Tenda

300Mbps Wireless N VDSL2 Modem Router

User Guide

Copyright Statement

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

Disclaimer

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

Preface

Thank you for choosing Tenda! Please read this user guide before you start with i6.

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
AP	Access Point
DDNS	Dynamic Domain Name System
DHCP	Dynamic Host Configuration Protocol
DLNA	Digital Living Network Alliance
DMZ	Demilitarized Zone
DNS	Domain Name System
IPTV	Internet Protocol Television
ISP	Internet Service Provider
L2TP	Layer 2 Tunneling Protocol

Acronym or Abbreviation	Full Spelling
MPPE	Microsoft Point-to-Point Encryption
PPP	Point To Point Protocol
PPPoE	Point-to-Point Protocol over Ethernet
PPTP	Point to Point Tunneling Protocol
SSID	Service Set Identifier
STB	Set Top Box
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WISP	Wireless Internet Service Provider
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.

☎ Hotline	Global: (86) 755-27657180	✉ Email	support@tenda.cn
	United States: 1-800-570-5892		
	Canada: 1-888-998-8966		
	Hong Kong: 00852-81931998		
	Australia: 1300787922		
	New Zealand: 800787922		
🏠 Website	http://www.tendacn.com	S Skype	tendasz

Contents

1 Get to Know the Device

1.1 Overview

V300 can serve as a VDSL2 modem with high downlink 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 Built-in ADSL2+ modem, wired router, wireless router and switch
- Optional Ethernet and ADSL Uplinks: Access the internet via DSL port or WAN port (RJ45 port)
- Multiple Internet Connection Types: Bridging, PPPoE, IPoE, PPPoA, IPoA, dynamic IP and static IP
- Tenda Quick Setup Wizard for easy and fast installation and configuration
- Up to 300 Mbps wireless transmission speed for HD video streaming and online gaming
- Compatible with 802.11b/g Wireless devices
- One-touch WPS ensures a quick and secure wireless network connection
- USB port lets you access and share files through an attached USB hard drive
- Port 1 can function either as a LAN or a WAN port
- Poet 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 keeps your kids Internet experience safe using flexible and customizable filter settings
- IPTV Service lets you surf Internet while watching online TV
- 6 kV lightning—proof design fits into lightning-intensive environment
- FDM technology enables telephoning, faxing and surfing activities to proceed concurrently without mutual interference
- Advanced Features: IPv6, DDNS, virtual server, DMZ, port triggering, IP filter, MAC filter, UPnP, and so on.

1.3 Packing List

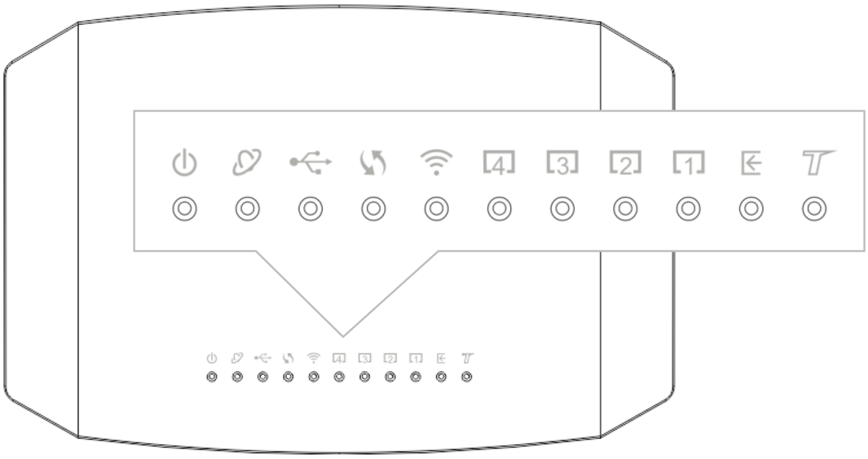
Your box should contain the following items:

- 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

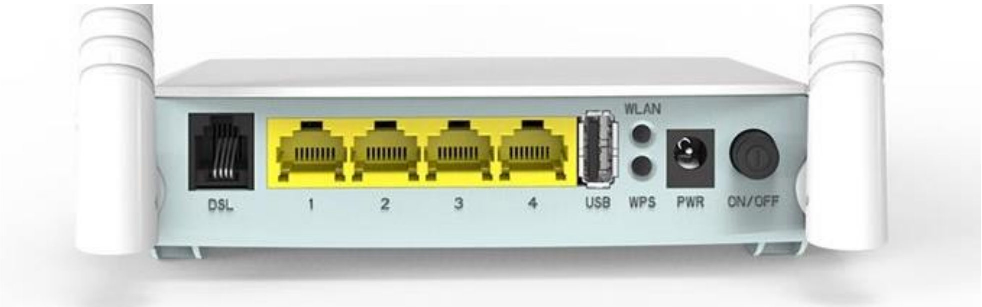
1.4.1 Front Panel



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 safely.
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.
4 3 2 1 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	The DSL negotiation is completed.
		Blinking	The device is doing DSL negotiation.
		Off	No connection is detected on the DSL port.
T			This LED is reserved.

1.4.2 Rear panel

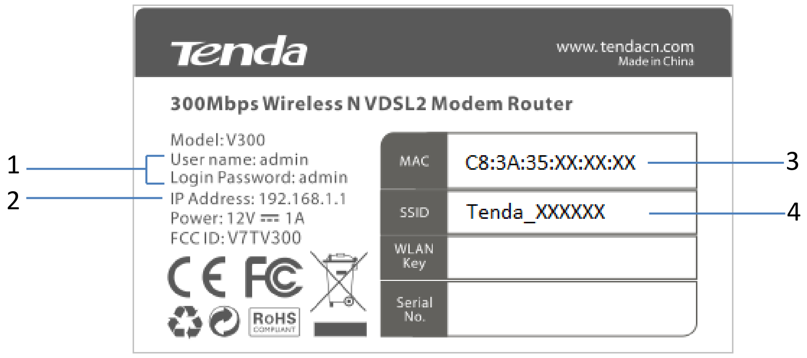


Button/Port	Description
ON/OFF	Power button. Used to turn on/off the modem router.
PWR	Power jack. Used to connect to the included power adapter for power supply.
WLAN	This button is used to enable or disable the wireless feature.
WPS	Enable the WPS function on the web UI of the modem router. Press this button for 3 seconds and then release it to perform the WPS negotiation process. Within 2 minutes, 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 a computer, switch, 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 telephone cable.
RST *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. Use of a power adapter with different voltage rating may damage the device.

1.4.3 Product Label



Tenda

www.tendacn.com
Made in China

300Mbps Wireless N VDSL2 Modem Router

Model: V300
User name: admin
Login Password: admin
IP Address: 192.168.1.1
Power: 12V ⎓ 1A
FCC ID: V7TV300

MAC	C8:3A:35:XX:XX:XX
SSID	Tenda_XXXXXX
WLAN Key	
Serial No.	

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: Enter this IP address in the address bar of a web browser to log in to the web UI of the modem router

3 MAC address of the modem router

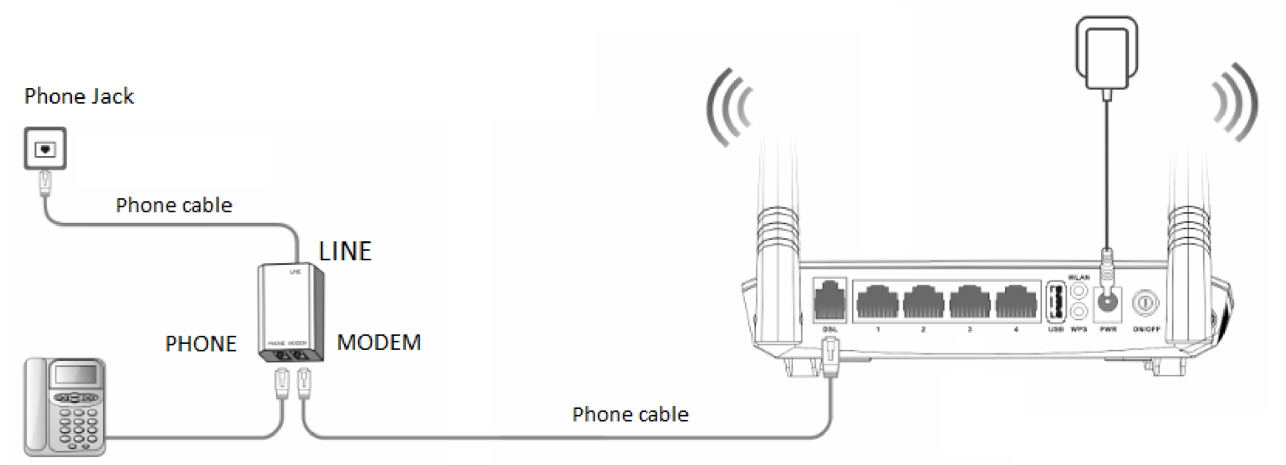
4 Default wireless network name of the modem router

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 phone jack.

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.

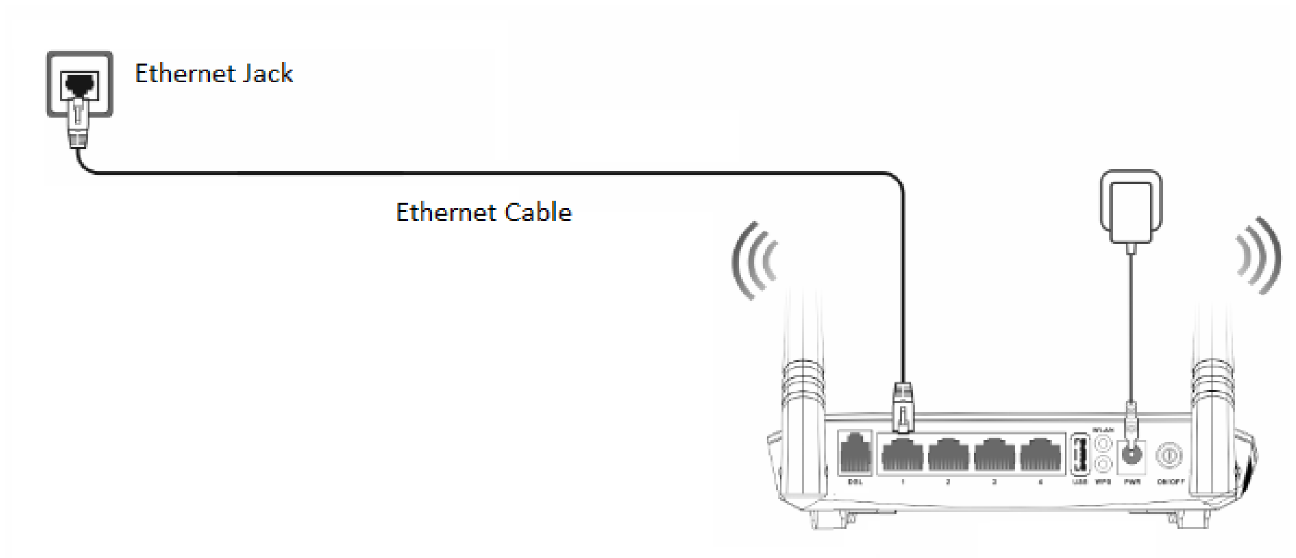
Step 4 Power on the modem router.

--End

If you do not need to use the phone service, directly connect the phone jack 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 Ethernet jack to the port 1 of the modem router.

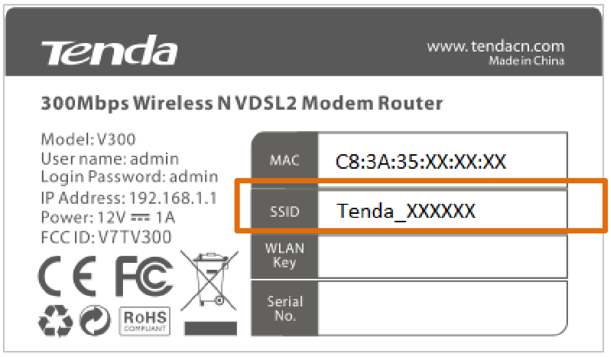
2.1.3 3G/4G Dongle

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 panel of the modem router.



Tenda www.tendacn.com Made in China

300Mbps Wireless N VDSL2 Modem Router

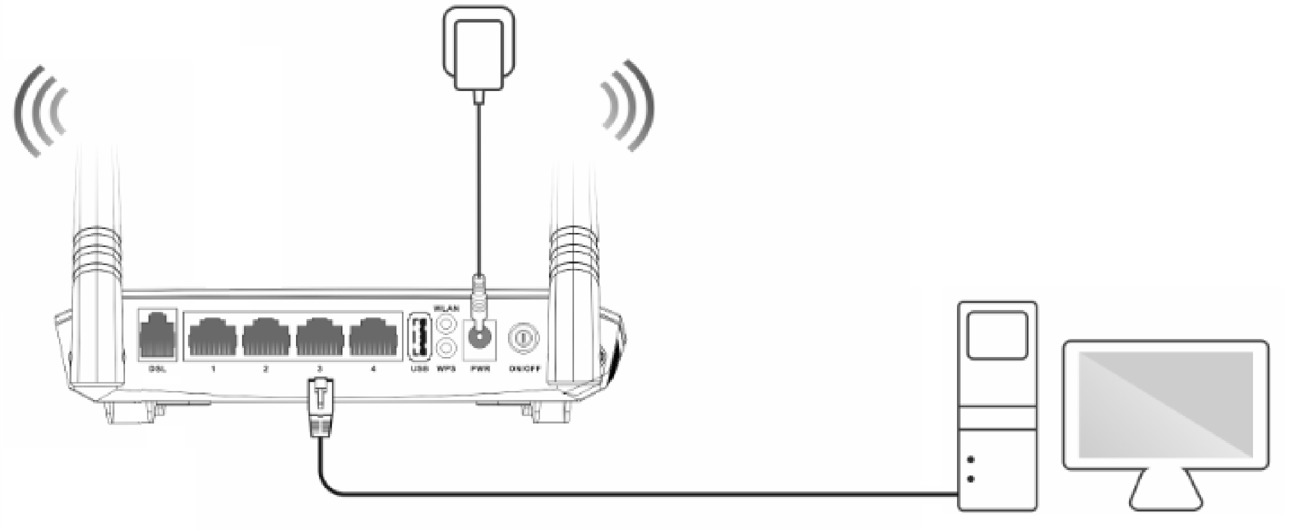
Model: V300
User name: admin
Login Password: admin
IP Address: 192.168.1.1
Power: 12V ⎓ 1A
FCC ID: V7TV300

MAC	C8:3A:35:XX:XX:XX
SSID	Tenda_XXXXXX
WLAN Key	
Serial No.	

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



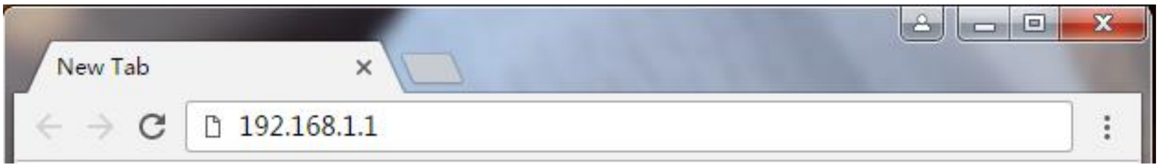
Connect your computer to an available LAN port (port 1, 2, 3, or 4) of the modem router.

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 tap **Enter** on the keyboard.

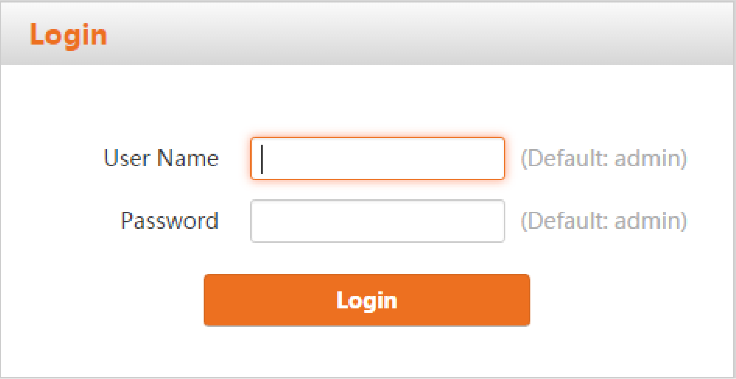
TIP

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



192.168.1.1

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


Login

User Name (Default: admin)

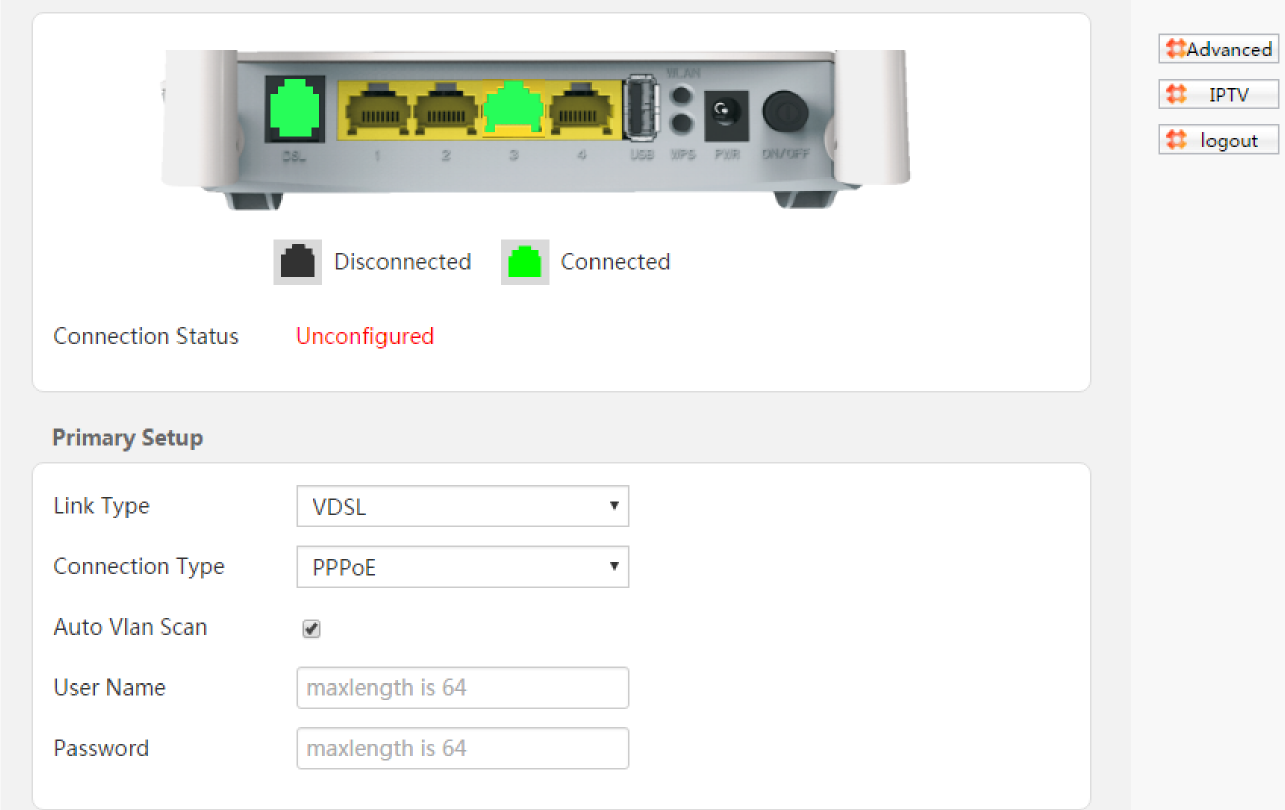
Password (Default: admin)

--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.



Connection Status Unconfigured

Primary Setup

Link Type: VDSL

Connection Type: PPPoE

Auto Vlan Scan ☑

User Name: maxlength is 64

Password: maxlength is 64

VDSL

If the link type your internet service provider provided to you is **VDSL**, follow the procedures 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 complete the related internet parameters.

Connection Type		Description
PPPoE		Select thus type if your internet service provider (ISP) provides a user name and password to you for internet access.
IPoE	Dynamic IP	Select thus type if your ISP does not provide any parameters to you for internet access.
	Static IP	Select thus type if your ISP provides a static IP address and other related information to you for internet access.
Bridge		Select thus 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 internet service provider 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 (PPP over Ethernet)		If your internet service provider (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 thus type if your ISP does not provide any parameters to you for internet access.
	Static IP	If your internet service provider 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 thus 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 internet service provider.

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.

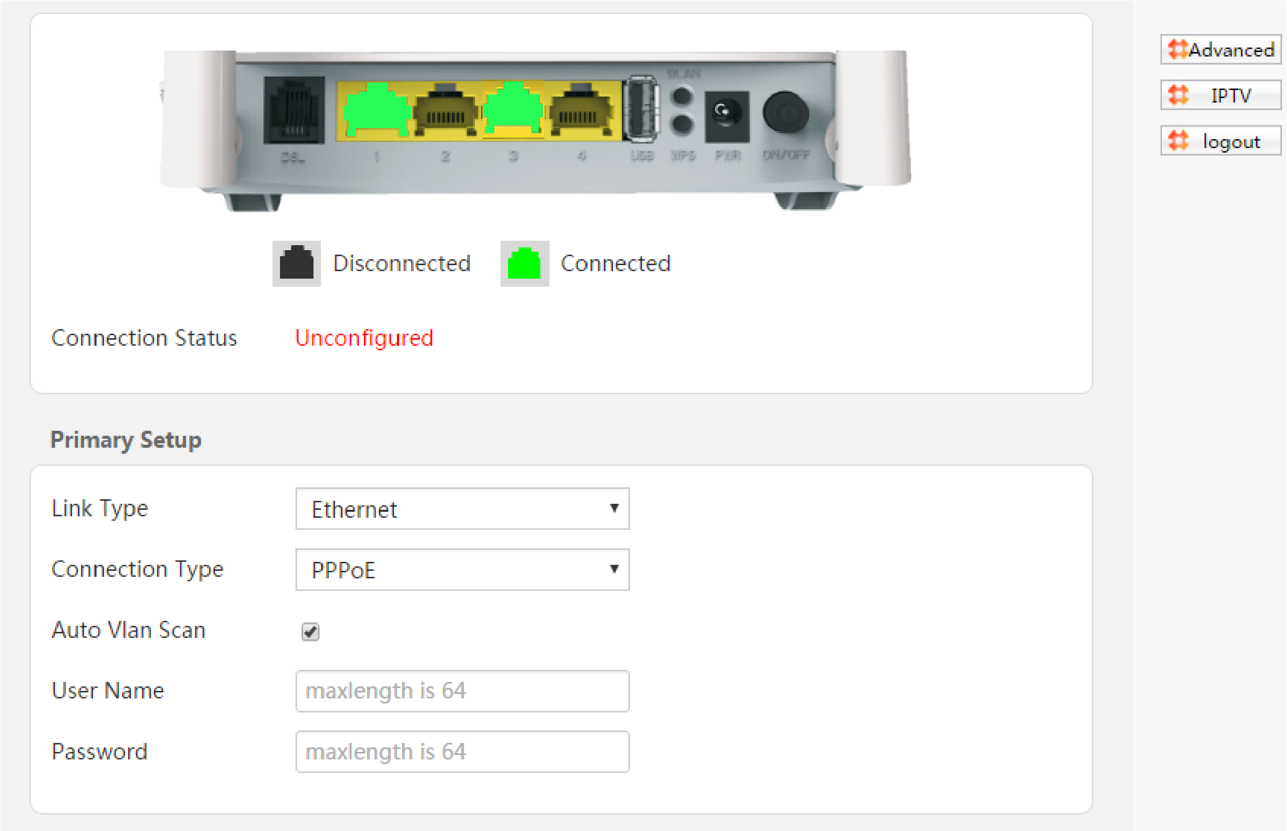
--End

TIP

If your country/region and ISP are not covered 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.



⬛ Disconnected 🟩 Connected

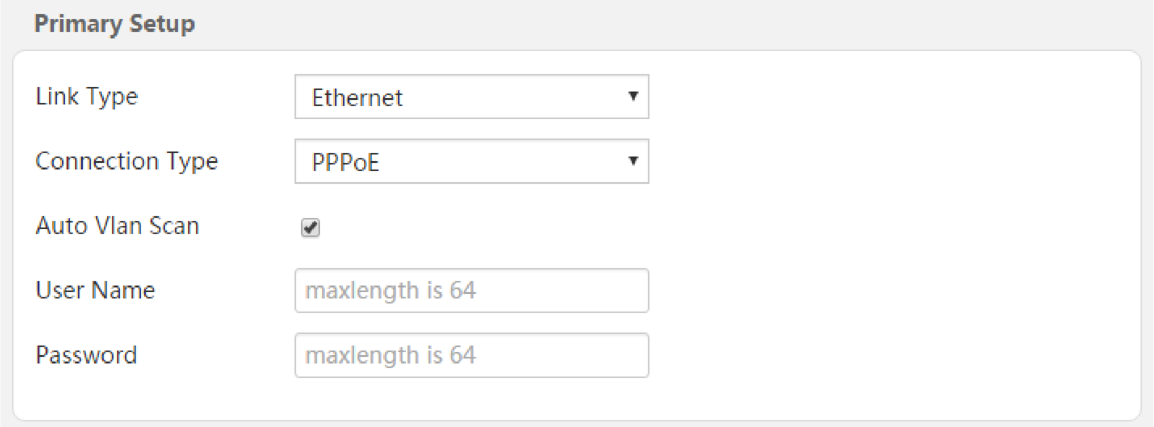
Connection Status	Unconfigured

Primary Setup

Link Type	Ethernet ▾
Connection Type	PPPoE ▾
Auto Vlan Scan	☑
User Name	maxlength is 64
Password	maxlength is 64

PPPoE

Use thus 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.



Primary Setup

Link Type	Ethernet ▾
Connection Type	PPPoE ▾
Auto Vlan Scan	☑
User Name	maxlength is 64
Password	maxlength is 64

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.

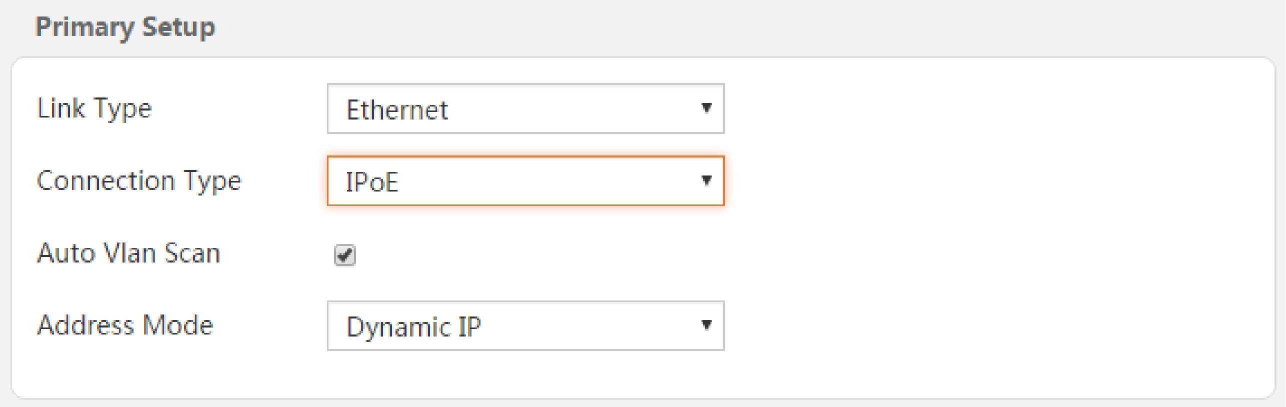
Step 5 Click **OK** on the bottom of the page to apply the settings.

--End

IPoE

Dynamic IP

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



Primary Setup

Link Type: Ethernet

Connection Type: IPoE

Auto Vlan Scan: ☑

Address Mode: Dynamic IP

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**.

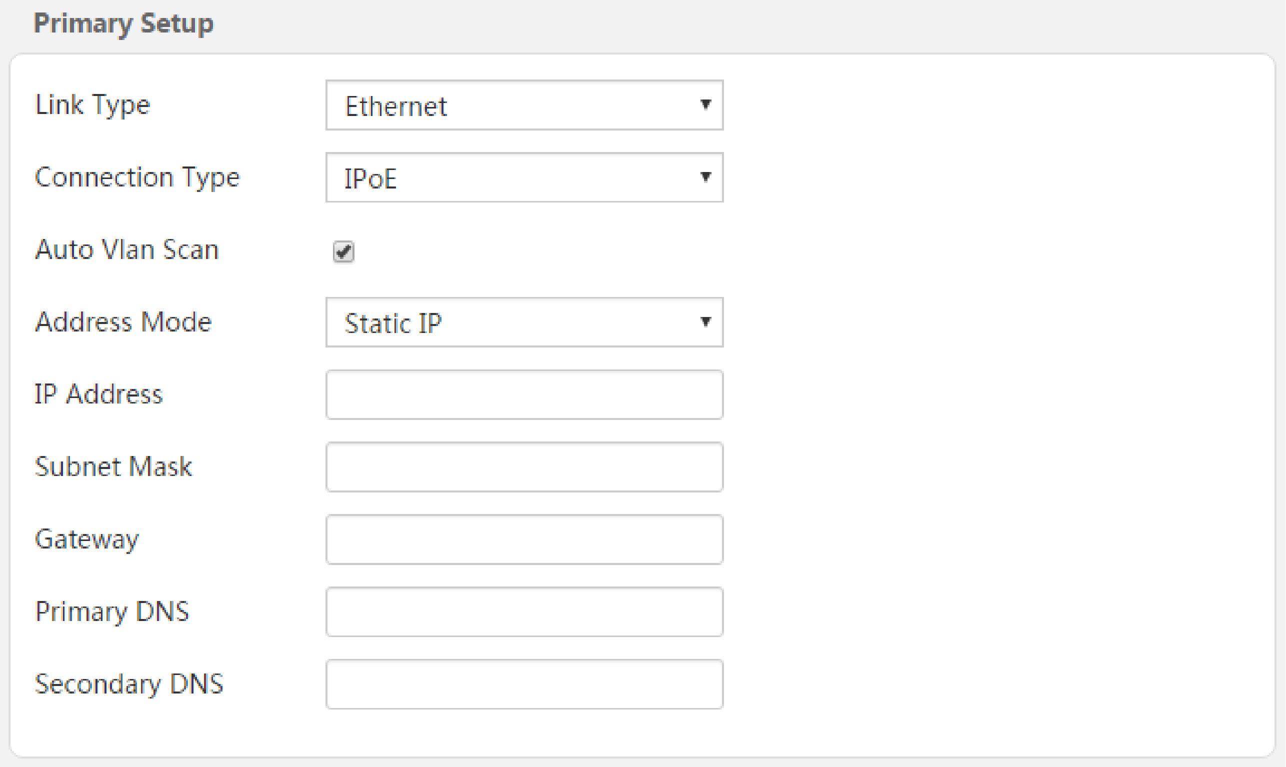
Step 4 **Address Mode**: Select **Dynamic IP**.

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

--End

Static IP

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



Primary Setup

Link Type: Ethernet

Connection Type: IPoE

Auto Vlan Scan: ☑

Address Mode: Static IP

IP Address:

Subnet Mask:

Gateway:

Primary DNS:

Secondary DNS:

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**.

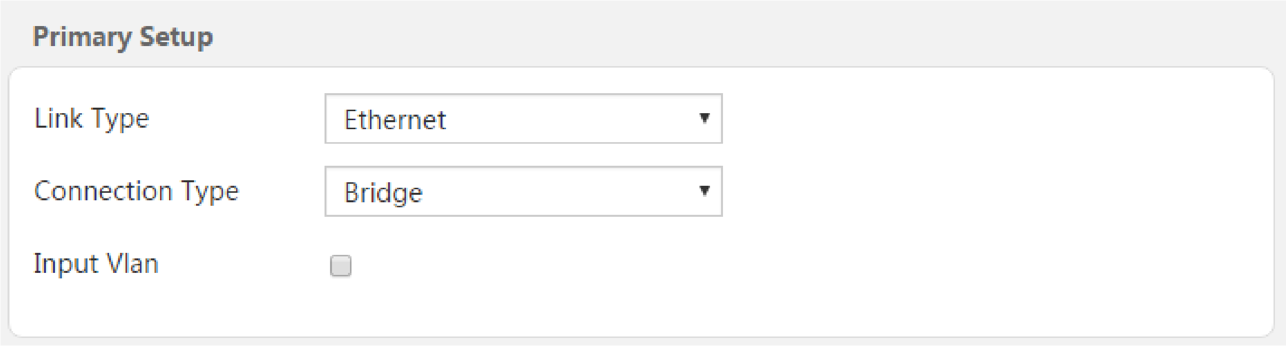
Step 5 Enter the static IP address, and other related parameters.

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

--End

Bridge

Select thus 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.



Primary Setup

Link Type: Ethernet

Connection Type: Bridge

Input Vlan: □

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

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

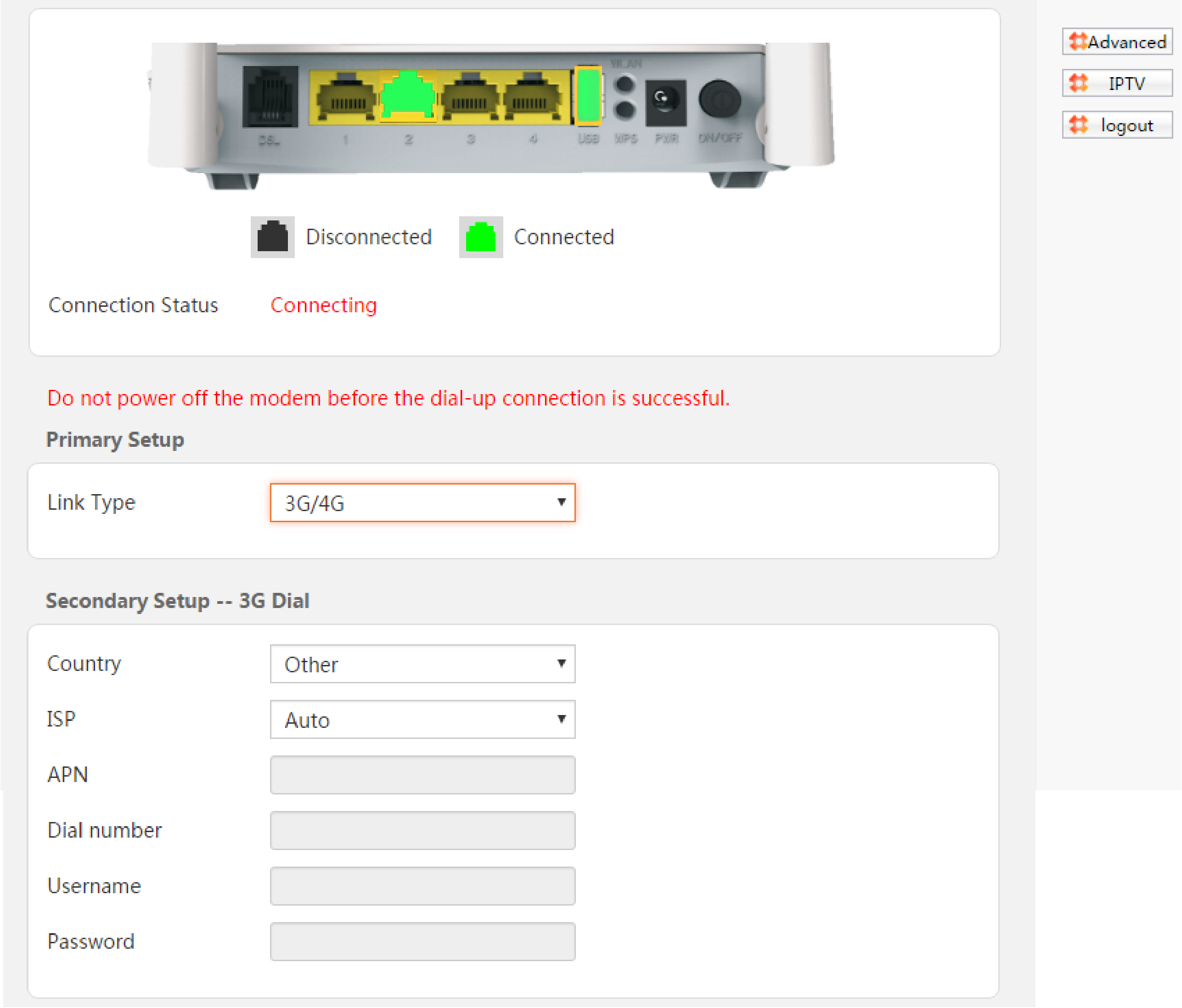
Step 3 **Connection Type**: Select **Bridge**.

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

--End

2.4.3 3G/4G Dial

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.



■ Disconnected 🟩 Connected

Connection Status Connecting

Do not power off the modem before the dial-up connection is successful.

Primary Setup

Link Type	3G/4G

Secondary Setup -- 3G Dial

Country	Other
ISP	Auto
APN	
Dial number	
Username	
Password	

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 internet service provider.

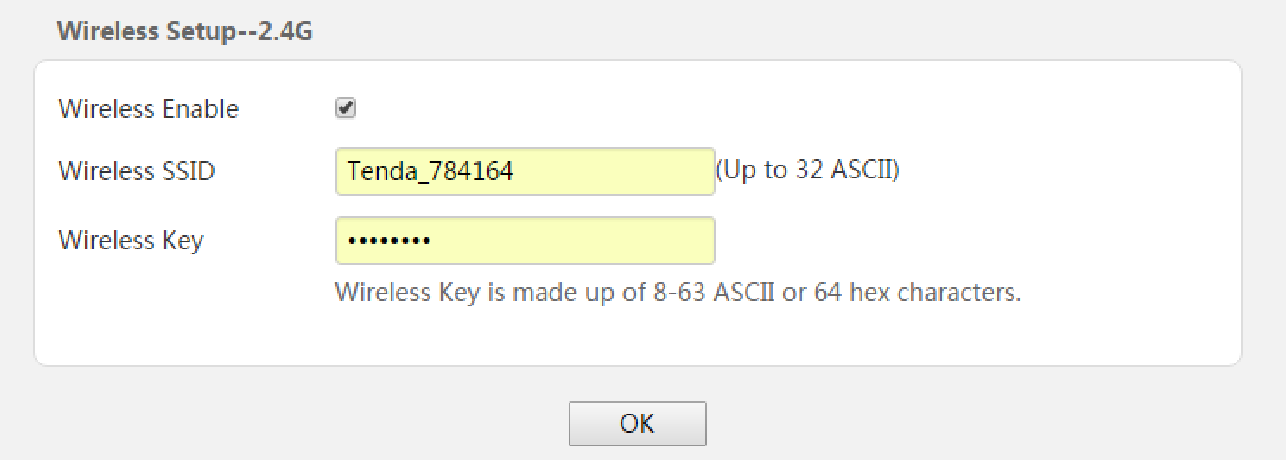
Step 5 **(Optional) APN/Dial number/Username/Password**: Generally, if you select correct country and ISP, the necessary parameters can be automatically filled in. If not, enter them manually according to the internet parameters your ISP provided.

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.



Wireless Setup--2.4G

Wireless Enable ☑

Wireless SSID: Tenda_784164 (Up to 32 ASCII)

Wireless Key: ••••••••

Wireless Key is made up of 8-63 ASCII or 64 hex characters.

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.

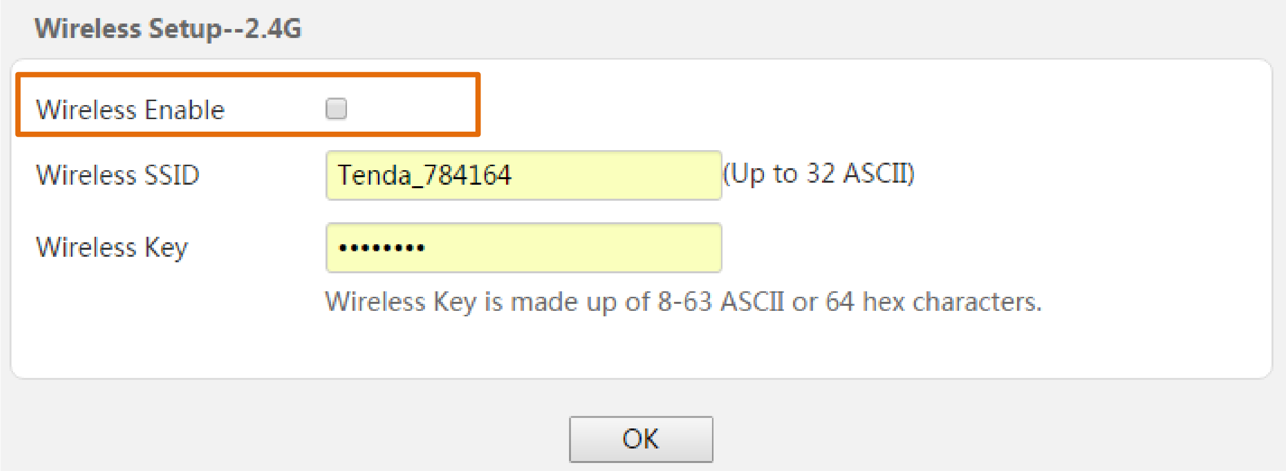
Step 3 Enter a new WiFi password in the **Wireless Key** box.

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

--End

To disable wireless feature:

Uncheck the **Wireless Enable** option, and click **OK**.



Wireless Setup--2.4G

Wireless Enable □

Wireless SSID: Tenda_784164 (Up to 32 ASCII)

Wireless Key: ••••••••

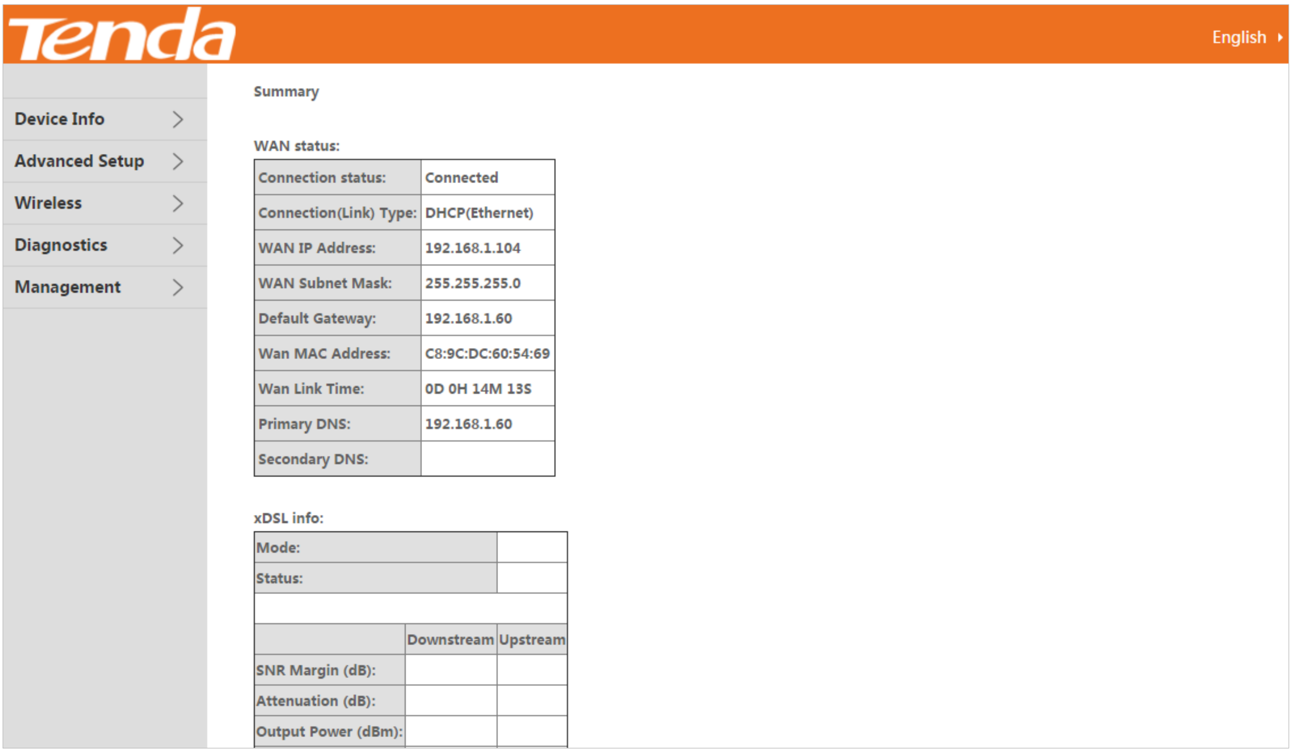
Wireless Key is made up of 8-63 ASCII or 64 hex characters.

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



Summary

WAN status:

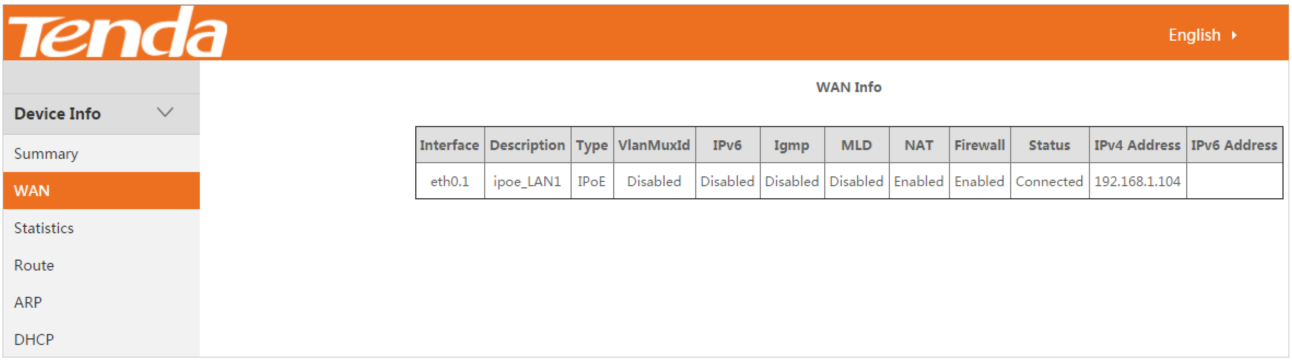
Connection status:	Connected
Connection(Link) Type:	DHCP(Ethernet)
WAN IP Address:	192.168.1.104
WAN Subnet Mask:	255.255.255.0
Default Gateway:	192.168.1.60
Wan MAC Address:	C8:9C:DC:60:54:69
Wan Link Time:	0D 0H 14M 13S
Primary DNS:	192.168.1.60
Secondary DNS:	

xDSL info:

Mode:		
Status:		
	Downstream	Upstream
SNR Margin (dB):		
Attenuation (dB):		
Output Power (dBm):		

3.2 WAN

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

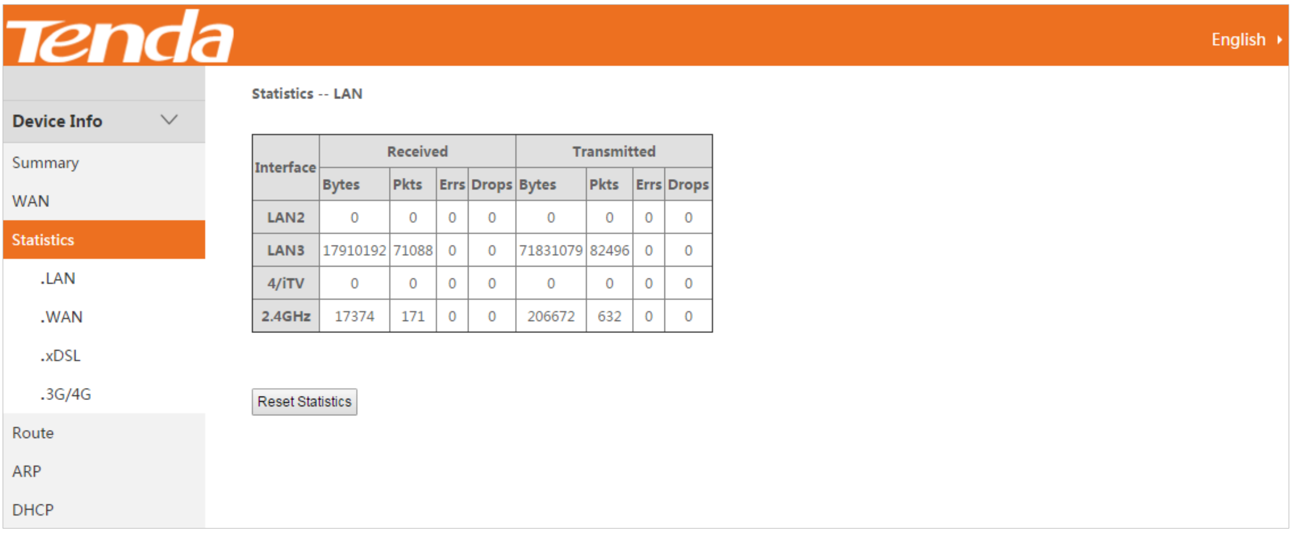


WAN Info

Interface	Description	Type	VlanMuxId	IPv6	Igmp	MLD	NAT	Firewall	Status	IPv4 Address	IPv6 Address
eth0.1	ipoe_LAN1	IPoE	Disabled	Disabled	Disabled	Disabled	Enabled	Enabled	Connected	192.168.1.104	

3.3 Statistics

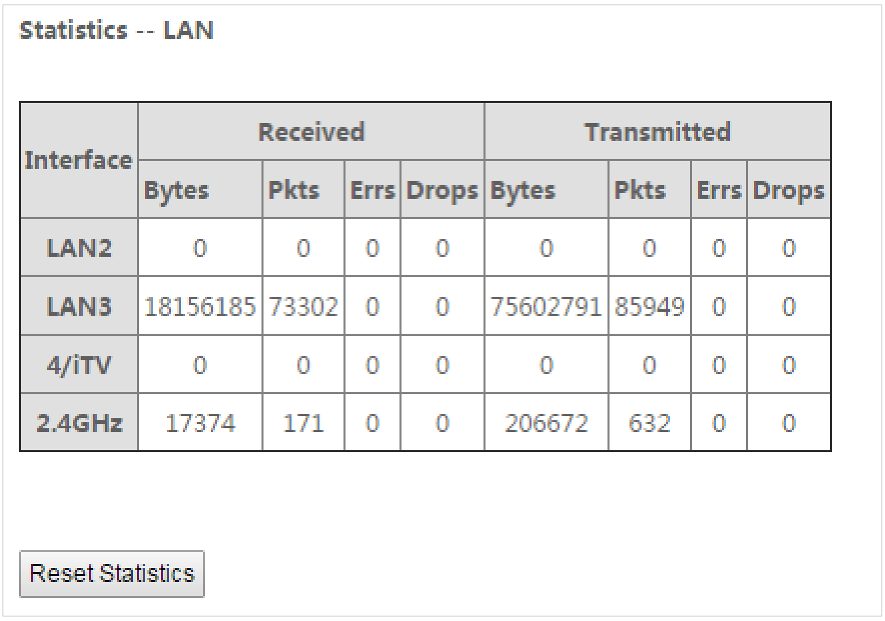
Here you can view the packets received and transmitted on LAN port, WAN port, DSL port, and USB port.



Statistics -- LAN

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
LAN2	0	0	0	0	0	0	0	0
LAN3	17910192	71088	0	0	71831079	82496	0	0
4/iTV	0	0	0	0	0	0	0	0
2.4GHz	17374	171	0	0	206672	632	0	0

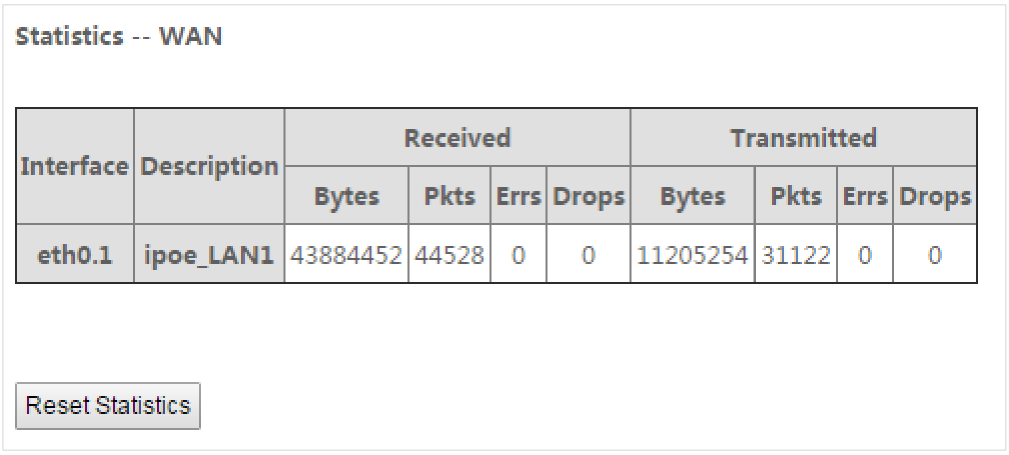
Statistics--LAN: Displays the packets received and transmitted on the LAN ports. Click **Reset Statistics** to clear the current statistics.



Statistics -- LAN

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
LAN2	0	0	0	0	0	0	0	0
LAN3	18156185	73302	0	0	75602791	85949	0	0
4/iTV	0	0	0	0	0	0	0	0
2.4GHz	17374	171	0	0	206672	632	0	0

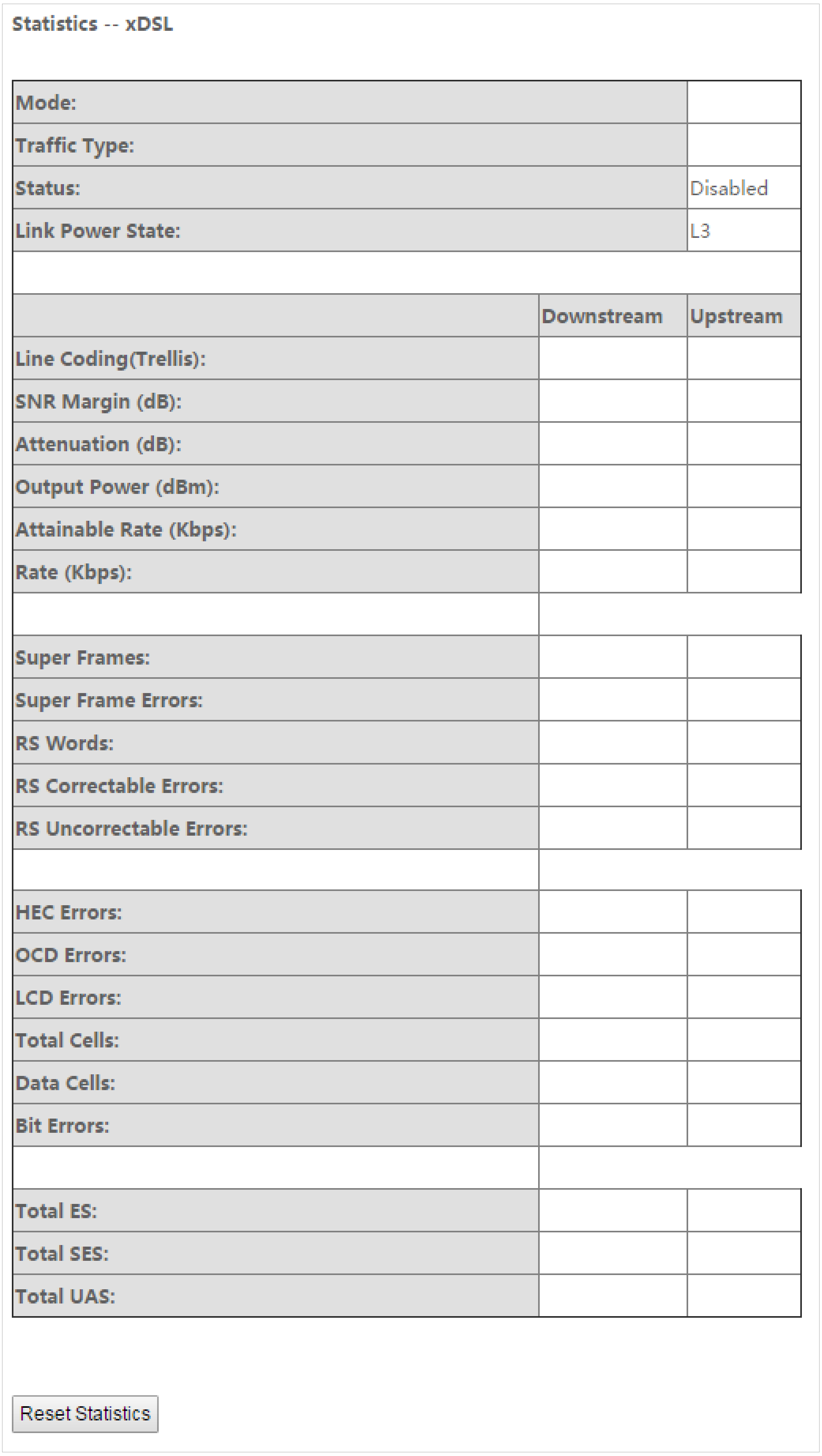
Statistics--WAN: Displays the packets received and transmitted on the WAN port. Click **Reset Statistics** to clear the current statistics.



Statistics -- WAN

Interface	Description	Received				Transmitted			
		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
eth0.1	ipoe_LAN1	43884452	44528	0	0	11205254	31122	0	0

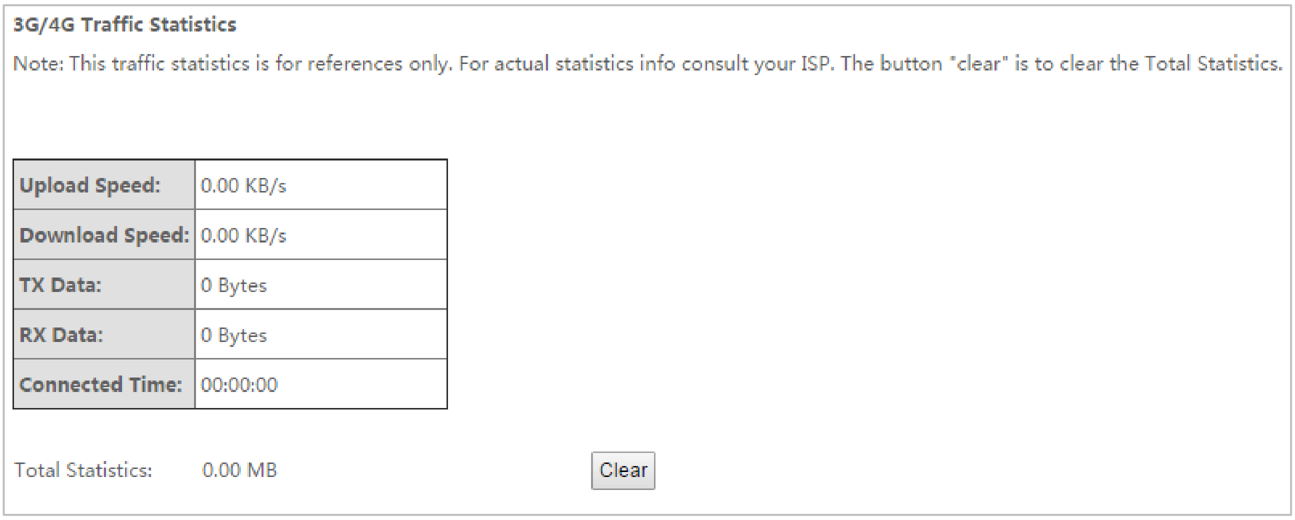
Statistics--xDSL: Displays the packets received and transmitted on the DSL port. Click **Reset Statistics** to clear the current statistics.



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:		

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



3G/4G Traffic Statistics

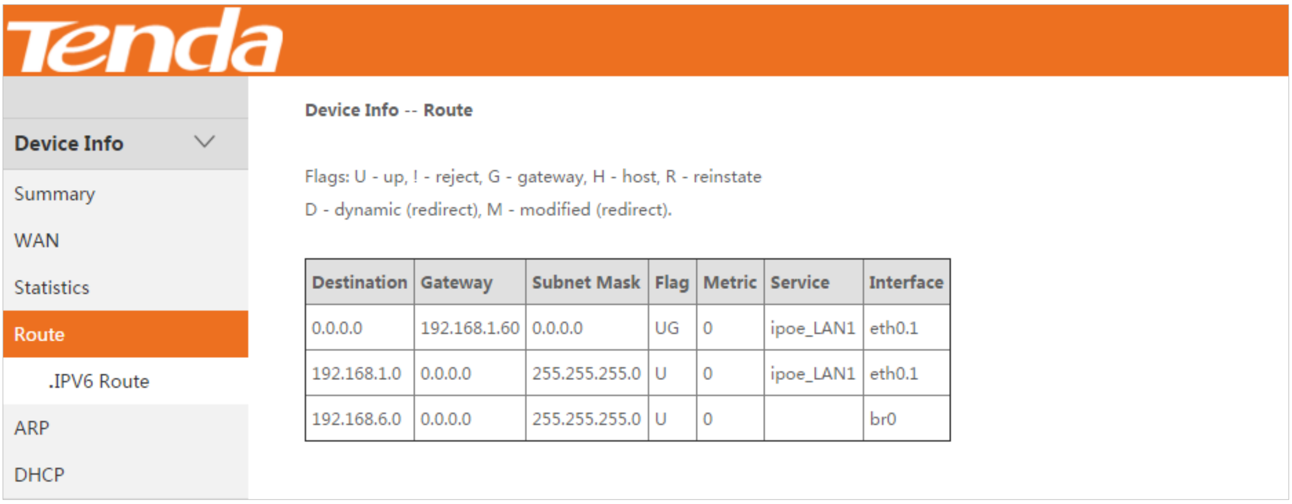
Note: This traffic statistics is for references only. For actual statistics info consult your ISP. The button "clear" is to clear the Total Statistics.

Upload Speed:	0.00 KB/s
Download Speed:	0.00 KB/s
TX Data:	0 Bytes
RX Data:	0 Bytes
Connected Time:	00:00:00

Total Statistics: 0.00 MB

3.4 Route

Here you can view the route table。



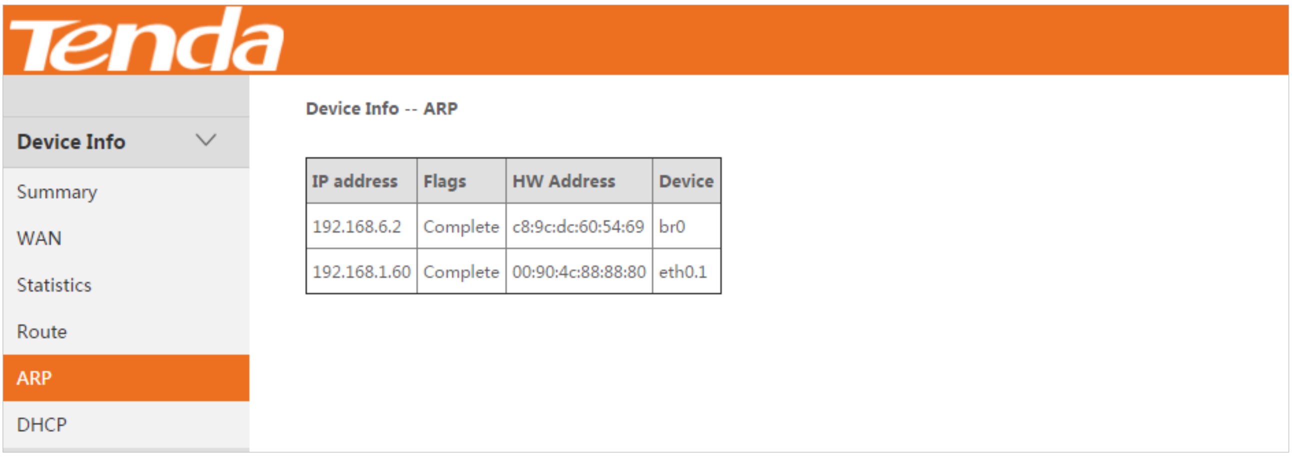
Device Info -- Route

Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate
D - dynamic (redirect), M - modified (redirect).

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
0.0.0.0	192.168.1.60	0.0.0.0	UG	0	ipoe_LAN1	eth0.1
192.168.1.0	0.0.0.0	255.255.255.0	U	0	ipoe_LAN1	eth0.1
192.168.6.0	0.0.0.0	255.255.255.0	U	0		br0

3.5 ARP

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

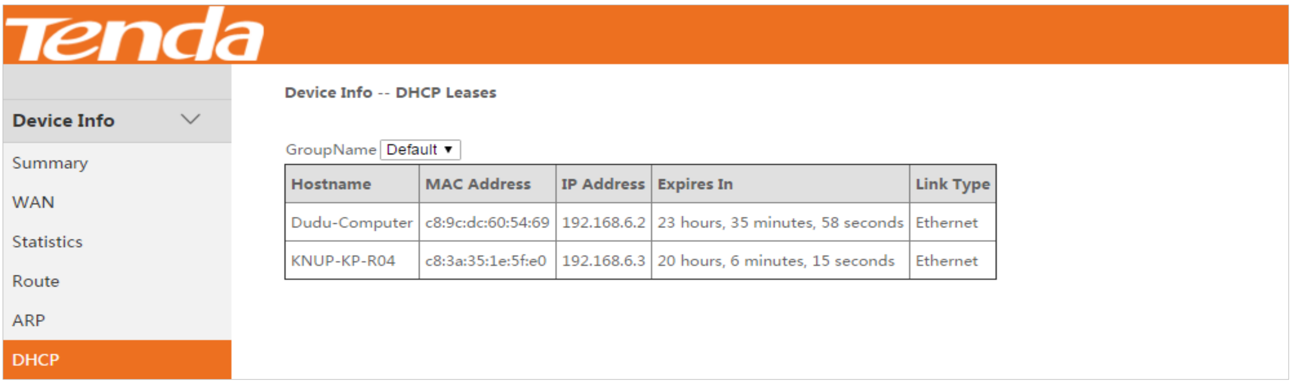


Device Info -- ARP

IP address	Flags	HW Address	Device
192.168.6.2	Complete	c8:9c:dc:60:54:69	br0
192.168.1.60	Complete	00:90:4c:88:88:80	eth0.1

3.6 DHCP

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



Device Info -- DHCP Leases

GroupName Default ▾

Hostname	MAC Address	IP Address	Expires In	Link Type
Dudu-Computer	c8:9c:dc:60:54:69	192.168.6.2	23 hours, 35 minutes, 58 seconds	Ethernet
KNUP-KP-R04	c8:3a:35:1e:5f:e0	192.168.6.3	20 hours, 6 minutes, 15 seconds	Ethernet

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:

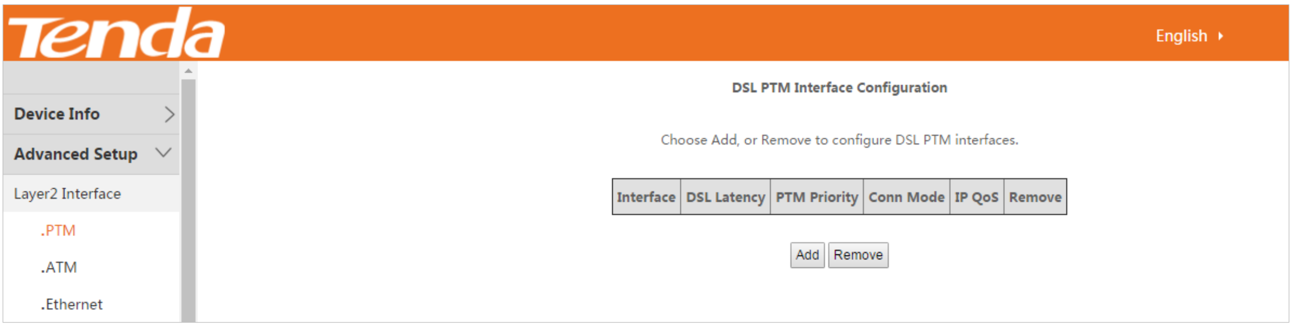
- PTM interface for VDSL broadband internet service

- ATM interface for ADSL broadband internet service

- ETH interface for connecting to the Internet via an Ethernet cable

4.1.1 To Set up the PTM Interface

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



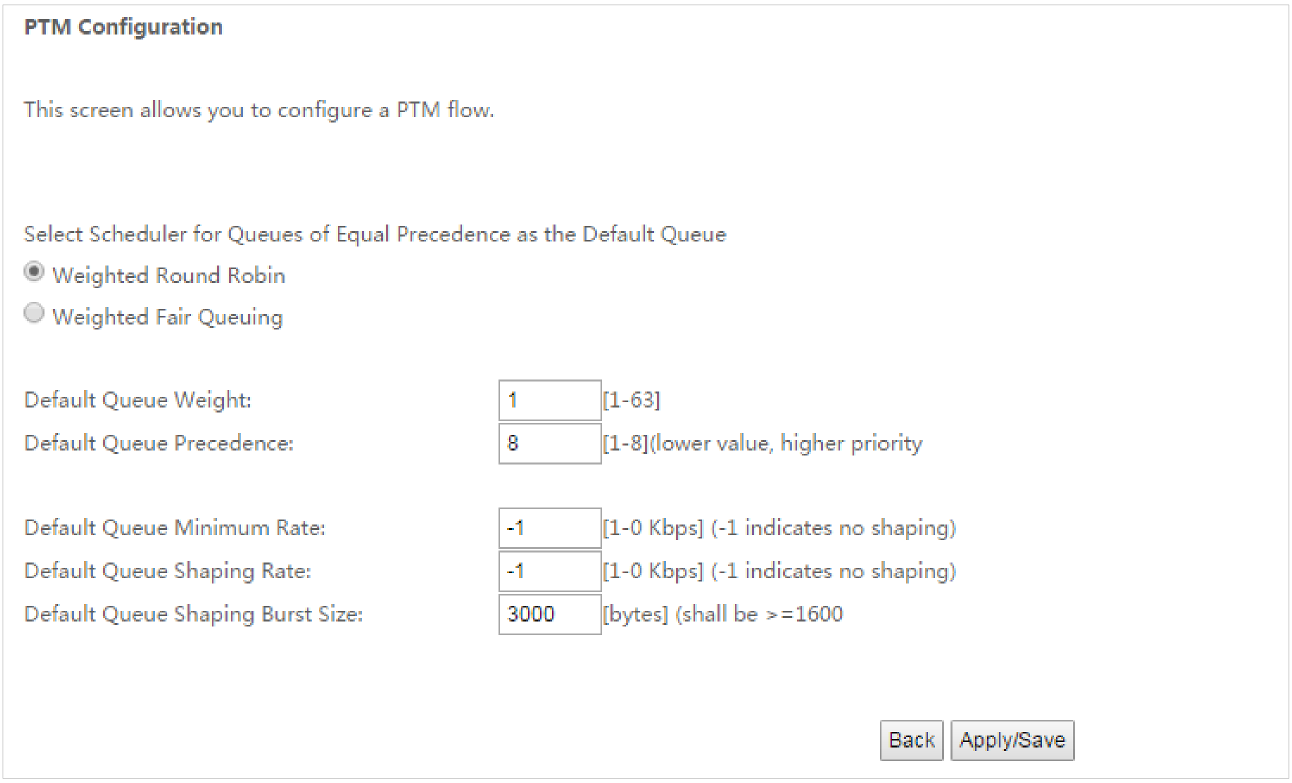
DSL PTM Interface Configuration

Choose Add, or Remove to configure DSL PTM interfaces.

Interface	DSL Latency	PTM Priority	Conn Mode	IP QoS	Remove

Step 1 Click **Add**.

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



PTM Configuration

This screen allows you to configure a PTM flow.

