

User's Manual

802.11n Wireless VDSL2 Bridge Router

VDR-301N





www.PLANET.com.tw

Copyright

Copyright © 2017 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, for example, use only shielded interface cables when connecting to computer or peripheral devices. Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

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

(1) This device may not cause harmful interference

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

Federal Communication Commission (FCC) Radiation Exposure Statement

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

R&TTE Compliance Statement

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

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

Safety

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

National Restrictions

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

Country	Restriction	Reason/remarks		
Bulgaria	None	General authorization required for outdoor use and public service.		
	Outdoor use limited to 10	Military Radiolocation use. Refarming of the 2.4 GHz		
France	mW e.i.r.p. within the band	band has been ongoing in recent years to allow current		
	2454-2483.5 MHz	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	way Implemented This subsection does not apply for the geographica within a radius of 20 km from the centre of Ny-Åles			
Russian Federation	None	Only for indoor applications		



WEEE regulation



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

Revision

User's Manual of 802.11n Wireless VDSL2 Bridge Router Model: VDR-301N Rev: 1.0 (March, 2017) Part No. EM-VDR-301N (**2080-AC0390-000**)



Table of Contents

CHAPTER 1 PRODUCT INTRODUCTION	
1.1 Package Contents	8
1.2 Product Description	9
1.3 Product Features	12
1.4 Product Specifications	13
CHAPTER 2 HARDWARE INSTALLATION	16
2.1 Hardware Description	16
2.1.1 Front Panel of VDR-301N	17
2.1.2 LED Indications of VDR-301N	17
2.1.3 Rear Panel of VDR-301N	18
CHAPTER 3 CONNECTING TO THE ROUTER	19
3.1 System Requirements	19
3.2 Installing the Router	19
CHAPTER 4 INSTALLATION GUIDE	21
4.1 Configuring the Network Properties	21
4.2 Configuring with Web Browser	25
CHAPTER 5 SYSTEM SETTINGS	26
CHAPTER 5 SYSTEM SETTINGS	
	27
5.1 Status	27
5.1 Status 5.1.1 Device Information	27 27 27
5.1.1 Device Information	
5.1 Status 5.1.1 Device Information 5.1.2 DSL 5.1.3 Statistics	27 27 27 27 28 28 29
5.1 Status 5.1.1 Device Information 5.1.2 DSL 5.1.3 Statistics 5.2 Wizard	27 27 27 27 28 28 29 30
5.1 Status 5.1.1 Device Information 5.1.2 DSL 5.1.3 Statistics 5.2 Wizard 5.2.1 Bridge	27 27 27 27 28 29 30 32
5.1 Status 5.1.1 Device Information 5.1.2 DSL 5.1.3 Statistics 5.2 Wizard 5.2.1 Bridge 5.2.2 IPoE	27 27 27 27 28 29 30 30 32 34
5.1 Status 5.1.1 Device Information 5.1.2 DSL 5.1.3 Statistics 5.2 Wizard 5.2.1 Bridge 5.2.2 IPoE 5.2.3 PPPoE	27 27 27 27 28 29 30 30 32 34 34 36
5.1 Status 5.1.1 Device Information 5.1.2 DSL 5.1.3 Statistics 5.2 Wizard 5.2.1 Bridge 5.2.2 IPoE 5.2.3 PPPoE 5.2.4 PPPoA	27 27 27 28 28 29 30 30 32 34 34 33
5.1 Status 5.1.1 Device Information 5.1.2 DSL 5.1.3 Statistics 5.1.3 Statistics 5.2 Wizard 5.2.1 Bridge 5.2.2 IPoE 5.2.3 PPPoE 5.2.4 PPPoA 5.2.5 1483 Routed	27 27 27 27 28 29 30 30 32 34 34 36 38 40
5.1 Status 5.1.1 Device Information 5.1.2 DSL 5.1.3 Statistics 5.2 Wizard 5.2.1 Bridge 5.2.2 IPoE 5.2.3 PPPoE 5.2.4 PPPoA 5.2.5 1483 Routed	27 27 27 28 29 30 30 32 34 34 34 36 38 40 40
5.1 Status 5.1.1 Device Information 5.1.2 DSL 5.1.3 Statistics 5.2 Wizard 5.2.1 Bridge 5.2.2 IPoE 5.2.3 PPPoE 5.2.4 PPPoA 5.2.5 1483 Routed 5.3.1 WAN	27 27 27 27 28 29 30 30 32 34 34 36 38 40 40 43

5.3.5 LAN	
5.3.6 WLAN	
5.4 Advanced	62
5.4.1 Route	
5.4.2 NAT	
5.4.3 QoS	
5.4.4 CWMP (TR-069)	
5.4.5 Port Mapping	
5.4.6 Others	
5.5 Service	81
5.5.1 IGMP	
5.5.2 UPnP	
5.5.3 DNS	
5.5.4 DDNS	85
5.5.5 VPN	
5.6 Firewall	
5.6.1 MAC Filter	
5.6.2 IP/Port Filter	
5.6.3 URL Filter	
5.6.4 ACL	
5.6.5 DoS	
5.7 Maintenance	
5.7.1 Update	
5.7.2 Password	
5.7.3 Reboot	101
5.7.4 Time	
5.7.5 Log	
5.7.6 Diagnostic	
HAPTER 6. QUICK CONNECTION TO A WIRELESS NETWORK	110
6.1 Windows XP (Wireless Zero Configuration)	110
6.2 Windows 7 (WLAN AutoConfig)	112
6.3 Mac OS X 10.x	115
6.4 iPhone/iPod Touch/iPad	

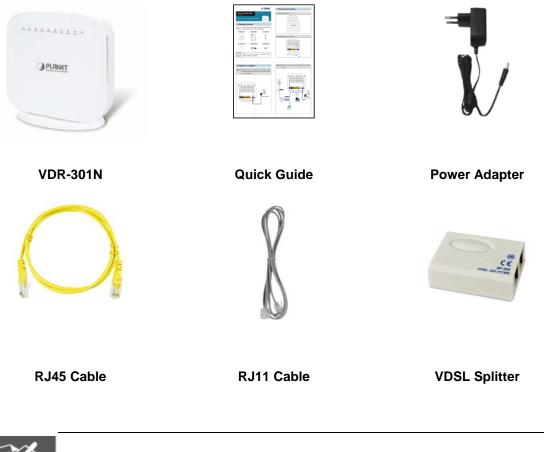
APPENDIX A: CABLE PROFILES	122
A.1 Device's RJ45 Pin Assignments	
A.2 RJ45 Cable Pin Assignment	

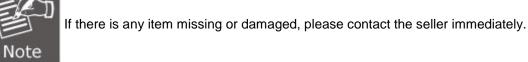


Chapter 1 Product Introduction

1.1 Package Contents

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



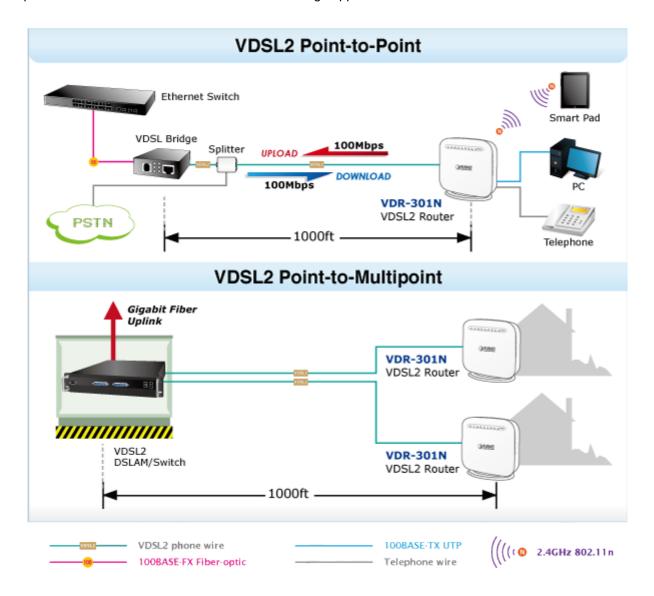




1.2 Product Description

High-performance Ethernet over VDSL2

Via the latest VDSL2 technology with **30a profile** supported, PLANET VDR-301N offers very high-performance access to Internet, up to **100Mbps** for both **downstream** and **upstream** data transmission. VDSL2 absolutely offers the fastest data transmission speed over the existing copper telephone lines without the need for rewiring. With integrated support for the ITU-T's new **G.993.5 Vectoring** technology, the VDR-301N works in conjunction with vectoring-enabled DSLAMs to remove crosstalk interference and improve maximum line bandwidth across the existing copper infrastructure.



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

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

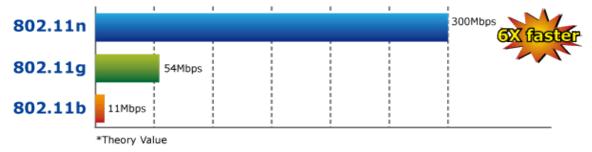


ADSL2+ Fallback

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

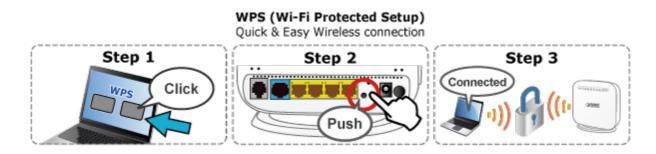
High-speed 802.11n Wireless Connectivity

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



Secure Wireless Access Control

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



Superior Management Functions

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



Multiple Functions for Broadband Communications

The VDR-301N integrates **VDSL2**, **ADSL2+** and **wireless LAN** services into one unit. It is designed to provide a simple and cost-effective xDSL Internet connection for a private Ethernet and 802.11b/g/n wireless network. The Router combines high-speed xDSL Internet connection and IP routing for the LAN and wireless connectivity in one package. It is usually preferred to provide high access performance applications for the individual users, SOHOs and small enterprises.



IPv6/IPv4 Dual Stack Capability

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

Robust TR-069 Remote Management

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



1.3 Product Features

Internet Access Features

- Shared Internet Access: All users on the LAN can access the Internet through the VDR-301N using only one single external IP address. The local (invalid) IP addresses are hidden from external sources. This process is called NAT (Network Address Translation).
- Built-in VDSL2 Modem: The VDR-301N provides VDSL2 modem and supports all common VDSL2 connections.
- **G. Vectoring**: G.993.5 (G. Vector) support for significant reduction of crosstalk levels and improvement of VDSL2 line performance
- Multiple WAN Connections: Upon the Internet (WAN port) connection, the VDR-301N supports ADSL2+ and VDSL2.

Advanced Internet Functions

- Virtual Servers: This feature allows Internet users to access Internet servers on your LAN. The setup is also quick and easy.
- **Firewall:** The VDR-301N supports simple firewall with NAT technology.
- Universal Plug and Play (UPnP): UPnP allows automatic discovery and configuration of the Broadband Router. UPnP is supported by Windows XP, 7 or later.
- DMZ Support: The VDR-301N can translate public IP addresses into private IP address to allow unlimited 2-way communication with the servers or individual users on the Internet. It provides the most flexible way to run programs smoothly for programs that might be restricted in NAT environment.
- **RIPv1/v2 Routing:** It supports RIPv1/v2 routing protocol for routing capability.

LAN Features

- 4-port Switch: The VDR-301N incorporates a 4-port 10/100BASE-TX switching hub, making it easy to create or extend your LAN.
- DHCP Server Support: Dynamic Host Configuration Protocol provides a dynamic IP address to PCs and other devices upon request. The VDR-301N can act as a DHCP Server for devices on your local LAN.

Wireless Features

- IEEE 802.11b/g/n Wireless Stations: The VDR-301N supports 802.11n standard which provides backward compatibility with the 802.11b and 802.11g standard, so 802.11b, 802.11g, and 802.11n can be used simultaneously. IEEE 802.11n wireless technology is capable of having a data rate of up to 300Mbps.
- WPS Push Button Control: The VDR-301N supports WPS (Wi-Fi Protected Setup) for users to easily connect to wireless network without configuring the security.
- Advanced Security: Supports 64/128-bit WEP, WPA / WPA2 and WPA-PSK / WPA2-PSK (TKIP/AES encryption), and 802.1x.
- Wireless MAC Access Control: The Wireless Access Control feature can check the MAC address (hardware address) of wireless stations to ensure that only trusted wireless stations can access your LAN.



