

Código: BHS\_RTA\_MAN\_AV\_ESPAÑA

Ed 1.0

Página 1 de 62

# BHS-RTA Manual de Usuario avanzado





## OBJETIVOS Y SERVICIOS DE VALOR AÑADIDO S.L.

### **BHS-RTA**

### Manual de Usuario avanzado







### **TABLA DE CONTENIDOS**

1	Introducción	3
1.1	LEDs e Interfaces	3
1.2	REQUERIMIENTOS DE SISTEMA	4
1.3	Características	4
2	Instalación Hardware	5
3	CONFIGURACIÓN WEB	7
3.1	Acceso al Dispositivo	7
3.2	CONFIGURACIONES	7
3.2	.1 Configuración de Internet	7
3.2	.2 Configuración de la Interfaz Inalámbrica	9
3.2	.3 Red Local	14
3.2	.4 Fecha y hora	16
3.2	5 Salida	17
3.3	Configuración Avanzada	17
3.3	.1 Advanced Wireless	18
3.3	.2 Apertura de Puertos	23
3.3	.3 DMZ	25
3.3	.4 SAMBA (Servidor de Ficheros)	26
3.3	.5 Configuración de conexión 3G	26
3.3	.6 Control parental	29
3.3		
3.3	3	
3.3	g	
3.3		
3.3		
3.3		
3.3	3,	
3.3	5	
3.3		
3.3	3	
3.4		
3.4		
3.4		
3.4		
3.4	• • • • • • • • • • • • • • • • • • • •	
3.4	J J	
3.4	( - 3 )	
3.5		
3.5	•	
3.5		
3.5		
3.5	- 5-	
3.5		
3.5	,	
3.5		
3.5	.8 Ayuda	62

Observa Telecom
Página 3 de 62

Código BHS\_RTA\_MAN\_AV\_ESPAÑA

Ed 1.0

### 1.- Introducción

El dispositivo soporta múltiples modos de línea. Con 4 interfaces Ethernet 10/100 base-T en el extremo de usuario, proporciona una conexión ADSL de alta velocidad.

Soporta conexión WAN por 3G, respaldo de conexión ADSL a través de 3G, compartición de ficheros de dispositivo USB en red LAN por SAMBA.

Conexión inalámbrica 2T2R cumpliendo con las especificaciones IEEE 802.11, 802.11b/g/n, seguridad WEP, WPA, y WPA2.

### 1.1.- LEDs e Interfaces

#### Panel frontal



La siguiente tabla describe los LEDs del dispositivo:

LED	Color	Estado	Descripción
Power		Apagado	El router está apagado
		Parpadeo Verde	El router está realizando el auto chequeo de arranque
	Rojo/Verde	Rojo Parpadeo de 2Hz /Fijo	Fallo en el auto chequeo de arranque.
		Verde fijo	Router encendido correctamente
		Encendido	La conexión Ethernet está establecida.
Ethernet	Verde	Parpadeo Verde	La conexión Ethernet está tramitando tráfico en alguno de los puertos Ethernet.
		Apagado	No hay conexión Ethernet establecida.
		Encendido	La conexión WiFi está disponible
Wifi	Verde	Apagado	La conexión WiFi no está disponible
		Parpadeando en Verde	Negociación o tráfico en la conexión.
		Verde fijo	WPS habilitado
WPS	Verde/Rojo	Parpadeo verde 2Hz	Ventana de Negociación WPS abierta.
		Rojo fijo (20 segundos)	Problemas en el registro WPS
		Parpadeando verde	Negociación
	Rojo/Verde	Verde fijo	Up
3G		Parpadeo verde rápido	Tráfico Tx/Rx en la línea
		Rojo fijo	Fallo de autenticación
		Apagado	El tráfico WAN está yendo por la conexión ADSL.
	Verde	Apagado	Router apagado
4561		Parpadeo 2Hz	Sin línea ADSL conectada
ADSL		Parpadeo 4Hz	Línea ADSL en estado de negociación
		Verde fijo	Línea ADSL establecida

### **BHS-RTA**

### Manual de Usuario avanzado

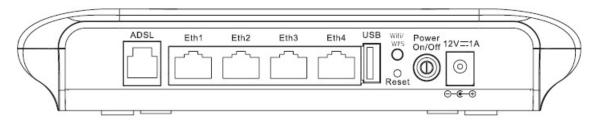


Ed 1.0



LED	Color	Estado	Descripción
		Parpadeando verde	Negociación PPP/DHCP
		Verde fijo	PPP/DHCP establecido
Internet	Verde/Rojo	Parpadeo verde rápido	Tráfico Tx/Rx en la línea
		Rojo fijo	Autenticación fallida

#### Panel trasero



La siguiente tabla describe los interfaces del dispositivo.

Interfaz/botón	Descripción
ADSL	Interfaz RJ-11 conectando a un punto de conexión telefónica a través de un cable telefónico.
Eth1/2/3/4	Interfaces Ethernet RJ-45 que conectan con los interfaces Ethernet de computadoras o dispositivos Ethernet.
USB	Para conectar un modem 3G u otro dispositivo de almacenamiento USB.
WLAN/WPS	Si se presiona el botón durante unos 4 segundos, se habilita/deshabilita la función inalámbrica.  Si se presiona el botón durante más de 10 segundos, se abrirá la ventana de negociación WPS.
Reset	Reinicia el modem a sus valores de fábrica.  Para hacerlo, mantenga el dispositivo encendido e introduzca un objeto punzante en el hueco de Reset. Presione el botón durante más de 10 segundos.
Power On/Off	Apagar/Encender el router.
12V1A	Interfaz para conectar un adaptador de corriente.

### 1.2.- Requerimientos de Sistema

- Su PC ha de tener instalada una tarjeta Ethernet 10 baseT/100BaseT.
- Hay un Hub o Switch (conectado a través de uno de los interfaces Ethernet del router, con varios PCs conectados a su vez)
- Sistemas operativos: Windows Vista, Windows 7, Windows 98SE, Windows 2000, Windows ME o Windows XP
- Internet Explorer V5.0 o superior, Netscape V4.0 o superior, Firefox 1.5 o superior

#### 1.3.- Características

- Varios modos de línea.
- Acceso por marcado PPPoE externo.
- Acceso por marcado PPPoE y PPPoA interno.
- Modo Leased line
- Acceso 1483B, 1483R, y MER

#### **BHS-RTA**

### Manual de Usuario avanzado



Código BHS RTA MAN AV ESPAÑA

Ed 1.0

Página 5 de 62

- Múltiples PVCs (hasta 8) y estos PVCs pueden ser independientes de los demás.
- Un único PVC con múltiples sesiones.
- Múltiples PVCs con múltiples sesiones.
- Asociación de puertos con PVCs
- Protocolos 802.1Q y 802.1P
- Servidor DHCP
- NAT y NAPT
- Rutas estáticas
- Actualización de Firmware por Web, TFTP, FTP
- Reinicio a parámetros de fábrica
- DNS relay
- Virtual server
- DMZ
- 2 niveles de usuario y contraseña.
- Interfaz de usuario por Web
- Telnet CLI
- Visualización de estado de sistema
- Sesión PPP con PAP y CHAP
- Filtro IP
- IP QoS
- Samba
- Control de acceso remoto.
- Testeo de estado de conexión de línea.
- Gestión remota (telnet, HTTP, TR069)
- Backup y restauración de fichero de configuración.
- Interfaz Ethernet soporta detección "crossover", auto corrección y corrección de polaridad.
- UPnP
- 3G WAN y 3G de respaldo
- Samba para almacenamiento USB.

### 2.- Instalación Hardware

**Paso 1.** Conecte el puerto **ADSL** del dispositivo con el puerto **Modem** del splitter con un cable telefónico. Conecte el teléfono con el Puerto **Phone** del splitter con un cable telefónico. Conecte el puerto **Line** del splitter con el punto de conexión telefónica con un cable de teléfono.

El splitter tiene 3 puertos:

- Line: Para conectar con el punto de conexión telefónica de pared (RJ-11 jack).
- Modem: Para conectar al puerto DSL del modem.
- Phone: Para conectar a un teléfono.

Paso 2. Conecte un puerto **Eth** del modem con la tarjeta de red del PC a través de un cable Ethernet (MDI/MDIX).

#### Nota

Utilice pares trenzados para conectar el dispositivo a un Hub o Switch.

**Paso 3.** Conecte un extreme del adaptador de corriente al enchufe y el otro extreme al puerto **Power** del dispositivo.

**Conexión 1**: La Figura 3 muestra el diagrama de aplicación para la conexión del dispositivo, PC, splitter y teléfono, cuando no se conecta ningún teléfono antes del splitter.

Observa Telecom
Página 6 de 62

Código BHS\_RTA\_MAN\_AV\_ESPAÑA

Ed 1.0

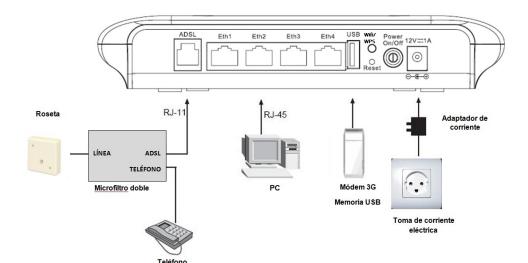


Figura 3. Diagrama de connexion (sin teléfono antes del splitter)

Conexión 2: La figura 4 muestra el diagram de aplicación para la conexión del dispositivo, PC, splitter y teléfono cuando se instala un teléfono antes del splitter.

Según se muestra en la siguiente figura, el splitter se instala cerca del dispositivo.

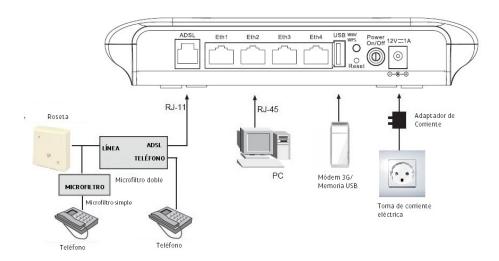


Figura 4. Diagrama de Conexión (con un teléfono antes del splitter)

#### Nota:

Cuando se utilice la conexión 2, el micro filtro debe ser instalado cerca del cable de teléfono. Ver Figura 4. No utilice el splitter para reemplazar el micro filtro.

Si se instala un teléfono directamente antes del splitter, puede causar un fallo de conexión entre el módem y la central, fallo de acceso a Internet o baja velocidad de conexión. Si realmente se necesita colocar un teléfono antes del splitter, debe añadirse un micro filtro antes del teléfono. No conecte varios teléfonos antes del splitter ni conecte varios teléfonos con el micro filtro.

Observa Telecom
Página 7 de 62

Código BHS\_RTA\_MAN\_AV\_ESPAÑA

Ed 1.0

### 3.- Configuración Web

#### 3.1.- Acceso al Dispositivo

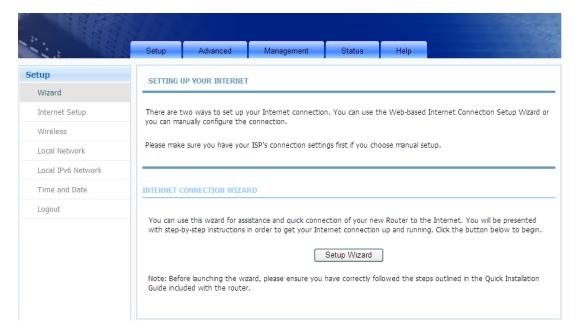
Este capítulo describe como configurar el dispositivo utilizando la utilidad de configuración Web.

La página de acceso a la Configuración avanzada del módem se muestra en la siguiente figura, para acceder al módem, teclee: <a href="http://192.168.1.1:8000">http://192.168.1.1:8000</a> en un navegador de internet, aparecerá la siguiente página en la que debe seleccionar el usuario **1234** e introduzca la password **1234**.



Copyright © OBSERVA Systems, Inc.

Si se ha accedido correctamente aparecerá la siguiente pantalla:



### 3.2.- Configuraciones

#### 3.2.1 Configuración de Internet



Código BHS\_RTA\_MAN\_AV\_ESPAÑA

Ed 1.0

Seleccione **Setup → Internet Setup.** Aparecerá la siguiente pantalla, en esta página, podrá configurar la interfaz WAN del equipo.



