PLANET
Networking & Communication

User's Manual

802.11n Dual Band Wireless VDSL2 Router

► VDR-300NU

www.PLANET.com.tw

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Plug the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio technician for help.

FCC Caution:

To assure continued compliance, (example-use only shielded interface cables when connecting to computer or peripheral devices) any changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the Following two conditions:

(1) This device may not cause harmful interference

(2) This Device must accept any interference received, including interference that may cause undesired operation.

Federal Communication Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm (8 inches) during normal operation.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/CE OF THE EUROPEAN PARLIAMENT AND THE COUNCIL OF 9 March 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE).

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

National Restrictions

This device is intended for home and office use in all EU countries (and other countries following the EU directive 1999/5/EC) without any limitation except for the countries mentioned below:

Country	Restriction	Reason/remark
Bulgaria	None	General authorization required for outdoor use and public service
France	Outdoor use limited to 10 mW e.i.r.p. within the band 2454-2483.5 MHz	Military Radiolocation use. Refarming of the 2.4 GHz band has been ongoing in recent years to allow current relaxed regulation. Full implementation planned 2012
Italy	None	If used outside of own premises, general authorization is required
Luxembourg	None	General authorization required for network and service supply(not for spectrum)
Norway	Implemented	This subsection does not apply for the geographical area within a radius of 20 km from the centre of Ny-Ålesund

Russian Federation	None	Only for indoor applications

WEEE regulation

To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste; WEEE should be collected separately.

Revision

User's Manual for 802.11n Dual band Wireless VDSL2 Router

Model: VDR-300NU

Rev: 1.0 (January, 2014)

Part No. EM-VDR-300NU_v1 (**2081-AC0360-000**)

Table of Contents

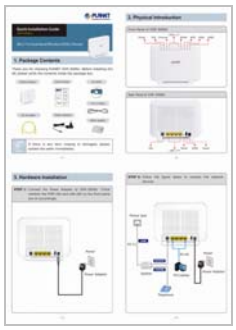
Chapter 1.Product Introduction

1.1 Package Contents

Thank you for choosing PLANET VDR-300NU. Before installing the router, please verify the contents inside the package box.

VDR-300NU

Quick Installation Guide



CD-ROM

(User Manual included)

Power Adapter

12V/2A DC output

100~240V AC input

Ethernet Cable

RJ-45 / CAT5E 1.5 meter UTP

Phone Cable

RJ11 telephone wire

VDSL Splitter

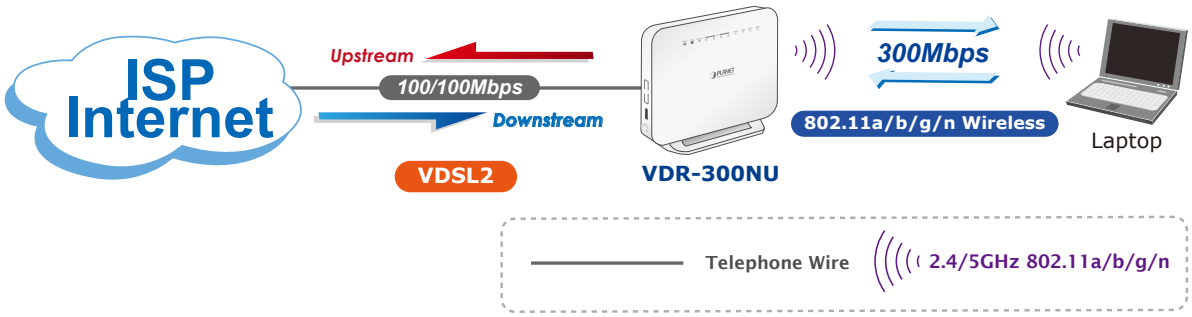
Note

If there is any item missing or damaged, please contact the seller immediately.

1.2 Product Description

High Performance Ethernet over VDSL

PLANET 802.11n Dual Band Wireless VDSL2 Router, VDR-300NU, applies 2T2R MIMO antenna technology and provides office and residential users with the ideal solution for sharing a high-speed VDSL2 broadband connection and four-10/100Mbps Fast Ethernet backbone. The VDR-300NU is developed with three core networking technologies: IEEE 802.11a/b/g/n, Ethernet and VDSL2 (Very High Speed Digital Subscriber Line 2). Via VDSL 2 technology, the VDR-300NU offers very high performance access to Internet, up to **100Mbps** for both downstream and upstream data transmission. VDSL2 absolutely offers the fastest data transmission speed over existing copper telephone lines without the need for rewiring.

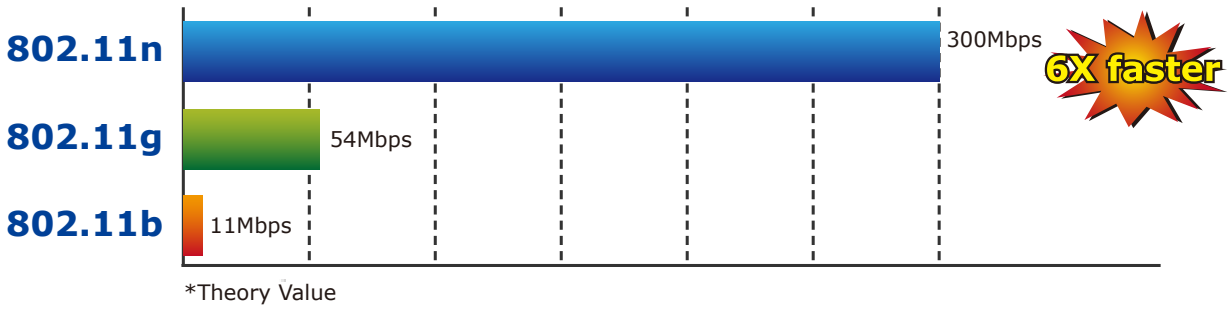


Delivering High-Demand Service Connectivity for ISP / Triple Play Devices

The VDR-300NU provides excellent bandwidth to satisfy the triple play devices for home entertainment and communication. With the capability of 100/100Mbps symmetric data transmission, the VDR-300NU enables many multi-media services to work on local Internet, such as **VOD (Video on Demand)**, Voice over IP, **Video phone**, **IPTV**, Internet caching server, **distance education**, and so on.

Dual Band High-Speed 802.11n Wireless

The VDR-300NU complies with ITU-T G993.2 standard and provides two modes for network applications -- **Bridge** and **Router**. With built-in IEEE 802.11b/g and 802.11a/n wireless network capability, the VDR-300NU allows any computer and wireless-enabled network device to connect to it without additional cabling. 802.11n wireless capability brings users the highest speed of wireless experience ever; the data transmission rate can be as high as **300Mbps.** The radio coverage is also doubled to offer high speed wireless connection even in widely spacious offices or houses.

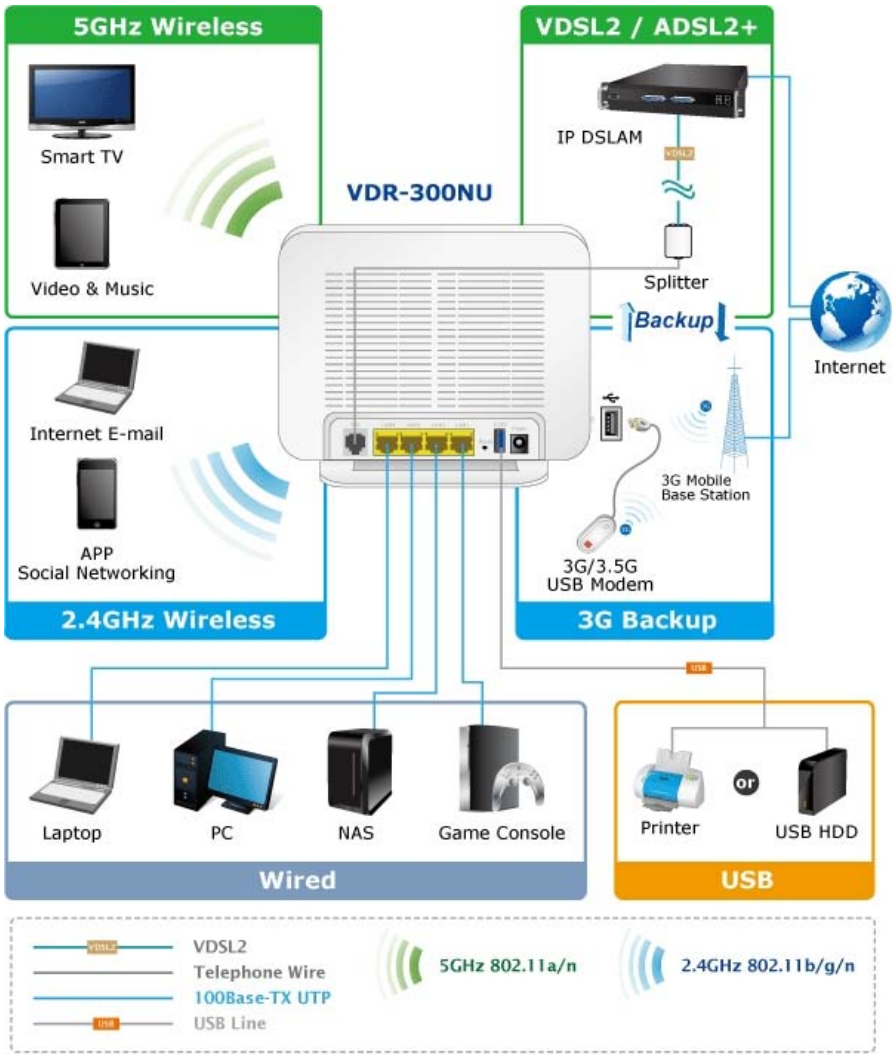


Secure Wireless Access Control

To secure wireless communication, the VDR-300NU supports most up-to-date encryptions including WEP, WPA-PSK and WPA2-PSK. Moreover, the VDR-300NU supports WPS configuration with PBC/PIN type for users to easily connect to a secured wireless network.

Multiple Functions for Broadband Communication

The VDR-300NU integrates **wireless LAN**, **USB storage**, and **3G WAN** services into one unit. It is designed to provide a simple and cost-effective xDSL Internet connection for a private Ethernet and 802.11a/b/g/n wireless network. The Router combines high-speed xDSL Internet connection, IP routing for the LAN and wireless connectivity in one package. It is usually preferred to provide high access performance applications for the individual users, the SOHOs, and the small enterprises.



Providing Superior Function

The VDR-300NU provides user-friendly management interface to be managed easily through standard web browsers. For networking management features, the VDR-300NU not only provides basic router functions such as DHCP server, virtual server, DMZ, QoS, and UPnP, but also provides full firewall functions including Network Address Translation (NAT), IP/Port/MAC Filtering and Content Filtering. Furthermore, the VDR-300NU serves as an Internet firewall to protect your network from being accessed by unauthorized users.

More Flexible File Sharing over USB port

The VDR-300NU is built-in with two USB 2.0 ports which can be connected to a USB printer or storage device for file sharing. It can recognize the USB printer or storage automatically without user experience. Thus, all clients on the network can share printer or mass storage through the VDR-300NU without complicated network configuration. Via the USB port, it also can output 5V DC power to charge any USB compliant devices.

1.3 Product Features

➢ **Internet Access Features**

- **Shared Internet Access:** All users on the LAN can access the Internet through the VDR-300NU using only one single external IP address. The local (invalid) IP addresses are hidden from external sources. This process is called NAT (Network Address Translation).
- **Built-in VDSL2 Modem:** The VDR-300NU provides VDSL2 modem and supports all common VDSL2 connections.
- **Multiple WAN Connections:** Upon the Internet (WAN port) connection, the VDR-300NU supports ADSL2+, VDSL2, and 3G with USB port.

➢ **Advanced Internet Functions**

- **Virtual Servers:** This feature allows Internet users to access Internet servers on your LAN. The setup is quick and easy.
- **Firewall:** The VDR-300NU supports simple firewall with NAT technology.
- **Universal Plug and Play (UPnP):** UPnP allows automatic discovery and configuration of the Broadband Router. UPnP is supported by Windows ME, XP, or later.
- **DMZ Support:** The VDR-300NU can translate public IP addresses into private IP address to allow unlimited 2-way communication with the servers or individual users on the Internet. It provides the most flexibility to run programs smoothly for programs that might be restricted in NAT environment.
- **RIP1/2 Routing:** It supports RIPv1/2 routing protocol for routing capability.
- **IGMP Snooping:** IGMP 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.

➢ **LAN Features**

- **4-Port Switch:** The VDR-300NU incorporates a 4-port 10/100Base-TX switching hub, making it easy to create or extend your LAN.
- **DHCP Server Support:** **D**ynamic **H**ost **C**onfiguration **P**rotocol provides a dynamic IP address to PCs and other devices upon request. The VDR-300NU can act as a DHCP Server for devices on your local LAN.

➢ **Wireless Features**

- **Supports IEEE 802.11a/b/g/n Dual Band Wireless Stations:** The VDR-300NU supports the selectable 2.4GHz and 5GHz wireless connection. 802.11n standard provides backward compatibility with the 802.11b and 802.11g standard, so 802.11b, 802.11g, and 802.11n can be used simultaneously. IEEE 802.11n wireless technology is capable of up to 300Mbps data rate.
- **WPS Push Button Control:** The VDR-300NU supports WPS (Wi-Fi Protected Setup) for users to easily connect to wireless network without configuring the security.
- **Advanced Security:** 64/128-bit WEP, WPA/WPA2 and WPA-PSK/WPA2-PSK(TKIP/AES encryption), 802.1x

- **Wireless MAC Access Control:** The Wireless Access Control feature can check the MAC address (hardware address) of wireless stations to ensure that only trusted wireless stations can access your LAN.
- **Dual-SSID:** It allows users to access different networks through a single AP.

1.4 Product Specifications

Model		VDR-300NU
Product Description		802.11n Dual Band Wireless VDSL2 Router
Hardware Specifications		
Interfaces	**LAN**	4 x 10/100Base-TX, Auto-Negotiation, Auto MDI/MDI-X RJ45 port
	WAN	1 x RJ-11
	USB	USB 2.0, Type-A, 5V DC/0.5A Output
Antenna		2.4GHz : 2 x 2.5dBi 5GHz: 2 x 2dBi
Button		1 x RESET button 1 x WPS button
LED Indicators		PWR, DSL, LAN1-4, WLAN, WPS, Security
Dimensions (W x D x H)		180 x 145 x 54 mm
Weight		306g
Power		12V DC, 2A
Power Consumption		18W (not including power adapter)
Router Features		
Internet Connection Type		Shares data and Internet access for users, supporting the following internet accesses: ■ PPPoE ■ Dynamic IP ■ Static IP
VDSL Features		● ITU-T G.993.2 VDSL2 ● Supports 8a,8b,12a,12b,17a,30a profile ● Supports G.vector ● Supports ATM and PTM ● Supports G.INP
ADSL Features		● T1.413i2, G.992.1 ● G.dmt, G.992.2, G.lite ● G.992.3 (G.bis/ADSL2) ● G.992.5 (ADSL2+) ● ITU G.994.1 (G.hs) ● Annex L (Reach Extended ADSL2) ● Supports ATM forum UNI3.0, 3.1 and 4.0 permanent virtual circuits (PVCs) ● Supports CBR, UBR, VBR-rt, VBR-nrt ● Supports multiple PVCs ● Supports ITU-T i.610F4/F5 OAM
Bridging Features		● Self-learning bridge (IEEE 802.1D Transparent Bridging) ● At least 64 learning MAC addresses ● Supports IGMP snooping

Protocol Features	● RFC2684 multiprotocol Encapsulation over ATM Adaptation Layer 5 ● RFC1483 multiprotocol Encapsulation over ATM Adaptation Layer 5 ● RFC2364 PPP over ATM ALL5 (PPPoA) ● RFC2516 PPP Over Ethernet (PPPoE) ● RFC1662 PPP in HDLC-like Framing ● RFC1332 PPP Internet Protocol Control Protocol ● RFC1577/2225 Classical IP and ARP over ATM (IPoA) ● RFC894 A Standard for the Transmission of IP Datagrams over Ethernet Networks ● RFC1042 A standard for the Transmission of IP Datagrams over IEEE 802 Networks ● MER (a.k.a IP over Ethernet over AAL5) ● Supports ALG (Application Level Gateways) ● IEEE802.3 ● IEEE802.3u ● IEEE 802.11b ● IEEE 802.11g ● IEEE 802.11n
Routing Features	● RFC768 User Datagram Protocol (UDP) ● RFC791 Internet Protocol (IP) ● RFC792 Internet Control Message Protocol (ICMP) ● RFC793 Transmission Control Protocol (TCP) ● RFC826 An Ethernet Address Resolution Protocol (ARP) ● RFC862 Echo Protocol ● Supports IP routing ● Supports transparent bridging ● Supports source and destination routing ● Supports DHCP server/client ● Supports UPnP ● Supports NAT,NAPT ● Supports DMZ ● Supports IP QoS ● Supports IGMP proxy ● Supports IPv6
Security	● Three-level login including local admin, local user, and remote technical support access ● Service access control based on incoming interface: WAN or LAN ● Service access control based on source IP addresses ● Protects DOS attacks from WAN: SYN flooding, IP surfing, ping of Death, fragile, UDP ECHO (port 7), teardrop, land ● PAP (RFC1334), CHAP (RFC1994), MSCHAP for PPP session ● IP filter, parental control

Management	● Device Configuration, Management and Update ● Web based GUI ● Localization support ● Embedded web server ● Download image via HTTP, TFTP client, TFTP server, FTP server ● Command Line Interface via serial port, telnet, or ssh ● Menu-driven CLI via serial port or telnet ● Universal Plug and Play (UPnP) Internet Gateway Device (IGDv1.0) ● WAN Management Protocol (TR-069) ● SNMP v1/v2 ● PSI configuration file upload and download ● Date/time update from SNTP Internet Time Server
Wireless Interface Specifications	
Wireless Standard	IEEE 802.11a/b/g/n
Frequency Band	2.4GHz: 2.412~2.484GHz 5GHz: 5.180~5.825GHz
Modulation Schemes	● 802.11g: 64QAM, 16QAM, QPSK, BPSK, DSSS ● 802.11b: CCK, DQPSK, DBPSK ● HT20 and HT40: 64 QAM, 16QAM, QPSK, BPSK
Data Transmission Rates	**802.11n(40MHz)**: up to 300 Mbps
	802.11n(20MHz): up to 144.4 Mbps
	802.11g: 54, 48, 36, 24, 18, 12, 9, 6 Mbps per channel, auto fallback for extended range
	802.11b: 1, 5.5, 2, 1 Mbps per channel, auto fallback for extended range
	802.11a: 54, 48, 36, 24, 18, 12, 9, 6 Mbps
RF Power	**2.4GHz:** 11b: 18±1.5dBm 11g: 14.5±1.5dBm 11n(20M): 16.5±1.5dBm (MCS0~3) 14.5±1.5dBm (MCS4~7) 16.5±1.5dBm (MCS8~11) 14.5±1.5dBm (MCS12~15) 11n(40M): 14±1.5dBm (MCS0~3) 12.5±1.5dBm (MCS4~7) 14±1.5dBm (MCS8~11) 12.5±1.5dBm (MCS12~15)
Wireless Data Encryption	64/128-bit WEP, WPA-PSK, WPA2-PSK, 802.1x encryption, and WPS PBC

Environment Specifications	
Temperature / Humidity	Operating: 0~40 degrees C, 10%~ 95% (non-condensing), Storage: -20~70 degrees C, 5~95% (non-condensing)
Certification	CE

Chapter 2. Hardware Installation

This chapter offers information about installing your router. If you are not familiar with the hardware or software parameters presented here, please consult your service provider for the values needed.

2.1 Hardware Description

2.1.1 Front Panel

The front panel provides a simple interface monitoring of the router. **Figure 2-1** shows the front panel of VDR-300NU.

Figure 2-1 VDR-300NU Front Panel

2.1.2 LED Indications

The LEDs on the top panel indicate the instant status of system power, WAN data activity and port links, and help monitor and troubleshoot when needed. **Figure 2-1** and **Table 2-1** show the LED indications of the VDR-300NU.

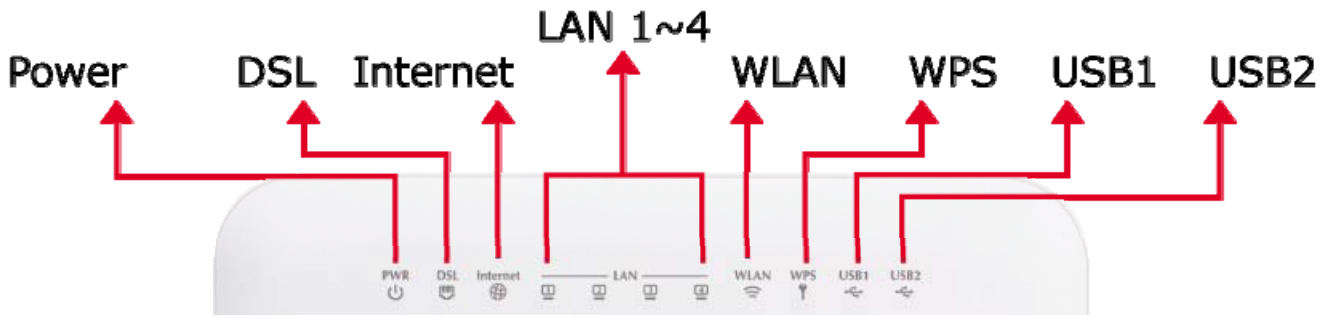


Figure 2-2 VDR-300NU LED

Front Panel LED Definition

LED	Color	State	Description
PWR	Green	ON	When the router is powered on, and in ready state.
		Flashing	The software is upgrading.
		OFF	The device is powered off.
	Red	ON	The device is initiating.
		Flashing	The software is upgrading.
DSL	Green	ON	The VDSL2 is connected successfully.
		Flashing	Router is trying to establish a VDSL2 connection to VDSL2 device or telecom's network.
		OFF	The device is powered off.
Internet	Green	ON	Internet is synchronized successfully in the route mode.
		Flashing	Internet data is being transmitted.
		OFF	Ethernet interface is disconnected.
	Red	ON	Authentication has failed.
LAN1-4	Green	ON	The Ethernet interface is connected.
		Flashing	Data is being transmitted or received via the corresponding LAN port.
		OFF	The Ethernet interface is disconnected.
WLAN	Green	ON	WLAN is enabled.
		Flashing	Data is being transmitted through the wireless interface.
		OFF	WLAN is disabled.
WPS	Green	ON	Connection succeeds under Wi-Fi Protected Setup.
		Flashing	Negotiation is in progress under Wi-Fi Protected Setup.
		OFF	Wi-Fi Protected Setup is disabled.
USB	Green	ON	The connection of 3G or USB device has established.
		Flashing	Data is being transmitted.
		OFF	No signal is detected.

Table 2-1 The LED indication of VDR-300NU

2.1.3 Rear Panel and Side Panel

The rear panel provides the physical connectors connected to the power adapter and any other network device. **Figure 2-2** and **Figure 2-3** shows the rear and side panel of the VDR-300NU.

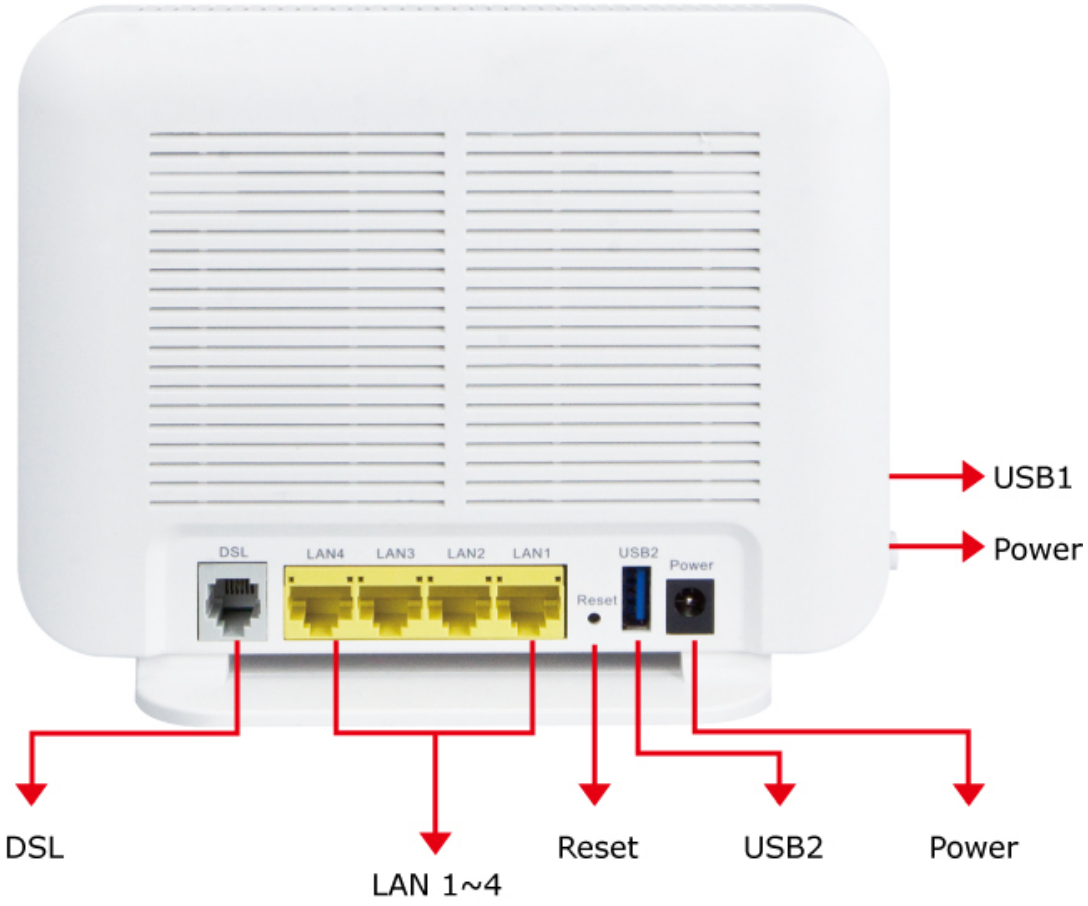


Figure 2-3 VDR-300NU Rear Panel

Rear Panel Port and Button Definition

Connector	Description
POWER	Power connector with 12V DC, 2 A
USB2	For connecting the 3G network adapter or other USB storage devices.
RESET	Press more than 2 seconds for resetting to factory default setting.
LAN (1-4)	Router is successfully connected to a device through the corresponding port (1, 2, 3, or 4). If the LED light of LNK/ACT is flashing, the Router is actively sending or receiving data over that port.
DSL	The RJ-11 connector allows data communication between the router and the DSL network through a twisted-pair phone wire

2.1.4 Right Side Panel

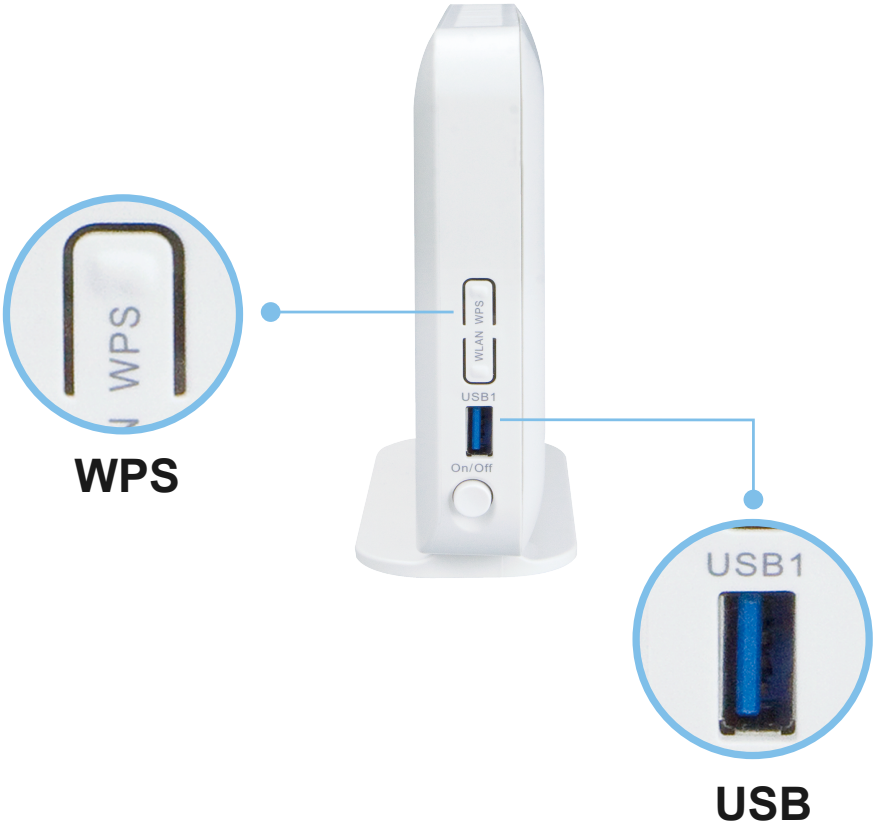


Figure 2-4 VDR-300NU Side Panel

Side Panel Interface and Button Definition

Connector	Description
On/Off	Power switch.
USB1	For connecting the 3G network adapter or other USB storage devices.
WLAN	WLAN switch, for enabling or disabling the WLAN function.
WPS	This button is used for enabling WPS PBC mode. If WPS is enabled, press this button, and then the wireless router starts to accept the negotiation of PBC mode.

Chapter 3. Connecting to the Router

3.1 System Requirements

- Broadband Internet Access Service (Cable/xDSL/Ethernet connection)
- One Cable/xDSL Modem that has an RJ-45 connector (not necessary if the Router is connected directly to the Ethernet.)
- PCs with a working Ethernet Adapter and an Ethernet cable with RJ-45 connectors
- PCs running Windows 98/ME, NT4.0, 2000/XP, Windows Vista / Win 7, MAC OS 9 or later, Linux, UNIX or other platforms are compatible with **TCP/IP** protocols
- The above PCs are installed with Web browser

Note

1. The Router in the following instructions is named as PLANET VDR-300NU.
2. It is recommended to use Internet Explorer 8.0 or above to access the Router.

3.2 Installing the Router

Please connect the device to you computer as follows:

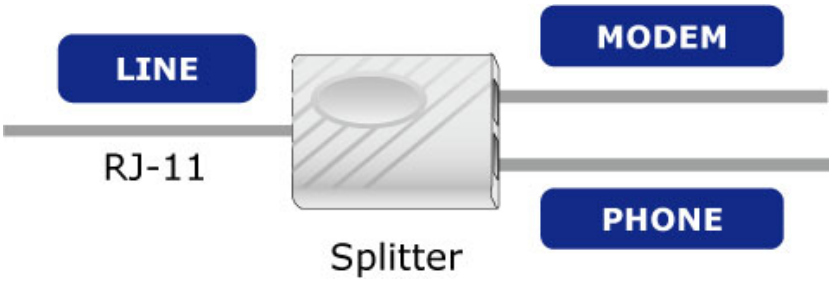
STEP 1. Connect the DSL port of the router and the Modem port of the splitter with a telephone cable; connect the phone to the phone port of the splitter through a cable; and connect the incoming line to the Line port of the splitter.

The spliiter has three ports:

Line: Connect to a wall phone jack (RJ-11 jack)

Modem: Connect to the Line interface of the router

Phone: Connect to a telephone set



STEP 2. Connect the Power Adapter to the VDR-300NU. Check whether the **PWR LED** on the front panel are on accordingly. **Figure3-1** shows the power adapter connection diagram.

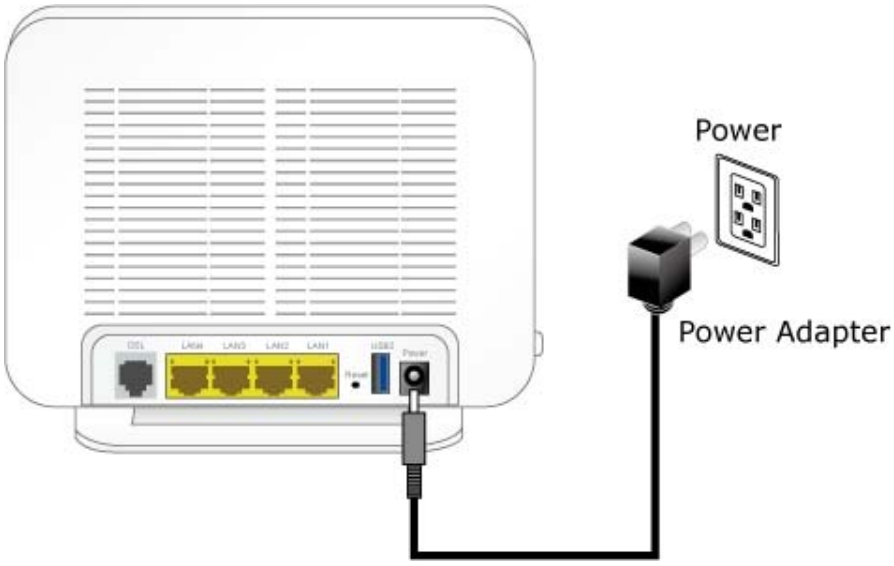


Figure 3-1: VDR-300NU Power Adapter Connection Diagram

STEP 3. Use Ethernet cable to connect “LAN” port of the router and “LAN” port of your computer. Follow **Figure 3-2** to connect the network devices.

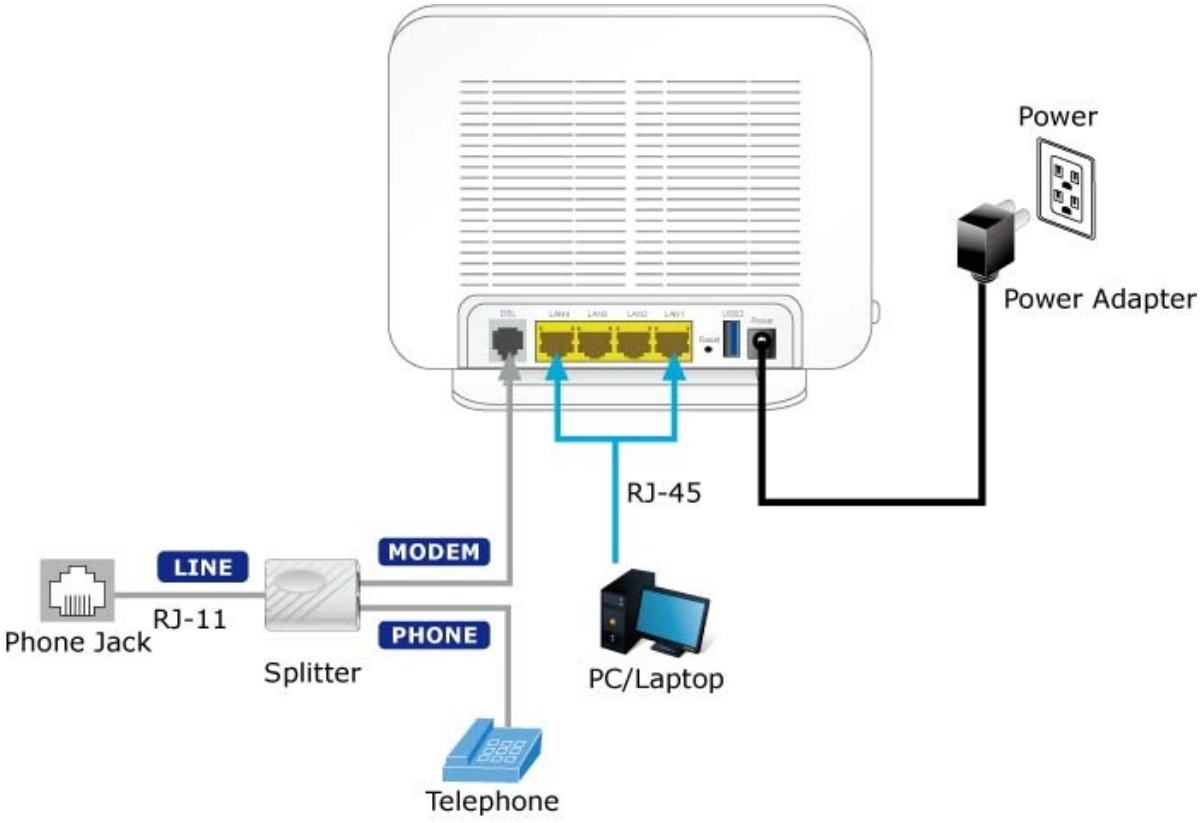


Figure 3-2: VDR-300NU Connection Diagram

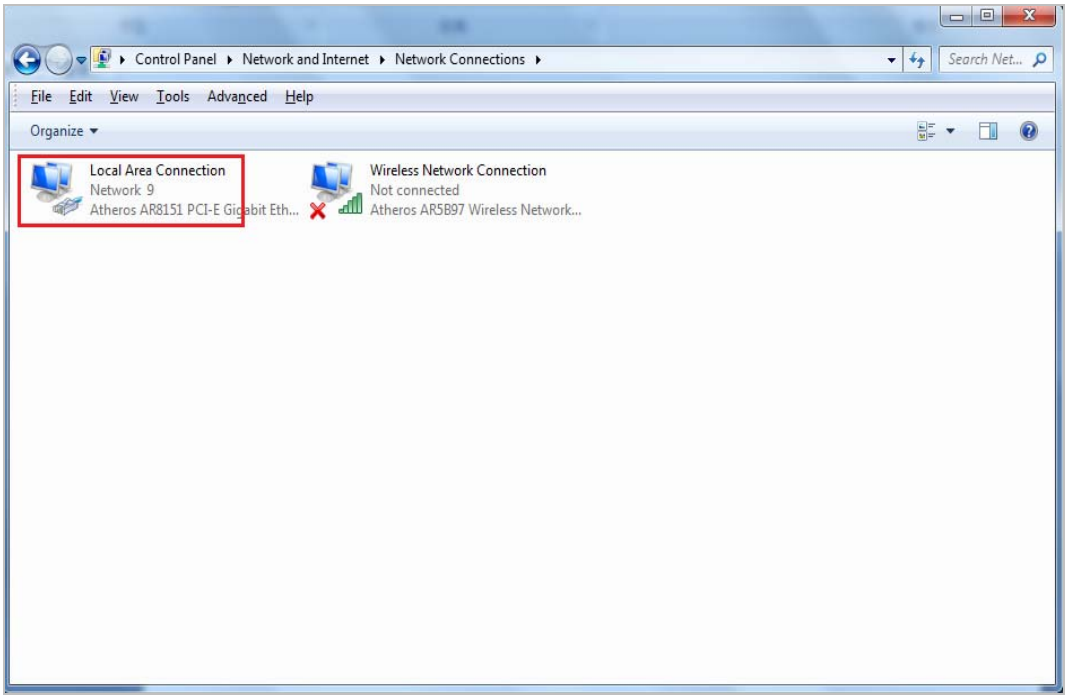
If you use 3G WAN service, connect the 3G USB data card to the **USB** port of the router.

Chapter 4. Installation Guide

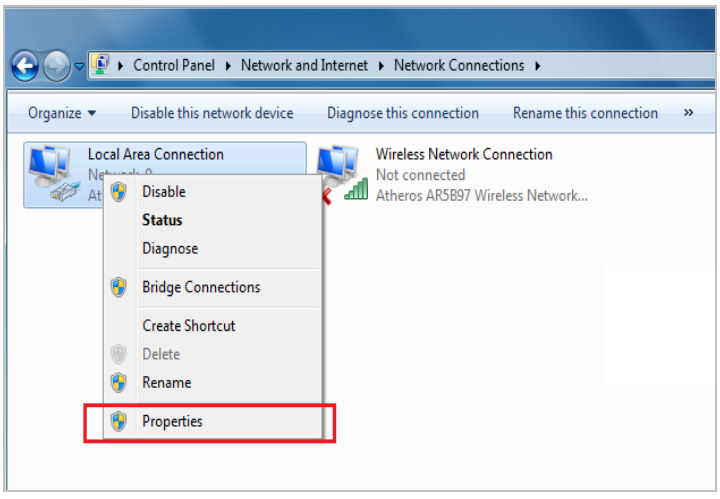
4.1 Configuring PC in Windows 7

1. Go to **Start / Control Panel / Network and Internet / Network and Sharing Center** and click **Change adapter settings** on the left banner.

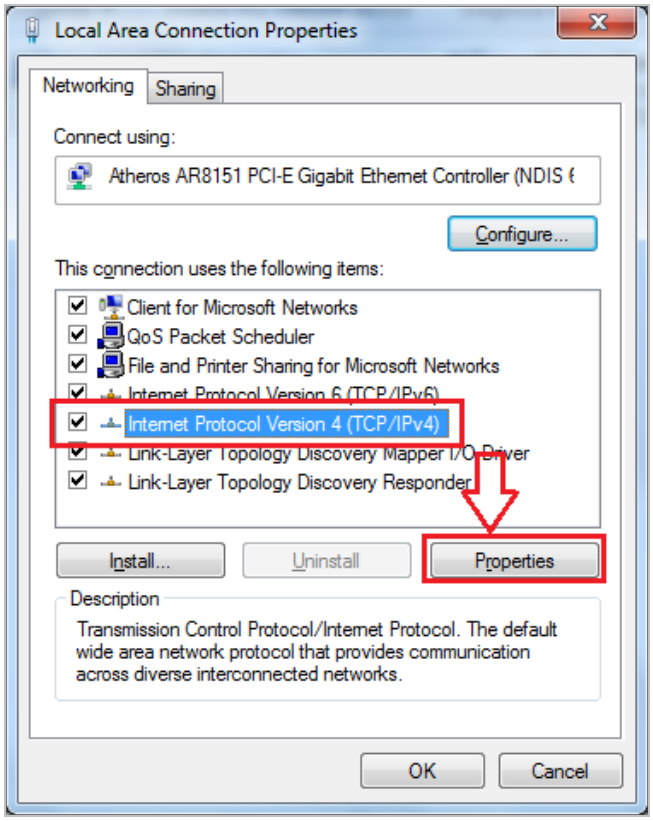
2. Double-click **Local Area Connection**.



3. In the **Local Area Connection Status** window, click **Properties**.

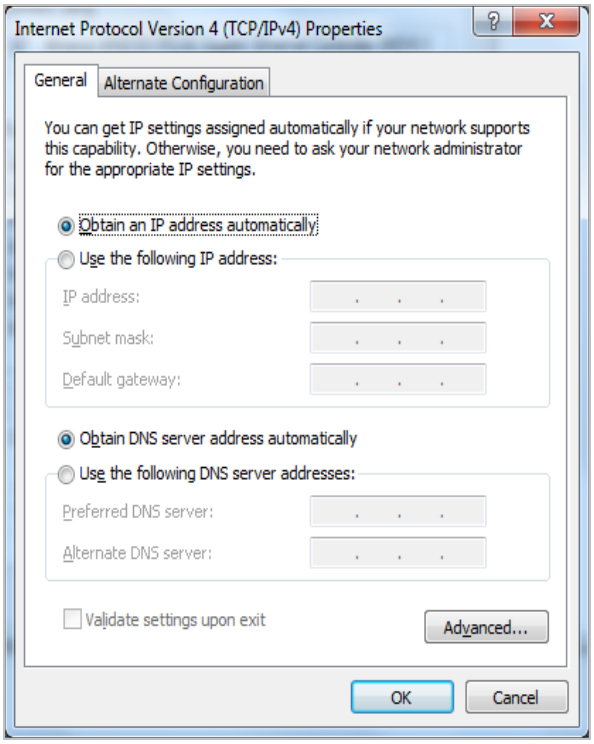


4. Select **Internet Protocol Version 4 (TCP/IPv4)** and **click Properties**.



5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** button.

