F@ST 4310

Reference Manual

Sagemcom

Sagemcom assiduously monitors technical developments and is constantly seeking to improve its products in order to let its clients take full advantage of them. It therefore reserves the right to modify its documentation accordingly without notice.

All brands mentioned in this guide are registered by their respective owners:

- **F@ST** is a registered trademark.
- **Sagemcom** is a registered trademark.
- **Windows**^{TM} and **Internet Explorer**^{TM} are registered trademarks of Microsoft Corporation.

The purpose of this reference manual is to give users the functions for operating and managing the equipment. The only access level required (**Administrator**) is protected by a password and allows one to access these functions in read and write mode for all the user and network parameters (Login: admin; password: xxxx).

Note
Configuration of the router by HTTP is described in detail (cf. section 5).

To ease legibility of the reference manual, the term "router" will be used throughout the document to designate F@ST 4310 equipment.

Guide to symbols used in this manual

Symbols	Definition
Note	Gives you important information which you must take into account.
Important	Warns you not to do an action, or commit a serious omission.

How should the document be used?

This reference manual is organised into sections and annexes. These sections and annexes cover the following subjects.

Section 1	Presentation of F@ST 4310 equipment
Section 2	Description of F@ST 4310 equipment
Section 3	Installation of F@ST 4310 equipment
Section 4	Configuration of network parameters
Section 5	Configuration of the router by HTTP
Section 6	Configuration of the advanced parameters
Section 6	Description of Internet access service
Section 7	Description of TV over ADSL service
Section 8	Updating the application
Annex A	Troubleshooting
Annex B	EC compliance declaration
Annex C	Environment
Annex D	Technical Characteristics
Annex E	Default configuration
Annex F	Glossary
Annex G	Connector technology

Contents

Pages

1. Introduction

This section covers	• presentation of the F@ST 4310 router	§ 1.1
	• composition of the packaging	§ 1.2
	• required hardware and software	§ 1.3

1.1 Presentation

This reference manual is dedicated to the F@ST 4310 equipment. This equipment is a router which gives users broadband Internet access from their computer or their game console by various Ethernet (10 or 100 BASE-T) or Wi-Fi (IEEE 802.11n) interfaces via an ADSL/ADSL2/ ADSL2+ network.

Using these interfaces, this router enables you both to surf the Internet and to watch television. It also allows give phone calls over the Internet from an IP SIP telephone linked by Wi-Fi to your router.

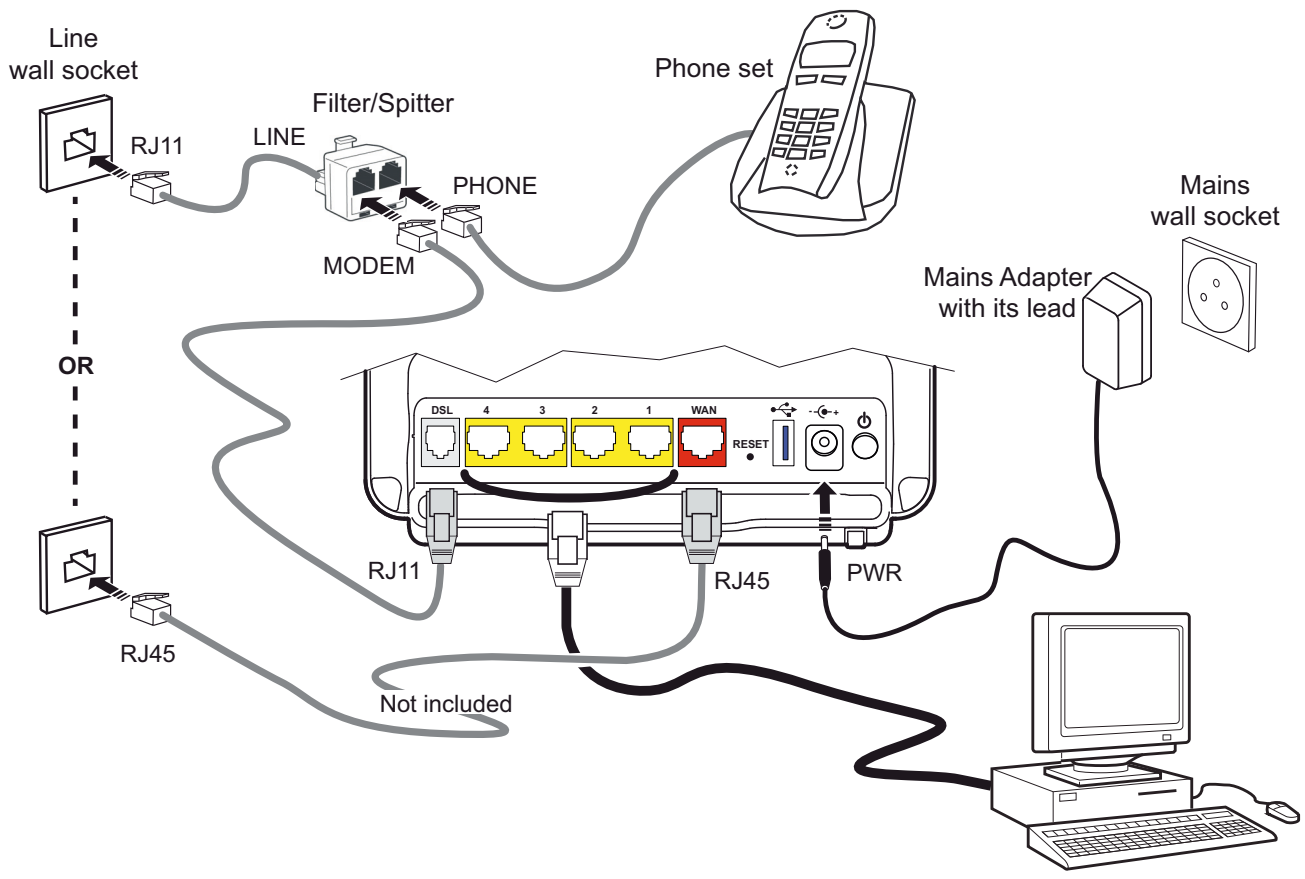
Important

F@ST 4310 products adapt the ADSL function respectively for POTS (UIT G.992.1/3/5 - Annex A) and for ISDN (UIT G.992.1/3/5 - Annex B).

1.1.1 Connection

Connecting your router

Make the connections as shown in the diagram below.



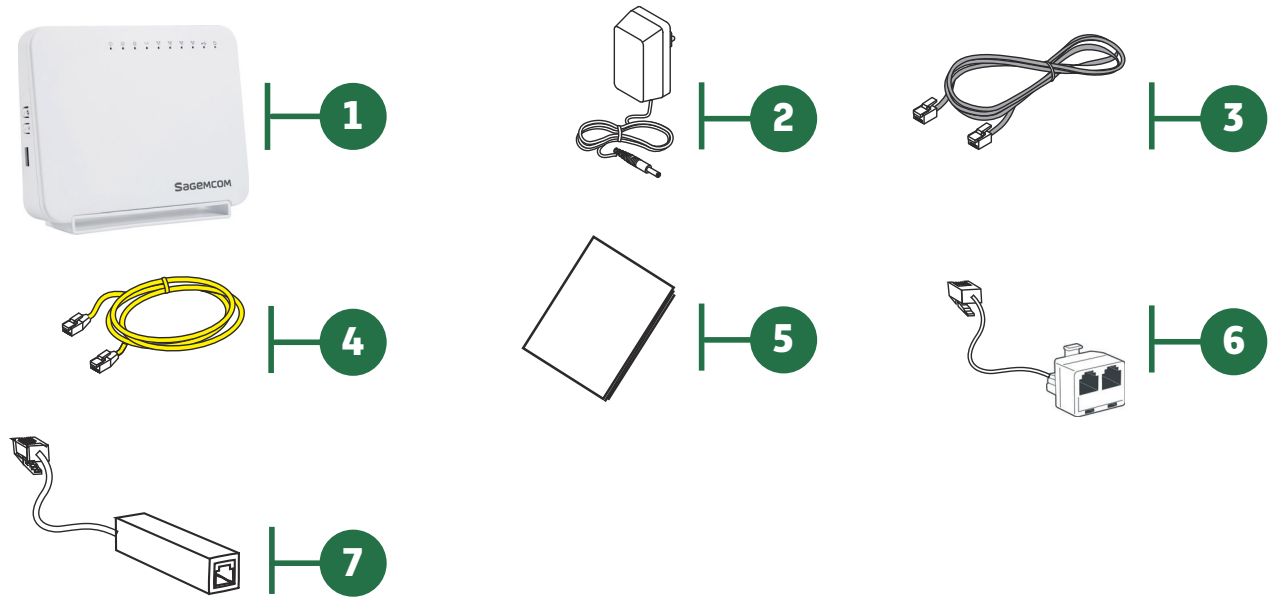
1.1.2 Characteristic

Its principal characteristics and functions are as follows:

- High-performance secure Bridge/Router with ADSL/ADSL2/ADSL2+ and Fast Ethernet (for FTTH) interfaces,
- User access:
  - 4 x 10/100BT Ethernet ports,
  - 1 Wi-Fi interface (802.11n),
  - 2 USB 2.0.,
  - HSDPA backup,
  - Samba server,
  - DLNA server v 1.5.
- DHCP Client/Server/Relay,
- DNS Server/Relay,
- Access control (FTP/TELNET/HTTP/SSH Client),
- NAT/PAT router - FTP Compatibility, IRC, Net2Phone, Netbios, DNS, Netmeeting, VPN passthrough (IPSec, IKE, PPTP, L2TP), CUSeeMe, RealAudio, Microsoft IM and others,
- Security,
- Firewall,
- Spanning tree,
- Multi-VC ATM and ATM Quality of service (CBR, UBR, VBR),
- UPnP,
- TR069,
- QoS,
- Upgrade Firmware (Local and Remote),
- Backup/Restore and Upgrade configuration file (Local and Remote).

1.2 Composition of router pack

The router pack is composed of the following elements (present content may vary):



Item	Description
1	F@ST 4310 router
2	Mains adapter
3	ADSL RJ11/11 FDT line cable (length = 3 m) used to connect your router to your telephone line
4	Ethernet RJ45/RJ45 cable (length = 1.75 m) used to connect your router to the Ethernet port of your computer
5	Quick Installation Guide
6	Filter/Splitter used to connect one phone set and your router to your telephone line*
7	Microfilter used to connect another phone set to your telephone line*
** Option depending on pack content requested*	

Note

Incomplete or damaged supply
If on its receipt the equipment is damaged or incomplete, contact your supplier.

1.3 (Minimum) prerequisites

Using a router requires a minimum of:

- a computer equipped with:
  - a Wi-Fi 802.11n interface,

  or
  - an Ethernet interface (10/100BASE-T).
- a WEB browser (Internet Explorer version 8 or higher recommended, Google Chrome, Firefox, Safari).

The minimum configuration of your computer must be:

- for Windows: Pentium IV, 2,8 GHz, RAM: 1Go,
- for MacOS: Power PC G5, 2,5GHz, RAM: 1Go,
- a monitor of minimum resolution: 1024 x 768.

If you wish to use the Wi-Fi function (standard IEEE 802.11n), you must have the Wi-Fi Standard pack (see Annex G for use of Wi-Fi).

Note

Before installing the router, we advise you to uninstall any modem or other router (for example, an ADSL router).

2. Description and connection of router

This section covers	• the description of your router	§ 2.1
	• connecting the ports of your router	§ 2.2
	• installing your router	§ 2.3
	• installation safety instructions	§ 2.4

2.1 Description

The following figure gives an overview of a router F@ST 4310.

Figure 2.1 - Overview of case

This case consists principally of a lid and a base. Inside is a printed circuit equipped with electronic components.

The front face of the lid has ten display LEDs (see § 2.1.2).
The base has the LED ideograms and the manufacturer logo.

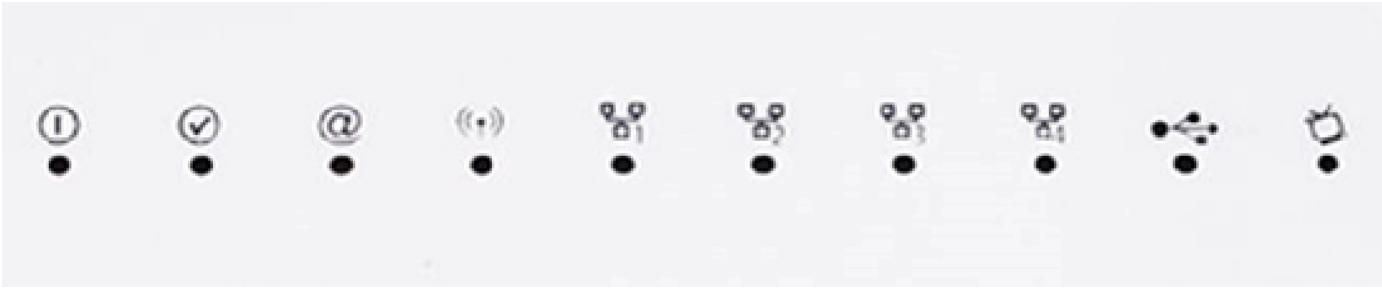
Behind the base is a label on which the product's identification code, serial number and barcode are shown.

2.1.1 Connectors

Marking	Meaning
LINE	RJ11 connector - 6 pts. This connector is identified by the colour grey. It is used for the connection to an ADSL line (WAN interface).
LAN x (1 to 4)	RJ45 connectors - 8 pts (10/100BASE-T Ethernet Interface). These connectors are identified by the colour yellow. They are used to connect to a computer or a television set (via a TV/Video Decoder).
WAN	RJ45 connector - 8 pts (10/100BASE-T Ethernet Interface). This connector is identified by the color red. FTTH dedicated port
RESET	This button allows the router to be reset to the factory configuration (see § A.7). This operation deletes the entire personalised configuration of your router: Password, Configuration, etc..
USB	“Master” USB type A female connector (USB Interface) used for “Memory sharing” and “Printer sharing”
⏻ **Power**	Miniature jack fixed connector. This connector enables the router to be supplied with direct current from a mains adapter unit.

2.1.2 LEDs and buttons

2.1.2.1 On the front panel



The following table describes the meaning of the LEDs on the front panel of the router:

LED	Status	Meaning
Power	**Off**	Power Off
	Green	Power On
	Red	Router in rescue mode
ADSL	**Green steady**	ADSL Up
	Green blinking	• ADSL Synchronisation in progress or • down
Internet	**Off**	• Power Off or • The Internet account must be configured or • Bridge mode
	Green steady	The Internet account is configured
	Green blinking	Tx/Rx traffic
	Red	Invalid or unauthorised Internet account
WLAN	**Off**	Wi-Fi deactivated
	Green steady	Wi-Fi activated
	Green blinking	Wi-Fi Tx/Rx
LAN x (1 to 4)	**Off**	No link detected on the Ethernet port
	Green steady	Ethernet port has detected a link with 100 Mbps device
	Green blinking	Tx/Rx traffic at 100 Mbps
USB	**Off**	No USB connection
	Green steady	USB connection available
	Green blinking	USB connection reading in progress
TV	**Green steady**	activated
	Green blinking	Playing IPTV

2.1.2.2 On the right panel

The following table describes the meaning of the buttons on the right panel of the router:

Button	Action
WPS	This button allows the router to switch to easy-pairing mode.
WLAN	This button allows to activate or deactivate the WiFi connection.

2.2 Connecting the ports of your router

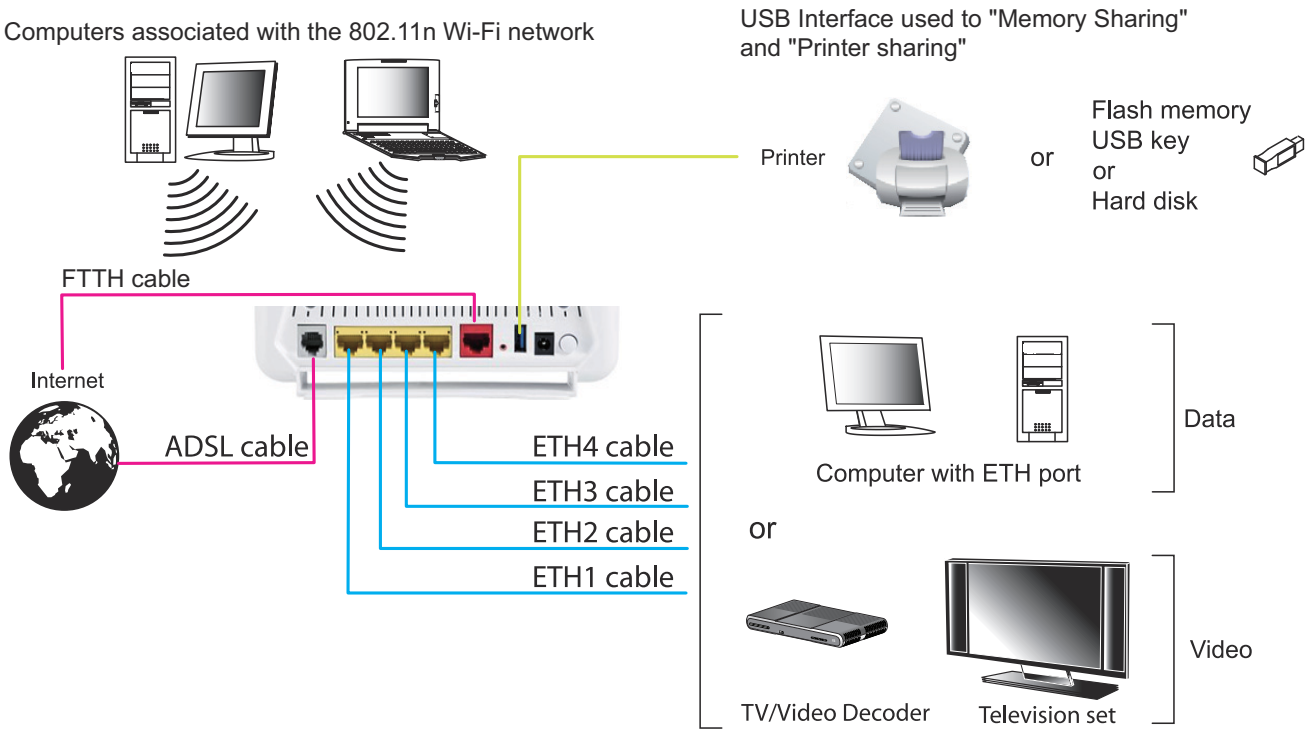


Figure 2.2 - Interconnection of ports of F@ST 4310

2.3 Installation of your F@ST 4310

2.3.1 Powering up

1. First connect the end of the mains adapter lead, supplied with the equipment, to the Power socket on your router.
2. Connect the other end of the mains adapter lead to a nearby power outlet.
3. The router switches on automatically.
4. The LED will light up first, followed by the four Ethernet LEDs (1 to 4), then these last four LEDs will be off. The and Ethernet (which corresponds to the connected interface) LEDs should be steady and the LED blinks during the establishment of the ADSL link, then steadies like the LED. The LED goes from blinking to steady when a PPP session has been created successfully.

Note

The powering up process lasts around one minute.

2.3.2 Connecting the ADSL cable

1. Connect one end of the RJ11/RJ11 cable supplied with the equipment to the LINE socket of your router.
2. Connect the other end of the cable as shown in the following figure.

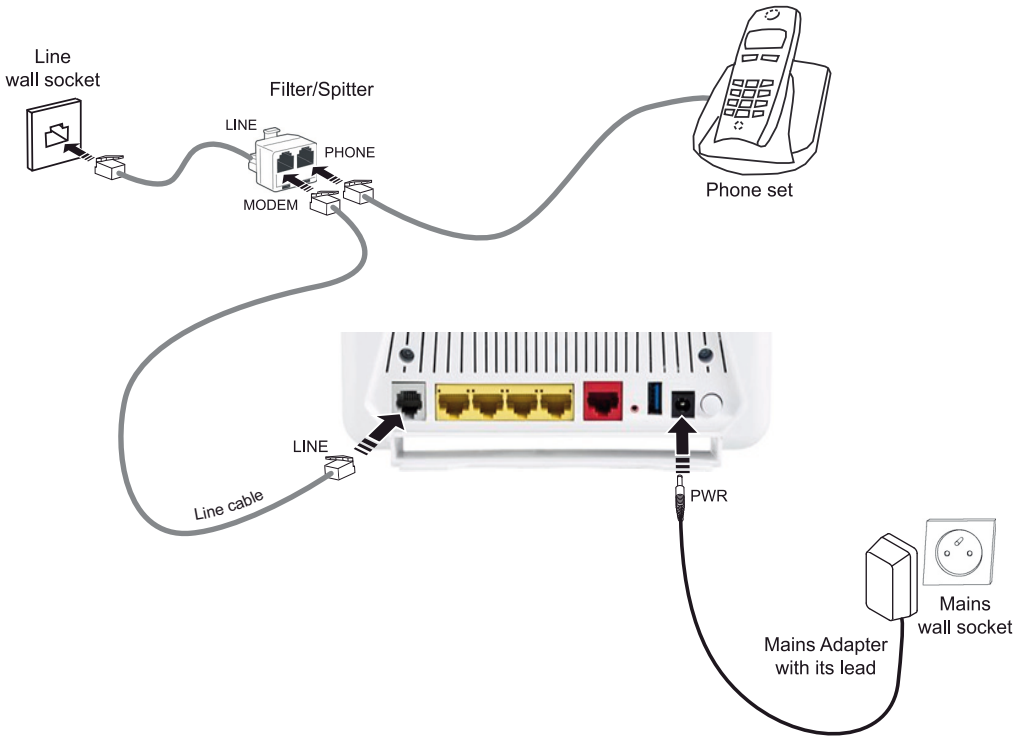


Figure 2.3 - ADSL line / Power Supply Connection

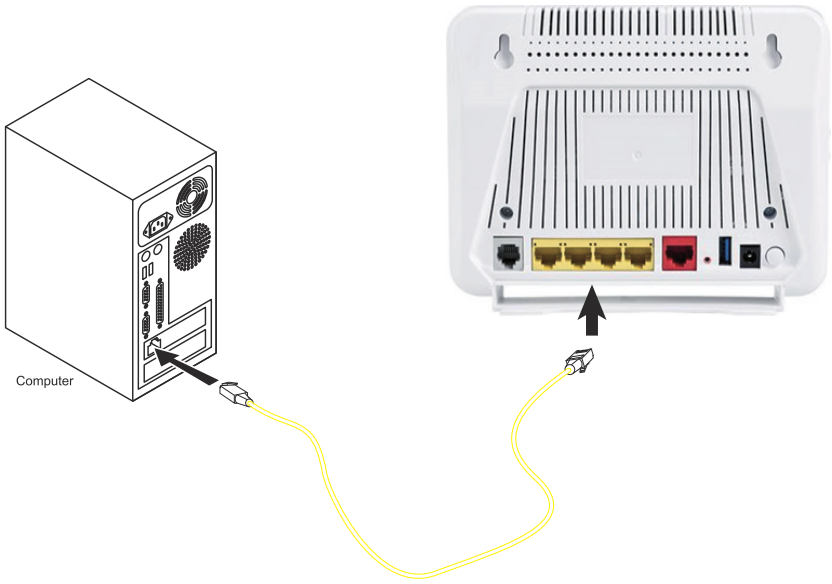
2.3.3 Connecting to your computer

Two kinds of connection can be made:

- Connection of the Ethernet interface of your router to your computer.
- Connection of the WLAN (Wi-Fi) interface to your computer.

2.3.3.1 Connecting the Ethernet interface of your router to your computer

1. Connect the end of the yellow Ethernet cable (RJ45/RJ45) supplied in the pack to the Ethernet fixed connector (marked **LAN1**, **LAN2**, **LAN3** or **LAN4**) of your router.
2. Connect the other end of the cable to your computer.



2.3.3.2 Connecting the Wi-Fi interface of your router to your computer

Wireless linking enables the router to be connected to your computer.

To make this connection you must have a Wi-Fi pack (option). This pack comprises the following elements:

- Wi-Fi 188470912 key (Dongle) in an anti-static plastic bag,
- CD-ROM.

Inserting a USB Wi-Fi key in your computer

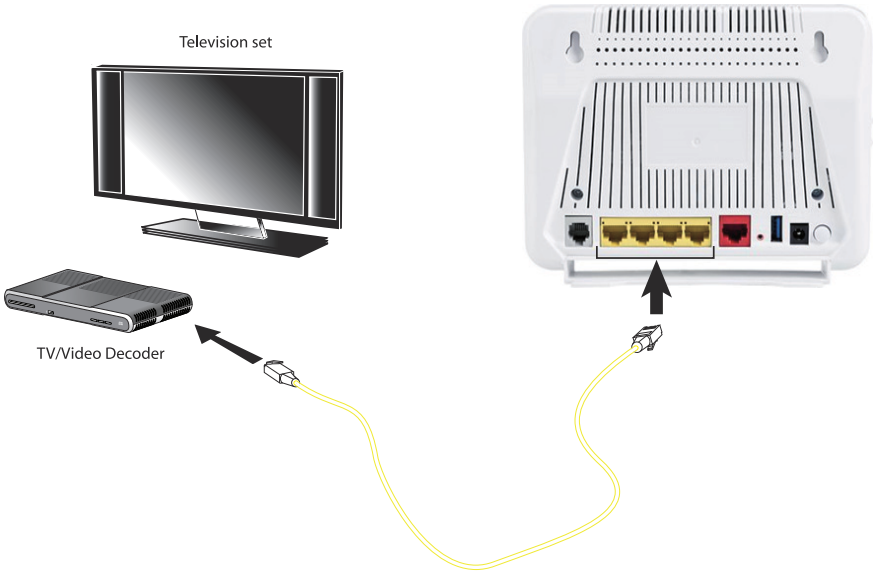
This key should only be connected to your computer during installation of the Wi-Fi drivers (standard 802.11n) (see Quick Installation Guide).

Note

You can also use the Wi-Fi adapter incorporated in your computer.

2.3.4 Connecting the Ethernet interface of your router to your TV decoder

1. Connect the end of the yellow Ethernet cable (RJ45/RJ45) supplied in the pack to the Ethernet fixed connector (marked **LAN1**, **LAN2**, **LAN3** or **LAN4**) of your router.
2. Connect the other end of the cable to a TV decoder.



Note

For connection to the decoder, refer to the manufacturer's documentation.

2.3.5 Connecting the USB interface of your router

1. Connect the end of the USB cable (type B Slave female USB Connector) to the USB interface of your router.
2. Connect the other end of the cable to your USB material (printer, Flash memory, USB key or hard disk).

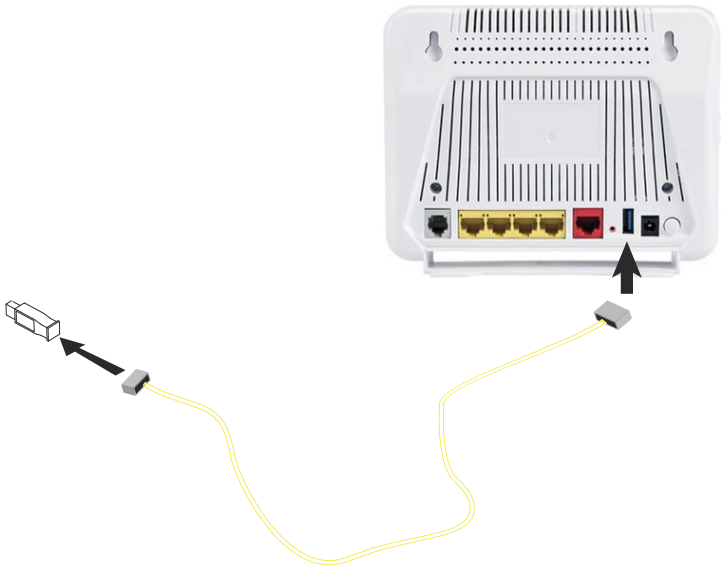


Figure 2.4 - USB Interface Connection

2.4 Installation safety instructions

Power supply source

- Do not cover the router's mains adapter.
- The router comes with its own mains adapter. Do not use another adapter.
- This class II adapter does not need to be grounded (earthed). The connection to the electrical network should comply with the indications given on the label.
- Use a readily accessible mains outlet located near the router. The power supply cord is 1.5 m long.
- Arrange the power supply cord in such a way as to avoid any accidental power cut to the router.
- The router is designed to be connected to a GG- (ground-to-ground) or GN- (ground-toneutral) type power supply network.
- The router is not designed to be connected to an electrical installation with IT type diagram (neutral connected to earth through an impedance).
- Protection against short-circuits and leaks between the phase, neutral and earth should be provided by the building's electrical installation. The power supply circuit for this equipment should be fitted with 16 A overcurrent protection and differential protection.
- Connect the router to the mains via a readily accessible wall socket ensuring the electric cutting.

Location conditions

By choosing an appropriate location, you will preserve the longevity of the device. Ensure that the selected location has the following characteristics:

- Install and use the router inside a building.
- The room temperature must not exceed 45°C.
- The router can be placed on a desktop or fixed vertically in its wall mounting.
- Do not expose the router to strong sunlight or place it near a substantial source of heat.
- Do not place the router in an environment where it could be subjected to considerable steam condensation.
- Do not expose the router to splashes of water.
- Do not cover the router's casing.
- Do not use the router or its peripherals for outdoor transmissions.

Maintenance

- Never open the casing. This must be done only by qualified personnel approved by your supplier.
- Do not use liquid or aerosol cleaning agents.

3. Installing and configuring the F@ST 4310 router

For the installation of the F@ST 4310,
please refer to the Quick Installation Guide of this product.

4. Configuration of network parameters

This section covers	• configuring as a DHCP client	§ 4.1
	• reading status of the DHCP server	§ 4.2
	• reading data of the DHCP client	§ 4.3

The aim of this section is:

1. to configure your computer so that it is able to communicate with your router.
2. to display the "Networks" parameters of your router.

Your router implements the DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol) server, relay and client functions in accordance with RFC 2131 and RFC 3132, whereas the computer connected directly to the router or via a local network by its LAN interface implements only the DHCP client function.

On receipt of a DHCP query from your computer (see ), whether or not it is connected to your router, the latter responds by indicating:

- an address from the range defined in the configuration,
- the sub-network mask,
- the default gateway (address of your router),
- the address of the gateway as DNS server. The "DNS Relay" function is activated automatically.

Note

The configured range of IP addresses must be the same in the sub-network as in the LAN interface.

Important

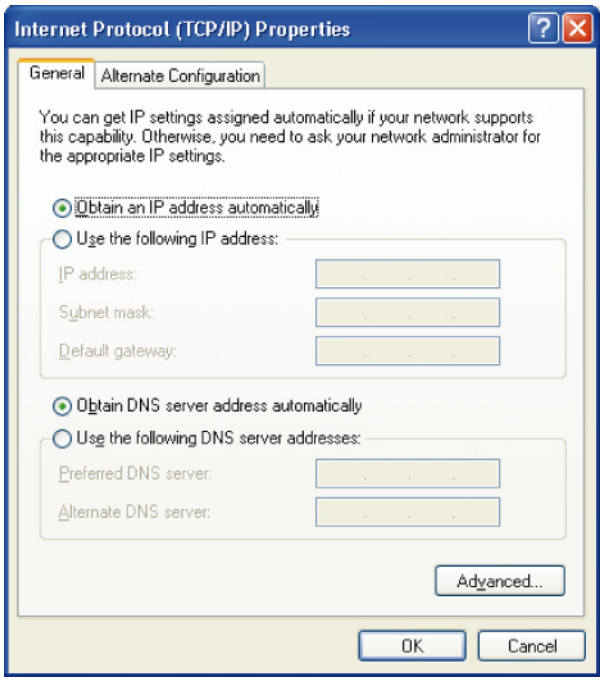
It is imperative that your computer is configured as a DHCP client or that it has a fixed IP address in the configuration range defined by the DHCP server.

Configuration as a DHCP client is the more commonly used solution.

4.1 Configuring as a DHCP client

In Windows XP

1. Click on **Start > Control Panel > Network Connections**.
2. Right-click the appropriate network, and then select **Properties**.
   The Local Area Connection Properties appears.
3. Select the protocol TCP/IP of the network card, and then click the **Properties** button.
   The screen Internet Protocol (TCP/IP) Properties appears.
4. Select the **General** tab, then the case "**Obtain an IP address automatically**" and the case "**Obtain the addresses of the DNS servers automatically**".
5. Click the **OK** button to confirm your choice.



4.2 Status of the DHCP server

To obtain the status of the DHCP server:

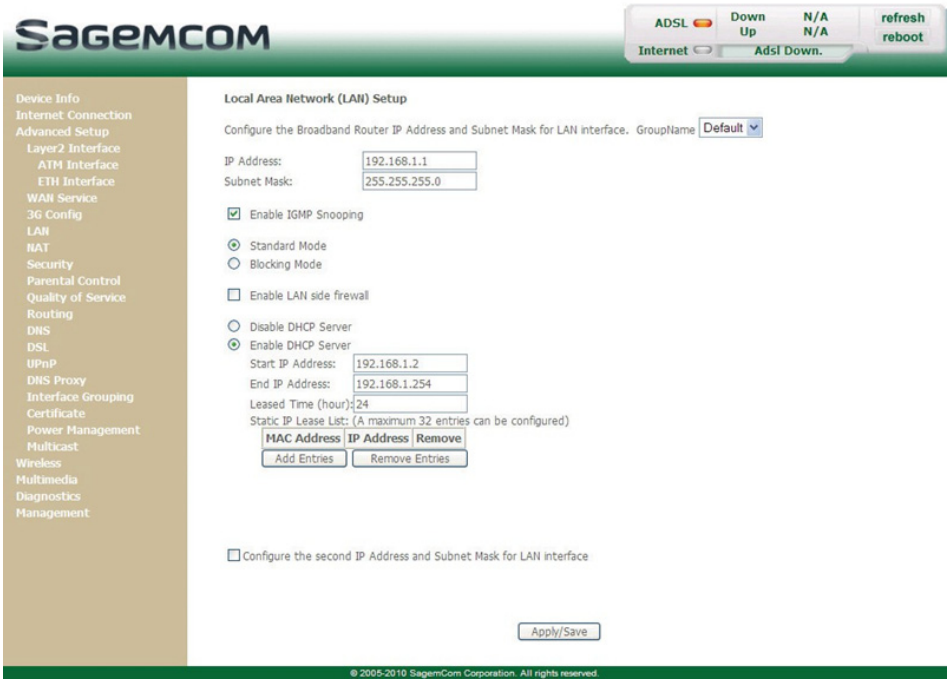
1. Open your browser.
2. Enter the router's IP address (by default **http://192.168.1.1**) or enter the following URL http://myrouter
3. In the login screen that appears, enter "**admin**" in the "User Name" field and the "Password" field (see note).

Note

The User name and Password values are written on the label.

4. Click on the **OK** button to validate.
5. Select **Advanced Setup** menu, then select the **LAN** menu.

   The following screen appears:



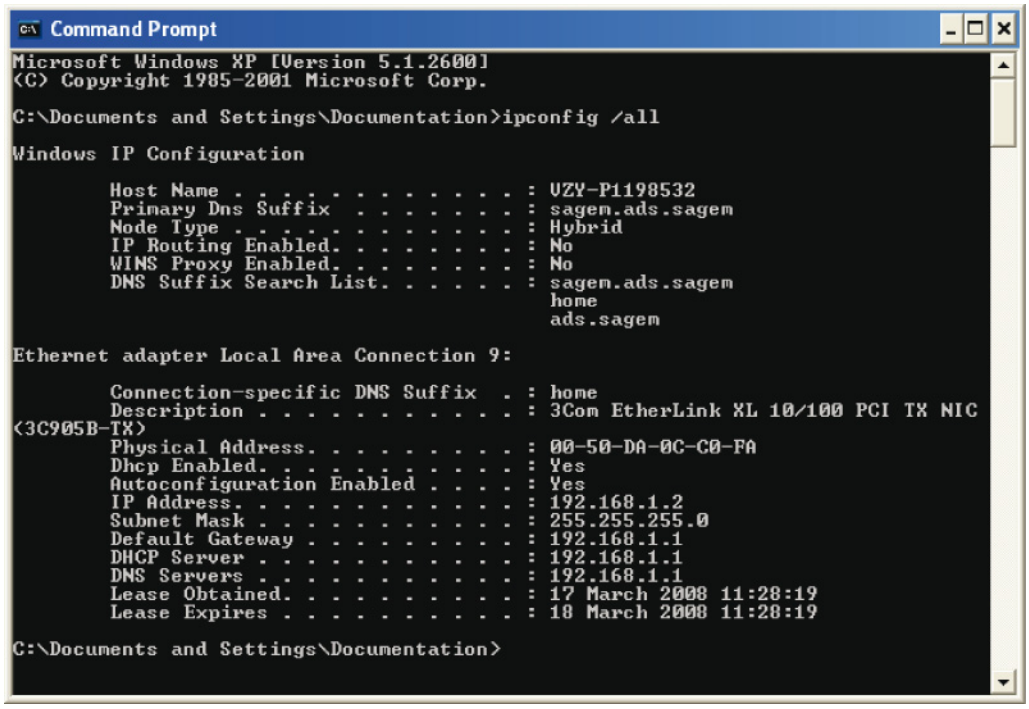
Field	Description	Display
IP Address	Displays the sub-network address.	192.168.1.1
Subnet Mask	Displays the sub-network mask of the IP network.	255.255.255.0
Start IP Address	Displays the first address attributed by the DHCP server. **Note:** This IP address must belong to the same sub-network as that of the local network.	192.168.1.2
End IP Address	Displays the last address attributed by the DHCP server. **Note:** This IP address must belong to the same sub-network as that of the local network.	192.168.1.254
Leased Time (hour)	Displays the period (in hours) for obtaining an IP address for a terminal.	24

4.3 Data of the DHCP client

To obtain this data:

In Windows XP

1. Click on **Start > Run**, enter **cmd** and then click **OK**.
   The command prompt screen appears.
2. Enter **ipconfig /all** (or **ipconfig/all**) then press **Enter**.



5. Information / Configuration

This section covers	• Accessing the welcome screen	§ 5.1
	• Recommendations for using the configuration screens	§ 5.2
	• The ADSL connection status	§ 5.3
	• Indications displayed on the display frame located in the HTTP configurer window	§ 5.4
	• The ”Device Info” section	§ 5.5
	• The ”Internet Connection” section	§ 5.6
	• The ”Advanced Setup” section	§ 5.7
	• The ”Wireless” section	§ 5.8
	• The "Multimedia" section	§ 5.9
	• The ”Diagnostics” section	§ 5.10
	• The ”Management” section	§ 5.11

5.1 Accessing the welcome screen

Note

To access this screen, you must have configured one of your computer's interfaces using the installation CD-ROM provided with your router (see section 3.).

If you are using your computer's Ethernet card to configure your router, connect it to an Ethernet port (**LAN1** to **LAN4**).

Your router is then configured using a simple Web browser (e.g. Internet Explorer).

Note

The router's DHCP server function is activated by default with an address range defined as indicated in subsection.6.4.4.

To access the configurer, proceed as follows:

To obtain the status of the DHCP server:

1. Click on Start > All Programs > F@ST 4310 > **Configuration**.
2. In the login screen that appears, enter your identification information.
   By default, the identification information is:

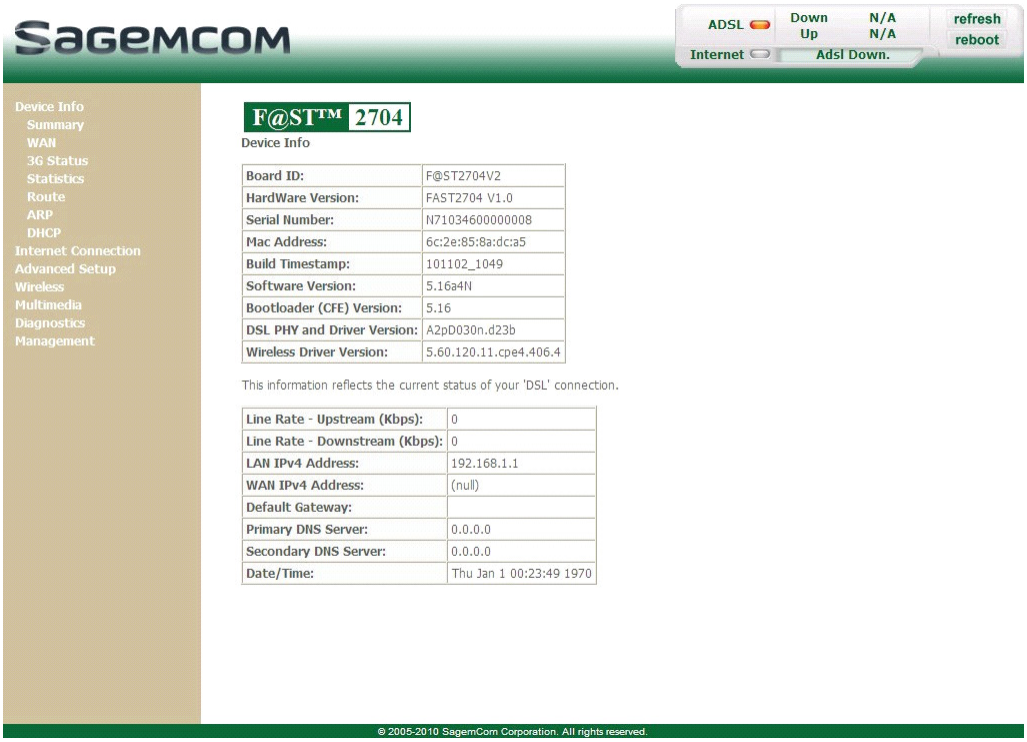
Username:	admin
Password:	(see on the label)

Note

The equipment's IP address (192.168.1.1) appears in the header bar.

3. Click on **OK** to validate.

4. Your computer's Web browser opens and displays the welcome screen of the router's HTTP configuration tool..
The configuration menus appear on the left hand side panel.



The HTTP configuration tool opens by default on the Device Info menu:

- the centre panel shows router's information and the current ADSL connection status (see subsection 5.3).
- the router's activity and status is always available at the top right corner, as a box which lets you know the status of the ADSL line, lets you refresh the data displayed and restart your router at any time (see subsection 5.4).

  left hand side panel gives you access to the router's configuration menus and submenus (see subsection 5.5 to 5.11).

Note

You can modify the password to access your router's configuration tool to optimise the safety of your network.

5.2 Recommendations

The meaning of the main buttons most commonly present in all the configuration windows is provided in the table below.

Button	Description
Add	Click on this button to add a new window to fill in the fields used to add an object.
Back	Click on this button to return to the previous screen.
Close	Click on this button to close the active window and return to the main screen.
Edit	Click on this button to display a new window to modify the fields that can be accessed for a previously selected object.
Next	Click on this button to display the next screen.
Remove	Click on this button to remove a selected object from a list. **Note:** You must check the "Remove" box to delete this object.
Save	Click on this button to save the entry in the router's non-volatile (flash) memory. **Note:** This value will only be taken into account when you restart your router.
Apply/Save	Click on this button to save the entry in the router's non-volatile (flash) memory. **Note:** This value will be taken into account immediately without you having to restart your router.
Save/Reboot	Click on this button to save the entry in the router's non-volatile (flash) memory then restart your computer.

Basic principles

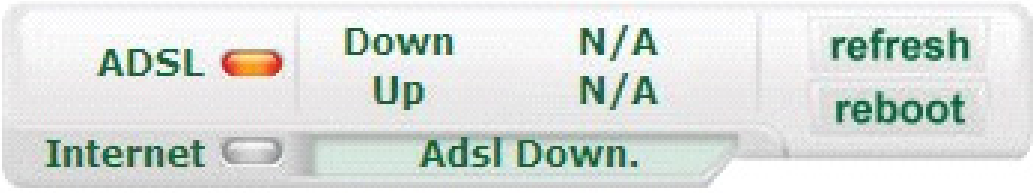
1. To make this guide easier to read and understand, it does not state that each time you enter information into a screen you must click on **Save** or **Apply/Save** or **Save/Reboot** (except, of course, if this is necessary).
2. When you select a section, the screen for the first menu in the section is displayed. In the same way, when you select a menu, the screen for the first sub-menu is displayed.
3. All the fields in the different screens are explained in a table.

5.3 ADSL connection status

Refer to subsection 6.2.1 - **/Summary**.

5.4 Display frame

The router's activity status is always visible at the left corner or the top right of the HTTP configuration tool.



You can perform the following actions:

- click on **Refresh** to update the data displayed
- click on **Reboot** to restart your router

ADSL information

The following table presents the possible states of the **ADSL** field:

Status	Meaning
Green	ADSL line synchronised
Yellow	ADSL line synchronising
Red	ADSL line not connected

The **Down** field displays the nominal downlink bit rate.

The **Up** field displays the nominal uplink bit rate.

Internet information

The following table presents the possible states of the **Internet** field:

Status	Status	Meaning
Off	**ADSL Down**	ADSL line not connected or not activated
	Not configured	The Internet account must be configured
	Router rebooting	Router is rebooting
Green	**Connected**	The Internet connection has succeeded
Yellow	**Waiting for ISP**	Connecting to the Internet service
Red	**Access denied**	Incorrect Internet account

5.5 Device Info

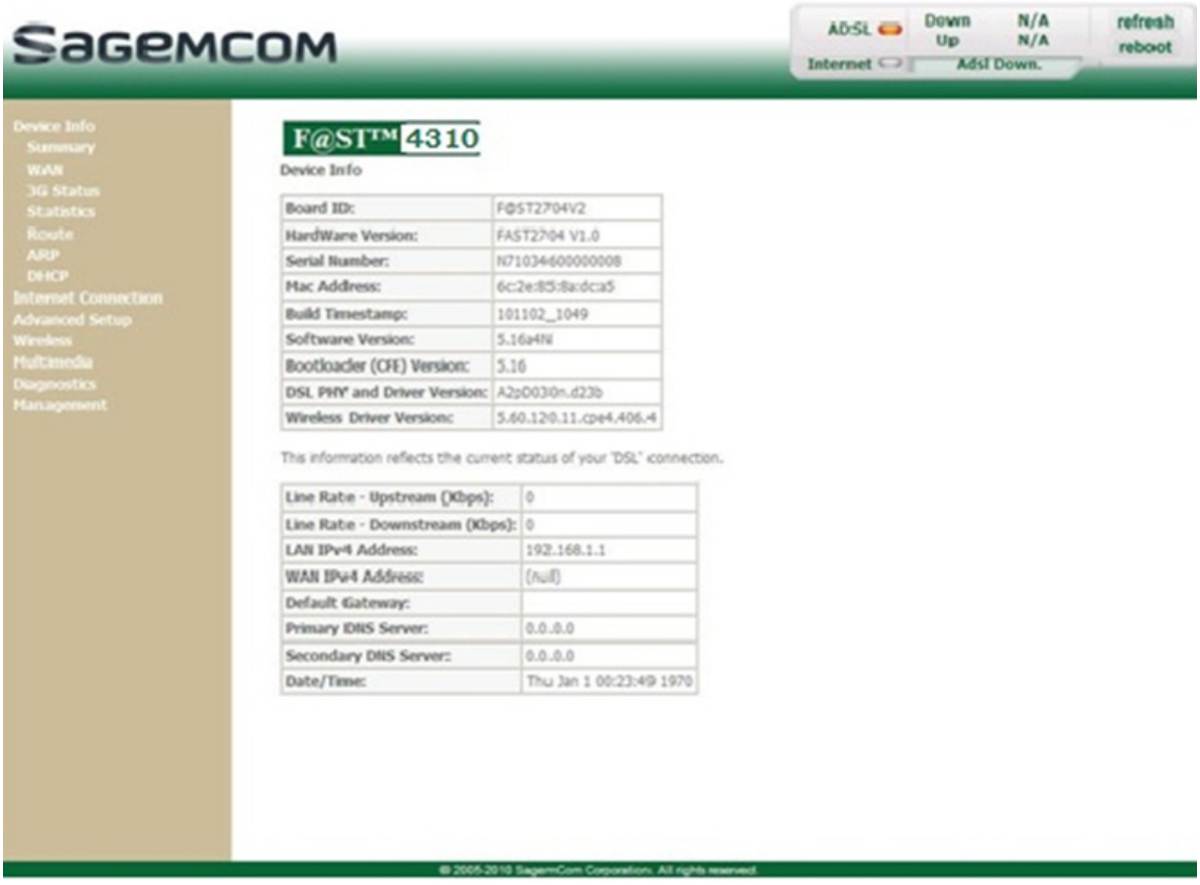
Clicking on this heading displays the following menus:

- Summary (see subsection 5.5.1)
- WAN (see subsection 5.5.2)
- 3G Status (see subsection 5.5.3)
- Statistics (see subsection 5.5.4)
- Route (see subsection 5.5.5)
- ARP (see subsection 5.5.6)
- DHCP (see subsection 5.5.7)

5.5.1 Summary

Object: This menu lets you display the current status of your Internet connection.

- In the **Device Info** menu, select **Summary**.
  The following screen opens:



Note

This screen also appears in the welcome screen (see subsection 5.1).

The following table provides the meaning of the different fields which are displayed.

Field	Meaning
Board ID	Router model
HardWare Version	Hardware version of the router
Serial Number	Serial number of the router
Mac Address	Mac address of the router
Software Version	Software version currently installed on the router
Bootloader (CFE) Version	Bootloader version currently installed on the router
Wireless Driver Version	Software version of the wireless card installed on the router
Line Rate - Upstream (kbps)	Nominal up line rate
Line Rate - Downstream (kbps)	Nominal down line rate
LAN IPv4 Address	Local network IPv4 address (LAN)
WAN IPv4 Address	Remote network IPv4 address (WAN)
Default Gateway	Default gateway address
Primary DNS Server	Primary DNS server address
Secondary DNS Server	Secondary DNS server address
LAN IPv6 ULA Address	Local network IPv6 address (LAN)
Default IPv6 Gateway	Default gateway IPv6 address

5.5.2 WAN

Object: This menu is used to display all the parameters which concern the remote network.

- In the **Device Info** menu, select **WAN**.
  The following screen opens:

5.5.3 3G Status

Object: This menu is used to display all the parameters which concern 3G connection.

- In the **Device Info** menu, select **3G Status**.
  The following screen opens:

5.5.4 Statistics

Object: This menu is used to display all the router's statistics.

This menu contains the following sub menus:

- LAN (see subsection 5.5.4.1)
- WAN Service (see subsection 5.5.4.2)
- xTM (see subsection 5.5.4.3)
- xDSL (see subsection 5.5.4.4)

5.5.4.1 LAN

Object: This menu is used to display all the parameters which concern the local network (LAN).

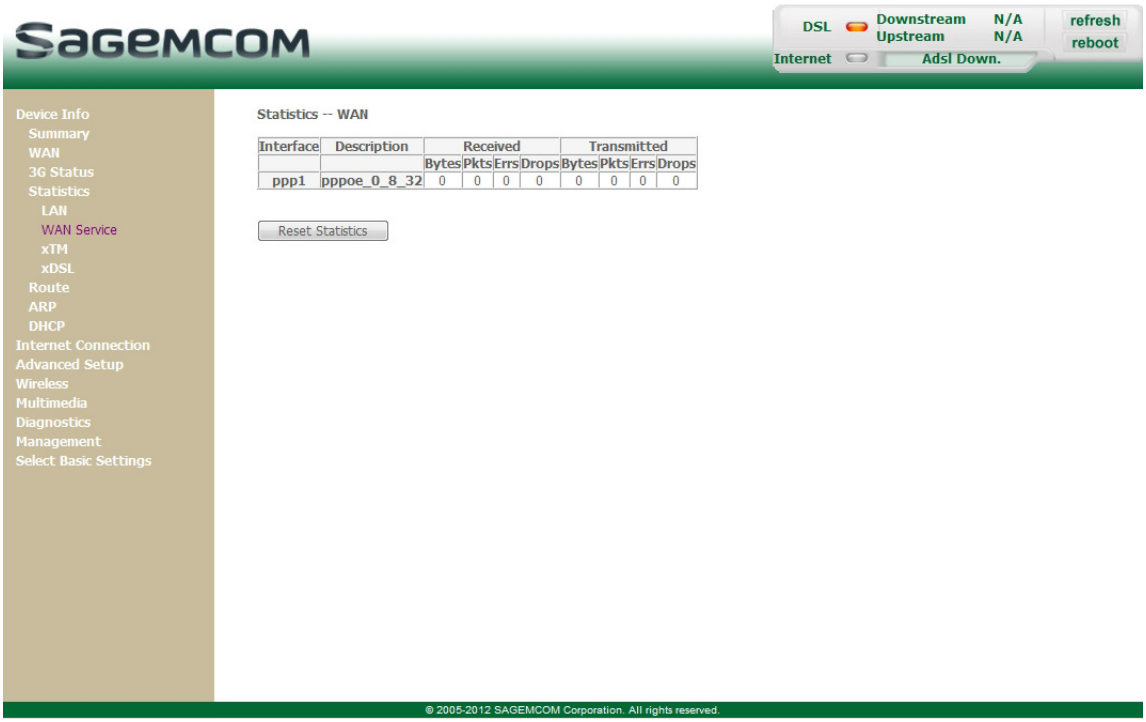
- In the **Device Info** menu, select **Statistics** then select **LAN**.
  The following screen opens:

- Click on the **Reset Statistics** button to reset statistics.