- Multiple SSIDs: It allows users to access different networks through a single AP.
- Management Features
 - TR069 compliant: Support for centralized management node of multiple VDSL2 CPEs

1.4 Product Specifications

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



ADSL Features	 Full-rate ANSI T1.413 Issue 2 ITU-T G.992.1(G.DMT) ITU-T G.994.1 (G.hs) ITU-T G.995.1 ITU-T G.992.3 (G.dmt.bis) ITU-T G.992.5 	
Protocol Features	 ATM Adaptation Layer Type 5 (AAL5) Multiple Protocol over AAL5 (RFC 2684, formerly RFC 148) ATM Forum UNI3.1/4.0 PPP over ATM (RFC 2364) PPP over Ethernet (RFC 2516) IPoA (RFC 1577/2225) Bridged or routed Ethernet encapsulation VC and LLC based multiplexing OAM F4/F5 ATM QoS: UBR, CBR, VBR-rt, VBR-nrt Dynamic and static IP IP unnumbered 	
Advanced Features	 Parent Control Traffic Shaping(ATM QoS) UBR, CBR, VBR-rt, VBR-nrt Dynamic Host Configuration Protocol (DHCP), DHCP relay Network Address Translation (NAT) PVC/Ethernet Port Grouping Static Routing, RIP v1/v2 (optional) DNS relay, DDNS G. vectoring IGMP proxy, MLD proxy PPTP, L2TP, IPSec VPN passthrough Virtual server, port triggering, UPnP, DMZ WMM, bandwidth control (IP QoS) 	
Security	 NAT firewall SPI firewall MAC / IP / URL filtering 	
Management Oevice configuration, management and update Web-based GUI Command line interface via telnet SSL for TR069		
Wireless Interface Specifications		
Wireless Standard	IEEE 802.11b/g/n	
Frequency Band	2.4GHz: 2.412~2.484GHz	
Modulation Schemes	 802.11g: 64QAM, 16QAM, QPSK, BPSK, DSSS 802.11b: CCK, DQPSK, DBPSK HT20 and HT40: 64 QAM, 16QAM, QPSK, BPSK 	



	802.11n(40MHz): up to 300 Mbps	
	802.11n(20MHz): up to 144.4 Mbps	
Data Transmission Rates	802.11g: 54, 48, 36, 24, 18, 12, 9, 6Mbps per channel, auto fallback for extended range	
	802.11b: 1, 5.5, 2, 1 Mbps per channel, auto fallback for extended range	
Transmit Power	<20dBm(EIRP)	
Wireless Data Encryption	64/128-bit WEP, WPA-PSK, WPA2-PSK, 802.1x encryption, and WPS PBC	
Environment Specifications		
Temperature / Humidity	Operating: 0~40 degrees C, 10~ 90% (non-condensing) Storage: -20~70 degrees C, 5~90% (non-condensing)	
Certification	CE	



Chapter 2 Hardware Installation

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

2.1 Hardware Description



VDR-301N Overview



2.1.1 Front Panel of VDR-301N

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

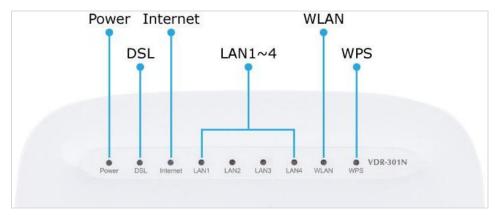


Figure 0-1 VDR-301N Front Panel

2.1.2 LED Indications of VDR-301N

The LEDs on the top panel indicate the instant status of system power, WAN data activity and port links, and help monitor and troubleshoot when needed. Figure 2-1 and Table 2-1 show the LED indications of the VDR-301N.

Front Panel LED Definition

LED	Color	State	Description
Devez	Green	ON	When the router is powered on, and in ready state.
Power	Green	OFF	The device is powered off.
		ON	The WAN is connected successfully.
DSL	Green	Flashing	Router is trying to establish a WAN connection to VDSL2 device or telecom's network.
		OFF	The device is powered off.
		ON	Internet is synchronized successfully in the route mode.
Internet	Green	Flashing	Internet data is being transmitted.
		OFF	Ethernet interface is disconnected.
		ON	The Ethernet interface is connected.
LAN1-4	Green	Flashing	Data is being transmitted or received via the corresponding LAN port.
		OFF	The Ethernet interface is disconnected.
		ON	WLAN is enabled.
WLAN	Green	Flashing	Data is being transmitted through the wireless interface.
		OFF	WLAN is disabled.
		ON	Connection succeeds under Wi-Fi Protected Setup.
WPS	Green	Flashing	Negotiation is in progress under Wi-Fi Protected Setup.
		OFF	Wi-Fi Protected Setup is disabled.

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



2.1.3 Rear Panel of VDR-301N

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

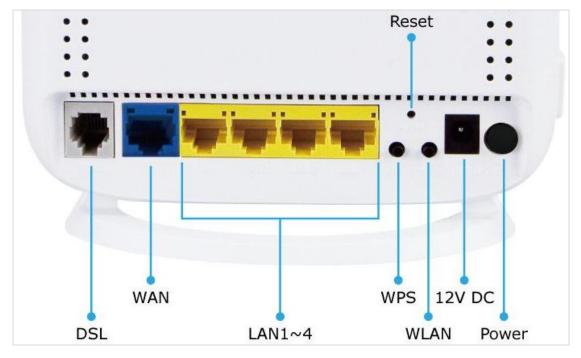


Figure 0-2 VDR-301N Rear Panel

Rear Panel Port and Button Definition

Connector	Description
POWER	Power on/off button
12V DC	Power connector with 12V DC, 0.5 A
WLAN	WLAN switch Press for over 3 seconds to enable or disable the WLAN function.
WPS	This button is used for enabling WPS PBC mode. If WPS is enabled, press this button for over 3 seconds and then the router starts to accept the negotiation in the PBC mode.
RESET	Press for more than 3 seconds to reset to factory default setting.
LAN (1-4)	Router is successfully connected to a device through the corresponding port (1, 2, 3, or 4). If the LED light is flashing, the router is actively sending or receiving data over that port.
WAN	The RJ45 WAN port allows data communication between the router and the network through a UTP cable
DSL	The RJ11 connector allows data communication between the router and the DSL network through a twisted-pair phone wire



Chapter 3 Connecting to the Router

3.1 System Requirements

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



1. The Router in the following instructions is named as PLANET VDR-301N.

2. It is recommended to use Internet Explore 8.0 or above to access the Router.

3.2 Installing the Router

Please connect the device to you computer as follows:

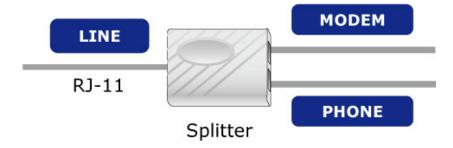
STEP 1. Connect the DSL port of the router and the Modem port of the splitter with a telephone cable; connect the phone to the phone port of the splitter through a cable and connect the incoming line to the Line port of the splitter.

The spliiter has three ports:

Line: Connect to a wall phone jack (RJ11 jack)

Modem: Connect to the Line interface of the router

Phone: Connect to a telephone set





STEP 2. Connect the Power Adapter to the VDR-301N. Check whether the **Power LED** on the front panel is on accordingly. Figure3-1 shows the power adapter connection diagram.

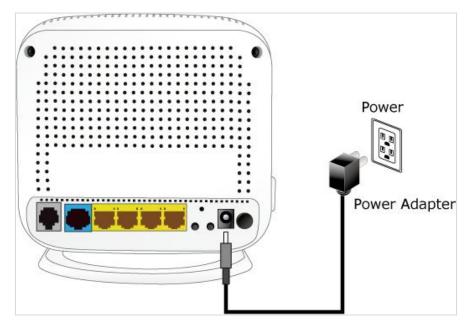


Figure 3-1 VDR-301N Power Adapter Connection Diagram

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

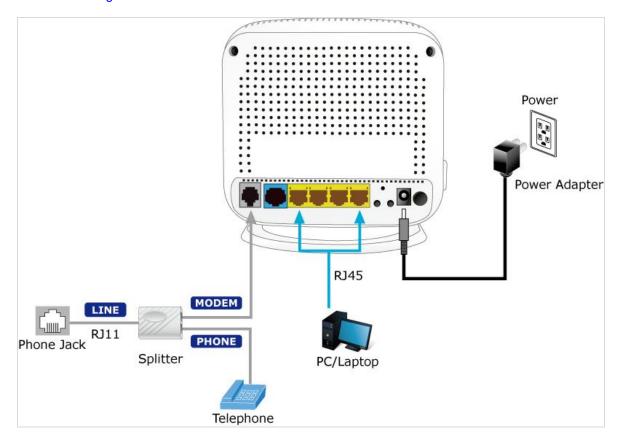


Figure 3-2 VDR-301N Connection Diagram



Chapter 4 Installation Guide

4.1 Configuring the Network Properties

Configuring PC in Windows 7

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

				x
Control Panel > Network and Internet > Network Connections >	• 4 9	Sean	ch Net	م
Ele Edit View Jools Advanced Help				
- Organize 🕶	÷	-		0
Local Area Connection Network 9 Atheros AR8151 PCI-E Gigabit Eth Www. AR5097 Wireless Network				

Figure 4-1 Select Local Area Connection

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

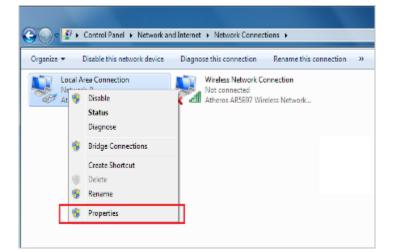


Figure 4-2 Network Connection Properties



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

Local Area Connection Properties
Networking Sharing
Connect using:
Atheros AR8151 PCI-E Gigabit Ethemet Controller (NDIS €
<u>C</u> onfigure
This connection uses the following items:
Client for Microsoft Networks
☑ 📮 QoS Packet Scheduler
File and Printer Sharing for Microsoft Networks
Internet Protocol Version 6 (TCP/IPv6)
Internet Protocol Version 4 (TCP/IPv4)
Link-Layer Topology Discovery Mapper I/O Briver Link-Layer Topology Discovery Responder
Install
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
OK Cancel

Figure 4-3 TCP/IP Setting

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

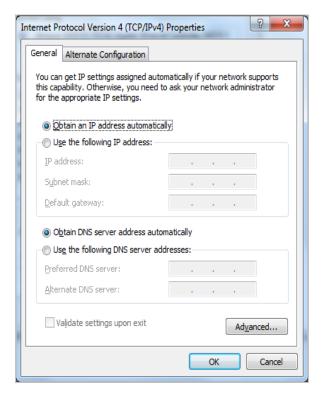


Figure 4-4 Obtain an IP address automatically



Configuring PC in Windows XP

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



Figure 4-5 Select Network Connections

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

🕹 Local Area Connection S	tatus 🛛 🕐 🔀
General Support	
Connection	
Status:	Connected
Duration:	00:19:32
Speed:	100.0 Mbps
Activity Sent —	- 🧞 Received
Packets:	27 0
Properties Disable	
	Close

Figure 4-6



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

etworking Sharing		
Connect using:		
Atheros AR815	51 PCI-E Gigabit Ethem	et Controller (NDIS &
		Configure
This connection uses	the following items:	Soundarout
Client for Mic		
QoS Packet		
		02-20-070700-0
File and Print	tor Shadna for Microsoft	Matuadra
	ter Sharing for Microsoft	
Internet Prot	ocol Version 6 (TCP/IP	v6)
Internet Prote	ocol Version 6 (TCP/IP) ocol Version 4 (TCP/IP)	v6) v4)
 Internet Prot Internet Prot Internet Prot Internet Prot Internet Prot Internet Prot 	ocol Version 6 (TCP/IP ocol Version 4 (TCP/IP opology Discovery Map	v6) v4) per I/O Driver
 Internet Prot Internet Prot Internet Prot Internet Prot Internet Prot Internet Prot 	ocol Version 6 (TCP/IP) ocol Version 4 (TCP/IP)	v6) v4) per I/O Driver
Internet Prot Internet Prot Internet Prot Internet Prot Internet Prot Int-Layer T Int-Layer T	ocol Version 6 (TCP/IP ocol Version 4 (TCP/IP opology Discovery Map	v6) v4) per I/O Driver ponder
✓ Internet Prot ✓ Internet Prot ✓ Internet Prot ✓ Link-Layer T ✓ Link-Layer T ✓ Ingstall	ocol Version 6 (TCP/IP ocol Version 4 (TCP/IP opology Discovery Map opology Discovery Res	v6) v4) per I/O Driver
✓ Internet Prot ✓ Internet Prot ✓ Internet Prot ✓ Link-Layer T ✓ Link-Layer T ✓ Link-Layer T ✓ Link-Layer T	ocol Version 6 (TCP/IP ocol Version 4 (TCP/IP opology Discovery Map opology Discovery Res	v6) v4) poer I/O Driver ponder Properties
Internet Prot Internet Prot Internet Prot Internet Prot Internet Prot Install Install Description Transmission Contr	ocol Version 6 (TCP/IP ocol Version 4 (TCP/IP opology Discovery Map opology Discovery Res	v6) v4) poper I/O Driver ponder <u>Properties</u> tocol. The default
✓ Internet Prot ✓ Internet Prot ✓ Internet Prot ✓ Link-Layer T ✓ Link-Layer T	ocol Version 6 (TCP/IP ocol Version 4 (TCP/IP opology Discovery Map opology Discovery Res Uninstall	v6) v4) poper I/O Driver ponder <u>Properties</u> tocol. The default

Figure 4-7TCP/IP Setting

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

eneral	Alternate Configuration				
this cap	get IP settings assigned aut ability. Otherwise, you need appropriate IP settings.				
00	otain an IP address automatic	ally:			
© U⊴	e the following IP address:				
IP ac	idress:	÷.	- 52	54	
Sybr	et mask:		16	(ii	1
⊵efa	ult gateway:		- (*	- 24	1
() O	tain DNS server address aut	omatically			
© Us	e the following DNS server a	ddresses:			
Prefe	erred DNS server:				
Alter	nate DNS server:		3	ě.)
⊡ v	alidate settings upon exit			Adya	nced

Figure 4-8 Obtain an IP address automatically



4.2 Configuring with Web Browser

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

Save this address in your Favorites for future reference.