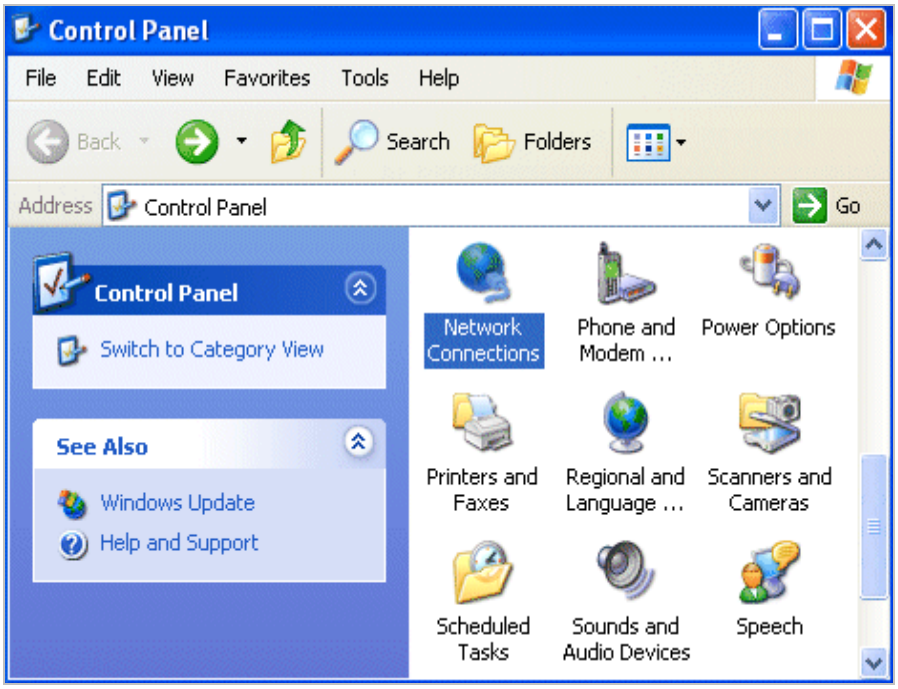
6. Click **OK** to finish the configuration.



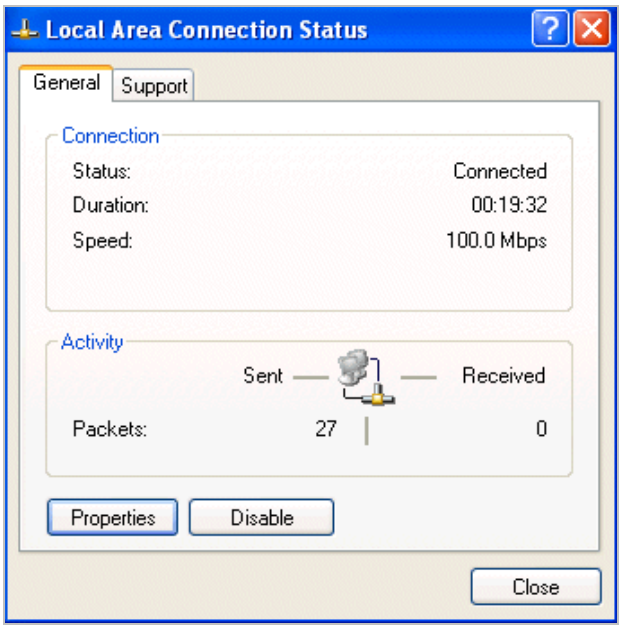
4.2 Configuring PC in Windows XP

1. Go to **Start / Control Panel (in Classic View)**. In the Control Panel, double-click on **Network Connections**

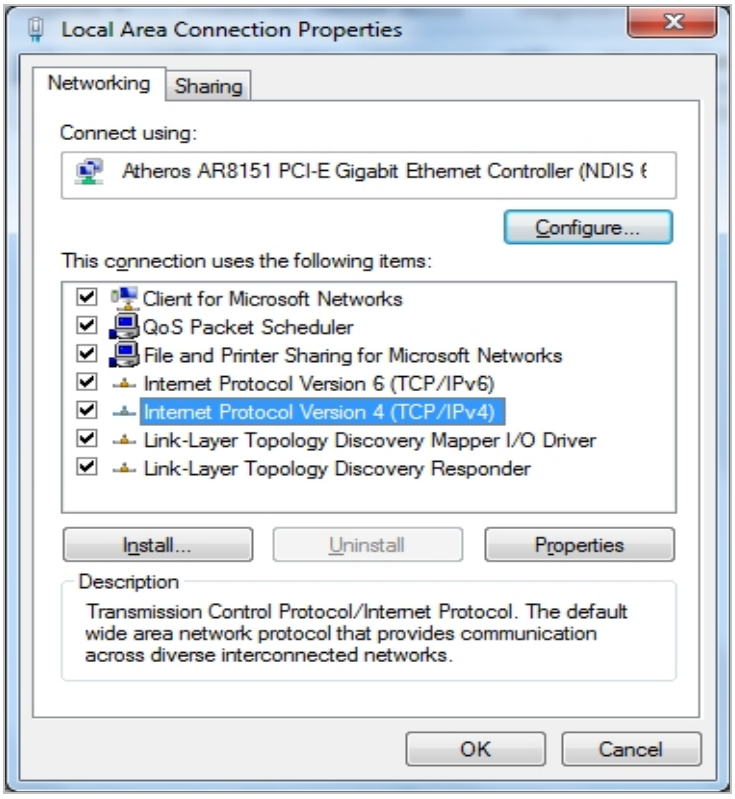
2. Double-click **Local Area Connection**.



3. In the **Local Area Connection Status** window, click **Properties**.

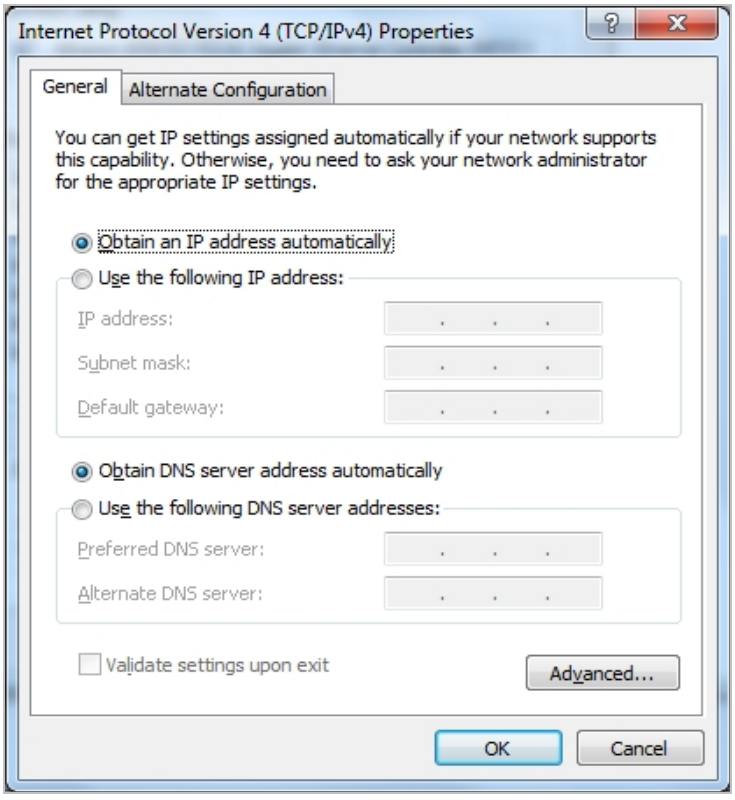


4. Select **Internet Protocol (TCP/IP)** and click **Properties**.



5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** button.

6. Click **OK** to finish the configuration.



Chapter 5. System Settings

Determine your Connection Settings

Before you configure the router, you need to know the connection information supplied by your Internet service provider.

Connecting the VDSL 2 Router to your Network

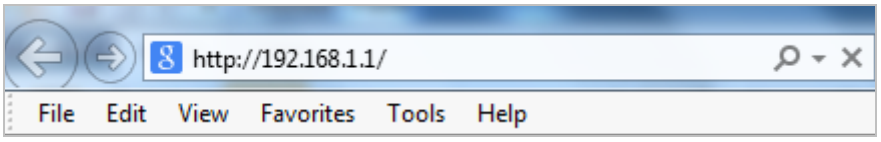
Unlike a simple hub or switch, the setup of the VDSL Router consists of more than simply plugging everything together. Because the Router acts as a DHCP server, you will have to set some values within the Router, and also configure your networked PCs to accept the IP Addresses the Router chooses to assign them.

Generally there are several different operating modes for your applications. And you can know which mode is necessary for your system from ISP. These modes are router, bridge, and PPPoE+NAT.

Configuring with Web Browser

It is advisable to change the administrator password to safeguard the security of your network. To configure the router, open your browser, type **"http: //192.168.1.1"** into the address bar and click **"Go"** to get to the login page.

Save this address in your Favorites for future reference.



At the User Name prompt, type **"admin"**, and the Password prompt, type **"admin"**. You can change these later if you wish. Click **"OK"** to login the router and you can start to configure it now.

5.1 Device Information

Choose **Device Info**, and the submenus of **Device Info** are shown below:

Figure 5-1-1

5.1.1 Summary

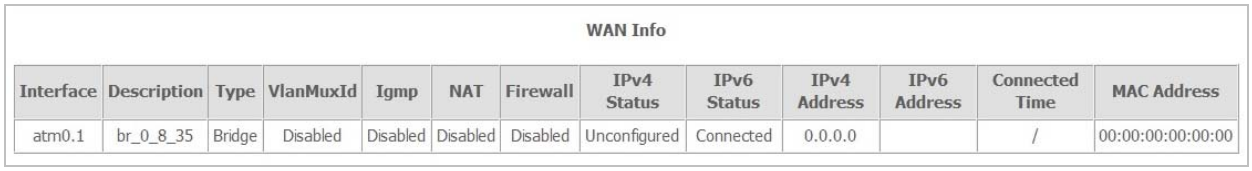
Choose **Device Info > Summary**, and the following page appears.

Figure 5-1-2

This page displays the device information such as the board ID, software version, and the information of your WAN connection such as the upstream rate and the LAN address.

5.1.2 WAN

Choose **Device Info > WAN** and the following page appears.



WAN Info

Interface	Description	Type	VlanMuxId	Igmp	NAT	Firewall	IPv4 Status	IPv6 Status	IPv4 Address	IPv6 Address	Connected Time	MAC Address
atm0.1	br_0_8_35	Bridge	Disabled	Disabled	Disabled	Disabled	Unconfigured	Connected	0.0.0.0		/	00:00:00:00:00:00

Figure 5-1-3

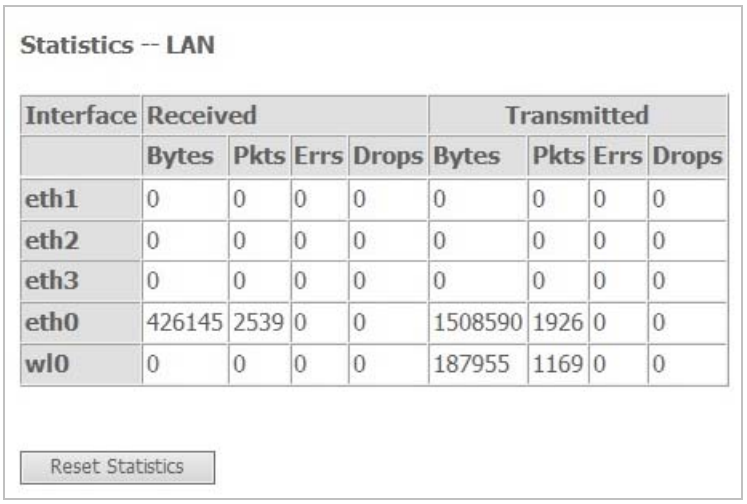
This page displays the information of the WAN interface. You can select from **Advanced Setup** > **Layer2 Interface** to choose the type you need.

5.1.3 Statistics

Choose **Device Info > Statistics**, and the following page appears.

■ LAN

Choose **Device Info > Statistics > LAN** and the following page appears.



Statistics -- LAN

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
eth1	0	0	0	0	0	0	0	0
eth2	0	0	0	0	0	0	0	0
eth3	0	0	0	0	0	0	0	0
eth0	426145	2539	0	0	1508590	1926	0	0
wl0	0	0	0	0	187955	1169	0	0

Reset Statistics

Figure 5-1-4

On this page, you can view the statistical information about the received and transmitted data packets of the Ethernet and wireless interfaces.

Click **Reset Statistics** to restore the values to zero and recount them.

■ WAN Service

Choose **Device Info > Statistics > WAN Service** and the following page appears.

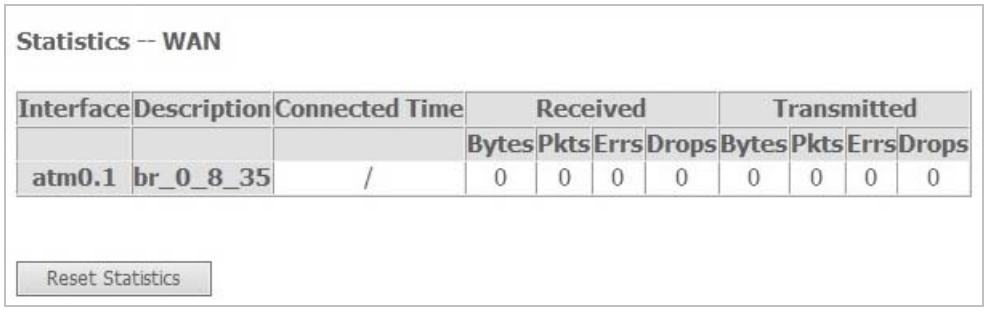


Figure 5-1-5

On this page, you can view the statistical information about the received and transmitted data packets of the WAN interface.

Click **Reset Statistics** to restore the values to zero and recount them.

■ xTM

Choose **Device Info > Statistics > xTM** and the following page appears.

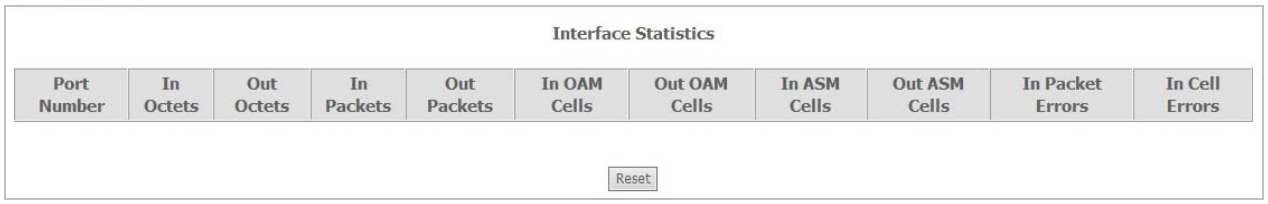


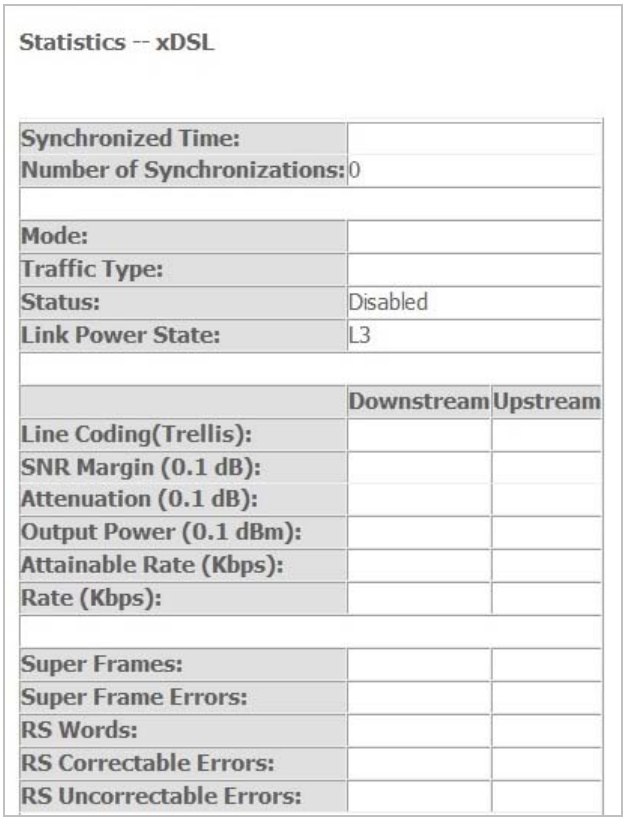
Figure 5-1-6

On this page, you can view the statistical information about the received and transmitted data packets at the xTM interfaces.

Click the **Reset** button to restore the values to zero and recount them.

■ xDSL

Choose **Device Info > Statistics** > **xDSL** and the following page appears.



Statistics -- xDSL

Synchronized Time:		
Number of Synchronizations:	0	
Mode:		
Traffic Type:		
Status:	Disabled	
Link Power State:	L3	
	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:		

Figure 5-1-7

On this page, you can view the statistical information about the received and transmitted data packets of the xDSL interfaces.

- **xDSL BER Test**

Click **xDSL BER Test** to perform a bit error rate (BER) test on the DSL line. The test page is as follows:

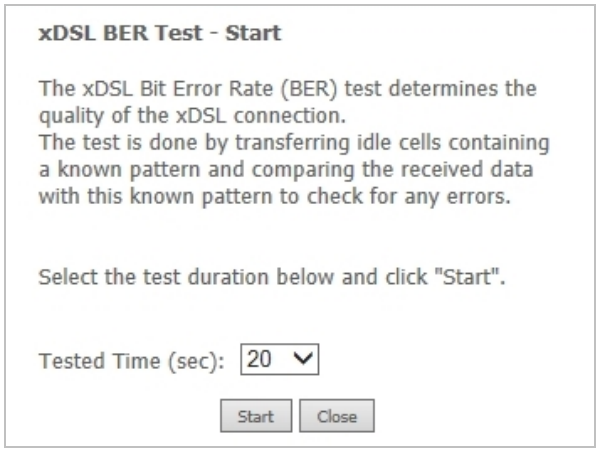


Figure 5-1-8

The **Tested Time (sec)** can be 1, 5, 10, 20, 60, 120, 180, 240, 300, or 360. Select a time in the drop-down list and click **Start**. The following pages appear.

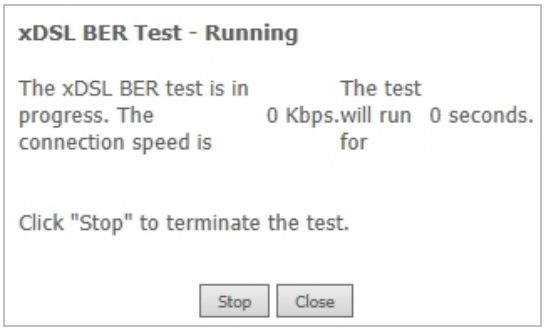


Figure 5-1-9

When the **xDSL BER Test** completes, the following page appears.

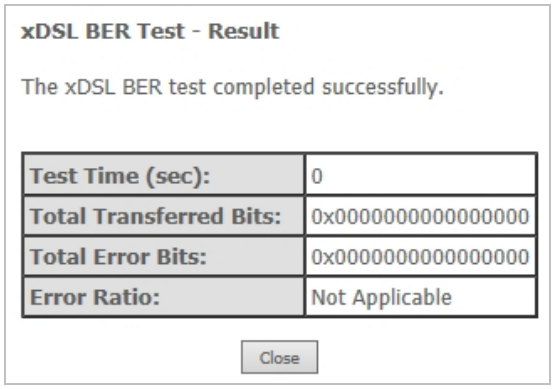


Figure 5-1-10

Note

If the BER reaches e-5, you cannot access the Internet.

5.1.4 Route

Choose **Device Info > Route** and the following page appears. On this page, you can view the route table information.

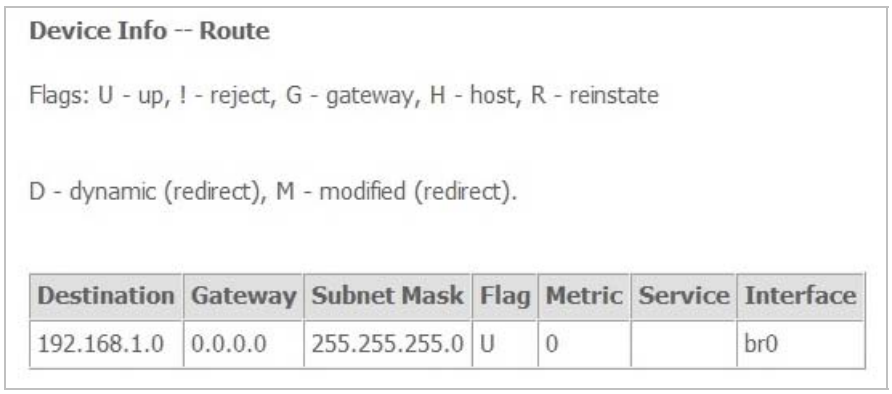


Figure 5-1-11

5.1.5 ARP

Choose **Device Info > ARP** and the following page appears.

Figure 5-1-12

On this page, you can view the MAC address and IP address information of the device connected to the router.

5.1.6 DHCP

Choose **Device Info > DHCP** and the following page appears.

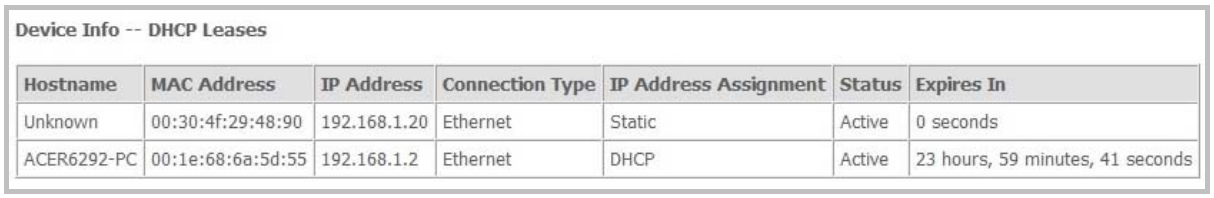


Figure 5-1-13

On this page, you can view the host name, the IP address assigned by the DHCP server, the MAC address corresponding to the IP address, and the DHCP lease time.

5.2 Advanced Setup

Choose **Advanced Setup** and the submenus of **Advanced Setup** are shown below:

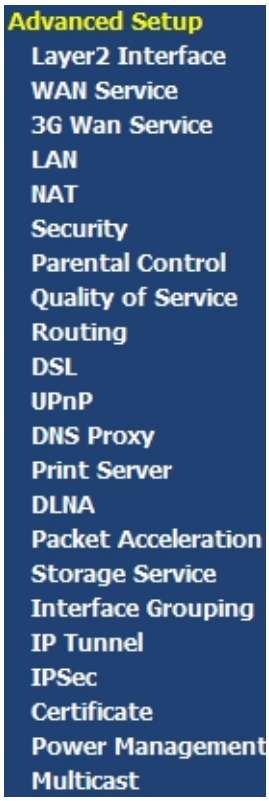


Figure 5-2-1

5.2.1 Layer2 Interface

Choose **Advanced Setup** > **Layer2 Interface** and the following page appears.

■ ATM Interface

Choose **Advanced Setup** > **Layer2 Interface > ATM Interface** . On this page, you can add or remove to configure DSL ATM Interfaces.

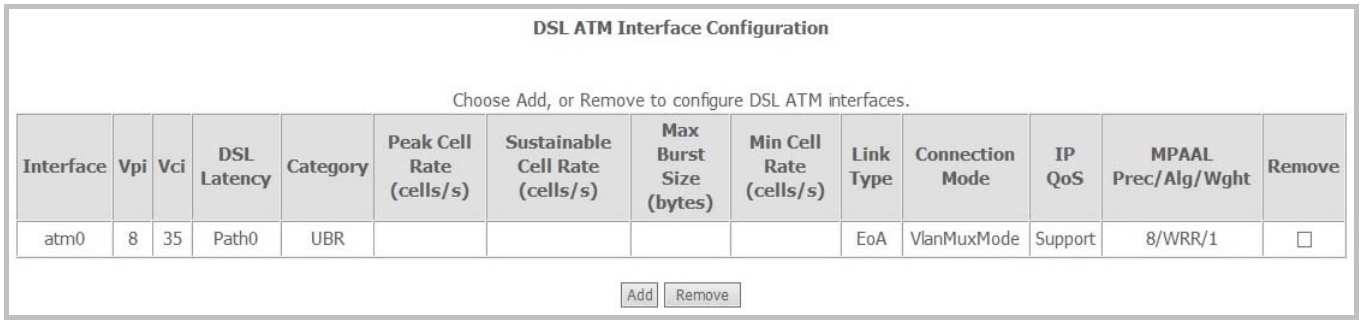


Figure 5-2-2

Click **Add** to add ATM Interface and the following page appears.

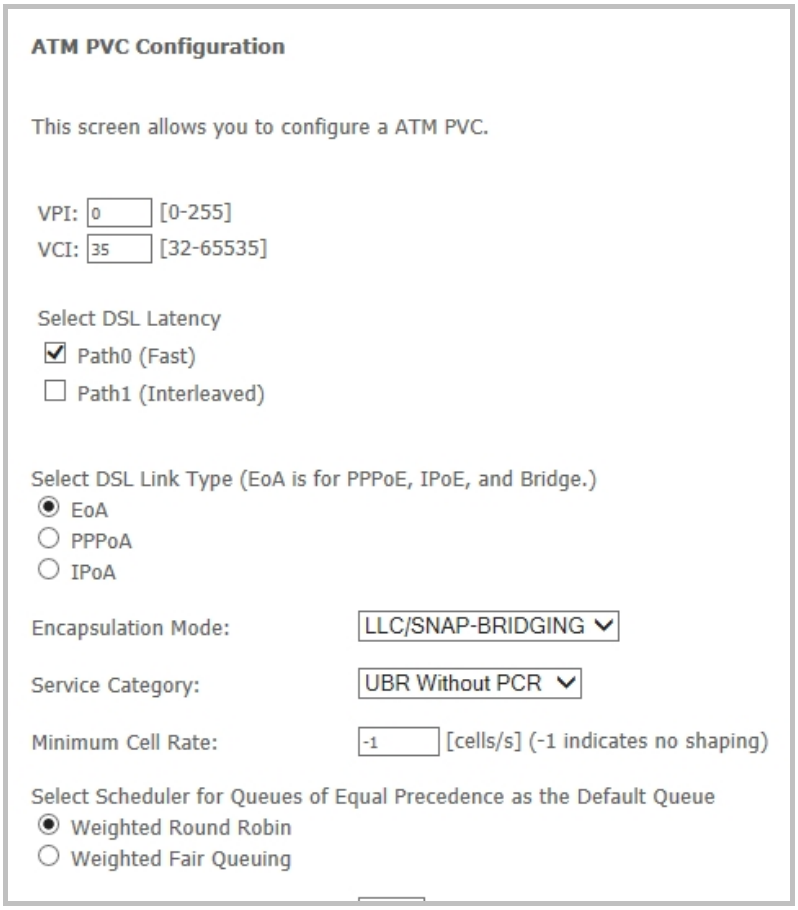


Figure 5-2-3

On this page, you can enter this PVC (VPI and VCI) value, and select DSL link type (EoA is for PPPoE, IPoE, and Bridge.), encapsulation mode and service category.

Object	Description
VPI (Virtual Path Identifier)	The virtual path between two points in an ATM network, and its valid value is from 0 to 255.
VCI (Virtual Channel Identifier)	The virtual channel between two points in an ATM network, ranging from 32 to 65535 (1 to 31 are reserved for known protocols).
DSL Link Type	EoA (It is for PPPoE, IPoE, and Bridge), PPPoA, or IPoA
Encapsulation Mode	LLC/SNAP-BRIDGING, or VC/MUX
Service Category	UBR Without PCR, UBR With PCR, CBR, Non Realtime VBR, Realtime VBR.
Select Scheduler for Queues of Equal Precedence as the Default Queue	Weighted Round Robin or Weighted Fair Queuing.

Click **Apply/Save** to save the configuration.

If you want to remove this Interface, please select the Remove check box and click **Remove**.

■ PTM Interface

Choose **Advanced Setup** > **Layer2 Interface > PTM Interface**, and the following page appears. On this page, you can add or remove to configure PTM WAN Interfaces.

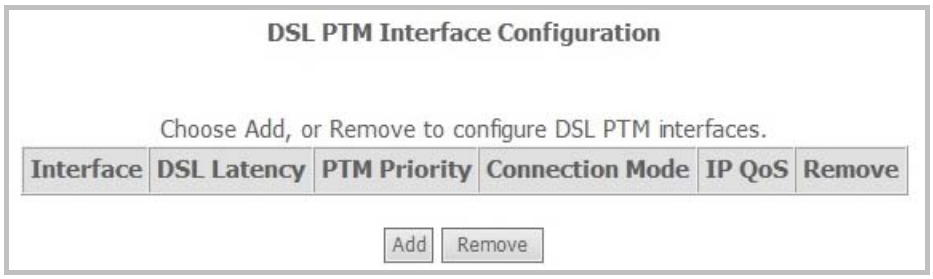


Figure 5-2-4

Click **Add** and the following page appears.

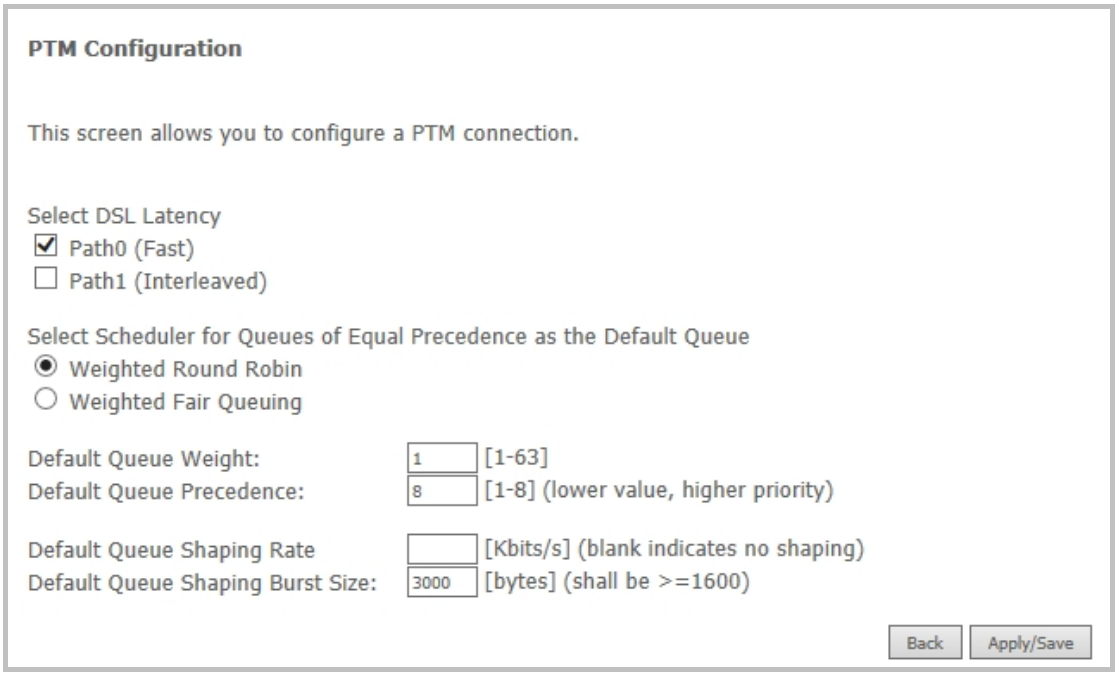


Figure 5-2-5

On this page, you can select scheduler for queues of equal precedence and enter the queue value. Click **Apply/Save** to save configuration.

■ ETH Interface

Choose **Advanced Setup** > **Layer2 Interface** > **ETH Interface** and the following page appears. On this page, you can add or remove to configure ETH WAN Interfaces.

Figure 5-2-6

Click **Add** and the following page appears.

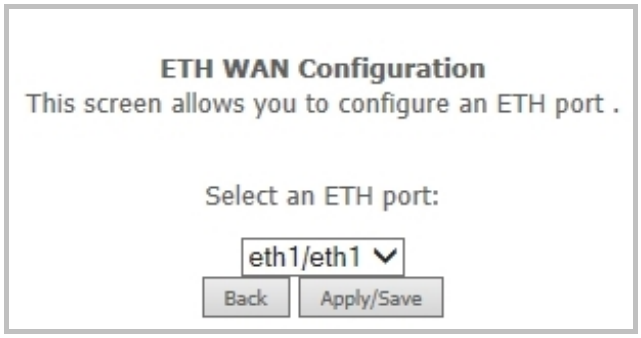


Figure 5-2-7

On this page, you can select an ETH port. Click **Apply/Save** to save configuration.

Note

If ETH Interface is selected, there are two WAN service types (PPPoE and IPoE).

5.2.2 WAN Service

Choose **Advanced Setup** > **WAN Service** and the following page appears.

Wide Area Network (WAN) Service Setup

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

Interface	Description	Type	Vlan802.1p	VlanMuxId	Igmp	NAT	Firewall	IPv4	IPv6	Mld	Remove	Edit	Action
atm0.1	br_0_8_35	Bridge	N/A	N/A	Disabled	Disabled	Disabled	Enabled	Enabled	Disabled	☐	edit	

Add Remove

Figure 5-2-8

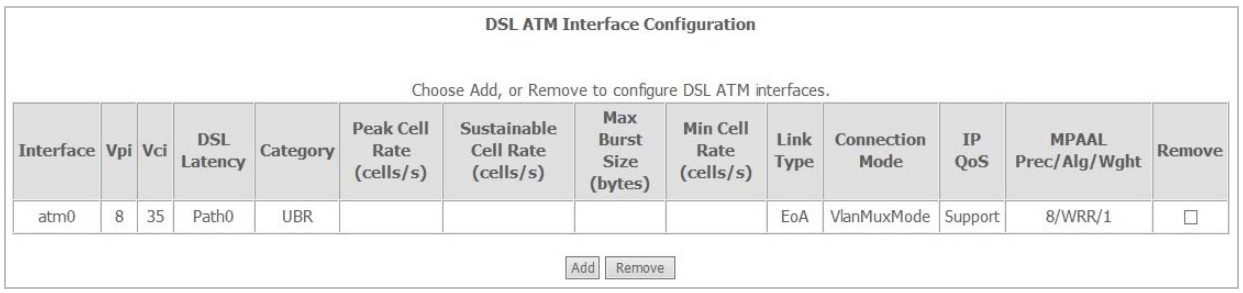
On this page, you are allowed to add, remove, or edit a WAN service.

If PTM Interface is selected, there are three WAN service types: **PPP over Ethernet (PPPoE)**, **IP over Ethernet**, and **Bridging**. And the corresponding configurations of PTM WAN service are the same as the configurations of ATM WAN service.

■ Adding a PPPoE WAN Service

This section describes the steps for adding the PPPoE WAN service.

Step1 First, add a proper ATM or PTM interface for this WAN service at **Layer2 Interface**.



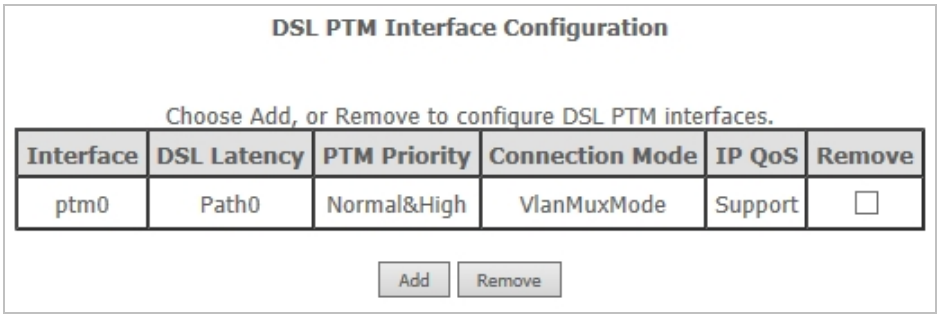
DSL ATM Interface Configuration

Choose Add, or Remove to configure DSL ATM interfaces.

Interface	Vpi	Vci	DSL Latency	Category	Peak Cell Rate (cells/s)	Sustainable Cell Rate (cells/s)	Max Burst Size (bytes)	Min Cell Rate (cells/s)	Link Type	Connection Mode	IP QoS	MPAAL Prec/Alg/Wght	Remove
atm0	8	35	Path0	UBR					EoA	VlanMuxMode	Support	8/WRR/1	☐

Add Remove

Figure 5-2-9



DSL PTM Interface Configuration

Choose Add, or Remove to configure DSL PTM interfaces.

Interface	DSL Latency	PTM Priority	Connection Mode	IP QoS	Remove
ptm0	Path0	Normal&High	VlanMuxMode	Support	☐

Add Remove

Figure 5-2-10

Step2 On the **WAN Service** page, click the **Add** button to display as **Figure 5-2-11 shows**. You can select ATM or PTM Interface for the WAN service and then click **Next**.

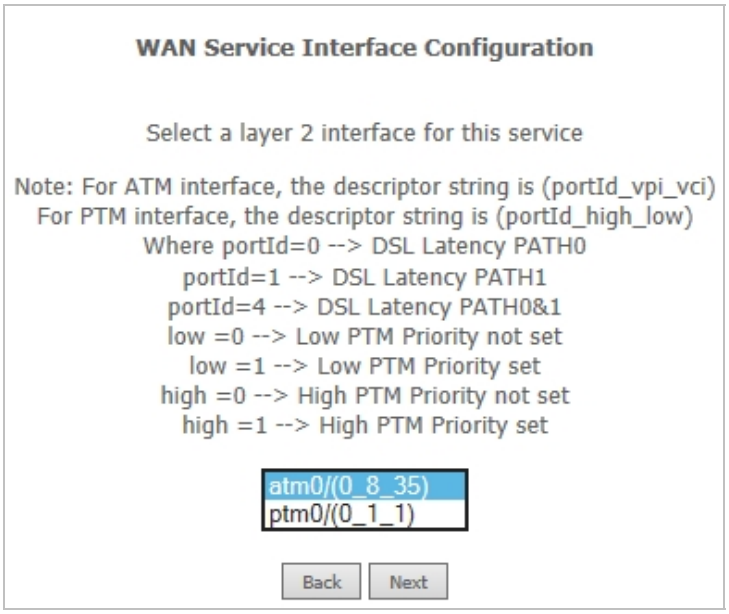


Figure 5-2-11

Step3 On this page, select the WAN service type to be **PPP over Ethernet (PPPoE)**. Click **Next** to continue the setting.

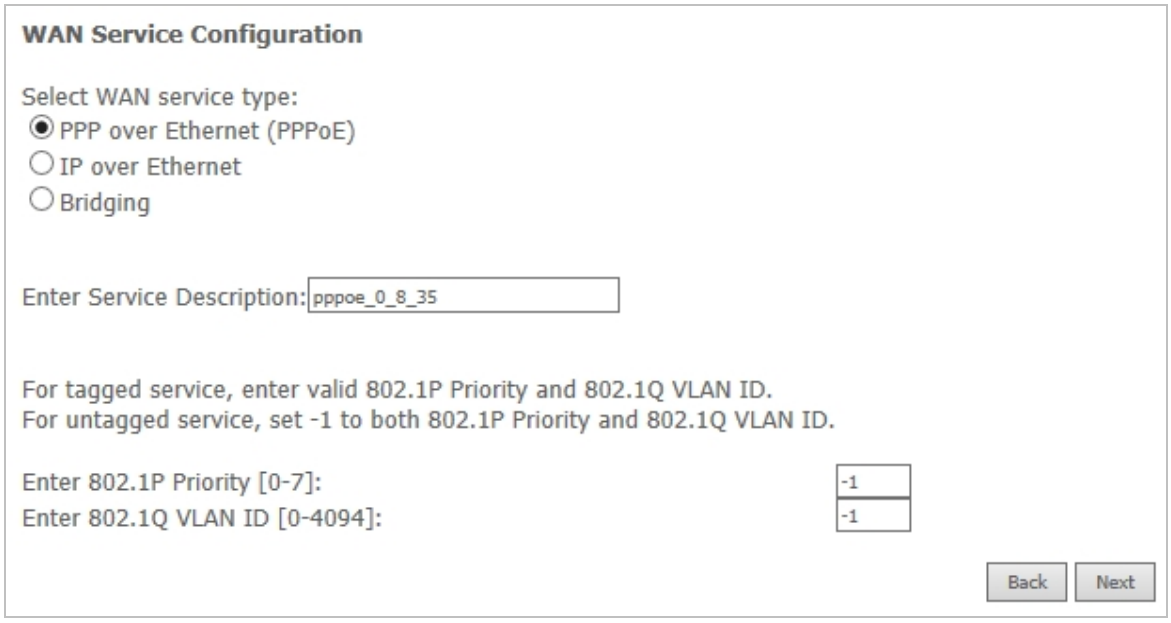


Figure 5-2-12

Step4 In this page, you can modify the PPP username, PPP password, PPPoE service name and authentication method.

