COMTREND CORPORATION

WAP-5813n

Router inalámbrico Gigabit

Manual de usuario

Versión 1.1-spa, octubre 7, 2009

Prefacio

Este manual facilita información relativa a la configuración del Router inalámbrico 11n para FTTH.

Al usuario que lea este manual se le supone cierta compresión 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 pesados sobre el cable eléctrico. Se debe impedir pisar, caminar o maltratar el cable.
- Use únicamente la fuente de alimentación eléctrica suministrada con el router inalámbrico 11n.
- Salvaguarde el producto de sobrecalentamientos, asegúrese que todas las aberturas de ventilación no están bloqueadas.

PRECAUCION:

- Para reducir el riesgo de fuego, use sólo cable de telecomunicaciones AWG nº 26 o superior
- Desconecte siempre todos los cables y conexiones 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

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.

Índice

1. Introducción

El WAP-5813n es un router inalámbrico Gigabit que facilita conectividad alámbrica e inalámbrica para aplicaciones de banda ancha en entornos residenciales o de negocios. Está diseñado para ser conectado a un modem xDSL o GPON (Gigabit-Capable Passive Iptical Network). El WAP-5813n facilita un puerto WAN 10/100/1000 Base-T Gigabit Ethernet y cuatro puertos LAN 10/100/1000 Base-T Gigabit Ethernet. También tiene soporte TR-068 cumpliendo con el panel de colores e indicadores luminosos para una fácil instalación y uso.

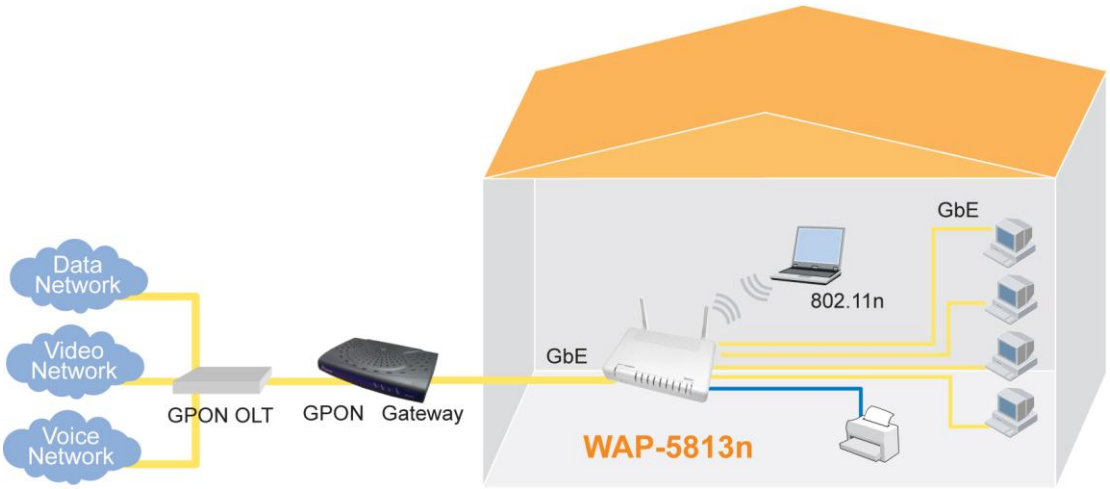
Un punto de acceso inalámbrico 802.11n (Draft) soporta conexiones más rápidas e incremento del ancho de banda, sin sacrificar compatibilidad con otros dispositivos inalámbricos 802.11b y 802.11g. Los botones WPS (Wi-Fi Protected Setup) y Wi-Fi On/Off están incluidos para facilitar la configuración de la red inalámbrica. Las opciones de encriptación de datos WPA, Firewall y VPN passthrough proporcionan el estado del arte de redes seguras.

1.1 Características

- Punto de acceso 802.11n integrado (compatible con 802.11b/g)
- WPA/WPA2 y 802.1x
- Cliente RADIUS
- Enrutamiento estático
- NAT/PAT
- IGMP Proxy
- Diagrama de aplicaciones
- Gestión basada en Web
- Soporte a gestión remota
- WMM y UPnP
- Filtrado IP
- Asignación de IP Dinámica
- Control Parental
- Servidor y cliente DHCP
- DNS Relay
- Backup y restauración de configuración
- Servidor FTP/TFTP

1.2 Aplicación

El siguiente diagrama muestra el uso del WAP-5813n en un entorno de aplicación GPON.


Data Network
Video Network
Voice Network
GPON OLT
GPON Gateway
GbE
802.11n
GbE
WAP-5813n

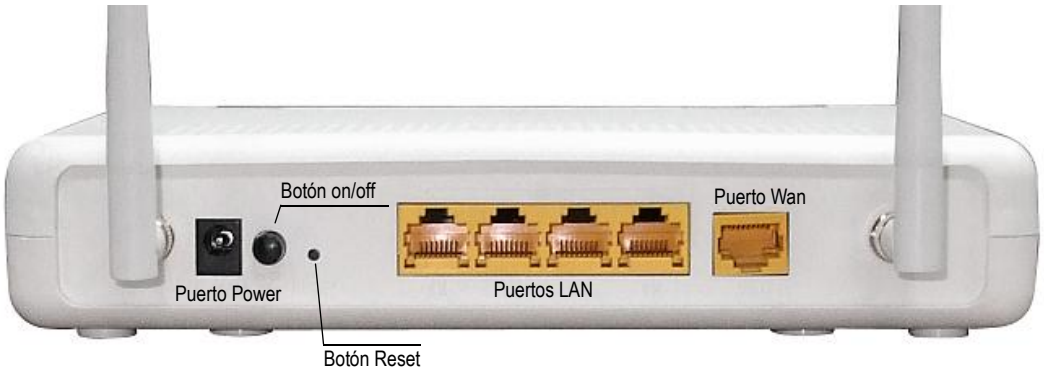
2. Instalación

2.1 Instalación Hardware

Siga las instrucciones descritas a continuación para completar la instalación hardware.

PANEL POSTERIOR

La siguiente figura muestra el panel posterior del dispositivo.



