P.DG A4001N

User Manual

CONTENTS

Welcome

ABOUT THIS GUIDE

This guide describes how to install and configure the **Home Station ADSL ADB P.DG A4001N**. This guide is intended for use by those responsible for installing and setting up network equipment; consequently, it assumes a basic working knowledge of LANs (Local Area Networks) and Internet Routers.

NAMING CONVENTION

Throughout this guide, the **P.DG A4001N** is referred to as the “Wireless Router”. Category 5 Ethernet Cables are referred to as Ethernet Cables throughout this guide.

CONVENTIONS

Table 1 and Table 2 list conventions that are used throughout this guide.

TABLE 1. Notice Icons

Icon	Notice Type	Description
ℹ	Information note	Information that describes important features or instructions.
⚠	Caution	Information that alerts you to potential loss of data or potential damage to an application, system, or device.

TABLE 1. Notice Icons

Icon	Notice Type	Description
⚠	Warning	Information that alerts you to potential personal injury.

TABLE 2. Text Conventions

Convention	Description
The words “enter” and “type”	When you see the word “enter” in this guide, you must type something, and then press Return or Enter. Do not press Return or Enter when an instruction simply says “type.”
Keyboard key names	If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press Ctrl+Alt+Del
Words in italics	Italics are used to: • Emphasize a point. • Denote a new term at the place where it is defined in the text. • Identify menu names, menu commands, and software button names. Examples: “From the *Help* menu, select *Contents*. Click *OK*.”

Introduction

INTRODUCTION

The **Home Station ADSL ADB P.DG A4001N** is designed to provide a cost-effective mean of sharing a single broadband Internet connection between several wired and wireless computers. The Data Gateway also provides protection in the form of an electronic "firewall" preventing anyone outside of your network from seeing your files or damaging your computers.

The **P.DG A4001N** is an ADSL2+ Data Gateway, targeted to residential environments and SOHO customers, that provides routed broadband services from a single and modular access point.

The **P.DG A4001N** is the ideal solution for:

1. Connecting multiple PCs and Video game consoles;
2. Sharing broadband internet connections with all home computers;
3. Sharing printers and peripherals.

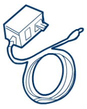
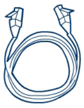
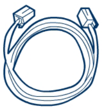
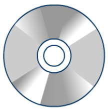
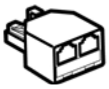
PACKAGE CONTENTS

Your new **Home Station ADSL ADB P.DG A4001N** ADSL2+ Data Gateway kit contains the related hardware and software. In it you will find:

1. One **P.DG A4001N** unit
2. One Power Supply
3. Nr.1 Ethernet CAT5 cable RJ-45 plug
4. Nr.1 Phone cable RJ-11 plug (ADSL)
5. Nr.3 DSL Microfilter

6. Nr.1 T-connector adapter
7. Nr.1 Quick Installation Guide & Safety leaflet
8. A CD-ROM

TABLE 1. Kit Material

	Quantity	DESCRIPTION
	1	*Home Station DSL ADB P.DG A4001N*
	*1*	*Power supply*
	*1*	*Ethernet Cable*
	*1*	*Phone cable*
	*1*	*CD-ROM*
	*1*	*T-Connector adapter*
	3	*ADSL MicroFilters*

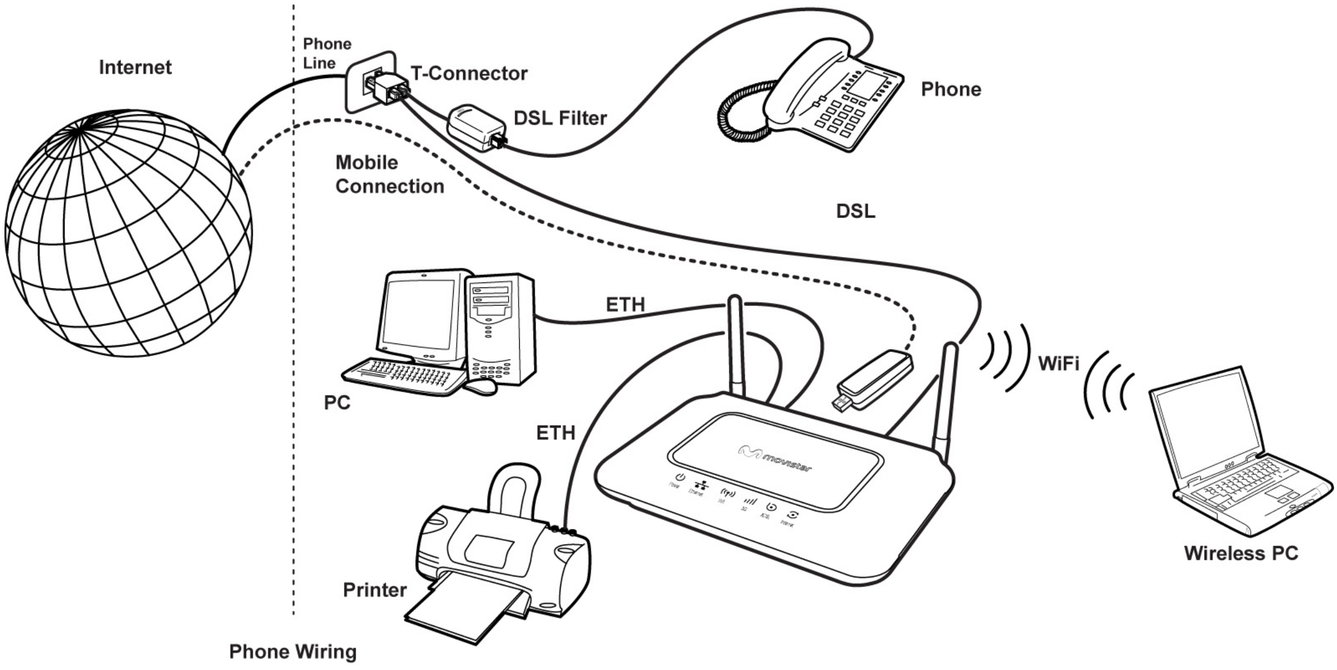
If any of the items included in the package is damaged, please contact your Service Provider.

It implements an high speed Asymmetric Digital Subscriber Line (ADSL2/2+) connection to the telephone line on the WAN side, as well as several local connectivity technologies on the LAN side:

- Four switched 10/100 Base-T/TX Ethernet ports
- A Wi-Fi connection to hosts devices

Figure 1 shows a sample network: your Home Station ADSL becomes your connection to the Internet. Connections can be made directly to the Home Station ADSL expanding the number of computers you can have in your network.

FIGURE 1. Sample Home Network



DATA GATEWAY ADVANTAGES

The advantages of the **Home Station ADSL ADB P.DG A4001N** include:

- Shared Internet connection for both wired and wireless computers

- High speed 802.11b/g/n wireless networking
- Cross-platform operation for compatibility with Microsoft® Windows, Linux and Apple® MAC computers
- Easy-to-use, Web-based setup and configuration
- Centralization of all network address settings (DHCP)
- A Virtual server to enable remote access to Web, FTP, and other services on your network
- A Security - Firewall protection - against Internet hacker attacks and encryption to protect wireless network traffic

APPLICATIONS

Many advantages networking features are provided by the **Home Station ADSL ADB P.DG A4001N**:

- **Wireless and Wired LAN**: the Home Station ADSL provides connectivity to 10/100 Mbps devices and wireless IEEE 802.11b/g/n compatible devices, making it easy to create a network in small offices or homes.
- **3G Access**: the Home Station ADSL allows you to have a primary or a backup line through 3G connectivity. Please contact your ISP to have the list of compatible 3G keys.
- **Internet Access**: this device supports Internet access through an ADSL connection or a 3G connection. Since many DSL providers use PPPoE or PPPoA to establish communications with end users, the Home Station ADSL includes built-in clients for these protocols, eliminating the need to install these services on your computer.

HARDWARE DESCRIPTION

The Home Station ADSL contains an integrated ADSL modem and connects to the Internet or to a remote site through the ADSL (RJ11) port. It can be connected directly through your PCs or to a local area network using the four Fast Ethernet LAN ports.

Access speed to the Internet depends on your service type. Full rate ADSL provides up to 8 Mbps downstream and 1 Mbps upstream. G.lite (or splitterless) ADSL provides up to 1.5 Mbps downstream and 512 kbps upstream. However, you should note that the actual rate provided by specific service providers may vary dramatically from these upper limits.

Data passing between devices connected to your local area network can run at up to 100 Mbps over the Fast Ethernet ports and up to 300 Mbps over the built-in wireless access point.

The Home Station ADSL makes available one USB 2.0 host interface for advanced added value services such as file sharing, HSPA Data Connection and Backup. 3G connectivity requires an additional dedicated hardware: please contact your service Operator dealer for further information on available 3G keys' compatible models.

MINIMUM SYSTEM AND COMPONENT REQUIREMENTS

Your Home Station ADSL requires the computer(s) and components in your network to be configured with at least the following:

- A computer with the Operating Systems that support TCP/IP networking protocols: Microsoft® Windows 2000, Windows XP 32bit, Vista 32bit, Windows 7 or Apple® MAC 10.x or Linux
- Internet access account from your Internet Service Provider (ISP)
- A PC using a dynamic IP address assigned via DHCP, as well as a gateway server address and DNS server address from your service provider
- A PC equipped with 10/100 Mbps Fast Ethernet adapter
- TCP/IP networks protocols installed on each PC that will access the Internet
- A Java-enabled web browser, such as Microsoft Internet Explorer 6.0 or above, Mozilla Firefox 2.0 or Above installed on one PC at your site for configuring the Data Gateway

FRONT PANEL

The front panel of the Home Station ADSL contains six indicator lights (LEDs) that help to describe the state of networking and connection operations.

FIGURE 2. Front Panel LEDs

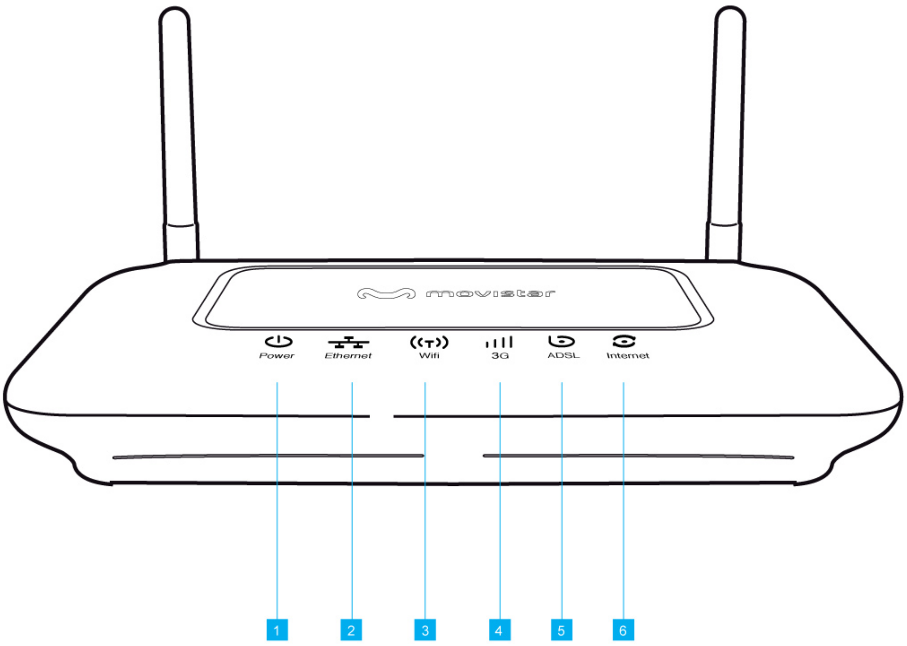


TABLE 2. **LED Description**

Ref.	LED	LED Colour		LED Description
1	***Power***	*Green/Red*	*On*	*Power on normal operation mode*
			Off	*Power off or failure*
2	***Ethernet***	*Red*	*On*	*Ethernet connection active*
			Blinking	*Data exchange*
			Off	No Ethernet connection active
3	***Wifi***	*Green*	*On*	Wireless functionality enabled
			Blinking	Wireless LAN activity present (traffic in either direction)
			Off	Wireless functionality disabled
4	***3G***	*Green*	*On*	*USB 3G Key is connected*
			Off	*USB 3G Key is not connected*
5	***ADSL***	*Green*	*On*	*ADSL link is up and connected*
			Blinking	*Router detects network clock and start DSL negotiation*
			Fast Blinking	*Router is in its final stage of link negotiation*
6	***Internet***	*Green*	*On*	*WAN IP address available (PPP active)*
			Off	*Modem power off or WAN IP address not available (PPP failure)*

REAR PANEL

The rear panel of the Router contains a Reset Configuration to Factory Default button, a power adapter socket, a Power on button, four LAN ports, one ADSL port, a Wifi button and one USB 2.0 device port.

FIGURE 3. **Rear Panel Ports**

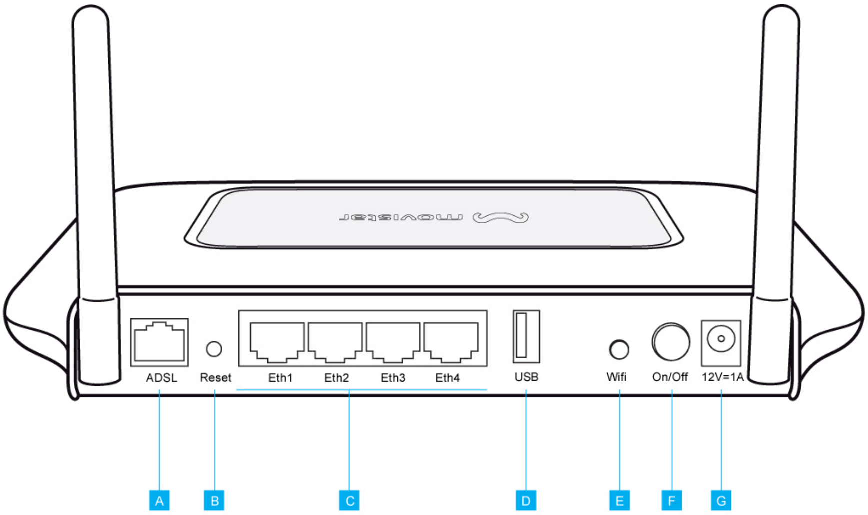


TABLE 3. **Port Description**

PORT	DESCRIPTION
A	*Phone ADSL connector (ADSL2/2+)*
B	*Reset Configuration to factory default*
C	*Four Ethernet ports 10/100 Mbps*
D	*USB 2.0 port*
E	*Wifi Button*
F	*Power Button*
G	*Power Adapter port*

The Wifi button is located on the rear panel. Press this button for at least 5 second when activating the WPS function.

This Page Intentionally left blank

Hardware Installation

This chapter will guide you through a basic installation of the **Home Station ADSL ADB P.DG A4001N** including:

1. Positioning the **P.DG A4001N**
2. Installing T-connector Micro Filters
3. Connecting the Home Station ADSL to your network
4. Setting up your computer for networking with the Home Station ADSL

⚠ *Please read carefully the Safety Information in Appendix "A"*

ISP SETTINGS

Please collect the following information from your ISP before setting up the Home Station ADSL:

- IP address for your ISP's Gateway Server and Domain Name Server

POSITIONING THE HOME STATION ADSL

The Home Station ADSL can be positioned at any convenient location in your office or home. No special wiring or cooling requirements are needed. You should, however, comply with the following guidelines:

- Keep the Home Station ADSL away from any heating devices
- Do not place the Home Station ADSL in a dusty or wet environment

You should also remember to turn off the power, remove the power cord from the outlet and keep your hands dry when you install the Home Station ADSL.

INSTALLING T-CONNECTOR AND MICRO FILTERS

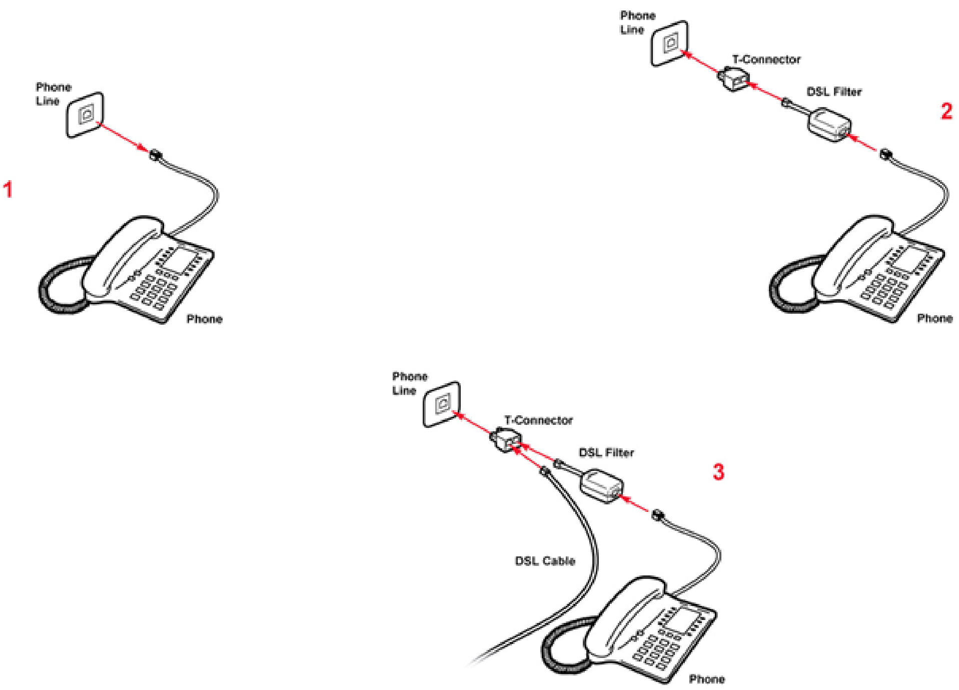
Before beginning installation you must locate devices in your house requiring a DSL filter such as phones, fax machines, answering machines, dial-up modems, Satellite TV dialers or monitored security systems and attach a DSL filter to any one of them sharing the same phone line as your DSL modem.

To install T-connector and DSL filters please follow these steps:

1. Disconnect the phone cable from the telephone wall socket
2. Insert the T-connector into the telephone wall socket
3. Insert the DSL Filter into one port of the T-connector and the phone cable into the DSL Micro-filter port
4. Insert the DSL cable into the other port of the T-connector

⚠ *You do not need to attach a DSL filter to unused wall sockets.*

FIGURE 2. Micro Filter Installation

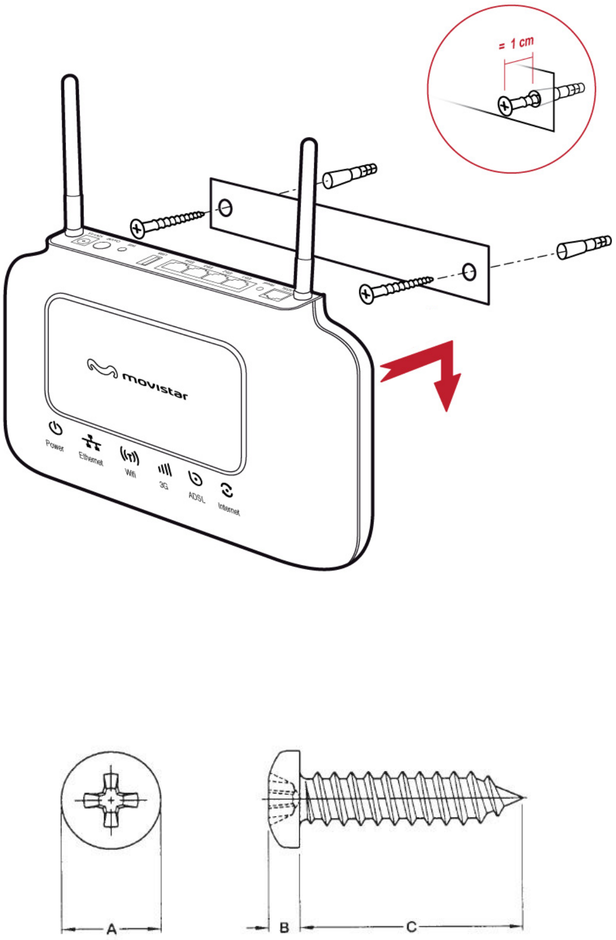


WALL MOUNTING

In case a wall mount would be needed, please follow below instructions:

1. Get hold of two screws and fitting nogs (not included) as shown in next Figure.
2. Fix the nogs, by using as holes' guide the board mask included in the box (and that can be cutted from the box itself.
3. Tighten the screws into the nogs, taking care to leave about 1 cm the screw head above wall surface
4. Remove the self-adhesive rubber feet from Home Station ADSL bottom base
5. Hang the bottom of Home Station DSL to screws' heads as shown in figure 3

FIGURE 3. **Wall mounting**



A :6.5 +-0.5mm
B :2.2+-0.2mm
C :25.5+-0.8mm
D:3.1---3mm
Unit: mm

POWERING UP THE HOME STATION ADSL

To power up the Home Station ADSL:

1. Plug the power adapter into the power adapter port located on the rear of the Home Station ADSL
2. Plug the power adapter into a standard electrical wall socket
3. Press the Power button located on the rear panel of the Home Station ADSL
4. Wait for the power LED to turn steady green

In case of power input failure, the Home Station ADSL will automatically restart and begin to operate once the input power is restored.

If the Home Station ADSL is properly configured, it will take about 90 seconds to establish a connection with the ADSL service provider after powering up.
During this time the ADSL LED will flash. After the ADSL connection has been established, the ADSL LED indicator will stay on.

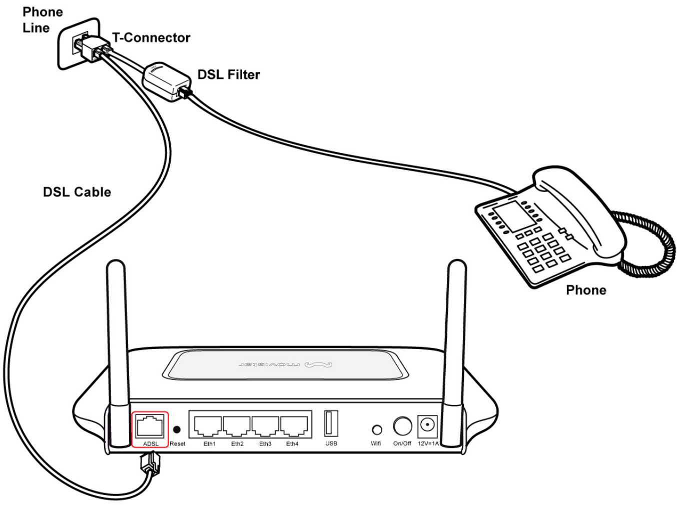
CONNECTING THE HOME STATION ADSL

The first step to install the Home Station ADSL is to physically connect it to the telephone socket and then to connect it to a computer with Ethernet connection. After these steps, in case a compatible 3G Key will be available, the 3G key connection and configuration will be needed.

To connect the phone cable:

1. Connect one end of the phone cable into the T-connector adapter which is inserted into the wall plug.
2. Connect the other end of the phone cable into the DSL port on the rear of the Home Station ADSL

FIGURE 4. Phone Cable Connection



To connect the Ethernet cable:

1. Connect one end of the Ethernet cable into one of the four Ethernet ports on the rear of the Home Station ADSL
2. Connect the other end of the Ethernet cable into the Ethernet Network card of your computer
3. Verify if the Ethernet Network card is configured as DHCP client, otherwise configure it to remain in the same local network of the Home Station ADSL interface (see chapter "Setting Up Your Computer")

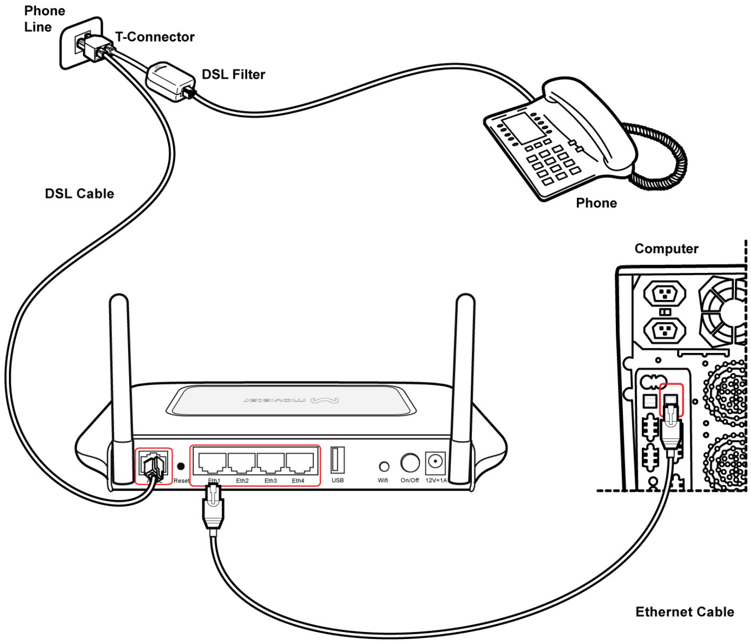
The LAN port on the Home Station ADSL auto-negotiates the connection speed and the duplex mode with the connecting device.

Use twisted-pair cabling to connect the Home Station ADSL to an Ethernet adapter on your PC. Otherwise, cascade any of the LAN ports on the Home Station ADSL to an Ethernet hub or switch. When inserting an RJ-45 connector, be sure the tab on the connector clicks into position to ensure that is properly seated.

⚠ *Do not plug a phone jack into RJ-45. This may damage the Home Station ADSL. Instead, use only twisted-pair cables with RJ-45 connectors that conform with FCC standards.*

ℹ *Use 100-ohm shielded or unshielded twisted-pair cable with RJ-45 connectors for all Ethernet ports. We recommend using Category 5 cable for connections with the device. Also, make sure the lenght of each twisted-pair cable does not exceed 100 meters (328 feet).*

FIGURE 5. Ethernet Cable Connection

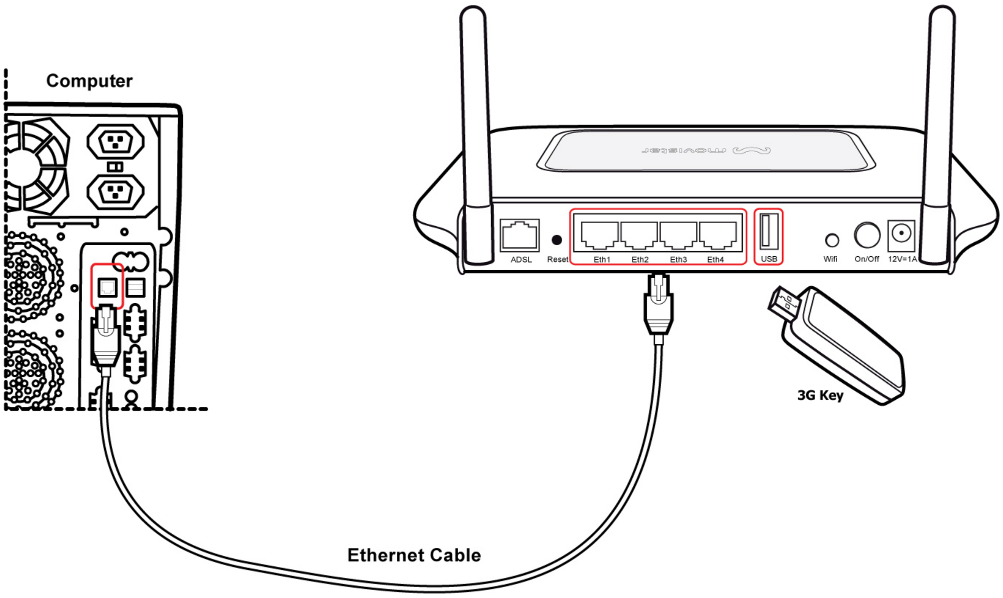


The Home Station ADSL has the ability to dynamically allocate network addresses to the computers on your network using DHCP. However, your computers need to be configured correctly for this to take place. To change the configuration of your computers to allow this, follow the instructions in this chapter.

To connect the compatible 3G Key (please verify with your ISP the key compatibility to your Home Station DSL device):

1. Plug the 3G key in the USB port on the rear of the Home Station ADSL
2. Access to the Home page of the Home Station DSL to properly configure the 3G key

FIGURE 6. **3G Key Connection**



Please refer to the paragraph “3G key” for a detailed how-to description.

ETHERNET CONNECTION

You have to verify the existence of a TCP/IP protocol stack and, then, according to your Operating System, to establish an Ethernet connection to the Home Station ADSL. This connection will require you to enable your computer to receive from the Home Station ADSL its own IP Address automatically: in such a case, the Home Station ADSL acts like the DHCP server in your local network.

TCP/IP CONFIGURATION

To access the Internet through the Home Station ADSL, you must configure the network settings of the computers on your LAN to use the same IP subnet as Home Station ADSL. The default IP settings for the Home Station ADSL are:

IP ADDRESS: 192.168.1.1

SUBNET MASK: 255.255.255.0

These settings can be changed to fit your network requirements, but you must first configure at least one computer to access the Home Station ADSL's web configuration interface in order to make the required changes.

ETHERNET CONNECTION >> TCP/IP PROTOCOL INSTALLATION

This procedure requires the TCP/IP protocol installed on your computer. Refer to the following chapters and to your Windows and MacOS operating systems manuals.

