

CT-536+

Router Inalámbrico ADSL2+

Guía de Configuración Rápida

Versión A1.0, 30 de Agosto del 2005



CAPÍTULO 1	CONFIGURACIÓN RÁPIDA.....	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>8</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>16</i>
1.3	PABRIR PUERTOS (USANDO SERVIDORES VIRTUALES).....	20
1.3.1	<i>Configurar el puerto NAT según CT-536+.....</i>	<i>22</i>
1.4	INALÁMBRICO.....	24
1.4.1	<i>Pantalla Básica de Inalámbrico</i>	<i>24</i>
1.4.2	<i>Seguridad.....</i>	<i>26</i>
1.4.3	<i>Filtro CMA.....</i>	<i>29</i>
1.4.4	<i>Puente Inalámbrico.....</i>	<i>31</i>
1.4.5	<i>Avanzado.....</i>	<i>32</i>
1.4.6	<i>Información sobre Estaciones.....</i>	<i>34</i>
1.5	GUARDAR Y REINICIAR.....	35
1.6	ACTUALIZAR EL SOFTWARE	36

Capítulo 1 Configuración rápida

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: admin.

- "admin" 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-536+ para que el cambio tenga efecto.

COMTREND ADSL Router

Access Control -- Passwords

Access to your DSL router is controlled through one user account: 1234

The user name "1234" has unrestricted access to change and view configuration of your DSL Router.

Use the fields below to enter up to 16 characters and click "Apply" to change or create passwords.

Username:

Old Password:

New Password:

Confirm Password:

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)

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								

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:	pppoe3@tid/pppoe
PPP Password:	*****
PPPoE Service Name:	
Authentication Method:	AUTO
☐ Dial on Demand (with idle timeout timer)	
☐ PPP IP extension	
☒ Enable NAT	
☐ 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	
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.	
Device Info Quick Setup Advanced Setup WAN LAN	IP Address: 192.168.1.1
	Subnet Mask: 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:	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

☐ Disable DHCP Server
☒ Enable DHCP Server
 Start IP Address:
 End IP Address:
 Leased Time (hour):
☒ 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								
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
VoIP	High				UDP			81

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:
 Priority:
 Protocol:
 Destination IP Address:
 Destination Subnet Mask:

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

Traffic Interface Control
 Traffic Interface :
 Minimum Rate : Kbps

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

abajo).

Management	FTP	☒ Enable	☒ Enable
Settings	HTTP	☒ Enable	☒ Enable
System Log	ICMP	Enable	☒ Enable
SNMP Agent	SNMP	☒ Enable	☐ Enable
Internet Time	SSH	☒ Enable	☐ Enable
Access Control			

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

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

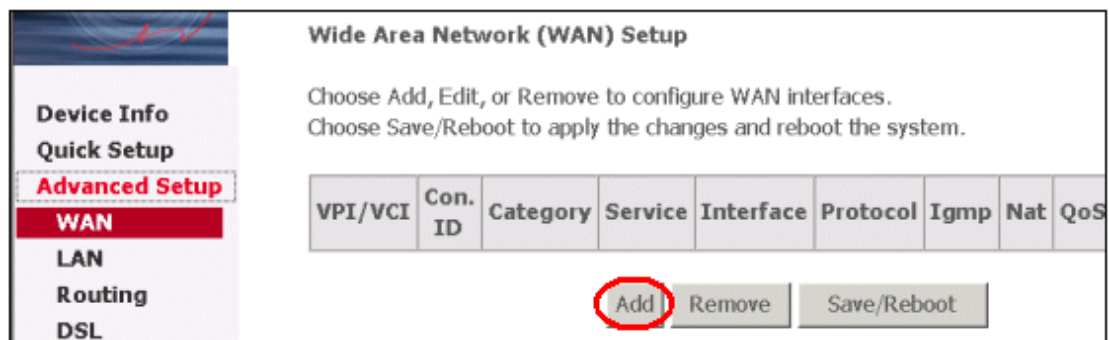
SNMP Agent	Access Control Mode: ☐ Disable ☒ Enable			
Internet Time	IP Address	Subnet Mask	Interface	Remove
Access Control	193.152.37.192	255.255.255.240	wan	☐
Services	0.0.0.0	0.0.0.0	lan	☐
IP Addresses				
Passwords				

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

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

Device Info
Quick Setup
Advanced Setup
WAN
LAN
Routing
DSL

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

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 (deschequeando la casilla), luego haga clic en el botón Siguiente (como se indica más abajo).