Encendido
Pulse el botón power a la posición OFF (fuera). Conecte el conector jack macho del adaptador de corriente al puerto power del router. Conecte al adaptador de corriente a una toma de corriente o enchufe eléctrico. Pulse el botón power a la posición ON (dentro). Si el indicador luminoso de encendido se ilumina, entonces el dispositivo está instalado correctamente. (Ver sección 2.2 Indicadores luminosos para más detalles)

Precaución: Si el dispositivo falla, o presenta mal función, primero verifique que el cable de corriente está conectado satisfactoriamente. Entonces pruebe a conectarlo de nuevo. Si el problema persiste contacte con el servicio técnico.

Precaución: Antes de realizar una operación de mantenimiento o desmontaje del dispositivo, desconecte todos los cables de alimentación eléctrica.

Botón Reset
Para restaurar los valores por defecto o de fábrica del dispositivo, presione el botón Reset durante al menos entre 5 y 10 segundos. Después de que el dispositivo se reinicie satisfactoriamente, el panel frontal debe mostrarse como se espera en el punto 2.2.

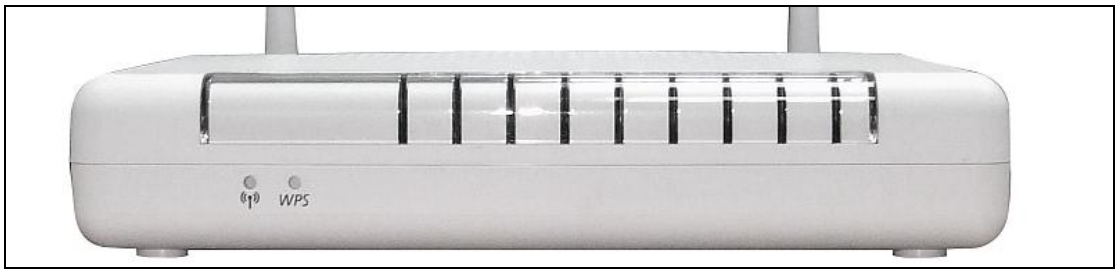
NOTA: Si presiona el botón Reset durante más de 20 segundos, el WAP-5813n mostrará la página de actualización de firmware (inicio en modo CFE). El firmware puede ser actualizado utilizando un navegador de internet introduciendo la dirección IP por defecto.

Puertos LAN ETHERNET
Utilice un cable RJ-45 para conectar hasta cuatro dispositivos. Estos puertos son auto-sensing MDI/MDX y cada uno puede ser usado con un cable recto o cruzado.

Puerto WAN ETHERNET
Utilice un cable RJ-45 para conectar un dispositivo. Esto puerto es auto-sensing MDI/MDX y puede ser usado con un cable recto o cruzado.

PANEL FRONTAL

Los botones Wi-Fi y WPS están situados en la parte izquierda del panel frontal, como se muestra en la figura.

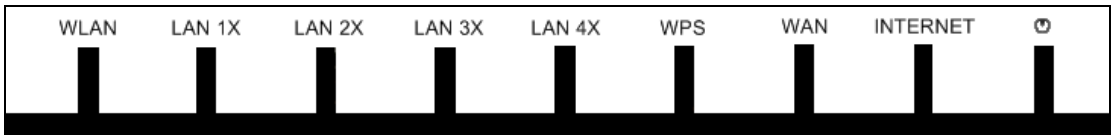


Botón WI-FI
Pulse el botón Wi-Fi para activar/desactivar el punto de acceso inalámbrico WLAN.

Botón WPS
Pulse el botón para iniciar la búsqueda de clientes WPS. Estos clientes deben soportar también el modo WPS push-button. Cuando WPS está disponible, el indicador luminoso WPS estará encendido.

2.2 Indicadores luminosos

Los indicadores luminosos están situados en el panel frontal como muestra la siguiente figura, la tabla posterior recoge una breve explicación de cada indicador luminoso.
Esta información puede ser usada para chequear el estado del dispositivo y sus conexiones.



Indicador luminoso	Color	Modo	Función
WLAN	Verde	Encendido	El modulo inalámbrico está disponible (instalado y habilitado)
		Apagado	El modulo inalámbrico no está disponible. (Ni instalado y deshabilitado).
		Parpadeando	Transmisión y recepción de datos en enlace inalámbrico.
LAN 1X-4X	Verde	Encendido	Conexión Ethernet establecida.
		Apagado	Conexión Ethernet no establecida.
		Parpadeando	Transmisión y recepción de datos en puerto LAN Ethernet

WPS	Verde	Encendido	WPS habilitado.
		Apagado	WPS deshabilitado.
		Parpadeando	El router está buscando clientes WPS.
WAN	Verde	Encendido	Conexión WAN establecida.
		Apagado	Conexión WAN no establecida.
		Parpadeando	Transmisión y recepción de datos en puerto WAN Ethernet
INTERNET	Verde	Encendido	Conexión IP y tráfico detectado únicamente en sesiones PPPoE.
		Apagado	Router apagado o en modo bridge. O el direccionamiento IP o sesión PPPoE se ha caído o perdido.
		Parpadeando	Conexión IP establecida y pasando tráfico Ip a través del dispositivo.
	Rojo	Encendido	El dispositivo está intentando establecer conexión pero esta falla, no recibe dirección IP, no se establece sesión PPPoE, fallo de autenticación PPPoE, no recibe dirección IP del IPCP, etc.
POWER (logo)	Verde	Encendido	Router inalámbrico encendido.
		Apagado	Router inalámbrico apagado.
	Rojo	Encendido	Fallo de POST (Auto testeo después de iniciar) o mal funcionamiento. Un malfuncionamiento es cualquier error o estado que muestra el dispositivo al conectarse al DSLAM, ONT, OLT o cualquier equipo cliente

3. Interfaz de usuario Web

Este apartado describe como acceder al dispositivo vía el interfaz de usuario web (WEBGUI) usando un navegador de Internet como el Internet Explorer (versión 5.0 o superior)

3.1 Parámetros por defecto

Los parámetros de fábrica o por defecto del dispositivo están indicados a continuación:

- Dirección IP LAN: 192.168.1.1
- Máscara de subred LAN: 255.255.255.0
- Acceso administrativo: (usuario: **1234** , contraseña: **1234**)
- User access (username: **user**, password: **user**)

- Dirección IP en la WAN: ninguna
- Acceso remoto via WAN: desactivado

- Punto de acceso inalámbrico (WLAN): desactivado
- Nombre de red inalámbrica o Service Set Identifier (SSID), ejemplo: WLAN_67E1

El WAP-5813 soporta los siguientes tipos de conexiones:

- PPP over Ethernet (PPPoE)
- IP over Ethernet (IPoW)
- Bridging o Bridge

Las siguientes conexiones están configuradas por defecto.

