PLANET
Networking & Communication

User's Manual

802.11n Wireless VDSL2 Bridge Router

► VDR-301N

www.PLANET.com.tw

Copyright

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, for 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/remarks
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 of 802.11n Wireless VDSL2 Bridge Router

Model: VDR-301N

Rev: 1.0 (March, 2017)

Part No. EM-VDR-301N (**2080-AC0390-000**)

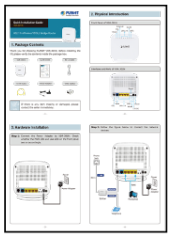
Table of Contents

Chapter 1 Product Introduction

1.1 Package Contents

Thank you for choosing PLANET VDR-301N. Before installing the router, please verify the contents inside the package box.

VDR-301N



Quick Guide

Power Adapter

RJ45 Cable

RJ11 Cable

VDSL Splitter

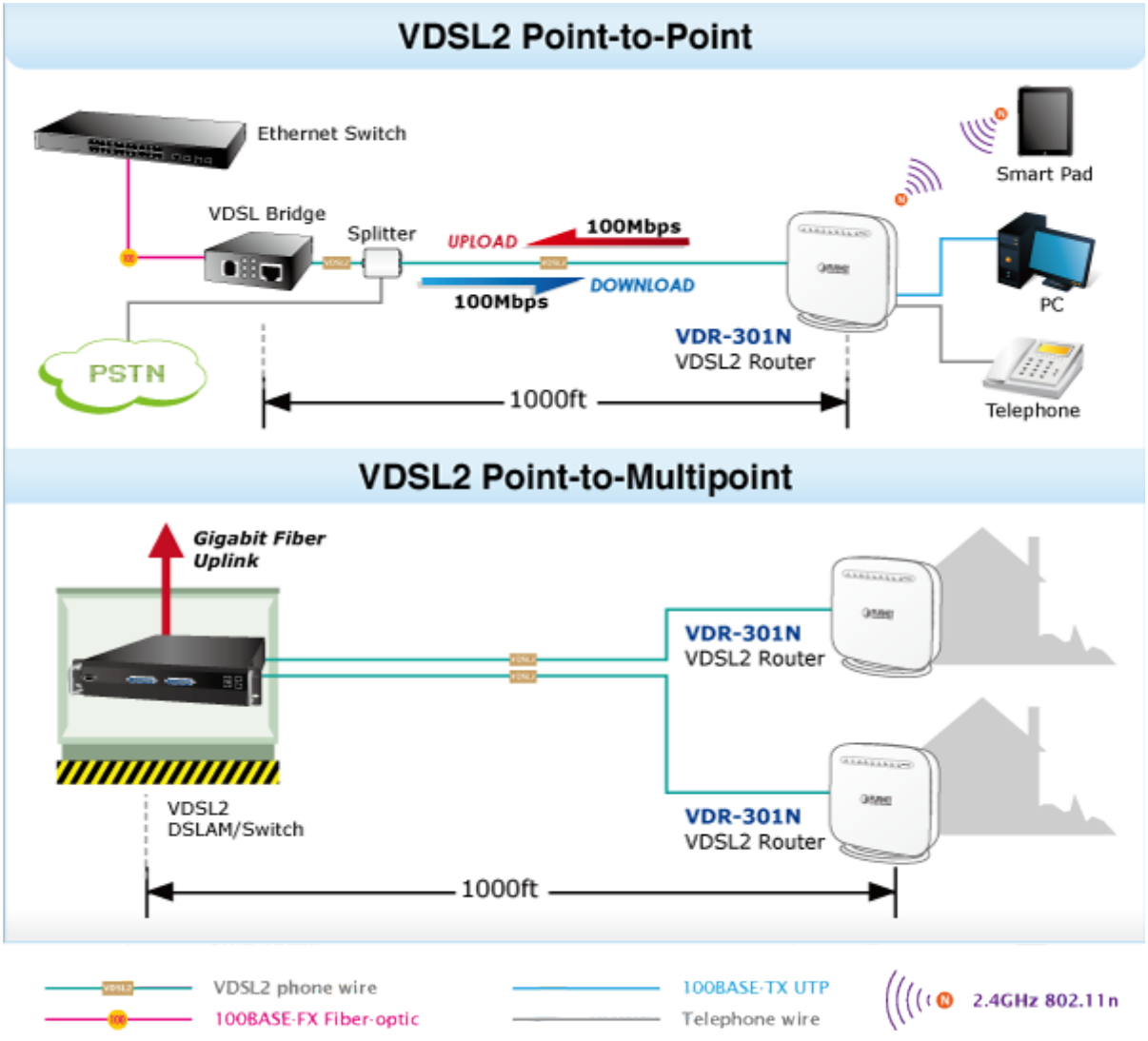
Note

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

1.2 Product Description

High-performance Ethernet over VDSL2

Via the latest VDSL2 technology with **30a profile** supported, PLANET VDR-301N 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 the existing copper telephone lines without the need for rewiring. With integrated support for the ITU-T's new **G.993.5 Vectoring** technology, the VDR-301N works in conjunction with vectoring-enabled DSLAMs to remove crosstalk interference and improve maximum line bandwidth across the existing copper infrastructure.



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

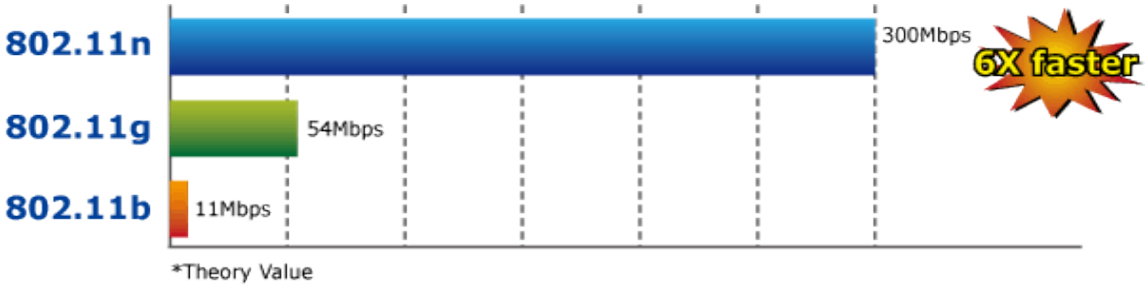
The VDR-301N provides excellent bandwidth to meet the demand of the triple play devices for home entertainment and communication. With the capability of 100/100Mbps symmetric data transmission, the VDR-301N enables many multi-media services to work on local Internet, such as **VOD (Video on Demand)**, Voice over IP, **Video phone**, **IPTV**, Internet caching server, **distance education**, and so on.

ADSL2+ Fallback

For those ISPs that still provide ADSL broadband service, the VDR-301N can support transmission rates up to 24Mbps downstream and 3.5Mbps upstream with ADSL2+ technology. The VDR-301N supports PPPoA (RFC 2364 - PPP over ATM Adaptation Layer 5), RFC 2684 encapsulation over ATM (bridged or routed), PPP over Ethernet (RFC 2516), and IP over ATM (IPoA, RFC 1483) to establish a connection with ISP and it can be also directly switched over to VDSL2 after the ISP network upgrade.

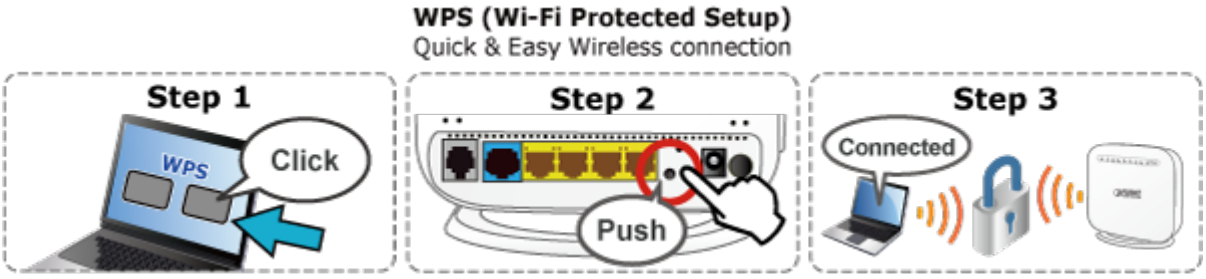
High-speed 802.11n Wireless Connectivity

The VDR-301N applies 2T2R MIMO antenna technology and provides two modes for network applications -- **Router** and **Bridge**. With built-in 2.4GHz IEEE 802.11b/g/n wireless network capability, the VDR-301N allows any computer and wireless-enabled network device to connect to it without additional cabling. 802.11n wireless capability brings users the data transmission rate as high as **300Mbps.** The radio coverage is also doubled to offer high-speed wireless connection even in spacious offices or houses.



Secure Wireless Access Control

To secure wireless communication, the VDR-301N supports most up-to-date encryptions including WEP, WPA-PSK and WPA2-PSK. Moreover, the VDR-301N supports WPS configuration with PBC/PIN type for users to easily connect to a secure wireless network.

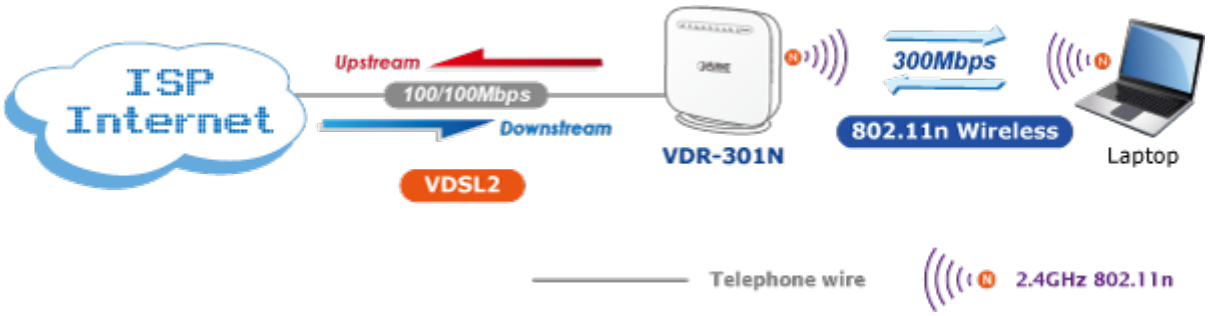


Superior Management Functions

The VDR-301N provides user-friendly management interface that can be managed easily through standard web browsers. For networking management features, the VDR-301N not only provides basic router functions such as DHCP server, virtual server, DMZ, QoS, and UPnP, but also full firewall functions including Network Address Translation (NAT), IP/Port/MAC Filtering and Content Filtering. Furthermore, the VDR-301N serves as an Internet firewall to protect your network from being accessed by unauthorized users.

Multiple Functions for Broadband Communications

The VDR-301N integrates **VDSL2**, **ADSL2+** and **wireless LAN** services into one unit. It is designed to provide a simple and cost-effective xDSL Internet connection for a private Ethernet and 802.11b/g/n wireless network. The Router combines high-speed xDSL Internet connection and 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, SOHOs and small enterprises.



IPv6/IPv4 Dual Stack Capability

With fully supporting both IPv4 and IPv6 protocols, the VDR-301N can work with original IPv4 network structure and also support the new IPv6 network structure now and in the future. As more network devices are growing and the need for larger addressing and higher security becomes critical, the VDR-301N is the best choice for ISPs to build the IPv6 FTTx edge service and for SMBs to connect with the IPv6 network.

Robust TR-069 Remote Management

To reduce the service provider's manpower needed for on-site maintenance, the VDR-301N supports TR069 (WAN Management Protocol) standard that allows an Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device remotely.

1.3 Product Features

- **Internet Access Features**
  - **Shared Internet Access:** All users on the LAN can access the Internet through the VDR-301N 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-301N provides VDSL2 modem and supports all common VDSL2 connections.
  - **G. Vectoring**: G.993.5 (G. Vector) support for significant reduction of crosstalk levels and improvement of VDSL2 line performance
  - **Multiple WAN Connections:** Upon the Internet (WAN port) connection, the VDR-301N supports ADSL2+ and VDSL2.

- **Advanced Internet Functions**
  - **Virtual Servers:** This feature allows Internet users to access Internet servers on your LAN. The setup is also quick and easy.
  - **Firewall:** The VDR-301N 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 XP, 7 or later.
  - **DMZ Support:** The VDR-301N 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 flexible way to run programs smoothly for programs that might be restricted in NAT environment.
  - **RIPv1/v2 Routing:** It supports RIPv1/v2 routing protocol for routing capability.

- **LAN Features**
  - **4-port Switch:** The VDR-301N 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-301N can act as a DHCP Server for devices on your local LAN.

- **Wireless Features**
  - **IEEE 802.11b/g/n Wireless Stations:** The VDR-301N supports 802.11n standard which 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 having a data rate of up to 300Mbps.
  - **WPS Push Button Control:** The VDR-301N supports WPS (Wi-Fi Protected Setup) for users to easily connect to wireless network without configuring the security.
  - **Advanced Security:** Supports 64/128-bit WEP, WPA / WPA2 and WPA-PSK / WPA2-PSK (TKIP/AES encryption), and 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.

- **Multiple SSIDs:** It allows users to access different networks through a single AP.

➢ **Management Features**

- **TR069 compliant:** Support for centralized management node of multiple VDSL2 CPEs

1.4 Product Specifications

Model		**VDR-301N**
Product Description		**300Mbps Wireless VDSL2 Bridge Router**
Hardware Specifications		
Interfaces	**LAN**	4 x 10/100BASE-TX, auto-negotiation, auto MDI/MDI-X RJ45 port
	WAN	1 x RJ11, 1 x 1000BASE-T RJ45
Antenna		2.4GHz: 2 x 4dBi internal antennas
Button		1 x Power button 1 x Reset button 1 x WPS button 1 x WLAN button
LED Indicators		PWR, DSL, LAN1-4, WLAN, WPS
Dimensions (W x D x H)		155 x 60 x 152 mm
Weight		238g
Power		12V DC, 0.5A
Power Consumption		6W
Software Features		
Internet Connection Type		● Bridge ● PPPoE ● Dynamic IP ● Static IP
VDSL Features		● ITU-T G.993.2 VDSL2 ● Supports 8a,8b,12a,12b,17a,30a profile ● Supports G. vectoring ● Supports ATM and PTM ● Supports Annex A, B

ADSL Features	● Full-rate ANSI T1.413 Issue 2 ● ITU-T G.992.1(G.DMT) ● ITU-T G.994.1 (G.hs) ● ITU-T G.995.1 ● ITU-T G.992.3 (G.dmt.bis) ● ITU-T G.992.5
Protocol Features	● ATM Adaptation Layer Type 5 (AAL5) ● Multiple Protocol over AAL5 (RFC 2684, formerly RFC 148) ● ATM Forum UNI3.1/4.0 ● PPP over ATM (RFC 2364) ● PPP over Ethernet (RFC 2516) ● IPoA (RFC 1577/2225) ● Bridged or routed Ethernet encapsulation ● VC and LLC based multiplexing ● OAM F4/F5 ● ATM QoS: UBR, CBR, VBR-rt, VBR-nrt ● Dynamic and static IP ● IP unnumbered
Advanced Features	● Parent Control ● Traffic Shaping(ATM QoS) UBR, CBR, VBR-rt, VBR-nrt ● Dynamic Host Configuration Protocol (DHCP), DHCP relay ● Network Address Translation (NAT) ● PVC/Ethernet Port Grouping ● Static Routing, RIP v1/v2 (optional) ● DNS relay, DDNS ● G. vectoring ● IGMP proxy, MLD proxy ● PPTP, L2TP, IPSec VPN passthrough ● Virtual server, port triggering, UPnP, DMZ ● WMM, bandwidth control (IP QoS)
Security	● NAT firewall ● SPI firewall ● MAC / IP / URL filtering
Management	● Device configuration, management and update ● Web-based GUI ● Command line interface via telnet ● SSL for TR069
Wireless Interface Specifications	
Wireless Standard	IEEE 802.11b/g/n
Frequency Band	2.4GHz: 2.412~2.484GHz
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, 6Mbps per channel, auto fallback for extended range
	802.11b: 1, 5.5, 2, 1 Mbps per channel, auto fallback for extended range
Transmit Power	<20dBm(EIRP)
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~ 90% (non-condensing) Storage: -20~70 degrees C, 5~90% (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

VDR-301N Overview

2.1.1 Front Panel of VDR-301N

The front panel provides a simple interface monitoring of the router. Figure 2-1 shows the front panel of the VDR-301N.

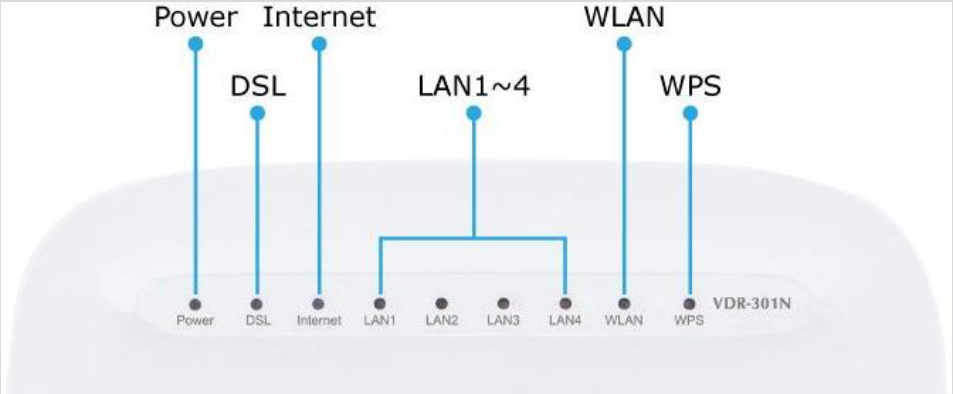


Figure 0-1 VDR-301N Front Panel

2.1.2 LED Indications of VDR-301N

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-301N.

Front Panel LED Definition

LED	Color	State	Description
Power	Green	ON	When the router is powered on, and in ready state.
		OFF	The device is powered off.
DSL	Green	ON	The WAN is connected successfully.
		Flashing	Router is trying to establish a WAN 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.
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.

Table 2-1 The LED Indication of VDR-301N

2.1.3 Rear Panel of VDR-301N

The rear panel provides the physical connectors connected to the power adapter and any other network device. Figure 2-2 shows the rear panel of the VDR-301N.

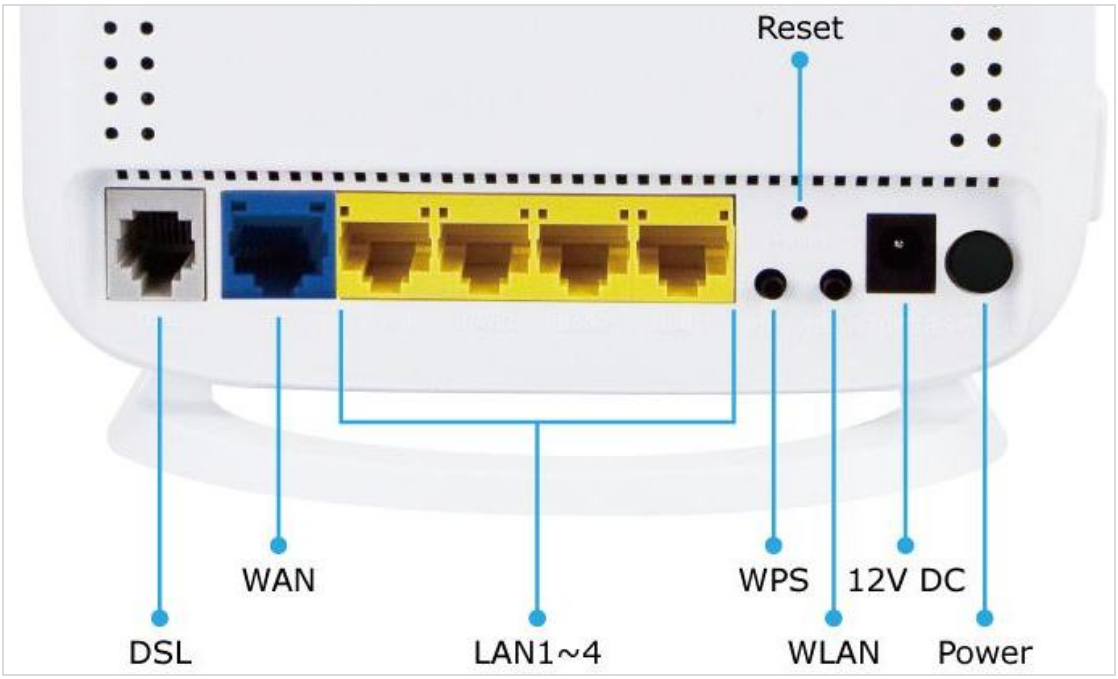


Figure 0-2 VDR-301N Rear Panel

Rear Panel Port and Button Definition

Connector	Description
POWER	Power on/off button
12V DC	Power connector with 12V DC, 0.5 A
WLAN	WLAN switch -- Press for over 3 seconds to enable or disable the WLAN function.
WPS	This button is used for enabling WPS PBC mode. If WPS is enabled, press this button for over 3 seconds and then the router starts to accept the negotiation in the PBC mode.
RESET	Press for more than 3 seconds to reset 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 is flashing, the router is actively sending or receiving data over that port.
WAN	The RJ45 WAN port allows data communication between the router and the network through a UTP cable
DSL	The RJ11 connector allows data communication between the router and the DSL network through a twisted-pair phone wire

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 RJ45 connector (not necessary if the Router is connected directly to the Ethernet.)
- PCs with a working Ethernet Adapter and an Ethernet cable with RJ45 connectors
- PC of subscribers running Windows XP, Windows Vista/Win 7, MAC OS 9 or later, Linux, UNIX or other platform compatible with **TCP/IP** protocols
- The above PC is installed with Web browser

Note

1. The Router in the following instructions is named as PLANET VDR-301N.
2. It is recommended to use Internet Explore 8.0 or above to access the Router.

3.2 Installing the Router

Please connect the device to you computer as follows:

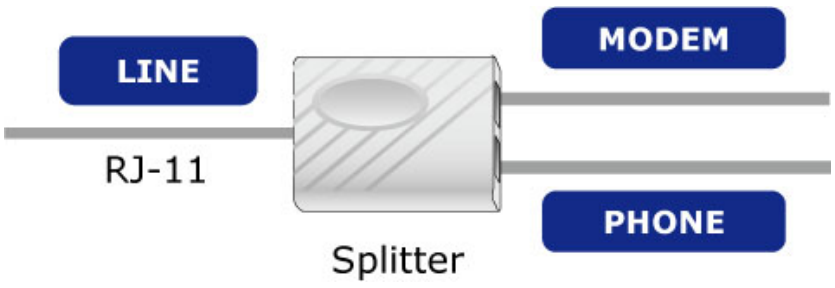
STEP 1. Connect the DSL port of the router and the Modem port of the splitter with a telephone cable; connect the phone to the phone port of the splitter through a cable and connect the incoming line to the Line port of the splitter.

The spliiter has three ports:

Line: Connect to a wall phone jack (RJ11 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-301N. Check whether the **Power LED** on the front panel is on accordingly. Figure3-1 shows the power adapter connection diagram.

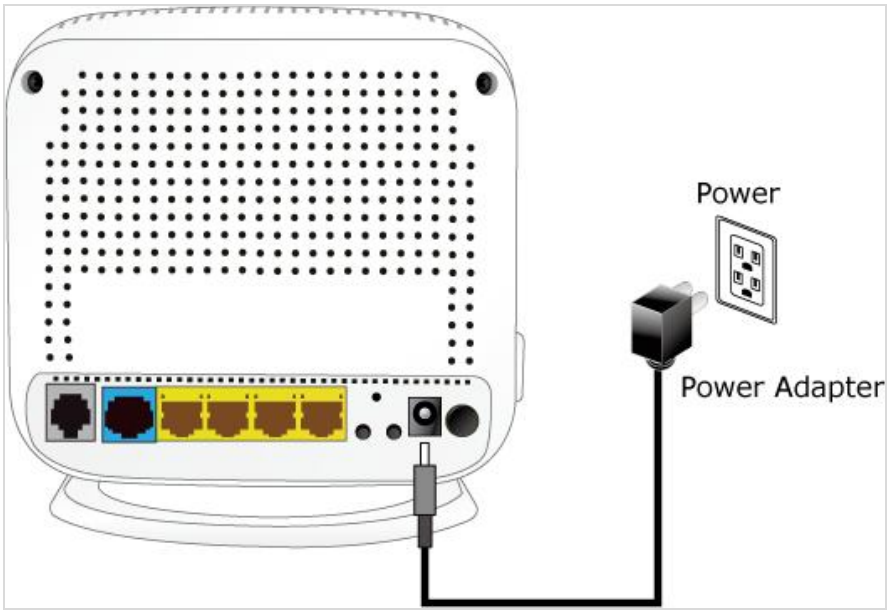


Figure 3-1 VDR-301N Power Adapter Connection Diagram

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.

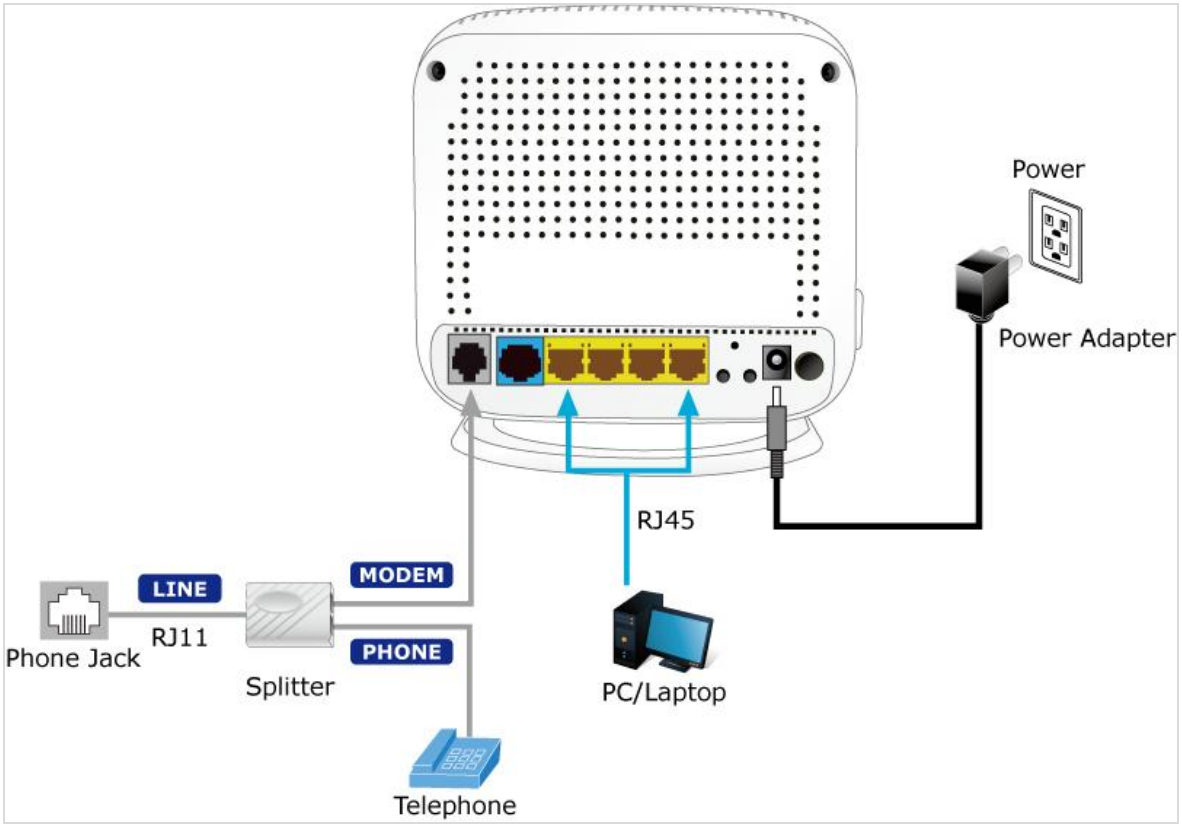


Figure 3-2 VDR-301N Connection Diagram

Chapter 4 Installation Guide

4.1 Configuring the Network Properties

Configuring PC in Windows 7

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

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

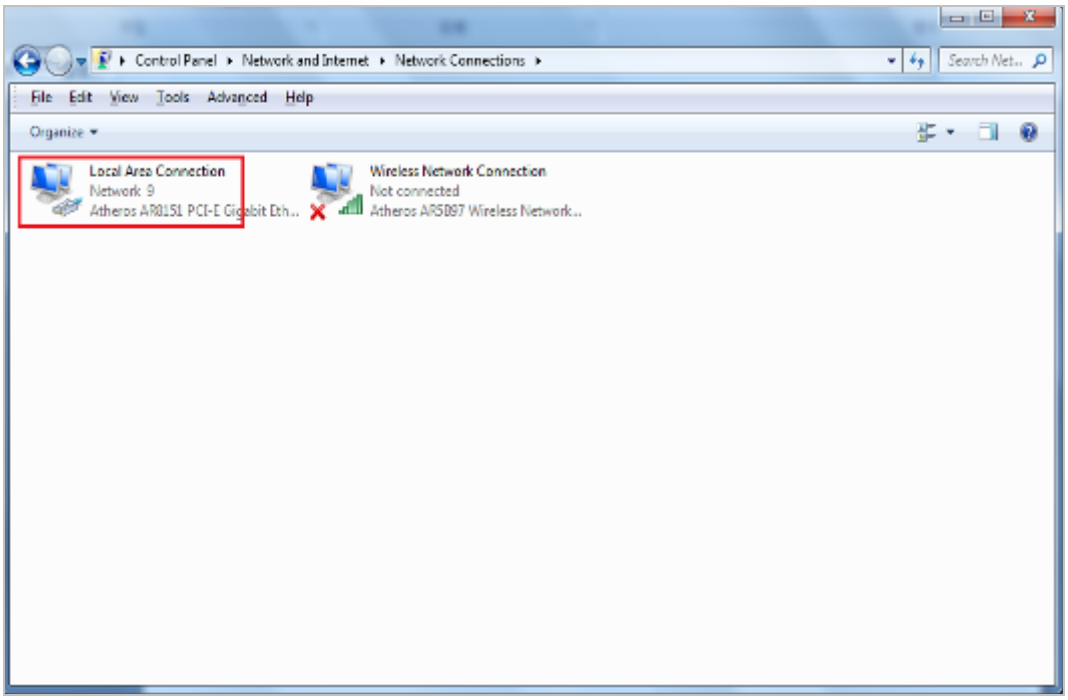


Figure 4-1 Select Local Area Connection

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

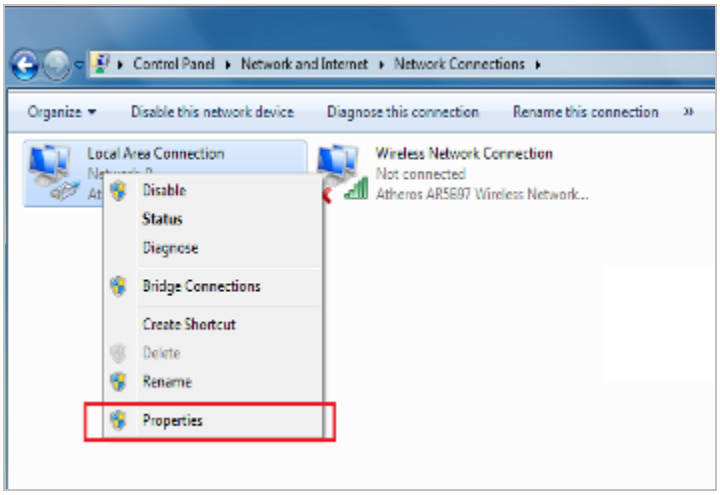


Figure 4-2 Network Connection Properties

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

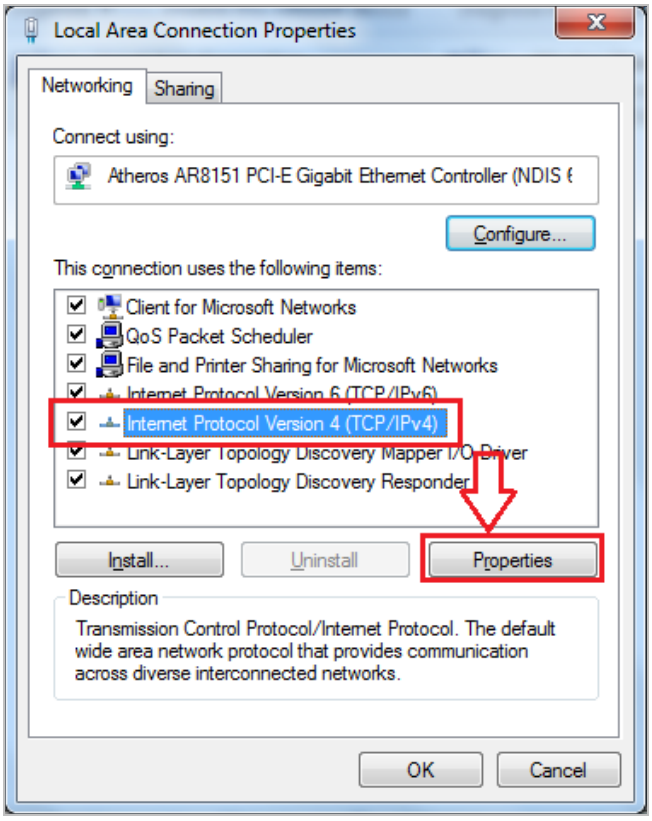


Figure 4-3 TCP/IP Setting

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

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

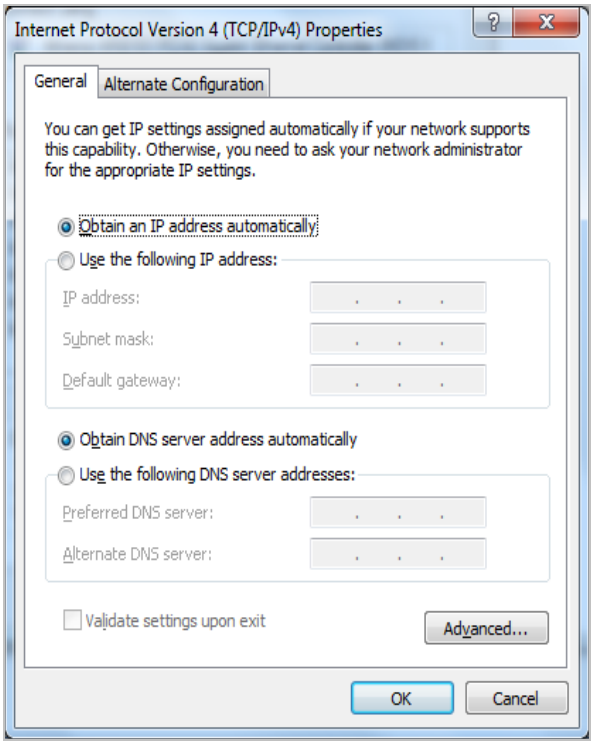


Figure 4-4 Obtain an IP address automatically

Configuring PC in Windows XP

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

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

Figure 4-5 Select Network Connections

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

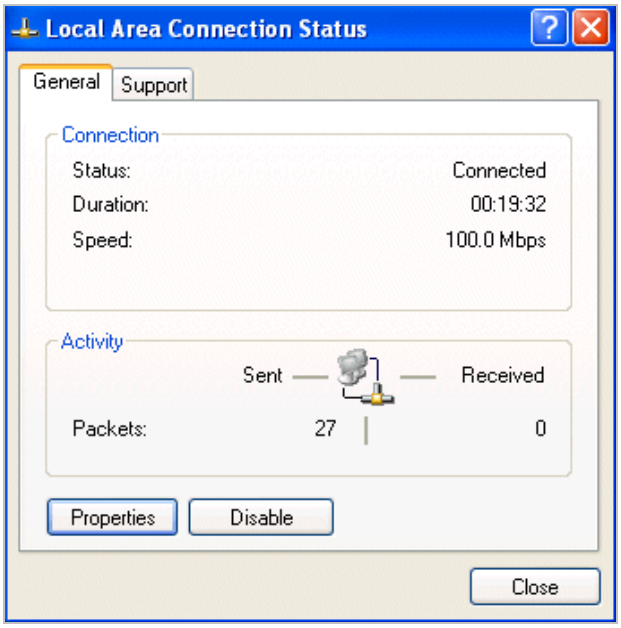


Figure 4-6

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

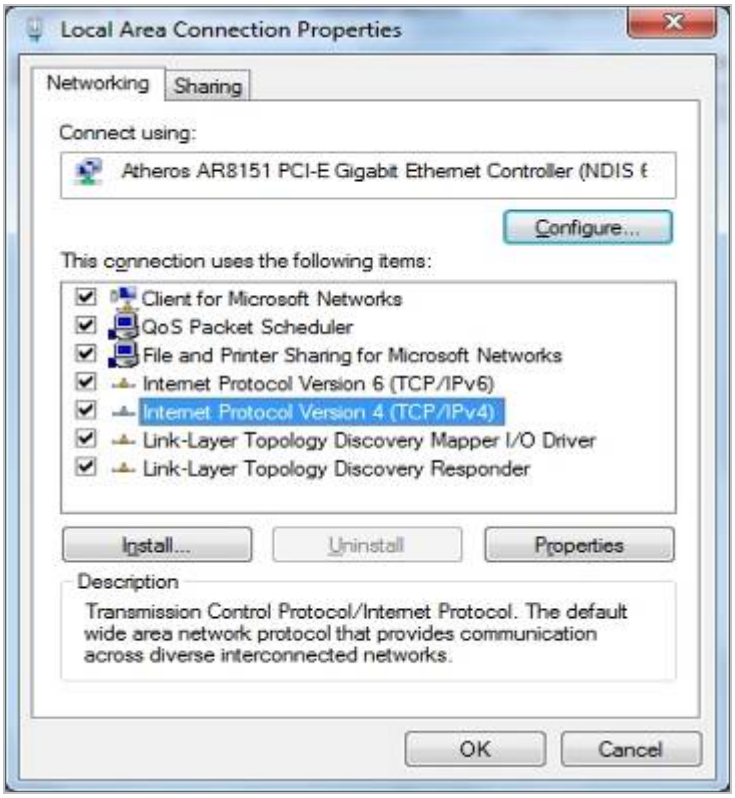


Figure 4-7TCP/IP Setting

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

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

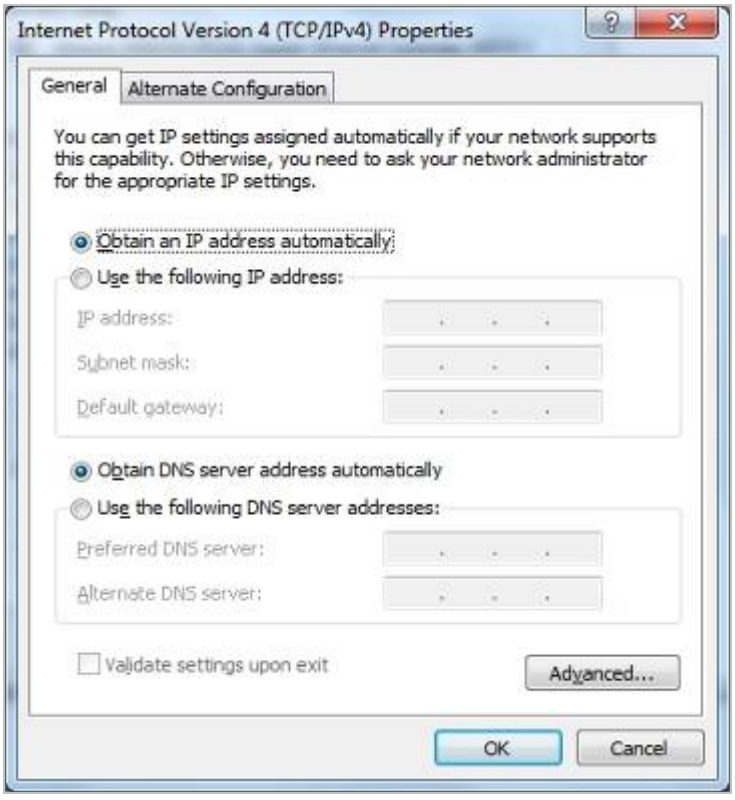


Figure 4-8 Obtain an IP address automatically

4.2 Configuring with Web Browser

It would be better 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.

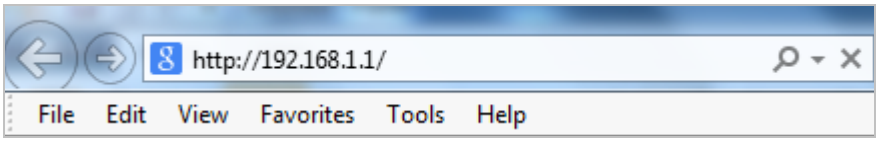


Figure 4-9 Login the Router

At the User Name and Password prompt, type your proper user name and password to login. The default user name and password are both **"admin**. You can change these later if you wish. Click **"OK".**

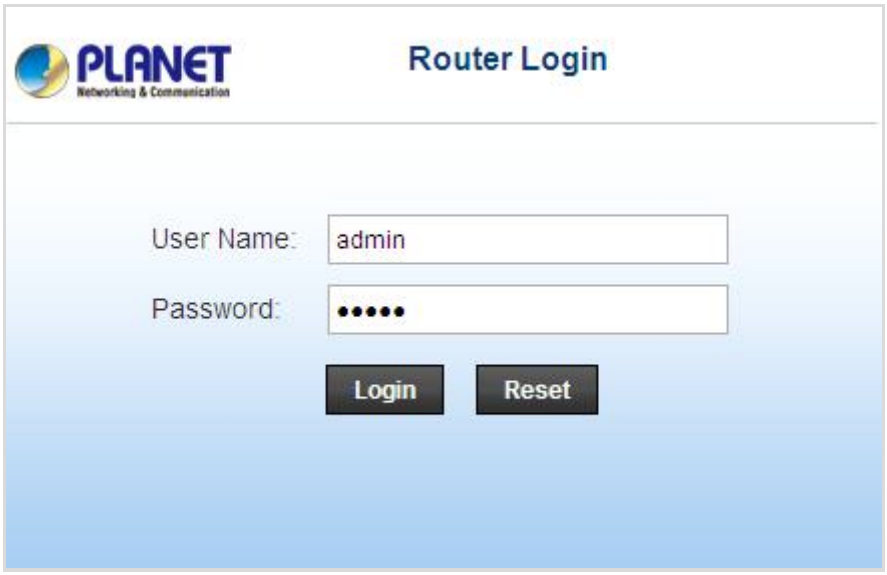


Figure 4-10 Login Window

If the user name and password are correct, you will log in to VDSL2 Router successfully and see the status page. Now you can configure the VDSL2 Router for your needs.

Chapter 5 System Settings

After logging in, the page shown in the following figure appears. You can check, configure and modify all the settings.

Figure 5-1 Status

5.1 Status

In the navigation bar, choose **Status**. On the **Status** page that is displayed contains: **Device Info** and **Statistics**.

5.1.1 Device Information

Choose **Status** > **Device Info** and the page displayed shows the current status and some basic settings of the router, such as software version, DSL status, CWMP status, LAN configuration, DNS status and WAN interfaces.

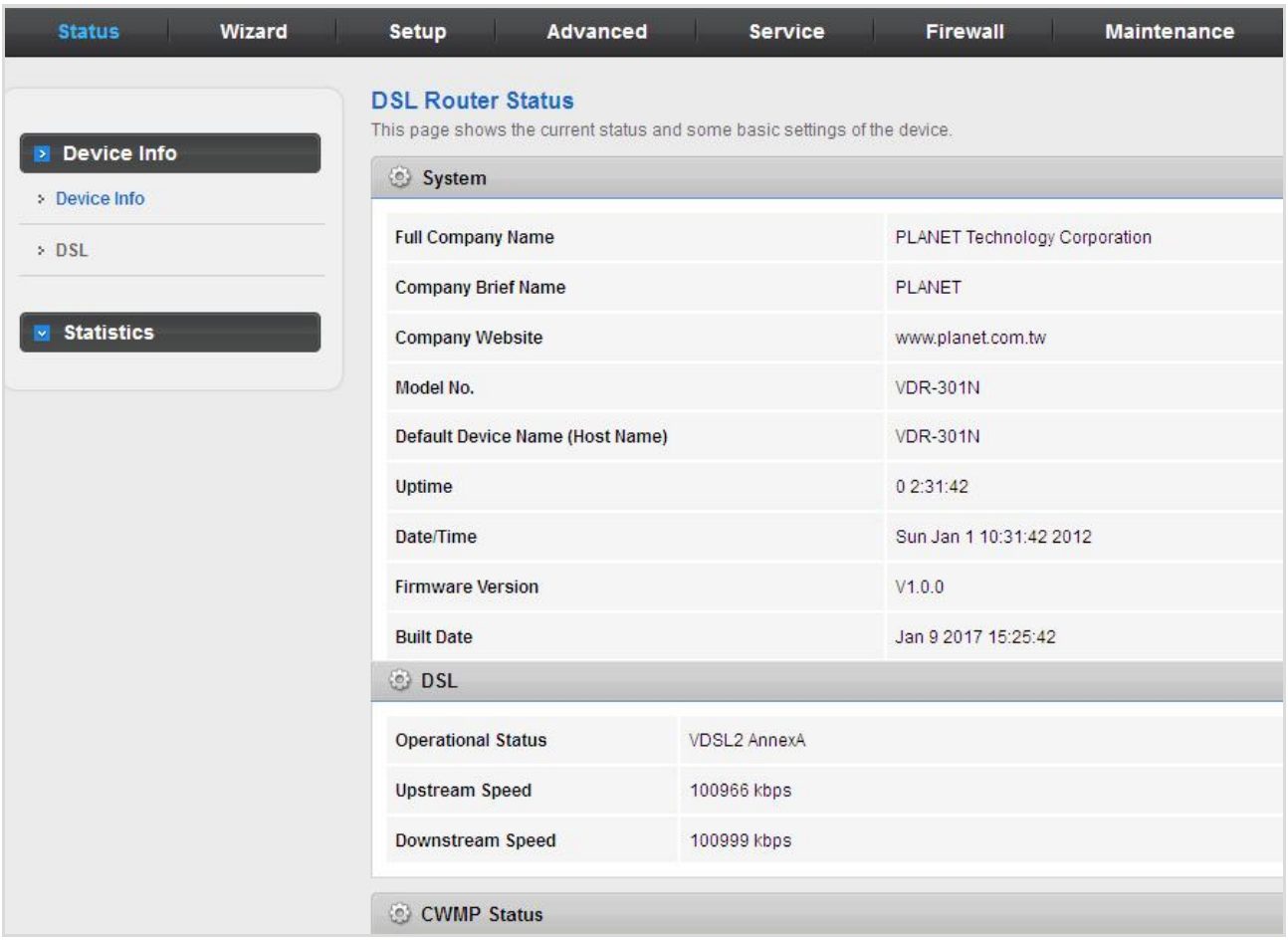


Figure 5-2 Device Info

5.1.2 DSL

Choose **Status** > **DSL** and the page displayed shows the current DSL status.

