



## Copyright

Copyright © 2014 by PLANET Technology Corp. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission of PLANET.

PLANET makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, this company reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

## Federal Communication Commission Interference Statement



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

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

### FCC Caution:

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

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

- (1) This device may not cause harmful interference
- (2) This Device must accept any interference received, including interference that may cause undesired operation.

## **Federal Communication Commission (FCC) Radiation Exposure Statement**

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

## **R&TTE Compliance Statement**

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

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

## **Safety**

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

## **National Restrictions**

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

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

Russian Federation	None	Only for indoor applications
--------------------	------	------------------------------

### WEEE regulation



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

### Revision

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

Model: VDR-300NU

Rev: 1.0 (January, 2014)

Part No. EM-VDR-300NU\_v1 (2081-AC0360-000)

## Table of Contents

<b>CHAPTER 1.PRODUCT INTRODUCTION .....</b>	<b>8</b>
<b>1.1 Package Contents .....</b>	<b>8</b>
<b>1.2 Product Description .....</b>	<b>9</b>
<b>1.3 Product Features .....</b>	<b>12</b>
<b>1.4 Product Specifications.....</b>	<b>14</b>
<b>CHAPTER 2. HARDWARE INSTALLATION .....</b>	<b>18</b>
<b>2.1 Hardware Description .....</b>	<b>18</b>
2.1.1 Front Panel.....	18
2.1.2 LED Indications .....	18
2.1.3 Rear Panel and Side Panel.....	20
2.1.4 Right Side Panel .....	21
<b>CHAPTER 3. CONNECTING TO THE ROUTER .....</b>	<b>22</b>
<b>3.1 System Requirements.....</b>	<b>22</b>
<b>3.2 Installing the Router.....</b>	<b>22</b>
<b>CHAPTER 4. INSTALLATION GUIDE.....</b>	<b>25</b>
<b>4.1 Configuring PC in Windows 7 .....</b>	<b>25</b>
<b>4.2 Configuring PC in Windows XP .....</b>	<b>27</b>
<b>CHAPTER 5. SYSTEM SETTINGS.....</b>	<b>29</b>
<b>5.1 Device Information .....</b>	<b>30</b>
5.1.1 Summary .....	30
5.1.2 WAN .....	31
5.1.3 Statistics .....	31
5.1.4 Route.....	34
5.1.5 ARP .....	35
5.1.6 DHCP .....	35
<b>5.2 Advanced Setup .....</b>	<b>36</b>
5.2.1 Layer2 Interface .....	36
5.2.2 WAN Service.....	40
5.2.3 3G WAN Service .....	57
5.2.4 LAN Configuration.....	60

5.2.5 NAT .....	63
5.2.6 Security .....	66
5.2.7 Parental Control .....	69
5.2.8 Quality of Service .....	71
5.2.9 Routing .....	74
5.2.10 DNS .....	77
5.2.11 DSL .....	78
5.2.12 UPnP .....	79
5.2.13 DNS Proxy .....	80
5.2.14 Print Server .....	80
5.2.15 DLNA .....	82
5.2.16 Packet Acceleration .....	82
5.2.17 Storage Service .....	83
5.2.18 Interface Grouping .....	87
5.2.19 IP Tunnel .....	88
5.2.20 IPSec .....	90
5.2.21 Certificate .....	91
5.2.22 Power Management .....	95
5.2.23 Multicast .....	96
<b>5.3 Wireless .....</b>	<b>97</b>
5.3.1 Basic Settings .....	97
5.3.2 Security .....	99
5.3.3 MAC Filter .....	108
5.3.4 Wireless Bridge .....	109
5.3.5 Advanced Settings .....	110
5.3.6 Station Info .....	113
<b>5.4 Diagnostics .....</b>	<b>114</b>
5.4.1 Diagnostics .....	114
5.4.2 Fault Management .....	114
<b>5.5 Management .....</b>	<b>116</b>
5.5.1 Settings .....	116
5.5.2 System Log .....	117
5.5.3 SNMP Agent .....	119
5.5.4 TR-69 Client .....	120

5.5.5 Internet Time .....	121
5.5.6 Access Control .....	121
5.5.7 Update Software .....	123
5.5.8 Reboot.....	123
<b>APPENDIX A: PLANET DDNS .....</b>	<b>124</b>
<b>APPENDIX B: PERFORMANCE OF VDSL ROUTER PROFILES .....</b>	<b>126</b>
<b>APPENDIX C: GLOSSARY.....</b>	<b>127</b>

# Chapter 1. Product Introduction

## 1.1 Package Contents

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

**VDR-300NU**



**Quick Installation  
Guide**



**CD-ROM**

(User Manual included)



**Power Adapter**



12V/2A DC output  
100~240V AC input

**Ethernet Cable**



RJ-45 / CAT5E 1.5 meter  
UTP

**Phone Cable**



RJ11 telephone wire

**VDSL Splitter**

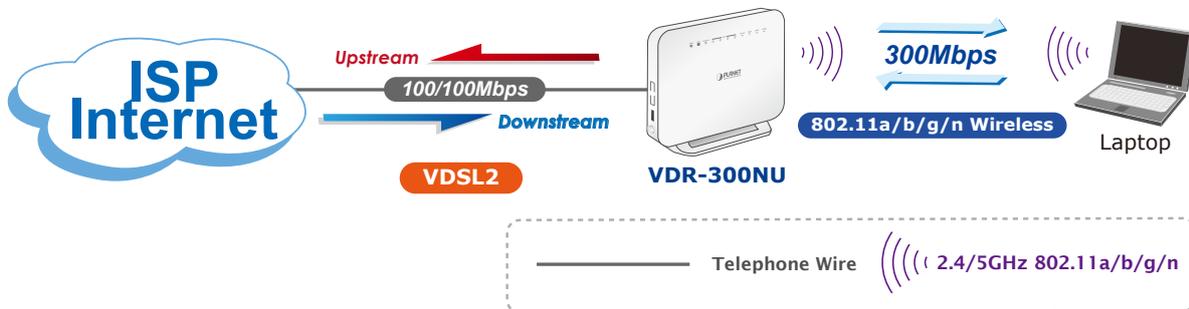


If there is any item missing or damaged, please contact the seller immediately.

## 1.2 Product Description

### High Performance Ethernet over VDSL

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

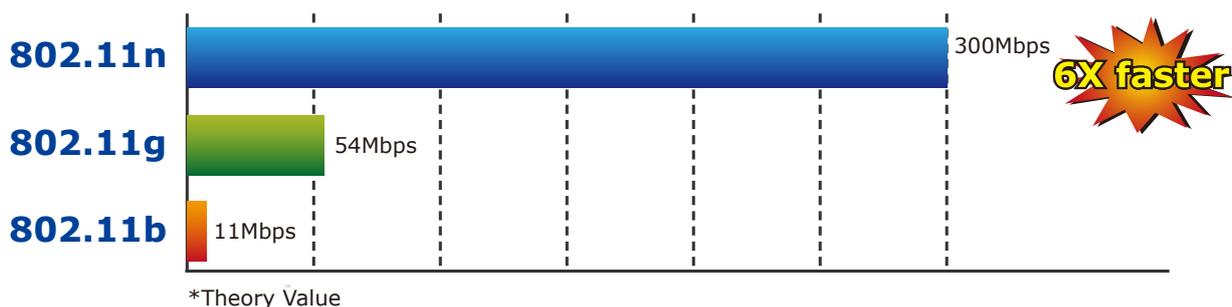


### Delivering High-Demand Service Connectivity for ISP / Triple Play Devices

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

### Dual Band High-Speed 802.11n Wireless

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



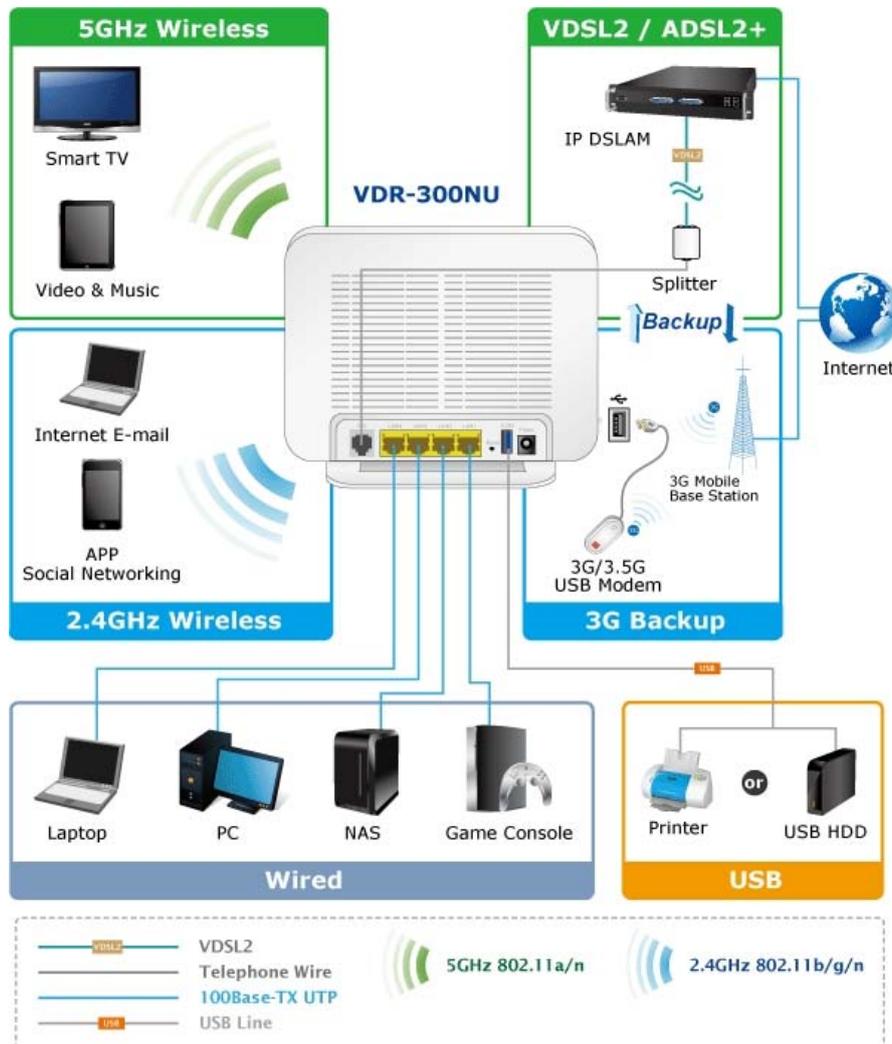
### Secure Wireless Access Control

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



### Multiple Functions for Broadband Communication

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



## Providing Superior Function

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

## More Flexible File Sharing over USB port

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



## 1.3 Product Features

### > **Internet Access Features**

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

### > **Advanced Internet Functions**

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

### > **LAN Features**

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

### > **Wireless Features**

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

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

## 1.4 Product Specifications

Model		VDR-300NU
Product Description		802.11n Dual Band Wireless VDSL2 Router
<b>Hardware Specifications</b>		
Interfaces	LAN	4 x 10/100Base-TX, Auto-Negotiation, Auto MDI/MDI-X RJ45 port
	WAN	1 x RJ-11
	USB	USB 2.0, Type-A, 5V DC/0.5A Output
Antenna		2.4GHz : 2 x 2.5dBi 5GHz: 2 x 2dBi
Button		1 x RESET button 1 x WPS button
LED Indicators		PWR, DSL, LAN1-4, WLAN, WPS, Security
Dimensions (W x D x H)		180 x 145 x 54 mm
Weight		306g
Power		12V DC, 2A
Power Consumption		18W (not including power adapter)
<b>Router Features</b>		
Internet Connection Type		Shares data and Internet access for users, supporting the following internet accesses: <ul style="list-style-type: none"> <li>■ PPPoE</li> <li>■ Dynamic IP</li> <li>■ Static IP</li> </ul>
VDSL Features		<ul style="list-style-type: none"> <li>● ITU-T G.993.2 VDSL2</li> <li>● Supports 8a,8b,12a,12b,17a,30a profile</li> <li>● Supports G.vector</li> <li>● Supports ATM and PTM</li> <li>● Supports G.INP</li> </ul>
ADSL Features		<ul style="list-style-type: none"> <li>● T1.413i2, G.992.1</li> <li>● G.dmt, G.992.2, G.lite</li> <li>● G.992.3 (G.bis/ADSL2)</li> <li>● G.992.5 (ADSL2+)</li> <li>● ITU G.994.1 (G.hs)</li> <li>● Annex L (Reach Extended ADSL2)</li> <li>● Supports ATM forum UNI3.0, 3.1 and 4.0 permanent virtual circuits (PVCs)</li> <li>● Supports CBR, UBR, VBR-rt, VBR-nrt</li> <li>● Supports multiple PVCs</li> <li>● Supports ITU-T i.610F4/F5 OAM</li> </ul>
Bridging Features		<ul style="list-style-type: none"> <li>● Self-learning bridge (IEEE 802.1D Transparent Bridging)</li> <li>● At least 64 learning MAC addresses</li> <li>● Supports IGMP snooping</li> </ul>

<p><b>Protocol Features</b></p>	<ul style="list-style-type: none"> <li>● RFC2684 multiprotocol Encapsulation over ATM Adaptation Layer 5</li> <li>● RFC1483 multiprotocol Encapsulation over ATM Adaptation Layer 5</li> <li>● RFC2364 PPP over ATM ALL5 (PPPoA)</li> <li>● RFC2516 PPP Over Ethernet (PPPoE)</li> <li>● RFC1662 PPP in HDLC-like Framing</li> <li>● RFC1332 PPP Internet Protocol Control Protocol</li> <li>● RFC1577/2225 Classical IP and ARP over ATM (IPoA)</li> <li>● RFC894 A Standard for the Transmission of IP Datagrams over Ethernet Networks</li> <li>● RFC1042 A standard for the Transmission of IP Datagrams over IEEE 802 Networks</li> <li>● MER (a.k.a IP over Ethernet over AAL5)</li> <li>● Supports ALG (Application Level Gateways)</li> <li>● IEEE802.3</li> <li>● IEEE802.3u</li> <li>● IEEE 802.11b</li> <li>● IEEE 802.11g</li> <li>● IEEE 802.11n</li> </ul>
<p><b>Routing Features</b></p>	<ul style="list-style-type: none"> <li>● RFC768 User Datagram Protocol (UDP)</li> <li>● RFC791 Internet Protocol (IP)</li> <li>● RFC792 Internet Control Message Protocol (ICMP)</li> <li>● RFC793 Transmission Control Protocol (TCP)</li> <li>● RFC826 An Ethernet Address Resolution Protocol (ARP)</li> <li>● RFC862 Echo Protocol</li> <li>● Supports IP routing</li> <li>● Supports transparent bridging</li> <li>● Supports source and destination routing</li> <li>● Supports DHCP server/client</li> <li>● Supports UPnP</li> <li>● Supports NAT,NAPT</li> <li>● Supports DMZ</li> <li>● Supports IP QoS</li> <li>● Supports IGMP proxy</li> <li>● Supports IPv6</li> </ul>
<p><b>Security</b></p>	<ul style="list-style-type: none"> <li>● Three-level login including local admin, local user, and remote technical support access</li> <li>● Service access control based on incoming interface: WAN or LAN</li> <li>● Service access control based on source IP addresses</li> <li>● Protects DOS attacks from WAN: SYN flooding, IP surfing, ping of Death, fragile, UDP ECHO (port 7), teardrop, land</li> <li>● PAP (RFC1334), CHAP (RFC1994), MSCHAP for PPP session</li> <li>● IP filter, parental control</li> </ul>