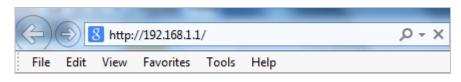


Figure 4-9 Login the Router

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

	Router Login	
User Name:	admin	
Password:	••••	
	Login Reset	

Figure 4-10 Login Window

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



Chapter 5 System Settings

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

PLANET Hetworking & Communication	802.11n Wireless VDSL2 Bridge Router VDR-301N					
Status Wizard	Setup Advanced	Service	Firewall	Maintenance		
Device Info	DSL Router Status This page shows the current status and System	some basic settings of	the device.			
> Device Info > DSL	Full Company Name		PLANET Technology Corporation			
Statistics	Company Brief Name Company Website		PLANET www.planet.com.tw			
	Model No.		VDR-301N			
	Default Device Name (Host Name) Uptime		VDR-301N 0 1:29:49			
	Date/Time		Sun Jan 1 9:29:49 2012			
	Firmware Version Built Date		V1.0.0 Jan 9 2017 15:25:42			

Figure 5-1 Status



5.1 Status

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

5.1.1 Device Information

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

	DSL Router Status This page shows the current sta	tus and some basic settings (of the device.	
Device Info	🕑 System			
DSL	Full Company Name		PLANET Technology Corporation	
	Company Brief Name		PLANET	
Statistics	Company Website		www.planet.com.tw	
	Model No.	Model No.		
	Default Device Name (Host N	Default Device Name (Host Name)		
	Uptime		0 2:31:42	
	Date/Time		Sun Jan 1 10:31:42 2012	
	Firmware Version		V1.0.0	
	Built Date		Jan 9 2017 15:25:42	
	💿 DSL			
	Operational Status	VDSL2 AnnexA		
	Upstream Speed	100966 kbps		
	Downstream Speed	100999 kbps		

Figure 5-2 Device Info

5.1.2 DSL

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



Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance
		DSL Config		_		
🔰 Device Info		This page shows	the setting of the DSL	_ Router.		
> Device Info		Dsl Line State	IS	SHOWTIME.		
> DSL		Dsl Mode		VDSL2-30A AnnexA		
		Up Stream		100966 kbps		
Statistics		Down Stream	L. C.	100999 kbps		
		Attenuation D	own Stream	0		
		Attenuation U	p Stream	1		
		SNR Margin D	lown Stream	29.5		
		SNR Margin U	lp Stream	6.8		
		Vendor ID RETK				
		Firmware Ver	sion	v134g113		
		CRC Errors		0		

Figure 5-3 DSL Info

5.1.3 Statistics

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

Status Wizard	Setup	Advanced	Ser		Firewall	Maintenanc	
Device Info Statistics	Statistics This page shows the Statistics:	ne packet statistics	for transmissio	n and reception r	egarding to networ	k interface.	
> Statistics	Interface	Rx pkt	Rx err	Rx drop	Tx pkt	Tx err	Tx dro
	- lan1	915	0	0	1861	0	0
	lan2	0	0	0	0	0	0
	lan3	0	0	0	0	0	0
	lan4	0	0	0	0	0	0
	WAN1	0	0	0	0	0	0
	WAN2	0	0	0	0	0	0
	w1	0	0	0	0	0	0
	w2	0	0	0	0	0	0
	w3	0	0	0	0	0	0
	w4	0	0	0	0	0	0
	w5	0	0	0	0	0	0

Figure 5-4 Statistics



5.2 Wizard

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

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

Status	Wizard	Setup Advai	nced Service	Firewall	Maintenance			
Vizard Wizard		Fast Config The wizard will help you do a Step 1: WAN Connection S Step 2: WLAN Connection S Step 3: Save Setting	etting	tep by step.				
		Step 1: WAN Connection S	Setting:	Please select the wan con	nection mode			
		Channel Type:	ATM 💌					
		VPI/VCI:	VPI: 0 (0-255) VCI: 0 (32-65535)					
		Encapsulation:	● LLC/SNAP ○ VC-Mux					
			○ Bridge					
			 ○ IPoE ● PPPoE ● PPPoA 					
		Connection Mode:						
			O 1483 Routed					
		IP Protocol:	Ipv4 💌					
		802.1q:	O Enable 💿 Dis	able				
		VLAN ID(1-4095):						
		PPP Settings:	Username: adm	in Password: •••	••			
		DNS Settings:	Attain DNS Au	omatically				
			O Set DNS Man	ally:				

Figure 5-5 Wizard

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



5.2.1 Bridge

Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance
Vizard > Wizard		Step 1: WAN C	help you do some bas onnection Setting Connection Setting	sic configurations st	ep by step.	
		Step 1: WAN	Connection Setting:		Please select the wan conne	ection mode
		Channel Type	:	ATM 🛩		
		VPI/VCI:		VPI: 0 (0-2	55) VCI: 0 (32-655)	35)
		Encapsulatio	n:	€ LLC/SNAP	/C-Mux	
				OBridge		
		Connection M	Node:			
				OPPPoA		
				O 1483 Routed		
		802.1q:		O Enable 💿 Disa	able	
		VLAN ID(1-40	95):			
		Next				

Figure 5-6 Wizard Bridge

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

Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance	
		Fast Config					
 Wizard Wizard 		Step 2:Wireless Fast Settings: Please config basic settings about wireless.					
		WLAN:		⊙Enable ○Disable			
		Band:		2.4 GHz (B+G+N) 💙			
		SSID:		PLANET_0556			
		Encryption:		None			
		Prev	Vext				

Figure 5-7 Wizard Bridge WLAN



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

Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance	
		Fast Config					
 Wizard Wizard 		Step 3:Save Settings	If you need finish "Cancel" or " Prev		nfig,please click "Apply C	changes".otherwise please cl	ick
		Settings as follo	DW:				
		VPI:			0		
		VCI:			32		
		Encapsulation:			LLC/SN	IAP	
		Channel Mode:			Bridge		
		WLAN:			Enable		
		Prev App	ly Changes Can	cel			

Figure 5-8 Wizard Bridge Saved



5.2.2 IPoE

Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance			
Wizard Wizard		Step 1: WAN	help you do some bas Connection Setting Connection Setting	ic configurations ste	ep by step.				
		Step 1: WAN	Connection Setting:		Please select the wan co	onnection mode			
		Channel Typ	e:	ATM 💌					
		VPI/VCI:		VPI: 0 (0-25	5) VCI: 0 (32-6	35535)			
		Encapsulati	on:	● LLC/SNAP ○ VC-Mux					
				OBridge					
				● IPoE● PPPoE					
		Connection	Mode:						
				O PPPoA					
				O 1483 Routed					
		IP Protocol:		Ipv4					
		802.1q:		O Enable 💿 Disa	ble				
		VLAN ID(1-4	095):						
		WAN IP Sett	ings:	€ Attain IP Automa	tically				
				O IP Manually:					
		DNS Setting	s:	Attain DNS Auto	matically				

Figure 5-9 Wizard IPoE

Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance
		Fast Config	l.			
WizardWizard		Step 2:Wirel	ess Fast Settings:	Please co	nfig basic settings ab	out wireless.
		WLAN:		⊙Enable ○Disable		
		Band:		2.4 GHz (B+G+N) 💙		
		S SID:		PLANET_0556		
		Encryption:		None		
		Prev	Vext			

Figure 5-10 Wizard IPoE WLAN



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

Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance			
		Fast Config							
Vizard Vizard		Step 3:Save Settings							
		Settings as foll	ow:						
		VPI:			0				
		VCI:			32				
		Encapsulation:			LLC/SNAP				
		Channel Mode:			IPoE				
		IP Protocol:			lpv4				
		IP Setting:			Ip Automatically				
		DNS Setting:			DNS Automatically				
		WLAN:			Enable				
		Prev App	oly Changes Car	ncel					

Figure 5-11 Wizard IPoE Saved



5.2.3 PPPoE

Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance		
Vizard > Wizard		Fast Config The wizard will help you do some basic configurations step by step. Step 1: WAN Connection Setting Step 2: WLAN Connection Setting Step 3: Save Setting						
		Step 1: WAN	Connection Setting:	Please select the wan connection mode				
		Channel Type	9:					
		VPI/VCI:		VPI: 0 (0-255) VCI: 0 (32-65535)				
		Encapsulatio						
		Connection M	O II n Mode: ⊙ F ○ F	OBridge				
				 ○ IP0E ● PPP0E ○ PPP0A 				
				O 1483 Routed				
		IP Protocol:		Ipv4				
		802.1q:		O Enable ③ Disable				
		VLAN ID(1-40	195):					
		PPP Settings	:	Username: admin	Password: ••••	•		
		DNS Settings	:	Attain DNS Automatica	lly			
				O Set DNS Manually :				

Figure 5-12 Wizard PPPoE

Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance
		Fast Config	1			
WizardWizard		Step 2:Wire	less Fast Settings:	Please c	onfig basic settings ab	out wireless.
		WLAN:		• Enable O Disable		
		Band:		2.4 GHz (B+G+N) 💌		
		S SID:		PLANET_0556		
		Encryption:		None		
		Prev	Next			

Figure 5-13 Wizard PPPoE WLAN



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

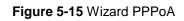
Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance			
		Fast Config							
Vizard Vizard		Step 3:Save Settings							
		Settings as fol	low:						
		VPI:			0				
		VCI:			32				
		Encapsulation			LLC/SNAP				
		Channel Mode			PPPoE				
		IP Protocol:			lpv4				
		ppp username	÷		admin				
		ppp password	:		admin				
		DNS Setting:			DNS Automatically				
		WLAN :			Enable				
		Prev Ap	ply Changes Car	icel					

Figure 5-14 Wizard PPPoE Saved



5.2.4 PPPoA

Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance		
 Wizard Wizard 		Fast Config The wizard will help you do some basic configurations step by step. Step 1: WAN Connection Setting Step 2: WLAN Connection Setting Step 3: Save Setting						
		Step 1: WAN	Connection Setting:	Pleas	e select the wan conr	nection mode		
		Channel Type	ə:	ATM 💌				
		VPI/VCI:		VPI: 0 (0-255) VCI: 0 (32-65535)				
		Encapsulatio	on:	● LLC/SNAP ○ VC-Mux				
				O Bridge				
		Connection		O IPOE				
				PPP0A				
				O 1483 Routed				
		IP Protocol:		Ipv4				
		802.1q:		O Enable				
		VLAN ID(1-40)95):					
		PPP Settings		Username: admin	Password: •••	••		
		DNS Settings	3:	Attain DNS Automatica	ally			
				O Set DNS Manually :				



Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance	
		Fast Config					
 Wizard Wizard 		Step 2:Wirel	ess Fast Settings:	Please config basic settings about wireless.			
		WLAN:		● Enable ○ Disable			
		Band:		2.4 GHz (B+G+N) 💙			
		S SID:		PLANET_0556			
		Encryption:		None			
		Prev	lext				

Figure 5-16 Wizard PPPoA WLAN



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

Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance
		Fast Config				
Vizard Vizard		Step 3:Save Settings	If you need finish "Cancel" or " Pre		config,please click "Apply	y Changes".otherwise please click
		Settings as fo	llow:			
		VPI:			0	
		VCI:			32	
		Encapsulation			LLC/SNAP	
		Channel Mode	r.		PPPoA	
		IP Protocol:			lpv4	
		ppp username	9:		admin	
		ppp password	i:		admin	
		DNS Setting:			DNS Automatically	
		WLAN:			Enable	
		Prev Ap	oply Changes Ca	ncel		

