



**COMTREND CORPORATION**

---

# CT-5361

## Router Inalámbrico ADSL2+

### Guía de Configuración Rápida

Versión A1.1, 23 de Octubre del 2005

---



---

260056-014

<b>CAPÍTULO 1. CONFIGURACIÓN RÁPIDA.....</b>	<b>3</b>
1. INTRODUCCIÓN .....	3
1.1 CAMBIAR CONTRASEÑA.....	3
1.2 CONFIGURAR EL ROUTER.....	4
1.2.1 <i>Cómo crear una configuración Multipuesto Dinámico.....</i>	<i>4</i>
1.2.2 <i>Cómo Crear una Configuración Multipuesto Estático.....</i>	<i>9</i>
1.2.3 <i>Cómo Crear una Configuración Monopuesto Dinámico.....</i>	<i>13</i>
1.2.4 <i>Cómo Crear una Configuración Monopuesto Estático.....</i>	<i>17</i>
1.3 ABRIR PUERTOS (USANDO SERVIDORES VIRTUALES).....	22
1.3.1 <i>Configurar el puerto NAT según CT-5361.....</i>	<i>23</i>
1.4 INALÁMBRICO.....	25
1.4.1 <i>Pantalla Básica de Inalámbrico.....</i>	<i>25</i>
1.4.2 <i>Seguridad.....</i>	<i>27</i>
1.4.3 <i>Filtro CMA.....</i>	<i>30</i>
1.4.4 <i>Puente Inalámbrico.....</i>	<i>32</i>
1.4.5 <i>Avanzado.....</i>	<i>33</i>
1.4.6 <i>Información sobre Estaciones.....</i>	<i>35</i>
1.5 GUARDAR Y REINICIAR.....	36
1.6 ACTUALIZAR EL SOFTWARE.....	37

# Capítulo 1. Configuración rápida

## 1. Introducción

Este documento ofrece una orientación para configurar el router ADSL/ADSL2+ Comtrend CT-5361, suministrado con el *Kit ADSL Router Inalámbrico* de Telefónica, a través del configurador web que incorpora este equipo.

Para la configuración del servicio ADSL que Telefónica le proporciona, se recomienda seguir las instrucciones indicadas en el *Manual de Usuario* que se incluye en el kit. Esta guía complementa dicho manual explicando cómo realizar las distintas tareas de configuración utilizando el configurador web del router ADSL/ADSL2+ en lugar de utilizar el asistente de configuración incluido en el kit para los sistemas operativos de Windows. Se recomienda utilizar preferentemente el asistente.

**AVISO:** Antes de utilizar las herramientas que ofrece el fabricante de este producto y respecto de las que Telefónica de España le informa con carácter meramente orientativo, le recordamos que Telefónica de España no ofrece ningún tipo de soporte técnico sobre las mismas.

### 1.1 Cambiar Contraseña

La opción Contraseñas configura las contraseñas de acceso del router. El acceso a su router ADSL está controlado por medio de una cuenta de un solo usuario: [1234](#).

- “[1234](#)” tiene acceso irrestringido para cambiar y ver la configuración de su router ADSL.
- Nombre de usuario: [1234](#)
- Contraseña: [1234](#)

Utilice los campos de debajo para introducir hasta 16 caracteres y haga clic en Aplicar para cambiar o crear contraseñas.

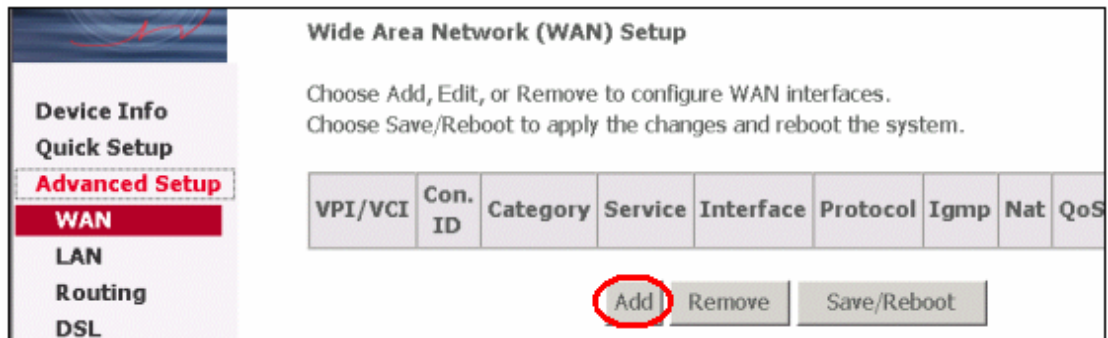
**Cambiar contraseña:** Para cambiar la contraseña, introduzca la antigua contraseña, introduzca la nueva contraseña y confirme la nueva contraseña introduciéndola de nuevo. Luego haga clic en Guardar/Aplicar. Tenga en cuenta que al cambiar la contraseña es necesario reiniciar CT-5361 para que el cambio tenga efecto.



## 1.2 Configurar el Router

### 1.2.1 Cómo crear una configuración *Multipuesto Dinámico*

**Paso 1-1:** Configurar el puerto WAN. (Vaya a Configuración avanzada/WAN o Configuración rápida; haga clic en el botón Añadir para crear una interfaz WAN, como se indica debajo)



**Paso 1-2:** Introduzca los valores VPI/VCI; seleccione "Categoría del Servicio"; active Calidad del Servicio (chequeando la casilla); luego haga clic en el botón Siguiente, como ilustrado debajo.

This screen allows you to configure an ATM PVC identifier (VPI and VCI) and select a service category.

VPI: [0-255]

VCI: [32-65535]

Service Category:

#### Enable Quality Of Service

Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. However, since QoS also consumes system resources, the number of PVCs will be reduced consequently. Use **Advanced Setup/Quality of Service** to assign priorities for the applications.

Enable Quality Of Service

**Paso 1-3:** Select **Seleccione PPP en Ethernet**; seleccione “**LLC/SNAP – BRIDGING**” como **Modo de Encapsulado**, luego haga clic en el botón **Siguiente**, como se indica más abajo.

#### Connection Type

Select the type of network protocol and encapsulation mode over the ATM PVC that your ISP has instructed you to use.

PPP over ATM (PPPoA)

PPP over Ethernet (PPPoE)

MAC Encapsulation Routing (MER)

IP over ATM (IPoA)

Bridging

#### Encapsulation Mode

**Paso 1-4:** Introduzca el nombre de usuario y Contraseña del PPP que encontrará en la carta con la información de usuario que le ha enviado Telefónica; seleccione “**AUTO**” como **Método de Autenticación**; active NAT; luego haga clic en el botón **Siguiente**, según ilustrado abajo.

PPP Username:	<input type="text" value="pppoe3@tid/pppoe"/>
PPP Password:	<input type="password" value="*****"/>
PPPoE Service Name:	<input type="text"/>
Authentication Method:	<input type="text" value="AUTO"/> ▼
<input type="checkbox"/> Dial on Demand (with idle timeout timer)	
<input type="checkbox"/> PPP IP extension	
<input checked="" type="checkbox"/> Enable NAT	
<input type="checkbox"/> Enable Firewall	

**Paso 1-5:** Siga haciendo clic en el botón Siguiente hasta que aparece la pantalla Guardar configuración WAN. Haga clic en GUARDAR.

**Paso 2-1:** Configurar el puerto LAN. (Vaya a Configuración avanzada/LAN como se indica más abajo)

Local Area Network (LAN) Setup	
<b>Device Info</b> <b>Quick Setup</b> <b>Advanced Setup</b> <b>WAN</b> <b>LAN</b>	Configure the DSL Router IP Address and Subnet Mask for LAN interface. Save button only saves the LAN configuration data. Save/Reboot button saves the LAN configuration data and reboots the router to make the new configuration effective.
	IP Address: <input type="text" value="192.168.1.1"/> Subnet Mask: <input type="text" value="255.255.255.0"/>

**Paso 2-2:** Introduzca la dirección IP y la máscara de subred de la LAN; introduzca la dirección IP y la máscara de subred de Loopback; active servidor DHCP e introduzca el rango IP/tiempo; active escucha IGMP (chequeando la casilla); como se indica más abajo y luego haga clic en el botón Guardar.