Select Scheduler for Queues of Equal Precedence as the Default Queue

● Weighted Round Robin

○ Weighted Fair Queuing

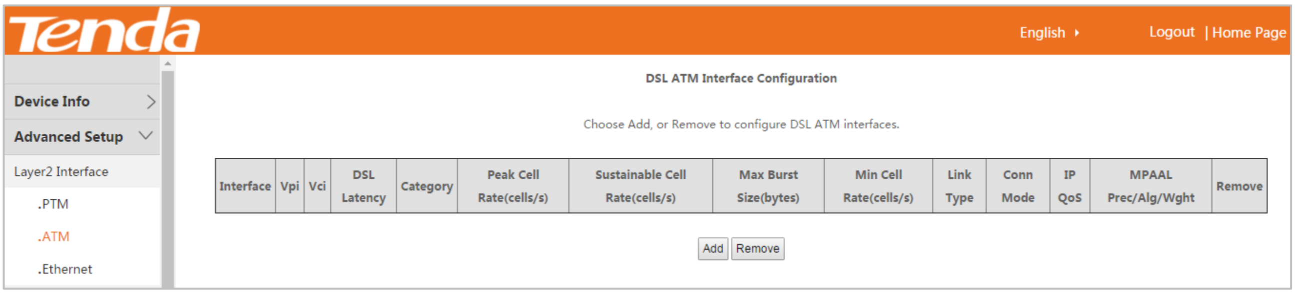
Default Queue Weight:	1	[1-63]
Default Queue Precedence:	8	[1-8](lower value, higher priority
Default Queue Minimum Rate:	-1	[1-0 Kbps] (-1 indicates no shaping)
Default Queue Shaping Rate:	-1	[1-0 Kbps] (-1 indicates no shaping)
Default Queue Shaping Burst Size:	3000	[bytes] (shall be >=1600

And then refer to To Set up WAN Service for PTM Interface to configure the WAN service for internet access.

--End

4.1.2 To Set up the ATM Interface

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



DSL ATM Interface Configuration

Choose Add, or Remove to configure DSL ATM interfaces.

Interface	Vpi	Vci	DSL Latency	Category	Peak Cell Rate(cells/s)	Sustainable Cell Rate(cells/s)	Max Burst Size(bytes)	Min Cell Rate(cells/s)	Link Type	Conn Mode	IP QoS	MPAAL Prec/Alg/Wght	Remove

Step 1 Click **Add**.

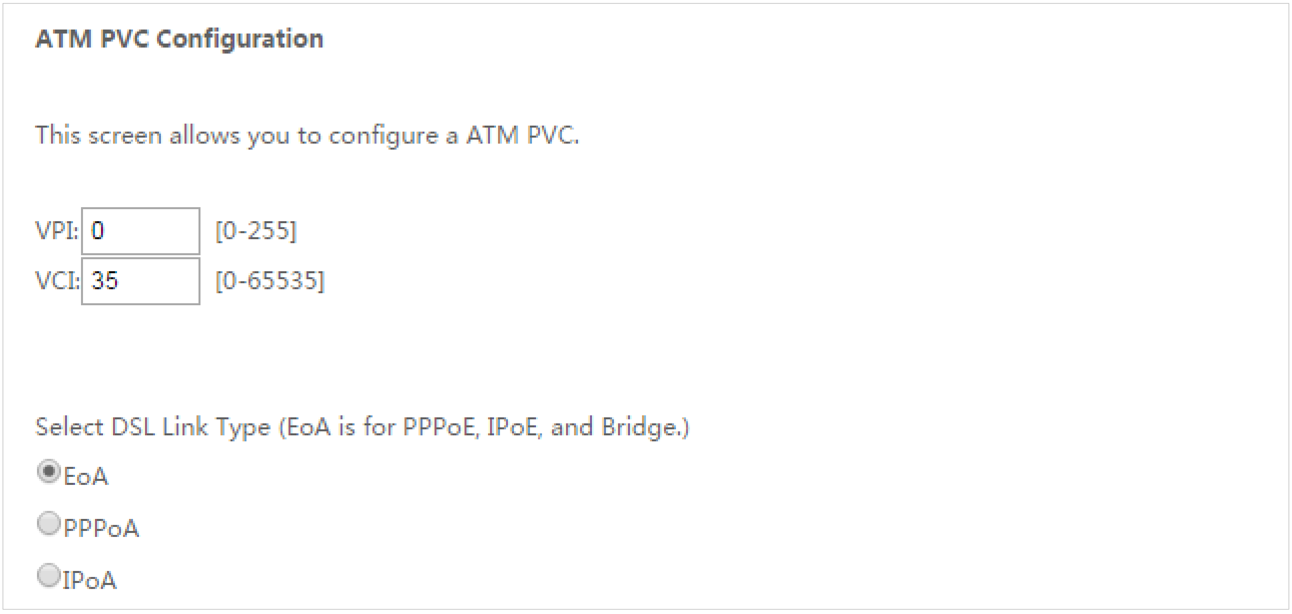
Step 2 Enter the **VPI** and **VCI** values.

Step 3 Select a DSL Link Type according to the instructions in the table below, and leave other options unchanged. EoA (EoA is for PPPoE, IPoE, and Bridge.), PPPoA or IPoA.

Step 4 Click **Apply/Save** on the bottom of the page.

Connection Type		**Description**
PPPoE (PPP over Ethernet)		If your internet service provider (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 thus type if your ISP does not provide any parameters to you for internet access.

	Static IP	If your internet service provider 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 thus 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.



ATM PVC Configuration

This screen allows you to configure a ATM PVC.

VPI: 0 [0-255]

VCI: 35 [0-65535]

Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)

● EoA

○ PPPoA

○ IPoA

And then refer to To Set up WAN Service for ATM Interface to configure the WAN service for internet access.

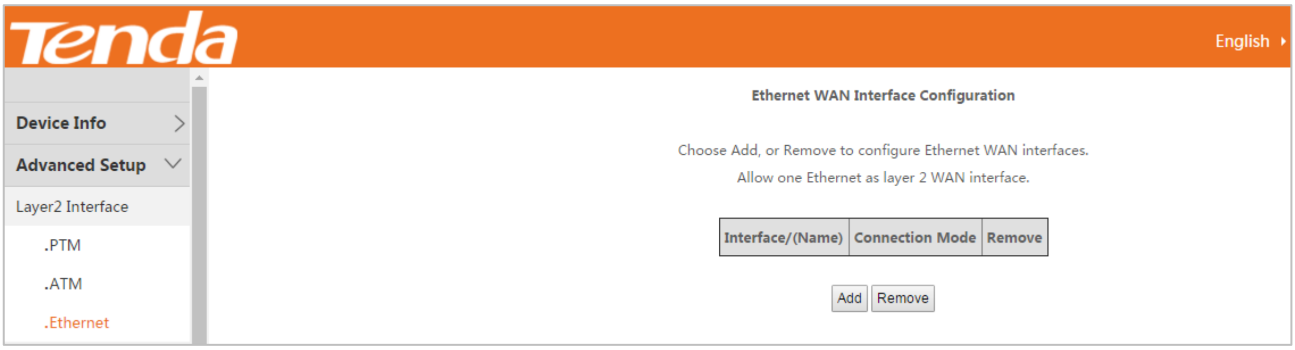
--End

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 is not covered there, ask your ISP to provide it.

4.1.3 To Set up the Ethernet Interface

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



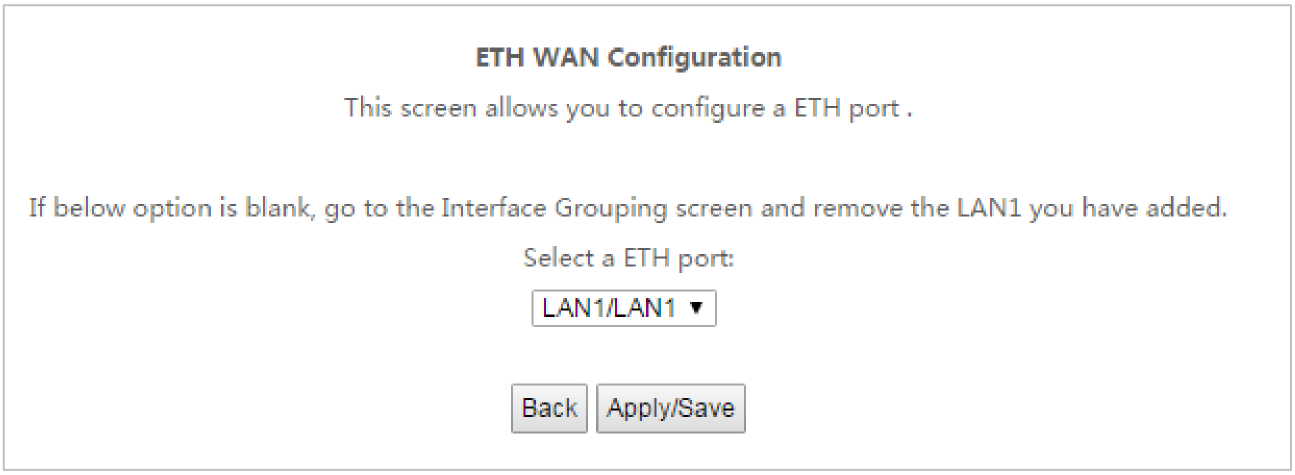
Ethernet WAN Interface Configuration

Choose Add, or Remove to configure Ethernet WAN interfaces.
Allow one Ethernet as layer 2 WAN interface.

Interface/(Name)	Connection Mode	Remove

Step 1 Click **Add**.

Step 2 Click **Apply/Save**.



ETH WAN Configuration

This screen allows you to configure a ETH port .

If below option is blank, go to the Interface Grouping screen and remove the LAN1 you have added.

Select a ETH port:

LAN1/LAN1 ▼

Back | Apply/Save

And then refer to To Set up WAN Service for Ethernet Interface to configure the WAN service for internet access.

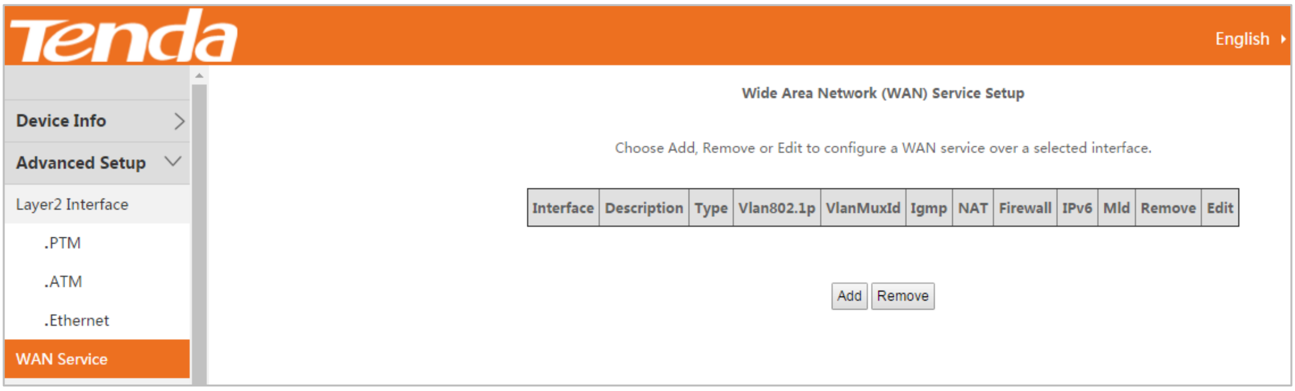
--End

4.2 WAN Service

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

4.2.1 To Set up WAN Service for PTM Interface

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



Wide Area Network (WAN) Service Setup

Choose Add, Remove or Edit to configure a WAN service over a selected interface.

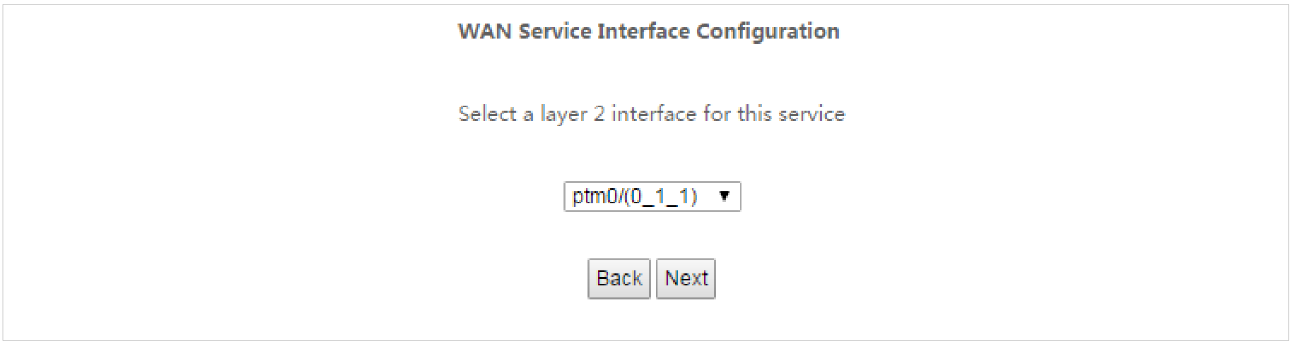
Interface	Description	Type	Vlan802.1p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	Remove	Edit

Add | Remove

Step 1 Click **Add**.

Step 2 Select the interface you create in Layer2 Interface, interface **ptm0/(0_1_1)** here.

Step 3 Click **Next**.



WAN Service Interface Configuration

Select a layer 2 interface for this service

ptm0/(0_1_1) ▼

Back | Next

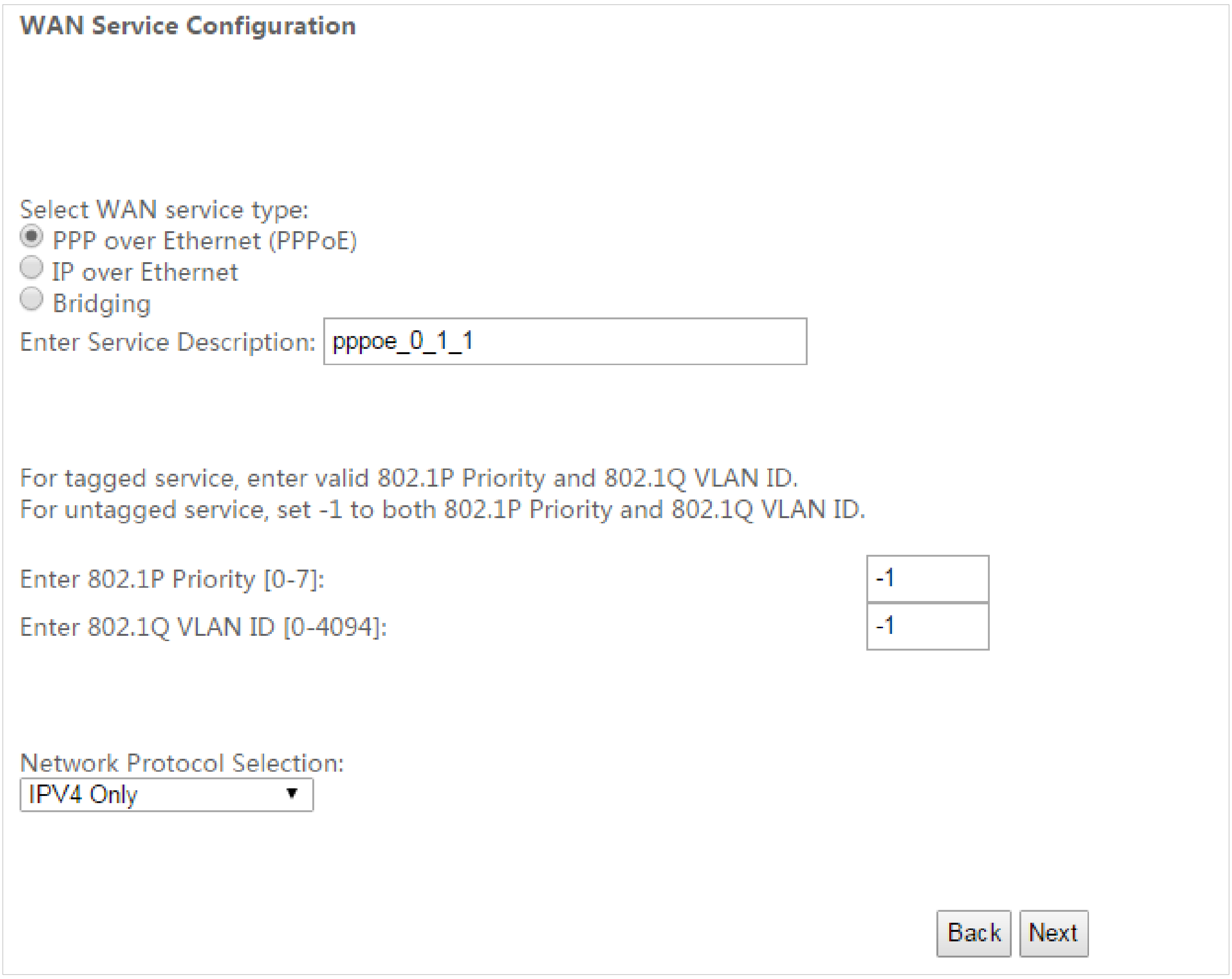
Step 4 Select a WAN service type according to the instructions in the table below. Here take **PPPoE** as an example.

Connection Type		Description
PPP over Ethernet (PPPoE)		Select thus type if your internet service provider (ISP) provides a user name and password to you for internet access.
IP over Ethernet	Dynamic IP	Select thus type if your ISP does not provide any parameters to you for internet access.
	Static IP	Select thus type if your ISP provides a static IP address and other related information to you for internet access.
Bridging		Select thus 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**.



WAN Service Configuration

Select WAN service type:
● PPP over Ethernet (PPPoE)
○ IP over Ethernet
○ Bridging

Enter Service Description: pppoe_0_1_1

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

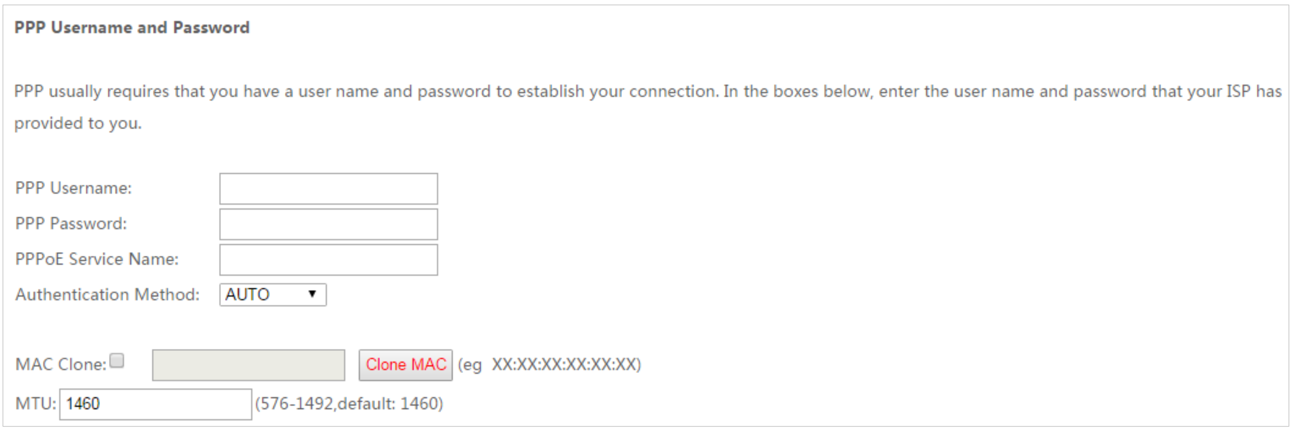
Enter 802.1P Priority [0-7]: -1

Enter 802.1Q VLAN ID [0-4094]: -1

Network Protocol Selection:
IPV4 Only

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.



PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:	
PPP Password:	
PPPoE Service Name:	
Authentication Method:	AUTO

MAC Clone: □ Clone MAC (eg XX:XX:XX:XX:XX:XX)

MTU: 1460 (576-1492,default: 1460)

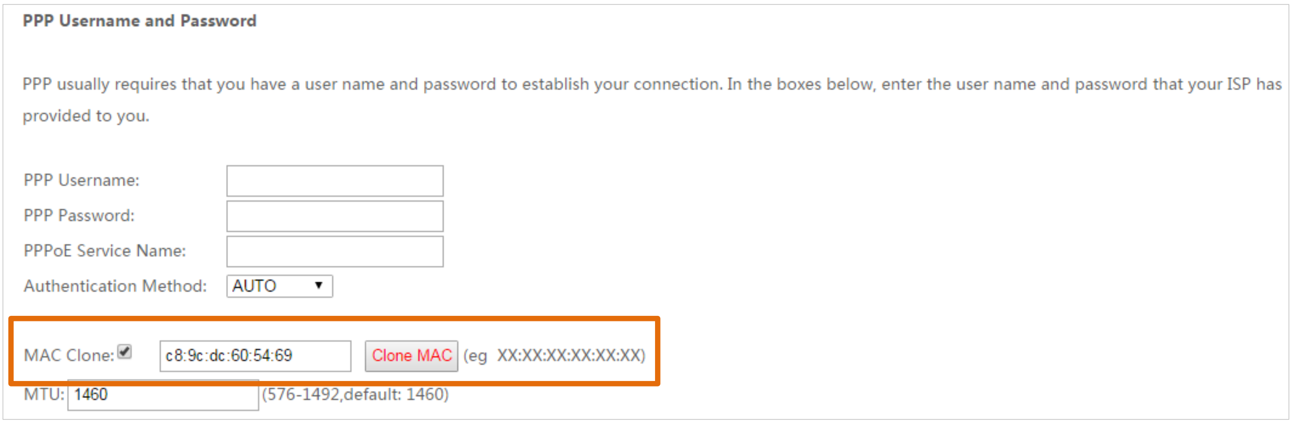
Optional Step: MAC Clone

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

Select the MAC address box.

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.



PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

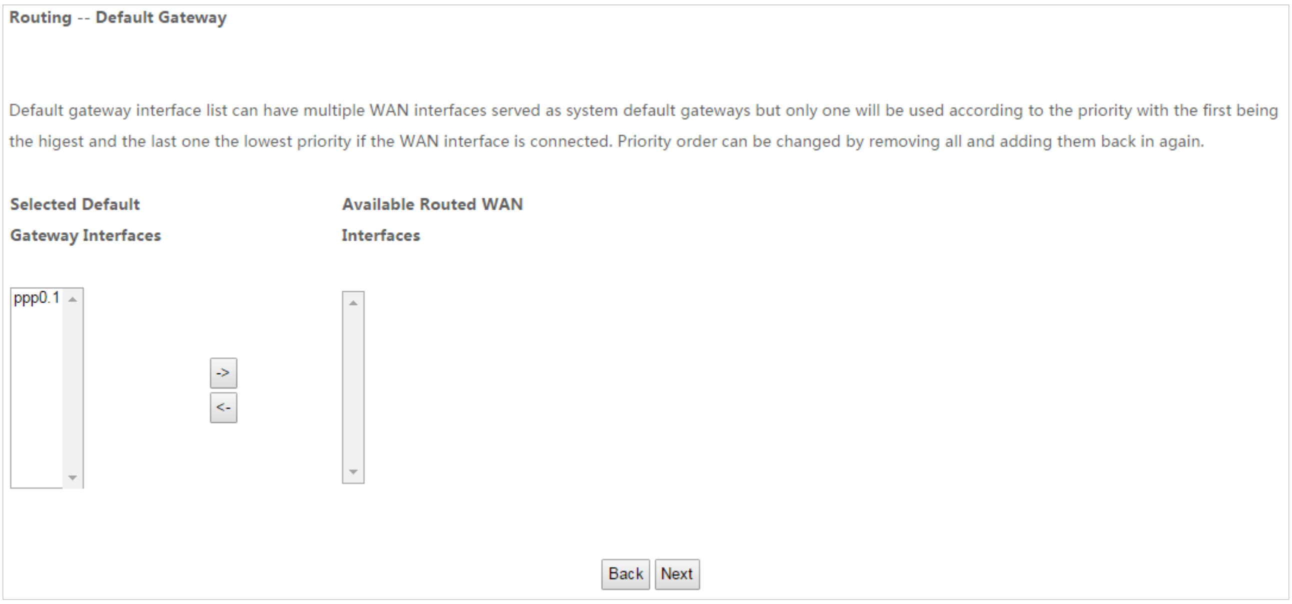
PPP Username:	
PPP Password:	
PPPoE Service Name:	
Authentication Method:	AUTO

MAC Clone: ☑ c8:9c:dc:60:54:69 Clone MAC (eg XX:XX:XX:XX:XX:XX)

MTU: 1460 (576-1492,default: 1460)

Step 10 Click **Next**.

Step 11 Leave the configuration unchanged, and click **Next**.



Routing -- Default Gateway

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

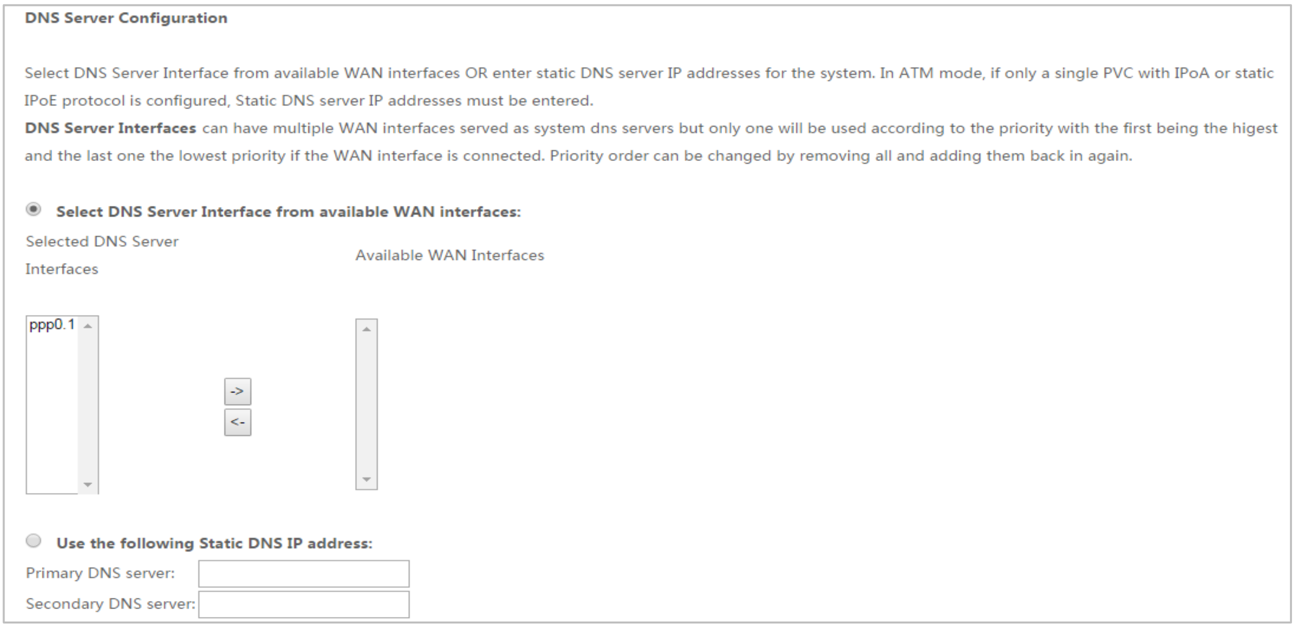
Selected Default Gateway Interfaces

ppp0.1

Available Routed WAN Interfaces

Step 12 Enter the DNS IP addresses information if they are provided by your ISP. If not, leave then blank.

Step 13 Click **Next**.



DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.
DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

● **Select DNS Server Interface from available WAN interfaces:**

Selected DNS Server Interfaces

ppp0.1

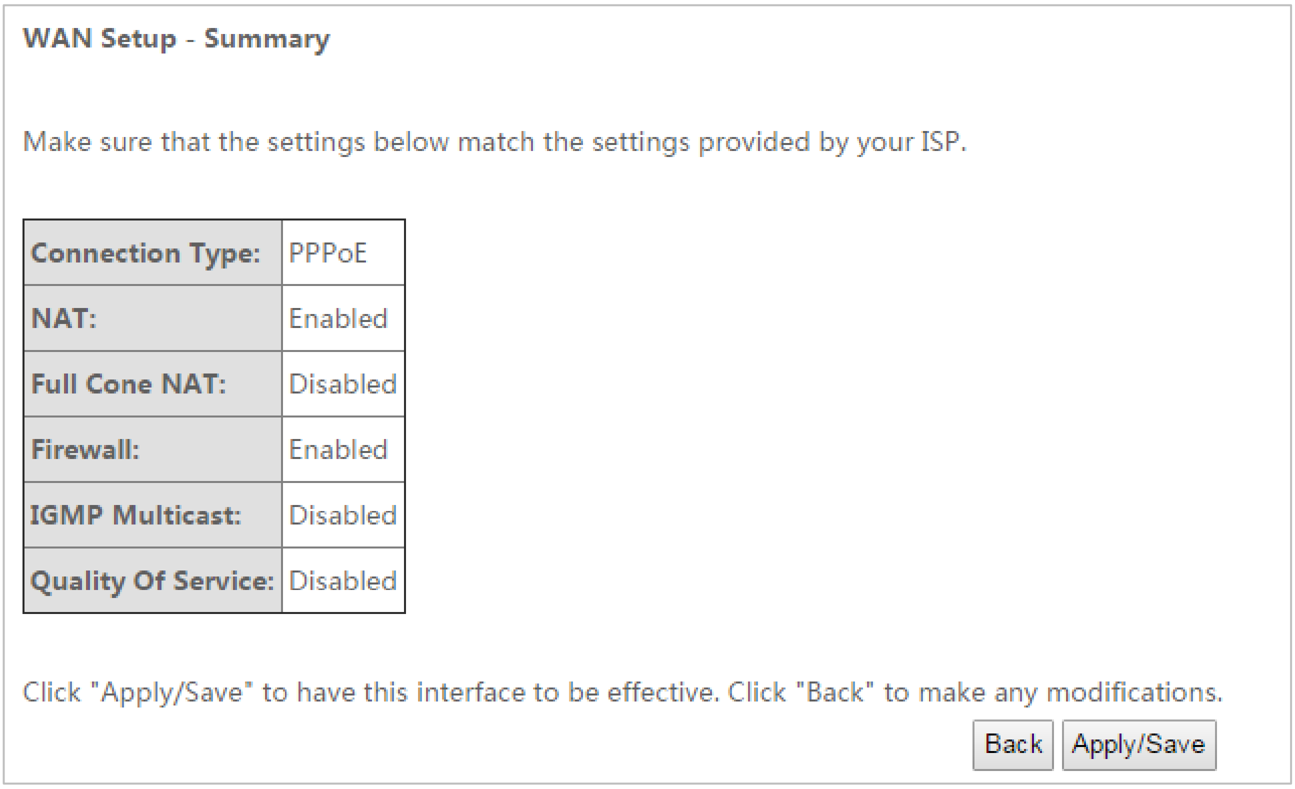
Available WAN Interfaces

○ **Use the following Static DNS IP address:**

Primary DNS server:

Secondary DNS server:

Step 14 Check the parameters you select or set, and click **Apply/Save**.



WAN Setup - Summary

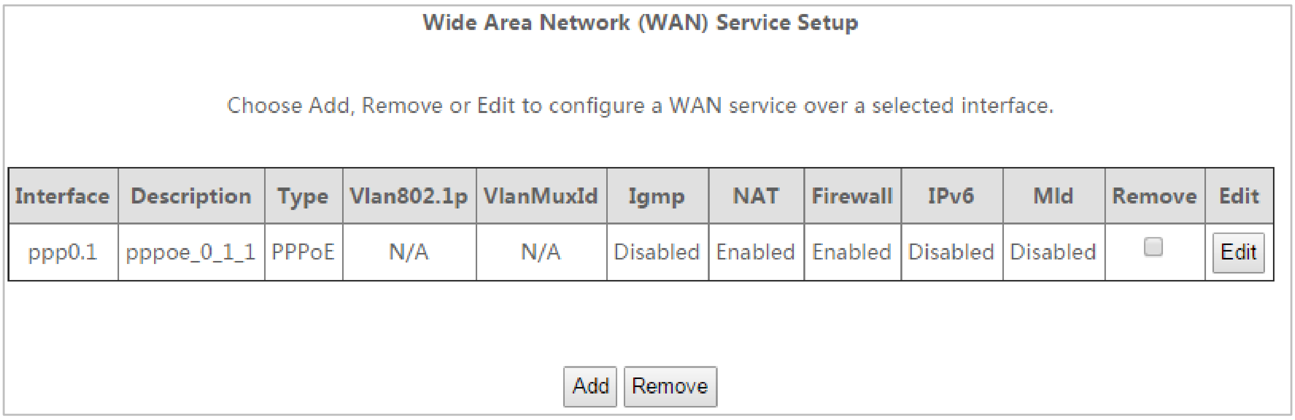
Make sure that the settings below match the settings provided by your ISP.

Connection Type:	PPPoE
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

--End

The WAN service you set is shown in **WAN Service** page.



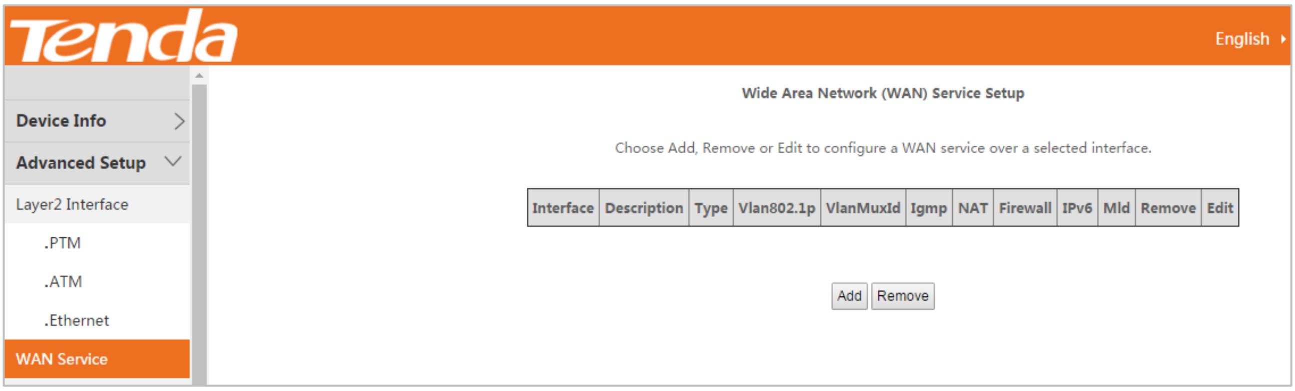
Wide Area Network (WAN) Service Setup

Choose Add, Remove or Edit to configure a WAN service over a selected interface.

Interface	Description	Type	Vlan802.1p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	Remove	Edit
ppp0.1	pppoe_0_1_1	PPPoE	N/A	N/A	Disabled	Enabled	Enabled	Disabled	Disabled	☐	Edit

4.2.2 To Set up WAN Service for ATM Interface

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



Wide Area Network (WAN) Service Setup

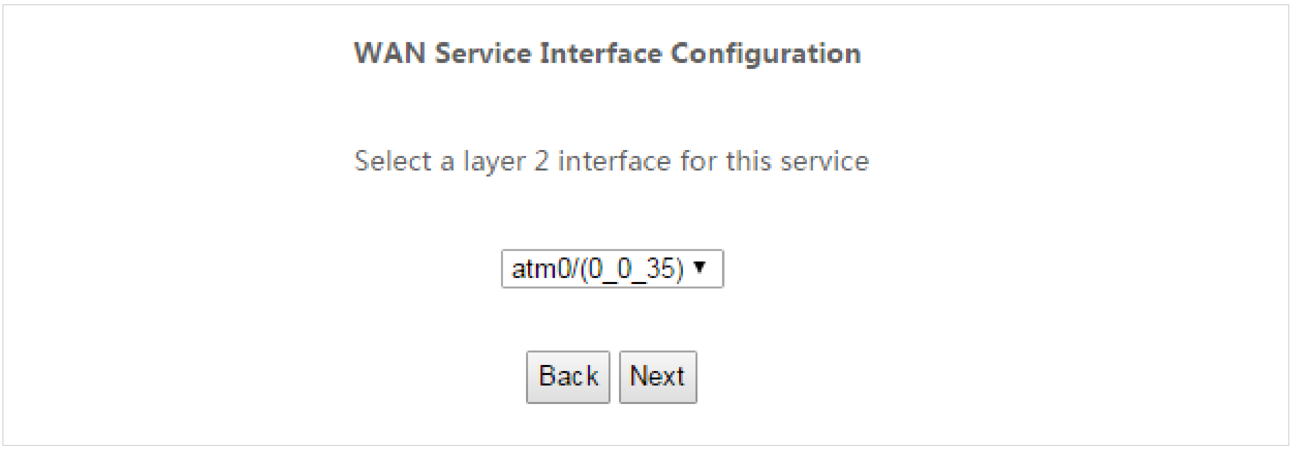
Choose Add, Remove or Edit to configure a WAN service over a selected interface.

Interface	Description	Type	Vlan802.1p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	Remove	Edit

Step 1 Click **Add**.

Step 2 Select the interface you create in Layer2 Interface, interface **atm0/(0_1_35)** here.

Step 3 Click **Next**.



WAN Service Interface Configuration

Select a layer 2 interface for this service

atm0/(0_0_35) ▾

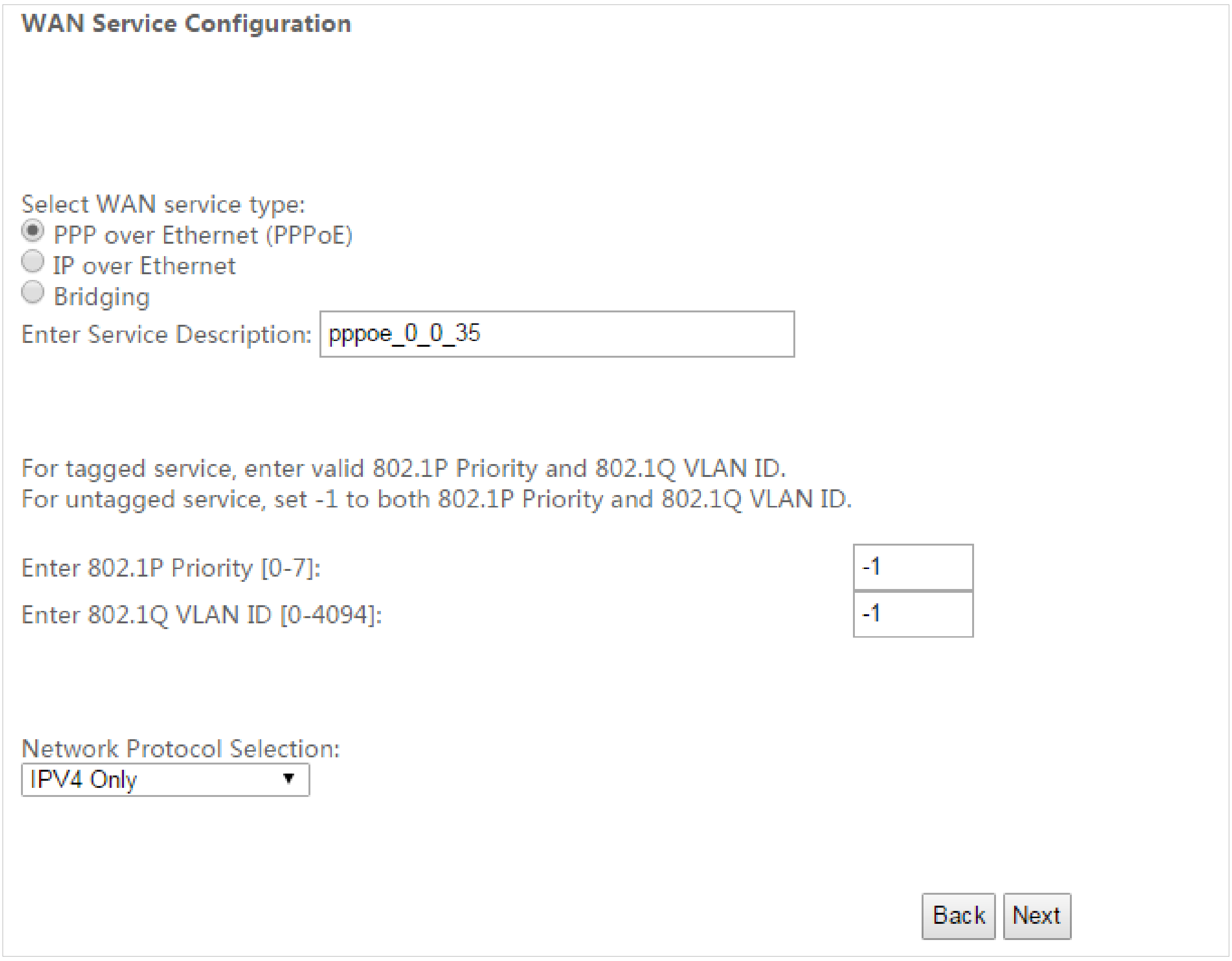
Step 4 Select a WAN service type according to the instructions in the table below. Here take **PPPoE** as an example.

Connection Type		**Description**
PPP over Ethernet (PPPoE)		Select thus type if your internet service provider (ISP) provides a user name and password to you for internet access.
IP over Ethernet	Dynamic IP	Select thus type if your ISP does not provide any parameters to you for internet access.
	Static IP	Select thus type if your ISP provides a static IP address and other related information to you for internet access.
Bridging		Select thus 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**.



WAN Service Configuration

Select WAN service type:

● PPP over Ethernet (PPPoE)
○ IP over Ethernet
○ Bridging

Enter Service Description: pppoe_0_0_35

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

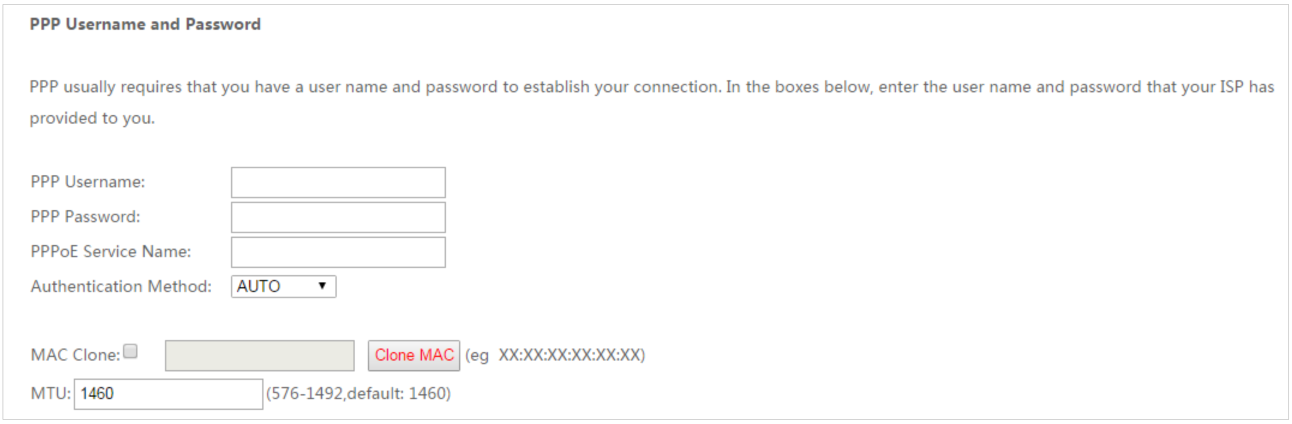
Enter 802.1P Priority [0-7]: -1

Enter 802.1Q VLAN ID [0-4094]: -1

Network Protocol Selection:
IPV4 Only

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.



PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:
PPP Password:
PPPoE Service Name:
Authentication Method: AUTO

MAC Clone: □ Clone MAC (eg XX:XX:XX:XX:XX:XX)

MTU: 1460 (576-1492,default: 1460)

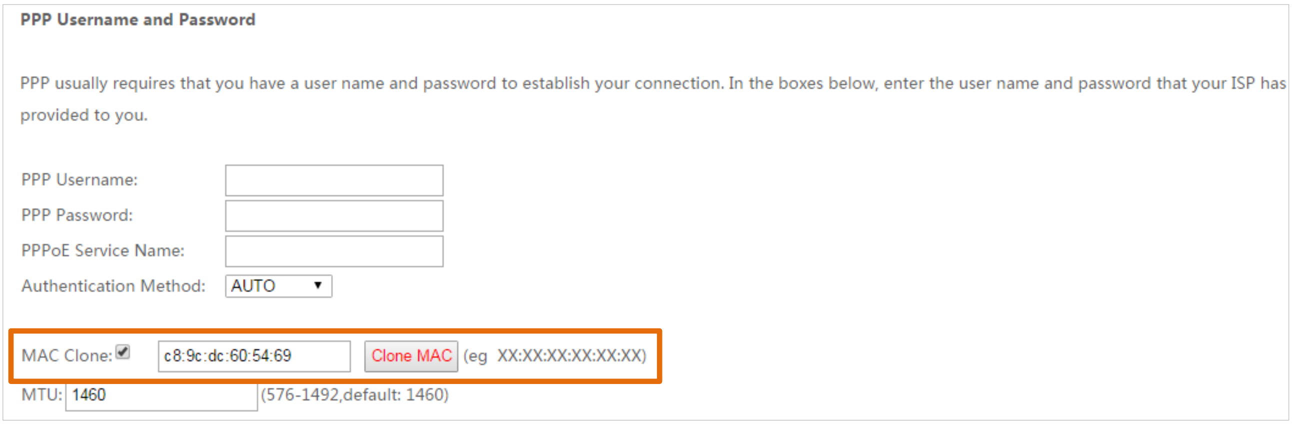
Optional Step: MAC Clone

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

Select the MAC address box.

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.



PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:

PPP Password:

PPPoE Service Name:

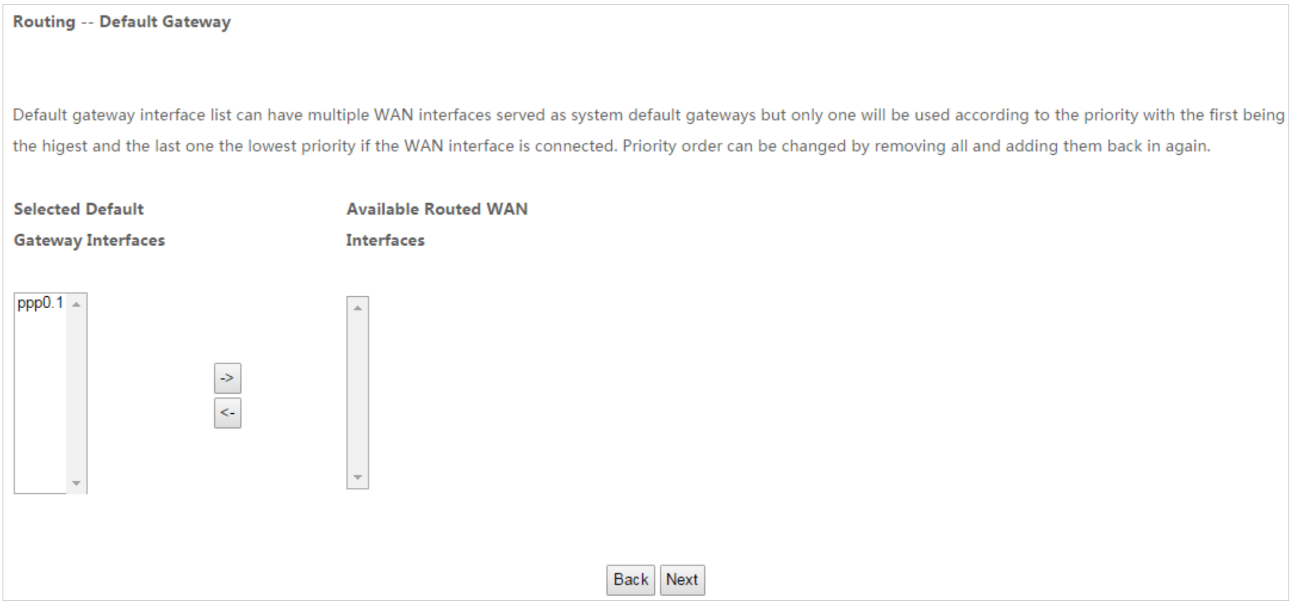
Authentication Method: AUTO

MAC Clone: ☑ c8:9c:dc:60:54:69 Clone MAC (eg XX:XX:XX:XX:XX:XX)

MTU: 1460 (576-1492,default: 1460)

Step 10 Click **Next**.

Step 11 Leave the configuration unchanged, and click **Next**.



Routing -- Default Gateway

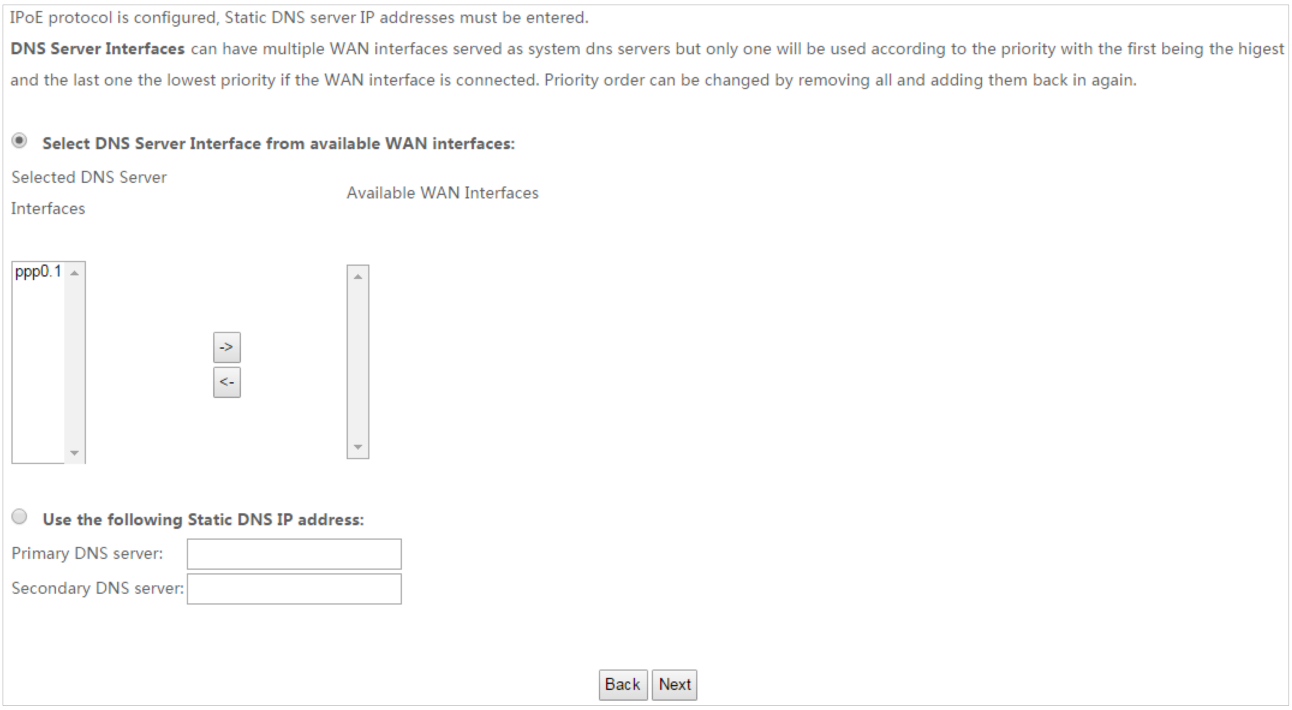
Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and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

Selected Default Gateway Interfaces: ppp0.1

Available Routed WAN Interfaces:

Step 12 Enter the DNS IP addresses information if they are provided by your ISP. If not, leave then blank.

Step 13 Click **Next**.



IPoE protocol is configured, Static DNS server IP addresses must be entered.

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

● **Select DNS Server Interface from available WAN interfaces:**

Selected DNS Server Interfaces: ppp0.1

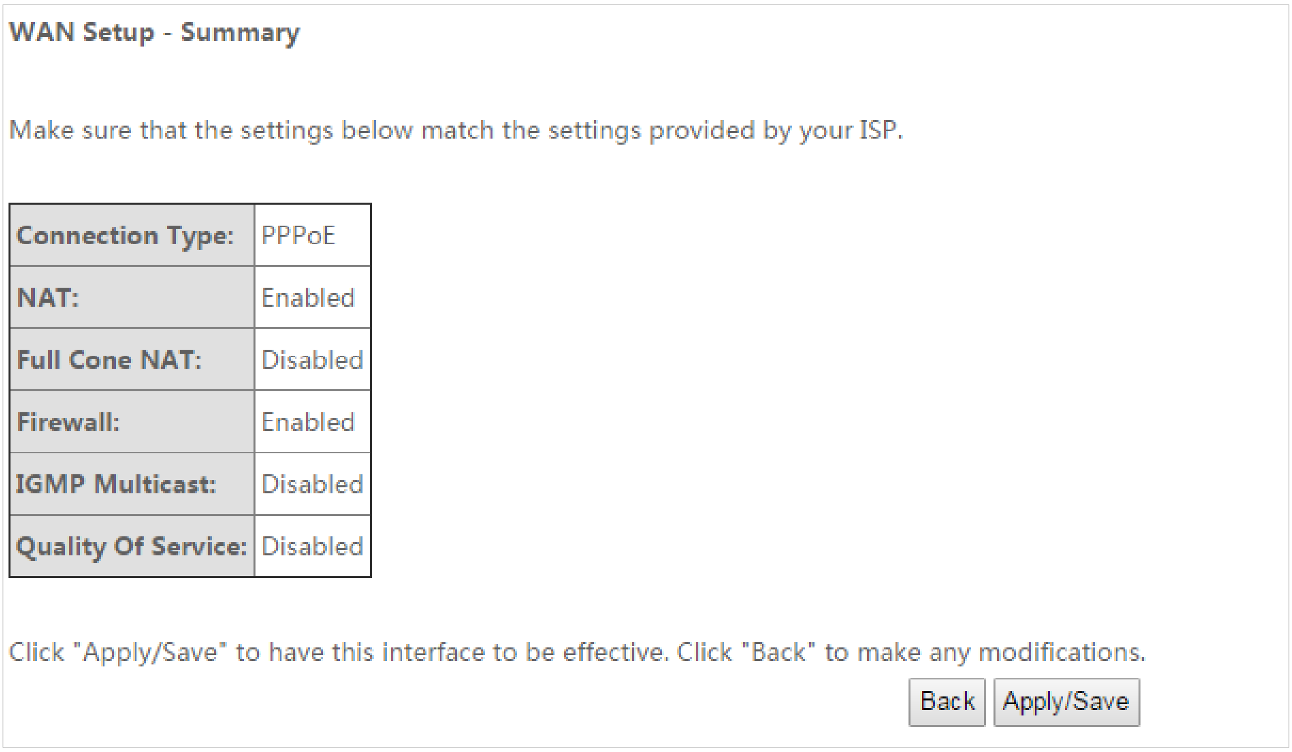
Available WAN Interfaces:

○ **Use the following Static DNS IP address:**

Primary DNS server:

Secondary DNS server:

Step 14 Check the parameters you select or set, and click **Apply/Save**.



WAN Setup - Summary

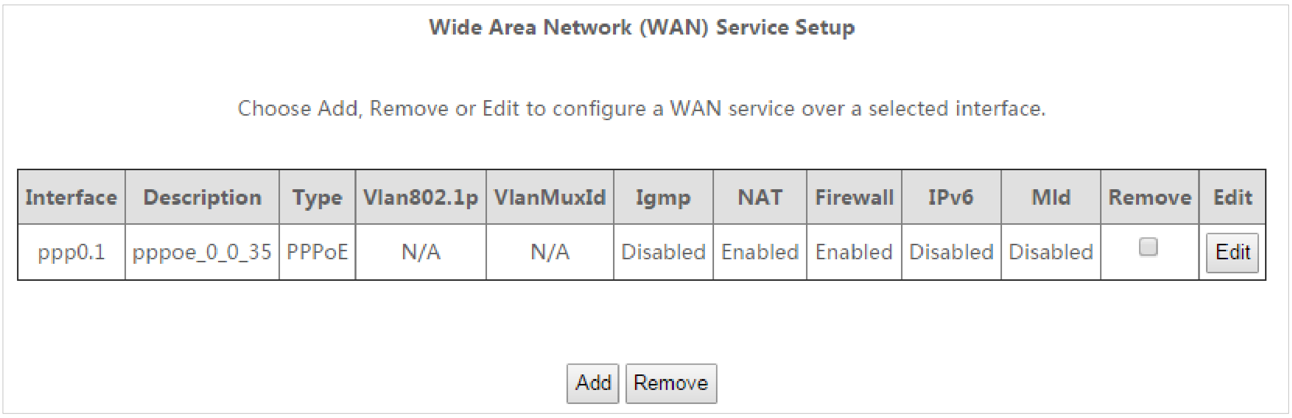
Make sure that the settings below match the settings provided by your ISP.

Connection Type:	PPPoE
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

--End

The WAN service you set is shown in **WAN Service** page.



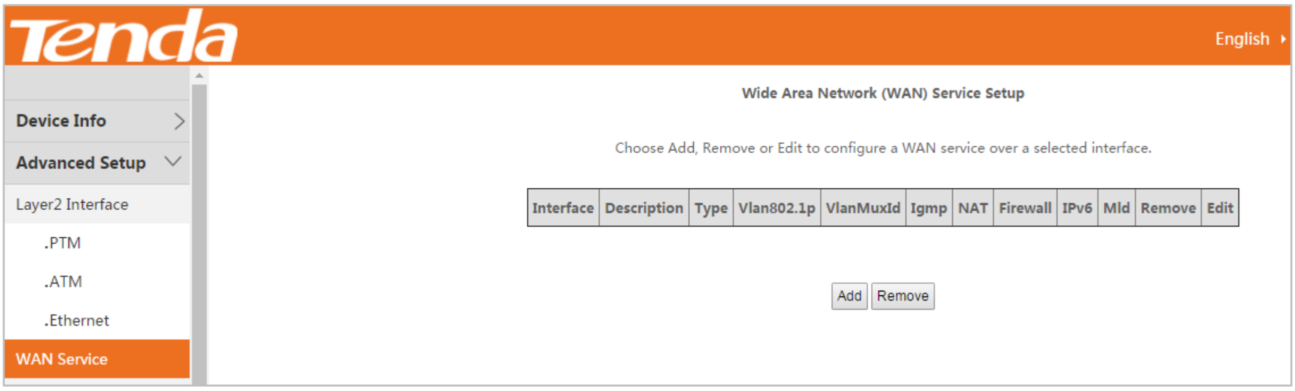
Wide Area Network (WAN) Service Setup

Choose Add, Remove or Edit to configure a WAN service over a selected interface.

Interface	Description	Type	Vlan802.1p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	Remove	Edit
ppp0.1	pppoe_0_0_35	PPPoE	N/A	N/A	Disabled	Enabled	Enabled	Disabled	Disabled	□	Edit

4.2.3 To Set up WAN Service for Ethernet Interface

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



Wide Area Network (WAN) Service Setup

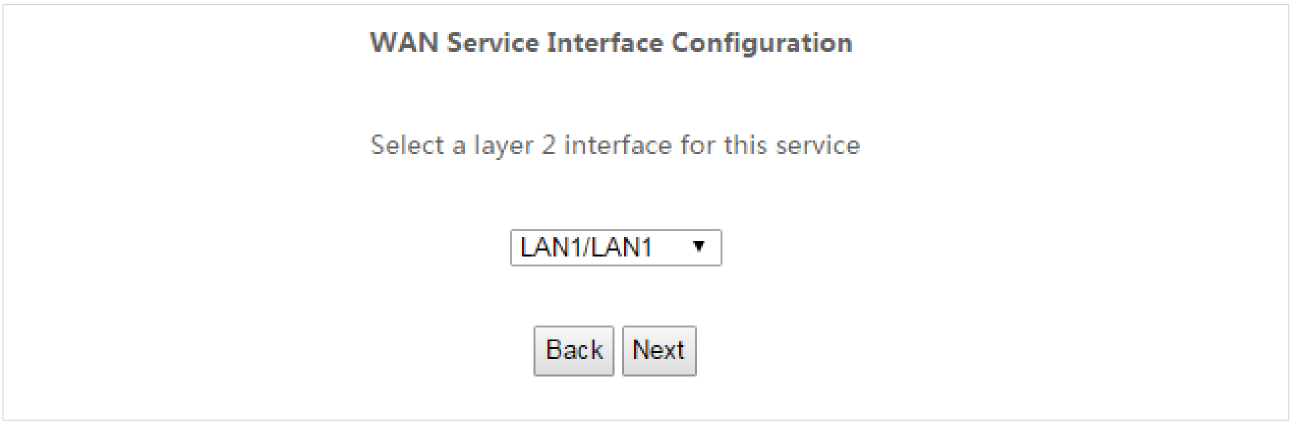
Choose Add, Remove or Edit to configure a WAN service over a selected interface.

Interface	Description	Type	Vlan802.1p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	Remove	Edit

Step 1 Click **Add**.

Step 2 Select the interface you create in Layer2 Interface, interface **atm0/(0_1_35)** here.

Step 3 Click **Next**.



WAN Service Interface Configuration

Select a layer 2 interface for this service

LAN1/LAN1 ▼

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

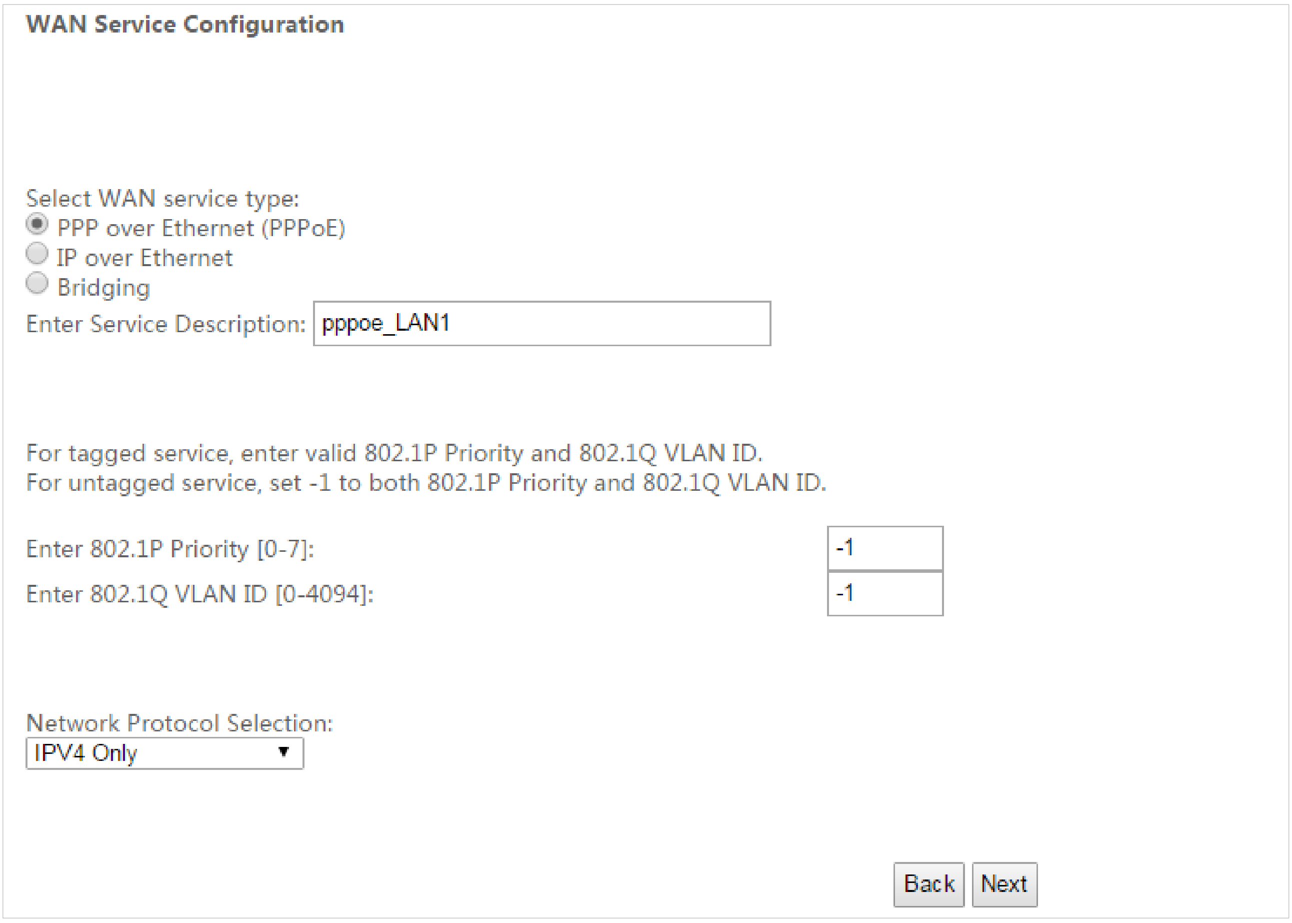
Connection Type		Description
PPP over Ethernet (PPPoE)		Select thus type if your internet service provider (ISP) provides a user name and password to you for internet access.
IP over Ethernet	Dynamic IP	Select thus type if your ISP does not provide any parameters to you for internet access.

	Static IP	Select thus type if your ISP provides a static IP address and other related information to you for internet access.
Bridging		Select thus 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**.



WAN Service Configuration

Select WAN service type:
● PPP over Ethernet (PPPoE)
○ IP over Ethernet
○ Bridging

Enter Service Description: pppoe_LAN1

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

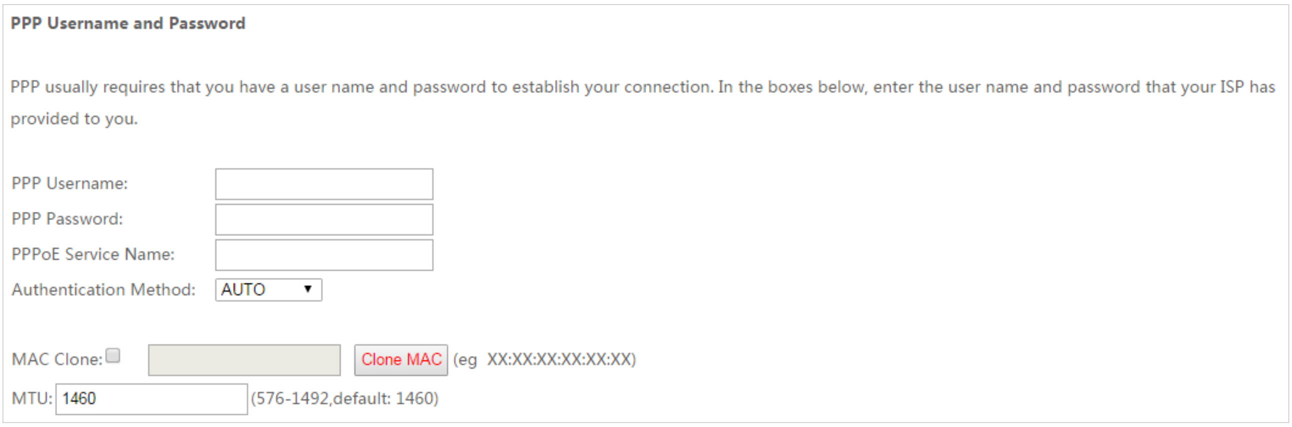
Enter 802.1P Priority [0-7]: -1

Enter 802.1Q VLAN ID [0-4094]: -1

Network Protocol Selection:
IPV4 Only ▼

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.



PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:

PPP Password:

PPPoE Service Name:

Authentication Method: AUTO ▼

MAC Clone: □ Clone MAC (eg XX:XX:XX:XX:XX:XX)

MTU: 1460 (576-1492,default: 1460)

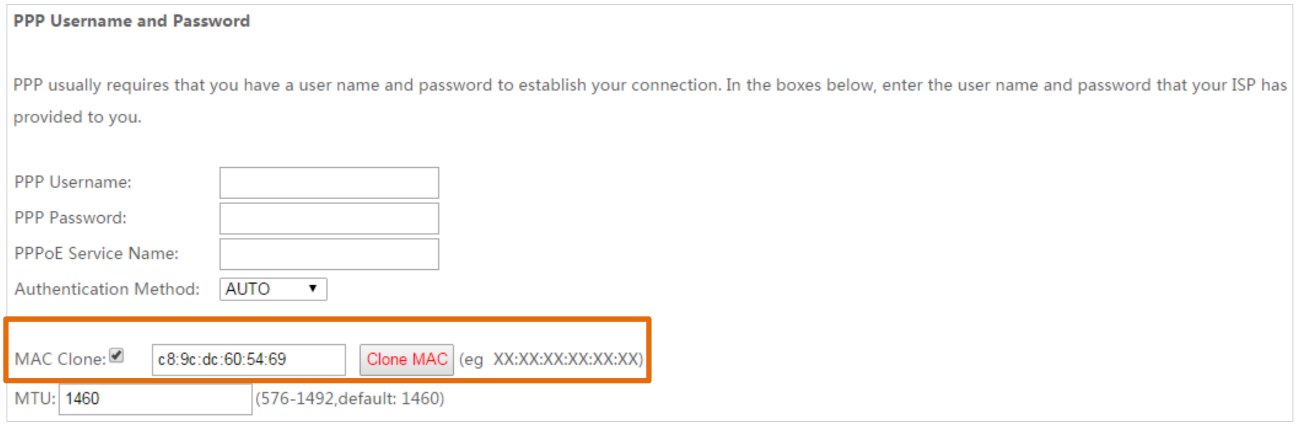
Optional Step: MAC Clone

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

Select the MAC address box.

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.



PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:

PPP Password:

PPPoE Service Name:

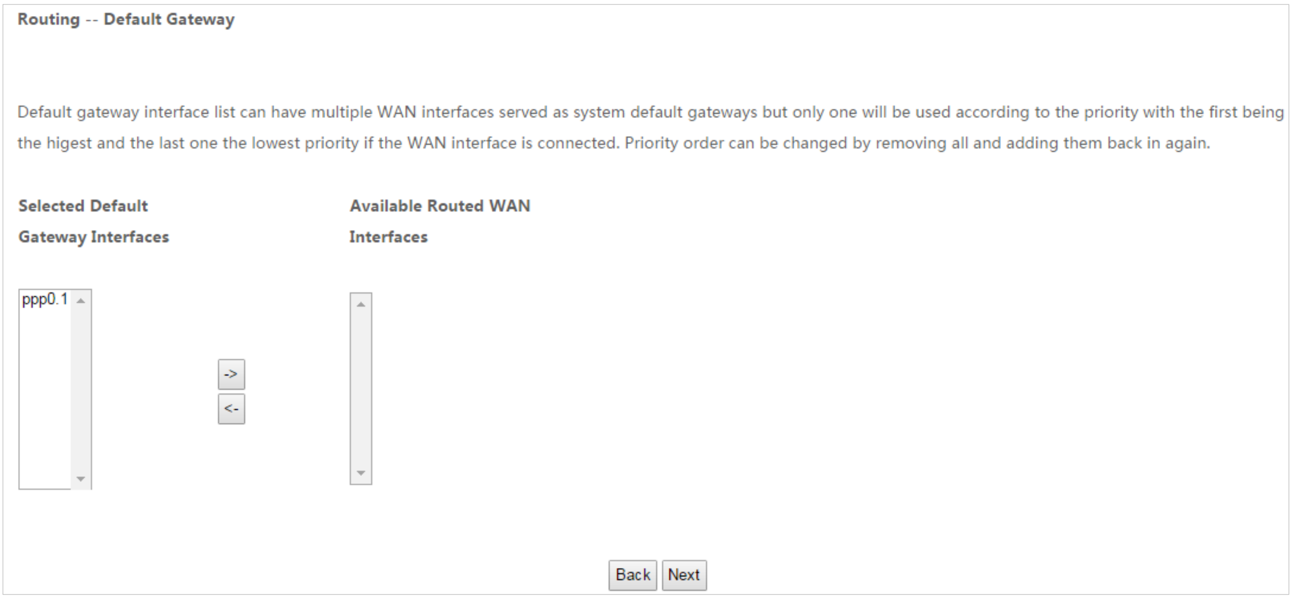
Authentication Method: AUTO ▾

MAC Clone: ☑ c8:9c:dc:60:54:69 Clone MAC (eg XX:XX:XX:XX:XX:XX)

MTU: 1460 (576-1492,default: 1460)

Step 10 Click **Next**.

Step 11 Leave the configuration unchanged, and click **Next**.