Figure 5-17 Wizard PPPoA Saved



5.2.5 1483 Routed

Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance
Vizard		Step 1: WAN C	help you do some bas connection Setting Connection Setting	ic configurations ste	p by step.	
		Step 1: WAN	Connection Setting:	1	Please select the wan conne	ection mode
		Channel Typ	B:	ATM 💌		
		VPI/VCI:		VPI: 0 (0-25	5) VCI: 0 (32-655)	35)
		Encapsulatio	on:	● LLC/SNAP ● V	C-Mux	
				O Bridge		
		Connection I	Mode:			
				OPPPOA		
		IP Protocol:		Ipv4 💌		
		802.1q:		O Enable O Disal	ble	
		VLAN ID(1-4)95):			
		WAN IP Setti	ngs:	O Attain IP Automa	tically	
				IP Manually:		
		IP Address:]	

Figure 5-18 Wizard 1483 Routed

Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance
		Fast Config				
WizardWizard		Step 2:Wirele	ess Fa <mark>s</mark> t Settings:	Please c	onfig basic settings ab	out wireless.
		WLAN:		⊙Enable ○Disable		
		Band:		2.4 GHz (B+G+N) 💙		
		S SID:		PLANET_0556		
		Encryption:		None		
		Prev	lext			

Figure 5-19 Wizard 1483 Routed WLAN



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

Status Wizard	Setup	Advanced	Service	Firewall	Maintenance
	Fast Config				
Wizard Wizard	Step 3:Save Settings	If you need finish "Cancel" or " Pre		onfig,please click "Apply	Changes".otherwise please click
	Settings as fol	low:			
	VPI:			0	
	VCI:			32	
	Encapsulation	1		LLC/SNAP	
	Channel Mode	:		1483 Router	
	IP Protocol:			lpv4	
	IP Setting:			lp Manually	
	IP Address:			10.1.1.1	
	Netmask:			255.255.255.0	
	DNS Setting:			DNS Automatically	
	WLAN :			Enable	
	Prev Ap	ply Changes Ca	ncel		

Figure 5-20 Wizard 1483 Routed Saved



5.3 Setup

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

5.3.1 WAN

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

Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance
💌 WAN			to configure the parar		iterface of your DSL and(or nect" and "Disconnect" but	r) Ethernet Modem/Router. Note : When ton will be enable.
> WAN > Auto PVC		WAN Physical	īype: 💿 D	SL WAN	○ Etherne	et WAN
> ATM		Default Route S	election: OA	uto 🔿 Specified		
IAN		Channel Type:	ATM			
VLAN		VPI:	0		VCI:	
		Encapsulation:	©⊔	.C	O VC-Mux	
		Channel Mode:	Brid	lge 🔽	Enable NAPT:	
		Enable IGMP:				
		VLAN:	⊙ D	isable	O Enable	
		VLAN ID(1-409	5):			
		PPP Settings:				
		User Name:			Password:	
		Туре:	Cor	itinuous 💌	Idle Time (min):	

Figure 5-21 WAN

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



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



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



5.3.2 Auto PVC

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

Status	Wizard	Setup Advance	d Service	Firewall	Maintenance
VAN		Auto PVC Configuration This page is used to configure pro		can add/delete auto pv	c search table.
> WAN		Probe WAN PVC	Probe		
> Auto PVC > ATM > DSL		VPI:	VCI:	Add	Delete
LAN		Ourrent Auto-PVC Table	:		
WLAN		PVC		VPI	VCI
		0		0	35
		1		8	35
		2		0	43
		3		0	51
		4		0	59
		5		8	43
		6		8	51
		7		8	59

Figure 5-22 Auto PVC

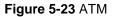
Field Description		
Probe WAN PVC	Click Probe to display WAN Permanent virtual circuit.	
VPI	Virtual Path Identifier. This is read-only field and is selected on the	
VPI	Select column of the Current ATM VC Table.	
	Virtual Channel Identifier. This is read-only field and is selected on the	
VO	Select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



5.3.3 ATM

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

Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance
💌 WAN		ATM Setting This page is use PCR,CDVT, SCR	d to configure the param	eters for the ATM of	your DSL Router. Here you	I may change the setting for QoS,
> WAN		VPI:	VCI:		Qos: UBR 💌	
Auto PVC ATM		PCR:	CDVT:		SCR:	MBS:
> DSL		Adsl Retrain:	Apply Changes	Undo		
		Current A	ATM VC Table:			
VLAN		Select V	VPI VCI	QoS	PCR CDVT	SCR MBS



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



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

5.3.4 DSL

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

Status Wizar	rd Setup	Advanced	Service	Firewall	Maintenance		
S WAN	DSL Settings This page allows yo	ou to choose which DS	3L modulation settings y	our modem router will	support.		
> WAN			G.Lite				
> Auto PVC			G.Dmt				
> ATM			🗹 T1.413				
> DSL	DSL modulation		ADSL2				
			ADSL2+				
🛛 LAN			VDSL2				
VLAN	AnnexL Option:	AnnexL Option: 🗹 Enabled					
	AnnexM Option:		Enabled				
			☑ 8A				
			✓ 88				
			☑ 8C				
	VDSL2 Profile:						
	VD3L2 FIGHE.		🗹 12A				
			✓ 12B				
			🗹 17A				
			🗹 30A				
	ADSL Capability		🗹 Bitswap Enable				
	and the culpublicy		SRA Enable				

Figure 5-24 DSL



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



5.3.5 LAN

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

5.3.2.1 LAN

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

Status Wizard	Setup Adva	anced Service	Firewall	Maintenance		
WAN	LAN Interface Setup This page is used to configuetc.		r. Here you may change	the setting for IP address, subnet mask,		
LAN	Interface Name:	Ethernet1				
> LAN > DHCP	IP Address:	192.168.1.1				
> DHCP Static	Subnet Mask:	255.255.255.0				
> LAN IPv6	Secondary IP					
	IGMP Snooping:	O Disable		Enable		
S WLAN	Apply Changes					
	MAC Address Control:			WLAN		
	Apply Changes					
	New MAC Address:		Add			
	Current Allowed MAC Address Table:					
		MAC Addr		Action		

Figure 5-25 LAN

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



5.3.2.2 DHCP

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

DHCP Server

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

Status	Wizard	Setup	Advanced		Service	Firewall	Maintenance	
WAN LAN		DHCP Mode This page can be used to config the DHCP mode:None,DHCP Relay or DHCP Server. (1)Enable the DHCP Server if you are using this device as a DHCP server. This page lists the IP address pools available to host on your LAN. The device distributes numbers in the pool to host on your network as they request Internet access. (2)Enable the DHCP Relay if you are using the other DHCP server to assign IP address to your host on the LAN. You can set the DHCP server IP address. (3)If you choose "None", then the modern will do nothing when the host request a IP address.						
> DHCP		LAN IP Addre	ss: 192.168.1.1	Subn	et Mask: 255.2!	55.25 <mark>5.</mark> 0		
> DHCP Static		DHCP Mode:		DH	CP Server 💌			
> LAN IPv6				-				
WLAN		Interface:		VA VA		VLAN3 VLAN4 V	WLAN ⊻VAPO ⊻VAP1 ⊻VAP2	
		IP Pool Range	e:	192.1	68.1. 2	- 192.168.1. 254	Show Client	
		Subnet Mask	:	255	255.255.0			
		Default Gatev	vay:	192	168.1.1			
		Max Lease T	me:	144	0 min	utes		
		Domain Name	e:	dom	iain.name			
		DNS Servers	<u>[]</u>	192	168.1.1			
		Apply Change	es Undo					

Figure 5-26 DHCP

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



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

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

s table shows the assigned IP address, MAC address and time expired for each DHCP leased client.
Name IP Address MAC Address Expiry(s) Type

Figure 5-27 DHCP Table

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



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

s page is used to con	figure the IP address range based on device type.
device name:	
start address:	192.168.1.
end address:	192.168.1.
Router address:	
option60	

Figure 5-28 Device IP Range Table

None

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

Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance
		DHCP Mode	e .			
WAN		This page can b (1)Enable the D	e used to config the DI HCP Server if you are u		CP server. This page lis	ts the IP address pools available to host
2 LAN		(2)Enable the D	HCP Relay if you are u		(a) The second s second second secon second second sec	y request Internet access. to your host on the LAN. You can set the
> LAN		DHCP server IP (3)If you choose		em will do nothing when t	he host request a IP ad	dress.
> DHCP		LAN IP Addre	ess: 192.168.1.1	Subnet Mask: 255.255	.255.0	
> DHCP Static		DHCP Mode:		None		
> LAN IPv6						
		Apply Chang	les Undo			
🛛 WLAN		Set VendorC	lass IP Range			

Figure 5-29 DHCP None





DHCP Relay

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

Status Wizard	Setup	Advanced	Service	Firewall	Maintenance	1
VAN LAN	(1)Enable the D on your LAN. Th (2)Enable the D DHCP server IP	e used to config the DH HCP Server if you are us e device distributes num HCP Relay if you are usi	ing this device as a DHC ibers in the pool to host ng the other DHCP serve	CP server. This page lis on your network as the er to assign IP address	sts the IP address pools ava y request Internet access, s to your host on the LAN. Yo dress,	
DHCP DHCP Static LAN IPv6	LAN IP Addr	ess: 192.168.1.1	Subnet Mask: 255.255.	255.0		
VIAN	Relay Server		192.168.2.242			

Figure 5-30 DHCP Relay

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



5.3.2.3 DHCP Static

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

Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance
wan				on your LAN. The device	e distributes the numbe	r configured to hosts on your network as
LAN		IP Address:		0.0.0.0		
> DHCP		Mac Address		00000000000 (ex. 00E086710502)	
> DHCP Static		Add D	elete Selected U	ndo		
> LAN IPv6		OHCP State	atic IP Table:			
VLAN		Select	IP Addr	ess		MAC Address

Figure 5-31 DHCP Static

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



5.3.2.4 LAN IPv6

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

Status Wizard	Setup Advance	ed Service Firewall Maintenance
	LAN IPv6 Setting This page is used to configurate	ipv6 Ian setting. User can set Ian RA server work mode and Ian DHCPv6 server work mode.
WAN	💿 Lan Global Address Se	etting
> LAN	Global Address:	
> DHCP	Apply Changes	
> DHCP Static	RA Setting	
> LAN IPv6	Enable:	V
WLAN	M Flag:	
	O Flag:	
	Max Interval:	600 Secs
	Min Interval:	200 Secs
	Prefix Mode:	Auto 💌
	ULA Enable:	
	RA DNS Enable:	
	Apply Changes	

Figure 5-32 LAN IPv6

The following table describes the parameters:

LAN Global Address Setting

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



RA Setting

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

DHCPv6 Setting

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

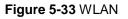


5.3.6 WLAN

5.3.6.1 Basic

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

Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance
wan		Wireless Bas This page is used	ic Settings I to configure the param	eters for your wireless r	network.	
		Disable W	ireless LA <mark>N Interface</mark>			
VLAN		Band:		2.4 GHz (F	3+G+N) 💙	
> Basic		Mode:		AP 🛩		
> Security		S SID:		PLANET_0	0556	
> MBSSID						
> Access Contro	ol List	Channel Width		40MHZ	~	
> Advanced		Control Sideba	and:	Upper 🗸	8	
> WPS						
		Channel Numt	per:	Auto 🕶 (Current Channel: 5	
		Wlan Domain:		● FCC 1~	11 O ETIS 1~13	
		Radio Power (Percent):	100% 🛩		
		Associated CI	ients:	Show Ac	tive Clients	
		Apply Change	S			



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



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

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

ociated wireless		ss, transmiss	ion, reception pack	et counters and en	crypted status for e
Active Wire	less Client	Table:			
MAC Address	Tx Packet	Rx Packet	Tx Rate (Mbps)	Power Saving	Expired Time (s)

Figure 5-34 Active Wireless Client Table



5.3.6.2 Security

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

Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance	
		Wireless Sec					
🛛 WAN		This page allows access to your wir		ss security. Turn on WEP (or WPA by using Encrypt	ion Keys could prevent an	/ unauthorized
🛛 LAN		SSID TYPE:			VAP1 OVAP2 OVA	Р3	
🛛 WLAN		Encryption:		None			
Basic Security		Use 802.1x	Authentication	O WEP 64bits O W	EP 128bits		
> MBSSID		WPA Authentio	ation Mode:	C Enterprise (RADIUS	3) 💿 Personal (Pre-Sh	nared Key)	
Access Control	ol List	Pre-Shared Ke	ey Format:	Passphrase	•		
> Advanced		Pre-Shared Ke	ey:	*****			
> WPS		Authentication	RADIUS Server:	Port 1812 IP ad	dress 0.0.0.0	Password]
		Note: When en	cryption WEP is sele	cted, you must set WEP k	ey value.		
		Apply Changes	5				

