BASIC CONFIGURATION GUIDE FOR ADSL ROUTER - AW4062 OBSERVA TELECOM

Release 1.4, 2010-07-02

INDEX

1. INTRODUCTION

This document is guideline of use and configuration of the ADSL router - AW4062 through the web interface.

For the configuration of the ADSL service provided by your ISP, it is recommended to follow the instructions in the *Installation Guide* provided in the router´s Kit. The present document is a complementary guide which explanations of how to configure the wireless router´s basic settings through the web interface, but the following document requires an advanced network knowledge.

It is highly recommended the use of Wizard-ADSL Agent provided in the CD into the router´s kit because of its simplicity.

2. BASIC OPERATIONS – ADSL ROUTER - AW4062

2.1. CHANGE PASSWORD-WEB ACCESS

There are two level accesses for the ADSL router AW4062:

- o **Administrator level** (full access)
- o **User level** (restricted access: it is not allowed to access to advanced network settings)

The first time you access the router, you will be required to enter default user and password for both levels **(it is recommended to change it)**. Open an internet web browser and input the router´s default IP address: http://192.168.1.1
You will be asked to enter username and password credentials of the router.
Default settings are:
> **Administrator level**: User=1234; Password=1234
> **User level**: User=user; Password=user
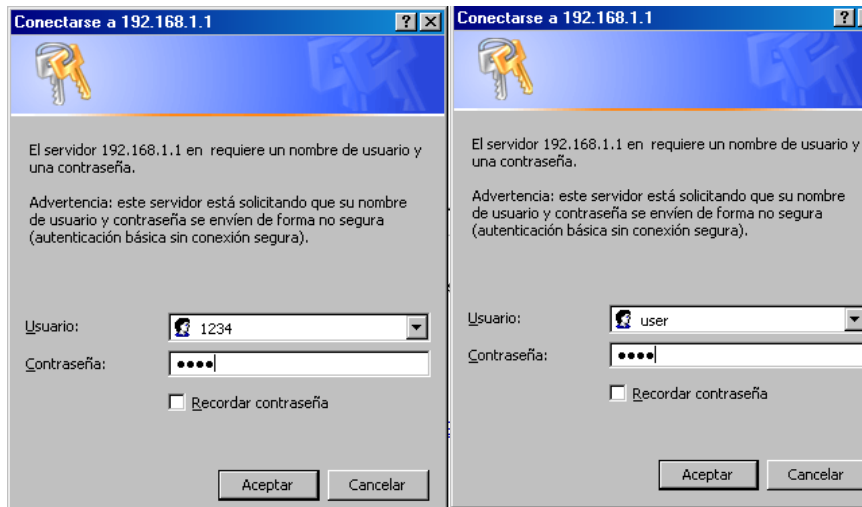
For changing the password in both levels, go to the web menu
Admin→Password and select the level access *User Name*: 1234 (Administrator level) or user (User level).

Write current password (*Old Password*), new password (*New Password*), and write it again (*Confirmed Password*).When you finish, press *Apply Changes:*

4

2.2. WAN –BASIC CONFIGURATIONS:

2.2.1. Dynamic multiPC configuration

MultiPC configuration will allow you to create a network of multiple PCs connected in your LAN, with Internet access through any of them.

With *dynamic* addressing (*PPPoE*), your router will obtain dynamically the IP address needed to access the Internet, each time it is connected, and as long as the connection is active.

The advantage of this configuration type is the security, due to the use of **NAT** (Network Address Translation): private address in your network PCs won´t be seen from the outside, as they are translated into a unique public IP valid through the Internet.

WAN Configuration:

STEP 1.- Access the web menu *WAN → Channel Config* and complete all the fields as follows:

> VPI/VCI: in environments without Imagenio, it is 8/32
> Encapsulation: LLC
> Channel Mode: PPPoE
> Enable NAPT: selected (NAT rules enabled)
> Enable QoS: selected (it will be applied the rules of Quality of Service)
> Admin Status: Enable
>
> PPP Settings:
> > User Name: specify the username for this connection. Default setting is *adslppp@telefonicanetpa*
> > Password: default setting is *adslppp*
> > Type: Continuous (Always on)
> > Idle Time (min): empty
>
> WAN IP Settings:
> > Default Route: Enable

When you finish, press *Add.*

STEP 2.- Access the web menu **WAN→ATM Settings** and specify the corresponding Quality of Service parameters (QoS) for the PVC:

In environments without Imagenio, QoS parameters=UBR, PCR=6000.

LAN Configuration:

You should configure your LAN settings with default IP 192.168.1.1, so your router assigns IP pool within this range.

STEP 1.- Access the web menu **LAN** to configure your local area network settings:

STEP 2.- Access the web menu **Services → DHCP Settings** to setup your router as DHCP Server and act as IP address Server within the IP address pool which you specify below:

2.2.2.   Static multiPC configuration

Whit this type of configuration your router will be assigned (by your ISP) a unique and static IP address as Gateway (**static**) to have access to the Internet, through a RFC1483 channel.

Currently it is also possible that your ISP provides you static IP address (always the same) through an IP DSLAM, so you will have to configure the channel in PPPoE mode. The BRAS (Broadband Remote Access Server) will provide you, when the authentication process has finished, a static IP address to your PC.