<b>Management</b>	<ul style="list-style-type: none"> <li>● Device Configuration, Management and Update</li> <li>● Web based GUI</li> <li>● Localization support</li> <li>● Embedded web server</li> <li>● Download image via HTTP, TFTP client, TFTP server, FTP server</li> <li>● Command Line Interface via serial port, telnet, or ssh</li> <li>● Menu-driven CLI via serial port or telnet</li> <li>● Universal Plug and Play (UPnP) Internet Gateway Device (IGDv1.0)</li> <li>● WAN Management Protocol (TR-069)</li> <li>● SNMP v1/v2</li> <li>● PSI configuration file upload and download</li> <li>● Date/time update from SNTP Internet Time Server</li> </ul>
<b>Wireless Interface Specifications</b>	
<b>Wireless Standard</b>	IEEE 802.11a/b/g/n
<b>Frequency Band</b>	2.4GHz: 2.412~2.484GHz 5GHz: 5.180~5.825GHz
<b>Modulation Schemes</b>	<ul style="list-style-type: none"> <li>● 802.11g: 64QAM, 16QAM, QPSK, BPSK, DSSS</li> <li>● 802.11b: CCK, DQPSK, DBPSK</li> <li>● HT20 and HT40: 64 QAM, 16QAM, QPSK, BPSK</li> </ul>
<b>Data Transmission Rates</b>	<b>802.11n(40MHz):</b> up to 300 Mbps
	<b>802.11n(20MHz):</b> up to 144.4 Mbps
	<b>802.11g:</b> 54, 48, 36, 24, 18, 12, 9, 6 Mbps per channel, auto fallback for extended range
	<b>802.11b:</b> 1, 5.5, 2, 1 Mbps per channel, auto fallback for extended range
	<b>802.11a:</b> 54, 48, 36, 24, 18, 12, 9, 6 Mbps
<b>RF Power</b>	<p><b>2.4GHz:</b></p> <p>11b: 18±1.5dBm</p> <p>11g: 14.5±1.5dBm</p> <p>11n(20M): 16.5±1.5dBm (MCS0~3) 14.5±1.5dBm (MCS4~7) 16.5±1.5dBm (MCS8~11) 14.5±1.5dBm (MCS12~15)</p> <p>11n(40M): 14±1.5dBm (MCS0~3) 12.5±1.5dBm (MCS4~7) 14±1.5dBm (MCS8~11) 12.5±1.5dBm (MCS12~15)</p>
<b>Wireless Data Encryption</b>	64/128-bit WEP, WPA-PSK, WPA2-PSK, 802.1x encryption, and WPS PBC

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

## Chapter 2. Hardware Installation

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

### 2.1 Hardware Description

#### 2.1.1 Front Panel

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



**Figure 2-1** VDR-300NU Front Panel

#### 2.1.2 LED Indications

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

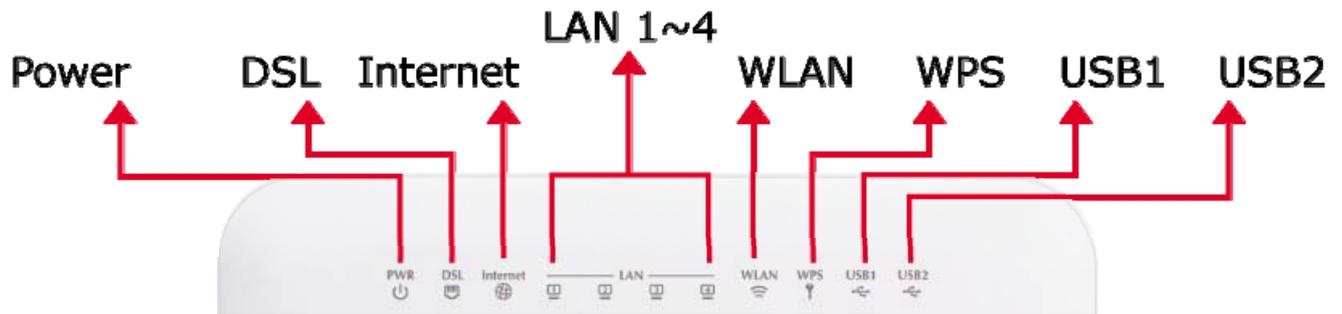


Figure 2-2 VDR-300NU LED

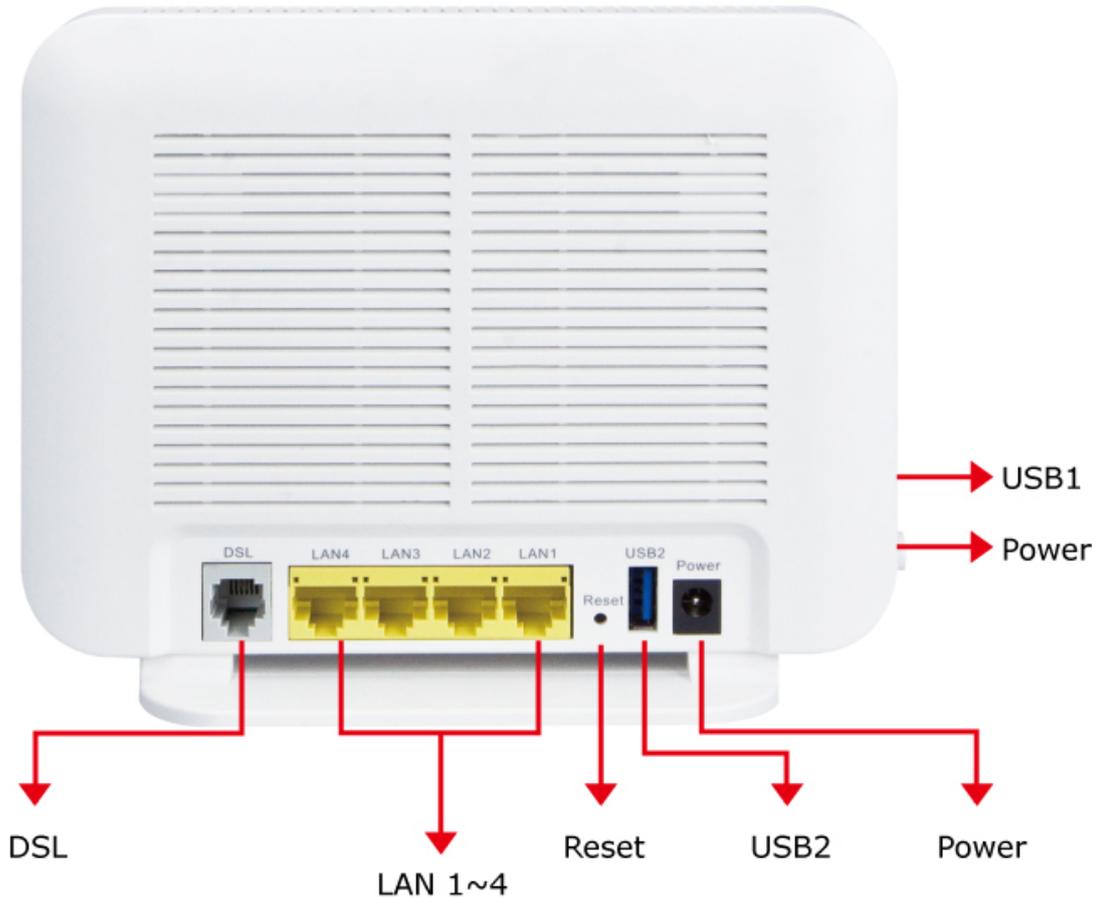
### Front Panel LED Definition

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

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

### 2.1.3 Rear Panel and Side Panel

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



**Figure 2-3** VDR-300NU Rear Panel

#### Rear Panel Port and Button Definition

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

## 2.1.4 Right Side Panel



Figure 2-4 VDR-300NU Side Panel

### Side Panel Interface and Button Definition

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

## Chapter 3. Connecting to the Router

### 3.1 System Requirements

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



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

### 3.2 Installing the Router

Please connect the device to you computer as follows:

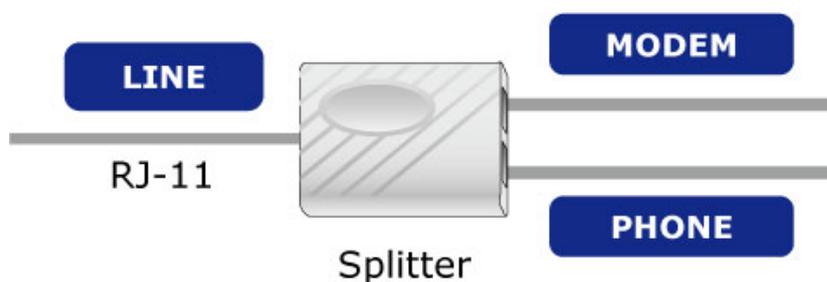
- STEP 1.** Connect the DSL port of the router and the Modem port of the splitter with a telephone cable; connect the phone to the phone port of the splitter through a cable; and connect the incoming line to the Line port of the splitter.

The splitter has three ports:

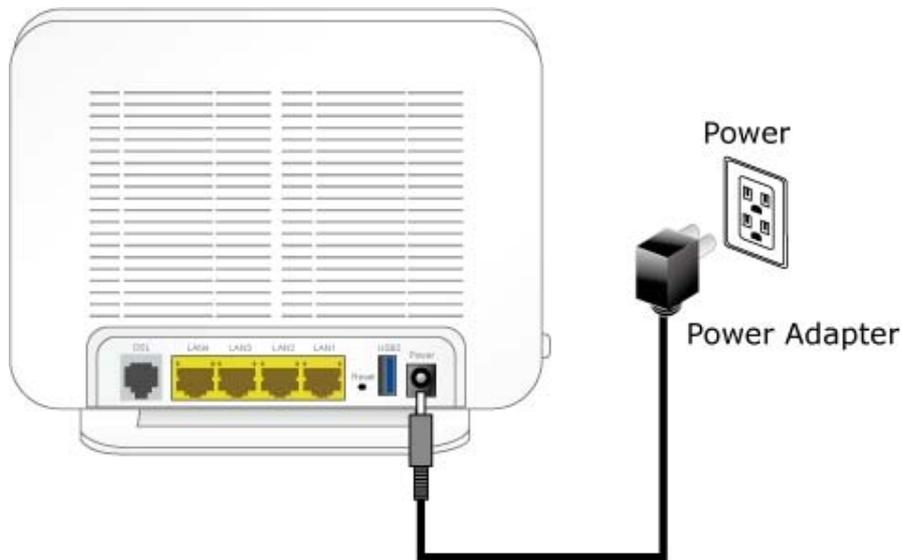
**Line:** Connect to a wall phone jack (RJ-11 jack)

**Modem:** Connect to the Line interface of the router

**Phone:** Connect to a telephone set

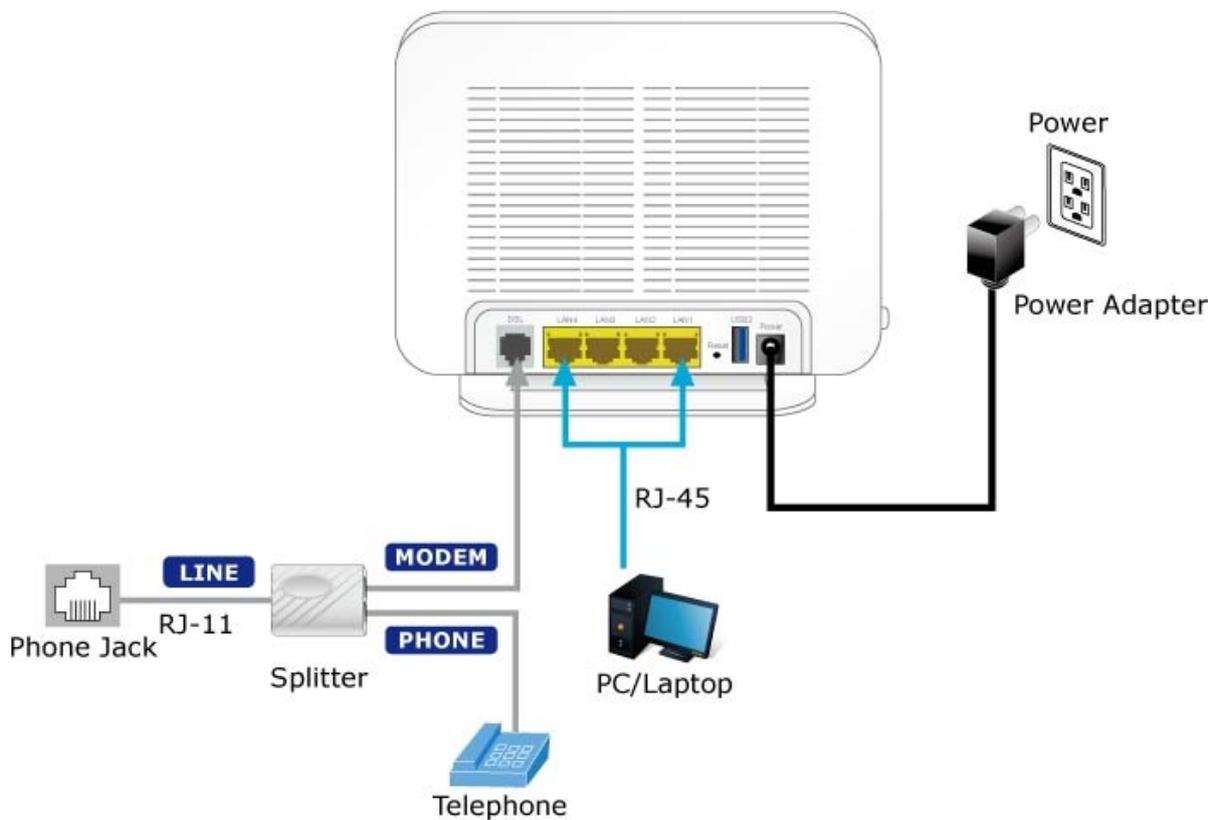


**STEP 2.** Connect the Power Adapter to the VDR-300NU. Check whether the **PWR LED** on the front panel are on accordingly. **Figure3-1** shows the power adapter connection diagram.



