P.DG A4010G

ADSL2+ Wireless Data Gateway

User Manual

Manual Code: HBK 939800040-A1

CONTENTS

Router Configuration 23

Device Info Section 25

Advanced Setup Section 33

Welcome

ABOUT THIS GUIDE

This guide describes how to install and configure the **P.DG A4010G**. 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 and Internet Routers.

NAMING CONVENTION

Throughout this guide, the **P.DG A4010G** is referred to as the "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
	Information note	Information that describes important features or instructions.

TABLE 1. Notice Icons

Icon	Notice Type	Description
	Caution	Information that alerts you to potential loss of data or potential damage to an application, system, or device.
	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 **P.DG A4010G** is designed to provide a cost-effective means of sharing a single broadband Internet connection between several wired and wireless computers. The Router 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 A4010G** is an ADSL2+ router, targeted to residential environments SOHO customers, that provides routed broadband services from a single and modular access point.

The **P.DG A4010G** is the ideal solution for:

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

PACKAGE CONTENTS

Your new **P.DG A4010G** ADSL2+ Router kit contains the related hardware and software. In it you will find:

1. One **P.DG A4010G** unit
2. One Power Supply adapter
3. One USB cable
4. One phone cable
5. One Ethernet cable
6. One Safety leaflet
7. One CD-ROM containing:
   - USB driver

P.DG A4010G

- User Manual
- Quick Installation Guide

TABLE 1. Kit Material

	Quantity	DESCRIPTION
	1	P.DG A4010G
	1	Power Supplier
	1	Ethernet Cable
	1	USB Cable
	1	Phone Cord
	1	CD-ROM
	1	Safety Leaflet

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 several local connectivity technologies on the LAN side:

- Four switched 10/100 Base-TX Ethernet ports
- One Universal Serial Bus 1.1 (USB) connection to a host PC
- A WiFi connection to hosts devices

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

FIGURE 1. Sample Home Network
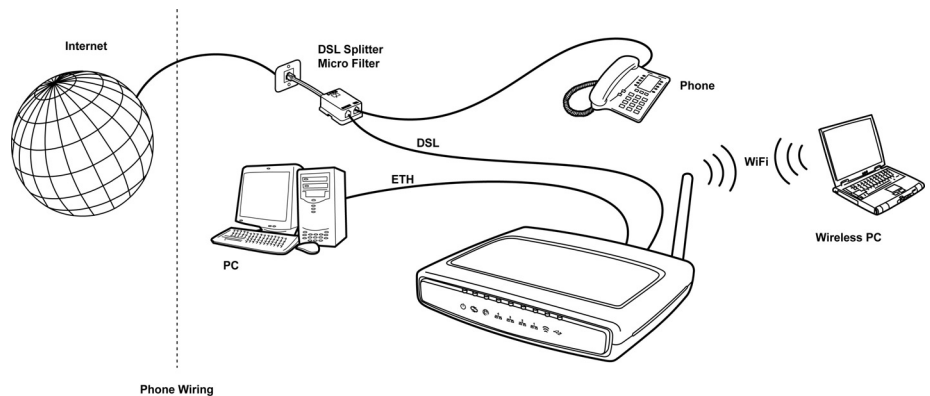
ROUTER ADVANTAGES   The advantages of the **P.DG A4010G** include:

- Shared Internet connection for wired and wireless computers
- No need for a dedicated, "always on" computer serving as your Internet connection
- Cross-platform operation for compatibility with Windows and Macintosh computers (see Technical description for supported platforms)
- Easy-to-use, Web-based setup and configuration
- Centralization of all network address settings (DHCP)

APPLICATIONS   Many advanced networking features are provided by the **P.DG A4010G**:

Wireless and Wired LAN. The Router provides connectivity to 10/100 Mbps devices, and wireless IEEE 802.11b/g compatible devices, making it easy to create a network in small offices or homes.

Internet Access. This device supports Internet access through an ADSL connection. Since many DSL providers use PPPoE or PPPoA to establish communica-

tions with end users, the Router includes built-in clients for these protocols, eliminating the need to install these services on your computer.

Shared IP Address. The Router provides Internet access for up to 253 users via a single shared IP address. Using only one ISP account, multiple users on your network can access the Internet at the same time.

HARDWARE DESCRIPTION

The Router contains an integrated ADSL2+ modem and connects to the Internet or to a remote site using its WAN port. This device can be connected directly to your PC or to a local area network using any of the four Fast Ethernet LAN ports.

Access speed to the Internet depends on your service type. Full-rate ADSL2+ provides up to 24 Mbps downstream and 1 Mbps upstream.

Data passing between devices connected to your local area network can run at up to 100 Mbps over the Fast Ethernet ports and 54 Mbps over the built-in wireless network adapter.

The Router includes an LED display on the front panel for system power and port indications that simplifies installation and network troubleshooting.

MINIMUM SYSTEM AND COMPONENT REQUIREMENTS

Your **P.DG A4010G** requires that the computer(s) and components in your network be configured with at least the following:

- A computer with the Operating Systems that support TCP/IP networking protocols: Windows 98SE, Windows ME, Windows 2000, Windows XP 32bit, Windows Vista 32bit, Windows 7 32 bit or Apple MAC OS 10.x
- An Ethernet 10Mbps or 10/100 Mbps NIC for each computer to be connected to one of the four Ethernet port at the rear of the Router
- A Wireless Ethernet card in case of WiFi access
- An USB 1.1 port
- At least, 60MB of free hard disk space
- At least, 128 MB of RAM
- Supported Browser: Internet Explorer 5.5 or higher

FRONT PANEL

The front panel of the Router contains nine indicator lights (LEDs) that help to describe the state of networking and connection operations.

FIGURE 2. Front Panel LEDs
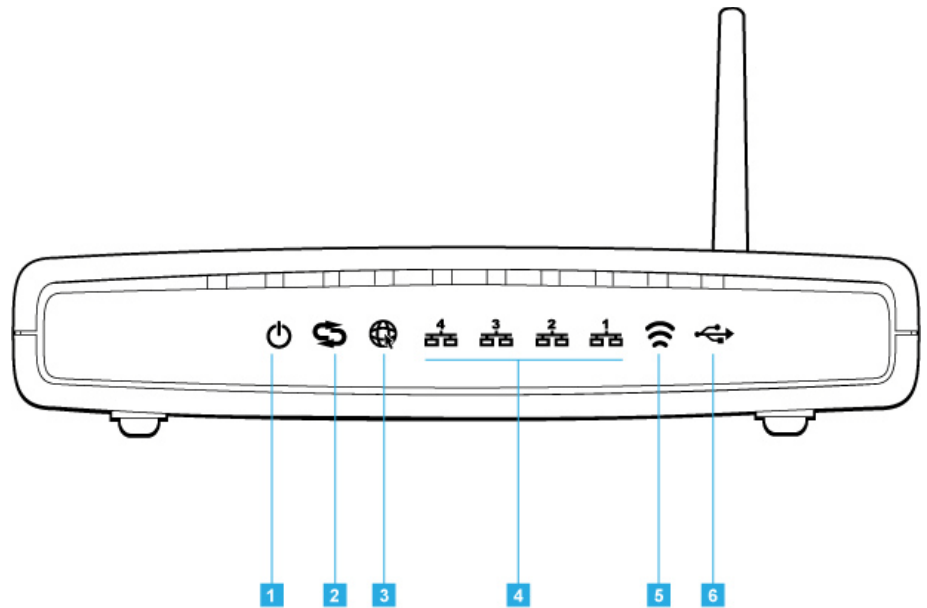
TABLE 2. LED Description

Ref.	LED	LED colour	LED description	
1	*POWER*	*Green*	*On*	*- Power On*
			Off	*- Power Off*
2	*ADSL*	*Green*	*On*	*- DSL connected*
			Blinking	*- No cable connected or no DSL line active*
			Off	*- No Cable connected/No DSL line active*
3	*Internet*	*Green*	*On*	*- WAN IP address available (PPP active)*
			Off	*- Modem power off or WAN IP address not available (PPP failure)*
4	*ETH1 ETH2 ETH3 ETH4*	*Green*	*On*	*- Ethernet Link established*
			Blinking	*- LAN activity present (traffic in either direction)*
			Off	*- No Ethernet Link established*
5	*WLAN*	*Green*	*On*	*- Wireless functionality enabled*
			Blinking	*- Wireless LAN activity present (traffic in either direction)*
			Off	*- Wireless functionality disabled*
6	*USB Device*	*Green*	*On*	*- USB Link Established*
			Blinking	*- USB activity present (traffic in either direction)*
			Off	*- No USB Link established*

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 and one USB 1.1 device port.

⚠️ *Do not force the antenna beyond its mechanical stops. Rotating the antenna further may cause damage.*

FIGURE 3. Rear Panel LEDs
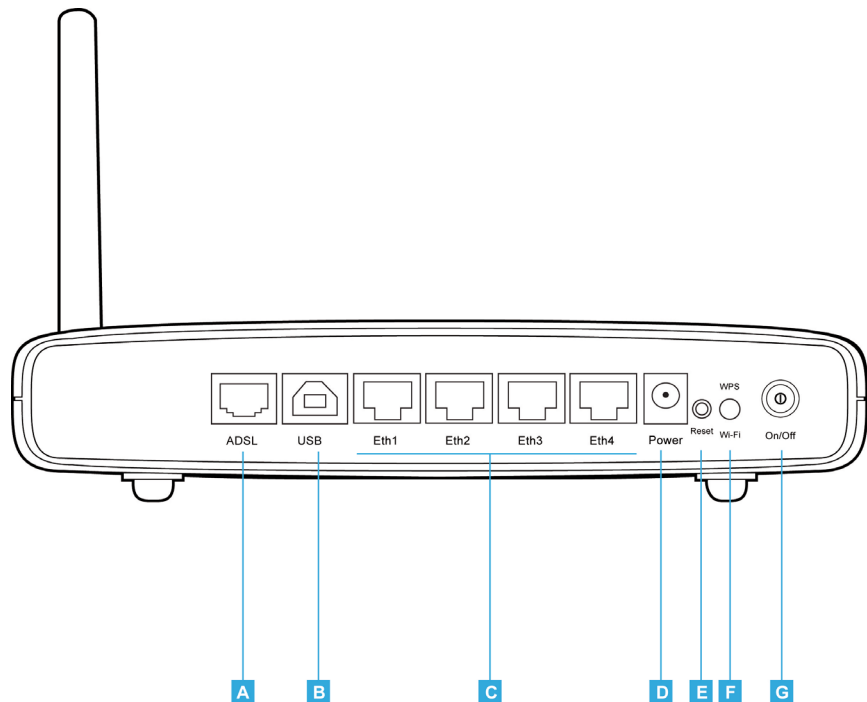
TABLE 3. Port Description

PORT	DESCRIPTION
a	Phone ADSL connector (ADSL2/2+)
b	USB 1.1 port
c	Four Ethernet ports 10/100 Mbps
d	Power Adapter port
e	Reset Configuration to factory default
f	WPS button
g	Power button

Hardware Installation

INTRODUCTION

This chapter will guide you through a basic installation of the Router including:

1. Positioning the **P.DG A4010G**
2. Installing Micro Filters
3. Connecting the Router to your network
4. Setting up your computer for networking with the Router

Please read carefully the Safety Information in the Safety Leaflet.

POSITIONING THE ROUTER

You should place the Router in such a location to ensure that:

- It is located near an electrical outlet and a phone wall socket
- Water or moisture cannot enter the case of the unit
- It is out of direct sunlight and away from sources of heat
- The cabling is away from power lines, fluorescent lighting fixtures, and sources of electrical noise such as radios, transmitters and broadband amplifiers.
- It is centrally located to the wireless computers that will connect to the Router. A suitable location might be on top of a high shelf to optimize wireless connections to computers in both horizontal and vertical directions, allowing wider coverage.

INSTALLING 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 DSL filters please follow these steps:

1. Disconnect the phone cable from the telephone wall socket
2. Insert the phone cable into the DSL filter socket identified with a phone symbol
3. Insert the DSL filter cable into the telephone wall socket

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

FIGURE 1. DSL filter installation
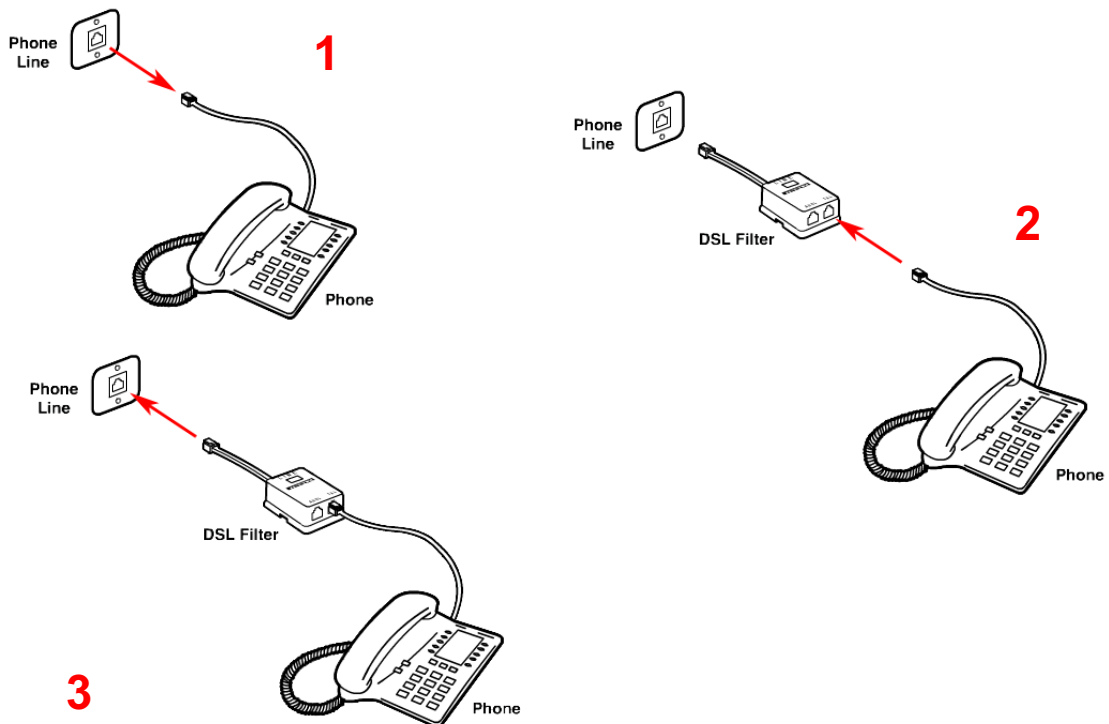
POWERING UP THE ROUTER

To power up the Router:

1. Plug the power adapter into the power adapter socket located on the rear panel of the Router

2. Plug the power adapter into a standard electrical wall socket

3. Press the Power button

4. Wait for the power LED to turn steady green

CONNECTING THE ROUTER The first step to install the router is to physically connect it to the telephone socket and then to connect it to a computer - by means of an Ethernet or an USB connection - to be able to access the Internet

To connect the phone cable:

1. Connect one end of the phone cable into the DSL filter socket identified with a computer symbol

2. Connect the other end of the phone cable into the DSL socket on the rear of the Router

FIGURE 2. **Phone cable connection**
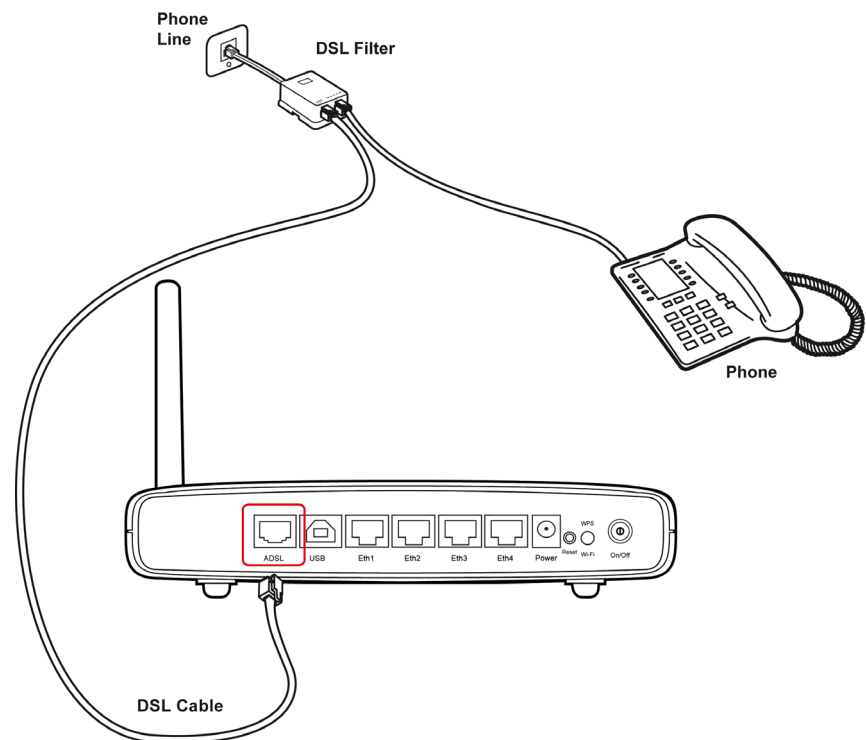
To connect the Ethernet cable:

1. Connect one end of the Ethernet cable into one of the four Ethernet sockets on the rear of the Router

2. Connect the other end of the ethernet cable into the Ethernet plug of your computer

FIGURE 3. **Ethernet cable connection**
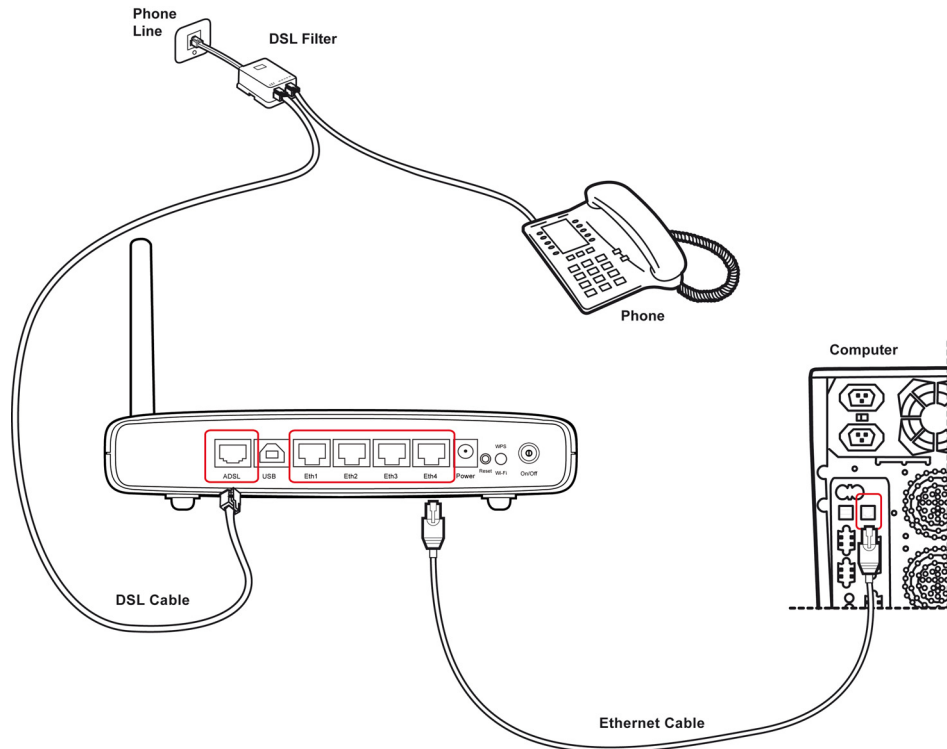
To connect the USB cable, follow the procedure according to your Operating System:

WINDOWS

1. Connect one end of the USB cable into the USB port of your PC

2. Browse till *x:\USB driver* folder (where "*x*" is the CD-ROM drive unit letter); launch the "setup.exe" executable ("x:\USB driver\setup.exe") and follow setup instructions

3. The setup software will invite you, at the right moment, to plug the other end of the USB cable into the USB port on the rear of the Router

MAC OS 10.X

1. Connect one end of the USB cable into the USB port of your PC

Connect the other end of the USB cable into the USB port on the rear of the Router. The Operating System will automatically recognize the device.

FIGURE 4. USB cable connection

HBK 939800040-A1
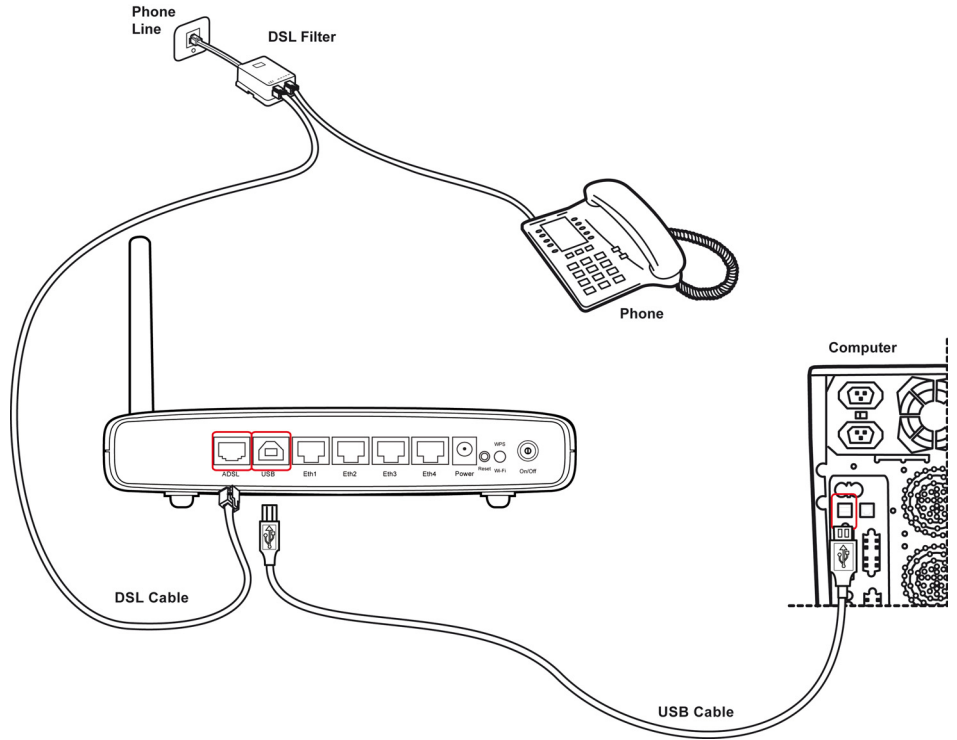
Setting Up Your Computer

The Router 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.

Before installing the P.DG A4010G software please close all applications to avoid any conflict.

INSTALL SOFTWARE

The very first time you set up your computer, we recommend you to use the Smart Setup Configuration Utility if your ISP has provided you with.

This utility offers a guided product tour, a step by step hardware installation guide, a software installation guide and setup depending on your connection choice (USB or ETHERNET) and a driven user registration with DSL Internet connection line check.

Smart Setup Configuration Utility allows, for supported Microsoft Windows Operating Systems, to setup automatically your computer Ethernet settings.

To launch Setup, insert Setup software CD-ROM in CD-ROM unit: if the autoplay function is enabled it will start automatically, otherwise click once on the "*Run...*" item in "*Start*" menu. In the opened panel type "*x:\install.exe*" where *x* is your CD-ROM drive letter.

ETHERNET CONNECTION

In case you already established a connection with your Router a first time and/ or you do need to set up manually a connection to your Router, please follow the instructions described in this chapter. You will be guided to set up an Ethernet connection to the Router. To do so, first 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 it. This connection will require you to enable your computer to receive from the Router its own IP Address automatically: in such a case, the Router acts like the DHCP server in your local network.

ETHERNET CONNECTION >> TCP/IP PROTOCOL INSTALLATION

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

Microsoft Windows 98SE, ME, 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* depending 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 / 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 and Internet -> Network Connections*

2. Select the Network Adapter icon and from the contextual menu, do select the *Properties* item

3. In the *Network* TAB panel, verify that *Internet Protocol (TCP/IPv4)* item is checked; if not, do check it and click on the *OK* button

Apple MAC OS 10.x.

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

ETHERNET CONNECTION >> MS WINDOWS 98SE, ME, 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 1. **Local Area Connection Properties**
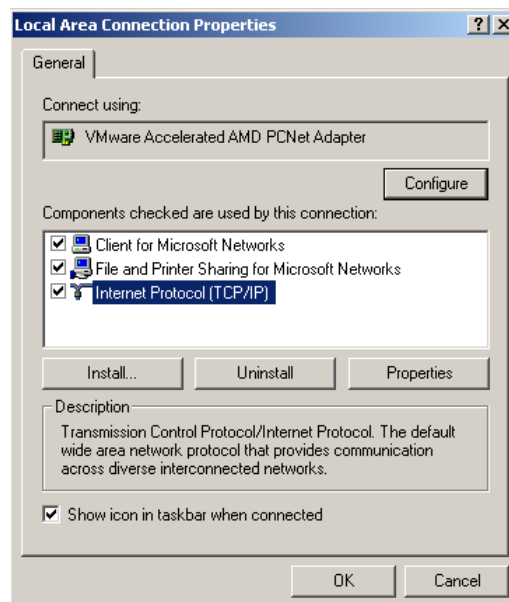
4. Select the *General* TAB panel, then check the *Obtain an IP address auto-matically* and *Obtain DNS server address automatically* radio buttons. Click on *OK* button.

FIGURE 2. **Internet Protocol (TCP/IP) Properties**
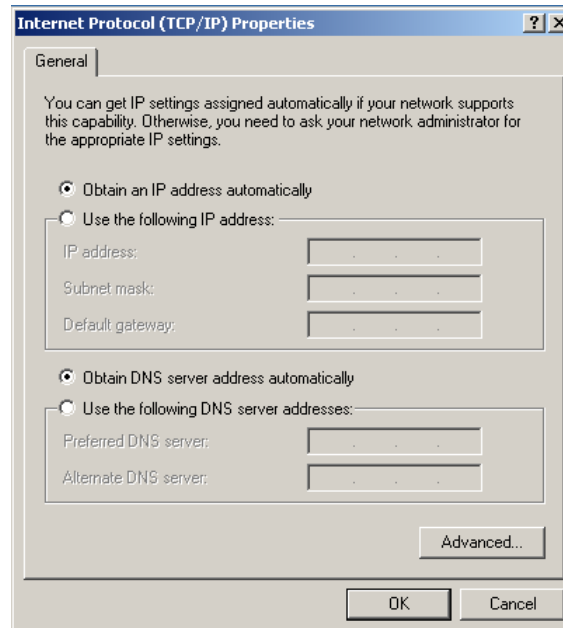
5. A system reboot will be required to make the changes real.

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 *Net-work 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 3. **Local Area Connection Properties**
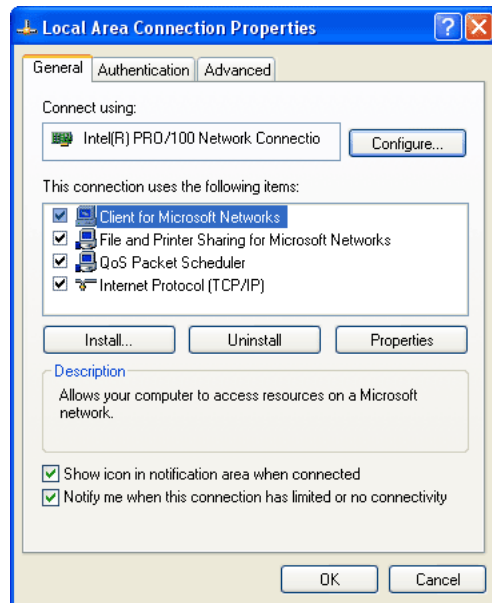
5. In the *General* TAB panel, check the *Obtain an IP address automatically* radio button and the *Obtain DNS server address automatically* radio button. Click on *OK* button.

FIGURE 4. **Internet Protocol (TCP/IP) Properties**
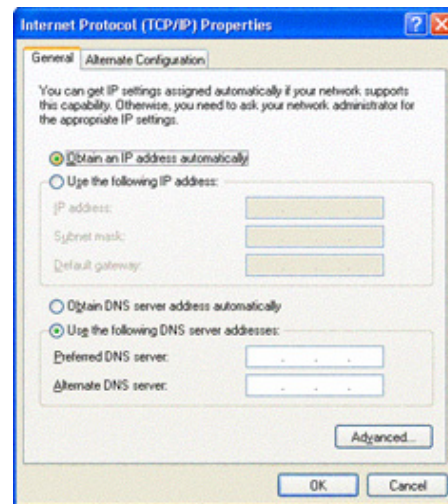
ETHERNET CONNECTION >> MS WINDOWS VISTA / 7

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

1. Select *Start -> Control Panel -> Network and Internet -> Network Connections*.

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 *Network* 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.

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.

FIGURE 5. **Network panel on MAC OS 10.x**
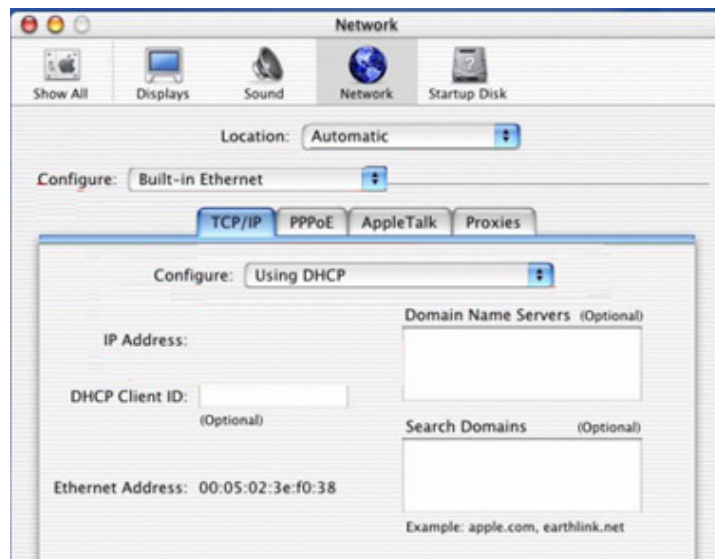
5. Click *Apply Now*.

6. Click on the *Register* button to save the changes in the Control Panel.

7. Enter *http://192.168.1.1/* in the address bar of your browser to open the **P.DG A4010G** Home Page.

USB CONNECTION

To connect your first Computer to the **P.DG A4010G** using USB port, you have to install the Router's USB driver on your computer.

Before connecting the USB Cable to the USB Port of the P.DG A4010G you have to run the setup software and to follow the instructions. Connect the USB Cable only when required from the installation software.

Only one Windows or Macintosh computer can be directly connected to the P.DG A4010G using the USB connection. Additional computers can be added to your network using the Ethernet connections.

USB CONNECTION >> MS WINDOWS

Using Windows 98SE the system could require the Operating System installation CD-ROM.

1. Browse the Setup CD-ROM and install the USB Windows driver selecting the folder x:\driver\windows (where x is the CD-ROM driver unit).
2. Make a double click on setup.exe file to start driver setup procedure.
3. When the message "NOW CONNECT THE USB CABLE" should appear, connect the USB cable from a free USB port of the computer to the **P.DG A4010G** USB port.
4. Enter *http://192.168.1.1/* in the address bar of your browser to open the **P.DG A4010G** Home Page.

USB CONNECTION >> MAC OS 10.X

As MAC OS 10.x will automatically recognize the device, no USB driver installation is required.

1. Enter *http://192.168.1.1/* in the address bar of your browser to open the **P.DG A4010G** Home Page.

WIFI CONNECTION

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 A4010G according to the configuration rules.

It requires a computer with 802.11b/g (WiFi Certified) wireless adapter installed.

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 A4010G.

4. Complete the configuration of the wireless adapter with the same parameters of the P.DG A4010G which are:

   - RF channel; automatically detect
   - WEP encryption enable or disable (default = Disable)
   - WEP key size
   - WEP key used

5. To check the connection, connect to the P.DG A4010G Home Page, entering http://192.168.1.1/ in the address bar of your browser.

Router Configuration

INTRODUCTION

The Router setup program is web based, which means that it is accessed through your web browser.

To access to Router's web server:

1. Launch your web browser on the computer
2. Enter the following URL in the location or address field of your browser: http://192.168.1.1

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 "Reset Configuration to Factory Default" operation should be done to be able to access again to the Router.

Access to DSL router configuration pages is controlled through *admin* user accounts with unrestricted access to change and view configuration of the DSL Router.

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

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 complete menu has the following main items:

1. **Device Info**: it allows to access to Device Information and Statistics.

2. **Advanced Setup**: it allows the access to the advanced configuration pan-
   els.

3. **Wireless**: to configure the Wireless parameters (Security, Filters etc.)

4. **Diagnostics**: a menu to show and run diagnostic test for troubleshooting or
   system behavior analysis.

5. **Management**: it allows to define Router parameters devoted to user
   access, log management, Router's time, Backup Router's configuration,
   etc.