Figure 5-35 Wireless Security

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



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

5.3.6.3 MBSSIDs (Multiple BSSIDs)

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

Status Wizard	Setup	Advanced	Service	Firewall	Maintenance			
WAN	This page allow:	ultiple BSSID Setup s you to set virtual access pe. click "Apply Changes"	points(VAP). Here you	can enable/disable virt	ual AP, and set its SSID and			
LAN	Enable V	AP0						
WLAN Basic	SSID:		PLANET_	0557				
> Security	Broadcast S	SID:	Enable	Enable O Disable				
> MBSSID	Relay Blocki	ng:	O Enable	O Enable ③ Disable				
Access Control List	Authenticatio	on Type:	O Open S	O Open System O Shared Key 💿 Auto				
> Advanced	Enable V	/AP1						
> WPS	S SID:		PLANET_	0558				
	Broadcast S	SID:	💿 Enable	Disable				
	Relay Blockii	ng:	O Enable	Oisable				
	Authenticatio	on Type:	O Open S	System 🔘 Shared Ke	y 💿 Auto			

Figure 5-36 Wireless MBSSIDs



5.3.6.4 Access Control List

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

Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance	
		Wireless Ac	cess Control				
🛛 WAN						the access control list will b the list will not be able to co	
🛛 LAN		Access Point.					
🗵 WLAN		Wireless Acc	cess Control Mode: Di	sable 🖌	Apply Changes		
> Basic		MAC Address	s:	(ex. 00E086710502)		Add Reset	
 Security 							
> MBSSID		Current /	Access Control List:				
Access Control	List		MA	C Address		Select	
> Advanced		Delete Selec	ted Delete All				

Figure 5-37 Wireless Access Control

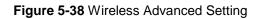
Field	Description
	The Selections are:
	Disable: Disable the wireless ACL feature.
	Allow Listed: When this option is selected, no wireless clients except
Wireless Access Control	those whose MAC addresses are in the current access control list will
Mode	be able to connect (to this device).
	Deny Listed: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



5.3.6.5 Advanced

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

Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance
VAN		These settings				/ledge about wireless LAN. These our Access Point.
VLAN		Authenticati	on Type:	O Open System	Shared Key 💿 Auto	
> Basic		Fragment TI	nreshold:	2346 (256-2	2346)	
> Security		RTS Thresh	old:	2347 (0-234	17)	
> MBSSID		Beacon Inte	rval:	100 (20-10)24 ms)	
> Access Contro	l List	DTIM Interva	11:	1 (1-255	i)	
Advanced		Data Rate:		Auto 💙		
> WPS		Preamble Ty	vpe:	Song Preamble €	Short Preamble	
		Broadcast S	SID:	Inabled ○ Disa	bled	
		Relay Block	ing:	C Enabled 💿 Disa	bled	
		Ethernet to	Wireless Blocking:	O Enabled 💿 Disa	bled	
		Wifi Multica	st to Unicast:	⊙ Enabled ○ Disa	bled	
		Aggregation	:	Inabled ○ Disa	bled	
		Short GI:		⊙ Enabled ○ Disa	bled	
		Apply Chang	jes			





5.3.6.6 WPS

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

Status Wizard	Setup	Advanced	Service	Firewall	Maintenance	R.	
	Wi-Fi Protecte	ed Setup					
🛛 WAN	This page allows y	ou to change the set	tting for WPS (Wi-Fi Protect onnect to the Access Point		feature could let your wireless ny hassle.	s client	
🗵 LAN							
🛛 WLAN	Disable W	42					
> Basic	WPS Status:		Configured O Un	Configured			
> Security	Self-PIN Number:		64413228 Regenerate PIN				
> MBSSID	Push Button Configuration: Start PBC				t PBC		
Access Control List	Apply Changes	Reset					
> Advanced	💿 Current Ke						
> WPS	Gr Current Re	y mio.					
	Authe	entication	Encryption		Key		
	(Open	None		N/A		
			I				
			Start PIN				

Figure 5-39 WPS

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



5.4 Advanced

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

PLANET Retworking & Commanderline		802.11	802.11n Wireless VDSL2 Bridge Router VDR-301N						
Status	Wizard	Setup	Advanced	Service	Firewall	Maintena	nce		
Route		Routing Con This page is used		g information. Here you	can add/delete IP route	es.			
 Static Route 		Enable:							
> IPv6 Static Rout	te	Destination:							
> RIP		Subnet Mask:							
NAT		Next Hop:							
QoS		Metric:		1					
🛛 СММР		Interface:		~					
Port MappirOthers	ıg	Add Route		e Selected Show	Routes				
		Select	State Des	tination	Subnet Mask	NextHop	Metric	ltf	

Figure 5-40 Advanced

5.4.1 Route

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

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



5.4.1.1 Static Route

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

Status Wizard	Setup	Advanced	Service	Firewall	Maintena	ince
Route	Routing Conf This page is used	120	ting information. Here	you can add/delete IP r	outes.	
Static Route	Enable:					
> IPv6 Static Route	Destination:					
> RIP	Subnet Mask:					
NAT	Next Hop:					
QoS	Metric:		1			
💌 СШМР	Interface:		~			
 Port Mapping Others 	Add Route		ete Selected S	how Routes		
	Static Rout	e Table:				
	Select	State D	estination	Subnet Mask	NextHop	Metric Itf

Figure 5-41 Static Route

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



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

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

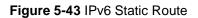
Destination	Subnet Mask	NextHop	Interface
192.168.1.1	255.255.255.255	*	Ethernet1
192.168.1.0	255.255.255.0	*	Ethernet1

Figure 5-42 IP Route Table

5.4.1.2 IPv6 Static Route

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

Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance
		IPv6 Routing	g Configuration			
Route		This page is use	d to configure the ipv6 ro	uting information. Here	you can add/delete IPv(6 routes.
> Static Route		Destination:				
> IPv6 Static Rou	ite	Prefix Length	1:			
> RIP		Next Hop:				
NAT		Interface:		~		
🛛 QoS		Add Route	Delete Selected			
CWMP		(6) IDv6 Stat	ic Route Table:			
🛛 🛛 Port Mappi	ng					
Others		Select	De	estination	NextHop	Interface





The following table describes the parameters:

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

5.4.1.3 RIP

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

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

Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance
Route	_	RIP Configu Enable the RIP i Protocol.		ce as a RIP-enabled rou	iter to communicate wi	th others using the Routing Informatio
Static Route IPv6 Static Route		RIP:		⊙ Off ○ On		Apply
≥ RIP		interface:				
MAT		Recv Version	1:	RIP1 🕶		
QoS		Send Version	1:	RIP1 ¥		
🗵 Port Mapping		Add De	elete			
Vithers		Rip Conf	ig List:			
		Select	interface	Red	v Version	Send Version

Figure 5-44 RIP



The following table describes the parameters:

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

5.4.2 NAT

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

5.4.2.1 DMZ

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

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



Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance
☑ Route NAT			IZ host contains devices a			d access to its local private network. P) servers, FTP servers, SMTP (e-mail
> DMZ		WAN Interfac	ce:		any 🗸	
> Virtual Server		DMZ Host IP	Address:			
> ALG						
> NAT Exclude IP		Apply Chang				
> Port Trigger		 O Current 	DMZ Table:			
> FTP ALG Port	Select		lect	WAN Interface		DMZ IP
> Nat IP Mapping		Delete Selec	ted			
💟 QoS						
CWMP						
💟 Port Mapping						
🛛 Others	1					

Figure 5-45 DMZ

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



5.4.2.2 Virtual Server

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

Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance	
🔽 Route		Virtual Serve This page allows		erver,so others can acces	s the server through the	Gateway.	
NAT		Service Type:					
> DMZ		Osual Ser	vice Name:	AUTH 🔽			
Virtual Server		O User-defin	ned Service Name:				
> ALG		Protocol:		TCP			
> NAT Exclude IF	þ	WAN Setting:		Interface 💌			
> Port Trigger		WAN Interface					
> FTP ALG Port				any 💙			
Nat IP Mapping	g	WAN Port:		113 (6	ex. 5001:5010)		
		LAN Open Por	t:	113			
QoS		LAN Setting:		Ip Address 💌			
CWMP		LAN IP Addres	is:				
👿 Port Mappi	ing						
🔽 Others		Apply Change	s				
		Ourrent V	irtual Server Forwa	arding Table:			
	ServerName Protocol Local IP Address Local Port WAN IP Address WAN Port State Acti						

Figure 5-46 Virtual Server

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



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

5.4.2.3 ALG

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

Status Wizaro	d Setup Advanc	ed Service	Firewall	Maintenanc
	NAT ALG and Pass-Thr Setup NAT ALG and Pass-Throu			
🛛 Route		gnoonigalaton		
NAT	IP Sec Pass-Through:	Enable		
> DMZ	L2TP Pass-Through:	Enable		
> Virtual Server	PPTP Pass-Through:	Enable		
> ALG	FTP:	Enable		
> NAT Exclude IP	H.323:	Enable		
> Port Trigger	SIP:	Enable		
> FTP ALG Port	RTSP:	Enable		
> Nat IP Mapping	ICQ:	Enable		
	MSN:	Enable		
🗹 QoS	Apply Chapters Depart			
CWMP	Apply Changes Reset			

Figure 5-47 ALG

5.4.2.4 NAT Exclude IP

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



Status	Wizard	Setup	Advanced	Service	Firewa	ll Mainte	enance
Route		NAT EXCLU This page is use specified interfac	d to config some source	ip address which u	se the purge route	mode when access in	ternet through the
NAT > DMZ		interface:		~			
> Virtual Server		IP Range:]		
> ALG		Apply Change	es Reset				
> NAT Exclude IP		Ourrent N	IAT Exclude IP Table:				
Port Trigger			WAN Interface		Low IP	High IP	Action
> FTP ALG Port							
> Nat IP Mapping							

Figure 5-48 NAT Exclude IP

5.4.2.5 Port Trigger

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

Status	Wizard	Setup	Advanced	Servic	e Fire	wall	Maintenance	e N	
Route		Nat Port Trigge Entries in this table of such filters can be	are used to restric			ur local network to	Internet through t	he Gateway. Use	
 DMZ 		Nat Port Trigger: C			O Enable 🕙 Disable				
> Virtual Server		Apply Changes							
> ALG		Application Type	:						
> NAT Exclude IP		Osual Applic	ation Name:		Selec	ct One	~		
> Port Trigger		O User-defined	d Application Nam	ne:					
> FTP ALG Port									
> Nat IP Mapping		Start Match Port	End Match Port	Trigger Protocol	Start Relate Port	End Relate Port	Open Protocol	Nat Type	
6				UDP 💌			UDP 💌	outgoing 🛩	
QoS				UDP 🔽			UDP 💌	outgoing 🛩	
				UDP 💌			UDP 💌	outgoing 💌	
🛛 Port Mapping				UDP 💌			UDP 💌	outgoing 🛩	
🛛 Others				UDP 💌			UDP 💌	outgoing 💙	
				UDP 💌			UDP 💌	outgoing	
		Apply Changes							

Figure 5-49 Port Trigger



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

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

5.4.2.6 FTP ALG Port

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

Status Wizard	Setup	Advanced	Service	Firewall	Maintenance
Route		onfiguration ed to configure FTP Serv	er ALG and FTP Client Al	_G ports .	
NAT	FTP ALG por	rt:			
> DMZ	Add Dest Po	orts Delete Selecte	ord DestDort		
> Virtual Server					
> ALG	() FTP AL	G ports Table:			
> NAT Exclude IP	Select			Ports	
	0			21	
> Port Trigger					
> FTP ALG Port					
> Nat IP Mapping					

Figure 5-50 FTP ALG Port

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



5.4.2.7 NAT IP Mapping

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

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

Status Wizard	Setup	Advanced	Service	Firewall	Maintenance	
		The second second second second				
Route		allow you to config one IF d address will select on			m lan,so one packet which's	source ip is in
NAT	Type: One-to-O	ne 💌				
> DMZ · Virtual Server	Local Start IP:					
> ALG	Local End IP:					
> NAT Exclude IP	Global Start IP:					
> Port Trigger	Global End IP:					
+ FTP ALG Port	Apply Changes	Reset				
Nat IP Mapping	© Current NAT	IP MAPPING Table:				
🛛 QoS	Local Start	IP Local En	id IP G	Global Start IP	Global End IP	Action
CWMP	Delete Selected	Delete All				
💆 Port Mapping						
😡 Others						