Enable NAT	☒
Enable Firewall	☐
Enable IGMP Multicast, and WAN Service	
Enable IGMP Multicast	☐
Enable WAN Service	☒
Service Name:	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	
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.	
Device Info Quick Setup Advanced Setup WAN LAN	IP Address: 192.168.1.1
	Subnet Mask: 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:	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

☐ Disable DHCP Server ☒ Enable DHCP Server	
Start IP Address:	192.168.1.33
End IP Address:	192.168.1.64
Leased Time (hour):	24
☒ 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).

Device Info Advanced Setup WAN LAN NAT Parental Control Quality of Service	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	FTP	☒ Enable	☒ Enable
Settings	HTTP	☒ Enable	☒ Enable
System Log	ICMP	Enable	☒ Enable
SNMP Agent	SNMP	☒ Enable	☐ Enable
Internet Time	SSH	☒ Enable	☐ Enable
Access Control			

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

Services	LAN	WAN
FTP	☒ Enable	☒ Enable
HTTP	☒ Enable	☒ Enable
ICMP	Enable	☒ Enable
SNMP	☒ Enable	☐ Enable
SSH	☒ Enable	☐ Enable
TELNET	☒ Enable	☒ Enable
TFTP	☒ Enable	☐ 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	☐
0.0.0.0	0.0.0.0	lan	☐

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

Internet Time	Click the button below to save and reboot the router.
Access Control	
Update Software	
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).

Device Info

Quick Setup

Advanced Setup

WAN

LAN

Routing

DSL

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								

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: UBR Without PCR ▼

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

LLC/SNAP-BRIDGING ▼

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	
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:	192.168.1.1
Subnet Mask:	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:	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

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
VoIP	High				UDP			8

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 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 SNMP Agent Internet Time Access Control	FTP	☒ Enable	☒ Enable
	HTTP	☒ Enable	☒ Enable
	ICMP	Enable	☒ Enable
	SNMP	☒ Enable	☐ Enable
	SSH	☒ Enable	☐ 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	☒ Enable
HTTP	☒ Enable
ICMP	Enable
SNMP	☒ Enable
SSH	☒ Enable
TELNET	☒ Enable
TFTP	☒ 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	☐
	0.0.0.0	0.0.0.0	lan	☐

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	

1.2.4 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).

Device Info Quick Setup Advanced Setup WAN LAN Routing DSL	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								

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]	8
VCI: [32-65535]	32
Service Category:	UBR Without PCR

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 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: 10.0.0.5

WAN Subnet Mask: 255.255.255.0

☒ Use the following default gateway:

☒ Use IP Address: 10.0.0.1

☐ 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 Servicio WAN; desactive NAT, Firewall e IGMP (deschequeando la casilla), luego haga clic en el botón Siguiente (como se indica más abajo).

Enable NAT	☐
Enable Firewall	☐
Enable IGMP Multicast, and WAN Service	
Enable IGMP Multicast	☐
Enable WAN Service	☒
Service Name:	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).