5.5.4.2 WAN Service

Object: This menu is used to display all the parameters which concern the remote network (WAN).

- In the **Device Info** menu, select **Statistics** then select **WAN Service**.
  The following screen opens:

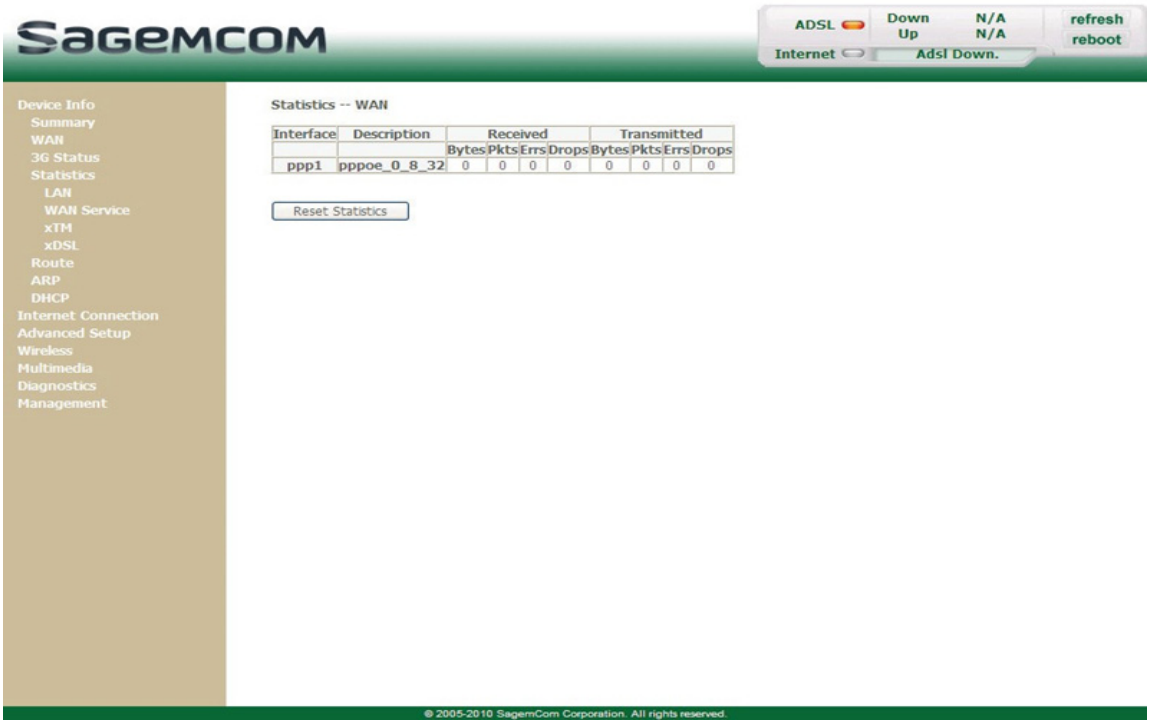


- Click on the **Reset Statistics** button to reset statistics.

5.5.4.3 xTM

Object: This menu is used to display all the xTM statistics of the line.

- In the **Device Info** menu, select **Statistics** then select **xTM**.
  The following screen opens:

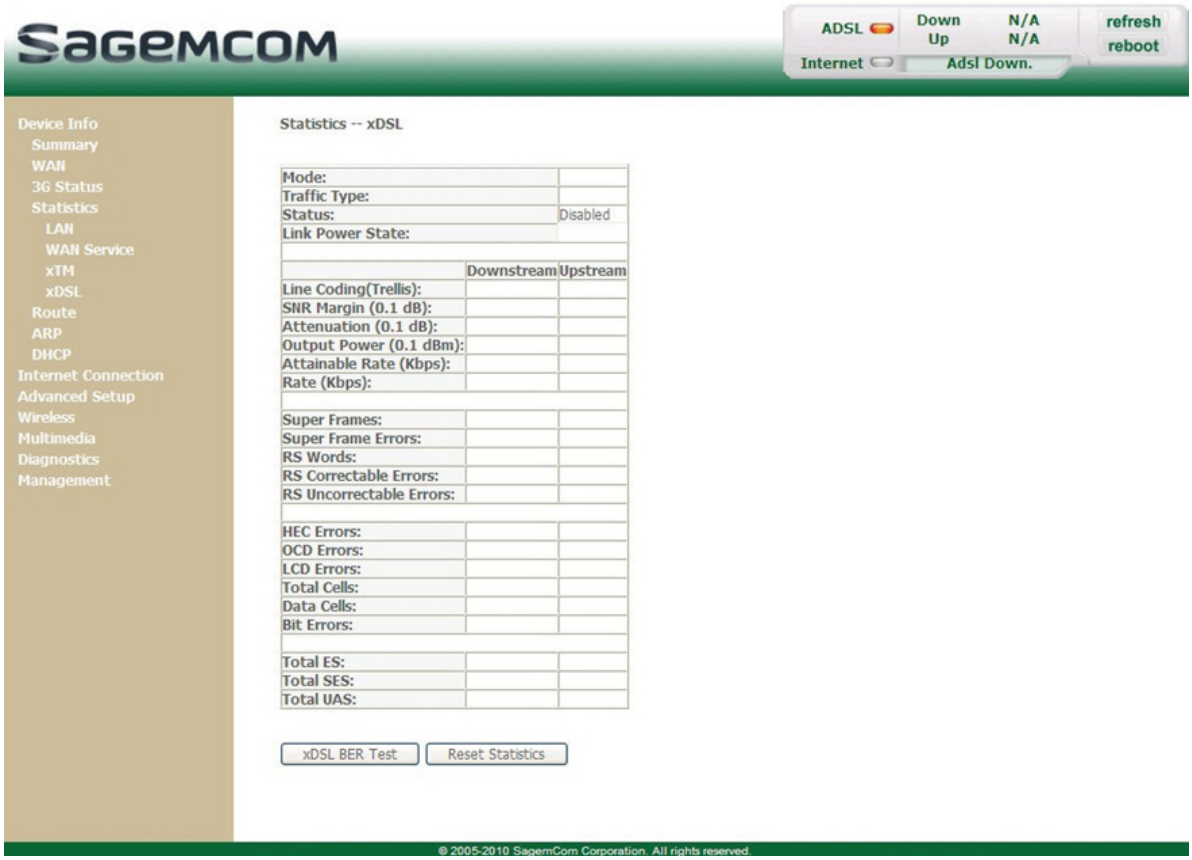


- Click on the **Reset** button to reset statistics.

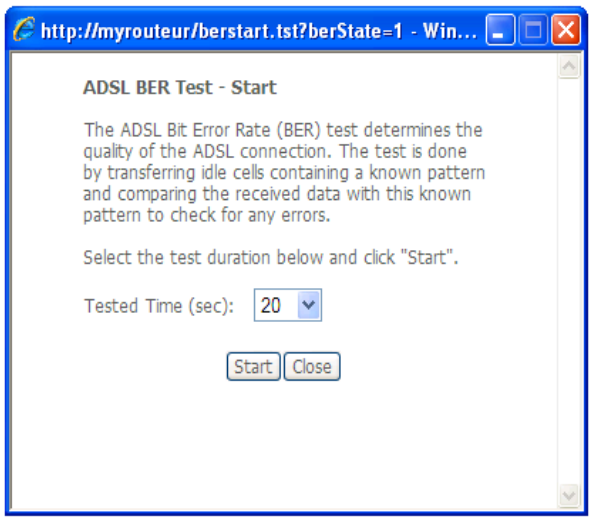
5.5.4.4 xDSL

Object: This menu is used to display all the xDSL statistics of the line.

- In the **Device Info** menu, select **Statistics** then select **xDSL**.
  The following screen opens:



- Click on the **Reset Statistics** button to reset statistics.
- Click on the **xDSL BER Test** button to display the following screen:

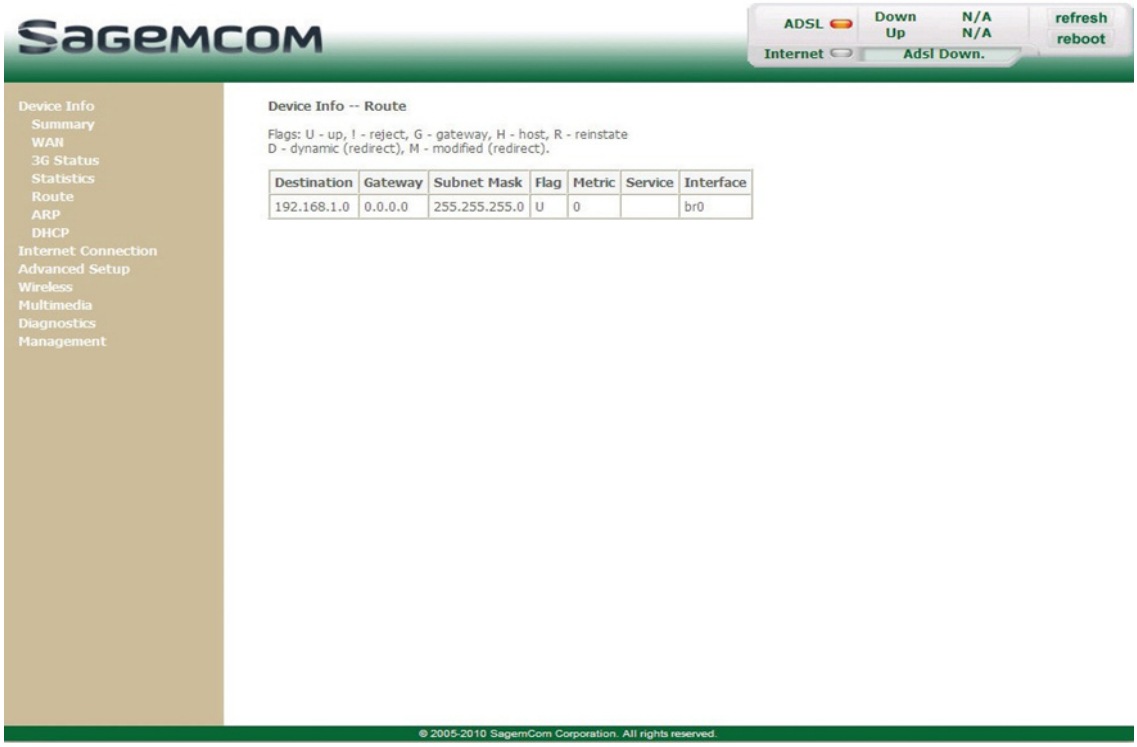


- In the **Tested Time (sec)** field, select the test time from the scroll down list.
- Click on the **Start** button to run the test. The results are displayed once the tests are completed.
- Click on the **Close** button to close the window and return to the previous screen.

5.5.5 Route

Object: This menu is used to display all the information concerning your router's routing.

- In the **Device Info** menu, select **Route**.
  The following screen opens:

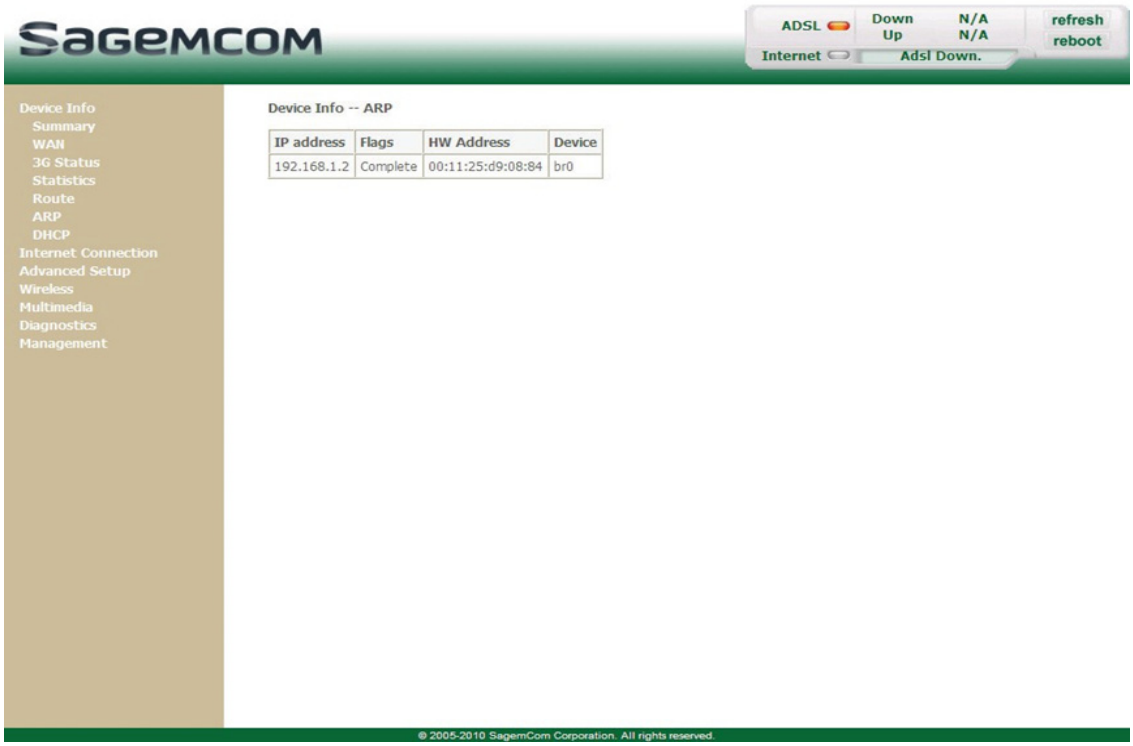


5.5.6 ARP

Object: This menu is used to display all the information concerning address resolution (ARP: **A**ddress **R**esolution **P**rotocol). This shows the physical address of a computer's network card, corresponding to an IP address.

- In the **Device Info** menu, select **ARP**.

  The following screen opens:

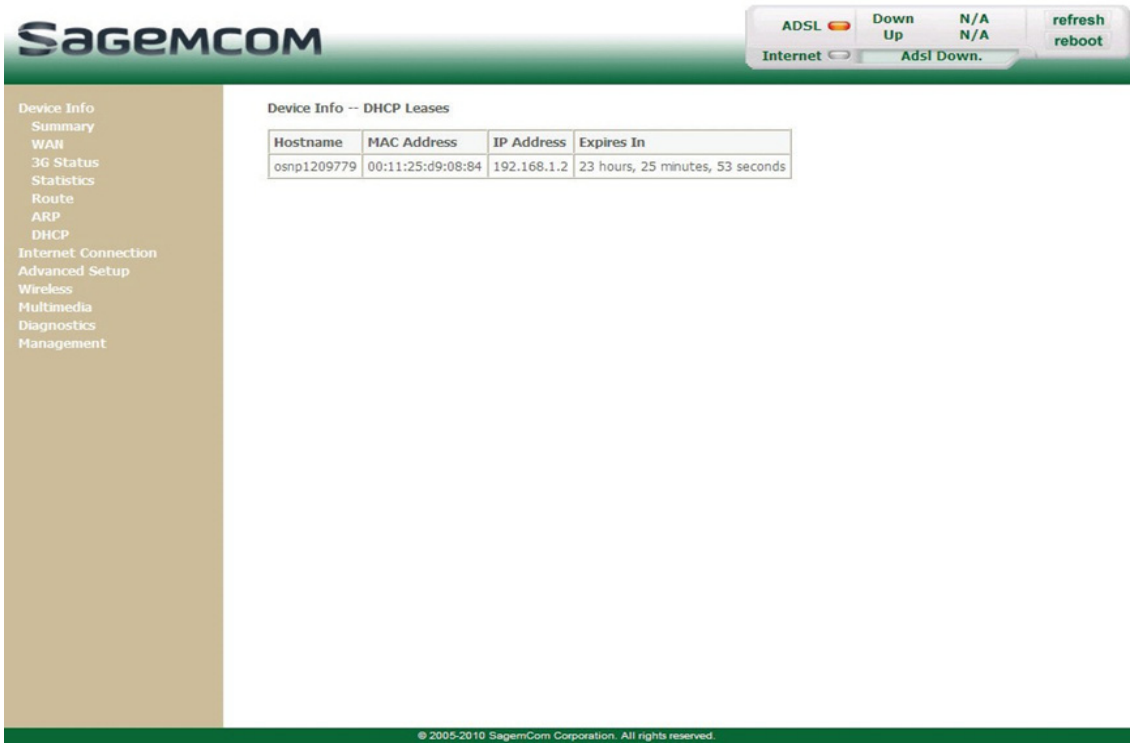


5.5.7 DHCP

Object: This menu is used to display all the computers which obtained an IP address from the router's DHCP server.

- In the **Device Info** menu, select **DHCP**.

  The following screen opens:



5.6 Internet Connection

Object: This menu lets you enter your connection ID and your connection password.

- Select the **Internet Connection** menu.
  The following screen opens:

Field	Action	Default value
PPP Username	Enter your connection ID. This information is provided to you by your **I**nternet **S**ervice **P**rovider (**ISP**).	-
PPP Password	Enter your connection password. This information is provided to you by your **I**nternet **S**ervice **P**rovider (**ISP**).	-

Important

If the message "**There is no ppp connection**" appears, this means that the remote network (WAN) parameters have not been filled in (see subsection 5.7.2 - **Advanced Setup > WAN Service**).

Disconnect

When you click on the button **Disconnect**:

- **Internet access is no longer possible**.
- In the supervision box, the "**Internet**" indicator switches off and the message "**Connected**" is replaced by "**PPP disconnected**".
- On the front panel of the router, the indicator @ **goes out**.

5.7 Advanced Setup

Object: This menu is used to configure the specific parameters for your router.

Important

This menu must only be used by experienced users.

This section contains the following menus:

- Layer2 Interface (see subsection 5.7.1)
- WAN Service (see subsection 5.7.2)
- 3G Config (see subsection 5.7.3)
- LAN (see subsection 5.7.4)
- NAT (see subsection 5.7.5)
- Security (see subsection 5.7.6)
- Parental Control (see subsection 5.7.7)
- Quality of Service (see subsection 5.7.8)
- Routing (see subsection 5.7.9)
- DNS (see subsection 5.7.10)
- DSL (see subsection 5.7.11)
- Upnp (see subsection 5.7.12)
- DNS Proxy (see subsection 5.7.13)
- Interface Grouping (see subsection 5.7.14)
- Certificate (see subsection 5.7.15)
- Power Management (see subsection 5.7.16)
- Multicast (see subsection 5.7.17)

Note

The menu **Quality of Service** only appears if you checked the "Enable Quality Of Service" box in the WAN interface configuration screen (see **Advanced Setup>WAN Service** - subsection 5.7.2>**Add**).

5.7.1 Layer2 Interface

Object: This menu is used to configure DSL interfaces.

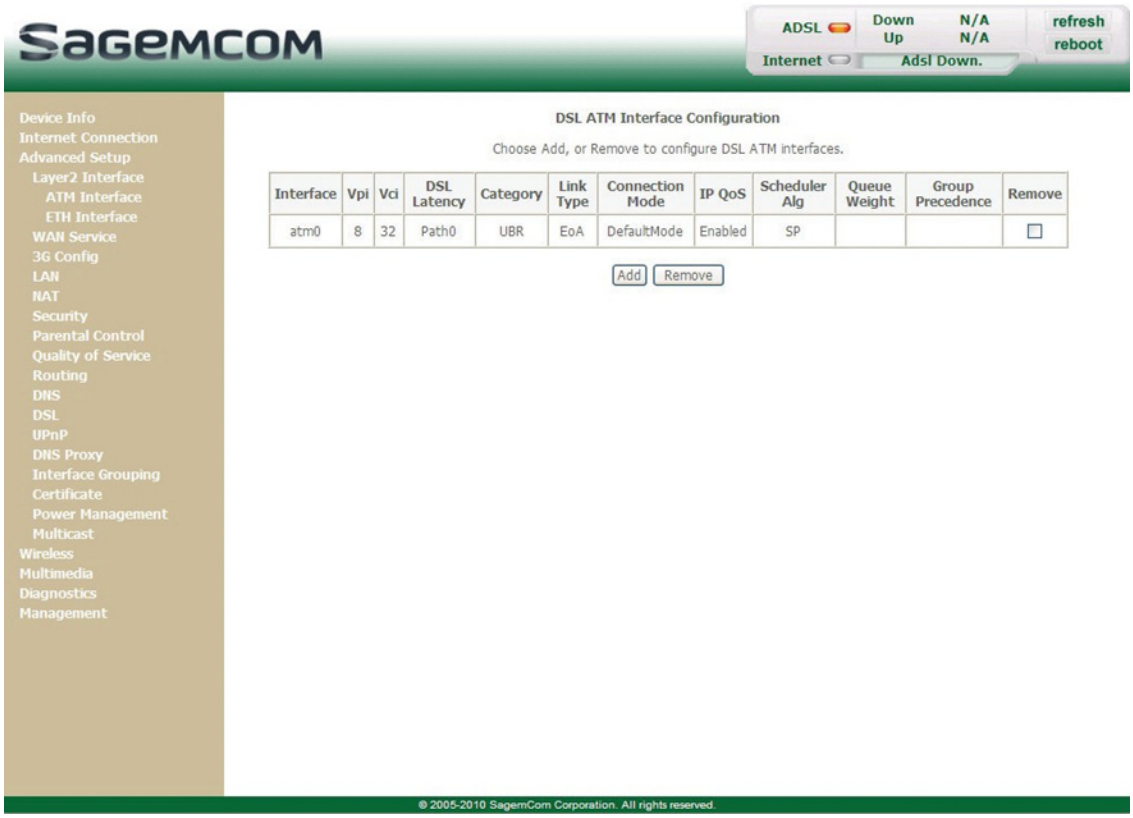
This section contains the following menus:

- ATM Interface (see subsection 5.7.1.1)
- ETH Interface (see subsection 5.7.1.3)

5.7.1.1 ATM Interface

Object: This menu is used to configure DSL ATM interfaces.

- In the **Advanced Setup** menu, select **Layer2 Interface** then **ATM Interface**.
  The following screen opens:

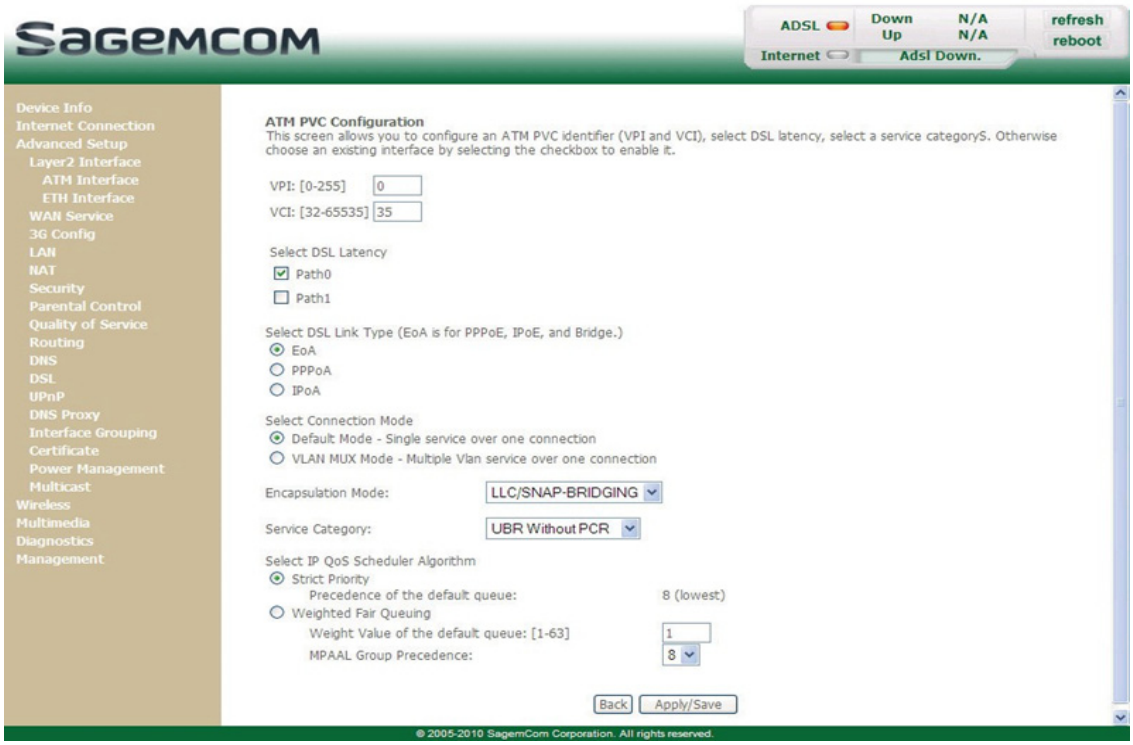


Field	Meaning
Interface	Name of the DSL ATM interface, allocated automatically.
Vpi	Value of the VPI.
Vci	Value of the VCI.
DSL Latency	DSL Latency.
Category	Type of service adapter to the traffic.
Link Type	Protocol used in the DSL ATM interface.
Connection Mode	Connection mode (Default mode, VLAN MUX Mode or MSC Mode).
IP Qos	Status (Enabled or Disabled) of the Quality of Service function.

Field	Meaning
Scheduler Alg	Value defined to perform multitasking (execute more than one process at a time) and multiplexing (transmit multiple flows simultaneously).
Queue Weight	Value defined to give the queue a priority (called a weight) versus the other queues.
Remove	Check this box and click on the [**Remove**] button to remove the selected object from the list.

5.7.1.2 Add

- Click on the **Add** button to display the following screen:



ATM PVC Configuration

Field	Action	Default value
VPI	Enter a VPI value[a] between 0 and 255.	**0**
VCI	Enter a VPI value[a.] between 32 and 65535.	**32**
Select DSL Latency	Select the DSL Latency: • Path0 • Path1	

Field	Action	Default value
Select DSL Link Type	Select the type of network protocol from the scroll down list: • **EoA**: **E**thernet **o**ver **A**TM • **PPPoA**: **PPP o**ver **A**TM • **IPoA**: **IP o**ver **A**TM **Note:** EoA is for PPPoE and IPoE.	**EoA**
Select Connection Mode	Select the connection mode: • Default Mode - Single service over one connection • VLAN MUX Mode - Multiple Vlan service over one connection For more details, a summary table is presented below for each type of protocol.	
Encapsulation mode	Select the encapsulation mode for the selected DSL link type. For more details, a summary table is presented below for each type of protocol.	**LLC/SNAP - BRIDGING**
Service Category	Select the type of service adapter to the traffic from the scroll down list: • UBR without PCR: **U**nspecified **B**it **R**ate • UBR with PCR: **U**nspecified **B**it **R**ate • CBR: **C**onstant **B**it **R**ate • Non Realtime VBR: **V**ariable **B**it **R**ate • Realtime VBR: **V**ariable **B**it **R**ate	**UBR without PCR**
Select IP QoS Scheduler Algorithm	• Strict Priority -Precedence of the lowest queue: • Weighted Fair Queuing -Weight Value of the default queue: [1-63] -MPAAL Group of Precedence:	**8 (lowest)** **1** **8**
Peak Cell Rate[b]	Enter a maximum number of cells transmitted per second, between 1 and 2491.	**-**
Sustainable Cell Rate[c]	Enter an average number of cells transmitted per second. **Note:** This number must be lower than the **P**eak **C**ell **R**ate (PCR).	**-**
Maximum Burst Size[c.]	Enter the maximum number of cells emitted in burst (value between 1 and 1000 000).	**-**

a. This value is delivered to you by your Internet Service Provider (ISP).
b. This field only appears when the "UBR with PCR", "CBR", "Non Realtime VBR" or "Realtime VBR" type of service is selected.
c. These fields only appear when the "Non Realtime VBR" or "Realtime VBR" type of service is selected.

Select Connection Mode

The Connection Mode selection only appears if you have selected the EoA DSL link type.

Field	Action	Default value
Default mode	Check this box to configure a single service over one connection.	**Checked**
VLAN MUX Mode	Check this box to configure Multiple Vlan service over one connection.	**Not checked**

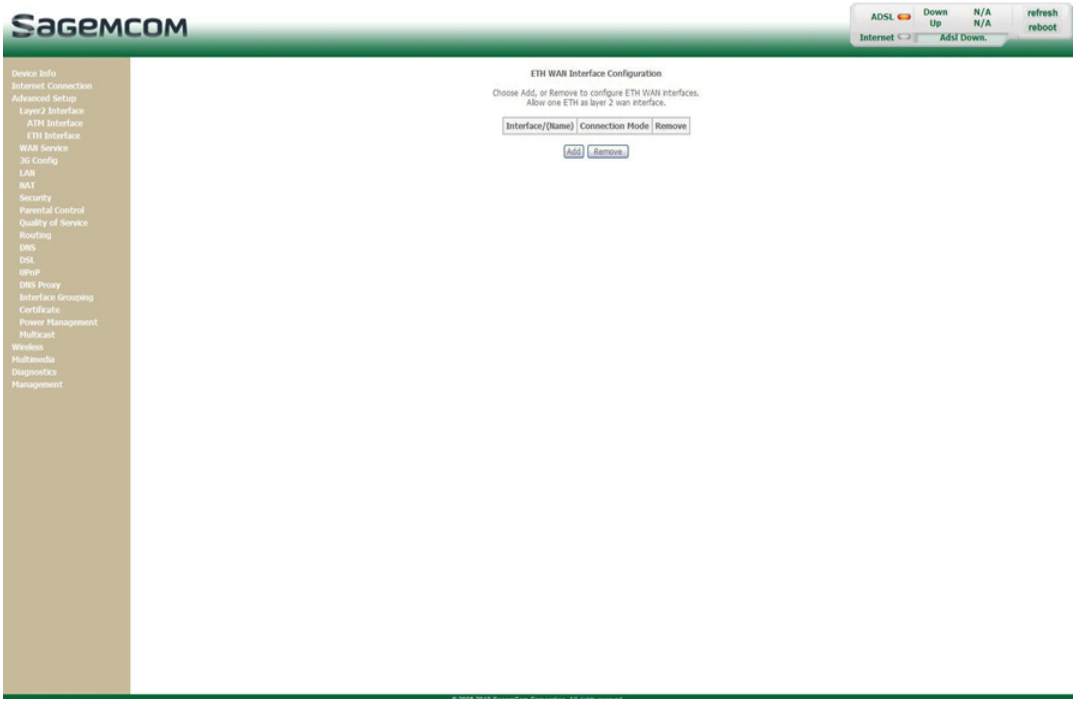
Encapsulation modes

DSL Link type	Action	Default value
EoA (Ethernet over ATM)	Select the encapsulation of your choice from the scroll down list. • LLC/SNAP-BRIDGING • VC/MUX	**LLC/SNAP-BRIDGING**
PPPoA (PPP over ATM)	Select the encapsulation of your choice from the scroll down list. • VC/MUX • LLC/ENCAPSULATION	**VC/MUX**
IPoA (IP over ATM)	Select the encapsulation of your choice from the scroll down list. • LLC/SNAP-ROUTING • VC/MUX	**LLC/SNAP-ROUTING**

5.7.1.3 ETH Interface

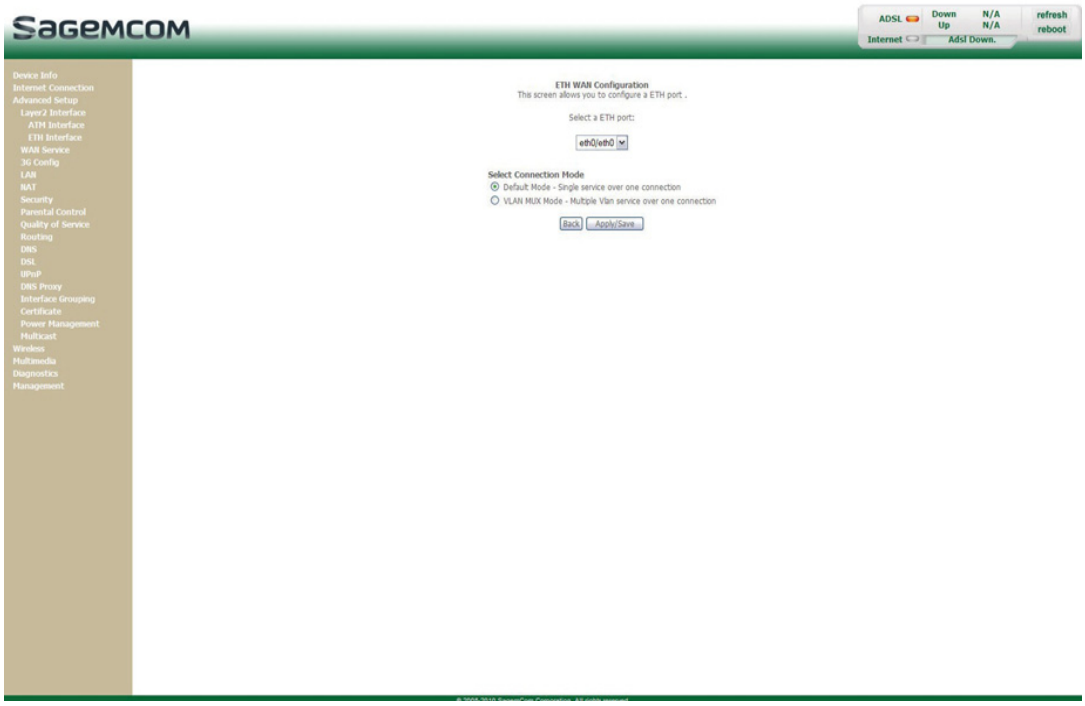
Object: This menu is used to configure DSL ETH interfaces.

- In the **Advanced Setup** menu, select **Layer2 Interface** then **ETH Interface**.
  The following screen opens:



5.7.1.4 Add

- Click on the **Add** button to display the following screen:



DSL Link type	Action	Default value
Select a ETH port	Select the encapsulation of your choice from the scroll down list (from 1 to 3).	**eth0/eth0**
Select Connection Mode	Select the connection mode of your choice from the scroll down list. • Default Mode - Single service over one connection • VLAN MUX Mode - Multiple Vlan service over one connection	**Default Mode checked**

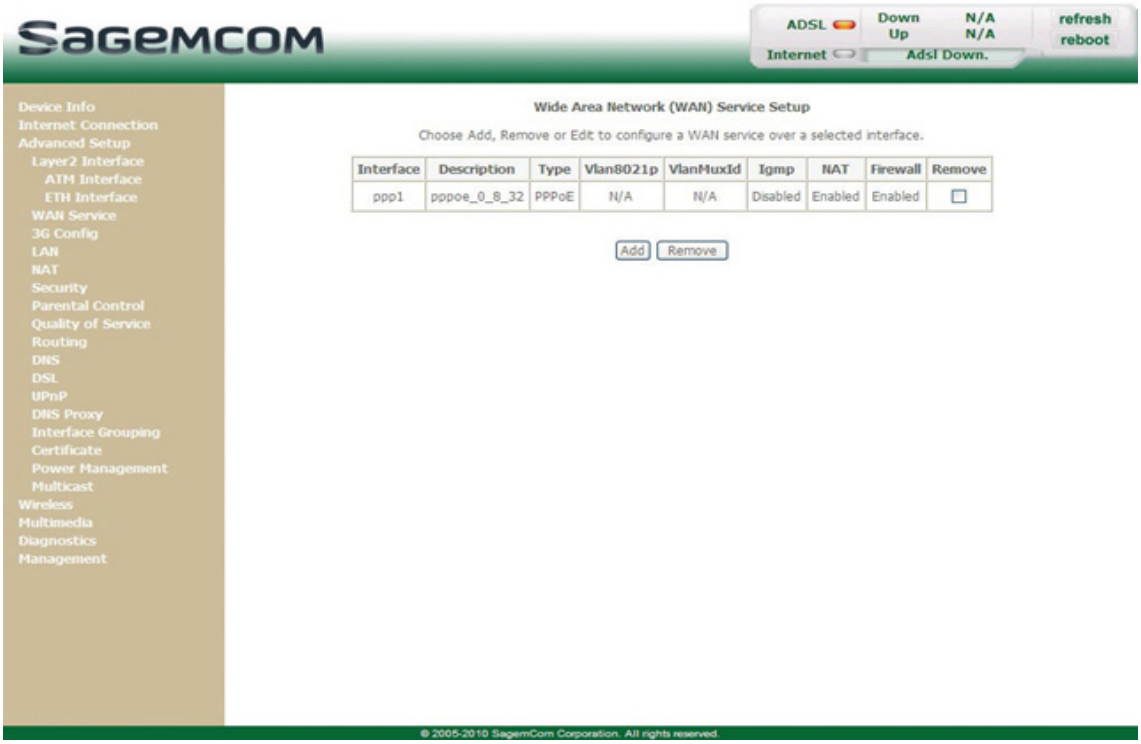
- Click on the **Apply/Save** button to confirm the creation of the new ETH interface.

5.7.2 WAN Service

Object: This menu is associated with the remote network. It is used to display the list of all the configured PVCs, and to add PVCs or remove them.

- In the **Advanced Setup** menu, select **WAN Service**.

  The following screen opens:



Field	Meaning
Interface	Name, allocated automatically, associated with the service name (for example, ppp0).
Description	Name of the ATM service. This name is made up as follows: Protocol_VPI_VCI_Index For example: pppoe_0_8_32.
Type	Data flow encapsulation mode.
Vlan8021p[a]	Value of the 802.1P Priority.
VlanMuxId[a.]	Value of the 802.1Q VLAN ID.
Igmp	Status (Enabled or Disabled) of the Igmp function. **Note:** This function enables the distribution of Multicast datagrams over the local network (LAN) and interaction between the router and the local network hosts.
NAT	Status (Enabled or Disabled) of the NAT.
Firewall	Status (Enabled or Disabled) of the Firewall.
Remove	Check this box and clik on the [**Remove**] button to remove the selected object from the list.

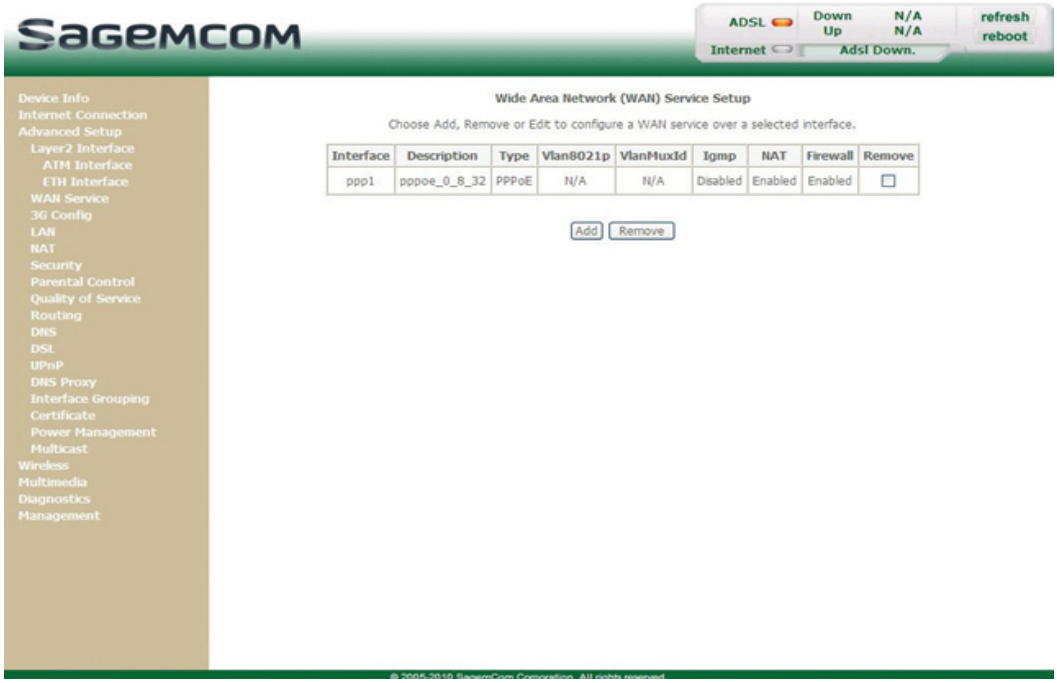
a. These values only appear if the WAN service is configured over a DSL ATM interface using VLAN MUX Mode.

5.7.2.1 Add

Note

You must have configured a DSL ATM interface (see section 5.7.1) to add a WAN service.

- Click on the **Add** button.



- Select the DSL ATM interface for the WAN service.

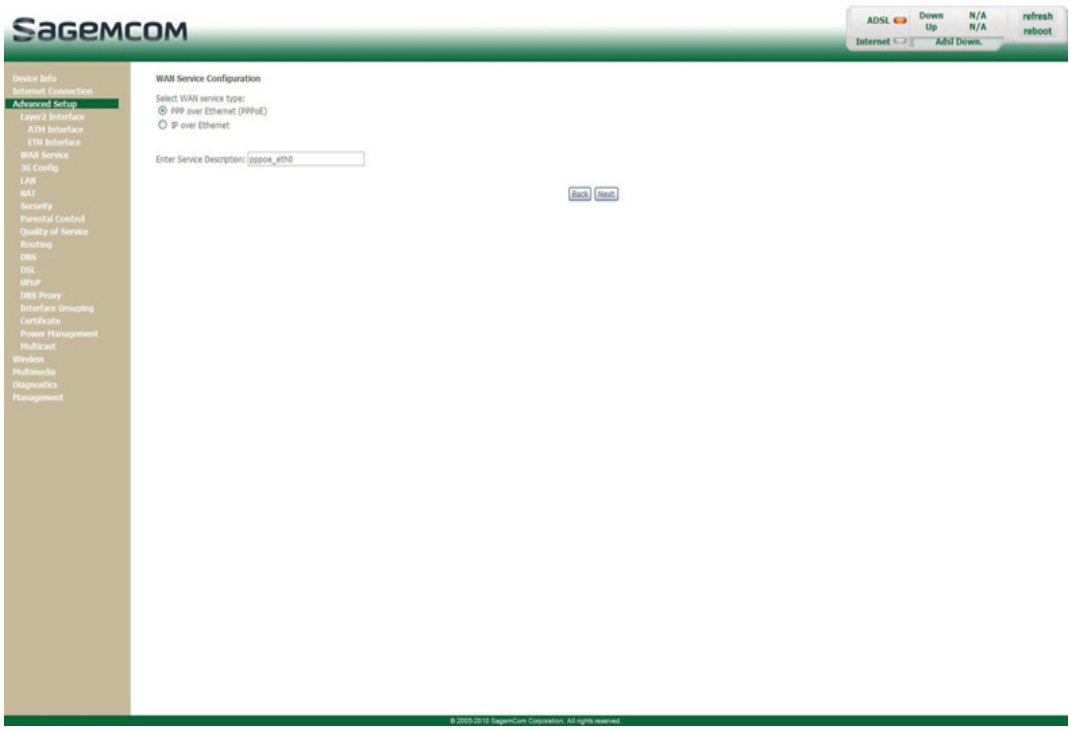
- Click on the **Next** button to continue configuring the WAN service.

Note

Depending on the type of network protocol configured for the selected DSL ATM interface (EoA, PPPoA or IPoA), the content of the following WAN interface configuration screens differs.
Therefore, and for more clarity, each type of protocol will be dealt with separately (screens + associated summary tables) below.

5.7.2.2 Ethernet over ATM – PPP over Ethernet (PPPoE)

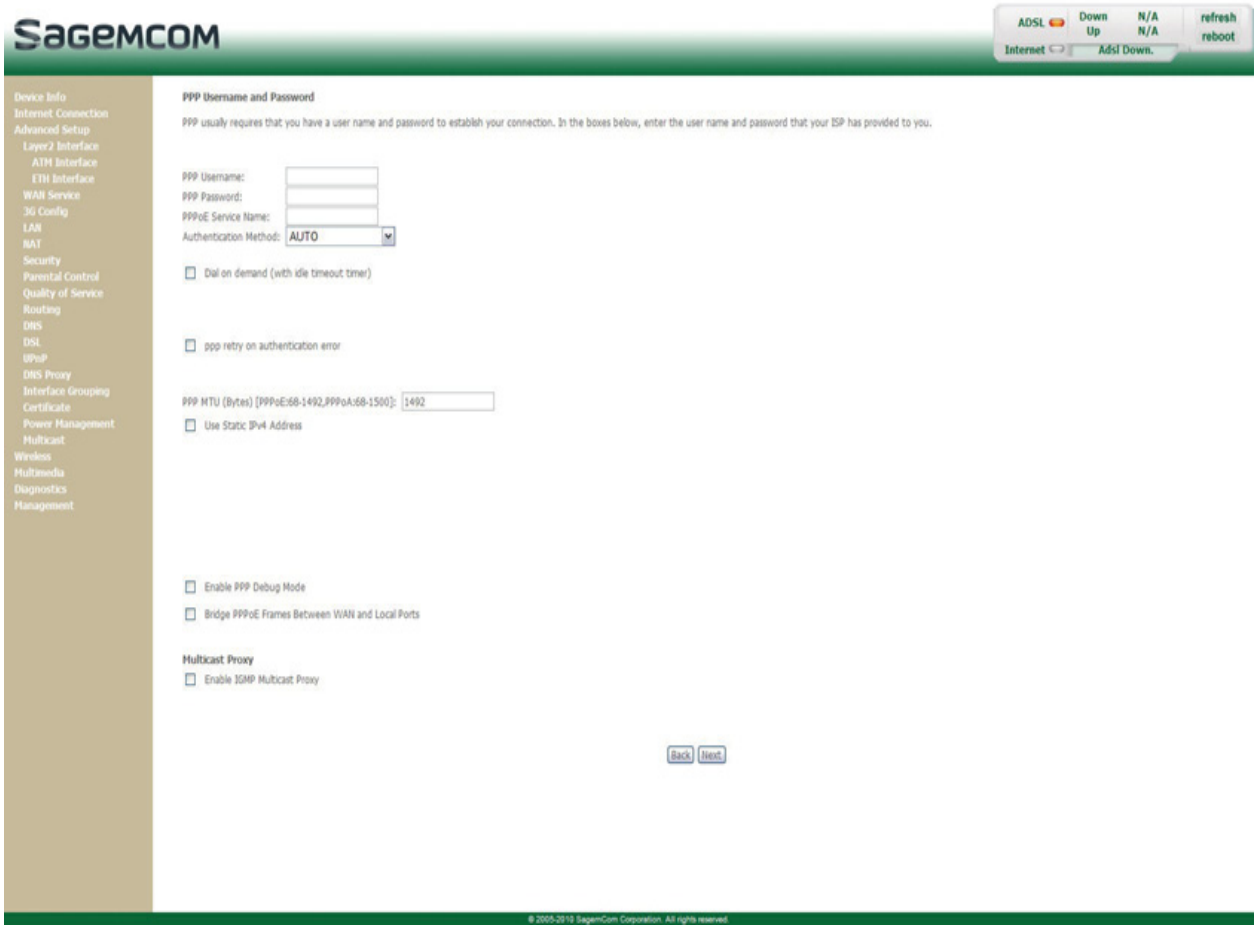
- Select the WAN service type **PPP over Ethernet (PPPoE)**.



Field	Action	Default value
Enter Service Description	Displays the name of the service being configured. This name, which is allocated automatically, is made up as follows: Protocol_VPI_ Index _ VCI For example: pppoe_eth0. **Note:** You may enter another service name.	**pppoe_eth0**
Enter 802.1P Priority[a]	Enter a value for the 802.1P Priority. This value is between 0 and 7.	**-1**
Enter 802.1Q VLAN ID[a.]	Enter a value for the 802.1QVLAN ID. This value is between 0 and 4094.	**-1**

a. These values only appear if the WAN service is configured over a DSL ATM interface using VLAN MUX Mode.

- Click on the **Next** button to continue configuring the WAN service.



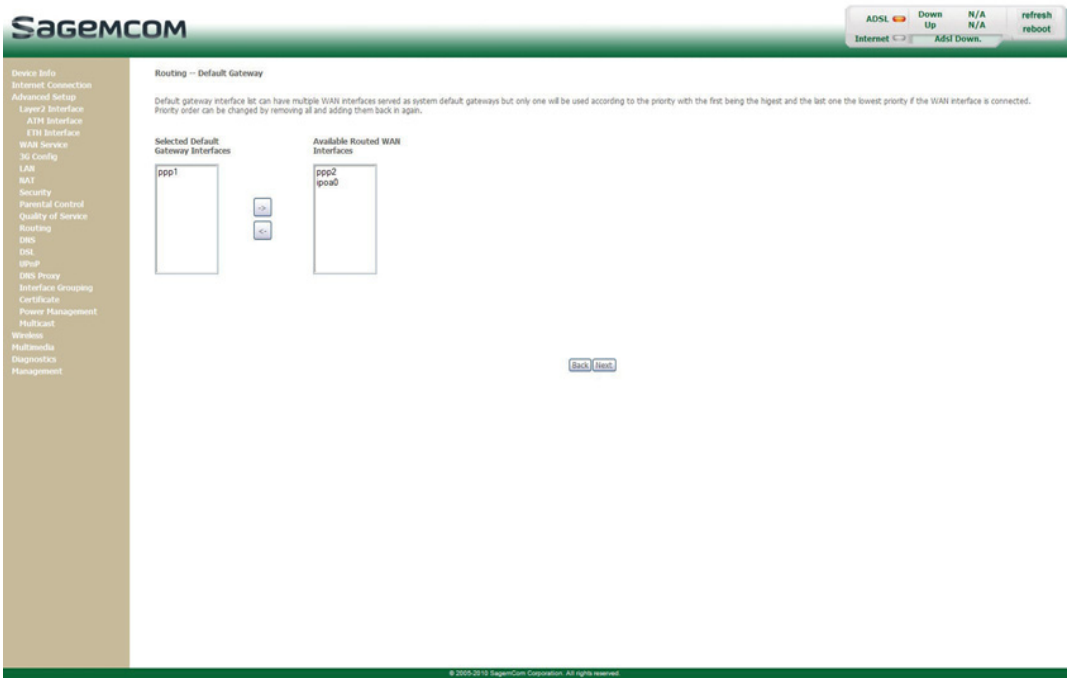
Field	Action	Default value
PPP Username	Enter your connection ID. This information is provided to you by your **I**nternet **S**ervice **P**rovider (**ISP**).	-
PPP Password	Enter your connection password. This information is provided to you by your **I**nternet **S**ervice **P**rovider (**ISP**).	-
PPPoE Service Name	Enter the name of the PPPoE service. This information is provided to you by your **I**nternet **S**ervice **P**rovider (**ISP**).	-
Authentication Method	Select the authentication method of your choice from the scroll down list: • AUTO • PAP • CHAP • MSCHAP	**AUTO**
Dial on demand (with idle timeout timer)	Check the box to connect to the Internet only when needed.	**Not Checked**

Field	Action	Default value
Inactivity Timeout (minutes):[1-4320][a]	Enter the inactivity time. This value (in minutes) is between 1 and 4320 (i.e. 72 hours). If there is no Internet traffic for this period of time, the PPPoE session is interrupted.	**0**
PPP retry on authentication error	Check the box, PPP can be retried again and again while authentication fails.	**Checked**
PPP retry period (seconds)):[3-65535][b]	Enter if required a retry period. This value (in seconds) is by default set to 15 seconds. You can set another value from 3 to 65535.	**15**
PPP MTU (Bytes)	Enter an MTU (**M**aximum **T**ransfer **U**nit) value. This value (in bytes) is between 38 and 1492. **Note:** The MTU specifies the maximum size of the data used (IP packets) expressed as a number of bytes.	**1492**
Use Static IPv4 Address	Check the box to use the static IPv4 address.	**Not checked**
IPv4 Address[c]	Enter the static IPv4 address.	**0.0.0.0**
Enable PPP Debug mode	Check the box to use the PPP Debug mode. In the event of connection failure, this option will enable you to trace a possible problem in the SYSLOG file.	**Not checked**
Bridge PPPoE frames between WAN and Local Ports	Check the box to enable the router when bridging the frames between WAN and local Ethernet ports.	**Not checked**
Enable IGMP Multicast Proxy	Check the box to activate the IGMP function.	**Not checked**

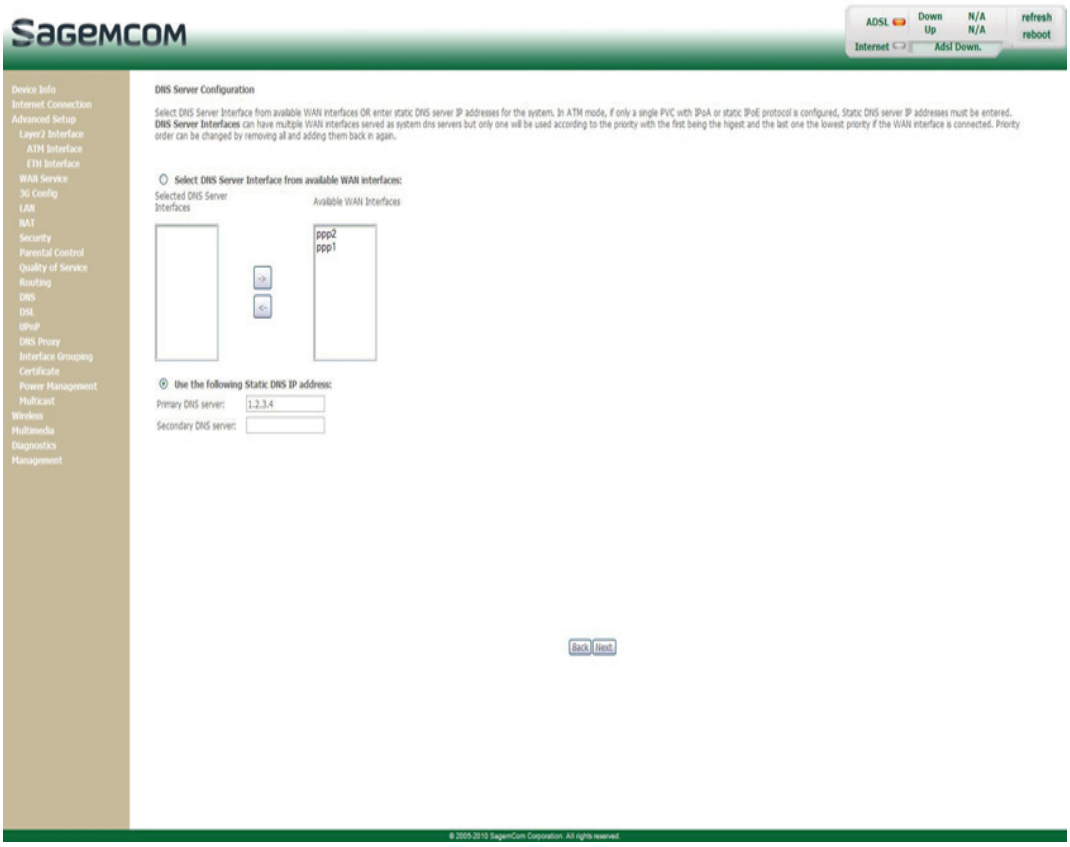
a. This field only appears when the "PPP retry on authentication error" field is activated (box checked).
b. This field only appears when the "PPP retry on authentication error" field is activated (box checked).
c. This field only appears when the "Use Static IPv4 Address" field is activated (box checked).

