| Canada | VDSL | Disabled | PPPoE |
| | Other | | |
| Chile | VDSL | Disabled | PPPoE |
| | Other | | |
| Colombia | VDSL | Disabled | PPPoE |
| | Other | | |
| Costa Rica | VDSL | Disabled | PPPoE |
| | Other | | |
| Czech Republic | VDSL | Disabled | PPPoE |
| | Other | | |
| Denmark | VDSL | Disabled | PPPoE |
| | Other | | |
| Dominican Republic | VDSL | Disabled | PPPoE |

| | | | |
|---|---|---|---|
| | Other | | |
| Egypt | VDSL | Disabled | PPPoE |
| | Other | | |
| Fiji | VDSL | Disabled | PPPoE |
| | Other | | |
| Finland | VDSL | Disabled | PPPoE |
| | Other | | |
| France | Orange | 835 | PPPoE |
| | Sfr(1) PPPoE | 835 | PPPoE |
| | Sfr(1) Dynamic IP | 835 | Dynamic IP |
| | Sfr(2) PPPoE | 836 | PPPoE |
| | Sfr(2) Dynamic IP | 836 | Dynamic IP |
| | Free | 836 | PPPoE |
| | Bouygues Telecom | 200 | PPPoE |
| | Numericable | 200 | PPPoE |
| | Ovh PPPoE | 835 | PPPoE |
| | Ovh Dynamic IP | 835 | Dynamic IP |
| | Nordnet PPPoE | 835 | PPPoE |
| | Nordnet Dynamic IP | 835 | Dynamic IP |
| | Other | | |
| Georgia | VDSL | 200 | Dynamic IP |
| | Other | | |
| Germany | 1&1 | 7 | PPPoE |
| | Alice(1) | 11 | PPPoE |
| | Alice(2) | 7 | PPPoE |
| | Congstar | 7 | PPPoE |
| | Easybell | 7 | PPPoE |
| | EncoLine | 142 | Dynamic IP |
| | EWE TEL | 2019 | PPPoE |
| | GMX | 7 | PPPoE |

| | | | |
|---|---|---|---|
| | KielNET | 7 | PPPoE |
| | M-Net | 40 | PPPoE |
| | Osnatel | 2019 | PPPoE |
| | O2(1) | 11 | PPPoE |
| | O2(2) | 7 | PPPoE |
| | NetCologne/NetAachen(1) | 10 | PPPoE |
| | NetCologne/NetAachen(2) | 7 | PPPoE |
| | QSC/Q-DSL | 7 | PPPoE |
| | Telekom | 7 | PPPoE |
| | Swb(1) | Disabled | PPPoE |
| | Swb(2) | 7 | PPPoE |
| | Versatel | 7 | PPPoE |
| | Vodafone/Arcor(1) | 132 | PPPoE |
| | Vodafone/Arcor(2) | 7 | PPPoE |
| | Wilhelm.tel | 7 | PPPoE |
| | Willy.tel | 2511 | PPPoE |
| | Other | | |
| Greece | CYTA | 835 | PPPoE |
| | Forthnet | 1102 | PPPoE |
| | Hellas Online | 835 | PPPoE |
| | OTE | 835 | PPPoE |
| | WIND | 835 | PPPoE |
| | Other | | |
| Guatemala | VDSL | 835 | PPPoE |
| | Other | | |
| Honduras | VDSL | 835 | PPPoE |
| | Other | | |
| Hong Kong | Hutchison PPPoE | Disabled | PPPoE |
| | Hutchison Dynamic IP | Disabled | Dynamic IP |
| | Hutchison Static IP | Disabled | Static IP |

