

CT-5365

Router Inalámbrico ADSL2+

Guía de Configuración Rápida

Versión Spa-1, 15 de junio de 2009.



261094-002

Prefacio

Este manual facilita información relativa a la configuración rápida del CT5365.

Al usuario que lea este manual se le supone cierta comprensión básica de terminología y conceptos en telecomunicaciones.

Si su producto está inoperativo o funciona incorrectamente, puede contactar con el servicio de soporte técnico en la dirección de correo INT-support@comtrend.com

Para actualizaciones, nuevos productos, revisión de manuales o actualizaciones de software, por favor visite <http://www.comtrend.com>

Instrucciones de seguridad.

Con la guía de desembalaje, instalación, uso y mantenimiento de su dispositivo eléctrico, son recomendadas las siguientes directrices:

- No usar o instalar este producto cerca del agua, alejar de Fuentes de fuego y alejar de zona de golpes. Por ejemplo, cerca de una bañera, lavadora, fuego de cocina o cerca de una piscina. Se recomienda no exponer el producto a rayos ni a zonas húmedas.
- No conectar la fuente de alimentación eléctrica en superficies elevadas. Impedir conectarlas al aire libre. No se deben colocar objetos pesado sobre el cable eléctrico. Se debe impedir pisar, caminar o maltratar el cable.
- Use únicamente la fuente de alimentación eléctrica suministrada con el CT5365.
- Salvaguarde el producto de sobrecalentamientos, asegúrese que todas las aberturas de ventilación no están bloqueadas.
- No usar el Teléfono durante una tormenta eléctrica. Existe el riesgo de descarga eléctrica producida por un rayo. Debe impedir usar el teléfono en una fuga de gas o en sus inmediaciones.
- Nunca instalar el cable telefónico durante unas condiciones meteorológicas adversas.

PRECAUCION:

- Para reducir el riesgo de fuego, use sólo cable de telecomunicaciones AWG nº 26 o superior
- Desconecte siempre todas las líneas telefónicas y de corriente eléctrica antes de realizar un mantenimiento o reparación del producto.



PELIGRO

- Desconecte la fuente de alimentación del dispositivo antes de la prestación de servicio.

- Las especificaciones de la fuente de alimentación están detalladas en el Anexo C de la Guía de Usuario.

Copyright

Copyright© 2009 Comtrend Corporation. Todos los derechos reservados. La información aquí contenida es propiedad de Comtrend Corporation. No está permitida la traducción, transcripción, reproducción, de ninguna forma, y por ningún medio sin el consentimiento previo por escrito de Comtrend Corporation.

NOTA: Este documento está sujeto a cambios sin previo aviso.

Protección de Medio Ambiente

	Este símbolo indica que cuando el equipo ha llegado al final de su vida útil, debe ser llevado a un centro de reciclado y procesado por separado de residuos domésticos.
---	---

La caja de cartón, el plástico contenido en el embalaje, y piezas componentes del router pueden ser recicladas de acuerdo con las regulaciones vigentes.

No mezclar los residuos de este componente eléctrico con los residuos domésticos.

Infringir esta regulación supone estar sujeto a penas o sanciones.

Solicite las instrucciones de eliminación de residuos a su gobierno municipal.

1. INTRODUCCIÓN.....6

2. CAMBIAR CONTRASEÑA.....6

3. CONFIGURACIÓN DEL ROUTER.....7

3.1 CONFIGURACIÓN MULTIPUESTO DINÁMICA7

3.1.1: *Configurar el puerto WAN (DSL)*.....7

3.1.2: *Configurar los parámetros de la LAN*.....9

3.1.3: *Configurar el Control del Acceso*.....10

3.2 CONFIGURACIÓN MULTIPUESTO ESTÁTICO12

3.2.1: *Configurar el puerto WAN (DSL)*.....12

3.2.3: *Configurar el puerto LAN*.....16

3.2.4: *Configurar el Control del Acceso*.....17

3.3 CONFIGURACIÓN MONOPUESTO DINÁMICO (BRIDGE).....18

3.3.1: *Configurar el puerto WAN (DSL)*.....18

3.3.2: *Configurar los parámetros de la LAN*.....21

3.3.3: *Configurar el Control del Acceso*.....21

3.4 CONFIGURACIÓN MONOPUESTO ESTÁTICO (IPOA)23

3.4.1: *Configurar el puerto WAN*23

3.4.2: *Configurar los parámetros de la LAN*.....25

3.4.3: *Configurar el Control del Acceso*.....25

3.5 ABRIR PUERTOS (USANDO SERVIDORES VIRTUALES)27

3.5.1: *Servidores Virtuales*.....27

3.5.2: *Ejemplo de configuración de un Virtual Server*28

3.6 INALÁMBRICO29

3.6.1: *Pantalla Básica de Inalámbrico*.....29

3.6.2: *Seguridad inalámbrica*.....31

3.6.3: *Filtrado MAC*.....36

3.6.5: *Avanzado*37

3.6.6: *Información sobre Estaciones*40

3.7 SALVAR Y REINICIAR41

3.8 ACTUALIZAR EL SOFTWARE41

1. Introducción

Este documento es una guía de referencia rápida para configurar el router ADSL/ADSL2+ Comtrend CT-5365, suministrado con el *Kit ADSL Router Inalámbrico* de Telefónica, a través del configurador web que este equipo incorpora.

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 de forma rápida 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 Microsoft Windows. Se recomienda utilizar preferente y preferiblemente el asistente.

NOTA: 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.

2. Cambiar Contraseña

Por motivos de seguridad se recomienda cambiar la password o contraseña por defecto del usuario “1234”.

La opción “**Passwords**” permite realizar la configuración de las contraseñas de acceso al router. El acceso a su router ADSL2+ está controlado por medio de la cuenta de usuario: “1234”. El usuario “1234” tiene acceso ilimitado para cambiar y ver la configuración de su router ADSL. Los parámetros de fábrica o por defecto son:

- Nombre de usuario: 1234
- Contraseña por defecto o de fábrica: 1234

Utilice los campos siguientes para introducir hasta 16 caracteres y haga clic en “**Save/Apply**” para cambiar o crear contraseñas.



Para realizar el cambio de contraseña siga los siguientes pasos;

1. Seleccione el usuario al que desea cambiar la contraseña en el campo **“Username”**
2. introduzca la contraseña actual en el campo **“Old Password”**
3. introduzca la nueva contraseña en el campo **“ New Password”**
4. y confirme la nueva contraseña introduciéndola de nuevo en el campo **“Confirm Password”**
5. Luego haga clic en el botón **“Save/Apply”**.
6. Tenga en cuenta que al cambiar la contraseña de acceso es necesario reiniciar el CT-5365 para que el cambio tenga efecto.
 - a. Para reiniciar el Router, seleccione en el menú principal la opción **“Management”**
 - b. Seleccione la opción **“Save/Reboot”**
 - c. Haga clic en el botón **“Save/Reboot”**
 - d. Espere a que el router se inicie de nuevo y utilice la nueva contraseña o password del usuario **“1234”**.

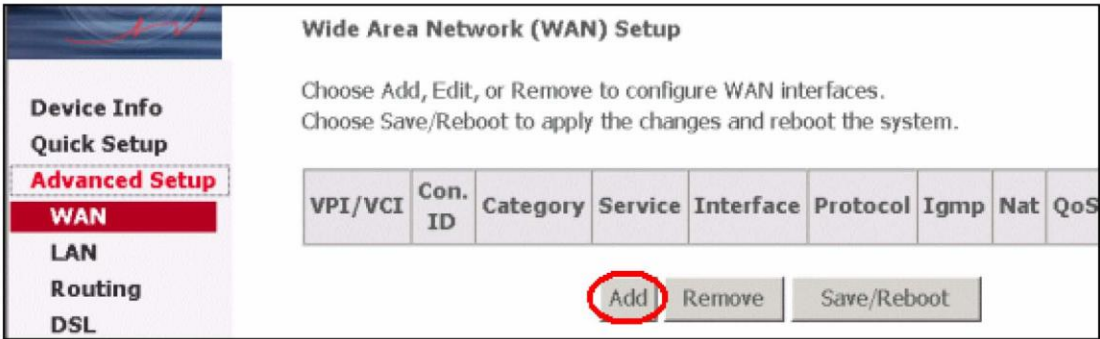
3. Configuración del Router

Por defecto su router se encuentra configurado con los parámetros adecuados para un correcto funcionamiento en las líneas ADSL de Telefónica si su acceso a internet se realiza a través de una configuración Multipuesto Dinámica.

3.1 Configuración Multipuesto Dinámica

3.1.1: Configurar el puerto WAN (DSL).

3.2.2.1 Haga clic en el menú **“Advanced Setup > WAN”**. Haga clic en el botón **“Add”** para crear una interfaz WAN)



3.2.2.2 Introduzca los valores VPI/VCI;

3.2.2.3 Seleccione **“Enable Quality Of service”**; active Calidad de Servicio marcando la casilla **“Enable Quality Of Service”**.

Haga clic en el botón **“Next”**.

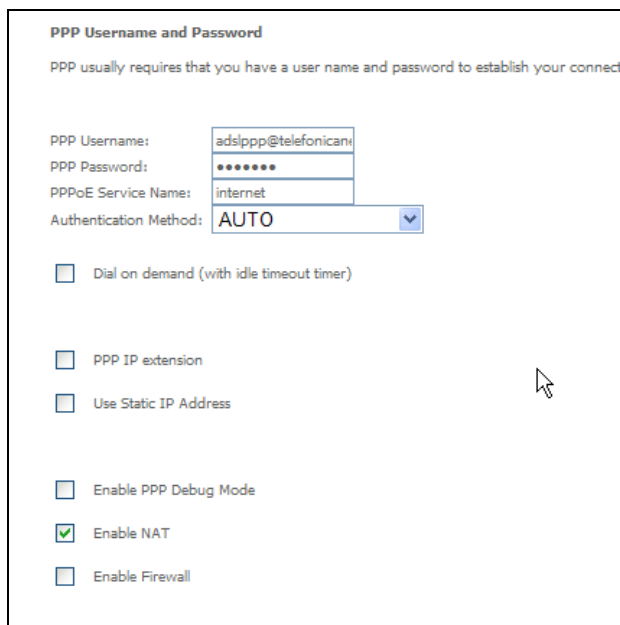
3.2.2.4 Seleccione **“PPP over Ethernet (PPPoE)”**; seleccione **“LLC/SNAP – BRIDGING”** como **“Encapsulation Mode”**

Haga clic en el botón **“Next”**

3.2.2.5 Introduzca el nombre de usuario y Contraseña del servicio PPP que encontrará en la carta con la información de usuario que le ha enviado Telefónica.