- Click on the **Next** button to continue configuring the remote network (WAN) in PPPoE mode.

- Select a preferred WAN interface as the system default gateway.



- Click on the **Next** button to continue configuring the remote network (WAN) in PPPoE mode.



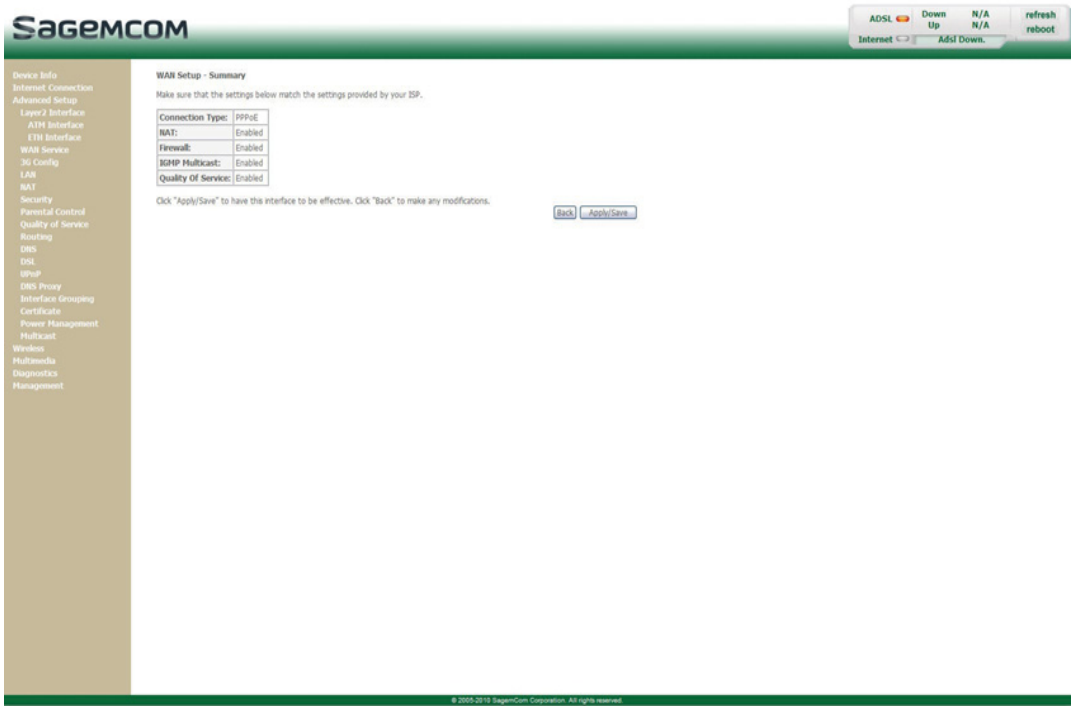
Field	Action	Default value
Select DNS Server Interface from available WAN interfaces	For more details, a summary table is presented below for each column.	**ppp1** **pppoa2**

Field	Action	Default value
Use the following Static DNS IP address	If you check this box, you must enter DNS server addresses.	**Not checked**
Primary DNS server	Enter a primary DNS server address.	**-**
Secondary DNS server	Enter a secondary DNS server address.	**-**

Select DNS Server Interface from available WAN interfaces

Button	Action
<-	Transfer the interfaces selected in the **Available WAN Interfaces** area to the **Selected DNS Server Interfaces** area.
->	Transfer the interfaces selected in the **Selected DNS Server Interfaces** area to the **Available WAN Interfaces** area.

- Click on the **Next** button to continue configuring the remote network (WAN) in PPPoE mode.

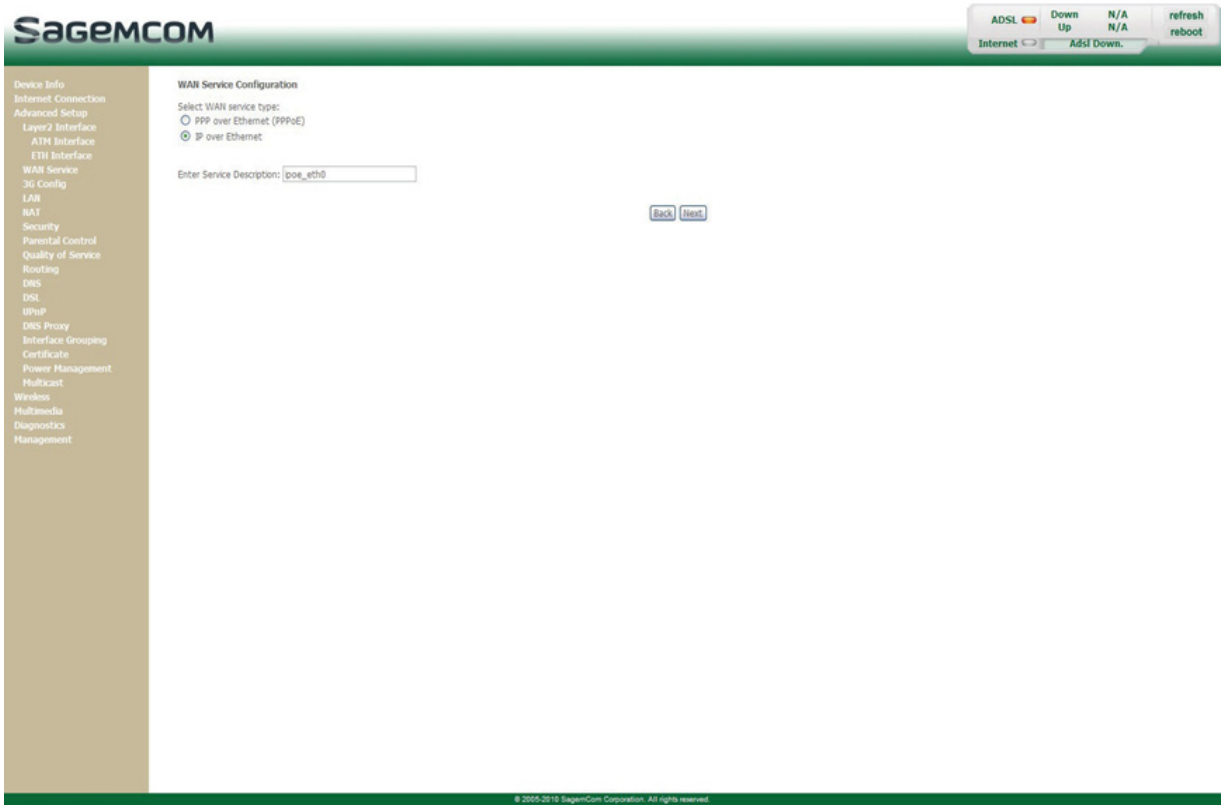


Field	Description
NAT	Displays the status of the NAT.
Firewall	Displays the status of the firewall.
IGMP Multicast	Displays the status of the IGMP function.
Quality of Service	Displays the status of the Quality of Service function.

- Click on the **Apply/Save** button to confirm the new WAN service.

5.7.2.3 Ethernet over ATM – IP over Ethernet (IPoE)

- Select the WAN service type **IP over Ethernet (IPoE)**.



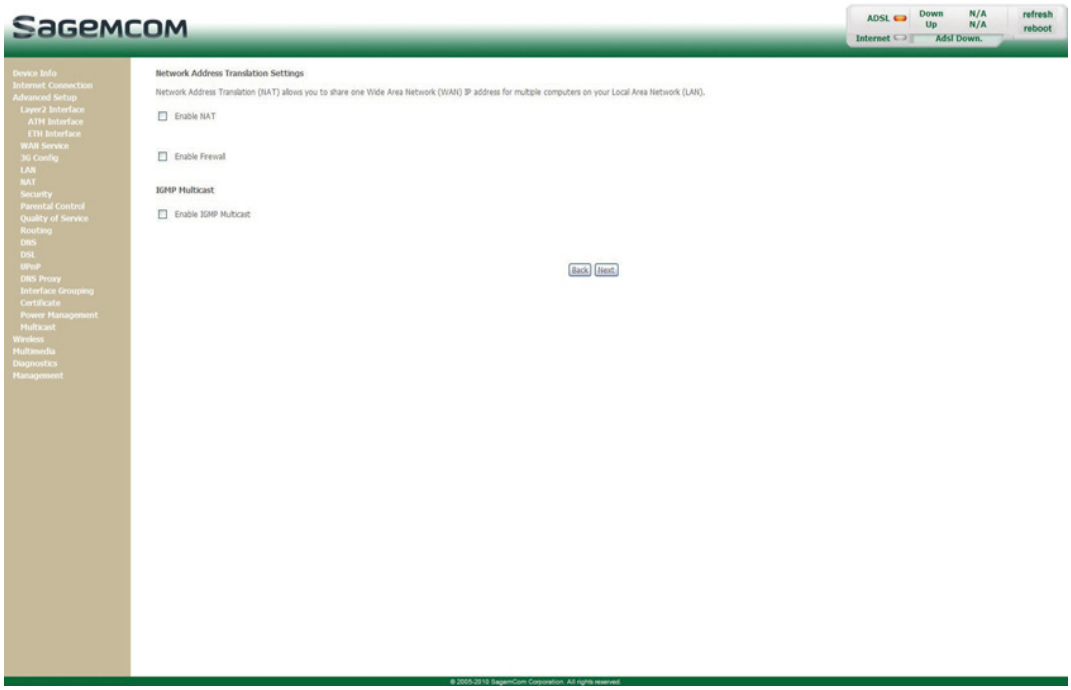
Field	Action	Default value
Enter Service Description	Displays the name of the service being configured. This name, which is allocated automatically, is made up as follows: Protocol_VPI_ Index _ VCI For example: ipoe_eth0. **Note:** You may enter another service name.	**ipoe_eth0**
Enter 802.1P Priority[a]	Enter a value for the 802.1P Priority. This value is between 0 and 7.	**-1**
Enter 802.1Q VLAN ID[a.]	Enter a value for the 802.1QVLAN ID. This value is between 0 and 4094.	**-1**

a. These values only appear if the WAN service is configured over a DSL ATM interface using VLAN MUX Mode.

- Click on the **Next** button to continue configuring the WAN service.

Field	Action	Default value
Obtain an IP address automatically	Check the box to obtain an IP address automatically from your router's DHCP server.	**Checked**
Option 60 Vendor ID	This feature allows a DHCP server to differentiate between the two kinds of client machines and process the requests from the two types of modems appropriately. If this feature is enabled on the DHCP server, and you want to use it, enter the vendor ID.	**-**
Option 61 IAID	This features allows a DHCP server to use an **I**dentity **A**ssociation **ID**entifier (**IAID**). If this feature is enabled on the DHCP server, and you want to use it, enter the DHCP Identity Association ID.	**-**
Option 61 DUID	This features allows a DHCP server to use a **D**HCP **U**nique **ID**entifier (**DUID**). If this feature is enabled on the DHCP server, and you want to use it, enter the DHCP Unique IDentifier.	**-**
Option 125	This feature allows you to enable/disable the DHCP Vendor-Identifying Vendor-Specific 125 option.	**Disable**
Use the following Static IP address:	If you check this box, you must enter a static WAN IP address and the dedicated WAN subnet mask and WAN gateway IP address.	**Not checked**
WAN IP Address	Enter the static IP address.	**-**
WAN Subnet Mask	Enter the subnet mask.	**-**
WAN gateway IP address	Enter the gateway IP address.	**-**

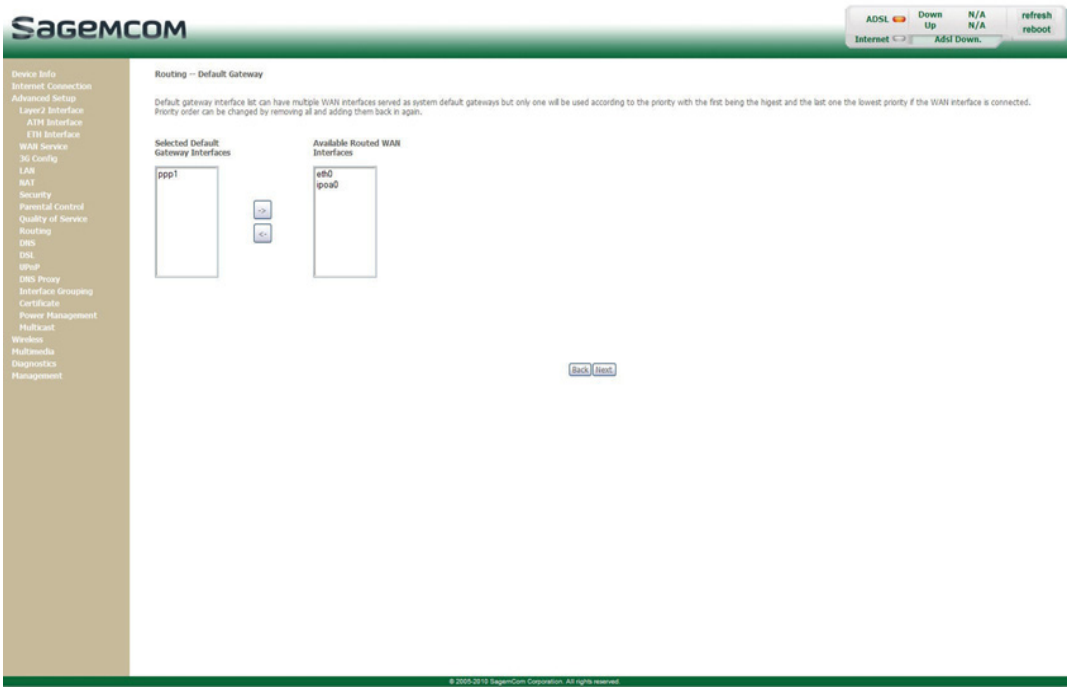
- Click on the **Next** button to continue configuring the remote network (WAN) in IPoE mode.



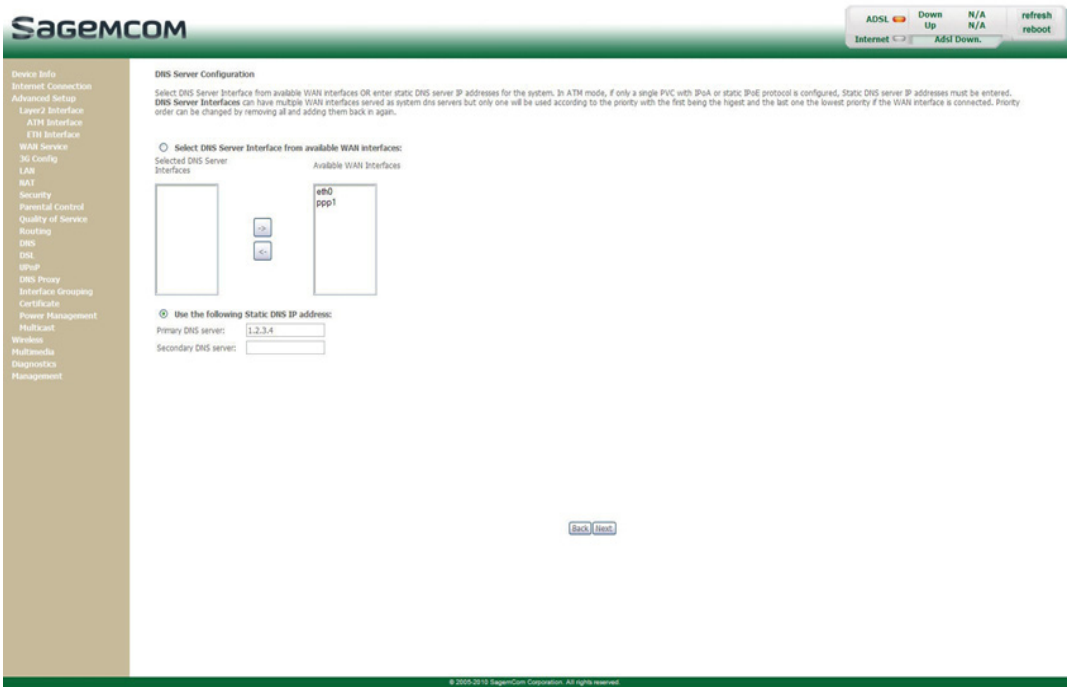
Field	Action	Default value
Enable NAT	Check the box to activate the NAT function. **Note:** NAT is a configurable IP address translation function which will be applied to the interfaces of your router which you will have activated for this function.	**Not checked**
Enable Fullcone NAT[a]	Check the box to activate the Fullcone NAT function.	**Not checked**
Enable Firewall	Check the box to activate the Firewall service.	**Not checked**
Enable IGMP Multicast	Check the box to activate the IGMP function.	**Not checked**

a. This field only appears when the "Enable NAT" field is activated (box checked).

- Select a preferred WAN interface as the system default gateway.



- Click on the **Next** button to continue configuring the remote network (WAN) in IPoE mode.

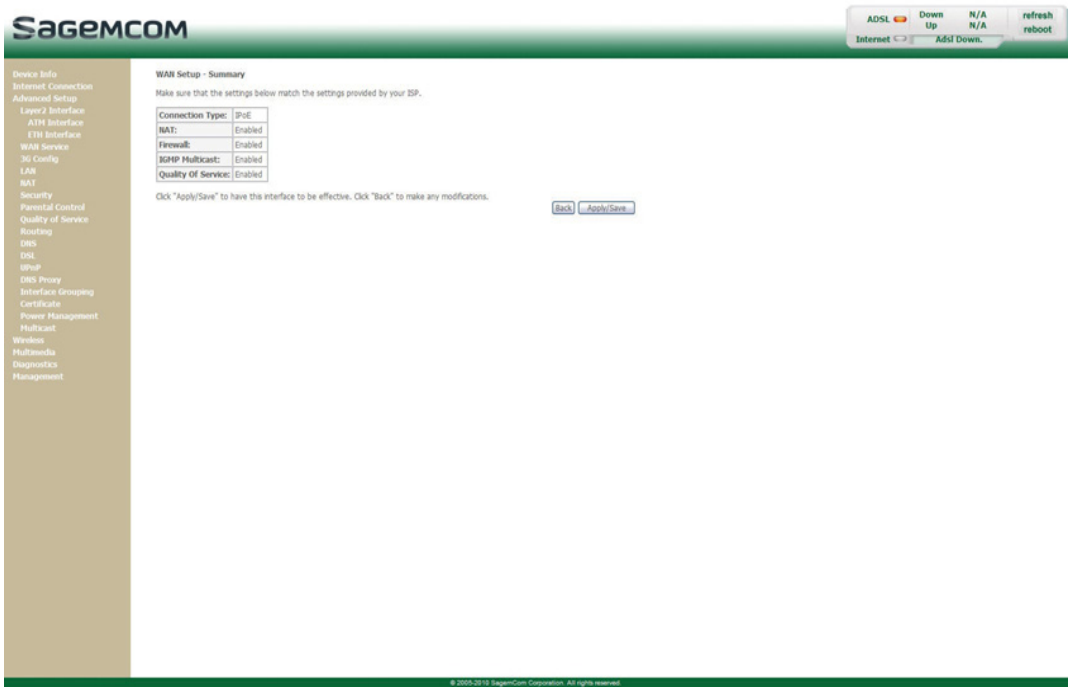


Field	Action
Selected DNS Server Interfaces	For more details, a summary table is presented below for each column.
Available WAN Interfaces	
Primary DNS server	Enter the primary DNS server
Secondary DNS server	Enter the primary DNS server

Select DNS Server Interface from available WAN interfaces

Button	Action
<-	Transfer the interfaces selected in the **Available WAN Interfaces** area to the **Selected DNS Server Interfaces** area.
->	Transfer the interfaces selected in the **Selected DNS Server Interfaces** area to the **Available WAN Interfaces** area.

- Click on the **Next** button to continue configuring the remote network (WAN) in IPoE mode.

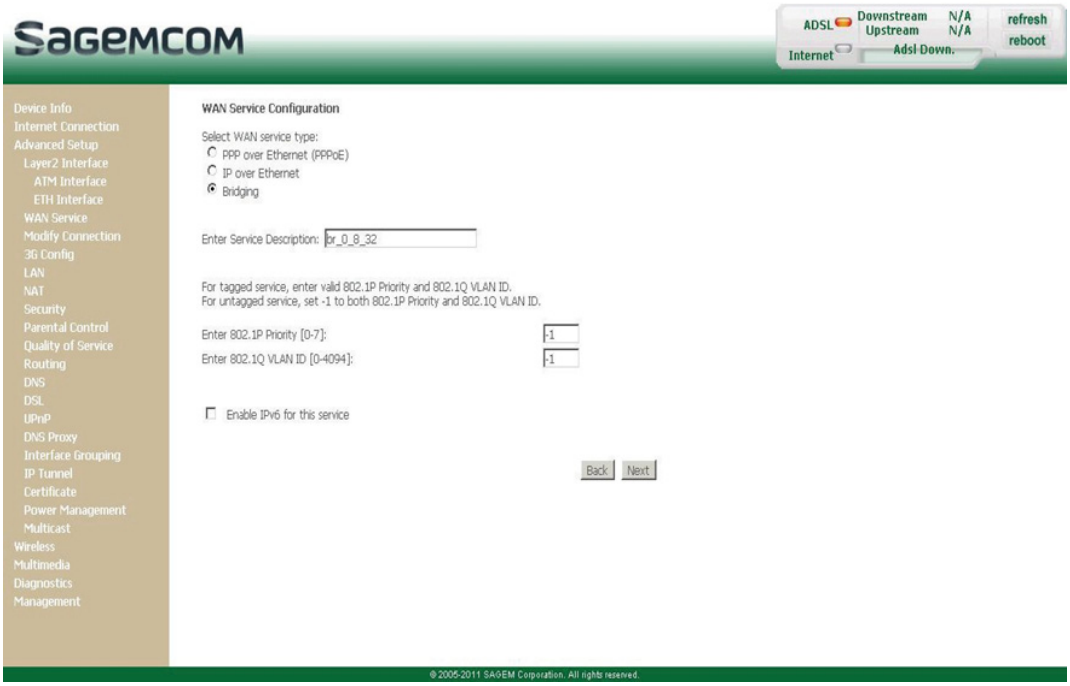


Field	Description
Connection Type	Displays the "IPoE" protocol
NAT	Displays the status of the NAT.
Firewall	Displays the status of the firewall.
IGMP Multicast	Displays the status of the IGMP function.
Quality Of Service	Displays the status of the Quality Of Service function.

- Click on the **Apply/Save** button to confirm the new WAN service.

5.7.2.4 Ethernet over ATM - Bridging

- Select the WAN service type **Bridging**.



Field	Action	Default value
Enter Service description	Displays the name of the service being configured. This name, which is allocated automatically, is made up as follows: Protocol_VPI_ Index _ VCI For example: br_0_8_32. **Note:** You may enter another service name.	**br_0_8_32**
Enter 802.1P Priority[a]	Enter a value for the 802.1P Priority. This value is between 0 and 7.	**-1**
Enter 802.1Q VLAN ID[a.]	Enter a value for the 802.1QVLAN ID. This value is between 0 and 4094.	**-1**

a. These values only appear if the WAN service is configured over a DSL ATM interface using VLAN MUX Mode.

- Click on the **Next** button to continue configuring the remote network (WAN) in Bridge mode.

Field	Description
NAT	Displays the status of the NAT.
Firewall	Displays the status of the firewall.
IGMP Multicast	In the "Bridge" connection, this field is: **Not Applicable**
Quality Of Service	Displays the status of the Quality Of Service function.

- Click on the **Apply/Save** button to confirm the new WAN service.

5.7.2.5 PPP over ATM (PPPoA)

Field	Action	Default value
Enter Service Description	Displays the name of the service being configured. This name, which is allocated automatically, is made up as follows: Protocol_VPI_ Index_VCI For example: pppoa_0_0_35. **Note:** You may enter another service name.	**pppoa_0_0_35**

- Click on the **Next** button to continue configuring the WAN service.

Field	Action	Default value
PPP Username	Enter your connection ID. This information is provided to you by your **I**nternet **S**ervice **P**rovider (ISP).	-
PPP Password	Enter your connection password. This information is provided to you by your **I**nternet **S**ervice **P**rovider (ISP).	-
Authentication Method	Select the authentication method of your choice from the scroll down list: • AUTO • PAP • CHAP • MSCHAP	**AUTO**
Dial on demand (with idle timeout timer)	Check the box to connect to the Internet only when needed.	**Not checked**
PPP retry on authentication error	Check the box, PPP can be retried again and again while authentication fails	**Checked**
PPP retry period (seconds)[a]	Enter if required a retry period. This value (in seconds) is by default set to 15 seconds. You can set another value from 3 to 65535.	**15**

Field	Action	Default value
PPP MTU (Bytes)	Enter an MTU (**M**aximum **T**ransfer **U**nit) value. This value (in bytes) is between 46 and 1500. **Note:** The MTU specifies the maximum size of the data used (IP packets) expressed as a number of bytes.	**1500**
Use Static IPv4 Address	Check the box to use the static IPv4 address.	**Not checked**
IPv4 Address:[b]	Enter the static IPv4 address.	**0.0.0.0**
Enable PPP Debug Mode	Check the box to use the PPP Debug mode. In the event of connection failure, this option will enable you to trace a possible problem in the SYSLOG file.	**Not checked**
Enable IGMP Multicast Proxy	Check the box to activate the IGMP function.	**Not checked**

a. This field only appears when the "PPP retry on authentication error" field is activated (box checked).
b. This field only appears when the "Use Static IPv4 Address" field is activated (box checked).

- Click on the **Next** button to continue configuring the remote network (WAN) in PPPoA mode.
- Select a preferred WAN interface as the system default gateway.

- Click on the **Next** button to continue configuring the remote network (WAN) in PPPoA mode.

Field	Action
Selected DNS Server Interfaces	For more details, a summary table is presented below for each column.
Available WAN Interfaces	
Primary DNS server	Enter the primary DNS server
Secondary DNS server	Enter the primary DNS server

Select DNS Server Interface from available WAN interfaces

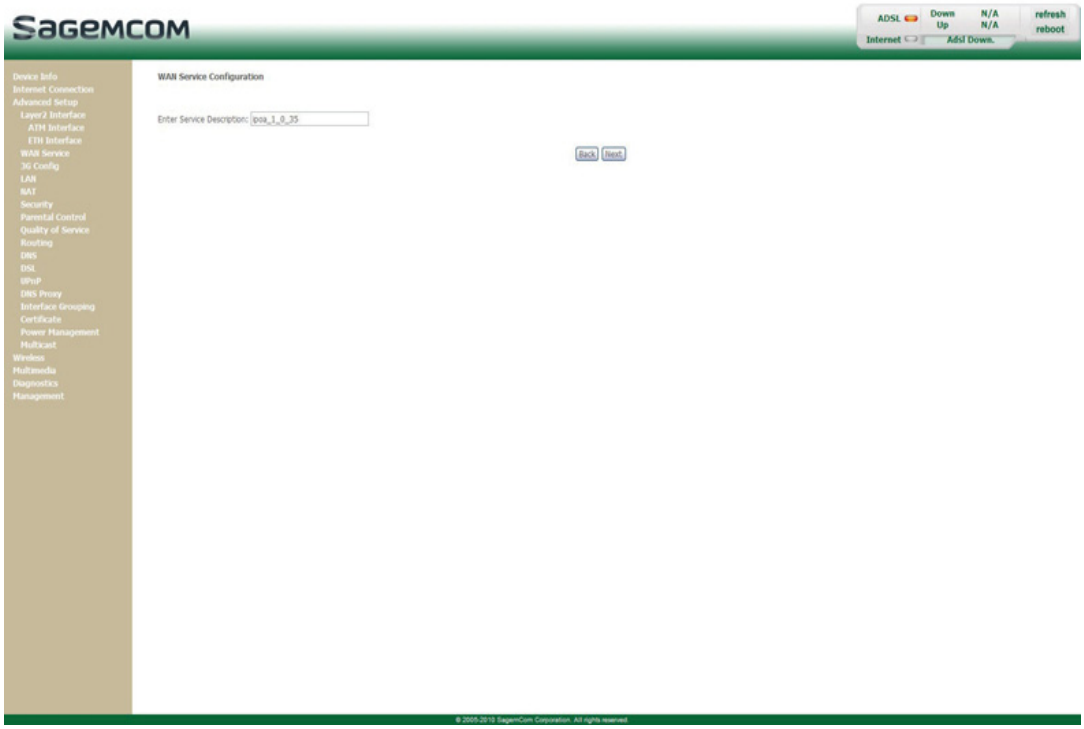
Button	Action
<-	Transfer the interfaces selected in the **Available WAN Interfaces** area to the **Selected DNS Server Interfaces** area.
->	Transfer the interfaces selected in the **Selected DNS Server Interfaces** area to the **Available WAN Interfaces** area.

- Click on the **Next** button to continue configuring the remote network (WAN) in PPPoA mode.

Field	Description
Connection Type	Displays the "PPPoA" protocol.
NAT	Displays the status of the NAT.
Firewall	Displays the status of the firewall.
IGMP Multicast	Displays the status of the IGMP function.
Quality of Service	Displays the status of the Quality of Service function.

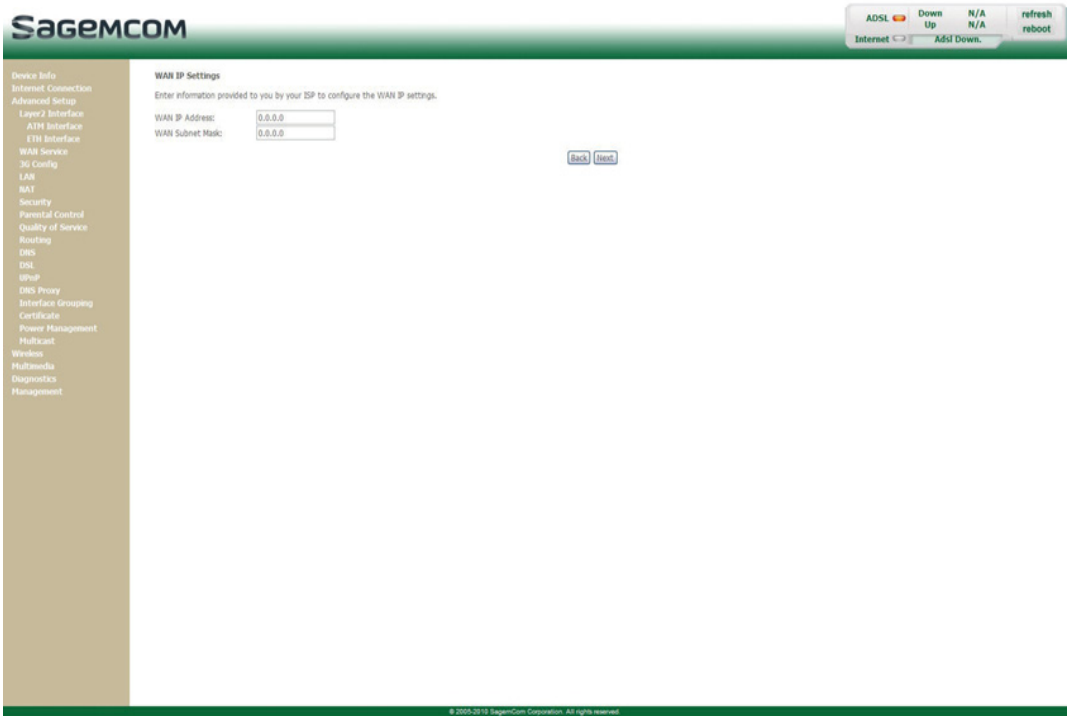
- Click on the **Apply/Save** button to confirm the new WAN service.

5.7.2.6 IP over ATM (IPoA)



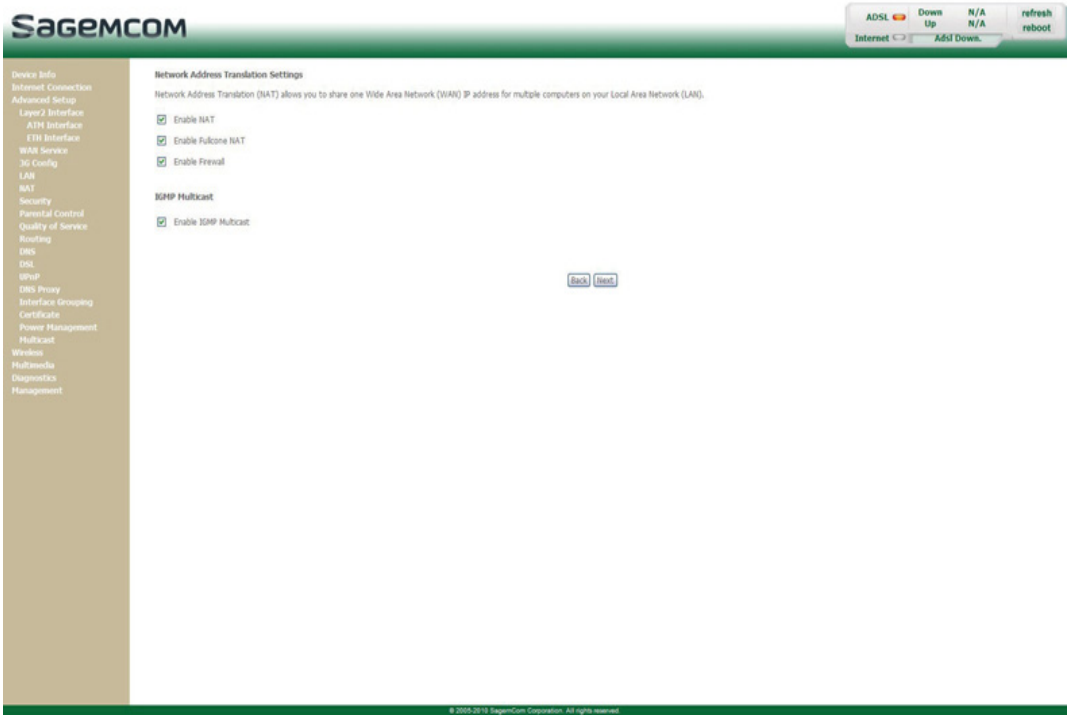
Field	Action	Default value
Enter Service Description	Displays the name of the service being configured. This name, which is allocated automatically, is made up as follows: Protocol_VPI_Index_VCI For example: ipoa_1_0_35. **Note:** You may enter another service name.	**ipoa_1_0_35**

- Click on the **Next** button to continue configuring the WAN service.



Field	Action	Default value
WAN IP Address	Enter the static IP address.	**0.0.0.0**
WAN Subnet Mask	Enter a subnet mask.	**0.0.0.0**

- Click on the **Next** button to continue configuring the remote network (WAN) in IPoA mode.

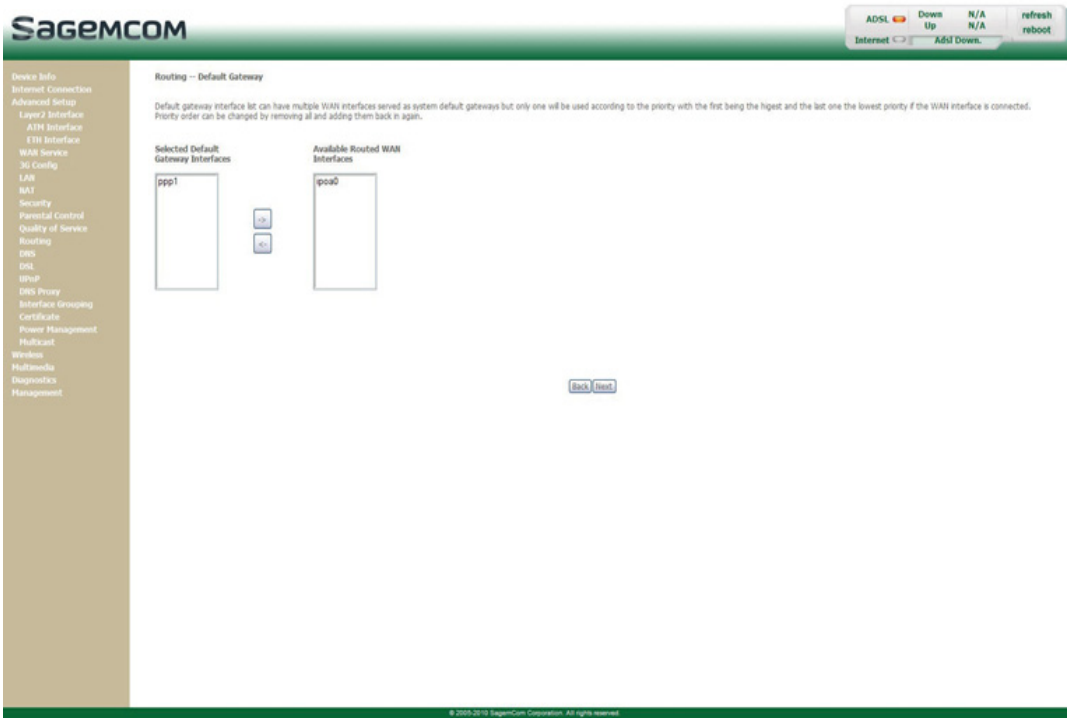


Field	Action	Default value
Enable NAT	Check the box to activate the NAT function. **Note:** NAT is a configurable IP address translation function which will be applied to the interfaces of your router which you will have activated for this function.	**Not checked**
Enable Fullcone NAT[a]	Check the box to activate the Fullcone NAT function.	**Not checked**
Enable Firewall	Check the box to activate the Firewall service.	**Not checked**
Enable IGMP Multicast	Check the box to activate the IGMP function.	**Not checked**

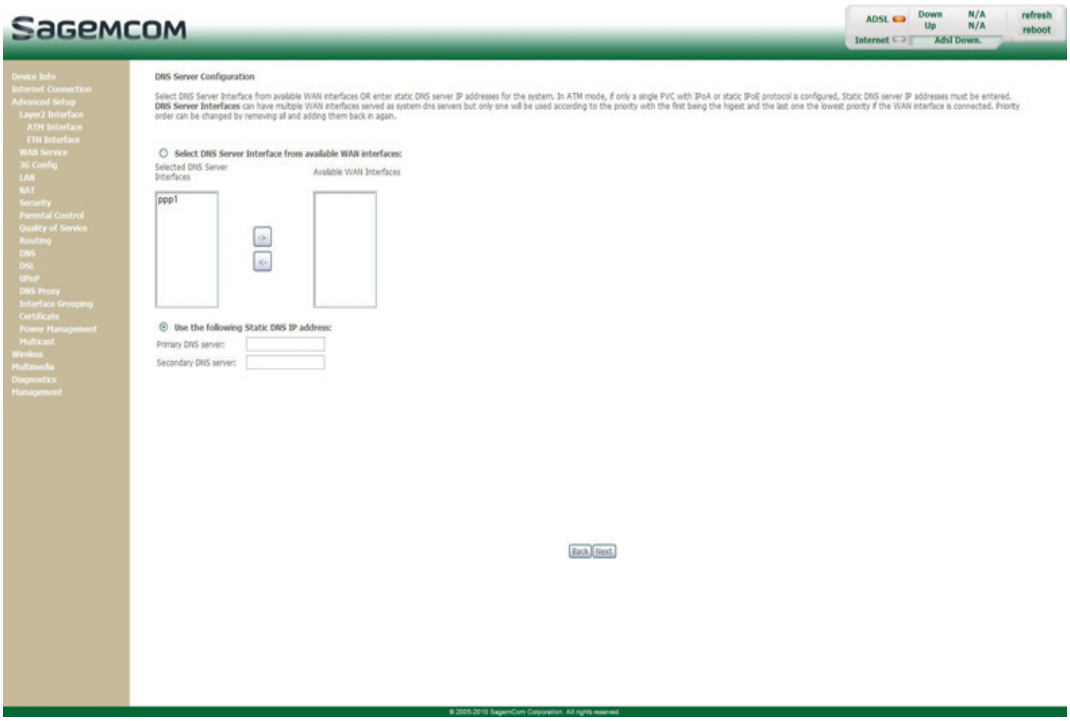
a. This field only appears when the "Enable NAT" field is activated (box checked).

- Click on the **Next** button to continue configuring the remote network (WAN) in IPoA mode.

- Select a preferred WAN interface as the system default gateway.



- Click on the **Next** button to continue configuring the remote network (WAN) in IPoA mode.

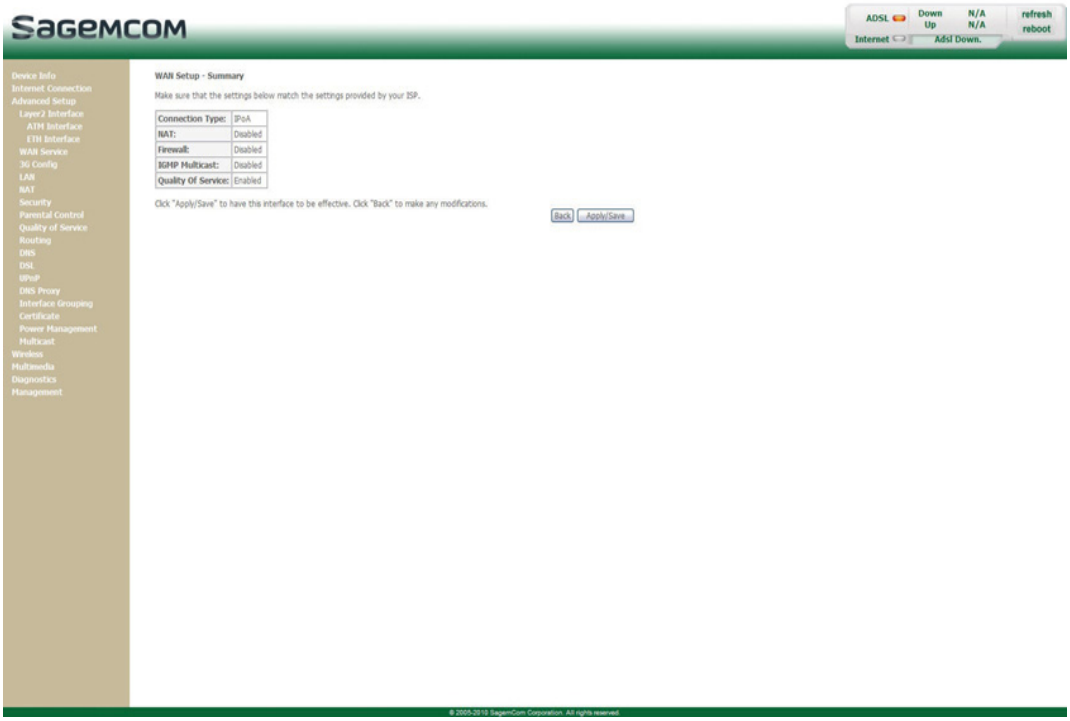


Field	Action
Selected DNS Server Interfaces	For more details, a summary table is presented below for each column.
Available WAN Interfaces	
Primary DNS server	Enter the primary DNS server
Secondary DNS server	Enter the primary DNS server

Select DNS Server Interface from available WAN interfaces

Button	Action
<-	Transfer the interfaces selected in the **Available WAN Interfaces** area to the **Selected DNS Server Interfaces** area.
->	Transfer the interfaces selected in the **Selected DNS Server Interfaces** area to the **Available WAN Interfaces** area.

- Click on the **Next** button to continue configuring the remote network (WAN) in IPoA mode.



Field	Description
Connection Type	Displays the "IPoA" protocol.
NAT	Displays the status of the NAT.
Firewall	Displays the status of the firewall.
IGMP Multicast	Displays the status of the IGMP function.
Quality of Service	Displays the status of the Quality of Service function.

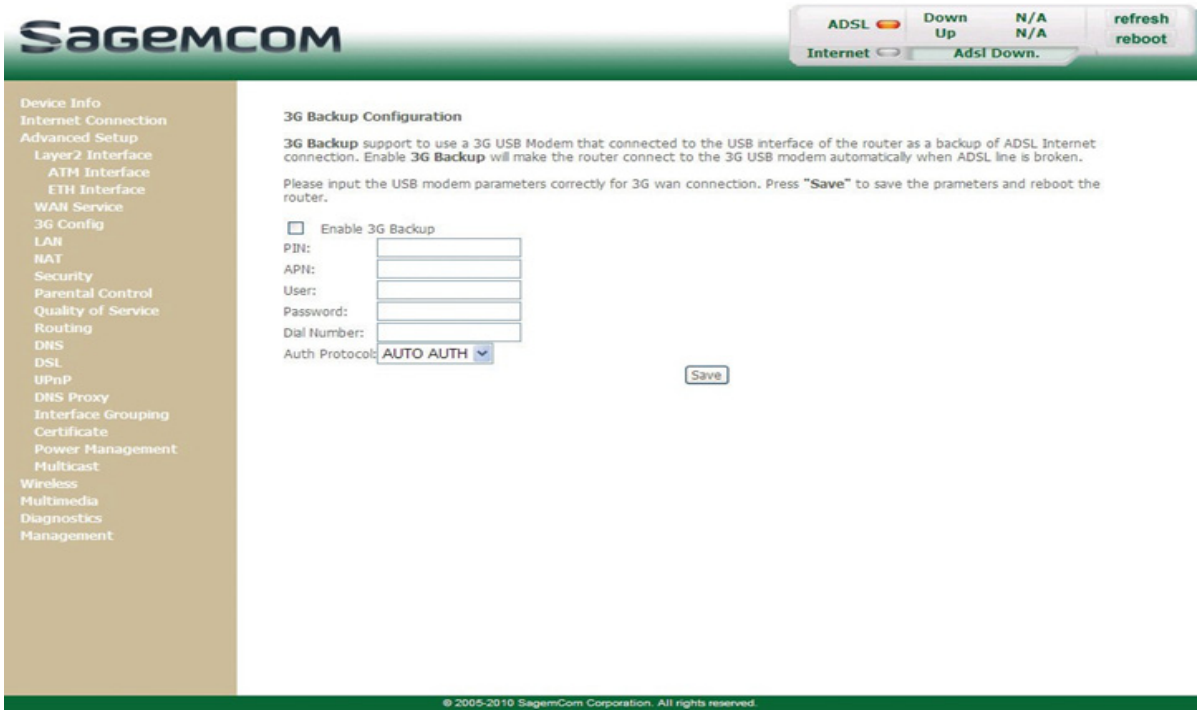
- Click on the **Apply/Save** button to confirm the new WAN service.

5.7.3 3G Config

Object: This menu lets you configure 3G backup support to use a 3G USB modem that connected to the USB interface of the router as a backup of ADSL Internet connection.

- In the **Advanced Setup** menu, select **3G Config**.

  The following screen opens:



Field	Action	Default value
Enable	Check the box to enable 3G backup. This backup will make the router connect to the 3G USB modem automatically when ADSL line is broken.	**Disabled**
PIN	Enter the PIN number.	-
APN	Enter the APN (Access Point Name) protocol which allows your Box to access the Internet.	-
User	Enter the user name.	-
Password	Enter the 3G USB modem password.	-
Dial Number	Enter the dial number of the 3G USB modem.	-
Auth Protocol	Select the protocol to use in the scrolling down list: • AUTO AUTH • PAP (**P**assword **A**uthentification **P**rotocol) • CHAP (**C**hallenge **H**andshake **A**uthentification **P**rotocol)	**AUTO AUTH**

- Click on the **Save** button to save the defined parameters.

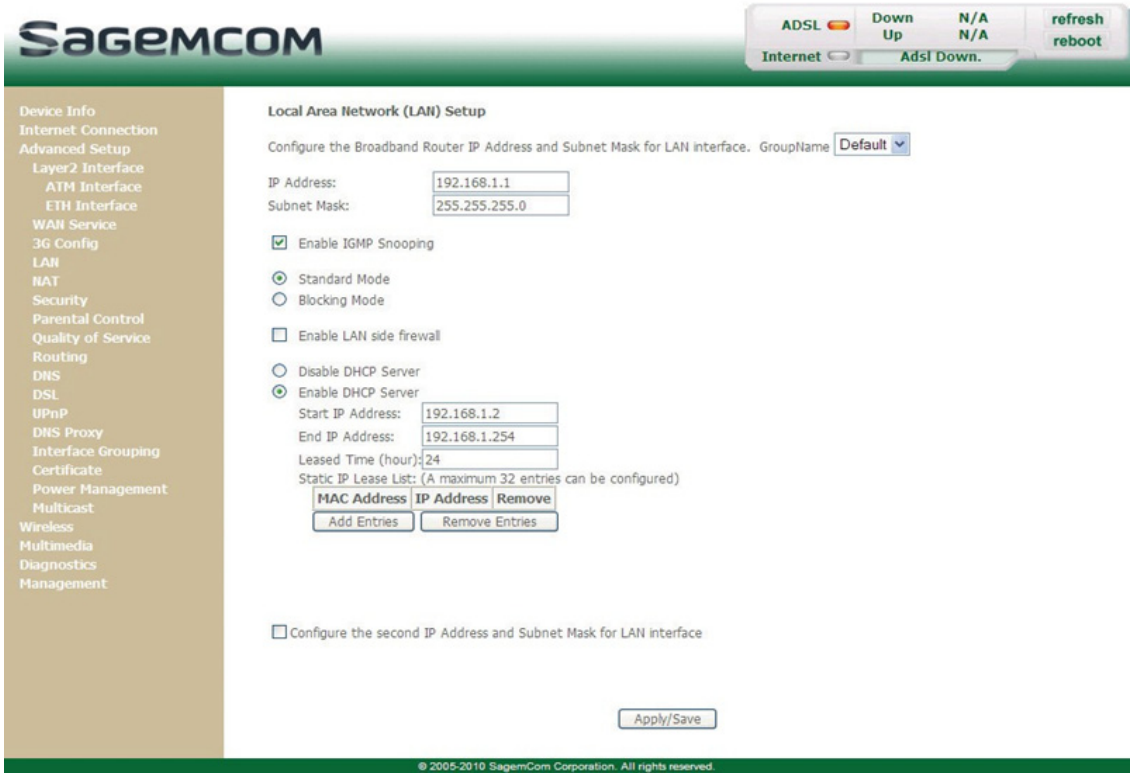
Note

The router needs to be rebooted to take the parameters into account.

