



AC1200 Dual-Band Wireless VDSL2/ADSL2+ Modem Router

User Guide

Copyright Statement

© 2019 Shenzhen Tenda Technology Co., Ltd. All rights reserve.

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 V1200.

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: <i>XX:XX:XX:XX:XX:XX</i>
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
	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.
	This format is used to highlight a procedure that will save time or resources.

Acronyms and Abbreviations

Acronym or Abbreviation	Full Spelling
ADSL	Asymmetric Digital Subscriber Line
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
DDNS	Dynamic Domain Name Server
DHCP	Dynamic Host Configuration Protocol
DSL	Digital Subscriber Line
DMZ	Demilitarized Zone

Acronym or Abbreviation	Full Spelling
DNS	Domain Name Server
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPTV	Internet Protocol Television
ISP	Internet Service Provider
LAN	Local Area Network
L2TP	Layer 2 Tunneling Protocol
PPP	Point to Point Protocol
PPPoE	Point-to-Point Protocol over Ethernet
PPTP	Point to Point Tunneling Protocol
RIP	Routing Information Protocol
SIP	Session Initiation Protocol
SSID	Service Set Identifier
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WPS	WiFi Protected Setup

Additional Information

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

Technical Support

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



Hotline

Global: (86) 755-27657180

United States: 1-800-570-5892

Canada: 1-888-998-8966

Hong Kong: 00852-81931998



Email

support@tenda.cn



Website

<http://www.tendacn.com>

Contents

1	PRODUCT OVERVIEW	1
1.1	INTRODUCTION	1
1.2	FEATURES	1
1.3	APPEARANCE	2
1.3.1	LED indicators	2
1.3.2	Ports and buttons	3
1.3.3	Label	4
2	QUICK SETUP	5
2.1	CONNECTING THE DEVICE TO THE INTERNET	5
	Phone cable connection	5
	Ethernet cable connection	6
	3G/4G data card	6
2.2	CONNECTING A CLIENT TO THE MODEM ROUTER FOR SETUP	7
	Connecting a wireless client to the modem router	7
	Connecting a wired client to the modem router	7
2.3	SETTING UP AN INTERNET CONNECTION	8
	2.3.1 Login	8
	2.3.2 Setting up the internet settings	8
2.4	WIRELESS SETUP	17
2.5	CONNECTING TO THE MODEM ROUTER FOR INTERNET ACCESS	18
3	DEVICE INFO	19
3.1	SUMMARY	19
	3.1.1 WAN status	19
	3.1.2 xDSL info	19
	3.1.3 Device info	20
3.2	WAN	21
3.3	STATISTICS	22
3.4	ROUTE	24

3.5 ARP	25
3.6 DHCP	26
4 ADVANCED SETUP	27
4.1 INTERNET SETTINGS	27
4.1.1 <i>Setting the ATM connection</i>	27
4.1.2 <i>Setting the PTM connection</i>	69
4.1.3 <i>Setting the Ethernet connection</i>	75
4.2 LAN	81
4.2.1 <i>Local Area Network (LAN) Setup</i>	81
4.2.2 <i>Connections limited</i>	86
4.2.3 <i>IPv6 autoconfig</i>	87
4.3 VPN	92
4.3.1 <i>Overview</i>	92
4.3.2 <i>Configuring modem router as a L2TP client</i>	92
4.3.3 <i>Configuring modem router as a PPTP client</i>	95
4.4 WAN 3G/4G	98
4.4.1 <i>Overview</i>	98
4.4.2 <i>Configuration procedure</i>	98
4.5 NAT	100
4.5.1 <i>Virtual server</i>	100
4.5.2 <i>Port triggering</i>	103
4.5.3 <i>DMZ host</i>	105
4.5.4 <i>Multi-NAT</i>	106
4.6 SECURITY	108
4.6.1 <i>DoS defence</i>	108
4.6.2 <i>IP filtering</i>	109
4.6.3 <i>MAC filtering</i>	112
4.7 PARENTAL CONTROL	116
4.7.1 <i>Time restriction</i>	116
4.7.2 <i>URL filter</i>	117
4.7.3 <i>Example of configuring parental control</i>	118

4.8 ALG	121
4.9 BANDWIDTH CONTROL	123
4.9.1 Overview.....	123
4.9.2 Adding a bandwidth control rule.....	123
4.10 QUALITY OF SERVICE	124
4.10.1 QoS queue	125
4.10.2 QoS classification.....	130
4.10.3 Example of configuring QoS	131
4.11 ROUTING	136
4.11.1 Default gateway.....	136
4.11.2 Static route	136
4.11.3 RIP	138
4.12 DNS.....	140
4.12.1 DNS server	140
4.12.2 Dynamic DNS.....	142
4.13 DSL.....	145
4.14 UPnP	147
4.14.1 Overview.....	147
4.14.2 Configuring the UPnP function	147
4.15 STORAGE SERVICE	148
4.15.1 Overview.....	148
4.15.2 Enabling the Samba and FTP servers	148
4.15.3 Example of configuring the storage service function	148
4.16 INTERFACE GROUPING	151
4.16.1 Overview.....	151
4.16.2 Example of configuring interface grouping	151
4.17 IP TUNNEL	153
4.17.1 IPv6inIPv4	153
4.17.2 IPv4inIPv6.....	154
4.18 IPSEC	156
4.18.1 Overview.....	156

4.18.2	Configuring the IPSec function	160
4.19	CERTIFICATE	162
4.19.1	Local	162
4.19.2	Trusted CA	164
4.20	MULTICAST	165
4.21	IPTV	168
4.21.1	ATM interface	168
4.21.2	ETH interface	169
4.21.3	PTM interface	169
5	WIRELESS.....	171
5.1	2.4G	171
5.1.1	Basic	171
5.1.2	Security.....	173
5.1.3	MAC filter	179
5.1.4	Wireless bridge.....	180
5.1.5	Station info	185
5.2	5G	186
5.2.1	Basic	186
5.2.2	Security.....	188
5.2.3	MAC filter	193
5.2.4	Wireless bridge.....	195
5.2.5	Station info	200
6	DIAGNOSTICS.....	201
6.1	PING.....	201
6.2	TRACEROUTE	202
6.3	NSLOOKUP.....	203
6.4	DIAGNOSTICS	204
7	MANAGEMENT	205
7.1	SETTINGS.....	205
7.1.1	Backup.....	205
7.1.2	Restore backup	205

7.1.3 Restore default	206
7.2 SYSTEM LOG	208
7.2.1 Overview.....	208
7.2.2 Viewing system logs	208
7.2.3 Configuring system logs	209
7.3 PASSWORDS	211
7.3.1 Overview.....	211
7.3.2 Changing the login password.....	211
7.4 SNMP AGENT	212
7.4.1 Overview.....	212
7.4.2 Configuring the SNMP agent.....	213
7.5 TR-069 CLIENT.....	214
7.5.1 Overview.....	214
7.5.2 Configuring the TR-069 Client	215
7.6 INTERNET TIME	216
7.6.1 Overview.....	216
7.6.2 Synchronizing the system time with the internet	216
7.7 ACCESS CONTROL	217
7.8 UPDATE SOFTWARE.....	218
7.8.1 Overview.....	218
7.8.2 Upgrading the firmware locally.....	218
7.8.3 Upgrading the firmware using FTP server.....	219
7.8.4 Upgrading the firmware using TFTP server.....	220
7.9 REBOOT	221
APPENDIX.....	222
A.1 FAQ.....	222
A.2 VPI/VCI LIST	223
A.3 VLAN LIST	233
A.4 FACTORY SETTINGS	245

1

Product overview

1.1 Introduction

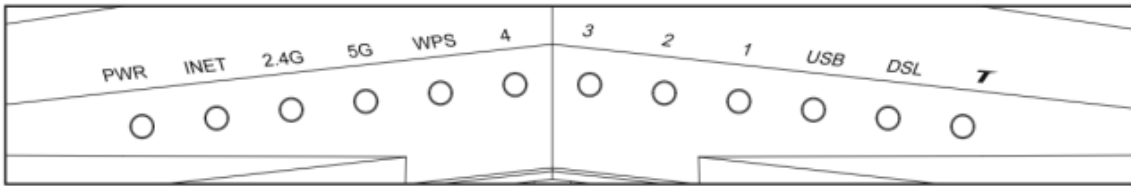
Compatible with VDSL2 Profile 17a, Tenda V1200 offers a VDSL broadband access speed as high as of 100 Mbps, 5x faster than ADSL2+. With DSL modem and WiFi router in one, it features an integrated DSL port that supports all standard DSL connections, including VDSL2, ADSL2+, ADSL2, and ADSL.

1.2 Features


- All-in-one device combines a VDSL2/ADSL2+ modem, wired router, wireless router and switch.
- Ethernet and VDSL uplinks: Access the internet via DSL port or WAN port (RJ45 port).
- Multiple internet connection types: Bridging, PPPoE, IPoE, PPPoA, and IPoA.
- Up to 1200 Mbps wireless transmission speed for excellent HD video streaming and online gaming.
- Compatible with IEEE 802.11b/g/n/ac Wireless devices.
- One-key WPS ensures quick and secure wireless network connection.
- USB port makes you access and share files through an attached USB storage device.
- Port 4 can function either as a LAN or a WAN port.
- The IPTV feature is supported.
- QoS feature helps prioritize media streaming and gaming applications for best entertainment experience.
- Parental Control controls internet access of children using flexible and customizable filter settings.
- 6 kV lightning - proof design fits into lightning-intensive environment.
- Advanced Features: IPv6, DDNS, virtual server, DMZ, port triggering, IP filter, MAC filter, UPnP, and so on.

1.3 Appearance

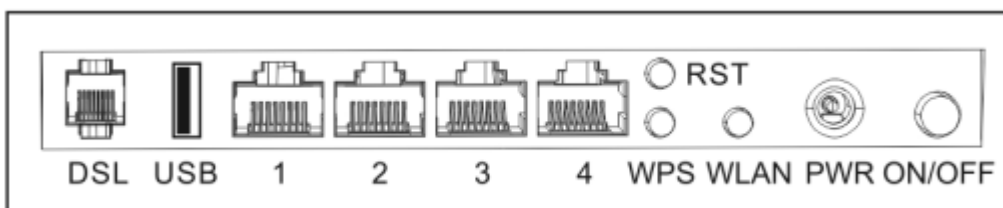
1.3.1 LED indicators



LED Indicator	Color	Status	Description
PWR	Red	Solid on	The modem router is starting.
		Blinking	The modem router is upgrading.
	Green	Solid on	The modem router is working properly.
INET	Green	Solid on	The modem router is connected to the internet successfully.
		Blinking	Data is being transmitted.
	Red	Blinking	The modem router fails to connect to the internet.
2.4G	Green	Solid on	2.4 GHz WiFi network is enabled.
		Blinking	Data is being transmitted over 2.4 GHz WiFi network.
	/	Off	2.4 GHz WiFi network is disabled.
5G	Green	Solid on	5 GHz WiFi network is enabled.
		Blinking	Data is being transmitted over 5 GHz WiFi network.
	/	Off	5 GHz WiFi network is disabled.
WPS	Green	Solid on for 2 mins->Off	A WPS connection is established.
		Blinking	The modem router is performing WPS negotiation.

LED Indicator	Color	Status	Description
	/	Off	The WPS feature is disabled, or the WPS feature is enabled but the modem router does not perform WPS negotiation.
1-4	Green	Solid on	This port is connected properly.
		Blinking	Data is being transmitted over the port.
	/	Off	The port is disconnected, or not connected properly.
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.
DSL	Green	Solid on	The DSL negotiation succeeds.
		Blinking	The modem router is performing DSL negotiation.
	/	Off	The port is disconnected, or not connected properly.
			This LED is reserved.

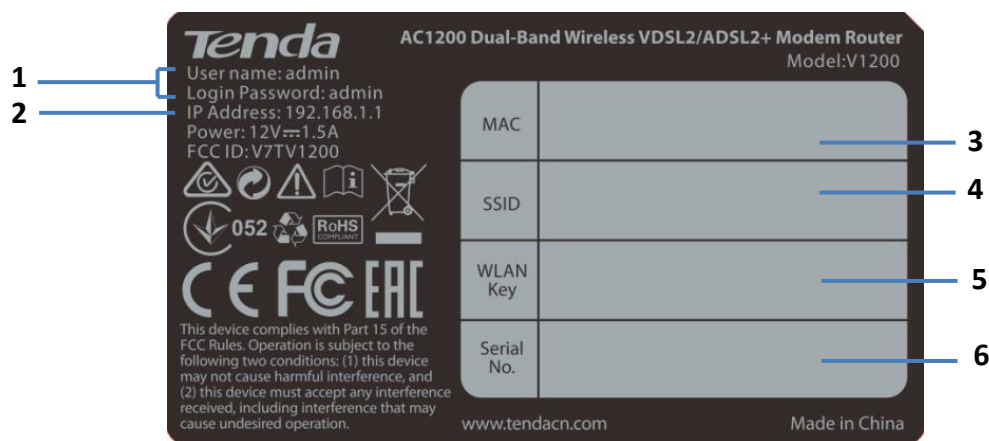
1.3.2 Ports and buttons



Button/Port	Description
ON/OFF	This button is used to turn on/off the modem router.
PWR	The power jack is used to connect to the included power adapter for power supply. To prevent device damage, use the included power adapter for power supply.

Button/Port	Description
WLAN	This button is used to enable or disable both 2.4 GHz and 5 GHz WiFi networks.
WPS	Enable the WPS function on the web UI of the modem router. Press this button for about 3 seconds and then release it to perform the WPS negotiation process. Within 2 minutes after pressing the button, enable the wireless device's WPS feature to establish WPS connection.
RST	Hold down this button for about 6 seconds to restore factory settings.
1/2/3	LAN Ports. Used to connect to computers, switches, and so on.
4	WAN/LAN port. When the modem router serves as a router only, port 4 can be used as a WAN port connected to an Ethernet jack. Otherwise, it serves as a LAN port.
USB	USBV2.0 port. Used to connect to a USB device. Warning: The output current of the USB 2.0 port should not exceed 0.5 A.
DSL	RJ11 port. Used to connect to a phone jack for internet access.

1.3.3 Label



- 1: Default login user name and password.
- 2: Default login IP address of the modem router.
- 3: MAC address of the modem router.
- 4: Default wireless network name of the modem router.
- 5: Default wireless password for the default wireless network.
- 6: The serial number of the modem router.

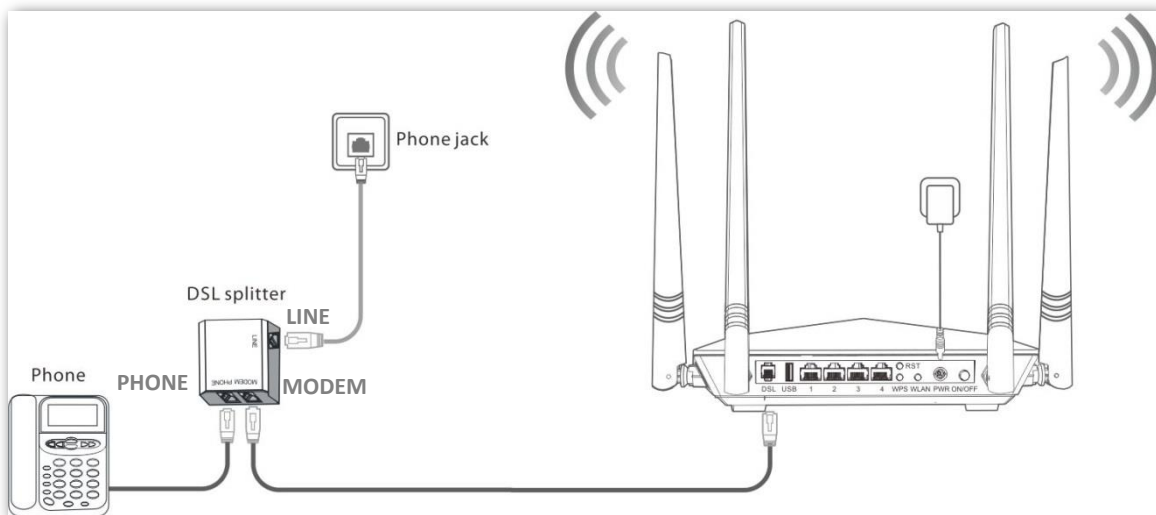
2 Quick setup

2.1 Connecting the device to the internet

The modem router supports [phone cable connection](#), [Ethernet cable connection](#), and [3G/4G data card](#). Select a connection type to follow according to your internet service.

Phone cable connection

If you access the internet with a phone cable, connect the modem router as follows:

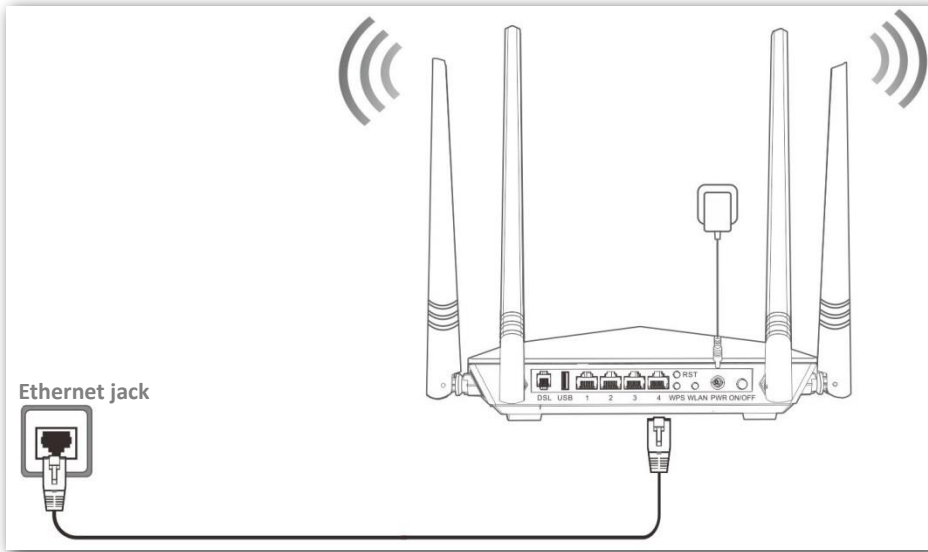


- Step 1** Connect the **LINE** port of the included splitter to the internet.
- Step 2** (Optional) If you do not need to use the phone service, skip this step. Connect the **PHONE** port of the splitter to your telephone.
- Step 3** Connect the **MODEM** port of the splitter to the **DSL** port of the modem router.
- Step 4** Use the included power adapter to connect the modem router to a power supply.
- Step 5** Turn the modem router on.

----End

Ethernet cable connection

If you access the internet with an Ethernet cable, connect the modem router as follows:



- Step 1** Connect port 4 of the modem router to the internet.
- Step 2** Use the included power adapter to connect the modem router to a power supply.
- Step 3** Turn the modem router on.

----End

3G/4G data card

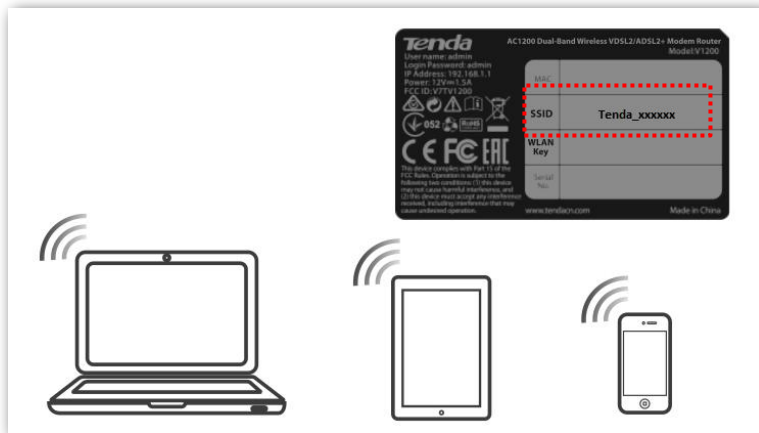
If you access the internet with a 3G/4G dongle, perform the following steps:

- Step 1** Use the included power adapter to connect the modem router to a power supply.
- Step 2** Turn the modem router on.
- Step 3** Insert a 3G/4G dongle provided by your ISP into USB port of the modem router for internet access.

----End

2.2 Connecting a client to the modem router for setup

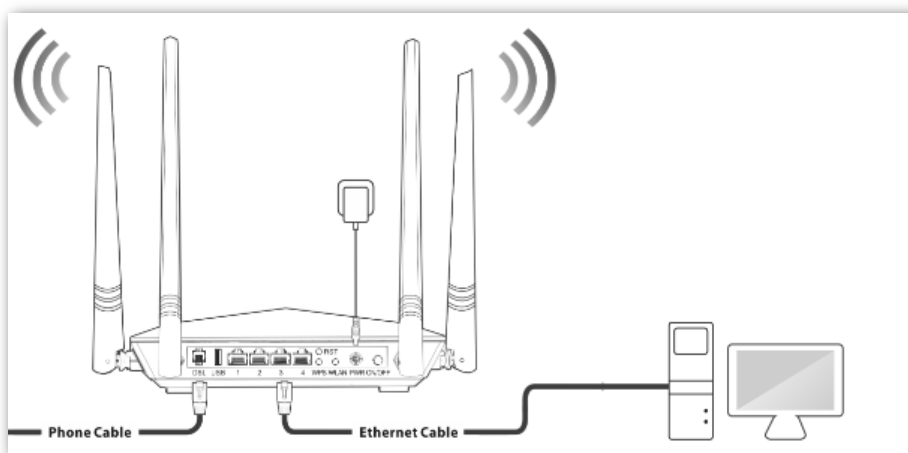
Connecting a wireless client to the modem router



Use your smart device to search and connect to the default SSID (WiFi name) of the modem router. The default SSID is specified on the product label. This label is on the bottom of the modem router. And by default, there is no WLAN key (WiFi password).

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

Connecting a wired client to the modem router



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

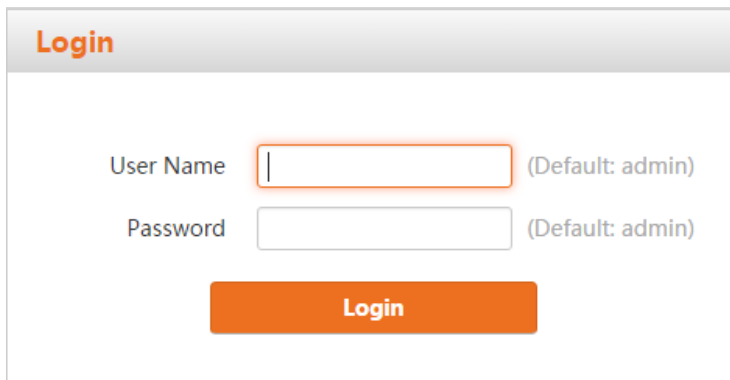
2.3 Setting up an internet connection

2.3.1 Login

Step 1 Start a web browser on the client connected to the modem router, and visit **192.168.1.1**.



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

A screenshot of a login page. The page has a title 'Login' in orange. Below the title, there are two input fields: 'User Name' and 'Password'. Both fields have a default value of 'admin' indicated in parentheses to the right of each field. Below the input fields is an orange 'Login' button.

To prevent an unauthorized user from changing the settings of the mode router, you'd better change the default login user name and password. Refer to [Passwords](#) for details.

----End

2.3.2 Setting up the internet settings

Select one to follow according to your internet connection type.

Phone cable connection

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

VDSL

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

Primary Settings

Link Type	<input type="text" value="VDSL"/>
Connection Type	<input type="text" value="PPPoE"/>
Auto Vlan scan	<input type="checkbox"/>
Country / Region	<input type="text" value="Other"/>
ISP	<input type="text" value="Other"/>
Input Vlan	<input type="checkbox"/>
User Name	<input type="text"/>
Password	<input type="text"/>

Step 1 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 enter the related internet parameters.

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

Step 4 **Auto Vlan scan:** If the VLAN ID is provided, set both the **Country/Region** and **ISP** to **Other**, select **Input Vlan**, and enter the VLAN ID in the **Vlan ID** box. If the VLAN ID is not provided, select your country or region, the VLAN ID will be automatically populated. Or select **Auto Vlan scan**, the modem router will try accessing the upstream device using the parameters in the **VLAN List** form in [A.3](#).

If you are uncertain about the VLAN ID, keep the default.

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



TIP

If you cannot access the internet after completing the primary settings, contact your ISP for help.

----End

ADSL

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

Primary Settings

Link Type: ADSL

Connection Type: PPPoE

Auto PVC scan:

Country / Region: Other

ISP: Other

VPI/VCI: VPI 0 (0-255) VCI 0 (32-65535)

User Name:

Password:

Step 1 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.

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

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

Step 5 ISP: Select your ISP.

Step 6 Auto PVC scan: Select your country or region from the drop-down list, and the VPI and VCI values will be automatically populated.

If your country/region and ISP are not available in the drop-down list or the VPI and VCI values are incorrect, select **Other** both from the **Country/Region** and **ISP** lists, and enter the **VPI** and **VCI** values manually.

If you are uncertain about the VPI and VCI, select **Auto PVC scan**.

Step 7 Enter other internet parameters provided by your ISP (if any).

Step 8 Click **OK** on the bottom of the page to apply the settings.



If you cannot access the internet after completing the primary settings, contact your ISP for help.

----End

Ethernet cable connection

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

PPPoE

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

The screenshot shows a 'Primary Settings' window with the following fields:

Link Type	Ethernet
Connection Type	PPPoE
Auto Vlan scan	<input checked="" type="checkbox"/>
Input Vlan	<input type="checkbox"/>
User Name	<input type="text"/>
Password	<input type="text"/>

Step 1 Enter the **Home** page.

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

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

Step 4 Auto Vlan scan: If the VLAN ID is provided, deselect **Auto Vlan scan**, and select your country or region. The VLAN ID will be automatically populated. If it is incorrect, change the value in the **Vlan ID** box.

If you cannot find your country or region in the drop-down list, set both the

Country/Region and **ISP** to **Other**, select **input Vlan**, and enter the VLAN ID in the **Vlan ID** box.

If you are uncertain about the VLAN ID, keep the default.

Step 5 Enter the user name and password provided by your ISP.

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

----End



If you cannot access the internet after completing the primary settings, contact your ISP for help.

IPoE

■ Dynamic IP

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

Primary Settings

Link Type	Ethernet ▼
Connection Type	IPoE ▼
Auto Vlan scan	<input checked="" type="checkbox"/>
Input Vlan	<input type="checkbox"/>
Address Mode	Dynamic IP ▼

Step 1 Enter the **Home** page.

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

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

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

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

----End

■ Static IP

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

Primary Settings

Link Type	Ethernet ▼
Connection Type	IPoE ▼
Auto Vlan scan	<input checked="" type="checkbox"/>
Input Vlan	<input type="checkbox"/>
Address Mode	Static IP ▼
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Gateway	0.0.0.0
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0

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.

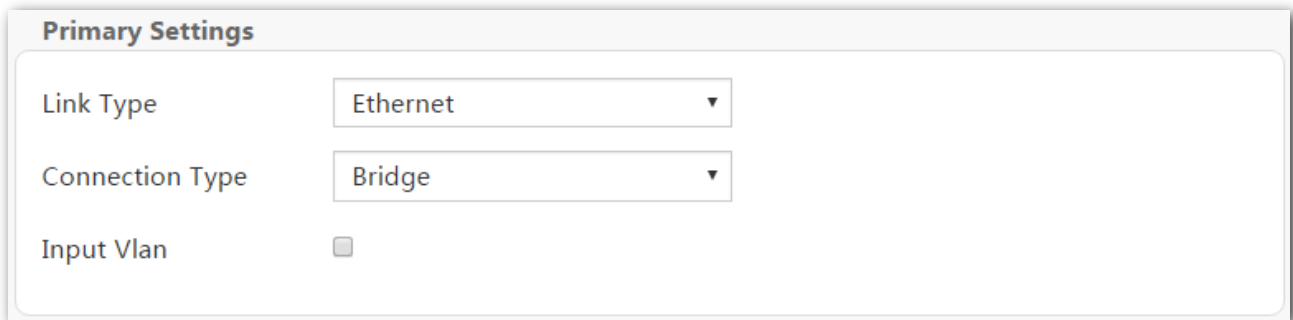
----End



If you cannot access the internet after completing the primary settings, contact your ISP for help.

Bridge

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



The image shows a 'Primary Settings' dialog box with three configuration options:

- Link Type:** A dropdown menu currently set to 'Ethernet'.
- Connection Type:** A dropdown menu currently set to 'Bridge'.
- Input Vlan:** A checkbox that is currently unchecked.

Step 1 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

3G/4G dongle

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

Primary Settings

Link Type	<input type="text" value="3G/4G"/>
Country / Region	<input type="text" value="Other"/>
ISP	<input type="text" value="Other"/>
APN	<input type="text"/>
Dial number	<input type="text"/>
User Name	<input type="text"/>
Password	<input type="text"/>

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

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

Step 3 **Country / Region:** Select your country or region.

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

Step 5 **(Optional) APN/Dial number/Username/Password:** Generally, if you select a correct country/region 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

2.4 Wireless setup

The wireless feature is enabled by default. The default SSID for 2.4 GHz wireless network is Tenda_XXXXXX, and for 5 GHz wireless network is Tenda_5G_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 for both 2.4 GHz and 5 GHz wireless networks. It takes effects when the **OK** button on the bottom of the page is clicked.

The screenshot shows two sections of the wireless settings interface. The top section is titled "Wireless Settings -- 2.4G" and contains three rows: "Wireless Enable" with a checked checkbox, "Wireless SSID" with a text box containing "Tenda_F02910" and a note "(Only 32 ASCII are allowed)", and "Wireless Key" with a masked password field "*****" and a note "Only 8-63 ASCII or 64 hex characters are allowed in password." The bottom section is titled "Wireless Settings -- 5G" and contains three rows: "Wireless Enable" with a checked checkbox, "Wireless SSID" with a text box containing "Tenda_5G_F02910" and a note "(Only 32 ASCII are allowed)", and "Wireless Key" with a masked password field "*****" and a note "Only 8-63 ASCII or 64 hex characters are allowed in password."

To customize a WiFi name and password:

- Step 1** Enter the **Home** page.
- Step 2** **Wireless SSID:** Enter new WiFi names for 2.4 GHz and 5 GHz wireless networks.
- Step 3** **Wireless Key:** Enter new WiFi passwords for 2.4 GHz and 5 GHz wireless networks.
- Step 4** Click **OK** to apply the settings.

----End

To disable wireless function:

Step 1 Enter the **Home** page.

Step 2 Deselect the **Wireless Enable** option for 2.4 GHz or 5 GHz wireless networks.

Step 3 Click **OK**.

The screenshot shows two sections of wireless settings. The top section is titled "Wireless Settings -- 2.4G" and contains a "Wireless Enable" checkbox (unchecked), a "Wireless SSID" field with the value "Tenda_F02910" (with a note "(Only 32 ASCII are allowed)"), and a "Wireless Key" field with seven dots (with a note "Only 8-63 ASCII or 64 hex characters are allowed in password."). The bottom section is titled "Wireless Settings -- 5G" and contains a "Wireless Enable" checkbox (unchecked), a "Wireless SSID" field with the value "Tenda_5G_F02910" (with a note "(Only 32 ASCII are allowed)"), and a "Wireless Key" field with seven dots (with a note "Only 8-63 ASCII or 64 hex characters are allowed in password."). An "OK" button is located at the bottom center of the interface.

----End

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

2.5 Connecting to the modem router for internet access

To access the internet with:

Wireless devices: connect your wireless devices to the WiFi networks of the modem router using the SSIDs and wireless keys you set.

Wired devices: connect the wired devices to ports 1, 2, 3 or 4 (if available) of the modem router.

3 Device info

3.1 Summary

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

3.1.1 WAN status

If a WAN connection is established, you can check the WAN status here, including connection status, connection type, link type, WAN IP address, gateway, WAN MAC address, WAN link time, and DNS server information.

WAN status:

Connection status:	Connected
Connection(Link) Type:	DHCP(Ethernet)
WAN IP Address:	192.168.0.142
WAN Subnet Mask:	255.255.255.0
Default Gateway:	192.168.0.1
Wan MAC Address:	C8:3A:35:14:4B:64
Wan Link Time:	0D 0H 3M 36S
Primary DNS:	192.168.0.1
Secondary DNS:	

3.1.2 xDSL info

If an ADSL/VDSL connection is established, you can check the ADSL/VDSL connection information here.

xDSL info:

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

3.1.3 Device info

You can check the basic information of the modem router here.

Device info:	
Board ID:	963167REF3
Symmetric CPU Threads:	2
Software Version:	V53.2.0.4_en_TDE01
Hardware Version:	V1.0.0
Bootloader (CFE) Version:	1.0.38-161.184
DSL PHY and Driver Version:	A2pv6F039v4.d26r
Wireless Driver Version:	7.14.89.14.cpe4.16L03.0-kdb
LAN IP:	192.168.1.1
LAN MAC:	c8:3a:35:14:4b:60
Uptime:	0D 0H 44M 34S
Date/Time:	Tue Feb 19 09:32:03 2019

Parameter description

Parameter	Description
Board ID	It specifies the model of the main chip.
Symmetric CPU Threads	It specifies the number of symmetric CPU threads of the modem router.
Software Version	It specifies the software version of the modem router.
Hardware Version	It specifies the hardware version of the modem router.
Bootloader (CFE) Version	It specifies the bootloader version of the modem router.
DSL PHY and Driver Version	It specifies the DSL physic and driver version of the modem router.
Wireless Driver Version	It specifies the wireless driver version of the modem router.
LAN IP	It specifies the LAN IP address of the modem router.
LAN MAC	It specifies the LAN MAC address of the modem router.
Uptime	It specifies the total time the modem router has been running since the latest reboot.
Date/Time	It speifies the current systemdate and time of the modem router.

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 Pxy	Igmp Src Enbl	MLD Pxy	MLD Src Enbl	NAT	Firewall	Status	IPv4 Address	IPv6 Address
eth3.1	ipoe_eth3	IPoE	Disabled	Disabled	Enabled	Enabled	Disabled	Disabled	Enabled	Enabled	Connected	192.168.60.100	

Parameter description

Parameter	Description
Interface	It specifies the interface that the WAN connection uses.
Description	It specifies the description of the WAN connection.
Type	It specifies the connection type of the WAN connection.
VlanMuxId	It specifies the VLAN ID value of the WAN connection.
IPv6	It specifies the IPv6 configuration information of the WAN connection.
Igmp Pxy	It specifies whether the IGMP Multicast Proxy is enabled.
Igmp Src Enbl	It specifies whether the IGMP Multicast Source is enabled.
MLD Pxy	It specifies whether the MLD Multicast Proxy is enabled.
MLD Src Enbl	It specifies whether the MLD Multicast Source is enabled.
NAT	It specifies whether the NAT feature is enabled.
Firewall	It specifies whether firewall is enabled.
Status	It specifies the WAN connection status.
IPv4 Address	It specifies the obtained IPv4 address.
IPv6 Address	It specifies the obtained IPv6 address.

3.3 Statistics

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

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

Statistics -- LAN

Interface	Received								Transmitted							
	Total				Multicast		Unicast	Broadcast	Total				Multicast		Unicast	Broadcast
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts
LAN1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
LAN2	49793807	221157	0	0	0	3778	215559	1820	175188650	186188	0	0	0	858	185315	15
LAN3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.4G	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5G	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Reset Statistics

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

Statistics -- WAN

Interface	Description	Received								Transmitted							
		Total				Multicast		Unicast	Broadcast	Total				Multicast		Unicast	Broadcast
		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts
eth3.1	ipoe_eth3	2272956	3672	0	0	31810	689	2963	20	713695	8271	0	0	0	0	8271	0

Reset Statistics

Statistics—Interface Statistics: Displays the statistics of each interface. Click **Reset** to clear the current statistics.

Interface Statistics

Port Number	In Octets	Out Octets	In Packets	Out Packets	In OAM Cells	Out OAM Cells	In ASM Cells	Out ASM Cells	In Packet Errors	In Cell Errors
Reset										

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

Mode:		
Traffic Type:		
Status:	Disabled	
Link Power State:		
	Downstream	Upstream
Line Coding(Trellis):		
SNR Margin (0.1 dB):		
Attenuation (0.1 dB):		
Output Power (0.1 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 of the modem router. If the modem router fails to access the internet, you can check the route table to find the problem.

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	192.168.60.1	0.0.0.0	UG	0	ipoe_eth3	eth3.1
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0
192.168.60.0	0.0.0.0	255.255.255.0	U	0	ipoe_eth3	eth3.1

Parameter description

Parameter	Description
Destination	It specifies the destination IP address of the route.
Gateway	It specifies the gateway address of the route.
Subnet Mask	It specifies the subnet mask corresponding to the destination IP address.
Flag	It specifies the status of the corresponding route.
Metric	It specifies a number of hops the route has.
Service	It specifies the WAN connection the route uses.
Interface	It specifies the interface that the route uses.

3.5 ARP

Here you can view the ARP list of the device. According to the information in the list, you can identify whether there is ARP attack in your network.

Device Info -- ARP

IP address	Flags	HW Address	Device
192.168.60.1	Complete	00:90:4c:88:88:80	eth3.1
169.254.140.8	Complete	c8:9c:dc:60:54:69	br0
192.168.1.2	Complete	c8:9c:dc:60:54:69	br0

Parameter description

Parameter	Description
IP address	It specifies the IP address of the connected device.
Flags	It specifies the status of the connection between the device and the modem router.
HW Address	It specifies the MAC address of the connected device.
Device	It specifies the interface the device uses to connect to the mode router.

3.6 DHCP

Here you can view the devices whose IP addresses are assigned by the DHCP server of the modem router. You can check the IP address, MAC address and hostname of the corresponding device and remaining lease time of the IP address.

Hostname	MAC Address	IP Address	Expires In	Status
Dudu-Computer	c8:9c:dc:60:54:69	192.168.1.2	17 hours, 35 minutes, 20 seconds	Ethernet

Parameter description

Parameter	Description
Hostname	It specifies the name of the connected device.
MAC Address	It specifies the MAC address of the connected device.
IP Address	It specifies the IP address that assigned to the connected device.
Expires In	It specifies the remaining lease time of the IP address that assigned to the connected device.
Status	It specifies the connection type the connected device uses to connect to the modem router.

4 Advanced setup

4.1 Internet settings

In this module, it allows you to set up multiple internet connections or set detailed parameters for internet access.

To set up an internet connection:

Step 1 Create an interface.

Step 2 Set up an internet connection.

This modem router provides three types of Layer2 Interface:

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

4.1.1 Setting the ATM connection

4.1.1.1 Creating an ATM interface.

Step 1 Choose **Advanced Setup > Layer2 Interface > ATM Interface** to enter the following page, and click **Add**.

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
<input type="button" value="Add"/> <input type="button" value="Remove"/>													

Step 2 Enter the **VPI** and **VCI** values provided by your ISP.

Step 3 Select a DSL Link Type according to the instructions in the table below, and leave other options unchanged. Select **EoA** when your link type is PPPoE, IPoE, or Bridge.

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

ATM PVC Configuration

This screen allows you to configure a ATM PVC.

VPI: [0-255]
VCI: [32-65535]

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

EoA
 PPPoA
 IPoA

Encapsulation Mode: ▼

Service Category: ▼

Select Scheduler for Queues of Equal Precedence

Round Robin (weight=1)
 Weighted Fair Queuing
Default Queue Weight: [1-63]

Default Queue Precedence: [1-8] (lower value, higher priority)
Note: For WFQ, the default queue precedence will be applied to all other queues in the VC.

Default Queue Drop Algorithm

DT (Drop Tail)

----End

Parameter description

Parameter	Description
Connection Type	<ul style="list-style-type: none"> • PPPoE (PPP over Ethernet), PPPoA (PPP over ATM): If your ISP (ISP) provides a user name and password to you for internet access, your connection type may be PPPoE or PPPoA, contact your ISP for details. • IPoE (IP over Ethernet) - Dynamic IP: Select this type if your ISP does not provide any parameters to you for internet access. • IPoE (IP over Ethernet) - Static IP, IPoA (IP over ATM) - Static IP: If your ISP provides a static IP address and other related information to you for internet access, your connection type may be IPoE or IPoA, contact your ISP for details. • Bridge: Select this type when this device only serves as a modem, and you want to set up a dial-up connection or enter other internet parameters directly on your computer for internet access.
Encapsulation Mode	It specifies the data encapsulation type in the ATM network. LLC and VC/MUX are supported. The default is recommended.
Service Category	It specifies the ATM QoS type assigned by the ISP. The default is recommended.

Select the default scheduler for the queues with equal precedence.

Select Scheduler for Queues of Equal Precedence

- Round Robin: It assigns different weights for different kinds of packets and provides the packets with different bandwidths based on the weights.
- Weighted Fair Queuing: It divides groups into different queues based on the service streaming, IP precedence, and Hash algorithm, and fairly assigns the bandwidth to the services with low precedence according to the weights while ensuring the performance of services with high precedence.

Default Queue It specifies to set up the weight of the default queue.

Default Queue It specifies to set up the precedence of the default queue.

Default Queue Drop It specifies the default queue drop algorithm. It cannot be changed.