Figure 5-51 NAT IP Mapping

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



5.4.3 QoS

5.4.3.1 QoS

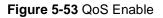
TheVDR-301N provides a control mechanism that can provide a different priority to different users or data flows. The QoS is enforced by the QoS rules in the QoS table. A QoS rule contains two configuration blocks: Traffic Classification and Action. The Traffic Classification enables you to classify packets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

Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance
		IP QoS				
Route		IP QoS:		\odot disable \bigcirc enable		
QoS		Apply				
> QoS						

Figure 5-52 QoS Disable

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

Status Wizard	Setup Advanced	Service Firewall Maintenance
	IP QoS	
Route	IP QoS:	◯ disable ④ enable
QoS > QoS	Schedule Mode:	strict prior
> Traffic Shaping	Apply	
	QoS Rule List	
☑ CWMP ☑ Port Mapping	src MAC dest MAC	src IP sPort dest IP dPort proto phy por
☑ Others	QoS Rule List(Continue)	
	IPP TOS DSCP	TC 802.1p Prior IPP Mark TOS Mark DSCP Mark TC Mark 802.1p Mark
	Delete Add Rule	





5.4.3.2 Traffic Shaping

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

Status	Wizard	Setup	Advance	∋d	Se	ervice		Firewall	Maint	enance	<u>k</u>
		IP QoS Traff	ic Shaping								
Route		Entries in this tal	ble are used for t	traffic cont	rol.						
NAT		Traffic St	haping in the r	network i	nterfac	e:					
QoS		Total Bandy	width(0, Unlimite	d):			U	P Stream 0	kbps		
> QoS							Dov	wn Stream 0	kbps		
Traffic Shaping		Apply									
	_	Traffic St	haping Rule Li	st							
Port Mappin	a	ID Wap Itf. Pro	otocol Src Port	Det Port	Sec ID	Det ID	Garanted Ba	andwidth(Kbps)	Max Band	width(Kbps)	Remove
Others	9		SIGCOL SIC POIL	DSLFOIL	JIC IF	USUIF	Up Floor	Down Floor	Up Ceiling	Down Ceiling	Kelliove
		Add Sa	ve/Apply								

Figure 5-54 Traffic Shaping



5.4.4 CWMP (TR-069)

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

Status V	Vizard Setup	Advanced	Service	Firewall	Maintenance
Route	TR-069 Confi This page is used		9 CPE. Here you may cf	nange the setting for the	ACS's parameters.
NAT	ACS:				
🗵 QoS	Enable:				
CWMP	URL:		http://172.21.70.44/cpe	/?pd128	
> CWMP	User Name:		admin		
💆 Port Mapping	Password:		admin		
🗵 Others	Periodic Inform	n Enable:	O Disable 💿 Enable		
	Periodic Inform	n Interval:	300	seconds	
	Connection Re	quest:			
	User Name:		admin		
	Password:		admin		
	Path:		/tr069		
	Port:		7547		

Figure 5-55 CWMP

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



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

5.4.5 Port Mapping

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

Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance
 ☑ Route ☑ NAT ☑ QoS ☑ CWMP ☑ Port Mappin 	ng	To manipulate a 1. Select a grou 2. Select interfac buttons to mani 3. Click "Apply C	ces from the available/grou pulate the required mappir changes" button to save the elected interfaces will be r	ng of the ports. e changes.	-	vailable interface list using the arrow led to the new group.
Port Mapping						
Others		LAN		Add <de< th=""><th></th><th></th></de<>		

Figure 5-56 Port Mapping



The following table describes the parameters:

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

5.4.6 Others

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

5.4.6.1 Bridge Setting

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

Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance
Route		Bridge Sett This page is use and its attached	ed to configure the bridge	parameters. Here you c	an change the setting	s or view some information on the bridge
NAT		Ageing Time		300	(seconds	0
🛛 QoS						, ,
🛛 СWMР		802.1d Span	ning Tree:	 Disal 	oled OEnabled	
🛛 Port Mappi	ng	Apply Chang	es Undo Sh	iow MACs		
Others		- 100				
Bridge Setting						

Figure 5-57 Bridge Setting

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



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

MAC Address	Port	Туре	Aging Time
01:80:c2:00:00:00	0	Static	300
00:30: <mark>4f:29:48:90</mark>	1(0)	Dynamic	300
a8:f7:e0:00:05:56	0	Static	300
ff.ff.ff.ff.ff.ff	0	Static	300

Figure 5-58 Forwarding Table

5.4.6.2 Client Limit

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

Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance
			Configuration	L 111 2 2		
Route		i nis page is us	ed to configure the capa	ability of force now mai	ny device can access to Int	ernet!
NAT		Client Limit (apability:	ODisable 💿 Ena	ble	
🔽 QoS						
🛛 СWMP]	Maximum De	evices:	4		
🛛 🛛 Port Mappi	ing					
Others		Apply Chang	es			
> Bridge Setting	1					
> Client Limit						

Figure 5-59 Client Limit

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



5.4.6.3 Tunnel

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

Status Wiza	rd Setup	Advanced	Service	Firewall	Maintenance
	Tunnel Conf				
🛛 Route	This page is use	d to configure v6inv4 tur	inel or v4inv6 tunnel.		
NAT	V6inV4 Tunne	əl:			
🛛 QoS	Enable:				
CWMP	Interface:		(Only support IF	v4 Wan Interface)	
🛛 Port Mapping	Mode:		6to4 Tunnel 🗸		
Others					
Bridge Setting	Apply Change	25			
> Client Limit					
> Tunnel	DS-Lite Tunne	el:			
> Telnet	Enable:				
> Others	Interface:		(Only support IF	v6 Wan Interface)	
	Mode:		Auto 💉		
	Apply Change	es			

Figure 5-60 Tunnel

The following table describes the parameters:

V6inV4 Tunnel

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

DS-Lite Tunnel

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



5.4.6.4 Telnet

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

Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance
		Telnet Confi	guration d to configure telnet fun	ction		
🛛 Route		This page is use	to configure temetricit	citon		
NAT		Telnet:		⊙Disable ○Enable		
🛛 QoS]	Apply Change				
CWMP		Арру спанус				
🛛 Port Mappin	g					
2 Others						
Bridge Setting						
> Client Limit						
> Tunnel						
> Telnet						

Figure 5-61 Telnet

5.4.6.5 Others

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

Status Wizard	Setup	Advanced	Service	Firewall	Maintenance
☑ Route ☑ NAT	Here you can se	nced Configuration t other miscellaneous ad en enable Half Bridge, the	vanced settings.	nnection type will set	to Continuous.
QoS	Half Bridge:		⊙ Disable O E	nable	
CWMP	Interface:		~		
🛛 Port Mapping					
Others	Apply Change	es Undo			
> Bridge Setting					
> Client Limit					
> Tunnel					
> Telnet					
> Others					

Figure 5-62 Others



5.5 Service

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

5.5.1 IGMP

5.5.1.1 IGMP Proxy

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

Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance	
IGMP IGMP IGMP Proxy		IGMP proxy enab IGMP interfaces . Enable IGMP p	Configuration oles the system to issue I The system acts as a pr roxy on WAN interface (up n LAN interface (downstre	oxy for its hosts when y stream), which conne	you enable it by doing the cts to a router running IG		
> MLD		IGMP Proxy:		0	O Disable 💿 Enable		
UPnP		Multicast All	owed:	0	Disable 💿 Enable		
🛛 DNS		Robust Count:			2		
DDNS		Last Member Query Count:			2		
VPN		Query Interv	al:	6	0 (seconds)		
		Query Response Interval:		1	100 (*100ms)		
		Group Leave	Delay:	2	000 (ms)		
		Apply Chang	es Undo				

Figure 5-63 IGMP Proxy

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



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

5.5.1.2 MLD

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

Status Wizard	Setup	Advanced	Service	Firewall	Maintenance	
	MLD Config MLD Proxy and S	uration Snooping can be configured h	ere.			
> IGMP Proxy	MLD proxy:		• D	isable O Enable		
> MLD	MLD snoop	ing:	⊙ D	isable OEnable		
	Robust Cou	nter:	2			
UPnP DNS	Query Inter	val:	125	(Second)		
DDNS	Query Response Interval:			10000 (millisecond)		
VPN	Response I	nterval of Last Group Mer	nber:	(Second)		
	Apply Chang	es Cancel				

Figure 5-64 MLD

Field	Description		
MLD Proxy	MLD Proxy can be used to support IPv6 multicast data. Enable/Disable		
	the function to access.		
	Snooping is an IPv6 multicast constraining mechanism that runs on		
	Layer 2 devices to manage and control IPv6 multicast groups. By		
MLD Speeping	analyzing received MLD messages, a Layer 2 device running MLD		
MLD Snooping	Snooping establishes mappings between ports and multicast MAC		
	addresses and forwards IPv6 multicast data based on these mappings.		
	Multicast Listener Discovery Snooping (MLD). Enable/Disable the		

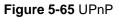


	function to access.
Robust Counter	Robust factor of the MLD Counter.
Quany Interval	The amount of time between IGMP General Query messages sent by
Query Interval	the router (if the router is a querier on this subnet).
	The maximum amount of time in seconds that the IGMP router waits to
	receive a response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

5.5.2 UPnP

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

Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance
		UPnP Confi	7			
IGMP		This page is use	ed to configure UPnP. The	e system acts as a daem	on when you enable L	JPnP.
UPnP		UPnP:		O Disable	Enable	
> UPnP		WAN Interfac	ce:			
DNS		Apply Change	es			



5.5.3 DNS

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

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



5.5.3.1 DNS

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

Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance
		DNS Config This page is use	juration ed to configure the DNS se	erver ip addresses for [DNS Relay.	
UPnP		• Attain DN	S Automatically			
DNS		O Set DNS I	Manually			
> DNS		DNS 1:	0.0.0	0		
> IPv6 DNS		DNS 2:				
DDNS		DNS 3:				
VPN		Apply Chang	es Reset Selected			

Figure 5-66 DNS

The following table describes the parameters:

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

5.5.3.2 IPv6 DNS

Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance
			onfiguration ed to configure the DNS s	erver ipv6 addresses.		
UPnP		Attain DN	IS Automatically			
DNS		O Set DNS	Manually			
> DNS						
> IPv6 DNS		DNS 1:			Interface:	~
DDNS		DN S 2:			Interface:	~
		DNS 3:			Interface:	~
		Apply Change	es Reset Selected			

Figure 5-67 IPv6 DNS



The following table describes the parameters:

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

5.5.4 DDNS

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

Status	Wizard	Setup	Advanced	Serv	vice	Firewall	Maintena	nce
IGMP					ress from DynDN	S.org or TZO or F	PLANET. Here you (can Add/Remove to
UPnP		DDNS provide	r:	Planet	~			
DDNS		Hostname:						
> DDNS		Interface:		💙				
		Enable:		V				
VPN								
		Settings:						
		Username:		admin				
		Password:		••••				
		Add Rer	nove					
		Oynamic	DDNS Table:					
		Select	State	Service	Hostname	Us	sername	Interface

Figure 5-68 DDNS

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



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

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

C PLANET DDNS	PLANET Website FAQ Support
Sign in	
Forgotten Password / Greate A New Account	

To select Service > DDNS

Dynamic DNS Configu This page is used to configure configure Dynamic DNS.	Iration the Dynamic DNS address from DynDNS.org or TZO or PLANET. Here you can Add/Remove to
DDNS provider:	DynDNS.org
Hostname:	
Interface:	
Enable:	

Step 1. Select Planet DDNS

Dynamic DNS Configu This page is used to configure configure Dynamic DNS.	ation e Dynamic DNS address from DynDNS.org or TZO or PLANET. Here you can Add/Remove to
DDNS provider:	DynDNS.org
Hostname:	DynDNS.org TZO PHDNS
Interface:	Planet
Enable:	



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

Step 3. Type the Password for your DDNS account.

Username:	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.