<u>**WAN Configuration:**</u>

<u>**STEP 1**</u>.- Access the web menu **WAN → Channel Config** and complete all the fields as follows:

> VPI/VCI: in environments without Imagenio, it is 8/32
> Encapsulation: LLC
> Channel Mode: 1483 Routed
> Enable NAPT: selected (NAT rules enabled)
> Admin Status: Enable
> Enable QoS: selected (QoS rules enabled)
> WAN IP Settings:
>> Type: Fixed IP
>> Local IP Address: static IP address provided by your ISP
>> Remote IP Address: static IP address-Gateway provided by your ISP
>> Subset Mask: subset mask provided by your ISP
>> Default Route: Enable

8

STEP 2.- Access the web menu **WAN→ATM Settings** and specify the Quality of Service parameters (QoS) for the PVC:

In environments without Imagenio, QoS parameters=UBR, PCR=6000.

LAN Configuration:

In this type of configuration (**static MultiPC**) your router will act as DHCP server within default range 192.168.1.33-192.168.1.254

STEP 1.- Access the web menu **LAN** to configure your local area network settings:

STEP 2.- Access the web menu **Services → DHCP Settings** to setup your router as DHCP Server and act as IP address Server within the IP address pool which you specify below:

2.2.3 Dynamic singlePC configuration

With the **SinglePC** configuration your PC will be directly connected to the Internet, as it is not applied the NAT rules. With this type of configuration, your PC will be the only machine in the network. It is highly recommended to make use of any network protection in your PC as: firewall, antivirus software, etc.