*In order to submit the changes of most of device parameters you have to click the **Save/
Apply** button to save permanently your changes. In some cases, the reboot of the Router is
required.*

FIGURE 1. **Router's Main Page**

Device Info Section

This chapter will describe the **Device Info Section** accessible from the *Home Page* of the **P.DG A4010G** 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
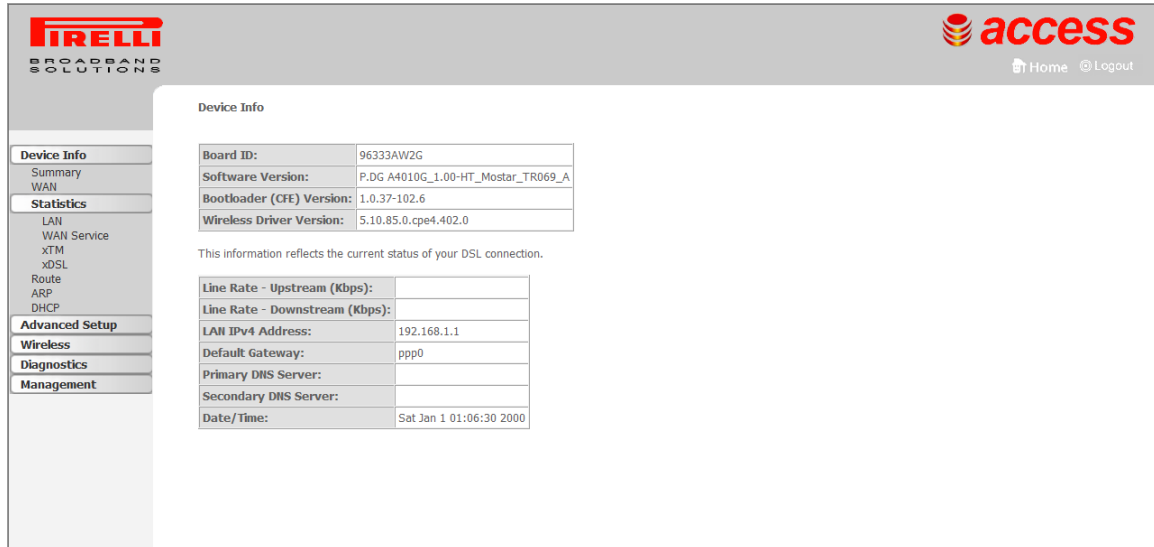
WAN

WAN Info section can be accessed by clicking on **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
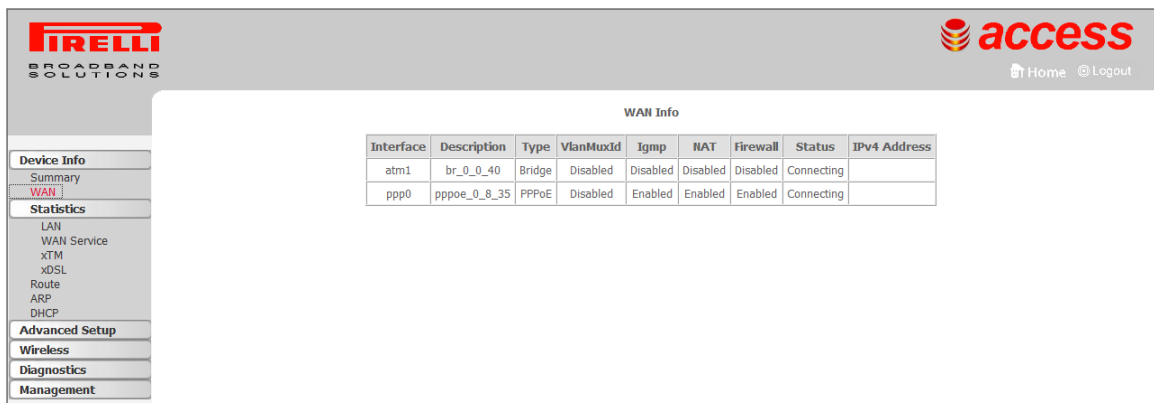
STATISTICS >> LAN

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

FIGURE 3. **Statistics LAN Panel**
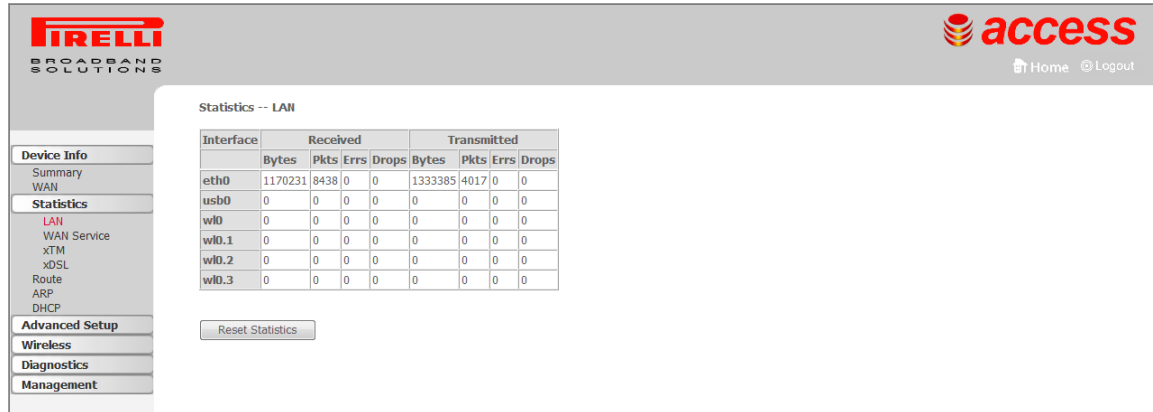
STATISTICS >> WAN SERVICE

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

FIGURE 4. **Statistics WAN Panel**
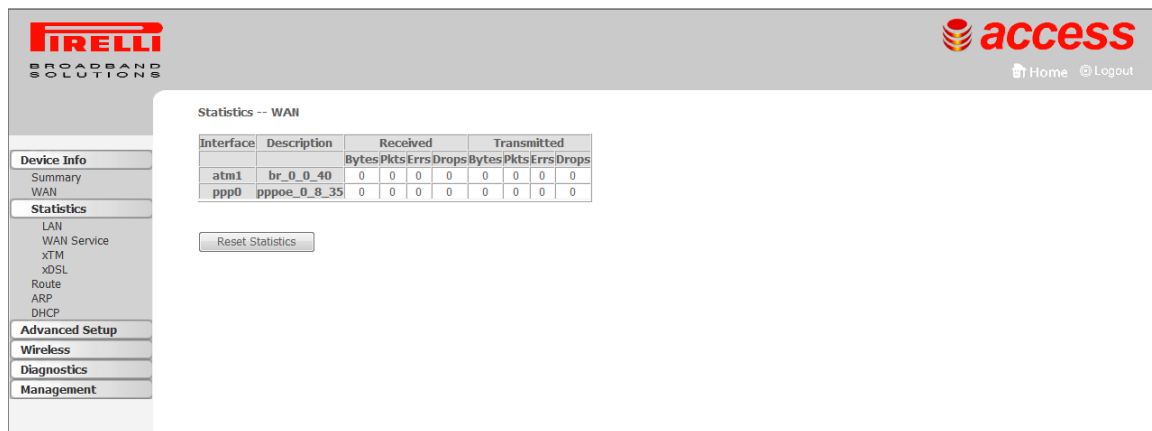
STATISTICS >> XTM

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

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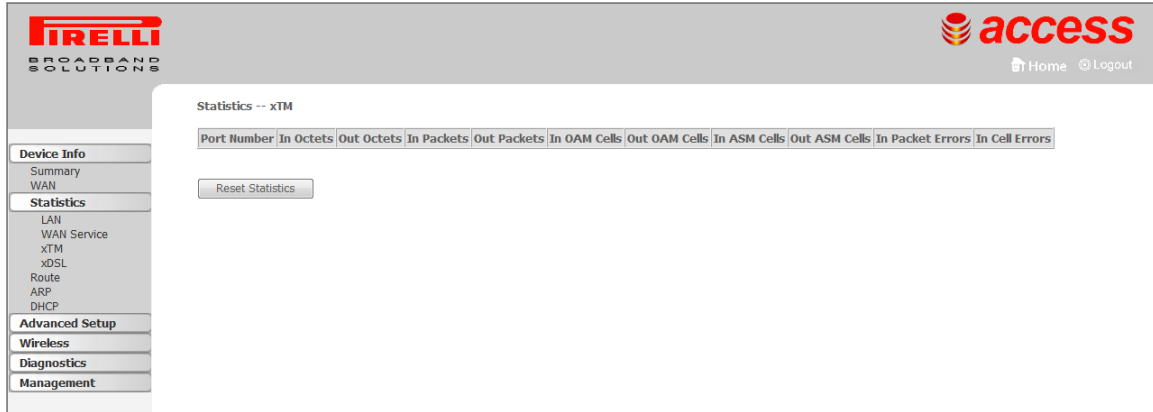
STATISTICS >> XDSL

Access the DSL statistics from the router by clicking on **Statistic >> xDSL**. Information contained in this screen is useful for troubleshooting and diagnostics of connection problems.

The **Reset Statistics** button, will reset statistic ADSL counters.

FIGURE 6. **Statistics >> xDSL Panel**
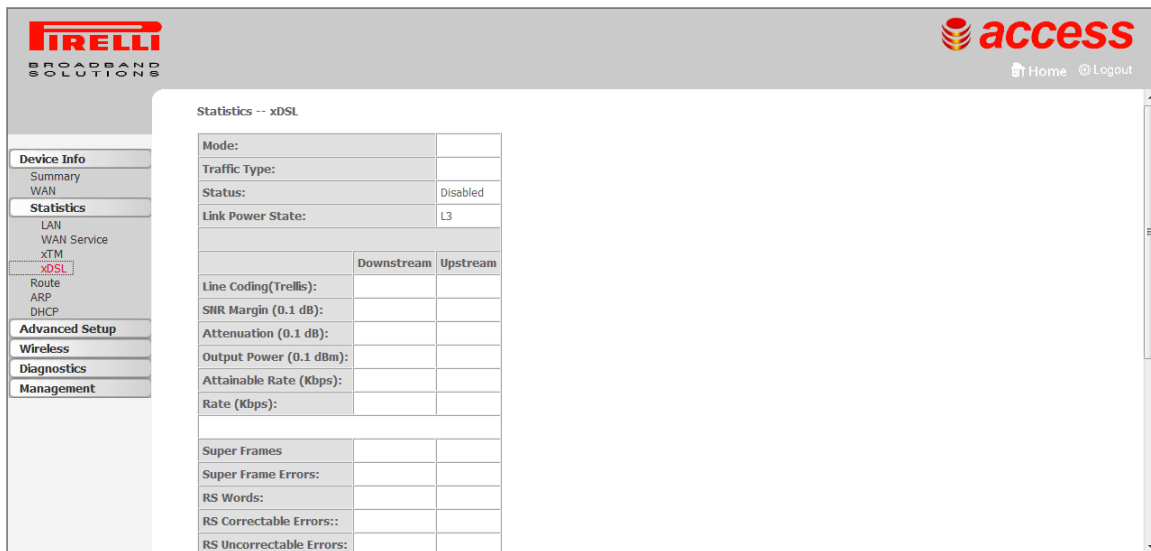
xDSL BER Test. A Bit Error Rate Test (BER Test) is a test that reflects the ratio of error bits to the total number transmitted. If you click on the **xDSL BER Test** button at the bottom of the xDSL Statistics screen, the pop-up window shown in

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

Start phase

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] [Close]

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

[Close]

ROUTE

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

FIGURE 8. **Route Panel**

ARP

Access the Routing Status report from the router by clicking on **Device Info >> ARP**.

ARP (Address Resolution Protocol) maps the IP address to the physical address, labeled HW Address (the MAC address) and helps to identify computers on the LAN.

FIGURE 9. **ARP Panel**
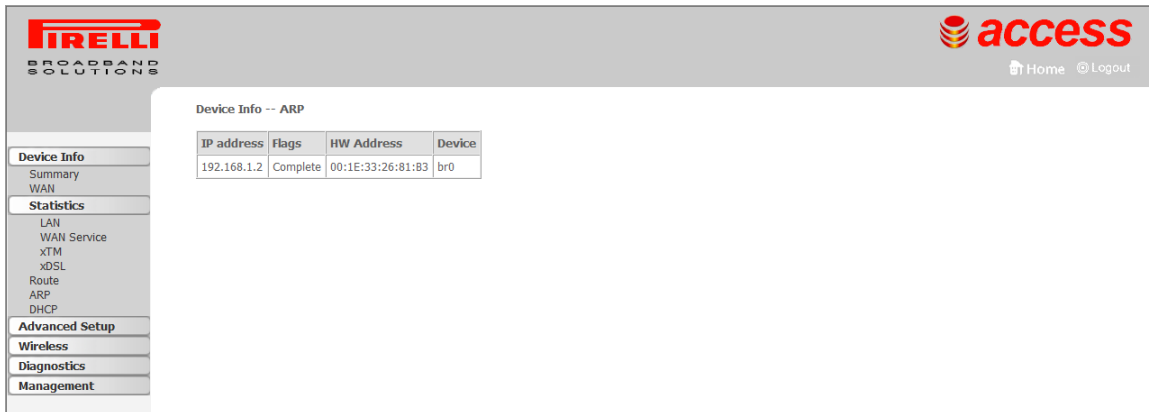
DHCP

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

FIGURE 10. **DHCP Panel**

Advanced
Setup Section

This chapter will describe the **Advanced Setup Section** accessible from the *Home Page* of the **P.DG A4010G**. This section is only

Be aware that any configuration change could compromise your connectivity.

accessible to a user with admin profile and is intended to collect most of the advanced configuration functions.

WAN SERVICE

By selecting **Advanced Setup >> WAN Service**, the page, shown in Figure 1, appears. It is used to configure the WAN settings as provided by your ISP.

FIGURE 1. WAN Service Panel
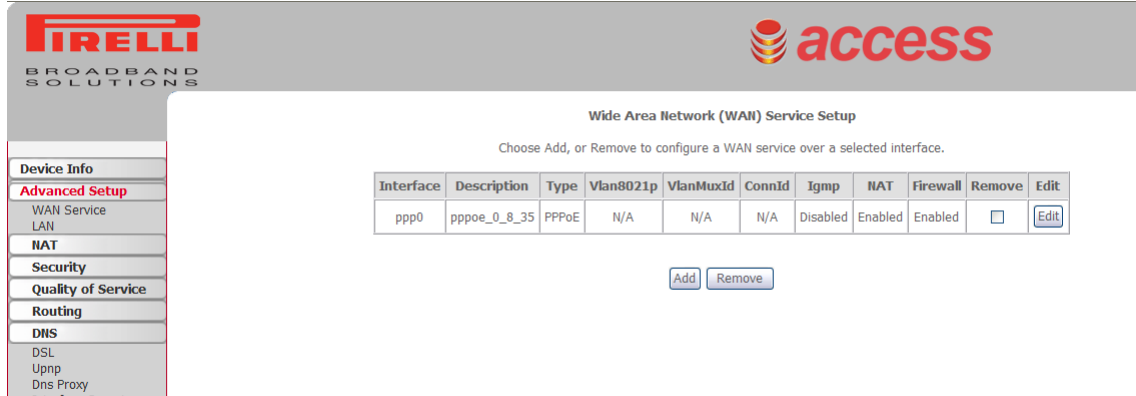
Click on the *Add* button if you want to add a new connection for the WAN interface. The ATM PVC Configuration screen is shown in Figure 2. The ATM PVC Configuration screen allows you to configure an ATM PVC identifier (VPI and VCI) and select a service category.

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

After an Add or Remove job, select the **Save/Reboot** button and the router will reboot thus saving the changes.

FIGURE 2. Adding a WAN interface - Step 1
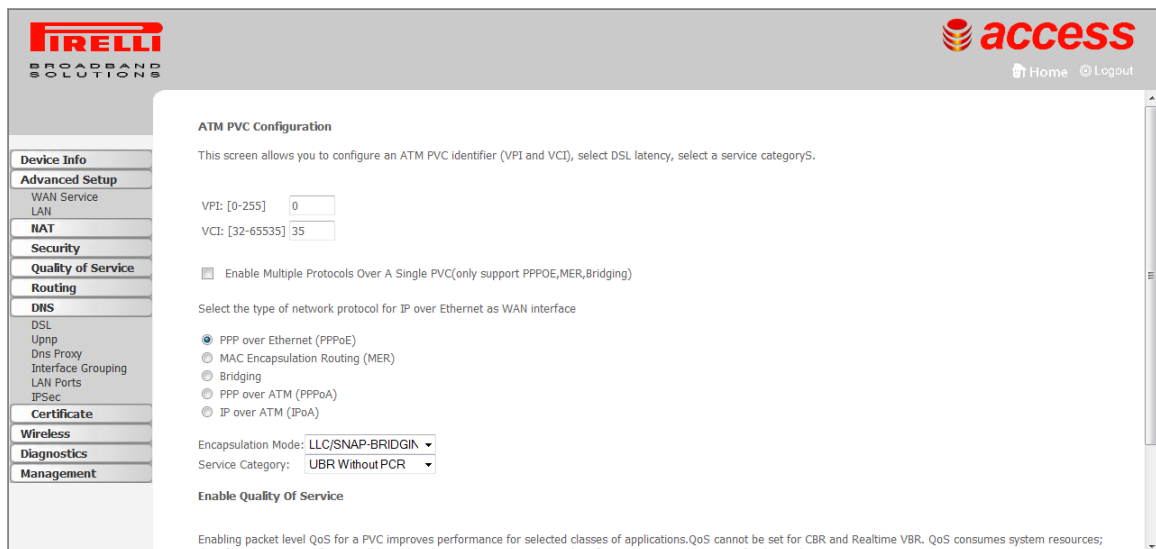
By clicking on the **Add** button, this screen allows you to configure an ATM PVC identifier (VPI and VCI) and select a service category. Find out the values listed in Table 1 from your ISP before you change them.