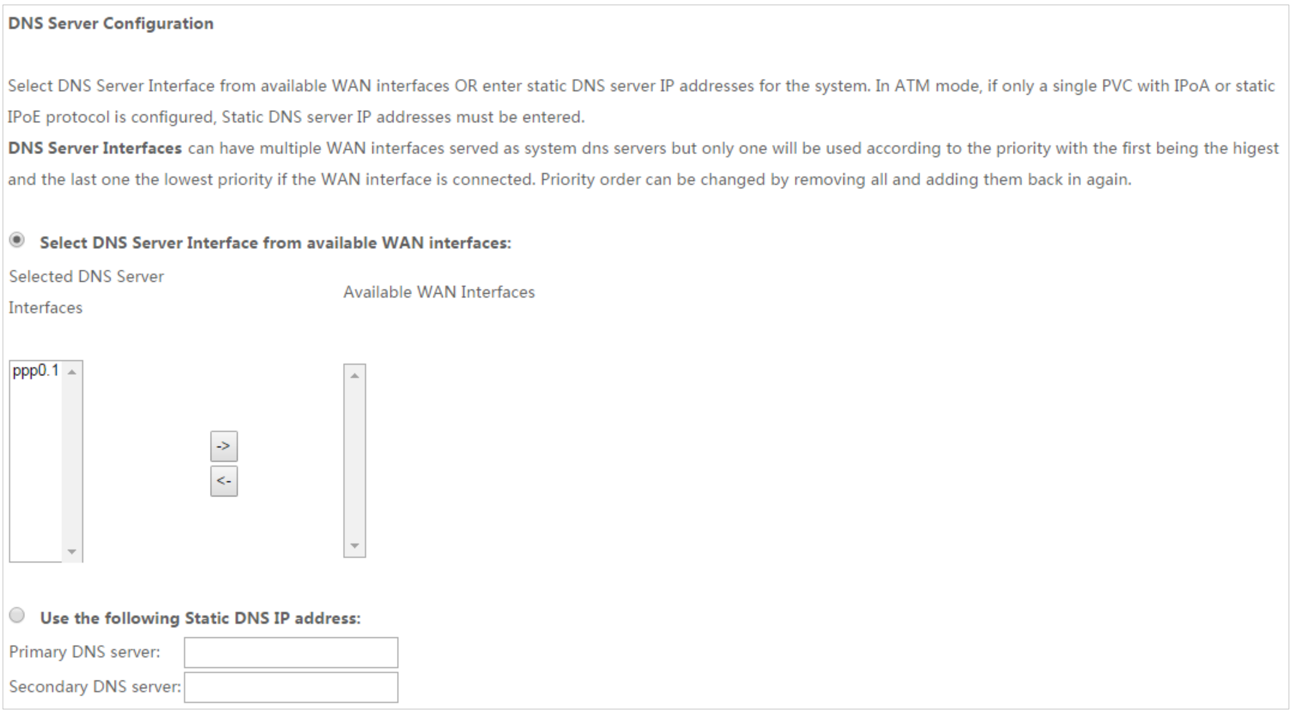
Routing -- Default Gateway

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

Selected Default Gateway Interfaces	Available Routed WAN Interfaces
ppp0.1	

Step 12 Enter the DNS IP addresses information if they are provided by your ISP. If not, leave then blank.

Step 13 Click **Next**.



DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.
DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

● **Select DNS Server Interface from available WAN interfaces:**

Selected DNS Server Interfaces: ppp0.1

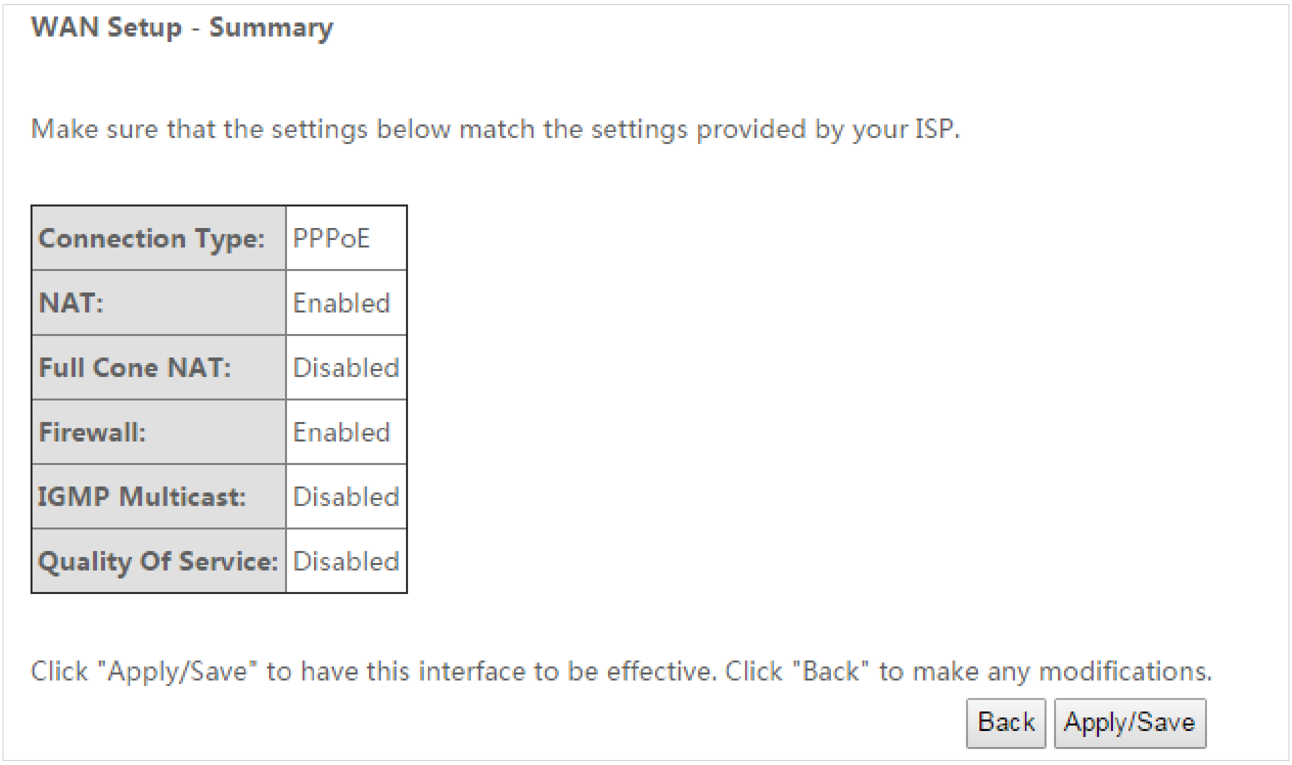
Available WAN Interfaces

○ **Use the following Static DNS IP address:**

Primary DNS server:

Secondary DNS server:

Step 14 Check the parameters you select or set, and click **Apply/Save**.



WAN Setup - Summary

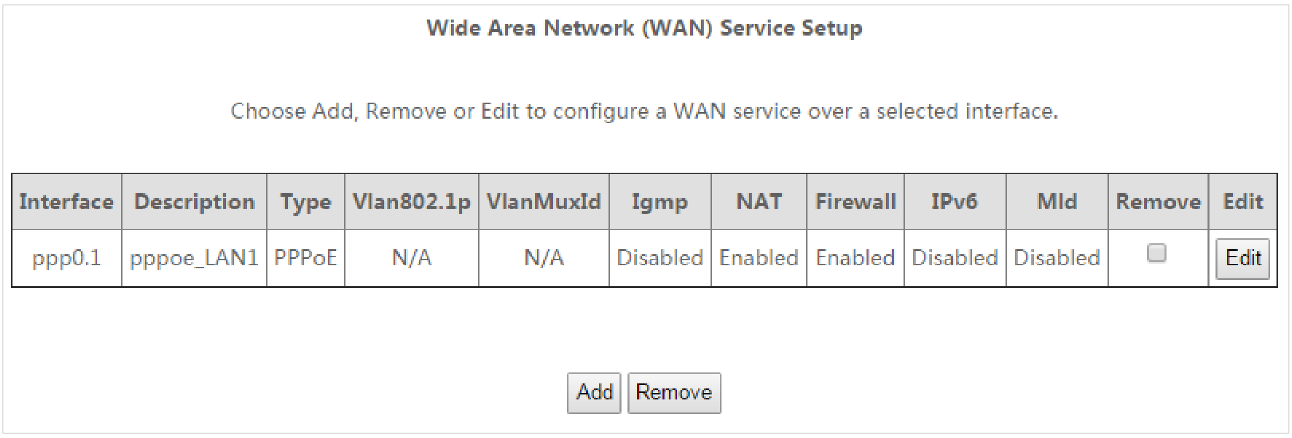
Make sure that the settings below match the settings provided by your ISP.

Connection Type:	PPPoE
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

--End

The WAN service you set is shown in **WAN Service** page.



Wide Area Network (WAN) Service Setup

Choose Add, Remove or Edit to configure a WAN service over a selected interface.

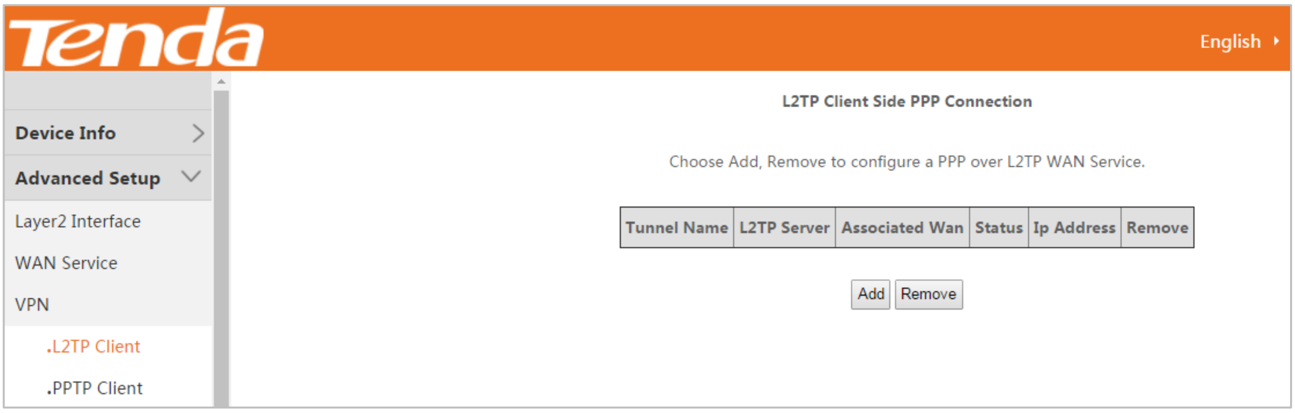
Interface	Description	Type	Vlan802.1p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	Remove	Edit
ppp0.1	pppoe_LAN1	PPPoE	N/A	N/A	Disabled	Enabled	Enabled	Disabled	Disabled	□	Edit

4.3 VPN

A VPN is a logical private network set up over a public network (usually the internet) without physical lines. This modem router can function as a PPTP/L2TP client. The following section describes how to configure the router as a PPTP/L2TP client.

4.3.1 L2TP Client

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

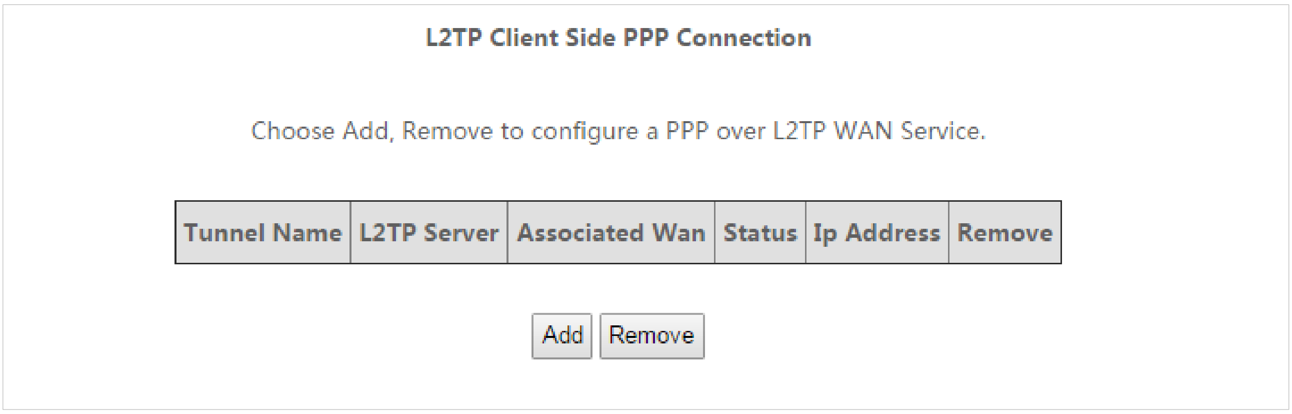


L2TP Client Side PPP Connection

Choose Add, Remove to configure a PPP over L2TP WAN Service.

Tunnel Name	L2TP Server	Associated Wan	Status	Ip Address	Remove

Step 1 Click **Add**.



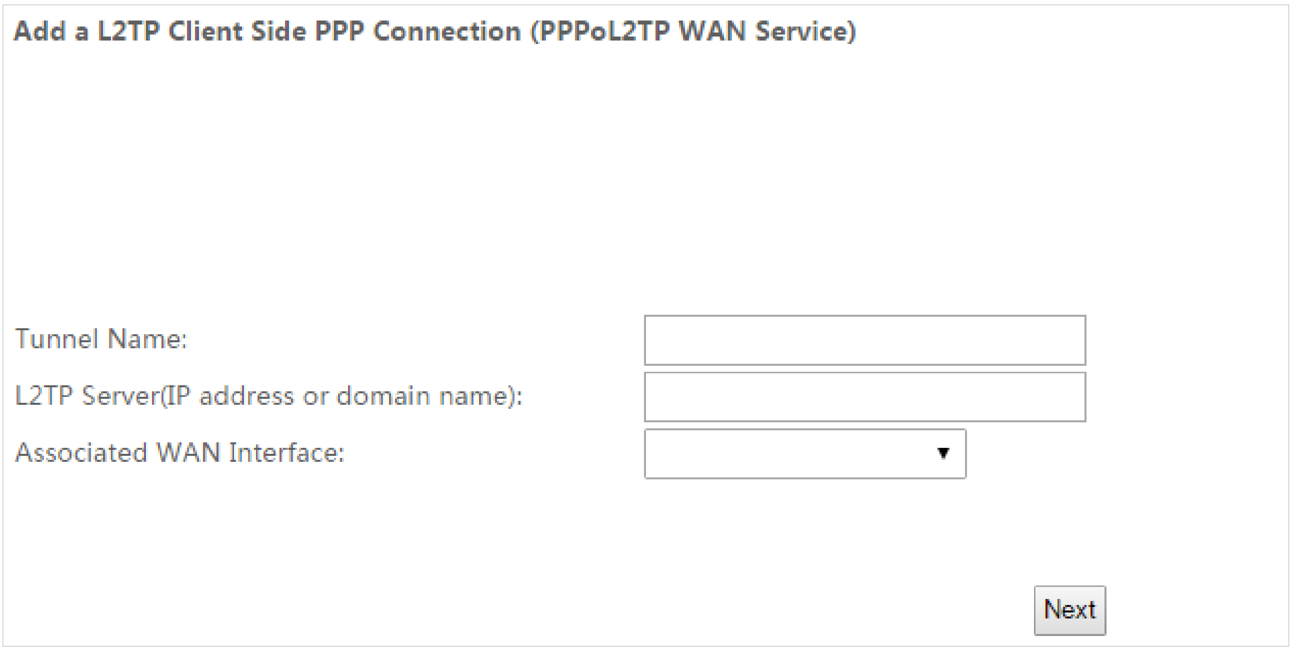
L2TP Client Side PPP Connection

Choose Add, Remove to configure a PPP over L2TP WAN Service.

Tunnel Name	L2TP Server	Associated Wan	Status	Ip Address	Remove

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

Step 3 Click **Next**.



Add a L2TP Client Side PPP Connection (PPPoL2TP WAN Service)

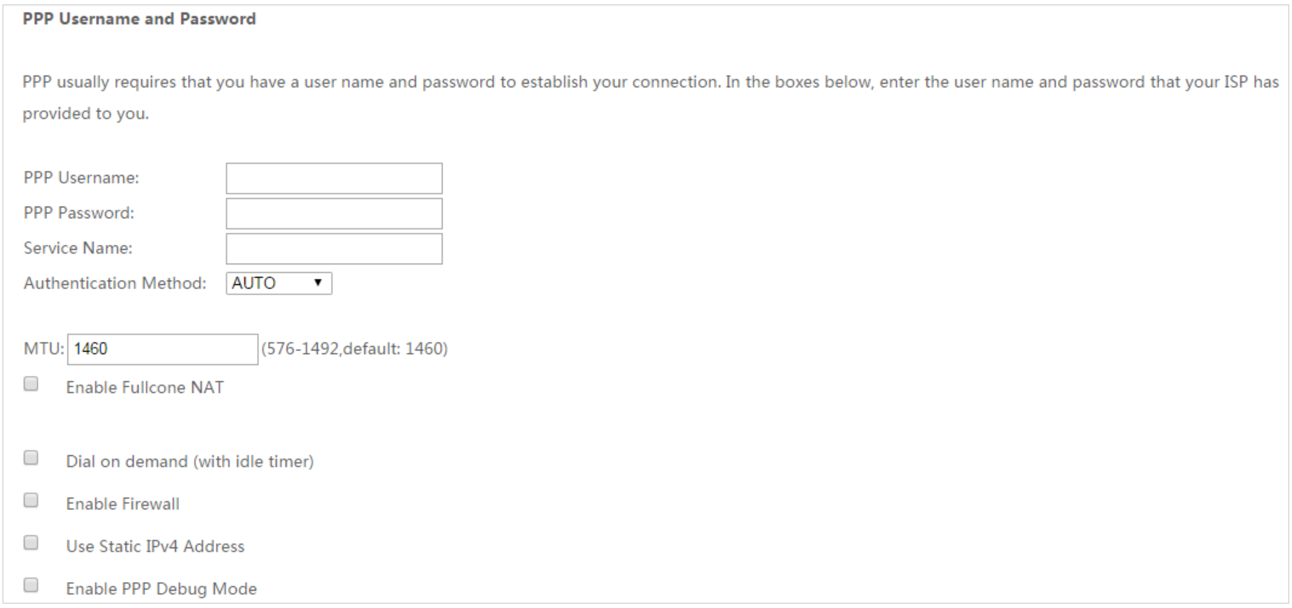
Tunnel Name:

L2TP Server(IP address or domain name):

Associated WAN Interface:

Step 4 Set **PPP Username**, **PPP Password**, and **Service Name** based on the information provided by your ISP.

Step 5 Click **Next**.



PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:

PPP Password:

Service Name:

Authentication Method: AUTO

MTU: 1460 (576-1492,default: 1460)

□ Enable Fullcone NAT

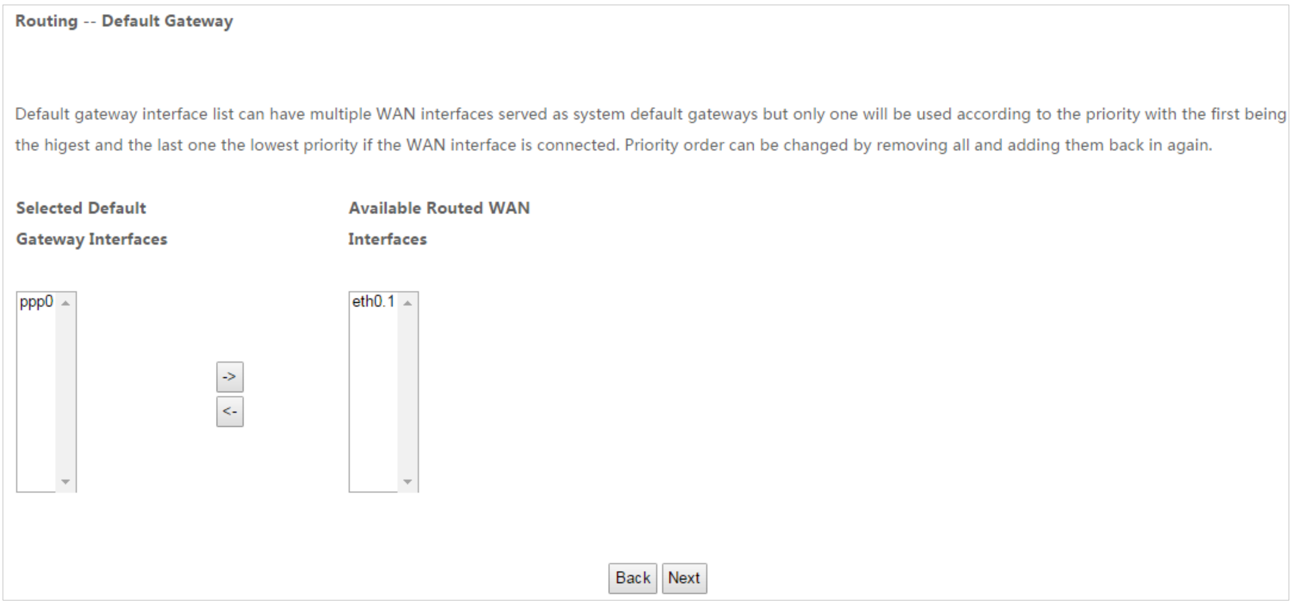
□ Dial on demand (with idle timer)

□ Enable Firewall

□ Use Static IPv4 Address

□ Enable PPP Debug Mode

Step 6 Click **Next**.



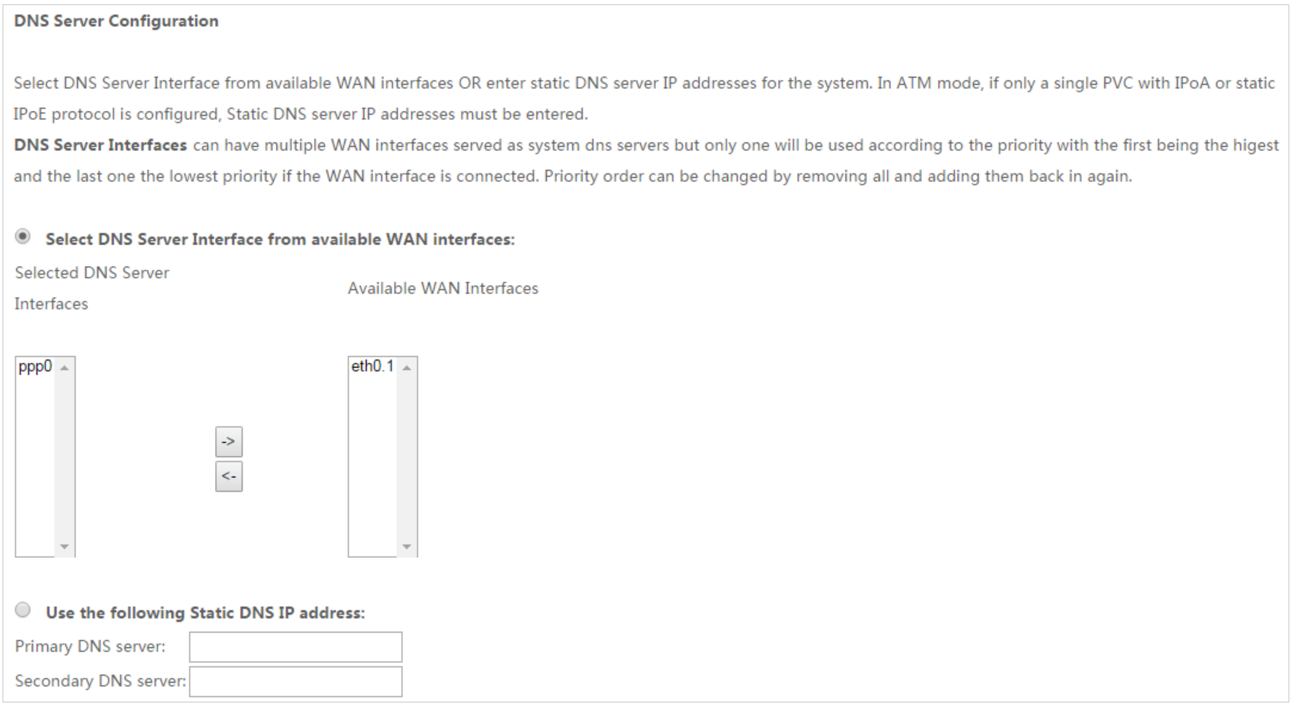
Routing -- Default Gateway

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

Selected Default Gateway Interfaces: ppp0

Available Routed WAN Interfaces: eth0.1

Step 7 Enter the DNS IP addresses information if they are provided by your ISP. If not, leave then blank.



DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

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

● **Select DNS Server Interface from available WAN interfaces:**

Selected DNS Server Interfaces: ppp0

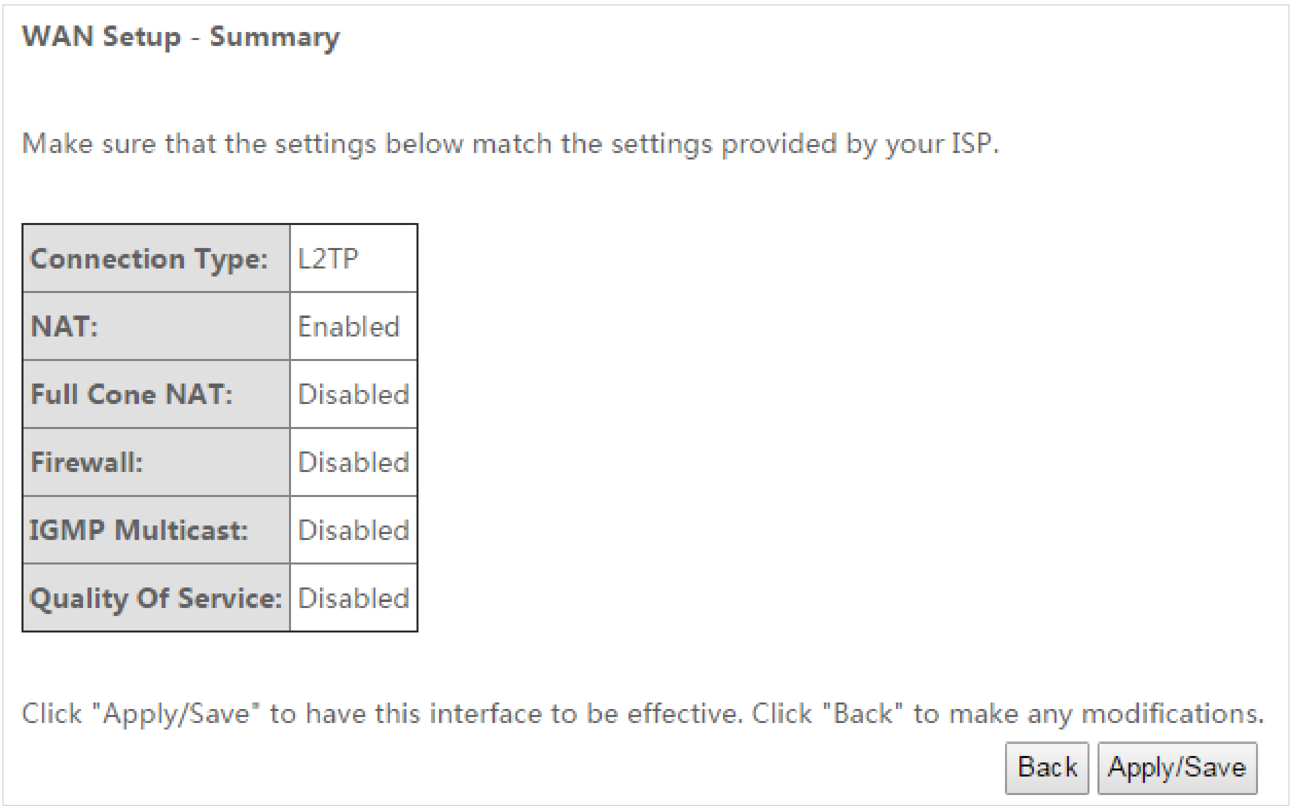
Available WAN Interfaces: eth0.1

○ **Use the following Static DNS IP address:**

Primary DNS server:

Secondary DNS server:

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



WAN Setup - Summary

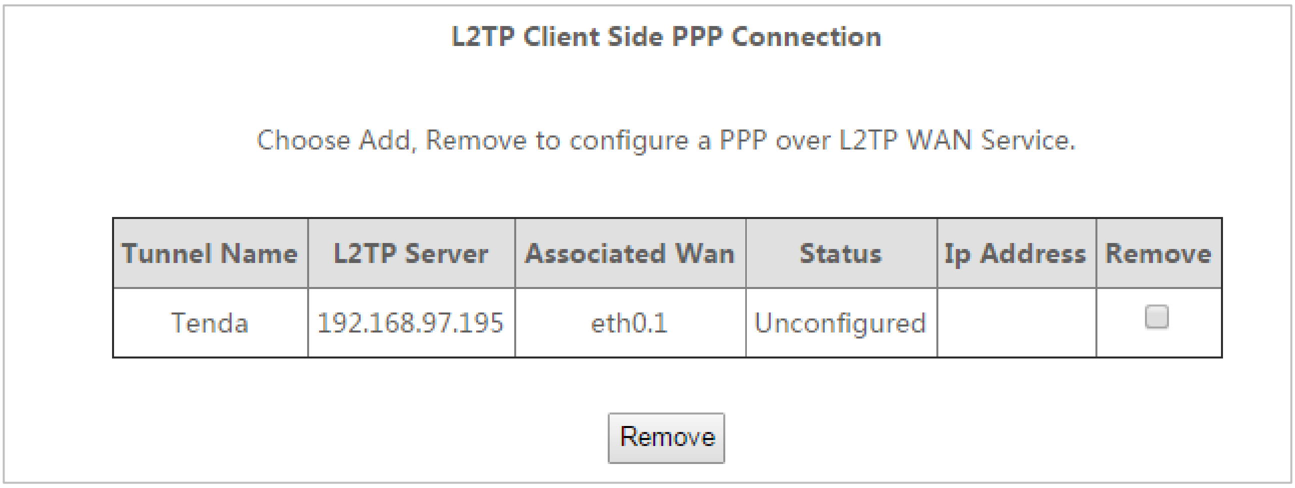
Make sure that the settings below match the settings provided by your ISP.

Connection Type:	L2TP
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

--End

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



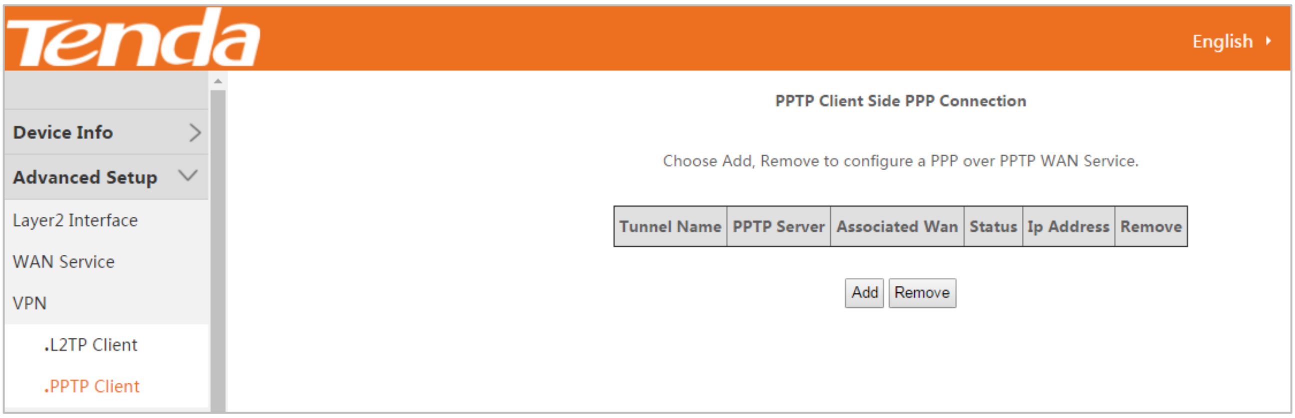
L2TP Client Side PPP Connection

Choose Add, Remove to configure a PPP over L2TP WAN Service.

Tunnel Name	L2TP Server	Associated Wan	Status	Ip Address	Remove
Tenda	192.168.97.195	eth0.1	Unconfigured		□

4.3.2 PPTP Client

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

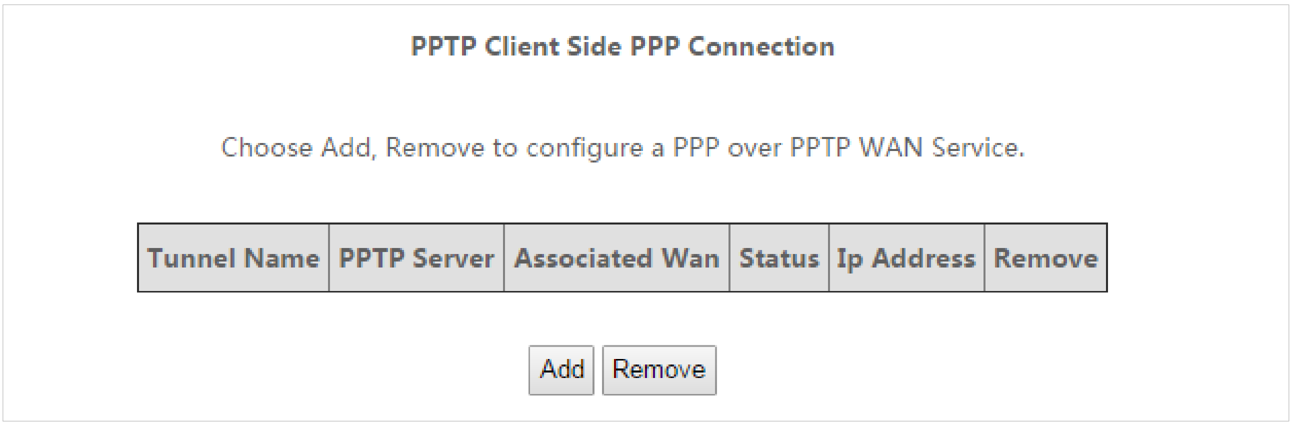


PPTP Client Side PPP Connection

Choose Add, Remove to configure a PPP over PPTP WAN Service.

Tunnel Name	PPTP Server	Associated Wan	Status	Ip Address	Remove

Step 1 Click **Add**.



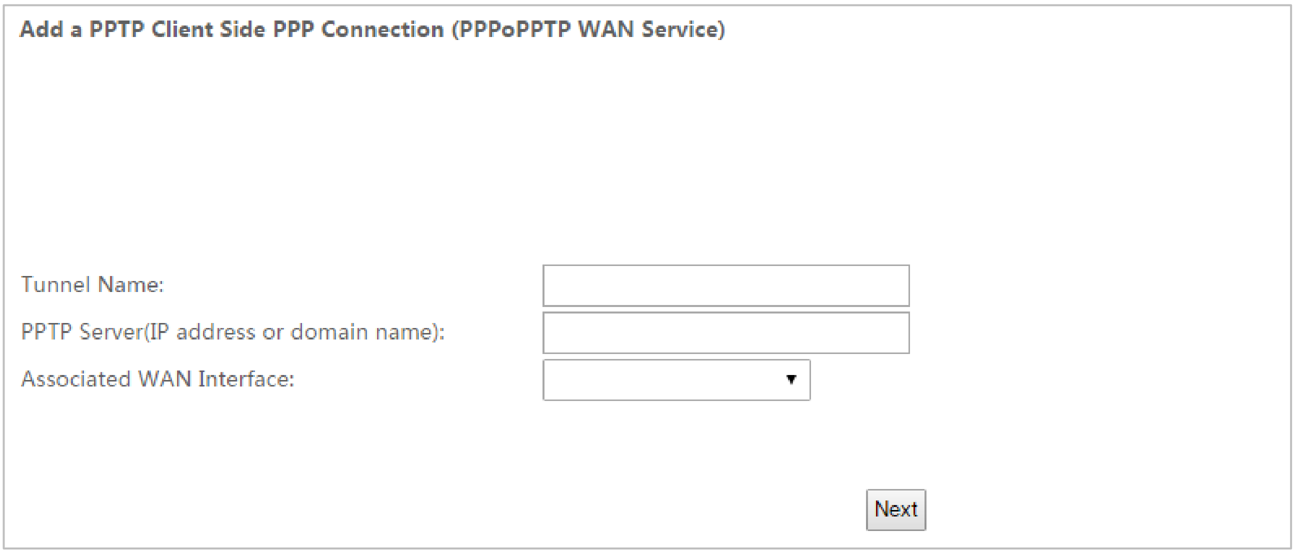
PPTP Client Side PPP Connection

Choose Add, Remove to configure a PPP over PPTP WAN Service.

Tunnel Name	PPTP Server	Associated Wan	Status	Ip Address	Remove

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

Step 3 Click **Next**.

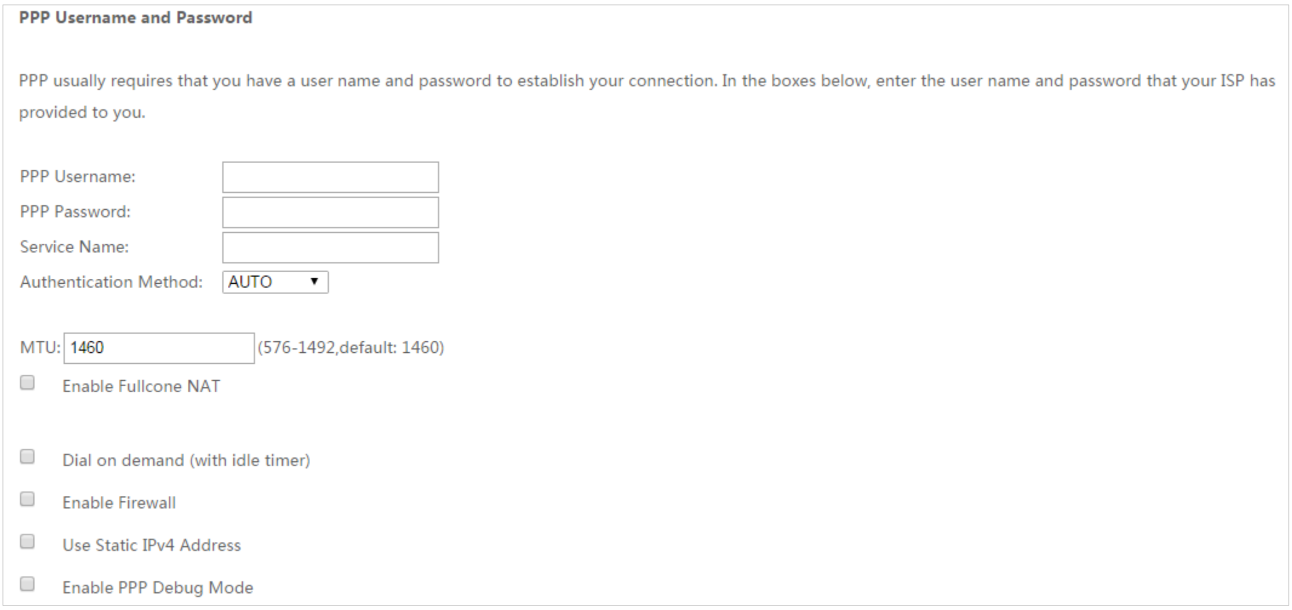


Add a PPTP Client Side PPP Connection (PPPoPPTP WAN Service)

Tunnel Name:	
PPTP Server(IP address or domain name):	
Associated WAN Interface:	▼

Step 4 Set **PPP Username**, **PPP Password**, and **Service Name** based on the information provided by your ISP.

Step 5 Click **Next**.



PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:

PPP Password:

Service Name:

Authentication Method: AUTO

MTU: 1460 (576-1492,default: 1460)

□ Enable Fullcone NAT

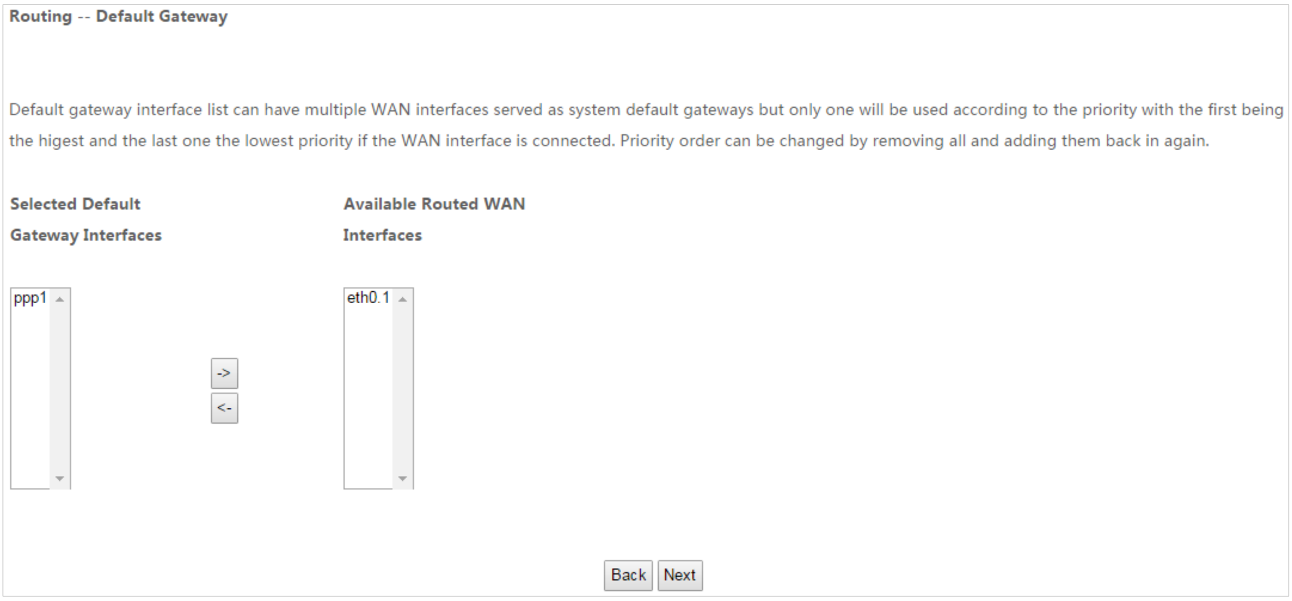
□ Dial on demand (with idle timer)

□ Enable Firewall

□ Use Static IPv4 Address

□ Enable PPP Debug Mode

Step 6 Click **Next**.

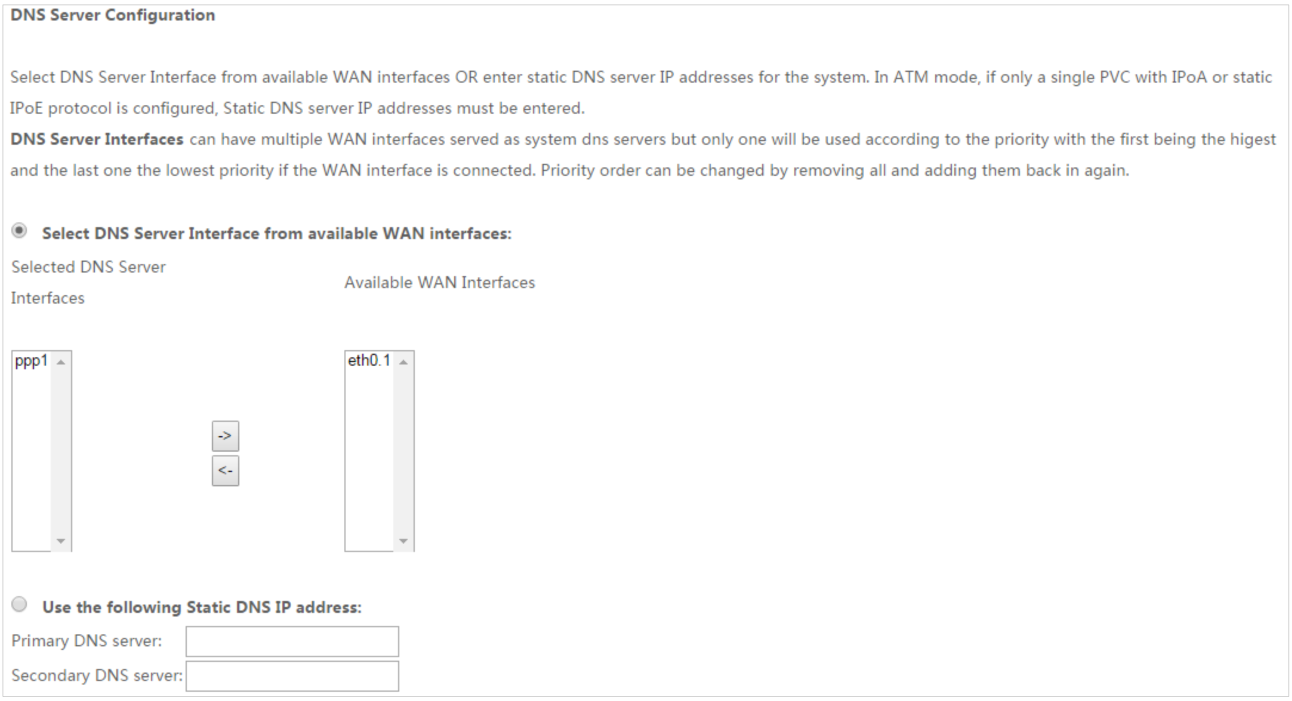


Routing -- Default Gateway

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

Selected Default Gateway Interfaces	Available Routed WAN Interfaces
ppp1	eth0.1

Step 7 Enter the DNS IP addresses information if they are provided by your ISP. If not, leave then blank.



DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

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

● **Select DNS Server Interface from available WAN interfaces:**

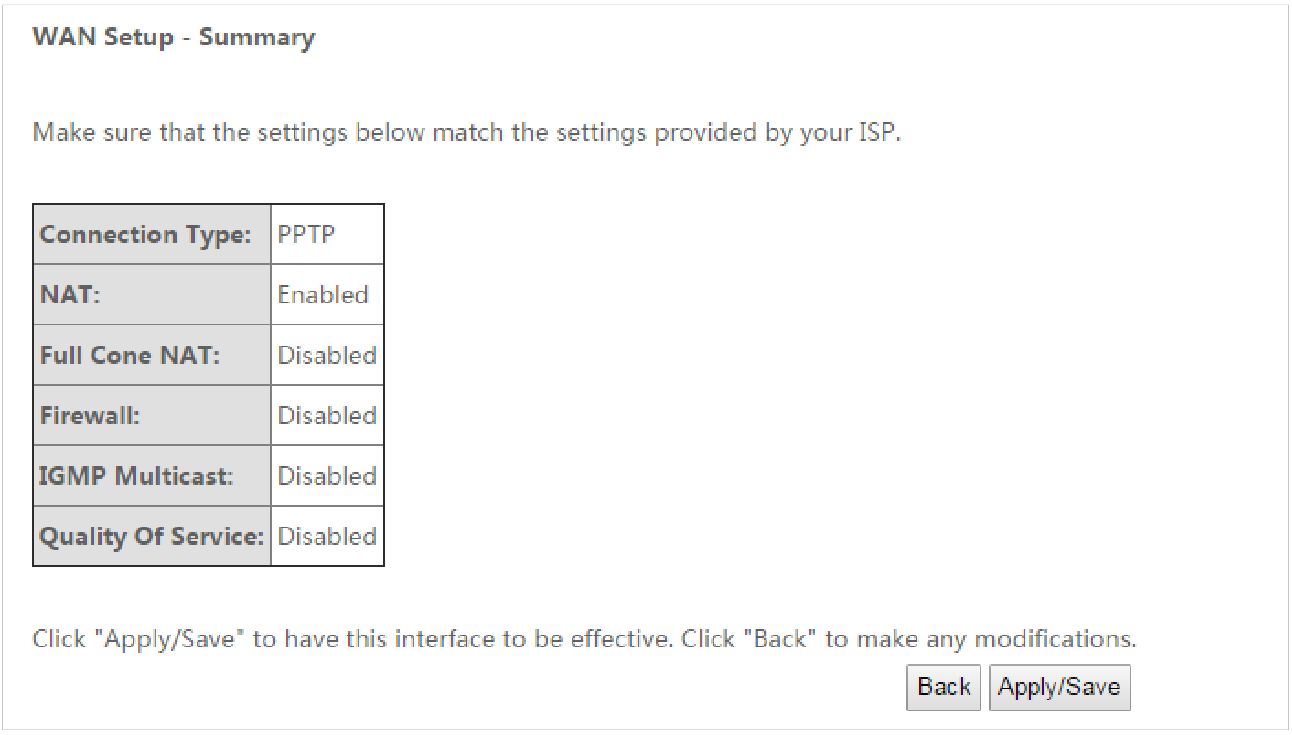
Selected DNS Server Interfaces		Available WAN Interfaces
ppp1	-> <-	eth0.1

○ **Use the following Static DNS IP address:**

Primary DNS server:

Secondary DNS server:

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



WAN Setup - Summary

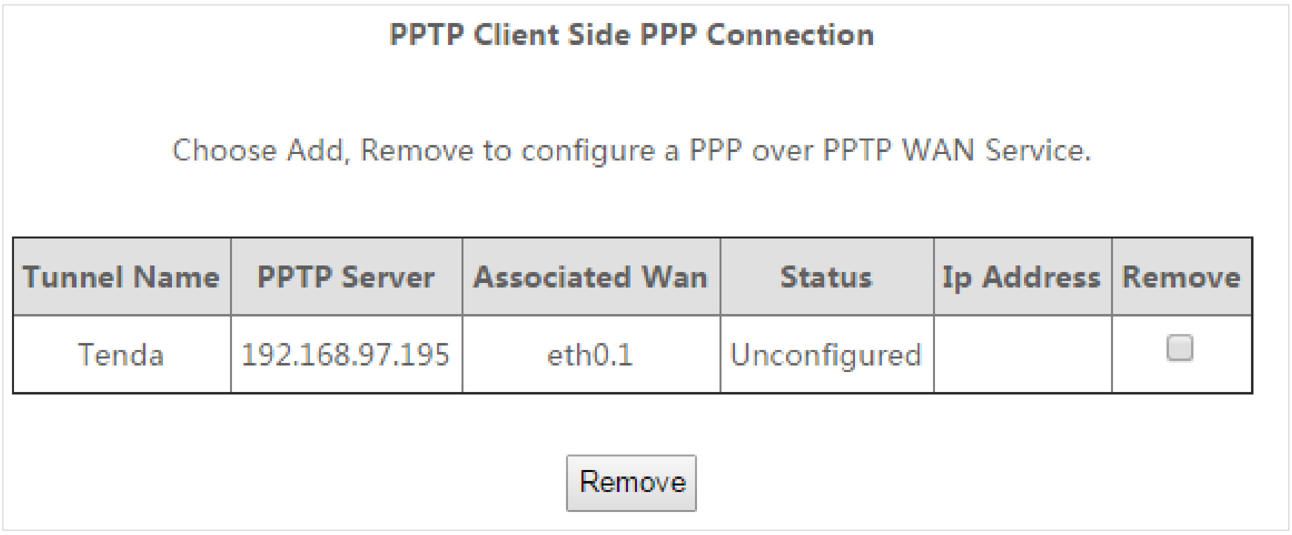
Make sure that the settings below match the settings provided by your ISP.

Connection Type:	PPTP
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

--End

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



PPTP Client Side PPP Connection

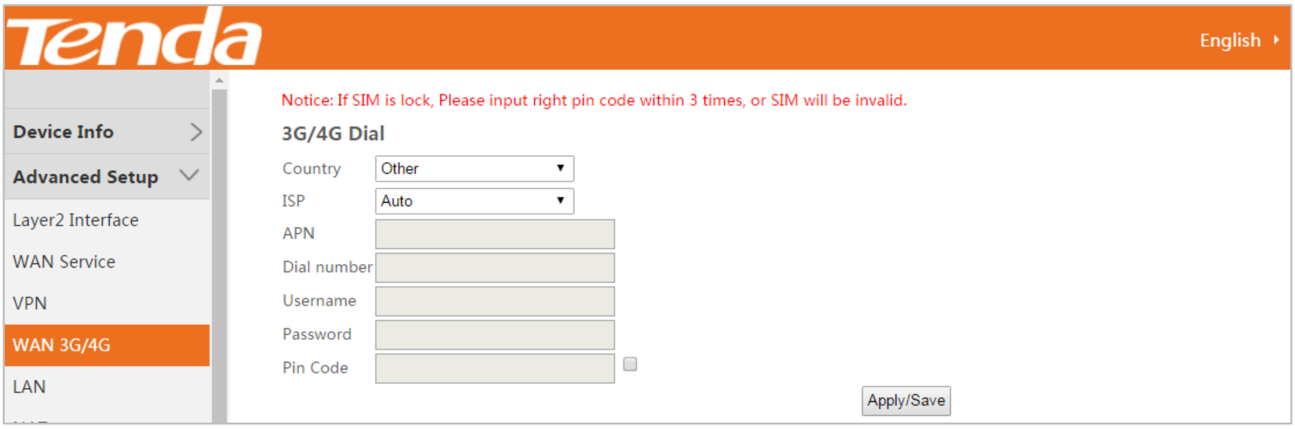
Choose Add, Remove to configure a PPP over PPTP WAN Service.

Tunnel Name	PPTP Server	Associated Wan	Status	Ip Address	Remove
Tenda	192.168.97.195	eth0.1	Unconfigured		□

4.4 3G/4G Dial

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 Dial**, you can refer to the configuration in this part.

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



Notice: If SIM is lock, Please input right pin code within 3 times, or SIM will be invalid.

3G/4G Dial

Country: Other

ISP: Auto

APN:

Dial number:

Username:

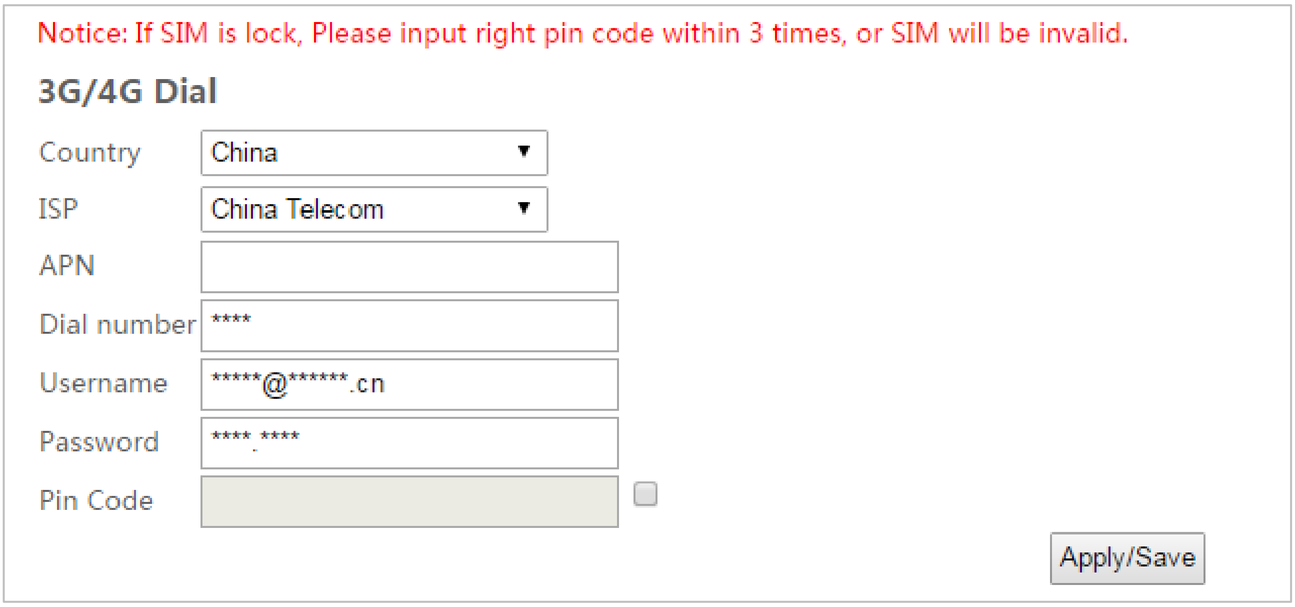
Password:

Pin Code: □

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**.



Notice: If SIM is lock, Please input right pin code within 3 times, or SIM will be invalid.

3G/4G Dial

Country	China
ISP	China Telecom
APN	
Dial number	****
Username	*****@******.cn
Password	****.****
Pin Code	□

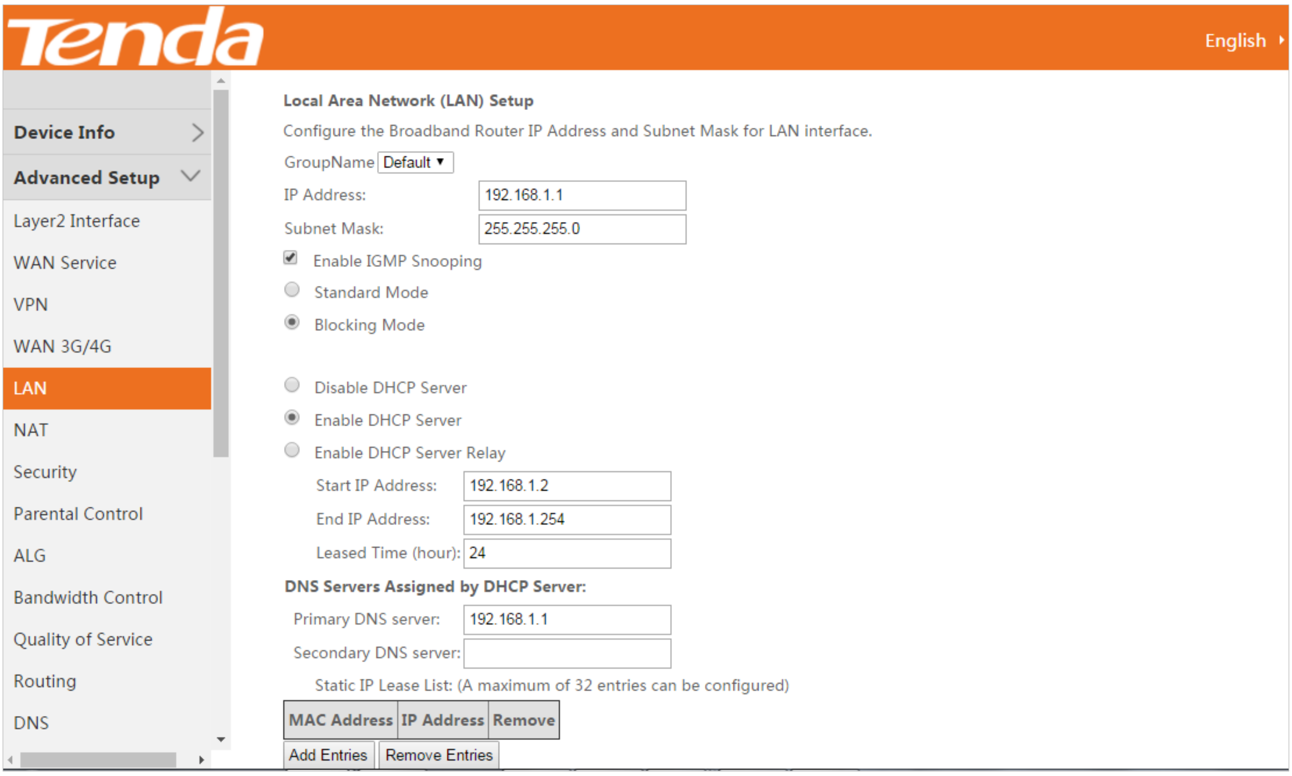
--End

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.



Local Area Network (LAN) Setup

Configure the Broadband Router IP Address and Subnet Mask for LAN interface.

GroupName Default

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

☑ Enable IGMP Snooping

○ Standard Mode

● Blocking Mode

○ Disable DHCP Server

● Enable DHCP Server

○ Enable DHCP Server Relay

Start IP Address: 192.168.1.2

End IP Address: 192.168.1.254

Leased Time (hour): 24

DNS Servers Assigned by DHCP Server:

Primary DNS server: 192.168.1.1

Secondary DNS server:

Static IP Lease List: (A maximum of 32 entries can be configured)

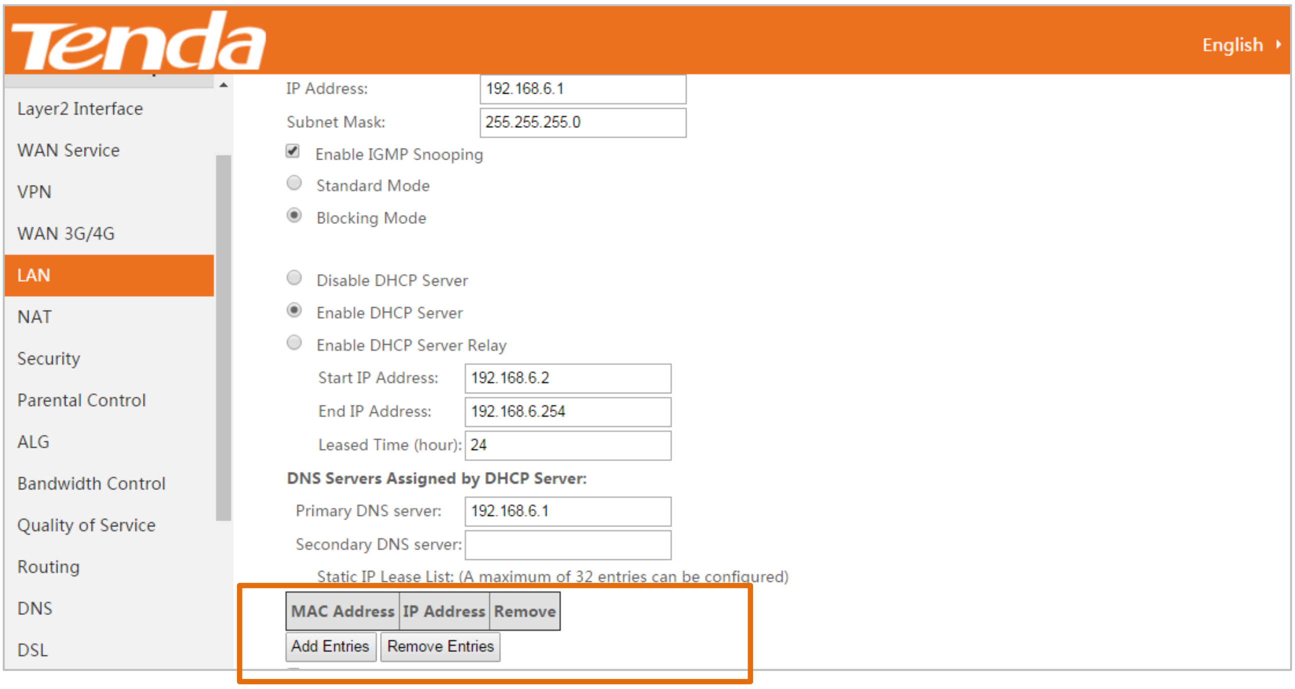
MAC Address	IP Address	Remove

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. Combined with the IP address, the IP Subnet Mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or modem router. You can change the subnet mask to fit your network.
Enable IGMP Snooping	Check to enable the IGMP Snooping feature and select either of the following two modes: Standard Mode and Blocking Mode.
Disable DHCP Server	Disable DHCP Server: It indicates that no IP address is assigned to the devices connected to the router (such as laptops and mobile phones). 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 enabled the DHCP server.
Enable DHCP Server	Enable DHCP Server: It indicates that the server that assigns one IP address within a specified IP address range to each device connected to the router. Start IP Address: Specify the start IP address of the range for the IP address pool of the DHCP server. End IP Address: Specify the end IP address of the range for the IP address pool of the DHCP server.
Leased Time	It specifies the validity period of one IP address assigned to a device connected to 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 fixed 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.



IP Address: 192.168.6.1

Subnet Mask: 255.255.255.0

☑ Enable IGMP Snooping

○ Standard Mode

● Blocking Mode

○ Disable DHCP Server

● Enable DHCP Server

○ Enable DHCP Server Relay

Start IP Address: 192.168.6.2

End IP Address: 192.168.6.254

Leased Time (hour): 24

DNS Servers Assigned by DHCP Server:

Primary DNS server: 192.168.6.1

Secondary DNS server:

Static IP Lease List: (A maximum of 32 entries can be configured)

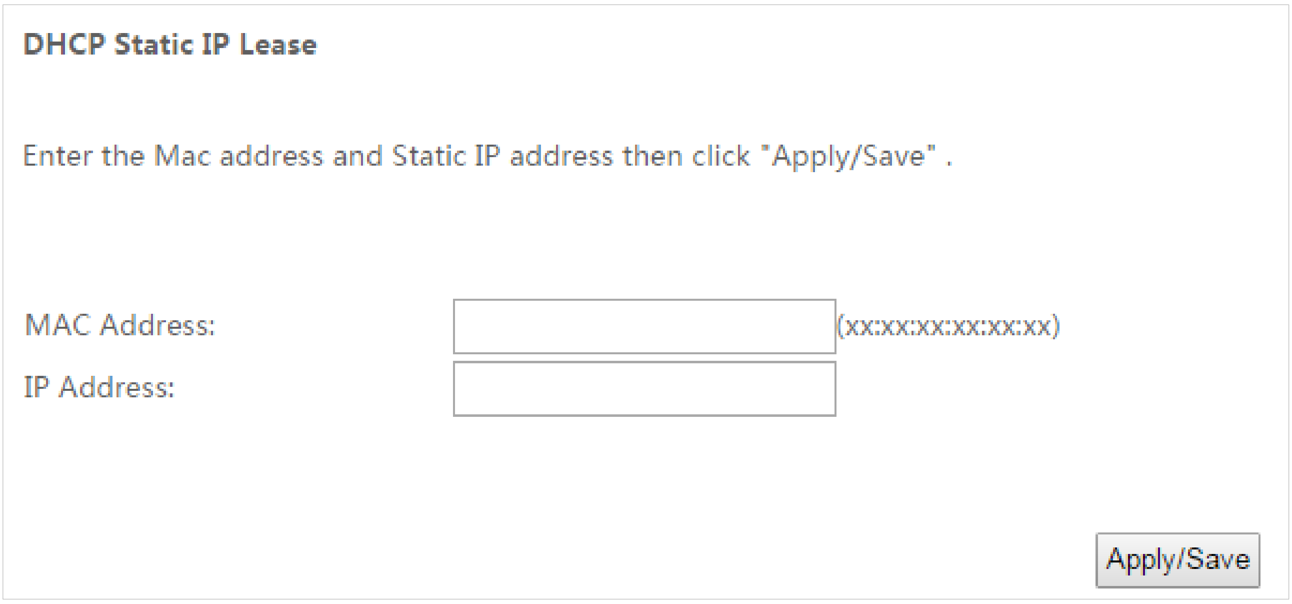
MAC Address	IP Address	Remove

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**.



DHCP Static IP Lease

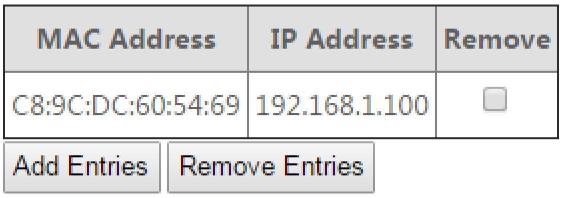
Enter the Mac address and Static IP address then click "Apply/Save" .

MAC Address: (xx:xx:xx:xx:xx:xx)

IP Address:

--End

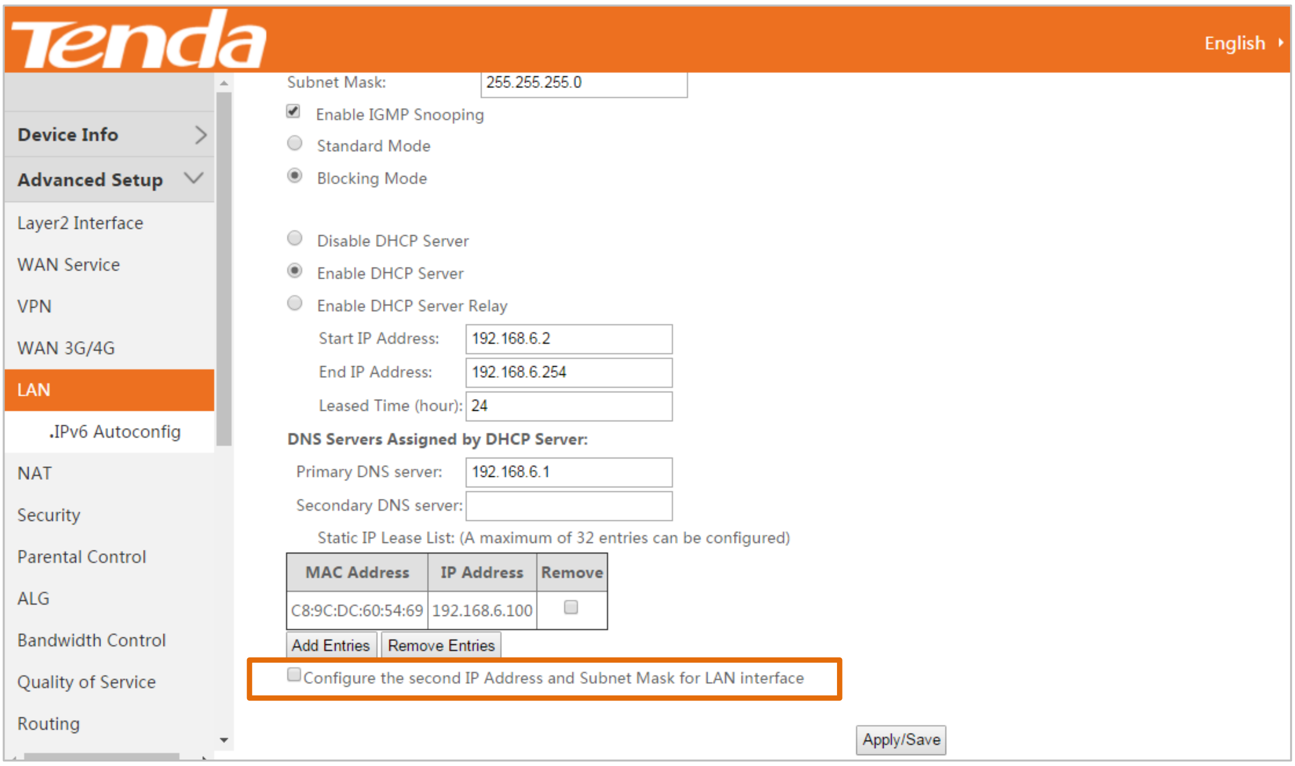
The added entry appears in the table.



MAC Address	IP Address	Remove
C8:9C:DC:60:54:69	192.168.1.100	□

To Configure a Second IP Address for LAN Interface

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



Subnet Mask: 255.255.255.0

☑ Enable IGMP Snooping

○ Standard Mode

● Blocking Mode

○ Disable DHCP Server

● Enable DHCP Server

○ Enable DHCP Server Relay

Start IP Address: 192.168.6.2

End IP Address: 192.168.6.254

Leased Time (hour): 24

DNS Servers Assigned by DHCP Server:

Primary DNS server: 192.168.6.1

Secondary DNS server:

Static IP Lease List: (A maximum of 32 entries can be configured)

MAC Address	IP Address	Remove
C8:9C:DC:60:54:69	192.168.6.100	□

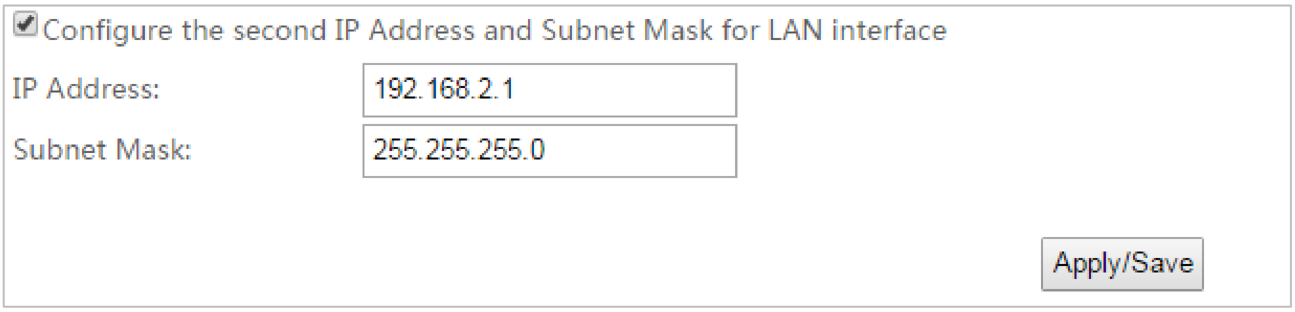
□ Configure the second IP Address and Subnet Mask for LAN interface

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 specifies a 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**.