| | | | |
|---|---|---|---|
| | WharfT&T PPPoE | Disabled | PPPoE |
| | WharfT&T Dynamic IP | Disabled | Dynamic IP |
| | WharfT&T Static IP | Disabled | Static IP |
| | Other | | |
| Hungary | VDSL | Disabled | PPPoE |
| | Other | | |
| Iceland | VDSL | Disabled | PPPoE |
| | Other | | |
| India | VDSL | Disabled | PPPoE |
| | Other | | |
| Indonesia | VDSL | Disabled | PPPoE |
| | Other | | |
| Iran | VDSL | Disabled | PPPoE |
| | Other | | |
| Ireland | Eircom | 10 | PPPoE |
| | Bbnet | 10 | PPPoE |
| | Other | | |
| Israel | BEZEQ | Disabled | PPPoE |
| | Other | | |
| Italy | VDSL | Disabled | PPPoE |
| | Other | | |
| Jamaica | VDSL | Disabled | PPPoE |
| | Other | | |
| Jordan | VDSL | Disabled | PPPoE |
| | Other | | |
| Kazakhstan | VDSL | Disabled | PPPoE |
| | Other | | |
| Kenya | VDSL | Disabled | PPPoE |
| | Other | | |
| Korea | VDSL | Disabled | PPPoE |

| | | | |
|---|---|---|---|
| | Other | | |
| kuwait | VDSL | Disabled | PPPoE |
| | Other | | |
| Lebanon | VDSL | Disabled | PPPoE |
| | Other | | |
| Lesotho | VDSL | Disabled | PPPoE |
| | Other | | |
| Macau | VDSL | Disabled | PPPoE |
| | Other | | |
| Malaysia | VDSL | Disabled | PPPoE |
| | Other | | |
| Mexico | VDSL | Disabled | PPPoE |
| | Other | | |
| Morocco | VDSL | Disabled | PPPoE |
| | Other | | |
| Nepal | VDSL | Disabled | PPPoE |
| | Other | | |
| Netherlands | KPN PPPoE | 6 | PPPoE |
| | KPN Dynamic IP | 6 | Dynamic IP |
| | Telfort PPPoE | 34 | PPPoE |
| | Telfort Dynamic IP | 34 | Dynamic IP |
| | Voiceworks | 101 | Dynamic IP |
| | XS4ALL PPPoE | 6 | PPPoE |
| | XS4ALL Dynamic IP | 6 | Dynamic IP |
| | Other | | |
| New Zealand | Spark/Telecom | 10 | PPPoE |
| | KiwiLink | 10 | PPPoE |
| | Slingshot | 10 | PPPoE |
| | Vodafone NZ | 10 | PPPoE |
| | Snap | 10 | PPPoE |

| | | | |
|---|---|---|---|
| | Myrepublic | 10 | PPPoE |
| | Callplus PPPoE | 10 | PPPoE |
| | Other | | |
| Norway | VDSL | Disabled | PPPoE |
| | Other | | |
| Oman | VDSL | Disabled | PPPoE |
| | Other | | |
| Pakistan | VDSL | Disabled | PPPoE |
| | Other | | |
| Palestine | VDSL | Disabled | PPPoE |
| | Other | | |
| Panama | VDSL | Disabled | PPPoE |
| | Other | | |
| Peru | VDSL | Disabled | PPPoE |
| | Other | | |
| Paraguay | VDSL | Disabled | PPPoE |
| | Other | | |
| Philippines | VDSL | Disabled | PPPoE |
| | Other | | |
| Poland | Orange | Disabled | PPPoE |
| | Netia | Disabled | PPPoE |
| | Other | | |
| Portugal | VDSL | Disabled | PPPoE |
| | Other | | |
| Puerto Rico | VDSL | Disabled | PPPoE |
| | Other | | |
| Qatar | Q-Tel/Ooreedo | 8 | PPPoE |
| | Other | | |
| Romania | VDSL | Disabled | PPPoE |
| | Other | | |