TABLE 1. ATM PVC Configuration parameters

Parameter	Value	Description
VPI	0-255	Virtual Path Identifier
VCI	32-65535	Virtual Channel Identifier
Service Category	UBR without PCR UBR with PCR CBR Non Realtime VBR Realtime VBR	- **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** (Unspecified Bit Rate with Peak Cell Rate) - **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-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** (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.
Enable Quality of service	true/false	Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. Use Advanced Setup/Quality of Service to assign priorities for the applications.
Peak Cell Rate [cells/sec]	1-255000	Can be set for all Service Categories with the exception of "UBR without PCR" Service Category
Sustainable Cell Rate [cells/s]		Can be set only for Realtime and Non Realtime VBR. Sustainable Cell Rate must be lower than Peak Cell Rate.
Maximum Burst Size: [cells]	1-1000000	Can be set only for Realtime and Non Realtime VBR.

Select the type of network protocol and encapsulation mode over the ATM PVC that your ISP has instructed you to use. Since this example uses a *PPPoE* connection, it is required to enter a PPP username and password. After filling in the page and making any selections your ISP has instructed you to, click on **Next** button to continue.

TABLE 2. Connection Type Configuration Parameters

Parameter	Value	Description
Connection Type	PPP over Ethernet (pppoE)	
	MAC Encapsulation Routing (MER)	
	Bridging	
	PPP over ATM (pppoA)	
	IP over ATM (IPoA)	
Encapsulation Mode	VC/MUX	- VC/MUX encapsulation is available to all connection types
	LLC/ENCAPSULATION	- LLC/ENCAPSULATION is available to PPPoA connection type
	LLC/SNAP-BRIDGING	- LLC/SNAP-BRIDGING is available to PPPoE, MER and Bridging connection types
	LLC/SNAP-ROUTING	- LLC/SNAP-ROUTING is available to IPoA connection type

FIGURE 3. Adding a WAN interface - Step 3 (PPPoE case)
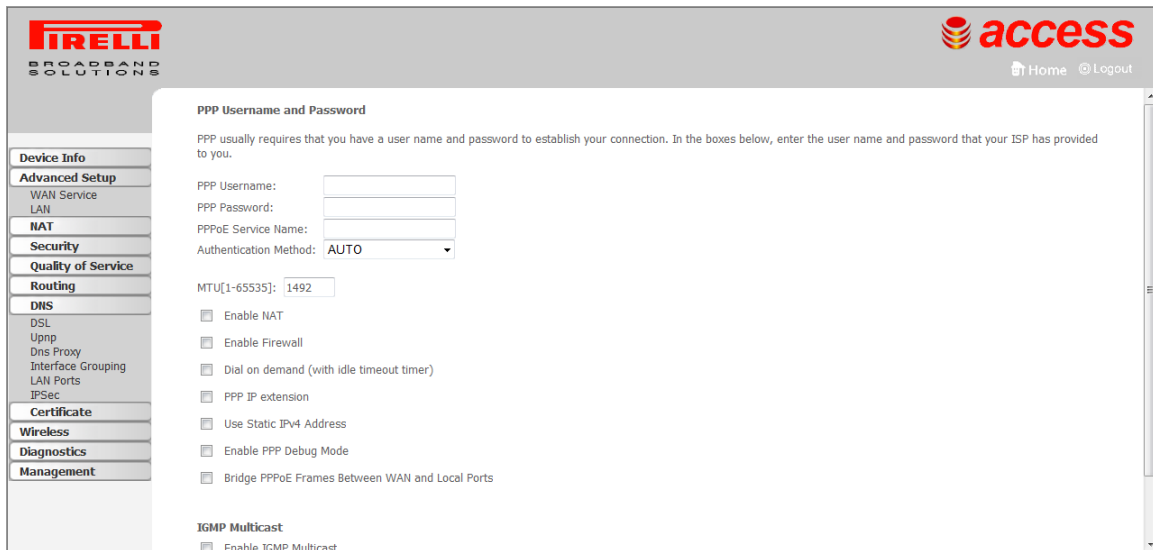
The next screen (Figure 4) allows you to configure NAT either by enabling or disabling it. Other services include IGMP multicast and WAN service. After making your selections, click on **Next** button to go on to the next page.

FIGURE 4. Adding a WAN interface - Step 4
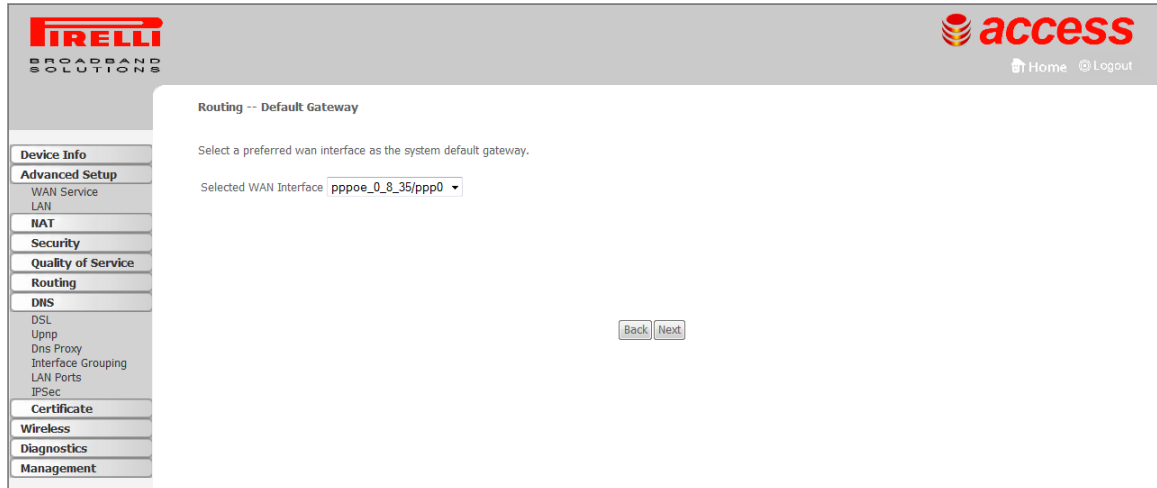
When the settings are complete, the screen in Figure 5 appears showing a **WAN Setup – Summary** screen to display the WAN configurations. Click on **Save** button to save the settings.

FIGURE 5. Adding a WAN interface - Step 5: Summary
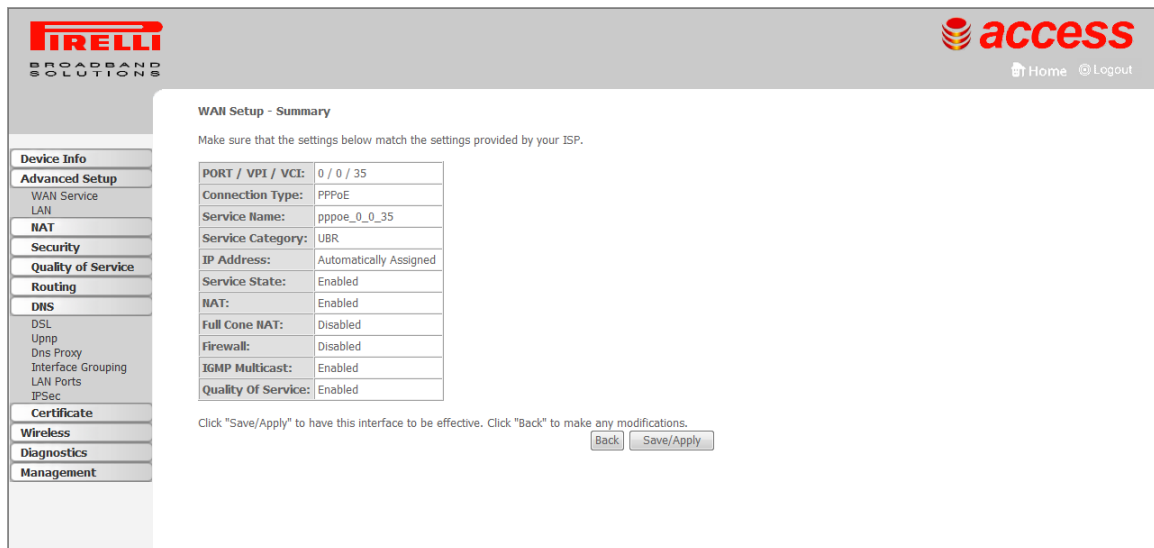
LAN

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. Click on **Next** button to continue.

The **Save** button only saves the LAN configuration data, but does not apply the configurations. Select the **Save/Reboot** button to save the LAN configuration data and reboot the router applying the new configurations.

FIGURE 6. LAN Panel
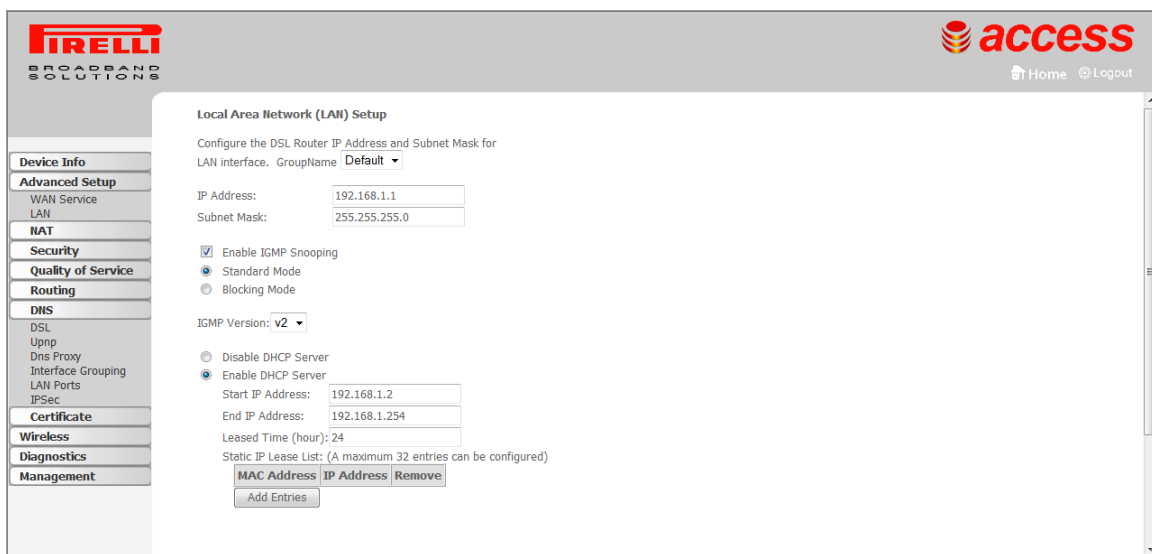
NAT >> ALG

From the ALG menu interface, please select the protocols to be enabled and press the **Save/Apply** button.

FIGURE 7. NAT - ALG Panel
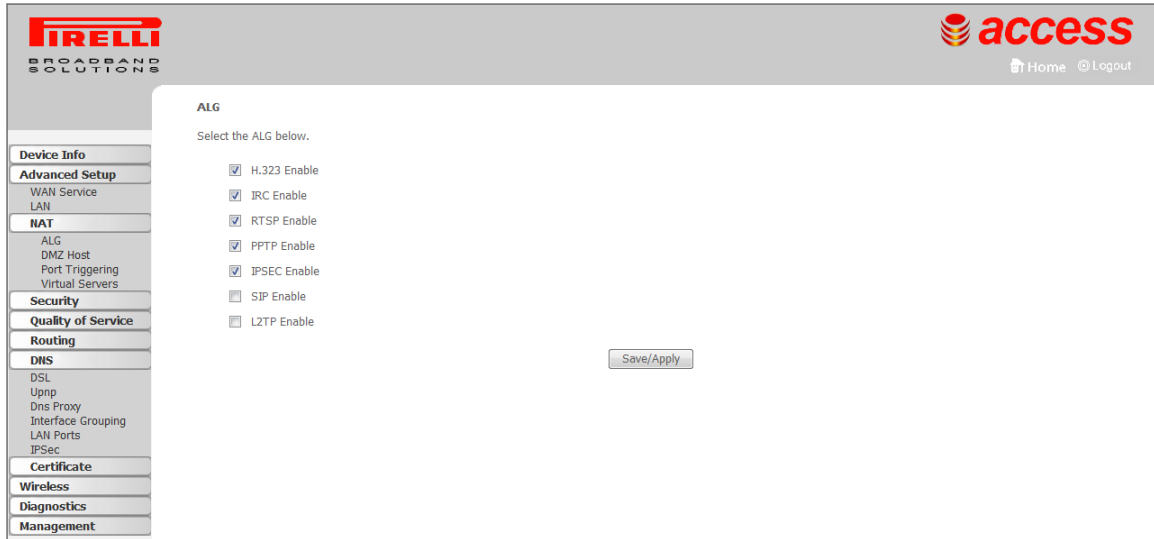
NAT >> DMZ HOST

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 8. NAT - DMZ Host Panel
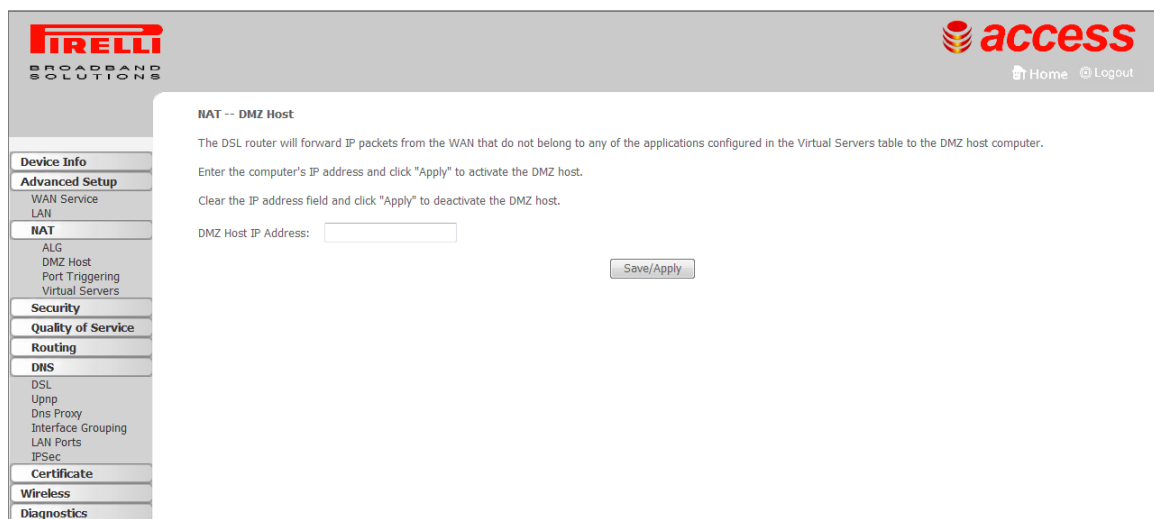
NAT >> PORT TRIGGERING

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'. A maximum of 32 entries can be configured.

FIGURE 9. **NAT - Port Triggering Setup Panel**
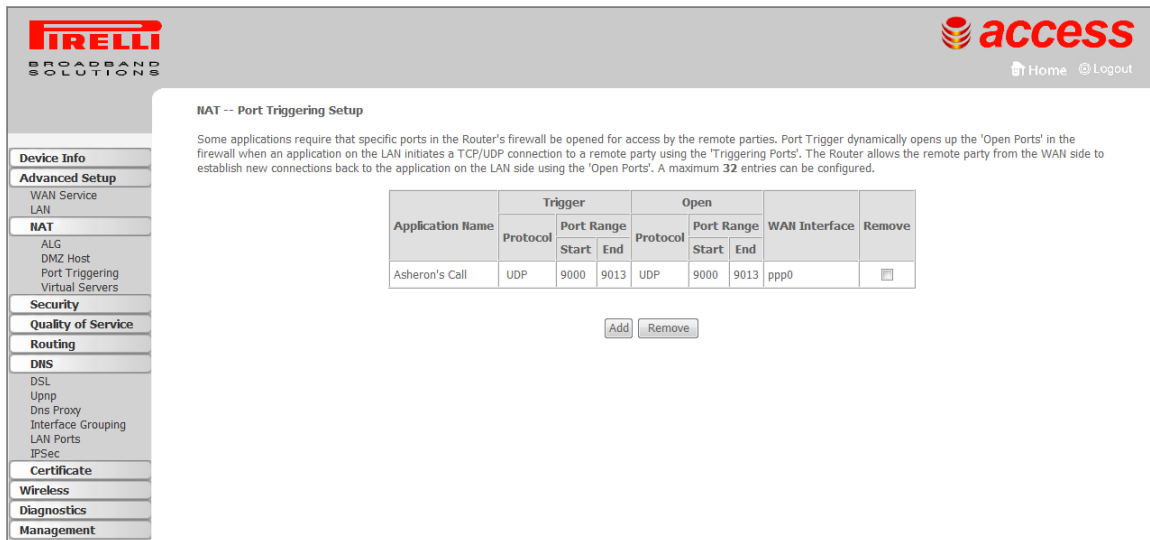
NAT >> VIRTUAL SERVERS

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. A maximum of 32 entries can be configured.