Seleccione **“AUTO”** como **“Authentication Method”**

Active NAT marcando la casilla **“Enable NAT”**

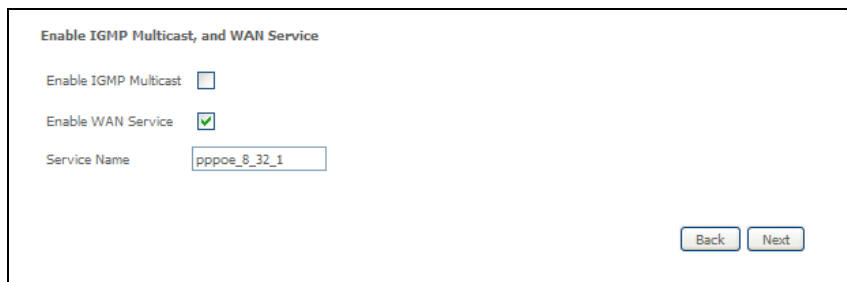


The screenshot shows a configuration window titled "PPP Username and Password". Below the title is a note: "PPP usually requires that you have a user name and password to establish your connect". The form contains the following fields and options:

- PPP Username:
- PPP Password:
- PPPoE Service Name:
- Authentication Method: (dropdown menu)
- ☐ Dial on demand (with idle timeout timer)
- ☐ PPP IP extension
- ☐ Use Static IP Address
- ☐ Enable PPP Debug Mode
- ☒ Enable NAT
- ☐ Enable Firewall

Haga clic en el botón **“Next”**.

3.2.2.6 Seleccione **“Enable WAN Service”**.



The screenshot shows a configuration window titled "Enable IGMP Multicast, and WAN Service". The form contains the following fields and options:

- Enable IGMP Multicast: ☐
- Enable WAN Service: ☒
- Service Name:

At the bottom right, there are two buttons: "Back" and "Next".

Haga clic en el botón **“Next”**.

3.2.2.7 Se mostrará en pantalla un resumen de la configuración introducida. Haga clic en el botón **“Save”** para confirmar la configuración o pulse el botón **“Back”** para corregir la configuración.

3.2.2.8 Una vez realizada la configuración de forma correcta, haga clic en el botón **“Save/Reboot”**.

3.1.2: Configurar los parámetros de la LAN.

3.1.2.1 Seleccione el menú **“Advanced Setup > LAN”**

3.1.2.2 Introduzca la dirección IP en el campo “**IP address**” y la máscara de subred en el campo “**Subnet Mask**”;

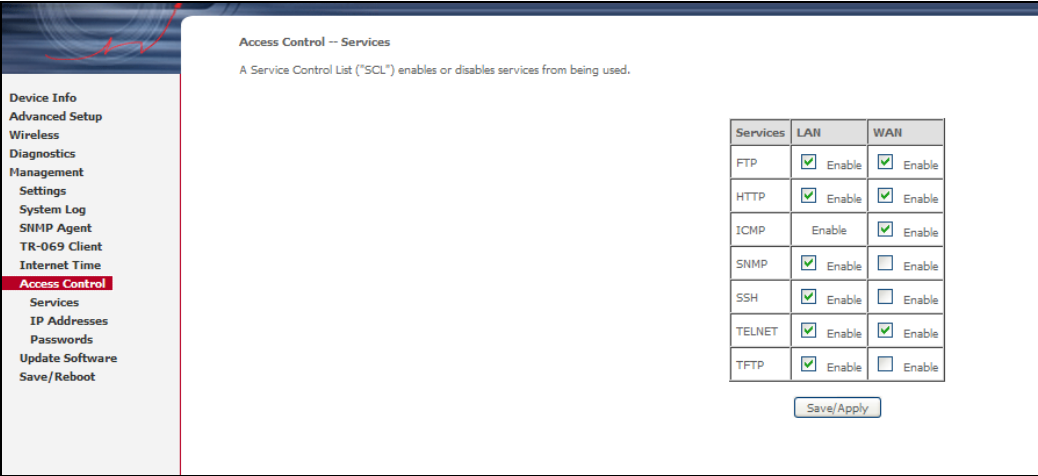
3.1.2.3 Si lo desea puede cambiar la dirección de Loopback, para ello introduzca la dirección IP y la máscara de subred de Loopback en el apartado “**loopback IP and Subnetmask**”;

3.1.2.4 Active el servidor DHCP marcando la casilla de verificación “**Enable DHCP Server**” e indique el rango de asignación de dirección IP introduciendo una dirección IP de inicio de rango y otra dirección de final de rango. También debe introducir el tiempo máximo de asignación de dirección IP por MAC.

3.1.2.5 Haga clic en el botón “**Save**”. O si lo prefiere en el botón “**Save/Reboot**”.

3.1.3: Configurar el Control del Acceso.

3.1.3.1 Seleccione “**Management > Access Control**”. En esta opción se le mostrará los servicios en los que tiene opción de permitir o restringir el acceso a la gestión del router.



3.1.3.2 Marque las casillas del “**Service Control Access List**” que desea permitir por el interfaz WAN o por el interfaz LAN.

Services	LAN	WAN
FTP	☒ Enable	☒ Enable
HTTP	☒ Enable	☒ Enable
ICMP	☐ Enable	☒ Enable
SNMP	☒ Enable	☐ Enable
SSH	☒ Enable	☐ Enable
TELNET	☒ Enable	☒ Enable
TFTP	☒ Enable	☐ Enable

3.1.3.3 Para realizar una gestión de direccionamiento IP a los servicios permitidos, seleccione “**IP Address**” del menú “**Access Control**”, Active el “**Modo de Control del Acceso**” marcando la casilla “**Enable**”

Access Control Mode: ☐ Disable ☒ Enable

IP Address	Subnet Mask	Interface	Remove

3.1.3.4 Para añadir una dirección IP que tenga permiso de acceso, haga clic en el botón “**Add**”.

3.1.3.5 Introduzca la dirección IP que tendrá permiso de gestión en el campo “**IP Address**”, introduzca la máscara de subred en el campo “**Subnet Mask**”, y seleccione el interfaz por el que esa dirección IP tendrá acceso a su router.

Access Control

Enter the IP address of the management station permitted to access the local management services, and click 'Save/Apply.'

IP Address	Subnet Mask	Interface
		none lan wan lan&wan

Save/Apply

3.1.3.6 Haga clic en el botón “**Save/Apply**”.

3.2 Configuración Multipuerto Estático

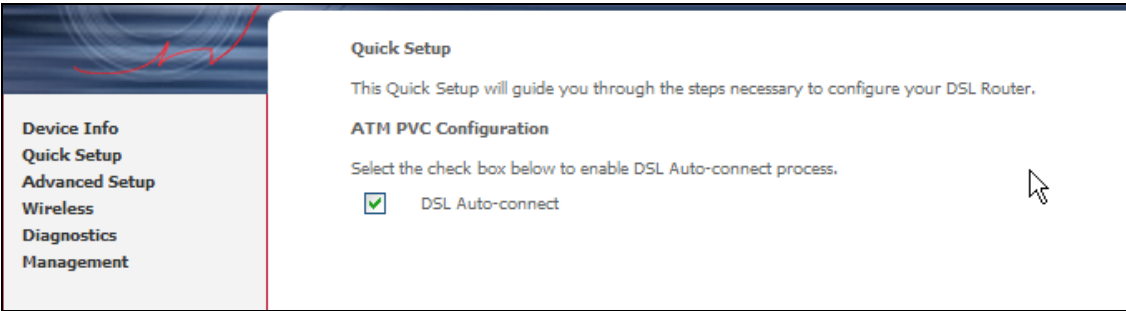
Para hacer uso de esta configuración su router **no** debe tener definido ningún perfil VCI/VPI en el menú “**Advanced Setup > WAN**”.

3.2.1: Configurar el puerto WAN (DSL).

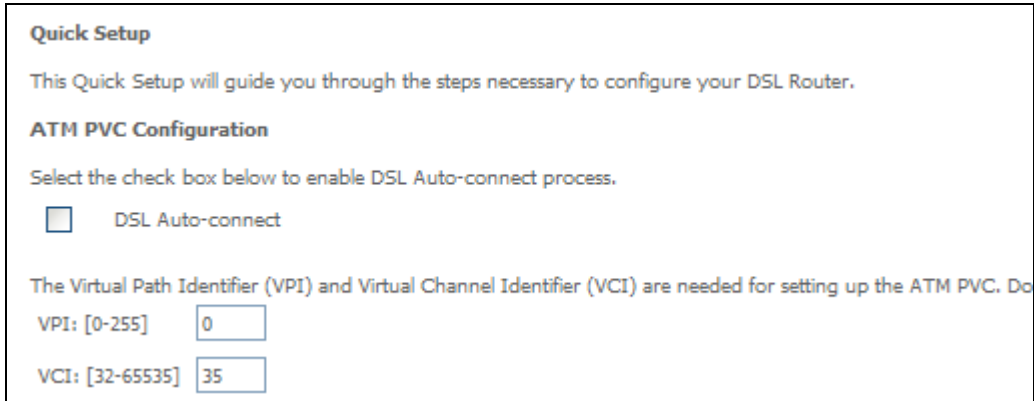
Seleccione “**Advanced Setup > WAN**” o la opción “**Quick Setup**” si se muestra en el menú principal; haga clic en el botón “**Add**” para crear una interfaz WAN.

Si ha seleccionado la opción “**Quick Setup**”, siga los apartados descritos a continuación, si ha seleccionado la opción “**Advanced Setup > WAN**” siga en la página 14.

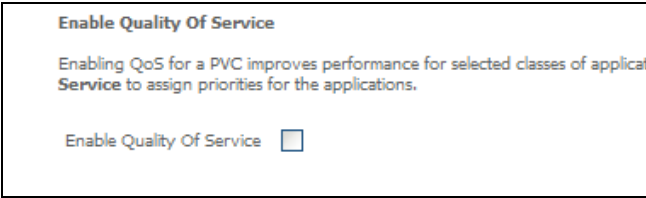
Quick Setup:



3.2.1.1 Desmarque la casilla “**DSL Auto-Connect**” e introduzca los valores VPI/VCI;



3.2.1.2 Active la casilla Calidad del Servicio marcando “**Enable Quality of Service**”.



Haga clic en el botón “**Next**”.

3.2.1.3 Seleccione la opción “**IP over ATM (IPoA)**”; seleccione “**LLC/SNAP – BRIDGING**” como “**Encapsulation Mode**”.

Connection Type

Select the type of network protocol and encapsulation

☐ PPP over ATM (PPPoA)

☐ PPP over Ethernet (PPPoE)

☐ MAC Encapsulation Routing (MER)

☒ IP over ATM (IPoA)

☐ Bridging

Encapsulation Mode

LLC/SNAP-ROUTING

Haga clic en el botón **“Next”**.