Microsoft Windows 2000

1. Put in the CD-ROM drive your Windows installation CD-ROM.
2. Starting from Start -> Settings -> Control Panel or Start -> Control Panel depending on the configuration of your computer.
3. Make a double click on the Network and Dial-up Connections icon.
4. Select the interested Network Adapter icon and from the contextual menu, do select the Properties item.
5. If the Internet Protocol (TCP/IP) component is not checked you must enable it by checking the Internet Protocol (TCP/IP) item; otherwise, if it is not listed, you must install it by selecting the Install... button.
6. Choose the Protocol Network component and click on the Add.. button.
7. In the Select Network Protocol panel, do choose Internet Protocol (TCP/IP) and the OK button.
8. After rebooting, you're ready to configure the TCP/IP setting, as described in the following paragraphs.

Microsoft Windows XP

TCP/IP stack is considered a core component of the operating system, so it cannot be installed or uninstalled. You must check in this case that Internet Protocol (TCP/IP) is enabled. To do so, follow these steps:

1. Starting from *Start -> Settings -> Control Panel* or *Start -> Control Panel* de-pending on the configuration of your computer.
2. Make a double click on the *Network Connections* icon.
3. Select the Network Adapter icon and from the contextual menu, do select the *Properties* item.
4. In the General TAB panel, verify that *Internet Protocol (TCP/IP)* item is checked; if not, do check it and click on the *OK* button.

Microsoft Windows Vista / Windows 7

TCP/IP stack is considered a core component of the operating system, so it cannot be installed or uninstalled. You must check in this case that Internet Protocol (TCP/IP) is enabled. To do so, follow these steps:

1. Starting from *Start -> Control Panel -> Network & Internet -> Network Connections* depending on the configuration of your computer.
2. Select the Network Adapter icon and from the contextual menu, do select the *Properties* item.
3. In the General TAB panel, verify that *Internet Protocol v4 (TCP/IPv4)* item is checked; if not, do check it and click on the *OK* button.

Apple MacOS 10.x

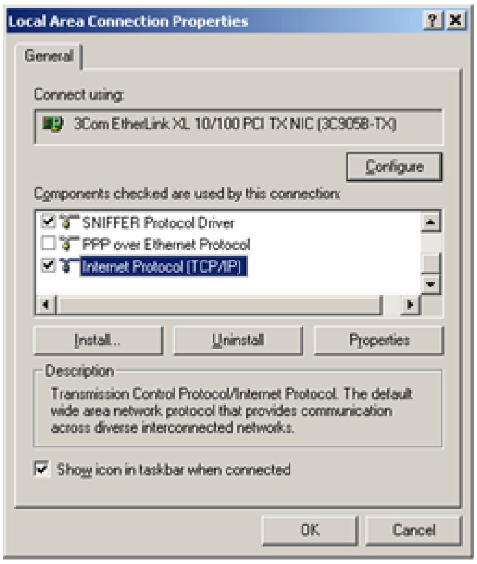
TCP/IP is installed on a MacOS system as part of Open Transport.

ETHERNET CONNECTION >> MS WINDOWS 2000

To configure TCP/IP on these Operating Systems follow these steps:

1. *Select Start -> Settings -> Control Panel* and make a double click on the *Network and Dial-up Connection* icon.
2. Select the adapter card interested by TCP/IP configuration and then select the Properties item from its contextual menu.
3. Select *Internet Protocol (TCP/IP)* item then click on *Properties* button.

FIGURE 7. Local Area Connection Properties



Local Area Connection Properties

Connect using:

3Com EtherLink XL 10/100 PCI TX NIC (3C905B-TX)

Components checked are used by this connection:

☑ SNIFFER Protocol Driver
□ PPP over Ethernet Protocol
☑ Internet Protocol (TCP/IP)

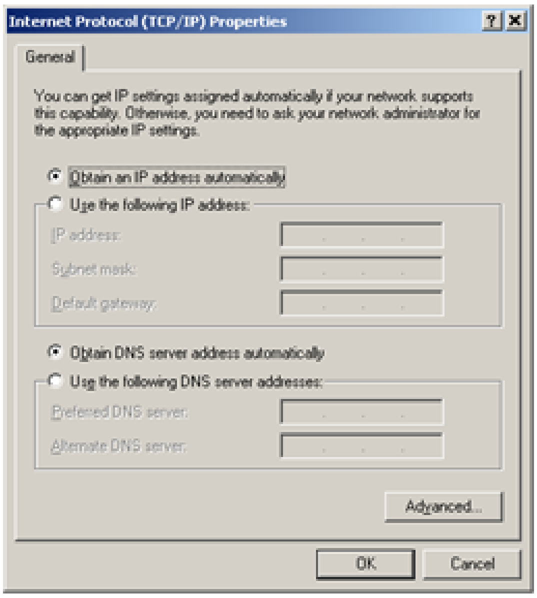
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in taskbar when connected

4. Select the *General* TAB panel, then check the *Obtain an IP address automatically* and *Obtain DNS server address automatically* radio buttons. Click on *OK* button.

FIGURE 8. Internet Protocol (TCP/IP) Properties



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

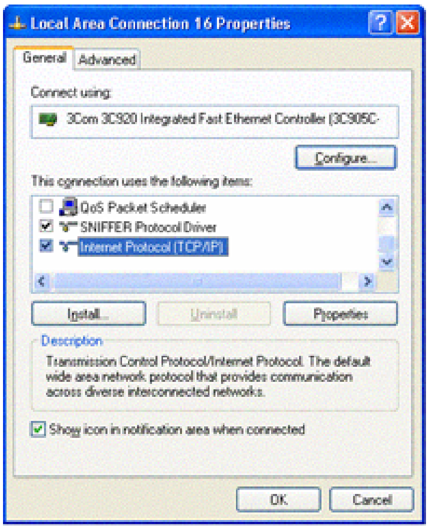
5. A system reboot will be required to make the changes real.

ETHERNET CONNECTION >> MS WINDOWS XP

To configure TCP/IP on MS Windows XP Operating System follow these steps:

1. Select *Start -> Settings -> Control Panel* and make a double click on the *Network Connections* icon.
2. Select the adapter card interested by TCP/IP configuration.
3. Select the *Properties* item from the contextual Adapter Card menu.
4. Select in the *General* TAB panel, the *Internet Protocol (TCP/IP)* item and then click on *Properties* button.

FIGURE 9. **Local Area Connection Properties**



Local Area Connection 16 Properties

General | Advanced

Connect using:

3Com 3C920 Integrated Fast Ethernet Controller (3C905C-

This connection uses the following items:

□ QoS Packet Scheduler
☑ SNIFFER Protocol Driver
☑ Internet Protocol (TCP/IP)

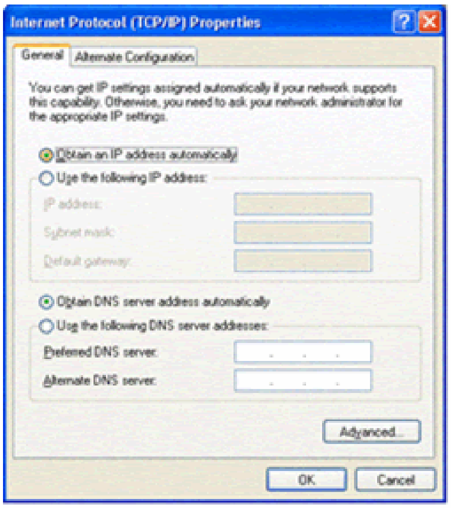
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in notification area when connected

5. In the *General* TAB panel, check the *Obtain an IP address automatically* radio button and the *Obtain DNS server address automatically* radio button. Click on *OK* button.

FIGURE 10. **Internet Protocol (TCP/IP) Properties**



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:

IP address:
Subnet mask:
Default gateway:

● Obtain DNS server address automatically
○ Use the following DNS server addresses:

Preferred DNS server: . . .
Alternate DNS server: . . .

ETHERNET CONNECTION >> MS WINDOWS VISTA / WINDOWS 7

To configure TCP/IP on MS Windows Vista / Windows 7 Operating Systems follow these steps:

1. Select *Start -> Control Panel -> Network & Internet* and make a double click on the *Network Connections* icon.
2. Select the adapter card interested by TCP/IP configuration.
3. Select the *Properties* item from the contextual Adapter Card menu.
4. Select in the *General* TAB panel, the *Internet Protocol (TCP/IPv4)* item and then click on *Properties* button.
5. In the *General* TAB panel, check the *Obtain an IP address automatically* radio button and the *Obtain DNS server address automatically* radio button. Click on *OK* button.

DISABLE HTTP PROXY

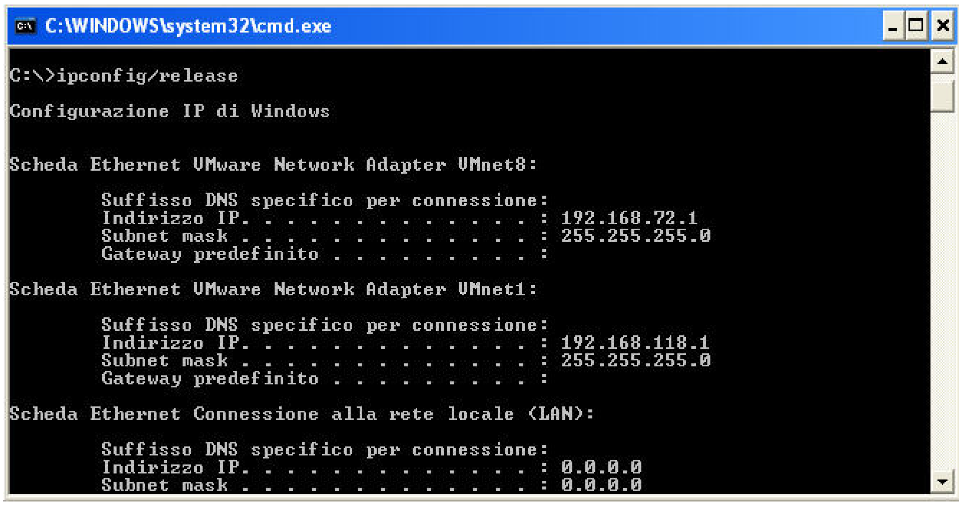
You need to verify that the "*HTTP proxy*" feature of your web browser is disabled. This is so that your browser can view the Home Station ADSL's HTML configuration pages.

OBTAIN IP SETTINGS FROM YOUR HOME STATION ADSL >> MS WINDOWS 2000

Now that you've configured your computer to connect to your Home Station ADSL, it needs to obtain new network settings. By releasing old DHCP IP settings and renewing them with settings from your Home Station ADSL, you can verify that you've configured your computer correctly.

1. On the Windows desktop, select the *Start > Programs > Accessories > Command Prompt* menu item
2. In the Command prompt window, type "*ipconfig/release*" and press the *ENTER* key

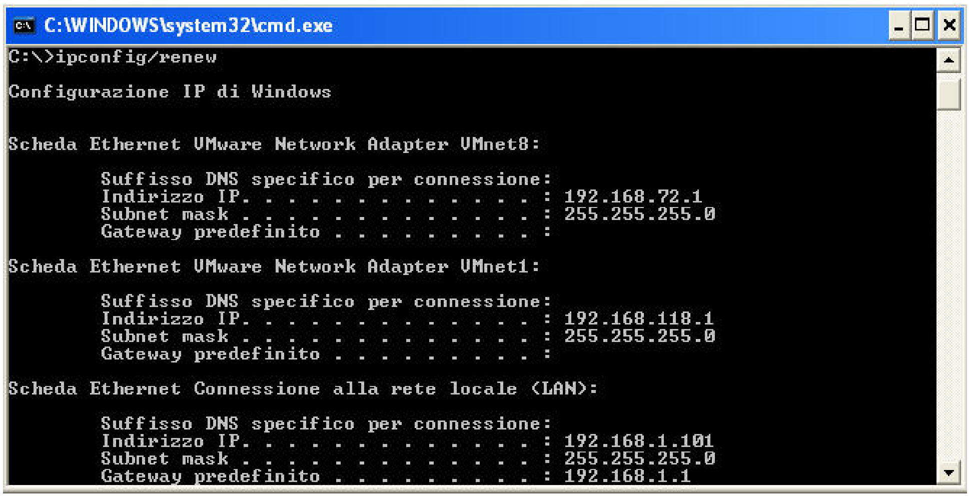
FIGURE 11. Command Prompt (IPCONFIG command)



```
C:\>ipconfig/release

Configurazione IP di Windows


Scheda Ethernet VMware Network Adapter VMnet8:

        Suffisso DNS specifico per connessione:
        Indirizzo IP. . . . . . . . . . . . . : 192.168.72.1
        Subnet mask . . . . . . . . . . . . . : 255.255.255.0
        Gateway predefinito . . . . . . . . . :

Scheda Ethernet VMware Network Adapter VMnet1:

        Suffisso DNS specifico per connessione:
        Indirizzo IP. . . . . . . . . . . . . : 192.168.118.1
        Subnet mask . . . . . . . . . . . . . : 255.255.255.0
        Gateway predefinito . . . . . . . . . :

Scheda Ethernet Connessione alla rete locale (LAN):

        Suffisso DNS specifico per connessione:
        Indirizzo IP. . . . . . . . . . . . . : 0.0.0.0
        Subnet mask . . . . . . . . . . . . . : 0.0.0.0
```

3. Type "*ipconfig/renew*" and press the *ENTER* key. Verify that your IP Address is now 192.168.1.xxx, your Subnet Mask is 255.255.255.0 and your Default Gateway is 192.168.1.1. These values confirm that your ADSL Home Station ADSL is functioning.

FIGURE 12. Command Prompt (IPCONFIG command)



```
C:\>ipconfig/renew

Configurazione IP di Windows


Scheda Ethernet VMware Network Adapter VMnet8:

        Suffisso DNS specifico per connessione:
        Indirizzo IP. . . . . . . . . . . . . : 192.168.72.1
        Subnet mask . . . . . . . . . . . . . : 255.255.255.0
        Gateway predefinito . . . . . . . . . :

Scheda Ethernet VMware Network Adapter VMnet1:

        Suffisso DNS specifico per connessione:
        Indirizzo IP. . . . . . . . . . . . . : 192.168.118.1
        Subnet mask . . . . . . . . . . . . . : 255.255.255.0
        Gateway predefinito . . . . . . . . . :

Scheda Ethernet Connessione alla rete locale (LAN):

        Suffisso DNS specifico per connessione:
        Indirizzo IP. . . . . . . . . . . . . : 192.168.1.101
        Subnet mask . . . . . . . . . . . . . : 255.255.255.0
        Gateway predefinito . . . . . . . . . : 192.168.1.1
```

4. Close the Command Prompt window

OBTAIN IP SETTINGS FROM YOUR HOME STATION ADSL >> MS WINDOWS XP / VISTA / 7

Now that you've configured your computer to connect to your Home Station ADSL, it needs to obtain new network settings. By releasing old DHCP IP settings and renewing them with settings from your Home Station ADSL, you can verify that you've configured your computer correctly.

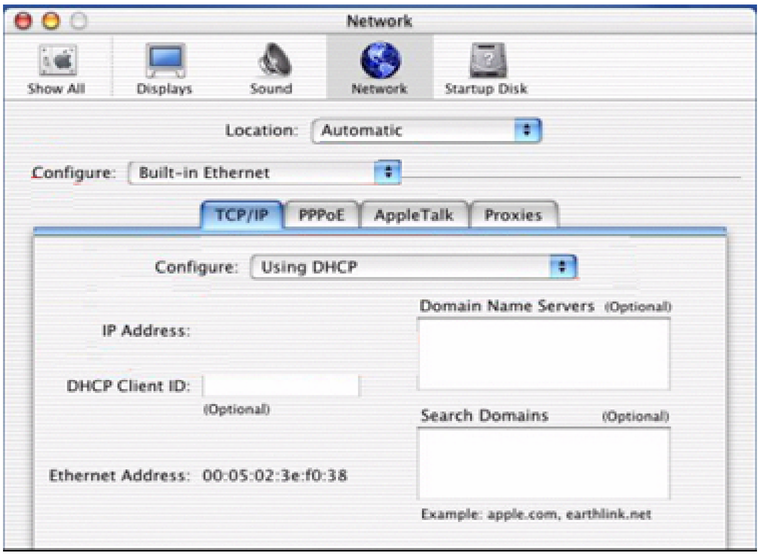
1. On the Windows desktop, click *Start* > *Programs* > *Accessories* > *Command Prompt* menu item
2. In the Command prompt window, type "*ipconfig/release*" and press the *ENTER* key
3. Type "*ipconfig/renew*" and press the *ENTER* key. Verify that your IP Address is now 192.168.1.xxx, your Subnet Mask is 255.255.255.0 and your Default Gateway is 192.168.1.1. These values confirm that your Home Station ADSL is functioning
4. Close the Command Prompt window

ETHERNET CONNECTION >> MAC OS 10.X

To configure TCP/IP on MAC OS 10.x follow these steps:

1. Open the *Apple Menu* > *System Preferences* and select *Network*.
2. From the *Show* drop down list, according to the type of connection used, select *Built-in Ethernet*.
3. Select the *TCP/IP* tab.
4. Select *DHCP* from the *Configure* pop-up menu to have a dynamic IP address. Click Apply Now.
5. Click on the *Register* button to save the changes in the Control Panel.
6. Enter *http://192.168.1.1/* in the address bar of your browser to open the **P.DG A4001N** Home Page.

FIGURE 13. **Network panel on MAC OS 10.x**



Location: Automatic

Configure: Built-in Ethernet

Configure: Using DHCP

Ethernet Address: 00:05:02:3e:f0:38

Example: apple.com, earthlink.net

WI-FI CONNECTION

It requires a computer with 802.11b/g/n (Wi-Fi Certified) wireless adapter installed.

1. Install your wireless adapter according to the manufacturer's instructions and verify that your computer is set to obtain an IP address automatically (DHCP mode).

*You will need to properly configure your adapter to communicate with the **P.DG A4001N** according to the configuration rules.*

2. In the configuration window of your wireless adapter scan the wireless network (marked with the relevant SSID name) present in your physical environment.
3. Select the SSID of the **P.DG A4001N**
4. Complete the configuration of the wireless adapter with the same parameters of the **P.DG A4001N** which are:
   - RF channel; automatically detect
   - WPA encryption enable or disable
   - WPA key used

To check the connection, connect to the **P.DG A4001N** Home Page, entering http://192.168.1.1/main.html

Router Configuration

Upon TCP/IP configuration on a client computer, it is possible to configure the Home Station ADSL using the web browser. Internet Explorer 6 or above, Netscape Navigator, Mozilla, Firefox and Opera are supported.

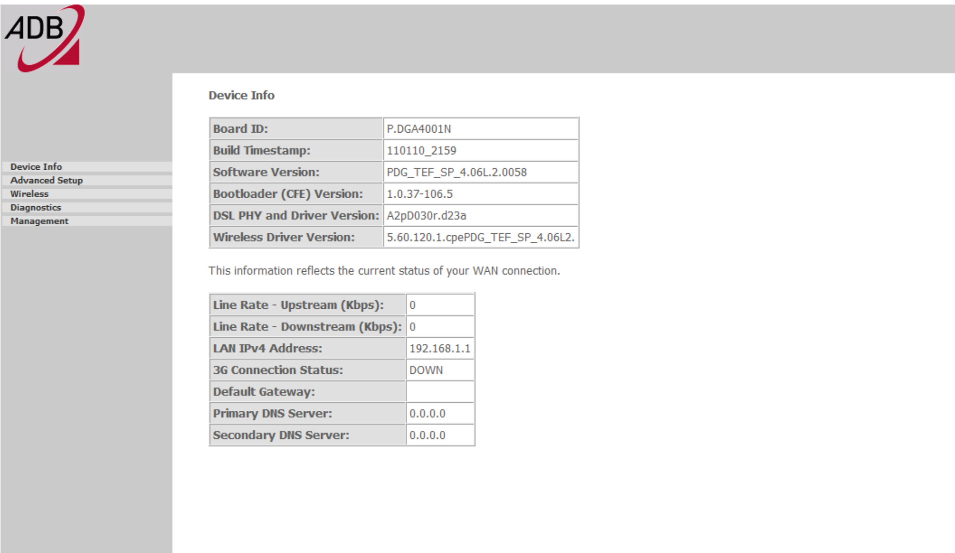
To access the management interface, enter the default IP address of the Data Gateway in your web browser: **http://192.168.1.1/main.html**

⚠ *The Router comes with a default IP address (192.168.1.1). If you change it, please take note of the new Router's IP address, otherwise a "Restore Default Settings" operation should be done to be able to access again to the Router.*

Access to Home Station ADSL configuration pages is controlled through *admin* user accounts with unrestricted access to change and view configuration of the Home Station ADSL. Default admin user and passwords are both "***1234***".

You will be asked to insert a *username* and a *password* as shown in Figure 1: insert them to access to Router's configuration panels. The *main page*, upon Router access, will be opened as shown in Figure 1.

FIGURE 1. Main page



Device Info

Board ID:	P.DGA4001N
Build Timestamp:	110110_2159
Software Version:	PDG_TEF_SP_4.06L.2.0058
Bootloader (CFE) Version:	1.0.37-106.5
DSL PHY and Driver Version:	A2pD030r.d23a
Wireless Driver Version:	5.60.120.1.cpePDG_TEF_SP_4.06L2.

This information reflects the current status of your WAN connection.

Line Rate - Upstream (Kbps):	0
Line Rate - Downstream (Kbps):	0
LAN IPv4 Address:	192.168.1.1
3G Connection Status:	DOWN
Default Gateway:	
Primary DNS Server:	0.0.0.0
Secondary DNS Server:	0.0.0.0

Password can contain from 3-12 alphanumeric characters and is case sensitive.

MAKING CONFIGURATION CHANGES

Configurable parameters have a dialog box or a drop-down menu. Once a configuration change has been made on a screen, click ***Apply/Save*** button on the screen to enable the new setting.

CONFIGURATION PARAMETERS

The *main page* contains a menu on the left - always available in all the web pages which is the starting point for any Router's configuration.

The left-hand side displays the main menu and the right-hand side shows descriptive information (see Figure 1).

The main menu item is described in the following table.

TABLE 1. Command menu items

PARAMETER	DESCRIPTION
Device Info	*it allows to access to Device Information and Statistics*
Advanced Setup	*it allows the access to the advanced configuration panels*
Wireless	*to configure the Wireless parameters (Security, Filters etc.)*
Diagnostics	*a menu to show and run diagnostic test for troubleshooting or system behavior analysis.*
Management	*it allows to define Router parameters devoted to user access, log management, Router's time, Backup Router's configuration, etc.*

This Page Intentionally Left Blank

Device Info Section

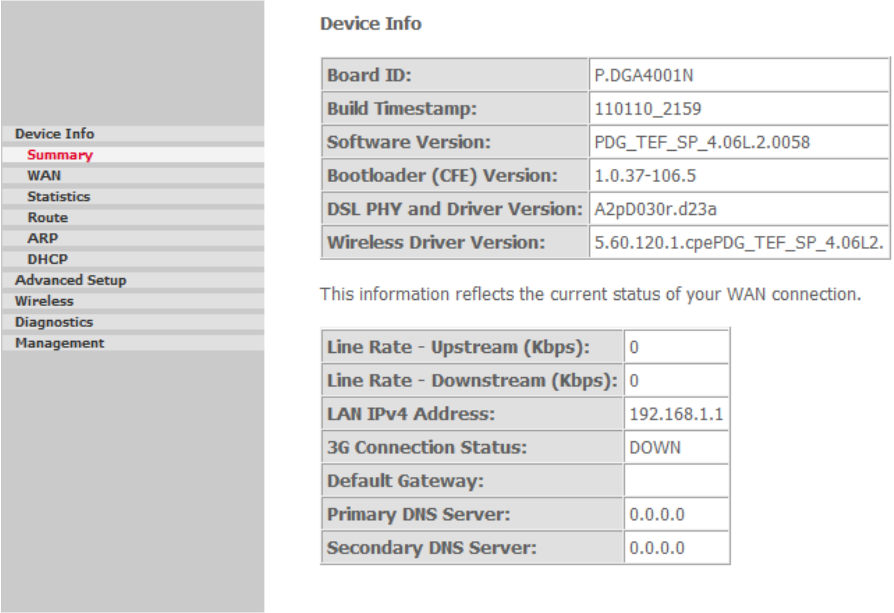
This chapter will describe the **Device Info Section** accessible from the *Home Page* of the **Home Station ADSL ADB P.DG A4001N** upon user authentication to the Router.

⚠ *Be aware that any configuration change could compromise your connectivity.*

SUMMARY

The *Summary* (see Figure 1), accessible through **Device Info >> Summary** item selection, is a read-only page and contains details of the router such as Hardware, Firmware and Software information, LAN IP address, the current status of your DSL connection etc.

FIGURE 1. **Summary Device Info Panel**



Device Info

Board ID:	P.DGA4001N
Build Timestamp:	110110_2159
Software Version:	PDG_TEF_SP_4.06L.2.0058
Bootloader (CFE) Version:	1.0.37-106.5
DSL PHY and Driver Version:	A2pD030r.d23a
Wireless Driver Version:	5.60.120.1.cpePDG_TEF_SP_4.06L2.

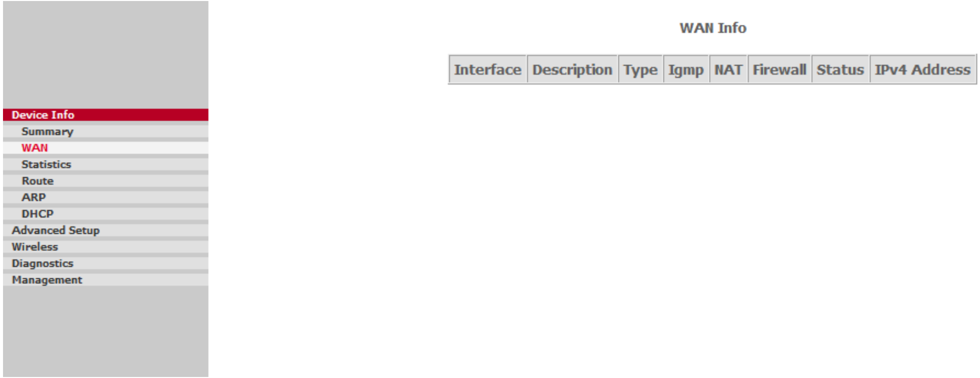
This information reflects the current status of your WAN connection.

Line Rate - Upstream (Kbps):	0
Line Rate - Downstream (Kbps):	0
LAN IPv4 Address:	192.168.1.1
3G Connection Status:	DOWN
Default Gateway:	
Primary DNS Server:	0.0.0.0
Secondary DNS Server:	0.0.0.0

WAN

The *WAN* (see Figure 2), accessible through **Device Info >> WAN.** Since a WAN connection has not been set up yet, there is no information to view. After completing the configurations for a WAN connection, you can return to this screen to view the information on your WAN status.

FIGURE 2. **WAN Info Panel**



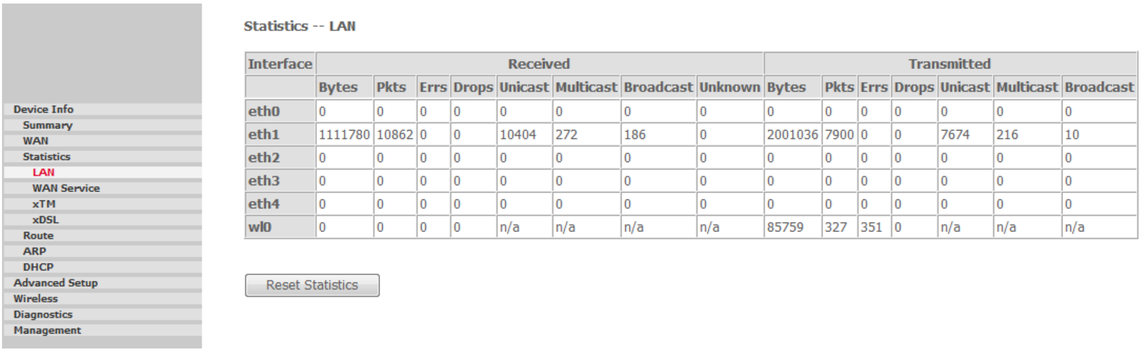
WAN Info

Interface	Description	Type	Igmp	NAT	Firewall	Status	IPv4 Address

STATISTICS >> LAN

Access the LAN statistics from the router by clicking on **Statistics >> LAN**. The **Reset Statistics** button, will reset statistic counters.