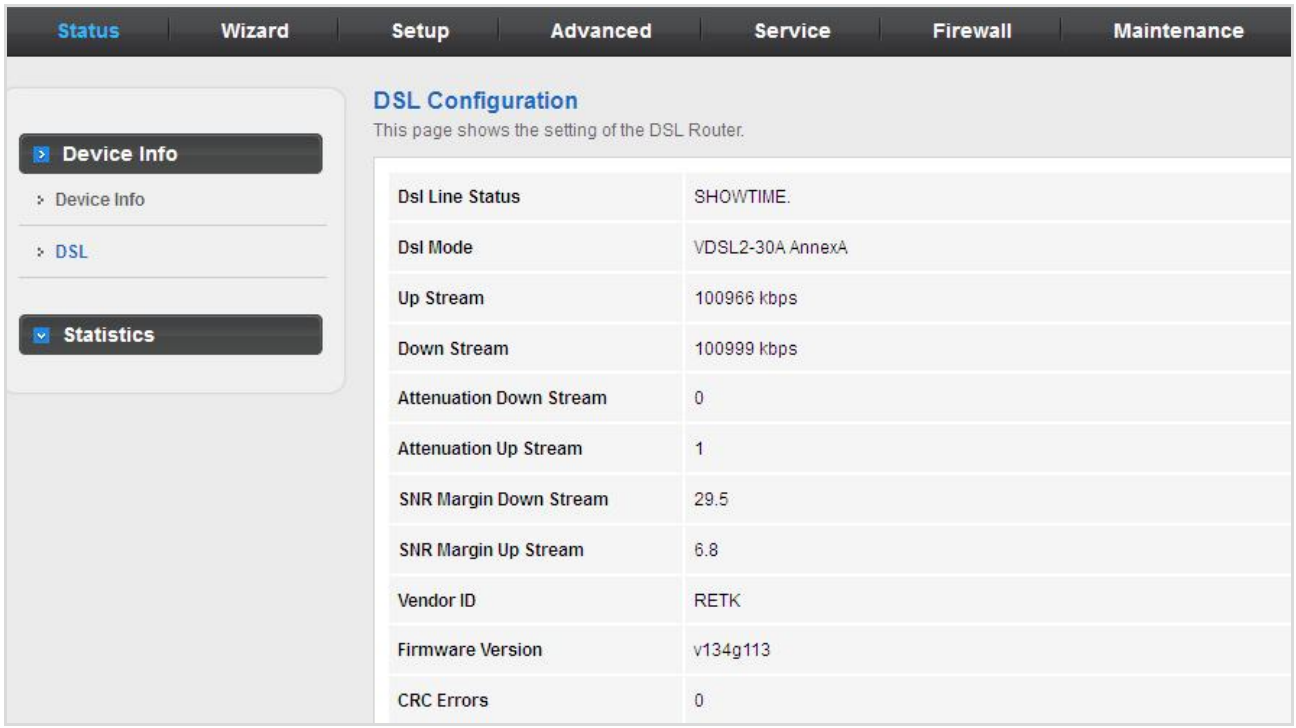


Figure 5-3 DSL Info

5.1.3 Statistics

Choose **Status** > **Statistics.** Click **Statistics** in the left pane and the page shown in the following figure appears. On this page, you can view the statistics of each network port.

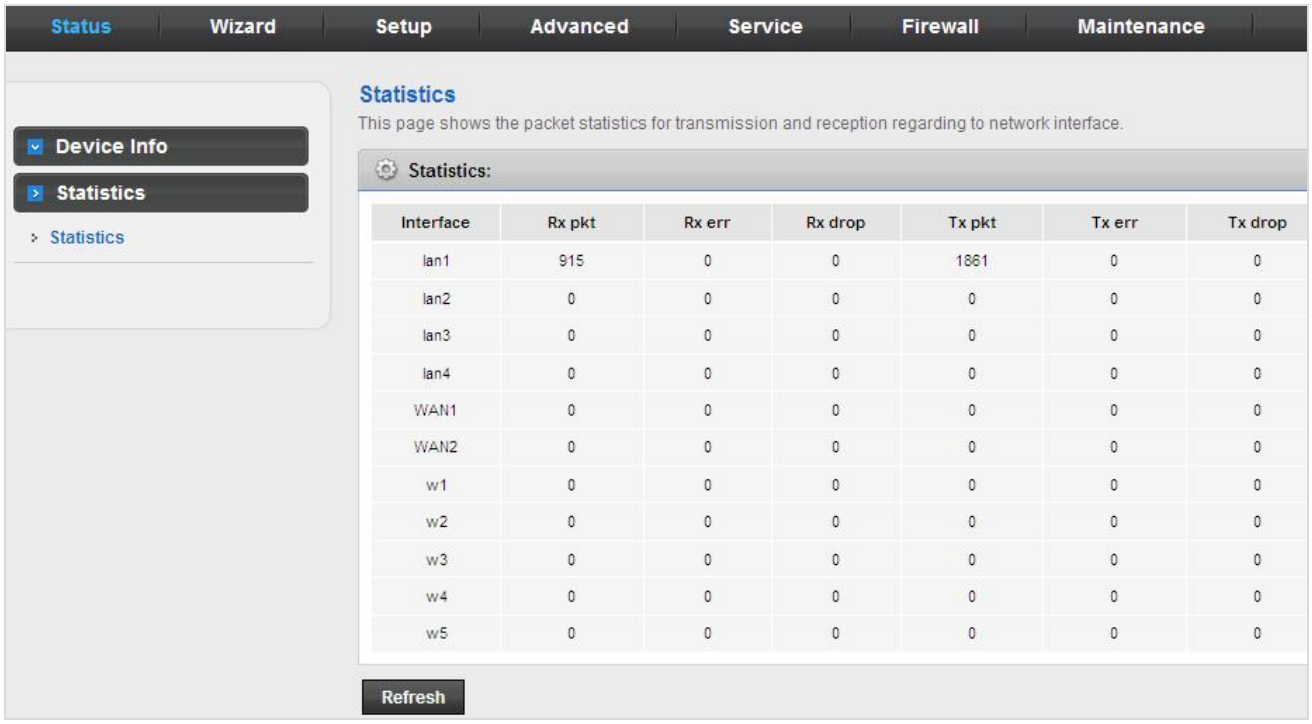


Figure 5-4 Statistics

5.2 Wizard

When subscribing to a broadband service, you should be aware of the method by which you are connected to the Internet. Your physical WAN device can be either Ethernet or RJ11 port. The technical information about the properties of your Internet connection is provided by your Internet Service Provider (ISP). For example, your ISP should inform you whether you are connected to the Internet using a static or dynamic IP address, and the protocol that you use to communicate on the Internet.

In the navigation bar, choose **Wizard**. The page shown in the following figure appears. The **Wizard** page guides fast and accurate configuration of the Internet connection and other important parameters. The following sections describe these various configuration parameters. Whether you configure these parameters or use the default ones, click **NEXT** to enable your Internet connection.

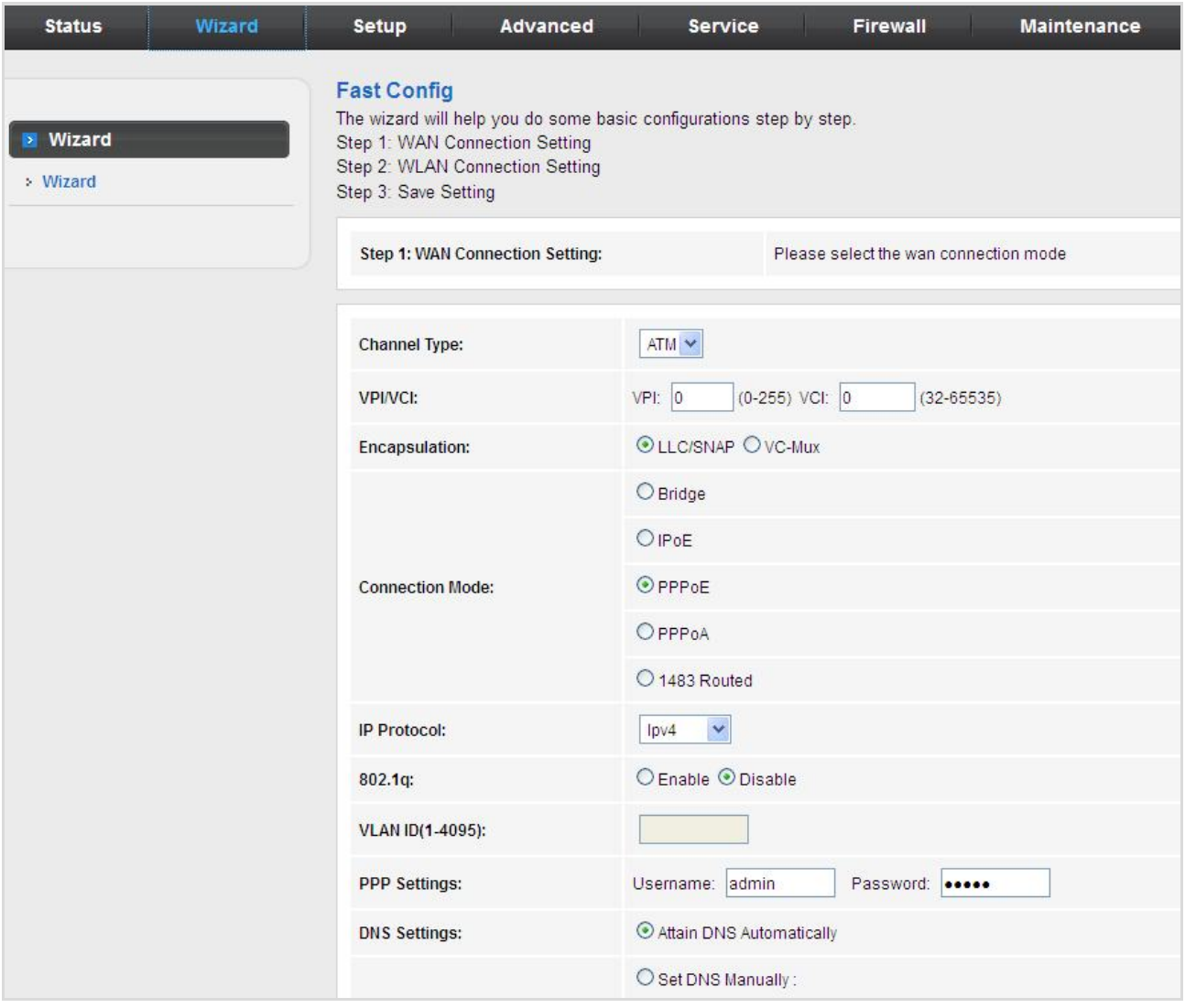


Figure 5-5 Wizard

There are two channel types, **ATM** or **PTM** and five connection modes: **Bridge, IPoE, PPPoE, PPPoA and 1483 Routed**. The following describes them respectively.

5.2.1 Bridge

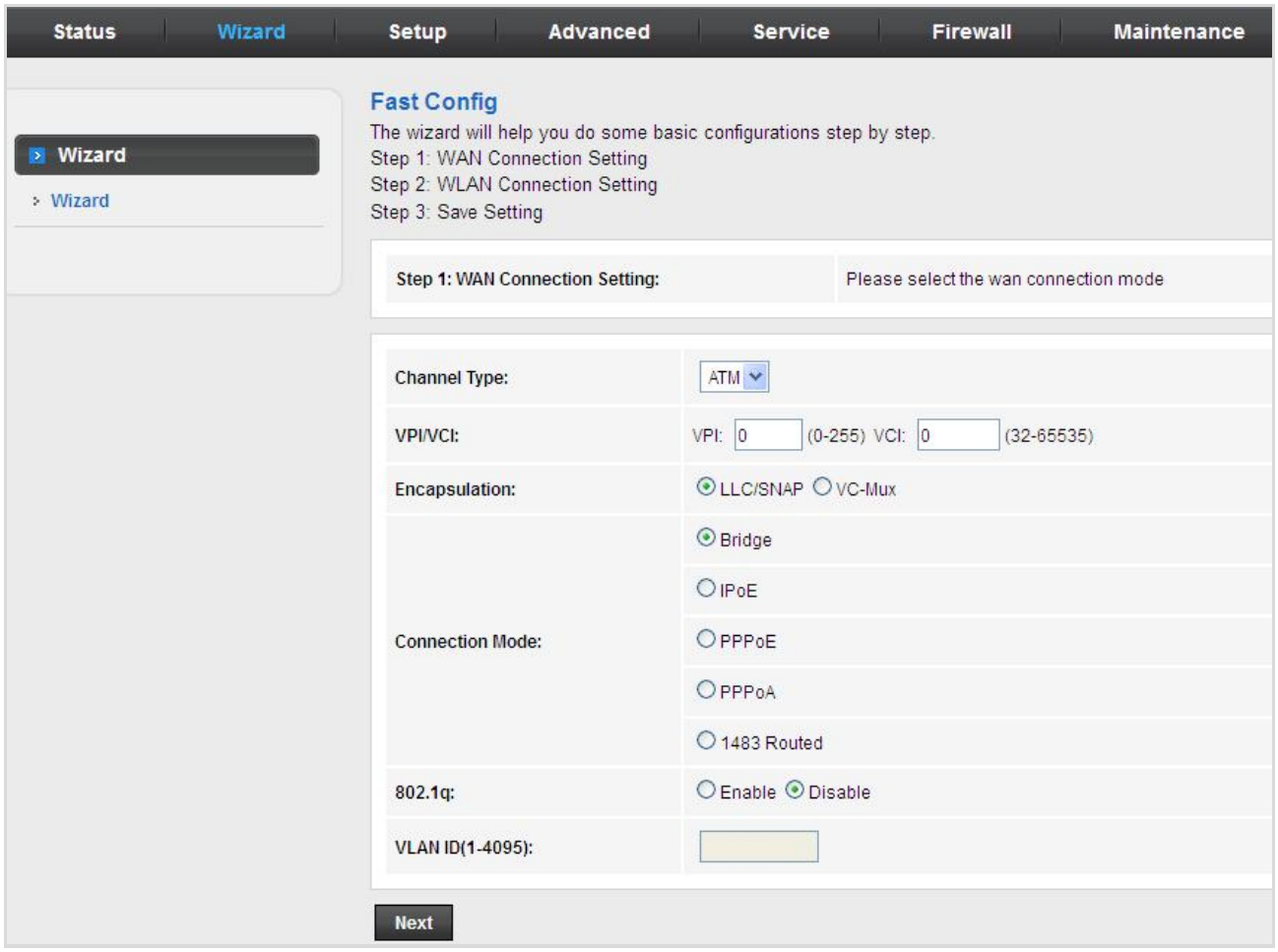


Figure 5-6 Wizard Bridge

After setting, click **Next** and the page as shown in the following figure appears.

Figure 5-7 Wizard Bridge WLAN

And click **Apply changes** to save the configuration.

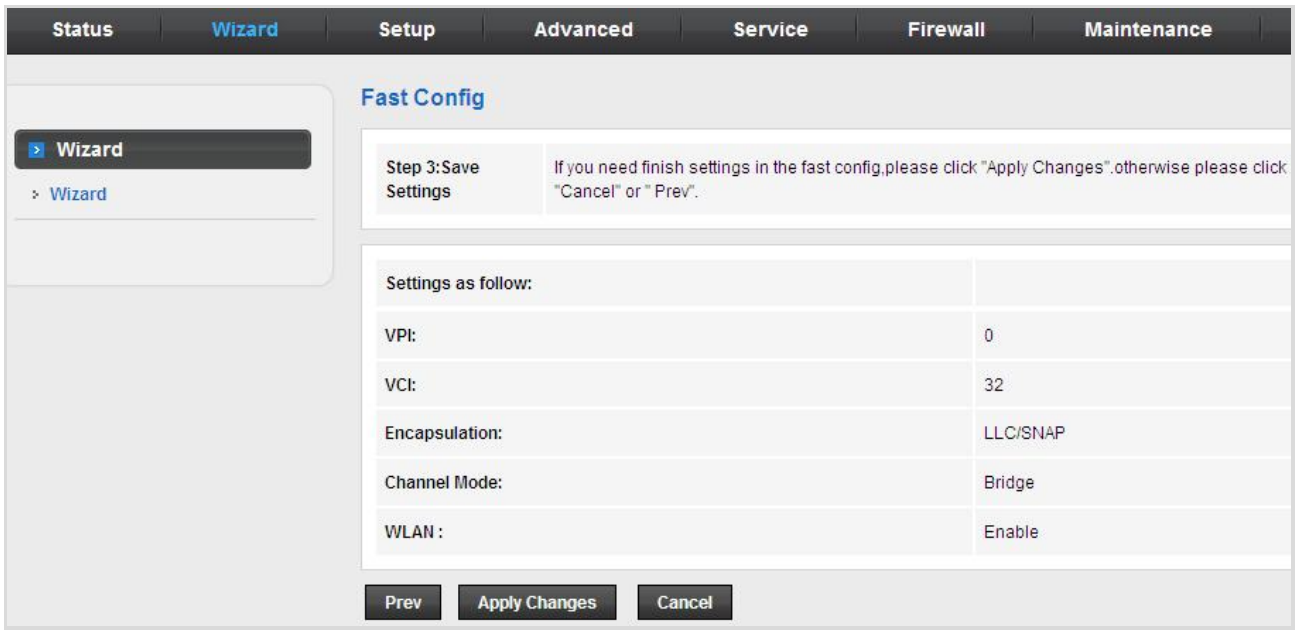


Figure 5-8 Wizard Bridge Saved

5.2.2 IPoE

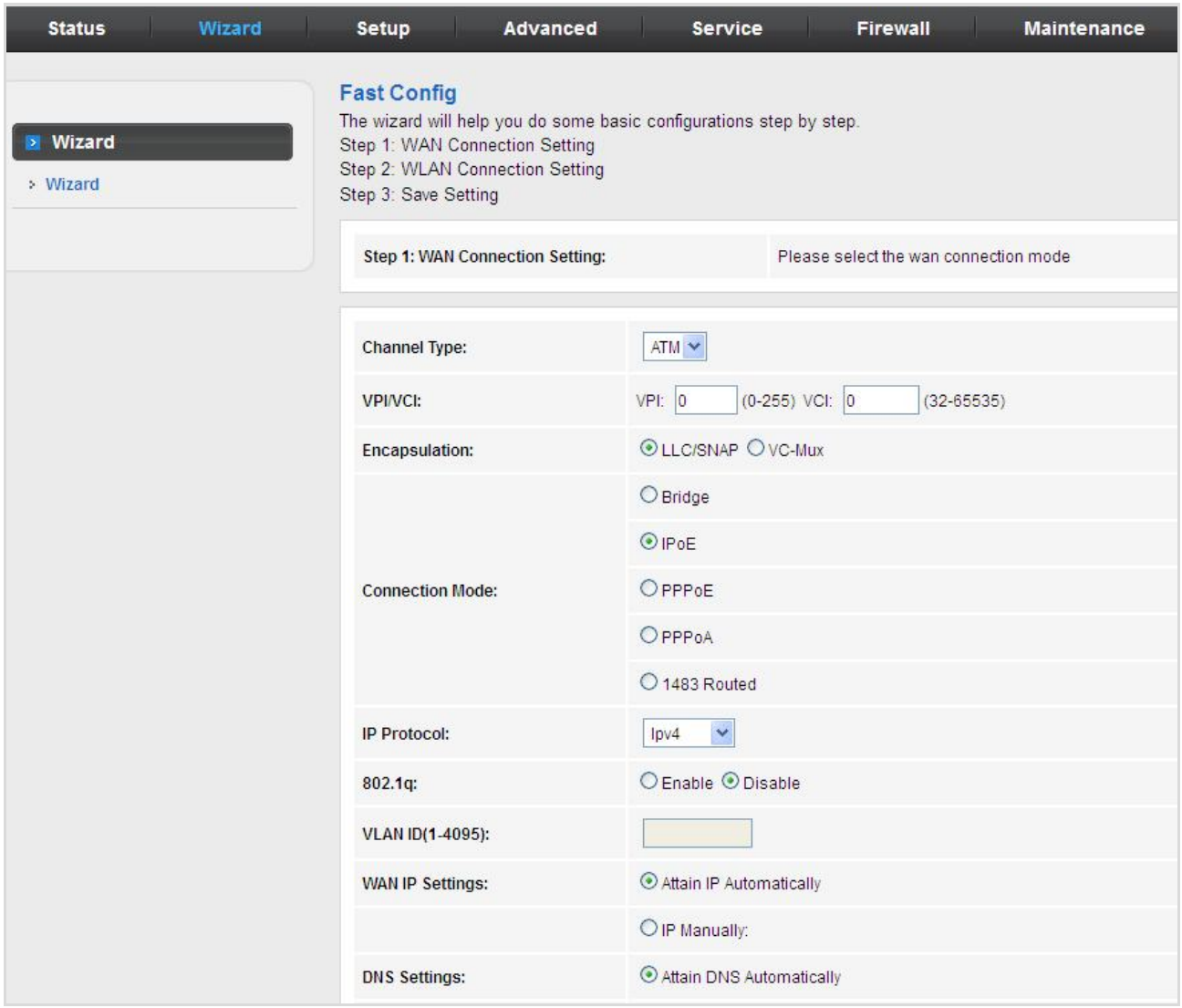


Figure 5-9 Wizard IPoE

Figure 5-10 Wizard IPoE WLAN

And click **Apply changes** to save the configuration.

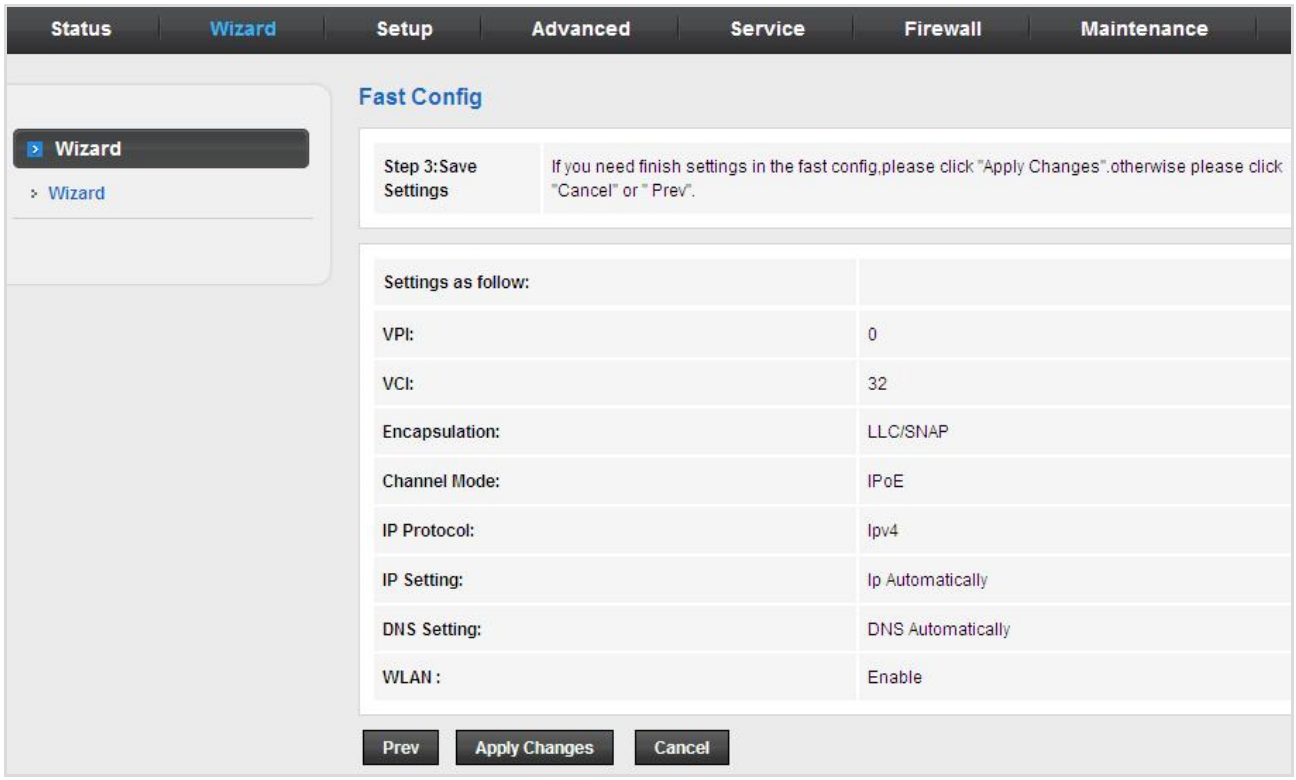


Figure 5-11 Wizard IPoE Saved

5.2.3 PPPoE

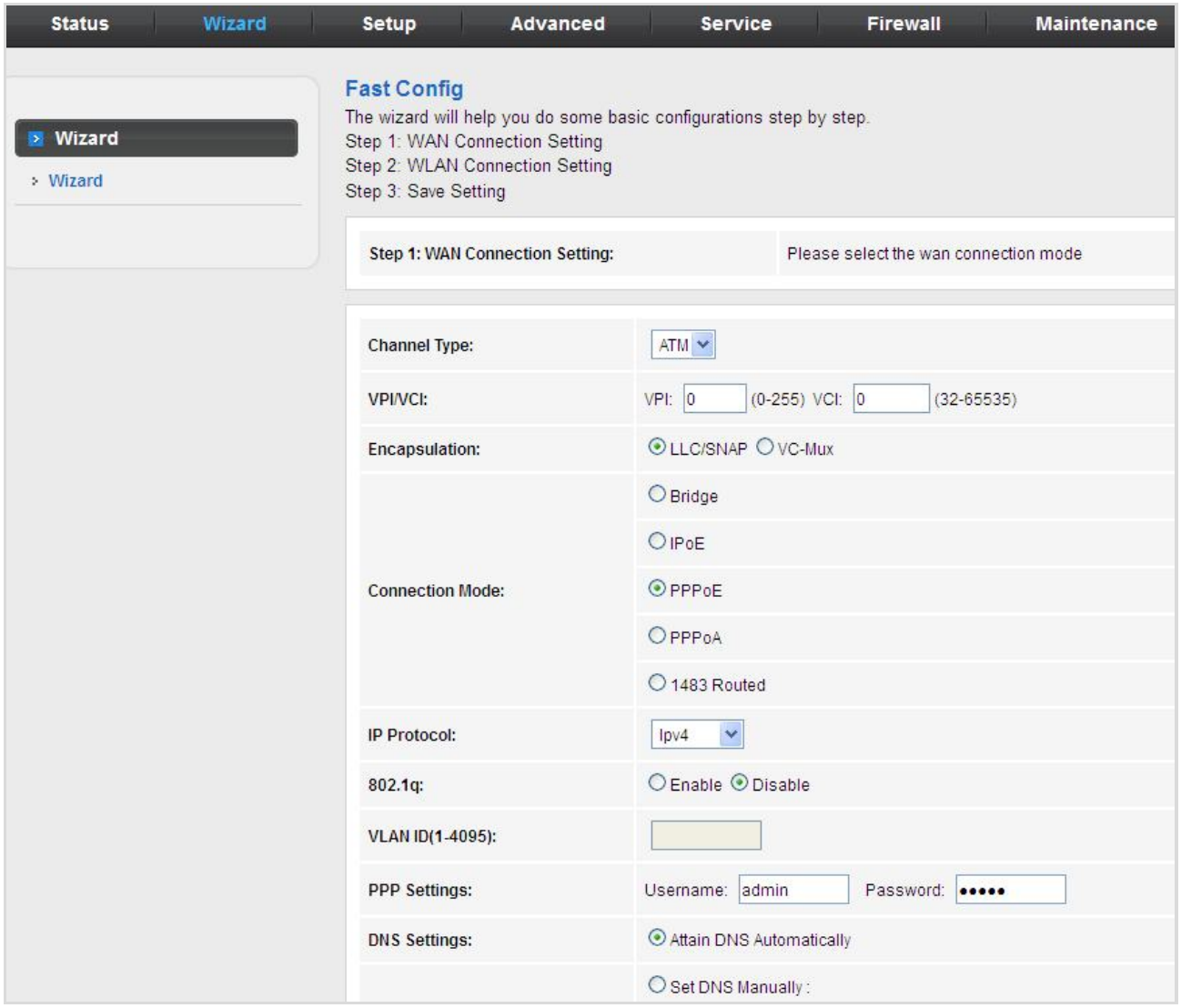


Figure 5-12 Wizard PPPoE

Figure 5-13 Wizard PPPoE WLAN

And click **Apply changes** to save the configuration.

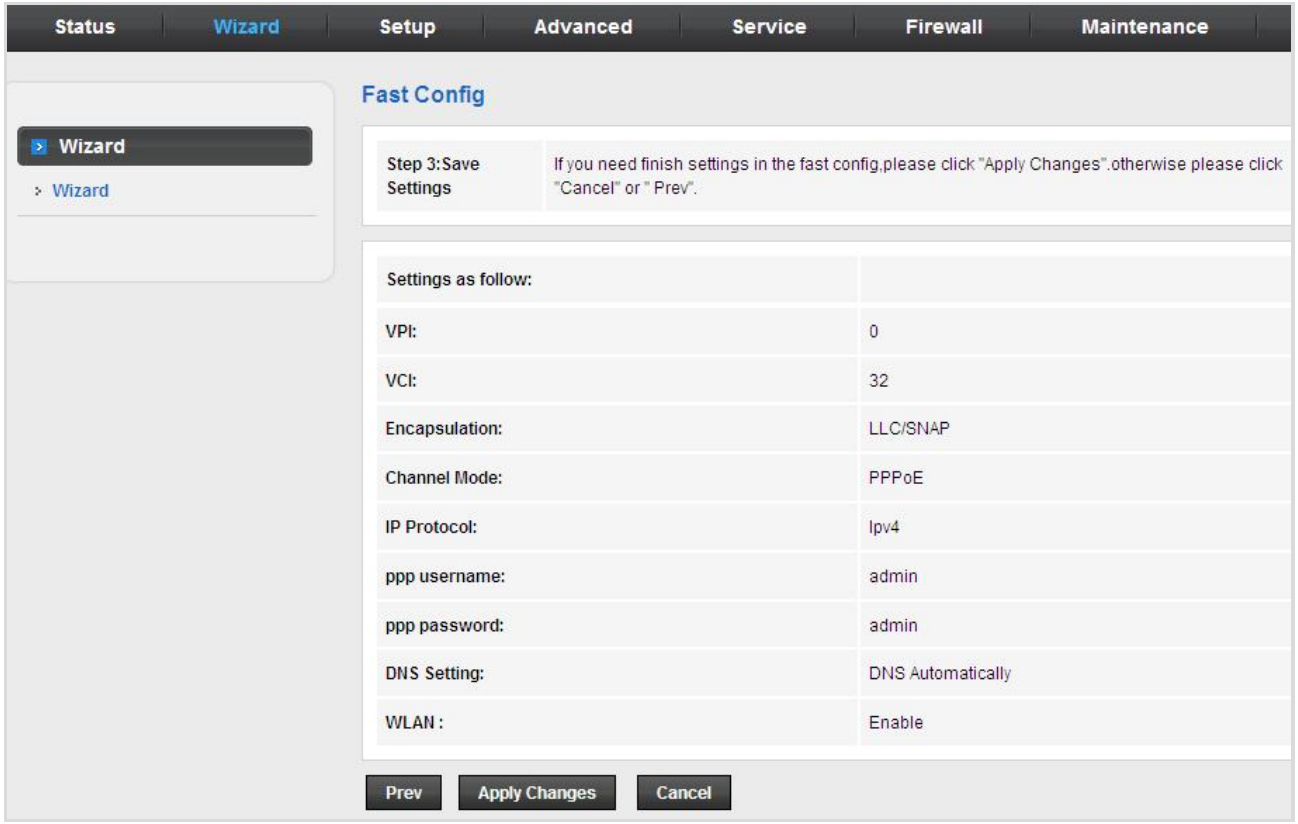


Figure 5-14 Wizard PPPoE Saved

5.2.4 PPPoA

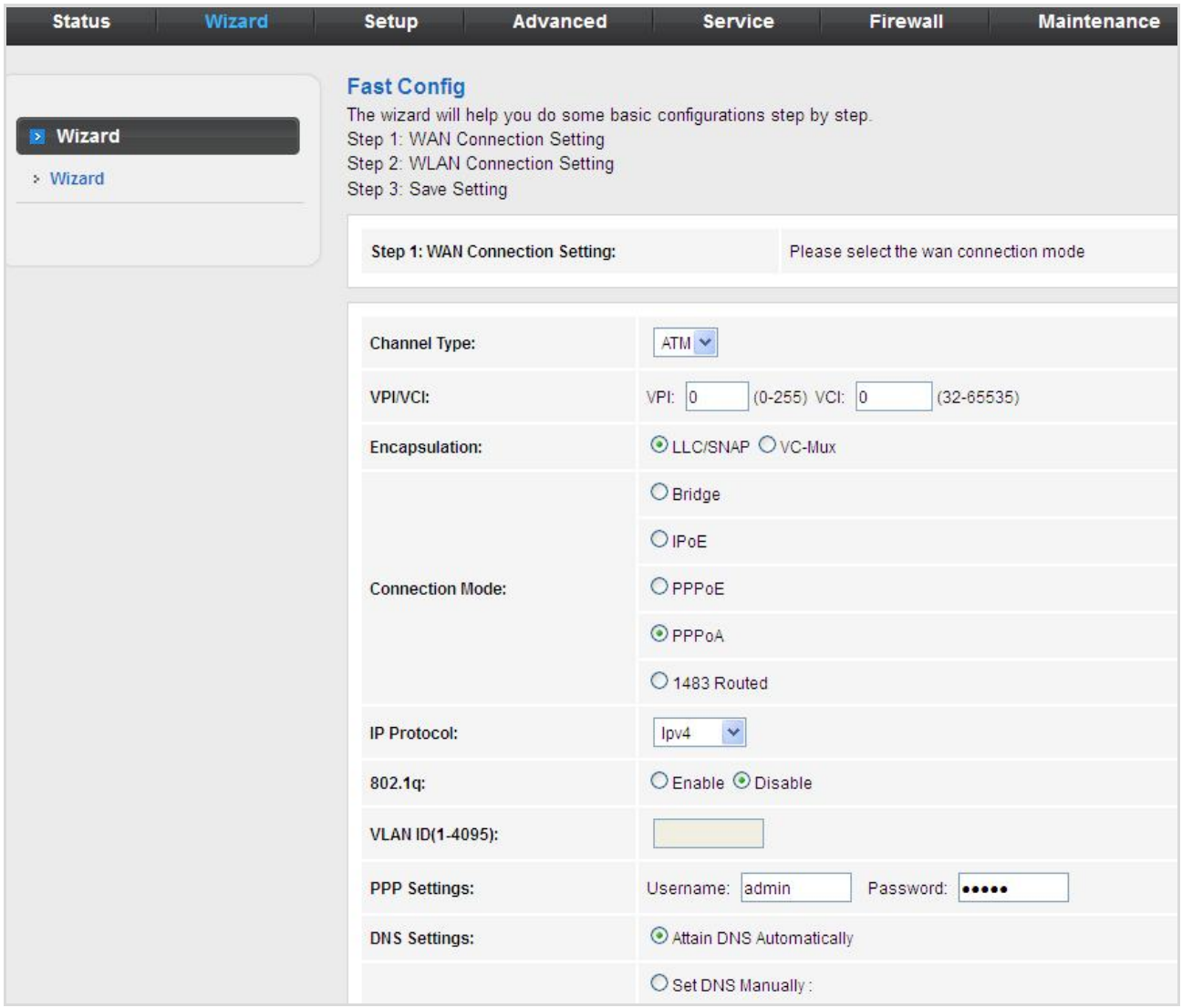


Figure 5-15 Wizard PPPoA

Figure 5-16 Wizard PPPoA WLAN

And click **Apply changes** to save the configuration.

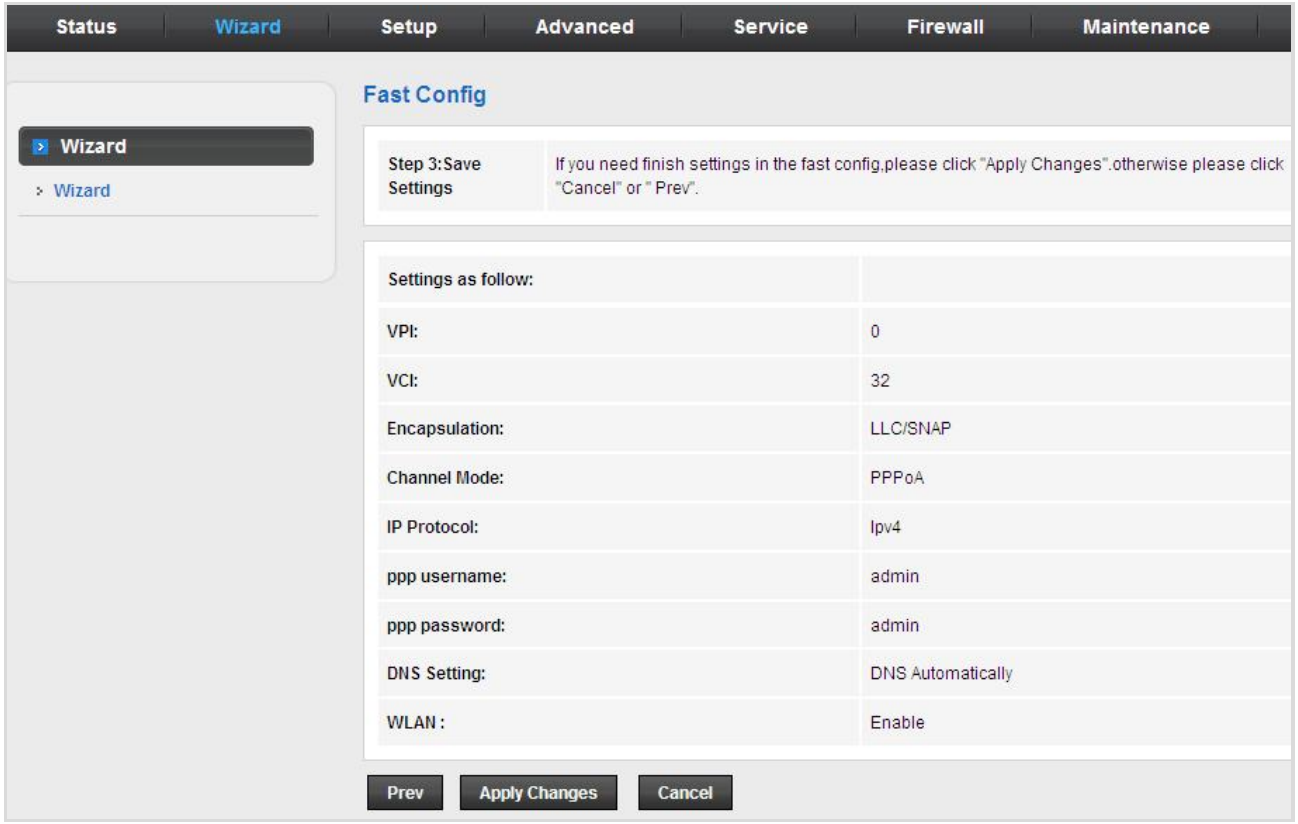


Figure 5-17 Wizard PPPoA Saved

5.2.5 1483 Routed

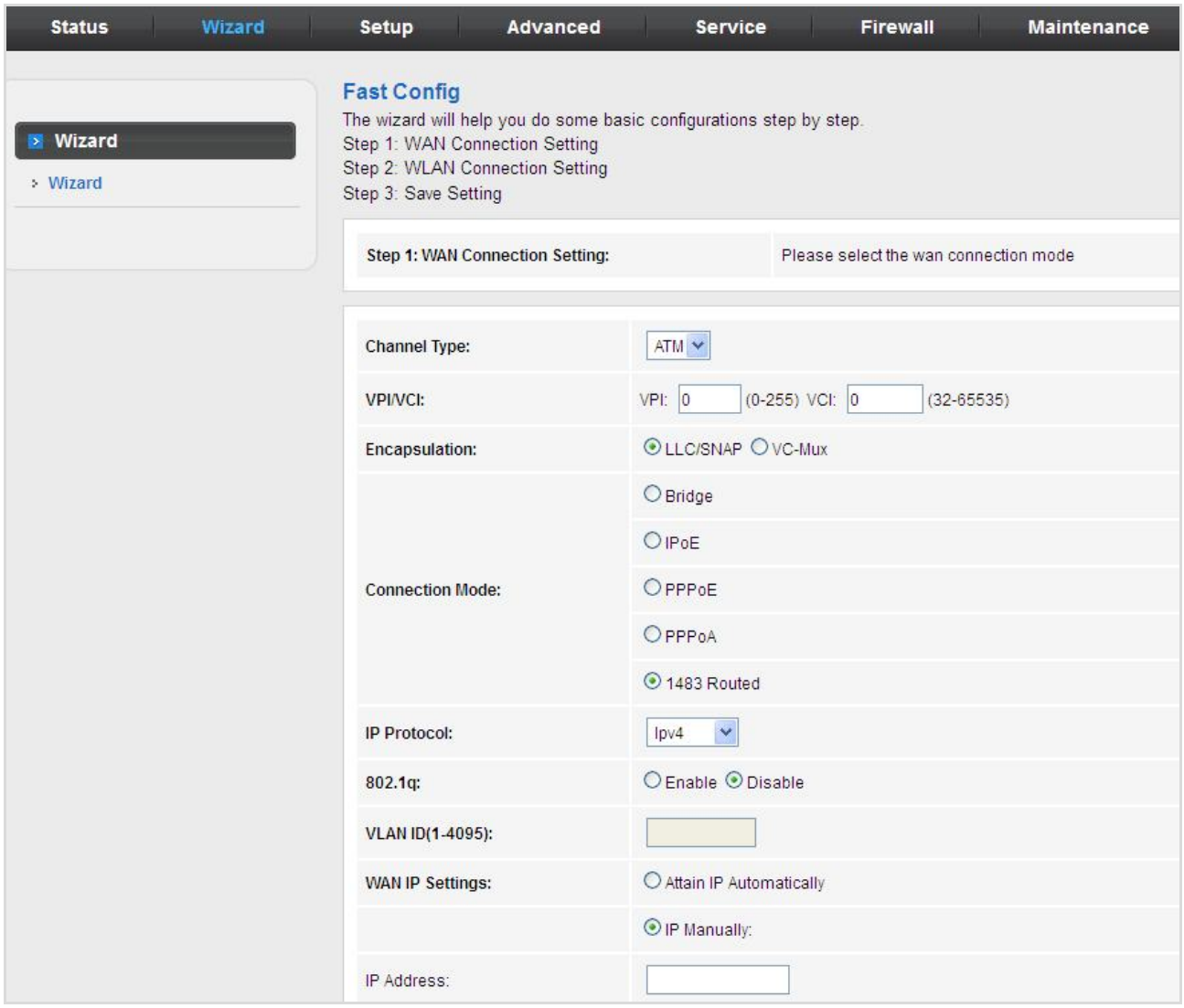


Figure 5-18 Wizard 1483 Routed

Figure 5-19 Wizard 1483 Routed WLAN

And click **Apply changes** to save the configuration.

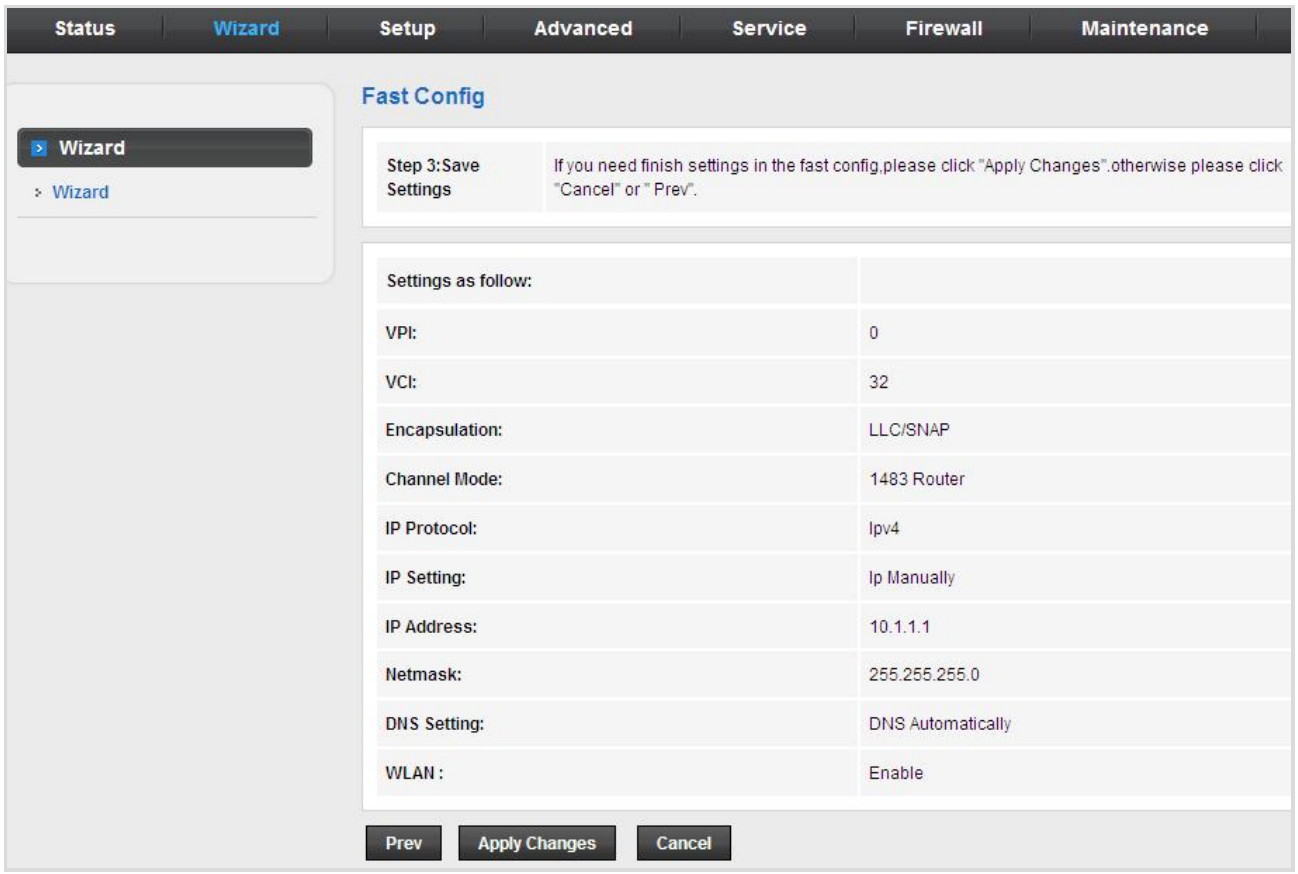


Figure 5-20 Wizard 1483 Routed Saved

5.3 Setup

In the navigation bar, click Setup. The Setup page that is displayed contains WAN, LAN and WLAN.

5.3.1 WAN

Choose **Setup** > **WAN** and the page is displayed below.