3.2.1.4 Introduzca la dirección IP pública **“(WAN IP Address)”** y Máscara de subred **“(WAN Subnet Mask)”** facilitada por su proveedor de acceso a Internet.

WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.

Notice: DHCP is not supported in IPoA mode. Changing the default gateway or the

WAN IP Address: 172.23.25.3

WAN Subnet Mask: 255.255.255.248

3.2.1.5 Marque la casilla **“Use the following default Gateway”** y marque la casilla **“Use WAN Interface”**.

☒ Use the following default gateway:

☐ Use IP Address:

☒ Use WAN Interface: ipoa_8_36/ipa_8_36

3.2.1.6 Marque la casilla **“Use the following DNS server addresses”** e introduzca las direcciones del servidor DSN primario y secundario.

☒ Use the following DNS server addresses:

Primary DNS server: 80.58.61.250

Secondary DNS server: 80.58.61.254

Haga clic en el botón **“Next”**.

Nota: Si su proveedor de acceso a Internet es Telefónica, encontrará todos estos datos en la carta que le suministra Telefónica junto a la información de usuario.

3.2.1.7 Marque la casilla de verificación **“Enable NAT”** y **“Enable WAN Service”**; desmarque la casilla **“Enable Firewall”** y **“Enable IGMP Multicast”**.

Enable NAT☒

Enable Firewall☐

Enable IGMP Multicast, and WAN Service

Enable IGMP Multicast☐

Enable WAN Service☒

Service Name:

Haga clic en el botón “Next”.

3.2.1.8 A continuación se le indicará como configurar la LAN de su router,

Device Setup

Configure the DSL Router IP Address and Subnet Mask for LAN interface.

IP Address:

192.168.1.1

Subnet Mask:

255.255.255.0

☐ Disable DHCP Server

☒ Enable DHCP Server

Start IP Address:

192.168.1.33

End IP Address:

192.168.1.254

Leased Time (hour):

24

Haga clic en el botón “Next” para continuar.

3.2.1.9 A continuación se le indicará como configurar la WLAN o acceso inalámbrico de su router. Por defecto está desactiva. Para activarla marque la casilla de verificación “Enable Wireless”

Wireless -- Setup

Enable Wireless☒

Enter the wireless network name (also known as SSID).

SSID:

WLAN_EF2C

Haga clic en el botón “Next” para continuar.

3.2.1.10 Se mostrará en pantalla un resumen de la configuración introducida. Haga clic en el botón “Save/Reboot” para confirmar la configuración o pulse el botón “Back” para corregir la configuración.

Advanced Setup > WAN:

Device Info

Quick Setup

Advanced Setup

WAN

LAN

Routing

DSL

Vendor Class ID

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	VlanId	State	Remove	Edit
Add Remove Save/Reboot												

3.2.2.1 Haga clic en el menú “**Advanced Setup > WAN**”. Haga clic en el botón “**Add**” para crear una interfaz WAN.

3.2.2.2 Introduzca los valores VPI/VCI;

ATM PVC Configuration

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

VPI: [0-255]

8

VCI: [32-65535]

36

Service Category:

UBR Without PCR

3.2.2.3 Active la casilla Calidad del Servicio marcando la casilla de verificación “**Enable Quality of Service**”.

Enable Quality Of Service

Enabling QoS for a PVC improves performance for selected classes of application Service to assign priorities for the applications.

Enable Quality Of Service

☐

Haga clic en el botón “**Next**”.

3.2.2.4 Seleccione la opción “**IP over ATM (IPoA)**”; seleccione “**LLC/SNAP – BRIDGING**” como “**Encapsulation Mode**”

Connection Type

Select the type of network protocol and encapsulation.

☐ PPP over ATM (PPPoA)

☐ PPP over Ethernet (PPPoE)

☐ MAC Encapsulation Routing (MER)

☒ IP over ATM (IPoA)

☐ Bridging

Encapsulation Mode

LLC/SNAP-ROUTING

Haga clic en el botón “**Next**”.

3.2.2.5 Introduzca la dirección IP pública “(**WAN IP Address**)” y Máscara de subred “(**WAN Subnet Mask**)” facilitada por su proveedor de acceso a Internet.

WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.

Notice: DHCP is not supported in IPoA mode. Changing the default gateway or the

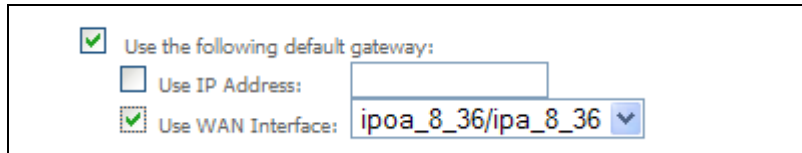
WAN IP Address:

172.23.25.3

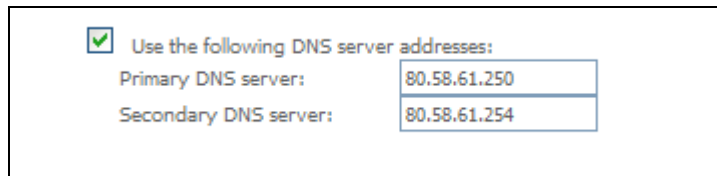
WAN Subnet Mask:

255.255.255.248

3.2.2.6 Marque la casilla de verificación **“Use the following default Gateway”** y marque la casilla **“Use WAN Interface”**.



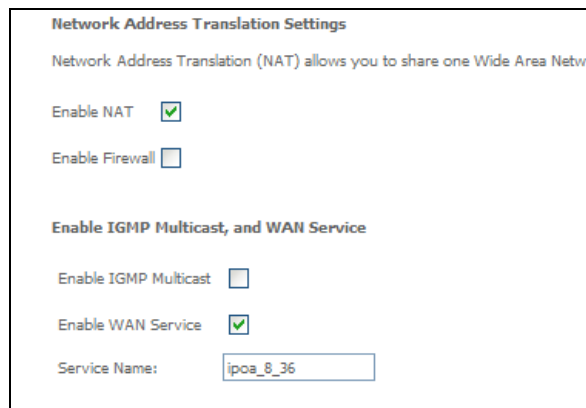
3.2.2.7 Marque la casilla de verificación **“Use the following DNS server addresses”** e introduzca las direcciones del servidor DSN primario y secundario.



Haga clic en el botón **“Next”**.

Nota: Si su proveedor de acceso a Internet es Telefónica, encontrará todos estos datos en la carta que le suministra Telefónica junto a la información de usuario.

3.2.2.8 Marque la casilla de verificación **“Enable NAT”** y **“Enable WAN Service”**; desmarque la casilla **“Enable Firewall”** y **“Enable IGMP Multicast”**.



Haga clic en el botón **“Next”**.

3.2.2.9 Se mostrará en pantalla un resumen de la configuración introducida. Haga clic en el botón **“Save”** para confirmar la configuración o pulse el botón **“Back”** para corregir la configuración.

3.2.2.10 Una vez realizada la configuración, haga clic en el botón **“Save/Reboot”**.

3.2.3: Configurar el puerto LAN.

3.2.3.1 Seleccione el menú **“Advanced Setup > LAN”**

Device Info
Advanced Setup
WAN
LAN
NAT
Parental Control
Quality of Service
Routing
DNS
DSL

Local Area Network (LAN) Setup

Configure the DSL Router IP Address and Subnet Mask for LAN in configuration effective.

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Loopback IP and Subnetmask

IP Address: 127.0.0.1

Subnetmask: 255.0.0.0

☐ Enable UPnP

3.2.3.2 Introduzca la dirección IP en el campo “**IP address**” y la máscara de subred en el campo “**Subnet Mask**”;

3.2.3.3 Si lo desea puede cambiar la dirección de loopback, para ello introduzca la dirección IP y la máscara de subred de Loopback en el apartado “**loopback IP and Subnetmask**”;

Loopback IP and Subnetmask

IP Address: 127.0.0.1

Subnetmask: 255.0.0.0

3.2.3.4 Active el servidor DHCP marcando la casilla “**Enable DHCP Server**” e indique el rango de asignación de dirección IP introduciendo una dirección IP de inicio y otra dirección de final. También debe introducir el tiempo máximo de asignación de dirección IP por MAC.

☐ Disable DHCP Server
☒ Enable DHCP Server

Start IP Address: 192.168.1.33

End IP Address: 192.168.1.254

Leased Time (hour): 24

3.2.3.5 Haga clic en el botón “**Save**”. O si lo prefiere en el botón “**Save/Reboot**”.

3.2.4: Configurar el Control del Acceso.

3.2.4.1 Seleccione “**Management > Access Control**”. En esta opción se le mostrará los servicios en los que tiene opción de permitir o restringir el acceso

Device Info
Advanced Setup
Wireless
Diagnostics
Management
Settings
System Log
SNMP Agent
TR-069 Client
Internet Time
Access Control
Services
IP Addresses
Passwords
Update Software
Save/Reboot

Access Control -- Services

A Service Control List ("SCL") enables or disables services from being used.

Services	LAN	WAN
FTP	☒ Enable	☒ Enable
HTTP	☒ Enable	☒ Enable
ICMP	☒ Enable	☒ Enable
SNMP	☒ Enable	☐ Enable
SSH	☒ Enable	☐ Enable
TELNET	☒ Enable	☒ Enable
TFTP	☒ Enable	☐ Enable

Save/Apply

3.2.4.2 Marque las casillas del **“Service Control Access List”** que desea permitir por el interfaz WAN o por el interfaz LAN.

Services	LAN	WAN
FTP	☒ Enable	☒ Enable
HTTP	☒ Enable	☒ Enable
ICMP	☐ Enable	☒ Enable
SNMP	☒ Enable	☐ Enable
SSH	☒ Enable	☐ Enable
TELNET	☒ Enable	☒ Enable
TFTP	☒ Enable	☐ Enable

3.2.4.3 Para realizar una gestión de direccionamiento IP a los servicios permitidos, seleccione **“IP Address”** del menú **“Access Control”**, Active el **“Modo de Control del Acceso”** marcando la casilla **“Enable”**

Access Control Mode: ☐ Disable ☒ Enable

IP Address	Subnet Mask	Interface	Remove

3.2.4.4 Para añadir una dirección IP que tenga permiso de acceso, haga clic en el botón **“Add”**.

3.2.4.5 Introduzca la dirección IP que tendrá permiso de gestión en el campo **“IP Address”**, introduzca la máscara de subred en el campo **“Subnet Mask”** , y seleccione el interfaz por el que esa dirección IP tendrá acceso a su router.

Access Control

Enter the IP address of the management station permitted to access the local management services, and click 'Save/Apply.'