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

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



**Figure 3-2: VDR-300NU Connection Diagram**



---

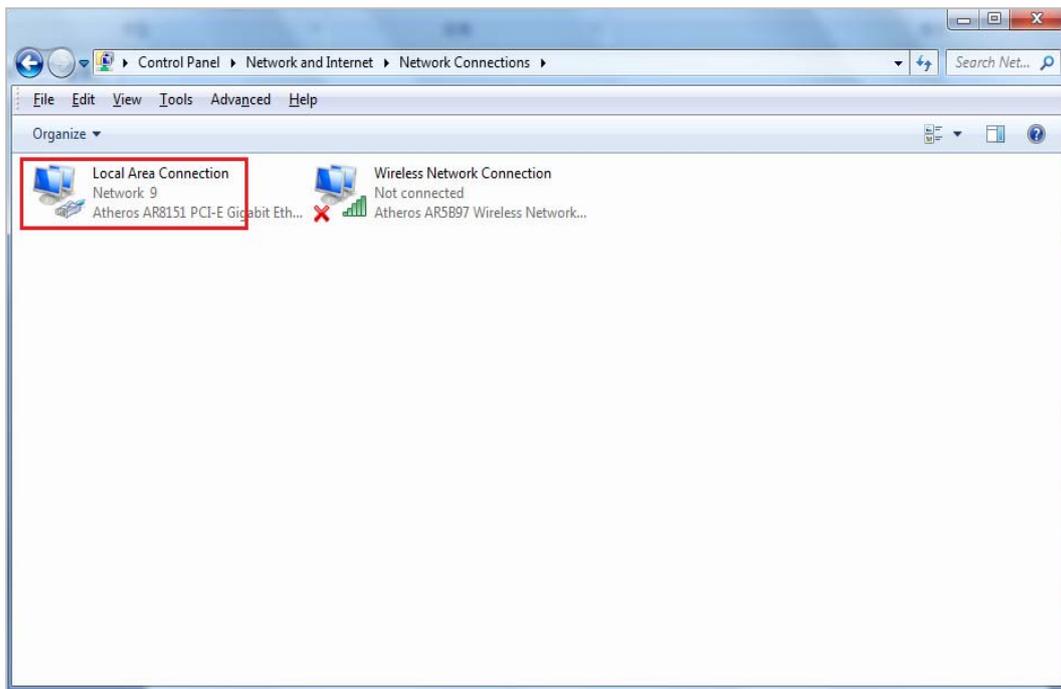
If you use 3G WAN service, connect the 3G USB data card to the **USB** port of the router.

---

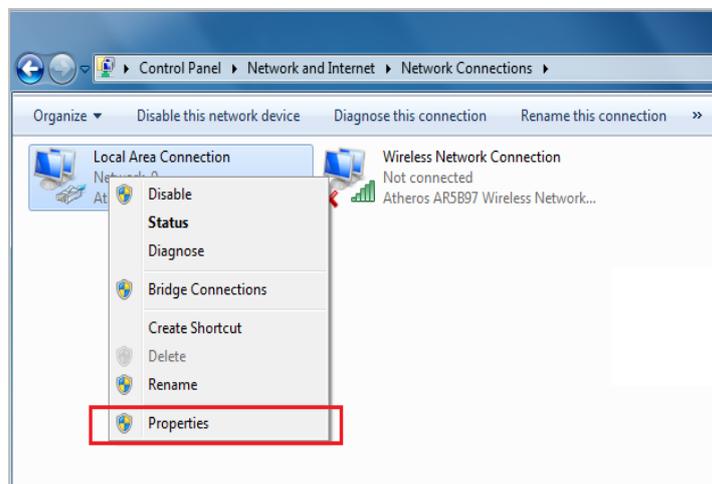
## Chapter 4. Installation Guide

### 4.1 Configuring PC in Windows 7

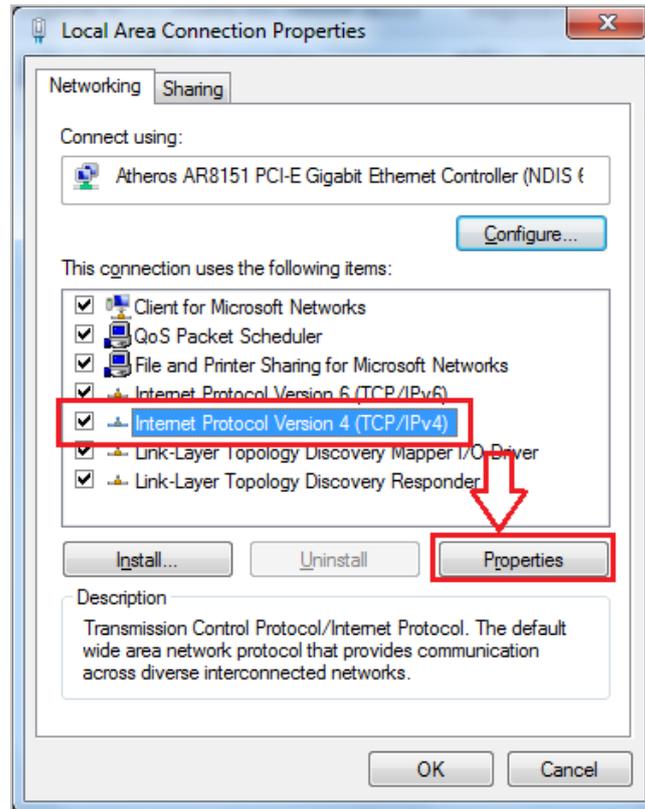
1. Go to **Start / Control Panel / Network and Internet / Network and Sharing Center** and click **Change adapter settings** on the left banner.
2. Double-click **Local Area Connection**.



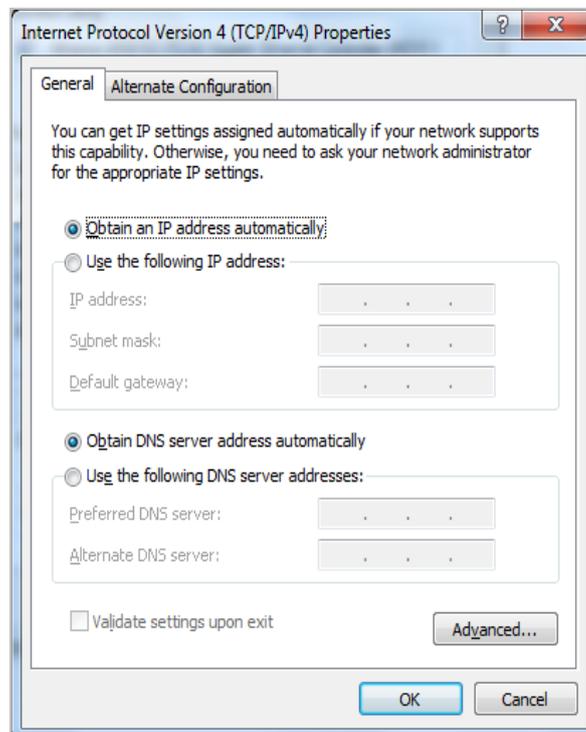
3. In the **Local Area Connection Status** window, click **Properties**.



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



5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** button.
6. Click **OK** to finish the configuration.

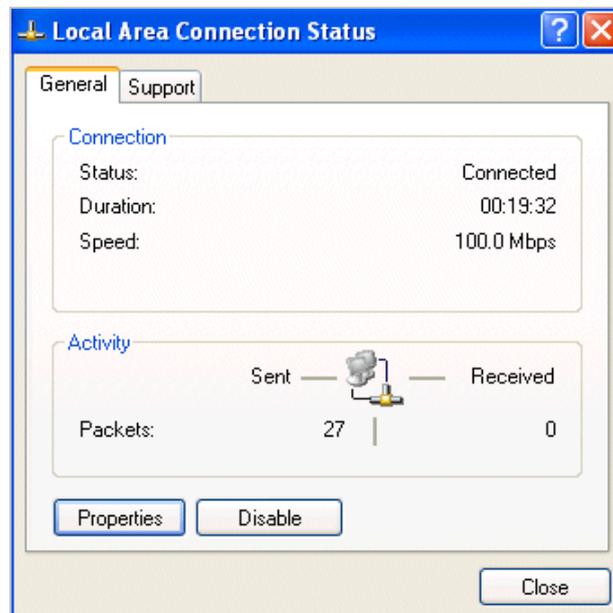


## 4.2 Configuring PC in Windows XP

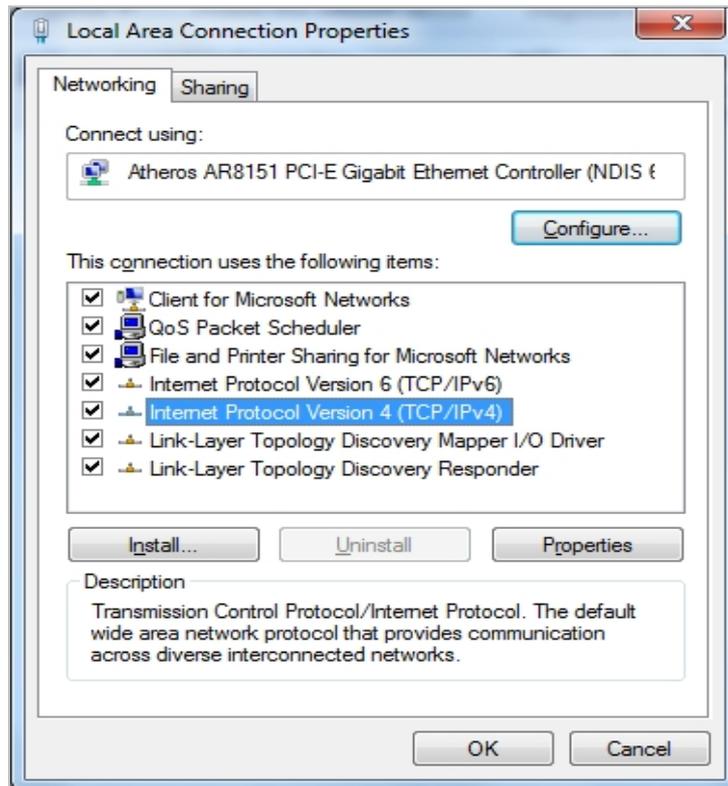
1. Go to **Start / Control Panel (in Classic View)**. In the Control Panel, double-click on **Network Connections**
2. Double-click **Local Area Connection**.



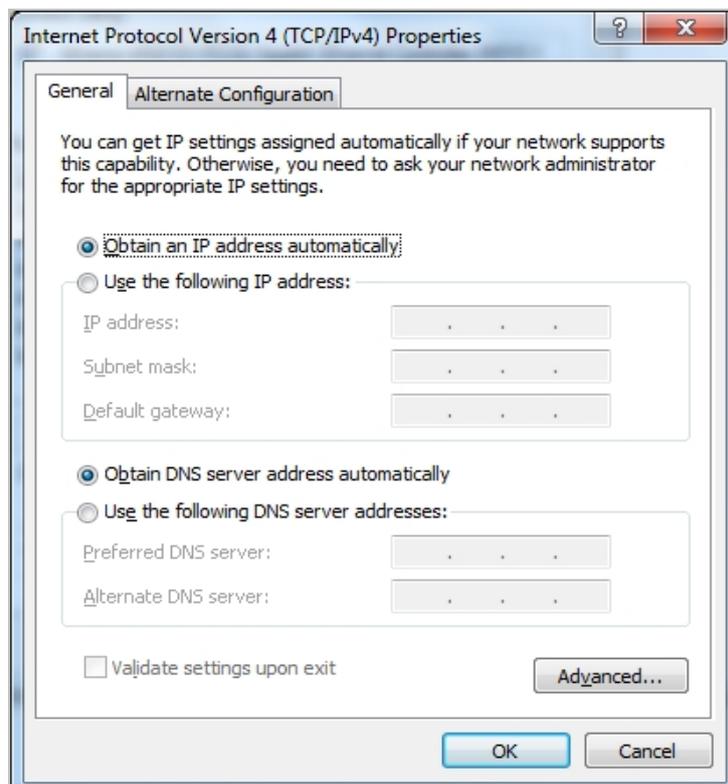
3. In the **Local Area Connection Status** window, click **Properties**.



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



5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** button.
6. Click **OK** to finish the configuration.



## Chapter 5. System Settings

### Determine your Connection Settings

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

### Connecting the VDSL 2 Router to your Network

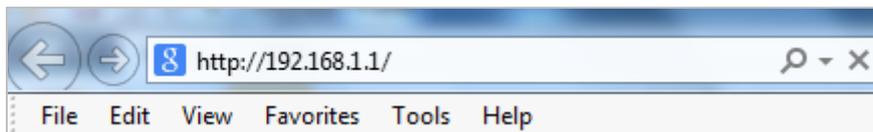
Unlike a simple hub or switch, the setup of the VDSL Router consists of more than simply plugging everything together. Because the Router acts as a DHCP server, you will have to set some values within the Router, and also configure your networked PCs to accept the IP Addresses the Router chooses to assign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

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

### Configuring with Web Browser

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

Save this address in your Favorites for future reference.



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



## 5.1 Device Information

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



Figure 5-1-1

### 5.1.1 Summary

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

 The screenshot shows the web interface for the VDR-300NU router. At the top left is the PLANET logo with the tagline 'Networking & Communication'. At the top right, it says 'VDR-300NU' and '802.11n Dual Band Wireless VDSL2 Router'. On the left side, there is a vertical menu with the following items: Device Info, Summary, WAN, Statistics, Route, ARP, DHCP, Advanced Setup, Wireless, Diagnostics, and Management. The main content area is titled 'Device Info' and contains a table with the following data:
 

Board ID:	VDR-300NU
Manufacturer:	Planet
Serial Number:	021018632680
Build Timestamp:	201312121358
Software Version:	1.0.0
Bootloader (CFE) Version:	1.0.38-114.170
DSL PHY and Driver Version:	A2pv6F038j.d24h
Wireless Driver Version:	6.30.163.23.cpe4.12L
Uptime:	0D 0H 13M 0S

Figure 5-1-2

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

## 5.1.2 WAN

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

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

**Figure 5-1-3**

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

## 5.1.3 Statistics

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

### ■ LAN

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

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

**Figure 5-1-4**

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

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

### ■ WAN Service

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

Statistics -- WAN

Interface	Description	Connected Time	Received				Transmitted			
			Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
atm0.1	br_0_8_35	/	0	0	0	0	0	0	0	0

Reset Statistics

Figure 5-1-5

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

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

## ■ xTM

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

Interface Statistics

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

Figure 5-1-6

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

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

## ■ xDSL

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

Statistics -- xDSL		
Synchronized Time:		
Number of Synchronizations:	0	
Mode:		
Traffic Type:		
Status:	Disabled	
Link Power State:	L3	
	Downstream	Upstream
Line Coding(Trellis):		
SNR Margin (0.1 dB):		
Attenuation (0.1 dB):		
Output Power (0.1 dBm):		
Attainable Rate (Kbps):		
Rate (Kbps):		
Super Frames:		
Super Frame Errors:		
RS Words:		
RS Correctable Errors:		
RS Uncorrectable Errors:		

Figure 5-1-7

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

- **xDSL BER Test**

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

**xDSL BER Test - Start**

The xDSL Bit Error Rate (BER) test determines the quality of the xDSL connection. The test is done by transferring idle cells containing a known pattern and comparing the received data with this known pattern to check for any errors.

Select the test duration below and click "Start".