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 10. NAT - Virtual Servers Setup Panel
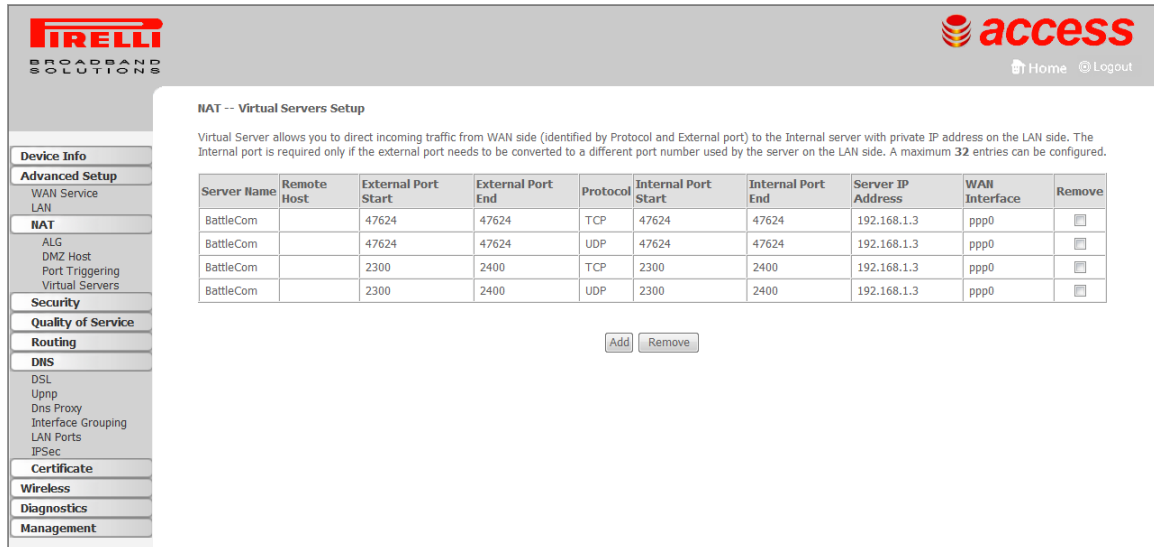
SECURITY >> IP FILTERING >> OUTGOING

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 11. IP Filtering - Outgoing Panel
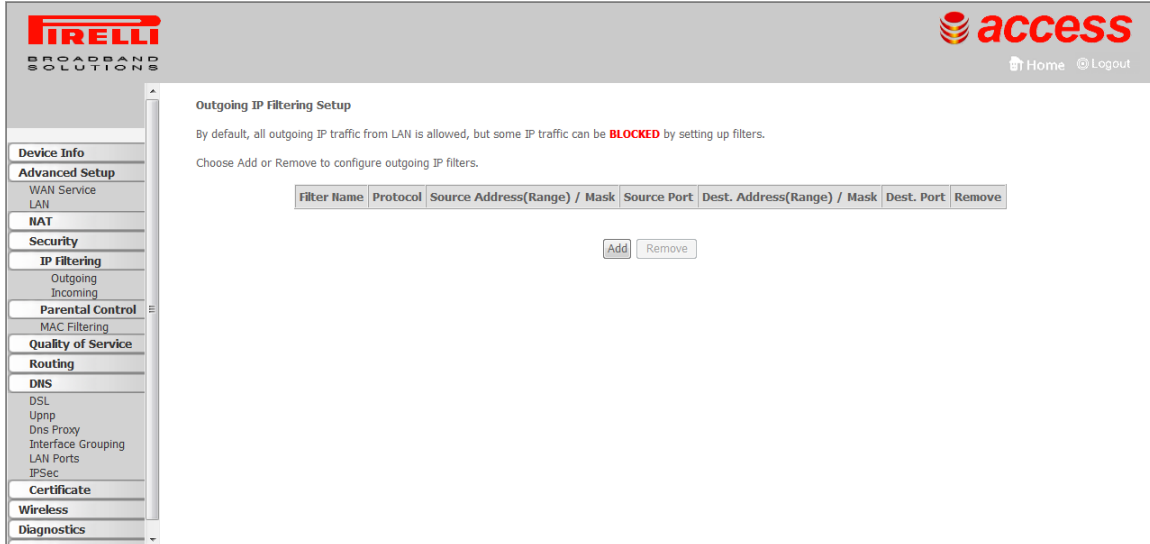
SECURITY >> IP FILTERING >> INCOMING

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 **Save/Apply** to save and activate the filter..

FIGURE 12. IP Filtering - Incoming Panel
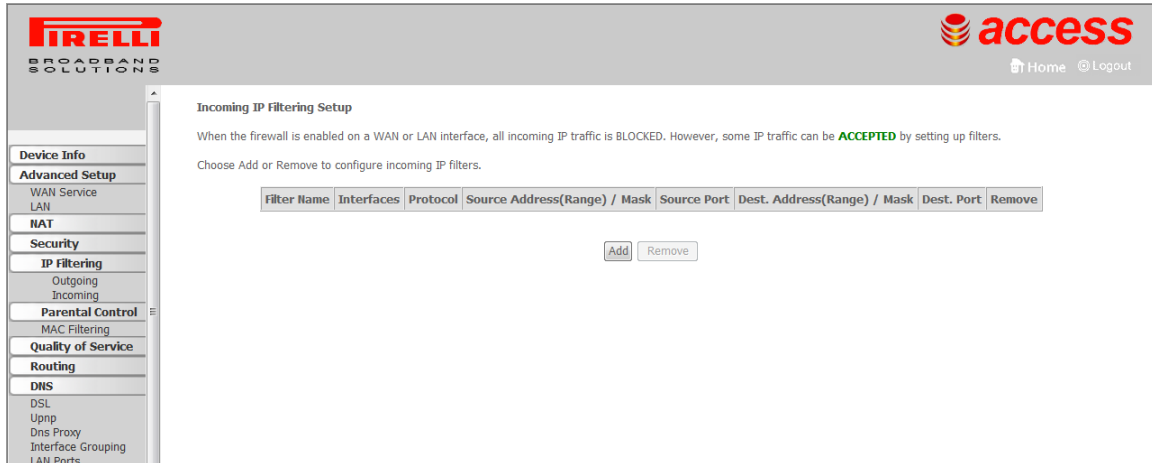
SECURITY >> PARENTAL CONTROL >> TIME RESTRICTION

In the Access Time Restriction panel a maximum 16 entries can be configured.

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

FIGURE 13. Parental Control - Time Restriction Panel
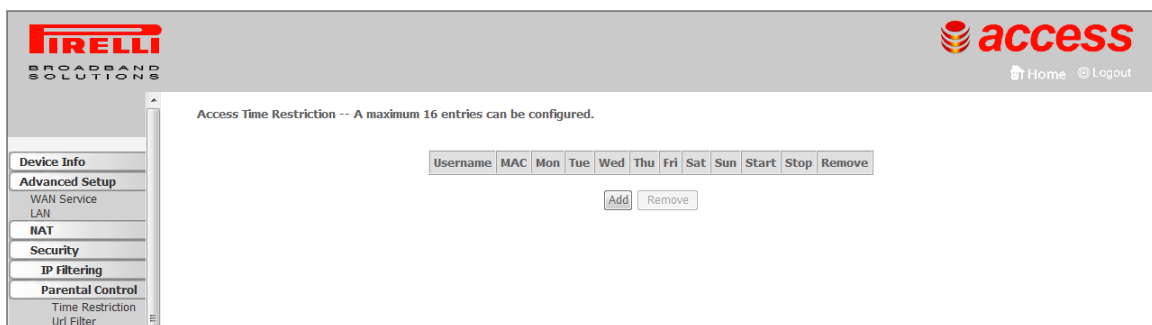
SECURITY >> PARENTAL CONTROL >> URL FILTER

In the URL Filter panel it is necessary to select the list type and then to configure the list entries. Maximum 100 entries can be configured. In the Add Url Filter panel, the URL address and port number must be inserted then clicking "Save/Apply" to add the entry to the URL filter..

FIGURE 14. Parental Control - Url Filter Panel

SECURITY >> MAC FILTERING

MAC Filtering is only effective on ATM PVCs configured in Bridge mode. FOR-WARD 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 15. MAC Filtering Panel
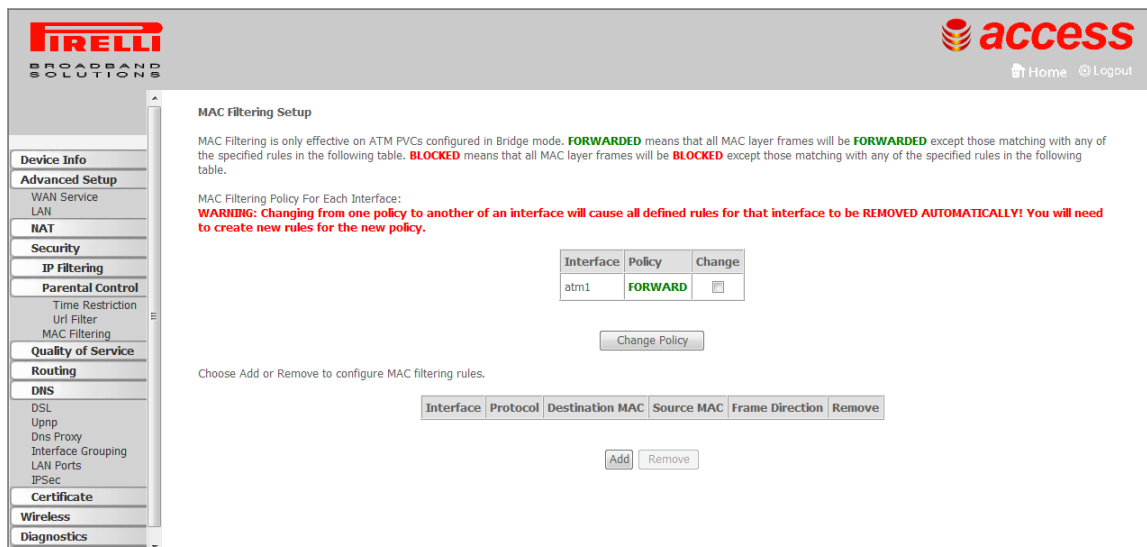
**QUALITY OF SERVICE >>
QUEUE CONFIG**

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

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 16. QoS - Queue Config Panel
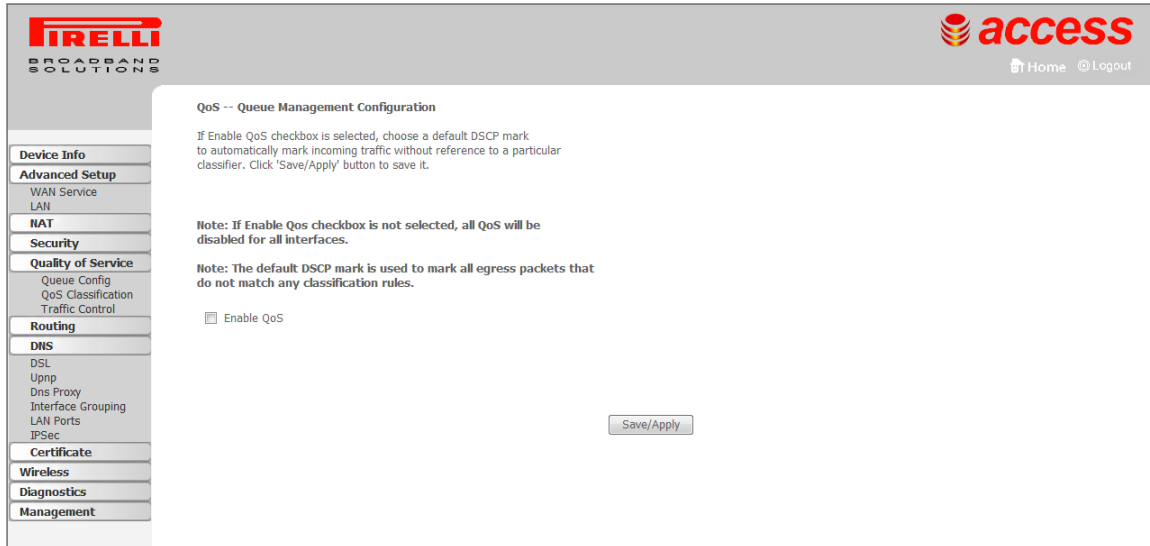
**QUALITY OF SERVICE >>
QOS CLASSIFICATION**

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 17. QoS Classification Panel
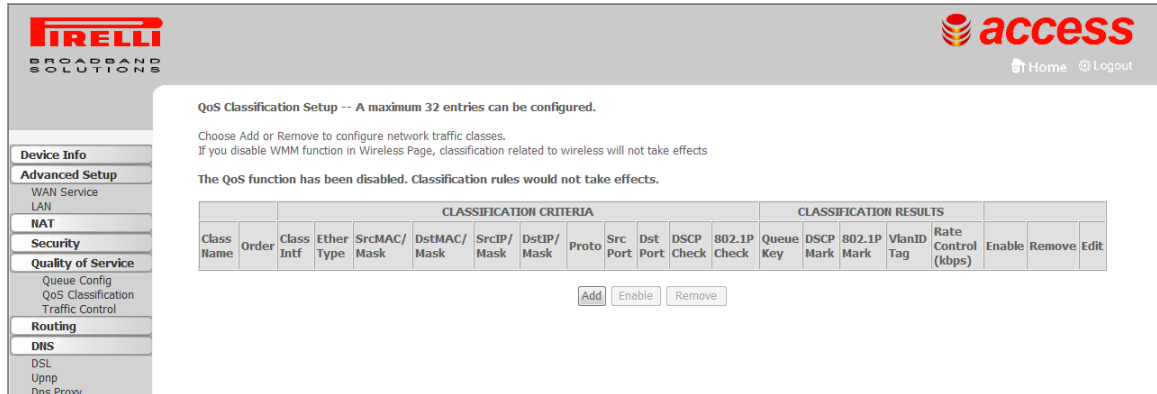
**QUALITY OF SERVICE >> TRAFFIC CONTROL**

In the traffic control panel it is possible to set the bandwidth dedicated to the single interfaces and to define the total amount.

FIGURE 18. QoS - Traffic Control Panel
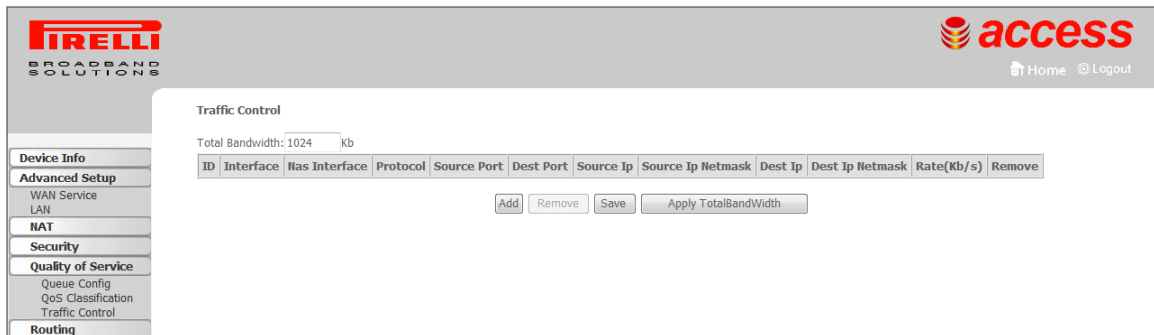
ROUTING >> DEFAULT GATEWAY

If *more than one WAN interface exists,* the router will need to define a preferred default gateway assignment. Click **Save/Apply** 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 19. Default Gateway Panel
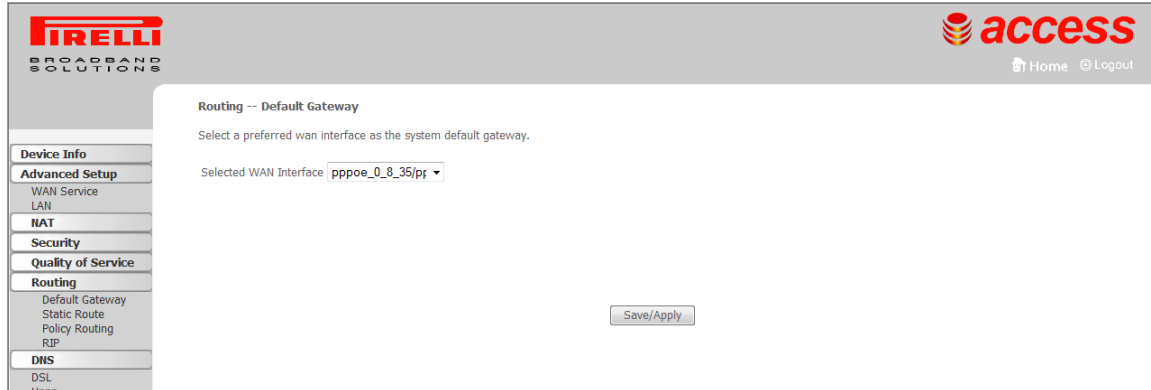
ROUTING >> STATIC ROUTE   The Static Route screen can be used to add a routing table (a maximum of 32 entries can be configured). Click on **Add** button to add a static route and, at the end of parameters' configuration, press the **Save/Apply** button. The **Remove** button, upon a route selection, 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 20. **Static Route Panel**

FIGURE 21. Add - Static Route Panel
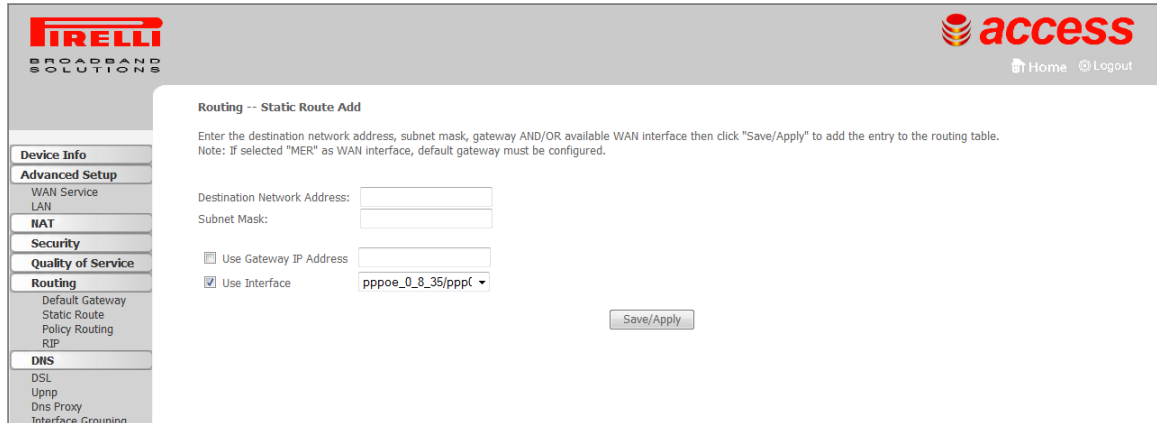
ROUTING >> POLICY ROUTING

In the Policy Routing Setting panel a maximum 8 entries can be configured.