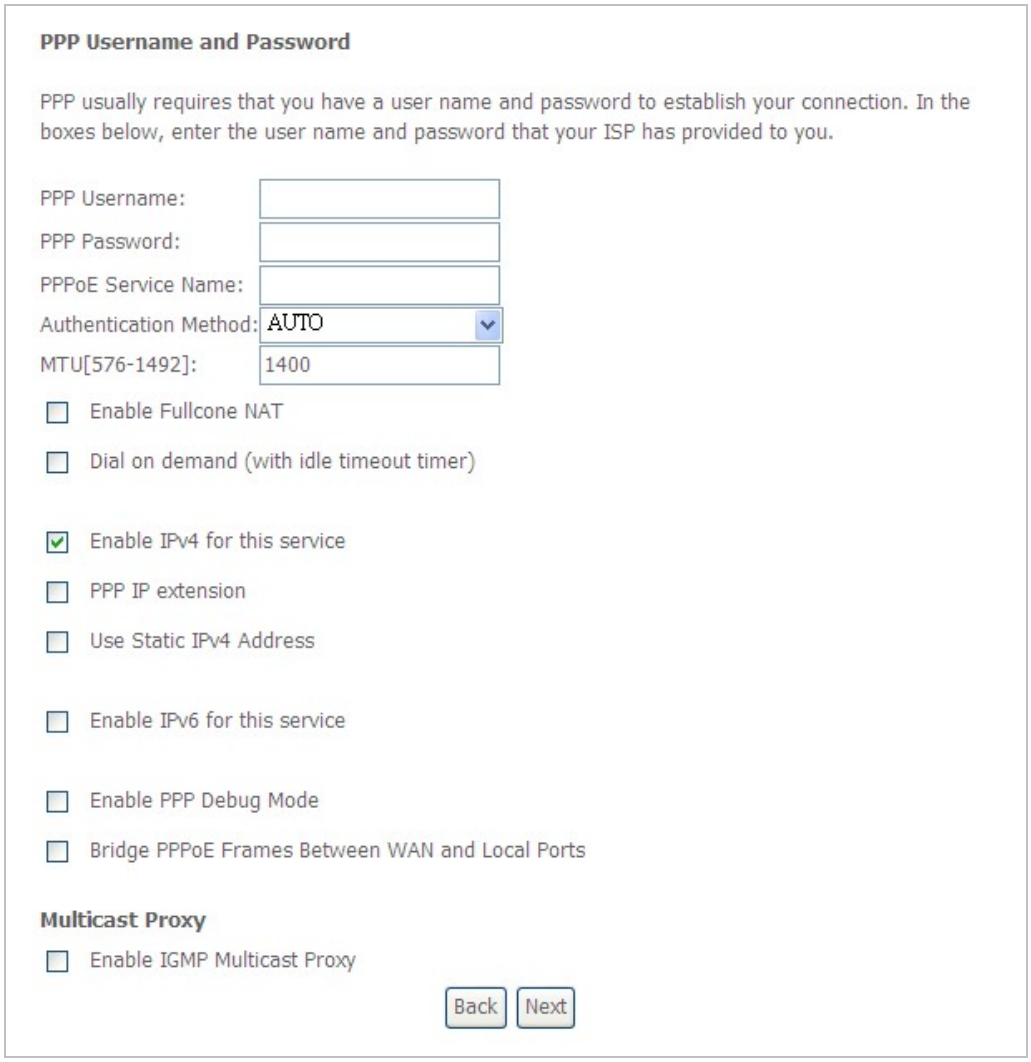


Figure 5-2-13

Object	Description
PPP Username	The correct user name provided by your ISP.
PPP Password	The correct password provided by your ISP.
PPPoE Service Name	If your ISP provides it to you, please enter it. If not, do not enter any information.
Authentication Method	The value can be AUTO, PAP, CHAP, or MSCHAP. Usually, you can select AUTO.
Enable Fullcone NAT	NAT is one where all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host, by sending a packet to the mapped external address.
Dial on demand (with idle timeout timer)	If this function is enabled, you need to enter the idle timeout time. Within the preset minutes, if the modem does not detect the flow of the user continuously, the modem automatically stops the PPPoE

	connection. Once it detects the flow (like access to a webpage), the modem restarts the PPPoE dialup. If this function is disabled, the modem performs PPPoE dial-up all the time. The PPPoE connection does not stop, unless the modem is powered off and DSLAM or uplink equipment is abnormal.
PPP IP extension	If you want to configure DMZ Host, you should enable it first.
Use Static IPv4 Address	If this function is disabled, the modem obtains an IP address assigned by uplink equipment such as BAS, through PPPoE dial-up. If this function is enabled, the modem uses this IP address as the WAN IP address.
Enable IPv6 for this service	Enable this function, you can use IPv6 service. It will also need you to check **Request IPv6 Address** and **Request Prefix Delegation**.
Enable PPP Debug Mode	Enable or disable this function.
Bridge PPPoE Frames Between WAN and Local Ports	Enable or disable this function.
Enable IGMP Multicast Proxy	If you want PPPoE mode to support IPTV, enable it.

Step5 After setting the parameters, click **Next** to display the following page. On this page, select a preferred WAN interface as the system default gateway.

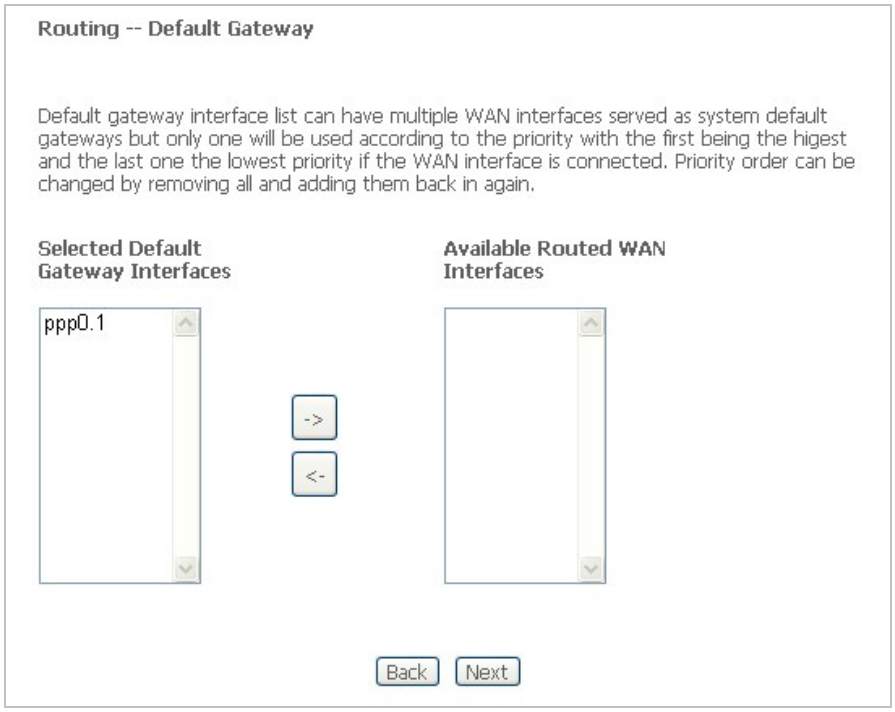


Figure 5-2-14

Step6 On this page, you can obtain the DNS server addresses from the selected WAN interface. Click **Next** to continue the setting.

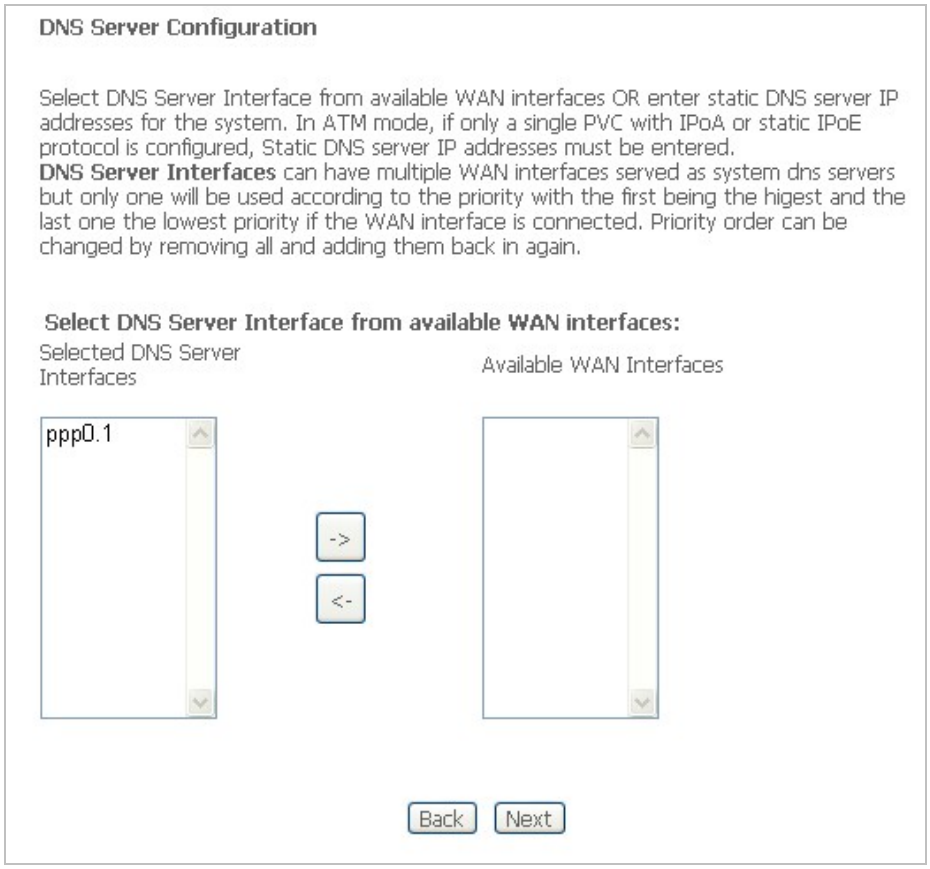


Figure 5-2-15

Step7 On this page, it displays the information about the PPPoE settings. Click **Apply/Save** to save and apply the settings.

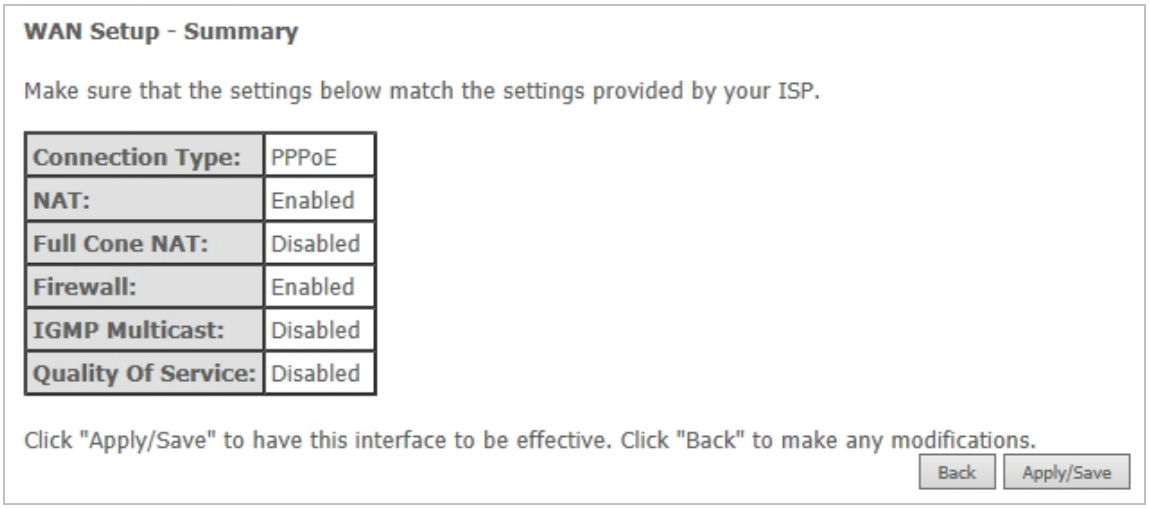


Figure 5-2-16

■ Adding an IP over Ethernet WAN service

This section describes the steps for adding the IP over Ethernet WAN service.

Step1 First, add a proper ATM or PTM interface for this WAN service at **Layer2 Interface**.

Step2 On the **WAN Service** page, click the **Add** button to display as **Figure 5-2-11** shows. You can select ATM or PTM Interface for the WAN service and then click **Next**.

Step3 On this page, select the WAN service type to be **IP over Ethernet**. Click **Next** to continue the setting.

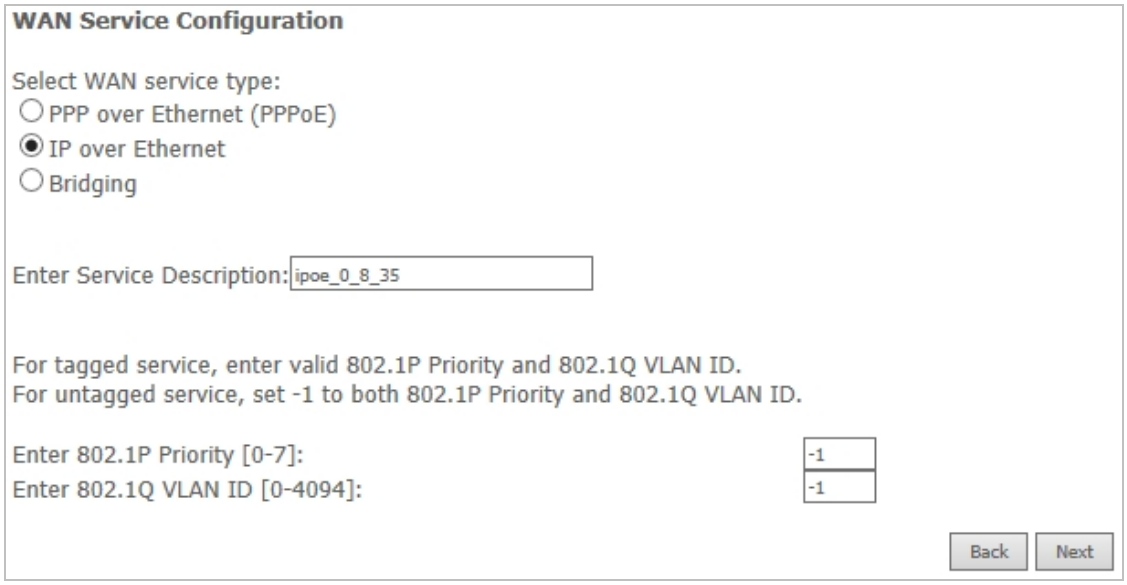


Figure 5-2-17

Step4 On this page, you may modify the WAN IP settings. You may select obtain an IP address automatically or manually enter the IP address provided by your ISP.

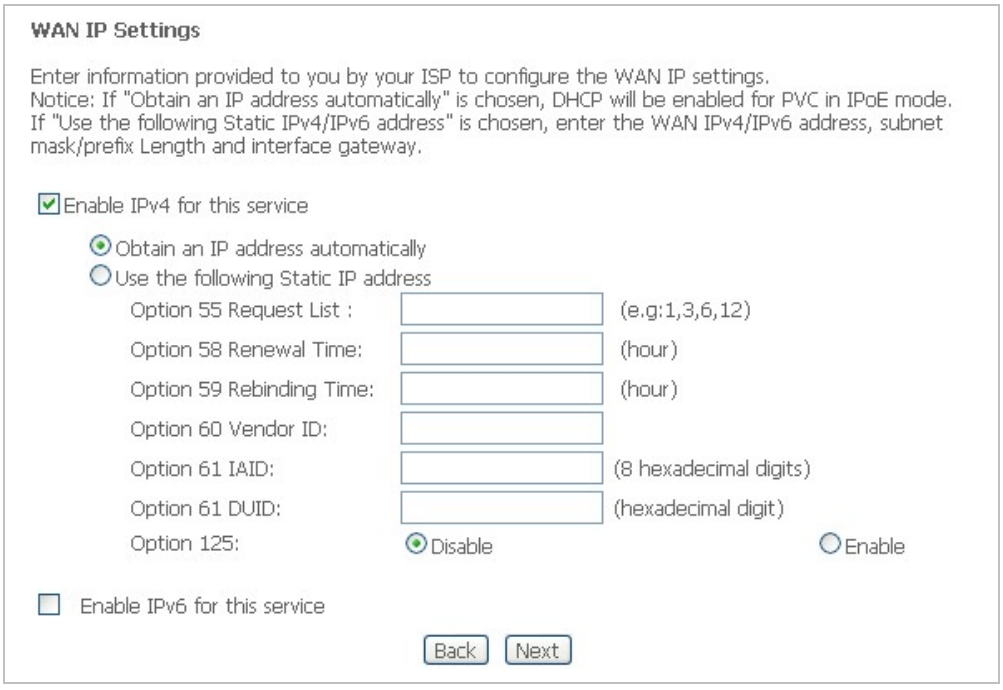


Figure 5-2-18

Note

If **Obtain an IP address automatically** is selected, DHCP will be enabled for PVC in IP over Ethernet mode.

If **Use the following Static IP address** is selected, please enter the WAN IP address, subnet mask and gateway IP address.

Step5 On this page, you can set the network address translation settings, for example, enabling NAT, enabling firewall, and enabling IGMP multicast. After finishing setting, click **Next**.

Figure 5-2-19

Step6 On this page, select a preferred WAN interface as the system default gateway.

Step7 On this page, you can obtain the DNS server addresses from the selected WAN interface. Click **Next** to continue the setting.

Step8 On this page, it displays the information about the IP over Ethernet settings. Click **Apply/Save** to save and apply the settings.

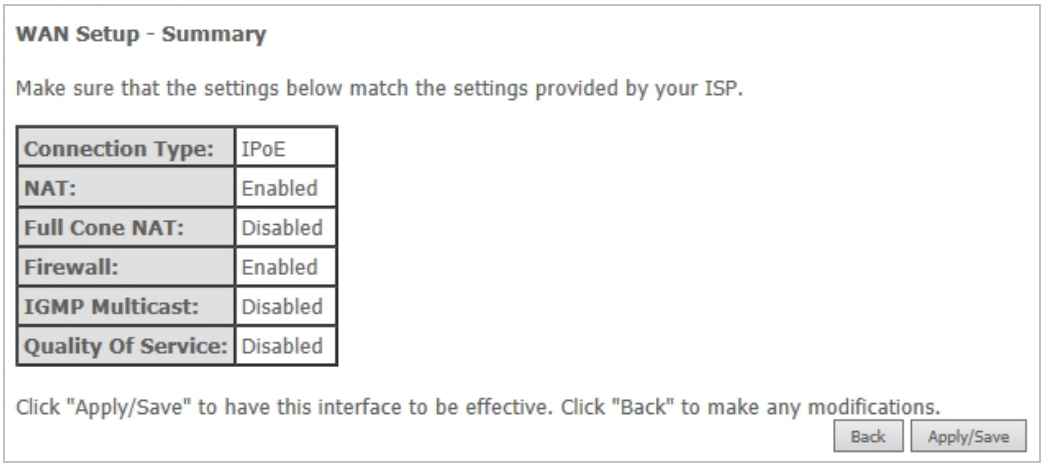


Figure 5-2-20

■ Adding a Bridging WAN service

This section describes the steps for adding the Bridging WAN service.

Step1 First, add a proper ATM or PTM interface for this WAN service at **Layer2 Interface**.

Step2 On the **WAN Service** page, click the **Add** button to display as **Figure 5-2-11**. You can select ATM or PTM Interface for the WAN service and then click **Next**.

Step3 On this page, select the WAN service type to be **Bridging**. Click **Next** to finish the setting.

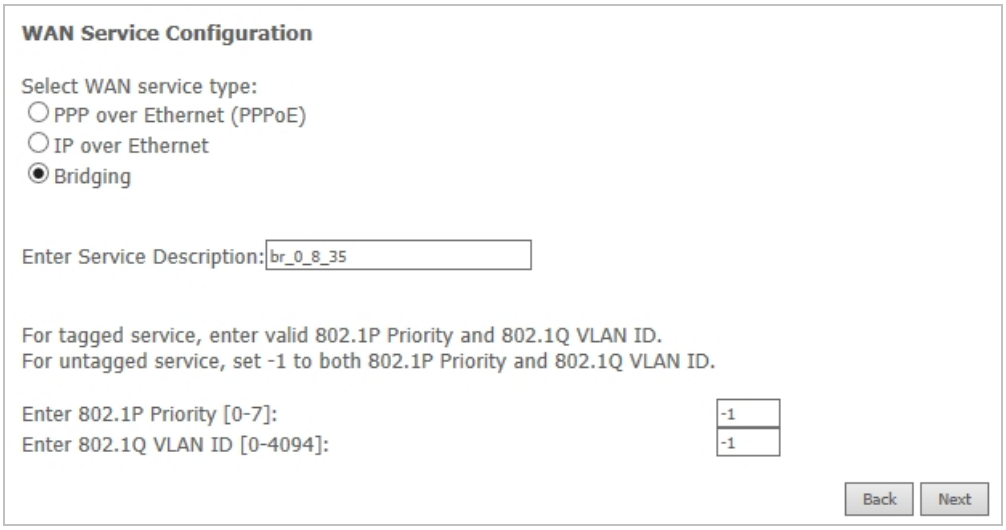


Figure 5-2-21

Step4 On this page, it displays the information about the bridge settings. Click **Apply/Save** to save and apply the settings. You can modify the settings by clicking the **Back** button if necessary.

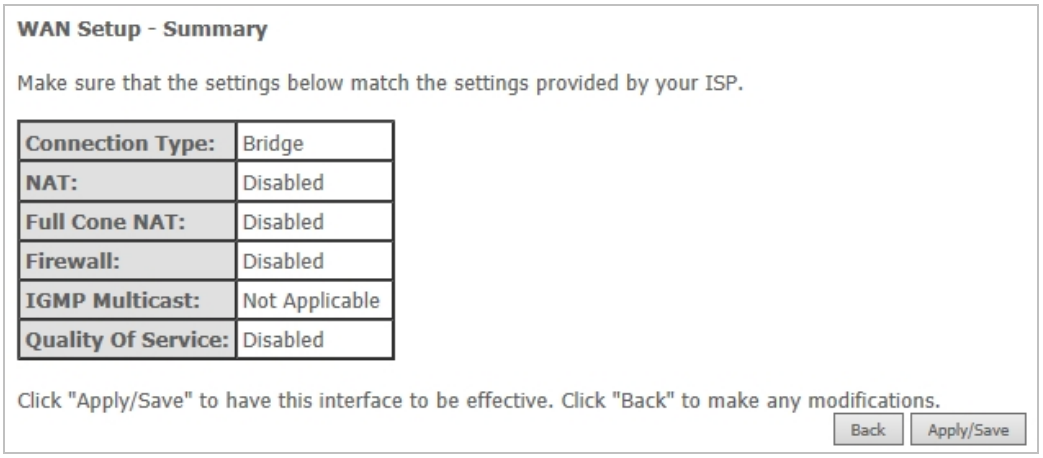


Figure 5-2-22

■ Adding a PPPoA WAN service

This section describes the steps for adding the PPPoA WAN service.

Step1 Choose **Advanced Setup > Layer2 Interface > ATM Interface** to dsiplay the ATM Interface Configuration page. On this page, you need to add a PVC for PPPoA mode. Click the **Add** button on the **ATM Interface Configuration** page to display the following page.

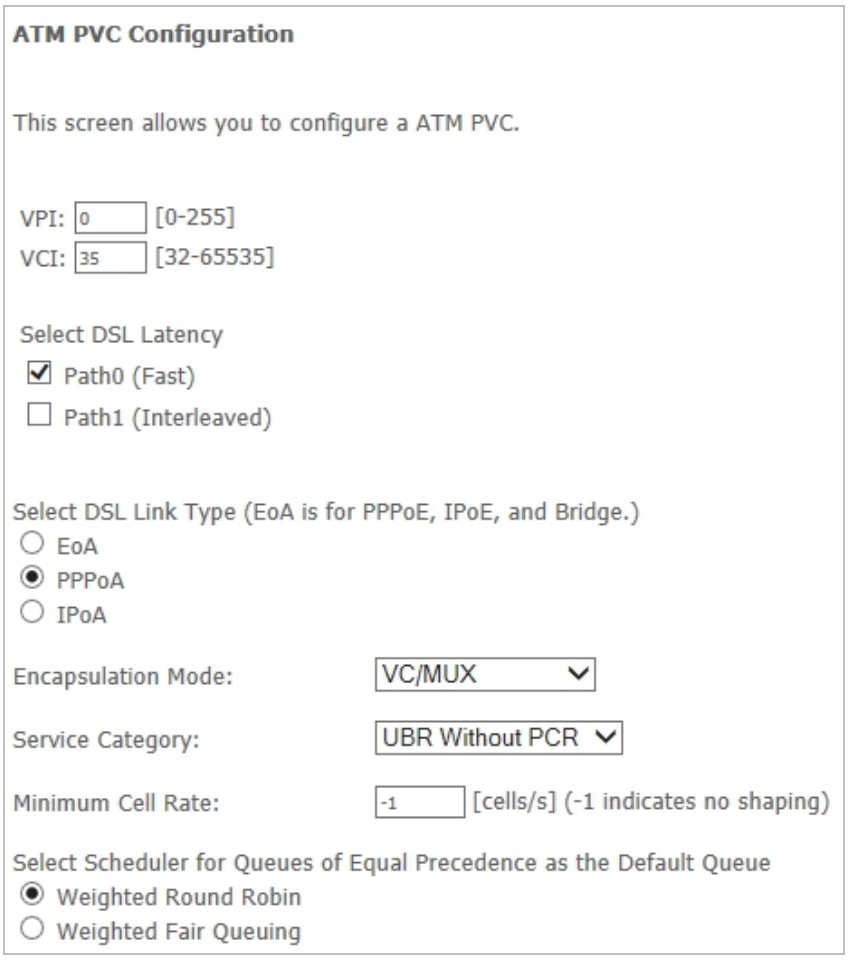


Figure 5-2-23

Step2 Select the DSL link type to be **PPPoA** and select the encapsulation mode to be **VC/MUX** (according to the uplink equipment). After finishing setting, click the **Apply/Save** button to apply the settings.

Step3 Choose **WAN Service** and click **Add** to display the following page.

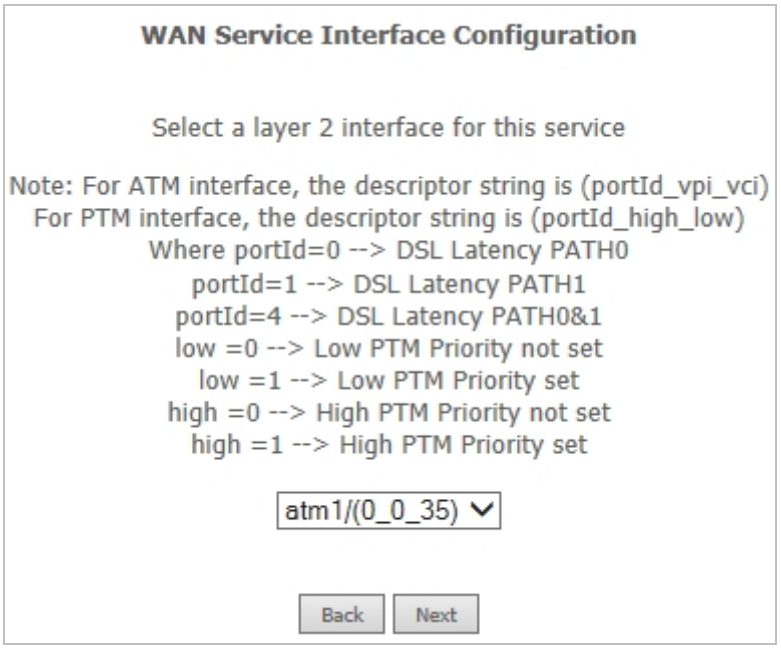


Figure 5-2-24

Step4 Select the proper interface for the WAN service and then click **Next** to display the following page.

Figure 5-2-25

Step5 On this page, you may modify the service description. Click **Next** to display the following page. You can enter the **PPP username** and **PPP password** provided by your ISP. Select the authentication method according to your requirement.

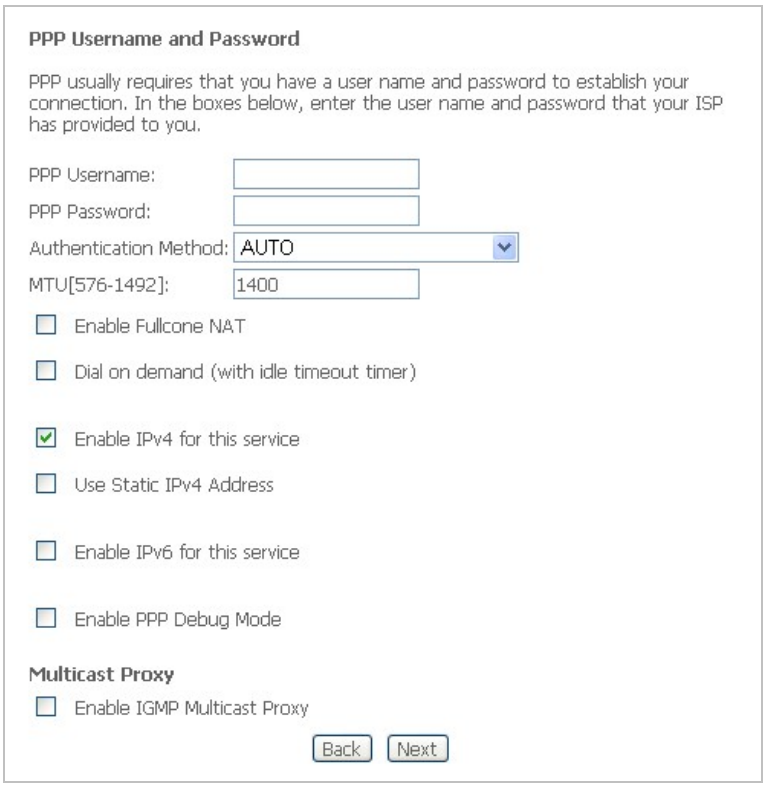


Figure 5-2-26

Object	Description
PPP Username	The correct user name provided by your ISP.
PPP Password	The correct password provided by your ISP.
Authentication Method	The value can be AUTO, PAP, CHAP, or MSCHAP. Usually, you can select AUTO.
Enable Fullcone NAT	NAT is one where all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host, by sending a packet to the mapped external address.
Dial on demand (with idle timeout timer)	If this function is enabled, you need to enter the idle timeout time. Within the preset minutes, if the modem does not detect the flow of the user continuously, the modem automatically stops the PPPoA connection. Once it detects the flow (like access to a webpage), the modem restarts the PPPoA dialup. If this function is disabled, the modem performs PPPoA dial-up all the time. The PPPoA connnection does not stop, unless the modem is powered off and DSLAM or uplink equipment is abnormal.
Enable IPv4 for this service	Enable this function, you can use Static IPv4 service.
Use Static IPv4 Address	If this function is disabled, the modem obtains an IP address assigned

	by an uplink equipment such as BAS, through PPPoA dial-up. If this function is enabled, the modem uses this IP address as the WAN IP address.
Enable IPv6 for this service	Enable this function, you can use IPv6 service. It will also need you to check **Request IPv6 Address** and **Request Prefix Delegation**.
Enable PPP Debug Mode	Enable or disable this function.
Enable IGMP Multicast Proxy	If you want PPPoA mode to support IPTV, enable it.

Step6 On this page, select a preferred WAN interface as the system default gateway and then click **Next**.

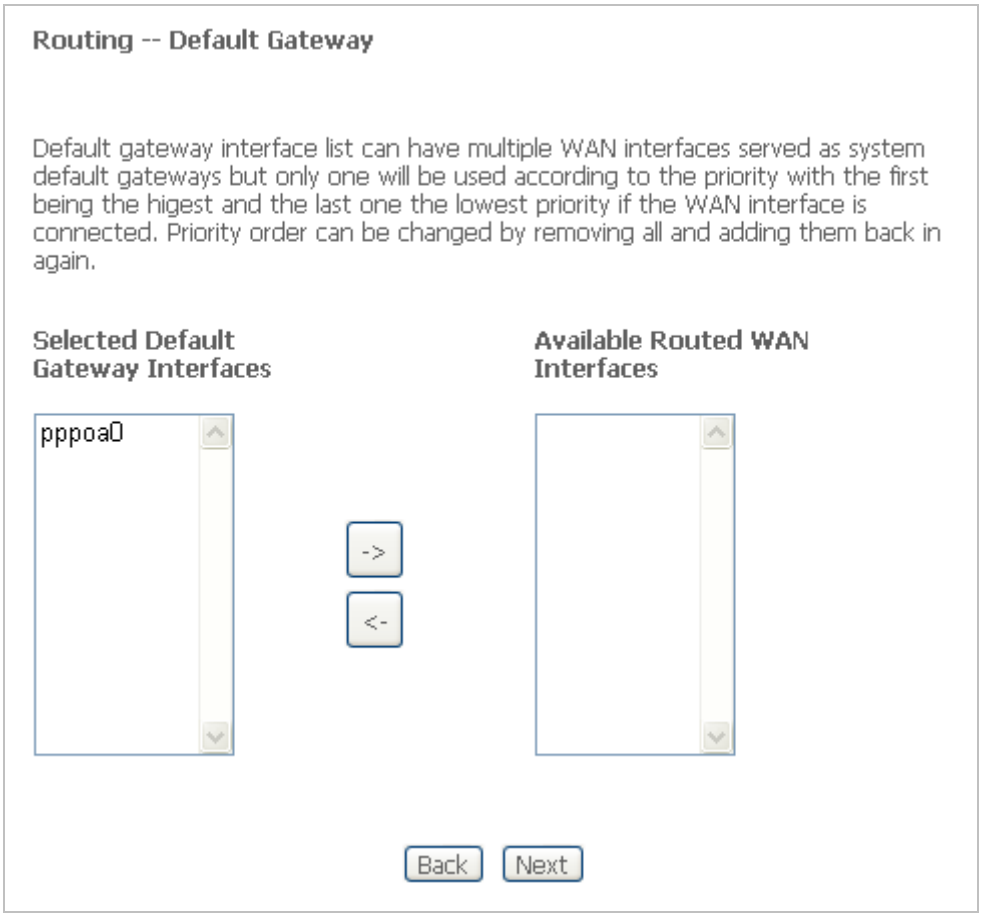


Figure 5-2-27

Step7 On this page, you can obtain the DNS server addresses from the selected WAN interface. After finishing setting, click **Next**.

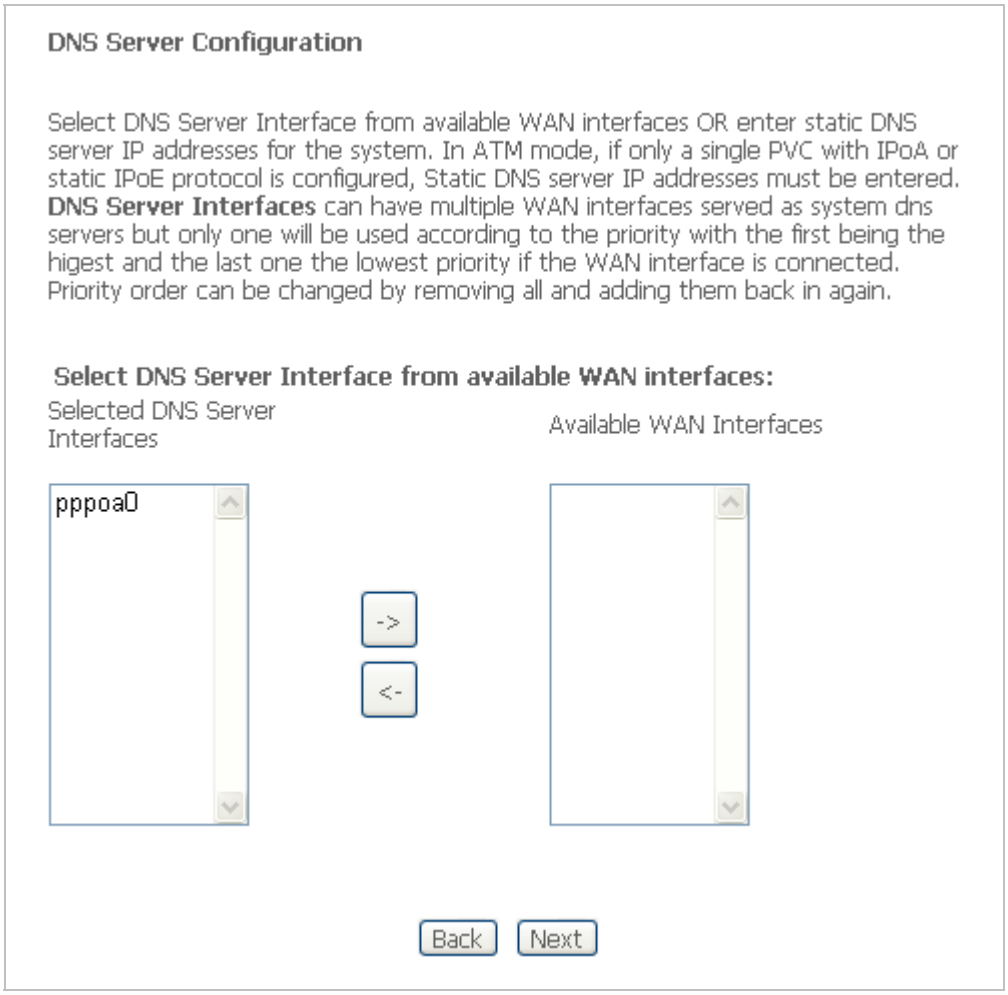


Figure 5-2-28

Step8 On this page, it displays the information about the PPPoA settngs. Click **Apply/Save** to apply the settings. You can modify the settings by clicking the **Back** button if necessary.

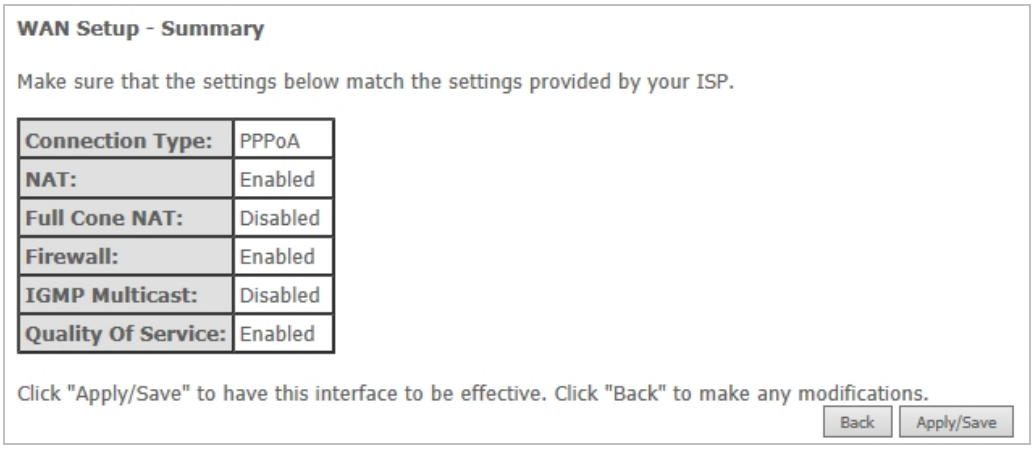


Figure 5-2-29

■ Adding an IPoA WAN service

This section describes the steps for adding the IPoA WAN service.

Step1 Choose **Advanced Setup > Layer2 Interface > ATM Interface** to dsiplay the **DSL ATM Interface Configuration** page. On this page, you need to add a PVC for IPoA mode. Click the **Add** button.

Step2 Select the DSL link type to be **IPoA**, and select the encapsulation mode to be **LLC/SNAP-ROUTING** (according to the uplink equipment). After finishing setting, click the **Apply/Save** button to save the settings

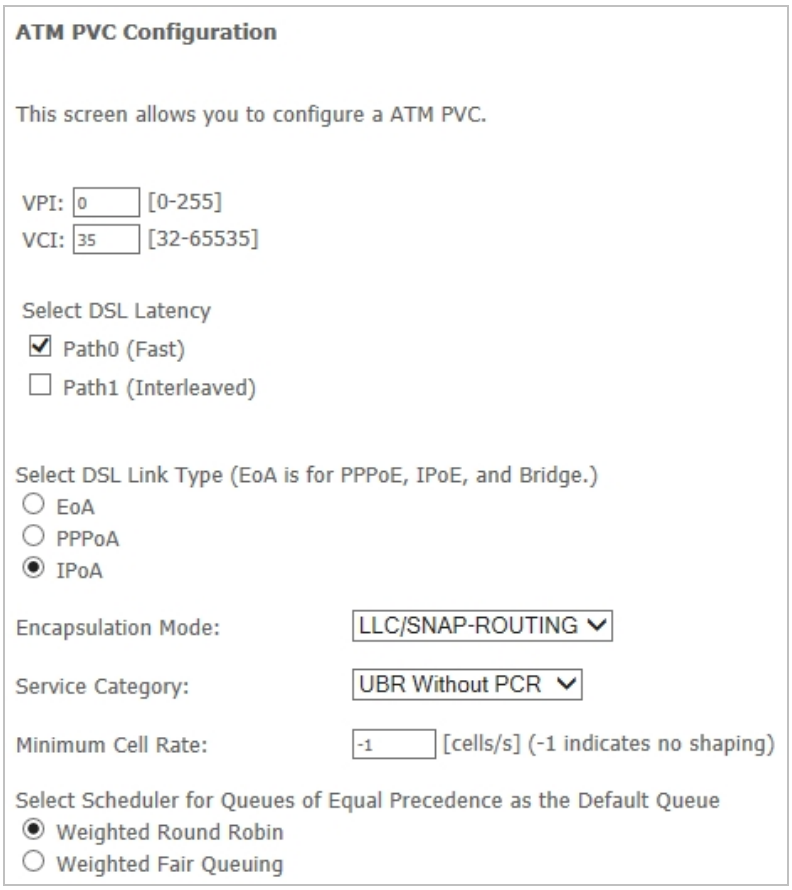


Figure 5-2-30

Step3 Choose **WAN Service** and click **Add** to display the following page.

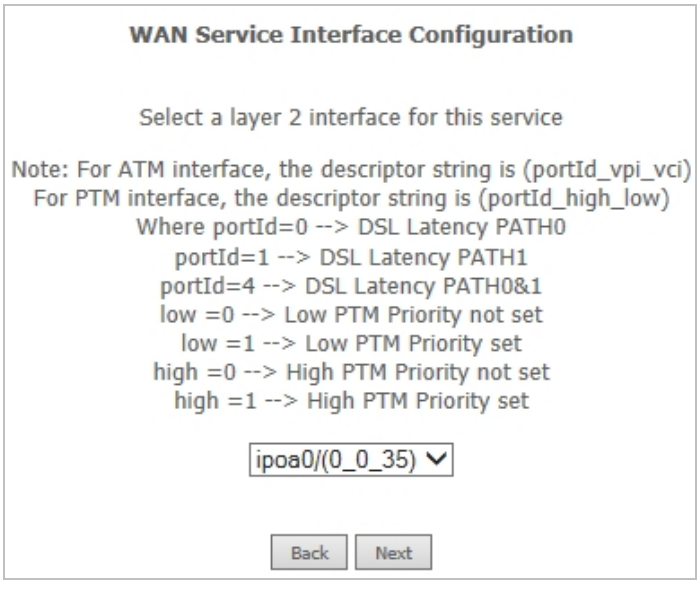


Figure 5-2-31

Step4 Select the proper interface for the WAN service and then click **Next** to display the following page.

Figure 5-2-32

Step5 On this page, you may modify the service description. Enter the WAN IP address, the WAN subnet mask, and primary DNS server provided by your ISP.