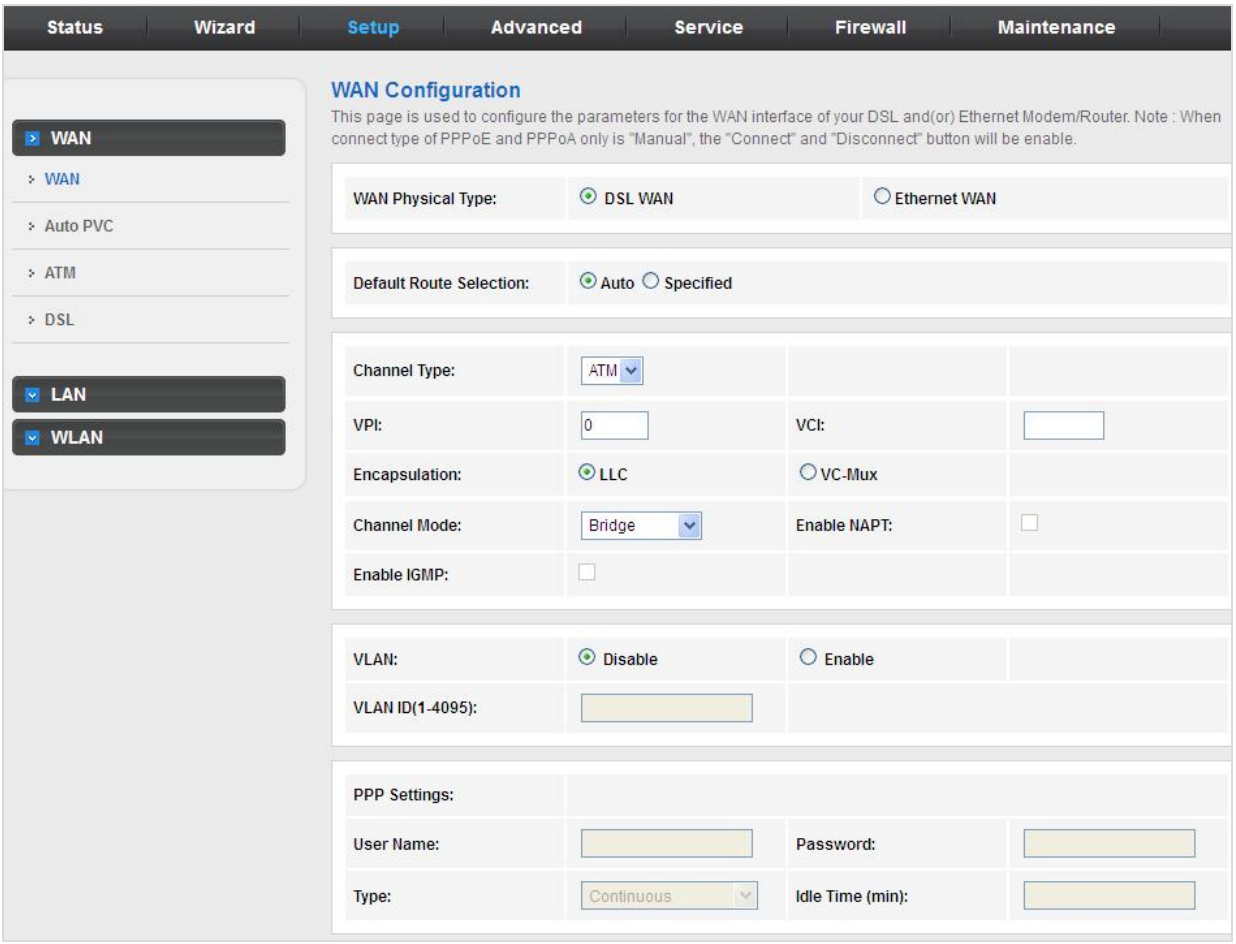


Figure 5-21 WAN

The following table describes the parameters:

Field	Description
WAN Physical Type	You can select **DSL WAN** or **Ethernet WAN** as default WAN port.
Default Route Selection	You can select **Auto** or **Specified**.
Channel Type	You can choose **ATM** or **PTM**.
VPI	The virtual path between two points in an ATM network, ranging from 0 to 255.
VCI	The virtual channel between two points in an ATM network, ranging from

	32 to 65535 (1 to 31 are reserved for known protocols)
Encapsulation	You can select **LLC** or **VC-Mux**.
Channel Mode	You can choose **Bridge**, **IPoE**, **PPPoE**, **PPPoA**, **1483 Routed**, **IPoA**
Enable NAPT	Select it to enable Network Address Port Translation (NAPT) function. If you do not select it and you want to access the Internet normally, you must add a route on the uplink equipment. Otherwise, the access to the Internet fails. Normally, it is enabled.
Enable IGMP	You can enable or disable Internet Group Management Protocol (IGMP) function.
VLAN	You can select **Disable** or **Enable** the VLAN
VLAN ID	You can enter the VLAN ID from 1 to 4095
IP Protocol	You can select **IPv4**, **IPv4/IPv6** or **IPv6**.
PPP Settings	
User Name	Enter the correct user name for PPP dial-up, which is provided by your ISP.
Password	Enter the correct password for PPP dial-up, which is provided by your ISP.
Type	You can choose **Continuous**, **Connect on Demand**, or **Manual**.
Idle Time (min)	To set the type to Connect on Demand, you need to enter the idle timeout time. Within the preset minutes, if the router does not detect the flow of the user continuously, the router automatically disconnects the PPPoE connection.
WAN IP Settings	
Type	You can choose **Fixed IP** or **DHCP**. ● To select Fixed IP, you should enter the local IP address, remote IP address and subnet mask. ● To select DHCP, the router is a DHCP client and the WAN IP address is assigned by the remote DHCP server.
Local IP Address	Enter the IP address of WAN interface provided by your ISP.
Remote IP Address	Enter the default gateway of WAN interface provided by your ISP.
Netmask	Enter the subnet mask of the local IP address.
Default Route	Select **Disable**, **Enable** or **Auto**. The default setting is **Auto**.
Unnumbered	Select this checkbox to enable IP unnumbered function.
Add	After configuring the parameters of this page, click it to add new WAN

	into the **WAN Interfaces Table**.
Modify	Select the WAN in the **WAN Interfaces Table**, and modify the parameters. After finishing, click it to apply the settings.
WAN Interfaces Table	This table shows the existing WAN settings. The maximum item of this table is eight.

5.3.2 Auto PVC

Choose **Setup** > **Auto PVC** and the page is displayed below. On this page, you can get a PVC automatically by detecting function. Add or delete the PVC that you do not need.

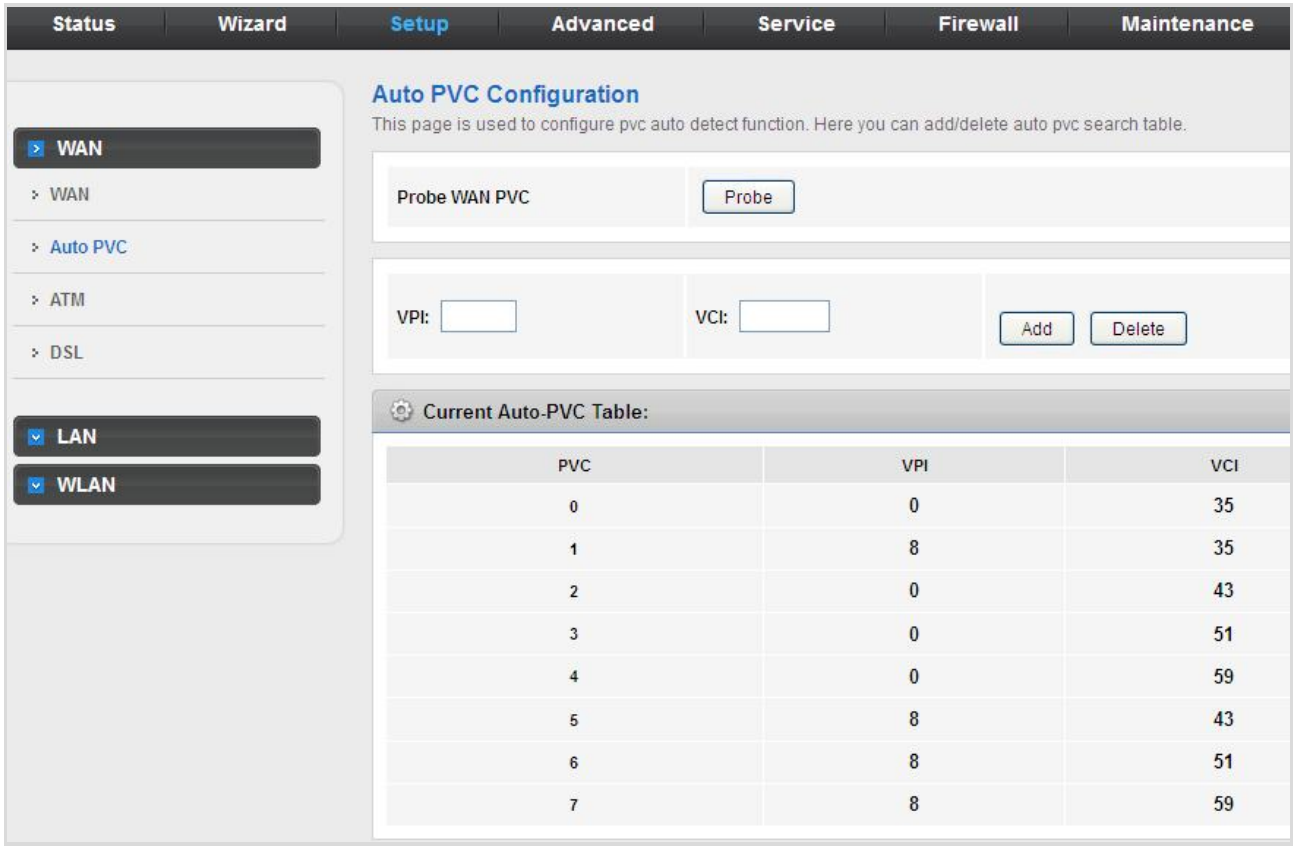


Figure 5-22 Auto PVC

The following table describes the parameters:

Field	Description
Probe WAN PVC	Click **Probe** to display WAN Permanent virtual circuit.
VPI	Virtual Path Identifier. This is read-only field and is selected on the Select column of the Current ATM VC Table.
VCI	Virtual Channel Identifier. This is read-only field and is selected on the Select column in the Current ATM VC Table. The VCI, together with VPI, is used to identify the next destination of a cell as it passes through the ATM switch.

5.3.3 ATM

Choose **Setup** > **ATM** and the page is displayed below. On this page, you can configure the parameters of the ATM, including QoS, PCR, CDVT, SCR and MBS.

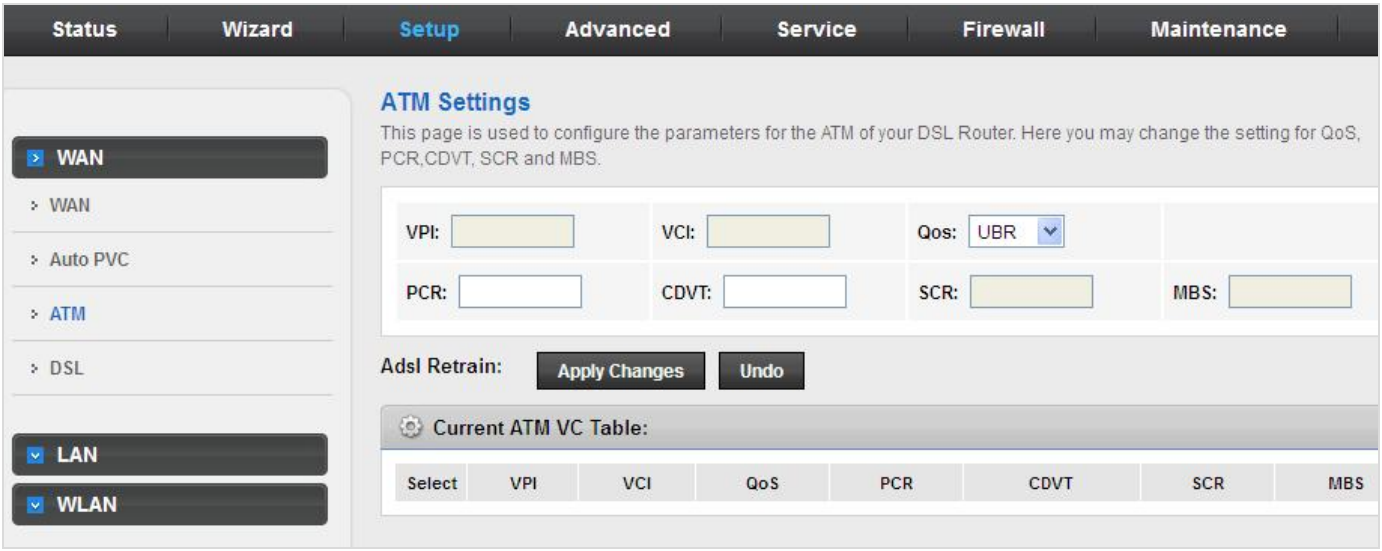


Figure 5-23 ATM

The following table describes the parameters:

Field	Description
VPI	Virtual Path Identifier. This is read-only field and is selected on the Select column of the Current ATM VC Table.
VCI	Virtual Channel Identifier. This is read-only field and is selected on the Select column in the Current ATM VC Table. The VCI, together with VPI, is used to identify the next destination of a cell as it passes through the ATM switch.
QoS	Quality of Server, a characteristic of data transmission that measures how accurately and how quickly a message or data is transferred from a source host to a destination host over a network. The four QoS options are ■ UBR (Unspecified Bit Rate): When UBR is selected; the SCR and MBS fields are disabled. ■ CBR (Constant Bit Rate): When CBR is selected; the SCR and MBS fields are disabled. ■ nrt-VBR (non-real-time Variable Bit Rate): When nrt-VBR is selected, the SCR and MBS fields are enabled. ■ rt-VBR (real-time Variable Bit Rate): When rt-VBR is selected, the SCR and MBS fields are enabled.
PCR	Peak Cell Rate, measured in cells/sec., is the cell rate which the source

	may never exceed.
CDVT	Cell delay variation tolerance (CDVT) is the amount of delay permitted between ATM cells (in microseconds).
SCR	Sustained Cell Rate, measured in cells/sec., is the average cell rate over the duration of the connection.
MBS	Maximum Burst Size, a traffic parameter that specifies the maximum number of cells that can be transmitted at the peak cell rate.

5.3.4 DSL

Choose **Setup** > **ATM** and the page is displayed below. On this page, you can select the DSL modulation. This factory default setting is mostly used. The router negotiates the modulation modes with the DSLAM.

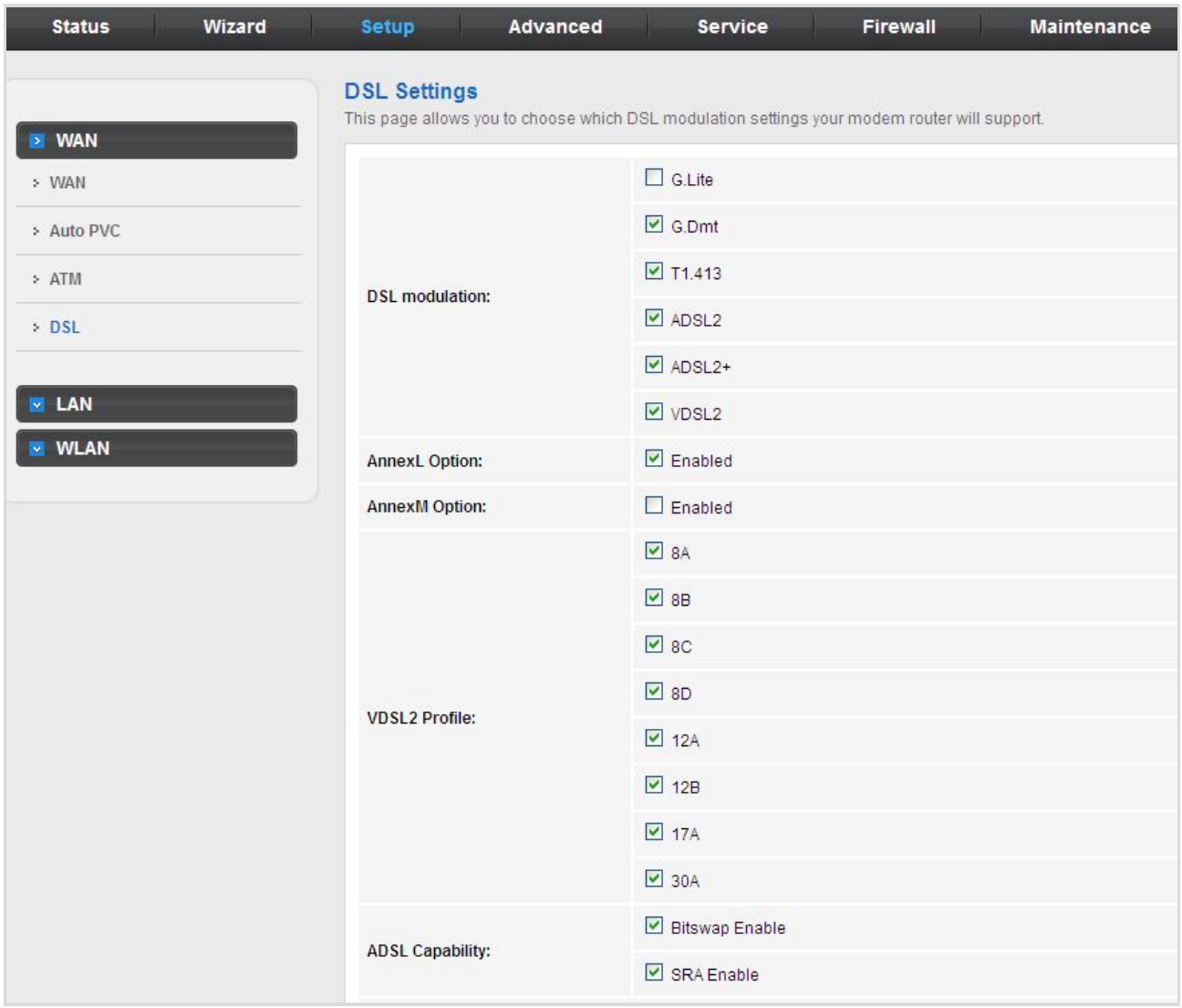


Figure 5-24 DSL

The following table describes the parameters:

Field	Description
DSL modulation	Choose preferred xDSL standard protocols. **G.Lite**: G.992.2 Annex A **G.Dmt**: G.992.1 Annex A **T1.413**: T1.413 issue #2 **ADSL2**: G.992.3 Annex A **ADSL2+**: G.992.5 Annex A **VDSL2**: ITU G.993.2
AnnexL Option	You can choose **Enable** or **Disable** ADSL2/ADSL2+ AnnexL capability.
AnnexM Option	You can choose **Enable** or **Disable** ADSL2/ADSL2+ AnnexM capability.
VDSL2 Profile	Select the VDSL2 profile that the DSLAM supported. **8A, 8B, 8C, 8D, 12A, 12B, 17A, 30A**
ADSL Capability	**Bitswap Enable**: You can choose **Enable** or **Disable** bitswap capability. **SRA Enable**: You can choose **Enable** or **Disable** SRA (seamless rate adaptation) capability.

5.3.5 LAN

Choose Setup > **LAN**. The **LAN** page that is displayed contains **LAN, DHCP, DHCP Static and LAN IPv6**.

5.3.2.1 LAN

Click **LAN** in the left pane and the page shown in the following figure appears. On this page, you can change IP address of the router. The default IP address is **192.168.1.1**, which is the private IP address of the router.

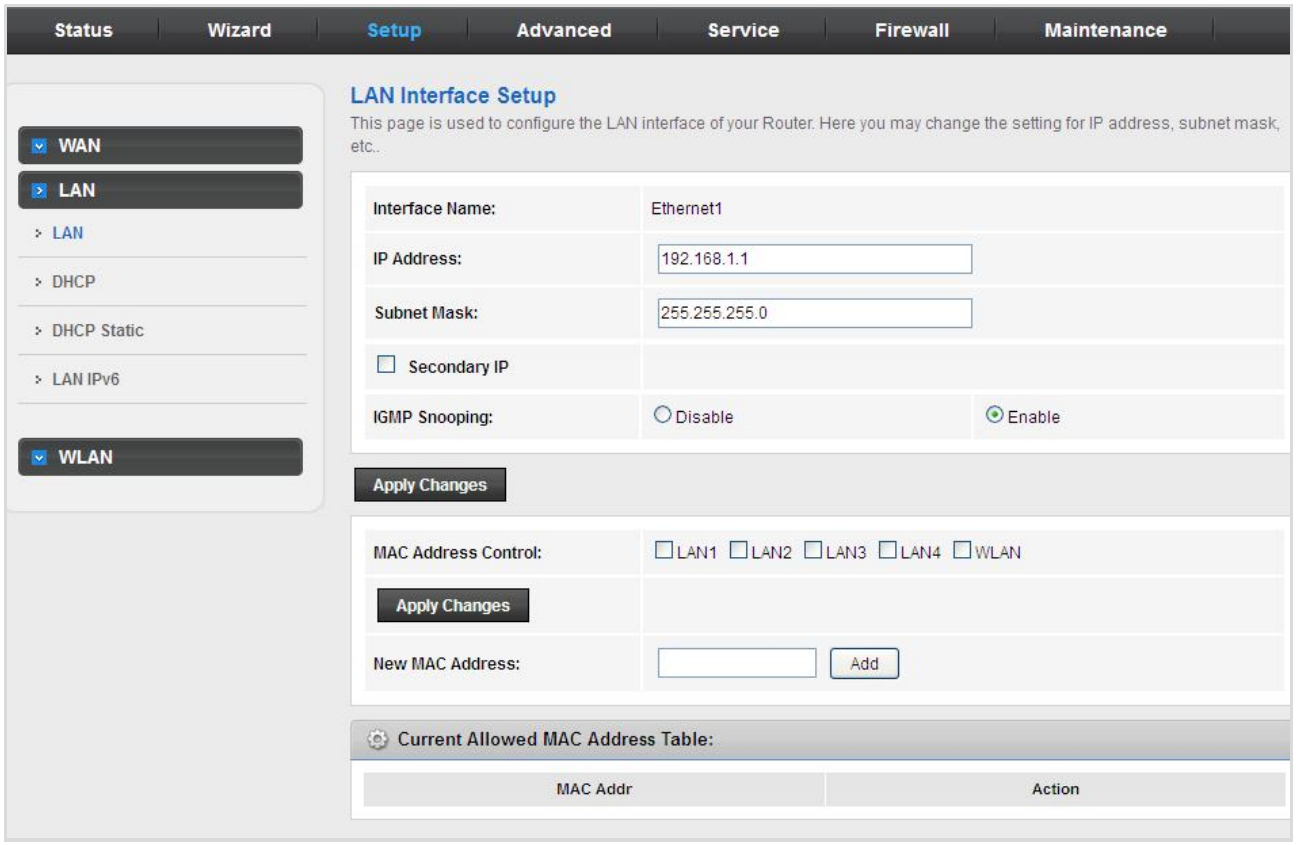


Figure 5-25 LAN

The following table describes the parameters:

Field	Description
IP Address	The IP address of your LAN hosts is used to identify the device's LAN port.
Subnet Mask	Enter the subnet mask of LAN interface.
Secondary IP	Select it to enable/disable a secondary LAN IP address. The two LAN IP addresses must be in the different network.
IGMP Snooping	**Enable** or **Disable** the IGMP snooping function for the multiple bridged LAN ports.
MAC Address Control	It is the access control based on MAC address. Select LAN1, LAN2, LAN3, LAN4, WLAN and the host whose MAC address listed in the Currently Allowed MAC Address Table can access the device. Then click "**Apply Changes**" to save the new settings.
New MAC Address	Enter MAC address and then click **Add** to add a new MAC address.

5.3.2.2 DHCP

Dynamic Host Configuration Protocol (DHCP) allows the individual PC to obtain the TCP/IP configuration from the centralized DHCP server. You can configure this router as a DHCP server or disable it. The DHCP server can assign IP address, IP default gateway, and DNS server to DHCP clients. This router can also act as a surrogate DHCP server (DHCP Relay) where it relays IP address assignment from an actual real DHCP server to clients. You can enable or disable DHCP server.

- **DHCP Server**

Click **DHCP** in the left pane and the page shown in the following figure appears.

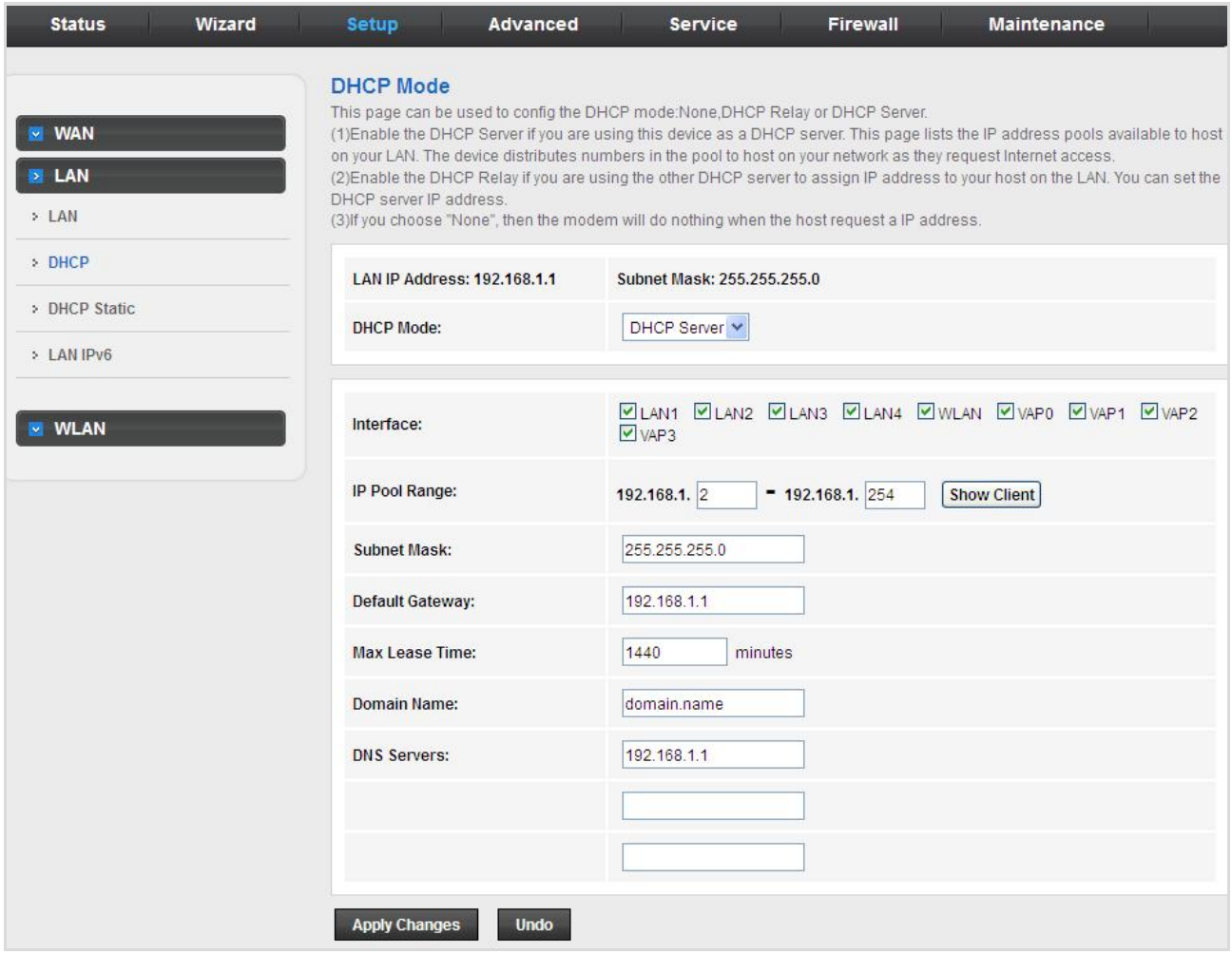


Figure 5-26 DHCP

The following table describes the parameters:

Field	Description
DHCP Mode	You can choose **None**, **DHCP Relay** or **DHCP Server**. If set to DHCP Server, the router can assign IP addresses, IP default gateway and DNS Servers to the host in Windows XP, Windows 7 and other operating systems that support the DHCP client.

Interface	By default, all ports are selected; click it to unselect and those ports cannot function with the IP address.
IP Pool Range	Specify the lowest and highest addresses in the pool. It specifies the first IP address in the IP address pool. The router assigns IP address based on the IP pool range to the host.
Show Client	Click it and the **Active DHCP Client Table** appears. It shows IP addresses assigned to clients.
Subnet Mask	Enter the subnet mask.
Default Gateway	Enter the default gateway of the IP address pool.
Max. Lease Time	The Lease Time is the amount of time that a network user is allowed to maintain a network connection to the device using the current dynamic IP address. At the end of the Lease Time, the lease is either renewed or a new IP is issued by the DHCP server. The amount of time is in units of seconds. The default value is 1440 minutes (1 day).
Domain Name	Domain Name is the most recognized system for assigning addresses to Internet web servers.
DNS Servers	You can configure the DNS server IP addresses for DNS Relay.

Click **Show Client** on the **DHCP Mode** page and the page shown in the following figure appears. You can view the IP address assigned to each DHCP client.

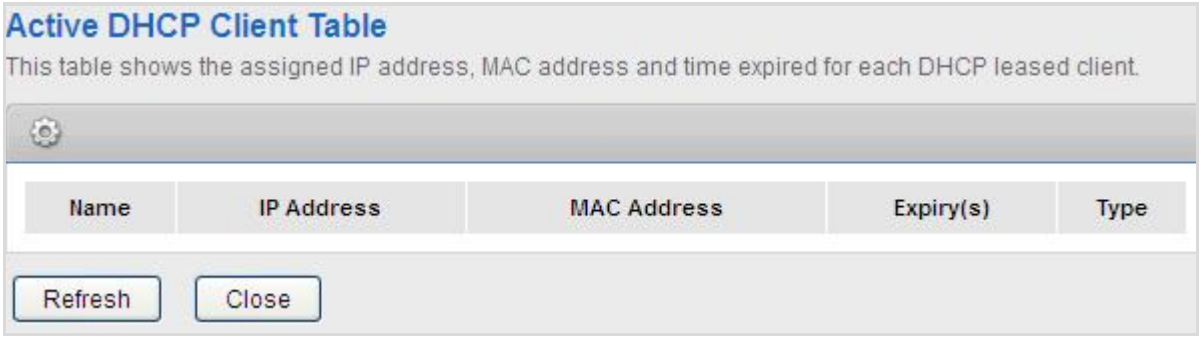


Figure 5-27 DHCP Table

The following table describes the parameters:

Field	Description
IP Address	It displays the IP address assigned to the DHCP client from the router.
MAC Address	It displays the MAC address of the DHCP client. Each Ethernet device has a unique MAC address. The MAC address is assigned at the factory and it consists of six pairs of hexadecimal character, for example, A8-F7-E0-00-11-22.
Expiry(s)	It displays the lease time. The lease time determines the period that the host retains the assigned IP addresses before the IP addresses change.
Refresh	Click it to refresh this page.
Close	Click it to close this page.

Click **Set Vendor Class IP Range** on the **DHCP Mode** page and the page as shown in the following figure appears. On this page, you can configure the IP address range based on the device type.

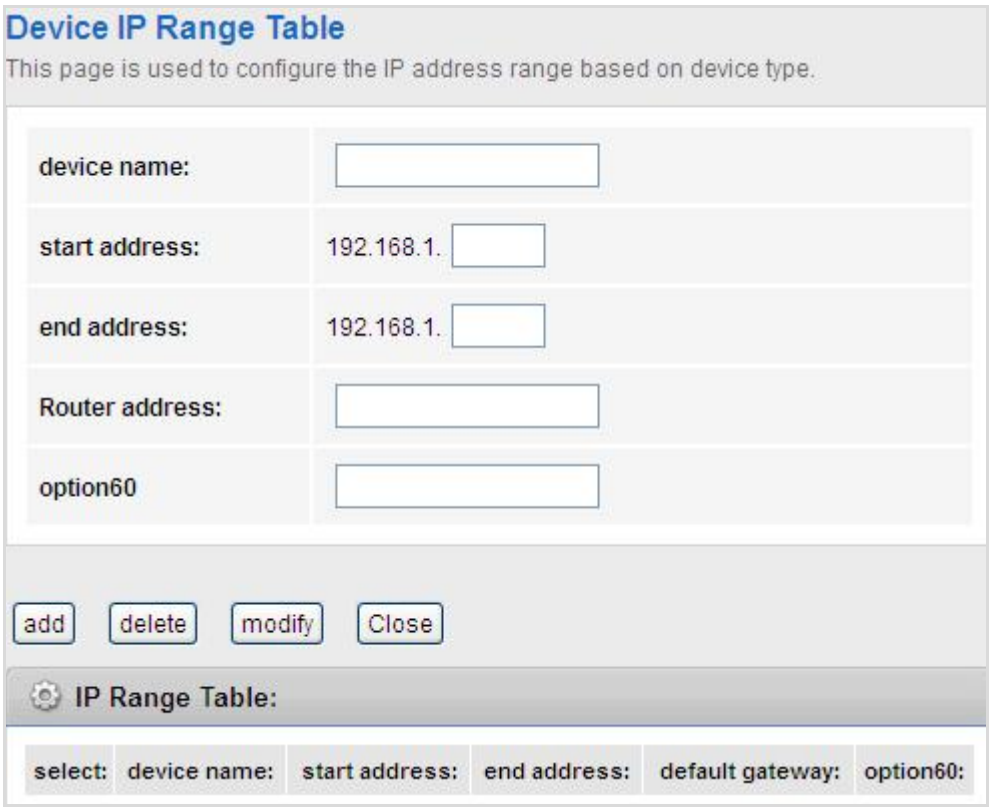


Figure 5-28 Device IP Range Table

- **None**

In the **DHCP Mode** field, choose **None** and the page shown in the following figure appears.

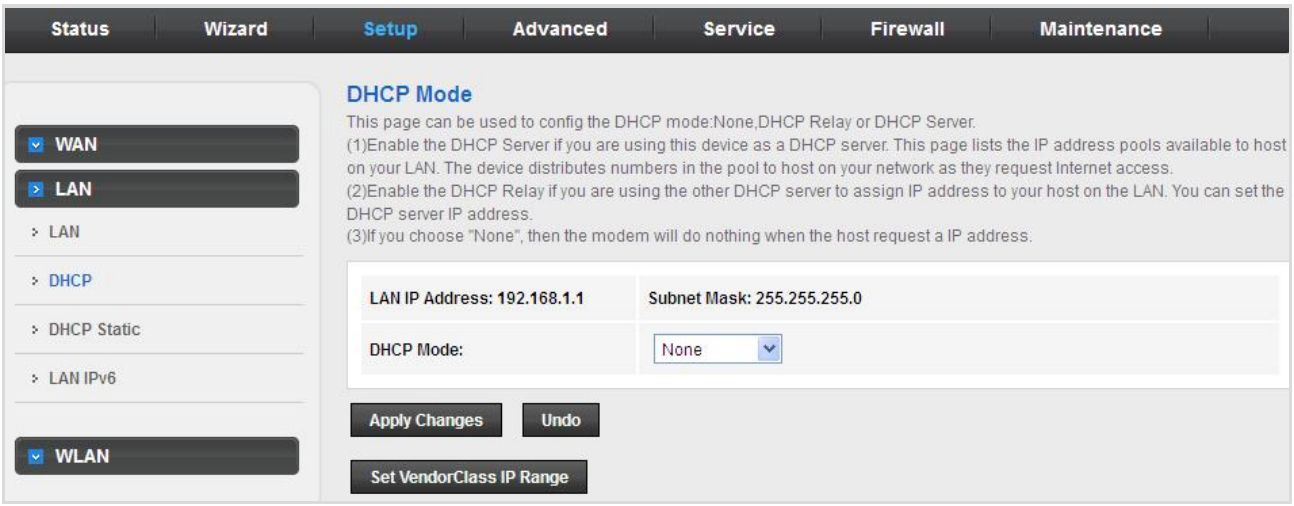


Figure 5-29 DHCP None

■ DHCP Relay

In the **DHCP Mode** field, choose **DHCP Relay** and the page shown in the following figure appears.

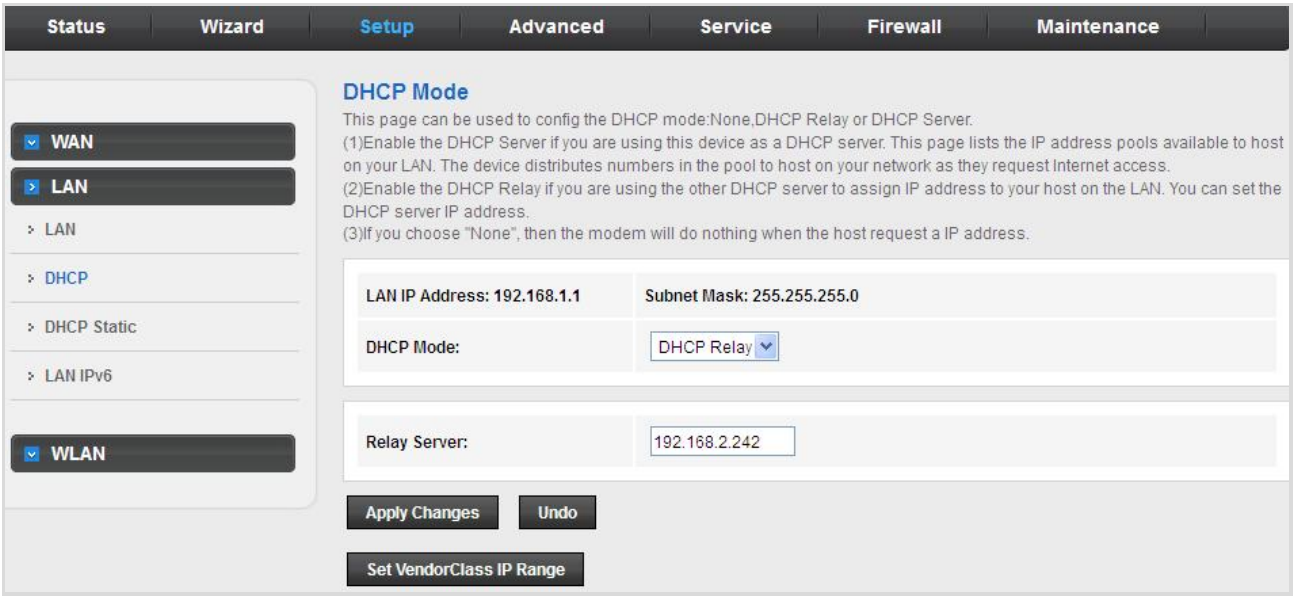


Figure 5-30 DHCP Relay

The following table describes the parameters:

Field	Description
DHCP Mode	If set to **DHCP Relay**, the router acts as a surrogate DHCP Server and relays the DHCP requests and responses between the remote server and the client.
Relay Server	Enter the DHCP server address provided by your ISP.
Apply Changes	Click it to save the settings on this page.
Undo	Click it to refresh this page.

5.3.2.3 DHCP Static

Click **DHCP Static** in the left pane and the page shown in the following figure appears. You can assign the IP addresses on the LAN to the specific individual PCs based on their MAC address.

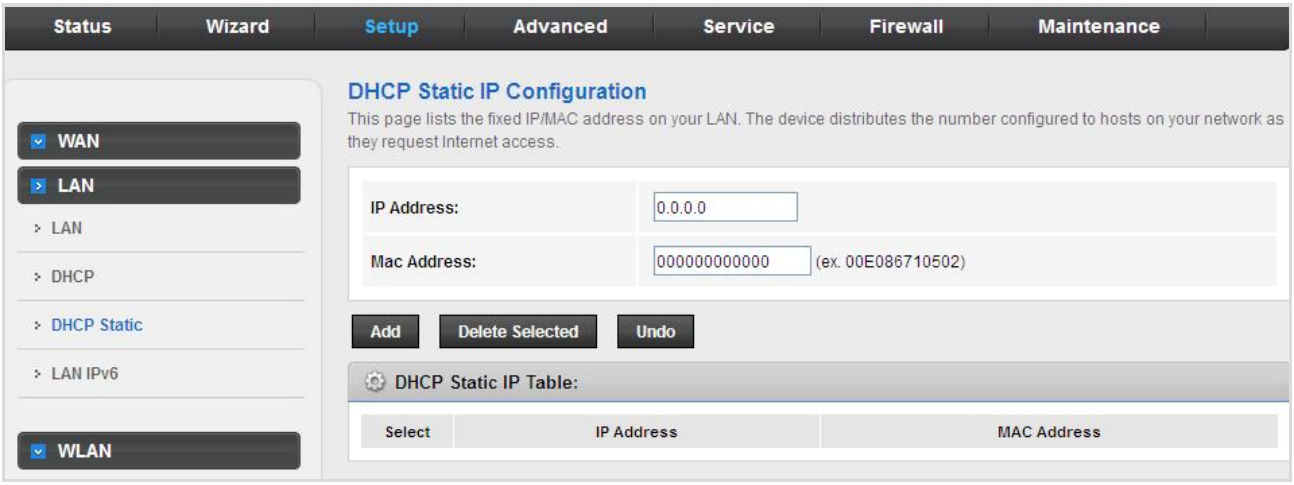


Figure 5-31 DHCP Static

The following table describes the parameters:

Field	Description
IP Address	Enter the specified IP address in the IP pool range, which is assigned to the host.
MAC Address	Enter the MAC address of a host on the LAN.
Add	After entering the IP address and MAC address, click it. A row will be added in the **DHCP Static IP Table**.
Delete Selected	Select a row in the **DHCP Static IP Table**; then click it and this row is deleted.
Undo	Click it to refresh this page.
DHCP Static IP Table	It shows the assigned IP address based on the MAC address.

5.3.2.4 LAN IPv6

On this page, you can configure the LAN IPv6. Choose **Setup** > **LAN** > **LAN IPv6**. The **IPv6 LAN setting** page as shown in the following figure appears.

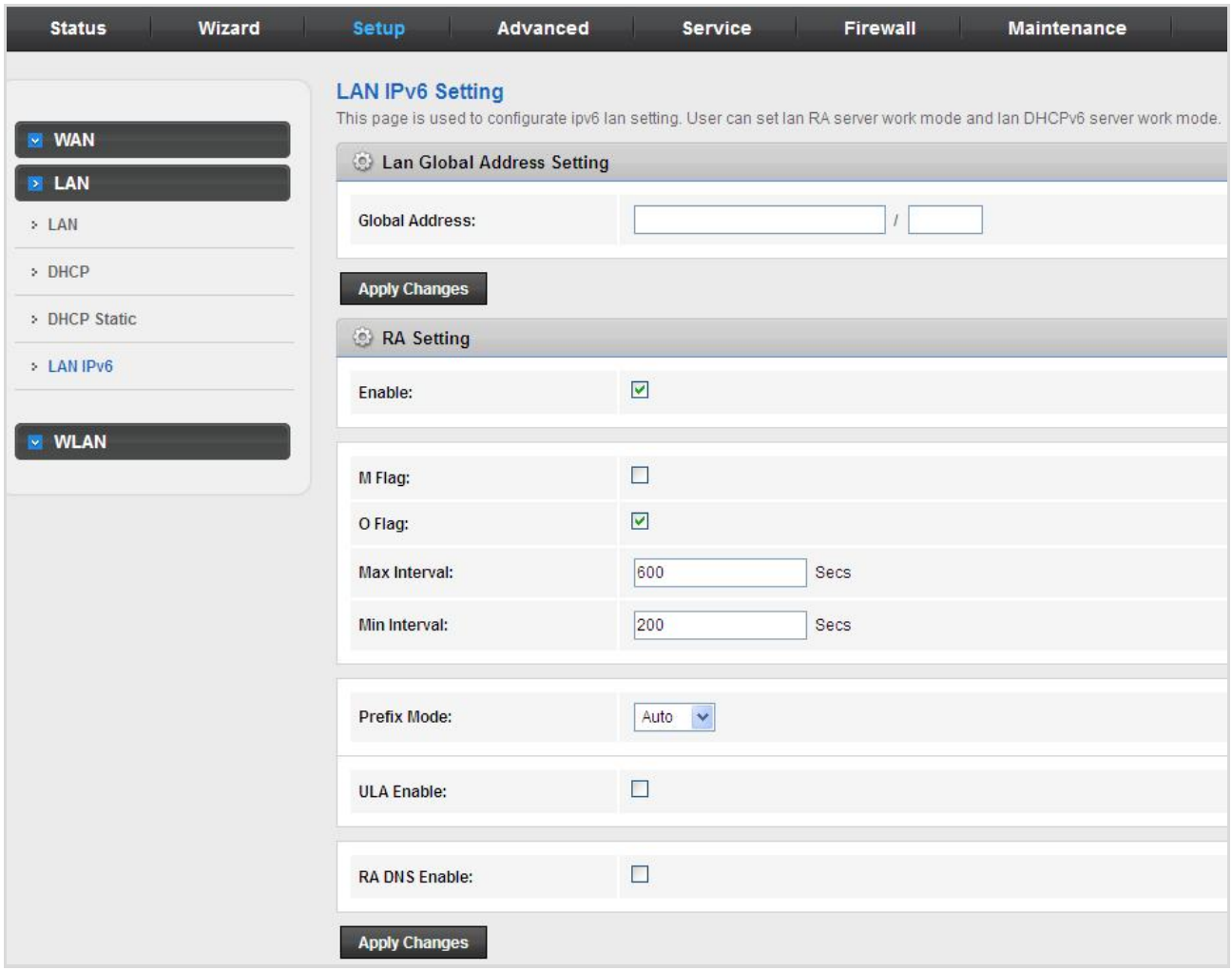


Figure 5-32 LAN IPv6

The following table describes the parameters:

LAN Global Address Setting

Field	Description
Global Address	Specify the LAN global IPv6 address; may be assigned by ISP.

RA Setting

Field	Description
Enable	Enable or disable the Router Advertisement feature.
M Flag	Enable or disable the “Managed address configuration” flag in RA packet.
O Flag	Enable or disable the “other configuration” flag in RA packet.
Max Interval	Maximum sending time interval.
Min Interval	Minimum sending time interval.
Prefix Mode	Specify the RA feature prefix mode **Auto:** The RA prefix will use WAN DHCP-pd prefix **Manual:** User will specify the **Prefix Address**, **Length**, **Preferred Time** and **Valid Time**.
ULA	Unique Local Address. Enable/Disable the feature to access.
RA DNS Enable	Enable/Disable the feature to access.

DHCPv6 Setting

Field	Description
DHCPv6 Mode	Select the Mode to **None**, **Manual Mode** or **Auto Mode**.
IPv6 Address Suffix Pool	Enter the IPv6 address.
IPv6 DNS Mode	Select the Mode to **Auto** or **Manual**.

5.3.6 WLAN

5.3.6.1 Basic

This page contains all the wireless basic settings. Most users will be able to configure the wireless portion and get it working properly using the setting on this screen.