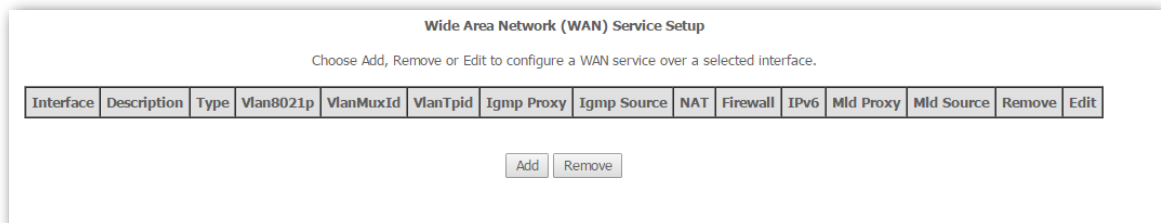
4.1.1.2 Setting up a WAN Service for the ATM Interface

PPPoE

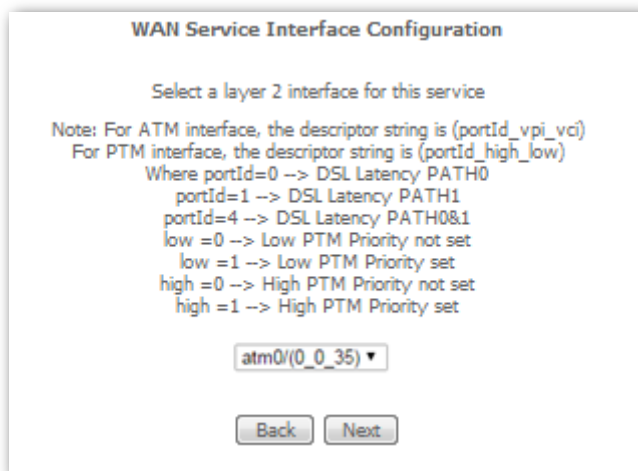
Choose the corresponding procedure to follow according to your IP address type: [IPv4 PPPoE](#), [IPv4&IPv6 PPPoE](#), and [IPv6 PPPoE](#).

IPv4 PPPoE

Step 1 Choose **Advanced Setup > WAN Service** to enter the following page, and click **Add**.



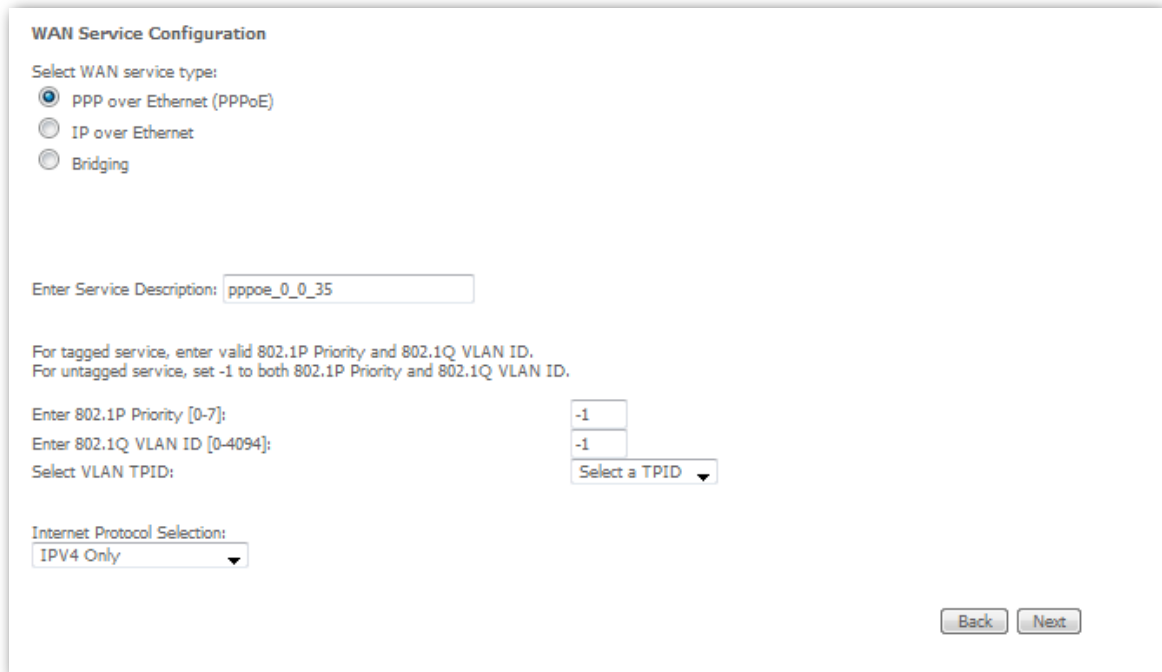
Step 2 Select ATM interface you create on the Layer2 Interface page, which is **atm0/(0_0_35)** in this example, and click **Next**.



Step 3 Select **PPP over Ethernet (PPPoE)**.

Step 4 Enter the **802.1P Priority** and **802.1Q VLAN ID**, and select the **VLAN TPID** according to the VLAN parameters provided by your ISP.

Step 5 Select **IPv4 Only** and click **Next**.



WAN Service Configuration

Select WAN service type:

- PPP over Ethernet (PPPoE)
- IP over Ethernet
- Bridging

Enter Service Description:

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.

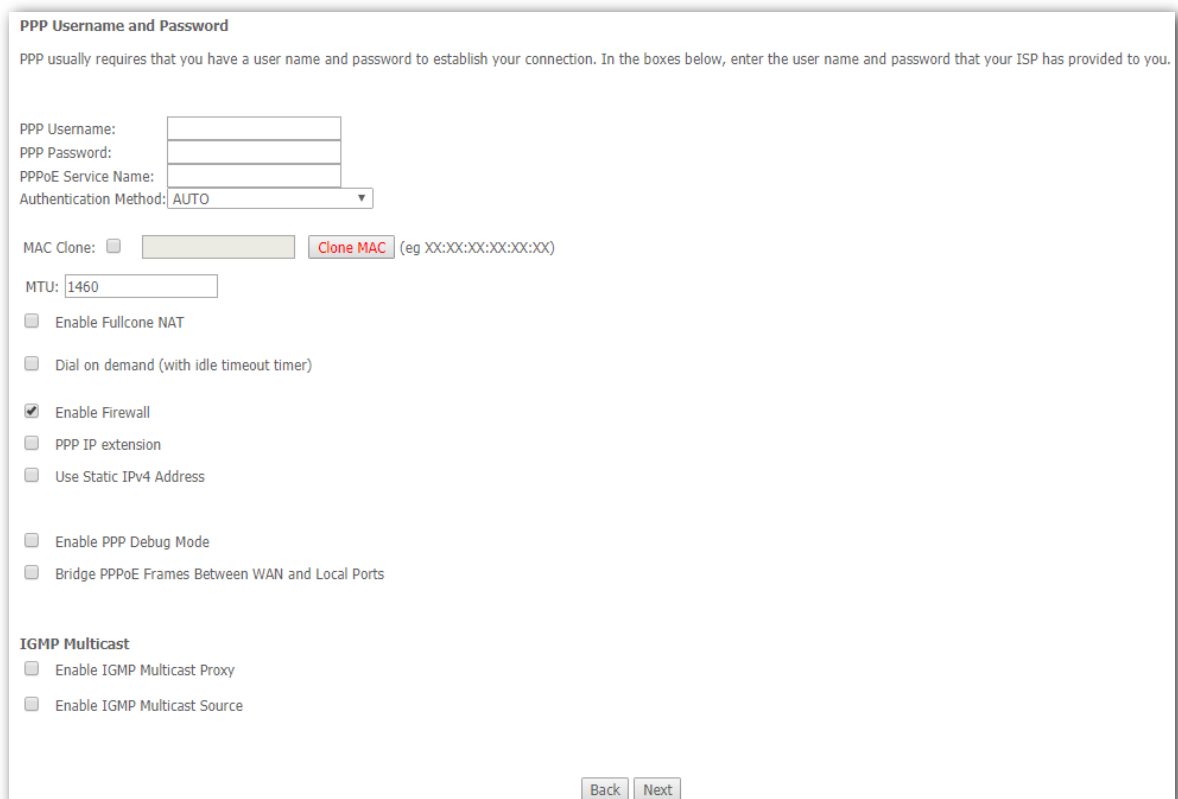
Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [0-4094]:

Select VLAN TPID:

Internet Protocol Selection:

Step 6 Enter the PPPoE user name and password provided by your ISP, and set other parameters as required.



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:

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

MTU:

- Enable Fullcone NAT
- Dial on demand (with idle timeout timer)
- Enable Firewall
- PPP IP extension
- Use Static IPv4 Address
- Enable PPP Debug Mode
- Bridge PPPoE Frames Between WAN and Local Ports

IGMP Multicast

- Enable IGMP Multicast Proxy
- Enable IGMP Multicast Source

Parameter description

Parameter	Description
PPPoE Service Name	If your ISP provides this name, enter it here. Otherwise, leave it blank.
Authentication Method	It specifies the authentication method the ISP-side uses to authenticate the client. If you do not certain about it, select AUTO.
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.
MTU	It specifies the maximum size of packet that the router can transmit. MTU varies across connection types.
Enable Fullcone NAT	Data transmitted by a computer in LAN through the UDP port A will be forwarded to the UDP port B in WAN. And data received by the UDP port B in WAN will be forwarded to the UDP port A of the corresponding computer in LAN.
Dial on demand (with idle timeout timer)	When there is no data exchange within the specified time, the device disconnects the connection between its WAN port and the ISP. Flow-based charging users can select this option to save cost. Month-based charging users do not need to select the option.
Enable Firewall	Check this option to enable the firewall of the modem router.
PPP IP extension	If this option is selected: <ul style="list-style-type: none">• The NAT and firewall functions are disabled.• Only a computer in LAN can obtain the IP address which is the same as that of the WAN port to access the internet. Other computers cannot obtain IP addresses to access the internet.
Use Static IPv4 Address	It is used to set up the IP address assigned by the ISP after the PPPoE dial-up succeeds. Do not set up it if you are not a professional.
Enable PPP Debug Mode	If it is enabled, you can check the PPPoE dial-up information on the System Log page. It is used to diagnose dial-up malfunctions.
Bridge PPPoE Frames Between WAN and Local Ports	If it is enabled, computers in LAN can share the WAN connection for internet access, use multiple active PPPoE accounts to access the internet (if any).
Enable IGMP Multicast Proxy	If it is enabled, the modem router can forward the multicast data to the users in LAN. If you requires multicast applications, such as VOD or AOD, you can

Step 7 Leave the configuration unchanged on **Routing - Default Gateway** page, 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 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	Available Routed WAN Interfaces
ppp0.1	eth6 ppp3g



Default gateway interface list can contain multiple WAN interfaces serving as system default gateways.

Step 8 If your ISP provides you with the DNS IP addresses, select **Use the following Static DNS IP address**, and enter the DNS IP addresses information. If not, select the option **Select DNS Server Interface from available WAN interfaces**, and 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 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.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces	Available WAN Interfaces
ppp0.1	eth6 ppp3g

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

Step 9 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 Proxy:	Disabled
IGMP Multicast Source Enabled:	Disabled
MLD Multicast Proxy:	Disabled
MLD Multicast Source Enabled:	Disabled
Quality Of Service:	Disabled

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

[Back](#) [Apply/Save](#)

----End

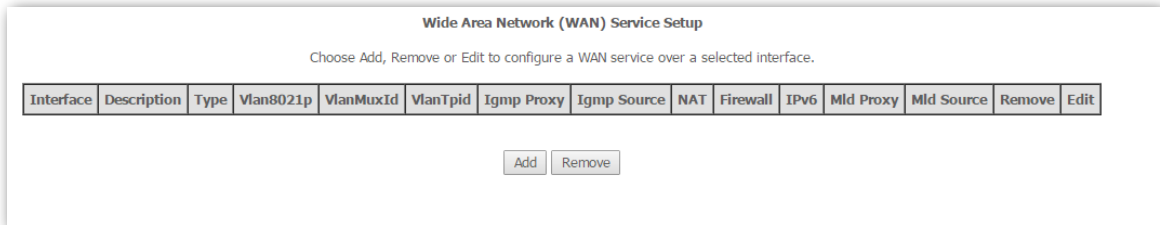
The WAN service you set is shown on the **WAN Service** page.

Wide Area Network (WAN) Service Setup														
Choose Add, Remove or Edit to configure a WAN service over a selected interface.														
Interface	Description	Type	Vlan8021p	VlanMuxId	VlanTpid	Igmp Proxy	Igmp Source	NAT	Firewall	IPv6	Mld Proxy	Mld Source	Remove	Edit
ppp0.1	pppoe_0_0_35	PPPoE	N/A	N/A	N/A	Disabled	Disabled	Enabled	Enabled	Disabled	Disabled	Disabled	<input type="checkbox"/>	Edit

[Add](#) [Remove](#)

IPv4&IPv6 PPPoE

Step 1 Choose **Advanced Setup > WAN Service** to enter the following page, and click **Add**.

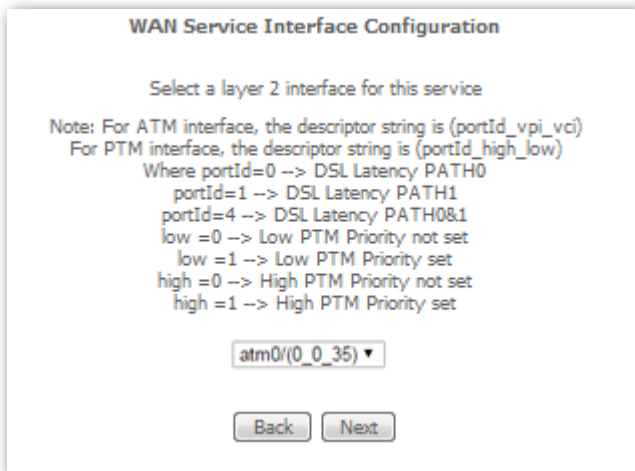


Wide Area Network (WAN) Service Setup

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

Interface	Description	Type	Vlan8021p	VlanMuxId	VlanTpid	Igmp Proxy	Igmp Source	NAT	Firewall	IPv6	Mld Proxy	Mld Source	Remove	Edit
-----------	-------------	------	-----------	-----------	----------	------------	-------------	-----	----------	------	-----------	------------	--------	------

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



WAN Service Interface Configuration


Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portId_vpi_vci)
For PTM interface, the descriptor string is (portId_high_low)
Where portId=0 --> DSL Latency PATH0
portId=1 --> DSL Latency PATH1
portId=4 --> DSL Latency PATH0&1
low =0 --> Low PTM Priority not set
low =1 --> Low PTM Priority set
high =0 --> High PTM Priority not set
high =1 --> High PTM Priority set

Step 3 Select **PPP over Ethernet (PPPoE)**.

Step 4 Enter the **802.1P Priority** and **802.1Q VLAN ID**, and select the **VLAN TPID** according to the VLAN parameters provided by your ISP.

Step 5 Select **IPv4&IPv6(Dual Stack)** and click **Next**.



WAN Service Configuration

Select WAN service type:

PPP over Ethernet (PPPoE)
 IP over Ethernet
 Bridging

Enter Service Description:

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]:

Enter 802.1Q VLAN ID [0-4094]:

Select VLAN TPID:

Internet Protocol Selection:

Step 6 Enter the PPPoE user name and password provided by your ISP, and set other parameters as required.

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.

PPP Username:

PPP Password:

PPPoE Service Name:

Authentication Method:

MAC Clone: **Clone MAC** (eg XX:XX:XX:XX:XX:XX)

MTU:

Enable Fullcone NAT

Dial on demand (with idle timeout timer)

Enable Firewall

PPP IP extension

Use Static IPv4 Address

Use Static IPv6 Address

Enable IPv6 Unnumbered Model

Launch Dhcp6c for Address Assignment (IANA)

Launch Dhcp6c for Prefix Delegation (IAPD)

Enable PPP Debug Mode

Bridge PPPoE Frames Between WAN and Local Ports

IGMP Multicast

Enable IGMP Multicast Proxy

Enable IGMP Multicast Source

MLD Multicast

Enable MLD Multicast Proxy

Enable MLD Multicast Source

Parameter description

Parameter	Description
PPPoE Service Name	If your ISP provides this name, enter it here. Otherwise, leave it blank.
Authentication Method	It specifies the authentication method the ISP-side uses to authenticate the client. If you do not certain about it, select AUTO.
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.
MTU	It specifies the maximum size of packet that the router can transmit. MTU varies across connection types.

Parameter	Description
Enable Fullcone NAT	Data transmitted by a computer in LAN through the UDP port A will be forwarded to the UDP port B in WAN. And data received by the UDP port B in WAN will be forwarded to the UDP port A of the corresponding computer in LAN.
Dial on demand (with idle timeout timer)	When there is no data exchange within the specified time, the device disconnects the connection between its WAN port and the ISP. Flow-based charging users can select this option to save cost. Month-based charging users do not need to select the option.
Enable Firewall	Check this option to enable the firewall of the modem router.
PPP IP extension	<p>If this option is selected:</p> <ul style="list-style-type: none"> • The NAT and firewall functions are disabled. • Only a computer in LAN can obtain the IP address which is the same as that of the WAN port to access the internet. Other computers cannot obtain IP addresses to access the internet.
Use Static IPv4 Address	It is used to set up the IPv4 IP address assigned by the ISP after the PPPoE dial-up succeeds. Do not set up it if you are not instructed by a professional.
Use Static IPv6 Address	It is used to set up the IP address assigned by the ISP after the PPPoE dial-up succeeds. Do not set up it if you are not instructed by a professional.
Enable IPv6 Unnumbered Model	It is used to enable the IPv6 unnumbered model. If your ISP is not required to select it, keep the default.
Launch Dhcp6c for Address Assignment (IANA)	If it is enabled, the device obtains the IPv6 WAN address using the stateful DHCPv6 type.
Launch Dhcp6c for Prefix Delegation (IAPD)	If it is enabled, the device gets the IPv6 prefix from the DHCPv6 server, and delivers it to its LAN ports.
Enable PPP Debug Mode	If it is enabled, you can check the PPPoE dial-up information on the System Log page. It is used to diagnose dial-up malfunctions.
Bridge PPPoE Frames Between WAN and Local Ports	If it is enabled, computers in LAN can share the WAN connection for internet access, use multiple active PPPoE accounts to access the internet (if any).
Enable IGMP Multicast Proxy	If it is enabled, the modem router can forward the multicast data to the users in LAN. If you requires multicast applications, such as VOD or AOD, you can
Enable MLD Multicast Proxy	It is used to enable the MLD multicast proxy.

Step 7 Leave the configuration unchanged on **Routing - Default Gateway** page, 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 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

eth3.1

->

<-

Available Routed WAN Interfaces

ppp0.1

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

Selected WAN Interface:



Default gateway interface list can contain multiple WAN interfaces serving as system default gateways.

Step 8 If your ISP provides you with the DNS IP addresses, select **Use the following Static DNS IP address/Use the following Static IPv6 DNS IP address**, and enter the DNS IP addresses. If not, select the option **Select DNS Server Interface from available WAN interfaces/Obtain IPv6 DNS info from a WAN interface**, and 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 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.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces

eth3.1

->

<-

Available WAN Interfaces

ppp0.1

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

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:

Use the following Static IPv6 DNS address:

Primary IPv6 DNS server:

Secondary IPv6 DNS server:

Step 9 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 Proxy:	Disabled
IGMP Multicast Source Enabled:	Disabled
MLD Multicast Proxy:	Disabled
MLD Multicast Source Enabled:	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 on the **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	Vlan8021p	VlanMuxId	VlanTpid	Igmp Proxy	Igmp Source	NAT	Firewall	IPv6	Mld Proxy	Mld Source	Remove	Edit
ppp0.1	pppoe_0_0_35	PPPoE	N/A	N/A	N/A	Disabled	Disabled	Enabled	Enabled	Enabled	Disabled	Disabled	<input type="checkbox"/>	<input type="button" value="Edit"/>

IPv6 PPPoE

Step 1 Choose **Advanced Setup > WAN Service** to enter the following page, and click **Add**.

Wide Area Network (WAN) Service Setup

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

Interface	Description	Type	Vlan8021p	VlanMuxId	VlanTpid	Igmp Proxy	Igmp Source	NAT	Firewall	IPv6	Mld Proxy	Mld Source	Remove	Edit
-----------	-------------	------	-----------	-----------	----------	------------	-------------	-----	----------	------	-----------	------------	--------	------

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

WAN Service Interface Configuration

Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portId_vpi_vci)
 For PTM interface, the descriptor string is (portId_high_low)
 Where portId=0 --> DSL Latency PATH0
 portId=1 --> DSL Latency PATH1
 portId=4 --> DSL Latency PATH0&1
 low =0 --> Low PTM Priority not set
 low =1 --> Low PTM Priority set
 high =0 --> High PTM Priority not set
 high =1 --> High PTM Priority set

atm0/(0_0_35) ▼

Back Next

Step 3 Select **PPP over Ethernet (PPPoE)**.

Step 4 Enter the **802.1P Priority** and **802.1Q VLAN ID**, and select the **VLAN TPID** according to the VLAN parameters provided by your ISP.

Step 5 Select **IPv6 Only** and click **Next**.

WAN Service Configuration

Select WAN service type:

PPP over Ethernet (PPPoE)
 IP over Ethernet
 Bridging

Enter Service Description:

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]:

Enter 802.1Q VLAN ID [0-4094]:

Select VLAN TPID:

Internet Protocol Selection:

Back Next

Step 6 Enter the PPPoE user name and password provided by your ISP, and set other parameters as required.

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

PPP Username:

PPP Password:

PPPoE Service Name:

Authentication Method:

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

MTU:

Enable Fullcone NAT

Enable Firewall

PPP IP extension

Use Static IPv4 Address

Use Static IPv6 Address

Enable IPv6 Unnumbered Model

Launch Dhcp6c for Address Assignment (IANA)

Launch Dhcp6c for Prefix Delegation (IAPD)

Enable PPP Debug Mode

Bridge PPPoE Frames Between WAN and Local Ports

MLD Multicast

Enable MLD Multicast Proxy

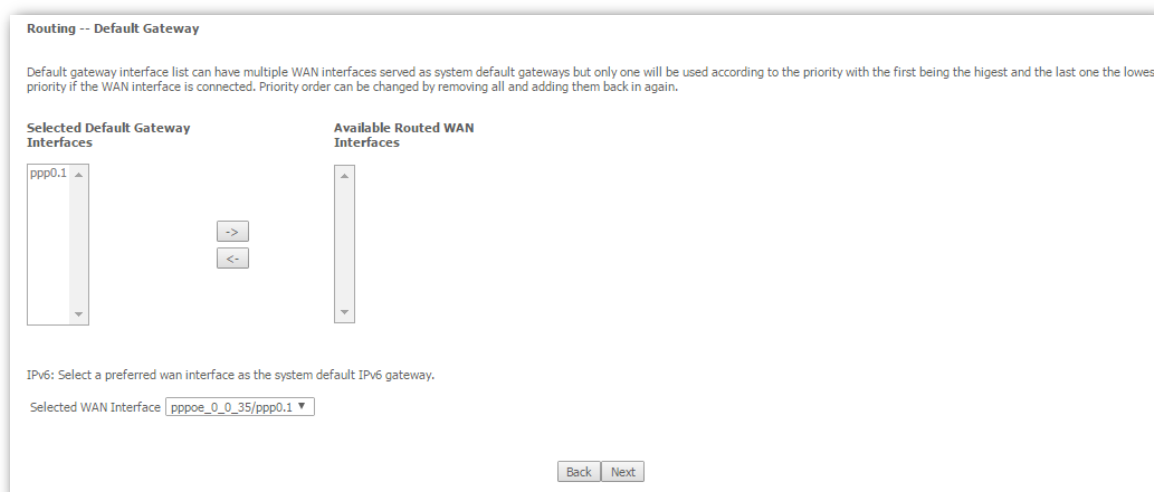
Enable MLD Multicast Source

Parameter description

Parameter	Description
PPPoE Service Name	If your ISP provides this name, enter it here. Otherwise, leave it blank.
Authentication Method	It specifies the authentication method the ISP-side uses to authenticate the client. If you do not certain about it, select AUTO.
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.
MTU	It specifies the maximum size of packet that the router can transmit. MTU varies across connection types.
Enable Fullcone NAT	Data transmitted by a computer in LAN through the UDP port A will be forwarded to the UDP port B in WAN. And data received by the UDP port B in WAN will be forwarded to the UDP port A of the corresponding computer in LAN.

Parameter	Description
Dial on demand (with idle timeout timer)	When there is no data exchange within the specified time, the device disconnects the connection between its WAN port and the ISP. Flow-based charging users can select this option to save cost. Month-based charging users do not need to select the option.
Enable Firewall	Check this option to enable the firewall of the modem router.
PPP IP extension	If this option is selected: <ul style="list-style-type: none"> • The NAT and firewall functions are disabled. • Only a computer in LAN can obtain the IP address which is the same as that of the WAN port to access the internet. Other computers cannot obtain IP addresses to access the internet.
Use Static IPv4 Address	It is used to set up the IPv4 IP address assigned by the ISP after the PPPoE dial-up succeeds. Do not set up it if you are not instructed by a professional.
Use Static Ipv6 Address	It is used to set up the IP address assigned by the ISP after the PPPoE dial-up succeeds. Do not set up it if you are not instructed by a professional.
Enable IPv6 Unnumbered Model	It is used to enable the IPv6 unnumbered model. If your ISP is not required to select it, keep the default.
Launch Dhcp6c for Address Assignment (IANA)	If it is enabled, the device obtains the IPv6 WAN address using the stateful DHCPv6 type.
Launch Dhcp6c for Prefix Delegation (IAPD)	If it is enabled, the device gets the IPv6 prefix from the DHCPv6 server, and delivers it to its LAN ports.
Enable PPP Debug Mode	If it is enabled, you can check the PPPoE dial-up information on the System Log page. It is used to diagnose dial-up malfunctions.
Bridge PPPoE Frames Between WAN and Local Ports	If it is enabled, computers in LAN can share the WAN connection for internet access, use multiple active PPPoE accounts to access the internet (if any).
Enable MLD Multicast Proxy	It is used to enable the MLD multicast proxy.

Step 7 Leave the configuration unchanged on **Routing - Default Gateway** page, and click **Next**.





Default gateway interface list can contain multiple WAN interfaces serving as system default gateways.

- Step 8** If your ISP provides you with the DNS IP addresses, select **Use the following Static IPv6 DNS IP address**, and enter the DNS IP addresses. If not, select the option **Obtain IPv6 DNS info from a WAN interface**, and 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 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.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces: ppp0.1
Available WAN Interfaces: [Empty list]
[->] [-<]

Use the following Static DNS IP address:

Primary DNS server: [Empty text box]
Secondary DNS server: [Empty text box]

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: pppoe_0_0_35/ppp0.1 ▼

Use the following Static IPv6 DNS address:

Primary IPv6 DNS server: [Empty text box]
Secondary IPv6 DNS server: [Empty text box]

- Step 9** 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 Proxy:	Disabled
IGMP Multicast Source Enabled:	Disabled
MLD Multicast Proxy:	Disabled
MLD Multicast Source Enabled:	Disabled
Quality Of Service:	Disabled

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

[Back] [Apply/Save]

----End

The WAN service you set is shown on the **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	Vlan8021p	VlanMuxId	VlanTpid	Igmp Proxy	Igmp Source	NAT	Firewall	IPv6	Mld Proxy	Mld Source	Remove	Edit
ppp0.1	pppoe_0_0_35	PPPoE	N/A	N/A	N/A	Disabled	Disabled	Disabled	Enabled	Enabled	Disabled	Disabled	<input type="checkbox"/>	Edit

IPoE

Choose the corresponding procedure to follow according to your IP address type: [IPv4 IPoE](#), [IPv4&IPv6 IPoE](#), and [IPv6 IPoE](#).

IPv4 IPoE

Step 1 Choose **Advanced Setup > WAN Service** to enter the following page, and click **Add**.

Wide Area Network (WAN) Service Setup

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

Interface	Description	Type	Vlan8021p	VlanMuxId	VlanTpid	Igmp Proxy	Igmp Source	NAT	Firewall	IPv6	Mld Proxy	Mld Source	Remove	Edit
-----------	-------------	------	-----------	-----------	----------	------------	-------------	-----	----------	------	-----------	------------	--------	------

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

WAN Service Interface Configuration

Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portId_vpi_vci)
 For PTM interface, the descriptor string is (portId_high_low)
 Where portId=0 --> DSL Latency PATH0
 portId=1 --> DSL Latency PATH1
 portId=4 --> DSL Latency PATH0&1
 low =0 --> Low PTM Priority not set
 low =1 --> Low PTM Priority set
 high =0 --> High PTM Priority not set
 high =1 --> High PTM Priority set

atm0/(0_0_35) ▾

Step 3 Select **IP over Ethernet**.

Step 4 Enter the **802.1P Priority** and **802.1Q VLAN ID**, and select the **VLAN TPID** according to the VLAN parameters provided by your ISP.

Step 5 Select **IPv4 Only** and click **Next**.

WAN Service Configuration

Select WAN service type:

PPP over Ethernet (PPPoE)
 IP over Ethernet
 Bridging

Enter Service Description:

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]:

Enter 802.1Q VLAN ID [0-4094]:

Select VLAN TPID:

Internet Protocol Selection:

Step 6 Set the WAN IP address.

- **Obtain an IP address automatically:** If your ISP does NOT provide you with the IP address information, select this option.
- **Use the following Static IP address:** If your ISP provides you with the IP address information, select this option and enter them.

Step 7 Set other parameters as required, and click **Next**.

WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.
 Notice: If "Obtain an IP address automatically" is chosen, DHCP will be enabled for PVC in IPoE mode.
 If "Use the following Static IP address" is chosen, enter the WAN IP address, subnet mask and interface gateway.

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

MTU: (576-1500,default:1500)

Obtain an IP address automatically

Option 60 Vendor ID:

Option 61 IAID: (8 hexadecimal digits)

Option 61 DUID: (hexadecimal digit)

Option 77 User ID:

Option 125: Disable Enable

Option 50 Request IP Address:

Option 51 Request Leased Time:

Option 54 Request Server Address:

Use the following Static IP address:

WAN IP Address:

WAN Subnet Mask:

WAN gateway IP Address:

Parameter description

Parameter	Description
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.
MTU	It specifies the maximum size of packet that the router can transmit. MTU varies across connection types.
Option 60 Vendor ID	It is used by the client to report its manufactory and configuration information.
Option 61 IAID	It is used to specify the IAID value of DHCP option 61 client-identifier.
Option 61 DUID	It is used to specify the DUID value of DHCP option 61.
Option 77 User ID	It is used to specify the User ID of DHCP option 77.
Option 125	It specifies the vendor-Identifying Vendor option. If you are not instructed by a professional, the default is recommended.
Option 50 Request IP Address	It is used to specify the request IP address of DHCP option 50.

Parameter	Description
Option 51 Request Leased Time	It is used to specify the request leased of DHCP option 51.
Option 54 Request Server Address	It is used to specify the request server address of DHCP option 54.

Step 8 Select the options as required based on the parameter description form below.

Parameter description

Parameter	Description
Enable NAT	It is used to enable the NAT.
Enable Fullcone NAT	Data transmitted by a computer in LAN through the UDP port A will be forwarded to the UDP port B in WAN. And data received by the UDP port B in WAN will be forwarded to the UDP port A of the corresponding computer in LAN.
Enable Firewall	Check this option to enable the firewall of the modem router.
Enable IGMP Multicast Proxy	If it is enabled, the modem router can forward the multicast data to the users in LAN. If you requires multicast applications, such as VOD or AOD, you can enable this option.

Step 9 Leave the configuration unchanged on **Routing - Default Gateway** page, 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 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

atm0.1

Available Routed WAN Interfaces

> <

Back Next



Default gateway interface list can contain multiple WAN interfaces serving as system default gateways.

Step 10 If your ISP provides you with the DNS IP addresses, select **Use the following Static DNS IP address**, and enter the DNS IP addresses information. If not, select the option **Select DNS Server Interface from available WAN interfaces**, and 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 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.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces

atm0.1

Available WAN Interfaces

> <

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

Step 11 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:	IPoE
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast Proxy:	Disabled
IGMP Multicast Source Enabled:	Disabled
MLD Multicast Proxy:	Disabled
MLD Multicast Source Enabled:	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 on the **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	Vlan8021p	VlanMuxId	VlanTpid	Igmp Proxy	Igmp Source	NAT	Firewall	IPv6	Mld Proxy	Mld Source	Remove	Edit
atm0.1	ipoe_0_0_35	IPoE	N/A	N/A	N/A	Disabled	Disabled	Enabled	Enabled	Disabled	Disabled	Disabled	<input type="checkbox"/>	<input type="button" value="Edit"/>

IPv4&IPv6 IPoE

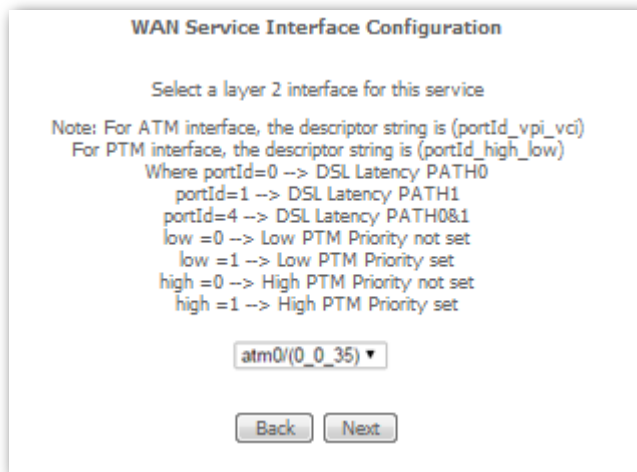
Step 1 Choose **Advanced Setup > WAN Service** to enter the following page, and click **Add**.

Wide Area Network (WAN) Service Setup

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

Interface	Description	Type	Vlan8021p	VlanMuxId	VlanTpid	Igmp Proxy	Igmp Source	NAT	Firewall	IPv6	Mld Proxy	Mld Source	Remove	Edit
-----------	-------------	------	-----------	-----------	----------	------------	-------------	-----	----------	------	-----------	------------	--------	------

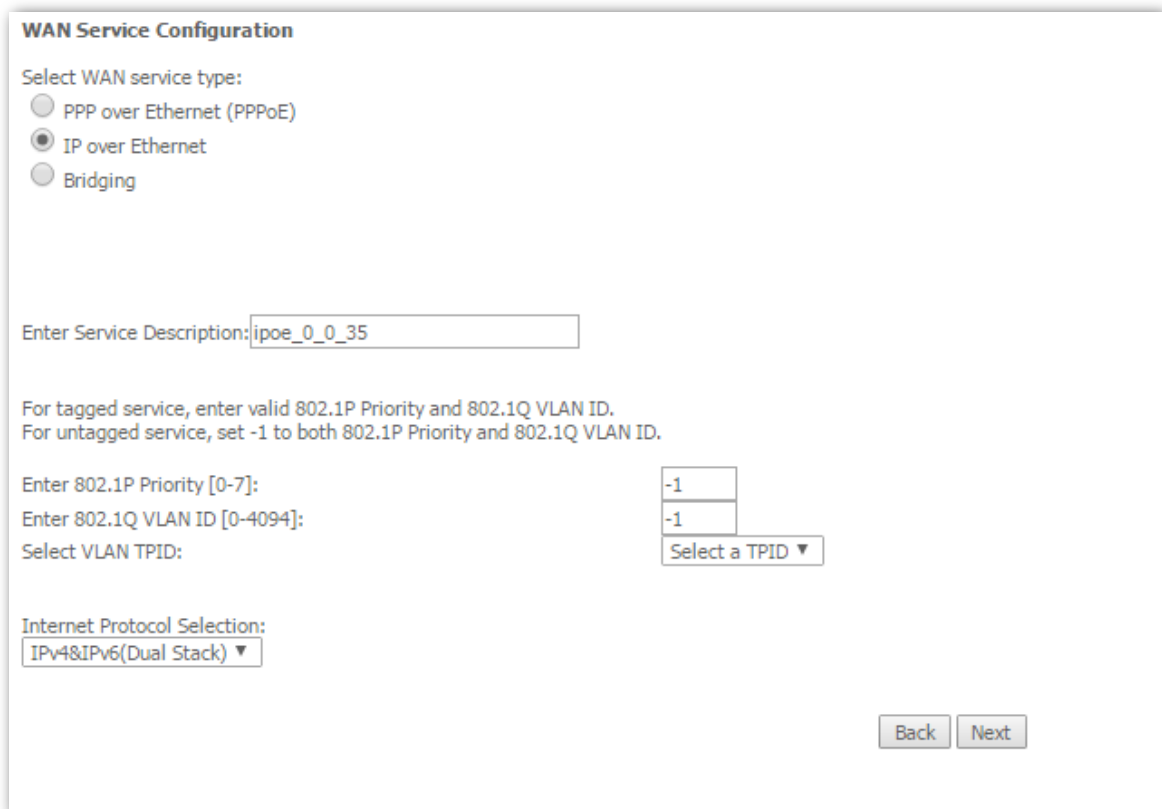
Step 2 Select ATM interface you create on the Layer2 Interface page, which is **atm0/(0_0_35)** in this example, and click **Next**.



Step 3 Select **IP over Ethernet**.

Step 4 Enter the **802.1P Priority** and **802.1Q VLAN ID**, and select the **VLAN TPID** according to the VLAN parameters provided by your ISP.

Step 5 Select **IPv4&IPv6(Dual Stack)** and click **Next**.



Step 6 Set the WAN IP address.

- **Obtain an IP address automatically:** If your ISP does NOT provide you with the IP address information, select this option.
- **Use the following Static IP address:** If your ISP provides you with the IP address information, select this option and enter them.

Step 7 Set other parameters as required, and click **Next**.

WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.
 Notice: If "Obtain an IP address automatically" is chosen, DHCP will be enabled for PVC in IPoE mode.
 If "Use the following Static IP address" is chosen, enter the WAN IP address, subnet mask and interface gateway.

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

MTU: (1280-1500,default:1500)

Obtain an IP address automatically

Option 60 Vendor ID:

Option 61 IAID: (8 hexadecimal digits)

Option 61 DUID: (hexadecimal digit)

Option 77 User ID:

Option 125: Disable Enable

Option 50 Request IP Address:

Option 51 Request Leased Time:

Option 54 Request Server Address:

Use the following Static IP address:

WAN IP Address:

WAN Subnet Mask:

WAN gateway IP Address:

Enter information provided to you by your ISP to configure the WAN IPv6 settings.
 Notice:
 If "Obtain an IPv6 address automatically" is chosen, DHCPv6 Client will be enabled on this WAN interface.
 If "Use the following Static IPv6 address" is chosen, enter the static WAN IPv6 address. If the address prefix length is not specified,

Obtain an IPv6 address automatically

Dhcpv6 Address Assignment (IANA)

Dhcpv6 Prefix Delegation (IAPD)

Use the following Static IPv6 address:

WAN IPv6 Address/Prefix Length:

Specify the Next-Hop IPv6 address for this WAN interface.
 Notice: This address can be either a link local or a global unicast IPv6 address.

WAN Next-Hop IPv6 Address:

Parameter description

Parameter	Description
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.
MTU	It specifies the maximum size of packet that the router can transmit. MTU varies across connection types.
Option 60 Vendor ID	It is used by the client to report its manufactory and configuration information.

Parameter	Description
Option 61 IAID	It is used to specify the IAID value of DHCP option 61 client-identifier.
Option 61 DUID	It is used to specify the DUID value of DHCP option 61.
Option 77 User ID	It is used to specify the User ID of DHCP option 77.
Option 125	It specifies the vendor-Identifying Vendor option. If you are not instructed by a professional, the default is recommended.
Option 50 Request IP Address	It is used to specify the request IP address of DHCP option 50.
Option 51 Request Leased Time	It is used to specify the request leased of DHCP option 51.
Option 54 Request Server Address	It is used to specify the request server address of DHCP option 54.
Obtain an IPv6 address automatically	If your ISP does not provide you with IP address information, select this option to obtain the IP address and other parameters from upstream device.
Dhcpv6 Address Assignment (IANA)	If it is enabled, the device obtains the IPv6 WAN address using the stateful DHCPv6 type.
Dhcpv6 Prefix Delegation (IAPD)	If it is enabled, the device gets the IPv6 prefix from the DHCPv6 server, and delivers it to its LAN ports.
Use the following Static IPv6 address	If your ISP provides you with IP address information, select this option to enter the IP address and other parameters.
WAN Next-Hop IPv6 Address	It specifies the gateway address by default.

Step 8 Select the options as required based on the parameter description form below.

Network Address Translation Settings

Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your

Enable NAT

Enable Fullcone NAT

Enable Firewall

IGMP Multicast

Enable IGMP Multicast Proxy

Enable IGMP Multicast Source

MLD Multicast

Enable MLD Multicast Proxy

Enable MLD Multicast Source

Parameter description

Parameter	Description
Enable NAT	It is used to enable the NAT.
Enable Fullcone NAT	Data transmitted by a computer in LAN through the UDP port A will be forwarded to the UDP port B in WAN. And data received by the UDP port B in WAN will be forwarded to the UDP port A of the corresponding computer in LAN.
Enable Firewall	Check this option to enable the firewall of the modem router.
Enable IGMP Multicast Proxy	If it is enabled, the modem router can forward the multicast data to the users in LAN. If you requires multicast applications, such as VOD or AOD, you can enable this option.
Enable MLD Multicast Proxy	It is used to enable the MLD multicast proxy.

Step 9 Leave the configuration unchanged on **Routing - Default Gateway** page, 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 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

atm0.1

Available Routed WAN Interfaces

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

Selected WAN Interface ipoe_0_0_35/atm0.1

Back Next



Default gateway interface list can contain multiple WAN interfaces serving as system default gateways.