Interfaz	Tipo	Vlan Tag	Vlan Mux	IGMP	NAT	FIREWALL
eth0.3	IPoW	4	3	N	Y	N
ppp0.6	PPPoE	1	6	N	Y	Y

Nota técnica

Durante el encendido del equipo, el dispositivo carga todos los valores por defecto. Posteriormente lee el perfil de configuración almacenado de forma permanente en la memoria flash. Los atributos por defecto son sustituidos por los atributos almacenados en la flash si son diferentes. El perfil de configuración almacenado permanentemente puede ser creado via el interfaz de usuario web o Telnet u otros protocolos de gestión. La configuración por defecto puede ser restaurada cada vez que se pulse el botón de Reset más de 5 segundos hasta que los indicadores luminosos parpadeen o haciendo clic en el botón "**Restore Default configuration**" en la opción del menú web "**Restore Setting**".

3.2 Configuración IP

MODO DHCP

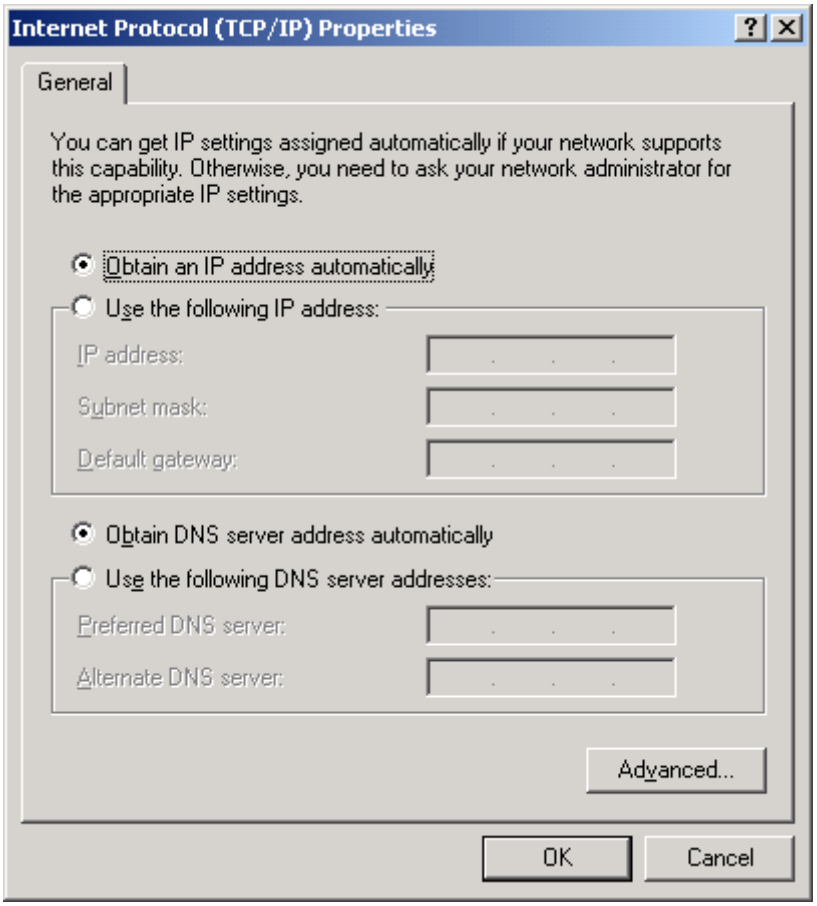
Cuando el Router inalámbrico 11n está funcionado, el servidor DHCP incluido estará levantado. Básicamente, el servidor DHCP reparte y reserva direcciones IP para los dispositivos conectados en la LAN, como puede ser un PC.
Para obtener una dirección IP el servidor DHCP, siga los pasos indicados a continuación:

NOTA:	El siguiente procedimiento asume que el usuario está utilizando un PC con Microsoft Windows XP. Sin embargo, los pasos generales son similares para la mayoría de los sistemas Operativos (SO). Consulte la documentación de su sistema Operativo para más detalles.

Paso 1: Desde la ventana de "Conexiones de Red", abra la *conexión de área local (*también se puede accede a esta ventana hacienda pulsando doble clic en el icono de *conexiones de área* local de la barra de tareas. Haga clic en el botón "**propiedades**"

Paso 2: Seleccione Protocolo Internet (TCP/IP) y haga clic en el botón "**Propiedades**".

STEP 3: Seleccione "**obtener una IP** automáticamente" como se muestra a continuación.



STEP 4: Haga clic en el botón "**OK**" para aplicar los cambios.

Si encuentra dificultades al usar el modo DHCP, puede probar a usar el modo de direccionamiento de IP estática.

Modo de direccionamiento de IP estático

En modo de direccionamiento de IP estático, asigne una dirección IP manualmente.