5.7.4 LAN

Object: This is used to configure the IP parameters for the local network (LAN).

- In the **Advanced Setup** menu, select **LAN**.
  The following screen opens:



Field	Action	Default value
Groupname	Select the required group.	**Default**
IP Address	Enter the address of your local network.	**192.168.1.1**
Subnet Mask	Enter your network's subnet mask.	**255.255.255.0**
Enable IGMP Snooping	Check this box to activate the IGMP (**I**nternet **G**roup **M**anagement **P**rotocol) protocol. This lets you manage the declarations of belonging to one or more groups with Multicast routers.	**Not checked**
Standard Mode[a]	Check the box if you wish the IGMP snooping runs in normal mode (transparency with IGMP frames).	**Checked**
Blocking Mode[a.]	Check the box if you wish the IGMP snooping runs in blocking mode (interception and removal of IGMP frames).	**Not checked**
Enable LAN side firewall	Check the box to activate the LAN side firewall.	**Not checked**
Disable DHCP Server	Check this box to deactivate your router's DHCP server. **Note:** You must configure your computer with the parameters appropriate to your local network (IP address, subnet mask and default gateway) as well as enter the primary and secondary DNS server addresses.	**Not checked**

Field	Action	Default value
Enable DHCP	Check this box to activate your router's DHCP server. **Note:** You must configure your computer as DHCP client and DNS client (or enter the primary and secondary DNS server addresses).	**Checked**
Start IP Address	Enter the first address attributed by your router's DHCP server.	**192.168.1.2**
End IP Address	Enter the last address attributed by your router's DHCP server.	**192.168.1.254**
Leased Time (hour)	Enter an unavailability time (in hours) for each attributed address.	**24**
Static IP Lease List	Enter if required the list of static IP Lease. **Note:** A maximum of 32 entries can be configured.	**-**
Configure the second IP Address and Subnet Mask for LAN interface	Check the box to configure the IP parameters (IP address, subnet mask) of a second address for the local network (LAN).	**Not checked**
IP Address[b]	Enter a second address for your local network (LAN).	**-**
Subnet Mask[b.]	Enter a subnet mask for the second address for your local network (LAN).	**-**

a. These fields only appear when the "Enable IGMP Snooping" field is activated (box checked).
b. These fields only appear when the "Configure the second IP Address and Subnet Mask for LAN interface" field is activated (box checked).

5.7.5 NAT

Object: NAT is a configurable IP address translation function which is applied to the interfaces of your router which you have activated for this function.

Several translation function configurations and the NAT actions can be configured and may be activated as indicated in section **5.7.5.1 > Add**.

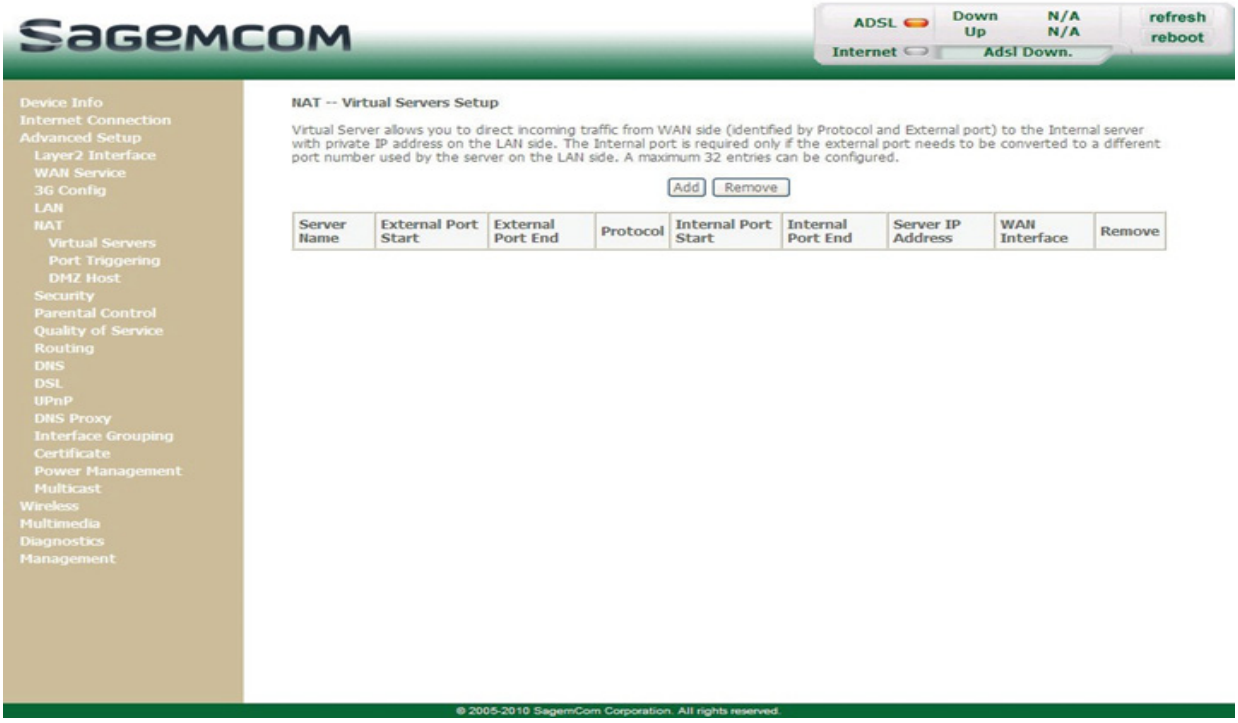
This section contains the following menus:

- Virtual Servers (see subsection 5.7.5.1)
- Port Triggering (see subsection 5.7.5.2)
- DMZ Host (see subsection 5.7.5.3)

5.7.5.1 Virtual Servers

Object: This menu is used to route directly to the External Ports the incoming data from a Service server (such as, for example, FTP Server, SNMP, TFTP etc.) of the remote network (WAN) to computers on the local network (LAN) via the Internal Ports.

- In the **Advanced Setup** menu, select **NAT** then select **Virtual Servers**.
  The following screen opens:

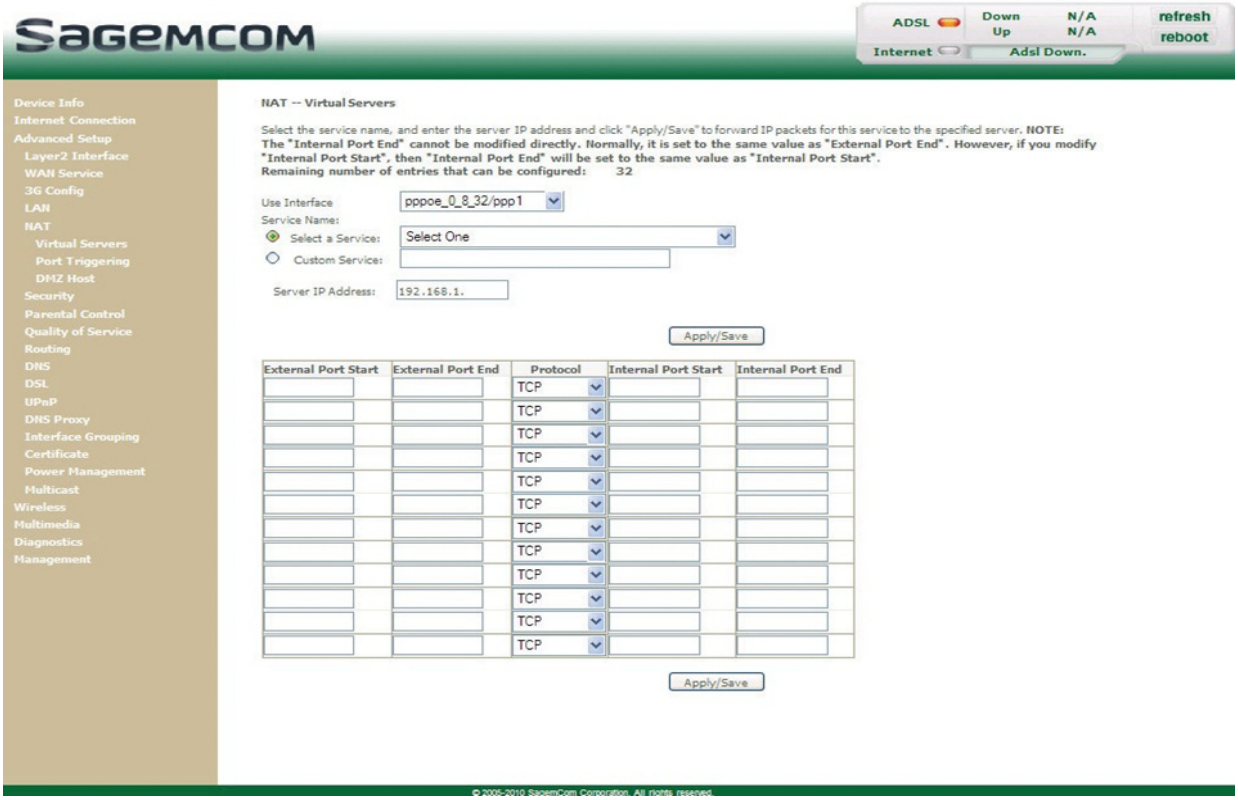


Field	Meaning
Server Name	• **Select a Service**: Service available over Internet (such as, for example FTP Server, SNMP, TFTP etc.). • **Custom Service**: Name you want to allocate to a local server.
External Port Start	Internal start port (WAN side).

Field	Meaning
External Port End	Internal end port (WAN side).
Protocol	Transport protocol (TCP, UDP or TCP/UDP).
Internal Port Start	Internal start port (LAN side).
Internal Port End	This internal end port (LAN side) is associated with the external end port (WAN) side. **Note:** This cannot be modified.
Server IP Address	Computer address delivered by your router's DHCP server.
WAN Interface	WAN interface used.
Remove	Check this box and click on the [**Remove**] button to remove the selected object from the list.

Add

- Click on the **Add** button; the following screen appears:



Proceed as follows:

- Select the required WAN interface in the **Use Interface** list.
- Check the **Select a Service** box, then select the service of your choice from the scroll down list, for example "SNMP".

  The **External Port Start**, **External Port End**, **Internal Port Start**, **Internal Port End** and **Protocol** fields (transport protocol associated with this service) are automatically filled in the table.

Note

You may complete the table by adding other ports associated with a protocol.

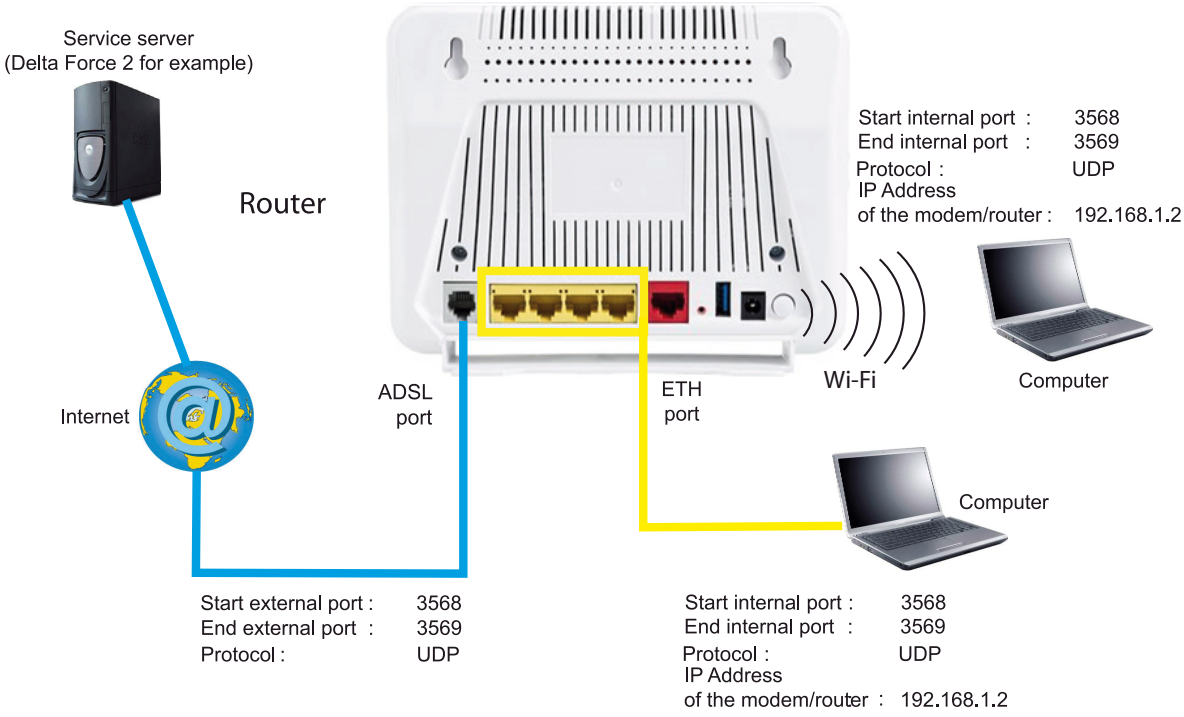
or

- Check the **Custom Service** box, enter the name of the server you want to connect to, then:
  - Complete the ID Host of your computer's IP address (this is attributed by your router's DHCP server).
  - Fill in the **External Port Start**, **External Port End**, **Internal Port Start**, **Internal Port End** and **Protocol** fields.

A few rules for entering values:

- When you want to select a single port, the start port (**External Port Start** or **Internal Port Start**) and the end port (**External Port End** or **Internal Port End**) must be identical.
- When you want to select a range of ports, the start port number must be lower than the end port number.
- You must always start entering with the **External Port Start** and **External Port End** ports.
- When you allocate a number to an **External Port Start**, the same number is automatically allocated to the **Internal Port Start** and identically for **External Port End**.

The following diagram contains an example:



The "Delta Force 2" service is available on your computer via the external ports 3568 and 3569 (WAN side) and via the internal ports 3568 and 3569 (LAN side).

5.7.5.2 Port Triggering

Object: The purpose of this menu is to open dynamically the firewall ports (open ports) via "Trigger Ports" when an application (such as games or video) opens a connection via the transport layer (TCP or UDP).

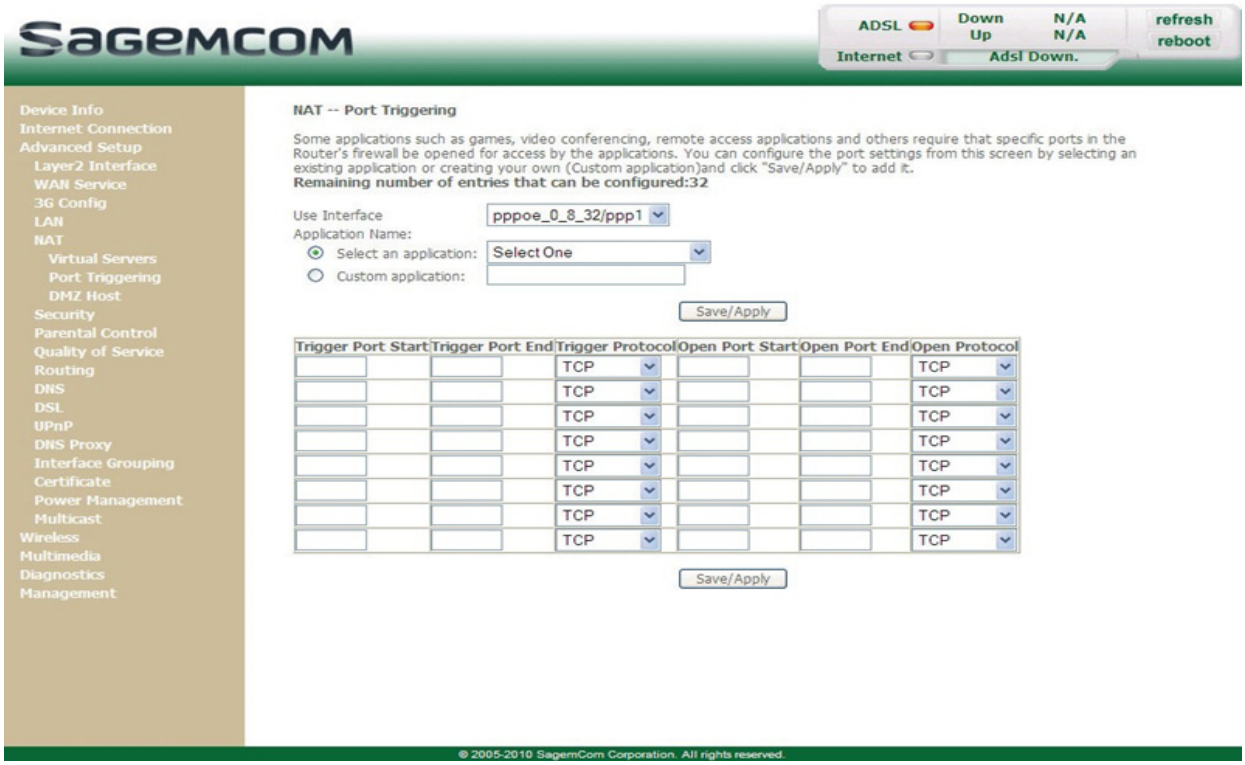
- In the **Advanced Setup** menu, select **NAT** then select **Port Triggering**.

  The following screen opens:

Field	Meaning
Application Name	Application name.
Trigger	• **Protocol**: Transport protocol (TCP, UDP or TCP/UDP). • **Port Range**: A port range contains a Start port and an End port. **Note:** A single port is characterised by an identical start port and end port.
Open	• **Protocol**: Transport protocol (TCP, UDP or TCP/UDP). • **Port Range**: A port range contains a Start port and an End port. **Note:** A single port is characterised by an identical start port and end port.
WAN Interface	WAN Interface used.
Remove	To remove an entry from the list, check the box and click on the [**Remove**] button.

Add

- Click on the **Add** button; the following screen appears:



To configure **Trigger Port** and **Open Port**, proceed as follows:

- Select the required WAN interface in the **Use Interface** list.
- Check the **Select an application** box, then select the service of your choice from the scroll down list, for example "Aim Talk".

  The **Trigger Port Start**, **Trigger Port End**, **Open Port Start**, **Open Port End** and **Protocol** fields (transport protocol associated with this service) are automatically filled in the table.

Note

You may complete the table by adding other ports associated with a protocol.

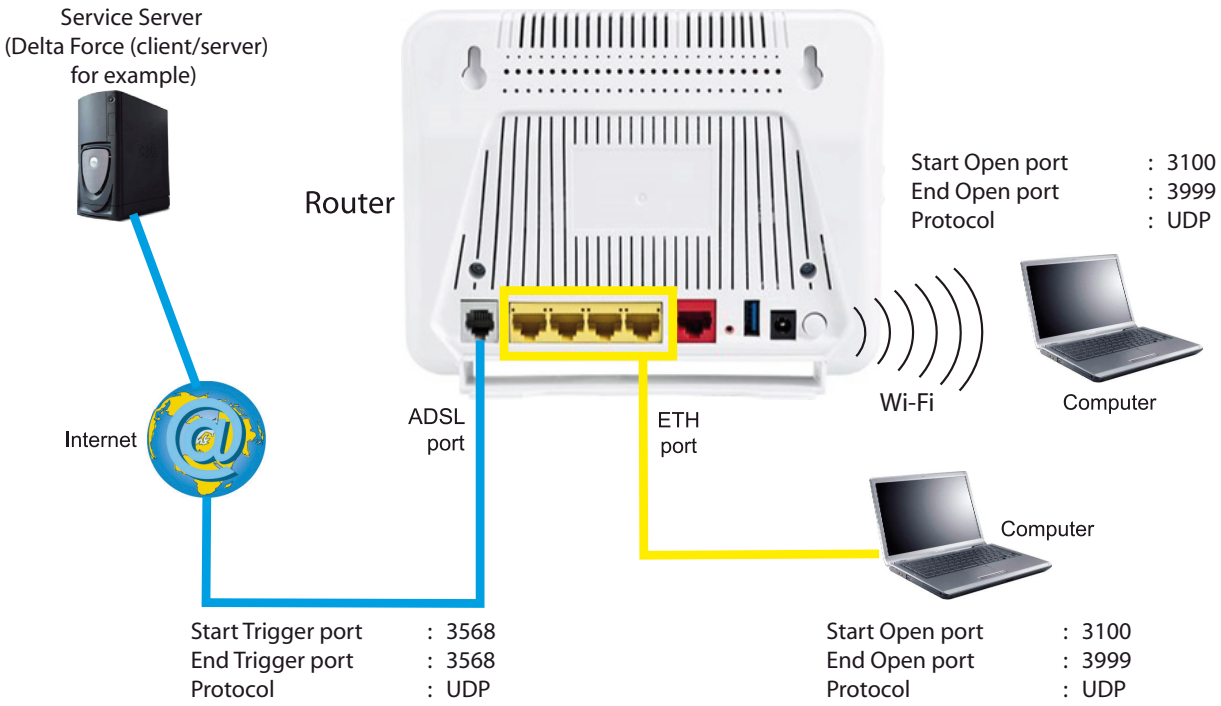
or

- Check the **Custom application** box to specify your own application, then:
  - Enter the name of your own application.
  - Fill in the **Trigger Port Start**, **Trigger Port End**, **Open Port Start**, **Open Port End** and **Protocol** fields.

A few rules for entering values:

- When you want to select a single port, the start port (**Trigger Port Start** or **Open Port Start**) and the end port (**Trigger Port End** or **Open Port End**) must be identical.
- When you want to select a range of ports, the start port number must be lower than the end port number.

The following diagram contains an example:



Using the "Trigger" 3568 port (WAN side), the "Delta Force" service server triggers the opening of port range 3100 to 3999 for your computer to access this service.

5.7.5.3 DMZ Host

Object: This "DMZ" (**De**M**ilitarized** **Z**one) lets you access the server you selected directly via the Internet without going through the "Firewall".

Important

Caution, this process presents an intrusion risk. It is therefore vital that you take precautions so that no connections may be initiated to the private network.

- In the **Advanced Setup** menu, select **NAT** then select **DMZ Host**.

  The following screen opens:

Field	Action	Default value
DMZ Host IP Address	Enter the IP address of a server to activate the "DMZ" and therefore access it directly from the Internet. To deactivate the "DMZ" zone, erase the address entered in the field. **Note:** Click on the **Apply/Save** button to take account of the address or its erasure.	-

Note

The **DMZ** zone is deactivated by default.

5.7.6 Security

5.7.6.1 IP Filtering

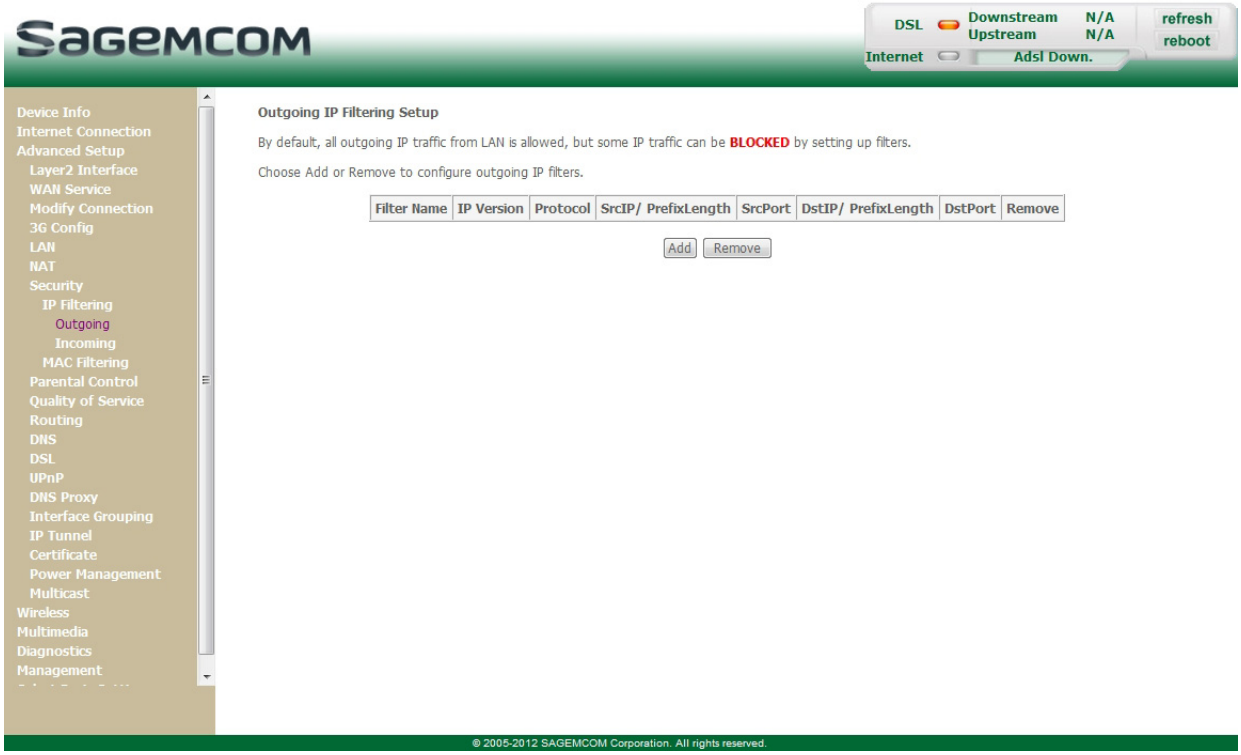
Outgoing

Object: This menu is used to create outgoing IP filters to refuse data from the LAN to the WAN and list the existing outgoing IP filters.

By default, all the outgoing data is accepted.

- In the **Advanced Setup** menu, select **Security > IP Filtering > Outgoing**.

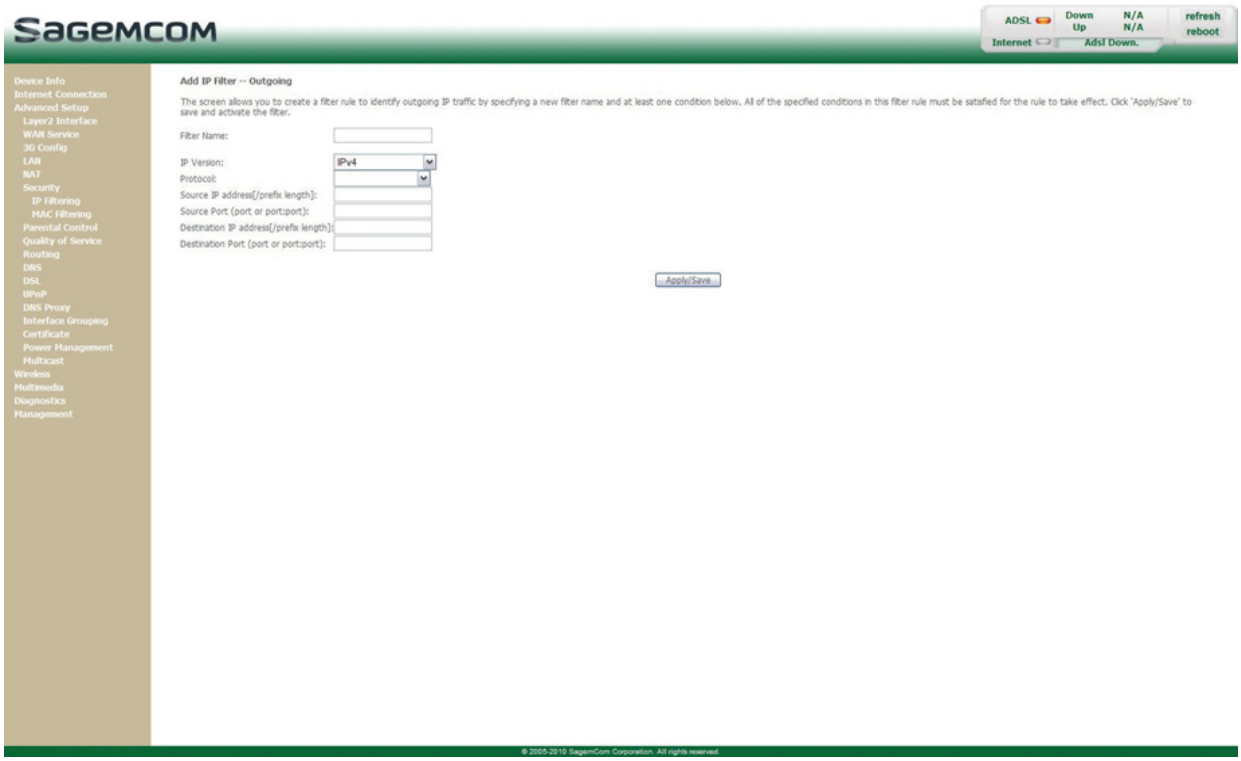
  The following screen opens:



Field	Meaning
Filter Name	Name of the filter.
IP Version	IP version used.
Protocol	Transport protocol.
SrcIP/ PrefixLength	"Source" address (your computer, for example) and associated subnet mask.
Source Port	Source port.
DstIP/ PrefixLength	"Destination" address (a machine on the Internet, for example) and associated subnet mask.
DstPort	Destination port.
Remove	Check the box and click on the [**Remove**] button to remove the object from this list.

Add

- Click on the **Add** button to display the following screen:



Field	Action
Filter Name	Enter a representative name for the filter.
IP Version	Select the dedicated IP version from the scroll down list (for example: IPv4).
Protocol	Select the dedicated protocol from the scroll down list (TCP/UDP, TCP, UDP, ICMP).
Source IP address[/prefix length]	Enter the Source IP address (LAN).
Source Subnet Mask	Subnet Mask.
Source Port (port or port:port)	Enter a "Source" port (LAN) or range of ports. **Note:** For one port, for example, enter 80. For a range of ports, enter 80:90.
Destination IP address[/prefix length]	Enter the Destination IP address (WAN).
Destination Port (port or port:port)	Enter a "Destination" port (WAN) or range of ports. **Note:** For one port, for example, enter 80. For a range of ports, enter 80:90.

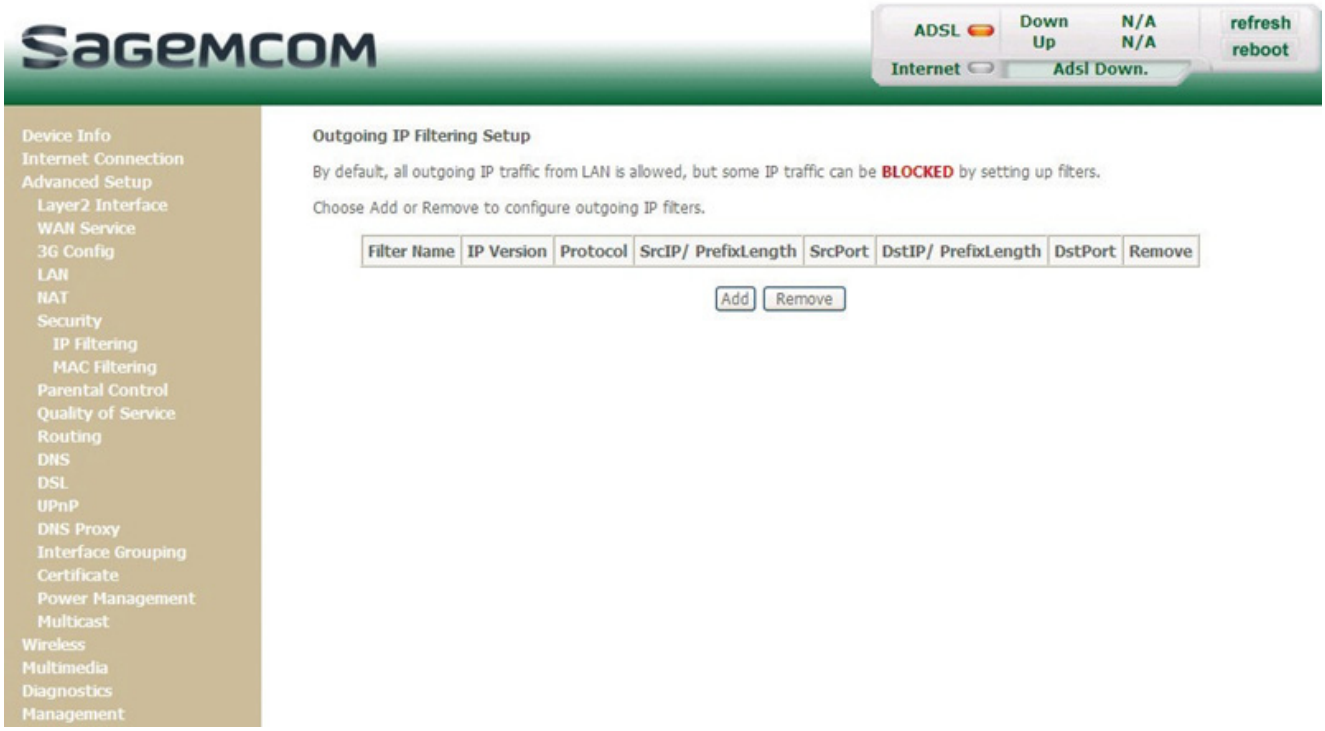
Incoming

Object: This menu is used to create incoming IP filters to refuse data from the WAN to the LAN and list the existing incoming IP filters.

By default, all the incoming data is refused when the Firewall is activated.

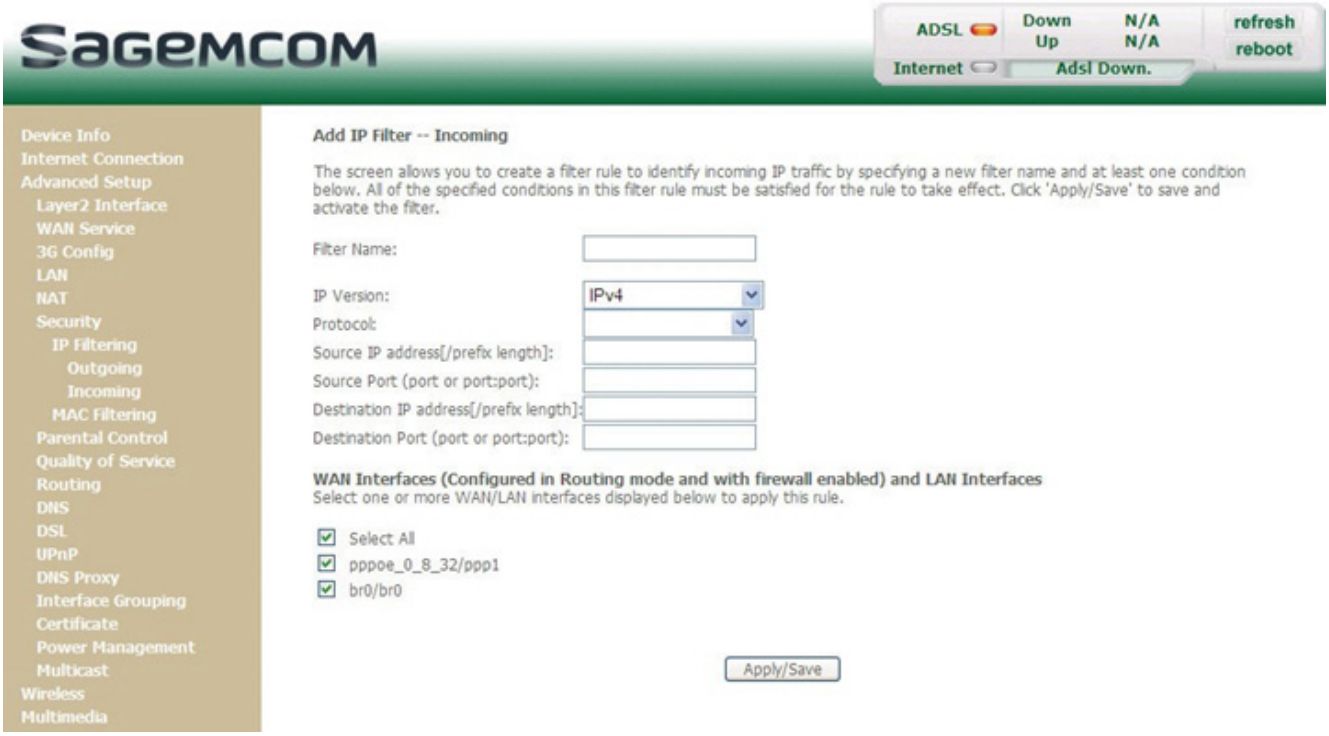
- In the **Advanced Setup** menu, select **Security > IP Filtering > Incoming**.

  The following screen opens:



Add

- Click on the **Add** button to display the following screen:



Field	Action
Filter Name	Enter a representative name for the filter.
IP Version	Select the dedicated IP version from the scroll down list (for example: IPv4).
Protocol	Select the dedicated protocol from the scroll down list (TCP/UDP, TCP, UDP, ICMP).
Source IP address[/prefix length]	Enter the Source IP address (WAN).
Source Port (port or port:port)	Enter a "Source" port (WAN) or range of ports. **Note:** For one port, for example, enter 80. For a range of ports, enter 80:90.
Destination IP address[/prefix length]	Enter the destination IP address (LAN).
Destination Port (port or port:port)	Enter a "destination" port (LAN) or range of ports. **Note:** For one port, for example, enter 80. For a range of ports, enter 80:90.

WAN interfaces

Field	Action	Default value
Select All	Check the box to select all WAN interfaces. **Note:** By unchecking the box, no interface is selected and the other WLAN/LAN interfaces displayed boxes become unchecked.	**Checked**
pppoe_0_8_32/ppp1	Check the box to select the displayed interface.	**Checked**
br0/br0	Check the box to select the displayed interface.	**Checked**

5.7.7 Parental Control

Object: This menu is used to create and manage access time and Url restrictions for LAN devices which are connected to the router.

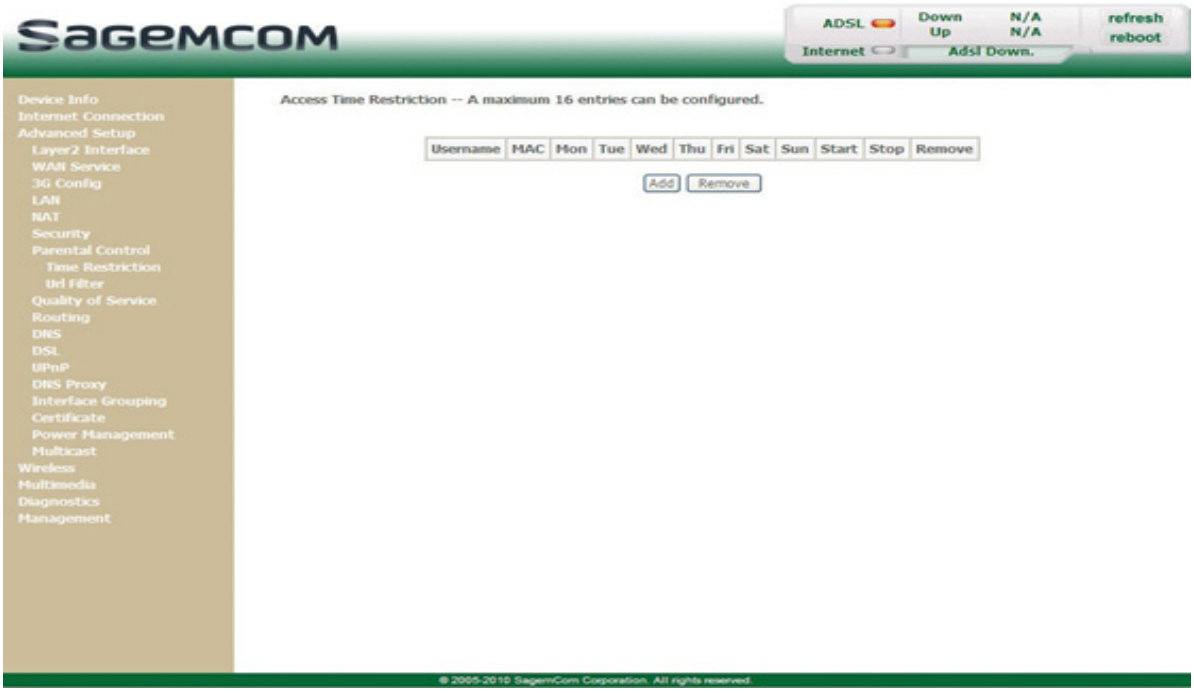
This section contains the following menus:

- Time Restriction (see subsection 5.7.7.1)
- Url Filter (see subsection 5.7.7.2)

5.7.7.1 Time Restriction

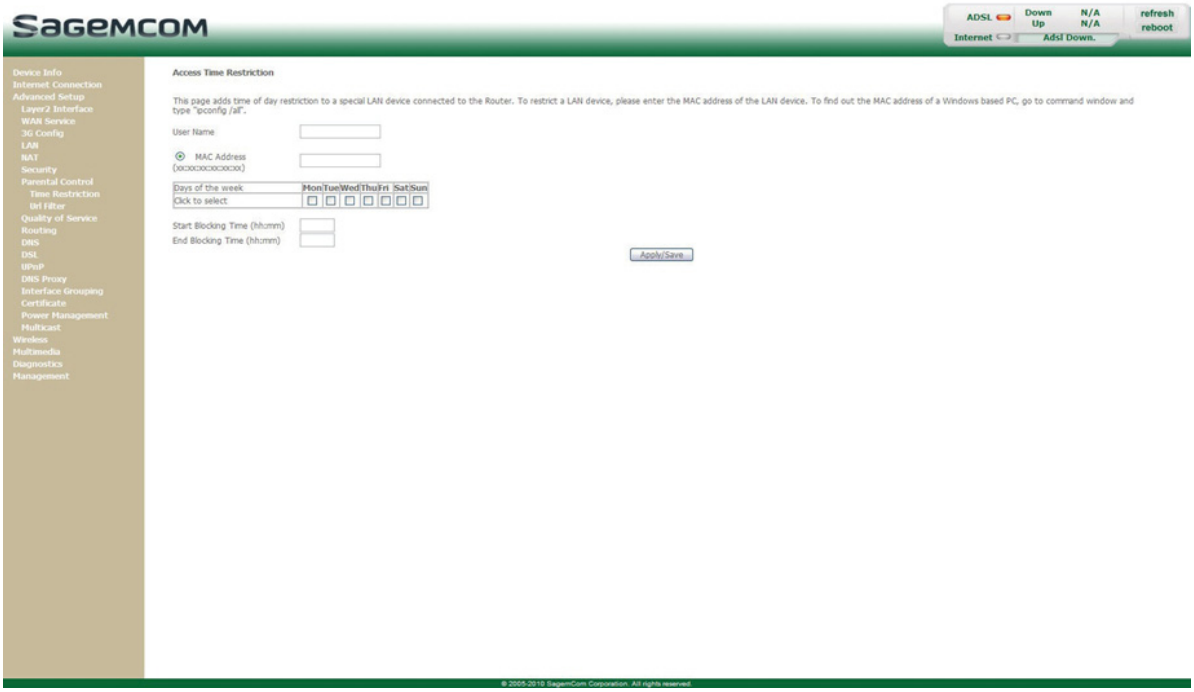
Object: This menu is used to create and manage access time restriction for LAN devices which are connected to the router.

- In the **Advanced Setup** menu, select **Parental Control > Time Restriction**.
  The following screen opens:



Add

- Click on the **Add** button to display the following screen:



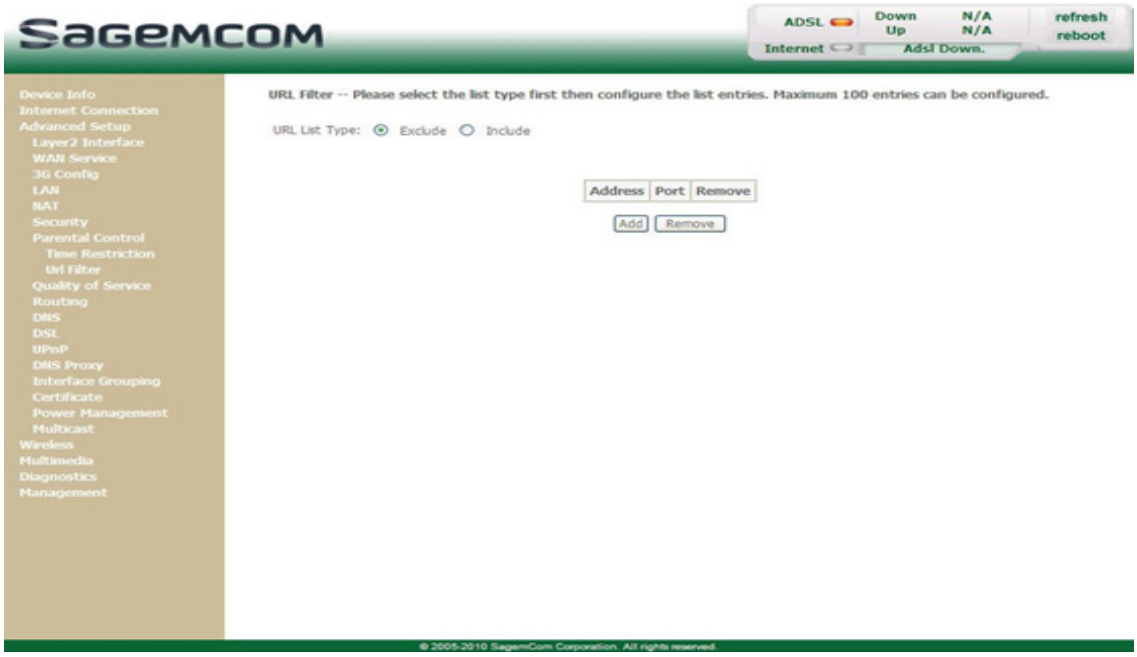
Field	Action
User Name	Enter a representative name for the LAN device.
MAC Address	Enter the MAC address of the required LAN device. **Note:** To find out the MAC address of a Windows based PC, open a command window and type "ipconfig /all".
Days of the week	Select the days of the week on which the restriction is effective by checking the corresponding box.
Start Blocking Time (hh:mm)	Enter the required blocking start hour (for example 08:00).
End Blocking Time (hh:mm)	Enter the required blocking end hour (for example 20:00).

5.7.7.2 Url Filter

Object: This menu is used to create and manage Url access restriction for LAN devices which are connected to the router.

- In the **Advanced Setup** menu, select **Parental Control > Url Filter**.

  The following screen opens:



Add

- Click on the **Add** button to display the following screen:

Field	Action
URL Address	Enter the Url address whose access must be restricted.
Port Number	Enter the port number of the address which access must be restricted. **Note:** 80 will be applied by default.

5.7.8 Quality of Service

This menu contains the following sub-menus:

- Queue Config (see subsection 5.7.8.1)
- QoS Classification (see subsection 5.7.8.2)

Object: This menu is used to allocate different types of traffic queues with different priorities in order to improve the traffic flow. To do this, the quality of service (QoS) provides the following three services: Classification (set-1, set-2), Marking (TOS, DSCP) and queues (Queuing).

The quality of service is only significant if all the traffic (data, video) is greater than the up rate of the ADSL line.

- In the **Advanced Setup** menu, select **Quality of Service**.

  The following screen opens:

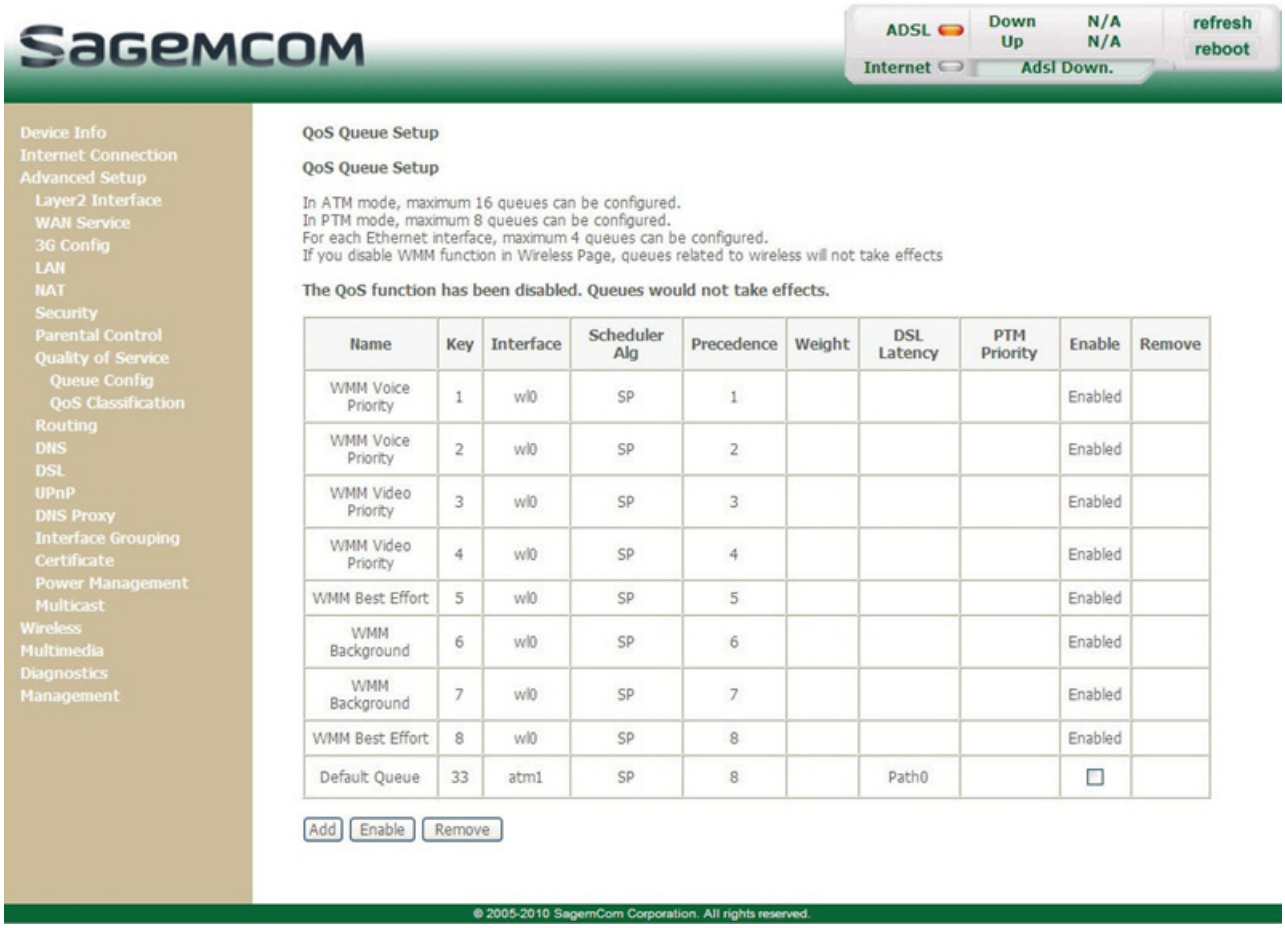
Field	Action
Enable QoS	Check the **Enable QoS** box to authorize QoS actions to be performed at the ingress and egress interfaces.
Select Default DSCP Mark	The IP datagram DSCP (**D**ifferentiated **S**ervices **C**ode **P**oint, priority value from 0 to 63) identifies which output queue a packet is to be assigned to. **Default DSCP Mark** is used to mark the priority of the packets when they are not tagged in the computer. In this case the router will do it with the values indicated. Select from the scroll down list: • No Change (-1) : Value of -1 indicates no change from the incoming packet, • Auto Marking (-2) • Default (000000) : Marks everything else to DSCP 0, • AF13 (001110) • AF12 (001100) : Recommended markings for Bulk-Data, • AF11 (001010) : Recommended markings for Bulk-Data, • CS1 (001000) : Recommended markings for Scavenger traffic, • AF23 (010110) • AF22 (010100) : Recommended markings for Transactional-Data, • AF21 (010010) : Recommended markings for Transactional-Data, • CS2 (010000) : Recommended markings for Network Management, • AF33 (011110) • AF32 (011100) : Recommended markings for Mission-Critical Data, • AF31 (011010) : Recommended markings for Mission-Critical Data, • CS3 (011000) : Call-Signalling markings, • AF43 (100110) • AF42 (100100) : Recommended markings for IP/VC, • AF41 (100010) : Recommended markings for IP/VC, • CS4 (100000) : Recommended markings for Streaming-Video, • EF (101110) : IP Phones mark Voice to EF, • CS5 (101000) • CS6 (11000) : Routers mark Routing traffic to CS6, • CS7 (111000) **Note:** This drop-down list is present only if the box **Enable Qos** is checked.

5.7.8.1 Queue Config

Object: This menu is used to enable or disable QoS on an interface, and to configure QoS to use policy maps attached to an interface.

- In the **Advanced Setup** menu, select **Quality of Service** then select **QoS Queue**.