In the Policy Routing Setup panenl, enter the policy name, policies, and WAN interface then click "Save/Apply" to add the entry to the policy routing table.

Note: If selected "MER" as WAN interface, default gateway must be configured.

FIGURE 22. Policy Routing Panel

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 'Save/Apply' 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 23. RIP Panel
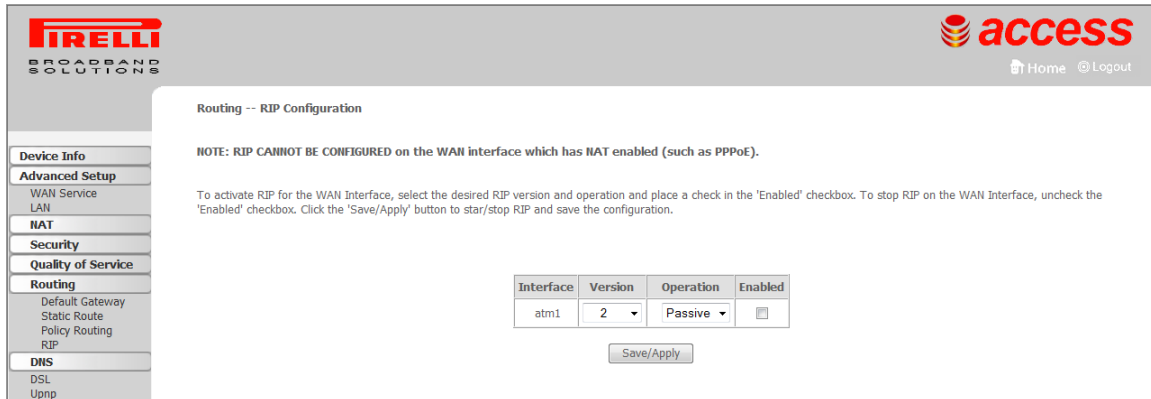
DNS >> DNS SERVER

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 24. DNS Server Panel
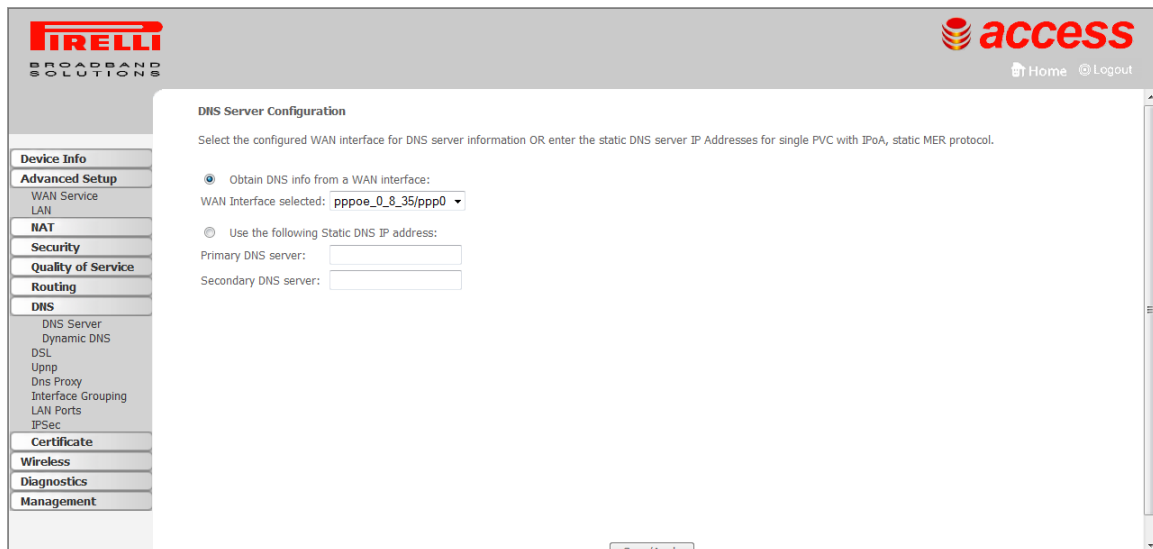
DNS >> DYNAMIC DNS

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 25. Dynamic DNS Panel

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

FIGURE 26. DSL Settings Panel

FIGURE 27. DSL Advanced Settings Panel

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

FIGURE 28. DSL Advanced Settings - Tone Selection Panel

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.

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

FIGURE 29. **Upnp Panel**
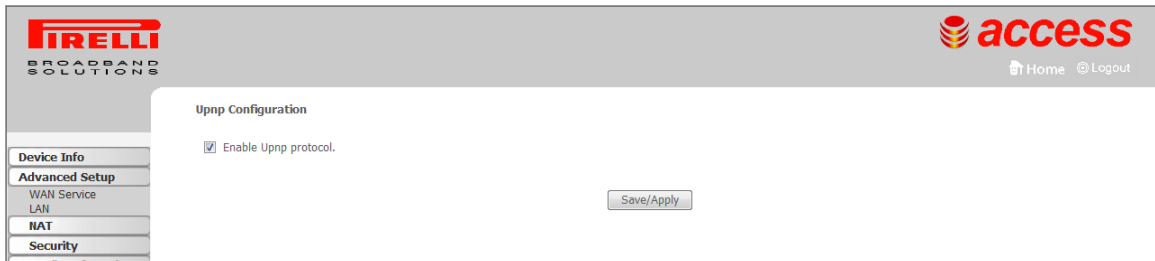
DNS PROXY
In the DNS Proxy panel it is possible to enable/disable the DNS Proxy functionality and, if enabled, to configure it.

FIGURE 30. **DNS Proxy Panel**
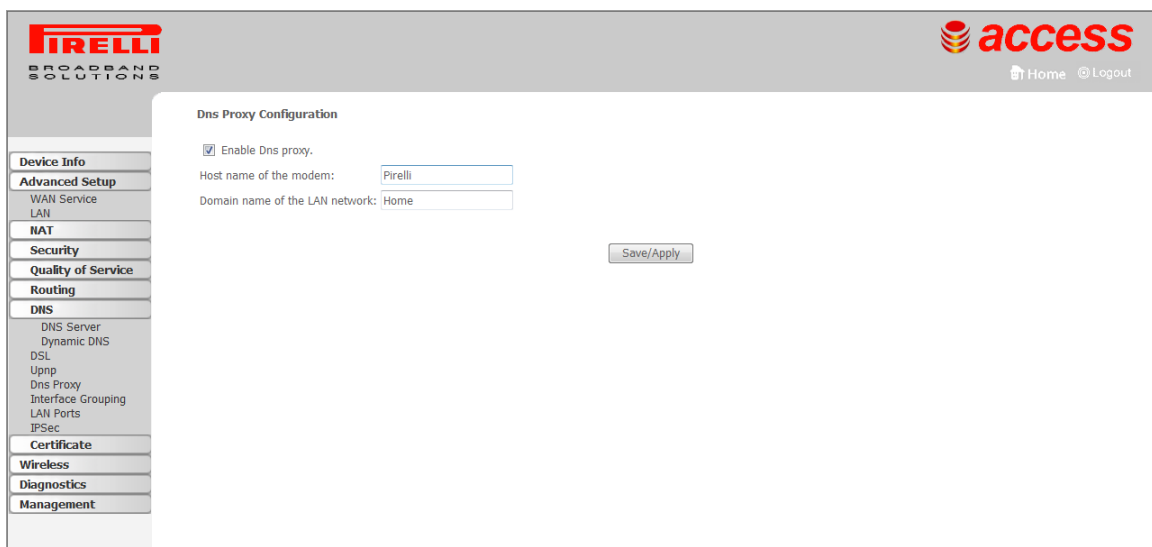
INTERFACE GROUPING
In the Interface Grouping panel a maximum16 entries can be configured.

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 31. Interface Grouping Panel

LAN PORTS

In the LAN Ports Configuration it is possible to enable/disable the Virtual LAN Ports feature.

FIGURE 32. LAN Ports Panel
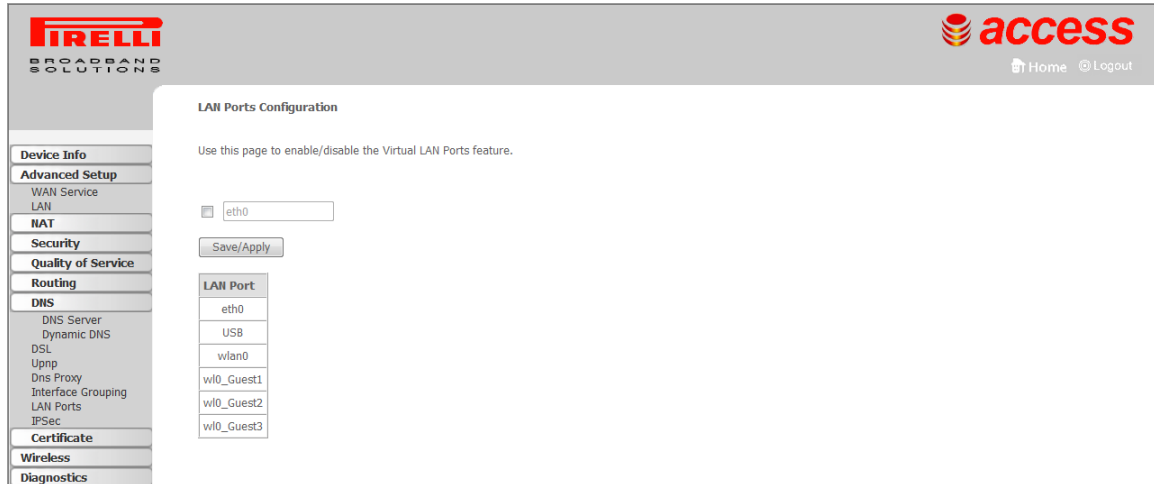
IPSEC   In the IPSec Tunnel Mode panel it is possible to add or to remove IPSec tunnel connections.

FIGURE 33. IPSec Panel
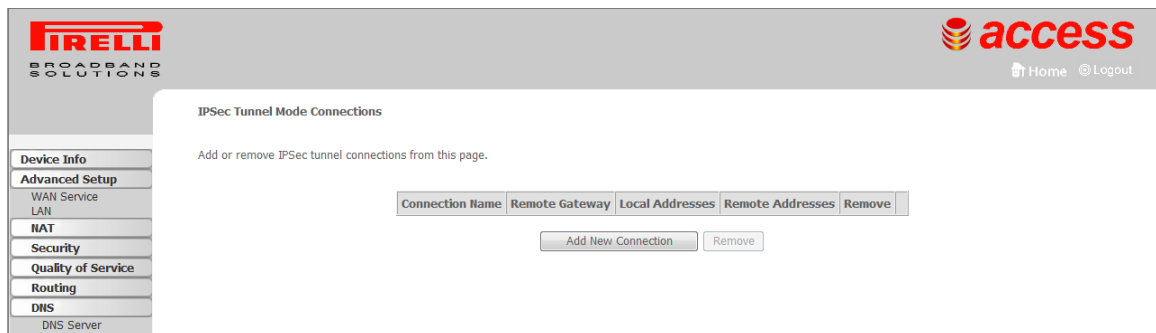
CERTIFICATE >> LOCAL   In the Local Certificates panel it is possible to add, View or Remove certificates. Local certificates are used by peers to verify your identity.

Maximum 4 certificates can be stored.

FIGURE 34. **Local Certificate Panel**
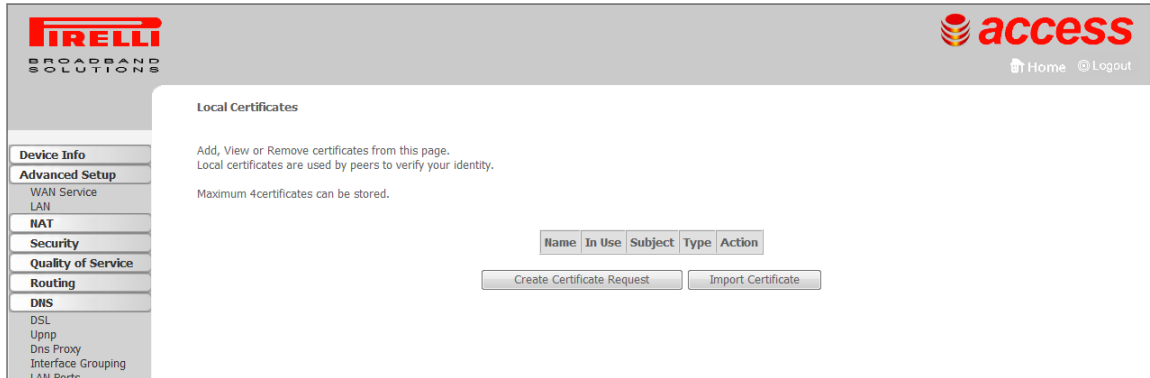
CERTIFICATE >> TRUSTED CA

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 35. **Trusted CA Panel**
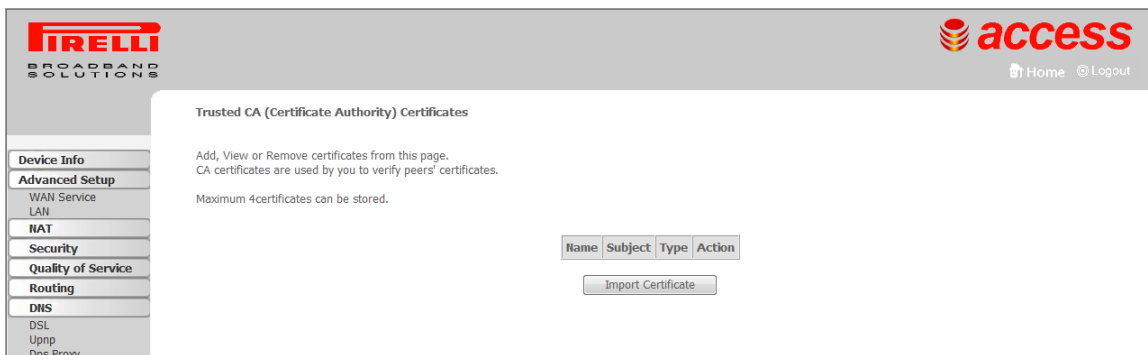
Wireless Section

This chapter will describe the **Wireless Section** accessible from the *Home Page* of the **P.DG A4010G**.

Be aware that any configuration change could compromise your connectivity.

This section is only accessible to a user with admin profile and is intended to collect most of the DNS configuration functions.

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

FIGURE 1. Wireless Basic Panel
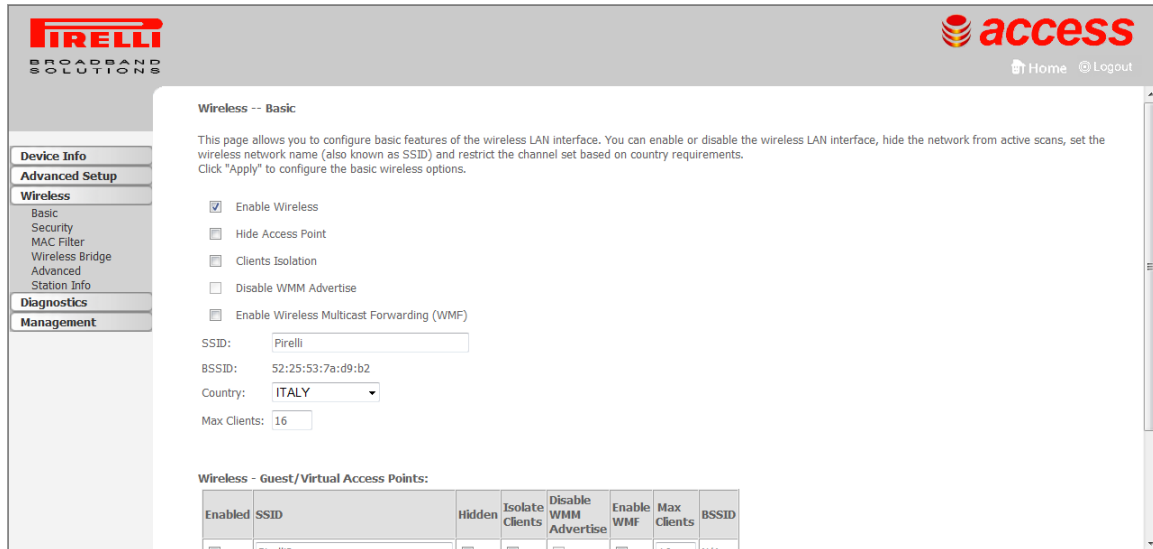
SECURITY

This page allows you to configure security features of the wireless LAN interface by means of a manual configuration or through a WiFi 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 "**Save/Apply**" button to configure the wireless security options.