Device Info Quick Setup Advanced Setup WAN LAN	Local Area Network (LAN) Setup	
	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:	192.168.1.1
	Subnet Mask:	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:	80.0.5.61
Subnet Mask:	255.255.255.252
Loopback IP and Subnetmask	
IP Address:	127.0.0.1
Subnetmask:	255.0.0.0
☐ Disable DHCP Server ☒ Enable DHCP Server	
Start IP Address:	80.0.5.62
End IP Address:	80.0.5.62
Leased Time (hour):	24
☐ Enable DHCP Server Relay DHCP Server IP Address:	
☒ 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	Destination Address / Mask	Destination Port
VoIP	High				UDP				8021

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 SNMP Agent Internet Time Access Control	FTP	☒ Enable	☒ Enable
	HTTP	☒ Enable	☒ Enable
	ICMP	Enable	☒ Enable
	SNMP	☒ Enable	☐ Enable
	SSH	☒ Enable	☐ Enable

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

Services	LAN	WAN
FTP	☒ Enable	☒ Enable
HTTP	☒ Enable	☒ Enable
ICMP	Enable	☒ Enable
SNMP	☒ Enable	☐ Enable
SSH	☒ Enable	☐ Enable
TELNET	☒ Enable	☒ Enable
TFTP	☒ Enable	☐ 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	☐
	0.0.0.0	0.0.0.0	lan	☐

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

1.3 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.

COMTREND

ADSL Router

Device Info

Advanced Setup

WAN

LAN

NAT

Virtual Servers

Port Triggering

DMZ Host

Parental Control

Quality of Service

Routing

DNS

DSL

Wireless

Diagnostics

Management

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
-------------	---------------------	-------------------	----------	---------------------	-------------------	-------------------	--------

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

COMTREND

ADSL Router

Device Info

Advanced Setup

WAN

LAN

NAT

Virtual Servers

Port Triggering

DMZ Host

Parental Control

Quality of Service

Routing

DNS

DSL

Wireless

Diagnostics

Management

NAT -- Virtual Servers

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

Server Name:

☒ Select a Service:

Select One

☐ Custom Server:

Server IP Address:

192.168.1.

Save/Apply

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

Save/Apply

Seleccione un Servicio	El usuario tiene que seleccionar un servicio de la lista.
O	O El usuario puede introducir un nombre a su elección.

Servidor Personalizado	
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-536+

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.