IP Address:	<input type="text" value="192.168.1.1"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
<b>Loopback IP and Subnetmask</b>	
IP Address:	<input type="text" value="127.0.0.1"/>
Subnetmask:	<input type="text" value="255.0.0.0"/>

<input type="radio"/> Disable DHCP Server
<input checked="" type="radio"/> Enable DHCP Server
Start IP Address: <input type="text" value="192.168.1.33"/>
End IP Address: <input type="text" value="192.168.1.64"/>
Leased Time (hour): <input type="text" value="24"/>
<input checked="" type="checkbox"/> Enable IGMP-SNOOPING

**Paso 3-1:** Configure la CS. (Actualice la pantalla GUI y vaya a Configuración avanzada/Calidad del Servicio, como se indica más abajo).

Quality of Service Setup																			
<b>Device Info</b> <b>Advanced Setup</b> <b>WAN</b> <b>LAN</b> <b>NAT</b> <b>Parental Control</b> <b>Quality of Service</b>	Choose Add or Remove to configure network traffic classes.																		
	<table border="1"> <thead> <tr> <th>Class Name</th> <th>Priority</th> <th>IP Precedence</th> <th>IP Type of Service</th> <th>802.1P</th> <th>Protocol</th> <th>Source Address / Mask</th> <th>Source Port</th> <th>D A M</th> </tr> </thead> <tbody> <tr> <td>VoIP</td> <td>High</td> <td></td> <td></td> <td></td> <td>UDP</td> <td></td> <td></td> <td>81 21</td> </tr> </tbody> </table>	Class Name	Priority	IP Precedence	IP Type of Service	802.1P	Protocol	Source Address / Mask	Source Port	D A M	VoIP	High				UDP			81 21
	Class Name	Priority	IP Precedence	IP Type of Service	802.1P	Protocol	Source Address / Mask	Source Port	D A M										
	VoIP	High				UDP			81 21										

**Paso 3-2:** Añada una Regla de Clase de Tráfico de Red haciendo clic en el botón Añadir en la pantalla CS; introduzca un nombre para la clase de tráfico; establezca la Prioridad Alta; configure el protocolo como UDP; introduzca la dirección IP y la máscara de subred del destino según se indica más abajo, luego haga clic en el botón Guardar/Aplicar.

Traffic Class Name:	VoIP
Priority:	High
Protocol:	UDP
Destination IP Address:	81.47.224.0
Destination Subnet Mask:	255.255.252.0

**Paso 3-3:** Seleccione una interfaz de tráfico; introduzca la Velocidad Mínima según se indica más abajo, luego haga clic en Guardar.

<b>Traffic Interface Control</b>	
Traffic Interface :	ppp_8_32_1
Minimum Rate :	32 Kbps

**Paso 4-1:** Configurar el Control del Acceso. (Vaya a Administración/Control de Acceso como de indica más abajo).

<b>Management Settings</b> <b>System Log</b> <b>SNMP Agent</b> <b>Internet Time</b> <b>Access Control</b>	FTP	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
	HTTP	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
	ICMP	Enable	<input checked="" type="checkbox"/> Enable
	SNMP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable
	SSH	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable

**Paso 4-2:** Haga una Lista de Control del Servicio según ilustrado más abajo.

Services	LAN	WAN
FTP	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
HTTP	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
ICMP	Enable	<input checked="" type="checkbox"/> Enable
SNMP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable
SSH	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable
TELNET	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
TFTP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable

**Paso 4-3:** Vaya al menu Dirección IP y seleccione Modo Control del Acceso e introduzca la dirección IP/máscara de subred de las interfaces como se indica más abajo.



SNMP Agent  
 Internet Time  
 Access Control  
 Services  
**IP Addresses**  
 Passwords

Access Control Mode:  Disable  Enable

IP Address	Subnet Mask	Interface	Remove
193.152.37.192	255.255.255.240	wan	<input type="checkbox"/>
0.0.0.0	0.0.0.0	lan	<input type="checkbox"/>

**Paso 5:** Seleccione Guardar/Reiniciar en el menu principal para guardar y reinicie el router (como se indica más abajo).

Internet Time  
 Access Control  
 Update Software  
**Save/Reboot**

Click the button below to save and reboot the router.

Save/Reboot

## 1.2.2 Cómo Crear una Configuración *Multipuesto Estático*

**Paso 1-1:** Configurar el puerto WAN. (Vaya a Configuración avanzada/WAN o Configuración rápida; haga clic en el botón Añadir para crear una interfaz WAN, como se indica más abajo)

Wide Area Network (WAN) Setup

Choose Add, Edit, or Remove to configure WAN interfaces.  
 Choose Save/Reboot to apply the changes and reboot the system.

VPI/VCI	Con. ID	Category	Service	Interface	Protocol	Igmp	Nat	QoS
<input checked="" type="button" value="Add"/> <input type="button" value="Remove"/> <input type="button" value="Save/Reboot"/>								

**Paso 1-2:** Introduzca los valores VPI/VCI; seleccione “Categoría del Servicio”; active Calidad del Servicio; luego haga clic en el botón Siguiente, según ilustrado más abajo.

This screen allows you to configure an ATM PVC identifier (VPI and VCI) and select a service category.

VPI: [0-255]

VCI: [32-65535]

Service Category:  ▼

### Enable Quality Of Service

Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. However, since QoS also consumes system resources, the number of PVCs will be reduced consequently. Use **Advanced Setup/Quality of Service** to assign priorities for the applications.

Enable Quality Of Service

**Paso 1-3:** Seleccione la IP en ATM (IPoA); seleccione “LLC/SNAP – BRIDGING” como **Modo de Encapsulado**, luego haga clic en el botón Siguiente, como se indica más abajo.

IP over ATM (IPoA)

Bridging

**Encapsulation Mode**

LLC/SNAP-ROUTING ▼

**Paso 1-4:** Introduzca la dirección IP/Máscara de subred de la WAN; seleccione “Utilizar las siguientes puertas predeterminadas” (chequeando la casilla) e introduzca “Utilizar dirección IP” (chequeando la casilla); seleccione “Utilizar las siguientes direcciones DSN del servidor” (chequeando la casilla) e introduzca las direcciones del servidor DSN primario/secundario; luego haga clic en el botón Siguiente (como se indica más abajo). Encontrará todos estos datos en la carta con la información de usuario que le ha enviado Telefónica.

WAN IP Address: 80.0.5.62

WAN Subnet Mask: 255.255.255.252

Use the following default gateway:

Use IP Address: 80.0.5.61

Use WAN Interface: ipoa\_8\_32/ipa\_8\_32 ▼

Use the following DNS server addresses:

Primary DNS server: 80.58.61.250


Secondary DNS server: 80.58.61.254

**Paso 1-5:** Introduzca el Servicio NAT & WAN; desactive el Firewall y IGMP (desmarcando la casilla), luego haga clic en el botón Siguiente (como se indica más abajo).

Enable NAT	<input checked="" type="checkbox"/>
Enable Firewall	<input type="checkbox"/>
<b>Enable IGMP Multicast, and WAN Service</b>	
Enable IGMP Multicast	<input type="checkbox"/>
Enable WAN Service	<input checked="" type="checkbox"/>
Service Name:	<input type="text" value="ipoa_8_32"/>

**Paso 1-6:** Haga clic en el botón GUARDAR para guardar la configuración WAN.

**Paso 2-1:** Configurar el puerto LAN. (Vaya a Configuración avanzada/LAN como se indica más abajo).

		<b>Local Area Network (LAN) Setup</b>
<b>Device Info</b> <b>Quick Setup</b> <b>Advanced Setup</b> <b>WAN</b> <b>LAN</b>		Configure the DSL Router IP Address and Subnet Mask for LAN interface. Save button only saves the LAN configuration data. Save/Reboot button saves the LAN configuration data and reboots the router to make the new configuration effective.
		IP Address: <input type="text" value="192.168.1.1"/> Subnet Mask: <input type="text" value="255.255.255.0"/>

**Paso 2-2:** Introduzca la dirección IP y la máscara de subred de la LAN; introduzca la dirección IP y la máscara de subred de Loopback; active servidor DHCP e introduzca el rango IP/tiempo; active IGMP (chequeando la casilla); como se indica más abajo y luego haga clic en el botón Guardar.