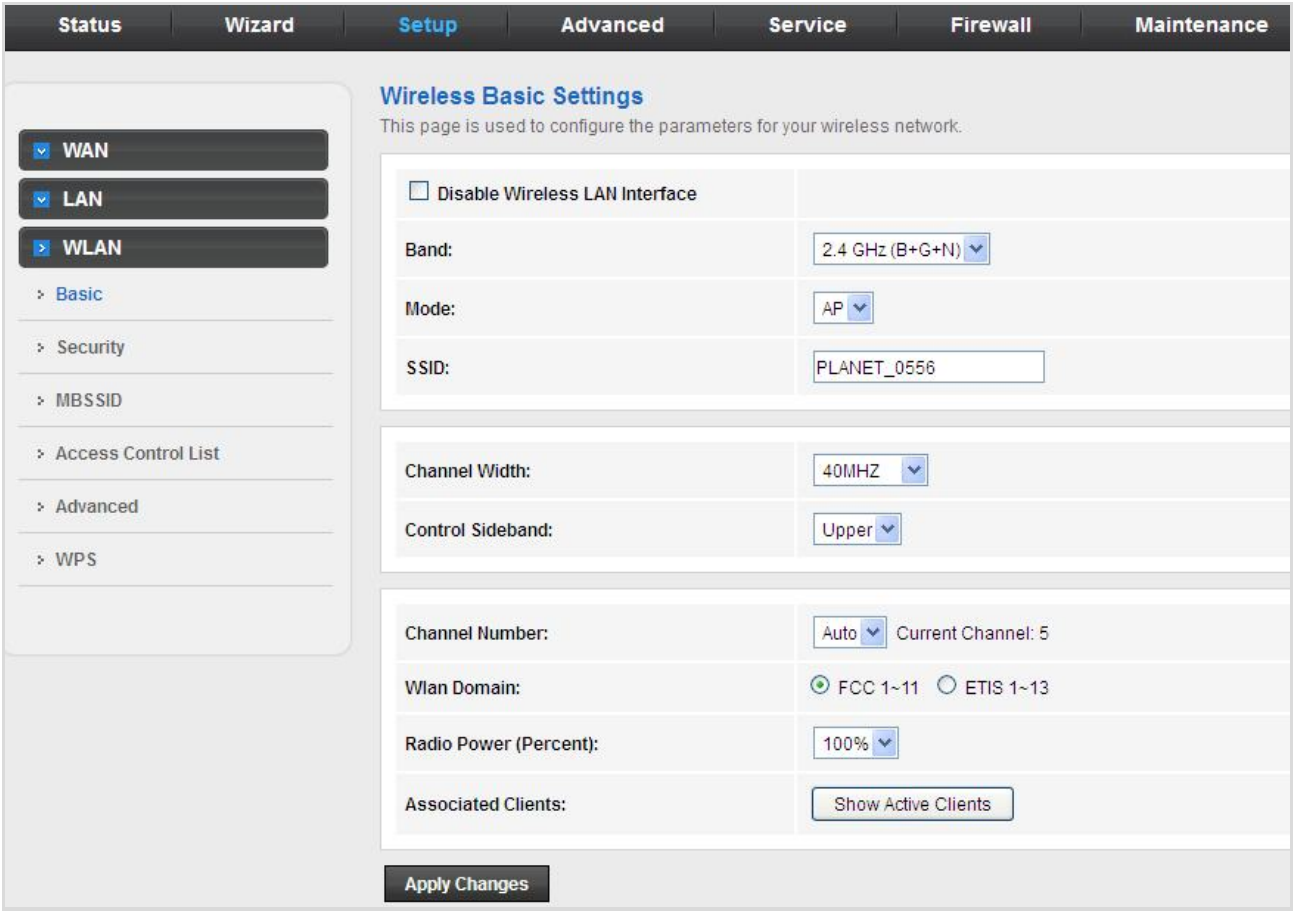


Figure 5-33 WLAN

The following table describes the parameters:

Field	Description
Disable Wireless LAN Interface	Enable/Disable the wireless function for VDR-301N.
Band	Select the appropriate band from the list provided to correspond with your network setting.
Mode	Select AP Mode.
SSID	The Service Set Identifier (SSID) or network name. It is case sensitive and must not exceed 32 characters, which may be any keyboard character. The mobile wireless stations will select the same SSID to be able to communicate with your VDSL2 Router.

Channel Width	Select channel width to **20MHz**, **40MHz** or **20/40MHz**.
Control Sideband	Select **Upper** or **Lower** sideband.
Channel Number	Select the appropriate channel from the list provided to correspond with your network settings. You will assign a different channel for each AP to avoid signal interference.
WLAN Domain	Select **FCC 1~11** or **ETSI 1~13**.
Radio Power (Percent)	100%, 80%, 50%, 25%, 10%.
Associated Clients	Click it to see the clients currently associated with VDR-301N.

Click **Show Active Client** and the page shown in the following figure appears. You can view the information of the clients connected to the VDSL2 Router.

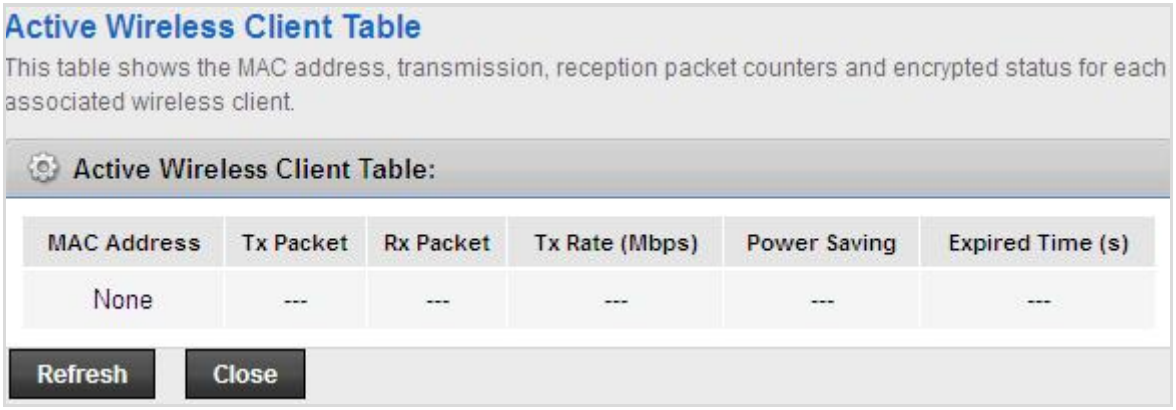


Figure 5-34 Active Wireless Client Table

5.3.6.2 Security

This screen allows you to set up the wireless security. Turn on WEP or WPA by using encryption keys that could prevent any unauthorized access to your WLAN.

Figure 5-35 Wireless Security

The following table describes the parameters:

Field	Description
SSID Type	Select the SSID Type.
Encryption	There are 4 types of security to be selected. To secure your WLAN, it's strongly recommended to enable this feature. **WEP:** Make sure that all wireless devices on your network are using the same encryption level and key. **WPA/WPA2 (TKIP):** WPA/WPA2 uses Temporal Key Integrity Protocol (TKIP) for data encryption. TKIP utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers. **WPA/WPA2 (AES):** WPA/WPA2, also known as 802.11i, uses Advanced Encryption Standard (AES) for data encryption. AES utilizes a symmetric 128-bit block data encryption. **WPA2 Mixed:** The AP supports WPA (TKIP) and WPA2 (AES) for data encryption. The actual selection of the encryption methods will depend on the clients.
Use 802.1x Authentication	Check it to enable 802.1x authentications. This option is selected only when the "Encryption" is chosen to either None or WEP. If the "Encryption" is WEP, you need to further select the WEP key length to be either WEP 64 character or WEP 128 character.

WPA Authentication Mode	There are 2 types of authentication mode for WPA. **Enterprise (RADIUS):** WPA RADIUS uses an external RADIUS server to perform user authentication. To use WPA RADIUS, enter the IP address of the RADIUS server, the RADIUS port (default is 1812) and the shared secret from the RADIUS server. **Personal (Pre-Shared Key):** Pre-Shared Key authentication is based on a shared secret that is known only by the parties involved. To use WPA Pre-Shared Key, select key format and enter a password in the "Pre-Shared Key Format" and "Pre-Shared Key" setting respectively.
Pre-Shared Key Format	**Passphrase:** Select this to enter the Pre-Shared Key secret as user-friendly textual secret. **Hex (64 characters):** Select this to enter the Pre-Shared Key secret as hexadecimal secret.
Pre-Shared Key	Specify the shared secret used by this Pre-Shared Key. If the "Pre-Shared Key Format" is specified as PassPhrase, then it indicates a passphrase of 8 to 64 character long or 64-hexadecimal number.
Authentication RADIUS Server	If the WPA-RADIUS is selected in "WPA Authentication Mode", the port (default is 1812), IP address and password of external RADIUS server are specified here.

5.3.6.3 MBSSIDs (Multiple BSSIDs)

This screen allows you to do the wireless multiple SSIDs setup.

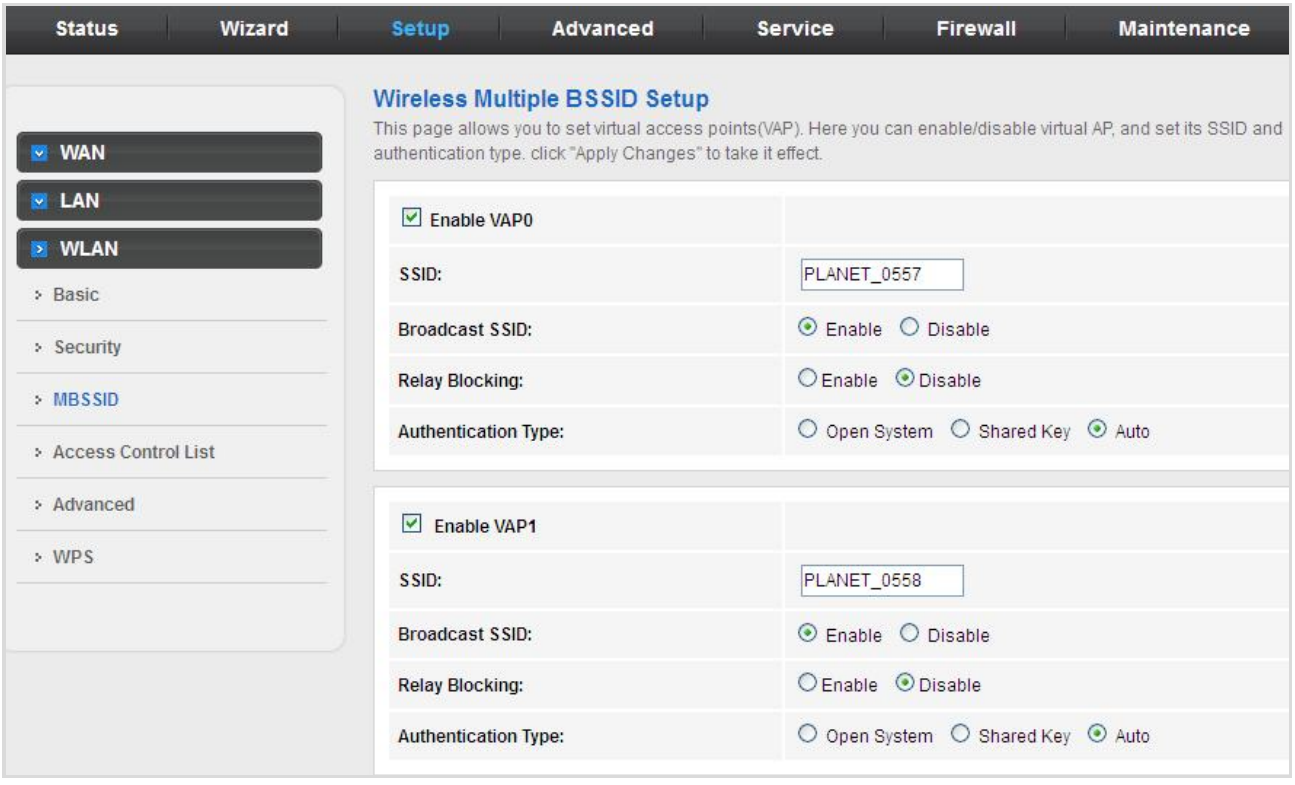


Figure 5-36 Wireless MBSSIDs

5.3.6.4 Access Control List

This page allows administrator to have access control by entering MAC address of client stations. When this function is enabled, MAC address can be added to access control list and only those clients whose wireless MAC address are in the access control list will be able to connect to your VDR-301N.

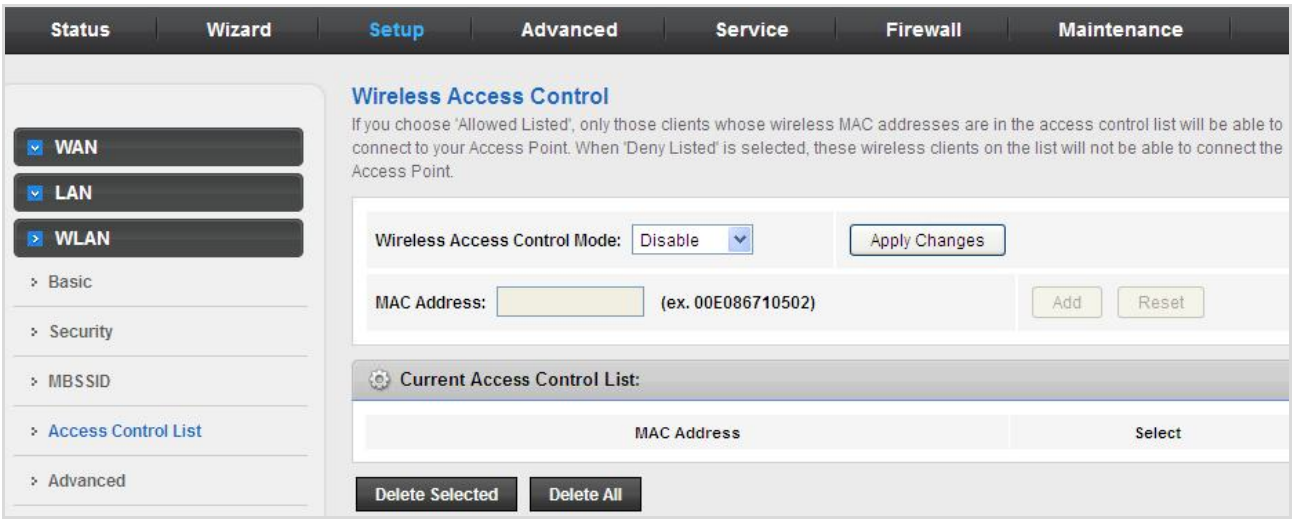


Figure 5-37 Wireless Access Control

The following table describes the parameters:

Field	Description
Wireless Access Control Mode	The Selections are: **Disable:** Disable the wireless ACL feature. **Allow Listed:** When this option is selected, no wireless clients except those whose MAC addresses are in the current access control list will be able to connect (to this device). **Deny Listed:** When this option is selected, all wireless clients except those whose MAC addresses are in the current access control list will not be able to connect (to this device).
MAC Address	Enter client MAC address.
Apply Changes	Click Apply Changes to add new settings; then it restarts.
Add	Click to add MAC address to the Current Access Control List.
Reset	Clear the settings.
Delete Selected	Select the rows to be deleted from Current Access Control List.
Delete All	Flush the list.

5.3.6.5 Advanced

This page allows advanced users who have sufficient knowledge of wireless LAN. These settings will not be changed unless you know exactly what will happen for the changes you made on your VDSL2 Router.

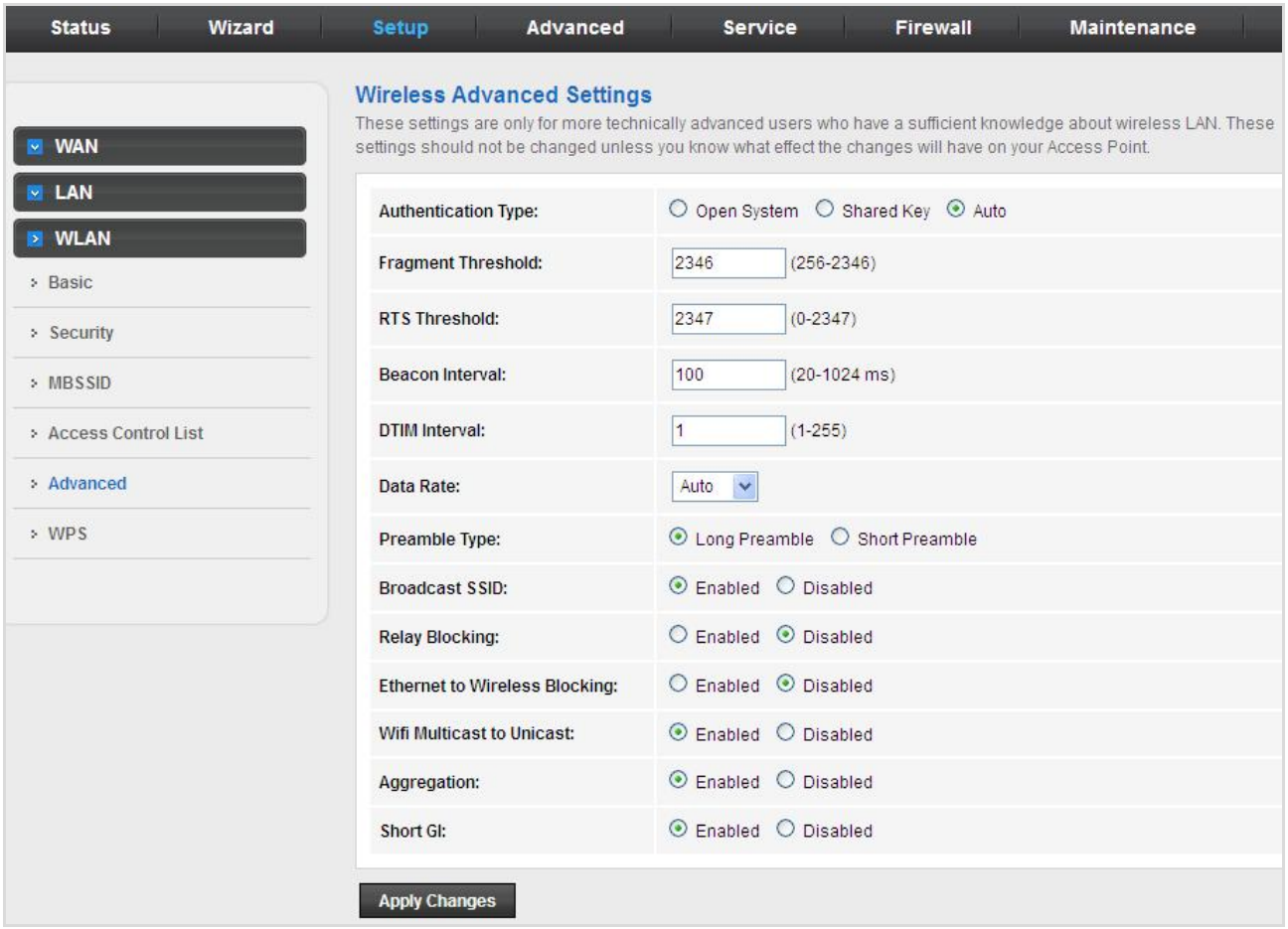


Figure 5-38 Wireless Advanced Setting

5.3.6.6 WPS

Wi-Fi Protected Setup (WPS) is a push-button or pin to simplify a secure network set-up.

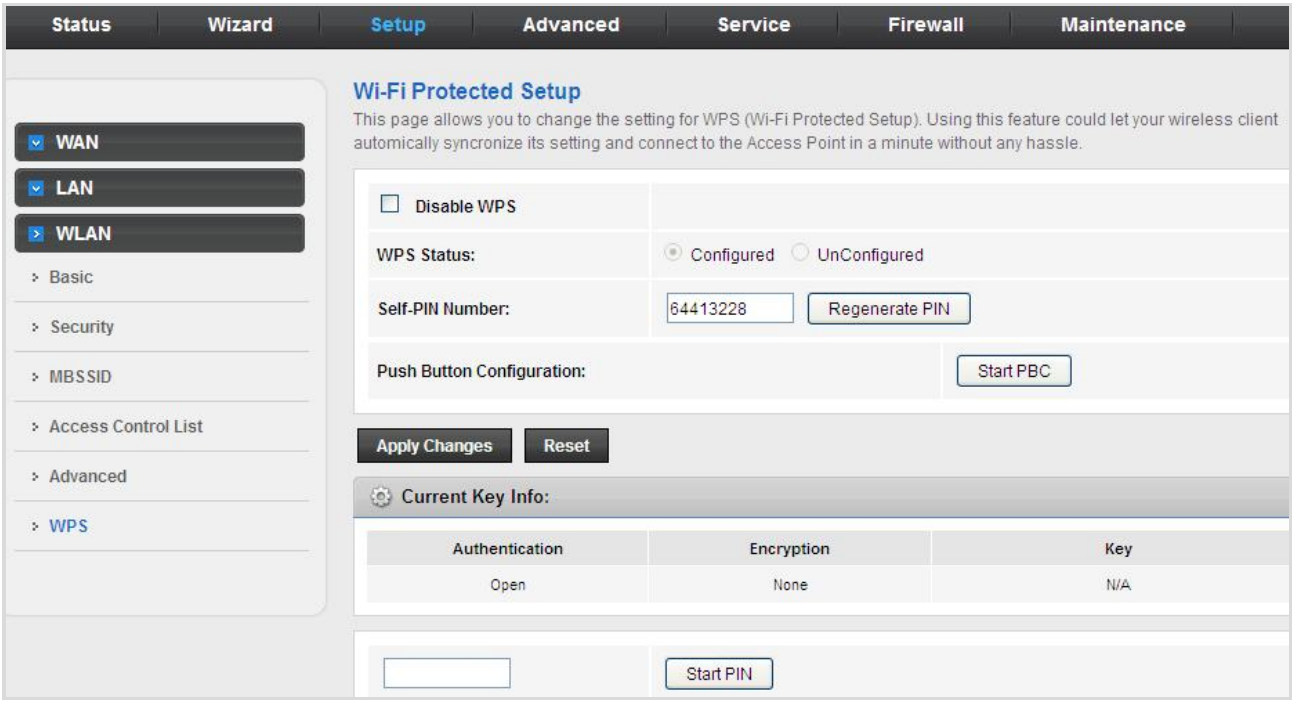


Figure 5-39 WPS

The following table describes the parameters:

Field	Description
Disable WPS	**Enable** or **Disable** the WPS function.
Self-Pin Number	Click Regenerate Pin to reset automatically to obtain an 8-digit number.
Push Button Configuration	Click the **Start PBC** button to connect from Wi-Fi dongle to device automatically.
Start Pin	Enter the Pin number to connect from device to Wi-Fi dongle.

5.4 Advanced

In the navigation bar, click **Advanced**. On the **Advanced** page that is displayed contains **Route**, **NAT**, **QoS**, **CWMP** (**TR-069**), **Port Mappings** and **Others**.

Figure 5-40 Advanced

5.4.1 Route

The Routing page enables you to define specific route for your Internet and network data. Most users do not need to define routes. On a typical small home or office LAN, the existing routes that set up the default gateways for your LAN hosts and for the VDSL2 Router provide the most appropriate path for all your Internet traffic.

- On your LAN hosts, a default gateway directs all Internet traffic to the LAN port(s) on the VDSL2 Router. Your LAN hosts know their default gateway either because you assigned it to them when you modified your TCP/IP properties, or because you configured them to receive the information dynamically from a server whenever they access the Internet.
- On the VDSL2 Router itself, a default gateway is defined to direct all outbound Internet traffic to a route at your ISP. The default gateway is assigned either automatically by your ISP whenever the device negotiates an Internet access, or manually by user to set up through the configuration. You may need to define routes if your home setup includes two or more networks or subnets, if you connect to two or more ISP services, or if you connect to a remote corporate LAN.

5.4.1.1 Static Route

Click **Static Route** in the left pane and the page shown in the following figure appears. This page is used to configure the routing information. You can add or delete IP routes.

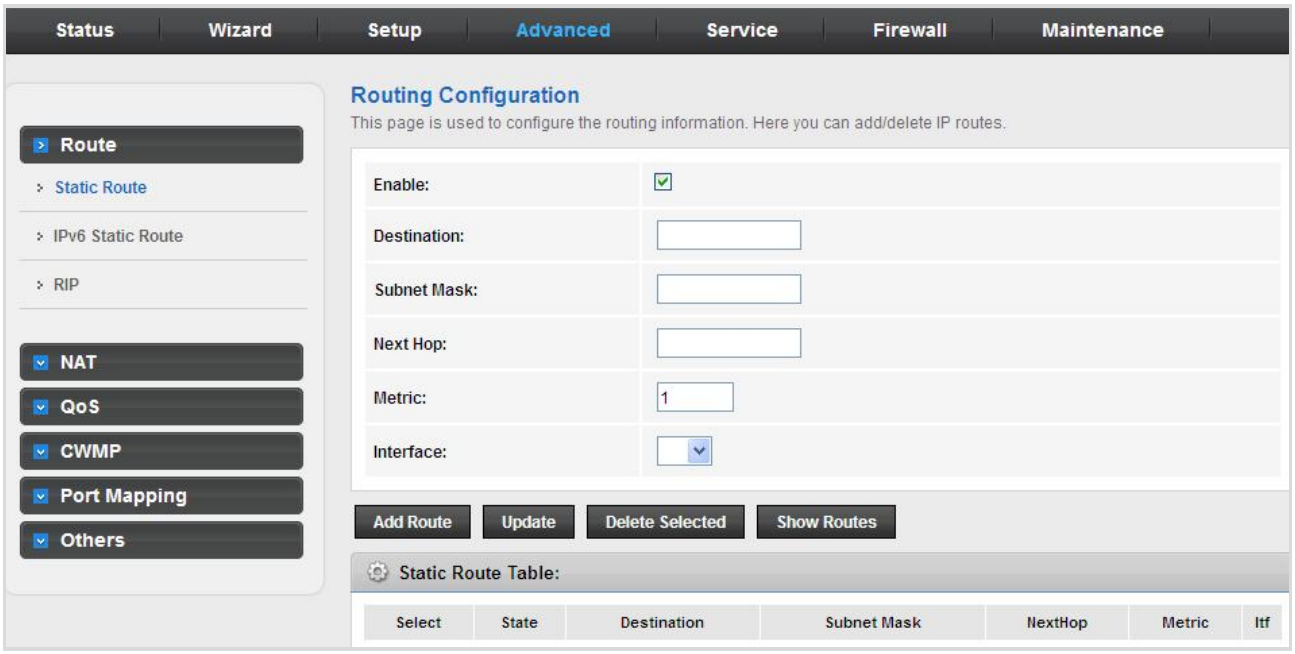


Figure 5-41 Static Route

The following table describes the parameters:

Field	Description
Enable	Click it to enable/disable the selected route or route to be added.
Destination	The network IP address of the subnet. The destination can be specified as the IP address of a subnet or a specific host in the subnet. It can also be specified as all zeros to indicate that this route should be used for all destinations for which no other route is defined (this is the route that creates the default gateway).
Subnet Mask	The network mask of the destination subnet.
Next Hop	The IP address of the next hop through which traffic will flow towards the destination subnet.
Metric	Defines the number of hops between network nodes that data packets travel.
Interface	The WAN interface to which a static routing subnet is to be applied.
Add Route	Add a user-defined destination route.

Update	Update the selected destination route on the Static Route Table.
Delete Selected	Delete a selected destination route on the Static Route Table.

Click **Show Routes** and the page shown in the following figure appears. You can view the information of the clients connected to the VDSL2 Router.

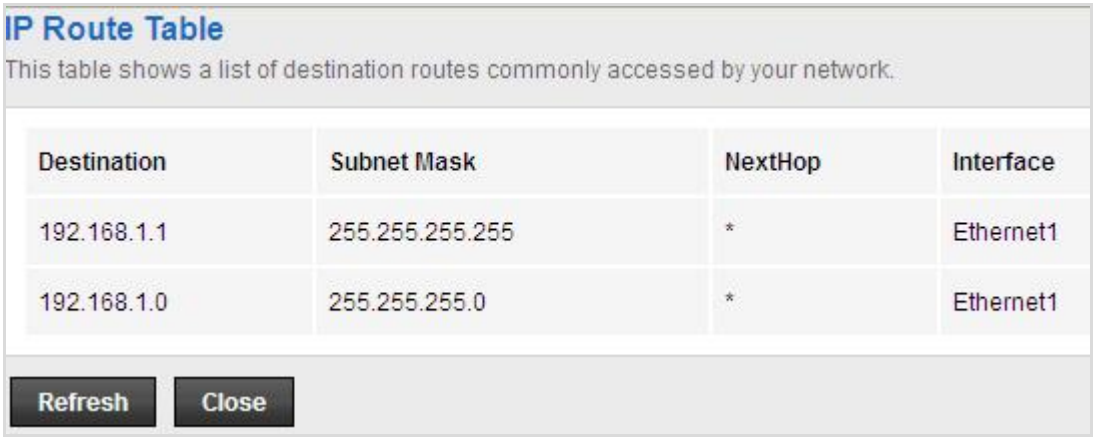


Figure 5-42 IP Route Table

5.4.1.2 IPv6 Static Route

Click **IPv6 Static Route** in the left pane and the page shown in the following figure appears. This page is used to configure the routing information. You can add or delete IP routes.

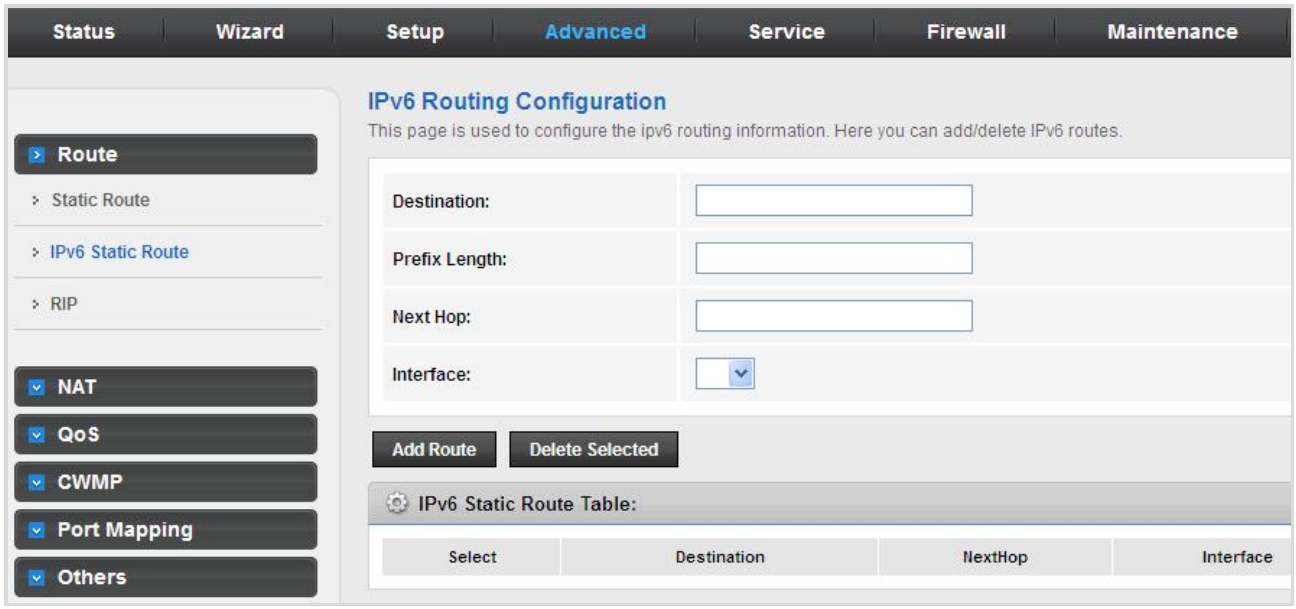


Figure 5-43 IPv6 Static Route

The following table describes the parameters:

Field	Description
Destination	Enter the IPv6 address of the destination device.
Prefix Length	Enter the prefix length of the IPV6 address.
Next Hop	Enter the IPv6 address of the next hop in the IPv6 route to the destination address.
Interface	The interface for the specified route.
Add Route	Click it to add the new static route to the IPv6 Static Route Table.
Delete the Selected	Select a row in the IPv6 Static Route Table and click it to delete the row.

5.4.1.3 RIP

RIP is an Internet protocol you can set up to share routing table information with other routing devices on your LAN, at your ISP's location, or on remote networks connected to your network via the fiber. Most small home or office networks do not need to use RIP; they have only one router, such as the VDSL2 Router, and one path to an ISP. In these cases, there is no need to share routes, because all Internet data from the network is sent to the same ISP gateway. You may want to configure RIP if any of the following circumstances apply to your network:

- Your home network setup includes an additional router or RIP-enabled PC (other than the VDSL2 Router). The VDSL2 Router and the router will need to communicate via RIP to share their routing tables.
- Your network connects via the fiber to a remote network, such as a corporate network. In order for your LAN to learn the routes used within your corporate network, they should both be configured with RIP.
- Your ISP requests that you run RIP for communication with devices on their network.

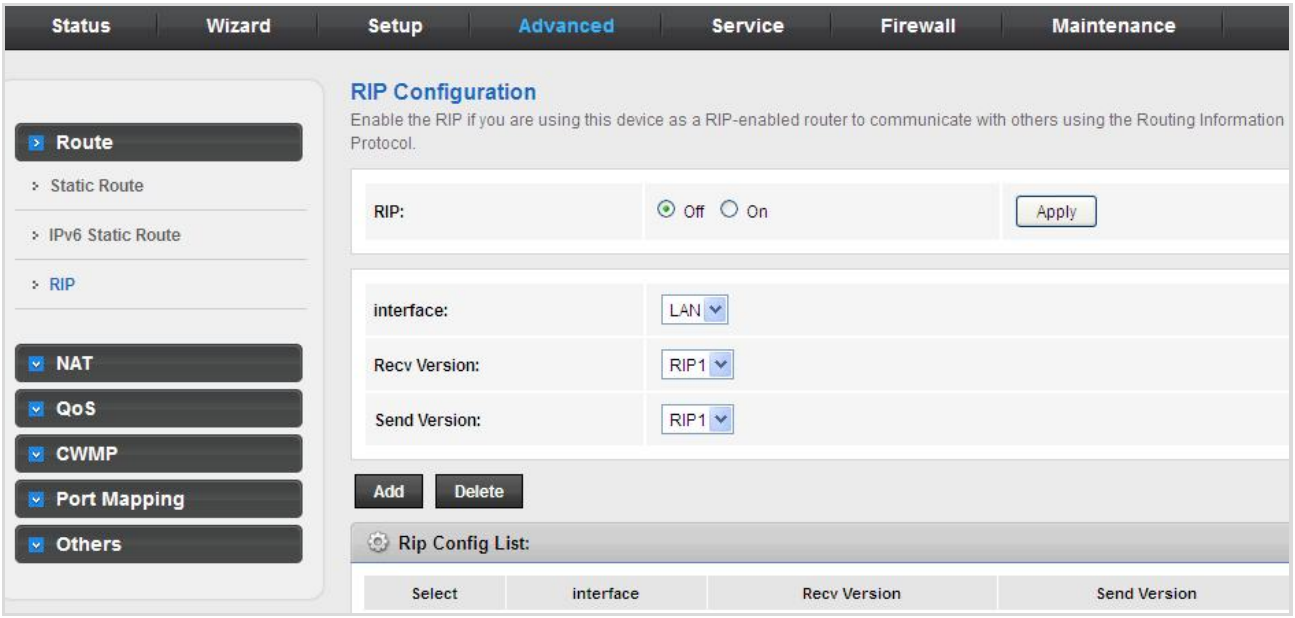


Figure 5-44 RIP

The following table describes the parameters:

Field	Description
RIP	You can select **Off** or **On**.
Apply	Click it to save the settings on this page.
Interface	Choose the router interface that uses RIP.
Recv Version	Choose the interface version that receives RIP messages. You can choose **RIP1**, **RIP2**, or **Both**. ● Choose **RIP1** to indicate the router receives RIP v1 messages. ● Choose **RIP2** to indicate the router receives RIP v2 messages. ● Choose **Both** to indicate the router receives RIP v1 and RIP v2 messages.
Send Version	The working mode for sending RIP messages. You can choose **RIP1** or **RIP2**. ● Choose **RIP1** to indicate the router broadcasts RIP1 messages only. ● Choose **RIP2** to indicate the router multicasts RIP2 messages only.
Add	Click it to add the RIP interface to the **Rip Config List**.
Delete	Select a row in the **Rip Config List** and click it to delete the row.

5.4.2 NAT

Choose **Advanced** > **NAT** and the page shown in the following figure appears. The page displayed contains **DMZ**, **Virtual Server**, **ALG**, **NAT Exclude IP**, **Port Trigger**, **FTP ALG Port**, and **NAT IP Mapping**.

5.4.2.1 DMZ

Demilitarized Zone (DMZ) is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

Click **DMZ** in the left pane and the page shown in the following figure appears. The following describes how to configure manual DMZ. Enter an IP address of the DMZ host. Click **Apply Changes** to save the settings on this page temporarily.

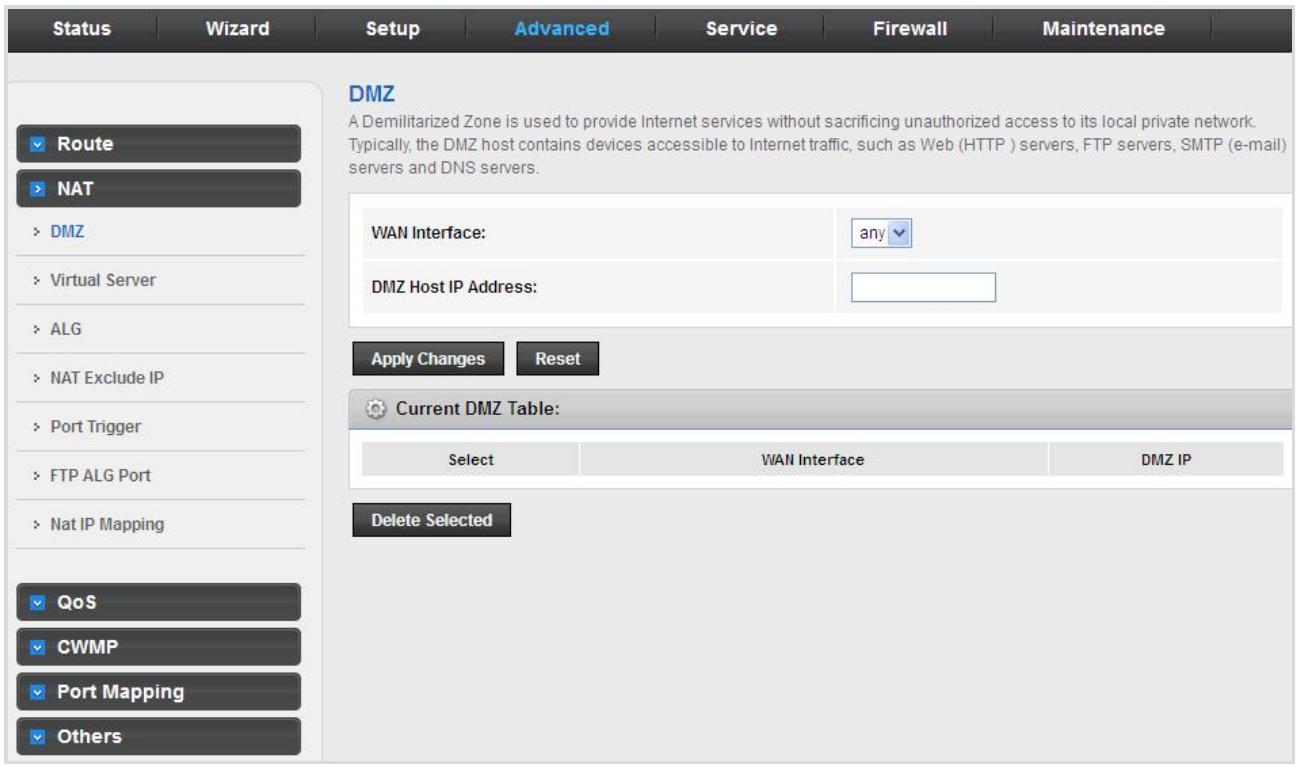


Figure 5-45 DMZ

The following table describes the parameters:

Field	Description
WAN Interface	Choose a WAN Interface.
DMZ Host IP Address	Enter an IP address of the DMZ host.
Current DMZ Table	A list of the previously configured DMZ information.
Apply Changes	Click Apply Changes to add new settings.
Reset	Clear the settings.
Delete the Selected	Select the number of rows from the Current DMZ Table to be deleted.

5.4.2.2 Virtual Server

Internet users would not be able to access a server on your LAN because of native NAT protection.The “virtual server” feature solves these problems and allows internet users to connect to your servers.

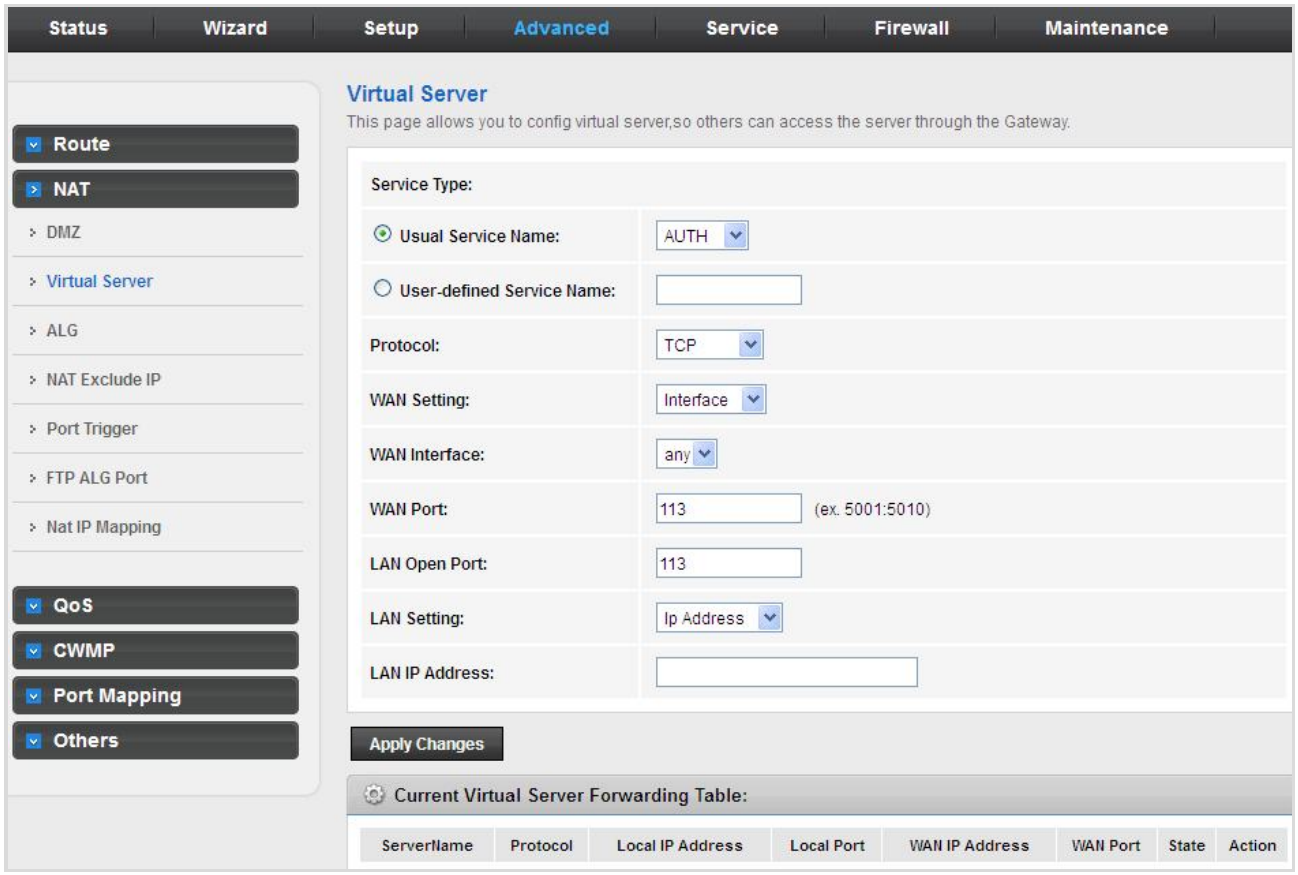


Figure 5-46 Virtual Server

The following table describes the parameters:

Field	Description
Service Type	You can select the common service type, for example, **AUTH**, **DNS** or **FTP**. You can also define a service name. ● If you select **Usual Service Name**, the corresponding parameter has the default settings. ● If you select **User-defined Service Name**, you need to enter the corresponding parameters.
Protocol	Choose the transport layer protocol that the service type uses. You can choose **TCP**, **UDP** or **TCP+UDP**.
WAN Setting	You can choose **Interface** or **IP Address**.
WAN Interface	Choose the WAN interface that will apply virtual server.
WAN Port	Choose the access port on the WAN.
LAN Open Port	Enter the port number of the specified service type.

LAN Setting	You can choose **IP Address**, **Hostname** or **MAC Address**.
LAN IP Address	Enter the IP address of the virtual server. It is in the same network segment with LAN IP address of the router.

5.4.2.3 ALG

An application layer gateway (ALG) is a feature that enables the gateway to parse application layer payloads and take decisions on them. ALG is typically employed to support applications that use the application layer payload to communicate the dynamic Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) ports on which the applications open data connections. Such applications include the File Transfer Protocol (FTP) and various IP telephony protocols.

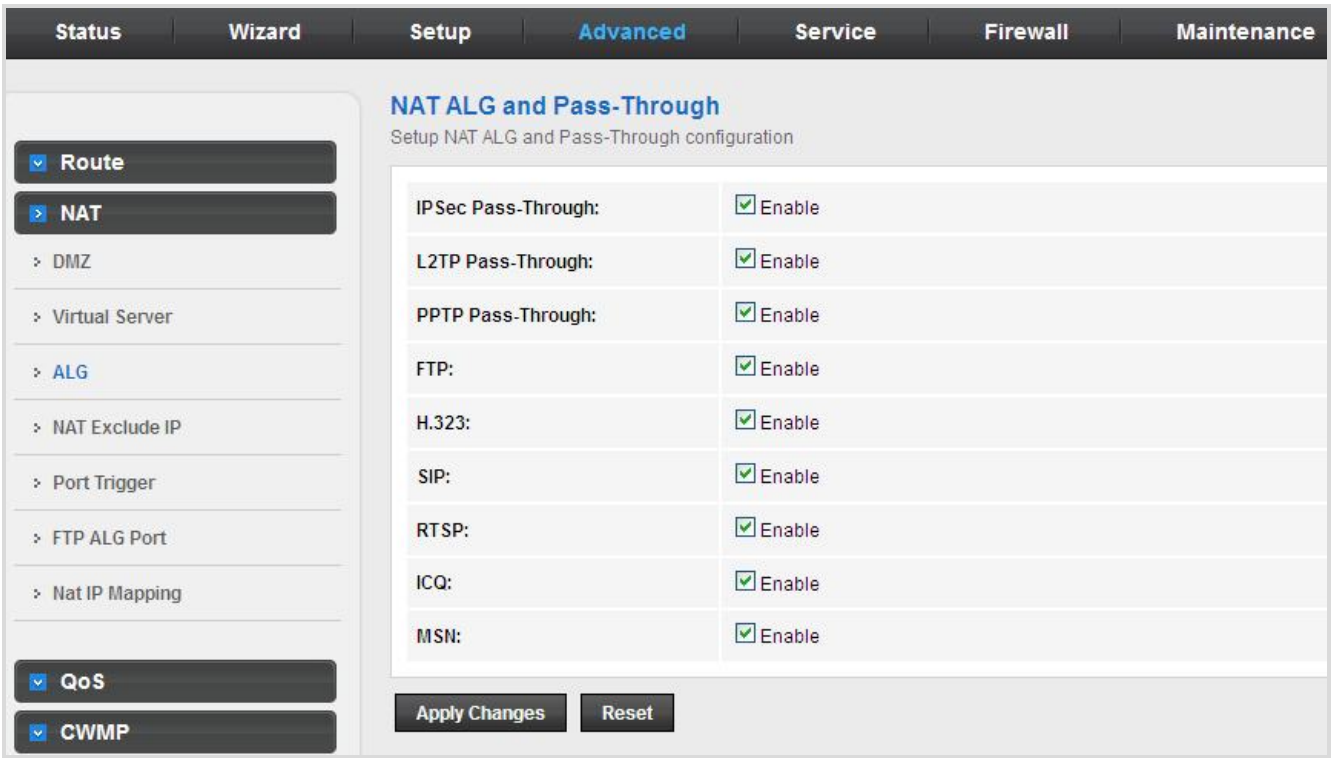


Figure 5-47 ALG

5.4.2.4 NAT Exclude IP

NAT improves network security in effect by hiding the private network behind one global and visible IP address. NAT address mapping can also be used to link two IP domains via a LAN-to-LAN connection. Network Address Translation (NAT) is the method by which the Router shares the single IP address assigned by your ISP with the other computers on your network. This function should only be used if your ISP assigns you multiple IP addresses or you need NAT disabled for an advanced system configuration. If you have a single IP address and you turn NAT off, the computers on your network will not be able to access the Internet. Other problems may also occur. Turning off NAT will disable your firewall functions.