☑ Configure the second IP Address and Subnet Mask for LAN interface

IP Address: 192.168.2.1

Subnet Mask: 255.255.255.0

--End

TIP

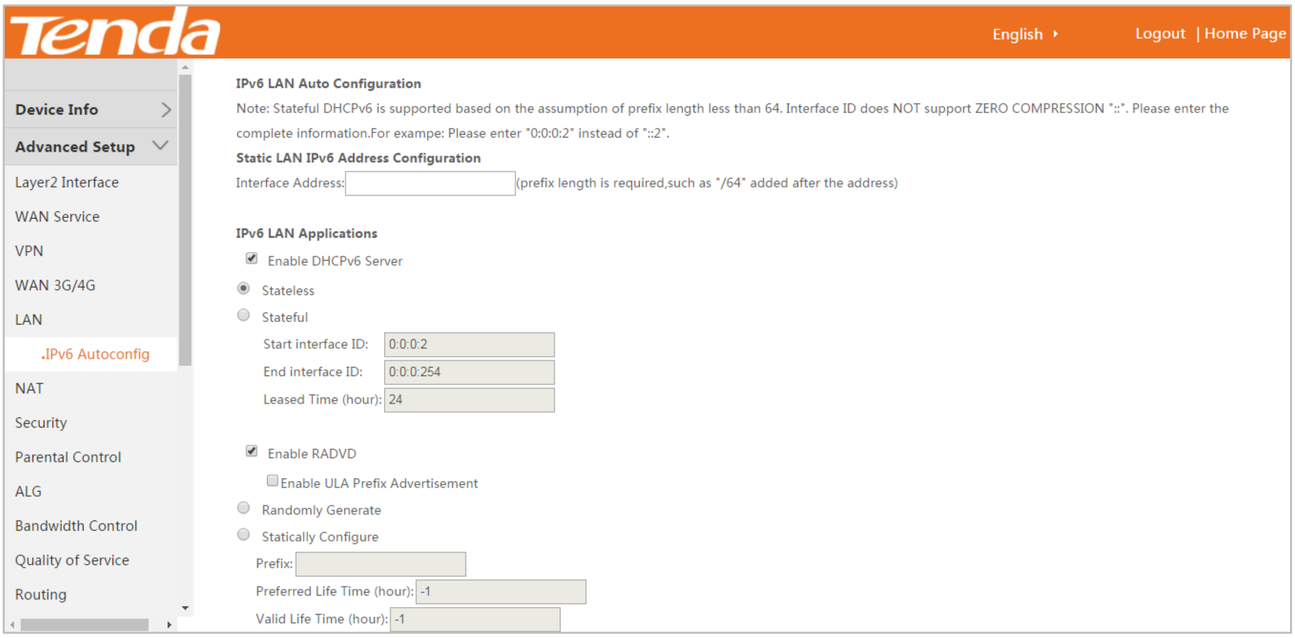
The second LAN IP address can also be used to log in to the web UI of the modem router.

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



IPv6 LAN Auto Configuration

Note: Stateful DHCPv6 is supported based on the assumption of prefix length less than 64. Interface ID does NOT support ZERO COMPRESSION "::". Please enter the complete information.For exampe: Please enter "0:0:0:2" instead of "::2".

Static LAN IPv6 Address Configuration

Interface Address: (prefix length is required,such as "/64" added after the address)

IPv6 LAN Applications

☑ Enable DHCPv6 Server

● Stateless

○ Stateful

Start interface ID: 0:0:0:2

End interface ID: 0:0:0:254

Leased Time (hour): 24

☑ Enable RADVD

□ Enable ULA Prefix Advertisement

○ Randomly Generate

○ Statically Configure

Prefix:

Preferred Life Time (hour): -1

Valid Life Time (hour): -1

Parameter	Description
Enable DHCPv6 Server	Check to enable the DHCPv6 Server.
Stateless	If selected, IPv6 clients will generate IPv6 addresses automatically based on the Prefix Delegation's IPv6 prefix and their own MAC addresses.
Stateful	Stateful DHCPv6 is supported based on the assumption of prefix length less than 64. Select this option and configure the start/end interface ID and leased time. The router will automatically assign IPv6 addresses to IPv6 clients.
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 a time length that the IP address is assigned to each device before it is refreshed.
Enable RADVD	The RADVD (Router Advertisement Daemon) implements link-local advertisements of IPv6 router addresses and IPv6 routing prefixes using the Neighbor Discovery Protocol (NDP) and is used by system administrators in stateless auto configuration methods of network hosts on Internet Protocol version 6 networks. Check the checkbox to enable the RADVD.
Enable ULA Prefix Advertisement	If enabled, the router will advertise ULA prefix periodically.
Randomly Generate	If selected, address prefix can be automatically generated.
Statically Configure	If you select this option, you need to manually configure the address prefix and life

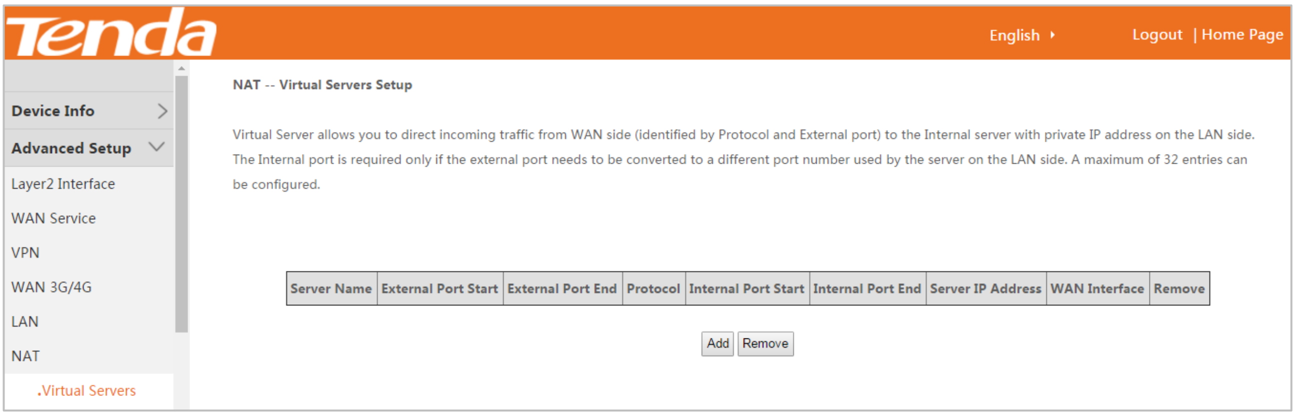
	time.
Prefix	Specify the prefix.
Preferred Life Time (hour)	Specify the preferred life time in hour.
Valid Life Time (hour)	Specify the valid life time in hour.
Enable MLD Snooping	MLD is used by IPv6 routers for discovering multicast listeners on a directly attached link. If disabled on layer2 devices, IPv6 multicast data packets will be broadcast on the entire layer2; if enabled, these packets will be multicast to only specified recipient instead of being broadcast on the entire layer2.

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.



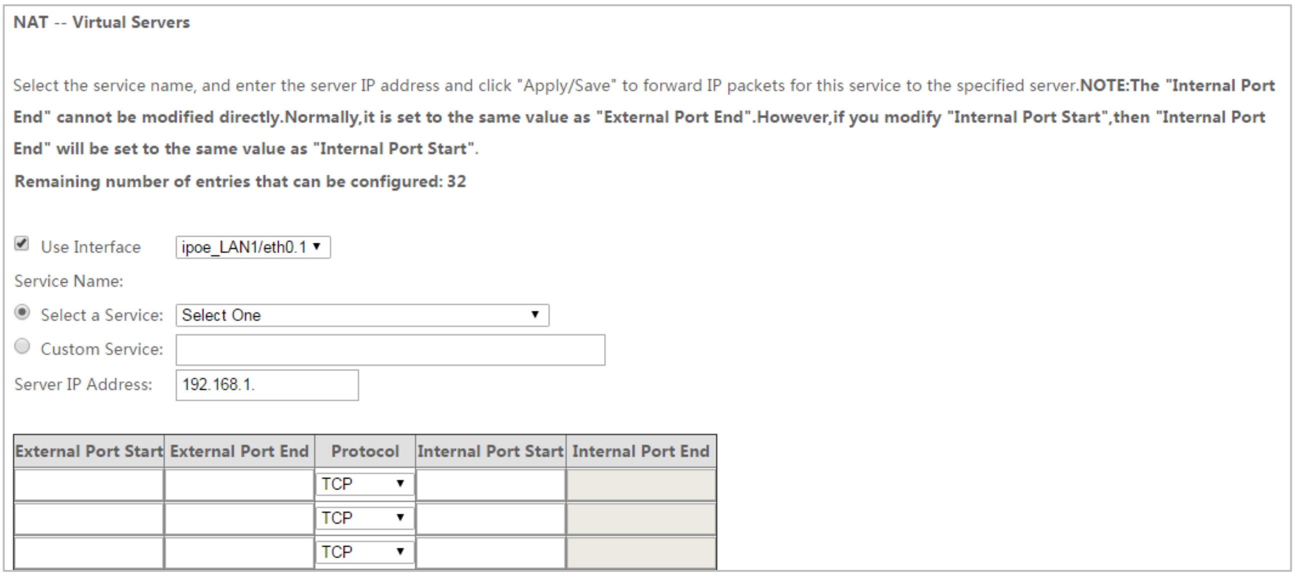
NAT -- Virtual Servers Setup

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum of 32 entries can be configured.

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	WAN Interface	Remove

Add Remove

Click **Add** to configure the function.



NAT -- Virtual Servers

Select the service name, and enter the server IP address and click "Apply/Save" to forward IP packets for this service to the specified server.**NOTE:The "Internal Port End" cannot be modified directly.Normally,it is set to the same value as "External Port End".However,if you modify "Internal Port Start",then "Internal Port End" will be set to the same value as "Internal Port Start".**

Remaining number of entries that can be configured: 32

☑ Use Interface ipoe_LAN1/eth0.1

Service Name:

● Select a Service: Select One

○ Custom Service:

Server IP Address: 192.168.1.

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
		TCP		
		TCP		
		TCP		

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. 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 router’s local area network (LAN).

Application Example

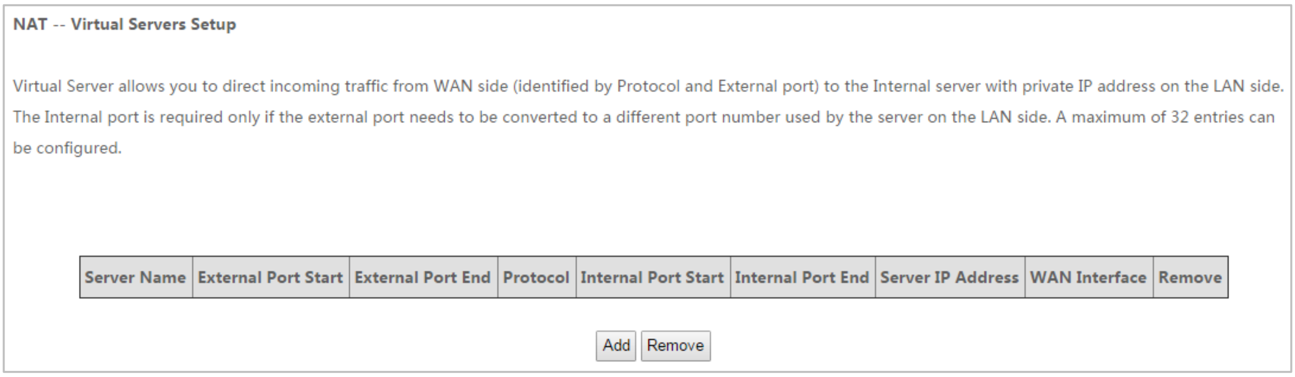
You have set up an FTP server on your LAN:

- 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 and web server on default port over the internet. To access your FTP or web server from the Internet, a remote user has to know the Internet IP address or internet 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*. Then follow instructions below:

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

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



NAT -- Virtual Servers Setup

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum of 32 entries can be configured.

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	WAN Interface	Remove

Step 1 Click **Add**.

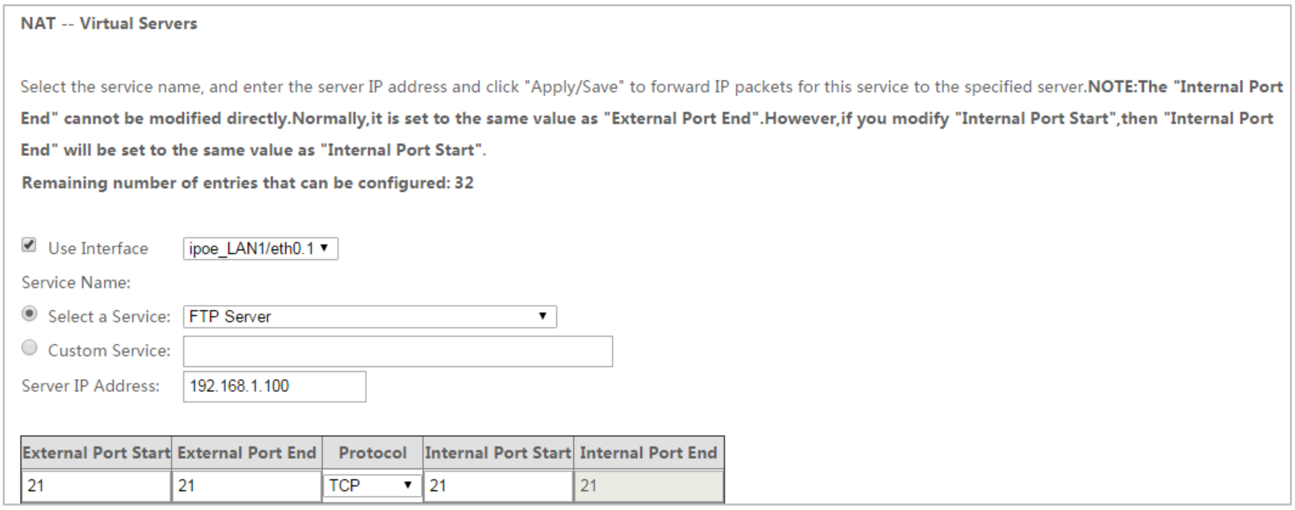
Step 2 Select FTP that you wish to host on your network from the Select a Service drop-down list. The port number (21) used by this service will then be automatically populated.

If you wish to define the service yourself, enter a descriptive name in the Custom Service, say 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 3 Select a protocol from the Protocol drop-down list. If you are unsure, select TCP/UDP.

Step 4 In the Server IP Address field, enter the last digit of the IP address of your local computer that offers this service. Here in this example, we enter *192.168.1.100*.

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



NAT -- Virtual Servers

Select the service name, and enter the server IP address and click "Apply/Save" to forward IP packets for this service to the specified server.**NOTE:The "Internal Port End" cannot be modified directly.Normally,it is set to the same value as "External Port End".However,if you modify "Internal Port Start",then "Internal Port End" will be set to the same value as "Internal Port Start".**

Remaining number of entries that can be configured: 32

☑ Use Interface ipoe_LAN1/eth0.1

Service Name:

● Select a Service: FTP Server

○ Custom Service:

Server IP Address: 192.168.1.100

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
21	21	TCP	21	21

--End

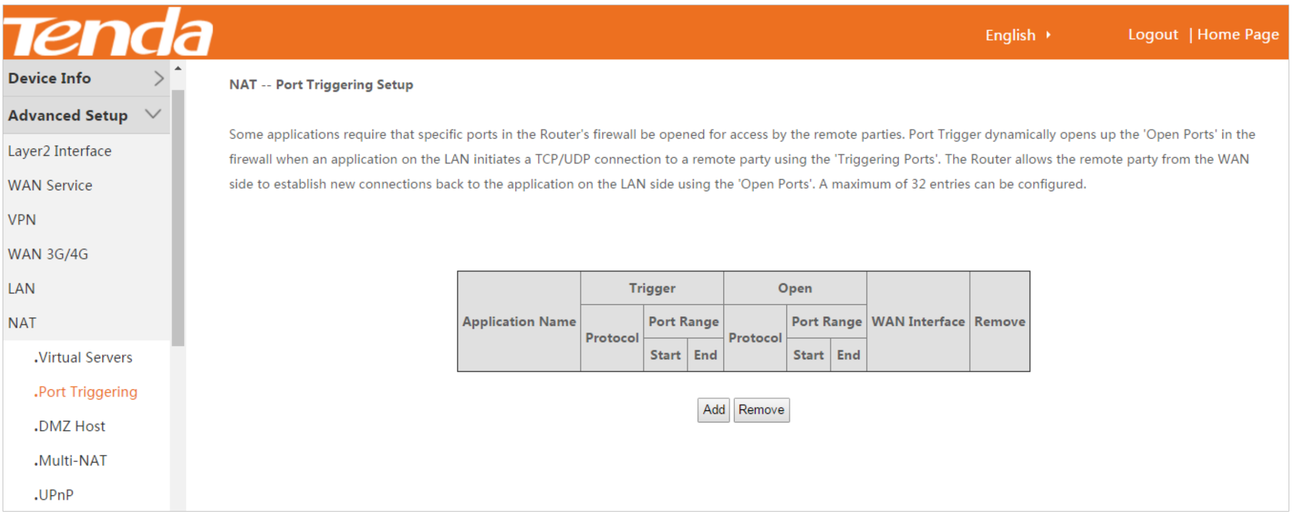
Remote Access:

Your friends can access your FTP server by entering "*ftp://183.37.227.201*" 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 Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'.

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

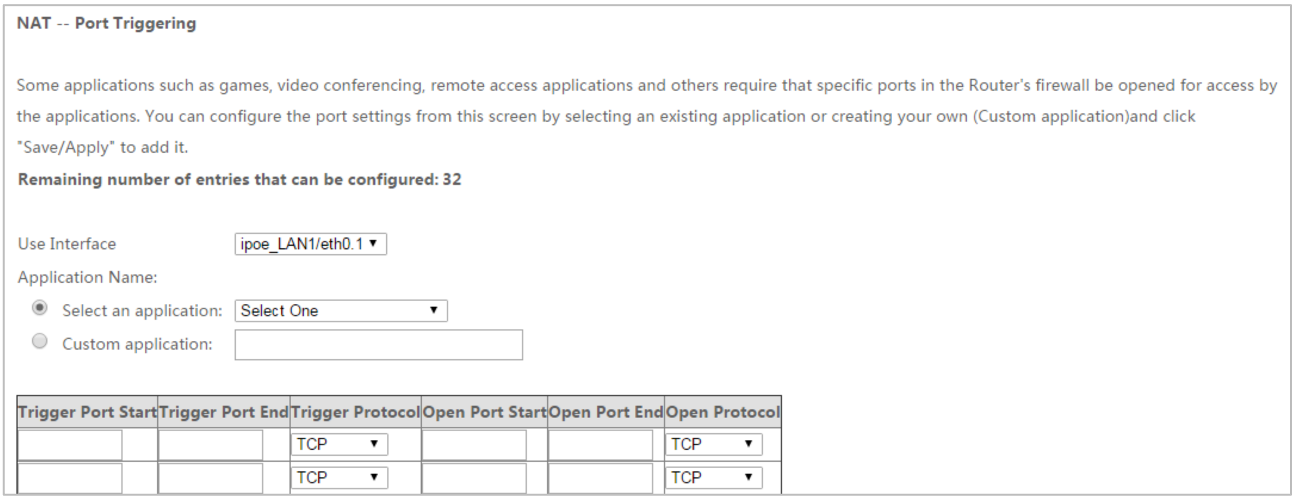


NAT -- Port Triggering Setup

Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum of 32 entries can be configured.

Application Name	Trigger			Open			WAN Interface	Remove
	Protocol	Port Range		Protocol	Port Range			
		Start	End		Start	End		

Click **Add** to configure the function.



NAT -- Port Triggering

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application)and click "Save/Apply" to add it.

Remaining number of entries that can be configured: 32

Use Interface ipoe_LAN1/eth0.1

Application Name:

● Select an application: Select One

○ Custom application:

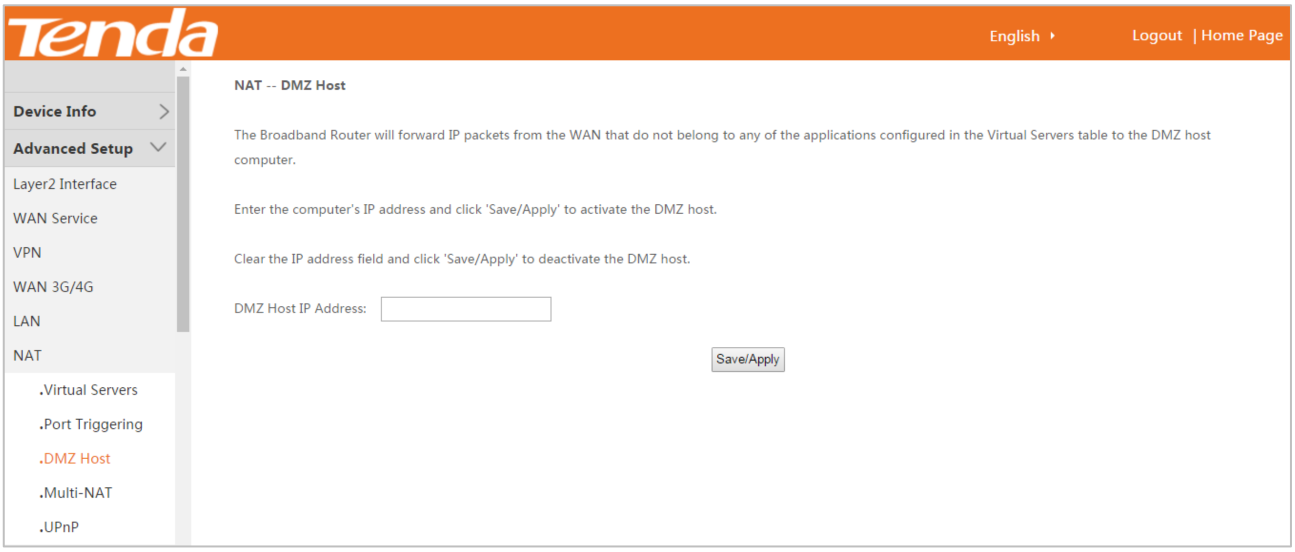
Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
		TCP			TCP
		TCP			TCP

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. 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 videoconferencing applications that are not compatible with NAT (Network Address Translation).

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



NAT -- DMZ Host

The Broadband Router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

Enter the computer's IP address and click 'Save/Apply' to activate the DMZ host.

Clear the IP address field and click 'Save/Apply' to deactivate the DMZ host.

DMZ Host IP Address:

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

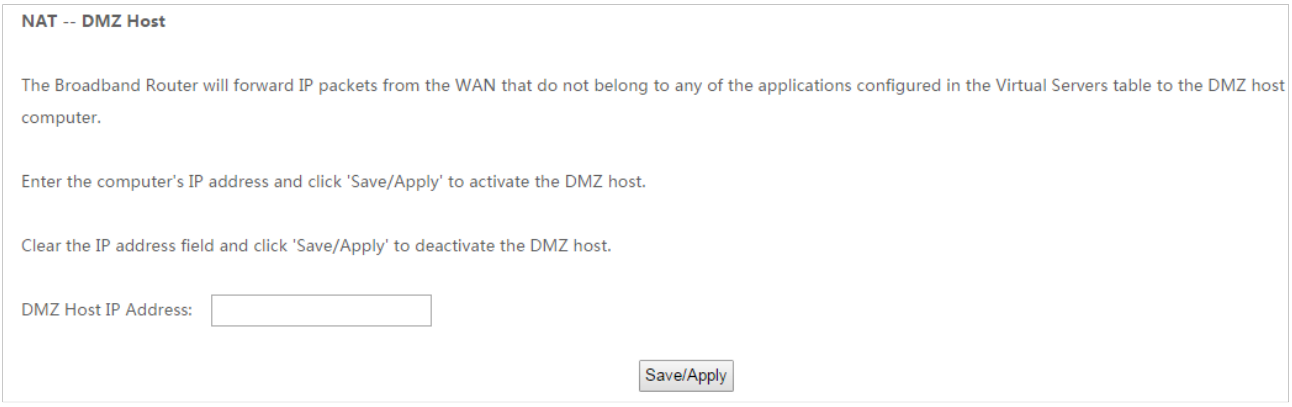
- A DMZ host is not protected by the firewall of the router. A hacker may leverage the DMZ host to attack your LAN. Therefore, enable the DMZ function only when necessary.
- Manually set the IP address of the LAN computer that functions as a DMZ host, to prevent IP address changes, which lead to DMZ 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 an IP address of the DMZ host.

Step 3 Click **Save/Apply**.


NAT -- DMZ Host

The Broadband Router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

Enter the computer's IP address and click 'Save/Apply' to activate the DMZ host.

Clear the IP address field and click 'Save/Apply' to deactivate the DMZ host.

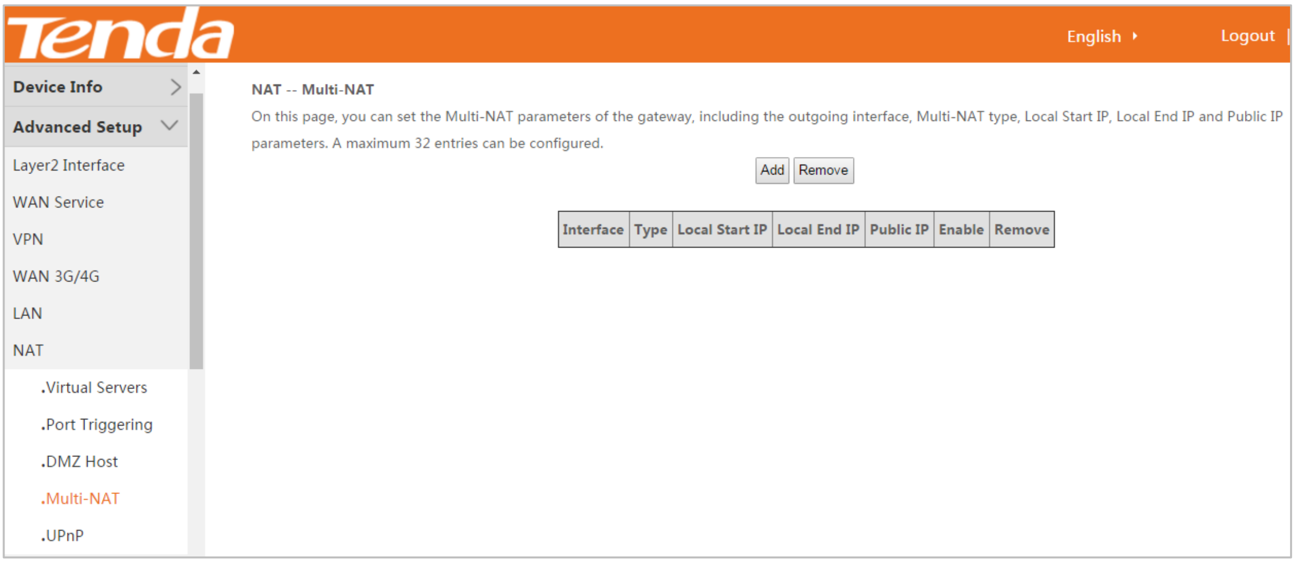
DMZ Host IP Address:

--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 internet (or local network) IP address. Multi-NAT has "one to one", and "many to one" types of configurations.

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

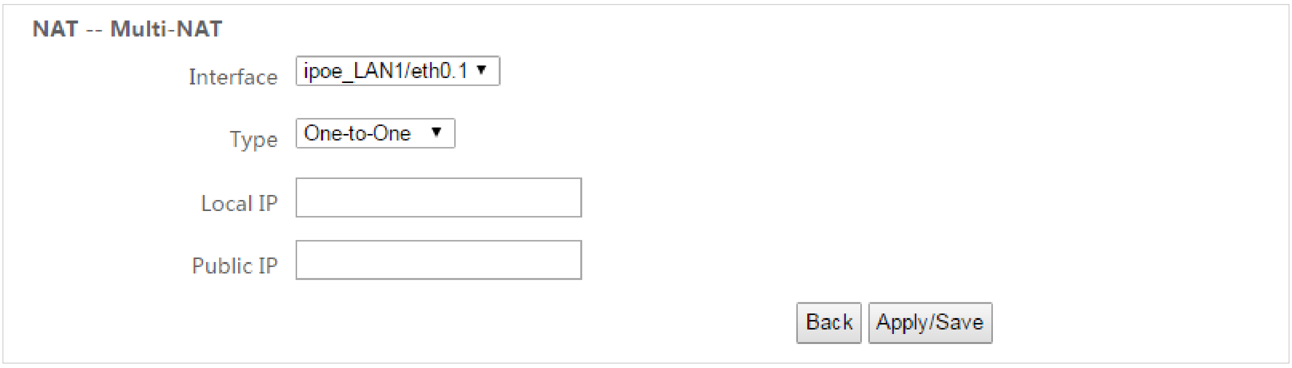


NAT -- Multi-NAT

On this page, you can set the Multi-NAT parameters of the gateway, including the outgoing interface, Multi-NAT type, Local Start IP, Local End IP and Public IP parameters. A maximum 32 entries can be configured.

Interface	Type	Local Start IP	Local End IP	Public IP	Enable	Remove

Click **Add** to configure the function.


NAT -- Multi-NAT

Interface: ipoe_LAN1/eth0.1

Type: One-to-One

Local IP

Public IP

Parameter	Description
Interface	Select a WAN interface that the function is used.
Type	One-to-One: Set a route from a local IP address to a public IP address Many-to-One: Set a route from many local IP addresses to a public IP address
Local IP	To specify a local IP address
Local Start/End IP	To specify a range of local IP address
Public IP	To 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

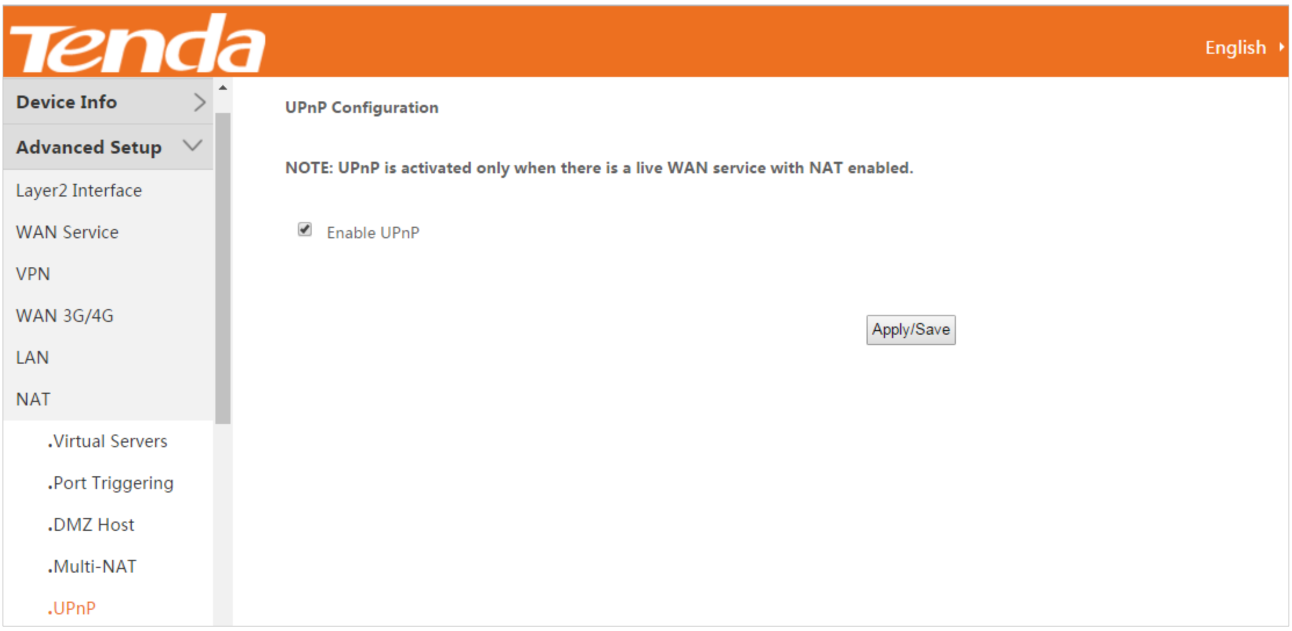
TIP

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.



UPnP Configuration

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

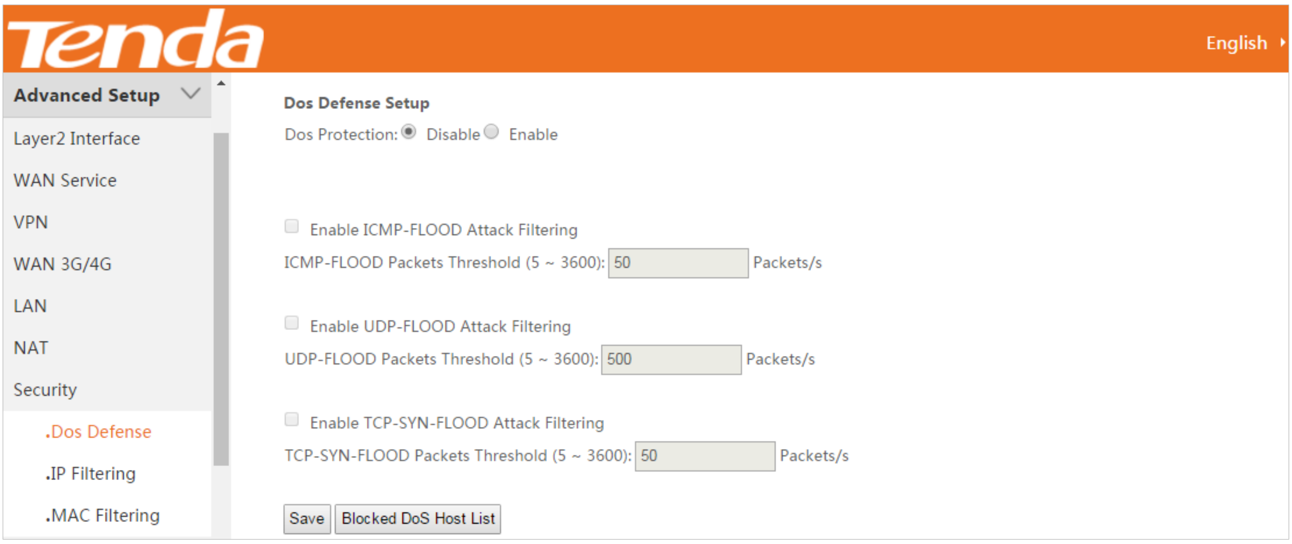
☑ Enable UPnP

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 from ICMP-FLOOD attack, UDP-FLOOD attack, and TCP-SYN-FLOOD attack.

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



Dos Defense Setup

Dos Protection: ● Disable ○ Enable

□ Enable ICMP-FLOOD Attack Filtering

ICMP-FLOOD Packets Threshold (5 ~ 3600): 50 Packets/s

□ Enable UDP-FLOOD Attack Filtering

UDP-FLOOD Packets Threshold (5 ~ 3600): 500 Packets/s

□ Enable TCP-SYN-FLOOD Attack Filtering

TCP-SYN-FLOOD Packets Threshold (5 ~ 3600): 50 Packets/s

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

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

Step 2 Select the corresponding attack filtering.

Step 3 Click **Save**.

--End

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

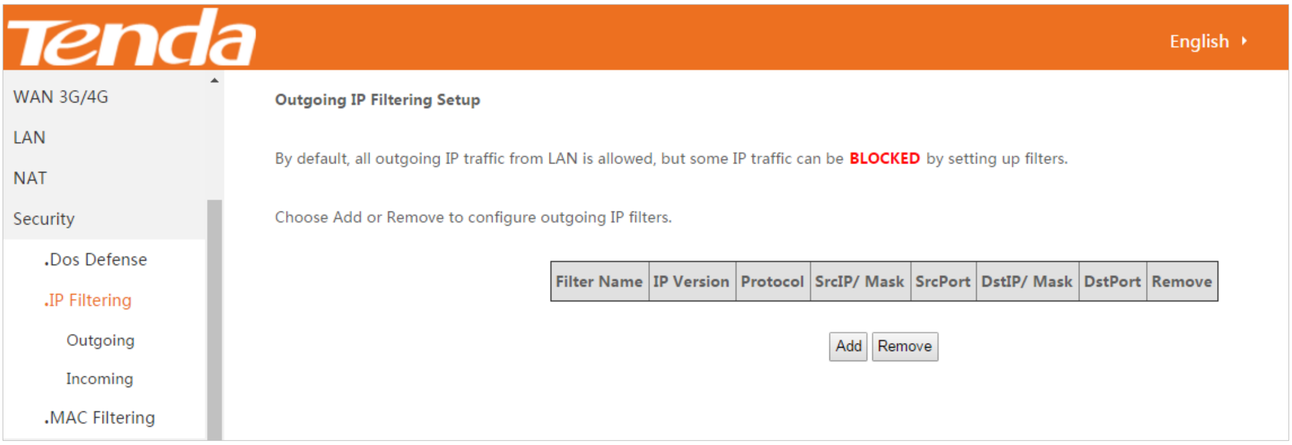
4.7.2 IP Filtering

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

Outgoing

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



Outgoing IP Filtering Setup

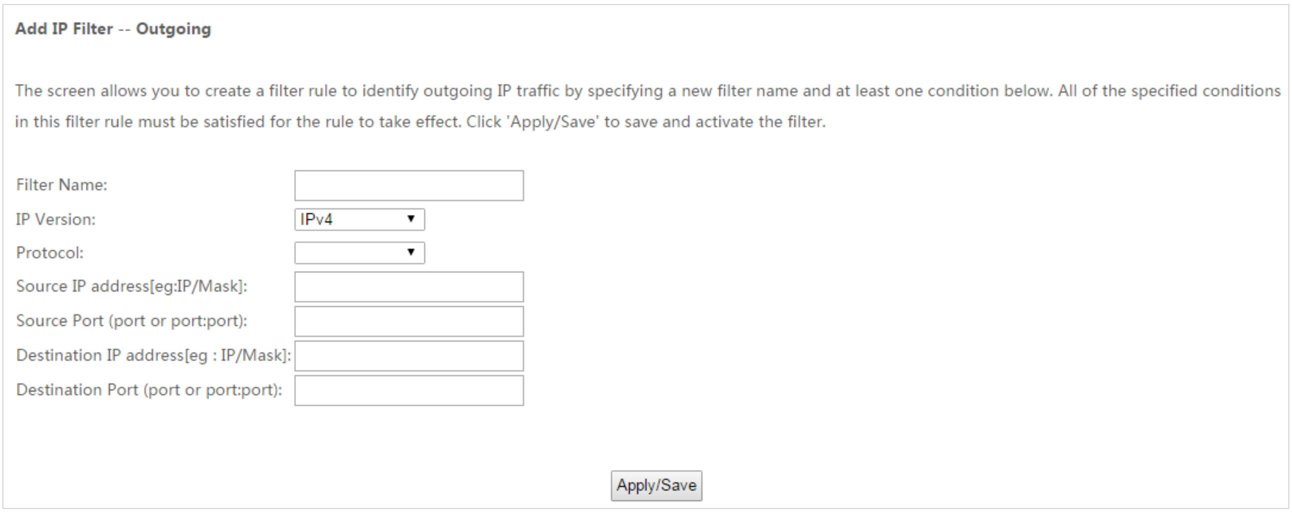
By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be BLOCKED by setting up filters.

Choose Add or Remove to configure outgoing IP filters.

Filter Name	IP Version	Protocol	SrcIP/ Mask	SrcPort	DstIP/ Mask	DstPort	Remove

To configure the Outgoing function, perform the following procedure:

Step 1 Click **Add**.



Add IP Filter -- Outgoing

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

Filter Name:	
IP Version:	IPv4
Protocol:	
Source IP address[eg:IP/Mask]:	
Source Port (port or port:port):	
Destination IP address[eg : IP/Mask]:	
Destination Port (port or port:port):	

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

Step 3 **IP Version:** Select your IP protocol, IPv4 or IPv6.

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

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

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

Step 7 **Destination IP address [/prefix length]:** 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 range of ports used by LAN PCs to access external network.

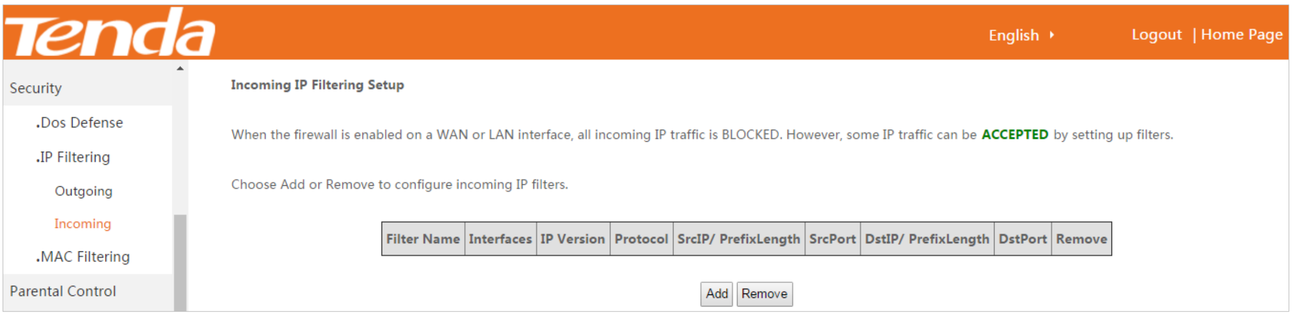
Step 9 Click **Apply/Save**.

--End

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 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.



Incoming IP Filtering Setup

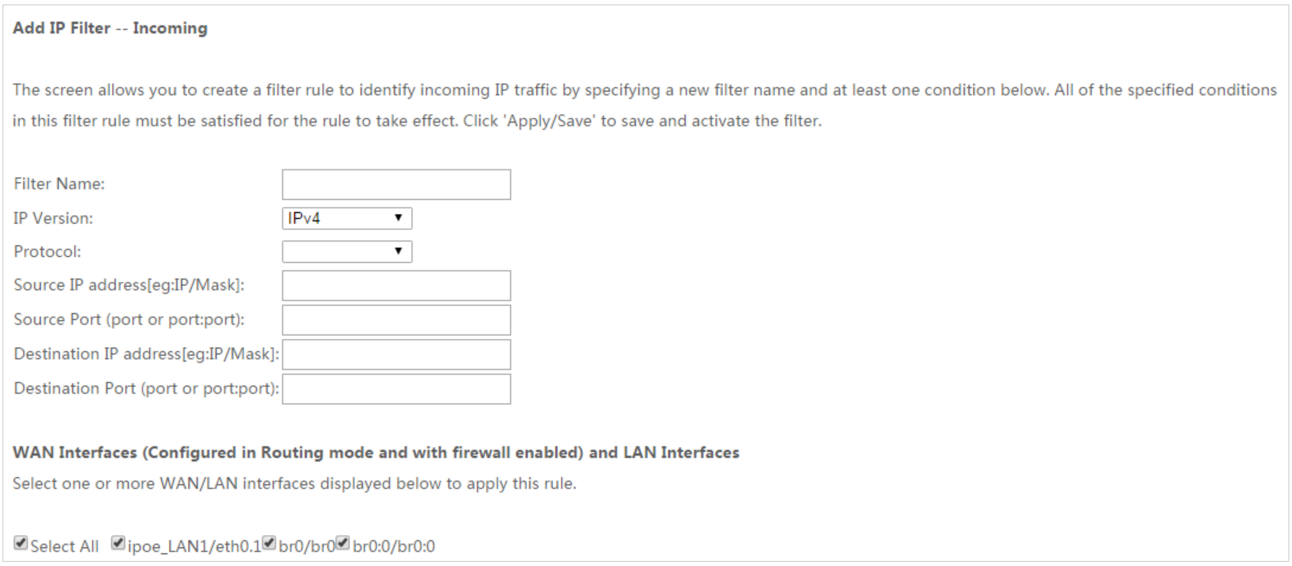
When the firewall is enabled on a WAN or LAN interface, all incoming IP traffic is BLOCKED. However, some IP traffic can be **ACCEPTED** by setting up filters.

Choose Add or Remove to configure incoming IP filters.

Filter Name	Interfaces	IP Version	Protocol	SrcIP/ PrefixLength	SrcPort	DstIP/ PrefixLength	DstPort	Remove

To configure the Outgoing function, perform the following procedure:

Step 1 Click **Add**.



Add IP Filter -- Incoming

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

Filter Name:

IP Version: IPv4

Protocol:

Source IP address[eg:IP/Mask]:

Source Port (port or port:port):

Destination IP address[eg:IP/Mask]:

Destination Port (port or port:port):

WAN Interfaces (Configured in Routing mode and with firewall enabled) and LAN Interfaces

Select one or more WAN/LAN interfaces displayed below to apply this rule.

☑Select All ☑ipoe_LAN1/eth0.1☑br0/br0☑br0:0/br0:0

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

Step 3 **IP Version:** Select your IP protocol, IPv4 or IPv6.

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

Step 5 **Source IP address [/prefix length]:** Enter the internal IP address [/prefix length] 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 [/prefix length]:** Specify the internal network IP address [/prefix length] to be accessed by the specified PCs from external network.

Step 8 **Destination Port** (port or port:port)**:** Specify a port number or a range of ports used by PCs from external network to access your internal network.

Step 9 Click **Apply/Save**.

--End

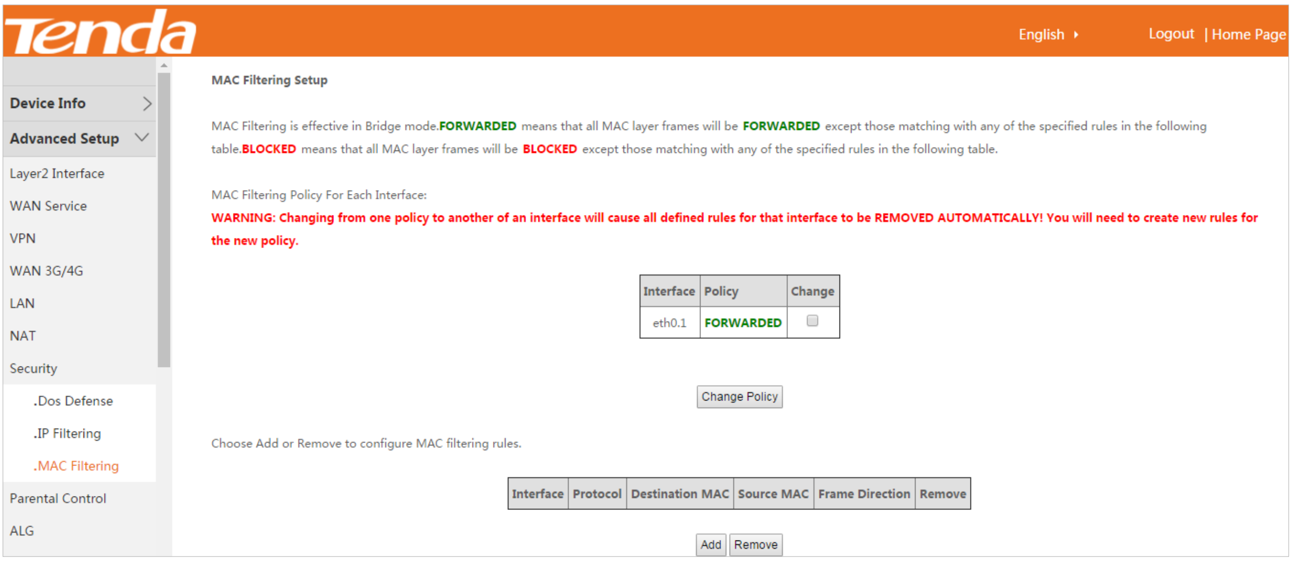
4.7.3 MAC Filtering

The MAC filtering is effective only when you create a Bridging WAN service. There are two policies of the function:

FORWARDED indicates that all MAC layer frames will be FORWARDED except those matching with any of the specified rules in the following table.

BLOCKED indicates that all MAC layer frames will be BLOCKED except those matching with any of the specified rules in the following table.

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



MAC Filtering Setup

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

MAC Filtering Policy For Each Interface:

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

Interface	Policy	Change
eth0.1	FORWARDED	□

Choose Add or Remove to configure MAC filtering rules.

Interface	Protocol	Destination MAC	Source MAC	Frame Direction	Remove

To add a FORWARDED rule, perform the following procedure:

Step 1 Click **Add**.

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

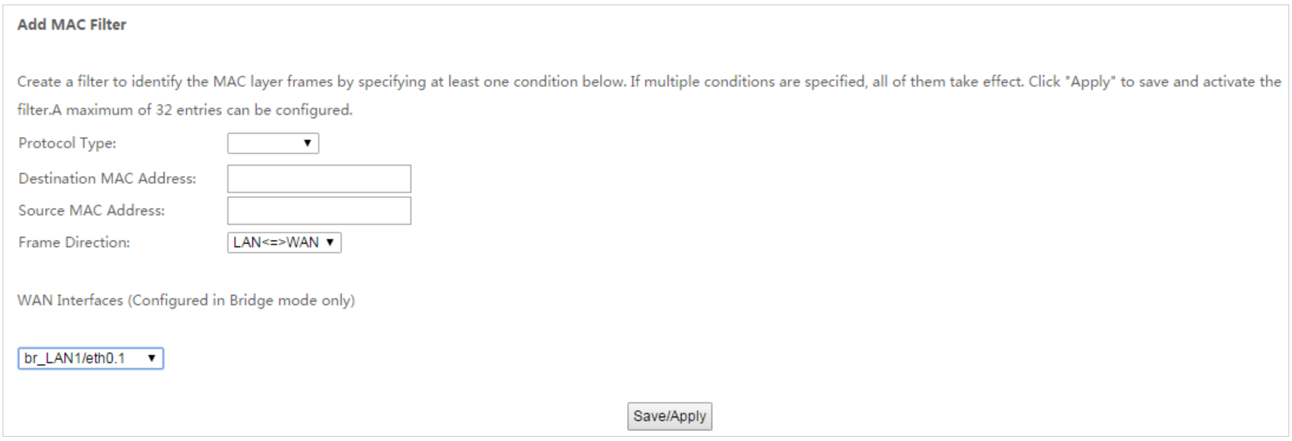
Step 3 **Destination MAC Address:** Enter the destination MAC address apply the MAC filtering rule to which you wish to apply the MAC filtering rule.

Step 4 **Source MAC Address:** Enter the source MAC address to which you wish 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**.



Add MAC Filter

Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click "Apply" to save and activate the filter.A maximum of 32 entries can be configured.

Protocol Type:

Destination MAC Address:

Source MAC Address:

Frame Direction: LAN<=>WAN

WAN Interfaces (Configured in Bridge mode only)

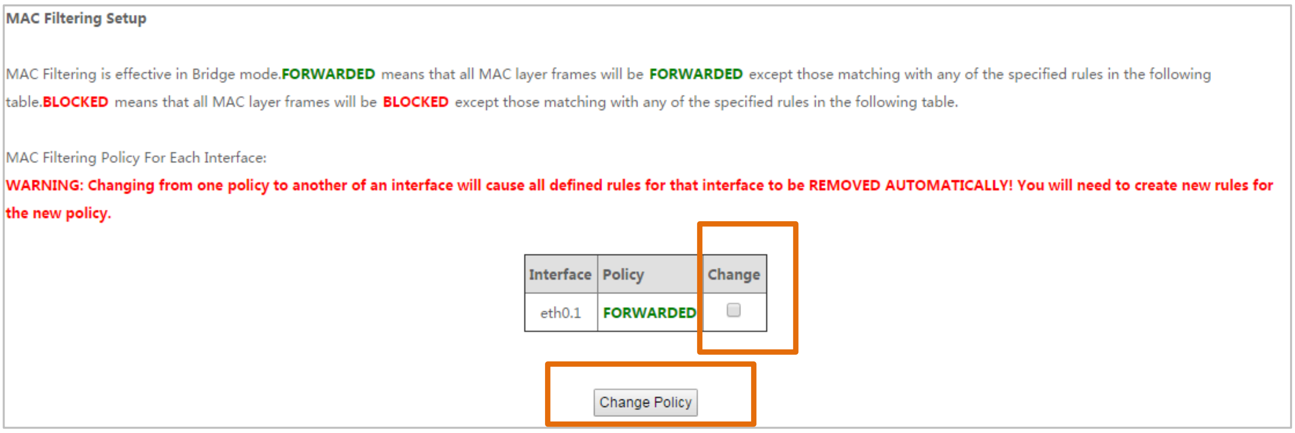
br_LAN1/eth0.1

--End

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

Step 1 Select **Change** box.

Step 2 Click **Change Policy**.



MAC Filtering Setup

MAC Filtering is effective in Bridge mode.**FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table.**BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching with any of the specified rules in the following table.

MAC Filtering Policy For Each Interface:

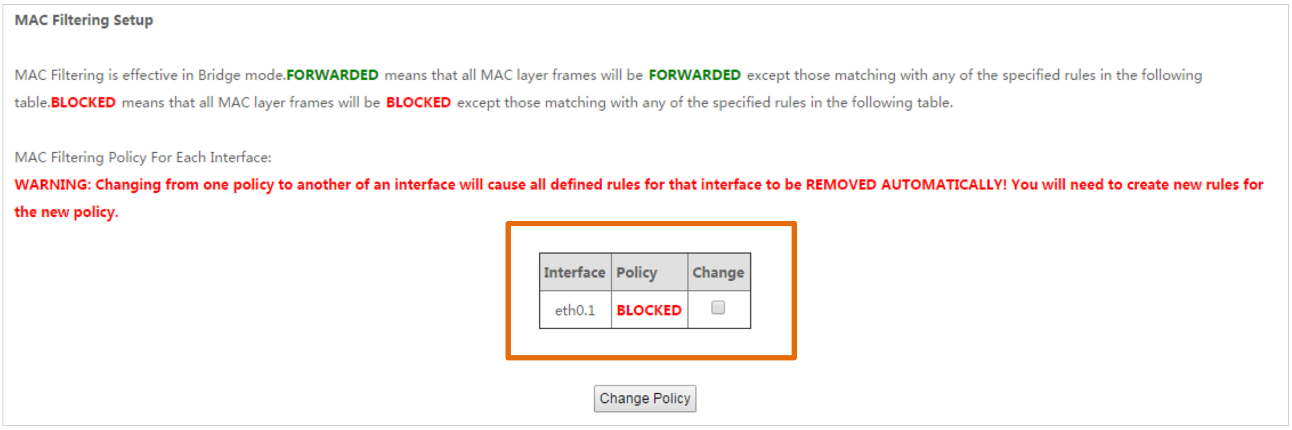
WARNING: Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.

Interface	Policy	Change
eth0.1	FORWARDED	□

--End

Verification

The policy is change to **BLOCKED**.



MAC Filtering Setup

MAC Filtering is effective in Bridge mode.**FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table.**BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching with any of the specified rules in the following table.

MAC Filtering Policy For Each Interface:

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

Interface	Policy	Change
eth0.1	BLOCKED	□

To add a BLOCKED rule, perform the following procedure:

Step 1 Change the policy to **BLOCKED**.

Step 2 Click **Add**.

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

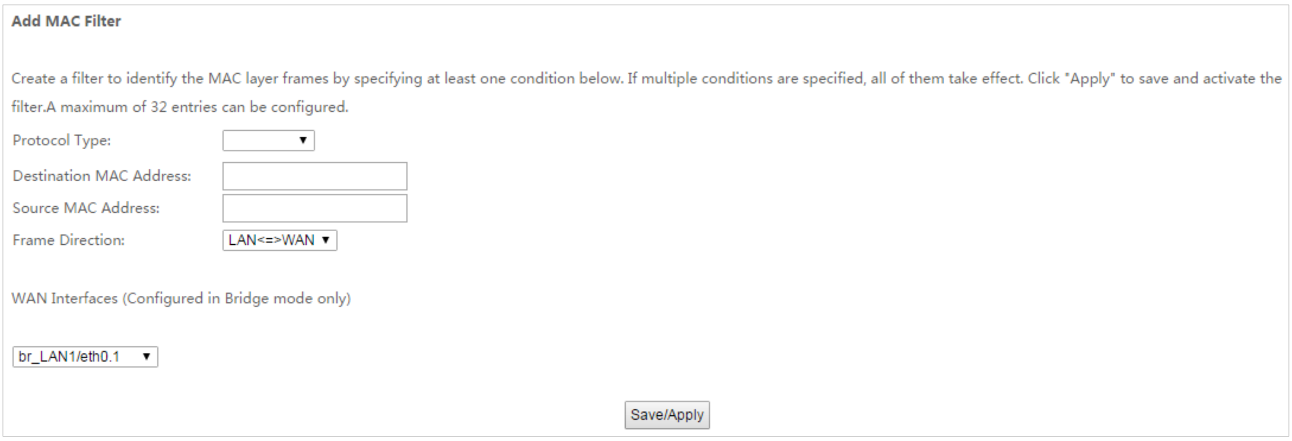
Step 4 **Destination MAC Address:** Enter the destination MAC address apply the MAC filtering rule to which you wish to apply the MAC filtering rule.

Step 5 **Source MAC Address:** Enter the source MAC address to which you wish 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**.



Add MAC Filter

Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click "Apply" to save and activate the filter.A maximum of 32 entries can be configured.

Protocol Type:

Destination MAC Address:

Source MAC Address:

Frame Direction: LAN<=>WAN

WAN Interfaces (Configured in Bridge mode only)

br_LAN1/eth0.1

--End

4.8 Parental Control

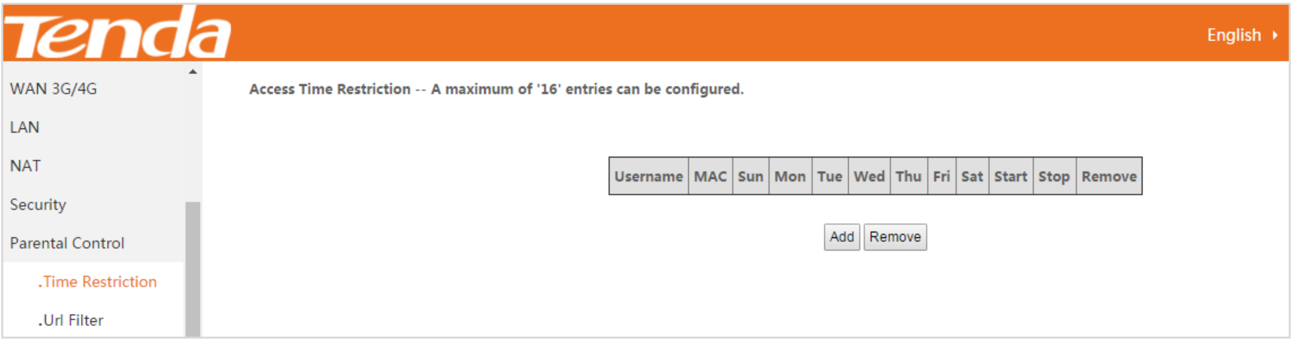
This function enables you to control internet connectivity availability and content accessibility for devices connected to the router, ensuring healthy internet usage.

4.8.1 Time Restriction

Time Restriction adds time of day restriction to a special LAN device connected to the modem Router.

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

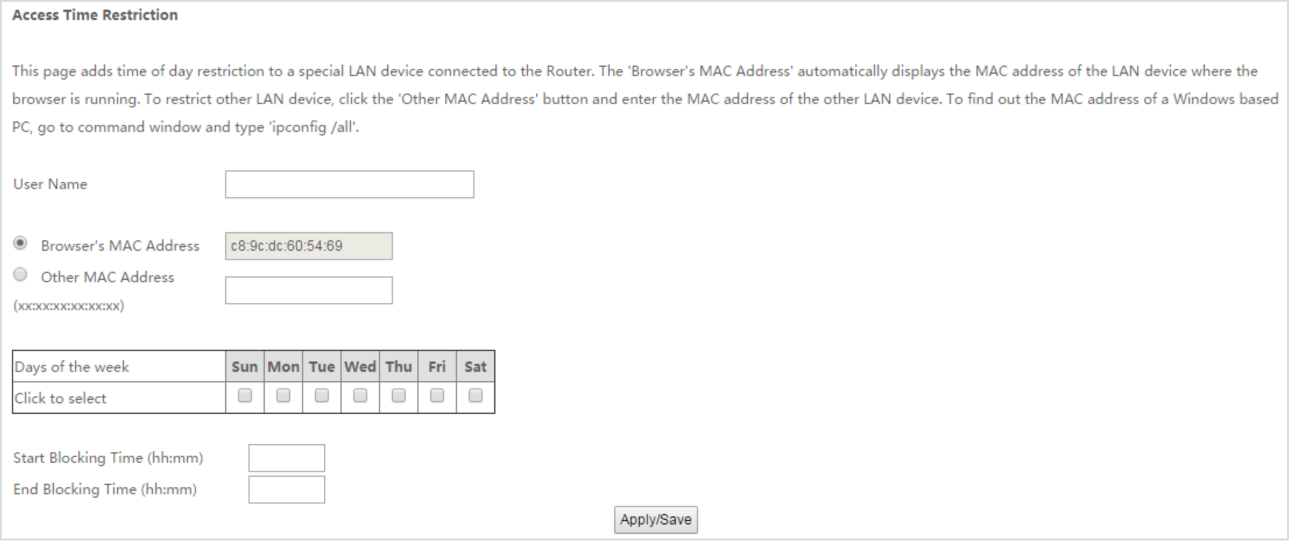
Choose **Advanced** >**Advanced Setup** > **Parental Control** >**Time Restriction** to enter the configuration page.



Access Time Restriction -- A maximum of '16' entries can be configured.

Username	MAC	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Start	Stop	Remove

Step 1 Click **Add**.



Access Time Restriction

This page adds time of day restriction to a special LAN device connected to the Router. The 'Browser's MAC Address' automatically displays the MAC address of the LAN device where the browser is running. To restrict other LAN device, click the 'Other MAC Address' button and enter the MAC address of the other LAN device. To find out the MAC address of a Windows based PC, go to command window and type 'ipconfig /all'.

User Name

● Browser's MAC Address c8:9c:dc:60:54:69

○ Other MAC Address

(xx:xx:xx:xx:xx:xx)

Days of the week	Sun	Mon	Tue	Wed	Thu	Fri	Sat
Click to select	□	□	□	□	□	□	□

Start Blocking Time (hh:mm)

End Blocking Time (hh:mm)

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

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

Step 4 **Days of week**: Click to select the days of the 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 time length of the day, this LAN device is blocked from internet. For example, if you set **start Blocking Time** to *23:00*, and **End Blocking Time** to *06:00*, the device this rule is applied for cannot access the internet during 23:00~06:00.

Step 6 Click **Apply/Save**.

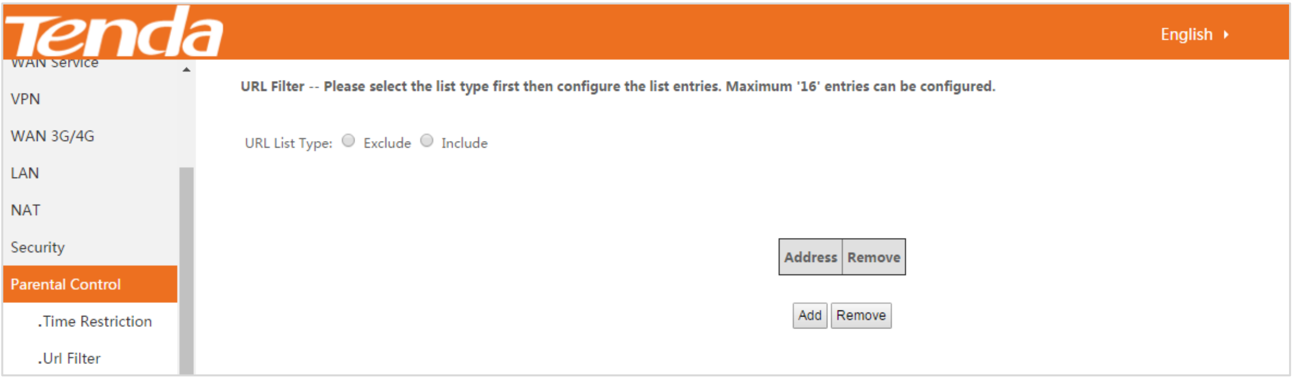
--End

4.8.2 URL Filter

URL Filter adds specific URL restrictions to a special LAN device

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

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



URL Filter -- Please select the list type first then configure the list entries. Maximum '16' entries can be configured.

URL List Type: ○ Exclude ○ Include

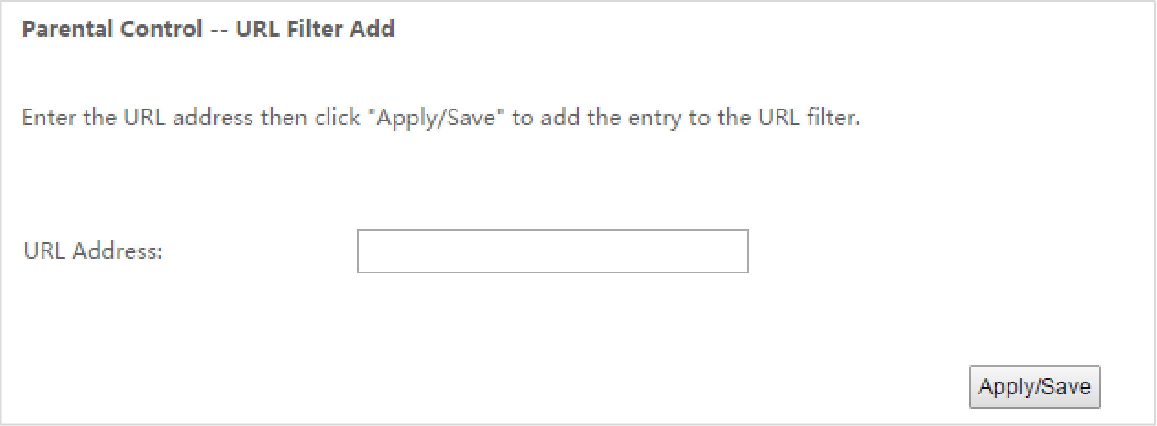
Step 1 Select **Exclude** or **Include**.

- **Exclude** indicates that the URLs added to the list are not allowed to visit.
- **Include** indicates that only the URLs added to the list are allowed to visit.

Step 2 Click **Add**.

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

Step 4 Click **Apply/Save**.



Parental Control -- URL Filter Add

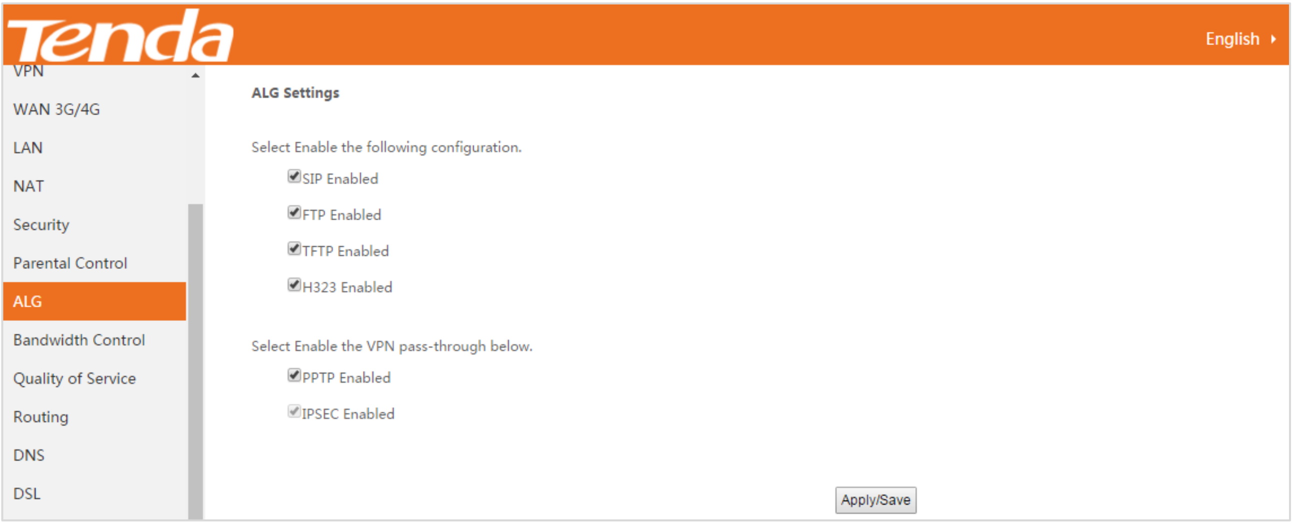
Enter the URL address then click "Apply/Save" to add the entry to the URL filter.

URL Address:

--End

4.9 ALG

ALG allows you to enable some configurations.



ALG Settings

Select Enable the following configuration.

☑ SIP Enabled

☑ FTP Enabled

☑ TFTP Enabled

☑ H323 Enabled

Select Enable the VPN pass-through below.

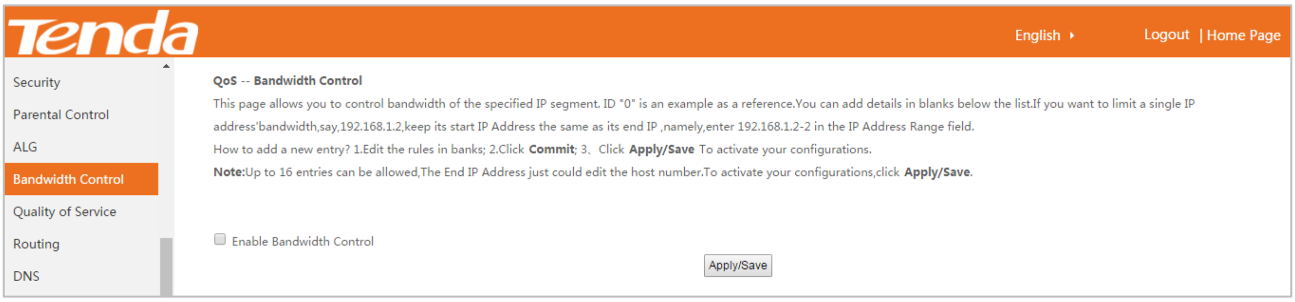
☑ PPTP Enabled

☑ IPSEC Enabled

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.



QoS -- Bandwidth Control

This page allows you to control bandwidth of the specified IP segment. ID "0" is an example as a reference.You can add details in blanks below the list.If you want to limit a single IP address'bandwidth,say,192.168.1.2,keep its start IP Address the same as its end IP ,namely,enter 192.168.1.2-2 in the IP Address Range field.

How to add a new entry? 1.Edit the rules in banks; 2.Click **Commit**; 3、 Click **Apply/Save** To activate your configurations.

Note: Up to 16 entries can be allowed,The End IP Address just could edit the host number.To activate your configurations,click **Apply/Save**.

□ Enable Bandwidth Control

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.

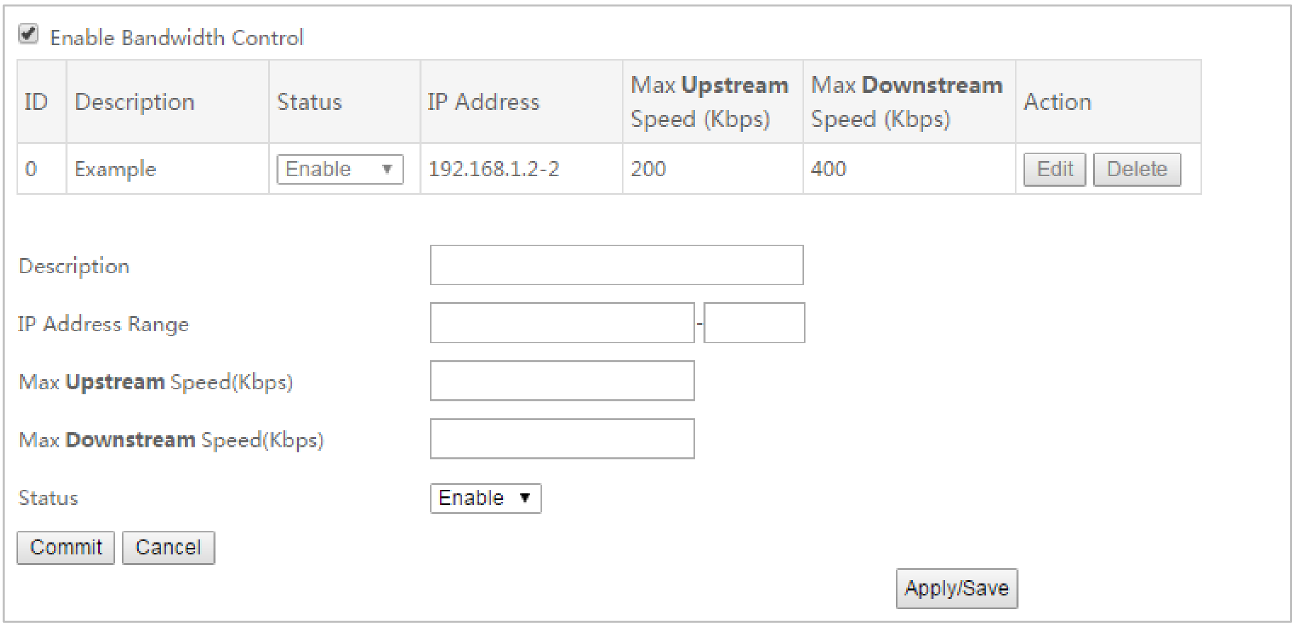
Step 4 Specify a maximum upstream and downstream speed.