Tested Time (sec):

Figure 5-1-8

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

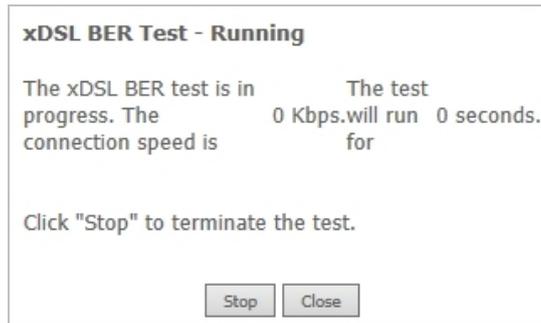


Figure 5-1-9

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

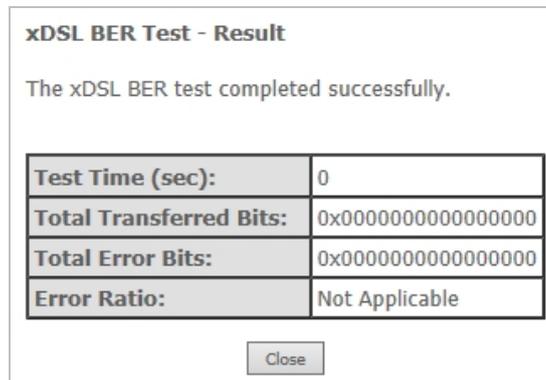


Figure 5-1-10



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

### 5.1.4 Route

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

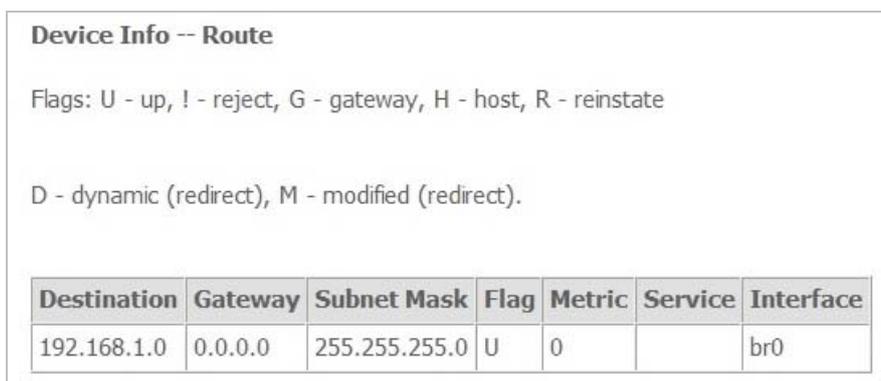


Figure 5-1-11

## 5.1.5 ARP

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

Device Info -- ARP			
IP address	Flags	HW Address	Device
192.168.1.2	Complete	b8:70:f4:b5:e5:da	br0

**Figure 5-1-12**

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

## 5.1.6 DHCP

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

Device Info -- DHCP Leases						
Hostname	MAC Address	IP Address	Connection Type	IP Address Assignment	Status	Expires In
Unknown	00:30:4f:29:48:90	192.168.1.20	Ethernet	Static	Active	0 seconds
ACER6292-PC	00:1e:68:6a:5d:55	192.168.1.2	Ethernet	DHCP	Active	23 hours, 59 minutes, 41 seconds

**Figure 5-1-13**

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

## 5.2 Advanced Setup

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



Figure 5-2-1

### 5.2.1 Layer2 Interface

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

#### ■ ATM Interface

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

DSL ATM Interface Configuration													
Choose Add, or Remove to configure DSL ATM interfaces.													
Interface	Vpi	Vci	DSL Latency	Category	Peak Cell Rate (cells/s)	Sustainable Cell Rate (cells/s)	Max Burst Size (bytes)	Min Cell Rate (cells/s)	Link Type	Connection Mode	IP QoS	MPAAL Prec/Alg/Wght	Remove
atm0	8	35	Path0	UBR					EoA	VlanMuxMode	Support	8/WRR/1	<input type="checkbox"/>
<input type="button" value="Add"/> <input type="button" value="Remove"/>													

Figure 5-2-2

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

**ATM PVC Configuration**

This screen allows you to configure a ATM PVC.

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

Select DSL Latency  
 Path0 (Fast)  
 Path1 (Interleaved)

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

Encapsulation Mode:  ▾

Service Category:  ▾

Minimum Cell Rate:  [cells/s] (-1 indicates no shaping)

Select Scheduler for Queues of Equal Precedence as the Default Queue  
 Weighted Round Robin  
 Weighted Fair Queuing

**Figure 5-2-3**

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

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

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

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

## ■ PTM Interface

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

**DSL PTM Interface Configuration**

Choose Add, or Remove to configure DSL PTM interfaces.

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

**Figure 5-2-4**

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

**PTM Configuration**

This screen allows you to configure a PTM connection.

Select DSL Latency

Path0 (Fast)  
 Path1 (Interleaved)

Select Scheduler for Queues of Equal Precedence as the Default Queue

Weighted Round Robin  
 Weighted Fair Queuing

Default Queue Weight:  [1-63]  
 Default Queue Precedence:  [1-8] (lower value, higher priority)

Default Queue Shaping Rate:  [Kbits/s] (blank indicates no shaping)  
 Default Queue Shaping Burst Size:  [bytes] (shall be >=1600)

**Figure 5-2-5**

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

## ■ ETH Interface

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



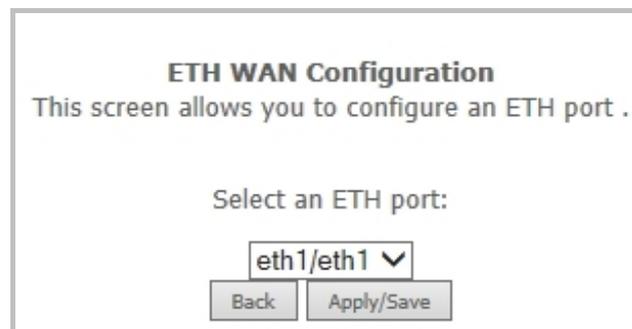
**ETH WAN Interface Configuration**

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

Name	Connection Mode	Remove
------	-----------------	--------

Figure 5-2-6

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



**ETH WAN Configuration**

This screen allows you to configure an ETH port .

Select an ETH port:

eth1/eth1 ▼

Figure 5-2-7

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



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

## 5.2.2 WAN Service

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

**Wide Area Network (WAN) Service Setup**

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

Interface	Description	Type	Vlan802.1p	VlanMuxId	Igmp	NAT	Firewall	IPv4	IPv6	Mld	Remove	Edit	Action
atm0.1	br_0_8_35	Bridge	N/A	N/A	Disabled	Disabled	Disabled	Enabled	Enabled	Disabled	<input type="checkbox"/>	<input type="button" value="edit"/>	

**Figure 5-2-8**

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



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

### ■ Adding a PPPoE WAN Service

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

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

**DSL ATM Interface Configuration**

Choose Add, or Remove to configure DSL ATM interfaces.

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

**Figure 5-2-9**

**DSL PTM Interface Configuration**

Choose Add, or Remove to configure DSL PTM interfaces.

Interface	DSL Latency	PTM Priority	Connection Mode	IP QoS	Remove
ptm0	Path0	Normal&High	VlanMuxMode	Support	<input type="checkbox"/>

**Figure 5-2-10**

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

**WAN Service Interface Configuration**

Select a layer 2 interface for this service

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

atm0/(0\_8\_35)  
 ptm0/(0\_1\_1)

**Figure 5-2-11**

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

**WAN Service Configuration**

Select WAN service type:

PPP over Ethernet (PPPoE)  
 IP over Ethernet  
 Bridging

Enter Service Description:

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

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [0-4094]:

**Figure 5-2-12**

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

**PPP Username and Password**

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

PPP Username:

PPP Password:

PPPoE Service Name:

Authentication Method: AUTO ▼

MTU[576-1492]:

Enable Fullcone NAT

Dial on demand (with idle timeout timer)

Enable IPv4 for this service

PPP IP extension

Use Static IPv4 Address

Enable IPv6 for this service

Enable PPP Debug Mode

Bridge PPPoE Frames Between WAN and Local Ports

**Multicast Proxy**

Enable IGMP Multicast Proxy

**Figure 5-2-13**

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

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

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

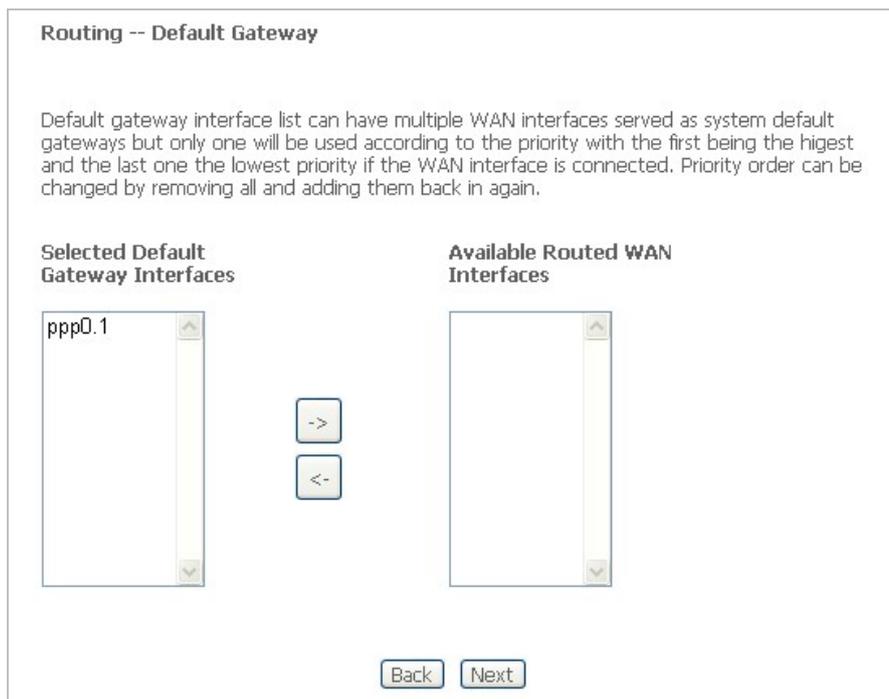


Figure 5-2-14



## ■ Adding an IP over Ethernet WAN service

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

- Step1** First, add a proper ATM or PTM interface for this WAN service at **Layer2 Interface**.
- Step2** On the **WAN Service** page, click the **Add** button to display as **Figure 5-2-11** shows. You can select ATM or PTM Interface for the WAN service and then click **Next**.
- Step3** On this page, select the WAN service type to be **IP over Ethernet**. Click **Next** to continue the setting.

Figure 5-2-17

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

Figure 5-2-18



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

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

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

**Network Address Translation Settings**

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

Enable NAT

Enable Firewall

**Multicast Proxy**

Enable IGMP Multicast

**Figure 5-2-19**

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

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

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

**WAN Setup - Summary**

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

<b>Connection Type:</b>	IPoE
<b>NAT:</b>	Enabled
<b>Full Cone NAT:</b>	Disabled
<b>Firewall:</b>	Enabled
<b>IGMP Multicast:</b>	Disabled
<b>Quality Of Service:</b>	Disabled

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

**Figure 5-2-20**

## ■ Adding a Bridging WAN service

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

- Step1** First, add a proper ATM or PTM interface for this WAN service at **Layer2 Interface**.
- Step2** On the **WAN Service** page, click the **Add** button to display as **Figure 5-2-11**. You can select ATM or PTM Interface for the WAN service and then click **Next**.
- Step3** On this page, select the WAN service type to be **Bridging**. Click **Next** to finish the setting.

**WAN Service Configuration**

Select WAN service type:

PPP over Ethernet (PPPoE)

IP over Ethernet

Bridging

Enter Service Description:

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

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [0-4094]:

Figure 5-2-21

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

**WAN Setup - Summary**

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

<b>Connection Type:</b>	Bridge
<b>NAT:</b>	Disabled
<b>Full Cone NAT:</b>	Disabled
<b>Firewall:</b>	Disabled
<b>IGMP Multicast:</b>	Not Applicable
<b>Quality Of Service:</b>	Disabled

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

Figure 5-2-22

## ■ Adding a PPPoA WAN service

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

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

**ATM PVC Configuration**

This screen allows you to configure a ATM PVC.

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

Select DSL Latency

Path0 (Fast)  
 Path1 (Interleaved)

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

EoA  
 PPPoA  
 IPoA

Encapsulation Mode:  ▼

Service Category:  ▼

Minimum Cell Rate:  [cells/s] (-1 indicates no shaping)

Select Scheduler for Queues of Equal Precedence as the Default Queue

Weighted Round Robin  
 Weighted Fair Queuing

**Figure 5-2-23**

- Step2** Select the DSL link type to be **PPPoA** and select the encapsulation mode to be **VC/MUX** (according to the uplink equipment). After finishing setting, click the **Apply/Save** button to apply the settings.
- Step3** Choose **WAN Service** and click **Add** to display the following page.

**WAN Service Interface Configuration**

Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portId\_vpi\_vci)  
 For PTM interface, the descriptor string is (portId\_high\_low)

Where portId=0 --> DSL Latency PATH0  
 portId=1 --> DSL Latency PATH1  
 portId=4 --> DSL Latency PATH0&1  
 low =0 --> Low PTM Priority not set  
 low =1 --> Low PTM Priority set  
 high =0 --> High PTM Priority not set  
 high =1 --> High PTM Priority set

atm1/(0\_0\_35) ▼

Figure 5-2-24

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

**WAN Service Configuration**

Enter Service Description:

Figure 5-2-25

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

**PPP Username and Password**

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

PPP Username:

PPP Password:

Authentication Method:  ▼

MTU[576-1492]:

Enable Fullcone NAT

Dial on demand (with idle timeout timer)

Enable IPv4 for this service

Use Static IPv4 Address

Enable IPv6 for this service

Enable PPP Debug Mode

**Multicast Proxy**

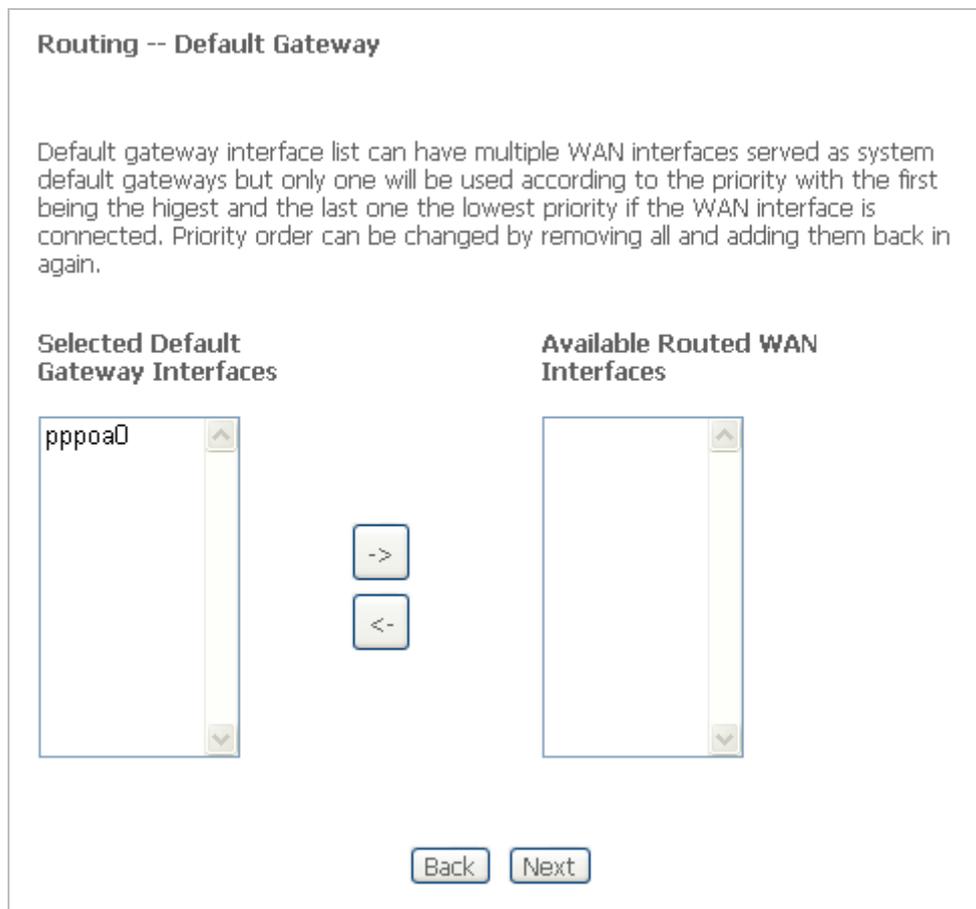
Enable IGMP Multicast Proxy

Figure 5-2-26

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

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

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



**Figure 5-2-27**

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

**DNS Server Configuration**

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

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

Selected DNS Server Interfaces                      Available WAN Interfaces

pppoa0

->

<-

Figure 5-2-28

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

**WAN Setup - Summary**

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

<b>Connection Type:</b>	PPPoA
<b>NAT:</b>	Enabled
<b>Full Cone NAT:</b>	Disabled
<b>Firewall:</b>	Enabled
<b>IGMP Multicast:</b>	Disabled
<b>Quality Of Service:</b>	Enabled

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

Figure 5-2-29

■ **Adding an IPoA WAN service**

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

- Step1** Choose **Advanced Setup > Layer2 Interface > ATM Interface** to display the **DSL ATM Interface Configuration** page. On this page, you need to add a PVC for IPoA mode. Click the **Add** button.
- Step2** Select the DSL link type to be **IPoA**, and select the encapsulation mode to be **LLC/SNAP-ROUTING** (according to the uplink equipment). After finishing setting, click the **Apply/Save** button to save the settings

**ATM PVC Configuration**

This screen allows you to configure a ATM PVC.