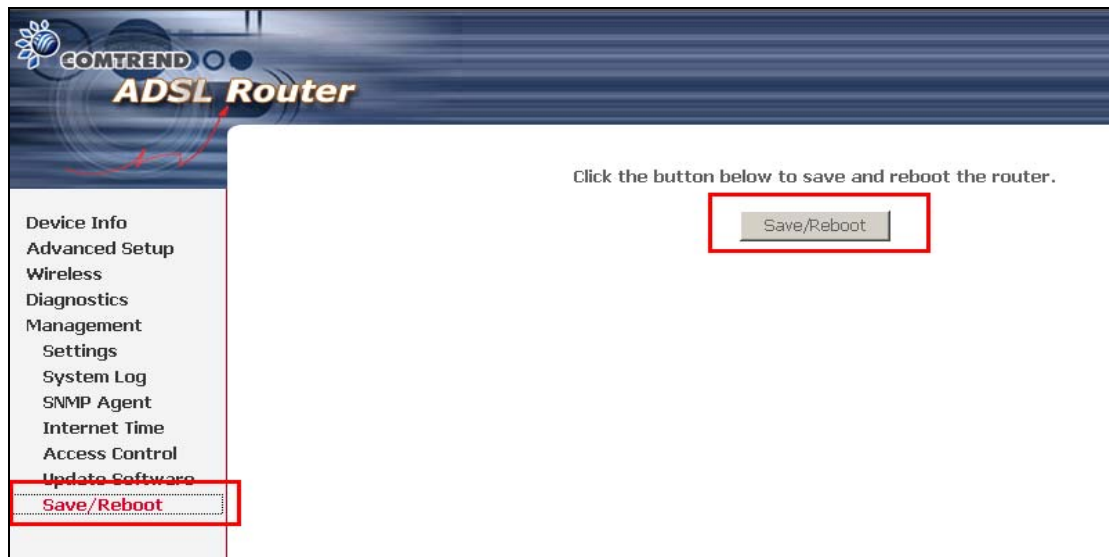
NAT -- Virtual Servers Setup

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	☐

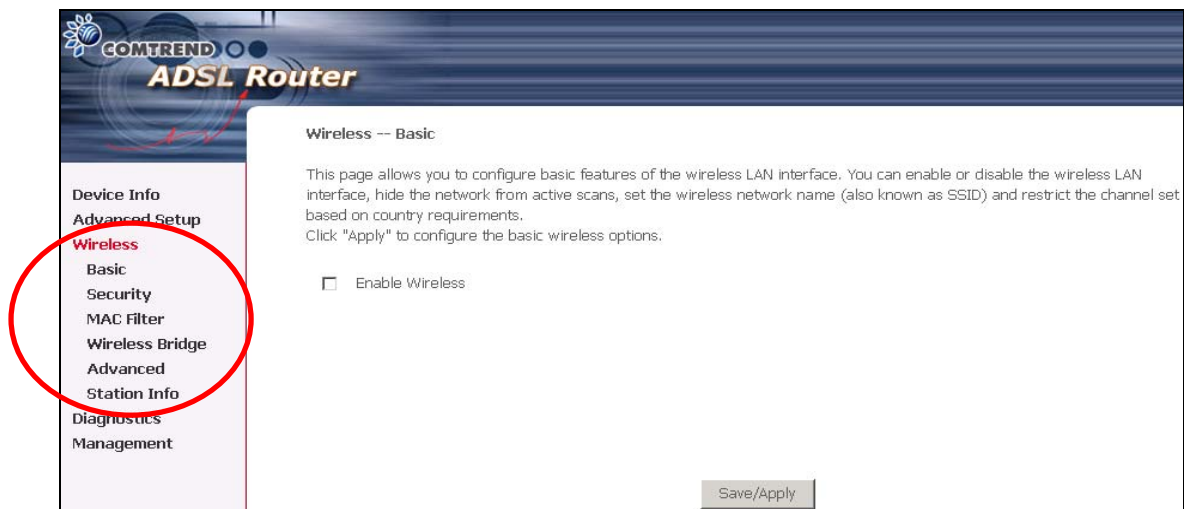
Finalmente, clic en Guardar/Reiniciar para que la Configuración surja efecto.



1.4 Inalámbrico

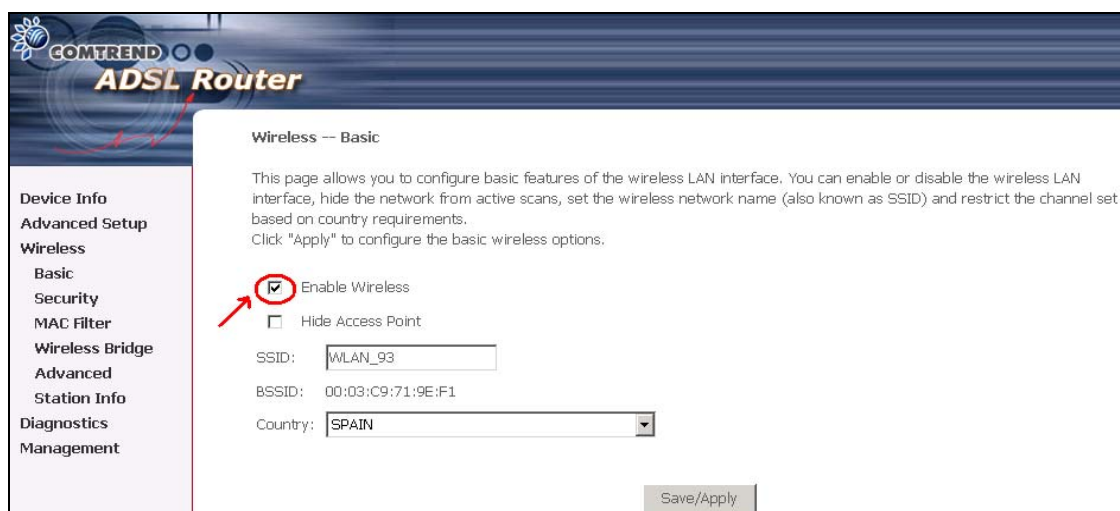
La casilla de diálogo Inalámbrico le permite activar la capacidad inalámbrica, oculta el punto de acceso, configura el nombre de la red inalámbrica y restringe el conjunto de canales.