Step 5 Select the status for the rule.

- **Enable**: When the Enable is selected, the rule takes effect.
- **Disable**: When the 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.



☑ Enable Bandwidth Control

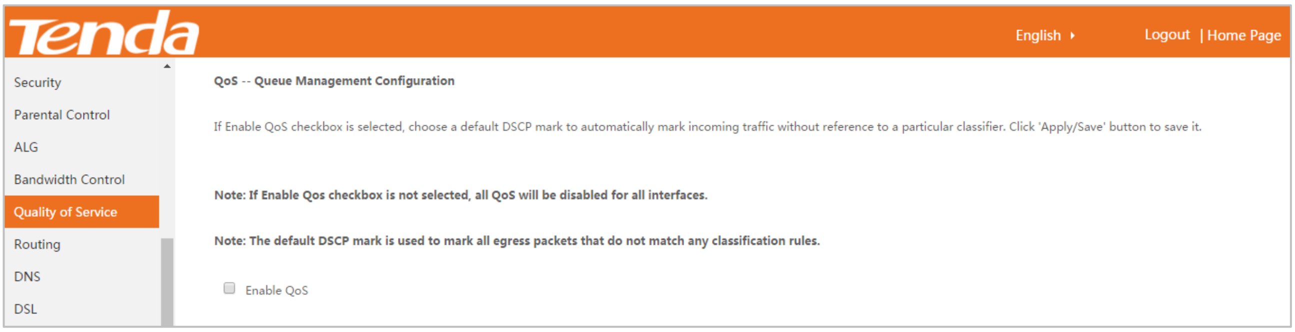
ID	Description	Status	IP Address	Max **Upstream** Speed (Kbps)	Max **Downstream** Speed (Kbps)	Action
0	Example	Enable ▼	192.168.1.2-2	200	400	Edit Delete

Description	
IP Address Range	-
Max **Upstream** Speed(Kbps)	
Max **Downstream** Speed(Kbps)	
Status	Enable ▼

--End

4.11 Quality of Service

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



QoS -- Queue Management Configuration

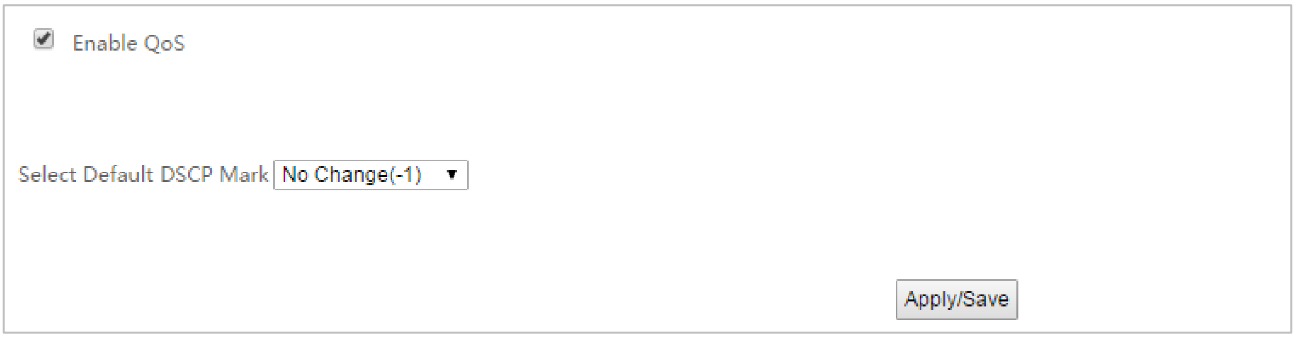
If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Click 'Apply/Save' button to save it.

Note: If Enable Qos checkbox is not selected, all QoS will be disabled for all interfaces.

Note: The default DSCP mark is used to mark all egress packets that do not match any classification rules.

□ Enable QoS

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 Default DSCP Mark: No Change(-1)

- **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.
- **No Change (-1)**: Do not tag 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.

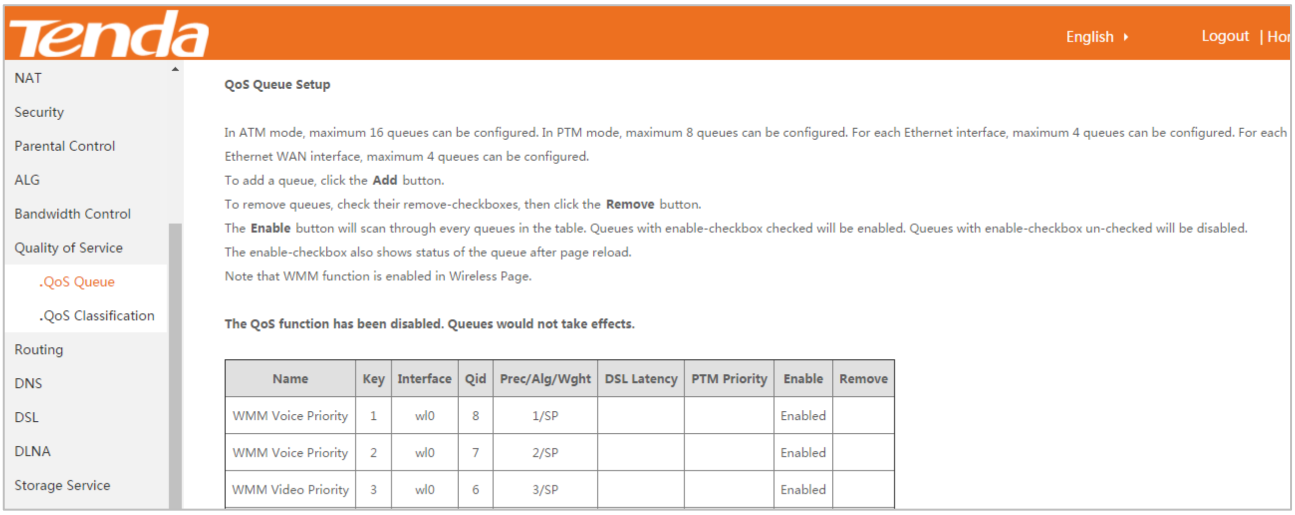
Packet-loss Priority	AF1	AF2	AF3	AF4
Low (1)	001010	010010	011010	100010
Medium (2)	001100	010100	011100	100100
High (3)	001110	010110	011110	100110

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.



QoS Queue Setup

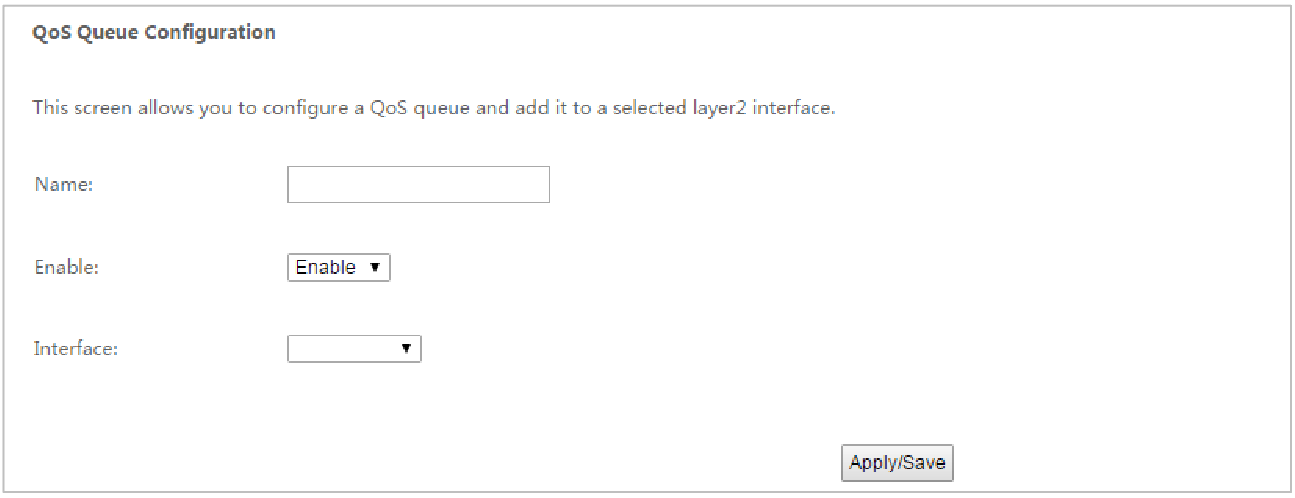
In ATM mode, maximum 16 queues can be configured. In PTM mode, maximum 8 queues can be configured. For each Ethernet interface, maximum 4 queues can be configured. For each Ethernet WAN interface, maximum 4 queues can be configured.
To add a queue, click the **Add** button.
To remove queues, check their remove-checkboxes, then click the **Remove** button.
The **Enable** button will scan through every queues in the table. Queues with enable-checkbox checked will be enabled. Queues with enable-checkbox un-checked will be disabled.
The enable-checkbox also shows status of the queue after page reload.
Note that WMM function is enabled in Wireless Page.

The QoS function has been disabled. Queues would not take effects.

Name	Key	Interface	Qid	Prec/Alg/Wght	DSL Latency	PTM Priority	Enable	Remove
WMM Voice Priority	1	wl0	8	1/SP			Enabled	
WMM Voice Priority	2	wl0	7	2/SP			Enabled	
WMM Video Priority	3	wl0	6	3/SP			Enabled	

To add a queue, perform the following procedure:

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



QoS Queue Configuration

This screen allows you to configure a QoS queue and add it to a selected layer2 interface.

Name:

Enable: Enable

Interface:

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

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

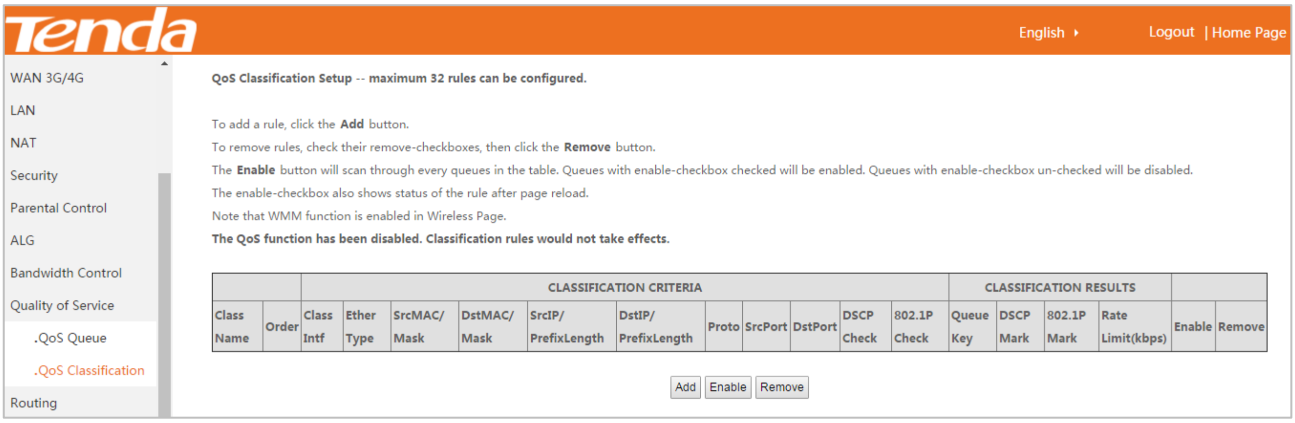
Step 4 **Interface**: Set an interface for the queue.

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.



QoS Classification Setup -- **maximum 32 rules can be configured.**

To add a rule, click the **Add** button.

To remove rules, check their remove-checkboxes, then click the **Remove** button.

The **Enable** button will scan through every queues in the table. Queues with enable-checkbox checked will be enabled. Queues with enable-checkbox un-checked will be disabled.

The enable-checkbox also shows status of the rule after page reload.

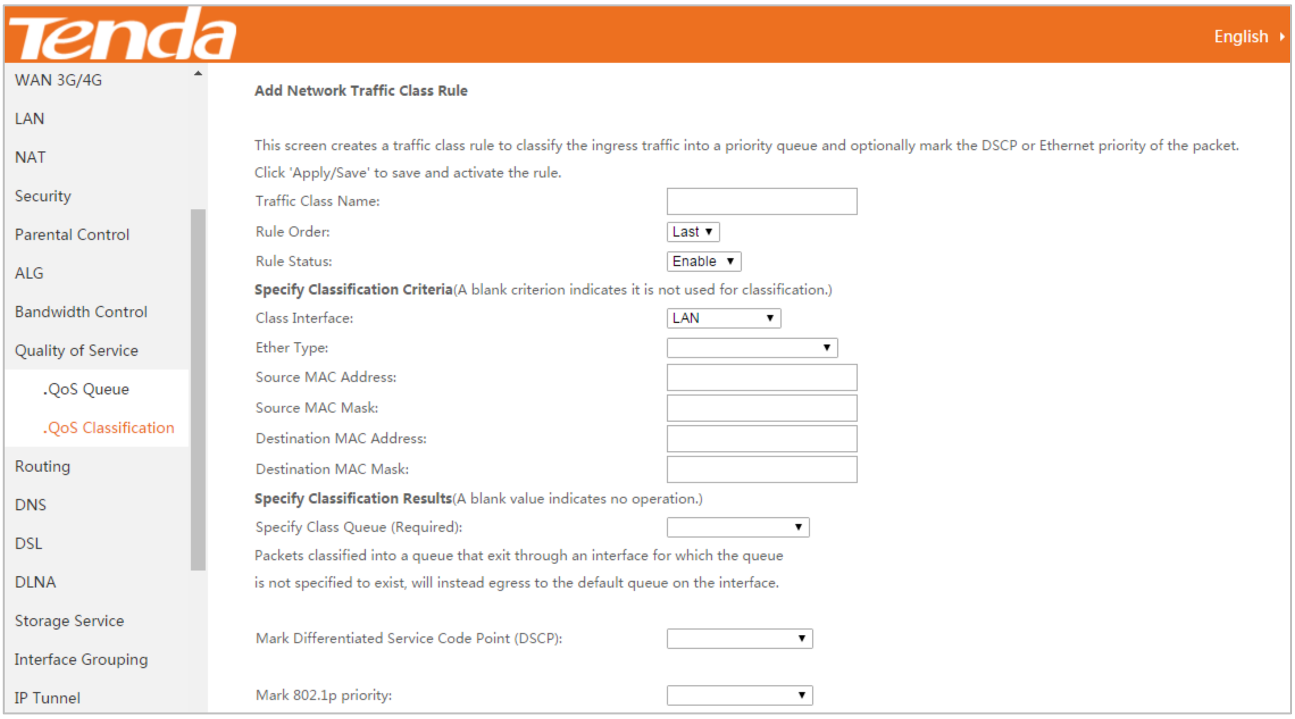
Note that WMM function is enabled in Wireless Page.

The QoS function has been disabled. Classification rules would not take effects.

		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

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

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



Add Network Traffic Class Rule

This screen creates a traffic class rule to classify the ingress traffic into a priority queue and optionally mark the DSCP or Ethernet priority of the packet.

Click 'Apply/Save' to save and activate the rule.

Traffic Class Name:

Rule Order: Last

Rule Status: Enable

Specify Classification Criteria(A blank criterion indicates it is not used for classification.)

Class Interface: LAN

Ether Type:

Source MAC Address:

Source MAC Mask:

Destination MAC Address:

Destination MAC Mask:

Specify Classification Results(A blank value indicates no operation.)

Specify Class Queue (Required):

Packets classified into a queue that exit through an interface for which the queue is not specified to exist, will instead egress to the default queue on the interface.

Mark Differentiated Service Code Point (DSCP):

Mark 802.1p priority:

Step 2 **Traffic Class Name**: Specify a name for the rule to describe the character of 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 address.
- **Source/Destination MAC Mask:** Leave them blank.

Step 6 Specify the classification results.

- **Specify Class Queue (Required)**: Specifies a queue that packets are classified into (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 it 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**.

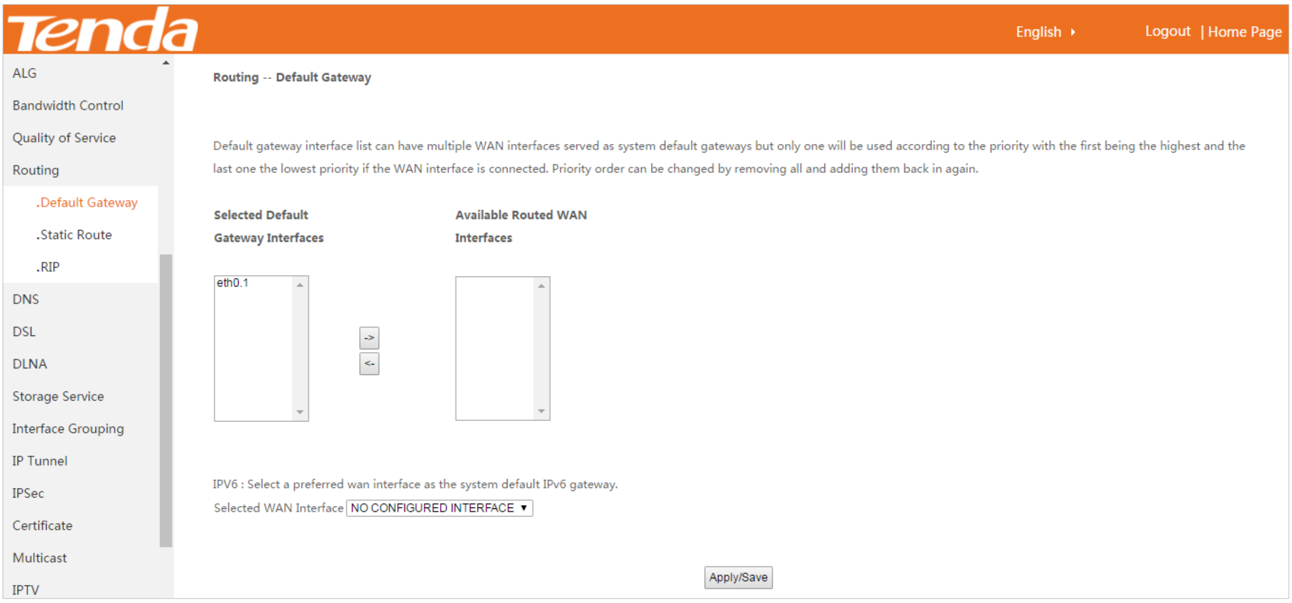
--End

4.12 Routing

4.12.1 Defauly Gateway

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

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



Routing -- Default Gateway

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

Selected Default Gateway Interfaces: eth0.1

Available Routed WAN Interfaces

IPV6 : Select a preferred wan interface as the system default IPv6 gateway.

Selected WAN Interface: NO CONFIGURED INTERFACE

Selected Default Gateway Interfaces: It specifies the current default IPv4 gateway interface in effect. 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.

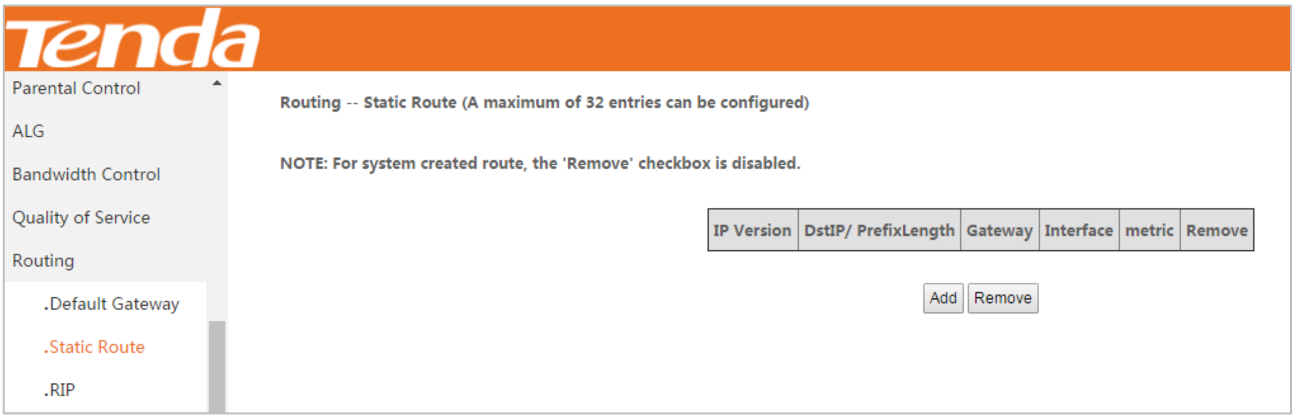
Available Routed WAN Interfaces: It Specifies the current alternative default IPv4 gateway interface. Select a WAN interface and click the <- button to add it to the **Selected Default Gateway Interfaces** box.

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 performed 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.



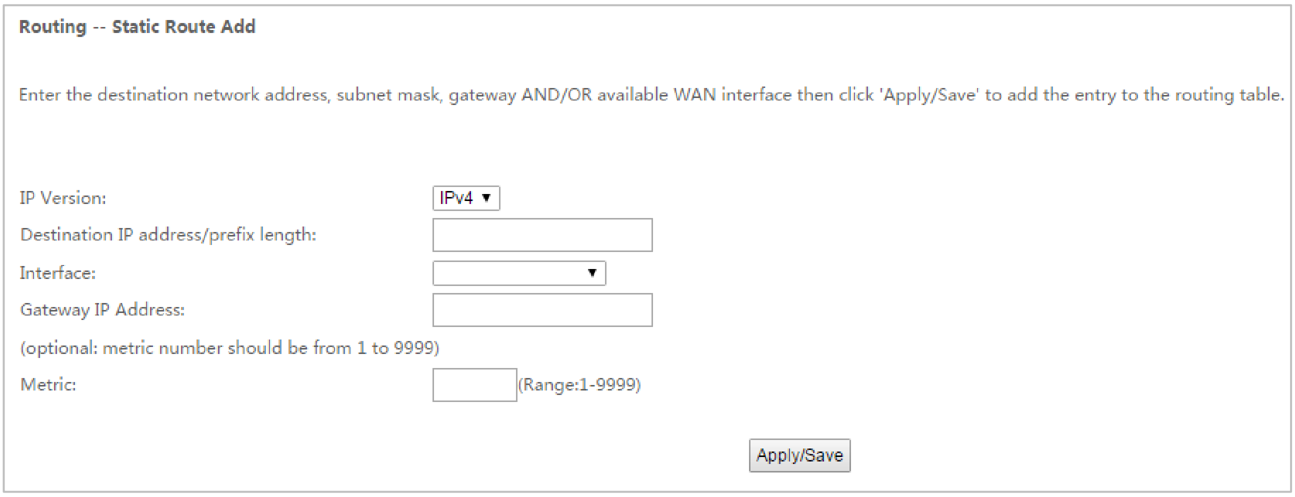
Routing -- Static Route (A maximum of 32 entries can be configured)

NOTE: For system created route, the 'Remove' checkbox is disabled.

IP Version	DstIP/ PrefixLength	Gateway	Interface	metric	Remove

To add a static route, perform the following procedure:

Step 1 Click **Add**.



Routing -- Static Route Add

Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click 'Apply/Save' to add the entry to the routing table.

IP Version: IPv4

Destination IP address/prefix length:

Interface:

Gateway IP Address:

(optional: metric number should be from 1 to 9999)

Metric: (Range:1-9999)

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

Step 3 **Destination IP address/prefix length**: Set a destination IP address.

- Destination Host is a specified host whose prefix length is 32. For example, the host 1.2.3.4 indicates “1.2.3.4/32”.
- Destination Network is a specified network whose IP address is the network address of the destination host. For example, the network 2.2.3.3/255.255.0.0 indicates “2.2.0.0/16” which represents all hosts whose IP address start with “2.2”.

Step 4 **Interface**: Specify an outgoing interface for the 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. Lower number leads to higher priority.

--End

TIP

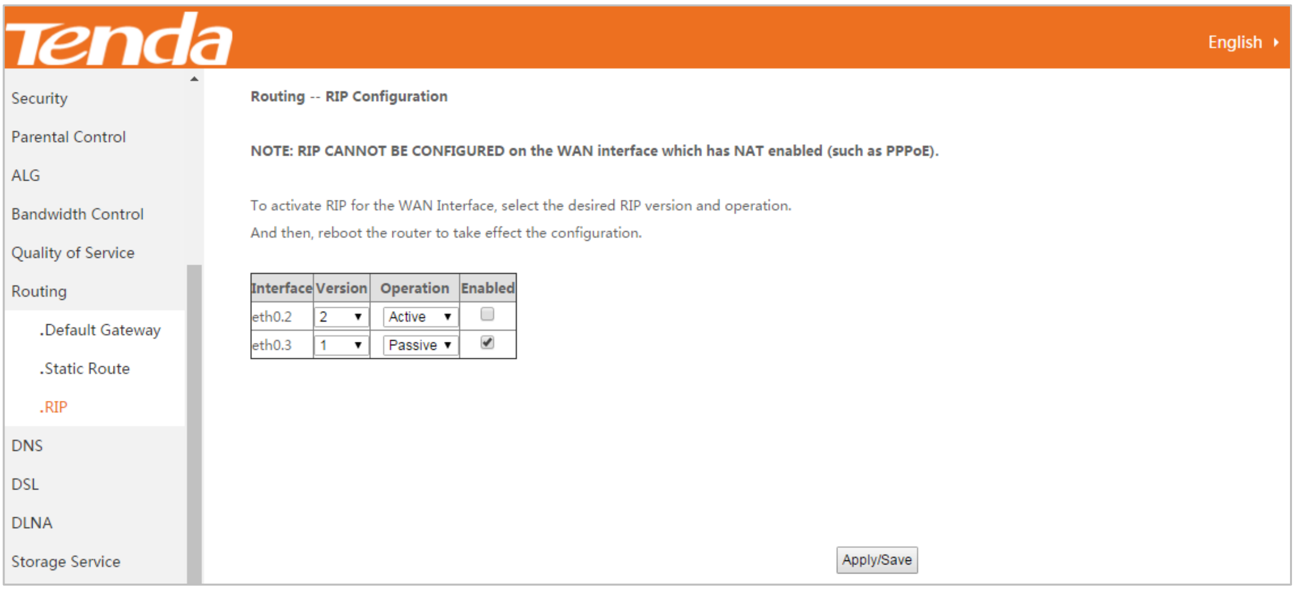
- Destination IP address cannot be in the same IP network segment as that of WAN or LAN of the modem router.

- 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. Unreasonable 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.



Routing -- RIP Configuration

NOTE: RIP CANNOT BE CONFIGURED on the WAN interface which has NAT enabled (such as PPPoE).

To activate RIP for the WAN Interface, select the desired RIP version and operation.
And then, reboot the router to take effect the configuration.

Interface	Version	Operation	Enabled
eth0.2	2	Active	☐
eth0.3	1	Passive	☑

Parameter	Description
Interface	It specifies the WAN interfaces you add in WAN service that disable NAT.
Version	It specifies two RIP versions the modem router supports: RIP 1 and RIP 2. RIP 1: The periodic routing updates do not carry subnet information. RIP 2: It included the ability to carry subnet information.
Operation	Active: The WAN interface sends and receives RIP packets. 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 interface that disables NAT is displayed in the list.
- After configuration, reboot the modem router to take effect the settings.

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.

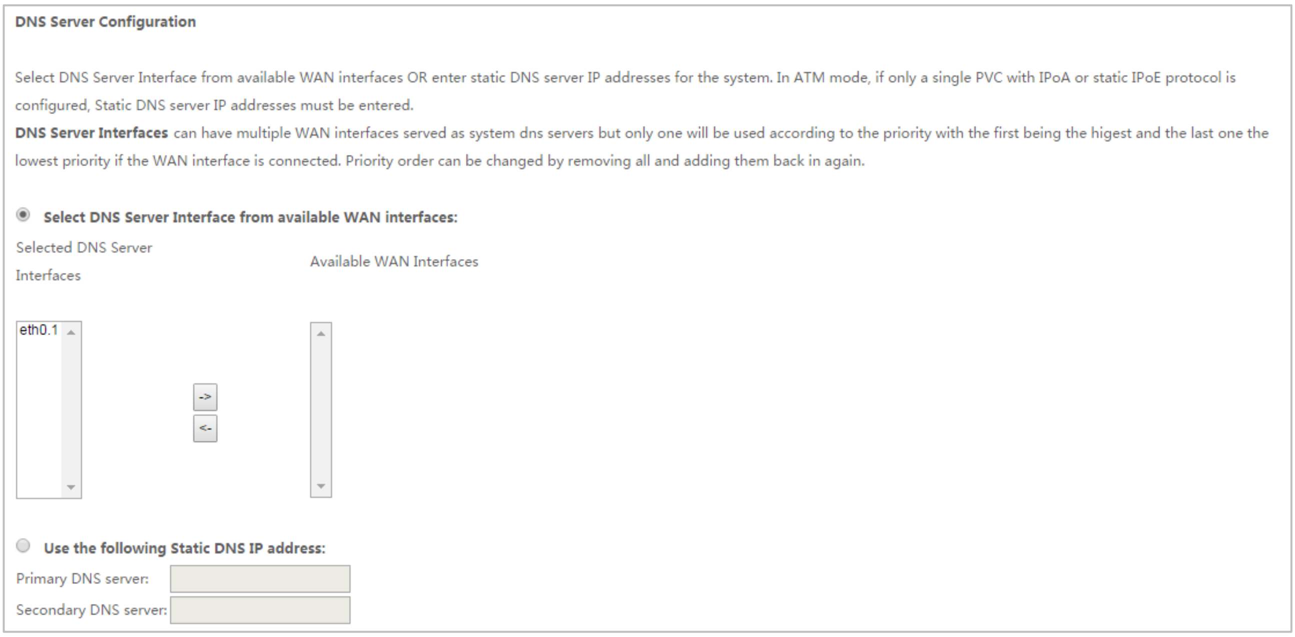
Choose **Advanced** > **Advanced Setup** > **DNS** > **DNS Server** to enter the configuration page.

For IPv4:

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

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

And then click **Apply/Save**.



DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

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

● **Select DNS Server Interface from available WAN interfaces:**

Selected DNS Server Interfaces: eth0.1

Available WAN Interfaces

○ **Use the following Static DNS IP address:**

Primary DNS server:

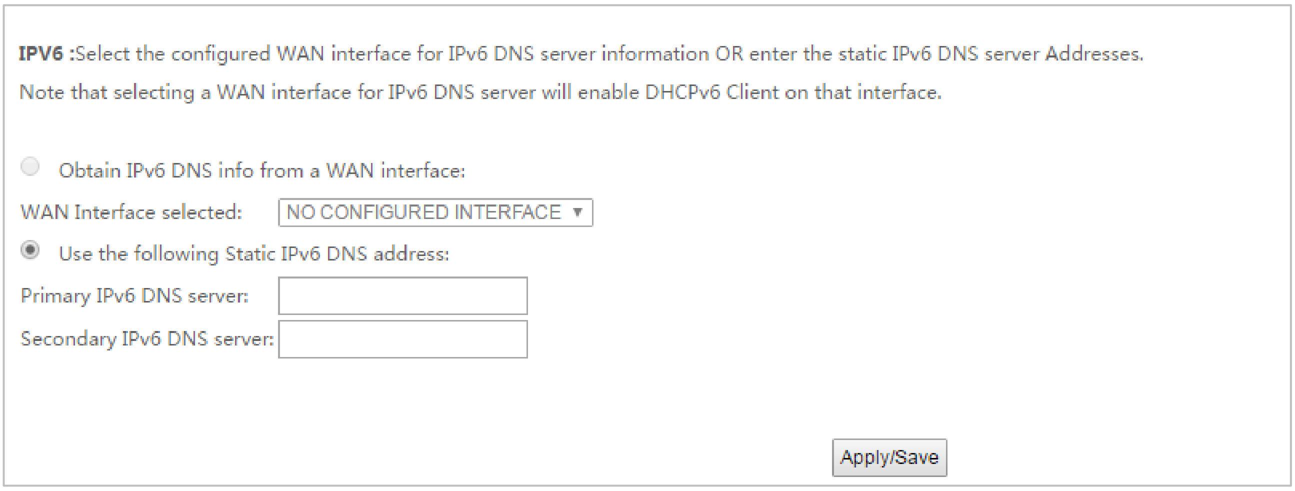
Secondary DNS server:

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**.



IPV6 :Select the configured WAN interface for IPv6 DNS server information OR enter the static IPv6 DNS server Addresses.

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

○ Obtain IPv6 DNS info from a WAN interface:

WAN Interface selected: NO CONFIGURED INTERFACE

● Use the following Static IPv6 DNS address:

Primary IPv6 DNS server:

Secondary IPv6 DNS server:

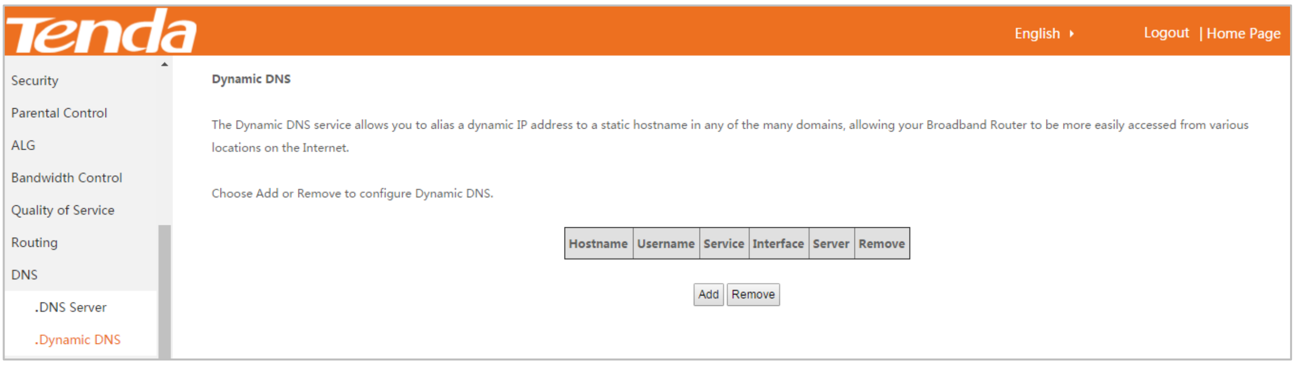
NOTE

- DNS Server Interfaces can have multiple WAN interfaces served as system DNS servers but only one is used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.
- In ATM mode, if only single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.
- If you cannot locate the static DNS server IP information, ask your ISP to provide it.
- The default settings are recommended if you are unsure about the DNS server addresses. If a wrong DNS server address is configured, webpages may not be open.

4.13.2 Dynamic DNS

DDNS maps the WAN IP address (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.



Dynamic DNS

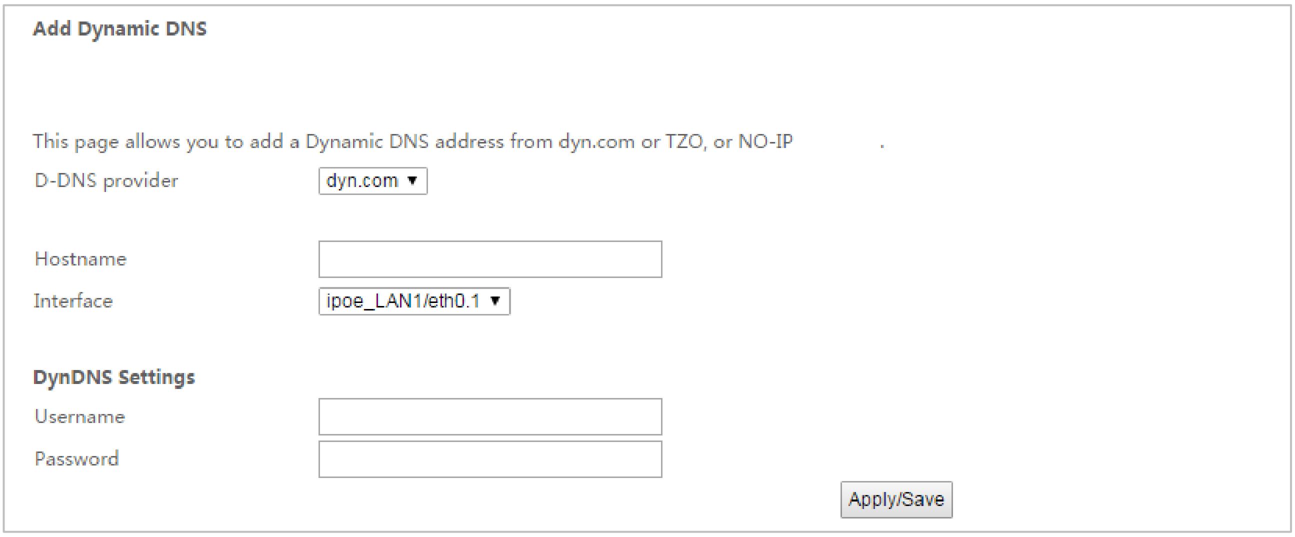
The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your Broadband Router to be more easily accessed from various locations on the Internet.

Choose Add or Remove to configure Dynamic DNS.

Hostname	Username	Service	Interface	Server	Remove

To configure the dynamic DNS function, perform the following procedure:

Step 1 Click **Add**.


Add Dynamic DNS

This page allows you to add a Dynamic DNS address from dyn.com or TZO, or NO-IP .

D-DNS provider: dyn.com ▼

Hostname:

Interface: ipoe_LAN1/eth0.1 ▼

DynDNS Settings

Username:

Password:

Step 2 **D-DNS provider**: Specify a DDNS service provider. The supported service providers include dyndns.org, oray.com.

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

Step 4 **Interface**: Specify a WAN connection interface.

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.

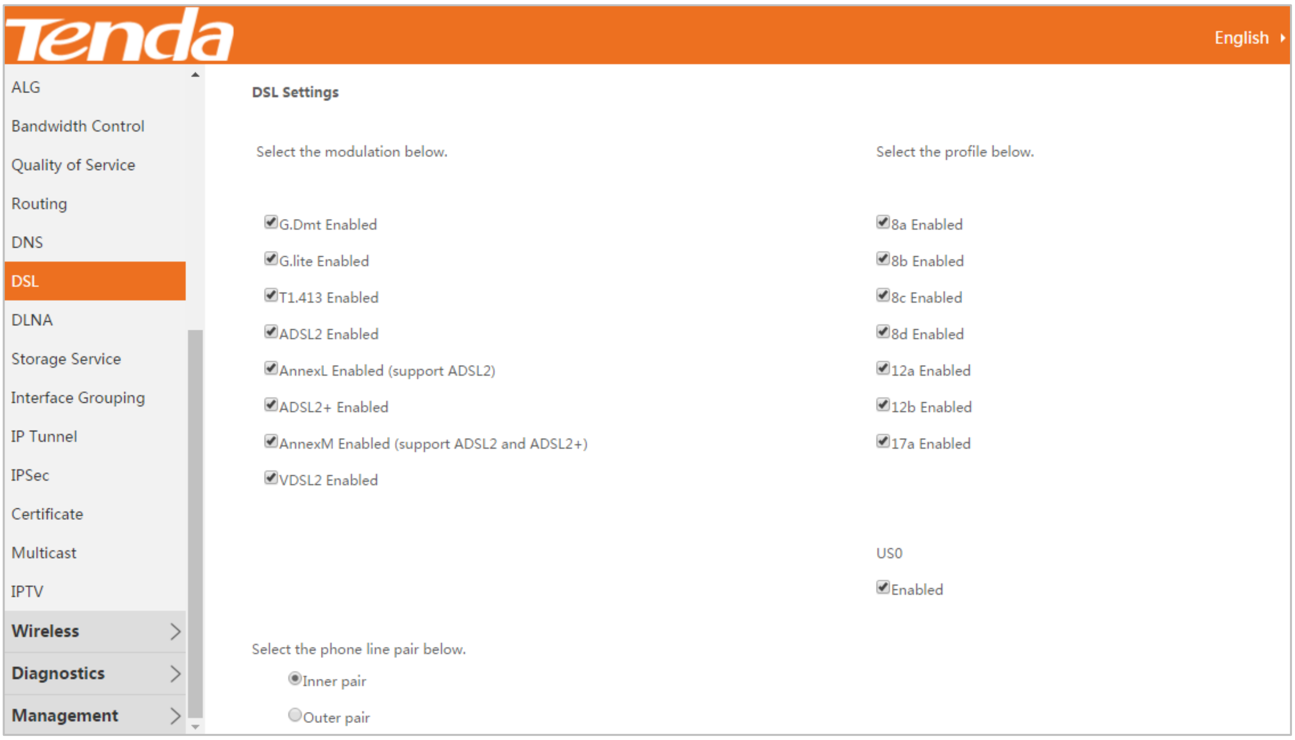
Step 6 Click **Apply/Save**.

--End

4.14 DSL

DSL parameter configurations must be supported by ISP to take effect. Actual parameters (refer to Statistics-xDSL) resulted from the negotiation between your router and ISP. Wrong configurations may fail your Internet access. The best DSL configurations are the factory defaults. Only change them if you are instructed by your ISP or our technical staff when your modem router fails to negotiate with ISP in DSL (ATM) mode. Usually, this failure can be identified and confirmed if the ADSL LED on the device keeps displaying a slow or quick blinking light.

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



DSL Settings

Select the modulation below.

- ☑G.Dmt Enabled
- ☑G.lite Enabled
- ☑T1.413 Enabled
- ☑ADSL2 Enabled
- ☑AnnexL Enabled (support ADSL2)
- ☑ADSL2+ Enabled
- ☑AnnexM Enabled (support ADSL2 and ADSL2+)
- ☑VDSL2 Enabled

Select the profile below.

- ☑8a Enabled
- ☑8b Enabled
- ☑8c Enabled
- ☑8d Enabled
- ☑12a Enabled
- ☑12b Enabled
- ☑17a Enabled

US0

☑Enabled

Select the phone line pair below.

●Inner pair

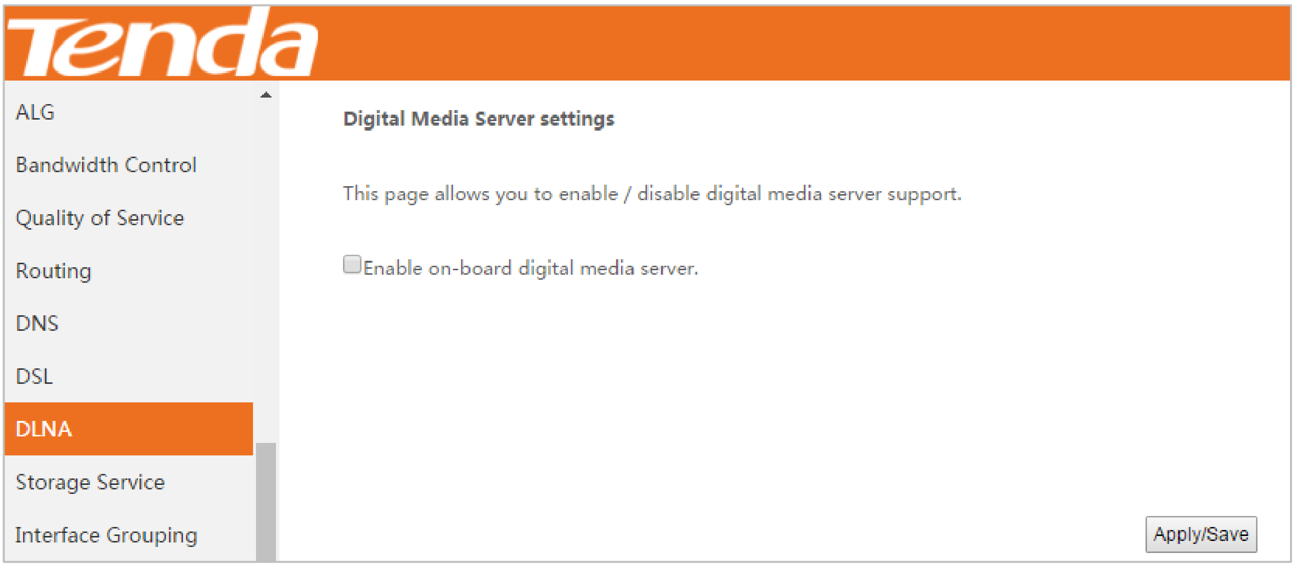
○Outer pair

Parameter	Description
G.Dmt	It specifies G992.1. The maximum uploading/downloading rate is 1.3 Mbps/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	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	Compatible with the upstreaming bandwidth extension mode, and based on G992.3 ADSL2 and G992.5 ADSL2+, the uploading rate of this mode increases to 2Mbps for ADSL2+ from 1 Mbps for ADSL2. 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. For example, you can use the mobile phone and the DLNA controller to enable your TV or computer to play the video and audio clips and display the images in your portable disk.

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



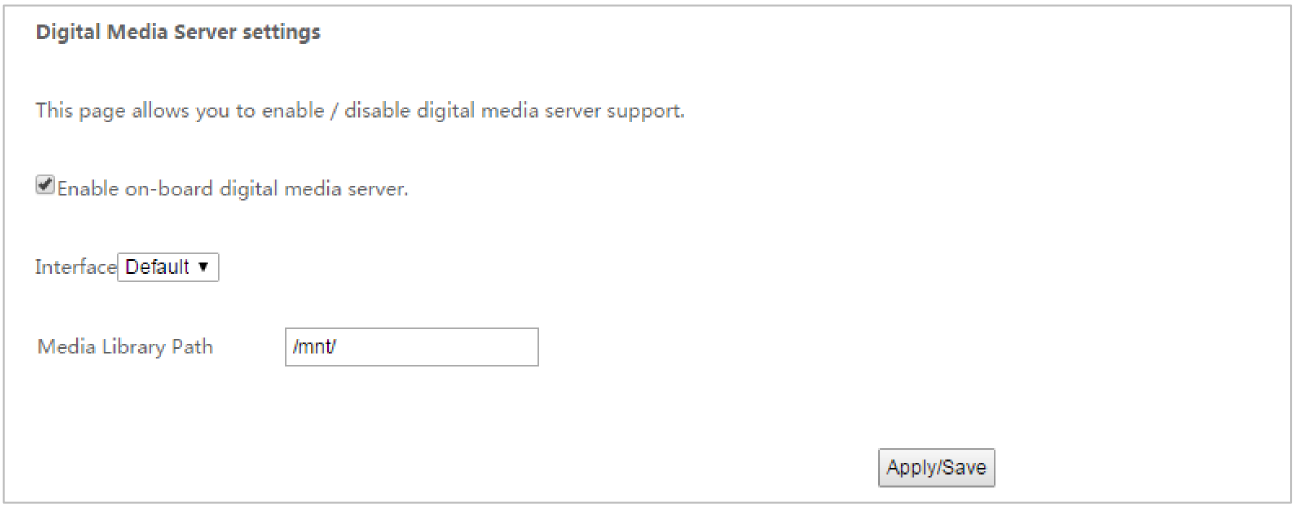
Digital Media Server settings

This page allows you to enable / disable digital media server support.

□Enable on-board digital media server.

To configure the DLNA function, perform the following procedure:

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



Digital Media Server settings

This page allows you to enable / disable digital media server support.

☑Enable on-board digital media server.

Interface Default ▾

Media Library Path /mnt/

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 the resources in the USB storage device attached to the modem router can be played.

Step 4 Click **Apply/Save**.

--End

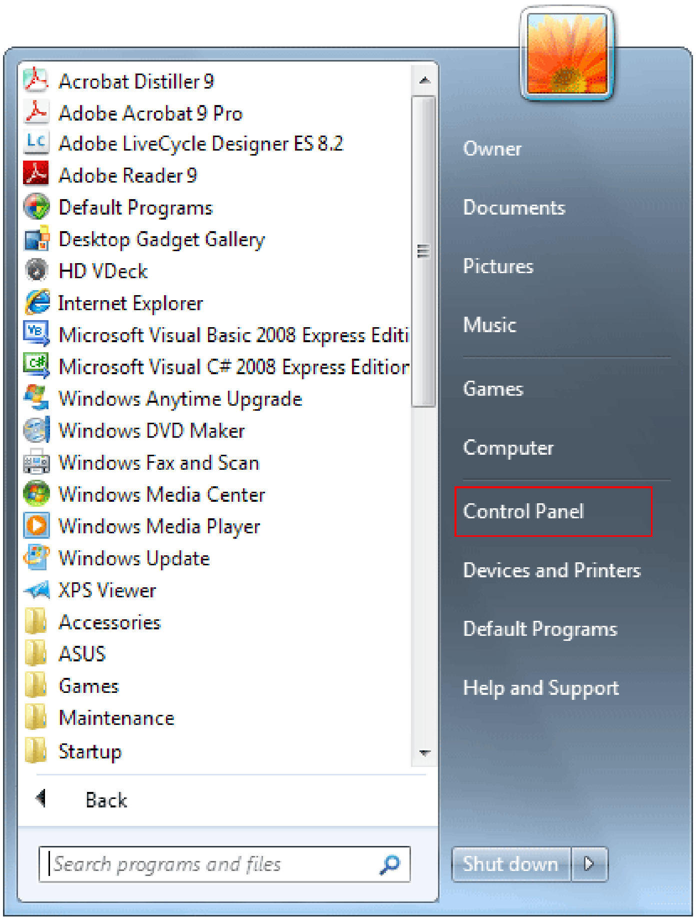
Application Scenario

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.

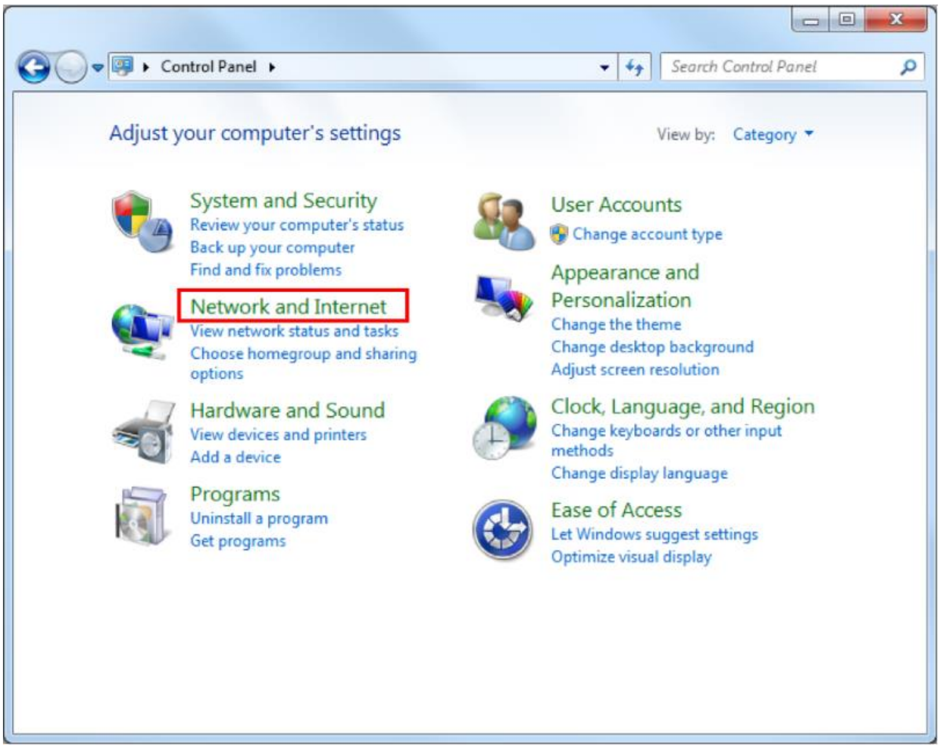
Sharing videos, audios, and images: (A computer running Windows 7 is taken as an example to describe the procedure.)

Step 1 Enable the media streaming function.

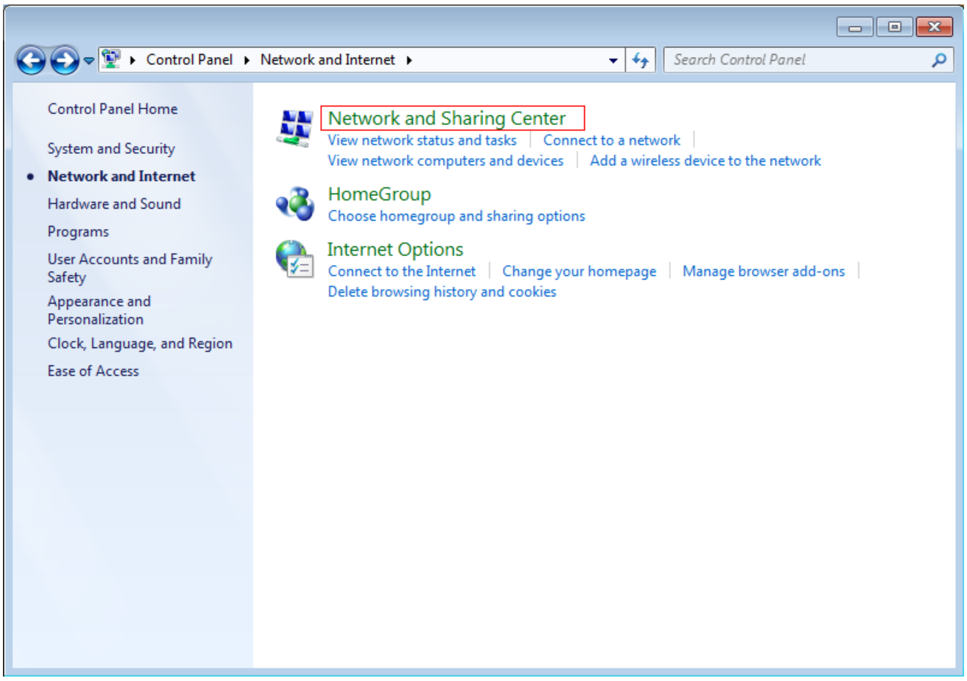
Click **Start** in the lower-left corner of the desktop and choose **Control Panel**.



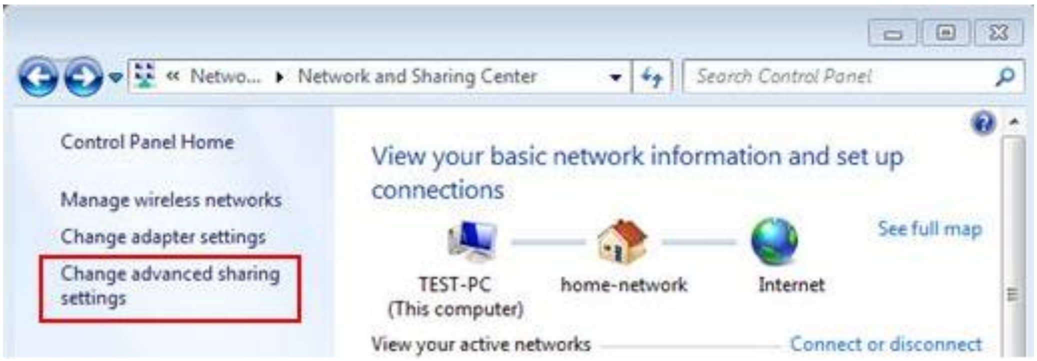
Click **Network and Internet**.



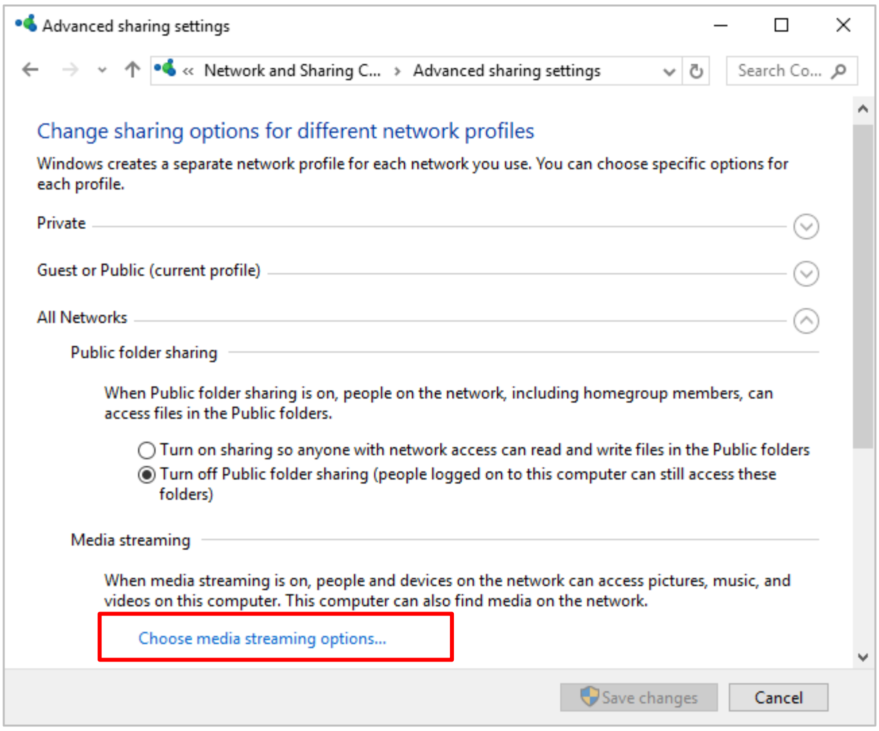
Click **Network and Sharing Center**.


Control Panel ▸ Network and Internet ▸
Search Control Panel
Control Panel Home
System and Security
Network and Internet
Hardware and Sound
Programs
User Accounts and Family Safety
Appearance and Personalization
Clock, Language, and Region
Ease of Access
Network and Sharing Center
View network status and tasks
Connect to a network
View network computers and devices
Add a wireless device to the network
HomeGroup
Choose homegroup and sharing options
Internet Options
Connect to the Internet
Change your homepage
Manage browser add-ons
Delete browsing history and cookies

Click **Change advanced sharing settings**.



Click **Choose media streaming options…**.


Advanced sharing settings
« Network and Sharing C... › Advanced sharing settings
Search Co...

Change sharing options for different network profiles

Windows creates a separate network profile for each network you use. You can choose specific options for each profile.

Private

Guest or Public (current profile)

All Networks

Public folder sharing

When Public folder sharing is on, people on the network, including homegroup members, can access files in the Public folders.

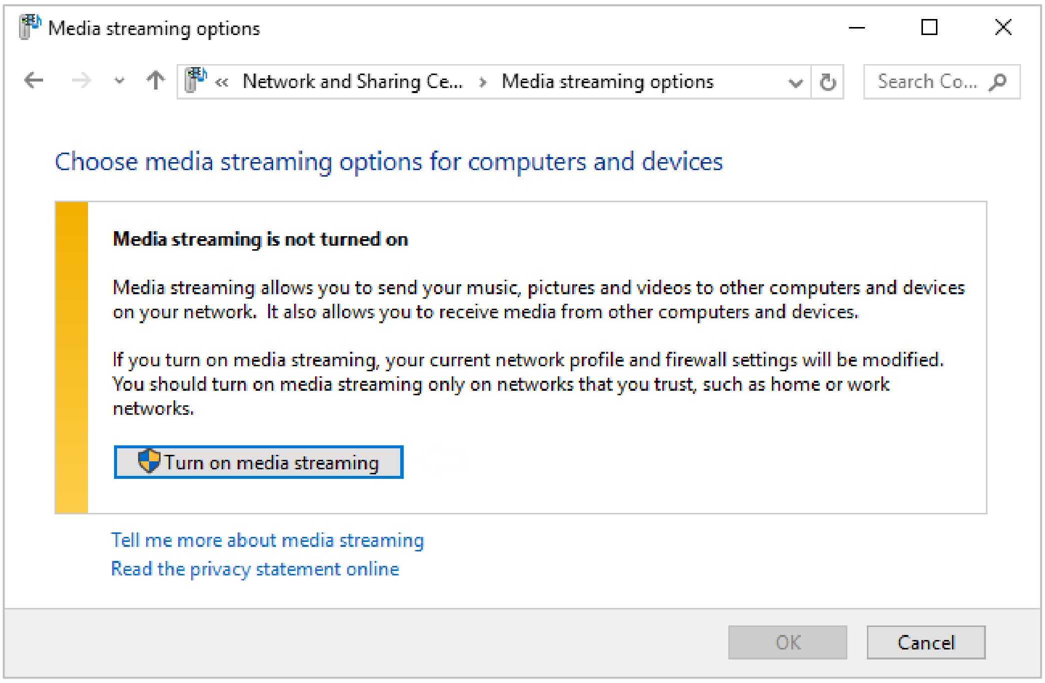
○ Turn on sharing so anyone with network access can read and write files in the Public folders

● Turn off Public folder sharing (people logged on to this computer can still access these folders)

Media streaming

When media streaming is on, people and devices on the network can access pictures, music, and videos on this computer. This computer can also find media on the network.

Click **Turn on media streaming**.



Media streaming options

Network and Sharing Ce... › Media streaming options

Choose media streaming options for computers and devices

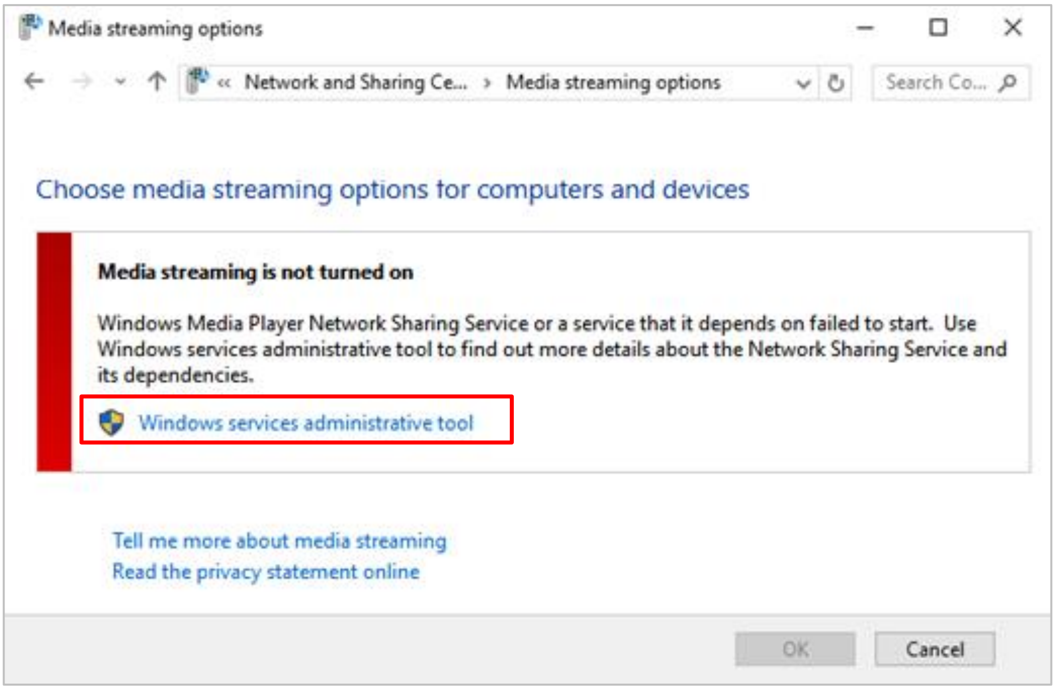
Media streaming is not turned on

Media streaming allows you to send your music, pictures and videos to other computers and devices on your network. It also allows you to receive media from other computers and devices.

If you turn on media streaming, your current network profile and firewall settings will be modified. You should turn on media streaming only on networks that you trust, such as home or work networks.

Turn on media streaming
Tell me more about media streaming
Read the privacy statement online
Search Co...
OK
Cancel

Click **Windows services administrative tool**.



Media streaming options

Network and Sharing Ce... › Media streaming options

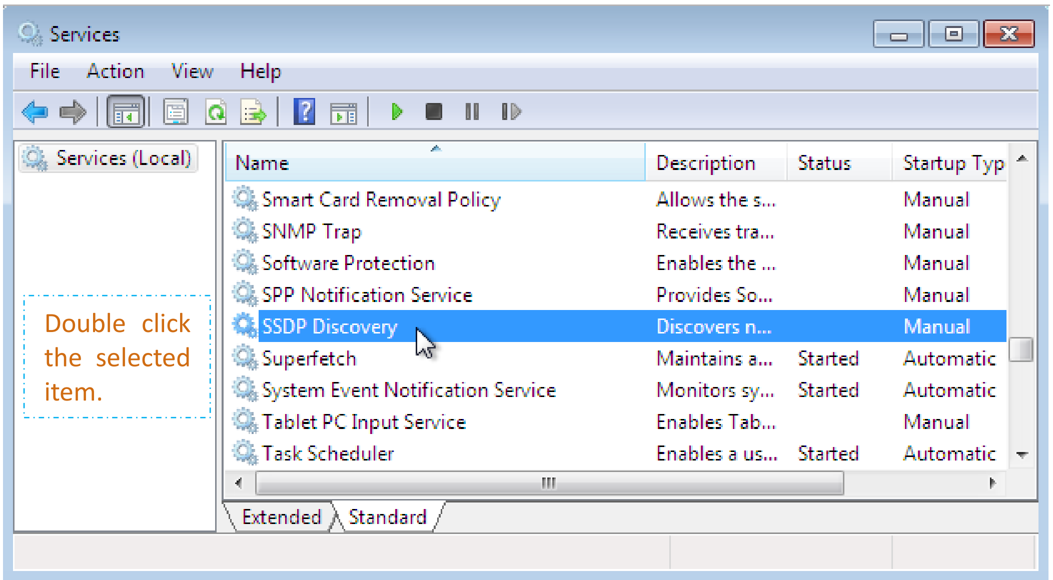
Choose media streaming options for computers and devices

Media streaming is not turned on

Windows Media Player Network Sharing Service or a service that it depends on failed to start. Use Windows services administrative tool to find out more details about the Network Sharing Service and its dependencies.

Windows services administrative tool
Tell me more about media streaming
Read the privacy statement online
Search Co...
OK
Cancel

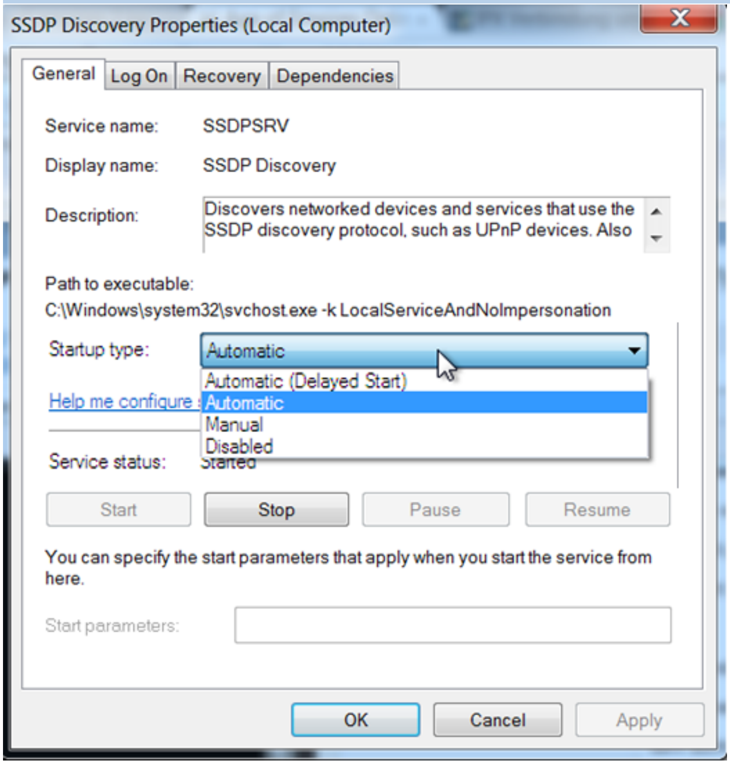
Set **Startup Type** of **SSDP Discovery**, **UPnP Device Host**, and **Windows Media Player Network Sharing Service** to **Automatic**.



Services

Name	Description	Status	Startup Typ
Smart Card Removal Policy	Allows the s...		Manual
SNMP Trap	Receives tra...		Manual
Software Protection	Enables the ...		Manual
SPP Notification Service	Provides So...		Manual
SSDP Discovery	Discovers n...		Manual
Superfetch	Maintains a...	Started	Automatic
System Event Notification Service	Monitors sy...	Started	Automatic
Tablet PC Input Service	Enables Tab...		Manual
Task Scheduler	Enables a us...	Started	Automatic

Double click the selected item.



SSDP Discovery Properties (Local Computer)

Service name: SSDPSRV

Display name: SSDP Discovery

Description: Discovers networked devices and services that use the SSDP discovery protocol, such as UPnP devices. Also

Path to executable:
C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation

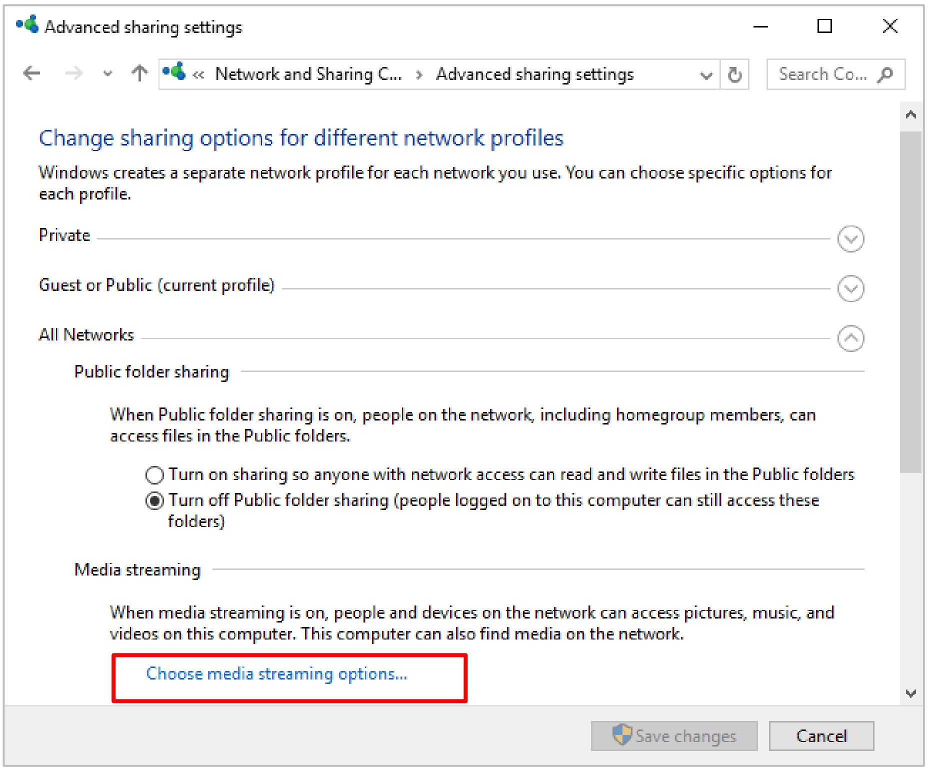
Startup type: Automatic

Service status: Started

You can specify the start parameters that apply when you start the service from here.

Start parameters:

Go to the **Advanced sharing settings** page and click **Choose media streaming options…**.



Advanced sharing settings

Network and Sharing C... › Advanced sharing settings

Search Co...

Change sharing options for different network profiles

Windows creates a separate network profile for each network you use. You can choose specific options for each profile.

Private

Guest or Public (current profile)

All Networks

Public folder sharing

When Public folder sharing is on, people on the network, including homegroup members, can access files in the Public folders.