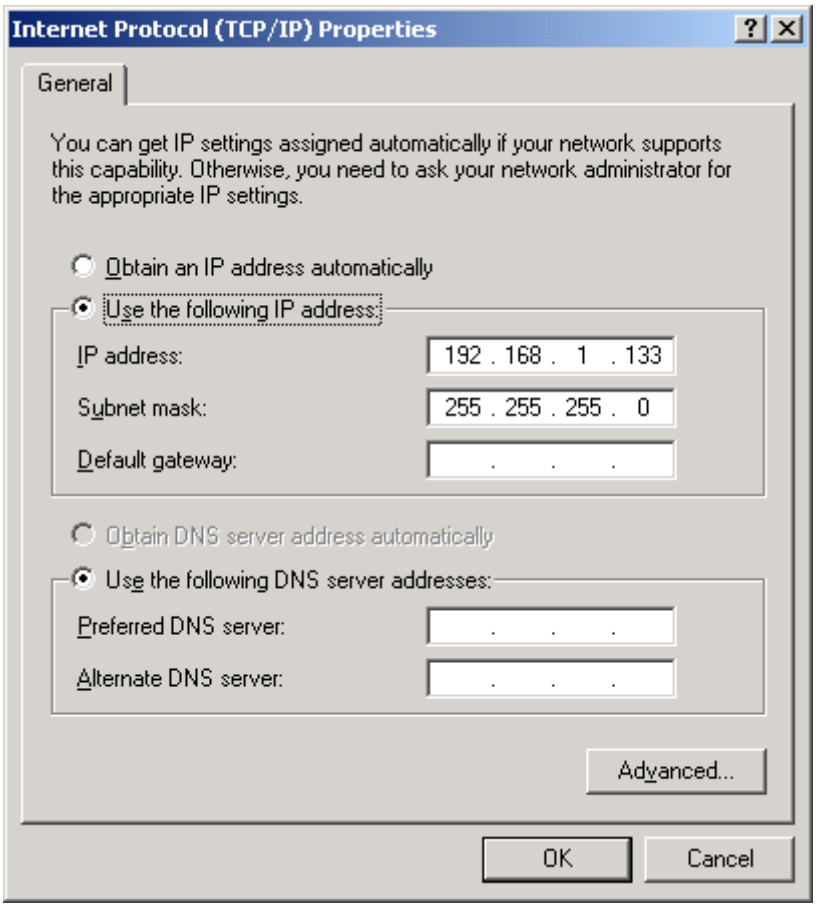
Siga estos pasos para configurar su propia dirección IP en la subred 192.168.1.x.

NOTA:	El siguiente procedimiento asume que el usuario está utilizando un PC con Microsoft Windows XP. Sin embargo, los pasos generales son similares para la mayoría de los sistemas Operativos (SO). Consulte la documentación de su Sistema Operativo para más detalles.

Paso 1: Desde la ventana de "Conexiones de Red", abra la *conexión de área local (*también se puede accede a esta ventana hacienda pulsando doble clic en el icono de *conexiones de área* local de la barra de tareas. Haga clic en el botón "**Propiedades**"

Paso 2: Seleccione Protocolo Internet (TCP/IP) y haga clic en el botón "**Propiedades**".

Paso 3: Cambie la dirección IP a una IP dentro del rango 192.168.1.x (1<x<255) con máscara de subred 255.255.255.0 como se muestra a continuación.



Paso 4: Haga clic en el botón "**OK**" para aplicar los cambios.

3.3 Procedimiento de inicio de sesión

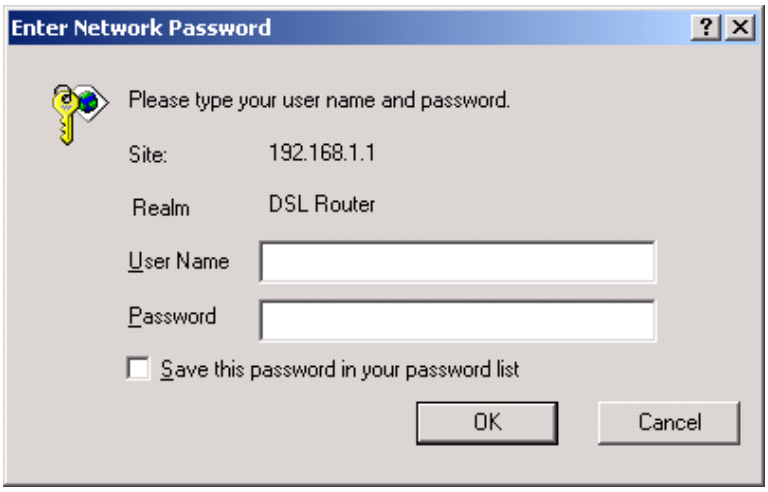
Realice los siguientes pasos para acceder a la interfaz de usuario web.

NOTA:	Puede encontrar los parámetros por defecto en el apartado 0.

STEP 1: Inicie el navegador de Internet e introduzca la dirección IP del dispositivo en la barra de direcciones web. Por ejemplo: http://192.168.1.1.

NOTA:	Para administración Local (por ejemplo acceso LAN), el PC que ejecuta el navegador de Internet debe estar conectado al Puerto Ethernet del Router

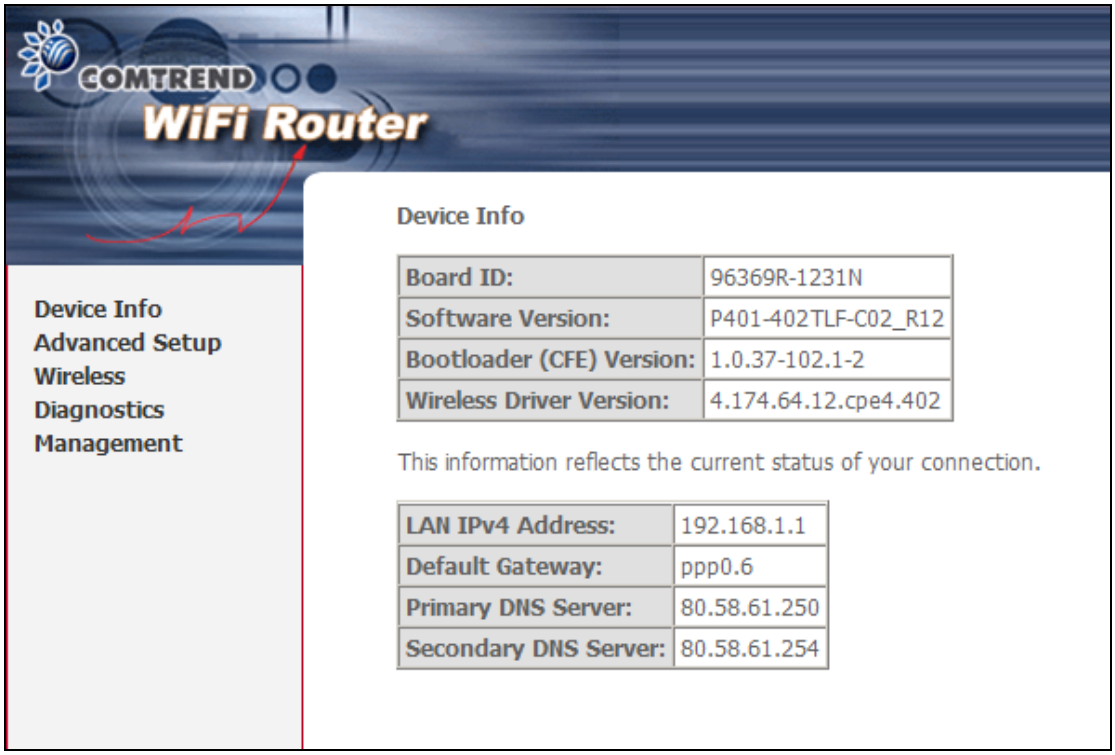
Paso 2: El siguiente cuadro de diálogo aparecerá, como se indica a continuación. Introduzca el nombre de usuario y contraseña. Introduzca los valores de usuario y contraseña por defecto como se indica en el apartado 3.1 Configuración por defecto.