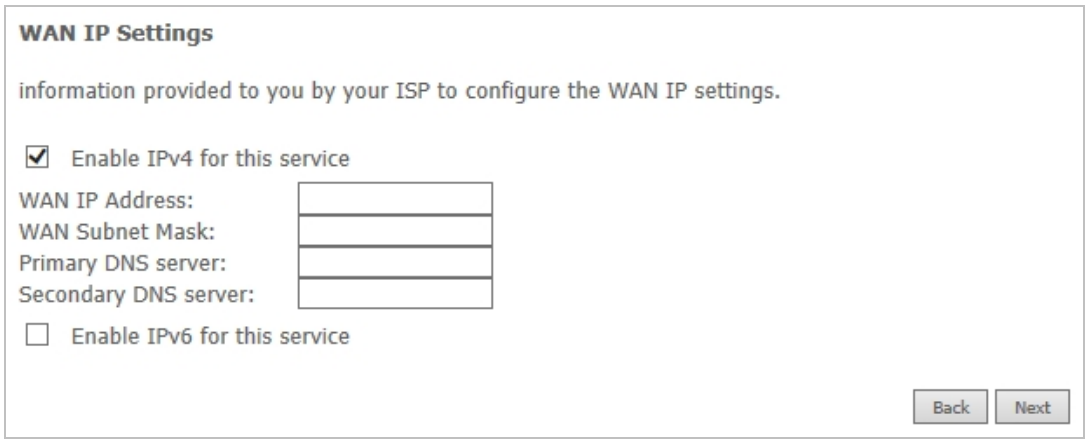


Figure 5-2-33

Step6 If you do not want to enable NAT, and wish the user of modem to access the Internet normally, you need to add a route on the uplink equipment. Otherwise, the access to the Internet fails. Normally, please enable the NAT function. After finishing setting, click **Next.**

Figure 5-2-34

Step7 Select a preferred WAN interface as the system default gateway and then click **Next.**

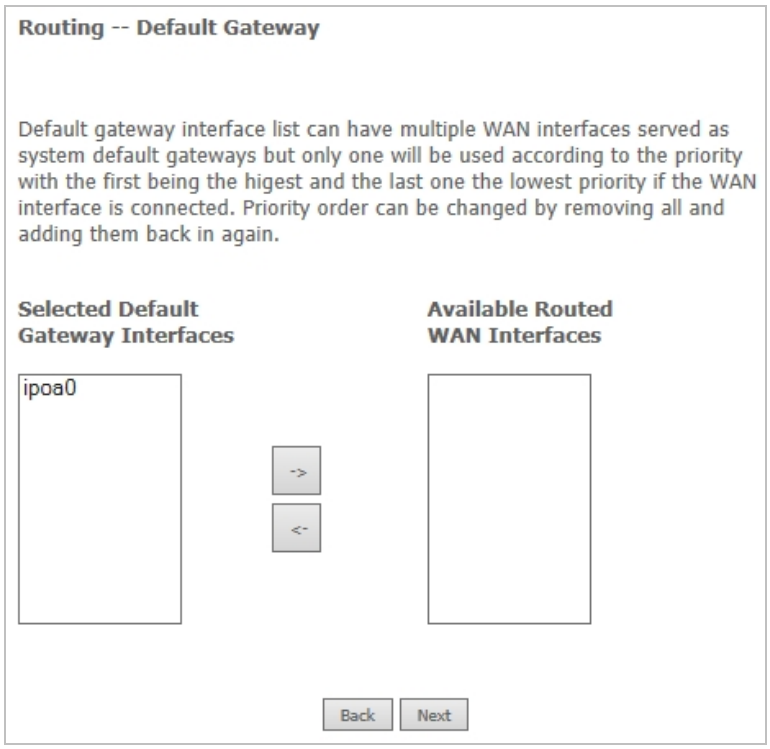


Figure 5-2-35

Step8 On this page, you can obtain the DNS server addresses from the selected WAN interface. After finishing setting, click **Next.**

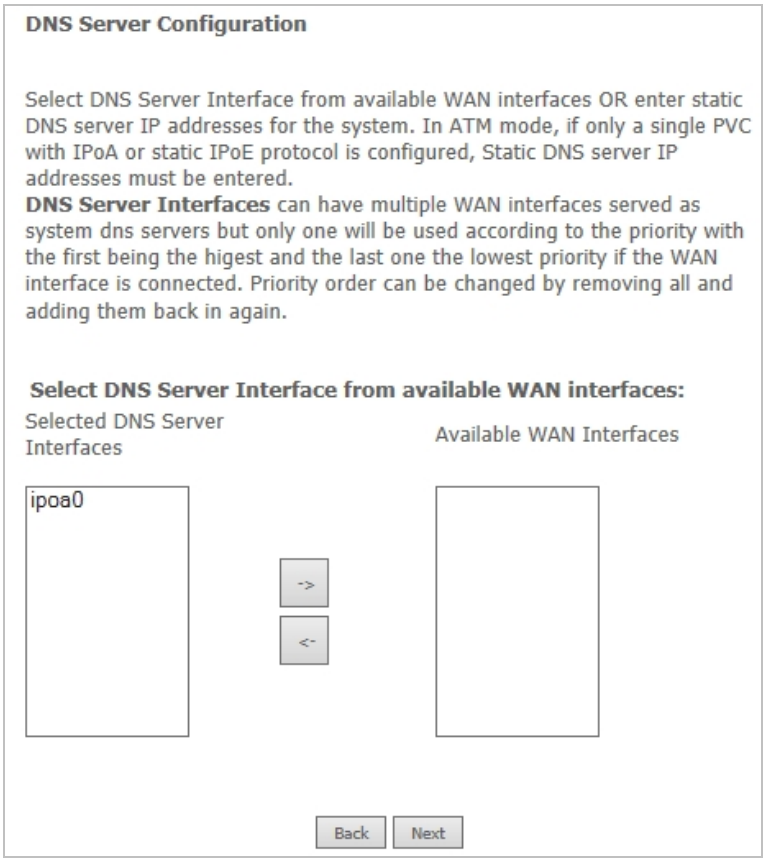


Figure 5-2-36

Step9 On this page, it displays the information about the IPoA settngs. Click **Apply/Save** to save and apply the settings. You can modify the settings by clicking the **Back** button if necessary.

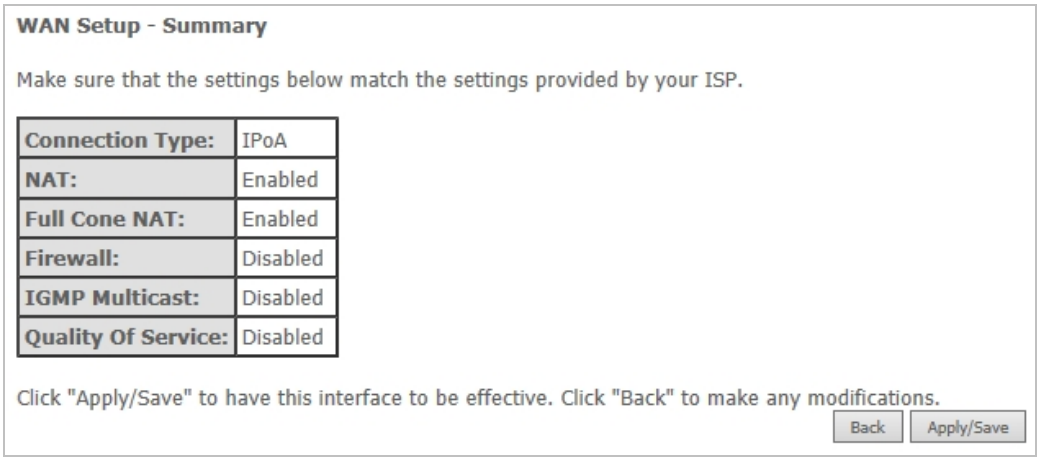


Figure 5-2-37

5.2.3 3G WAN Service

Choose **Advanced Setup > 3G WAN Service** and the following page appears.

Figure 5-2-38

This page is used to configure 3G connection. If you want to access the Internet through 3G connection, a 3G network card is required. Connect the 3G network card to the USB interface of the Router.

Object	Description
Information	Click it to display the information of the 3G network card.
Pin Manage	Click it to configure the 3G PIN.
Upload Driver	For an un-support USB dongle, click it to upload the new driver for supporting the USB. The driver is a text file.

Click **Add** in the **WAN Service for 3 G Mobile Setup** to display the following page.

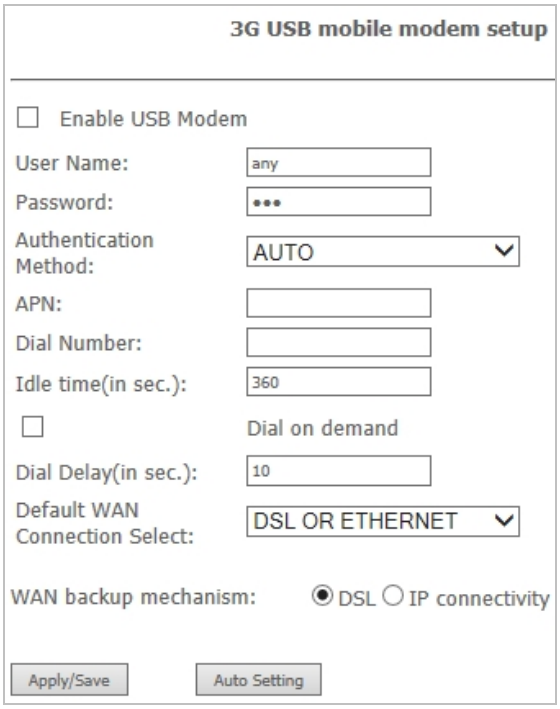


Figure 5-2-39

On this page, you are allowed to configure the settings of the 3G USB modem.

Object	Description	
Enable USB Modem	If you want to access the Internet through the 3G network card, you must enable the USB modem.	
User Name	Username provided by your 3G ISP.	
Password	Password provided by your 3G ISP.	
Authentication Method	Select a proper authentication method in the drop- down list. You can select Auto, PAP, CHAP, or MSCHAP.	
APN	APN (Access Point Name) is used to identify the service type. Enter the APN provided by your 3G ISP.	
Dial Number	Enter the dial number provided by your 3G ISP.	
Idle time (in sec.)	If no traffic for the present time, the 3G will disconnect automatically.	
Dial on demand	Within the preset minutes, if the modem does not detect the flow of the user continuously, the modem automatically stops the 3G connection. Once it detects the flow (like access to a webpage), the modem restarts the 3G dialup.	
Dial Delay (in sec.)	The 3G delays dial after the DSL is disconnected.	
Default WAN Connection Select	You can select DSL OR ETHERNET or 3G from the drop-down list.	
WAN back mechanism	The 3G connection is backup for the DSL connection.	**DSL:** If the DSL is disconnected, the 3G starts to dial.
		IP connectivity: If the system fails to ping the specified IP address, the 3G starts to dial.

After finishing setting, click the **Apply/Save** button to save the settings.

You may also click the **Auto Setting** button to automatically configure the 3G connection.

After clicking the **Apply/Save** button, the following page appears.

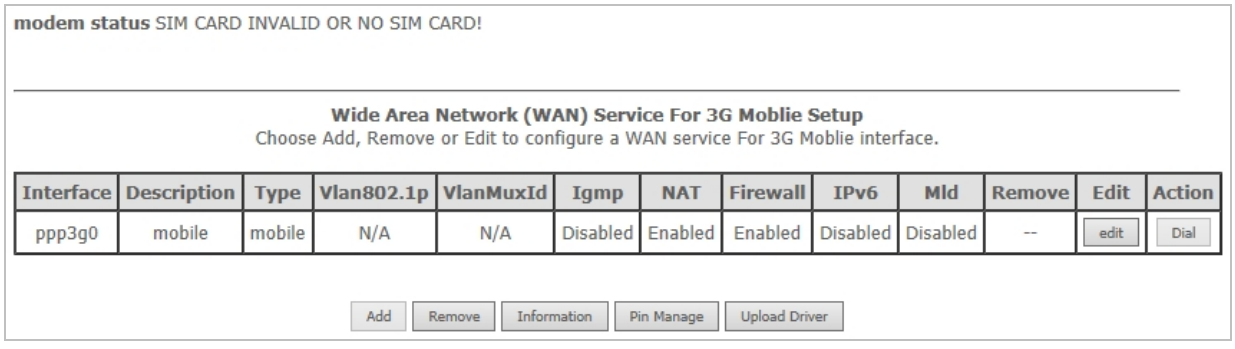


Figure 5-2-40

If the 3G network card is installed, you may click the button on the **Action** column to establish or disconnect the 3G connection.

When there is no DSL WAN connection, insert the 3G network card, and then system will perform dial-up automatically. If the DSL WAN connection and the 3G connection coexist, the DSL WAN connection takes priority over the 3G connection. When the DSL WAN connection starts to perform dial-up, the 3G connection will be disconnected. If the DSL WAN connection has established, you may manually to perform 3G dial-up, and then the DSL WAN connection will be disconnected.

5.2.4 LAN Configuration

Choose **Advanced Setup > LAN** and the following page appears.

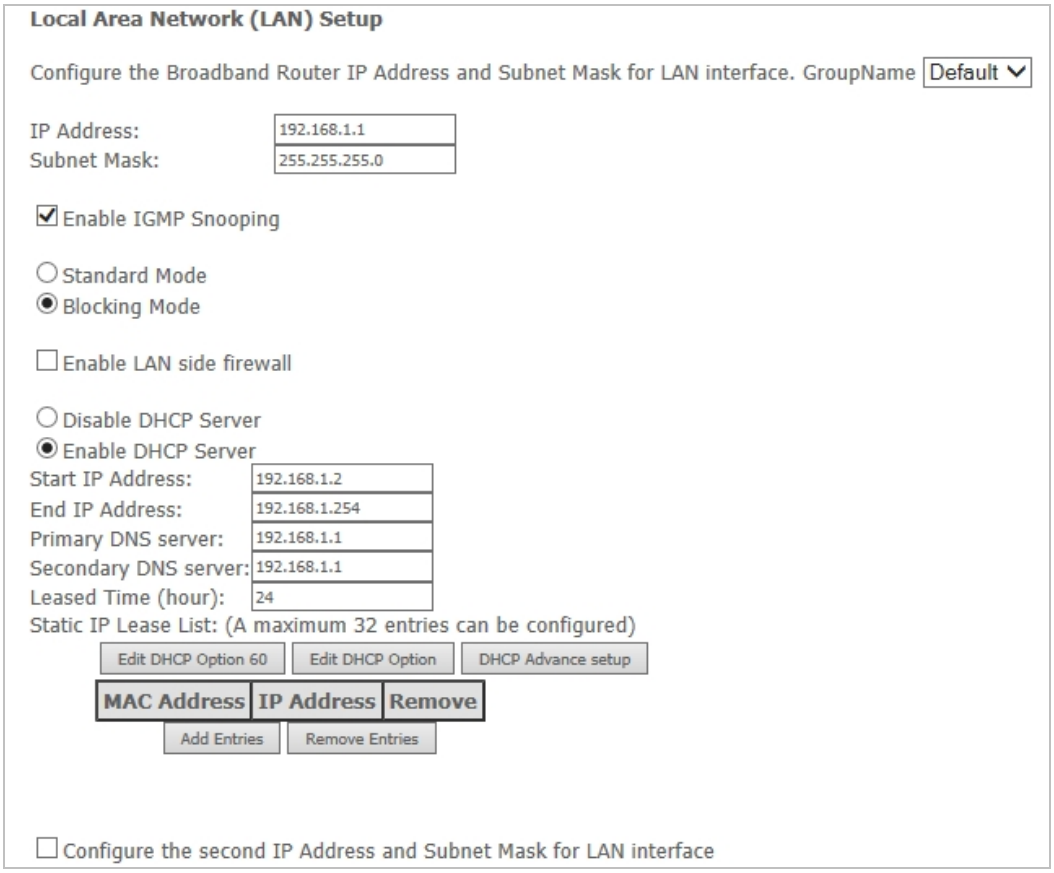


Figure 5-2-41

On this page, you can configure an IP address for the DSL router, enable IGMP snooping, enable or disable the DHCP server, edit the DHCP option, configure the DHCP advanced setup and set the binding between a MAC address and an IP address.

Configuring the Private IP Address for the DSL Router

Object	Description
IP Address	The default IP address is 192.168.1.1.
Subnet Mask	The default Subnet Mask is 255.255.255.0.
Enable IGMP Snooping	IGMP snooping enables the router to forward multicast traffic intelligently, instead of flooding all ports in the VLAN. With IGMP snooping, the router listens to IGMP membership reports, queries and leave messages to identify the switch ports that are members of multicast groups. Multicast traffic will only be forwarded to ports identified as members of the specific multicast group or groups..
Enabling the LAN Side Firewall	Firewall can prevent unexpected traffic on the Internet from your host in the LAN. Enable or disable the LAN side firewall.

DHCP Server	**Disable DHCP Server:** If the DHCP server is disabled, you need to manually set the start IP address, end IP address and the lease time for the clients in the LAN.
	Enable DHCP Server: If you enable the DHCP sever, the clients will automatically acquire the IP address from the DHCP server.
Edit DHCP Option60	You can add, edit or delete the DHCP60 options.
Edit DHCP option	You can add, edit or delete the DHCP options, and these options will be sent to the DHCP client.
DHCP Advance setup	You can enable or disable DHCP for every LAN interface.
Add Entries	Enter the MAC address of the LAN host and the static IP address that is reserved for the host
Remove Entries	Remove the entries you set.
Configuring the Second IP Address and Subnet Mask for a LAN Interface	After enabling Configure the second IP Address and Subnet Mask for LAN interface, enter an IP address and a subnet mask for the LAN interface.

■ IPv6 Auto-configuration

Click **Advanced Setup > LAN >IPv6 Autoconfig** and the following page appears.

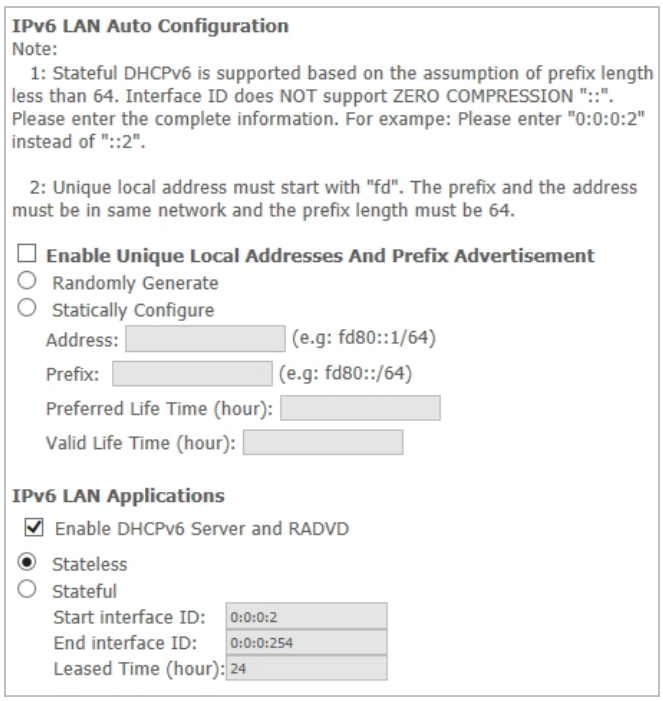


Figure 5-2-42

On this page, you can set an IP address for the DSL IPv6 router, enable the DHCPv6 server, enable RADVD and enable the MLD snooping function.

Object	Description
DHCPv6 Server	WIDE-DHCPv6 is an open-source implementation of dynamic host configuration protocol for IPv6 (DHCPv6) originally developed by the KAME project. The implementation mainly complies with the following standards: RFC3315, RFC3319, RFC3633, RFC3646, RFC4075, RFC 4272 etc.
Enable RADVD	The router advertisement daemon (RADVD) is run by Linux or BSD systems acting as IPv6 routers. It sends router advertisement messages, specified by RFC2461, to a local Ethernet LAN periodically and when requested by a node sending a router solicitation message. These messages are required for IPv6 stateless auto-configuration.
Enable MLD Snooping	Multicast Listener Discovery Snooping (MLD Snooping) is an IPv6 multicast constraining mechanism that runs on Layer 2 devices to manage and control IPv6 multicast groups. By analyzing received MLD messages, a Layer 2 device running MLD Snooping establishes mappings between ports and multicast MAC addresses and forwards IPv6 multicast data based on these mappings

After finishing setting, click the **Save/Apply** button to apply the settings.

5.2.5 NAT

■ Virtual Servers

Firewall can prevent unexpected traffic on the Internet from your host on the LAN. The virtual server can create a channel that can pass through the firewall. In that case, the host on the Internet can communicate with a host on your LAN within certain port range.

Choose **Advanced Setup > NAT > Virtual Servers** and the following page appears.

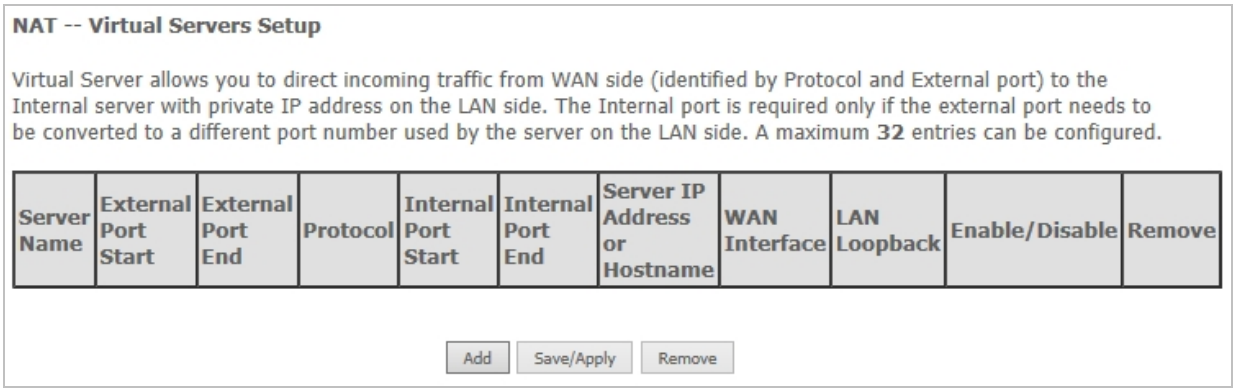


Figure 5-2-43

On this page, you are allowed to add or remove a virtual server entry. To add a virtual server, do as follows:

Click the **Add** button to display the following page.

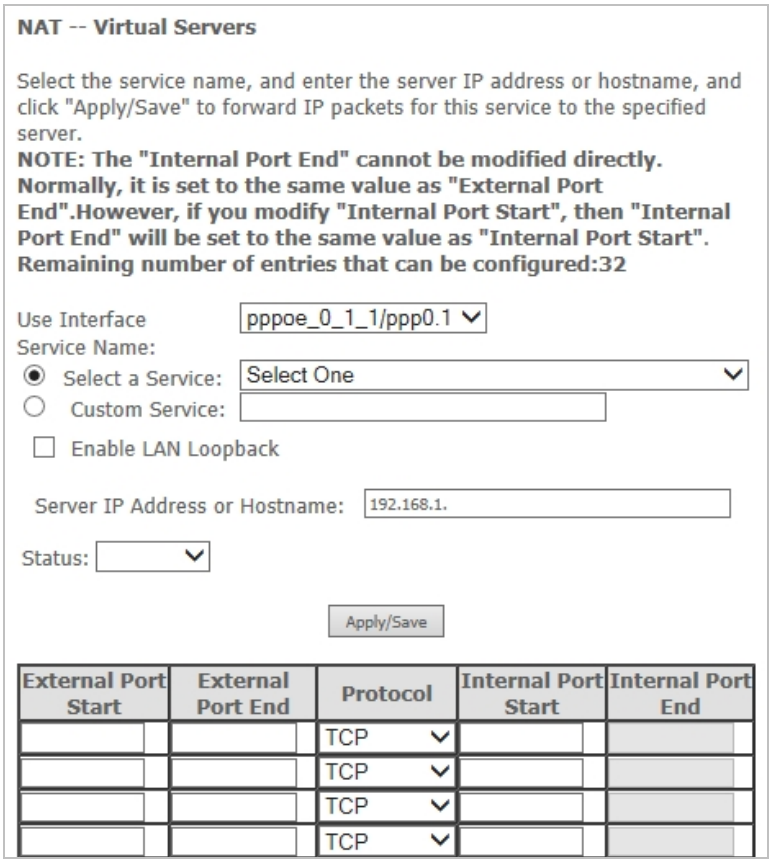


Figure 5-2-44

Object	Description
Use Interface	Select an interface that you want to configure
Select a Service	Select a proper service in the drop-down list.
Custom Server	Enter a new service name to establish a user service type.
Server IP Address	Assign an IP address to virtual server.
External Port Start	When selecting a service, the port number will automatically be displayed. You can modify it if necessary.
External Port End	When selecting a service, the port number will automatically be displayed. You can modify it if necessary.
Protocol	You may select TCP/UDP, TCP, or UDP in the drop-down list.
Internal Port Start	When selecting a service, the port number will automatically be displayed. You can modify it if necessary.
Internal Port End	When selecting a service, the port number will automatically be displayed. You can modify it if necessary.

After finishing setting, click **Save/Apply** to save and apply the settings.

■ Port Triggering

Some applications need some ports to be opened in the firewall for the remote access. When an application initializes a TCP/UDP to connect to a remote user, port triggering dynamically opens the open ports of the firewall.

Choose **Advanced Settings > NAT > Port Triggering** and the following page appears.

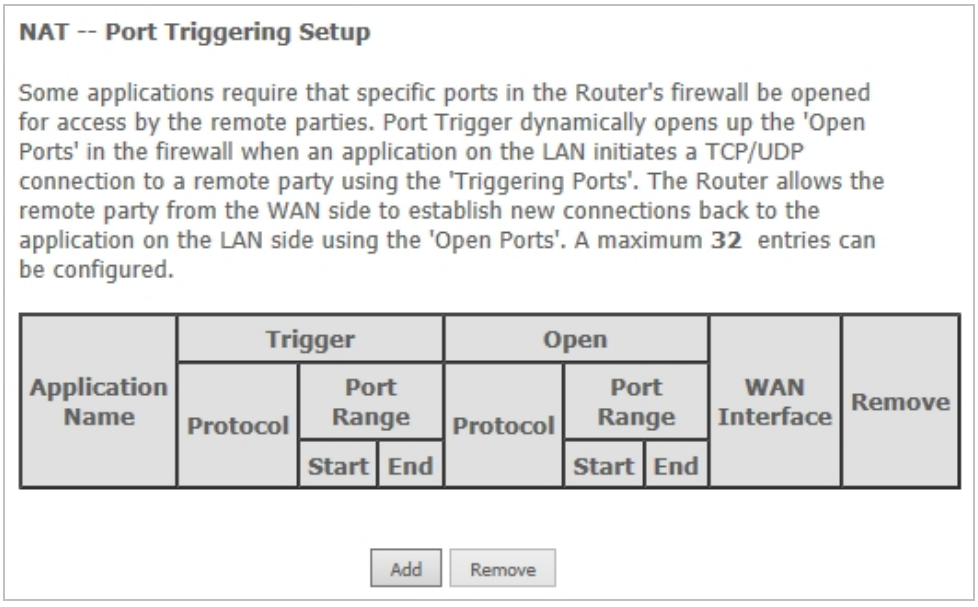


Figure 5-2-45

On this page, you may add or remove an entry of port triggering. Click the **Add** button to display the following page.

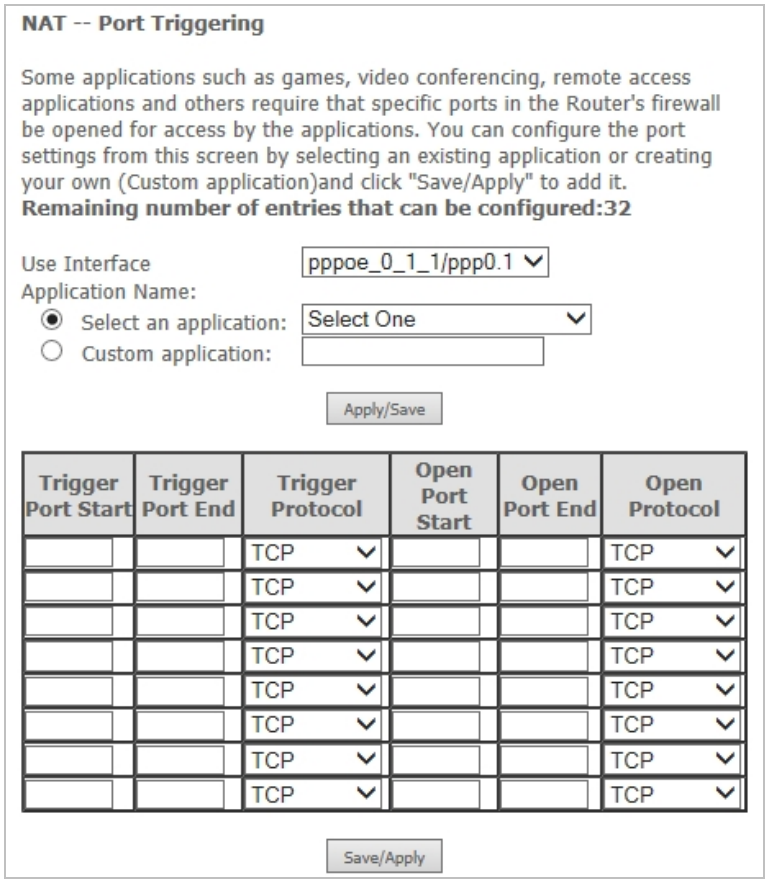


Figure 5-2-46

Object	Description
Use Interface	Select an interface that you want to configure
Select an application	Select a proper application in the drop-down list.
Custom application	Enter a new service name to establish a user service type.
Trigger port Start	The start port number that LAN uses to trigger the open port.
Trigger port End	The end port number that LAN uses to trigger the open port.
Trigger Protocol	Select the application protocol. You may select TCP/UDP, TCP, or UDP.
Open Port Start	The start port number that is opened to WAN.
Open Port End	The end port number that is opened to WAN.
Open Protocol	Select the proper protocol that is opened to WAN. You may select TCP/UDP, TCP, or UDP.

After finishing setting, click **Save/Apply** to apply the settings.

You can use a single port number, several port numbers separated by commas, port blocks consisting of two port numbers separated by a dash, or any combination of these, for example 80, 90-140, 180.

■ DMZ Host

DMZ allows all the ports of a PC on your LAN to be exposed to the Internet. Set the IP address of the PC to be DMZ host, so that the DMZ host will not be blocked by firewall.

Choose **Advanced Setup > NAT > DMZ** host to display the following page.

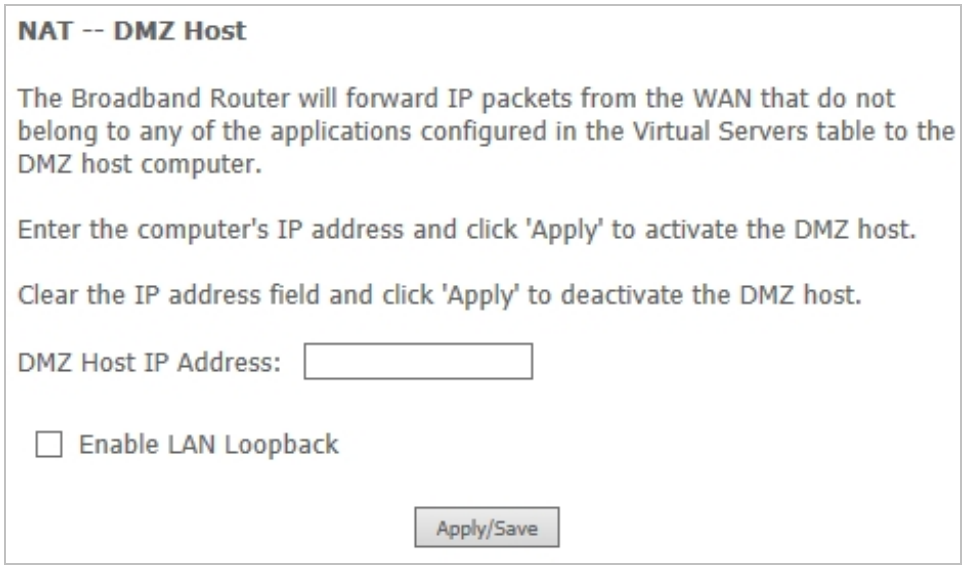


Figure 5-2-47

On this page, enter the IP address of the DMZ host. After finishing the settings, click the **Apply/Save** button to apply the settings.

If you want to clear the DMZ function of the host, please delete the IP address of the host in the field of DMZ Host IP Address and then click the **Apply/Save** button.

5.2.6 Security

■ Firewall

Choose **Security > Firewall** and the following page appears.

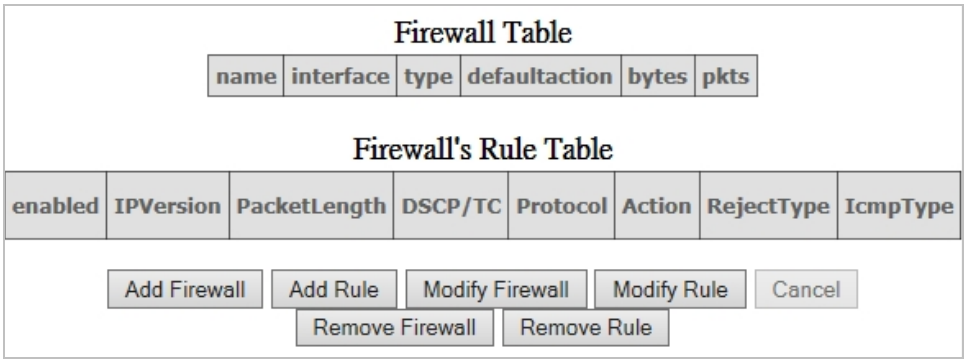


Figure 5-2-48

Click **Add Firewall** and the following page appears.

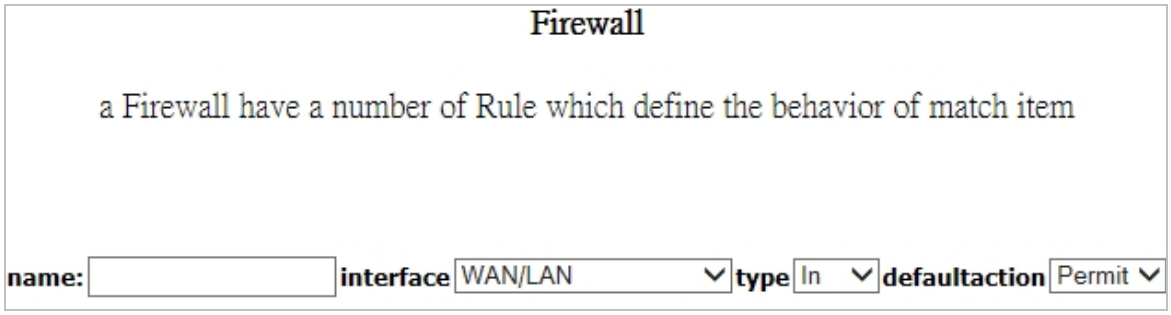


Figure 5-2-49

Object	Description
name	The name of firewall.
interface	You can select LAN or WAN from the drop-down list.
type	You can select IN or OUT from the drop-down list.
defaultaction	You can select Permit or Drop from the drop-down list.

Click **Modify Firewall** or **Remove Firewall** to modify or remove the firewall. And click **Modify Rule** or **Remove Rule** to modify or remove the rule.

■ MAC Filtering Setup

In some cases, you may want to manage Layer2 MAC address to block or permit a computer within the home network. When you enable MAC filter rules, the DSL router serves as a firewall that works at layer 2.

MAC filtering is only effective on ATM PVCs configured in bridge mode.

Choose **Security > MAC Filtering** and the following page appears.

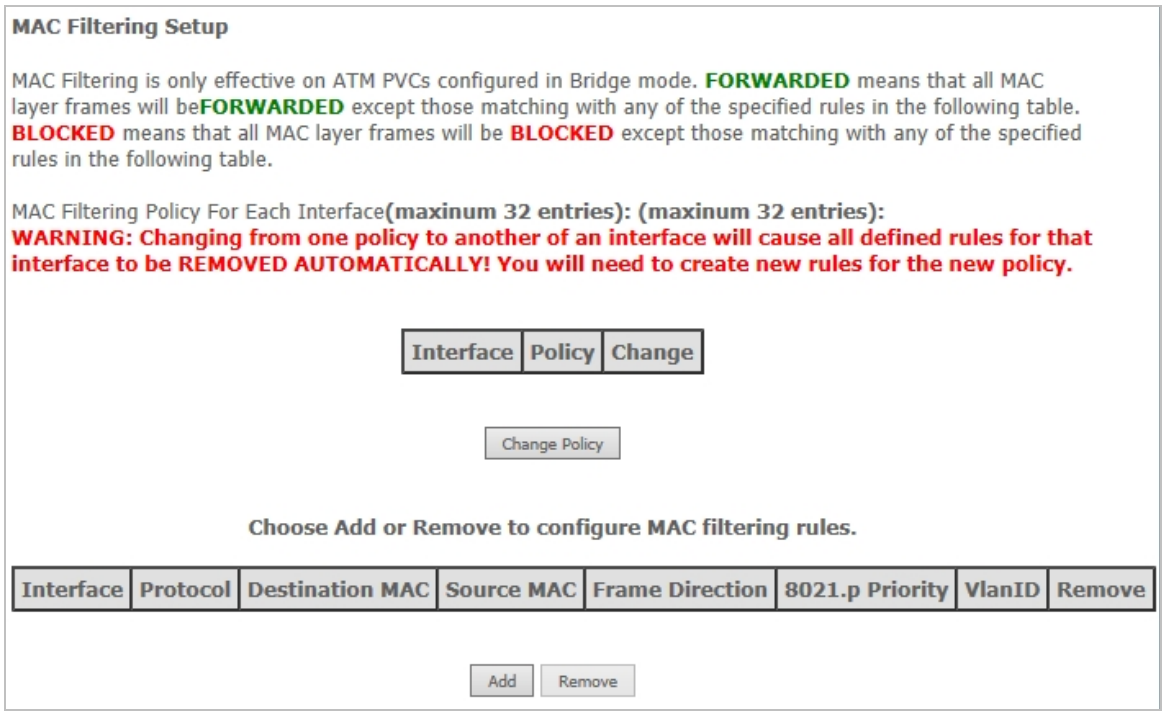


Figure 5-2-50

On this page, you can add or remove the MAC filtering rule. You may change the MAC filtering policy from FORWARDED to BLOCKED by clicking the **Change Policy** button.

Click the **Add** button to display the following page.

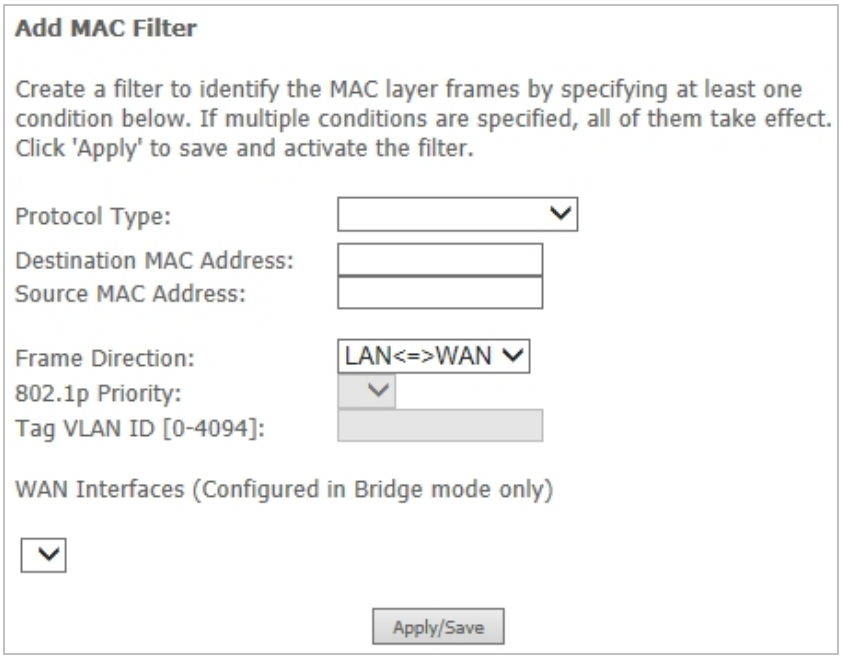


Figure 5-2-51

Object	Description
Protocol Type	Select the proper protocol type.
Destination MAC Address	Enter the destination MAC address.
Source MAC Address	Enter the source MAC address.
Frame Direction	The direction of transmission frame.
WAN Interface	Select the proper WAN interface in the drop-down list.

After finishing setting, click **Apply/Save** to save and apply the filtering rule.

5.2.7 Parental Control

■ Time Restriction

Choose **Advanced Setup > Parental Control > Time Restriction** and the following page appears.

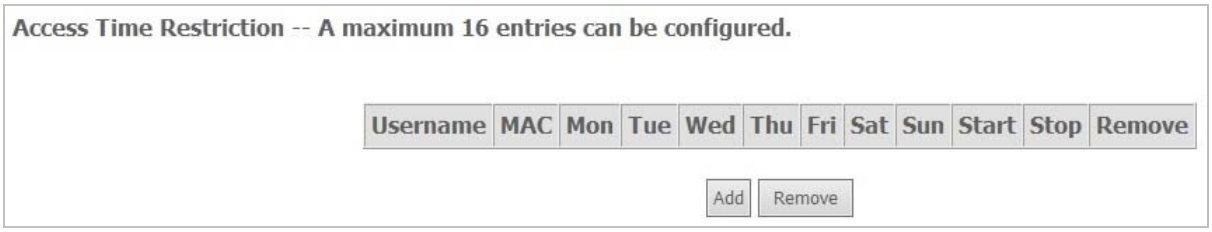


Figure 5-2-52

Click **Add** button to display the following page. This page is used to control the time restriction to a special LAN device that connects to the DSL router. On this page, select the user name and configure the time settings.