Due to the router will be setup as **Bridge mode**, in order to manage the connections with the Internet you must have installed a **PPPoE client** in your PC. You can follow below steps, for instance, for Windows Vista PPPoE default client (for the rest of OS the screenshots may be different):
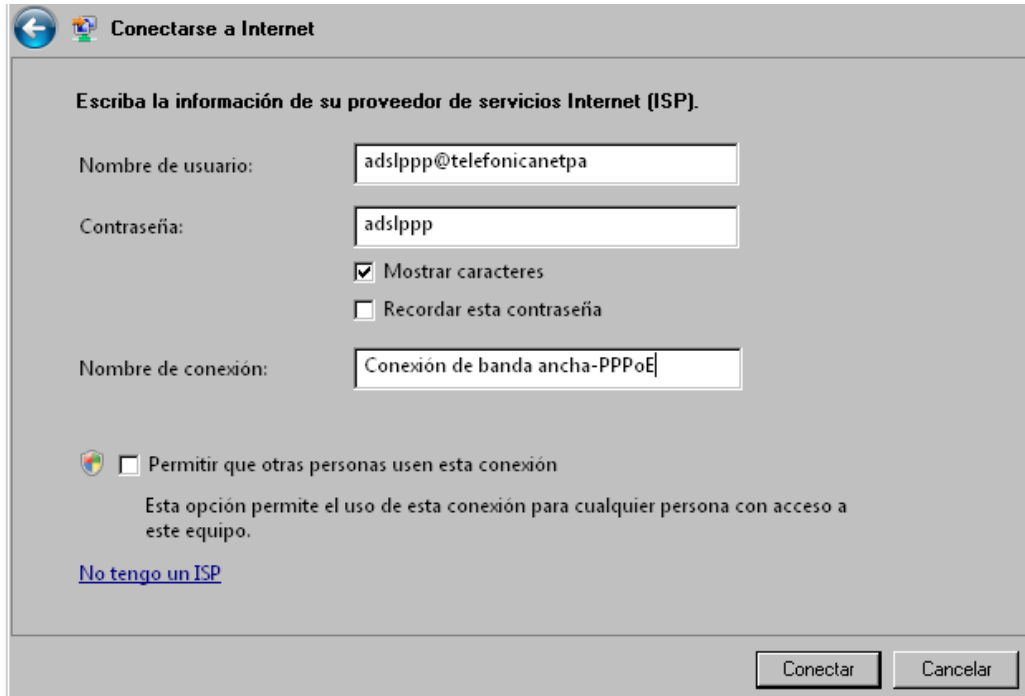
1.- Go to network connection manager→ setup network connection
2.- Connect to Internet
3.- Create a new connection:
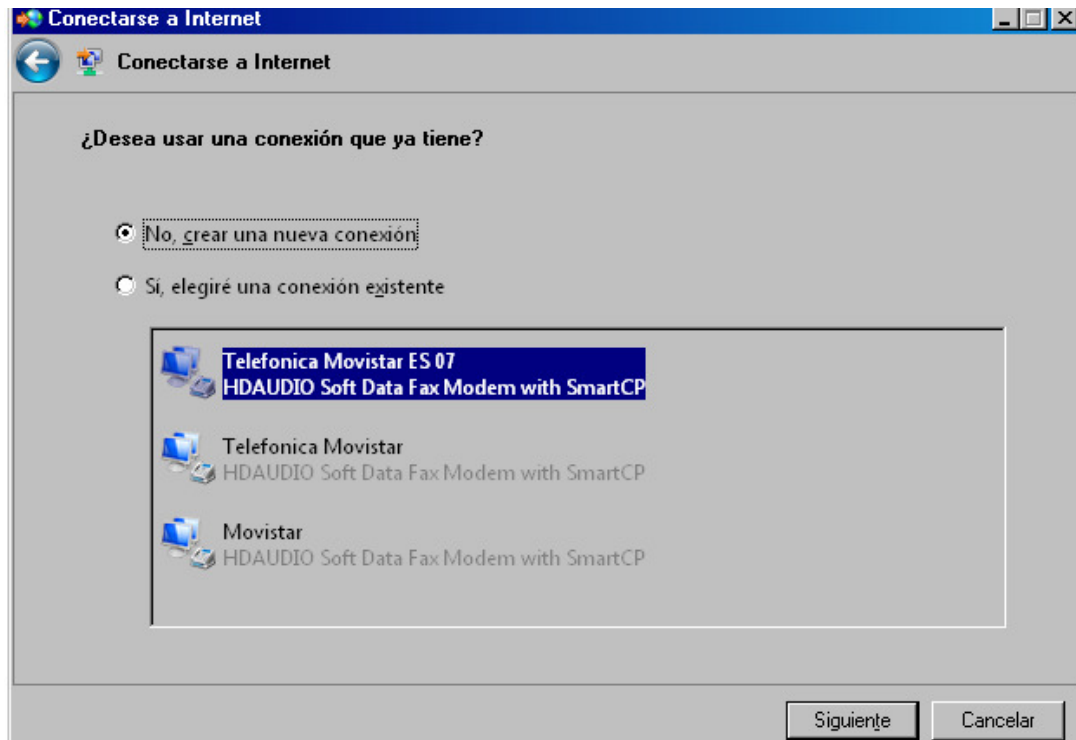
4.- Select broadband PPPoE:
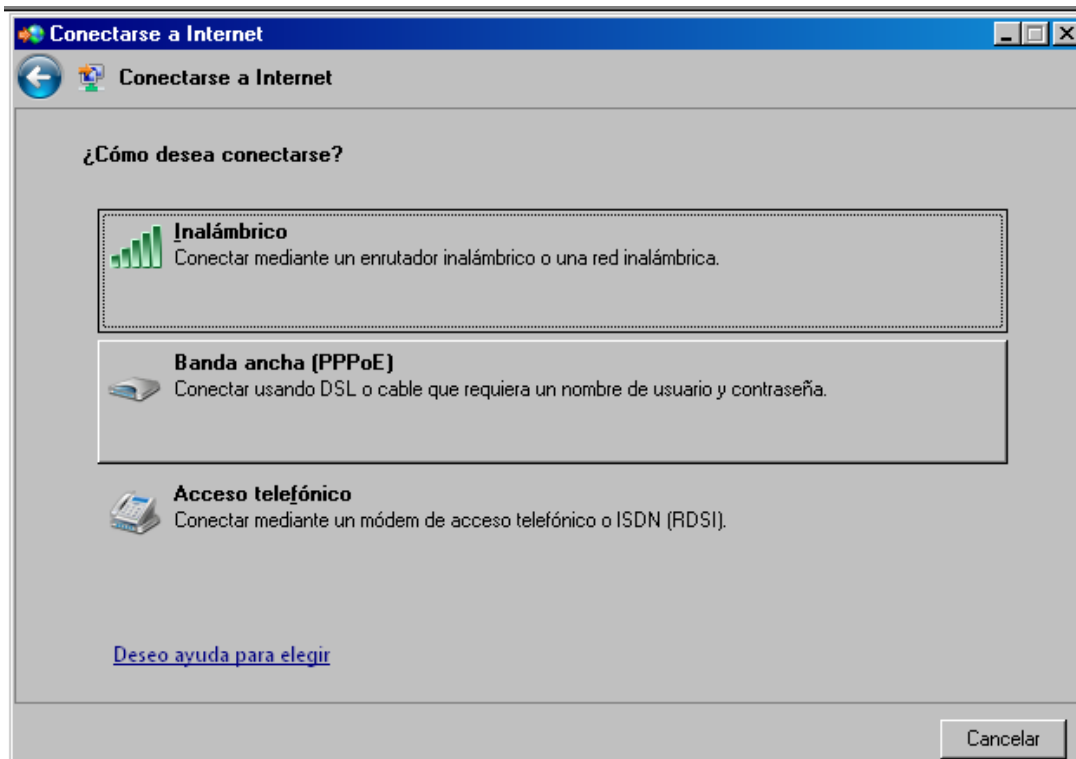
