SAGEM F@st™ 2604
SAGEM F@st™ 2644

Reference Manual

253 080 888-A

Edition of May 2008

SAGEM

Sagem Communications 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:

- **SAGEM F@st™** is a registered brand of **Sagem Communications**.
- **Windows™** and **Internet Explorer™** are registered brands 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: admin).

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 SAGEM F@st™ 2604 and SAGEM F@st™ 2644 equipment.

Guide to symbols used in this manual

Warns you not to do an action, or commit a serious omission.

Gives you important information which you must take into account

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 SAGEM F@st™ 2604 and 2644 equipment
Section 2	Description of SAGEM F@st™ 2604 and 2644 equipment
Section 3	Installation of SAGEM F@st™ 2604/2644 equipment
Section 4	Configuration of network parameters
Section 5	Configuration of the router by HTTP
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	CE compliance declaration
Annex C	Environment
Annex D	Technical Characteristics
Annex E	Default configuration
Annex F	Glossary
Annex G	Connection technology

Contents

List of figures

1. Introduction

This section covers	➢ presentation of the SAGEM F@st™ 2604 and SAGEM F@st™ 2604 ranges	§ 1.1
	➢ composition of the packaging	§ 1.2
	➢ required hardware and software	§ 1.3

1.1 Presentation

This reference manual is dedicated to the SAGEM F@st™ 2604 and SAGEM F@st™ 2644 product ranges. These products are routers which give users, broadband Internet access from their computer or their games console by various Ethernet (10 or 100 BASE-T) or Wi-Fi (IEEE 802.11g) 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 lets you telephone over the Internet from an IP SIP telephone linked by Wi-Fi to your router.

SAGEM F@st™ 2604 and SAGEM F@st™ 2644 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).

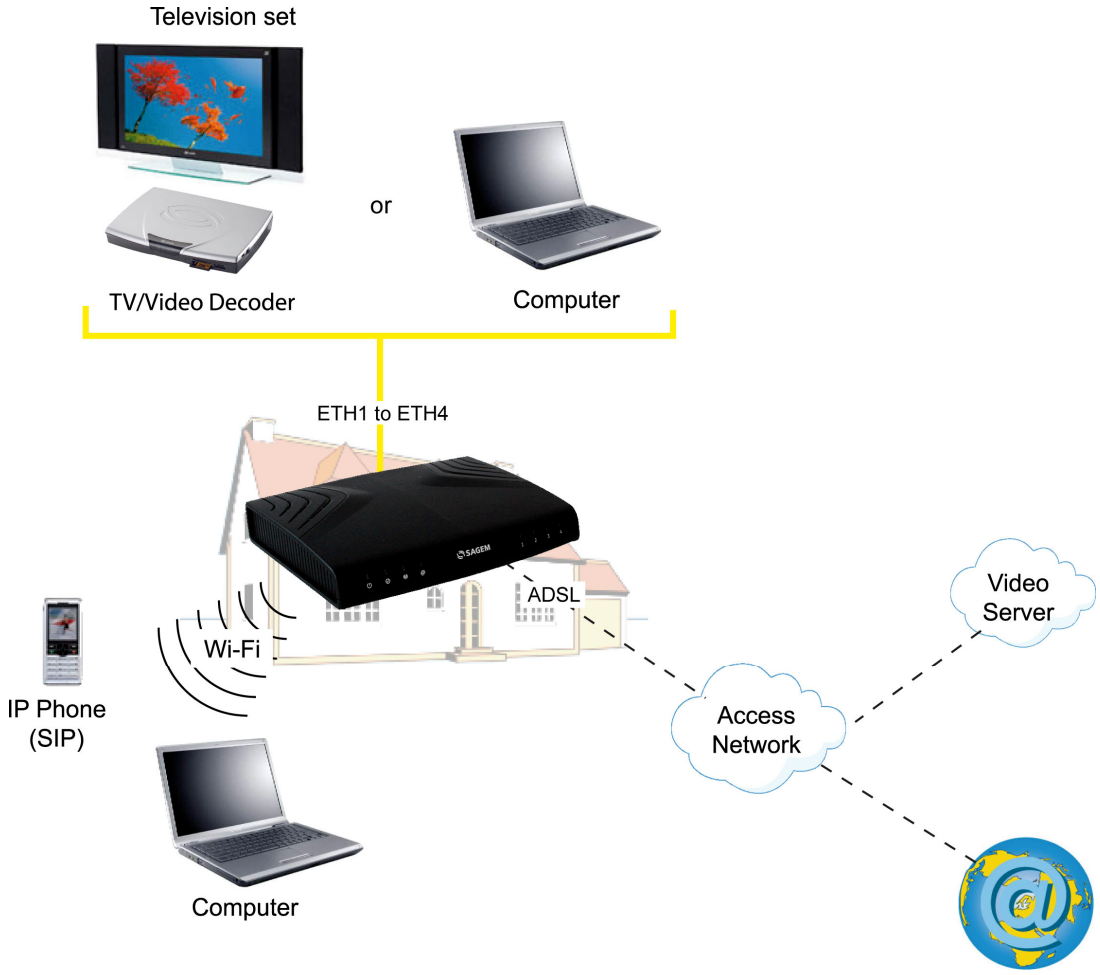


Figure 1.1 - Supervising your router

Its principal characteristics and functions are as follows:

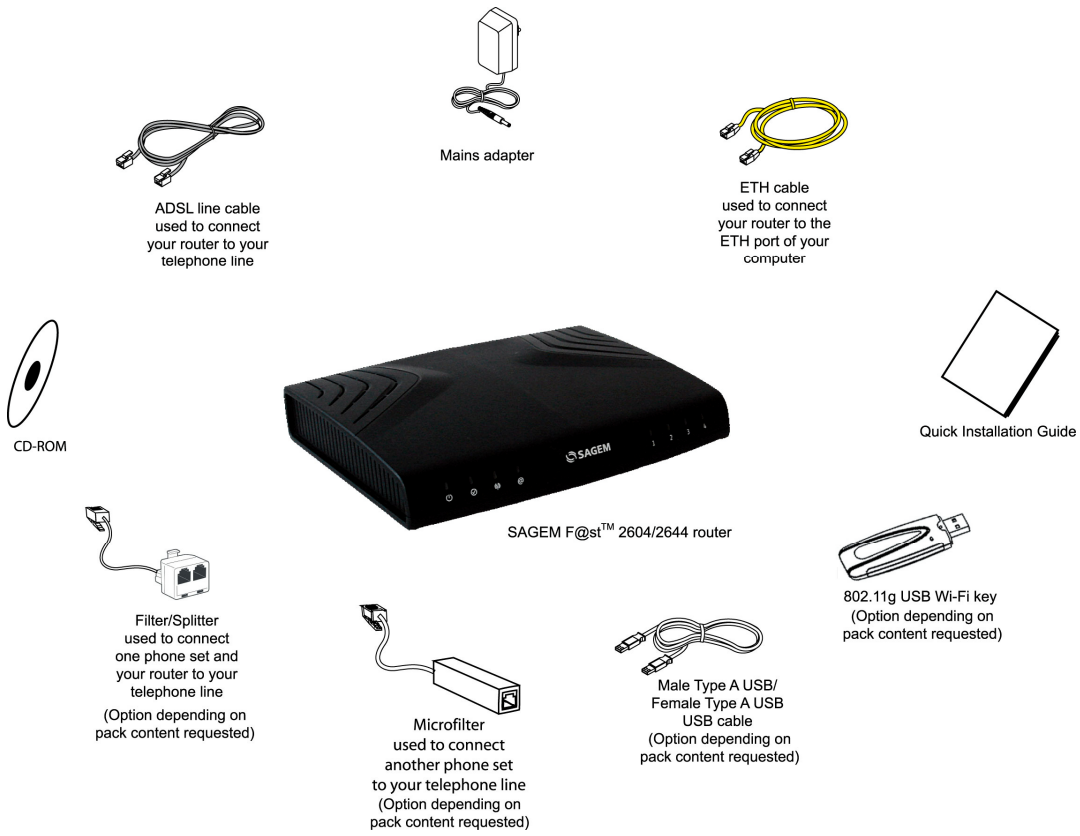
- High-performance secure Bridge/Router with ADSL/ADSL2/ADSL2+ interface,
- User access:
  - 4 x 10/100BT Ethernet ports,
  - 1 Wi-Fi port (802.11b/g) by mini-PCI,
- DHCP Client/Server/Relay,
- DNS Server/ Relay,
- Access control (FTP/TELNET/HTTP/SSH Client),
- NAT/PAT router - FTP Compatibility, IRC, 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 is supplied in a pack the composition of which changes according to the equipment (SAGEM F@st™ 2604 and SAGEM F@st™ 2644):

As an example, please find below the "pack" chosen for the SAGEM F@st™ 2604 router, i.e.:

- 1 SAGEM F@st™ 2604,
- 1 mains adapter unit,
- 1 Gray ADSL RJ11/RJ11 FDT line cord (length = 3 m),
- 1 Yellow Ethernet RJ45/RJ45 linking cord (length = 1.75 m),
- 1 Quick Installation Guide,
- 1 Installation CD-ROM,
- 1 USB Wi-Fi key (optional),
- 1 USB Type A male/Type A female cable (length = 1.5 m) (optional),
- microfilter(s) (optional),
- 1 filter/splitter (optional).



The CD ROM contains:

- the application for installing the USB interface.
- the Reference Manual (SAGEM F@st™ 2604 and SAGEM F@st™ 2644) in PDF format file.
- the CE declaration of the chosen router.

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 802.11b/g interface,

  or
  - an Ethernet interface (10BASE-T or 10/100BASE-T).
- a WEB browser (Internet Explorer version 5 or higher recommended).

The minimum configuration of your computer must be:

- for Windows: Pentium II, 400 MHz, RAM: 128 MB,
- for MacOS: Power PC G3, 233 MHz, RAM: 128 MB,
- a monitor of minimum resolution: 1024 x 768.

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

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 instructions	§ 2.4

2.1 Description

Figure 2.1 gives an overview of a router (SAGEM F@st™ 2604 or SAGEM F@st™ 2644).

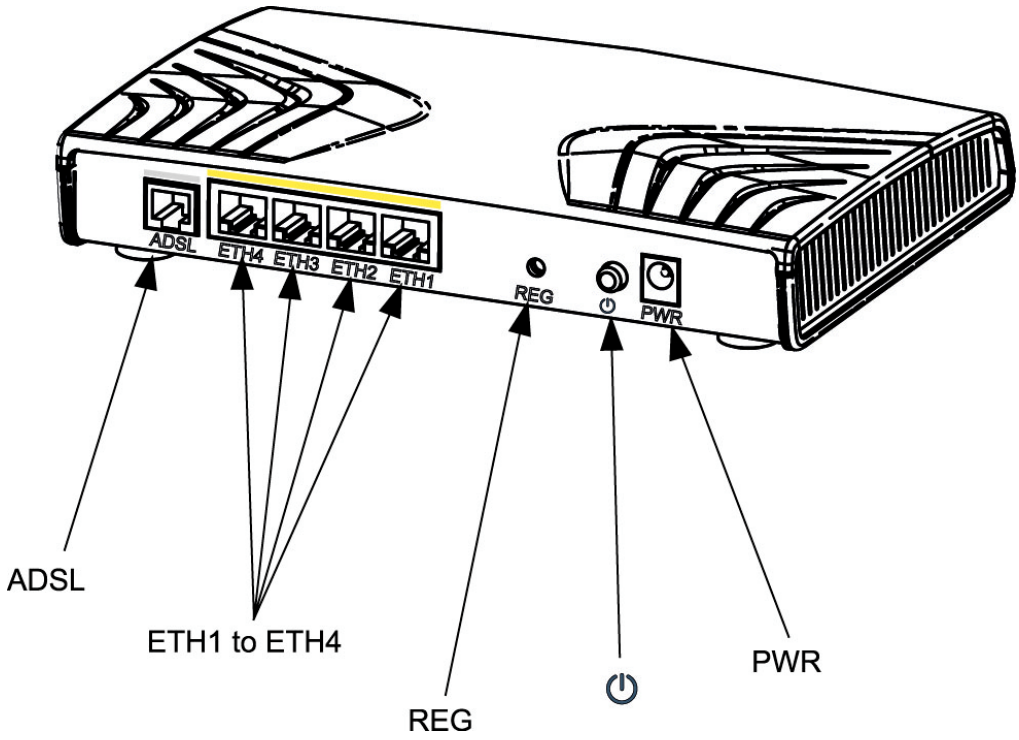
Figure 2.1 - Overview of case

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

The components of the base different according to the equipment (SAGEM F@st™ 2604 or SAGEM F@st™ 2644)(see § 2.1.1)
The front face of the lid has eight display LEDs (see § 2.1.2).
The base has the LED ideograms, SAGEM's logo or the operator's logo.

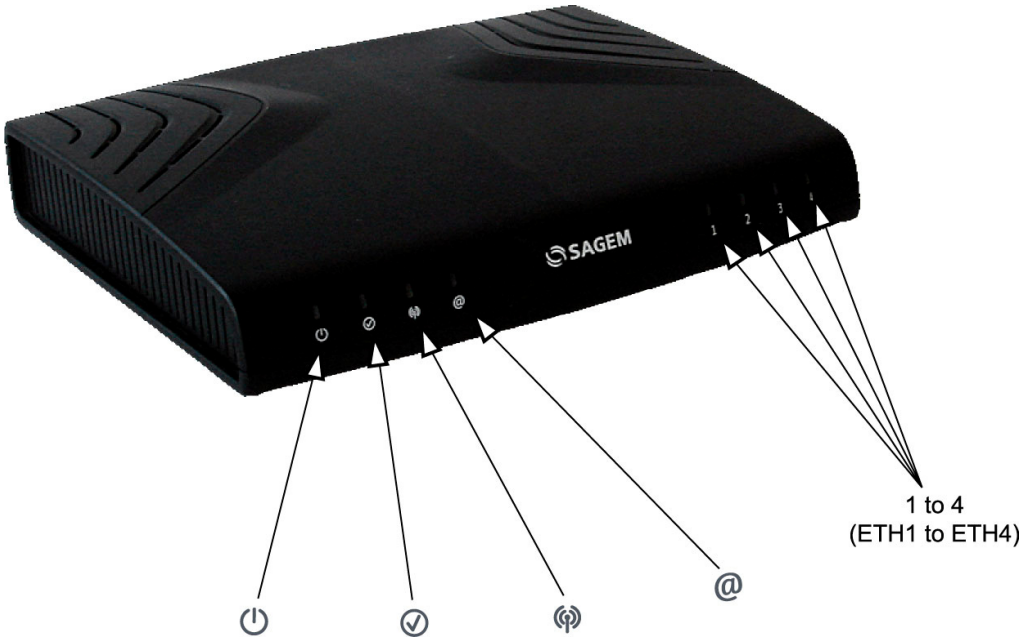
Below the base is a label on which the product's identification code, series number and barcode are shown.

2.1.1 Connectors



Marking	Meaning
ADSL	RJ11 connector - 6 pts. This connector is identified by a grey line on the base (SAGEM F@st™ 2604/2644). It is used for the connection to an ADSL line (WAN interface).
ETH1 to ETH4	RJ45 connectors - 8 pts (10/100BASE-T Ethernet Interface). These connectors are identified by a yellow line on the base. They are used to connect to a computer or a television set (via a TV/Video Decoder).
REG	This button allows the router to be reset to the factory configuration (see § A.7). **Note:** It is reset relative to the other elements to prevent an accidental loss of configuration.
⏻	On/Off switch.
PWR	Miniature jack fixed connector. This connector enables the router to be supplied with direct current from a mains adapter unit.

2.1.2 LEDs



The different LEDs of the figure above are described in the following table:

Status	Colour	⏻	✓	Wi-Fi	@
Lit steady	Green	Power On	ADSL Up	Wi-Fi activated	A PPP session has been created
	Amber	x	x	x	ADSL link is established
Flickering	Green	x	x	Wi-Fi Tx/Rx	Tx/Rx traffic
Blinking	Amber	x	x	x	ADS is training
Slow Blinking	Green	x	Line not detected	Wi-Fi pairing	x
Fast Blinking	Green	x	ADSL synchronisation training	x	x
Off	Green	Power Off		Wi-Fi deactivated	Power Off or Bridge mode or ADSL down

Status	Colour	1	2	3	4
Lit on steady	**Green**	Ethernet port (ETH1, ETH2, ETH3 or ETH4) has detected a link with 100 Mbps device			
Flickering		Tx/Rx traffic at 100 Mbps			
Lit on steady	**Amber**	Ethernet port (ETH1, ETH2, ETH3 or ETH4) has detected a link with 10 Mbps device			
Flickering		Tx/Rx traffic at 10 Mbit/s			
Off	x	No link detected on the Ethernet port			

2.2 Connecting the ports of your router

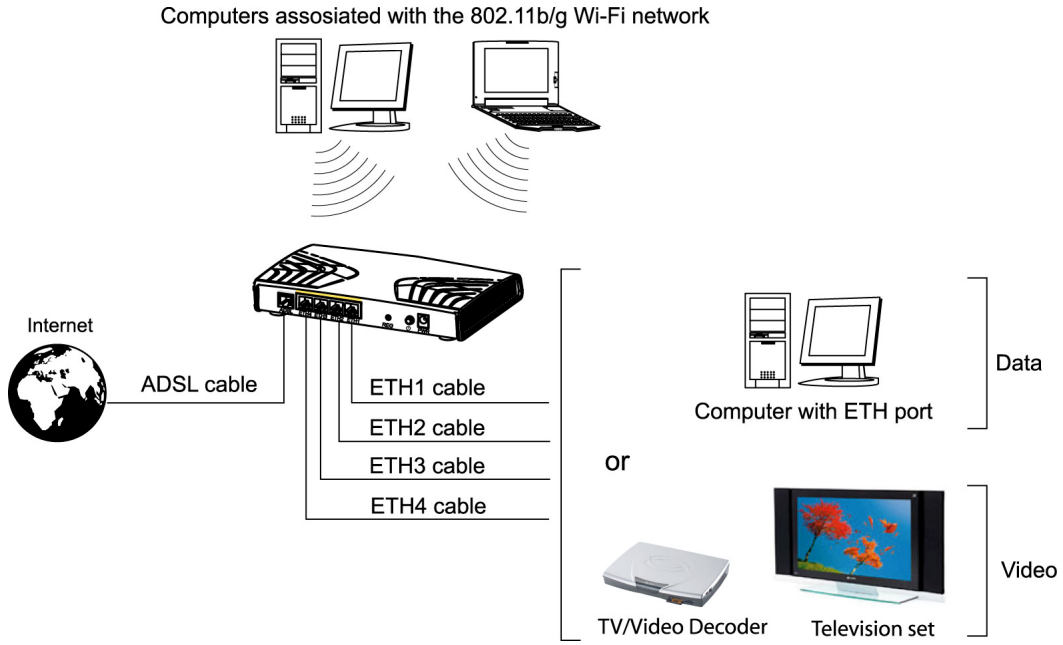


Figure 2.2 - Interconnection of ports of SAGEM F@st™ 2604 et 2644

2.3 Installing your SAGEM F@st™ 2604/2644

2.3.1 Powering up

- First connect the end of the mains adapter lead, supplied with the equipment, to the PWR socket on your Residential Gateway,
- Connect the adapter to a nearby power outlet,
- Switching on,
- 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 should be steady and turn from "**Red**" to "**Green**" when a PPP session has been created.

Ces dernières

Note: It lasts around one minute.

2.3.2 Connecting the ADSL cable

- Connect one end of the RJ11/RJ11 cable supplied with the equipment to the **ADSL** socket of your Residential Gateway.
- Connect the other end of this cable as shown in the Figure 2.3.

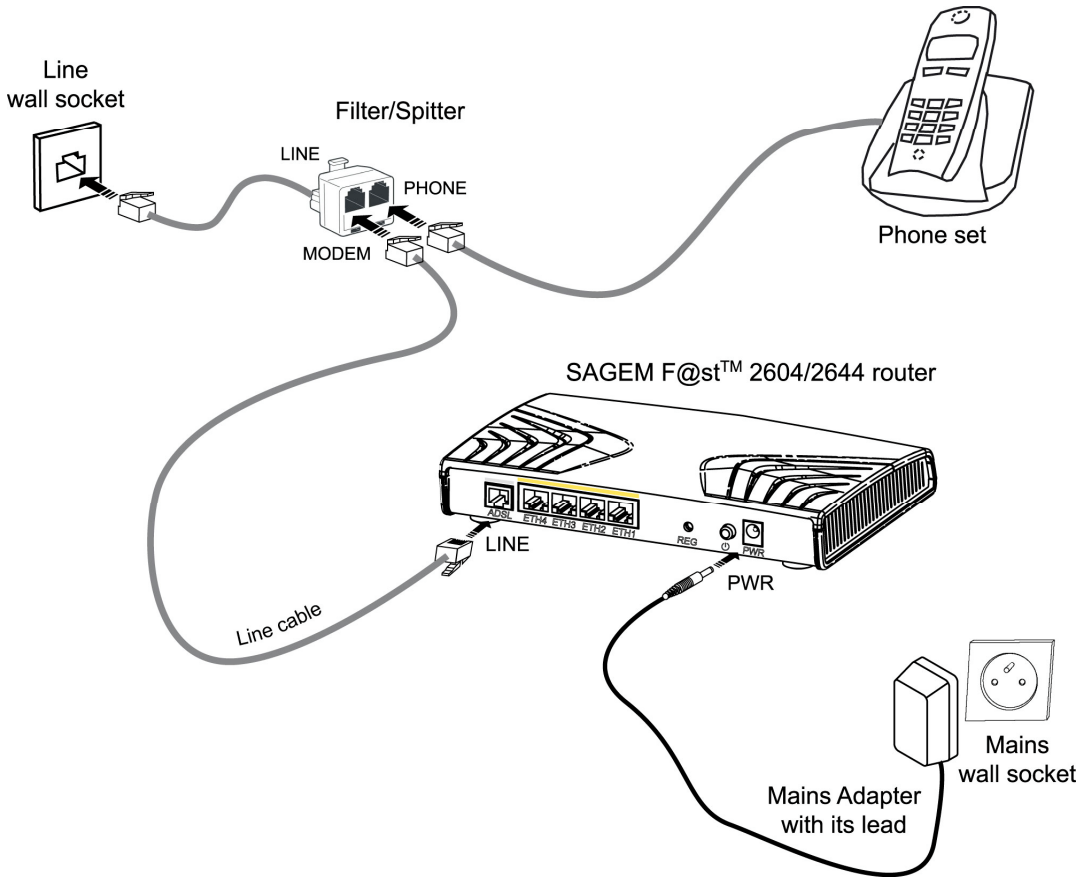


Figure 2.3 - ADSL line / Power Supply Connection

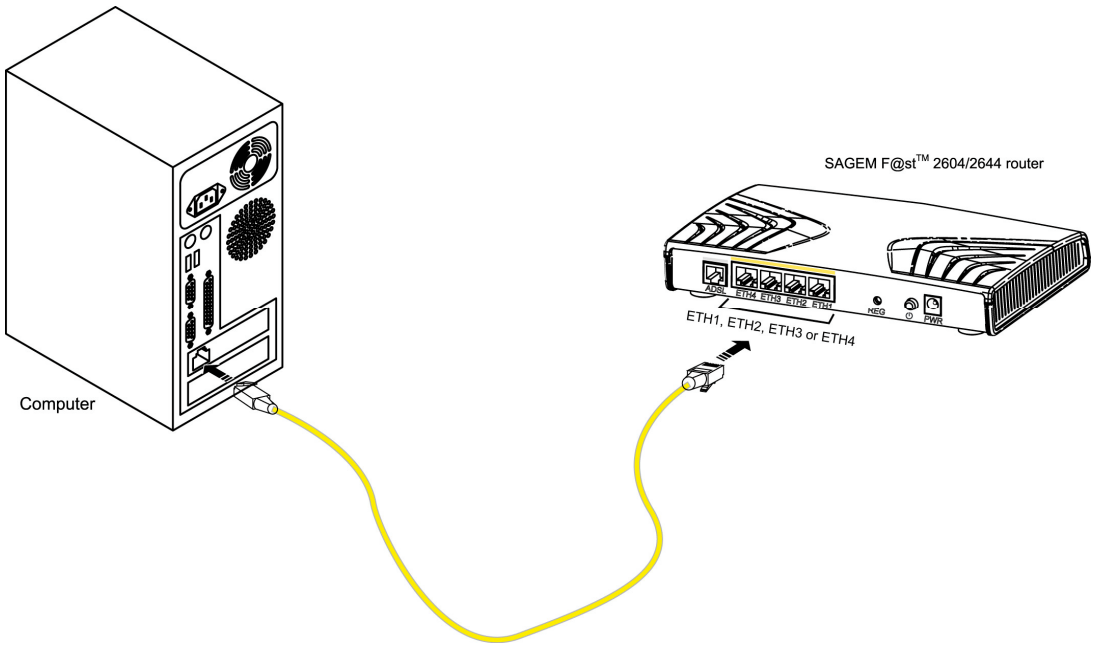
2.3.3 Connecting to your computer

Two connections may need to 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

- Connect the end of the yellow Ethernet cable (RJ45/RJ45) supplied in the pack to the Ethernet fixed connector (marked **ETH1**, **ETH2**, **ETH3** or **ETH4**) in the case of the SAGEM F@st™ 2604 and SAGEM F@st™ 2644) of your router,
- 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:

- 1 Wi-Fi 188470912 key (Dongle) in an anti-static plastic bag,
- 1 USB adapter cord for Dongle,
- 1 CD-ROM.

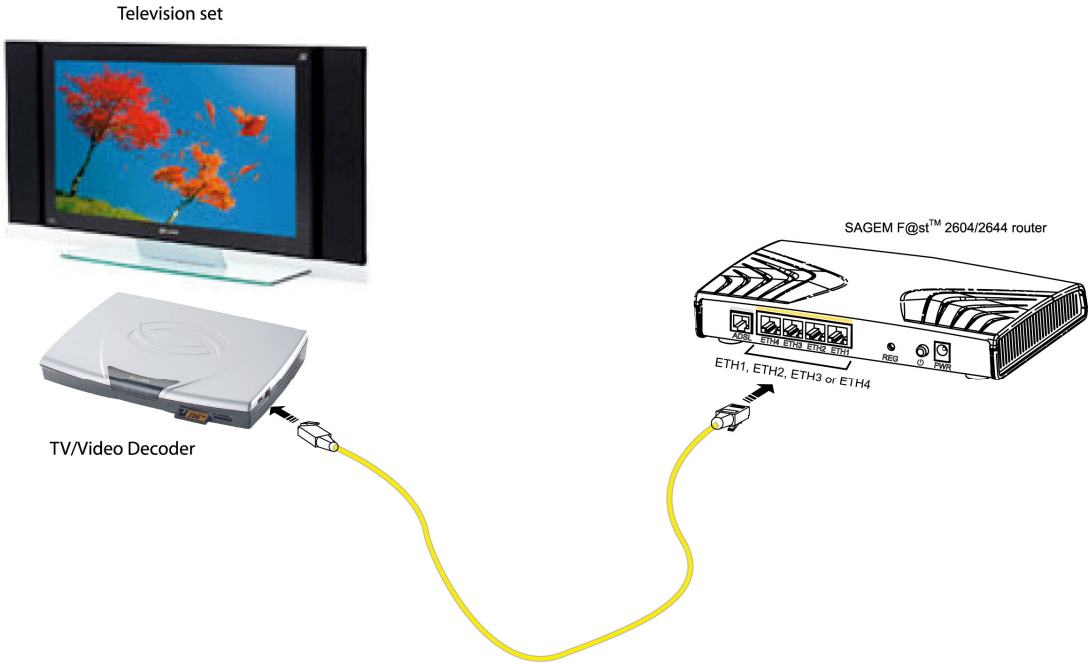
Inserting a USB Wi-Fi key in your computer

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

You can also use the wifi adapter incorporated in your computer.

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

- Connect the end of the yellow Ethernet cable (RJ45/RJ45) supplied in the pack to the Ethernet fixed connector (marked **ETH1**, **ETH2**, **ETH3** or **ETH4**) of your router.
- Connect the other end of the cable to a TV decoder.



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

2.4 Installation instructions

Environment

- The router must be installed and used inside a building.
- The ambient temperature must not exceed 45°C.
- The router must not be exposed to direct strong sunlight nor to an intense heat source.
- The router must not be placed in an environment subject to vapour condensation.
- The router must not be exposed to water projections.
- The router unit must not be covered.

Power source

- Use a network socket with easy access, which is close to the equipment. The power cord is 2 m in length.
- Arrange the power cord so as to prevent any accidental cutoff of the router.
- The router is designed to be connected to a TT or TN type power network.
- The router is not designed to be connected to an electrical installation with an IT type diagram (neutral connected to earth through an impedance).
- Protection against short circuits and inter-phase leakages, neutral and earth must be ensured by the building's electrical installation. The power circuit of this equipment must be fitted with a 16 A protection against power surges, and with a differential protection.

Maintenance

- It is prohibited to open the case. Only qualified personnel approved by your supplier may do so.
- Do not use liquid or spray cleaning agents.

3. Installing and configuring the SAGEM F@st™ 2604/2644 router

For the installation of the SAGEM F@st™ 2604/2644,
please refer to the Quick Installation Guide of this product

4. Configuration of network parameters

This section covers	➢ configuring as a DHCP client	Page 4-3
	➢ reading status of the DHCP server	Page 4-4
	➢ reading data of the DHCP client	Page 4-5

The aim of this section is:

1) to configure your computer so that it is able to communicate with your router.

2) and 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.

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

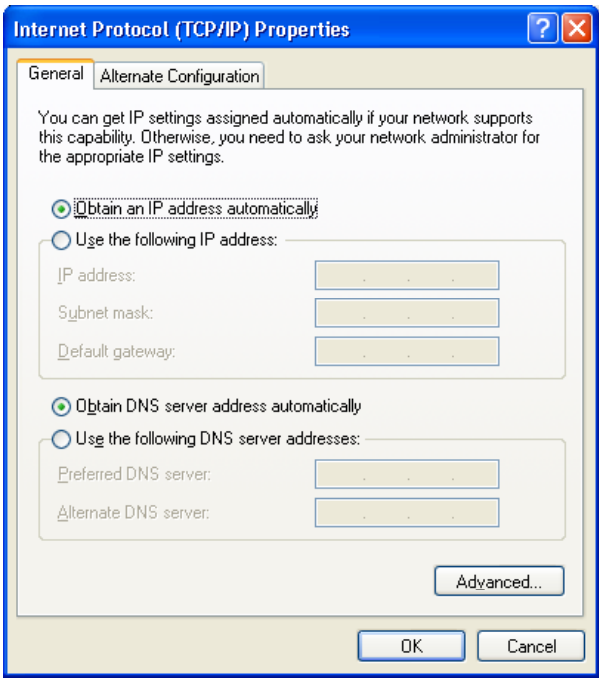
It is imperative that your computer is configured as a DHCP client or that it has a fixed IP address in the configuration range defined by the DHCP server.

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

1) Configuring as a DHCP client

In Windows XP

- click Start/Control Panel/Network Connections.
- right-click the appropriate network, and then select Properties; the Local Area Connection Properties appears.
- select the protocol TCP/IP of the network card, and then click the Properties button; the screen Internet Protocol (TCP/IP) Properties appears.
- select the general tab, then the case "Obtain an IP address automatically" and the case "Obtain the addresses of the DNS servers automatically".
- click the OK button to confirm your choice.



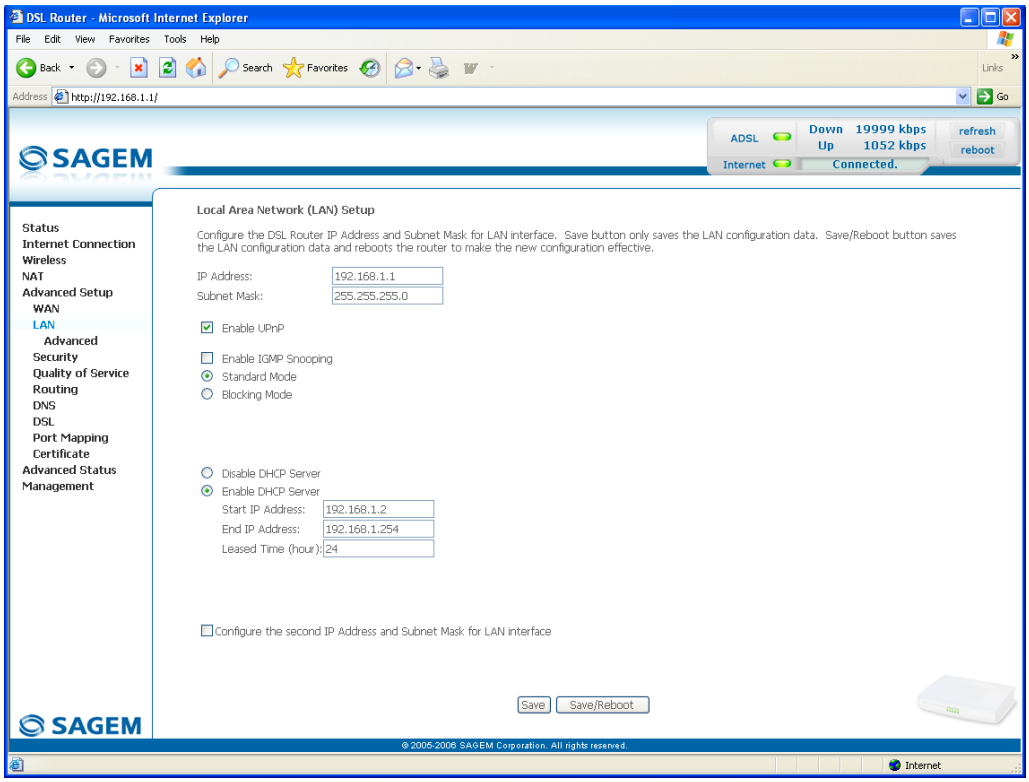
2) Status of the DHCP server

To obtain this status:

- Open your browser and then enter **http://myrouter** or **http://192.168.1.1** (default IP address of your Residential Gateway) to access the welcome screen,
- Enter "**admin**" in the "User Name" field (see note).
- Enter "**admin**" in the "Password" field (see note).
- Then click on the "**OK**" button to validate.

Note: This value depends on the level of security. The ISP gives users this one.

- Click the "**LAN**" menu of the heading **Advanced Setup**; the following screen appears:



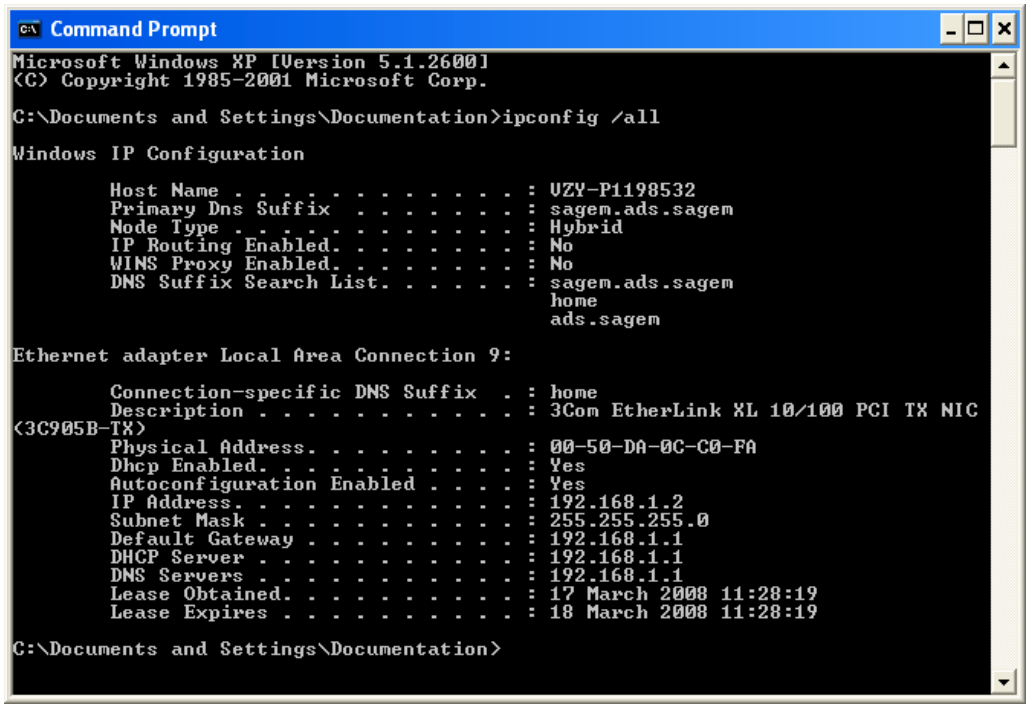
Field	Meaning	Display
IP Address	Displays the sub-network address	192.168.1.1
Subnet Mask	Displays the sub-network mask of the IP network.	255.255.255.0
Start IP Address	Displays the first address attributed by the DHCP server. **Note :** This IP address must belong to the same sub-network as that of 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 for obtaining (in hours) an IP address for a terminal.	24

3) Data of the DHCP client

To obtain this data:

In Windows XP, 2000 and Me

- Click the **Start** button, select **Execute**, enter **cmd** and then click **OK**; the command prompt screen appears. Enter **ipconfig /all** (or **ipconfig/all**) then confirm by pressing **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 "**Status**" section	§ 5.5
	➢ The "**Internet Connection**" section	§ 5.6
	➢ The "**Wireless**" section	§ 5.7
	➢ The "**NAT**" section	§ 5.8
	➢ The "**Advanced Setup**" section	§ 5.9
	➢ The "**Advanced Status**" section	§ 5.10
	➢ The "**Management**" section	§ 5.11

5.1 Accessing the welcome screen

To access this screen, you must have configured one of your computer's interfaces using the installation CD-ROM provided with your router:

- SAGEM F@st™ 2604/2644 see chapter 3.

If you are using your computer's Ethernet card to configure your router, connect it to an Ethernet port (ETH1 to ETH4)).

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

The router's DHCP server function is activated by default with an address range defined as indicated in subsection.5.9.2.

To access the configurer, proceed as follows:

1 In the **Start** menu, select **All Programs** / **SAGEM F@st 2604**, then left click on Configuration .

2 The following screen asks you to connect.

Enter **admin** by default in the "Username" field.

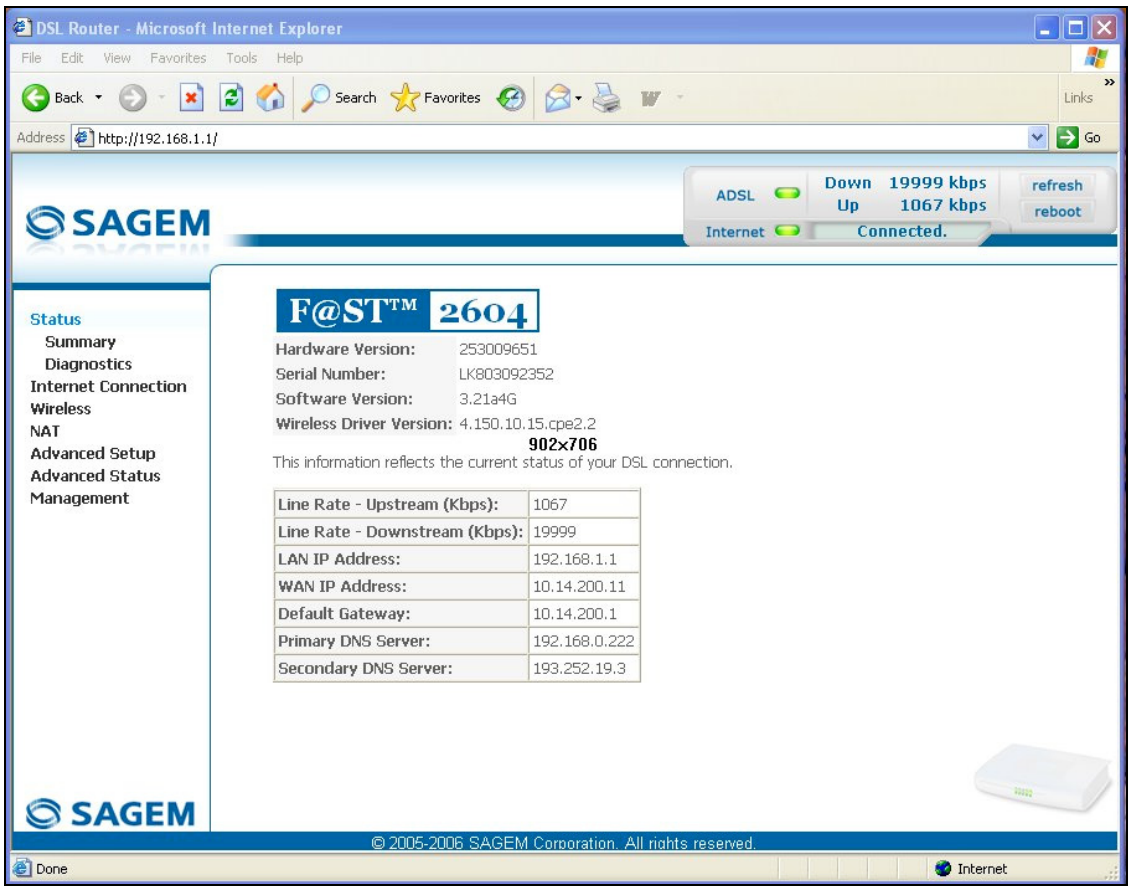
Enter **admin** by default in the "Password" field.

Then click on **OK** to confirm.

Note: The equipment's IP address (192.168.1.1) appears in the bar at the top of the screen.

3 Your computer's Web browser opens and displays the router's welcome screen. The equipment's name is displayed in title (SAGEM F@st™ 2604 or SAGEM F@st™ 2644).

Equipment configuration sections appear in the left hand side of the welcome screen.



This screen displays:

- ☞ in the centre, an area which shows the current ADSL connection status (see subsection 5.3).
- ☞ in the top right, a display box which lets you know the status of the ADSL line, lets you refresh the window displayed and restart your router at any time (see subsection 5.4).
- ☞ to the left, a list of 7 sections (see subsection 5.5 to 5.11) made up of menus and sub-menus. These let you view and configure your router's parameters.

You can modify the password to access your router's configurer 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.

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.
Save/Apply	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 **Save/Apply** 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 5.5.1 - **Status/Summary**.

5.4 Display frame

This supervision box is displayed permanently at the top right of each HTTP configurer window.

The objects it contains are explained below.

LEDs

ADSL	**Green**	Synchronised ADSL line	
	Yellow	ADSL line synchronising	
	Red	ADSL line not connected	
Internet	**Green**	**Connected**	Public address (WAN) distributed to the router.
	Yellow	**Waiting for ISP**	ADSL line synchronising or public address (WAN) not distributed to the router
	Off	**ADSL Down**	Public address (WAN) not distributed to the router, or ADSL line not synchronised.
		Not configured	No VC (Virtual Channel) configured
		Router Rebooting	Router restarted
	Red	**Access denied**	Wrong Login and/or Password

Transmission rates

Down	Displays the nominal down line transmission rate
Up	Displays the nominal up line transmission rate

Buttons

refresh	Allows data displayed on the screen to be refreshed
reboot	Allows your router to be started

5.5 Status

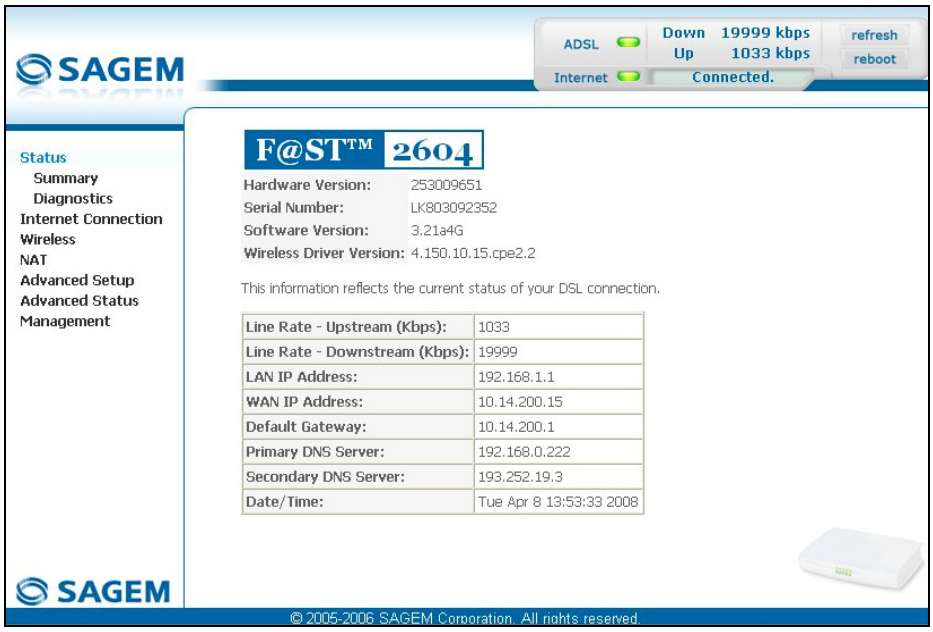
Clicking on this heading displays the following menus:

- Summary (see subsection 5.5.1),
- Diagnostics (see subsection 5.5.2).

5.5.1 Summary

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

- Select the **Summary** menu in the **Status** section; the following screen opens:



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
Software Version	Software version currently installed.
Line Rate - Upstream (kbps)	Nominal up line rate
Line Rate - Downstream (kbps)	Nominal down line rate
LAN IP Address	Local network IP address (LAN)
WAN IP Address	Remote network IP address (WAN)
Default Gateway	Default gateway address
Primary DNS Server	Primary DNS server address
Secondary DNS Server	Secondary DNS server address
Date / Time	Date and Time (see Note)

Note: This field only appears if the "**Automatically synchronize with Internet time servers**" box is checked in the "**Management / Internet Time**" menu (see subsection 5.11.5).

5.5.2 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".

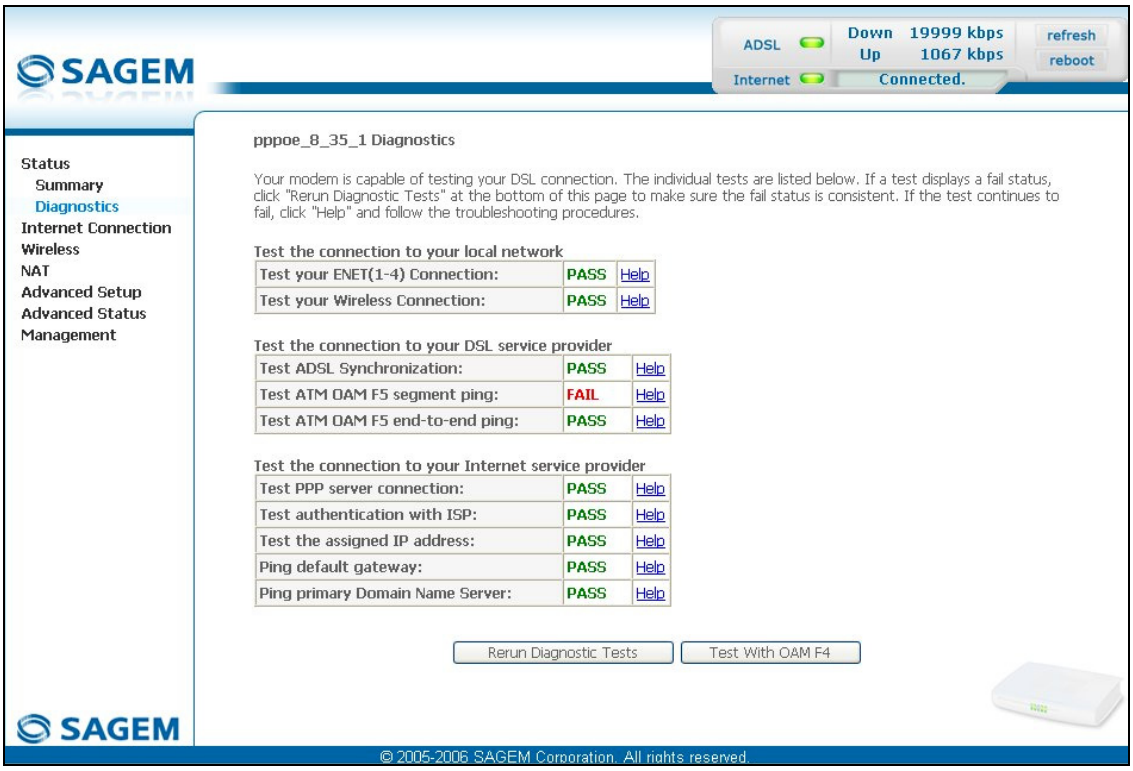
A hypertext link (help) enables the user to access context-related help. This help gives an explanation concerning the state of the connection (**PASS** in green, **DOWN** in orange and **FAIL** in red) and supplies the appropriate troubleshooting procedures.

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

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

If a test displays a "FAIL" status, click on "Help" and then the button "Rerun Diagnostic Tests" at the bottom of the "Help" page, to check that the test has been conclusive. If the test still displays "FAIL", you must follow the troubleshooting procedure displayed on this page.

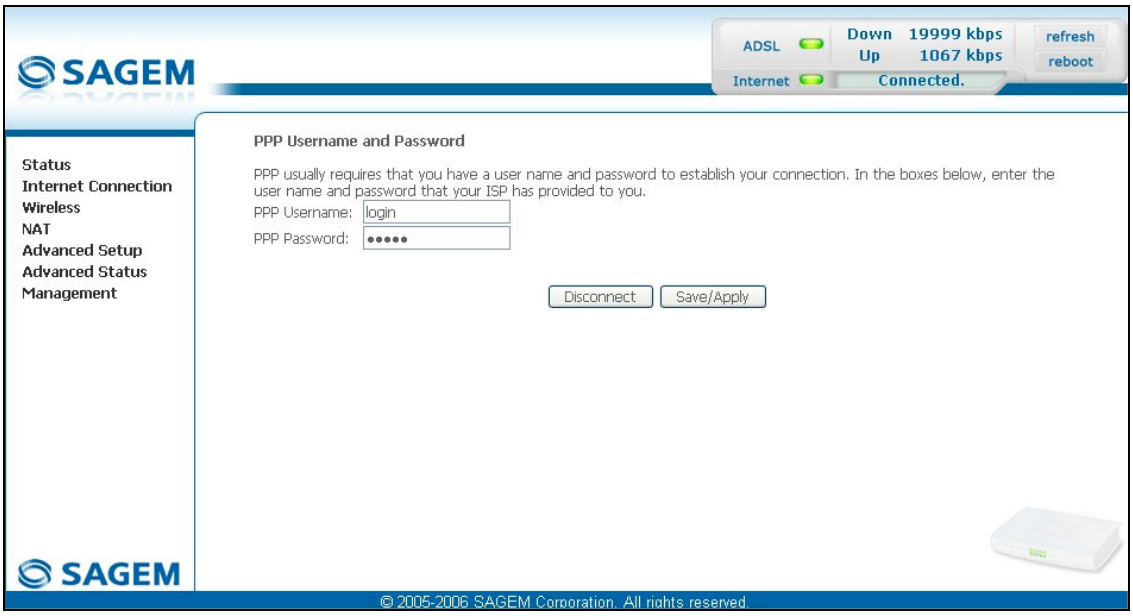
- Select the **Diagnostics** menu in the **Status** section; the following screen opens:



5.6 Internet Connection

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

- Select the **Internet Connection** heading to display the following connection configuration screen:



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

If the message "**There is no ppp connection**" appears, this means that the remote network (WAN) parameters have not been filled in (see subsection 5.9.1 - Advanced Setup / WAN).