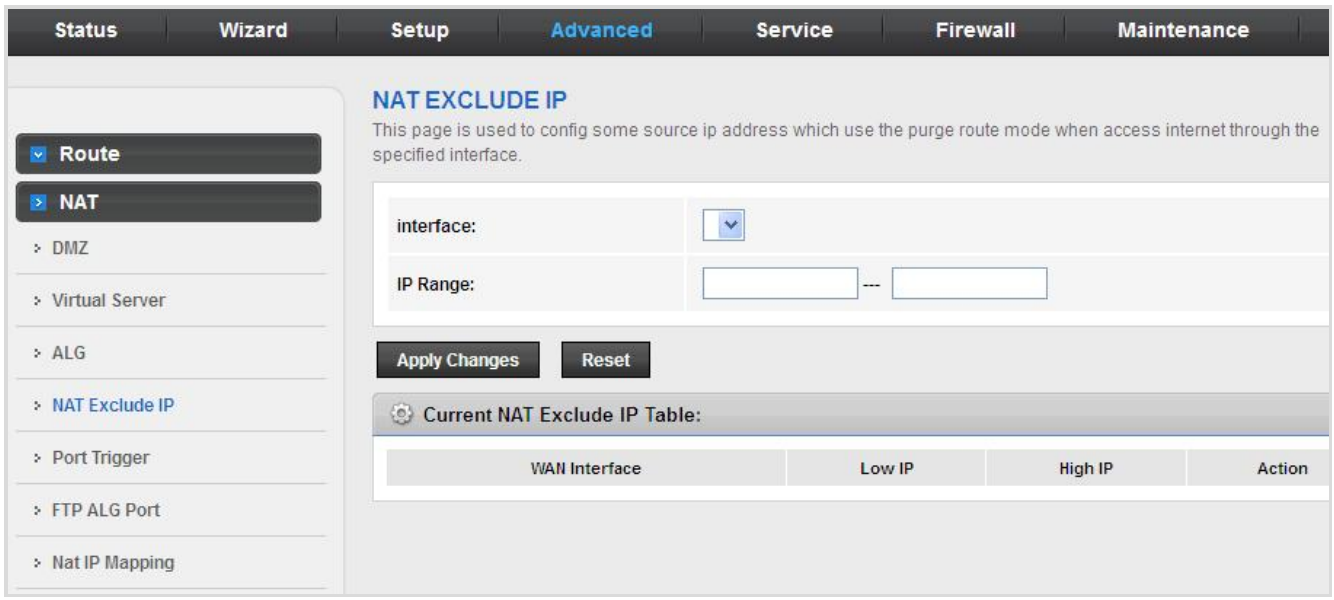


Figure 5-48 NAT Exclude IP

5.4.2.5 Port Trigger

Some applications require multiple connections, like Internet games, video conferencing, Internet calling and so on. These applications cannot work with a pure NAT Router. Port Trigger is used for some of these applications that can work with an NAT Router.

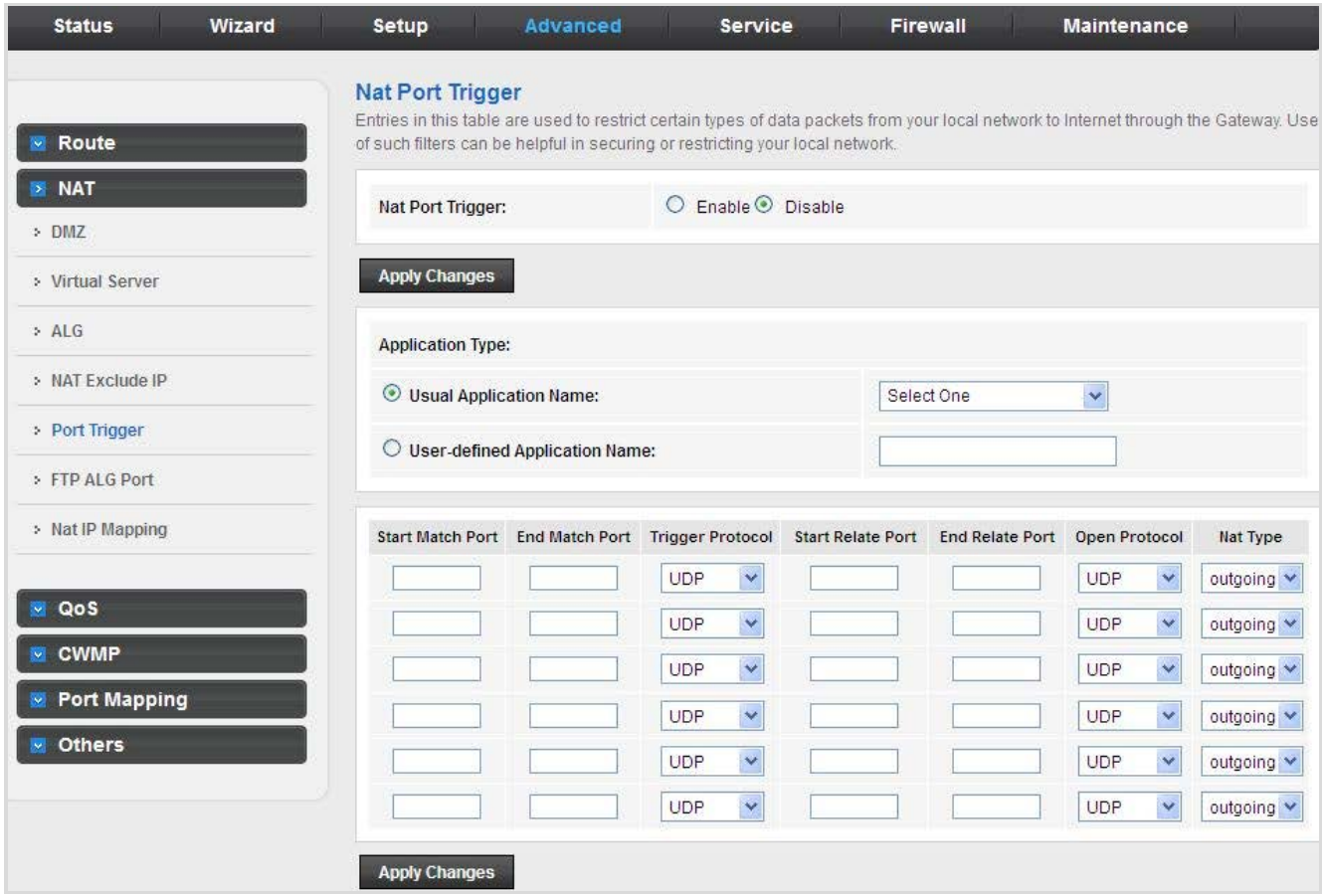


Figure 5-49 Port Trigger

Click the **Usual Application Name** drop-down menu to choose the application you want to set up for port triggering. When you have chosen an application the default Trigger settings will populate the table below.

If the application you want to set up isn't listed, click the **User-defined Application Name** button and type in a name for the trigger in the Custom application field. Configure the **Start Match Port**, **End Match Port**, **Trigger Protocol**, **Start Relate Port**, **End Relate Port**, **Open Protocol** and **Nat Type** settings for the port trigger you want to configure. When it is finished, click the **Apply changes** button.

5.4.2.6 FTP ALG Port

FTP uses two communication channels, one for control commands and one for the actual files being transferred. When an FTP session is opened, the FTP client establishes a TCP connection (the control channel) to (usually) port 21 on the FTP server. What happens after this point depends on the mode of FTP being used.

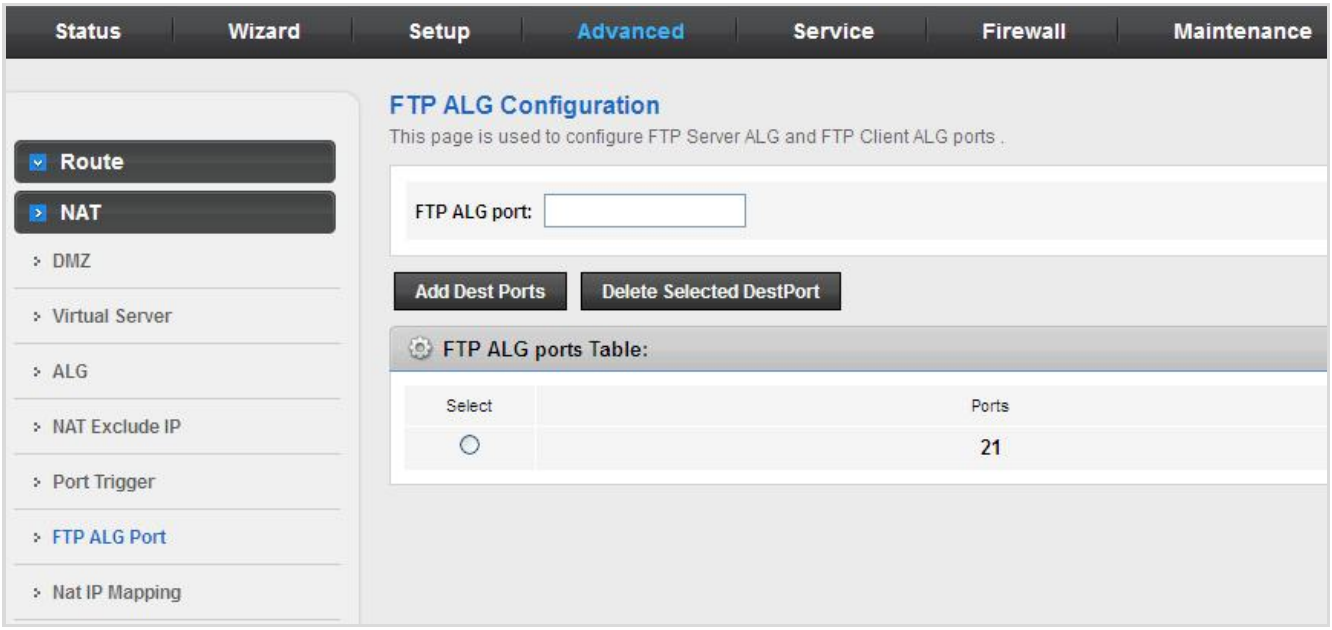


Figure 5-50 FTP ALG Port

The following table describes the parameters:

Field	Description
FTP ALG port	Set an FTP ALG port.
Add Dest Ports	Add a port configuration.
Delete Selected Dest Port	Delete a selected port configuration from the list.

5.4.2.7 NAT IP Mapping

NAT is short for Network Address Translation. The Network Address Translation Settings window allows you to share one WAN IP address for multiple computers on your LAN. Click **NAT IP Mapping** in the left pane and the page shown in the following figure appears.

Entries in this table allow you to configure one IP pool for specified source IP address from LAN, so one packet whose source IP is in range of the specified address will select one IP address from the pool for NAT.

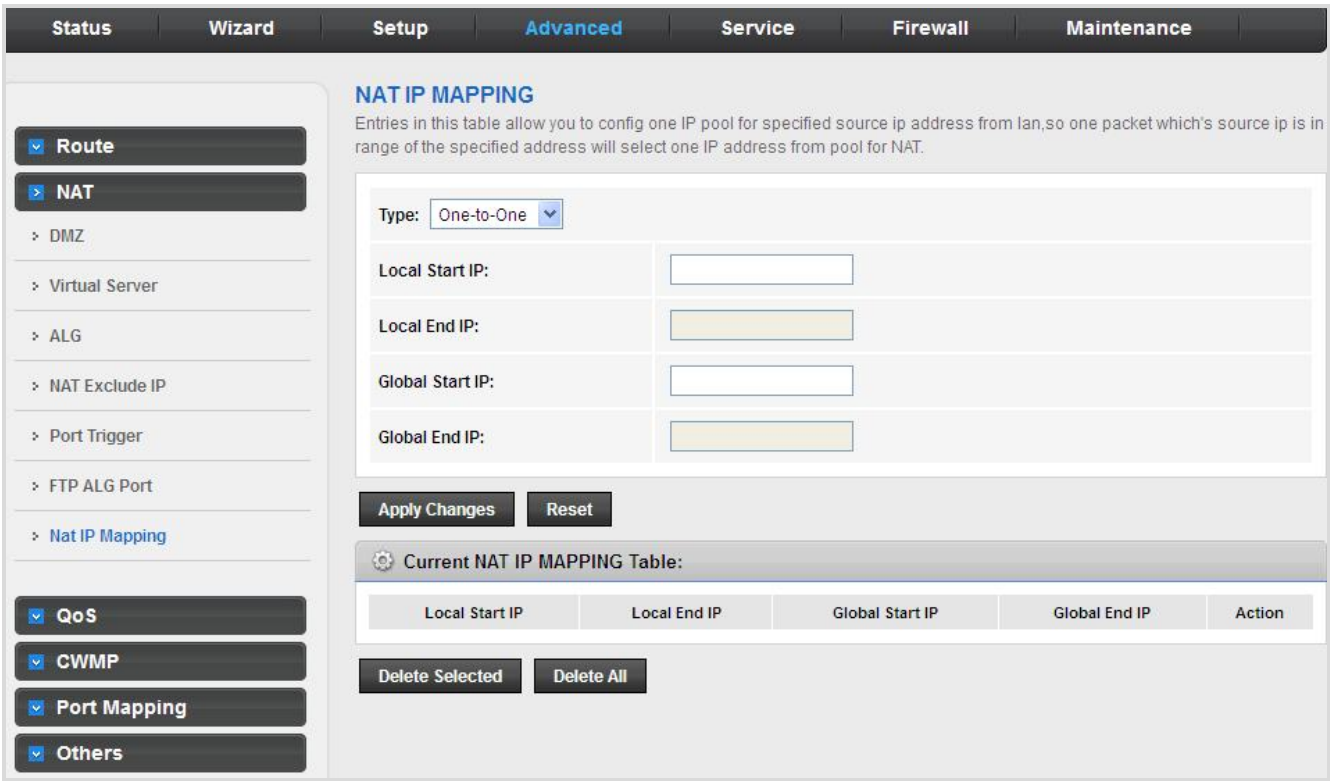


Figure 5-51 NAT IP Mapping

The following table describes the parameters:

Field	Description
Type	There are four types: **One-to-One**, **Many-to-One**, **Many-to-Many** and **One-to-Many**.
Local Start & End IP	Enter the local IP Address you plan to map to. Local Start IP is the starting local IP address and Local End IP is the ending local IP address. If the rule is for all local IPs, then the Start IP is 0.0.0.0 and the End IP is 255.255.255.255
Global Start & End IP	Enter the Globe IP Address you want to do NAT. Global Start IP is the starting global IP address and Global End IP is the ending global IP address. If you have a dynamic IP, enter 0.0.0.0 as the global Start IP.
NAT IP Mapping Table	This displays the information about the Mapping addresses.

5.4.3 QoS

5.4.3.1 QoS

TheVDR-301N provides a control mechanism that can provide a different priority to different users or data flows. The QoS is enforced by the QoS rules in the QoS table. A QoS rule contains two configuration blocks: Traffic Classification and Action. The Traffic Classification enables you to classify packets on the basis of various fields in the packet and perhaps the physical ingress port. The Action enables you to assign the strict priority level and mark some fields in the packet that matches the Traffic Classification rule. You can configure any or all fields as needed in these two QoS blocks for a QoS rule.

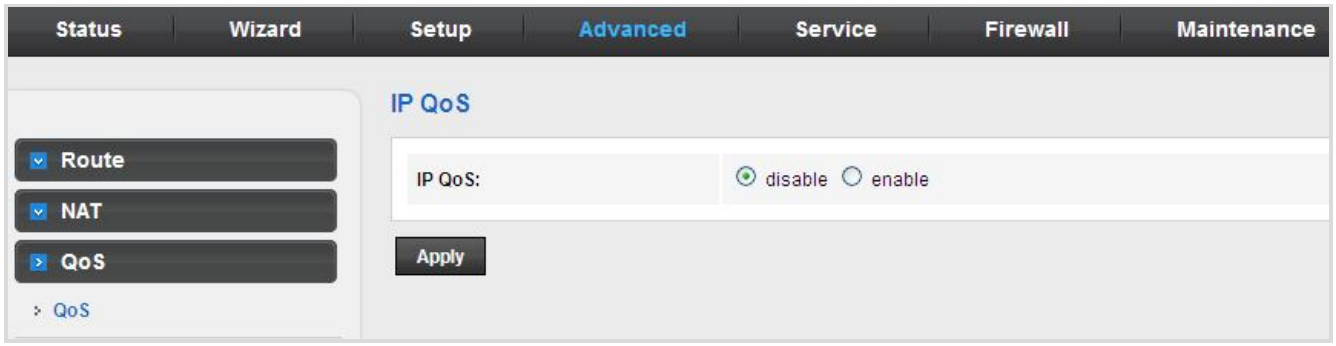


Figure 5-52 QoS Disable

Enable QoS and click **Apply** to enable IP QoS function. Click **Add rule** to add a new IP QoS rule.

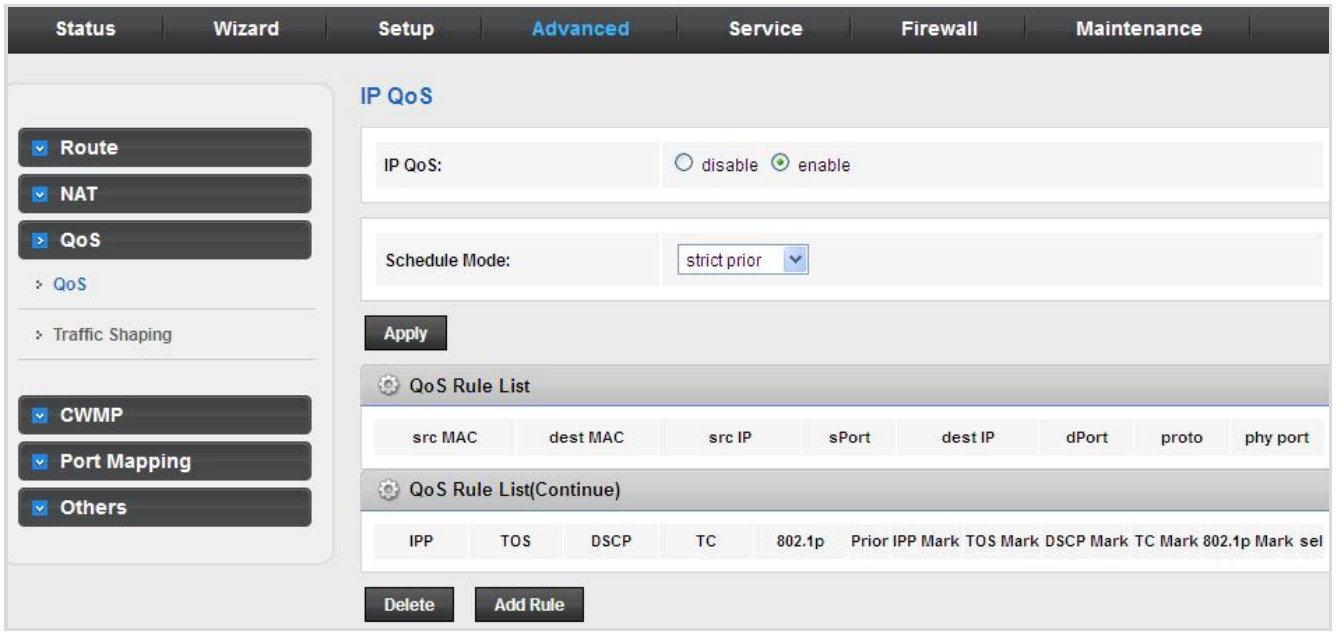


Figure 5-53 QoS Enable

5.4.3.2 Traffic Shaping

Choose **Advanced** > **QoS** > **Traffic Shaping** and the page shown in the following page appears. The traffic shaping function allows you to regulate network data transfer to ensure or prioritize performance by limiting uplink and downlink speeds.

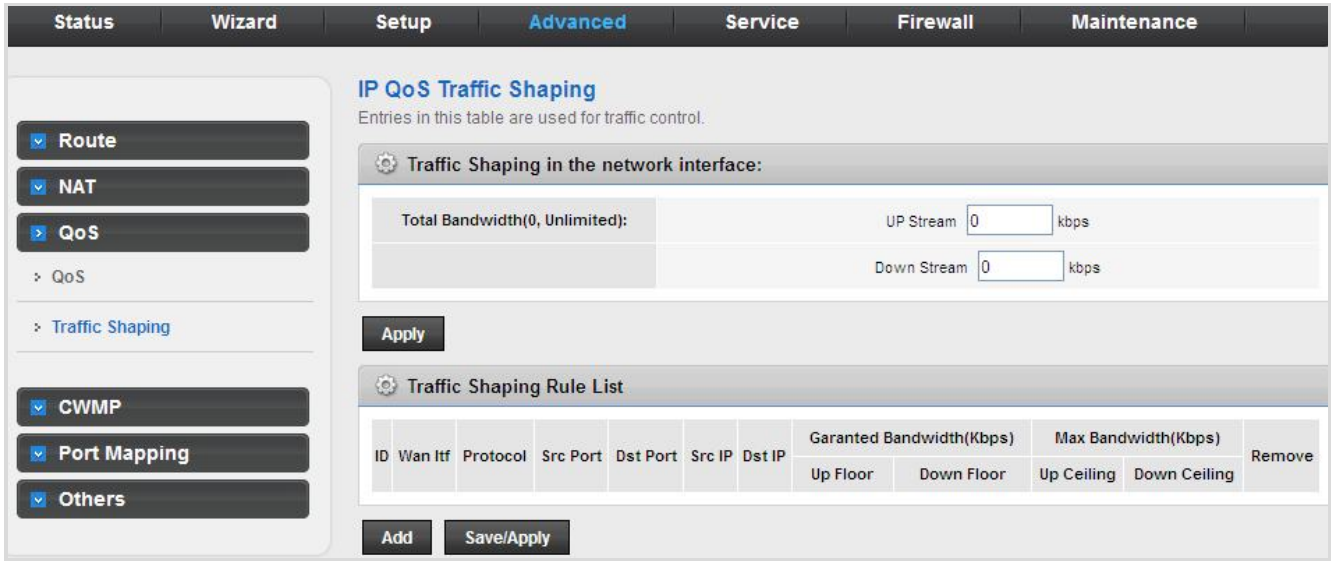


Figure 5-54 Traffic Shaping

5.4.4 CWMP (TR-069)

Choose **Advanced** > **CWMP** and the page shown in the following page appears. On this page, you can configure the TR-069 CPE.

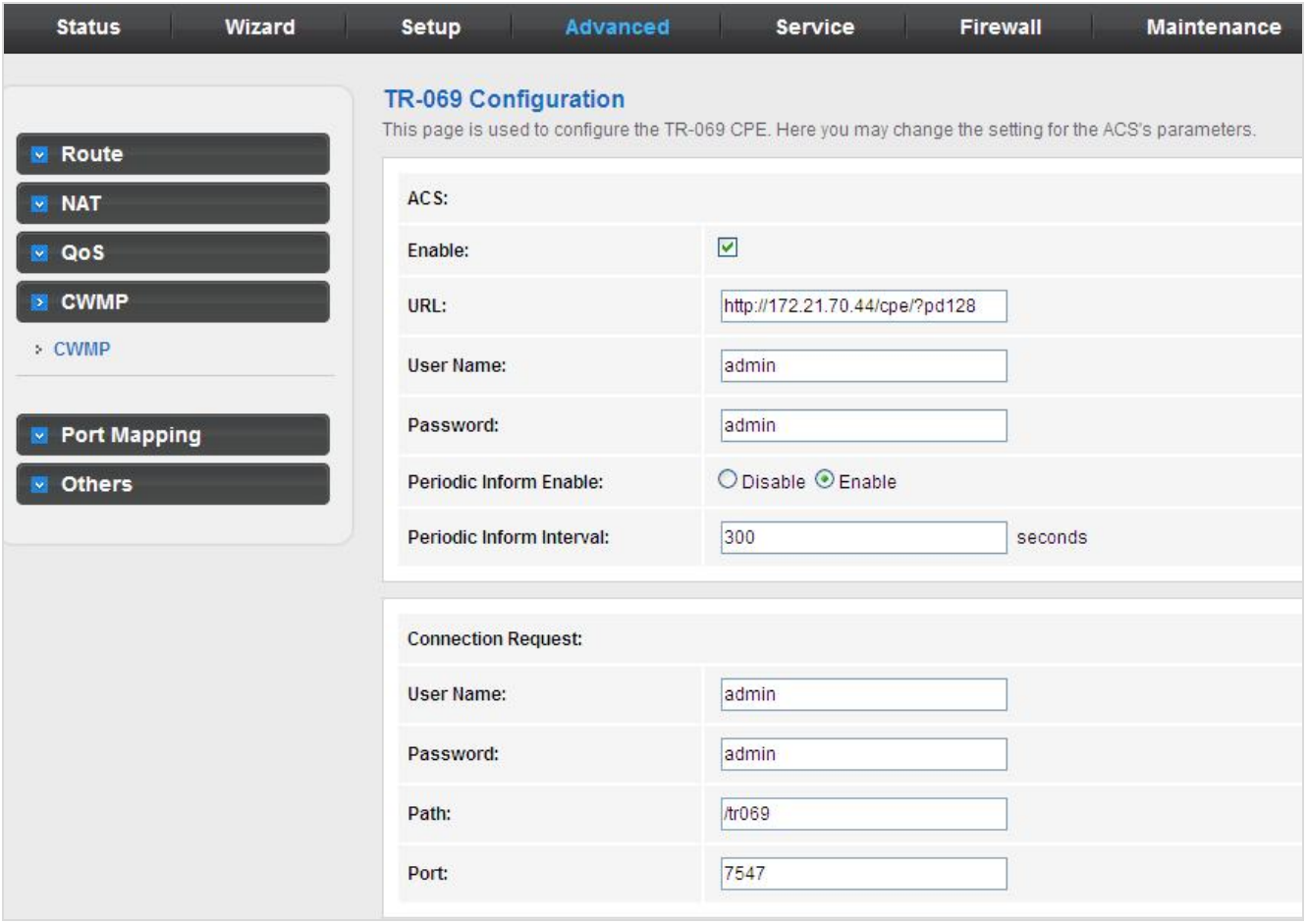


Figure 5-55 CWMP

The following table describes the parameters:

Field	Description
ACS	
Enable	Enable/Disable the function to access.
URL	The URL of the auto-configuration server to connect to.
User Name	The user name for logging in to the ACS.
Password	The password for logging in to the ACS.
Periodic Inform Enable	Select **Enable** to periodically connect to the ACS to check whether the configuration updates.
Periodic Inform Interval	Specify the amount of time between connections to ACS.
Connection Request	

User Name	The connection username provided by TR-069 service.
Password	The connection password provided by TR-069 service.
Debug	
Show Message	Select **Enable** to display ACS SOAP messages on the serial console.
CPE sends GetRPC	Select **Enable** to enable the router to contact the ACS to obtain configuration updates.
Skip MReboot	Specify whether to send an MReboot event code in the inform message.
Delay	Specify whether to start the TR-069 program after a short delay.
Auto-Execution	Specify whether to automatically start the TR-069 after the router is powered on.

5.4.5 Port Mapping

The VDR-301N provides multiple interface groups. Up to five interface groups are supported including one default group. The LAN and WAN interfaces could be included. Traffic coming from one interface of a group can only be flowed to the interfaces in the same interface group. Thus, the VDR-301N can isolate traffic from group to group for some applications. By default, all the interfaces (LAN and WAN) belong to the default group, and the other four groups are all empty. It is possible to assign any interface to any group but only one group.

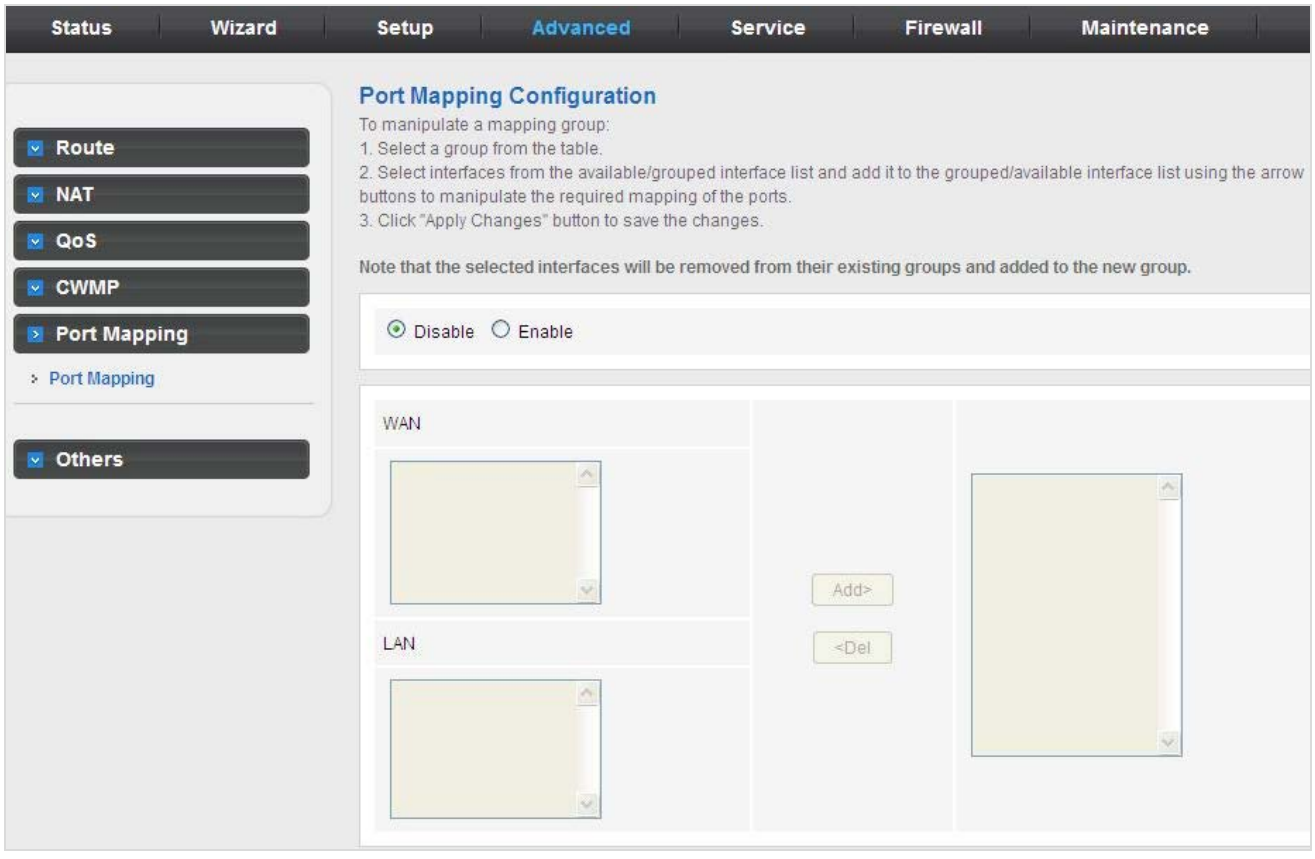


Figure 5-56 Port Mapping

The following table describes the parameters:

Field	Description
Enabled/Disabled	Click the **radio** button to enable/disable the interface group feature. If disabled, all interfaces belong to the default group.
Interface groups	To manipulate a mapping group: 1. Select a group from the table. 2. Select interfaces from the available/grouped interface list and add it to the grouped/available interface list using the arrow buttons to manipulate the required mapping of the ports.

5.4.6 Others

Choose **Advance** > **Others** and the page shown in the following figure appears. The page displayed contains **Bridge Setting**, **Client Limit**, **Tunnel**, Telnet and **Others**.

5.4.6.1 Bridge Setting

Choose **Advance** > **Others** > **Bridge Setting** and the page shown in the following figure appears. This page is used to configure the bridge parameters. You can change the settings or view some information on the bridge and its attached ports.

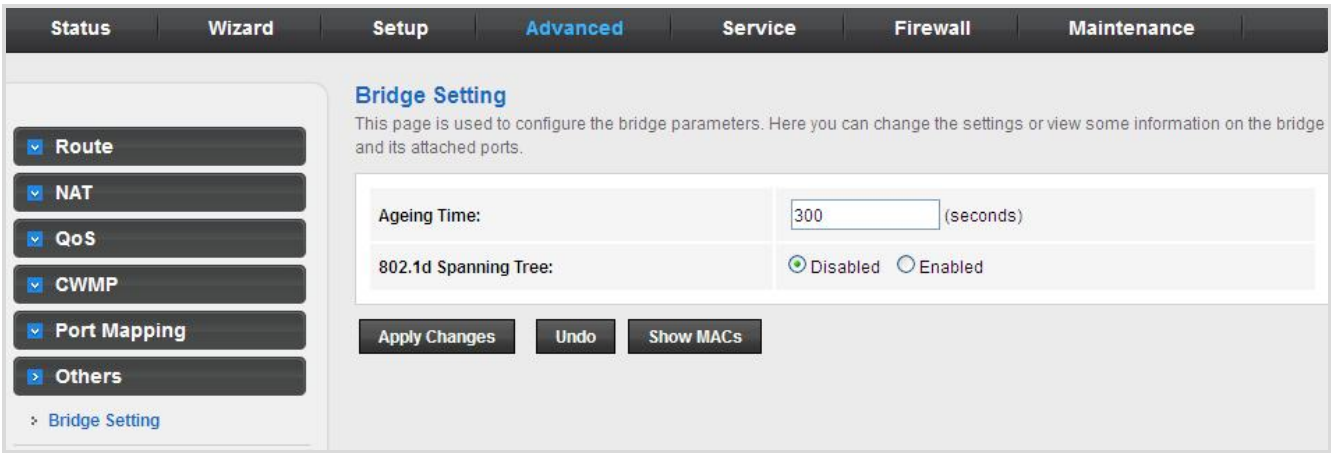


Figure 5-57 Bridge Setting

The following table describes the parameters:

Field	Description
Aging Time	If the host is idle for 300 seconds (default value), its entry is deleted from the bridge table.
802.1d Spanning Tree	You can select **Disable** or **Enable**. Select **Enable** to provide path redundancy while preventing undesirable loops in your network.
Show MACs	Click it to show a list of the learned MAC addresses for the bridge.

Click **Show MACs** and the page shown in the following figure appears. This table shows a list of learned MAC addresses for this bridge.

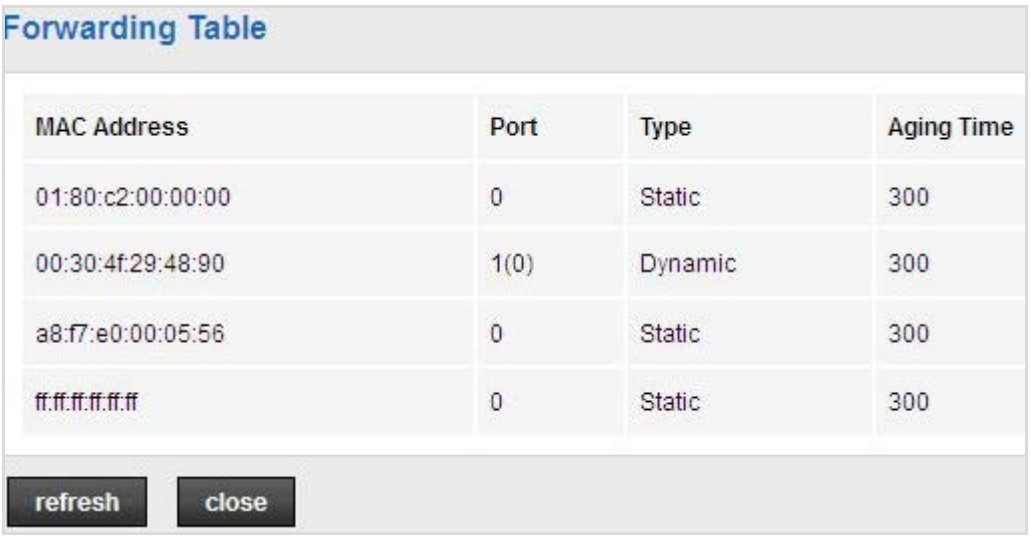


Figure 5-58 Forwarding Table

5.4.6.2 Client Limit

Choose **Advance** > **Others** > **Client Limit** and the page shown in the following figure appears. This page is used to configure the capability of forcing how many devices can access the Internet.

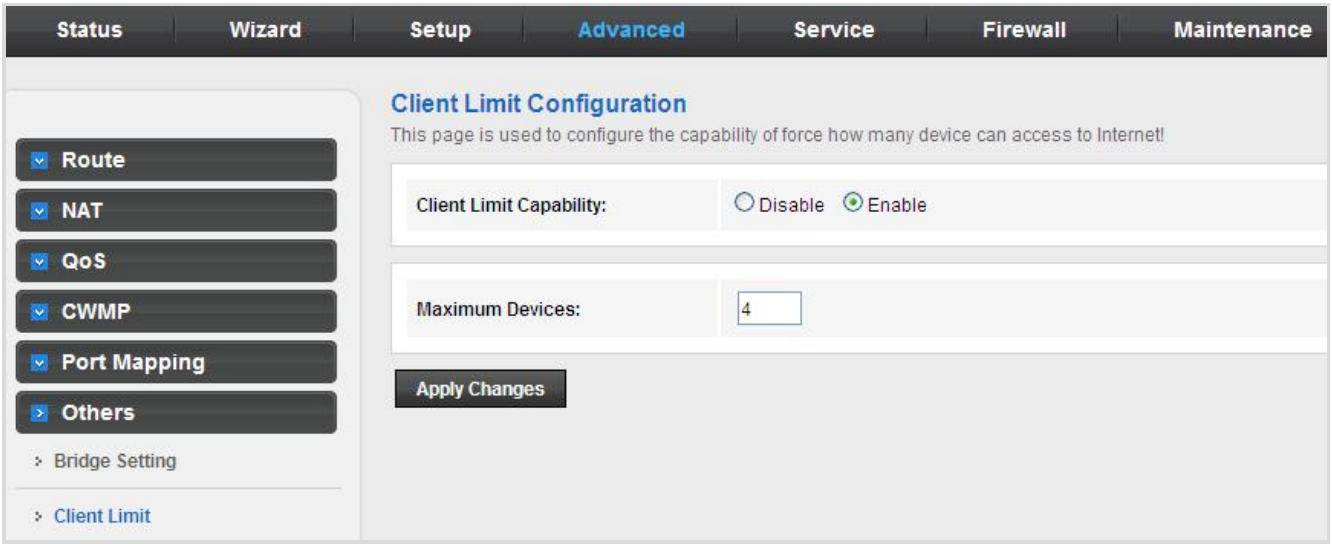


Figure 5-59 Client Limit

The following table describes the parameters:

Field	Description
Client Limit Capability	Enable/Disable the function to access If enabled, maximum devices would be 32; default is 4.

5.4.6.3 Tunnel

Choose **Advanced** > **Others** > **Tunnel** and the page shown in the following figure appears. This page is used to configure the IPv6 with LAN to transfer to IPv4.

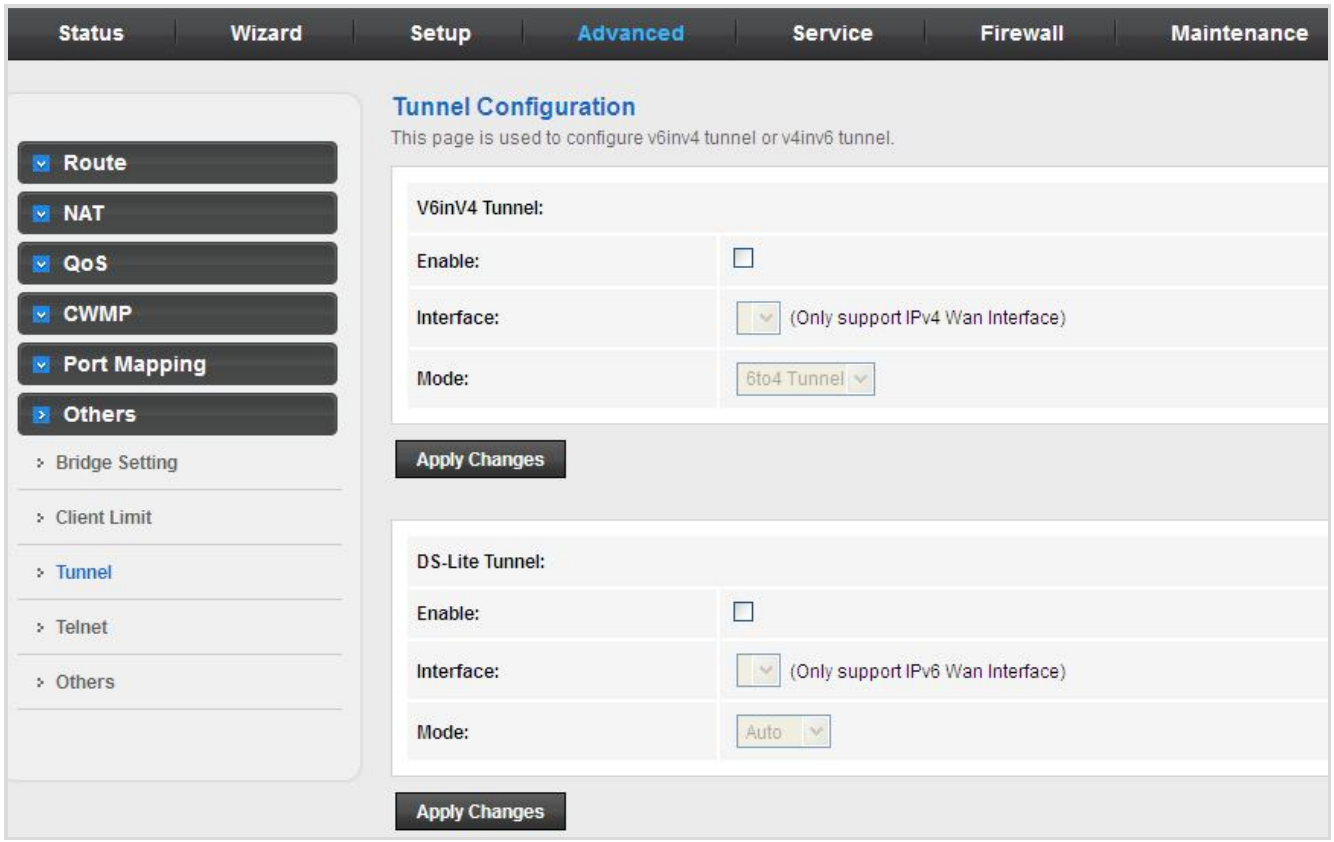


Figure 5-60 Tunnel

The following table describes the parameters:

V6inV4 Tunnel

Field	Description
Enable	Enable or Disable the V6inV4 Tunnel.
Interface	Select the current WAN interface used as tunnel interface.
Mode	**6to4 Tunnel** or **6rd Tunnel**.

DS-Lite Tunnel

Field	Description
Enable	Enable or disable the DS-Lite tunnel.
Interface	Select the current WAN interface used as tunnel interface.
Mode	**Auto** or **Manual**.

5.4.6.4 Telnet

Choose **Advanced > Others > Telnet** in the left pane and the page shown in the following figure appears. You can enable or disable the Telnet function on this page.

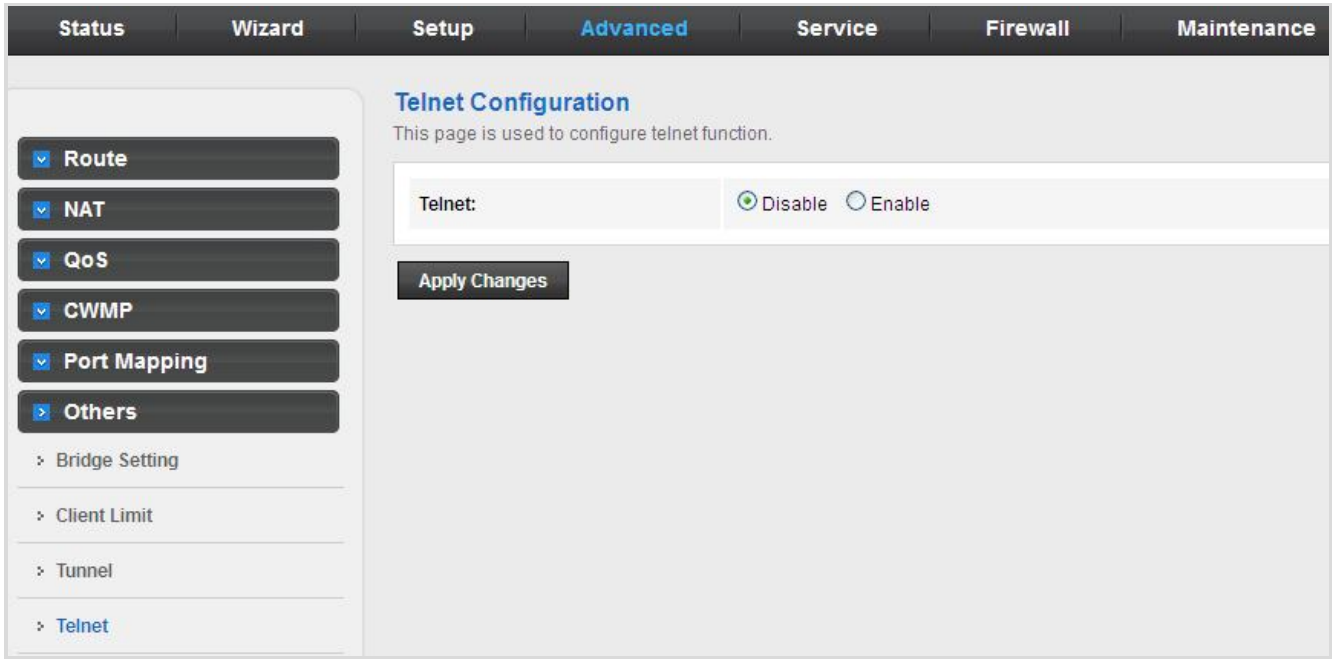


Figure 5-61 Telnet

5.4.6.5 Others

Choose **Advanced > Others > Others** in the left pane and the page shown in the following figure appears. You can enable half bridge so that the PPPoE or PPPoA connection will set to Continuous.