Haga clic en el botón "**OK**" para continuar

NOTA:	La contraseña de acceso puede ser cambiada posteriormente (ver apartado 8.5.1)

Paso 3: Después de acceder satisfactoriamente la primera vez, se le mostrará la siguiente pantalla.



4. Información de dispositivo

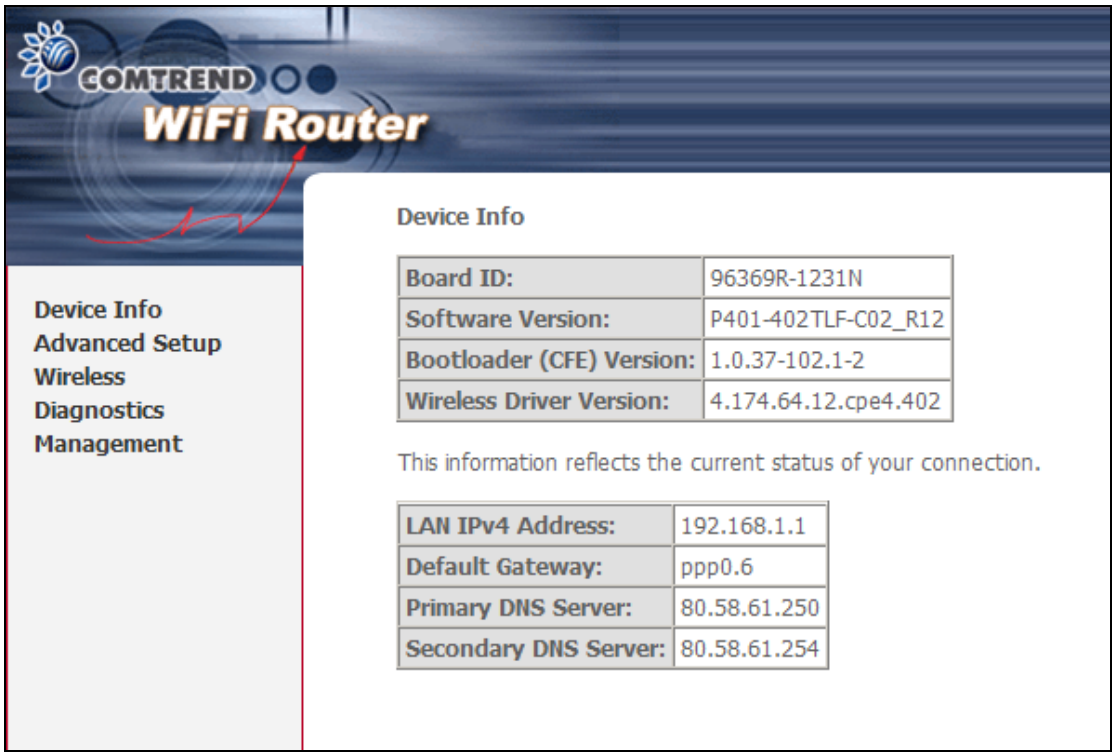
El interfaz de usuario Web está dividido en dos paneles, el menú principal (a la izquierda) y ventana de contenidos (a la derecha). El menú principal tiene varias opciones y seleccionando cada una de ellas se abrirá un submenú con más opciones a seleccionar.

NOTA:	Los detalles mostrados en el menú están basados en las conexiones configuradas y los privilegios de la cuenta de usuario. Por ejemplo, si NAT y Firewall están activados, el menú principal mostrará los submenús NAT y Security. Si están deshabilitados, se mostraran los menús y submenús correspondientes.

"**Device Info"** es la primera selección del menú principal y la primara en mostrarse. Posteriormente se mostrará una introducción.

Posteriormente los capítulos introducirán la secuencia de otras opciones del menú principal.

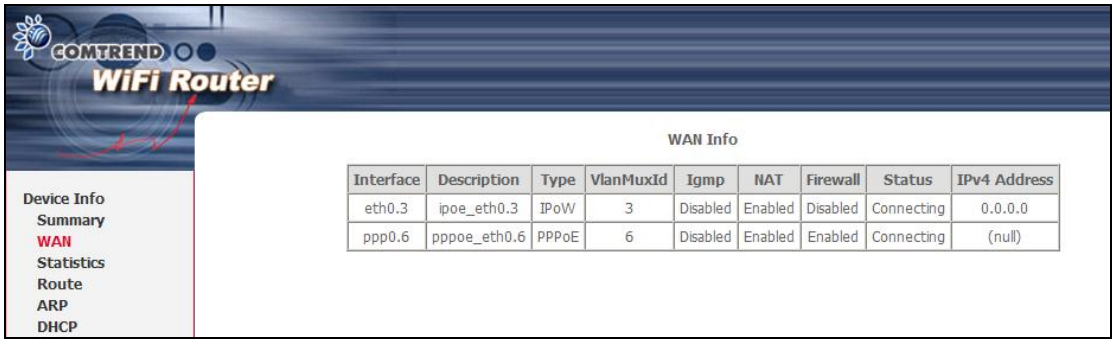
La pantalla Device Info Summary se mostrará al inicio.



Esta pantalla muestra la información relativa al hardware, software, configuración IP, etc.

4.1 WAN

Seleccione el submenú WAN del menú Device Info para mostrar los PVCs configurados.