Disconnect

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

- Internet access is no longer possible.
- In the supervision box, indicator "Internet" passes from the green to the yellow and the text "Connected" is replaced by "Waiting for ISP".
- On the front panel, the indicator @ goes out.

5.7 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 five menus:

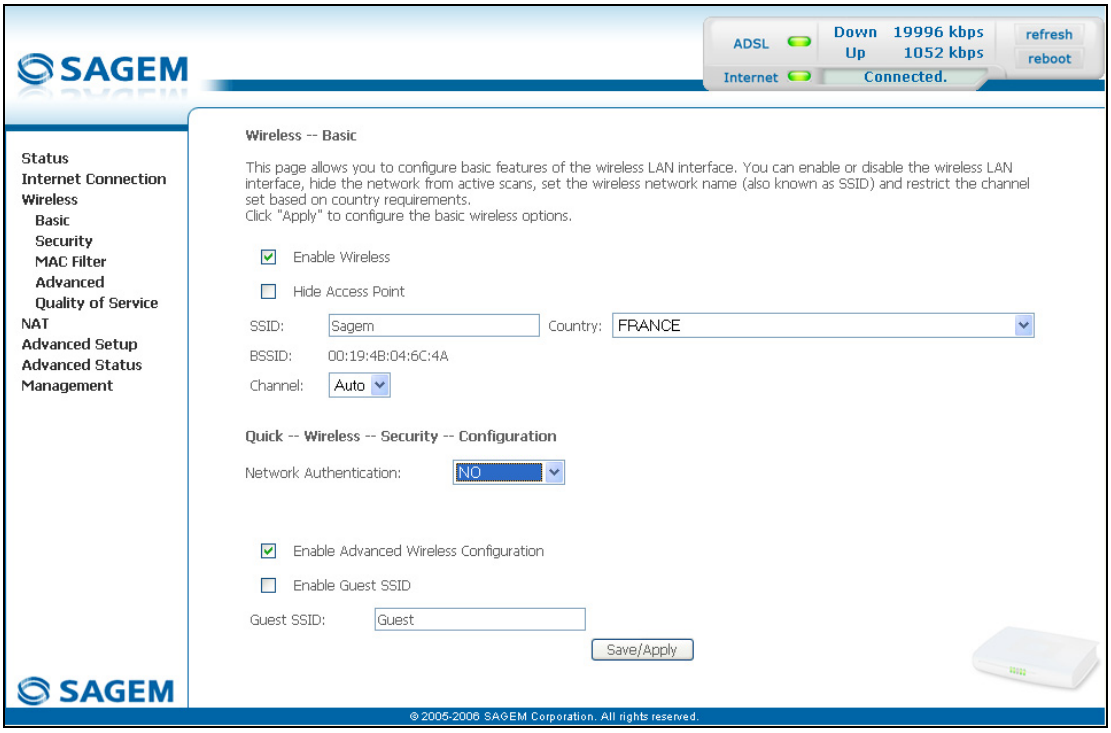
- Basic (see subsection 5.7.1),
- Security (see subsection 5.7.2),
- MAC Filter (see subsection 5.7.3),
- Advanced (see subsection 5.7.4),
- Quality of Service (see subsection 5.7.5).

The **Security**, **MAC Filter**, **Advanced** and **Quality of Service** menus are used to configure the advanced parameters in the **Wireless** section. These menus are only displayed if, in the **Basic** menu, the "**Enable Advanced Wireless Configuration**" box is checked (not checked by default).

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

5.7.1 Basic

- Select the **Basic** menu in the **Wireless** section to display the following wireless network configuration screen:



5.7.1.1 Wireless - Basic

Field	Action/Meaning	Default:
Enable Wireless	Check the appropriate 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.	**Box checked**
Hide Access Point	Check the appropriate box to mask the broadcast of the SSID and prevent any Wi-Fi connection 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).	**Box not checked**
SSID	Enter your router's SSID. **Note:** This is indicated on the label stuck to the box.	**Sagem**
Country	Select the country of your choice from the scroll down list.	**FRANCE**
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. **Non modifiable**	**–**
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. You will find an identical "Channel" field in the "Advanced" menu of this same section. Any modifications are carried over from one field to another. Conform to the CE Declaration of conformity / Radio rules list in appendix B to paragraph B.2.	**Auto**

5.7.1.2 Quick Wireless - Security - Configuration

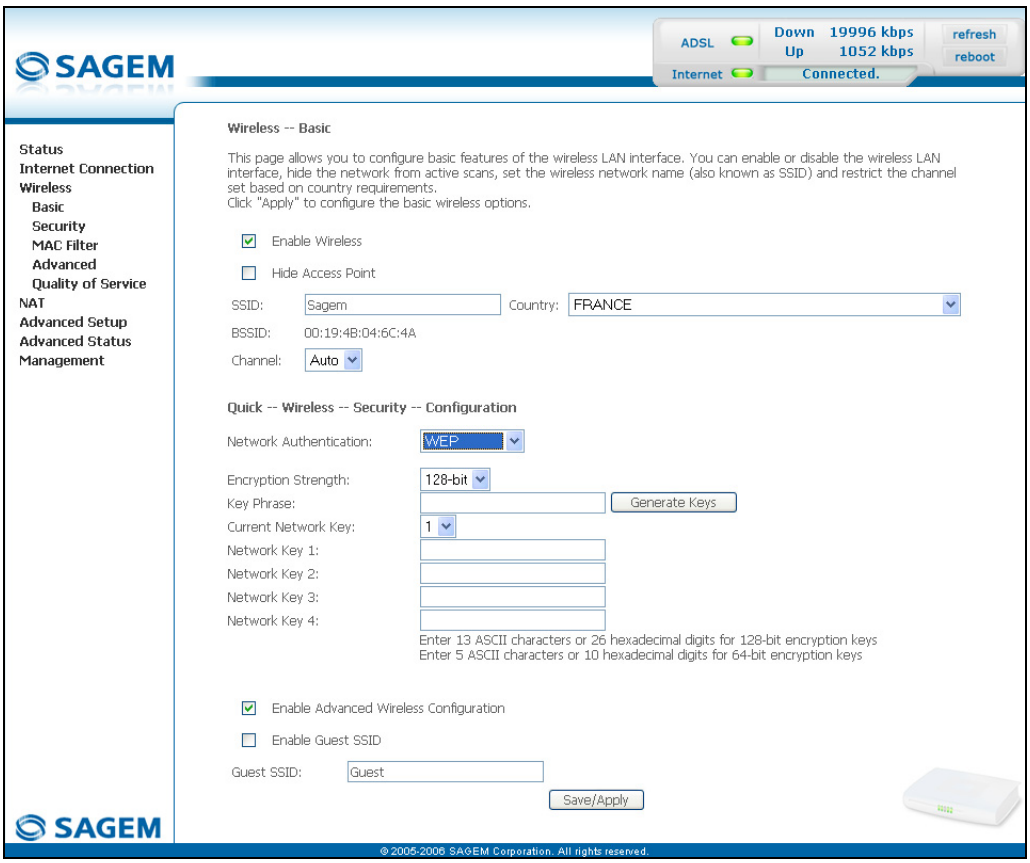
Field	Action/Meaning	Default:
Network Authentication	From the scroll down list, select the security adapted to your router's wireless network. The list suggests the following choices: • **NO** : There is no protection for the wireless network, • **WEP** : Activation of WEP (**W**ired **E**quivalent **P**rivacy) encryption • **WPA-PSK** : Activation of the WPA (**W**ireless **P**rotected **A**ccess) • **WPA2-PSK** : Activation of the WPA2 (**W**ireless **P**rotected **A**ccess) • **Other** (see subsection 5.7.2.1).	**NO**

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.

WEP

- Select the "WEP" encryption mode from the scroll down list; the following screen appears:



Field	Action/Meaning	Default:
Encryption Strength	Select **64-bit** or **128-bit** for an encryption at 64 bits or 128 bits respectively.	**128-bit**
Key phrase	Enter a phrase that consists of up to 15 alphanumeric characters then click the **Generate Keys** button.	**Empty**
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".	**Empty**

Store the key phrase and the keys in a safe location.

Do not write them in a file on your computer.

You may automatically generate encryption keys or manually enter the keys.

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.

WPA-PSK

See subsection 5.7.2.1 - WPA-PSK

WPA2-PSK

See subsection 5.7.2.1 - WPA2-PSK

Other

See subsection 5.7.2.1.

Advanced Wireless

Field	Meaning	Default
Enable advanced Wireless Configuration	**Check the appropriate box to be able to display the Security**, **MAC Filter**, **Advanced** and **Quality of Service menus in the "Wireless" section.** **Note:** If you check this box, the "Enable Guest SSID" and "Guest SSID" fields appear.	**Box not checked**
Enable Guest SSID	Check the appropriate box to activate the "Guest SSID".	**Box not checked**
Guest SSID	Enter a name for the "Guest SSID".	**Guest**

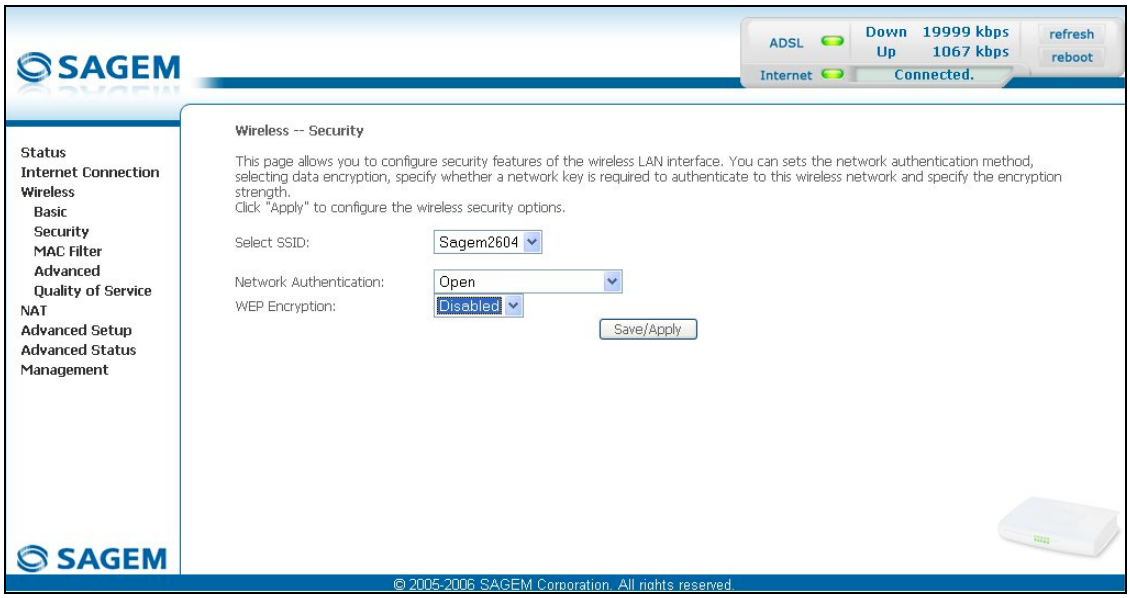
5.7.2 Security

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. Among these, two are commonly used:

- WEP (**W**ired **E**quivalent **P**rotocol),
- WPA (**W**i-Fi **P**rotected **A**ccess) 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.

- Select the **Security** menu in the **Wireless** section to display the following screen:



Field	Meaning	Default
Select SSID	Select the "SSID" of your choice from the scroll down list (sagem or Guest).	**sagem**
Network Authentication	From the scroll down list, select the security adapted to your router's wireless network. The list suggests the following choices: • **Open** : There is no protection for the wireless network (Open System). • **Shared** : • **802.1x** : Activation of the 802.1x standard, • **WPA** : Activation of **WPA** (**W**ireless **P**rotected **A**ccess), • **WPA-PSK** : Activation of **WPA-PSK**, • **WPA2** : Activation of **WPA2**, • **WPA2-PSK** : Activation of **WPA2-PSK**, • **Mixed WPA2/WPA** : Activation of **Mixed WPA2/WPA**, • **Mixed WPA2/WPA-PSK** : Activation of **Mixed WPA2/WPA-PSK**, This choice will modify the Wireless configuration screen.	**Open**
WEP Encryption	Select from the scroll down list: • **Disabled** to not use WEP encryption. • **Enabled** to use WE encryption (see subsection 5.7.1.2 - WEP).	**Disabled**

5.7.2.1 Network Authentication

The scroll down list in the "Network Authentication" field shows 9 possible authentication types:

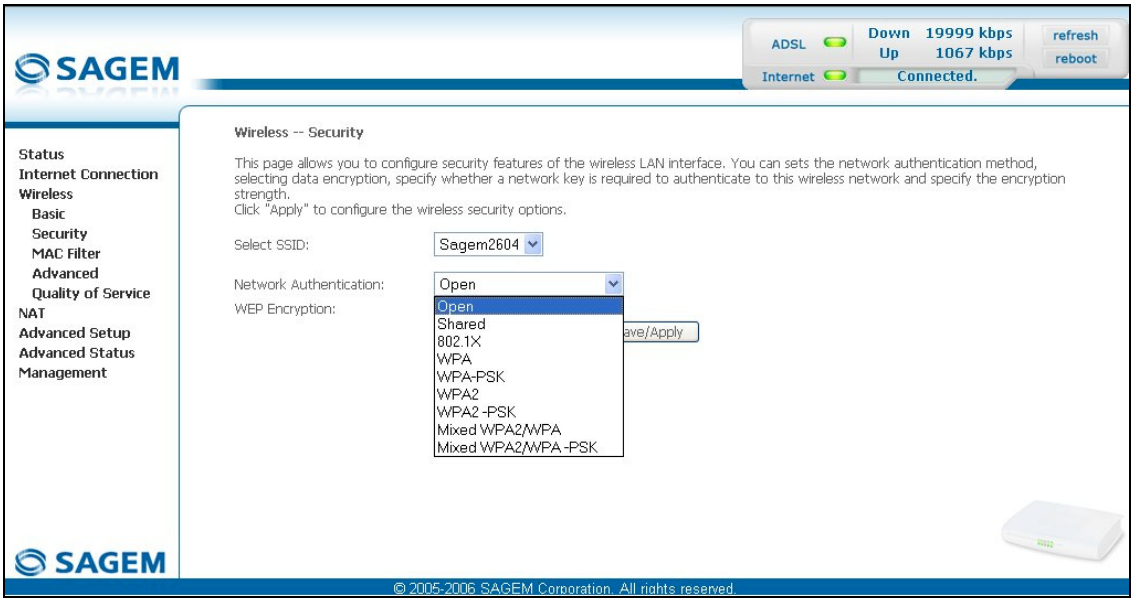
- Open,
- Shared,
- 802.1x,
- WPA,
- WPA-PSK,
- WPA2,
- WPA2-PSK,
- Mixed WPA2/WPA,
- Mixed WPA2/WPA-PSK.

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.

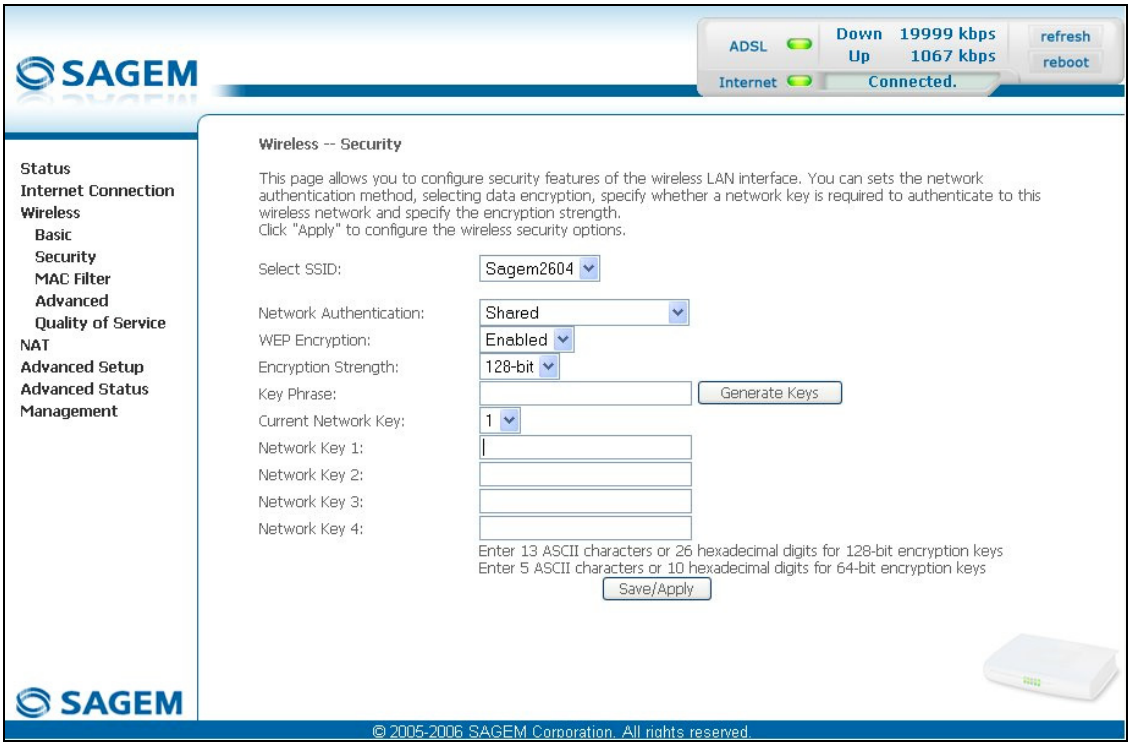


Shared

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:



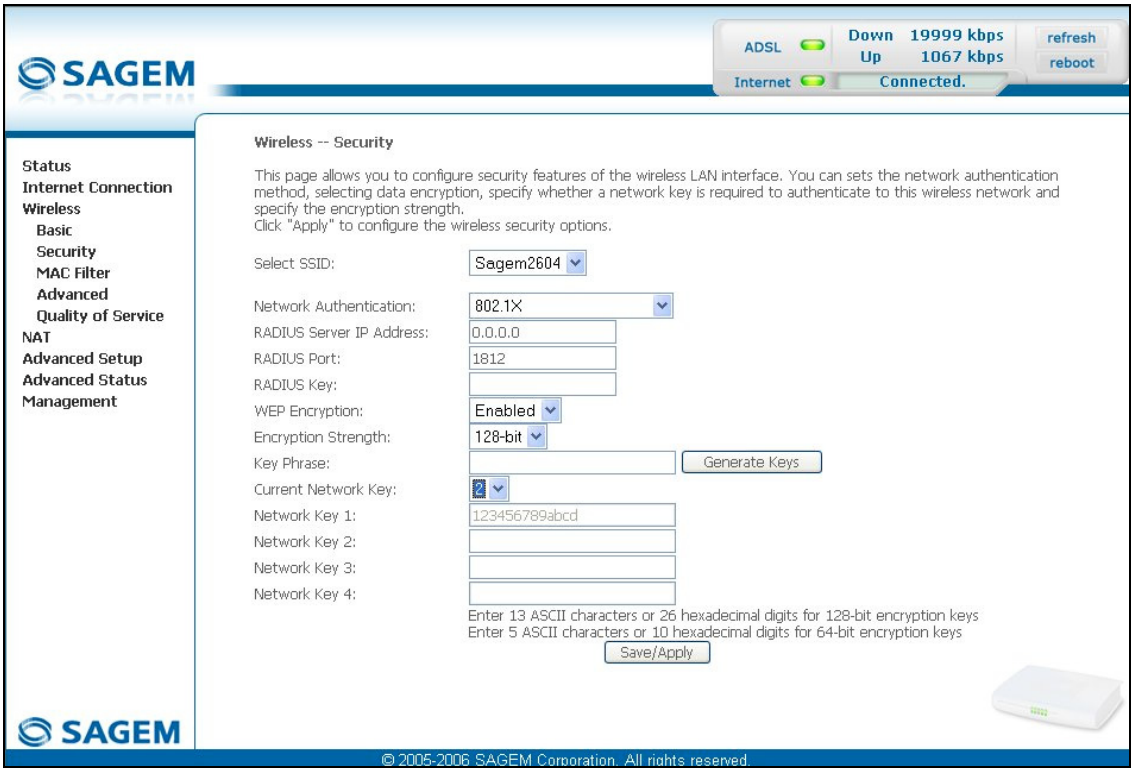
Field	Action	Default
WEP Encryption	**Note:** This field is always active (Enabled).	**Enabled (non modifiable)**
Encryption Strength	See subsection 5.7.1.2 - WEP.	**128-bit**
Key Phrase	See subsection 5.7.1.2 - WEP.	**Empty**
Current Network Key	See subsection 5.7.1.2 - WEP.	**2**
Network Key x (1 to 4)	See subsection 5.7.1.2 - WEP.	**Empty**

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:



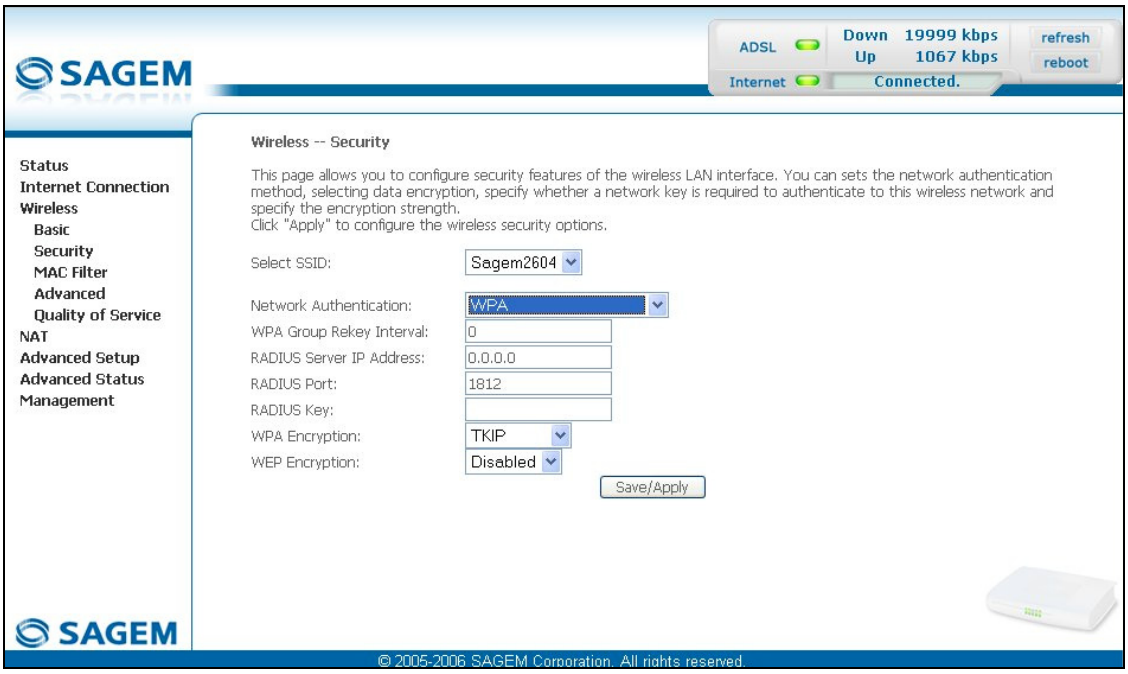
Field	Action	Default
RADIUS Server IP Address	Enter the IP address of the "RADIUS" authentication server.	**0.0.0.0**
RADIUS Port	Enter the port used for the "RADIUS" authentication server.	**1812**
RADIUS Key	Enter the secret key shared between the authentication server and its clients	**–**
WEP Encryption	**Note:** This field is always active (Enabled).	**Enabled**
Encryption Strength	See subsection 5.7.1.2 - WEP.	**128-bit**
Key Phrase	See subsection 5.7.1.2 - WEP.	**Empty**
Current Network Key	Select key 2 or 3 (see subsection 5.7.1.2 - WEP).	**2**

Field	Action		Default
Network Key x (1 to 4)	**1**	This field is empty or displays the key value entered earlier (greyed out)	**Non modifiable**
	2	Enter the encryption on the key you selected in the "Current Key" (see subsection 5.7.1.2- WEP).	
	3	Enter the encryption on the key you selected in the "Current Key" (see subsection 5.7.1.2- WEP).	
	4	This field is empty or displays the key value entered earlier (greyed out)	**Non 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:



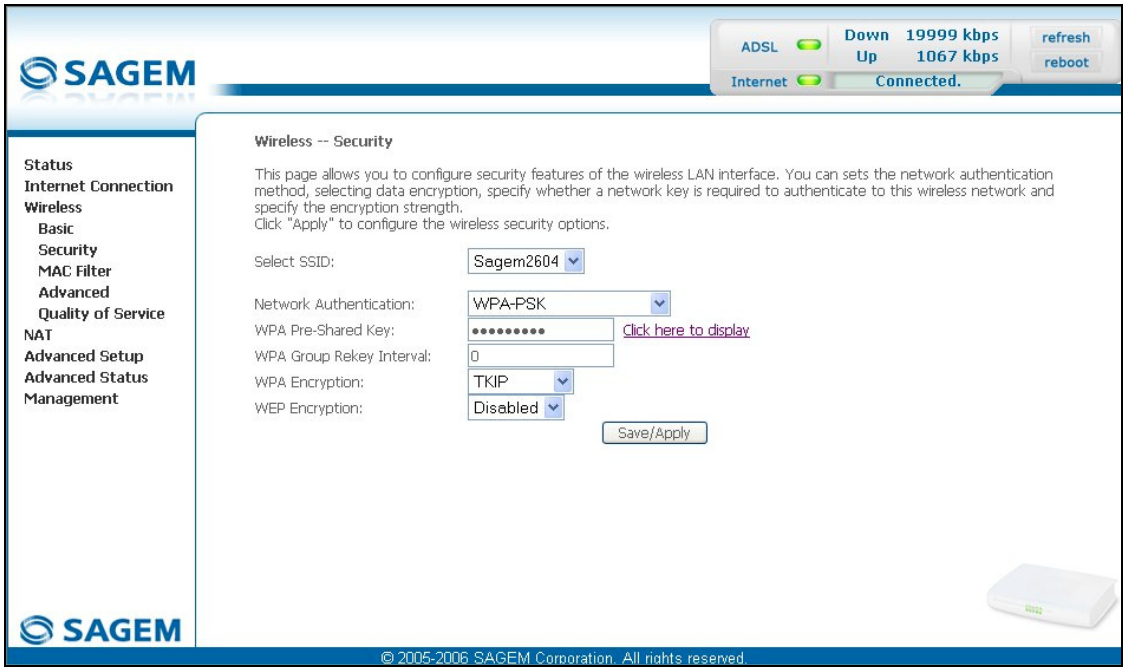
Field	Action	Default
WPA Group Rekey Interval	Enter a value (in seconds) which determines the period after which the WPA key will be regenerated (Renewing) in broadcast / multicast (LAN broadcast).	**0**
RADIUS Server IP Address	Enter the IP address of the "RADIUS" authentication server.	**0.0.0.0**
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 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**

Field	Action	Default
WEP encryption	Select from the scroll down list: • **Disabled** to use WPA encryption only. • **Enabled** to use both WPA and WEP encryption (see subsection 5.7.1.2 - WEP).	**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:



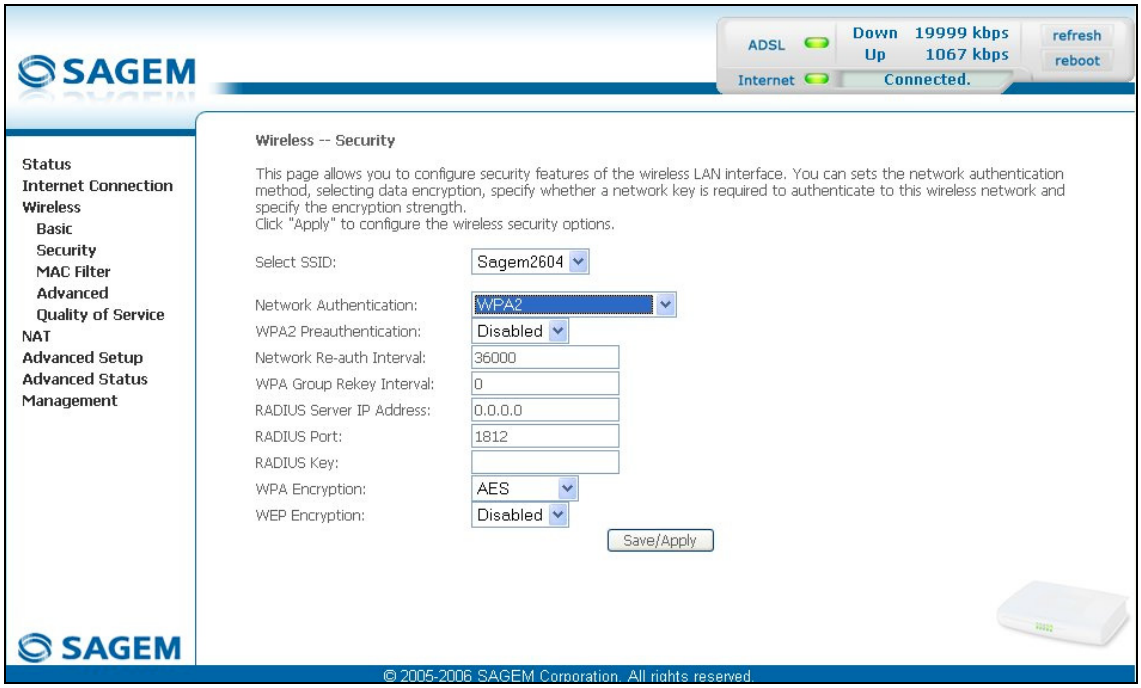
Field	Action	Default
WPA Pre-Shared Key	Enter the secret shared key. This may contain 8 to 63 ASCII characters or 64 hexadecimal symbols (256 bits). Click on the "Save/Apply" button to validate the entry. **Note:** You may display your secret phrase by clicking on "**Click here to display**".	**Empty**
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 encryption	Select the WPA encryption required from the scroll down list: • TKIP, • AES, • TKIP+ AES.	**TKIP**

Field	Action	Default
WEP encryption	Select from the scroll down list: • **Disabled** to use WPA encryption only. • **Enabled** to use both WPA and WEP encryption (see subsection 5.7.1.2 - WEP).	**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:

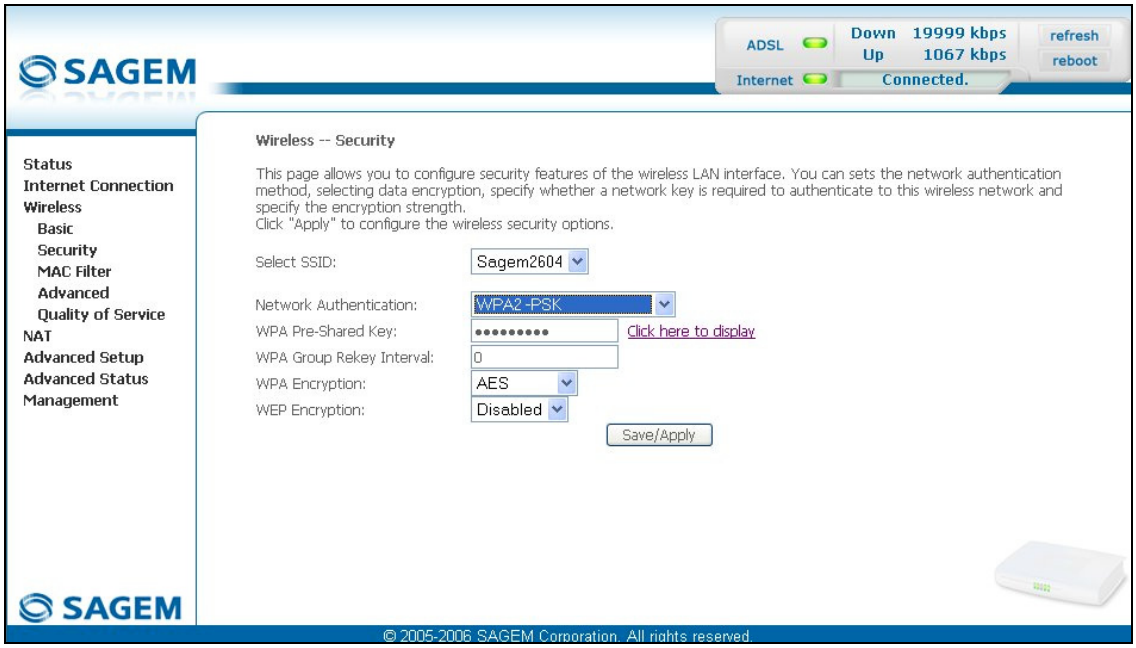


Field	Action	Default
WPA2 Preauthentication-	Select from the scroll down list: • **Disabled** to deactivate the WPA2 pre-authentication, • **Enabled** to activate the WPA2 pre-authentication,	**Disabled**
Network Re-auth Interval	Enter a value (in seconds) which determines the period after which the 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 encryption	Select the WPA encryption required from the scroll down list: • TKIP, • AES, • 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 (see subsection 5.7.1.2 - WEP).	**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:



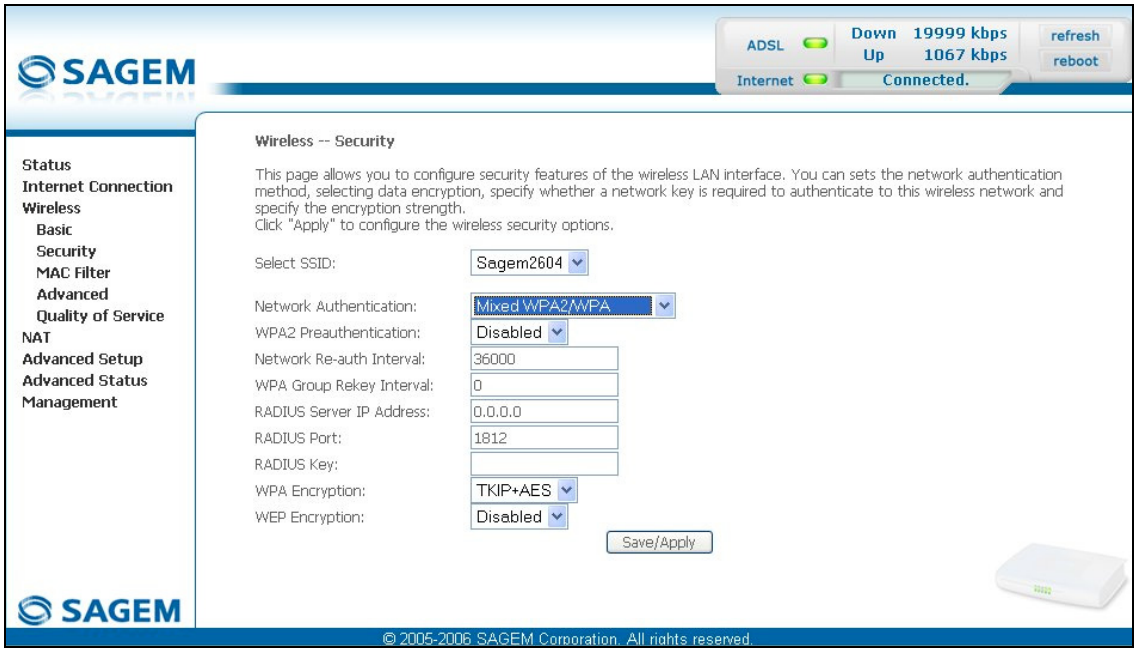
Field	Action	Default
WPA Pre-Shared Key	Enter a secret phrase. This may contain 8 to 63 ASCII characters or 64 hexadecimal symbols (256 bits). Click on the "Save/Apply" button to validate the entry. **Note:** You may display your secret phrase by clicking on "**Click here to display**".	**Empty**
WPA Group Rekay 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 encryption	Select the WPA encryption required from the scroll down list: • TKIP, • AES, • TKIP+ AES.	**AES**

Field	Action	Default
WEP encryption	Select from the scroll down list: • **Disabled** to use WPA encryption only. • **Enabled** to use both WPA and WEP encryption (see subsection 5.7.1.2 - WEP).	**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:



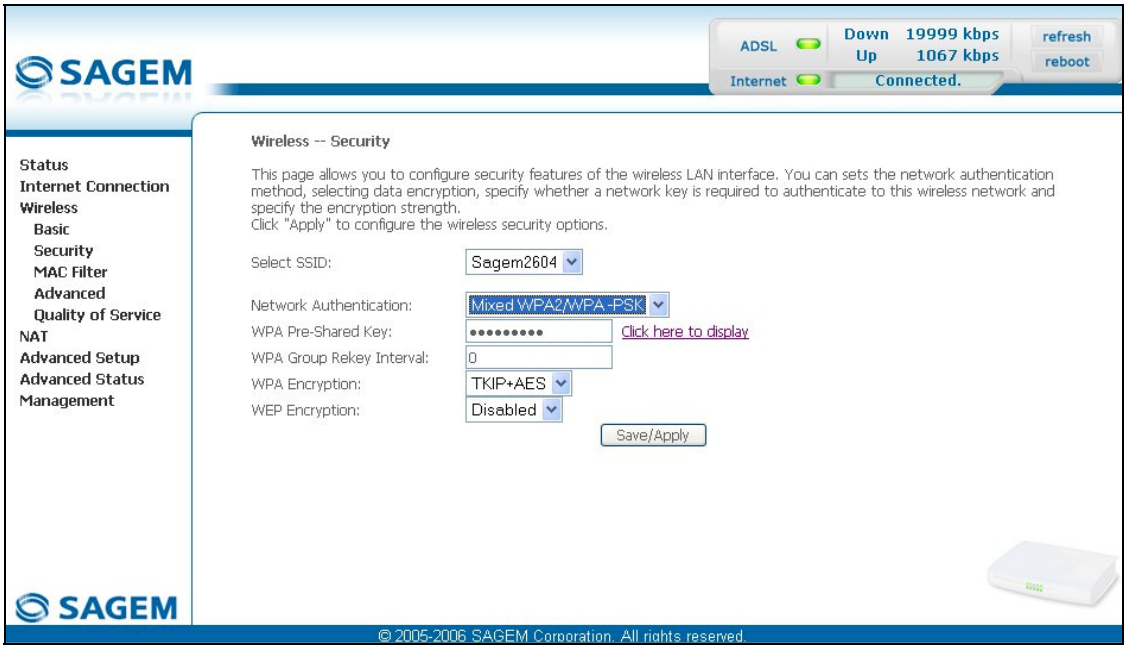
Field	Action	Default
WPA2 Preauthentication-	Select from the scroll down list: • **Disabled** to deactivate the WPA2 pre-certification, • **Enabled** to activate the WPA2 pre-certification,	**Disabled**
Network Re-auth Interval	Enter a value (in seconds) which determines the period after which the WPA 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	**–**

Field	Action	Default
WPA encryption	Select the WPA encryption required from the scroll down list: • TKIP, • AES, • TKIP+ AES.	**TKIP+AES**
WEP Encryption	Select from the scroll down list: • **Disabled** to not use WEP encryption. • **Enabled** to use WE encryption (see subsection 5.7.1.2 - WEP).	**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:



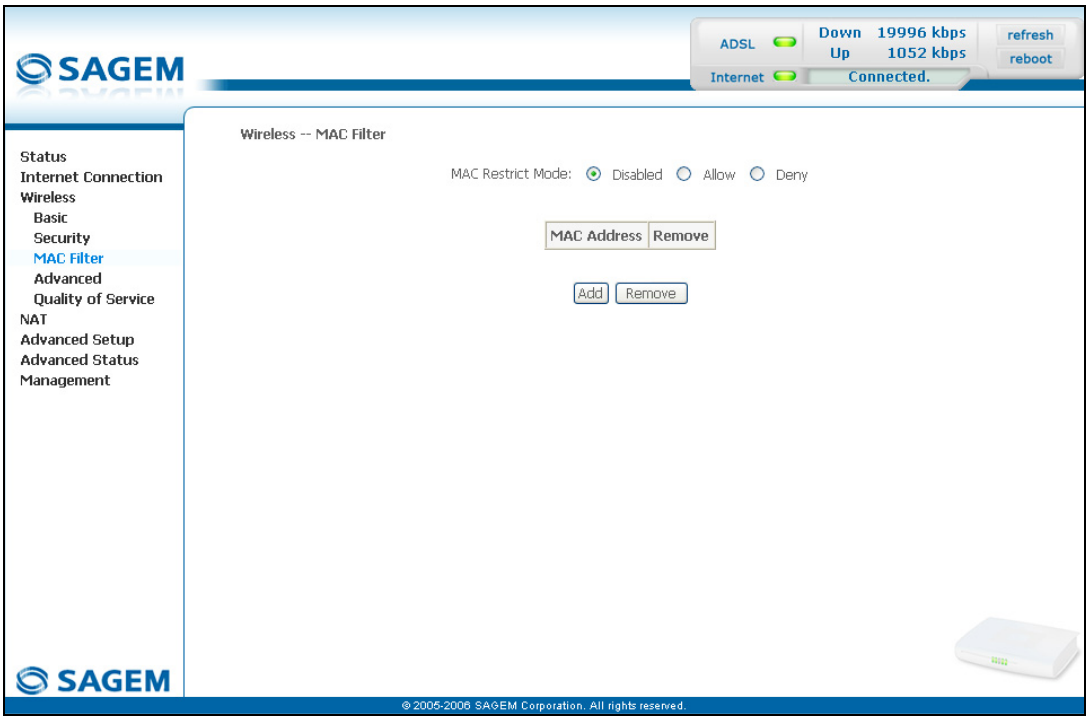
Field	Action	Default
WPA Pre-Shared Key	Enter a secret phrase. This may contain 8 to 63 ASCII characters or 64 hexadecimal symbols (256 bits). Click on the "Save/Apply" button to validate the entry. **Note:** You may display your secret phrase by clicking on "**Click here to display**".	**Empty**

Field	Action	Default
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 encryption	Select the WPA encryption required from the scroll down list: • TKIP, • AES, • TKIP+ AES.	**TKIP+ AES**
WEP Encryption	Select from the scroll down list: • **Disabled** to not use WEP encryption. • **Enabled** to use WE encryption (see subsection 5.7.1.2 - WEP).	**Disabled**

5.7.3 MAC Filter

Object: The "MAC Filter" function is used to limit the number of computers which can access your wireless network.

- Select the **MAC Filter** menu in the **Wireless** section to display the following screen:



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

Add

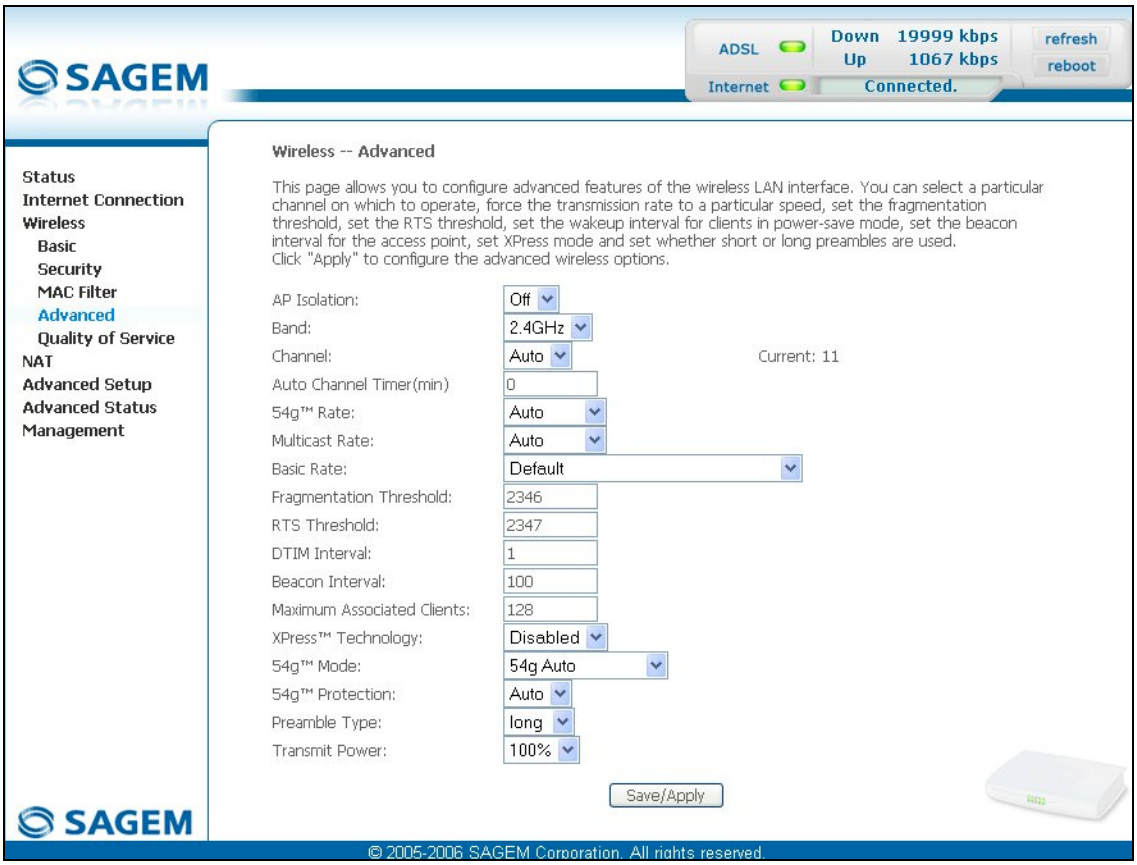
- Click on the **Add** button to add a MAC address to be filtered (address of a computer authorised to connect to a wireless network).

Note: The MAC address can be added automatically at the time of the Wi-Fi installation, by a short push on button “REG”.
After approximately 5 minutes, the new address fits in the list and F@st™ 2604 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.

5.7.4 Advanced

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

- Select the **Advanced** menu in the **Wireless** section to display the following screen:



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	Meaning	Default
AP Isolation	Select from the scroll down list: **Off** : to not isolate the **A**ccess **P**oint i.e. authorise machines connected to the router to communicate with each other. **On** : to isolate the Access point, i.e. prohibit machines connected to the router to communicate with each other.	**Off**
Band	Select the 2.4 GHz band for the IEEE 802.11g standard.	**2.4GHz-802.11g**
Channel	See Wireless/Basic subsection 5.7.1.1.	**Auto**
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).	**0**
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.	**Auto**
Multicast Rate	From 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**

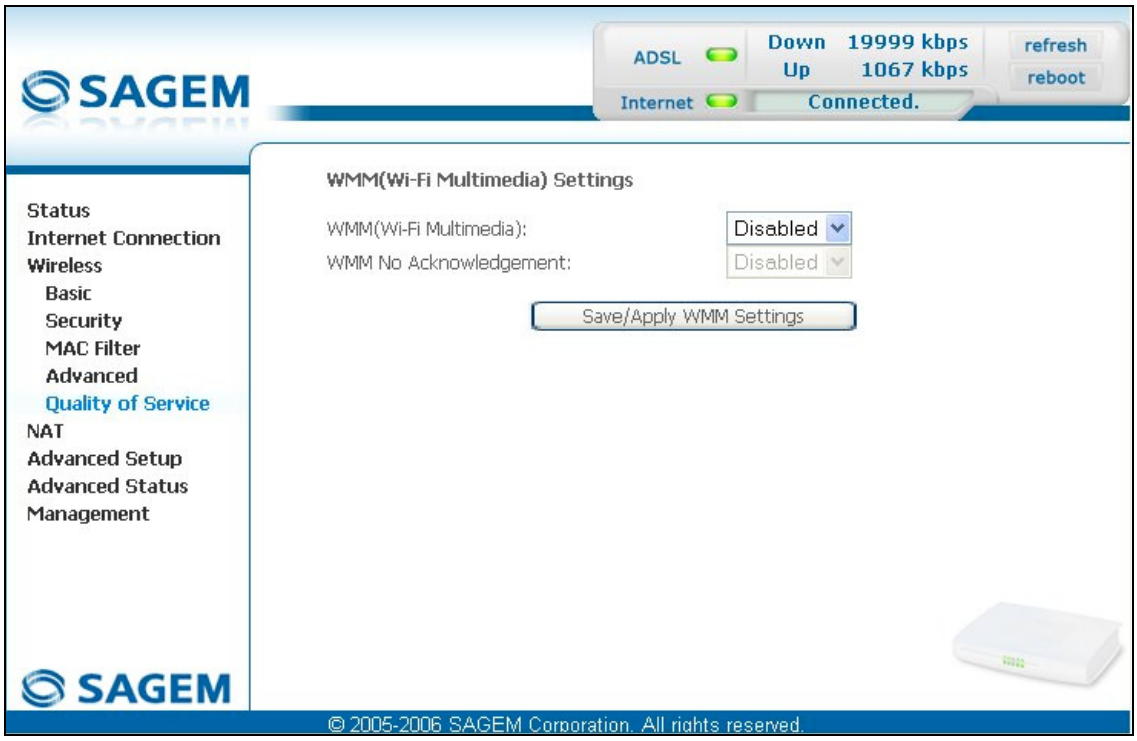
Field	Meaning	Default
RTS Threshold	The RTS/CTS protocol (**R**equest **T**o **S**end / **C**lear **T**o **S**end) is used to reduce the probability of collisions between stations. **Note:** As packet size is set by default to 2346, the RTS/CTS protocol is inhibited as its value is set by default to 2347. Enter a threshold value (in bytes) between 1 and 2347.	**2347**
DTIM Interval	The DTIM counting area (**D**elivery **T**raffic **I**ndication **M**essage) enables Wi-Fi clients to listen to broadcast and multicast messages saved in your router's "Buffer" memory. Enter an interval value (in seconds) between 1 and 255.	**1**
Beacon Interval	Enter a time interval value between two beacon signals which shows the activity of the wireless network. This interval value (in milliseconds) is between 1 and 1000.	**100**
Maximum Associated Clients	Enter the maximum number wireless customers for your router.	**128**
XPress™ Technology	From the scroll down list, select **Enabled** to apply the "XPress™" technology or **Disabled** to not apply it.	**Disabled**
54g™ Mode	In the scroll down list, select (54g Auto, 54g Performance, 54g LRS or 802.11b Only)	**54g Auto**
54g Protection	Select **Auto** to improve the quality in the mixed 802.11 environments (g and b for example) or **Off** to improve the quality only on the 802.11g environments but degrade it on other environments (802.11b for example).	**Auto**

Field	Meaning	Default
Preamble Type	In the IEEE 802.11 standard, the "preamble" is used to synchronise the Emitter and Receiver correctly. The "long preamble" is generally commonly used. For reasons of bandwidth gain, this standard proposes reducing the length of the "preamble". “Preamble Type” defines the length of block CRC (Cyclical Redundancy Checking). If your network does not include any peripheral 802.11b, you can configure the type of preamble on “**short**” for an optimal result. The type of preamble “**long**” must be used if the peripherals 802.11g and 802.11b are both present on the network. In the scroll down list, select **long** to keep a 128 bit "preamble" or **short** to reduce it to 56 bits.	**long**
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%**

5.7.5 Quality of Service

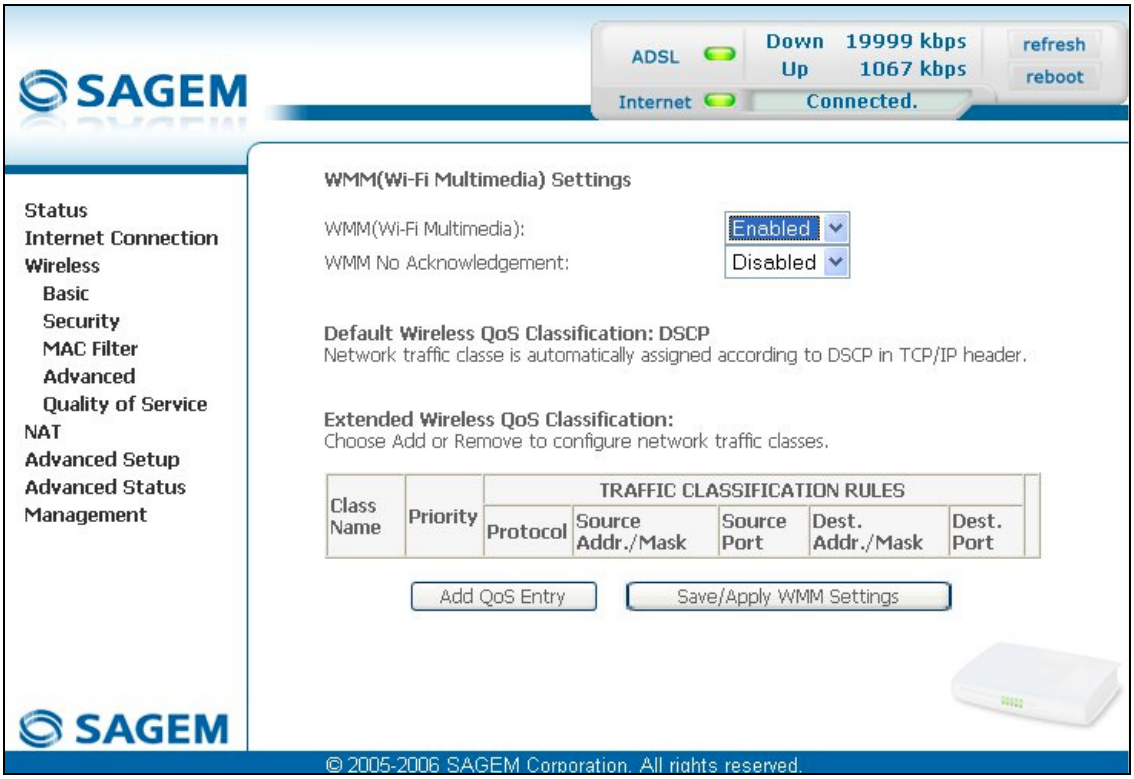
Object: The Wi-Fi quality of service for your router conforms to the WMM (**W**ifi **M**ulti**M**edia) specification. This standard improves the performances of Wi-Fi links by acting on the data flows (packet size, bit rates, etc.) and the length of queues while respecting bandwidth requirements (managed by the router).