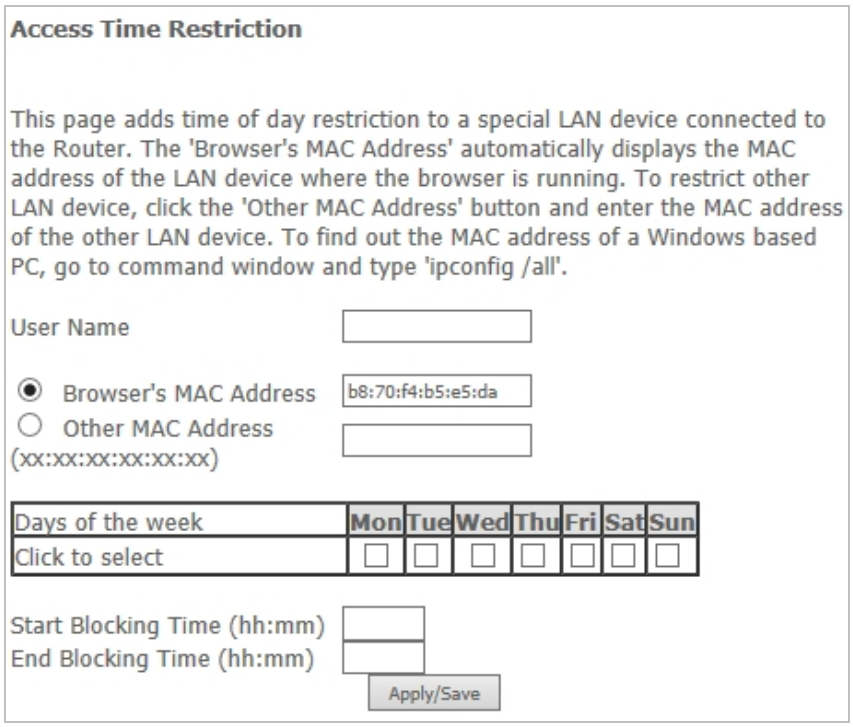


Figure 5-2-53

After finishing setting, click **Apply/Save** button to save and apply the settings.

■ Url Filter

Click **Advanced Setup > Parental Control > Url Filter** and the following page appears.

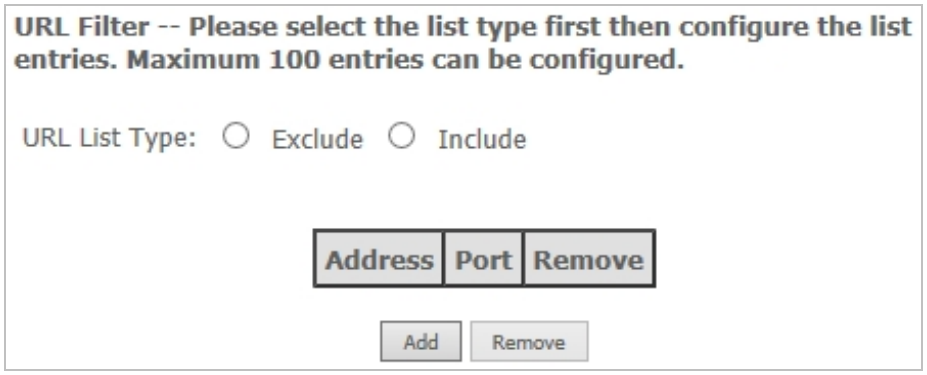


Figure 5-2-54

This page is used to prevent the LAN users from accessing some Websites in the WAN.

On this page, you may select the Exclude URL list type or the Include URL list type.

Object	Description
Exclude	The URLs in the list are not accessible.
Include	You are allowed to access the URLs in the list.

Click the **Add** button to display the following page.

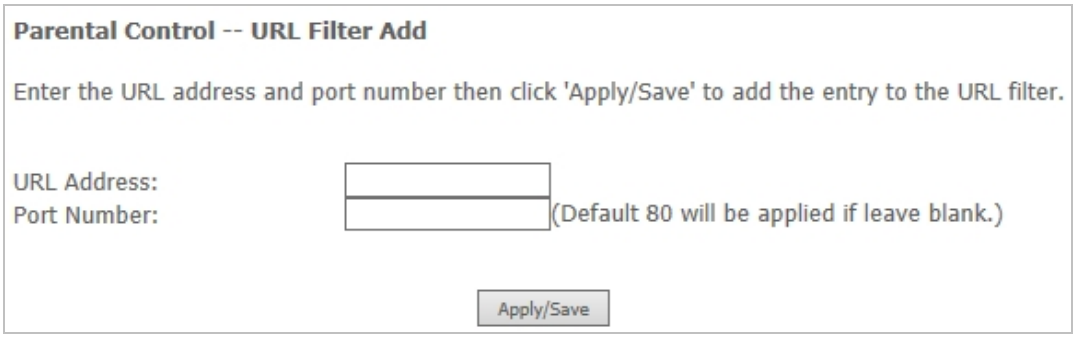


Figure 5-2-55

On this page, enter the URL address and its corresponding port number. For example, enter the URL address ***http://www.google.com*** and the port number **80** and then click the **Apply/Save** button.

5.2.8 Quality of Service

Choose **Advance Setup > Quality of Service** and the following page appears.

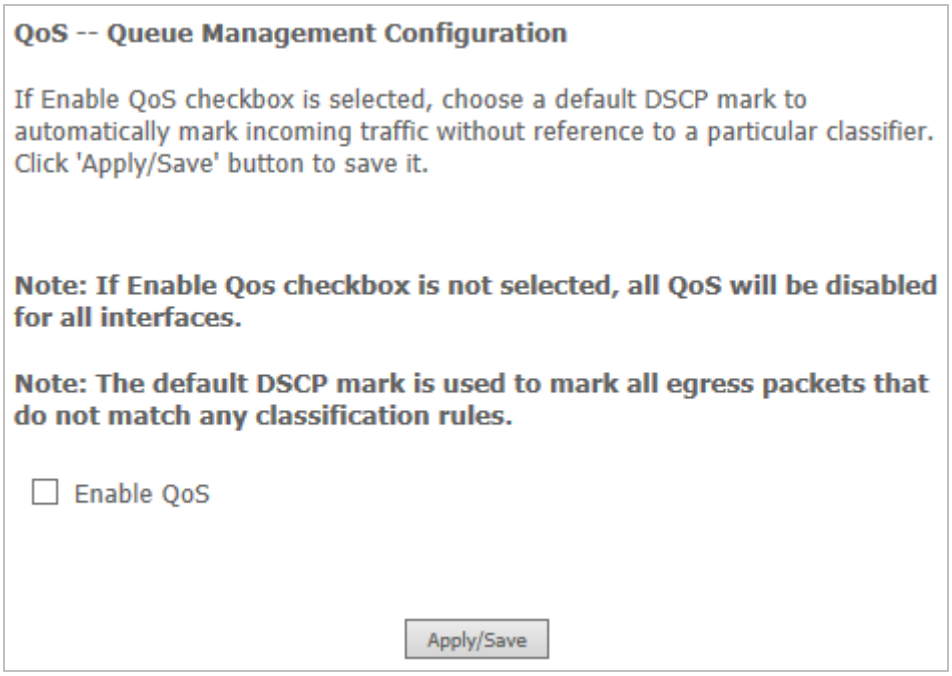


Figure 5-2-56

Select **Enable QoS** to enable QoS and configure the default DSCP mark.

After finishing setting, click **Apply/Save** to save and apply the settings.

If the Enable Qos checkbox is not selected, all QoS will be disabled for all interfaces. The default DSCP mark is used to mark all egress packets that do not match any classification rules.

■ Queue Configuration

Choose **Advanced Setup > Quality of Service > QoS Queue** and the following page appears. On this page, you can enable, add or remove a QoS rule.

QoS Queue Setup

In ATM mode, maximum 16 queues can be configured.
In PTM mode, maximum 8 queues can be configured.
For each Ethernet interface, maximum 3 queues can be configured.
To add a queue, click the **Add** button.
To remove queues, check their remove-checkboxes, then click the **Remove** button.
The **Enable** button will scan through every queues in the table. Queues with enable-checkbox checked will be enabled. Queues with enable-checkbox un-checked will be disabled.
The enable-checkbox also shows status of the queue after page reload.
If you disable WMM function in Wireless Page, queues related to wireless will not take effects

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

Name	Key	Interface	Qid	Prec/Alg/Wght	DSL Latency	PTM Priority	Min Bit Rate (bps)	Shaping Rate (bps)	Burst Size (bytes)	Enable	Remove
WMM Voice Priority	1	wl0	0	1/SP						Enabled	
WMM Voice Priority	2	wl0	0	2/SP						Enabled	
WMM Video Priority	3	wl0	0	3/SP						Enabled	
WMM Video	4	wl0	0	4/SP						Enabled	

Figure 5-2-57

Note

The lower integer value for precedence indicates the higher priority.

Click the **Add** button to display the following page.

QoS Queue Configuration

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

Name:

Enable: Disable

Interface:

Apply/Save

Figure 5-2-58

Object	Description
Name	Enter the name of QoS queue.
Enable	Enable or disable the QoS queue.
Interface	Select the proper interface for the QoS queue.

After finishing setting, click **Apply/Save** to save and apply the settings.

■ QoS Classification

Choose **Advanced Setup > Quality of Service > QoS Classification** and the following page appears.

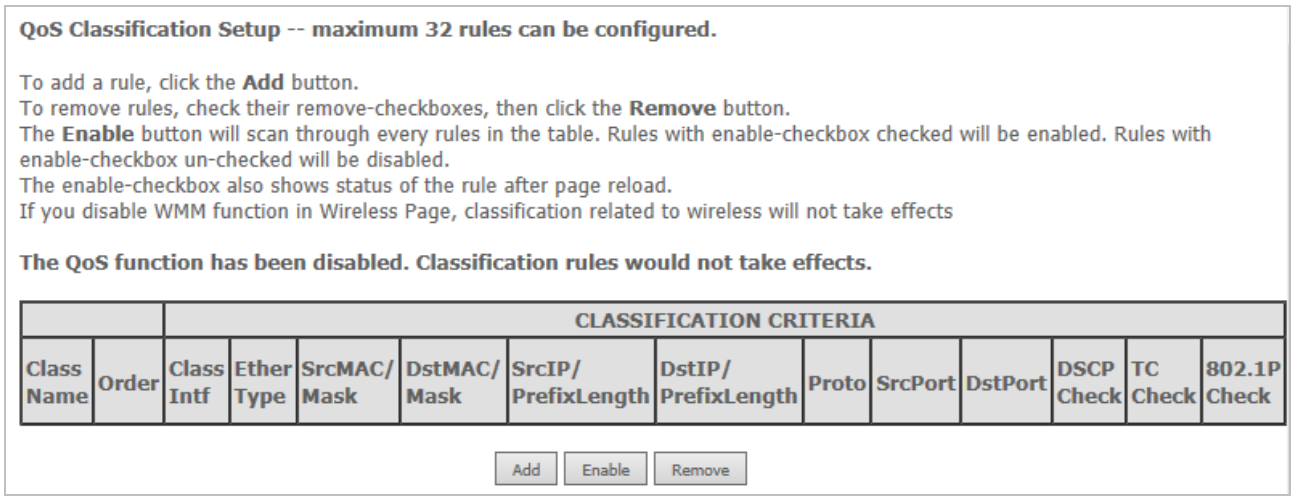


Figure 5-2-59

On this page, you can enable, add or remove a QoS classification rule.

Click the **Add** button to display the following page.

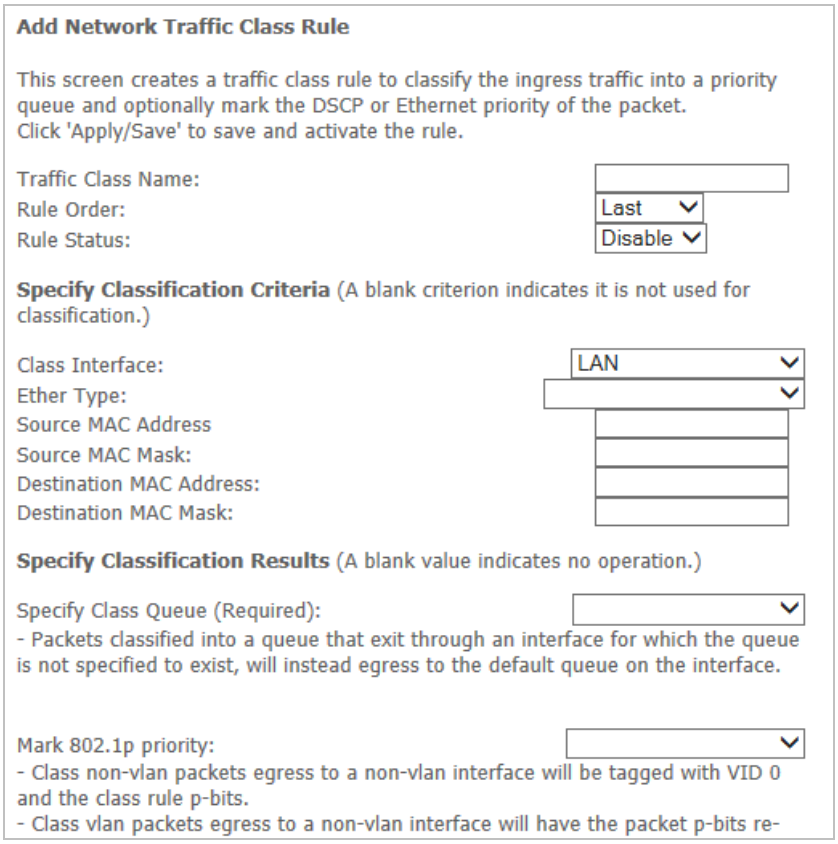


Figure 5-2-60

5.2.9 Routing

■ Default Gateway

Choose **Advanced Setup > Routing > Default Gateway** and the following page appears.

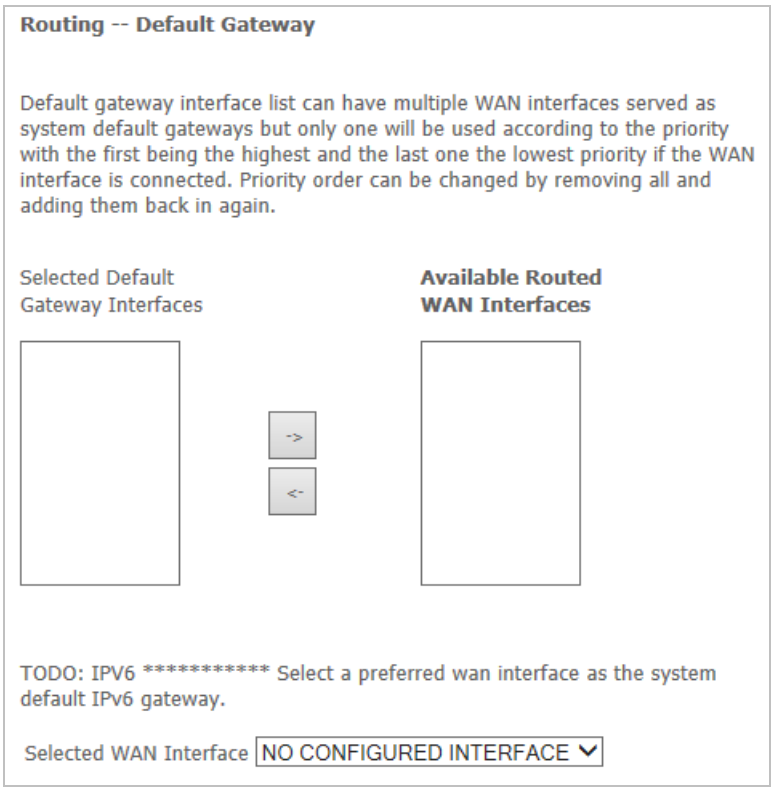


Figure 5-2-61

On this page, you can modify the default gateway settings.

Select a proper WAN interface in the drop-down list of **Selected WAN Interface** as the system default gateway. After finishing setting, click **Apply/Save** to save and apply the settings.

■ Static Route

Choose **Advanced Setup > Routing > Static Route** and the following page appears.

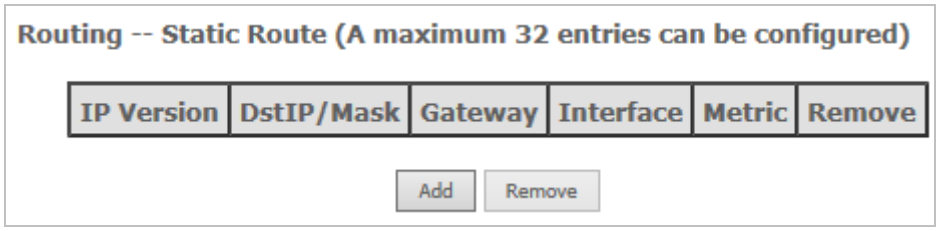


Figure 5-2-62

In this page, you can add or remove a static routing rule. Click the **Add** button to display the following page.

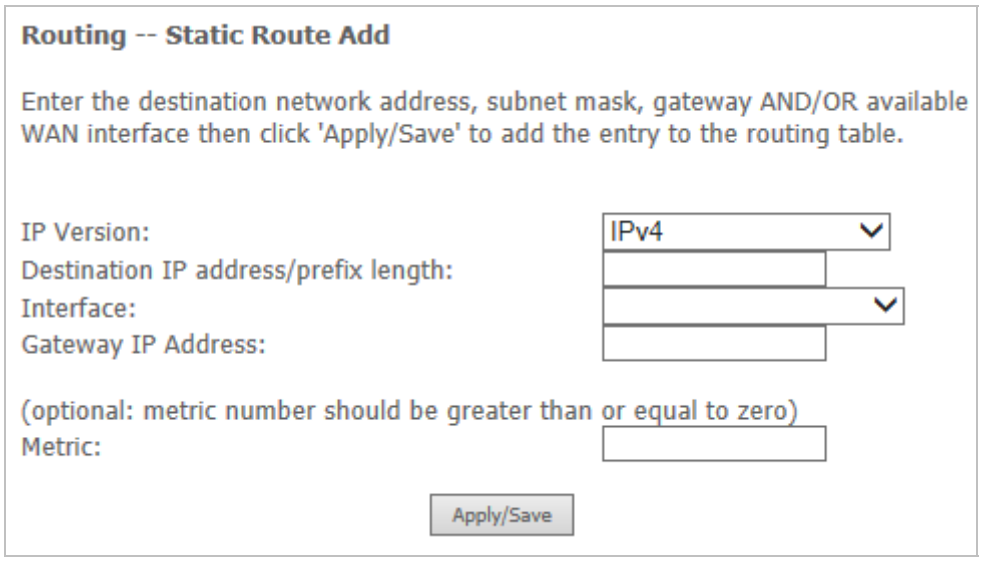


Figure 5-2-63

Object	Description
IP Version	Select the IP version. IPv4 or IPv6.
Destination IP address/prefix length	Enter the destination IP address.
Interface	Select the proper interface for the rule.
Gateway IP Address	The next-hop IP address.
Metric	The metric value of routing.

After finishing setting, click **Apply/Save** to save and apply the settings.

■ Policy Routing

Choose **Advanced Setup > Routing > Policy Routing** and the following page appears.

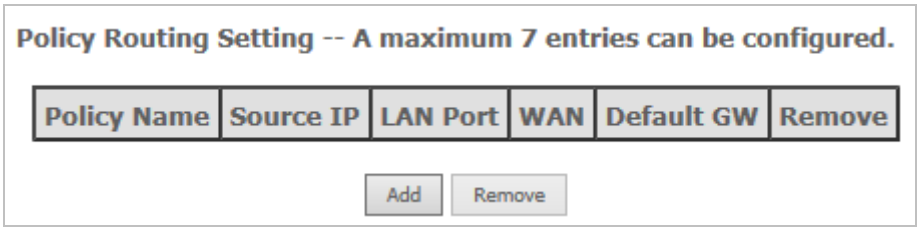


Figure 5-2-64

On this page, you can add or remove a static policy rule. Click the **Add** button to display the following page.

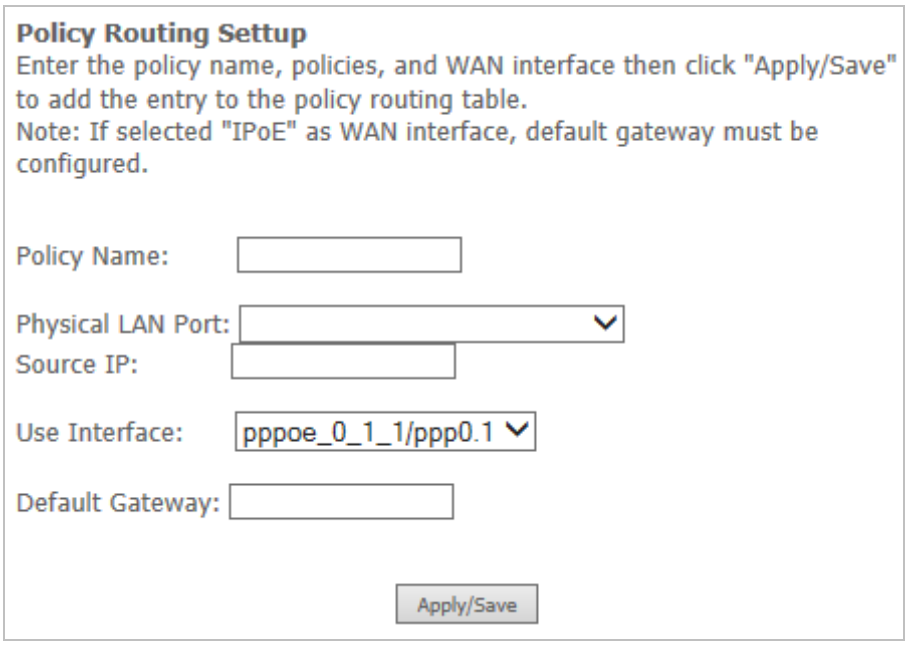


Figure 5-2-65

On this page, enter the policy name, source IP and default gateway, and select the physical LAN port and interface. After finishing setting, click **Apply/Save** to save and apply the settings.

■ RIP

Choose **Advanced Setup > Routing > RIP** and the following page appears.

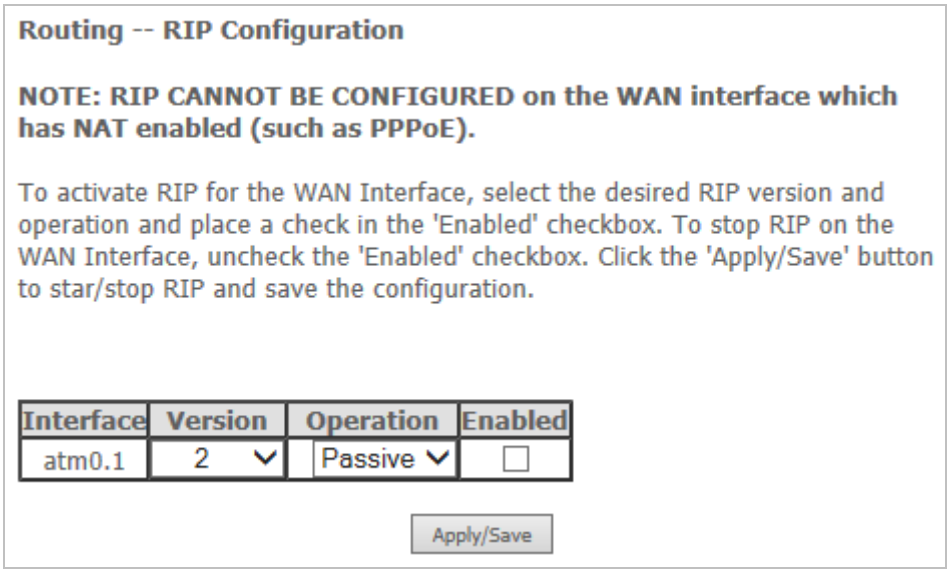


Figure 5-2-66

On this page, if you want to configure an individual interface, select the desired RIP version and operation, and then select the **Enabled** checkbox for the interface.

After finishing setting, click **Apply/Save** to save and apply the settings.

5.2.10 DNS

■ DNS Server

Choose **Advanced Setup > DNS > DNS Server** and the following page appears.

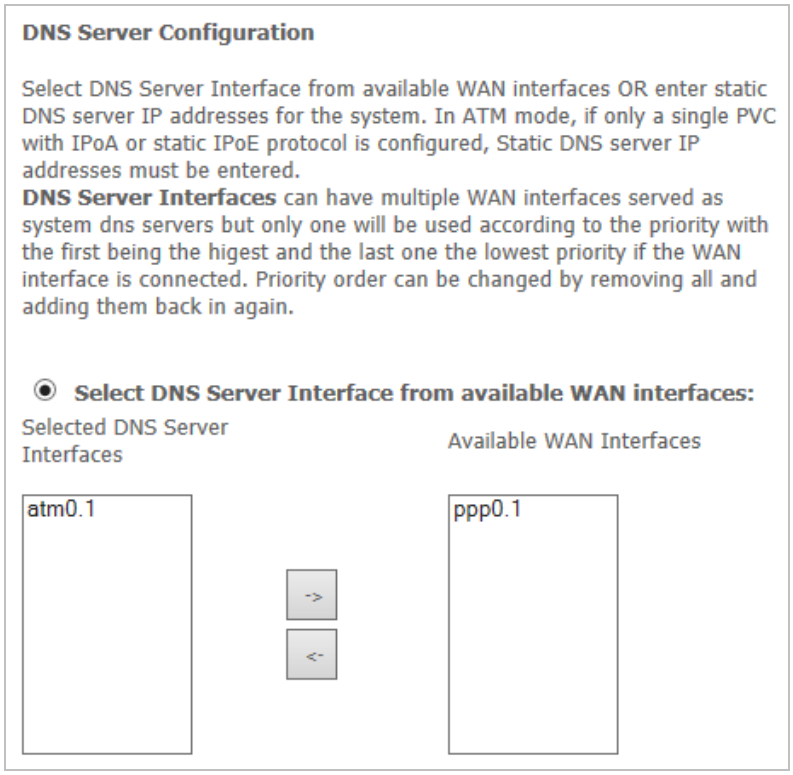


Figure 5-2-67

On this page, you can select a DNS server interface from the available interfaces, manually enter the DNS server addresses, or obtain the DNS address from a WAN interface.

After finishing setting, click **Apply/Save** to save and apply the settings.

■ Dynamic DNS

Choose **Advanced Setup > DNS > Dynamic DNS** and the following page appears.

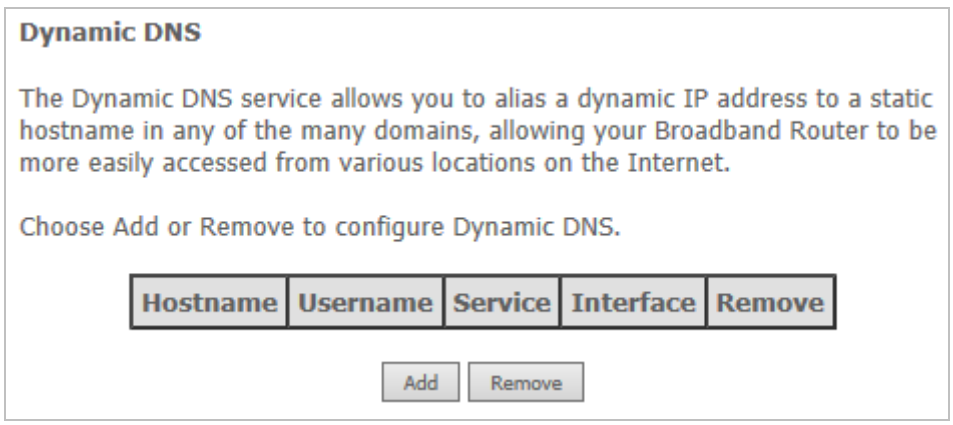


Figure 5-2-68

On this page, you are allowed to modify the DDNS settings.

Click the **Add** button to display the following page.

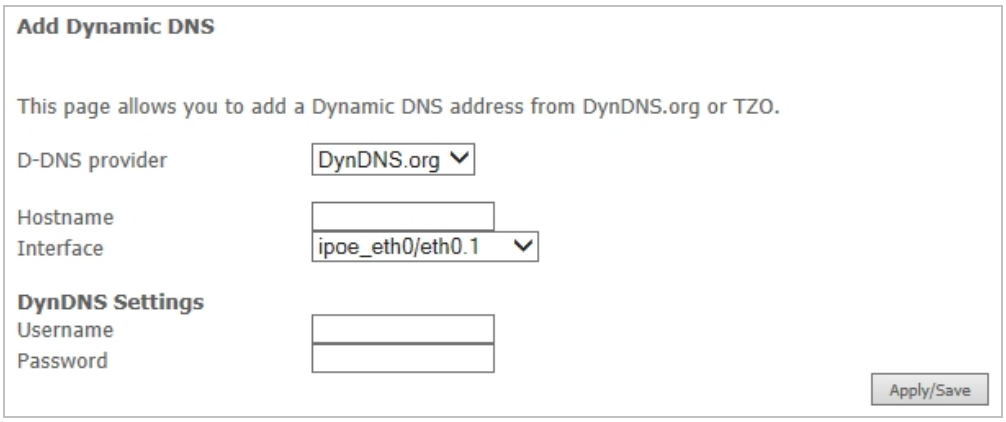


Figure 5-2-69

Object	Description
Hostname	It is the domain name and it can be modified.
Interface	The interface that the packets pass through on the DSL router.
Username	Enter the username for accessing the DDNS management interface.
Password	Enter the password for accessing the DDNS management interface.

D-DNS provider: Select a proper DDNS server in the drop-down list. After finishing setting, click **Apply/Save** to save and apply the settings.

5.2.11 DSL

Choose **Advanced Setup > DSL** and the following page appears. On this page, you can view the DSL settings. Usually, you can keep this factory default setting. The modem negotiates the modulation mode with the DSLAM. If you select VDSL2 Enabled check box, you can set the VDSL2 parameters on the right area.

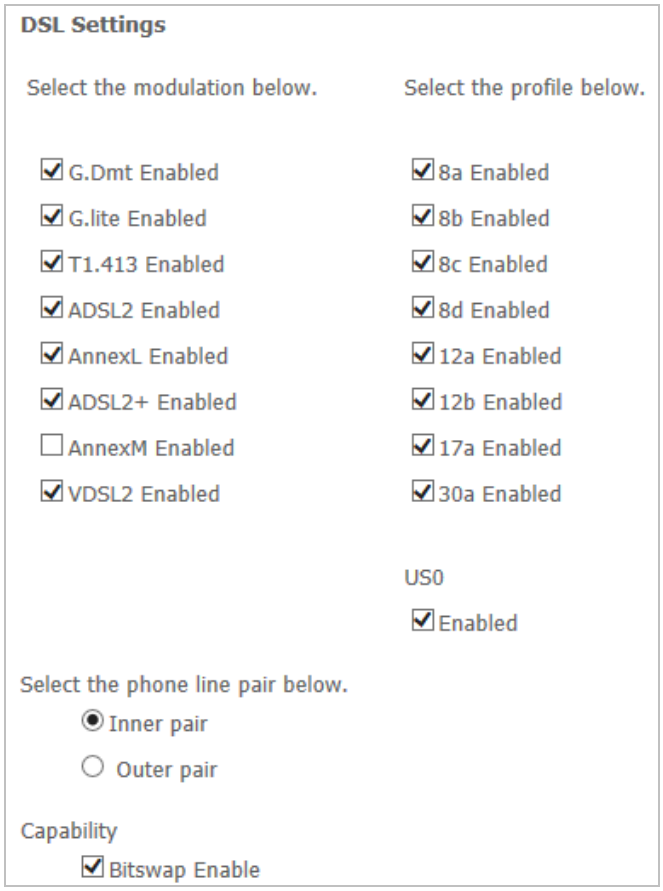


Figure 5-2-70

On this page, you can set the DSL settings. Usually, you do not need to modify the factory default settings. After finishing setting, click **Apply/Save** to save and apply the settings.

5.2.12 UPnP

Choose **Advanced Setup > UPnP** and the following page appears.

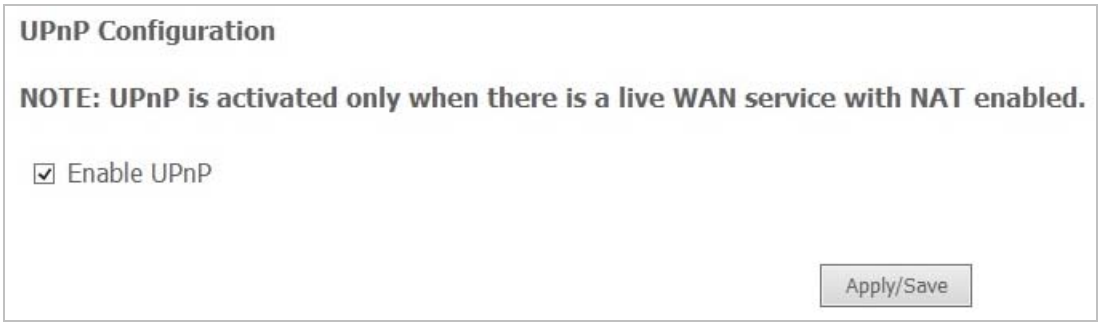


Figure 5-2-71

On this page, you can enable or disable the UPnP function. After finishing setting, click **Apply/Save** to save and apply the settings.

5.2.13 DNS Proxy

Choose **Advanced Setup > DNS Proxy** and the following page appears.

Figure 5-2-72

On this page, you can enable or disable the DNS proxy function. After enabling the DNS proxy function, enter the host name of the broadband router and the domain name of the LAN network and then click **Apply/Save** to save and apply the settings.

5.2.14 Print Server

The USB printer service allows you to connect a USB printer to the device and thus all clients on your network can print anything they want on their PCs. The device can identify a printer automatically as long as it is successfully connected.

Choose **Advanced Setup > Printer Server** and the following page appears.

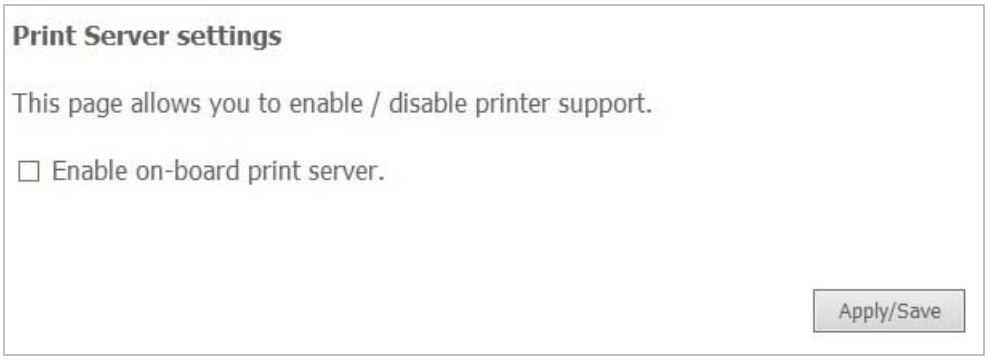


Figure 5-2-73

On this page, you can enable or disable the printer server. After finishing setting, click **Apply/Save** to save and apply the settings.

1. GDI interface printers are not supported.
2. Multifunction printers are not supported.

5.2.15 DLNA

Choose **Advanced Setup > DLNA** and the following page appears.

Figure 5-2-74

On this page, select the **Enable on-board digital media server** check box and the following page appears. On this page, enter the media library path to run digital media server.

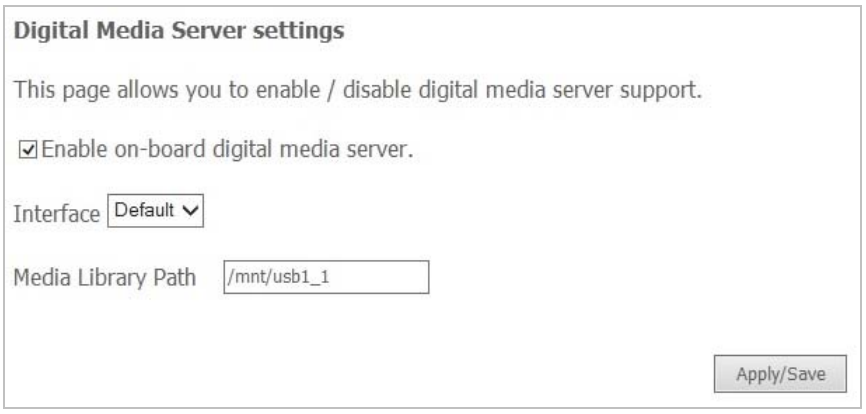


Figure 5-2-75

5.2.16 Packet Acceleration

Choose **Advanced Setup > Packet Acceleration** and the following page appears. On this page, you can enable packet flow accelerator.

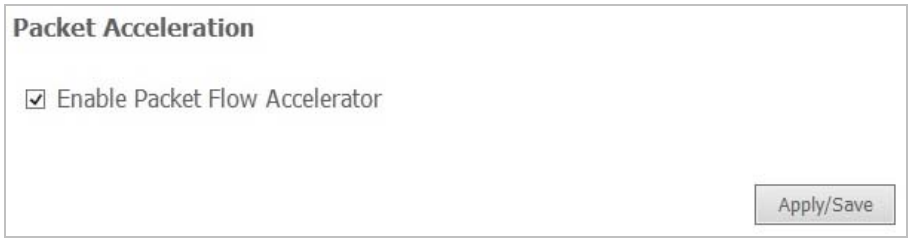


Figure 5-2-76

5.2.17 Storage Service

Share a USB storage device with PC/Laptop on the local network of the VDRT-300NU.

Insert a USB storage device, such as a flash drive or external hard drive, into the USB port on the right side or rear side of the VDR-300NU. The VDR-300NU can automatically identify attached storage and load its root directory folder. Follow the directions below for your operating system.

■ Storage Device Info

Choose **Advanced Setup > Storage Service > Storage Device Info** and the following page appears.

This page is used to display the information of the storage device that connects to the DSL router.

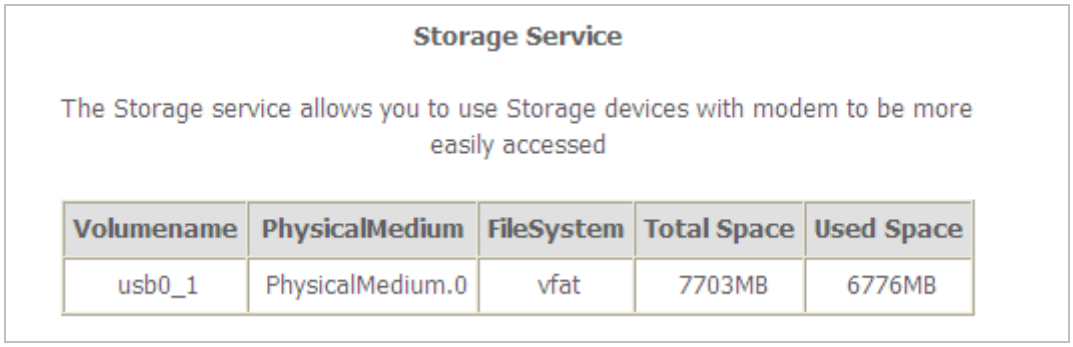


Figure 5-2-77

■ User Accounts

Choose **Advanced Setup > Storage Service > User Accounts** and the following page appears

You can Choose **Add**, or **Remove** to configure User Accounts.

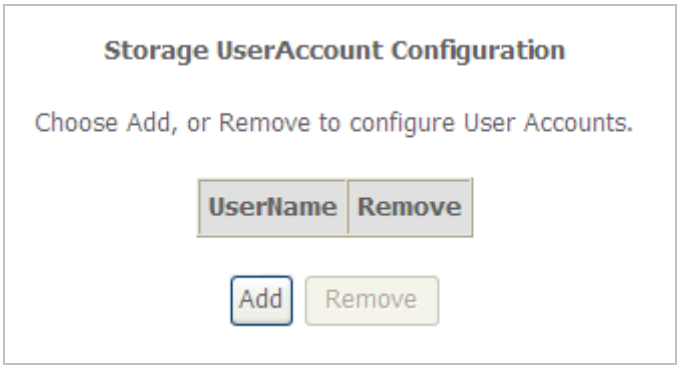
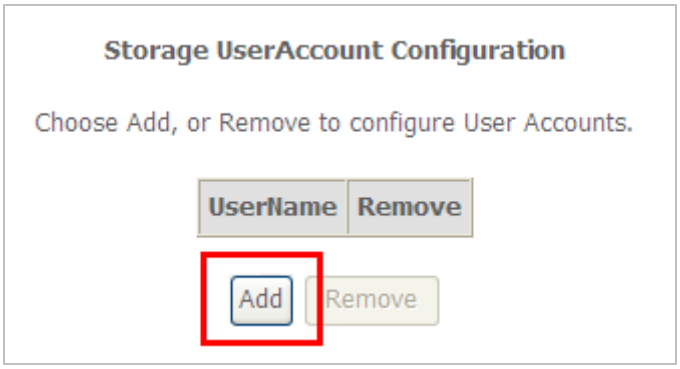


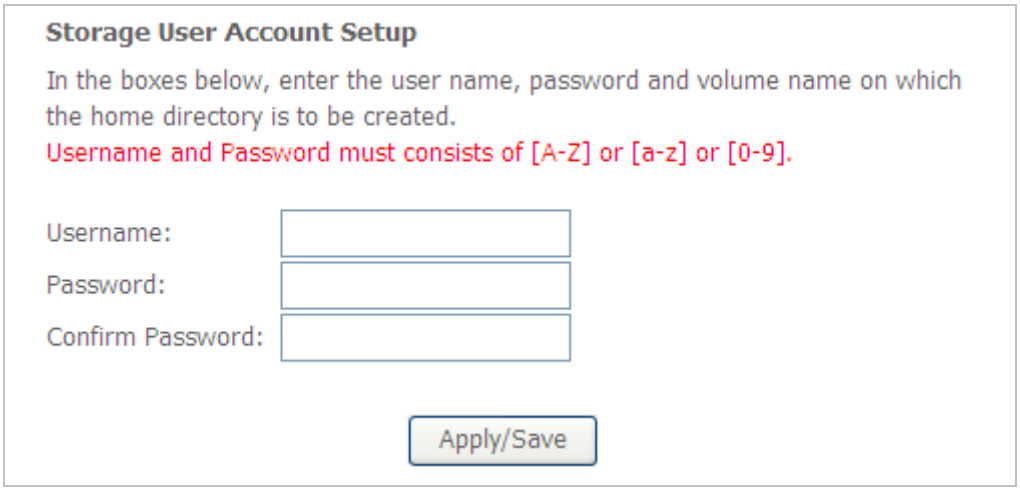
Figure 5-2-78

Operation Instructions:

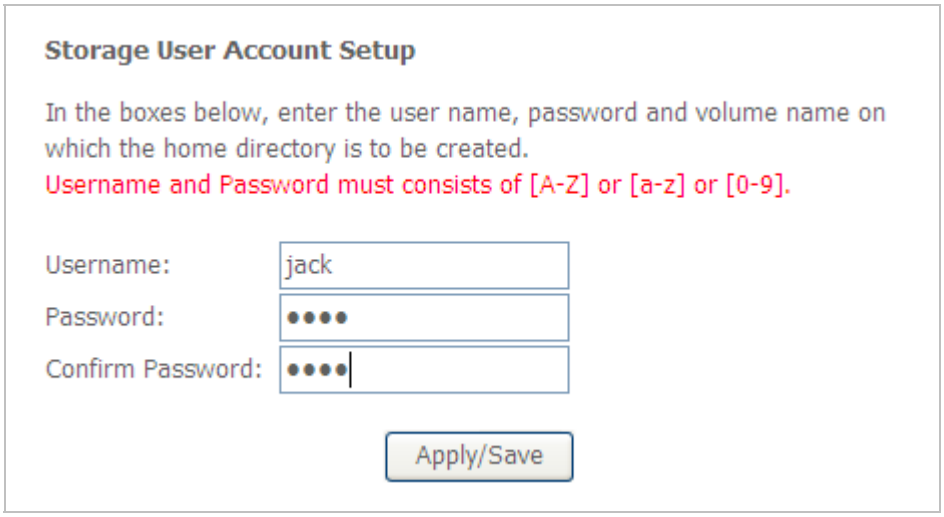
Step 1. Create an account.