FIGURE 3. Statistics LAN Panel



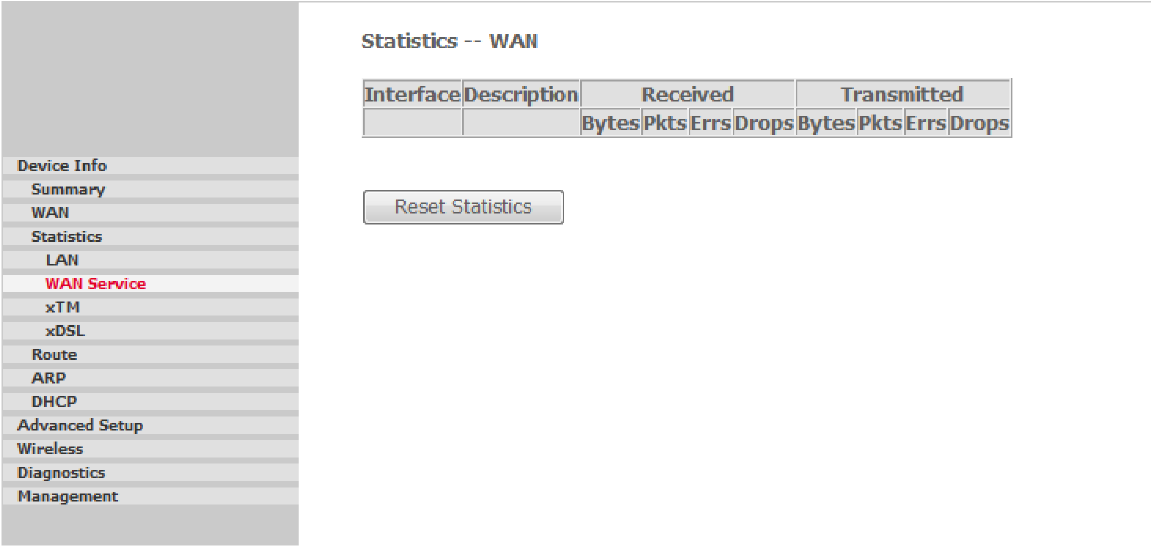
Statistics -- LAN

Interface	Received								Transmitted						
	Bytes	Pkts	Errs	Drops	Unicast	Multicast	Broadcast	Unknown	Bytes	Pkts	Errs	Drops	Unicast	Multicast	Broadcast
eth0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
eth1	1111780	10862	0	0	10404	272	186	0	2001036	7900	0	0	7674	216	10
eth2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
eth3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
eth4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
wl0	0	0	0	0	n/a	n/a	n/a	n/a	85759	327	351	0	n/a	n/a	n/a

STATISTICS >> WAN SERVICE

Access the WAN statistics from the router by clicking on **Statistics >> WAN Service**. The **Reset Statistics** button, will reset statistic counters.

FIGURE 4. Statistics WAN Panel



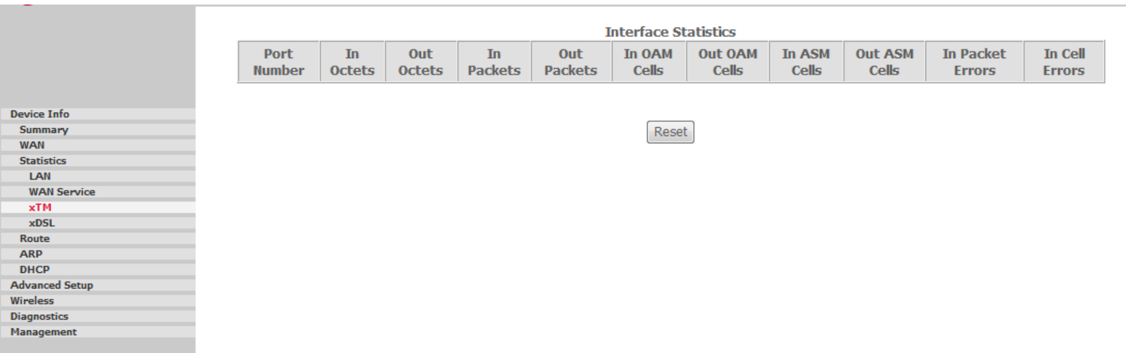
Statistics -- WAN

Interface	Description	Received				Transmitted			
		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops

STATISTICS >> XTM

Access the xTM statistics from the router by clicking on **Statistics >> xTM**. The **Reset** button, will reset statistic xTM counters.

FIGURE 5. **Statistics >> xTM Panel**



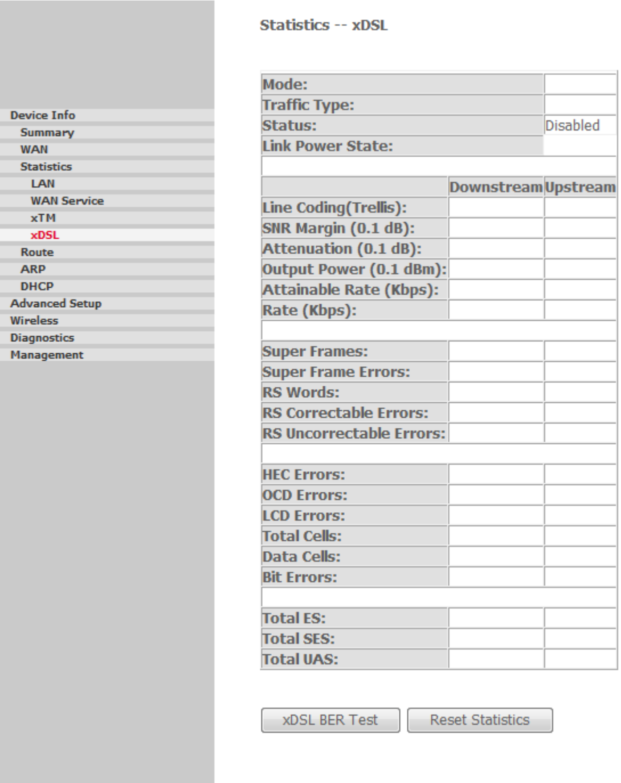
Interface Statistics

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

STATISTICS >> XDSL

Access the DSL statistics from the router by clicking on **Statistics >> xDSL**. The Information contained in this screen is useful for troubleshooting and diagnostics of connection problems. The **Reset Statistics** button, will reset statistic xDSL counters.

FIGURE 6. **Statistics >> xDSL Panel**



Statistics -- xDSL

Mode:	
Traffic Type:	
Status:	Disabled
Link Power State:	

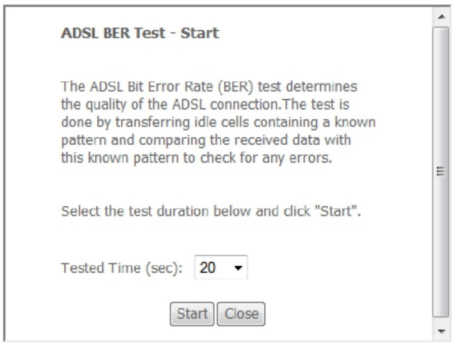
	Downstream	Upstream
Line Coding(Trellis):		
SNR Margin (0.1 dB):		
Attenuation (0.1 dB):		
Output Power (0.1 dBm):		
Attainable Rate (Kbps):		
Rate (Kbps):		
Super Frames:		
Super Frame Errors:		
RS Words:		
RS Correctable Errors:		
RS Uncorrectable Errors:		
HEC Errors:		
OCD Errors:		
LCD Errors:		
Total Cells:		
Data Cells:		
Bit Errors:		
Total ES:		
Total SES:		
Total UAS:		

xDSL BER Test. A Bit Error Rate Test (BER Test) is a test that reflects the ratio of error bits to the total number transmitted.
If you click on the **xDSL BER Test** button at the bottom of the xDSL Statistics screen, the pop-up window shown in Figure 7 will appear.

Upon test duration choice (in seconds), and by pressing the ***Start*** button, the test will start running. At its end a result page will be shown.

Do close this page by selecting the ***Close*** button.

FIGURE 7. xDSL BER Test Panels



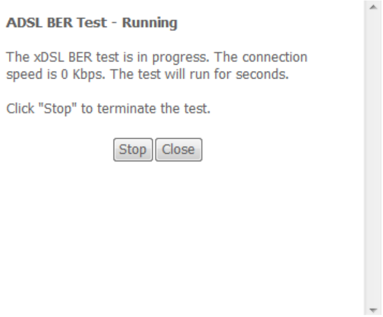
ADSL BER Test - Start

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

Select the test duration below and click "Start".

Tested Time (sec): 20

Start phase

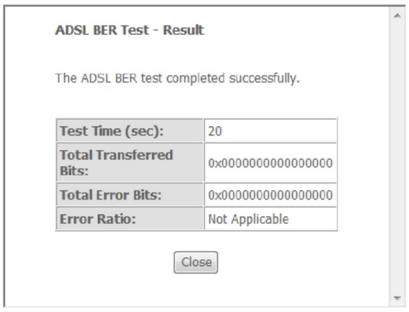


ADSL BER Test - Running

The xDSL BER test is in progress. The connection speed is 0 Kbps. The test will run for seconds.

Click "Stop" to terminate the test.

Result phase



ADSL BER Test - Result

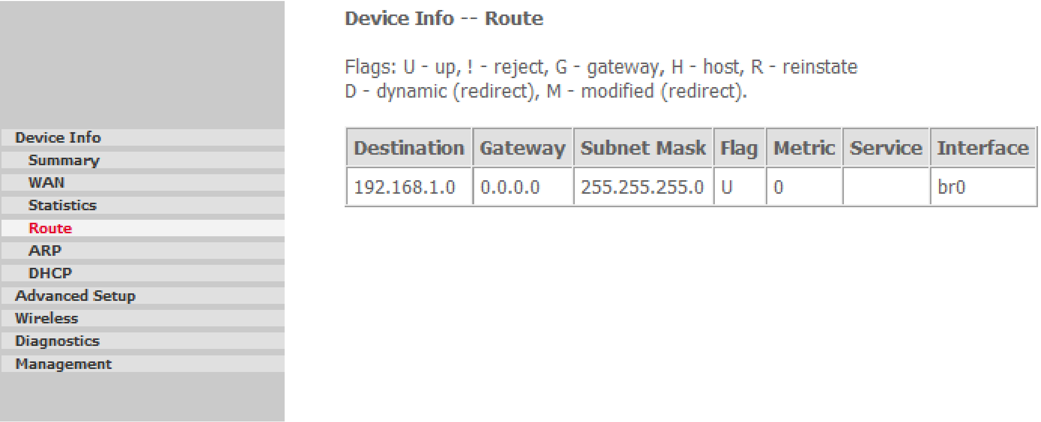
The ADSL BER test completed successfully.

Test Time (sec):	20
Total Transferred Bits:	0x0000000000000000
Total Error Bits:	0x0000000000000000
Error Ratio:	Not Applicable

ROUTE

Access the Routing Status report from the router by clicking on **Device Info >> Route.** (see Figure 8).

FIGURE 8. Route Panel



Device Info -- Route

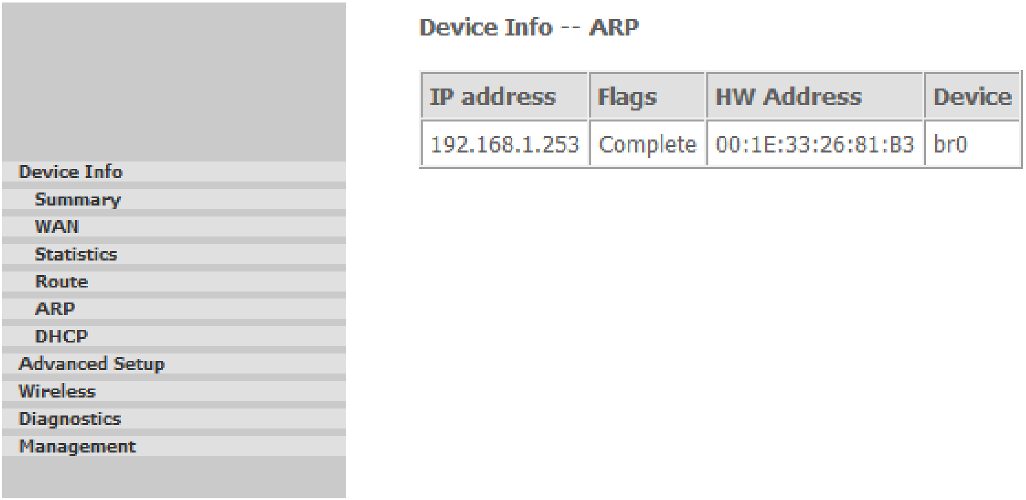
Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate
D - dynamic (redirect), M - modified (redirect).

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0

ARP

Access the ARP Status report from the router by clicking on **Device Info >> ARP.** ARP (Address Resolution Protocol) maps the IP address to the physical address, labelled HW Address (the MAC address) and helps to identify computers on the LAN.

FIGURE 9. ARP Panel



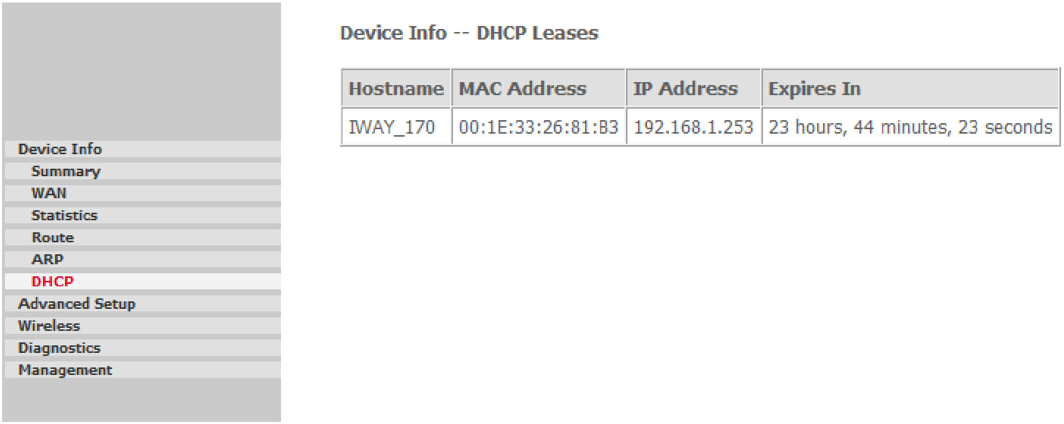
Device Info -- ARP

IP address	Flags	HW Address	Device
192.168.1.253	Complete	00:1E:33:26:81:B3	br0

DHCP

Access the DHCP leases report from the router by clicking on **Device Info >> DHCP**.

FIGURE 10. DHCP Panel



Device Info -- DHCP Leases

Hostname	MAC Address	IP Address	Expires In
IWAY_170	00:1E:33:26:81:B3	192.168.1.253	23 hours, 44 minutes, 23 seconds

This Page Intentionally Left Blank

Advanced Setup Section

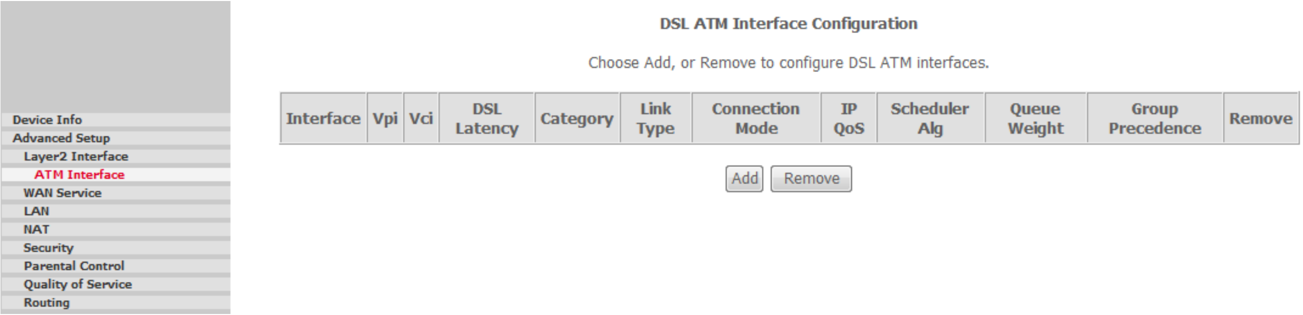
This chapter will describe the **Advanced Setup Section** accessible from the *Home Page* of the **Home Station ADSL P.DG A4001N**. This section is only accessible to a user with admin profile and is intended to collect most of the advanced configuration functions.

⚠ *Be aware that any configuration change could compromise your connectivity.*

LAYER 2 >> ATM

By selecting **Advanced Setup >> Layer2 Interface >> ATM Interface** the page, shown in Figure 1, appears. It is used to configure the DSL ATM Interface.

FIGURE 1. **Layer 2 ATM panel**



DSL ATM Interface Configuration

Choose Add, or Remove to configure DSL ATM interfaces.

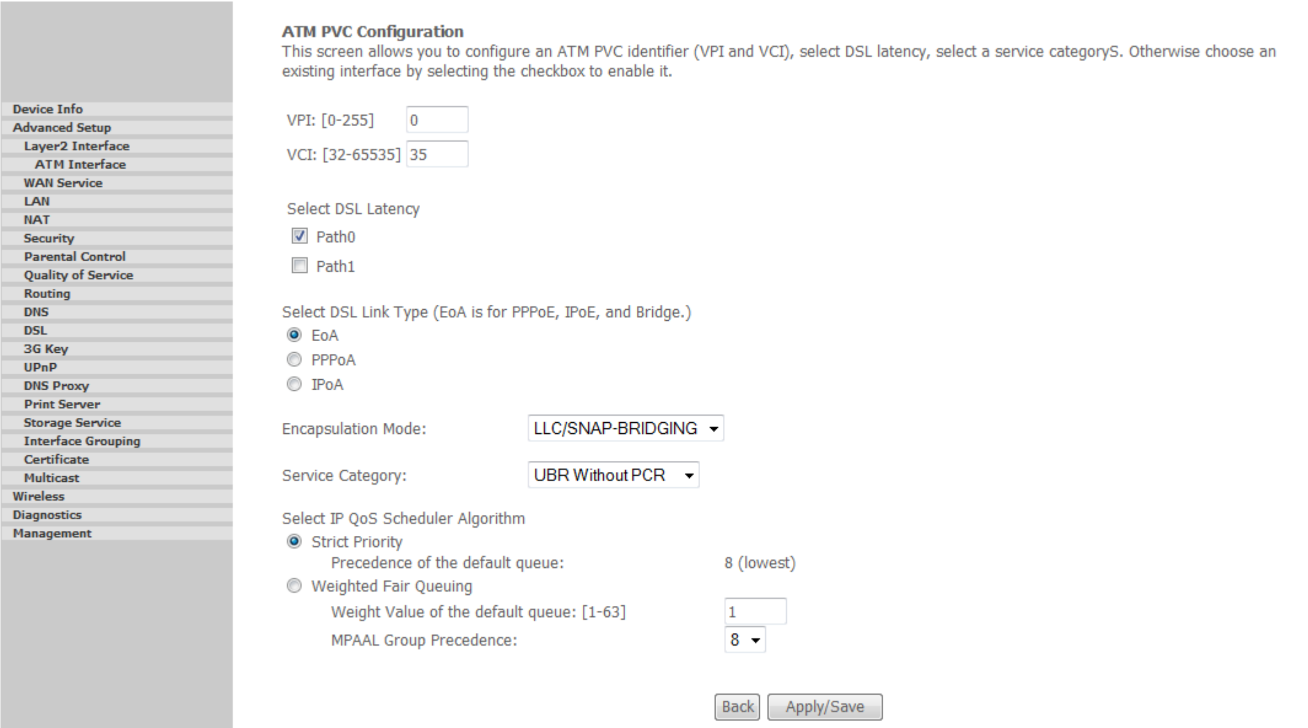
Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	IP QoS	Scheduler Alg	Queue Weight	Group Precedence	Remove

Click on the ***Add*** button if you want to add a new connection for the DSL ATM interface. The DSL ATM Configuration screen is shown in Figure 2.

The ATM PVC Configuration screen allows you to configure an ATM PVC identifier (VPI and VCI) and select a service category.

Check the **Remove** check-box and select the **Remove** button to delete a DSL ATM configuration.

FIGURE 2. **Adding Layer 2 ATM interface panel**



ATM PVC Configuration

This screen allows you to configure an ATM PVC identifier (VPI and VCI), select DSL latency, select a service categoryS. Otherwise choose an existing interface by selecting the checkbox to enable it.

VPI: [0-255] 0

VCI: [32-65535] 35

Select DSL Latency

☑ Path0

□ Path1

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

● EoA

○ PPPoA

○ IPoA

Encapsulation Mode: LLC/SNAP-BRIDGING

Service Category: UBR Without PCR

Select IP QoS Scheduler Algorithm

● Strict Priority

Precedence of the default queue: 8 (lowest)

○ Weighted Fair Queuing

Weight Value of the default queue: [1-63] 1

MPAAL Group Precedence: 8

By clicking on the **Add** button, this screen allows you to configure an ATM PVC identifier (VPI and VCI) and select a service category.

Find out the values listed in Table 1 from your ISP before you change them.

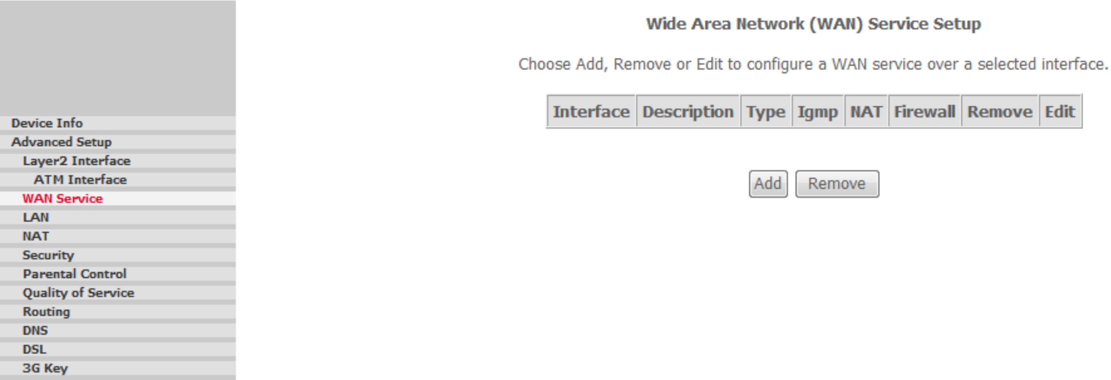
TABLE 1. ATM PVC Configuration parameters

Parameter	Value	Description
VPI	*0-255*	*Virtual Path Identifier*
VCI	*32-65535*	*Virtual Channel Identifier*
DSL Latency	*Path0 / Path1*	
DSL Link Type	*EoA / PPPoA / IPoA*	*Note: EoA is for PPPoE, IPoE, and Bridge*
Encapsulation Mode	*LLC/SNAP Bridging* *LLC/SNAP Routing* *VC/MUX* *LLC/ENCAPSULATION*	
Service Category	*UBR without PCR*	***UBR Without PCR*** *(Unspecified Bit Rate without Peak Cell Rate). UBR service is suitable for applications that can tolerate variable delays and some cell losses. Applications suitable for UBR service include text/data/image transfer, messaging, distribution, and retrieval and also for remote terminal applications such as telecommuting.*
	UBR with PCR	***UBR With PCR*** *(Unspecified Bit Rate with Peak Cell Rate)*
	CBR	***CBR*** *(Constant Bit Rate) used by applications that require a fixed data rate that is continuously available during the connection time. It is commonly used for uncompressed audio and video information such as videoconferencing, interactive audio (telephony), audio / video distribution (e.g. television, distance learning, and pay-per-view), and audio / video retrieval (e.g. video-on-demand and audio library).*
	Non Realtime VBR	***Non Realtime VBR*** *(Non-Real-time Variable Bit Rate) can be used for data transfers that have critical response-time requirements such as airline reservations, banking transactions, and process monitoring.*
	Realtime VBR	***Realtime VBR*** *(Real-time Variable Bit Rate) used by time-sensitive applications such as real-time video. Rt-VBR service allows the network more flexibility than CBR.*
IP QoS Scheduler Algorithm	*Strict Priority* *Weighted Fair Queuing*	

WAN SERVICE

By selecting **Advanced Setup >> WAN Service** It is possible to configure WAN services on created interfaces.

FIGURE 3. **WAN Service Panel**



Wide Area Network (WAN) Service Setup

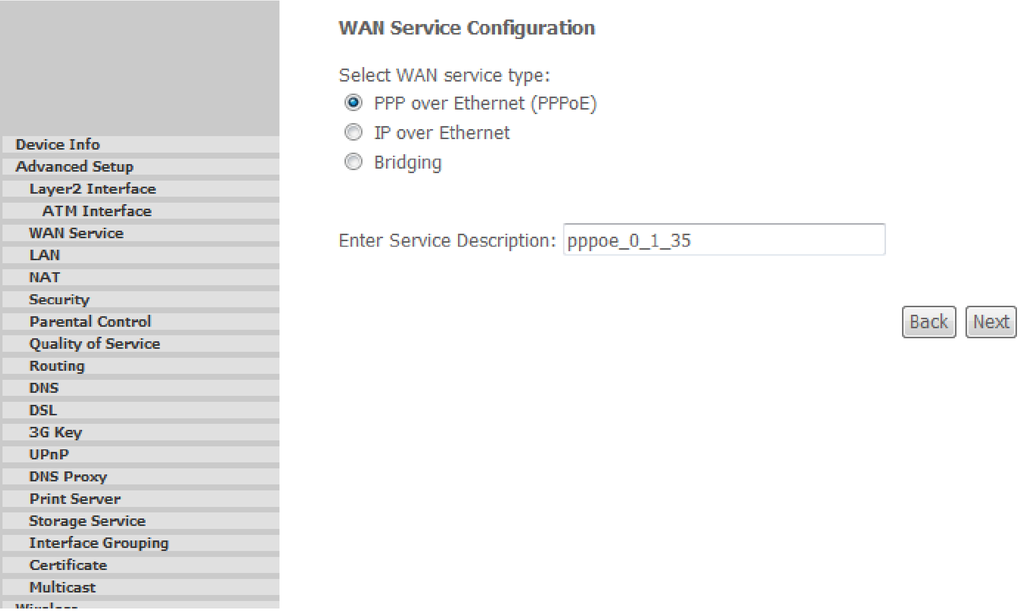
Choose Add, Remove or Edit to configure a WAN service over a selected interface.

Interface	Description	Type	Igmp	NAT	Firewall	Remove	Edit

Click on the ***Add*** button if you want to add a new connection for the WAN interface.
Check the **Remove** check-box and select the **Remove** button to delete a WAN configuration.
By clicking on the **Add** button, this screen allows you to configure a WAN service over a created interface.

The next screen allows you to select a layer 2 interface. After making your selections, click on **Next** button to go on to the next page.

FIGURE 4. **Adding a WAN interface - Step 1**



WAN Service Configuration

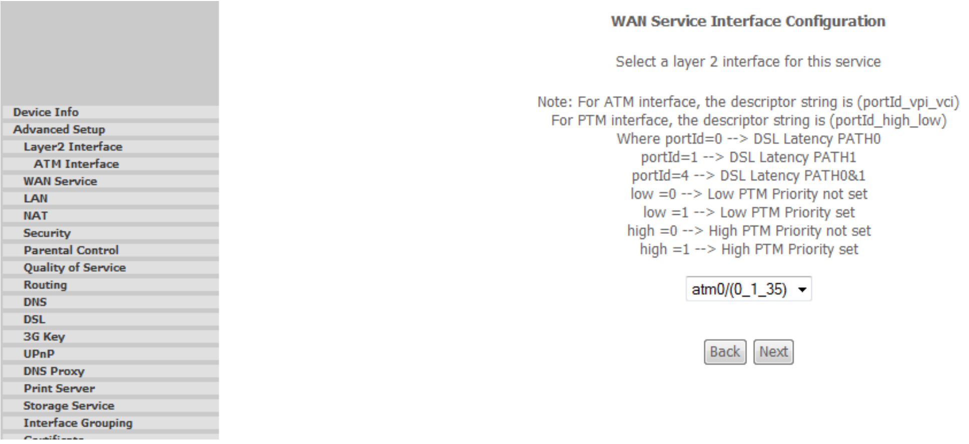
Select WAN service type:

● PPP over Ethernet (PPPoE)
○ IP over Ethernet
○ Bridging

Enter Service Description: pppoe_0_1_35

The next screen allows you to select a layer 2 interface. After making your selections, click on **Next** button to go on to the next page.

FIGURE 5. Adding a WAN interface - Step 2



WAN Service Interface Configuration

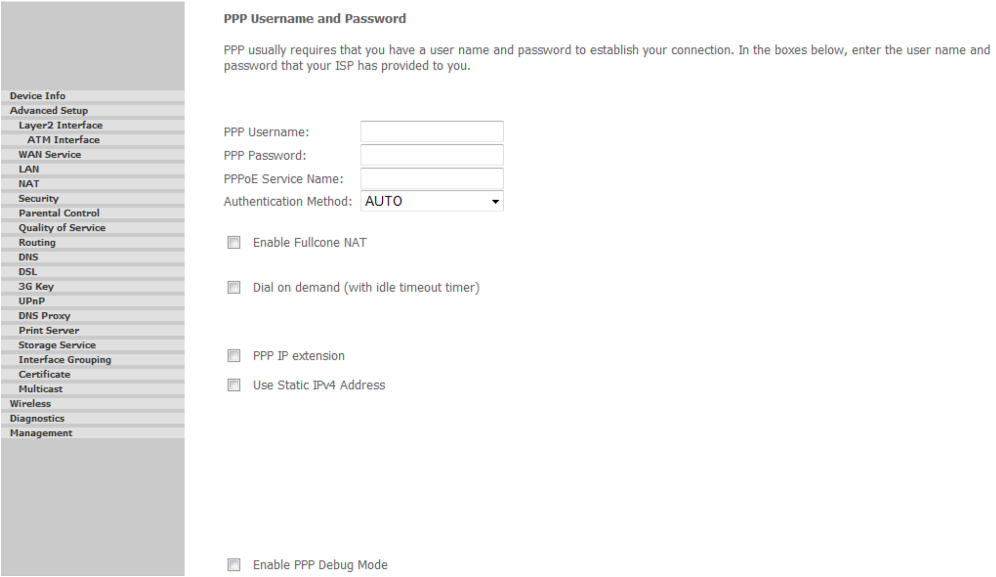
Select a layer 2 interface for this service

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

atm0/(0_1_35)

The next screen allows you to configure the chosen service. After making your selections, click on **Next** button to go on to the next page.