- Select the **Quality of Service** menu in the **Wireless** section to display the following screen:



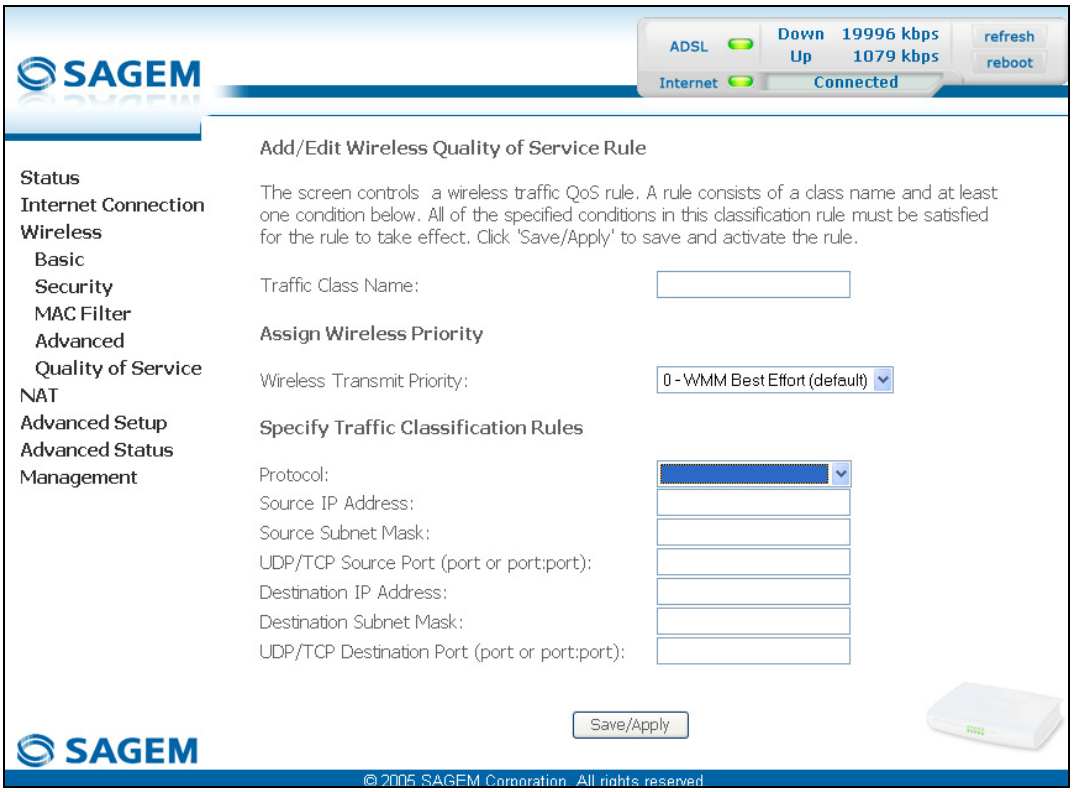
Field	Meaning	Default
WMM (Wi-Fi Multimedia)	In the scroll down list, select the activation (**Enabled**) or deactivation (**Disabled**) of the WMM support.	**Disabled**
WMM No Acknowledgement	**Note:** The scroll down list may only be operational if the "WMM (Wi-Fi Multimedia)" field is activated. In the scroll down list, select **Enabled** or **Disabled** to permit or prohibit a more effective bit rate of the data flow with, on the other hand, a higher error rate.	**Greyed out**

The following screen appears as soon as you activate "WMM".



Add

- Click on the **Add QoS Entry** button to add a Wi-Fi Quality of Service (wifi QoS) rule; the following screen appears.



Field	Action	Default
Traffic Class Name	Enter a name for the traffic class you want to create.	**Empty**
Wireless Transmit Priority	In the scroll down list, select the priority you want to allocate to the traffic class you selected (see table below).	**0 - WMM Best Effort (default)**
Protocol	Select the appropriate protocol from the scroll down list (TCP/UDP, TCP, UDP, ICMP).	**Empty**
Source IP Address	Enter a Source IP address (LAN).	**Empty**
Source Subnet Mask	Enter a sub-net mask associated with the "Source" IP address.	**Empty**
UDP/TCP Source Port (port or port:port)	Enter a "Source" port or range of ports. **Note:** For one port, for example, enter 80. For a range of ports, enter 80:90.	**Empty**
Destination IP Address	Enter a "Destination" IP address (WAN).	**Empty**
Destination Subnet Mask	Enter a sub-net mask associated with the "Destination" IP address.	**Empty**
UDP/TCP Destination Port (port or port:port)	Enter a "Destination" port or range of ports. **Note:** For one port, for example, enter 80. For a range of ports, enter 80:90.	**Empty**

Transmission priority	Meaning
0 - WMM Best Effort (default)	This is the lowest priority. This provides no guarantee of data transmission.
1 - WMM Background	These are intermediate priorities. These provide routing without too much data flow loss.
2 - WMM Background	
3 - WMM Best Effort	This priority provides no guarantee of data transmission.
4 - WMM Video priority	These are intermediate priorities. They provide a correct routing for "Video".
5 - WMM Video priority	
6 - WMM Voice priority	These are higher priorities. They provide complete routing for voice
7 - WMM Voice priority	

Click on the 

button to save the parameters.

5.8 NAT

Object: 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.
Several translation function configurations, the NAT actions, can be configured and may be activated as indicated in the 5.8.1 - **Add** paragraph.

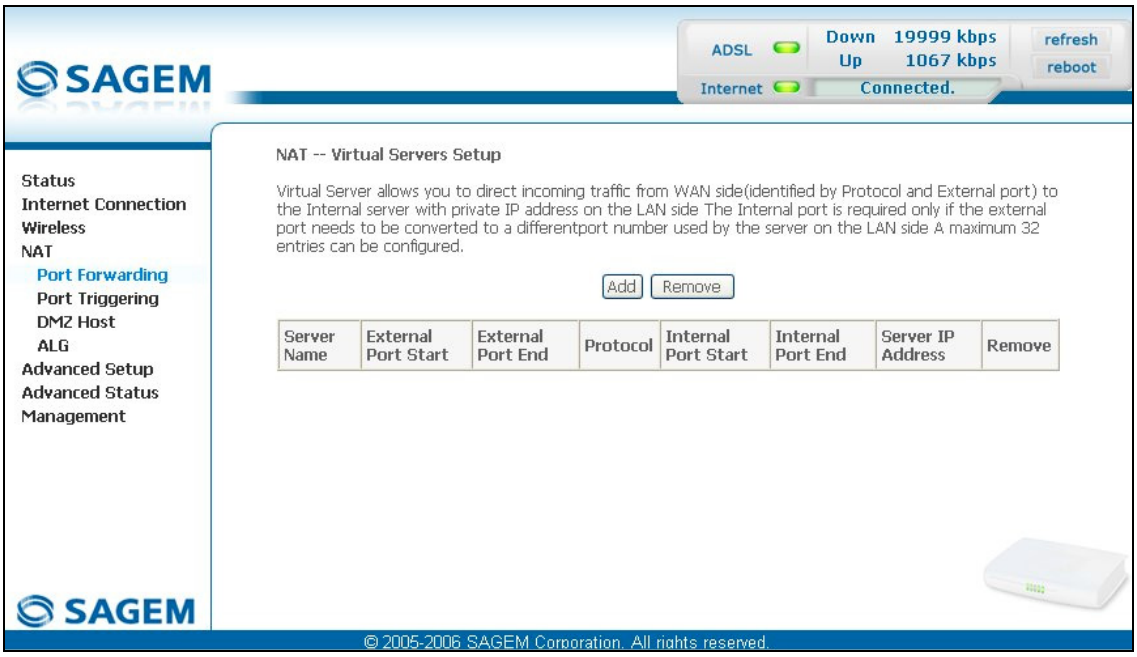
This section contains the following four menus:

- Port forwarding (see subsection 5.8.1),
- Port Triggering (see subsection 5.8.2),
- DMZ Host (see subsection 5.8.3),
- ALG (see subsection 5.8.4).

5.8.1 Port forwarding

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.

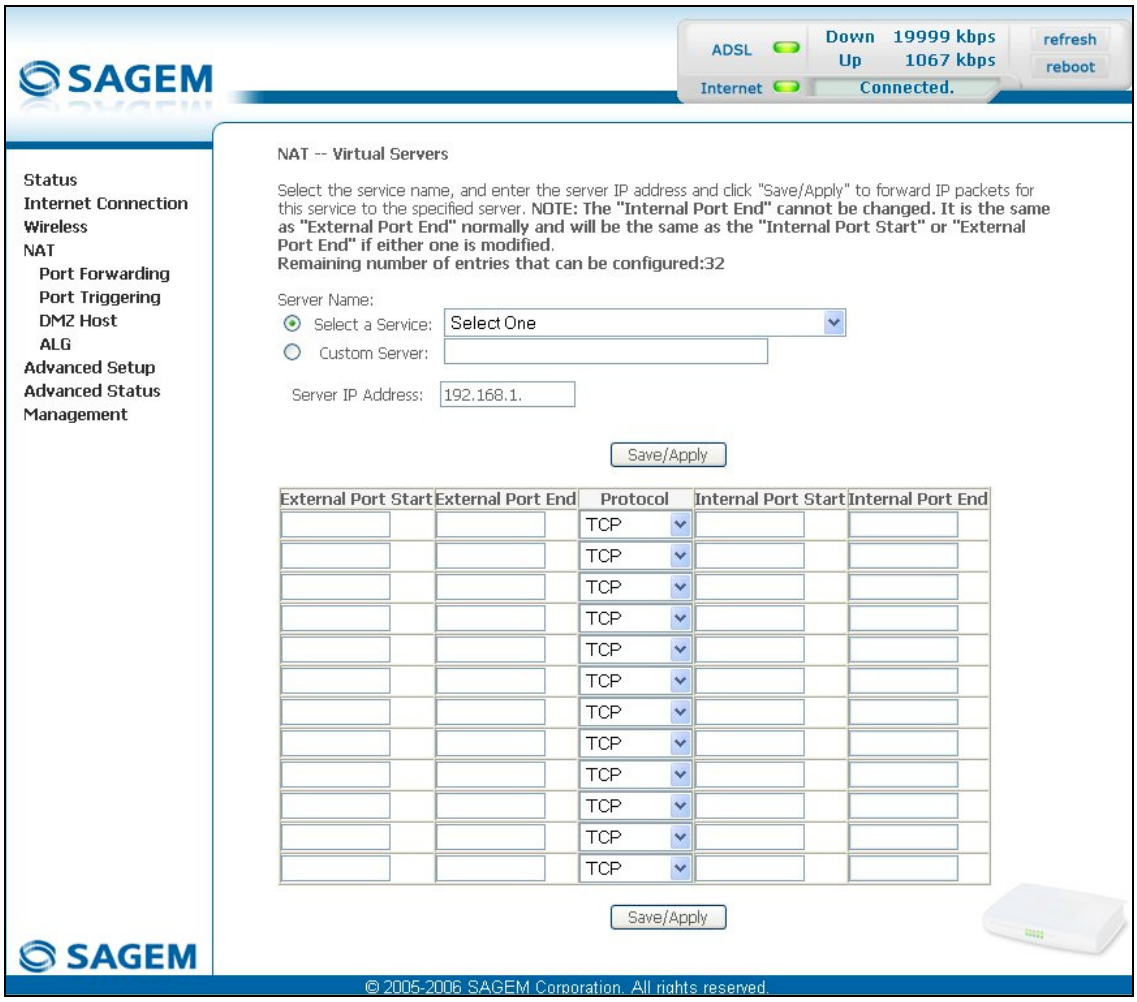
- Select the **Port forwarding** menu in the **NAT** section to display the following screen:



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

Add

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



Proceed as follows:

- 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.

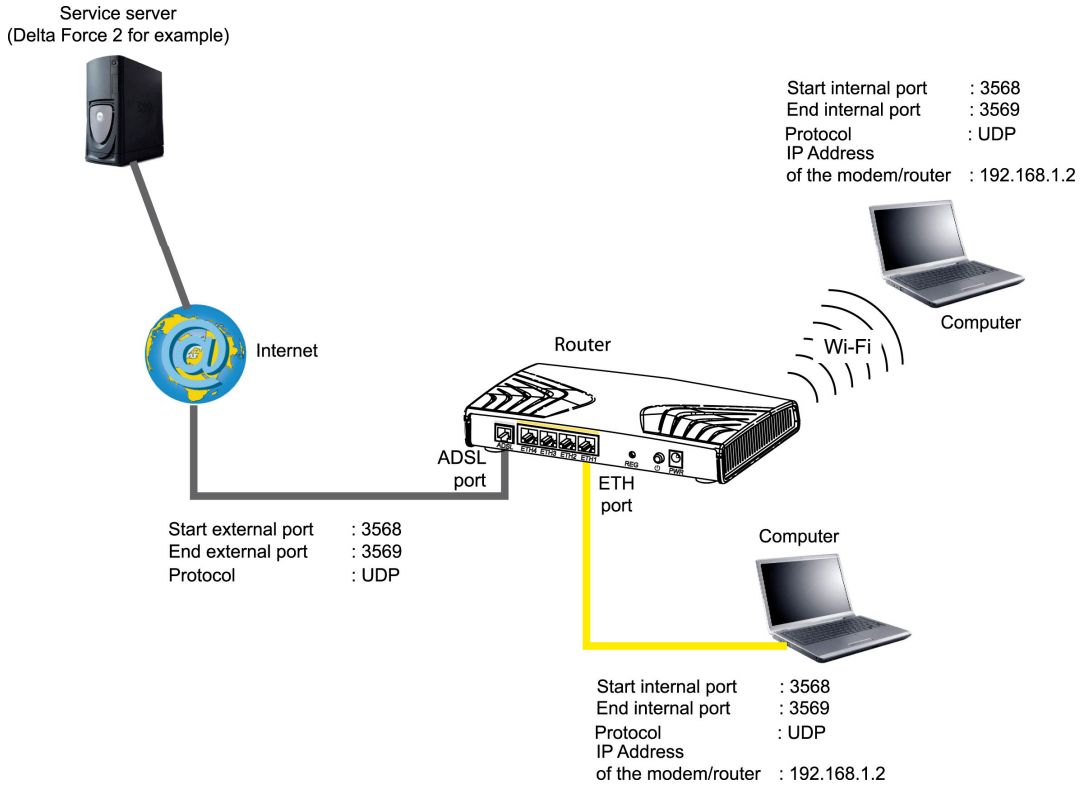
or

- Check the "**Custom Server**" 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:

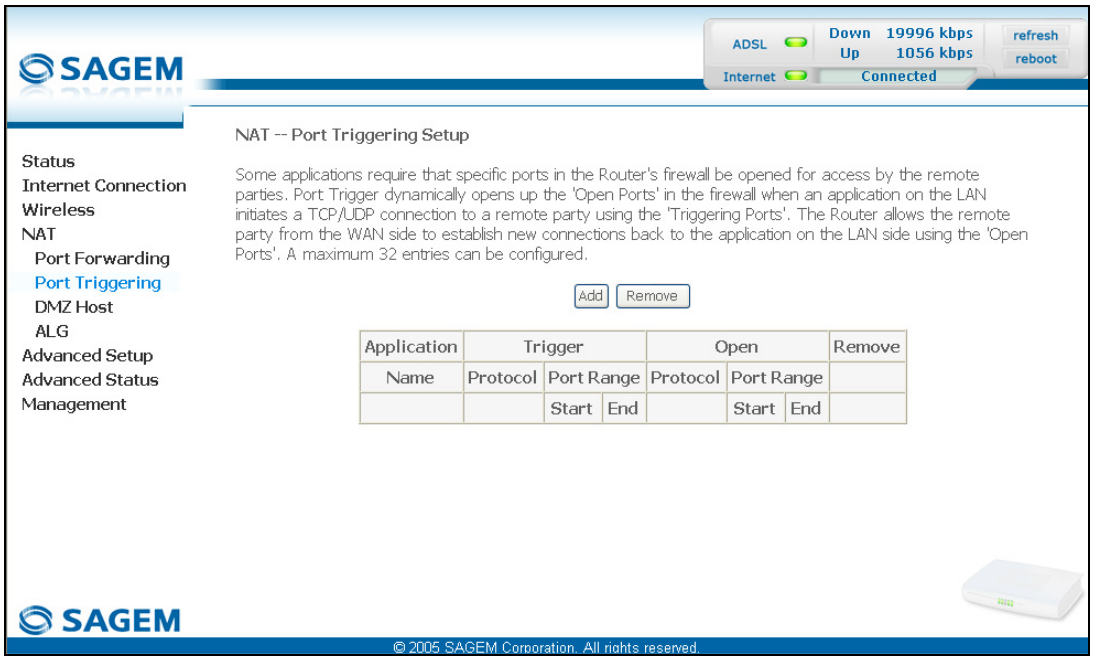


The "Delta Force 2" service is available on your computer via the external ports 3568 and 3569 (WAN side) and via the internal ports 3568 and 3569 (LAN side).

5.8.2 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).

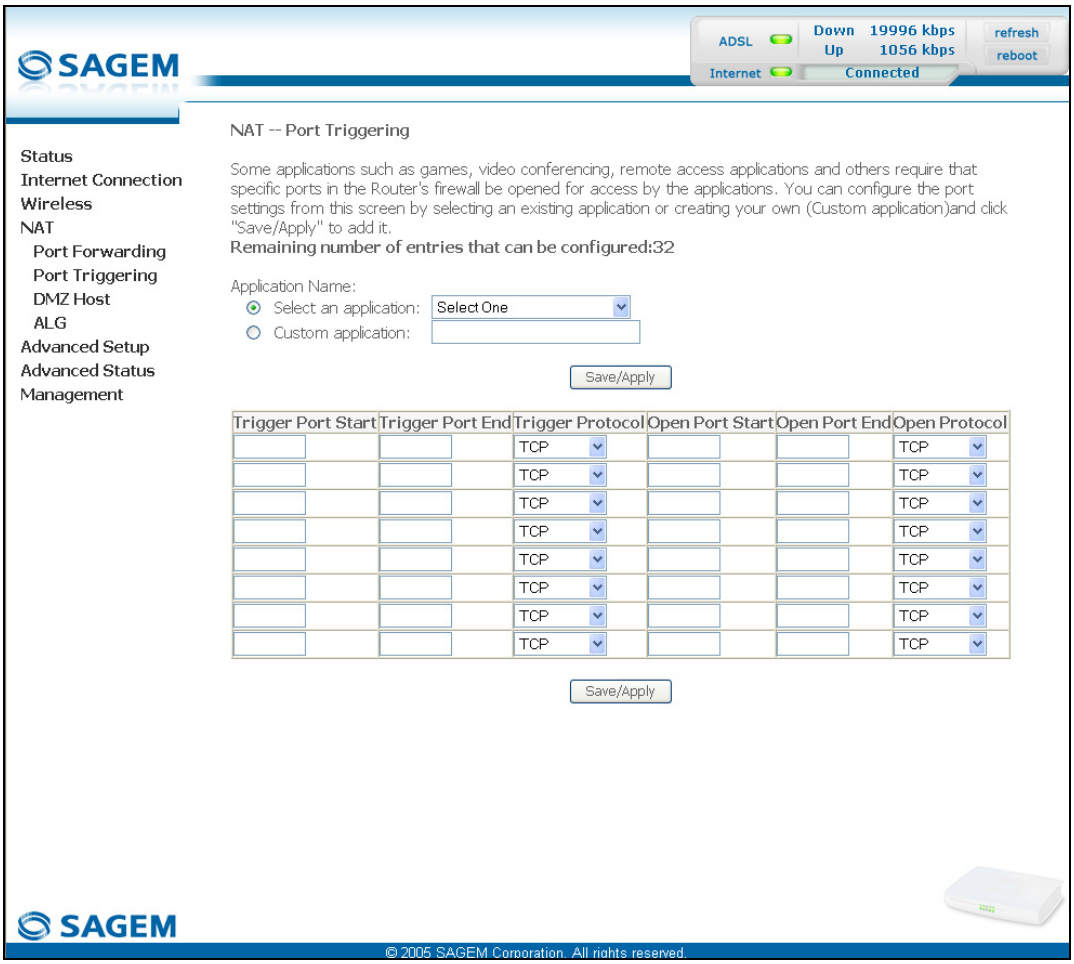
- Select the **Port Triggering** menu in the **NAT** section to display the following screen:



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.

Add

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



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

➢ 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**", "**Trigger Port Start**", "**Trigger 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

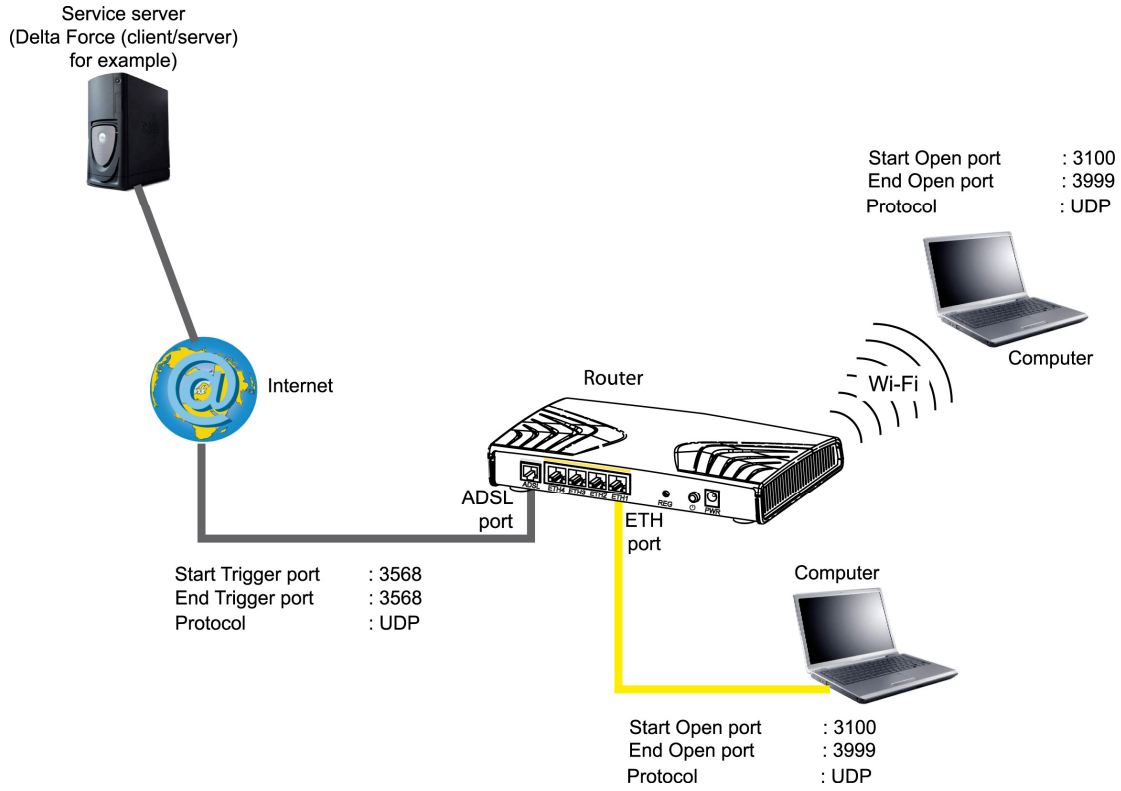
➢ Check the "**Custom Server**" box then enter the name of the server you want to connect to, then:

- Complete the ID Host of your computer's IP address (this is attributed by your router's DHCP server).
- Fill in the "**Trigger Port Start**", "**Trigger Port End**", "**Trigger Port Start**", "**Trigger 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:



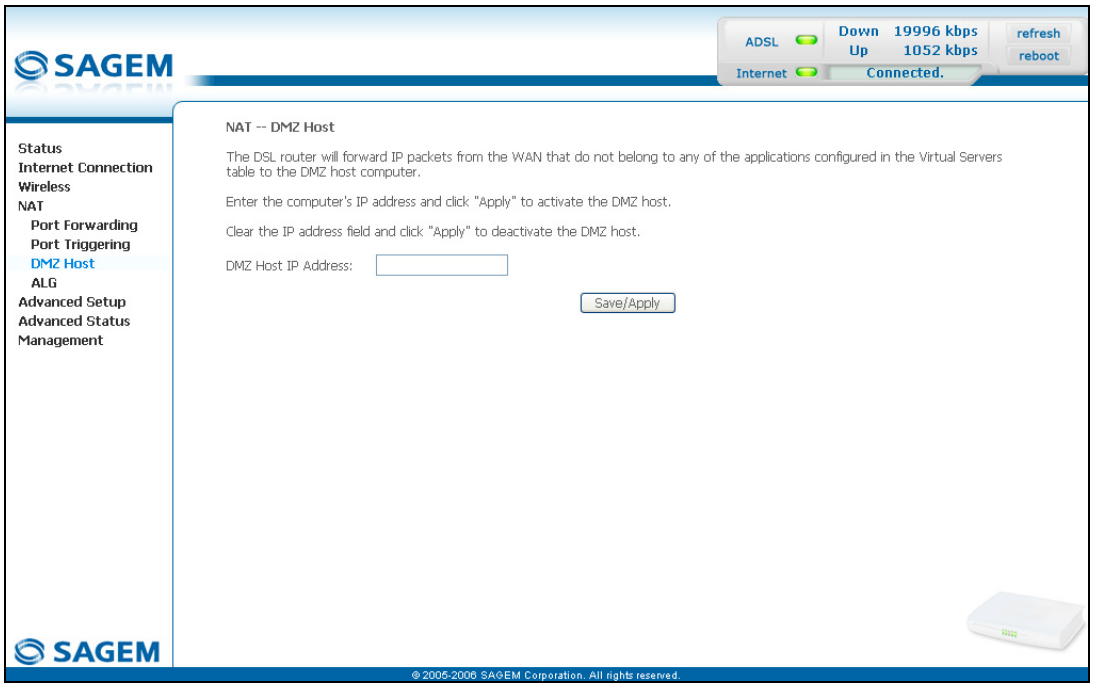
Using the "Trigger" 3568 port (WAN side), the "Delta Force" service server triggers the opening of port range 3100 to 3999 for your computer to access this service.

5.8.3 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".

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.

- Select the **DMZ Host** menu in the **NAT** section to display the following screen:



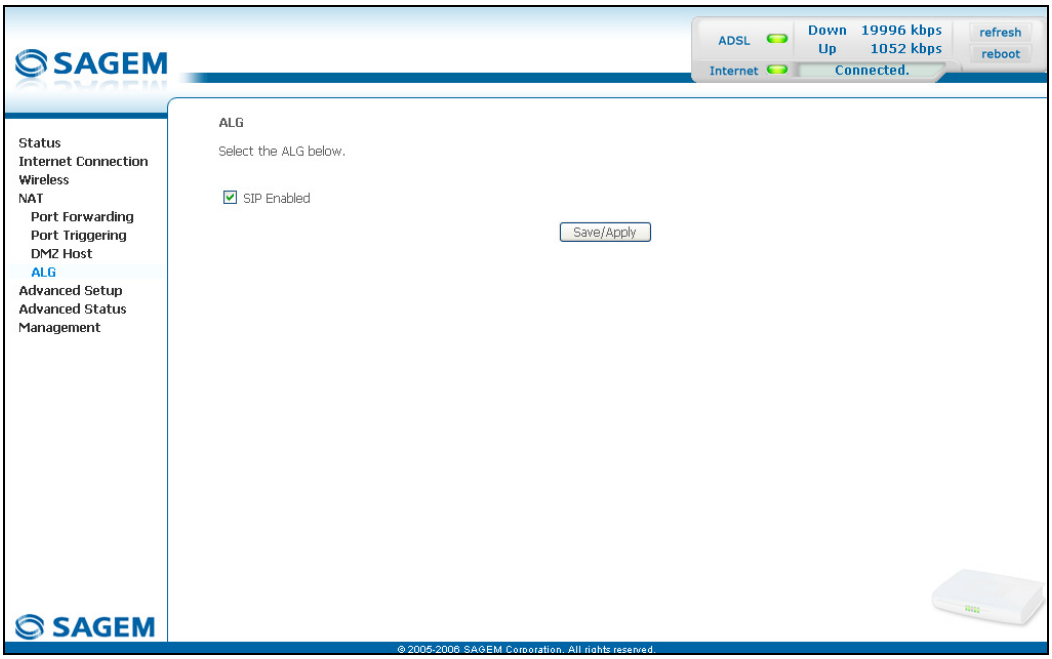
Field	Action	Default
DMZ Host IP Address	Enter the IP address of a server to activate the "DMZ" and therefore access it directly from the Internet. To deactivate the "DMZ" zone, erase the address entered in the field. **Note**: Click on the **Save/Apply** button to take account of the address or its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

The "DMZ" zone is deactivated by default.

5.8.4 ALG

Object: The ALG (**A**pplication **L**ayer **G**ateway) service is used to take charge of the SIP protocol via the Wi-Fi or Ethernet interfaces in the telephony over IP (VoIP) context.

- Select the **ALG** menu in the **NAT** section to display the following screen:



Field	Meaning	Default
SIP Enabled	Check the box to permit telephoning in VoIP via the Wi-Fi or Ethernet interfaces using the SIP protocol.	**Checked**

5.9 Advanced Setup

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

This menu must only be used by experienced users.

This section contains the following nine menus:

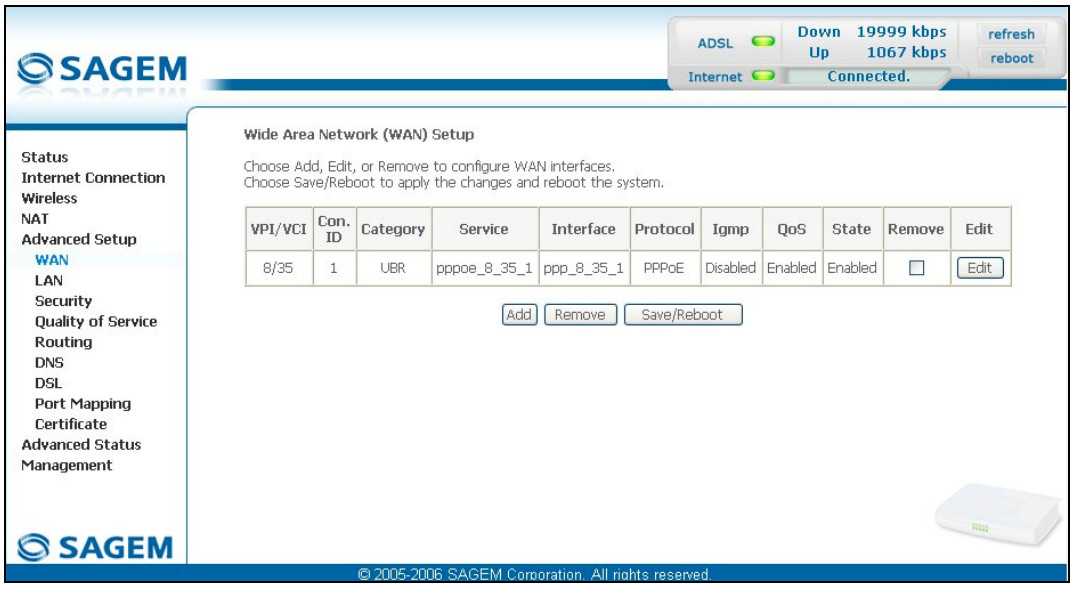
- WAN (see subsection 5.9.1),
- LAN (see subsection 5.9.2),
- Security (see subsection 5.9.3),
- Quality of Service (see subsection 5.9.4)(see note),
- Routing see subsection 5.9.5),
- DNS (see subsection 5.9.6),
- DSL (see subsection 5.9.7),
- Port Mapping (see subsection 5.9.8),
- Certificate (see subsection 5.9.9).

Note: This menu only appears if you checked the "Enable Quality Of Service" box in the WAN interface configuration screen (see Advanced Setup/WAN – subsection 5.9.1/Add).

5.9.1 WAN

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

- Select the **WAN** menu in the **Advanced Setup** section to display the following screen:

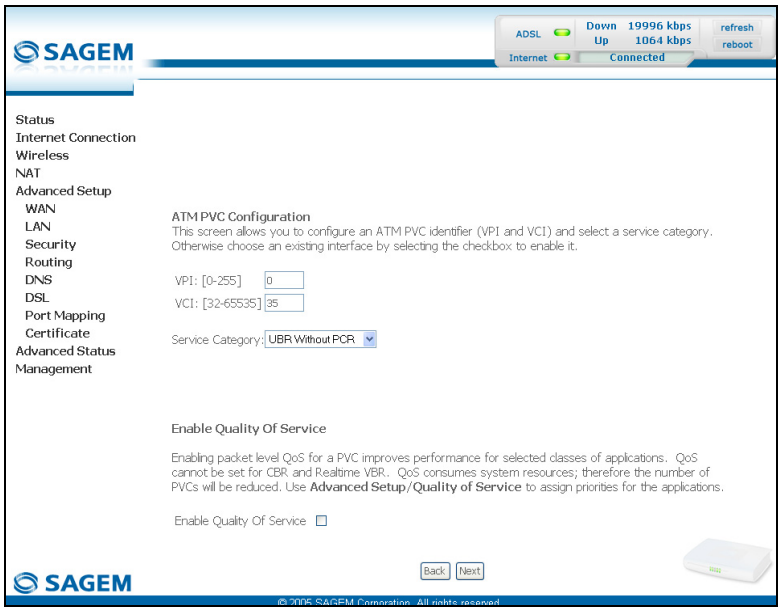


Field	Meaning
VPI/VCI	PVC identifier to configure.
Con. ID	Connection Identification. This is used to identify the different PPP connections which belong to the same PVC. To do so, you need only increment the "VC number" in the "Service" field when adding a new "PVC".
Category	ATM type of service
Service	Name of the ATM service. This name is made up as follows: Protocol_VPI_VCI_Index For example: pppoe_0_35_1.
Interface	Name, allocated automatically, associated with the service name (for example, ATM interface "ppp_0_35_1" associated with the ATM service pppoe_0_35_1).
Protocol	Data flow encapsulation mode.
Igmp	Status (Enabled or Disabled) of the IGMP function. (see Note).
QoS	Status (Enabled or Disabled) of the Quality of Service (QoS).
State	Status (Enabled or Disabled) of the WAN interface.

Note: This function enables the distribution of Multicast datagrams over the local network (LAN) and interaction between the router and the local network hosts.

Add

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



ATM PVC Configuration

Field	Action	Default
VPI	Enter a VPI value[1] between 0 and 255.	**0**
VCI	Enter a VPI value[1] between 32 and 65535.	**35**
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**
Peak Cell Rate[2]	Enter a maximum number of cells transmitted per second, between 1 and 2491.	**0**
Sustainable Cell Rate[3]	Enter an average number of cells transmitted per second. **Note:** This number must be lower than the **P**eak **C**ell **R**ate (PCR).	**0**
Maximum Burst Size[3]	Enter the maximum number of cells emitted in burst (value between 1 and 1000 000).	**0**

Enable Quality Of Service

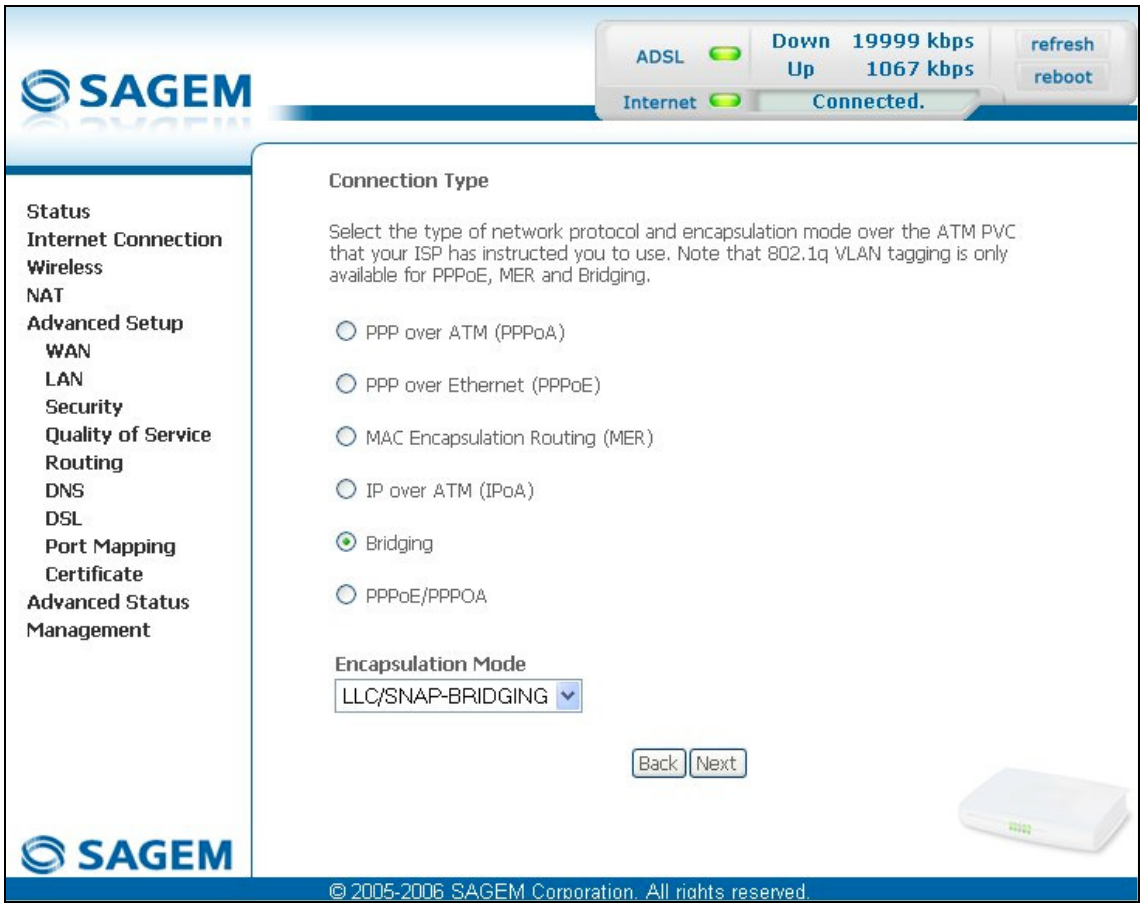
Field	Action	Default
Enable Quality Of Service	Check the box to activate the quality of service and display the new "Quality of Service" menu in the **Advanced Setup** section.	**Not checked**

[1] This value is delivered to you by your **I**nternet **S**ervice **P**rovider (ISP).

[2] This field only appears when the "UBR with PCR", "CBR", "Non Realtime VBR" or "Realtime VBR" type of service is selected.

[3] This file only appears when the "Non Realtime VBR" or "Realtime VBR" type of service is selected.

- Click on the **Next** button to continue configuring the remote network (WAN) and display the following screen:



Depending on the type of network protocol selected, the encapsulation modes suggested in the scroll down list in the appropriate field are different.

Therefore, and to provide more clarity, a summary table will be presented below for each type of protocol.

PPP over ATM (PPPoA)

Field	Action	Default
Encapsulation Mode	Select the encapsulation of your choice from the scroll down list. • VC/MUX, • LLC/ENCAPSULATION.	**VC/MUX**

PPP over Ethernet (PPPoE)

Field	Action	Default
Encapsulation Mode	Select the encapsulation of your choice from the scroll down list. • LLC/SNAP-BRIDGING, • VC/MUX.	**LLC/SNAP-BRIDGING**

MAC Encapsulation Routing (MER)

Field	Action	Default
Encapsulation Mode	Select the encapsulation of your choice from the scroll down list. • LLC/SNAP-BRIDGING, • VC/MUX.	**LLC/SNAP-BRIDGING**

IP over ATM (IPoA)

Field	Action	Default
Encapsulation Mode	Select the encapsulation of your choice from the scroll down list. • LLC/SNAP-ROUTING, • VC/MUX.	**LLC/SNAP-ROUTING**

Bridging

Field	Action	Default
Encapsulation Mode	Select the encapsulation of your choice from the scroll down list. • LLC/SNAP-BRIDGING, • VC/MUX.	**LLC/SNAP-BRIDGING**

PPPoE/PPPoA

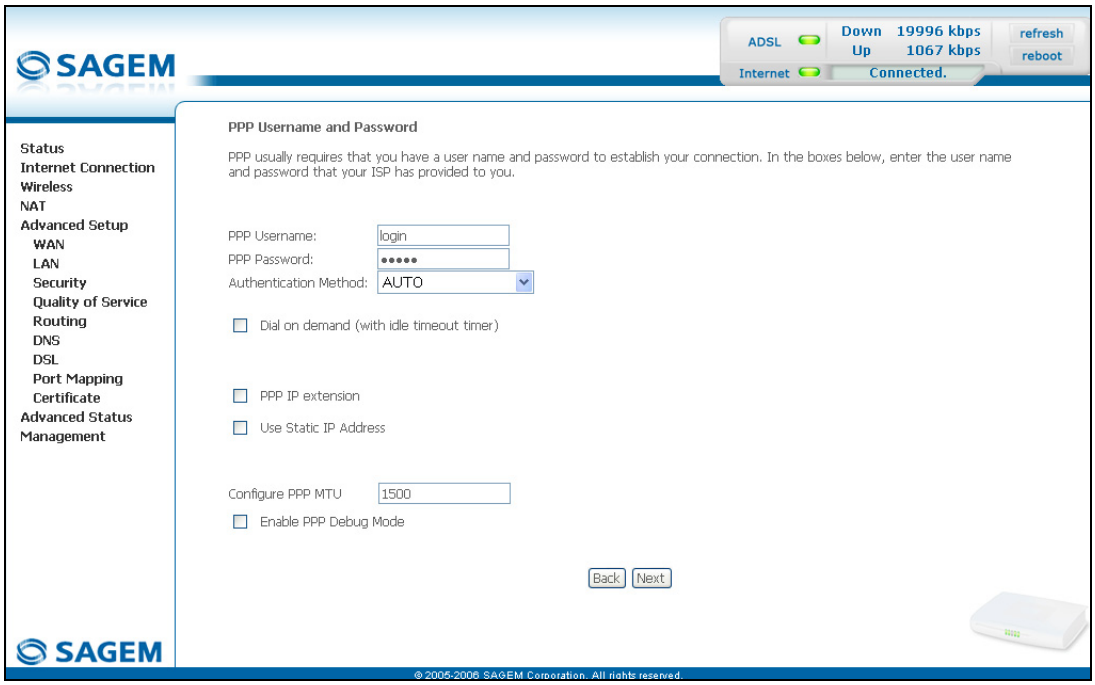
The encapsulation mode field will be selected automatically with PPPoE/PPPoA protocol type.

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

Depending on the type of network protocol (PPPoA, PPPoE, MER, IPoA or Bridging) selected earlier, 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.

PPP over ATM (PPPoA)



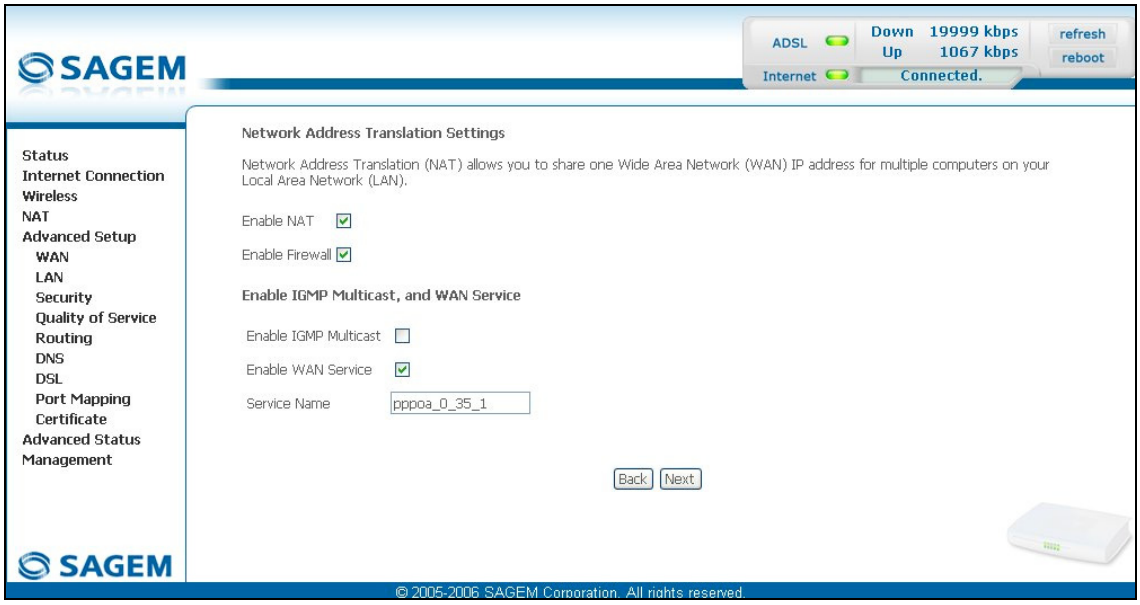
Field	Action	Default
PPP Username	Enter your connection ID. This information is provided to you by your **I**nternet **S**ervice **P**rovider (ISP).	**Empty**
PPP Password	Enter your connection password. This information is provided to you by your **I**nternet **S**ervice **P**rovider (ISP).	**Empty**
Authentification 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 Internet only for "Traffic" on the ADSL line.	**Not checked**
Inactivity Timeout (minutes) [1-4320]: [4]	Enter a value (in minutes) between 1 and 4320 (i.e. 72 hours).	**0**

[4] This field only appears when the "Dial on demand (with idle timeout timer)" field is activated (box checked).

Field	Action	Default
PPP IP extension	Check the box to allocate your computer the public address obtained from the DHCP server of your **I**nternet **S**ervice **P**rovider (ISP). Your router will then act as a bridge between the server and your computer.	**Not checked**
Use Static IP Address	Check the box to use the static IP address.	**Not checked**
IP Address:[5]	Enter the static IP address	**0.0.0.0**
Configure PPP MTU	Enter an MTU (**M**aximum **T**ransfer **U**nit) value between 38 and 1492 (see Note).	**1492**
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.	**Box Not checked**

Note: The MTU specifies the maximum size of the data used for packets expressed as a number of bytes.

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

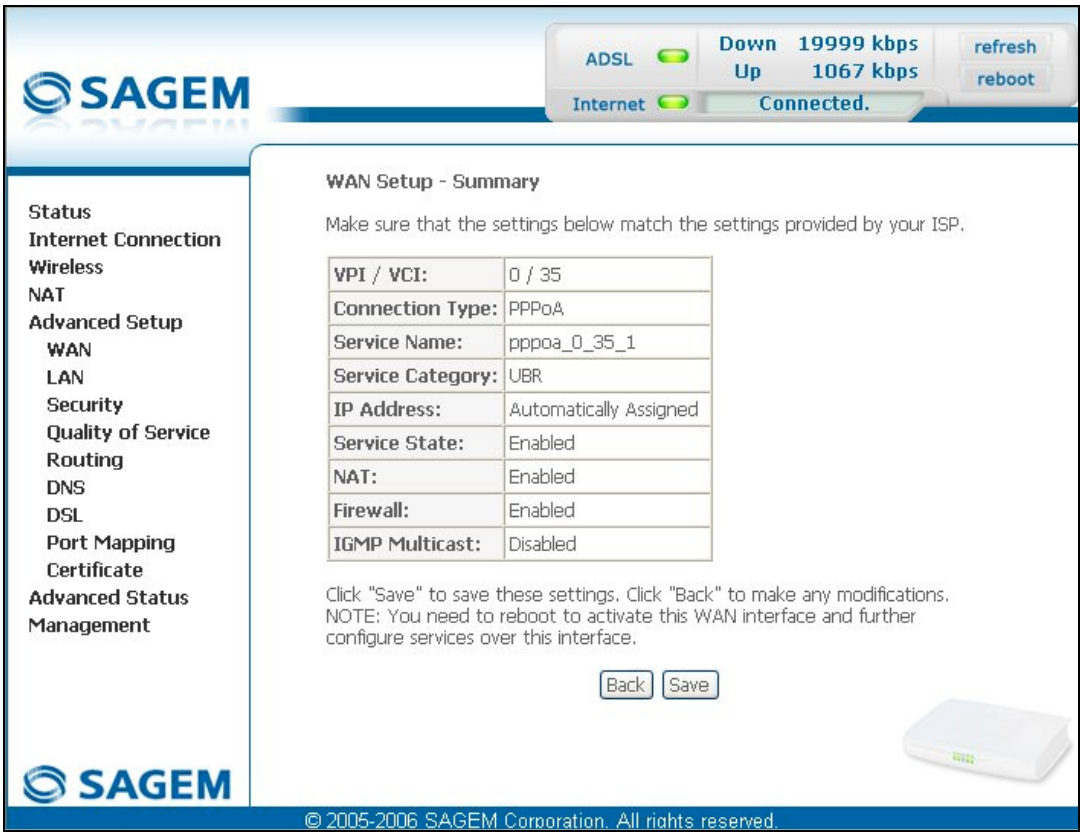


[5] This field only appears when the "Use Static IP Address" field is activated (box checked).