  The following screen opens:

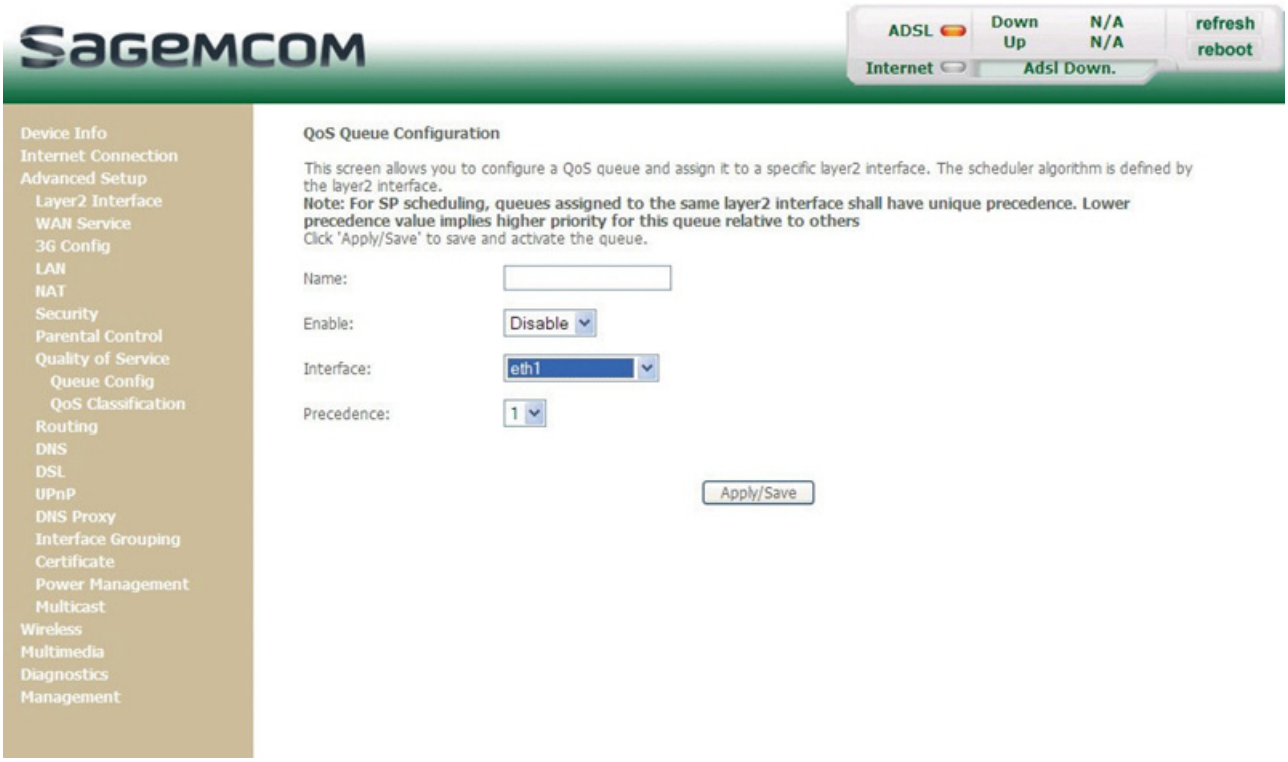


Field	State
Name	Queue entry name
Key	Sequence number allocated by the system, incremented of a unit to each addition of a QoS Queue.
Interface	Name of the network interface configured (8/32 for example).
Scheduler Alg	Scheduler algorithm allocated to this queue.
Precedence	Priority allocated to "Queue Precedence" from 1 to 3.
DSL Latency[a]	DSL Latency
PTM Priority	PTM priority
Enable	QoS enabled or disabled for this interface. **Note:** This status can be amended starting from this window.
Remove	Check the box and click on the [**Remove**] button to remove the queue from this list.

a. This field appears only if the DSL mode selected is IPOA.

Add

- Click on the **Add** button to display the following screen:



Field	Action
Name	Enter a representative name.
Enable	Select from the scroll down list: • **Disable**: To disable the QoS queue entry • **Enable**: To enable the QoS queue entry
Interface	Select from the scroll down list: • **Blank** • **8/32**: Interface name.
Precedence	Select from the scroll down list: • **Blank** • **1**: High priority for this queue, • **2**: Medium priority for this queue, • **3**: Low priority for this queue. **Note:** A high priority leads to low packet loss.
Queue Weight [1-63][a]	Enter the corresponding value of the queue weight.
DSL Latency[a]	Select the DSL latency from the scroll down list.

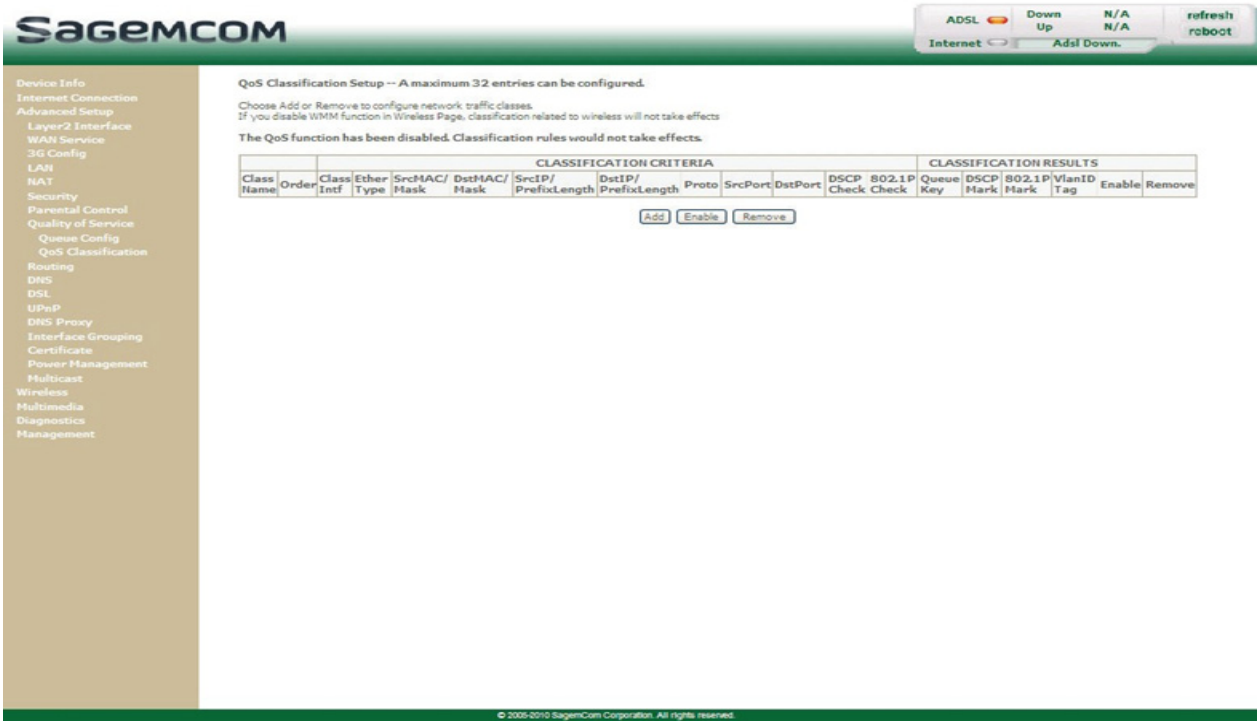
a. This field appears only if the DSL mode selected is IPOA.

5.7.8.2 QoS Classification

Object: This menu is used for the classification of packets into traffic classes, and for the enforcement of policies using queuing.

- In the **Advanced Setup** menu, select **Quality of Service** then select **QoS Classification**.

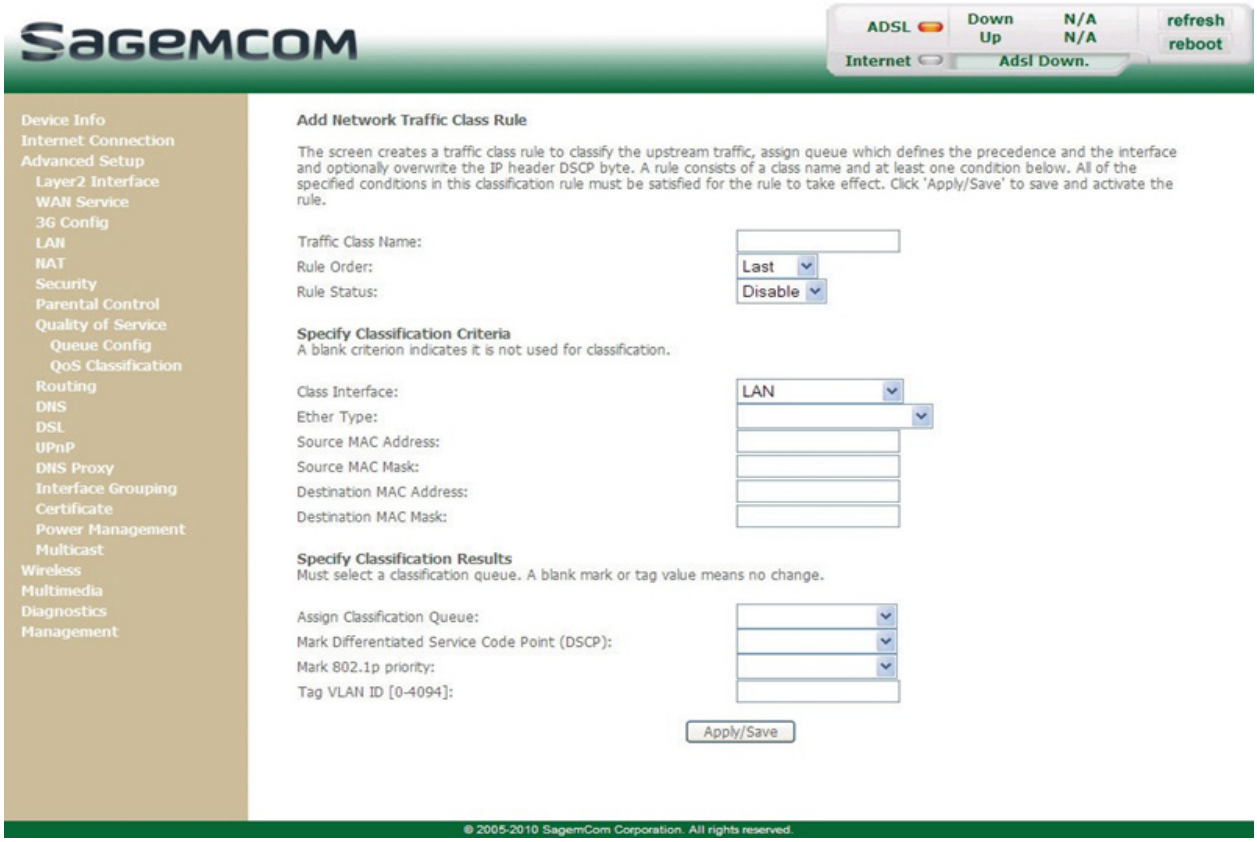
  The following screen opens:



Field		State
Class Name		Traffic Class Name.
Order		Sequence number.
Classification Criteria		
	Class Intf	Class Interface (Local, eth0, wl0).
	Ether Type	Nature of the LAN port.
	SrcMAC/Mask	"Source" MAC address (your computer, for example) and associated subnet mask.
	DstMAC/Mask	"Destination" MAC address (a machine on the Internet, for example) and associated subnet mask.
	SrcIP/Prefixlength	"Source" address (your computer, for example) and associated subnet mask.
	DstIP/Prefixlength	"Destination" address (a machine on the Internet, for example) and associated subnet mask.
	Proto	Protocol used.
	Src Port	"Source" port.
	Dst Port	"Destination" port.
	DSCP Check	Differentiated Services Code Point, priority value from Default to CS7.
	802.1P Check	Priority field 802.1P (value between 0 and 7).
Classification Results		
	Queue Key	Queue number, allocated by the system according to the selected precedence.
	DSCP Mark	DSCP priority (from Default to CS7).
	802.1P Mark	Priority field 802.1P (value between 0 and 7).
	Enable	QoS enabled or disabled for this traffic class. **Note:** This status can be amended starting from this window.
	Remove	Check this box and click on the [**Remove**] button to remove the selected object from the list.

Add

- Click on the **Add** button to display the following screen:



Field	Action
Traffic Class Name	Enter a name for the traffic class you want to create.
Rule Order	Select from the scroll down list: • **Blank** • **Last** • **Number**: Number allotted by the system to the existing rules
Rule Status	Select from the scroll down list: • **Disable**: QoS disabled for this static class rule • **Enable**: QoS enabled for this static class rule
Class Interface	Select from the scroll down list: • **LAN** • **WAN** • **Local** • **ipoa1** • **pp1/atm0** • **...**

Field	Action
Ether Type	Select from the scroll down list: • **IP** • **ARP** • **IPv6** • **PPPoE_DISC** • **PPPoE_SES** • **8865** • **8866** • **8021Q**
Source MAC Address	Enter a "Source" MAC address.
Source MAC Mask	Enter a "Source" MAC mask.
Destination MAC Address	Enter a "Destination" MAC address.
Destination MAC Mask	Enter a "Destination" MAC mask.
Specify Class Queue	Select from the scroll down list: • **Blank** • **Number**: Priority number and associated queue number, defined by the system starting from the "Queue Precedence" (see subsection 5.7.8.1).
Mark Differentiated Service Code Point (DSCP)	Select the type of Differentiated Services Code Point (DSCP) mark to be allocated (6-bit coding) from the scroll down list. Default to CS7: 000000 to 111000
Mark 802.1p priority	Select Blank or a priority value between 0 and 7 from the scroll down list.
Tag VLAN ID [0-4094]	Enter a value from 0 to 4094.

5.7.9 Routing

This menu contains the following sub-menus:

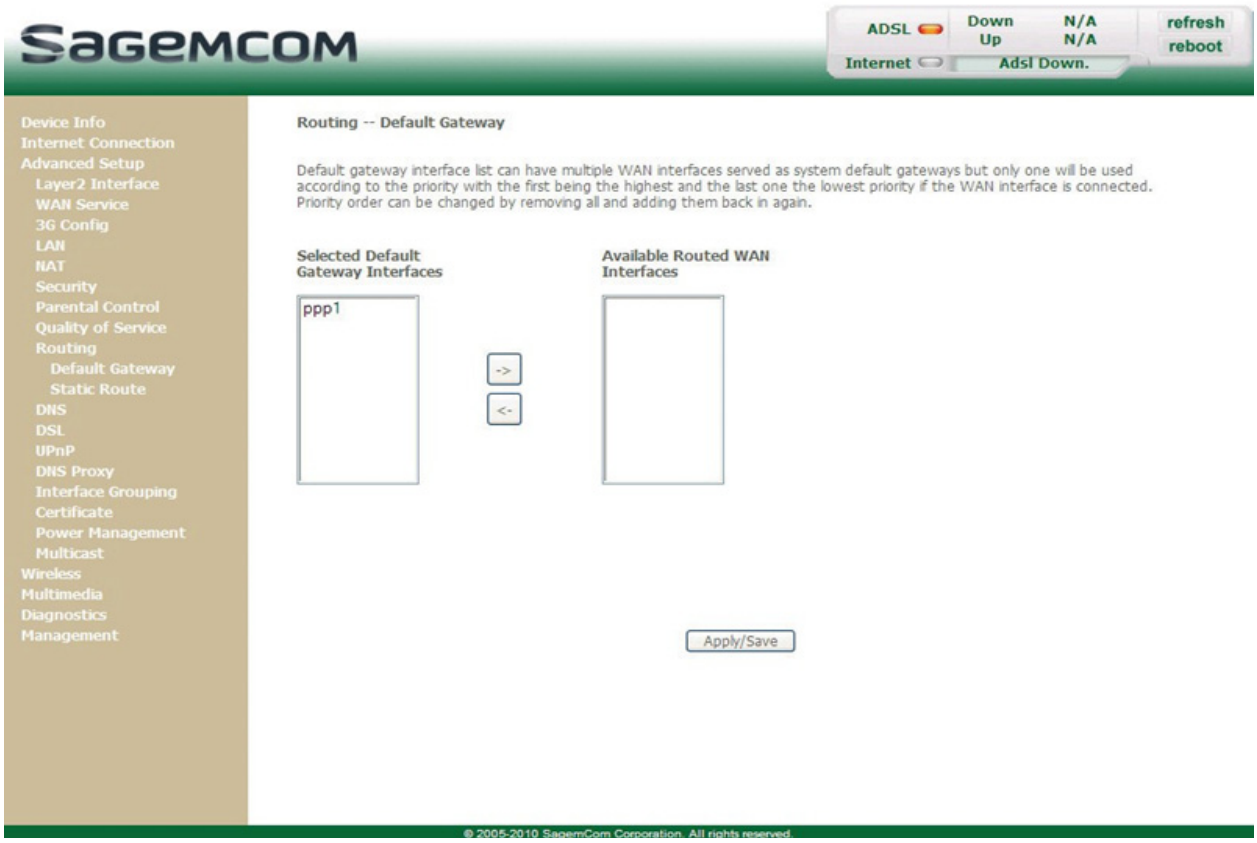
- Default Gateway (see subsection 5.7.9.1)
- Static Route (see subsection 5.7.9.2)

5.7.9.1 Default Gateway

Object: This menu is used either to allocate dynamically a default gateway address to the router from a PVC or to enter an address or choose an interface.

- In the **Advanced Setup** menu, select **Routing** then select **Default Gateway**.

The following screen opens:



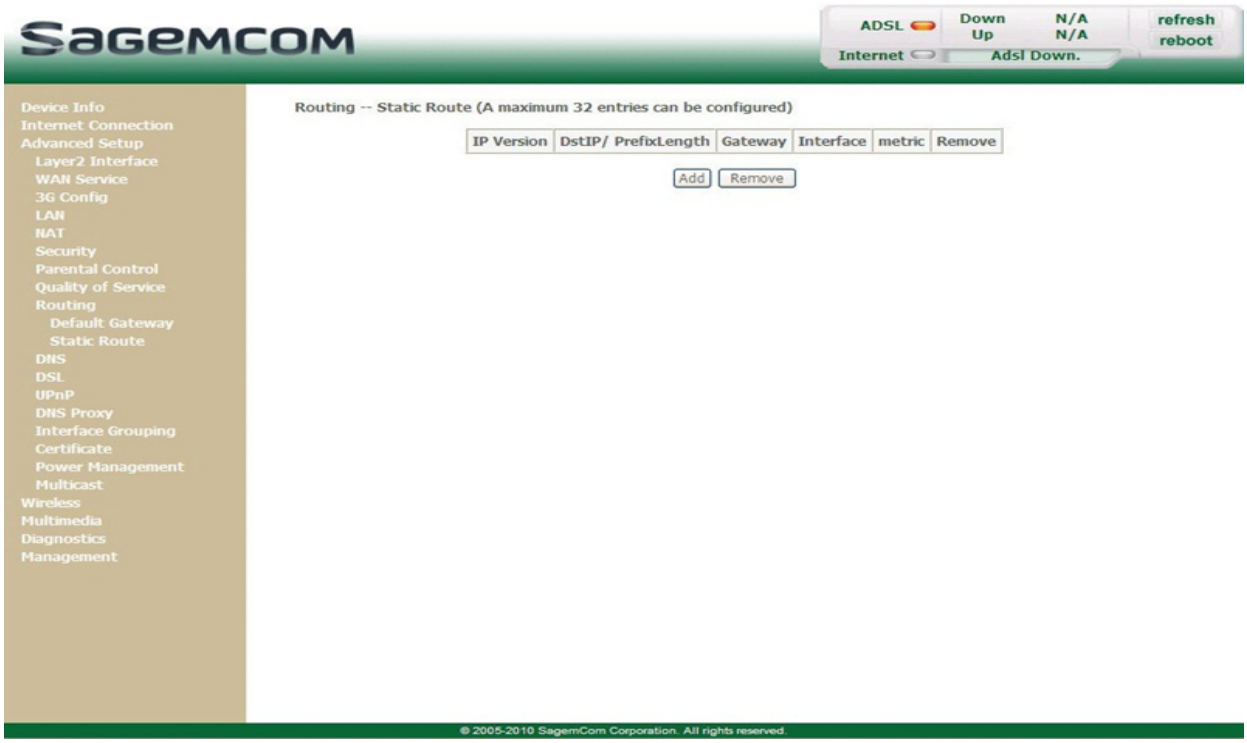
Default Gateway

Button	Action
<-	Transfer the interfaces selected in the **Available Routed WAN Interfaces** area to the **Selected Default Gateway Interfaces** area.
->	Transfer the interfaces selected in the **Selected Default Gateway Interfaces** area to the **Available Routed WAN Interfaces** area.

5.7.9.2 Static Route

Object: This menu is used to add a static route.

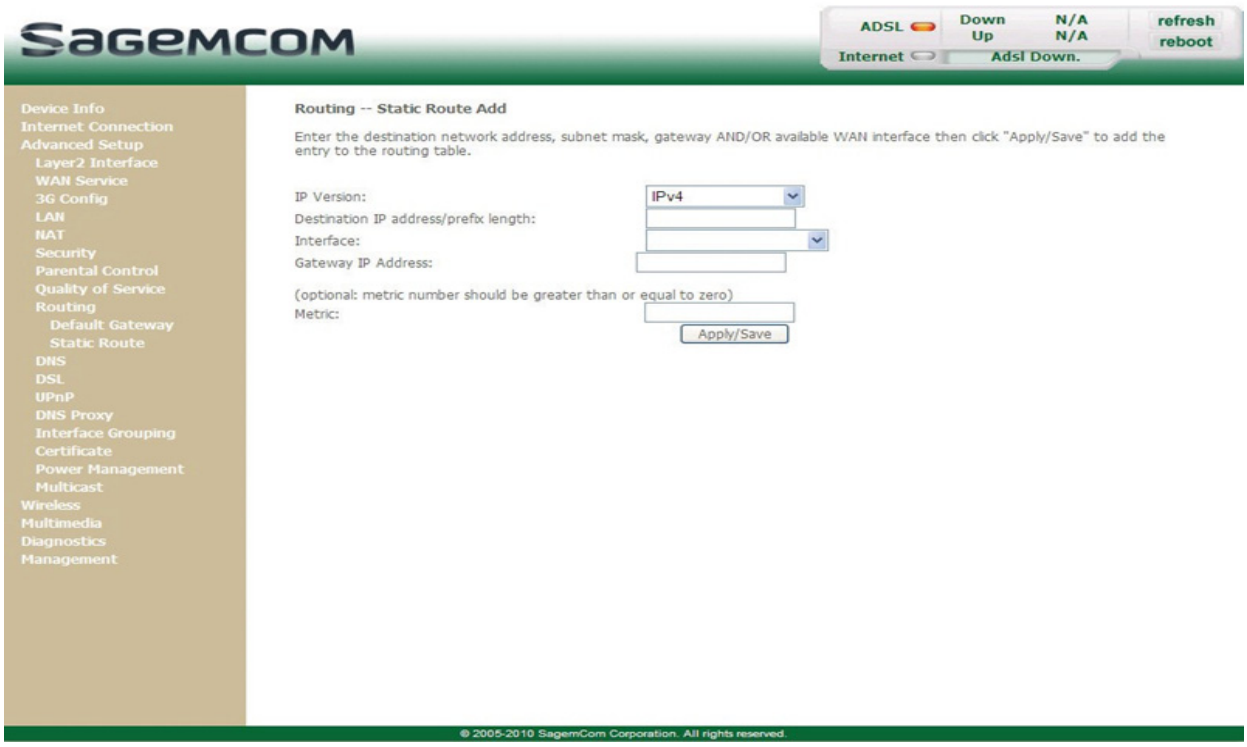
- In the **Advanced Setup** menu, select **Routing** then select **Static Route**.
  The following screen opens:



Field	Meaning
IP Version	Internet Protocol version 4.
DstIP/ PrefixLength	"Destination" address (a machine on the Internet, for example) and associated subnet mask.
Gateway	Default gateway of the remote network.
Interface	Remote network interface.
Metric	Number of hops to reach a distant terminal from the Residential Gateway.
Remove	Check this box and click on the [**Remove**] button to remove the selected object from the list.

Add

- Click on the **Add** button to display the following screen:



Field	Action
IP Version	Internet Protocol.
Destination Network Address/prefix length	Enter the IP address of the remote network.
Interface	Select the interface you want to use from the scroll down list (pppoa_0_8_32 for example).
Gateway IP Address	Enter the gateway IP address.
Metric	Number of hops to reach a distant terminal from the Residential Gateway. **Note:** Metric number should be greater than or equal to one.

5.7.10 DNS

Object: This menu lets you select DNS Server Interface from available WAN interfaces or enter static DNS server IP addresses for the system.

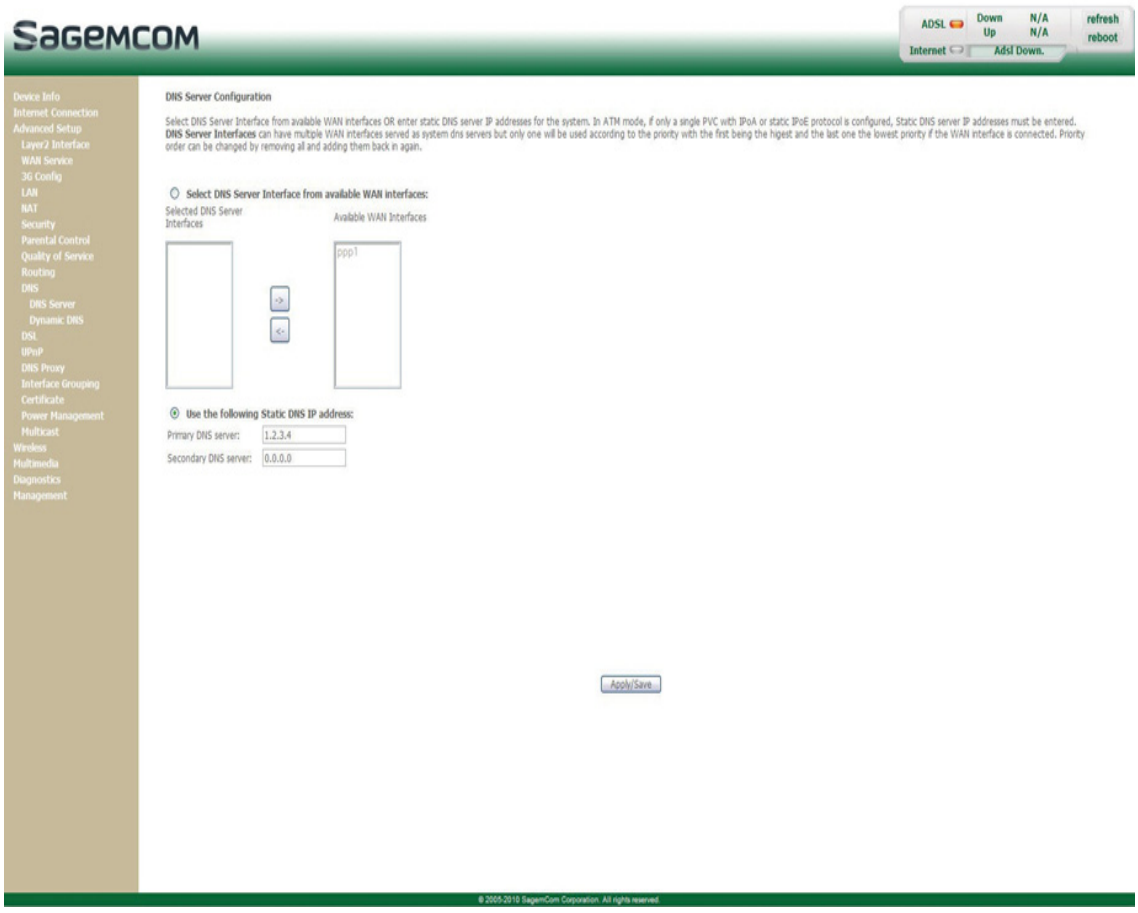
This section contains the following subtitles:

- DNS Server (see subsection 5.7.10.1)
- Dynamic DNS (see subsection 5.7.10.2)

5.7.10.1 DNS Server

Object: This menu enables the automatic resolution of domain names by polling remote servers.

- In the **Advanced Setup** menu, select **DNS** then select **DNS Server**.
  The following screen opens:



Field	Action
Selected DNS Server Interfaces	For more details, a summary table is presented below for each column.
Available WAN Interfaces	
Primary DNS server	Enter the primary DNS server
Secondary DNS server	Enter the primary DNS server

Select DNS Server Interface from available WAN interfaces

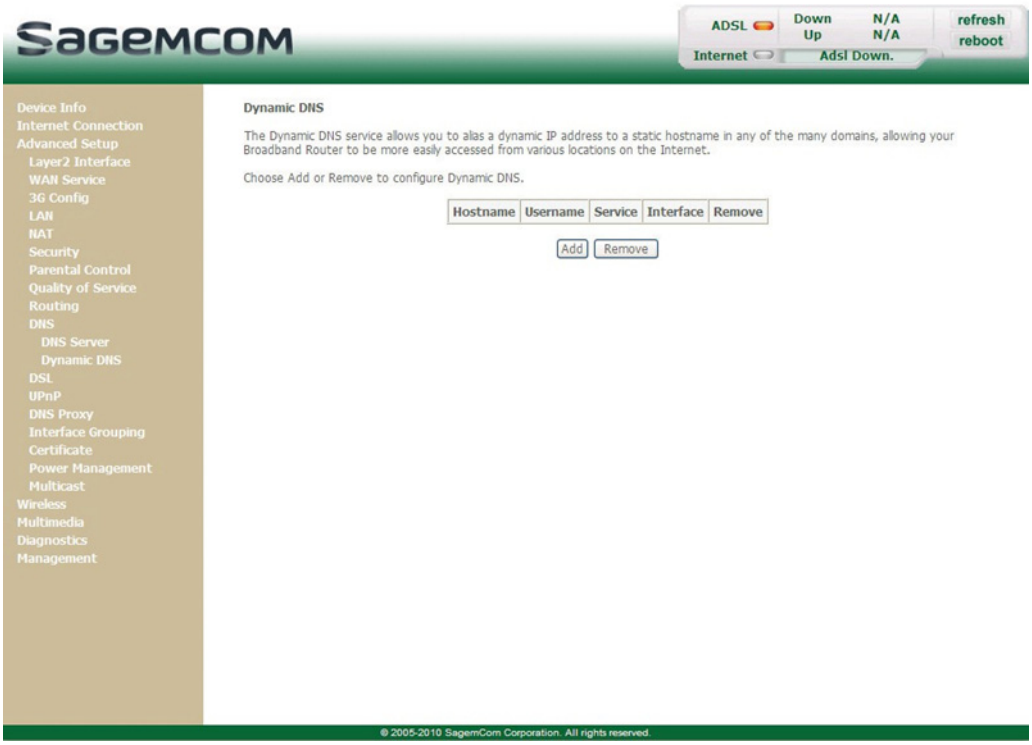
Button	Action
<-	Transfer the interfaces selected in the **Available WAN Interfaces** area to the **Selected DNS Server Interfaces** area.
->	Transfer the interfaces selected in the **Selected DNS Server Interfaces** area to the **Available WAN Interfaces** area.

5.7.10.2 Dynamic DNS

Object: Enables a web surfer to access your router (having no fixed IP address but only a DNS entry) through a dynamic DNS provider such as, for example, **dyndns.org**.

- In the **Advanced Setup** menu, select **DNS** then select **Dynamic DNS**.

  The following screen opens:



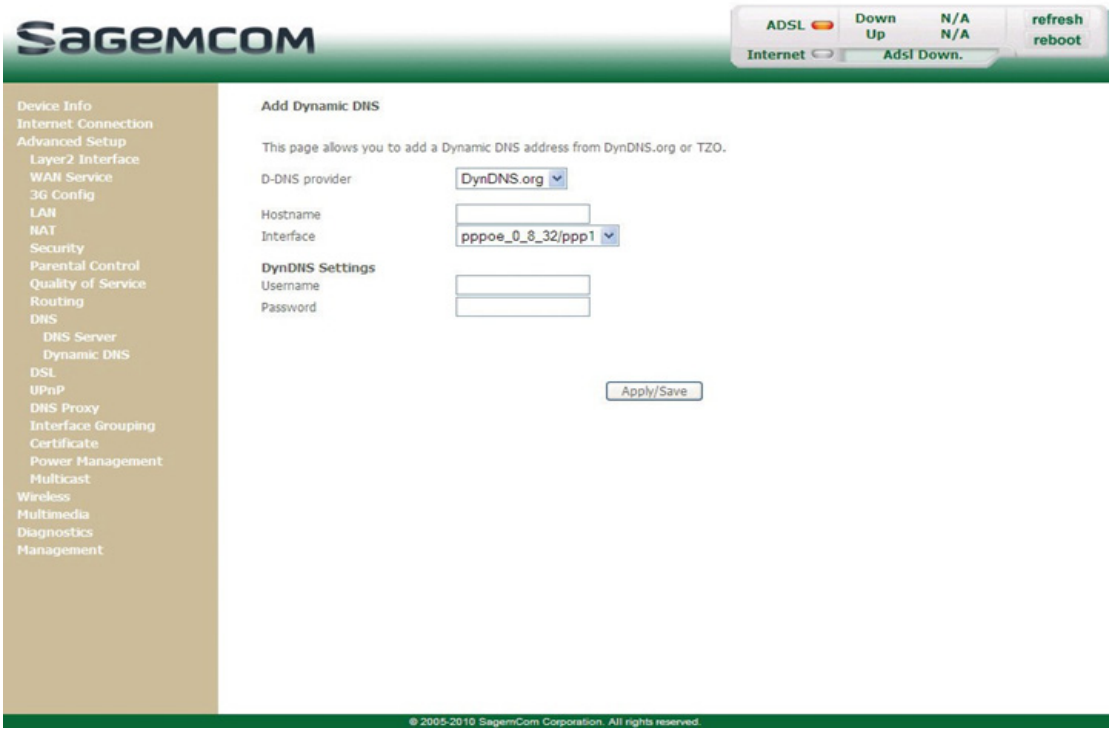
Refer to the next subsection (**Add**) for detailed information on the fields of the table.

Note

The "Service" field is automatically filled by the system in "**dyndns**".

Add

The following screen opens:



Add dynamic DDNS

Field	Action
D-DNS provider	Select from the relevant drop-down list: • DynDNS.org • TZO
Hostname	Enter the symbolic name (for example butterfly) that you want to assign to your Residential Gateway. This is the name provided to you by your dynamic DNS provider (see Note).
Interface	Select from the relevant drop-down list the WAN interface which you want to use (pppoa_0_8_32/pppoa0 for example).

Note

If you enter the name "butterfly", the dynamic DNS provider (dyndns.org for example) incorporates this name in the domain name (butterfly.dyndns.org). The web surfer who wants to access your Residential Gateway receives from the dynamic DNS provider the dynamic IP address (transcription of the domain name) of your Residential Gateway supplied by your Internet service provider.

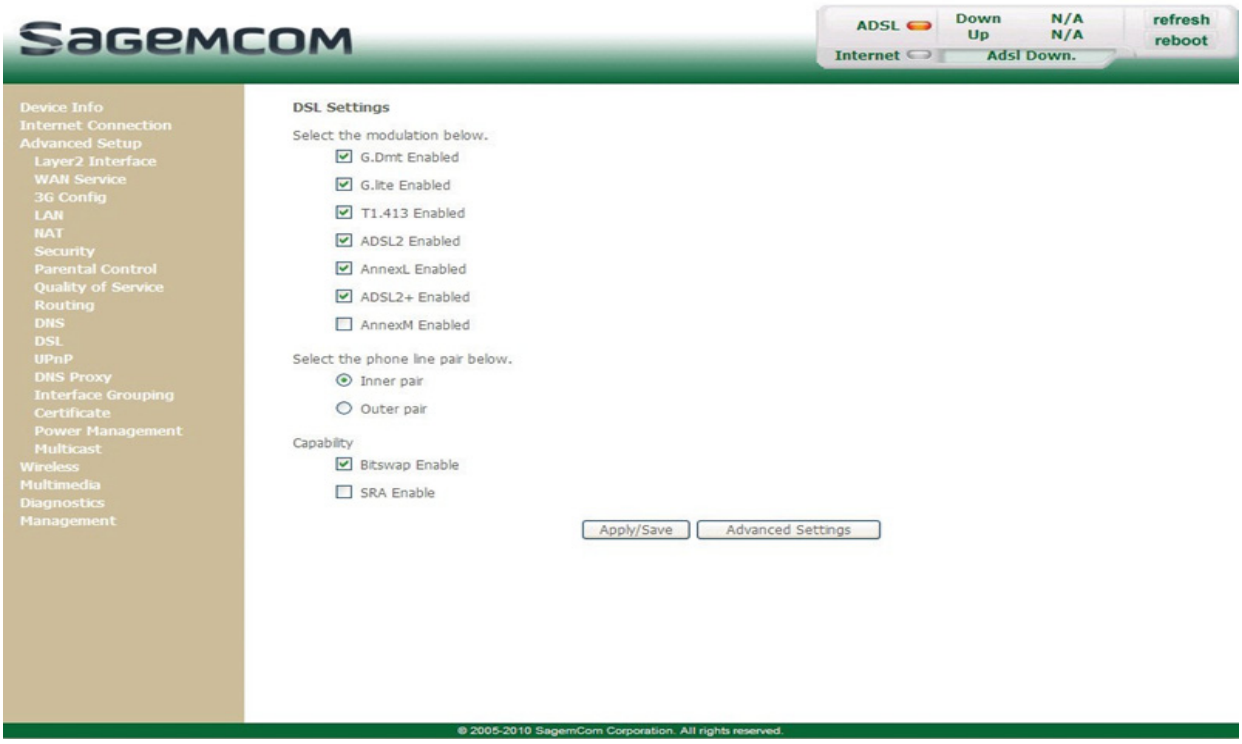
DynDNS Settings

Field	Action
Username	Enter the account name supplied to you by the dynamic DNS provider.
Password	Enter the account password provided to you by the dynamic DNS provider.

5.7.11 DSL

Object: The purpose of this menu is to parameter your ADSL line.

- In the **Advanced Setup** menu, select **DSL**.
  The following screen opens:



Modulation

- Check the boxes according to the characteristics of your line.

Field	Default value
G.Dmt Enabled	Checked
G.lite Enabled	Checked
T1.413 Enabled	Checked
ADSL2 Enabled	Checked
AnnexL Enabled	Checked
ADSL2+ Enabled	Checked
AnnexM Enabled	Not checked

Phone line pair

- Check the boxes according to the characteristics of your line.

Field	Default value
Inner pair	Checked
Outer pair	Not checked

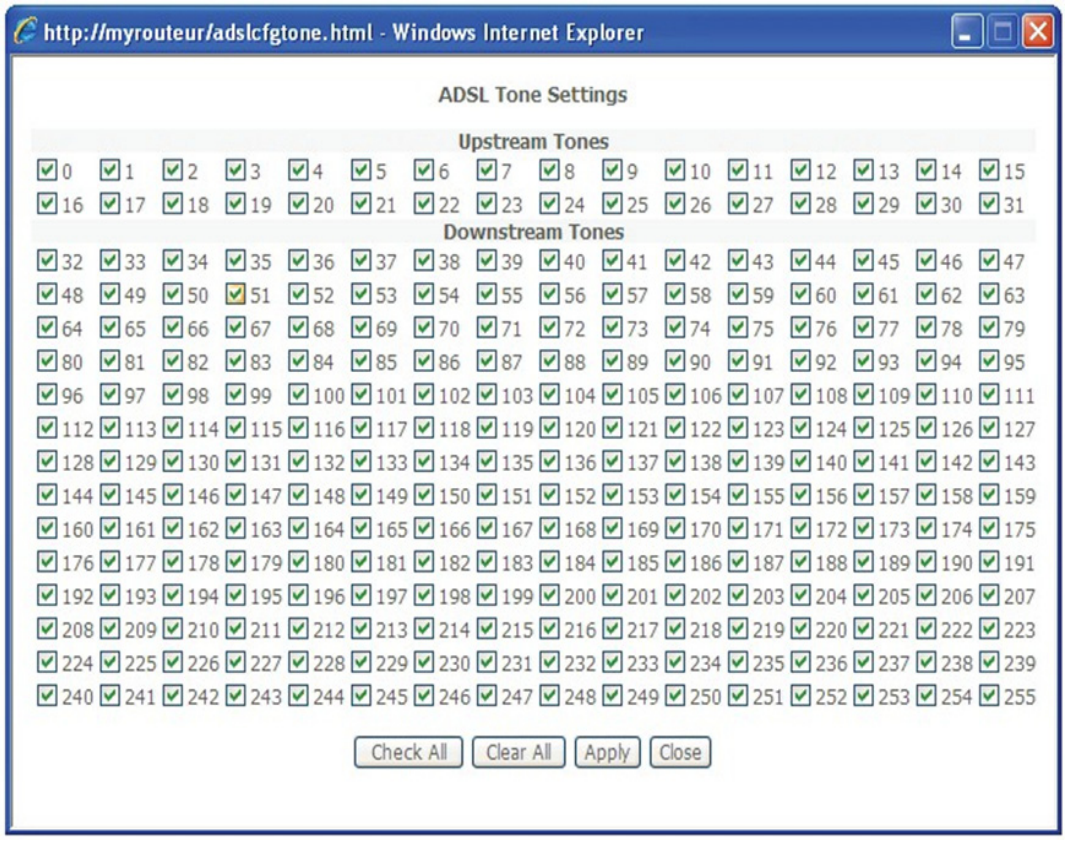
Capability

Field	Default value
Bitswap Enable	Checked
SRA Enable	Not checked

- Click on the **Advanced Settings** button to display the following screen:

Field	Default value
Normal	Checked
Reverb	Not checked
Medley	Not checked
No retrain	Not checked
L3	Not checked

- Click on the **Tone Selection** button to display the following screen:



Note

There are 32 ascending tones and 224 descending tones.

- Click on the **Check All** button to select all the tones or the **Clear All** button to select none of them.

Note

All the tones are selected by default.
To select a tone, simply check the associated box.
To unselect a tone, simply leave its associated box empty.

5.7.12 Upnp

Object: This menu is used to enable or disable the Upnp protocol.
The Upnp function lets you automatically join a network dynamically and obtain an IP address.

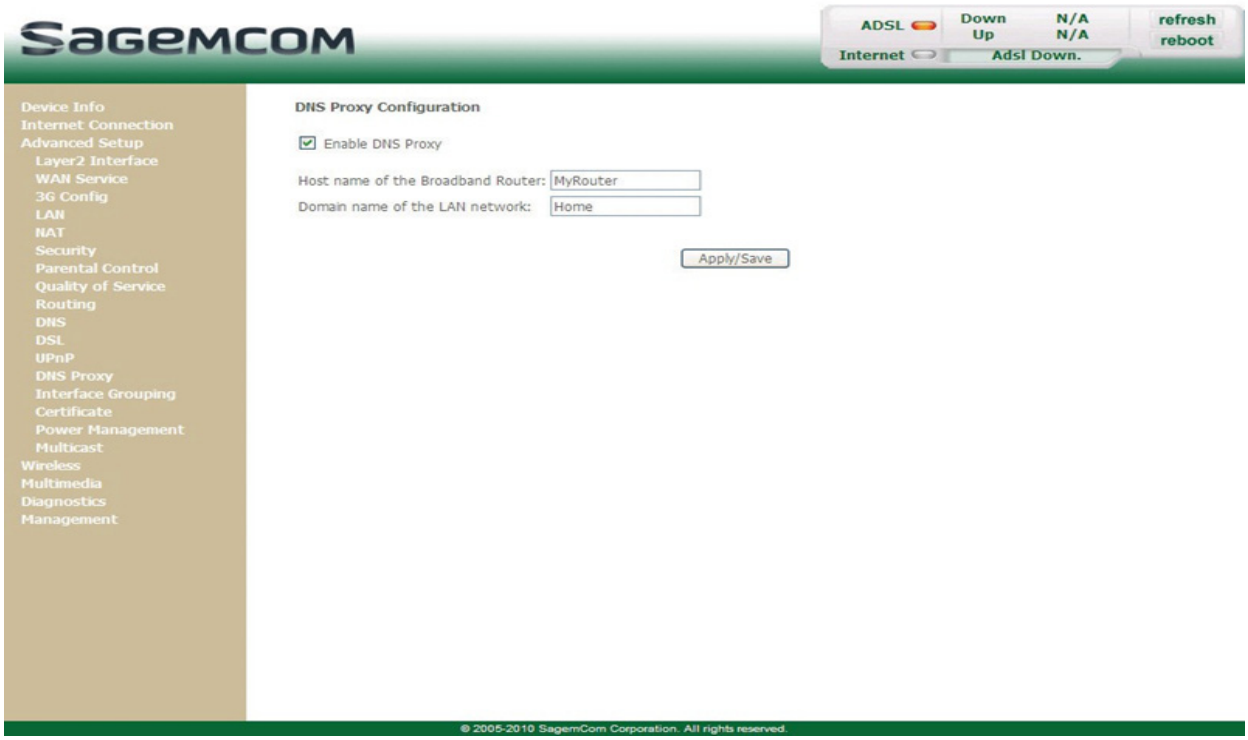
- In the **Advanced Setup** menu, select **Upnp**.
  The following screen opens:

- To enable Upnp protocol, check the box. To disable it, uncheck the box.

5.7.13 DNS Proxy

Object: This menu is used to enable or disable DNS proxy.

- In the **Advanced Setup** menu, select **DNS Proxy**.
  The following screen opens:



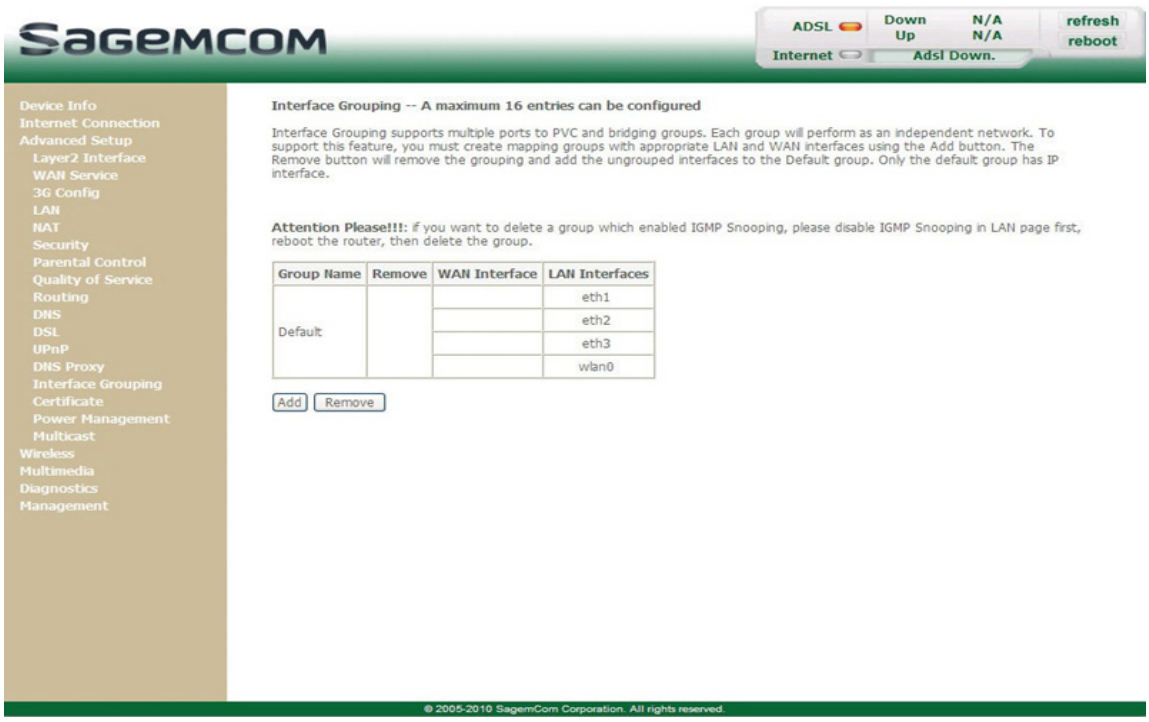
Field	Action	Default value
Enable Dns Proxy	To enable Dns proxy, check the box. To disable it, uncheck the box.	**Checked**
Hostname of the modem	Default hostname of the modem.	**MyRouter**
Domain name of the LAN network	Default domain name of the LAN network.	**Home**

5.7.14 Interface Grouping

Object: This menu is used to host a service (Video, Data, SIP) on an interface (ETH or Wi-Fi) of your router.

- In the **Advanced Setup** menu, select **Interface Grouping**.

  The following screen opens:



Field	Meaning
Group Name	Group name (see Note).
Remove	Check the box and click the [**Remove**] button to remove the group.
WAN Interface	WAN interface used.
LAN Interfaces	Lists all your router's interfaces. **Note:** This list depends on the network configuration.

Note

By default, all the interfaces are dedicated to data and are associated with the first VC (**V**irtual **C**hannel) existing or created.

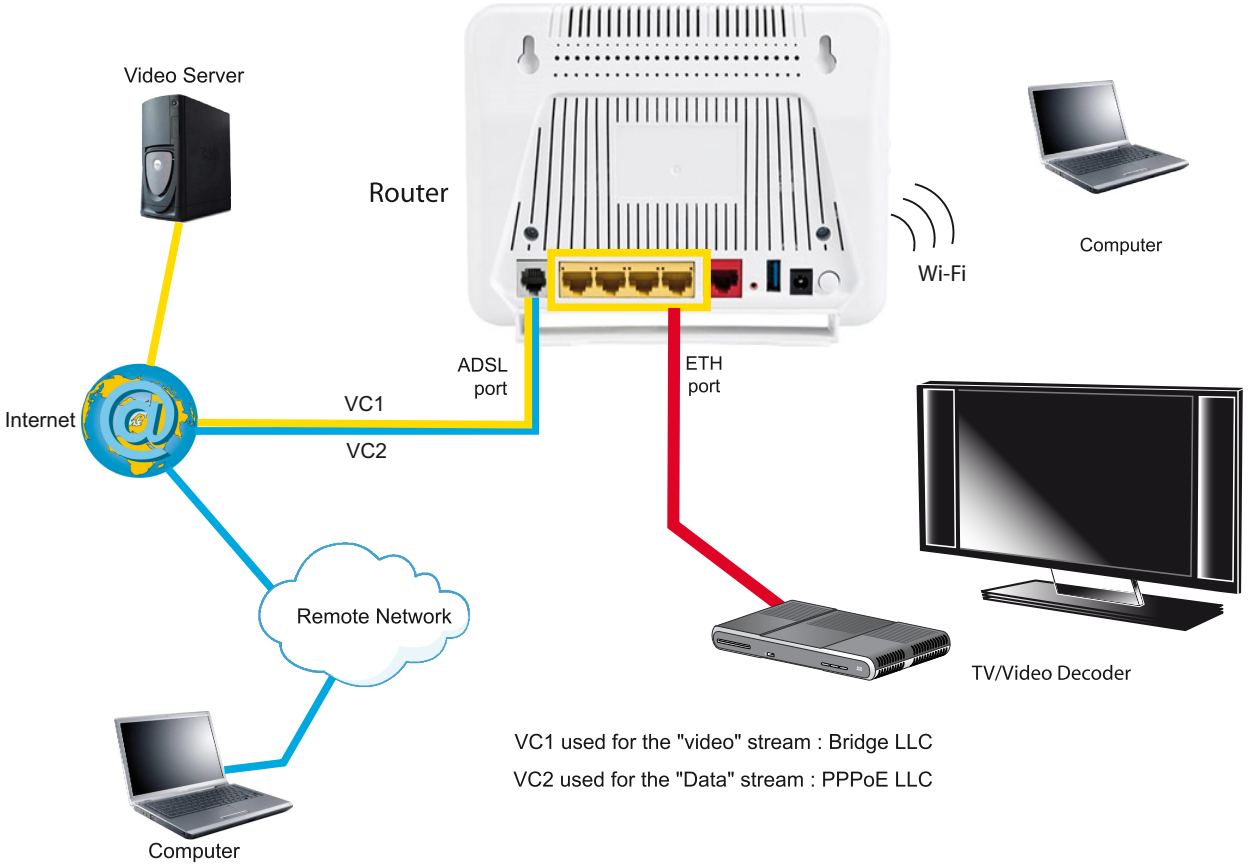
Add

- Click on the **Add** button to display the following screen:

Field	Meaning
Group Name	Enter a name which represents the service you want to associate with a desired interface (for example "video_eth" if you want to associate the TV over UP service with the interface (Ethernet)).
WAN Interface used in the grouping	Select the WAN interface you want to use in the grouping.
Grouped LAN Interfaces	Displays the interfaces associated with a service you selected in the **Available LAN Interfaces** area then transferred with the <- button.
Available LAN Interfaces	Lists all your router's interfaces. **Note:** This list depends on the network configuration.