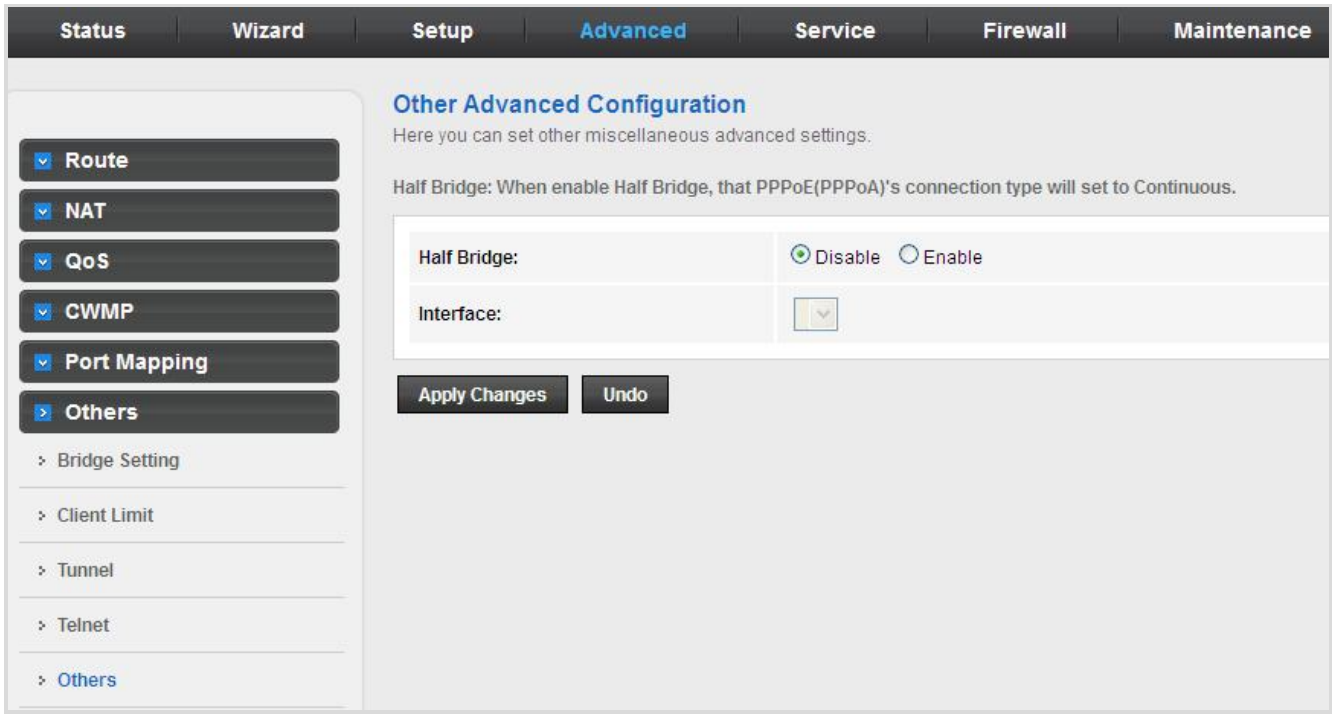


Figure 5-62 Others

5.5 Service

In the navigation bar, click **Service**. On the **Service** page that is displayed contains **IGMP**, **UPnP**, **DNS**, **DDNS** and **VPN**.

5.5.1 IGMP

5.5.1.1 IGMP Proxy

Choose **Service** > **IGMP** and the page shown in the following figure appears. IGMP proxy enables the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces. The system acts as a proxy for its hosts after you enable it.

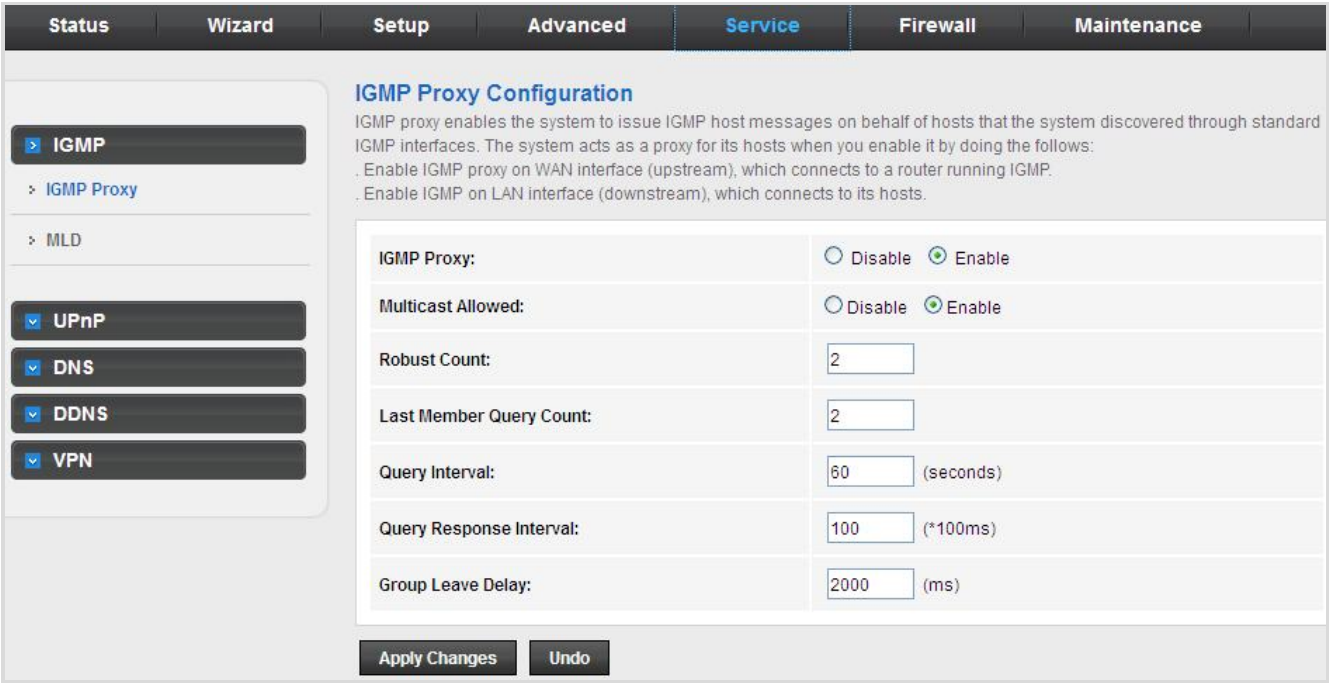


Figure 5-63 IGMP Proxy

The following table describes the parameters:

Field	Description
IGMP Proxy	The Internet Group Management Protocol**.** Enable/Disable the function to access.
Multicast Allowed	Enable/Disable the function to access.
Robust Count	Robust factor of the IGMP Proxy Counter.
Last Member Query Count	The last-member query interval is the maximum amount of time between group-specific query messages, including those sent in response to leave-group messages. You can configure this interval to change the amount of time it takes a routing device to detect the loss of the last member of a group.

Query Interval	The amount of time between IGMP General Query messages sent by the router (if the router is a querier on this subnet).
Query Response Interval	The maximum amount of time in seconds that the IGMP router waits to receive a response to a General Query message. The query response interval is the Maximum Response Time field in the IGMP v2 Host Membership Query message header. The default query response interval is 10 seconds and must be less than the query interval.
Group Leave Delay	The amount of time in seconds that the IGMP router waits to receive a response to a Group-Specific Query message. The last member query interval is also the amount of time in seconds between successive Group-Specific Query messages.

5.5.1.2 MLD

MLD means Multicast Listener Discovery -- its component of the IPv6. MLD is used by IPv6 routers for discovering multicast listeners on a directly-attached link, much like IGMP being used in IPv4.

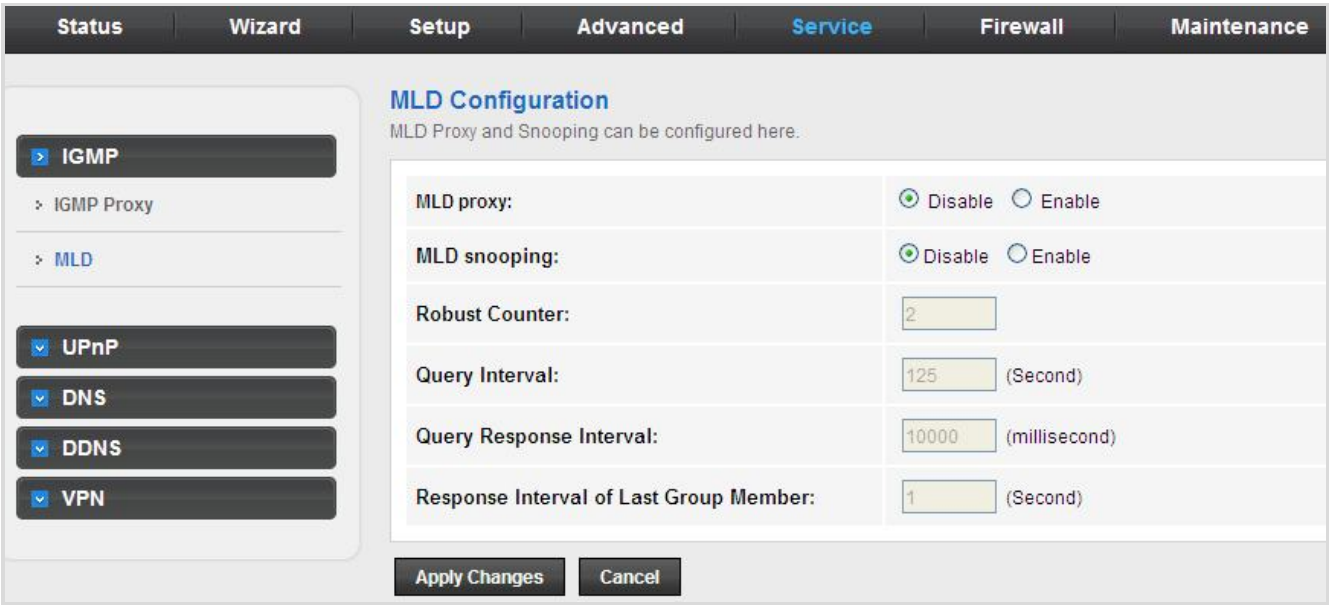


Figure 5-64 MLD

The following table describes the parameters:

Field	Description
MLD Proxy	MLD Proxy can be used to support IPv6 multicast data. Enable/Disable the function to access.
MLD Snooping	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. Multicast Listener Discovery Snooping (MLD). Enable/Disable the

	function to access.
Robust Counter	Robust factor of the MLD Counter.
Query Interval	The amount of time between IGMP General Query messages sent by the router (if the router is a querier on this subnet).
Query Response Interval	The maximum amount of time in seconds that the IGMP router waits to receive a response to a General Query message. The query response interval is the Maximum Response Time field in the IGMP v2 Host Membership Query message header. The default query response interval is 10 seconds and must be less than the query interval.
Response Interval of Last Group Member	The amount of time in seconds that the IGMP router waits to receive a response to a Group-Specific Query message. The last member query interval is also the amount of time in seconds between successive Group-Specific Query messages.

5.5.2 UPnP

Choose **Service** > **UPnP** and the page shown in the following figure appears. This page is used to configure UPnP. The system acts as a daemon after you enable it.

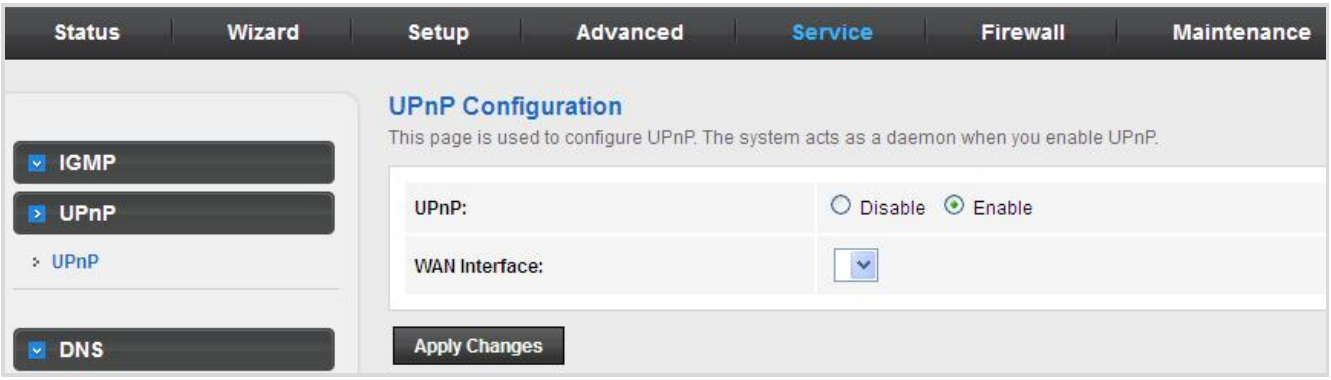


Figure 5-65 UPnP

5.5.3 DNS

Domain Name System (DNS) is an Internet service that translates the domain name into IP address. Because the domain name is alphabetic, it is easier to remember. The Internet, however, is based on IP addresses. Every time you use a domain name, DNS translates the name into the corresponding IP address. For example, the domain name www.example.com might be translated to 198.105.232.4. The DNS has its own network. If one DNS server does not know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

Choose **Service** > **DNS**. The **DNS** page that is displayed contains **DNS** and **IPv6 DNS**.

5.5.3.1 DNS

Click **DNS** in the left pane and the page shown in the following figure appears.

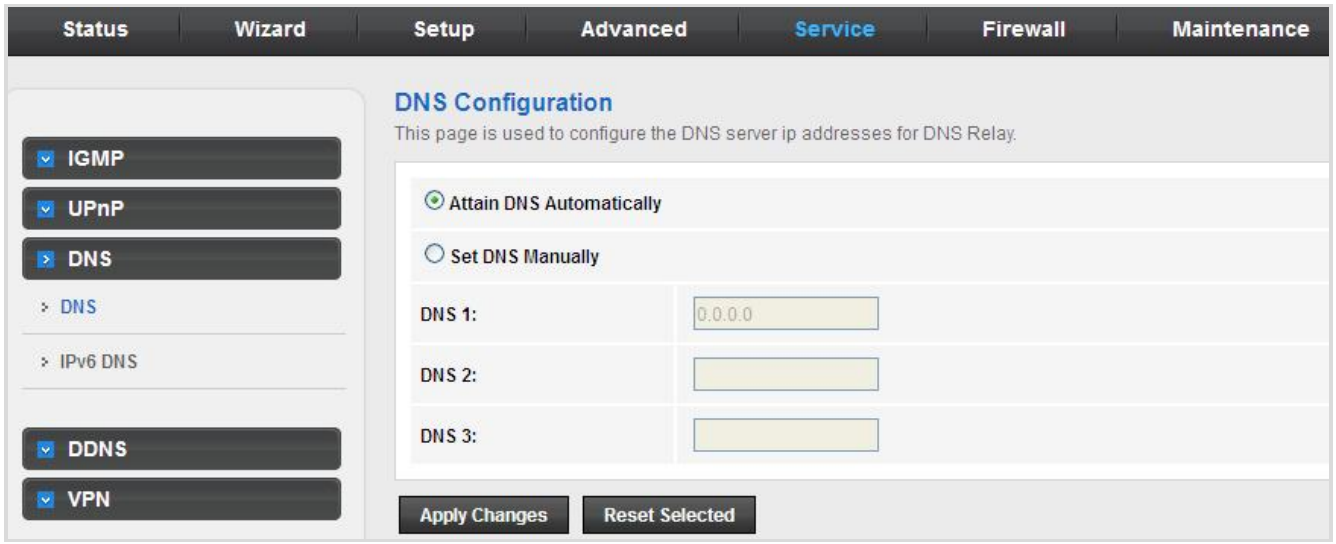


Figure 5-66 DNS

The following table describes the parameters:

Field	Description
Attain DNS Automatically	Select it, and the router accepts the first received DNS assignment from one of the PPPoA, PPPoE or MER enabled PVC(s) during the connection establishment.
Set DNS Manually	Select it to enter the IP addresses of the DNS 1, DNS 2, DNS 3, servers manually.

5.5.3.2 IPv6 DNS

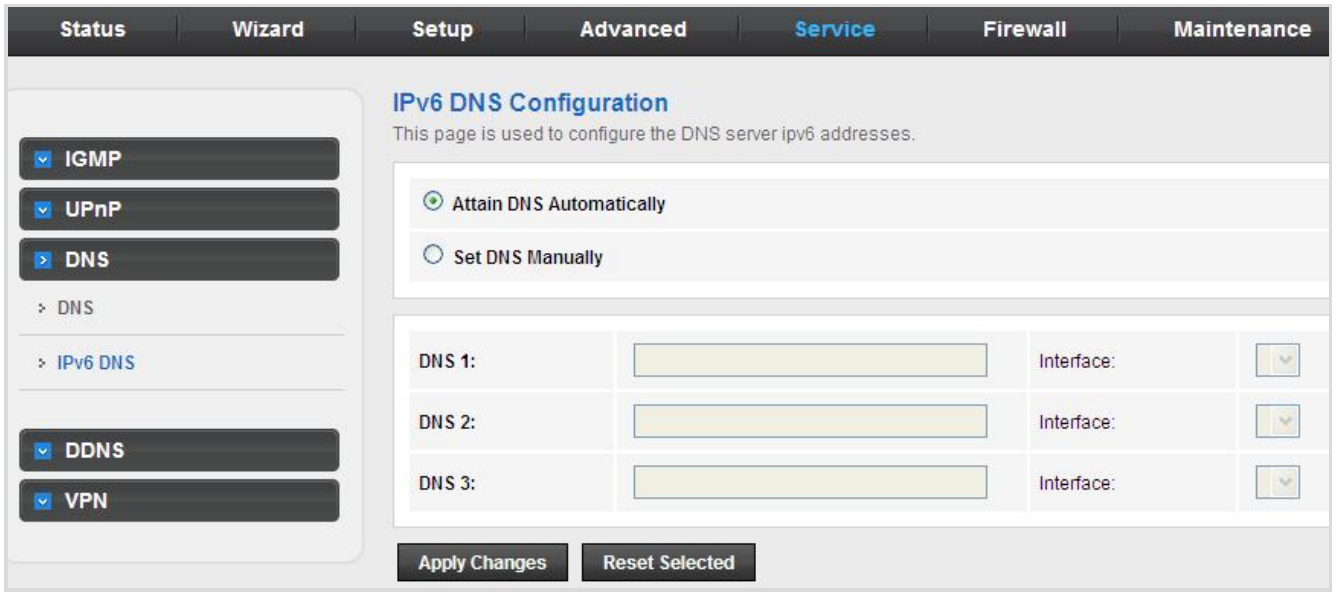


Figure 5-67 IPv6 DNS

The following table describes the parameters:

Field	Description
Attain DNS Automatically	Select it and the router accepts the first received DNS assignment from one of the PPPoA, PPPoE or MER enabled PVC(s) during the connection establishment.
Set DNS Manually	Select it and enter the IP addresses of the primary and secondary DNS server.

5.5.4 DDNS

Click **DDNS** in the left pane and the page shown in the following figure appears. This page is used to configure the dynamic DNS address from DynDNS.org, TZO, PHDNS or PlanetDDNS. You can add or remove to configure dynamic DNS. The Planet DDNS is free for customers

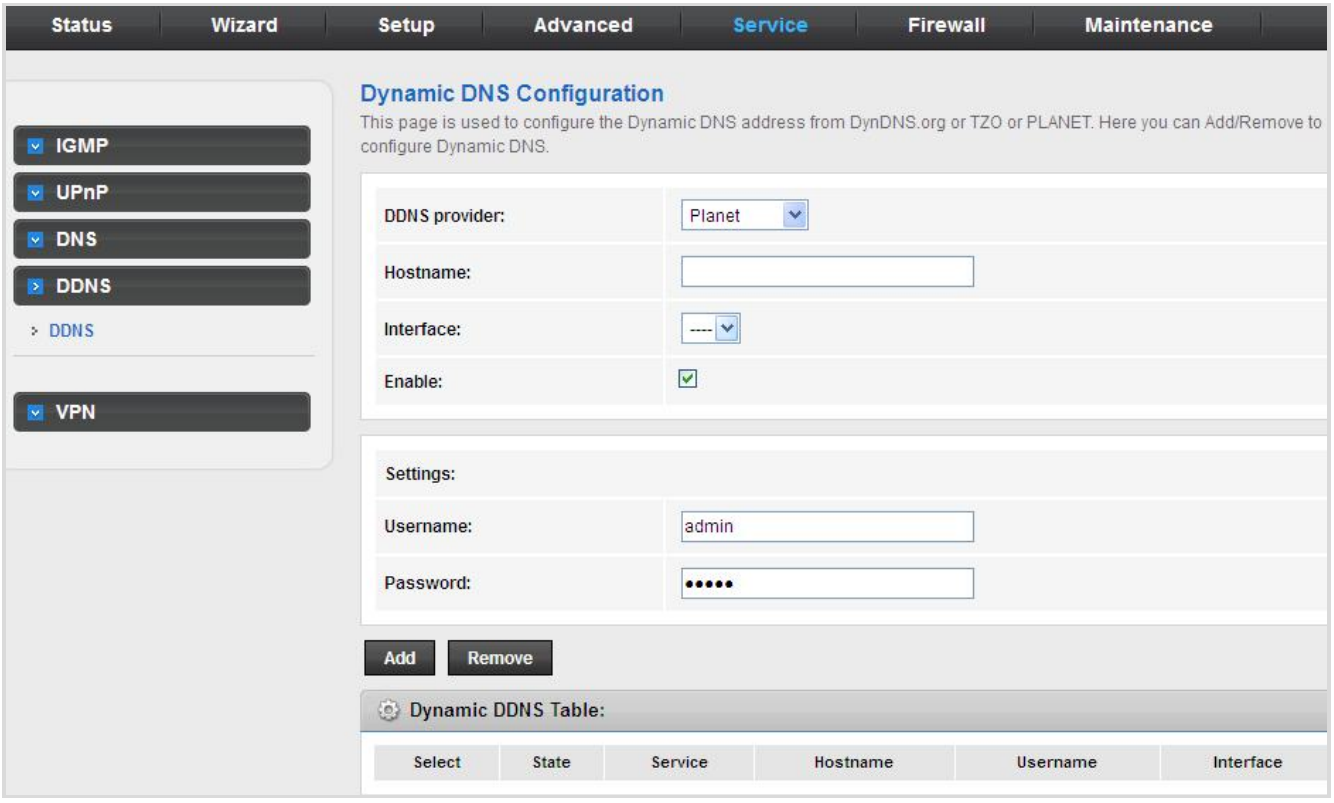


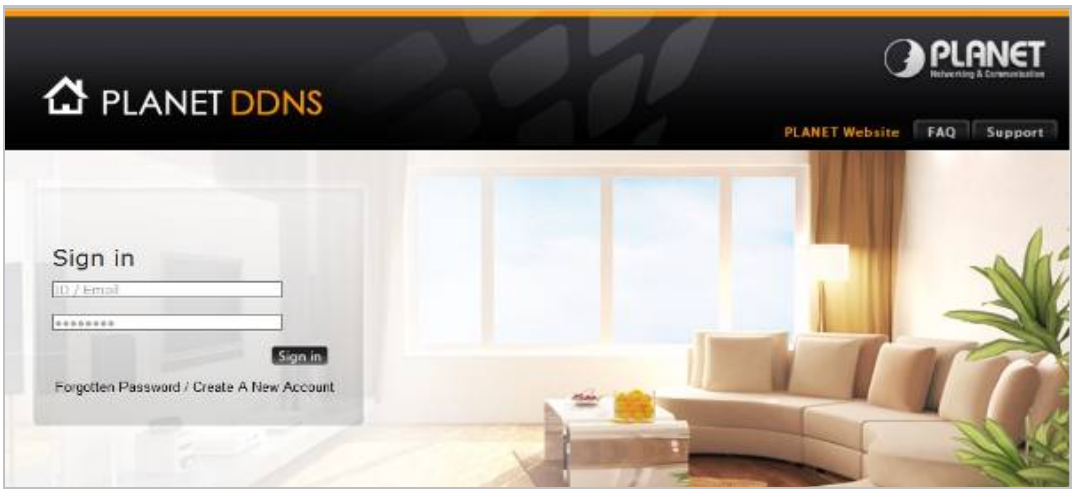
Figure 5-68 DDNS

The following table describes the parameters:

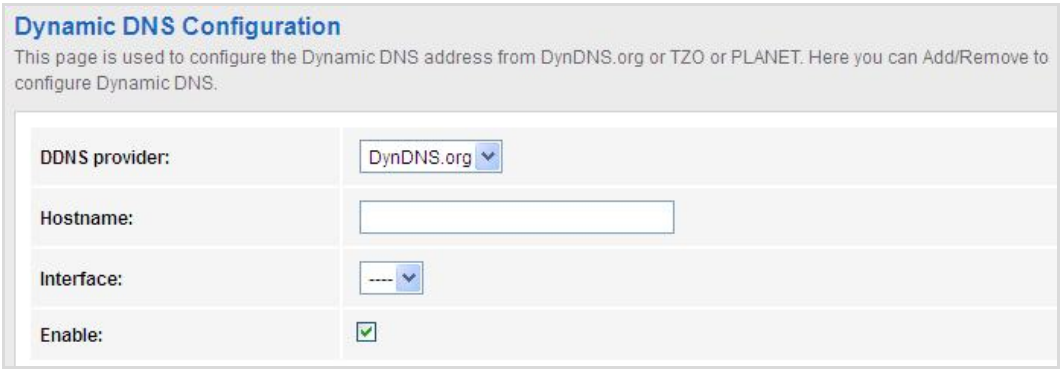
Field	Description
DDNS provider	Choose the DDNS provider name. You can choose DynDNS.org, TZO, PHDNS or Planet.
Host Name	The DDNS identifier.
Interface	The WAN interface of the VDSL2 Router.
Enable	Enable or disable DDNS function.

Username	The name provided by DDNS provider.
Password	The password provided by DDNS provider.

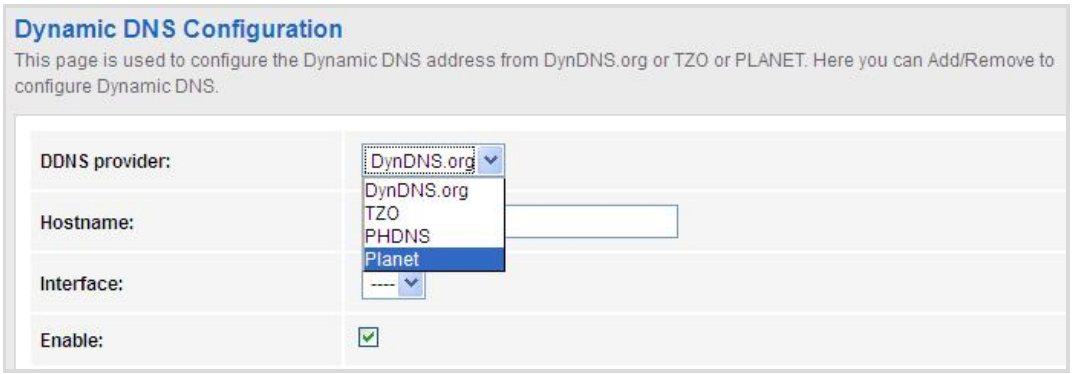
First of all, please go to http://www.planetddns.com to register a Planet DDNS account, and refer to the FAQ (http://www.planetddns.com/index.php/faq) for how to register a free account.



To select **Service > DDNS**



Step 1. Select **Planet DDNS**

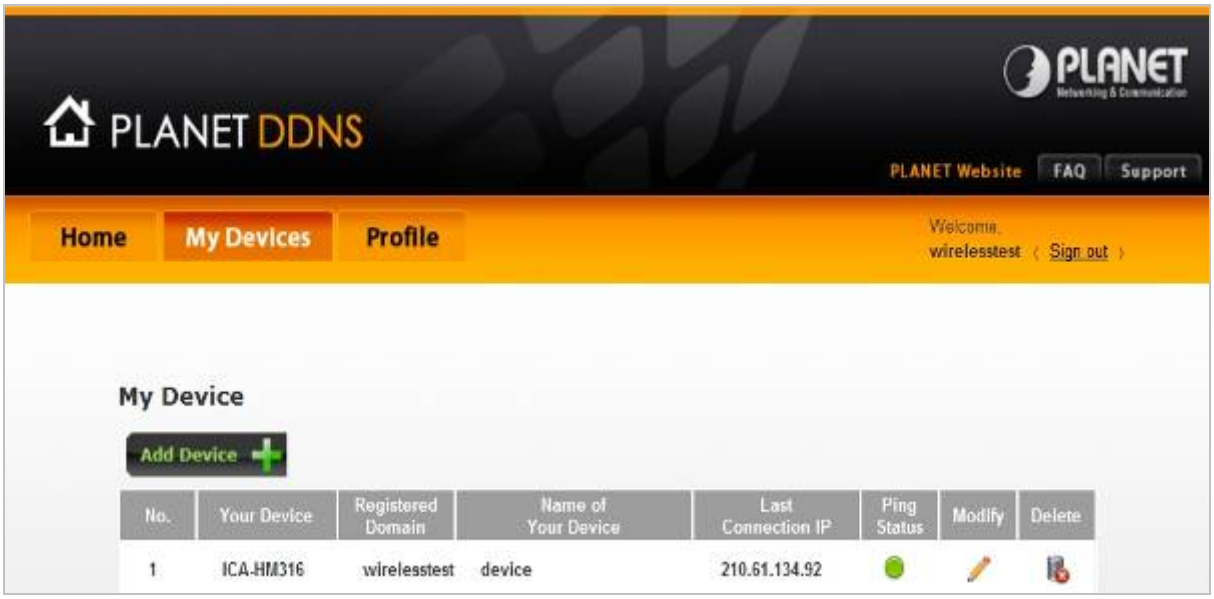


Step 2. Type the User Name for your DDNS account.

Step 3. 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.



5.5.5 VPN

Click **VPN** in the left pane and the page shown in the following figure appears.

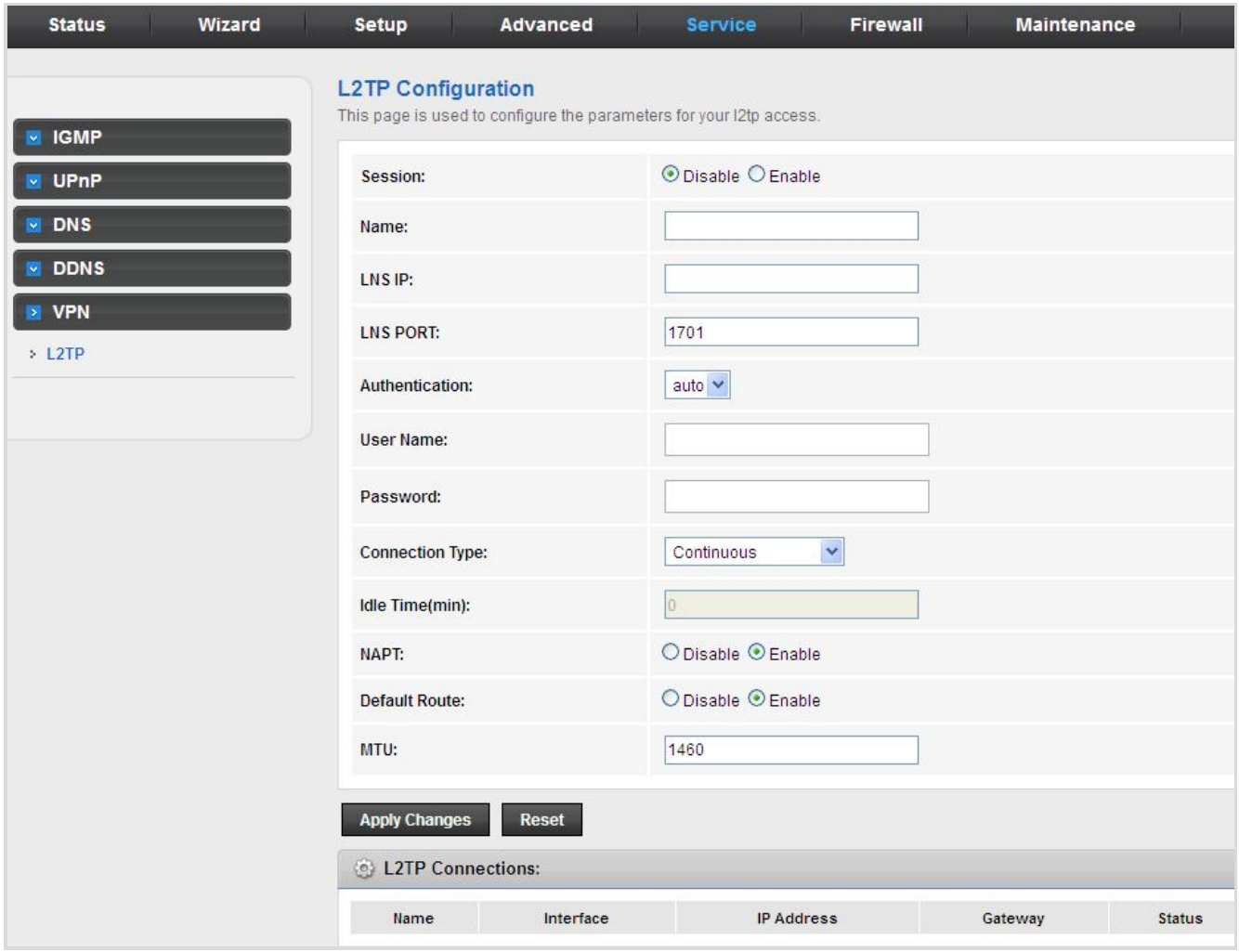


Figure 5-69 VPN

The following table describes the parameters:

Field	Description
Name	Enter the name of the VPN server
LNS IP	Enter the IP of VPN server
Username	Enter the username of VPN server
Password	Enter the password of VPN server
Apply Changes	Press **Apply Changes** to save the setting

5.6 Firewall

Choose **Firewall** and the Firewall page that is displayed contains **MAC Filter**, **IP/Port Filter**, **URL Filter**, **ACL** and **DoS**.

5.6.1 MAC Filter

Click **MAC Filter** in the left pane and the page shown in the following figure appears. Entries in the table are used to restrict certain types of data packets from your local network to Internet through the gateway. These filters are helpful in securing or restricting your local network.

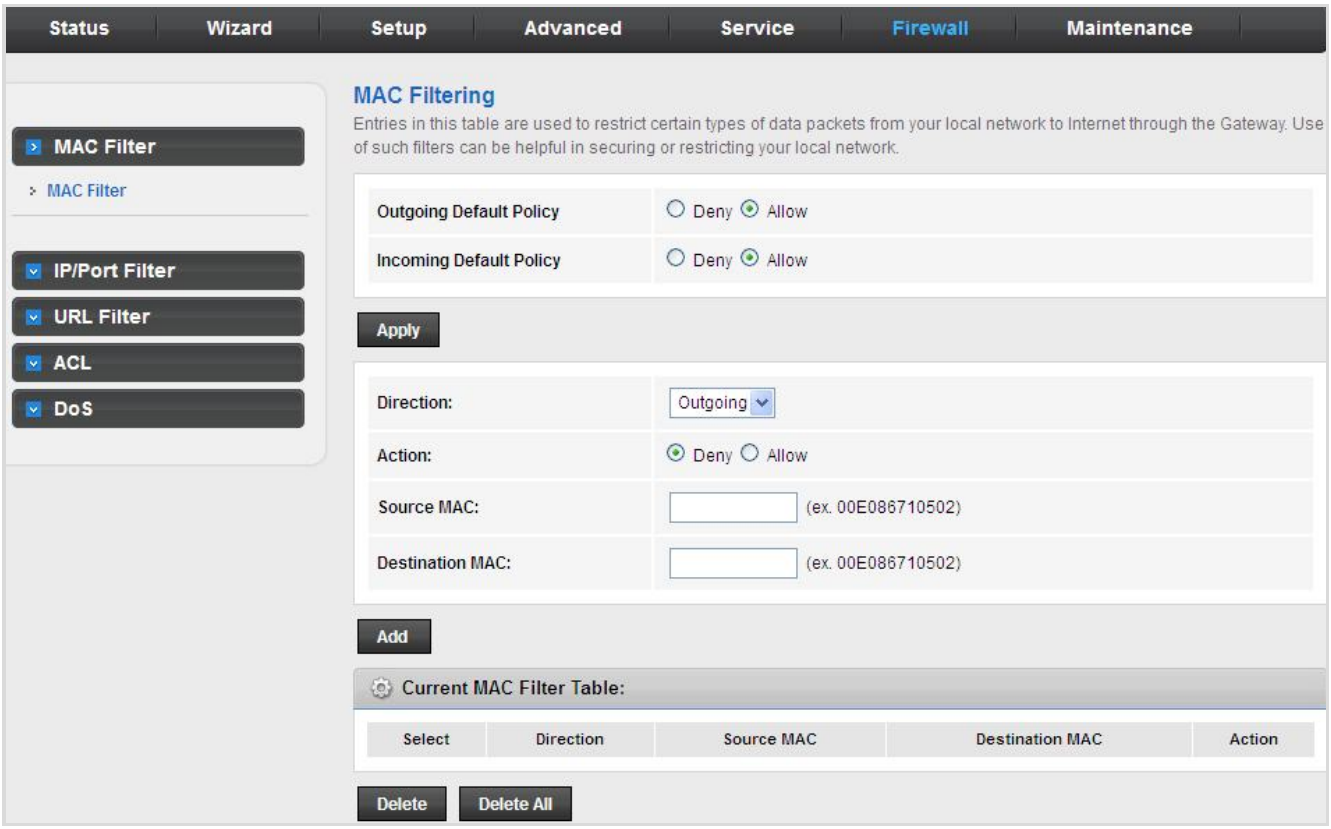


Figure 5-70 MAC Filter

The following table describes the parameters:

Field	Description
Outgoing Default Policy	Specify the default action on the LAN to WAN bridging/forwarding path.
Incoming Default Policy	Specify the default action on the WAN to LAN bridging/forwarding path.
Direction	Traffic **Outgoing**/**Incoming** direction.
Action	Deny or allow traffic when matching this rule.
Source MAC	The source MAC address must be xxxxxxxxxxxx format.
Destination MAC	The destination MAC address must be xxxxxxxxxxxx format.

5.6.2 IP/Port Filter

5.6.2.1 IP/Port Filter

Click **IP/Port Filter** in the left pane and the page shown in the following figure appears. Entries in the table are used to restrict certain types of data packets through the gateway. These filters are helpful in securing or restricting your local network.

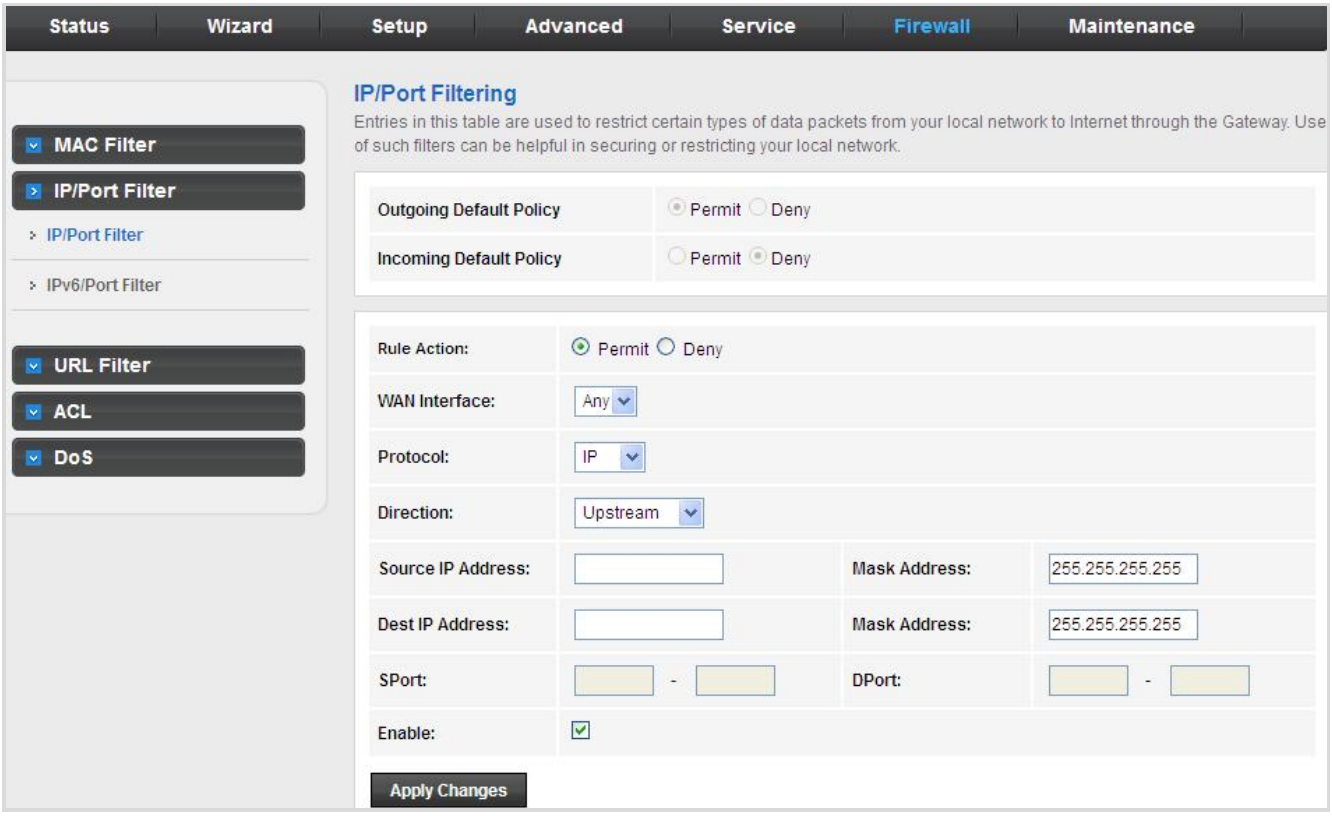


Figure 5-71 IP/Port Filter

The following table describes the parameters:

Field	Description
Rule Action	Permit or deny traffic when matching this rule.
WAN Interface	Select the WAN interface of the VDSL2 Router.
Protocol	There are 4 options available: **IP**, **ICMP**, **TCP**, and **UDP**.
Direction	Traffic forwarding direction.
Source IP Address	The source IP address assigned to the traffic on which filtering is applied.
Mask Address	Subnet-mask of the source IP.
Dest IP Address	The destination IP address assigned to the traffic on which filtering is applied.
Mask Address	Subnet-mask of the destination IP.
S Port	Starting and ending source port numbers.
D Port	Starting and ending destination port numbers.
Enable	Enable/Disable the function to access.

5.6.2.2 IPv6/Port Filter

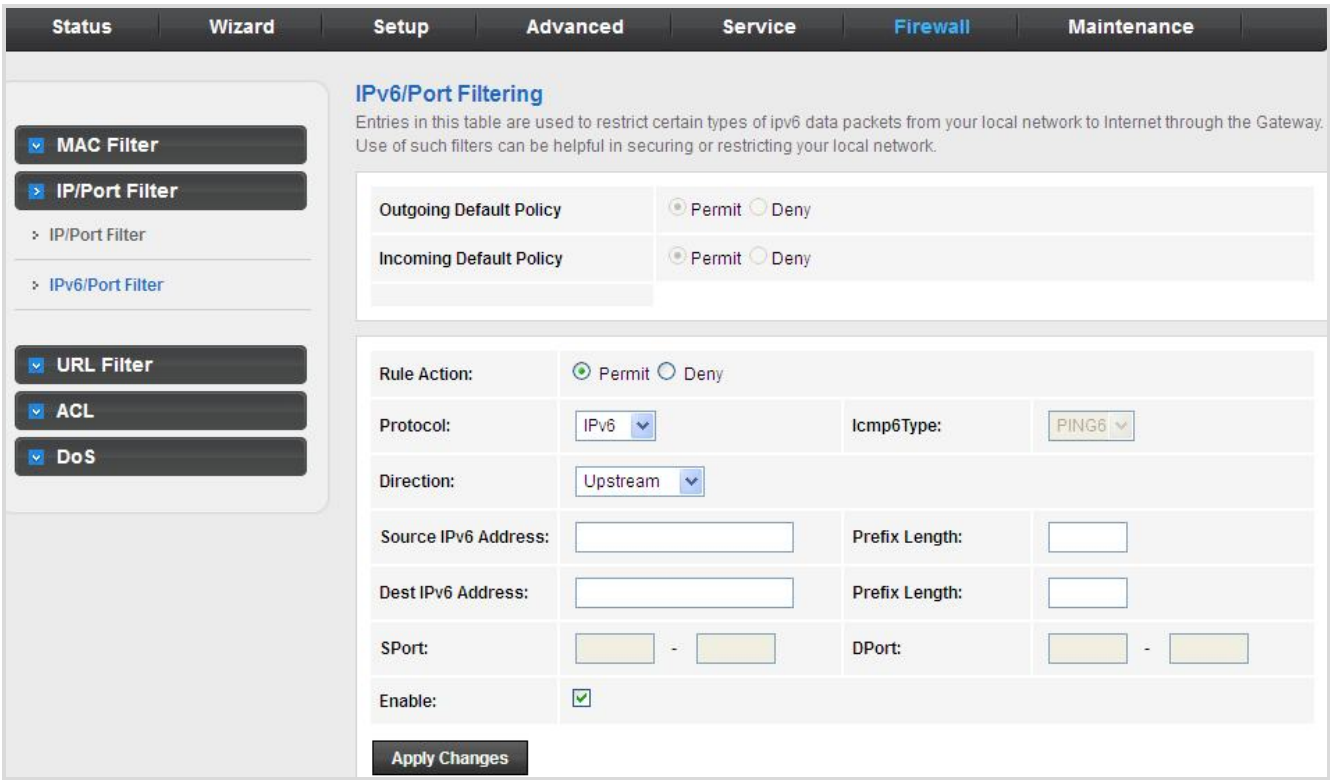


Figure 5-72 IPv6/Port Filter

The following table describes the parameters:

Field	Description
Rule Action	Permit or deny traffic when matching this rule.
Protocol	There are 4 options available: **IPv6**, **ICMP6**, **TCP**, and **UDP**.
ICMP6 Type	Select the PING6 type.
Direction	Traffic forwarding direction.
Source IPv6 Address	The source IP address assigned to the traffic on which filtering is applied.
Prefix Length	Subnet-mask of the source IP.
Dest IPv6 Address	The destination IP address assigned to the traffic on which filtering is applied.
Prefix Length	Subnet-mask of the destination IP.
S Port	Starting and ending source port numbers.
D Port	Starting and ending destination port numbers.
Enable	Enable/Disable the function to access.

5.6.3 URL Filter

Click **URL Filter** in the left pane and the page shown in the following figure appears. This page is used to block a fully qualified domain name, such as tw.yahoo.com and filtered keyword (yahoo). You can add or delete fully qualified domain name and filtered keyword.

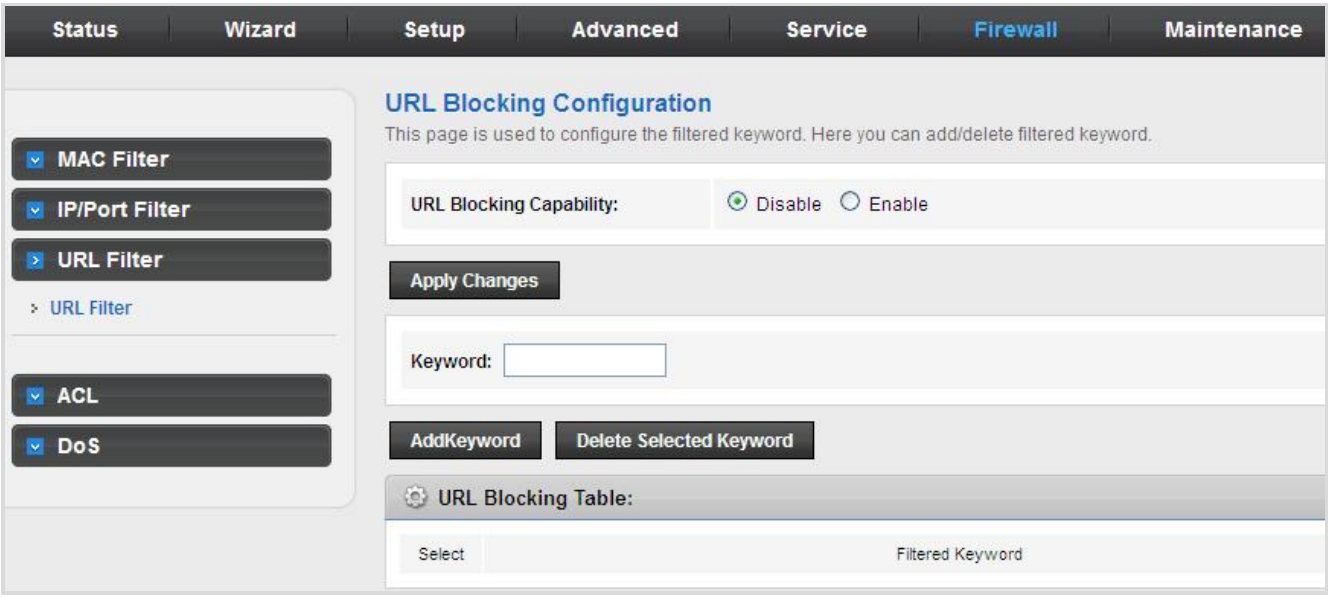


Figure 5-73 URL Filter

The following table describes the parameters:

Field	Description
URL Blocking Capability	You can choose **Disable** or **Enable**. ● Select **Disable** to disable URL blocking and keyword filtering function. ● Select **Enable** to block access to the URLs and keywords specified in the **URL Blocking Table**.
Keyword	Enter the keyword to block.
Add Keyword	Click it to add a URL/keyword to the **URL Blocking Table**.
Delete Selected Keyword	Select a row in the **URL Blocking Table** and click it to delete the row.
URL Blocking Table	A list of the URLs to which access is blocked.