IP Address	Subnet Mask	Interface
		none lan wan lan&wan

Save/Apply

3.2.4.6 Haga clic en el botón **“Save/Apply”**.

3.3 Configuración Monopuesto Dinámico (Bridge)

3.3.1: Configurar el puerto WAN (DSL).

3.3.1.1 Haga clic en el menú **“Advanced Setup > WAN”**. Haga clic en el botón **“Add”** para crear una interfaz WAN)

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
Add Remove Save/Reboot								

3.3.1.2 Introduzca los valores VPI/VCI;

ATM PVC Configuration
This screen allows you to configure an ATM PVC identifier (VPI and

VPI: [0-255]

VCI: [32-65535]

Service Category: ▼

3.3.1.3 Seleccione **“Enable Quality Of service”**; active Calidad de Servicio marcando la casilla **“Enable Quality Of Service”**.

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 Real Time applications. For more information, see the [Advanced Setup/Quality of Service](#) to assign priorities for the applications.

Enable Quality Of Service ☒

Back Next

Haga clic en el botón **“Next”**.

3.3.1.4 Seleccione **“Bridging”**; seleccione **“LLC/SNAP – BRIDGING”** como **“Encapsulation Mode”**.

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

LLC/SNAP-BRIDGING ▼

Enable 802.1q ☐

Haga clic en el botón **“Next”**.

3.3.1.5 Seleccione **“Enable Bridge Service”**.

Unselect the check box below to disable this WAN service

Enable Bridge Service: ☒

Service Name:

Haga clic en el botón **“Next”**.

3.3.1.6 Se mostrará en pantalla un resumen de la configuración introducida. Haga clic en el botón **“Save”** para confirmar la configuración o pulse el botón **“Back”** para corregir la configuración.

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

VPI / VCI:	3 / 35
Connection Type:	Bridge
Service Name:	br_3_35
Service Category:	UBR
IP Address:	Not Applicable
Service State:	Enabled
NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Not Applicable
Quality Of Service:	Enabled

Click "Save" to save these settings. Click "Back" to make any modifications.
NOTE: You need to reboot to activate this WAN interface and further configure services over this interface.

3.3.1.7 Una vez realizada la configuración, haga clic en el botón **“Save/Reboot”**.

3.3.2: Configurar los parámetros de la LAN.

3.3.2.1 Seleccione el menú “Advanced Setup > LAN”

Local Area Network (LAN) Setup

Configure the DSL Router IP Address and Subnet Mask for LAN in configuration effective.

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Loopback IP and Subnetmask

IP Address: 127.0.0.1

Subnetmask: 255.0.0.0

☐ Enable UPnP

3.3.2.2 Introduzca la dirección IP en el capo “**IP address**” y la máscara de subred en el campo “**Subnet Mask**”;

3.3.2.3 Si lo desea puede cambiar la dirección de loopback, para ello introduzca la dirección IP y la máscara de subred de Loopback en el apartado “**loopback IP and Subnetmask**”;

Loopback IP and Subnetmask

IP Address: 127.0.0.1

Subnetmask: 255.0.0.0

3.3.2.4 Active el servidor DHCP marcando la casilla “**Enable DHCP Server**” e indique el rango de asignación de dirección IP introduciendo una dirección IP de inicio y otra dirección de final. También debe introducir el tiempo máximo de asignación de dirección IP por MAC.

☐ Disable DHCP Server

☒ Enable DHCP Server

Start IP Address: 192.168.1.33

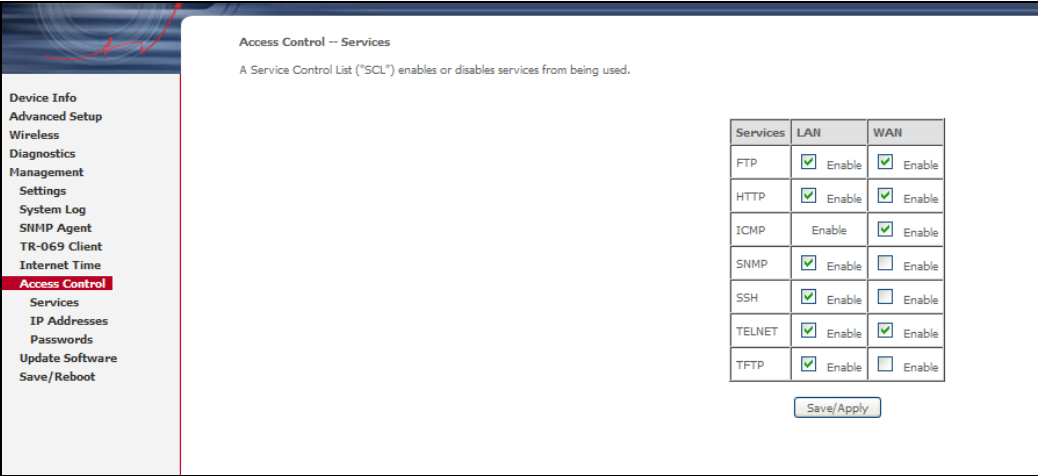
End IP Address: 192.168.1.254

Leased Time (hour): 24

3.3.2.5 Haga clic en el botón “**Save**”. O si lo prefiere en el botón “**Save/Reboot**”.

3.3.3: Configurar el Control del Acceso.

3.3.3.1 Seleccione “**Management > Access Control**”. En esta opción se le mostrará los servicios en los que tiene opción de permitir o restringir el acceso



3.3.3.2 Marque las casillas del “**Service Control Access List**” que desea permitir por el interfaz WAN o por el interfaz LAN.

Services	LAN	WAN
FTP	☒ Enable	☒ Enable
HTTP	☒ Enable	☒ Enable
ICMP	Enable	☒ Enable
SNMP	☒ Enable	☐ Enable
SSH	☒ Enable	☐ Enable
TELNET	☒ Enable	☒ Enable
TFTP	☒ Enable	☐ Enable

3.3.3.3 Para realizar una gestión de direccionamiento IP a los servicios permitidos, seleccione “**IP Address**” del menú “**Access Control**”, Active el “**Modo de Control del Acceso**” marcando la casilla “**Enable**”

Access Control Mode: ☐ Disable ☒ Enable

IP Address	Subnet Mask	Interface	Remove

3.3.3.4 Para añadir una dirección IP que tenga permiso de acceso, haga clic en el botón “**Add**”.

3.3.3.5 Introduzca la dirección IP que tendrá permiso de gestión en el campo “**IP Address**”, introduzca la máscara de subred en el campo “**Subnet Mask**”, y seleccione el interfaz por el que esa dirección IP tendrá acceso a su router.

Access Control

Enter the IP address of the management station permitted to access the local management services, and click 'Save/Apply.'

IP Address	Subnet Mask	Interface
		none lan wan lan&wan

Save/Apply

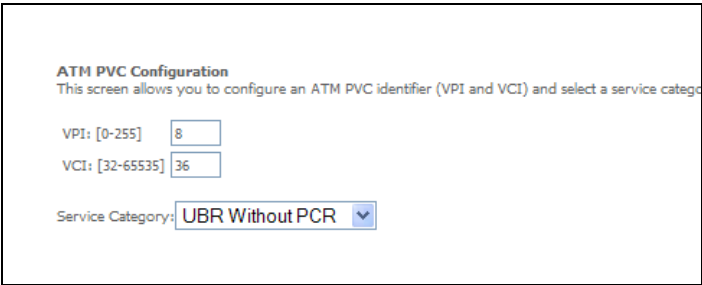
3.3.3.6 Haga clic en el botón “**Save/Apply**”.

3.4 Configuración Monopuesto Estático (IPoA)

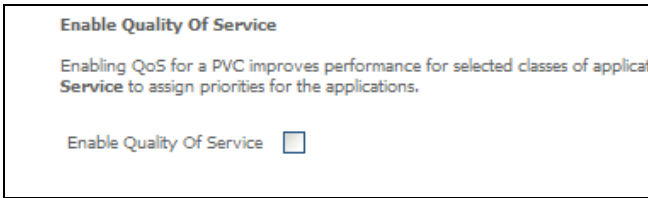
3.4.1: Configurar el puerto WAN

3.4.1.1 Haga clic en el menú “**Advanced Setup > WAN**”. Haga clic en el botón “**Add**” para crear una interfaz WAN)

3.4.1.2 Introduzca los valores VPI/VCI;

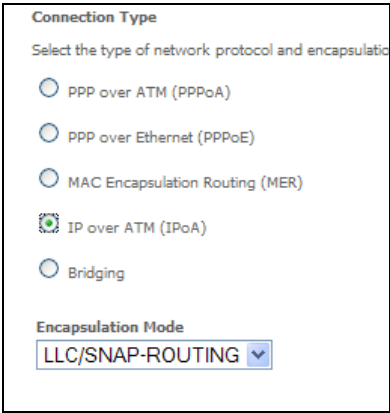


3.4.1.3 Active la casilla Calidad del Servicio marcando “**Enable Quality of Service**”.



Haga clic en el botón “**Next**”.

3.4.1.4 Seleccione la opción “**IP over ATM (IPoA)**”; seleccione “**LLC/SNAP – BRIDGING**” como “**Encapsulation Mode**”.



Haga clic en el botón “**Next**”.

3.4.1.5 Introduzca la dirección IP pública “(**WAN IP Address**)” y Máscara de subred “(**WAN Subnet Mask**)” facilitada por su proveedor de acceso a Internet.

WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.

Notice: DHCP is not supported in IPoA mode. Changing the default gateway or the

WAN IP Address:

WAN Subnet Mask:

3.4.1.6 Marque la casilla **“Use the following default Gateway”** y marque la casilla **“Use IP Address”**, e introduzca la dirección IP en el campo **“Use IP Address”**,

☒ Use the following default gateway:

☒ Use IP Address:

☐ Use WAN Interface:

3.4.1.7 Marque la casilla **“Use the following DNS server addresses”** e introduzca las direcciones del servidor DSN primario y secundario.

☒ Use the following DNS server addresses:

Primary DNS server:

Secondary DNS server:

Haga clic en el botón **“Next”**.

Nota: Si su proveedor de acceso a Internet es Telefónica, encontrará todos estos datos en la carta que le suministra Telefónica junto a la información de usuario.

3.4.1.8 Marque la casilla **“Enable NAT”** y **“Enable WAN Service”**; desmarque la casilla **“Enable Firewall”** y **“Enable IGMP Multicast”**.

Network Address Translation Settings

Network Address Translation (NAT) allows you to share one Wide Area Network

Enable NAT ☒

Enable Firewall ☐

Enable IGMP Multicast, and WAN Service

Enable IGMP Multicast ☐

Enable WAN Service ☒

Service Name:

Haga clic en el botón **“Next”**.