Presione en "Add" si quiere añadir una nueva Interfaz, aparecerá la siguiente pantalla:

INTERNET SETUP		
This screen allows you to configure an ATM P	VC identifier (VPI and VCI)	and select a service category.
ATM PVC CONFIGURATION		
VPI:	0	(0-255)
VCI:	35	(32-65535)
Service Category:	UBR With PCR	
Peak Cell Rate :	0	(cells/s)
Sustainable Cell Rate :	0	(cells/s)
Maximum Burst Size :	0	(cells)
CONNECTION TYPE		
Protocol :	Bridging	<b>~</b>
Encapsulation Mode :	LLC 💌	
802.1Q VLAN ID :	0	(0 = disable, 1 - 4094)
Priority :	0	(0 - 7)
Enable QinQ:		
	Enable Proxy Arp	
	Apply Cancel	]

La siguiente tabla describe los parámetros de la página:

	Descripción
C	Descripción
Campo	
•	



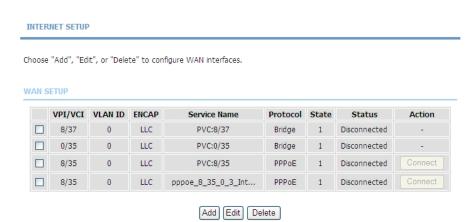
Código BHS\_RTA\_MAN\_AV\_ESPAÑA

Ed 1.0

Descripción Campo VPI: Camino virtual entre 2 puntos de la red ATM, sus valores válidos van de 0 a **PVC Settings** VCI: Camino virtual entre 2 puntos de la red ATM, su rango va de 32 a 65535 (Del 0 al 31 se reservan para gestión local del tráfico ATM). Se puede seleccionar una categoría de servicio de la siguiente lista: UBR With PCR UBR Without PCR Service Category UBR With PCR CBR Non Realtime VBR Realtime VBR Se puede seleccionar un protocolo de la siguiente lista: PPP over ATM (PPPoA) Protocol PPP over Ethernet (PPPoE) MAC Encapsulation Routing (MER) IP over ATM (IPoA) Bridging Seleccionar el método de encapsulación provisto por su ISP. Se puede **Encapsulation Mode** 

Presione en "Apply", aparecerá la pantalla de la siguiente figura.

seleccionar LLC o VCMUX.



#### 3.2.2 Configuración de la Interfaz Inalámbrica

Seleccione **Setup → Wireless.** Aparecerá la siguiente pantalla:





Código BHS\_RTA\_MAN\_AV\_ESPAÑA

Ed 1.0

#### 3.2.2.1 Configuración básica de la interfaz inalámbrica

En la página de Wireless, presione sobre **Wireless Basic,** se mostrará la siguiente página. En esta página puede configurar los parámetros de la interfaz inalámbrica para que los clientes inalámbricos puedan conectar al módem.



La siguiente tabla describe los parámetros en esta página:

Campo	Descripción	
Enable Wireless	Para apagar/encender la interfaz inalámbrica.	
Enable MultiAP Isolation	Activar/desactivar que las múltiples redes inalámbricas sean independientes.	
Wireless Network Name (SSID)	El nombre de la Red Inalámbrica es un nombre único que identificará la red. Todos los dispositivos de una red deben compartir el mismo nombre de red para poder comunicarse dentro de la red. Si decide cambiar el nombre de red de los parámetros por defecto, introduzca el nuevo nombre de la red inalámbrica en este campo.	
Visibility Status	Puede seleccionar <b>Visible</b> (para que la red sea visible) <b>o Invisible</b> (el nombre de la red no será visible aunque esté activa)	
Country	Seleccione el país de la lista.	
Control Sideband	Seleccione el modo de selección de canal, <b>Upper</b> o <b>Lower</b> .	
Wireless Channel	Seleccione el canal inalámbrico de la lista.	
802.11 Mode	Seleccione el modo 802.11 apropiado basado en los clients inalámbricos de su red. Tendrá como opciones: <b>802.11b</b> , <b>802.11g</b> , <b>802.11n</b> / <b>g</b> y <b>802.11b</b> / <b>g</b> /n.	



Código BHS\_RTA\_MAN\_AV\_ESPAÑA

Ed 1.0

Campo	Descripción
Band Width	Seleccione la banda apropiada: 20M, 40M o 20M/40M del menú.

Presione en "**Apply"** para guardar los cambios.



Código BHS\_RTA\_MAN\_AV\_ESPAÑA

Ed 1.0

#### 3.2.2.2 Seguridad Inalámbrica

Cuando el modo de seguridad está configurado como WEP, aparecerá la siguiente pantalla.

WIRELESS SECURITY	
Use this section to configure the wireless security settings for your router. Please note that changes made on this secti will also need to be duplicated to your wireless clients and PC.	ion
WIRELESS SECURITY MODE	
To protect your privacy you can configure wireless security features. This device supports three wireless security mode including: WEP, WPA and WPA2. WEP is the original wireless encryption standard. WPA and WPA2 provides a higher le of security.	
Security Mode : WEP	
WEP	
If you choose the WEP security option this device will <b>ONLY</b> operate in <b>Legacy Wireless mode (802.11B/G)</b> .	
WEP is the wireless encryption standard. To use it you must enter the same key(s) into the router and the wireless stations. For 64 bit keys you must enter 10 hex digits into each key box. For 128 bit keys you must enter 26 hex digit into each key box. A hex digit is either a number from 0 to 9 or a letter from A to F. For the most secure use of WEP the authentication type to "Shared Key" when WEP is enabled.	
You may also enter any text string into a WEP key box, in which case it will be converted into a hexadecimal key using ASCII values of the characters. A maximum of 5 text characters can be entered for 64 bit keys, and a maximum of 13 characters for 128 bit keys.	the

WEP Key Length: 64 bits(10 hex digits or 5 char)

Choose WEP Key: 1

WEP Key1: •••••

WEP Key2: 

WEP Key3: 

WEP Key4: 

Authentication: Open

Please take note of your SSID and security Key as you will need to duplicate the same settings to your wireless devices and PC.



La siguiente tabla describe los campos configurables de la página:

Campo	Descripción
WEP Key Length	Seleccionar la longitud de la clave WEP. Puede elegir entre <b>64-bit</b> o <b>128-bit</b> .
Choose WEP Key	Elegir el índice de la clave WEP. Puede elegir <b>Key 1</b> , <b>2</b> , <b>3</b> o <b>4</b> .
WEP Key 1/2/3/4	Las claves de encriptación se utilizan para encriptar los datos. Tanto el módem como los clientes inalámbricos han de utilizar la misma clave de encriptación para la transmisión de datos.

Presione **Apply** para guardar los cambios de configuración.



Código BHS\_RTA\_MAN\_AV\_ESPAÑA

Ed 1.0

Cuando el modo seguridad está configurado como **Auto (WPA or WPA2)**, **WPA2 only** o **WPA only**, aparecerá la siguiente pantalla:

Use this section to configure the wirele will also need to be duplicated to your	ess security settings for your router. Please note that changes made on this section wireless clients and PC.
VIRELESS SECURITY MODE	
	gure wireless security features. This device supports three wireless security modes P is the original wireless encryption standard. WPA and WPA2 provides a higher leve
Security Mode	: Auto(WPA or WPA2)
WPA Encryption	: TKIP+AES V
VPA	
clients while maintaining higher securit	ty with stations that are WPA2 capable. Also the strongest cipher that the client
clients while maintaining higher securit supports will be used. For best securit	ry with stations that are WPA2 capable. Also the strongest cipher that the client ry, use <b>WPA2 Only</b> mode. This mode uses AES(CCMP) cipher and legacy stations ar r. For maximum compatibility, use <b>WPA Only</b> . This mode uses TKIP cipher. Some
clients while maintaining higher securit supports will be used. For best securit not allowed access with WPA security gaming and legacy devices work only i	ry, use WPA2 Only mode. This mode uses AES(CCMP) cipher and legacy stations ar r. For maximum compatibility, use WPA Only. This mode uses TKIP cipher. Some
clients while maintaining higher securit supports will be used. For best security not allowed access with WPA security gaming and legacy devices work only in To achieve better wireless performance	by with stations that are WPA2 capable. Also the strongest cipher that the client by, use <b>WPA2 Only</b> mode. This mode uses AES(CCMP) cipher and legacy stations are. For maximum compatibility, use <b>WPA Only</b> . This mode uses TKIP cipher. Some in this mode.
clients while maintaining higher securit supports will be used. For best security not allowed access with WPA security gaming and legacy devices work only in To achieve better wireless performance WPA-PSK does not require an authen	by with stations that are WPA2 capable. Also the strongest cipher that the client strongest cipher and legacy stations are f. For maximum compatibility, use <b>WPA Only</b> . This mode uses TKIP cipher. Some in this mode. The cipher is the cipher of the ci
clients while maintaining higher securit supports will be used. For best security not allowed access with WPA security gaming and legacy devices work only in To achieve better wireless performance WPA-PSK does not require an authen	ty with stations that are WPA2 capable. Also the strongest cipher that the client strongest cipher that the client strongest cipher and legacy stations are. For maximum compatibility, use WPA Only. This mode uses TKIP cipher. Some in this mode.  The cuse WPA2 Only security mode (or in other words AES cipher).  The tication server. The WPA option requires an external RADIUS server.
clients while maintaining higher securit supports will be used. For best security not allowed access with WPA security gaming and legacy devices work only in the control of the control o	ty with stations that are WPA2 capable. Also the strongest cipher that the client strongest cipher that the client strongest cipher and legacy stations are. For maximum compatibility, use WPA Only. This mode uses TKIP cipher. Some in this mode.  The cuse WPA2 Only security mode (or in other words AES cipher).  The tication server. The WPA option requires an external RADIUS server.
clients while maintaining higher securit supports will be used. For best security not allowed access with WPA security gaming and legacy devices work only in the control of the control o	ty with stations that are WPA2 capable. Also the strongest cipher that the client strongest cipher that the client strongest cipher and legacy stations are. For maximum compatibility, use WPA Only. This mode uses TKIP cipher. Some in this mode.  The cuse WPA2 Only security mode (or in other words AES cipher).  The tication server. The WPA option requires an external RADIUS server.
clients while maintaining higher securit supports will be used. For best security not allowed access with WPA security gaming and legacy devices work only in the control of the control o	ty with stations that are WPA2 capable. Also the strongest cipher that the client by, use WPA2 Only mode. This mode uses AES(CCMP) cipher and legacy stations are. For maximum compatibility, use WPA Only. This mode uses TKIP cipher. Some in this mode.  The transport of the company security mode (or in other words AES cipher).  The transport of the transport of the company of the company of the client of th
clients while maintaining higher securit supports will be used. For best security not allowed access with WPA security gaming and legacy devices work only in the control of the control o	ty with stations that are WPA2 capable. Also the strongest cipher that the client by, use WPA2 Only mode. This mode uses AES(CCMP) cipher and legacy stations are. For maximum compatibility, use WPA Only. This mode uses TKIP cipher. Some in this mode.  The transport of the company security mode (or in other words AES cipher).  The transport of the transport of the company of the company of the client of th

La siguiente tabla describe los parámetros en esta página:

Field	Description
Security Mode	Configurar el modo de encriptación inalámbrica, puede elegir: None, WEP, Auto(WPA or WPA2), WPA 2 Only o WPA Only.
WPA Encryption	Cuando WPA o WPA2 están seleccionadas, puede seleccionar que la encriptación WPA sea <b>AES</b> o <b>TKIP+AES</b> .
	PSK (Pre-Shared Key), introduzca la clave precompartida en el campo Pre-Shared Key.
WPA Mode	<b>Enterprise (RADIUS)</b> , introduzca puerto, dirección IP y contraseña del servidor Radius. Necesita introducer el usuario y contraseña que provee el servidor Radius cuando los clients conecten al módem.
Group Key Update Interval	Cuando se aplica encriptación WPA, los mensajes enviados están encriptados con una contraseña. Para mayor seguridad, la contraseña WPA se actualiza periódicamente, este valor es el interval de actualización de la contraseña WPA.



Código BHS\_RTA\_MAN\_AV\_ESPAÑA

Ed 1.0

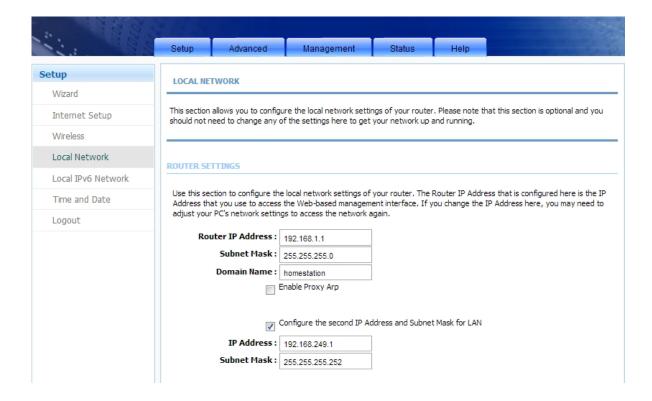
Página 14 de 62

#### 3.2.3 Red Local

La IP de LAN está pre configurada con 192.168.1.1, podrá utilizar la configuración de fábrica y el servicio DHCP para gestionar la configuración IP para la red privada. La dirección del dispositivo es la dirección base utilizada para DHCP. Para utilizar el dispositivo para DHCP en su LAN, el pool de direcciones utilizado para DHCP debe ser compatible con la dirección IP del módem. Las direcciones IP disponibles en el pool de DHCP cambiarán si se cambia la dirección IP del módem.

También podrá habilitar una dirección de LAN secundaria. Las 2 direcciones de LAN deben estar en redes distintas.