Step 10 If your ISP provides you with the DNS IP addresses, select **Use the following Static DNS IP address/Use the following Static IPv6 DNS IP address**, and enter the DNS IP addresses. If not, select the option **Select DNS Server Interface from available WAN interfaces/Obtain IPv6 DNS info from a WAN interface**, and 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 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.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces

atm0.1

Available WAN Interfaces

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

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: ipoe_0_0_35/atm0.1

Use the following Static IPv6 DNS address:

Primary IPv6 DNS server:

Secondary IPv6 DNS server:

Step 11 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:	IPoE
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast Proxy:	Disabled
IGMP Multicast Source Enabled:	Disabled
MLD Multicast Proxy:	Disabled
MLD Multicast Source Enabled:	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 on the **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	Vlan8021p	VlanMuxId	VlanTpid	Igmp Proxy	Igmp Source	NAT	Firewall	IPv6	Mld Proxy	Mld Source	Remove	Edit
atm0.1	ipoe_0_0_35	IPoE	N/A	N/A	N/A	Disabled	Disabled	Enabled	Enabled	Enabled	Disabled	Disabled	<input type="checkbox"/>	<input type="button" value="Edit"/>

IPv6 IPoE

Step 1 Choose **Advanced Setup > WAN Service** to enter the following page, and click **Add**.

Wide Area Network (WAN) Service Setup

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

Interface	Description	Type	Vlan8021p	VlanMuxId	VlanTpid	Igmp Proxy	Igmp Source	NAT	Firewall	IPv6	Mld Proxy	Mld Source	Remove	Edit
-----------	-------------	------	-----------	-----------	----------	------------	-------------	-----	----------	------	-----------	------------	--------	------

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

WAN Service Interface Configuration

Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portId_vpi_vci)
 For PTM interface, the descriptor string is (portId_high_low)
 Where portId=0 --> DSL Latency PATH0
 portId=1 --> DSL Latency PATH1
 portId=4 --> DSL Latency PATH0&1
 low =0 --> Low PTM Priority not set
 low =1 --> Low PTM Priority set
 high =0 --> High PTM Priority not set
 high =1 --> High PTM Priority set

atm0/(0_0_35) ▾

Back Next

Step 3 Select **IP over Ethernet**.

Step 4 Enter the **802.1P Priority** and **802.1Q VLAN ID**, and select the **VLAN TPID** according to the VLAN parameters provided by your ISP.

Step 5 Select **IPv6 Only** and click **Next**.

WAN Service Configuration

Select WAN service type:

PPP over Ethernet (PPPoE)
 IP over Ethernet
 Bridging

Enter Service Description: ipoe_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

Select VLAN TPID: Select a TPID ▾

Internet Protocol Selection:
 IPv4&IPv6(Dual Stack) ▾

Back Next

Step 6 Set the WAN IP address.

- **Obtain an IP address automatically:** If your ISP does NOT provide you with the IP address information, select this option.
- **Use the following Static IP address:** If your ISP provides you with the IP address information, select this option and enter them.

Step 7 Set other parameters as required, and click **Next**.

WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.
 Notice: If "Obtain an IP address automatically" is chosen, DHCP will be enabled for PVC in IPoE mode.
 If "Use the following Static IP address" is chosen, enter the WAN IP address, subnet mask and interface gateway.

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

MTU: (1280-1500,default:1500)

Obtain an IP address automatically

Option 60 Vendor ID:

Option 61 IAID: (8 hexadecimal digits)

Option 61 DUID: (hexadecimal digit)

Option 77 User ID:

Option 125: Disable Enable

Option 50 Request IP Address:

Option 51 Request Leased Time:

Option 54 Request Server Address:

Use the following Static IP address:

WAN IP Address:

WAN Subnet Mask:

WAN gateway IP Address:

Enter information provided to you by your ISP to configure the WAN IPv6 settings.
 Notice:
 If "Obtain an IPv6 address automatically" is chosen, DHCPv6 Client will be enabled on this WAN interface.
 If "Use the following Static IPv6 address" is chosen, enter the static WAN IPv6 address. If the address prefix length is not specified, it will be default to /64.

Obtain an IPv6 address automatically

Dhcpv6 Address Assignment (IANA)

Dhcpv6 Prefix Delegation (IAPD)

Use the following Static IPv6 address:

WAN IPv6 Address/Prefix Length:

Specify the Next-Hop IPv6 address for this WAN interface.
 Notice: This address can be either a link local or a global unicast IPv6 address.

WAN Next-Hop IPv6 Address:

Parameter description

Parameter	Description
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.
MTU	It specifies the maximum size of packet that the router can transmit. MTU varies across connection types.
Option 60 Vendor ID	It is used by the client to report its manufactory and configuration information.
Option 61 IAID	It is used to specify the IAID value of DHCP option 61 client-indentifier.
Option 61 DUID	It is used to specify the DUID value of DHCP option 61.

Parameter	Description
Option 77 User ID	It is used to specify the User ID of DHCP option 77.
Option 125	It specifies the vendor-Identifying Vendor option. If you are not instructed by a professional, the default is recommended.
Option 50 Request IP Address	It is used to specify the request IP address of DHCP option 50.
Option 51 Request Leased Time	It is used to specify the request leased of DHCP option 51.
Option 54 Request Server Address	It is used to specify the request server address of DHCP option 54.
Obtain an IPv6 address automatically	If your ISP does not provide you with IP address information, select this option to obtain the IP address and other parameters from upstream device.
Dhcpv6 Address Assignment (IANA)	If it is enabled, the device obtains the IPv6 WAN address using the stateful DHCPv6 type.
Dhcpv6 Prefix Delegation (IAPD)	If it is enabled, the device gets the IPv6 prefix form the DHCPv6 server, and delivers it to its LAN ports.
Use the following Static IPv6 address	If your ISP provides you with IP address information, select this option to enter the IP address and other parameters.
WAN Next-Hop IPv6 Address	It specifies the gateway address by default.

Step 8 Select the options as required based on the parameter description form below.

Parameter description

Parameter	Description
Enable NAT	It is used to enable the NAT.
Enable MLD Multicast Proxy	It is used to enable the MLD multicast proxy.

Step 9 Leave the configuration unchanged on **Routing - Default Gateway** page, 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 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

eth3.1 ▲

->

<-

Available Routed WAN Interfaces

atm0.1 ▲

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

Selected WAN Interface:



Default gateway interface list can contain multiple WAN interfaces serving as system default gateways.

Step 10 If your ISP provides you with the DNS IP addresses, select **Use the following Static DNS IP address/Use the following Static IPv6 DNS IP address**, and enter the DNS IP addresses. If not, select the option **Select DNS Server Interface from available WAN interfaces/Obtain IPv6 DNS info from a WAN interface**, and 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 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.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces

eth3.1 ▲

->

<-

Available WAN Interfaces

atm0.1 ▲

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

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:

Use the following Static IPv6 DNS address:

Primary IPv6 DNS server:

Secondary IPv6 DNS server:

Step 11 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:	IPoE
NAT:	Disabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast Proxy:	Disabled
IGMP Multicast Source Enabled:	Disabled
MLD Multicast Proxy:	Disabled
MLD Multicast Source Enabled:	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 on the **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	Vlan8021p	VlanMuxId	VlanTpid	Igmp Proxy	Igmp Source	NAT	Firewall	IPv6	Mld Proxy	Mld Source	Remove	Edit
atm0.1	ipoe_0_0_35	IPoE	N/A	N/A	N/A	Disabled	Disabled	Disabled	Enabled	Enabled	Disabled	Disabled	<input type="checkbox"/>	<input type="button" value="Edit"/>

Bridge

Step 1 Choose **Advanced Setup > WAN Service** to enter the following page, and click **Add**.

Wide Area Network (WAN) Service Setup

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

Interface	Description	Type	Vlan8021p	VlanMuxId	VlanTpid	Igmp Proxy	Igmp Source	NAT	Firewall	IPv6	Mld Proxy	Mld Source	Remove	Edit
-----------	-------------	------	-----------	-----------	----------	------------	-------------	-----	----------	------	-----------	------------	--------	------

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

WAN Service Interface Configuration

Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portId_vpi_vci)
 For PTM interface, the descriptor string is (portId_high_low)
 Where portId=0 --> DSL Latency PATH0
 portId=1 --> DSL Latency PATH1
 portId=4 --> DSL Latency PATH0&1
 low =0 --> Low PTM Priority not set
 low =1 --> Low PTM Priority set
 high =0 --> High PTM Priority not set
 high =1 --> High PTM Priority set

atm0/(0_0_35) ▾

Step 3 Select **Bridging**, set other parameters as required, and click **Next**.

WAN Service Configuration

Select WAN service type:

PPP over Ethernet (PPPoE)
 IP over Ethernet
 Bridging
 Allow as IGMP Multicast Source
 Allow as MLD Multicast Source

Enter Service Description:

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]:

Enter 802.1Q VLAN ID [0-4094]:

Select VLAN TPID:

Step 4 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:	Bridge
NAT:	Disabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast Proxy:	Not Applicable
IGMP Multicast Source Enabled:	Enabled
MLD Multicast Proxy:	Not Applicable
MLD Multicast Source Enabled:	Enabled
Quality Of Service:	Disabled

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

Back

Apply/Save

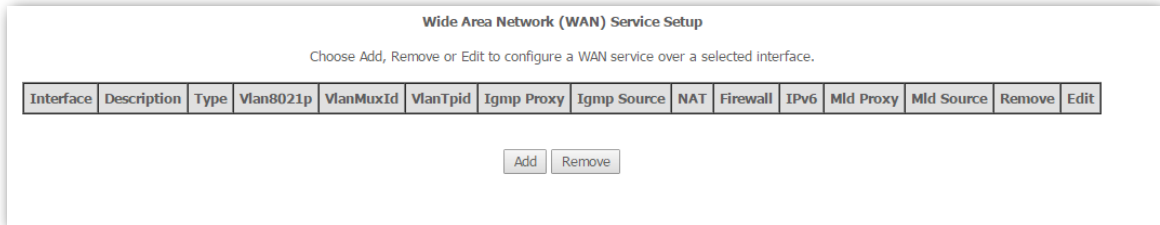
----End

After the settings take effect, you need to set the internet settings on the devices connected to the modem router for internet access.

PPPoA (Only for internet access through phone cable)

If the DSL Link Type is set to PPPoA when you create an ATM interface, refer to the following procedure.

Step 1 Choose **Advanced Setup > WAN Service** to enter the following page, and click **Add**.

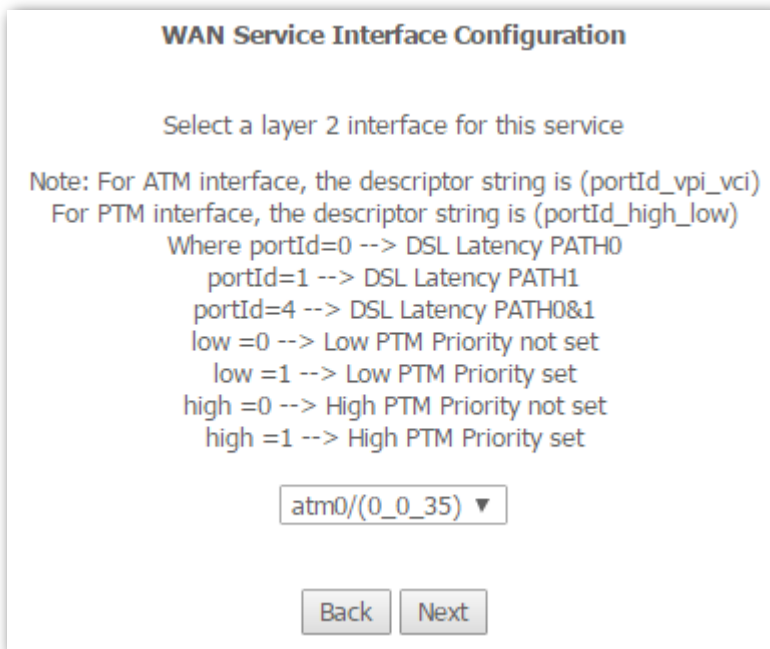


Wide Area Network (WAN) Service Setup

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

Interface	Description	Type	Vlan8021p	VlanMuxId	VlanTpid	Igmp Proxy	Igmp Source	NAT	Firewall	IPv6	Mld Proxy	Mld Source	Remove	Edit
-----------	-------------	------	-----------	-----------	----------	------------	-------------	-----	----------	------	-----------	------------	--------	------

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



WAN Service Interface Configuration

Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portId_vpi_vci)
For PTM interface, the descriptor string is (portId_high_low)
Where portId=0 --> DSL Latency PATH0
portId=1 --> DSL Latency PATH1
portId=4 --> DSL Latency PATH0&1
low =0 --> Low PTM Priority not set
low =1 --> Low PTM Priority set
high =0 --> High PTM Priority not set
high =1 --> High PTM Priority set

Step 3 Select your internet protocol, and click **Next**. IPv4 is used to illustrate here.



WAN Service Configuration

Enter Service Description:

Internet Protocol Selection:

Step 4 Enter the user name and password provided by your ISP, set other parameters as required,

and 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

PPP Username:

PPP Password:

Authentication Method:

Enable Fullcone NAT

Dial on demand (with idle timeout timer)

Enable Firewall

Use Static IPv4 Address

Enable PPP Debug Mode

IGMP Multicast

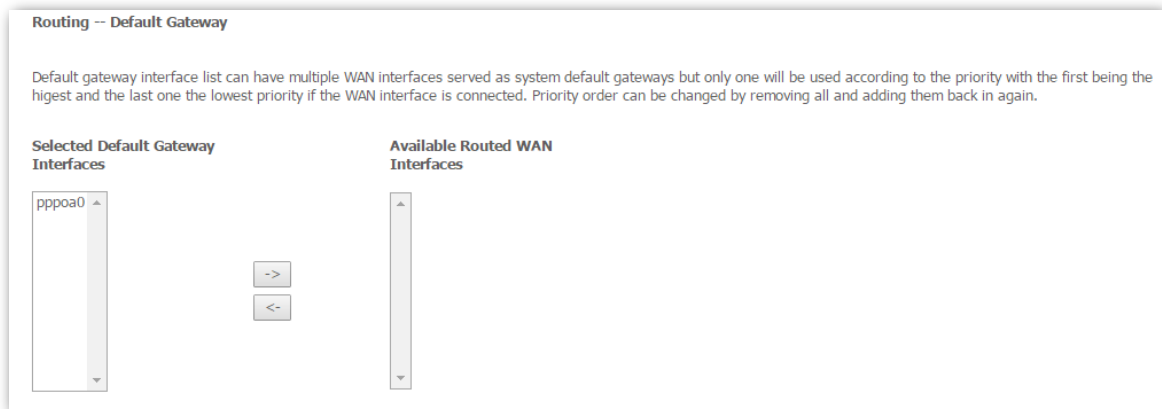
Enable IGMP Multicast Proxy

Enable IGMP Multicast Source

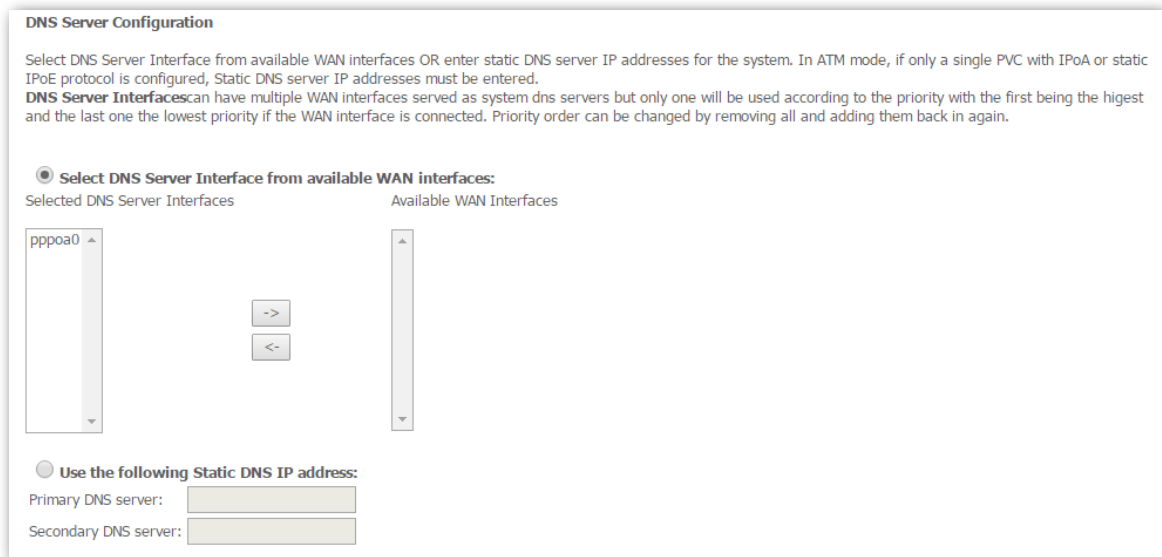
Parameter description

Parameter	Description
Authentication Method	It specifies the authentication method the ISP-side uses to authenticate the client. If you do not certain about it, select AUTO.
Enable Fullcone NAT	Data transmitted by a computer in LAN through the UDP port A will be forwarded to the UDP port B in WAN. And data received by the UDP port B in WAN will be forwarded to the UDP port A of the corresponding computer in LAN.
Dial on demand (with idle timeout timer)	When there is no data exchange within the specified time, the device disconnects the connection between its WAN port and the ISP. Flow-based charging users can select this option to save cost. Month-based charging users do not need to select the option.
Enable Firewall	Check this option to enable the firewall of the modem router.
Use Static IPv4 Address	It is used to set up the IP address assigned by the ISP after the PPPoE dial-up succeeds. Do not set up it if you are not a professional.
Enable PPP Debug Mode	If it is enabled, you can check the PPPoE dial-up information on the System Log page. It is used to diagnose dial-up malfunctions.
Enable IGMP Multicast Proxy	If it is enabled, the modem router can forward the multicast data to the users in LAN. If you requires multicast applications, such as VOD or AOD, you can

Step 5 Leave the configuration unchanged on **Routing - Default Gateway** page, and click **Next**.



Step 6 If your ISP provides you with the DNS IP addresses, select **Use the following Static DNS IP address**, and enter the DNS IP addresses. If not, select the option **Select DNS Server Interface from available WAN interfaces**, and click **Next**.



Step 7 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:	PPPoA
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast Proxy:	Disabled
IGMP Multicast Source Enabled:	Disabled
MLD Multicast Proxy:	Disabled
MLD Multicast Source Enabled:	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 on the **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	Vlan8021p	VlanMuxId	VlanTpid	Igmp Proxy	Igmp Source	NAT	Firewall	IPv6	Mld Proxy	Mld Source	Remove	Edit
pppoa0	pppoa_0_0_35	PPPoA	N/A	N/A	N/A	Disabled	Disabled	Enabled	Enabled	Disabled	Disabled	Disabled	<input type="checkbox"/>	<input type="button" value="Edit"/>

IPoA (Only for internet access through phone cable)

If the DSL Link Type is set to IPoA when you create an ATM interface, refer to the following procedure.

Step 1 Choose **Advanced Setup > WAN Service** to enter the following page, and click **Add**.

Wide Area Network (WAN) Service Setup

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

Interface	Description	Type	Vlan8021p	VlanMuxId	VlanTpid	Igmp Proxy	Igmp Source	NAT	Firewall	IPv6	Mld Proxy	Mld Source	Remove	Edit
-----------	-------------	------	-----------	-----------	----------	------------	-------------	-----	----------	------	-----------	------------	--------	------

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

WAN Service Interface Configuration

Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portId_vpi_vci)
 For PTM interface, the descriptor string is (portId_high_low)
 Where portId=0 --> DSL Latency PATH0
 portId=1 --> DSL Latency PATH1
 portId=4 --> DSL Latency PATH0&1
 low =0 --> Low PTM Priority not set
 low =1 --> Low PTM Priority set
 high =0 --> High PTM Priority not set
 high =1 --> High PTM Priority set

Step 3 Change the service description if required, and click **Next**.

WAN Service Configuration

Enter Service Description:

Step 4 Enter the WAN IP address and subnet mask provided by your ISP, and click **Next**.

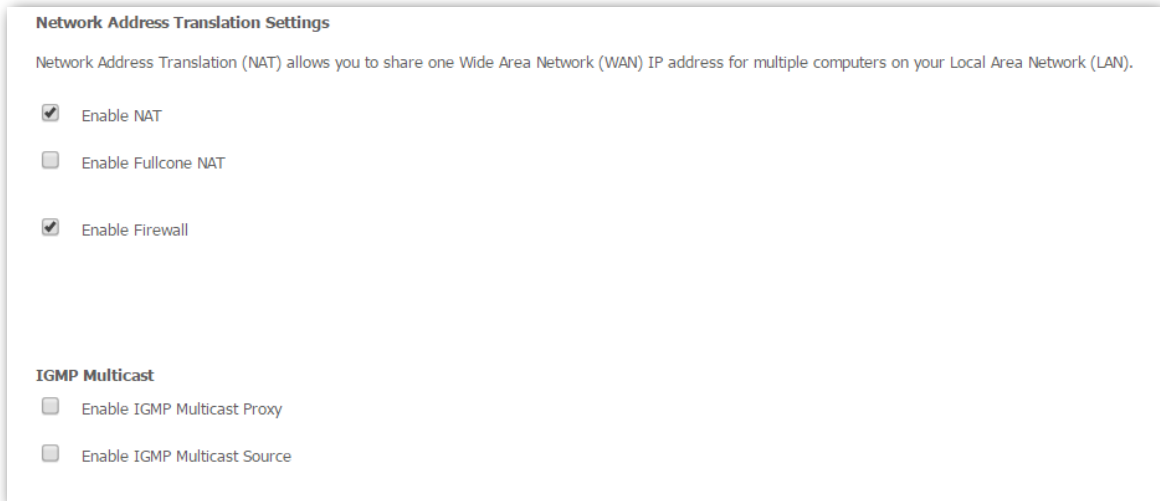
WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.

WAN IP Address:

WAN Subnet Mask:

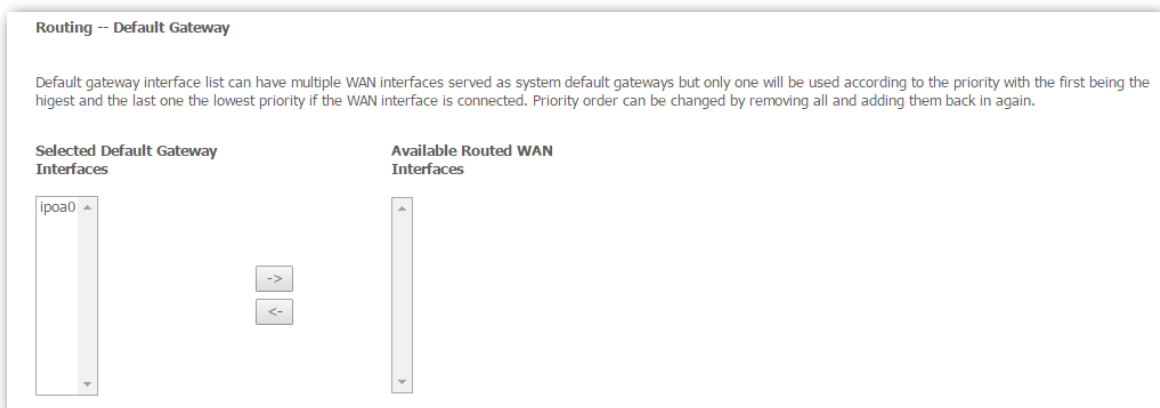
Step 5 Set other parameters as required, and click **Next**.



Parameter description

Parameter	Description
Enable NAT	It is used to enable the NAT.
Enable Fullcone NAT	Data transmitted by a computer in LAN through the UDP port A will be forwarded to the UDP port B in WAN. And data received by the UDP port B in WAN will be forwarded to the UDP port A of the corresponding computer in LAN.
Enable Firewall	Check this option to enable the firewall of the modem router.
Enable IGMP Multicast Proxy	If it is enabled, the modem router can forward the multicast data to the users in LAN. If you requires multicast applications, such as VOD or AOD, you can enable this option.

Step 6 Leave the configuration unchanged on **Routing - Default Gateway** page, and click **Next**.



Step 7 If your ISP provides you with the DNS IP addresses, select **Use the following Static DNS IP address**, and enter the DNS IP addresses. If not, select the option **Select DNS Server Interface from available WAN interfaces**, and 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 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.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces: Available WAN Interfaces

▲

▼

▲

▼

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:	IPoA
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast Proxy:	Disabled
IGMP Multicast Source Enabled:	Disabled
MLD Multicast Proxy:	Disabled
MLD Multicast Source Enabled:	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 on the **WAN Service** page.

Wide Area Network (WAN) Service Setup

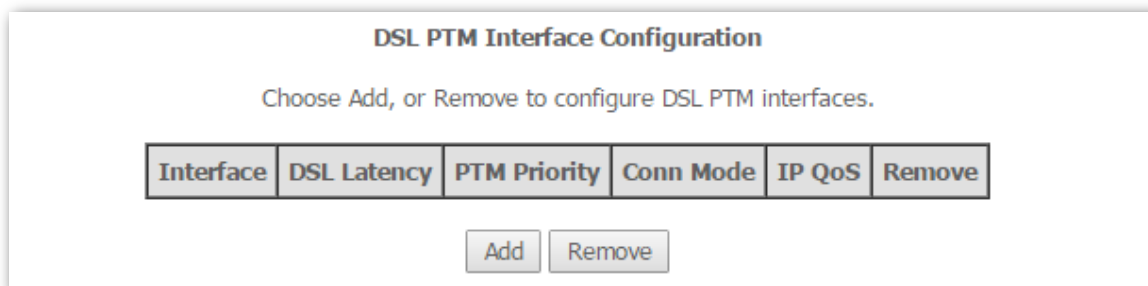
Choose Add, Remove or Edit to configure a WAN service over a selected interface.

Interface	Description	Type	Vlan8021p	VlanMuxId	VlanTpid	Igmp Proxy	Igmp Source	NAT	Firewall	IPv6	Mld Proxy	Mld Source	Remove	Edit
ipoa0	ipoa_0_0_35	IPoA	N/A	N/A	N/A	Disabled	Disabled	Enabled	Enabled	Disabled	Disabled	Disabled	<input type="checkbox"/>	<input type="button" value="Edit"/>

4.1.2 Setting the PTM connection

Step 1 Create a PTM interface.

1. Choose **Advanced Setup > Layer2 Interface > PTM Interface** to enter the following page, and click **Add**.

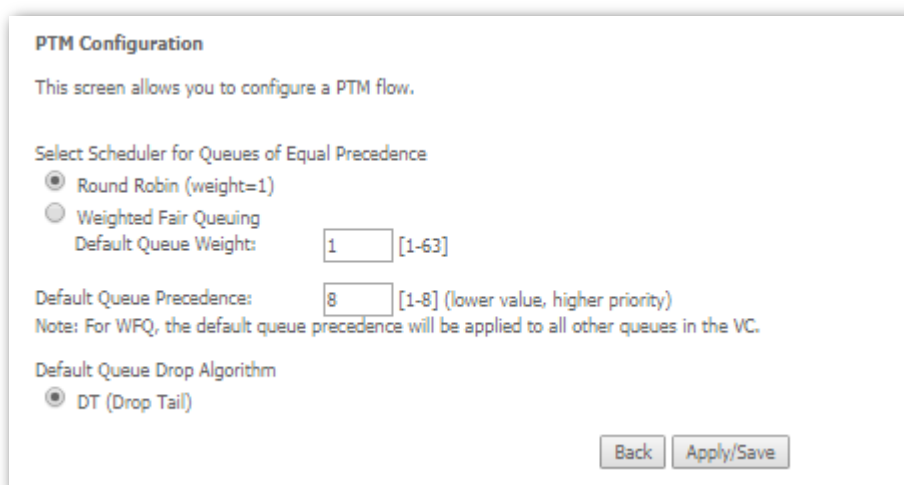


DSL PTM Interface Configuration

Choose Add, or Remove to configure DSL PTM interfaces.

Interface	DSL Latency	PTM Priority	Conn Mode	IP QoS	Remove
<div style="display: flex; justify-content: center; gap: 20px;"> Add Remove </div>					

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



PTM Configuration

This screen allows you to configure a PTM flow.

Select Scheduler for Queues of Equal Precedence

Round Robin (weight=1)
 Weighted Fair Queuing

Default Queue Weight: [1-63]

Default Queue Precedence: [1-8] (lower value, higher priority)

Note: For WFQ, the default queue precedence will be applied to all other queues in the VC.

Default Queue Drop Algorithm

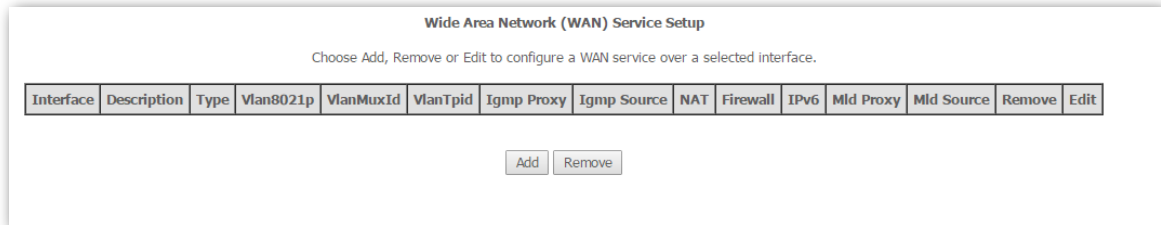
DT (Drop Tail)

Parameter description

Parameter	Description
Select Scheduler for Queues of Equal Precedence	Select the default scheduler for the queues with equal precedence.
Round Robin	It specifies a QoS packet scheduling algorithm. It assigns different weights for different kinds of packets and provides the packets with different bandwidths based on the weights.
Weighted Fair Queuing	It specifies a QoS packet scheduling algorithm. It divides groups into different queues based on the service streaming, IP precedence, and Hash algorithm, and fairly assigns the bandwidth to the services with low precedence according to the weights while ensuring the performance of services with high precedence.
Default Queue Weight	It specifies to set up the weight of the default queue.
Default Queue Precedence	It specifies to set up the precedence of the default queue.
Default Queue Drop Algorithm	It specifies the default queue drop algorithm. It cannot be changed.

Step 2 Set up a WAN service for the PTM interface.

1. Choose **Advanced Setup > WAN Service** to enter the following page, and click **Add**.

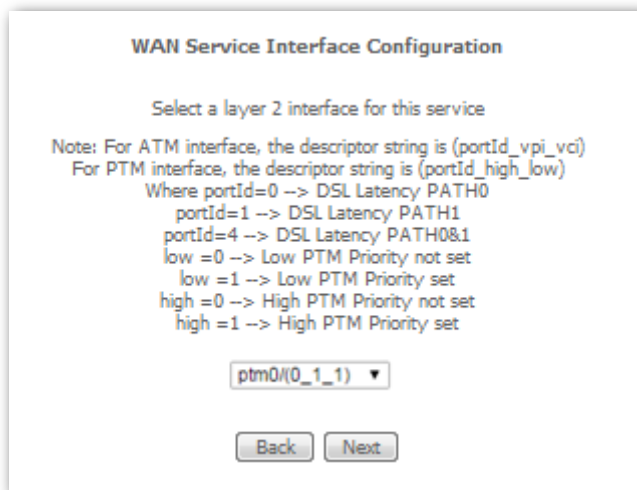


Wide Area Network (WAN) Service Setup

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

Interface	Description	Type	Vlan8021p	VlanMuxId	VlanTpid	Igmp Proxy	Igmp Source	NAT	Firewall	IPv6	Mld Proxy	Mld Source	Remove	Edit
-----------	-------------	------	-----------	-----------	----------	------------	-------------	-----	----------	------	-----------	------------	--------	------

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



WAN Service Interface Configuration

Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portId_vpi_vci)
For PTM interface, the descriptor string is (portId_high_low)
Where portId=0 --> DSL Latency PATH0
portId=1 --> DSL Latency PATH1
portId=4 --> DSL Latency PATH0&1
low =0 --> Low PTM Priority not set
low =1 --> Low PTM Priority set
high =0 --> High PTM Priority not set
high =1 --> High PTM Priority set

3. Select a WAN service type according to the instructions in the table below. Here takes **PPPoE** as an example.
4. Enter the 802.1P priority and 802.1Q VLAN ID parameters provided by your ISP.



If you are unsure about the 802.1P priority and 802.1Q VLAN ID parameters, refer to [Appendix A.3 VLAN List](#). If the parameters are not available, ask your ISP to provide it.

5. Select your network protocol type as required, and click **Next**. IPv4 is used to illustrate here. Refer to [Setting up a WAN Service for the ATM Interface](#) for the instruction of other network protocols.

WAN Service Configuration

Select WAN service type:

PPP over Ethernet (PPPoE)
 IP over Ethernet
 Bridging

Enter Service Description:

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]:
Enter 802.1Q VLAN ID [0-4094]:
Select VLAN TPID:

Internet Protocol Selection:

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

- Enter the user name and password provided by your ISP, set other parameters as required according to the parameter description form, and 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

PPP Username:

PPP Password:

PPPoE Service Name:

Authentication Method:

MAC Clone: [Clone MAC](#) (eg XX:XX:XX:XX:XX:XX)

MTU:

Enable Fullcone NAT

Dial on demand (with idle timeout timer)

Enable Firewall

PPP IP extension

Use Static IPv4 Address

Enable PPP Debug Mode

Bridge PPPoE Frames Between WAN and Local Ports

IGMP Multicast

Enable IGMP Multicast Proxy

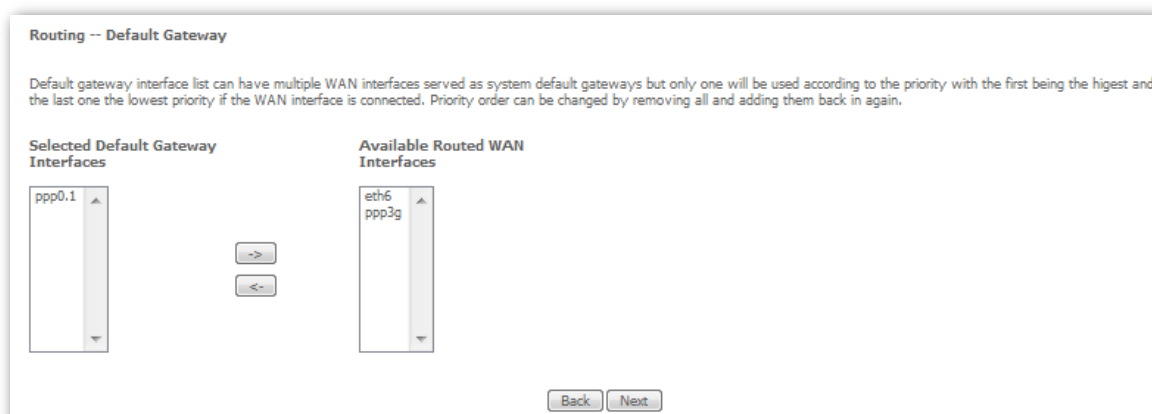
Enable IGMP Multicast Source

Parameter description

Parameter	Description
PPPoE Service Name	If your ISP provides this name, enter it here. Otherwise, leave it blank.
Authentication Method	It specifies the authentication method the ISP-side uses to authenticate the client. If you do not certain about it, select AUTO.
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.
MTU	It specifies the maximum size of packet that the router can transmit. MTU varies across connection types.
Enable Fullcone NAT	Data transmitted by a computer in LAN through the UDP port A will be forwarded to the UDP port B in WAN. And data received by the UDP port B in WAN will be forwarded to the UDP port A of the corresponding computer in LAN.
Dial on demand (with idle timeout timer)	When there is no data exchange within the specified time, the device disconnects the connection between its WAN port and the ISP. Flow-based charging users can select this option to save cost. Month-based charging users do not need to select the option.
Enable Firewall	Check this option to enable the firewall of the modem router.

Parameter	Description
PPP IP extension	<p>If this option is selected:</p> <ul style="list-style-type: none"> • The NAT and firewall functions are disabled. • Only a computer in LAN can obtain the IP address which is the same as that of the WAN port to access the internet. Other computers cannot obtain IP addresses to access the internet.
Use Static IPv4 Address	It is used to set up the IP address assigned by the ISP after the PPPoE dial-up succeeds. Do not set up it if you are not a professional.
Enable PPP Debug Mode	If it is enabled, you can check the PPPoE dial-up information on the System Log page. It is used to diagnose dial-up malfunctions.
Bridge PPPoE Frames Between WAN and Local Ports	If it is enabled, computers in LAN can share the WAN connection for internet access, use multiple active PPPoE accounts to access the internet (if any).
Enable IGMP Multicast Proxy	If it is enabled, the modem router can forward the multicast data to the users in LAN. If you requires multicast applications, such as VOD or AOD, you can

7. Enter the PPPoE user name and password, set other parameters as required based on the parameter description above, and click **Next**.
8. Leave the configuration unchanged on **Routing - Default Gateway** page, and click **Next**.



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

9. If your ISP provides you DNS IP addresses, select **Use the following Static DNS IP address**, and enter the DNS IP addresses information. If not, select **Select DNS Server Interface from available WAN interfaces**, and 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 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.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces: Available WAN Interfaces:

ppp0.1

-->

<--

eth6

ppp3g

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

10. 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 Proxy:	Disabled
IGMP Multicast Source Enabled:	Disabled
MLD Multicast Proxy:	Disabled
MLD Multicast Source Enabled:	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 on the **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	Vlan8021p	VlanMuxId	VlanTpid	Igmp Proxy	Igmp Source	NAT	Firewall	IPv6	Mld Proxy	Mld Source	Remove	Edit
ppp0.1	pppoe_0_1_1	PPPoE	N/A	N/A	N/A	Disabled	Disabled	Enabled	Enabled	Disabled	Disabled	Disabled	<input type="checkbox"/>	<input type="button" value="Edit"/>

4.1.3 Setting the Ethernet connection

Step 1 Create an Ethernet interface.

1. Choose **Advanced Setup > Layer2 Interface > ETH Interface** to enter the following page, and click **Add**.

The screenshot shows the 'ETH WAN Interface Configuration' page. At the top, it says 'Choose Add, or Remove to configure ETH WAN interfaces. Allow one ETH as layer 2 wan interface.' Below this is a table with three columns: 'Interface/(Name)', 'Connection Mode', and 'Remove'. Underneath the table are two buttons: 'Add' and 'Remove'.

2. Click **Apply/Save**.

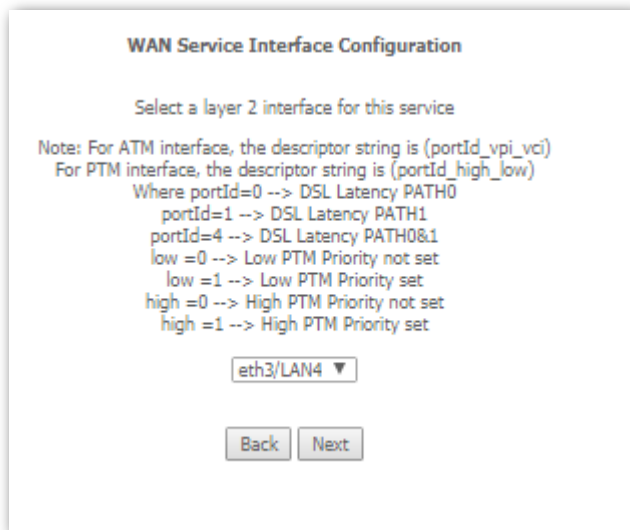
The screenshot shows the 'ETH WAN Configuration' page. It says 'This screen allows you to configure a ETH port.' Below this is the text 'Select a ETH port:' followed by a dropdown menu showing 'eth3/LAN4'. At the bottom are two buttons: 'Back' and 'Apply/Save'.

Step 2 Set up a WAN service for the Ethernet interface.

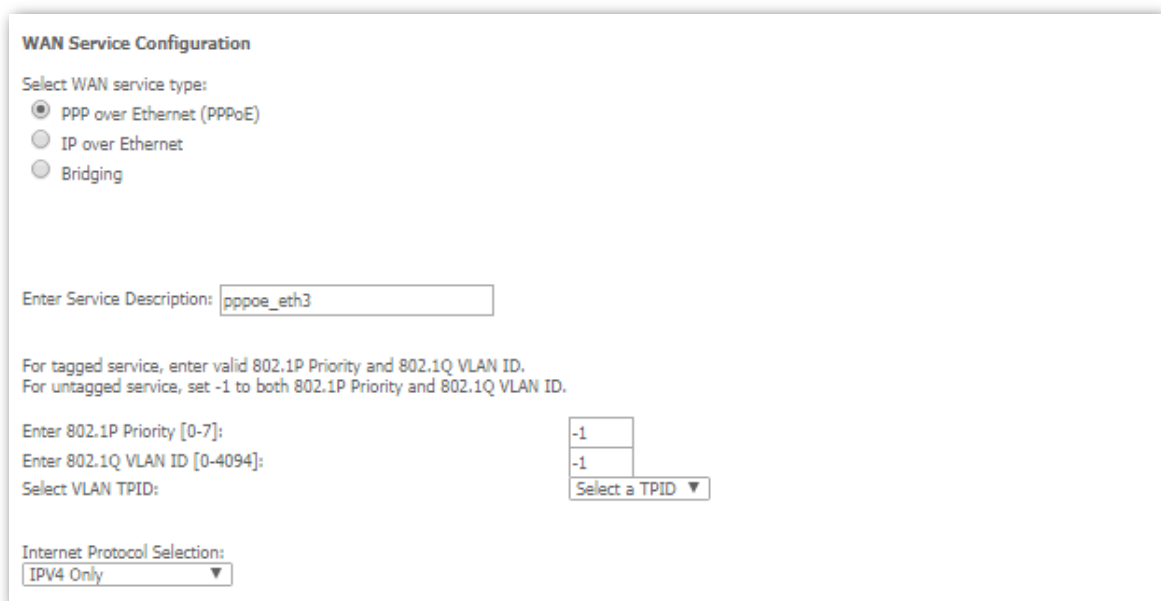
1. Choose **Advanced Setup > WAN Service** to enter the following page, and click **Add**.