3.4.1.9 Se mostrará en pantalla un resumen de la configuración introducida. Haga clic en el botón **“Save”** para confirmar la configuración o pulse el botón **“Back”** para corregir la configuración.

3.4.1.10 Una vez realizada la configuración, haga clic en el botón **“Save/Reboot”**.

3.4.2: Configurar los parámetros de la LAN.

3.4.2.1 Seleccione el menú “Advanced Setup > LAN”

Local Area Network (LAN) Setup

Configure the DSL Router IP Address and Subnet Mask for LAN in configuration effective.

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Loopback IP and Subnetmask

IP Address: 127.0.0.1

Subnetmask: 255.0.0.0

☐ Enable UPnP

3.4.2.2 Introduzca la dirección IP en el capo “**IP address**” y la máscara de subred en el campo “**Subnet Mask**”;

3.4.2.3 Si lo desea puede cambiar la dirección de loopback, para ello introduzca la dirección IP y la máscara de subred de Loopback en el apartado “**loopback IP and Subnetmask**”;

Loopback IP and Subnetmask

IP Address: 127.0.0.1

Subnetmask: 255.0.0.0

3.4.2.4 Active el servidor DHCP marcando la casilla “**Enable DHCP Server**” e indique el rango de asignación de dirección IP introduciendo una dirección IP de inicio y otra dirección de final. También debe introducir el tiempo máximo de asignación de dirección IP por MAC.

☐ Disable DHCP Server

☒ Enable DHCP Server

Start IP Address: 192.168.1.33

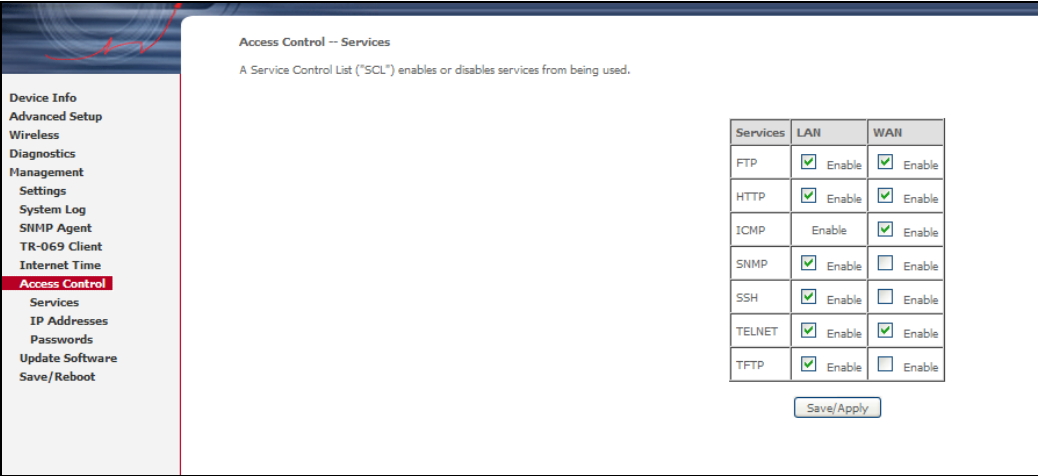
End IP Address: 192.168.1.254

Leased Time (hour): 24

3.4.2.5 Haga clic en el botón “**Save**”. O si lo prefiere en el botón “**Save/Reboot**”.

3.4.3: Configurar el Control del Acceso.

3.4.3.1 Seleccione “**Management > Access Control**”. En esta opción se le mostrará los servicios en los que tiene opción de permitir o restringir el acceso



3.4.3.2 Marque las casillas del “**Service Control Access List**” que desea permitir por el interfaz WAN o por el interfaz LAN.

Services	LAN	WAN
FTP	☒ Enable	☒ Enable
HTTP	☒ Enable	☒ Enable
ICMP	☐ Enable	☒ Enable
SNMP	☒ Enable	☐ Enable
SSH	☒ Enable	☐ Enable
TELNET	☒ Enable	☒ Enable
TFTP	☒ Enable	☐ Enable

3.4.3.3 Para realizar una gestión de direccionamiento IP a los servicios permitidos, seleccione “**IP Address**” del menú “**Access Control**”, Active el “**Modo de Control del Acceso**” marcando la casilla “**Enable**”

Access Control Mode: ☐ Disable ☒ Enable

IP Address	Subnet Mask	Interface	Remove

3.4.3.4 Para añadir una dirección IP que tenga permiso de acceso, haga clic en el botón “**Add**”.

3.4.3.5 Introduzca la dirección IP que tendrá permiso de gestión en el campo “**IP Address**”, introduzca la máscara de subred en el campo “**Subnet Mask**” , y seleccione el interfaz por el que esa dirección IP tendrá acceso a su router.

Access Control

Enter the IP address of the management station permitted to access the local management services, and click 'Save/Apply.'

IP Address	Subnet Mask	Interface
		none none lan wan lan&wan

Save/Apply

3.4.3.6 Haga clic en el botón “**Save/Apply**”.

3.5 Abrir Puertos (Usando Servidores Virtuales)

Para hacer uso de esta opción, debe existir al menos un PVC con la opción NAT activada.

NAT no estará disponible en la configuración en modo Bridge.

3.5.1: Servidores Virtuales

Los Servidores Virtuales permiten dirigir el tráfico entrante desde la WAN (identificado por el Protocolo y Puerto Externo) a la dirección IP interna del Servidor Interno en el lado de la LAN.

El Puerto Interno es requerido sólo si el puerto externo necesita ser convertido en un número de puerto diferente del utilizado por el servidor del lado de la LAN.

Pueden configurarse un máximo de 32 entradas.

Para añadir un servidor Virtual, seleccione en el menú “**Advanced setup > NAT**”.

The screenshot shows the 'NAT -- Virtual Servers Setup' page. On the left is a sidebar menu with options: Device Info, Advanced Setup, WAN, LAN, NAT (highlighted), Virtual Servers, Port Triggering, DMZ Host, and ALG. The main content area has a title 'NAT -- Virtual Servers Setup' and a description: '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.' Below the text are 'Add' and 'Remove' buttons. At the bottom is a table with 8 columns: Server Name, External Port Start, External Port End, Protocol, Internal Port Start, Internal Port End, Server IP Address, and Remove.

Haga clic en el botón “**Add**”. Se le mostrará la pantalla:

The screenshot shows the 'NAT -- Virtual Servers' configuration page. The sidebar menu is similar to the previous page but includes additional options like Security, Quality of Service, Routing, DNS, DSL, Port Mapping, Certificate, Wireless, Diagnostics, and Management. The main content area has a title 'NAT -- Virtual Servers' and a note: 'Select the service name, and enter the server IP address and click "Save/Apply" to forward IP packets for this service to the specified server. NOTE: The "Internal Port End" cannot be changed. It is the same as "External Port End" normally and will be the same as the "Internal Port Start" or "External Port End" if either one is modified. Remaining number of entries that can be configured:32'. Below the text are 'Server Name:' with a radio button for 'Select a Service:' (selected) and a dropdown menu showing 'Select One', and a radio button for 'Custom Server:' with a text input field. Below that is 'Server IP Address:' with a text input field showing '192.168.1.'. There are two 'Save/Apply' buttons. At the bottom is a table with 5 columns: External Port Start, External Port End, Protocol, Internal Port Start, and Internal Port End. The table has 12 rows, all with 'TCP' in the Protocol column.

Seleccione un Servicio	El usuario tiene que seleccionar un servicio de la lista.
O	O
Servidor Personalizado	El usuario puede introducir un nombre personalizado
Dirección IP del Servidor	Introduzca la dirección IP del servidor Interno.
Puerto externo de inicio	Introduzca el número de principio del rango de puertos externos (si selecciona Servidor Personalizado). Cuando un servicio es seleccionado, los rangos del puerto se configuran automáticamente al seleccionar dicho servicio.
Puerto Externo de final	Introduzca el número de final del rango de puertos externos (si selecciona Servidor Personalizado). Cuando un servicio es seleccionado, los rangos del puerto se configuran automáticamente al seleccionar dicho servicio.
Protocolo	El usuario puede seleccionar entre: TCP, TCP/UDP o UDP.
Puerto Interno de inicio	Introduzca el número de comienzo del rango de puertos internos (si selecciona Servidor Personalizado). Cuando un servicio es seleccionado, los rangos del puerto se configuran automáticamente al seleccionar dicho servicio.
Puerto interno de final	Introduzca el número de final del rango de puertos internos (si selecciona Servidor Personalizado). Cuando un servicio es seleccionado, los rangos del puerto se configuran automáticamente al seleccionar dicho servicio.

3.5.2: Ejemplo de configuración de un Virtual Server

Ejemplo: configurar puerto origen externo UDP 6681 a puerto destino interno UDP 6689 para el host local 192.168.1.2.

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.

AddRemove

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	Remove
-------------	---------------------	-------------------	----------	---------------------	-------------------	-------------------	--------

- 3.5.2.1 Haga clic en el botón “Add”.
- 3.5.2.2 Seleccione la opción “Custom Server”, Rellene el nombre del servicio en el capo “Custom Server”

Server Name:

☐ Select a Service:

Select One

▼

☒ Custom Server:

3.5.2.3 Introduzca la dirección IP de su servidor interno o host local en el campo “**Server IP Address**”

Server IP Address:

192.168.1.

3.5.2.4 Introduzca el valor 6681 como inicio del rango del Puerto Externo en el campo “**External Port Start**”

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
		TCP		
		TCP		

3.5.2.5 Introduzca el valor 6681 como fin del rango del Puerto Externo en el campo “**External Port End**”

3.5.2.6 Seleccione UDP como protocolo en el campo “**Protocol**”.

3.5.2.7 Introduzca el valor 6689 como inicio del rango del Puerto Interno en el campo “**Internal Port Start**”

3.5.2.8 Introduzca el valor 6689 como fin del rango del Puerto Interno en el campo “**Internal Port End**”

3.5.2.9 Haga clic en el botón “**Save/Apply**” para salvar.

3.6 Inalámbrico

El menú “**Wireless**” facilita el acceso a la configuración de la red inalámbrica incluyendo el nombre de la red o SSID, restricciones de canales (basado según país), seguridad inalámbrica, punto de acceso visible u oculto, punto de acceso o puente inalámbrico (bridging) e información de estaciones.

3.6.1: Pantalla Básica de Inalámbrico

La opción “**Basic**” permite configurar las propiedades básicas de la interfaz inalámbrica.

Wireless Basic

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable restrict the channel set based on country requirements. Click “Apply” to configure the basic wireless options.

☒ Enable Wireless

Al marcar la casilla “**Enable Wireless**”, aparecen las siguientes opciones:

- 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.