Vaya al menú **Setup > Local Network.** Aparecerá la siguiente pantalla:



Por defecto, **Enable DHCP Server** está seleccionado en la interfaz LAN del módem. El servicio DHCP provee configuración IP a los equipos configurados para obtener automáticamente una dirección IP que se conectan al módem a través de la interfaz Ethernet. Cuando el módem se utiliza para DHCP, se convierte en la ruta por defecto para los clientes conectados a él. Si se cambia la dirección del módem, se debe cambiar también el rango de direcciones IP en el pool utilizado para DHCP en la LAN. El pool de direcciones IP puede tener hasta 253 direcciones.



Código BHS\_RTA\_MAN\_AV\_ESPAÑA

Ed 1.0

Página 15 de 62

	Enable DHCP Relay	
Relay IP Address:		
Use this section to configure th	e built-in DHCP Server to a	ssign IP addresses to the computers on your network.
<b>V</b>	Enable DHCP Server	
DHCP IP Address Range :	192.168.1.33	to 192.168.1.254
DHCP IP Mask:	255.255.255.0	
DHCP Router IP:	192.168.1.1	
DHCP Lease Time :	43200	(seconds)
Use the following DNS server a	ddresses:	
<b>✓</b>	Enable static DNS	
Preferred DNS server:	80.58.61.250	
Alternate DNS server:	80.58.61.254	
<b>V</b>	Enable DNS Relay	
Use this section to configure th	e DHCP Server in lan port i	ndividual:
<b>V</b>	LAN Port1	
<b>✓</b>	LAN Port2	
₹	LAN Port3	
<b>✓</b>	LAN Port4	
<b>▼</b>	WLAN Port1	
<b>V</b>	WLAN Port2	
<b>▼</b>	WLAN Port3	
<b>V</b>	WLAN Port4	
DHOD OTTENT OF ACCUSE	A	oply Cancel

Presione **Apply** para guardar los cambios.

La sección **DHCP Client Class List** que se muestra en la siguiente figura:

### DHCP CLIENT CLASS LIST

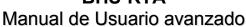


Si se pulsa en Add, aparecerá el siguiente menú:

# ADD DHCP CLIENT CLASS(OPTIONAL) Client Class Name: Min IP Address: DNS Address:



### **BHS-RTA**





Código BHS RTA MAN AV ESPAÑA

Ed 1.0

En la página de Local Network, podrá asignar direcciones IP de la LAN a PCs específicos basándose en su dirección MAC.

#### **DHCP RESERVATIONS LIST** Status Computer Name MAC Address **IP Address** Edit Delete

Presione en Add para añadir DHCP estático (opcional). Aparecerá la siguiente página:

### ADD DHCP RESERVATION (OPTIONAL) Enable: Computer Name: IP Address: MAC Address: Cancel Apply

Seleccione Enable para reservar las direcciones IP a los PCs con las MACs configuradas. El campo Computer Name ayudará a reconocer el PC por su dirección MAC, por ejemplo. "Laptop de papá". Presione en "Apply" para guardar los cambios.

Después de que se guarda la configuración de reserva de DHCP, se mostrará en la lista de DHCP reservations.

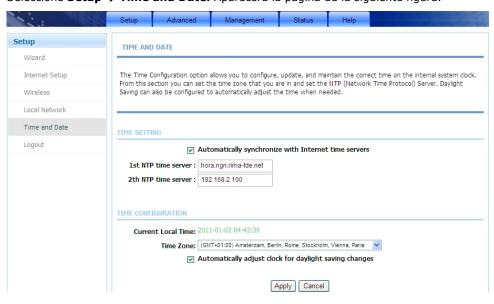
La página de NUMBER OF DYNAMIC DHCP CLIENTS muestra los clientes DHCP actuales (PCs o Laptop) conectados al dispositivo y la información detallada del computador conectado.

#### NUMBER OF DYNAMIC DHCP CLIENTS: 0

Computer Name	MAC Address	IP Address	Expire Time

#### 3.2.4 Fecha y hora

Seleccione **Setup > Time and Date.** Aparecerá la página de la siguiente figura.





Código BHS RTA MAN AV ESPAÑA

Ed 1.0

Página 17 de 62

En la página de **Time and Date**, se puede configurar, actualizar y mantener la hora correcta de reloj interno de sistema. Puede seleccionar la zona horaria donde se encuentre y el servidor de Protocolo de tiempo de red (NTP). También puede configurar "Daylight saving" para ajustar la hora cuando sea necesario.

Seleccione Automatically synchronize with Internet time servers.

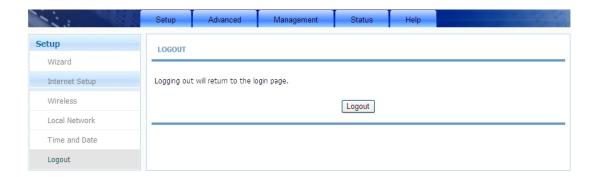
Seleccione el servidor de tiempo específico y la zona horaria de la lista.

Seleccione **Automatically adjust clock for daylight saving changes** si es necesario. Configure el daylight según quiera.

Presione en Apply para guardar los cambios.

#### 3.2.5 Salida

Seleccione Setup →Logout. Aparecerá la siguiente página donde puede salir de la página de configuración.



#### 3.3.- Configuración Avanzada

Esta sección incluye características avanzadas para la gestión de red, seguridad y herramientas administrativas para gestionar el dispositivo. Puede ver el estado y otra información utilizada para revisar las funcionalidades y realizar gestión de problemas.

En el interfaz principal, presione sobre la pestaña de **Advanced** para acceder al menú avanzado. Los sub menús son: **Advanced Wireless**, **Port Fowarding**, **DMZ**, **SAMBA**, **3G Configuration**, **Parental Control**, **Filtering Options**, **QoS Configuration**, **Firewall Settings**, **DNS**, **Dynamic DNS**, **Network Tools**, **Routing**, **Schedules**, **DLNA** y **Logout**.



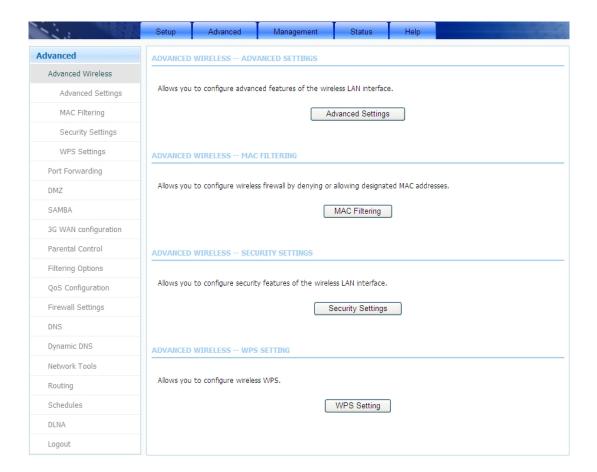
Código BHS\_RTA\_MAN\_AV\_ESPAÑA

Ed 1.0

#### 3.3.1 Advanced Wireless

Esta función se utilice para modificar el estándar 802.11g de las configuraciones de radio inalámbrica. Se sugiere que no se modifiquen los parámetros por defecto ya que una configuración incorrecta puede reducir las funcionalidades inalámbricas. Los parámetros por defecto proveen el mejor desarrollo inalámbrico en la mayoría de los entornos.

Seleccione **Advanced Advanced Wireless.** Aparecerá la siguiente página:





Código BHS\_RTA\_MAN\_AV\_ESPAÑA

Ed 1.0

### 3.3.1.1 <u>Configuraciones Avanzadas</u>

Seleccione **Advance Settings.** Aparecerá la siguiente página:

ADVANCED SETTINGS		
	the factory defaults. I	eir 802.11g wireless radio from the standard setting. It is not incorrect settings may affect your wireless performance. The ost environments.
ADVANCED WIRELESS SETTINGS		
Transmission Rate :	Auto	
Multicast Rate :		
Transmit Power :	100%	
Beacon Period :	100	(20 ~ 1000)
RTS Threshold :	2346	(256 ~ 2346)
Fragmentation Threshold :	2345	(256 ~ 2346)
DTIM Interval:	1	(1 ~ 255)
Preamble Type :	long 🔻	
SSID		
Enable Wireless :	√	
Wireless Network Name (SSID) :	MOVISTAR_67CA	
	Visible T	, nvisible
User Isolation :		
WMM Advertise :	On 🔻	
Max Clients :	16	(1 ~ 32)
GUEST/VIRTUAL ACCESS POINT-1 Enable Wireless Guest Network :		1
Guest SSID :		
	○ Visible ○ Ir	nvisible
User Isolation : WMM Advertise :		
Max Clients :		(1 ~ 32)
GUEST/VIRTUAL ACCESS POINT-2	10	(1 ~ 32)
Enable Wireless Guest Network :		
Guest SSID :	WLAN_Obdd	
	Visible T	nvisible
User Isolation :		
WMM Advertise :	On 🔻	
Max Clients :	16	(1 ~ 32)
GUEST/VIRTUAL ACCESS POINT-3		
Enable Wireless Guest Network :		
Guest SSID :	WLAN_Obde	
	Visible D In	nvisible
User Isolation :		
WMM Advertise ;		
Max Clients :	16	(1 ~ 32)
	(Apply) (C	ancel



Código BHS\_RTA\_MAN\_AV\_ESPAÑA

Ed 1.0

### 3.3.1.2 Filtrado por MAC

MAC ADDRESS
The MAC Address Access Control mode, if enabled, permits access to this route from host with MAC addresses contained in the Access Control List.
Enter the MAC address of the management station permitted to access this route, and click "Apply".
ACCESS CONTROL MAC ADDRESSES
Enable Access Control Mode
MAC Address
Add Delete
Seleccione <b>Enable Access Control Mode,</b> y presione <b>Add</b> para añadir una dirección MAC como se muestra en la siguiente figura:
MAC ADDRESS
MAC Address :
Apply Cancel

Presione **Apply** para terminar.

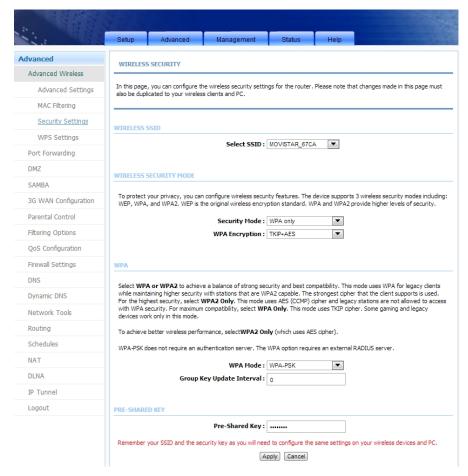


Código BHS\_RTA\_MAN\_AV\_ESPAÑA

Ed 1.0

#### 3.3.1.3 Configuraciones de Seguridad

Seleccione Security Settings, aparecerá la siguiente pantalla:



Seleccione el SSID que quiere configurar de la lista. Seleccione el método de encriptación de la lista de posibilidades en **Security Mode.** Puede seleccionar **None, WEP, AUTO (WPA o WPA2), WPA Only o WPA2 Only.** 

Si selecciona WEP, aparecerá lo siguiente:

EP	
If you choose the W	EP security option this device will <b>ONLY</b> operate in <b>Legacy Wireless mode (802.11B/G)</b> .
stations. For 64 bit k into each key box. A	encryption standard. To use it you must enter the same key(s) into the router and the wireless eys you must enter 10 hex digits into each key box. For 128 bit keys you must enter 26 hex digits hex digit is either a number from 0 to 9 or a letter from A to F. For the most secure use of WEP set ope to "Shared Key" when WEP is enabled.
	iny text string into a WEP key box, in which case it will be converted into a hexadecimal key using th haracters. A maximum of 5 text characters can be entered for 64 bit keys, and a maximum of 13 t keys.
W	EP Key Length: 64 bits(10 hex digits or 5 char)
Ch	oose WEP Key: 1 💌
	WEP Key1: •••••
	WEP Key2:
	WEP Key3:
	WEP Key4:
	Authentication : Open
Please take note of y PC.	rour SSID and security Key as you will need to duplicate the same settings to your wireless devices at



Código BHS\_RTA\_MAN\_AV\_ESPAÑA

Ed 1.0

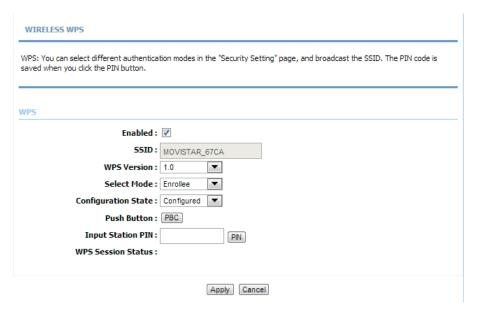
Si selecciona AUTO (WPA o WPA2, WPA Only o WPA2 Only) aparecerá la siguiente pantalla:

WPA	
clients suppo not all	(PA or WPA2 mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client rts will be used. For best security, use WPA2 Only mode. This mode uses AES(CCMP) cipher and legacy stations are owed access with WPA security. For maximum compatibility, use WPA Only. This mode uses TKIP cipher. Some g and legacy devices work only in this mode.
To act	nieve better wireless performance use <b>WPA2 Only</b> security mode (or in other words AES cipher).
WPA-F	PSK does not require an authentication server. The WPA option requires an external RADIUS server.
	WPA Mode: Auto(WPA or WPA2)-PSK
	Group Key Update Interval: 100
RE-SH	IARED KEY
	Pre-Shared Key :
Please PC.	take note of your SSID and security Key as you will need to duplicate the same settings to your wireless devices an
	Apply Cancel

Presione **Apply** para guardar los cambios. Para información detallada, vea el punto 3.2.3.2 Wireless Security de esta quía.