FIGURE 6. Adding a WAN interface - Step 3



PPP Username and Password

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

PPP Username:
PPP Password:
PPPoE Service Name:
Authentication Method: AUTO

□ Enable Fullcone NAT

□ Dial on demand (with idle timeout timer)

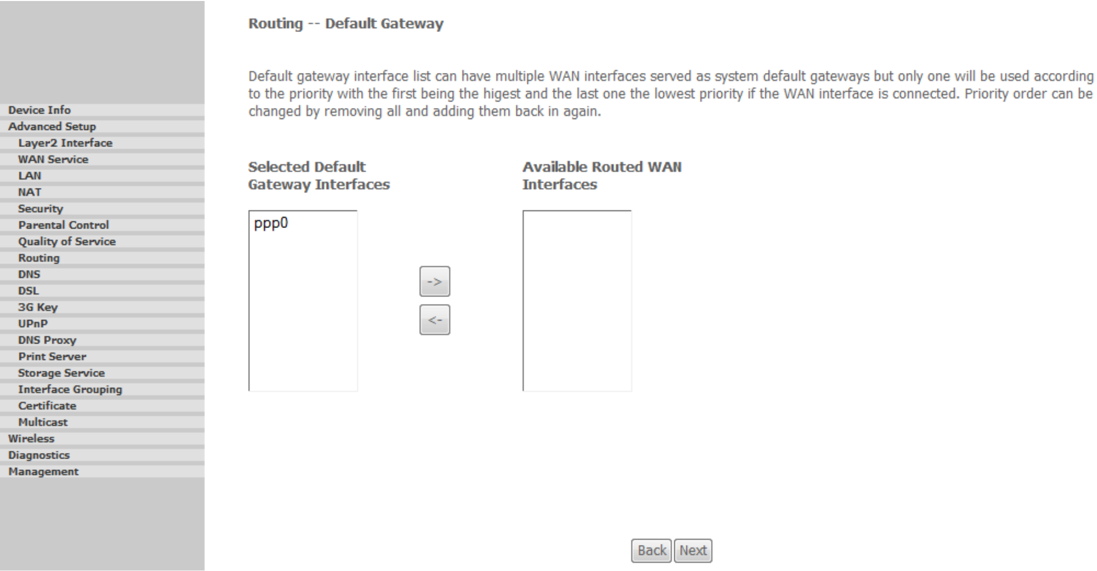
□ PPP IP extension

□ Use Static IPv4 Address

□ Enable PPP Debug Mode

The next screen allows you to select the default gateway interfaces. After making your selections, click on **Next** button to go on to the next page.

FIGURE 7. **Adding a WAN interface - Step 4**



Routing -- Default Gateway

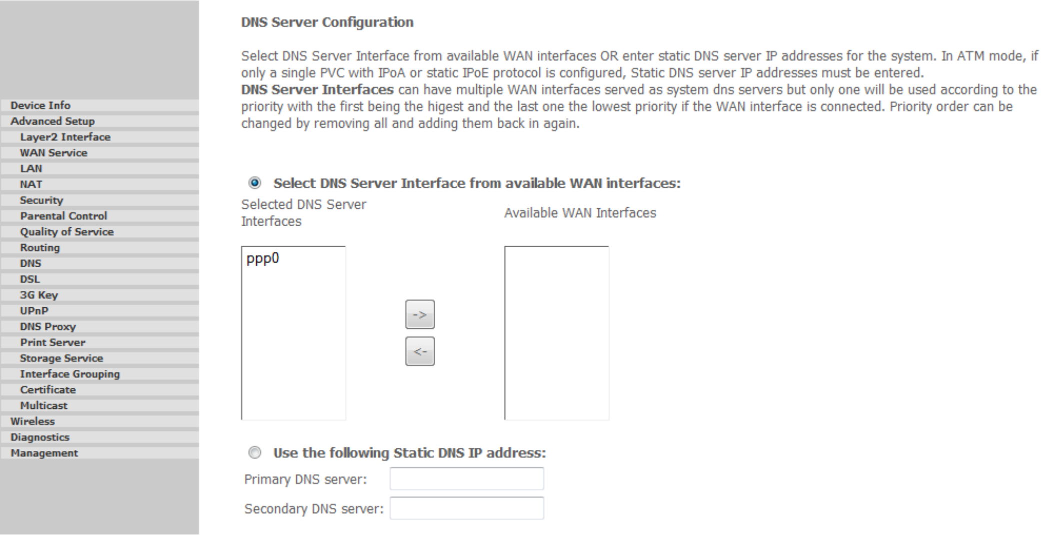
Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and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

Selected Default Gateway Interfaces: ppp0

Available Routed WAN Interfaces:

The next screen allows you to select the DNS server interface. After making your selections, click on **Next** button to go on to the next page.

FIGURE 8. **Adding a WAN interface - Step 5**



DNS Server Configuration

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

● Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces: ppp0

Available WAN Interfaces:

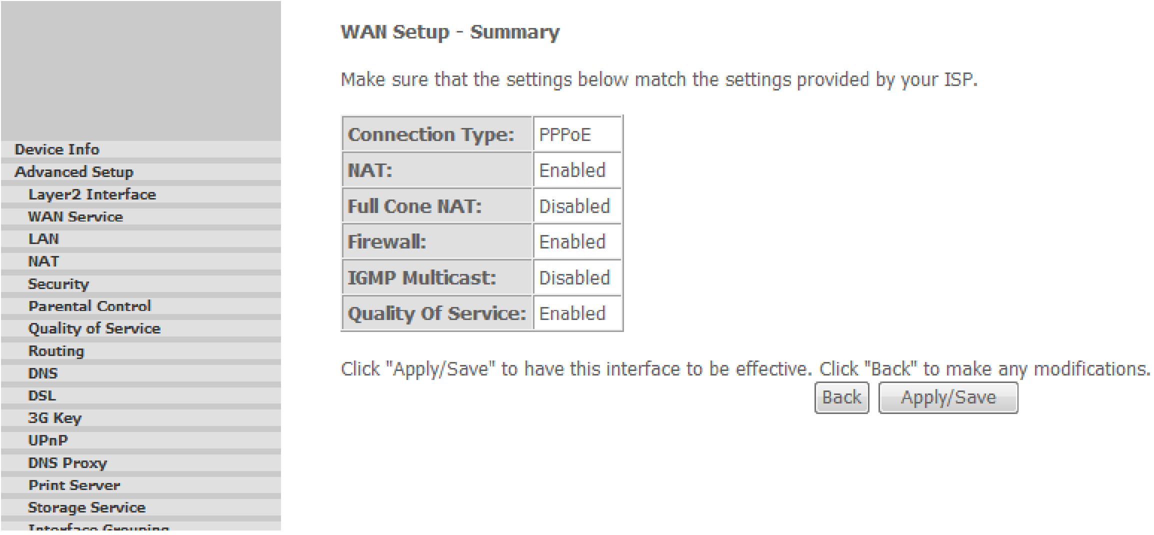
○ Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

When the settings are complete, the screen in Figure 5 appears showing a **WAN Setup – Summary** screen to display the WAN configurations. Click on **Apply/Save** button to save the settings.

FIGURE 9. Adding a WAN interface - Step 6



WAN Setup - Summary

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

Connection Type:	PPPoE
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Enabled

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

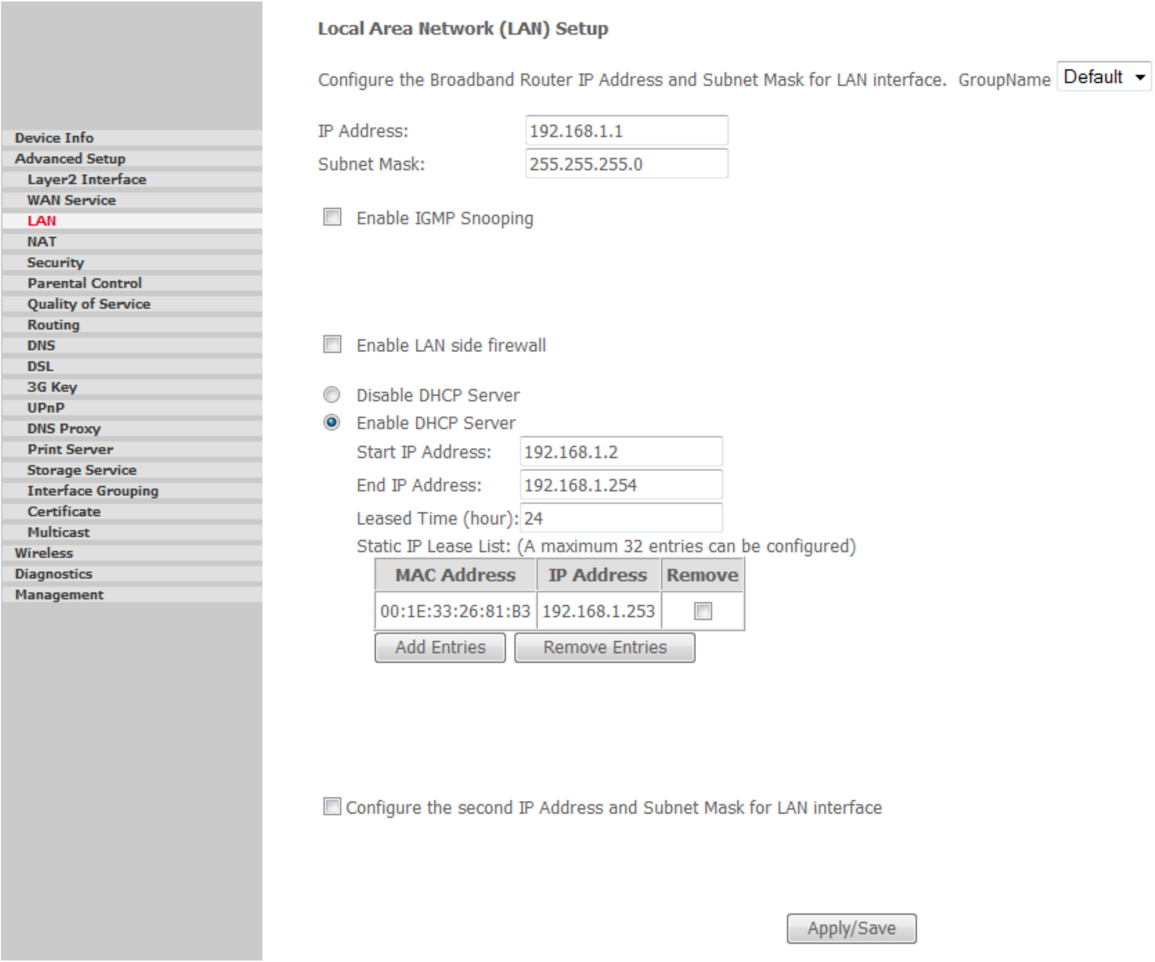
LAN

You can configure the DSL Router IP address and Subnet Mask for the LAN interface to correspond to your LAN's IP Subnet.

If you want the DHCP server to automatically assign IP addresses, then enable the DHCP server and enter the range of IP addresses that the DHCP server can assign to your computers.

Disable the DHCP server if you prefer to manually assign IP addresses.

FIGURE 10. LAN Panel



Local Area Network (LAN) Setup

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

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

□ Enable IGMP Snooping

□ Enable LAN side firewall

○ Disable DHCP Server

● Enable DHCP Server

Start IP Address: 192.168.1.2

End IP Address: 192.168.1.254

Leased Time (hour): 24

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

MAC Address	IP Address	Remove
00:1E:33:26:81:B3	192.168.1.253	□

Add Entries   Remove Entries

□ Configure the second IP Address and Subnet Mask for LAN interface

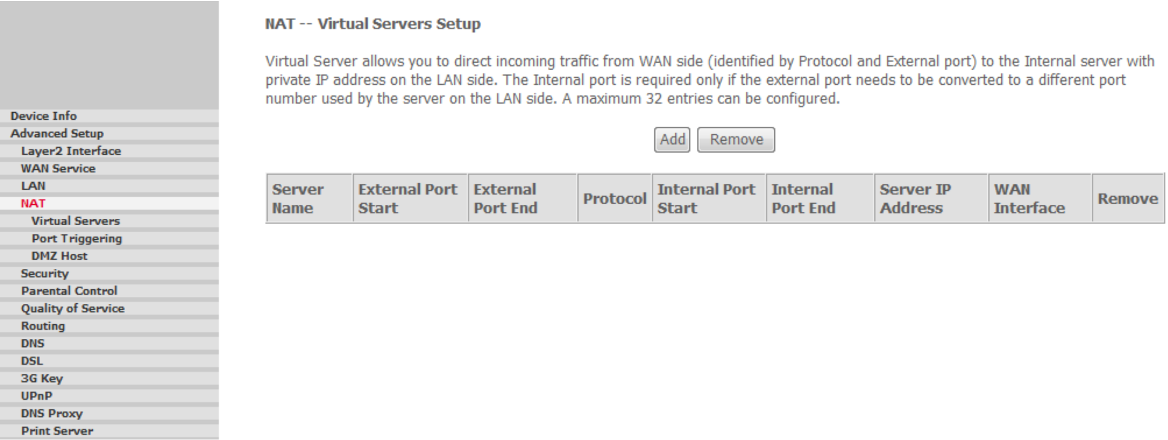
Apply/Save

NAT >> VIRTUAL SERVER

If you enable NAT (Network Address Translation), you can configure the Virtual Server, Port Triggering and DMZ Host.

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

FIGURE 11. NAT - Virtual Servers Setup Panel



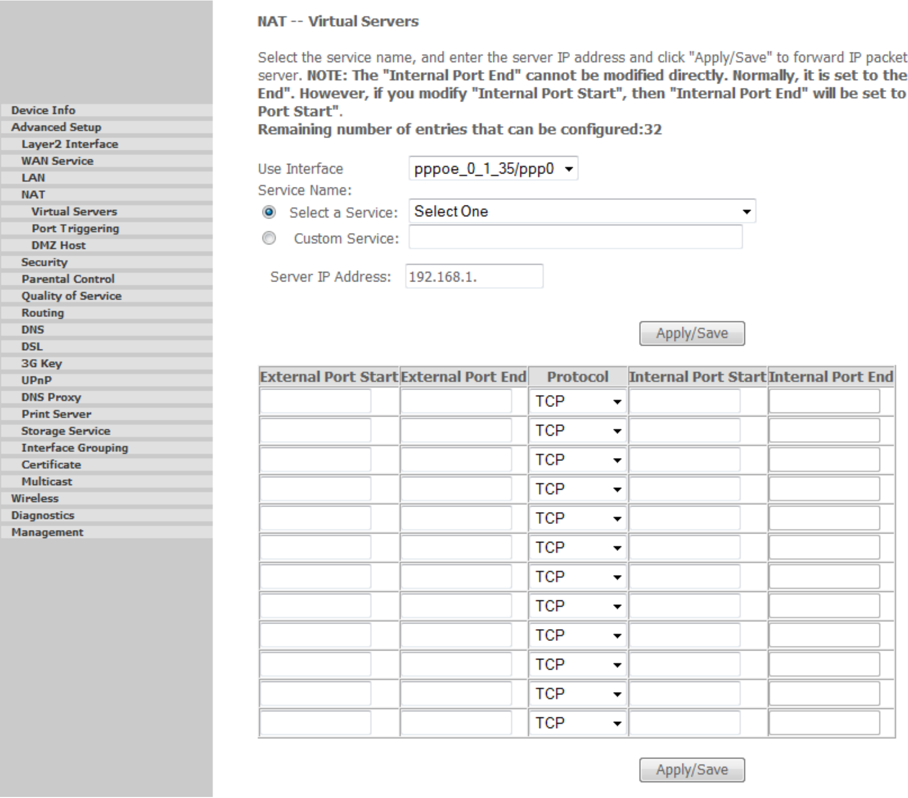
NAT -- Virtual Servers Setup

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

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	WAN Interface	Remove

To add additional virtual servers, click on the **Add** button. If you need to remove any of the server names, select the check box and click on the **Remove** button.

FIGURE 12. **Adding NAT - Virtual Servers Setup Panel**



NAT -- Virtual Servers

Select the service name, and enter the server IP address and click "Apply/Save" to forward IP packets for this service to the specified server. **NOTE: The "Internal Port End" cannot be modified directly. Normally, it is set to the same value as "External Port End". However, if you modify "Internal Port Start", then "Internal Port End" will be set to the same value as "Internal Port Start".**

Remaining number of entries that can be configured:32

Use Interface: pppoe_0_1_35/ppp0

Service Name:

● Select a Service: Select One

○ Custom Service:

Server IP Address: 192.168.1.

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

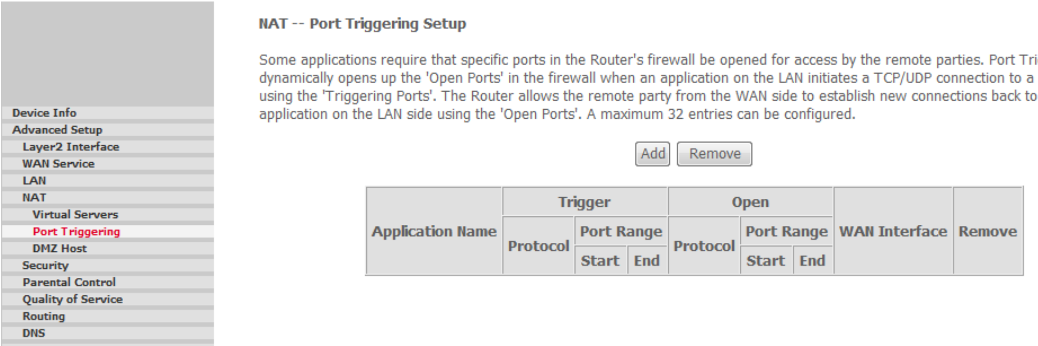
NAT >> PORT TRIGGERING

Some applications require that specific ports in the Router's firewall be opened for access by the remote parties.

Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'.

The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'.

FIGURE 13. NAT – Port Triggering Setup Panel



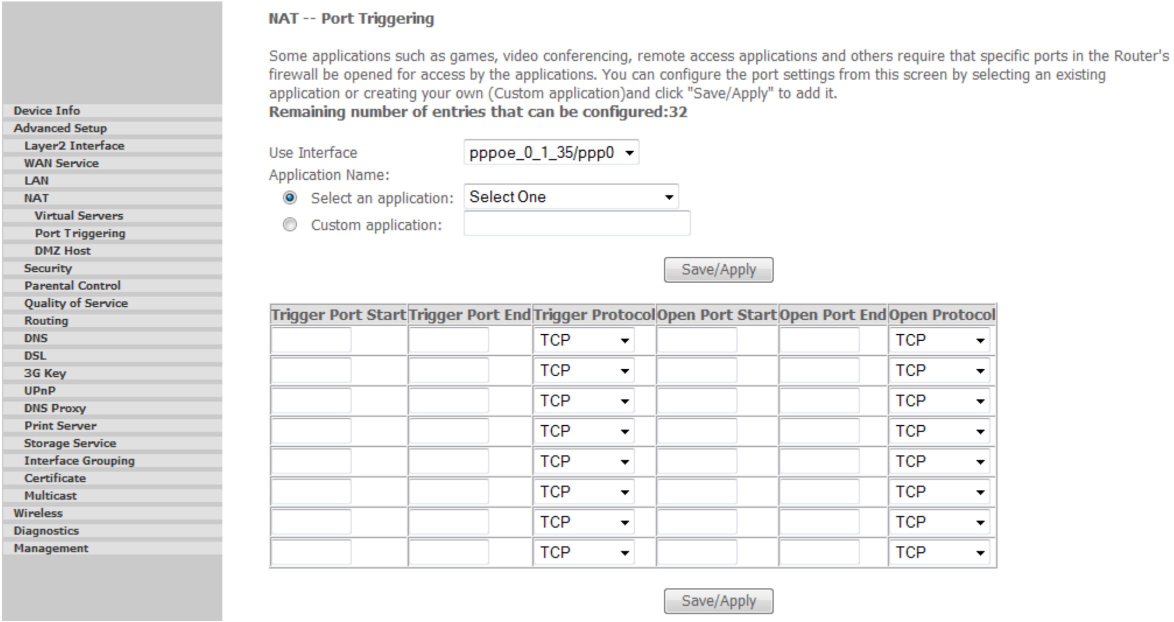
NAT -- Port Triggering Setup

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

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

To trigger a specific port, click on the **Add** button. If you need to remove any of the server names, select the check box and click on the **Remove** button.

FIGURE 14. Adding NAT - Port Triggering Setup Panel



NAT -- Port Triggering

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

Remaining number of entries that can be configured:32

Use Interface: pppoe_0_1_35/ppp0

Application Name:

● Select an application: Select One

○ Custom application:

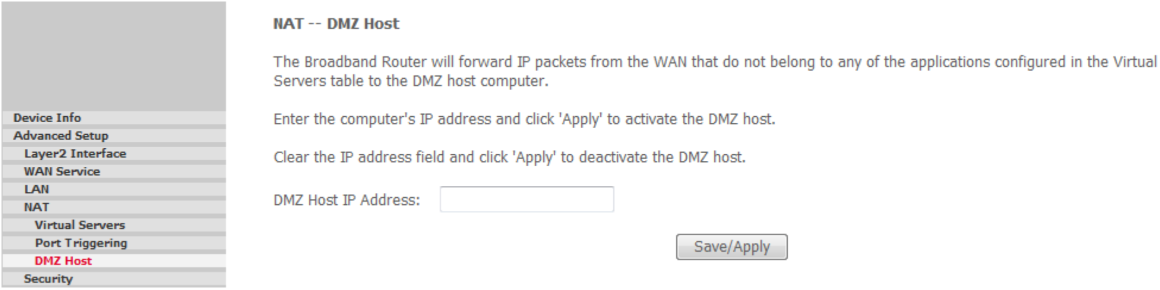
Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP

NAT >> DMZ HOST

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

Enter the IP address and click on **Save/Apply** button.

FIGURE 15. NAT – DMZ Host Panel



NAT -- DMZ Host

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

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

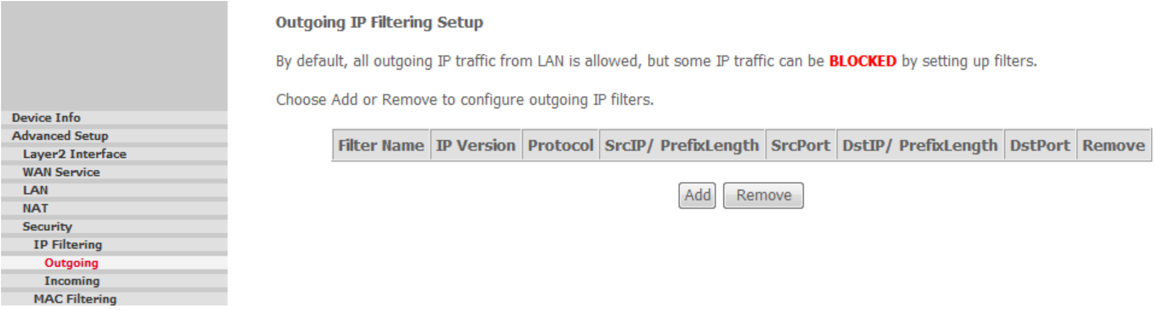
Clear the IP address field and click 'Apply' to deactivate the DMZ host.

DMZ Host IP Address:

SECURITY >> IP FILTERING >> OUTGOING

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be BLOCKED by setting up filters. Choose **Add** or **Remove** buttons to configure outgoing IP filters. The Add screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click **Save/ Apply** to save and activate the filter.

FIGURE 16. IP Filtering - Outgoing Panel



Outgoing IP Filtering Setup

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be BLOCKED by setting up filters.

Choose Add or Remove to configure outgoing IP filters.

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

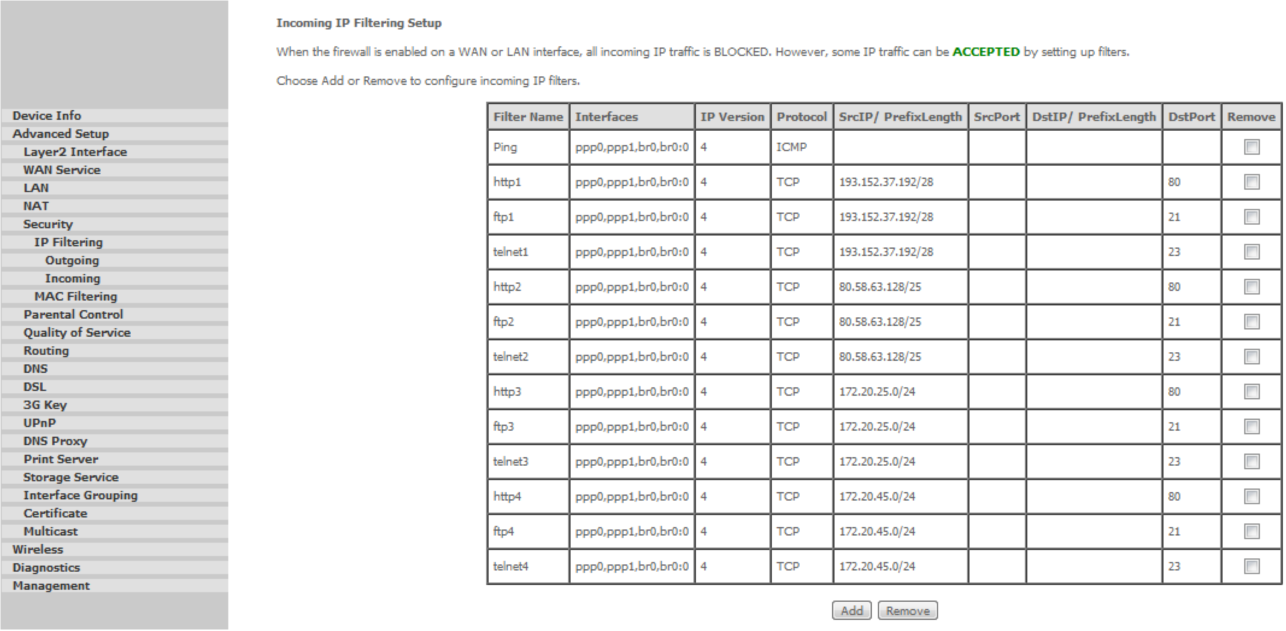
SECURITY >> IP FILTERING

>> INCOMING

When the firewall is enabled on a WAN or LAN interface, all incoming IP traffic is BLOCKED. However, some IP traffic can be ACCEPTED by setting up filters. Choose **Add** or **Remove** button to configure incoming IP filters.

The Add screen allows to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click **Apply/Save** to save and activate the filter.

FIGURE 17. IP Filtering - Incoming Panel



Incoming IP Filtering Setup

When the firewall is enabled on a WAN or LAN interface, all incoming IP traffic is BLOCKED. However, some IP traffic can be **ACCEPTED** by setting up filters.

Choose Add or Remove to configure incoming IP filters.

Filter Name	Interfaces	IP Version	Protocol	SrcIP/ PrefixLength	SrcPort	DstIP/ PrefixLength	DstPort	Remove
Ping	ppp0,ppp1,br0,br0:0	4	ICMP					□
http1	ppp0,ppp1,br0,br0:0	4	TCP	193.152.37.192/28			80	□
ftp1	ppp0,ppp1,br0,br0:0	4	TCP	193.152.37.192/28			21	□
telnet1	ppp0,ppp1,br0,br0:0	4	TCP	193.152.37.192/28			23	□
http2	ppp0,ppp1,br0,br0:0	4	TCP	80.58.63.128/25			80	□
ftp2	ppp0,ppp1,br0,br0:0	4	TCP	80.58.63.128/25			21	□
telnet2	ppp0,ppp1,br0,br0:0	4	TCP	80.58.63.128/25			23	□
http3	ppp0,ppp1,br0,br0:0	4	TCP	172.20.25.0/24			80	□
ftp3	ppp0,ppp1,br0,br0:0	4	TCP	172.20.25.0/24			21	□
telnet3	ppp0,ppp1,br0,br0:0	4	TCP	172.20.25.0/24			23	□
http4	ppp0,ppp1,br0,br0:0	4	TCP	172.20.45.0/24			80	□
ftp4	ppp0,ppp1,br0,br0:0	4	TCP	172.20.45.0/24			21	□
telnet4	ppp0,ppp1,br0,br0:0	4	TCP	172.20.45.0/24			23	□

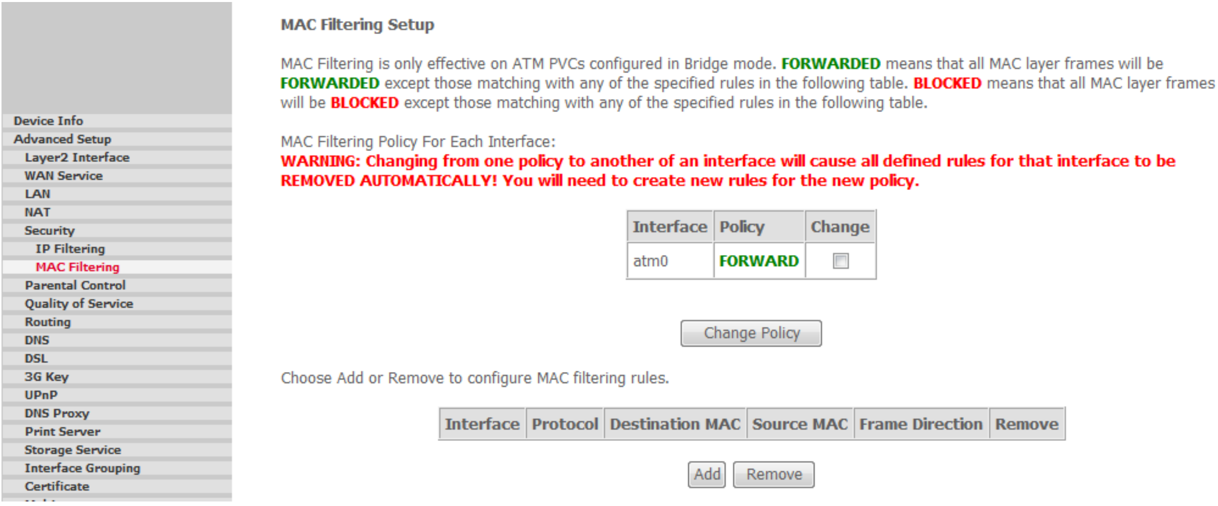
SECURITY >> MAC FILTERING

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

WARNING: Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.