Button	Action
<-	Transfer the interfaces selected in the **Available LAN Interfaces** area to the **Grouped LAN Interfaces** area.
->	Transfer the interfaces selected in the **Grouped LAN Interfaces** area to the **Available LAN Interfaces** area.

The following diagram illustrates the path of the "Video" and "Data" flows.



5.7.15 Certificate

This menu contains the following sub-menus:

- Local (see subsection 5.7.15.1)
- Trusted CA (see subsection 5.7.15.2)

5.7.15.1 Local

Object: This menu is used to manage your router's identity certificates. These certificates, which are used by TR-69 (in SSL mode), enable the mutual authentication of the CPE and the ACS.

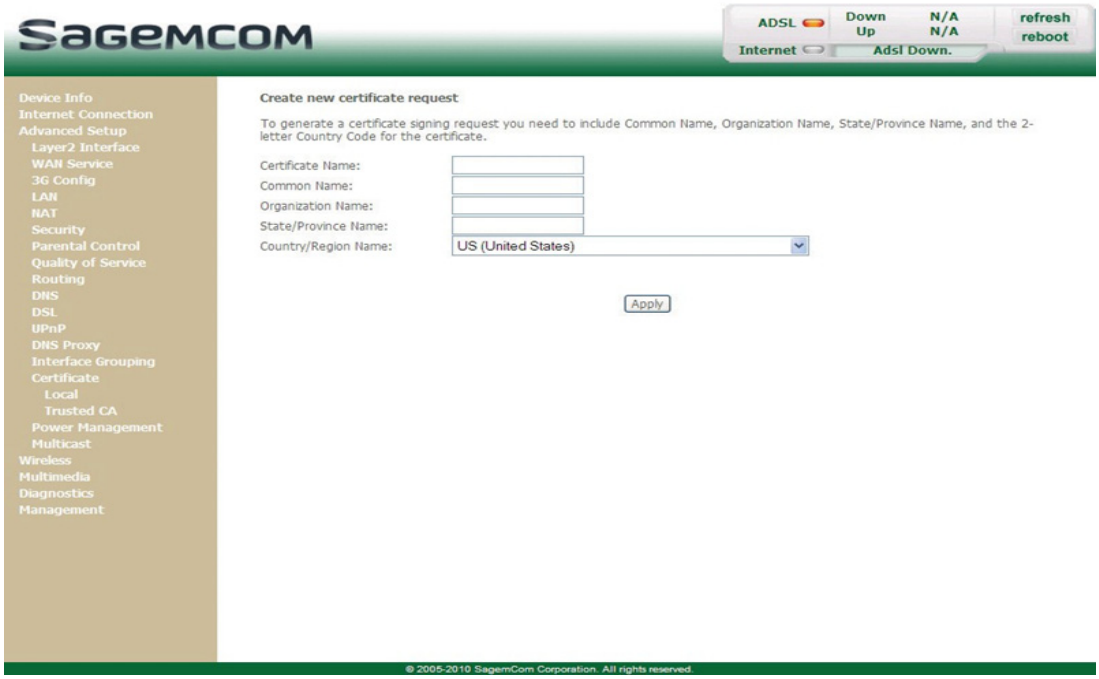
- In the **Advanced Setup** menu, select **Certificate** then **Local**.

  The following screen opens:

Field	Meaning
Name	Name of the certificate.
In Use	Indicates whether the certificate can be used or not.
Subject	Summarises the main characteristics of the certificate.
Type	Indicates the status of the certificate (e.g.: request).
Action	Select the action from the list: view, load signed certificate, remove.

Create Certificate Request

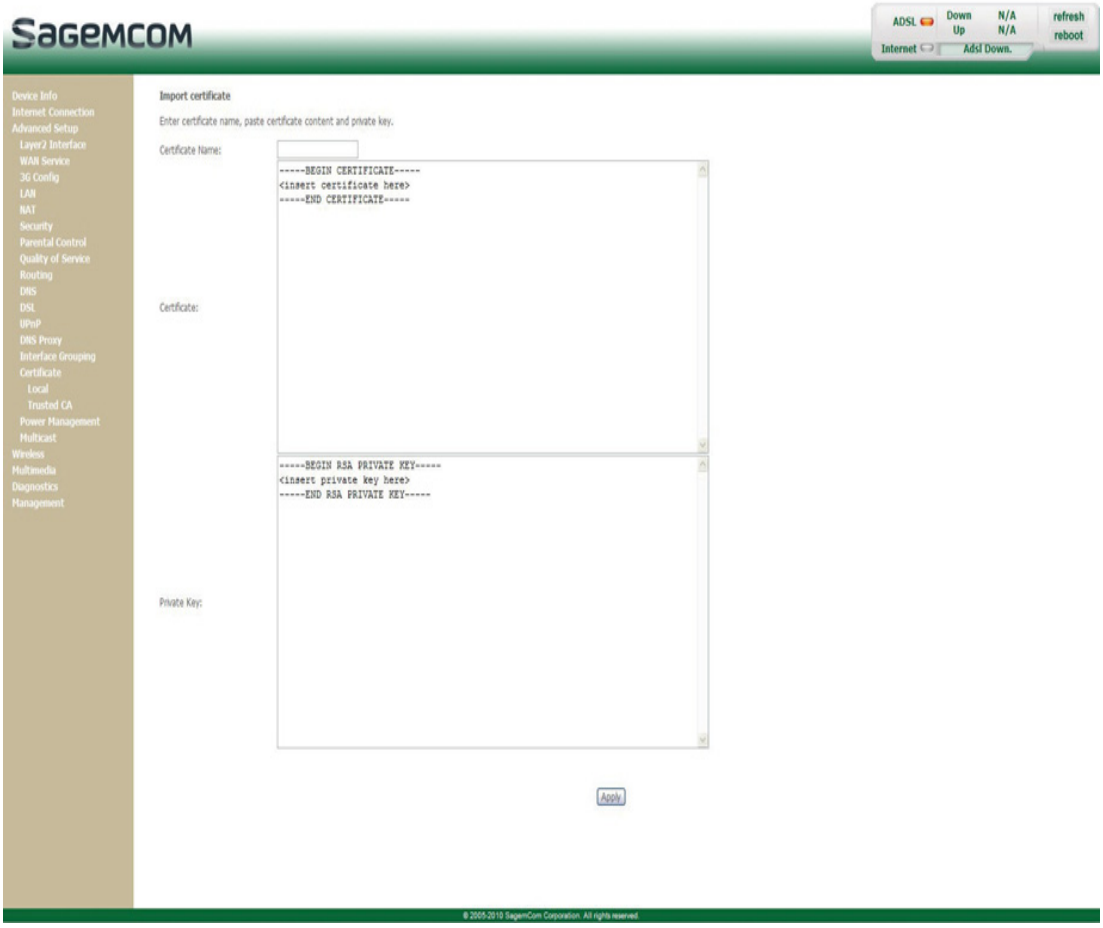
- Click on the **Create Certificate Request** button to display the following screen:



Field	Action
Certificate Name	Enter the name of the certificate.
Common Name	Enter the name of the certificate's owner.
Organization Name	Enter the name of the organisation which owns the certificate.
State/Province Name	Enter the name of the state or province.
Country/Region Name	Select the country from the scroll down list.

Import Certificate

- Click on the **Import Certificate** button to display the following screen:

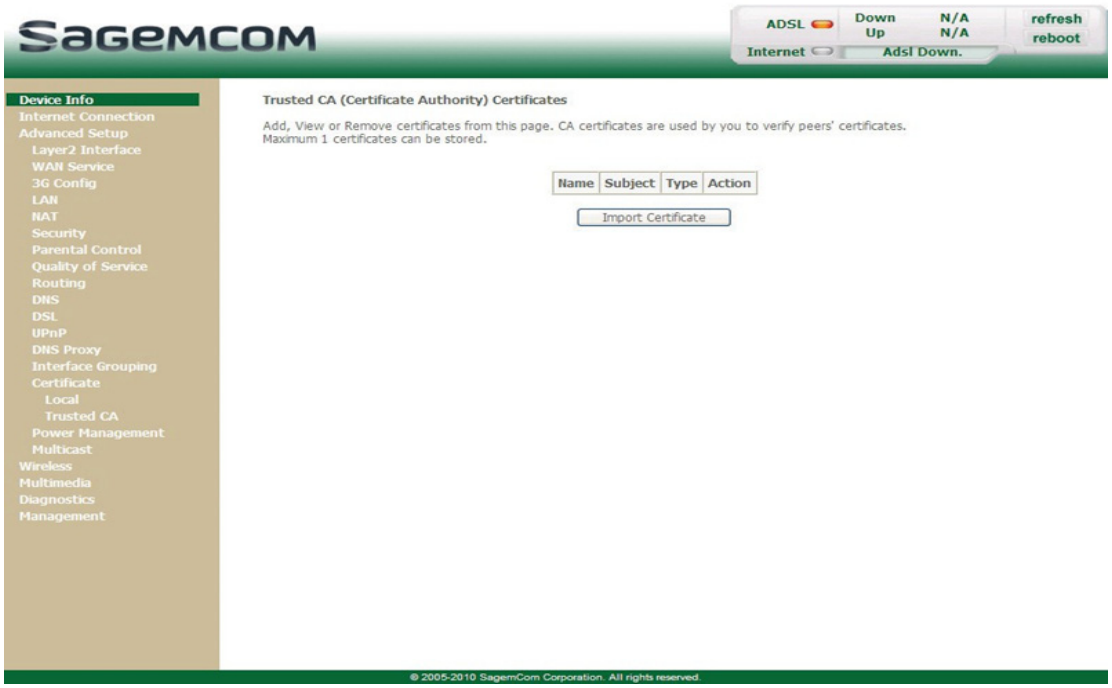


Field	Action
Certificate Name	Enter the name of the certificate.
Certificate	Insert the certificate here.
Private key	Insert the private key here.

5.7.15.2 Trusted CA

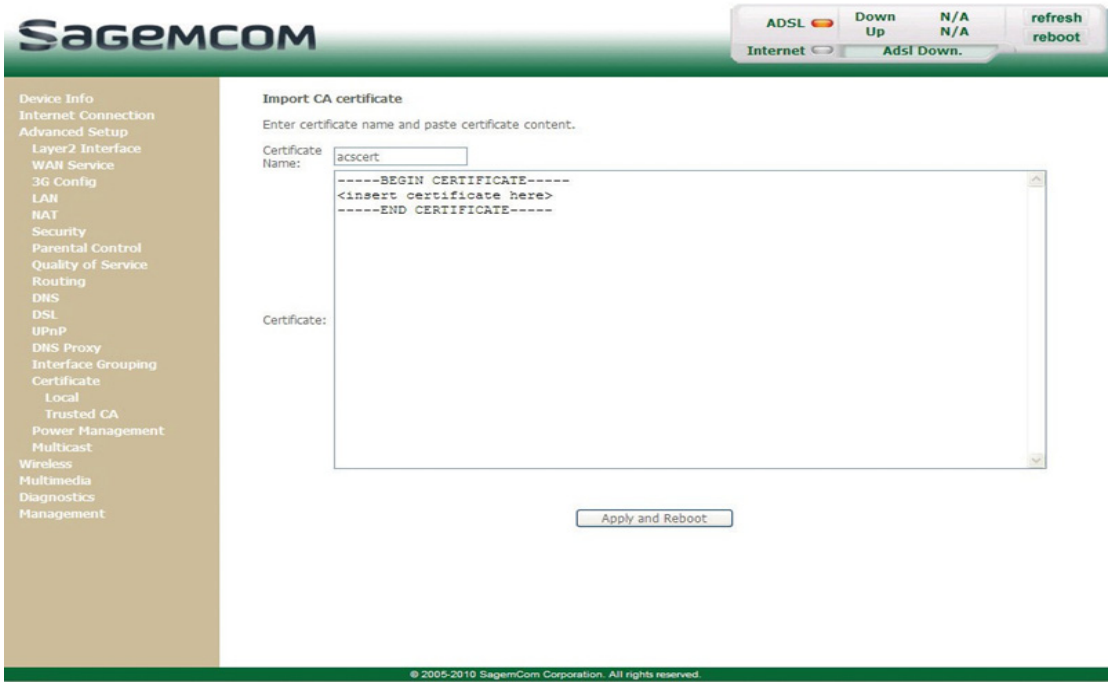
Object: This menu is used to manage the identity certificates of the remote servers. These certificates, which are used by TR-69 (in SSL mode), enable the mutual authentication of the CPE and the ACS.

- In the **Advanced Setup** menu, select **Certificate** then **Trusted CA**.
  The following screen opens:



Import Certificate

- Click on the **Import Certificate** button to display the following screen:



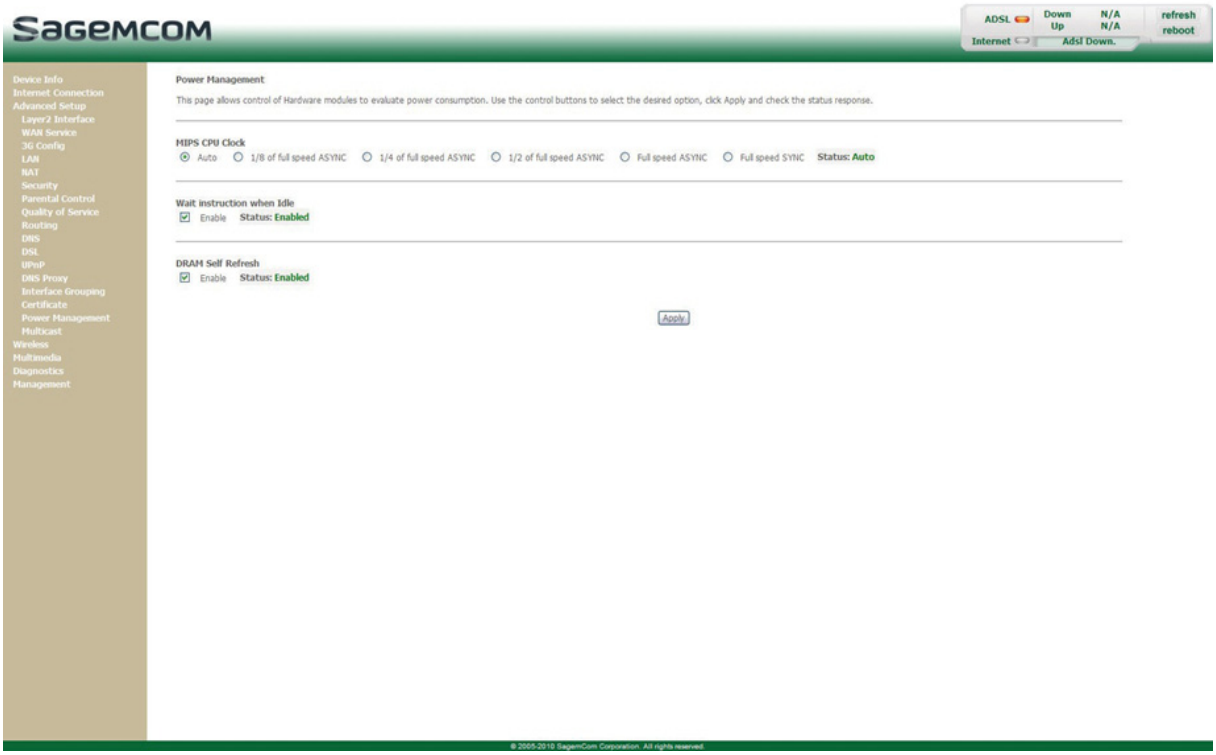
Field	Action
Certificate Name	Enter the name of the certificate.
Certificate	Insert the certificate here.

5.7.16 Power Management

Object: This menu lets you control power consumption selecting the different options.

- In the **Advanced Setup** menu, select **Power Management**.

  The following screen opens:



Field	Action	Default value
MIPS CPU Clock	Check the box to enable the corresponding option: • Auto • 1/8 of full speed ASYNC • 1/4 of full speed ASYNC • 1/2 of full speed ASYNC • Full speed ASYNC • Full speed SYNC	**Auto**
Wait instruction when Idle	Check the box to enable the power management.	**Enabled**
DRAM Self Refresh	Check the box to enable the DRAM Self Refresh.	**Enabled**

5.7.17 Multicast

Object: This menu lets you configure IGMP protocol necessary to use video conferencing and teleconferencing applications for example.

- In the **Advanced Setup** menu, select **Multicast**.

  The following screen opens:

Field	Action	Default value
Default Version	Allows you to set the WAN side version of IGMP protocol version. LAN side always sends IGMPv3 queries. IGMP proxy/snooping module can handle all the backward compatibility issues if it receives any version of IGMP messages. **Note**: By default it starts with IGMP version 3.	**3**
Query Interval	Allows you to set the query interval.	**125**
Query Response Interval	Allows you to set the query response interval.	**10**
Last Member Query Interval	Allows you to set the last member query interval.	**10**
Robustness Value	Allows you to set the robustness value.	**2**
Maximum Multicast Groups	This value sets the maximum number of groups allowed per interface. It can be changed dynamically.	**25**

Field	Action	Default value
Maximum Multicast Data Sources (for IGMPv3 : (1 - 24)	Allows you to set the maximum number of groups sources allowed per multicast group. It can be changed dynamically between values 1 to 24.	**10**
Maximum Multicast Group Members	Allows you to set the maximum number of groups allowed per group. It can be changed dynamically.	**25**
Fast Leave Enable	If this value is enabled, IGMP proxy removes the membership of a group member immediately without sending an IGMP membership query on downstream.	**Checked**

5.8 Wireless

Object: This menu lets you activate a network and also allows you to configure all the basic and advanced parameters of a wireless network.

This section contains the following menus:

- Basic (see subsection 5.8.1)
- Security (see subsection 5.8.2)
- MAC Filter (see subsection 5.8.3)
- Wireless Bridge (see subsection 5.8.4)
- Advanced (see subsection 5.8.5)
- Station Info (see subsection 5.8.6)

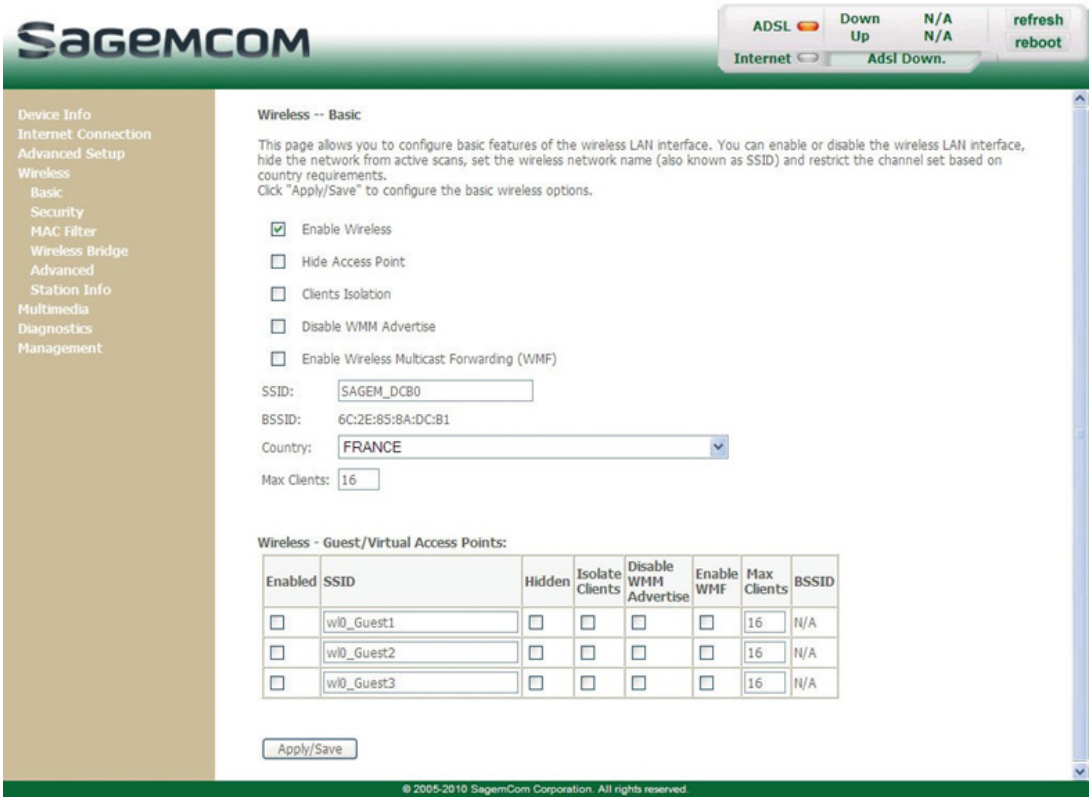
Important

These menus must only be accessed/modified by experienced users.

5.8.1 Basic

- In the **Wireless** menu, select **Basic**.

  The following screen opens:



5.8.1.1 Wireless - Basic

Field	Action/Meaning	Default value
Enable Wireless	Check the box to activate the wireless network (Wi-Fi). **Note:** The steady "**Wi-Fi**" LED on the front of the router shows that the wireless network (Wi-Fi) is activated.	**Checked**
Hide Access Point	Check the box to mask the broadcast of the SSID and prevent any unwanted Wi-Fi user to connect on your router. **Note:** When this box is checked, the router's SSID is absent from the Wi-Fi adaptor user's own list of monitored sites (Access Point).	**Not checked**
Clients isolation	Check the box to select the desired state: • **Disabled**: do not isolate the **A**ccess **P**oint i.e. authorise machines connected to the router to communicate with each other. • **Enabled**: isolate the **A**ccess **P**oint, i.e. prohibit machines connected to the router to communicate with each other.	**Not checked**
Disable WMM Advertise	Check the box to disable Wi-Fi Multimedia feature (Not used here).	**Not checked**
Enable Wireless Multicast Forwarding (WMF)	Check the box to enable multicast frames forwarding over wireless.	**Not checked**
SSID	Enter your router's SSID. **Note:** This is indicated on the label stuck to the box.	**SAGEM_ABCD**
BSSID	This is the MAC address of the router's Wi-Fi interface (Access Point). In the "Structure" mode, this address identifies a cell (BSS in English **B**asic **S**ervice **S**et). This cell is a set formed by the access point and the stations located in its coverage area. **You cannot modify this setting.**	**[Non modifiable]**
Country	Select the country of your choice from the scroll down list.	**FRANCE**
Max Clients	Maximum number of wireless customers for your router.	**16**

Note

The router may or may not be secured, at the request of the customer. This level of security is indicated on the label pasted to the box.
This choice will modify the Wireless configuration screen.

5.8.1.2 Guest/Virtual Access Points

Field	Action/Meaning	Default value
Enabled	Check the box to activate the second wireless network (Wi-Fi).	**Unchecked**
SSID	Enter the SSID of your second wireless network.	**wl0_Guest1**
Hidden	Check the box to mask the broadcast of the SSID and prevent any unwanted Wi-Fi user to connect on your router. **Note:** When this box is checked, the router's SSID is absent from the Wi-Fi adaptor user's own list of monitored sites (Access Point).	**Unchecked**
Isolate Clients	Check the box to select the desired state: • **Disabled**: do not isolate the **A**ccess **P**oint i.e. authorise machines connected to the router to communicate with each other. • **Enabled**: isolate the **A**ccess **P**oint, i.e. prohibit machines connected to the router to communicate with each other.	**Unchecked**
Disable WMM Advertise	Check the box to disable Wi-Fi Multimedia feature.	**Unchecked**
Enable WMF	Check the box to enable multicast frames forwarding over wireless.	**Unchecked**
Max Clients	Enter the maximum number of wireless customers for your router.	**16**
BSSID	This is the MAC address of the router's Wi-Fi interface (Access Point). In the "Structure" mode, this address identifies a cell (BSS for **B**asic **S**ervice **S**et). This cell is a set formed by the access point and the stations located in its coverage area. **You cannot modify this setting.**	**N/A**

5.8.2 Security

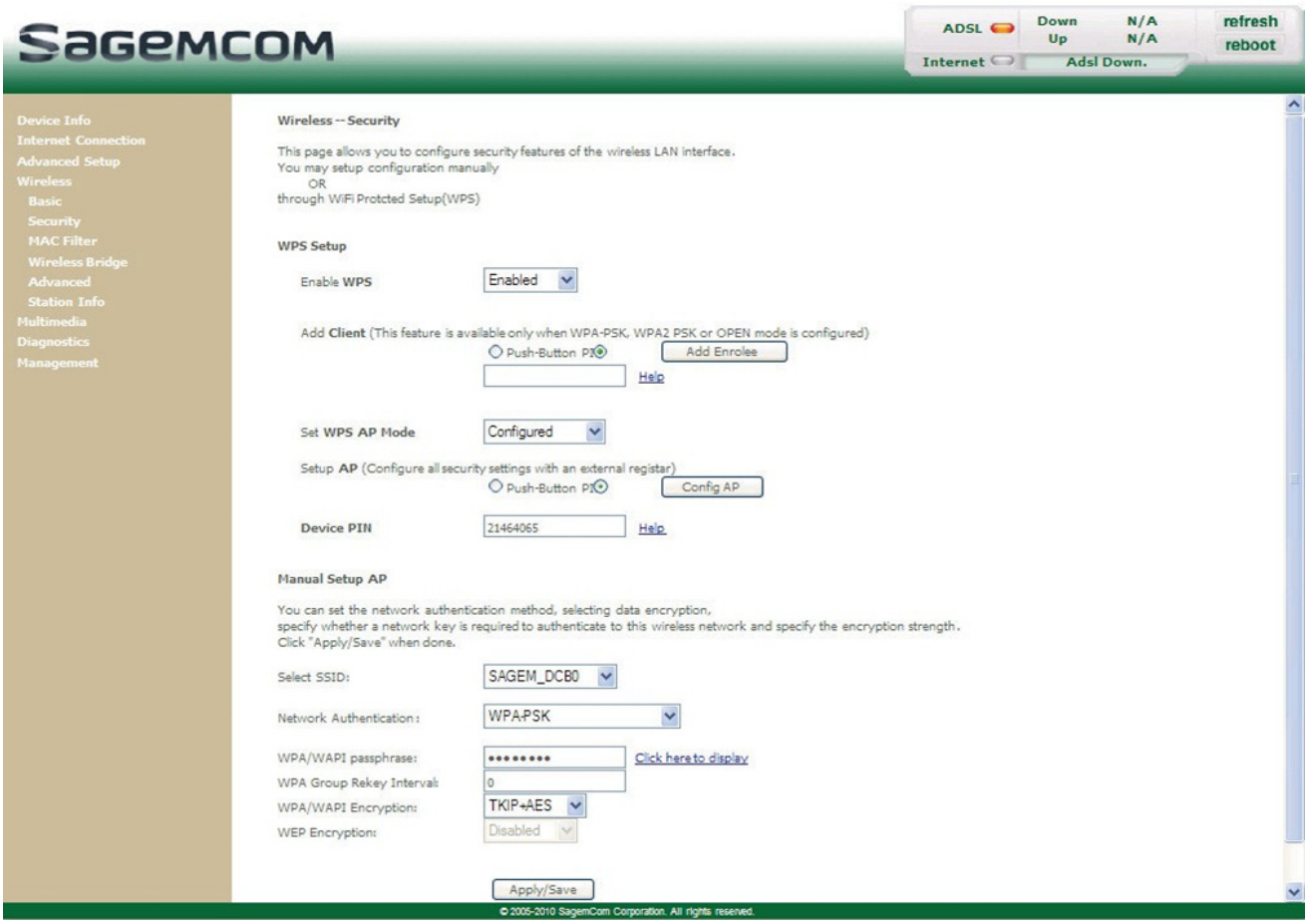
Object: The purpose of this menu is to secure your wireless network (Wi-Fi). All types of ingenious solutions have been deployed to combat attacks from hackers. Encryption modes have been implemented to secure your wireless network. Two of them are commonly used:

- WEP (Wired Equivalent Protocol)
- WPA (Wi-Fi Protected Access) and its derivatives (WPA-PSK, WPA2 etc.).

The WPA encryption mode is the most robust and the best adapted to correctly securing your wireless network.

- In the **Wireless** menu, select **Security**.

The following screen opens:



5.8.2.1 WPS Setup

Field	Action/Meaning	Default value
Enable WPS	Check the box to activate WPS.	**Enabled**
Add Client[a]	Choose the method to bind a client: • Push-Button • PIN	**PIN**
Set Authorized Station MAC	Set authorised MAC clients.	**-**
Set WPS AP Mode	Choose whether you router is already configured or not.	**Configured**
Setup AP	Configure all security settings with an external registar • Push-Button • PIN	**PIN**
Device PIN	CPE PIN number	**-**

a. This feature is available only when WPA-PSK, WPA2 PSK or OPEN mode is configured.

5.8.2.2 Manual Setup AP

Field	Action/Meaning	Default value
Select SSID	Select the "SSID" of your choice from the scroll down list (sagem or Guest).	**SAGEM_ABCD**
Network Authentication	From the scroll down list, select the security adapted to your router's wireless network. This choice will modify the Wireless configuration screen. For more details, a summary table is presented below in section Network Authentication (see subsection 5.8.2.3).	**Open**
WEP Encryption	Select from the scroll down list: • **Disabled** to not use WEP encryption. • **Enabled** to use WE encryption (see subsection WEP).	**Disabled**

5.8.2.3 Network Authentication

Note

The scroll down list in the **Network Authentication** field shows the following possible authentication types:

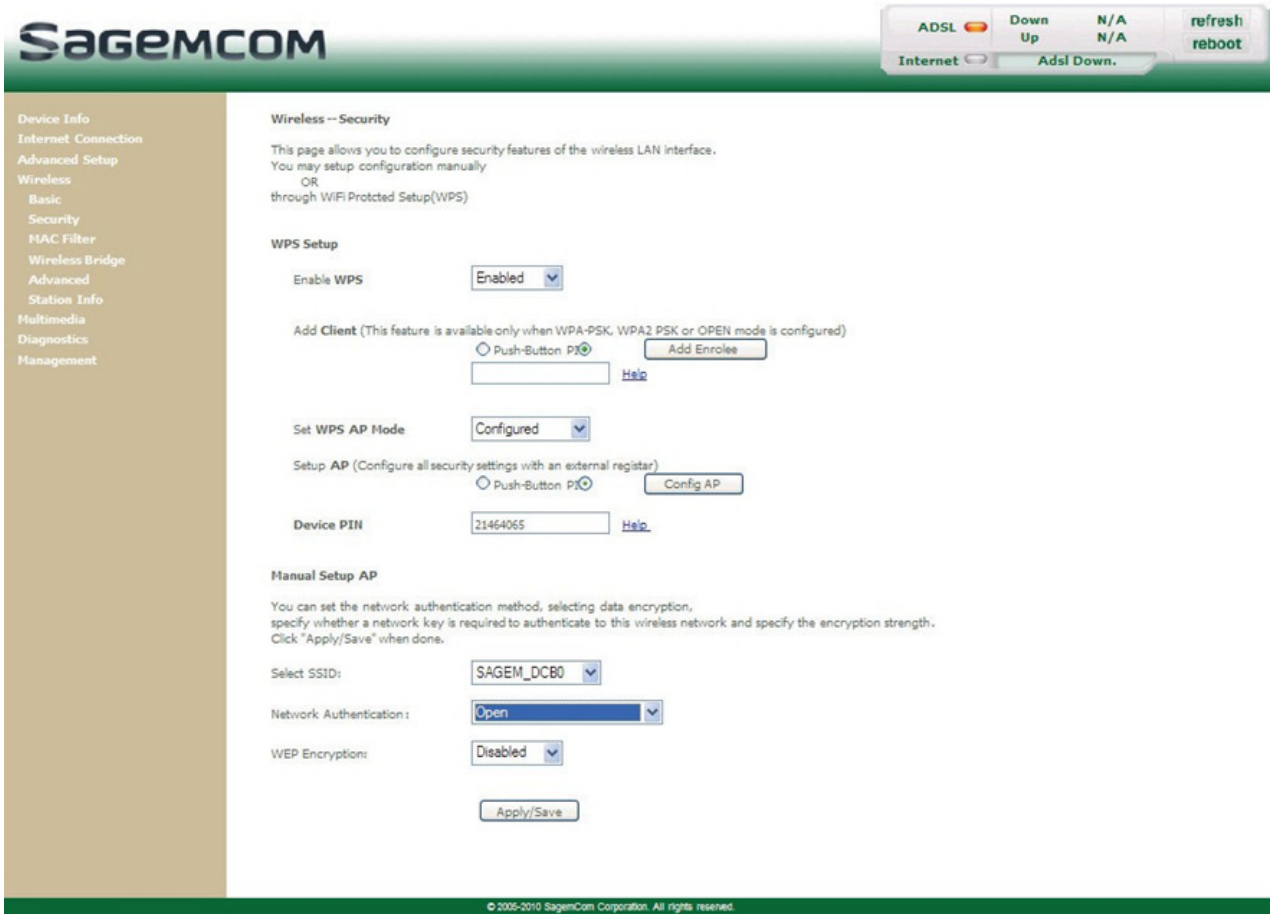
- Open
- Shared
- 802.1x
- WPA
- WPA-PSK
- WPA2
- WPA2-PSK
- Mixed WPA2/WPA
- Mixed WPA2/WPA-PSK

A different screen appears for each authentication type.

Open

Object: The **Open System** authentication enables all users of the Wi-Fi network to authenticate themselves with the router. No restrictions concerning security are demanded.

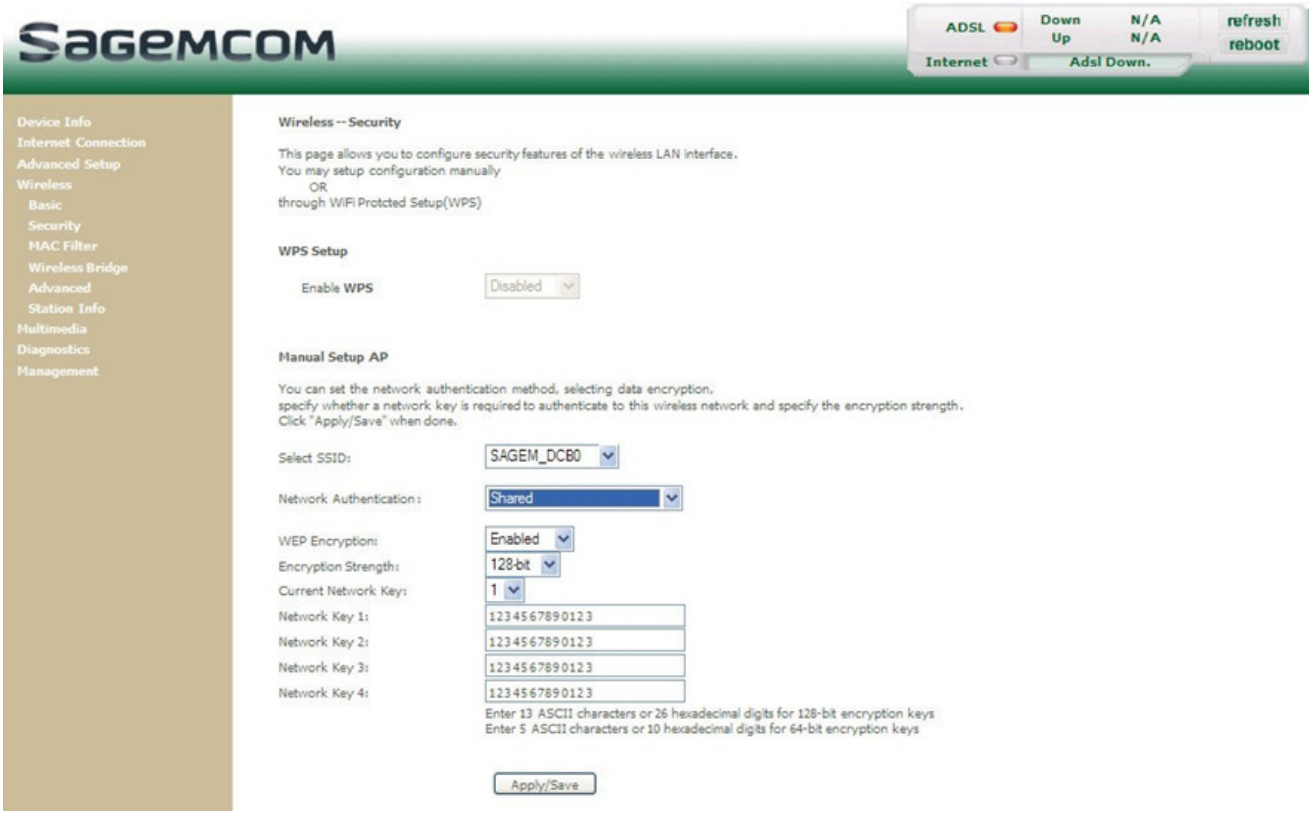
In this authentication mode, only the WEP key may be used to encrypt data.



Shared

Object: This level of security enables users of the Wi-Fi network to be authenticated using their SSID or their WEP key.
In this authentication mode, the WEP key is used to encrypt data.

- Select the **Shared** security from the scroll down list; the following screen appears:



Field	Action/Meaning	Default value
WEP Encryption	**This field is always active (Enabled).**	**Enabled**
Encryption strength	Select **64-bit** or **128-bit** for an encryption at 64 bits or 128 bits respectively.	**128-bit**
Current network key	Select a key from the four suggested. The emission key is used to encrypt the data sent by your computer.	**1**
Network Key x (1 to 4)	The WEP key is customised for your router. You may modify the keys by entering them directly into the boxes. The characters are "0" to "9" and "A" to "F".	**1234567890123**

Important

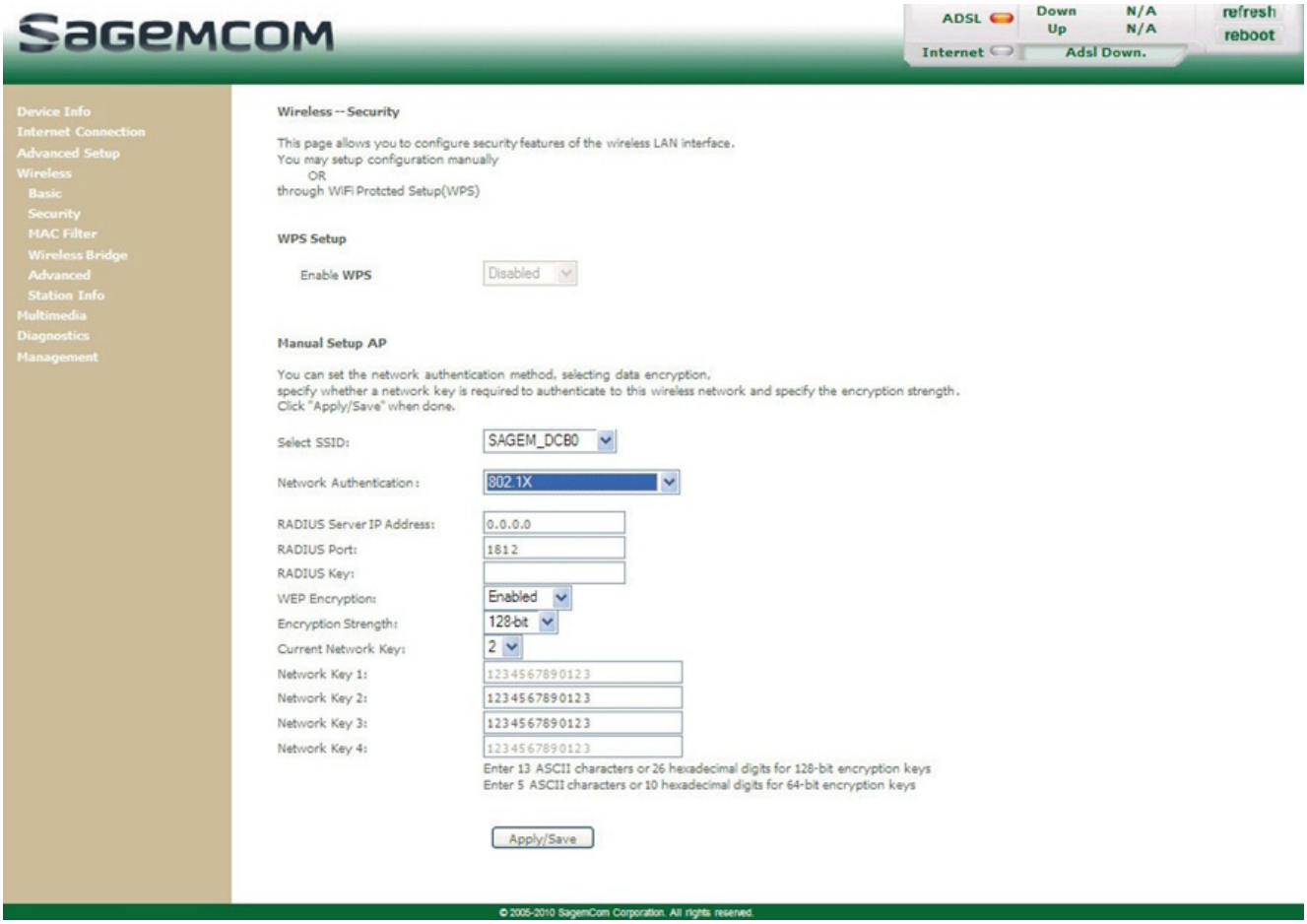
Store the key phrase and the keys in a safe location.
Do not write them in a file on your computer.
The "Key phrase" can consist of up to 15 alphanumeric characters.
To manually configure the encryption key, enter five hexadecimal pairs of digits for each 64-bit key, or enter 13 pairs for the single 128-bit key (A hexadecimal digit is a number or letter in the range 0-9 or A-F). Note that the WEP key protects data transmitted between wireless nodes, but does not protect any transmissions over your wired network (LAN) or over Internet (WAN) using Internet Explorer 5.0 or above.

802.1x

Object: The "802.1x" standard is based on the EAP protocol (**E**xtensible **A**uthentication **P**rotocol). This enables users of the Wi-Fi network to be authenticated using a "RADIUS" authentication server (**R**emote **A**uthentication **D**ial-**i**n **U**ser **S**ervice).

In this case, the WEP key is used exclusively for data encryption.

- Select the security according to the **802.1x** protocol from the scroll down list; the following screen appears:



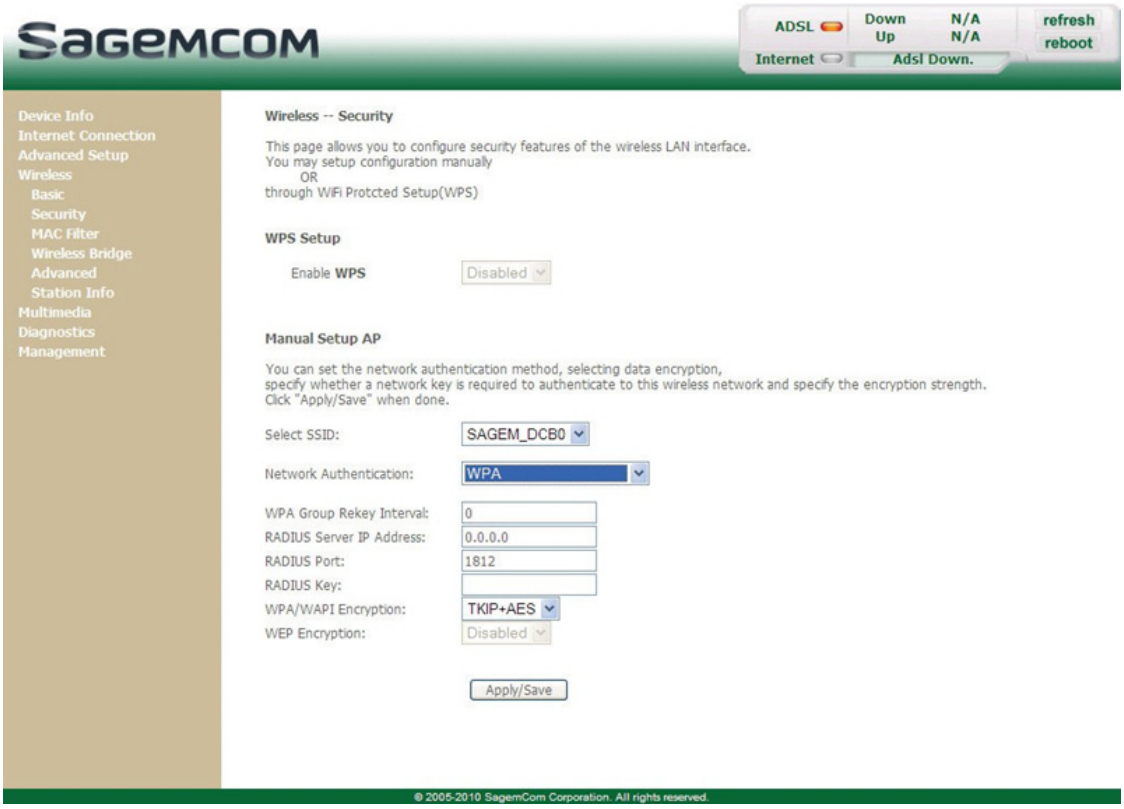
Field	Action/Meaning	Default value
RADIUS Server IP Address	Enter the IP address of the "RADIUS" authentication server.	**0.0.0.0**
RADIUS Port	Enter the port used for the "RADIUS" authentication server.	**1812**
RADIUS Key	Enter the secret key shared between the authentication server and its clients	**-**
WEP Encryption	This field is always active (Enabled).	**Enabled**
Encryption Strength	Select 64-bit or 128-bit for an encryption at 64 bits or 128 bits respectively.	**128-bit**
Current Network Key	Select key 2 or 3.	**2**

Field	Action/Meaning		Default value
Network Key x (1 to 4)	1	This field is empty or displays the key value entered earlier (greyed out)	**[Not modifiable]**
	2	Enter the encryption on the key you selected in the "Current Key".	**1234567890123**
	3	Enter the encryption on the key you selected in the "Current Key".	**1234567890123**
	4	This field is empty or displays the key value entered earlier (greyed out).	**[Not modifiable]**

WPA

Object: This encryption mode applies the functionalities of the WPA protocol and requires the use of a "RADIUS" authentication server.

- Select the **WPA** security from the scroll down list; the following screen appears:



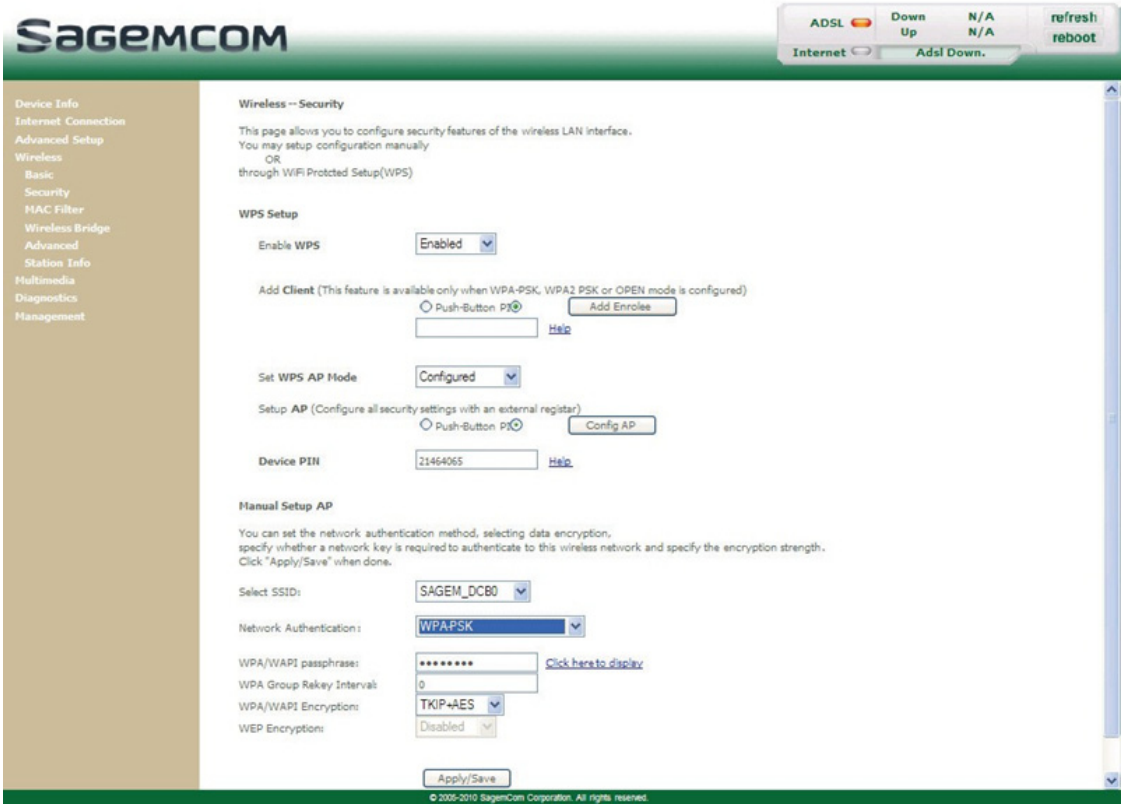
Field	Action/Meaning	Default value
WPA Group Rekey Interval	Enter a value (in seconds) which determines the period after which the WPA key will be regenerated (Renewing) in broadcast / multicast (LAN broadcast).	**0**
RADIUS Server IP Address	Enter the IP address of the "RADIUS" authentication server.	**0.0.0.0**
RADIUS Port	Enter the port used for the "RADIUS" authentication server.	**1812**
RADIUS Key	Enter the secret key shared between the authentication server and its clients	**-**

Field	Action/Meaning	Default value
WPA/WAPI Encryption	Select the WPA encryption required from the scroll down list: • TKIP (**T**emporal **K**ey **I**ntegration **P**rotocol) • AES (**A**dvanced **E**ncryption **S**tandard) • TKIP + AES	**TKIP**
WEP Encryption	Select from the scroll down list: • **Disabled** to use WPA encryption only. • **Enabled** to use both WPA and WEP encryption.	**Disabled**

WPA-PSK

Object: This encryption mode applies the functionalities of the WPA protocol with a pre-shared key, but does not require an authentication server. The key is regenerated after a period which can be configured (**WPA Group Rekey Interval**).

- Select the **WPA-PSK** security from the scroll down list; the following screen appears:



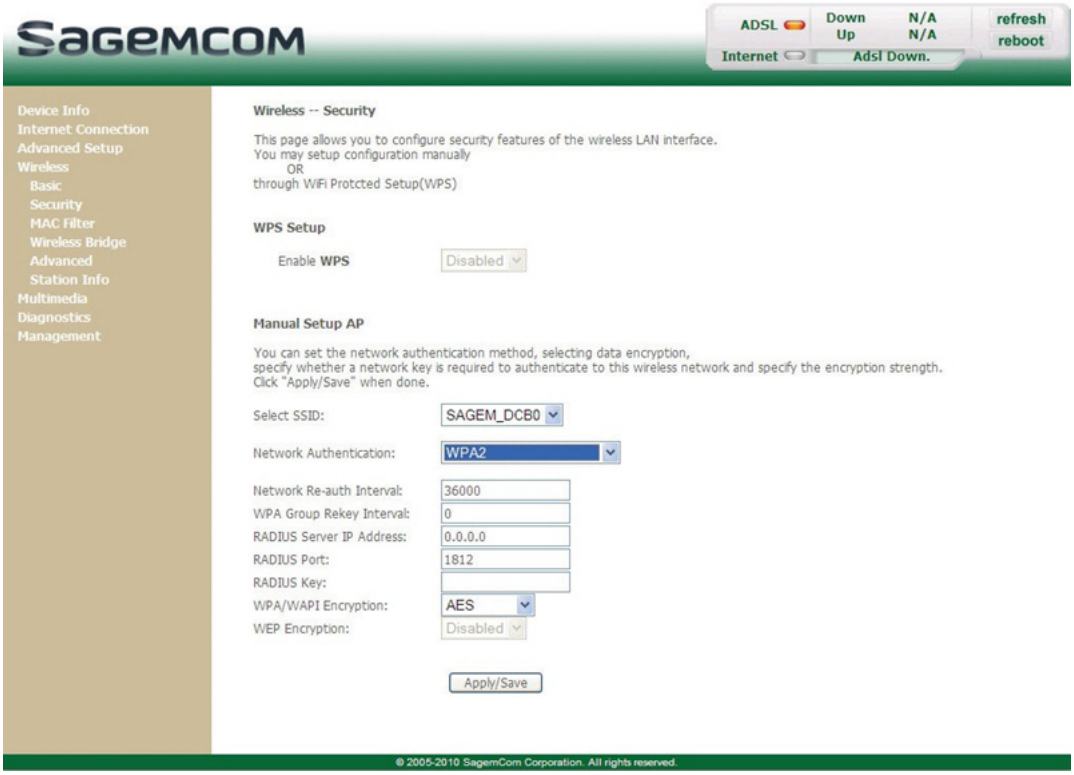
Field	Action/Meaning	Default value
WPA/WAPI passphrase	Enter the secret shared key. This may contain 8 to 63 ASCII characters or 64 hexadecimal symbols (256 bits). Click on the **Apply/Save** button to validate the entry. **Note:** You may display your secret phrase by clicking on **Click here to display**.	**ABCDEF23**
WPA Group Rekey Interval	Enter a value (in seconds) which determines the period after which the WPA key will be regenerated (Renewing) in broadcast / multicast (LAN broadcast).	**0**

Field	Action/Meaning	Default value
WPA/WAPI Encryption	Select the WPA encryption required from the scroll down list: • TKIP (**T**emporal **K**ey **I**ntegration **P**rotocol) • AES (**A**dvanced **E**ncryption **S**tandard) • TKIP + AES	**TKIP**
WEP Encryption	Select from the scroll down list: • **Disabled** to use WPA encryption only. • **Enabled** to use both WPA and WEP encryption.	**Disabled**

WPA2

Object: This encryption mode applies the functionalities of the WPA2 protocol and requires the use of a "RADIUS" authentication server.