FIGURE 2. **Wireless Security Panel**
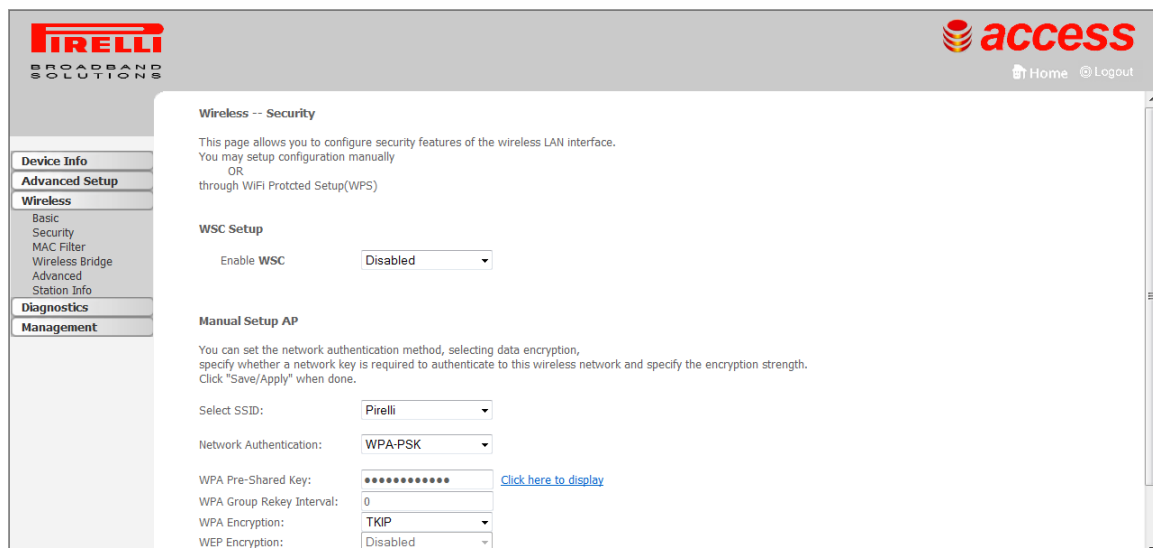
In case the WSC setup will be chosen (thus setting "Enable WSC" field to "Enabled"), the push button or PIN based connection must be selected according to shown parameters' configuration.

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**" 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**
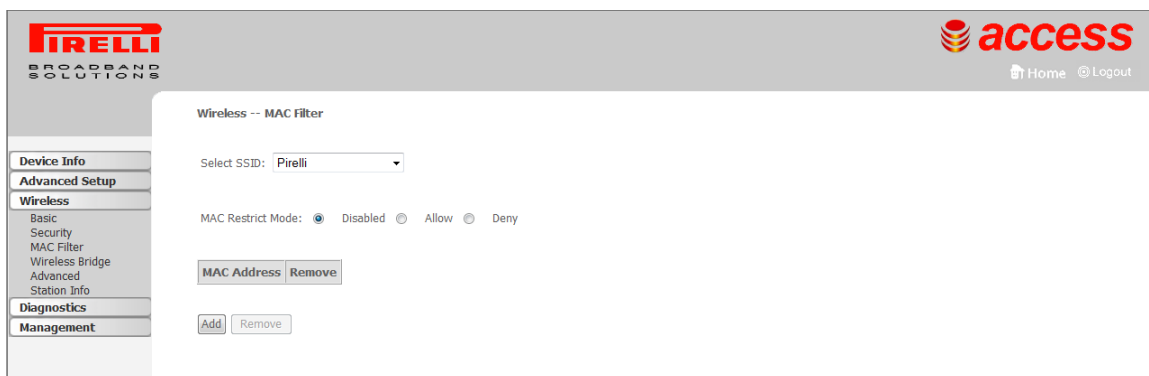
WIRELESS BRIDGE

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.

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

FIGURE 4. **Wireless Bridge Panel**
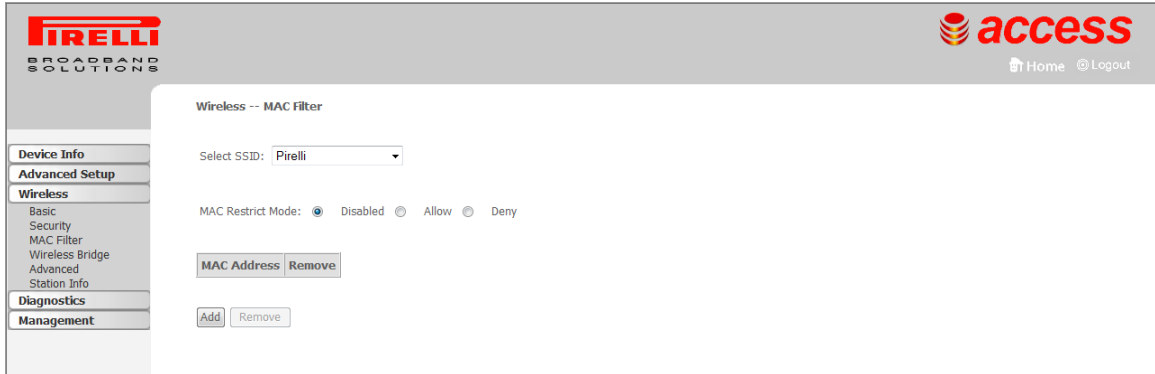
ADVANCED

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

FIGURE 5. **Wireless Advanced Panel**
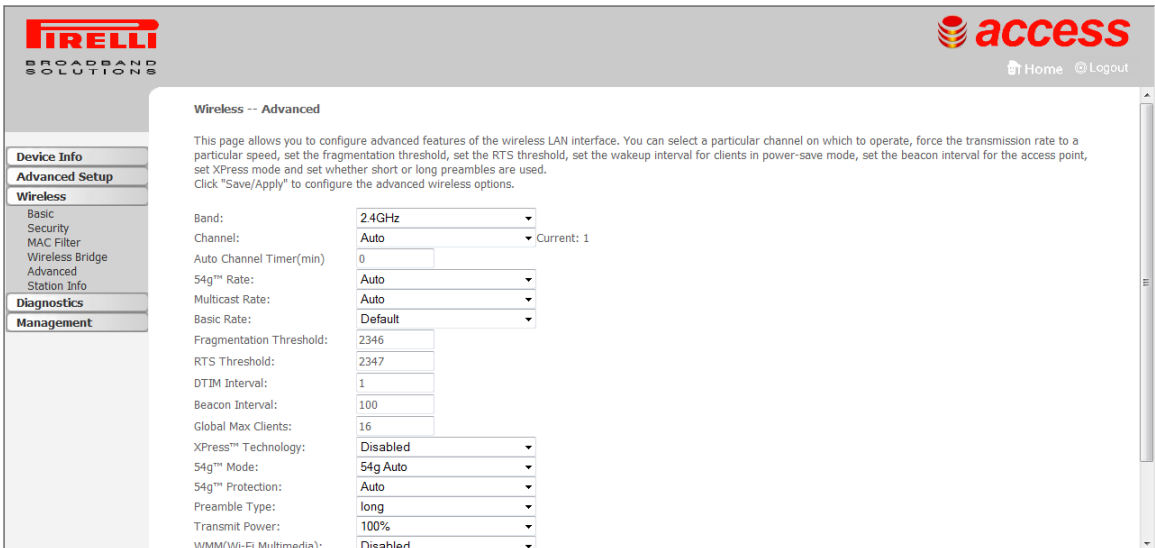
STATION INFO

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**
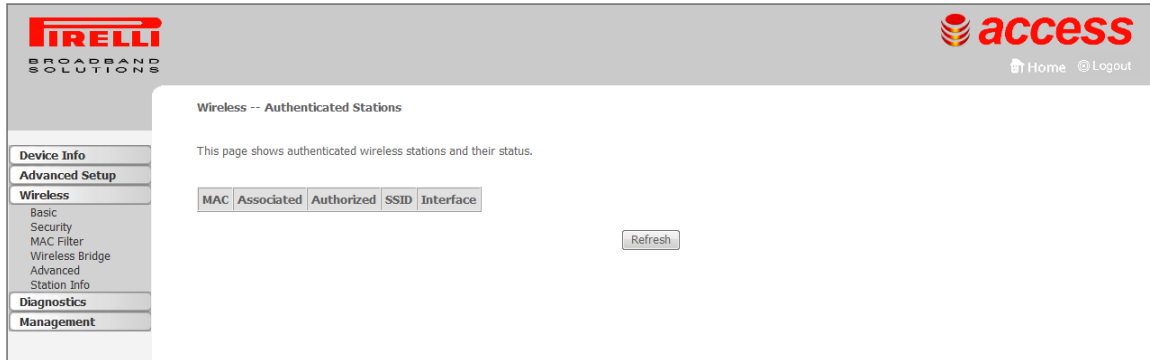
Diagnostics Section

This chapter will describe the **Diagnostics Section** accessible from the *Home Page* of the **P.DG A4010G**.

Be aware that any configuration changes 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

There are three buttons at the bottom of the screen: **Test**, **Test with OAM F5** and **Test with OAM F4**, which will allow you to execute the test again, if necessary.

FIGURE 1. **Diagnostics Panel**

Management Section

This chapter will describe the **Management Section** accessible from the *Home Page* of the **P.DG A4010G**.

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.

FIGURE 1. Backup Panel
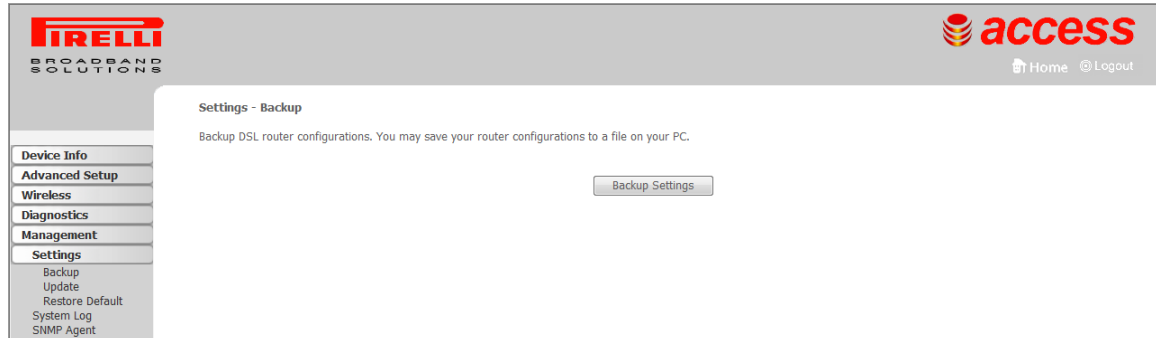
A pop-up screen will appear with a prompt to open or save the file to your computer.

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
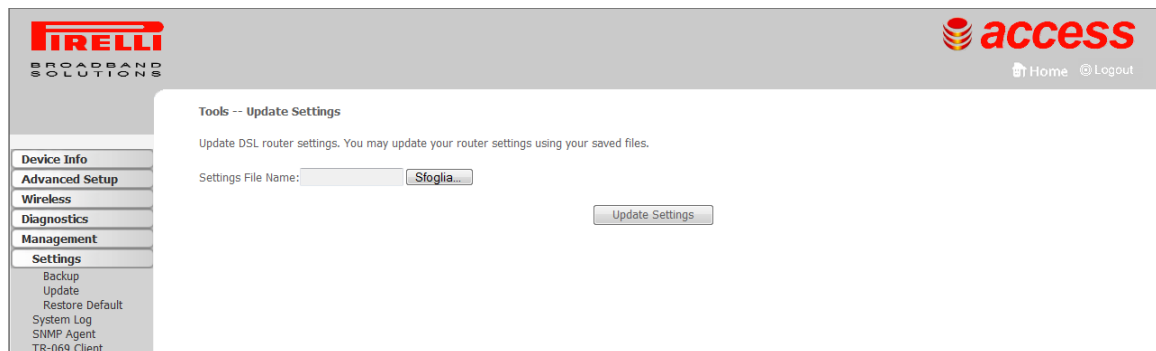
SETTINGS RESTORE DEFAULT

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** 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 Panel
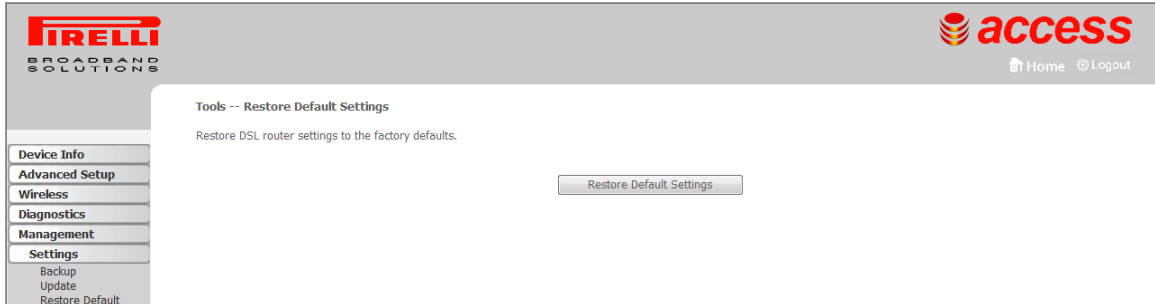
SYSTEM LOG

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
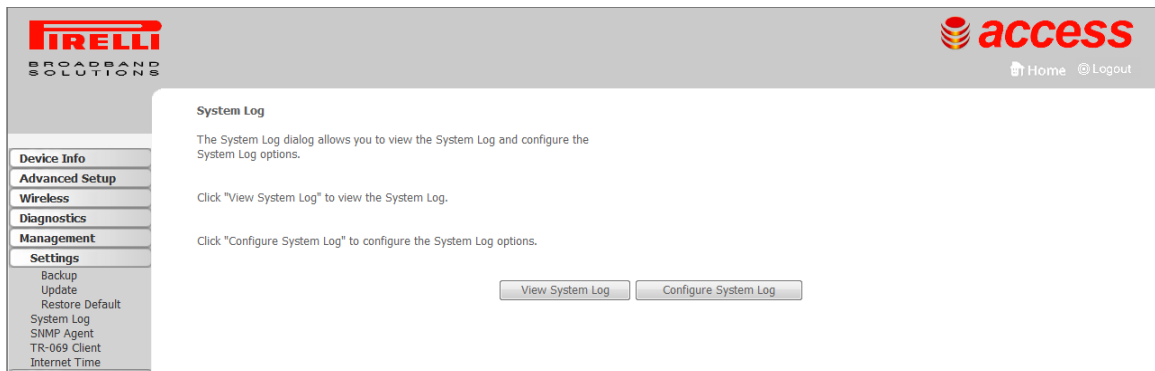
SNMP AGENT

The **SNMP Agent** configuration panel allows a management application to retrieve statistics and status from the SNMP agent in this device. Select the desired values and click "**Save/Apply**" to configure the SNMP options.

FIGURE 5. **SNMP Agent Panel**

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 "Save/Apply" to configure the TR-069 client options.

FIGURE 6. **TR-069 Client Panel**

INTERNET TIME

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

P.DG A4010G

FIGURE 7. Internet Time Panel
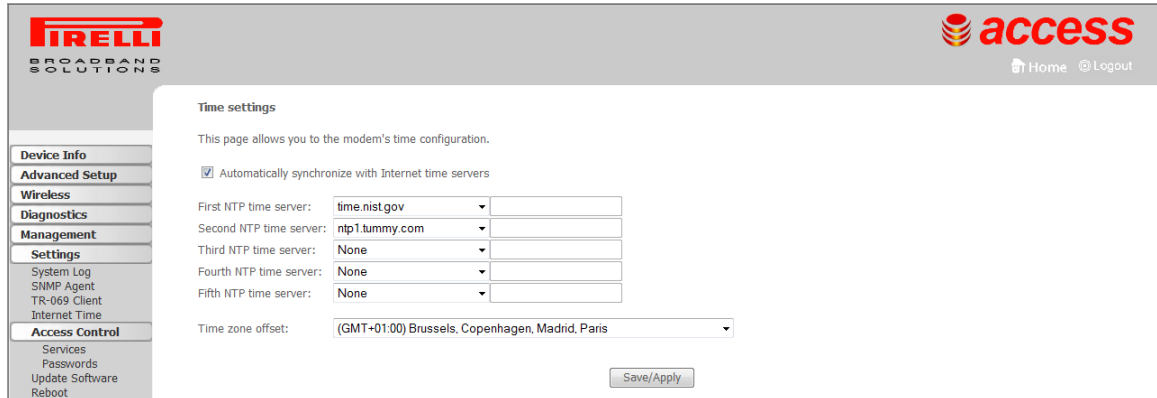
**ACCESS CONTROL >>
SERVICES**

It is possible to enable or disable some services of your router by LAN or WAN. If no WAN connection is defined, then only the LAN side can be configured. Services that can be enabled include HTTP, ICMP, TELNET and TFTP. Click on **Save/Apply** when finished.