In the Add MAC Filter panel, it is possible to create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click "**Apply**" to save and activate the filter.

FIGURE 18. MAC Filtering Panel



MAC Filtering Setup

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

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

Interface	Policy	Change
atm0	FORWARD	□

Choose Add or Remove to configure MAC filtering rules.

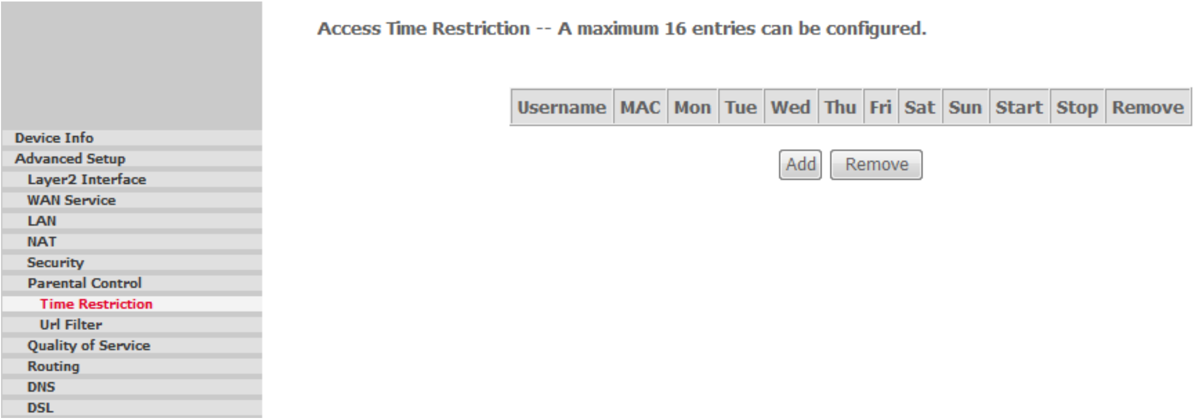
Interface	Protocol	Destination MAC	Source MAC	Frame Direction	Remove

PARENTAL CONTROL >> TIME RESTRICTION

By selecting **Parental Control >> Time Restriction** It is possible to configure the access time restrictions.
Choose **Add** or **Remove** button to configure the access time restrictions.

The Add screen allows to create a maximum of 16 entries.

FIGURE 19. Parental Control Time Restrictions Panel



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

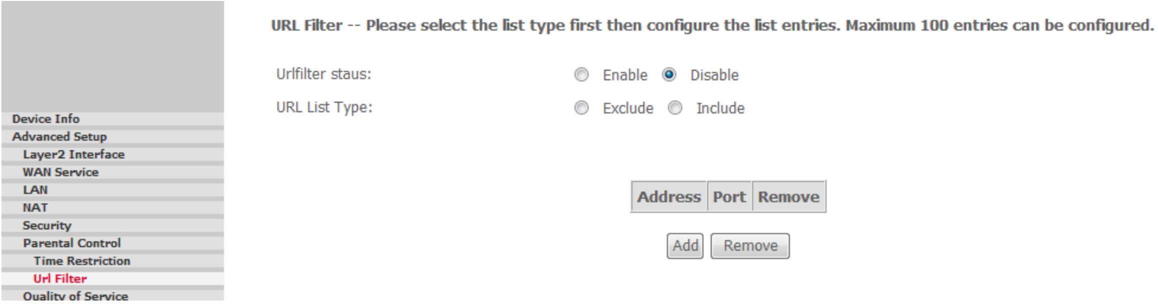
Username	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Remove

PARENTAL CONTROL >> URL FILTER

By selecting **Parental Control >> URL Filter** It is possible to configure the parental control.
Choose **Add** or **Remove** button to configure the parental control.

The Add screen allows to create a maximum of 16 entries.

FIGURE 20. URL Filter Panel



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

Urlfilter staus: ○ Enable ● Disable

URL List Type: ○ Exclude ○ Include

Address	Port	Remove

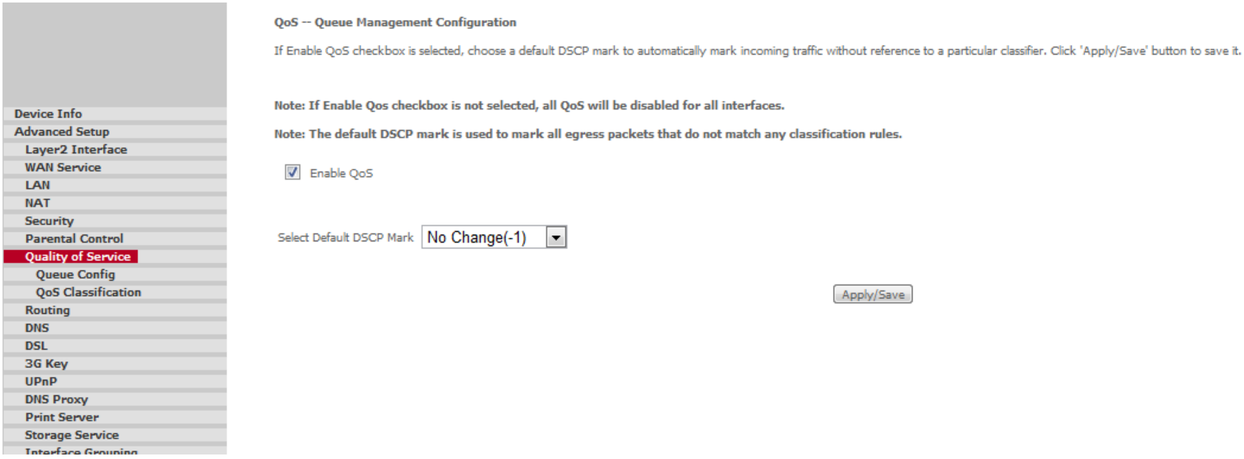
QUALITY OF SERVICE

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

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

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

FIGURE 21. QoS Panel



QoS -- Queue Management Configuration

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

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

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

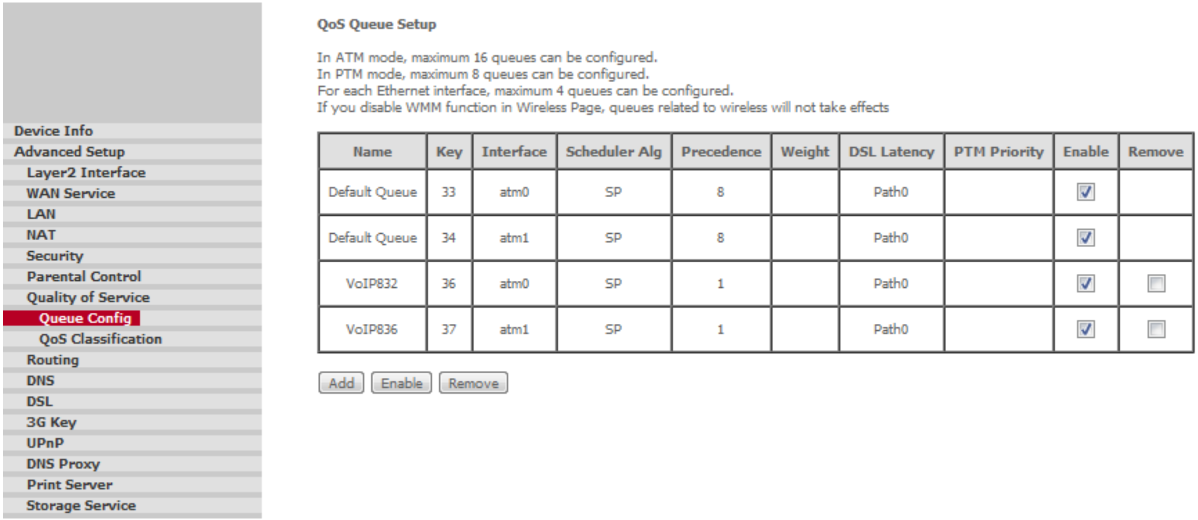
☑ Enable QoS

Select Default DSCP Mark: No Change(-1)

QUALITY OF SERVICE >> QUEUE CONFIG

In the QoS Queue Setup a maximum 16 entries can be configured. If you disable WMM function in Wireless Page, queues related to wireless will not take effects. SP and WRR can not be enabled at the same time.

FIGURE 22. QoS – Queue Config Panel



QoS Queue Setup

In ATM mode, maximum 16 queues can be configured.
In PTM mode, maximum 8 queues can be configured.
For each Ethernet interface, maximum 4 queues can be configured.
If you disable WMM function in Wireless Page, queues related to wireless will not take effects

Name	Key	Interface	Scheduler Alg	Precedence	Weight	DSL Latency	PTM Priority	Enable	Remove
Default Queue	33	atm0	SP	8		Path0		☑	
Default Queue	34	atm1	SP	8		Path0		☑	
VoIP832	36	atm0	SP	1		Path0		☑	□
VoIP836	37	atm1	SP	1		Path0		☑	□

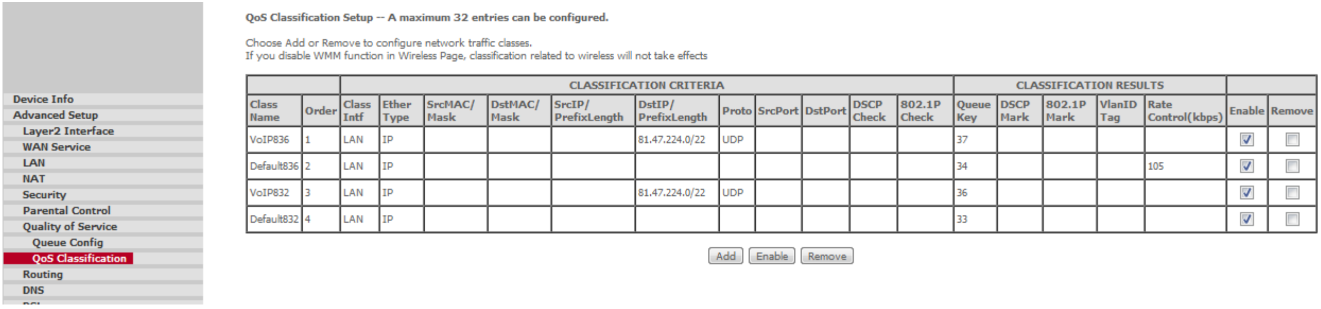
QUALITY OF SERVICE >> QOS CLASSIFICATION

In the QoS Classification Setup a maximum 32 entries can be configured. Choose Add or Remove to configure network traffic classes. If you disable WMM function in Wireless Page, classification related to wireless will not take effects.

In the Add Network Traffic Class Rule panel it is possible to create a traffic class rule to classify the upstream traffic, assign queue which defines the precedence and the interface and optionally overwrite the IP header DSCP byte. A rule consists of a class name and at least one condition below.

All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click **'Save/Apply'** to save and activate the rule.

FIGURE 23. **QoS Classification Panel**



QoS Classification Setup -- A maximum 32 entries can be configured.

Choose Add or Remove to configure network traffic classes.
If you disable WMM function in Wireless Page, classification related to wireless will not take effects

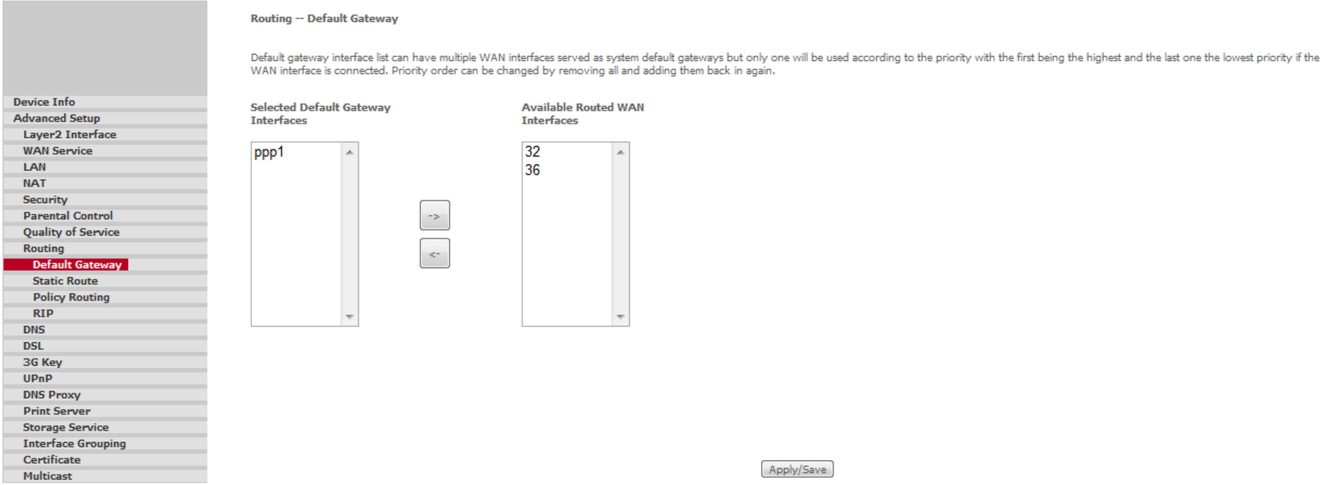
		CLASSIFICATION CRITERIA											CLASSIFICATION RESULTS						
Class Name	Order	Class Intf	Ether Type	SrcMAC/ Mask	DstMAC/ Mask	SrcIP/ PrefixLength	DstIP/ PrefixLength	Proto	SrcPort	DstPort	DSCP Check	802.1P Check	Queue Key	DSCP Mark	802.1P Mark	VlanID Tag	Rate Control(kbps)	Enable	Remove
VoIP836	1	LAN	IP				81.47.224.0/22	UDP					37					☑	□
Default836	2	LAN	IP										34				105	☑	□
VoIP832	3	LAN	IP				81.47.224.0/22	UDP					36					☑	□
Default832	4	LAN	IP										33					☑	□

ROUTING >> DEFAULT GATEWAY

If *more than one WAN interface exists*, the router will need to define a preferred default gateway assignment. Click **Apply/Save** button to save it.

If changing the Automatic Assigned Default Gateway from unselected to selected, You must reboot the router to get the automatic assigned default gateway.

FIGURE 24. **Default Gateway Panel**



Routing -- Default Gateway

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

Selected Default Gateway Interfaces: ppp1

Available Routed WAN Interfaces: 32, 36

ROUTING >> STATIC ROUTE

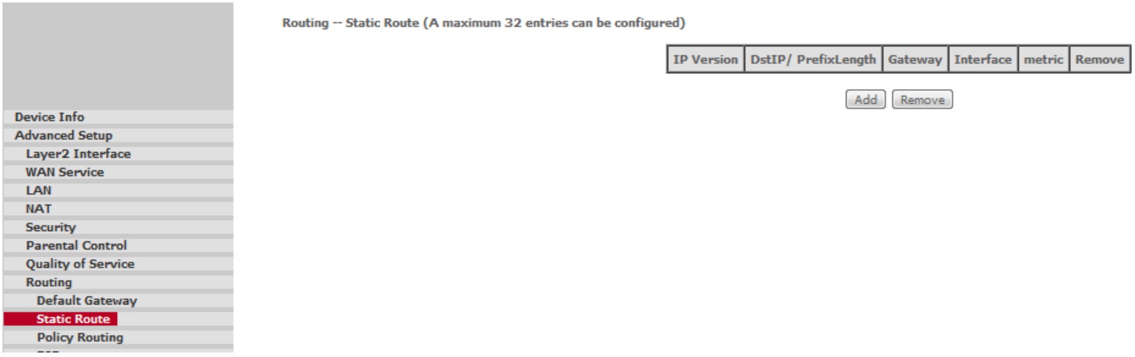
The Static Route screen can be used to add a routing table (a maximum of 32 entries can be configured). Click on **Add** button to add a static route and, at the end of parameters' configuration, press the **Apply/Save** button.

The **Remove** button, upon a route selection, will delete existing static routes.

TABLE 3. **Static Route Parameters**

Parameter	Description	Example
Destination	*Destination Network address*	*20.0.0.0*
Subnet Mask	*Subnet mask*	*255.255.255.0*
Gateway	*Gateway IP address*	
Interface	*Available WAN interfaces*	*br0*

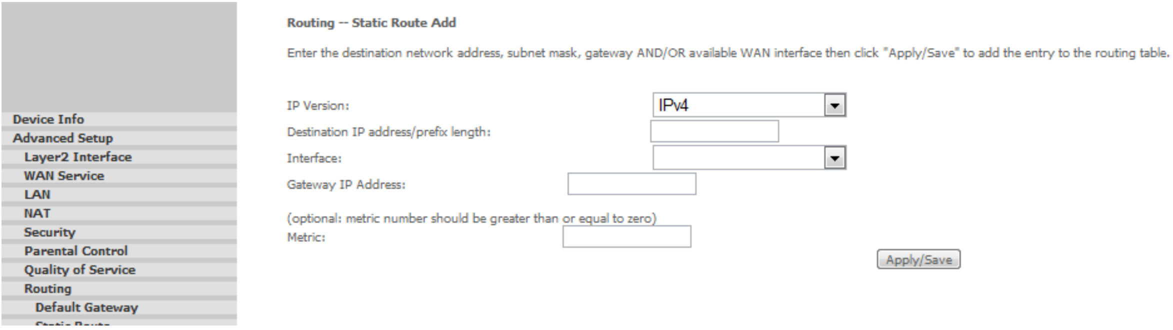
FIGURE 25. **Static Route Panel**



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

IP Version	DstIP/ PrefixLength	Gateway	Interface	metric	Remove

FIGURE 26. **Add Static Route Panel**



Routing -- Static Route Add

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

IP Version: IPv4

Destination IP address/prefix length:

Interface:

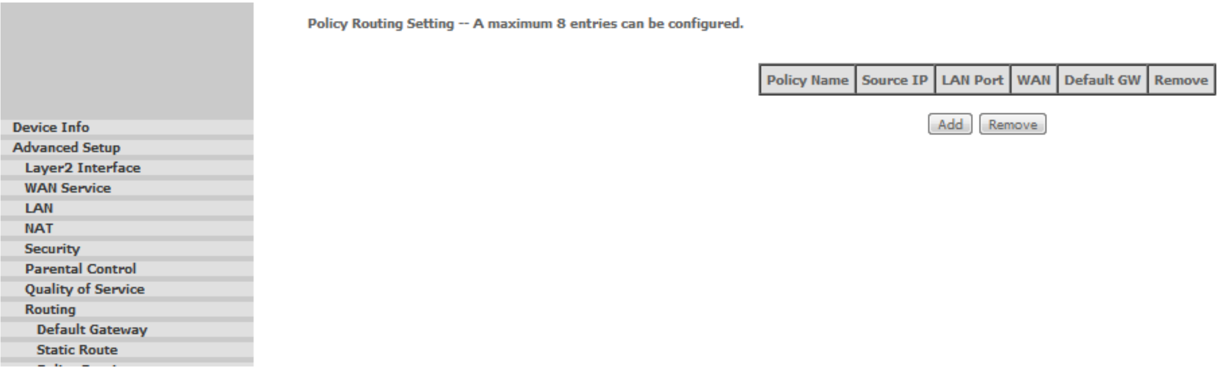
Gateway IP Address:

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

ROUTING >> POLICY ROUTING

In the Policy Routing Setting panel a maximum 8 entries can be configured.
In the Policy Routing Setup panel, enter the policy name, policies, and WAN interface then click "Save/Apply" to add the entry to the policy routing table.

FIGURE 27. **Policy Routing Panel**



Policy Routing Setting -- A maximum 8 entries can be configured.

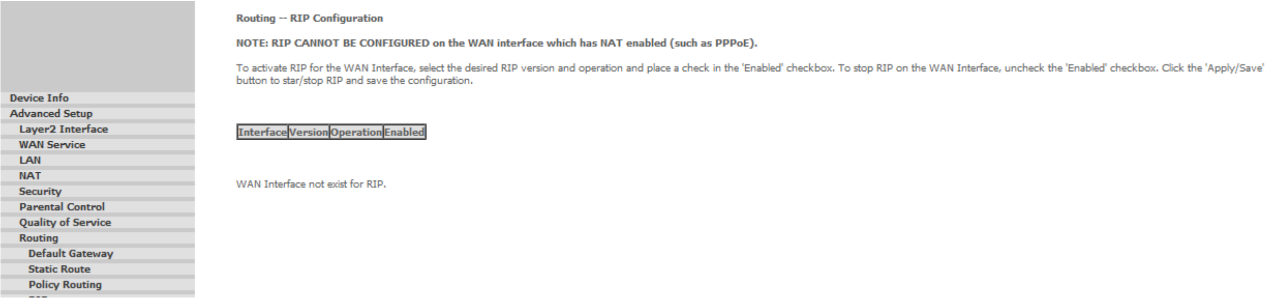
Policy Name	Source IP	LAN Port	WAN	Default GW	Remove

ROUTING >> RIP

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

NOTE: Rip cannot be configured on the WAN interface which has NAT enabled (such as PPPoE).

FIGURE 28. **Rip Panel**



Routing -- RIP Configuration

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

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

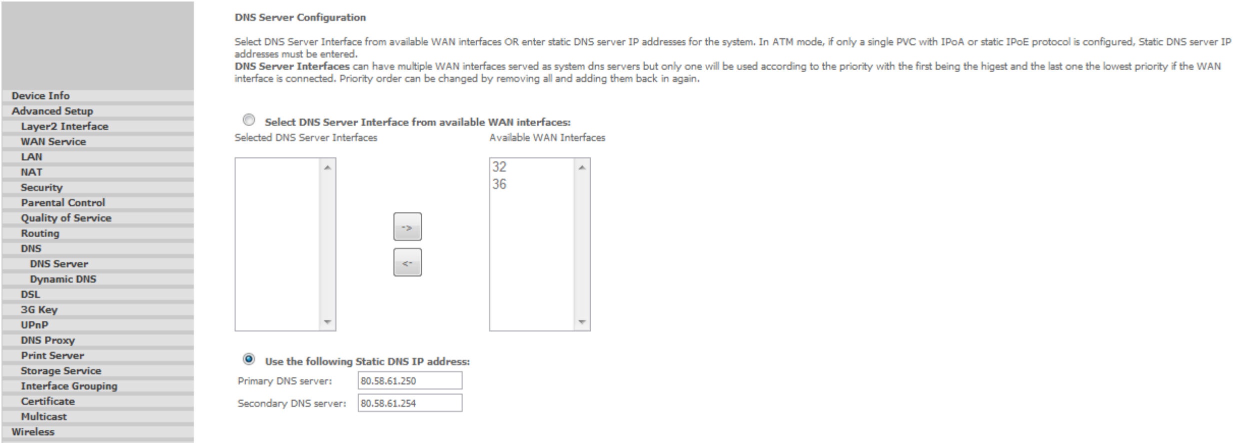
Interface	Version	Operation	Enabled

WAN Interface not exist for RIP.

DNS >> DNS SERVER

In the DNS Server Configuration panel, select the configured WAN interface for DNS server information OR enter the static DNS server IP Addresses for single PVC with IPoA, static MER protocol.

FIGURE 29. DNS Server Panel



DNS Server Configuration

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

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

Selected DNS Server Interfaces

Available WAN Interfaces
32
36

● **Use the following Static DNS IP address:**

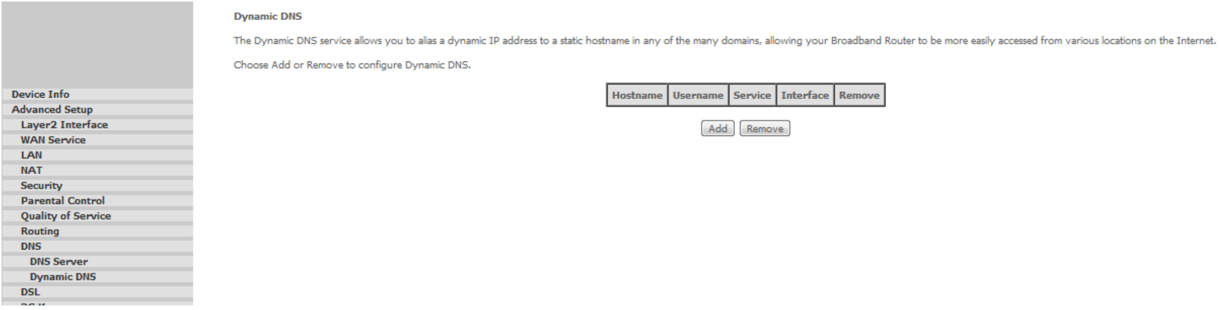
Primary DNS server: 80.58.61.250

Secondary DNS server: 80.58.61.254

DNS >> DYNAMIC DNS

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your DSL router to be more easily accessed from various locations on the Internet.
Choose Add or Remove to configure Dynamic DNS.
In the Add Dynamic DNS panel, it is possible to add a Dynamic DNS address from DynDNS.org or TZO.

FIGURE 30. Dynamic DNS Panel



Dynamic DNS

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

Choose Add or Remove to configure Dynamic DNS.

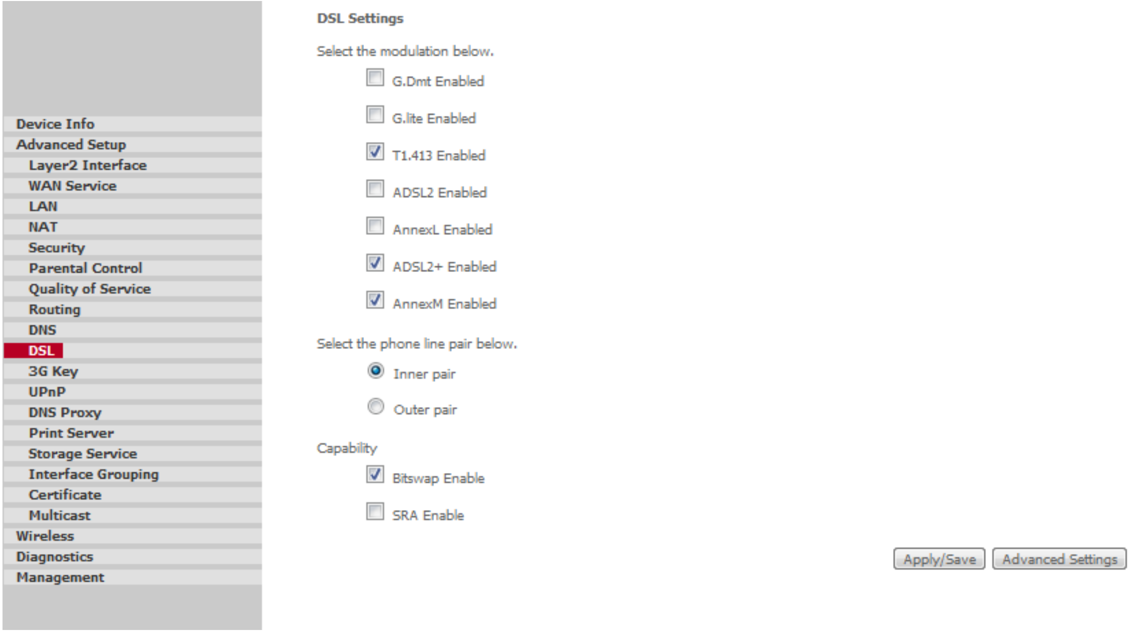
Hostname	Username	Service	Interface	Remove

DSL

The DSL settings screen contains three sections: modulation, phone line, and capability that should be specified by your ISP.
Consult with your ISP to select the correct settings for each.

Click on **Apply/Save** if you are finished or click on **Advanced Settings** button if you want to configure more advanced settings.

FIGURE 31. DSL Settings Panel



DSL Settings

Select the modulation below.

□ G.Dmt Enabled

□ G.lite Enabled

☑ T1.413 Enabled

□ ADSL2 Enabled

□ AnnexL Enabled

☑ ADSL2+ Enabled

☑ AnnexM Enabled

Select the phone line pair below.