- Select the **WPA2** security from the scroll down list; the following screen appears:



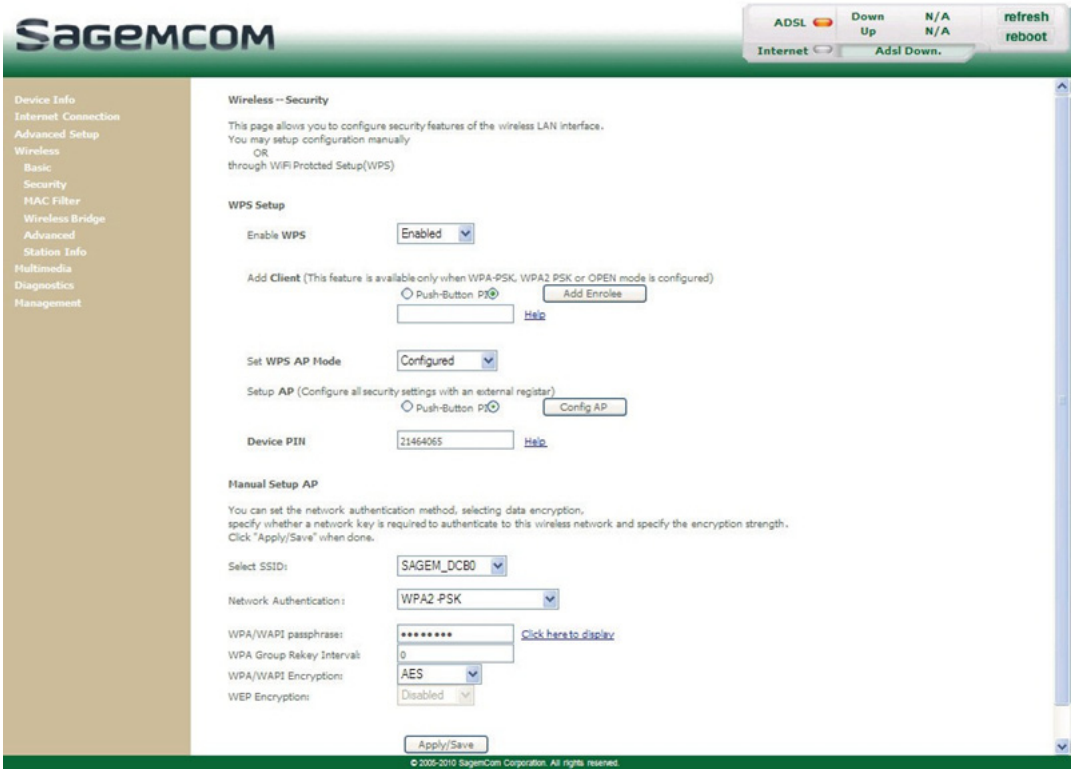
Field	Action/Meaning	Default value
Re-auth Interval	Enter a value (in seconds) which determines the period after which the WPA key will be certified.	**36000**
WPA Group Rekey Interval	Enter a value (in seconds) which determines the period after which the WPA key will be regenerated (Renewing) in broadcast / multicast (LAN broadcast).	**0**
RADIUS Server IP Address	Enter the IP address of the "RADIUS" authentication server.	**0.0.0.0**
RADIUS Port	Enter the port used by the "RADIUS" authentication server.	**1812**

Field	Action/Meaning	Default value
RADIUS Key	Enter the secret key shared between the authentication server and its clients.	-
WPA/WAPI Encryption	Select the WPA encryption required from the scroll down list: • TKIP (**T**emporal **K**ey **I**ntegration **P**rotocol) • AES (**A**dvanced **E**ncryption **S**tandard) • TKIP + AES	**AES**
WEP Encryption	Select from the scroll down list: • **Disabled** to use WPA encryption only. • **Enabled** to use both WPA and WEP encryption.	**Disabled**

WPA2-PSK

Object: This encryption mode uses the WPA2 protocol with a pre-shared key, but does not require an authentication server. The key is regenerated after a period which can be configured (**WPA Group Rekey Interval**).

- Select the **WPA2-PSK** security from the scroll down list; the following screen appears:



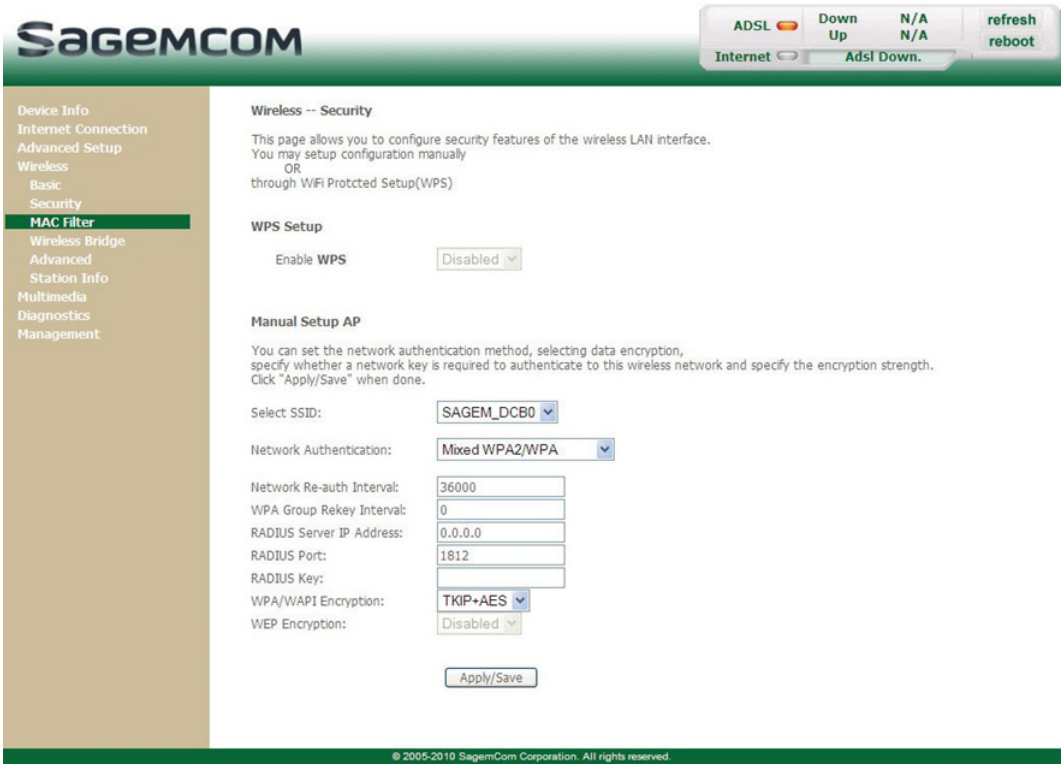
•

Field	Action/Meaning	Default value
WAP/WAPI passphrase	Enter a secret phrase. This may contain 8 to 63 ASCII characters or 64 hexadecimal symbols (256 bits). Click on the **Apply/Save** button to validate the entry. **Note:** You may display your secret phrase by clicking on **Click here to display**.	**ABCDEF23**
WPA Group Rekey Interval	Enter a value (in seconds) which determines the period after which the WPA key will be regenerated (Renewing) in broadcast / multicast (LAN broadcast).	**0**
WPA/WAPI Encryption	Select the WPA encryption required from the scroll down list: • TKIP (**T**emporal **K**ey **I**ntegration **P**rotocol) • AES (**A**dvanced **E**ncryption **S**tandard) • TKIP + AES	**AES**
WEP Encryption	Select from the scroll down list: • **Disabled** to use WPA encryption only. • **Enabled** to use both WPA and WEP encryption.	**Disabled**

Mixed WPA2/WPA

Object: This encryption mode applies the functionalities of the WPA2 and WPA protocols. It needs a "RADIUS" authentication server.

• Select the **Mixed WPA2/WPA** security from the scroll down list; the following screen appears:

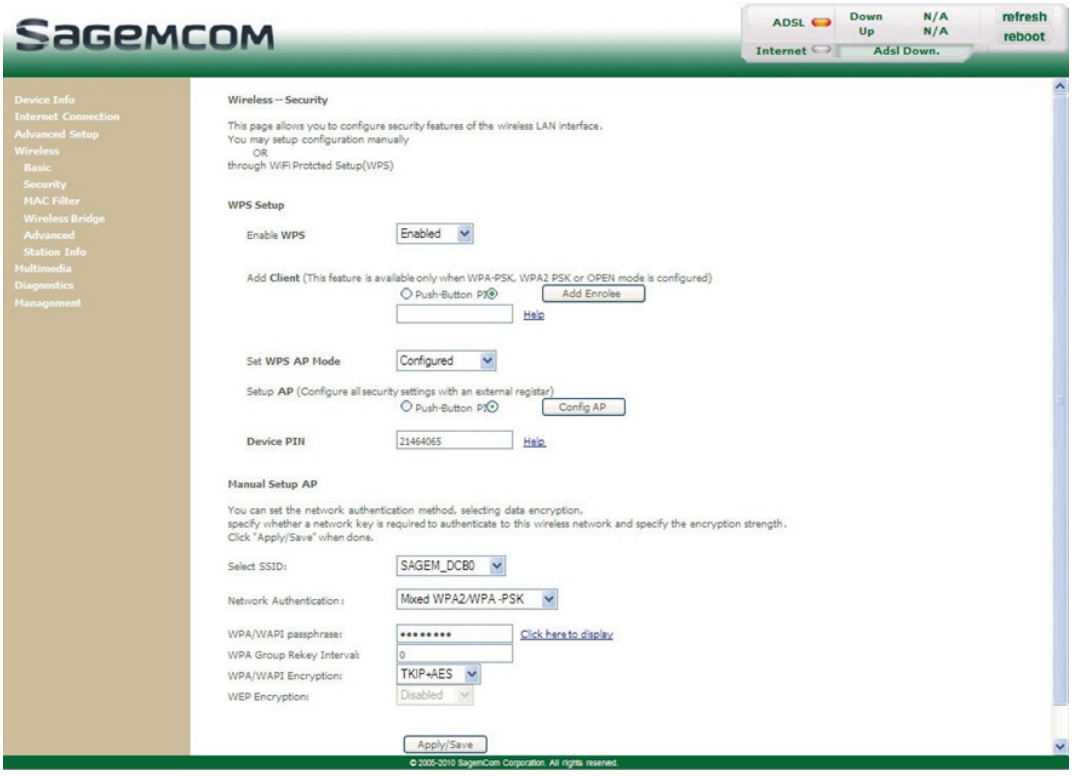


Field	Action/Meaning	Default value
Network Re-auth Interval	Enter a value (in seconds) which determines the period after which the WPA key will be certified.	**36000**
WPA Group Rekey Interval	Enter a value (in seconds) which determines the period after which the WPA key will be regenerated (Renewing) in broadcast / multicast (LAN broadcast).	**0**
RADIUS Server IP Address	Enter the IP address of the "RADIUS" authentication server.	**0.0.0.0**
RADIUS Port	Enter the port used by the "RADIUS" authentication server.	**1812**
RADIUS Key	Enter the secret key shared between the authentication server and its clients.	**-**
WPA/WAPI Encryption	Select the WPA encryption required from the scroll down list: • TKIP (**T**emporal **K**ey **I**ntegration **P**rotocol) • AES (**A**dvanced **E**ncryption **S**tandard) • TKIP + AES	**TKIP + AES**
WEP Encryption	Select from the scroll down list: • **Disabled** to use WPA encryption only. • **Enabled** to use both WPA and WEP encryption.	**Disabled**

Mixed WPA2/WPA-PSK

Object: This encryption mode applies the functionalities of the WPA2-PSK and WPA-PSK protocols. It does not need a "RADIUS" authentication server.

- Select the **Mixed WPA2 /WPA-PSK** security from the scroll down list; the following screen appears:



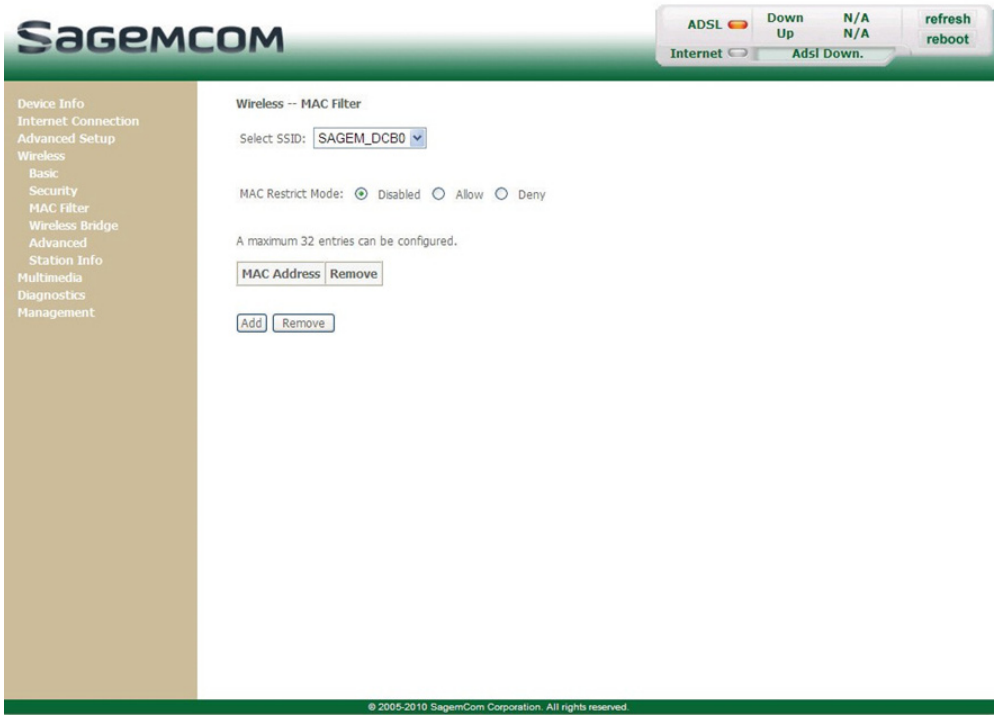
Field	Action/Meaning	Default value
WPA/WAPI passphrase	Enter a secret phrase. This may contain 8 to 63 ASCII characters or 64 hexadecimal symbols (256 bits). Click on the **Apply/Save** button to validate the entry. **Note:** You may display your secret phrase by clicking on **Click here to display**.	**ABCDEF23**
WPA Group Rekey Interval	Enter a value (in seconds) which determines the period after which the WPA key will be regenerated (Renewing) in broadcast / multicast (LAN broadcast).	**0**
WPA/WAPI Encryption	Select the WPA encryption required from the scroll down list: • TKIP (**T**emporal **K**ey **I**ntegration **P**rotocol) • AES (**A**dvanced **E**ncryption **S**tandard) • TKIP + AES	**TKIP + AES**
WEP Encryption	Select from the scroll down list: • **Disabled** to use WPA encryption only. • **Enabled** to use both WPA and WEP encryption.	**Disabled**

5.8.3 MAC Filter

Object: The "MAC Filter" function is used to restrict the access to the wireless network.

- In the **Wireless** menu, select **MAC Filter**.

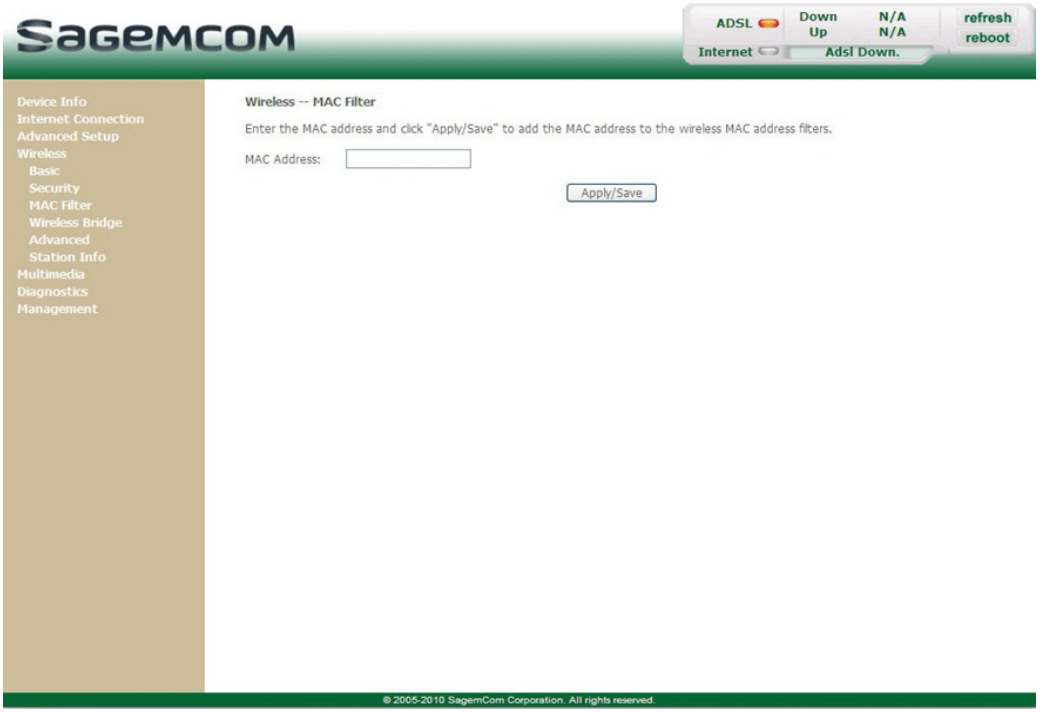
  The following screen opens:



Field	Action/Meaning	Default value
MAC Restrict Mode	Select the command by checking the appropriate box: • **Disabled**: Deactivates the MAC filtering • **Allow**: Enables only computers whose MAC address is in the list to use your wireless network • **Deny**: Refuses computers whose MAC address is in the list to use your wireless network.	**Disabled**

Add

- Click on the **Add** button to add a MAC address to be filtered (address of a computer - authorised or non authorized, according the deny or allow list - to connect to a wireless network).



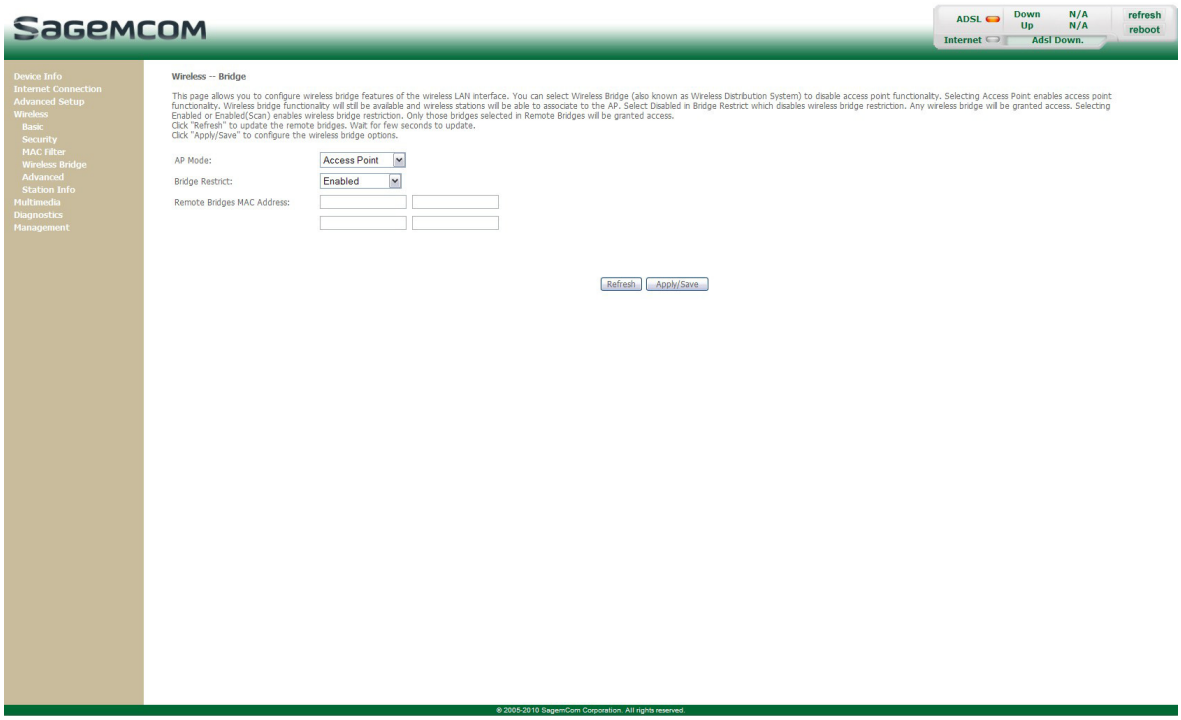
Note

The MAC address can be added automatically at the time of the Wi-Fi installation, by a short push on button "WLAN/WPS".
After approximately 5 minutes, the new address fits in the list and the router passes in mode of filtering (MAC Restrict Mode) "Allow" to authorize only the computers whose MAC address appears in the list to be connected to your router.

5.8.4 Wireless Bridge

Object: This menu is used to configure wireless bridge features of the wireless LAN interface

- In the **Wireless** menu, select **Wireless Bridge**.
  The following screen opens:



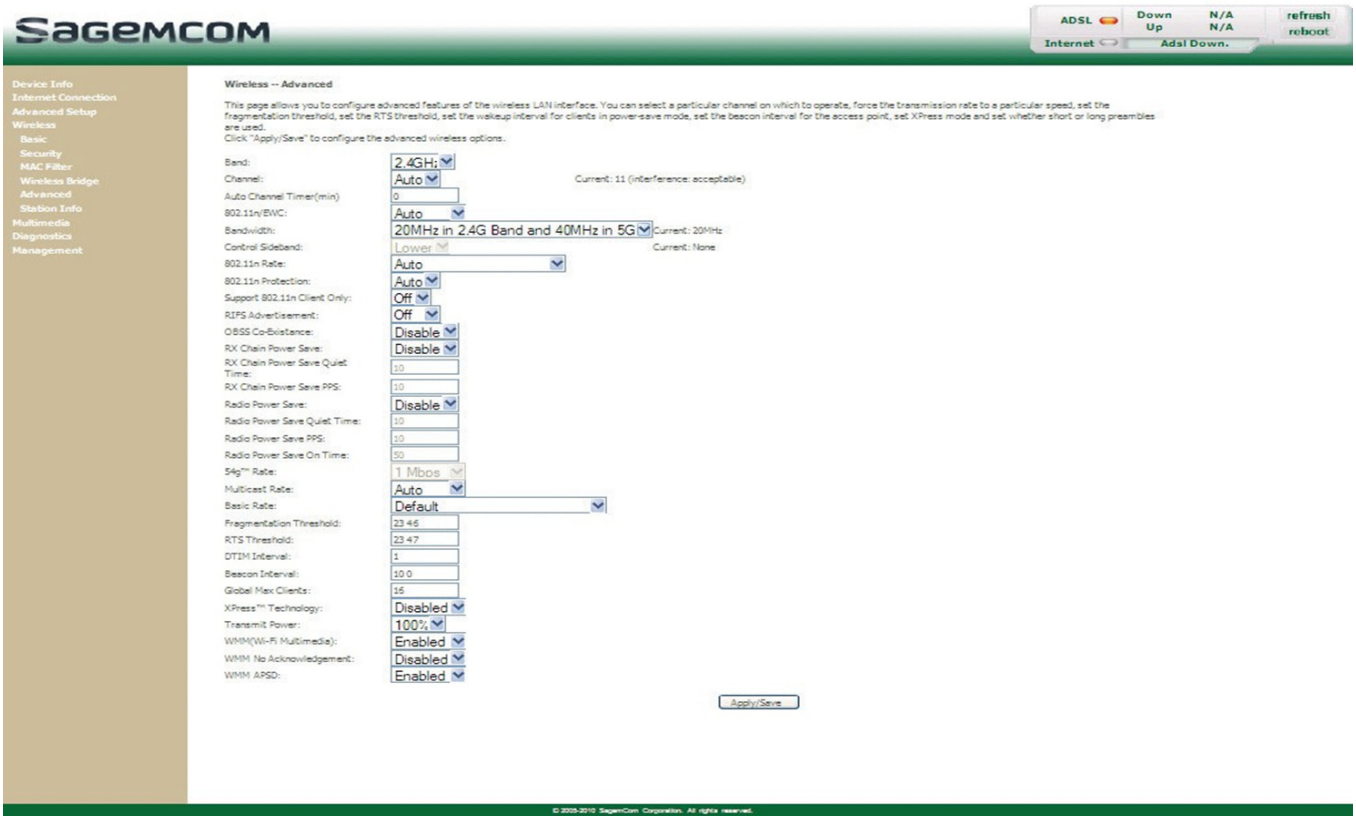
Field	Action/Meaning	Default value
AP Mode	Select: • **Wireless Bridge** to set the CPE as a bridge in your WDS network, • **Access Point** enables access point functionality.	**Access Point**
Bridge Restrict	Select one of the following options: • **Disabled** to disable wireless bridge restriction. **Note:** Any wireless bridge will be granted access. • **Enabled** or **Enabled(Scan)** to enable wireless bridge restriction.	**Enabled**
Remote Bridges MAC Address	Enter the bridges MAC addresses which must be granted access.	-

5.8.5 Advanced

Object: This menu is used to configure the essential parameters of your wireless network (WLAN) 802.11 and configure certain security parameters.

- In the **Wireless** menu, select **Advanced**.

  The following screen opens:



Important

The table below indicates in more detail how to access your Wi-Fi port (or **A**ccess **P**oint).

Nevertheless, it is best to leave the default values for easier usage.

Field	Action/Meaning	Default value
Band	Select the 2.4 GHz band for the IEEE 802.11g standard.	**2.4GHz**
Channel	This is the radio channel used by the router and its Wi-Fi clients to communicate with each other. This channel must be the same for the router and all its Wi-Fi clients. Select the **channel** you want from the scroll down list (auto, channels 1 to 13). **Note:** Channel 11 corresponds to frequency 2462 MHz. **Note:** If you select "Auto", the Wi-Fi equipment will select the access point channel (router) which will emit the strongest signal. Conform to the CE Declaration of conformity / Radio rules list in Annex A to paragraph B.2.	**Auto**

Field	Action/Meaning	Default value
Auto Channel Timer (min)	Configure the duration, in minutes, during which the router must seek the best wireless channel. This option is only available when the selection of the channel is configured in **Auto** (Automatic).	**Auto**
802.11n/EWC	Select **Auto** to enable the 802.11n standard and enjoy ideal speeds for the digital home devices (HDTV, DVD, ...) to 270 Mbit/s.	**Auto**
Brandwidth	Select the bandwidht 20 MHz or 40 MHz.	**20 MHz**
Control Sideband	Select in the drop-down list the required value to specify if the extension channel should be in the **Upper** or **Lower** sideband.	**Lower**
802.11n Rate	Select in the drop-down list the Physical Layer (NPHY) rate required. **Note:** These rates are only available when the 802.11n mode is set to Automatic.	**Auto**
802.11n Protection	The 802.11g standards provide a protection method in order 802.11g and 802.11b devices to coexist in the same network without exchanging data at the same time. • Select **Off** only if there is a possibility that 802.11b or 802.11g devices will use your wireless network. • Select **Auto** for the wireless devices use RTS/CTS to improve 802.11n performance in mixed 802.11g/802.11b networks	**Auto**
Support 802.11n Client Only	Select On in the drop-down list to enable support for 802.11n clients only. **Note:** In this case, note that 802.11g and 802.11b clients will not be able to connect to the network.	**Off**
RIFS Advertisement	RIFS stands for Reduced Interframe Space. RIFS were introduced with 802.11n to improve efficiency for transmissions to the same receiver in which a SIFS-separated response is not required, such as a transmission burst.	**Auto**
OBSS Co-Existance	Select **On** in the drop-down list number of cases in which the primary and the non-primary channels overlap.	**Enable**
RX Chain Power Save	Enabling this feature turns off one of the Receive chains.	**Disable**
RX Chain Power Save Quiet Time	The number of seconds the traffic must be below the PPS value below before the Rx Chain Power Save feature activates itself.	**10**
RX Chain Power Save PPS	The maximum number of packets per seconds that can be processed by the WLAN interface for a duration of Quiet Time, described above, before the Rx Chain Power Save feature activates itself.	**10**
Radio Power Save	Enabling this feature turns off one of the Transmit chains.	**Disable**
Radio Power Save Quiet Time	The number of seconds the traffic must be below the PPS value below before the Radio Chain Power Save feature activates itself.	**10**

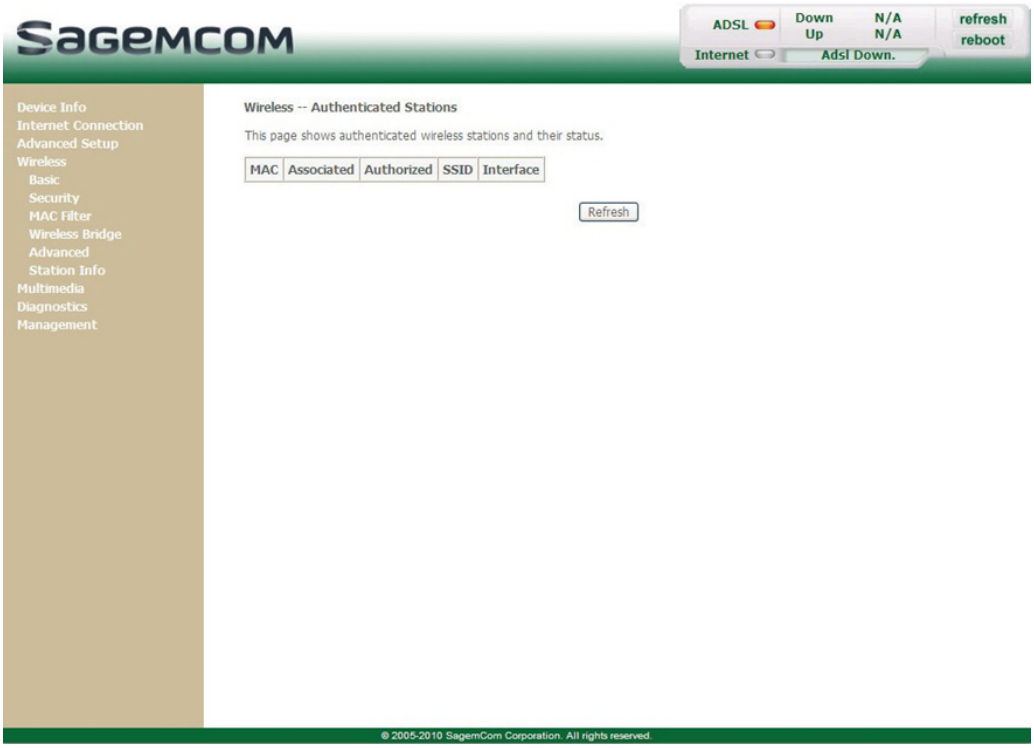
Field	Action/Meaning	Default value
Radio Power Save PPS	The maximum number of packets per seconds that can be processed by the WLAN interface for a duration of Quiet Time, described above, before the Radio Chain Power Save feature activates itself.	**10**
54g™ Rate	In the scroll down list, select the transmission rate at which the information (data or video) will be transmitted or received on your wireless network (Auto, 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 or 54 Mbps). **Note:** If you select "Auto", the information will be transmitted at an optimised rate which takes account of the transmission constraints.	**1 Mbps**
Multicast Rate	From the scroll down list, select the transmission rate at which the "Multicast" packets are transmitted (Auto, 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 or 54 Mbps). **Note:** If you select "Auto", the information will be transmitted at an optimised rate which takes account of the transmission constraints. Video conferencing and teleconferencing are "Multicast" applications.	**Auto**
Basic Rate	From the scroll down list, select the basic rate at which the information will be transmitted or received over your wireless network (Default, All, 1 & 2 Mbps or 1 & 2 & 5.5 & 6 & 11 & 12 & 24 Mbps).	**Default**
Fragmentation threshold	This packet fragmentation mechanism is used to limit errors and repetitions. It is recommended not to reduce the packet size too much to avoid reducing the bandwidth. Enter a threshold value (in bytes) between 256 and 2347.	**2346**
RTS Threshold	The RTS/CTS protocol (**R**equest **T**o **S**end / **C**lear **T**o **S**end) is used to reduce the probability of collisions between stations. **Note:** As packet size is set by default to 2346, the RTS/CTS protocol is inhibited as its value is set by default to 2347. Enter a threshold value (in bytes) between 1 and 2347.	**2347**
DTIM Interval	Enter a time interval value between two beacon signals which shows the activity of the wireless.	**1**
Beacon Interval	A beacon is basically a heartbeat for a wireless client or gateway, sending out a signal informing wireless clients that the wireless network is still active. Enter a time in milliseconds between beacon transmissions between 1 and 1000 milliseconds. The default beacon interval is 100 ms.	**100**
Global Max Clients	Enter the maximum number wireless customers for your router.	**16**
XPress™ Technology	From the scroll down list, select **Enabled** to apply the "XPressTM" technology or **Disabled** to not apply it.	**Disabled**
Transmit Power	If 802.11 h is selected, in the scroll down list select the cyclical emission ratio (20%, 40 %, 60 %, 80 % or 100 %) at which you want to transmit. **Note:** The power rate will be selected according to your environment.	**100%**

Field	Action/Meaning	Default value
WMM(Wi-Fi Multimedia)	Select **Enabled** to apply the WMM support, or **Disabled** not to apply it in the scroll down list.	**Enabled**
WMM No Acknowledgement	Select **Enabled** or **Disabled** in the scroll down list to permit or prohibit a more effective bit rate of the data flow with, on the other hand, a higher error rate. **Note:** The scroll down list may only be operational if the "WMM (Wi-Fi Multimedia)" field is activated.	**Disabled**
WMM APSD	**WMM** (**W**i-**F**i MultiMedia) with **APSD** (**A**utomatic **P**ower **S**ave **D**elivery) option manages battery-powered radio devices to extend their autonomy in some cases. This option provides a longer range tag to launch an application that requires a short interval of packet exchange. Select **Enabled** to activate this option.	**Enabled**

5.8.6 Station Info

Object: This menu is used to display all the wireless stations certified, with their status.

- In the **Wireless** menu, select **Station Info**.
  The following screen opens:



- Click on the **Refresh** button to refresh the screen.

Note

Only appear the MAC addresses (BSSIDs) of the computers associated with the router and/or authorized by this one to use your wireless network (see subsection 5.8.3 - MAC Filter).

5.9 Multimedia

Object: This menu is used to activate or deactivate the options of the multimedia interface of the router.

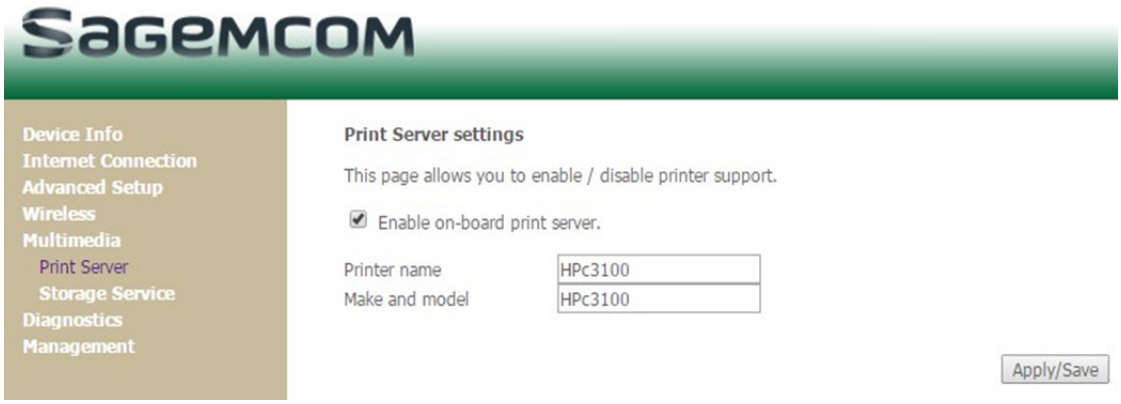
This section contains the following subtitles:

- Print Server (see subsection 5.9.1)
- Storage Service (see subsection 5.9.2)

5.9.1 Print Server

Object: This menu allows you to enable/disable printer support of the router.

- Select the **Multimedia** menu, then select **Print Server**.



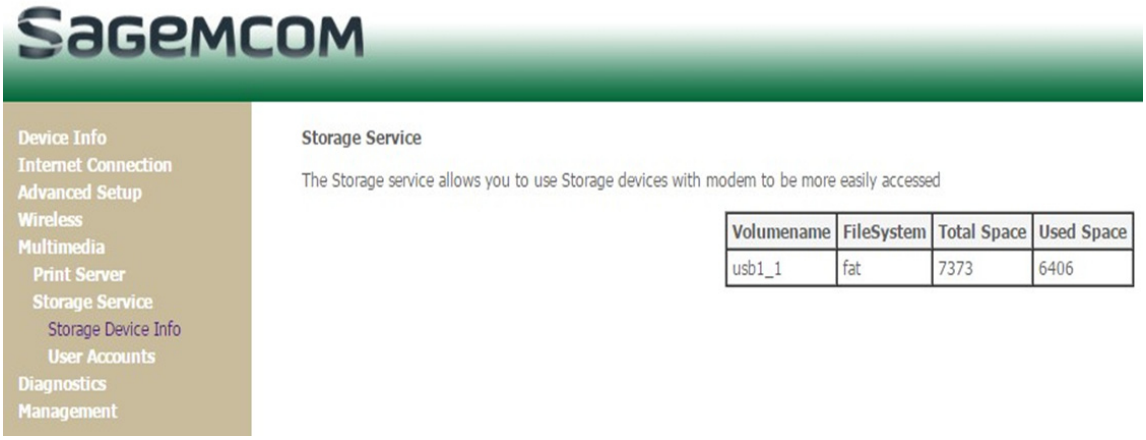
- Check the box to enable the print server of the router.
- Set a printer name and a printer model. (You can set to any name and model)
- Click on the **Apply/Save** button to save the parameters.

5.9.2 Storage Service

Object: This menu allows you to plug a USB hard drive on the modem and share its content with all clients connected to the network. You can also create user accounts to control access to shared contents.

- Select the **Multimedia** menu, then select **Storage Service**.

5.9.2.1 Storage Device Info



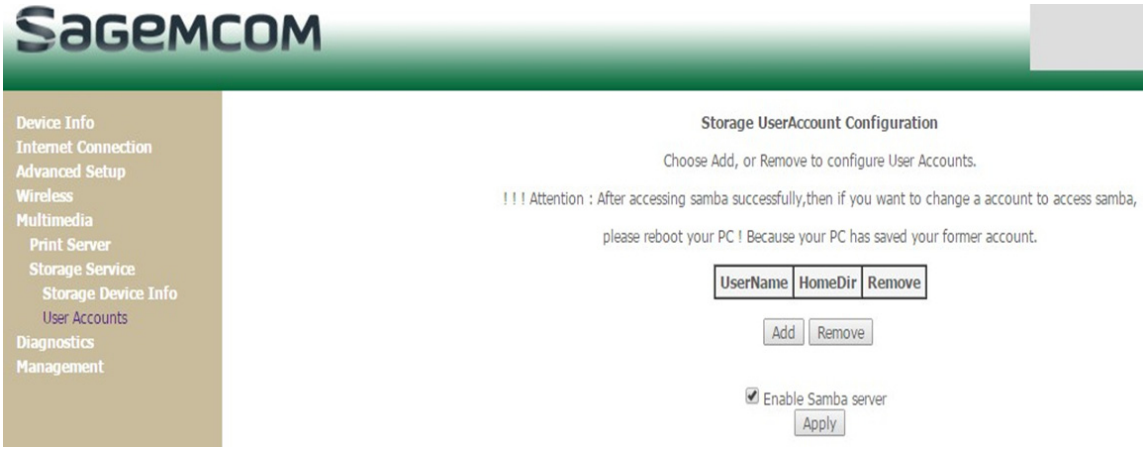
5.9.2.2 User accounts

Storage UserAccount Configuration

- Choose Add, or Remove to configure User Accounts.

Attention

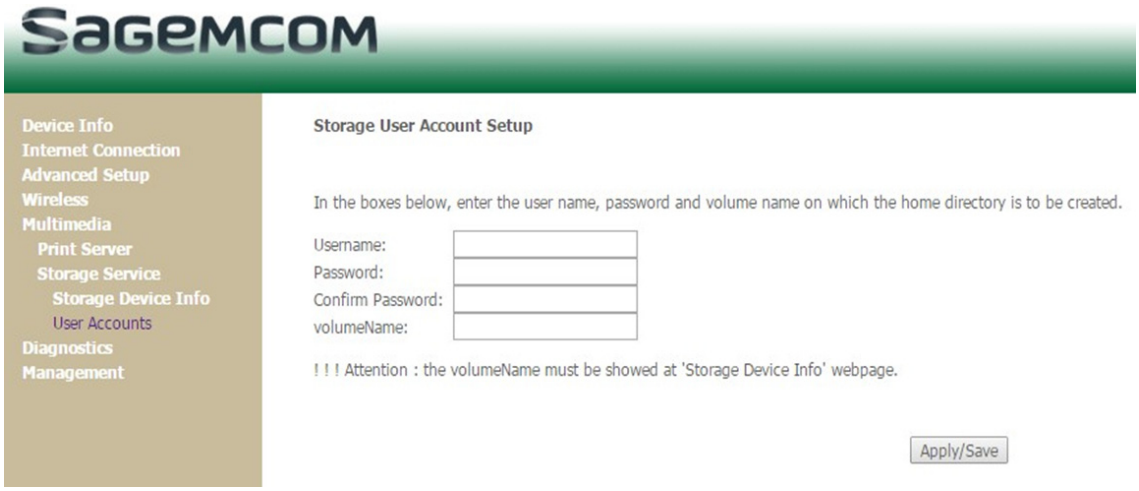
After accessing samba successfully, then if you want to change a account to access samba, please reboot your PC ! Because your PC has saved your former account.



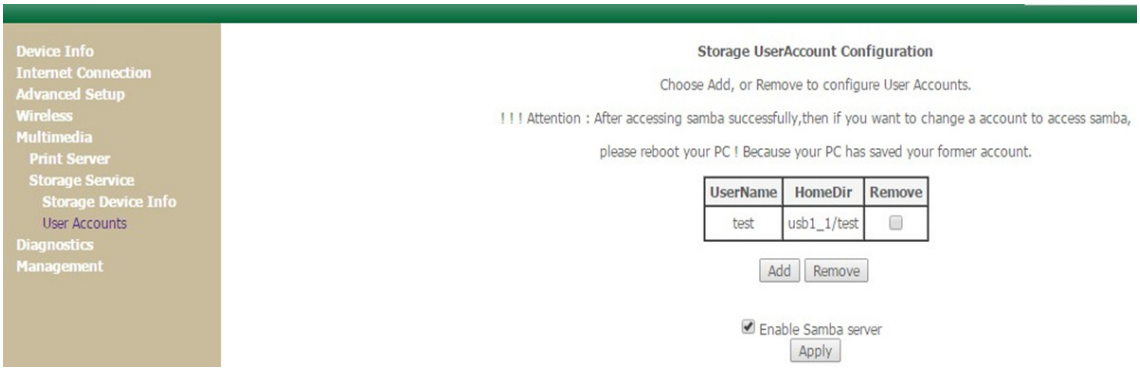
- In the boxes below, enter the user name, password and volume name on which the home directory is to be created.

Attention

the **volumeName** must be showed at '**Storage Device Info**' webpage



- In this example , the Username = test , the password = test , the volumeName is showed in the storage device info = usb1_1.



5.10 Diagnostics

Object: This menu is used to display all the tests performed on the connections made from your router to your **I**nternet **S**ervice **P**rovider (ISP). These tests concern:

- connection to your local network (LAN),
- connection to your "DSL Service Provider",
- connection to your "Internet Service Provider".

Note

A hypertext link (help) enables the user to access context-related help. This help gives an explanation concerning the state of the connection (**PASS** in green, **DOWN** in orange and **FAIL** in red) and supplies the appropriate troubleshooting procedures.

The ADSL line translates the three statuses detailed in the table below.

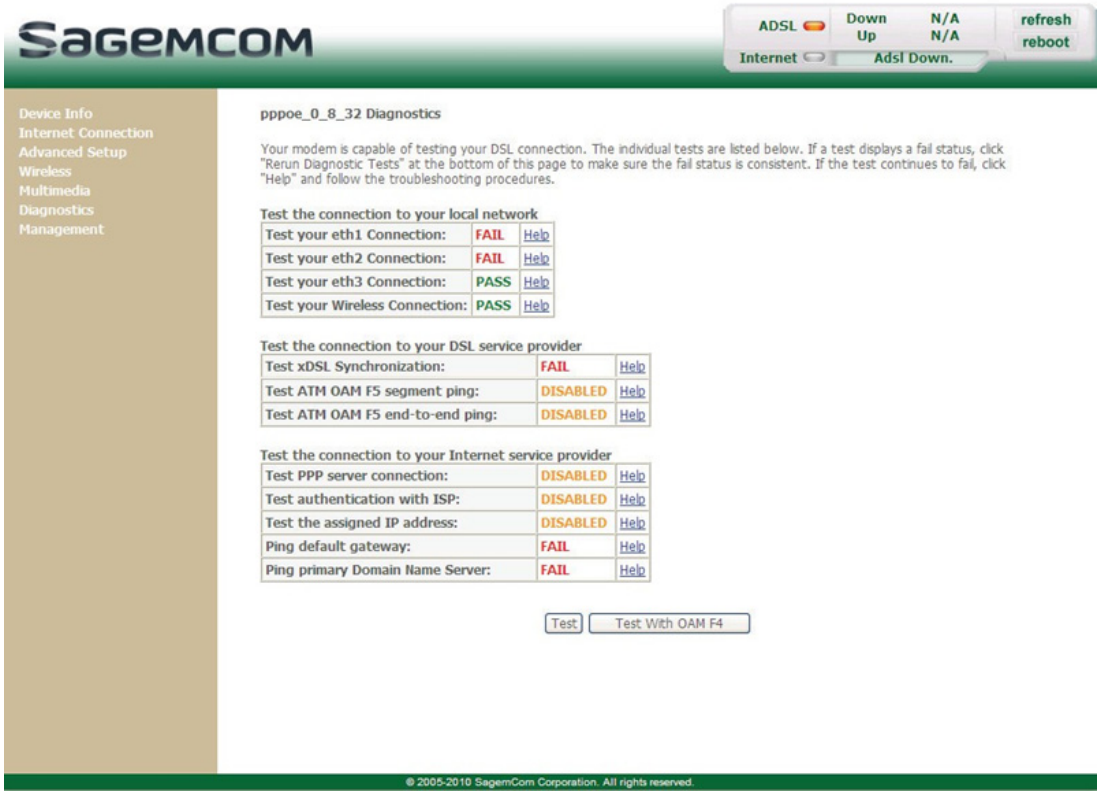
State	Meaning
PASS	Indicates that the test was completed successfully.
DOWN	Indicates that an interface (ETH, Wi-Fi) has not been detected.
FAIL	Indicates that the test has failed, or that it is impossible to start a command.

If a test fails, proceed as follows:

1. Click on the corresponding **Help** link to access detailed information and problem-solving procedures.
2. Click on **Test** to check the problem is solved and resume the connection tests.

To access the Diagnostic tool:

- Select the **Diagnostics** menu.



5.11 Management

Object: This menu lets you manage your router.

This section contains the following menus:

- Settings (see subsection 5.11.1)
- System Log (see subsection 5.11.2)
- Security Log (see subsection 5.11.3)
- TR-069 Client (see subsection 5.11.4)
- Internet Time (see subsection 5.11.5)
- Access Control (see subsection 5.11.6)
- Update Software (see subsection 5.11.7)
- Reboot (see subsection 5.11.8)
- Reboot (see subsection 5.11.8)

5.11.1 Settings

This menu contains the following sub menus:

- Backup (see subsection 5.11.1.1)
- Update (see subsection 5.11.1.2)
- Restore Default (see subsection 5.11.1.3)

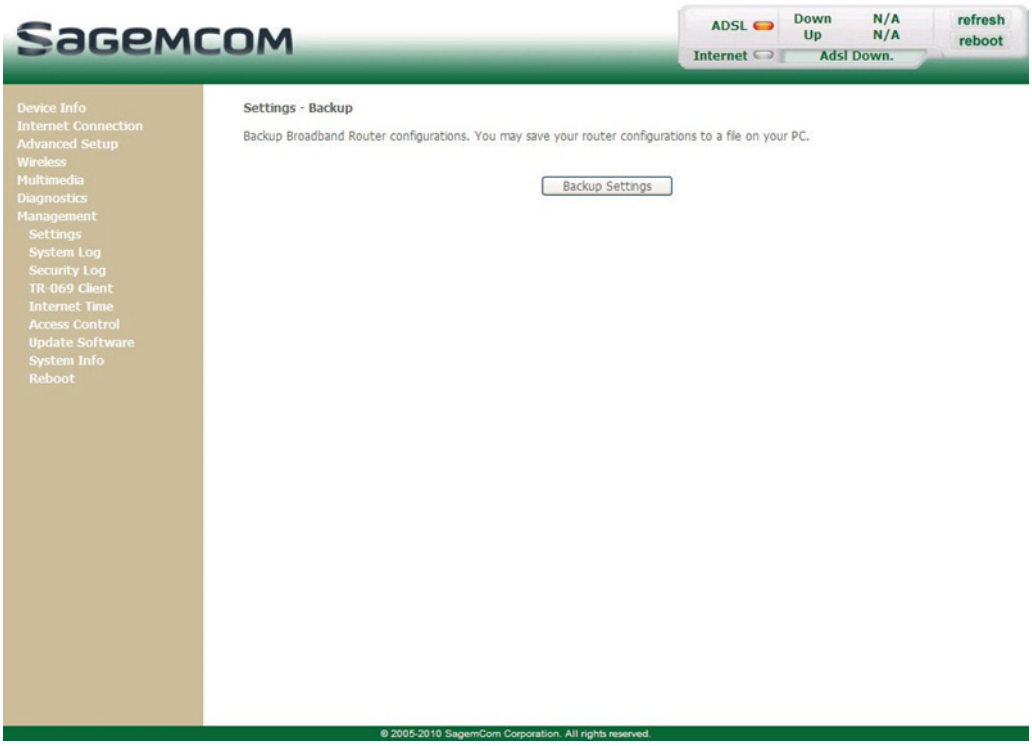
5.11.1.1 Backup

Object: This menu is used to backup the current configuration to a file with a .conf extension.

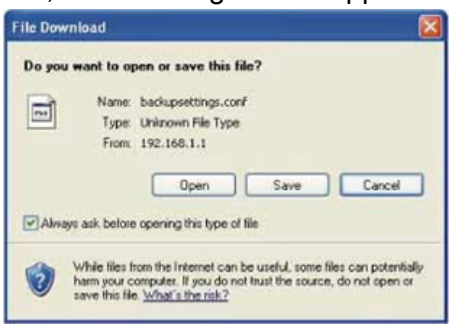
Important

It is recommended to save the current configuration on your computer to a file.

- In the **Management** menu, select **Settings** then **Backup**.
  The following screen opens:



- Click on the **Backup Settings** button; the following screen appears:



Save

- Click on the **Save** button to save the current configuration file, for example, on your computer.

- Select the directory where you want to save the "backupsettings.conf" configuration file.