IP Address:	<input type="text" value="192.168.1.1"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
<b>Loopback IP and Subnetmask</b>	
IP Address:	<input type="text" value="127.0.0.1"/>
Subnetmask:	<input type="text" value="255.0.0.0"/>

<input type="radio"/> Disable DHCP Server	
<input checked="" type="radio"/> Enable DHCP Server	
Start IP Address:	<input type="text" value="192.168.1.33"/>
End IP Address:	<input type="text" value="192.168.1.64"/>
Leased Time (hour):	<input type="text" value="24"/>
<input checked="" type="checkbox"/> Enable IGMP-SNOOPING	

**Paso 3-1:** Configurar la CS. (Actualice la pantalla GUI y vaya a Configuración avanzada/Calidad del Servicio, como se indica más abajo).

Quality of Service Setup									
Choose Add or Remove to configure network traffic classes.									
Class Name	Priority	IP Precedence	IP Type of Service	802.1P	Protocol	Source Address / Mask	Source Port	D	A
VoIP	High				UDP			8	2

**Paso 3-2:** Añada una Regla de Clase de Tráfico de Red haciendo clic en el botón Añadir en la pantalla CS; introduzca un nombre para la Clase de Tráfico; establezca la Prioridad Alta; configure el protocolo como UDP; introduzca la dirección IP destino y la máscara de subred según se indica más abajo, luego haga clic en el botón Guardar/Aplicar.

Traffic Class Name:	VoIP
Priority:	High
Protocol:	UDP
Destination IP Address:	81.47.224.0
Destination Subnet Mask:	255.255.252.0

**Paso 3-3:** Seleccione la Interfaz de Tráfico; introduzca la Velocidad Mínima según se indica más abajo, luego haga clic en Guardar.

Traffic Interface Control	
Traffic Interface :	ppp_8_32_1
Minimum Rate :	32 Kbps

**Paso 4-1:** Configurar el Control del Acceso. (Vaya a Administración/Control del acceso como se indica más abajo).

Management Settings			
System Log		FTP	<input checked="" type="checkbox"/> Enable <input checked="" type="checkbox"/> Enable
SNMP Agent		HTTP	<input checked="" type="checkbox"/> Enable <input checked="" type="checkbox"/> Enable
Internet Time		ICMP	Enable <input checked="" type="checkbox"/> Enable
<b>Access Control</b>		SNMP	<input checked="" type="checkbox"/> Enable <input type="checkbox"/> Enable
		SSH	<input checked="" type="checkbox"/> Enable <input type="checkbox"/> Enable

**Paso 4-2:** Haga una Lista de Control del Servicio según ilustrado más abajo.

Services	LAN	WAN
FTP	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
HTTP	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
ICMP	Enable	<input checked="" type="checkbox"/> Enable
SNMP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable
SSH	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable
TELNET	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
TFTP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable

**Paso 4-3:** Vaya al menu Dirección IP para seleccionar Modo Control del Acceso e introduzca la dirección IP/máscara de subred de las interfaces como se indica más abajo.

**SNMP Agent**

**Internet Time**

**Access Control**

**Services**

**IP Addresses**

**Passwords**

Access Control Mode:  Disable  Enable

IP Address	Subnet Mask	Interface	Remove
193.152.37.192	255.255.255.240	wan	<input type="checkbox"/>
0.0.0.0	0.0.0.0	lan	<input type="checkbox"/>

**Paso 5:** Seleccione Guardar/Reiniciar en el menu principal para guardar y reinicie el router. (como se indica más abajo).

**Internet Time**

**Access Control**

**Update Software**

**Save/Reboot**

**Click the button below to save and reboot the router.**

Save/Reboot

### 1.2.3 Cómo Crear una Configuración *Monopuesto Dinámico*

**Paso 1-1:** Configurar el puerto WAN. (Vaya a Configuración avanzada/WAN o Configuración rápida; haga clic en el botón Añadir para crear una interfaz WAN, como se indica más abajo).

**Paso 1-2:** Introduzca los valores VPI/VCI; seleccione “Service Category”; active Calidad del Servicio (chequeando la casilla); luego haga clic en el botón Siguiente, como se indica más abajo.

This screen allows you to configure an ATM PVC identifier (VPI and VCI) and select a service category.

VPI: [0-255]

VCI: [32-65535]

Service Category:

**Enable Quality Of Service**

Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. However, since QoS also consumes system resources, the number of PVCs will be reduced consequently. Use **Advanced Setup/Quality of Service** to assign priorities for the applications.

Enable Quality Of Service

**Paso 1-3:** Seleccione Puente; seleccione “LLC/SNAP – BRIDGING” como **Modo de Encapsulado**, luego haga clic en el botón Siguiente, como se indica más abajo.

IP over ATM (IPoA)

Bridging

**Encapsulation Mode**

**Paso 1-4:** [Siga](#) haciendo clic en el botón Siguiente hasta que aparezca la pantalla GUARDAR configuración WAN. Haga clic en GUARDAR.

**Paso 2-1:** Configurar el puerto LAN. (Vaya a Configuración avanzada/LAN como se indica más abajo)

Local Area Network (LAN) Setup	
<b>Device Info</b> <b>Quick Setup</b> <b>Advanced Setup</b> <b>WAN</b> <b>LAN</b>	Configure the DSL Router IP Address and Subnet Mask for LAN interface. Save button only saves the LAN configuration data. Save/Reboot button saves the LAN configuration data and reboots the router to make the new configuration effective.
	IP Address: <input type="text" value="192.168.1.1"/> Subnet Mask: <input type="text" value="255.255.255.0"/>

**Paso 2-2:** Introduzca la dirección IP y la máscara de subred de la LAN; introduzca la dirección IP y la máscara de subred de Loopback; desactive el servidor DHCP (deschequeando la casilla) como se indica más abajo; luego haga clic en el botón Guardar.

IP Address:	<input type="text" value="192.168.1.1"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
<b>Loopback IP and Subnetmask</b>	
IP Address:	<input type="text" value="127.0.0.1"/>
Subnetmask:	<input type="text" value="255.0.0.0"/>

**Paso 3-1:** Configurar la CS. (Actualice la pantalla GUI y vaya a Configuración avanzada/Calidad del Servicio, como se indica más abajo).

Quality of Service Setup																							
<b>Device Info</b> <b>Advanced Setup</b> <b>WAN</b> <b>LAN</b> <b>NAT</b> <b>Parental Control</b> <b>Quality of Service</b>	Choose Add or Remove to configure network traffic classes.																						
	<table border="1"> <thead> <tr> <th>Class Name</th> <th>Priority</th> <th>IP Precedence</th> <th>IP Type of Service</th> <th>802.1P</th> <th>Protocol</th> <th>Source Address / Mask</th> <th>Source Port</th> <th>D</th> <th>A</th> <th>M</th> </tr> </thead> <tbody> <tr> <td>VoIP</td> <td>High</td> <td></td> <td></td> <td></td> <td>UDP</td> <td></td> <td></td> <td>8</td> <td>2</td> <td></td> </tr> </tbody> </table>	Class Name	Priority	IP Precedence	IP Type of Service	802.1P	Protocol	Source Address / Mask	Source Port	D	A	M	VoIP	High				UDP			8	2	
	Class Name	Priority	IP Precedence	IP Type of Service	802.1P	Protocol	Source Address / Mask	Source Port	D	A	M												
	VoIP	High				UDP			8	2													

**Paso 3-2:** Añada una Regla de Clase de Tráfico de Red haciendo clic en el botón Añadir en la pantalla CS; introduzca un nombre para la Clase de Tráfico; establezca la Prioridad Alta; configure el Protocolo como UDP; introduzca la dirección IP y la máscara de subred del destino según se indica más abajo, luego haga clic en el botón Guardar/Aplicar.

Traffic Class Name:	<input type="text" value="VoIP"/>
Priority:	<input type="text" value="High"/>
Protocol:	<input type="text" value="UDP"/>
Destination IP Address:	<input type="text" value="81.47.224.0"/>
Destination Subnet Mask:	<input type="text" value="255.255.252.0"/>

**Paso 3-3:** Seleccione la Interfaz de Tráfico; introduzca la Velocidad Mínima según se indica más abajo, luego haga clic en Guardar.