1). Click "**Add**" to display a dialogue box below:

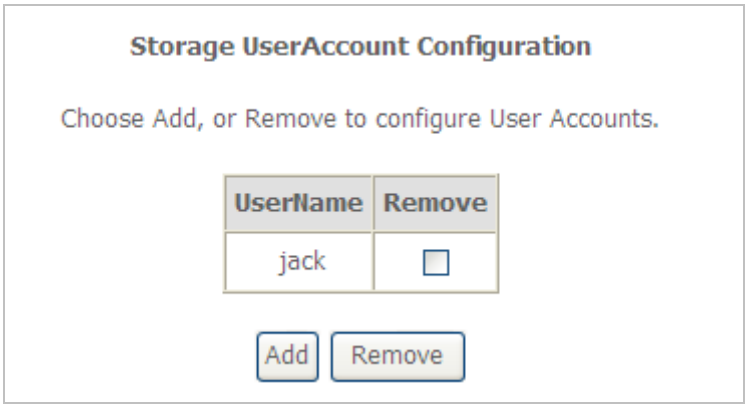




2) Enter a user name and a password, which will be used by clients when accessing the USB storage device for sharing files thereon.

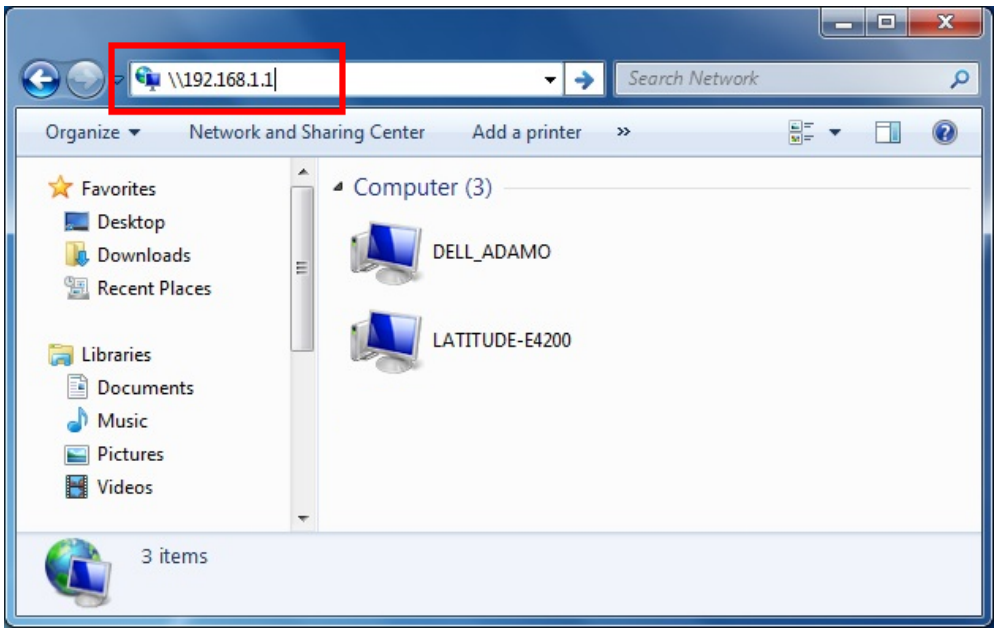


3) Re-type to confirm password and then click the "**Apply/Save**" button.

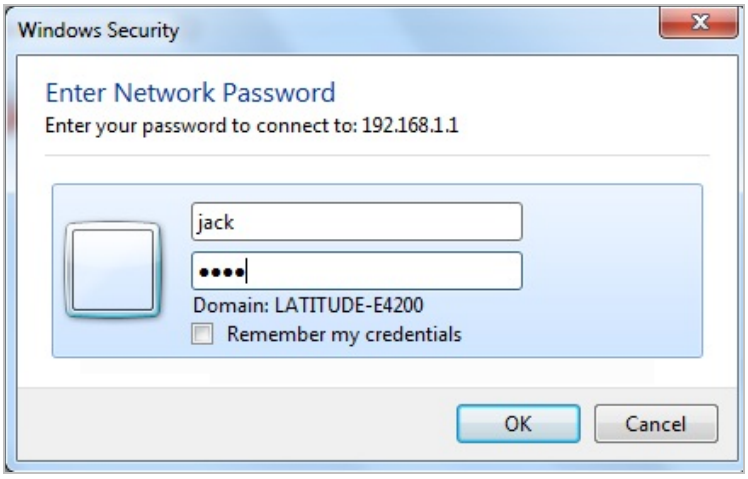


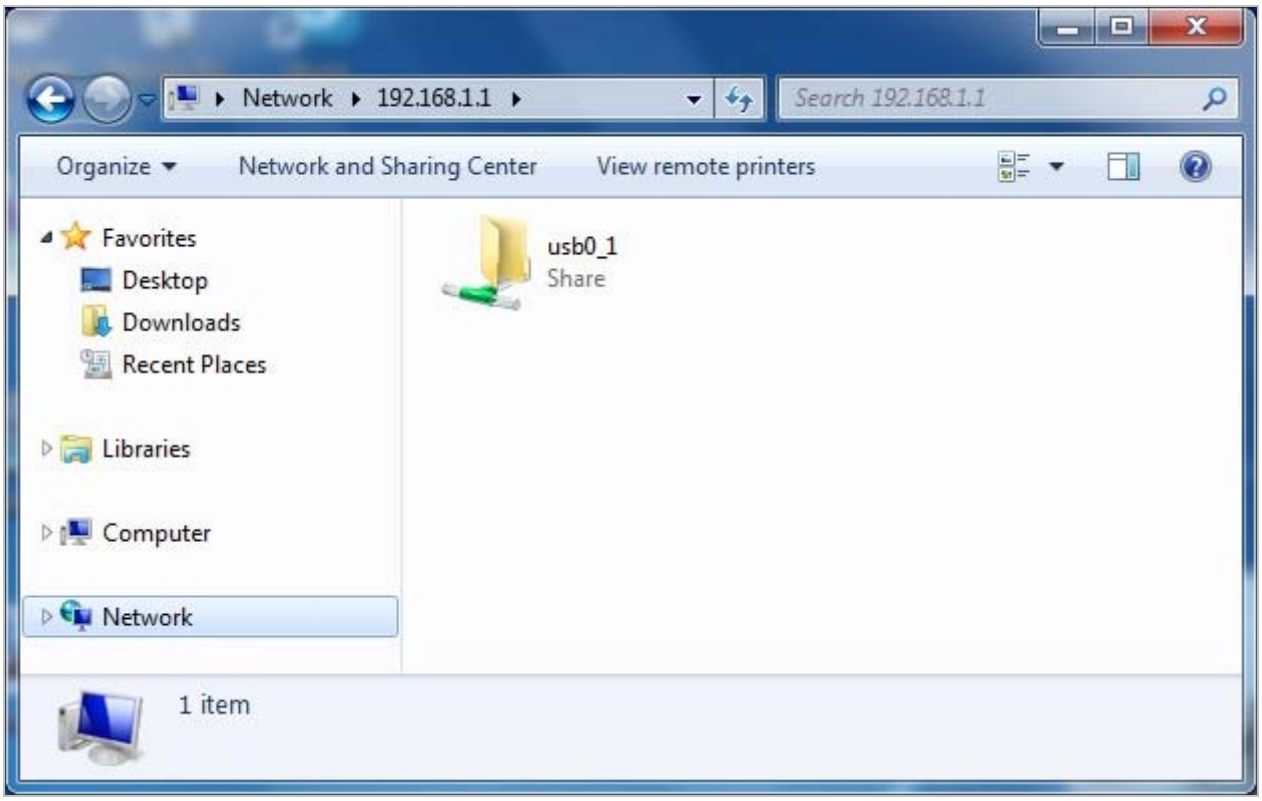
Step 2. Access shared file

To access resources on such storage device, double click "**Computer**" on your PC and enter \\192.168.1.1 (The LAN IP address of the router).



At the User Name and Password prompt, type your proper user name and password to login.





Note

The filename only supports **Unicode**.

5.2.18 Interface Grouping

Choose **Advanced Setup > Interface Grouping** and the following page appears.

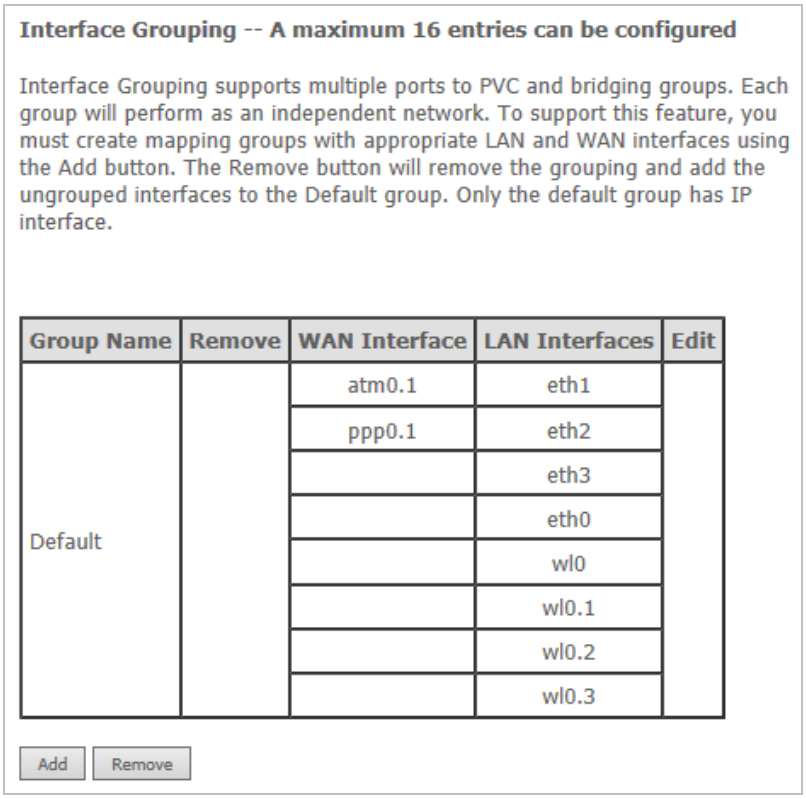


Figure 5-2-79

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 the 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.

Click the **Add** button to display the following page.

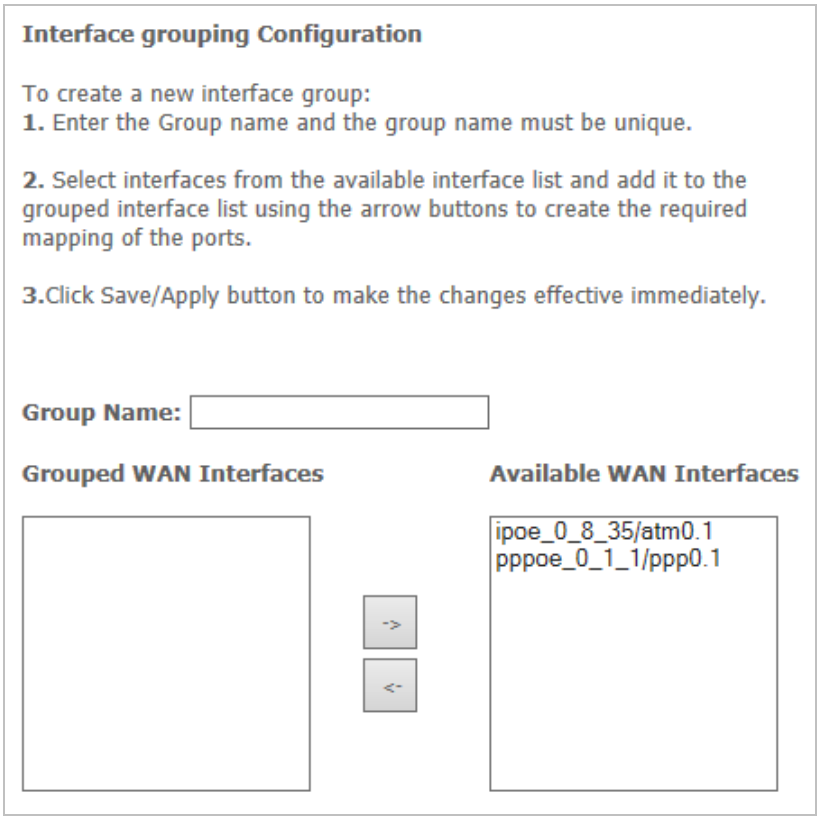


Figure 5-2-80

On this page, please follow the on-screen configuration steps to configure the parameters of the interface grouping. After finishing setting, click **Apply/Save** to save and apply the settings.

5.2.19 IP Tunnel

■ IPv6 in IPv4

Choose **Advanced Setup > IP Tunnel > IPv6inIPv4** and the following page appears. The default value is IPv6 in IPv4 information.

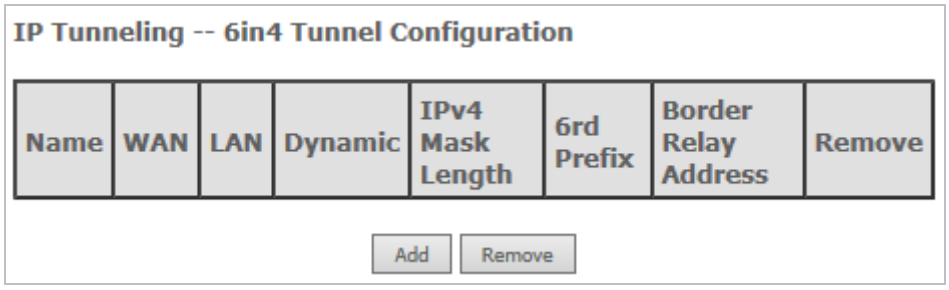


Figure 5-2-81

Click **Add** and the following page appears. On this page, you can add a new tunnel.

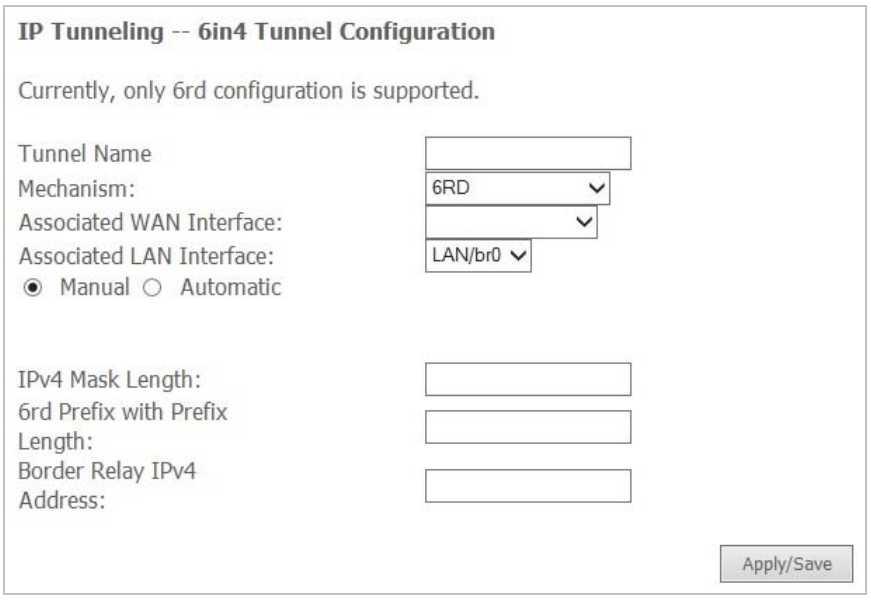


Figure 5-2-82

■ IPv4 in IPv6

Choose **Advanced Setup > IP Tunnel > IPv4inIPv6** and the following page appears.

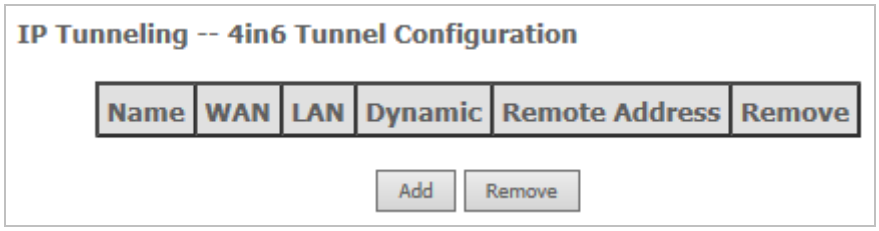


Figure 5-2-83

Click **Add** and the following page appears. On this page, you can add a new tunnel of IPv4 in IPv6.

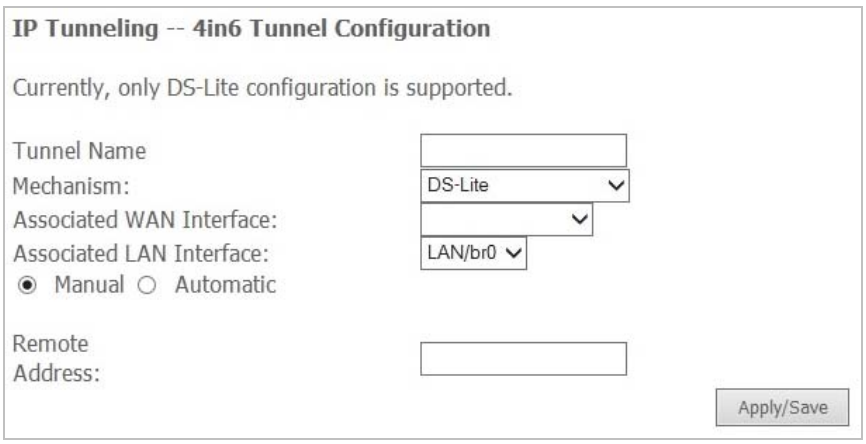


Figure 5-2-84

5.2.20 IPSec

Choose **Advanced Setup > IPSec** and the following page appears.

Figure 5-2-85

On this page, you can add or remove the IPSec tunnel connections. Click the **Add** button to display the following page.

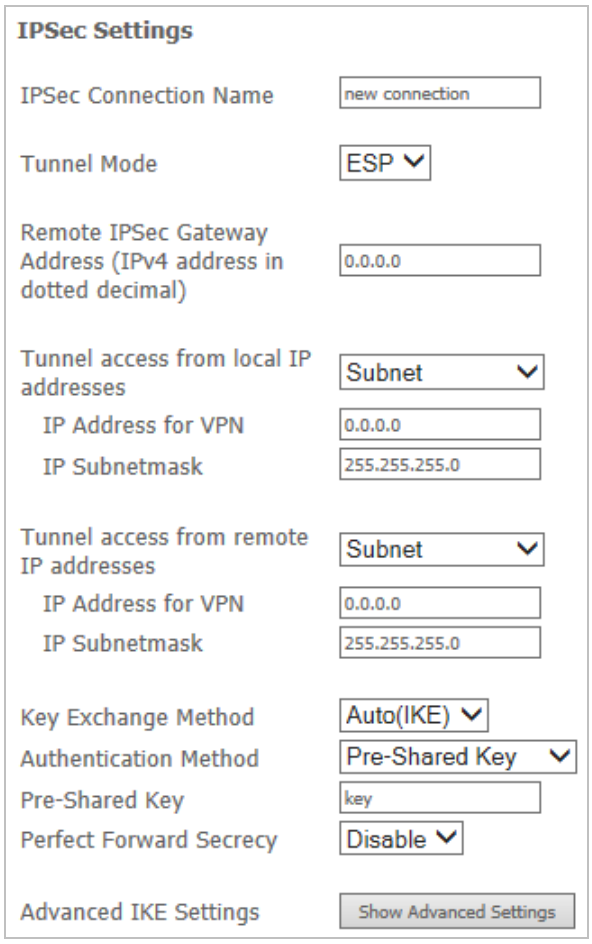


Figure 5-2-86

On this page, set the parameters such as the IPSec connection name, tunnel mode, and remote IPSec gateway address.

If you need to configure the advanced settings of this IPSec tunnel connection, please click the **Show Advanced Settings** button to display the other parameters.

After finishing setting, click **Apply/Save** to save and apply the settings.

5.2.21 Certificate

■ Local

Choose **Advanced Setup > Certificate > local** and the following page appears.

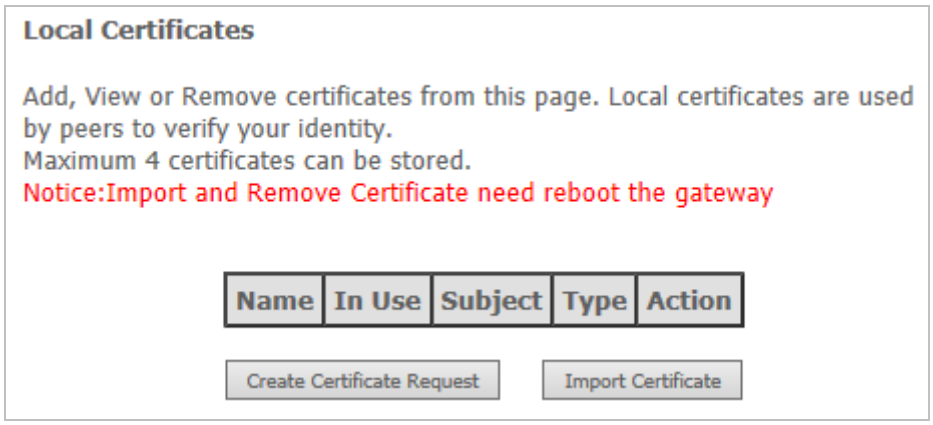


Figure 5-2-87

On this page, you can acquire the local certificate by creating a certificate request or importing a certificate. You may also create or remove a certificate.

■ **Creating a New Certificate Request**

Click the **Create Certificate Request** button to display the following page.

Figure 5-2-88

On this page, please set the following parameters.

Object	Description
Certificate name	Set the certificate name.
Common Name	The common name is the "fully qualified domain name," (or FQDN) used for DNS lookups of your server (for example,

	www.mydomain.com). Browsers use this information to identify your Web site. Some browsers will refuse to establish a secure connection with your site if the server name does not match the common name in the certificate. Please do not include the protocol symbol "http://" or any port numbers or pathnames in the common name. Do not use wildcard characters such as * or ?, and do not use an IP address
Organization Name	The name of the organization to which the entity belongs (such as the name of a company).
State/Province Name	This is the name of the state or province where your organization's head office is located. Please enter the full name of the state or province.
Country/Region Name	This is the two-letter ISO abbreviation for your country (for example, GB for the United Kingdom).

After finishing setting, click the **Apply** button to apply the settings.

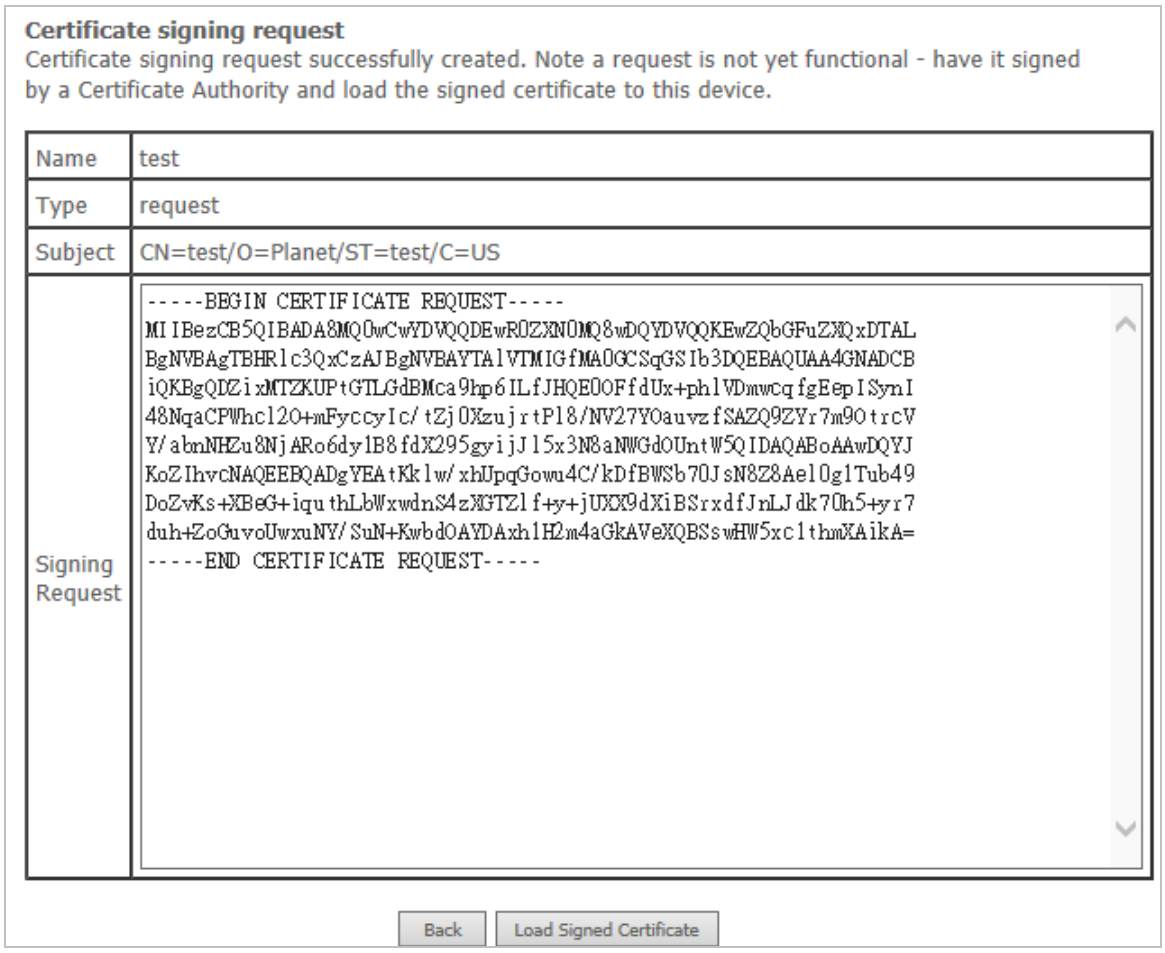


Figure 5-2-89

The certificate request needs to be submitted to a certificate authority, which will sign the request. Then the signed certificate needs to be loaded to the DSL router. Click **Load Signed Certificate** on this page and the following page appears.

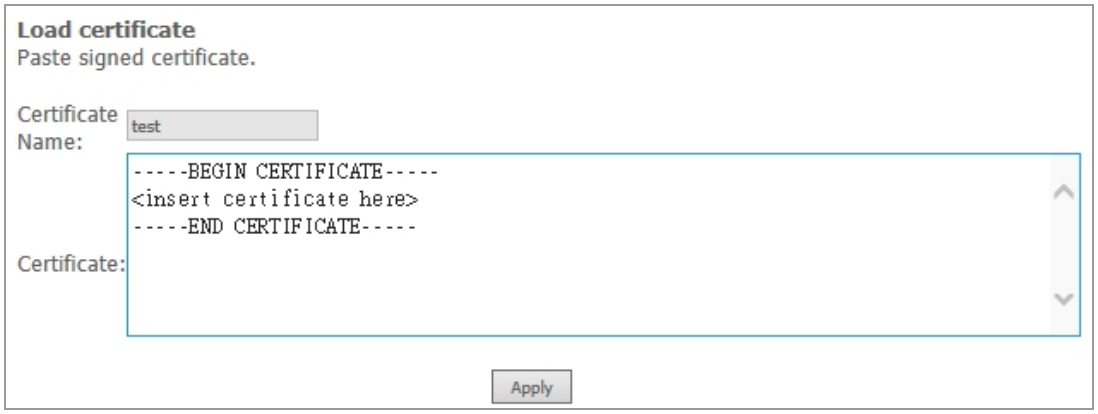


Figure 5-2-90

On this page, paste the signed certificate and then click the **Apply** button. A new certificate is created.

- **Importing an Existing Local Certificate**

To import an existing certificate, click the **Import Certificate** button to display the following page.

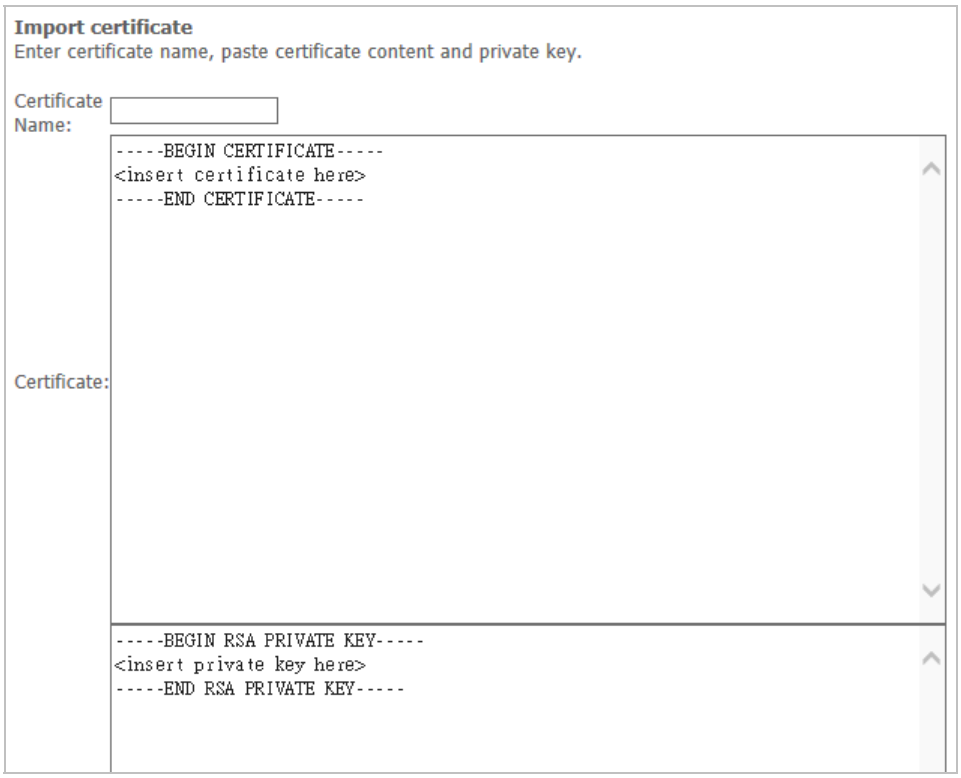


Figure 5-2-91

On this page, paste the certificate and the private key. Finally, click the **Apply** button to import the certificate.

■ Trusted CA

Choose **Advanced Setup > Certificate > Trusted CA** and the following page appears.

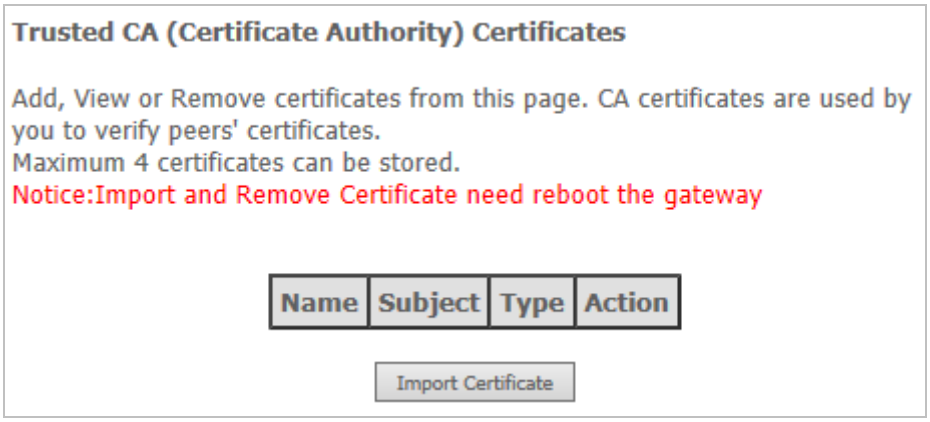


Figure 5-2-92

On this page, you may import or remove a CA certificate. Click the **Import Certificate** button to display the following page.

Figure 5-2-93

On this page, enter the certificate name and paste the certificate content. Finally, click the **Apply** button to import the certificate.

5.2.22 Power Management

Choose **Advanced Setup > Power Management** and the following page appears. This page allows control of Hardware modules to evaluate power consumption. Use the control buttons to select the desired option.

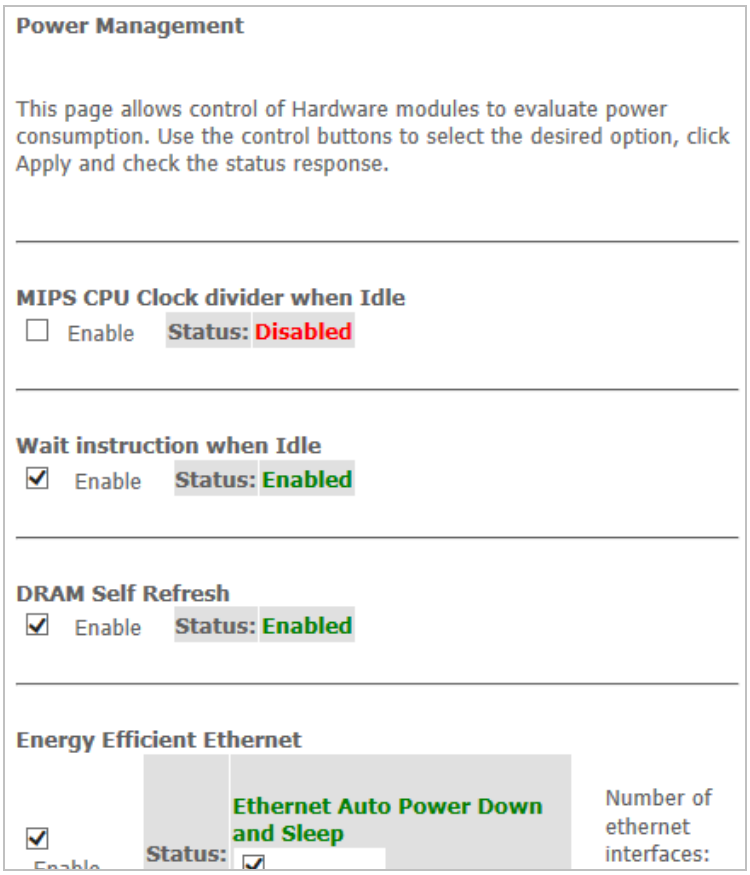


Figure 5-2-94

After proper configurations, click **Apply** to take the configurations effect.

5.2.23 Multicast

Choose **Advanced Setup > Multicast** and the following page appears.

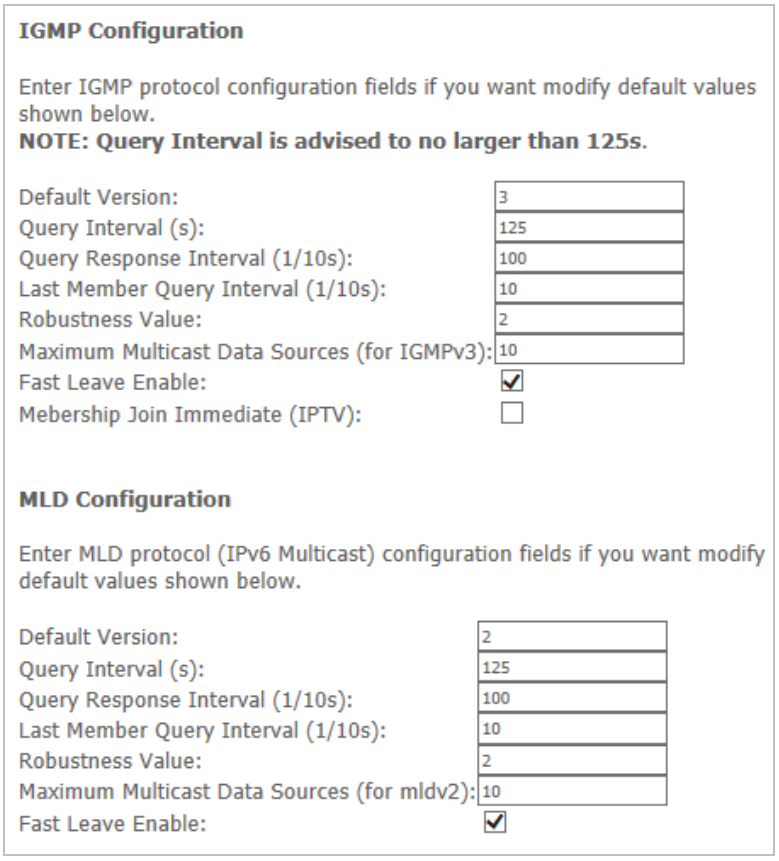


Figure 5-2-95

On this page, you can configure the multicast parameters. After finishing setting, click **Apply/Save** to save and apply the settings.

5.3 Wireless

Choose **Wireless** and the submenus of Wireless are shown below:

Figure 5-3-1

5.3.1 Basic Settings

Choose **Wireless > Basic** to display the following page. On this page, the figure in the right area is 2-dimensional code. It includes the wireless SSID and password. You can obtain the wireless SSID and password through scanning this figure.

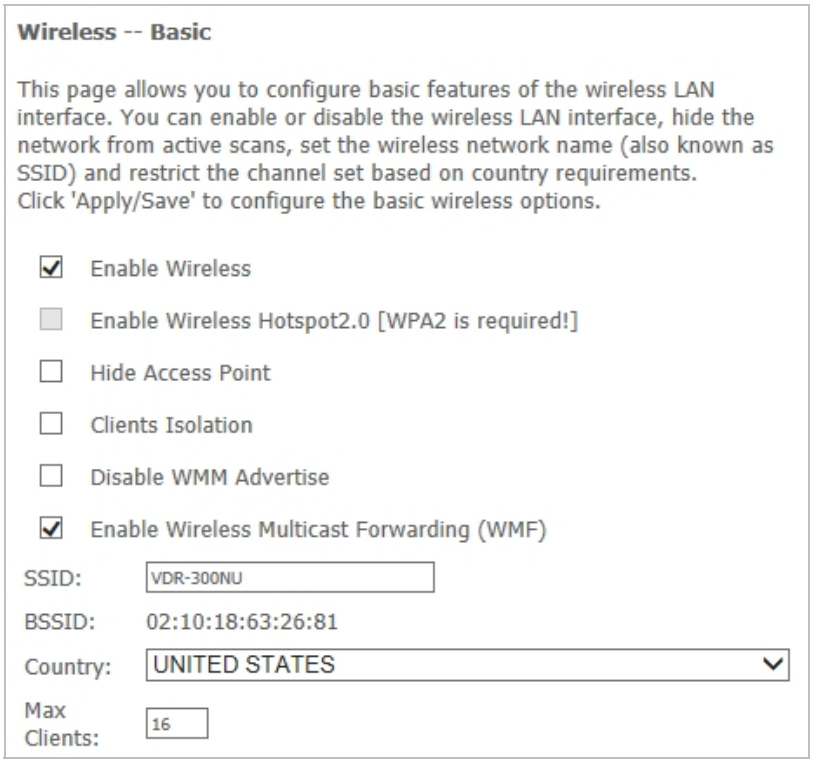


Figure 5-3-2

This page allows you to configure the basic features of the wireless LAN interface.

Object	Description
Enable Wireless	Enable or disable the wireless function.
Hide Access Point	If you want to hide any access point for your router, select this option, and then a station cannot obtain the SSID through the passive

	scanning.
Clients Isolation	When many clients connect to the same access point, they can access each other. If you want to disable the access between the clients that connect to the same access point, you can select this option.
Disable WMM Advertise	After enabling this option, the transmission performance multimedia of the voice and video data can be improved.
Enable Wireless Multicast Forwarding (WMF)	After enabling this option, the transmission quality of video service such as IPTV can be improved.
SSID	For the security reason, you should change the default SSID to a unique name.
BSSID	Display the MAC address of the wireless interface.
Country	The name of the country with which your gateway is configured. This parameter further specifies your wireless connection. For example, the channel will adjust according to nations to adapt to each nation's frequency provision.
Max Clients	Specify the maximum wireless client stations to be enabled to link with AP. Once the clients exceed the max value, all other clients are refused. The value of maximum clients is 16.
Wireless	Guest/Virtual Access Points: If you want to make Guest/Virtual network function be available, you have to check those boxes in the table below. In the current software version, three virtual access points can be configured.

After finishing setting, click **Apply/Save** to save the basic wireless settings and make the settings take effect.

5.3.2 Security

Choose **Wireless > Security** to display the following page.

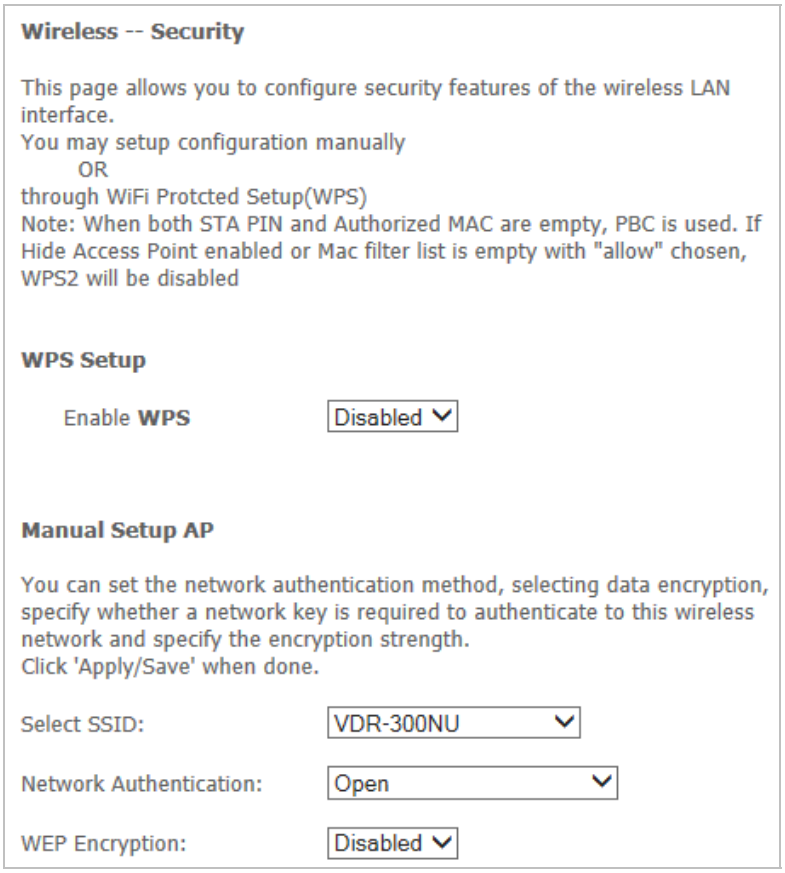


Figure 5-3-3

This page allows you to configure the security features of the wireless LAN interface. On this page, you can configure the network security settings by the **Wi-Fi Protected Setup** (**WPS**) method or setting the network authentication mode.