5.6.4 ACL

5.6.4.1 ACL

Choose **Service** > **ACL** and the page shown in the following figure appears. On this page, you can permit the data packets from LAN or WAN to access the router. You can configure the IP address for Access Control List (ACL). If ACL is enabled, only the effective IP address in the ACL can access the router.

> **Note**
>
> If you select **Enable** in ACL capability, ensure that your host IP address is in ACL list before it takes effect.

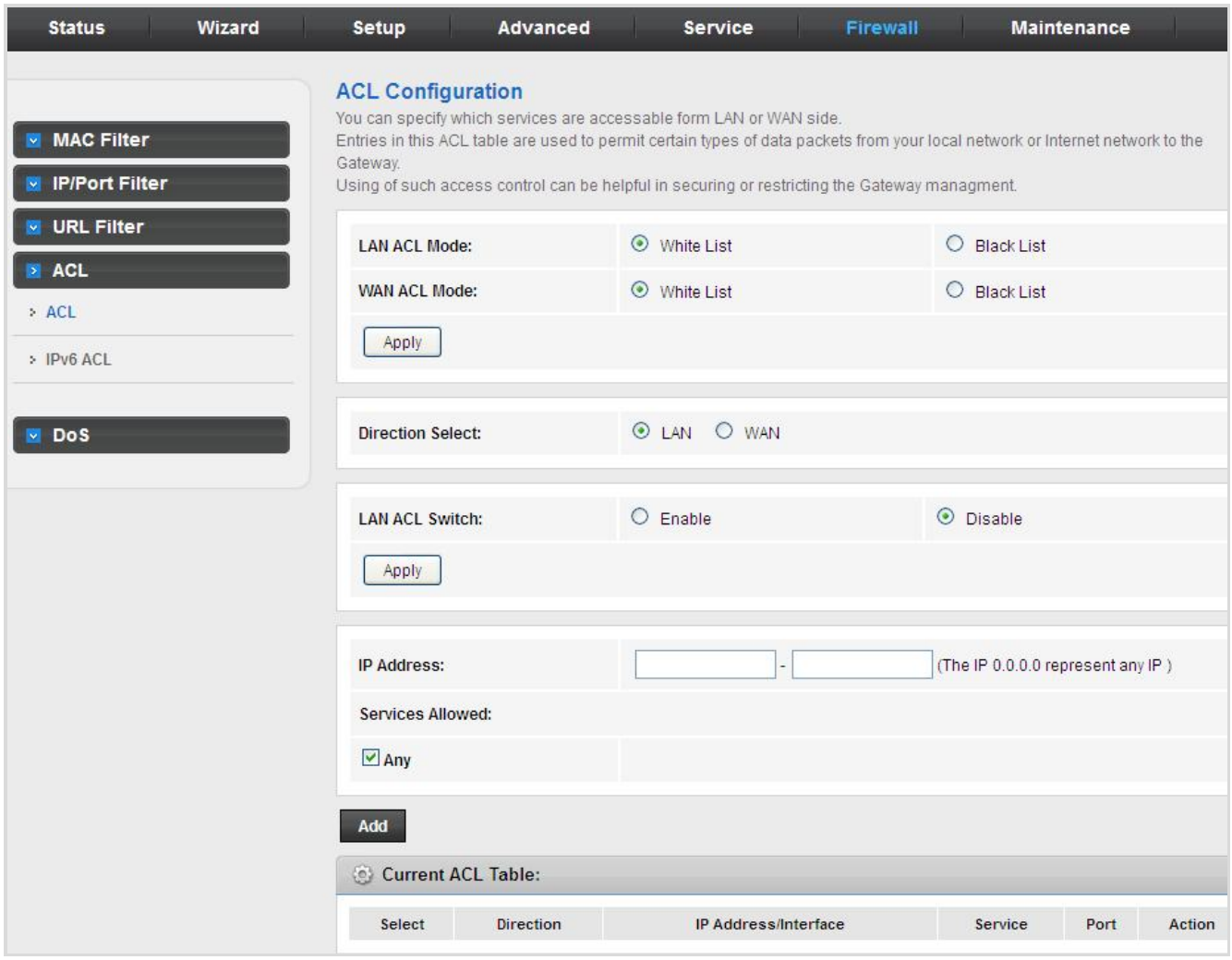


Figure 5-74 ACL

The following table describes the parameters:

Field	Description
Direction Select	Select the router interface. You can select **LAN** or **WAN**. In this example, **LAN** is selected.
LAN ACL Switch	Select it to enable or disable ACL function.
IP Address	Enter the IP address of the specified interface. Only the IP address that is in the same network segment with the IP address of the specified interface can access the router.
Services Allowed	You can choose the following services from LAN: **Web**, **Telnet**, **SSH**, **FTP**, **TFTP** or **PING**. You can also choose all the services.
Add	After setting the parameters, click it to add an entry to the **Current ACL Table**.

If **WAN** is selected in the field of **Direction Select**, the page is shown in the following figure.

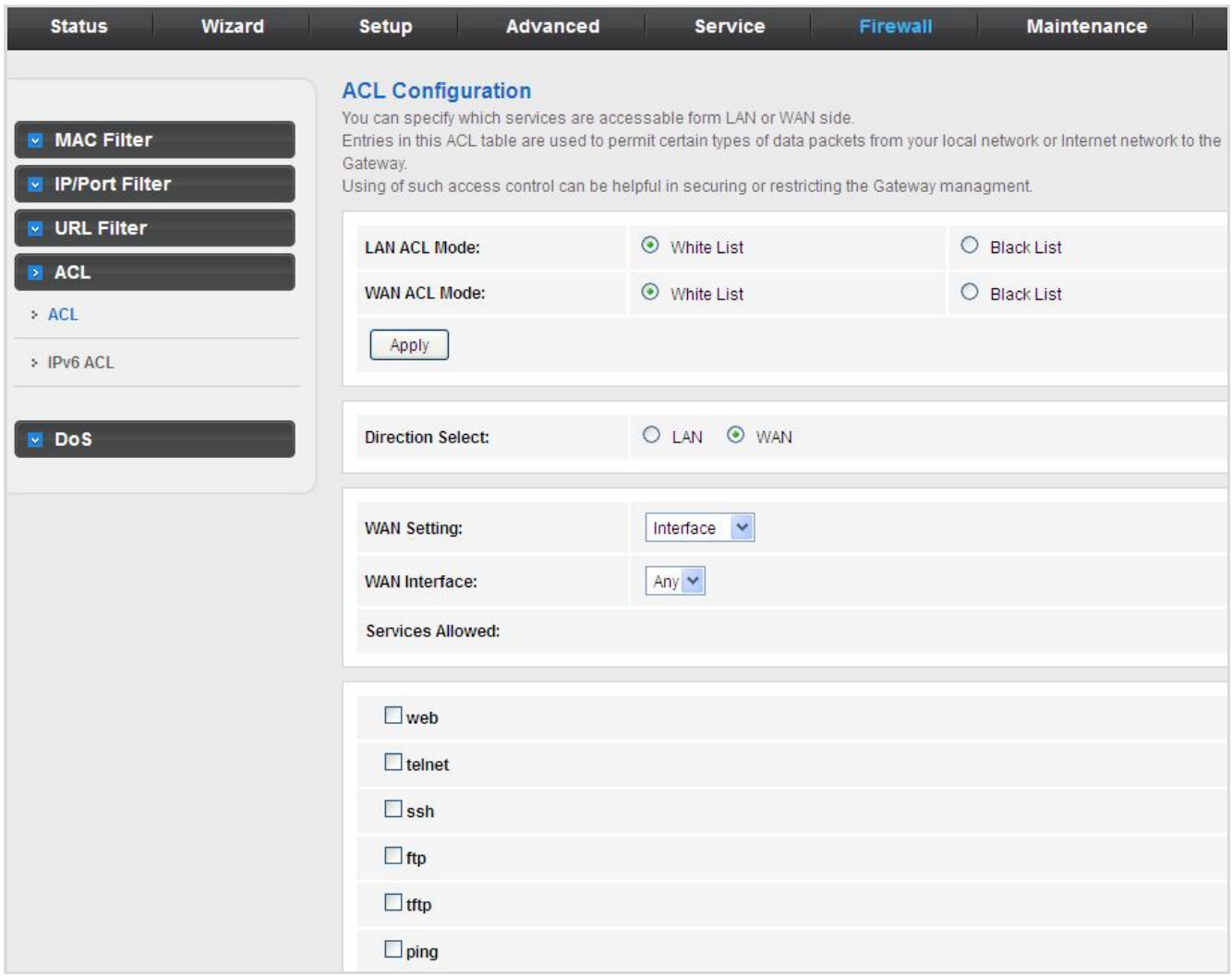


Figure 5-75 ACL WAN

5.6.4.2 IPv6 ACL

Choose **Service** > **IPv6 ACL** and the page shown in the following figure appears.

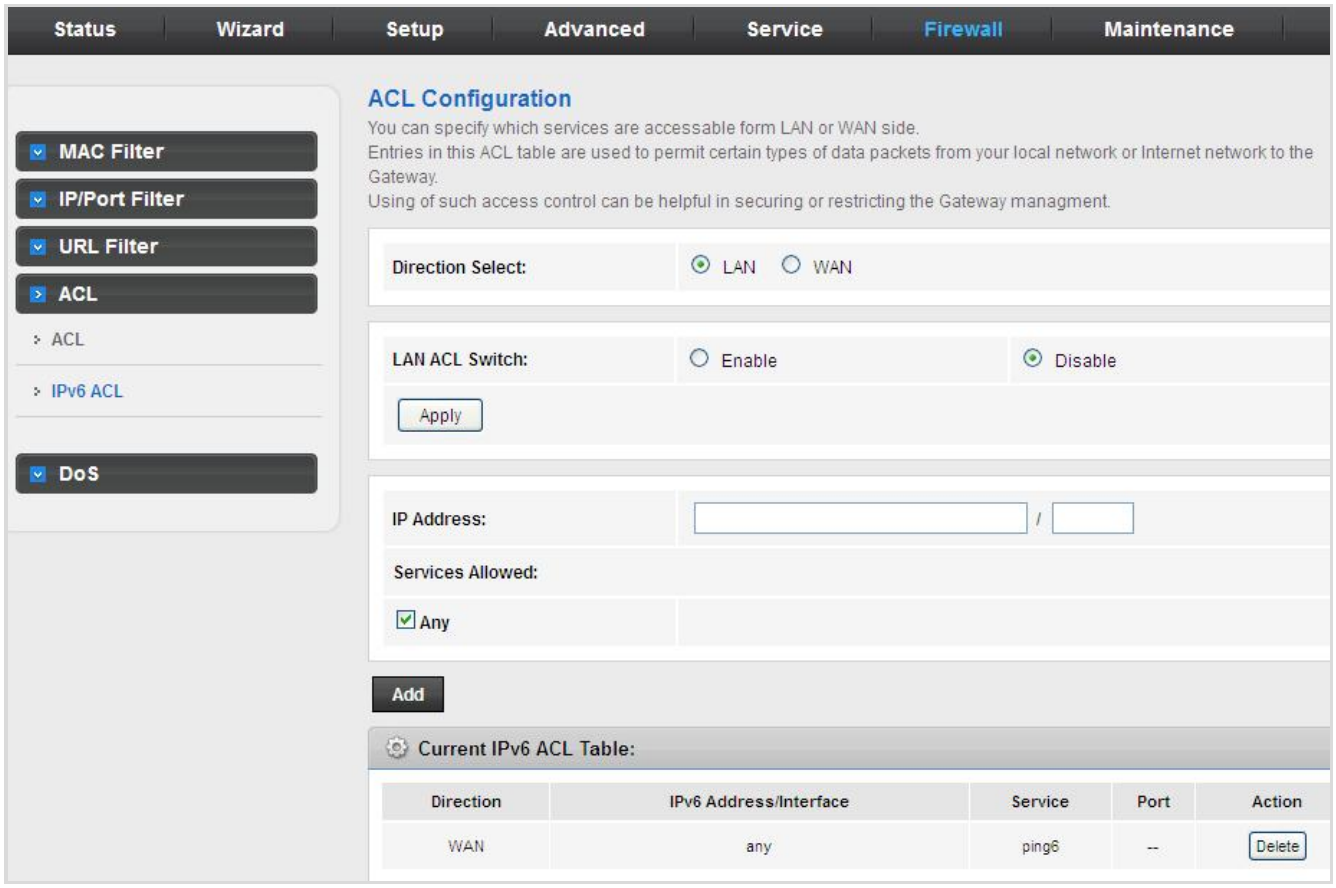


Figure 5-76 IPv6 ACL

If **WAN** is selected in the field of **Direction Select**, the page is shown in the following figure.

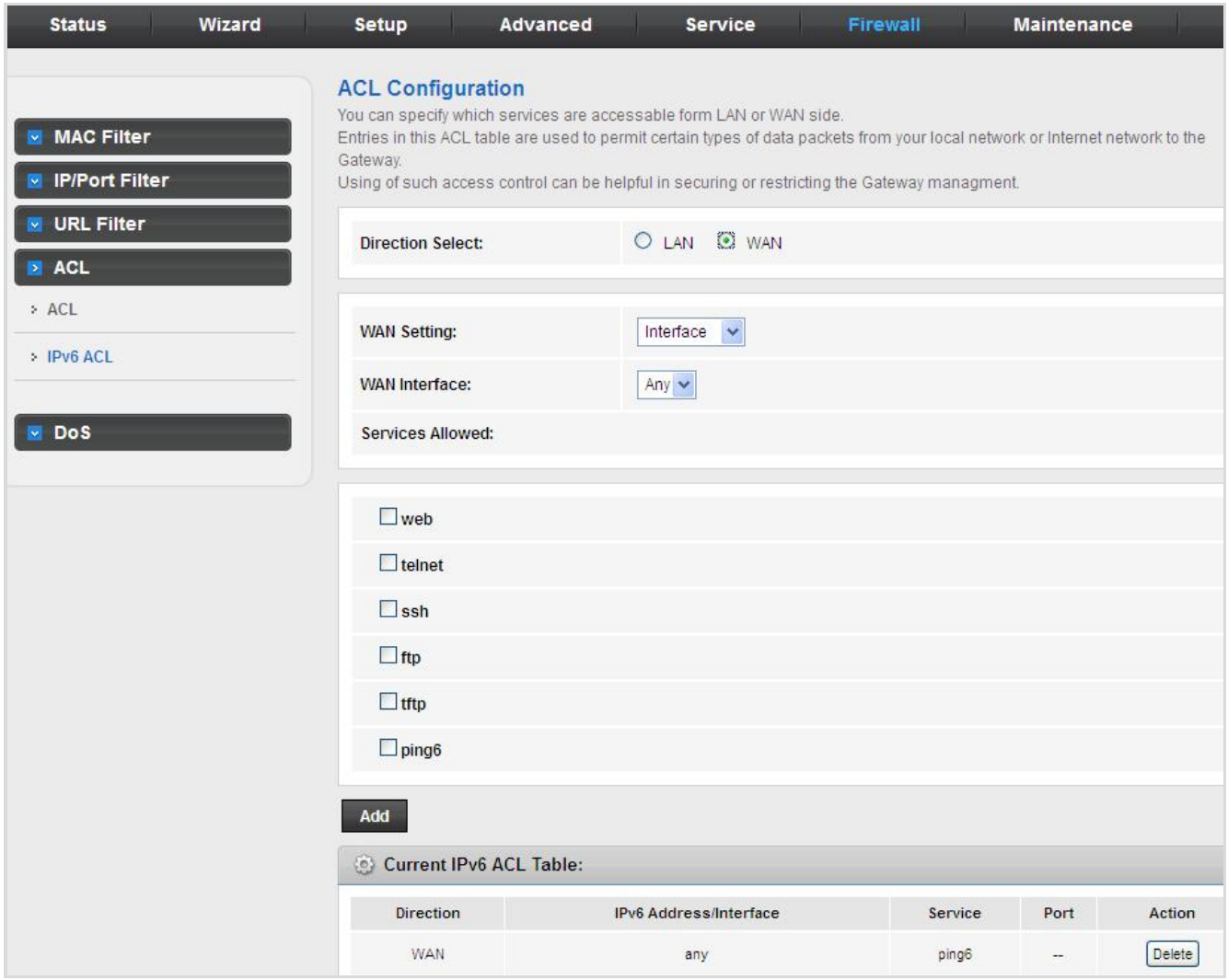


Figure 5-77 IPv6 ACL WAN

5.6.5 DoS

Denial-of-Service Attack (DoS attack) is a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic.

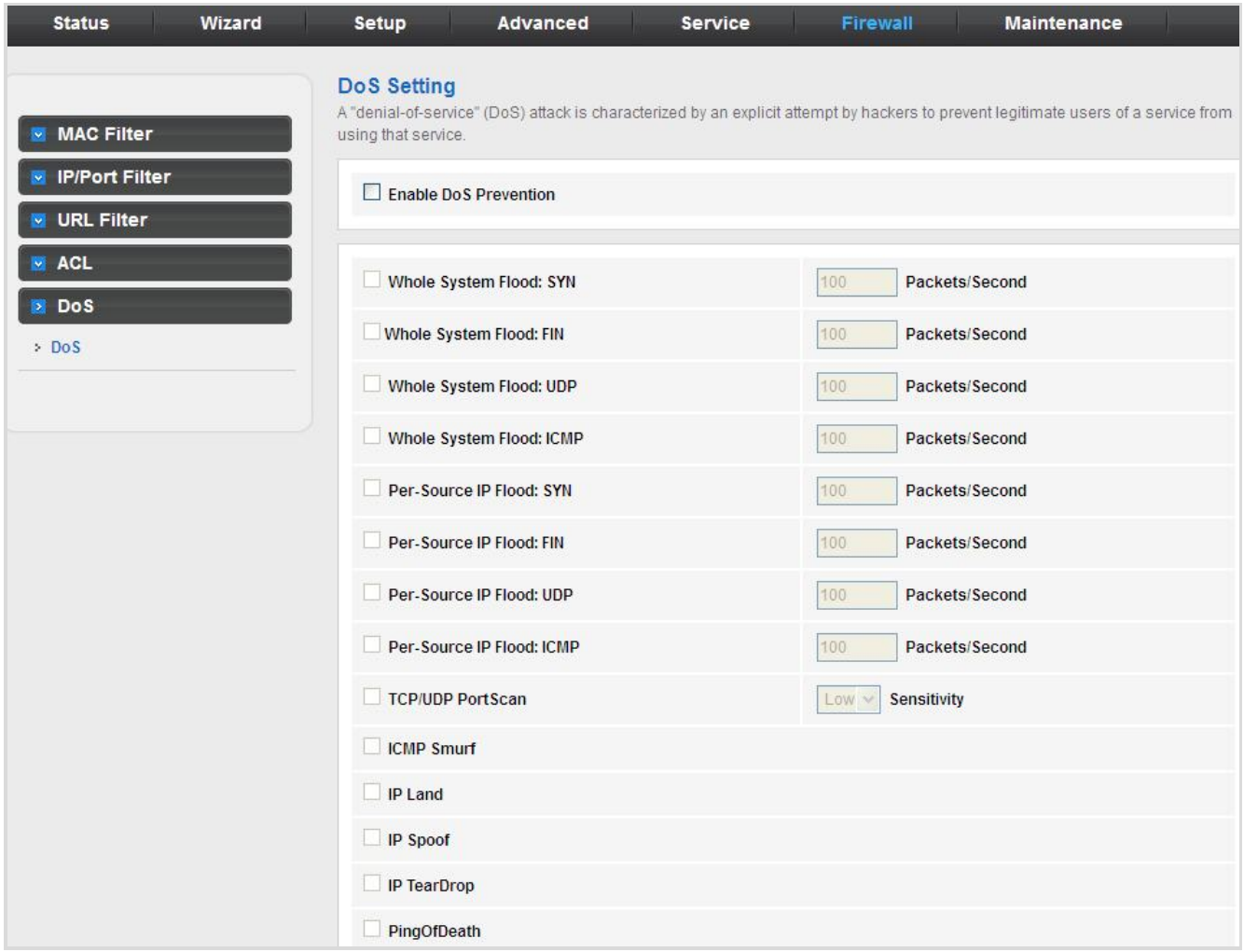


Figure 5-78 DoS

The following table describes the parameters:

Field	Description
Enable DoS Prevention	Enable denial-of-service feature to access.
Enable Source IP Blocking	Enable the function to block IP Source and set the time in seconds.

5.7 Maintenance

In the navigation bar, click Maintenance. The Maintenance page displayed contains **Update**, **Password**, **Reboot**, **Time**, **Log** and **Diagnostics**.

5.7.1 Update

Choose **Maintenance** > **Update**. The **Update** page displayed contains **Upgrade Firmware** and **Backup/Restore**.

Caution	Do not turn off the router or press the Reset button while the procedure is in progress.

5.7.1.1 Firmware Update

Click **Firmware** Update in the left pane and the page shown in the following figure appears. On this page, you can upgrade the firmware of the router.

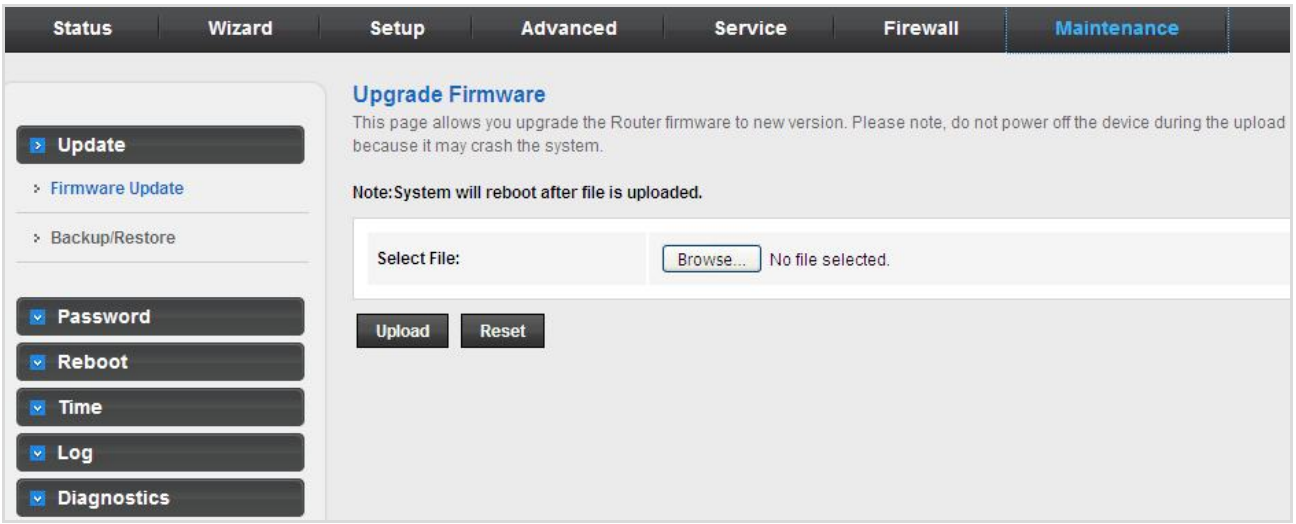


Figure 5-79 Firmware Update

The following table describes the parameters:

Field	Description
Select File	Click **Browse** or **Choose File** to select the firmware file.
Upload	After selecting the firmware file, click **Upload** to start upgrading the firmware file.
Reset	Click it to start selecting the firmware file.

5.7.1.2 Backup/Restore

Click **Backup/Restore** in the left pane and the page shown in the following figure appears. You can back up the current settings to a file and restore the settings from the file that was saved previously.

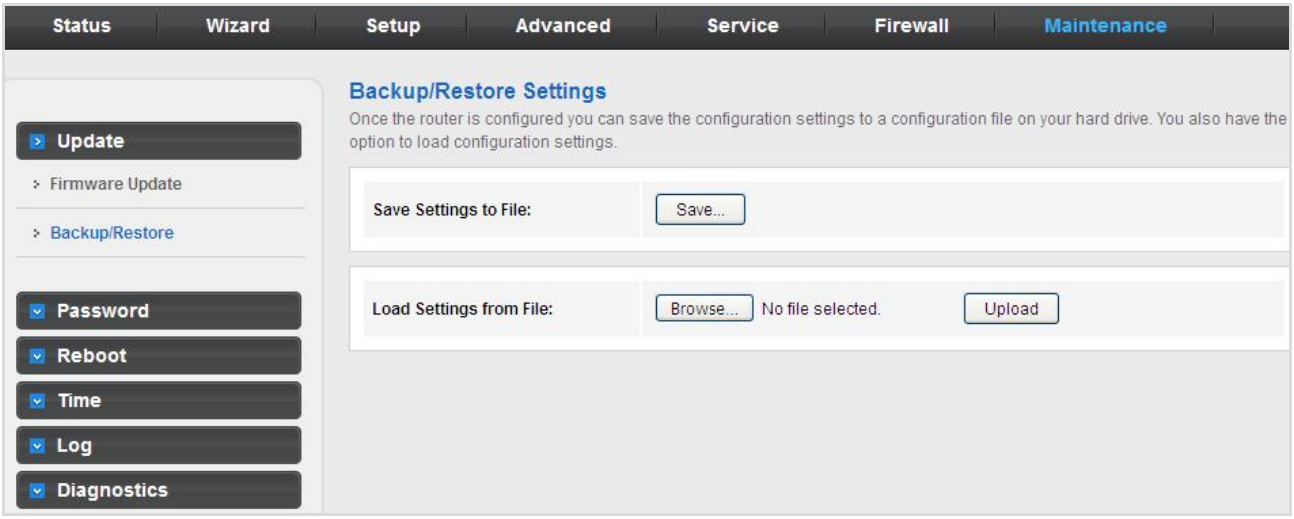


Figure 5-80 Backup/Restore

The following table describes the parameters:

Field	Description
Save Settings to File	Click it and select the path. Then you can save the configuration file of the router.
Load Settings from File	Click **Browse** or **Choose File** to select the configuration file.
Upload	After selecting the configuration file of the router, click **Upload** to start uploading the configuration file of the router.

5.7.2 Password

Choose **Maintenance** > **Password** and the page shown in the following figure appears. By default, the user name and password of the administrator are **admin** and **admin** respectively. The user name and password of the common user are **user** and **user** respectively.

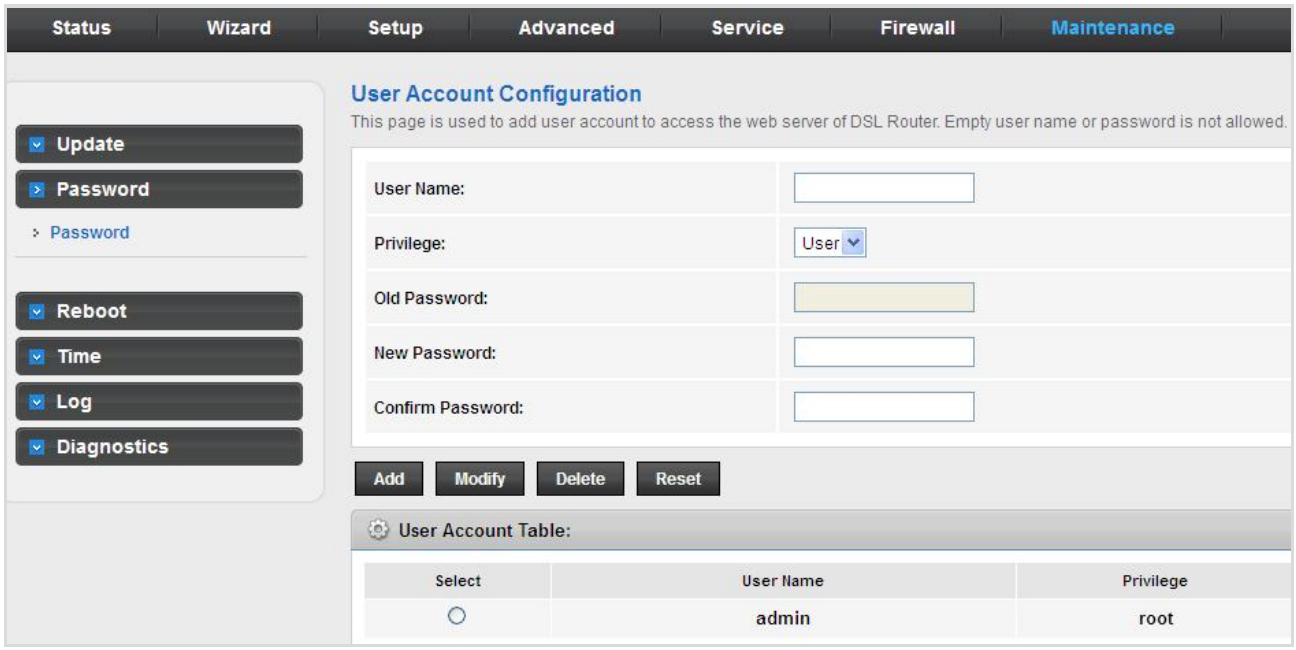


Figure 5-81 Password

The following table describes the parameters:

Field	Description
User Name	Choose the user name for accessing the router. You can choose **admin** or **user**.
Privilege	Choose the privilege for the account.
Old Password	Enter the old password
New Password	Enter your new password to which you want to change.
Confirmed Password	For confirmation, enter the new password again.

5.7.3 Reboot

Choose **Maintenance** > **Reboot** and the page shown in the following figure appears. You can set the router reset to the default settings or set the router to commit the current settings.

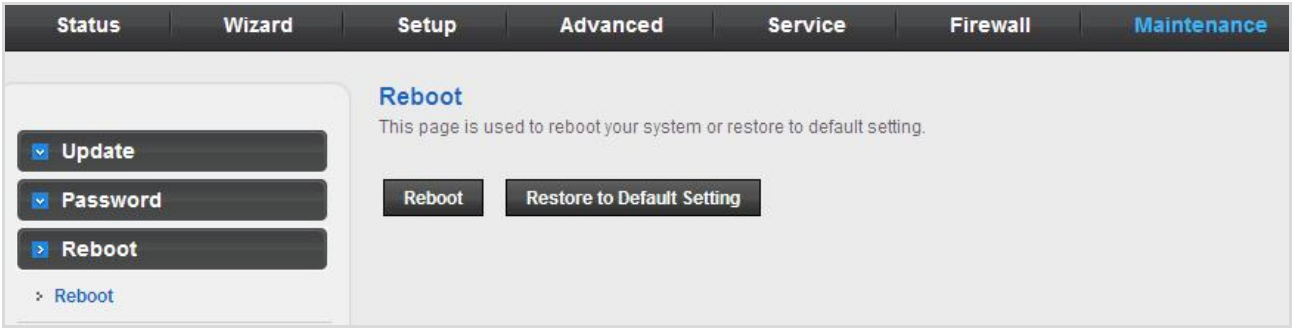


Figure 5-82 Reboot

The following table describes the parameters:

Field	Description
Reboot	It takes around 30 seconds to reboot the device and then again log in User Name and Password.
Restore to Default Setting	It helps to change to default settings. It takes around 30 seconds to restart the device and then again log in User Name and Password.

Note	Do not turn off the VDR-301N or press the reset button while this procedure is in progress.

5.7.4 Time

Choose **Maintenance** > **Time** and the page shown in the following figure appears. You can configure the system time manually or get the system time from the time server.

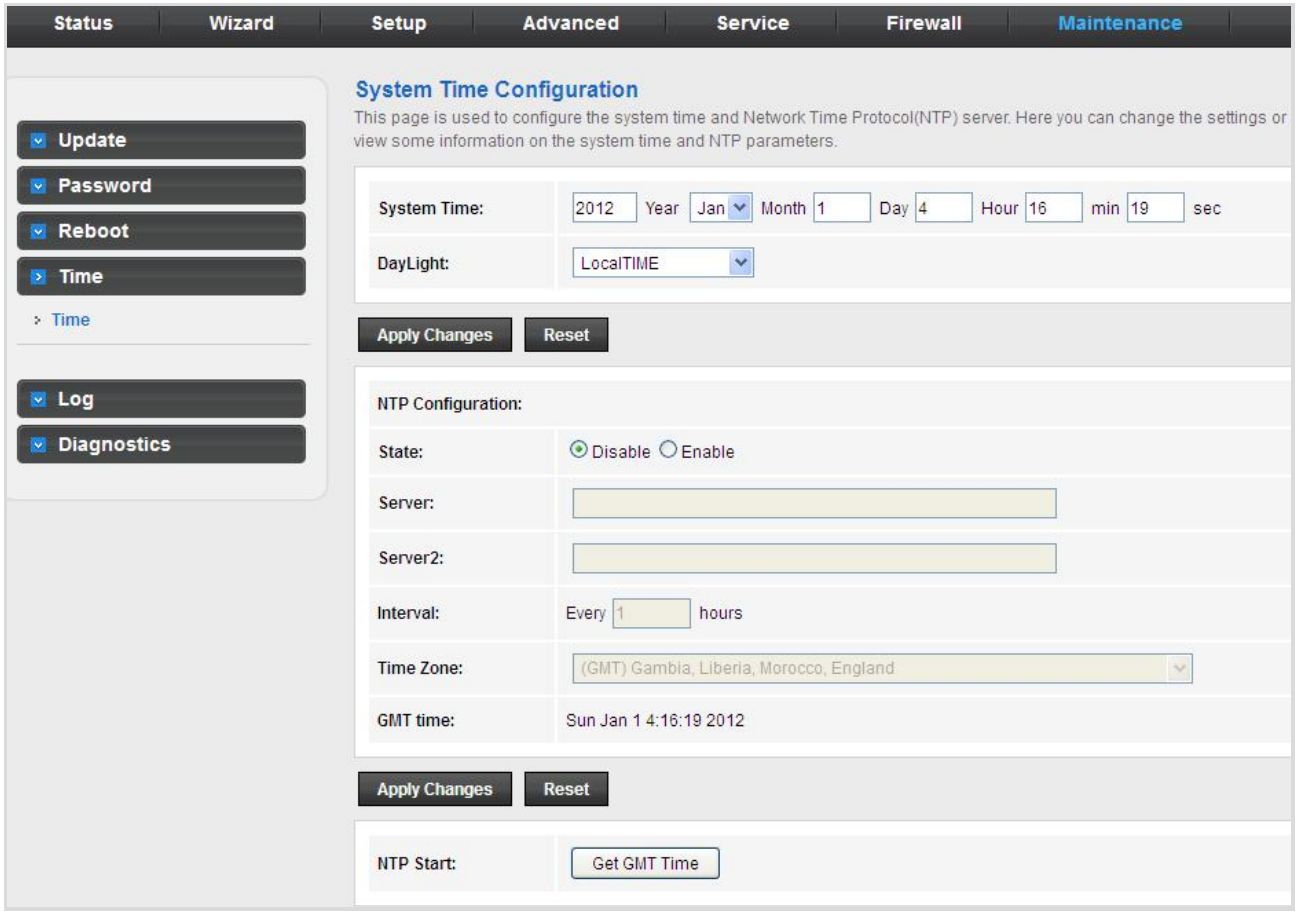


Figure 5-83 Time

The following table describes the parameters:

Field	Description
System Time	Configure the system time manually.
Day Light	Daylight Saving Time.
State	Enable the option to update the system clock automatically. Disable the option to update the system clock manually.
Server	Configure the primary NTP server manually.
Server2	Configure the secondary NTP server manually.
Interval	NTP updating time interval.
Time Zone	Choose the time zone of your country from the drop-down list.
GMT Time	Greenwich Mean time.

5.7.5 Log

Choose **Maintenance** > **Log** and the page shown in the following figure appears. On this page, you can enable or disable system log function and view the system log.

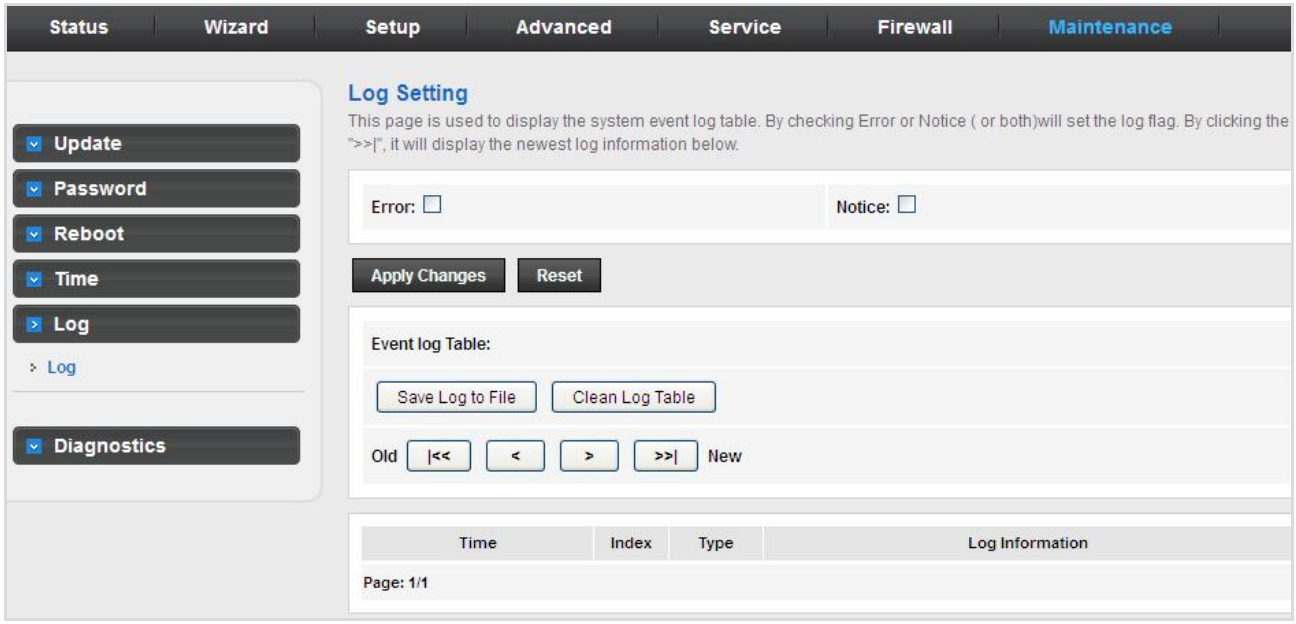


Figure 5-84 Log

The following table describes the parameters:

Field	Description
Error	Enable/Disable the function to display the Error.
Notice	Enable/Disable the function to notify the Error.

5.7.6 Diagnostic

In the navigation bar, click **Diagnostic**. The **Diagnostic** page displayed contains **Ping**, **Ping6**, **Traceroute**, **Traceroute6**, and **Diag-Test**.

5.7.6.1 Ping

Choose **Diagnostic** > **Ping** and the page shown in the following figure appears.

Figure 5-85 Ping

The following table describes the parameters:

Field	Description
Host Address	Enter IP address you want to ping.
Interface	Choose a WAN interface.

5.7.6.2 Ping6

Choose **Diagnostic** > **Ping6** and the page shown in the following figure appears.

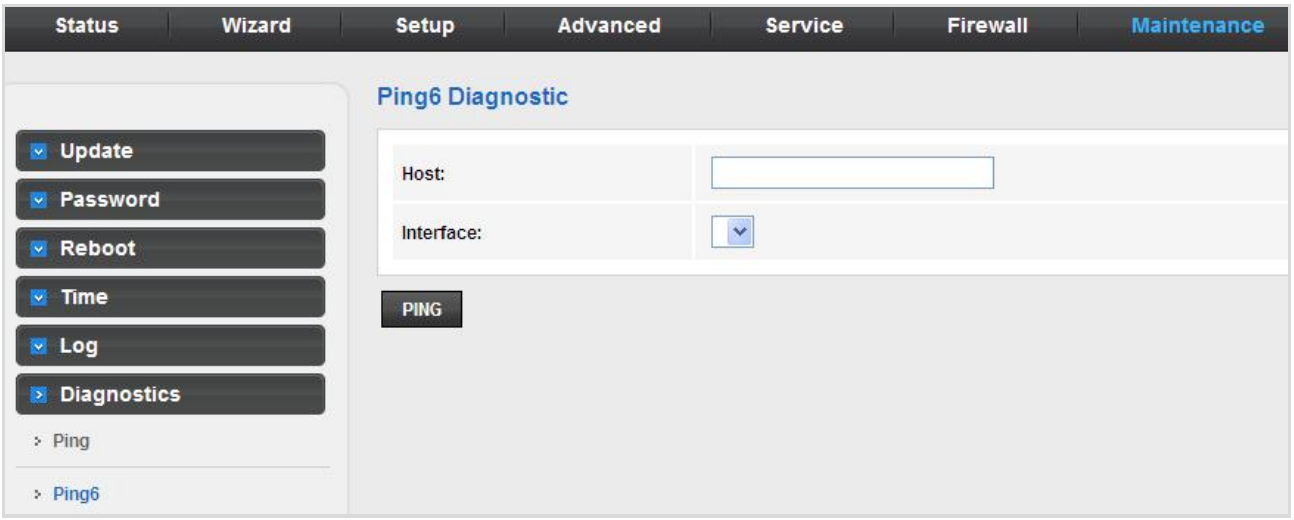


Figure 5-86 Ping6

The following table describes the parameters:

Field	Description
Host Address	Enter IPv6 address you want to ping.
Interface	Choose a WAN interface.

5.7.6.3 Traceroute

Choose **Diagnostic** >**Traceroute** and the following page appears. By Traceroute Diagnostic, you can track the route path through the information which is from your computer to the other side host on the Internet.

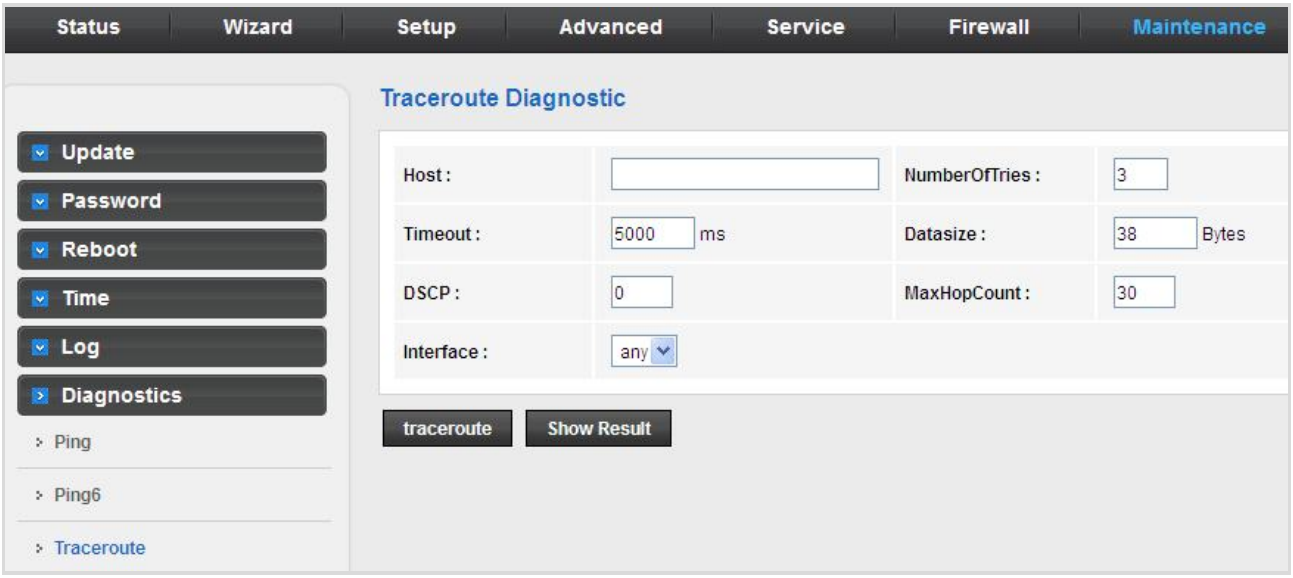


Figure 5-87 Traceroute

The following table describes the parameters:

Field	Description
Host	Enter the destination host address for diagnosis.
NumberOfTries	Number of repetitions.
Timeout	Put in the timeout value.
Datasize	Packet size.
DSCP	Differentiated Services Code Point, You should set a value between 0-63.
MaxHopCount	Maximum number of routes.
Interface	Select the interface.

5.7.6.4 Traceroute6

Choose **Diagnostic** >**Traceroute6** and the following page appears. By Traceroute Diagnostic, you can track the route path through the information which is from your computer to the other side host on the Internet.

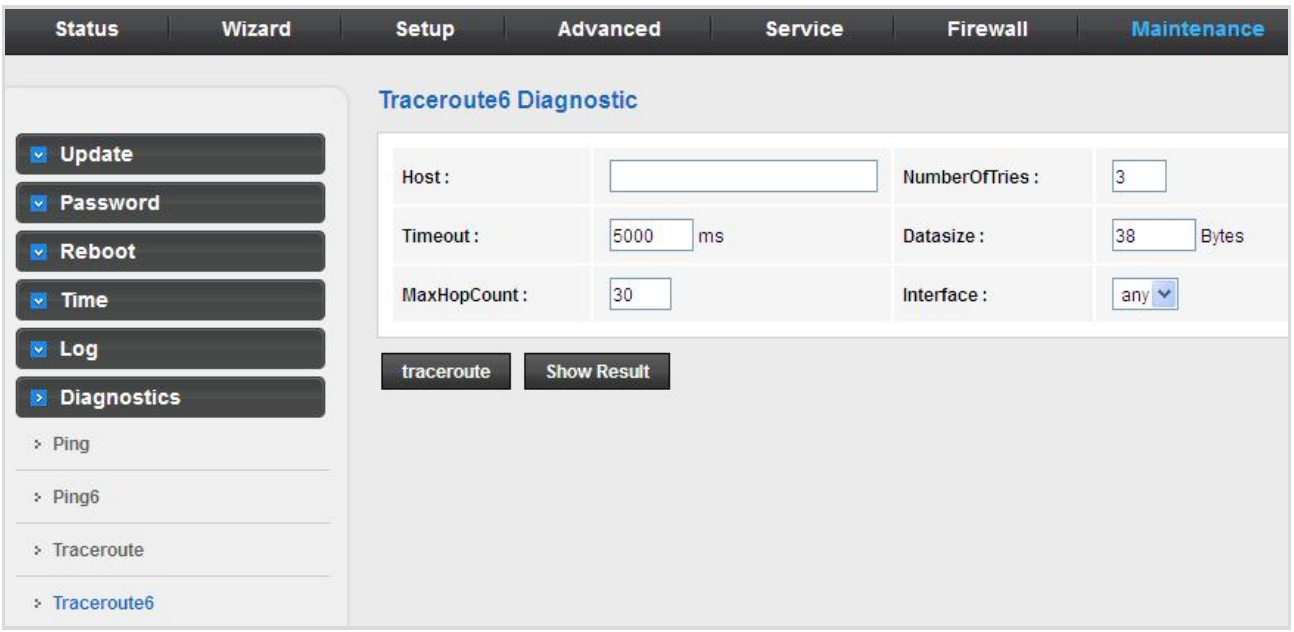


Figure 5-88 Traceroute6

The following table describes the parameters:

Field	Description
Host	Enter the destination host address for diagnosis.
NumberOfTries	Number of repetitions.
Timeout	Put in the timeout value.
Datasize	Packet size.
MaxHopCount	Maximum number of routes.
Interface	Select the interface.