Traffic Interface Control	
Traffic Interface :	<input type="text" value="ppp_8_32_1"/>
Minimum Rate :	<input type="text" value="32"/> Kbps

**Paso 4-1:** Configurar el Control del Acceso. (Vaya a Administración/Control del Acceso como se indica más abajo).

<b>Management Settings</b> <b>System Log</b> <b>SNMP Agent</b> <b>Internet Time</b> <b>Access Control</b>	FTP	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
	HTTP	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
	ICMP	Enable	<input checked="" type="checkbox"/> Enable
	SNMP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable
	SSH	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable

**Paso 4-2:** Haga una Lista de Control del Servicio según ilustrado más abajo. (Active todos los servicios en la LAN)

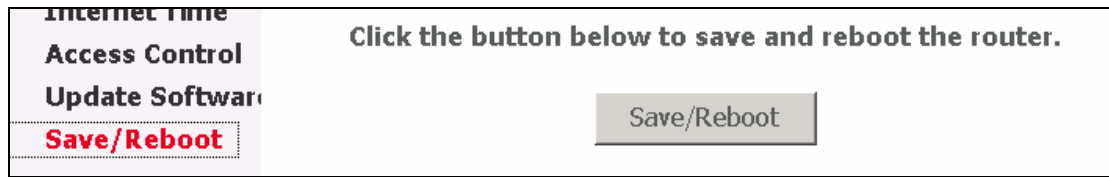
Services	LAN
FTP	<input checked="" type="checkbox"/> Enable
HTTP	<input checked="" type="checkbox"/> Enable
ICMP	Enable
SNMP	<input checked="" type="checkbox"/> Enable
SSH	<input checked="" type="checkbox"/> Enable
TELNET	<input checked="" type="checkbox"/> Enable
TFTP	<input checked="" type="checkbox"/> Enable

**Paso 4-3:** Vaya al menu Dirección IP para seleccionar Modo Control del Acceso e introduzca la dirección IP/máscara de subred de las interfaces como se indica más abajo.

<b>SNMP Agent</b> <b>Internet Time</b> <b>Access Control</b> <b>Services</b> <b>IP Addresses</b> <b>Passwords</b>	Access Control Mode: <input type="radio"/> Disable <input checked="" type="radio"/> Enable			
	IP Address	Subnet Mask	Interface	Remove
	193.152.37.192	255.255.255.240	wan	<input type="checkbox"/>
	0.0.0.0	0.0.0.0	lan	<input type="checkbox"/>

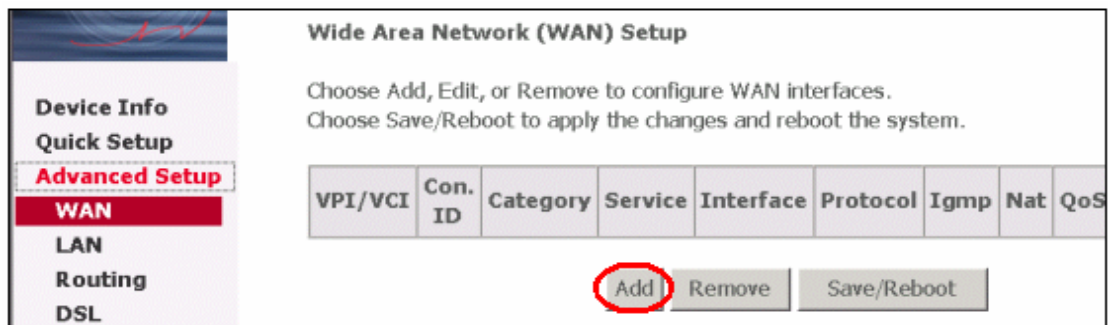


**Paso 5:** Seleccione Guardar/Reiniciar en el menu principal para guardar y reinicie el router (como se indica más abajo).



## 1.2.4 Cómo Crear una Configuración *Monopuesto Estático*

**Paso 1-1:** Configurar el puerto WAN. (Vaya a Configuración avanzada/WAN o Configuración rápida; haga clic en el botón Añadir para crear una interfaz WAN, como se indica más abajo).



**Paso 1-2:** Introduzca los valores VPI/VCI; seleccione "Categoría del Servicio"; active Calidad del Servicio (chequeando la casilla); luego haga clic en el botón Siguiente, según ilustrado más abajo.

This screen allows you to configure an ATM PVC identifier (VPI and VCI) and select a service category.

VPI: [0-255]

VCI: [32-65535]

Service Category:

---

**Enable Quality Of Service**

Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. However, since QoS also consumes system resources, the number of PVCs will be reduced consequently. Use **Advanced Setup/Quality of Service** to assign priorities for the applications.

Enable Quality Of Service

**Paso 1-3:** Seleccione la IP en ATM (IpoA); seleccione “LLC/SNAP – BRIDGING” como **Modo de Encapsulado**, luego haga clic en el botón Siguiente, como se indica más abajo.

<input checked="" type="radio"/> IP over ATM (IPoA)
<input type="radio"/> Bridging
<b>Encapsulation Mode</b>
LLC/SNAP-ROUTING ▼

**Paso 1-4:** Introduzca la dirección IP/Máscara de subred de la WAN; seleccione “Utilizar las siguientes puertas predeterminadas” (chequeando la casilla) e introduzca “Utilizar dirección IP” (chequeando la casilla); seleccione “Utilizar la siguiente dirección DSN del servidor” (chequeando la casilla) e introduzca la dirección del servidor DSN primario/secundario. Encontrará todas estas informaciones en la carta con la información de usuario que le ha enviado Telefónica. Haga clic en el botón Siguiente (como se indica más abajo).

WAN IP Address:	<input type="text" value="10.0.0.5"/>
WAN Subnet Mask:	<input type="text" value="255.255.255.0"/>
<input checked="" type="checkbox"/> Use the following default gateway:	
<input checked="" type="checkbox"/> Use IP Address:	<input type="text" value="10.0.0.1"/>
<input type="checkbox"/> Use WAN Interface:	<input style="border: none; background-color: #f0f0f0; padding: 2px 5px;" type="text" value="ipoa_8_32/ipa_8_32"/>
<input checked="" type="checkbox"/> Use the following DNS server addresses:	
Primary DNS server:	<input type="text" value="80.58.61.250"/>
Secondary DNS server:	<input type="text" value="80.58.61.254"/>

**Paso 1-5:** Introduzca Servicio WAN; desactive NAT, Firewall e IGMP (deschequeando la casilla), luego haga clic en el botón Siguiente (como se indica más abajo).

Enable NAT	<input type="checkbox"/>
Enable Firewall	<input type="checkbox"/>
<b>Enable IGMP Multicast, and WAN Service</b>	
Enable IGMP Multicast	<input type="checkbox"/>
Enable WAN Service	<input checked="" type="checkbox"/>
Service Name:	<input type="text" value="ipoa_8_32"/>

**Paso 1-6:** Haga clic en el botón GUARDAR para guardar la configuración WAN.

**Paso 2-1:** Configurar el puerto LAN. (Vaya a Configuración avanzada/LAN como se indica más abajo).

Local Area Network (LAN) Setup	
<b>Device Info</b> <b>Quick Setup</b> <b>Advanced Setup</b> <b>WAN</b> <b>LAN</b>	Configure the DSL Router IP Address and Subnet Mask for LAN interface. Save button only saves the LAN configuration data. Save/Reboot button saves the LAN configuration data and reboots the router to make the new configuration effective.
	IP Address: <input type="text" value="192.168.1.1"/> Subnet Mask: <input type="text" value="255.255.255.0"/>

**Paso 2-2:** Introduzca la dirección IP y la máscara de subred de la LAN; introduzca la dirección IP y la máscara de subred de Loopback; active servidor DHCP (chequeando la casilla) e introduzca el rango IP/tiempo; active escuchar IGMP (chequeando la casilla); como se indica más abajo y luego haga clic en el botón Guardar.

IP Address:	<input type="text" value="80.0.5.61"/>
Subnet Mask:	<input type="text" value="255.255.255.252"/>
<b>Loopback IP and Subnetmask</b>	
IP Address:	<input type="text" value="127.0.0.1"/>
Subnetmask:	<input type="text" value="255.0.0.0"/>
<input type="radio"/> Disable DHCP Server <input checked="" type="radio"/> Enable DHCP Server	
Start IP Address:	<input type="text" value="80.0.5.62"/>
End IP Address:	<input type="text" value="80.0.5.62"/>
Leased Time (hour):	<input type="text" value="24"/>
<input type="radio"/> Enable DHCP Server Relay DHCP Server IP Address: <input type="text"/>	
<input checked="" type="checkbox"/> Enable IGMP-SNOOPING	

**Paso 3-1:** Configurar la CS. (Actualice la pantalla GUI y vaya a Configuración avanzada/Calidad del Servicio, como se indica más abajo).