The screenshot shows the 'Wide Area Network (WAN) Service Setup' page. It says 'Choose Add, Remove or Edit to configure a WAN service over a selected interface.' Below this is a table with the following columns: Interface, Description, Type, Vlan8021p, VlanMuxId, VlanTpid, Igmp Proxy, Igmp Source, NAT, Firewall, IPv6, Mld Proxy, Mld Source, Remove, and Edit. At the bottom are two buttons: 'Add' and 'Remove'.

2. Select the interface you create in Layer2 Interface, which is **eth3/LAN4** in this example, and click **Next**.



3. Select a WAN service type according to the instructions in the table below. Here takes **PPPoE** as an example.
4. Select your network protocol type as required, and click **Next**. IPv4 is used to illustrate here. Refer to [Setting up a WAN Service for the ATM Interface](#) for the instruction of other network protocols.



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

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

- Enter the user name and password provided by your ISP, set other parameters as required according to the parameter description form, and 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

PPP Username:

PPP Password:

PPPoE Service Name:

Authentication Method:

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

MTU:

Enable Fullcone NAT

Dial on demand (with idle timeout timer)

Enable Firewall

PPP IP extension

Use Static IPv4 Address

Enable PPP Debug Mode

Bridge PPPoE Frames Between WAN and Local Ports

IGMP Multicast

Enable IGMP Multicast Proxy

Enable IGMP Multicast Source

Parameter description

Parameter	Description
PPPoE Service Name	If your ISP provides this name, enter it here. Otherwise, leave it blank.
Authentication Method	It specifies the authentication method the ISP-side uses to authenticate the client. If you do not certain about it, select AUTO.
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.
MTU	It specifies the maximum size of packet that the router can transmit. MTU varies across connection types.

Parameter	Description
Enable Fullcone NAT	Data transmitted by a computer in LAN through the UDP port A will be forwarded to the UDP port B in WAN. And data received by the UDP port B in WAN will be forwarded to the UDP port A of the corresponding computer in LAN.
Dial on demand (with idle timeout timer)	When there is no data exchange within the specified time, the device disconnects the connection between its WAN port and the ISP. Flow-based charging users can select this option to save cost. Month-based charging users do not need to select the option.
Enable Firewall	Check this option to enable the firewall of the modem router.
PPP IP extension	<p>If this option is selected:</p> <ul style="list-style-type: none"> • The NAT and firewall functions are disabled. • Only a computer in LAN can obtain the IP address which is the same as that of the WAN port to access the internet. Other computers cannot obtain IP addresses to access the internet.
Use Static IPv4 Address	It is used to set up the IP address assigned by the ISP after the PPPoE dial-up succeeds. Do not set up it if you are not a professional.
Enable PPP Debug Mode	If it is enabled, you can check the PPPoE dial-up information on the System Log page. It is used to diagnose dial-up malfunctions.
Bridge PPPoE Frames Between WAN and Local Ports	If it is enabled, computers in LAN can share the WAN connection for internet access, use multiple active PPPoE accounts to access the internet (if any).
Enable IGMP Multicast Proxy	If it is enabled, the modem router can forward the multicast data to the users in LAN. If you requires multicast applications, such as VOD or AOD, you can

6. Enter the PPPoE user name and password, set other parameters as required based on the parameter description above, and click **Next**.
7. Leave the configuration unchanged, and click **Next**.





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

8. Enter the DNS IP addresses information if they are provided by your ISP. If not, leave then blank.
9. 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 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.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces Available WAN Interfaces

eth3.1 ▲

-><

<->

ppp0.1 ▲

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

10. 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 Proxy:	Disabled
IGMP Multicast Source Enabled:	Disabled
MLD Multicast Proxy:	Disabled
MLD Multicast Source Enabled:	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 on the **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	Vlan8021p	VlanMuxId	VlanTpid	Igmp Proxy	Igmp Source	NAT	Firewall	IPv6	Mld Proxy	Mld Source	Remove	Edit
ppp0.1	pppoe_eth3	PPPoE	N/A	N/A	N/A	Disabled	Disabled	Enabled	Enabled	Disabled	Disabled	Disabled	<input type="checkbox"/>	Edit

4.2 LAN

Here you can configure the LAN settings. Choose **Advanced Setup > LAN** to enter the configuration page.

It allows you to modify the LAN IP of the modem router, configure the DHCP server settings, and DNS server settings.

4.2.1 Local Area Network (LAN) Setup

4.2.1.1 Primary lan ip address

Local Area Network (LAN) Setup

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

IP Address:

Subnet Mask:

Parameter description

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 LAN port. It specifies the network segment of the LAN IP address.



After the LAN IP address is changed, the computers in LAN need release their IP addresses and obtain them again to ensure gateway of the computers is the new LAN IP address.

4.2.1.2 IGMP snooping

Enable IGMP Snooping

Standard Mode

Blocking Mode

Enable IGMP LAN to LAN Multicast:

(LAN to LAN Multicast is enabled until the first WAN service is connected, regardless of this setting.)

Parameter description

Parameter	Description
Enable IGMP Snooping	IGMP snooping is an IPv4 layer-2 multicast constraint mechanism, which is used to manage and control IPv4 multicast groups. If it is enabled, the specified multicast data of IPv4 multicast groups can be forwarded to the specified LAN port.
Standard Mode	If a multicast group has no member, data of the group will be broadcast. If a multicast group has members, data of the group will be forwarded to the LAN port the members use.
Blocking Mode	If a multicast group has no member, data of the group will be discarded. If a multicast group has members, data of the group will be forwarded to the LAN port the members use.

4.2.1.3 DHCP server

Parameter description

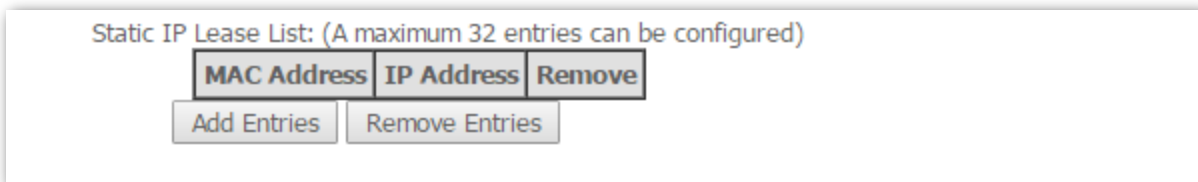
Parameter	Description
Disable DHCP Server	If this option is selected, the DHCP server of this modem router is disabled. In this case, this modem router does not assign IP addresses and related parameters to its clients.
Enable DHCP Server	<p>It indicates that the modem router can assign IP addresses to connected devices.</p> <ul style="list-style-type: none"> • Start IP Address: It specifies the start IP address of the IP address pool of the DHCP server. • End IP Address: It specifies the end IP address of the IP address pool of the DHCP server.
Enable DHCP Server Relay	If this option is selected, the modem router works as a DHCP relay. The DHCP requests from local computers will forward to the DHCP server runs on WAN side.
Leased Time (hour)	It specifies the validity period of one IP address assigned to a device by the modem

Parameter	Description
	router.
Primary DNS server	It specifies the primary DNS IP addresses assigned to connected devices.
Secondary DNS server	It specifies the secondary DNS IP addresses assigned to connected devices.

4.2.1.4 DHCP reservation

Overview

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



Parameter description

Parameter	Description
Static IP Lease List	It 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 added.
Remove Entries	Click to remove a static IP lease entry.

To bind an IP address to a specified device

- Step 1** Choose **Advanced Setup > LAN** to enter the configuration page.
- Step 2** Click **Add Entries**.
- Step 3** Enter the MAC address of the specified device in the **MAC Address** box.
- Step 4** Enter an IP address included in the DHCP pool of the device. Assume that the IP address of the device is **192.168.1.1**. You can enter **192.168.1.X** (X ranges from 2 to 253).
- Step 5** Click **Apply/Save**.

DHCP Static IP Lease

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

MAC Address:

IP Address:

----End

The added entry displays in the following table.

MAC Address	IP Address	Remove
C8:9C:DC:60:54:69	192.168.1.100	<input type="checkbox"/>

The IP address specified in the table will be always assigned to the device with the specified MAC address in the table after the rule takes effect.

4.2.1.5 Secondary lan ip address

Overview

By default, there is only one LAN IP address for the modem router, and you can access the web UI of the modem router by this IP address. And the modem router allows you to set up a second LAN IP address for the modem router.

Configure the second IP Address and Subnet Mask for LAN interface

To set up a second LAN IP address

- Step 1** Check the **Configure the second IP Address and Subnet Mask for LAN interface** option.
- Step 2** Specify an IP address that belongs to a different network segment of the first IP address, such as **192.168.2.1**.
- Step 3** Specify a subnet mask that fits the network segment, such as **255.255.255.0**.
- Step 4** Click **Apply/Save**.

Configure the second IP Address and Subnet Mask for LAN interface

IP Address:

Subnet Mask:

----End



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

4.2.2 Connections limited

4.2.2.1 Overview

This function allows you to specify the maximum connections between the modem router and a specified IP address or IP network segment.

connections limited List -- Maximum 32 entries can be configured.

IP Address	Max Connections	Remove
------------	-----------------	--------

Parameter description

Parameter	Description
IP Address	It specifies the IP address or IP network segment of the clients.
Max Connections	It specifies the maximum number of point-to-point connections that the modem router can handle at the same time.

4.2.2.2 To add a connection limited rule

Step 1 Choose **Advanced Setup > LAN > Connections Limited** to enter the configuration page.

Step 2 Click **Add**.

Step 3 Enter an IP address or an IP network segment.

Step 4 Enter the number of the maximum connections.

Step 5 Click **Apply/Save**.

Lan -- Connections Limited Add

Enter an IP address or an IP network segment and the max connections, then click "Apply/Save" to add the entry.

IP Address:

Max Connections:

----End

4.2.3 IPv6 autoconfig

This section allows you to set up an IPv6 internet connection through auto configuration, including the following 2 parts:

[Static LAN IPv6 Address Configuration](#): Setting up an IPv6 global unicast address for the LAN port.

[IPv6 LAN Applications](#): Setting up the DHCPv6 server to assign IPv6 addresses to the computers in LAN.

Choose **Advanced Setup > LAN > IPv6 Autoconfig** to enter the configuration page.

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 example: Please enter "0:0:0:2" instead of "::2".

Static LAN IPv6 Address Configuration
Interface Address (prefix length is required):

IPv6 LAN Applications

Enable DHCPv6 Server

Stateless
 Stateful

Start interface ID:
End interface ID:
Leased Time (hour):

Enable RADVD

Enable ULA Prefix Advertisement

Randomly Generate
 Statically Configure

Prefix:
Preferred Life Time (hour):
Valid Life Time (hour):

4.2.3.1 Static LAN IPv6 Address Configuration

Overview

This part allows you to set up an IPv6 address for the LAN port, which is an aggregate global unicast address.

Configuration procedure

- Step 1** Choose **Advanced Setup > LAN > IPv6 Autoconfig** to enter the configuration page.
- Step 2** Enter an IPv6 address and the prefix length.
- Step 3** Click **Save/Apply**.

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 example: Please enter "0:0:0:2" instead of "::2".

Static LAN IPv6 Address Configuration
Interface Address (prefix length is required):

----End

The computers in LAN can visit this address to log in to the web UI of the modem router. For example, if the address is set to **2000::1/64**, enter **http://[2000::1]** in the address bar to access the web UI.

4.2.3.2 IPv6 LAN Applications

The Modem router supports two IPv6 address auto-configuration types: [Stateless Address Auto Configuration](#) and [Stateful Address Auto Configuration](#). Select one to follow as required.

Stateless address auto configuration

■ Overview

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

IPv6 LAN Applications

Enable DHCPv6 Server

Stateless
 Stateful

Start interface ID:

End interface ID:

Leased Time (hour):

Enable RADVD

Enable ULA Prefix Advertisement

Randomly Generate
 Statically Configure

Prefix:

Preferred Life Time (hour):

Valid Life Time (hour):

Parameter description

Parameter	Description
Enable DHCPv6 Server	It specifies whether to enable the DHCPv6 Server.
Stateless	The computers in LAN only obtain prefix and DNS information from the modem router. The interface ID is generated based on its MAC address automatically.

Parameter	Description
Enable RADVD	The RADVD (Router Advertisement Daemon) implements link-local advertisements of IPv6 router addresses and IPv6 routing prefixes using the Neighbor Discovery Protocol (NDP) and is used by system administrators for stateless auto configuration of network hosts on Internet Protocol version 6 networks. Select the checkbox to enable the RADVD.
Enable ULA Prefix Advertisement	If enabled, the modem router will advertise ULA prefix periodically. The ULA prefix can be generated by the modem router, or be set up manually.
Randomly Generate	If this option is selected, the ULA prefix can be automatically generated.
Statically Configure	If this option is selected, you need to manually set up the ULA prefix and validity period.
Prefix	It specifies the prefix of the IPv6 address.
Preferred Life Time (hour)	It specifies the preferred life time in hour. When the time is out, the computer can continue to use the address in initiated communications, but cannot use it in new initiated communications.
Valid Life Time (hour)	It specifies the valid life time of the IP address in hour. When the time is out, the address is invalid.

■ Configuration procedure

Step 1 Choose **Advanced Setup > LAN > IPv6 Autoconfig** to enter the configuration page.

Step 2 Select **Enable DHCPv6 Server**.

Step 3 Select **Stateless**.

Step 4 Select **Enable RADVD**.

Step 5 Click **Save/Apply**.

----End

Stateful address auto configuration

■ Overview

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

IPv6 LAN Applications

Enable DHCPv6 Server

Stateless

Stateful

Start interface ID:

End interface ID:

Leased Time (hour):

Enable RADVD

Enable ULA Prefix Advertisement

Randomly Generate

Statically Configure

Prefix:

Preferred Life Time (hour):

Valid Life Time (hour):

Parameter description

Parameter	Description
Stateful	Stateful DHCPv6 is supported based on the assumption of prefix length less than 64. Select this option and configure the start/end interface ID and lease time. The modem router will automatically assign IPv6 addresses to IPv6 clients.
Start interface ID/End interface ID	It specifies 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)	It specifies the validity period of one IP address assigned to a device connected to the modem router.
Enable RADVD	The RADVD (Router Advertisement Daemon) implements link-local advertisements of IPv6 router addresses and IPv6 routing prefixes using the Neighbor Discovery Protocol (NDP) and is used by system administrators for stateless auto configuration of network hosts on Internet Protocol version 6 networks. Select the checkbox to enable the RADVD.
Enable ULA Prefix Advertisement	If enabled, the modem router will advertise ULA prefix periodically.
Randomly Generate	If this option is selected, address prefix can be automatically generated.

Parameter	Description
Statically Configure	If this option is selected, you need to manually configure the address prefix and validity period.
Prefix	It specifies the prefix of the IPv6 address.
Preferred Life Time (hour)	It specifies the preferred life time in hour. When the time is out, the computer can continue to use the address in initiated communications, but cannot use it in new initiated communications.
Valid Life Time (hour)	It specifies the valid life time of the IP address in hour. When the time is out, the address is invalid.

■ Configuration procedure

Step 1 Choose **Advanced Setup > LAN > IPv6 Autoconfig** to enter the configuration page.

Step 2 Select **Enable DHCPv6 Server**.

Step 3 Select **Stateful**.

Step 4 **Start/End interface ID**: Enter a start/end interface ID.

Step 5 **Lease Time**: Enter the valid time of an IPv6 address .

Step 6 Select **Enable RADVD**.

Step 7 Click **Save/Apply**.

----End

4.3 VPN

4.3.1 Overview

A VPN is a virtual private network set up over a public network (usually the internet).

This modem router can function as two kinds of VPN clients: PPTP or L2TP client. The following section describes how to configure the router as a PPTP/L2TP client. If you set up a PPTP/L2TP server, you can enable PPTP/L2TP client function to help you visit the PPTP/L2TP server.

4.3.2 Configuring modem router as a L2TP client

Step 1 Choose **Advanced Setup > VPN > L2TP Client** to enter the configuration page, and click **Add**.



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 set on the L2TP server, and select an **Associated WAN Interface**, and click **Next**.



Tunnel Name:

L2TP Server(IP address or domain name):

Associated WAN Interface:

Parameter	Description
Tunnel Name	It specifies the name of the L2TP connection to be set up.
L2TP Server(IP address or domain name)	It specifies the IP address or domain name of the L2TP VPN server to be connected. Generally, it refers to the IP address or domain name of the WAN port of the peer VPN router that functions as the L2TP server.
Associated WAN Interface	It specifies the WAN port of the router for setting up a VPN connection.

Step 3 Set **PPP Username**, **PPP Password**, and **PPPoE Service Name** based on the information set on the L2TP server, and 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:

PPPoE Service Name:

Authentication Method:

MTU:

Parameter	Description
PPP Username	It specifies the user name and password assigned by peer L2TP server.
PPP Password	
PPPoE Service Name	Optional. If a special service name is specified on peer L2TP server, it can be entered here. If not, leave it blank.
Authentication Method	It specifies the authentication method of the L2TP VPN connection.
MTU	It specifies the maximum transmission unit size. The default setting is recommended.

Step 4 Select default gateway interfaces from the **Available Routed WAN Interfaces**, and click  to move it to the **Select Default Gateway Interfaces** box, and then 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 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

ppp0

Available Routed WAN Interfaces

eth3.1

Step 5 Select DNS server interfaces from the **Available WAN Interfaces**, and click  to move it to the **Select DNS Server Interfaces** box. If your ISP provides DNS address(es), select **Use the following Static DNS IP address**, and enter it/them.

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 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.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces Available WAN Interfaces

ppp0 eth3.1

-> <-

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

Parameter	Description
Select DNS Server Interface from available WAN Interfaces	You can select this option to automatically get DNS server information from the selected WAN interface.
Use the following Static DNS IP address	You can select this option to manually enter the primary/secondary DNS server IP addresses.
Primary DNS server	The primary/secondary DNS server IP addresses.
Second DNS server	

Step 6 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 Proxy:	Disabled
IGMP Multicast Source Enabled:	Disabled
MLD Multicast Proxy:	Disabled
MLD Multicast Source Enabled:	Disabled
Quality Of Service:	Disabled

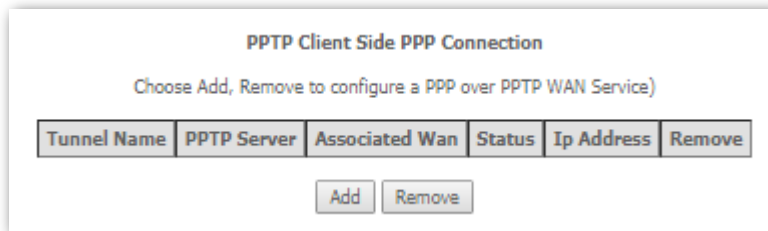
Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

Back Apply/Save

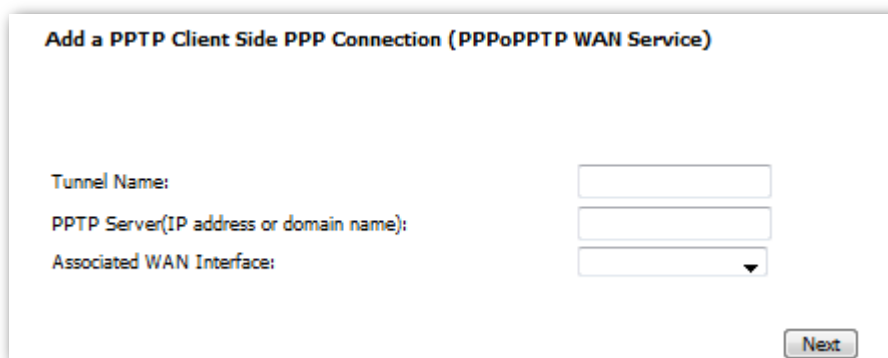
----End

4.3.3 Configuring modem router as a PPTP client

Step 1 Choose **Advanced Setup > VPN > PPTP Client** to enter the configuration page, and click **Add**.

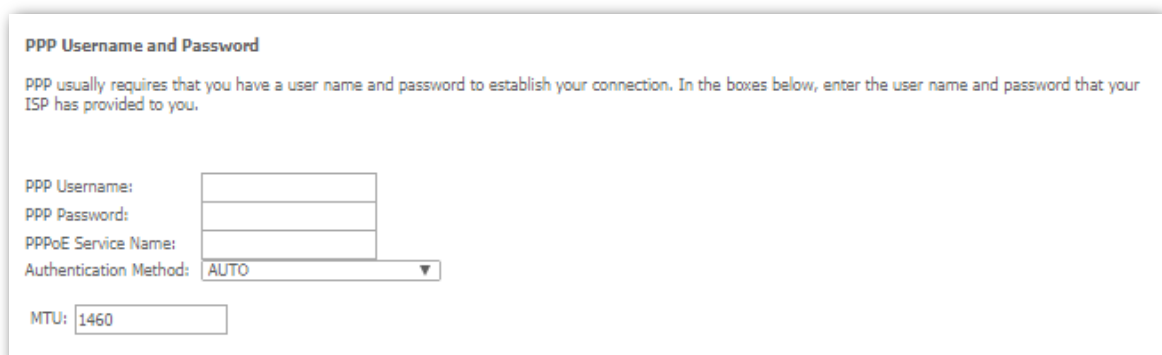


Step 2 Set **Tunnel Name** and **PPTP Server(IP address/domain name)** based on the information set on the PPTP server, select an **Associated WAN Interface**, and click **Next**.




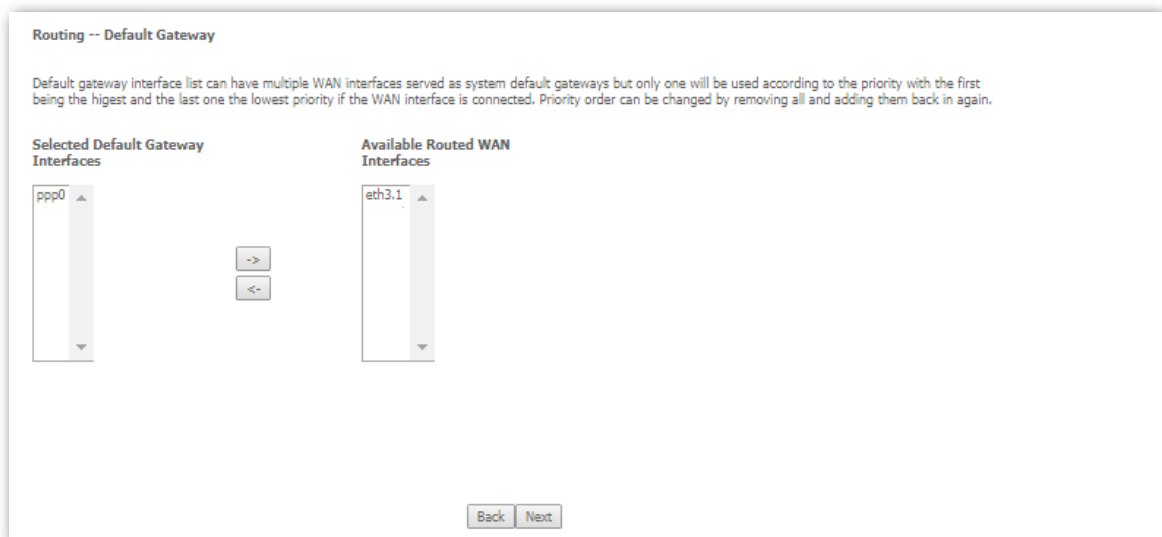
Parameter	Description
Tunnel Name	It specifies the name of the PPTP connection to be set up.
PPTP Server(IP address or domain name)	It specifies the IP address or domain name of the PPTP VPN server to be connected. Generally, it refers to the IP address or domain name of the WAN port of the peer VPN router that functions as the PPTP server.
Associated WAN Interface	It specifies the WAN port of the router for setting up a PPTP VPN connection.


Step 3 Set **PPP Username**, **PPP Password**, and **PPPoE Service Name** based on the information set on the PPTP server, and click **Next**.



Parameter	Description
PPP Username	It specifies the user name and password assigned by peer PPTP server.
PPP Password	
PPPoE Service Name	Optional. If a special service name is specified on peer PPTP server, it can be entered here. If not, leave it blank.
Authentication Method	It specifies the authentication method of the VPN connection.
MTU	It specifies the maximum transmission unit size. The default is not recommended.

Step 4 Select default gateway interfaces from the **Available Routed WAN Interfaces**, and click  to move it to the **Select Default Gateway Interfaces** box, and click **Next**.



Step 5 Select DNS server interfaces from the **Available WAN Interfaces**, and click  to move it to the **Select DNS Server Interfaces** box. If your ISP provides DNS address(es), select **Use the following Static DNS IP address**, and enter it/them.

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 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.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces Available WAN Interfaces

ppp0 eth3.1

-> <-

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

Parameter	Description
Select DNS Server Interface from available WAN Interfaces	You can select this option to automatically get DNS server information from the selected WAN interface.
Use the following Static DNS IP address	You can select this option to manually enter the primary/ secondary DNS server IP addresses provided by your ISP.
Primary DNS server	The primary/secondary DNS server IP addresses provided by your ISP.
Second DNS server	

Step 6 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 Proxy:	Disabled
IGMP Multicast Source Enabled:	Disabled
MLD Multicast Proxy:	Disabled
MLD Multicast Source Enabled:	Disabled
Quality Of Service:	Disabled

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

Back Apply/Save

----End

4.4 WAN 3G/4G

4.4.1 Overview

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

Choose **Advanced Setup** > **WAN 3G/4G** 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	<input type="text" value="Other"/>
ISP	<input type="text" value="Auto"/>
APN	<input type="text"/>
Dial number	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>
Pin Code	<input type="text"/>

Parameter	Description
Country	It specifies the country/region where the modem router is used.
ISP	It specifies the 3G/4G service provider.
APN	Access point Name. It will be auto populated after you select your country/region and ISP. If it is incorrect, you can change it manually.
Dial number	The number to set up a connection. It will be auto populated after you select your country/region and ISP. If it is incorrect, you can change it manually.
Username	Enter the user name and password for your 3G/4G internet service. It will be auto populated after you select your country/region and ISP. If it is incorrect, you can change it manually.
Password	
Pin Code	It specifies the pin number of the SIM card.

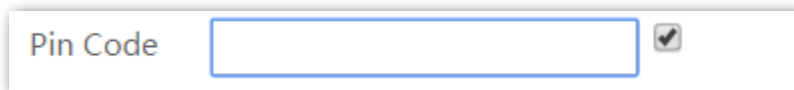
4.4.2 Configuration procedure

Step 1 Choose **Advanced Setup** > **WAN 3G/4G** to enter the configuration page.

Step 2 Select your country/region and ISP.

Step 3 APN/Dial number/Username/Password: Generally, if you select correct country/region 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 4 PIN Code: If the PIN code is provided, check the option box on the right of the input box of Pin Code, and enter the Pin code in the input box.

A screenshot of a web form element. It consists of a light gray rectangular container. On the left side of the container, the text "Pin Code" is displayed in a dark gray font. To the right of this text is a white rectangular input box with a thin blue border. Further to the right, within the same container, is a small, dark gray square checkbox with a white checkmark inside.

Step 5 Click **Apply/Save**.

----End

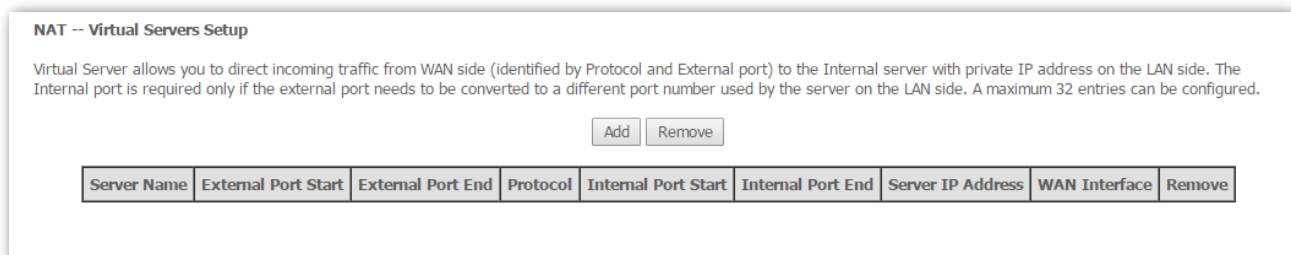
4.5 NAT

4.5.1 Virtual server

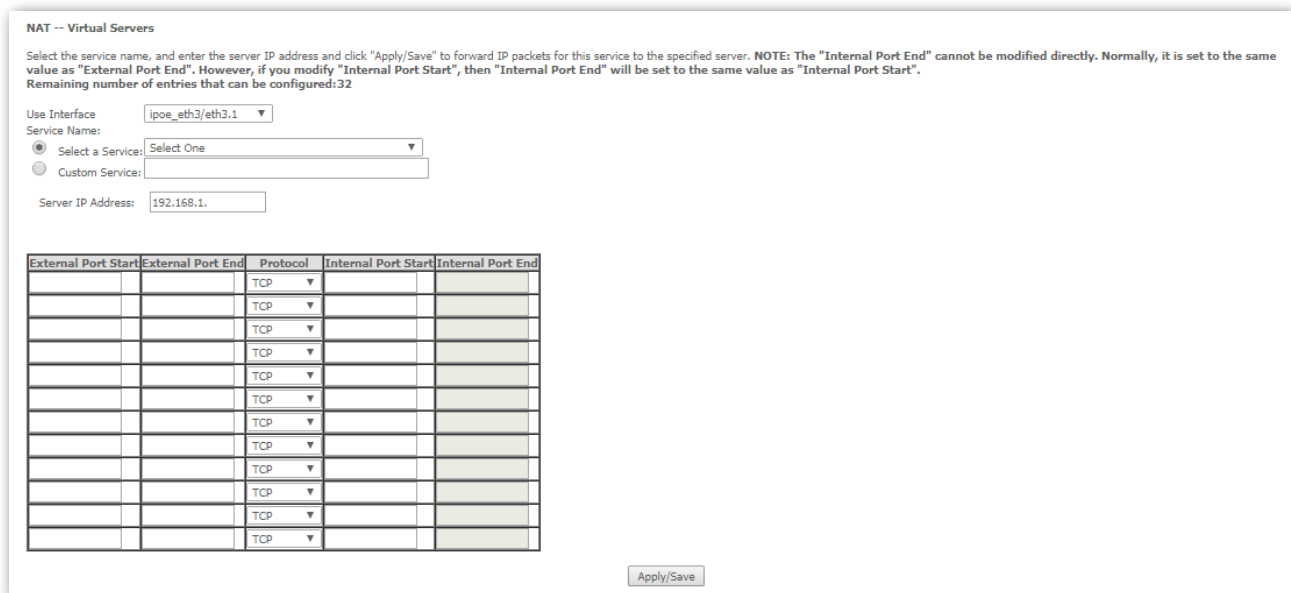
4.5.1.1 Overview

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



Click **Add** to configure the function.



Parameter description

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

Parameter	Description
Service Name	<ul style="list-style-type: none"> • 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 provides 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 service ports of a server on the LAN of the modem router.

4.5.1.2 Example of configuring virtual server

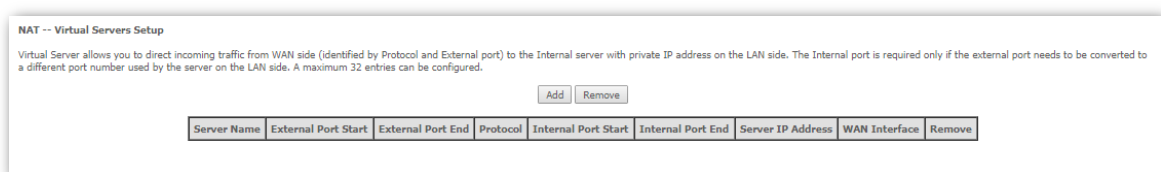
You have set up an FTP server on your LAN:

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

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

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

Step 1 Choose **Advanced Setup > NAT > Virtual Servers** to enter the configuration page, and click **Add**.



Step 2 Select a use interface from the drop-down box.

Step 3 Select **FTP Server** in the drop-down box for service.

Step 4 If you want to define the service yourself, enter a descriptive name in the **Custom Service**, such as **My FTP**, and then manually set the port number (21) used by this service in the **Internal Port Start**, **Internal Port End**, **External Port Start** and **External Port End**.

Step 5 Select a protocol from the **Protocol** drop-down list. If you are unsure about which protocol is required, select **TCP/UDP**.

Step 6 In the **Server IP Address** field, enter the IP address of your local computer that offers this service, which is **192.168.1.100** in this example.

Step 7 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_eth3/eth3.1

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
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		

Apply/Save

----End

Remote access:

Your friends from the internet can access your FTP server by entering <ftp://183.37.227.201:21> in the address bar of a web browser.



As the WAN ip address changes dynamically, to ensure the stability of this function, it is recommended to use this function together with DDNS function to allow internet users to access the service through domain names.

4.5.2 Port triggering

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

Choose **Advanced 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 32 entries can be configured. The total number of Trigger port or Open port cannot exceed 999.

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:

Application Name:

Select an application:
 Custom application:

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

Parameter description

Parameter	Description
Use Interface	Select a WAN connection to which the rules apply. When there is only one WAN connection available, the rules will be automatically applied to it.
Application Name	<ul style="list-style-type: none"> • 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.

Parameter	Description
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 are automatically opened by the built-in firewall when connections initiated by an application are established.
Open Protocol	The protocol to be used by the built-in firewall when connections are initiated.

4.5.3 DMZ host

4.5.3.1 Overview

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

Choose **Advanced 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 'Apply' to activate the DMZ host.

Clear the IP address field and click '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.



- 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.

4.5.3.2 Configuring the DMZ host function

Step 1 Choose **Advanced Setup > NAT > DMZ Host** to access the configuration page.

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

Step 3 Click **Save/Apply**.

----End

4.5.4 Multi-NAT

4.5.4.1 Overview

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

Choose **Advanced 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.

■ One-to-One

NAT -- Multi-NAT

Interface:

Type:

Local IP:

Public IP:

■ Many-to-One

NAT -- Multi-NAT

Interface:

Type:

Local Start IP:

Local End IP:

Public IP:

Parameter description

Parameter	Description
Interface	Select a WAN interface that the function uses.
Type	<ul style="list-style-type: none">• 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	It specifies a local IP address.
Public IP	It specifies a public IP address.

4.5.4.2 Configuring the Multi-NAT function

- Step 1** Choose **Advanced Setup > NAT > Multi-NAT** to enter the configuration page, and 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**. If you need to set multiple routes for a local network, select **Many-to-One**.
- Step 4** If you select **One-to-One**, specify a local IP address. If you select **Many-to-One**, specify the **Local Start IP** and **Local End IP**.
- Step 5** Set **Public IP** to a public IP address.
- Step 6** Click **Apply/Save**.

----End



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

4.6 Security

4.6.1 DoS defence

4.6.1.1 Overview

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

Choose **Advanced 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): Packets/s

Enable UDP-FLOOD Attack Filtering
UDP-FLOOD Packets Threshold (5 ~ 3600): Packets/s

Enable TCP-SYN-FLOOD Attack Filtering
TCP-SYN-FLOOD Packets Threshold (5 ~ 3600): Packets/s

Parameter description

Parameter	Description
Dos Protection	It specifies whether to enable Dos protection function.
Enable ICMP-FLOOD Attack Filtering	It specifies whether to enable ICMP-FLOOD attack filtering.
ICMP-FLOOD Packets Threshold (5 ~ 3600)	It specifies the maximum number of incoming ICMP packets allowed in one second. If the threshold is exceeded, it is inferred that the modem router is under ICMP Flood attack.
Enable UDP-FLOOD Attack Filtering	It specifies whether to enable UDP-FLOOD attack filtering.
UDP-FLOOD Packets Threshold (5 ~ 3600)	It specifies the maximum number of incoming UDP packets allowed in one second. If the threshold is exceeded, it is inferred that the modem router is under UDP Flood attack.

Parameter	Description
Enable TCP-SYN-FLOOD Attack Filtering	It specifies whether to enable TCP-SYN-FLOOD attack filtering.
TCP-SYN-FLOOD Packets Threshold (5 ~ 3600)	It specifies the maximum number of incoming TCP SYN packets allowed in one second. If the threshold is exceeded, it is inferred that the modem router is under SYN Flood attack.

4.6.1.2 Enabling the Dos Defense function

Step 1 Choose **Advanced Setup > Security > Dos Defense** to enter the configuration page.

Step 2 Select the **Enable** option of Dos Protection.

Step 3 Select the corresponding attack filtering.

Step 4 Click **Save**.

----End

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

4.6.2 IP filtering

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

4.6.2.1 Outgoing

Overview

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

Configuring the Outgoing IP Filtering function

Step 1 Choose **Advanced Setup > Security > IP Filtering > Outgoing** to enter the configuration page, and click **Add**.

Step 2 Filter Name: Enter a descriptive filtering name.

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

- Step 4 Protocol:** Select a protocol for the filter rule.
- Step 5 Source IP address[/prefix length]:** Enter the LAN IP address to be filtered.
- Step 6 Source Port (port or port:port):** Enter a port number or a port range used by LAN computers to access the internet. If you are not sure, leave it blank.
- Step 7 Destination IP address[/prefix length]:** Enter the external network IP address to be accessed by specified LAN computers.
- Step 8 Destination Port (port or port: port):** Enter a port number or a port range that the internet service you restrict uses.
- Step 9** Click **Apply/Save**.

----End

Parameter description

Parameter	Description
Filter Name	It specifies the name of a rule.
IP Version	It allows you to select an IP protocol, IPv4, or IPv6.
Protocol	It allows you to select a protocol for the filter rule.
Source IP address[/prefix length]	It specifies the LAN IP address to be filtered.
Source Port (port or port:port)	It specifies the source port used by packets. Source port is for TCP/UDP protocol. If protocol ICMP is selected, this field is not required. Since the source port of the data packet is changeable, you'd better set the port to 1:65535 or leave it blank.
Destination IP address[/prefix length]	It specifies the external network IP address to be accessed by specified LAN computers.
Destination Port (port or port:port)	It specifies the port number used by the internet service to be restricted. Destination port is for TCP/UDP protocol. If protocol ICMP is selected, this field is not required.

4.6.2.2 Incoming

Overview

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 filtering rules. The Incoming IP Filtering function allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition.

Configuring the Ingoing IP Filtering function

Step 1 Choose **Advanced Setup > Security > IP Filtering > Incoming** to enter the configuration page, and click **Add**.

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

Step 2 Filter Name: Enter a descriptive filtering name.

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

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

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

Step 6 Source Port (port or port:port): Enter a port number or a range of ports used by computers from external network to access your internal network.

Step 7 Destination IP address[/prefix length]: Enter the internal network IP address [eg: IP/Mask] to be accessed by the specified computers from external network.

Step 8 Destination Port (port or port:port): Enter the port used by the internet service to be restricted.

Step 9 Click **Apply/Save**.

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:

Protocol:

Source IP address[/prefix length]:

Source Port (port or port:port):

Destination IP address[/prefix length]:

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_eth3/eth3.1 pppoe_eth3/ppp0.2 br0/br0

----End

Parameter description

Parameter	Description
Filter Name	It specifies the name of a rule.
IP Version	It allows you to select an IP protocol, IPv4, or IPv6.
Protocol	It allows you to select a protocol for the filter rule.
Source IP address[/prefix length]	It specifies the IP address and its prefix length of the computer from the internet which is allowed to access the LAN service.
Source Port (port or port:port)	It specifies the source port used by packets. Source port is for TCP/UDP protocol. If protocol ICMP is selected, this field is not required. Since the source port of the data packet is changeable, you'd better set the port to 1:65535 or leave it blank.
Destination IP address[/prefix length]	It specifies the IP address and its prefix length of the LAN server which allows the internet users to access.
Destination Port (port or port:port)	It specifies the port number used by the LAN service which allows the internet users to access.

4.6.3 MAC filtering

4.6.3.1 Overview

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

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

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

4.6.3.2 Adding a frame forwarding rule

Step 1 Choose **Advanced Setup > Security > MAC Filtering** to enter the configuration page, and click Add.

MAC Filtering Setup

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

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
eth3.1	FORWARD	<input type="checkbox"/>

Choose Add or Remove to configure MAC filtering rules.

Interface	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
-----------	----------	-----------------	------------	-----------------	--------

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

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

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

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

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

Step 7 Click **Save/Apply**.

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.