Título	Descripción
Interfaz	Nombre del interfaz WAN
Descripción	Nombre de la conexión WAN
Tipo	Muestra los tipos de conexión
VlanMuxId	Muestra el ID 802.1Q de la VLAN
IGMP	Muestra el estado de Internet Group Management Protocol (IGMP)
NAT	Muestra el estado de Network Address Translation (NAT)
Firewall	Muestra el estado del Firewall
Status	Lista el estado de conexión DSL
IPv4 Address	Muestra la dirección IPv4 para el interfaz WAN

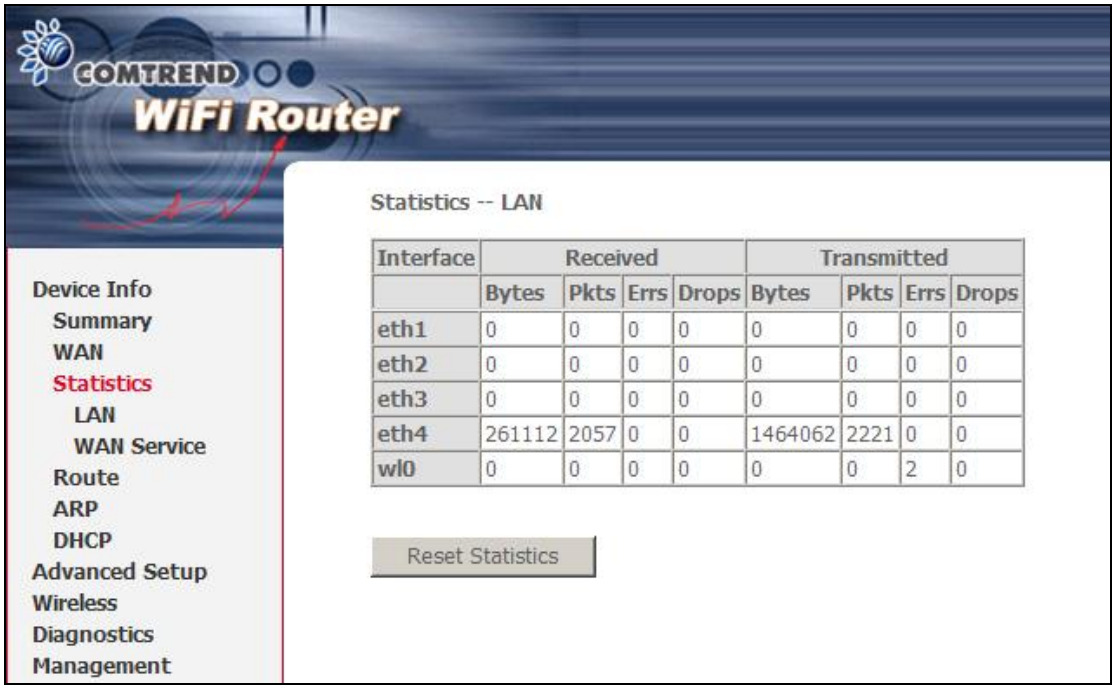
4.2 Estadísticas

Esta sección muestra las estadísticas facilitadas por los diferentes interfaces LAN, WAN, ATM y ADSL

NOTA:	Esta pantalla se actualiza cada 15 segundos.

4.2.1 Estadísticas LAN

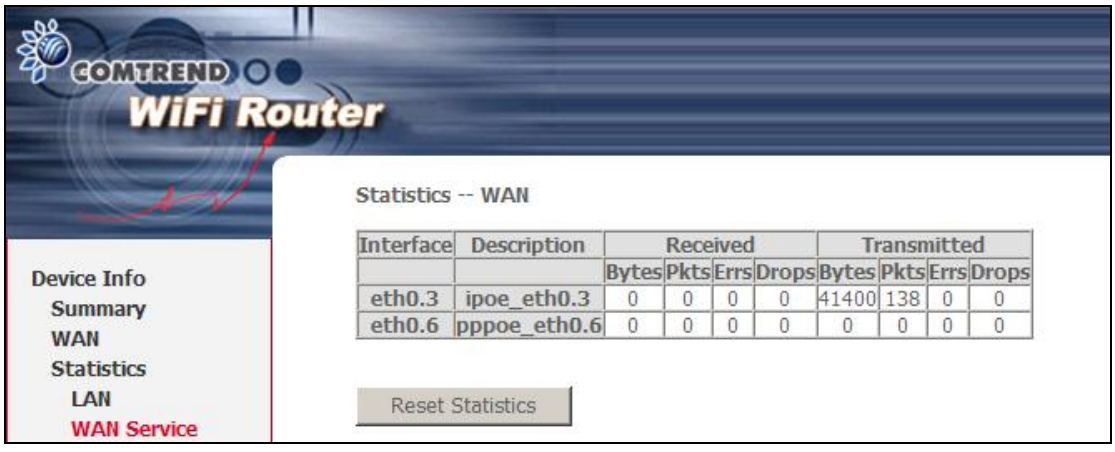
Esta pantalla muestra las estadísticas de tráfico de datos para cada interfaz LAN.



Título	Descripción
Interfaz	LAN interface(s)
Recibido/Transmitido: - Bytes - Pkts - Errs - Drops	Número de Bytes Número de paquetes Número de paquetes con errores Número de paquetes perdidos

4.3 Estadísticas WAN

Esta pantalla muestra las estadísticas de cada interfaz WAN.



Titulo	Descripción
Interfaz	Interfaces WAN
Descripción	Etiqueta de servicio WAN

Titulo		Descripción
Recibido/Transmitido	- Bytes - Pkts - Errs - Drops	Número de Bytes Número de paquetes Número de paquetes con errores Número de paquetes perdidos