Field	Action	Default
Enable NAT	Check the box to activate the NAT function.	**Checked**
Enable Firewall	Check the box to activate the Firewall service.	**Checked**
Enable IGMP Multicast	Check the box to activate the IGMP function.	**Not checked**
Enable WAN Service	Check the box to activate the remote network service (WAN). See the note of **information** below.	**Checked**
Service Name	Displays the name of the service being configured. This name, which is allocated automatically, is made up as follows: Protocol_VPI_VCI_Index For example: pppoa_0_35_1. **Note:** You may enter another service name.	pppoa_0_35_1

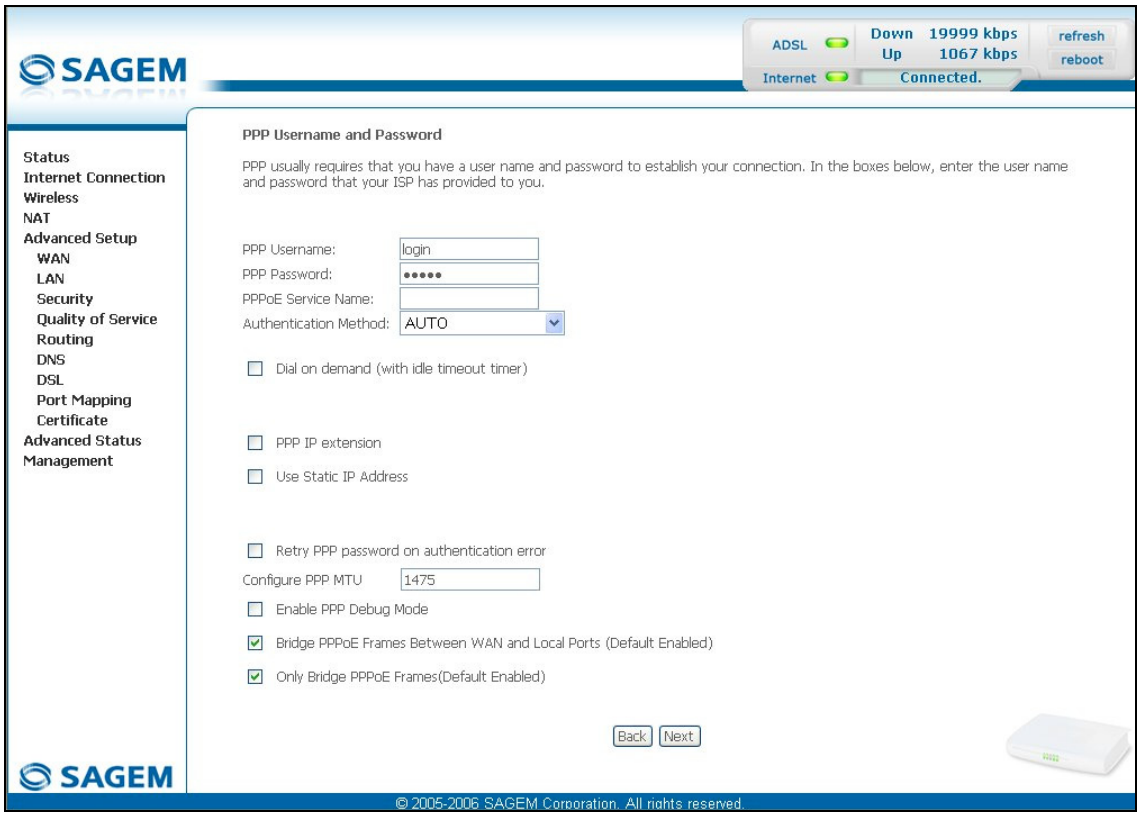
The "**Enable WAN Service**" function makes it possible to disable connection types in a list to use only the selected connection type. The "**WAN**" menu of the "**Advanced Status**" section shows the "State is disable" if "**Enable WAN Service**" has not been selected.

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



Field	Action
VPI/VCI	Displays the VPI/VCI specific to the "PPPoA" connection
Connection Type	Displays the "PPPoA" protocol
Service Name	Displays the name of the service: pppoa_0_35_1
Service Category	Displays the type of service adapted to the traffic required.
IP Address	Indicates that the IP address is allocated automatically: **Automaticaly Assigned**
Service State	Displays the status of the service: **Enabled**
NAT	Displays the status of the NAT: **Enabled**
Firewall	Displays the status of the firewall: **Enabled**
IGMP Multicast	Displays the status of the IGMP function: **Disabled**

PPP over Ethernet (PPPoE)

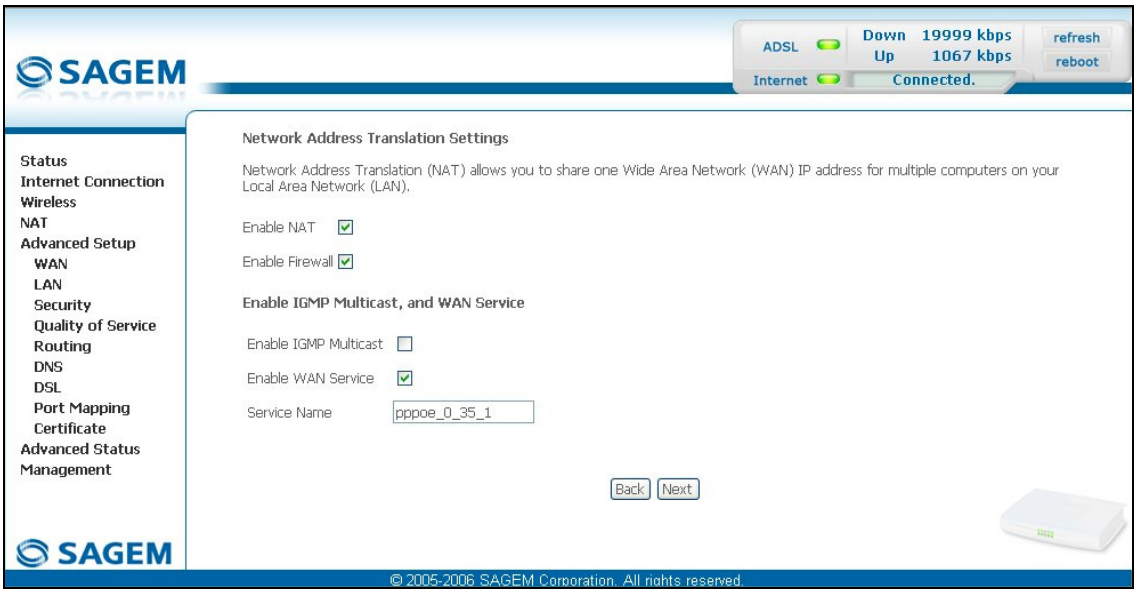


Field	Action	Default
PPP Username	Enter your connection ID. This information is provided to you by your **I**nternet **S**ervice **P**rovider (ISP).	**Empty**
PPP Password	Enter your connection password. This information is provided to you by your **I**nternet **S**ervice **P**rovider (ISP).	**Empty**
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).	**Empty**
Authentification 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 only connect to the Internet on "Traffic".	**–**
Inactivity Timeout (minutes) [1-4320]:[4]	Enter the inactivity time. This value (in minutes) is between 1 and 4320 (i.e. 72 hours). If there is no traffic for a certain period of time, the PPPoE session is interrupted.	**0**

Field	Action	Default
PPP IP extension	Check the box to allocate the public address obtained from the DHCP server of your **I**nternet **S**ervice **P**rovider (ISP) to your computer. Your router will then act as a bridge between the server and your computer.	–
Use Static IP Address	Check the box to use the static IP address.	–
IP Address:[5]	Enter the static IP address.	**0.0.0.0**
Retry PPP password on authentication error	Check the box, PPP can be retried again and again while authentication fails	**Box Not checked**
Configure PPP MTU	Enter an MTU (**M**aximum **T**ransfer **U**nit) value. This value (in bytes) is between 38 and 1492 (see Note).	**1492**
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.	**Box 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	**Checked**
Only Bridge PPPoE Frames	Check the box to filter out all the non-PPPoE packets when bridging the frames between WAN and local ports.	**Checked**

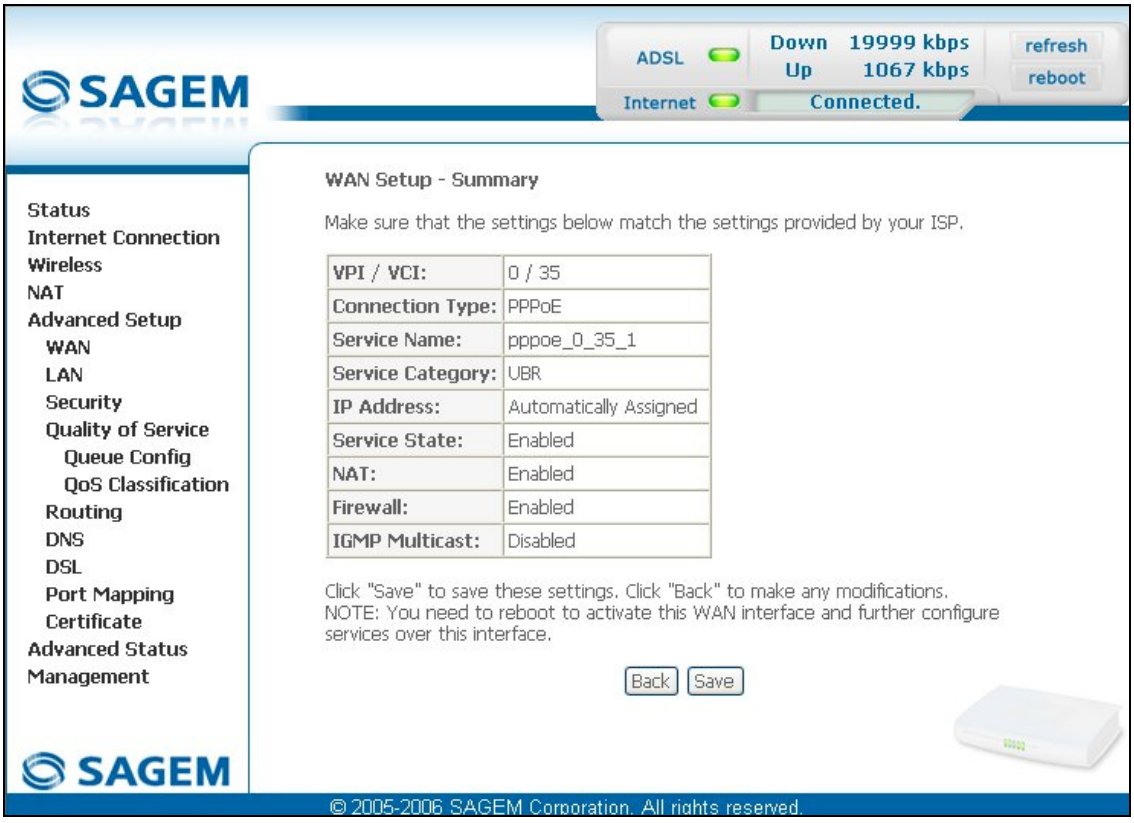
Note: The MTU specifies the maximum size of the data used (IP packets) expressed as a number of bytes.

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



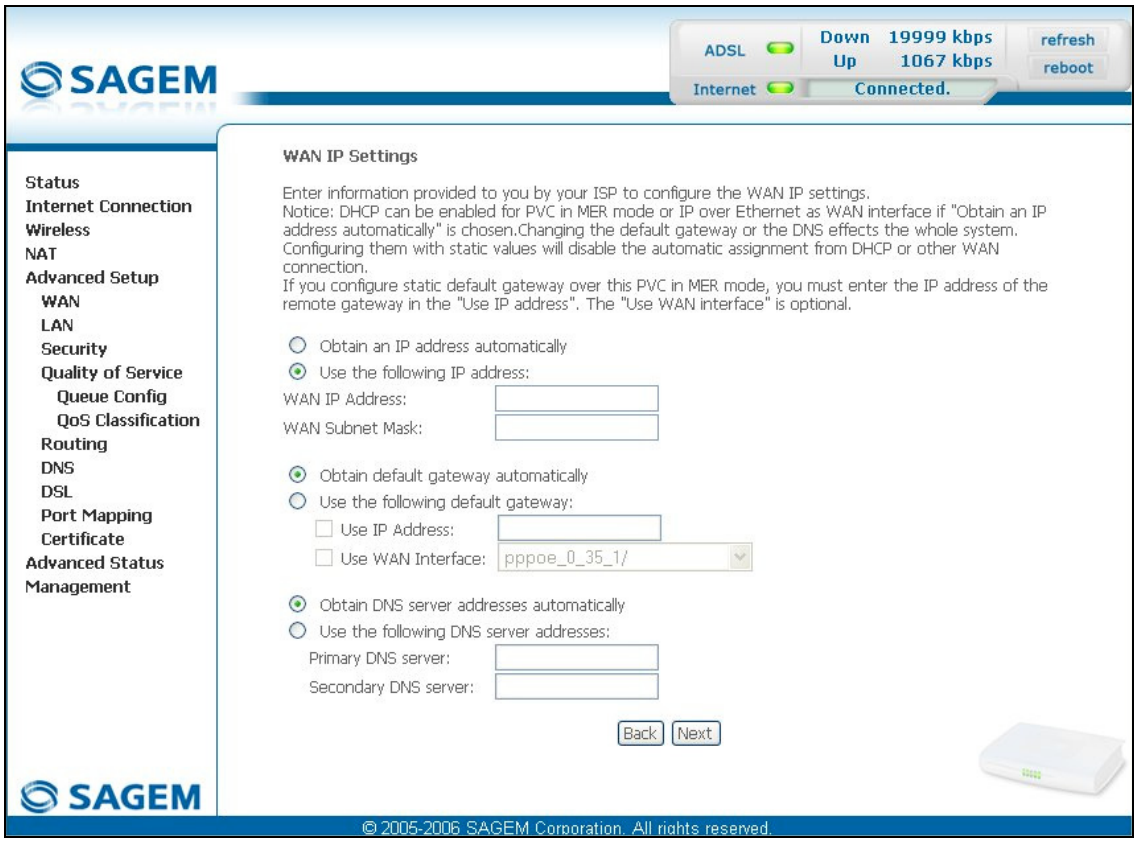
Field	Action	Default
Enable NAT	Check the box to activate the NAT function.	**Checked**
Enable Firewall	Check the box to activate the Firewall service.	**Checked**
Enable IGMP Multicast	Check the box to activate the IGMP function.	**Not checked**
Enable WAN Service	Check the box to activate the WAN service.	**Checked**
Service Name	Displays the name of the service being configured. This name, which is allocated automatically, is made up as follows: Protocol_VPI_VCI_Index For example: pppoe_0_35_1. **Note:** You may enter another service name.	pppoe_0_35_1

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



Field	Action
VPI/VCI	Displays the VPI/VCI specific to the "PPPoE" connection
Connection Type	Displays the "PPPoE" protocol
Service Name	Displays the name of the service: pppoe_0_35_1
Service Category	Displays the type of service adapted to the traffic required.
IP Address	Indicates that the IP address is allocated automatically: **Automaticaly Assigned**
Service State	Displays the status of the service: **Enabled**
NAT	Displays the status of the NAT: **Enabled**
Firewall	Displays the status of the firewall: **Enabled**
IGMP Multicast	Displays the status of the IGMP function: **Disabled**

MAC Encapsulation Routing (MER)



Field	Action	Default
Obtain an IP address automatically	Check the box to obtain an IP address automatically from your router's DHCP server.	**Box Not checked**
Use the following IP address:	If you check this box, you must enter a static IP address and the dedicated subnet mask.	**Box checked**
WAN IP Address[6]	Enter the static IP address.	**0.0.0.0**
WAN Subnet Mask:[6]	Enter the subnet mask.	**0.0.0.0**
Obtain default gateway automatically	Check the box to obtain the gateway IP address automatically from your router's DHCP server.	**Box checked**
Use the following default gateway:	If you check this box, you must enter the default gateway address.	**–**
Use IP Address[7]	Enter the default gateway address.	**–**
Use WAN Interface:[7]	Select the WAN interface of your choice from the scroll down list (optional)	**–**

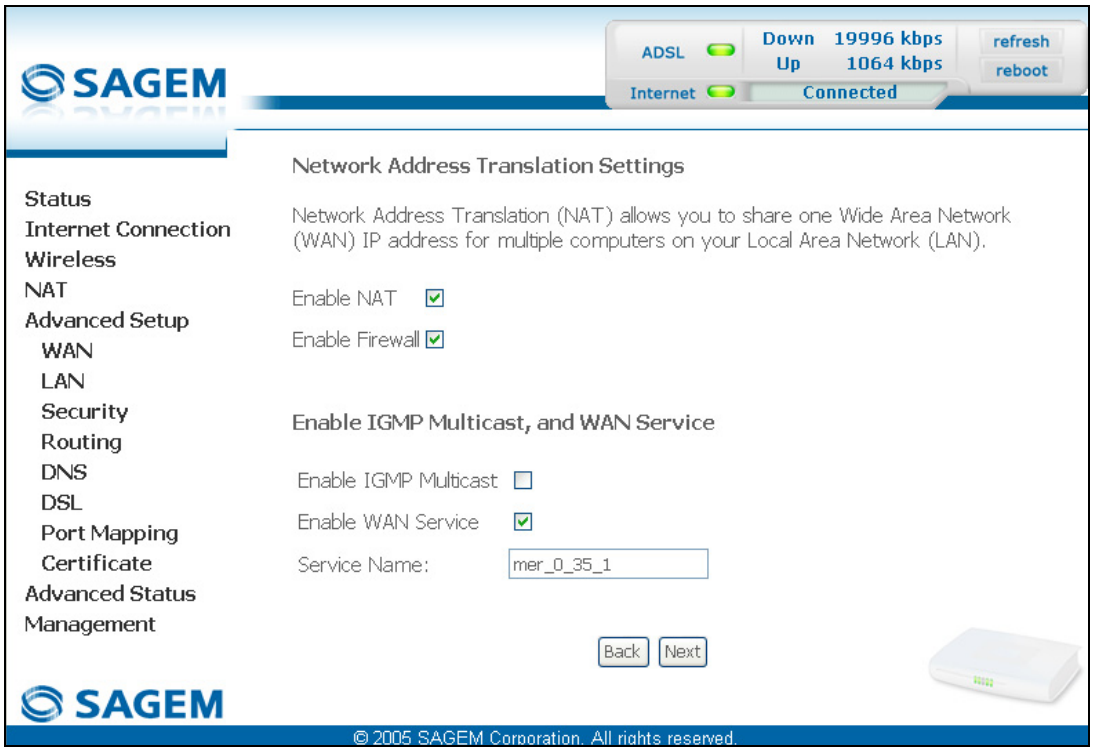
[6] This field only appears when the "Use the following IP address:" field is activated (box checked).

[7] This field only appears when the "Use the following default gateway:" field is activated (box checked).

Field	Action	Default
Obtain DNS server addresses automatically	Check the box to obtain DNS server addresses automatically.	**Box checked**
Use the following DNS server addresses:	If you check this box, you must enter DNS server addresses.	_
Primary DNS server[8]	Enter a primary DNS server address.	_
Secondary DNS server[8]	Enter a secondary DNS server address.	_

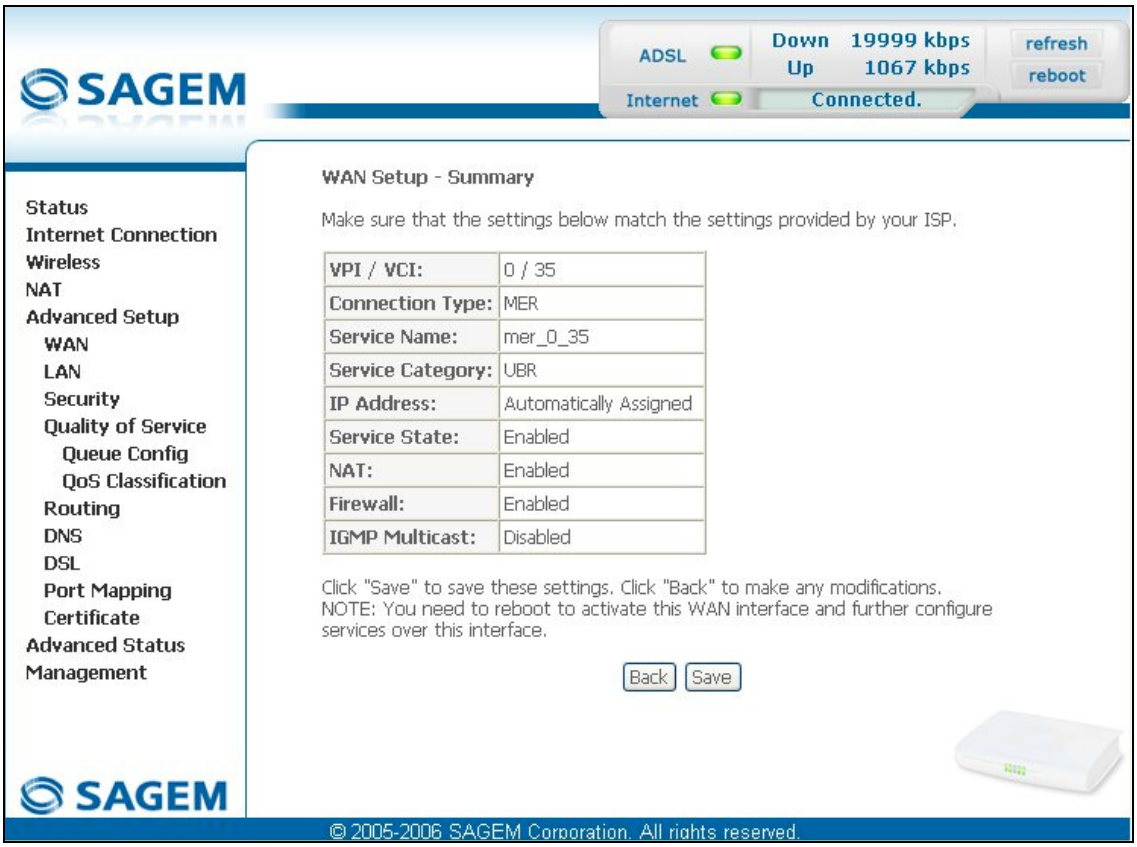
[8] This field only appears when the "Use the following DNS server addresses:" field is activated (box checked).

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



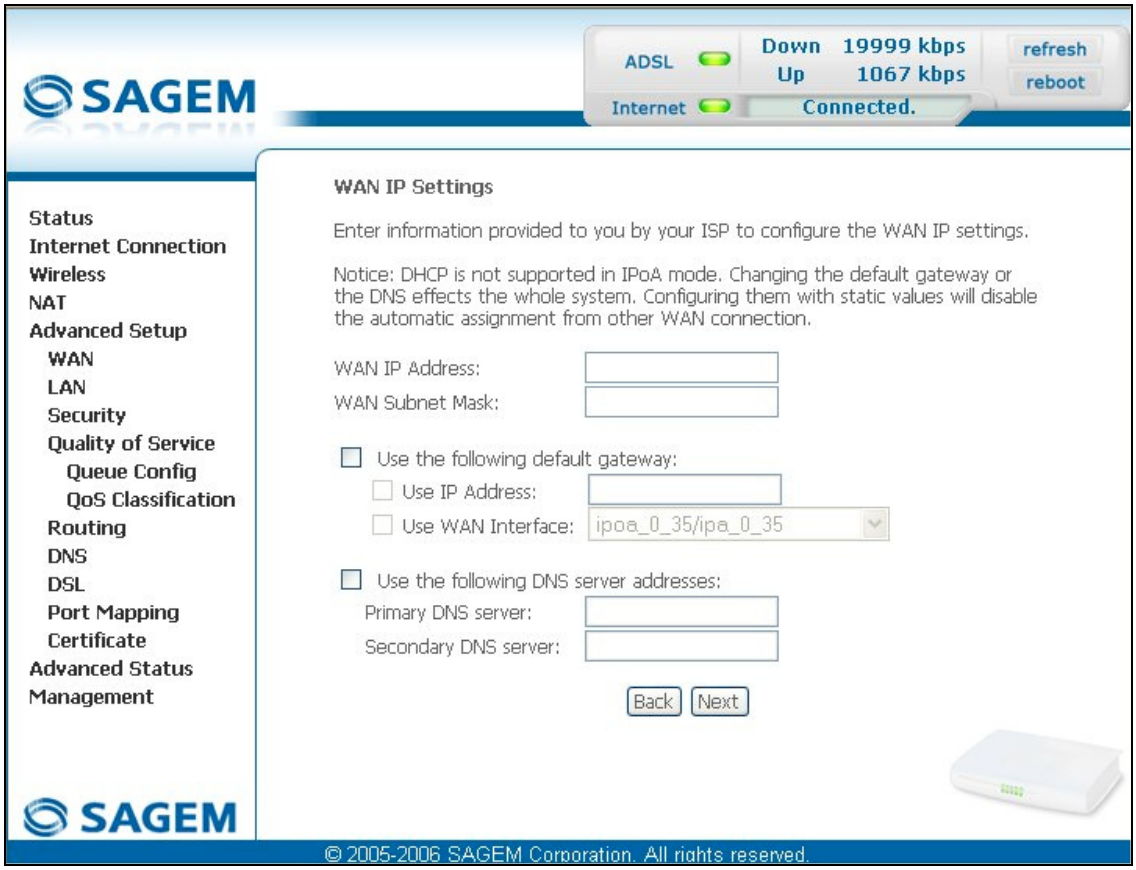
Field	Action	Default
Enable NAT	Check the box to activate the NAT function.	**Checked**
Enable Firewall	Check the box to activate the firewall service.	**Checked**
Enable IGMP Multicast	Check the box to activate the IGMP function.	**Not checked**
Enable WAN Service	Check the box to activate the WAN service.	**Checked**
Service Name	Displays the name of the service being configured. This name, which is allocated automatically, is made up as follows: Protocol_VPI_VCI_Index For example: mer_0_35_1. **Note:** You may enter a different service name.	mer_0_35_1

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



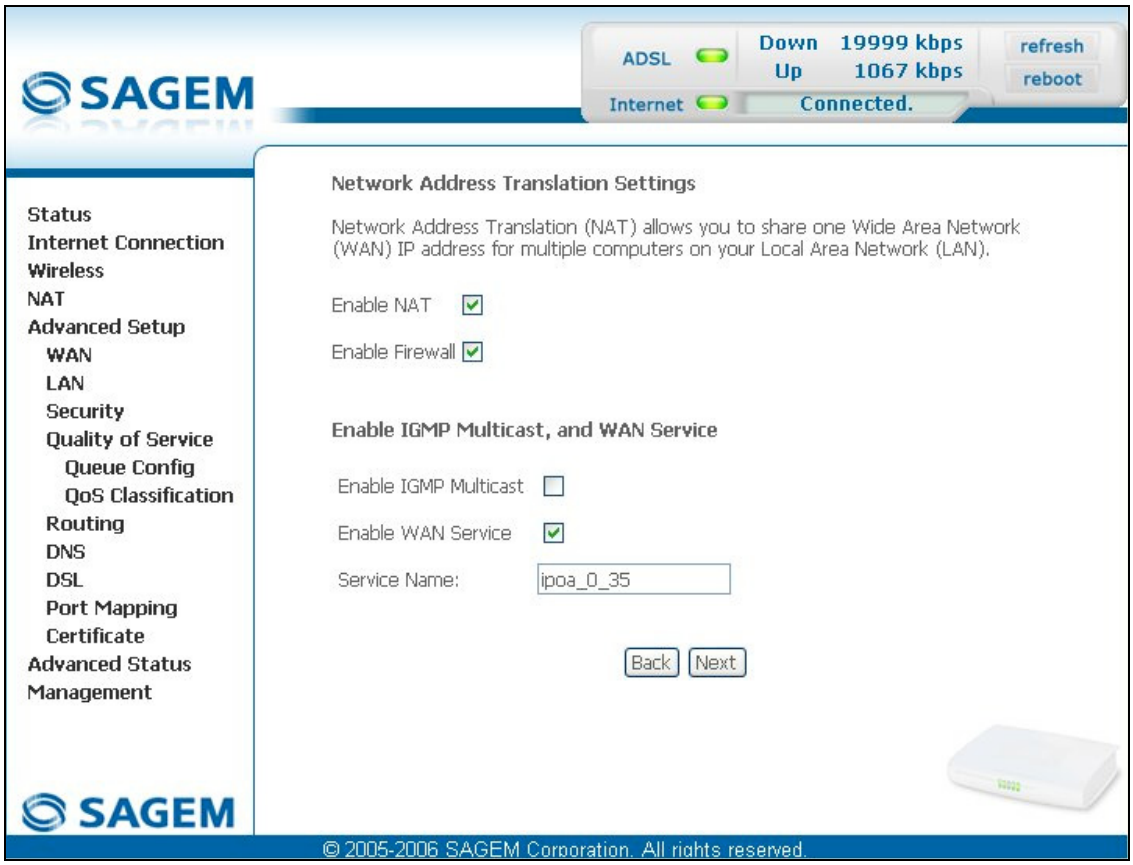
Field	Action
VPI/VCI	Displays the VPI/VCI specific to the "MER" connection
Connection Type	Displays the "MER" protocol
Service Name	Displays the name of the service: mer_0_35_1
Service Category	Displays the type of service adapted to the traffic required.
IP Address	Indicates that the IP address is allocated automatically: **Automatically Assigned**
Service State	Displays the status of the service: **Enabled**
NAT	Displays the status of the NAT: **Enabled**
Firewall	Displays the status of the firewall: **Enabled**
IGMP Multicast	Displays the status of the IGMP function: **Disabled**

IP over ATM (IPoA)



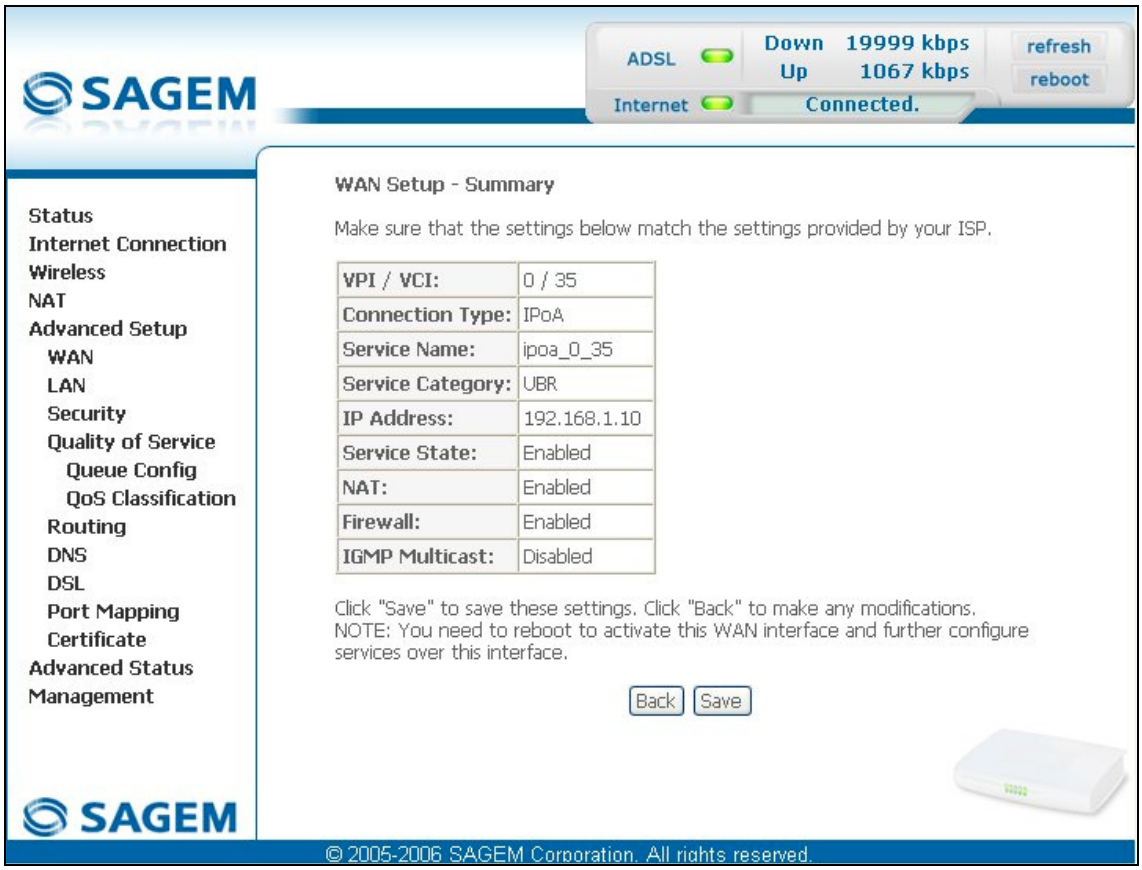
Field	Action	Default
WAN IP Address[6]	Enter the static IP address.	**0.0.0.0**
WAN Subnet Mask:[6]	Enter a subnet mask.	**0.0.0.0**
Use the following default gateway:	If you check this box, you must enter a default gateway address.	**_**
Use IP Address[7]	Enter the default gateway address.	**_**
Use WAN Interface:[7]	Select the WAN interface of your choice from the scroll down list (optional)	**_**
Obtain DNS server addresses automatically	Check the box to obtain DNS server addresses automatically.	**Box checked**
Use the following DNS server addresses:	If you check this box, you must enter DNS server addresses.	**_**
Primary DNS server[8]	Enter a primary server DNS Address.	**_**
Secondary DNS server[8]	Enter a secondary server DNS Address.	**_**

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



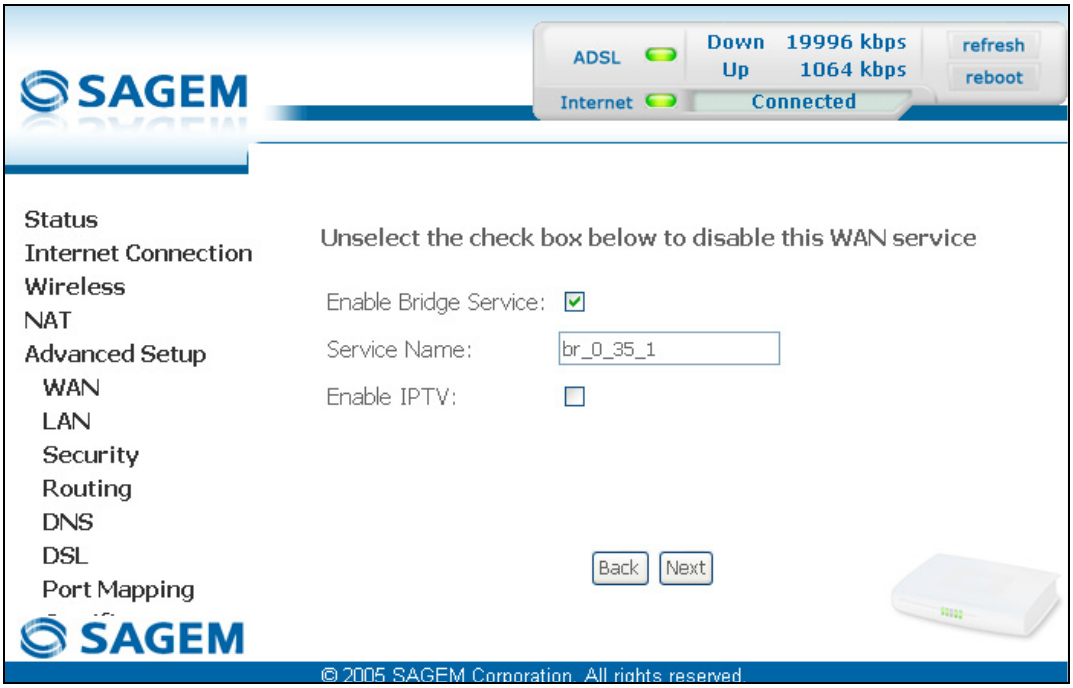
Field	Action	Default
Enable NAT	Check the box to activate the NAT function.	**Box checked**
Enable Firewall	Check the box to activate the firewall service.	**Box checked**
Enable IGMP Multicast	Check the box to activate the IGMP function.	**Box not checked**
Enable WAN Service	Check the box to activate the WAN service.	**Box checked**
Service Name	Displays the name of the service being configured. This name, which is allocated automatically, is made up as follows: Protocol_VPI_VCI_Index For example: ipoa _0_35_1. **Note:** You may enter another service name.	ipoa_0_35_1

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

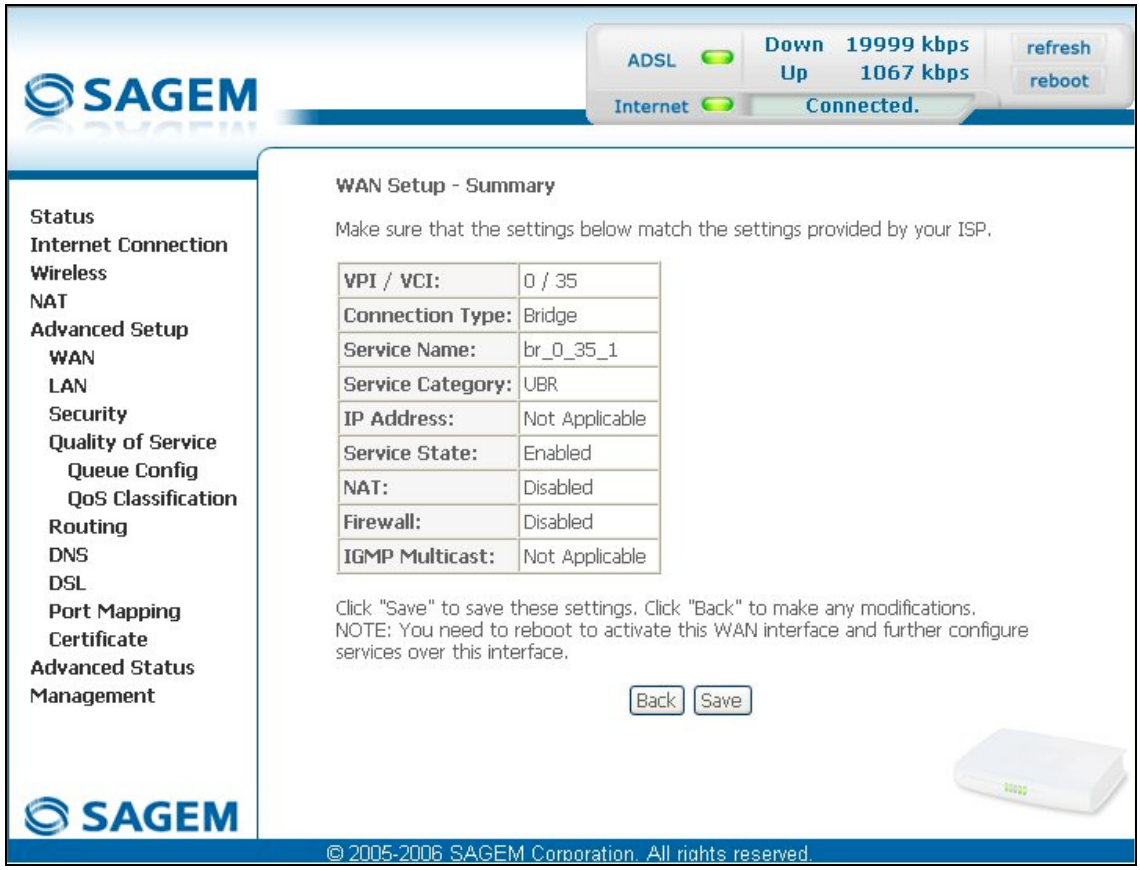


Field	Action
VPI/VCI	Displays the VPI/VCI specific to the "IPoA" connection
Connection Type	Displays the "IPoA" protocol
Service Name	Displays the name of the service: ipoa_0_35_1
Service Category	Displays the type of service adapted to the traffic required.
IP Address	Displays the IP address entered: 192.168.1.10
Service State	Displays the status of the service: **Enabled**
NAT	Displays the status of the NAT: **Enabled**
Firewall	Displays the status of the firewall: **Enabled**
IGMP Multicast	Displays the status of the IGMP function: **Disabled**

Bridging

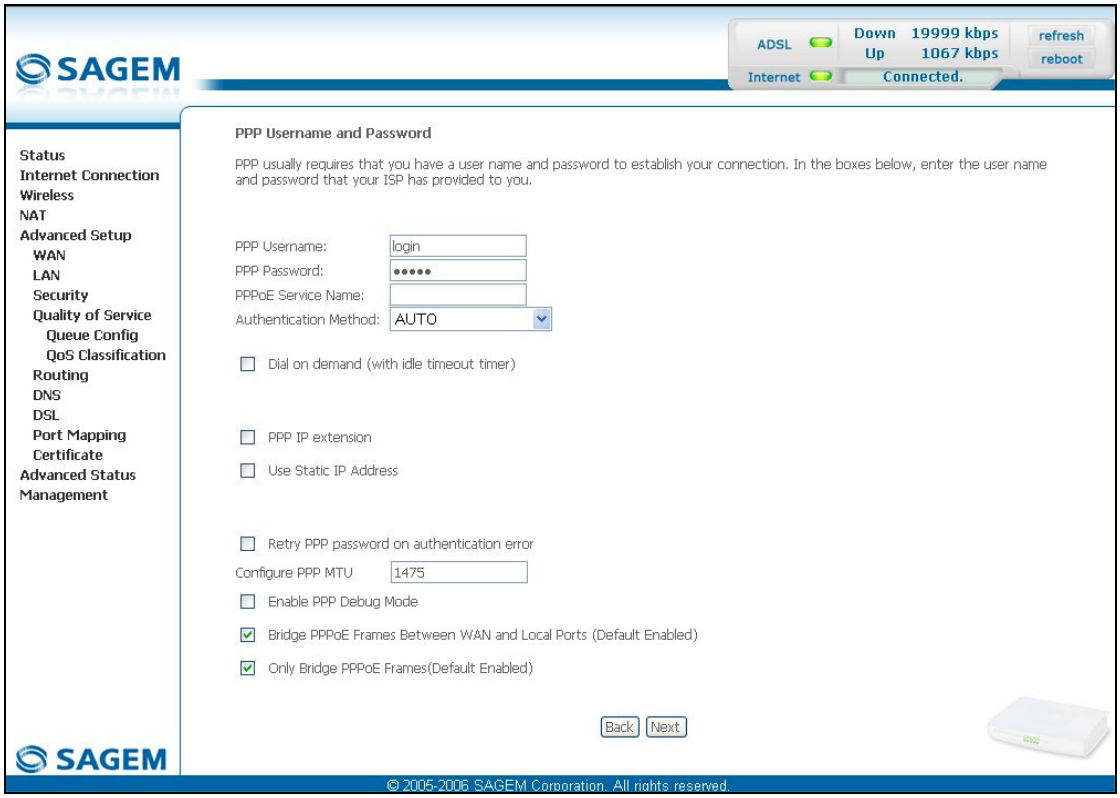


Field	Action	Default
Enable Bridge service	Check the box to activate the "Bridge" service.	**Box checked**
Service Name	Displays the name of the service being configured. This name, which is allocated automatically, is made up as follows: Protocol_VPI_VCI_Index (For example: br_8_35_1. **Note:** You may enter another service name.	–
Enable IPTV	Check the box to be able to enter another IP address of the external network of the "Set Top Box" connected virtually to this "PVC".	–
IPTV Name	This field only appears if the **Enable IPTV** box in the previous field is checked. Enter the IP address of the external network of the "Set Top Box" connected virtually to this "PVC".	–



Field	Action
VPI/VCI	Displays the VPI/VCI specific to the "Bridge" connection
Connection Type	Displays the "Bridge" protocol
Service Name	Displays the name of the service: br_0_35_1
Service Category	Displays the type of service adapted to the traffic required
IP Address	In the "Bridge" connection, this field is: **Not Applicable**
Service State	Displays the status of the service: **Enabled**
NAT	Displays the status of the NAT: **Disabled**
Firewall	Displays the status of the firewall: **Disabled**
IGMP Multicast	In the "Bridge" connection, this field is: **Not Applicable**

PPPoE/PPPoA

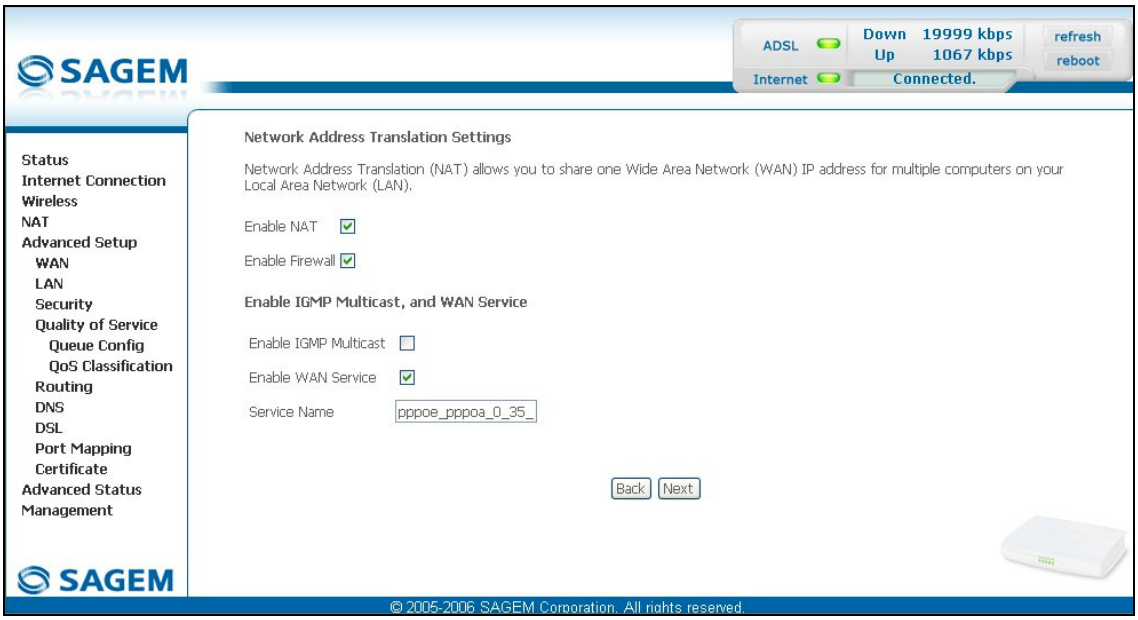


Field	Action	Default
PPP Username	Enter your connection ID. This information is provided to you by your **I**nternet **S**ervice **P**rovider (ISP).	**Empty**
PPP Password	Enter your connection password. This information is provided to you by your **I**nternet **S**ervice **P**rovider (ISP).	**Empty**
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).	**Empty**
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 only connect to the Internet on "Traffic".	**–**
Inactivity Timeout (minutes) [1-4320]:[4]	Enter the inactivity time. This value (in minutes) is between 1 and 4320 (i.e. 72 hours). If there is no traffic for a certain period of time, the PPPoE/PPPoA session is interrupted.	**0**

Field	Action	Default
PPP IP extension	Check the box to allocate the public address obtained from the DHCP server of your **I**nternet **S**ervice **P**rovider (ISP) to your computer. Your router will then act as a bridge between the server and your computer.	–
Use Static IP Address	Check the box to use the static IP address.	–
IP Address:[5]	Enter the static IP address.	**0.0.0.0**
Retry PPP password on authentication error		**Box Not checked**
Configure PPP MTU	Enter an MTU (**M**aximum **T**ransfer **U**nit) value. This value (in bytes) is between 38 and 1492 (see Note).	**1492**
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.	**Box 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	**Checked**
Only Bridge PPPoE Frames	Check the box to filter out all the non-PPPoE packets when bridging the frames between WAN and local ports.	**Checked**

Note: The MTU specifies the maximum size of the data used (IP packets) expressed as a number of bytes.

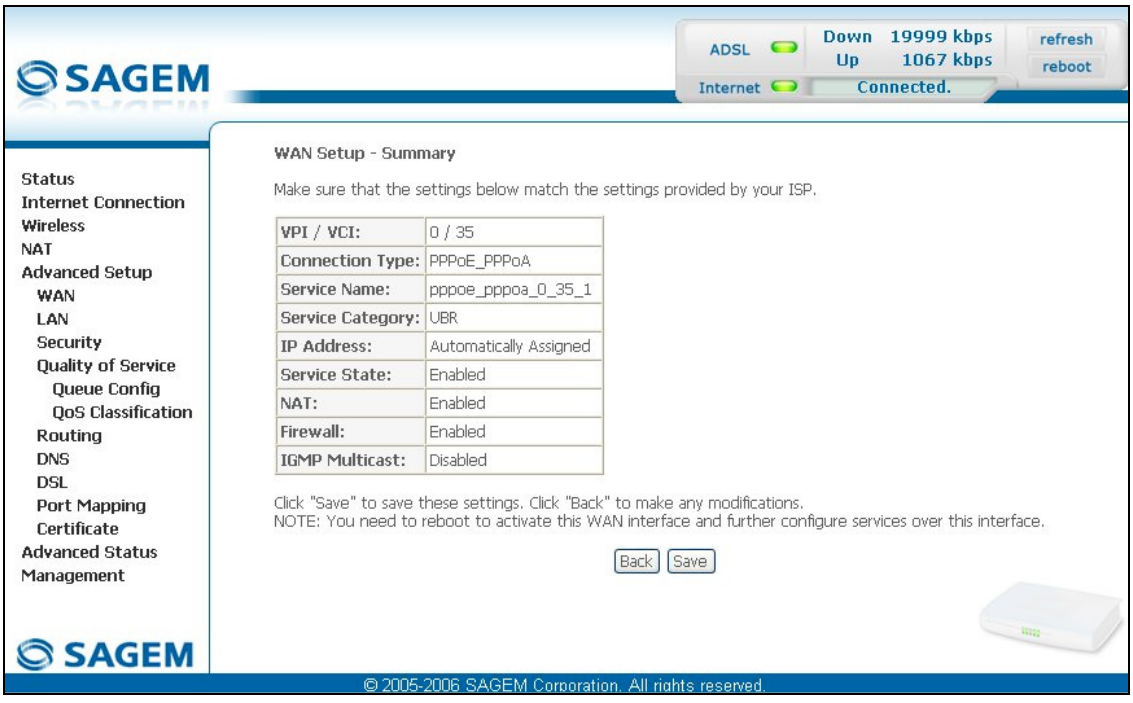
- Click on the **Next** button to continue configuring the remote network (WAN) in PPPoE/PPPoA mode.



Field	Action	Default
Enable NAT	Check the box to activate the NAT function.	**Checked**
Enable Firewall	Check the box to activate the Firewall service.	**Checked**
Enable IGMP Multicast	Check the box to activate the IGMP function.	**Not checked**
Enable WAN Service	Check the box to activate the remote network service (WAN). See the note of **information** below.	**Checked**
Service Name	Displays the name of the service being configured. This name, which is allocated automatically, is made up as follows: Protocol_VPI_VCI_Index For example: pppoe_pppoa_0_35_1. **Note:** You may enter another service name.	pppoe_pppoa_0_35_1

The "**Enable WAN Service**" function makes it possible to disable connection types in a list to use only the selected connection type.