○ Turn on sharing so anyone with network access can read and write files in the Public folders

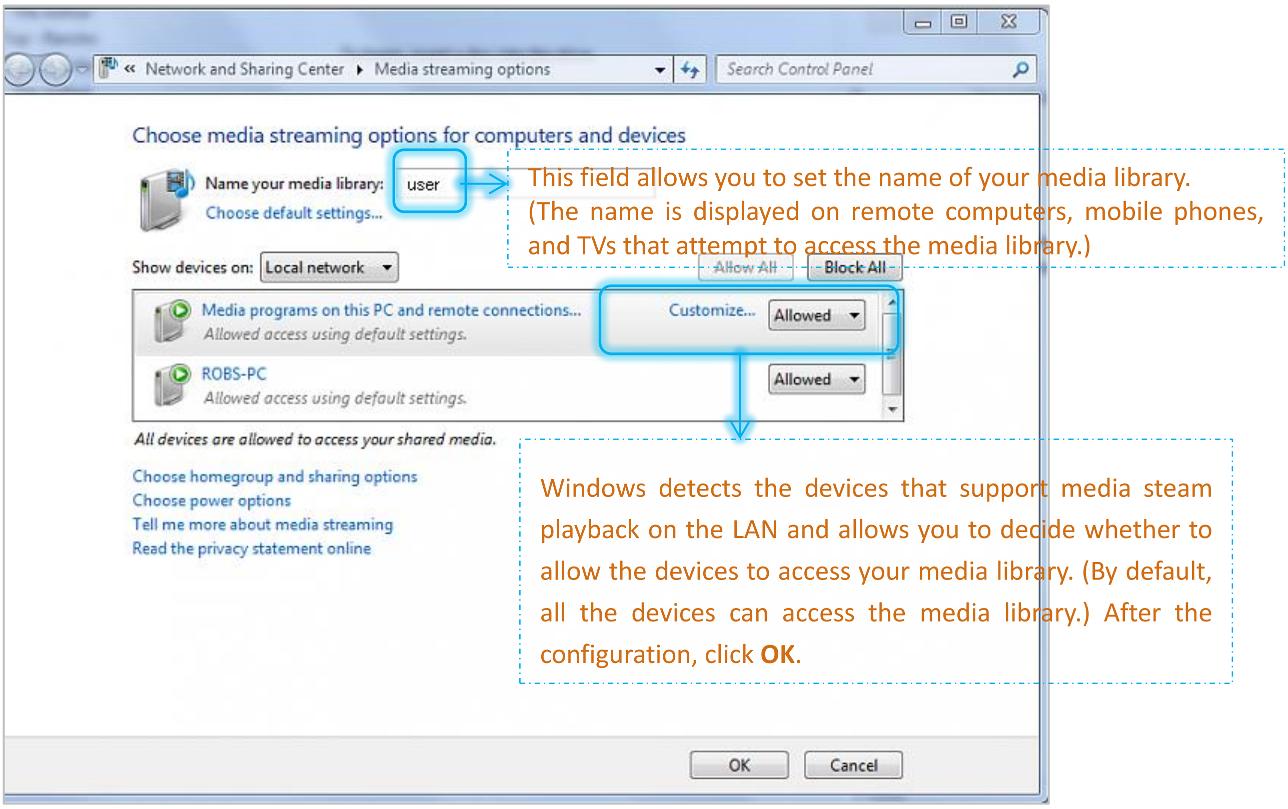
● Turn off Public folder sharing (people logged on to this computer can still access these folders)

Media streaming

When media streaming is on, people and devices on the network can access pictures, music, and videos on this computer. This computer can also find media on the network.

Choose media streaming options...

The **Media streaming options** page appears, showing that the media streaming function is enabled.



Network and Sharing Center › Media streaming options

Search Control Panel

Choose media streaming options for computers and devices

Name your media library: user

Choose default settings...

Show devices on: Local network

Allow All | Block All

Media programs on this PC and remote connections... — Customize... — Allowed

Allowed access using default settings.

ROBS-PC — Allowed

Allowed access using default settings.

All devices are allowed to access your shared media.

Choose homegroup and sharing options

Choose power options

Tell me more about media streaming

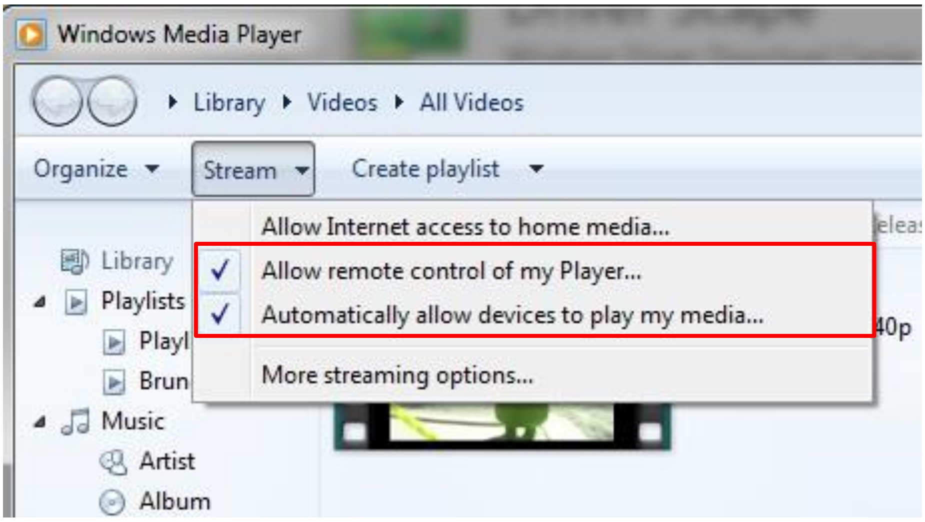
Read the privacy statement online

This field allows you to set the name of your media library. (The name is displayed on remote computers, mobile phones, and TVs that attempt to access the media library.)

Windows detects the devices that support media steam playback on the LAN and allows you to decide whether to allow the devices to access your media library. (By default, all the devices can access the media library.) After the configuration, click **OK**.

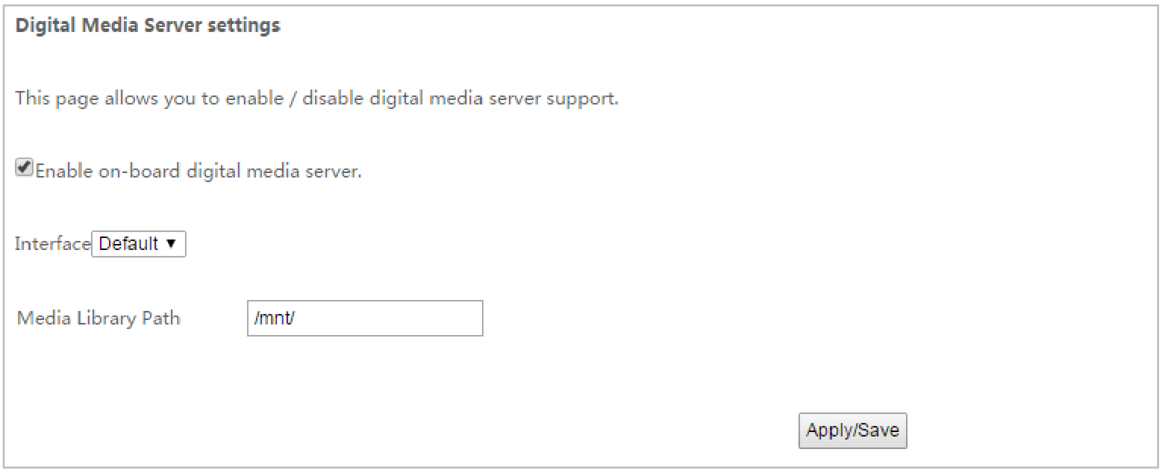
Windows Media Player of a Windows OS can access the devices where DLNA is enabled and function as a platform for playing the media resources of the devices locally.

Run Windows Media Player, click **Stream**, and select the **Allow remote control of my Player** and **Automatically allow devices to play my media** menu items. If a confirmation dialog box appears when you select the menu items, follow the onscreen instruction to confirm the operation.


Windows Media Player
Library ▸ Videos ▸ All Videos
Organize
Stream
Create playlist
Allow Internet access to home media...
✓ Allow remote control of my Player...
✓ Automatically allow devices to play my media...
More streaming options...
Library
Playlists
Playl
Brun
Music
Artist
Album

Step 2 Enable the DLNA function of the modem router.

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



Digital Media Server settings

This page allows you to enable / disable digital media server support.

☑Enable on-board digital media server.

Interface Default ▾

Media Library Path /mnt/

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

Click Apply/Save.

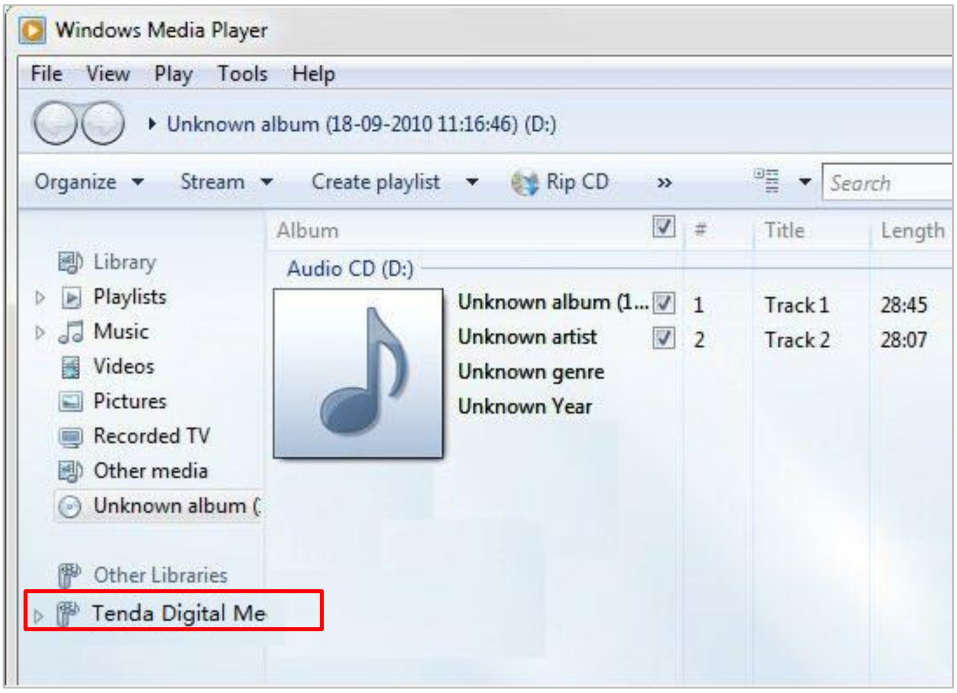
Step 3 On the computer, browse the video, audio, and image files in the USB storage device attached to the modem router.

1. Run Windows Media Player.

The USB storage device is displayed in the **Other Libraries** of the left pane.

Click the USB storage device.

The video, audio, and image files in the USB storage device appear.

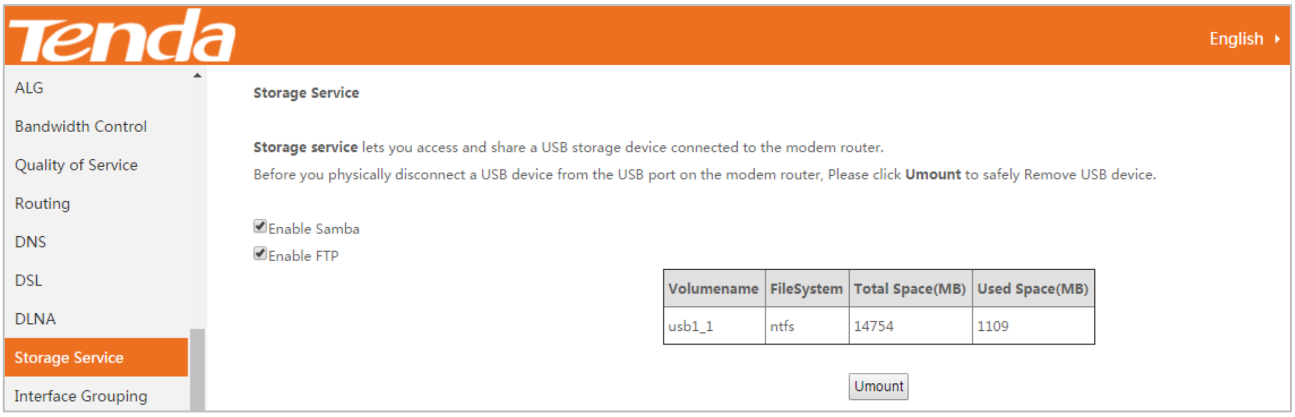


--End

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.

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



Storage Service

Storage service lets you access and share a USB storage device connected to the modem router.
Before you physically disconnect a USB device from the USB port on the modem router, Please click **Umount** to safely Remove USB device.

☑Enable Samba
☑Enable FTP

Volumename	FileSystem	Total Space(MB)	Used Space(MB)
usb1_1	ntfs	14754	1109

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

Step 1 Select **Enable Samba**.

Step 2 Select **Enable FTP**.

--End

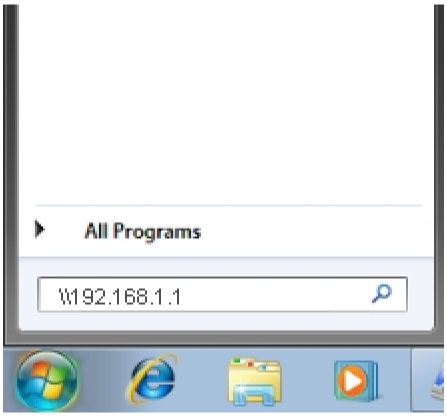
Accessing the USB Storage Device Connected to the Modem Router over the LAN

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 server address is 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.)

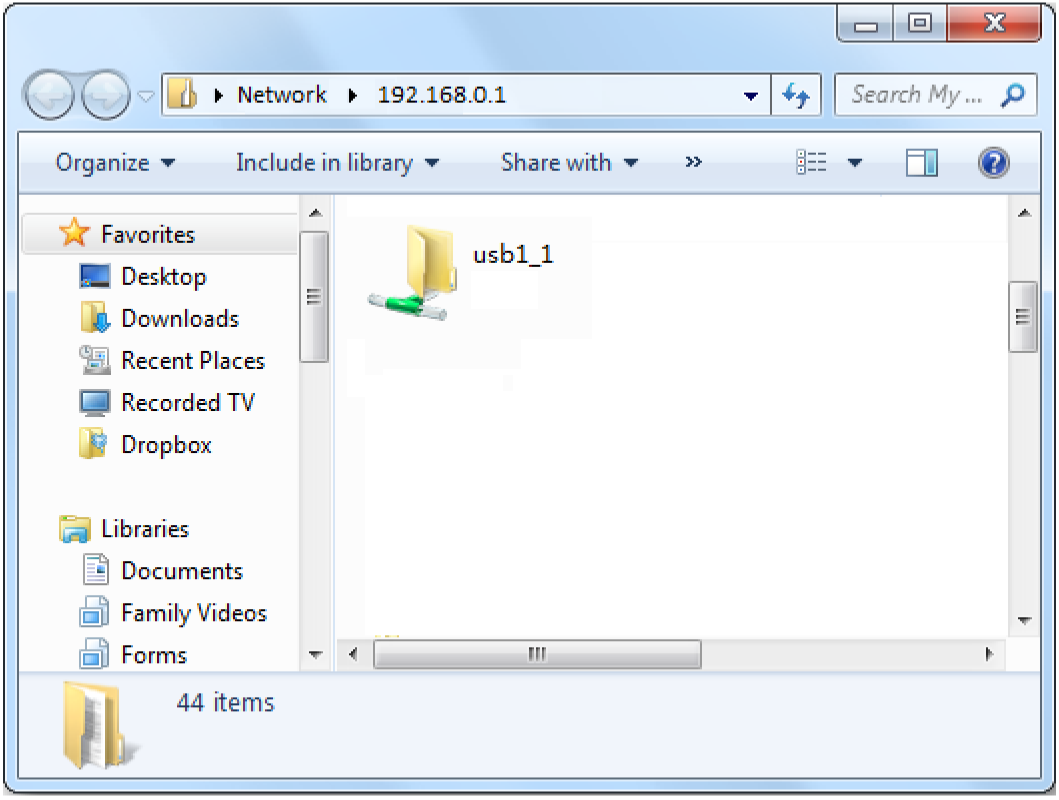
Step 1 Click and enter **\\192.168.1.1**.



\\192.168.1.1

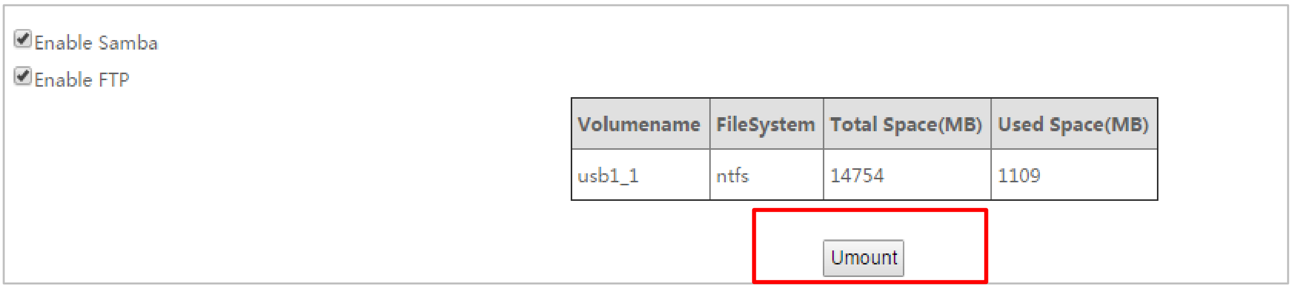
Step 2 Press **Enter** on the keyboard.

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.



☑Enable Samba

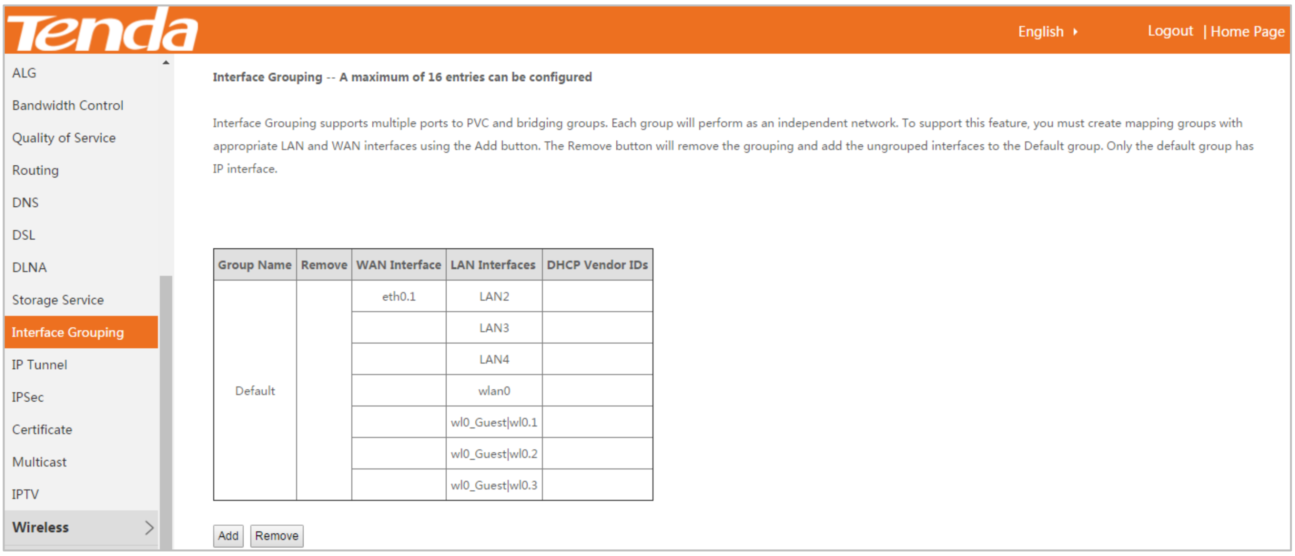
☑Enable FTP

Volumename	FileSystem	Total Space(MB)	Used Space(MB)
usb1_1	ntfs	14754	1109

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 create mapping groups with appropriate LAN and WAN interfaces. Each group performs as an independent network.

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



Interface Grouping -- A maximum of 16 entries can be configured

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

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

To create a mapping group, perform the following procedure:

Assume that:

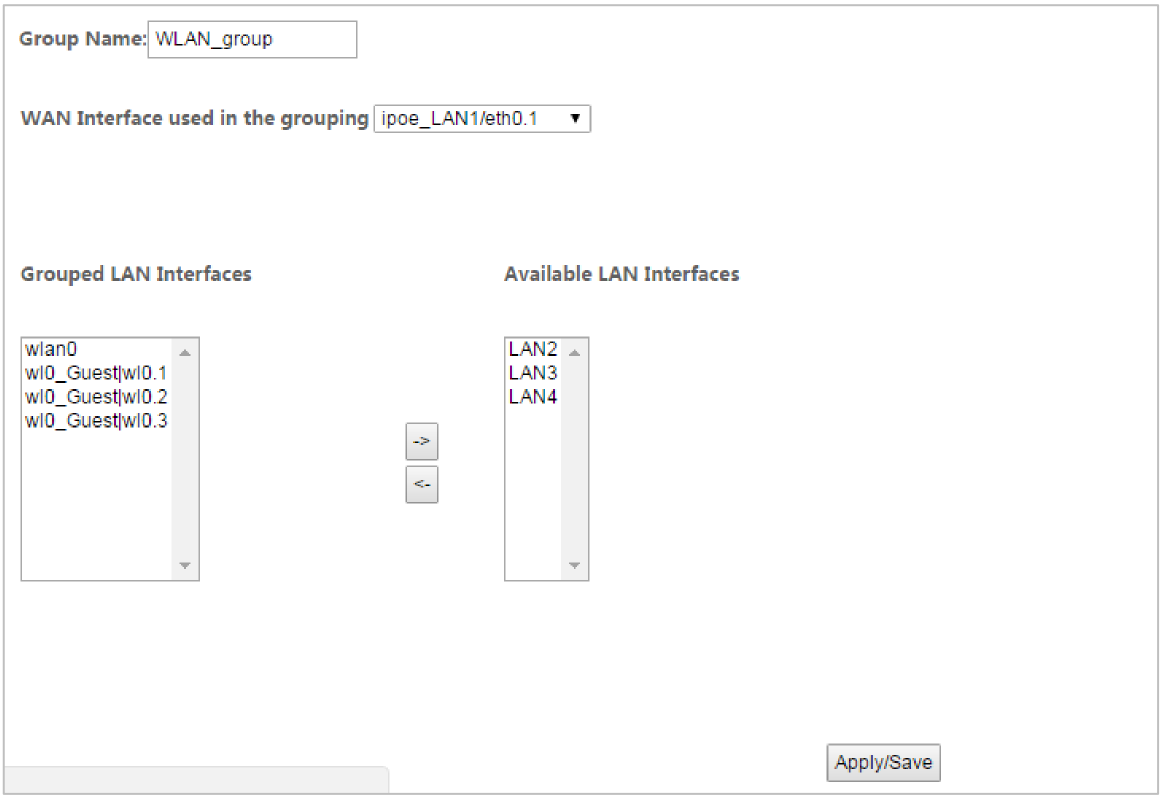
- The modem router accesses the internet through port 1 using an Ethernet cable.
- You create two WAN services: the WAN service type for one is **IP over Ethernet** and **Obtain an IP address automatically**, and the other is **bridging**.
- You want all wireless devices to use **IP over Ethernet** WAN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

Step 1 Click **Add**.

Step 2 Specify a group name.

Step 3 Select a WAN service you create, **ipoe_LAN1/eth0.1** here.

Step 4 Select an interface in **Available LAN Interfaces** list and click <- button to move it to **Grouped ALN Interfaces** list. Move all wireless interfaces to **Grouped ALN Interfaces** list here.



Group Name: WLAN_group

WAN Interface used in the grouping ipoe_LAN1/eth0.1

Grouped LAN Interfaces

wlan0
wl0_Guest|wl0.1
wl0_Guest|wl0.2
wl0_Guest|wl0.3

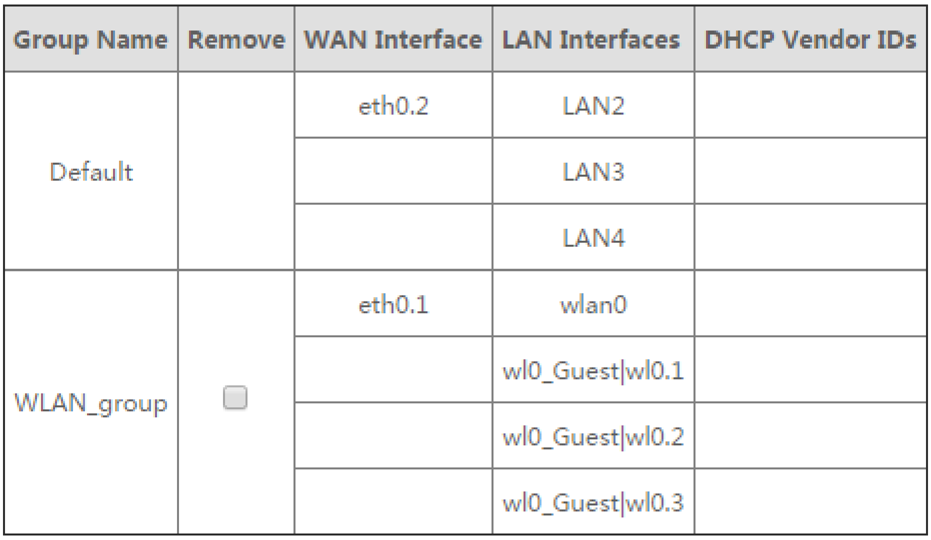
Available LAN Interfaces

LAN2
LAN3
LAN4

Step 5 Click **Apply/Save**.

--End

After the configuration takes effect, all wireless interfaces are classified into the **WLAN_group** using the WAN service **IP over Ethernet** (eth0.1), and all wired interfaces (port 1, 2, and 3) are classified into the default group using 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 the following groups follow the same rule.
- 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

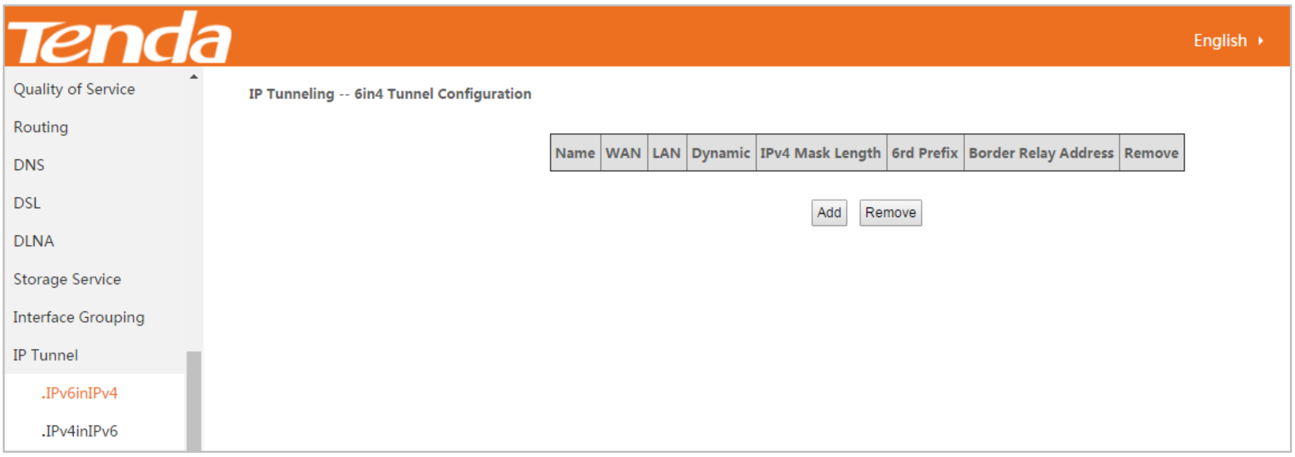
An IP tunnel is an Internet Protocol (IP) network communications channel between two networks. It is used to transport another network protocol by encapsulation of its packets.

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.

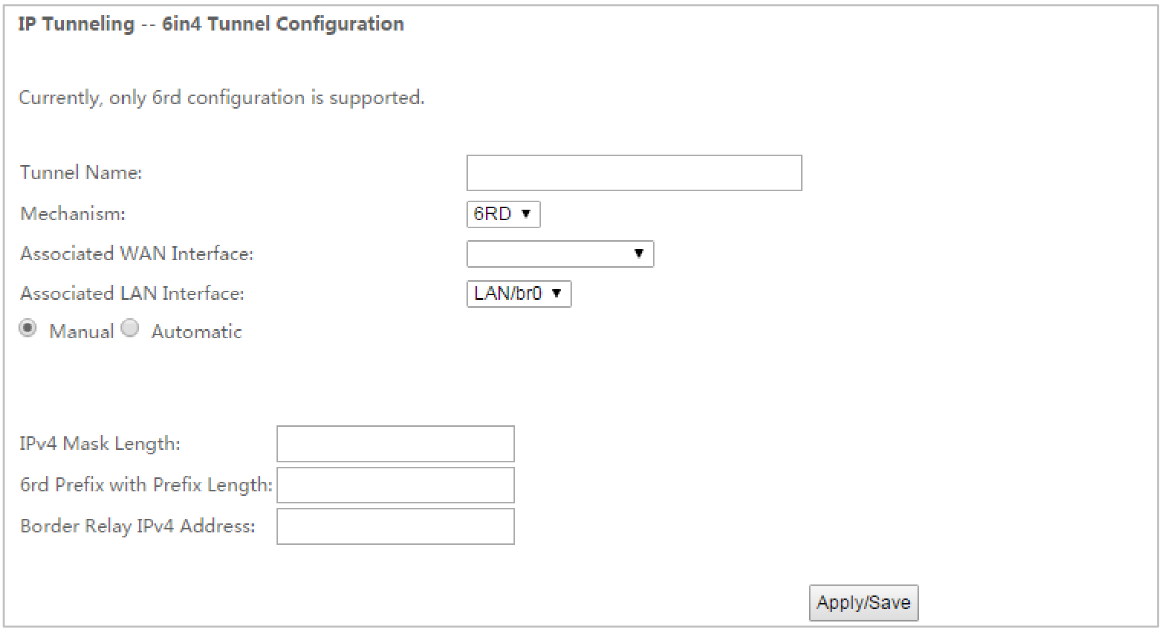
Choose **Advanced** > **Advanced Setup** > **IP Tunnel > IPv6inIPv4** to enter the configuration page.



IP Tunneling -- 6in4 Tunnel Configuration

Name	WAN	LAN	Dynamic	IPv4 Mask Length	6rd Prefix	Border Relay Address	Remove

To configure the IPv6inIPv4 tunnel, perform the following procedure:



IP Tunneling -- 6in4 Tunnel Configuration

Currently, only 6rd configuration is supported.

Tunnel Name:	
Mechanism:	6RD ▼
Associated WAN Interface:	▼
Associated LAN Interface:	LAN/br0 ▼

● Manual ○ Automatic

IPv4 Mask Length:	
6rd Prefix with Prefix Length:	
Border Relay IPv4 Address:	

Step 1 Click **Add**.

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

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

Step 4 **Associated WAN Interface**: Specify 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 the type of obtaining border relay address: manual or automatic.

- **Manual**: Manually set a 6RD-BR address.
- **Automatic**: Automatically obtain a 6RD-BR address from upstream device. 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.

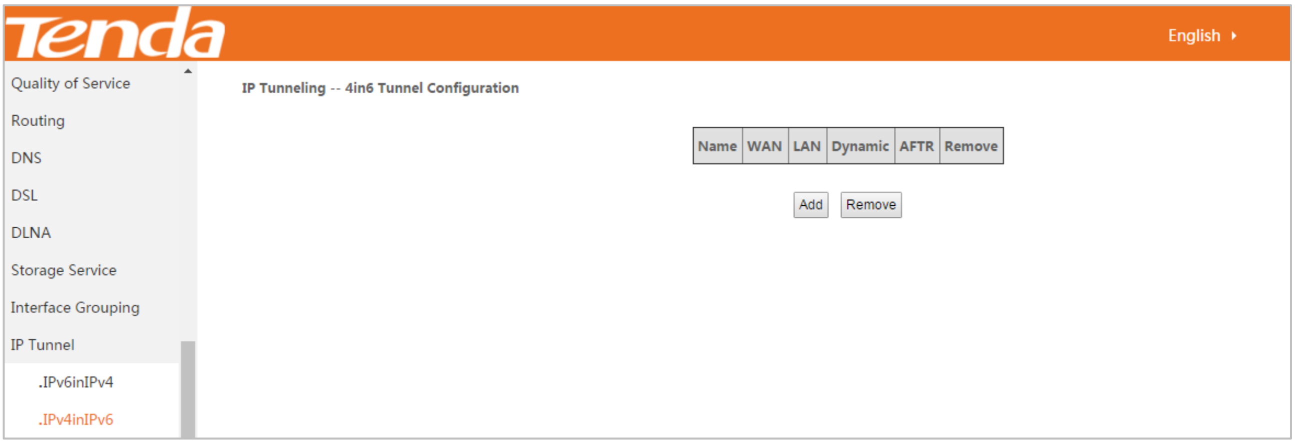
Step 10 Click **Apply/Save**.

--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.

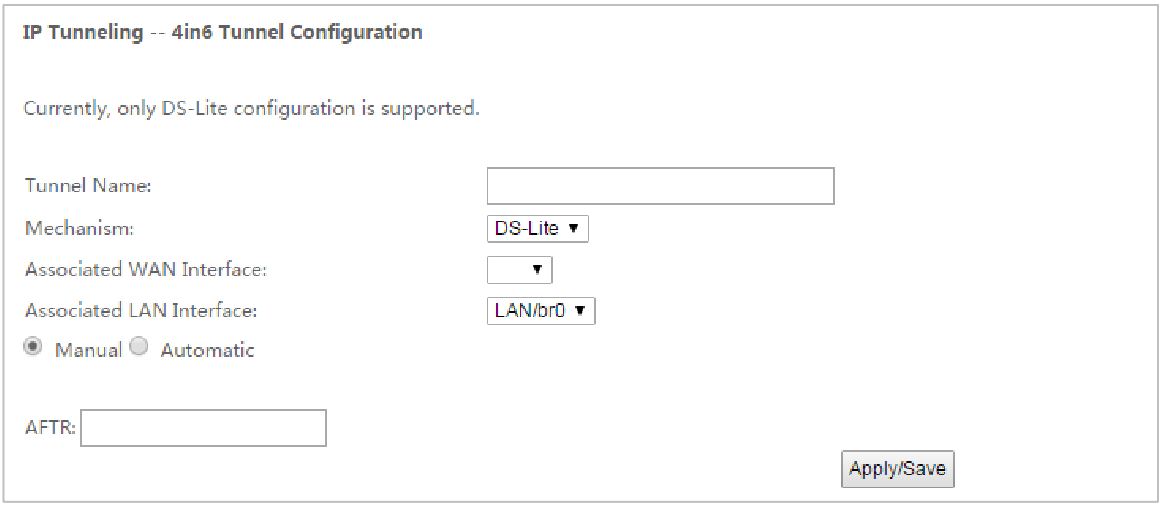
Choose **Advanced** > **Advanced Setup** > **IP Tunnel > IPv4inIPv6** to enter the configuration page.



IP Tunneling -- 4in6 Tunnel Configuration

Name	WAN	LAN	Dynamic	AFTR	Remove

To configure the IPv4inIPv6 tunnel, perform the following procedure:



IP Tunneling -- 4in6 Tunnel Configuration

Currently, only DS-Lite configuration is supported.

Tunnel Name:	
Mechanism:	DS-Lite ▼
Associated WAN Interface:	▼
Associated LAN Interface:	LAN/br0 ▼

● Manual ○ Automatic

AFTR:

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 the type of obtaining AFTR IPv6 address: manual or automatic.

- **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.

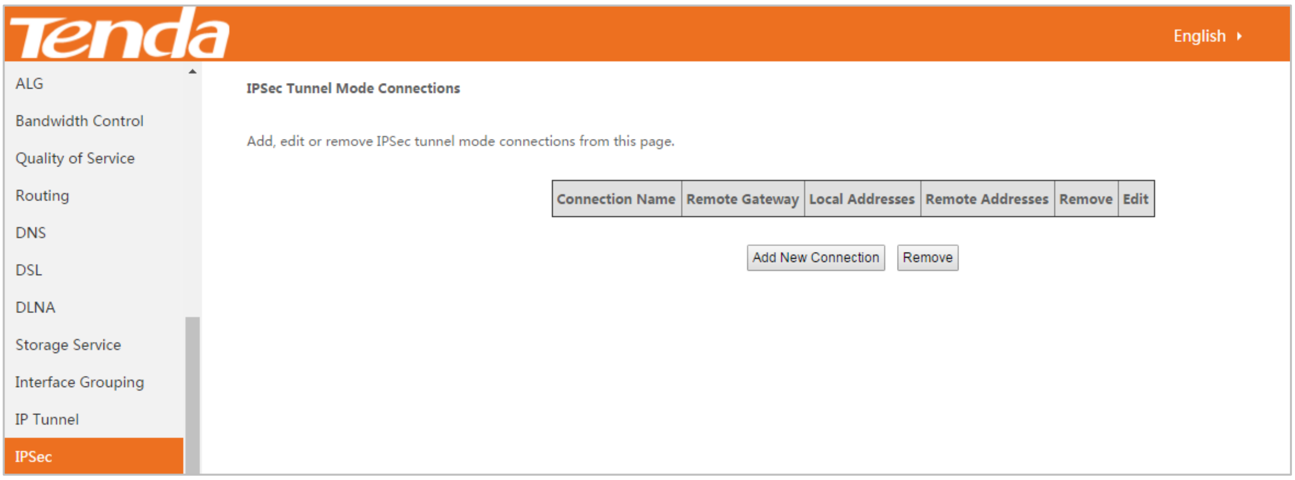
Step 8 Click **Apply/Save**.

--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.



IPSec Tunnel Mode Connections

Add, edit or remove IPSec tunnel mode connections from this page.

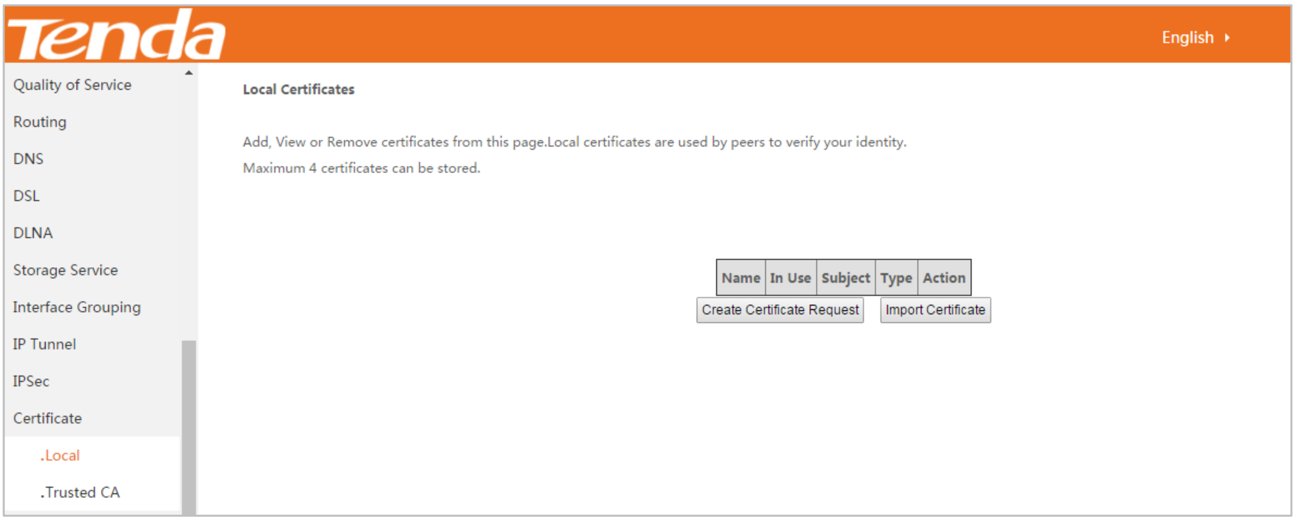
Connection Name	Remote Gateway	Local Addresses	Remote Addresses	Remove	Edit

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.



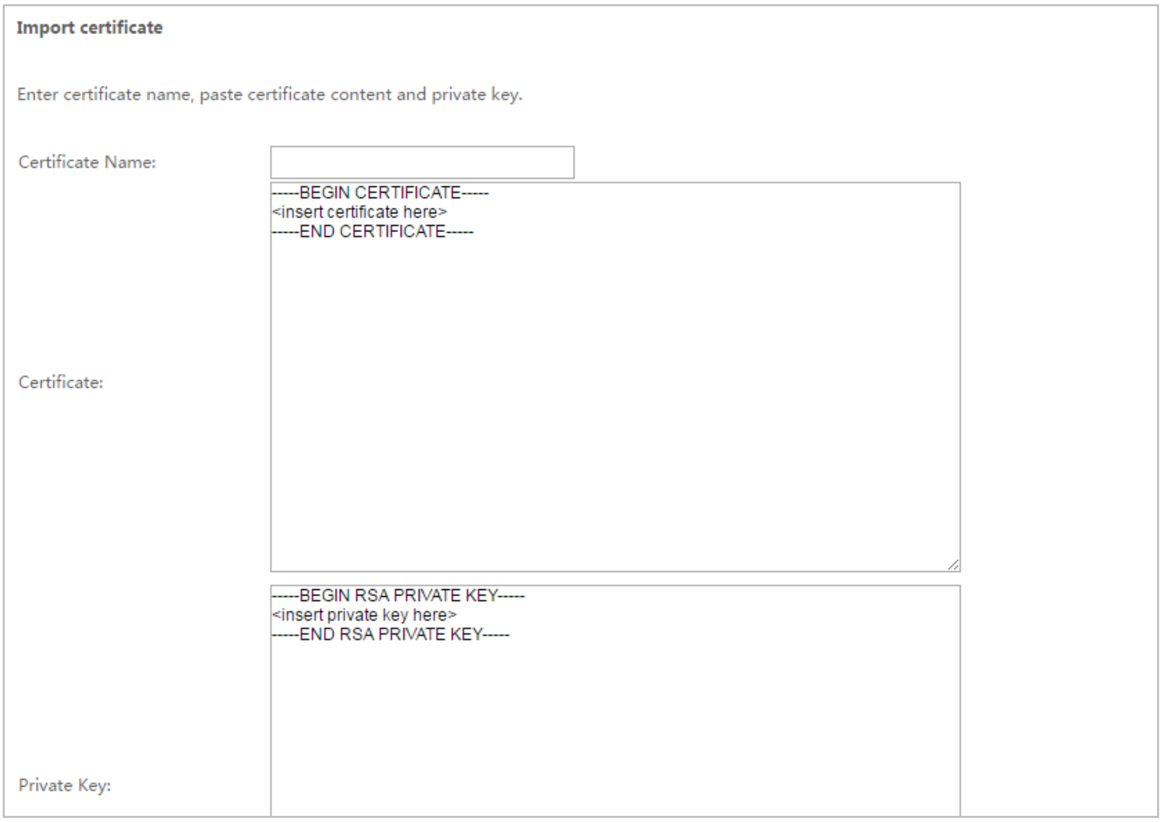
Local Certificates

Add, View or Remove certificates from this page.Local certificates are used by peers to verify your identity.
Maximum 4 certificates can be stored.

Name	In Use	Subject	Type	Action

To import a certificate, perform the following procedure:

Step 1 Click **Import Certificate**.



Import certificate

Enter certificate name, paste certificate content and private key.

Certificate Name:

Certificate:

```
-----BEGIN CERTIFICATE-----
<insert certificate here>
-----END CERTIFICATE-----
```

Private Key:

```
-----BEGIN RSA PRIVATE KEY-----
<insert private key here>
-----END RSA PRIVATE KEY-----
```

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 box.

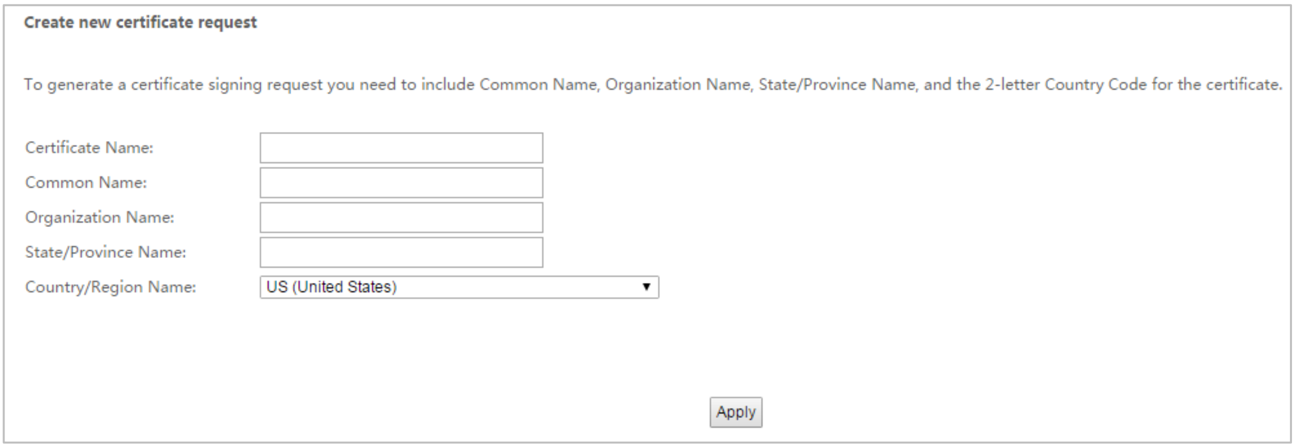
Step 4 **Private Key**: Copy the private key information which is generated when you apply the certificate to the box.

Step 5 Click **Apply**.

--End

To create a new certificate, perform the following procedure:

Step 1 Click **Create Certificate Request**.



Create new certificate request

To generate a certificate signing request you need to include Common Name, Organization Name, State/Province Name, and the 2-letter Country Code for the certificate.

Certificate Name:

Common Name:

Organization Name:

State/Province Name:

Country/Region Name: US (United States)

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 applier, such as **Tendacn.com**, **Tenda** or **Lucy**.

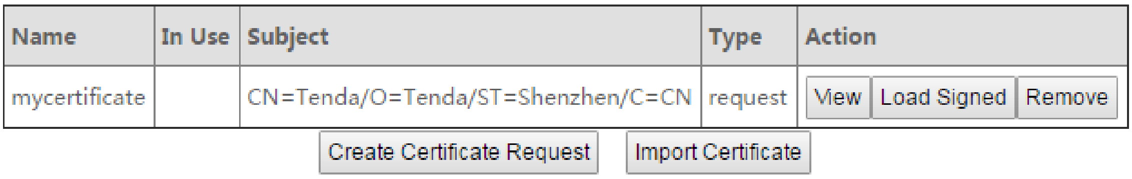
Step 4 **Organization Name**: Enter the name of an organization/company, such as **Tenda**.

Step 5 **State/Province Name**: Enter the located state.

Step 6 **Country/Region Name**: Select the located country.

Step 7 Click **Apply.**

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



Name	In Use	Subject	Type	Action
mycertificate		CN=Tenda/O=Tenda/ST=Shenzhen/C=CN	request	View Load Signed Remove

Request: The certificate is being applied.

View: To view the details of the certificate.

Load Signed: To import and apply the certificate.

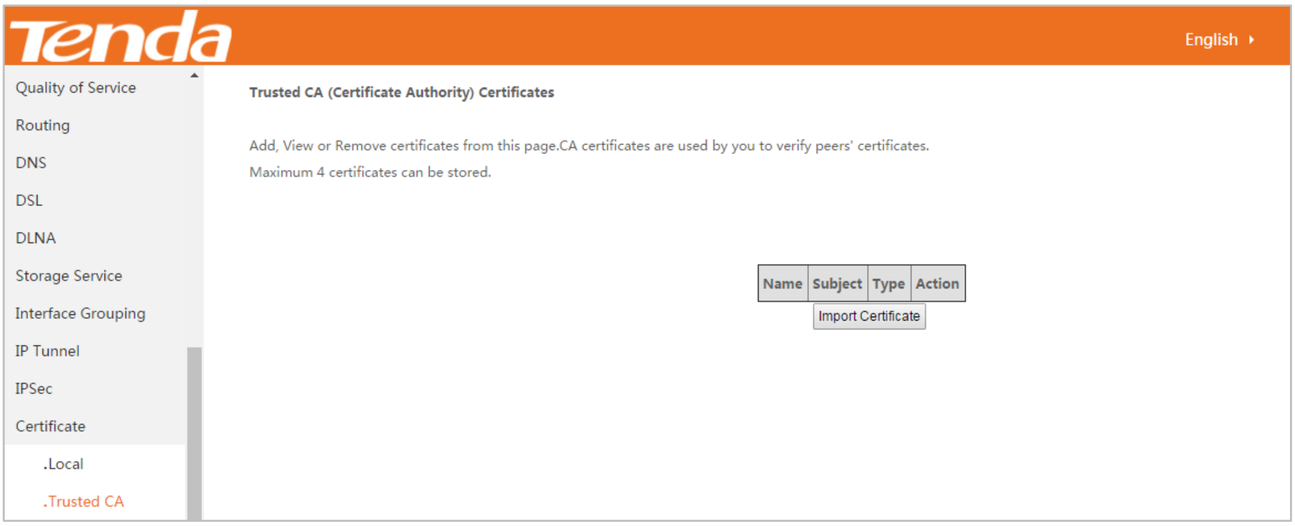
Remove: To delete the certificate.

--End

4.20.2 Trusted CA

Import a certificate of other network device to authenticate the identity of the modem router.

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



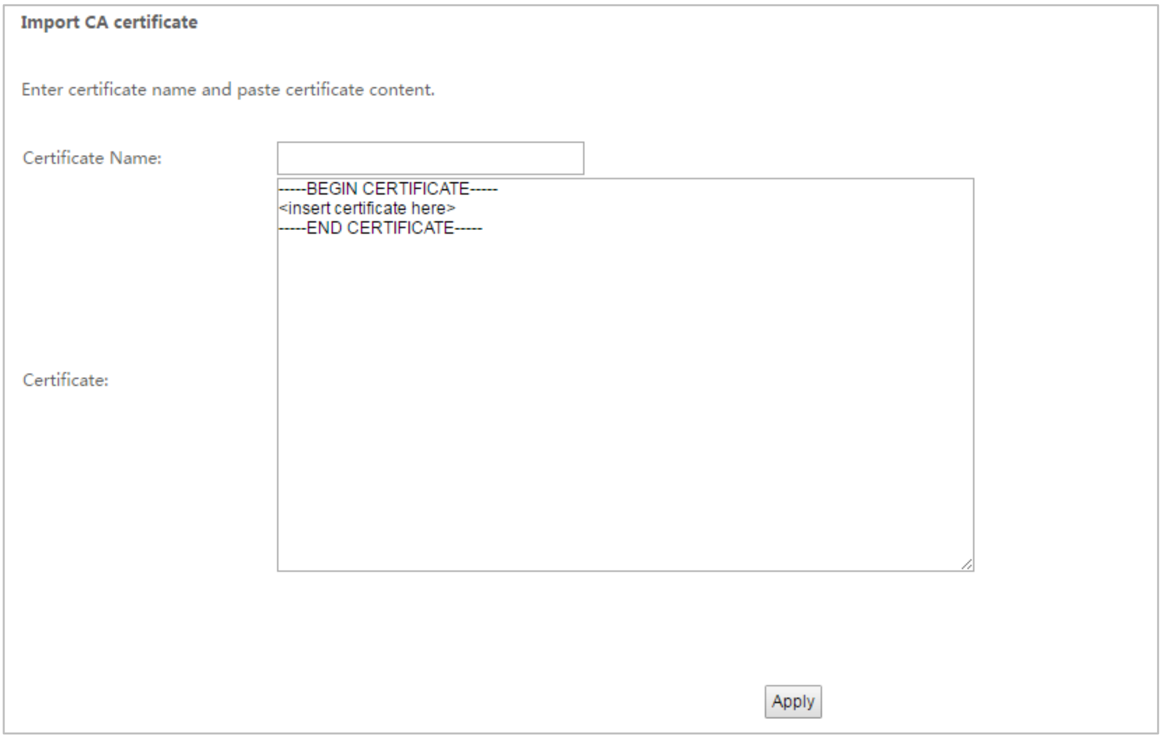
Trusted CA (Certificate Authority) Certificates

Add, View or Remove certificates from this page.CA certificates are used by you to verify peers' certificates.

Maximum 4 certificates can be stored.

Name	Subject	Type	Action

To import a certificate, perform the following procedure:



Import CA certificate

Enter certificate name and paste certificate content.

Certificate Name:

Certificate:

```
-----BEGIN CERTIFICATE-----
<insert certificate here>
-----END CERTIFICATE-----
```

Step 1 Click **Import Certificate**.

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

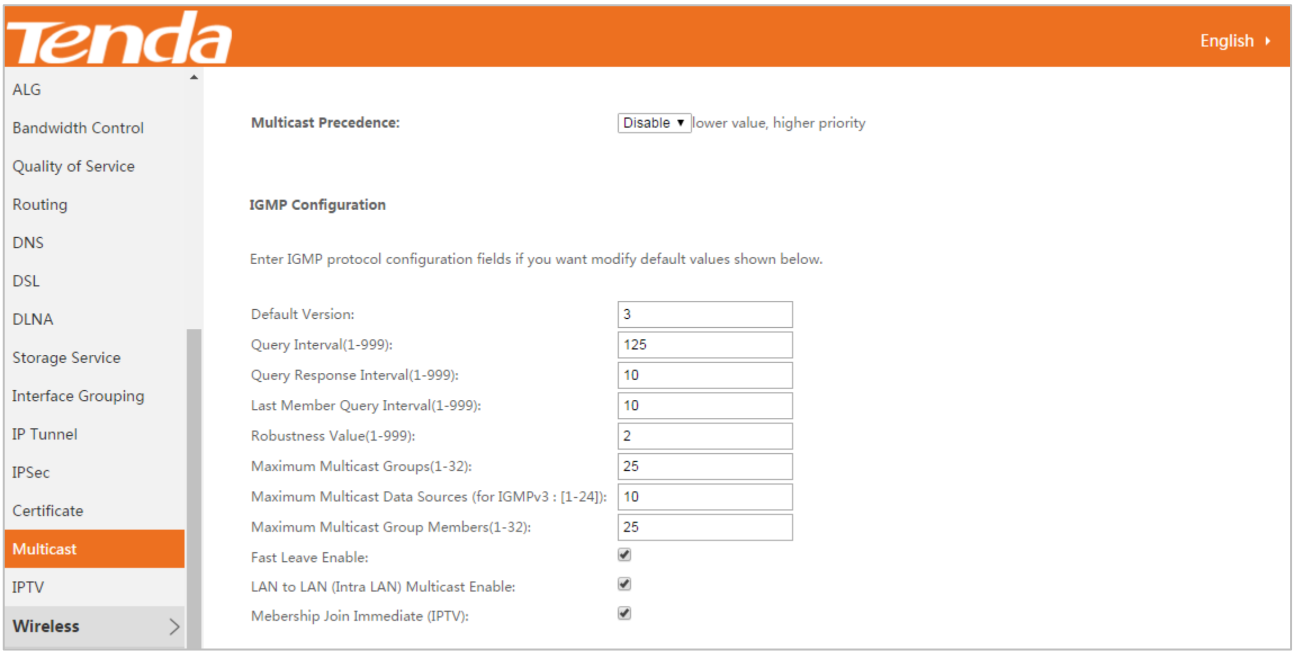
Step 3 **Certificate:** Enter the content of the certificate.

Step 4 Click **Apply**.

--End

4.21 Multicast

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



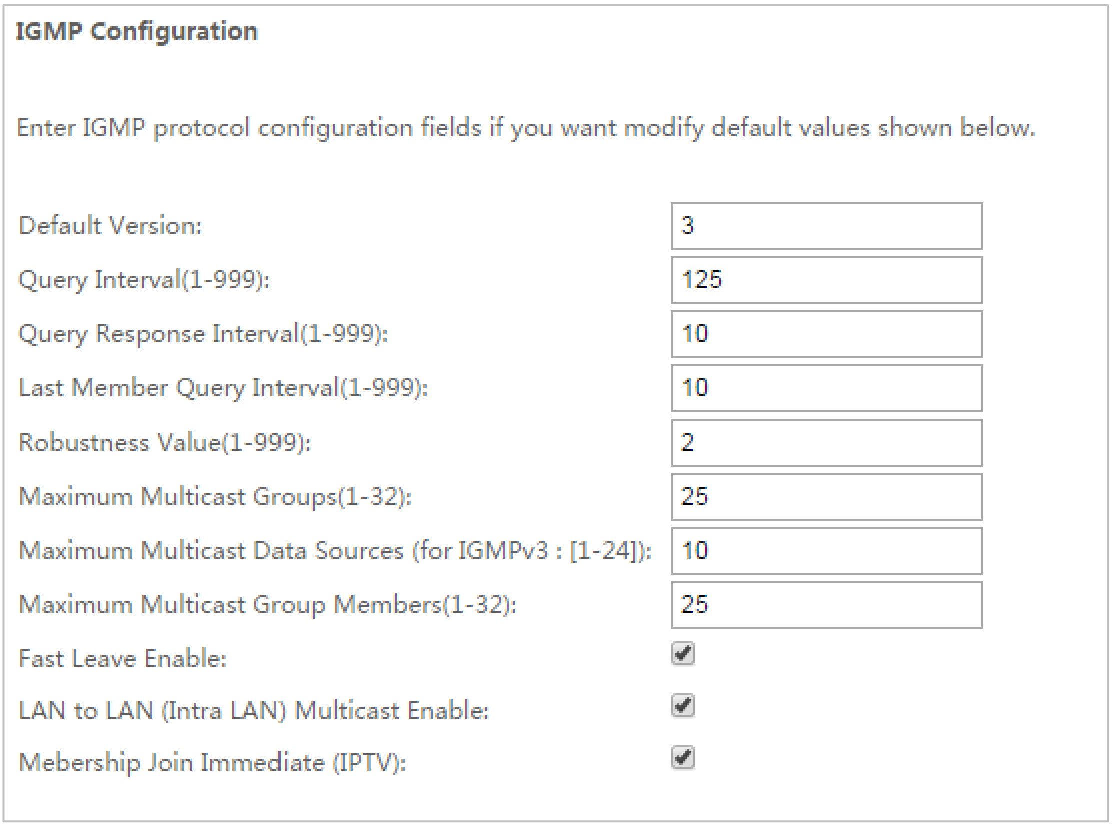
Multicast Precedence: Disable lower value, higher priority

IGMP Configuration

Enter IGMP protocol configuration fields if you want modify default values shown below.

Default Version:	3
Query Interval(1-999):	125
Query Response Interval(1-999):	10
Last Member Query Interval(1-999):	10
Robustness Value(1-999):	2
Maximum Multicast Groups(1-32):	25
Maximum Multicast Data Sources (for IGMPv3 : [1-24]):	10
Maximum Multicast Group Members(1-32):	25
Fast Leave Enable:	☑
LAN to LAN (Intra LAN) Multicast Enable:	☑
Mebership Join Immediate (IPTV):	☑

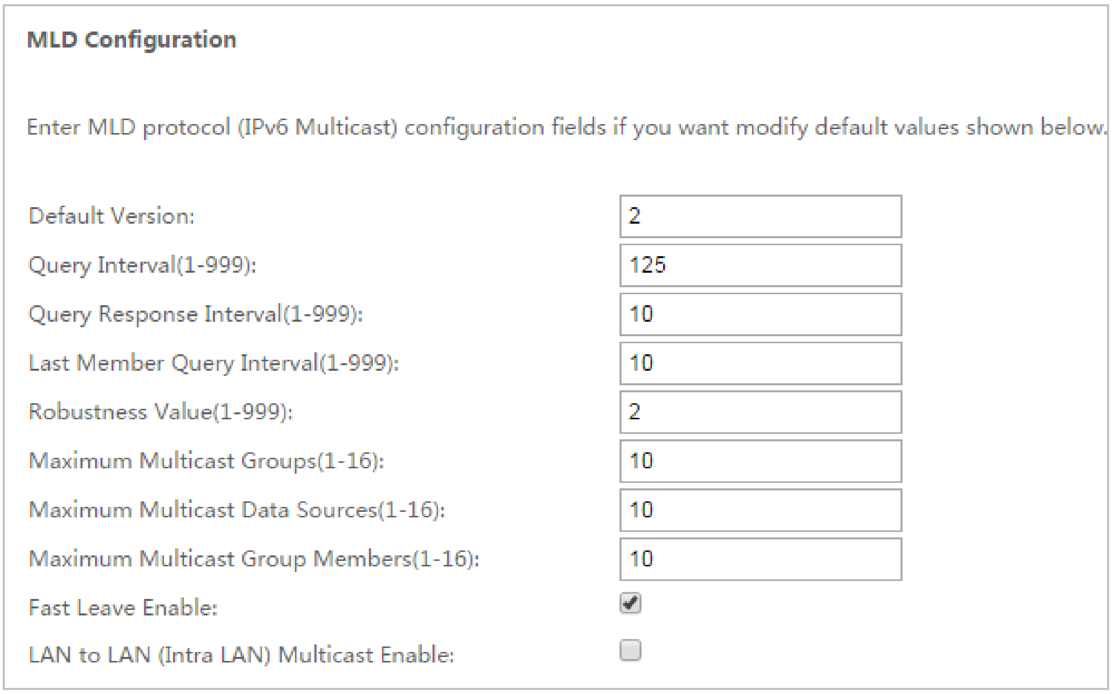
Multicast Precedence: Set the priority for the multicast data. Lower value leads to higher priority.



IGMP Configuration

Enter IGMP protocol configuration fields if you want modify default values shown below.

Default Version:	3
Query Interval(1-999):	125
Query Response Interval(1-999):	10
Last Member Query Interval(1-999):	10
Robustness Value(1-999):	2
Maximum Multicast Groups(1-32):	25
Maximum Multicast Data Sources (for IGMPv3 : [1-24]):	10
Maximum Multicast Group Members(1-32):	25
Fast Leave Enable:	☑
LAN to LAN (Intra LAN) Multicast Enable:	☑
Mebership Join Immediate (IPTV):	☑



MLD Configuration

Enter MLD protocol (IPv6 Multicast) configuration fields if you want modify default values shown below.

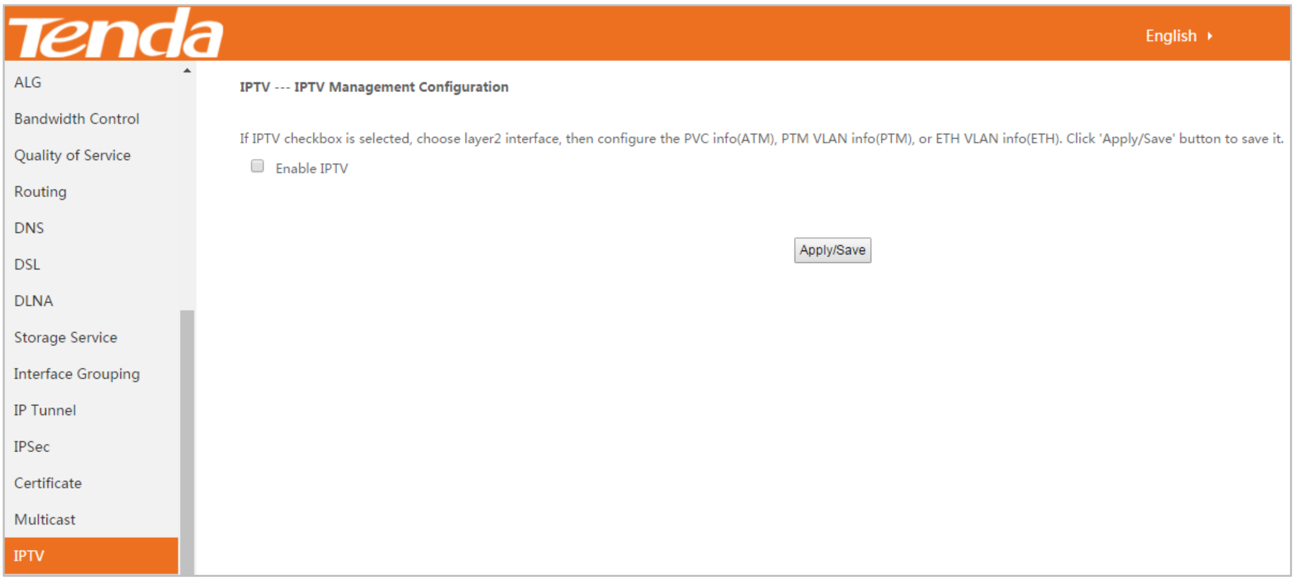
Default Version:	2
Query Interval(1-999):	125
Query Response Interval(1-999):	10
Last Member Query Interval(1-999):	10
Robustness Value(1-999):	2
Maximum Multicast Groups(1-16):	10
Maximum Multicast Data Sources(1-16):	10
Maximum Multicast Group Members(1-16):	10
Fast Leave Enable:	☑
LAN to LAN (Intra LAN) Multicast Enable:	□

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 range of the query interval is from 1 to 999. The unit is “s”.
Query Response Interval (1-999)	It specifies the response interval for the query message. The default is 10. The range of the query interval is from 1 to 999. The unit is “s”.

Last Member Query Interval (1-999)	It specifies the interval for sending query message of specified group. The default is 10. The range of the query interval is from 1 to 999. The unit is “s”.
Robustness Value (1-999)	It specifies the robustness value of IGMP (MLD) querier. The default is 2. The range of the query interval is from 1 to 999.
Maximum Multicast Groups (1-32)	It specifies the maximum number of multicast group for each interface. The default is 25. The range of the query interval is from 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 range of the query interval is from 1 to 24.
Maximum Multicast Group Members (1-32)	It specifies the maximum number of multicast group member.
Fast Leave Enable	This function is useful when you use some applications, such as IPTV, which require changeable fast channel.
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.



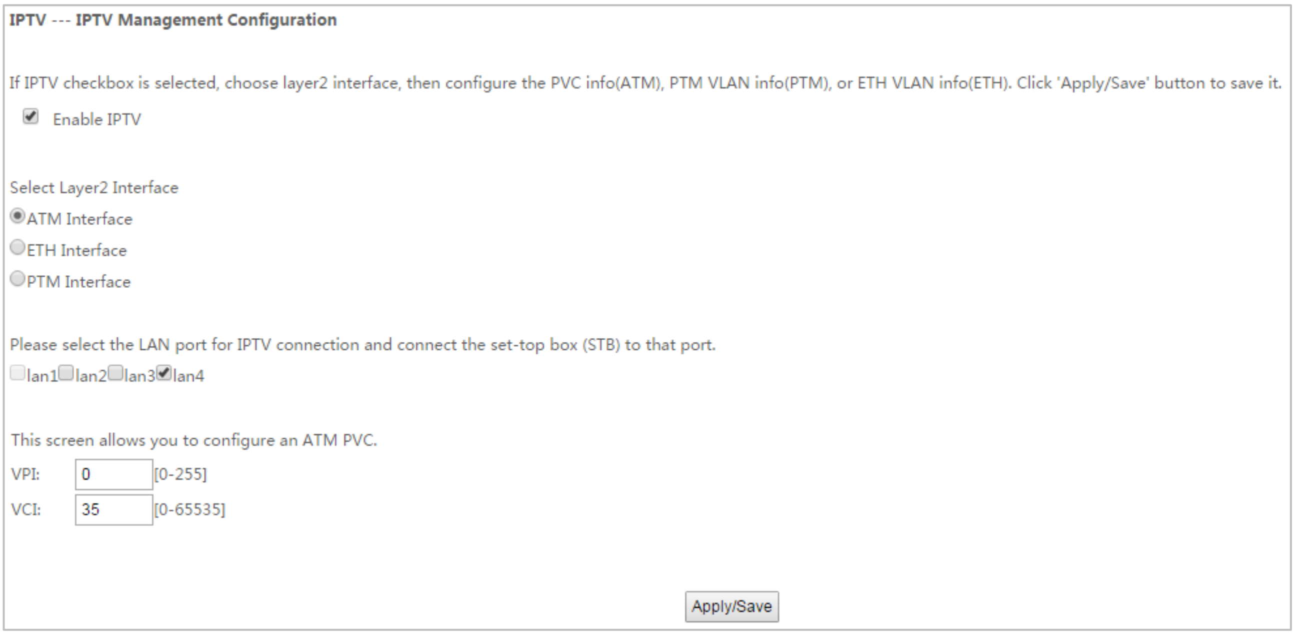
IPTV --- IPTV Management Configuration

If IPTV checkbox is selected, choose layer2 interface, then configure the PVC info(ATM), PTM VLAN info(PTM), or ETH VLAN info(ETH). Click 'Apply/Save' button to save it.

□ Enable IPTV

To configure the IPTV function, perform the following procedure:

Step 1 Select **Enable IPTV** option.



IPTV --- IPTV Management Configuration

If IPTV checkbox is selected, choose layer2 interface, then configure the PVC info(ATM), PTM VLAN info(PTM), or ETH VLAN info(ETH). Click 'Apply/Save' button to save it.

☑ Enable IPTV

Select Layer2 Interface

● ATM Interface
○ ETH Interface
○ PTM Interface

Please select the LAN port for IPTV connection and connect the set-top box (STB) to that port.

□lan1 □lan2 □lan3 ☑lan4

This screen allows you to configure an ATM PVC.

VPI: 0 [0-255]
VCI: 35 [0-65535]

Step 2 Select a layer2 interface. Select the one you create in **Layer2 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**.

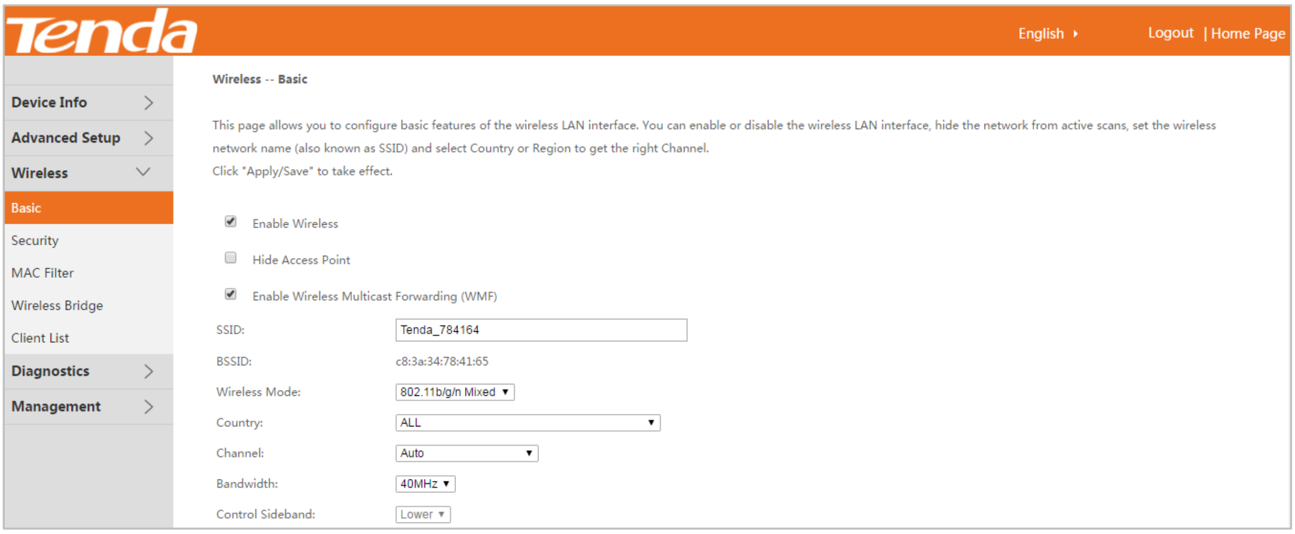
--End

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.



Wireless -- Basic

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and select Country or Region to get the right Channel.
Click "Apply/Save" to take effect.