Protocol Type:

Destination MAC Address:

Source MAC Address:

Frame Direction:

WAN Interfaces (Configured in Bridge mode only)

----End

Parameter description

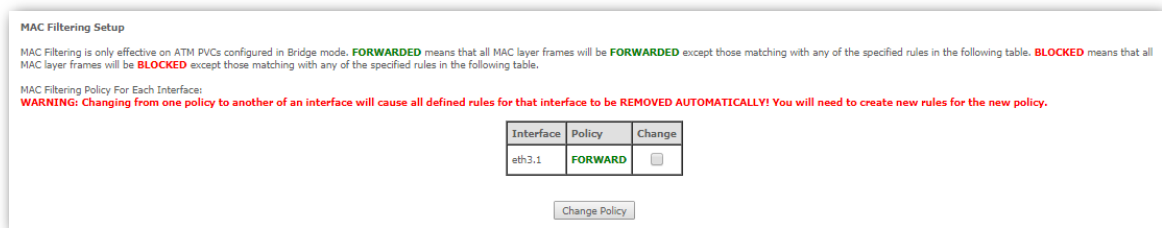
Parameter	Description
Protocol Type	It allows you to select the protocol type from the drop-down list.
Destination MAC Address	It specifies the destination MAC address to which the MAC filter rule applies.
Source MAC Address	It specifies the source MAC address to which the MAC filter rule applies.
Frame Direction	It specifies the direction the frame that you want to restrict.

4.6.3.3 Changing the policy from FORWARDED to BLOCKED

Step 1 Choose **Advanced Setup > Security > MAC Filtering** to enter the configuration page.

Step 2 Select **Change** checkbox.

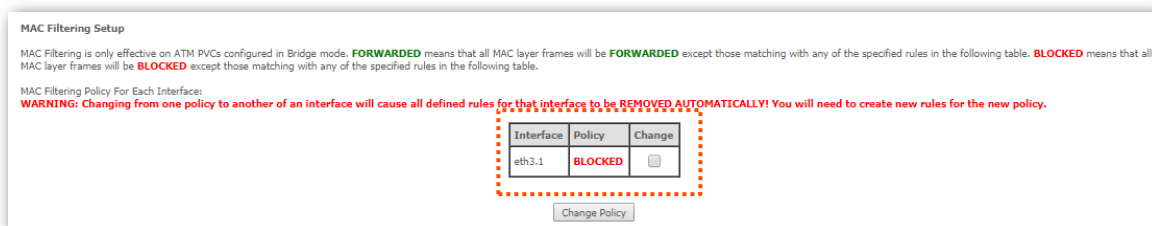
Step 3 Click **Change Policy**.



----End

Verification

The policy is change to **BLOCKED**.



4.6.3.4 Adding a frame blocking rule

Step 1 Choose **Advanced Setup > Security > MAC Filtering** to enter the configuration page.

Step 2 Change the policy to **BLOCKED**. Refer to [To change the policy from FORWARDED to BLOCKED](#).

Step 3 Click **Add**.

Step 4 Protocol Type: Select a protocol type from the drop-down list.

Step 5 Destination MAC Address: Enter the destination MAC address apply the MAC filtering rule

to which you want to apply the MAC filtering rule.

Step 6 Source MAC Address: Enter the source MAC address to which you want to apply the MAC filtering rule.

Step 7 Frame Direction: Select a frame direction from the drop-down list.

Step 8 WAN Interfaces: Select a WAN interface from the drop-down list.

Step 9 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:

WAN Interfaces (Configured in Bridge mode only)

----End

4.7 Parental control

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

4.7.1 Time restriction

4.7.1.1 Overview

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

4.7.1.2 Adding a time restriction rule

Step 1 Choose **Advanced Setup > Parental Control > Time Restriction** to enter the configuration page, and click **Add**.

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

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

Step 3 Select **Browser's MAC Address** if the rule is applied to the computer where the current browser is running (the browser used to log in to the web UI of the modem router). If not, select **Other MAC Address**, and enter the MAC address of a computer to which the rule is applied.

Step 4 **Days of the week:** Select the days of week during which the rule takes effect.

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

Step 6 Click **Apply/Save**.

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

Days of the week	Mon	Tue	Wed	Thu	Fri	Sat	Sun
Click to select	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Start Blocking Time (hh:mm)

End Blocking Time (hh:mm)

----End

Parameter description

Parameter	Description
User Name	It specifies the description of the rule.
Browser's MAC Address/Other MAC Address	It specifies the MAC address of the computer where the current browser is running (the browser used to log in to the web UI of the modem router). If the rule needs to apply to this device, select this option. Otherwise, select Other MAC Address, and enter the MAC address of the device to which the rule is applied.
Days of the week	It specifies the dates on which the rule takes effect.
Start Blocking Time (hh:mm)	It specifies the start time of period in which the rule takes effect.
End Blocking Time (hh:mm)	It specifies the end time of period in which the rule takes effect.

4.7.2 URL filter

4.7.2.1 Overview

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

4.7.2.2 Adding a URL Filter rule

Step 1 Choose **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 32 entries can be configured.

URL List Type: Exclude Include

Address	Port	Remove

Step 2 Select **URL List Type**.

Exclude indicates that the URLs added to the list cannot be accessed.

Include indicates that only the URLs added to the list can be accessed.

Step 3 Click **Add**.

Step 4 Enter a URL. For example, Set **URL Address** to www.google.com.

Step 5 Specify a port number based on the URL you entered.

Step 6 Click **Apply/Save**.

Parental Control -- URL Filter Add

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

URL Address:

Port Number: (Default 80 will be applied if leave blank.)

----End

4.7.3 Example of configuring parental control

4.7.3.1 Networking requirement

Assume that a wireless network whose SSID is **Home** has been set up at your home. You want to disallow your children, Lily and Tom, to visit YouTube from 18:00 to 20:00 on weekdays. The MAC addresses of their computers are C8:3A:35:00:00:11 and C8:3A:35:00:00:12.

4.7.3.2 Solution

Set up time restriction and URL filter rules.

4.7.3.3 Configuration procedure

Step 1 Add time restriction rules.

1. Choose **Advanced Setup > Parental Control > Time Restriction** to enter the configuration page, and click **Add**.

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

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

2. Set the **User Name** to **Lily**.
3. Select **Other MAC Address**, and enter **C8:3A:35:00:00:11**.
4. Select **Mon to Fri**.
5. Set the **Start Blocking Time** and **End Blocking Time** to **18:00** and **20:00** respectively.
6. Click **Apply/Save**.

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

Other MAC Address
(xxxxxxxx:xxxx:xxxx)

Days of the week	Mon	Tue	Wed	Thu	Fri	Sat	Sun
Click to select	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Start Blocking Time (hh:mm)

End Blocking Time (hh:mm)

7. Perform step 2 to 6 to add the other rule **Tom**.

The added rules are shown in the following table.

Username	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Remove
Lily	C8:3A:35:00:00:11	x	x	x	x	x			18:0	20:0	<input type="checkbox"/>
Tom	C8:3A:35:00:00:12	x	x	x	x	x			18:0	20:0	<input type="checkbox"/>

Step 2 Set a URL filter rule.

1. Choose **Advanced Setup > Parental Control > URL Filter** to enter the configuration page.
2. Select **URL List Type** to **Exclude**, and click **Add**.

URL Filter -- Please select the list type first then configure the list entries. Maximum 32 entries can be configured.

URL List Type: Exclude Include

Address	Port	Remove
		<input type="button" value="Add"/> <input type="button" value="Remove"/>

3. Enter **www.youtube.com** in the **URL Address** box.
4. Enter **80** in the **Port Number** box.
5. Click **Apply/Save**.

Parental Control -- URL Filter Add

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

URL Address:

Port Number: (Default 80 will be applied if leave blank.)

The added rule is shown in the following table.

Address	Port	Remove
www.youtube.com	80	<input type="checkbox"/>

----End

4.7.3.4 Verification

During 18:00 to 20:00 on weekdays, the computers with MAC address C8:3A:35:00:00:11 and C8:3A:35:00:00:12 are not allowed to visit YouTube.

4.8 ALG

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

ALG Settings

Select Enable the following configuration.

- SIP Enabled
- FTP Enabled
- TFTP Enabled
- H323 Enabled
- RTSP Enabled

Select Enable the VPN pass-through below.

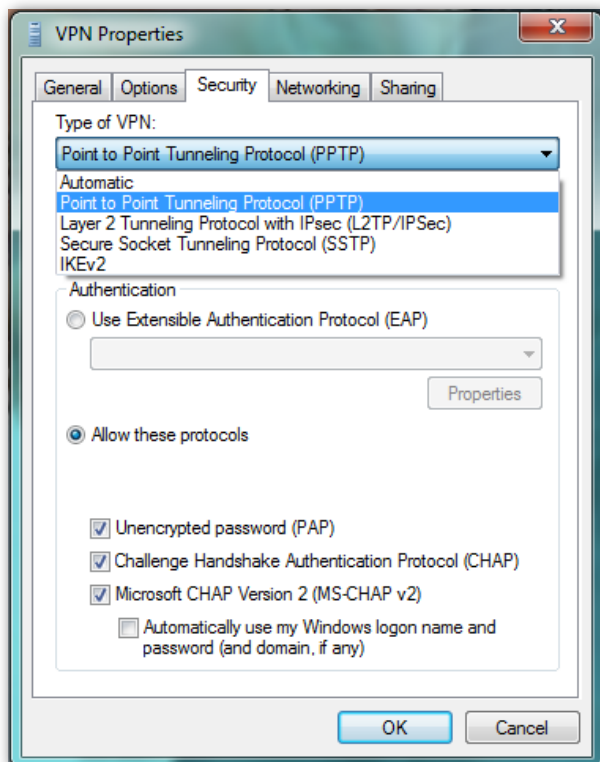
- PPTP Enabled
- L2TP Enabled
- IPSEC Enabled

Parameter description

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

VPN pass-through

- **PPTP Enabled:** If you select PPTP protocol when you create a VPN connection on your computer, it takes effect only when this checkbox is selected.
- **L2TP/IPSEC Enabled:** If you select L2TP or IPSEC protocol when you create a VPN connection on your computer, it takes effect only when this checkbox is selected.



4.9 Bandwidth control

4.9.1 Overview

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.

4.9.2 Adding a bandwidth control rule

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

Step 2 Select **Enable Bandwidth Control**.

Step 3 Specify a name for the rule.

Step 4 Specify an IP address, or an IP address range.

Step 5 Specify a maximum upstream and downstream speed.

Step 6 Select the status for the rule.

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

Step 7 Click **Commit** to add the rule to the list.

Step 8 Click **Apply/Save** to apply the settings.

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

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 ▾

----End

4.10 Quality of service

QoS helps to prioritize data. By attaching special identification marks or headers to incoming packets, QoS determines queue of packets based on priority. It is useful when there are certain types of data you want to give higher priority, such as voice data packets give higher priority than Web data packets. This function provides better service of selected network traffic over various technologies.

Choose **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

Select Default DSCP Mark

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

- **Enable QoS:** Select it to enable the QoS feature of the modem feature.
- **Select Default DSCP Mark:** Select a DSCP mark for the packets not matching the created QoS classification rules.
- **No Change (-1):** Do not add DSCP mark, and keep the original packets.
- **Auto Marking (-2):** Randomly select a mark from the following mark list to tag the packets.
- **Default (000000):** Default PHB (Per-Hop Behaviors). It specifies the best-effort internet service.
- **EF (101110):** EF (Expedited Forwarding PHB). It specifies the highest priority of the internet service.

- **Class-Selector PHB:** It specifies that the DSCP mark is **XXX000** where **X** can be **0** or **1**. The class of service of Class-Selector PHB is the same as that of IP Precedence used in the current internet. When the **XXX** are all **0**, it is the default PHB.
- **Assured Forwarding PHB:** RFC2597. It is applicable to video service, VPN service, and so on. AF PHB has four service classes which require the corresponding bandwidths and caches. Each service class has three packet-loss priorities.

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



- 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.

4.10.1 QoS queue

The QoS queue part includes QoS configuration and WLAN queue.

4.10.1.1 QoS configuration

Overview

■ ATM interface

QoS Queue Configuration

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

Name:

Enable:

Interface:

Queue Precedence: (lower value, higher priority)

- The precedence list shows the scheduler algorithm configured at each precedence level.
 - Note that precedence level with SP scheduler may have only one queue.
 - precedence level with WRR/WFQ scheduler may have multiple queues.

Queue Weight: [1-63]

Drop Algorithm
 DT (Drop Tail)

DSL Latency:

Parameter description

Parameter	Description
Name	It specifies the description of the QoS queue rule.
Enable	It specifies whether to enable the QoS queue rule.
Interface	It specifies the interface to which the QoS queue rule applies.
Queue Precedence	It specifies the precedence value of the queue. <ul style="list-style-type: none">• Queues with the same precedence: It is scheduled using WRR and WFQ, and the device assigns the bandwidth based on the queue weight.• Queues with different precedence: It is scheduled according to the precedence value.
Queue Weight	It specifies the weight of the queue. You can specify the queue weight for the queues with the same precedence.
Drop Algorithm	It specifies the default queue drop algorithm. It cannot be changed.
DSL Latency	It specifies the DSL latency mode of the ATM interface.

■ Ethernet interface

QoS Queue Configuration

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

Name:

Enable: ▾

Interface: ▾

Queue Precedence: ▾ (lower value, higher priority)

- The precedence list shows the scheduler algorithm configured at each precedence level.
- Note that precedence level with SP scheduler may have only one queue.
- precedence level with WRR/WFQ scheduler may have multiple queues.

Drop Algorithm

DT (Drop Tail)

Parameter description

Parameter	Description
Name	It specifies the description of the QoS queue rule.
Enable	It specifies whether to enable the QoS queue rule.

Parameter	Description
Interface	It specifies the interface to which the QoS queue rule applies.
Queue Precedence	<p>It specifies the precedence value of the queue.</p> <ul style="list-style-type: none"> • Queues with the same precedence: It is scheduled using WRR and WFQ, and the device assigns the bandwidth based on the queue weight. • Queues with different precedence: It is scheduled according to the precedence value.
Drop Algorithm	It specifies the default queue drop algorithm. It cannot be changed.

■ PTM interface

QoS Queue Configuration

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

Name:

Enable:

Interface:

Queue Precedence: (lower value, higher priority)

- The precedence list shows the scheduler algorithm configured at each precedence level.
- Note that precedence level with SP scheduler may have only one queue.
- precedence level with WRR/WFQ scheduler may have multiple queues.

Scheduler Algorithm

Weighted Round Robin

Weighted Fair Queuing

Queue Weight: [1-63]

Drop Algorithm

DT (Drop Tail)

PTM Priority:

DSL Latency:

Parameter description

Parameter	Description
Name	It specifies the description of the QoS queue rule.
Enable	It specifies whether to enable the QoS queue rule.

Parameter	Description
Interface	It specifies the interface to which the QoS queue rule applies.
Queue Precedence	<p>It specifies the precedence value of the queue.</p> <ul style="list-style-type: none"> • Queues with the same precedence: It is scheduled using WRR and WFQ, and the device assigns the bandwidth based on the queue weight. • Queues with different precedence: It is scheduled according to the precedence value.
Scheduler Algorithm	<ul style="list-style-type: none"> • Weighted Round Robin: It specifies a QoS packet scheduling algorithm. It assigns different weights for different kinds of packets and provides the packets with different bandwidths based on the weights. • Weighted Fair Queuing: It specifies a QoS packet scheduling algorithm. It divides groups into different queues based on the service streaming, IP precedence, and Hash algorithm, and fairly assigns the bandwidth to the services with low precedence according to the weights while ensuring the performance of services with high precedence.
Queue Weight	It specifies the weight of the queue. You can specify the queue weight for the queues with the same precedence.
Drop Algorithm	It specifies the default queue drop algorithm. It cannot be changed.
DSL Latency	It specifies the DSL latency mode of the ATM interface.

Creating a QoS Queue

Step 1 Choose **Advanced Setup > Quality of Service > QoS Queue > QoS Configuration** to enter the configuration page, and click **Add**.

QoS Queue Setup

In ATM mode, maximum16queues can be configured.
In PTM mode, maximum8queues can be configured.
For each Ethernet interface, maximum4queues can be configured.
For each Ethernet WAN interface, maximum4queues 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.

Name	Key	Interface	Qid	Prec/Alg/Wght	DslLatency	PtmPrio	DropAlg/ LoMin/LoMax/HiMin/HiMax	ShapingRate (bps)	MinBitRate(bps)	BurstSize(bytes)	Enable	Remove
<div style="display: flex; justify-content: space-between; padding: 5px;"> Add Enable Remove </div>												

Step 2 Name: Enter a name for the queue.

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

Step 4 Interface: Select an interface for the queue.

Step 5 Click **Apply/Save**.

QoS Queue Configuration

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

Name:

Enable: ▾

Interface: ▾

Drop Algorithm

DT (Drop Tail)

----End

4.10.1.2 Wlan queue

It displays the QoS rules of wireless networks.

QoS Wlan Queue Setup

Note: If WMM function is disabled in Wireless Page, queues related to wireless will not take effects.

Name	Key	Interface	Qid	Prec/Alg/Wght	Enable
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
WMM Video Priority	4	wl0	5	4/SP	Enabled
WMM Best Effort	5	wl0	4	5/SP	Enabled
WMM Background	6	wl0	3	6/SP	Enabled
WMM Background	7	wl0	2	7/SP	Enabled
WMM Best Effort	8	wl0	1	8/SP	Enabled
WMM Voice Priority	33	wl1	8	1/SP	Enabled
WMM Voice Priority	34	wl1	7	2/SP	Enabled
WMM Video Priority	35	wl1	6	3/SP	Enabled
WMM Video Priority	36	wl1	5	4/SP	Enabled
WMM Best Effort	37	wl1	4	5/SP	Enabled
WMM Background	38	wl1	3	6/SP	Enabled
WMM Background	39	wl1	2	7/SP	Enabled

Parameter description

Parameter	Description
Name	It specifies the description of the QoS queue rule.

Key	It specifies the key number of the QoS queue rule.
Interface	It specifies the wireless interface the QoS queue rule applies.
Qid	It specifies the value the QoS queue rule.
Prec/Alg/Wght	It specifies the priority level of the QoS queue rule. A lower value indicates a higher priority.
Enable	It specifies the status of the QoS queue rule.

4.10.2 QoS classification

To add a QoS classification rule:

Step 1 Choose **Advanced Setup > Quality of Service > QoS Classification** to enter the configuration page, and click **Add**.

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 rules in the table. Rules with enable-checkbox checked will be enabled. Rules with enable-checkbox un-checked will be disabled.
 The enable-checkbox also shows status of the rule after page reload.
 If you disable WMM function in Wireless Page, classification related to wireless will 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
<input type="button" value="Add"/> <input type="button" value="Enable"/> <input type="button" value="Remove"/>																		

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

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

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

Step 5 Set the required parameters of specify classification criteria.

1. **Ingress Interface:** Select an interface from which the data traffic comes.
2. **Ether Type:** Select an Ether type of the Ethernet packets.
3. **Source/Destination MAC Address:** Enter the source/destination MAC addresses.
4. **Source/Destination MAC Mask:** Leave them blank.

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

- **Source/Destination IP Address[/Mask]:** If you do not specify the source/destination MAC address, you need to specify the source/destination IP Address for the classification.
- **Differentiated Service Code Point (DSCP) Check:** Select a DSCP mark for the data streaming.
- **Protocol:** Select a protocol.
- **UDP/TCP Source/Destination Port:** Enter the port information for the data streaming.

Step 6 Set the required parameters of specify the classification results.

1. **Specify Egress Interface (Required):** Select an interface.
2. **Specify Egress Queue (Required):** Select a queue to which packets are distributed (The queue should be set in **Advanced Setup >Quality of Service > QoS Queue > QoS Configuration** in advance.)
3. **Mark Differentiated Service Code Point (DSCP):** Select a mark for the queue when the queue exits.
4. **Mark 802.1p priority:** Select an 802.1p priority mark for the data stream.
5. **Set Rate Limit:** Set the maximum transmission speed of the queue.

Step 7 Click **Apply/Save**.

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.)

Ingress 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 Egress Interface (Required):

Specify Egress 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:

- Class non-vlan packets egress to a non-vlan interface will be tagged with VID 0 and the class rule p-bits.
 - Class vlan packets egress to a non-vlan interface will have the packet p-bits re-marked by the class rule p-bits. No additional vlan tag is added.
 - Class non-vlan packets egress to a vlan interface will be tagged with the interface VID and the class rule p-bits.
 - Class vlan packets egress to a vlan interface will be additionally tagged with the packet VID, and the class rule p-bits.

Set Rate Limit: [Kbits/s]

----End

4.10.3 Example of configuring QoS

Network requirement

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

Assume that:

- The company accesses the internet through phone cable.
- UDP ports for video conference: 1718, 1719, and 1720.

- UDP port for IP phone: 65060.
- Online video uses PPlive. UDP port for PPlive: 7100 and 7101.

Solution

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

Configuration procedure

Step 1 Enable QoS function.

1. Choose **Advanced Setup > Quality of Service** to enter the configuration page.
2. Select **Enable QoS**.
3. Click **Apply/Save**.

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. 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

Select Default DSCP Mark

Step 2 Configure QoS Queues.

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

QoS Queue Setup

In ATM mode, maximum16queues can be configured.
 In PTM mode, maximum8queues can be configured.
 For each Ethernet interface, maximum4queues can be configured.
 For each Ethernet WAN interface, maximum4queues 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.

Name	Key	Interface	Qid	Prec/Alg/Wght	DslLatency	PtmPrio	DropAlg/ LoMin/LoMax/HiMin/HiMax	ShapingRate (bps)	MinBitRate(bps)	BurstSize(bytes)	Enable	Remove
Default Queue	65	atm0	1	8/WRR/1	Path0		DT				<input checked="" type="checkbox"/>	

- (2) **Name:** Enter a name for the queue.
- (3) **Enable:** Select **Enable**.
- (4) **Interface:** Select **atm0**.
- (5) **Queue Precedence:** Select **1 (WRR)**.
- (6) Click **Apply/Save**.

QoS Queue Configuration

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

Name:

Enable:

Interface:

Queue Precedence: (lower value, higher priority)
 - The precedence list shows the scheduler algorithm configured at each precedence level.
 - Note that precedence level with SP scheduler may have only one queue.
 - precedence level with WRR/WFQ scheduler may have multiple queues.

Queue Weight: [1-63]

Drop Algorithm
 DT (Drop Tail)

DSL Latency:

3. Perform the procedure in [Step 2](#) to add IP phone, online video, web, FTP and Email queues.

QoS Queue Setup

In ATM mode, maximum16queues can be configured.
 In PTM mode, maximum8queues can be configured.
 For each Ethernet interface, maximum4queues can be configured.
 For each Ethernet WAN interface, maximum4queues 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.

Name	Key	Interface	Qid	Prec/Alg/Wght	DslLatency	PtmPrio	DropAlg/ LoMin/LoMax/HiMin/HiMax	ShapingRate (bps)	MinBitRate(bps)	BurstSize(bytes)	Enable	Remove
Default Queue	65	atm0	1	8/WRR/1	Path0		DT				<input checked="" type="checkbox"/>	<input type="checkbox"/>
VideoConference	68	atm0	2	1/WFQ/1	Path0		DT				<input checked="" type="checkbox"/>	<input type="checkbox"/>
IP_Phone	69	atm0	3	2/WFQ/20	Path0		DT				<input checked="" type="checkbox"/>	<input type="checkbox"/>
online_video	70	atm0	4	2/WFQ/10	Path0		DT				<input checked="" type="checkbox"/>	<input type="checkbox"/>
Web	71	atm0	5	3/WFQ/20	Path0		DT				<input checked="" type="checkbox"/>	<input type="checkbox"/>
FTP_Email	72	atm0	6	3/WFQ/10	Path0		DT				<input checked="" type="checkbox"/>	<input type="checkbox"/>

Step 3 Configure QoS classification.

1. Choose **Advanced Setup > Quality of Service > QoS Classification** to enter the configuration page, and click **Add**.
2. **Traffic Class Name:** Enter a name for the classification, which is **VideoConference** in this example.
3. **Rule Order/Rule Status:** Keep the default values.
4. **Ingress Interface:** Select **Local**.
5. **Ether Type:** Select **IP (0x800)**.
6. **Protocol/UDP/TCP Destination Port:** Select **UDP**, and set the **UDP/TCP Destination Port** to **1718:1720**.
7. **Specify Egress Interface (Required):** Select the egress interface for the queue from the drop-down list.
8. **Specify Egress Queue (Required):** Select the egress queue from the drop-down list.
9. Click **Apply/Save**.

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:

Rule Status:

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

Ingress Interface:

Ether Type:

Differentiated Service Code Point (DSCP) Check:

Protocol:

UDP/TCP Source Port (port or port:port):

UDP/TCP Destination Port (port or port:port):

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

Specify Egress Interface (Required):

Specify Egress 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):

Set Rate Limit: [Kbits/s]

Step 4 Perform the procedure in [Step 3](#) to add classifications for IP phone, online video, web, FTP and Email services.

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 rules in the table. Rules with enable-checkbox checked will be enabled. Rules with enable-checkbox un-checked will be disabled.
 The enable-checkbox also shows status of the rule after page reload.
 If you disable WMM function in Wireless Page, classification related to wireless will not take effects

Class Name	Order	CLASSIFICATION CRITERIA										CLASSIFICATION RESULTS				Enable	Remove	
		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)
VideoConference	1	Local	IP					UDP		1718:1720			66				<input checked="" type="checkbox"/>	<input type="checkbox"/>
IP_Phone	2	Local	IP					UDP		65060			67				<input checked="" type="checkbox"/>	<input type="checkbox"/>
online_Video	3	Local	IP					UDP		7100:7101			68				<input checked="" type="checkbox"/>	<input type="checkbox"/>
Web	4	Local	IP					TCP		80			69				<input checked="" type="checkbox"/>	<input type="checkbox"/>
FTP_Email	5	Local	IP					TCP		20:21			70				<input checked="" type="checkbox"/>	<input type="checkbox"/>

----End

Verification

The network services of the company can be identified by the modem router. Video conference is higher than IP phone and online video. FTP/Web/Email service has the lowest priority. It ensures the efficient operation of the network when the network overload or congestion.

4.11 Routing

The Routing part includes default gateway and static route.

4.11.1 Default gateway

Default gateway interface list can contain multiple WAN interfaces serving as system default gateways.

Choose **Advanced Setup > Routing > Default 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

eth3.1 ▲

▼

➔

⬅

Available Routed WAN Interfaces

▲


▼


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

Selected WAN Interface: NO CONFIGURED INTERFACE ▼

Apply/Save

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

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

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

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

4.11.2 Static route

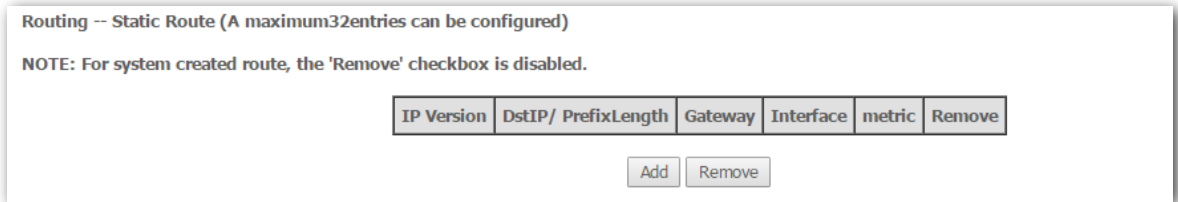
4.11.2.1 Overview

Static Route is used to select the best route for delivering data from a source address to a destination address. A static route is a manually configured route, which is simple, efficient, and

reliable. Appropriate static routes help reduce the number of route selection problems and reduce route selection load, increasing the packet forwarding speed.

4.11.2.2 Adding a static route

Step 1 Choose **Advanced Setup > Routing > Static Route** to enter the configuration page, and click **Add**.



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

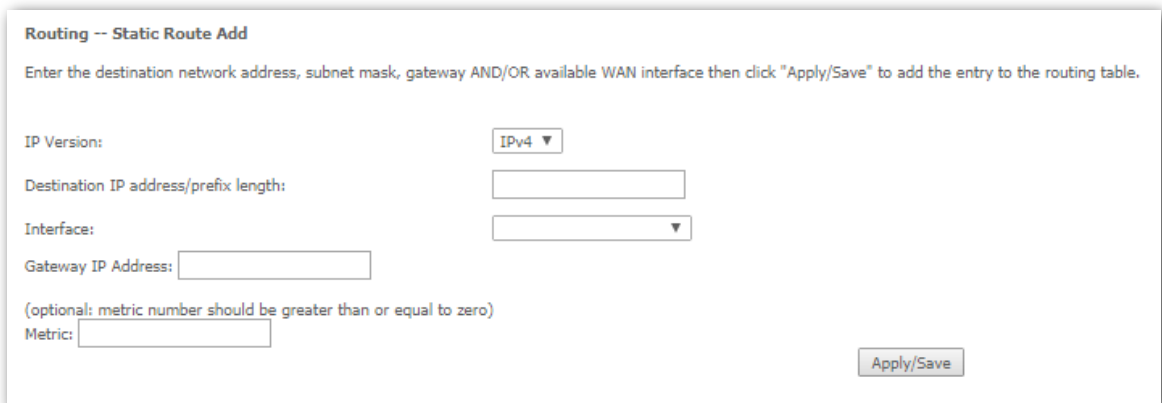
Step 3 **Destination IP address/prefix length:** Set an IP address of a specified host or a specified network.

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

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

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

Step 6 **(Optional: metric number should be greater than or equal to zero) Metric:** Set a metric value for the static route. A smaller number indicates a higher priority.



----End



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

4.11.3 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 Setup > Routing > RIP** to enter the configuration page.

Routing -- RIP Configuration

NOTE: If selected interface has NAT enabled, only Passive mode is allowed.

To activate RIP for the WAN Interface, select the desired RIP version and operation and place a check in the 'Enabled' checkbox. To stop RIP on the WAN Interface, uncheck the 'Enabled' checkbox. Click the 'Apply/Save' button to star/stop RIP and save the configuration.

Interface	Version	Operation	Enabled
eth3.1	2 ▼	Passive ▼	<input type="checkbox"/>
eth6	2 ▼	Passive ▼	<input type="checkbox"/>

Apply/Save

Parameter description

Parameter	Description
Interface	It specifies the WAN interfaces you add in a WAN service with NAT disabled.
Version	It specifies two RIP versions the modem router supports: RIPv1 and RIPv2. RIP 1: The periodic routing updates do not carry subnet information. RIP 2: The periodic routing updates 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.



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

4.12 DNS

The DNS part includes DNS server and Dynamic DNS.

4.12.1 DNS server

4.12.1.1 Overview

The DNS server translates domain names to IP addresses. It is used to look up site addresses based on their names. It allows you to set the DNS server information manually.

4.12.1.2 Configuring IPv4 DNS server manually

- Step 1** Choose **Advanced Setup > DNS > DNS Server** to enter the configuration page.
- Step 2** Select the **Use the following Static DNS IP address** checkbox and enter static DNS server IP addresses for the system.
- Step 3** 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 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.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces Available WAN Interfaces

eth3.1

-> <-

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

----End

4.12.1.3 Configuring IPv6 DNS server manually

- Step 1** Choose **Advanced Setup > DNS > DNS Server** to enter the configuration page.
- Step 2** Select **Use the following Static IPv6 DNS address** and enter the static IPv6 DNS server Addresses.
- Step 3** Click **Apply/Save**.

TODO: 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:

Use the following Static IPv6 DNS address:

Primary IPv6 DNS server:

Secondary IPv6 DNS server:

----End



- In ATM mode, static DNS server IP addresses must be entered if only single PVC with IPoA or static IPoE protocol is configured.
 - If a wrong DNS server address is configured, webpages may not be accessible.
-

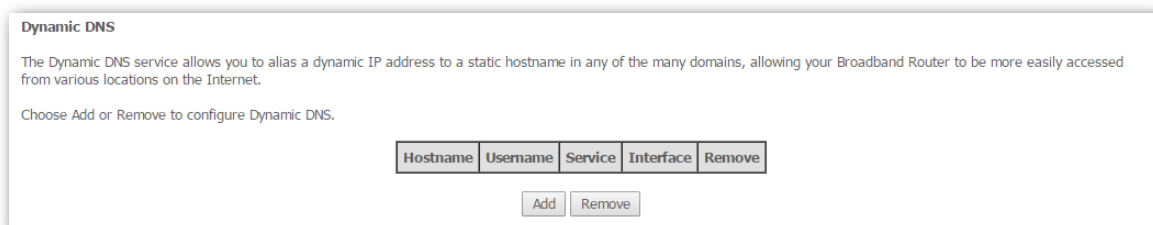
4.12.2 Dynamic DNS

4.12.2.1 Overview

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

4.12.2.2 Configuring the DDNS function

Step 1 Choose **Advanced Setup > DNS > Dynamic DNS** to enter the configuration page, and click **Add**.



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	Remove
----------	----------	---------	-----------	--------

Add Remove

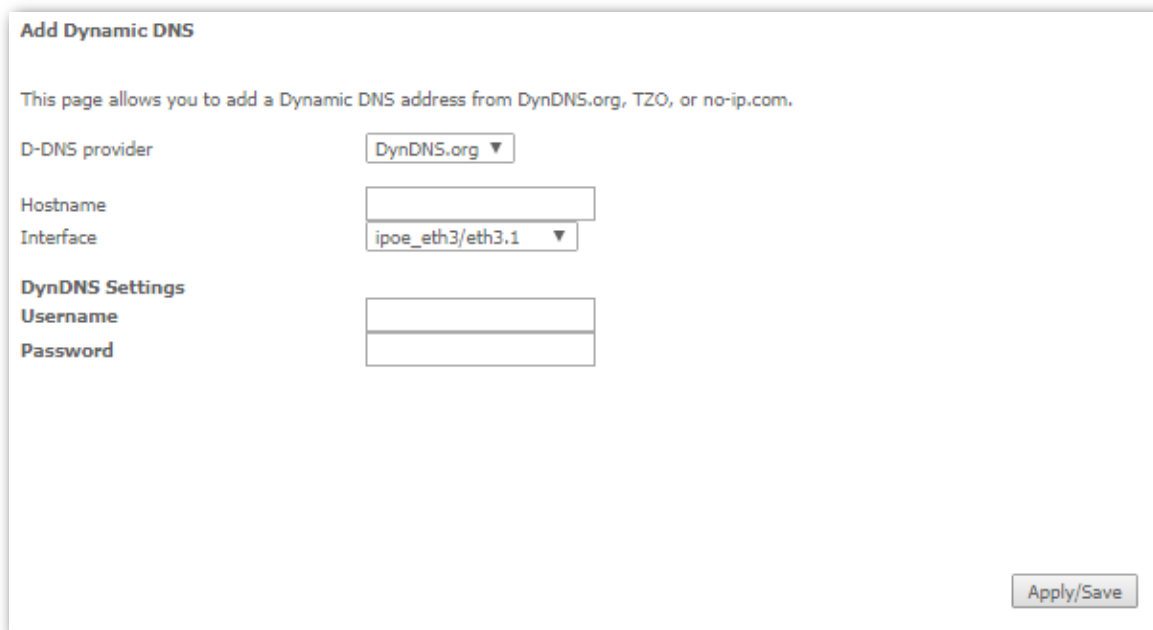
Step 2 **D-DNS provider:** Select a DDNS service provider. The supported service providers include dyn.com, TZO, and NO-IP.

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

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

Step 5 **Username/Password:** Set 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**.



Add Dynamic DNS

This page allows you to add a Dynamic DNS address from DynDNS.org, TZO, or no-ip.com.

D-DNS provider: DynDNS.org ▼

Hostname:

Interface: ipoe_eth3/eth3.1 ▼

DynDNS Settings

Username:

Password:

Apply/Save

----End

Parameter description

Parameter	Description
D-DNS provider	It specifies a DDNS provider that can map changeable IP addresses to one static domain name. The modem router supports the DynDNS.org, TZO and no-ip.com DDNS providers.
Hostname	It specifies the domain name of the DNS server registered on a DDNS service provider's website.
Interface	It specifies the interface of the WAN service.
Username	It specifies the login user name of a DDNS provider. You can sign up on a DDNS provider's website to obtain a login user name.
Password	It specifies the login password for a user name assigned by a DDNS provider. You are asked to set a login password when you sign up with the provider.

4.12.2.3 Example of configuring the DDNS function

Networking requirement

An enterprise uses V1200 to deploy its WLAN network. The modem router is connected to the internet. Now the enterprise establishes a web server and wants to be accessed by internet users. Thus when employees are not in the enterprise, they can also access the web server.

Solution

You can use virtual servers function to meet this requirement. In addition, to enable internet users to access the web server using a static domain name instead of a changeable IP address, enable the DDNS function.

Assume that:

- External port is 80.
- IP address of the web server is 192.168.1.100.
- Your DDNS provider: no-ip
- Registered domain name: tenda.ddns.net
- Registered user name/Password: tenda/tenda

Configuration procedure

Step 1 Configure the virtual servers function.

1. Choose **Advanced Setup > NAT > Virtual Servers** to access the configuration page, and click **Add**.
2. Select an interface, which is **ipoe_eth3/eth3.1** in this example.
3. **Select a Service:** Select **Web Server (HTTP)** from the drop-down list.
4. Set **Server IP Address** to **192.168.1.100**.

5. Set **Internal Port Start** to **80**.
6. Set **External Port Start** to **80**.
7. Set **Protocol** to **TCP/UDP**.

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	WAN Interface	Remove
Web Server (HTTP)	80	80	TCP	80	80	192.168.1.100	eth3.1	<input type="checkbox"/>

8. Click **Apply/Save**.

Step 2 Configure the DDNS function.

1. Choose **Advanced Setup > DNS > Dynamic DNS** to enter the configuration page, and click **Add**.
2. **D-DNS provider:** Select a DDNS service provider, which is **no-ip** in this example.
3. **Hostname:** Set the DDNS domain name registered on a DDNS service provider's website, which is **tenda.ddns.net**.
4. **Interface:** Select a WAN service, which is **ipoe_eth3/eth3.1** in this example. It should be the same as the interface set in the virtual servers function.
5. **Username/Password:** Set the user name and password registered on a DDNS service provider's website for logging in to the DDNS service.
6. Click **Apply/Save**.

Hostname	Username	Service	Interface	Remove
tenda.ddns.net	tenda	noip	eth3.1	<input type="checkbox"/>

----End

Verification

Verify that internet users can access the local web server at <http://tenda.ddns.net:80>.

4.13 DSL

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

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

Choose **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
- ADSL2+ Enabled
- AnnexM Enabled
- 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

Capability

- Bitswap Enable
- SRA Enable

Apply/Save

Parameter description

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 clients.
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 clients.

Parameter	Description
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 clients.
ADSL2	It specifies G992.3. The maximum uploading/downloading rate is 1 Mbps/12 Mbps.
AnnexL	It specifies reach Extended ADSL2. When the clients are far away from the modem router, this mode can improve the coverage. The maximum uploading/downloading rate is 1.5 Mbps/15 Mbps.
ADSL2+	It specifies G992.5. The maximum uploading/downloading rate is 1 Mbps/24 Mbps.
AnnexM	This mode is compatible with the upstreaming bandwidth extension mode and implemented based on G992.3 ADSL2 and G992.5 ADSL2+. In this mode, the upload rate of ADSL2+ is increased from 1 Mbps to 2.5 Mbps. AnnexM takes effect only when ADSL2, AnnexL or ADSL2+ is selected.
VDSL2	It specifies G993.2. The maximum uploading/downloading transmission rate of this device is 50 Mbps/80 Mbps.
Phone Line Pair	The phone line pair is used to work with the DSLAM. The default is recommended.
Bitswap	Bitswap can improve the ADSL adaptation capacity and the stability of ADSL line in the dynamic environment.
SRA	SRA (Seamless Rate Adaptation) is a dynamic rate adaptation protocol, really achieving ADSL rate adaptation. It dynamically adjust bit and power assignment to make the noise margin of the line within a suitable range when the ADSL line changes in running process, ensuring the stability of the line.
8a/8b/8c/8d/12a/12b/17a	These profiles are defined by the VDSL2 standard which enables the modem router to support CO, FTTC applications and so on, reducing the complexity and cost of the product development.
US0	It specifies a DSL frequency spectrum used to improve the negotiation rate.

4.14 UPnP

4.14.1 Overview

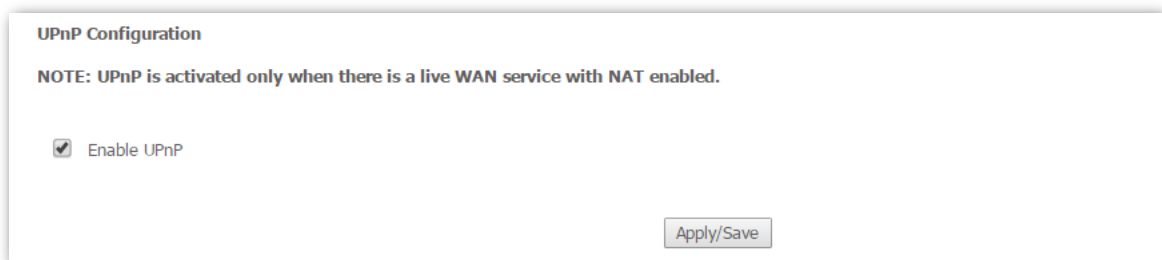
After the UPnP function is enabled, it can automatically enable ports for UPnP-supported programs, such as P2P and gaming software, in the internal network to improve your network experience.

4.14.2 Configuring the UPnP function

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

Step 2 Check the **Enable UPnP** option.

Step 3 Click **Apply/Save**.