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

Select DSL Latency  
 Path0 (Fast)  
 Path1 (Interleaved)

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

Encapsulation Mode:  ▼

Service Category:  ▼

Minimum Cell Rate:  [cells/s] (-1 indicates no shaping)

Select Scheduler for Queues of Equal Precedence as the Default Queue  
 Weighted Round Robin  
 Weighted Fair Queuing

Figure 5-2-30

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

**WAN Service Interface Configuration**

Select a layer 2 interface for this service

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

▼

Figure 5-2-31

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

**WAN Service Configuration**

Enter Service Description:

**Figure 5-2-32**

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

**WAN IP Settings**

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

Enable IPv4 for this service

WAN IP Address:

WAN Subnet Mask:

Primary DNS server:

Secondary DNS server:

Enable IPv6 for this service

**Figure 5-2-33**

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

**Network Address Translation Settings**

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

Enable NAT

Enable Fullcone NAT

ONLY IF REQUIRED -- DISABLES NETWORK ACCELERATION AND SOME SECURITY

Enable Firewall

**Multicast Proxy**

Enable IGMP Multicast

**Figure 5-2-34**

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

**Routing -- Default Gateway**

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

**Selected Default Gateway Interfaces**

ipoa0

**Available Routed WAN Interfaces**

->

<-

Back Next

**Figure 5-2-35**

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

**DNS Server Configuration**

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

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

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

**Selected DNS Server Interfaces**

ipoa0

**Available WAN Interfaces**

->

<-

Back Next

**Figure 5-2-36**

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

**WAN Setup - Summary**

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

<b>Connection Type:</b>	IPoA
<b>NAT:</b>	Enabled
<b>Full Cone NAT:</b>	Enabled
<b>Firewall:</b>	Disabled
<b>IGMP Multicast:</b>	Disabled
<b>Quality Of Service:</b>	Disabled

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

**Figure 5-2-37**

### 5.2.3 3G WAN Service

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

Figure 5-2-38

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

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

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

Figure 5-2-39

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

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

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

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

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

**modem status** SIM CARD INVALID OR NO SIM CARD!

---

**Wide Area Network (WAN) Service For 3G Mobile Setup**  
Choose Add, Remove or Edit to configure a WAN service For 3G Mobile interface.

Interface	Description	Type	Vlan802.1p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	Remove	Edit	Action
ppp3g0	mobile	mobile	N/A	N/A	Disabled	Enabled	Enabled	Disabled	Disabled	--	<input type="button" value="edit"/>	<input type="button" value="Dial"/>

Figure 5-2-40

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



---

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

---

## 5.2.4 LAN Configuration

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

**Local Area Network (LAN) Setup**

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

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Enable IGMP Snooping

Standard Mode

Blocking Mode

Enable LAN side firewall

Disable DHCP Server

Enable DHCP Server

Start IP Address: 192.168.1.2

End IP Address: 192.168.1.254

Primary DNS server: 192.168.1.1

Secondary DNS server: 192.168.1.1

Leased Time (hour): 24

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

Edit DHCP Option 60
Edit DHCP Option
DHCP Advance setup

<b>MAC Address</b>	<b>IP Address</b>	<b>Remove</b>
<span style="border: 1px solid gray; padding: 2px 5px;">Add Entries</span>	<span style="border: 1px solid gray; padding: 2px 5px;">Remove Entries</span>	

Configure the second IP Address and Subnet Mask for LAN interface

**Figure 5-2-41**

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

Configuring the Private IP Address for the DSL Router

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

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

## ■ IPv6 Auto-configuration

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

**IPv6 LAN Auto Configuration**

Note:

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

2: Unique local address must start with "fd". The prefix and the address must be in same network and the prefix length must be 64.

**Enable Unique Local Addresses And Prefix Advertisement**

Randomly Generate

Statically Configure

Address:  (e.g: fd80::1/64)

Prefix:  (e.g: fd80::/64)

Preferred Life Time (hour):

Valid Life Time (hour):

**IPv6 LAN Applications**

Enable DHCPv6 Server and RADVD

Stateless

Stateful

Start interface ID:

End interface ID:

Leased Time (hour):

Figure 5-2-42

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

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

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

## 5.2.5 NAT

### Virtual Servers

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

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

**NAT -- Virtual Servers Setup**

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

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address or Hostname	WAN Interface	LAN Loopback	Enable/Disable	Remove
<input type="button" value="Add"/> <input type="button" value="Save/Apply"/> <input type="button" value="Remove"/>										

Figure 5-2-43

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

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

**NAT -- Virtual Servers**

Select the service name, and enter the server IP address or hostname, and click "Apply/Save" to forward IP packets for this service to the specified server.

**NOTE: The "Internal Port End" cannot be modified directly. Normally, it is set to the same value as "External Port End". However, if you modify "Internal Port Start", then "Internal Port End" will be set to the same value as "Internal Port Start". Remaining number of entries that can be configured:32**

Use Interface:  ▼

Service Name:

Select a Service:  ▼

Custom Service:

Enable LAN Loopback

Server IP Address or Hostname:

Status:  ▼

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

Figure 5-2-44

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

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

## ■ Port Triggering

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

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

**NAT -- Port Triggering Setup**

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

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

Figure 5-2-45

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

**NAT -- Port Triggering**

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application) and click "Save/Apply" to add it.  
**Remaining number of entries that can be configured:32**

Use Interface:

Application Name:

Select an application:

Custom application:

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>
<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>
<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>
<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>
<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>
<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>
<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>
<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>
<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>
<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>

Figure 5-2-46

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

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



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

## ■ DMZ Host

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

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

**NAT -- DMZ Host**

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

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

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

DMZ Host IP Address:

Enable LAN Loopback

**Figure 5-2-47**

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

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

## 5.2.6 Security

### ■ Firewall

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

**Firewall Table**

name	interface	type	defaultaction	bytes	pkts
------	-----------	------	---------------	-------	------

**Firewall's Rule Table**

enabled	IPVersion	PacketLength	DSCP/TC	Protocol	Action	RejectType	IcmpType
---------	-----------	--------------	---------	----------	--------	------------	----------

Add Firewall
Add Rule
Modify Firewall
Modify Rule
Cancel

Remove Firewall
Remove Rule

Figure 5-2-48

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

**Firewall**

a Firewall have a number of Rule which define the behavior of match item

**name:**

**interface**  ▼

**type**  ▼

**defaultaction**  ▼

Figure 5-2-49

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

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

### ■ MAC Filtering Setup

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



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

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

**MAC Filtering Setup**

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

MAC Filtering Policy For Each Interface (maximum 32 entries): (maximum 32 entries):  
**WARNING: Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.**

Interface	Policy	Change
-----------	--------	--------

Choose Add or Remove to configure MAC filtering rules.

Interface	Protocol	Destination MAC	Source MAC	Frame Direction	802.1p Priority	VlanID	Remove

**Figure 5-2-50**

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

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

**Add MAC Filter**

Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click 'Apply' to save and activate the filter.

Protocol Type:

Destination MAC Address:

Source MAC Address:

Frame Direction:

802.1p Priority:

Tag VLAN ID [0-4094]:

WAN Interfaces (Configured in Bridge mode only)

**Figure 5-2-51**

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

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

## 5.2.7 Parental Control

### ■ Time Restriction

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

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

Username	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Remove
<div style="display: flex; justify-content: center; gap: 20px;"> <span style="border: 1px solid gray; padding: 2px 10px;">Add</span> <span style="border: 1px solid gray; padding: 2px 10px;">Remove</span> </div>											

**Figure 5-2-52**

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

**Access Time Restriction**

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

User Name

Browser's MAC Address

Other MAC Address

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

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

Start Blocking Time (hh:mm)

End Blocking Time (hh:mm)

Figure 5-2-53

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

## ■ Url Filter

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

**URL Filter -- Please select the list type first then configure the list entries. Maximum 100 entries can be configured.**

URL List Type:  Exclude  Include

Address	Port	Remove

Figure 5-2-54

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

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

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

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

**Parental Control -- URL Filter Add**

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

URL Address:

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

**Figure 5-2-55**

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

## 5.2.8 Quality of Service

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

**QoS -- Queue Management Configuration**

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

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

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

Enable QoS

**Figure 5-2-56**

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

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



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

## Queue Configuration

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

**QoS Queue Setup**

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

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

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

Figure 5-2-57

The lower integer value for precedence indicates the higher priority.

Note

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

**QoS Queue Configuration**

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

Name:

Enable:  ▾

Interface:  ▾

Figure 5-2-58

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

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

## ■ QoS Classification

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

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

To add a rule, click the **Add** button.  
 To remove rules, check their remove-checkboxes, then click the **Remove** button.  
 The **Enable** button will scan through every rules in the table. Rules with enable-checkbox checked will be enabled. Rules with enable-checkbox un-checked will be disabled.  
 The enable-checkbox also shows status of the rule after page reload.  
 If you disable WMM function in Wireless Page, classification related to wireless will not take effects

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

CLASSIFICATION CRITERIA													
Class Name	Order	Class Intf	Ether Type	SrcMAC/ Mask	DstMAC/ Mask	SrcIP/ PrefixLength	DstIP/ PrefixLength	Proto	SrcPort	DstPort	DSCP Check	TC Check	802.1P Check
<input type="button" value="Add"/> <input type="button" value="Enable"/> <input type="button" value="Remove"/>													

Figure 5-2-59

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

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

**Add Network Traffic Class Rule**

This screen creates a traffic class rule to classify the ingress traffic into a priority queue and optionally mark the DSCP or Ethernet priority of the packet. Click 'Apply/Save' to save and activate the rule.

Traffic Class Name:

Rule Order:  ▾

Rule Status:  ▾

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

Class Interface:  ▾

Ether Type:  ▾

Source MAC Address:

Source MAC Mask:

Destination MAC Address:

Destination MAC Mask:

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

Specify Class Queue (Required):  ▾

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

Mark 802.1p priority:  ▾

- Class non-vlan packets egress to a non-vlan interface will be tagged with VID 0 and the class rule p-bits.  
 - Class vlan packets egress to a non-vlan interface will have the packet p-bits re-

Figure 5-2-60

## 5.2.9 Routing

### ■ Default Gateway

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

**Routing -- Default Gateway**

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

**Selected Default  
Gateway Interfaces**

->

<-

**Available Routed  
WAN Interfaces**

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

Selected WAN Interface NO CONFIGURED INTERFACE ▾

**Figure 5-2-61**

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

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

### ■ Static Route

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

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

IP Version	DstIP/Mask	Gateway	Interface	Metric	Remove

Add

Remove

**Figure 5-2-62**

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

**Routing -- Static Route Add**

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

IP Version:

Destination IP address/prefix length:

Interface:

Gateway IP Address:

(optional: metric number should be greater than or equal to zero)

Metric:

Figure 5-2-63

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

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

## Policy Routing

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

**Policy Routing Setting -- A maximum 7 entries can be configured.**

Policy Name	Source IP	LAN Port	WAN	Default GW	Remove

Figure 5-2-64

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

**Policy Routing Setup**  
 Enter the policy name, policies, and WAN interface then click "Apply/Save" to add the entry to the policy routing table.  
 Note: If selected "IPoE" as WAN interface, default gateway must be configured.

Policy Name:

Physical LAN Port:

Source IP:

Use Interface:

Default Gateway:

Figure 5-2-65

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

## ■ RIP

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

**Routing -- RIP Configuration**

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

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

Interface	Version	Operation	Enabled
atm0.1	2 <input type="text" value="v"/>	Passive <input type="text" value="v"/>	<input type="checkbox"/>

Figure 5-2-66

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

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

## 5.2.10 DNS

### ■ DNS Server

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

**DNS Server Configuration**

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

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

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

<p>Selected DNS Server Interfaces</p> <div style="border: 1px solid black; padding: 5px; min-height: 100px;">atm0.1</div>	<div style="border: 1px solid gray; padding: 2px 5px; margin: 5px 0;">-&gt;</div> <div style="border: 1px solid gray; padding: 2px 5px; margin: 5px 0;">&lt;-</div>	<p>Available WAN Interfaces</p> <div style="border: 1px solid black; padding: 5px; min-height: 100px;">ppp0.1</div>
---	---	---

Figure 5-2-67

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

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

### ■ Dynamic DNS

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

**Dynamic DNS**

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

Choose Add or Remove to configure Dynamic DNS.

Hostname	Username	Service	Interface	Remove
----------	----------	---------	-----------	--------

Add

Remove

Figure 5-2-68

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

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

**Add Dynamic DNS**

This page allows you to add a Dynamic DNS address from DynDNS.org or TZO.

D-DNS provider

Hostname

Interface

**DynDNS Settings**

Username

Password

**Figure 5-2-69**

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

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

### 5.2.11 DSL

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

**DSL Settings**

Select the modulation below.                      Select the profile below.

<input checked="" type="checkbox"/> G.Dmt Enabled <input checked="" type="checkbox"/> G.lite Enabled <input checked="" type="checkbox"/> T1.413 Enabled <input checked="" type="checkbox"/> ADSL2 Enabled <input checked="" type="checkbox"/> AnnexL Enabled <input checked="" type="checkbox"/> ADSL2+ Enabled <input type="checkbox"/> AnnexM Enabled <input checked="" type="checkbox"/> VDSL2 Enabled	<input checked="" type="checkbox"/> 8a Enabled <input checked="" type="checkbox"/> 8b Enabled <input checked="" type="checkbox"/> 8c Enabled <input checked="" type="checkbox"/> 8d Enabled <input checked="" type="checkbox"/> 12a Enabled <input checked="" type="checkbox"/> 12b Enabled <input checked="" type="checkbox"/> 17a Enabled <input checked="" type="checkbox"/> 30a Enabled  US0 <input checked="" type="checkbox"/> Enabled
--	--

Select the phone line pair below.

Inner pair  
 Outer pair

Capability

Bitswap Enable

Figure 5-2-70

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

## 5.2.12 UPnP

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

**UPnP Configuration**

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

Enable UPnP

Figure 5-2-71

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

## 5.2.13 DNS Proxy

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

**DNS Proxy Configuration**

Enable DNS Proxy

Host name of the Broadband Router:

Domain name of the LAN network:

Figure 5-2-72

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

## 5.2.14 Print Server

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



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

**Print Server settings**

This page allows you to enable / disable printer support.