■ WPS Setup

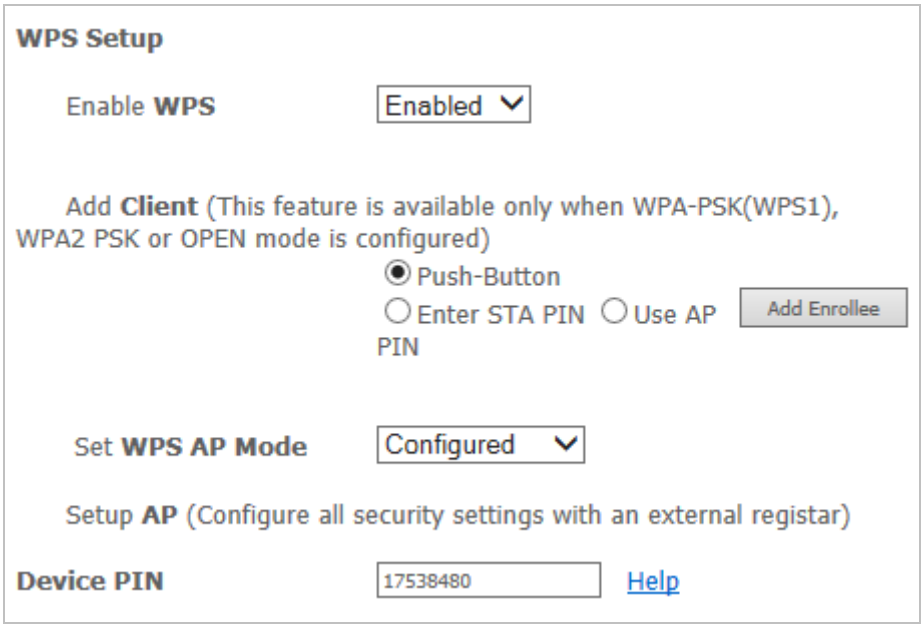


Figure 5-3-4

There are 2 primary methods used in the Wi-Fi Protected Setup:

- PIN entry, a mandatory method of setup for all WPS certified devices.

  Enter STA PIN: If you select it, you need to enter the station PIN from client.

  Use AP PIN: The PIN is generated by AP.

- Push button configuration (PBC), an actual push button on the hardware or through a simulated push button in the software. (This is an optional method on wireless client).

If you are using the PIN method, you will need a Registrar (access point/wireless router) to initiate the registration between a new device and an active access point/wireless router.

The PBC method may also need a Registrar when used in a special case where the PIN is all zeros

In order to use the push-button for WPS authentication, you must ensure that the network card supports the function. If it supports, you need not to do any configuration. You can press the WPS button directly to enable the WPS function.

■ Manual Setup AP

This page provides 9 types of network authentication modes, including Open, Shared, 802.1X, WPA, WPA-PSK, WPA2, WPA2-PSK, Mixed WPA2/WPA, and Mixed WPA2/WPA-PSK.

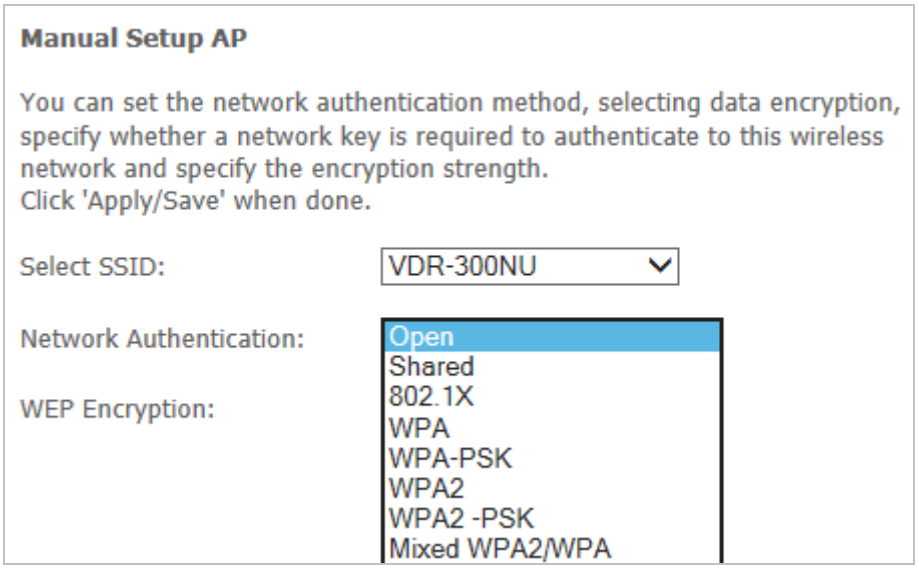


Figure 5-3-5

- **Open Mode**

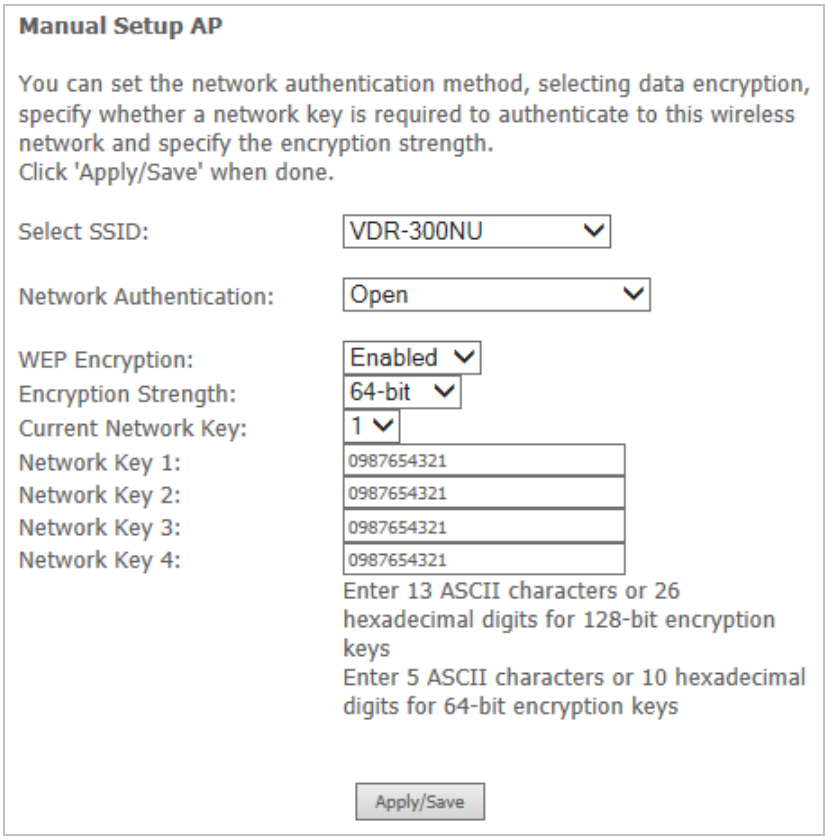


Figure 5-3-6

Object	Description
Select SSID	Select a SSID for configuring the security settings.
Network	Select the Open mode.

Authentication	
WEP Encryption	Enable or disable WEP encryption. After enabling this function, you can set the encryption strength, current network key, and network keys.
Encryption Strength	You can set 64-bit or 128-bit key.
Current Network Key	The current key that you use.
Network Key1/2/3/4	Set the network key. If it is 128-bit key, you need to enter 13 ASCII characters or 26 hexadecimal digits. For the 64-bit key, you need to enter 5 ASCII characters or 10 hexadecimal digits.

- **Shared Mode**

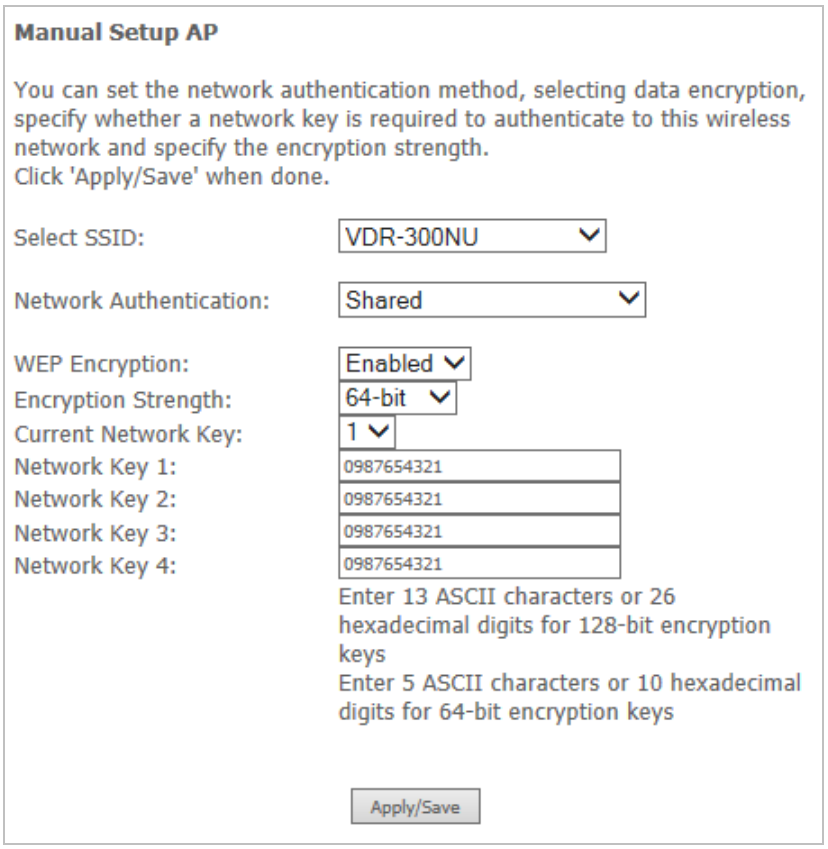


Figure 5-3-7

For the parameters' description of shared mode, please refer to the **Open Mode**.

- **802.1x**

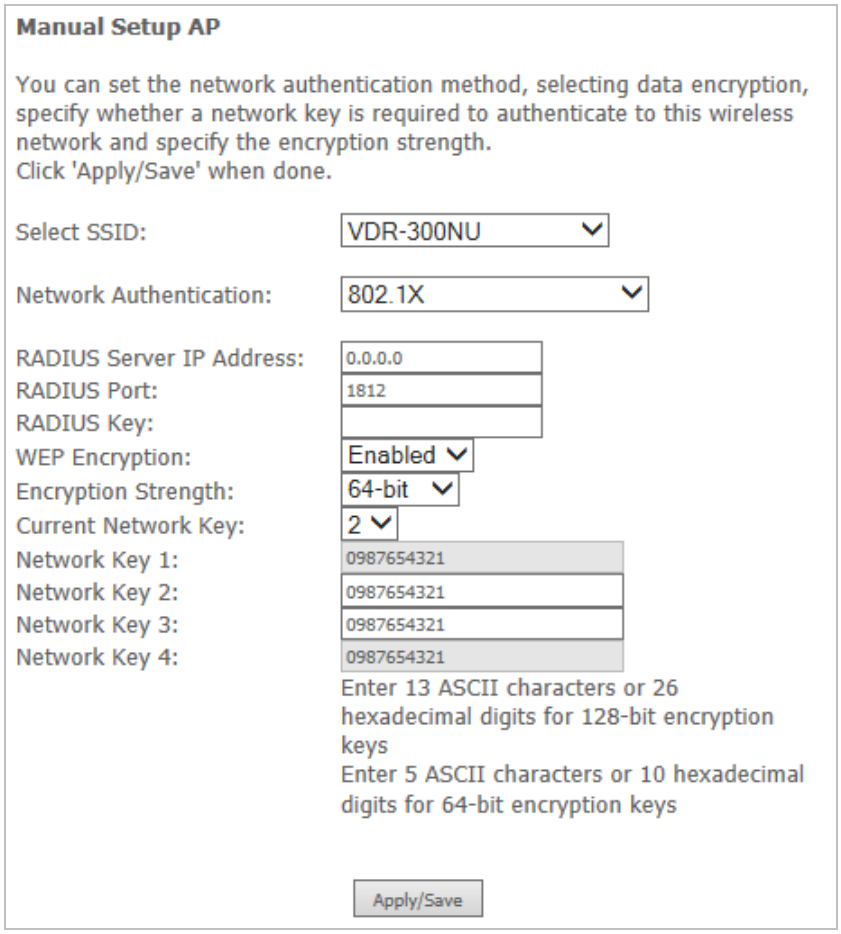


Figure 5-3-8

Object	Description
Select SSID	Select a SSID for configuring the security settings.
Network Authentication	Select the 802.1X in the drop-down list.
RADIUS Server IP Address	Enter the IP address of the RADIUS server. RADIUS server is used to authenticate the hosts on the wireless network.
RADIUS Port	The port number that the RADIUS server uses. The default port number is 1812. You may change it according to the server setting.
RADIUS Key	Set the RADIUS key for accessing the RADIUS server.
WEP Encryption	You can only select **Enabled**.
Encryption Strength	You can set 64-bit or 128-bit key.
Current Network Key	The current key that you use.
Network Key1/2/3/4	Set the network key. If it is 128-bit key, you need to enter 13 ASCII characters or 26 hexadecimal digits. For the 64-bit key, you need to enter 5 ASCII characters or 10 hexadecimal digits.

■ **WPA Mode**

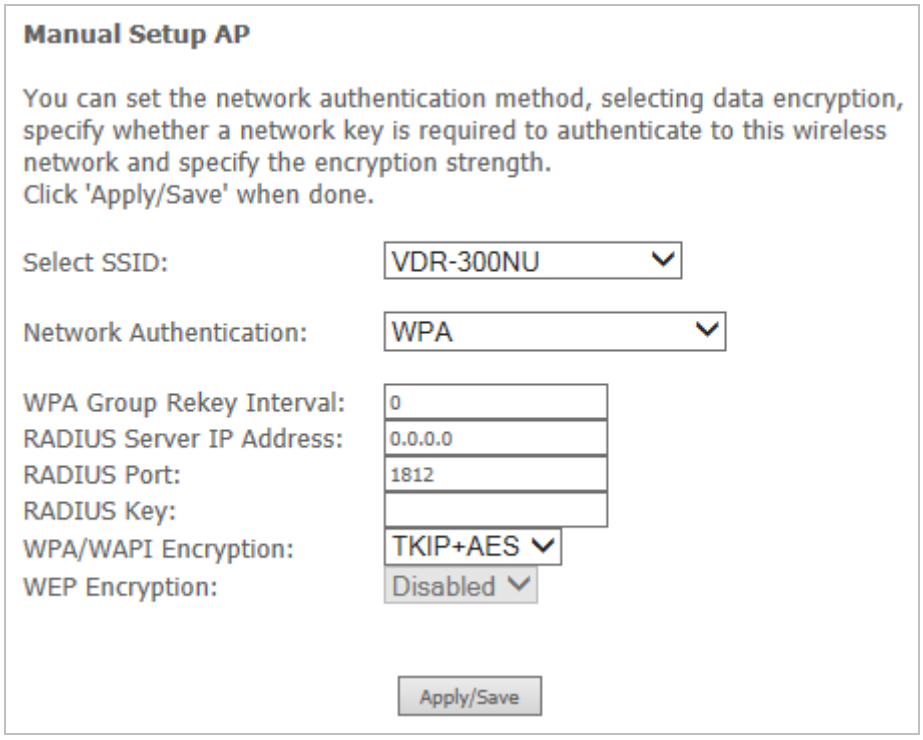


Figure 5-3-9

Object	Description
Select SSID	Select a SSID for configuring the security settings.
Network Authentication	Select the WPA mode.
WPA Group Rekey Interval	Setting the interval for renewing key.
RADIUS Server IP Address	Enter the IP address of the RADIUS server. RADIUS server is used to authenticate the hosts on the wireless network.
RADIUS Port	The port number that the RADIUS server uses. The default port number is 1812. You may change it according to the server setting.
RADIUS Key	Set the RADIUS key for accessing the RADIUS server.
WPA/WAPI Encryption	You may select AES, or TKIP+AES.

■ **WPA-PSK Mode**

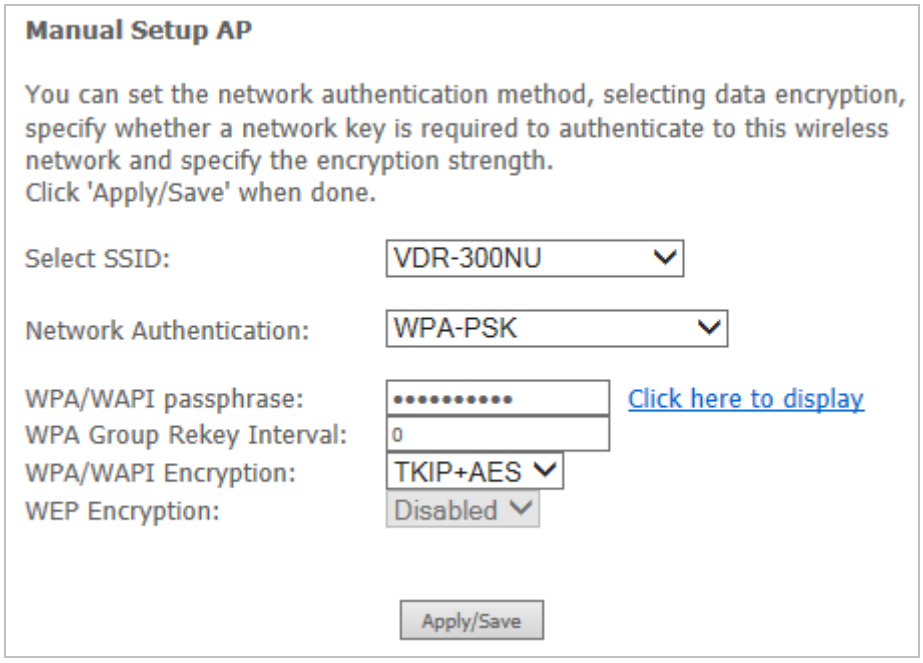


Figure 5-3-10

Object	Description
Select SSID	Select a SSID for configuring the security settings.
Network Authentication	Select the WPA-PSK mode.
WPA/WAPI passphrase	The key for WPA encryption. Click the Click here to display button to display the current key. The default key is 87654321.
WPA Group Rekey Interval	Setting the interval for renewing key.
WPA/WAPI Encryption	You may select AES, or TKIP+AES.

■ **WPA2 Mode**

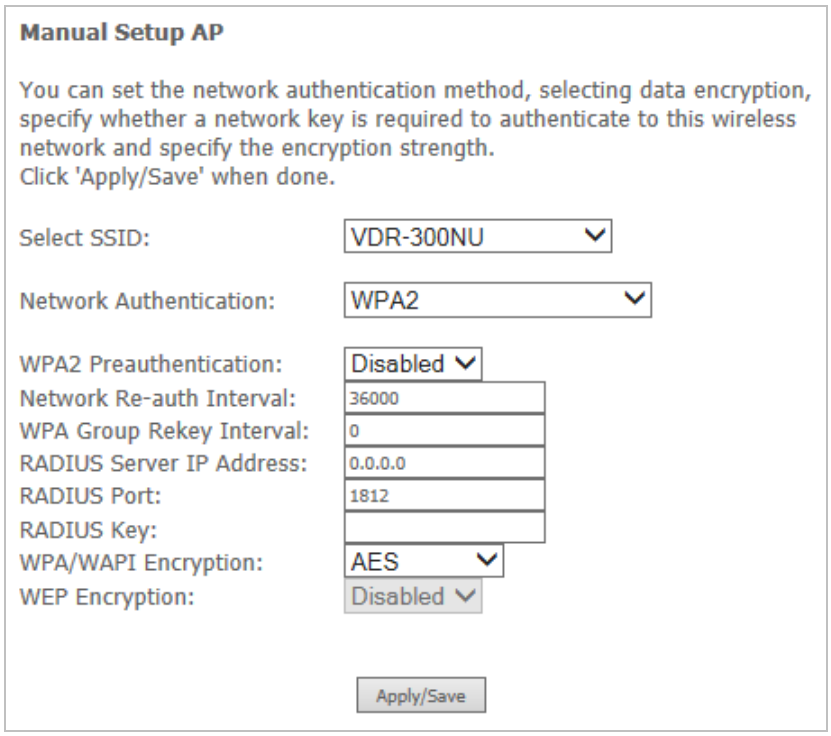


Figure 5-3-11

Object	Description
Select SSID	Select a SSID for configuring the security settings.
Network Authentication	Select the WPA2 mode.
WPA2 Preauthentication	Enable or disable pre-authentication.
Network Re-auth Interval	Set the network re-auth interval.
WPA Group Rekey Interval	Setting the interval for renewing key.
RADIUS Server IP Address	Enter the IP address of the RADIUS server. RADIUS server is used to authenticate the hosts on the wireless network.
RADIUS Port	The port number that the RADIUS server uses. The default port number is 1812. You may change it according to the server setting.
RADIUS Key	Set the RADIUS key for accessing the RADIUS server.
WPA/WAPI Encryption	You may select AES, or TKIP+AES.

- **WPA2-PSK**

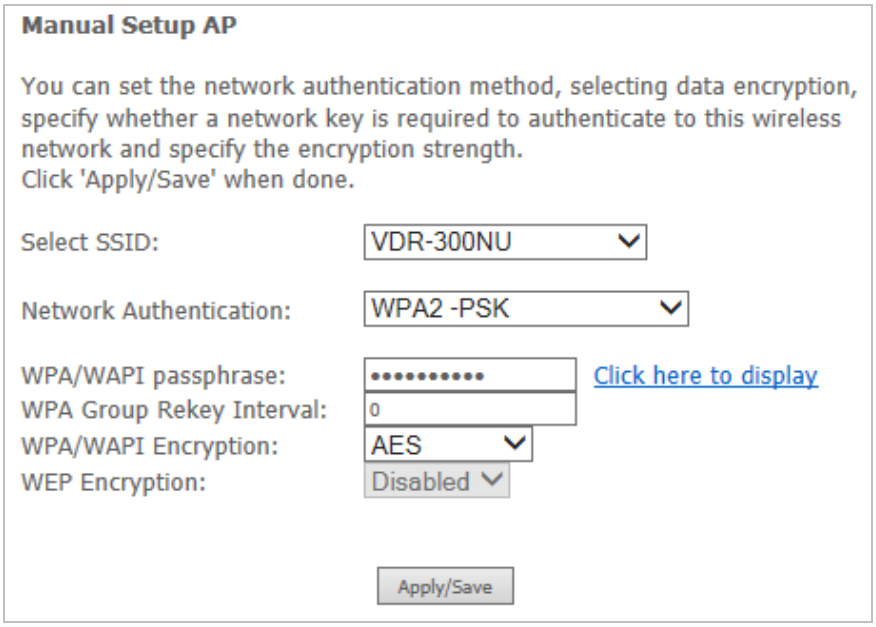


Figure 5-3-12

For the parameters' description of WPA2-PSK mode, please refer to the **WPA-PSK mode**.

- **Mixed WPA2/WPA**

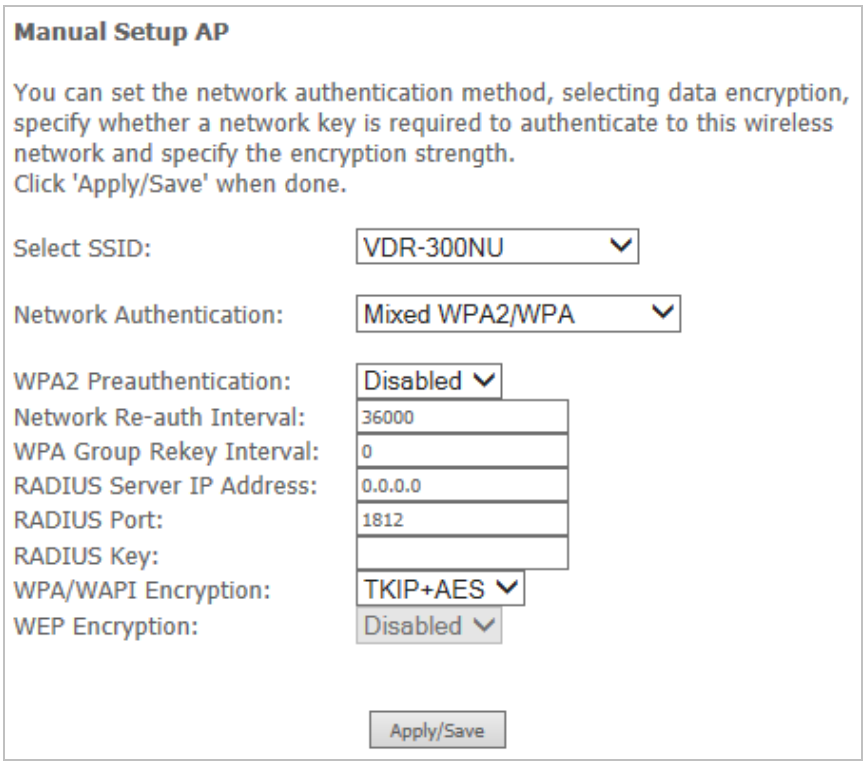


Figure 5-3-13

For the parameters' description of Mixed WPA2/WPA mode, please refer to the **WPA2 mode**.

- **Mixed WPA2/WPA-PSK**

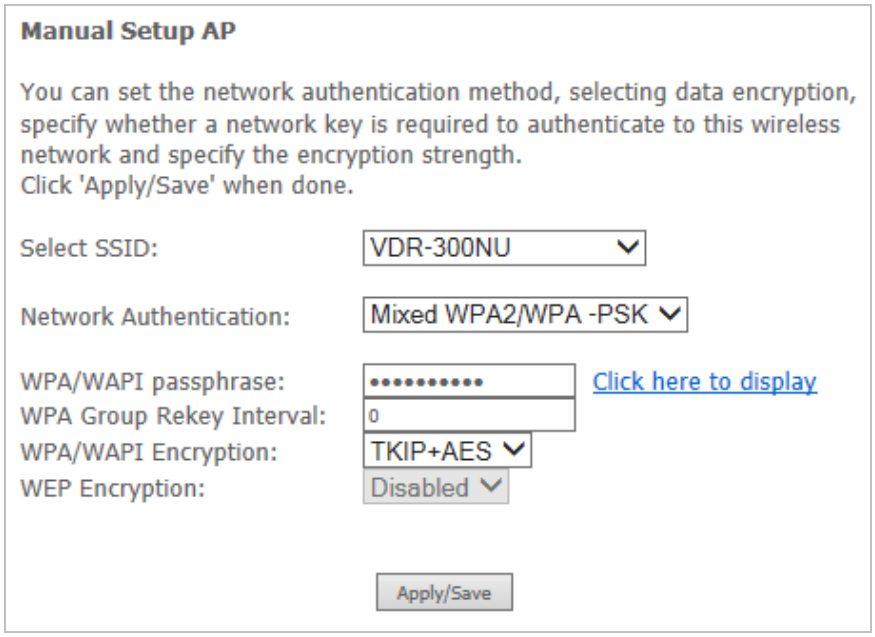


Figure 5-3-14

For the parameters' description of Mixed WPA2/WPA-PSK mode, please refer to the **WPA-PSK** mode.

5.3.3 MAC Filter

Choose **Wireless > MAC Filter** to display the following page.

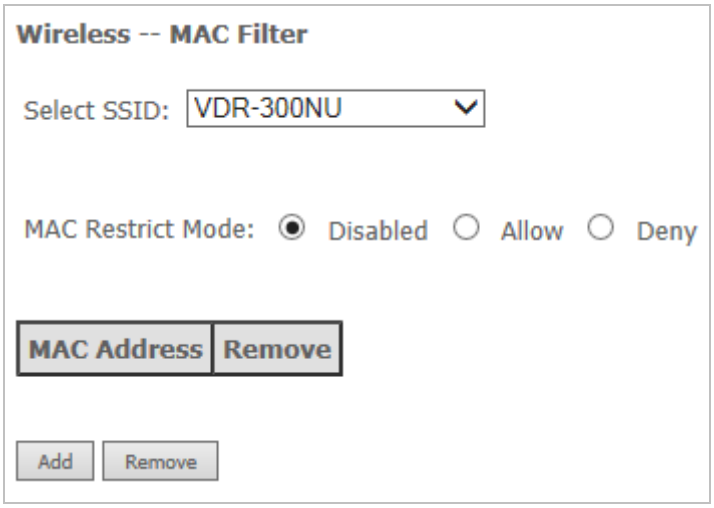


Figure 5-3-15

This page is used to allow or reject the wireless clients to access the wireless network of the wireless router. In this page, you can add or remove the MAC filters.

The MAC restrict modes include **Disabled**, **Allow**, and **Deny**.

Object	Description
Disabled	Disable the wireless MAC address filtering function.
Allow	Allow the wireless clients with the MAC addresses in the MAC Address list to access the wireless network of the wireless router.
Deny	Reject the wireless clients with the MAC addresses in the MAC Address list to access the wireless network of the wireless router.

Click the **Add** button to display the following page.

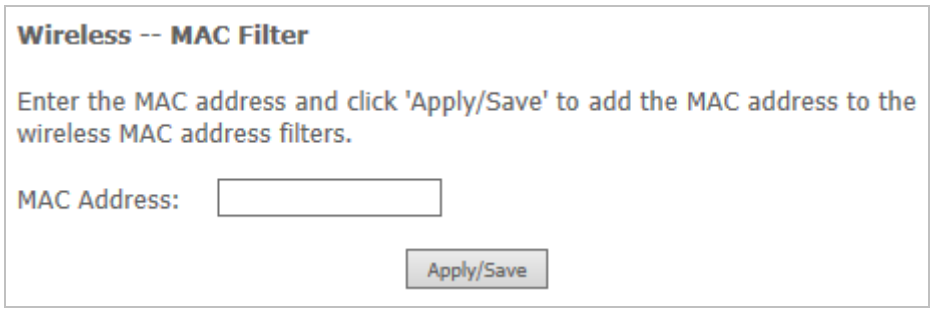


Figure 5-3-16

On this page, enter the MAC address of the wireless client, and then click the **Apply/Save** button to add the MAC address to the MAC address list.

5.3.4 Wireless Bridge

Choose **Wireless > Wireless Bridge** to display the following page.

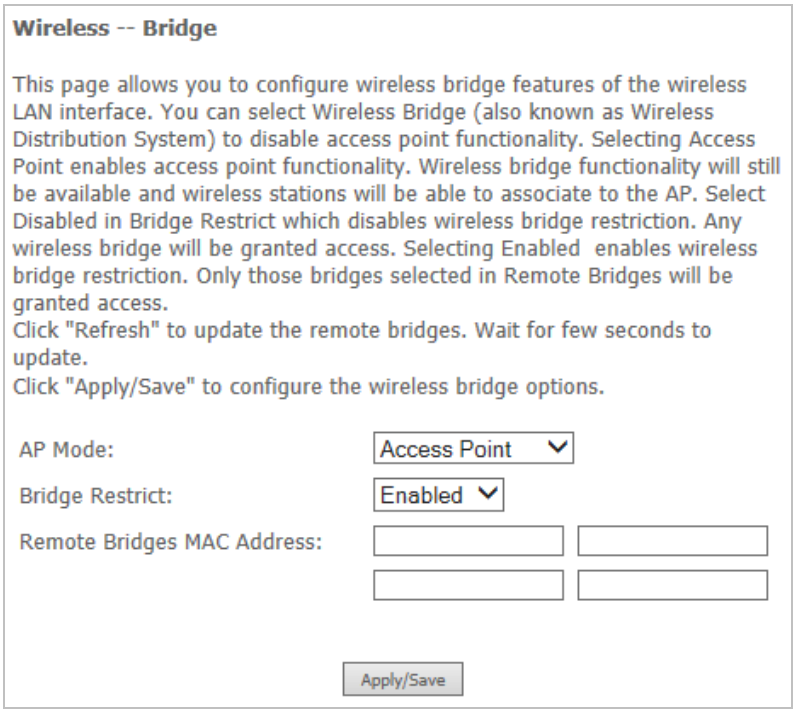


Figure 5-3-17

This page allows you to configure the wireless bridge features of the wireless LAN interface.

Object	Description
AP mode	You may select Access Point or Wireless Bridge.
Bridge Restrict	Enable or disable the bridge restrict function.
Remote Bridges MAC Address	Enter the remote bridge MAC address.

After finishing setting, click the **Apply/Save** button to save and apply the settings.

5.3.5 Advanced Settings

Choose **Wireless > Advanced** to display the following page. This page allows you to configure the advanced features of the wireless LAN interface. Usually, you do not need to change the settings on this page.

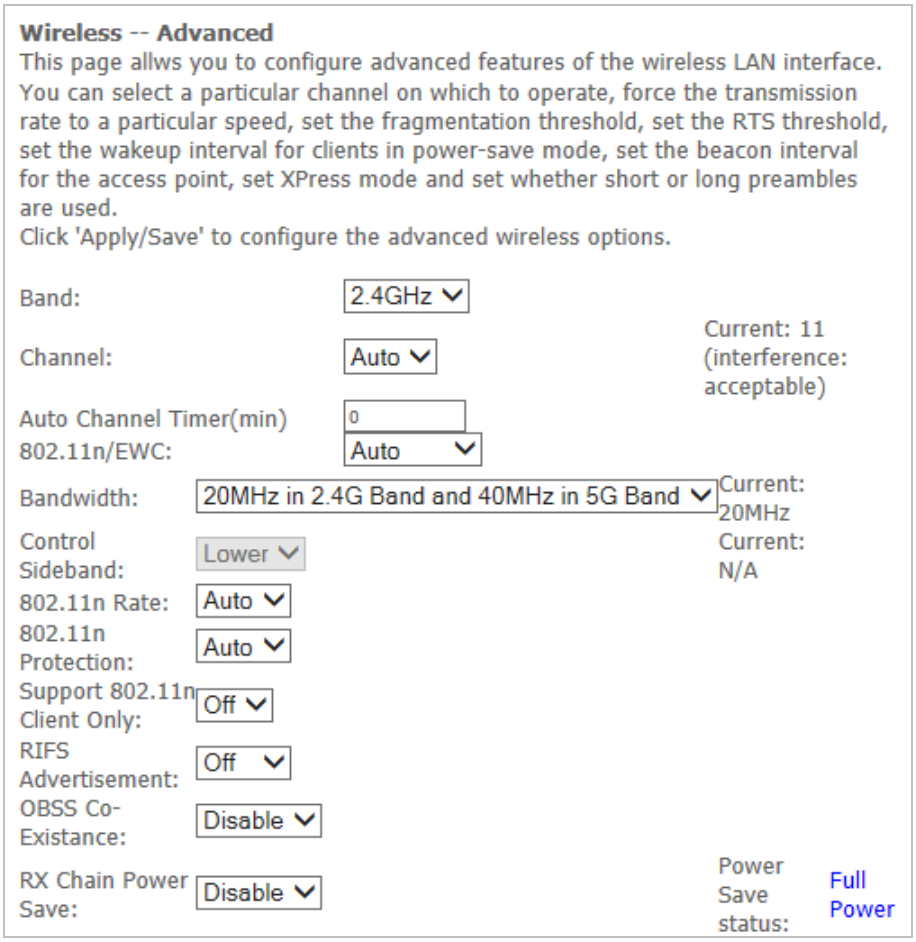


Figure 5-3-18

Object	Description
Band	You can select 2.4GHz or 5GHz.

Channel	Fill in the appropriate channel to correspond with your network settings. All devices in your wireless network must use the same channel in order to work correctly. This router supports auto channeling functionality.
Auto Channel Timer(min)	Specifies the timer of auto channeling.
802.11n/EWC	Select disable 802.11n or Auto.
Bandwidth	Select the bandwidth for the network. You can select 20MHz in Both Bands, 20MHz in 2.4G Band and 40MHz in 5G Band, or 40MHz in Both Bands.
Control Sideband	If you select 20MHz in Both Bands or 20MHz in 2.4G Band and 40MHz in 5G Band, the service of control sideband does not work. When you select 40MHz in Both Bands as the bandwidth, the following page appears. Then you can select Lower or Upper as the value of sideband. As the control sideband, when you select Lower, the channel is 1~7. When you select Upper, the channel is 5~11.
802.11n Rate	Select the transmission rate for the network. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select Auto to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client. The default value is **Auto**.
802.11n Protection	The 802.11n standards provide a protection method so 802.11b/g and 802.11n devices can co-exist in the same network without “speaking” at the same time.
Support 802.11n Client Only	Only stations that are configured in 802.11n mode can associate.
RIFS Advertisement	RIFS is one of the new feature introduced in IEEE 802.11n to improve its efficiency.
OBSS Co-Existance	OBSS (Overlapping BSS) is the term that the standards community uses to indicate that other APs overlap with the BSS (AP).
RX Chain Power Save	Enable or Disable this function.
Multicast Rate	Select the multicast transmission rate for the network. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select Auto to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router

	and a wireless client. The default value is **Auto**.
Basic Rate	Select the basic transmission rate ability for the AP.
Fragmentation Threshold	Packets that are larger than this threshold are fragmented into multiple packets. Try to increase the fragmentation threshold if you encounter high packet error rates. Do not set the threshold too low, since this can result in reduced networking performance.
RTS Threshold	This value should remain at its default setting of 2347.Should you encounter inconsistent data flow, only minor reductions are recommended. Should you encounter inconsistent data flow, only minor reduction of the default value, 2347, is recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. The RTS Threshold value should remain at its default value of 2347.
DTIM Interval	Enter a value between 1 and 255 for the Delivery Traffic Indication Message (DTIM.) A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.
Beacon Interval	A beacon is a packet of information that is sent from a connected device to all other devices where it announces its availability and readiness. A beacon interval is a period of time (sent with the beacon) before sending the beacon again. The beacon interval may be adjusted in milliseconds (ms). Default (100) is recommended.
XPress Technology	Select Enable or Disable. This is a special accelerating technology for IEEE802.11g. The defaule is Disabled.
Transmit Power	Adjust the transmission range here. This tool can be helpful for security purposes if you wish to limit the transmission range.
WMM (Wi-Fi Multimedia)	Select whether WMM is enable or disabled. Before you disable WMM, you should understand that all QoS queues or traffic classes relate to wireless do not take effects.
WMM No Acknowledgement	Select whether ACK in WMM packet. By default, the 'Ack Policy' for each access category is set to Disable, meaning that an acknowledge packet is returned for every packet received. This provides a more reliable transmission but increases traffic load, which decreases performance. To disable the acknowledgement can be useful for Voice, for example, where speed of transmission is important and packet loss is tolerable to a certain degree.
WMM APSD	APSD is short for automatic power save delivery, Selecting enable will

	make it has very low power consumption. WMM Power Save is an improvement to the 802.11e amendment adding advanced power management functionality to WMM.

Click **Apply/Save** to configure the advanced wireless options and make the changes take effect.

The advanced wireless setting is only for the advanced user. For the common user, do not change any settings on this page.

5.3.6 Station Info

Choose **Wireless > Station Info** to display the following page.

Figure 5-3-19

This page shows the authenticated wireless stations and their status.

5.4 Diagnostics

5.4.1 Diagnostics

Click **Diagnostics > Diagnostics**, and the following page appears.

This page is used to test the connection to your local network, the connection to your DSL service provider, and the connection to your Internet service provider.

You may diagnose the connection by clicking the **Test** button or click the **Test With OAM F4** button. If the test continues to fail, click Help and follow the troubleshooting procedures.

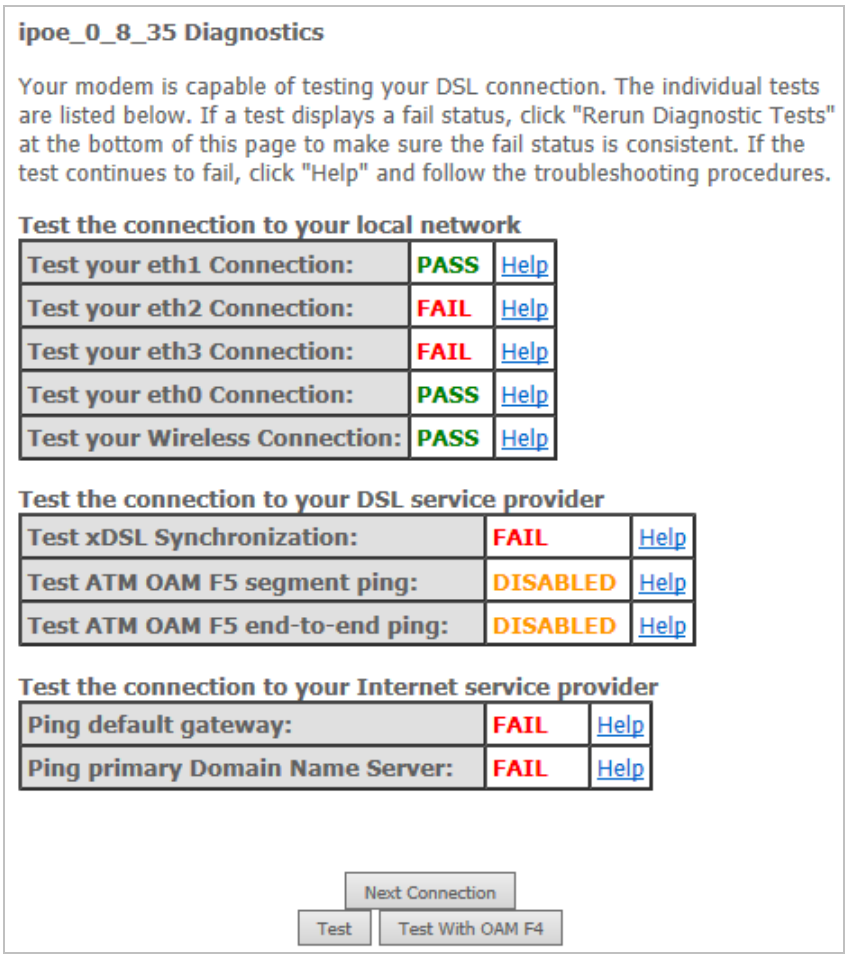


Figure 5-4-1

5.4.2 Fault Management

The Fault Management is only available for VDSL PTM

Click **Diagnostics > Fault Management** and the following page appears.