5. Specify the information of username and password provided for your ISP for PPPoE connection, and press **Connect**:
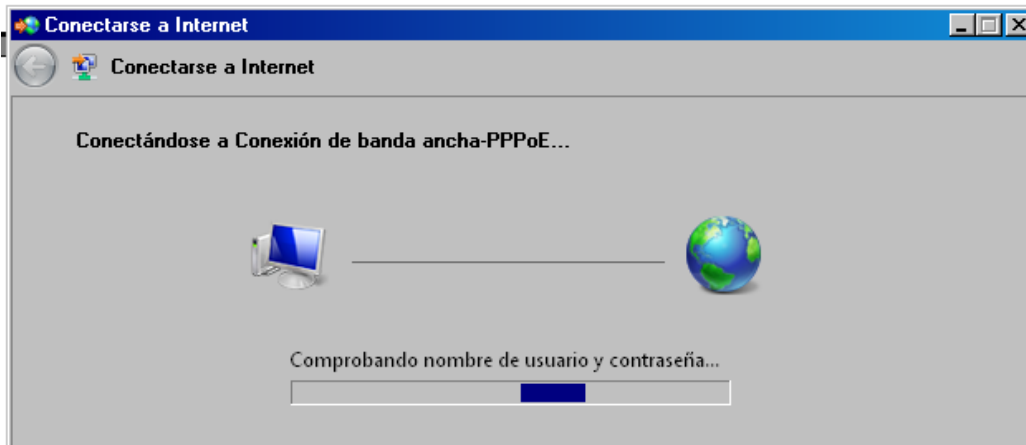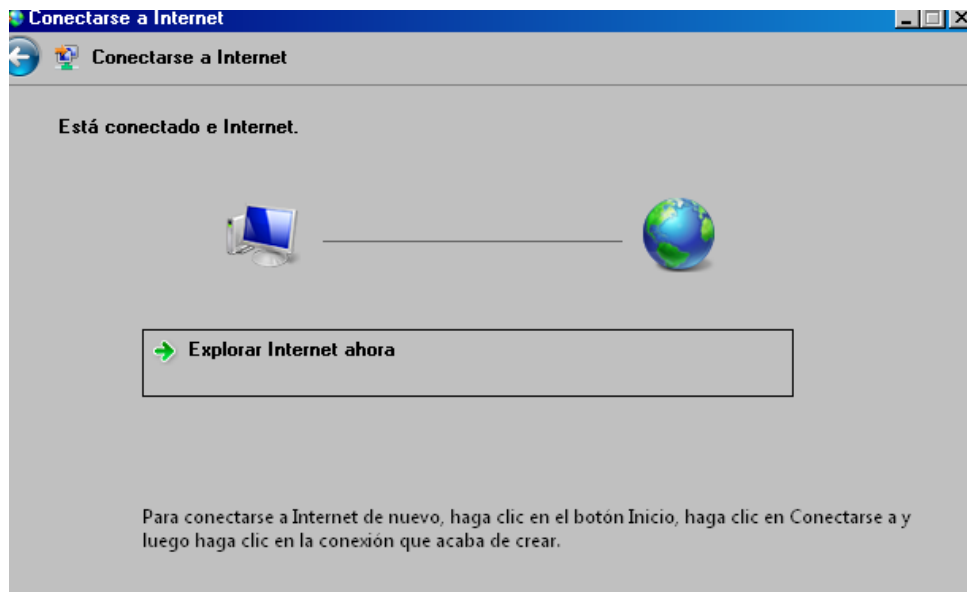
6.- Once you have created the PPPoE connection, the next time you want to connect you only have to select the connection you have created from the list of "Connect to a network":
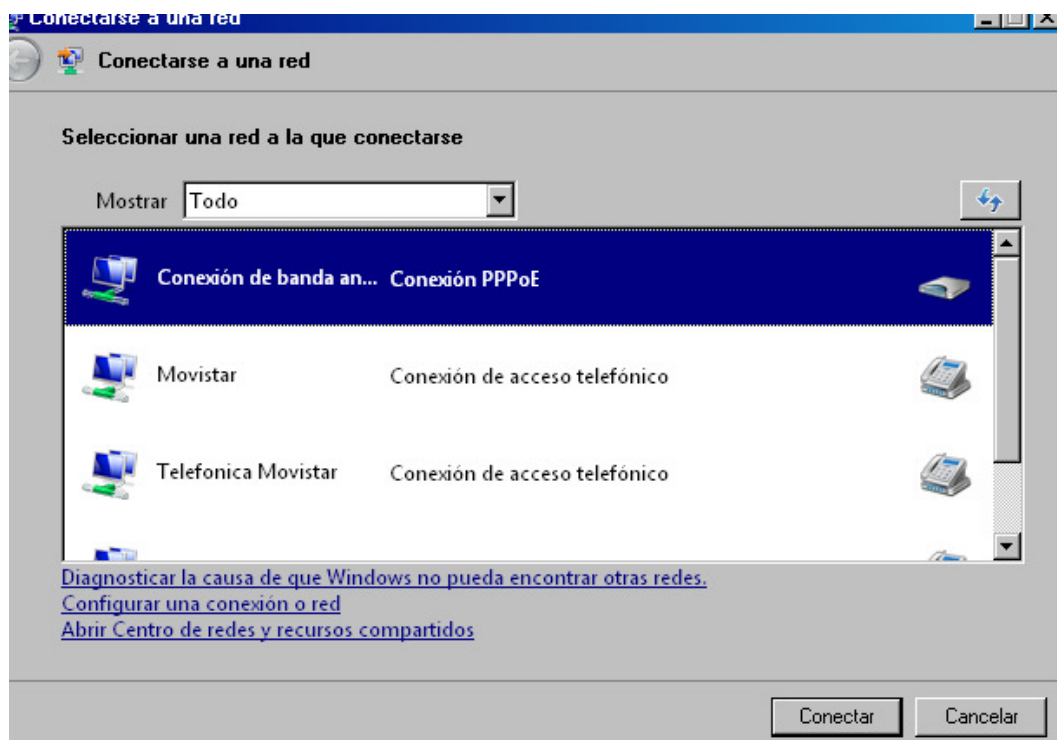
7.- Introduce username and password provided by your ISP for PPPoE connection, and press **Connect**:

WAN Configuration:

STEP 1.- Access the web menu *WAN → Channel Config* and specify all the fields as below:

VPI/VCI: in environments without Imagenio, it is 8/32
Encapsulation: LLC
Channel Mode: 1483 Bridged
Enable QoS: selected
Admin Status: Enable

STEP 2.- Access the web menu **WAN→ATM Settings** and specify the Quality of Service parameters (QoS) for the PVC:

In environments without Imagenio, QoS parameters=UBR, PCR=6000.

LAN Configuration:

STEP 1.- Access the web menu **LAN** to configure your local area network settings:

STEP 2.- Access the web menu **Services → DHCP Settings** to setup your router as DHCP Server and act as IP address Server within the IP address pool which you specify below:

2.2.4 Static singlePC configuration

With this type of configuration, your PC will be the only machine in the network (**singlePC**) through the only IP address to access the internet (**static**) provided by your ISP. It is highly recommended to make use of any network protection in your PC as: firewall, antivirus software, etc.
Currently it is also possible that your ISP provides you static IP address (always the same) through an IP DSLAM, so you will have to configure the channel in PPPoE mode. The BRAS (Broadband Remote Access Server) will provide you, when the authentication process has finished, a static IP address to your PC.

WAN Configuration:

STEP 1.- Access the web menu **WAN → Channel Config** and specify all the fields as below:

> VPI/VCI: in environments without Imagenio, it is 8/32
> Encapsulation: LLC
> Channel Mode: 1483 Routed
> Enable NAPT: NOT selected (NAT disabled)
> Admin Status: Enable
> Enable QoS: selected
> WAN IP Settings:
>> Type: Fixed IP
>> Local IP Address: static IP address provided by your ISP
>> Remote IP Address: static IP address-Gateway provided by your ISP
>> Subset Mask: sunet mask provided by your ISP
>> Default Route: Enable

STEP 2.- Access the web menu **WAN→ATM Settings** and specify the Quality of Service parameters (QoS) for the PVC:

In environments without Imagenio, QoS parameters=UBR, PCR=6000.

LAN Configuration:

STEP 1.- Access the web menu **Services → DHCP Settings** to setup your router as DHCP Server and act as Server of the range of the only one IP address available: In order to know the IP address to be configured as Gateway, you must do the following logic binary operation from the public IP address and subnet mask provided by your ISP in the welcome letter: (public IP address) AND (subnet mask)) OR 1.

     1.1 Setup *start IP pool address=end IP pool address* into **IP Pool Range** as the public IP address provided in your welcome letter
     1.2 Setup as *Gateway* the IP address you have previously calculated

STEP 2.- Access the web menu **LAN** to setup your local area network with the static IP address provided by your ISP:

After you *Apply Changes* in LAN with a different IP address than default (192.168.1.1), you will lose the web management into the router through old IP 192.168.1.1, so you need to renew the IP assignment in your LAN. You can open a MSDOS Windows and type: **ipconfig /release** and after that **ipconfig /renew**. You can also reboot the router and the PC. With these actions you will force the renewal of the IP address in your PC, according to the new LAN settings.

2.3. WIRELESS CONFIGURATION

2.3.1.   Enable/Disable wireless interface

If you want to enable/disable the wireless interface by means of the web manager, you can access to **Wireless → Basic Settings:**

o **Enable**: unselect the option *Disable Wireless LAN Interface* to enable the wireless interface in the router, and press A*pply Changes.* After some seconds, the frontal WLAN LED will be ON in green colour, which indicates that the wireless interface has been enabled successfully.

o **Disable**: select the option *Disable Wireless LAN Interface* to disable the wireless interface, and press *Apply Changes.* After some seconds, the frontal WLAN LED will be OFF, which indicates that the wireless interface has been disabled successfully.

2.3.2. Change SSID and radio channel

As default, the wireless network identifier (SSID) will be setup as **WLAN_XXXX**, where XXXX are the last 4 characters in your router´s MAC address.

As a first step to achieve wireless security into your network, it is recommended to change default SSID in the web section **Wireless → Basic Settings → SSID**

Furthermore, as default the radio channel is setup as automatic (Auto), in order to assign the less used channel. If you want to change the radio channel, select the channel in **Channel Number** box (1-13) and press **Apply Changes**:

2.3.3. Show/Hide SSID

As default settings, the router will broadcast your wireless name identifier (SSID) to everyone, so any other user can see the router´s network.