#### 3.3.1.4 Configuración WPS

Seleccione **WPS Settings.** Esta página se utiliza para configurar las opciones de WPS.



La siguiente tabla describe los parámetros de esta página:

Campo	Descripción		
Enabled	Habilita la función WPS.		
Select SSID	Selecciona uno de los SSIDs habilitados de la BHS		
Select Mode	Para seleccionar el modo <b>Registrar</b> o <b>Enrollee</b> . Cuando un AP utilice el modo Registrar, el otro extreme debe usar el modo Enrollee.		
Configuration State	Cuando se selecciona el estado <b>Configured,</b> los parámetros inalámbricos (por ejemplo, encriptación y contraseña) son proporcionados por el CPE en la negociación WPS.		



Código BHS RTA MAN AV ESPAÑA

Ed 1.0

Campo	Descripción		
Cuando se selecciona el estado <b>Unconfigured,</b> los parámetros proporcionados por el otro extremo (por ejemplo, el PC)			
Push Button	Para presionar el botón de WPS de forma software, el CPE conectará con la estación automáticamente.		
Input Station PIN	Tendrá que introducir el PIN que generó la estación en modo Enrollee. Tras esto, presione el botón para conectar con el otro extremo con el PIN.		

Cuando se selecciona el modo Registrar, aparecerá la siguiente pantalla, solo podrá usarse el botón PIN.

Enabled :	. ✓
SSID:	MOVISTAR_67CA
WPS Version :	1.0 ▼
Select Mode :	Registrar 🔻
Configuration State:	Configured 🔻
Generate PIN :	12345670 New PIN
Pin Station :	PIN
WPS Session Status :	
	Apply Cancel

La siguiente tabla describe los parámetros de esta página:

Campo	Descripción
Generate PIN	Presione el botón para generar un PIN que se utilizará por el módem y la estación que conecte.
PIN Station	Presione el botón para conectar con la estación utilizando el PIN.
WPS Session Status	Muestra el estado de la sesión.

#### 3.3.2 Apertura de Puertos

Esta función se utiliza para abrir puertos en la BHS y redirigir los datos a través de estos puertos a un PC en su red ( tráfico WAN to LAN). Permite a los usuarios remotos acceder a servicios en su LAN, como un FTP para transferencia de ficheros o SMTP y POP3 para e-mail. El dispositivo acepta peticiones remotas para estos servicios en su IP pública. Se utiliza el protocolo TCP o UDP especificados y el número de puerto y se redirigen estas peticiones al servidor en la LAN con la dirección IP que se especifique. Nota: La dirección IP privada debe estar dentro del rango disponible de la subred dónde el dispositivo esté conectado.

Seleccione **Advanced** → **Port Forwarding.** Aparecerá la siguiente pantalla:



Código BHS\_RTA\_MAN\_AV\_ESPAÑA

Ed 1.0

Página 24 de 62



Presione en Add para añadir un Servidor Virtual.

Remaining number of entries that can be configured: 80							
Remaining number of	entries that can be co	ontigurea:	80				
V	VAN Connection(s):	PVC:8/35	~				
	Server Name :						
	Select a Service :	(Click to Sel	lect)	~			
	Ocustom Server:						
	Schedule :		View Available Schedu	les			
	ddress(Host Name):	-					
External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Remote Ip		
		TCP 💌					
		TCP 💌					
		TCP 💌					
		TCP 💌					
		TCP 💌					
		TCP 💌					
		TCP V					
		TCP V					
		TCP V					
		TCP Y					
		TCP 💌					
		TCP 💌					
		Apply	Cancel				

Seleccione un servicio de una aplicación pre configurada o introduzca el nombre en el campo **Custom Server**.

Introduzca la dirección IP en el campo **Server IP Address** para apuntar al correspondiente PC para recibir los paquetes enviados.

Los campos **Ports** muestran los puertos que se quieran abrir en el módem. En el campo **TCP/UDP** se seleccionará el protocolo de los puertos abiertos.

Presione **Apply** para guardar los cambios. Aparecerá la siguiente página cuando se haya añadido un servidor Virtual.



Código BHS RTA MAN AV ESPAÑA

Ed 1.0

\_\_\_\_\_J

#### PORT FORWARDING

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

Select the service name, and enter the server IP address and click "Apply" to forward IP packets for this service to the specified server. Note: Modifying the **Internal Port Start** or **Internal Port End** is not recommended. If the **External Port Start** or the **External Port End** changes, the **Internal Port Start** or **Internal Port End** automatically changes accordingly.

#### PORT FORWARDING SETUP

Server Name	Wan Connection	External Port Start/End	Protocol	Internal Port Start/End	Server IP Address	Schedule Rule	Remote IP
Active W	PVC:8/35	3000/3000	tcp	3000/3000	192.168.1.2	Always	
Active W	PVC:8/35	5670/5670	tcp	5670/5670	192.168.1.2	Always	
Active W	PVC:8/35	7777/7777	tcp	7777/7777	192.168.1.2	Always	
Active W	PVC:8/35	7000/7000	tcp	7000/7000	192.168.1.2	Always	

#### 3.3.3 DMZ

Ya que algunas aplicaciones no son compatibles con NAT, el dispositivo soporta también el uso de dirección IP DMZ para un único host en la LAN. Esta dirección IP no se protege por NAT y es visible para agentes en Internet que tengan el software adecuado. Tenga en cuenta que un PC cliente en DMZ está expuesto a varios tipos de riesgos de seguridad. Si utiliza DMZ, tome medidas (como anti virus en el PC) para proteger a los demás PCs en su LAN de posibles virus a través del DMZ.

Seleccione **Advanced > DMZ.** Se mostrará la siguiente página:



Presione **Apply** para guardar los cambios.

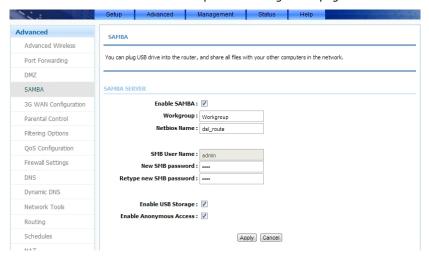


Código BHS\_RTA\_MAN\_AV\_ESPAÑA

Ed 1.0

### 3.3.4 SAMBA (Servidor de Ficheros)

Seleccione Advanced -> SAMBA. Aparecerá la siguiente página:



La siguiente tabla describe los parámetros de esta página:

Campo Descripción				
Enable SAMBA	Marque la opción para habilitar el servicio de SAMBA.			
Workgroup	Introduzca el nombre de su red local (LAN)			
Netbios Name	Introduzca el nombre netbios que se utilize en servicio netbios funcionando en un computador.			
New SMB password Introduzca la contraseña de SAMBA para el usuario root.				
Retype new SMB password	Reconfirme la contraseña de SAMBA en este campo.			
Enable USB Storage	Marque esta opción para soportar almacenamiento USB.			
Enable Anonymous Access	Seleccione esta opción para permitir el acceso a usuarios anónimos.			

### 3.3.5 Configuración de conexión 3G

Seleccione Advanced > 3G WAN Configuration. Aparecerá la página:



Si se quiere acceder a Internet utilizando la conexión 3G, se requiere tener un módem 3G conectado a la interfaz USB del router, en este caso aparecerá lo siguiente:



Código BHS\_RTA\_MAN\_AV\_ESPAÑA

Ed 1.0

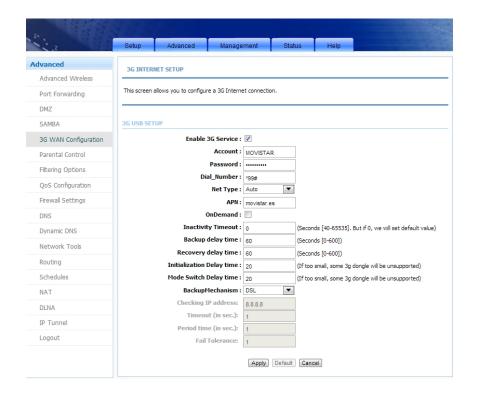
Choose "Add", "Edit", or "Delete" to configure 3G WAN interfaces.

3G Status: Ready
Inform: CONNECTTED

Service Name Protocol State Status Default Gateway Action

Add Edit Delete Pin Manage DongleInfo

Presione en **Add** para configurar los parámetros de la conexión a Internet por 3G:



La siguiente tabla describe los parámetros de esta página:

Campo	Descripción
Enable 3G Service	Para habilitar o deshabilitar la conexión 3G.
Account	Nombre de cuenta
Password	Nombre de contraseña
Dial_Number	Número a marcar
APN Punto de acceso	
OnDemand	Si decide seleccionar la conexión en modo "On Demand"
Inactivity Timeout	Configurar el periodo de tiempo sin flujo de datos antes de desconectar el 3G. Cuando se selecciona 0, la conexión 3G estará siempre establecida.
Backup delay time	Tiempo de espera antes de iniciar la conexión 3G tras la desconexión ADSL.
Initialization Delay time	Configurar el tiempo de inicio del módem 3G USB.
Mode Switch Delay time	Configurar el tiene de un módem 3G para conmutar de un dispositivo de almacenamiento a un dispositivo de comunicaciones.



Código BHS\_RTA\_MAN\_AV\_ESPAÑA

Ed 1.0

Campo	Descripción	
	Cuando se selecciona DSL, la llamada de 3G se iniciará tras la desconexión del ADSL, usualmente se utiliza esta opción.	
Backup Mechanism	Cuando se selecciona el mecanismo IPCHECK, la llamada 3G se iniciará cuando la conexión DSL esté establecida y no pueda hacerse un ping a la dirección IP configurada en "Checking IP address".	
Checking IP address  Es una dirección para la detección de 3G. Tras levantar la línea A puede hacerse ping a esta dirección, se iniciará la llamada 3G.		
Timeout (in sec.)	Configurar el timeout para ping.	
Period time (in sec.)	Configurar el intervalo entre 2 tiempos de ping.	
Fail Tolerance	Configurar los tiempos permitidos para fallo de ping.	

Puede presionar en **DongleInfo** para ver la información de la tarjeta 3G, como se muestra en la siguiente pantalla:

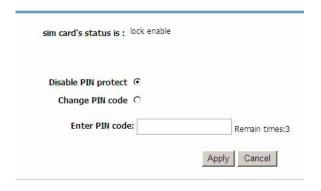


Presione en **Pin Manage** para habilitar el código PIN de la tarjeta 3G como se muestra en la siguiente pantalla:



Introduzca el código PIN en el campo Enter PIN code y presione en Apply para terminar.

Puede deshabilitar el código PIN del módem 3G como se muestra en la siguiente figura:



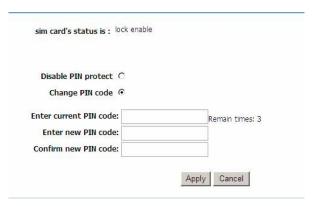
Observa Telecom Página 29 de 62

Código BHS\_RTA\_MAN\_AV\_ESPAÑA

Ed 1.0

Seleccione **Disable PIN protect**, y presione en **Apply** para terminar.

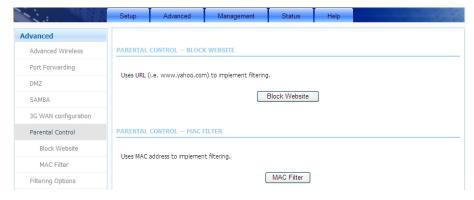
Puede cambiar el código PIN según se muestra en la siguiente pantalla:



Introduzca el código PIN Actual y el nuevo PIN y presione Apply para terminar.

### 3.3.6 Control parental

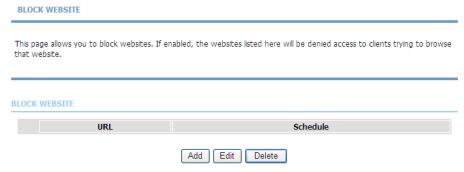
Seleccione **Advanced > Parental Control.** Se mostrará la siguiente pantalla:



Esta página le proporcionará herramientas útiles para restringir el acceso a Internet. **Block Websites** le permitirá crear rápidamente una lista de todos los sitios web que quiera deshabilitar para el acceso de usuarios. **Block MAC Address** le permitirá controlar cuando los PCs clientes de un dispositivo tengan permitido el acceso a Internet.