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.

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



Opción	Descripción
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	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. 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. En Windows XP, vaya a la función Red>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.
SSID	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) La convenciones con respecto al nombramiento son: Mínimo es un carácter y el número máximo de caracteres: 32 bytes.
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	Un menu desplegable que permite configuraciones internacionales y nacionales específicas. Cada país listado en el menu impone regulaciones específicas limitando el rango de canales: ● US = internacional ● Japón=1-14 ● Jordania= 10-13 ● Israel= TBD

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; en este caso la captura del tráfico de la red inalámbrica. Si la encriptación de la información está activada, las llaves de encriptación compartida secreta 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.



The screenshot shows the 'Wireless -- Security' configuration page of a COMTREND ADSL Router. The page has a blue header with the COMTREND logo and 'ADSL Router' text. On the left is a navigation menu with options: Device Info, Advanced Setup, Wireless, Basic, Security, MAC Filter, Wireless Bridge, Advanced, Station Info, Diagnostics, and Management. The main content area is titled 'Wireless -- Security' and contains the following text: 'This page allows you to configure security features of the wireless LAN interface. 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 "Apply" to configure the wireless security options.'

The configuration options are as follows:

- Network Authentication: Open (dropdown menu)
- WEP Encryption: Enabled (dropdown menu)
- Encryption Strength: 128-bit (dropdown menu)
- Buttons: 'Set Encryption Keys' and 'Save/Apply'

Opción	Descripción
Autenticación de la red	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. Otro tipo de autenticación origina requisitos diferentes de configuración. Si elige 802.1X, introduzca la dirección IP del servidor RADIUS, el puerto RADIUS y la llave RADIUS. Asimismo, active la encriptación WEP y el Grado de Encriptación. Network Authentication: 802.1X RADIUS Server IP Address: 0.0.0.0 RADIUS Port: 1812 RADIUS Key: WEP Encryption: Enabled Encryption Strength: 128-bit Set Encryption Keys Si selecciona WPA, tiene que introducir el intervalo de refresco del grupo WPA. 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

	Si selecciona WPA-PSK, tiene que introducir la Llave pre-compartida WPA y el intervalo de refresco del grupo WPA. Network Authentication: WPA-PSK WPA Pre-Shared Key: WPA Group Rekey Interval: 0 WPA Encryption: TKIP WEP Encryption: Disabled
Encriptado WEP	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.
Grado de Encriptado	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. La configuración Grado de Encriptación no se presenta hasta que se chequea la casilla Autenticación de la Red (Modo compartido).

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.

COMTREND ADSL Router

Device Info
Advanced Setup
Wireless
Basic
Security
MAC Filter
Wireless Bridge
Advanced
Station Info
Diagnostics
Management

Wireless -- Bridge

This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disables access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access.

Click "Refresh" to update the remote bridges. Wait for few seconds to update.
Click "Save/Apply" to configure the wireless bridge options.

AP Mode:

Bridge Restrict:

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.

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 - 802.11g
Channel:	12
Rate:	Auto
Multicast Rate:	Auto
Basic Rate:	Default
Fragmentation Threshold:	2346
RTS Threshold:	2347
DTIM Interval:	1
Beacon Interval:	100
XPress™ Technology:	Disabled
54g™ Mode:	54g Auto
54g Protection:	Auto