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

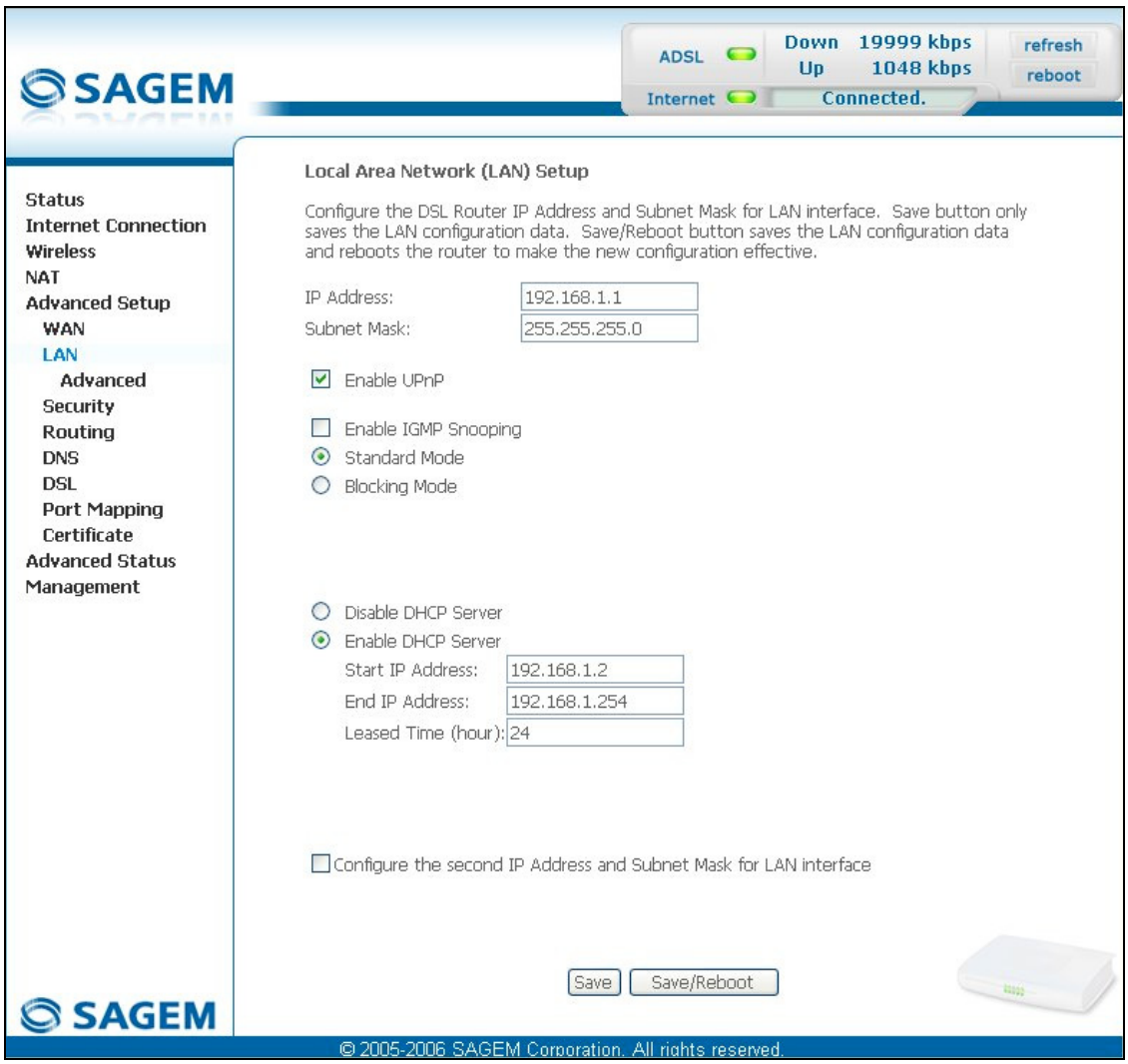


Field	Action
VPI/VCI	Displays the VPI/VCI specific to the "PPPoE" connection
Connection Type	Displays the "PPPoE/PPPoA" protocol
Service Name	Displays the name of the service: pppoe_pppoa_0_35_1
Service Category	Displays the type of service adapted to the traffic required.
IP Address	Indicates that the IP address is allocated automatically: **Automatically Assigned**
Service State	Displays the status of the service: **Enabled**
NAT	Displays the status of the NAT: **Enabled**
Firewall	Displays the status of the firewall: **Enabled**
IGMP Multicast	Displays the status of the IGMP function: **Disabled**

5.9.2 LAN

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

- Select the **LAN** menu in the **Advanced Setup** section to display the following screen:



Field	Action	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 UPnP	Check the box to activate the "UpnP" function. **Note:** This function lets you automatically: • join a network dynamically, • obtain an IP address.	**Box checked**
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.	**Box not checked**

Field	Action	Default
Standard Mode	Check the box if you wish the IGMP snooping runs in normal mode (transparency with IGMP frames).	**Box checked**
Blocking Mode	Check the box if you wish the IGMP snooping runs in blocking mode (interception and removal of IGMP frames).	**Box not checked**
Disable DHCP	Check this box to not activate 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.	**Box not checked**
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).	**Box checked**
Start IP Address	Enter the first address attributed by your router's DHCP server.	**192.168.1.2**
End IP Address[9]	Enter the last address attributed by your router's DHCP server.	**192.168.1.254**
Lease Time (hour)[9]	Enter an unavailability time (in hours) for each attributed address.	**24**
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).	**Box not checked**
IP Address[10]	Enter a second address for your local network (LAN).	**–**
Subnet Mask[10]	Enter a subnet mask for the second address for your local network (LAN).	**–**

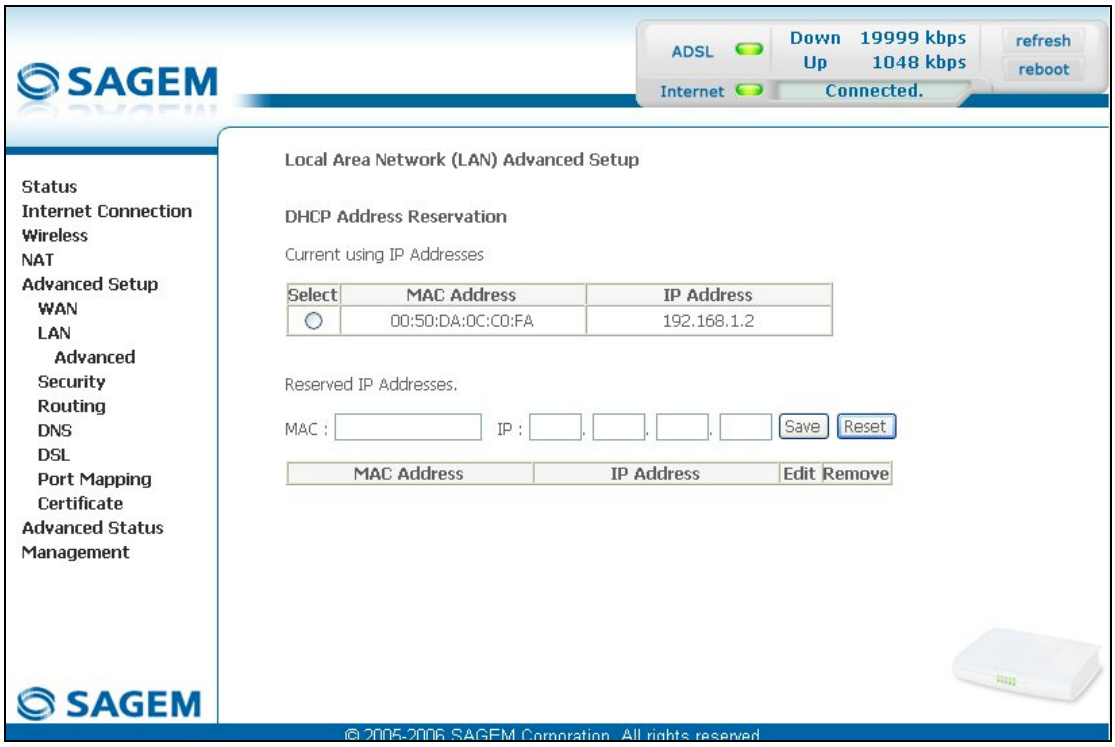
[9] This field only appears when the "Enable DHCP" field is activated (box checked).

[10] This field only appears when the "Configure the second IP Address and Subnet Mask for LAN interface" field is activated (box checked).

5.9.2.1 Advanced

Object: This allows to display addresses delivered by your router's DHCP server and reserve any addresses.

- Select the **LAN** menu then the **Advanced** submenu in the **Advanced Setup** section to display the following screen:

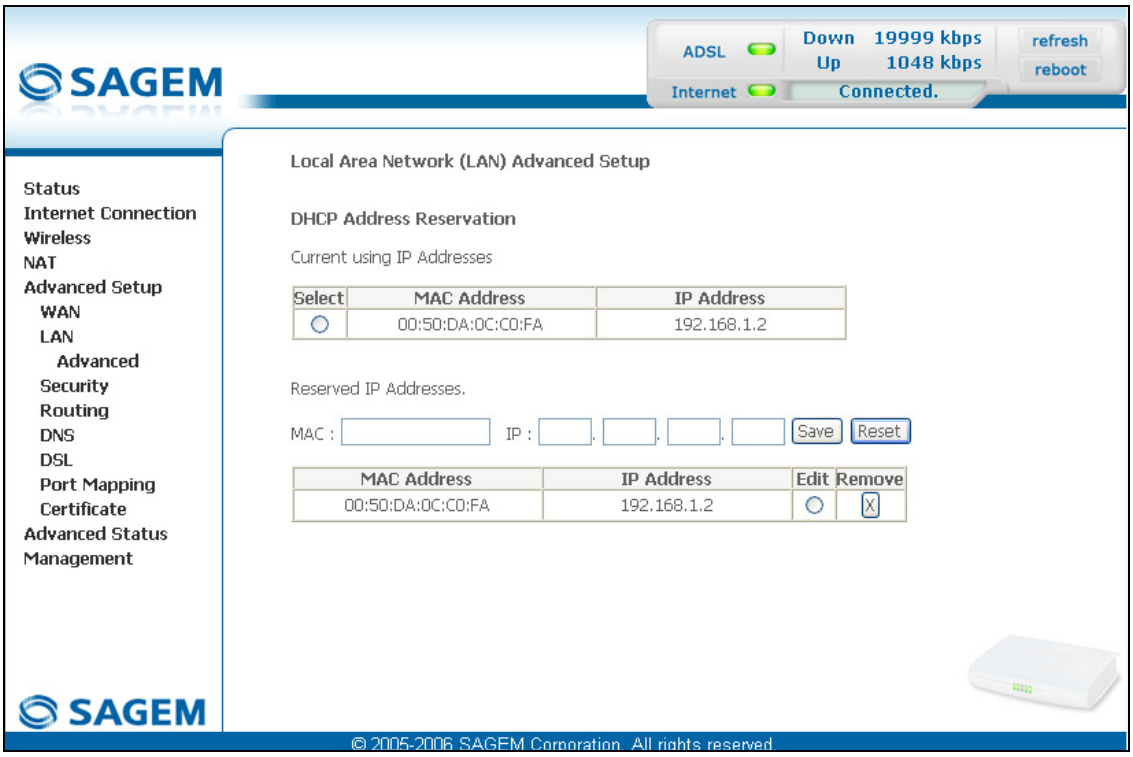


Current using IP addresses

Field	Action	Default
MAC Address	Displays the **MAC Address** of a computer connected to your router. This computer can be part of a LAN (**L**ocal **A**rea **N**etwork).	**00:50:DA:0C:C0:FA**
IP Address	Displays the **IP Address** delivered by your router's DHCP server to your computer.	**192.168.1.1**

Reserved IP addresses

To reserve the current address, check the "**Select**" box; both "**MAC Address**" and "**IP Address**" fields appear in the relevant fields of the "**Reserved IP Addresses**" area, then click on the Save button.

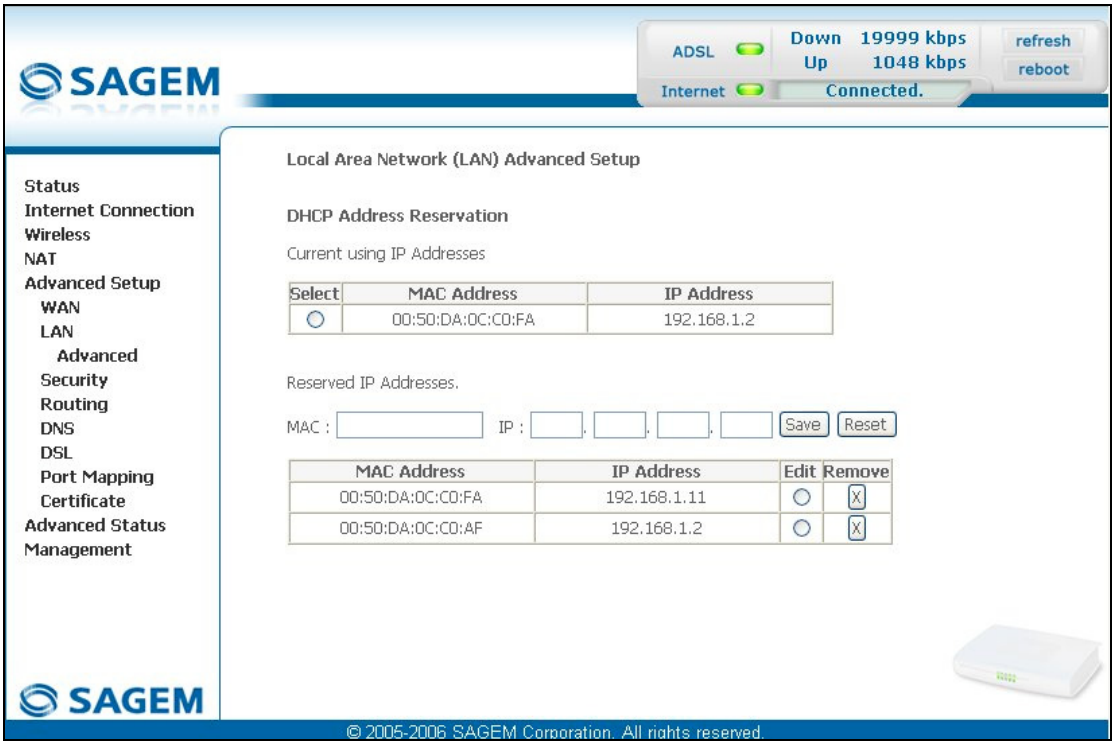


To reserve the other addresses, two methods are possible:

- Check the "**Select**" box; both "**MAC Address**" and "**IP Address**" fields appear in the relevant fields of the "**Reserved IP Addresses**" area then click on the Save button.

or

- Enter the "**MAC Address**" and "**IP Address**" in the relevant fields then click on the Save button.



Buttons

Save	Click on this button to take into account the entry of both "**MAC Address**" and "**IP Address**" fields. Then these ones appear in a table.
Reset	Click on this button to clear both "**MAC Address**" and "**IP Address**" fields.

Boxes

Edit	Check in the box to modify **MAC Address** or **IP Address** of the table.
Remove	Click in the box to delete **MAC Address** and **IP Address** of the table.

All the reserved addresses belong to the range of addresses assigned by router's DHCP server (192.168.1.2 to 192.168.1.254).

5.9.3 Security

This menu contains 2 sub-menus:

- IP Filtering (see subsection 5.9.3.1),
- Block Sites (see subsection 5.9.3.2).

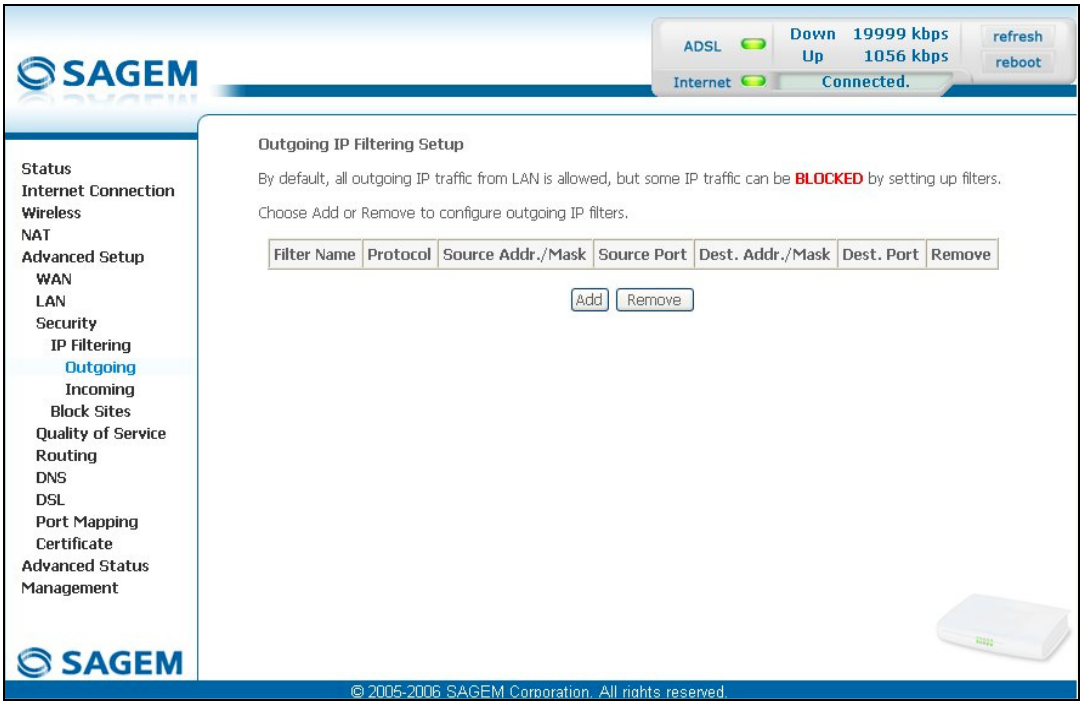
5.9.3.1 IP Filtering

5.9.3.1.1 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.

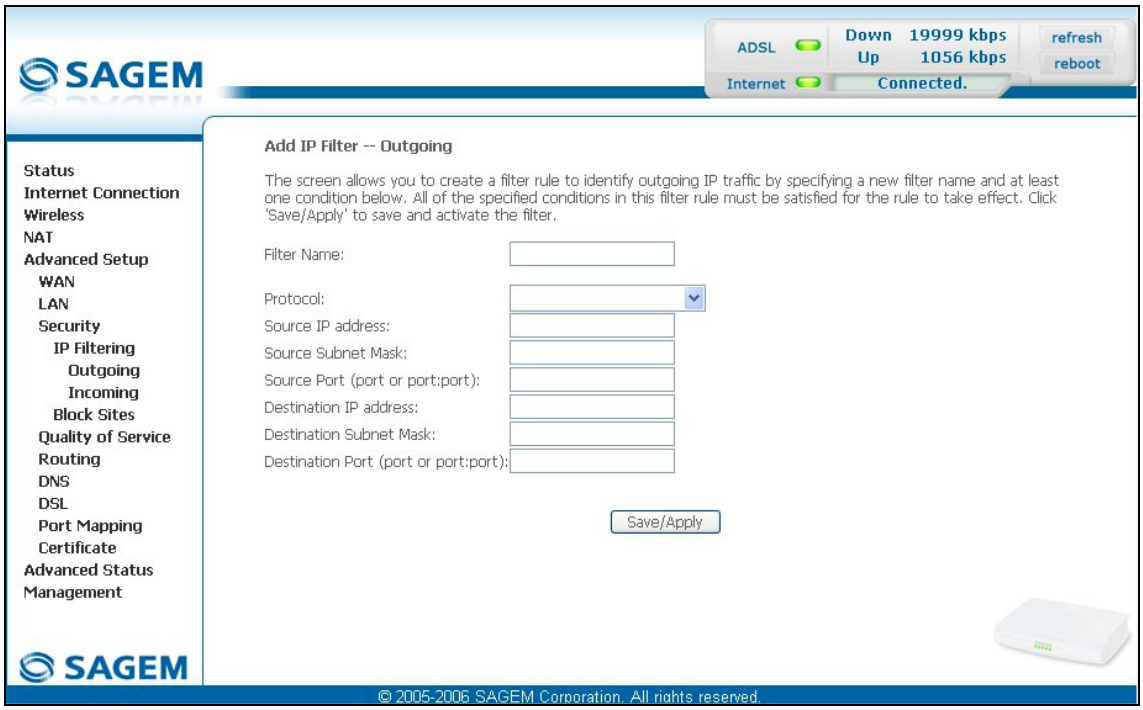
- Select the **Outgoing** sub-menu in the **Security** menu in the **Advanced Setup** section to display the following screen:



Field	Meaning
Filter Name	Name of the filter.
Protocol	Transport protocol.
Source Address / Mask	Source IP address / Subnet mask.
Source Port	Source port
Dest. Address / Mask	Destination IP address / Subnet mask.
Dest. Port	Destination port.

Add

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



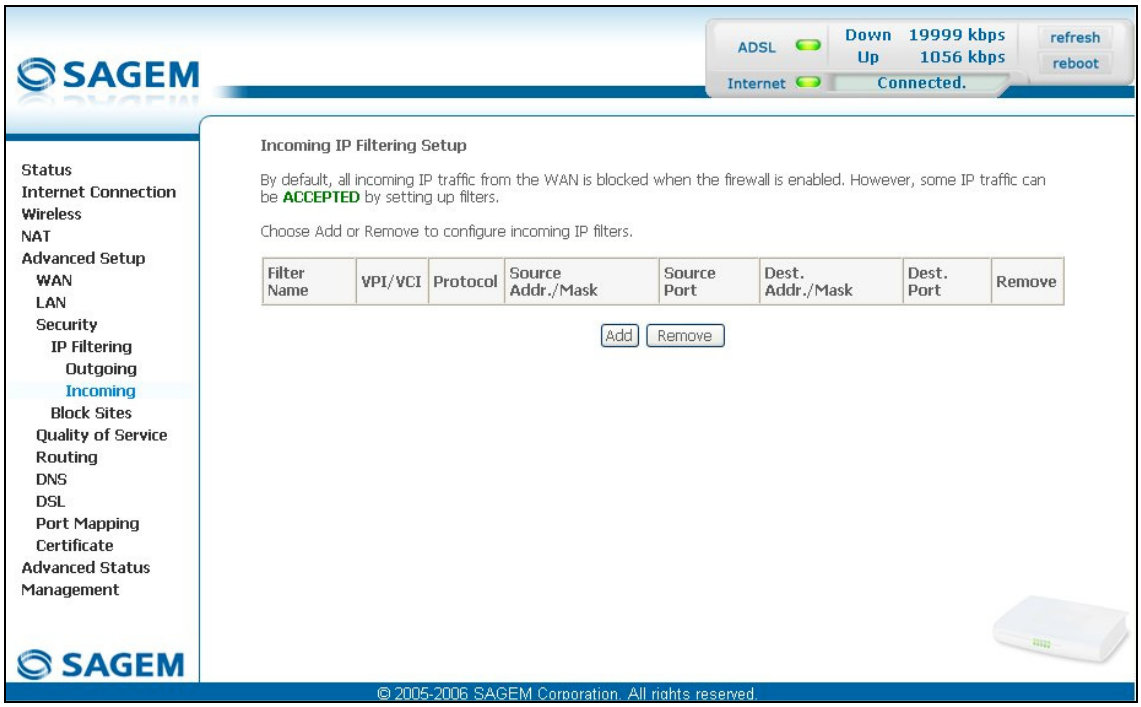
Field	Action
Filter Name	Enter a representative name for the filter.
Protocol	Select the dedicated protocol from the scroll down list (TCP/UDP, TCP, UDP, ICMP).
Source IP Address	Enter the Source IP address (LAN).
Source Subnet Mask	Subnet mask.
Source Port (port or port:port)	Enter a "Source" port (LAN)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

5.9.3.1.2 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.

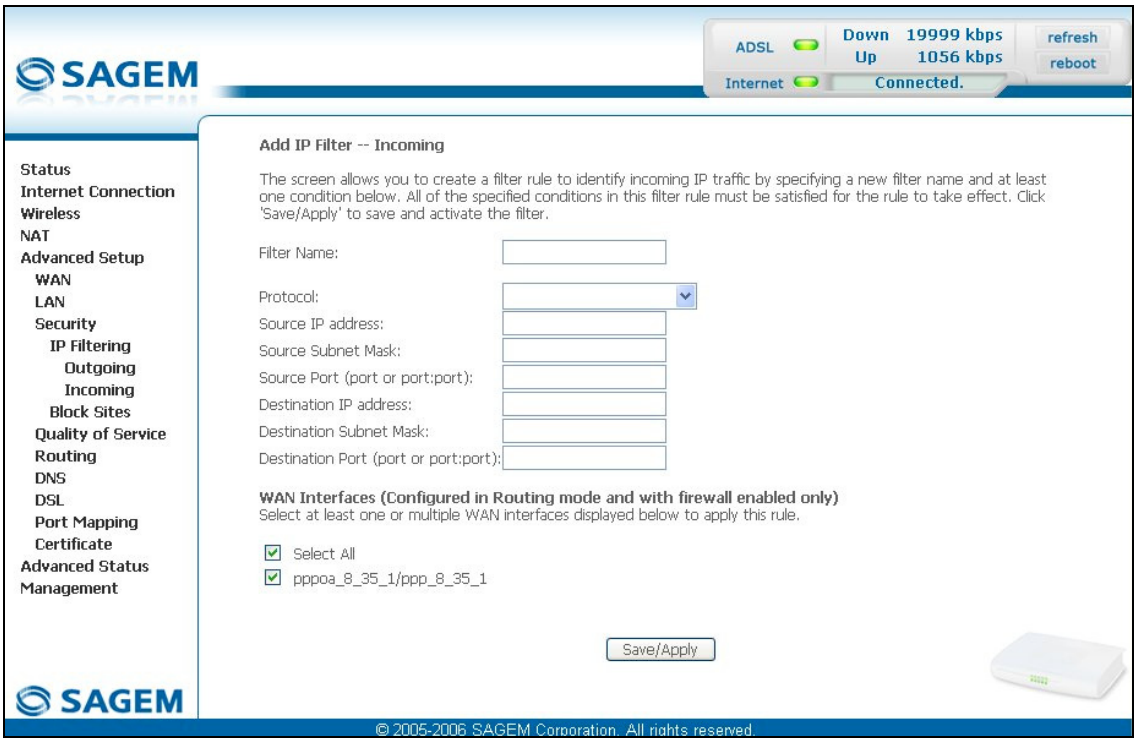
By default, all the incoming data is refused when the Firewall is activated.

- Select the **Incoming** sub-menu in the **Security** menu in the **Advanced Setup** section to display the following screen:



Add

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



Field	Action
Filter Name	Enter a representative name for the filter.
Protocol	Select the dedicated protocol from the scroll down list (TCP/UDP, TCP, UDP, ICMP).
Source IP Address	Enter the Source IP address (WAN).
Source Subnet Mask	Subnet mask.
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.
Dest. IP Address	Enter the destination IP address (LAN).
Dest. Subnet Mask	Subnet mask.
Dest. 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.

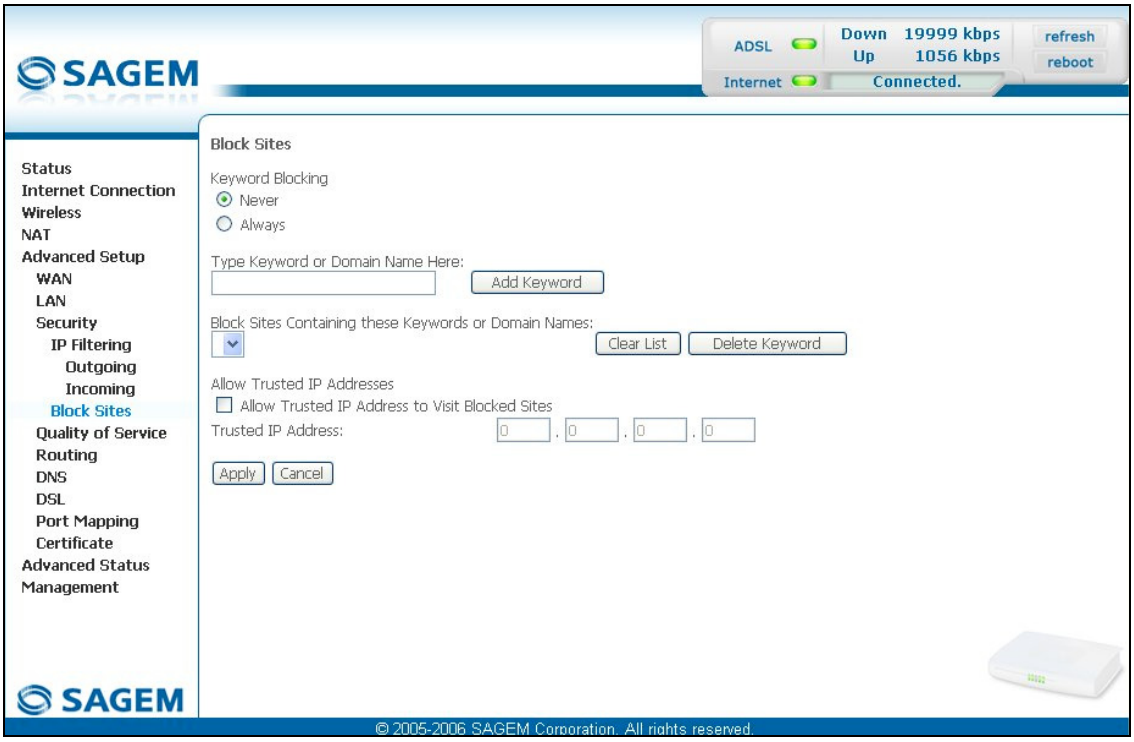
WAN interfaces

Field	Action	Default
Select all	Check the box to select all WAN interfaces. **Note:** Checking out the box, you do not select any interface and you also check out the **pppoe_8_35_1/ ppp_8_35_1** box.	**Box checked**
pppoe_8_35_1/ ppp_8_35_1	Check the box to select the displayed interface.	**Box checked**

5.9.3.2 Block Sites

Object: This menu is used to block the access of the Local Area Network to sites defined by a "keyword or a "Domain Name".

- Select the **Block Sites** sub-menu in the **Security** menu in the **Advanced Setup** section to display the following screen:



Field	Action
Keyword Blocking	Check the box: **Never** to disable the blocking, **Always** to enable the blocking.
Type Keyword or Domain Name Here	Type Keyword or Domain Name in the relevant field.
Add Keyword	Click this button to save Keyword or Domain Name. Following this action, Keyword or Domain Name will appear below in the scroll-down list.
Block Sites Containing Keyword or Domain Name	This scroll-down list displays existing Keywords or Domain Names.
Clear List	Click this button to delete the list of Keywords or Domain Names.
Delete Keyword	Click this button to delete the Keyword or Domain Name which you have selected using the scroll-down list.
Allow Trusted IP Address to Visit Blocked Sites	Check this box to authorize the computer with the IP address specified below to visit blocked sites.
Trusted IP Address	Enter the IP address of the LAN computer to be authorized access to blocked sites.

5.9.4 Quality of Service

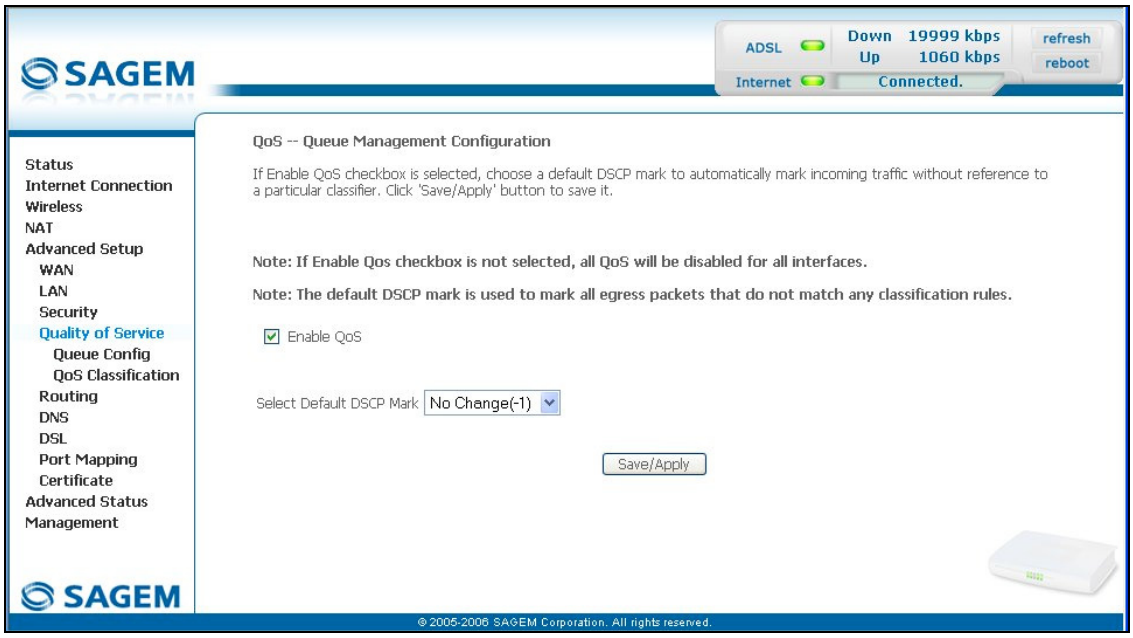
It is essential to check the box **"Enable Quality Of Service"** in the **"WAN**" menu of the section **"Advanced Setup"** so that menu "Quality of Service" is diplayed.

This menu contains 2 sub-menus:

- Queue Config (see subsection 5.9.4.1),
- QoS Classification (see subsection 5.9.4.2).

Subject: This menu is used to allocated 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.

- Select the **Quality of Service** menu in the **Advanced Setup** section to display the following screen:



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 (Differentiated Services Code Point, 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, 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.

5.9.4.1 Queue Config

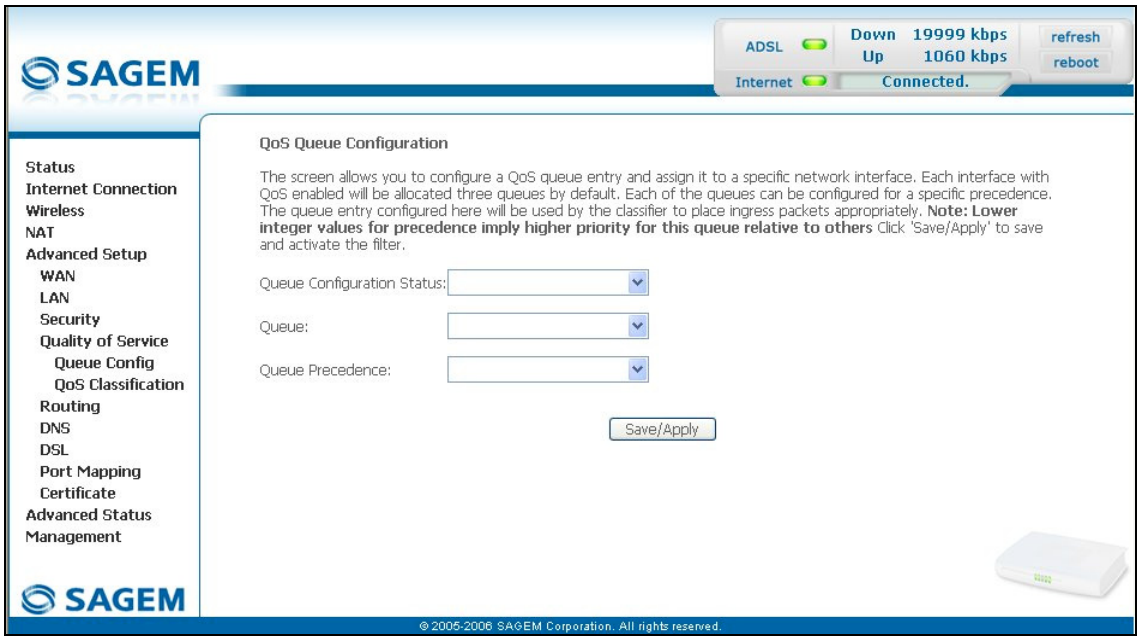
Subject: Enabling or disabling QoS on an interface.
Configuring QoS to use policy maps attached to an interface.

- Select the **Queue Config** sub-menu in the **Quality of Service** menu to display the following screen:

Field	State
Interfacename	Name of the network interface configured (8/35 for example).
Precedence	Priority allocated to "Queue Precedence" from 1 to 3.
Queue Key	Sequence number allocated by the system, incremented of a unit to each addition of a QoS Queue.
Enable	QoS enabled or disabled for this interface. **Note:** This status can be amended starting from this window.

Add

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

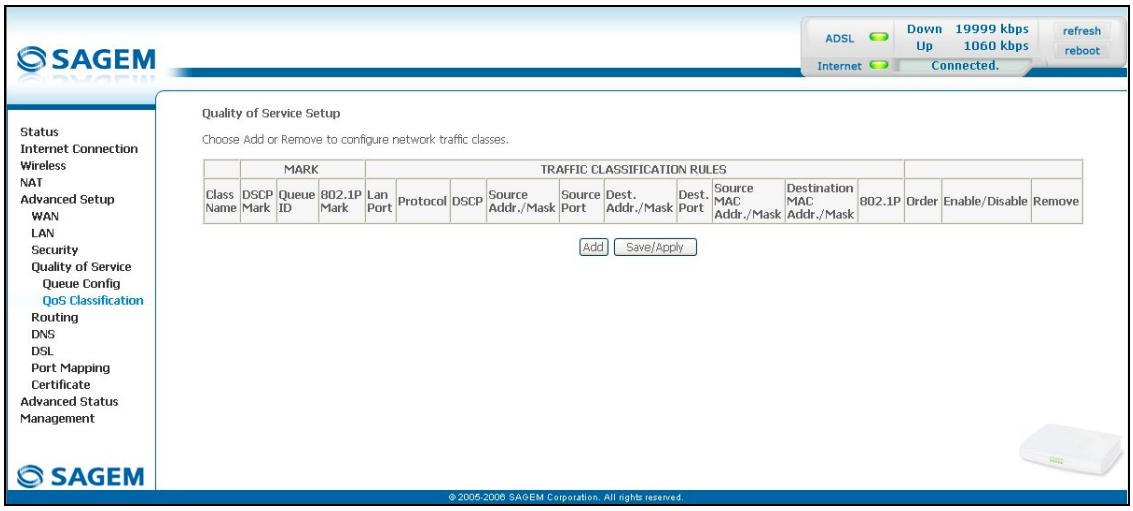


Field	Action
Queue Configuration Status	Select from the scroll down list: Blank : Disable : To disable the QoS queue entry, Enable : To enable the QoS queue entry.
Queue	Select from the scroll down list: Blank : 8/35 : Interface name.
Queue Precedence	Select from the scroll down list: Blank : 1 : High 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.

5.9.4.2 QoS Classification

Subject: Classification of packets into traffic classes.
Enforcement of policies using queing.

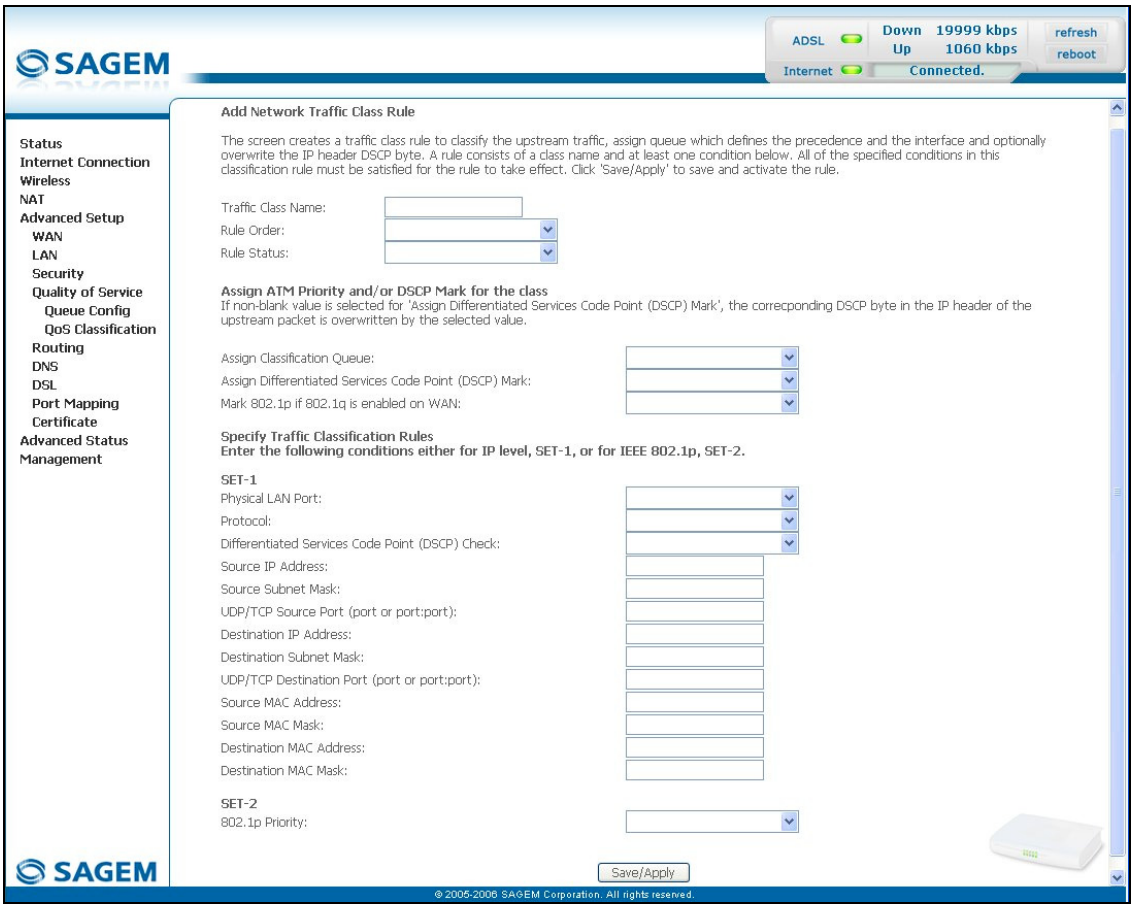
- Select the **QoS Classification** sub-menu in the **Quality of Service** menu to display the following screen:



Field	State
Class Name	Traffic Class Name.
MARK	
DSCP Mark	DSCP priority (from Default to CS7, see the first table of this chapter).
Queue ID	Queue number, allocated by the system according to the selected precedence.
802.1PMark	Priority field 802.1P (value between 0 and 7).
TRAFFIC CLASSIFICATION RULES	
LAN port	Nature of the LAN port.
Protocol	Protocol used.
DSCP	Differentiated Services Code Point, priority value from Default to CS7, see the first table of this chapter.
Source Addr./Mask	"Source" address (your computer, for example) and associated subnet mask.
Source Port	"Source" port.
Dest. Addr./Mask	"Destination" address (a machine on the Internet, for example) and associated subnet mask.
Dest. Port	"Destination" port.
Source MAC Addr./Mask	"Source" MAC address (your computer, for example) and associated subnet mask.
Destination MAC Addr./Mask	"Destination" MAC address (a machine on the Internet, for example) and associated subnet mask.
802.1P	Priority field 802.1P (value between 0 and 7).
Order	Sequence number.
Enable/Disable	QoS enabled or disabled for this traffic class. **Note:** This status can be amended starting from this window.

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: Blank :, Disable : QoS disabled for this static class rule, Enable : QoS enabled for this static class rule.
Assign Classification 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 5.9.4.1).
Assign Differentiated Services Code Point (DSCP) Mark	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 See the first table of this chapter.
Mark 802.1p if 802.1q is enabled on WAN	Select Blank or a priority value between 0 and 7 from the scroll down list. **Note:** The "Enable 802.1q" box is only present in "Bridging" mode. This condition is transparent for the other modes.

Field		Action
SET-1	**Physical LAN Port**	Select Blank or the interface of your choice (ENET(1-4), Wireless or Wireless_Guest) from the scroll down list.
	Protocol	Select Blank or the protocol of your choice from the scroll down list (TCP/UDP, TCP, UDP or ICMP).
	Differentiated Services Code Point (DSCP) Check	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 See the first table of this chapter.
	Source IP Address	Enter a "Source" IP address.
	Source Subnet Mask	Enter a "Source" subnet mask.
	UDP/TCP source Port (port or port:port)	Enter a "Source" port or range of ports. **Note:** For one port, for example, enter 80. For a range of ports, enter 80:90.
	Destination IP Address	Enter a "Destination" IP address.
	Destination Subnet Mask	Enter a "Destination" subnet mask.
	UDP/TCP Destination Port (port or port:port)	Enter a "Destination" port or range of ports. **Note:** For one port, for example, enter 80. For a range of ports, enter 80:90.
	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.
SET-2	**802.1p Priority**	Select Blank or a priority value between 0 and 7 from the scroll down list. **Note:** 802.1p Priority cannot be selected together with IP traffic condition.

5.9.5 Routing

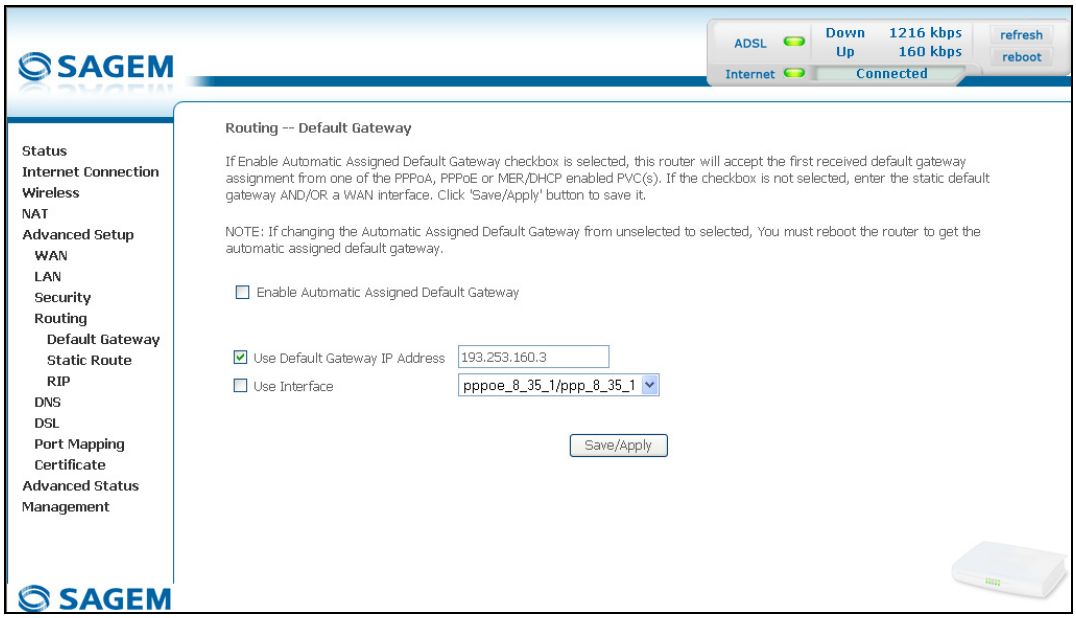
This menu contains 3 sub-menus:

- Default Gateway (see subsection 5.9.5.1),
- Static Route (see subsection 5.9.5.2),
- RIP (see subsection 5.9.5.3).

5.9.5.1 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.

- Select the **Default Gateway** sub-menu in the **Routing** menu in the **Advanced Setup** section to display the following screen:



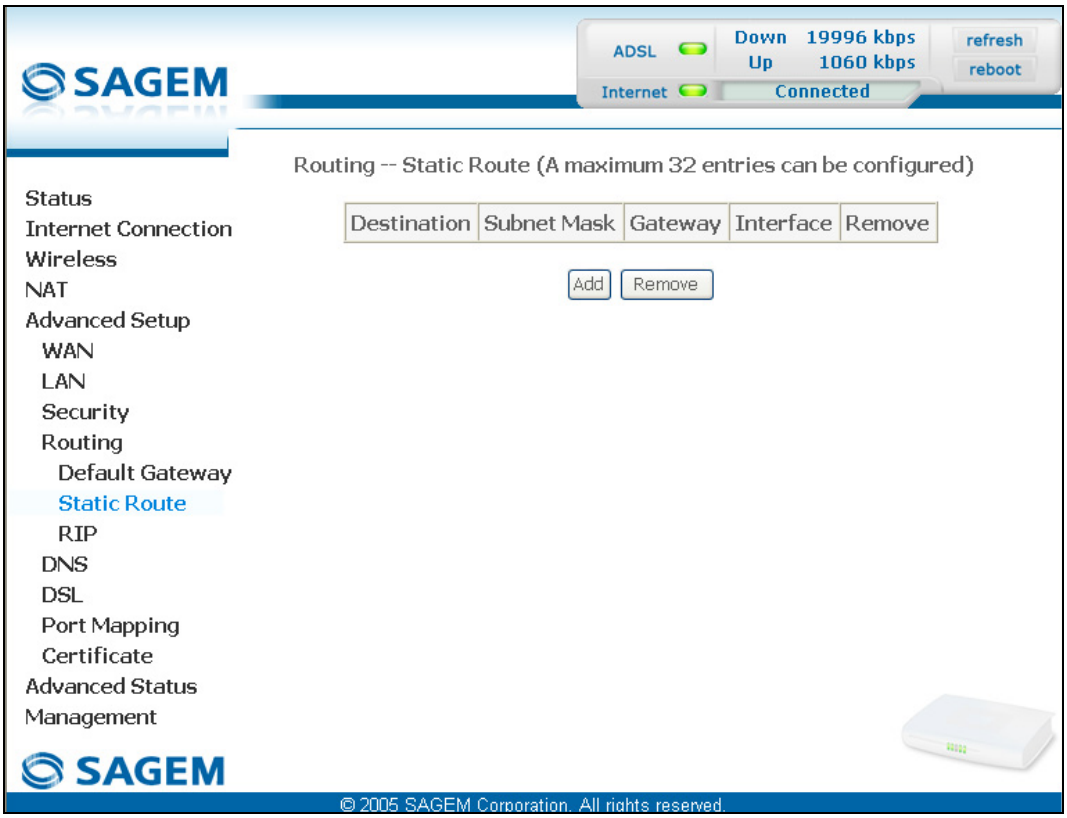
Field	Action	Default
EnableAutomatic Assigned Default Gateway	Check the box to allocate automatically a default gateway for your router.	**Box checked**
Use Default Gateway IP Address[11]	Check the box to use a default address.	**Box checked** **Not empty**
Use Interface[11]	Select the interface you want to use from the scroll down list (pppoe_8_35_1 for example).	**Box not checked** **Interface used**

[11] this field only appears when the "Enable Automatic Assigned Default Gateway" field is deactivated (box not checked).