А п	ANET DDN	10	20	10		(NET
	ANEIDDP	19			PLAN	ET Website	FAQ	Support
Home	My Devices	Profile				Veicome, virelesstes	t (<u>Signout</u>)	
My	Device							
A	dd Device 🕂							
N	o. Your Device	Registered Domain	Name of Your Device	Last Connection IP	Ping Status	Modify	Delete	
1	ICA-HM316	wirelesstest	device	210.61.134.92	۲	1	18	



5.5.5 VPN

Status Wizard	Setup Advance	d Service Fir	ewall Maintenance	
	L2TP Configuration This page is used to configure the	parameters for your I2tp access.		
UPnP	Session:	⊙ Disable ○ Enable		
👿 DNS	Name:			
DDNS	LNS IP:			
VPN	LNS PORT:	1701		
> L2TP	Authentication:	auto 🛩		
	User Name:			
	Password:			
	Connection Type:	Continuous		
	Idle Time(min):	0		
	NAPT:	O Disable 💿 Enable		
	Default Route:	O Disable 💿 Enable		
	MTU:	1460		
	Apply Changes Reset			
	L2TP Connections:			
	Name Interf	ace IP Address	Gateway	Status

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

Figure 5-69 VPN

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



5.6 Firewall

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

5.6.1 MAC Filter

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

Status Wi	izard Setup	Advanced	Service	Firewall	Maintenance	
MAC Filter		able are used to restrict of	certain types of data packet j or restricting your local net		ork to Internet through th	e Gateway. Use
MAC Filter	Outgoing De	efault Policy	O Deny 💿 Allow			
P/Port Filter		efault Policy	O Deny 🖲 Allow			
URL Filter	Apply					
DoS	Direction:		Outgoing 💙			
	Action:		⊙ Deny ○ Allow			
	Source MAG	2	(ex. 00)	E086710502)		
	Destination	MAC:	(ex. 00	E086710502)		
	Add					
	🛞 Current	MAC Filter Table:				
	Select	Direction	Source MAC	Destina	ation MAC	Action
	Delete	Delete All				

Figure 5-70 MAC Filter

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



5.6.2 IP/Port Filter

5.6.2.1 IP/Port Filter

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

Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance
🗵 MAC Filter			e are used to restric	t certain types of data pao ng or restricting your local		work to Internet through the Gateway. Use
IP/Port Filter IP/Port Filter	er	Outgoing Defau	Ilt Policy	Permit O Deny		
> IP/Port Filter	:	Incoming Defau	Ilt Policy	O Permit Deny		
URL Filter		Rule Action: WAN Interface:		t 🔿 Deny		
DoS		Protocol:	IP 🗸			
		Direction:	Upstrea	m 💌		
		Source IP Addr	ess:		Mask Address:	255.255.255.255
		Dest IP Addres	s:		Mask Address:	255.255.255.255
		SPort:		-	DPort:	-
		Enable:				
		Apply Change	!S			

Figure 5-71 IP/Port Filter

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



5.6.2.2 IPv6/Port Filter

Status	Wizard	Setup Ad	vanced	Service	Firewall	Maintenance
MAC Filter		IPv6/Port Filtering Entries in this table are us Use of such filters can be				al network to Internet through the Gateway.
IP/Port Filte	r	Outgoing Default Polic	:y	Permit Deny		
IP/Port Filter IPv6/Port Filter		Incoming Default Polic	sy	Permit O Deny		
🗵 URL Filter		Rule Action:	Permit	O Deny		
		Protocol:	IPv6 🗸		Icmp6Type:	PING6 V
Do S		Direction:	Upstream	n 🗸		
		Source IPv6 Address:			Prefix Length:	
		Dest IPv6 Address:			Prefix Length:	
		SPort:		-	DPort:	-
		Enable:				
		Apply Changes				

Figure 5-72 IPv6/Port Filter

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



5.6.3 URL Filter

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

Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance
		URL Blocki	ng Configuration			
MAC Filter		This page is us	ed to configure the filtere	d keyword. Here you can	add/delete filtered key	word.
🛛 IP/Port Filte	er	URL Blocking	g Capability:	⊙ Disable ○ Enable	е	
🔁 URL Filter		Apply Chang	es			
> URL Filter						
_		Keyword:				
ACL						
🔽 DoS		AddKeyword	Delete Selected	Keyword		
		③ URL Blo	cking Table:			
		Select		Filte	ered Keyword	

Figure 5-73 URL Filter

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



5.6.4 ACL

5.6.4.1 ACL

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



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

Status Wizard	Setup	Advanced	Service	Firewall	Maintenance	
MAC Filter	Entries in this ACL t Gateway.	ch services are acce able are used to per			twork or Internet network to the nent.	
URL Filter ACL	LAN ACL Mode: WAN ACL Mode:		 White List White List 		lack List	
> ACL > IPv6 ACL	WAN ACL Mode: White List Black List Apply					
🛛 DoS	Direction Select		⊗ LAN O WAN			
	LAN ACL Switch:		O Enable	⊙ Di:	Oisable	
	IP Address: Services Allowe	d:	-	(The IF	0.0.0.0 represent any IP)	
	🗹 Any					
	Add	. Table:				
	Select	Direction	IP Address/Int	terface S	ervice Port Action	

Figure 5-74 ACL



The following table describes the parameters:

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

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

Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance	
MAC Filter		Entries in this AC Gateway	which services are acce CL table are used to pe	essable form LAN or WA rmit certain types of data Ipful in securing or restr	i packets from your loca	I network or Internet network to the agment.	
URL Filter		LAN ACL Mod	le:	• White List	C	Black List	
> ACL		WAN ACL Mo	de:	• White List	C	Black List	
> IPv6 ACL		Apply					
DoS		Direction Select: O LAN O WAN					
		WAN Setting:		Interface 💌			
		WAN Interfac	e:	Any 🕶			
		Services Allowed:					
		web					
		telnet					
		ssh					
		🗖 ftp					
		🗆 tftp					
		D ping					

Figure 5-75 ACL WAN





5.6.4.2 IPv6 ACL

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

Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance	
MAC Filter	r	Entries in this A Gateway.	which services are acce CL table are used to per			etwork or internet network to ment.	the
URL Filter		Direction Se	lect:				
> ACL > IPv6 ACL		LAN ACL Sw Apply	vitch:	O Enable		sable	
🛛 DoS		IP Address:			1		
		Services All	owed:				
		Add					
			IPv6 ACL Table:		1	E and E	
		Directio	in IF	Pv6 Address/Interface	Service	_	_
		WAN		any	ping6	Dele	ete

Figure 5-76 IPv6 ACL



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

Status Wizard	Setup	Advanced	Service	Firewall	P	Maintenanc	e
MAC Filter	Entries in this ACL t Gateway	ch services are acce able are used to per	mit certain types (or WAN side. of data packets from you r restricting the Gateway			twork to the
URL Filter	Direction Select:	•	O LAN 🖸	WAN			
> ACL > IPv6 ACL	WAN Setting: WAN Interface: Services Allowe		Interface 💌				
	web	u.					
	□ telnet						
tfp tfp tfp tfp ping6							
	Add						
	Direction	IF	v6 Address/Inter any	face	Service ping6	Port 	Action Delete

Figure 5-77 IPv6 ACL WAN



5.6.5 DoS

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

Status Wizard	Setup Advanced S	ervice Firewall Maintenance		
MAC Filter	DoS Setting A "denial-of-service" (DoS) attack is characterized using that service.	by an explicit attempt by hackers to prevent legitimate users of a service from		
 IP/Port Filter URL Filter 	Enable DoS Prevention			
ACL	Whole System Flood: SYN	100 Packets/Second		
> DoS	Whole System Flood: FIN	100 Packets/Second		
	Whole System Flood: UDP	100 Packets/Second		
	Whole System Flood: ICMP	100 Packets/Second		
	Per-Source IP Flood: SYN	100 Packets/Second		
	Per-Source IP Flood: FIN	100 Packets/Second		
	Per-Source IP Flood: UDP	100 Packets/Second		
	Per-Source IP Flood: ICMP	100 Packets/Second		
	TCP/UDP PortScan	Low Sensitivity		
	CMP Smurf			
	IP Land			
	IP Spoof			
	IP TearDrop			
	PingOfDeath			

Figure 5-78 DoS

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



5.7 Maintenance

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

5.7.1 Update

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



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

5.7.1.1 Firmware Update

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

Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance	
 Update Firmware Upda 	te	because it may			on. Please note, do not j	oower off the device during the uplo	ad
> Backup/Restore	9	Select File:		Desure No file o			
		Select File:		Browse No file s	elected.		
Password		Upload	Reset				
Reboot							
Time							
Discussion							
Diagnostics	8						

Figure 5-79 Firmware Update

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



5.7.1.2 Backup/Restore

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

Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance	ſ.
			store Settings	save the configuration set	ings to a configuration t	île on your hard drive. You al:	so have the
🔰 Update	19 1		infiguration settings.	are the configuration coa		no on jour nard ante. Tod an	o navo uro
> Firmware Upda	ate						
Backup/Restor	re	Save Setting	s to File:	Save			
					_		
Password		Load Setting	s from File:	Browse No file s	elected.	Ipload	
🗵 Reboot							
🔽 Time							
🔽 Log	2						
🔽 Diagnostic	5						

Figure 5-80 Backup/Restore

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



5.7.2 Password

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

Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance		
👿 Update			nt Configuration ad to add user account to	access the web s	erver of DSL Router. Empty	user name or password is not allowed.		
Password		User Name:						
> Password		Privilege:			User 💌			
🛛 Reboot		Old Passwor	rd:					
🛛 Time		New Passwo	ord:					
🛛 Log		Confirm Pase	sword:					
Diagnostics		Add Mo	odify Delete	Reset				
		💿 User Acc	ount Table:					
		Selec	:t	UserN	ser Name Privilege			
		0		admin		root		

Figure 5-81 Password

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



5.7.3 Reboot

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

Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance
		Reboot				
			ed to reboot your system o	r restore to default setti	ng.	
🗵 Update						
🛛 Password	2	Reboot	Restore to Default Sett	ing		
🛛 Reboot						
> Reboot						

Figure 5-82 Reboot

The following table describes the parameters:

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



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



5.7.4 Time

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

Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance
👿 Update			o configure the syste	m time and Network Tim ne and NTP parameters.	e Protocol(NTP) server	: Here you can change the settings or
Password		System Time:	2012 Y	ear Jan 💙 Month 1	Day 4 Hou	ur 16 min 19 sec
Time		DayLight:	LocalTIME	~		
> Time		Apply Changes	Reset			
🐱 Log		NTP Configurati	on:			
💟 Diagnostics		State:	Oisable	Enable		
		Server:				
		Server2:				
		Interval:	Every 1	hours		
		Time Zone:	(GMT) Ga	mbia, Liberia, Morocco, E	England	~
		GMT time:	Sun Jan 1 4	:16:19 2012		
		Apply Changes	Reset			
		NTP Start:	Get GMT	Time		

Figure 5-83 Time

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



5.7.5 Log

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

Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance
		Log Setting				
🔽 Update			ed to display the system ev ay the newest log informa		cking Error or Notice (or I	both)will set the log flag. By clicking the
🛛 Password		Error:			Notice:	
🛛 Reboot						
🛛 Time		Apply Change	es Reset			
🛛 Log		Event log Tab	le:			
> Log		Save Log		able		
😡 Diagnostics		Old I<<		>> New		
		Т	ime Index	Туре	Log	Information
		Page: 1/1				

Figure 5-84 Log

The following table describes the parameters:

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

5.7.6 Diagnostic

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

5.7.6.1 Ping

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



Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance
		Ping Diagno	ostic			
🗵 Update		Host:				
🔽 Password		11030		L		
🔽 Reboot		Interface:				
🗹 Time		PING				
🛛 Log						
Diagnostics						
> Ping						

Figure 5-85 Ping

The following table describes the parameters:

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

5.7.6.2 Ping6

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

Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance
		Ping6 Diagr	ostic			
☑ Update ☑ Password		Host:				
Reboot		Interface:				
🔽 Time		PING				
🛛 Log						
Diagnostics						
> Ping						
> Ping6						

Figure 5-86 Ping6

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



5.7.6.3 Traceroute

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

Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance
		Traceroute [Diagnostic			
🛛 Update		Host :			NumberOfTries :	3
🛛 Password						
👿 Reboot		Timeout :	5000 m	S	Datasize :	38 Bytes
👿 Time		DSCP :	0		MaxHopCount :	30
🔽 Log		Interface :	any			
🗵 Diagnostics	•	6				
> Ping		traceroute	Show Result			
> Ping6						
> Traceroute						

Figure 5-87 Traceroute

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



5.7.6.4 Traceroute6

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

Status V	Vizard Setup	Advanced	Service	Firewall	Maintenance
	Traceroute6	Diagnostic			
☑ Update ☑ Password	Host:			NumberOfTries :	3
Reboot	Timeout :	5000 n	ns	Datasize :	38 Bytes
🛛 Time	MaxHopCoun	t: 30		Interface :	any 💙
🛛 Log	traceroute	Show Result			
Diagnostics		Show Result			
> Ping					
> Pin <mark>g</mark> 6					
> Traceroute					
> Traceroute6					

Figure 5-88 Traceroute6

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



5.7.6.5 OAM Loopback

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

Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance		
🛛 Update		Connectivity verif	Management - Con fication is supported by th the VCC loopback functio	e use of the OAM loopb	ack capability for both \	/P and VC connections. This p	page is	
Password		Flow Type:						
Time		 F5 Segm F5 End-to 						
LogDiagnostics		F4 Segment F4 End-to-End						
> Ping > Ping6		VPI:						
Traceroute Traceroute6		VCI:						
> OAM Loopback		Go !						