Save/Apply

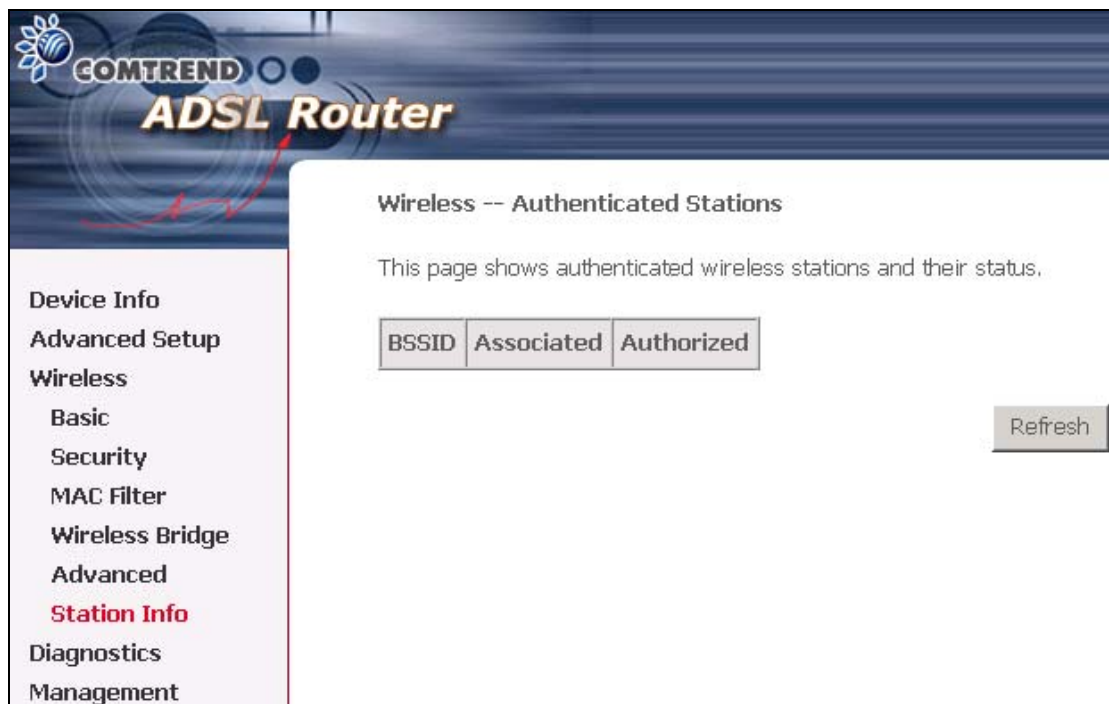
Opción	Descripción
Aislamiento PA	Seleccionar Encendido o Apagado. Activando esta propiedad, los clientes inalámbricos asociados al Punto de Acceso podrán interconectarse.
Banda	La nueva enmienda permite a las unidades IEEE 802.11g recurrir a velocidades de 11 Mbps, así que en la misma red pueden coexistir 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 Mbps cuando es posible, pero salta a velocidades más bajas si es necesario. Velocidades fijadas de 1 Mbps, 2Mbps, 5Mbps, o 11Mbps. El ajuste adecuado depende de la fuerza de la señal.
Multicast Rate	Setting multicast packet transmit rate
Velocidad Básica	Configurar la velocidad básica de transmisión
Umbral de Fragmentación	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. Introduzca un valor entre 256 y 2346. 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.
Umbral RTS	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.
Intervalo DTIM	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.
Intervalo Beacon	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. 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). El valor introducido está representado en ms. Por defecto es 100. Un intervalo de entrada aceptable es de 1 a 0xffff

	(65535)
Tecnología Xpress™	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™	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.

The screenshot shows the Comtrend ADSL Router web interface. On the left is a navigation menu with the following items: Device Info, Advanced Setup, Wireless, Diagnostics, Management, Settings, System Log, SNMP Agent, Internet Time, Access Control, Update Software (highlighted in red), and Save/Reboot. The main content area is titled 'Tools -- Update Software'. It contains three steps: 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. Below the steps is a note: 'NOTE: The update process takes about 2 minutes to complete, and your DSL Router will reboot.' At the bottom of the main area, there is a 'Software File Name:' label followed by a text input box, a 'Browse...' button, and an 'Update Software' button.

COMTREND
ADSL Router

Device Info
Advanced Setup
Wireless
Diagnostics
Management
Settings
System Log
SNMP Agent
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:

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.