Quality of Service Setup																							
<b>Device Info</b> <b>Advanced Setup</b> <b>WAN</b> <b>LAN</b> <b>NAT</b> <b>Parental Control</b> <b>Quality of Service</b>	Choose Add or Remove to configure network traffic classes.																						
	<table border="1"> <thead> <tr> <th>Class Name</th> <th>Priority</th> <th>IP Precedence</th> <th>IP Type of Service</th> <th>802.1P</th> <th>Protocol</th> <th>Source Address / Mask</th> <th>Source Port</th> <th>D</th> <th>A</th> <th>M</th> </tr> </thead> <tbody> <tr> <td>VoIP</td> <td>High</td> <td></td> <td></td> <td></td> <td>UDP</td> <td></td> <td></td> <td>8</td> <td></td> <td>2</td> </tr> </tbody> </table>	Class Name	Priority	IP Precedence	IP Type of Service	802.1P	Protocol	Source Address / Mask	Source Port	D	A	M	VoIP	High				UDP			8		2
	Class Name	Priority	IP Precedence	IP Type of Service	802.1P	Protocol	Source Address / Mask	Source Port	D	A	M												
	VoIP	High				UDP			8		2												

**Paso 3-2:** Añada una Regla de Clase de Tráfico de Red haciendo clic en el botón Añadir en la pantalla CS; introduzca un nombre para la clase de tráfico; establezca la Prioridad Alta; configure el protocolo como UDP; introduzca la dirección IP destino y la máscara de subred según se indica más abajo, luego haga clic en el botón Guardar/Aplicar.

Traffic Class Name:	VoIP
Priority:	High
Protocol:	UDP
Destination IP Address:	81.47.224.0
Destination Subnet Mask:	255.255.252.0

**Paso 3-3:** Seleccione la Interfaz de Tráfico; introduzca la Velocidad Mínima según se indica más abajo, luego haga clic en Guardar.

<b>Traffic Interface Control</b>	
Traffic Interface :	ppp_8_32_1
Minimum Rate :	32 Kbps

**Paso 4-1:** Configurar el Control del Acceso. (Vaya a Administración/Control del Acceso como se indica más abajo).

<b>Management Settings</b> <b>System Log</b> <b>SNMP Agent</b> <b>Internet Time</b> <b>Access Control</b>	FTP	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
	HTTP	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
	ICMP	Enable	<input checked="" type="checkbox"/> Enable
	SNMP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable
	SSH	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable

**Paso 4-2:** Haga una Lista de Control del Servicio según ilustrado más abajo.

Services	LAN	WAN
FTP	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
HTTP	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
ICMP	Enable	<input checked="" type="checkbox"/> Enable
SNMP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable
SSH	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable
TELNET	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
TFTP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable

**Paso 4-3:** Vaya al menu Dirección IP para seleccionar Modo Control del Acceso e introduzca la dirección IP/máscara de subred de las interfaces como se indica más abajo.

<b>SNMP Agent</b> <b>Internet Time</b> <b>Access Control</b> <b>Services</b> <b>IP Addresses</b> <b>Passwords</b>	Access Control Mode: <input type="radio"/> Disable <input checked="" type="radio"/> Enable			
	<b>IP Address</b>	<b>Subnet Mask</b>	<b>Interface</b>	<b>Remove</b>
	193.152.37.192	255.255.255.240	wan	<input type="checkbox"/>
	0.0.0.0	0.0.0.0	lan	<input type="checkbox"/>

**Paso 5:** Seleccione Guardar/Reiniciar en el menu principal para guardar y reinicie el router (como se indica más abajo).

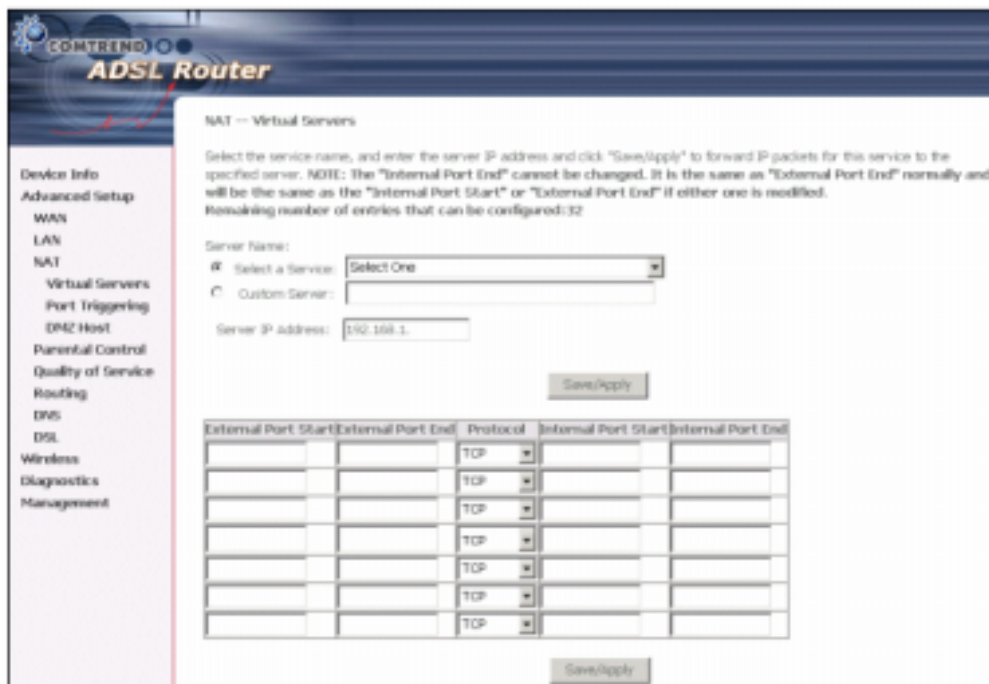
<b>Internet Time</b> <b>Access Control</b> <b>Update Software</b> <b>Save/Reboot</b>	<b>Click the button below to save and reboot the router.</b>	
	<b>Save/Reboot</b>	

## 1.3 Abrir Puertos (Usando Servidores Virtuales)

Los Servidores Virtuales le permiten dirigir el tráfico entrante desde la WAN (identificado por el Protocolo y Puerto Externo) al Servidor Interno con dirección IP privada en el lado de la LAN. El Puerto Interno está requerido sólo si el puerto externo necesita ser convertido en un número diferente de puerto utilizado por el servidor del lado de la LAN. Pueden configurarse un máximo de 32 entradas.



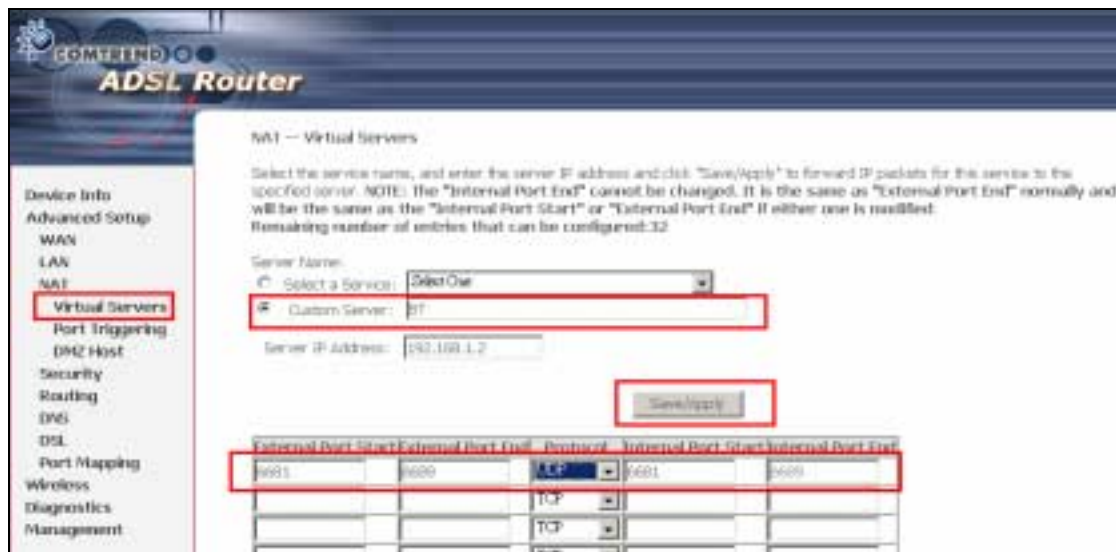
Para añadir un servidor Virtual, simplemente haga clic en el botón Añadir. Se le mostrará lo siguiente:



Seleccione un Servicio O Servidor Personalizado	El usuario tiene que seleccionar un servicio de la lista. O El usuario puede introducir un nombre a su elección.
Dirección IP del Servidor	Introduzca la dirección IP del servidor.
Principio del puerto externo	Introduzca el número de principio del puerto externo (si selecciona Servidor Personalizado). Los rangos del puerto se configuran automáticamente al seleccionar un servicio.
Final del Puerto Externo	Introduzca el número de final del puerto externo (si selecciona Servidor Personalizado). Los rangos del puerto se configuran automáticamente al seleccionar un servicio.
Protocolo	El usuario puede seleccionar entre: TCP, TCP/UDP o UDP.
Comienzo del Puerto Interno	Introduzca el número de comienzo del puerto interno (si selecciona Servidor Personalizado). Los rangos del puerto se configuran automáticamente al seleccionar un servicio.
Final del Puerto Interno	Introduzca el número de final del puerto interno (si selecciona Servidor Personalizado). Los rangos del puerto se configuran automáticamente al seleccionar un servicio.

### 1.3.1 Configurar el puerto NAT según CT-5361

Por ejemplo: configure UDP 6681 a 6689 para el host local 192.168.1.2. Rellene el nombre del servicio en la opción “Servidor Personal” y establezca el rango del puerto UDP. El “Servidor Personalizado” está definido por el usuario. Si el puerto es único, configure puerto Comienzo y Final idénticos.



En el cuadro se muestra una nueva entrada. “Añadir” es para añadir una nueva entrada. Después de hacer clic

en “Añadir” no verá ninguna entrada en la lista de configuración. Por favor configure los ajustes que desea.

#### NAT -- Virtual Servers Setup

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

[Add](#) [Remove](#)

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	Remove
BT	6681	6689	UDP	6681	6689	192.168.1.2	<input type="checkbox"/>

Finalmente, clic en Guardar/Reiniciar para que la Configuración surja efecto.





## 1.4 Inalámbrico

La casilla de diálogo Inalámbrico le permite activar la capacidad inalámbrica, oculta el punto de acceso, configura el nombre de la red inalámbrica y restringe el conjunto de canales.

### 1.4.1 Pantalla Básica de Inalámbrico



La opción Básico le permite configurar las propiedades básicas de la interfaz inalámbrica LAN. Puede activar o desactivar la interfaz LAN, ocultar la red a los escaneos activos, establecer el nombre de la red inalámbrica (también conocida como SSID) y restringir el conjunto de canales en base de los requisitos del país.

Marque la casilla Activar Inalámbrico para activar la opción inalámbrica. Haga clic en **Aplicar** para configurar las opciones básicas de inalámbrico.



<b>Opción</b>	<b>Descripción</b>
Activar Inalámbrico	Una casilla que activa o desactiva la interfaz inalámbrica LAN. Si está seleccionada, la IU Web presenta la configuración del punto Acceso Oculto, de SSID y de País. Como predeterminado está desactivar Inalámbrico.
Ocultar Punto de Acceso	<p>Seleccione Punto de Acceso Oculto para proteger el punto de acceso del router ADSL2+ de ser detectado por los escaneos activos inalámbricos. Si no desea que el punto de acceso sea detectado automáticamente por una estación inalámbrica, chequee esta casilla.</p> <p>La estación no descubrirá este punto de acceso. Para conectar una estación a los puntos de acceso disponibles, la estación tiene que añadir manualmente el nombre de este punto de acceso a su configuración inalámbrica.</p> <p>En Windows XP, vaya a la función Red&gt;Programas para ver todos los puntos de acceso disponibles. También puede utilizar otros programas software como por ej. NetStumbler para ver los puntos de acceso disponibles.</p>
SSID	<p>Configura el nombre de la red inalámbrica. SSID significa Identificador del Conjunto de Servicio. Para acceder a la LAN, todas las estaciones tienen que configurarse con el SSID correcto. Si el SSID no es exacto, al usuario correspondiente no se le permitirá el acceso. (los últimos dos dígitos del SSID corresponden a los últimos dos dígitos de la dirección MAC del equipo)</p> <p>Las convenciones con respecto al nombramiento son: Mínimo es un carácter y el número máximo de caracteres: 32 bytes.</p>
BSSID	BSSID es una identidad de 48 bits utilizada para identificar un BSS (Set Básico de Servicios) dentro de un área. En redes con infraestructura BSS, el BSSID es la dirección CMA (Control Medio del Acceso) del PA (Punto de Acceso) y en redes BSS independientes o ad hoc, el BSSID se genera aleatoriamente.
País	<p>Un menú desplegable que permite configuraciones internacionales y nacionales específicas. Cada país listado en el menú impone regulaciones específicas limitando el rango de canales:</p> <ul style="list-style-type: none"> <li>● US = internacional</li> <li>● Japón=1-14</li> <li>● Jordania= 10-13</li> <li>● Israel= TBD</li> </ul>

## 1.4.2 Seguridad

Las opciones de seguridad incluyen servicios de autenticación y encriptación basados en el algoritmo de la privacidad alámbrica equivalente (PAE). PAE es un conjunto de servicios de seguridad utilizados para proteger redes 802.11 frente a accesos no autorizados, como escuchas o escuchas ocultas; en este caso la captura del tráfico de la red inalámbrica. Si la encriptación de la información está activada, las claves de encriptación compartidas secretas están generadas y utilizadas por la estación origen y la estación destino para modificar los bits de frames, evitando así ser relevadas a través de las escuchas clandestinas.

802.11 soporta dos subtipos de servicios de autenticación de red: sistema abierto y llave compartida. Bajo autenticación de sistema abierto, cualquier estación inalámbrica puede requerir autenticación. El sistema que necesita autenticar con otra estación inalámbrica envía un frame de gestión de la autenticación que contiene la identidad de la estación emisora. La estación receptora envía entonces una frame que indica si reconoce la identidad de la estación emisora.

Bajo autenticación de llave compartida, se asume que cada estación inalámbrica ha recibido una llave secreta compartida a través de un canal seguro independiente del canal de red de comunicaciones inalámbrico 802.11

Al seleccionar Seguridad aparece la siguiente pantalla. La página Seguridad le permite configurar las propiedades de seguridad de la interfaz inalámbrica LAN. Puede configurar el método de autenticación de la red, seleccionar la encriptación de los datos, especificar si se requiere una llave de red para autenticar frente a esta red inalámbrica y especificar el grado de encriptación.

Haga clic en **Aplicar** para configurar las opciones de seguridad inalámbrica.