● Inner pair

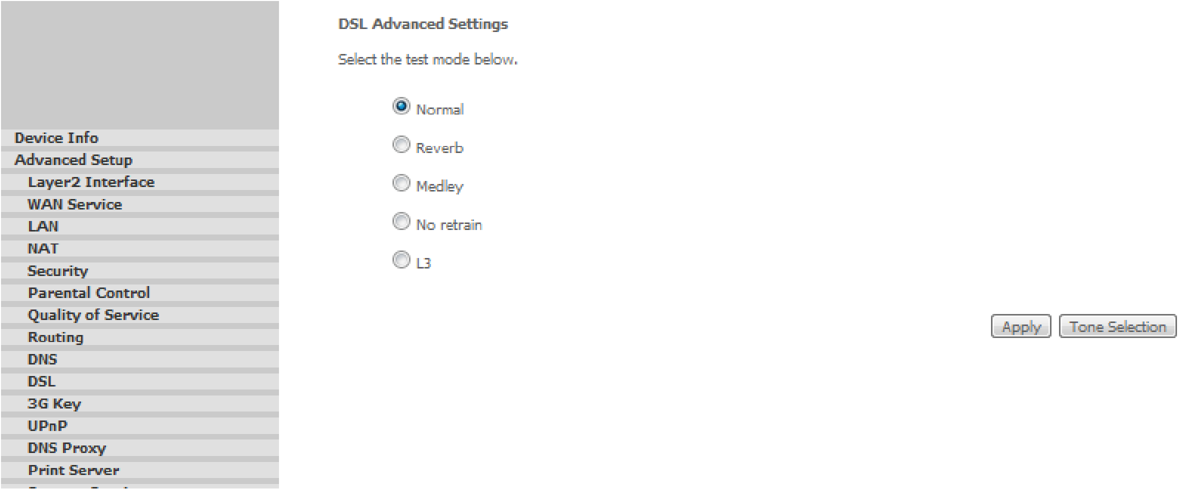
○ Outer pair

Capability

☑ Bitswap Enable

□ SRA Enable

FIGURE 32. DSL Advanced Settings Panel



DSL Advanced Settings

Select the test mode below.

● Normal

○ Reverb

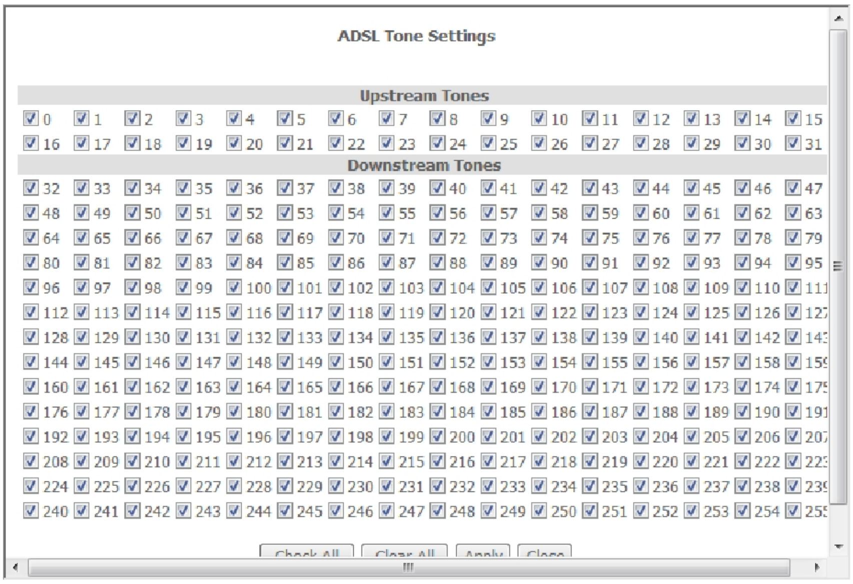
○ Medley

○ No retrain

○ L3

The test mode can be selected from the DSL Advanced Settings screen. Test modes include normal, reverb, medley, no retrain, and L3.

FIGURE 33. DSL Advanced Settings - Tone Selection Panel



ADSL Tone Settings

Upstream Tones

☑ 0 ☑ 1 ☑ 2 ☑ 3 ☑ 4 ☑ 5 ☑ 6 ☑ 7 ☑ 8 ☑ 9 ☑ 10 ☑ 11 ☑ 12 ☑ 13 ☑ 14 ☑ 15
☑ 16 ☑ 17 ☑ 18 ☑ 19 ☑ 20 ☑ 21 ☑ 22 ☑ 23 ☑ 24 ☑ 25 ☑ 26 ☑ 27 ☑ 28 ☑ 29 ☑ 30 ☑ 31

Downstream Tones

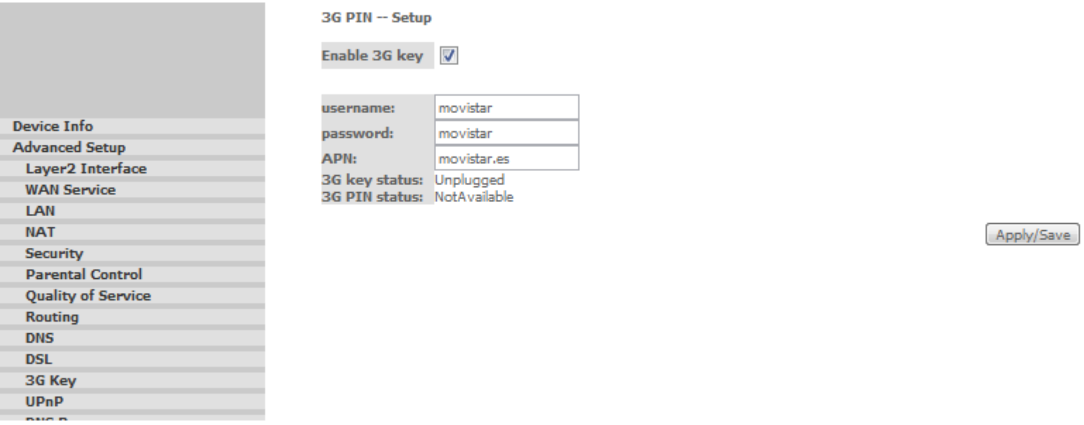
☑ 32 ☑ 33 ☑ 34 ☑ 35 ☑ 36 ☑ 37 ☑ 38 ☑ 39 ☑ 40 ☑ 41 ☑ 42 ☑ 43 ☑ 44 ☑ 45 ☑ 46 ☑ 47
☑ 48 ☑ 49 ☑ 50 ☑ 51 ☑ 52 ☑ 53 ☑ 54 ☑ 55 ☑ 56 ☑ 57 ☑ 58 ☑ 59 ☑ 60 ☑ 61 ☑ 62 ☑ 63
☑ 64 ☑ 65 ☑ 66 ☑ 67 ☑ 68 ☑ 69 ☑ 70 ☑ 71 ☑ 72 ☑ 73 ☑ 74 ☑ 75 ☑ 76 ☑ 77 ☑ 78 ☑ 79
☑ 80 ☑ 81 ☑ 82 ☑ 83 ☑ 84 ☑ 85 ☑ 86 ☑ 87 ☑ 88 ☑ 89 ☑ 90 ☑ 91 ☑ 92 ☑ 93 ☑ 94 ☑ 95
☑ 96 ☑ 97 ☑ 98 ☑ 99 ☑ 100 ☑ 101 ☑ 102 ☑ 103 ☑ 104 ☑ 105 ☑ 106 ☑ 107 ☑ 108 ☑ 109 ☑ 110 ☑ 111
☑ 112 ☑ 113 ☑ 114 ☑ 115 ☑ 116 ☑ 117 ☑ 118 ☑ 119 ☑ 120 ☑ 121 ☑ 122 ☑ 123 ☑ 124 ☑ 125 ☑ 126 ☑ 12
☑ 128 ☑ 129 ☑ 130 ☑ 131 ☑ 132 ☑ 133 ☑ 134 ☑ 135 ☑ 136 ☑ 137 ☑ 138 ☑ 139 ☑ 140 ☑ 141 ☑ 142 ☑ 14
☑ 144 ☑ 145 ☑ 146 ☑ 147 ☑ 148 ☑ 149 ☑ 150 ☑ 151 ☑ 152 ☑ 153 ☑ 154 ☑ 155 ☑ 156 ☑ 157 ☑ 158 ☑ 15
☑ 160 ☑ 161 ☑ 162 ☑ 163 ☑ 164 ☑ 165 ☑ 166 ☑ 167 ☑ 168 ☑ 169 ☑ 170 ☑ 171 ☑ 172 ☑ 173 ☑ 174 ☑ 17
☑ 176 ☑ 177 ☑ 178 ☑ 179 ☑ 180 ☑ 181 ☑ 182 ☑ 183 ☑ 184 ☑ 185 ☑ 186 ☑ 187 ☑ 188 ☑ 189 ☑ 190 ☑ 191
☑ 192 ☑ 193 ☑ 194 ☑ 195 ☑ 196 ☑ 197 ☑ 198 ☑ 199 ☑ 200 ☑ 201 ☑ 202 ☑ 203 ☑ 204 ☑ 205 ☑ 206 ☑ 20
☑ 208 ☑ 209 ☑ 210 ☑ 211 ☑ 212 ☑ 213 ☑ 214 ☑ 215 ☑ 216 ☑ 217 ☑ 218 ☑ 219 ☑ 220 ☑ 221 ☑ 222 ☑ 22
☑ 224 ☑ 225 ☑ 226 ☑ 227 ☑ 228 ☑ 229 ☑ 230 ☑ 231 ☑ 232 ☑ 233 ☑ 234 ☑ 235 ☑ 236 ☑ 237 ☑ 238 ☑ 23
☑ 240 ☑ 241 ☑ 242 ☑ 243 ☑ 244 ☑ 245 ☑ 246 ☑ 247 ☑ 248 ☑ 249 ☑ 250 ☑ 251 ☑ 252 ☑ 253 ☑ 254 ☑ 25

The frequency band of ADSL is split up into 256 separate tones, each spaced 4.3125 kHz apart. With each tone carrying separate data, the technique operates as if 256 separate modems were running in parallel. The tone range is from 0 to 31 for upstream and from 32 to 255 for downstream. Do not change these settings unless so directed by your ISP.

3G Key

In the 3G Key panel it is possible to enable/disable the 3G key functionality, and when enabled, to define the mobile operator service provider username, password and APN.
To apply settings, please select the **Apply/Save** button.

FIGURE 34. **3G Key Panel**



3G PIN -- Setup

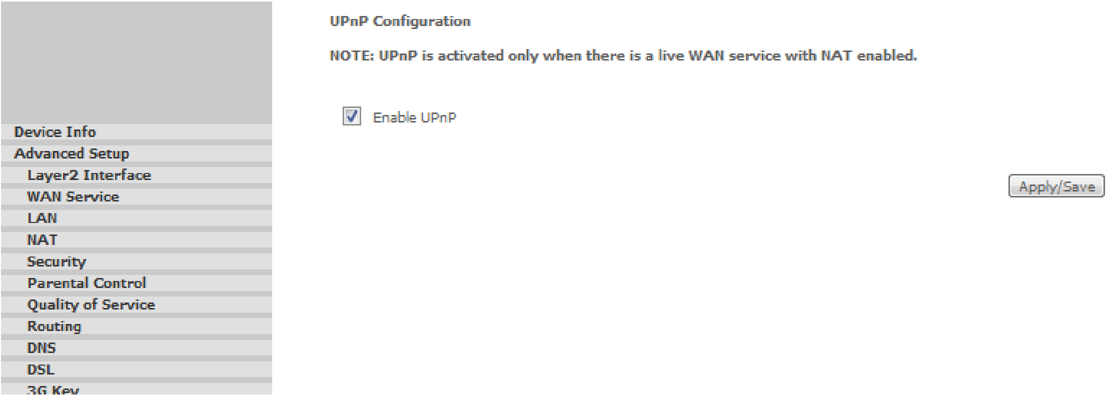
Enable 3G key ☑

username:	movistar
password:	movistar
APN:	movistar.es
3G key status:	Unplugged
3G PIN status:	NotAvailable

UPNP

In the UPnP panel it is possible to enable/disable the UPnP functionality.

FIGURE 35. **UPnP Panel**



UPnP Configuration

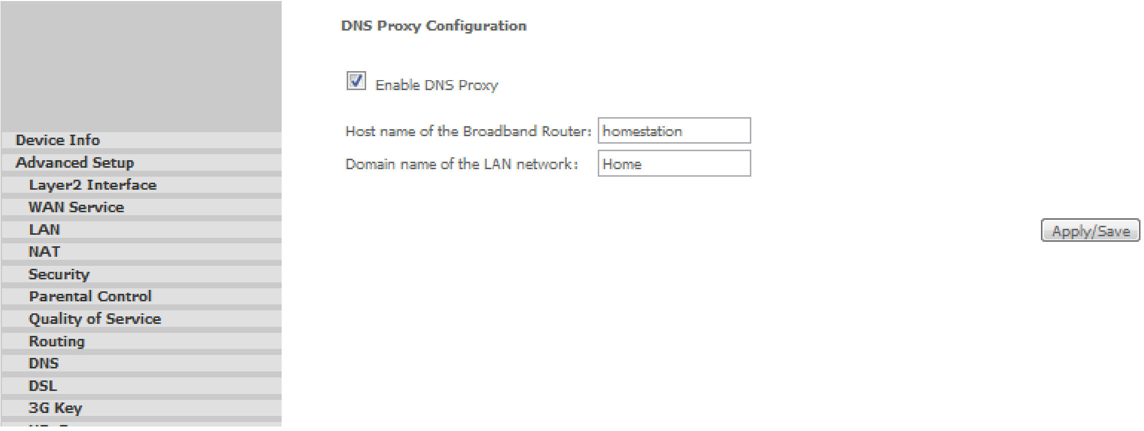
NOTE: UPnP is activated only when there is a live WAN service with NAT enabled.

☑ Enable UPnP

DNS PROXY

In the DNS Proxy panel it is possible to enable/disable the DNS Proxy functionality and, if enabled, to configure it.

FIGURE 36. **DNS Proxy Panel**



DNS Proxy Configuration

☑ Enable DNS Proxy

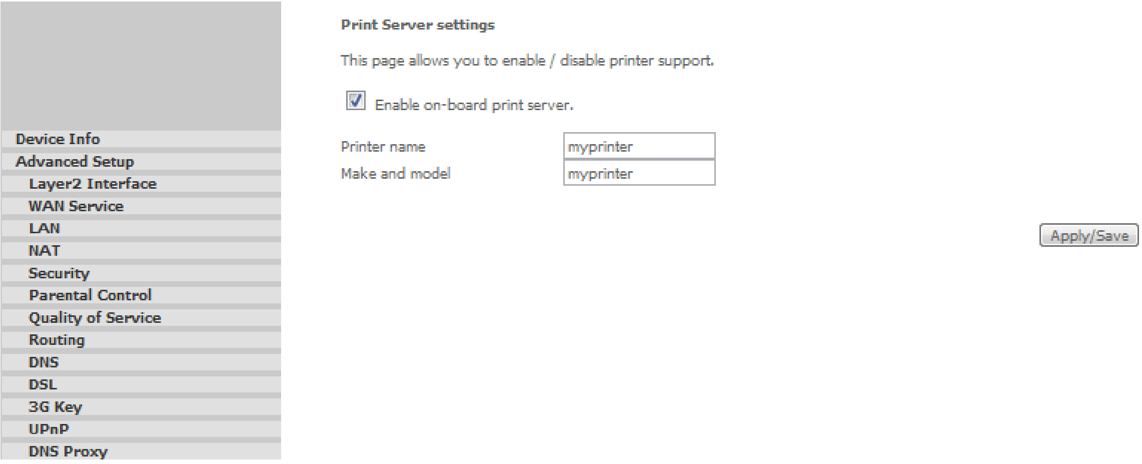
Host name of the Broadband Router: homestation

Domain name of the LAN network: Home

PRINT SERVER

This page allows you to enable / disable printer support.

FIGURE 37. **Print Server Panel**



Print Server settings

This page allows you to enable / disable printer support.

☑ Enable on-board print server.

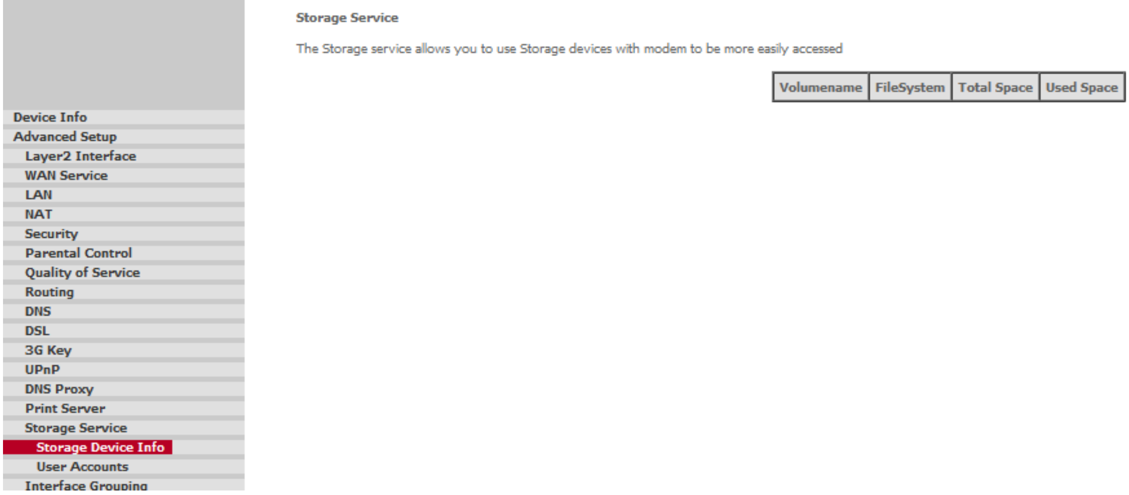
Printer name: myprinter

Make and model: myprinter

STORAGE SERVICE >> DEVICE INFO

In the Storage Device Info panel it is possible to find the attached storage information. The Storage service allows you to use Storage devices with modem to be more easily accessed.

FIGURE 38. **Storage Service – Device Info Panel**



Storage Service

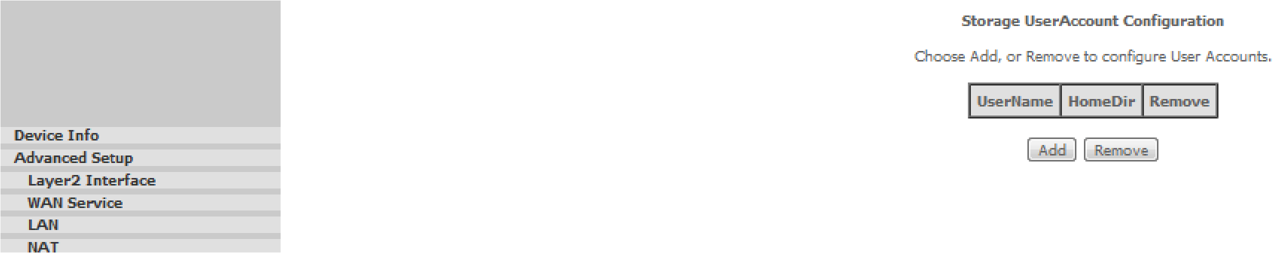
The Storage service allows you to use Storage devices with modem to be more easily accessed

Volumename	FileSystem	Total Space	Used Space

STORAGE SERVICE >> USER ACCOUNT

In the Storage User Account panel it is possible to configure User Accounts. Choose **Add** or **Remove** button to configure User Accounts.

FIGURE 39. **Storage Service – User AccountPanel**



Storage UserAccount Configuration

Choose Add, or Remove to configure User Accounts.

UserName	HomeDir	Remove

INTERFACE GROUPING

In the Interface Grouping panel a maximum of 16 entries can be configured.

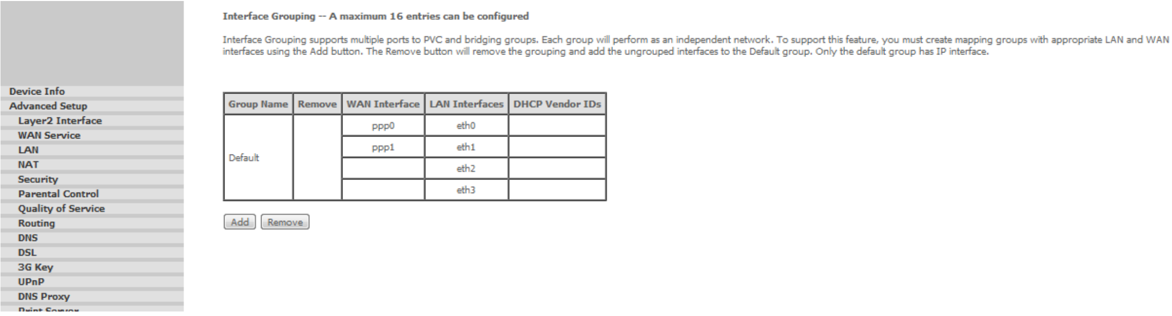
Interface Grouping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped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

1. Enter the Group name and the group name must be unique and select either 2. (dynamic) or 3. (static) below:

2. If you like to automatically add LAN clients to a WAN Interface in the new group add the DHCP vendor ID string. By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.
3.Select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. Note that these clients may obtain public IP addresses

4. Click **Save/Apply** button to make the changes effective immediately

FIGURE 40. Interface Grouping Panel



Interface Grouping -- A maximum 16 entries can be configured

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

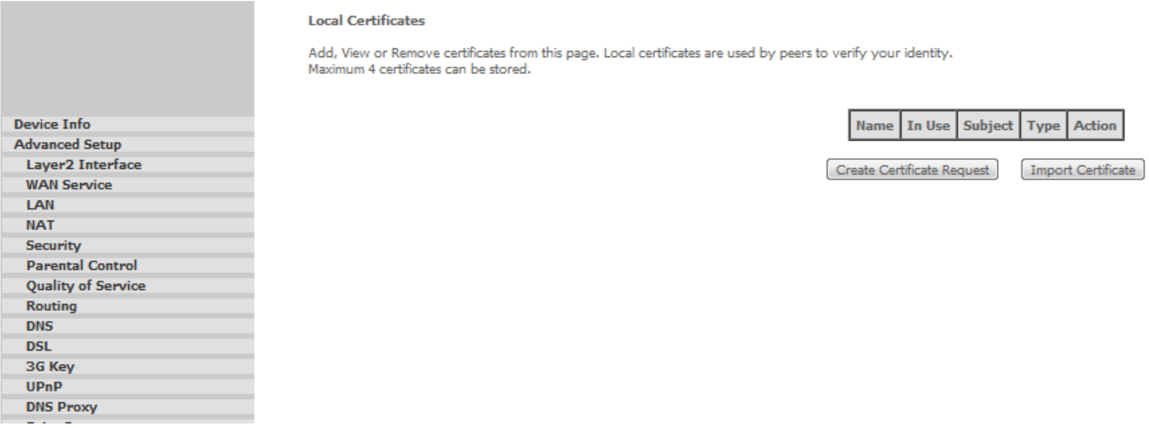
Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs
Default		ppp0	eth0	
		ppp1	eth1	
			eth2	
			eth3	

CERTIFICATE >> LOCAL

In the Local Certificates panel it is possible to add, View or Remove certificates. Local certificates are used by peers to verify your identity.

Maximum 4 certificates can be stored.

FIGURE 41. Local Certificate Panel



Local Certificates

Add, View or Remove certificates from this page. Local certificates are used by peers to verify your identity.
Maximum 4 certificates can be stored.

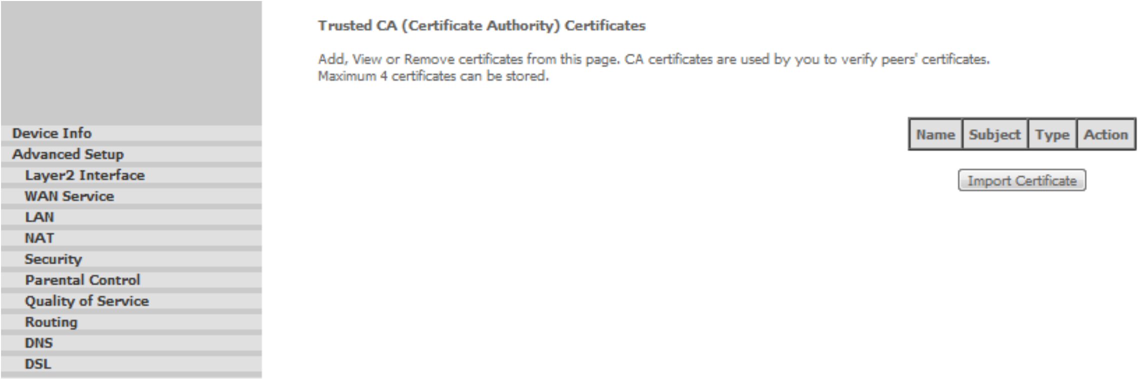
Name	In Use	Subject	Type	Action

CERTIFICATE >> TRUSTED CA

In the Trusted CA (Certificate Authority) Certificates panel it is possible to add, View or Remove certificates from this page. CA certificates are used by you to verify peers' certificates.

Maximum 4 certificates can be imported and stored.

FIGURE 42. Trusted CA Panel



Trusted CA (Certificate Authority) Certificates

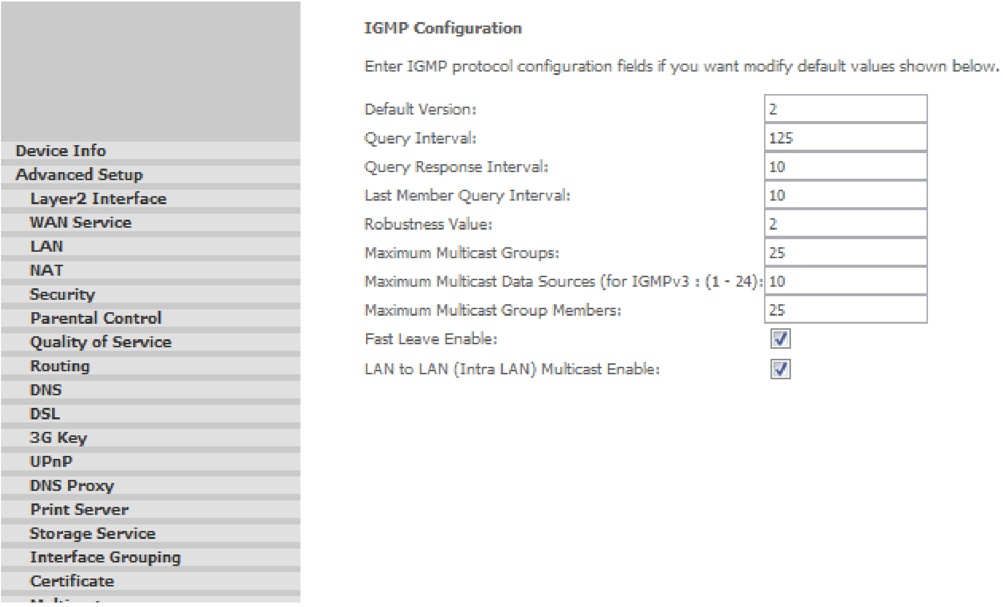
Add, View or Remove certificates from this page. CA certificates are used by you to verify peers' certificates.
Maximum 4 certificates can be stored.

Name	Subject	Type	Action

MULTICAST

In the Multicast panel it is possible to configure the IGMP Protocol. Select the **Apply/Save** button to apply changes.

FIGURE 43. **Multicast Panel**



IGMP Configuration

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

Default Version:	2
Query Interval:	125
Query Response Interval:	10
Last Member Query Interval:	10
Robustness Value:	2
Maximum Multicast Groups:	25
Maximum Multicast Data Sources (for IGMPv3 : (1 - 24):	10
Maximum Multicast Group Members:	25
Fast Leave Enable:	☑
LAN to LAN (Intra LAN) Multicast Enable:	☑

This Page Intentionally Left Blank

Wireless Section

This chapter will describe the Wireless Section accessible from the Home Page of the P.DG A4001N.

This section is only accessible to a user with admin profile.

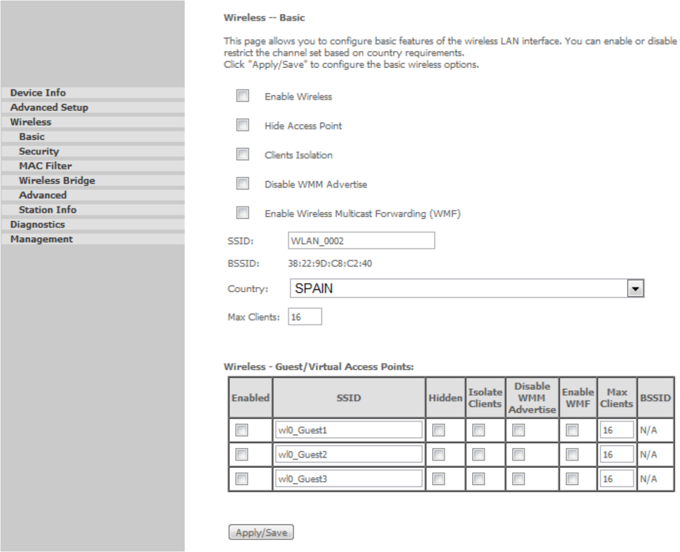
Be aware that any configuration change could compromise your connectivity.

BASIC

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless SSID and restrict the channel set based on country requirements.

Click "**Apply/Save**" button to configure the basic wireless options.

FIGURE 1. **Wireless Basic Panel**



Wireless -- Basic

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

□ Enable Wireless

□ Hide Access Point

□ Clients Isolation

□ Disable WMM Advertise

□ Enable Wireless Multicast Forwarding (WMF)

SSID: WLAN_0002

BSSID: 38:22:9D:C8:C2:40

Country: SPAIN

Max Clients: 16

Wireless - Guest/Virtual Access Points:

Enabled	SSID	Hidden	Isolate Clients	Disable WMM Advertise	Enable WMF	Max Clients	BSSID
□	wl0_Guest1	□	□	□	□	16	N/A
□	wl0_Guest2	□	□	□	□	16	N/A
□	wl0_Guest3	□	□	□	□	16	N/A

SECURITY

This page allows you to configure security features of the wireless LAN interface by means of a manual configuration or through a Wi-Fi protected Setup (WPS).