Enable on-board print server.

Figure 5-2-73

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



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

## 5.2.15 DLNA

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



**Digital Media Server settings**

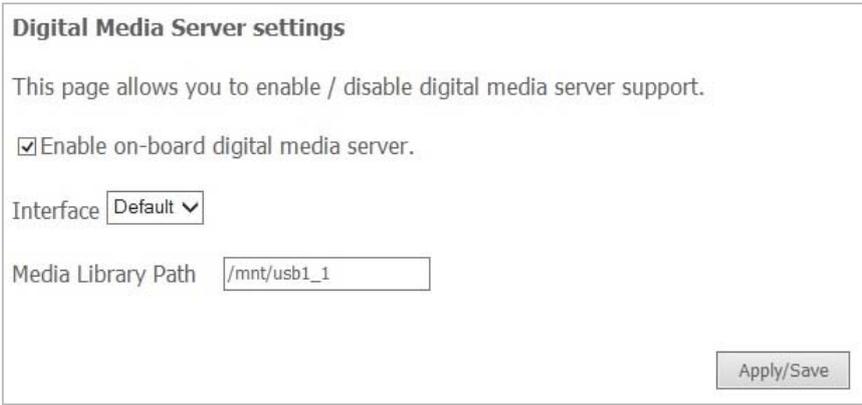
This page allows you to enable / disable digital media server support.

Enable on-board digital media server.

Apply/Save

Figure 5-2-74

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



**Digital Media Server settings**

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

Enable on-board digital media server.

Interface

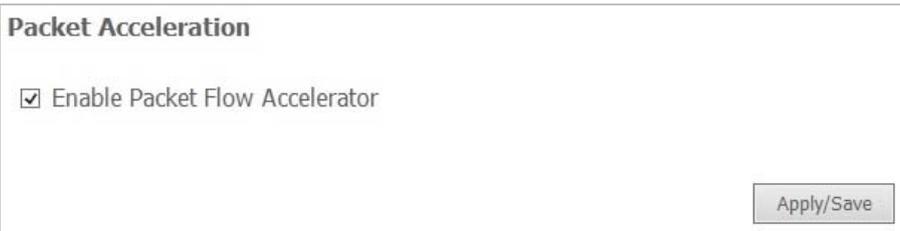
Media Library Path

Apply/Save

Figure 5-2-75

## 5.2.16 Packet Acceleration

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



**Packet Acceleration**

Enable Packet Flow Accelerator

Apply/Save

Figure 5-2-76

## 5.2.17 Storage Service

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

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



### ■ Storage Device Info

Choose **Advanced Setup > Storage Service > Storage Device Info** and the following page appears. This page is used to display the information of the storage device that connects to the DSL router.

Storage Service				
The Storage service allows you to use Storage devices with modem to be more easily accessed				
Volumename	PhysicalMedium	FileSystem	Total Space	Used Space
usb0_1	PhysicalMedium.0	vfat	7703MB	6776MB

Figure 5-2-77

### ■ User Accounts

Choose **Advanced Setup > Storage Service > User Accounts** and the following page appears. You can Choose **Add**, or **Remove** to configure User Accounts.

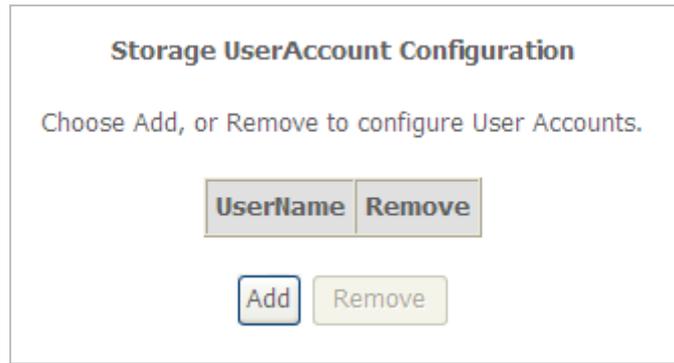
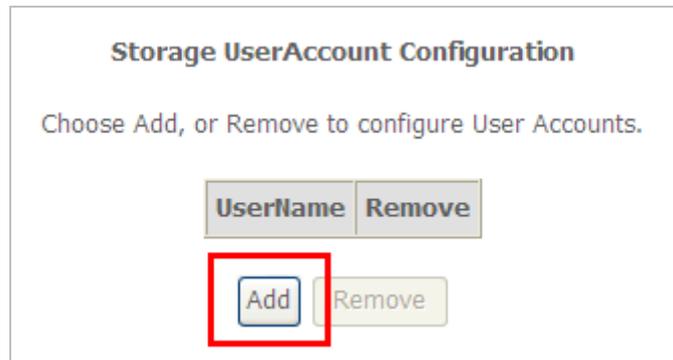


Figure 5-2-78

Operation Instructions:

**Step 1. Create an account.**

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



**Storage User Account Setup**

In the boxes below, enter the user name, password and volume name on which the home directory is to be created.

Username and Password must consists of [A-Z] or [a-z] or [0-9].

Username:

Password:

Confirm Password:

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

**Storage User Account Setup**

In the boxes below, enter the user name, password and volume name on which the home directory is to be created.  
**Username and Password must consists of [A-Z] or [a-z] or [0-9].**

Username:

Password:

Confirm Password:

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

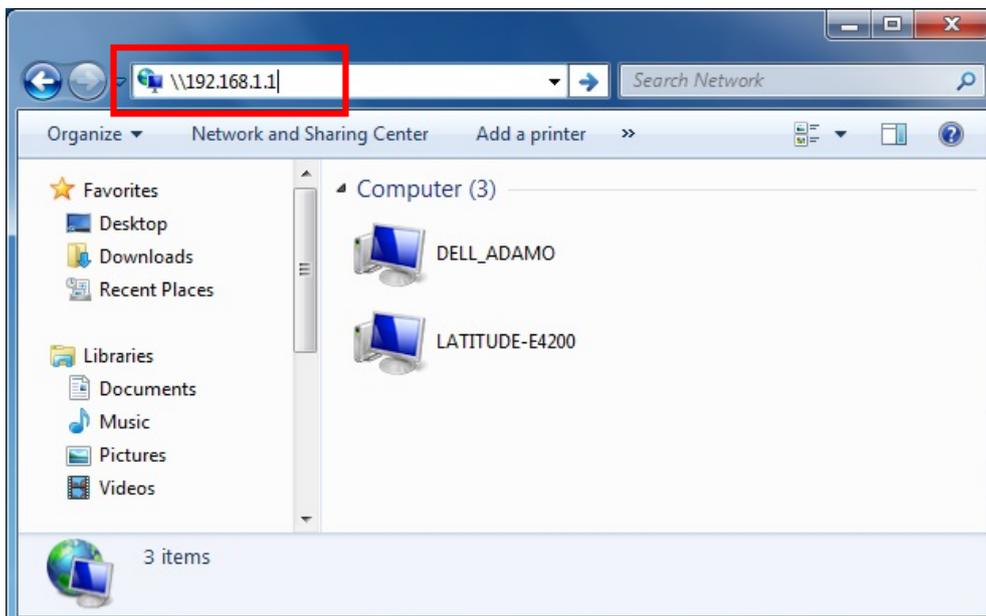
**Storage UserAccount Configuration**

Choose Add, or Remove to configure User Accounts.

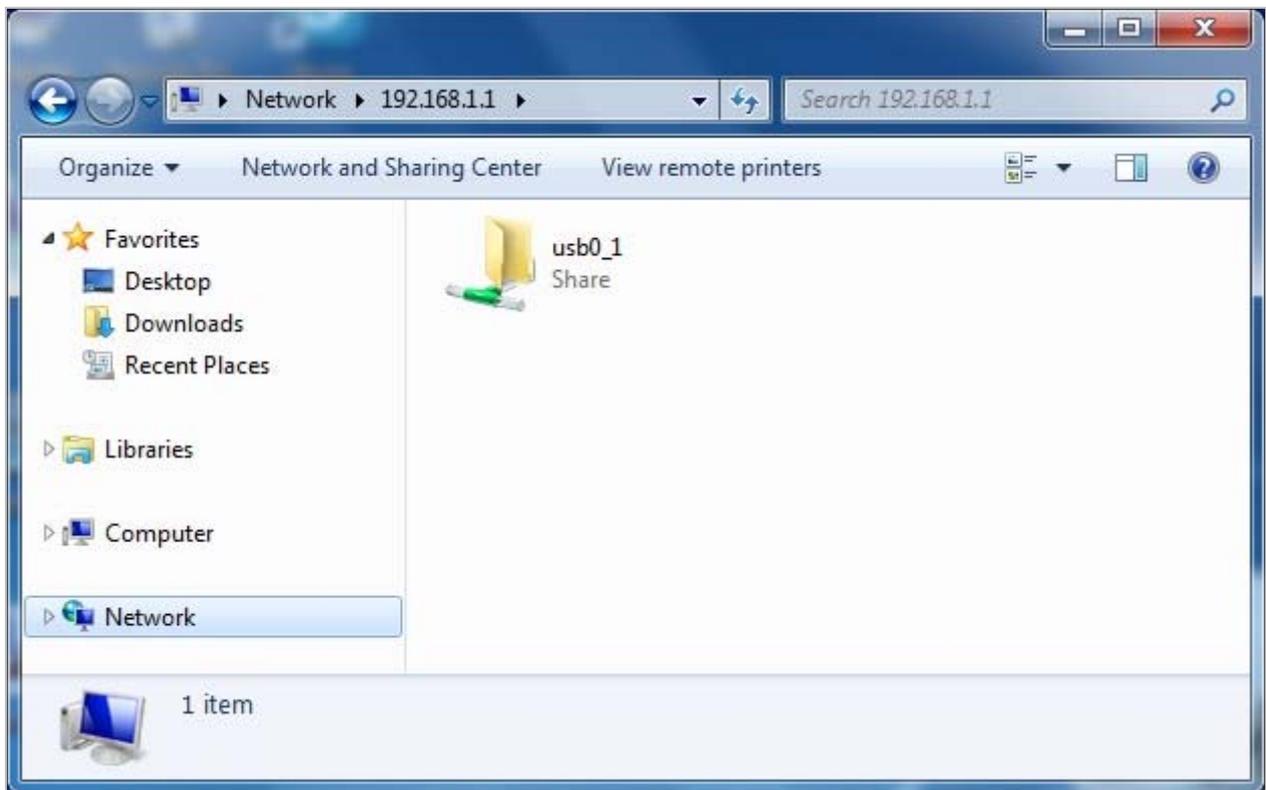
Username	Remove
jack	<input type="checkbox"/>

**Step 2. Access shared file**

To access resources on such storage device, double click **“Computer”** on your PC and enter [\\192.168.1.1](http://192.168.1.1) (The LAN IP address of the router).



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



The filename only supports **Unicode**.

## 5.2.18 Interface Grouping

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

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

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

Group Name	Remove	WAN Interface	LAN Interfaces	Edit
Default		atm0.1	eth1	
		ppp0.1	eth2	
			eth3	
			eth0	
			wl0	
			wl0.1	
			wl0.2	
			wl0.3	

**Figure 5-2-79**

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

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

**Interface grouping Configuration**

To create a new interface group:

1. Enter the Group name and the group name must be unique.
2. Select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports.
3. Click Save/Apply button to make the changes effective immediately.

Group Name:

**Grouped WAN Interfaces**                      **Available WAN Interfaces**

ipoe\_0\_8\_35/atm0.1  
 pppoe\_0\_1\_1/ppp0.1

Figure 5-2-80

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

## 5.2.19 IP Tunnel

### ■ IPv6 in IPv4

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

**IP Tunneling -- 6in4 Tunnel Configuration**

Name	WAN	LAN	Dynamic	IPv4 Mask Length	6rd Prefix	Border Relay Address	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/>							

Figure 5-2-81

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

**IP Tunneling -- 6in4 Tunnel Configuration**

Currently, only 6rd configuration is supported.

Tunnel Name:

Mechanism:

Associated WAN Interface:

Associated LAN Interface:

Manual  Automatic

IPv4 Mask Length:

6rd Prefix with Prefix Length:

Border Relay IPv4 Address:

Figure 5-2-82

## ■ IPv4 in IPv6

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

**IP Tunneling -- 4in6 Tunnel Configuration**

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

Figure 5-2-83

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

**IP Tunneling -- 4in6 Tunnel Configuration**

Currently, only DS-Lite configuration is supported.

Tunnel Name:

Mechanism:

Associated WAN Interface:

Associated LAN Interface:

Manual  Automatic

Remote Address:

Figure 5-2-84

## 5.2.20 IPSec

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

**IPSec Tunnel Mode Connections**

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

Connection Name	Remote Gateway	Local Addresses	Remote Addresses	Remove

**Figure 5-2-85**

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

**IPSec Settings**

IPSec Connection Name

Tunnel Mode  ▼

Remote IPSec Gateway Address (IPv4 address in dotted decimal)

Tunnel access from local IP addresses  ▼

IP Address for VPN

IP Subnetmask

Tunnel access from remote IP addresses  ▼

IP Address for VPN

IP Subnetmask

Key Exchange Method  ▼

Authentication Method  ▼

Pre-Shared Key

Perfect Forward Secrecy  ▼

Advanced IKE Settings

**Figure 5-2-86**

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

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

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

## 5.2.21 Certificate

### Local

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

Figure 5-2-87

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

#### Creating a New Certificate Request

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

Figure 5-2-88

On this page, please set the following parameters.

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

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

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

**Certificate signing request**  
 Certificate signing request successfully created. Note a request is not yet functional - have it signed by a Certificate Authority and load the signed certificate to this device.

<b>Name</b>	test
<b>Type</b>	request
<b>Subject</b>	CN=test/O=Planet/ST=test/C=US
<b>Signing Request</b>	<pre> -----BEGIN CERTIFICATE REQUEST----- MIIBezCB5QIBADA8MQ0wCwYDVQQDEwR0ZXN0MQ8wDQYDVQQKEwZQbGFuZXMxDTAL BgNVBAGTBHRlc3QxCzAJBgNVBAYTA1VTMIGfMA0GCSCqGSIs3DQEBAAQAA4GNADCB iQKBgQDZixMTZKUPtGTLGdBMca9hp6ILfJHQE0OFfdUx+phlVdmmwCqfgEepISynI 48NqaCPWhc120+mFycCyIc/tZj0XzujrtP18/NV27YOauvfSAZQ9ZYr7m90trcV Y/albnNHZu8NjARo6dy1B8fdX295gyijj15x3N8aNWGd0UntW5QIDAQABoAAwDQYJ KoZlhvcNAQEEBQADgYEA+Kklw/xhUpqGowu4C/kDfBWSb70Jsn8Z8Ael0g1Tub49 DoZvKs+XBEG+iqu thLbWxwdnS4zXGTZl f+y+jUXX9dXiBSrxdJnLJdk70h5+y7 duh+z0GuvoUwxuNY/SuN+Kwbd0AYDAxh1H2m4aGkAVeXQBSsWHW5xc1thmXAikA= -----END CERTIFICATE REQUEST-----                     </pre>

Figure 5-2-89

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

**Figure 5-2-90**

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

#### ■ Importing an Existing Local Certificate

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

**Figure 5-2-91**

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

## ■ Trusted CA

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

**Trusted CA (Certificate Authority) Certificates**

Add, View or Remove certificates from this page. CA certificates are used by you to verify peers' certificates.  
 Maximum 4 certificates can be stored.  
**Notice: Import and Remove Certificate need reboot the gateway**

Name	Subject	Type	Action
<input type="button" value="Import Certificate"/>			

**Figure 5-2-92**

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

**Import CA certificate**  
 Enter certificate name and paste certificate content.  
**Notice: If certificate use for tr069, the Certificate Name must be "acscert"**

Certificate Name:

Certificate: 

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

**Figure 5-2-93**

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

## 5.2.22 Power Management

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

**Power Management**

This page allows control of Hardware modules to evaluate power consumption. Use the control buttons to select the desired option, click **Apply** and check the status response.