#### 3.3.6.1 Bloquear páginas web

En la página web de Control Parental, presionamos sobre Block Website. Se mostrará la siguiente página:



Presione **Add.** La página mostrará la página de la siguiente figura:



Código BHS\_RTA\_MAN\_AV\_ESPAÑA

Ed 1.0

Página 30 de 62

URL:	http://
Schedule :	always 🔻 View Available Schedules
O Manual Schedule :	
Day(s):	○ All Week ® Select Day(s)
	Sun ☐ Mon ☐ Tue ☐ Wed
	☐ Thu ☐ Fri ☐ Sat
All Day - 24 hrs:	
Start Time :	: (hour:minute, 24 hour time)
End Time:	: (hour:minute, 24 hour time)

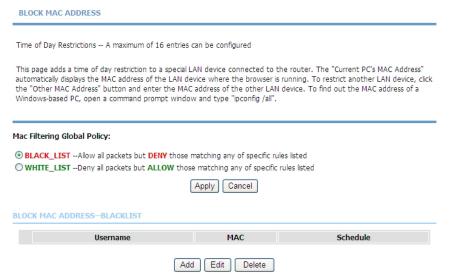
Introduzca la página web en el campo **URL.** Seleccione la programación (**Schedule**) de la lista asociada o seleccione Programación manual (**Manual Schedule**) y seleccione las correspondientes horas y días.

Presione Apply para añadir la página web a la tabla de BLOCK WEBSITE. Se mostrará la siguiente página.

at website.		
OCK WEBSITE		
	URL	Schedule
	www.xxx	Always

#### 3.3.6.2 Bloqueo por MAC

Presione **Block MAC Address**, aparecerá la siguiente pantalla:

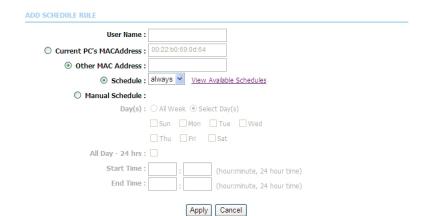


Seleccione BLACK\_LIST (direcciones no permitidas) o WHITE LIST (direcciones permitidas)

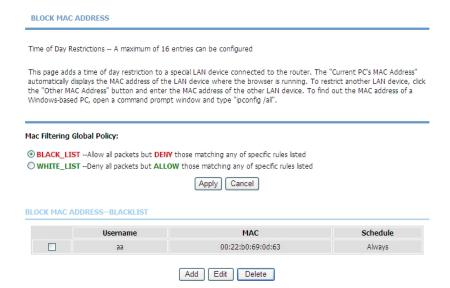


Código BHS\_RTA\_MAN\_AV\_ESPAÑA

Ed 1.0



Introduzca el nombre de usuario y la dirección MAC así como sus correspondientes horas y días. Presione en **Apply** para añadir la dirección MAC a la tabla **BLOCK MAC Address**. Aparecerá la siguiente pantalla:



#### 3.3.7 Opciones de Filtrado

Seleccione **Advanced**  $\rightarrow$  **Filtering Options.** Se mostrará la siguiente página:





Código BHS RTA MAN AV ESPAÑA

Ed 1.0

Página 32 de 62

### 3.3.7.1 Filtrado IPv4

En el menú de **Filtering Options**, pulse sobre **IPv4 Filtering**. Aparecerá la siguiente pantalla donde puede configurar la función de firewall IPv4.

#### **IPV4 FILTER**

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

#### **FIREWALL** Name Interface In/Out Default action **Bytes** Pkts Local/Forward Add Filter Edit Filter Delete Filter RULE IP Protocol OrigIP/ DestIP/ Enabled DestPort Bytes Pkts Action RejectType IcmpType OrigPort Mask Mask Type Add Rule Edit Rule Delete Rule

Presione en Add Filter. Se mostrará la siguiente página:

#### FILTER INFO



Introduzca el Nombre de Filtro en **Filter Name** y especifique al menos uno de los siguientes criterios: Interfaz, In/Out, Default Action (Permitir o denegar) y Local/Forward.

Presione en **Apply** para salvar los cambios.

Nota: Los cambios son aplicables únicamente cuando el Firewall está habilitado.

Presione sobre Add Rule. Se mostrará la siguiente página:



Código BHS\_RTA\_MAN\_AV\_ESPAÑA

Ed 1.0



Apply Cancel

La siguiente tabla describe los parámetros de esta página:

Campo	Descripción
Enable	Marcar para habilitar el Firewall.
Protocol	Elegir protocol para la regla. TCP, UDP o ICMP.
Action	Acción cuando se cumpla la regla. <b>Permit</b> significa permitir pasar los paquetes, <b>Drop</b> significa descartar el mensaje sin respuesta y <b>Reject</b> descartar el mensaje con respuesta
Reject Type	Tipo de mensaje enviado en una acción de Reject.
Icmp Type	Tipo de mensajes ICMP
origIPAddress	Dirección IP origen
origMask	Máscara de dirección IP origen
origStart/End Port	Puerto inicio/final de origen: Rango de puertos de la IP origen.
destIPAddress	Dirección destino
destMask	Máscara de la dirección destino
dest Start/End Port	Puerto inicio/final de destino: Rango de puertos de la IP destino.

Tras configurar los parámetros, presione en **Apply**, se mostrará la siguiente página:



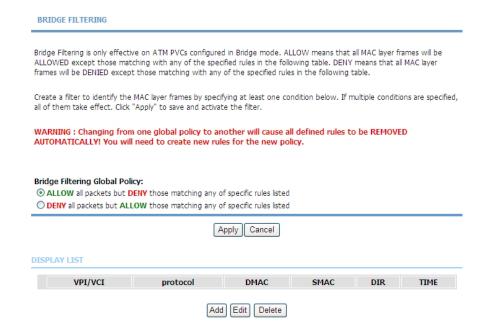
Observa Telecom Página 34 de 62

Código BHS RTA MAN AV ESPAÑA

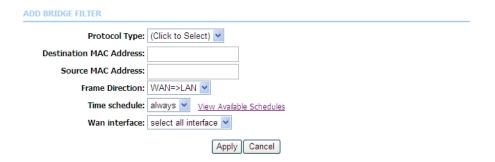
Ed 1.0

### 3.3.7.2 Filtrado Bridge

En el menú de **Filtering Options** presione sobre **Bridge Filtering**. Aparecerá la siguiente pantalla, dónde se configura y se ven parámetros bridge y sus puertos asociados.



Presione sobre **Add** para añadir un filtro bridge. Aparecerá la siguiente pantalla.



La siguiente tabla describe los parámetros de esta página:

Campo	Descripción
Protocol Type	Elegir un protocol de nivel 3 para filtrado bridge de la lista desplegable. Podrá elegir: <b>PPPoE</b> , <b>IPv4</b> , <b>IPv6</b> , <b>AppleTalk</b> , <b>IPX</b> , <b>NetBEUI</b> o <b>IGMP</b> .
Destination MAC Address	Dirección MAC de destino del mensaje.
Source MAC Address	Dirección MAC del origen del mensaje.
Frame Direction	Elegir la dirección de envoi: de WAN a LAN o de LAN a WAN.
Time schedule	Elegir la estrategia de filtrado always (siempre) o never (nunca).
Wan interface	Elegir un interfaz efectivo para aplicar la regla de filtrado.

Presione **Apply** para guardar los cambios.

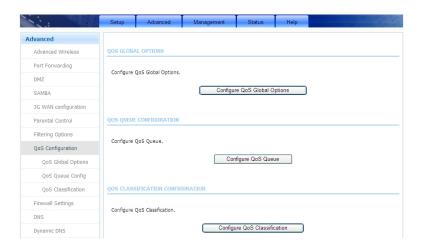


Código BHS RTA MAN AV ESPAÑA

Ed 1.0

### 3.3.8 Configuración QoS

Elija **Advanced > QoS Configuration.** Aparecerá la página de configuración de QoS.



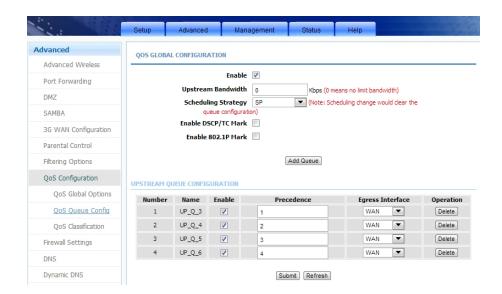
### 3.3.8.1 Opciones Globales de QoS

En el menú **QoS Configuration,** presione sobre **QoS Global Options.** Aparecerá la siguiente pantalla, podrá seleccionar "Enable Queuing Operation" y presione **Submit** para habilitar la operación de encolamiento.



#### 3.3.8.2 Configuración de Colas de QoS

En el menú de **QoS Configuration**, presione sobre **QoS Queue Config.** Aparecerá la siguiente pantalla, donde podrá configurar Control de flujo QoS (QoS flow control)



Observa Telecom Página 36 de 62

Código BHS\_RTA\_MAN\_AV\_ESPAÑA

Ed 1.0

La siguiente tabla describe los parámetros de esta página:

Campo Descripción				
Direction	Encolamiento <b>Upstream</b> (subida) o encolamiento en <b>Downstream</b> (bajada).			
Enable	Selecciónelo para habilitar el encolado.			
Upstream Bandwidth	Bandwidth total para el flujo de subida			
Scheduling Strategy	Algoritmo de programación de las colas de QoS.			
Enable DSCP/TC Mark	Selecciónelo para permitir el marcado DSCP/TC.			
Enable 802.1P Mark	Selecciónelo para permitir el marcado 802.1P.			

Tras configurar los distintos parámetros, presione en Add Queue para añadir una cola.

En la siguiente página, cuando se selecciona **Upstream** (subida o LAN→WAN), tendría que configurar los parámetros de la siguiente figura:

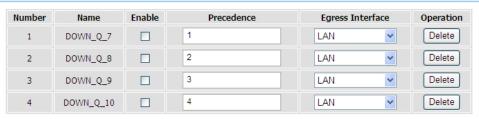
#### **UPSTREAM QUEUE CONFIGURATION**

Number	Name	Enable	Precedence	Egress Interface	Operation
1	UP_Q_3	✓	1	WAN	Delete
2	UP_Q_4	✓	2	WAN	Delete
3	UP_Q_5	✓	3	WAN	Delete
4	UP_Q_6	<b>V</b>	4	WAN	Delete

Submit Refresh

Cuando se selecciona Downstream (bajada o WAN $\rightarrow$ LAN), tendría que configurar los parámetros de la siguiente figura

### DOWNSTREAM QUEUE CONFIGURATION



Submit Refresh

Tras modificar una cola, presione en **Submit** para habilitar la modificación. Presione en **Refresh** para refrescar la cola.



Código BHS\_RTA\_MAN\_AV\_ESPAÑA

Ed 1.0

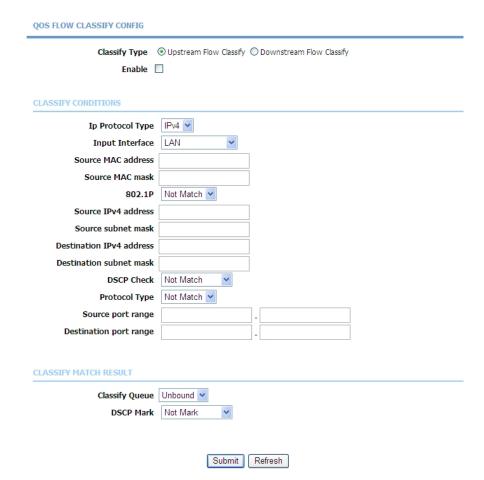
Página 37 de 62

#### 3.3.8.3 **QoS Classification**

En el menú de **QoS Configuration,** presione sobre **QoS Classification.** Se mostrará la siguiente pantalla donde puede configurar las reglas de la colas de QoS.



Presione en Add Classification Rule, se mostrará la siguiente pantalla:





Código BHS\_RTA\_MAN\_AV\_ESPAÑA

Ed 1.0

La siguiente tabla describe los parámetros de esta página:

Field	Description	
Classify Type	Configura la regla de QoS como <b>Upstream</b> o <b>Downstream</b> .	
Enable	Seleccionar para habilitar esta regla de QoS	
Ip Protocol Type	Seleccionar el tipo de protocolo <b>IPv4</b> .	
Input Interface	Elegir un interfaz WAN/LAN basándose en el tipo de clasificación.	
802.1P	Elegir una prioridad 802.1P VLAN correspondiente.	
DSCP Check	Elegir un tipo DSCP correspondiente.	
Protocol Type	Elegir un tipo de protocolo correspondiente a la regla QoS.	
Classify Queue	Elegir una cola QoS para la regla.	
DSCP Mark	Configurar una marca DSCP para la regla QoS.	