Opción	Descripción
Autenticación de la red	<p data-bbox="497 237 1348 488">Especifica la autenticación de la red. Si esta casilla está chequeada, especifica que se utilizará una llave de red para autenticar frente la red inalámbrica. Si la casilla Autenticación de Red (modo compartido) no está chequeada (es decir, si se utiliza la autenticación de sistema abierto), no se proporciona ninguna autenticación. La autenticación de sistema abierto realiza sólo verificaciones de identidad.</p> <p data-bbox="497 528 1257 600">Otro tipo de autenticación origina requisitos diferentes de configuración.</p> <p data-bbox="497 640 1342 712">Si elige <b>802.1X</b>, introduzca la dirección IP del servidor RADIUS, el puerto RADIUS y la llave RADIUS.</p> <p data-bbox="497 752 1177 824">Asimismo, active la encriptación WEP y el Grado de Encriptación.</p> <div data-bbox="497 855 1355 1415" style="border: 1px solid black; padding: 5px;"> <p data-bbox="504 878 1027 913">Network Authentication: <input type="text" value="802.1X"/></p> <p data-bbox="504 1034 1158 1070">RADIUS Server IP Address: <input type="text" value="0.0.0.0"/></p> <p data-bbox="504 1088 1158 1124">RADIUS Port: <input type="text" value="1812"/></p> <p data-bbox="504 1142 1158 1178">RADIUS Key: <input type="text"/></p> <p data-bbox="504 1272 1008 1308">WEP Encryption: <input type="text" value="Enabled"/></p> <p data-bbox="504 1361 1342 1397">Encryption Strength: <input type="text" value="128-bit"/> <input type="button" value="Set Encryption Keys"/></p> </div> <p data-bbox="497 1451 1321 1523">Si selecciona <b>WPA</b>, tiene que introducir el intervalo de refresco del grupo WPA.</p> <div data-bbox="497 1527 1181 1993" style="border: 1px solid black; padding: 5px;"> <p data-bbox="513 1550 1040 1585">Network Authentication: <input type="text" value="WPA"/></p> <p data-bbox="513 1657 1174 1693">WPA Group Rekey Interval: <input type="text" value="0"/></p> <p data-bbox="513 1711 1174 1747">RADIUS Server IP Address: <input type="text" value="0.0.0.0"/></p> <p data-bbox="513 1765 1174 1800">RADIUS Port: <input type="text" value="1812"/></p> <p data-bbox="513 1818 1174 1854">RADIUS Key: <input type="text"/></p> <p data-bbox="513 1904 1046 1939">WPA Encryption: <input type="text" value="TKIP"/></p> <p data-bbox="513 1957 1027 1993">WEP Encryption: <input type="text" value="Disabled"/></p> </div>

	<p>Si selecciona <b>WPA-PSK</b>, tiene que introducir la Llave pre-compartida WPA y el intervalo de refresco del grupo WPA.</p> <div data-bbox="496 304 1163 763" style="border: 1px solid black; padding: 5px;"> <p>Network Authentication: <input type="text" value="WPA-PSK"/></p> <p>WPA Pre-Shared Key: <input type="text"/></p> <p>WPA Group Rekey Interval: <input type="text" value="0"/></p>   <p>WPA Encryption: <input type="text" value="TKIP"/></p> <p>WEP Encryption: <input type="text" value="Disabled"/></p> </div>
<p>Encriptado WEP</p>	<p>Especifica que una llave de red está utilizada para encriptar la información enviada a través de la red. Cuando esta casilla está chequeada, activa la codificación de la información y origina el menu desplegable Grado de Encriptado. Encriptado de la Información (WEP activado) y Autenticación de la Red utilizan la misma llave.</p>
<p>Grado de Encriptado</p>	<p>La longitud de la llave de sesión está proporcional con el número de bits binarios comprendiendo el fichero de llave de sesión. Esto significa que las llaves de sesión con un mayor número de bits tienen un grado de seguridad más alto y son considerablemente más difíciles de decodificar por la fuerza. Este menu desplegable define sea una llave de 64 8-bit (5-caracteres o 10-caracteres hexadecimales o una de 128 8-bit (13-caracteres o 10-caracteres). Si establece una llave de mínimo 128 bits, los usuarios que intenten establecer un canal de comunicación seguro con su servidor tienen que utilizar un navegador capaz de comunicar con una llave de sesión de 128 bits.</p> <p>La configuración Grado de Encriptación no se presenta hasta que se chequea la casilla Autenticación de la Red (Modo compartido).</p>

### 1.4.3 Filtro CMA

Esta página del Filtro CMA permite restringir/permitir el acceso en base de una dirección CMA. Todos los NIC tienen una única dirección CMA de 48 bits grabada en el chip ROM o en la tarjeta. Al activar el filtro de direcciones CMA, está restringiendo los NICs que tienen permitida la conexión a su punto de acceso. Por lo tanto, un punto de acceso permitirá el acceso a cualquier ordenador que utilice un NIC cuya dirección CMA figura en su lista de “permitidas”.

Los routers Wi-Fi y los puertos de acceso que soportan filtrado CMA le permiten especificar una lista de direcciones CMA que pueden conectarse al punto de acceso y dictar de este modo qué unidades están autorizadas a acceder a la red inalámbrica. Si una unidad utiliza filtrado CMA, a cualquier dirección no definida explícitamente se le denegará el acceso.

Modo CMA restringido: **Apagado**- desactiva el filtrado CMA; **Permitir**- permite el acceso a las direcciones CMA especificadas; **Impedir**- rechaza el acceso a las direcciones CMA especificadas, luego haga clic en el botón **CONFIGURAR**.

Para eliminar una entrada, seleccione la entrada en la parte inferior de la pantalla y luego haga clic en el botón **Eliminar**, situado en el lado derecho de la pantalla.

Para añadir una entrada CMA, haga clic en **Añadir** e introduzca la dirección CMA



Después de elegir el botón Añadir, aparece la siguiente pantalla. Introduzca la dirección CMA y haga clic en **Aplicar** para añadir la dirección CMA a los filtros de direcciones CMA inalámbricas.



Opción	Descripción
Modo CMA restringido	Botones radio que permiten la configuración de: Apagado: la función de filtrado CMA está desactivada. Permitir: Permiten a los ordenadores con direcciones CMA listadas que se conecten al punto de acceso. Impedir: Impide que los ordenadores con CMA listadas se conecten al punto de acceso.
Dirección CMA	Lista as direcciones CMA sujetas a ordenes de Apagar Permitir o Impedir. El botón Añadir origina un campo de entrada que le requiere que teclee una dirección CMA en una convención de dos-caracteres y 6-bytes xx:xx:xx:xx:xx:xx donde xx son números hexadecimales. El número máximo de direcciones CMA que pueden añadirse es 60.

## 1.4.4 Puente Inalámbrico

Esta página le permite configurar las propiedades del puente inalámbrico de la interfaz de la LAN inalámbrica. Puede seleccionar Puente Inalámbrica (también conocida como Sistema de Distribución Inalámbrica) para desactivar la función del punto de acceso. Seleccionar Punto de Acceso activa el funcionamiento del punto de acceso. La función Puente Inalámbrico seguirá siendo disponible y las estaciones inalámbricas podrán asociarse al PA. Seleccionar Desactivar en Restringir Puente desactivará la restricción del puente inalámbrico. El acceso será concedido a cualquier puente inalámbrico. Seleccionar Activado o Activado (Scan) activa la restricción del puente. El acceso se concederá sólo a aquellos puentes seleccionados en Puentes Remotos.



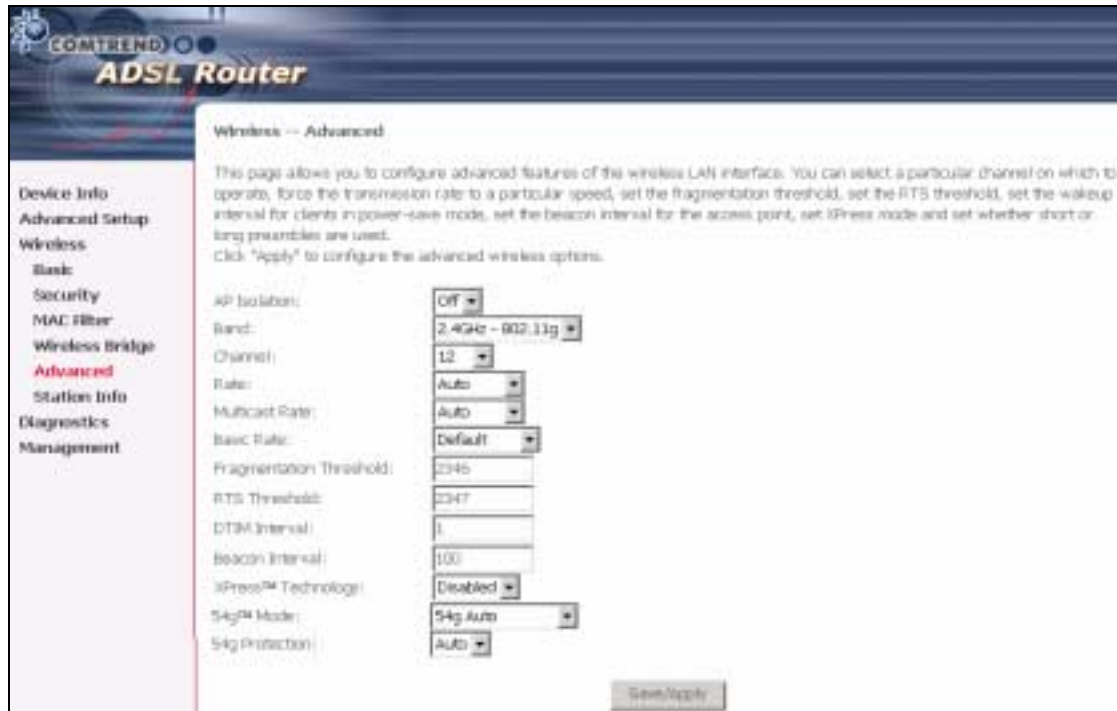
Opción	Descripción
Modo AP	Punto de Acceso Puente Inalámbrico
Restringir Puente	Activado Activado (Scan) Desactivado



## 1.4.5 Avanzado

La página Avanzado le permite configurar las propiedades avanzadas de la interfaz inalámbrica LAN. Puede seleccionar un cierto canal en el cual operar, forzar la velocidad de transmisión a un cierto ritmo, definir el umbral de fragmentación, definir el límite de RTS, ajustar el intervalo de despertar de los clientes en el modo de ahorro de energía, definir un intervalo beacon para el punto de acceso y determinar si se utilizan preámbulos cortos o largos.