---

**MIPS CPU Clock divider when Idle**  
 Enable    Status: **Disabled**

---

**Wait instruction when Idle**  
 Enable    Status: **Enabled**

---

**DRAM Self Refresh**  
 Enable    Status: **Enabled**

---

**Energy Efficient Ethernet**

<input checked="" type="checkbox"/>	<b>Ethernet Auto Power Down and Sleep</b>	Number of ethernet interfaces:
Enable	Status: <input checked="" type="checkbox"/>	

Figure 5-2-94

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

## 5.2.23 Multicast

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

<b>IGMP Configuration</b>	
Enter IGMP protocol configuration fields if you want modify default values shown below.	
<b>NOTE: Query Interval is advised to no larger than 125s.</b>	
Default Version:	<input type="text" value="3"/>
Query Interval (s):	<input type="text" value="125"/>
Query Response Interval (1/10s):	<input type="text" value="100"/>
Last Member Query Interval (1/10s):	<input type="text" value="10"/>
Robustness Value:	<input type="text" value="2"/>
Maximum Multicast Data Sources (for IGMPv3):	<input type="text" value="10"/>
Fast Leave Enable:	<input checked="" type="checkbox"/>
Mebership Join Immediate (IPTV):	<input type="checkbox"/>
<b>MLD Configuration</b>	
Enter MLD protocol (IPv6 Multicast) configuration fields if you want modify default values shown below.	
Default Version:	<input type="text" value="2"/>
Query Interval (s):	<input type="text" value="125"/>
Query Response Interval (1/10s):	<input type="text" value="100"/>
Last Member Query Interval (1/10s):	<input type="text" value="10"/>
Robustness Value:	<input type="text" value="2"/>
Maximum Multicast Data Sources (for mldv2):	<input type="text" value="10"/>
Fast Leave Enable:	<input checked="" type="checkbox"/>

**Figure 5-2-95**

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

## 5.3 Wireless

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



Figure 5-3-1

### 5.3.1 Basic Settings

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

**Wireless -- Basic**

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements. Click 'Apply/Save' to configure the basic wireless options.

Enable Wireless

Enable Wireless Hotspot2.0 [WPA2 is required!]

Hide Access Point

Clients Isolation

Disable WMM Advertise

Enable Wireless Multicast Forwarding (WMF)

SSID:

BSSID: 02:10:18:63:26:81

Country:

Max Clients:

Figure 5-3-2

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

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

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

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

## 5.3.2 Security

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

**Wireless -- Security**

This page allows you to configure security features of the wireless LAN interface.  
You may setup configuration manually  
OR  
through WiFi Protected Setup(WPS)  
Note: When both STA PIN and Authorized MAC are empty, PBC is used. If Hide Access Point enabled or Mac filter list is empty with "allow" chosen, WPS2 will be disabled

**WPS Setup**

Enable WPS:

**Manual Setup AP**

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

Select SSID:

Network Authentication:

WEP Encryption:

**Figure 5-3-3**

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



## ■ WPS Setup

**WPS Setup**

Enable **WPS**

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

Push-Button  
 Enter STA PIN  Use AP

PIN

Set **WPS AP Mode**

Setup **AP** (Configure all security settings with an external registrar)

Device **PIN**  [Help](#)

**Figure 5-3-4**

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

- PIN entry, a mandatory method of setup for all WPS certified devices.
  - Enter STA PIN:** If you select it, you need to enter the station PIN from client.
  - Use AP PIN:** The PIN is generated by AP.
- Push button configuration (PBC), an actual push button on the hardware or through a simulated push button in the software. (This is an optional method on wireless client).

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



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

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

## ■ Manual Setup AP

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

**Manual Setup AP**

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

Select SSID:

Network Authentication:

WEP Encryption:

Figure 5-3-5

■ Open Mode

**Manual Setup AP**

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

Select SSID:

Network Authentication:

WEP Encryption:

Encryption Strength:

Current Network Key:

Network Key 1:

Network Key 2:

Network Key 3:

Network Key 4:

Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys  
 Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys

Figure 5-3-6

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

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

■ **Shared Mode**

**Manual Setup AP**

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

Select SSID:

Network Authentication:

WEP Encryption:

Encryption Strength:

Current Network Key:

Network Key 1:

Network Key 2:

Network Key 3:

Network Key 4:

Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys  
 Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys

**Figure 5-3-7**

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

■ **802.1x**

**Manual Setup AP**

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

Select SSID:

Network Authentication:

RADIUS Server IP Address:

RADIUS Port:

RADIUS Key:

WEP Encryption:

Encryption Strength:

Current Network Key:

Network Key 1:

Network Key 2:

Network Key 3:

Network Key 4:

Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys  
Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys

Figure 5-3-8

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

## ■ WPA Mode

**Manual Setup AP**

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

Select SSID:

Network Authentication:

WPA Group Rekey Interval:

RADIUS Server IP Address:

RADIUS Port:

RADIUS Key:

WPA/WAPI Encryption:

WEP Encryption:

Figure 5-3-9

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

## ■ WPA-PSK Mode

**Manual Setup AP**

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

Select SSID:

Network Authentication:

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

WPA Group Rekey Interval:

WPA/WAPI Encryption:

WEP Encryption:

**Figure 5-3-10**

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

## ■ WPA2 Mode

**Manual Setup AP**

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

Select SSID:

Network Authentication:

WPA2 Preauthentication:

Network Re-auth Interval:

WPA Group Rekey Interval:

RADIUS Server IP Address:

RADIUS Port:

RADIUS Key:

WPA/WAPI Encryption:

WEP Encryption:

Figure 5-3-11

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

## ■ WPA2-PSK

**Manual Setup AP**

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

Select SSID:

Network Authentication:

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

WPA Group Rekey Interval:

WPA/WAPI Encryption:

WEP Encryption:

**Figure 5-3-12**

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

## ■ Mixed WPA2/WPA

**Manual Setup AP**

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

Select SSID:

Network Authentication:

WPA2 Preauthentication:

Network Re-auth Interval:

WPA Group Rekey Interval:

RADIUS Server IP Address:

RADIUS Port:

RADIUS Key:

WPA/WAPI Encryption:

WEP Encryption:

**Figure 5-3-13**

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

## ■ Mixed WPA2/WPA-PSK

**Manual Setup AP**

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

Select SSID:

Network Authentication:

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

WPA Group Rekey Interval:

WPA/WAPI Encryption:

WEP Encryption:

**Figure 5-3-14**

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

### 5.3.3 MAC Filter

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

**Wireless -- MAC Filter**

Select SSID:

MAC Restrict Mode:  Disabled  Allow  Deny

MAC Address	Remove
-------------	--------

**Figure 5-3-15**

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

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

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

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

**Wireless -- MAC Filter**

Enter the MAC address and click 'Apply/Save' to add the MAC address to the wireless MAC address filters.

MAC Address:

**Figure 5-3-16**

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

### 5.3.4 Wireless Bridge

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

**Wireless -- Bridge**

This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disable access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access. Click "Refresh" to update the remote bridges. Wait for few seconds to update. Click "Apply/Save" to configure the wireless bridge options.

AP Mode:

Bridge Restrict:

Remote Bridges MAC Address:

**Figure 5-3-17**

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

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

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

### 5.3.5 Advanced Settings

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

**Wireless -- Advanced**  
 This page allws you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used.  
 Click 'Apply/Save' to configure the advanced wireless options.

Band:  Current: 11  
(interference: acceptable)

Channel:

Auto Channel Timer(min)   
 802.11n/EWC:

Bandwidth:  Current: 20MHz

Control Sideband:  Current: N/A

802.11n Rate:

802.11n Protection:

Support 802.11n Client Only:

RIFS Advertisement:

OBSS Co-Existance:

RX Chain Power Save:  Power Save status: Full Power

Figure 5-3-18

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

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

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

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

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



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

### 5.3.6 Station Info

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



**Figure 5-3-19**

This page shows the authenticated wireless stations and their status.

## 5.4 Diagnostics

### 5.4.1 Diagnostics

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

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

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

**ipoe\_0\_8\_35 Diagnostics**

Your modem is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.

**Test the connection to your local network**

Test your eth1 Connection:	<b>PASS</b>	<a href="#">Help</a>
Test your eth2 Connection:	<b>FAIL</b>	<a href="#">Help</a>
Test your eth3 Connection:	<b>FAIL</b>	<a href="#">Help</a>
Test your eth0 Connection:	<b>PASS</b>	<a href="#">Help</a>
Test your Wireless Connection:	<b>PASS</b>	<a href="#">Help</a>

**Test the connection to your DSL service provider**

Test xDSL Synchronization:	<b>FAIL</b>	<a href="#">Help</a>
Test ATM OAM F5 segment ping:	<b>DISABLED</b>	<a href="#">Help</a>
Test ATM OAM F5 end-to-end ping:	<b>DISABLED</b>	<a href="#">Help</a>

**Test the connection to your Internet service provider**

Ping default gateway:	<b>FAIL</b>	<a href="#">Help</a>
Ping primary Domain Name Server:	<b>FAIL</b>	<a href="#">Help</a>

Next Connection  
Test    Test With OAM F4

Figure 5-4-1

### 5.4.2 Fault Management



The Fault Management is only available for VDSL PTM

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

**802.1ag Connectivity Fault Management**

This diagnostic is only used for VDSL PTM mode.

Maintenance Domain (MD) Level:

Destination MAC Address:

802.1Q VLAN ID: [0-4095]

**VDSL Traffic Type:**

**Test the connection to another Maintenance End Point (MEP)**

**Loopback Message (LBM):**

**Find Maintenance End Points (MEPs)**

Linktrace Message (LTM):				

Figure 5-4-2

## 5.5 Management

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

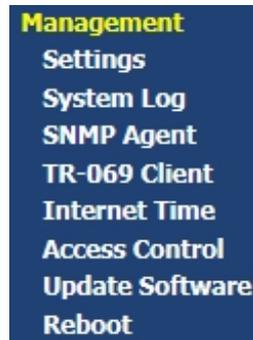


Figure 5-5-1

### 5.5.1 Settings

#### ■ Backup

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

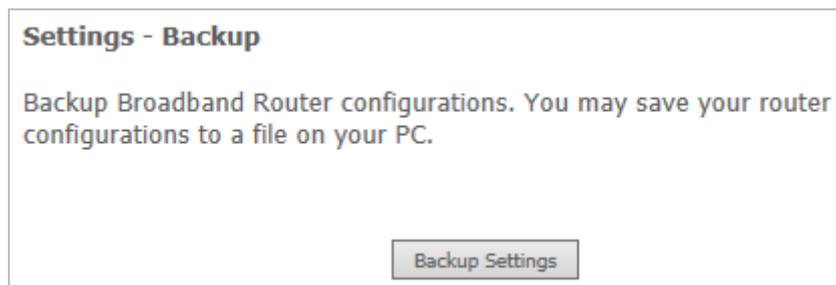


Figure 5-5-2

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

#### ■ Update

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

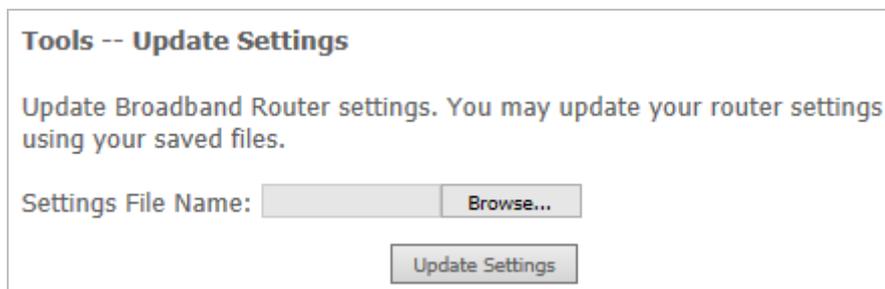


Figure 5-5-3

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

## ■ Restore Default

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

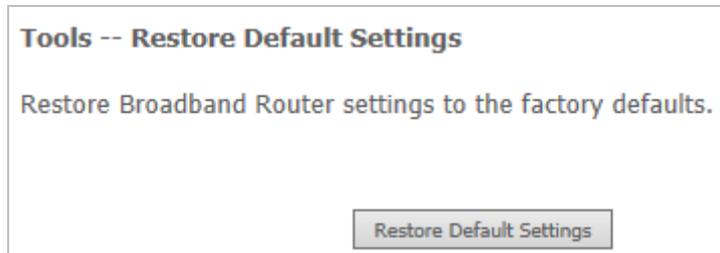


Figure 5-5-4

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

## 5.5.2 System Log

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

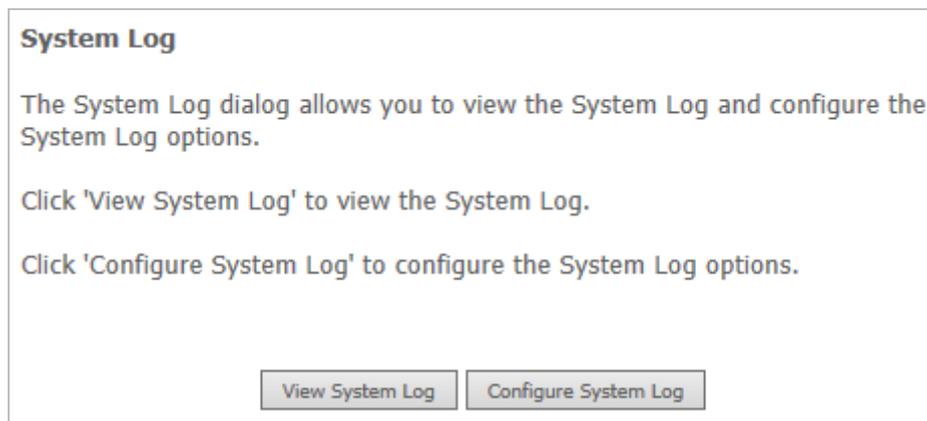


Figure 5-5-5

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

## ■ Configuring the System Log

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

**System Log -- Configuration**

If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.