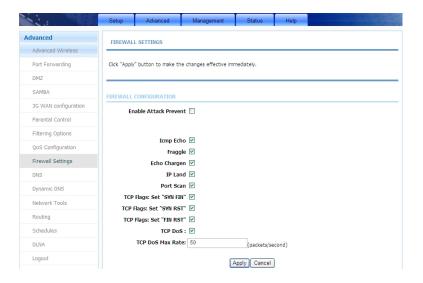
Puede presionar **Edit** para modificar una regla de clasificación ya existente.

#### 3.3.9 Configuración Firewall

Un ataque denegación de servicio (DoS attack) se caracteriza por un intento explícito de atacantes de evitar a usuarios legítimos de un servicio de utilizar este servicio.

La protección de Port Scan (escaneo de puertos) está diseñada para bloquear intentos de descubrir puertos o servicios vulnerables que pueden ser explotados desde la WAN.

Elija Advanced -> Firewall Settings. Aparecerá la siguiente pantalla:



Presione Apply para guardar los cambios.

#### 3.3.10 DNS

Domain Name System (DNS) es un servicio de Internet de internet que traslada nombres de dominio a direcciones IP, ya que los nombre de dominio son alfabéticos y son más fáciles de recordar. Internet está basado en direcciones IP. Cada vez que se utiliza un nombre de dominio, el servicio de DNS tiene que trasladar el nombre a su correspondiente dirección IP. Por ejemplo, el nombre de dominio: <a href="https://www.example.com">www.example.com</a>, podría ser trasladado a 192.108.232.4

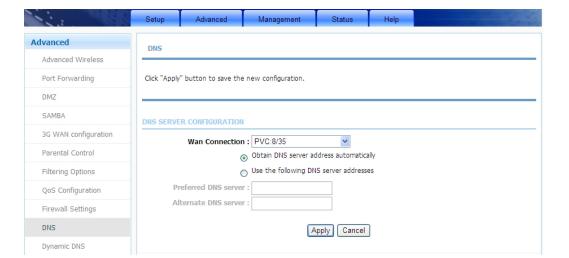
El sistema DNS, es de hecho, una red en sí mismo. Si un servidor DNS no sabe como trasladar un dominio particular, preguntará a otro servidor y así sucesivamente hasta que se devuelva la dirección IP correcta.

Seleccione **Advanced > DNS**, aparecerá la siguiente pantalla:



Código BHS\_RTA\_MAN\_AV\_ESPAÑA

Ed 1.0



Si está utilizando el módem para servicio DHCP en la LAN o utilizando los servidores DNS de la red de su proveedor, seleccione **Obtain DNS server address automatically.** 

Si tiene las direcciones IP de los DNS proporcionados por su proveedor, introduzca estas direcciones IP en los campos disponibles para servidor DNS preferido (Preferred DNS Server) y el servidor DNS alternativo (Alternate DNS Server).

Presione en Apply para guardar los cambios.

#### 3.3.11 DNS Dinámico

El módem soporta Servicio de Servidor de nombres dinámico (DDNS). Este servicio permite una dirección IP dinámica pública ser asociada con un nombre de host estático en cualquiera de los muchos dominios y permite el acceso a un host específico desde varios lugares de internet. Presione en el hiperlink de URL in el formato de hostname.dyndns.org y permita el acceso remoto a un host. Muchos ISPs asignan una dirección IP pública utilizando DHCP, por lo que localizar un host en la LAN utilizando un DNS estándar es difícil. Por ejemplo, si tiene un servidor web público funcionando en su LAN, el DDNS asegurará que el host puede ser localizado desde Internet incluso si la dirección pública cambia. DDNS requiere que se configure una cuenta con uno de los proveedores del servicio DDNS soportados (DyndDNS.org o dlinkddns.com)

Seleccione Advanced -> Dynamic DNS, aparecerá la siguiente página:



Presione en Add para añadir un DNS dinámico. Aparecerá la siguiente pantalla:



Código BHS\_RTA\_MAN\_AV\_ESPAÑA

Ed 1.0

Página 40 de 62

ADD DYNAMIC DNS	
DDNS provider:	DynDNS.org ♥
Hostname :	
Interface :	PVC:8/35
Username :	
Password :	
	Apply Cancel

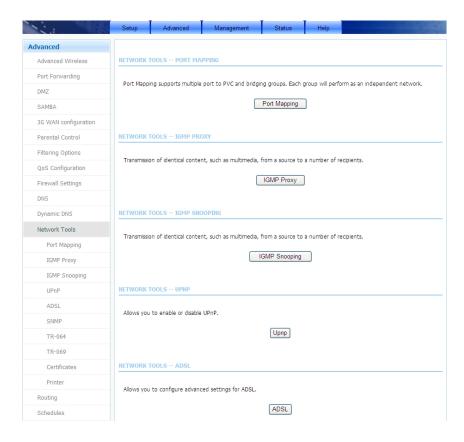
La siguiente tabla describe los parámetros de esta página:

Campo	Descripción
DDNS provider	Seleccione una de las organizaciones de registro DDNS de la lista disponible. DynDns.org y dlinkddns.com.
Host Name	Introduzca el nombre de host que registró con su proveedor de DDNS.
Username	Introduzca el usuario de su cuenta DDNS
Password	Introduzca la contraseña de su cuenta DDNS.

Presione en Apply para guardar la configuración.

### 3.3.12 Herramientas de Red

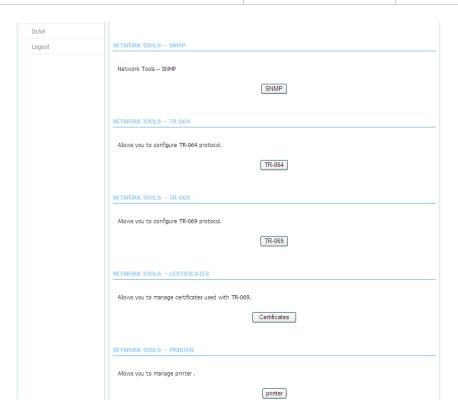
Seleccione **Advanced > Network Tools.** Aparecerá la siguiente pantalla:





Código BHS\_RTA\_MAN\_AV\_ESPAÑA

Ed 1.0



### 3.3.12.1 Mapeo de Puertos

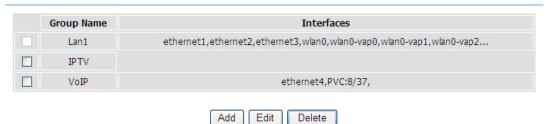
Seleccione **Advanced > Network Tools** y presione sobre **Port Mapping.** Aparecerá la siguiente página. En esta página, puede ligar la interfaz WAN y la interfaz LAN al mismo grupo.

#### PORT MAPPING

Port Mapping -- A maximum 5 entries can be configured

Port Mapping supports multiple port to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the "Add" button. The "Delete" button will remove the grouping and add the ungrouped interfaces to the Default group.

### PORT MAPPING SETUP

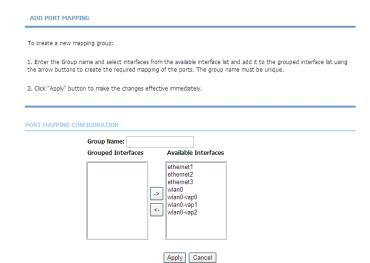


Presione en **Add** para añadir un mapeo de puertos, aparecerá la siguiente pantalla:



Código BHS\_RTA\_MAN\_AV\_ESPAÑA

Ed 1.0

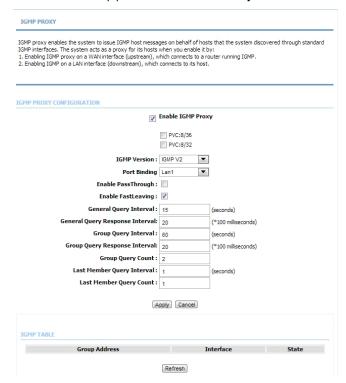


El procedimiento para crear un grupo de mapeo es el siguiente:

- Paso 1. Introduzca el nombre del grupo en Group Name.
- **Paso 2.** Seleccione los interfaces de la lista de interfaces disponibles **Available Interface** y presione el botón con la flecha ← para añadirlo a la lista **Grouped Interfaces**, para crear el mapeo de puertos requerido. El nombre del grupo debe ser único.
- Paso 3. Presione en Apply para guardar los cambios.

#### 3.3.12.2 **IGMP Proxy**

Seleccione **Advanced > Network Tools** y presione en **IGMP Proxy.** Se mostrará la siguiente página:



El IGMP Proxy habilita al sistema a propagar mensajes de host IGMP en nombre de los hosts que el sistema descubrió a través de interfaces IGMP estándar. El sistema actúa como proxy para los hosts tras habilitarlo.



Código BHS\_RTA\_MAN\_AV\_ESPAÑA

Ed 1.0

La siguiente tabla describe los parámetros de la página.

Campo	Descripción
Enable PassThrough	El dispositivo mantiene el campo de dirección IP de los paquetes de IGMP cuando se envían en sentido de subida al DSLAM.
Enable FastLeaving	Habilita al usuario IGMP a desconectarse de un grupo multicast inmediatamente, sin realizar el procedimiento de verificación con mensajes IGMP GSQ.
General Query Interval	El dispositivo enviará mensajes para chequear usuarios IGMP periódicamente. Medida en segundos.
General Query Response Interval	El dispositivo espera a que el usuario IGMP responda. Unidad en 100* milisegundos.
Group Query Interval	El dispositivo enviará peticiones de grupo multicast para comprobar si los usuarios IGMP están aún actives. Unidad en segundos.
Group Query Response Interval	El dispositivo espera a que el usuario IGMP responda. Unidad en 100* milisegundos.
Group Query Count	Este parámetro especifica cuantas veces envió el dispositivo mensajes de grupo multicast.
Last Member Query Interval	Cuando abandona el último miembro, el dispositivo envia query mensajes periódicamente. Unidad en segundos.
Last Member Query Count	Este parámetro especifica cuantas veces envió el dispositivo mensajes de query.

Presione en **Apply** para guardar los cambios.

### 3.3.12.3 IGMP Snooping

Seleccione **Advanced > Network Tools** y presione sobre **IGMP Snooping**. Aparecerá la página de la siguiente figura. Cuando está habilitado el IGMP Snooping, los datos de multicast se transmitirán sólo por el puerto LAN específico que recibió el informe de solicitud. (request report)

IGMP		
Fransmission of identical content, s	uch as multimedia, f	from a source to a number of recipients.
GMP SETUP		
Enabled :	✓	
${\bf Last Member Query Interval:}$	200000	
HostTimeout:	3000000	
MrouterTimeout:	1	
LeaveTimeout:	0	
	100	

#### 3.3.12.4 **UPnP**

Seleccione **Advanced** → **Network Tools** y presione sobre **UPnP**. Aparecerá la siguiente página:



Código BHS\_RTA\_MAN\_AV\_ESPAÑA

Ed 1.0

Página 44 de 62

UPNP			
Universal Plug and Play (UPnP) supports peer-to-peer Plug and Play functionality for network devices.			
UPNP SETUP			
WAN Connection: PVC:8/35			
LAN Connection: br0 💌			
Apply Cancel			

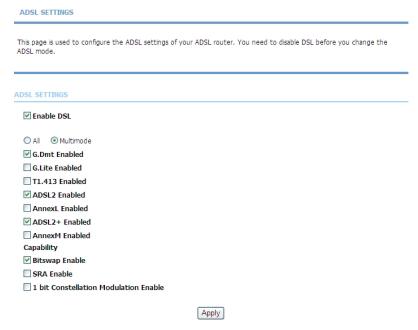
En esta página podrá configurar Universal Plug and Play (UPnP).

UPnP se utiliza para software audio visual, permite descubrir automáticamente el dispositivo en la red. Si se conectó con seguridad UPnP, puede deshabilitarlo. El bloqueo de ICMP debe estar habilitado para que el dispositivo no responda a peticiones maliciosas desde Internet.

Presione **Apply** para guardar los cambios.

### 3.3.12.5 ADSL

Seleccione **Advanced > Network Tools** y presione sobre **ADSL.** Aparecerá la siguiente página:



En esta página, puede configurar la modulación ADSL. Normalmente, puede mantener la configuración por defecto. El dispositivo negociará la modulación con el DSLAM. Presione en **Apply** para guardar los cambios.

### 3.3.12.6 **SNMP**

Seleccione **Advanced > Network Tools** y presione sobre **SNMP.** Aparecerá la siguiente página, donde puede configurar los parámetros SNMP.