Note

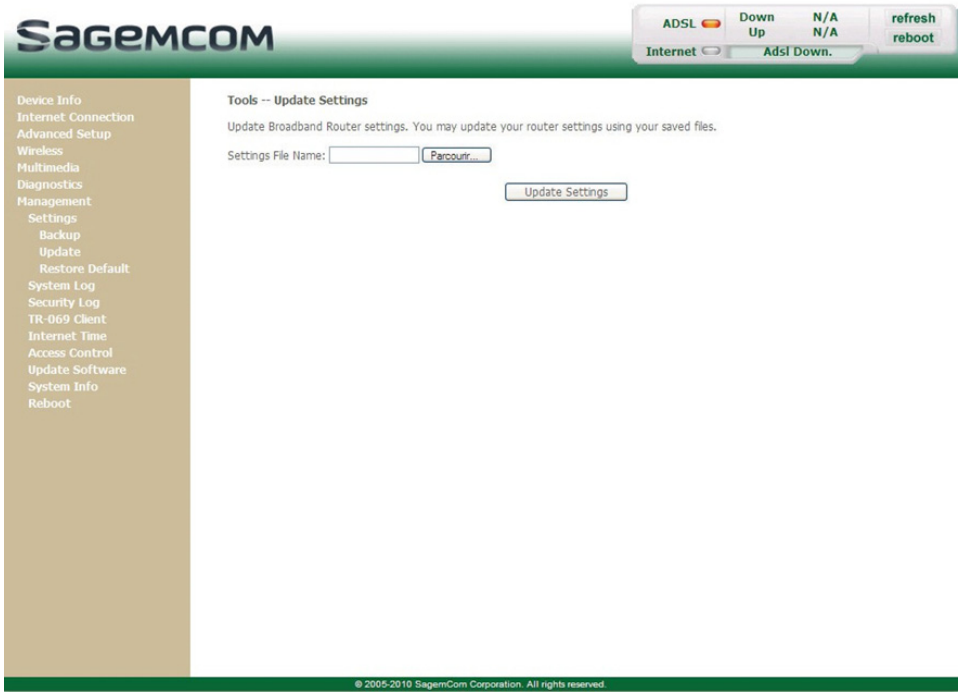
The process takes a few seconds.

5.11.1.2 Update

Object: This menu enables the router to recover a configuration which has already been saved to a file with a .conf extension.

- In the **Management** menu, select **Settings** then **Update**.

  The following screen opens:



Proceed as follows for your router configurer to display a configuration which has already been saved:

- Enter the path then the name of the configuration file.

or

- Click on the **Browse** button and select the path then the configuration file.
- Select the configuration file then click on the **Update Settings** button to recover a configuration which has already been saved.

Note

The process takes around 2 minutes.

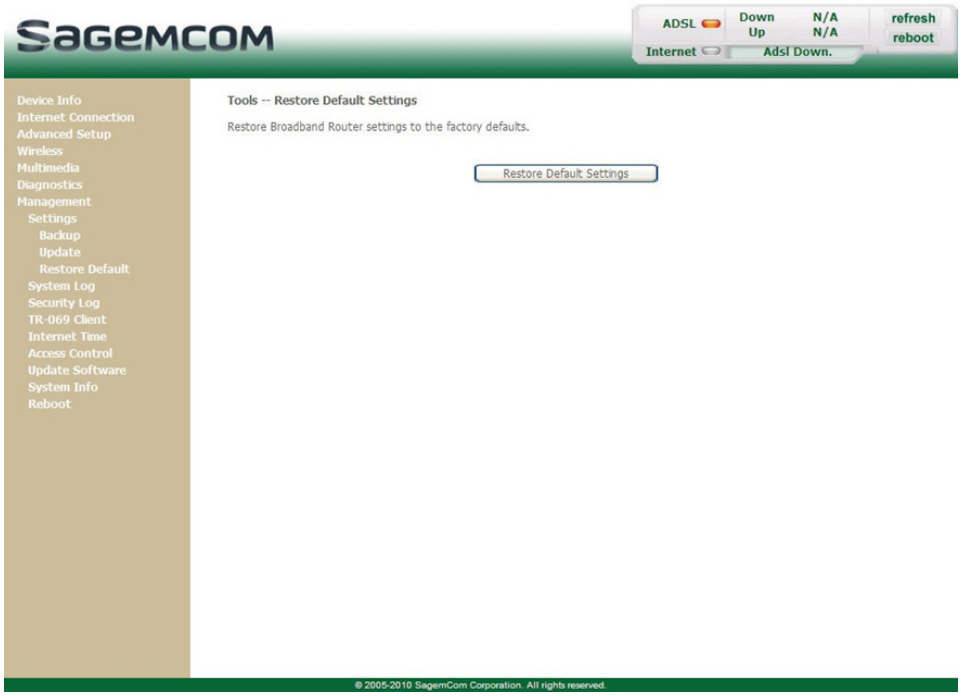
5.11.1.3 Restore Default

Object: This menu is used to return to factory configuration.

Important

The existing configuration is completely overwritten.

- In the **Management** menu, select **Settings** then **Restore Default**.
  The following screen opens:



- Click on the **Restore Default Settings** button; the following screen appears:

- Click on the **OK** button if you really want to return to the factory configuration.

Note

All the LEDs go off except for the green "WLAN" - if the wired network is activated; the green POWER LED then all the LEDs and the process for returning to the factory configuration starts. It lasts for around 2 minutes.

Once the restore performed, the **Internet Connection** menu appears. Refer to paragraph 5.6.

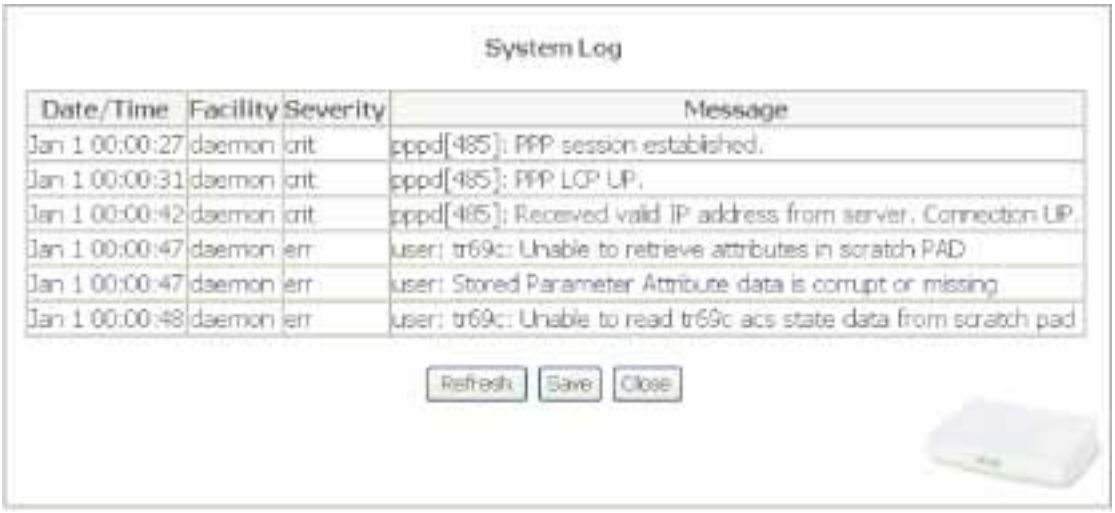
5.11.2 System Log

Object: This menu is used to view and/or configure the events which occur on your router.

- In the **Management** menu, select **System Log**.
  The following screen opens:

5.11.2.1 View System Log

- Click on the **View System Log** button to display the events with the severity you configured (see table in section **Configure System Log**).



5.11.2.2 Configure System Log

- Click on the **Configure System Log** button to configure the events which occur on your router.

Field	Action	Default value
Log	Select **Enable** to activate the saving of all the events to a log and display on screen or **Disable** to deactivate.	**Disable**
Log Level	Select the appropriate severity from the scroll down list. All the events with this severity, or a higher severity, will be saved to your router's volatile "flash" memory. The severities are classified in decreasing order of importance. • Emergency • Alert • Critical • Error • Warning • Notice • Informational • Debugging	**Debugging**
Display Level	Select the appropriate severity from the scroll down list. All the events with this severity, or a higher severity, can be viewed by pressing the **View System Log** button. The displayed events are classified in decreasing order of importance.	**Error**

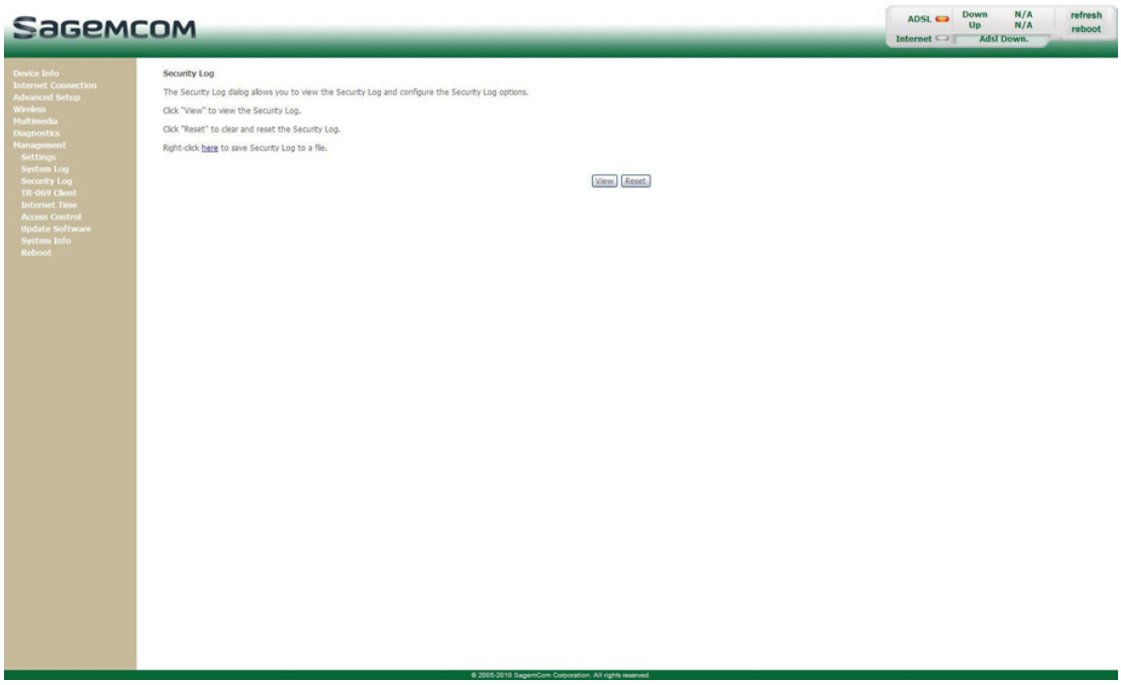
Field	Action	Default value
Mode	Select the destination ID from the scroll down list: • **Local**: All the events are returned to your router via a "Buffer" memory. • **Remote**: All the events are returned to the "Syslog" server. • **Both** : Both modes.	**Local**
Server IP Address[a]	Enter the IP address of the "Syslog" address on which all the events will be saved.	**0.0.0.0**
Server UDP Port[a.]	Enter the number of the port associated with the "Syslog" server.	**514**

a. These fields only appear when the mode selected is "Remote" or "Both".

5.11.3 Security Log

Object: This menu allows you to view the Security Log and configure the Security Log options. This log deals with all the events (connections, failure, and so on) relative to the firewall rules.

- In the **Management** menu, select **Security Log**.
  The following screen opens:

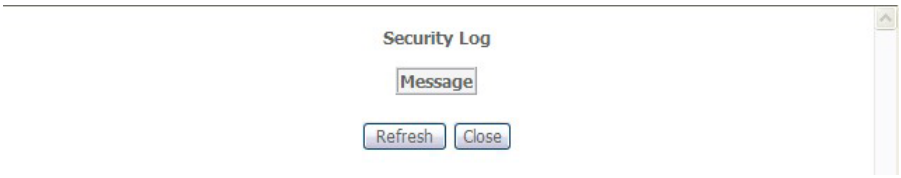


5.11.3.1 Save the security log

Make a right click on the link to save the security log to a text file.

5.11.3.2 View the security log

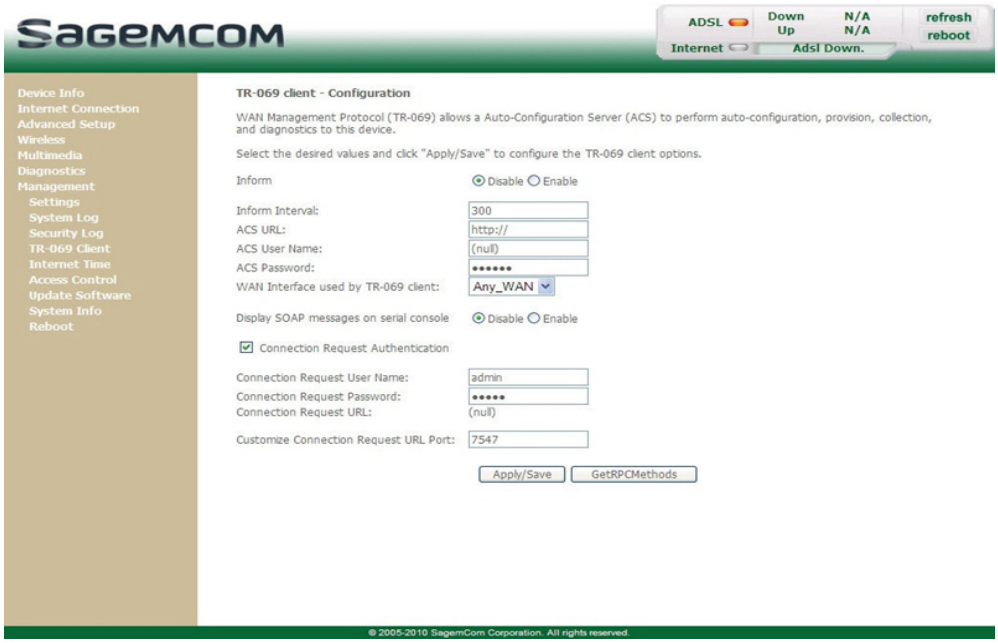
- Click on the View button to view the security log.
  The following screen opens:



5.11.4 TR-069 Client

Object: The TR-069 protocol (WAN Management Protocol) is used, via a remote server (**A**uto-**C**onfiguration **S**erver (ACS)) to auto configure your router, provide it with certain services and manage it by establishing "diagnostics".

- In the **Management** menu, select **TR-069 Client**.
  The following screen opens:



Field	Action	Default value
Inform	Check the **Enable** box to activate the "TR-069" or **Disable** to deactivate it.	**Disable**
Inform Interval	Enter a time interval between two pieces of information sent from the router to the ACS server. This interval is a value (in seconds).	**300**
ACS URL	Enter the URL or the IP address of the ACS server.	**-**
ACS User Name	Enter the name of the user of the ACS server.	**admin**
ACS Password	Enter the ACS server password.	**admin**
WAN Interface used by TR-069 client	Select in the scroll down list the desired WAN interface.	**Any_WAN**
Display SOAP Messages on serial console	Check the **Enable** box to activate it or **Disable** to deactivate it.	**Disable**
Connection Request Authentication	Check the box to activate authentication or uncheck it to deactivate it.	**Checked**
Connection Request User Name	Enter the name of the user of your router.	**admin**
Connection Request Password	Enter your password for your router.	**admin**
Customize Connection Request URL Port	Enter the port to use for Connection request from the ACS.	**7547**

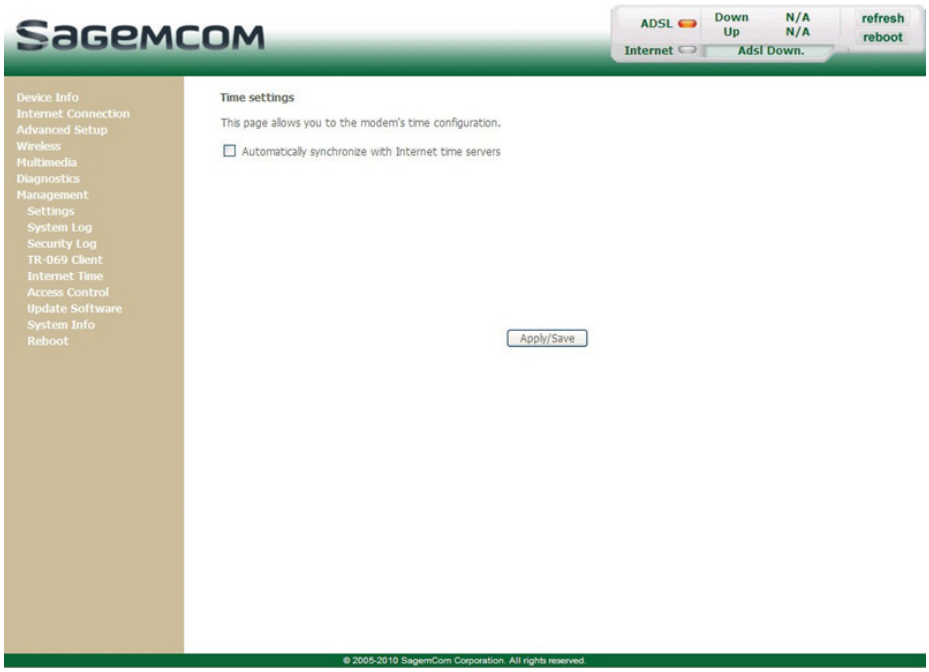
- Click on the **Get RPCMethods** button to launch the auto-configuration procedure of your router.

5.11.5 Internet Time

Object: This menu lets you display the date and time in the Date / Time field of your HTTP configurer:

- either the one delivered by your router. The date and time when the router starts are set to: "Jan 1 / 00:00:00" (i.e. 1st January at 0 am).
- or the one delivered automatically by an Internet time server.

- In the Management menu, select Internet Time.
  The following screen opens:



Field	Action	Default value
Automatically Synchronise with Internet time servers	• Uncheck the box so that the **Date / Time** field (which appears, for example in the "Management/System Log" screens) displays the date and time delivered by your router, or • Check the appropriate box so that the **Date / Time** field (which appears, for example, in the "Device Info/Summary" and "Management/System Log" screen) displays the date and time delivered by the NTP servers (Network Time Protocol) you selected. These servers display the date and time GMT (**G**reenwich **M**ean **T**ime). **Note:** For these events to be displayed and/or saved at an effective date and time, you should check this box.	**Not checked**

5.11.6 Access Control

This menu contains the following sub menus:

- Passwords (see subsection 5.11.6.1)

5.11.6.1 Passwords

- In the **Management** menu, select **Access Control** then **Passwords**.
  The following screen opens:

Field	Action
User Name	Select a user name from the scroll down list: • Admin • Support • User **Note:** This list is established in increasing order of restriction.
Old Password	Enter your old password
New Password	Enter your new password
Confirm Password	Confirm your new password

Note

The password is a string of a maximum of 16 alphanumerical characters.

5.11.7 Update Software

Object: This menu lets you update the latest version of the router software.

- In the **Management** menu, select **Update Software**.
  The following screen opens:

Proceed as follows to update your router's software version:

- Enter the path then the name of the software version file,

or

- Click on the **Browse** button and select the path then the software version file.
- Click on the **Update Software** button to update the software version.

Note

The process takes around 2 minutes.

The application of a new software version for the router does not modify the current configuration at all.

Important

Throughout the download procedure (up to five minutes), you must:

- not power down the router
- not disconnect from the ADSL line.

5.11.8 Reboot

Object: This menu lets you save all the modifications made to the current configuration and restart the router with its new parameters.

- In the **Management** menu, select **Reboot**.

  The following screen opens:

Click on the **Reboot** button to restart the router.

Note

The process takes around 1 minute.

A countdown is displayed to tell the user how long is left to wait.

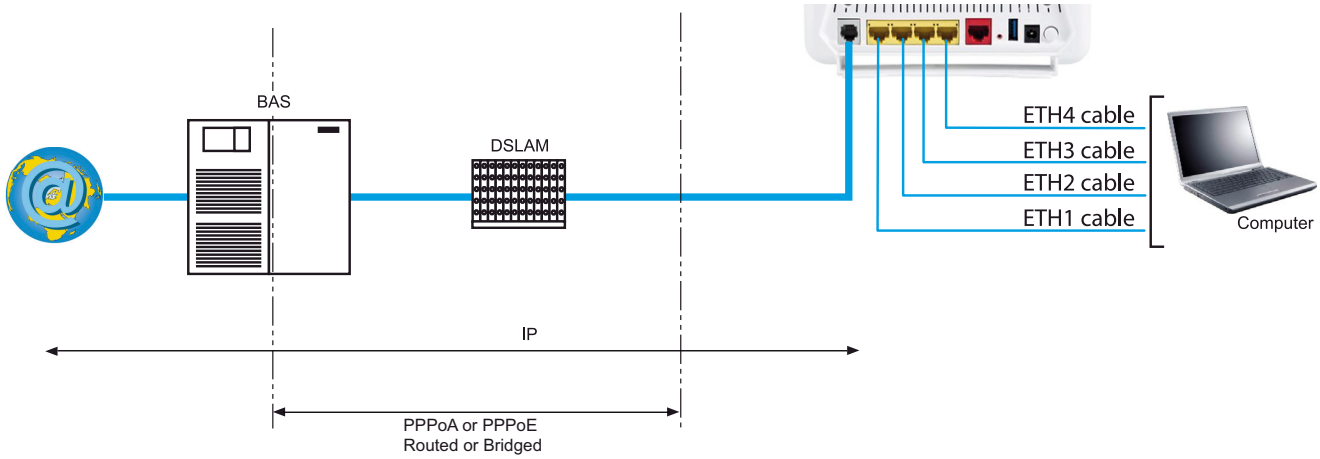
6. Internet access service

This section covers	• Description of the Internet access service	p. 6-2

The router has been designed to enable you to access the Internet as simply as possible.

Most of the router's parameters are already set:

- It is configured by default as a DHCP server.
- It relays DNS queries from the local network to the Internet.



Depending on your contract with your **I**nternet **S**ervice **P**rovider (ISP), you can also have access to television on ADSL (see section 8).

The configuration parameters of your router are entered during installation (connection identifier, connection password). These parameters can also be entered or modified in the **Internet connection** menu of the HTTP configuration tool (PPP Username, PPP Password).

Observations

If the terminals are not DHCP clients, your local network then uses a static addressing plan.

Check that:

- the router belongs to this addressing plan,
- the default gateway of the equipment in the local network matches the address of your router,
- the DNS addresses are correctly configured in each terminal. The router enables DNS queries to be relayed.

7. TV over ADSL service

This section covers	• the introduction	§ 7.1
	• access to the optional TV over ADSL service	§ 7.2

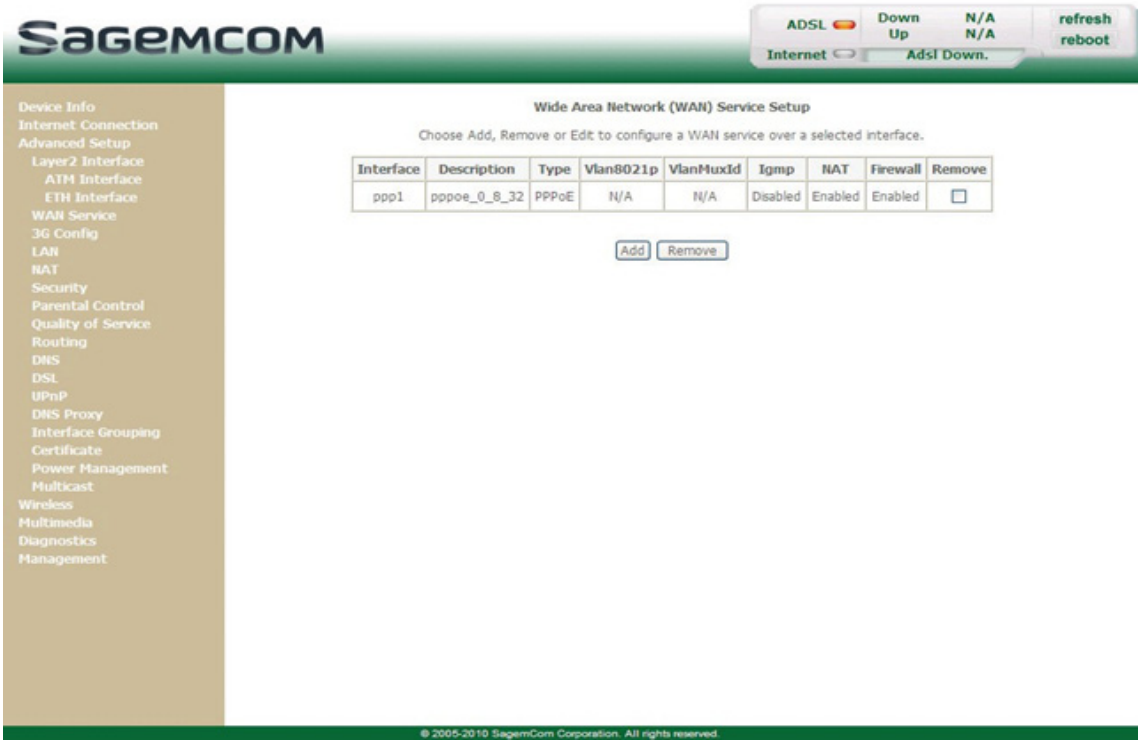
7.1 Introduction

Your router is compatible with TV over ADSL technology.

7.2 Access to the optional TV over ADSL service

To access this service, you must have:

- made the connection in accordance with section 2.3.4,
- necessarily taken a subscription with your **I**nternet **S**ervice **P**rovider (ISP)
- configured one VC (**V**irtual **C**hannel) dedicated to video, and another VC dedicated to data (see screen below)



Note

In the example above, the ATM interface "ppp_8_35_1" is dedicated to data and the ATM interface "nas_8_50_1" is dedicated to video.

- configured accordingly "Port Mapping" in **Advanced Setup** (see section **6**).

8. Updating the firmware

This section covers	• setting up the download	p. 8-2

You can update the firmware using one of the following methods:

- via HTTP
- via TR69 protocol
- automatically: the new firmware version download is performed automatically on starting up the router.

Important

Throughout the download procedure (up to five minutes), **you must**:

- not power down the router,
- not disconnect from the ADSL line.

The download process is transparent on the router side: there is no LED blinking informing you of the download process. **So please make sure to wait for the router to reboot completly**. The HTTP tool configuration however shows the download status in the Supervision box.

Note

To check that the new version has been correctly downloaded, select in the HTTP configuration tool the **Device info** menu; the **Software version** field displays the last software version installed.

HTTP update

You can download the new firmware to update your router using the **Management** menu in the HTTP configuration tool (see section 5).

TR69 protocol

Operators can use "TR69" protocol to upgrade the router's firmware from their ACS server.

Annex A - Troubleshooting

This section covers	• checking the assignment of an IP address	§ A.1
	• Front panel LEDs	§ A.2
	• Supervision of your router	§ A.3
	• the "Diagnostics" tool	§ A.4
	• interpreting the lights	§ A.5
	• reinitialising your router	§ A.6
	• resetting factory configuration	§ A.7
	• Offline connection mode	§ A.8

A.1 Checking the assignment of an IP address

In Windows Seven, Vista, XP

1. Click on **Start > Run**, enter **cmd** and then click **OK**.
   (**Start** > **all programs** > **accessories** >**Run** for Windows seven)
   The command prompt screen appears.
2. Enter **ipconfig** then press **Enter**.
3. Check that the entry IP Address contains a value other than **0.0.0.0** (for example ***192.168.1.10***).

Note

If no IP address is displayed, enter **ipconfig /release** then enter **ipconfig /renew**.

Note

All the troubleshooting procedures described below are undertaken in **Windows® XP**. These procedures in other Windows operating systems® (Seven and 8, 8.1) can be slightly different.

Many sources of information are available to help you identify and resolve issues you may experience:

- the LEDs on the front panel of the router.
- the HTTP configuration tool.

For step-by-step and advanced problem-solving procedures, use the **Diagnostic tool** available in the HTTP configuration tool.

A.2 Front panel LEDs

Note

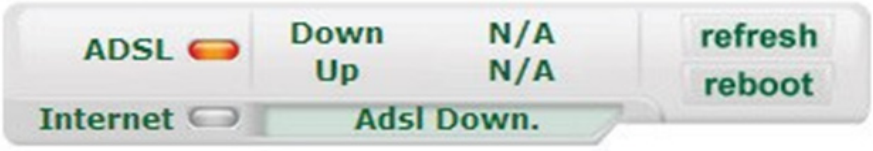
When the router is switched on, the ⏻ LED is green.
If no connection is made, the @ LED is off.

LED	Status	Meaning
⏻ Power	**Off**	Power Off
	Green	Power On
	Red	Router in rescue mode
ADSL	**Green steady**	ADSL Up
	Green blinking	• ADSL Synchronisation in progress or • down
@ Internet	**Off**	• Power Off or • The Internet account must be configured or • Bridge mode
	Green steady	The Internet account is configured
	Green blinking	Tx/Rx traffic
	Red	Invalid or unauthorised Internet account
LAN x (1 to 4)	**Off**	No link detected on the Ethernet port
	Green steady	Ethernet port has detected a link with 100 Mbps device
	Green blinking	Tx/Rx traffic at 100 Mbps
WLAN	**Off**	Wi-Fi deactivated
	Green steady	Wi-Fi activated
	Green blinking	Wi-Fi Tx/Rx
USB	**Off**	No USB connection
	Green steady	USB connection available
	Green blinking	USB connection reading in progress
TV	**Green steady**	IP TV Activated
	Green blinking	Playing IP TV

A.3 Supervising your router

You can monitor the router's activity and status using the router's built-in "DSL Router" HTTP controller, available in the HTTP configuration tool.

The router's activity status is always visible at the left corner or the top right of the HTTP configuration tool.



You can perform the following actions:

- click on **Refresh** to update the data displayed
- click on **Reboot** to restart your router

ADSL information

The following table presents the possible states of the **ADSL** field:

Status	Meaning
Green	ADSL line synchronised
Yellow	ADSL line synchronising
Red	ADSL line not connected

The **Downstream** field displays the nominal downlink bit rate.

The **Upstream** field displays the nominal uplink bit rate.

Internet information

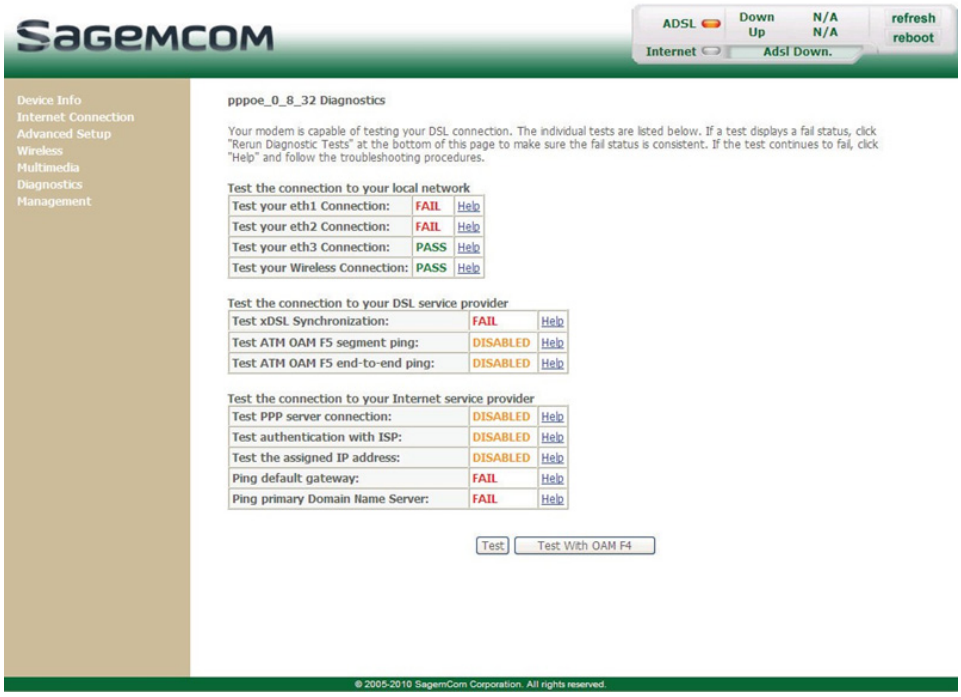
The following table presents the possible states of the **Internet** field:

Status	Status	Meaning
Off	**ADSL Down**	ADSL line not connected or not activated
	Not configured	The Internet account must be configured
	Router rebooting	Router is rebooting
Green	**Connected**	The Internet connection has succeeded
Yellow	**Waiting for ISP**	Connecting to the Internet service
Red	**Access denied**	Incorrect Internet account

A.4 Diagnostics tool

To access the Diagnostic tool:

1. Open your browser.
2. Enter the router's IP address or enter the following URL: http://myrouter.
3. In the login screen that appears, enter your username and password.
   Default values are:
   - User name: **admin**
   - Password: (see the router sticker)
4. The welcome page of the HTTP configuration tool appears.
5. Select the **Diagnostics** menu.



6. Click on **Test**. The connections to the LAN, to your DSL Service Provider and to your Internet Service Provider are tested step-by-step:
   - successful tests are marked as a pass.
   - unsuccessful tests are marked as a fail.

Note

Status **DOWN** means that an interface was not detected (LAN or Wi-Fi).

Note

FAIL test

Depending on the nature of the test, it is possible that operation of the router or access to the Internet may not be prejudiced. For example if you do a "Ping" either to an ATM OAM F5 segment or to a DNS primary address.

7. If a test fails, click on the corresponding **Help** link to access detailed information and problem-solving procedures.
8. Click on **Test** to check the problem is solved and resume the connection tests.

If none of the above helps you solve the problem, and you are still having trouble connecting to the Internet, we recommend that you restart your router (cf. § A.6) and eventually reset the factory configuration (cf. § A.7). You will then need to re-configure your router as a first-time setup.

A.5 Interpreting the LEDs

A.5.1 The "ADSL" LED blinks slowly

1. Check the connection of your ADSL filters. Each telephone socket of your installation which is used must be equipped with an ADSL filter.
2. Check that the RJ11 type line cord delivered with your router is connected to one of your sockets. It is recommended that no telephone extension is used.
3. Finally, check with your ISP that the ADSL service is available on your telephone line.

A.5.2 "Wi-Fi" LED off

If this LED is off, this indicates that the WLAN interface of the router is not active.

To activate the wireless network, access the HTTP configuration tool and check the box "Enable Wireless" in the **Wireless** menu (see section 5).

A.5.3 All LEDs are off

1. Check that the type of power available in your premises is compatible with the mains voltage required for powering your router.
2. Check that the delivered power cord is properly connected at one end to the mains power network.
3. Check that the power connector is inserted correctly in the corresponding connector (power) of the router.

A.6 Restarting your router

We recommend that you restart your router if you notice that the router does not operate properly.

To restart your router, use one of the following methods:

- Press the **Power** button located on the rear panel of the router. Press it again to switch it back on.
- Click on the **Reboot** action of the HTTP configuration tool.

During restarting, the status of the LEDs is the following:

The LED will light up first, followed by the four Ethernet LEDs (1 to 4), then these last four LEDs will be off. The and Ethernet (which corresponds to the connected interface) LEDs should be steady and the LED blinks during the establishment of the ADSL link, then steadies like the LED. The goes from blinking to steady when a PPP session has been created successfully.

Note

The powering up process lasts around one minute.

A.7 Resetting factory configuration

If you lose your password or if, after having entered new parameters in your router, you cannot access the Internet nor the HTTP configuration tool, you can restore the normal operation with the "factory" parameters via the **Restore Default** procedure.

When the procedure is finished you will have to enter again your connection ID and connection password delivered by your Internet Service Provider (see **Internet Connection** - section 5.6)

To reset the default settings and therefore restore the router to its factory configuration, use one of the following methods:

Important

This operation deletes the entire personalised configuration of your router: Password, Configuration, customized wireless settings, etc.
After a factory configuration reset, it is **necessary to install your router again** using the installation CD-ROM, or to enter again the ADSL connection data supplied by your **I**nternet **S**ervice **P**rovider (ISP) (see Internet Connection section 5.6).

- Press and hold for about 10 seconds the **Reset** button located on the rear panel of the router.
- In the HTTP configuration tool, select **Management > Settings > Restore default**.

A.8 Offline mode

To start configuring the router in HTTP mode, the browser opens, the default IP address of the router's LAN interface appears in the browser's Address field **but the home screen does not appear**.

The screen opposite appears. Click **Connect**.	
The screen opposite appears. Click **Settings**.	
The screen opposite appears. Select the **Connections** tab and then the **Never dial a connection**[a]. Click **OK** to confirm your choice.	

a. When the router is installed, this box is checked.

In the menu bar, select the **File** menu then deselect the **Work Offline** command.

Click **OK** in the browser's **Address** field to display the home screen.

Annex B - Warnings for safety

This section covers	• Warnings for safety	§ B.1
	• EC compliance declaration	§ B.2

B.1 Warnings for safety

The router is in compliance with standard EN 60950 Ed December 2001.

The safety levels in the sense of this standard are as follows:

B.1.1 Safety levels in relation to the case

Connecteurs	Position	Safety level
Adaptator	Primary Power Supply port	HPV[a]
PWR	DC Power Supply port	SELV[b]
LINE	ADSL port	TNV3[c]
LAN1 to LAN4	Ethernet port	SELV[b].

a. **H**azardous **P**rimary **V**oltage circuit
b. **S**afety **E**xtra **L**ow **V**oltage Circuit
c. Level **3** **T**elecommunication **N**etwork **V**oltage

B.2 EC compliance declaration

CE marking

The CE marking certifies that the product complies with the essential requirements of the Directive 1999/5/EC concerning radio equipment and telecommunication equipment, and of Directives 2006/95/EC concerning safety and 2004/108/EC concerning electromagnetic compatibility, defined by the European Parliament and Council to reduce electromagnetic interferences and protect the health and safety of users.

The product named F@ST 4310 can be operated in the European Union without restrictions indoor but cannot be operated in France in the whole of the band until further notice.

The CE declaration of conformity can be viewed in the support section of the Sagemcom site www.sagemcom.com, or it can be obtained from the following address:

Sagemcom - Customer relations department
250, Route de l'Empereur
92848 RUEIL MALMAISON CEDEX - FRANCE

Annex C - Environment

This section covers	• directive E 2002/96/CE	§ C.1

C.1 Directive E 2002/96/CE

ENVIRONMENT. Preservation of the environment as part of a sustainable development logic is an essential concern of Sagemcom.

Sagemcom aim is to operate systems safeguarding the environment and consequently it has decided to integrate environmental performance considerations in the life cycle of its products, from manufacturing to commissioning, use and disposal.

PACKAGING

The presence of the logo (green dot) means that a contribution is paid to an approved national organization to improve packaging recovery and recycling infrastructures.

To facilitate recycling, please respect the sorting rules set up locally for this kind of waste.

BATTERIES

If your product contains batteries, they must be disposed of at appropriate collection points.

THE PRODUCT

The crossed-out waste bin marked on the product or its accessories means that the product belongs to the family of electrical and electronic equipment.

In this respect, the European regulations require you to dispose of it selectively:

- At sales points on purchasing similar equipment,
- At the collection points made available to you locally (drop-off center, selective collection, etc.).

In this way, you can participate in the re-use and upgrading of Electrical Electronic Equipment Waste, which can have an effect on the environment and health.

Annex D - Technical Characteristics

This section covers	• mechanics and display	§ D.1
	• the characteristics of the different interfaces	§ D.2
	• environmental characteristics	§ D.3
	• the application and the protocols	§ D.4

D.1 Mechanics: Display

Mechanical characteristics	
Dimensions (mm)	
Width:	175 mm
Depth:	144 mm
Thickness:	65 mm
Weight of router	268 g

Display		
Marking	**Abbreviation**	**Meaning**
	**PWR**	• Green Power LED
	**ADSL**	• Green ADSL LED
	**Wi-Fi**	• Green WLAN LED
	**Internet**	• Green/Red Internet LED
	**USB**	• Green USB LED
	**LAN**	• Green LAN LED
	**IPTV**	• oGreen IPTV LED

D.2 Characteristics of the different interfaces

ADSL / ADSL2 / ADSL2+ Interface	
Standards supported	• G.992.1 (ADSL), G.992.3 (ADSL2), G.992.5 (ADSL2+) • G.994.1 (G.Handshake)
Transmission Code	• DMT
Maximum upward transmission rate	• 24,5 Mbit/s
Maximum downward transmission rate	• 1,3 Mbit/s
Latence	• Simple (Fast or interleaved)
TX Power	• 12,5 dB
Access Impedance	• 100 Ù
Range	• According to standard G.992.1 table Annex
Connection technology	• RJ11

Interface LAN Ethernet	
Rate	• 10 Mbit/s or 100 Mbit/s, self-configurable
	• Half / Full Duplex
Standard	• IEEE 802.3
Connection technology	• RJ45
	• Type MDI or MDI-x self-detecting port
	• Crossed or straight cord

Wireless Interface	
Standard	• **IEEE 802.1b/g1n**
Frequencies band	• 2412 MHz to 2472 MHz (ISM band)
Transmission rate	• Up to 300 Mbit/s
Safety	• WEP 64 / 128 bits, WPA, WPA2
	• Filtering by list of MAC addresses
Range	• Up to 300 m in free space
	• 10 to 100 m inside buildings

Mains Power Supply	
Type	• Plug-in external adapter unit
Class	• II
Input voltage	• 100 to 240 V, 50 Hz / 60 Hz
Power absorbed	• < 9 W
Output voltage	• 12 V
Mains Connection technology	• Europlug type A socket
Use Connection technology	• Cord 2 m + jack diam. 3.5 mm

DC Power Supply Input of router	
Input Voltage	• 11 V - 13 V
Power absorbed	• < 7 W
Connection technology	• Miniature jack fixed connector diam. 3.5 mm

D.3 Environmental characteristics

Climatic and mechanical environment	
Storage	• ETS 300 019-1-1 Category T1.2
Transport	• ETS 300 019-1-2 Category T2.3
Operation	• ETS 300 019-1-3 Category T3.2 Temperature : -5°C / +45°C

Electrical robustness	
Standard	• UIT-T K21 Ed 2000 : basic level

Electromagnetic compatibility	
Transmission	• EN 55022 (January 1999) Class B
Harmonic currents	• EN 61000-3-2
Flicker and fluctuations of voltage	• EN 61000-3-3
Immunity	• EN 55024

Radio part for ISM band at 2.4 GHz	
Transmission 802.11n	• ETR 300 328-2 Ed. Juillet 2000

D.4 Application and protocols

IP characteristics	
TCP-IP, UDP, ICMP, ARP	• Server, Relay
DHCP	• Relay
DNS	
Routing (LAN et WAN)	• Static
NAT / PAT	• RFC 1631
Firewall	• By protocol
	• By IP address
	• By port
	• Statefull / Stateless
IP QoS	• DiffServ

ATM characteristics	
Signalling	• PVC
Adaptation layer	• AAL5
Number of VCI	• 8
Quality of service	• UBR, VBR, nrtVBR, VBRrt, CBR
Signalling	• RFC 2516
self-configuration	• Detection of VPI/VCI
	• Detection of encapsulation
	• Detection of PPPoE / PPPoA
	• Detection of PAP / CHAP

Encapsulation protocols	
PPP over ATM	• RFC 2364
PPP over ETH over ATM	• RFC 2516, RFC 1483/2684
IP over ATM	• RFC 1483/2684
ETH over ATM	• RFC 1483/2684

Configuration	
HTTP	• LAN or WAN port (with specific option)
Management	• From ETH and WAN (with specific option)
Downloading of version	• Client by http mode
CLI	• Telnet
TR69	• Via a ACS server

Annex E - Default configuration

This section covers	• the default username and password	§ E.1
	• the default configuration for the local network (LAN)	§ E.2
	• the default configuration for the local wireless network (WLAN)	§ E.3

This section details the values of the default parameters of your F@ST 4310 when it leaves the factory.

These default parameters can be modified by a particular preconfiguration of your F@ST 4310.

E.1 Default username and password

Username:	admin
Password:	see information given on the router sticker

Note

The **Username** and **Password** can be different according to the ISP (**I**nternet **S**ervice **P**rovider).

E.2 Default configuration for the local network(LAN)

The following table details the values of the principal LAN parameters of your router (**LAN1** to **LAN4**):

LAN characteristics	Value	State
LAN1 IP address	192.168.1.1/24	Internet and HTTP configuration tool access (bridged)
LAN2 IP address		
LAN3 IP address		
LAN4 IP address		
BROADCAST, ARP, MULTICAST	_	Activated
Router	_	The LAN traffic is routed to your ISP
NAT/PAT	_	Activated

E.3 Default configuration for the local wireless network (WLAN)

The following table supplies the principal default WLAN parameters of your router.

Characteristics (Wi-Fi)	Value
IP address	192.168.1.1/24
Enable Wireless	Box checked
SSID	see information given on the router sticker
Channel	Auto
Network Authentication	No

Annex F - Glossary

Glossary.

ACL	**A**ccess **C**onfiguration **L**ist
ACS	**A**uto **C**onfiguration **S**erver
ADSL	**A**synchronous **D**igital **S**ubscriber **L**ine
AP	**A**ccess **P**oint
ARP	**A**ddress **R**esolution **P**rotocol
CC	**C**ontinuity **C**heck
CCK	**C**omplimentary **C**ode **K**eying
CHAP	**C**hallenge **H**andshake **A**uthentication **P**rotocol
CLI	**C**ommand **L**ine **I**nterface
CPE	**C**ustomer **P**remises **E**quipment
CTS	**C**lear **T**o **S**end
DBPSK	**D**emodulator **B**aseband **P**hase **S**hift **K**eying
DHCP	**D**ynamic **H**ost **C**onfiguration **P**rotocol
DNS	**D**omain **N**ame **S**erver
DQPSK	**D**ifferential **Q**uadrature **P**hase **S**hift **K**eying
DSSS	**D**irect **S**equence **S**pread **S**pectrum
DTIM	**D**elivery **T**raffic **I**ndication **M**essage
ESSID	**E**xtended **S**ervice **S**et **ID**entifier
FHSS	**F**requency **H**opping **S**pread **S**pectrum
FTP	**F**ile **T**ransfer **P**rotocol
HTML	**H**yper **T**ext **M**arkup **L**anguage
HTTP	**H**yper **T**ext **T**ransfer **P**rotocol
IAD	**I**ntegrated **A**ccess **D**evice
ICMP	**I**nternet **C**ontrol **M**essage **P**rotocol
IEEE	**I**nstitute of **E**lectrical and **E**lectronics **E**ngineers
IEEE 802.11b/g	Specifications which use the MAC protocol suitable for the wireless local network (WLAN) in the 2.4 GHz band
IEEE 802.11n	IEEE 802.11n-2009 is an amendment to the IEEE 802.11-2007 wireless networking standard. It governs wireless networking transmission methods, commonly used today in its 802.11a, 802.11b, 802.11g and 802.11n versions.
IGMP	**I**nternet **G**roup **M**embership **P**rotocol
IMAP	**I**nternet **M**essage **A**ccess **P**rotocol
IP	**I**nternet **P**rotocol
ISDN	**I**ntegrated **S**ervice **D**igital **N**etwork
ISP	**I**nternet **S**ervice **P**rovider

L2TP	**L**ayer **2** **T**unneling **P**rotocol
LAN	**L**ocal **A**rea **N**etwork
LCP	**L**ink **C**ontrol **P**rotocol
LLC	**L**ogical **L**ink **C**ontrol
MAC	**M**edium **A**ccess **C**ontrol
MDI	**M**edia **D**ependent **I**nterface
MER	**M**AC **E**ncapsulation **R**outing
MTU	**M**aximum **T**ransfer **U**nit
NAPT	**N**etwork **A**ddress **P**ort **T**ranslation
NAT	**N**etwork **A**ddress **T**ranslation
OAM	**O**peration, **A**dministration and **M**aintenance
PAP	**P**assword **A**uthentification **P**rotocol
PCI	**P**eripheral **C**omponent **I**nterconnect
PCM	**P**ulse **C**ode **M**odulation
PCMA	**P**ulse **C**ode **M**odulation Loi **A**
PCMCIA	**P**ersonal **C**omputer **M**emory **C**ard **I**nternational **A**ssociation
PCMU	**P**ulse **C**ode **M**odulation Loi **u**
PID	**P**rotocol **ID**entifier
PING	**P**acket **I**nter**N**et **G**roper
PLC	**P**aquet **L**oss **C**oncealment
POP3	**P**oste **O**ffice **P**rotocol version **3**
POTS	**P**lain **O**ld **T**elephone **S**ervice
PSTN	**P**ublic **S**witching **T**elephonic **N**etwork
PPP	**P**oint to **P**oint **P**rotocol
PPPoE	**PPP o**ver **E**thernet
PVC	**P**ermanent **V**irtual **C**ircuit
QoS	**Q**uality **o**f **S**ervice
RADIUS	**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice
RFC	**R**equest **F**or **C**omments
RNIS	**R**éseau **N**umérique **I**ntégration de **S**ervices
RIP	**R**outing **I**nformation **P**rotocol
RTCP	**R**eal **T**ime **C**ontrol **P**rotocol
RTP	**R**eal-time **T**ransport **P**rotocol
SCR	**S**ustained **C**ell **R**ate
SMTP	**S**imple **M**ail **T**ransfer **P**rotocol

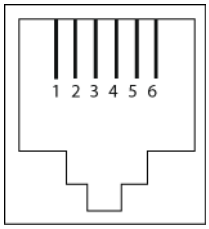
SNDCP	**S**ub **N**etwork **D**ependent **C**onvergence **P**rotocol
SNAP	**S**ub**N**etwork **A**ttachment **P**oint
SNMP	**S**imple **N**etwork **M**anagement **P**rotocol
SOAP	**S**imple **O**bject **A**ccess **P**rotocol
SSID	**S**ervice **S**et **ID**entifier
STB	**S**et **T**op **B**ox
TCP	**T**ransmission **C**ontrol **P**rotocol
TELNET	**TEL**ecommunication **NET**work
TFTP	**T**rivial **F**ile **T**ransfer **P**rotocol
UBR	**U**nspecified **B**it **R**ate
UDP	**U**ser **D**atagram **P**rotocol
UPnP	**U**niversal **P**lug a**n**d **P**lug
URL	**U**niformed **R**esource **L**ocator
UTP	**U**nshielded **T**wisted **P**air
VBR-nrt	**V**ariable **B**it **R**ate - **n**on **r**eal **t**ime
VBR-rt	**V**ariable **B**it **R**ate - **r**eal **t**ime
VC	**V**irtual **C**hannel
VCC	**V**irtual **C**hannel **C**onnection
VCI	**V**irtual **C**hannel **I**dentifier
VC MUX	**VC Mu**ltiple**X**ing (encapsulation without header)
VP	**V**irtual **P**ath
VPI	**V**irtual **P**ath **I**dentifier
VPN	**V**irtual **P**rivate **N**etwork
WAN	**W**ide **A**rea **N**etwork
WEB	Meshed network of information servers
WEP	**W**ired **E**quivalent **P**rivacy
WFQ	**W**eighted **F**air **Q**ueuing
Wi-Fi	**Wi**reless **Fi**delity (wireless network)
WLAN	**W**ireless **L**ocal **A**rea **N**etwork
WPA	**W**ireless **P**rotected **A**ccess

Annex G - Connector Technology

This section covers	• pinouts of the **LINE** connector	§ G.1
	• pinouts of the **PWR** connector	§ G.2
	• pinouts of the **LAN1**, **LAN2**, **LAN3** and **LAN4** connectors	§ G.3

G.1 Pinouts of the LINE connector

The equipment is connected to ADSL using a RJ11 fixed connector (6 pins).



Contact N°	Signal	Meaning
3	LINE-A	Line A signal
4	LINE-B	Line B signal
1	NC	Not connected
2	NC	Not connected
5	NC	Not connected
6	NC	Not connected

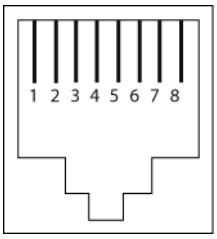
G.2 Pinouts of the PWR connector

The mains unit is connected to the equipment using the miniature fixed connector of the case.

Contact N°	Signal	Meaning
Intérieur	+12 V	Connexion DC "+"
Extérieur	Masse	Connexion DC "-"

G.3 Pinouts of the LAN1, LAN2, LAN3 and LAN4 connectors

The Ethernet interface is connected to the equipment using a RJ45 fixed connector (8 pins).



Contact No	Signal	Meaning
1	TXD+	(+) Emission to terminal
2	TXD-	(-) Emission to terminal
3	RXD+	(+) Reception of terminal
4	NC	Not connected
5	NC	Not connected
6	RXD-	(-) Reception of terminal
7	NC	Not connected
8	NC	Not connected

Note

The Ethernet port is self-detecting. You can use either straight or crossed cables. An emission or reception signal is detected automatically.

Sagemcom

Sagemcom Broadband SAS
Headquarters: 250, route de l'Empereur
92848 Rueil-Malmaison Cedex - FRANCE
Tel : +33 (0)1 57 61 10 00 - Fax : +33 (0)1 57 61 10 01
www.sagemcom.com

14/11/14