In case the manual setup AP is the preferred choice, the network authentication method, selecting data encryption, specifying whether a network key is required to authenticate to this wireless network and specifying the encryption strength are to be selected. This page allows you to select the network authentication method and to enable or disable WEP encryption.

Depending on the network authentication that is selected, the screen will change accordingly so additional fields can be configured for the specific authentication method.

Allowed Network Authentication are:

1. **Open** — anyone can access the network. The default is a disabled WEP encryption setting.

2. **Shared** — WEP encryption is enabled and encryption key strength of 64-bit or 128-bit needs to be selected. Click on Set Encryption Keys to manually

set the network encryption keys. Up to 4 different keys can be set and you can come back to select which one to use at anytime.

3. **802.1X** — requires mutual authentication between a client station and the router by including a RADIUS-based authentication server. Information about the RADIUS server such as its IP address, port and key must be entered. WEP encryption is also enabled and the encryption strength must also be selected.

4. **WPA** — (WiFi Protected Access) — usually used for the larger Enterprise environment, it uses a RADIUS server and TKIP (Temporal Key Integrity Protocol) encryption (instead of WEP encryption which is disabled). TKIP uses128-bit dynamic session keys (per user, per session, and per packet keys).

5. **WPA-PSK** (WiFi Protected Access – Pre-Shared Key)—WPA for home and SOHO environments also using the same strong TKIP encryption, per-packet key construction, and key management that WPA provides in the enterprise environment. The main difference is that the password is entered manually. A group re-key interval time is also required.

6. **WPA2** (WiFi Protected Access 2) —second generation of WPA which uses AES (Advanced Encryption Standard) instead of TKIP as its encryption method. Network re-auth interval is the time in which another key needs to be dynamically issued.

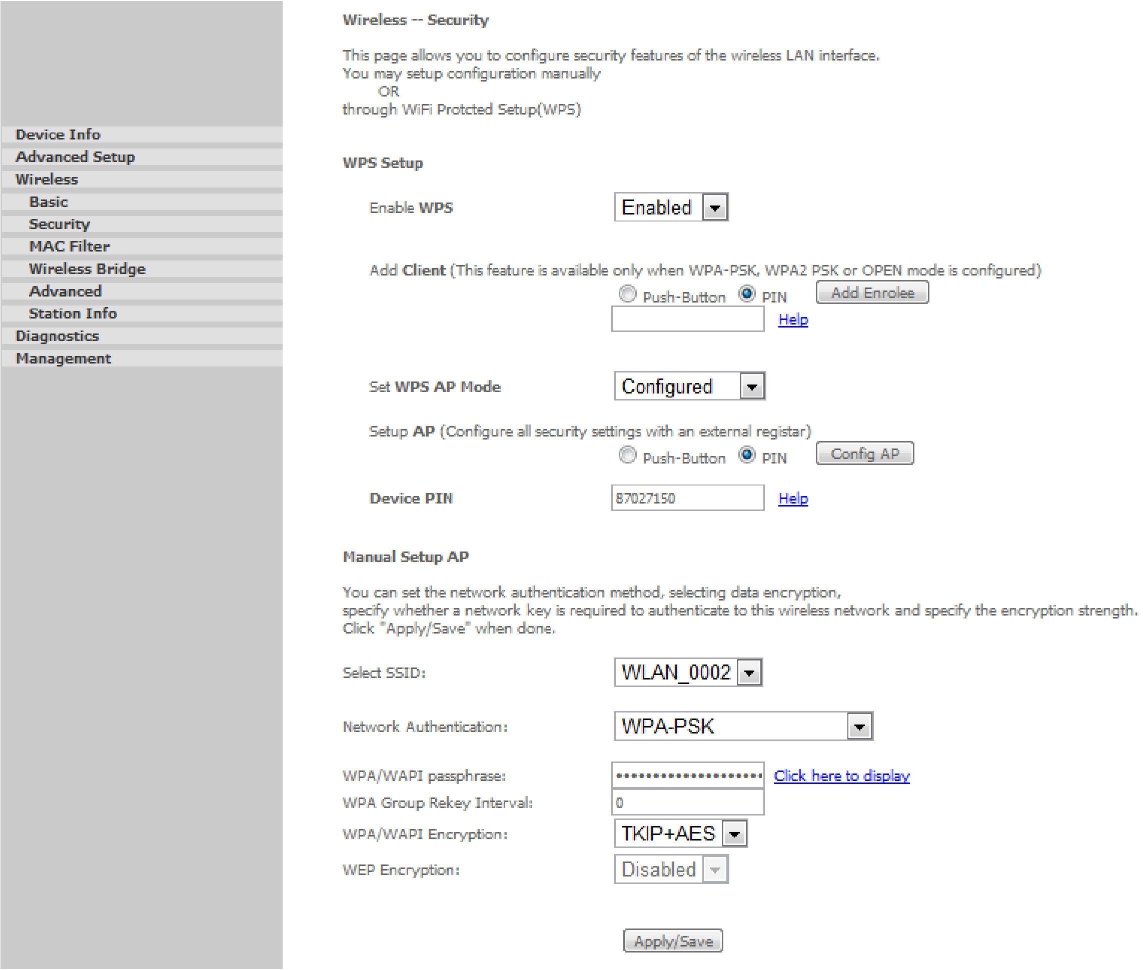
7. **WPA2-PSK** (WiFi Protected Access 2 – Pre-Shared Key)—suitable for home and SOHO environments, it also uses AES encryption and requires you to enter a password and an re-key interval time.

8. **Mixed WPA2 / WPA** —during transitional times for upgrades in the enterprise environment, this mixed authentication method allows “upgraded” and users not yet “upgraded” to access the network via the router. RADIUS server information must be entered for WPA and a as well as a group re-key interval time. Both TKIP and AES are used.

9. **Mixed WPA2 / WPA-PSK** —useful during transitional times for upgrades in the home or SOHO environment, a pre-shared key must be entered along with the group re-key interval time. Both TKIP and AES are also used.

Click "**Apply/Save**" button to configure the wireless security options.

FIGURE 2. **Wireless Security Panel**



Wireless -- Security

This page allows you to configure security features of the wireless LAN interface.
You may setup configuration manually
OR
through WiFi Protcted Setup(WPS)

WPS Setup

Enable **WPS**: Enabled

Add **Client** (This feature is available only when WPA-PSK, WPA2 PSK or OPEN mode is configured)
○ Push-Button ● PIN

Set **WPS AP Mode**: Configured

Setup **AP** (Configure all security settings with an external registar)
○ Push-Button ● PIN

Device PIN: 87027150

Manual Setup AP

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

Select SSID: WLAN_0002

Network Authentication: WPA-PSK

WPA/WAPI passphrase: ••••••••••••••••••••
WPA Group Rekey Interval: 0
WPA/WAPI Encryption: TKIP+AES
WEP Encryption: Disabled

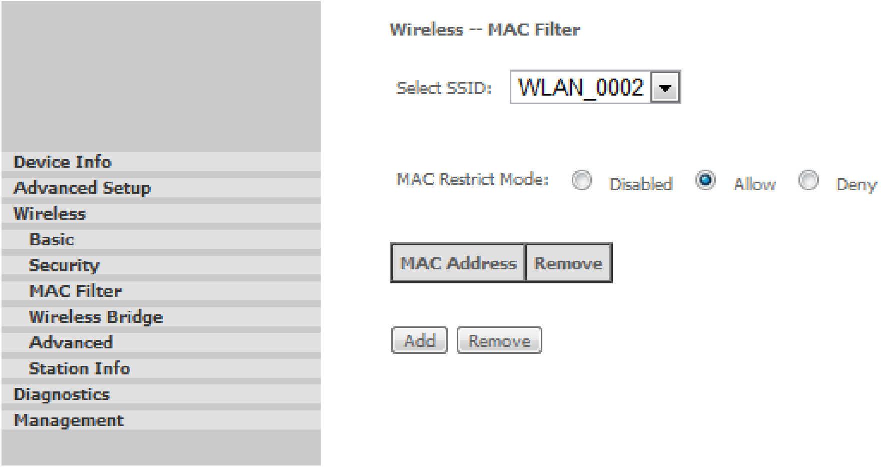
In case the WPS setup will be chosen (thus setting “Enable WPS” field to “Enabled”), the push button or PIN based connection must be selected according to shown parameters’ configuration.

MAC FILTER

In the MAC Filter panel it is possible, if enabled, to set a list of devices (identified by means of their MAC address) whose access is allowed or denied.

The list can be managed through the Add and Remove buttons: by clicking on the “**Add**” button, you will be asked to enter the MAC address and click the "**Apply/Save**" button to add the MAC address to the wireless MAC address filters; by checking the Remove check-box and by clicking on the Remove button, the selected MAC address will be removed from the list.

FIGURE 3. **Wireless MAC Filter Panel**



Wireless -- MAC Filter

Select SSID: WLAN_0002

MAC Restrict Mode: ○ Disabled ● Allow ○ Deny

WIRELESS BRIDGE

This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge to disables access point functionality.

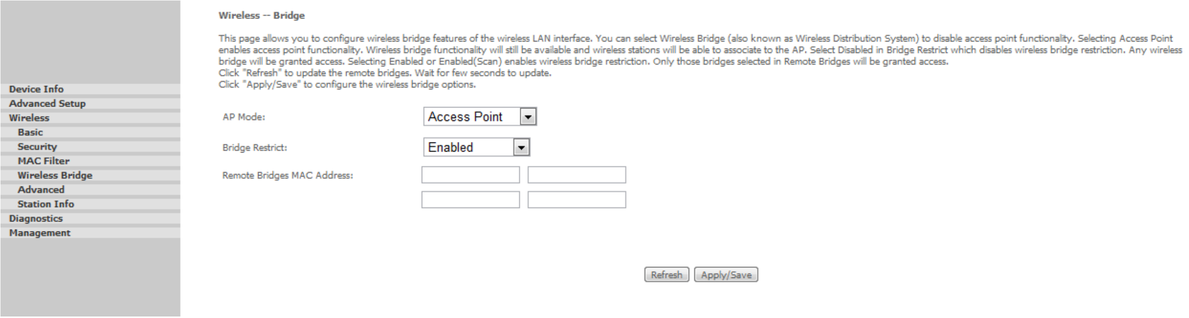
Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select “Disabled” in Bridge Restrict disables wireless bridge restriction. Any wireless bridge will be granted access.

By selecting “Enabled” or “Enabled(Scan)”, it enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access.

Click "**Refresh**" to update the remote bridges. Wait for few seconds to update.

Click "**Apply/Save**" to configure the wireless bridge options.

FIGURE 4. **Wireless Bridge settings**



Wireless -- Bridge

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

AP Mode: Access Point

Bridge Restrict: Enabled

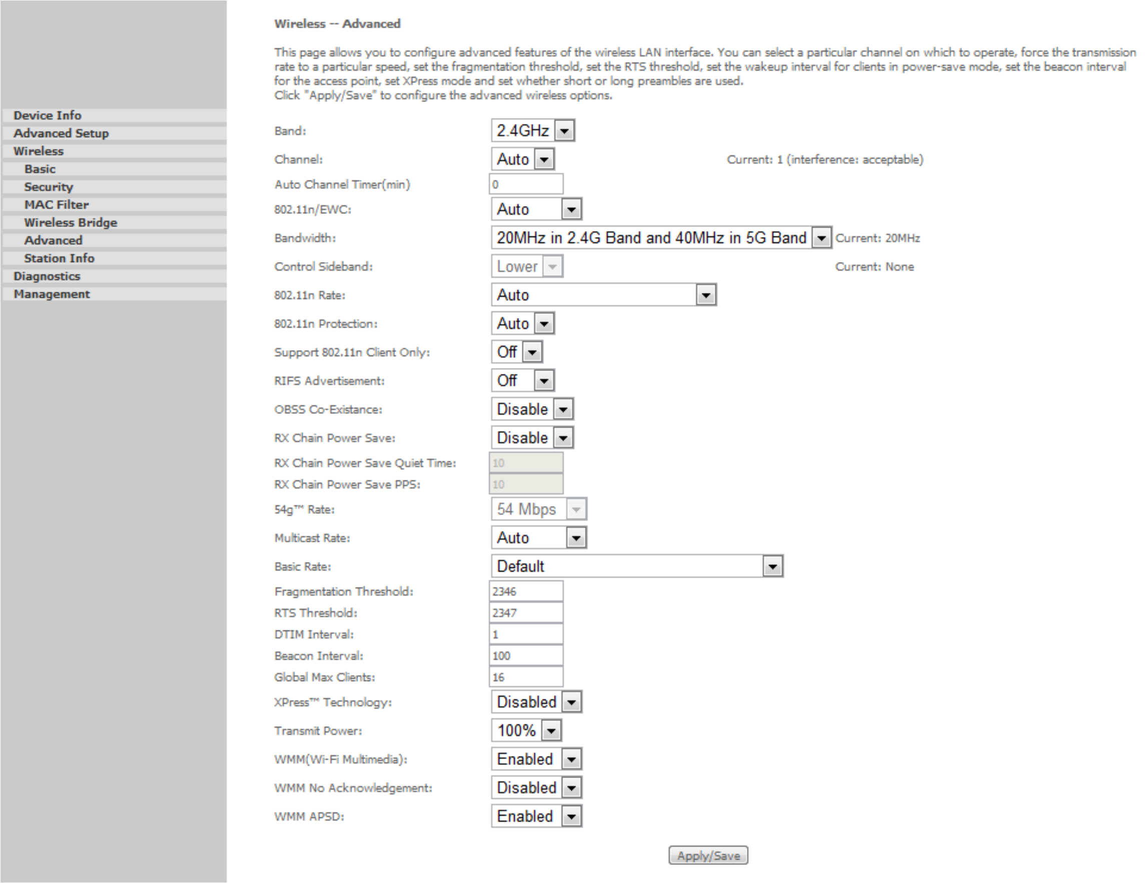
Remote Bridges MAC Address:

ADVANCED

This page allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wake-up interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used.

Click "**Apply/Save**" to configure the advanced wireless options.

FIGURE 5. Wireless Advanced Panel



Wireless -- Advanced

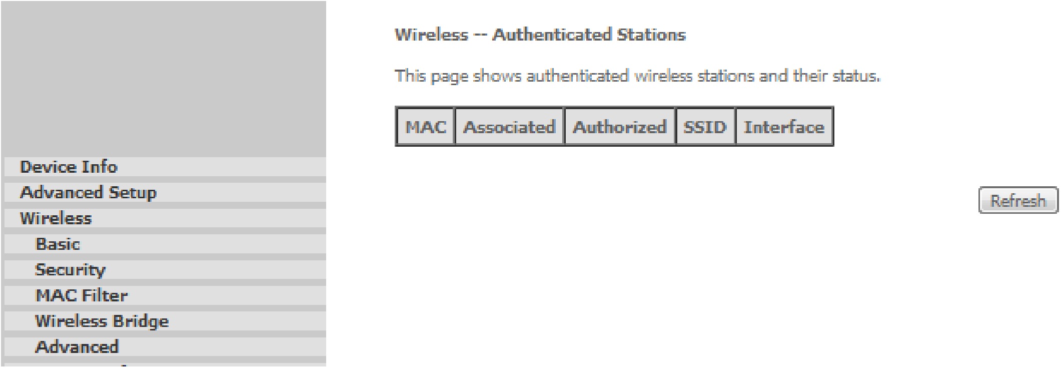
This page allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode,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

Band:	2.4GHz	
Channel:	Auto	Current: 1 (interference: acceptable)
Auto Channel Timer(min)	0	
802.11n/EWC:	Auto	
Bandwidth:	20MHz in 2.4G Band and 40MHz in 5G Band	Current: 20MHz
Control Sideband:	Lower	Current: None
802.11n Rate:	Auto	
802.11n Protection:	Auto	
Support 802.11n Client Only:	Off	
RIFS Advertisement:	Off	
OBSS Co-Existance:	Disable	
RX Chain Power Save:	Disable	
RX Chain Power Save Quiet Time:	10	
RX Chain Power Save PPS:	10	
54g™ Rate:	54 Mbps	
Multicast Rate:	Auto	
Basic Rate:	Default	
Fragmentation Threshold:	2346	
RTS Threshold:	2347	
DTIM Interval:	1	
Beacon Interval:	100	
Global Max Clients:	16	
XPress™ Technology:	Disabled	
Transmit Power:	100%	
WMM(Wi-Fi Multimedia):	Enabled	
WMM No Acknowledgement:	Disabled	
WMM APSD:	Enabled	

STATION INFO

This page shows authenticated wireless stations and their status. Click on the **Refresh** button to refresh the stations' list.

FIGURE 6. **Wireless Station Info Panel**



Wireless -- Authenticated Stations

This page shows authenticated wireless stations and their status.

MAC	Associated	Authorized	SSID	Interface

Diagnostic Section

This chapter will describe the Diagnostics Section accessible from the Home Page of the P.DG A4001N.

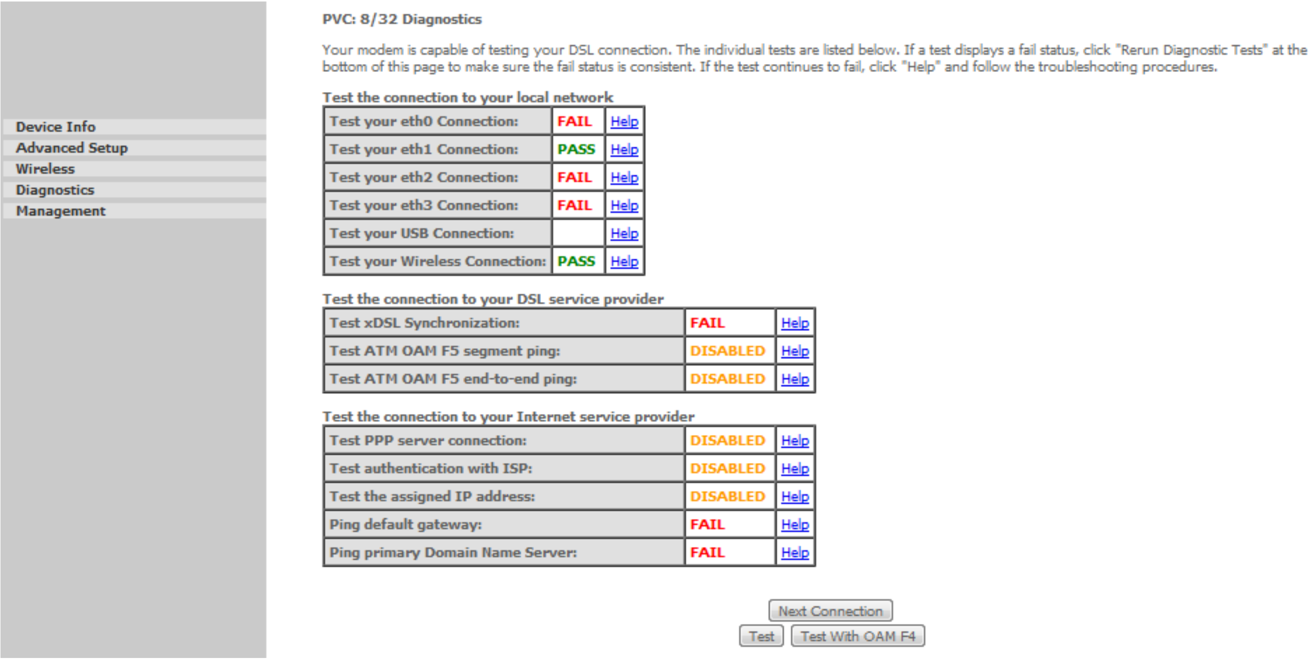
⚠ *Be aware that any configuration change could compromise your connectivity.*

By selecting Diagnostics, the page, shown in Figure 1, is shown. By means of this page it will be possible to run diagnostic tests to check your DSL connection. The results will show test results of three connections:

1. Connection to your local network
2. Connection to your DSL Service Provider
3. Connection to your Internet Service Provider

The "**Test**" button, will allow you to execute the test again, if necessary.

FIGURE 1. **Diagnostic Panel**



PVC: 8/32 Diagnostics

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

Test the connection to your local network

Test your eth0 Connection:	FAIL	Help
Test your eth1 Connection:	PASS	Help
Test your eth2 Connection:	FAIL	Help
Test your eth3 Connection:	FAIL	Help
Test your USB Connection:		Help
Test your Wireless Connection:	PASS	Help

Test the connection to your DSL service provider

Test xDSL Synchronization:	FAIL	Help
Test ATM OAM F5 segment ping:	DISABLED	Help
Test ATM OAM F5 end-to-end ping:	DISABLED	Help

Test the connection to your Internet service provider

Test PPP server connection:	DISABLED	Help
Test authentication with ISP:	DISABLED	Help
Test the assigned IP address:	DISABLED	Help
Ping default gateway:	FAIL	Help
Ping primary Domain Name Server:	FAIL	Help

The "**Next Connection**" button, allows the see the test results for all configured

Management Section

This chapter will describe the Management Section accessible from the Home Page of the P.DG A4001N.

⚠ *Be aware that any configuration change could compromise your connectivity.*

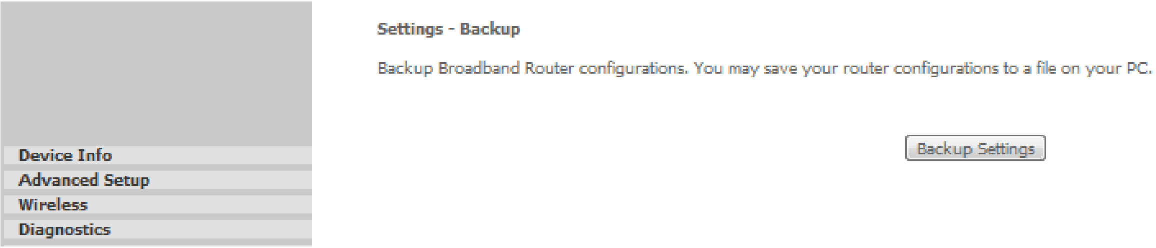
The Management section gives you access to certain setups for the purpose of maintaining the system, including backing up the configurations, viewing system log, maintaining access control, updating software, etc.

SETTINGS >> BACKUP

By selecting "Settings >> Backup", the page, shown in Figure 1, is shown. By means of this page it will be possible to backup DSL router configuration.

A pop-up screen will appear with a prompt to open or save the file to your computer.

FIGURE 1. **Backup Panel**



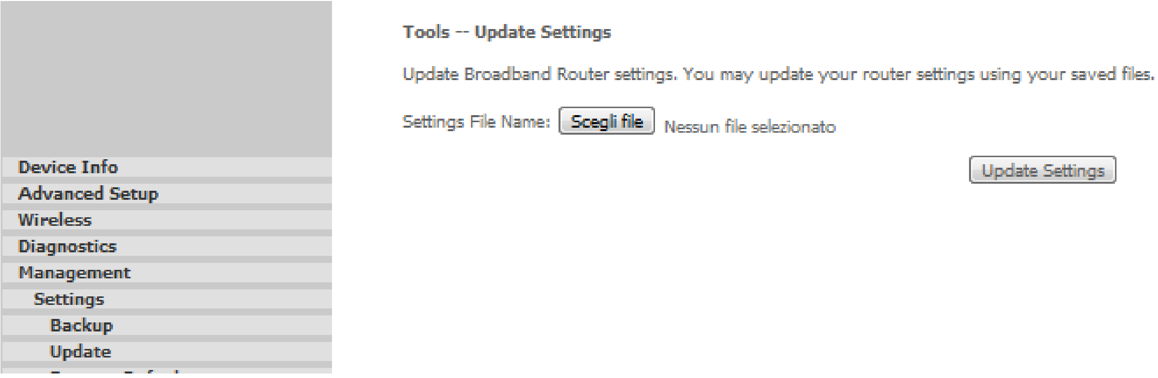
Settings - Backup

Backup Broadband Router configurations. You may save your router configurations to a file on your PC.

SETTINGS >> UPDATE

To update DSL Router settings, do select the “Settings >> Update” item (see Figure 2) and select a previously saved file. Then click on **Update Settings** button.

FIGURE 2. **Update Settings Panel**



Tools -- Update Settings

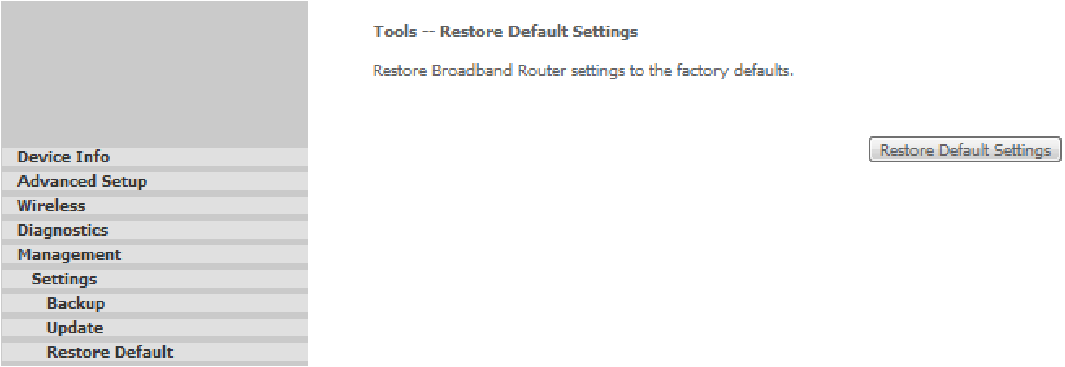
Update Broadband Router settings. You may update your router settings using your saved files.

Settings File Name: Scegli file Nessun file selezionato

SETTINGS >> RESTORE DEFAULT

Settings >> Restore Default item will delete all current settings and restore the router to factory default settings (see Figure 3). Click on the **Restore Default Settings** button. Click on **OK** when the pop-up window appears confirming that you want to restore factory default settings to your router. The router will restore the default settings and reboot.

FIGURE 3. **Restore Default Settings Panel**



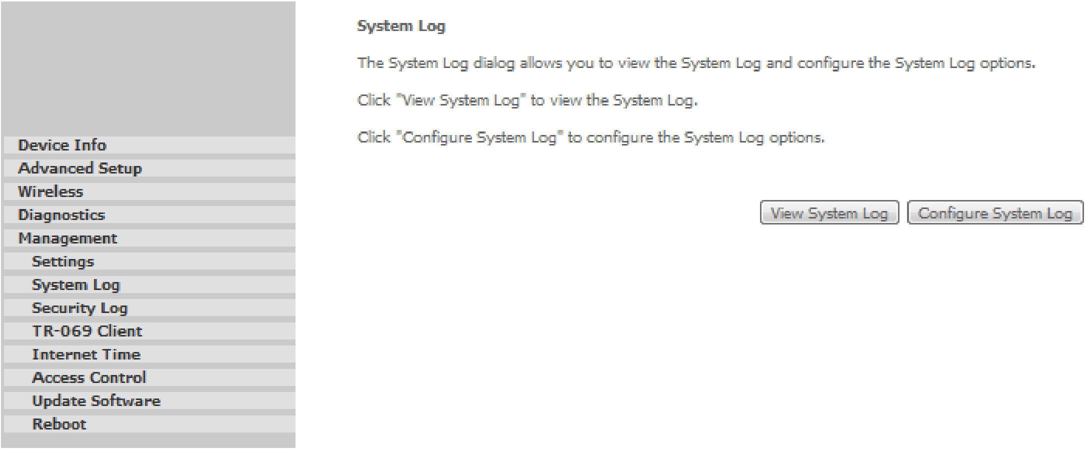
Tools -- Restore Default Settings

Restore Broadband Router settings to the factory defaults.

SYSTEM LOG

The System Log item allows you to view the System Log and configure the System Log options. To view the System Log click on the "**View System Log**" button and check the log file.

FIGURE 4. **System Log Panel**



System Log

The System Log dialog allows you to view the System Log and configure the System Log options.

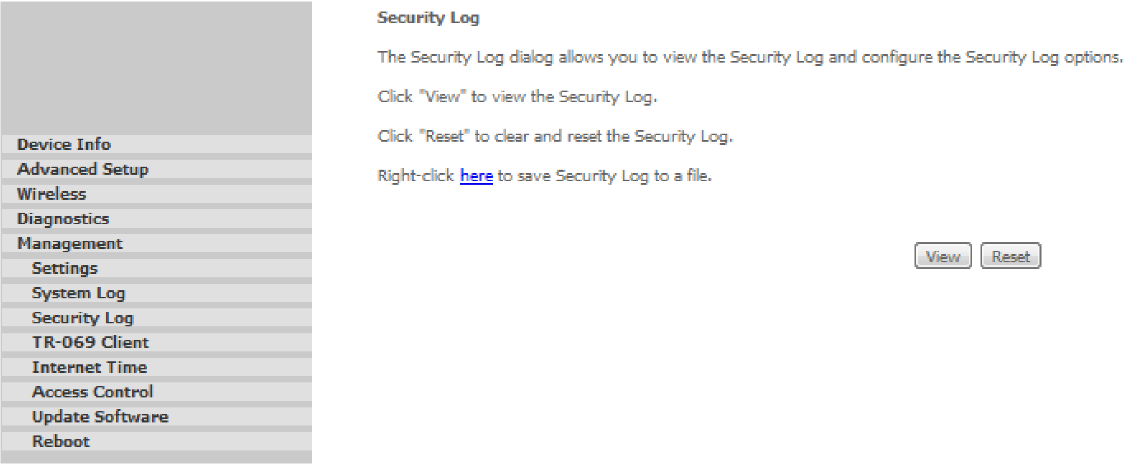
Click "View System Log" to view the System Log.