As a second step to achieve wireless security, it is recommended to avoid the broadcast of your SSID into the web menu **Wireless➔ Advanced Settings➔ Broadcast SSID**, and select **Disable**. Next, press **Apply Changes:**

2.3.4. Change wireless encryption/key

As default settings, your router will be setup with the following wireless information regarding the encryption type and key (you can see details in the label on the bottom of the router):

If you want to disable the wireless security (open network: not recommended, as anyone would be able to access your network) or change the encryption type and wireless key, you can go to **Wireless➔Security**:

The different encryption types supported in the ADSL router-AW4062 are:

- No encryption (open)
- WEP
- WPA PSK (TKIP, AES, TKIP+AES)
- WPA2 PSK (TKIP, AES, TKIP+AES)
- WPA2 Mixed PSK (TKIP, AES, TKIP+AES)

None:

To configure your wireless network without encryption (without key) please uncheck all encryption types in the wireless section **Wireless→Security.**

In this mode, your wireless network will be open (no encryption) and any other user with wireless connection may enter your network, as all the information in your system is transmitted without encryption. **It is recommended the use of some of the encryption types described below.**

WEP (*Wired Equivalent Privacy*):

In the menu **Wireless→Security**, select **Encryption=WEP**, and press **Set WEP Key**:

ADSL Router

TECOM

Site contents:
- Status
- LAN
- Wireless
  - Basic Settings
  - Advanced Settings
  - Security
  - Access Control
  - WPS
- WAN
- Services
- Firewall
- Advance
- Diagnostic
- Admin
- Statistics

Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Encryption:
- ☐ WEP
- ☐ WPA(TKIP)
- ☐ WPA(AES)
- ☐ WPA2(TKIP)
- ☐ WPA2(AES)

[Set WEP Key]

☐ Use 802.1x Authentication   ○ WEP 64bits ○ WEP 128bits

WPA Authentication Mode: ○ Enterprise (RADIUS) ● Personal (Pre-Shared Key)

Pre-Shared Key Format: [Passphrase ▼]

Pre-Shared Key: [●●●●●●●●●●●●●●●●●●●]

Authentication Server: Port [1812]   IP address [0.0.0.0]   Password [   ]

Note: When encryption WEP is selected, you must set WEP key value.

[Apply Changes]

Wireless WEP Key Setup

This page allows you setup the WEP key value. You could choose and select ASCII or Hex as the format of input value.

Key Length:	64-bit ▼
Key Format:	ASCII (5 characters) ▼
	ASCII (5 characters)
Default Tx Key:	Hex (10 characters)
Encryption Key 1:	*****
Encryption Key 2:	*****
Encryption Key 3:	*****
Encryption Key 4:	*****

[Apply Changes] [Close] [Reset]

Wireless WEP Key Setup

This page allows you setup the WEP key value. You could choose and select ASCII or Hex as the format of input value.

Key Length:	128-bit ▼
Key Format:	ASCII (13 characters) ▼
	ASCII (13 characters)
Default Tx Key:	Hex (26 characters)
Encryption Key 1:	*************
Encryption Key 2:	*************
Encryption Key 3:	*************
Encryption Key 4:	*************

[Apply Changes] [Close] [Reset]

Choose the length and format for the wireless key: 64-bit (ASCII-5 characters, Hex-10 characters), or 128-bit (ASCII-13 characters, Hex-20 characters).

Next select the key to be transmitted as default (**Default Tx Key**), and the corresponding value in **Encryption Key**.

When you have finished, press **Apply Changes** in both menus *(Wireless Key Setup and Wireless Security Setup.*

WPA (*WiFi Protected Access*):

This encryption method uses more complex functions for generating and managing the encrypted information, so this is more secure and recommended than WEP method.

Go to web menu **Wireless→ Wireless Security Setup**, and select the WPA method in some of its variants: **WPA PSK (TKIP, AES, TKIP+AES), WPA2 PSK (TKIP, AES, TKIP+AES), WPA2 Mixed PSK (TKIP, AES, TKIP+AES).**
IT ALLOWS CHECKING SEVERAL BOXES AT THE SAME TIME.

If you have an authentication Server (**Radius**), in your network, select the option **Enterprise (RADIUS)** and setup the IP address and port number of your radius.
On the other hand, select **Personal (Pre-Shared Key).**
Next, select the format of the key to be transmitted (Passphrase or Hex-64 characters).

The format "Passphrase" allows a set of characters in ASCII with a minimum length of 8 characters (printable from 32 - 126), except **< >] "**
It is not allowed to start or end with blanks, or set two consecutive blanks in the middle.

When you finish, press **Apply Changes.**

2.3.5.   Wireless MAC filtering

As another step to achieve security into your wireless network, you may want to restrict the access to a specific set of machines to your network (trusted devices), and forbid the access to the rest. With this action, you will guarantee that the only machines to access your network will be the set of devices you trust in.

In this section, you will be able to configure the rules to restrict the wireless traffic into your network by allowing or denying access to the MAC addresses you specify.

Go to web menu **Wireless→Access Control**, and select the rule you want to be applied:

- o **Disable** (all machines are allowed to access your network)
- o **Allow Listed** (only the listed MAC addresses are allowed to access your network)

Deny Listed (all machines are allowed to access, except the specific set of MAC addresses in the list):

Once you have entered all the rules and MAC addresses, press **Add.**

2.3.6.   WPS (Wireless Protected Setup)

Although home Wi-Fi networks have become more and more popular, users still have trouble with the initial set up of network. This obstacle forces users to use the open security and increases the risk of eavesdropping. Therefore, the Wi-Fi Protected Setup (WPS) is designed to ease set up of security-enabled Wi-Fi networks and subsequently network management.