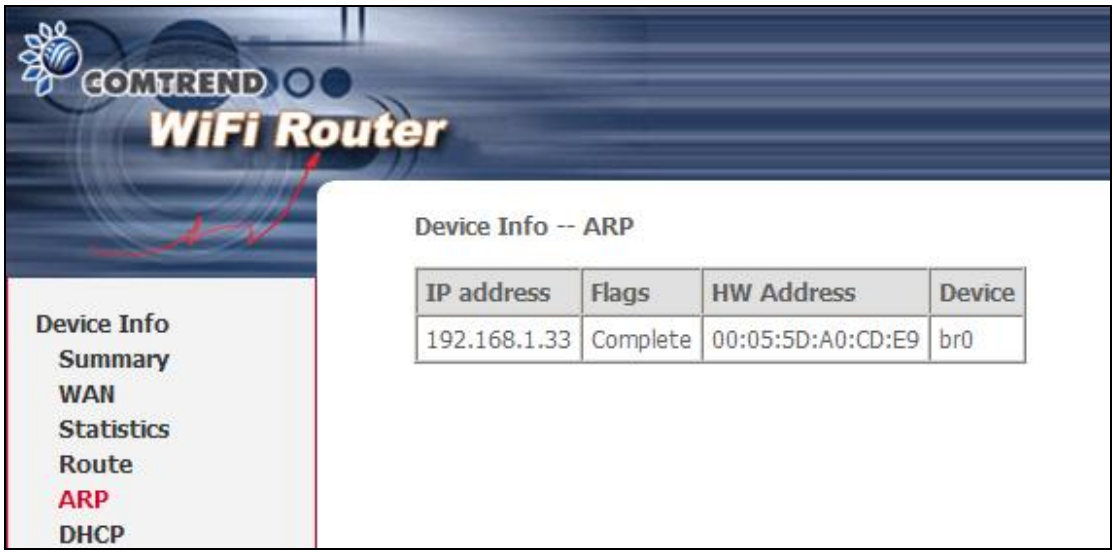
4.4 Enrutamiento

Seleccione **Route** para mostrar las rutas que el WAP-5813n ha encontrado.

Campo	Descripción
Destino	Red de destino o Host de destino
Gateway	Puerta de enlace
Subnet Mask	Máscara de subred de destino
Flag	U: ruta está activa !: ruta rechazada G: Gateway en uso H: el objetivo es un host R: restablecer la ruta para enrutamiento dinámico D: redirección o subred para configuración dinámica. M: Modificado desde la subred enrutada o redirigida
Metric	La "distancia" al objetivo (normalmente contada en saltos).
Service	Muestra la etiqueta de conexiones WAN
Interface	Muetras la conexión de las interfaces

4.5 ARP

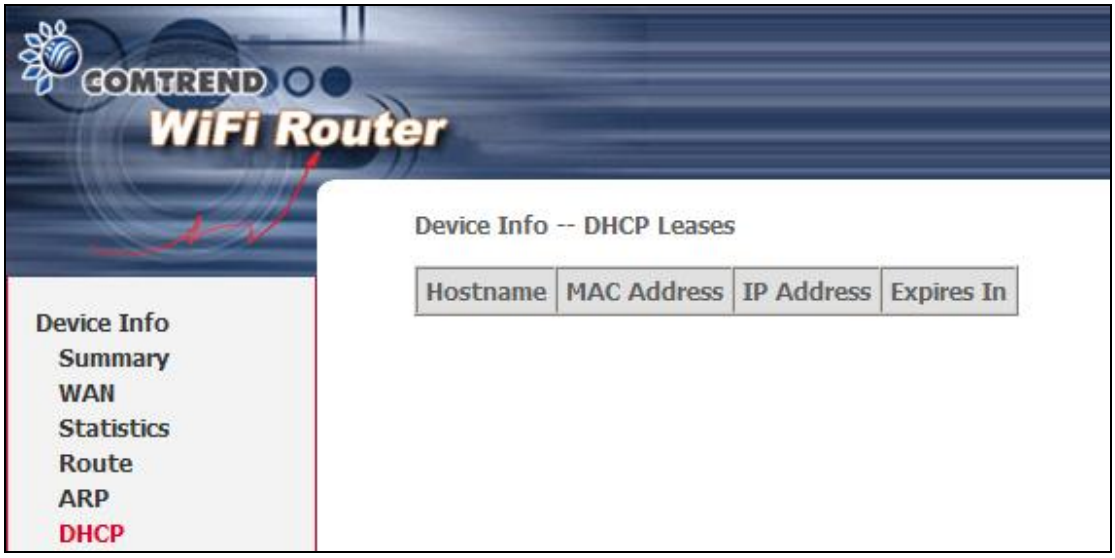
Seleccione **ARP** para mostrar la información ARP.



Campo	Descripción
IP address	Muestra la dirección de cada host o PC
Flags	Complete, Incomplete, Permanent, or Publish
HW Address	Muestra la dirección MAC del host o PC
Device	Muestra el interfaz de conexión

4.6 DHCP

Seleccione **DHCP** para mostrar todos los DHCP Leases.



Campo	Descripción
Hostname	Muestra el nombre de red del dispositivo/host/PC
MAC Address	Muestra la dirección MAC del dispositivo/host/PC

Campo	Descripción
IP Address	Muestra la dirección IP del dispositivo/host/PC
Expires In	Muestra cuanto tiempo le queda a cada DHCP Lease

5. Configuración Avanzada

Este capítulo explica las siguientes opciones del menú:

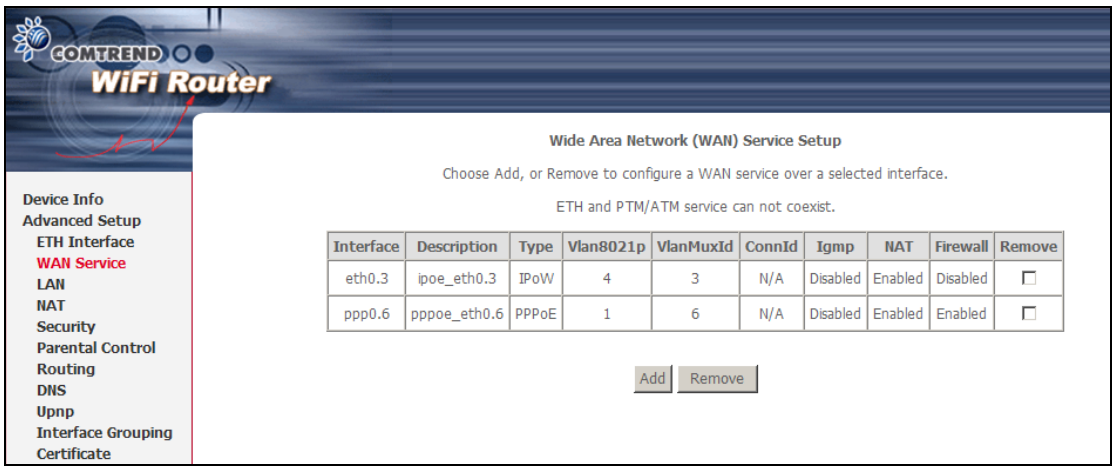
5.1 ETH WAN INTERFACE

Esta pantalla muestra la configuración de "**Ethernet WAN Interface**".