5.9.5.2 Static Route

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

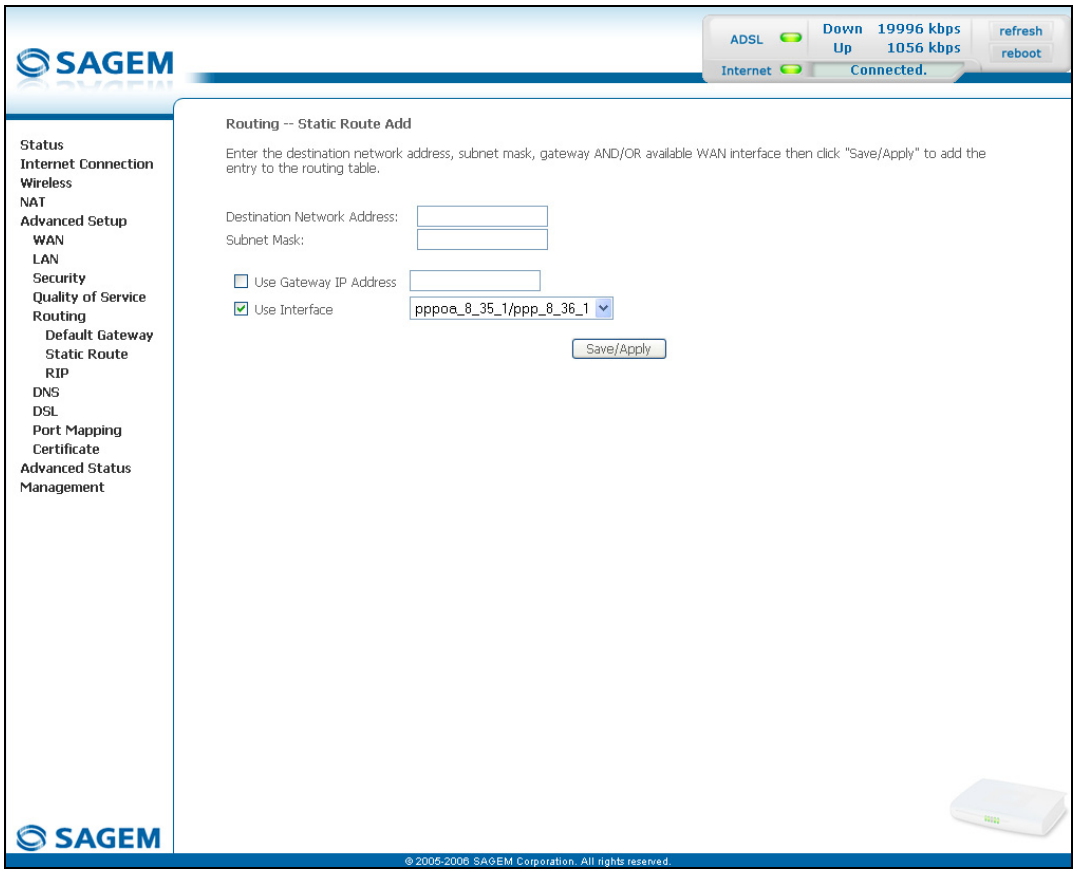
- Select the **Static Route** sub-menu in the **Routing** menu in the **Advanced Setup** section to display the following screen:



Field	Meaning
Destination	Remote network IP address
Subnet Mask	Remote subnet mask
Gateway	Default gateway of the remote network
Interface	Remote network interface

Add

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



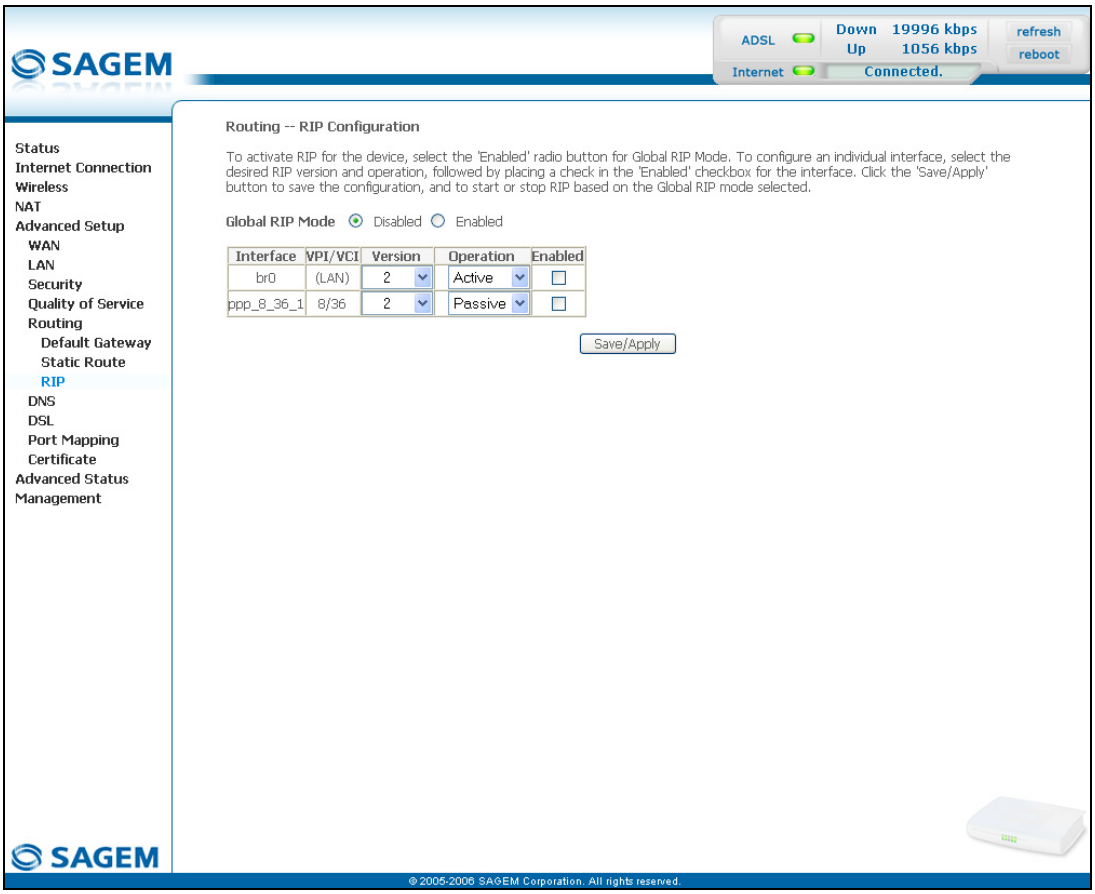
Field	Action	Default
Destination Network Address	Enter the IP address of the remote network.	**Empty**
Subnet Mask	Enter the remote subnet mask.	**Empty**
Use Gateway IP Address	Check the appropriate box then enter the IP address of the gateway.	**Box not checked** **Empty**
Use Interface	Select the interface you want to use from the scroll down list (pppoa_8_35_1 for example).	**Box checked** **Interface used**

5.9.5.3 RIP

Object: The "RIP" protocol (**R**outing **I**nformation **P**rotocol) lets you tell routers the distance (number of hops) which separates them.

This protocol only takes account of the distance between two machines in terms of hops.

- Select the **RIP** sub-menu in the **Routing** menu in the **Advanced Setup** section to display the following screen:



Field	Action/Meaning	Default
Global RIP Mode	Check the appropriate box to activate (Enabled) or deactivate (Disabled) the RIP function (**R**outing **I**nformation **P**rotocol).	**Disabled**
Interface	Created or native interface.	**Br0**
VPI/VCI	VPI/VCI associated with the interface.	**(LAN)**
Version	Select the RIP version of your choice from the scroll down list. • **1** for RIP1, • **2** for RIP2, • **Both**.	**2**

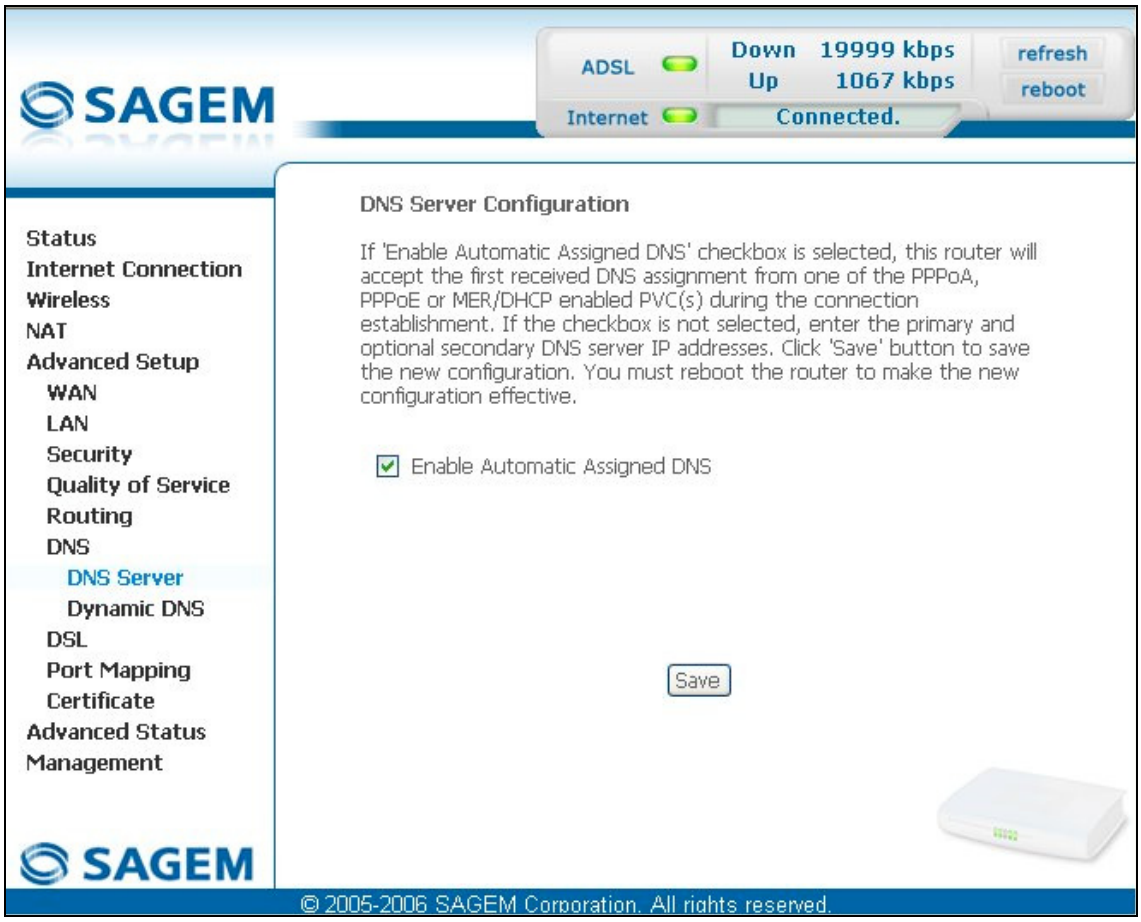
Field	Action/Meaning	Default
Operation	In the scroll down list, select **Active** to transmit the routing information to the other routers and receive it from them or **Passive** to listen to the **RIP** broadcasts and update its routing table, but not indicate its own routes (silent mode).	**Active**
Enabled	Check the box to activate the "RIP" function on the interface you want (LAN or WAN for example).	**Box not checked**

5.9.6 DNS

5.9.6.1 DNS Server

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

- Select the **DNS** menu in the **Advanced Setup** section to display the following screen:



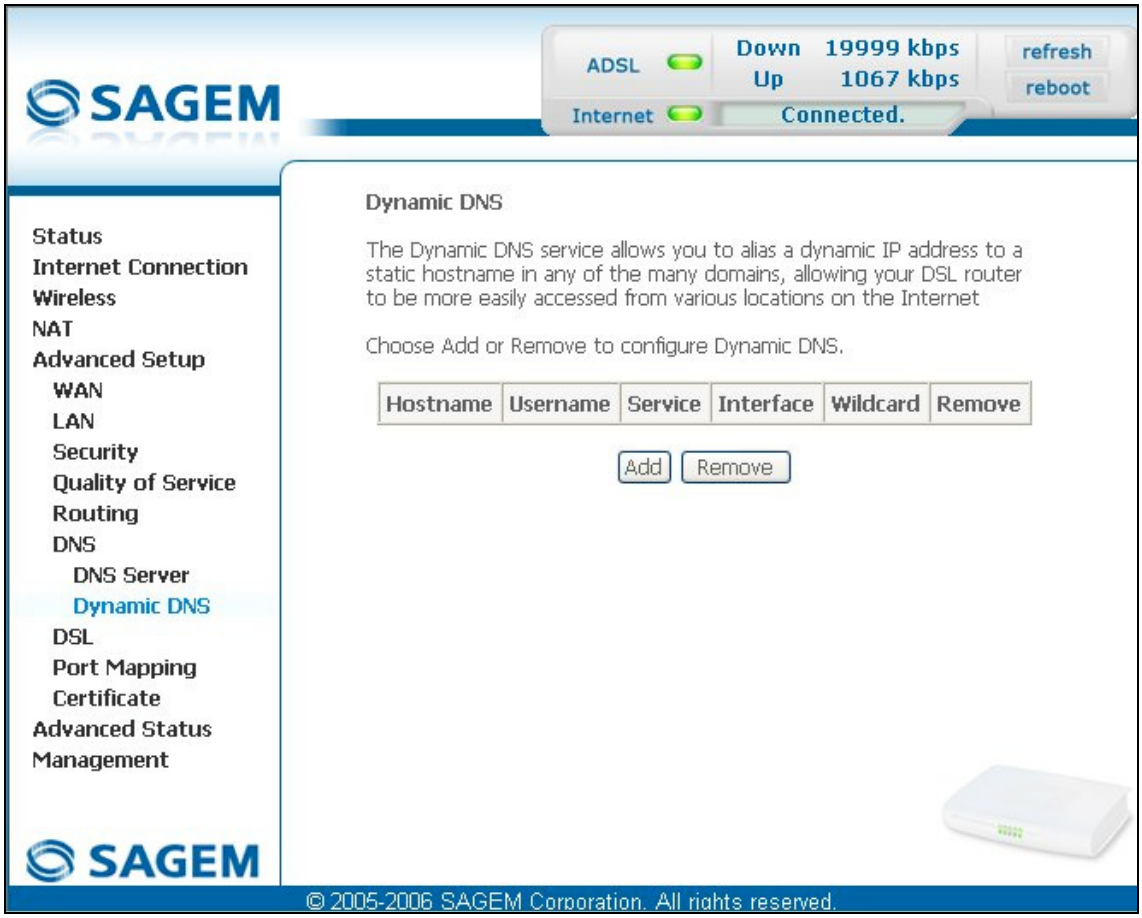
Field	Action	Default
Enable Automatic Assigned DNS	Check the appropriate box to allocate a domain name address.	**Box checked**
Primary DNS server[12]	Enter a primary DNS server address.	_
Secondary DNS server[12]	Enter a secondary DNS server address.	_

[12] This field only appears when the "Enable Automatic Assigned DNS" field is deactivated (box not checked).

5.9.6.2 Dynamic DNS

Subject: 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**.

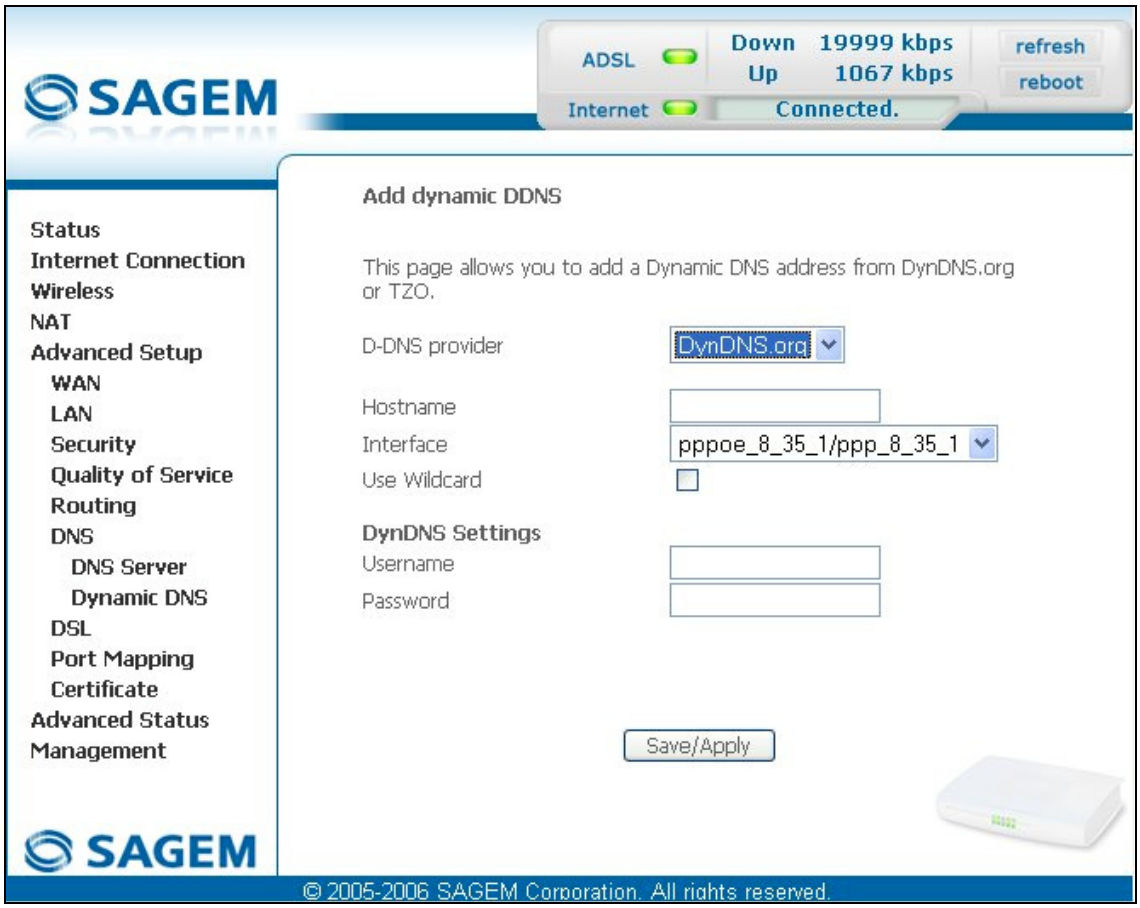
In the **Advanced setup** section, select the **DNS** menu then select the **Dynamic DNS** sub-menu.
The following screen appears.



On the screen above, The fields of the table are detailed in the next subsection (Add).

Note: On the screen above, The fields of the table are detailed in the next subsection (Add). The "Service" field is automatically filled by the system in "**dyndns**".

Add


SAGEM
ADSL
Down 19999 kbps
Up 1067 kbps
Internet
Connected.
refresh
reboot
Status
Internet Connection
Wireless
NAT
Advanced Setup
WAN
LAN
Security
Quality of Service
Routing
DNS
DNS Server
Dynamic DNS
DSL
Port Mapping
Certificate
Advanced Status
Management
Add dynamic DDNS
This page allows you to add a Dynamic DNS address from DynDNS.org or TZO.
D-DNS provider
DynDNS.org
Hostname
Interface
pppoe_8_35_1/ppp_8_35_1
Use Wildcard
DynDNS Settings
Username
Password
Save/Apply
SAGEM
© 2005-2006 SAGEM Corporation. All rights reserved.

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 (Note).
Interface	Select from the relevant drop-down list the WAN interface which you want to use (pppoe_8_35_1/ppp_8_35_1 for example).
Use Wildcard	Check the appropriate box if you wish to choose this option.

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.

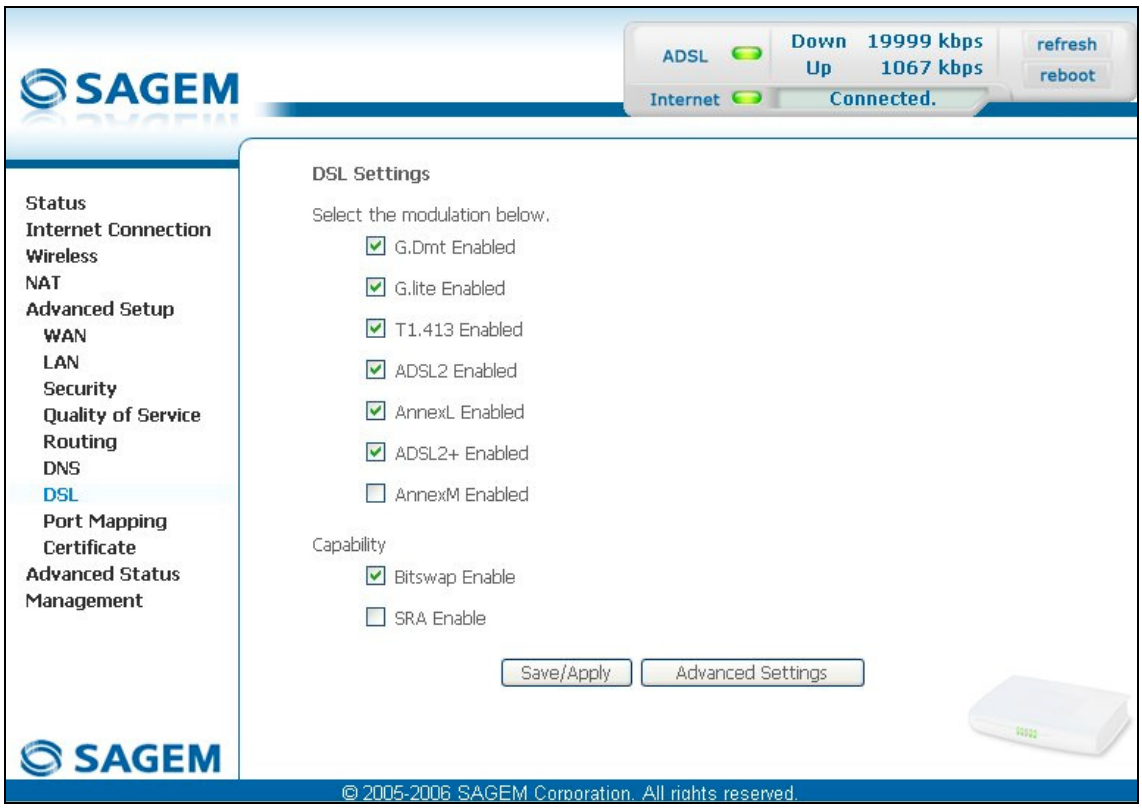
DynDNS Settings

User Name	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.

5.9.7 DSL

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

- Select the **DSL** menu in the **Advanced Setup** section to display the following screen:



Modulation

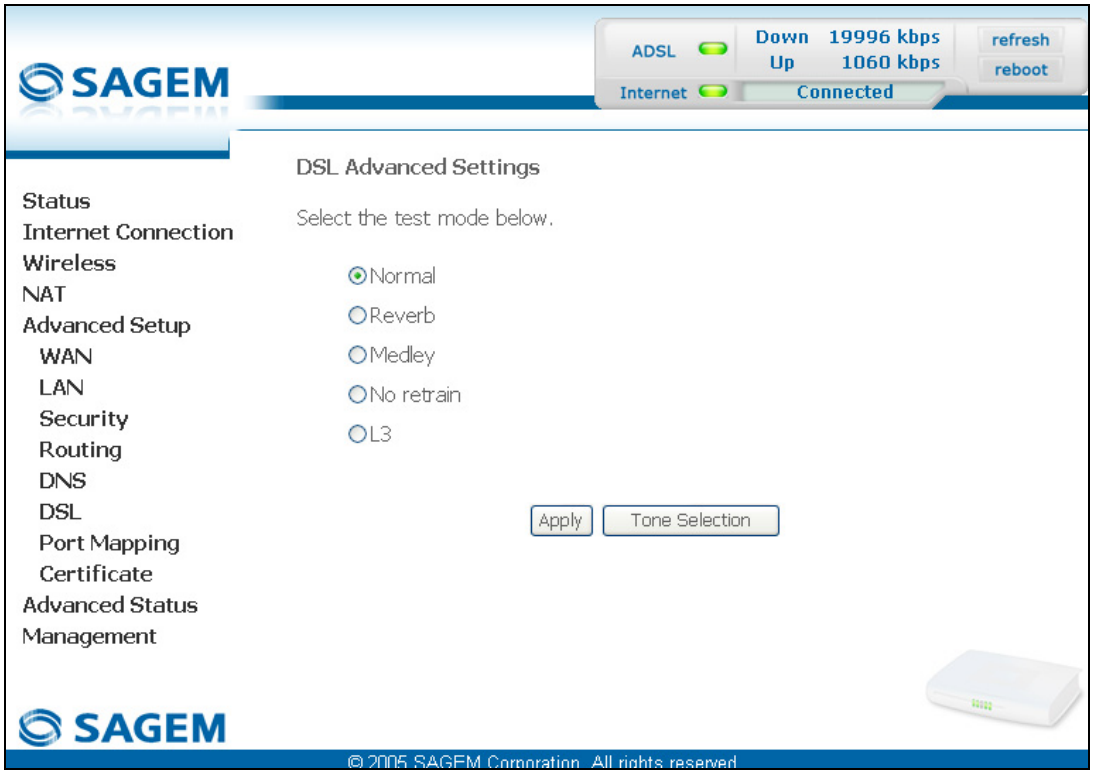
Field	Default
G.Dmt Enabled	Box checked
G.lite Enabled	Box checked
T1.413 Enabled	Box checked
ADSL2 Enabled	Box checked
AnnexL Enabled	Box checked
ADSL2+ Enabled	Box checked
AnnexM Enabled	Box not checked

Check the boxes according to the characteristics of your line.

Capability

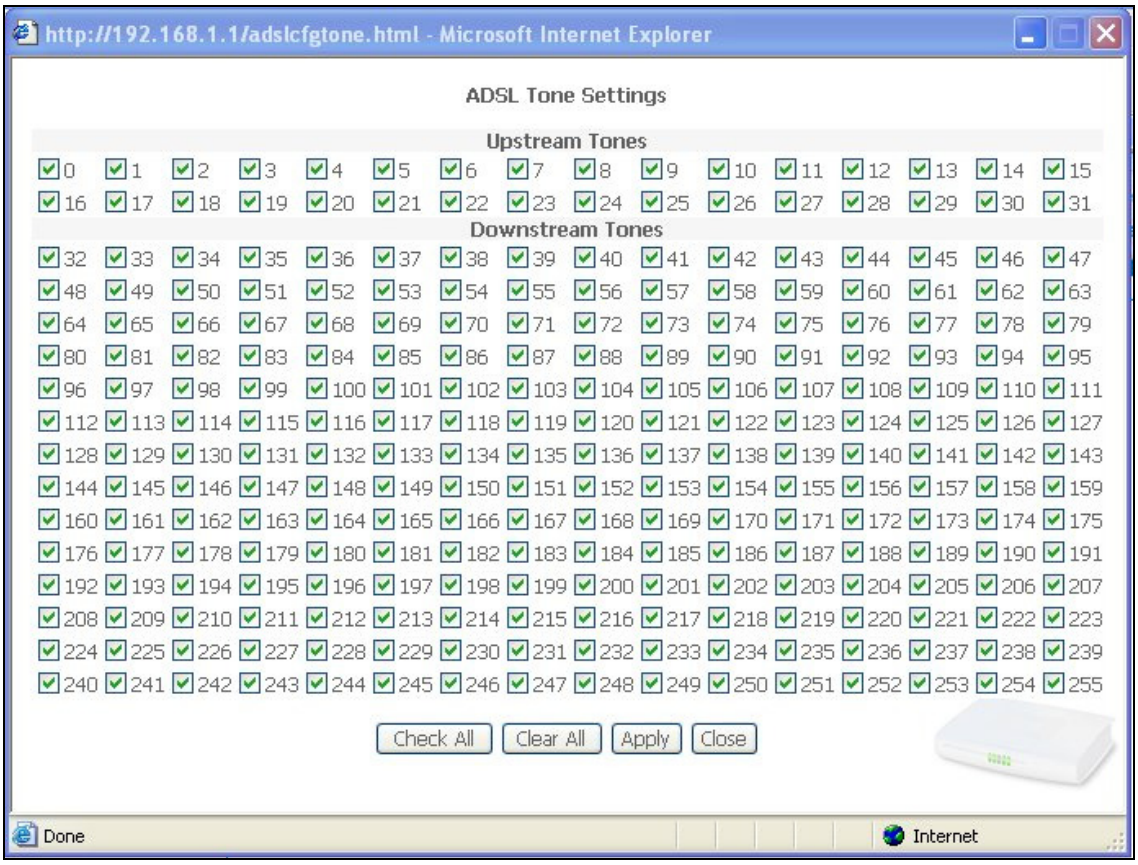
Field	Default
Bitswap Enable	Box checked
SRA Enable	Box not checked

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



Field	Default
Normal	Selected box
Reverb	Box not selected
Medley	Box not selected
No retrain	Box not selected
L3	Box not selected

- 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.

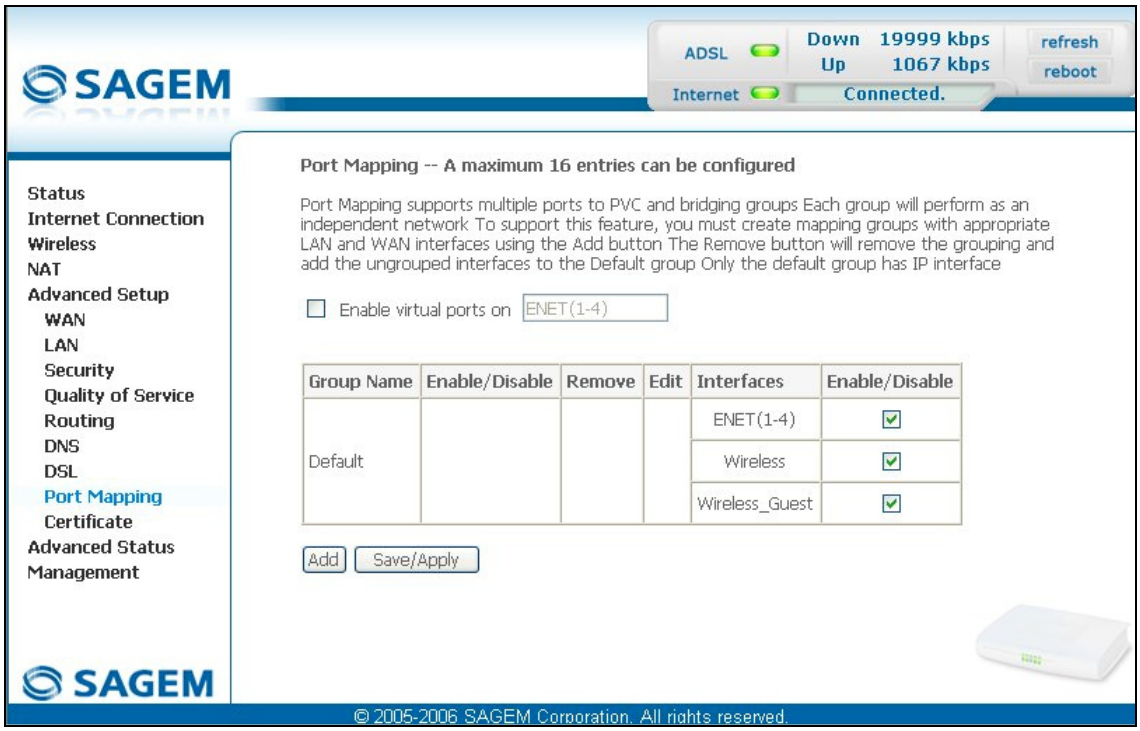
All the tones are selected by default.

To select a tone, simply check the associated box.
To not select a tone, simply leave its associated box empty.

5.9.8 Port Mapping

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

- Select the **Port Mapping** menu in the **Advanced Setup** section to display the following screen:



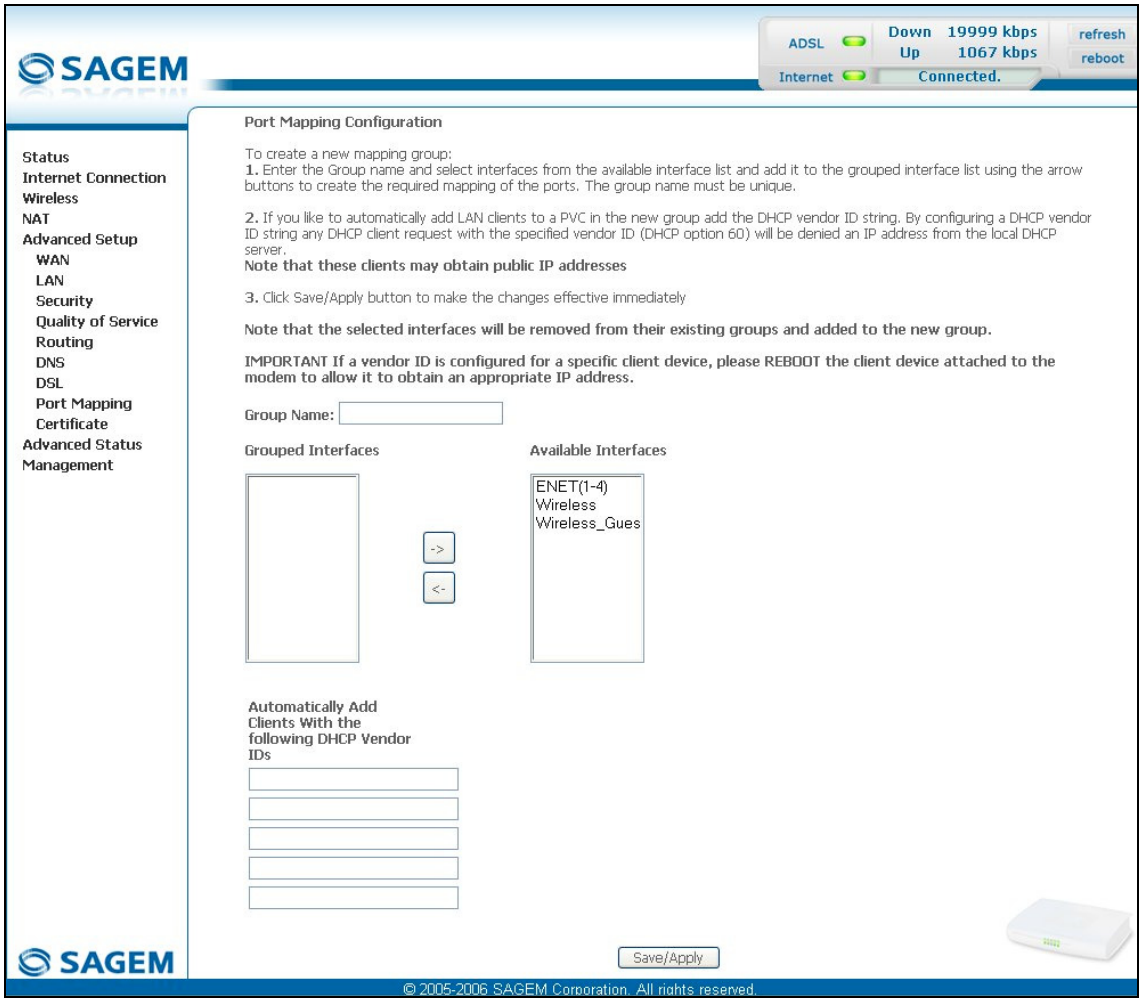
Field	Meaning	Default
Enable virtual ports on	If the box is not checked, the Ethernet 1 to 4 (ENET (1-4)) ports are gathered and seen like only one virtual port. When the box is checked, these ports are independently seen but a fall of the performances of the transfers between ports is noted.	**Box not checked**

Field	Meaning
Group Name	Group name (see "Information" icon).
Enable/Disable	Allows to enable / disable a group of interfaces.
Interfaces	Lists all your router's interfaces. **Note:** Only the "nas_8_50" interface is not resident on the router. It corresponds to a "Bridge" ATM interface.
Enable/Disable	Allows to enable / disable each interface.

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	Default
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)).	–
Grouped Interfaces	Displays the interfaces associated with a service you selected in the "Available Interfaces" area then transferred with the <- button.	–
Available Interfaces	Lists all your router's interfaces. **Note:** Only the "nas_8_50" interface is not resident on the router. It corresponds to a "Bridge" ATM interface.	–

<-	Used to transfer the interfaces selected in the "**Available Interfaces**" area to the "**Grouped Interfaces**" area.
->	Used to transfer the interfaces selected in the "**Grouped Interfaces**" area to the "**Available Interfaces**" area.

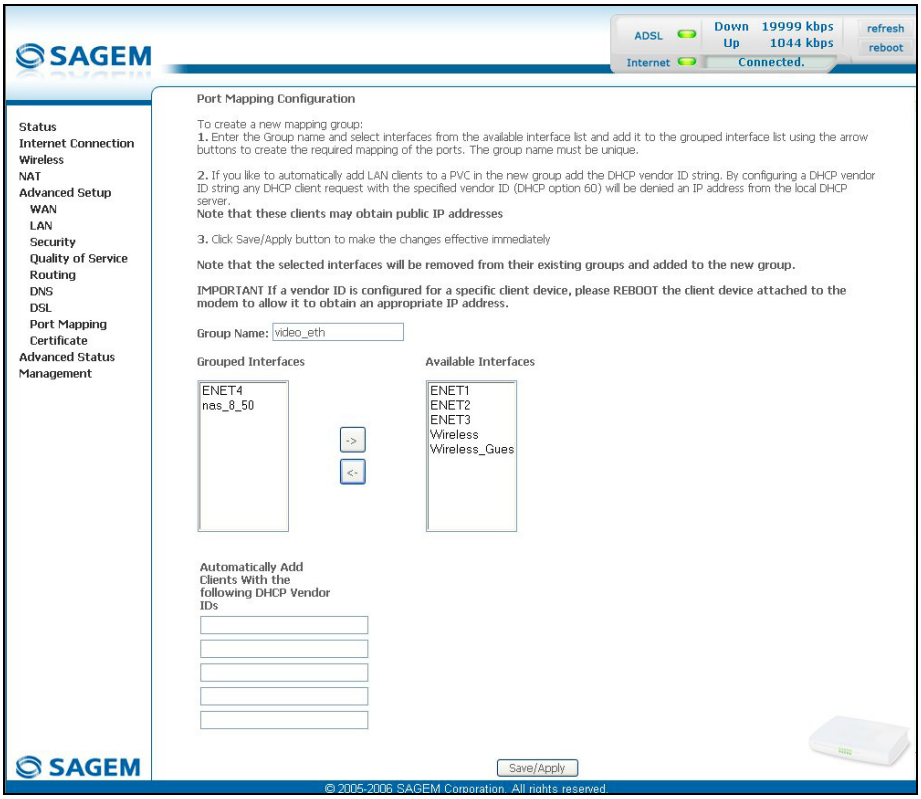
Field	Meaning
Automatically Add Clients with the DHCP Vendor IDs	This functionality allows to recognize the equipment connected to a port and to automatically affect this port to it. To do that, the router receives from this equipment (for example a decoder TV) a DHCP request which contains a client specific identification (Vendor ID). **Note:** As soon as this assignment is carried out, it becomes permanent.

Example

If you want to associate the "Video" service with the Ethernet interface:

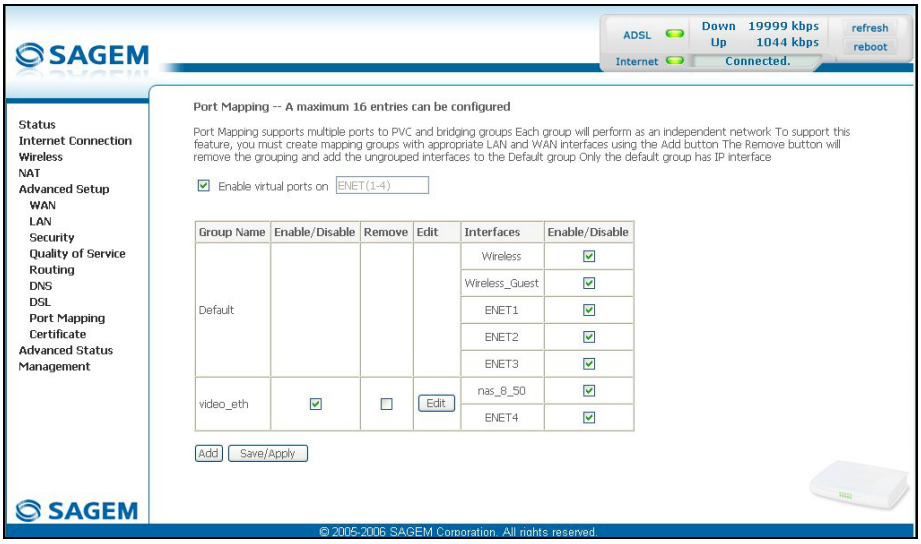
- in the "Group Name" area enter a representative name such as "video_eth".
- in the "Available Interfaces" area select **ENET4** for the Ethernet interface.
- then click on the <- button to transfer this interface to the "Grouped Interfaces" area.
- in the "Available Interfaces" area select the ATM **nas_8_50** interface associated with the ATM "br_8_50" service ("Bridge" protocol) created earlier using the Advanced Setup / WAN) menu.
- then click on the <- button to transfer this interface to the "**Grouped Interfaces**" area.

The following screen shows the operations which have been carried out.



Note: You are recommended to associate the "Bridge" protocol with the "Video" service.

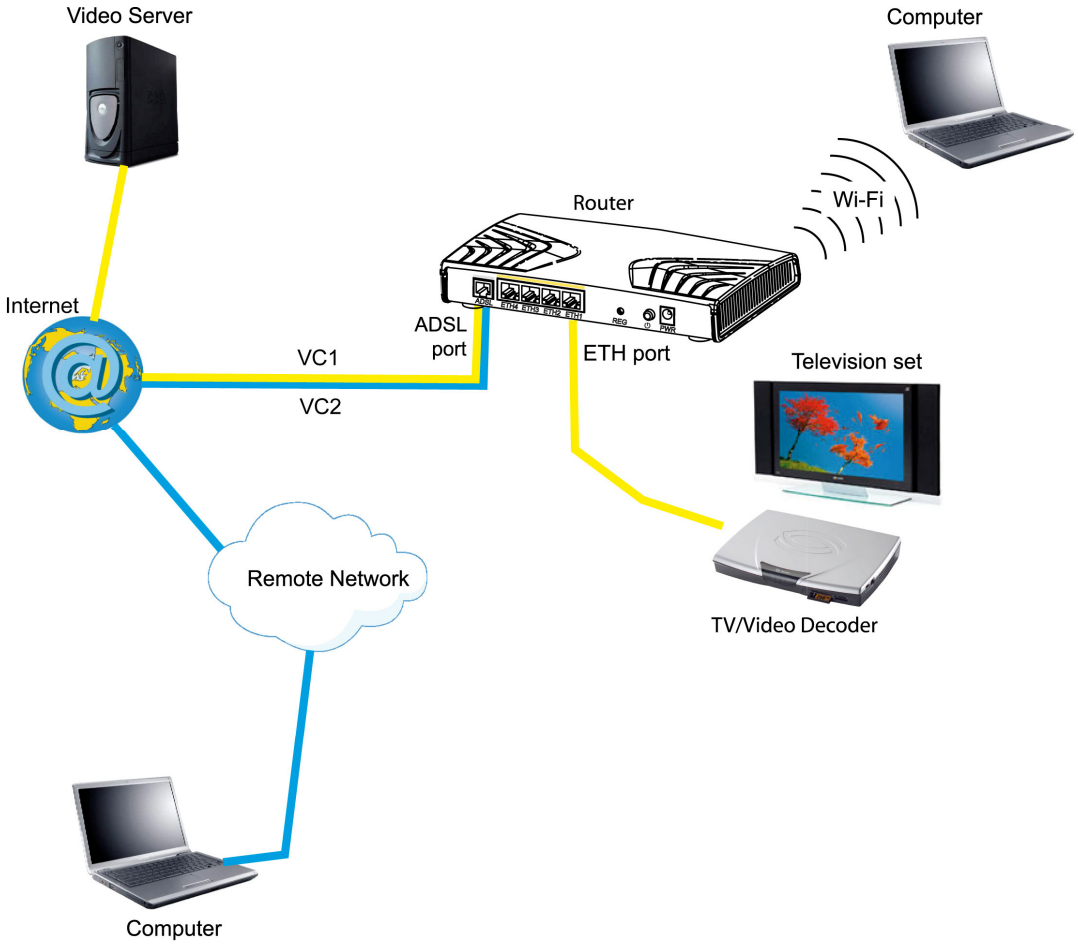
- click on the Save/Apply button to save the addition. The following screen displays all the entries which have been configured.



This screen indicates that:

- the **Default** "Group Name" associates the "Data" service with the interfaces by default (Wireless, Wireless_Guest, ENET1, ENET2, ENET3).
- the dedicated ATM interface **nas_8_50** and the Ethernet interface **ENET4** are associated with the "Video" service.

To enable you to understand better, the following diagram shows the path of the "Video" and "Data" flows.



VC1 used for the "video" stream : Bridge LLC

VC2 used for the "Data" stream : PPPoE LLC

5.9.9 Certificate

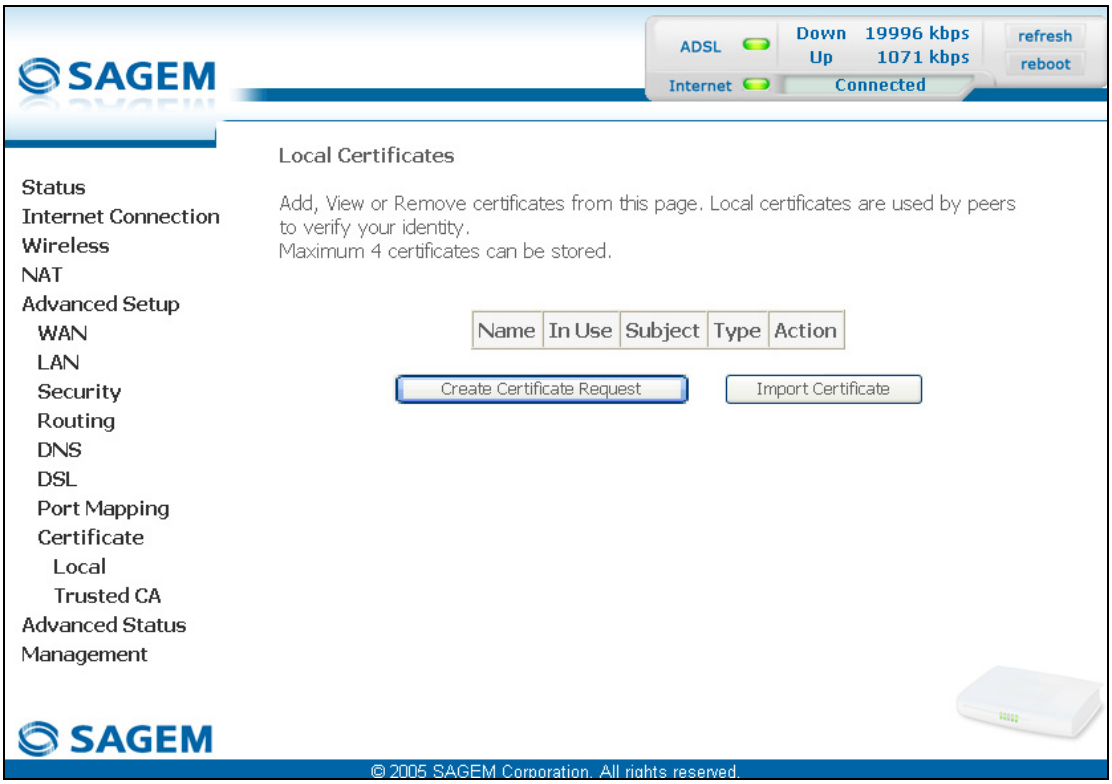
This menu contains 2 sub-menus:

- Local (see subsection 5.9.9.1),
- Trusted CA (see subsection 5.9.9.2).

5.9.9.1 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.