Código BHS\_RTA\_MAN\_AV\_ESPAÑA

Ed 1.0

Página 45 de 62

SNMP CONFIGURATION	
This page is used to configure the	SNMP protocol.
SNMP CONFIGURATION	
	Enable SNMP Agent
Read Community:	public
Set Community:	private
Trap Manager IP:	
Trap Community:	
Trap Version:	v2c <b>▼</b>
Presione en <b>Apply</b> para guardar lo	Apply Cancel s cambios.
3.3.12.7 <u>TR-064</u>	
Seleccione <b>Advanced</b> → <b>Networ</b> l puede habilitar el servicio TR-064.	k Tools y presione sobre TR-064. Aparecerá la siguiente página, donde
TR064 CONFIGURATION	
This page is used to configure the TRO	54 protocol.
TR064 CONFIGURATION	
☐ Enab	ole TR064

Apply Cancel

Observa Telecom Página 46 de 62

Código BHS\_RTA\_MAN\_AV\_ESPAÑA

Ed 1.0

### 3.3.12.8 TR-069

Seleccione **Advanced** → **Network Tools** y presione sobre **TR-069**. Aparecerá la siguiente página, donde puede configurar los parámetros TR-069.

TR-069				
WAN management protocol (TR-069) enables an auto-configuration server (ACS) to perform auto-configuration, provision, collection, and diagnostics on the device.				
Set the appropriate values and click "Apply" to save the settings of TR-069 dient.				
TR-069 CLIENT CONFIGURATION				
Cwmp:	Disabled Enabled			
Inform:	Disabled			
Inform Interval:	86400			
ACS URL:	https://main.acs.telefonic			
ACS User Name:	ACS1234			
ACS Password:				
<b>V</b>	Connection Request Authentication			
Connection Request User Name:	ACSCR1234			
Connection Request Password:				
	Apply Cancel			

Presione en Apply para guardar los cambios.

### 3.3.12.9 Certificados

Seleccione **Advanced > Network Tools** y presione sobre **Certificates**. Aparecerá la siguiente página:

Trusted CA certificates are used by you to verify peers' certificates.

Trusted CA

Presione en el botón **Trusted CA** para importar un certificado.

Add, View or Remove certificates from this page. CA certificates are used by you to verify peers' certificates. Only one certificates can be stored. Notice you have to synchronize your time when use certificate

TRUSTED CA (CERTIFICATE AUTHORITY) CERTIFICATES

Name	Subject	Туре	Action
cert	O=Grupo Telefonica/O=TME/ST=A7	self signed certific	Delete

Input Certificate

Observa Telecom

Código BHS\_RTA\_MAN\_AV\_ESPAÑA

Ed 1.0

Página 47 de 62

Nota: Podría introducir un certificado tras borrar el ya existente

er certificate name a	and paste certificate content.	
ORT CA CERTIFICA	ATE .	
Certificate Name:		
Certificate:	BEGIN CERTIFICATE	^
	<pre><incert certificate="" here="">END CERTIFICATE</incert></pre>	
		<u>~</u>

### 3.3.12.10 **Impresora**

Seleccione **Advanced > Network Tools** y presione sobre **Printer.** Aparecerá la siguiente página dónde puede habilitar/deshabilitar el soporte de impresión.

PRINT SERVER SETTINGS			
his page allows you to enable/	disable printer support		
Enable	<b>V</b>		
Printer Name	HomeStation		
URL: http://192.168.1.1:631/printers/HomeStation			
DISPLAY LIST			
Manufacturer	Model	CMD	Firmware Version
UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN

Apply Cancel

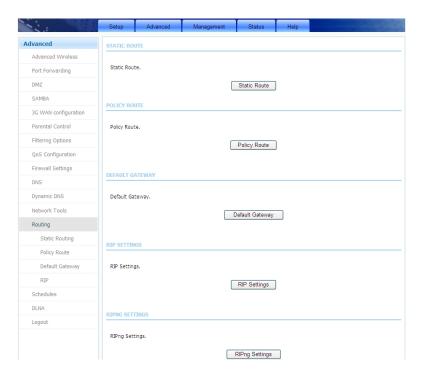
Observa Telecom Página 48 de 62

Código BHS\_RTA\_MAN\_AV\_ESPAÑA

Ed 1.0

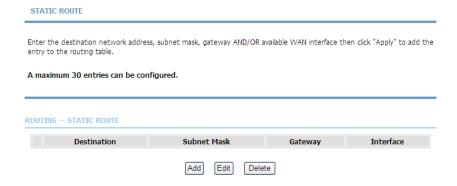
### 3.3.13 Enrutamiento (Routing)

Seleccione **Advanced > Routing.** Aparecerá la siguiente página:

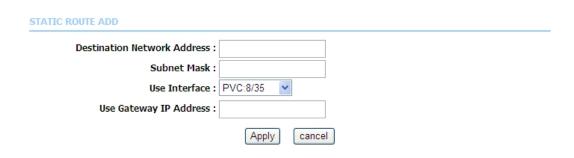


### 3.3.13.1 Enrutamiento estático

Seleccione **Advanced →Routing** y seleccione **Static Route**. Aparecerá la siguiente pantalla, que se utilize para configurar información de routing, en esta pantalla podrá añadir o borrar rutas IP.



Presione en Add para añadir una ruta estática. Aparecerá la siguiente pantalla:





Código BHS\_RTA\_MAN\_AV\_ESPAÑA

Ed 1.0

En la siguiente tabla se describen los parámetros de esta página:

Field	Description
Destination Network Address	Dirección destino de la ruta.
Subnet Mask	Máscara de subred de la dirección IP destino.
Use Interface	Nombre de la interfaz del Puerto de salida de la ruta.
Use Gateway IP Address	Dirección IP del gateway de la ruta.

Presione en Apply para guardar los cambios.

### 3.3.13.2 Políticas de enrutamiento (Policy Route)

Seleccione **Advanced →Routing** y seleccione **Policy Route**. Aparecerá la siguiente pantalla, el policy permite unir una conexión WAN a un interfaz LAN.

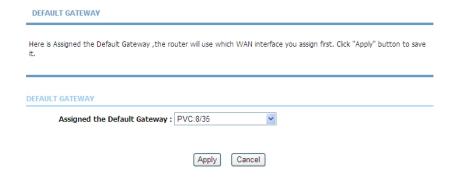


Presione en add, aparecerá la siguiente página:



### 3.3.13.3 Ruta por defecto

Seleccione **Advanced > Routing** y presione en **Default Gateway.** Aparecerá la siguiente página donde se puede asignar una ruta por defecto al módem.



Presione en **Apply** para guardar los cambios.

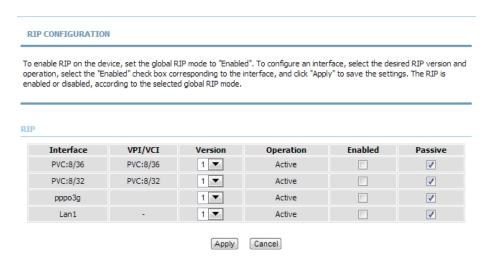


Código BHS\_RTA\_MAN\_AV\_ESPAÑA

Ed 1.0

#### 3.3.13.4 RIP

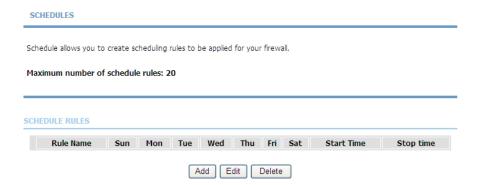
Seleccione **Advanced → Routing** y presione en **RIP Settings.** Aparecerá la siguiente página donde se pueden seleccionar los interfaces en su dispositivo que utilizan RIP y la versión del protocolo utilizada.



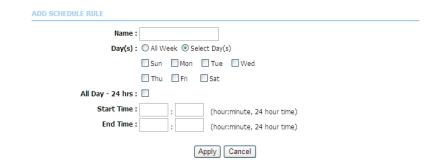
Si está utilizando el dispositivo con RIP habilitado para comunicarse con otros utilizando el protocolo RIP, habilite RIP y aplique en **Apply** para guardar los cambios.

#### 3.3.14 Programaciones

Seleccione **Advanced** → **Schedules.** Aparecerá la siguiente pantalla:



Presione en Add para añadir una progamación, aparecerá la siguiente pantalla:



Presione en **Apply** para guardar los cambios.

Observa Telecom Página 51 de 62

Código BHS\_RTA\_MAN\_AV\_ESPAÑA

Ed 1.0

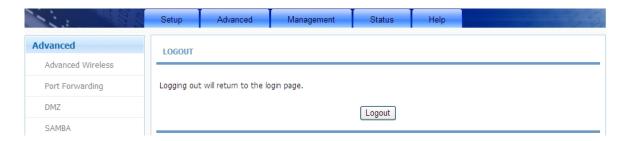
### 3.3.15 DLNA

Seleccione **Advanced** > **DLNA**. Aparecerá la siguiente pantalla, donde puede habilitar DLNA y presione en **Apply.** 

DLNA		
You can Enable or Disable DLNA here.		
DLNA SETTING		
Enable DLNA:		
	Apply Cancel	

### 3.3.16 Logout

Seleccione **Advanced** > **Logout**. Aparecerá la siguiente pantalla, donde puede abandonar la página de configuración.





Código BHS RTA MAN AV ESPAÑA

Ed 1.0

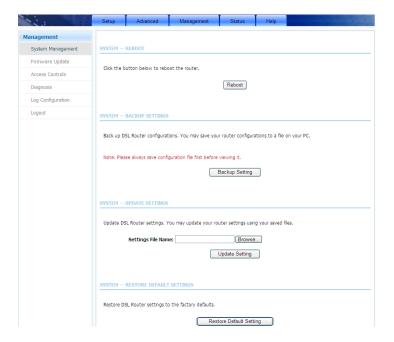
1.0 Página 52 de 62

#### 3.4.- GESTIÓN

En el menú principal seleccione la pestaña **Management** para acceder al menú de gestión que parece en la siguiente figura. Los sub menús son: **System Management, Firmware Update, Access Controls, Diagnosis, Log Configuration y Logout.** 

#### 3.4.1 Gestión de Sistema

Seleccione el menú Management -> System Management. Aparecerá la siguiente pantalla:



Desde esta página puede rebotar el módem (**Reboot**), hacer un backup del fichero de configuración (**Backup Settings**), actualizar la configuración utilizando un fichero de configuración previamente guardado y reiniciar (**Update Settings** → **Settings File Name**) el módem a sus parámetros de fábrica (**Restore Default Settings**).

#### 3.4.2 Actualización de Firmware

Selecciona Management > Firmware Update. Se mostrará la siguiente pantalla:





Código BHS RTA MAN AV ESPAÑA

Ed 1.0

Página 53 de 62

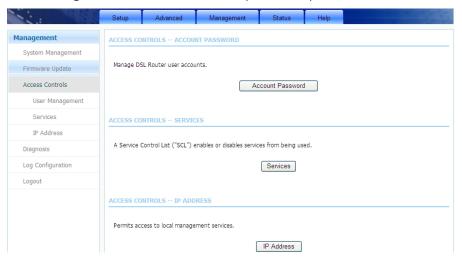
Para actualizar el Firmware siga los siguientes pasos:

- 1) Presione en **Browse** para encontrar el fichero dónde lo haya guardado previamente.
- 2) Marque Clear Config
- 3) Presione sobre **Update Firmware** para copiar el fichero.

El modem cargará el fichero y se reiniciará automáticamente.

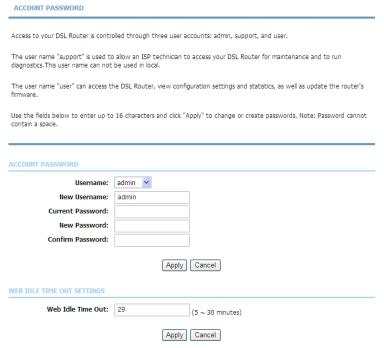
#### 3.4.3 Control de Accesos

Seleccione el menú **Management → Access Controls.** Aparecerá la pantalla:



### 3.4.3.1 Contraseñas para cuentas de acceso (Account Password)

En la página **Access Controls**, presione sobre **Account Password**. Aparecerá la siguiente pantalla, dónde puede cambiar la contraseña de usuario y el tiempo para salida automática.



Seleccione el usuario cuya contraseña quiere cambiar de la lista desplegable de usuarios. Tras esto introduzca la contraseña actual del usuario (**Current Password**) y la nueva contraseña que desee configurar (**New Password**) confirmando esta nueva contraseña en **Confirm Password**.

Por último, presione en Apply para guardar los cambios.