The largest difference between WPS-enabled devices and legacy devices is that users do not need the knowledge about SSID, channel and security settings, but they could still surf in a security-enabled Wi-Fi network.

These are the elements involved into the WPS process:

o **Registrar**: network entity which provides/revokes the credentials for the access (*router* or wireless Access Point)

o **Enrolee**: client devices which want to be connected through a secure wireless network (wireless USB adapters, cameras, phones…).

25

The process of activation and connection is quite simple:

1. User has a AP or router which supports WPS method, and one or some client devices want to be connected through a secure network

2. User powers on all devices

3. User pushes WPS button in the AP and in client devices

4. All devices are connected in secure mode, without the need of knowing or introducing the SSID or key

5. The network name and encryption are transmitted in a secure mode

6. It can be added easily a new client device, by pushing the corresponding WPS button

The ADSL router - AW4062 supports both methods **Push Button** and **PIN:**

Push Button method (PCB):

The Push Button method can be started in two ways:

o From the **router´s web page** (**SW method**): pushing **"Start PBC":**

o Or by pushing the **physical push button** placed in **the rear panel** in the router and labelled with the wireless symbol (**HW method**), at least during **8 seconds**

26
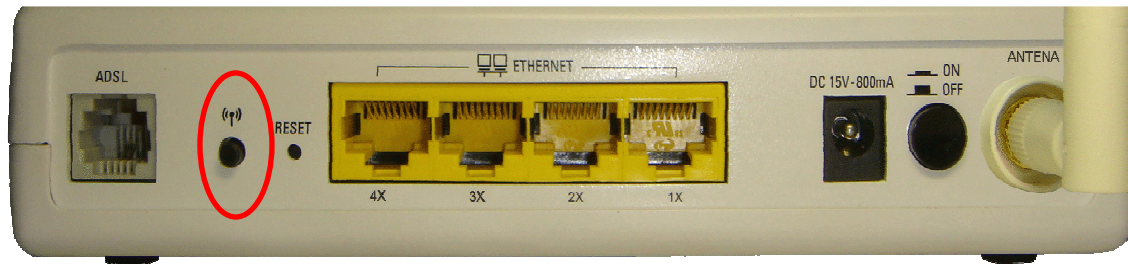
From this moment on, you must activate the WPS method in the client (for instance, a wireless USB adapter which supports this option), by pushing also its corresponding WPS push button, within a time window of 2 minutes as maximum. If you don't push the WPS client push button within 2 minutes, the window for association will be closed, and you will have to push the router´s WPS push button again to start the process.

Frontal WPS Led status in the router during the WPS process:

- o **Blinking Yellow** → WPS activation in process (max. duration: **2 minutes**)
- o **Blinking Red** → WPS process failure (whatever the reason is). It keeps red for **30 seconds** and then turns off.
- o **Steady Green** → WPS connection established successfully between Registrar (router) and Enrolee (client). It keeps steady green for **10 seconds** and then turns off**.**

Example of WPS-Push Button with the following elements:

- o ADSL router - AW4062 Observa Telecom.
- o Wireless adapter Observa Telecom- USB Edimax 11g-7318Ug
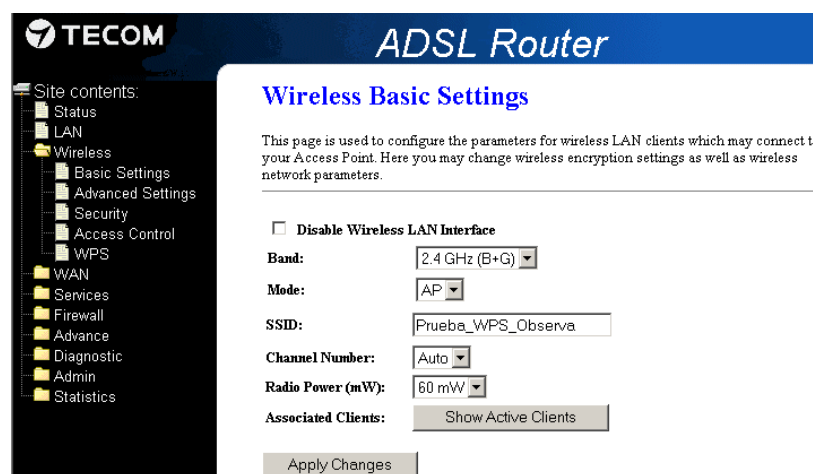
- o Connect the wireless USB adapter in your PC and open the wireless network manager application.
- o Push the router´s WPS push button and the corresponding into the wireless USB adapter (within 2 minutes as maximum).