| | | | |
|---|---|---|---|
| Russia | Rostelecom | Disabled | PPPoE |
| | Other | | |
| Saudi Arabia | VDSL | Disabled | PPPoE |
| | Other | | |
| Singapore | VDSL | Disabled | PPPoE |
| | Other | | |
| Slovakia | T-COM | 2510 | PPPoE |
| | Orange | 2510 | PPPoE |
| | AMIS | Disabled | PPPoE |
| | Other | | |
| South Africa | VDSL | Disabled | PPPoE |
| | Other | | |
| Spain | Telefonica | 6 | PPPoE |
| | Vodafone | 100 | PPPoE |
| | Jazztel | 1074 | PPPoE |
| | Other | | |
| Sri Lanka | VDSL | Disabled | PPPoE |
| | Other | | |
| Sweden | VDSL | Disabled | PPPoE |
| | Other | | |
| Switzerland | Swisscom | 10 | PPPoE |
| | Other | | |
| Syria | SAMA-Net | 10 | PPPoE |
| | Other | | |
| Taiwan | VDSL | Disabled | PPPoE |
| | Other | | |
| Thailand | VDSL | Disabled | PPPoE |
| | Other | | |
| Tonga | VDSL | Disabled | PPPoE |
| | Other | | |

| | | | |
|---|---|---|---|
| Trinidad and Tobago | VDSL | Disabled | PPPoE |
| | Other | | |
| Turkey | Turktelekom | 35 | PPPoE |
| | Superonline | 35 | PPPoE |
| | Vodafone | 35 | PPPoE |
| | Turknet | 35 | PPPoE |
| | D-Smart | 35 | PPPoE |
| | Other | | |
| Ukraine | VDSL | Disabled | PPPoE |
| | Other | | |
| United Arab Emirates | VDSL | Disabled | PPPoE |
| | Other | | |
| United Kingdom | AAISP | 101 | PPPoE |
| | BT | 101 | PPPoE |
| | Claranet | 101 | PPPoE |
| | EE | 101 | PPPoE |
| | Idnet | 101 | PPPoE |
| | Plusnet | 101 | PPPoE |
| | TalkTalk | 101 | Dynamic IP |
| | Vispa | 101 | PPPoE |
| | Zen | 101 | PPPoE |
| | Other | | |
| United States | VDSL | Disabled | PPPoE |
| | Other | | |
| Uraguay | VDSL | Disabled | PPPoE |
| | Other | | |
| Uzbekistan | VDSL | Disabled | PPPoE |
| | Other | | |
| Venezuela | VDSL | Disabled | PPPoE |
| | Other | | |

| | | | |
|---|---|---|---|
| Vietnam | VDSL | Disabled | PPPoE |
| | Other | | |
| Yemen | VDSL | Disabled | PPPoE |
| | Other | | |
| Zimbabwe | VDSL | Disabled | PPPoE |
| | Other | | |

## 8.6 Safety and Emission Statement

**Declaration of Conformity**

Hereby, SHENZHEN TENDA TECHNOLOGY CO. LTD. declares that the radio equipment type V300 is in compliance with Directive 2014/53/EU.

The full text of the EU declaration of conformity is available at the following internet address: http://www.tendacn.com/en/service/page/ce.html

Operate Frequency: 2412-2472 MHz

EIRP Power (Max.): 19.5 dBm

Software Version:

Operating Temperature: 0°C~40°C

Operating Humidity: (10~90) %RH, non-condensing

CE

**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 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.

 Caution:

Adapter Model: BN036-A12012U

Manufacture: SHENZHEN HEWEISHUN NETWORK TECHNOLOGY CO.,LTD.

Input: 100-240V~, 50/60Hz 0.4A

Output: 12Vdc, 1.0A

: DC Voltage


RECYCLING

This product bears the selective sorting symbol for Waste electrical and electronic equipment (WEEE). This means that this product must be handled pursuant to European directive 2012/19/EU in order to be recycled or dismantled to minimize its impact on the environment.

User has the choice to give his product to a competent recycling organization or to the retailer when he buys a new electrical or electronic equipment.

**FCC Statement**

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference 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 or more 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.

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.

**Radiation Exposure Statement**

This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

**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.

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.