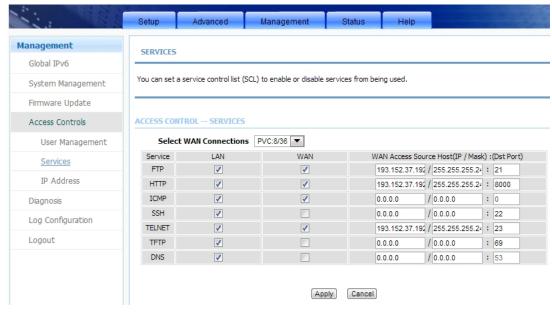


Código BHS RTA MAN AV ESPAÑA

Ed 1.0

#### 3.4.3.2 Servicios

En la página de Access Controls, presione en Services. Aparecerá la siguiente pantalla;



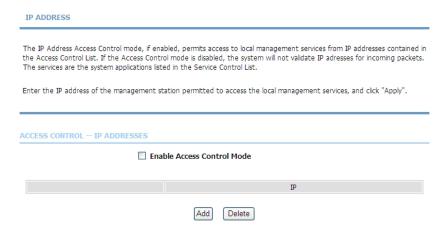
En esta página, podrá habilitar o deshabilitar los servicios que se utilizan por hosts remotos. Por ejemplo, si el servicio telnet está habilitado y su puerto es el 23, un host remoto podrá acceder al dispositivo por telnet a través del puerto 23. Normalmente, no es necesario cambiar la configuración por defecto.

Seleccione los servicios de gestión que quiera habilitar/deshabilitar en la LAN y/o WAN. Presione en **Apply** para guardar los cambios.

Nota: Si deshabilita el servicio HTTP para la LAN, no podrá volver a acceder por web al equipo.

#### 3.4.3.3 <u>Dirección IP</u>

En la página de Access Controls, presione en IP Address. Aparecerá la siguiente pantalla:



En esta página podrá configurar las direcciones IP para la lista de control de acceso (ACL). Si el ACL está habilitado, solo los dispositivos con las direcciones IPs especificadas podrán acceder al dispositivo.

Marque Enable Access Control Mode para habilitar el ACL.

Nota: Antes de habilitar el ACL, asegúrese de la dirección IP de los hosts en la lista de ACL.

Para añadir una IP a la lista, presione sobre Add. Aparecerá la siguiente pantalla:



Código BHS\_RTA\_MAN\_AV\_ESPAÑA

Ed 1.0

IP ADDRESS			
	IP Address:		

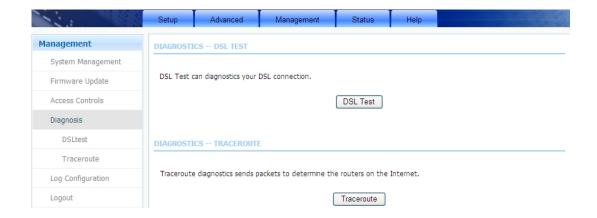
Cancel

Apply

Presione sobre Apply para aplicar la configuración.

### 3.4.4 Diagnósticos

Seleccione el menú **Management → Diagnosis**, aparecerá el menú para realizar tests de DSL y de Traceroute. (**DSL Test** and **Traceroute**)



#### 3.4.4.1 Pruebas ADSL

En la página de Diagnosis , presione sobre DSL Tests. En esta página podrá chequear su conexión DSL

#### DIAGNOSTICS

The DSL router can test your DSL connection. The individual tests are listed below. If a test displays a fail status, click the "Run Diagnostic Test" button again to make sure the fail status is consistent.



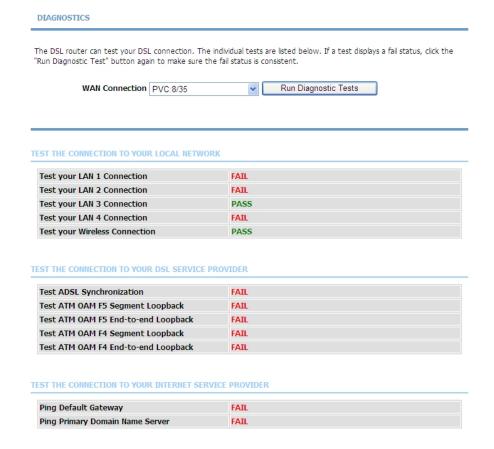
Presione sobre **Run Diagnostic Tests.** Tras el test, aparecerá la siguiente pantalla:



Código BHS\_RTA\_MAN\_AV\_ESPAÑA

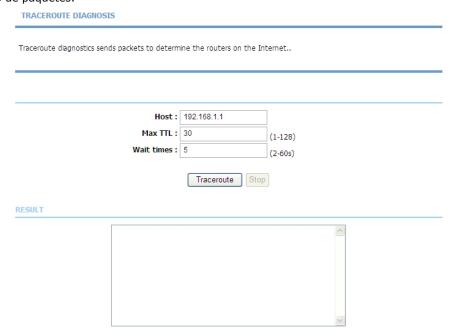
Ed 1.0

Página 56 de 62



### 3.4.4.2 Traceroute

En el menú de **Diagnosis,** presione sobre **Traceroute.** En esta página podrá determinar las rutas en Internet para el envío de paquetes.



Presione en **Traceroute** para empezar el diagnóstico. Tras terminar, aparecerá la siguiente pantalla:



Código BHS RTA MAN AV ESPAÑA

Ed 1.0

Página 57 de 62

RESULT

Tranceroute Status: Traceroute has finished traceroute to 192.168.1.1 (192.168.1.1), 30 hops max, 38 byte packets
1 homestation (192.168.1.1) 0.000 ms
0.000 ms 0.000 ms

#### 3.4.5 Configuración de Log

Vaya al menú Management → Log Configuration. Aparecerá la siguiente página de System Log:

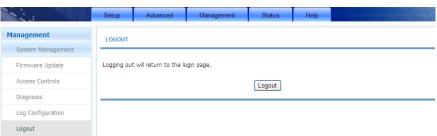


Esta página muestra los datos de eventos de logs de forma cronológica. Podrá leer los logs de forma local o enviarlos a un sistema de servidor de logs. Los niveles de severidad disponibles son los siguientes: Emergency, Alert, Critical, Error, Warning, Notice, Informational and Debugging. En esta página, podrá habilitar o deshabilitar la función de log de sistema.

- Paso 1. Seleccione "Enable log"
- Paso 2. Seleccione el modo de mostrar los logs de la lista de opciones de "Mode".
- Paso 3. Introduzca la dirección IP del Servidor (Server IP Address) y el puerto del servidor UDP (Server UDP Port) si se seleccionó como modo Both o Remote.
- Paso 4. Presione en Apply para guardar la configuración.
- Paso 5. Presione en View System Log para ver la información detallada del sistema de logs.

### 3.4.6 Salida (Logout)

Seleccione **Management →Logout.** Aparecerá la siguiente página donde puede salir de la página de configuración.





Código BHS RTA MAN AV ESPAÑA

Ed 1.0

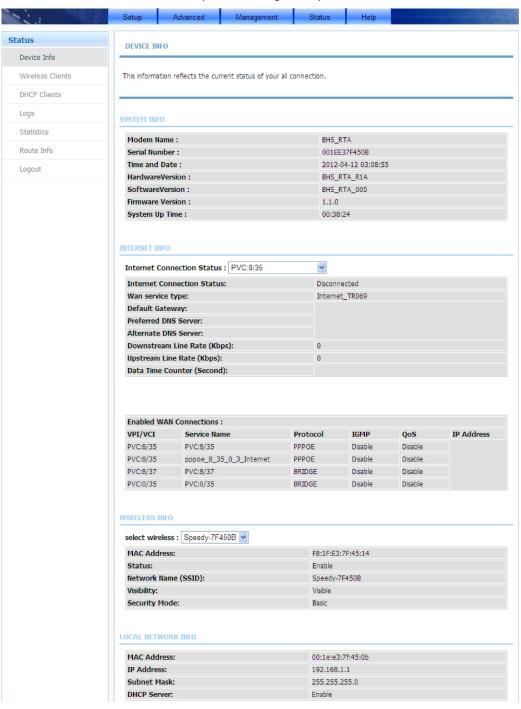
11.0

### 3.5.- Estado (Status)

En la interfaz principal, presione en la pestaña de **Status** para acceder al menú de Estado como se muestra en la siguiente pantalla. Los sub menús son **Device Info** (información del dispositivo), **Wireless Clients** (Clientes inalámbricos), **DHCP Clients** (Clientes DHCP), **Logs, Route Info** (Información de rutas) y **Logout** (salida). Puede monitorizar la información de sistema y desarrollo.

### 3.5.1 Información de Dispositivo

Seleccione Status -> Device Info. Aparecerá la siguiente pantalla.



La página muestra un resumen del estado del módem. Incluye información de la versión de Firmware, velocidad en subida, bajada, el tiempo que lleva arriba el sistema, configuración de Internet (para las interfaces Ethernet e Inalámbrica)

Observa Telecom Página 59 de 62

Código BHS RTA MAN AV ESPAÑA

Clientes Inalámbricos

Ed 1.0

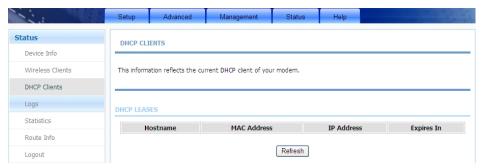
Seleccione **Status > Wireless Clients.** Aparecerá la siguiente pantalla que muestra las estaciones inalámbricas autenticadas y su estado.



### 3.5.3 Clientes DHCP

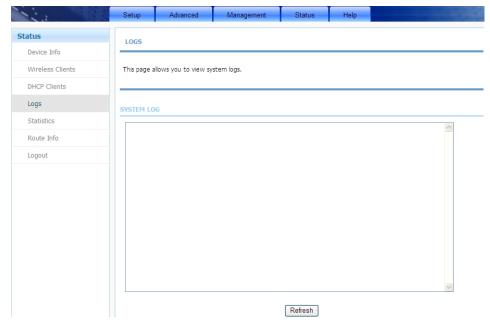
3.5.2

Seleccione **Status > DHCP Clients.** Aparecerá la siguiente pantalla que muestra todos los clientes que obtuvieron dirección IP del módem. Podrá ver el nombre de host, la dirección IP, la dirección MAC y el tiempo en que expira.



### 3.5.4 Logs

Seleccione **Status → Logs.** Aparecerá la siguiente pantalla que muestra el log de sistema. Presione sobre "**Refresh"** para actualizar el log de sistema mostrado en la tabla.



Observa Telecom Página 60 de 62

Código BHS\_RTA\_MAN\_AV\_ESPAÑA

Ed 1.0

### 3.5.5 Estadísticas

Seleccione **Status > Statistics.** Se mostrará la siguiente pantalla, que muestra estadísticas de la red y la transferencia de datos. Esta información podrá ayudar al técnico a identificar si el dispositivo está funcionando correctamente. La información no afecta a la función del dispositivo.

#### **DEVICE INFO**

It indicates the current status of all the connections.

#### LOCAL NETWORK & WIRELESS

interface	Received				Transmitted			
	Bytes	Pkts	Errs	Rx drop	Bytes	Pkts	Errs	Tx drop
LAN3	1793848	16528	0	0	3570350	14148	0	0
MOVISTAR_67CA	2918589534	11779900	0	0	22712846	59483	0	0

#### INTERNET

Service	VPI/VCI	Protocol	Received			Transmitted				
			Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
PVC:8/36	PVC:8/36	PPPOE								
PVC:8/32	PVC:8/32	PPPOE								
ррро3д		PPPOE								

#### ADSL

Mode:			0				
Туре:	0						
DSL Driver Version:	01-24-13 ver 4924c727 2windingX						
Line Coding:	Enable						
Status:			ACTIVATING.				
Up Time:							
	Downstream		Upstream				
SNR Margin (0.1dB):	0		0				
Attenuation (0.1dB):	0		0				
Output Power (dBm):	0.0		0.0				
Attainable Rate (Kbps):	0		0				
Rate (Kbps):	0		0				
D (interleave depth):	0		0				
Delay (msec):	0		0				
Data Counter:		0 Clear	0 Clear				
HEC Errors:	0		Ö				
OCD Errors:	0		0				
LCD Errors:	0		0				
CRC Errors:	0		0				
FEC Errors:	0		0				
Total ES	0		0				
Total Frames	0		510				

Observa Telecom
Página 61 de 62

Código BHS\_RTA\_MAN\_AV\_ESPAÑA

Ed 1.0

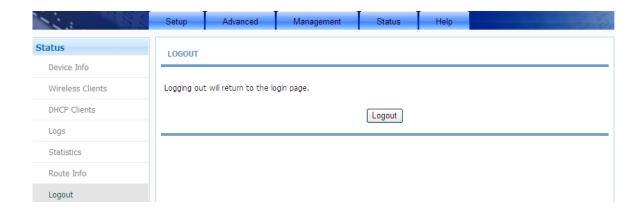
### 3.5.6 Información de Rutas (Route Info)

Seleccione **Status** → **Route Info,** la página muestra una lista de rutas por destinos comúnmente accedidos por la red.



### 3.5.7 **Salida**

Seleccione **Status** → **Logout.** Para desautenticarse de la página del módem.



Observa Telecom Página 62 de 62

Código BHS\_RTA\_MAN\_AV\_ESPAÑA

Ed 1.0

### 3.5.8 Ayuda

En la interfaz principal, presione sobre la pestaña **Help** para acceder al menú de ayuda en la siguiente figura. Esta sección provee información de configuración detallada para el módem. Presione sobre el enlace del que quiera ver la información.