Figure 5-89 OAM Loopback

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



5.7.6.6 DSL Diagnostic

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

Status Wizard	d Setup	Advanced	Service	Firewall	Maintenance	
	Diagnostic DS	SL				
🔽 Update	Dsl Tone Diagnost					
Password	Start					
🛛 Reboot			Downstream		Upstream	
🔽 Time	Hlin Scale					
🔽 Log	Loop Attenua	tion(dB)				
Diagnostics	Signal Attenu	ation(dB)				
> Ping	SNR Margin(d					
> Ping6						
> Traceroute		Attainable Rate(Kbps) Output Power(dBm)				
> Traceroute6	oupuriower					
> OAM Loopback	Tone Numbe	r H.Real	H.Image	SNR	QLN	Hlog
> DSL Diagnostic	0					

Figure 5-90 DSL Diagnostic

Click Start to start ADSL tone diagnostics.



5.7.6.7 Diag-Test

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

Status	Wizard	Setup	Advanced	Service	Firewall	Maintenance
💟 Update						low. If a test displays a fail status, click
 Password Reboot 		Select the Int	ternet Connection: WAN	J1 🕶	Run Diagnostic Te	st
👿 Time						
🛛 Log						
Diagnostics						
> Ping						
> Ping6						
> Traceroute						
> Traceroute6						
> OAM Loopback	t I					
> DSL Diagnostic	:					
> Diag-Test						

Figure 5-91 Diag-Test

Click Run Diagnostic Test to start testing.



Chapter 6. Quick Connection to a Wireless Network

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

6.1 Windows XP (Wireless Zero Configuration)

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



Figure 6-1 System Tray – Wireless Network Icon

Step 2: Select [View Available Wireless Networks]

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

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

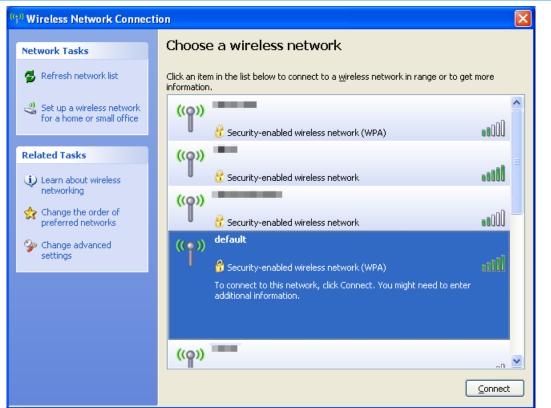


Figure 6-2 Choose a wireless network



Step 4: Enter the encryption key of the Wireless AP

- (1) The Wireless Network Connection box will appear
- (2) Enter the encryption key that is configured in section 5.3.3.2
- (3) Click the [Connect] button

Wireless Network Conne	ection	×			
	es a network key (also called a WEP key or WPA key). unknown intruders from connecting to this network.				
Type the key, and then click Connect.					
Network <u>k</u> ey:	•••••				
C <u>o</u> nfirm network key:	••••••				
	Cancel				

Figure 6-3 Enter the network key

Step 5: Check if "Connected" is displayed

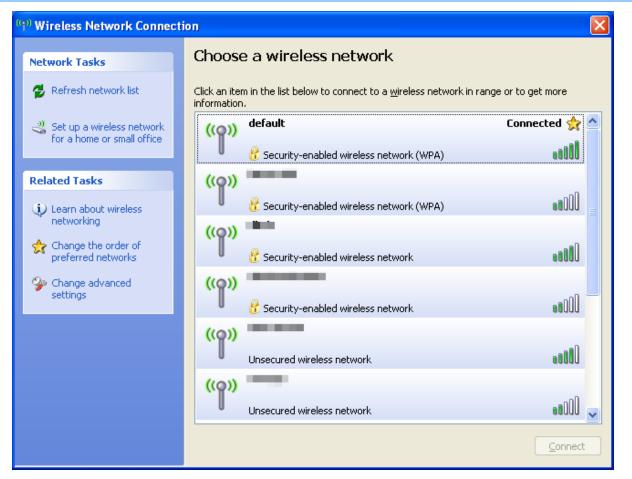


Figure 6-4 Choose a wireless network -- Connected





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

6.2 Windows 7 (WLAN AutoConfig)

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

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



Figure 6-5 Network icon

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

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



Figure 6-6 WLAN AutoConfig





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

Step 4: Enter the encryption key of the Wireless AP

- (1) The Connect to a Network box will appear
- (2) Enter the encryption key that is configured in section 5.3.3.2
- (3) Click the [OK] button

ype the netwo	'k security key
Security key:	
	Hide characters
6	You can also connect by pushing the button on the router.

Figure 6-7 Type the network key

P Connect to a Network	×
Connecting to default	
	Cancel

Figure 6-8 Connecting to a Network



Step 5: Check if "Connected" is displayed



Figure 6-9 Connected to a Network



6.3 Mac OS X 10.x

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

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

The AirPort Network Connection menu will appear



Figure 6-10 Mac OS – Network icon

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

- (1) Select and SSID [default]
- (2) Double-click on the selected SSID



Figure 6-11 Highlight and select the wireless network

Step 4: Enter the encryption key of the Wireless AP

- (1) Enter the encryption key that is configured in section 5.3.3.2
- (2) Click the [OK] button



The network "default" requires a WPA password.
Password:
Show password Remember this network
Cancel OK

Figure 6-12 Enter the Password



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

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

		* 🛜	•			Ø	Q.
	AirPort: On Turn AirPort Off						
100 C 100 C 100 C	√default	6 1		-			
	The second se	0					
	The second se	((;;					
		1					
		ê 🔶	1		*		
	1081-0800CM	((+					
	incast.	9	-				
and the first when the	and the second se	ê 🔶	1.00				
	100 C	9					
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	jone) Terred	ê 🤅	125				
a second s	Inc. Management	₽ 🔶	-				
	The second s	₽ 🔅					
	Join Other Network Create Network Open Network Preferences						
		_					

Figure 6-13 Connected to the Network



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

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

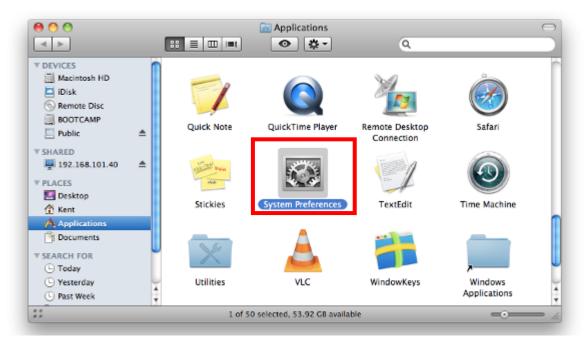


Figure 6-14 System Preferences

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



Figure 6-15 System Preferences -- Network



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

- (1) Choose the AirPort on the left-menu (make sure it is ON)
- (2) Select Network Name [default] here

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

0 0	Network		
Show All		٩	
L	ocation: Automatic	•	
USB Ethernet Not Connected	Status: On	Turn AirPort Off	
• 802.11dapter		ort is turned on but is not connected to work.)
• AirPort	Network Name 🗸 No	network selected	
Home VPN			(î: (
	def	ault	
			÷.
			(¢
			<u></u>
			÷.
		n Other Network eate Network	
+ - &-	Show AirPort status in r	menu bar Advanced	?
Click the lock to preve	nt further changes.	ssist me Revert	Apply

Figure 6-16 Select the Wireless Network



6.4 iPhone/iPod Touch/iPad

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

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



Figure 6-17 iPhone – Settings icon

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

- (3) Tap [General] \ [Network]
- (4) Tap [Wi-Fi]

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

iPad	10:35 AM	100%
Settings	General	
Airplane Mode OFF		
S Wi-Fi Not Connected	About	>
Notifications On	Usage	>
Carrier	Sounds	>
🕎 Cellular Data		
🙀 Brightness & Wallpaper	Network	>
Picture Frame	Bluetooth	Off >
General	Location Services	On >
Salendars Mail, Contacts, Calendars	Spotlight Search	>
Mafari Safari		

Figure 6-18 Wi-Fi Setting



Pad	10:35 AM 🛞 100% 📾
Settings	General Network
Airplane Mode OFF	
Wi-Fi Not Connected	VPN Not Connected >
Notifications On	Wi-Fi Not Connected >
Carrier	
🕎 Cellular Data	
🙀 Brightness & Wallpaper	
Picture Frame	
General	
Mail, Contacts, Calendars	
🛃 Safari	

Figure 6-19 Wi-Fi Setting - Not Connected

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

- (1) Turn on Wi-Fi by tapping "Wi-Fi"
- (2) Select SSID [default]

iPad		11:23 PM	A 76%
Se	ttings	Network Wi-Fi	Networks
Airplane M	ode OFF		
🛜 Wi-Fi	Not Connected	Wi-Fi	ON
Notification	ns On	Choose a Network	
Location S	ervices On	default	₽ \$ 0
🔣 Cellular Da	ita	Other	>
Brightness	& Wallpaper	Ask to Join Networks	
Picture Fra	me		e joined automatically. If no available, you will be asked
General			ng a new network.

Figure 6-20 Turn on Wi-Fi

Step 4: Enter the encryption key of the Wireless AP

- (1) The password input screen will be displayed
- (2) Enter the encryption key that is configured in section 5.3.3.2



(3) Tap the [Join] button

		_	11:20 PM					@ 78%
Settings		1100	eqtk	Wi	Fi Netv	vorks		
Airplane Mode	OFF							
Wi-Fi	CA8-4		Wi-Fi				ON	
Notifications	On		Choose a	Network				
Location	4	10000	V CA8-4		-		84	0
Cellular Curter	1		password for				8.5	• •
Brightne		- Contraction	1 1 0 0 0 1	TOTA			-10	5
Picture I Passv	word		••					-
							2N	
General							anke	no ed
Mail, Co								
👸 Safari							- 84	
iPod							- 8	
Video							- 8	
Photos								
Notes								
Store								
Store								
inge		5		7		0		
Store	4	5	6	7	8	9	0	e
inge	4	5	6	7	8	9	-	Join
1 2 3	4	5 (6) ?	ų	-	-	-	Join #+=

Figure 6-21 iPhone -- Enter the Password

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

If "Yes", then there will be a "check" symbol in the front of the SSI	f "Yes",	then there	will be a '	'check" s	ymbol in	the front	of the SS
---	----------	------------	-------------	-----------	----------	-----------	-----------

iPad	11:25 PM 💽 75%	
Settings	Network Wi-Fi Networks	
Airplane Mode OFF		
🛜 Wi-Fi default	Wi-Fi ON	
Notifications On	Choose a Network	
Location Services On	✓ default 🔒 🗢 📀	
🕎 Cellular Data	Other >	
🙀 Brightness & Wallpaper	Ask to Join Networks	
Picture Frame	Known networks will be joined automatically. If no known networks are available, you will be asked before joining a new network.	
🚳 General		

Figure 6-22 iPhone -- Connected to the Network



Appendix A: Cable Profiles

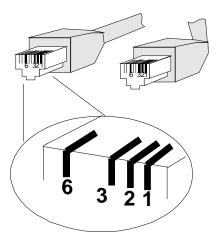
A.1 Device's RJ45 Pin Assignments

■ 10/100Mbps, 10/100BASE-TX

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

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

A.2 RJ45 Cable Pin Assignment



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



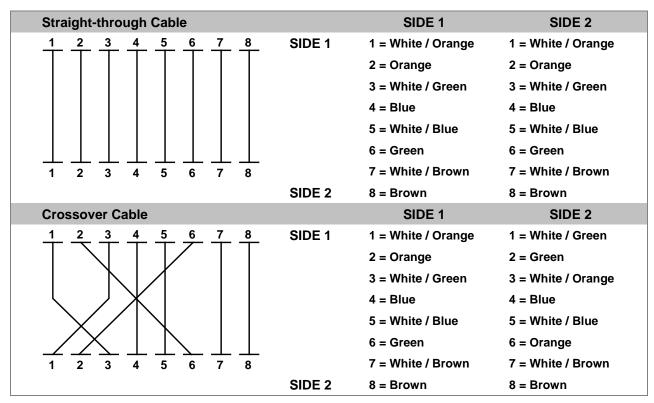


Figure A-1: Straight-through and Crossover Cables

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

EC Declaration of Conformity

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