☑ Enable Wireless

□ Hide Access Point

☑ Enable Wireless Multicast Forwarding (WMF)

SSID: Tenda_784164

BSSID: c8:3a:34:78:41:65

Wireless Mode: 802.11b/g/n Mixed

Country: ALL

Channel: Auto

Bandwidth: 40MHz

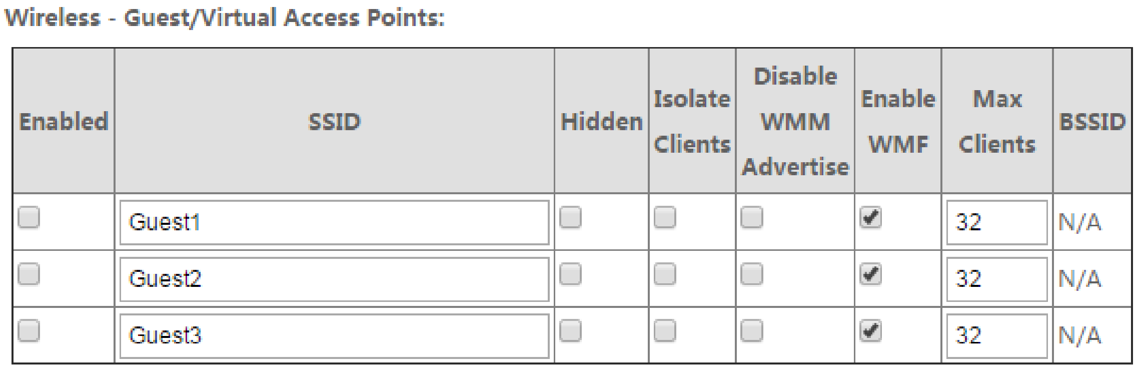
Control Sideband: Lower

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, the wireless device cannot search the SSID (wireless network name) of the modem router. It is required to enter the SSID manually for connection.
SSID	The wireless network name of the modem router.
BSSID	The 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 of 11 Mbps wireless rate is supported in this mode. • 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. • 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. • 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. • 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.

To Enable multiple SSID

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



Wireless - Guest/Virtual Access Points:

Enabled	SSID	Hidden	Isolate Clients	Disable WMM Advertise	Enable WMF	Max Clients	BSSID
☐	Guest1	☐	☐	☐	☑	32	N/A
☐	Guest2	☐	☐	☐	☑	32	N/A
☐	Guest3	☐	☐	☐	☑	32	N/A

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, the wireless device cannot search 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 usually transmitted at the lowest rate, such as 1 Mbps, leading to poor transmission efficiency. WMF leverages the high auto-negotiated 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 connected to this SSID.

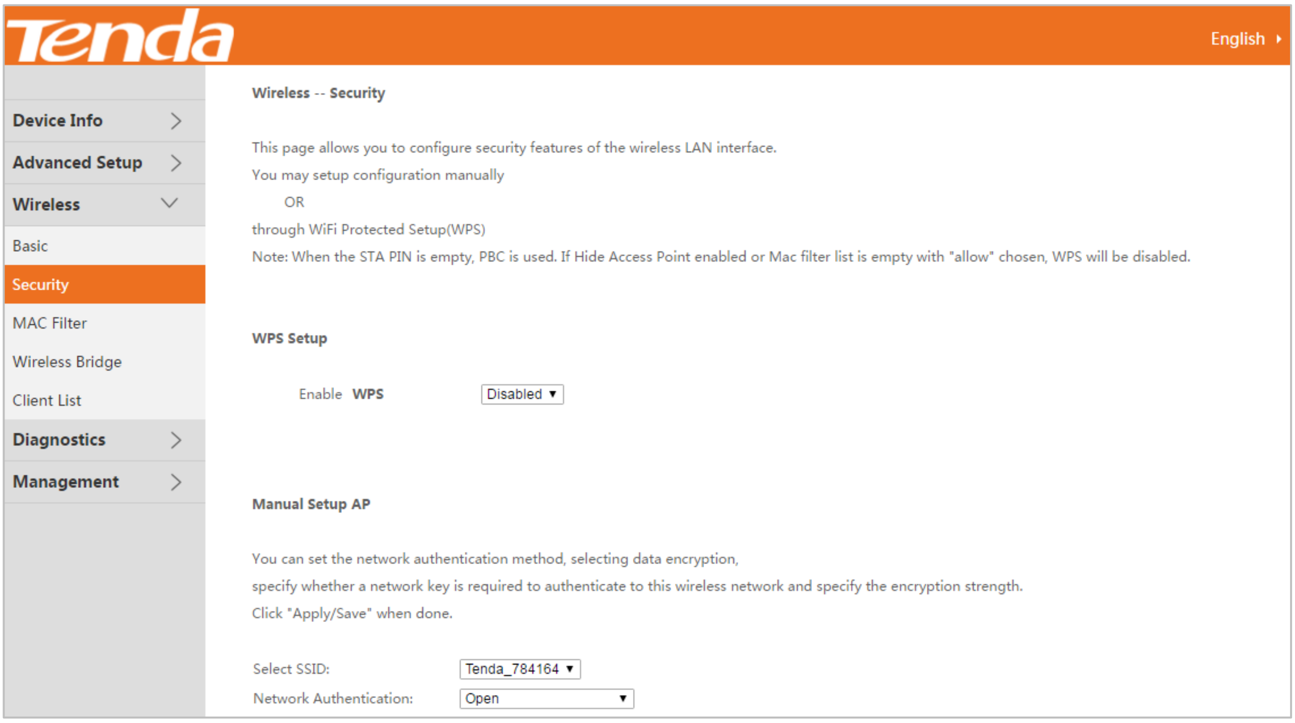
Step 7 Click **Apply/Save**.

--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.



Wireless -- Security

This page allows you to configure security features of the wireless LAN interface.
You may setup configuration manually
OR
through WiFi Protected Setup(WPS)
Note: When the STA PIN is empty, PBC is used. If Hide Access Point enabled or Mac filter list is empty with "allow" chosen, WPS will be disabled.

WPS Setup

Enable WPS: Disabled

Manual Setup AP

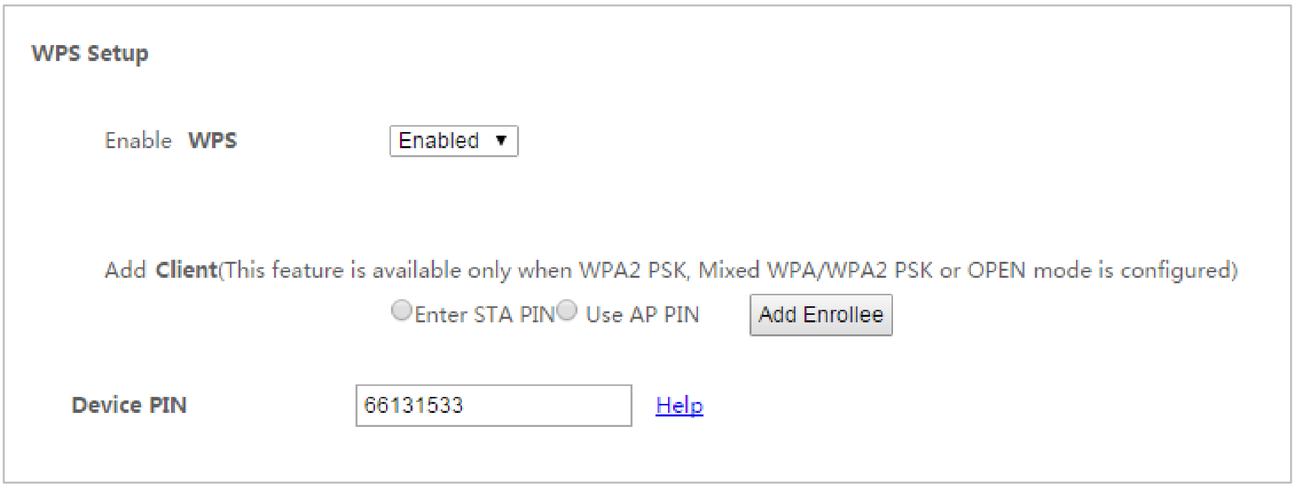
You can set the network authentication method, selecting data encryption,
specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.
Click "Apply/Save" when done.

Select SSID: Tenda_784164
Network Authentication: Open

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. Simply enter a PIN code on the device web interface or press hardware WPS button (on the back panel of the device).

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



WPS Setup

Enable WPS: Enabled

Add Client(This feature is available only when WPA2 PSK, Mixed WPA/WPA2 PSK or OPEN mode is configured)
○Enter STA PIN ○ Use AP PIN

Device PIN: 66131533

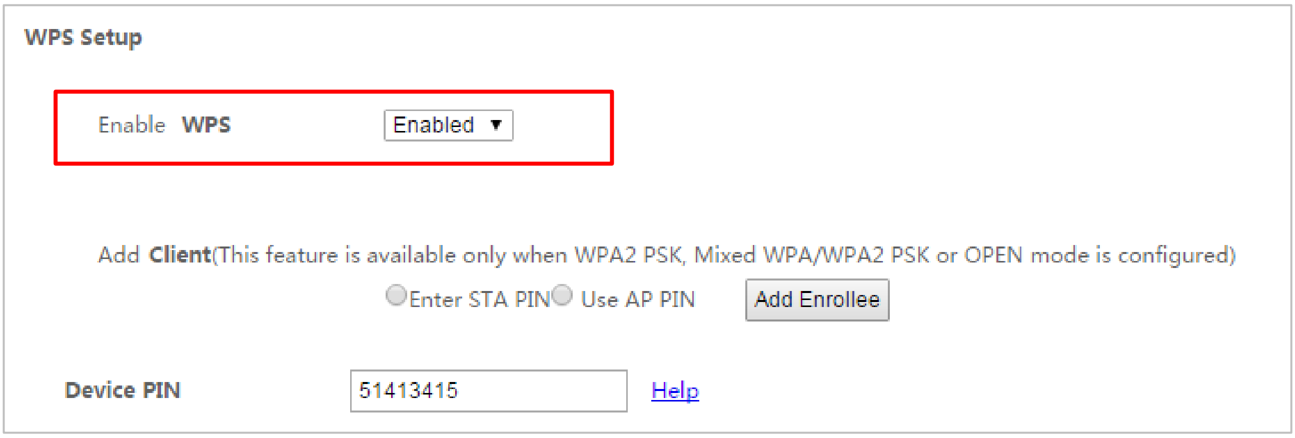
If the wireless network of the modem router is not encrypted, or the wireless network is encrypted, but you forget or do not want to enter the complicated password, you can use WPS function to encrypt or connected to it quickly. There are three options for you:

Option 1: PBC Negotiation

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.



WPS Setup

Enable WPS: Enabled ▼

Add Client(This feature is available only when WPA2 PSK, Mixed WPA/WPA2 PSK or OPEN mode is configured)

○Enter STA PIN○ Use AP PIN

Device PIN: 51413415

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. The SSID and password are changed to random ones.

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.

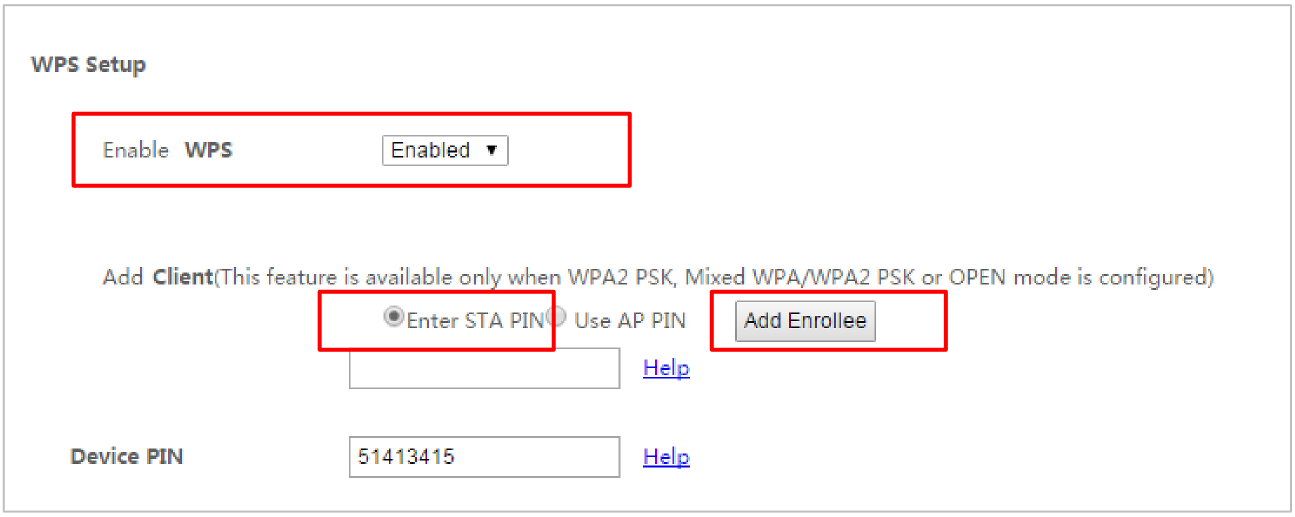
Step 2 Select **Enabled** to enable the function.

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

Step 4 Select **Enter STA PIN**.

Step 5 Enter the WPS PIN code of the wireless device in the box.

Step 6 Click **Add Enrollee**.


WPS Setup

Enable WPS: Enabled ▾

Add Client(This feature is available only when WPA2 PSK, Mixed WPA/WPA2 PSK or OPEN mode is configured)

● Enter STA PIN ○ Use AP PIN [Add Enrollee]

Help

Device PIN: 51413415 Help

--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. The SSID and password are changed to random ones.

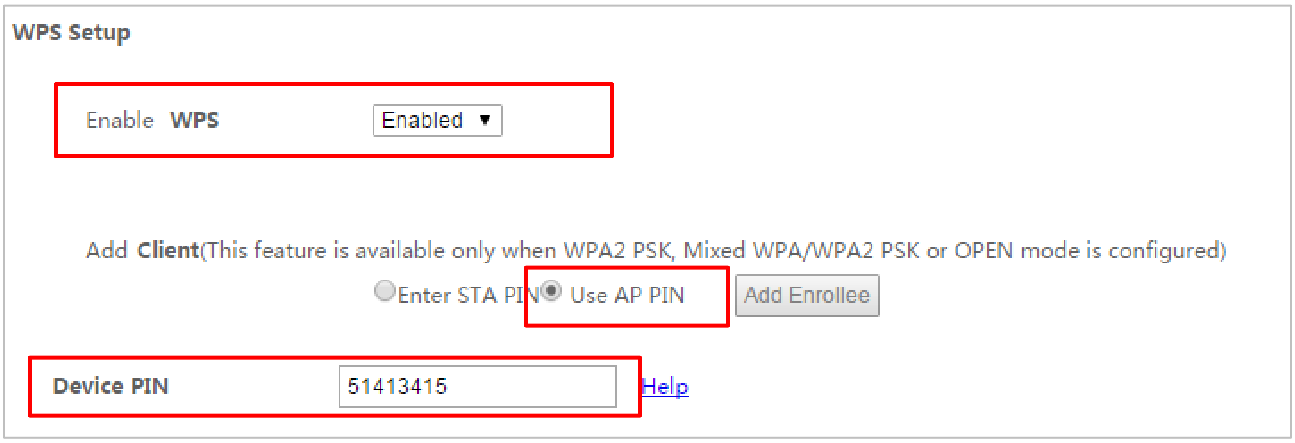
Option 3 Using the WPS PIN Code of the Modem Router

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**.


WPS Setup

Enable WPS: Enabled ▾

Add Client(This feature is available only when WPA2 PSK, Mixed WPA/WPA2 PSK or OPEN mode is configured)

○ Enter STA PIN ● Use AP PIN [Add Enrollee]

Device PIN: 51413415 Help

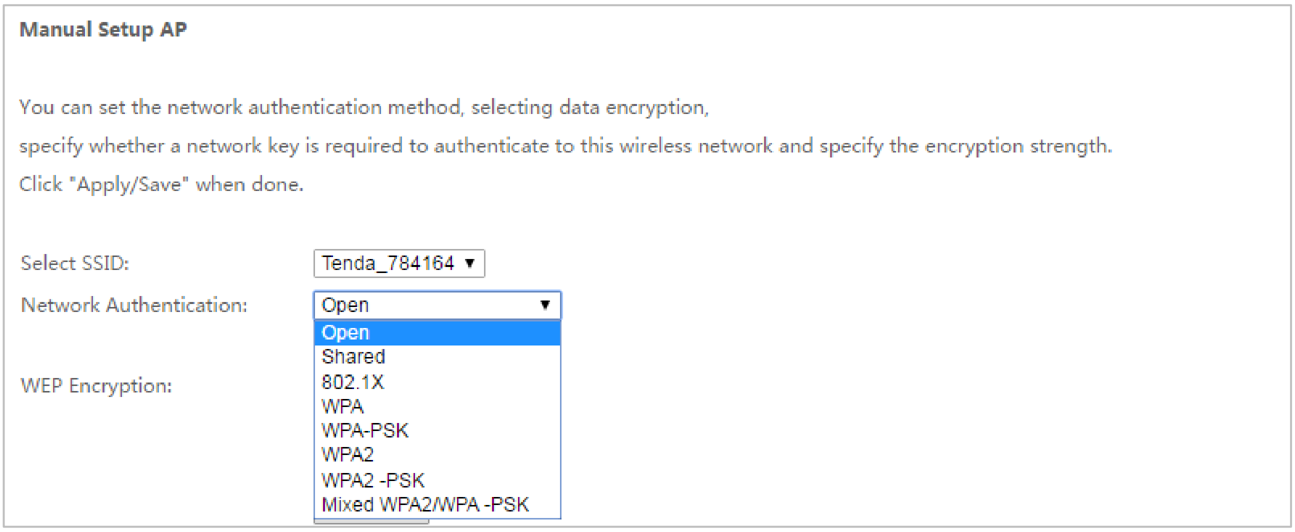
Step 5 Enter the **Device PIN** on your wireless device.

--End

After the negotiation process is successful, 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.



Manual Setup AP

You can set the network authentication method, selecting data encryption,
specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.
Click "Apply/Save" when done.

Select SSID: Tenda_784164

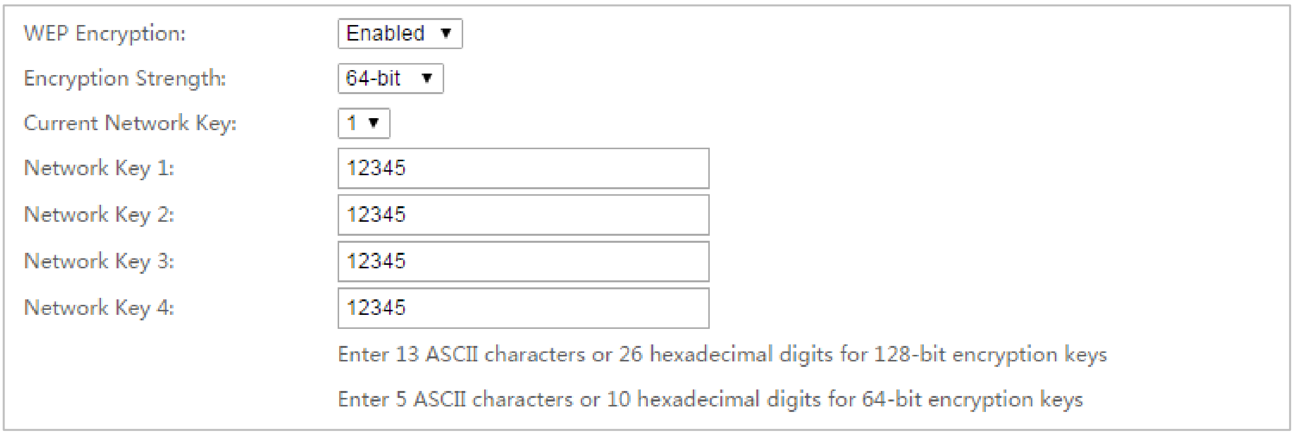
Network Authentication: Open

WEP Encryption:

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. For better network security, this kind of encryption is not suggested.



WEP Encryption: Enabled

Encryption Strength: 64-bit

Current Network Key: 1

Network Key 1: 12345

Network Key 2: 12345

Network Key 3: 12345

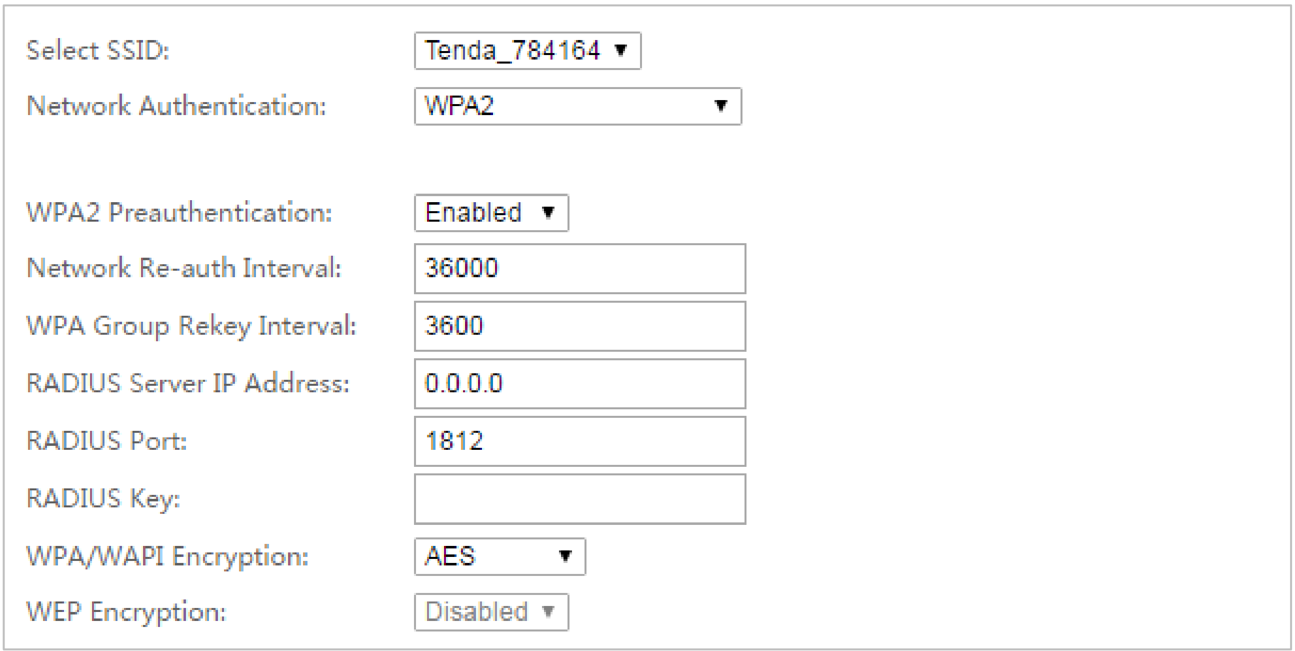
Network Key 4: 12345

Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys

Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys

Parameter	Description
WEP Encryption	When the Open option is selected, you can select to enable/disable WEP encryption. But if Shared or 802.1X option is selected, the WEP encryption is enabled by default.
Encryption Strength	Select 128-bit or 64-bit according to your needs.
Current Network Key	Select a network key to be active.
Network Key 1/2/3/4	Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys; enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.

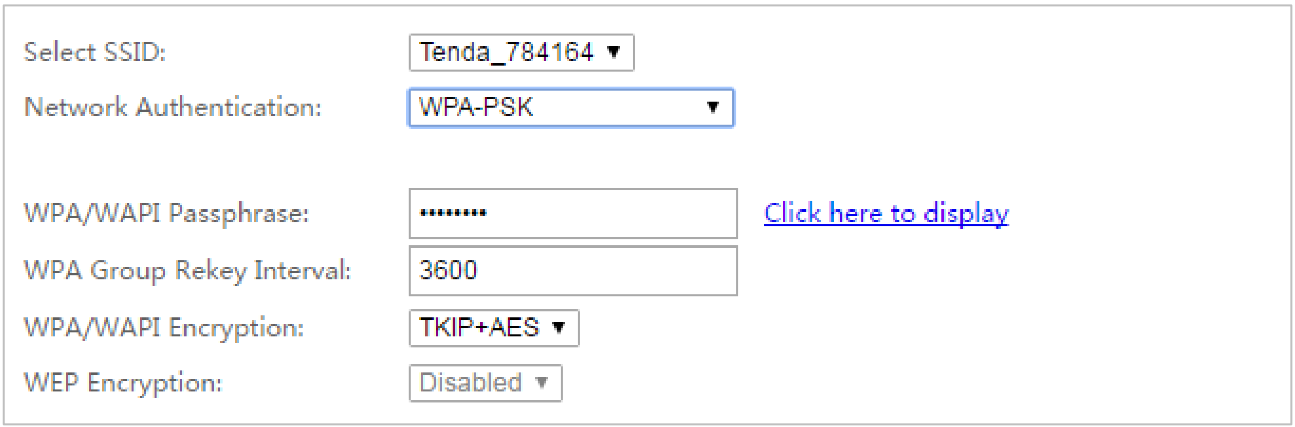
WPA/WPA2



Select SSID:	Tenda_784164 ▼
Network Authentication:	WPA2 ▼
WPA2 Preauthentication:	Enabled ▼
Network Re-auth Interval:	36000
WPA Group Rekey Interval:	3600
RADIUS Server IP Address:	0.0.0.0
RADIUS Port:	1812
RADIUS Key:	
WPA/WAPI Encryption:	AES ▼
WEP Encryption:	Disabled ▼

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. • AES: If selected, the maximum wireless speed can reach 300Mbps. • 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



Select SSID: Tenda_784164

Network Authentication: WPA-PSK

WPA/WAPI Passphrase: ••••••••• Click here to display

WPA Group Rekey Interval: 3600

WPA/WAPI Encryption: TKIP+AES

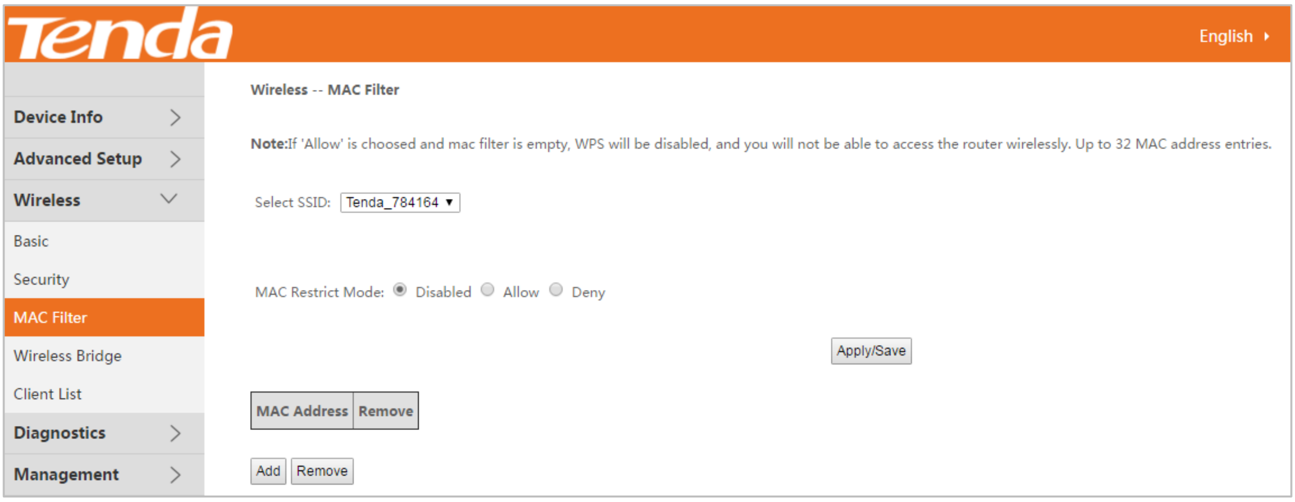
WEP Encryption: Disabled

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. • AES: If selected, the maximum wireless speed can reach 300Mbps. • 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 forbid clients to connect to your wireless network.

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



Wireless -- MAC Filter

Note:If 'Allow' is choosed and mac filter is empty, WPS will be disabled, and you will not be able to access the router wirelessly. Up to 32 MAC address entries.

Select SSID: Tenda_784164

MAC Restrict Mode: ● Disabled ○ Allow ○ Deny

Parameter	Description
Select SSID	Select a SSID to apply the rule. The rule is only applicable to the devices connected to the modem router wirelessly.
MAC Restrict Mode	**Disabled**: Disable this feature.
	Allow: Only allow devices at specified MAC addresses (in the list) to connect to your wireless network.
	Deny: Only forbid devices at 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 applies.
Add	Click the button to add a rule.
Remove	Select a rule you want to remove, and then click the button to remove the rule.

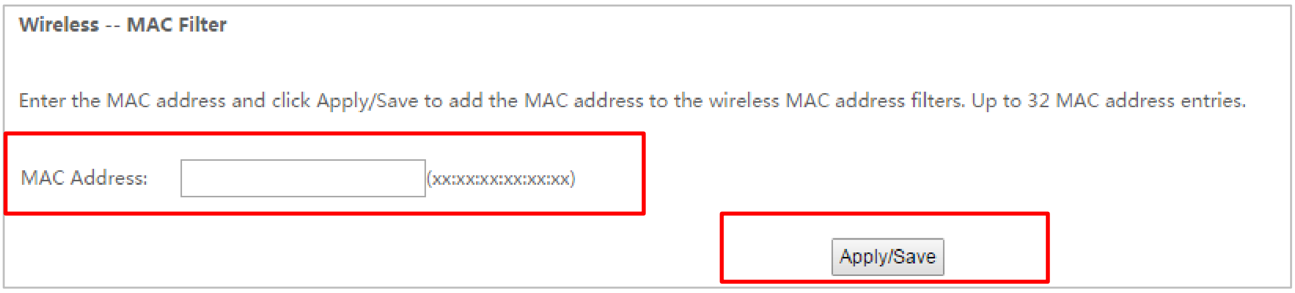
To add a MAC filter rule, perform the following procedure:

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**.



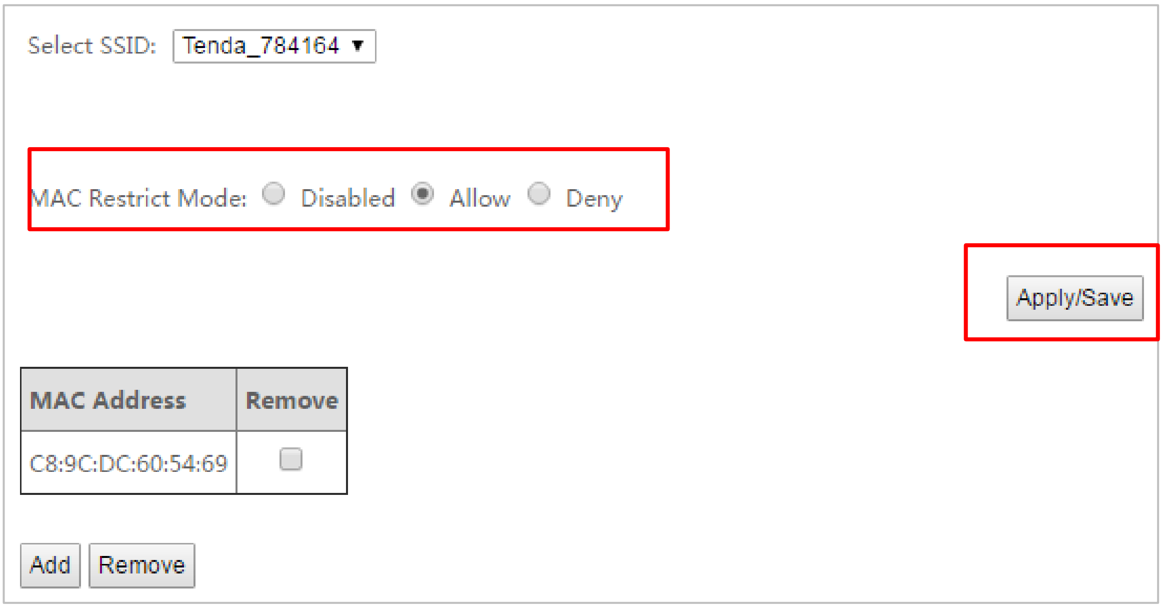
Wireless -- MAC Filter

Enter the MAC address and click Apply/Save to add the MAC address to the wireless MAC address filters. Up to 32 MAC address entries.

MAC Address: (xx:xx:xx:xx:xx:xx)

Step 5 Select Allow or Deny according to your needs.

Step 6 Click **Apply/Save**.



Select SSID: Tenda_784164 ▾

MAC Restrict Mode: ○ Disabled ● Allow ○ Deny

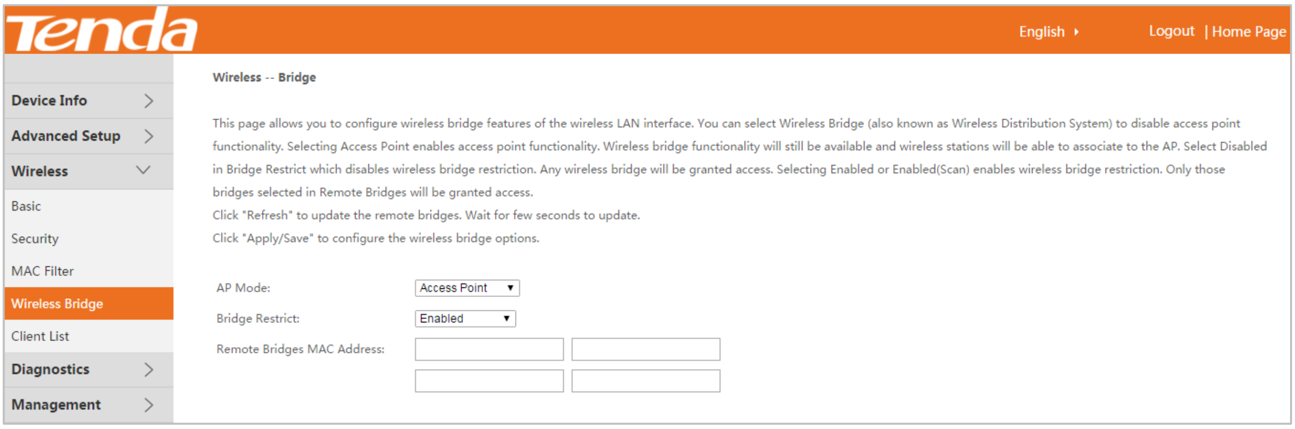
MAC Address	Remove
C8:9C:DC:60:54:69	□

--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.



Wireless -- Bridge

This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disable access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access.

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

Click "Apply/Save" to configure the wireless bridge options.

AP Mode: Access Point ▾

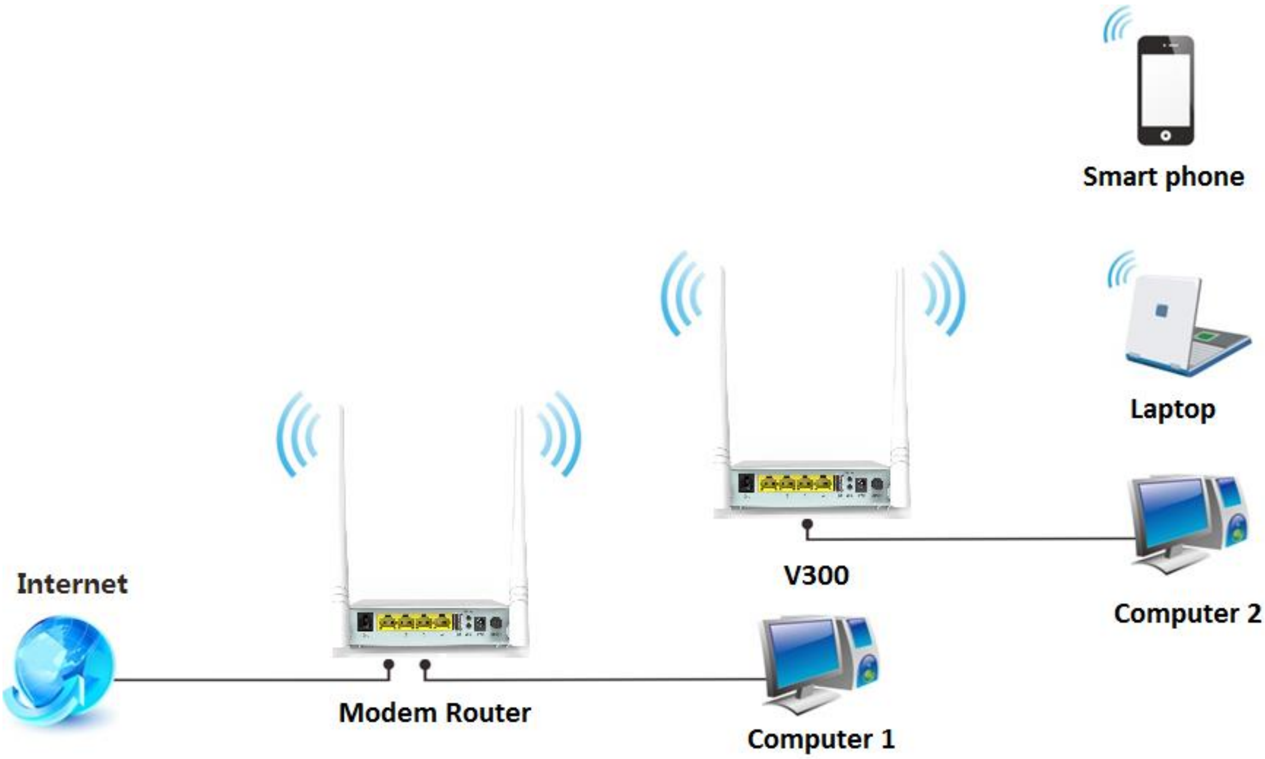
Bridge Restrict: Enabled ▾

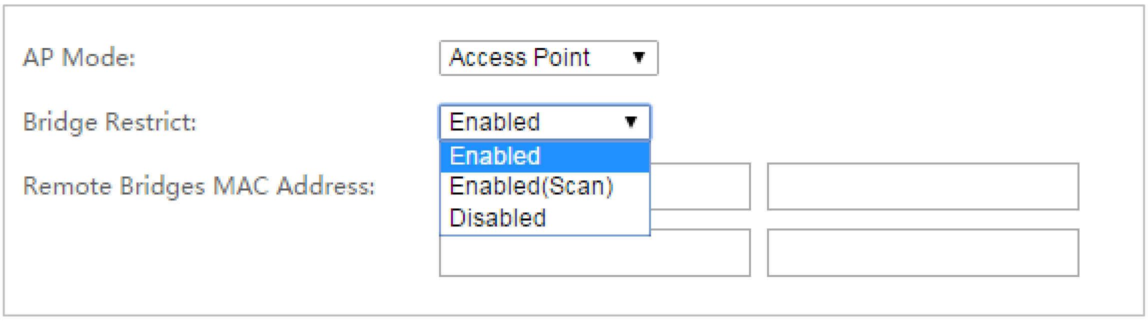
Remote Bridges MAC Address:

Access Point

When the modem router enables access point function, it can extend the wireless network of the upstream wireless router as well as serves as an access point, providing wireless network to wireless devices.

Network Topology:




AP Mode: Access Point

Bridge Restrict: Enabled

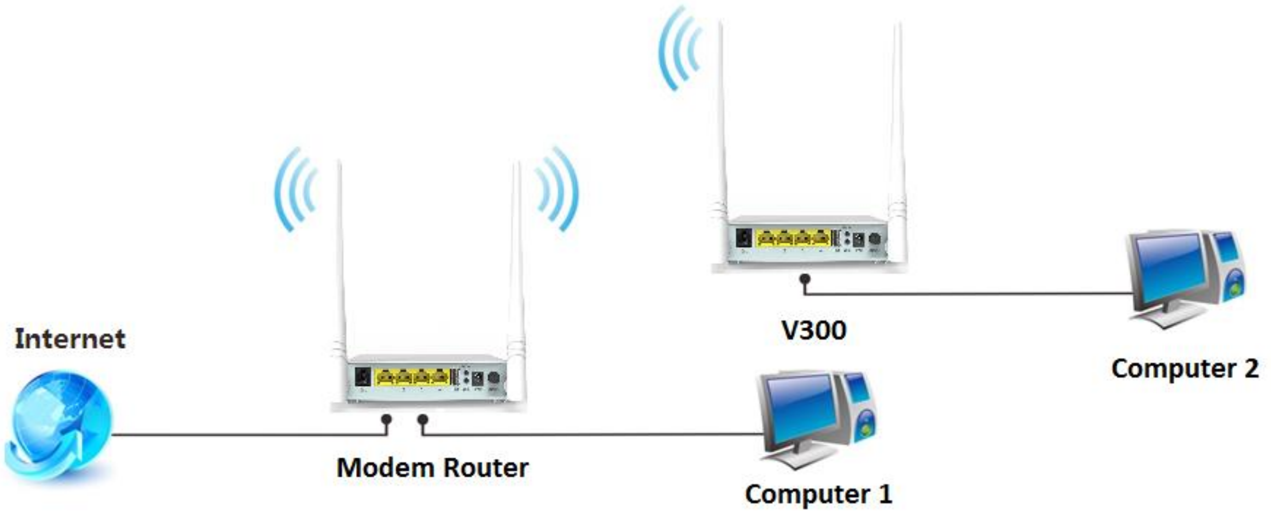
Remote Bridges MAC Address:

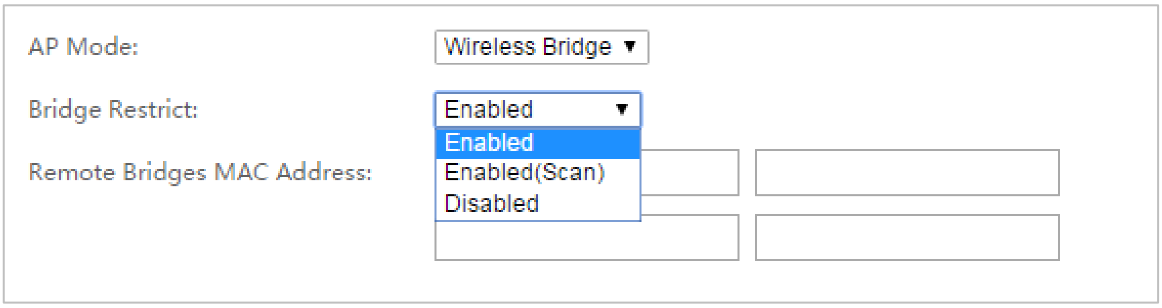
Parameter	Description
AP Mode	It specifies the mode in which the modem router works. The modem router allows you to bridge the maximum of four wireless networks concurrently.
Bridge Restrict	Enabled: Enable the access point function, and you need to manually enter the MAC address of upstream wireless 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	Enter the MAC address of upstream wireless router.

Wireless Bridge

When the modem router enables wireless bridge function, it can extend the wireless network of the upstream wireless router. But the devices can only connect to the modem router using an Ethernet cable for internet access.

Network Topology:





AP Mode:	Wireless Bridge ▼
Bridge Restrict:	Enabled ▼
Remote Bridges MAC Address:	

Parameter	Description
AP Mode	It specifies the mode in which the modem router works. The modem router allows you to bridge the 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 poor in the bedroom and study room to access the internet.

Solution

To improve internet connectivity, 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:

Enable access point function to extend the wireless network.

The wireless information of the upstream wireless router is shown in the following table:

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:

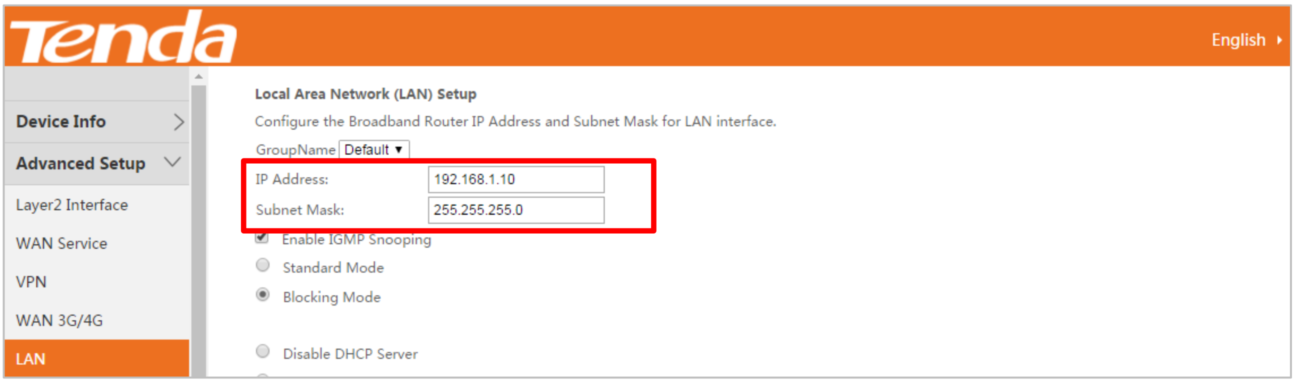
Step 1 Configure the modem router.

1. Set the LAN IP of the modem router to one that is in the same network segment but different from that of the upstream wireless router. For example, the LAN IP of the upstream wireless router is **192.168.1.1**, and then we can 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 the **IP Address** to **192.168.1.10**.

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



Local Area Network (LAN) Setup

Configure the Broadband Router IP Address and Subnet Mask for LAN interface.

GroupName Default

IP Address: 192.168.1.10

Subnet Mask: 255.255.255.0

☑ Enable IGMP Snooping

○ Standard Mode

● Blocking Mode

○ Disable DHCP Server

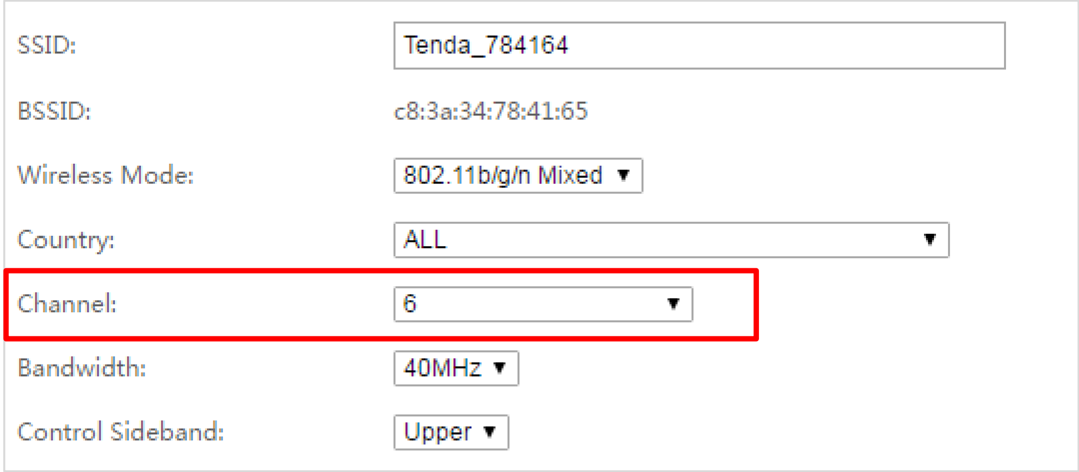
Change the wireless channel, encryption, and password to the same as those of the upstream router.

(4) 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.)

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

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

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



SSID: Tenda_784164

BSSID: c8:3a:34:78:41:65

Wireless Mode: 802.11b/g/n Mixed ▼

Country: ALL ▼

Channel: 6 ▼

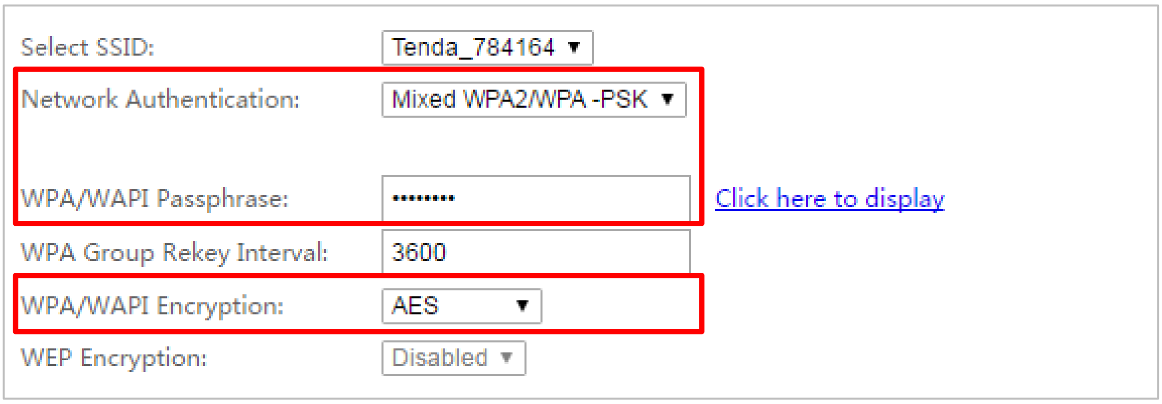
Bandwidth: 40MHz ▼

Control Sideband: Upper ▼

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

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

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



Select SSID: Tenda_784164 ▼

Network Authentication: Mixed WPA2/WPA -PSK ▼

WPA/WAPI Passphrase: •••••••• Click here to display

WPA Group Rekey Interval: 3600

WPA/WAPI Encryption: AES ▼

WEP Encryption: Disabled ▼

Configure the access point function.

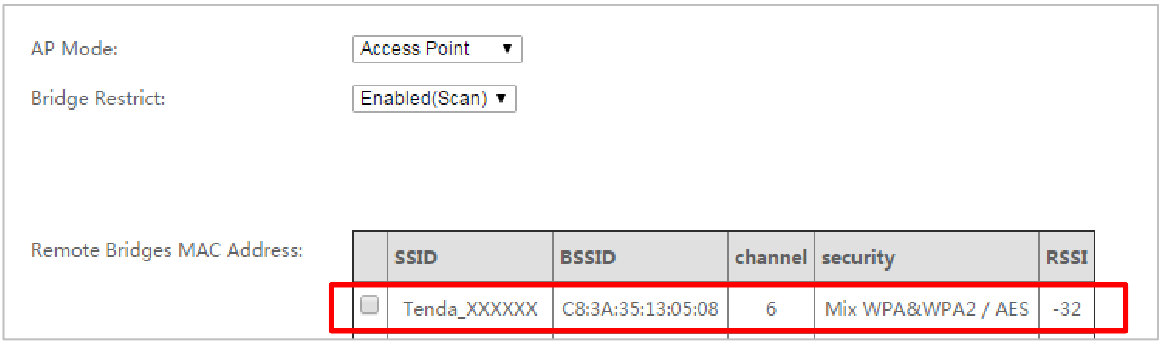
(11) Choose **Advanced** > **Wireless** > **Wireless Bridge** to enter the configuration page.

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

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

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

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



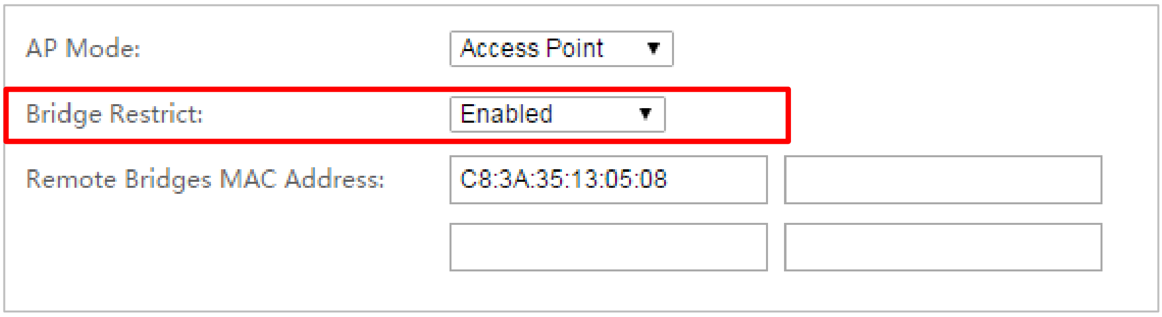
AP Mode: Access Point

Bridge Restrict: Enabled(Scan)

Remote Bridges MAC Address:

	SSID	BSSID	channel	security	RSSI
☐	Tenda_XXXXXX	C8:3A:35:13:05:08	6	Mix WPA&WPA2 / AES	-32

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



AP Mode: Access Point

Bridge Restrict: Enabled

Remote Bridges MAC Address: C8:3A:35:13:05:08

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

Step 2 Configure the upstream router. Perform the steps in step “3”.

--End

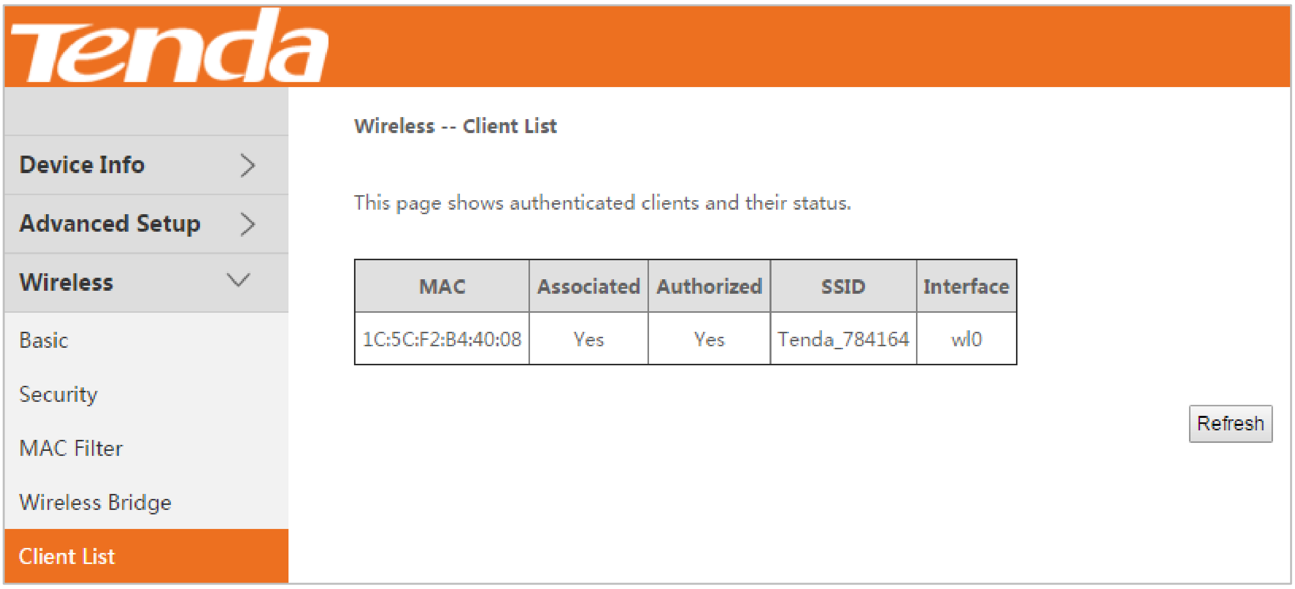
Verification

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 that connected to the wireless networks of the modem router.

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



Wireless -- Client List

This page shows authenticated clients and their status.

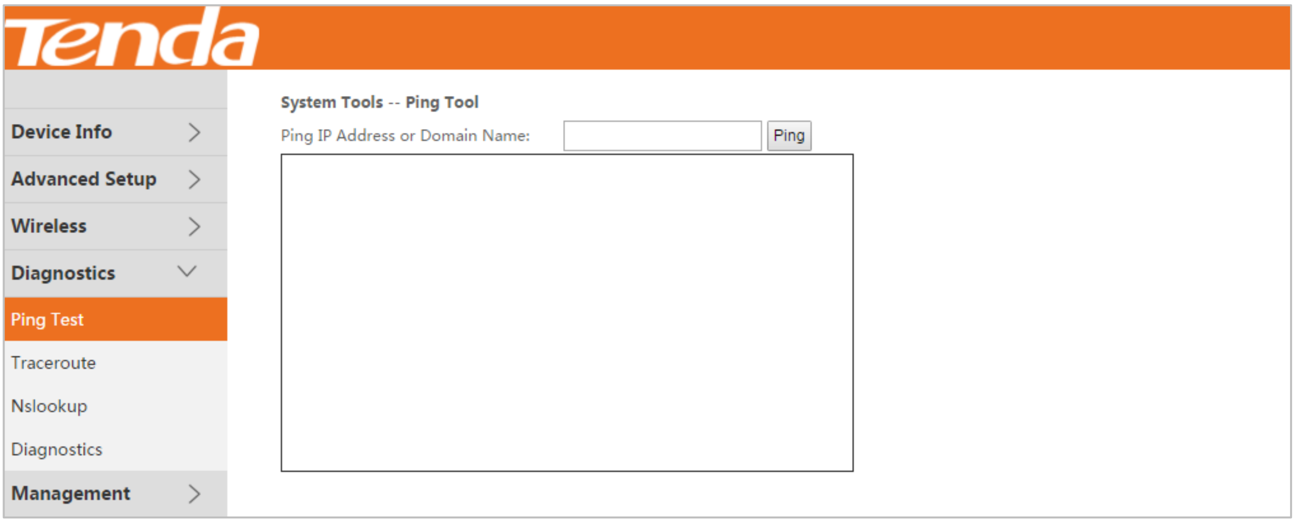
MAC	Associated	Authorized	SSID	Interface
1C:5C:F2:B4:40:08	Yes	Yes	Tenda_784164	wl0

6 Diagnostics

6.1 Ping Test

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

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



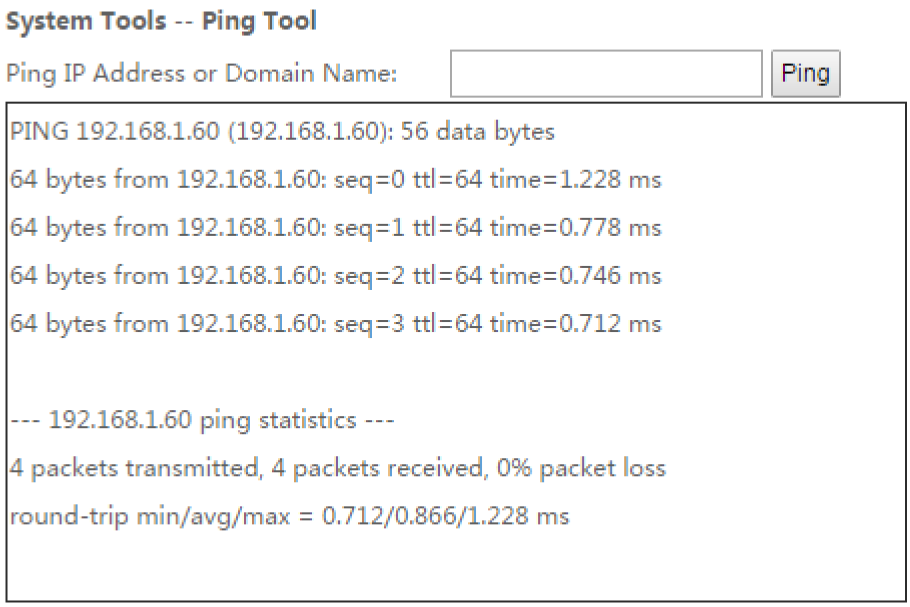
To perform the ping test:

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 screen shown as below, it indicates the connection between the Ping object (Here is 192.168.1.60) and the device has been established.



System Tools -- Ping Tool

Ping IP Address or Domain Name:

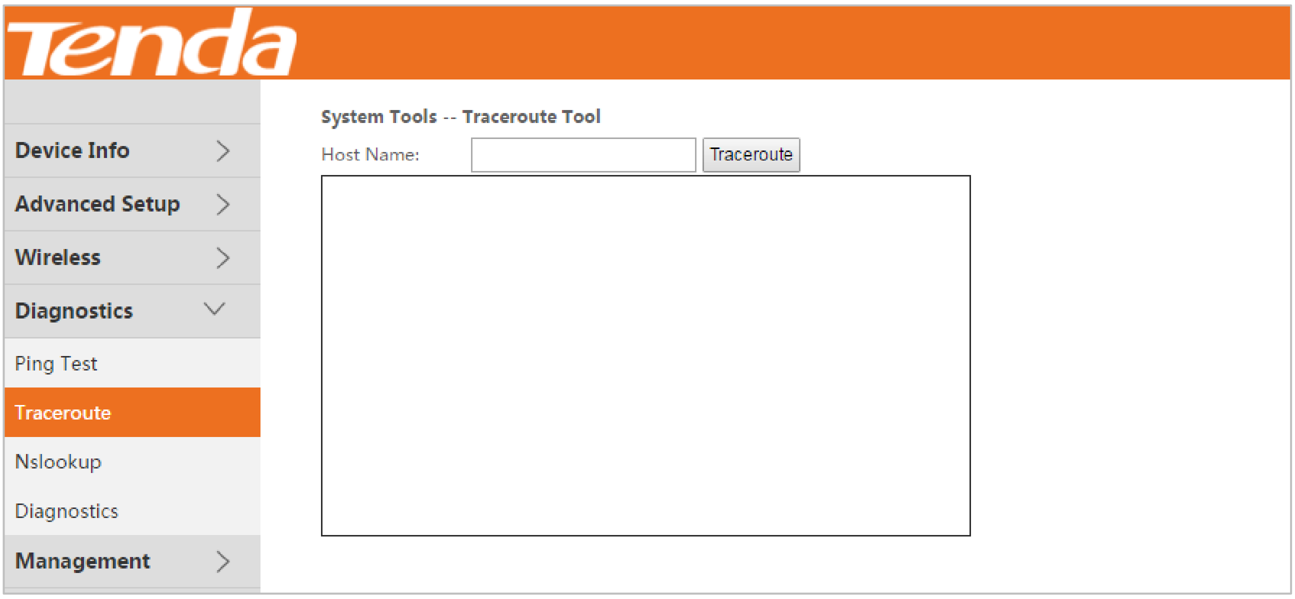
```
PING 192.168.1.60 (192.168.1.60): 56 data bytes
64 bytes from 192.168.1.60: seq=0 ttl=64 time=1.228 ms
64 bytes from 192.168.1.60: seq=1 ttl=64 time=0.778 ms
64 bytes from 192.168.1.60: seq=2 ttl=64 time=0.746 ms
64 bytes from 192.168.1.60: seq=3 ttl=64 time=0.712 ms

--- 192.168.1.60 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.712/0.866/1.228 ms
```

6.2 Traceroute

Traceroute helps you check the specific routes to a host.

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



System Tools -- Traceroute Tool

Host Name:

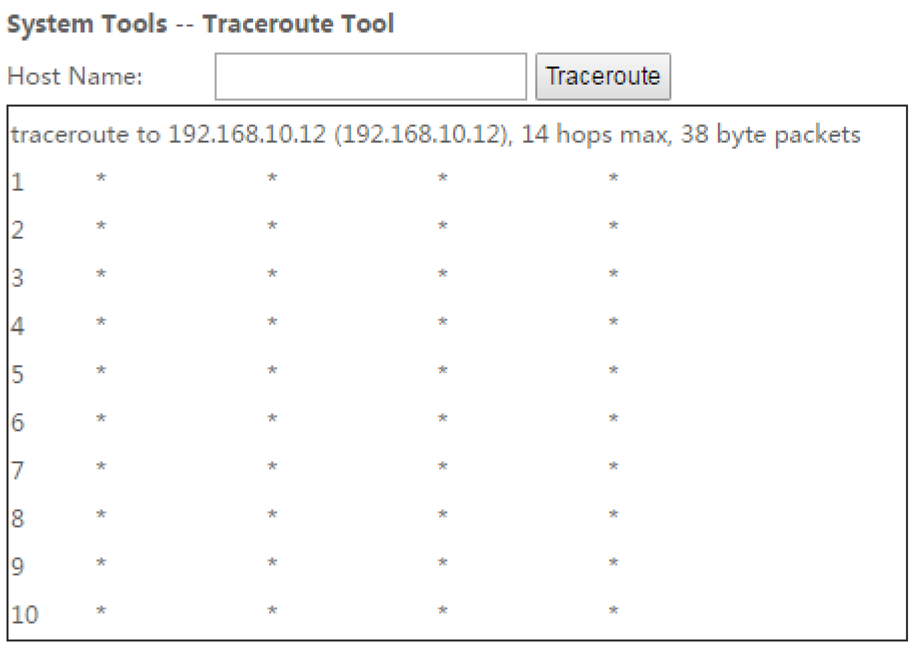
To perform the traceroute:

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.



System Tools -- Traceroute Tool

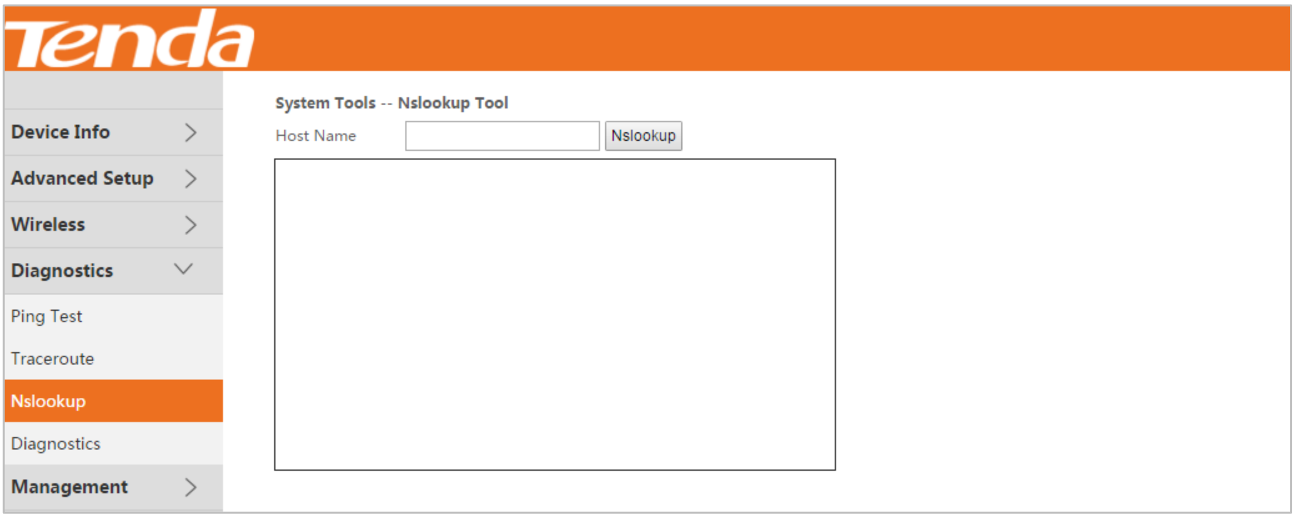
Host Name:

```
traceroute to 192.168.10.12 (192.168.10.12), 14 hops max, 38 byte packets
1    *    *    *    *
2    *    *    *    *
3    *    *    *    *
4    *    *    *    *
5    *    *    *    *
6    *    *    *    *
7    *    *    *    *
8    *    *    *    *
9    *    *    *    *
10   *    *    *    *
```

6.3 Nslookup

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

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



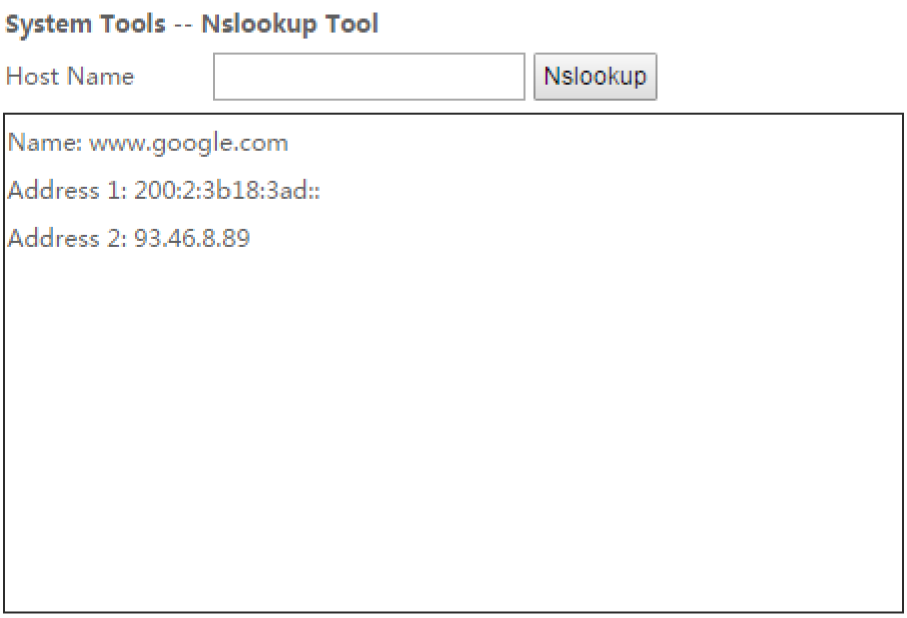
To translate a domain name, to perform the following procedure:

Step 1 Enter a domain name in the **Host Name** field.

Step 2 Click **Nslookup**.

--End

Then you can check the result.



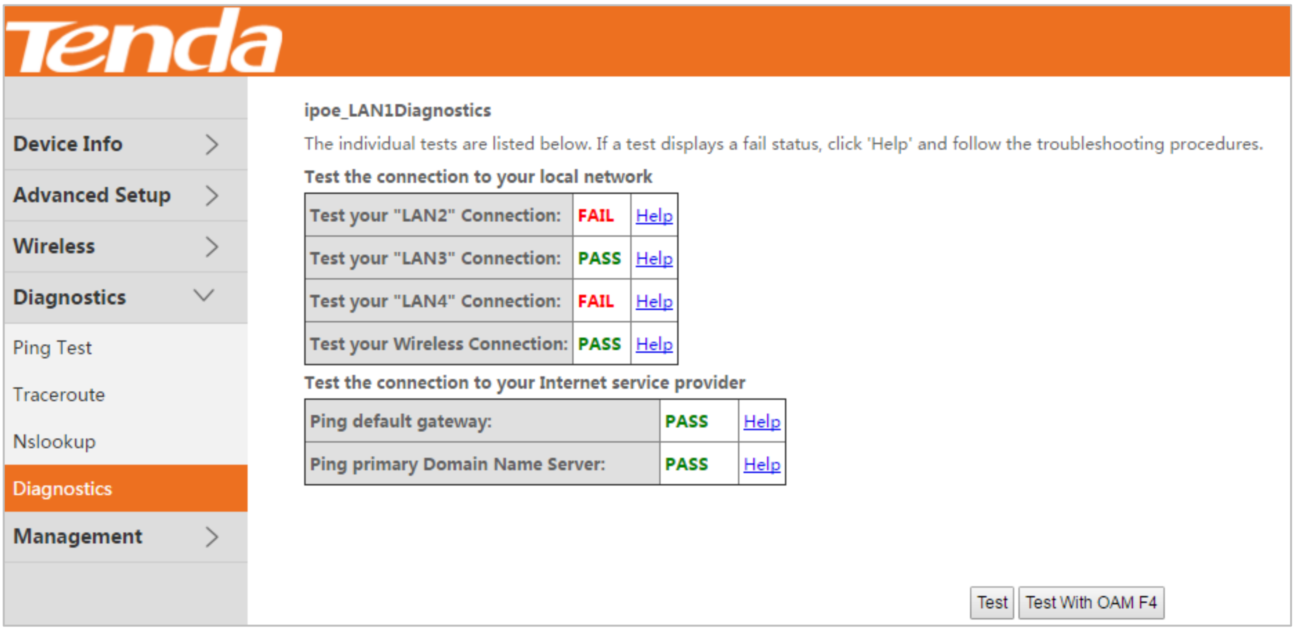
System Tools -- Nslookup Tool

Host Name

```
Name: www.google.com
Address 1: 200:2:3b18:3ad::
Address 2: 93.46.8.89
```

6.4 Diagnostics

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



ipoe_LAN1Diagnostics

The individual tests are listed below. If a test displays a fail status, click 'Help' and follow the troubleshooting procedures.