Click "Configure System Log" to configure the System Log options.

SECURITY LOG

The System The Security Log dialog allows you to view the Security Log and configure the Security Log options. Click "**View**" to view the Security Log. Click "**Reset**" to clear and reset the Security Log.

FIGURE 5. Security Log Panel



Security Log

The Security Log dialog allows you to view the Security Log and configure the Security Log options.

Click "View" to view the Security Log.

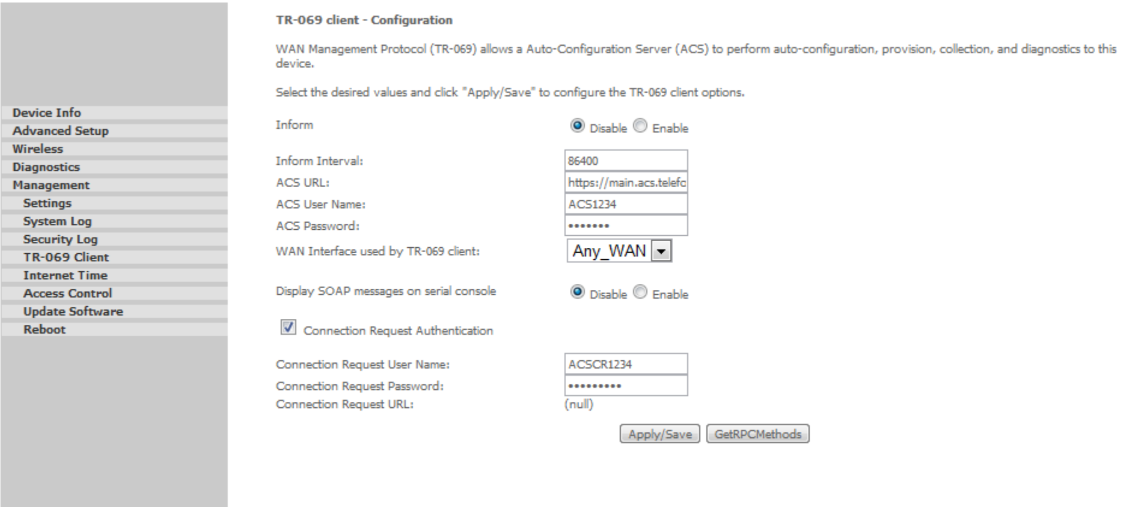
Click "Reset" to clear and reset the Security Log.

Right-click here to save Security Log to a file.

TR-069 CLIENT

The TR-069 Client item allows an Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device. Select the desired values and click **Apply/Save** button to configure the TR-069 client options.

FIGURE 6. TR-069 Client Panel



TR-069 client - Configuration

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

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

Inform ● Disable ○ Enable

Inform Interval: 86400

ACS URL: https://main.acs.telefc

ACS User Name: ACS1234

ACS Password: •••••••

WAN Interface used by TR-069 client: Any_WAN

Display SOAP messages on serial console ● Disable ○ Enable

☑ Connection Request Authentication

Connection Request User Name: ACSCR1234

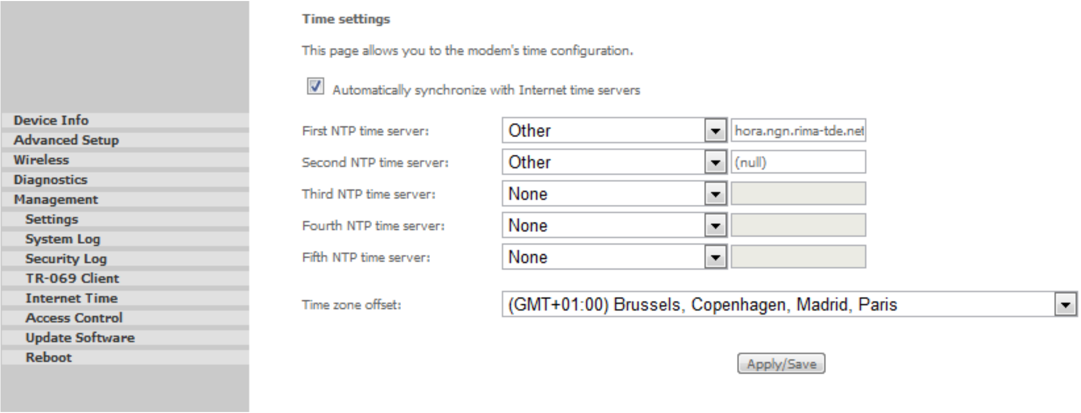
Connection Request Password: •••••••••

Connection Request URL: (null)

INTERNET TIME

The Internet Time item allows the modem's time configuration.

FIGURE 7. Internet Time Panel



Time settings

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

☑ Automatically synchronize with Internet time servers

First NTP time server: Other hora.ngn.rima-tde.net

Second NTP time server: Other (null)

Third NTP time server: None

Fourth NTP time server: None

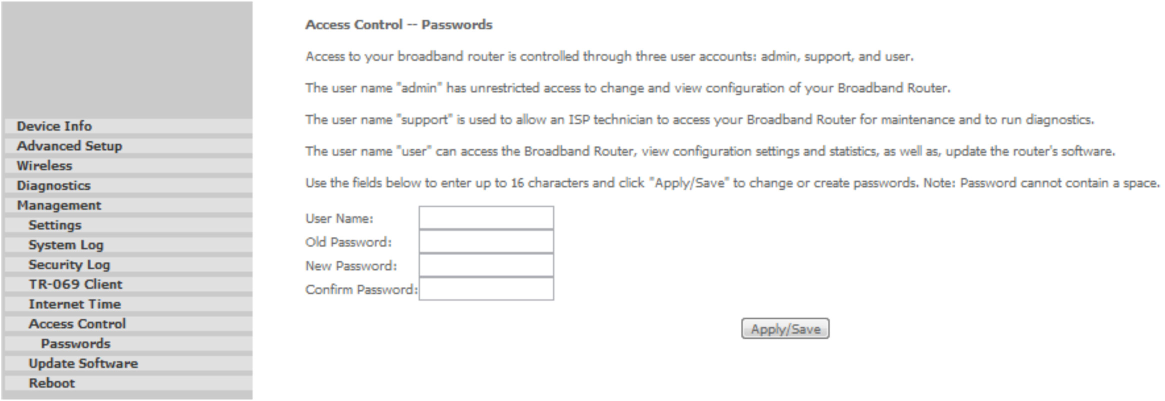
Fifth NTP time server: None

Time zone offset: (GMT+01:00) Brussels, Copenhagen, Madrid, Paris

ACCESS CONTROL >> PASSWORDS

Access the Passwords screen under the Access section to change a password. Select an account and enter the current password and the new password and then click on the **Apply/Save** button.

FIGURE 8. Passwords Panel



Access Control -- Passwords

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

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

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

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

Use the fields below to enter up to 16 characters and click "Apply/Save" to change or create passwords. Note: Password cannot contain a space.

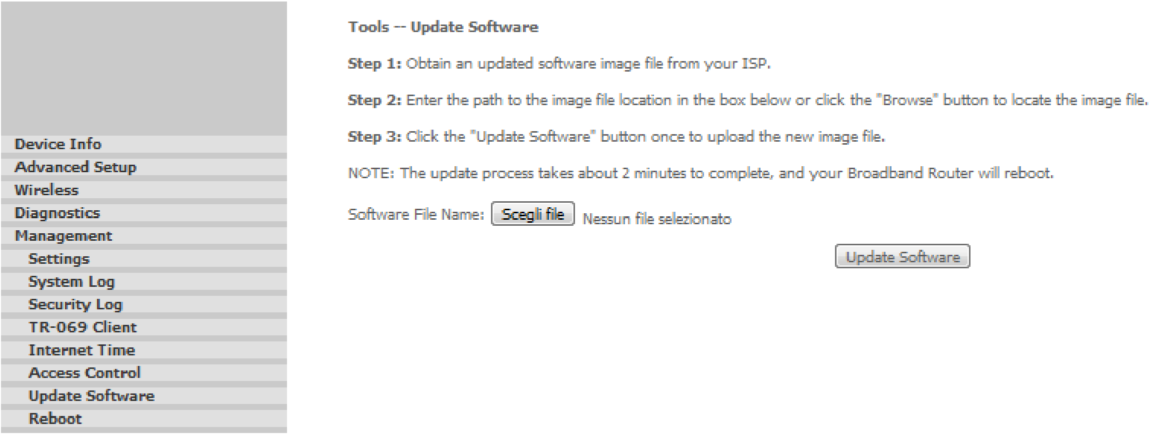
User Name:
Old Password:
New Password:
Confirm Password:

UPDATE

If your ISP releases new software for this router, follow these steps to perform an upgrade.

1. Obtain an updated software image file from your ISP.
2. Enter the path to the image file location or click on the Browse button to locate the image file.
3. Click the Update Software button once to upload the new image file.

FIGURE 9. **Update Panel**



Tools -- Update Software

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

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

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

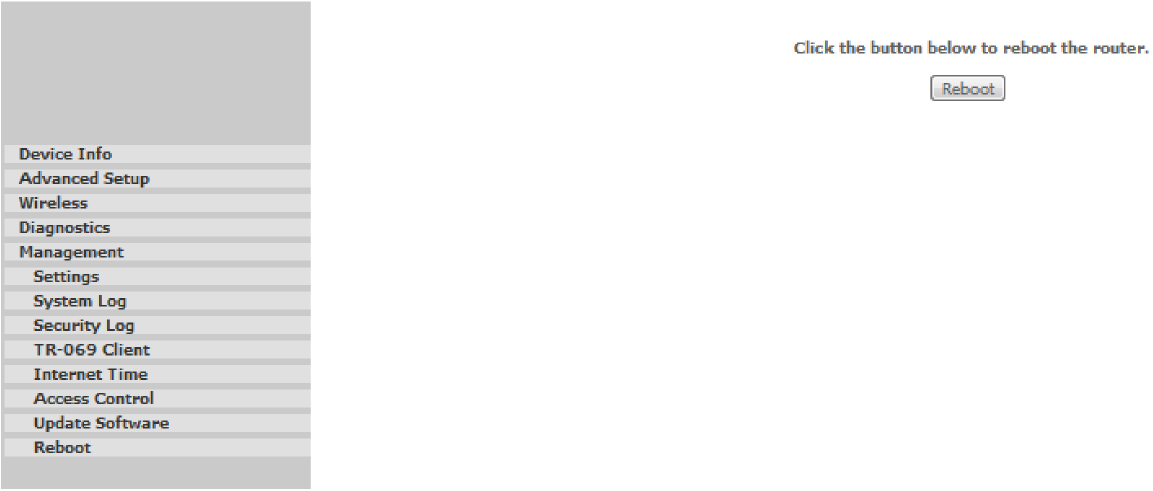
NOTE: The update process takes about 2 minutes to complete, and your Broadband Router will reboot.

Software File Name: Scegli file Nessun file selezionato

REBOOT

Click the **Reboot** button to reboot the router using the web interface. The router will save the current configuration and reboot itself using the new configuration.

FIGURE 10. **Reboot Panel**



Click the button below to reboot the router.

This Page Intentionally Left Blank

IP Addressing

A

The Internet Protocol Suite

The Internet protocol suite consists of a well-defined set of communications protocols and several standard application protocols. Transmission Control Protocol/Internet Protocol (TCP/IP) is probably the most widely known and is a combination of two of the protocols (IP and TCP) working together. TCP/IP is an internationally adopted and supported networking standard that provides connectivity between equipment from many vendors over a wide variety of networking technologies.

Managing the Router over the Network

To manage a device over the network, the Router must be correctly configured with the following IP information:

- An IP address
- A Subnet Mask

IP Addresses and Subnet Masks

Each device on your network must have a unique IP address to operate correctly. An IP address identifies the address of the device to which data is being sent and the address of the destination network. IP addresses have the format n.n.n.x where n is a decimal number between 0 and 255 and x is a number between 1 and 254 inclusive.

However, an IP Address alone is not enough to make your device operate. In addition to the IP address, you need to set a subnet mask. All networks are divided into smaller sub-networks and a subnet mask is a number that enables a device to identify the sub-network to which it is connected.

For your network to work correctly, all devices on the network must have:

- The same sub-network address.
- The same subnet mask.

The only value that will be different is the specific host device number. This value must always be unique.

An example IP address is '192.168.1.8'. However, the size of the network determines the structure of this IP Address. In using the Router, you will probably only encounter two types of IP Address and subnet mask structures.

Type One

In a small network, the IP address of '192.168.1.8' is split into two parts:

- Part one ('192.168.1') identifies the network on which the device resides.
- Part two ('.8') identifies the device within the network.

This type of IP Address operates on a subnet mask of '255.255.255.0'.

Type Two

In larger networks, where there are more devices, the IP address of ‘192.168.1.8’ is, again, split into two parts but is structured differently:

- Part one (‘192.168’) identifies the network on which the device resides.
- Part two (‘.1.8’) identifies the device within the network.

This type of IP Address operates on a subnet mask of ‘255.255.0.0’.

How does a Device Obtain an IP Address and Subnet Mask?

There are three different ways to obtain an IP address and the subnet mask. These are:

- Dynamic Host Configuration Protocol (DHCP) Addressing
- Static Addressing
- Automatic Addressing (Auto-IP Addressing)

DHCP Addressing

The Router contains a DHCP server, which allows computers on your network to obtain an IP address and subnet mask automatically. DHCP assigns a temporary IP address and subnet mask which gets reallocated once you disconnect from the network.

DHCP will work on any client Operating System. Also, using DHCP means that the same IP address and subnet mask will never be duplicated for devices on the network. DHCP is particularly useful for networks with large numbers of users on them.

Static Addressing

You must enter an IP Address and the subnet mask manually on every device. Using a static IP and subnet mask means the address is permanently fixed.

Auto-IP Addressing

Network devices use automatic IP addressing if they are configured to acquire an address using DHCP but are unable to contact a DHCP server. Automatic IP addressing is a scheme where devices allocate themselves an IP address at random from the industry standard subnet of 169.254.x.x (with a subnet mask of 255.255.0.0). If two devices allocate themselves the same address, the conflict is detected and one of the devices allocates itself a new address. Automatic IP addressing support was introduced by Microsoft in the Windows 98 operating system and is also supported in Windows 2000, Windows XP, Windows Vista and Windows 7.

B

Technical Specifications

This section lists the technical specifications for the **Home Station ADSL ADB P.DG A4001N**.

Interfaces/Standard

WAN Interface

N°1 Line port (RJ-11 plug) supporting the following standards:

- *ADSL (G.992.1, G992.2, T1.413, G994.1, G.997.1)*
- *ADSL2 (G.992.3)*
- *ADSL2+ (G992.5)*

Annex A/Annex B are available in different product version

LAN Interface

- *N° 4 10/100BASE-T/TX Ethernet ports (RJ-45 plug), compliant IEEE 802.3, with auto MDIX and auto-negotiation*
- *N°1 USB Host v. 2.0*

Wireless Interface

Wi-Fi access point solution is compliant with:

- *IEEE 802.11b/g/n*
- *WPA/WPA2 (IEEE 802.11i)*
- *WMM (IEEE 802.11e)*
- *N°2 antennas*
- *Wifi/WPS Push Button*

DSL (ATM) Features

- *AAL5 (ITU-T I.363.5)*
- *UBR, VBR-nrt, VBR-rt, CBR traffic classes*
- *Multiple VC/PPP connections*
- *Multi-protocol encapsulation over AAL5, RFCs 2684*
- *Up to 8 PVC*
- *Pre-emptive SAR*
- *Possibility of multiple physical queues (up to 8) per traffic class, with priority-based scheduling support*
- *OAM (ITU-T I.610)*
  - *F4, F5*
  - *Loop-back*
- *Encapsulation modes in ATM stack: LLC SNAP and VC-Mux*

WAN Protocol Encapsulation

- *Bridged/Routed Ethernet over ATM (RFC 2684 / RFC 1483)*
- *PPP over Ethernet (RFC 2516)*
- *PPP over ATM (RFC 2364)*
- *IP over ATM (RFC 1577)*

Routing / Bridging

- *IPv4*
- *RIP v1/v2 and static routing*
- *NAT/NAPT, RFCs 3022, Static NAT/NAPT*
- *DHCP Server/Client/Relay*
- *DNS relay*
- *VPN pass-through*
- *Application Level Gateway (ALGs) modules*
- *Spanning tree protocol*
- *IP Multicasting – IGMP v1, v2, v3*
- *Transparent Bridging (IEEE802.1d)*

QoS

- *IP QoS*
- *Traffic shaping (ATM layer)*
- *Priority-based scheduling (up to 8* queues, max 4 per PVC)*
- *Diffserv (RFC2474, RFC2475) marking and queuing according to connection type, network interface, MAC, IP*
- *Port based QoS*

Security

- *Programmable firewall, Stateful Packet Inspection (SPI) Firewall*
- *IP protocol filtering*

Management

- *Broadband Forum TR-069 CPE Management Protocol:*
  - *Auto- configuration and dynamic service provisioning*
  - *Software/firmware image management*
  - *Status and performance monitoring*
- *TFTP client for remote firmware upgrade*
- *Diagnostics and LOGs*
- *Telnet with CLI*
- *WEB server with Admin/User configuration Pages*

Environmental Specifications

Temperature (ETS 300-019-1-3):

- *Operating: +0° to 40° C*
- *Non Operating: -20° to 65°C*

Relative Humidity (ETS 300-019-1-3):

- *Operating: 10% to 90% non-condensing*
- *Non Operating: 5% to 95% non-condensing*

Power Adapter

- *INPUT: 100/240Vac 50/60 Hz*
- *OUTPUT: 12Vdc 1A*

This Page Intentionally Left Blank

Glossary

C

802.11b

The IEEE specification for wireless Ethernet which allows speeds of up to 11 Mbps. The standard provides for 1, 2, 5.5 and 11 Mbps data rates. The rates will switch automatically depending on range and environment.

802.11g

The IEEE specification for wireless Ethernet which allows speeds of up to 54 Mbps. The standard provides for 6, 9, 12, 18, 24, 36, 48 and 54 Mbps data rates. The rates will switch automatically depending on range and environment.

802.11n

The IEEE specification for wireless Ethernet which allows speeds of up to 300 Mbps. The standard provides for 7,2 up to 300 Mbps data rates. The rates will switch automatically depending on range and environment.

10BASE-T

The IEEE specification for 10 Mbps Ethernet over Category 3, 4 or 5 twisted pair cable.

100BASE-TX

The IEEE specification for 100 Mbps Fast Ethernet over Category 5 twisted-pair cable.

Access Point

An Access Point is a device through which wireless clients connect to other wireless clients and which acts as a bridge between wireless clients and a wired network, such as Ethernet. Wireless clients can be moved anywhere within the coverage area of the access point and still connect with each other. If connected to an Ethernet network, the access point monitors Ethernet traffic and forwards appropriate Ethernet messages to the wireless network, while also monitoring wireless client radio traffic and forwarding wireless client messages to the Ethernet LAN.

Ad Hoc mode

Ad Hoc mode is a configuration supported by most wireless clients. It is used to connect a peer to peer network together without the use of an access point. It offers lower performance than infrastructure mode, which is the mode the router uses. (see also Infrastructure mode.

Auto-negotiation

Some devices in the range support auto-negotiation. Auto-negotiation is where two devices sharing a link, automatically configure to use the best common speed. The order of preference (best first) is: 100BASE-TX full duplex, 100BASE-TX half duplex, 10BASE-T full duplex, and 10BASE-T half duplex. Auto-negotiation is defined in the IEEE 802.3 standard for Ethernet and is an operation that takes place in a few milliseconds.

Bandwidth

The information capacity, measured in bits per second, that a channel can transmit. The bandwidth of Ethernet is 10 Mbps, the bandwidth of Fast Ethernet is 100 Mbps. The bandwidth for 802.11b wireless is 11Mbps.

Category 5 Cables

One of five grades of Twisted Pair (TP) cabling defined by the EIA/TIA-586 standard. Category 5 can be used in Ethernet (10BASE-T) and Fast Ethernet networks (100BASE-TX) and can transmit data up to speeds of 100 Mbps. Category 5 cabling is better to use for network cabling than Category 3, because it supports both Ethernet (10 Mbps) and Fast Ethernet (100 Mbps) speeds.

Channel

Similar to any radio device, the Wireless Cable/DSL router allows you to choose different radio channels in the wireless spectrum. A channel is a particular frequency within the 2.4GHz spectrum within which the Router operates.

Client

The term used to described the desktop PC that is connected to your network.

DHCP

Dynamic Host Configuration Protocol. This protocol automatically assigns an IP address for every computer on your network. Windows 95, Windows 98 and Windows NT 4.0 contain software that assigns IP addresses to workstations on a network. These assignments are made by the DHCP server software that runs on Windows NT Server, and Windows 95 and Windows 98 will call the server to obtain the address. Windows 98 will allocate itself an address if no DHCP server can be found.

DMZ

DMZ (Demilitarized Zone) is an area outside the firewall, to let remote users to have access to items on your network (Web site, FTP download and upload area, etc.).

DNS Server Address

DNS stands for Domain Name System, which allows Internet host computers to have a domain name (such as adbglobal.com) and one or more IP addresses (such as 192.168.10.8). A DNS server keeps a database of host computers and their respective domain names and IP addresses, so that when a domain name is requested (as in typing “adbglobal.com” into your Internet browser), the user is sent to the proper IP address. The DNS server address used by the computers on your home network is the location of the DNS server your ISP has assigned.

DSL

Short for digital subscriber line, but is commonly used in reference to the asymmetric version of this technology (ADSL) that allows data to be sent over existing copper telephone lines at data rates of from 1.5 to 9 Mbps when receiving data (known as the downstream rate) and from 16 to 640 Kbps when sending data (known as the upstream rate). ADSL requires a special ADSL modem. ADSL is growing in popularity as more areas around the world gain access.

DSL modem

DSL stands for digital subscriber line. A DSL modem uses your existing phone lines to send and receive data at high speeds.

Encryption

A method for providing a level of security to wireless data transmissions. The Router uses two levels of encryption; 40/64 bit and 128 bit. 128 bit is a more powerful level of encryption than 40/64 bit.

Ethernet

A LAN specification developed jointly by Xerox, Intel and Digital Equipment Corporation. Ethernet networks use CSMA/CD to transmit packets at a rate of 10 Mbps over a variety of cables.

Ethernet Address

See MAC address.

Fast Ethernet

An Ethernet system that is designed to operate at 100 Mbps.

Firewall

Electronic protection that prevents anyone outside of your network from seeing your files or damaging your computers.

Full Duplex

A system that allows packets to be transmitted and received at the same time and, in effect, doubles the potential throughput of a link.

IEEE

Institute of Electrical and Electronics Engineers. This American organization was founded in 1963 and sets standards for computers and communications.

IETF

Internet Engineering Task Force. An organization responsible for providing engineering solutions for TCP/IP networks. In the network management area, this group is responsible for the development of the SNMP protocol.

IGMP

The Internet Group Management Protocol (IGMP) is an Internet protocol that provides a way for an Internet computer to report its multicast group membership to adjacent routers. Multicasting allows one computer on the Internet to send content to multiple other computers that have identified themselves as interested in receiving the originating computer's content. Multicasting can be used for such applications as updating the address books of mobile computer users in the field, sending out company newsletters to a distribution list, and "broadcasting" high-bandwidth programs of streaming media to an audience that has "tuned in" by setting up a multicast group membership.

Infrastructure mode

Infrastructure mode is the wireless configuration supported by the Router. You will need to ensure all of your clients are set up to use infrastructure mode in order for them to communicate with the Access Point built into your Router. (see also Ad Hoc mode)

IP

Internet Protocol. IP is a layer 3 network protocol that is the standard for sending data through a network. IP is part of the TCP/IP set of protocols that describe the routing of packets to addressed devices. An IP address consists of 32 bits divided into two or three fields: a network number and a host number or a network number, a subnet number, and a host number.

IP Address

Internet Protocol Address. A unique identifier for a device attached to a network using TCP/IP. The address is written as four octets separated with periods (full-stops), and is made up of a network section, an optional subnet section and a host section.

ISP

Internet Service Provider. An ISP is a business that provides connectivity to the Internet for individuals and other businesses or organizations.

LAN

Local Area Network. A network of end stations (such as PCs, printers, servers) and network devices (hubs and switches) that cover a relatively small geographic area (usually not larger than a floor or building). LANs are characterized by high transmission speeds over short distances (up to 1000 metres).

MAC

Media Access Control. A protocol specified by the IEEE for determining which devices have access to a network at any one time.

MAC Address

Media Access Control Address. Also called the hardware or physical address. A layer 2 address associated with a particular network device. Most devices that connect to a LAN have a MAC address assigned to them as they are used to identify other devices in a network. MAC addresses are 6 bytes long.

Mbps

Megabits per second.

MDI/MDIX

In cable wiring, the concept of transmit and receive are from the perspective of the PC, which is wired as a Media Dependant Interface (MDI). In MDI wiring, a PC transmits on pins 1 and 2. At the hub, switch, router, or access point, the perspective is reversed, and the hub receives on pins 1 and 2. This wiring is referred to as Media Dependant Interface - Crossover (MDI-X).

NAT

Network Address Translation. NAT enables all the computers on your network to share one IP address. The NAT capability of the Router allows you to access the Internet from any computer on your home network without having to purchase more IP addresses from your ISP.

Network

A Network is a collection of computers and other computer equipment that are connected for the purpose of exchanging information or sharing resources. Networks vary in size, some are within a single room, others span continents.

Network Interface Card (NIC)

A circuit board installed into a piece of computing equipment, for example, a computer, that enables you to connect it to the network. A NIC is also known as an adapter or adapter card.

Protocol

A set of rules for communication between devices on a network. The rules dictate format, timing, sequencing and error control.

PSTN

Public Switched Telephone Network.

PPPoA

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

PPPoE

Point-to-Point Protocol over Ethernet. Point-to-Point Protocol is a method of data transmission originally created for dial-up connections; PPPoE is for Ethernet connections.

RJ-45

A standard connector used to connect Ethernet networks. The “RJ” stands for “registered jack”.

Router

A device that acts as a central hub by connecting to each computer's network interface card and managing the data traffic between the local network and the Internet.

Server

A computer in a network that is shared by multiple end stations. Servers provide end stations with access to shared network services such as computer files and printer queues.

SSID

Service Set Identifier. Some vendors of wireless products use SSID interchangeably with ESSID.

Subnet Address

An extension of the IP addressing scheme that allows a site to use a single IP network address for multiple physical networks.

Subnet mask

A subnet mask, which may be a part of the TCP/IP information provided by your ISP, is a set of four numbers configured like an IP address. It is used to create IP address numbers used only within a particular network (as opposed to valid IP address numbers recognized by the Internet, which must assigned by InterNIC).

Subnets

A network that is a component of a larger network.

Switch

A device that interconnects several LANs to form a single logical LAN that comprises of several LAN segments. Switches are similar to bridges, in that they connect LANs of a different type; however they connect more LANs than a bridge and are generally more sophisticated.

TCP/IP

Transmission Control Protocol/Internet Protocol. This is the name for two of the most well-known protocols developed for the interconnection of networks. Originally a UNIX standard, TCP/IP is now supported on almost all platforms, and is the protocol of the Internet.

TCP

It relates to the content of the data travelling through a network — ensuring that the information sent arrives in one piece when it reaches its destination. IP relates to the address of the end station to which data is being sent, as well as the address of the destination network.

Traffic

The movement of data packets on a network.

Universal plug and play

Universal plug and play is a system which allows compatible applications to read some of their settings from the Router. This allows them to automatically configure some, or all, of their settings and need less user configuration.

URL Filter

A URL Filter is a feature of a firewall that allows it to stop its clients form browsing inappropriate Web sites.

USB

Universal Serial Bus is a specification to establish communication between devices and a host controller (usually personal computers).

UTP

Unshielded twisted pair is the cable used by 10BASE-T and 100BASE-Tx Ethernet networks.

VCI

VCI - Virtual Channel Identifier. The identifier in the ATM (Asynchronous Transfer Mode) cell header that identifies to which virtual channel the cell belongs.

VPI

VPI - Virtual Path Identifier. The field in the ATM (Asynchronous Transfer Mode) cell header that identifies to which VP (Virtual Path) the cell belongs.

WAN

Wide Area Network. A network that connects computers located in geographically separate areas (for example, different buildings, cities, or countries). The Internet is an example of a wide area network.

WEP

Wired Equivalent Privacy. A shared key encryption mechanism for wireless networking. Encryption strength is 40/64 bit or 128 bit.

Wi-Fi

Wireless Fidelity. This is the certification granted by WECA to products that meet their inter operability criteria. (see also 802.11b, WECA)

Wi-Fi Alliance

The Wi-Fi Alliance is a trade group, owning the trademark to Wi-Fi, aiming at performing the testing, certifying interoperability of products and promoting the technology.

Wireless Client

The term used to describe a desktop or mobile PC that is wirelessly connected to your wireless network

Wireless LAN Service Area

Another term for ESSID (Extended Service Set Identifier)

Wizard

A Windows application that automates a procedure such as installation or configuration.

WLAN

Wireless Local Area Network. A WLAN is a group of computers and devices connected together by wireless in a relatively small area (such as a house or office).

WPA

Wi-Fi Protected Access. A dynamically changing encryption mechanism for wireless networking. Encryption strength is 256 bit.

ADB Broadband S.p.A
Viale Sarca 222
20126 Milano

http://broadband.adbglobal.com