COMTrend

ADSL Router

Device Info

Advanced Setup

Wireless

Basic

Security

MAC Filter

Wireless Bridge

Advanced

Quality of Service

Station Info

Diagnostics

Management

Wireless -- Basic

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements. Click "Apply" to configure the basic wireless options.

☒

Enable Wireless

☐

Hide Access Point

SSID:

BSSID:

Country:

☐

Enable Wireless Guest Network

Guest SSID:

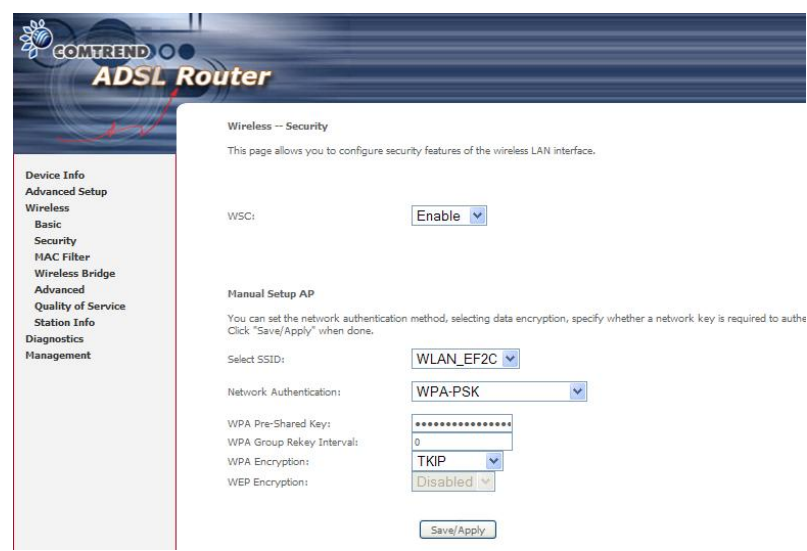
Save/Apply

Opción	Descripción
Enable Wireless	Marcando esta casilla, se activa o desactiva la interfaz inalámbrica. Si está seleccionada, la Interfaz de usuario Web muestra las siguientes opciones: Punto de Acceso Oculto, SSID y País. Por defecto, esta casilla está sin marcar por lo que el enlace inalámbrico está desactivado.
Hide Access Point	Seleccione Hide Access Point para proteger el punto de acceso del router ADSL2+ al ser detectado por escaneos de redes inalámbricos. Si no desea que el punto de acceso sea detectado automáticamente por una estación inalámbrica, marque esta casilla. La estación no descubrirá este punto de acceso. Para conectar una estación a los puntos de acceso disponibles, la estación tiene que ser añadida manualmente a su configuración inalámbrica con el nombre de este punto de acceso.
SSID	Configura el nombre de la red inalámbrica. SSID es el Identificador del Conjunto de Servicio. Para acceder a la WLAN, 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.
BSSID	BSSID es un identificador de 48 bits utilizado para identificar un BSS (Set Básico de Servicios) dentro de un área. En redes con infraestructura BSS, el BSSID es la dirección MAC (Control Medio del Acceso) del PA (Punto de Acceso) y en redes BSS independientes o ad hoc, el BSSID se genera aleatoriamente.
Country	En este campo aparece un menú desplegable que permite configuraciones internacionales y nacionales específicas.

	Cada país listado en el menú impone regulaciones específicas limitando el rango de canales: ✎ US = internacional ✎ Japón=1-14 ✎ Jordania= 10-
--	--

3.6.2: Seguridad inalámbrica

El menú de seguridad Inalámbrica “**Wireless > Security**” permite realizar la configuración de los parámetros de seguridad de la red inalámbrica utilizando el método WPS o de forma manual. Para usar el método WPS el CT5365 tiene activado la opción WSC (WiFi Simple Configuration) por defecto. El método WSC configura automáticamente los parámetros de seguridad. En comparación, el método manual requiere que el usuario seleccione e introduzca todos los valores de seguridad en cada uno de sus dispositivos clientes inalámbricos.



La configuración manual de los parámetros del Punto de Acceso está descrita en la siguiente tabla:

Select SSID
Configura el nombre de la red inalámbrica. SSID es el Identificador del Conjunto de Servicio. Para acceder a la WLAN, 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.

Network Authentication
Esta opción especifica la clave de red utilizada para la autenticación en la red inalámbrica. Cada tipo de autenticación tiene sus propios parámetros de configuración.
Por ejemplo, seleccionando encriptación WEP puede seleccionar los parámetros mostrados a continuación.

Select SSID:

Comtrend

Network Authentication:

802.1X

RADIUS Server IP Address:

0.0.0.0

RADIUS Port:

1812

RADIUS Key:

WEP Encryption:

Enabled

Encryption Strength:

128-bit

Current Network Key:

2

Network Key 1:

Network Key 2:

Network Key 3:

Network Key 4:

Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys
Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys

Save/Apply

Los parámetros de autenticación WPA son mostrados a continuación:

Select SSID:

Comtrend

Network Authentication:

WPA

WPA Group Rekey Interval:

0

RADIUS Server IP Address:

0.0.0.0

RADIUS Port:

1812

RADIUS Key:

WPA Encryption:

TKIP

WEP Encryption:

Disabled

Save/Apply

Los parámetros de autenticación WPA-PSK son mostrados a continuación

Select SSID:

Comtrend

Network Authentication:

WPA-PSK

WPA Pre-Shared Key:

[Click here to display](#)

WPA Group Rekey Interval:

0

WPA Encryption:

TKIP

WEP Encryption:

Disabled

Save/Apply

WPS

WPS es un estándar para dispositivos certificados que simplifica la configuración de seguridad de la red inalámbrica. Cada dispositivo certificado tiene dos métodos, método Push Button y método PIN. EL CT5365 tiene ambos métodos implementados. El método Push Buton se

realiza utilizando el botón WPS situado en el frontal del router inalámbrico y también a través del interfaz Web incluido en el mismo.

Los dispositivos con el logo WPS (mostrado aquí) soportan WPS. Sin embargo, el logo WPS no debe estar presente en el dispositivo. En este caso consulte la documentación del dispositivo facilitada para la opción WPS.



NOTA: WPS solo está disponible en los modos de autenticación WPA-PSK, WPA2-PSK o mixto WPA/WPA-PSK. Otros modos de autenticación que no usan WPS deben ser configurados manualmente.

Push Button

A continuación se indica cómo realizar la configuración inalámbrica utilizando el método Push Button

1. Seleccionar el modo de autenticación de red

Paso 1: Seleccionar el modo de autenticación WPA-PSK, WPA2-PSK o mixto WPA2/WPA-PSK desde la sección “**Manual Setup AP**” del menú “**Wireless > Security**”. El ejemplo descrito a continuación muestra el modo WPA2-PSK.

Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click "Save/Apply" when done.

Select SSID:

Comtrend

Network Authentication:

WPA2-PSK

WPA Pre-Shared Key:

WPA Group Rekey Interval:

0

WPA Encryption:

AES

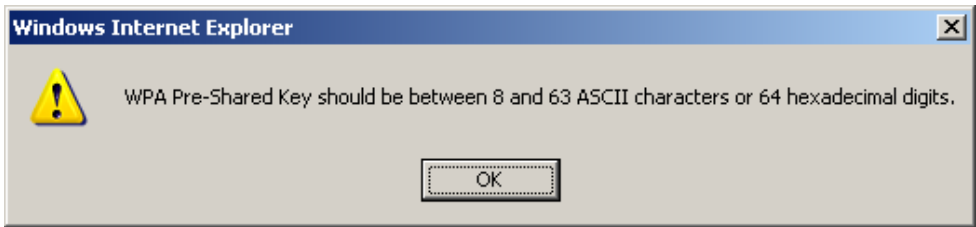
WEP Encryption:

Disabled

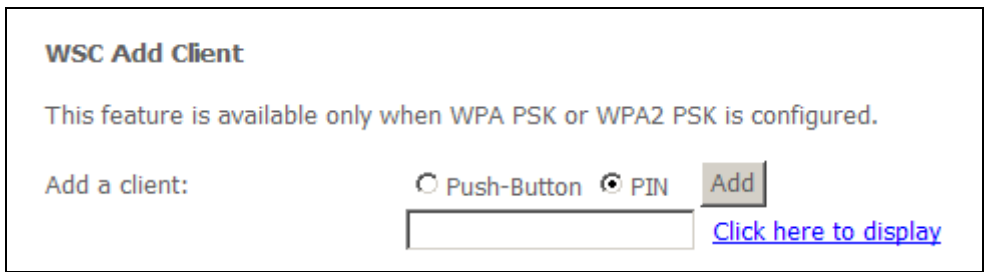
Save/Apply

Pasos 1 y 2

Paso 2: Introduzca una clave WPA Pre-Shared Key y haga clic en el botón **“Save/Apply”**. Verá el siguiente cuadro de diálogo si la clave es demasiado larga o demasiado corta.



Step 3: La sección **“WSC Add Client section”** debe aparecer ahora, como se muestra a continuación.



II. Configuración Push Button

El método de configuración push-button facilita un método de configuración semi-automatizado. El botón WPS del panel frontal del router puede ser usado en vez de usar el interfaz Web exclusivamente.

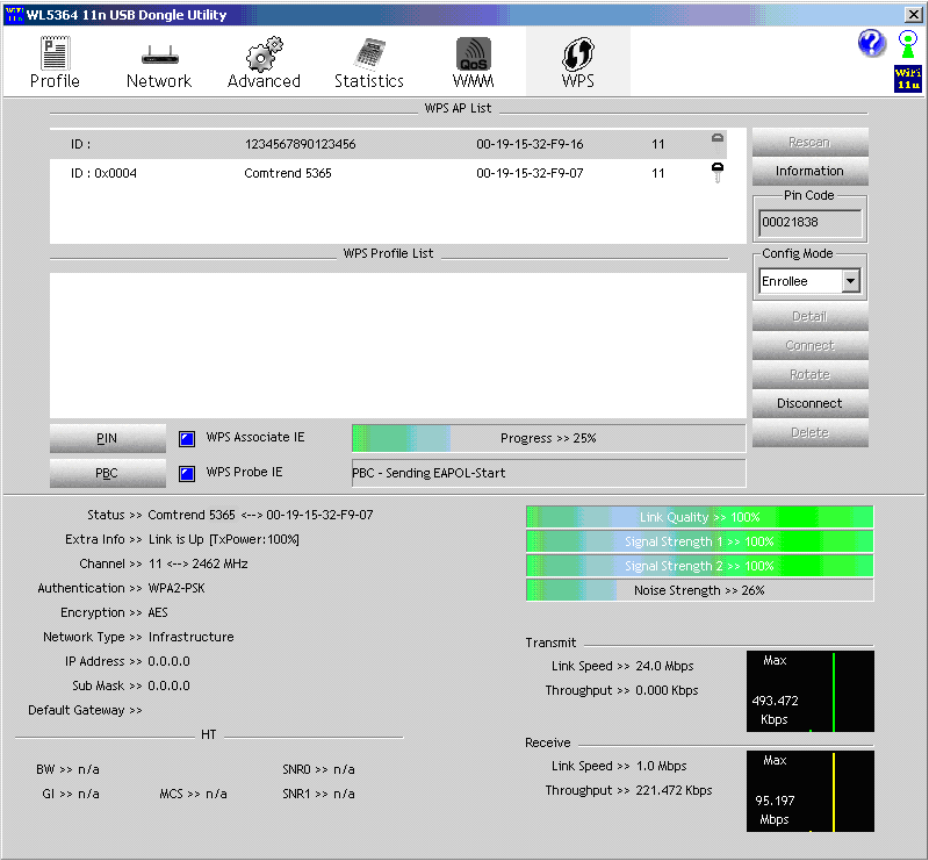
El método de configuración push-button que se describe a continuación es el usado utilizando el botón WPS del frontal del router. Se supone que la función inalámbrica del router está activada y que el router está configurado como punto de acceso inalámbrico.