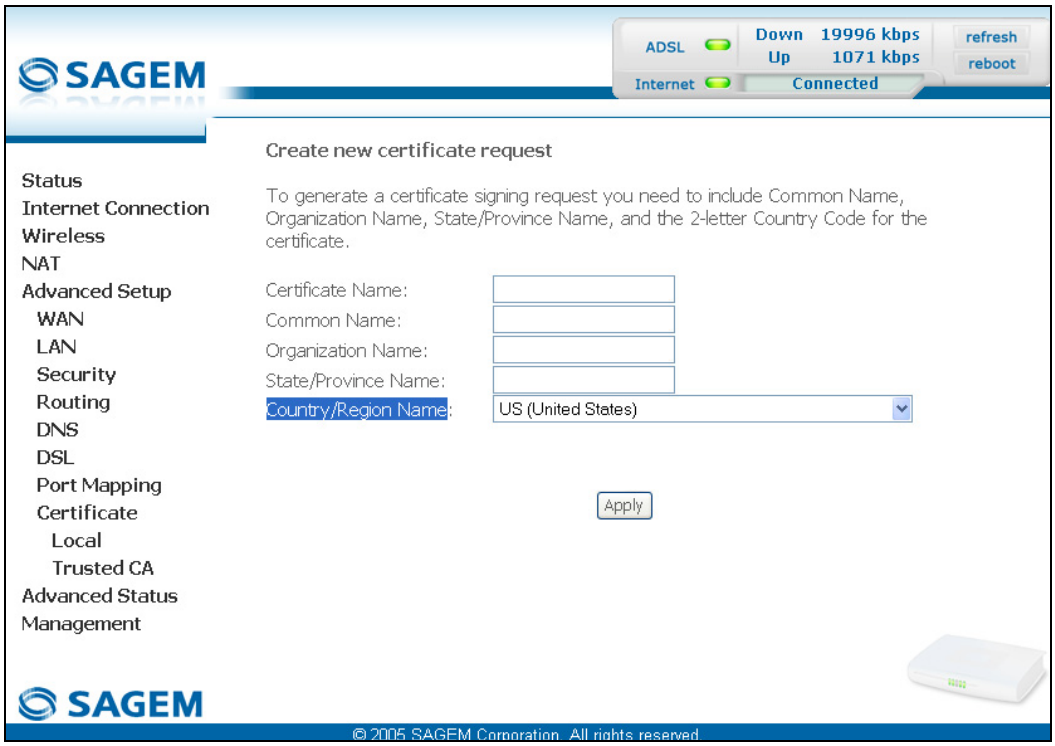
- Select the **Local** sub-menu in the **Certificate** menu in the **Advanced Setup** section to display the following screen:



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

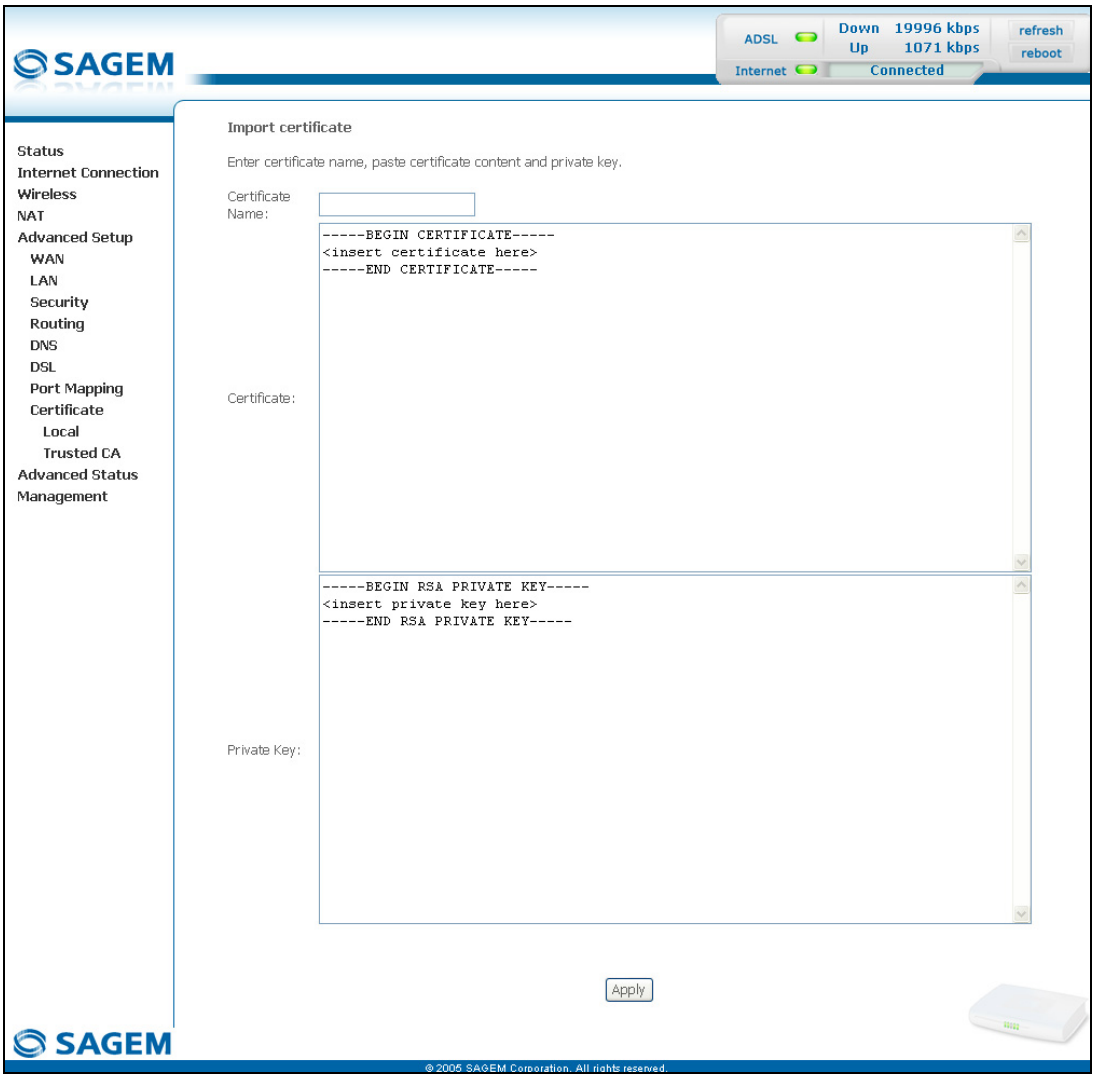
- Click on the **Create Certificate Request** button to display the following screen:



Field	Action	Default
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 of 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:

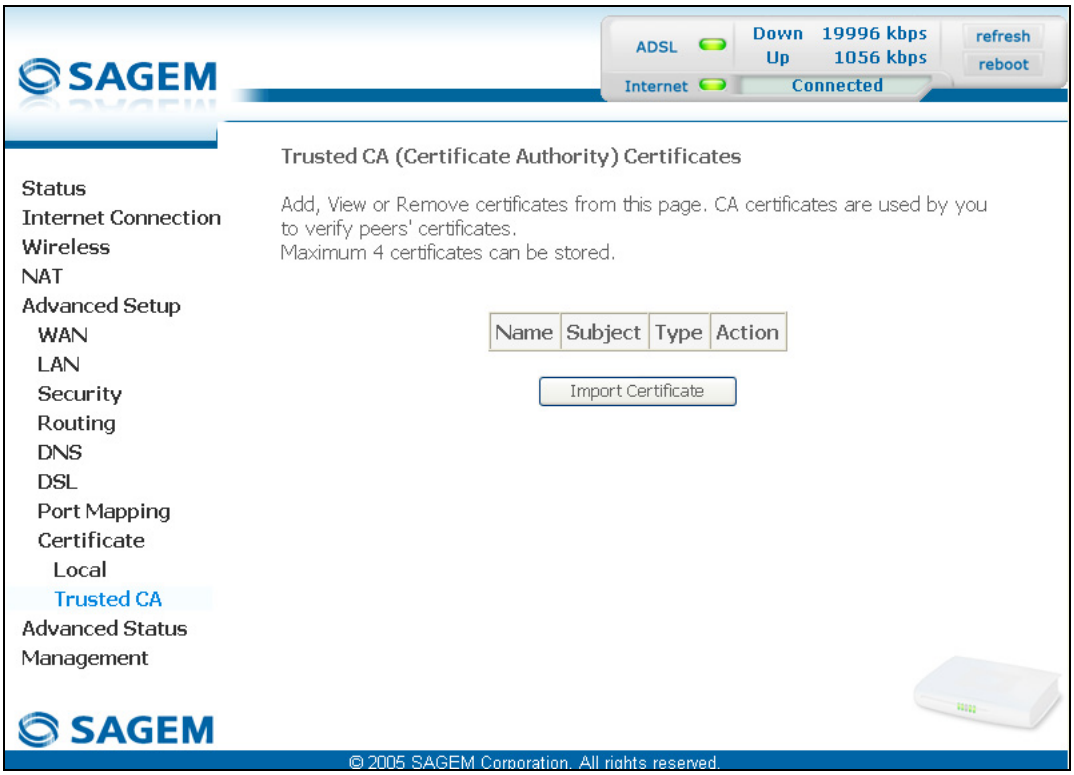


Field	Action	Default
Certificate Name	Enter the name of the certificate	_
Certificate	Insert the certificate here	_
Private key	Insert the private key here	_

5.9.9.2 Trusted CA

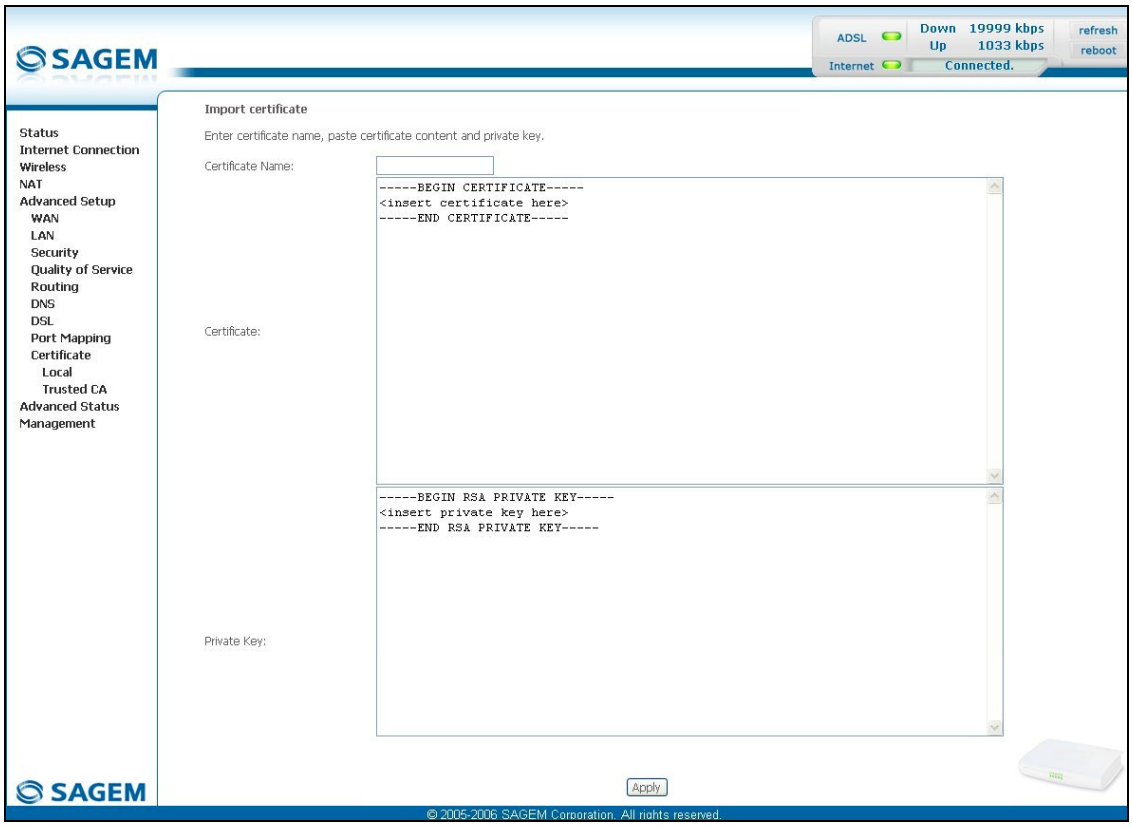
Object: This menu is used to manage the identity certificates of the remote servers. These certificates, which are used by TR-69 (in SSL mode), enable the mutual authentication of the CPE and the ACS.

- Select the **Trusted** sub-menu in the **Certificate** menu in the **Advanced Setup** section to display the following screen:



Import Certificate

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



Field	Action	Default
Certificate Name	Enter the name of the certificate to be imported.	_
Certificate	Insert the certificate here.	_
Private Key	Insert the private key here.	_

5.10 Advanced Status

Object: This heading is used to display the status of your router.

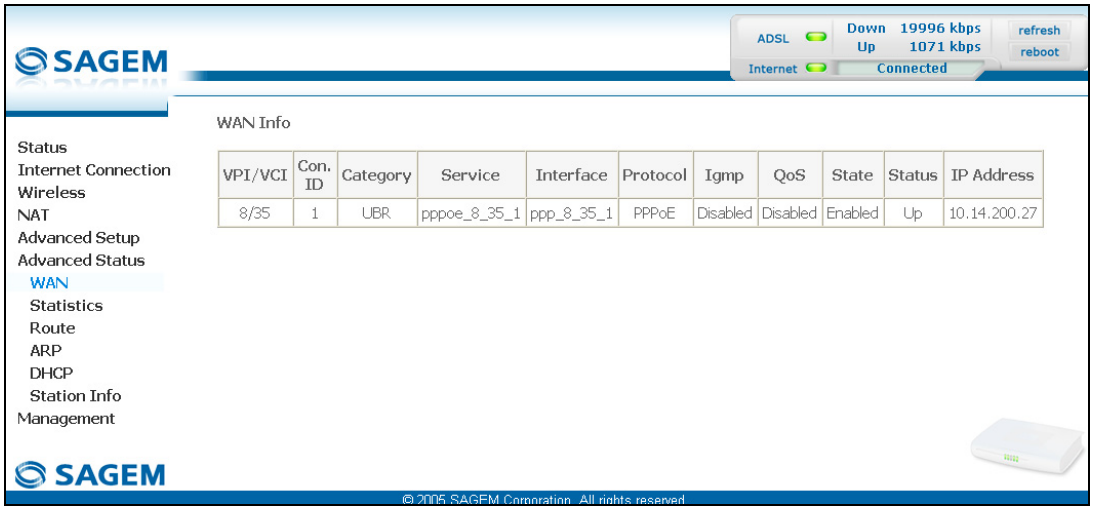
This section contains the following six menus:

- WAN (see subsection 5.10.1),
- Statistics (see subsection 5.10.2),
- Route (see subsection 5.10.3),
- ARP (see subsection 5.10.4),
- DHCP (see subsection 5.10.5),
- Station Info (see subsection 5.10.6).

5.10.1 WAN

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

- Select the **WAN** menu in the **Advanced Status** section to display the following screen:



5.10.2 Statistics

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

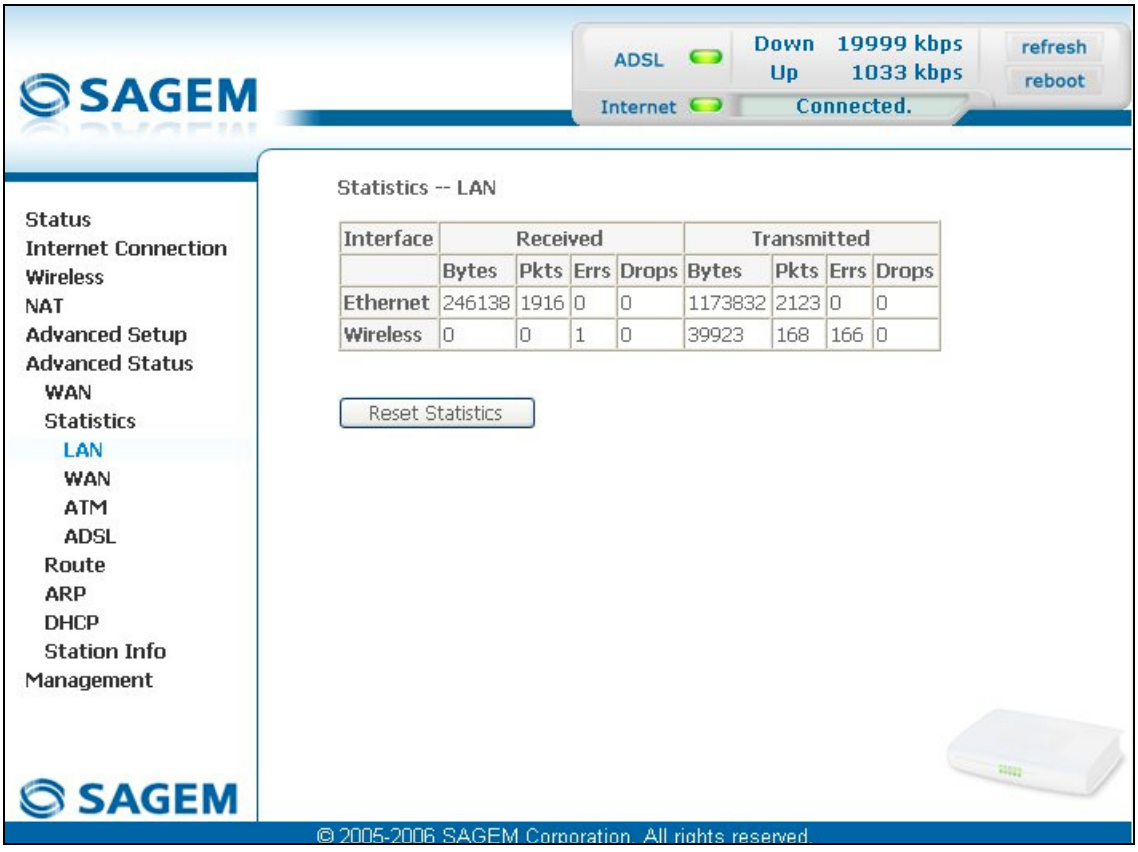
This menu contains the following four sub menus:

- LAN (see subsection 5.10.2.1),
- WAN (see subsection 5.10.2.2),
- ATM (see subsection 5.10.2.3),
- ADSL (see subsection 5.10.2.4).

5.10.2.1 LAN

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

- Select the **LAN** sub menu in the **Statistics** menu in the **Advanced Status** section to display the following screen:

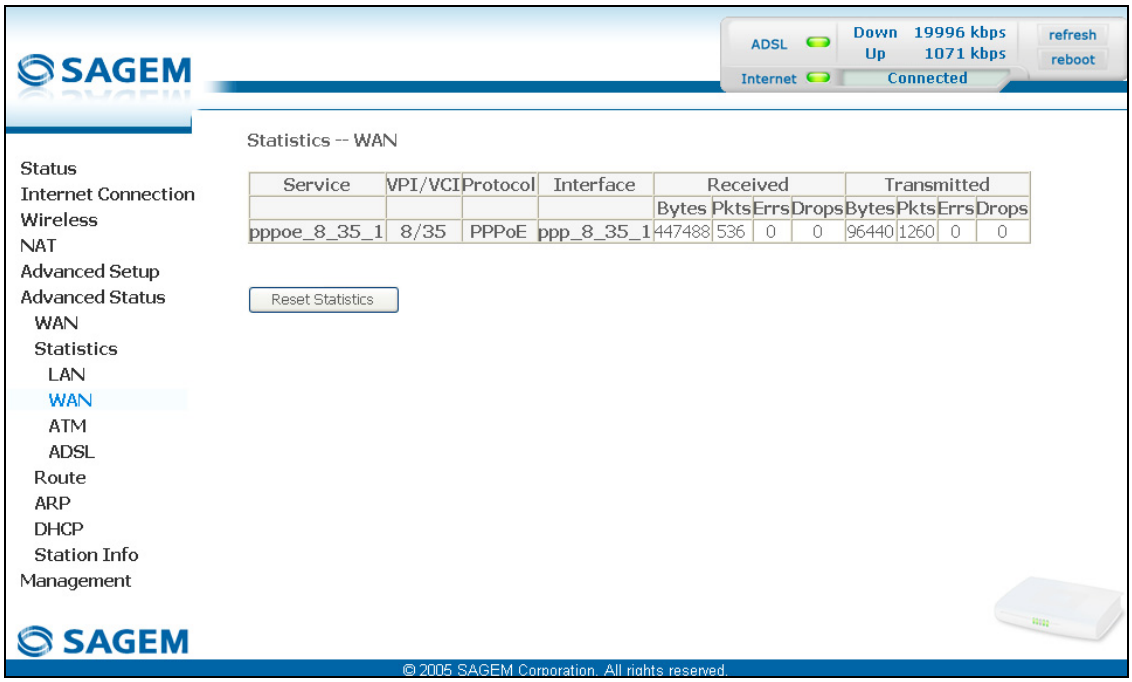


- click on the Reset Statistics button to reset statistics.

5.10.2.2 WAN

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

- Select the **WAN** sub menu in the **Statistics** menu in the **Advanced Status** section to display the following screen:

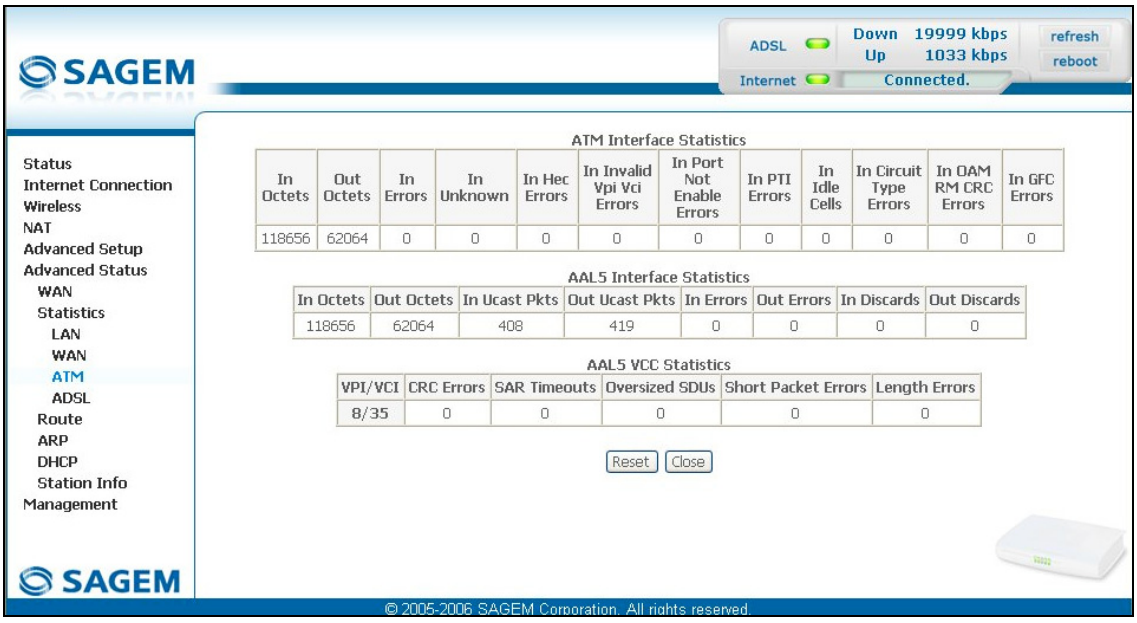


- click on the Reset Statistics button to reset statistics.

5.10.2.3 ATM

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

- Select the **ATM** sub menu in the **Statistics** menu in the **Advanced Status** section to display the following screen:

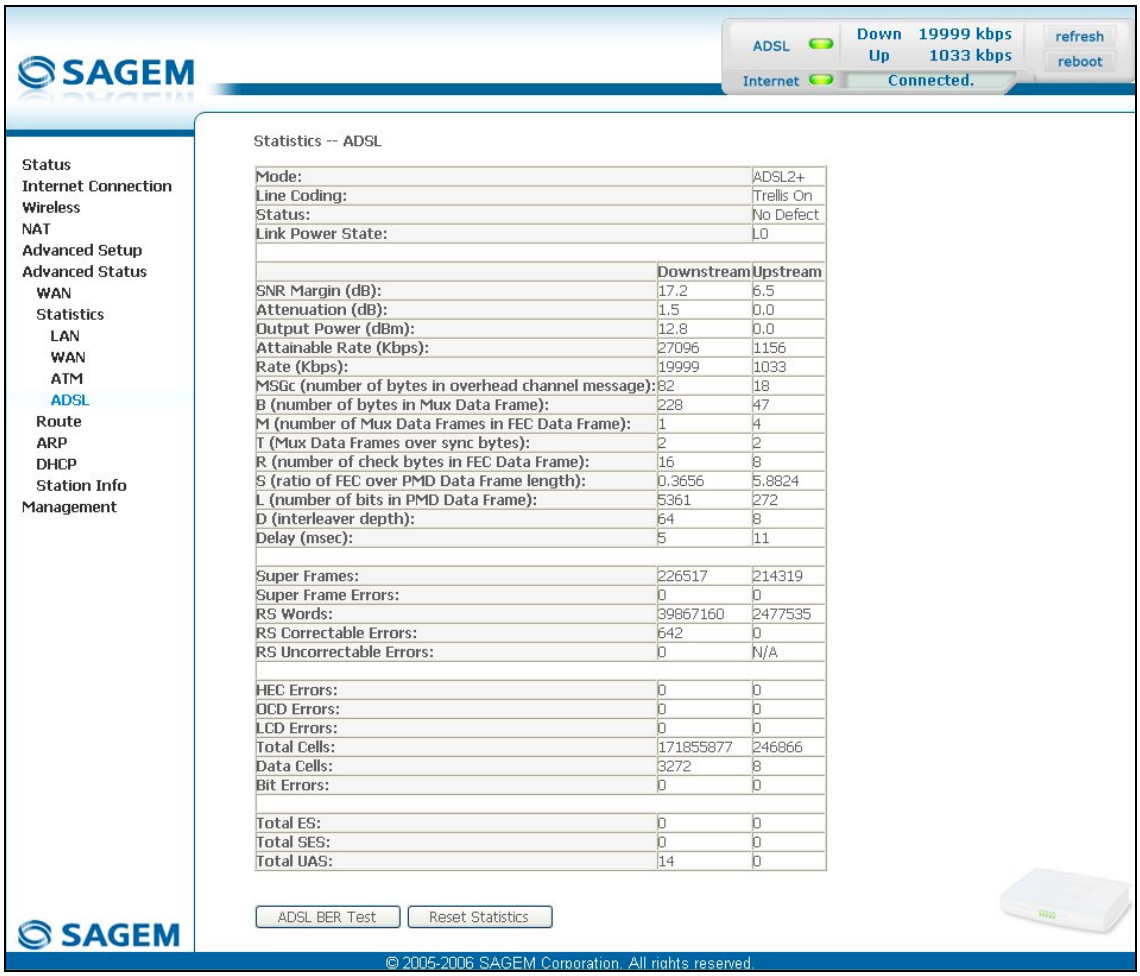


- click on the Reset button to reset statistics.

5.10.2.4 ADSL

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

- Select the **ADSL** sub menu in the **Statistics** menu in the **Advanced Status** section to display the following screen:



- click on the Reset Statistics button to reset statistics.

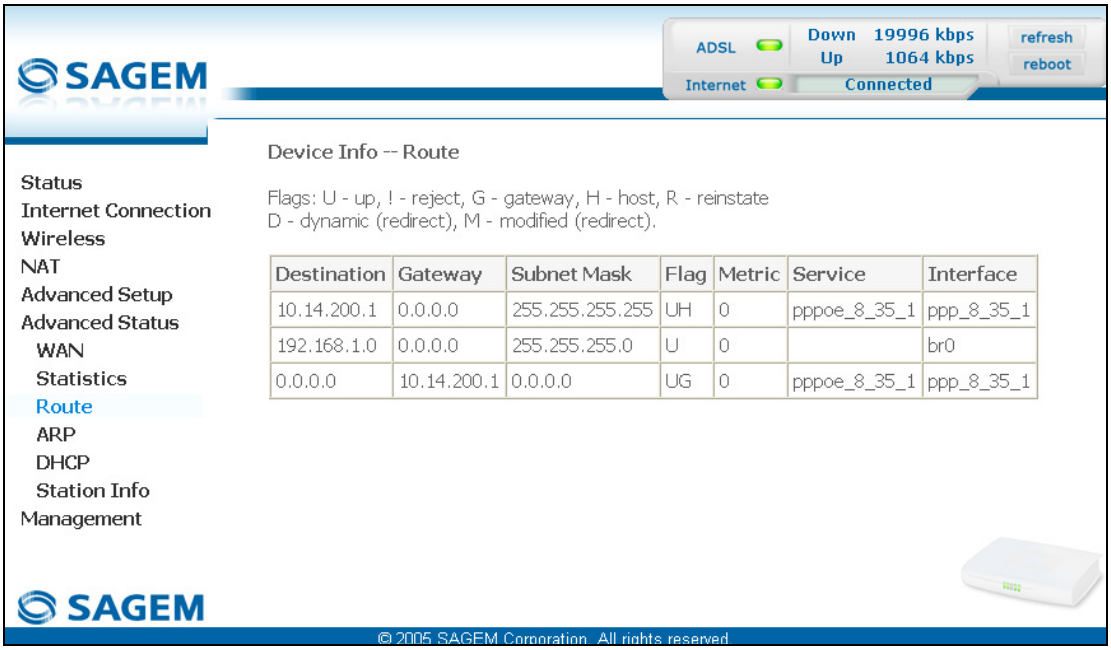
- Cliquez sur le bouton ADSL BER Test pour afficher l'écran suivant :

- in the "Test Time (sec)" field, select the test time from the scroll down list.
- Click on the Start button to run test.
- Click on the Close button to shut window and return to the previous screen.

5.10.3 Route

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

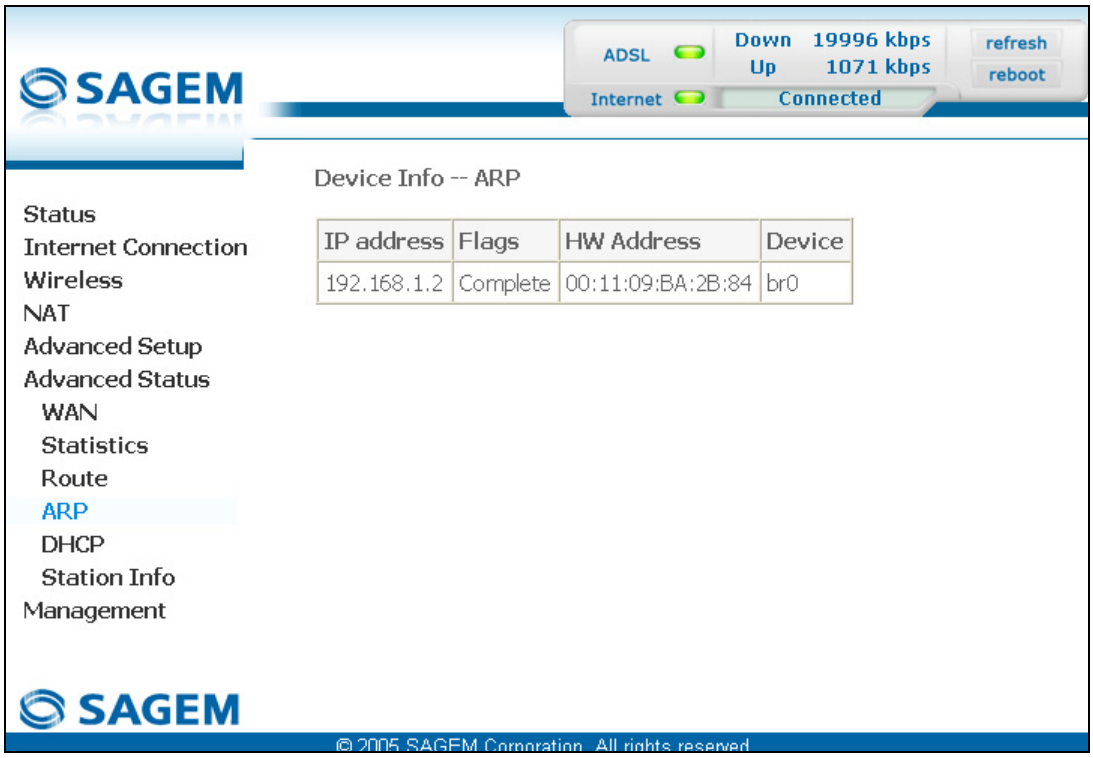
- Select the **Route** menu in the **Advanced Status** section to display the following screen:



5.10.4 ARP

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

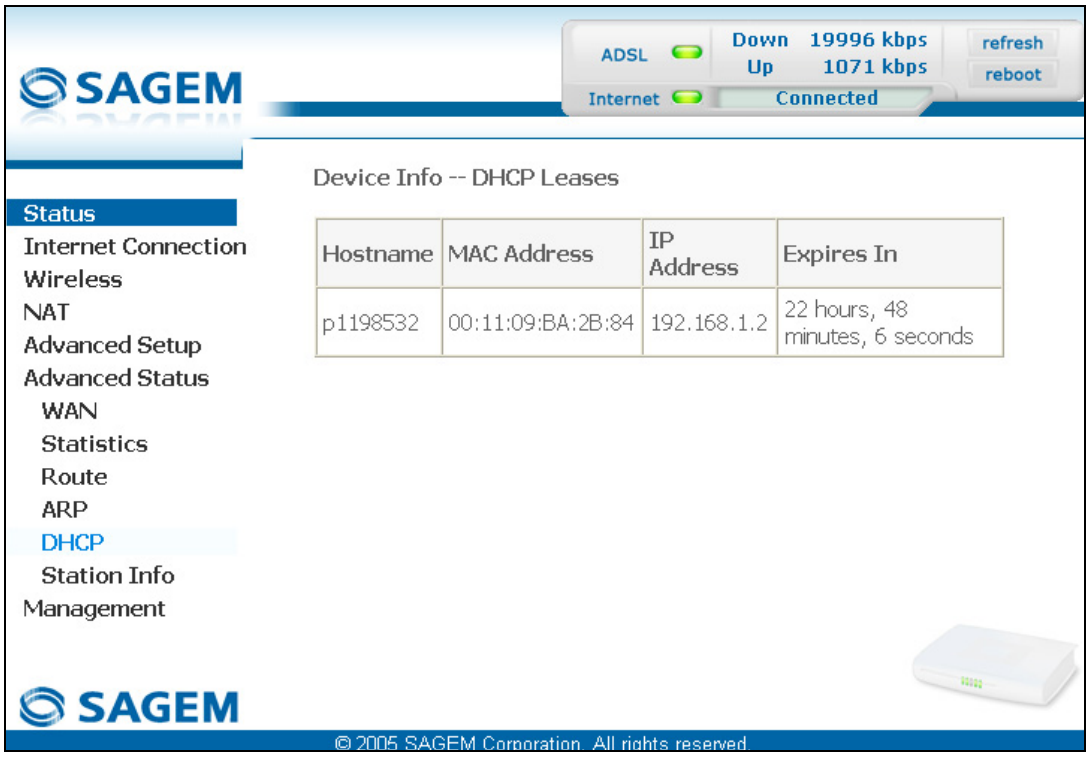
- Select the **ARP** menu in the **Advanced Status** section to display the following screen:



5.10.5 DHCP

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

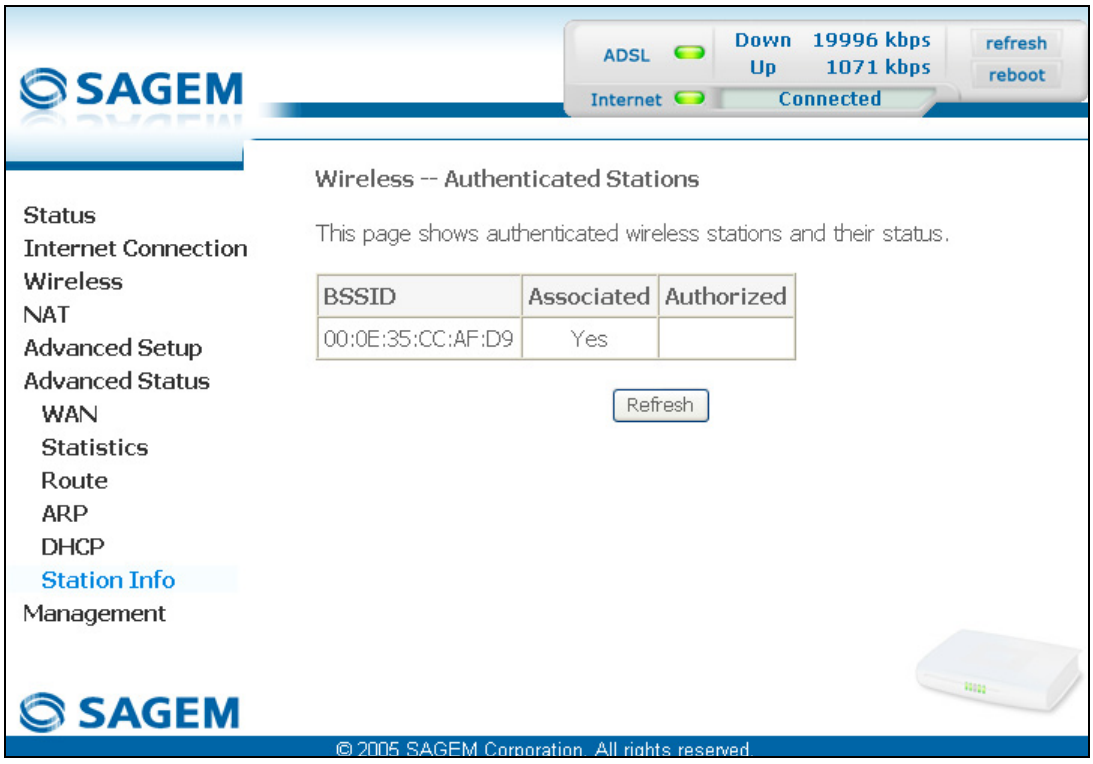
- Select the **DHCP** menu in the **Advanced Status** section to display the following screen:



5.10.6 Station Info

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

- Select the **Station Info** menu in the **Advanced Status** section to display the following screen:



- Click on the Refresh button to refresh screen.

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 5.7.3 - MAC Filter).

5.11 Management

Object: This menu lets you manage your router.

This section contains the following seven menus:

- Settings (see subsection 5.11.1),
- System Log (see subsection 5.11.2),
- SNMP Agent (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),
- System Info (see subsection 5.11.8),
- Save/Reboot (see subsection 5.11.9).

5.11.1 Settings

This menu contains the following three sub menus:

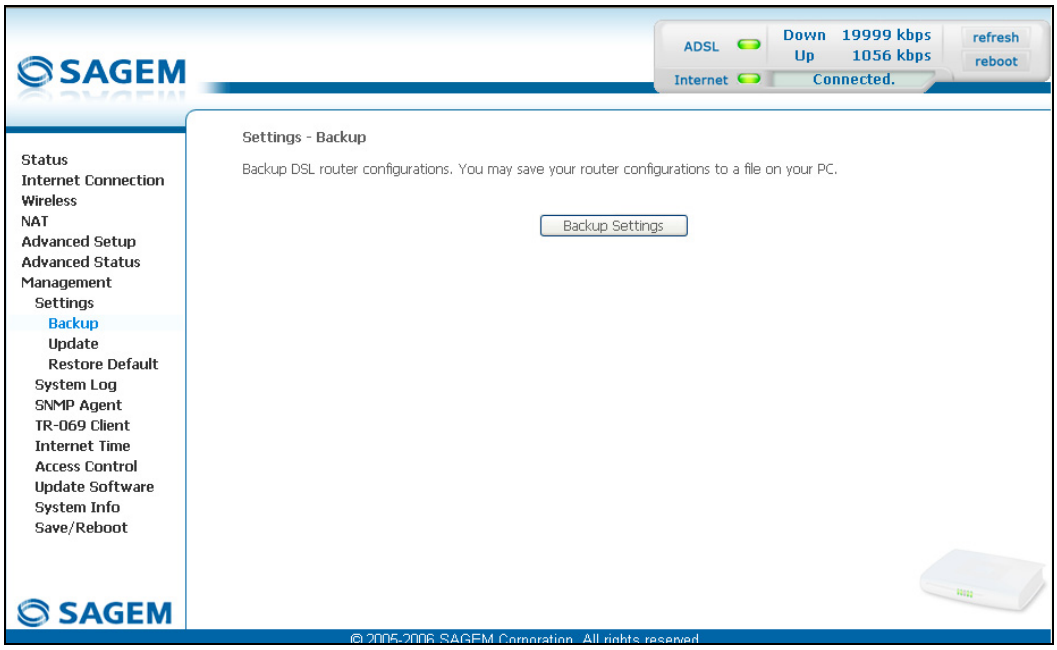
- Backup (see subsection 5.11.1.1),
- Update (see subsection 5.11.1.2),
- Restore Default (see subsection 5.11.1.3).

5.11.1.1 Backup

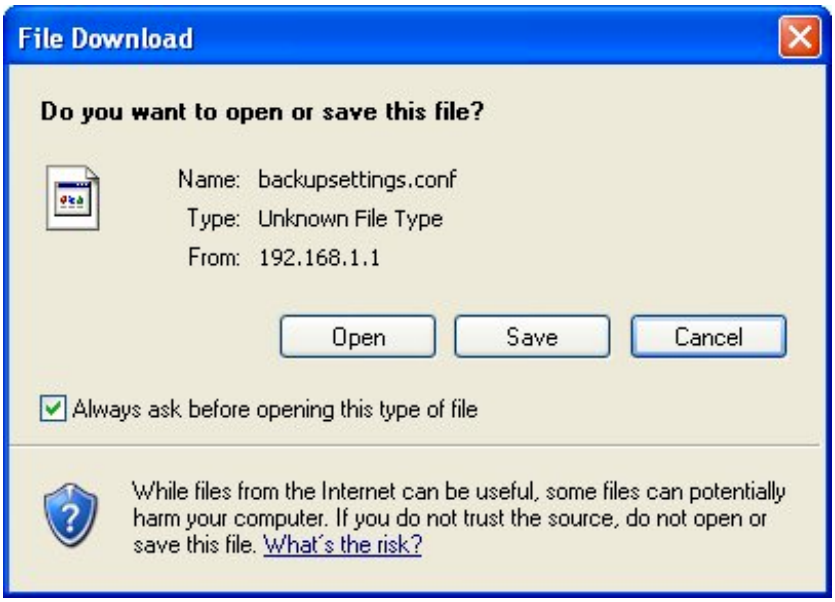
Object: This menu is used to backup the current configuration to a file with a .conf extension.

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

- Select the **Backup** sub menu in the **Settings** menu of the **Management** section to display the following screen:



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



Save

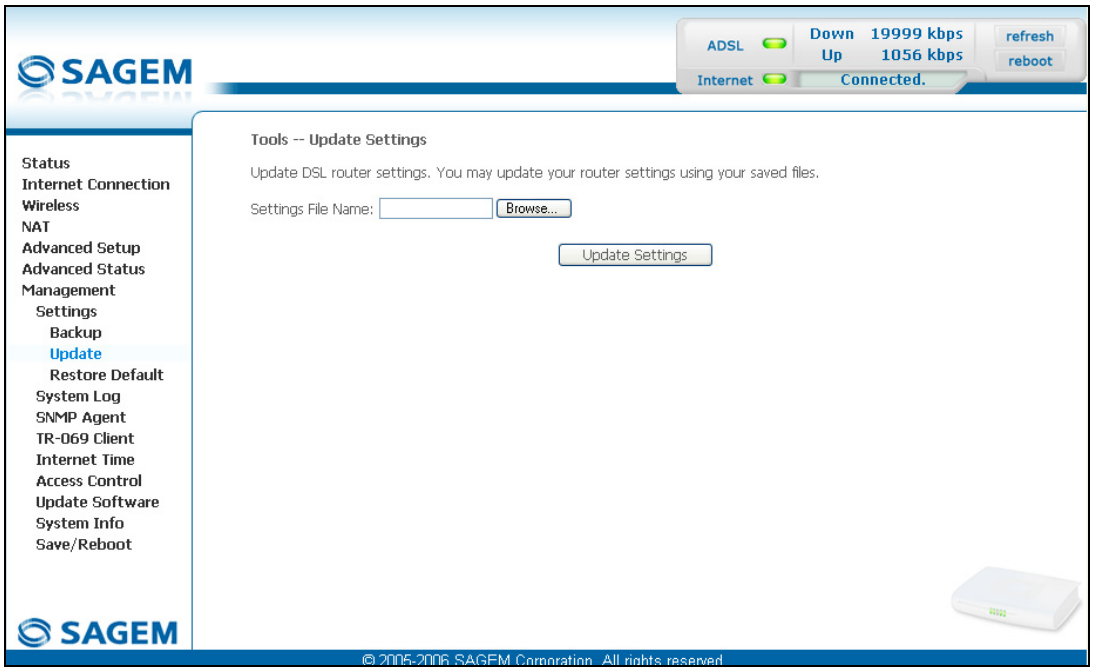
- Click on the **Save** button to save the current configuration file, for example, on your computer.
- Select the directory where you want to save the "backupsettings.conf" configuration file.

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.

- Select the **Update** sub menu in the **Settings** menu of the **Management** section to display the following screen:



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.

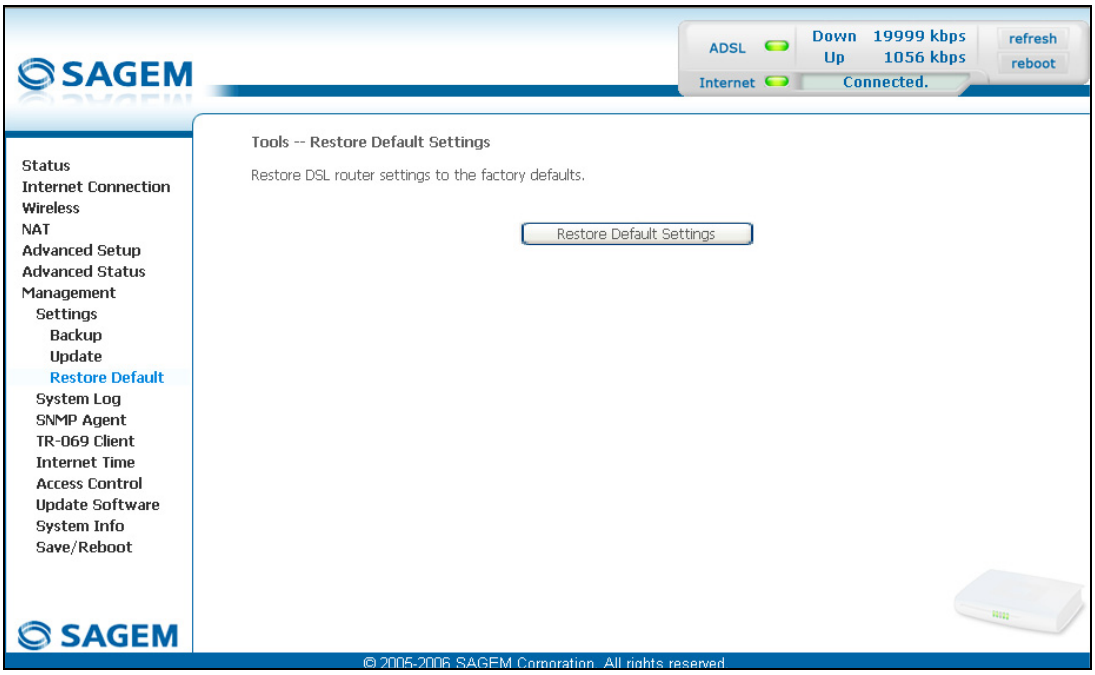
The process takes around 2 minutes.

5.11.1.3 Restore Default

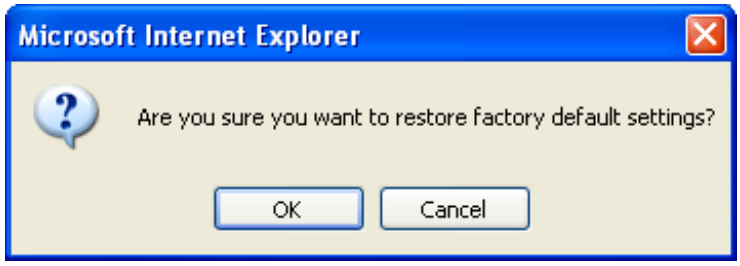
Object: This menu is used to return to factory configuration.

The existing configuration is completely overwritten.

- Select the **Restore Default** sub menu in the **Settings** menu of the **Management** section to display the following screen:



- click on the **Restore Default Settings** button and the following screen appears:



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

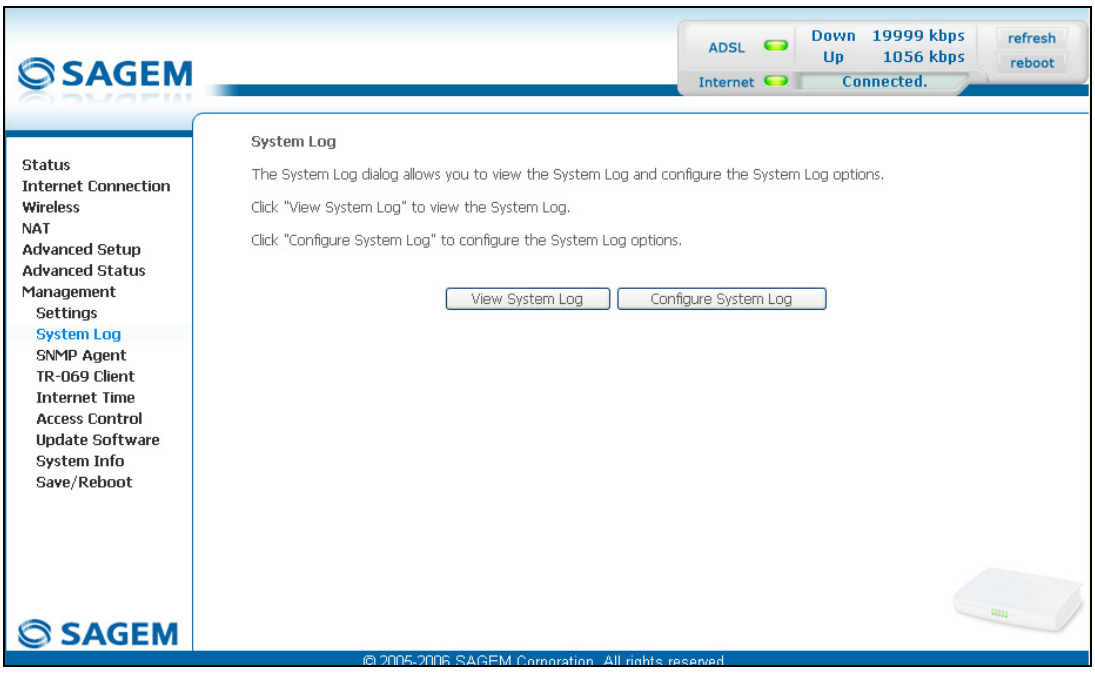
A few moments after, the screen of the "Internet Connection" menu appears. Refer to paragraph 5.6.

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

5.11.2 System Log

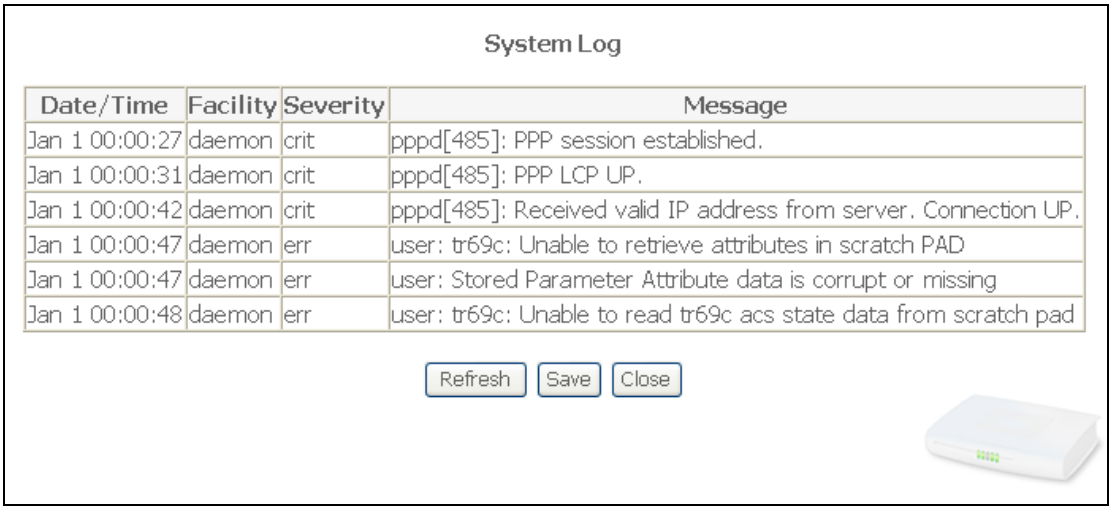
Object: This menu is used to view and/or configure the events which occur on your router.

- Select the **System Log** menu in the **Management** section to display the following screen:



View System Log

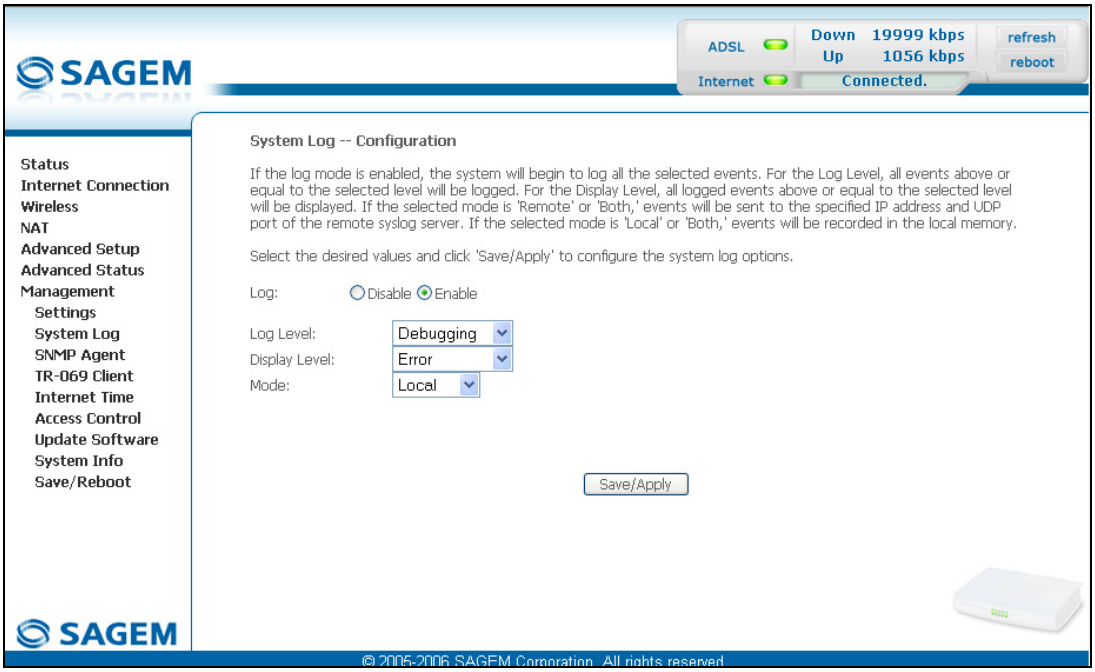
- Click on the **View System Log** button to display the events with the severity you configured (see table in the next paragraph - "**Configure System Log**").



- Click on the **Save** button to save all the events allocated to the severity you configured.

Configure System Log

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



Field	Action	Default
Log	Select **Enable** to activate the saving of all the events to a log and display on screen or **Disable** to deactivate.	**Enable**
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, • 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 severities are classified in decreasing order of importance. • Emergency, • Alert, • Critical, • Error, • Notice, • Informational, • Debugging.	**Error**

Field	Action	Default
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[13]	Enter the IP address of the "Syslog" address on which all the events will be saved.	**0.0.0.0**
Server UDP Port[13]	Enter the number of the port associated with the "Syslog" server.	**514**

[13] This field only appears when the mode selected is "Remote or "Both".