o It will show up the following window into the USB adapter manager, which means that the WPS network profile is being created:
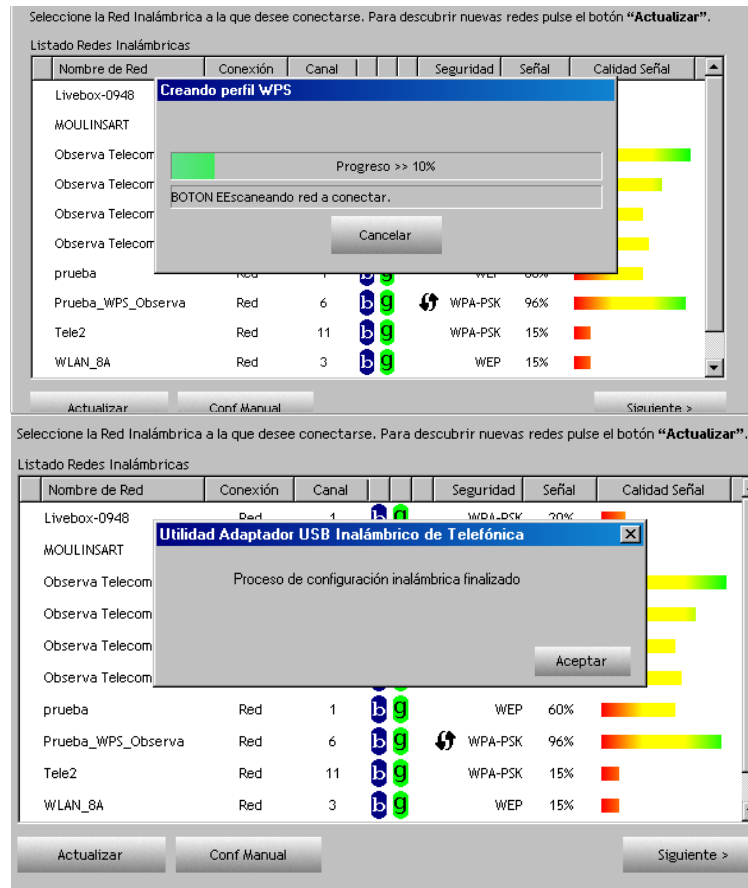
o Once the profile is created, the ADSL router –AW4062 and the USB adapter will be associated automatically:

o From this moment on, you will be able to surf in the Internet in secure mode with your ADSL router - AW4062.

2.4. OPEN PORTS (Port Forwarding)

With the **MultiPC** configuration (NAT enabled: translation of public into private addresses), you may be interested in opening some port of a specific application, in order to make this application run faster.

Go to the web menu **Firewall → Port Forwarding**, and complete the information required below:

Field	Description
Port Forwarding	Check this item to enable the port-forwarding feature.
Protocol	TCP, UDP or both.
Enable	Check this item to enable this entry
Local IP Address	IP address of your local server that will be accessed by Internet.
Local Port	The destination port number that is made open for this application on the LAN-side.
Remote IP Address	The source IP address from which the incoming traffic is allowed. Leave blank for all.
Public Port	The destination port number that is made open for this application on the WAN-side
Interface	Select the WAN interface on which the port-forwarding rule is to be applied.

2.5. FIRMWARE UPGRADE

If you want to upgrade the firmware version in your router, go to web menu *Admin→Upgrade Firmware*, and browse the path where the FW file is located by pressing *Examinar*:
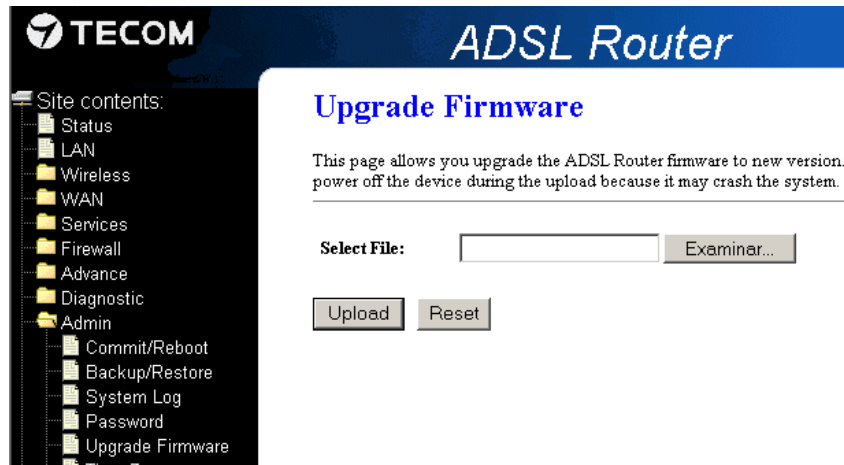
After Browning the file, press "**Upload**" to launch the new firmware file upgrade. After the process is finished, the router will reboot automatically.

IMPORTANT: DO NOT POWER OFF THE ROUTER DURING THIS PROCESS, OR IT

MAY BE LOST SOME CRUCIAL DATA WHICH MAY CAUSE THE SYSTEM CRASH

The process will be finished once you see the frontal LEDs status in green (normal status).

NOTE:

➢ During the FW upgrade, **all LEDs except Ethernet will be blinking in Green at the same time** (if wireless network was disabled before starting the process, the WLAN LED won´t blink either)

➢ After finishing the process, all the LEDs will return to normal status

➢ If during the process the router finds a **recoverable failure** (punctual failure: for instance, if you browse a wrong format file, the system will roll back without affecting the system functioning), all the LEDs except the Ethernet will be **SOLID GREEN during 15 seconds** to show you it happened a failure. After that time, all the LEDs will go back to normal status

➢ If during the process the router finds a **non-recoverable failure** (system failure which cannot be roll back: for instance, corrupt file or disconnection from the power during the process), the **POWER LED** will be **SOLID RED**. In this case happens, you must contact your technical service for repair.