Además el cliente inalámbrico también debe estar encendido, configurado correctamente y soportar la función WPS.

NOTA: El punto de acceso inalámbrico del router buscará clientes WPS durante 2 minutos. Si el router para la búsqueda antes de completar el paso 5, es necesario volver de nuevo al paso 4.

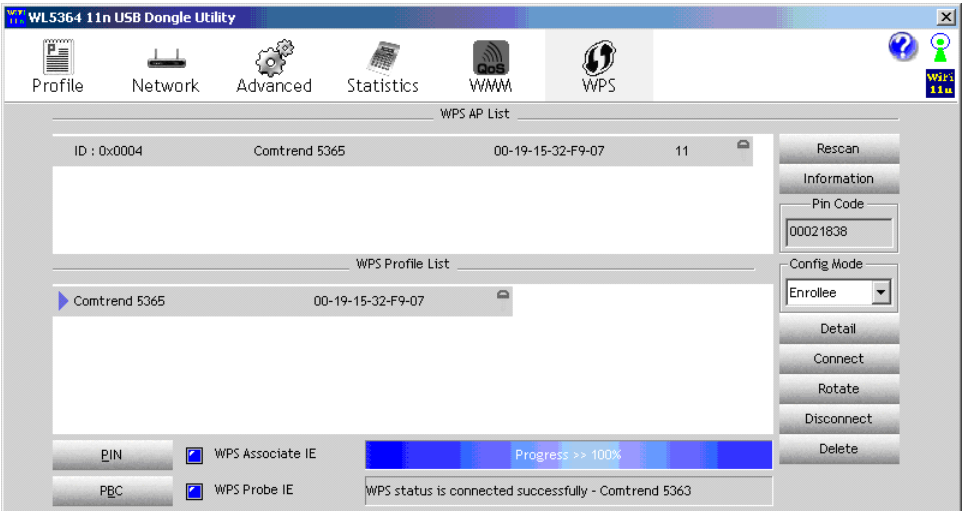
Paso 4: Presionar el botón WPS. Presione el botón WPS del panel frontal del router. El LED WPS parpadeará para mostrar que el router está buscando clientes WPS.

Paso 5: Ir al cliente inalámbrico WPS y activar la función Push Button. Una captura de pantalla típica de un cliente software WPS es como la mostrada a continuación:

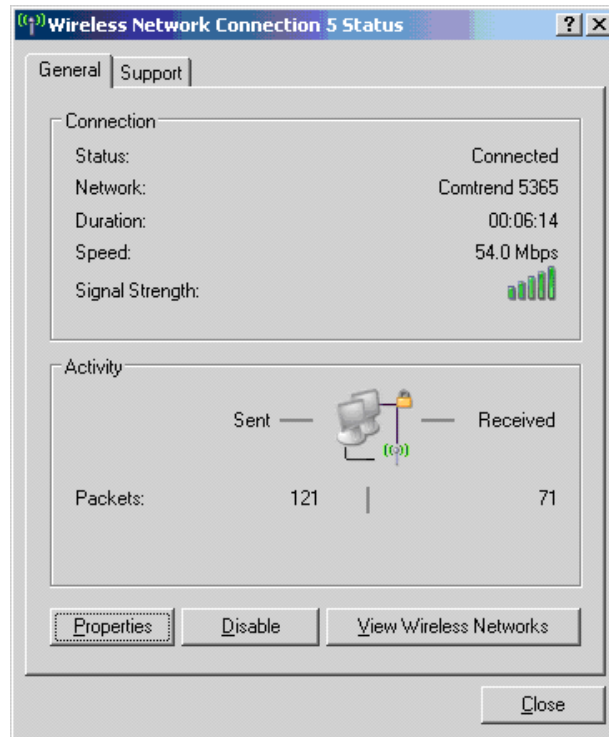


III. Chequear la conexión.

Paso 6: Si el método de configuración WPS se realizó con éxito, tendrá acceso a la red inalámbrica desde su cliente WPS. La herramienta software del cliente inalámbrico debe mostrar el estado. El ejemplo mostrado a continuación muestra una conexión establecida satisfactoriamente.



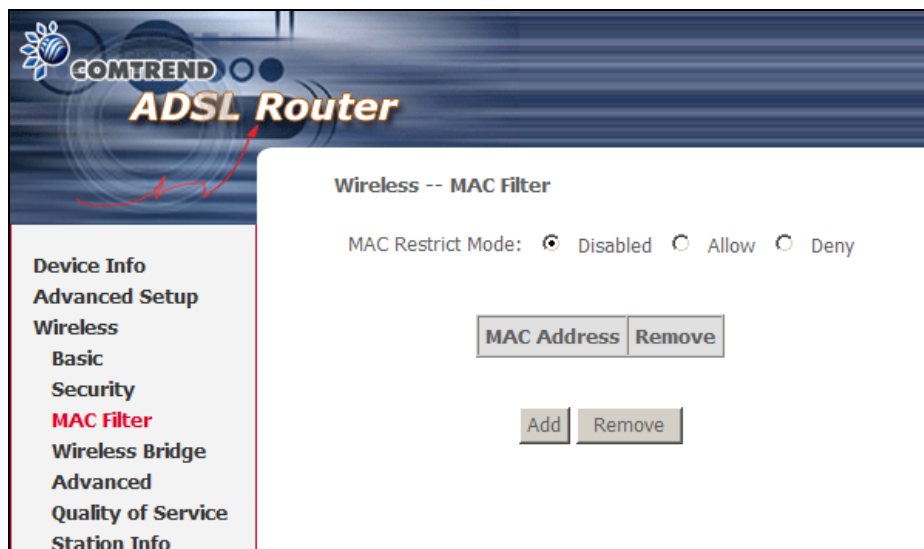
Haga doble clic en el icono de la conexión de red inalámbrica de las conexiones de red de Microsoft Windows para confirmar la nueva conexión. Deberá aparecer como se muestra en el cuadro de diálogo mostrado a continuación:



3.6.3: Filtrado MAC

Esta opción permite al router gestionar el acceso a la red inalámbrica basado en la dirección MAC del cliente inalámbrico. Cada dispositivo de red tiene un identificador único de 48 bits conocido como dirección MAC. Cuando una dirección MAC tiene el filtro habilitado, el dispositivo tiene restringido la posibilidad de conexión al Punto de acceso.

Para añadir un filtro de dirección MAC, haga clic en el botón **“Add”**.



Para eliminar un filtro, seleccione el filtro a eliminar de la tabla y haga clic en el botón **“Remove”**.

Opción	Descripción
MAC Restrict Mode	Off – Desactiva el filtrado MAC Allow – Permite el acceso a las direcciones MAC especificadas Deny – Rechaza el acceso a las direcciones MAC especificadas
MAC Address	Lista de direcciones MAC sujeta a MAC Restrict Mode. La acción sobre el botón “Add” requiere que sea introducida la dirección MAC de dos en dos caracteres, según la convención de 6 byte: xx:xx:xx:xx:xx:xx, donde xx son números hexadecimales. El número máximo de direcciones MAC que se pueden añadir es de 60.

Introduzca la dirección MAC en el campo **“MAC Address”** y haga clic en el botón **“Save/Apply”**.



3.6.5: Avanzado

El submenú **“Advanced”** del menú **“Wireless”** permite realizar la configuración avanzada de las características del interfaz WLAN. Entre otras acciones, puede seleccionar el canal de operación, forzar el rango transmisión a una velocidad en particular, fijar el umbral de fragmentación (Fragmentation threshold), fijar el umbral RTS (RTS threshold), fijar el wakeup interval para clientes en modo power-save, fijar el beacon interval para el punto de acceso, fijar el modo Xpress y fijar preámbulo, ya sea corto o largo.

Haga clic en el botón **“Save/Apply”** para salvar y aplicar los nuevos cambios en las opciones avanzadas de WLAN.

COMTREND

ADSL Router

Device Info

Advanced Setup

Wireless

Basic

Security

MAC Filter

Wireless Bridge

Advanced

Quality of Service

Station Info

Diagnostics

Management

Wireless -- Advanced

This page allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used.

Click "Apply" to configure the advanced wireless options.