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

Log:             Disable  Enable

Log Level:         ▼

Display Level:    ▼

Mode:             ▼

**Figure 5-5-6**

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

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

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



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

## ■ View System Log

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

**System Log**

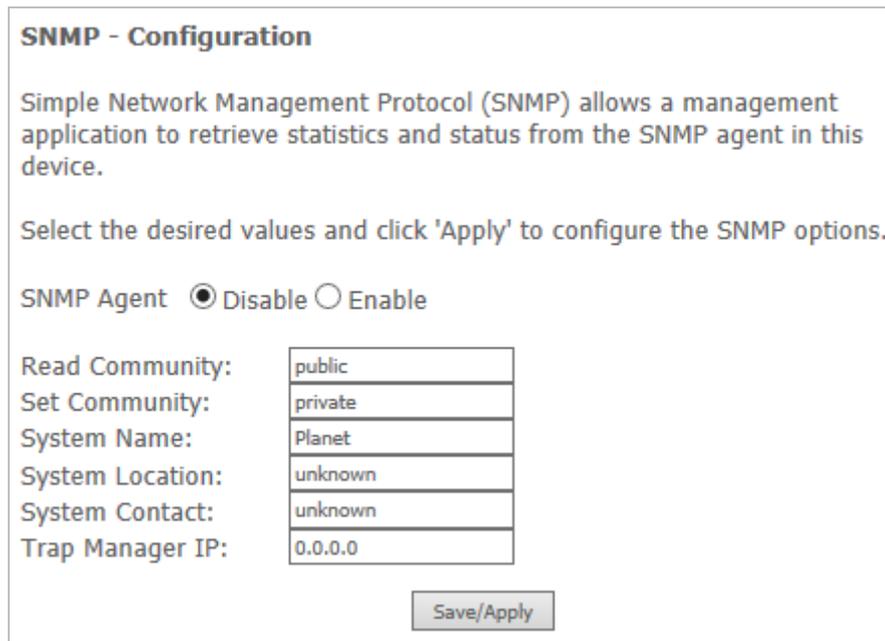
Date/Time	Facility	Severity	Message

**Figure 5-5-7**

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

### 5.5.3 SNMP Agent

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



**SNMP - Configuration**

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

Select the desired values and click 'Apply' to configure the SNMP options.

SNMP Agent  Disable  Enable

Read Community:	public
Set Community:	private
System Name:	Planet
System Location:	unknown
System Contact:	unknown
Trap Manager IP:	0.0.0.0

**Figure 5-5-8**

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

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

## 5.5.4 TR-69 Client

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

**TR-069 client - Configuration**

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

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

Enable WAN Management Protocol (TR-069).  
 Inform  Disable  Enable

Inform Interval:

ACS URL:

ACS User Name:

ACS Password:

WAN Interface used by TR-069 client:

Display SOAP messages on serial console  Disable  Enable

Connection Request Authentication

Connection Request User Name:

Connection Request Password:

Connection Request Port:

Connection Request URL:

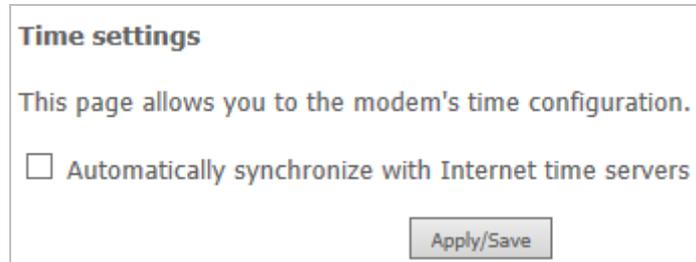
**Figure 5-5-9**

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

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

## 5.5.5 Internet Time

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



**Time settings**

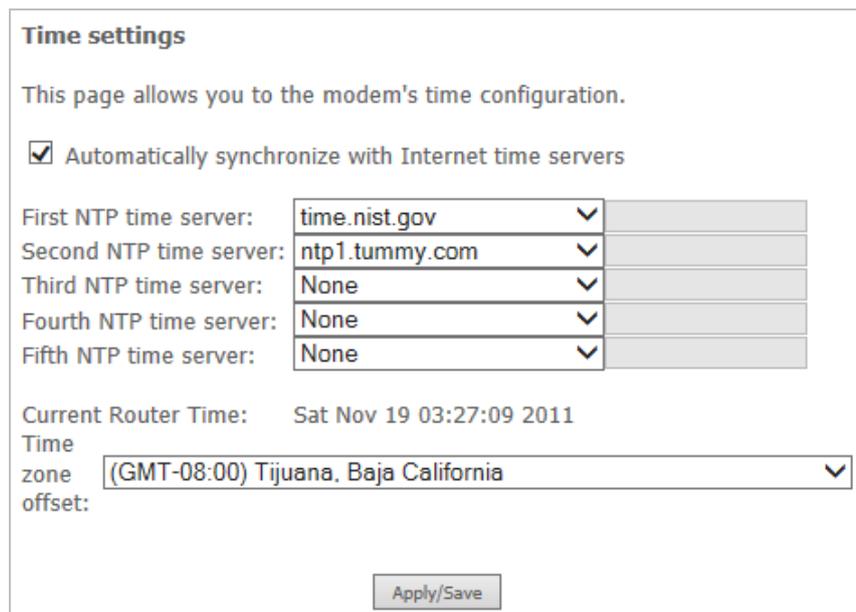
This page allows you to the modem's time configuration.

Automatically synchronize with Internet time servers

Apply/Save

**Figure 5-5-10**

On this page, you may configure the router to synchronize its time with the Internet time servers. After enabling **Automatically synchronize with Internet time servers**, the following page appears.



**Time settings**

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

Automatically synchronize with Internet time servers

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

Current Router Time: Sat Nov 19 03:27:09 2011

Time zone offset: (GMT-08:00) Tijuana, Baja California ▼

Apply/Save

**Figure 5-5-11**

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

## 5.5.6 Access Control

### ■ Passwords

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

**Access Control -- Passwords**

Access to your DSL router is controlled through three user accounts:admin,support and user .

The user name "admin" has unrestricted access to change and view configuration of your DSL Router.

The user name "support" is used to allow an ISP technician to access your DSL Router for maintenance and to run diagnostics.

The user name "user" can access the DSL Router, view configuration settings and statistics, as well as, update the router's software.

Use the fields below to enter up to 15 characters and click 'Apply/Save' to change or create passwords. Note: Password cannot contain a space.

Username:

New Username:

Old Password:

New Password:

Confirm Password:

Figure 5-5-12

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

**Services**

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

**Access Control -- Services**

Services access control list (SCL) enable or disable the running services.

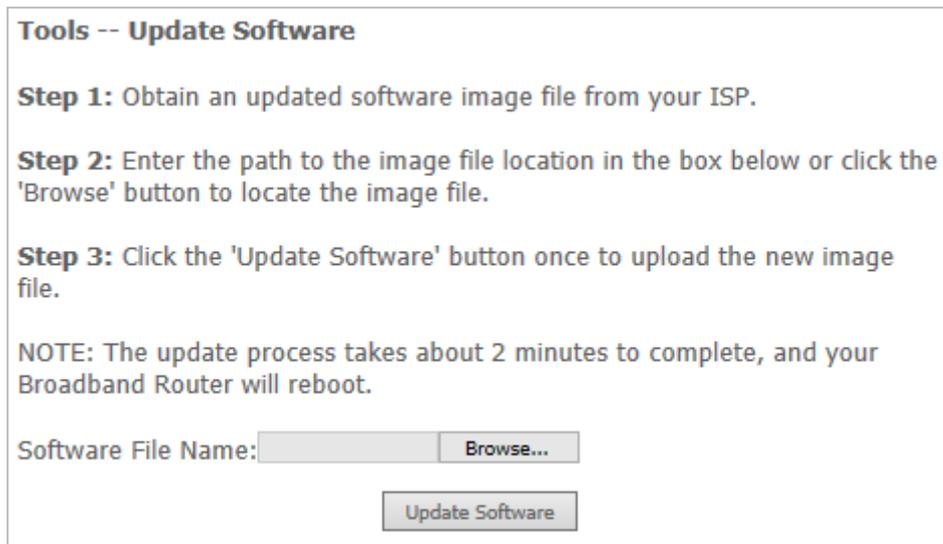
Services	LAN	LAN Port	WAN	Port
HTTP	<input checked="" type="checkbox"/> enable	<input type="text" value="80"/>	<input type="checkbox"/> enable	<input type="text" value="80"/>
TELNET	<input type="checkbox"/> enable	<input type="text" value="23"/>	<input type="checkbox"/> enable	<input type="text" value="23"/>
SSH	<input type="checkbox"/> enable	<input type="text" value="22"/>	<input type="checkbox"/> enable	<input type="text" value="22"/>
FTP	<input checked="" type="checkbox"/> enable	<input type="text" value="21"/>	<input type="checkbox"/> enable	<input type="text" value="21"/>
TFTP	<input checked="" type="checkbox"/> enable	<input type="text" value="69"/>	<input type="checkbox"/> enable	<input type="text" value="69"/>
ICMP	<input checked="" type="checkbox"/> enable	<input type="text" value="0"/>	<input type="checkbox"/> enable	<input type="text" value="0"/>
SNMP	<input checked="" type="checkbox"/> enable	<input type="text" value="161"/>	<input type="checkbox"/> enable	<input type="text" value="161"/>
SAMBA	<input checked="" type="checkbox"/> enable	<input type="text" value="445"/>	<input type="checkbox"/> enable	<input type="text" value="445"/>

Figure 5-5-13

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

## 5.5.7 Update Software

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



**Tools -- Update Software**

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

**Step 2:** Enter the path to the image file location in the box below or click the 'Browse' button to locate the image file.

**Step 3:** Click the 'Update Software' button once to upload the new image file.

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

Software File Name:

Figure 5-5-14

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



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

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

## 5.5.8 Reboot

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



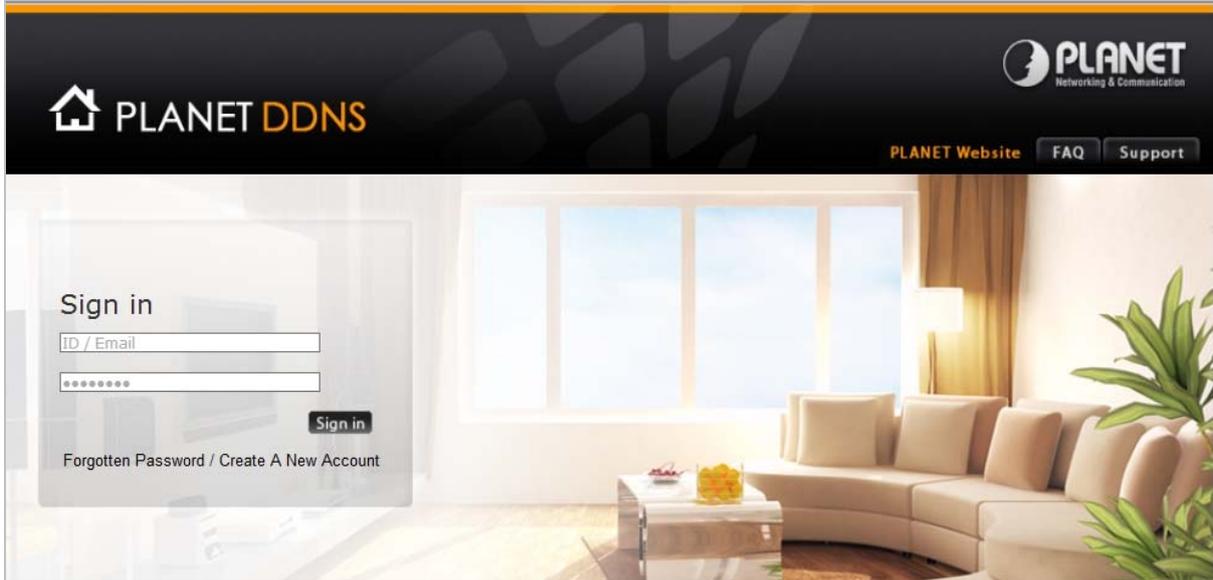
Click the button below to reboot the router.

Figure 5-5-15

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

# Appendix A: Planet DDNS

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



To select **DNS > Dynamic DDNS**

**Dynamic DNS**

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

Choose Add or Remove to configure Dynamic DNS.

Hostname	Username	Service	Interface	Remove
<div style="display: flex; justify-content: center; gap: 20px;"> <span>Add</span> <span>Remove</span> </div>				

**Step 1.** Press **Add** button

**Step 2.** Select **Planet DDNS**

**Add Dynamic DNS**

This page allows you to add a Dynamic DNS address from DynDNS.org or TZO.

D-DNS provider: DynDNS.org  
TZO  
**PlanetDNS**

Hostname:

Interface: pppoe\_0\_1\_1/ppp0.1 ▼

**PlanetDNS Settings**

Username:

Password:

Apply/Save

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

**Step 4.** Type the Password for your DDNS account.

### Add Dynamic DNS

This page allows you to add a Dynamic DNS address from DynDNS.org or TZO.

D-DNS provider PlanetDNS ▾

Hostname

Interface pppoe\_0\_1\_1/ppp0.1 ▾

#### PlanetDNS Settings

Username

Password

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.

PLANET  
Networking & Communication

[PLANET Website](#)
[FAQ](#)
[Support](#)

[Home](#)
[My Devices](#)
[Profile](#)

Welcome,  
wirelesstest ( [Sign out](#) )

#### My Device

Add Device
+

No.	Your Device	Registered Domain	Name of Your Device	Last Connection IP	Ping Status	Modify	Delete
1	ICA-HM316	wirelesstest	device	210.61.134.92	●		

## Appendix B: Performance of VDSL Router Profiles

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

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

(Data Rate: Mbps)

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



Note

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

## Appendix C: Glossary

### **Address mask**

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

### **VDSL**

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

### **ADSL**

Asymmetric digital subscriber line

### **AAL5**

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

### **ATM**

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

### **AWG**

American Wire Gauge - The measurement of thickness of a wire

### **Bridge**

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

### **Broadband**

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

**CO**

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

**CPE**

Customer Premises Equipment located in a user's premises

**DHCP (Dynamic Host Configuration Protocol)**

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

**DMT**

Discrete Multi-Tone frequency signal modulation

**Downstream rate**

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

**DSLAM**

Digital Subscriber Line Access Multiplex

**Dynamic IP Addresses**

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

**Encapsulation**

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

**Ethernet**

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

**FTP**

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

**Hop count**

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

**HTML**

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

**HTML browser**

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

**http**

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

**ICMP**

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

**Internet address**

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

**Internet Protocol (IP)**

The network layer protocol for the Internet protocol suite

**IP address**

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

**ISP**

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

**MAC**

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

**MIB**

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

**NAT**

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

**NVT**

Network Virtual Terminal

**PAP**

Password Authentication Protocol

**PORT**

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

**POTS**

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

**PPP**

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

**PPPoE**

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

**Remote server**

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

### **RFC**

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

### **Route**

The path that network traffic takes from its source to its destination. The route a datagram may follow can include many gateways and many physical networks.

In the Internet, each datagram is routed separately.

### **Router**

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

### **Routing Table**

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

### **Routing Information Protocol**

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

### **SNMP**

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

### **SOCKET**

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

### **Spanning-Tree Bridge Protocol (STP)**

Spanning-Tree Bridge Protocol (STP) - Part of an IEEE standard. A mechanism for detecting and preventing loops from occurring in a multi-bridged environment.

When three or more LAN's segments are connected via bridges, a loop can occur. Because of a bridge forwards all packets that are not recognized as being local, some packets can circulate for long periods of time, eventually degrading system performance. This algorithm ensures only one path connects any pair of stations, selecting one bridge as the 'root' bridge, with the highest priority one as identifier, from which all paths should radiate.

### **Spoofing**

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

### **Static IP Address**

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

### **Subnet**

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

### **TCP**

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

### **TFTP**

Trivial File Transfer Protocol. A simple file transfer protocol (a simplified version of FTP) that is often boot diskless workstations and other network devices such as routers over a network (typically a LAN).

### **Telnet**

The virtual terminal protocol in the Internet suite of protocols - Allows users of one host to log into a remote host and act as normal terminal users of that host.

### **Transparent bridging**

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

### **UDP**

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

### **UNI signaling**

User Network Interface signaling for ATM communications.

### **Virtual Connection (VC)**

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

**WAN**

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

## EC Declaration of Conformity

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