FIGURE 8. Services Panel
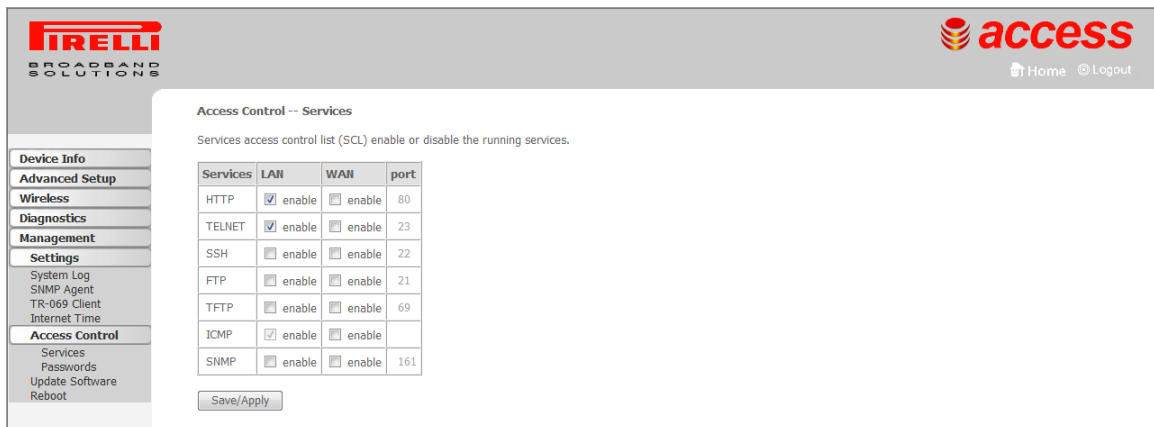
**ACCESS CONTROL >>
PASSWORDS**

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

FIGURE 9. Passwords Panel
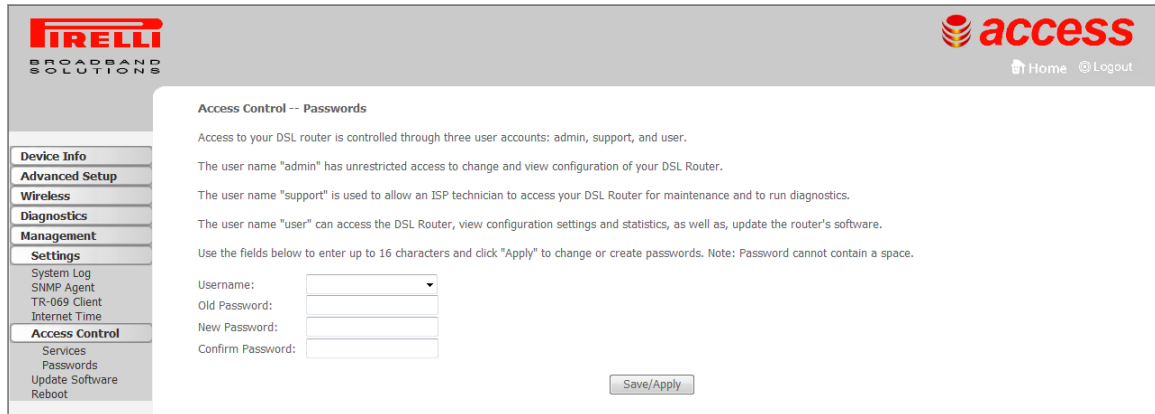
UPDATE SOFTWARE

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 10. Update Software
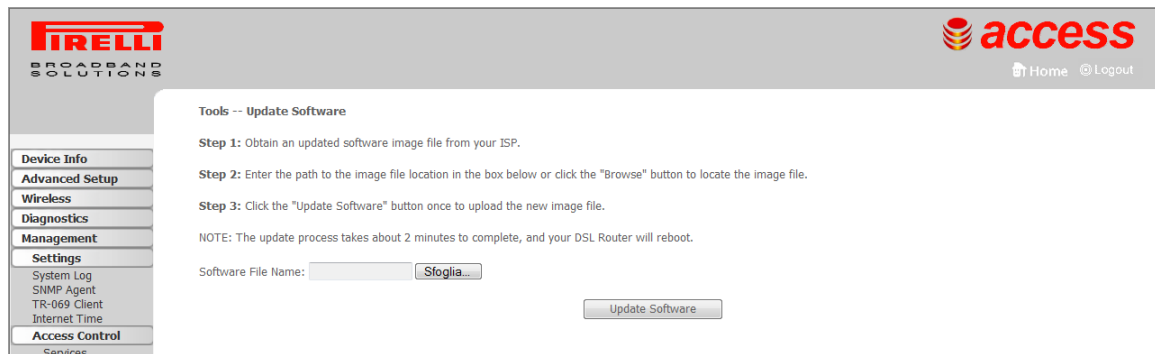
REBOOT

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 11. Reboot Panel
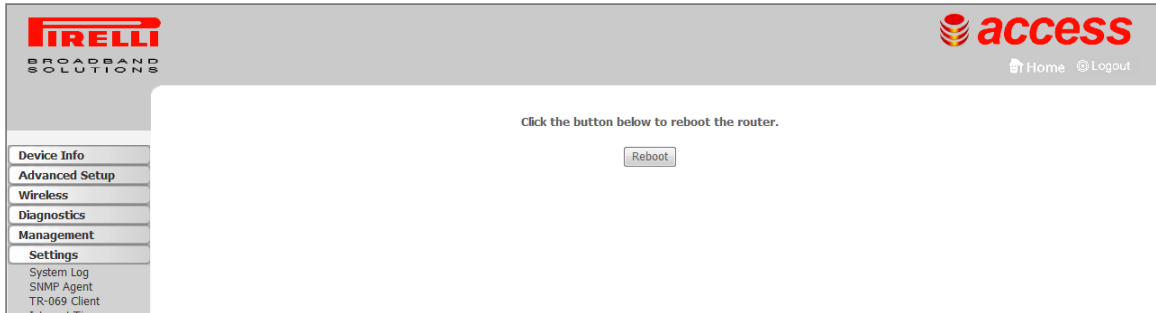
Troubleshooting

BASIC CONNECTION CHECKS

- Check that the Router is connected to your computers and to the telephone line, and that all the equipment is powered on. Check that the ETH or USB Status (according to your connection type) and DSL LEDs on the Router are illuminated, and that any corresponding LEDs on the NIC are also illuminated.
- Ensure that the computers have completed their start-up procedure and are ready for use. Some network interfaces may not be correctly initialized until the start-up procedure has completed.
- If the link status LED does not illuminate for a port that is connected, check that you do not have a faulty cable. Try a different cable.

POWER LED OFF

If the power led is off, check the following:

- Check connections between the Router, the external power supply, and the wall outlet.
- If the power indicator does not turn on when the power cord is plugged in, you may have a problem with the power outlet, power cord, or external power supply. However, if the unit powers off after running for a while, check for loose power connections, power losses, or surges at the power outlet. If you still cannot isolate the problem, then the external power supply may be defective. In this case, contact Technical Support for assistance.

LINK LED OFF

If the Link LED is off, check the following:

- Verify that the Router and attached device are powered on.
- Be sure the cable is plugged into both the Router and the corresponding device.
- Verify that the proper cable type is used and that its length does not exceed the specified limits.
- Be sure that the network interface on the attached device is configured for the proper communication speed and duplex mode.

- Check the adapter on the attached device and cable connections for possible defects. Replace any defective adapter or cable if necessary.

ROUTER NOT RECHEABLE

If the Router cannot be pinged from LAN, check the following:

- Verify that the IP addresses are properly configured. For most applications, you should use the Router's DHCP function to dynamically assign IP addresses to hosts on the attached LAN. However, if you manually configure IP addresses on the LAN, verify that the same network address (network component of the IP address) and subnet mask are used for both the Router and any attached LAN devices.
- Be sure the device you want to ping (or from which you are pinging) has been configured for TCP/IP.

BROWSING TO THE ROUTER CONFIGURATION SCREENS

If you have connected your Router and computers together but cannot browse to the Router configuration screens, check the following:

- Confirm that the physical connection between your computer and the Router is OK, and that the ETH Status LEDs on the Router and NIC are illuminated. Some NICs do not have status LEDs, in which case a diagnostic program may be available that can give you this information.
- Ensure that you have configured your computer as described in "Setting Up Your Computer" on page 15. Restart your computer while it is connected to the Router to ensure that your computer receives an IP address.
- When entering the address of the Router into your web browser, ensure that you use the full URL including the "*http://*" prefix (e.g. http://192.168.1.1).
- Ensure that you do not have a Web proxy enabled on your computer. Go to the Control Panel and click on Internet Options. Select the Connections tab and click on the LAN Settings button at the bottom. Make sure that the Proxy Server option is unchecked.
- If you cannot browse to the Router, use the *winipcfg* utility in Windows 98/ME to verify that your computer has received the correct address information from the Router. From the Start menu, choose Run and then enter *winipcfg*. Check that the computer has an IP address of the form 192.168.1.xxx (where xxx is in the range 2-254), the subnet mask is 255.255.255.0, and the default Router is 192.168.1.1 (the address of the Router). If these are not correct, use the Release and Renew functions to obtain a new IP address from the Router. Under Windows 2000 and Windows XP, use the *ipconfig* command-line utility to perform the same functions.

CONNECTING TO THE INTERNET

If you can browse to the Router configuration screens but cannot access sites on the Internet, check the following:

- Confirm that the physical connection between the Router and the telephone line is OK, and that the DSL LED on the Router is GREEN on.
- Ensure that you have entered the correct information into the Router configuration screens as required. Use the "Internet Settings" screen to verify this.
- Check that the user name and password are correct.
- Check that the INTERNET LED is green on
- Ensure that your computers are not configured to use a Web proxy. On Windows computers, this can be found under Control Panel >Internet Options > Connections.

FORGOTTEN PASSWORD AND RESET CONFIGURATION TO FACTORY DEFAULTS

If you can browse to the Router configuration screen but cannot log on because you do not know or have forgotten the password, follow the steps below to reset the Router to it's factory default configuration.

All your configuration changes will be lost, and you will need to configure again your network before you can re-establish your Router connection to the Internet. Also, other computer users will lose their network connections whilst this process is taking place, so choose a time when this would be convenient.

1. Switch off the Router.
2. Disconnect all your computers and the telephone line from the Router.
3. Re-apply power to the Router, and wait for it to finish booting up.
4. Press the Reset Configuration to Factory Default button on the rear panel for a while.
5. The Router will restart, and when the start-up sequence has completed, browse to: http://192.168.1.1 and configure your network.
6. Reconnect your network as it was before.

WIRELESS NETWORKING

- Ensure that you have an 802.11b or 802.11g wireless adapter for each wireless computer, and that it is correctly installed and configured. Verify that each Wireless computer has either Windows 98SE or higher or MAC OS 10.x or higher.
- If you have a wired and a wireless NIC in the same computer, ensure that the wired NIC is disabled.
- Check the status of the Router LED.
- Ensure that the TCP/IP settings for all devices are correct.
- Ensure that the Wireless Clients are using the same SSID or Service Area Name as the Router. The SSID is case-sensitive.
- Ensure that the encryption method and level that you use on your clients are the same as those configured on the Router. The Router cannot simultaneously support WPA and WEP encryption.
- Ensure that you have the Wireless computer enabled in the list of allowed MAC addresses if you are using MAC Address Filtering on the Router.
- If you are having difficulty connecting or are operating at a low speed try changing the antenna positions on the rear of the Router. For more effective coverage you can try reorientating your antenna. Additionally consider moving the wireless computer closer to the Router to confirm that the building structure or fittings are not adversely affecting the connectivity. If this resolves the problem consider relocating the Wireless computer or the Router, or trying a different channel on the Router.
- Sources of interference: The 2.4GHz ISM band is used for 802.11b and 802.11g. This is generally a licence free band for low power applications, and you may have other devices at your location that operate in this frequency band. You should take care to ensure that there are no devices like microwave ovens for example close to the Router or wireless computers as this could affect receiver sensitivity and reduce the performance of your network. If you are unsure try relocating both the wireless computers and the Router to establish whether this problem exists.
- Most wireless computer Adapters will scan the channels for the wireless Router. If a wireless computer has not located the Router then try initiating a search manually if the client software supports this feature or manually set the channel on your wireless computer to correspond to the Router channel number. Please refer to your Wireless computer adapter documentation and vendor to do this.
- Speed of connection: The 802.11b and 802.11g standards will automatically choose the best speed depending on the quality of your connection. As the signal quality weakens then the speed falls back to a lower speed. The speeds supported by 802.11g are 54 Mbps, 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12 Mbps, and 6 Mbps. The speeds supported by 802.11b are 11

Mbps, 5.5 Mbps, 2 Mbps and 1 Mbps. In general the closer you are to the Router the better the speed. If you are not achieving the speed you had anticipated then try moving the antenna on the Router or moving the Wireless computer closer to the Router. In an ideal network the Router should be located in the centre of the network with Wireless computers distributed around it. Applications are generally available with the computer wireless card to carry out a site survey. Use this application to find the optimal siting for your wireless computer. Consult your Computer Card documentation and vendor for more details.

FREQUENTLY ASKED QUESTIONS

How do I reset the Router to Factory Defaults? Press the Restore Configuration to Factory Default button for more than 10 seconds.

How many computers on the LAN does the Router support? Up to a maximum of 256 computers on the LAN are supported.

The Quality of Service (QoS) is related to the guaranteed level of throughput (the amount of data transferred from the Router to the clients). As many clients are connected as lower is the Quality as Service.

How are additional computers connected? You can expand the number of connections available on your LAN by using hubs, switches and wireless access points connected to the Router. Wireless access points and hubs and switches provide a simple, reliable means of expanding your network; contact your supplier for more information, or visit: http://www.pirelli.com/

I connected the modem before installing the USB Drivers. How should I proceed? You must unplug the USB cable, restart your computer and start over following the procedure described at chapter "USB Connection >> MS Windows"

Why sometimes the Internet Connection is slow? It happens that sometimes a network congestion may produce a slower connection. Try again in a different day period: if you experience many times this fact, contact your network provider.

IP Addressing

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 '192.168.10.8'. 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 '192.168.10.8' is split into two parts:

- Part one ('192.168.10') 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 '192.168.10.8' is, again, split into two parts but is structured differently:

- Part one ('192.168') identifies the network on which the device resides.

- Part two ('.10.8') 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 and Windows XP.

Technical Specifications

This section lists the technical specifications for the P.DG A4010G.

WAN Interface

1 ADSL Line port (RJ-11plug) supporting the following standards:
- ADSL (G.992.1, G992.2, T1.413, G9941, G.997.1)
- ADSL2 (G.992.3)
- ADSL2+ (G992.5)
Annex A/Annex B are available in different product versions

LAN Interfaces

- N° 4 10/100BASE-T Ethernet ports (RJ-45 plug), compliant IEEE 802.3, with auto MDIX and auto-negotiation. Ports can be configured in order to be dedicated to video traffic to/from a STB
- N° 1 USB Device v 1.1

Wireless Interface

IEEE 802.11b/g
- UBR, VBR-nrt, VBR-rt, CBR traffic classes
- Up to 8 PVC
- Pre-emptive SAR
- Multiple physical queues (up to 8) per traffic class, with priority-based scheduling support.

ATM Features

ATM (AAL5) payload format
- UBR, VBR-nrt, VBR-rt, CBR traffic classes
- Up to 8 PVC
- Pre-emptive SAR
- Possibility of multiple physical queues (up to 8) per traffic class, with priority-based scheduling support

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)
- MTU settable

Routing/Bridging

- RIP v1/v2 and static routing
- NAT/NAPT (with ALGs)
- IP QoS
- DHCP Server/Client
- VPN pass-through
- IPv4
- DNS relay
- NTP
- IGMPv2 proxy

QoS
- Traffic shaping (ATM layer)
- Priority-based scheduling (up to 8 queues,max 4 per PVC)
- DSCP/TOS remarking

Security
- Programmable Firewall

Remote Management
DSL Forum TR-069
- FTP/TFTP client for remote firmware upgrade
- Diagnostics and LOGs
- Telnet with CLI
- WEB server with Admin/User configuration Pages

VLAN
- Supports multiple VLAN ID per ports
- Configurable layer-two switching

Power Adapter
- European Plug
- INPUT: 230Vac 50Hz 135mA
- OUTPUT: 15Vac 0.8 A

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 85% non condensing
- Non Operating:5% to 95% non condensing

Compliance
- ITU-T K.21
- RoHS Directive 2002/95/EC on the restriction of the use of certain hazardous substances in electrical and electronic equipment

Glossary

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, 12, 24, 36, 48 and 54 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 pirelli.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 "pirelli.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.

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.

WiFi

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

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

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

PIRELLI Broadband Solutions

Viale Sarca 222
20126 Milano
Italy