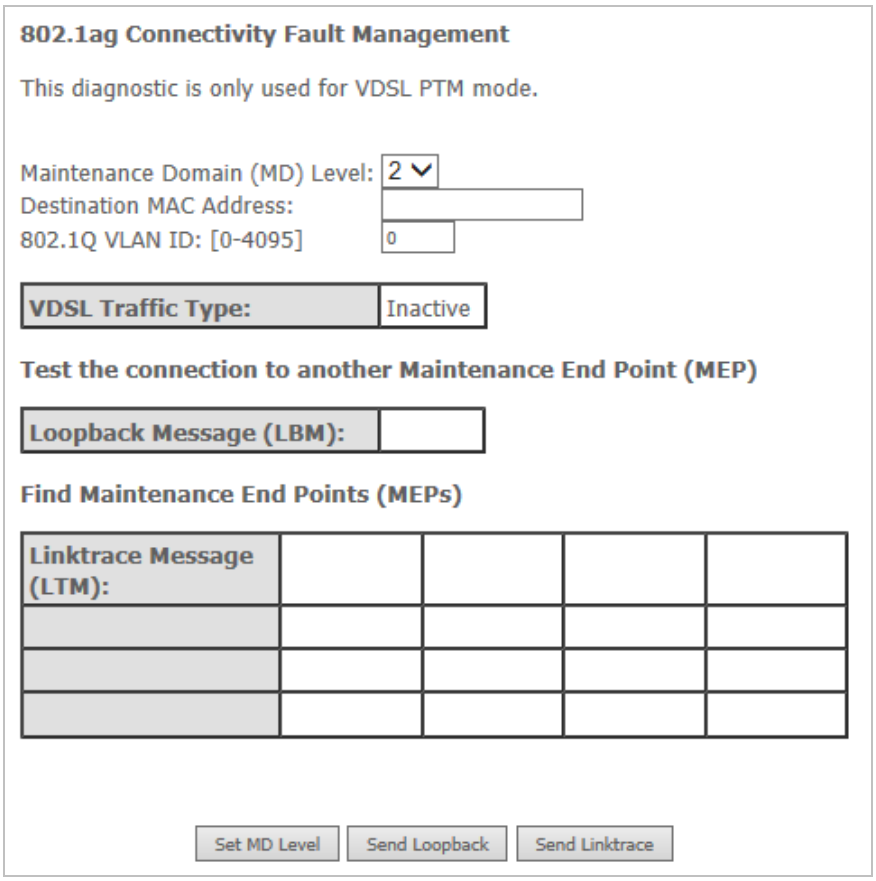


Figure 5-4-2

5.5 Management

Choose **Management** and the submenus of Management are shown below:

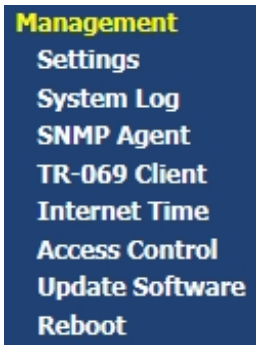


Figure 5-5-1

5.5.1 Settings

■ Backup

Choose **Management > Settings > Backup** to display the following page.

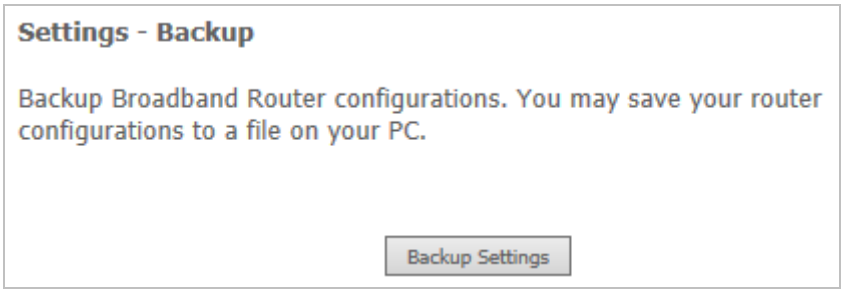


Figure 5-5-2

On this page, click the **Backup Settings** button to save your router's settings to your local PC.

■ Update

Choose **Management > Settings > Update**, and the following page appears.

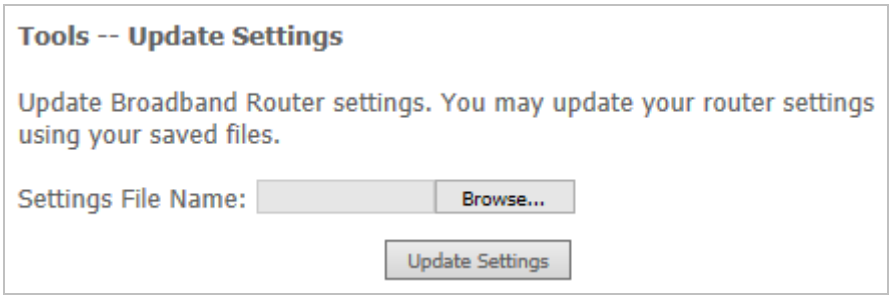


Figure 5-5-3

On this page, click the **Browse…** button to select the correct new settings file and then click the **Update Settings** button to update the router's settings.

■ Restore Default

Choose **Management > Settings > Restore Default** to display the following page.

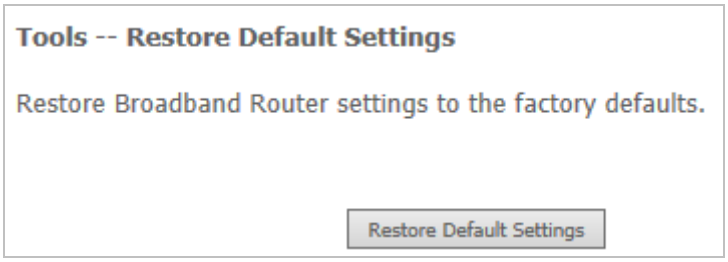


Figure 5-5-4

On this page, click the **Restore default settings** button, and then system returns to the default settings.

5.5.2 System Log

Choose **Management > System Log** to display the following page.

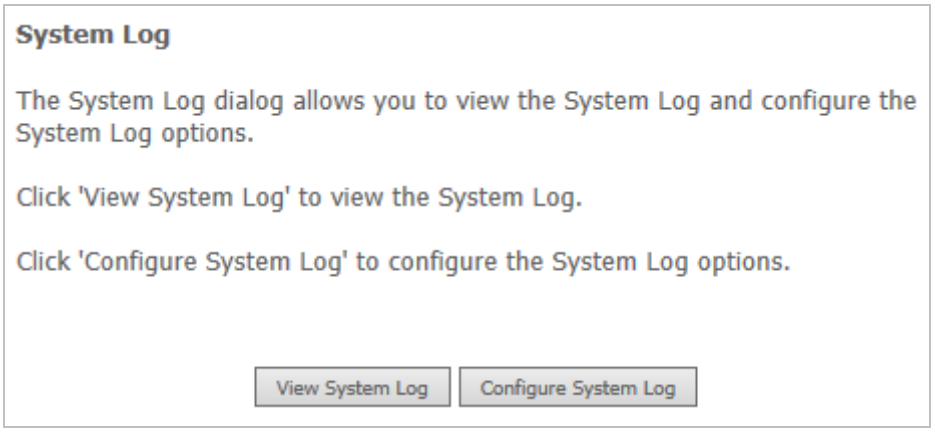


Figure 5-5-5

On this page, you are allowed to configure the system log and view the security log.

■ Configuring the System Log

Click the **Configure System Log** button to display the following page.

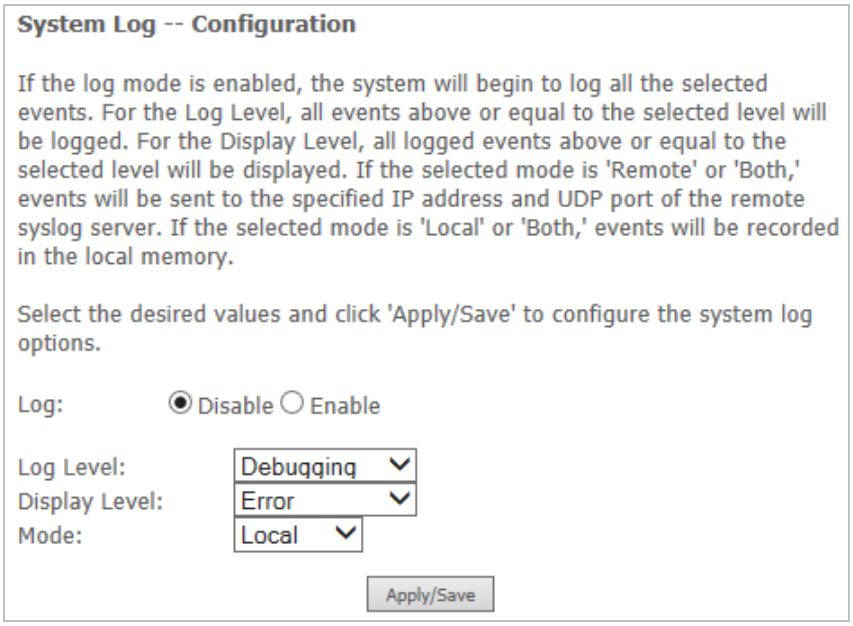


Figure 5-5-6

On this page, you can set 3 types of system log modes, including Local, Remote, and Both.

Object	Description
Local	When selecting Local, the events are recorded in the local memory.
Remote	When selecting Remote, the events are sent to the specified IP address and UDP port of the remote system log server.
Both	When selecting Both, the events are recorded in the local memory or sent to the specified IP address and UDP port of the remote system log server.

After finishing setting, click the **Apply/Save** button to save and apply the settings.

If you want to log all the events, you need to select the Debugging log level.

■ View System Log

Click the **View System Log** button to display the following page.

Figure 5-5-7

On this page, you can view the system log. Click the **Refresh** button to refresh the system log. Click the **Close** button to exit.

5.5.3 SNMP Agent

Choose **Management > SNMP Agent**,and the following page appears.

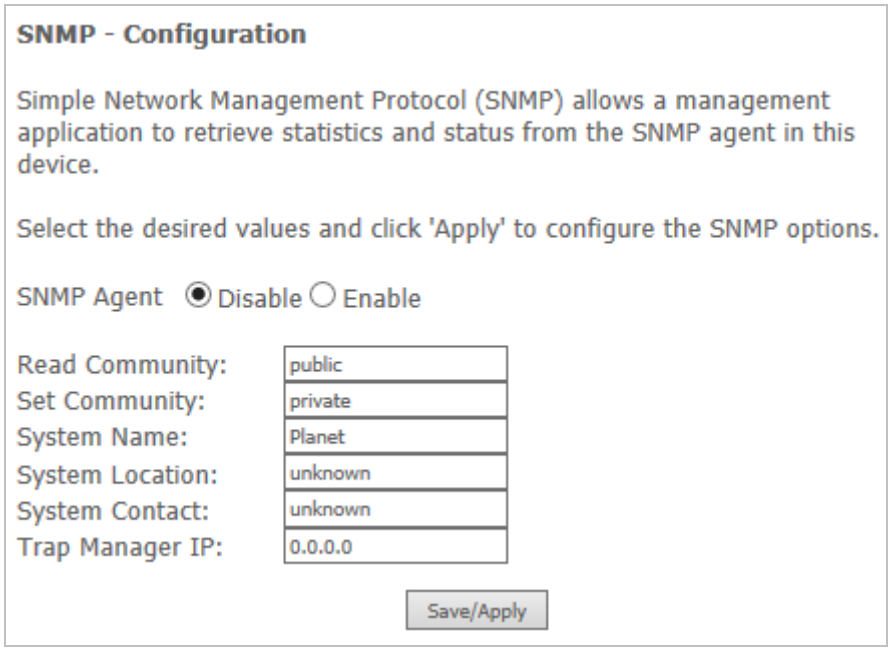


Figure 5-5-8

Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device. On this page, you may enable or disable the SNMP agent and set the parameters such as the read community, system name and trap manager IP.

After finishing setting, click the **Save/Apply** button to save and apply the settings.

5.5.4 TR-69 Client

Choose **Management > TR-069Client** to display the following page.

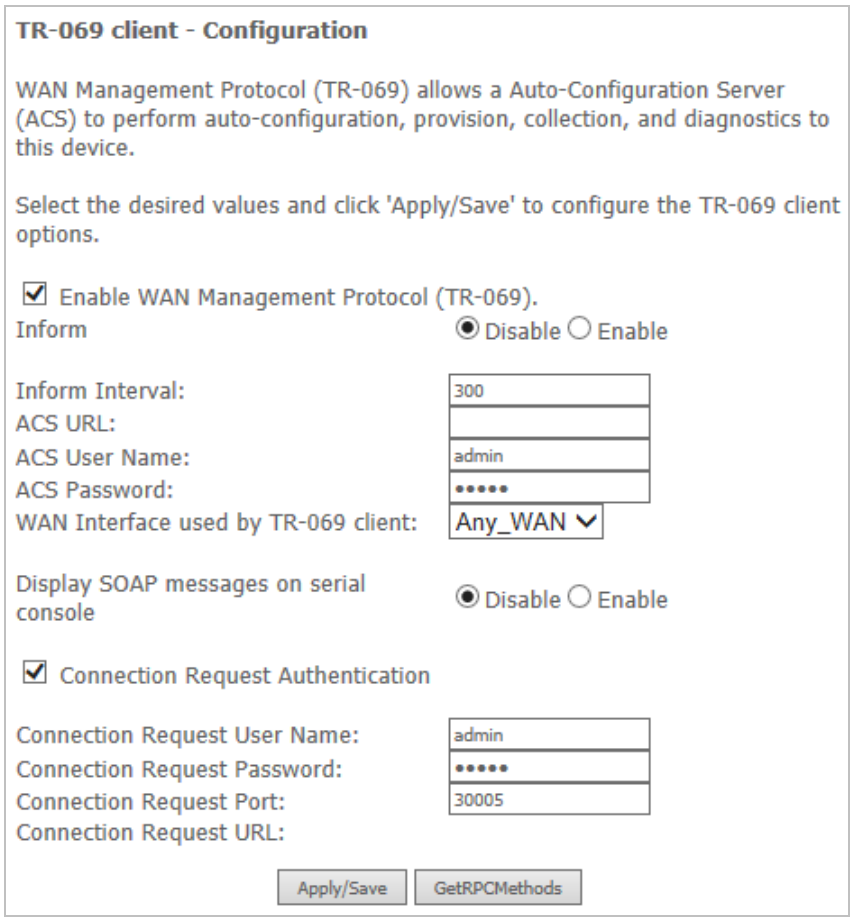


Figure 5-5-9

WAN Management Protocol (TR-069) allows an **Auto-Configuration Server** (**ACS**) to perform auto-configuration, provision, collection, and diagnostics to this device. On this page, you may configure the parameters such as the ACS URL, ACS password, and connection request user name.

After finishing setting, click the **Apply/Save** button to save and apply the settings.

5.5.5 Internet Time

Choose **Management > Internet Time** to display the following page.

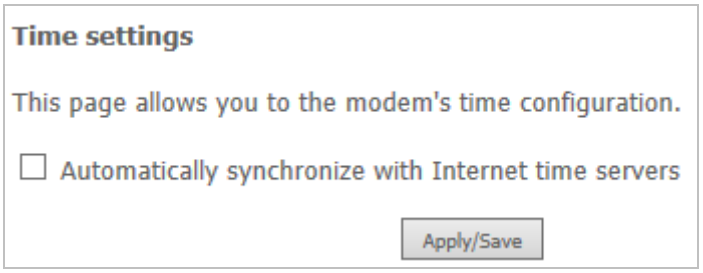


Figure 5-5-10

On this page, you may configure the router to synchronize its time with the Internet time servers.

After enabling **Automatically synchronize with Internet time servers**, the following page appears.

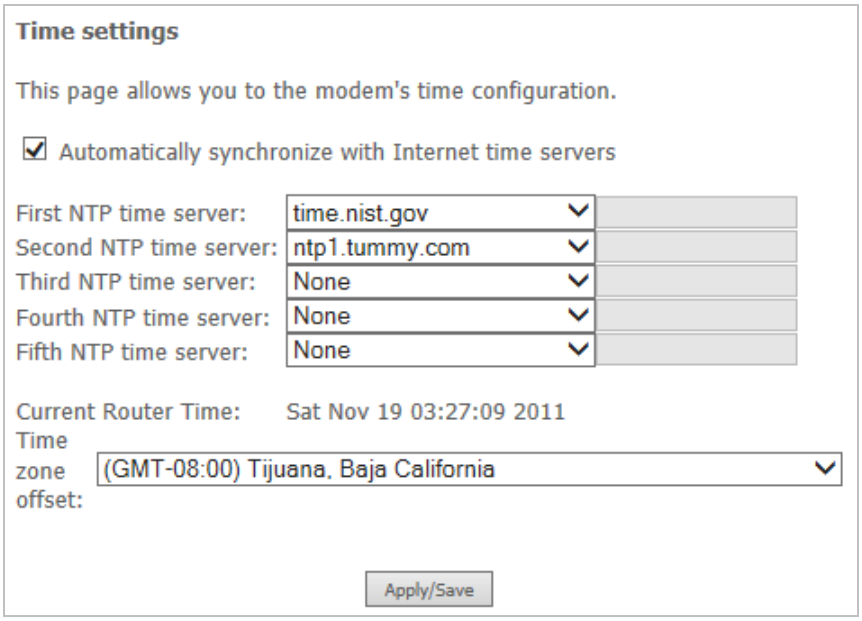


Figure 5-5-11

On this page, set the proper time servers, and then click the **Apply/Save** button to save and apply the settings.

5.5.6 Access Control

■ Passwords

Choose **Management > Access Control > Passwords** and the following page appears.

Figure 5-5-12

On the page, you can modify the username and password of different users. After finishing setting, click the **Apply/Save** button to save and apply the settings.

■ Services

Choose **Management > Access Control > Services Control** and the following page appears.

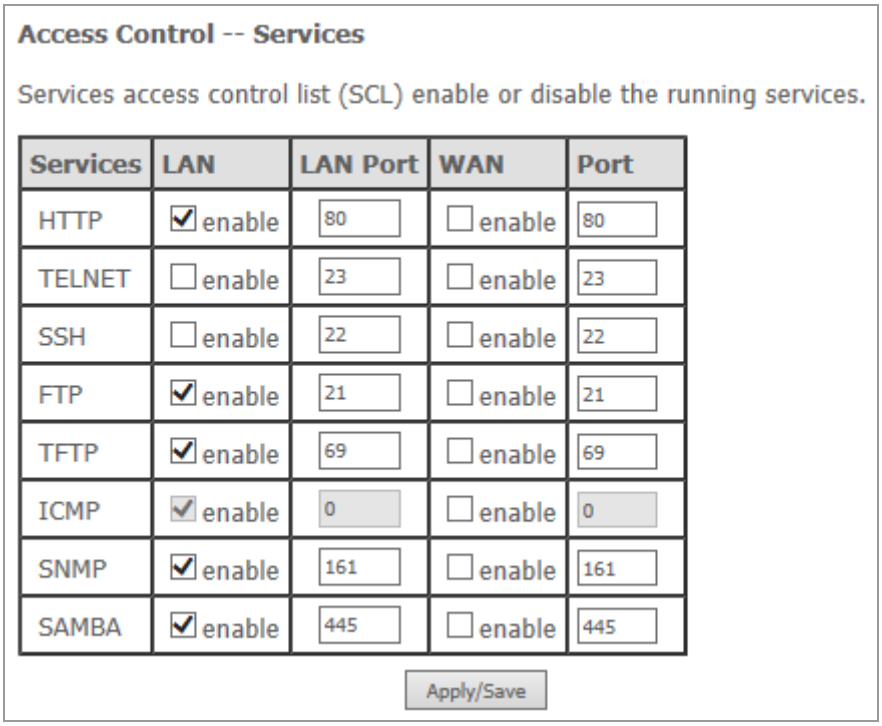


Figure 5-5-13

On this page, you can enable or disable the different types of services. After finishing setting, click the **Apply/Save** button to save and apply the settings.

5.5.7 Update Software

Choose **Management > Update Software** and the following page appears.

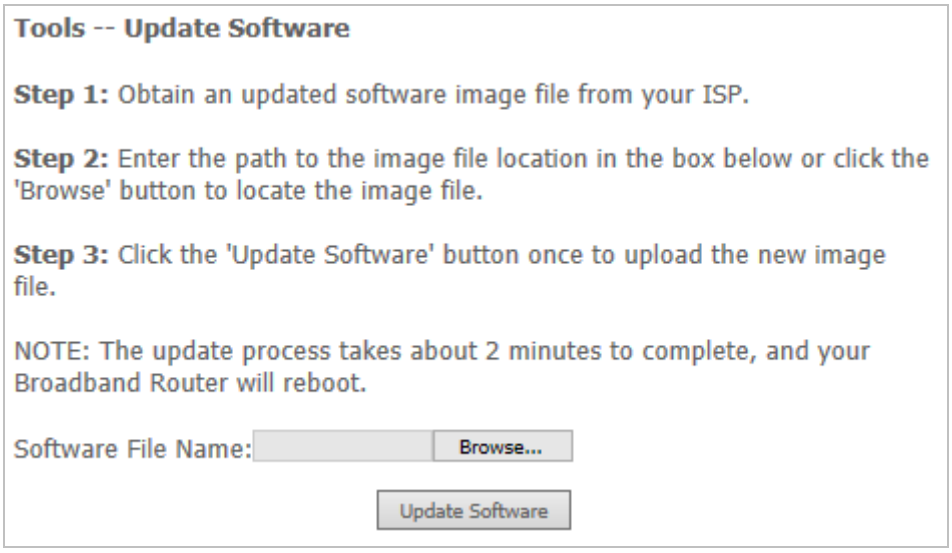


Figure 5-5-14

If you want to upload the software, click the **Browse…** button to choose the new software and then click the **Update Software** button.

Note

When software update is in progress, DO NOT shut down the router. After software update completes, the router automatically reboots.

Please make sure that the new software for updating is correct, and do not use other software to update the router.

5.5.8 Reboot

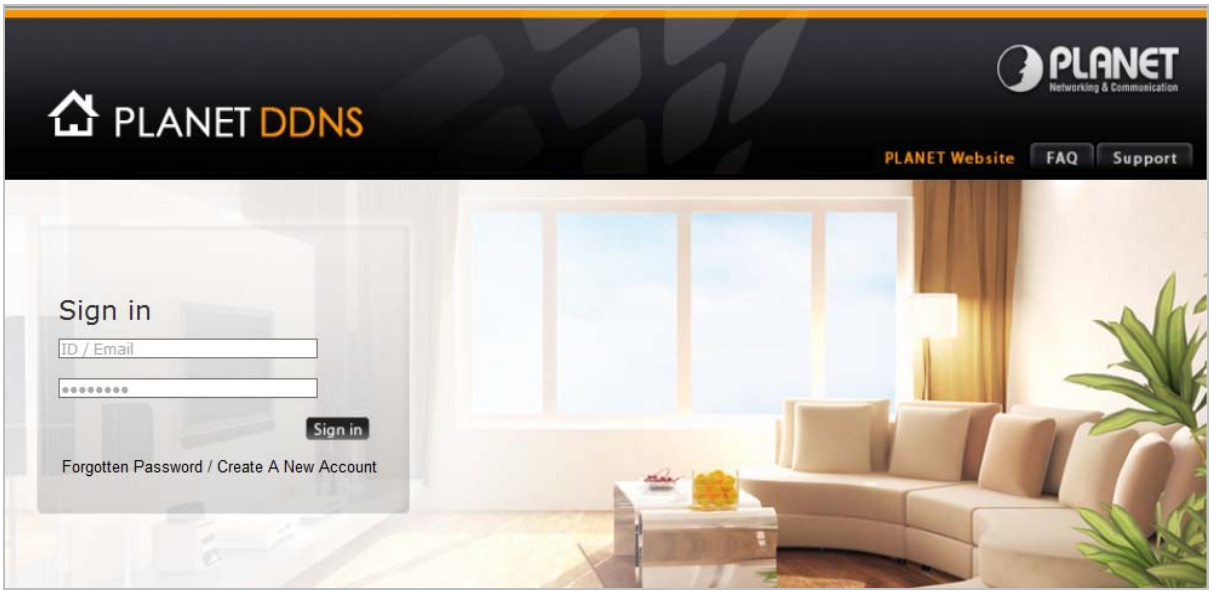
Choose **Management > Reboot** and the following page appears.

Figure 5-5-15

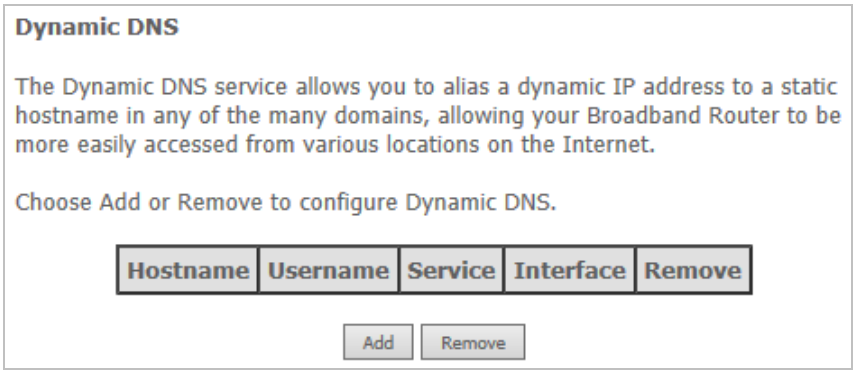
On this page, click the **Reboot** button and then the router reboots.

Appendix A: Planet DDNS

First of all, please go to http://www.planetddns.com to register a Planet DDNS account, and refer to the FAQ (http://www.planetddns.com/index.php/faq) for how to register a free account.

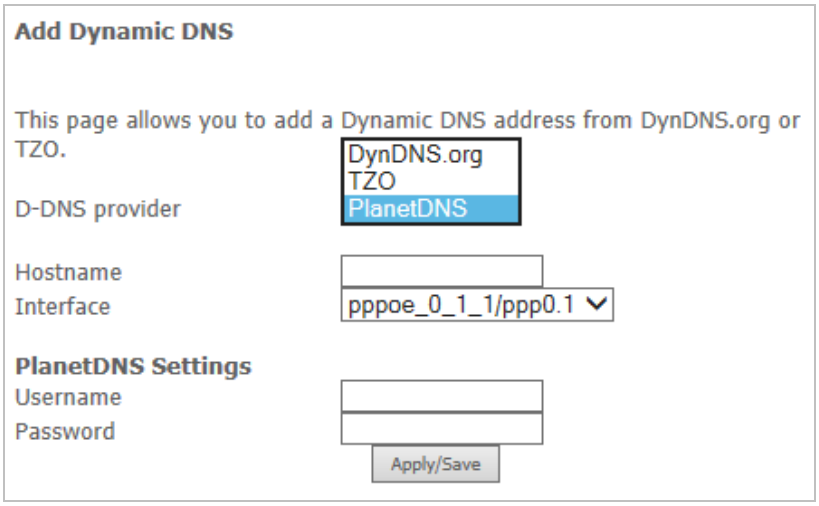


To select **DNS > Dynamic DDNS**



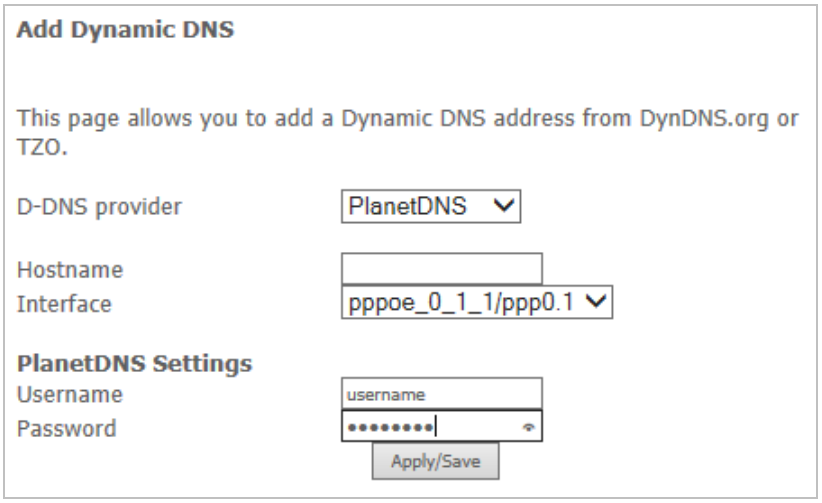
Step 1. Press **Add** button

Step 2. Select **Planet DDNS**



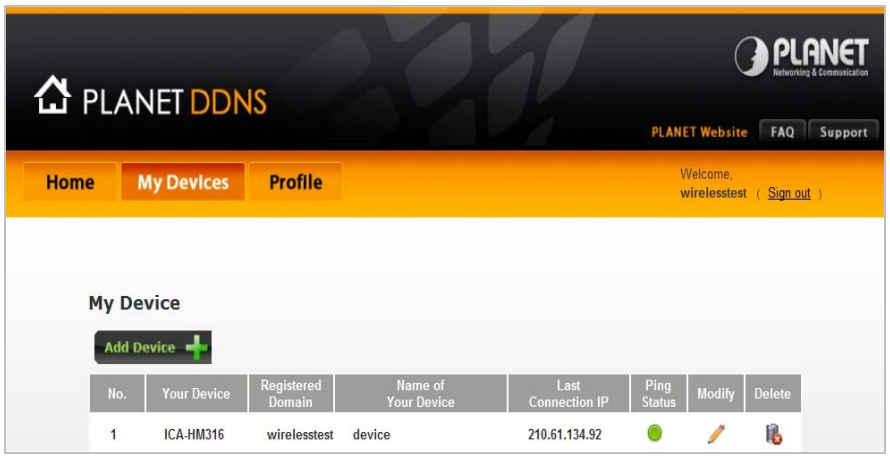
Step 3. Type the User Name for your DDNS account.

Step 4. Type the Password for your DDNS account.



Apply the settings and ensure you have connected the WAN port to the Internet. In a remote device, enter the Domain Name to the internet browser's address bar.

You can go to My Devices page of Planet DDNS website to check if the "Last Connection IP" is displayed. This indicates your DDNS service is working properly.



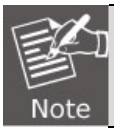
Appendix B: Performance of VDSL Router Profiles

The table below is a performance table for profile and line distance; this data is just for reference. The actual data rate will vary on the quality of the telephone line and environmental factors.

For better performance, we suggest you use the AWG-26 or above cable for your connection, and the best line distance is about 1km.

(Data Rate: Mbps)

Profile / Distance		200m	400m	800m	1000m
AnnexA_EU-32_30a	Up	100	50	5	
	Down	100	100	60	
AnnexA_ EU-32_17a	Up	55	45	20	7
	Down	100	100	55	50
AnnexA_EU-32_12a	Up	55	45	20	7
	Down	80	70	60	50
AnnexA_EU-32_12b	Up	55	45	20	7
	Down	80	70	60	50
AnnexA_EU-32_8a	Up	15	13	9	6
	Down	80	72	60	50
AnnexA_EU-32_8b	Up	15	13	9	6
	Down	80	72	60	50
AnnexA_EU-32_8c	Up	15	14	10	7.5
	Down	80	72	60	50
AnnexA_EU-32_8d	Up	15	13	9	6
	Down	80	72	60	50



The real data rate and distance are based on your real environment. This is just for reference.

Appendix C: Glossary

Address mask

A bit mask select bits from an Internet address for subnet addressing. The mask is 32 bits long and selects the network portion of the Internet address
and one or more bits of the local portion. Sometimes it called subnet mask.

VDSL

VDSL2 (Very High-Bit-Rate Digital Subscriber Line 2), G.993.2 is the newest and most advanced standard of xDSL broadband wire line communications.

ADSL

Asymmetric digital subscriber line

AAL5

ATM Adaptation Layer - This layer maps higher layer user data into ATM cells, making the data suitable for transport through the ATM network.

ATM

Asynchronous Transfer Mode - A cell-based data transfer technique in which channel demand determines packet allocation. ATM offers fast packet technology,
real time, and demand led switching for efficient use of network resources.

AWG

American Wire Gauge - The measurement of thickness of a wire

Bridge

A device connects two or more physical networks and forward packets between them. Bridges can usually be made to filter packets, that is, to forward only certain traffic. Related devices are repeaters which simply forward electrical signals from one cable to the other and full-fledged routers which make routing decisions based on several criteria.

Broadband

Characteristic of any network multiplexes independent network carriers onto a single cable. Broadband technology allows several networks to coexist on one single cable; traffic from one network does not interfere with traffic from another. Broadcast a packet delivery system where a copy of a given packet is given to all hosts attached to the network. Example: Ethernet.

CO
Central Office. Refers to equipment located at a Telco or service provider's office.

CPE
Customer Premises Equipment located in a user's premises

DHCP (Dynamic Host Configuration Protocol)
DHCP is software that automatically assigns IP addresses to client stations logging onto a TCP/IP network. DHCP eliminates having to manually assign permanent IP addresses to every device on your network. DHCP software typically runs in servers and is also found in network devices such as Routers.

DMT
Discrete Multi-Tone frequency signal modulation

Downstream rate
The line rate for return messages or data transfers from the network machine to the user's premises machine.

DSLAM
Digital Subscriber Line Access Multiplex

Dynamic IP Addresses
A dynamic IP address is an IP address that is automatically assigned to a client station (computer, printer, etc.) in a TCP/IP network. Dynamic IP addresses are typically assigned by a DHCP server, which can be a computer on the network or another piece of hardware, such as the Router. A dynamic IP address may change every time your computer connects to the network.

Encapsulation
The technique layer protocols in which a layer adds header information to the protocol data unit (PDU) from the layer above. As an example, in Internet terminology, a packet would contain a header from the physical layer, followed by a header from the network layer (IP), followed by a header from the transport layer (TCP), and followed by the application protocol data.

Ethernet
One of the most common local area network (LAN) wiring schemes, Ethernet has a transmission rate of 10 Mbps.

FTP

File Transfer Protocol. The Internet protocol (and program) transfer files between hosts.

Hop count

A measure of distance between two points on the Internet. It is equivalent to the number of gateways that separate the source and destination.

HTML

Hypertext Markup Language - The page-coding language for the World Wide Web.

HTML browser

A browser used to traverse the Internet, such as Netscape or Microsoft Internet Explorer.

http

Hypertext Transfer Protocol - The protocol carry world-wide-web (www) traffic between a www browser computer and the www server being accessed.

ICMP

Internet Control Message Protocol - The protocol handle errors and control messages at the IP layer. ICMP is actually part of the IP protocol.

Internet address

An IP address is assigned in blocks of numbers to user organizations accessing the Internet. These addresses are established by the United States Department
of Defense's Network Information Center. Duplicate addresses can cause major problems on the network, but the NIC trusts organizations to use individual
addresses responsibly. Each address is a 32-bit address in the form of x.x.x.x where x is an eight- bit number from 0 to 255. There are three classes: A, B and C, depending on how many computers on the site are likely to be connected.

Internet Protocol (IP)

The network layer protocol for the Internet protocol suite

IP address

The 32-bit address assigned to hosts that want to participate in a TCP/IP Internet.

ISP

Internet service provider - A company allows home and corporate users to connect to the Internet.

MAC
Media Access Control Layer - A sub-layer of the Data Link Layer (Layer 2) of the ISO OSI Model responsible for media control.

MIB
Management Information Base - A collection of objects can be accessed via a network management protocol, such as SNMP and CMIP (Common Management Information Protocol).

NAT
Network Address Translation - A proposal for IP address reuse, where the local IP address is mapped to a globally unique address.

NVT
Network Virtual Terminal

PAP
Password Authentication Protocol

PORT
The abstraction used in Internet transport protocols to distinguish among multiple simultaneous connections to a single destination host.

POTS
Plain Old Telephone Service - This is the term describe basic telephone service.

PPP
Point-to-Point-Protocol - The successor to SLIP, PPP provides router-to-router and host-to-network connections over both synchronous and asynchronous circuits.

PPPoE
PPP over Ethernet is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

Remote server
A network computer allows a user to log on to the network from a distant location.

RFC

Request for Comments - Refers to documents published by the Internet Engineering Task Force (IETF) proposing standard protocols and procedures for the Internet. RFC can be found at www.ietf.org.

Route

The path that network traffic takes from its source to its destination. The route a datagram may follow can include many gateways and many physical networks.
In the Internet, each datagram is routed separately.

Router

A system is responsible for making decisions about which of several paths network (or Internet) traffic will follow. To do this, it uses a routing protocol to gain information about the network and algorithms to choose the best route based on several criteria known as "routing metrics".

Routing Table

Information stored within a router that contains network path and status information. It is used to select the most appropriate route to forward information along.

Routing Information Protocol

Routers periodically exchange information with one another so that they can determine minimum distance paths between sources and destinations.

SNMP

Simple Network Management Protocol - The network management protocol of choice for TCP/IP-based Internet.

SOCKET

(1) The Berkeley UNIX mechanism for creating a virtual connection between processes.
(2) IBM term for software interfaces that allow two UNIX application programs to talk via TCP/IP protocols.

Spanning-Tree Bridge Protocol (STP)

Spanning-Tree Bridge Protocol (STP) - Part of an IEEE standard. A mechanism for detecting and preventing loops from occurring in a multi-bridged environment.
When three or more LAN's segments are connected via bridges, a loop can occur. Because of a bridge forwards all packets that are not recognized as being local,
some packets can circulate for long periods of time, eventually degrading system performance. This algorithm ensures only one path connects any pair of stations, selecting one bridge as the 'root' bridge, with the highest priority one as identifier, from which all paths should radiate.

Spoofing

A method of fooling network end stations into believing that keep alive signals have come from and returned to the host. Polls are received and returned locally at
either end

Static IP Address
A static IP address is an IP address permanently assigned to computer in a TCP/IP network. Static IP addresses are usually assigned to networked devices that are consistently accessed by multiple users, such as Server PCs, or printers. If you are using your Router to share your cable or DSL Internet connection, contact your ISP to see if they have assigned your home a static IP address. You will need that address during your Router's configuration.

Subnet
For routing purposes, IP networks can be divided into logical subnets by using a subnet mask. Values below those of the mask are valid addresses on the subnet.

TCP
Transmission Control Protocol - The major transport protocol in the Internet suite of protocols provides reliable, connection-oriented full-duplex streams.

TFTP
Trivial File Transfer Protocol. A simple file transfer protocol (a simplified version of FTP) that is often boot diskless workstations and other network devices such as routers over a network (typically a LAN).
Telnet
The virtual terminal protocol in the Internet suite of protocols - Allows users of one host to log into a remote host and act as normal terminal users of that host.

Transparent bridging
The intelligence necessary to make relaying decisions exists in the bridge itself and is thus transparent to the communicating workstations. It involves frame forwarding, learning workstation addresses, and ensuring no topology loops exist (in conjunction with the Spanning-Tree algorithm).

UDP
User Datagram Protocol - A connectionless transport protocol that runs on top of TCP/IP's IP. UDP, like TCP, uses IP for delivery; however, unlike TCP, UDP provides for exchange of datagram without acknowledgments or guaranteed delivery. Best suited for small, independent requests, such as requesting a MIB value from an SNMP agent, in which first setting up a connection would take more time than sending the data.

UNI signaling
User Network Interface signaling for ATM communications.

Virtual Connection (VC)
A link that seems and behaves like a dedicated point-to-point line or a system that delivers packets in sequence, as happens on an actual point-to-point network. In reality, the data is delivered across a network via the most appropriate route. The sending and receiving devices do not have to be aware of the options and the route is chosen only when a message is sent. There is no pre-arrangement, so each virtual connection exists only for the duration of that one transmission.

WAN

Wide area network - A data communications network that spans any distance and is usually provided by a public carrier (such as a telephone company or service provider).

EC Declaration of Conformity

English	Hereby, **PLANET Technology Corporation,** declares that this **802.11n Dual band Wireless VDSL2 Router** is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.	**Lietuviškai**	Šiuo **PLANET Technology Corporation,**, skelbia, kad **802.11n Dual band Wireless VDSL2 Router** tenkina visus svarbiausius 1999/5/EC direktyvos reikalavimus ir kitas svarbias nuostatas.
Česky	Společnost **PLANET Technology Corporation,** tímto prohlašuje, že tato **802.11n Dual band Wireless VDSL2 Router** splňuje základní požadavky a další příslušná ustanovení směrnice 1999/5/EC.	**Magyar**	A gyártó **PLANET Technology Corporation**, kijelenti, hogy ez a **802.11n Dual band Wireless VDSL2 Router** megfelel az 1999/5/EK irányelv alapkövetelményeinek és a kapcsolódó rendelkezéseknek.
Dansk	**PLANET Technology Corporation,** erklærer herved, at følgende udstyr **802.11n Dual band Wireless VDSL2 Router** overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF	**Malti**	Hawnhekk, **PLANET Technology Corporation,** jiddikjara li dan **802.11n Dual band Wireless VDSL2 Router** jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC
Deutsch	Hiermit erklärt **PLANET Technology Corporation,** dass sich dieses Gerät **802.11n Dual band Wireless VDSL2 Router** in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 1999/5/EG befindet". (BMWi)	**Nederlands**	Hierbij verklaart , **PLANET Technology orporation,** dat **802.11n Dual band Wireless VDSL2 Router** in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG
Eesti keeles	Käesolevaga kinnitab **PLANET Technology Corporation,** et see **802.11n Dual band Wireless VDSL2 Router** vastab Euroopa Nõukogu direktiivi 1999/5/EC põhinõuetele ja muudele olulistele tingimustele.	**Polski**	Niniejszym firma **PLANET Technology Corporation,** oświadcza, że **802.11n Dual band Wireless VDSL2 Router** spełnia wszystkie istotne wymogi i klauzule zawarte w dokumencie „Directive 1999/5/EC”.
Ελληνικά	*ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ* , **PLANET Technology Corporation,** *ΔΗΛΩΝΕΙ ΟΤΙ ΑΥΤΟ* **802.11n Dual band Wireless VDSL2 Router***ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ* *ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ*	**Português**	**PLANET Technology Corporation**, declara que este **802.11n Dual band Wireless VDSL2 Router** está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Español	Por medio de la presente, **PLANET Technology Corporation,** declara que **802.11n Dual band Wireless VDSL2 Router** cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE	**Slovensky**	Výrobca **PLANET Technology Corporation,** týmto deklaruje, že táto **802.11n Dual band Wireless VDSL 2 Router** je v súlade so základnými požiadavkami a ďalšími relevantnými predpismi smernice 1999/5/EC.
Français	Par la présente, **PLANET Technology Corporation,** déclare que les appareils du **802.11n Dual band Wireless VDSL2 Router** sont conformes aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE	**Slovensko**	**PLANET Technology Corporation**, **s tem potrjuje,** da je ta **802.11n Dual band Wireless VDSL2 Router** skladen/a z osnovnimi zahtevami in ustreznimi določili Direktive 1999/5/EC.
Italiano	Con la presente , **PLANET Technology Corporation,** dichiara che questo **802.11n Dual band Wireless VDSL2 Router** è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.	**Suomi**	**PLANET Technology Corporation,** vakuuttaa täten että **802.11n Dual band Wireless VDSL2 Router** tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Latviski	Ar šo **PLANET Technology Corporation,** apliecina, ka šī **802.11n Dual band Wireless VDSL2 Router** atbilst Direktīvas 1999/5/EK pamatprasībām un citiem atbilstošiem noteikumiem.	**Svenska**	Härmed intygar, **PLANET Technology Corporation,** att denna **802.11n Dual band Wireless VDSL2 Router** står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.