UPnP Configuration

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

Enable UPnP

Apply/Save

----End

4.15 Storage service

4.15.1 Overview

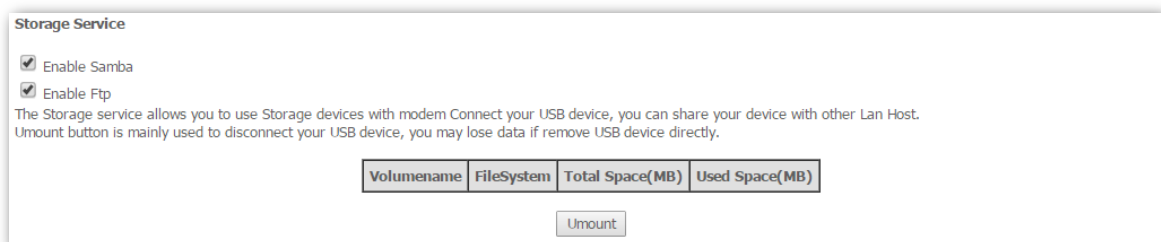
The modem router can automatically recognize a USB storage device connected to the USB port of the modem router. The device can be accessed over the LAN through FTP or Samba.

4.15.2 Enabling the Samba and FTP servers

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

Step 2 Select **Enable Samba**.

Step 3 Select **Enable FTP**.



Storage Service

Enable Samba
 Enable Ftp

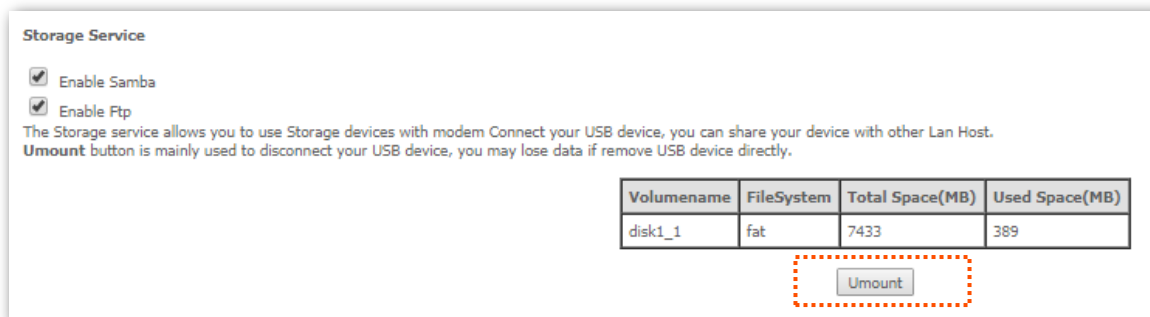
The Storage service allows you to use Storage devices with modem Connect your USB device, you can share your device with other Lan Host. Umount button is mainly used to disconnect your USB device, you may lose data if remove USB device directly.

Volumename	FileSystem	Total Space(MB)	Used Space(MB)

Umount

----End

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



Storage Service

Enable Samba
 Enable Ftp

The Storage service allows you to use Storage devices with modem Connect your USB device, you can share your device with other Lan Host. **Umount** button is mainly used to disconnect your USB device, you may lose data if remove USB device directly.

Volumename	FileSystem	Total Space(MB)	Used Space(MB)
disk1_1	fat	7433	389

Umount

4.15.3 Example of configuring the storage service function

4.15.3.1 Network requirement

A V1200 modem router is used to set up a LAN in an apartment. Users in the apartment need to share some pictures and videos over the LAN through FTP or Samba.

4.15.3.2 Solution

Connect a USB storage device with the pictures and videos to the USB port of the modem router. The modem router can function as a file server.

Assume that:

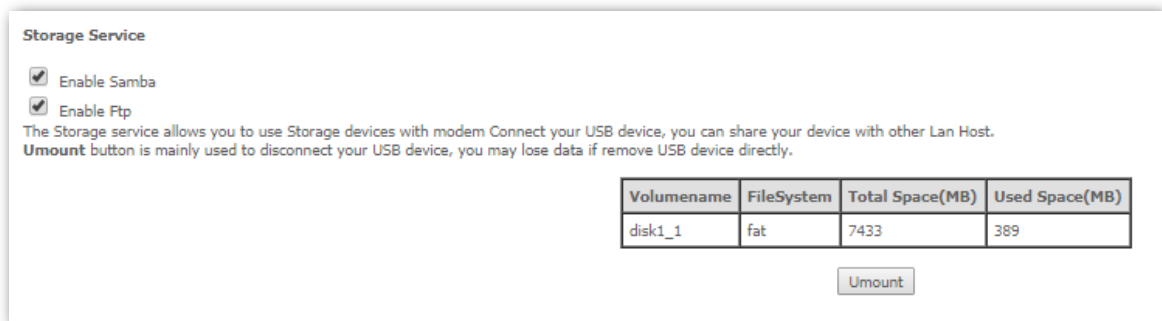
The server address is **192.168.1.1** (the LAN IP address of the modem router).

4.15.3.3 Configuration procedure

Step 1 Insert the USB storage device (compliant with USBV2.0 port) to the USB port of the modem router.

Step 2 Choose **Advanced Setup > Storage Service** to enter the configuration page.


Step 3 Check the **Enable Samba** and **Enable Ftp** options.

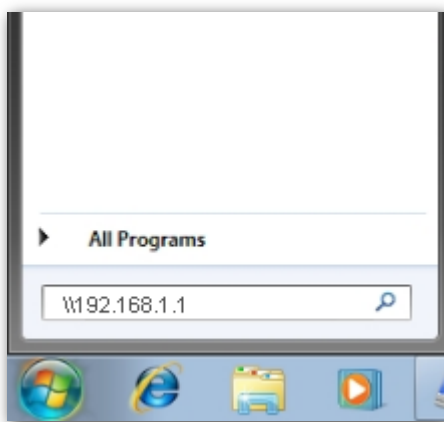


----End

4.15.3.4 Verification

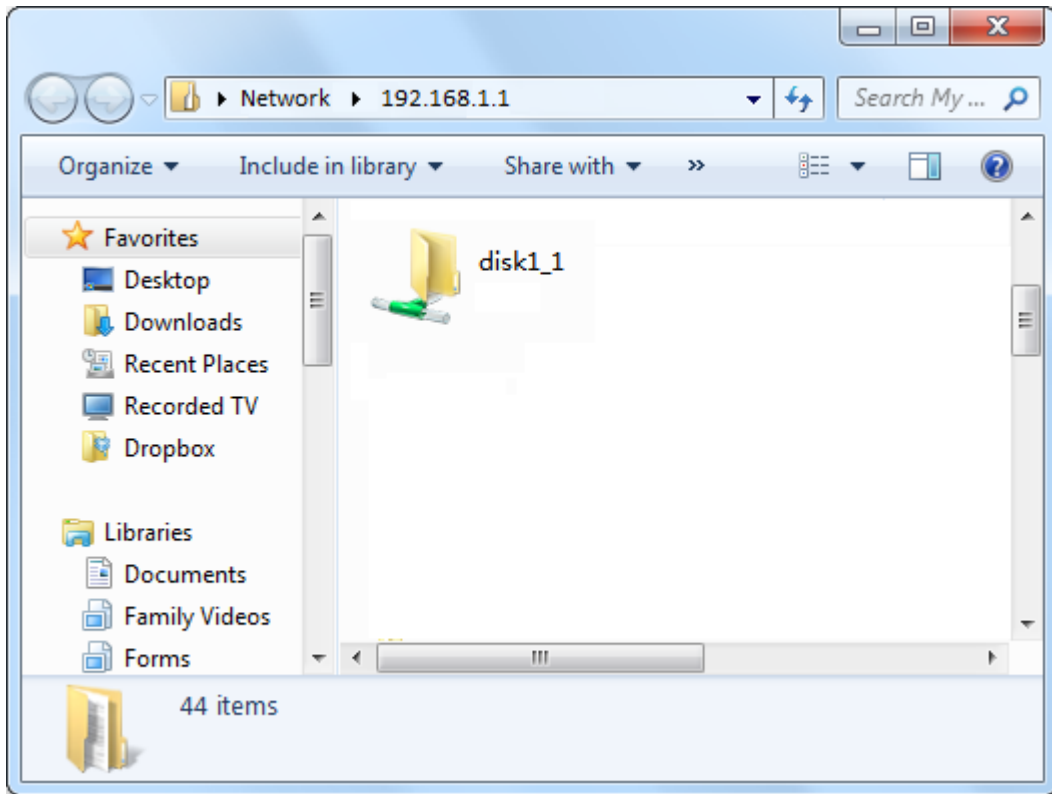
To access the USB storage device over the LAN through Samba, perform the following procedure: (OS example: Windows 7)

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



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

Step 3 Double-click the **disk1_1** folder.

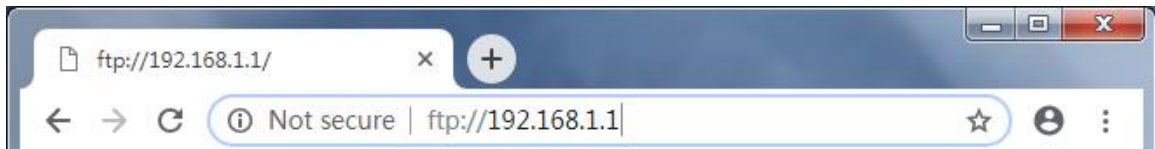


----End

To access the USB storage device over the LAN through FTP, perform the following procedure:
(Browser example: Google Chrome)

Step 1 Start the Google Chrome, enter **ftp://192.168.1.1** in the address bar.

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



----End

4.16 Interface grouping

4.16.1 Overview

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

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

Interface Grouping -- A maximum 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		eth3.1	LAN1	
			LAN2	
			LAN3	
		wlan0		
		wlan1		

4.16.2 Example of configuring interface grouping

Assume that:


- The modem router accesses the internet through port 4 using an Ethernet cable.
- You create two WAN services:
WAN1: WAN service type is set to **Bridging**.
WAN2: WAN IP settings are set to **IP over Ethernet** and **Obtain an IP address automatically**.
- You want all wireless devices to use **IP over Ethernet** WAN service, and all wired device use **bridging** WAN service.

To create an interface group, perform the following procedure:

Step 1 Choose **Advanced Setup > Interface Grouping** to enter the configuration page, and click **Add**.

Step 2 Enter a group name, which is **WLAN_group** in this example.

Step 3 Select a WAN service you create, which is **ipoe_LAN3/eth3.1** in this example.

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

Group Name:

WAN Interface used in the grouping:

Grouped LAN Interfaces

- wlan0
- wlan1

Available LAN Interfaces

- LAN3
- LAN2
- LAN1

-> <-

Step 5 Click **Apply/Save**.

----End

After the configuration takes effect, all wireless interfaces belong to **WLAN_group**, and use the WAN service **IP over Ethernet** (eth3.1). All wired interfaces (port 1, 2, and 3) belong to the default group, and use the WAN service **Bridging** (eth3.2).

Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs
Default		eth3.2	LAN3	
			LAN2	
			LAN1	
WLAN_group	<input type="checkbox"/>	eth3.1	wlan0	
			wlan1	



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

4.17 IP tunnel

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

The modem router provides two IP tunnels: [IPv6inIPv4](#) and [IPv4inIPv6](#).

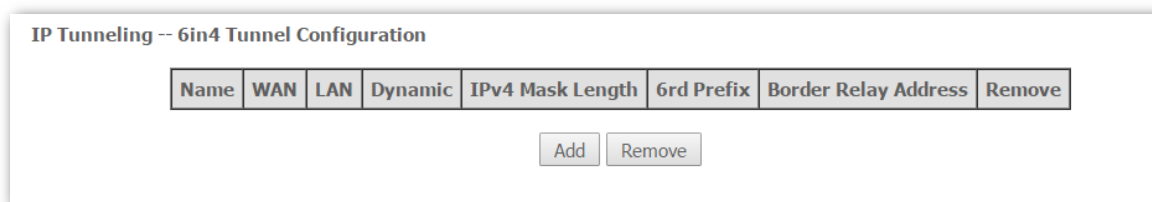
4.17.1 IPv6inIPv4

4.17.1.1 Overview

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.

4.17.1.2 Configuring the IPv6inIPv4 tunnel

Step 1 Choose **Advanced Setup > IP Tunnel > IPv6inIPv4** to enter the configuration page, and click **Add**.



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

Step 2 Tunnel Name: Specify a name for the tunnel you set up.

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

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

Step 5 Associated LAN Interface: Select the LAN interface uses IPv6.

Step 6 Select a type of obtaining border relay address.

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

Step 7 IPv4 Mask Length: Enter the IPv4 mask length.

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

Step 9 Border Relay IPv4 Address: Enter the border relay IPv4 address of WAN interface.

Step 10 Click **Apply/Save**.

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:

Apply/Save

----End

4.17.2 IPv4inIPv6

4.17.2.1 Overview

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.

4.17.2.2 Configuring the IPv4inIPv6 tunnel

Step 1 Choose **Advanced Setup > IP Tunnel > IPv4inIPv6** to enter the configuration page, and click **Add**.

IP Tunneling -- 4in6 Tunnel Configuration

Name	WAN	LAN	Dynamic	AFTR	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/>					

Step 2 Tunnel Name: Enter a tunnel name.

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

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

Step 5 Associated LAN Interface: Select the LAN interface uses IPv4.

Step 6 Select a type of obtaining AFTR IPv6 address.

- **Manual:** Manually set an AFTR IPv6 address.

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

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

Step 8 Click **Apply/Save**.

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:

Apply/Save

----End

4.18 IPSec

4.18.1 Overview

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 Setup > IPSec** to enter the configuration page.

IPSec Tunnel Mode Connections

Add, remove or enable/disable IPSec tunnel connections from this page.

Connection Name	Remote Gateway	Local Addresses	Remote Addresses	Remove
-----------------	----------------	-----------------	------------------	--------

Click **Add New Connection** to create a new connection.

IPSec Settings

IPSec Connection Name

IP Version:

Tunnel Mode

Local Gateway Interface:

Remote IPSec Gateway Address

Tunnel access from local IP addresses

IP Address for VPN

Mask or Prefix Length

Tunnel access from remote IP addresses

IP Address for VPN

Mask or Prefix Length

Key Exchange Method

Authentication Method

Pre-Shared Key

Perfect Forward Secrecy

Advanced IKE Settings

Parameter description

Parameter	Description
IPSec Connection Name	It specifies a name for the IPSec connection.
IP Version	Select an IP version to which the rule applies.
Tunnel Mode	<p>It specifies tunnel protocol the rule uses.</p> <ul style="list-style-type: none"> • ESP: It specifies Encapsulating Security Payload. This protocol is used to test data integrity and encryption. Even the encrypted packet is intercepted, the third party also cannot obtain correct message. • AH: It specifies Authentication Header. This protocol is used to test data integrity. If a packet is tampered during transmission, the receiver discards the packet when it performs data integrity test.
Local Gateway Interface	Select a WAN service for the rule.
Remote IPSec Gateway Address	It specifies the WAN IP address or domain name of the peer device enabled IPSec function.
Tunnel access from local IP addresses	<ul style="list-style-type: none"> • Subnet: When Subnet is selected, you can specify any network address on LAN and the corresponding subnet mask. • Single Address: When Single Address is selected, you can only specify an IP address of a local host.
IP Address for VPN	It specifies the IP address of a local host.
Mask or Prefix Length	It specifies the subnet mask of the LAN you specified in IP Address for VPN .
Tunnel access from remote IP addresses	<ul style="list-style-type: none"> • Subnet: When Subnet is selected, you can specify all hosts on the peer network. • Single Address: When Single Address is selected, you can only specify one host on the peer network.
IP Address for VPN	It specifies IP address of a host on peer network.
Mask or Prefix Length	It specifies LAN IP network segment of the peer router.
Key Exchange Method	<p>It specifies the key negotiation method.</p> <ul style="list-style-type: none"> • Auto(IKE): When Auto(IKE) is selected, the negotiation process is divided into two stages: <ul style="list-style-type: none"> Stage 1: Both communication sides exchange verification algorithm, encryption algorithm and so on security protocols, and establish an ISAKMP (Internet Security Association and Key Management Protocol) SA (Security Association) which is used to exchange more information in stage 2.

Parameter	Description
	<p>Stage 2: Both communication sides take ISAKMP SA as IPSec security protocol parameters, and create IPSec SA which is used to secure data transmission.</p> <ul style="list-style-type: none"> • Manual: Refer to Key Exchange Method-Manual.

Key Exchange Method-Manual

When **Manual** is selected, the following parameters appear.

Parameter description

Parameter	Description
Perfect Forward Secrecy	<p>It specifies the property that ensures that a session key derived from a set of long-term public and private keys will not be compromised if one of the (long-term) private keys is compromised in the future.</p> <p>Select Enable or Disable according to your needs. It is disabled by default.</p>
Advanced IKE Settings	Refer to Advanced IKE Settings .
Encryption Algorithm	<p>When the Tunnel Mode is set to ESP, you can configure ESP encryption algorithm. The modem router supports the following encryption algorithm:</p> <ul style="list-style-type: none"> • DES: It specifies Data Encryption Standard. • 3DES: It specifies Triple DES. • AES(aes-cbc): It specifies Advanced Encryption Standard.
Encryption Key	It specifies an encryption key. Both communication sides should set it to the same one.
Authentication Algorithm	<p>When the Tunnel Mode is set to AH, you can configure AH authentication algorithm. The modem router supports the following authentication algorithm:</p> <ul style="list-style-type: none"> • MD5: It specifies Message Digest Algorithm. The system generates a 128 bit

Parameter	Description
	<p>message digest for a message.</p> <ul style="list-style-type: none"> • SHA1: It specifies Secure Hash Algorithm. The system generates a 128 bit message digest for a message.
Authentication Key	It specifies an authentication key. Both communication sides should set it to the same one.
SPI	It specifies Security Parameter Index. It is an identification tag added to the header while using IPsec for tunneling the IP traffic. This tag helps the kernel discern between two traffic streams where different encryption rules and algorithms may be in use.

Advanced IKE Settings

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

Parameter description

Parameter	Description
Mode	<p>The mode should be set to the same one as that of the peer device.</p> <ul style="list-style-type: none"> • Main: This mode provides identity protection, and is applicable to high requirement situation for identity protection. • Aggressive: This mode does not provide identity protection, and is applicable to not high requirement situation for identity protection.

Parameter	Description
Encryption Algorithm	<ul style="list-style-type: none"> • DES: It specifies Data Encryption Standard. • 3DES: It specifies Triple DES. • AES: It specifies Advanced Encryption Standard. AES - 128/192/256 indicates that the key length is 128/192/256 bit.
Integrity Algorithm	<ul style="list-style-type: none"> • MD5: It specifies Message Digest Algorithm. The system generates a 128 bit message digest for a message. • SHA1: It specifies Secure Hash Algorithm. The system generates a 128 bit message digest for a message.
Select Diffie-Hellman Group for Key Exchange	It specifies the group information of Diffie-Hellman algorithm. It is used to generate session key encrypted IKE tunnel.
Key Life Time	It specifies the life time of IPSec SA.

4.18.2 Configuring the IPSec function

- Step 1** Choose **Advanced Setup > IPSec** to enter the configuration page, and click **Add New Connection**.
- Step 2** Enter an IPSec connection name, which is **IPSec_1** in this example.
- Step 3** Enter the IP version, which is **IPv4** in this example.
- Step 4** Select a local gateway interface, which is **ipoe_LAN1/eth3.1** in this example.
- Step 5** Enter a remote IPSec gateway address, which is **210.76.200.101** in this example.
- Step 6** Set Tunnel access from local IP address to Subnet, and set a local network segment which is **192.168.1.0** and **255.255.255.0** in this example.
- Step 7** Set Tunnel access from remote IP address to Subnet, and set a local network segment of the peer router which is **192.168.0.0** and **255.255.255.0** in this example.
- Step 8** Enter a Pre-Shared key which is **12345678** in this example. And leave other parameters unchanged.
- Step 9** Click **Apply/Save**.

IPSec Settings

IPSec Connection Name: IPSec_1

IP Version: IPv4

Tunnel Mode: ESP

Local Gateway Interface: ipoe_eth3/eth3.1

Remote IPSec Gateway Address: 210.76.200.101

Tunnel access from local IP addresses: Subnet

IP Address for VPN: 192.168.1.0

Mask or Prefix Length: 255.255.255.0

Tunnel access from remote IP addresses: Subnet

IP Address for VPN: 192.168.0.0

Mask or Prefix Length: 255.255.255.0

Key Exchange Method: Auto(IKE)

Authentication Method: Pre-Shared Key

Pre-Shared Key: 12345678

Perfect Forward Secrecy: Disable

Advanced IKE Settings: Show Advanced Settings

Apply/Save

----End

The rule is displayed in the list shown as below.

IPSec Tunnel Mode Connections

Add, remove or enable/disable IPSec tunnel connections from this page.

Connection Name	Remote Gateway	Local Addresses	Remote Addresses	Remove
IPSec_1	210.76.200.101	192.168.1.0	192.168.0.0	<input type="checkbox"/>

Add New Connection Remove

4.19 Certificate

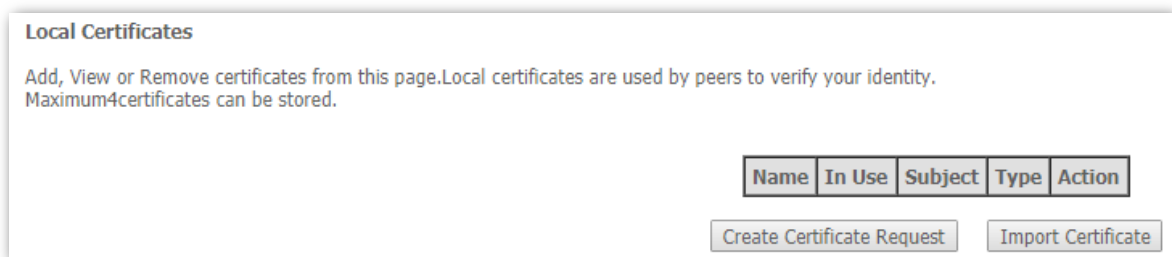
4.19.1 Local

4.19.1.1 Overview

Local certificate is used by peers to verify your identity.

4.19.1.2 Importing a certificate

Step 1 Choose **Advanced Setup > Certificate > Local** to enter the configuration page, and click **Import Certificate**.



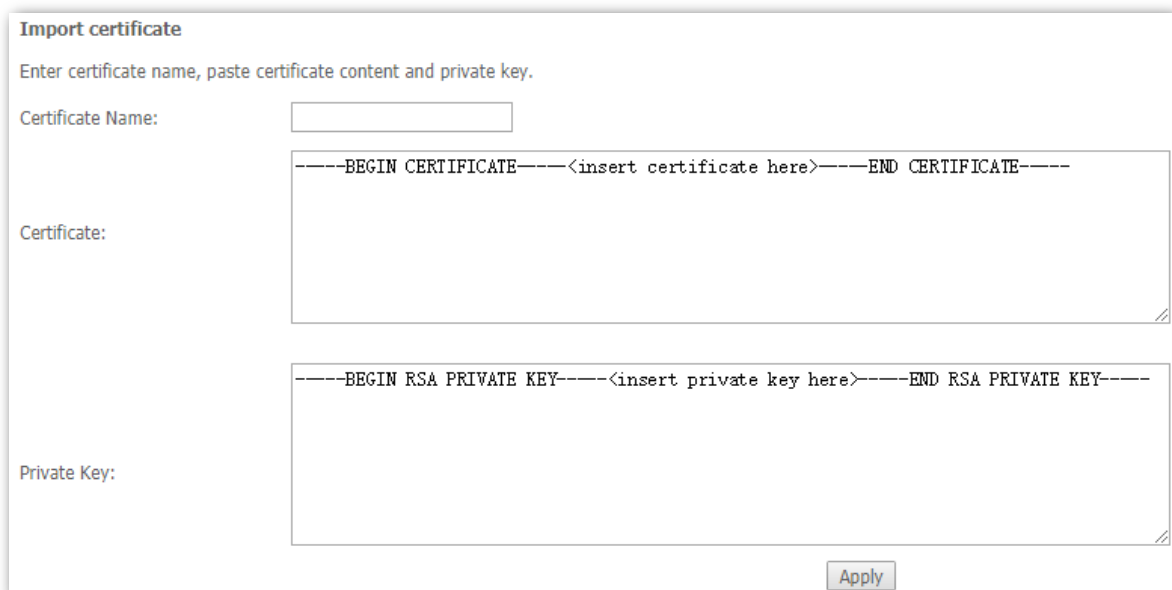
The screenshot shows a web interface titled "Local Certificates". Below the title is a descriptive text: "Add, View or Remove certificates from this page. Local certificates are used by peers to verify your identity. Maximum 4 certificates can be stored." At the bottom right, there is a table with five columns: "Name", "In Use", "Subject", "Type", and "Action". Below the table are two buttons: "Create Certificate Request" and "Import Certificate".

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

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

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

Step 5 Click **Apply**.

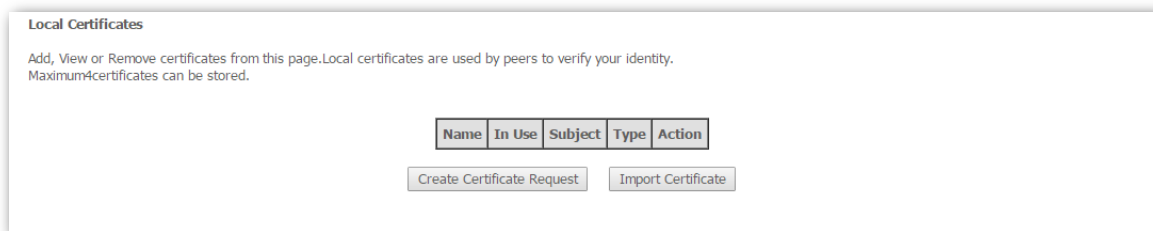


The screenshot shows a web interface titled "Import certificate". Below the title is a descriptive text: "Enter certificate name, paste certificate content and private key." There are three input fields: "Certificate Name:" with a text box, "Certificate:" with a large text area containing the placeholder text "-----BEGIN CERTIFICATE-----<insert certificate here>-----END CERTIFICATE-----", and "Private Key:" with a large text area containing the placeholder text "-----BEGIN RSA PRIVATE KEY-----<insert private key here>-----END RSA PRIVATE KEY-----". At the bottom right, there is an "Apply" button.

----End

4.19.1.3 Creating a new certificate

Step 1 Choose **Advanced Setup > Certificate > Local** to enter the configuration page, and click **Create Certificate Request**.



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

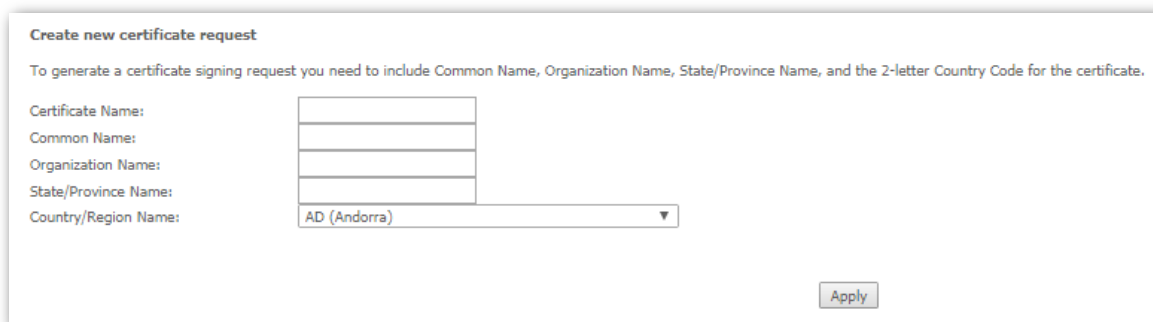
Step 3 **Common Name:** Enter the website domain name, company name or name of the applicant, such as **Tendacn.com, Tenda** or **Lucy**.

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

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

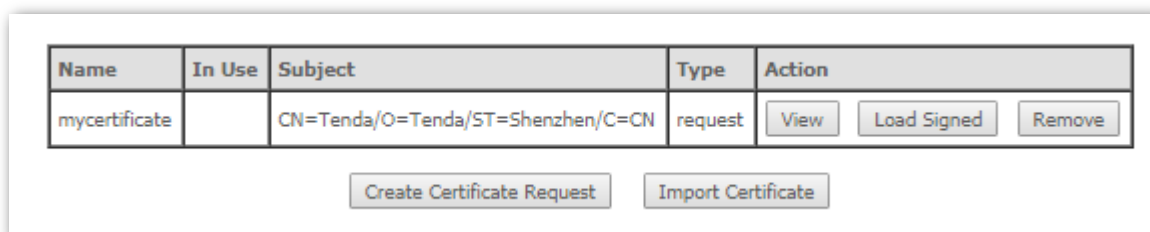
Step 6 **Country/Region Name:** Select the country/region where the certificate is to be used.

Step 7 Click **Apply**.



----End

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



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

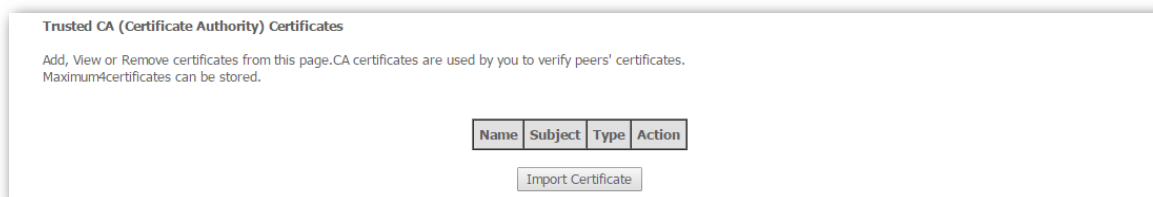
4.19.2 Trusted CA

4.19.2.1 Overview

CA certificates are used by user to verify peers' certificates.

4.19.2.2 Importing a certificate

Step 1 Choose **Advanced Setup > Certificate > Trusted CA** to enter the configuration page, and click **Import Certificate**.



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
------	---------	------	--------

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**.



Import CA certificate

Enter certificate name and paste certificate content.

Certificate Name:

Certificate:

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

Apply

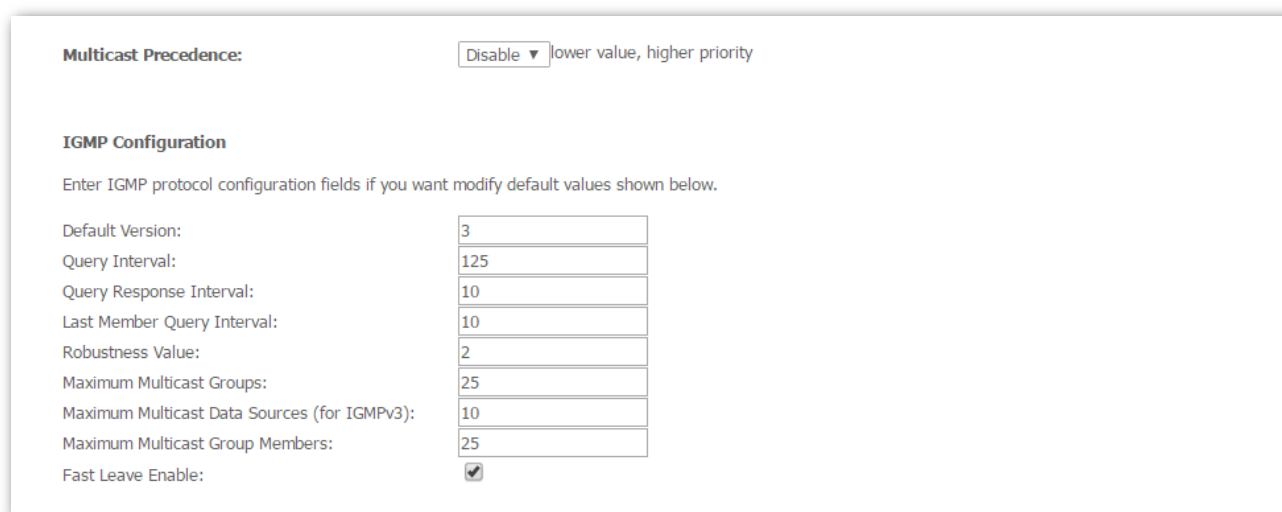
----End

4.20 Multicast

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

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

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



Multicast Precedence: Disable ▾ lower value, higher priority

IGMP Configuration

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

Default Version:	<input type="text" value="3"/>
Query Interval:	<input type="text" value="125"/>
Query Response Interval:	<input type="text" value="10"/>
Last Member Query Interval:	<input type="text" value="10"/>
Robustness Value:	<input type="text" value="2"/>
Maximum Multicast Groups:	<input type="text" value="25"/>
Maximum Multicast Data Sources (for IGMPv3):	<input type="text" value="10"/>
Maximum Multicast Group Members:	<input type="text" value="25"/>
Fast Leave Enable:	<input checked="" type="checkbox"/>

Parameter description

Parameter	Description
Default Version	It specifies the IGMP version for WAN. The default is IGMPv3.
Query Interval	It specifies the interval for sending IGMP query message. The default is 125 . The value range is 1 to 999. The unit is second.
Query Response Interval	It specifies the response interval for the query message. The default is 10 . The value range is 1 to 999. The unit is "second".
Last Member Query Interval	It specifies the interval for sending query message of specified group. The default is 10 . The value range is 1 to 999. The unit is second.
Robustness Value	It specifies the robustness value of IGMP querier. The default is 2 . The value range is 1 to 999.
Maximum Multicast Groups	It specifies the maximum number of multicast groups for each interface. The default is 25 . The value range is 1 to 32.
Maximum Multicast Data Sources (for IGMPv3)	It specifies the maximum number of multicast data sources. The default is 10 . The value range is 1 to 24.

Parameter	Description
Maximum Multicast Group Members	It specifies the maximum number of multicast group members. The default is 25. The value range is 1 to 32.
Fast Leave Enable	If the function is enabled, the modem router does not send group specific-queries when it receives a leave message.

MLD Configuration

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

Default Version:	<input style="width: 60%;" type="text" value="2"/>
Query Interval:	<input style="width: 60%;" type="text" value="125"/>
Query Response Interval:	<input style="width: 60%;" type="text" value="10"/>
Last Member Query Interval:	<input style="width: 60%;" type="text" value="10"/>
Robustness Value:	<input style="width: 60%;" type="text" value="2"/>
Maximum Multicast Groups:	<input style="width: 60%;" type="text" value="10"/>
Maximum Multicast Data Sources (for mldv2):	<input style="width: 60%;" type="text" value="10"/>
Maximum Multicast Group Members:	<input style="width: 60%;" type="text" value="10"/>
Fast Leave Enable:	<input checked="" type="checkbox"/>

Parameter description

Parameter	Description
Default Version	It specifies the MLD version for WAN. The default is MLDv2.
Query Interval	It specifies the interval for sending MLD query message. The default is 125 . The value range is 1 to 999. The unit is second.
Query Response Interval	It specifies the response interval for the query message. The default is 10 . The value range is 1 to 999. The unit is "second".
Last Member Query Interval	It specifies the interval for sending query message of specified group. The default is 10 . The value range is 1 to 999. The unit is second.
Robustness Value	It specifies the robustness value of MLD querier. The default is 2 . The value range is 1 to 999.
Maximum Multicast Groups	It specifies the maximum number of multicast groups for each interface. The default is 10. The value range is 1 to 16.
Maximum Multicast Data Sources (for mldv2)	It specifies the maximum number of multicast data sources. The default is 10 . The value range is 1 to 16.
Maximum Multicast Group Members	It specifies the maximum number of multicast group members. The default is 10. The value range is 1 to 16.

Parameter	Description
Fast Leave Enable	If the function is enabled, the modem router does not send group specific-queries when it receives a leave message.

4.21 IPTV

If your ISP provides IPTV service, this function enables you to watch IPTV programs through TV and the network set-top box while surfing the internet

4.21.1 ATM interface

If your layer 2 interface is **ATM Interface**, perform the following procedure:

- Step 1** Choose **Advanced Setup > IPTV** to enter the configuration page.
- Step 2** Select **Enable IPTV** option.
- Step 3** Select **ATM Interface**.
- Step 4** Select a LAN port to serves as an IPTV port for connecting to the set-top box. The default IPTV port is **lan1** (port 1).
- Step 5** Enter the VPI/VCI value provided by your ISP.
- Step 6** Click **Apply/Save**.

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

----End

4.21.2 ETH interface

If your layer 2 interface is **Ethernet Interface**, perform the following procedure:

- Step 1** Choose **Advanced Setup > IPTV** to enter the configuration page.
- Step 2** Select **Enable IPTV** option.
- Step 3** Select **Ethernet Interface**.
- Step 4** Select a LAN port to serves as an IPTV port for connecting to the set-top box. The default IPTV port is **lan1** (port 1).
- Step 5** Enter the 802.1P priority and 802.1Q VLAN ID values provided by your ISP.
- Step 6** Click **Apply/Save**.

The screenshot shows the 'IPTV --- IPTV Management Configuration' page. It includes a checkbox for 'Enable IPTV' which is checked. Under 'Select Layer2 Interface', 'ETH Interface' is selected with a radio button. Below that, 'Please select the LAN port for IPTV connection and connect the set-top box (STB) to that port.' shows 'lan1' selected with a checkbox. At the bottom, there are two input fields: 'Enter 802.1P Priority [0-7]:' with '-1' and 'Enter 802.1Q VLAN ID [1-4094]:' with '-1'. An 'Apply/Save' button is located at the bottom right.

----End

4.21.3 PTM interface

If your layer2 interface is **PTM Interface**, perform the following procedure:

- Step 1** Choose **Advanced Setup > IPTV** to enter the configuration page.
- Step 2** Select **Enable IPTV** option.
- Step 3** Select **PTM Interface** you create in [Layer2 Interface](#).
- Step 4** Select a LAN port to serves as an IPTV port for connecting to the set-top box. The default IPTV port is **lan1** (port 1).
- Step 5** Enter the 802.1P priority and 802.1Q VLAN ID values provided by your ISP. This VLAN ID is NOT the same as that of the WAN connection.
- Step 6** Click **Apply/Save**.

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

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]:

Enter 802.1Q VLAN ID [1-4094]:

Apply/Save

----End

5 Wireless

5.1 2.4G

5.1.1 Basic

5.1.1.1 Overview

This section allows you to configure basic features of the 2.4 GHz wireless network.

Choose **Wireless > 2.4G > 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 restrict the channel set based on country requirements. Click "Apply/Save" to configure the basic wireless options.

Enable Wireless

Hide Access Point

Disable WMM Advertise

Enable Wireless Multicast Forwarding (WMF)

SSID:

BSSID: C8:3A:35:14:4B:61

Wireless Mode:

Country:

Channel: Current:11(interference: acceptable)

Bandwidth: Current:40MHz

Control Sideband: Current:Upper

Parameter description

Parameter	Description
Enable Wireless	Select the option to enable the wireless function.
Hide Access Point	Select the option to hide the SSID of the modem router. In this case, wireless clients cannot find the SSID (wireless network name) of the modem route. The SSID must be manually entered on the wireless clients for connecting the clients to the modem router.
Disable WMM Advertise	Select the option to disable WMM advertise of the modem router. WMM optimizes the communication experience of end-users, providing high-quality network connectivity performance for data, voice, music, and video applications in a complex network

Parameter	Description
	environment and communications environment.
Enable Wireless Multicast Forwarding (WMF)	Select the option to enable WMF of the modem router. Wireless multicast forwarding is a network data transmission method, which improves the efficiency of data transmission to effectively save network bandwidth and reduce network load.
SSID	Wireless network name of the modem router.
BSSID	MAC address of the wireless network.
Wireless Mode	<ul style="list-style-type: none"> • If 802.11b is selected, only 11b wireless devices can connect to the wireless network. The maximum wireless rate supported in this mode is 11 Mbps. • 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 or region.
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.
Control Sideband	It specifies the channel extension direction. When the bandwidth is set to 40MHz, you can choose upper or lower to define the direction of channel extension.

5.1.1.2 Enabling multiple SSIDs

By setting up multiple SSIDs on a wireless modem router, the modem router can be deployed to multiple wireless networks, and users can connect to different wireless LANs to avoid interference with each other.

To enable multiple SSIDs:

Step 1 choose **Wireless > 2.4G > Basic** to enter the configuration page.

Step 2 Select **Enable** option to enable the corresponding SSID.

Step 3 Customize the wireless network name for the SSID if you want.

Step 4 Hidden: It specifies whether to hide the SSID. If the option is selected, wireless devices cannot find the SSID.

Step 5 Disable WMM Advertise: WMM (Wi-Fi Multimedia) is a Wi-Fi Alliance interoperability

certification based on the IEEE 802.11e standard. Select it if you need to disable WMM advertise.

Step 6 Enable WMF: It specifies whether to forward multicast packets through unicast tunnels. Generally, multicast packets are transmitted at the lowest rate, such as 1 Mbps, leading to poor transmission efficiency. WMF leverages the auto-negotiated high rate, reliable feedback mechanism, and other advantages of unicast packets to address multicast problems such as video playback stalls caused by packet loss and long delays over a wireless network.

Step 7 Click **Apply/Save**.