AP Isolation:Off

Band:2.4GHz

Channel:11Current: 11

Auto Channel Timer(min)-1062731266

54g^m Rate:Auto

Multicast Rate:Auto

Basic Rate:Default

Fragmentation Threshold:2346

RTS Threshold:2347

DTIM Interval:1

Beacon Interval:100

Maximum Associated Clients:128

XPresstm Technology:Disabled

54g^m Mode:54g Auto

54g^m Protection:Auto

Preamble Type:long

Transmit Power:100%

Save/Apply

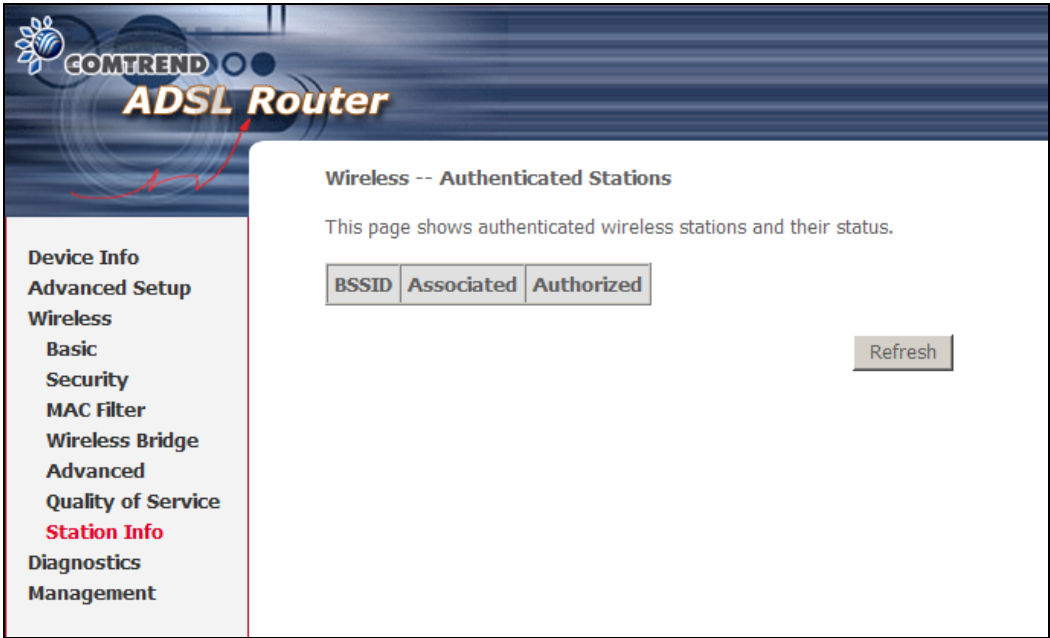
Campo	Descripción
AP Isolation	Seleccionar On u Off. Si esta característica está habilitada, los clientes inalámbricos asociados al punto de acceso no pueden conectar entre ellos.
Band	La normativa 802.11g permite compatibilidad hacia velocidades de 11 Mbps, por lo que dispositivos 802.11b y 802.11g pueden coexistir en la misma red inalámbrica. Ambas normas se aplican en la banda de frecuencia de 2,4GHz. IEEE 802.11g aumenta el ancho de banda inalámbrico hasta los 54 Mbps, igualando con 802.11a que opera en el rango de frecuencias de 5GHz.
Channel	Permite la selección del canal específico o modo automático ("Auto mode"). EL canal actual se muestra en el campo de la derecha.
Auto Channel Timer (min)	Auto búsqueda de canales con temporizador en minutos (0 lo desactiva).
54g Rate	Especifica el rango de transmisión de datos. En modo "Auto2 (por defecto) se usa el rango máximo si es posible, cayendo a tasas más bajas cuando sea necesario. El parámetro apropiado es dependiente de la fuerza de la señal (cobertura inalámbrica). Otros valores están dentro del rango de 1 a 54 Mbps.
Multicast Rate	Configuración del rango de transmisión de paquetes multicast (1-54 Mbps)

Basic Rate	Configuración del rango de transmisión básico.
Fragmentation Threshold	Un umbral, específico de bytes, que determina el tamaño en el que se fragmentarán los paquetes. En una WLAN 802.11, los paquetes que excedan el umbral de fragmentación son divididos en unidades más pequeñas adecuadas al tamaño del circuito. Los paquetes más pequeños que el valor del umbral especificado no son fragmentados. Los valores a introducir deben estar entre 256 y 2345. El valor por defecto es 2346, el establecimiento de un umbral de fragmentación demasiado bajo puede dar lugar a malas prestaciones. Si tiene un alto índice de error de paquetes, trate de aumentar ligeramente el umbral de fragmentación.
RTS Threshold	Solicitud de envío, fijado en bytes, especifica el tamaño de paquete que la tarjeta WLAN solicita en el mecanismo de RTS/CTS. Los paquetes que excedan el umbral de RTS especificado activación el mecanismo RTS/CTS. Los Paquetes más pequeños son enviados sin usar RTS/CTS. La configuración por defecto a 2347 (longitud máxima) desactiva el umbral total RTS.
DTIM Interval	Delivery Traffic Indication Message (DTIM) es también conocido como el rango de Beacon. El rango de estrada está entre 1 y 65535. Un DTIM es un variable que informa a los clientes de la siguiente ventana para escuchar mensajes broadcast y multicast. Cuando el AP tiene mensajes multicast o broadcast taponando a los clientes asociados, este envía el próximo DTIM con un valor de intervalo DTIM. Los puntos de acceso clientes escuchan el Beacon y empiezan a recibir los mensajes broadcast y multicast. Por defecto es 1.
Beacon Interval	La cantidad de tiempo en milisegundos entre Beacon transmitidos. Por defecto está a 100 ms y el rango aceptable es de 1 a 65535. La Transmisión del Beacon identifica la presencia de un punto de acceso. Por defecto, todos los dispositivos de red pasivos escanean todos los canales RF escuchando el Beacon del punto de acceso. Antes de que una estación entre en modo de power-save (ahorro de energía), la estación necesita el intervalo de Beacon para conocer cuando debe escuchar de nuevo para recibir el Beacon (y saber si hay frames taponando el punto de acceso)
Maximum Associated Clients	El número máximo permitido de clientes conectados al Router.
Xpress TM	La tecnología Xpress es compatible con el borrador de especificaciones de los dos estándares inalámbricos planteados. Por

Technology	defecto está desactivado.
54g TM Mode	Seleccionar el modo “ Auto ” para mayor compatibilidad. Seleccionar el modo “ Performance ” para mayores prestaciones entre equipos certificados 54g. Seleccionar modo “ LRS ” si hay alguna dificultad con equipamiento 802.11b. Si esta no trabaja correctamente, se debe probar sólo el modo 802.11b únicamente.
54g Protection	En modo “ Auto ”, el router usará RTS/CTS para mejorar las prestaciones 802.11g en redes mixtas 802.11g/802.11b. Situando la protección en “ Off ” maximizará las prestaciones 802.11g en la mayoría de las condiciones.
Preamble Type	El preámbulo corto se destina para aplicaciones donde se desea un rendimiento máximo pero no funciona correctamente con equipos más antiguos. El preámbulo largo trabaja con la actual especificación DSSS de 1 y 2 Mbps como describe el estándar IEEE 802.11-1999
Transmit Power	Configurar la potencia de transferencia (por porcentaje) deseada.

3.6.6: Información sobre Estaciones

Este submenú muestra las estaciones inalámbricas autenticadas y su estado. Haga clic en el botón “**Refresh**” para actualizar la lista de estaciones en la WLAN.

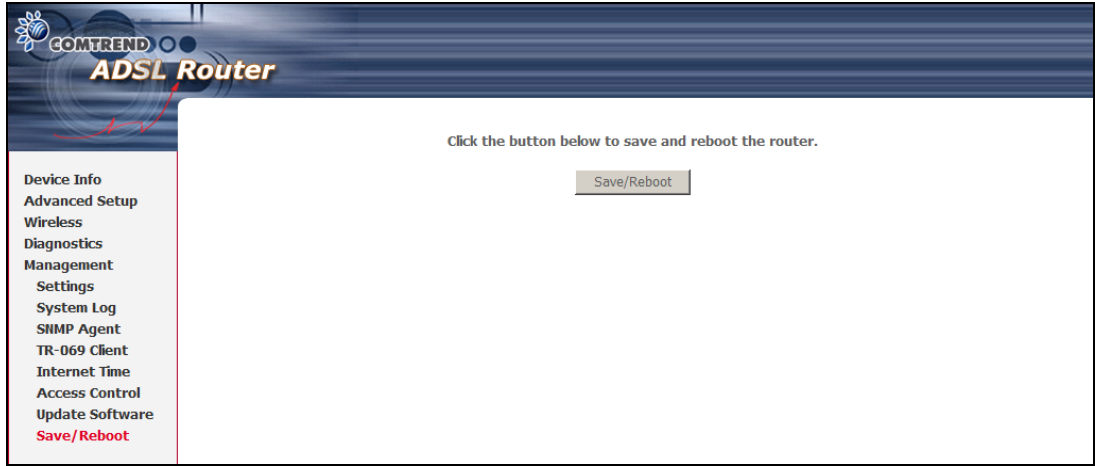


Campo	Descripción
-------	-------------

BSSID	BSSID es un identificador de 48 bits utilizado para identificar un BSS (Set Básico de Servicios) dentro de un área. En redes con infraestructura BSS, el BSSID es la dirección MAC (Control Medio del Acceso) del PA (Punto de Acceso) y en redes BSS independientes o ad hoc, el BSSID se genera aleatoriamente.
Associated	Lista de todas las estaciones que están asociadas al punto de acceso, junto con la cantidad de tiempo y paquetes transmitidos de cada una de ellas. Si una estación está parada durante mucho tiempo, esta será eliminada de la lista.
Authorized	Lista de dispositivos con acceso autorizado.

3.7 Salvar y Reiniciar

Este submenú guarda la configuración actual y reinicia el router CT5365.



NOTA: Puede necesitar reconfigurar los parámetros TCP/IP después de reiniciar. Por ejemplo si el servidor DHCP es deshabilitado y el cliente no tiene una dirección IP fija configurada.

NOTA: Si pierde todo el acceso a la interfaz de usuario web, será necesario que cierre su navegador, espere unos pocos minutos, y reinicie el acceso al interfaz web. Si aun así no accede correctamente, presione el botón reset en el panel trasero de su router durante 5 a 7 segundos para restaurar los parámetros por defecto.

3.8 Actualizar el software

El submenú “**Update Software**” permite actualizar el firmware. Las actualizaciones manuales del dispositivo desde un fichero local pueden ser realizadas desde esta opción.

COMTREND
ADSL Router

Device Info
Advanced Setup
Wireless
Diagnostics
Management
Settings
System Log
SNMP Agent
TR-069 Client
Internet Time
Access Control
Update Software
Save/Reboot

Tools -- Update Software

Step 1: Obtain an updated software image file from your ISP.

Step 2: Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.

Step 3: Click the "Update Software" button once to upload the new image file.

NOTE: The update process takes about 2 minutes to complete, and your DSL Router will reboot.

Software File Name:

Para realizar la actualización de software siga los siguientes pasos:

Paso 1: Obtener el fichero de software imagen desde su propio ISP.

Paso 2: Introduzca la dirección y nombre del fichero imagen en el campo **"Software File Name"** o haga clic en el botón **"Browse"** y localice el fichero imagen.

Paso 3: Haga clic en el botón **"Update software"** una vez para cargar e instalar el fichero.

NOTA: El proceso de actualización puede demorarse hasta 2 minutos hasta que se complete. El router se reiniciará y la ventana del navegador se refrescará indicando en pantalla que la actualización se ha realizado satisfactoriamente.

NOTA: Es recomendable que compare el valor del campo **"Software version"** de la parte superior del menú **"Device info"** de la opción **"Summary"** con la versión de software instalada, para confirmar que la instalación fue satisfactoria.