5.11.3 SNMP Agent

Subject: This menu allows to configure your SNMP agent. SNMP (**S**imple **N**etwork **M**anagement **P**rotocol) allows to manage the elements of network from a supervision station also called "Manager".

Select **SNMP Agent** menu in the **Management** section ; the following screen appears:

In the SNMP Agent field, click on the relevant box to **Disable** or **Enable** your SNMP Agent.

Inform the fields as shown in the table herafter:

Read Community	You can to preserve "public" or enter another name for the SNMP Agent (for example the computer connected to your router). **Note:** These rights are **Read only** (RO).	public
Set Community	You can to preserve "private" or enter another name for the SNMP Manager integrated into your router. **Note:** The rights are **Read / Write** (RW).	private
System Name	Enter the name of the SNMP server.	Sagem
System Location	Enter the place where is your SNMP server.	unknown

Field	Action	Default value
System Contact	Enter the "URL" or "IP address" of the SNMP server.	unknown
Trap Manager IP	Enter the IP address towards which the traps of the hosts are directed. **Note:** This is the gateway address of your router.	0.0.0.0

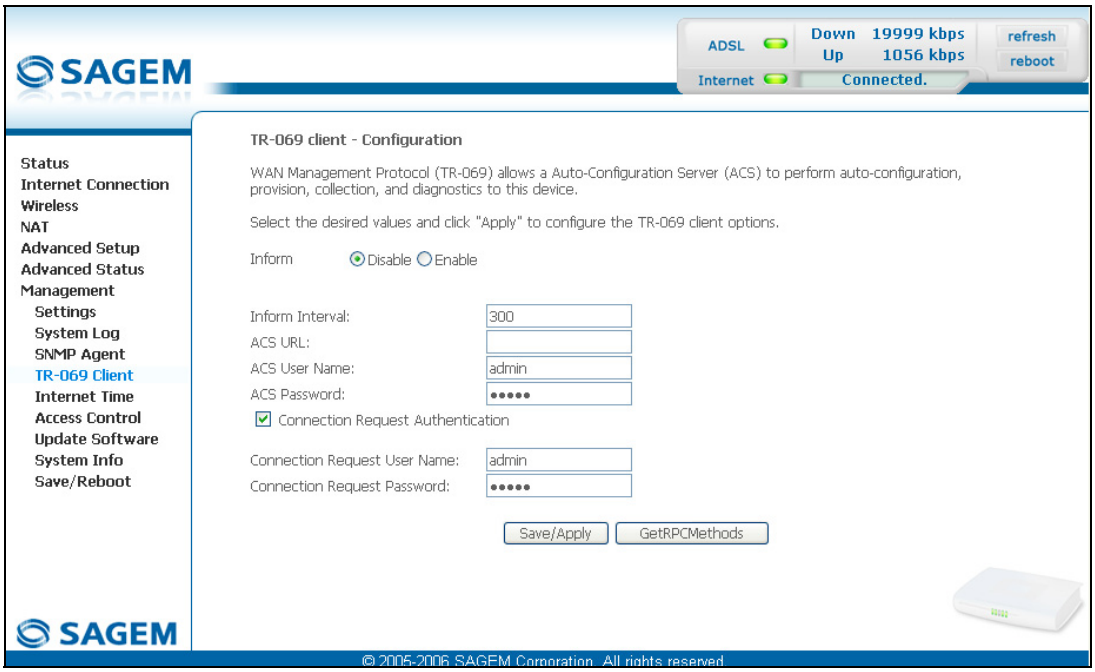
Hereafter, an example of SNMP configuration:

Field	Action
Read Community	Iris (RO)
Set Community	Cyclamen (RW)
System Name	rose
System Location	France
System Contact	Myrouter@sagem/com
Trap Manager IP	192.168.1.1

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".

- Select the **TR-069 Client** menu in the **Management** section to display the following screen:



Field	Action	Default
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.	**Empty**
ACS User Name	Enter the name of the user of the "ACS" server.	**admin**
ACS Password	Enter the "ACS" server password.	**admin**

Field	Action	Default
Connection Request User Name	Enter the name of the user of your router.	**admin**
Connection Request Password	Enter your password for your router.	**admin**

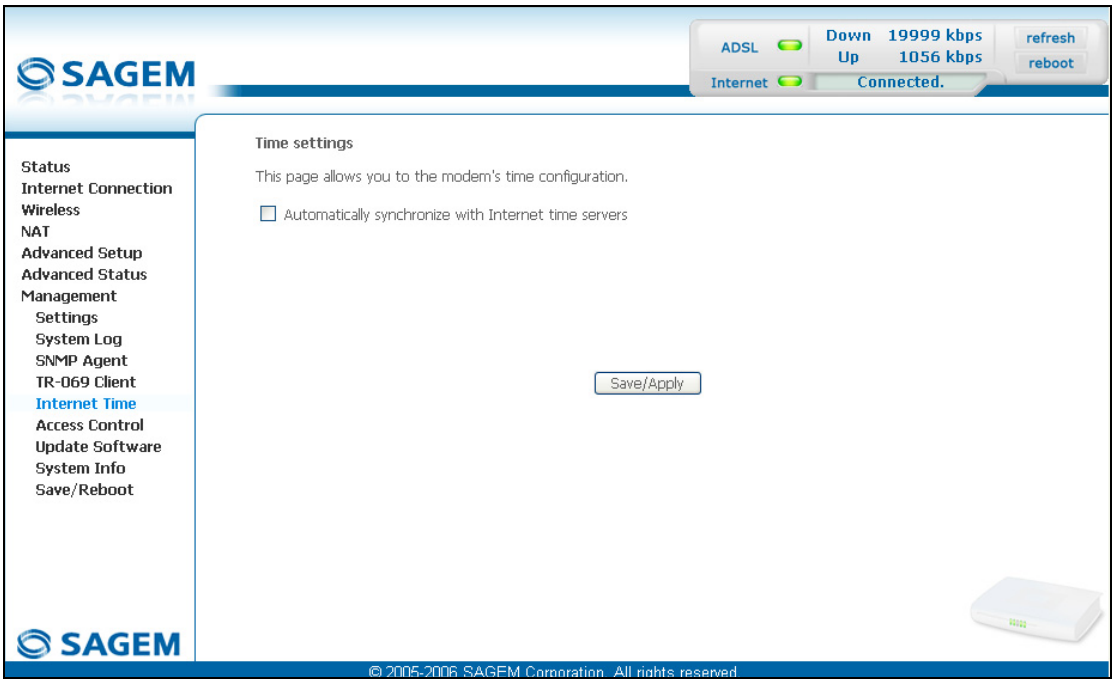
- Click on the GetRPCMethods button to launch the auto-configuration procedure of your router.

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.

- Select the **Internet Time** menu in the **Management** section to display the following screen:



Field	Action	Default
Automatically synchronize with Internet time servers	Do not check 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 "Status/Summary" and "Management/System Log" screen) displays the date and time delivered by the NTP servers (**N**etwork **T**ime **P**rotocol) 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.	**Box not checked**

Field	Action	Default
First NTP time server	Select a first NTP server from the scroll down list.	**Clock.fmt.he.net**
Second NTP time server	Select a second NTP server from the scroll down list.	**None**
Time zone offset	In the scroll down list, select the appropriate correction (GMT+1 - Paris for example) to adjust the GMT time to that of the country where you live with the seasonal correction (Summer time or Winter time).	**(GMT-12:00) International Date Line West**

5.11.6 Access Control

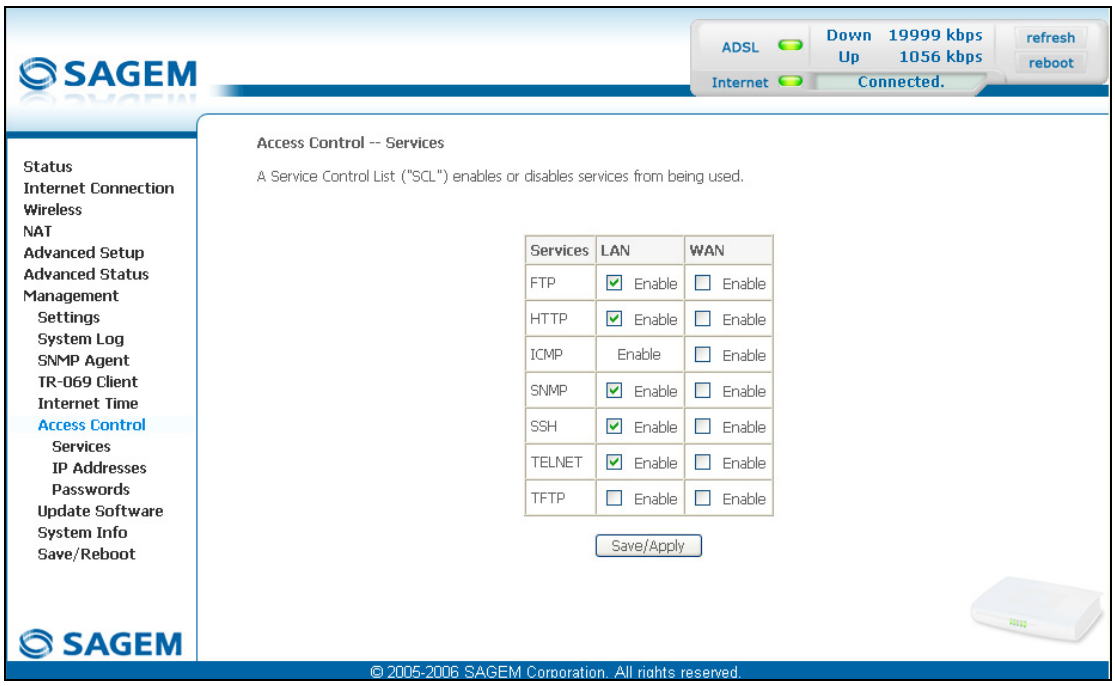
This menu contains the following three sub menus:

- Services (see subsection 5.11.6.1),
- IP Address (see subsection 5.11.6.2),
- Passwords (see subsection 5.11.6.3).

5.11.6.1 Services

Object: this sub menu is used to activate or deactivate Services such as FTP, FTPP etc.

- Select the **Services** sub menu in the **Access Control** menu of the **Management** section to display the following screen:



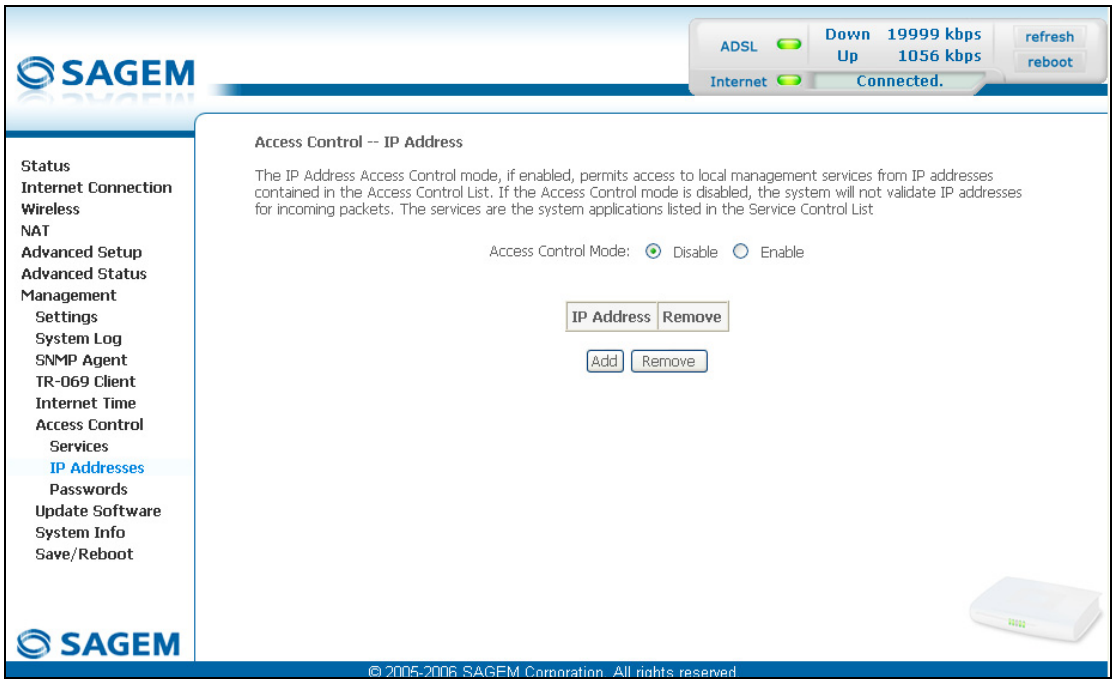
The table displayed in the screen above indicates that the services listed such as FTP, HTTP, ICMP, SNMP, SSH, TELNET and TFTP are all activated ("Enable" box checked) on the local network (LAN) and deactivated ("Enable" box not checked) on the remote network (WAN).

Check the **Enable** box to activate the selected service on the local network (LAN) or on the remote network (WAN).

Note: The ICMP service is always activated on the local network (LAN) and may be activated or deactivated on the remote network (WAN).

5.11.6.2 IP Address

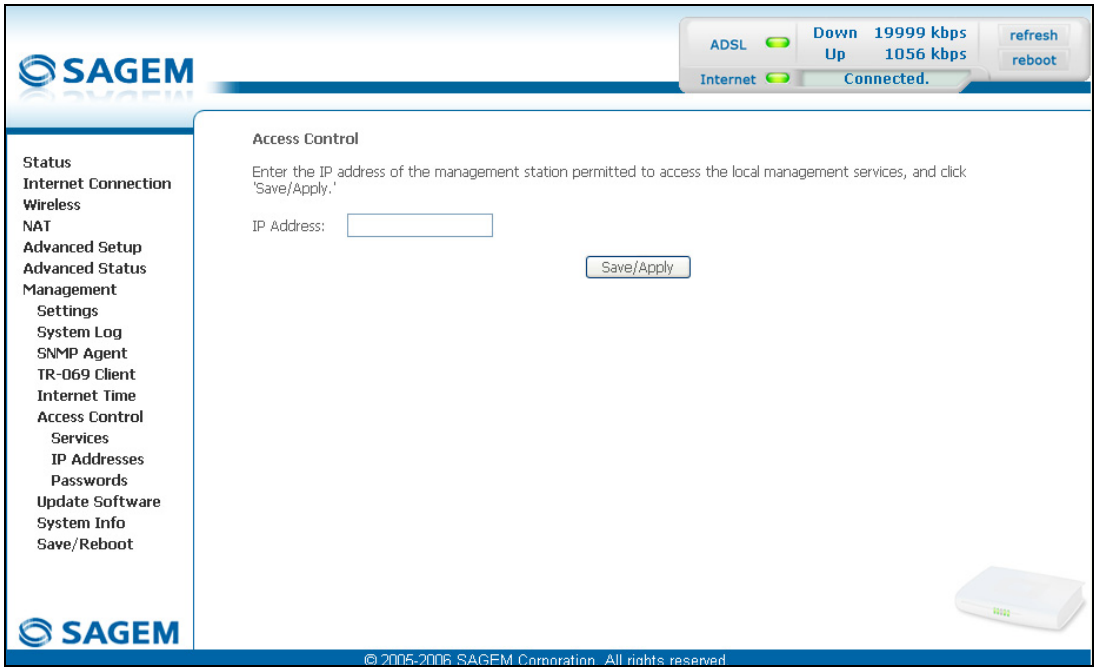
- Select the **IP Address** sub menu in the **Access Control** menu of the **Management** section to display the following screen:



Field	Action	Default
Access Control Mode	Select **Enable** to activate the access control mode or **Disable** to not activate it.	**Box not checked**

Add

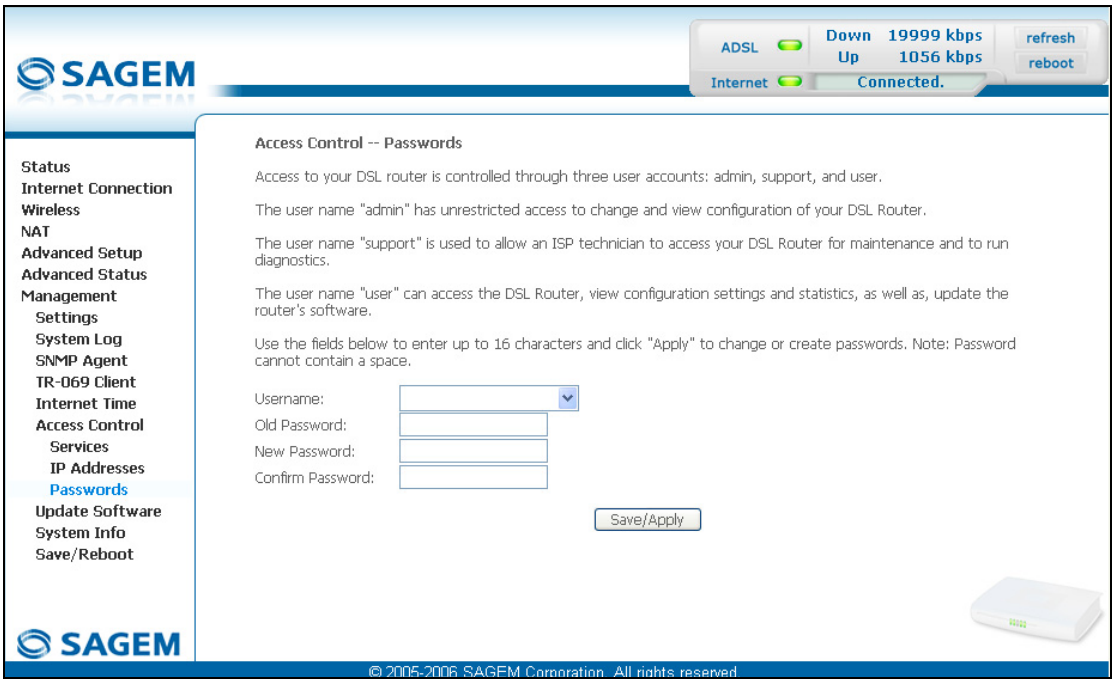
Click on the **Add** button to add an IP address.



Note: From this address you may access the local management services when the access control is active.

5.11.6.3 Passwords

- Select the **Passwords** sub menu in the **Access Control** menu of the **Management** section to display the following screen:



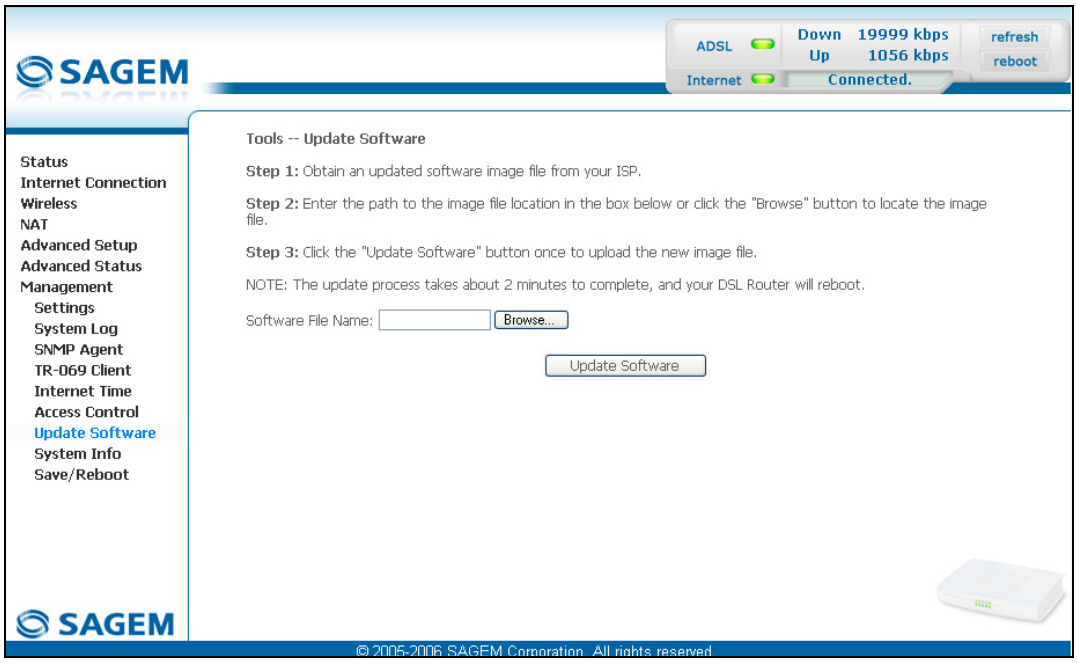
Field	Action
User Name	Select a user name from the scroll down list: • Admin, • Support, • User. **Note:** This list has been established in increasing order of restriction.
Old Password	Enter your old password
New Password	Enter your new password
Confirm Password	Confirm your new password

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.

- Select the **Update Software** menu in the **Management** section to display the following screen:



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.

The process takes around 2 minutes.

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

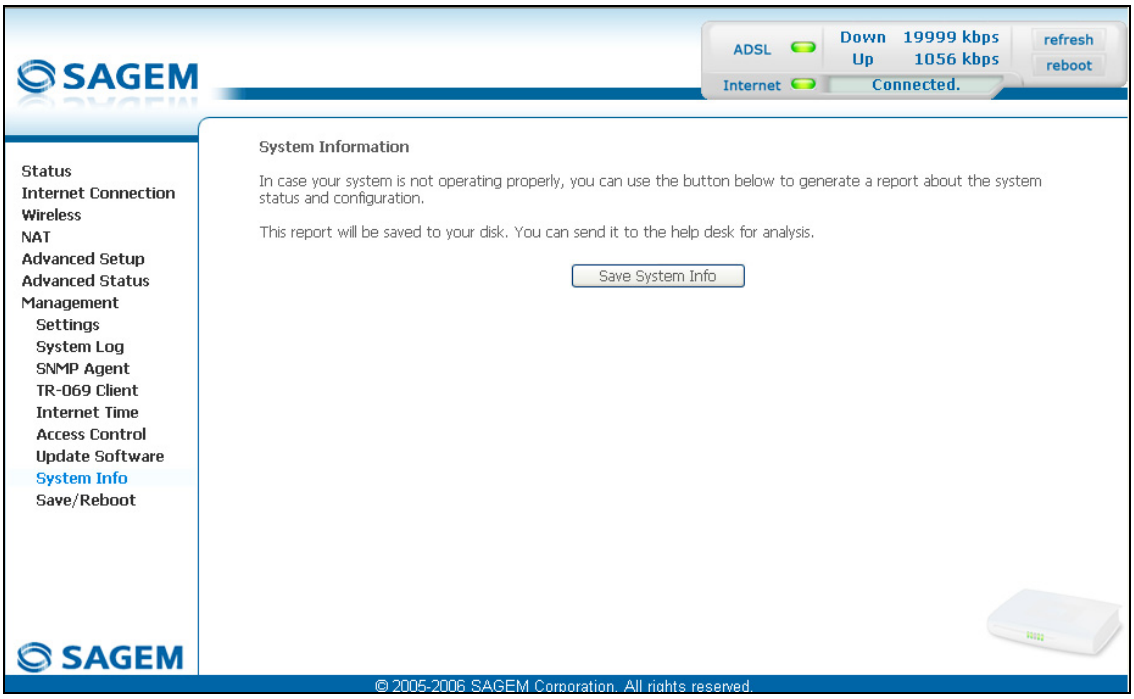
Throughout the download procedure (up to five minutes), **you must**:

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

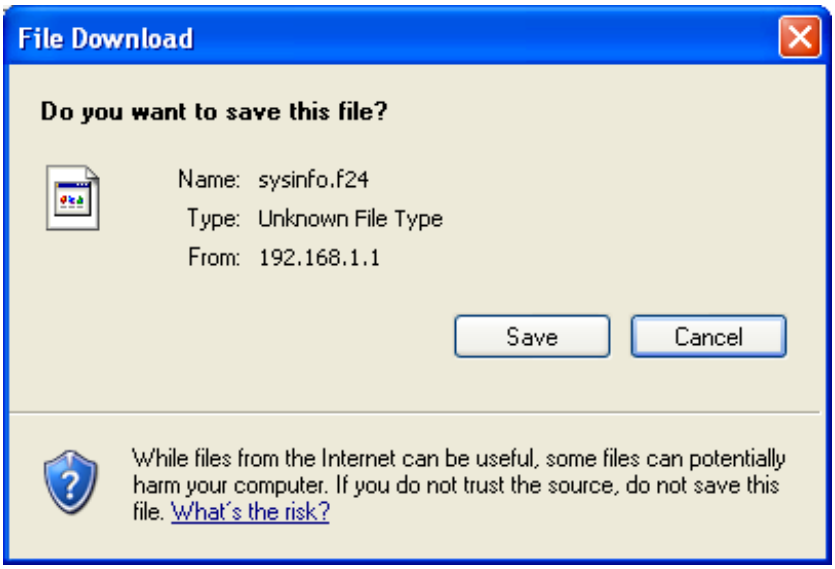
5.11.8 System Info

Subject: This menu allows to generate a report about the system status and configuration and to save the current report in a file (sysinfo) with f24 type.

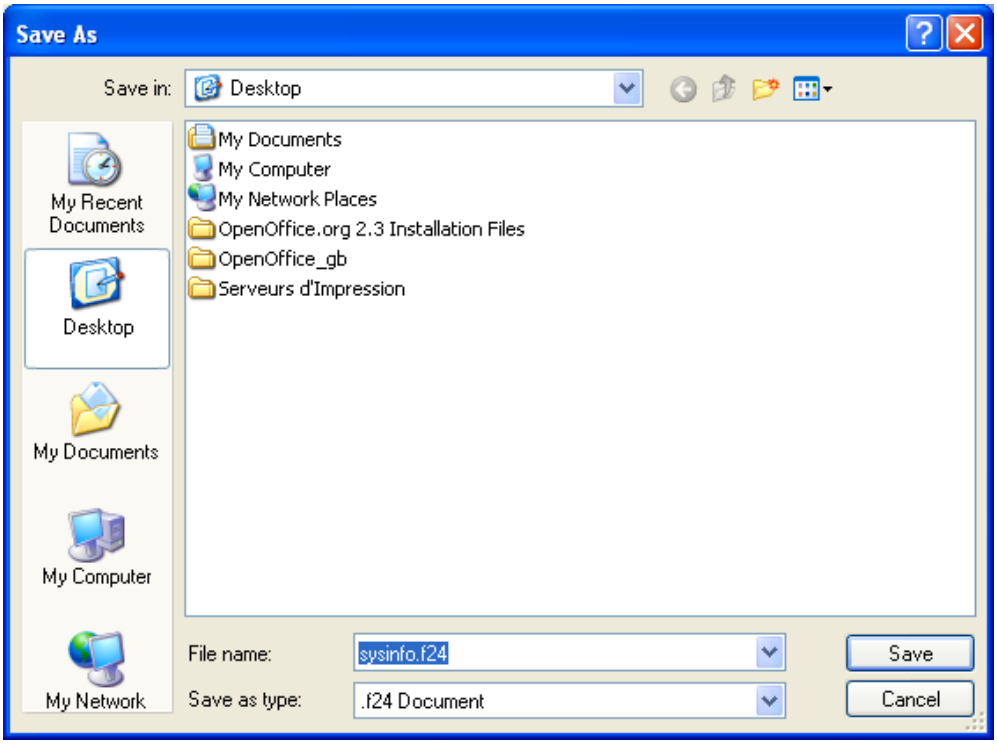
- Select **System Info** menu in the **Management** section ; the following screen appears:



- click on the Save System Info button to generate a report ; the following screen appears:



- click on the Save button to save ; the following scren appears:



The "sysinfo.f24f" appears in the **File name** field. You can rename this file and save in the path that you wish.

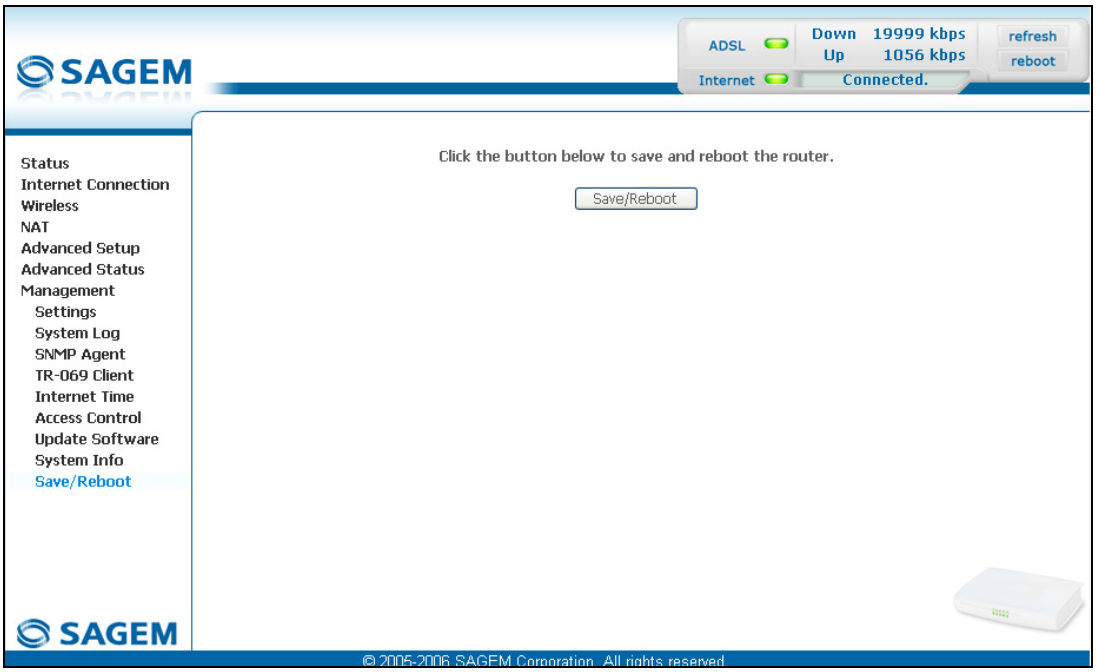
- click on the Save button to validate.

Note: This file can be opened with different apllications as spreadsheet program, word processing for example Microsoft Excel, Microsoft Word, Notepad and so on.

5.11.9 Save/Reboot

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

- Select the **Save/Reboot** menu in the **Management** section to display the following screen:



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

The process takes around 1 minute.

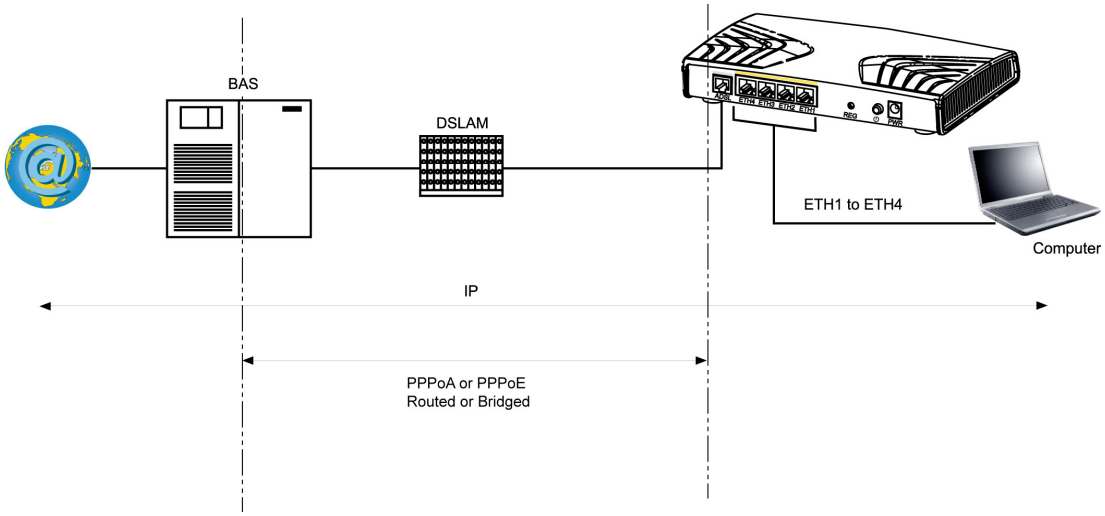
A countdown is displayed to tell the user how long is left to wait.

6. Internet access service

This section covers	➢ of the introduction	P6-2

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.



Using your installation CD-ROM you can quickly obtain Internet access.

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 menu **Internet connection** of the HTTP configurator (PPP Username, PPP Password).

Observation: 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

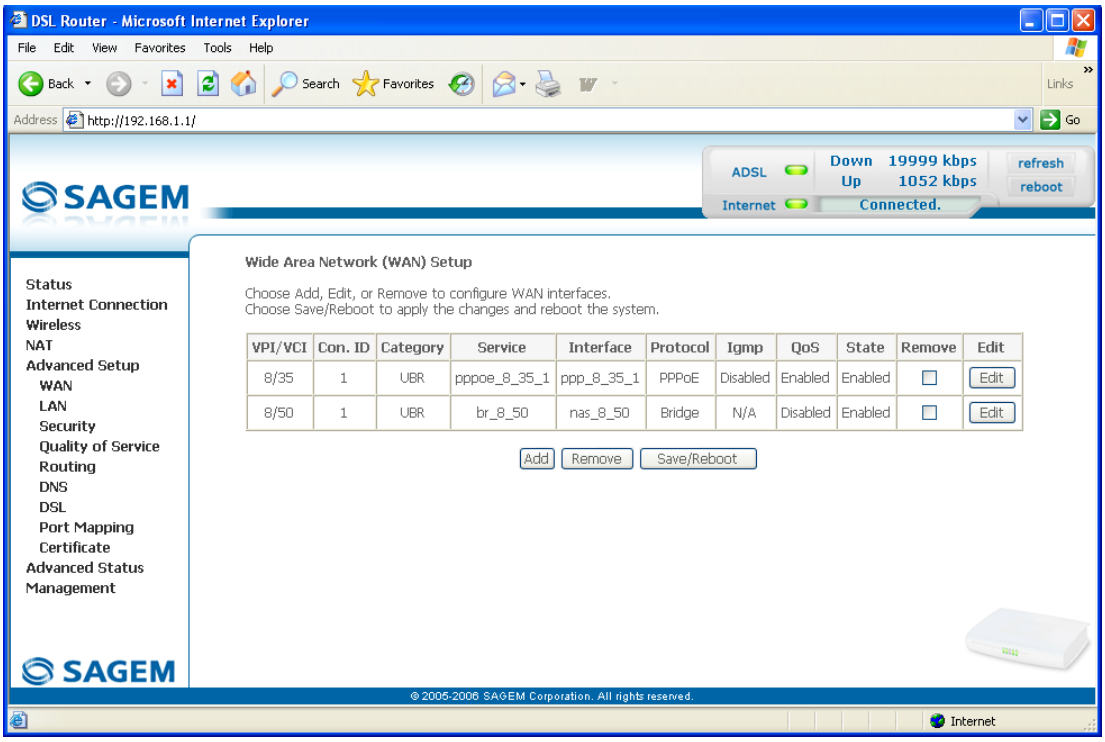
7.1 Introduction

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 2.2.4,
- 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.

- configure "Port Mapping" in accordance with section 6.9.8.

8. Updating the firmware

This section covers	➢ setting up the download.	P8-2

Three possibilities are offered to you for updating the firmware:

- via HTTP,
- via TR69 protocol.

If necessary, the new firmware version download is performed automatically on starting up the router.

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

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

During the download, the eight LEDs of your router lights in turn except the ⏻ LED that stays on steady.

When the download is finished, your **router** restarts automatically to the new firmware version.

To check that the new version has been correctly downloaded, click top left in the home screen, on the **Status / Summary** heading ; the last software version displays in the "**Software Version**" field.

HTTP update

You can download the new firmware to update your router as indicated in subsection 5.5.7 of the HTTP configurator.

TR69 protocol

Operators can use "TR69" protocol to upgrade the router's firmware from an HTTP or FTP server.

A. 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 with the factory configuration	§ A.7
	➢ no-connection mode	§ A.8

A.1 Checking the assignment of an IP address

In Windows Vista, XP, 2000 and ME

- Click button **Start**, select **Execute**, enter **cmd** and then click **OK**; the command prompt screen appears. Enter **ipconfig** and then confirm by pressing **Enter**.
- Check that the entry IP Address contains a value other than **0.0.0.0** (**192.168.1.10** for example).

If no address is displayed on the screen, enter **ipconfig /release** followed by **ipconfig /renew**.

All the troubleshooting procedures described below are undertaken in **Windows® XP**. These procedures in other Windows operating systems® (98, ME and 2000) can be slightly different.

To help locate the fault, the user has the following sources:

- States of Front panel LEDs,
- Data accessible by the configurator by "DSL Router" onboard HTTP of your router:
  - supervision of the router,
  - "Diagnostics" tool.

A.2 Front panel LEDs

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

Status	Colour	⏻	✓	Wi-Fi	@
Lit steady	Green	Power On	ADSL Up	Wi-Fi activated	A PPP session has been created
	Amber	x	x	x	ADSL link is established
Flickering	Green	x	x	Wi-Fi Tx/Rx	Tx/Rx traffic
Blinking	Amber	x	x	x	ADS is training
Slow Blinking	Green	x	Line not detected	Wi-Fi pairing	x
Fast Blinking	Green	x	ADSL synchronisation training	x	x
Off	Green	Power Off	x	Wi-Fi deactivated	Power Off or Bridge mode or ADSL down

Status	Colour	1	2	3	4
Lit on steady	Green	Ethernet port (ETH1, ETH2, ETH3 or ETH4) has detected a link with 100 Mbps device			
Flickering		Tx/Rx traffic at 100 Mbps			
Lit on steady	Amber	Ethernet port (ETH1, ETH2, ETH3 or ETH4) has detected a link with 10 Mbps device			
Flickering		Tx/Rx traffic at 10 Mbit/s			
Off	x	No link detected on the Ethernet port			

A.3 Supervising your router

The supervision box is permanently displayed in a frame at the top right of each window of the configurator.

LEDs

ADSL	**Green** : Synchronised ADSL line. **Red** : ADSL line not connected.
Internet	**Green** : Public IP address (WAN) distributed to the router. **Yellow** : Synchronised ADSL line. **Red** : Public IP address (WAN) not distributed to the router, or ADSL line not connected.

Transmission rate

Down	Displays the nominal down line transmission rate
Up	Displays the nominal up line transmission rate

Buttons

Refresh	Allows data displayed on the screen to be refreshed.
Reboot	Allows your router to be started.

A.4 "Diagnostics" tool

To access this tool:

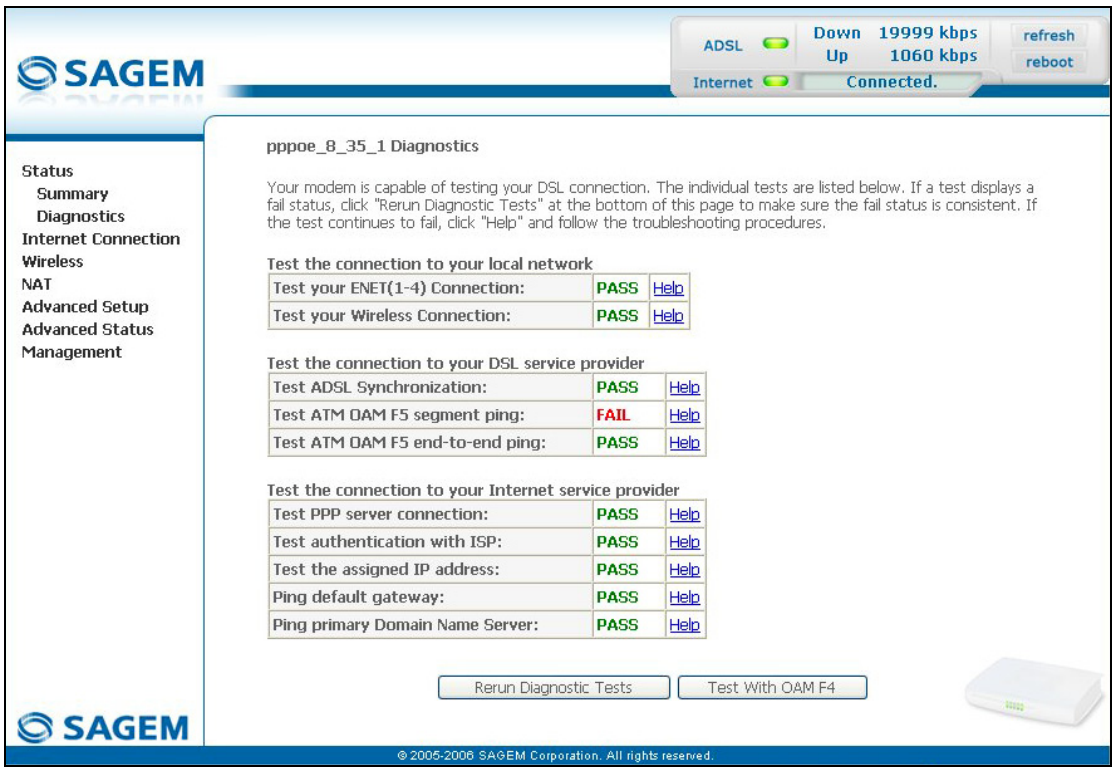
- open your browser and then, in the address bar, enter:
  - the following URL : http://myrouter,
  - or the following address : http://192.168.1.1.

a "Login" window appears; enter the login and password. Default:

- **admin** in the "User name" field,
- **admin** in the "Password" field.

You have access to the HTTP configurator of your router.

- select the heading "Diagnostics" in the suitable list to the left of each window; the following screen appears:



The results of the tests made by the "DSL router" configurator on your modem/router are displayed in the "Diagnostics" window. These tests concern the connections to the LAN, to your DSL Service Provider and to your **I**nternet **S**ervice **P**rovider (ISP).

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.

State of connection

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

If a test displays a "FAIL" state, click on "Help" and then the button "Rerun Diagnostic Tests" at the bottom of the "Help" page, to check that the test has been conclusive. If the test still displays "FAIL", you must follow the troubleshooting procedure displayed on this page.

IMPORTANT

If you experience difficulties connecting to the Internet, we recommend that you restart your router (cf.A.6) or possibly re-establish the factory configuration (cf. § A.7).

A.5 Interpreting the LEDs

A.5.1 The "ADSL" LED blinks slowly

- Check the connection of your ADSL filters. Each telephone socket of your installation which is used must be equipped with an ADSL filter.
- 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.
- Finally, check with your ISP on the availability of the ADSL service 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, check the box "Enable Wireless" in the "**Basic**" menu of the "**Wireless**" heading of the HTTP configurator (see sub-section 5.7.1).

A.5.3 All LEDs are off

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

A.6 Restarting your router

When your router does not operate properly, we advise you to restart it:

- switch off the button located on the rear panel of your router then switch it on again.

or

- click on the "**Reboot**" button located in the top right of the welcome page of your HTTP configurator.

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

The LED lights in first followed-up by the four Ethernet LEDs (1 to 4), then these last light out. The and Ethernet (that which corresponds to the connected interface) LEDs light on steady and the LED blinks during the time of the establishment of the ADSL link then lights on steady like the LED. The LED lights "**Red**" on steady then lights "**Green**" on steady when a PPP session has been created.

Note: It lasts around one minute.

A.7 Returning to the factory configuration

If you loose your password or if, after having entered new parameters in your router, you cannot access the Internet nor the HTTP configurator, 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 ISP (**I**nternet **S**ervice **P**rovider) (see Internet Connection - subsection 5.6)

To return to the factory configuration:

- In the top left of your configuration tool's welcome page, select the **Management** heading then the **Restore default** sub-menu in the **Setting** menu.
- or press and hold for about 10 seconds on the button marked "**REG**" on the back of your router.

This operation deletes the entire personalised configuration of your router: Password, Configuration, etc.

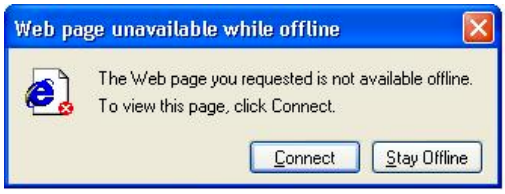
After a return to factory configuration, it is **necessary to install your router again** using the installation CD-ROM, or to enter again the ADSL connection data supplied by your **I**nternet **S**ervice **P**rovider (ISP) (see Internet Connection section - § 5.6).

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**.

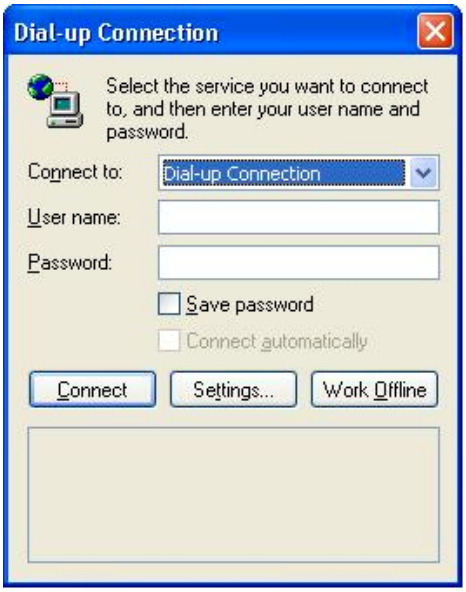
The screen opposite appears.

Click Connect .



The screen opposite appears.

Click Settings... .



The screen opposite appears.

Select the Connections tabs and then the "**Never dial a connection**"[1].

Click OK to confirm your choice.

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.

[1] When the router is installed, this box is checked.

B. Annex B - Warnings for safety

This section covers	➢ Warnings for safety	§ B.1
	➢ the 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[1]
PWR	DC Power Supply port	SELV [2]
ADSL	ADSL port	TNV3[3]
ETH1 to ETH4	Ethernet port	SELV [2]

B.2 EC compliance declaration

CE !

This equipment can be operated in the EU without restrictions indoor, but cannot be operated outdoors in France in the whole of the band until further notice.

Sagem Communications declares that the **SAGEM F@st™ 2604/2644** product conforms to the requirements of European directives 1999/5/CE and the essential requirements of directives 2004/108/CE and 2006/95/CE.

The EC déclaration of conformity for the **SAGEM F@st™ 2604/2644** product is made within the framework of the R&TTE directive.

[1] **H**azardous **P**rimary **V**oltage circuit
[2] **S**afety **E**xtra **L**ow **V**oltage Circuit
[3] Level **3** **T**elecommunication **N**etwork **V**oltage

C. 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 **Sagem Communications**.
Sagem Communications' 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.

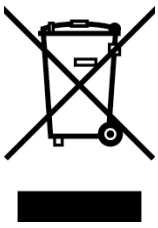
PACKAGING

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 **E**lectrical **E**lectronic **E**quipment **W**aste, which can have an effect on the environment and health.

D. Annex D - Technical Characteristics

This section covers	➢ mechanics and displays	§ 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	: 190 mm
	• Depth	: 143 mm
	• Thickness	: 34 mm
Weight of router		: 290 g

Display		
Marking	**Abbreviation**	**Meaning**
	**PWR**	• **Green Power LED**
	**ADSL**	• **Green ADSL LED**
	**WLAN**	• **Green WLAN LED**
	**Internet**	• **Green/Red Internet 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 ou interleaved)
TX Power	• 12,5 dB
Access Impedance	• 100 Ω
Range	• According to standard G.992.1 table Annexe G
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 802.11b DSSS**
Frequencies band	• 2412 MHz to 2472 MHz (ISM band)
Transmission rate	• 1/2/5.5/11 Mbit/s
Modulation method	• DBPSK, DQPSK, CCK
Safety	• WEP 64 / 128 bits
	• Filtering by list of MAC addresses
	• WPA (encryption mode: TKIP or AES)
Range	• Up to 300 m in free space
	• 10 to 100 m inside buildings
Standard	• **IEEE 802.11g OFDM**
Frequencies band	• 2412 MHz to 2472 MHz (ISM band)
Transmission rate	• 6 / 9 / 12 / 18 / 24 / 36 / 48 / 54 Mbit/s
Modulation method	• OFDM, CCK
Safety	• WEP 64 / 128 bits
	• Filtering by list of MAC addresses
	• WPA (encryption mode: TKIP or AES)
Range	• 200 m in free space
	• 30 m inside buildings

Mains Power Supply	
Type	• Plug-in external adapter unit
Class	• II
Input voltage	• 200 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

Electromagnétic 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 forpour ISM band at 2.4 GHz	
Transmission 802.11g/b	• 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	• Par protocole
	• By IP address
	• By port
	• Statefull / Stateless
IP QoS	• DiffServ

ATM charactéristics	
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, USB and WAN (with specific option)
Downloading of version	• Client by http mode
CLI	• Telnet
TR69	• Via a ACS server

E. Annex E - Default configuration

This section covers	➢ the default username and password	§ E.1
	➢ the default configuration for the local network (LAN)	§ 0
	➢ the default configuration for the local wireless network (WLAN)	§ E.3

This section indicates the values of the default parameters of your **SAGEM F@st™ 2604/2644** when it leaves the factory.

These default parameters can be modified by a particular preconfiguration of your **SAGEM F@st™ 2604/2644**.

E.1 Default username and password

Username	**admin**
Password	**admin**

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 gives the values of the principal LAN parameters of your **SAGEM F@st™ 2604/2644** (**ETH1** to **ETH4**) :

LAN characteristics	Value	State
ETH1 IP address ( )	192.168.1.1/24	Internet and HTTP configurator access (bridged)
ETH2 IP address ( )		
ETH3 IP address ( )		
ETH4 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 **SAGEM F@st™ 2604/2644**.

Wireless

Characteristics (Wi-Fi)	Value
IP address	**192.168.1.1/24**
Enable Wireless	**Box checked**
SSID	**Sagem2604**
Channel	**Auto**
Network Autentication	**No**

Annexe E - Configuration par défaut

F. 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**uthentification **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**ransfert **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
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 Routing
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 of **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**ubNetwork **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

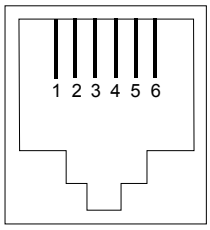
VBR-rt	**V**ariable **B**it **R**ate - **r**eal **t**ime
VC	**V**irtual **C**hannel
VCC	**V**irtual **C**hannel **C**onnection
VCI	**V**irtual **C**hannel **I**dentifier
VC MUX	**VC** M**u**ltiple**X**ing (encapsulation sans en-tête)
VP	**V**irtual **P**ath
VPI	**V**irtual **P**ath **I**dentifier
VPN	**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 (réseau sans fil)
WLAN	**W**ireless **L**ocal **A**rea **N**etwork
WPA	**W**ireless **P**rotected **A**ccess

G. Annex G - Connector Technology

This section covers	➢ pinouts of the "**ADSL**" connector	§ G.1
	➢ pinouts of the "**PWR**" connector	§ G.2
	➢ pinouts of the "**ETH1**", "**ETH2**", "**ETH3**" and "**ETH4**" connectors	§ G.3

G.1 Pinouts of the "ADSL" 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

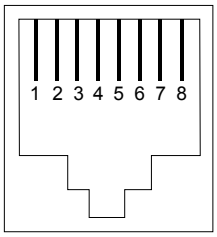
G.2 Pinouts of the "PWR" connector

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

Contact No	Signal	Meaning
Intérieur	+12 V	Connexion DC "+"
Extérieur	Masse	Connexion DC "-"

G.3 Pinouts of the "ETH1", "ETH2", "ETH3" and "ETH4" 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

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

Siège social : Le Ponant de Paris - 27, rue Leblanc - 75015 PARIS - FRANCE
Tél. : +33 (0)1 58 11 77 00 - Fax : +33 (0)1 58 11 77 77
http://www.sagem-communications.com

S.**A**.**S** au capital de 158 291 895 € - 440 294 510 RCS Paris