Test the connection to your local network

Test your "LAN2" Connection:	FAIL	Help
Test your "LAN3" Connection:	PASS	Help
Test your "LAN4" Connection:	FAIL	Help
Test your Wireless Connection:	PASS	Help

Test the connection to your Internet service provider

Ping default gateway:	PASS	Help
Ping primary Domain Name Server:	PASS	Help

7 Management

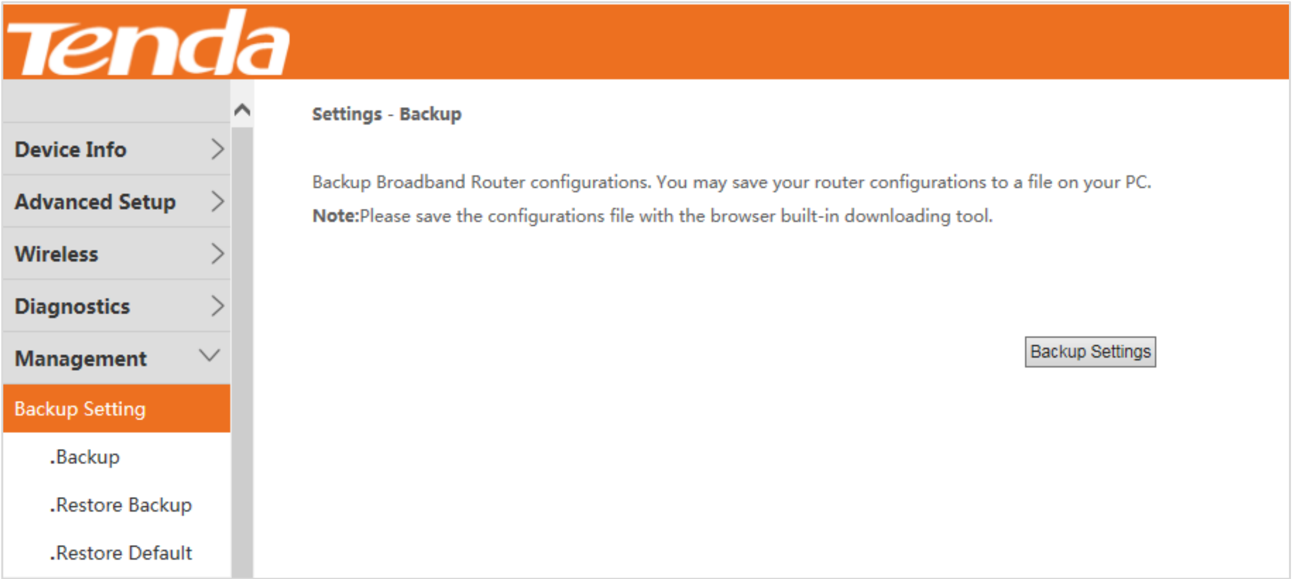
7.1 Backup Settings

Here you can backup 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.



Settings - Backup

Backup Broadband Router configurations. You may save your router configurations to a file on your PC.

Note: Please save the configurations file with the browser built-in downloading tool.

To back up the settings, perform the following procedure:

Step 1 Click **Backup Settings**.

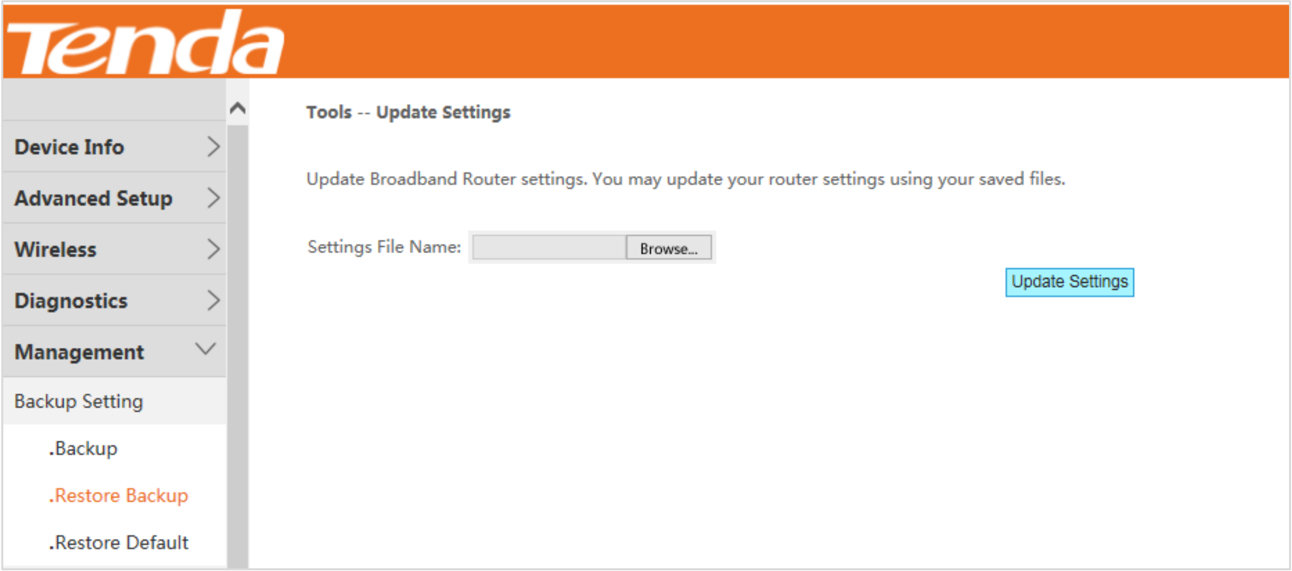
Step 2 Follow the on-screen instructions to save the file to a local path.

---End

7.1.2 Restore

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.



Tools -- Update Settings

Update Broadband Router settings. You may update your router settings using your saved files.

Settings File Name:

To restore the settings, perform the following procedure:

Step 1 Click **Browse**.

Step 2 Select a configuration file on your PC.

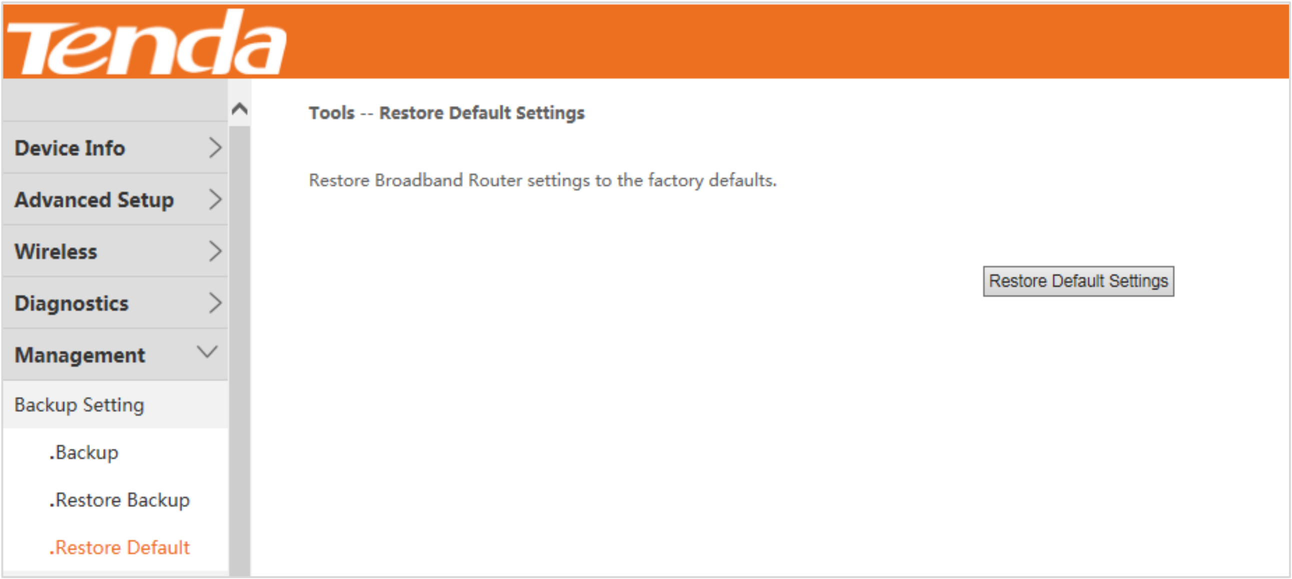
Step 3 Click **Update Settings**.

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.



Tools -- Restore Default Settings

Restore Broadband Router settings to the factory defaults.

To restore the settings, perform the following procedure:

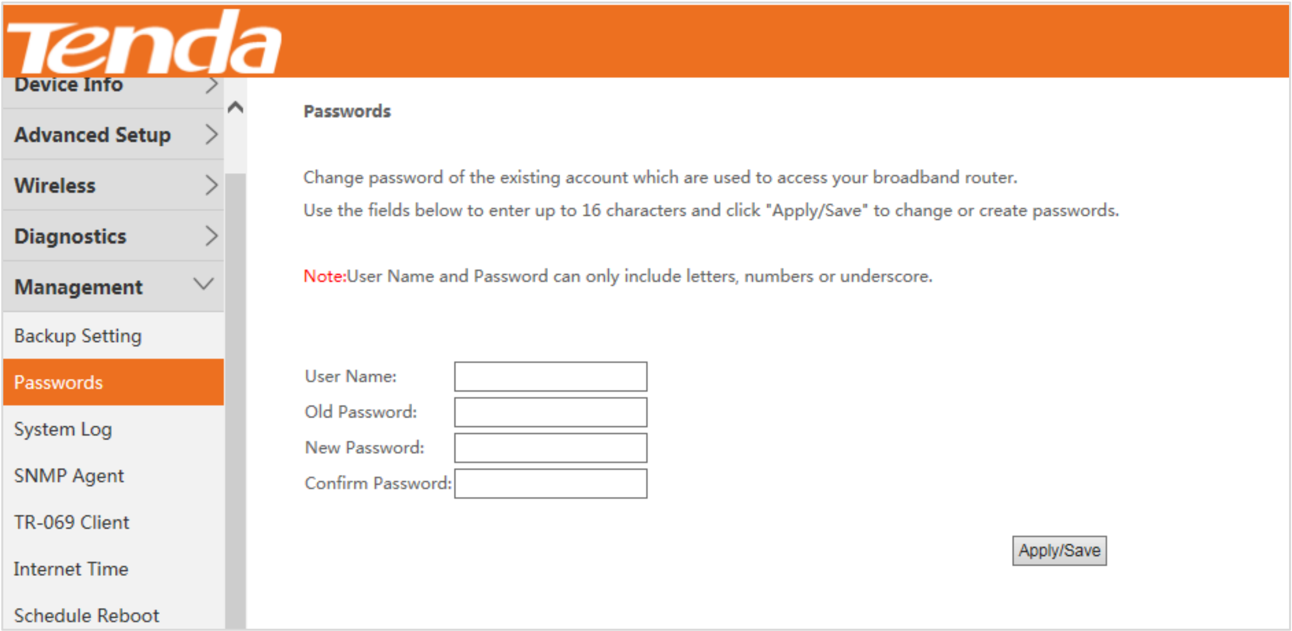
Step 1 Click **Restore Default Settings**.

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.



Passwords

Change password of the existing account which are used to access your broadband router.
Use the fields below to enter up to 16 characters and click "Apply/Save" to change or create passwords.

Note:User Name and Password can only include letters, numbers or underscore.

User Name:
Old Password:
New Password:
Confirm Password:

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**.

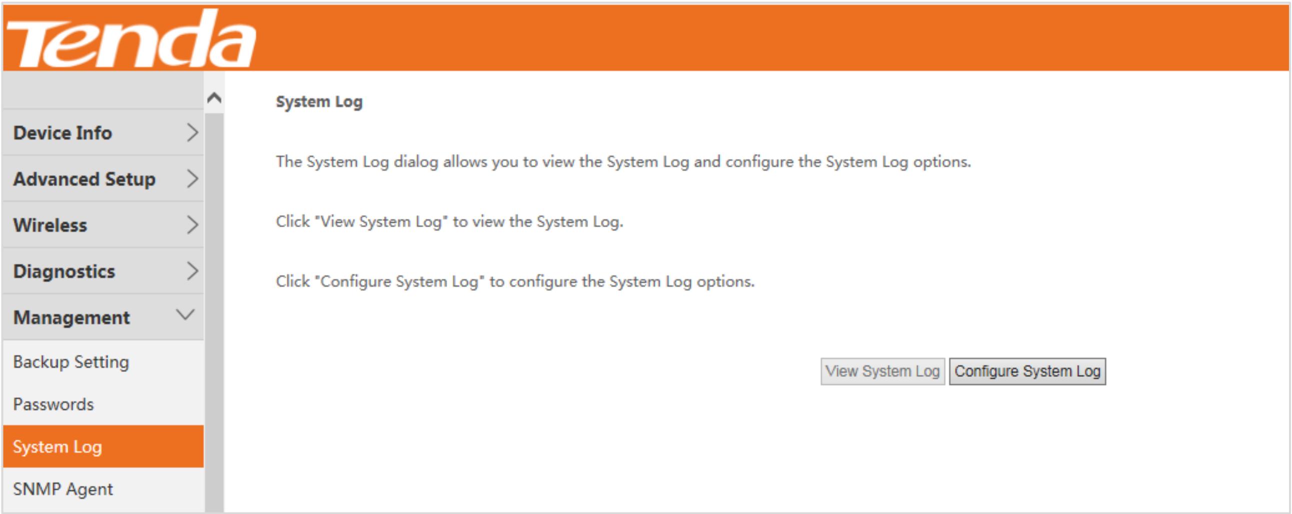
Step 4 Set **Confirm Password** to the same value as **New Password**.

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.



System Log

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

Click "View System Log" to view the System Log.

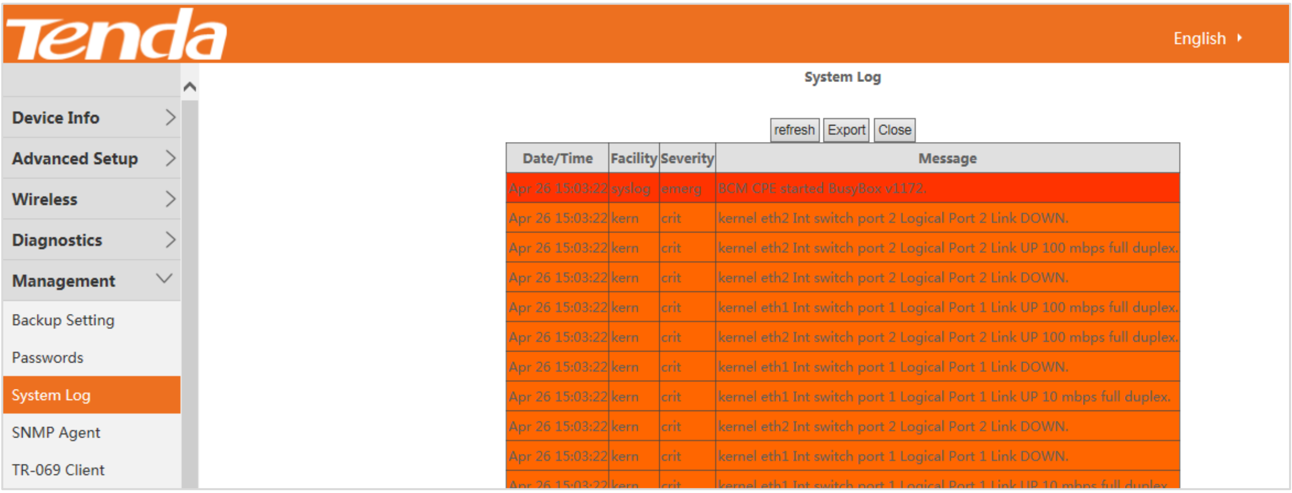
Click "Configure System Log" to configure the System Log options.

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**.



System Log

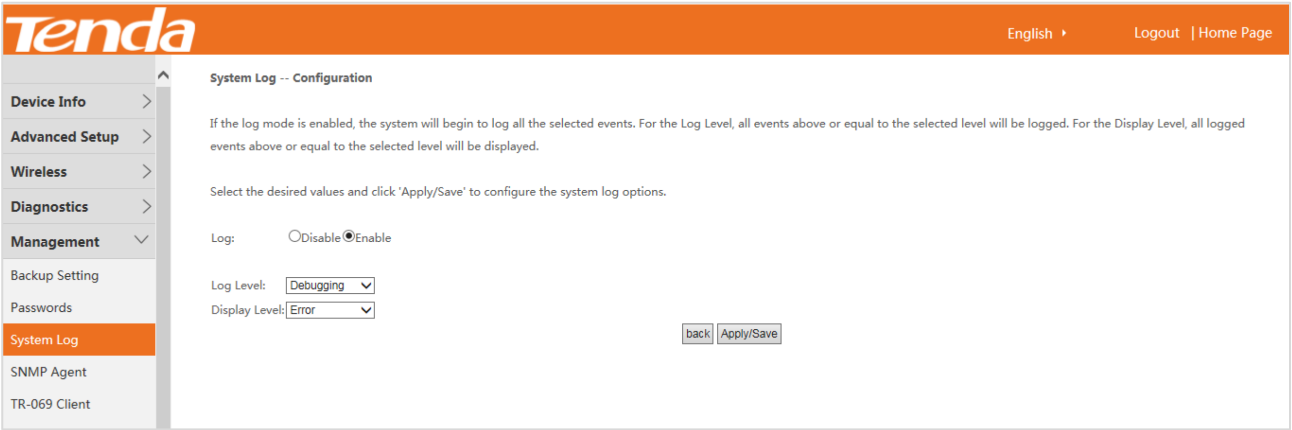
Date/Time	Facility	Severity	Message
Apr 26 15:03:22	syslog	emerg	BCM CPE started BusyBox v1172.
Apr 26 15:03:22	kern	crit	kernel eth2 Int switch port 2 Logical Port 2 Link DOWN.
Apr 26 15:03:22	kern	crit	kernel eth2 Int switch port 2 Logical Port 2 Link UP 100 mbps full duplex.
Apr 26 15:03:22	kern	crit	kernel eth2 Int switch port 2 Logical Port 2 Link DOWN.
Apr 26 15:03:22	kern	crit	kernel eth1 Int switch port 1 Logical Port 1 Link UP 100 mbps full duplex.
Apr 26 15:03:22	kern	crit	kernel eth2 Int switch port 2 Logical Port 2 Link UP 100 mbps full duplex.
Apr 26 15:03:22	kern	crit	kernel eth1 Int switch port 1 Logical Port 1 Link DOWN.
Apr 26 15:03:22	kern	crit	kernel eth1 Int switch port 1 Logical Port 1 Link UP 10 mbps full duplex.
Apr 26 15:03:22	kern	crit	kernel eth2 Int switch port 2 Logical Port 2 Link DOWN.
Apr 26 15:03:22	kern	crit	kernel eth1 Int switch port 1 Logical Port 1 Link DOWN.
Apr 26 15:03:22	kern	crit	kernel eth1 Int switch port 1 Logical Port 1 Link UP 10 mbps full duplex.

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.



System Log -- Configuration

If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed.

Select the desired values and click 'Apply/Save' to configure the system log options.

Log: ○Disable ●Enable

Log Level: Debugging

Display Level: Error

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.

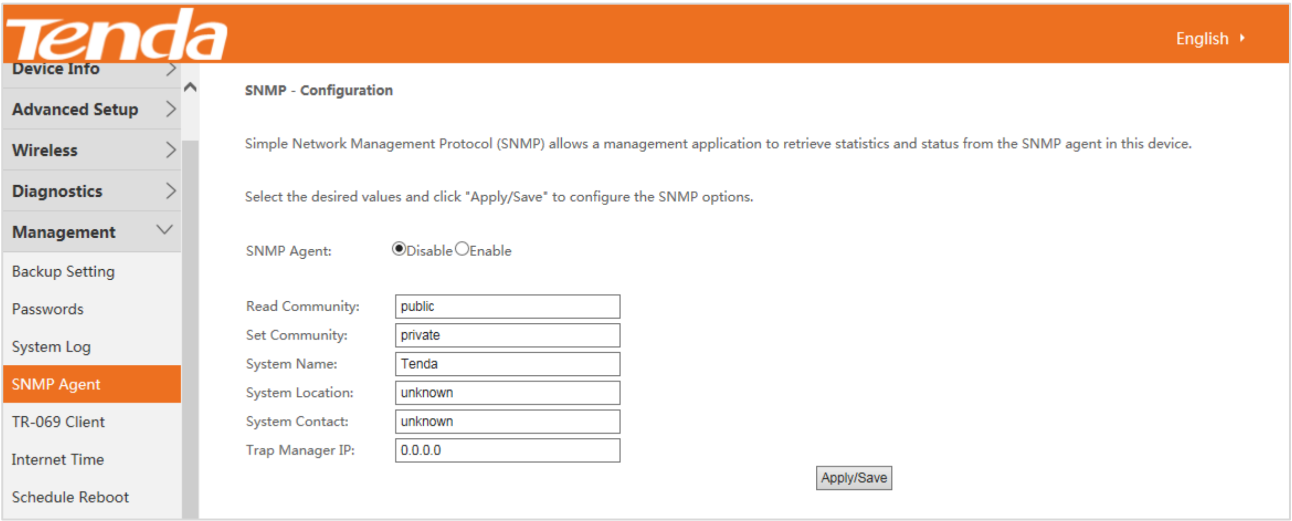
Step 4 Click **Apply/Save**.

---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.



SNMP - Configuration

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

Select the desired values and click "Apply/Save" to configure the SNMP options.

SNMP Agent: ●Disable ○Enable

Read Community: public

Set Community: private

System Name: Tenda

System Location: unknown

System Contact: unknown

Trap Manager IP: 0.0.0.0

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.

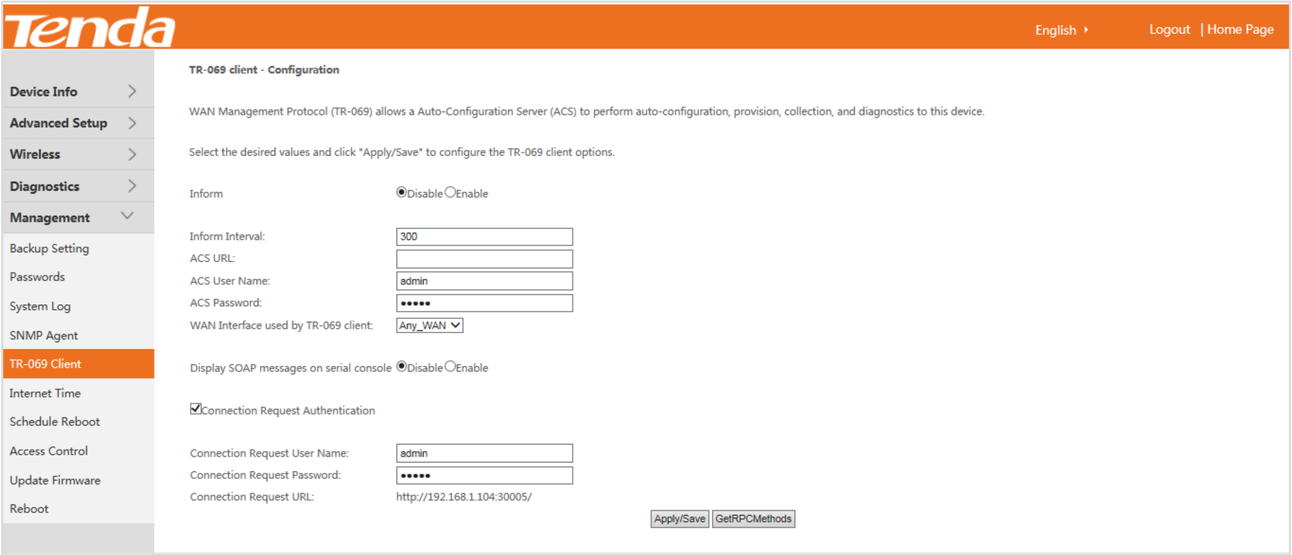
Step 7 Set **Trap Manager IP** to the IP address of the Trap Manager.

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.



TR-069 client - Configuration

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

Select the desired values and click "Apply/Save" to configure the TR-069 client options.

Inform ● Disable ○ Enable

Inform Interval: 300
ACS URL:
ACS User Name: admin
ACS Password: •••••
WAN Interface used by TR-069 client: Any_WAN

Display SOAP messages on serial console ● Disable ○ Enable

☑ Connection Request Authentication

Connection Request User Name: admin
Connection Request Password: •••••
Connection Request URL: http://192.168.1.104:30005/

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:

Set **Connection Request User Name** to the user name for connection request authentication.

Set **Connection Request Password** to the password for connection request authentication.

Set **Connection Request URL** to the URL for connection request authentication.

Step 9 Click **Apply/Save**.

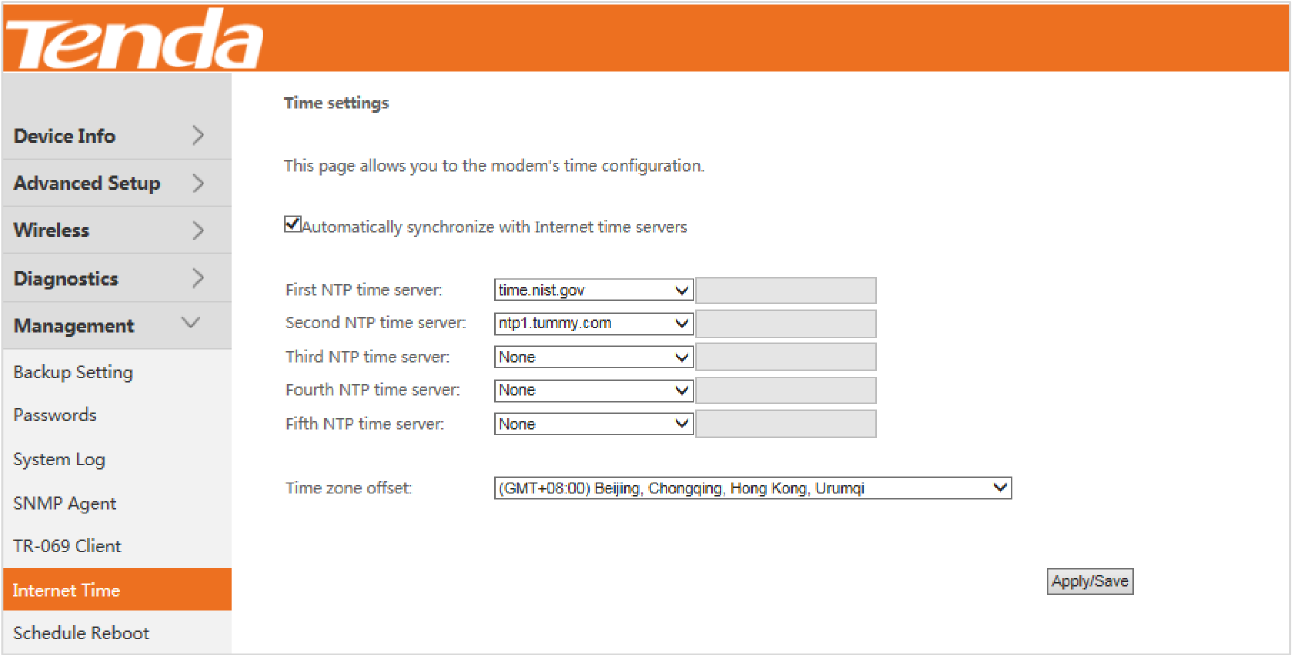
---End

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.



Time settings

This page allows you to the modem's time configuration.

☑ Automatically synchronize with Internet time servers

First NTP time server: time.nist.gov
Second NTP time server: ntp1.tummy.com
Third NTP time server: None
Fourth NTP time server: None
Fifth NTP time server: None

Time zone offset: (GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi

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.

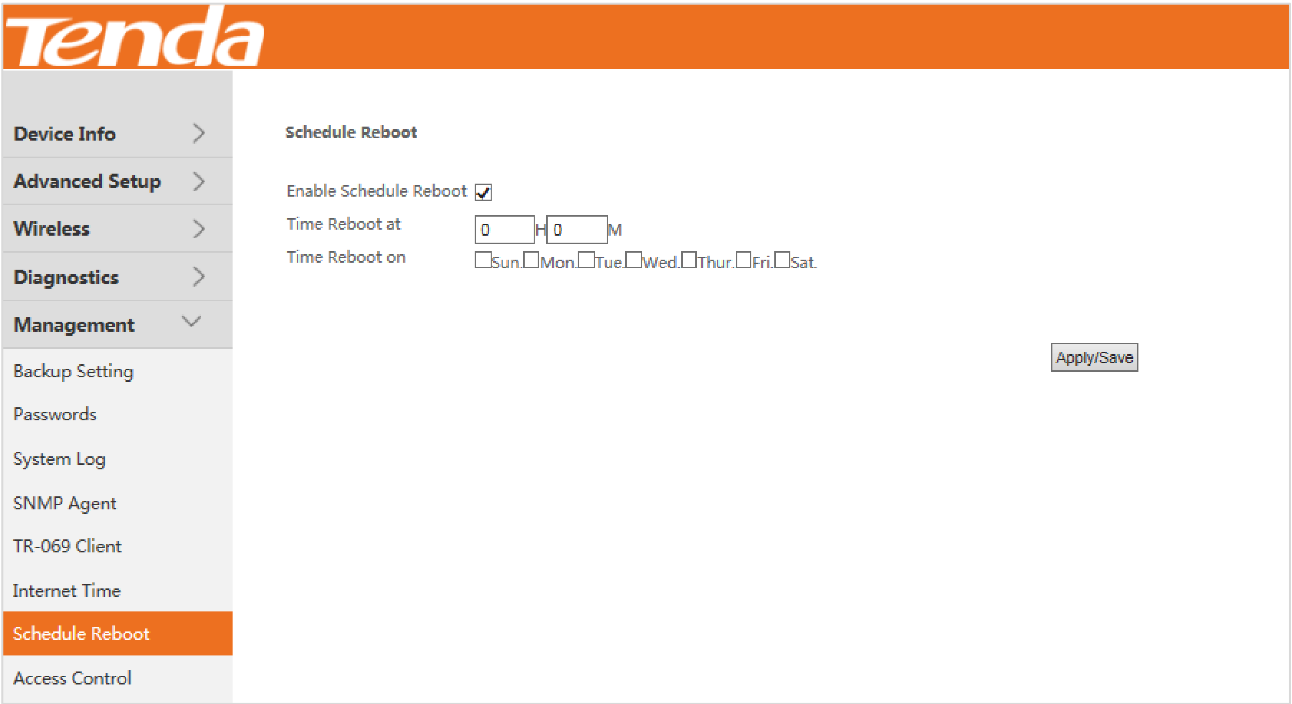
Step 7 Select your time zone from the **Time zone offset** drop-down list box.

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.



Schedule Reboot

Enable Schedule Reboot ☑

Time Reboot at 0 H 0 M

Time Reboot on □Sun □Mon □Tue □Wed □Thur □Fri □Sat

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.

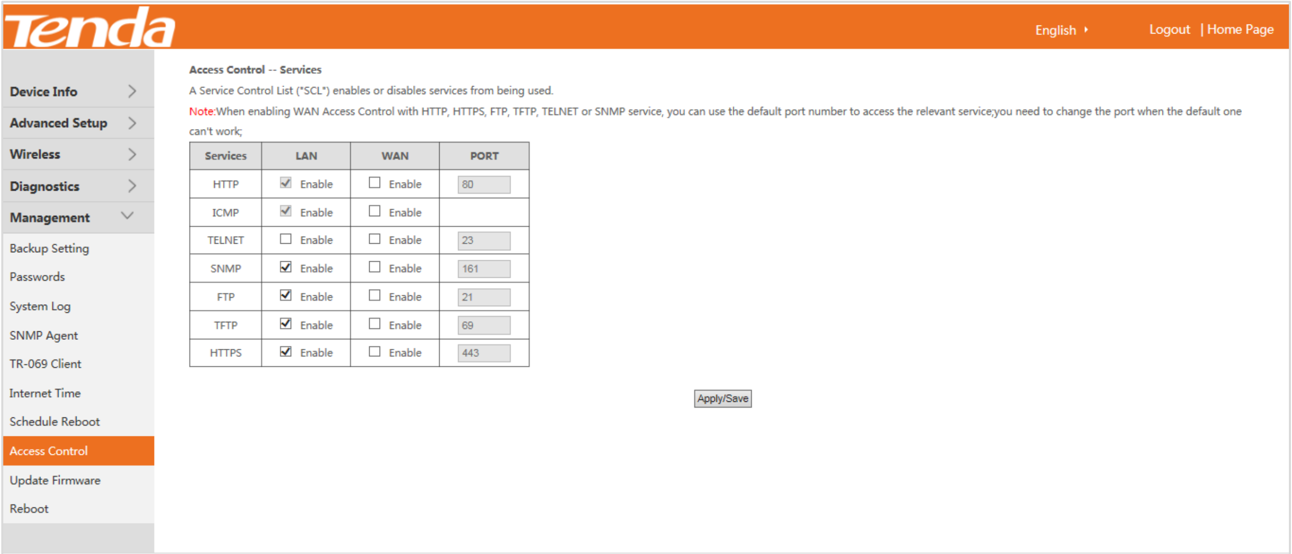
Step 3 Set **Time Reboot On** to the days when you want the device to reboot.

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.



Access Control -- Services

A Service Control List ("SCL") enables or disables services from being used.

Note:When enabling WAN Access Control with HTTP, HTTPS, FTP, TFTP, TELNET or SNMP service, you can use the default port number to access the relevant service;you need to change the port when the default one can't work;

Services	LAN	WAN	PORT
HTTP	☑ Enable	□ Enable	80
ICMP	☑ Enable	□ Enable	
TELNET	□ Enable	□ Enable	23
SNMP	☑ Enable	□ Enable	161
FTP	☑ Enable	□ Enable	21
TFTP	☑ Enable	□ Enable	69
HTTPS	☑ Enable	□ Enable	443

To control service accessibility, perform the following procedure:

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

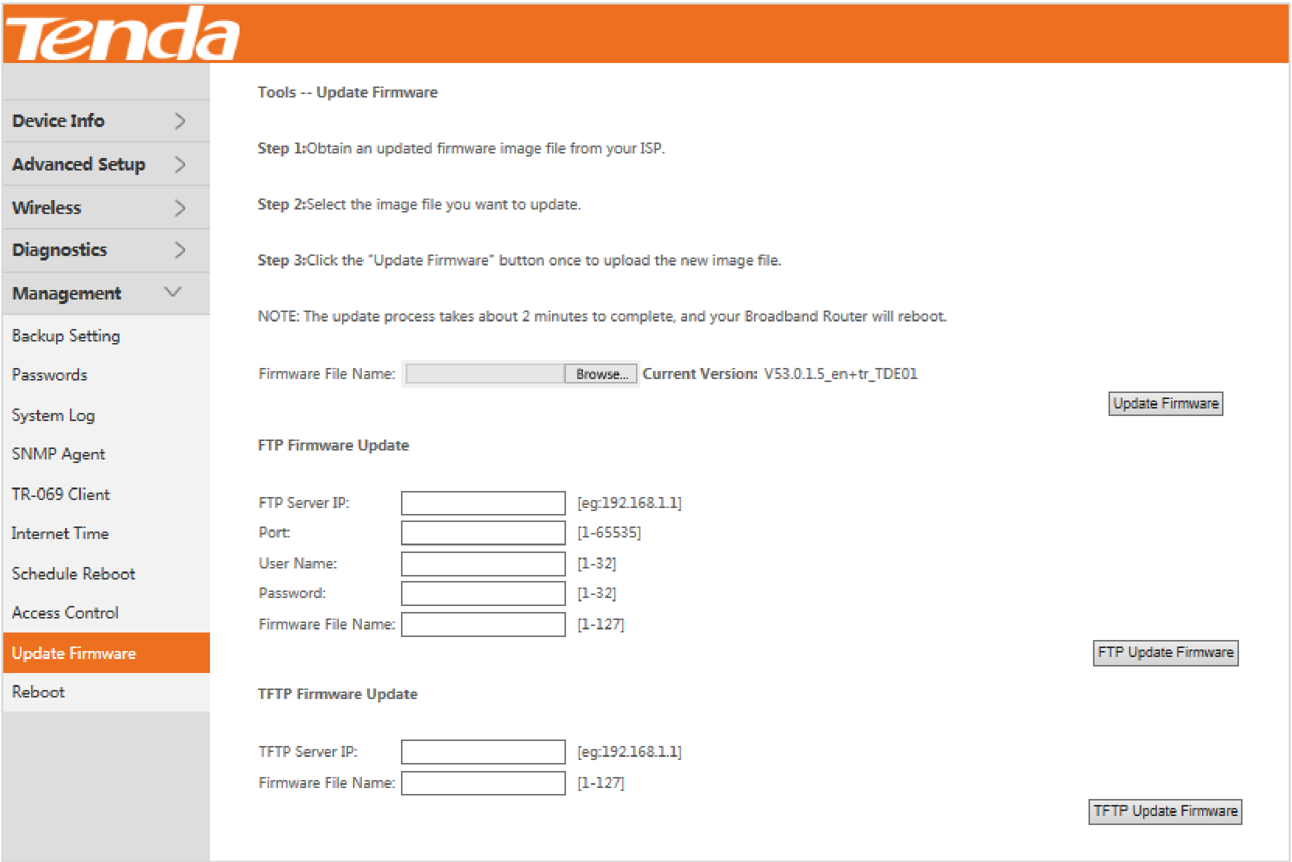
Step 2 Change the default ports if they are being used.

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.



Tools -- Update Firmware

Step 1: Obtain an updated firmware image file from your ISP.

Step 2: Select the image file you want to update.

Step 3: Click the "Update Firmware" button once to upload the new image file.

NOTE: The update process takes about 2 minutes to complete, and your Broadband Router will reboot.

Firmware File Name: **Current Version:** V53.0.1.5_en+tr_TDE01

FTP Firmware Update

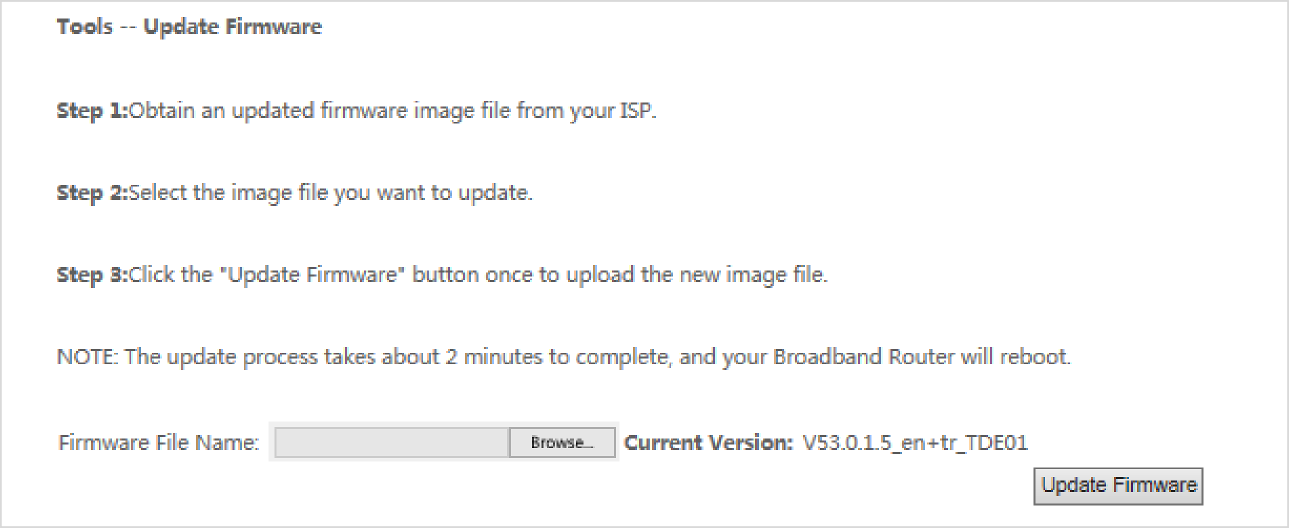
FTP Server IP: [eg:192.168.1.1]
Port: [1-65535]
User Name: [1-32]
Password: [1-32]
Firmware File Name: [1-127]

TFTP Firmware Update

TFTP Server IP: [eg:192.168.1.1]
Firmware File Name: [1-127]

7.9.1 Upgrading the Firmware Locally

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



Tools -- Update Firmware

Step 1: Obtain an updated firmware image file from your ISP.

Step 2: Select the image file you want to update.

Step 3: Click the "Update Firmware" button once to upload the new image file.

NOTE: The update process takes about 2 minutes to complete, and your Broadband Router will reboot.

Firmware File Name: **Current Version:** V53.0.1.5_en+tr_TDE01

To upgrade the firmware locally, perform the following procedure:

Step 1 Click **Browse**.

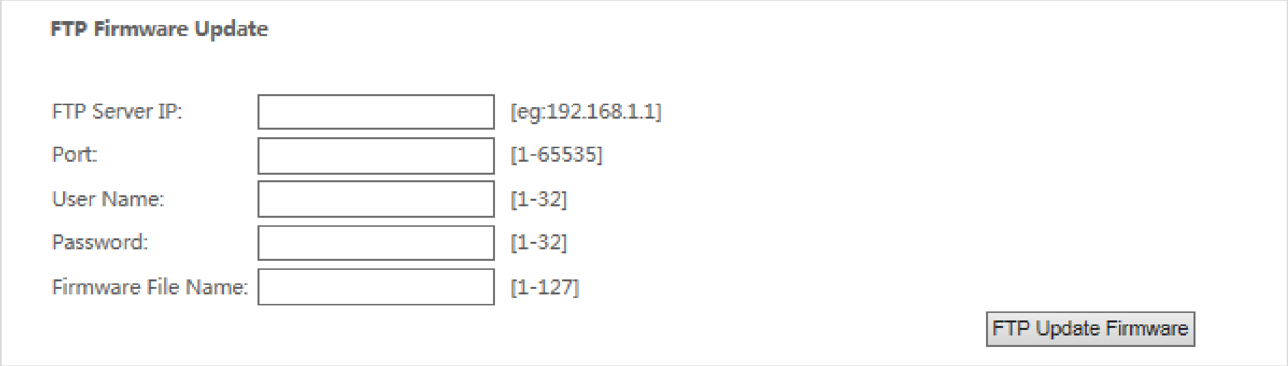
Step 2 Select the firmware downloaded to your PC.

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.



FTP Firmware Update

FTP Server IP:		[eg:192.168.1.1]
Port:		[1-65535]
User Name:		[1-32]
Password:		[1-32]
Firmware File Name:		[1-127]

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.

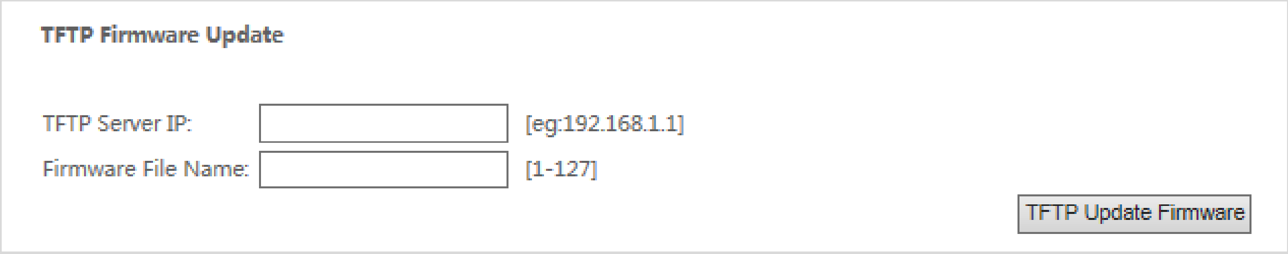
Step 5 Set **Firmware File Name** to the file name of the target firmware.

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.



TFTP Firmware Update

TFTP Server IP:		[eg:192.168.1.1]
Firmware File Name:		[1-127]

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.

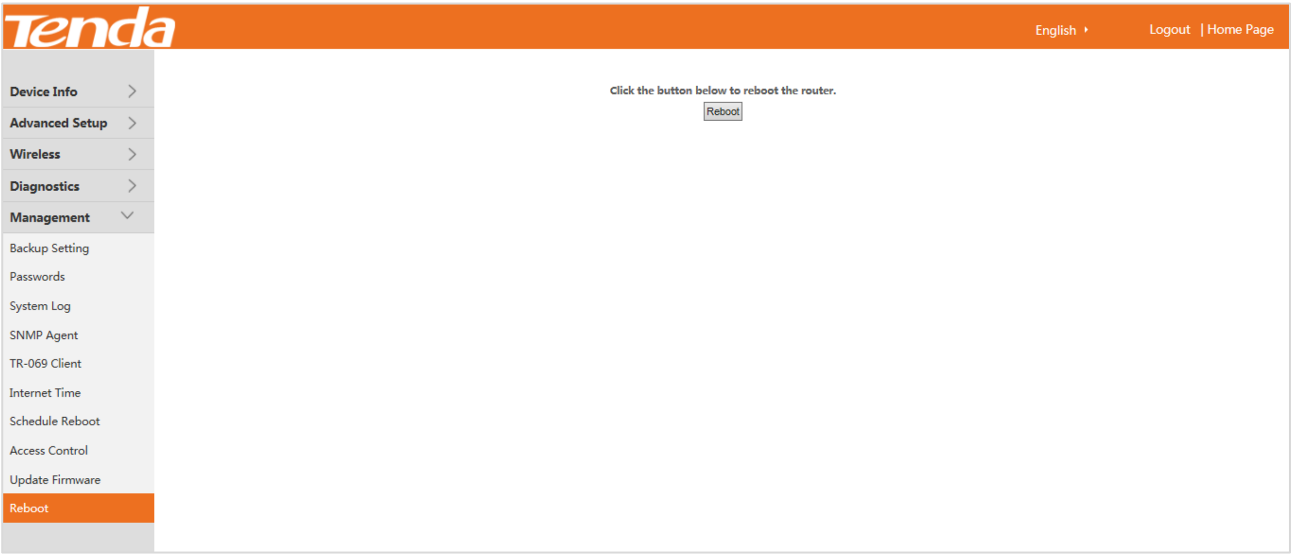
Step 3 Click **TFTP Update Firmware**.

---End

7.10 Reboot

This function allows you to manually reboot the device.

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



Click the button below to reboot the router.

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

8 Appendix

8.1 Connecting a Computer to the WiFi Network

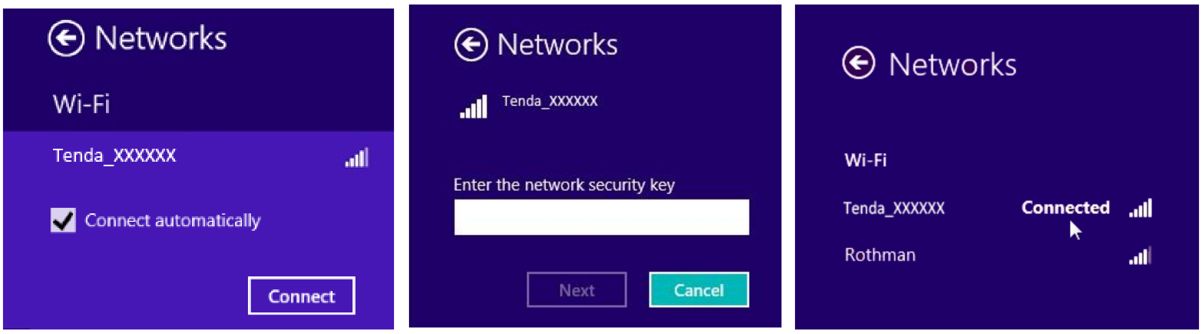
A computer can connect to the WiFi network of the router only if it has a wireless network adapter.

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

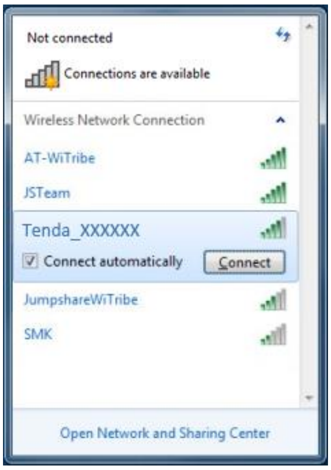
- If you cannot find the icon, move the cursor to the upper-right corner of the desktop, choose **Settings** > **Control Panel** > **Network and Internet** > **Network and Sharing Center**, click **Change adapter settings**, right-click **WiFi**, and choose **Disable**. Then, right-click **WiFi**, and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

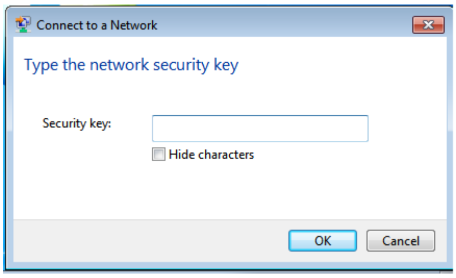
Windows 7

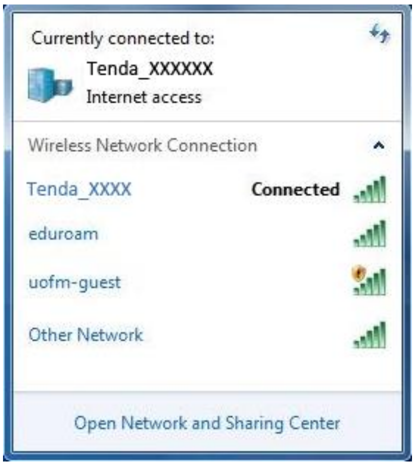
Step 1 Right-click in the lower-right corner of the desktop.

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

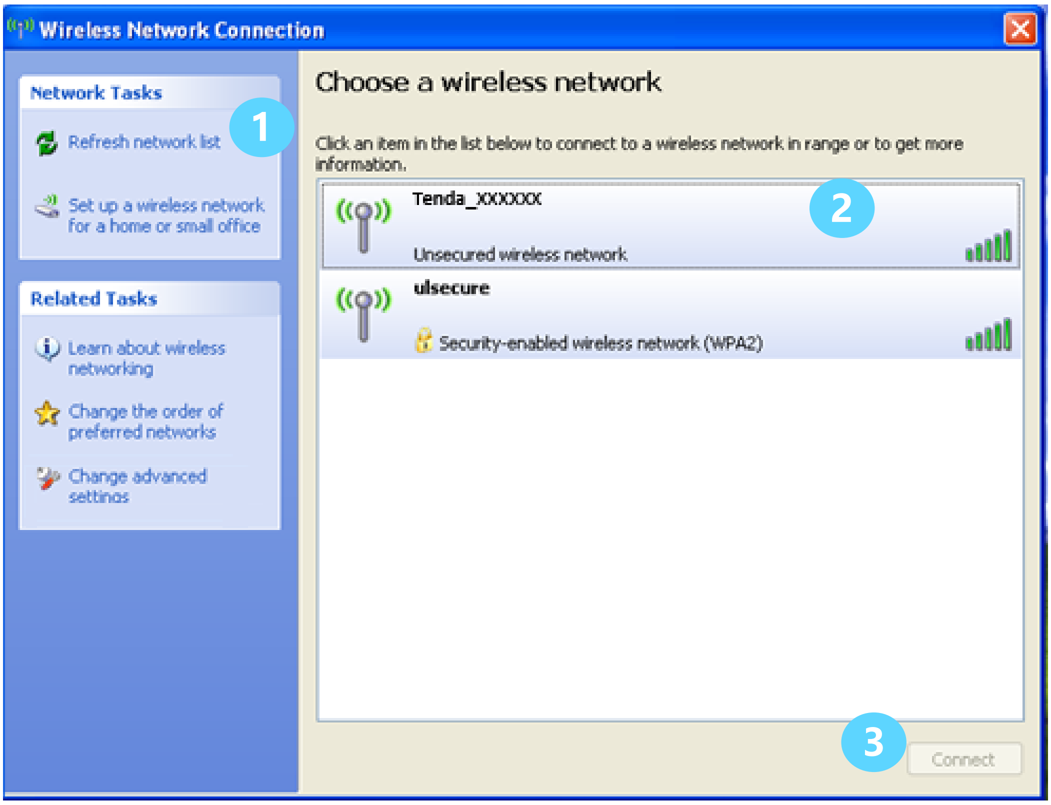
- If you cannot find the icon, choose **Start** > **Control Panel** > **Network and Internet** > **Network and Sharing Center**, click **Change adapter settings**, right-click **Wireless Network Connection**, and choose **Disable**. Then, right-click **Wireless Network Connection**, and choose **Enable**.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

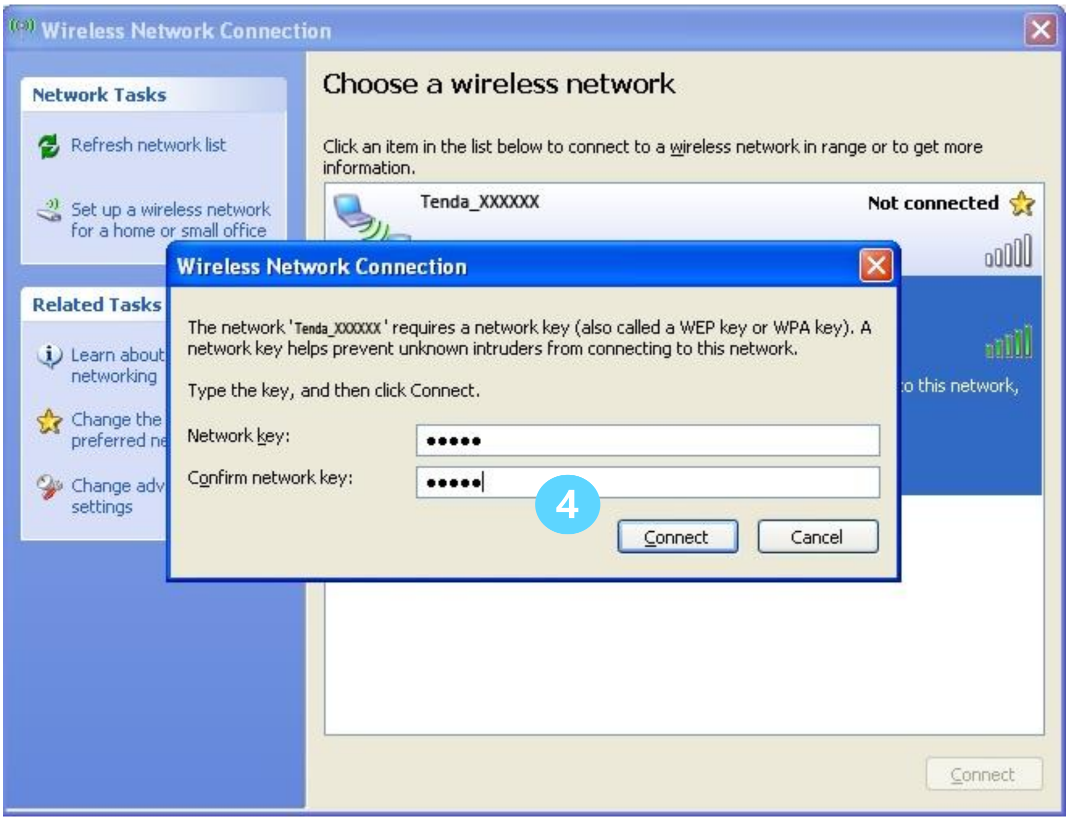
Windows XP

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.


Wireless Network Connection
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Choose a wireless network
Click an item in the list below to connect to a wireless network in range or to get more information.
Tenda_XXXXXX
Unsecured wireless network
ulsecure
Security-enabled wireless network (WPA2)
Connect
1
2
3



Wireless Network Connection

Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

Tenda_XXXXXX Not connected

Wireless Network Connection

The network 'Tenda_XXXXXX' requires a network key (also called a WEP key or WPA key). A network key helps prevent unknown intruders from connecting to this network.

Type the key, and then click Connect.

Network key: ●●●●●

Confirm network key: ●●●●●

--End

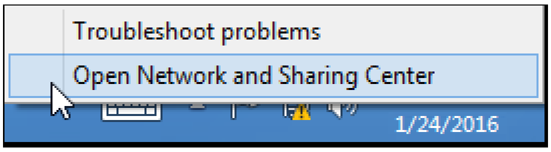
If the computer is connected to the network, Connected appears.

8.2 Configuring the Computer

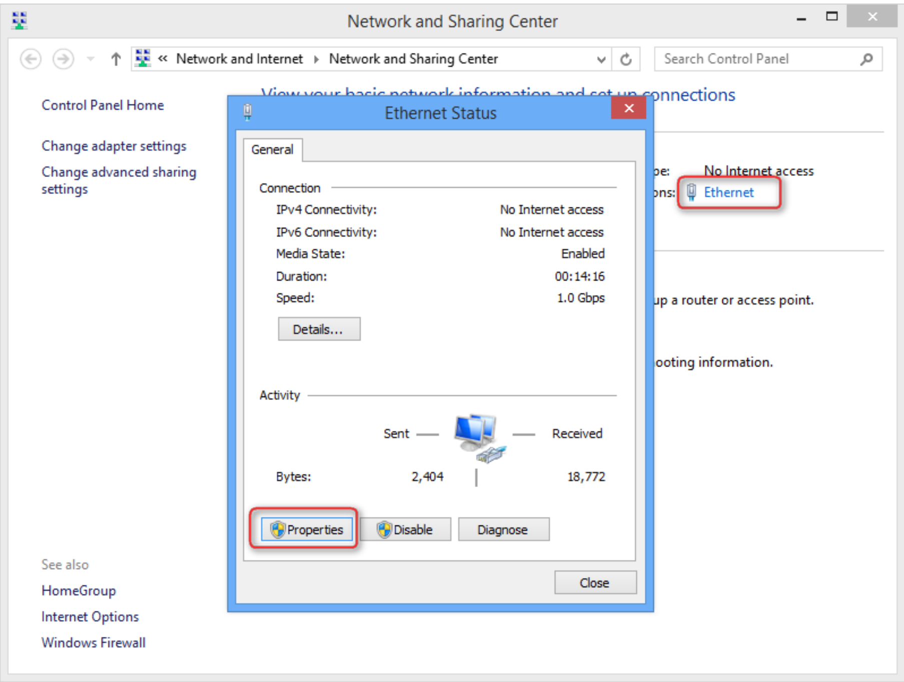
Perform the configuration procedure corresponding to Windows 8, Windows 7, or Windows XP, depending on your OS. A computer installed with a wired network adapter is used as an example to describe the procedures. The procedures for configuring computers installed with a wireless network adapter are similar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



Connection

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

Activity

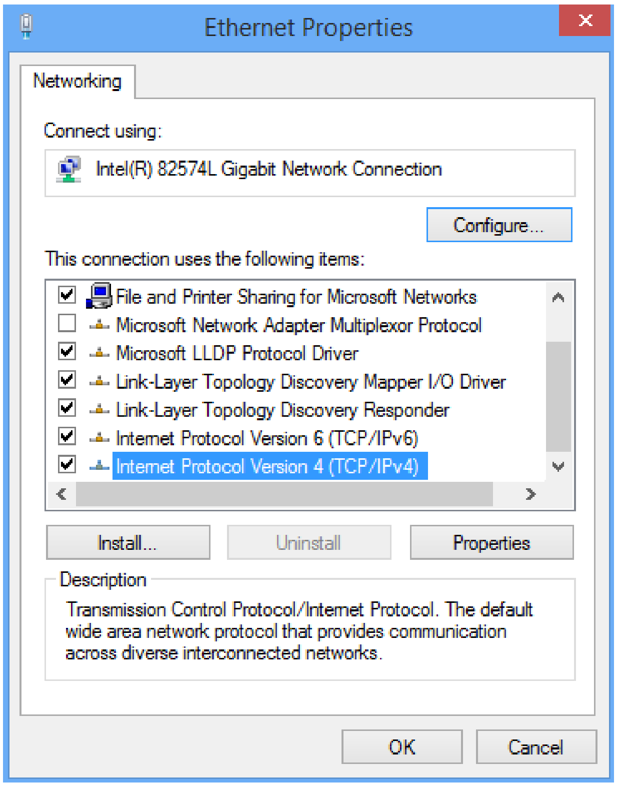
	Sent	Received
Bytes:	2,404	18,772

pe: No Internet access
ns: Ethernet

up a router or access point.

ooting information.

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



Connect using:

Intel(R) 82574L Gigabit Network Connection

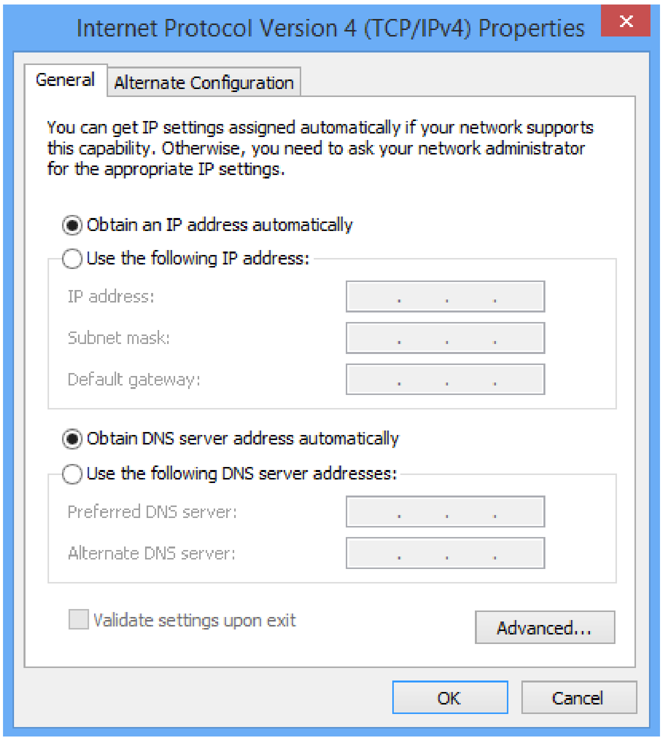
This connection uses the following items:

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

Description

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

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



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

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

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

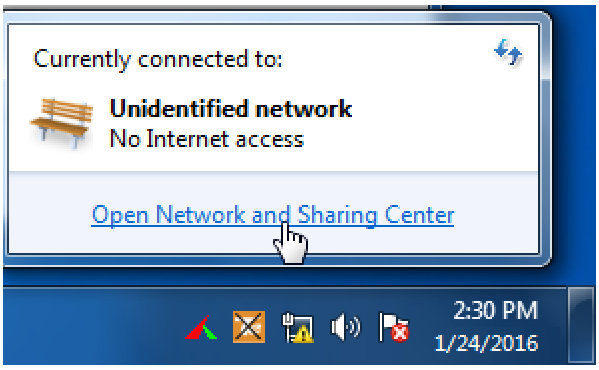
□ Validate settings upon exit

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

---End

Windows 7

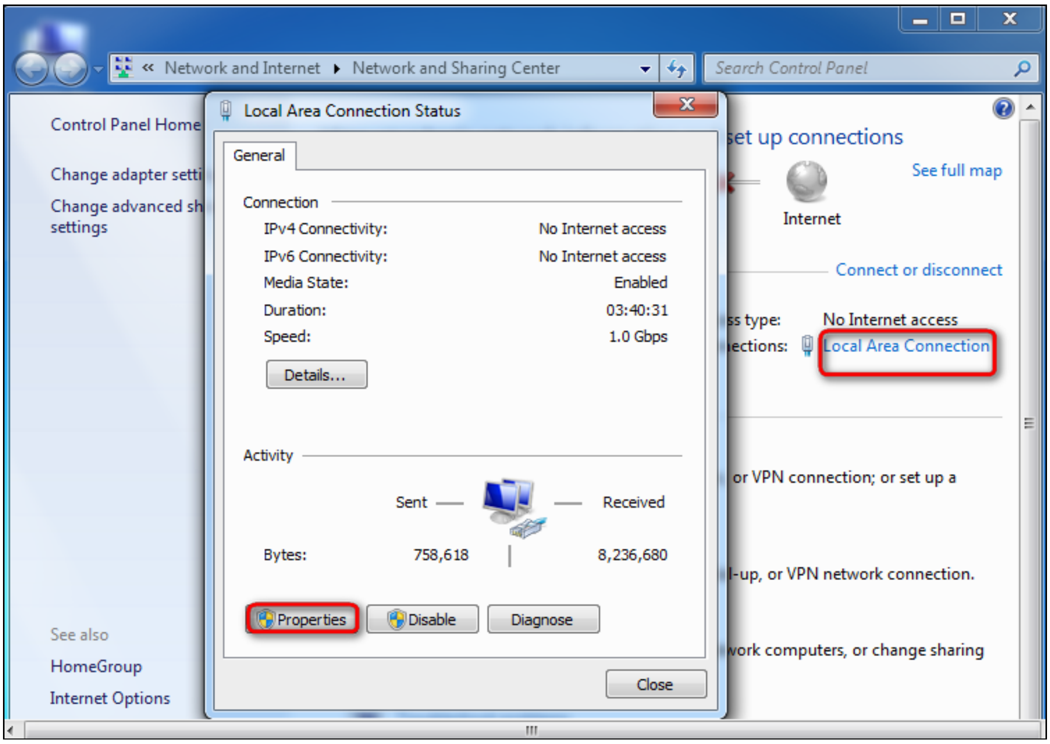
Step 1 Click in the lower-right corner of the desktop and choose **Open Network and Sharing Center**.



Currently connected to:

Unidentified network
No Internet access

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



Local Area Connection Status

General

Connection

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

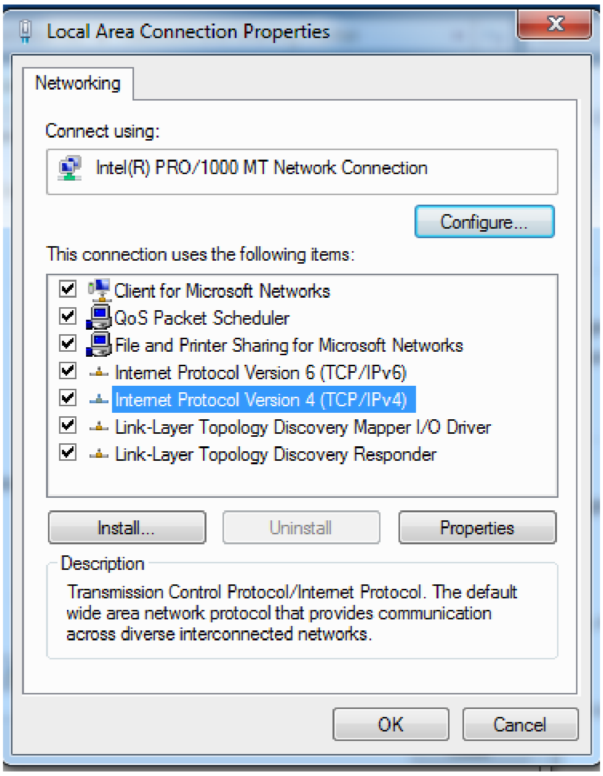
Activity

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

No Internet access

Local Area Connection

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



Local Area Connection Properties

Networking

Connect using:

Intel(R) PRO/1000 MT Network Connection

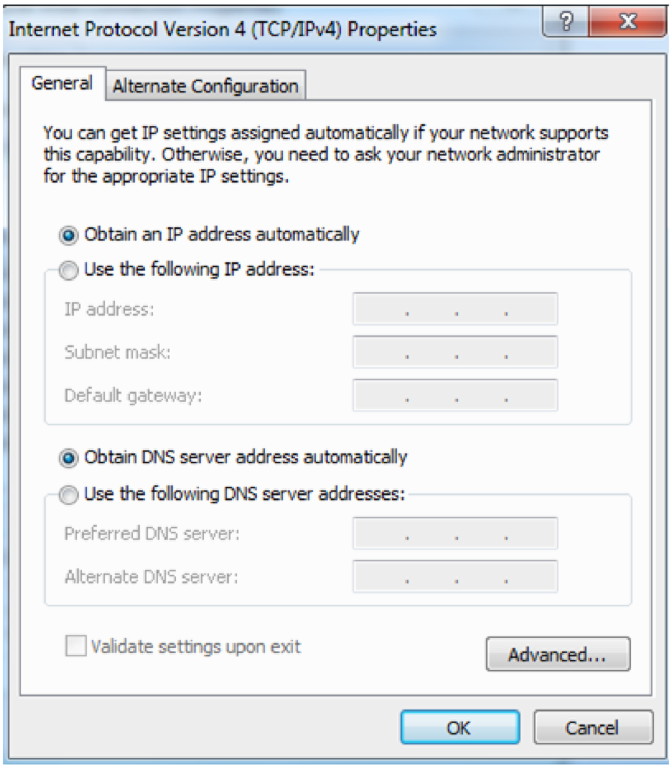
This connection uses the following items:

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

Description

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

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



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

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

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

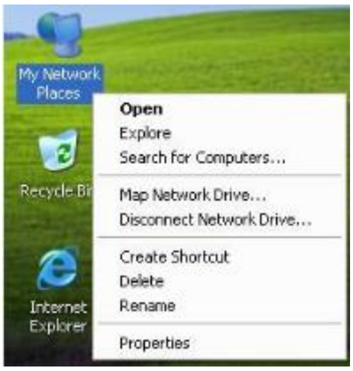
□ Validate settings upon exit

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

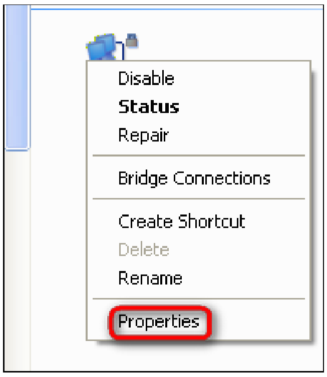
---End

Windows XP

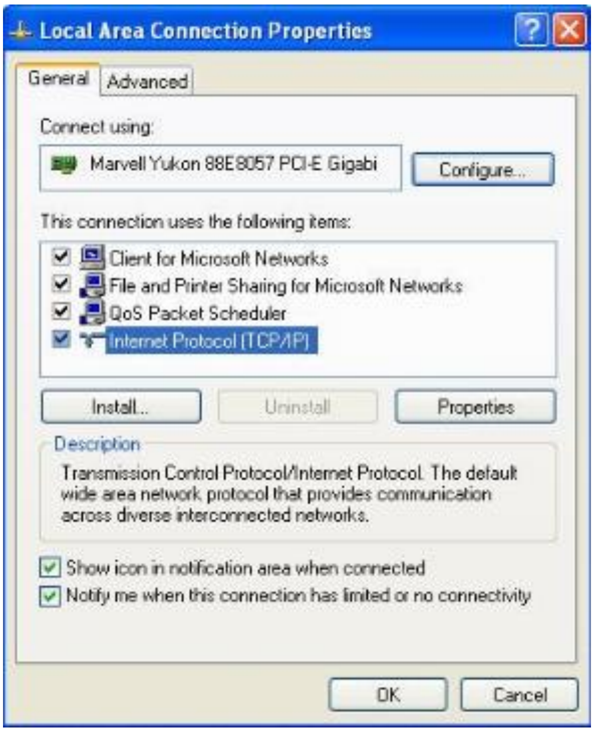
Step 1 Right-click **My Network Places** on the desktop and choose **Properties**.



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



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



Local Area Connection Properties

General | Advanced

Connect using:

Marvell Yukon 88E8057 PCI-E Gigabi

Configure...

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol (TCP/IP)

Install... | Uninstall | Properties

Description

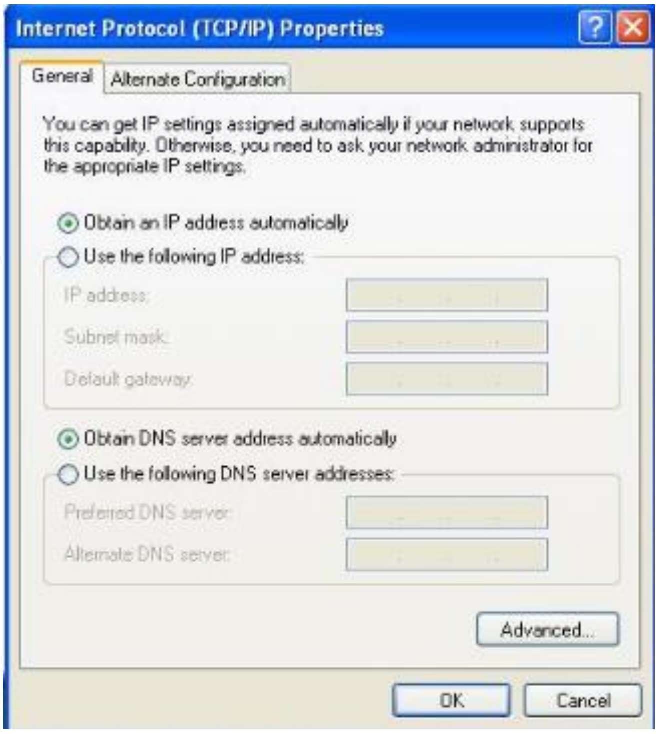
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in notification area when connected

☑ Notify me when this connection has limited or no connectivity

OK | Cancel

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



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

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

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

Advanced...

OK | Cancel

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.
- 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 internet service provider 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] 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	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 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 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.