Wireless - Guest/Virtual Access Points:					
Enabled	SSID	Hidden	Disable WMM Advertise	Enable WMF	Enable HSPOT
<input type="checkbox"/>	guest2.4G_1	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	N/A
<input type="checkbox"/>	guest2.4G_2	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	N/A
<input type="checkbox"/>	guest2.4G_3	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	N/A

----End

5.1.2 Security

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

Choose **Wireless > 2.4G > 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 both STA PIN and Authorized MAC are empty, PBC is used. If Hide Access Point enabled or Mac filter list is empty with "allow" chosen, WPS2 will be disabled

WPS Setup

EnableWPS

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:

Network Authentication:

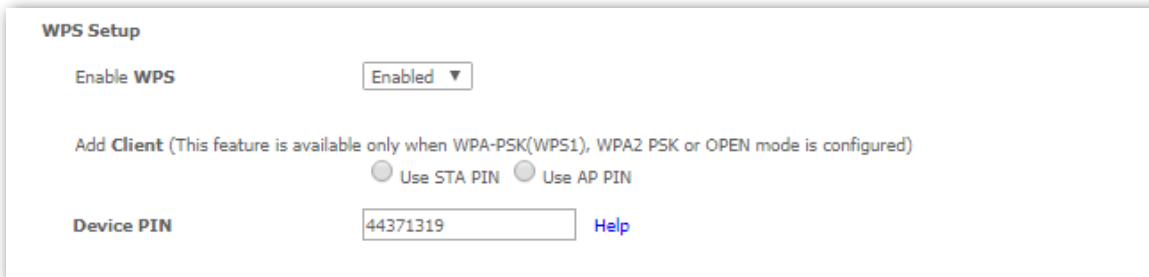
WPA/WAPI passphrase: [Click here to display](#)

WPA/WAPI Encryption:

5.1.2.1 WPS setup

Wi-Fi Protected Setup makes it easy for home users who know little of wireless security to establish a home network, as well as to add new devices to an existing network without entering long passphrases or configuring complicated settings. They can set up network connections simply by entering a PIN code on the device web interface or pressing hardware WPS button (on the back panel of the device).

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



WPS Setup

Enable WPS

Add Client (This feature is available only when WPA-PSK(WPS1), WPA2 PSK or OPEN mode is configured)

Use STA PIN Use AP PIN

Device PIN [Help](#)

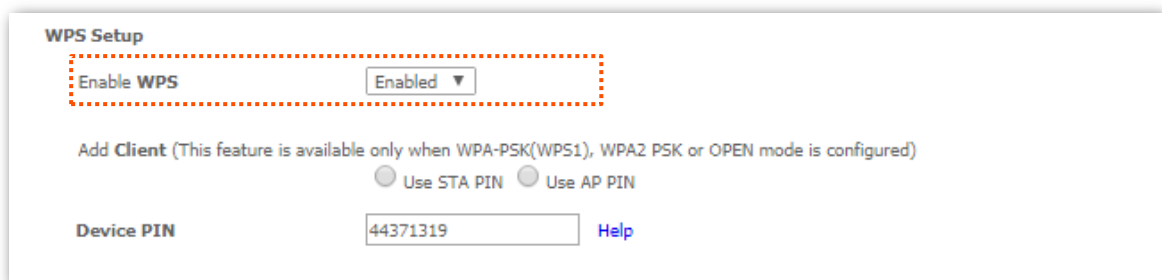
If the wireless network of the modem router is not encrypted, or the wireless network is encrypted but you forget or do not want to enter the complicated password, you can use WPS function to encrypt or connect clients to it quickly. There are three options for you:

Option 1: PBC negotiation

Step 1 Choose **Wireless > 2.4G > 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

Add Client (This feature is available only when WPA-PSK(WPS1), WPA2 PSK or OPEN mode is configured)

Use STA PIN Use AP PIN

Device PIN [Help](#)

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

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

----End

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

Option 2: Using the WPS PIN code of the wireless device

Step 1 Log in to the web UI of the modem router, choose **Wireless > 2.4G > Security** to enter the

configuration page.

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

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

Step 4 Select **Enter STA PIN**.

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

Step 6 Click **Apply/Save**.

The screenshot shows the 'WPS Setup' configuration page. At the top, 'Enable WPS' is set to 'Enabled'. Below this, there is a section for 'Add Client' with a note: '(This feature is available only when WPA-PSK(WPS1), WPA2 PSK or OPEN mode is configured)'. Under 'Add Client', the 'Use STA PIN' radio button is selected, and the 'Device PIN' field contains the value '31192668'. There are 'Help' links next to the 'Use AP PIN' and 'Device PIN' fields.

----End

The WPS LED indicator blinks for about 2 minutes, and then turns to solid green. It indicates that the wireless device is connected to the modem router, and the wireless network is encrypted.

Option 3: Using the WPS PIN code of the modem router

Step 1 Log in to the web UI of the modem router, choose **Wireless > 2.4G > 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**.

The screenshot shows the 'WPS Setup' configuration page. At the top, 'Enable WPS' is set to 'Enabled'. Below this, there is a section for 'Add Client' with a note: '(This feature is available only when WPA-PSK(WPS1), WPA2 PSK or OPEN mode is configured)'. Under 'Add Client', the 'Use AP PIN' radio button is selected, and the 'Device PIN' field contains the value '44371319'. There are 'Help' links next to the 'Use STA PIN' and 'Device PIN' fields.

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

----End

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

5.1.2.2 Manual setup AP

Overview

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

A wireless network uses radio, which is open to the public, as its data transmission medium. If the wireless network is not protected by necessary measures, any client can connect to the network to use the resources of the network or access unprotected data over the network. To ensure communication security, transmission links of wireless networks must be encrypted for protection.

The modem router supports various security modes for network encryption, including **Open**, **Shared**, **WPA-PSK**, **WPA2-PSK**, **Mixed WPA/WPA2-PSK**, and **WPA2 Enterprise**.

■ Open/Shared

Open/Shared supports WEP encryption.

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

The screenshot shows a configuration interface for WEP encryption. It includes the following fields and options:

- Select SSID:** Tenda_F02910
- Network Authentication:** Shared
- Encryption Strength:** 128-bit
- Current Network Key:** 1
- Network Key 1:** 1234567890123
- Network Key 2:** 1234567890123
- Network Key 3:** 1234567890123
- Network Key 4:** 1234567890123

Below the keys, there is a note: "Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys" and "Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys". An "Apply/Save" button is located at the bottom.

Parameter description

Parameter	Description
Encryption Strength	Select 128-bit or 64-bit according to your needs.
Current Network Key	Select a network key to be used.
Network Key 1/2/3/4	Enter 13 ASCII characters or 26 hexadecimal digits as a 128-bit encryption key; enter 5 ASCII characters or 10 hexadecimal digits as a 64-bit encryption keys.

■ WPA2 Enterprise

Select SSID: Tenda_F02910 ▼

Network Authentication: WPA2 Enterprises ▼

Network Re-auth Interval: 36000

RADIUS Server Address: (null)

RADIUS Port: 1812

RADIUS Key: *****

RADIUS Server2 Address: (null)

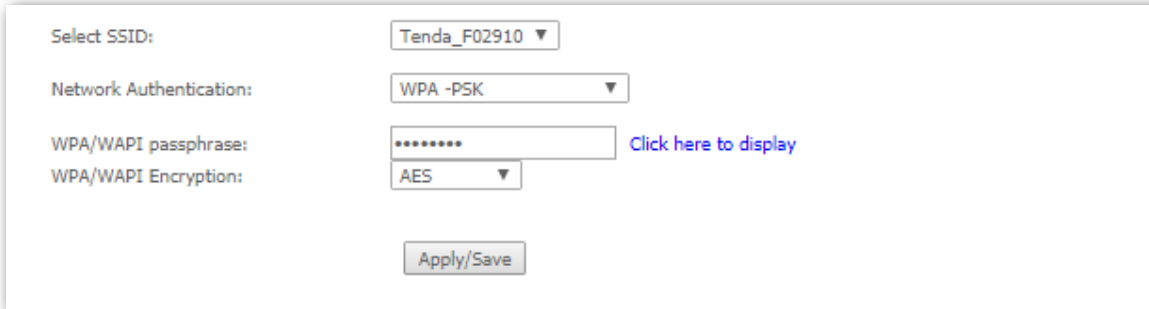
WPA/WAPI Encryption: AES ▼

Apply/Save

Parameter description

Parameter	Description
WPA2 Enterprise	Security modes implemented based on the IEEE 802.1x, which requires the third-party RADIUS server for authentication.
Network Re-auth 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 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.
RADIUS Server2 Address	It specifies the IP address of the secondary RADIUS server for authentication.
WPA/WAPI Encryption	<p>It specifies an algorithm for WPA2 enterprise encryption.</p> <ul style="list-style-type: none"> • AES: If selected, AES enabled wireless clients can join your wireless network. • TKIP+AES: If selected, both AES and TKIP enabled wireless clients can join your wireless network.

■ WPA-PSK/WPA2-PSK/Mixed WPA2/WPA-PSK



The screenshot shows a configuration interface with the following fields:

- Select SSID: Tenda_F02910
- Network Authentication: WPA -PSK
- WPA/WAPI passphrase: [masked with asterisks] [Click here to display](#)
- WPA/WAPI Encryption: AES
- Apply/Save button

Parameter description

Parameter	Description
WPA-PSK/WPA2-PSK/Mixed WPA2/WPA-PSK	They specify the security modes implemented based on a shared key.
WPA/WAPI Passphrase	It specifies the password of the wireless network.
WPA/WAPI Encryption	It specifies an algorithm for WPA encryption. <ul style="list-style-type: none">• 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.

Changing the encryption settings of an SSID

- Step 1** Choose **Wireless > 2.4G > Security** to enter the configuration page.
 - Step 2** Select a SSID to be configured from the drop-down list.
 - Step 3** Select the network authentication type and set the related parameters as required.
 - Step 4** Click **Apply/Save**.
- End

5.1.3 MAC filter

5.1.3.1 Overview

The MAC-based wireless access control feature can be used to allow or disallow clients to connect to your 2.4 GHz wireless networks.

Choose **Wireless > 2.4G > MAC Filter** to enter the configuration page.

Wireless -- MAC Filter

Select SSID: Tenda_144B60 ▼

MAC Restrict Mode: Disabled Allow Deny Note: If 'allow' is choosed and mac filter is empty, WPS will be disabled

MAC Address Remove

Add Remove

Parameter description

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

5.1.3.2 Adding a MAC filter rule

Step 1 Choose **Wireless > 2.4G > MAC Filter** to enter the configuration page.

Step 2 Select a SSID to apply the rule if you enable multiple SSIDs.

Step 3 Click **Add**.

Step 4 Enter the MAC address of the device to which the rule applies.

Step 5 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.

MAC Address:

Step 6 Select **Allow** or **Deny** according to your needs.

Wireless -- MAC Filter

Select SSID:

MAC Restrict Mode: Disabled Allow Deny Note: If 'allow' is choosed and mac filter is empty, WPS will be disabled

MAC Address	Remove
00:01:6C:06:A6:29	<input type="checkbox"/>

----End

5.1.4 Wireless bridge

5.1.4.1 Overview

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 wireless bridge as well.

Choose **Wireless > 2.4G > Wireless Bridge** to enter the configuration page.

Wireless -- Bridge

This page allows you to configure wireless bridge features of the wireless LAN interface. 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.

Bridge Restrict:

5.1.4.2 Configuration procedure

Step 1 Login to the web UI of V1200, choose **Wireless > 2.4G > Basic** to enter the configuration page to set the channel and bandwidth to the same with the upstream router.

SSID:	<input type="text" value="Tenda_F02910"/>	
BSSID:	50:2B:73:F0:29:11	
Wireless Mode:	<input type="text" value="802.11b/g/n Mixed"/>	
Country:	<input type="text" value="ALL"/>	
Channel:	<input type="text" value="Auto"/>	Current: 11 (interference: acceptable)
Bandwidth:	<input type="text" value="40MHz"/>	Current: 40MHz
Control Sideband:	<input type="text" value="Lower"/>	Current: Upper

Step 2 Choose **Wireless > 2.4G > Security** to set up the network authentication type and security key (if required) to the same with the upstream router.

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:	<input type="text" value="Tenda_F02910"/>
Network Authentication:	<input type="text" value="Open"/>
WEP Encryption:	<input type="text" value="Disabled"/>

Step 3 Choose **Wireless > 2.4G > Wireless Bridge** to access the configuration page set up wireless bridge.

1. Bridge Restrict: Select **Enabled(Scan)**. It displays the available WiFi network list automatically.

Wireless -- Bridge

This page allows you to configure wireless bridge features of the wireless LAN interface. 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.

Bridge Restrict:	<input type="text" value="Enabled(Scan)"/>
------------------	--

Remote Bridges MAC Address:

	SSID	BSSID
<input type="checkbox"/>	Tenda_888888	00:90:4c:88:88:89

2. Select the SSID you want to bridge, and click **Apply/Save**.

The screenshot shows a configuration window with the following elements:

- Bridge Restrict:** A dropdown menu set to "Enabled".
- Remote Bridges MAC Address:** A table with two rows and two columns. The first row contains the MAC address "50:2b:73:f0:27:51" in the first column and an empty box in the second. The second row contains two empty boxes.
- Buttons:** "Refresh" and "Apply/Save" buttons are located at the bottom right.

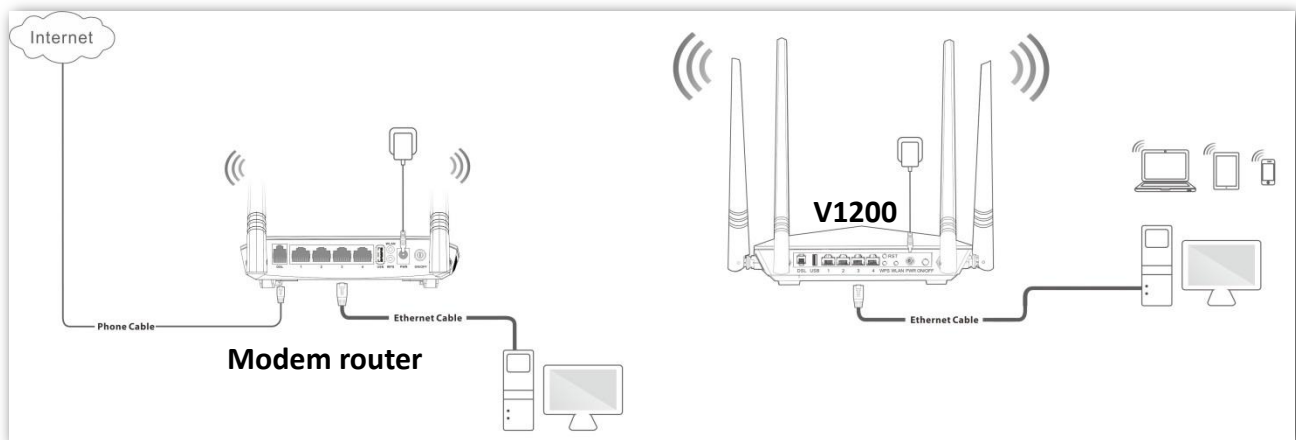
----End



Ensure both the channel and bandwidth are the same with the router you want to bridge. Otherwise, the SSID will not be shown in the list.

When you set up wireless bridge successfully, it can extend the wireless network of the upstream wireless router to provide both wired and wireless internet connection.

Network topology:



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

5.1.4.3 Example of configuring the wireless bridge function

Network requirement

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

Solution

To improve internet connectivity in the bedroom and study room, the user can add a V1200 modem router and configure the wireless bridge function of the router to extend the 2.4 GHz WiFi network coverage. That will eliminate blind areas in the apartment, enabling the user to access the internet anywhere in the apartment.

Assume that:

The upstream wireless router uses the following wireless settings for 2.4 GHz.

Parameter	Description
Wireless Network Name	Tenda_123456
Wireless Network Password	12345678
Wireless Encryption	Mixed WPA2/WPA-PSK, AES
Wireless Channel	6
Bandwidth	40MHz
LAN IP	192.168.1.10

Configuration procedure

Step 1 Configure V1200.

1. Change the wireless channel, encryption, and password to the same as those of the upstream router.
 - (1) Choose **Wireless > 2.4G > Basic** to enter the configuration page.
 - (2) Set **Channel** to **6**.
 - (3) Set **Bandwidth** to **40MHz**.
 - (4) Click **Apply/Save** on the bottom of this page.

SSID: Tenda_F02910
 BSSID: 50:2B:73:F0:29:11
 Wireless Mode: 802.11b/g/n Mixed
 Country: ALL
 Channel: 6 Current: 6 (interference: acceptable)
 Bandwidth: 40MHz Current: 40MHz
 Control Sideband: Upper Current: Upper

- (5) Choose **Wireless > 2.4G > Security** to enter the configuration page.
- (6) Set the **Network Authentication, WPA/WAPI Passphrase, and WPA/WAPI Encryption** to **Mixed WPA2/WPA-PSK, 12345678, and AES** respectively.
- (7) Click **Apply/Save** on the bottom of this page.

Select SSID: Tenda_F02910
 Network Authentication: Mixed WPA2/WPA -PSK
 WPA/WAPI passphrase: ●●●●●● [Click here to display](#)
 WPA/WAPI Encryption: AES
 Apply/Save

2 Configure the wireless bridge function.

- (1) Choose **Wireless > 2.4G > Wireless Bridge** to enter the configuration page.
- (2) Set the **Bridge Restrict** to **Enabled(Scan)**.
- (3) Select the SSID (wireless network name) of the upstream router which is **Tenda_123456** in this example.
- (4) Click **Apply/Save**.

Bridge Restrict: Enabled(Scan)

Remote Bridges MAC Address:

	SSID	BSSID
<input type="checkbox"/>	110hasa	c8:3a:35:f3:0f:f9
<input type="checkbox"/>	12345678	00:1a:3f:ed:04:99
<input type="checkbox"/>	ZYD ~ MW3	b4:0f:3b:d5:3a:91
<input checked="" type="checkbox"/>	Tenda_123456	c8:3a:35:84:3f:01

- (5) Click **Apply/Save**. **Bridge Restrict** turns to **Enabled**.

Bridge Restrict:

Remote Bridges MAC Address:

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

Step 2 Configure the upstream router. Perform the steps in [procedure 2](#).

----End

Verification

Connect your wireless devices to the WiFi network of the modem router, or connect your wired devices to ports 1, 2 or 3 of the modem router, and try accessing the internet in the bedroom and study room.

5.1.5 Station info

This section allows you to check the information of wireless clients connected to the 2.4 GHz wireless networks of the modem router.

Choose **Wireless > 2.4G > Station Info** to enter this page.

Wireless -- Authenticated Stations

This page shows authenticated wireless stations and their status.

MAC	Associated	Authorized	SSID	Interface

Click **Refresh** to view the latest wireless stations and their status.

5.2 5G

5.2.1 Basic

5.2.1.1 Overview

This section allows you to configure basic features of the wireless network of 5 GHz.

Choose **Wireless > 5G > 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 restrict the channel set based on country requirements. Click "Apply/Save" to configure the basic wireless options.

- Enable Wireless
- Hide Access Point
- Disable WMM Advertise
- Enable Wireless Multicast Forwarding (WMF)

SSID:

BSSID: C8:3A:35:14:4B:62

Wireless Mode:

Country:

Channel: Current:48

Bandwidth: Current:80MHz

Parameter description

Parameter	Description
Enable Wireless	Select the option to enable the wireless function.
Hide Access Point	Select the option to hide the SSID of the modem router. In this case, wireless clients cannot find the SSID (wireless network name) of the modem route. The SSID must be manually entered on the wireless clients for connecting the clients to the modem router.
Disable WMM Advertise	Select the option to disable WMM advertise of the modem router. WMM optimizes the communication experience of end-users, providing high-quality network connectivity performance for data, voice, music, and video applications in a complex network environment and communications environment.
Enable Wireless Multicast Forwarding (WMF)	Select the option to enable WMF of the modem router. Wireless multicast forwarding is a network data transmission method, which improves the efficiency of data transmission to effectively save network bandwidth and reduce network load.
SSID	Wireless network name of the modem router.

Parameter	Description
BSSID	MAC address of the wireless network.
Wireless Mode	<ul style="list-style-type: none"> • 802.11ac: If 802.11ac is selected, only 11ac wireless devices can connect to the wireless network. The maximum of 866 Mbps wireless rate is supported in this mode. • 802.11a/n/ac Mixed: If 802.11a/n/ac Mixed is selected, 11a, 11n or 11ac wireless devices can connect to the wireless network. The maximum of 866 Mbps wireless rate is supported in this mode.
Country	Select your country or region.
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.

5.2.1.2 Enabling multiple SSIDs

By setting up multiple SSIDs on a wireless modem router, the modem router can be deployed to multiple wireless networks, and users can connect to different wireless LANs to avoid interference with each other.

To enable multiple SSIDs:

- Step 1** Choose **Wireless > 5G > Basic** to enter the configuration page.
- Step 2** Select **Enable** option to enable the corresponding SSID.
- Step 3** Customize the name for the SSID if you want.
- Step 4** **Hidden:** It specifies whether to hide the SSID. If the option is selected, wireless devices cannot find the SSID.
- Step 5** **Disable WMM Advertise:** WMM (Wi-Fi Multimedia) is a Wi-Fi Alliance interoperability certification based on the IEEE 802.11e standard. Select it if you need to disable WMM advertise.
- Step 6** **WMF:** It specifies whether to forward multicast packets through unicast tunnels. Generally, multicast packets are transmitted at the lowest rate, such as 1 Mbps, leading to poor transmission efficiency. WMF leverages the auto-negotiated high rate, reliable feedback mechanism, and other advantages of unicast packets to address multicast problems such as video playback stalls caused by packet loss and long delays over a wireless network.
- Step 7** Click **Apply/Save**.

Wireless - Guest/Virtual Access Points:

Enabled	SSID	Hidden	Disable WMM Advertise	Enable WMF	Enable HSPOT
<input type="checkbox"/>	guest5G_1	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	N/A
<input type="checkbox"/>	guest5G_2	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	N/A
<input type="checkbox"/>	guest5G_3	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	N/A

----End

5.2.2 Security

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

Choose **Wireless > 5G > 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 both STA PIN and Authorized MAC are empty, PBC is used. If Hide Access Point enabled or Mac filter list is empty with "allow" chosen, WPS2 will be disabled

WPS Setup

EnableWPS

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:

Network Authentication:

WPA/WAPI passphrase: [Click here to display](#)

WPA/WAPI Encryption:

5.2.2.1 WPS setup

Wi-Fi Protected Setup makes it easy for home users who know little of wireless security to establish a home network, as well as to add new devices to an existing network without entering long passphrases or configuring complicated settings. They can set up network connections simply by entering a PIN code on the device web interface or pressing hardware WPS button (on the back panel of the device).

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

WPS Setup

Enable WPS Enabled ▾

Add Client (This feature is available only when WPA-PSK(WPS1), WPA2 PSK or OPEN mode is configured)

Use STA PIN Use AP PIN

Device PIN [Help](#)

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

Option 1: PBC negotiation

- Step 1** Choose **Wireless > 5G > 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 WPA-PSK(WPS1), WPA2 PSK or OPEN mode is configured)

Use STA PIN Use AP PIN

Device PIN [Help](#)

- Step 4** Press the WPS hardware button on the rear panel of the modem router for 3 seconds, and then release it. (The WPS LED indicator starts blinking)
 - Step 5** Within 2 minutes, enable the WPS negotiation function on your wireless device.
- End**

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

Option 2: Using the WPS PIN code of the wireless device

- Step 1** Log in to the web UI of the modem router, choose **Wireless > 5G > Security** to enter the configuration page.
- Step 2** Select **Enabled** to enable the function.
- Step 3** Click **Apply/Save** on the bottom of this page.
- Step 4** Select Enter STA PIN.
- Step 5** Check the WPS PIN code on your wireless device and enter it to the blank box on the WPS Setup page of the web UI.

Step 6 Click **Apply/Save**.

The screenshot shows the 'WPS Setup' configuration page. At the top, 'Enable WPS' is set to 'Enabled'. Below this, there is a section for 'Add Client' with a note: '(This feature is available only when WPA-PSK(WPS1), WPA2 PSK or OPEN mode is configured)'. Underneath, 'Use STA PIN' is selected with a radio button, and 'Use AP PIN' is unselected. A text input field for the PIN is empty. At the bottom, 'Device PIN' is set to '31192668'. There are 'Help' links next to the radio buttons and the Device PIN field.

----End

The WPS LED indicator blinks for about 2 minutes, and then turns to solid green. It indicates that the wireless device is connected to the modem router, and the wireless network is encrypted.

Option 3: Using the WPS PIN code of the modem router

Step 1 Log in to the web UI of the modem router, choose **Wireless > 5G > 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**.

The screenshot shows the 'WPS Setup' configuration page. 'Enable WPS' is set to 'Enabled'. The 'Add Client' section has a note: '(This feature is available only when WPA-PSK(WPS1), WPA2 PSK or OPEN mode is configured)'. Underneath, 'Use STA PIN' is unselected and 'Use AP PIN' is selected with a radio button. A text input field for the PIN contains '44371319'. At the bottom, 'Device PIN' is set to '44371319'. There are 'Help' links next to the radio buttons and the Device PIN field.

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

----End

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

5.2.2.2 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:

Network Authentication:

WEP Encryption:

Open/Shared

Open/Shared supports WEP encryption.

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

Select SSID:

Network Authentication:

Encryption Strength:

Current Network Key:

Network Key 1:

Network Key 2:

Network Key 3:

Network Key 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

Parameter description

Parameter	Description
Encryption Strength	Select 128-bit or 64-bit according to your needs.
Current Network Key	Select a network key to be used.
Network Key 1/2/3/4	Enter 13 ASCII characters or 26 hexadecimal digits as a 128-bit encryption key; enter 5 ASCII characters or 10 hexadecimal digits as a 64-bit encryption keys.

WPA2 Enterprise

Parameter description

Parameter	Description
WPA2 Enterprise	Security modes implemented based on the IEEE 802.1x, which requires the third-party RADIUS server for authentication.
Network Re-auth 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 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.
RADIUS Server2 Address	It specifies the IP address of the secondary RADIUS server for authentication.
WPA/WAPI Encryption	<p>It specifies an algorithm for WPA2 enterprise encryption.</p> <ul style="list-style-type: none"> • AES: If it is selected, AES enabled wireless clients can join your wireless network. • TKIP+AES: If it is 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_5G_F02910 ▼

Network Authentication: WPA -PSK ▼

WPA/WAPI passphrase: ***** [Click here to display](#)

WPA/WAPI Encryption: AES ▼

Apply/Save

Parameter description

Parameter	Description
WPA-PSK/WPA2-PSK/ Mixed WPA-PSK/WPA2-PSK	They specify the security modes implemented based on a shared key.
WPA/WAPI Passphrase	It specifies the password of the wireless network.
WPA/WAPI Encryption	It specifies an algorithm for WPA encryption. <ul style="list-style-type: none">• AES: If it is selected, the maximum wireless speed can reach 300Mbps.• TKIP+AES: If it is selected, both AES and TKIP enabled wireless clients can join your wireless network.

5.2.3 MAC filter

5.2.3.1 Overview

The MAC-based wireless access control feature can be used to allow or disallow clients to connect to your 5 GHz wireless networks.

Choose **Wireless > 5G > MAC Filter** to enter the configuration page.

Wireless -- MAC Filter

Select SSID: Tenda_5G_144B60 ▼

MAC Restrict Mode: Disabled Allow Deny Note: If 'allow' is choosed and mac filter is empty, WPS will be disabled

MAC Address Remove

Add Remove

Parameter description

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

5.2.3.2 Adding a MAC filter rule

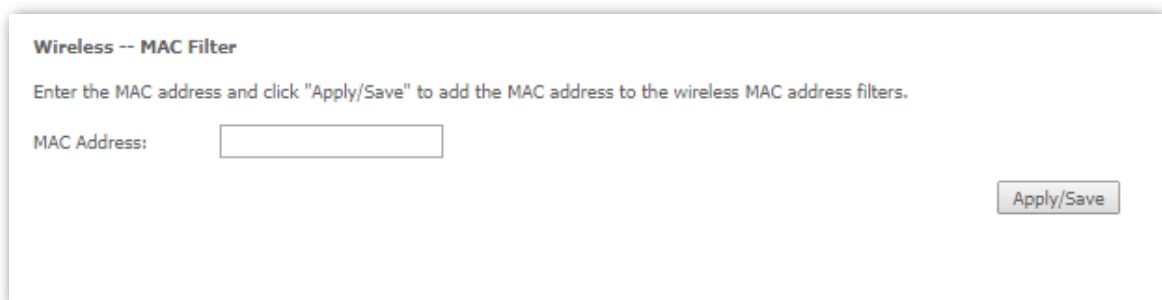
Step 1 Choose **Wireless > 5G > MAC Filter** to enter the configuration page.

Step 2 Select a SSID to apply the rule if you enable multiple SSIDs.

Step 3 Click **Add**.

Step 4 Enter the MAC address of the device to which the rule applies.

Step 5 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.

MAC Address:

Apply/Save

Step 6 Select **Allow** or **Deny** according to your needs.

Wireless -- MAC Filter

Select SSID: Tenda_5G_F02910 ▼

MAC Restrict Mode: Disabled Allow Deny

Note: If 'allow' is choosed and mac filter is empty, WPS will be disabled

MAC Address	Remove
00:01:6C:06:A6:29	<input type="checkbox"/>

Add Remove

----End

5.2.4 Wireless bridge

5.2.4.1 Overview

This section allows you to configure wireless bridge function of the modem router for 5 GHz. The function requires that the upstream wireless router supports wireless bridge for 5 GHz as well.

Choose **Wireless > 5G > Wireless Bridge** to enter the configuration page.

Wireless -- Bridge

This page allows you to configure wireless bridge features of the wireless LAN interface. 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.

Bridge Restrict: Disabled ▼

Refresh Apply/Save

5.2.4.2 Configuration procedure

Step 1 Login to the web UI of V1200, choose **Wireless > 5G > Basic** to enter the configuration page, and set channel and bandwidth to the same with the upstream router.

SSID:	<input type="text" value="Tenda_F02910"/>	
BSSID:	50:2B:73:F0:29:11	
Wireless Mode:	<input type="text" value="802.11b/g/n Mixed"/>	
Country:	<input type="text" value="ALL"/>	
Channel:	<input type="text" value="Auto"/>	Current: 11 (interference: acceptable)
Bandwidth:	<input type="text" value="40MHz"/>	Current: 40MHz
Control Sideband:	<input type="text" value="Lower"/>	Current: Upper

Step 2 Choose **Wireless > 5G > Security** to set up the security information, and set the network authentication type to the same with the upstream router.

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:

Network Authentication:

WEP Encryption:

Step 3 Choose **Wireless > 5G > Wireless Bridge** to access the configuration page set up wireless bridge.

- 1. Bridge Restrict:** Select **Enabled(Scan)**. It displays the available WiFi network list automatically.

Wireless -- Bridge

This page allows you to configure wireless bridge features of the wireless LAN interface. 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.

Bridge Restrict:

Remote Bridges MAC Address:

	SSID	BSSID
<input type="checkbox"/>		c8:3a:38:18:06:e7
<input type="checkbox"/>	Tenda_5G_144E10	c8:3a:35:14:4e:12
<input type="checkbox"/>		c8:3a:38:18:06:e6
<input type="checkbox"/>		c8:3a:38:18:06:e5
<input type="checkbox"/>	000888888	c8:3a:35:84:18:69
<input type="checkbox"/>	Tenda_F13090	50:2b:73:f1:30:95

- 2.** Select the SSID you want to bridge, and click **Apply/Save**.

Bridge Restrict:

Remote Bridges MAC Address:

3. **Bridge Restrict** turns to **Enabled** automatically, click **Apply/Save**.

----End



TIP
Ensure the channel and bandwidth are the same with the router you want to bridge. Otherwise, the SSID (wireless network name) will not show in the list.

5.2.4.3 Example of configuring the wireless bridge function

Network requirement

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

Solution

To improve internet connectivity in the bedroom and study room, the user can add a V1200 modem router and configure the wireless bridge function of the router to extend the 5 GHz WiFi network coverage. That will eliminate blind areas in the apartment, enabling the user to access the internet anywhere in the apartment.

Assume that:

The upstream wireless router uses the following wireless settings for 5 GHz.

Parameter	Description
Wireless Network Name	Tenda_5G_123456
Wireless Network Password	12345678
Wireless Encryption	Mixed WPA2/WPA-PSK, AES
Wireless Channel	149

Parameter	Description
Bandwidth	80MHz
LAN IP	192.168.1.10

Configuration procedure

Step 1 Configure V1200.

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

- (1) Choose **Wireless > 5G > Basic** to enter the configuration page.
- (2) Set **Channel** to **149**.
- (3) Set **Bandwidth** to **80MHz**.
- (4) Click **Apply/Save** on the bottom of this page.

SSID:
 BSSID: 50:2B:73:F0:29:12
 Wireless Mode: ▼
 Country: ▼
 Channel: ▼ Current: 149
 Bandwidth: ▼ Current: 80MHz

- (5) Choose **Wireless > 5G > Security** to enter the configuration page.
- (6) Set the **Network Authentication**, **WPA/WAPI Passphrase**, and **WPA/WAPI Encryption** to **Mixed WPA2/WPA-PSK**, **12345678**, and **AES** respectively.
- (7) Click **Apply/Save** on the bottom of this page.

Select SSID: ▼
 Network Authentication: ▼
 WPA/WAPI passphrase: [Click here to display](#)
 WPA/WAPI Encryption: ▼

2 Configure the wireless bridge function.

- (1) Choose **Wireless > 5G > Wireless Bridge** to enter the configuration page.
- (2) Set the **Bridge Restrict** to **Enabled(Scan)**.
- (3) Select the SSID (wireless network name) of the upstream router which is **Tenda_5G_123456** in this example.

Bridge Restrict: Enabled(Scan) ▼

Remote Bridges MAC Address:

	SSID	BSSID
<input type="checkbox"/>	Sunrise-Finance_5G	b8:08:d7:4f:ba:58
<input type="checkbox"/>	AC9-lhy-5G	00:90:4c:88:88:8d
<input type="checkbox"/>	1111Tenda_1C3590_5G	b4:0f:3b:1c:35:95
<input type="checkbox"/>	CMCC-Achy-5G	18:69:da:96:ca:4f
<input type="checkbox"/>	G5528X-2	50:2b:73:82:60:c9
<input type="checkbox"/>	CH149-3	c8:3a:35:f9:0e:71
<input type="checkbox"/>	CH149-4	c8:3a:35:84:4c:c1
<input type="checkbox"/>	CH149-3	c8:3a:35:21:20:86
<input type="checkbox"/>	CH149-2	c8:3a:35:00:22:e1
<input type="checkbox"/>	CH149-2	c8:3a:35:21:20:72
<input checked="" type="checkbox"/>	Tenda_5G_123456	c8:3a:35:84:3f:05

(4) Click **Apply/Save**, Bridge Restrict turns to **Enabled** automatically.

Bridge Restrict: Enabled ▼

Remote Bridges MAC Address:

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

Step 2 Configure the upstream router. Perform the steps in [procedure 2](#).

----End

Verification

Connect your wireless devices to the WiFi network of the modem router, or connect your wired devices to ports 1, 2 or 3 of the modem router, and try accessing the internet in the bedroom and study room.

5.2.5 Station info

This section allows you to check the information of wireless clients connected to the 5 GHz wireless networks of the modem router.

Choose **Wireless > 5G > Station Info** to enter this page.

Wireless -- Authenticated Stations

This page shows authenticated wireless stations and their status.

MAC	Associated	Authorized	SSID	Interface
1C:5C:F2:B4:40:08	Yes	Yes	Tenda_5G_144B60	w1

Click **Refresh** to view the latest wireless stations and their status.

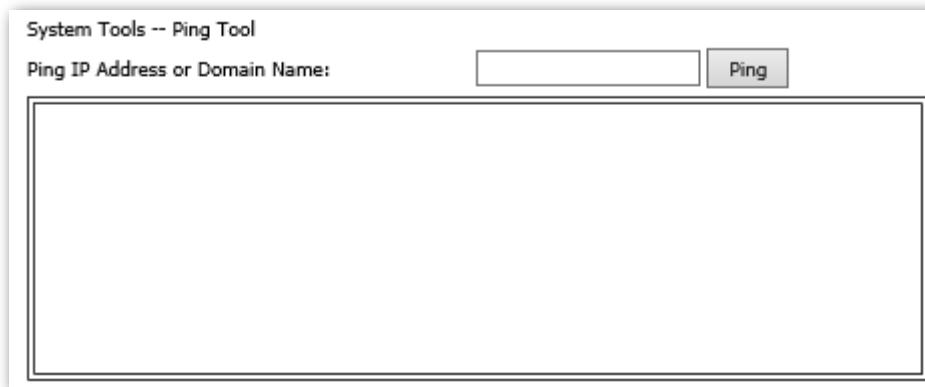
6 Diagnostics

6.1 Ping

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

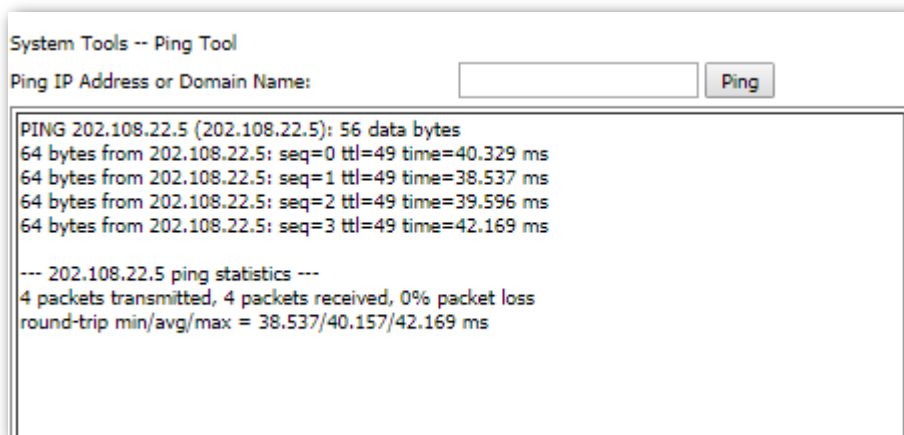
To perform the ping test:

- Step 1** Choose **Diagnostics > Ping** to enter the configuration page.
- Step 2** Enter the IP address or domain name of the host in the **Ping IP Address or Domain Name** field.
- Step 3** Click **Ping**.



----End

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

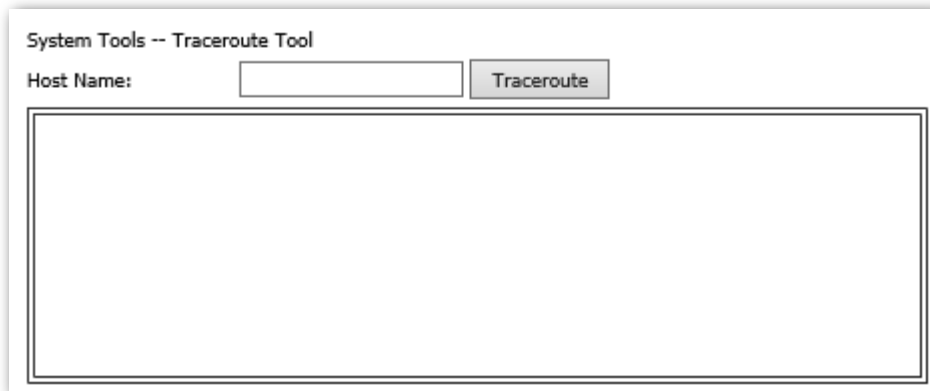


6.2 Traceroute

Traceroute helps you check the specific routes to a host.

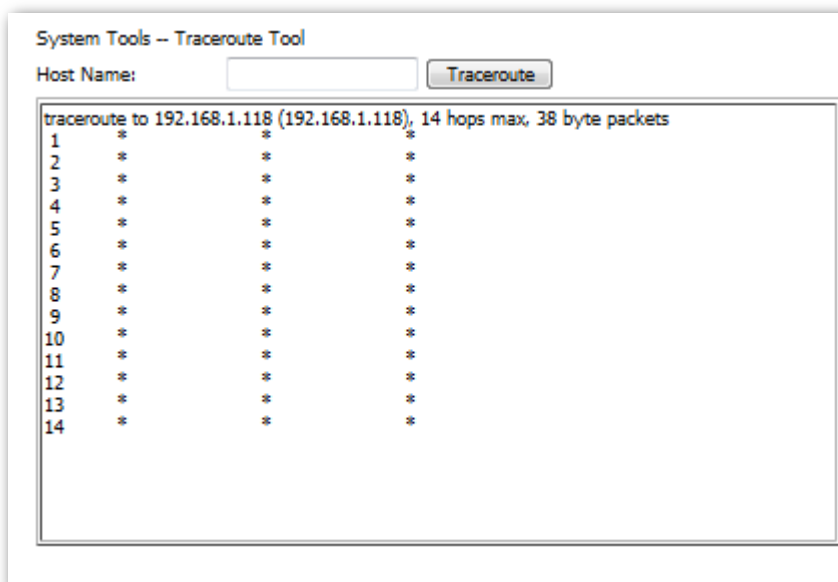
To perform the traceroute:

- Step 1** Choose **Diagnostics > Traceroute** to enter the configuration page.
- Step 2** Enter the IP address or domain name of the host in the **Host Name** field.
- Step 3** Click **Traceroute**.