5.7.6.5 OAM Loopback

Choose **Diagnostic** > **OAM Loopback** and the page shown in the following figure appears. On this page, you can use VCC loopback function to check the connectivity of the VCC. The ATM loopback test is useful for troubleshooting problems with the DSLAM and ATM network.

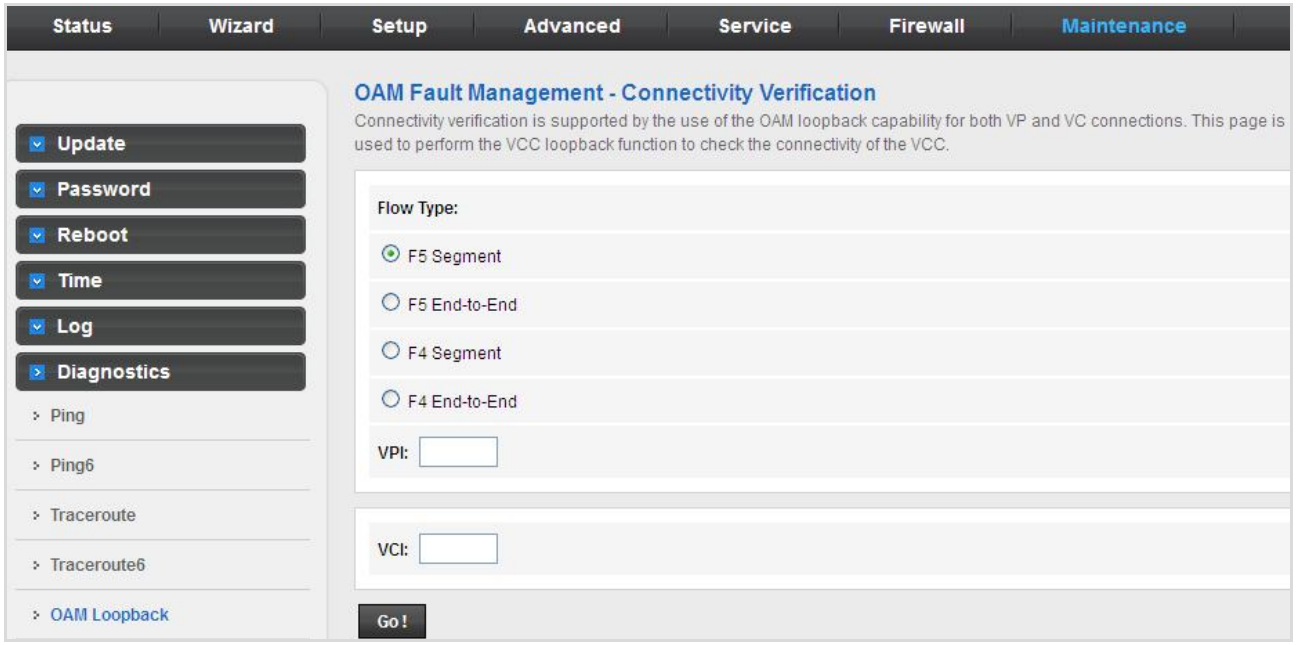


Figure 5-89 OAM Loopback

The following table describes the parameters:

Field	Description
Flow Type	There are 4 flow types. The selection can be F5 Segment, F5 End-to-End, F4 Segment and F4 End-to-End
VPI	Virtual Path Identifier
VCI	Virtual Circuit Identifier.

5.7.6.6 DSL Diagnostic

Choose **Diagnostic** > **DSL Diagnostic** and the page shown in the following figure appears. It is used for xDSL tone diagnostics.

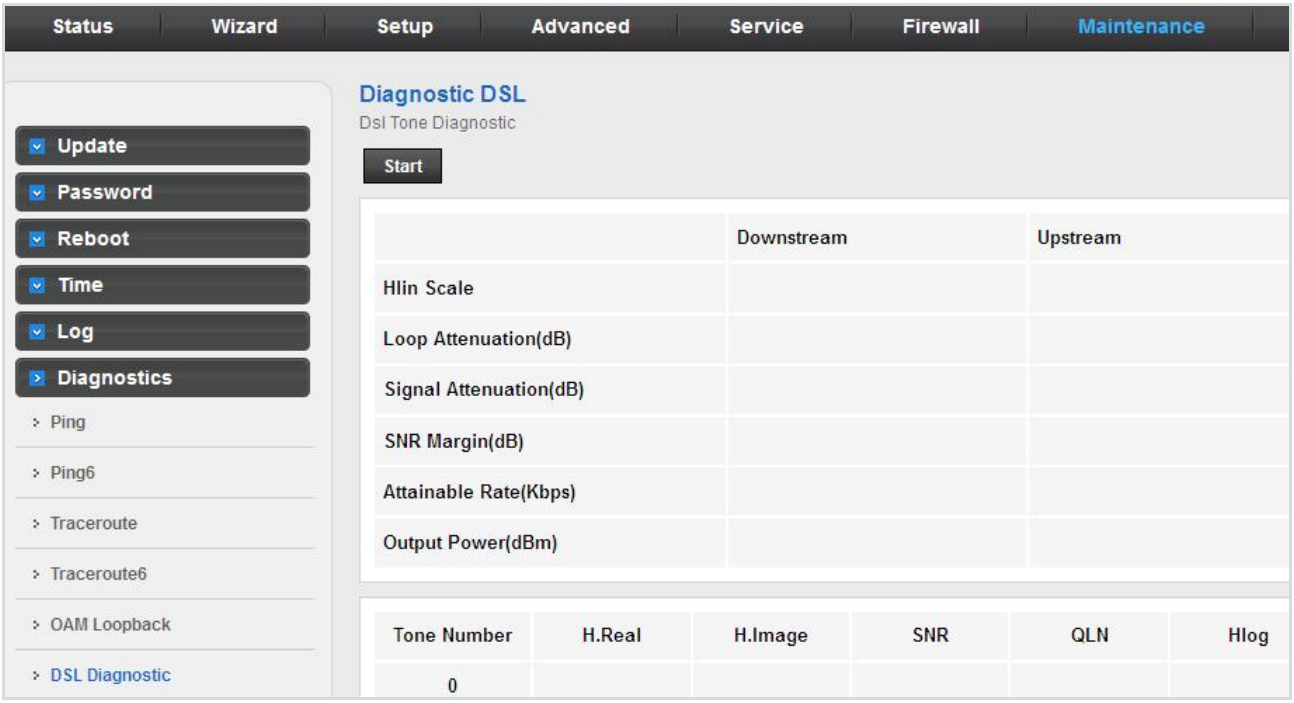


Figure 5-90 DSL Diagnostic

Click **Start** to start ADSL tone diagnostics.

5.7.6.7 Diag-Test

Choose **Diagnostics** > **Diag-Test** and the page shown in the following figure appears. On this page, you can test the VDSL2 Router connection. You can also view the LAN status connection and fiber connection.

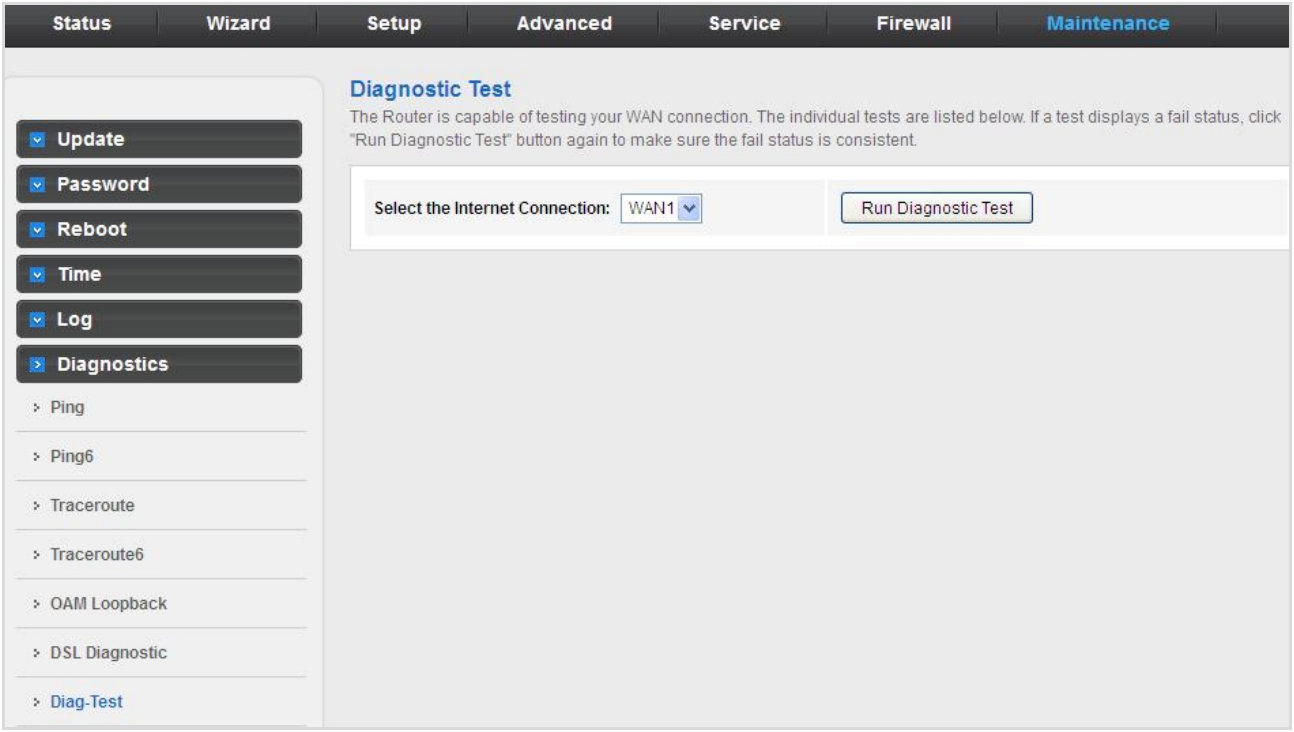


Figure 5-91 Diag-Test

Click **Run Diagnostic Test** to start testing.

Chapter 6. Quick Connection to a Wireless Network

In the following sections, the **default SSID** of the VDR-301N is configured to "**default**".

6.1 Windows XP (Wireless Zero Configuration)

Step 1: Right-click on the **wireless network icon** displayed in the system tray

Figure 6-1 System Tray – Wireless Network Icon

Step 2: Select [**View Available Wireless Networks**]

Step 3: Highlight and select the wireless network (SSID) to connect

(1) Select SSID [default]

(2) Click the [**Connect**] button

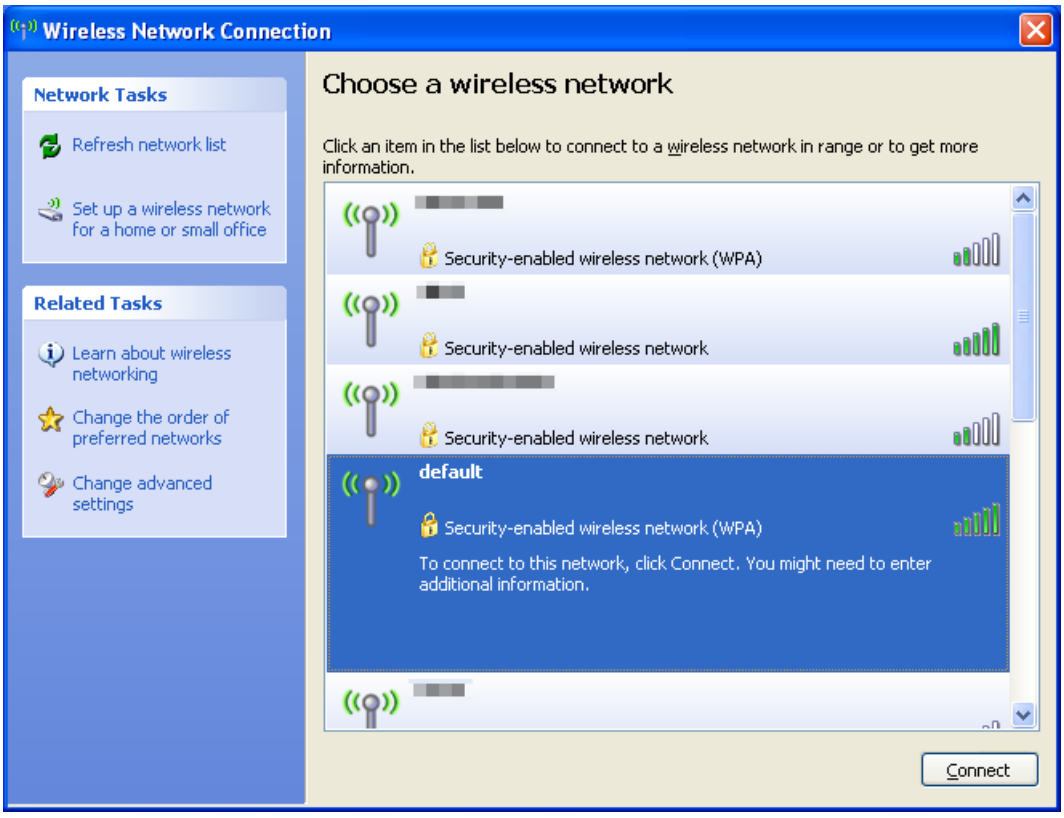


Figure 6-2 Choose a wireless network

Step 4: Enter the **encryption key** of the Wireless AP

(1) The Wireless Network Connection box will appear

(2) Enter the encryption key that is configured in section 5.3.3.2

(3) Click the [Connect] button

Figure 6-3 Enter the network key

Step 5: Check if "**Connected**" is displayed

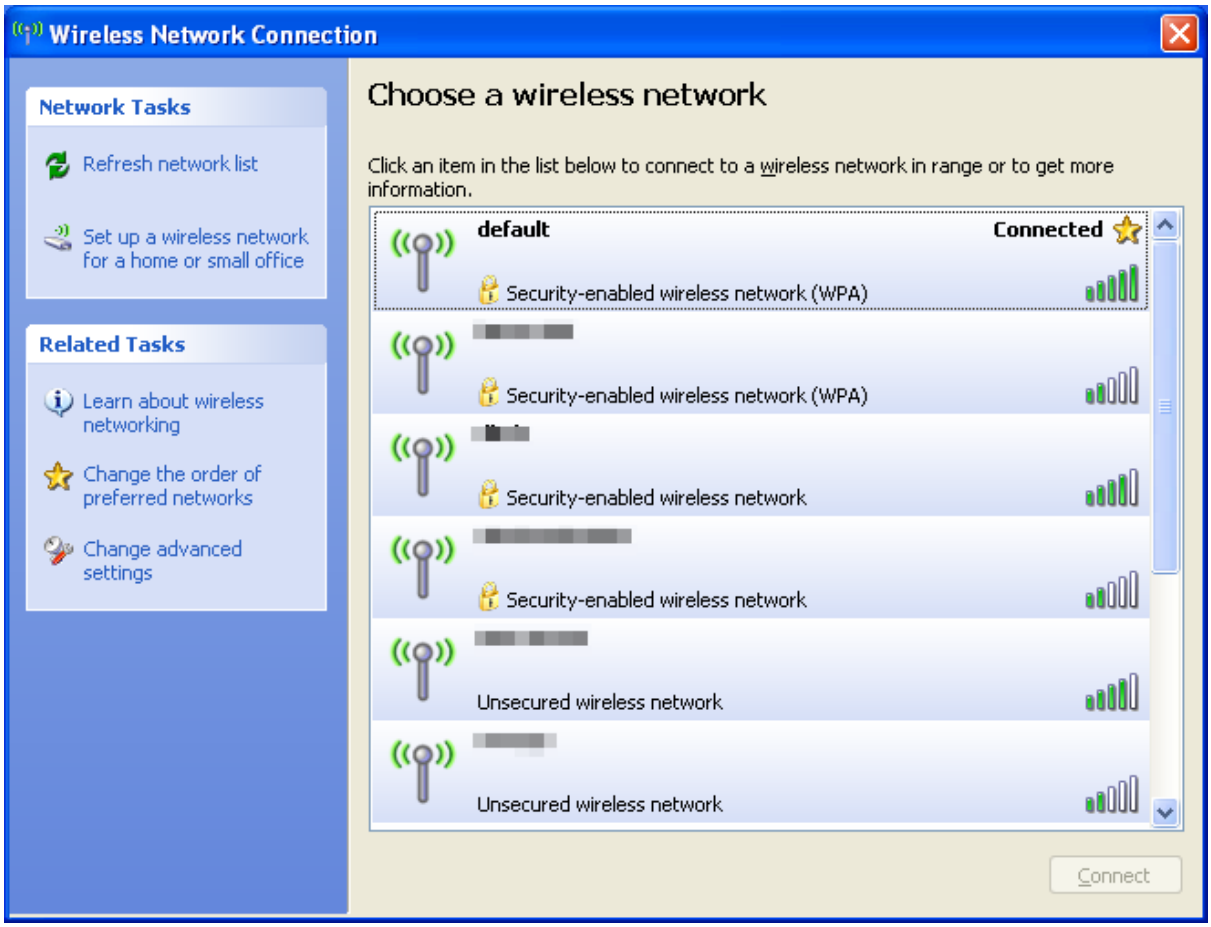


Figure 6-4 Choose a wireless network -- Connected

Some laptops are equipped with a “Wireless ON/OFF” switch for the internal wireless LAN. Make sure the hardware wireless switch is switched to “ON” position.

6.2 Windows 7 (WLAN AutoConfig)

WLAN AutoConfig service is built-in in Windows 7 to enable to detect and connect to wireless network. This built-in wireless network connection tool is similar to the wireless zero configuration tool in Windows XP.

Step 1: Right-click on the **network icon** displayed in the system tray

Figure 6-5 Network icon

Step 2: Highlight and select the wireless network (SSID) to connect

(1) Select SSID [**default**]
(2) Click the [**Connect**] button

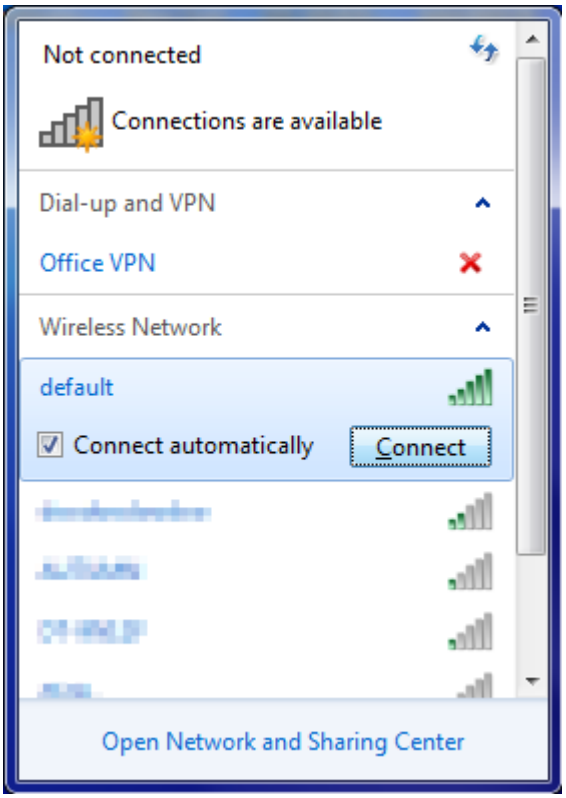


Figure 6-6 WLAN AutoConfig

Note

If you will be connecting to this Wireless AP in the future, check [**Connect automatically**].

Step 4: Enter the **encryption key** of the Wireless AP

(1) The Connect to a Network box will appear

(2) Enter the encryption key that is configured in section 5.3.3.2

(3) Click the [OK] button

Figure 6-7 Type the network key

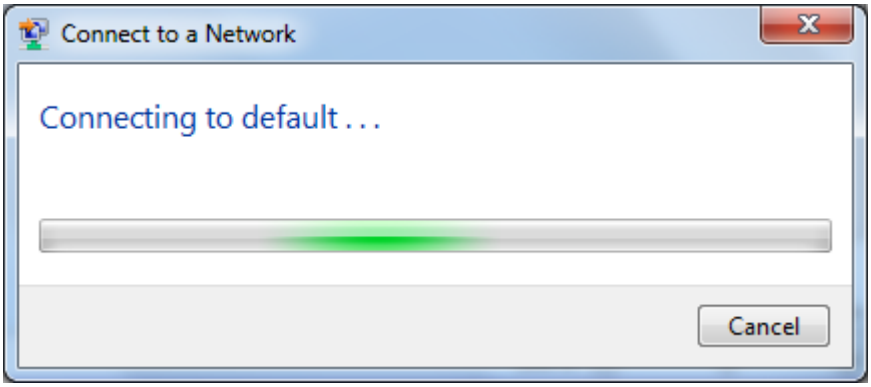


Figure 6-8 Connecting to a Network

Step 5: Check if "**Connected**" is displayed

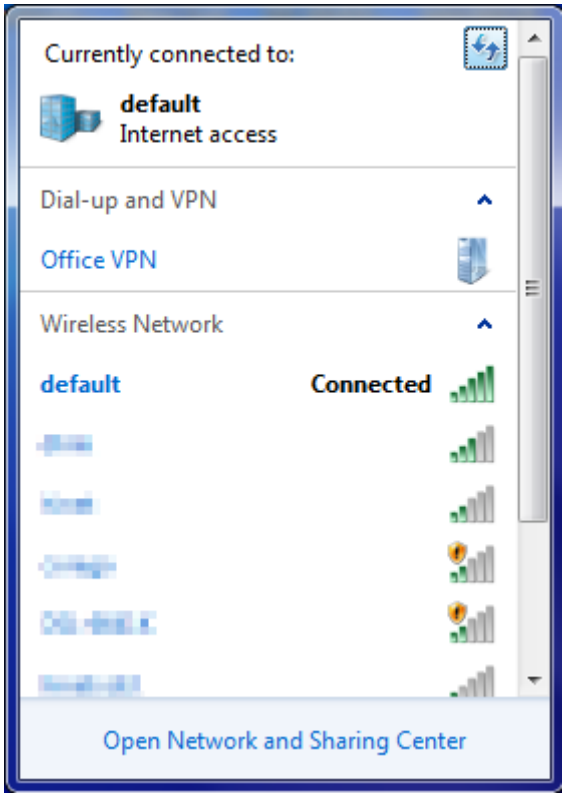


Figure 6-9 Connected to a Network

6.3 Mac OS X 10.x

In the following sections, the default SSID of the VDR-301N is configured to “default”.

Step 1: Right-click on the **network icon** displayed in the system tray

The AirPort Network Connection menu will appear

Figure 6-10 Mac OS – Network icon

Step 2: Highlight and select the wireless network (SSID) to connect

(1) Select and SSID [**default**]

(2) Double-click on the selected SSID

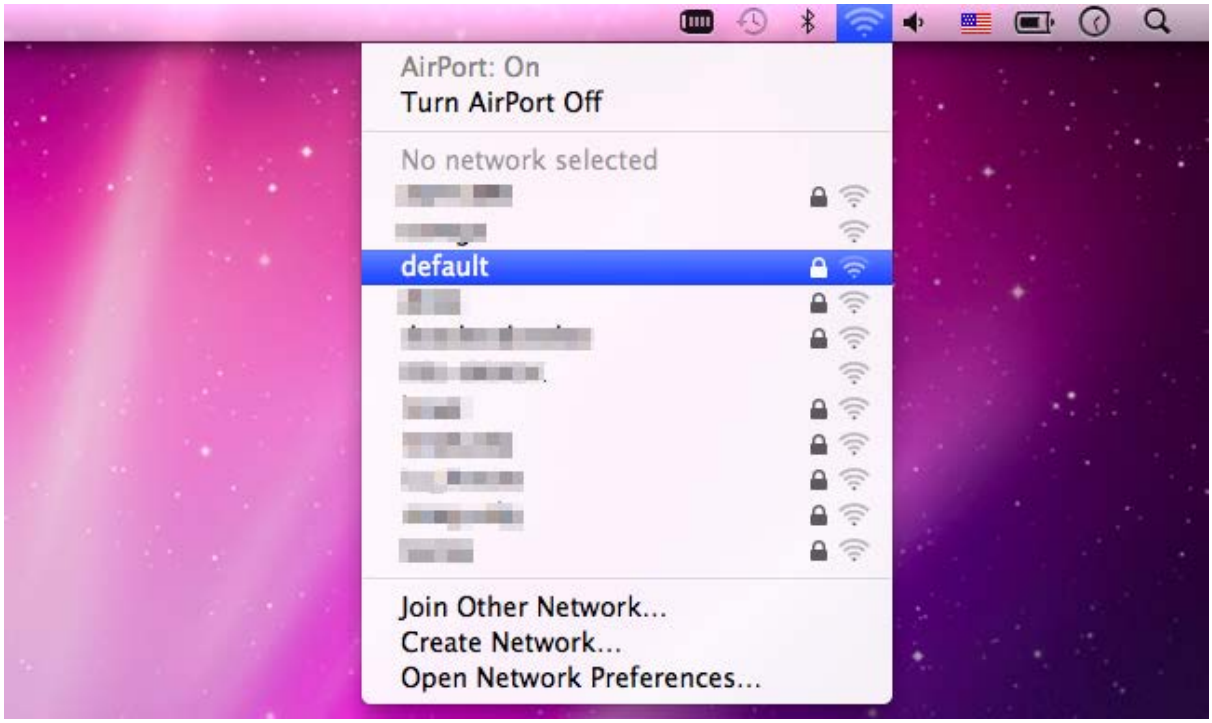


Figure 6-11 Highlight and select the wireless network

Step 4: Enter the **encryption key** of the Wireless AP

(1) Enter the encryption key that is configured in section 5.3.3.2

(2) Click the [OK] button

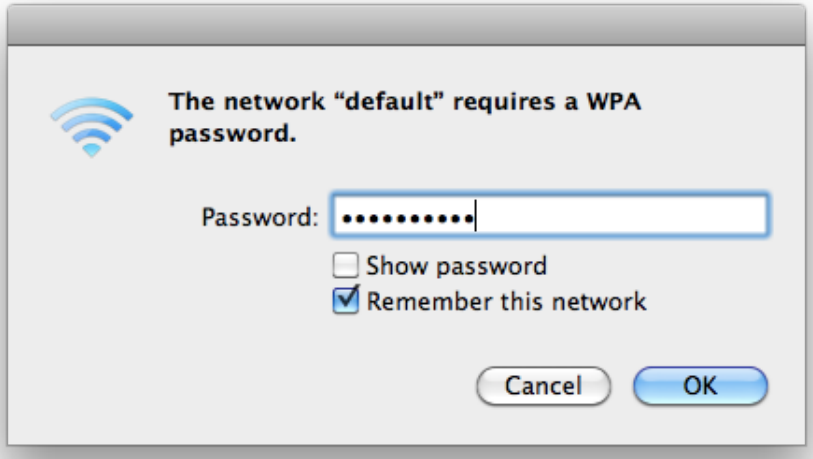


Figure 6-12 Enter the Password

Note

If you will be connecting to this Wireless AP in the future, check [**Remember this network**].

Step 5: Check if the AirPort is connected to the selected wireless network.

If "Yes", then there will be a "check" symbol in the front of the SSID.

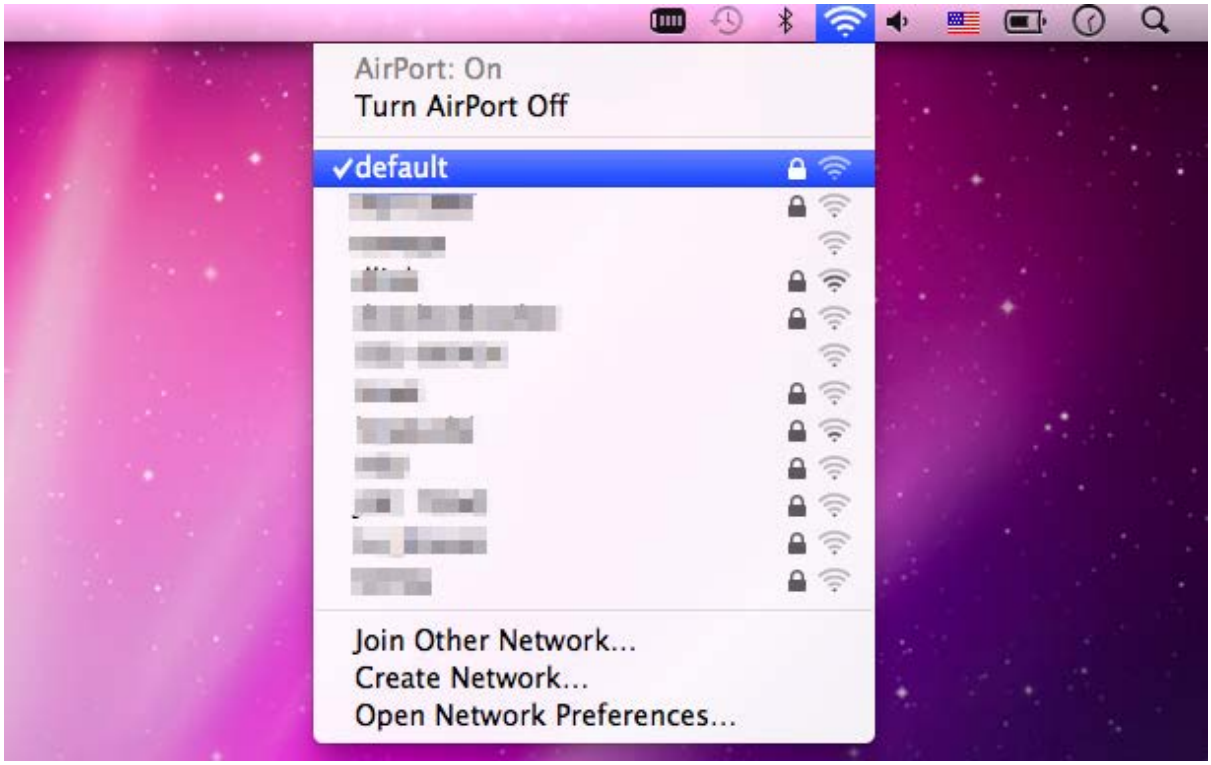


Figure 6-13 Connected to the Network

There is another way to configure the MAC OS X Wireless settings:

Step 1: Click and open the [**System Preferences**] by going to **Apple** > **System Preference** or **Applications**

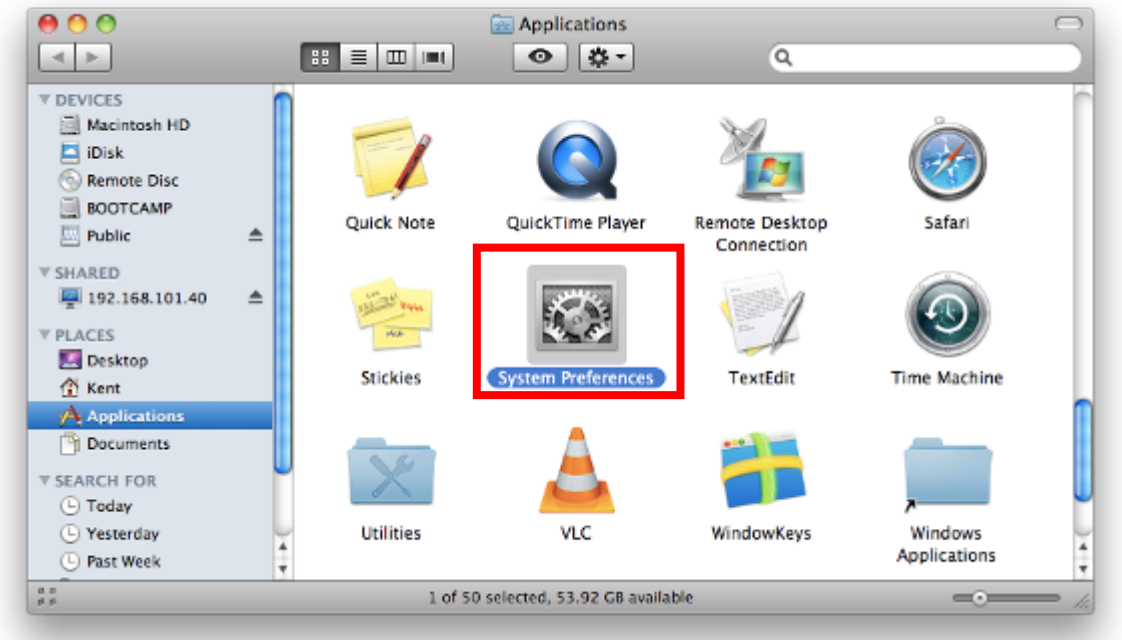


Figure 6-14 System Preferences

Step 2: Open **Network Preference** by clicking on the [**Network**] icon

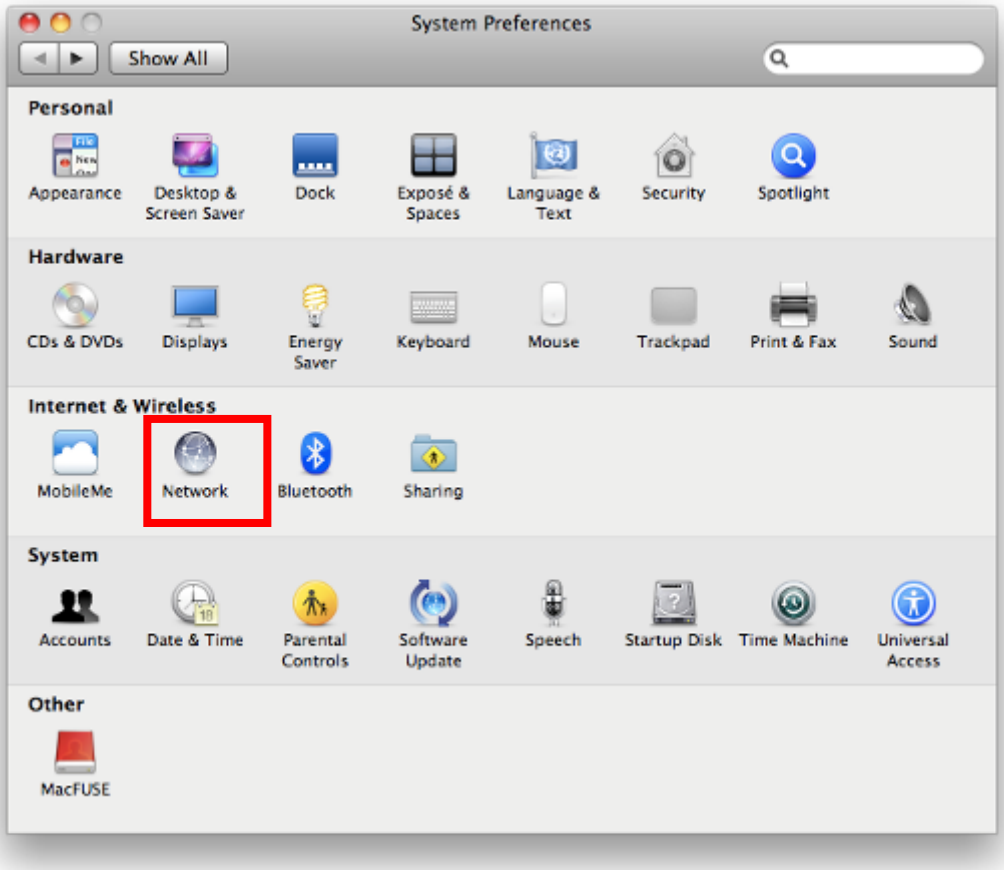


Figure 6-15 System Preferences -- Network

Step 3: Check Wi-Fi setting and select the available wireless network

(1) Choose the **AirPort** on the left-menu (make sure it is ON)

(2) Select Network Name [**default**] here

If this is the first time to connect to the Wireless AP, it should show “Not network selected”.

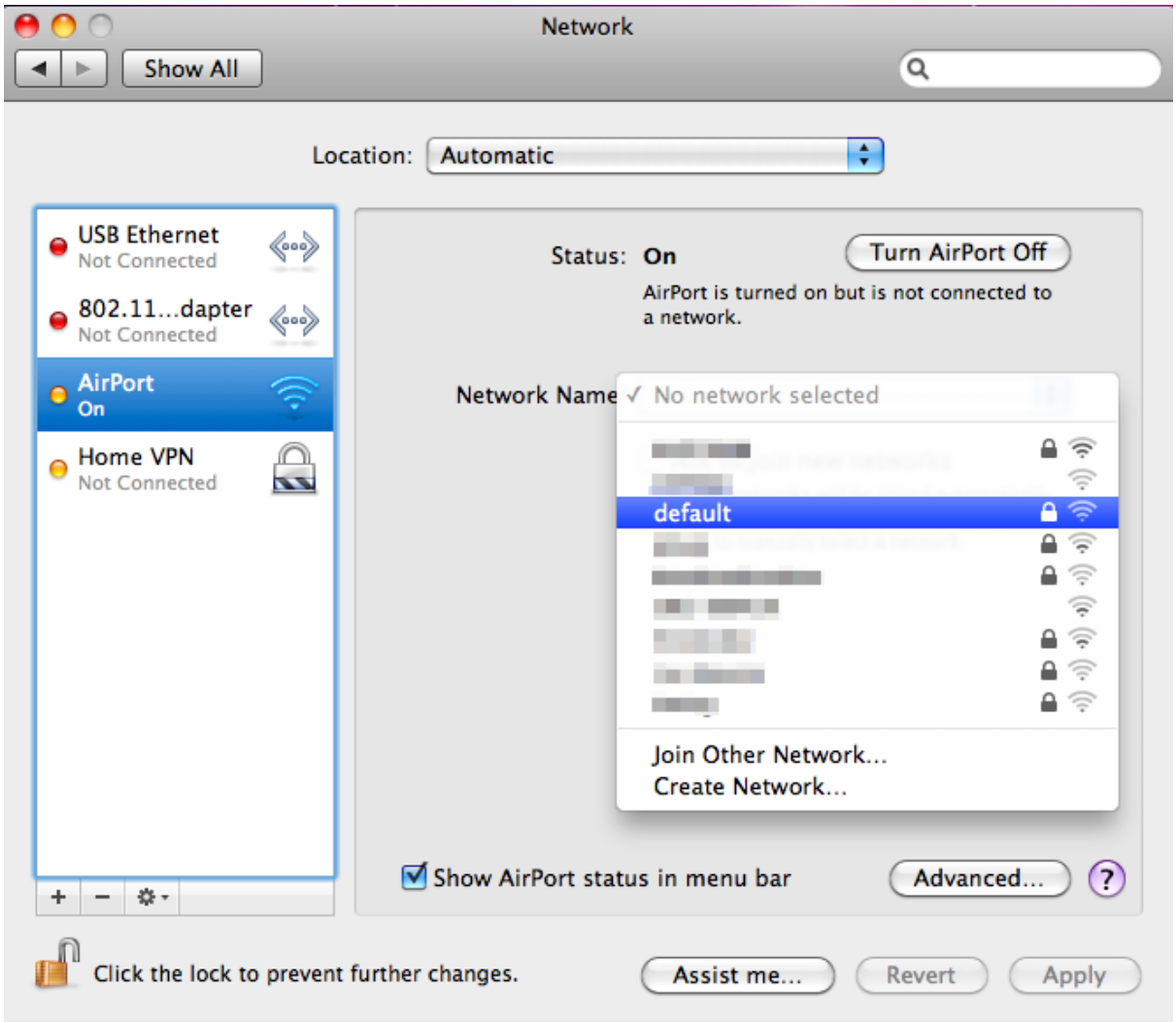


Figure 6-16 Select the Wireless Network

6.4 iPhone/iPod Touch/iPad

In the following sections, the **default SSID** of the VDR-301N is configured to "**default**".

Step 1: Tap the [**Settings**] icon displayed in the home screen

Figure 6-17 iPhone – Settings icon

Step 2: Check Wi-Fi setting and select the available wireless network

(3) Tap [**General**] \ [**Network**]

(4) Tap [**Wi-Fi**]

If this is the first time to connect to the Wireless AP, it should show "Not Connected".

Figure 6-18 Wi-Fi Setting

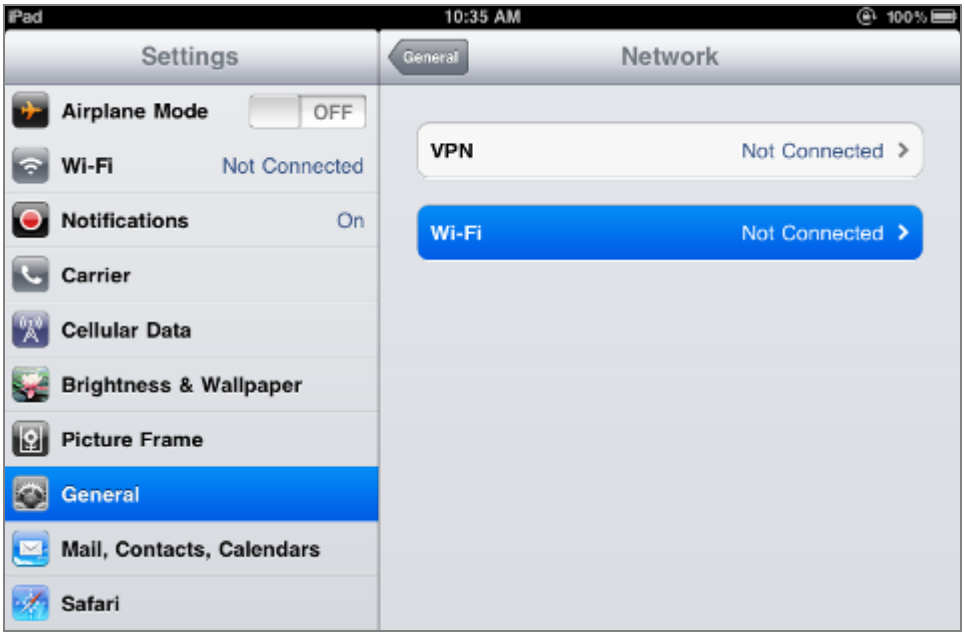


Figure 6-19 Wi-Fi Setting – Not Connected

Step 3: Tap the target wireless network (SSID) in "**Choose a Network…**"

(1) Turn on Wi-Fi by tapping "**Wi-Fi**"

(2) Select SSID [**default**]

Figure 6-20 Turn on Wi-Fi

Step 4: Enter the **encryption key** of the Wireless AP

(1) The password input screen will be displayed

(2) Enter the encryption key that is configured in section 5.3.3.2

(3) Tap the [**Join**] button

Figure 6-21 iPhone -- Enter the Password

Step 5: Check if the device is connected to the selected wireless network.

If “Yes”, then there will be a “check” symbol in the front of the SSID.

Figure 6-22 iPhone -- Connected to the Network

Appendix A: Cable Profiles

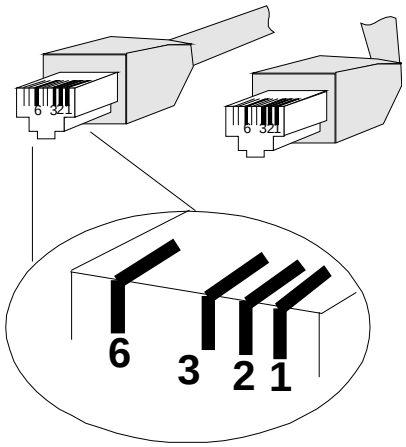
A.1 Device's RJ45 Pin Assignments

■ **10/100Mbps, 10/100BASE-TX**

Contact	MDI	MDI-X
1	1 (TX +)	3
2	2 (TX -)	6
3	3 (RX +)	1
6	6 (RX -)	2
4, 5, 7, 8	Not used	Not used

Implicit implementation of the crossover function within a twisted-pair cable, or at a wiring panel, while not expressly forbidden, is beyond the scope of this standard.

A.2 RJ45 Cable Pin Assignment



There are 8 wires on a standard UTP/STP cable and each wire is color-coded. The following shows the pin allocation and color of straight-through cable and crossover cable connection:

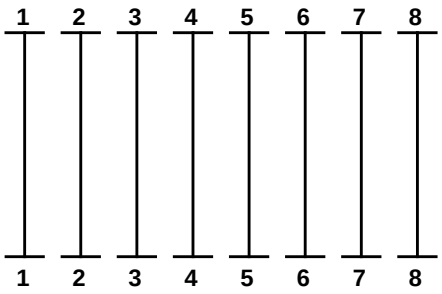
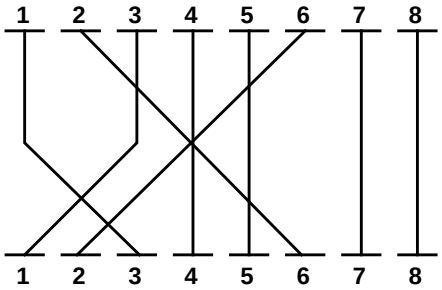
Straight-through Cable		SIDE 1	SIDE 2
	SIDE 1	1 = White / Orange	1 = White / Orange
		2 = Orange	2 = Orange
		3 = White / Green	3 = White / Green
		4 = Blue	4 = Blue
		5 = White / Blue	5 = White / Blue
		6 = Green	6 = Green
		7 = White / Brown	7 = White / Brown
	SIDE 2	8 = Brown	8 = Brown
Crossover Cable		**SIDE 1**	**SIDE 2**
	SIDE 1	1 = White / Orange	1 = White / Green
		2 = Orange	2 = Green
		3 = White / Green	3 = White / Orange
		4 = Blue	4 = Blue
		5 = White / Blue	5 = White / Blue
		6 = Green	6 = Orange
		7 = White / Brown	7 = White / Brown
	SIDE 2	8 = Brown	8 = Brown

Figure A-1: Straight-through and Crossover Cables

Please make sure your connected cables are with the same pin assignment and color as the above table before deploying the cables into your network.

EC Declaration of Conformity

English	Hereby, **PLANET Technology Corporation**, declares that this **802.11n Wireless Internet 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 Wireless Internet 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 Wireless Internet VDSL2 Router** splňuje základní požadavky a další příslušná ustanovení směrnice 1999/5/EC.	**Magyar**	A gyártó **PLANET Technology Corporation** n, kijelenti, hogy ez a **802.11n Wireless Internet VDSL2 Router** r megfelel az 1999/5/EK irányelv alapkövetelményeinek és a kapcsolódó rendelkezéseknek.
Dansk	**PLANET Technology Corporation**, erklærer herved, at følgende udstyr **802.11n Wireless Internet 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 Wireless Internet 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 Wireless Internet 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 Corporation**, dat **802.11n Wireless Internet 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 Wireless Internet VDSL2 Router** vastab Euroopa Nõukogu direktiivi 1999/5/EC põhinõuetele ja muudele olulistele tingimustele.	**Polski**	Niniejszym firma **PLANET Technology Corporation**, oświadcza, że **802.11n Wireless Internet 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 Wireless Internet 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 Wireless Internet 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 Wireless Internet 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 Wireless Internet VDSL2 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 Wireless Internet 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 Wireless Internet 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 Wireless Internet 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 Wireless Internet 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 Wireless Internet VDSL2 Router** atbilst Direktīvas 1999/5/EK pamatprasībām un citiem atbilstošiem noteikumiem.	**Svenska**	Härmed intygar, **PLANET Technology Corporation**, att denna **802.11n Wireless Internet VDSL2 Router** står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.