Haga clic en **Aplicar** para configurar las opciones avanzadas de inalámbrico.



Opción	Descripción
Aislamiento PA	Seleccionar Encendido o Apagado. Activando esta propiedad, los clientes inalámbricos asociados al Punto de Acceso podrán interconectarse.
Banda	La nueva enmienda permite a las unidades IEEE 802.11g recurrir a velocidades de 11 Mbps, así que en la misma red pueden coexistir unidades IEEE 802.11b y IEEE 802.11g. Los dos estándares se aplican a la banda de frecuencia de 2.4 GHz. IEEE 802.11g crea paridad de datos-tasa de 2.4 GHz con IEEE 802.11a estándar, cual tiene una velocidad de 54 Mbps a 5 GHz. (IEEE 802.11a presenta otras diferencias comparado con IEEE 802.11b o g, como por ejemplo que ofrece más canales.)
Canal	Menu desplegable que permite seleccionar un canal específico
Velocidad	Menu desplegable que especifica las siguientes velocidades fijadas: Auto: Predefinida. Utiliza una velocidad de datos de 11

	<p>Mbps cuando es posible, pero salta a velocidades más bajas si es necesario.</p> <p>Velocidades fijadas de 1 Mbps, 2Mbps, 5Mbps, o 11Mbps. El ajuste adecuado depende de la fuerza de la señal.</p>
Multicast Rate	Setting multicast packet transmit rate
Velocidad Básica	Configurar la velocidad básica de transmisión
Umbral de Fragmentación	<p>Un umbral, especificado en bytes, que determina si los paquetes serán fragmentados y en qué tamaño. En una WLAN 802.11, los paquetes que exceden el umbral de fragmentación se fragmentan, es decir se dividen en unidades más pequeñas, adecuadas al tamaño del circuito. Los paquetes más pequeños que el valor especificado del umbral de fragmentación no serán fragmentados.</p> <p>Introduzca un valor entre 256 y 2346.</p> <p>Si experimenta una cuota alta de error de paquete, intente aumentar ligeramente su Umbral de Fragmentación. El valor tendría que permanecer a su configuración predefinida de 2346. Configurar el Umbral de Fragmentación demasiado bajo tiene como resultado un rendimiento bajo.</p>
Umbral RTS	<p>Requerir Enviar, cuando está definido en bytes, especifica el tamaño de paquete a partir del cual la Tarjeta WLAN invoca su mecanismo RTS/CTS. Los paquetes que exceden el umbral RTS especificado hacen funcionar el mecanismo RTS/CTS. El NIC transmite paquetes pequeños sin utilizar RTS/CTS. La configuración predefinida de 2347 (longitud máxima) desactiva el umbral RTS.</p>
Intervalo DTIM	<p>Delivery Traffic Indication Message (DTIM), conocido también como Velocidad Beacon. El intervalo de entrada es un valor entre 1 y 65535. Un DTIM es una cuenta atrás informando a los clientes de la siguiente ventana para escuchar mensajes emitidos y múltiples. Cuando el PA ha memorizado mensajes emitidos o múltiples para los clientes asociados, envía el siguiente DTIM con un valor de Intervalo DTIM. Los clientes del PA escuchan las balizas y despiertan para recibir los mensajes emitidos y múltiples. El predefinido es 100.</p>
Intervalo Beacon	<p>El intervalo de tiempo entre las transmisiones de balizas. Cada transmisión de baliza identifica la presencia de un punto de acceso. Por defecto, los NICs radio escanean pasivamente todos los canales RF y escuchan las balizas proviniendo del punto de acceso para encontrar un punto de acceso adecuado.</p> <p>Antes de que una estación entre en el modo de ahorro de energía, la estación necesita el intervalo de balizas para saber cuándo despertar para recibir la baliza (y saber si hay frames memorizadas en el punto de acceso).</p> <p>El valor introducido está representado en ms. Por defecto es 100. Un intervalo de entrada aceptable es de 1 a 0xffff (65535)</p>

Tecnología Xpress <sup>TM</sup>	Tecnología Xpress cumple con las especificaciones redactadas de los estándares de la industria inalámbrica de dos planos.
Extensión Media Inalámbrica	Proporciona una solución CS intermedia para redes 802.11 hasta la emisión de 802.11e. WRAP (Wireless Robust Authenticated Protocol). Un protocolo de encriptación en el estándar 802.11. WRAP está basado en el modo de Libro de Códigos Offset (LCO) de AES. WRAP está sustituido por CCMP.
Modo 54g <sup>TM</sup>	Seleccione el modo 54g Auto para la mayor compatibilidad. Seleccione el modo a Rendimiento 54g para un rendimiento más rápido entre equipos certificados 54g. Configure el modo a 54g LRS si experimenta dificultades con las herramientas del legado 802.11b.
Protección 54g	En modo Auto el router utilizará RTS/CTS para aumentar el rendimiento de 802.11g en redes mixtas 802.11g/802.11b. Apague la protección para maximizar la capacidad de procesamiento de 802.11g. en la mayoría de las condiciones.
Tipo de preámbulo	Menu desplegable que permite seleccionar largo o corto. El preámbulo define la longitud del bloque CRC para la comunicación entre el punto de acceso y la tarjeta de roaming. Las áreas de tráfico de red elevado tendrían que utilizar el tipo de preámbulo corto. El predefinido es el largo.

#### 1.4.6 Información sobre Estaciones

Esta página presenta las estaciones inalámbricas autenticadas y su estado.



BSSID	BSSID es una identidad de 48 bits utilizada para identificar un CBS (Conjunto Básico de Servicios) dentro de un área. En redes con infraestructura BSS, el BSSID es la dirección CMA (Control Medio del Acceso) del PA (Punto de Acceso) y en redes BSS independientes o ad hoc, el BSSID se genera aleatoriamente.
Asociado	Lista todas las estaciones asociadas al Punto De Acceso, junto con el intervalo de tiempo desde que los paquetes han sido transferidos hasta y desde cada estación. Si una estación está inactiva demasiado tiempo, se elimina de la lista.
Autorizado	Lista las unidades con acceso autorizado

## 1.5 Guardar y Reiniciar

Las opciones Guardar/Reiniciar guardan y reinician el router. Cierre la ventana Configuración del Router ADSL y espere 2 minutos antes de abrir su explorador web. Si es necesario, reconfigure la dirección IP de su ordenador para que concuerde con su nueva configuración.



## 1.6 Actualizar el software

La pantalla Actualizar Software le permite obtener de su PSI un fichero de imagen de software actualizado. Las actualizaciones manuales desde un fichero archivado local pueden efectuarse a través de la siguiente pantalla.



**Paso 1:** Obtenga de su PSI un fichero de imagen del software actualizado.

**Paso 2:** Introduzca la ruta de la ubicación del fichero de imagen en la casilla de debajo o haga clic en el botón **Examinar** para localizar el fichero de imagen.

**Paso 3:** Haga clic una vez en el botón “Actualizar Software” para cargar el nuevo fichero de imagen.

**NOTA:** El proceso de actualización necesita unos 2 minutos para completarse y su Router ADSL se reiniciará.