----End

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



```
tracert to 192.168.1.118 (192.168.1.118), 14 hops max, 38 byte packets
 1  *          *          *
 2  *          *          *
 3  *          *          *
 4  *          *          *
 5  *          *          *
 6  *          *          *
 7  *          *          *
 8  *          *          *
 9  *          *          *
10  *          *          *
11  *          *          *
12  *          *          *
13  *          *          *
14  *          *          *
```



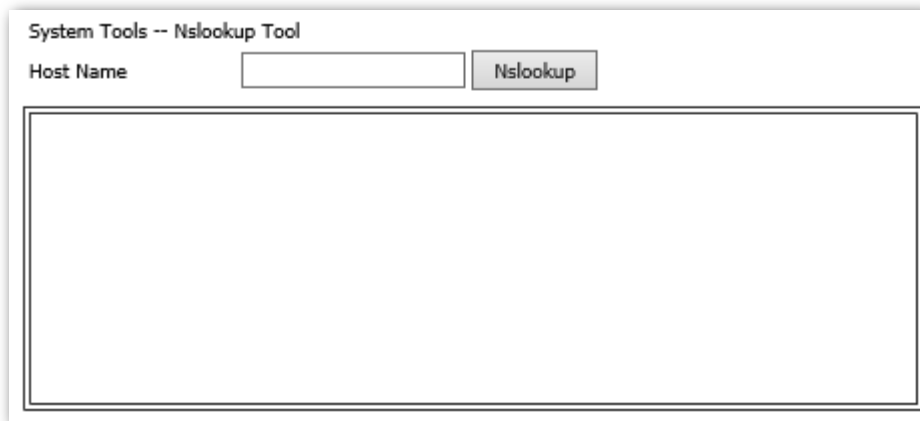
If the host is unreachable, the route table is blank.

6.3 Nslookup

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

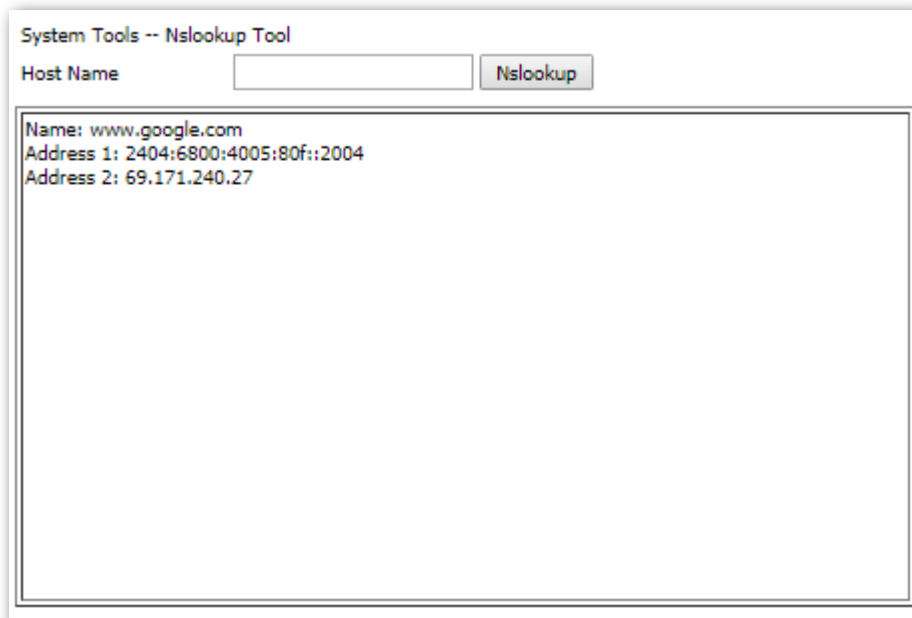
To translate a domain name:

- Step 1** Choose **Diagnostics > Nslookup** to enter the configuration page.
- Step 2** Enter a domain name in the **Host Name** field.
- Step 3** Click **Nslookup**.



----End

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



6.4 Diagnostics

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

ipoe_eth3Diagnostics

Your modem is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.

Test the connection to your local network

Test your LAN1 Connection:	FAIL	Help
Test your LAN2 Connection:	PASS	Help
Test your LAN3 Connection:	FAIL	Help
Test your 2.4G Wireless Connection:	PASS	Help
Test your 5G Wireless Connection:	PASS	Help

Test the connection to your DSL service provider

Test xDSL Synchronization:	FAIL	Help
Test ATM OAM F5 segment ping:	DISABLED	Help
Test ATM OAM F5 end-to-end ping:	DISABLED	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 Settings

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

7.1.1 Backup

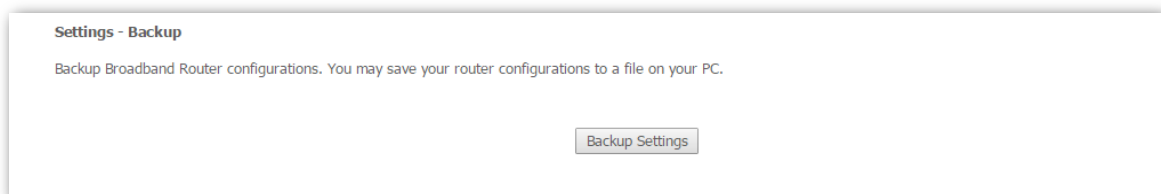
7.1.1.1 Overview

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

7.1.1.2 Backing up the settings

Step 1 Choose **Management > Settings > Backup** to access the configuration page.

Step 2 Click **Backup Settings**.



----End

7.1.2 Restore backup

7.1.2.1 Overview

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

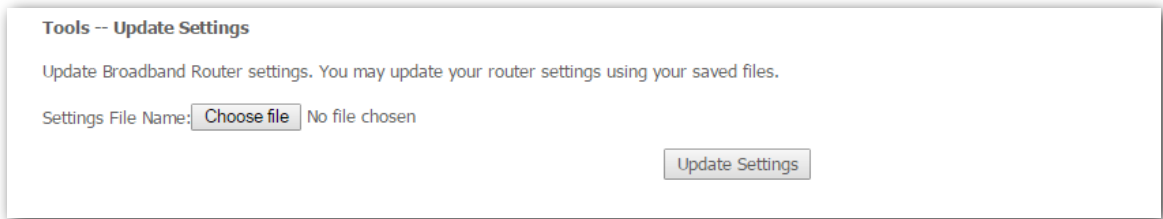
7.1.2.2 Restoring the settings

Step 1 Choose **Management > Settings > Restore Backup** to access the configuration page.

Step 2 Click **Choose File**.

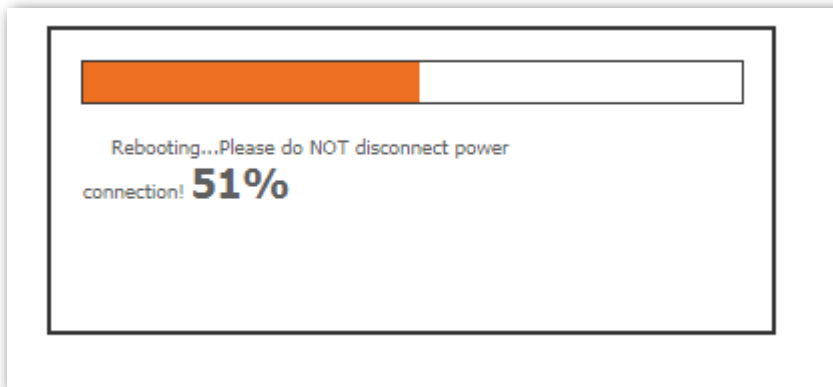
Step 3 Select a configuration file on your computer.

Step 4 Click **Update Settings**.



----End

Wait until the progress bar elapses.



7.1.3 Restore default

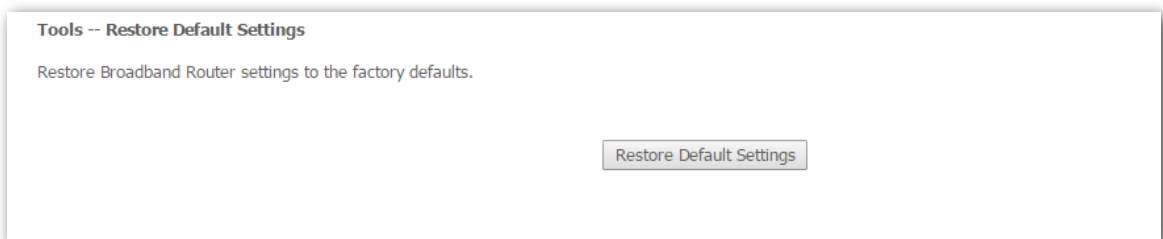
7.1.3.1 Overview

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

7.1.3.2 Restoring default settings

Step 1 Choose **Management > Setting > Restore Default** to access the configuration page.

Step 2 Click **Restore Default Settings**.



Step 3 Click **OK**.

192.168.1.1 says

Are you sure you want to restore factory default settings?

OK

Cancel

----End

7.2 System log

7.2.1 Overview

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

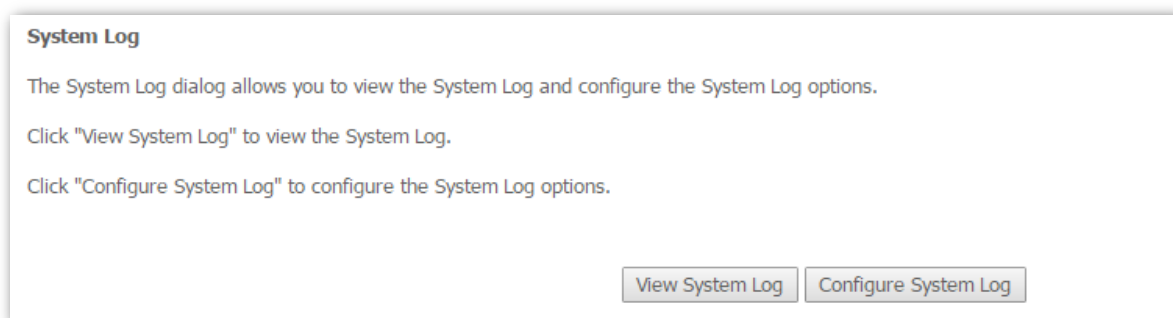
7.2.2 Viewing system logs



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

Step 1 Choose **Management > System Log** to enter the configuration page.

Step 2 Click **View System Log**.



----End

System Log			
Date/Time	Facility	Severity	Message
Oct 15 11:10:32	kern	crit	kernel: eth4 (Int switch port: 4) (Logical Port: 4) Link UP 0 mbps half duplex
Oct 15 11:10:32	kern	crit	kernel: eth5 (Int switch port: 6) (Logical Port: 6) Link UP 0 mbps half duplex
Oct 15 11:10:32	kern	err	kernel: ddos_log_tg_init.
Oct 15 11:10:32	kern	err	kernel: /proc/ddoshost/ddoshostlist create successfully.
Oct 15 11:10:32	kern	crit	kernel: eth3 (Int switch port: 3) (Logical Port: 3) Link UP 1000 mbps full duplex
Oct 15 11:10:32	kern	crit	kernel: eth2 (Int switch port: 2) (Logical Port: 2) Link UP 100 mbps full duplex
Oct 15 11:10:32	kern	crit	kernel: eth2 (Int switch port: 2) (Logical Port: 2) Link DOWN.
Oct 15 11:10:32	kern	crit	kernel: eth3 (Int switch port: 3) (Logical Port: 3) Link DOWN.
Oct 15 11:10:32	kern	crit	kernel: eth3 (Int switch port: 3) (Logical Port: 3) Link UP 1000 mbps full duplex
Oct 15 11:10:32	kern	crit	kernel: eth2 (Int switch port: 2) (Logical Port: 2) Link UP 100 mbps full duplex
Oct 15 11:10:32	kern	crit	kernel: eth2 (Int switch port: 2) (Logical Port: 2) Link DOWN.
Oct 15 11:10:32	kern	crit	kernel: eth1 (Int switch port: 1) (Logical Port: 1) Link UP 100 mbps full duplex
Oct 15 11:10:32	kern	crit	kernel: eth1 (Int switch port: 1) (Logical Port: 1) Link DOWN.
Oct 15 11:10:32	kern	crit	kernel: eth1 (Int switch port: 1) (Logical Port: 1) Link UP 10 mbps full duplex
Oct 15 11:10:32	kern	crit	kernel: Line 0: ADSL G.992 started
Oct 15 11:10:32	kern	crit	kernel: Line 0: xDSL link down
Oct 15 11:10:32	kern	crit	kernel: eth1 (Int switch port: 1) (Logical Port: 1) Link DOWN.
Oct 15 11:10:32	kern	crit	kernel: eth1 (Int switch port: 1) (Logical Port: 1) Link UP 100 mbps full duplex
Oct 15 11:10:32	kern	crit	kernel: eth1 (Int switch port: 1) (Logical Port: 1) Link DOWN.
Oct 15 11:10:32	kern	crit	kernel: eth1 (Int switch port: 1) (Logical Port: 1) Link UP 100 mbps full duplex
Oct 15 11:10:32	kern	crit	kernel: eth1 (Int switch port: 1) (Logical Port: 1) Link DOWN.
Oct 15 11:10:32	kern	crit	kernel: eth1 (Int switch port: 1) (Logical Port: 1) Link UP 100 mbps full duplex
Oct 15 11:10:32	kern	crit	kernel: eth1 (Int switch port: 1) (Logical Port: 1) Link DOWN.
Oct 15 11:10:32	kern	crit	kernel: eth2 (Int switch port: 2) (Logical Port: 2) Link UP 100 mbps full duplex
Oct 15 11:10:32	kern	crit	kernel: eth1 (Int switch port: 1) (Logical Port: 1) Link UP 100 mbps full duplex
Oct 15 11:10:32	kern	crit	kernel: eth2 (Int switch port: 2) (Logical Port: 2) Link DOWN.

On the page that appears:

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

7.2.3 Configuring system logs

Step 1 Choose **Management > System Log** to access the configuration page.

Step 2 Click **Configure System Log**.

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.

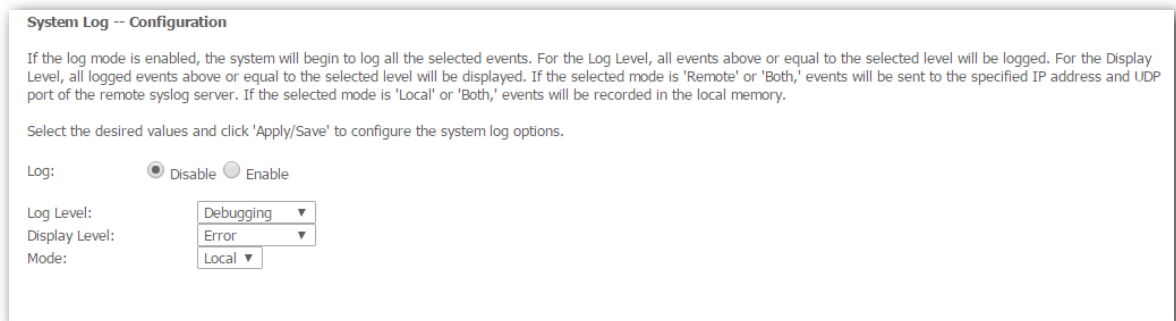
Click "Configure System Log" to configure the System Log options.

Step 3 Set **Log** to **Enable**.

Step 4 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 5 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 6 Click **Apply/Save**.



The screenshot shows a dialog box titled "System Log -- Configuration". It contains the following text and controls:

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. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.

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

Log: Disable Enable

Log Level:

Display Level:

Mode:

----End

Choose **Management > System Log > View System Log** to check the logs.

7.3 Passwords

7.3.1 Overview

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

7.3.2 Changing the login password

- Step 1** Choose **Management > Passwords** to access the configuration page.
- Step 2** Set **User Name** to the current user name, such as the user name **admin**.
- Step 3** Set **Old Password** to the current password, such as the default password of the administrator account **admin**.
- Step 4** Set **New Password** to the new password consisting of 1 to 16 letters, digits, or underscores, such as **admin1**.
- Step 5** Set Confirm Password to the same value as New Password.
- Step 6** Click **Apply/Save**.

Access Control -- Passwords

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

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

The user name "support" is used to allow an ISP technician to access your Broadband Router for maintenance and to run diagnostics.

The user name "user" can access the Broadband Router, view configuration settings and statistics, as well as, update the router's software.

Use the fields below to enter up to 16 characters and click "Apply/Save" to change or create passwords. Note: Password cannot contain a space.

User Name:

Old Password:

New Password:

Confirm Password:

----End

7.4 SNMP agent

7.4.1 Overview

The Simple Network Management Protocol (SNMP) is the most widely used network management protocol in TCP/IP networks. SNMP enables you to remotely manage all your network devices compliant with this protocol, such as monitoring the network status, changing network device settings, and receive network event alarms.

SNMP allows automatic management of devices from various vendors regardless of physical differences among the devices.

SNMP Management Framework

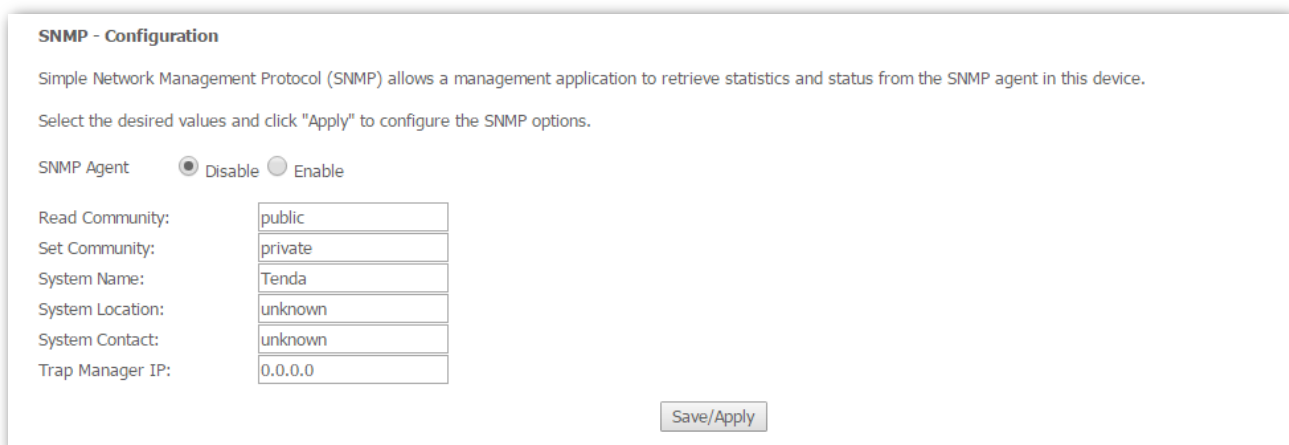
The SNMP management framework consists of SNMP manager, SNMP agent, and Management Information Base (MIB).

- **SNMP manager:** It is a system that controls and monitors network nodes using the SNMP protocol. The SNMP manager most widely used in network environments is Network Management System (NMS). An NMS can be a dedicated network management server, or an application that implements management functions in a network device.
- **SNMP agent:** It is a software module in a managed device. The module is used to manage data about the device and report the management data to an SNMP manager.
- **MIB:** It is a collection of managed objects. It defines a series of attributes of managed objects, including names, access permissions, and data types of objects. Each SNMP agent has its MIB. An SNMP manager can read and/or write objects in the MIB based on the permissions assigned to the SNMP manager.

An SNMP manager manages SNMP agents in an SNMP network. The SNMP manager exchanges management information with the SNMP agents using the SNMP protocol.

Parameter description

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" to configure the SNMP options.

SNMP Agent Disable Enable

Read Community:	<input type="text" value="public"/>
Set Community:	<input type="text" value="private"/>
System Name:	<input type="text" value="Tenda"/>
System Location:	<input type="text" value="unknown"/>
System Contact:	<input type="text" value="unknown"/>
Trap Manager IP:	<input type="text" value="0.0.0.0"/>

Parameter	Description
SNMP Agent	It specifies whether to enable the SNMP agent function of the modem router. By default, it is disabled.
Read Community	It specifies the read password shared between SNMP managers and this SNMP agent. The default password is public .
Set Community	It specifies the set password shared between SNMP managers and this SNMP agent. The default password is private .
System Name	It specifies the device name of the modem router. The default system name is the brand of the modem router.
System Location	It specifies the location where the modem router is used. The default location is unknown .
System Contact	It specifies the contact information of the modem router. The default location is unknown .
Trap Manager IP	It specifies the IP address of the server or terminal where alarm information is sent to.

7.4.2 Configuring the SNMP agent

- Step 1** Choose **Management > SNMP Agent** to access the configuration page.
 - Step 2** Set **SNMP Agent** to **Enable**.
 - Step 3** Set **Read Community** to the password for reading data. The default value is public.
 - Step 4** Set **Set Community** to the password for writing data. The default value is private.
 - Step 5** Set **System Name** to the name of the modem router.
 - Step 6** Set **System Location** to the location of the modem router.
 - Step 7** Set **System Contact** to the contact information of the modem router.
 - Step 8** Set **Trap Manager IP** to the IP address of the Trap Manager.
 - Step 9** Click **Apply/Save**.
- End

7.5 TR-069 client

7.5.1 Overview

The WAN Management Protocol (TR-069) allows an Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to the modem router from the internet.

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:

ACS URL:

ACS User Name:

ACS Password:

WAN Interface used by TR-069 client:

Display SOAP messages on serial console Disable Enable

Connection Request Authentication

Connection Request User Name:

Connection Request Password:

Connection Request URL:

Parameter description

Parameter	Description
Inform Interval	It specifies the interval at which the CPE uses the inform method to send messages to the ACS.
ACS URL	It specifies the domain name of the ACS.
ACS User Name	It specifies the user name used to authenticate the CPE when the CPE connects to the ACS using the TR-069 protocol.
ACS Password	It specifies the password used to authenticate the CPE when the CPE connects to the ACS using the TR-069 protocol.
WAN Interface used by TR-069 client	It specifies the interface used by the TR-069 client in WAN side.
Display SOAP messages on serial console	It specifies whether to display the TR-069 SOAP messages on the serial port. This function is generally used to debug by professionals. After it is enabled, some memory will be consumed which causes performance degradation. So generally it is disabled.

Parameter	Description
Connection Request Authentication	It specifies whether to authenticate the connection request sent by the ACS.
Connection Request User Name	It specifies the user name used to authenticate the ACS when it sends the connection request to the CPE.
Connection Request Password	It specifies the password used to authenticate the ACS when it sends the connection request to the CPE.
Connection Request URL	It specifies the domain name used by the ACS when it sends the connection request to the CPE. After the WAN port used by the TR-069 client is selected, this domain name will be generated automatically.

7.5.2 Configuring the TR-069 Client

Step 1 Choose **Management > TR-069 Client** to enter the configuration page.

Step 2 Set **Inform** to **Enable**. By default, it is disabled.

Step 3 Set **Inform Interval** to the interval at which inform packets are sent.

Step 4 Set **ACS URL** to the URL of the ACS.

Step 5 Set **ACS User Name** to the user name of the ACS.

Step 6 Set **ACS Password** to the password of the ACS.

Step 7 Select the WAN port used by the TR-069 client from the **WAN Interface used by TR-069 client** drop-down list box.

Step 8 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 9 Select **Connection Request Authentication** if connection request authentication is required.

If it is selected, perform the following steps:

1. Set **Connection Request User Name** to the user name for connection request authentication.
2. Set **Connection Request Password** to the password for connection request authentication.
3. The **Connection Request URL** will be automatically generated after the WAN interface used by the TR-069 client is selected.

Step 10 Click **Apply/Save**.

----End



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

7.6 Internet time

7.6.1 Overview

This function allows you to synchronize the time of the device with the internet time.

7.6.2 Synchronizing the system time with the internet

- Step 1** Choose **Management > Internet Time** to access the configuration page.
- Step 2** Select **Automatically synchronize with Internet time servers**.
- Step 3** Set **First/Second/Third/Fourth/Fifth NTP time server** to the first/second/third/fourth/fifth time server with which the device time is synchronized.
- Step 4** Select your time zone from the **Time zone offset** drop-down list box.
- Step 5** Click **Apply/Save**.

Time settings

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

Automatically synchronize with Internet time servers

First NTP time server:	time.cachetworks.com ▼	
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 ▼

Apply/Save

----End

7.7 Access control

This function allows you to use the HTTP, ICMP, SSH, TELNET, SNMP, FTP, TFTP and HTTPS to manage the modem router from LAN or WAN side.

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	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	80
ICMP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	
SSH	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	22
TELNET	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	23
SNMP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	161
FTP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	21
TFTP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	69
HTTPS	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	443

Parameter description

Parameter	Description
HTTP	After it is enabled, users can manage the modem router using HTTP protocol through the browser from the corresponding sides (LAN or WAN). This method is acceptable for most users.
ICMP	After it is enabled, it allows users to ping the modem router from the corresponding sides (LAN or WAN) for connectivity diagnosis.
SSH	After it is enabled, users can manage the modem router through the Secure Shell connection (SSH).
TELNET	After it is enabled, users can use TELNET to establish a connection with the device, and visit the command-line interface of the device from the corresponding sides (LAN or WAN).
SNMP	After it is enabled, the SNMP management software can establish a connection with the device, and check some parameters of the device through MIB nodes from the corresponding sides (LAN or WAN).
FTP	After it is enabled, the modem router servers as a server and users can use FTP protocol to check, upload, or download files of the device from the corresponding sides (LAN or WAN).

Parameter	Description
TFTP	After it is enabled, the device servers as a server and users can use TFTP protocol to check, upload, or download files of the device from the corresponding sides (LAN or WAN).
HTTPS	After it is enabled, users can manage the device using HTTPS protocol through the browser from the corresponding sides (LAN or WAN).

7.8 Update software

7.8.1 Overview

This function allows you to upgrade the firmware of the device locally, using FTP, or using TFTP for better and more stable performance.

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

Tools -- Update Software

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

Step 2: Enter the path to the image file location in the box below or click the Browse button to locate the image file.

Step 3: Click the "Update Software" 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: No file chosen **Current Version:** V53.2.0.4_en_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]

7.8.2 Upgrading the firmware locally

- Step 1** Choose **Management > Update Software** to access the configuration page.
- Step 2** Click **Choose File**.
- Step 3** Select the firmware downloaded from the Tenda official website to your computer.
- Step 4** Click **Update Firmware**.

Tools -- Update Software

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

Step 2: Enter the path to the image file location in the box below or click the Browse button to locate the image file.

Step 3: Click the "Update Software" 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: No file chosen **Current Version:** V53.2.0.1_en_TDE01

Step 5 Click **OK**.

192.168.1.1 says

Are you sure to upgrade software?

----End

7.8.3 Upgrading the firmware using FTP server

- Step 1** Choose **Management > Update Software** to access the configuration page.
- Step 2** Set **FTP Server IP** to the IP address of the FTP server where the target firmware resides.
- Step 3** Set **Port** to the port number of the FTP server.
- Step 4** Set **User Name** to the user name for logging in to the FTP server.
- Step 5** Set **Password** to the password for logging in to the FTP server.
- Step 6** Set **Firmware File Name** to the file name of the target firmware.
- Step 7** Click **FTP Update Firmware**.

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]

----End



Ensure that the route between the modem router and the FTP server is reachable.

7.8.4 Upgrading the firmware using TFTP server

- Step 1** Choose **Management > Update Software** to access the configuration page.
- Step 2** Set **TFTP Server IP** to the IP address of the TFTP server where the target firmware resides.
- Step 3** Set **Firmware File Name** to the file name of the target firmware.
- Step 4** Click **TFTP Update Firmware**.

TFTP Firmware Update

TFTP Server IP: [eg:192.168.1.1]

Firmware File Name: [1-127]

----End

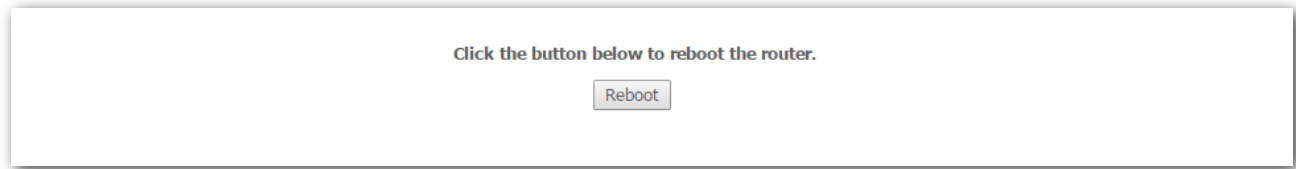


TIP Ensure that the route between the modem router and the TFTP server is reachable.

7.9 Reboot

This function allows you to manually reboot the device on the web UI.

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



To manually reboot the device, click **Reboot**, and then wait for the modem router to restart.

Appendix

A.1 FAQ

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

A1: Use the following method to troubleshoot the fault, and then try again.

- Ensure that the Ethernet cable between your computer and the modem router is connected properly.
- Ensure that your computer is set to **Obtain an IP address automatically**.
- Ensure that the login IP address (192.168.1.1) you entered is correct.
- Clear cache of your browser, or change another browser.
- Use another computer, smart phone or tablet to log in to the web UI.
- Hold down the **RST** button for about 6 seconds to restore to factory settings.

Q2: I cannot access the internet after completing the configuration, what should I do?

A2: Use the following method to troubleshoot the fault.

- Observe the **DSL** LED indicator. If it doesn't light up, check whether the connection between the DSL port and Phone jack is proper.

If you access the internet via the WAN port (port 4) of the modem router, check whether the connection between port 4 and the upstream device or Ethernet jack is proper.
- Observe the **INET** LED indicator. If it lights red, check whether the parameters you entered for internet access are correct, and the connection status on the web UI of the modem router is connected.
- Check whether your computers are set to **Obtain an IP address automatically**.
- 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.

- Log in to the web UI of the modem router, and check it on the **Wireless Settings** part.
- If you forget the login password of the web UI as well, reset the modem router. By default, there is no WiFi password.

Q4: How to reset the modem router?

A4: When the **PWR** LED indicator is solid green, hold down the **RST** button for 6 seconds.

A.2 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/Region	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

Country/Region	ISP	VPI	VCI	Encapsulation
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

Country/Region	ISP	VPI	VCI	Encapsulation
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

Country/Region	ISP	VPI	VCI	Encapsulation
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

Country/Region	ISP	VPI	VCI	Encapsulation
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

Country/Region	ISP	VPI	VCI	Encapsulation
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

Country/Region	ISP	VPI	VCI	Encapsulation
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

Country/Region	ISP	VPI	VCI	Encapsulation
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

Country/Region	ISP	VPI	VCI	Encapsulation
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	GWl	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

Country/Region	ISP	VPI	VCI	Encapsulation
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

Country/Region	ISP	VPI	VCI	Encapsulation
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

A.3 VLAN List

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

Country/Region	ISP	VLANID	Protocol
	Other		
Austria	Telekom	7	PPPoE
	Other		
Bahrain	VDSL	Disabled	PPPoE
	Other		
Balize	VDSL	Disabled	PPPoE
	Other		
Belgium	VDSL	Disabled	PPPoE
	Other		
Bengal	VDSL	Disabled	PPPoE
	Other		
Bolivia	VDSL	Disabled	PPPoE
	Other		
Brazil	VDSL	Disabled	PPPoE
	Other		
Cameroon	VDSL	Disabled	PPPoE
	Other		
Canada	VDSL	Disabled	PPPoE
	Other		
Chile	VDSL	Disabled	PPPoE
	Other		
Colombia	VDSL	Disabled	PPPoE
	Other		
Costa Rica	VDSL	Disabled	PPPoE

Country/Region	ISP	VLANID	Protocol
	Other		
Czech Republic	VDSL	Disabled	PPPoE
	Other		
Denmark	VDSL	Disabled	PPPoE
	Other		
Dominican Republic	VDSL	Disabled	PPPoE
	Other		
Egypt	VDSL	Disabled	PPPoE
	Other		
Fiji	VDSL	Disabled	PPPoE
	Other		
Finland	VDSL	Disabled	PPPoE
	Other		
France	Orange	835	PPPoE
	Sfr(1) PPPoE	835	PPPoE
	Sfr(1) Dynamic IP	835	Dynamic IP
	Sfr(2) PPPoE	836	PPPoE
	Sfr(2) Dynamic IP	836	Dynamic IP
	Free	836	PPPoE
	Bouygues Telecom	200	PPPoE
	Numericable	200	PPPoE
	Ovh PPPoE	835	PPPoE
	Ovh Dynamic IP	835	Dynamic IP
Nordnet PPPoE	835	PPPoE	

Country/Region	ISP	VLANID	Protocol
	Nordnet Dynamic IP	835	Dynamic IP
	Other		
Georgia	VDSL	200	Dynamic IP
	Other		
	1&1	7	PPPoE
	Alice(1)	11	PPPoE
	Alice(2)	7	PPPoE
	Congstar	7	PPPoE
	Easybell	7	PPPoE
	EncoLine	142	Dynamic IP
	EWE TEL	2019	PPPoE
	GMX	7	PPPoE
	KielNET	7	PPPoE
Germany	M-Net	40	PPPoE
	Osnatel	2019	PPPoE
	O2(1)	11	PPPoE
	O2(2)	7	PPPoE
	NetCologne/NetAachen(1)	10	PPPoE
	NetCologne/NetAachen(2)	7	PPPoE
	QSC/Q-DSL	7	PPPoE
	Telekom	7	PPPoE
	Swb(1)	Disabled	PPPoE
	Swb(2)	7	PPPoE
	Versatel	7	PPPoE

Country/Region	ISP	VLANID	Protocol
	Vodafone/Arcor(1)	132	PPPoE
	Vodafone/Arcor(2)	7	PPPoE
	Wilhelm.tel	7	PPPoE
	Willy.tel	2511	PPPoE
	Other		
	CYTA	835	PPPoE
	Forthnet	1102	PPPoE
	Hellas Online	835	PPPoE
Greece	OTE	835	PPPoE
	WIND	835	PPPoE
	Other		
	VDSL	835	PPPoE
Guatemala	Other		
	VDSL	835	PPPoE
Honduras	Other		
	Hutchison PPPoE	Disabled	PPPoE
	Hutchison Dynamic IP	Disabled	Dynamic IP
	Hutchison Static IP	Disabled	Static IP
Hong Kong	WharfT&T PPPoE	Disabled	PPPoE
	WharfT&T Dynamic IP	Disabled	Dynamic IP
	WharfT&T Static IP	Disabled	Static IP
	Other		
	VDSL	Disabled	PPPoE
Hungary	Other		

Country/Region	ISP	VLANID	Protocol
Iceland	VDSL	Disabled	PPPoE
	Other		
India	VDSL	Disabled	PPPoE
	Other		
Indonesia	VDSL	Disabled	PPPoE
	Other		
Iran	VDSL	Disabled	PPPoE
	Other		
Ireland	Eircom	10	PPPoE
	Bbnet	10	PPPoE
	Other		
Israel	BEZEQ	Disabled	PPPoE
	Other		
Italy	VDSL	Disabled	PPPoE
	Other		
Jamaica	VDSL	Disabled	PPPoE
	Other		
Jordan	VDSL	Disabled	PPPoE
	Other		
Kazakhstan	VDSL	Disabled	PPPoE
	Other		
Kenya	VDSL	Disabled	PPPoE
	Other		
Korea	VDSL	Disabled	PPPoE

Country/Region	ISP	VLANID	Protocol
	Other		
kuwait	VDSL	Disabled	PPPoE
	Other		
Lebanon	VDSL	Disabled	PPPoE
	Other		
Lesotho	VDSL	Disabled	PPPoE
	Other		
Macau	VDSL	Disabled	PPPoE
	Other		
Malaysia	VDSL	Disabled	PPPoE
	Other		
Mexico	VDSL	Disabled	PPPoE
	Other		
Morocco	VDSL	Disabled	PPPoE
	Other		
Nepal	VDSL	Disabled	PPPoE
	Other		
Netherlands	KPN PPPoE	6	PPPoE
	KPN Dynamic IP	6	Dynamic IP
	Telfort PPPoE	34	PPPoE
	Telfort Dynamic IP	34	Dynamic IP
	Voiceworks	101	Dynamic IP
	XS4ALL PPPoE	6	PPPoE
	XS4ALL Dynamic IP	6	Dynamic IP

Country/Region	ISP	VLANID	Protocol
	Other		
New Zealand	Spark/Telecom	10	PPPoE
	KiwiLink	10	PPPoE
	Slingshot	10	PPPoE
	Vodafone NZ	10	PPPoE
	Snap	10	PPPoE
	Myrepublic	10	PPPoE
	Callplus PPPoE	10	PPPoE
	Other		
Norway	VDSL	Disabled	PPPoE
	Other		
Oman	VDSL	Disabled	PPPoE
	Other		
Pakistan	VDSL	Disabled	PPPoE
	Other		
Palestine	VDSL	Disabled	PPPoE
	Other		
Panama	VDSL	Disabled	PPPoE
	Other		
Peru	VDSL	Disabled	PPPoE
	Other		
Paraguay	VDSL	Disabled	PPPoE
	Other		
Philippines	VDSL	Disabled	PPPoE

Country/Region	ISP	VLANID	Protocol
	Other		
Poland	Orange	Disabled	PPPoE
	Netia	Disabled	PPPoE
	Other		
Portugal	VDSL	Disabled	PPPoE
	Other		
Puerto Rico	VDSL	Disabled	PPPoE
	Other		
Qatar	Q-Tel/Ooreedo	8	PPPoE
	Other		
Romania	VDSL	Disabled	PPPoE
	Other		
Russia	Rostelecom	Disabled	PPPoE
	Other		
Saudi Arabia	VDSL	Disabled	PPPoE
	Other		
Singapore	VDSL	Disabled	PPPoE
	Other		
Slovakia	T-COM	2510	PPPoE
	Orange	2510	PPPoE
	AMIS	Disabled	PPPoE
	Other		
South Africa	VDSL	Disabled	PPPoE
	Other		

Country/Region	ISP	VLANID	Protocol
Spain	Telefonica	6	PPPoE
	Vodafone	100	PPPoE
	Jazztel	1074	PPPoE
	Other		
Sri Lanka	VDSL	Disabled	PPPoE
	Other		
Sweden	VDSL	Disabled	PPPoE
	Other		
Switzerland	Swisscom	10	PPPoE
	Other		
Syria	SAMA-Net	10	PPPoE
	Other		
Taiwan	VDSL	Disabled	PPPoE
	Other		
Thailand	VDSL	Disabled	PPPoE
	Other		
Tonga	VDSL	Disabled	PPPoE
	Other		
Trinidad and Tobago	VDSL	Disabled	PPPoE
	Other		
Turkey	Turktelekom	35	PPPoE
	Superonline	35	PPPoE
	Vodafone	35	PPPoE
	Turknet	35	PPPoE

Country/Region	ISP	VLANID	Protocol
	D-Smart	35	PPPoE
	Other		
Ukraine	VDSL	Disabled	PPPoE
	Other		
United Arab Emirates	VDSL	Disabled	PPPoE
	Other		
United Kingdom	AAISP	101	PPPoE
	BT	101	PPPoE
	Claranet	101	PPPoE
	EE	101	PPPoE
	Idnet	101	PPPoE
	Plusnet	101	PPPoE
	TalkTalk	101	Dynamic IP
	Vispa	101	PPPoE
	Zen	101	PPPoE
	Other		
United States	VDSL	Disabled	PPPoE
	Other		
Uruguay	VDSL	Disabled	PPPoE
	Other		
Uzbekistan	VDSL	Disabled	PPPoE
	Other		
Venezuela	VDSL	Disabled	PPPoE
	Other		

Country/Region	ISP	VLANID	Protocol
Vietnam	VDSL	Disabled	PPPoE
	Other		
Yemen	VDSL	Disabled	PPPoE
	Other		
Zimbabwe	VDSL	Disabled	PPPoE
	Other		

A.4 Factory settings

Parameter	Default Setting	
Login Information	Login Method	HTTP (web UI)
	Login IP	192.168.1.1
	Login User name/Password	admin/admin
	Web Logout	3 minutes
Network Settings	Link Type	VDSL
	Connection Type	PPPoE
	IP Address Type	IPv4
	Firewall	Enabled
	NAT	Enabled
	IGMP Multicast Proxy	Disabled
	802.1P Priority	-1 (indicates disabled)
	802.1Q VLAN ID	-1 (indicates disabled)
DSL Settings	DSL Link Type	EoA (include PPPoE, IPoE, and Bridge)
	Encapsulation Mode for EoA	LLC/SNAP-BRIDGING
	Encapsulation Mode for PPPoA	VC/MUX
	Encapsulation Mode for IPoA	LLC/SNAP-ROUTING
	Scheduler for Queues of Equal Precedence	Round Robin
Wireless Settings	Wireless feature	Enabled
	Hide Access Point	Disabled
	SSID	2.4GHz: Tenda_XXXXXX 5GHz: Tenda_5G_XXXXXX XXXXXX is the last six characters of the MAC address of the modem router.

Parameter	Default Setting	
	BSSID	2.4GHz: The MAC address on the product label + 1. 5GHz: The MAC address on the product label + 2.
	WMF	Enabled
	Channel	Auto
	Network Authentication	Open
	WPS Setup	Disabled
	MAC Filter	Disabled
	Wireless Bridge	Disabled
LAN Settings	IP Address	192.168.1.1
	Subnet Mask	255.255.255.0
	Primary DNS server	192.168.1.1
DHCP Setting	Status	Enabled
	Start IP	192.168.1.2
	End IP	192.168.1.254
	Lease Time	24 hours
Management	TR-069 client	Disabled
	Login User Name/Password	Administrator account: admin/admin
		Support account: support/support
		User account: user/user
	Access Control-Services	HTTP (LAN), ICMP (LAN), SSH (LAN), SNMP (LAN), FTP (LAN), TFTP (LAN) and HTTPS (LAN)
Others	Time settings	Automatically synchronize with Internet time servers (GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi
	Parental Control	Disabled
	Quality of Service	Enabled

Parameter	Default Setting
Virtual Servers	Disabled
Port Triggering	Disabled
DMZ Host	Disabled
UPnP	Enabled
Storage Service	Enabled
IPTV	Disabled