Título	Descripción
Interface/ (Name)	ETH WAN Interface
Connection Mode	Default Mode – Único servicio para una conexión Vlan Mux Mode – Múltiples servicios de VLAN para una conexión MSC Mode – Múltiples servicios para una conexión
Remove	Seleccionar la casilla de verificación y haga clic para eliminar la conexión.

5.2 WAN

Esta pantalla muestra la configuración de los interfaces WAN en "**WAN Service**".

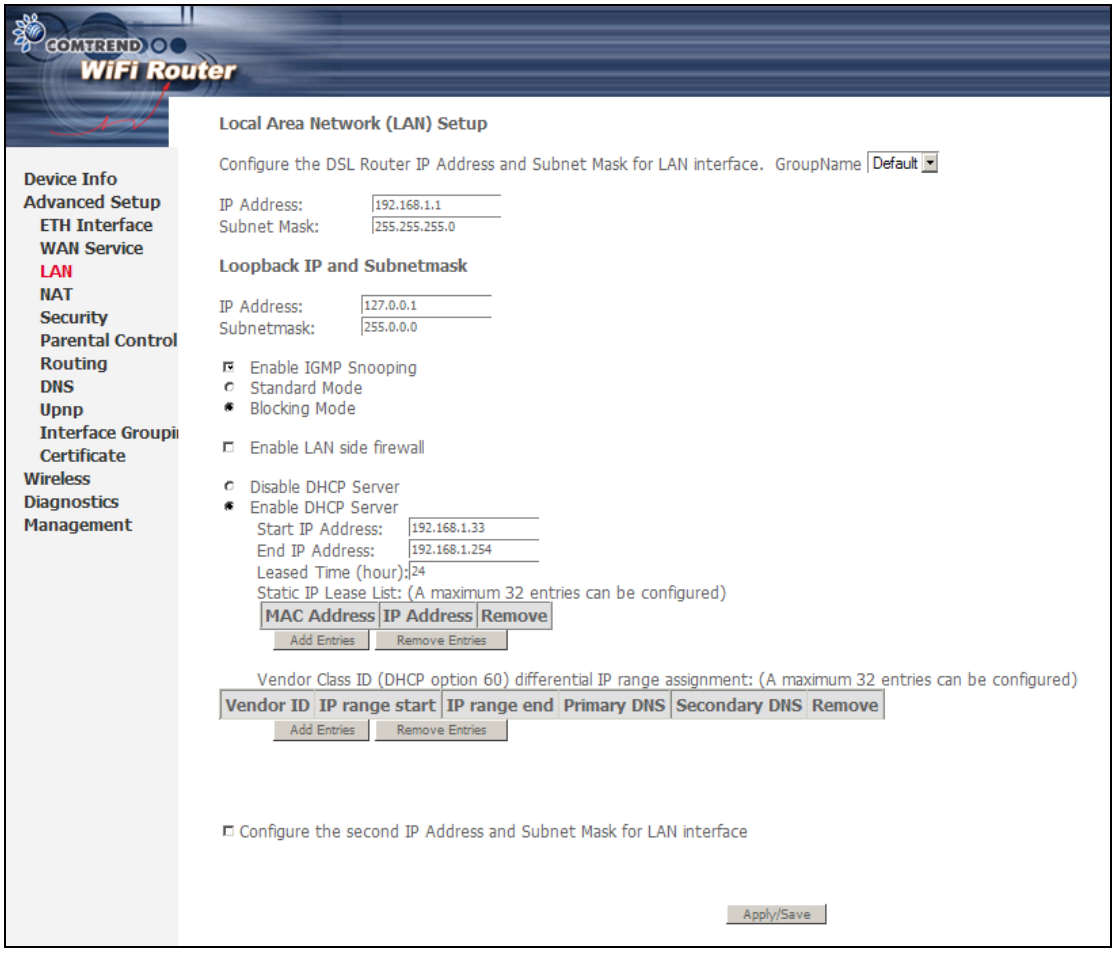


Titulo	Descripción
Interface	Nombre del interfaz para la WAN
Description	Nombre de la conexión WAN
Type	Muestra el tipo de conexión
Vlan8021p	VLAN ID es usado para VLAN Tagging (IEEE 802.1Q)
VlanMuxId	Muestra 802.1Q VLAN ID
IGMP	Muestra el estado de Internet Group Management Protocol (IGMP)
NAT	Muestra el estado de Network Address Translation (NAT)
Firewall	Muestra el estado de Firewall
Status	Estado de la conexión DSL
IPv4 Address	Muestra la dirección IPv4 de la WAN

Para eliminar una conexión, seleccione la casilla de verificación correspondiente y haga clic en el botón "**Remove**".
Para añadir una conexión, haga clic en el botón "**Add**" y siga las instrucciones.

5.3 LAN

Desde esta pantalla, la configuración del interfaz LAN puede ser realizada.



NOTA: El NAT está habilitado de manera que la opción **DHCP Server Relay** está oculta. (Ver notas subrayadas a continuación).

Consulte la descripción del campo a continuación para más detalles.

LOCAL AREA NETWORK (LAN) SETUP

GroupName: Puede ignorar esta casilla de verificación.

IP Address: Introduzca la dirección IP para la LAN.

Subnet Mask: Introduzca la máscara de subred de la LAN.

LOOPBACK IP AND SUBNETMASK

IP Address: Introduzca la dirección IP.

Subnet Mask: Introduzca la máscara de subred.

Enable IGMP Snooping: Marque la casilla de verificación para activarlo☑.

Standard Mode**:** En modo estándar, el tráfico multicast inundará todos los puertos cuando no haya ningún cliente suscrito a un grupo multicast, incluso si IGMP snooping está activado.

Blocking Mode**:** En modo bloqueo, el tráfico de datos multicast será bloqueado y no inundará todos los puertos

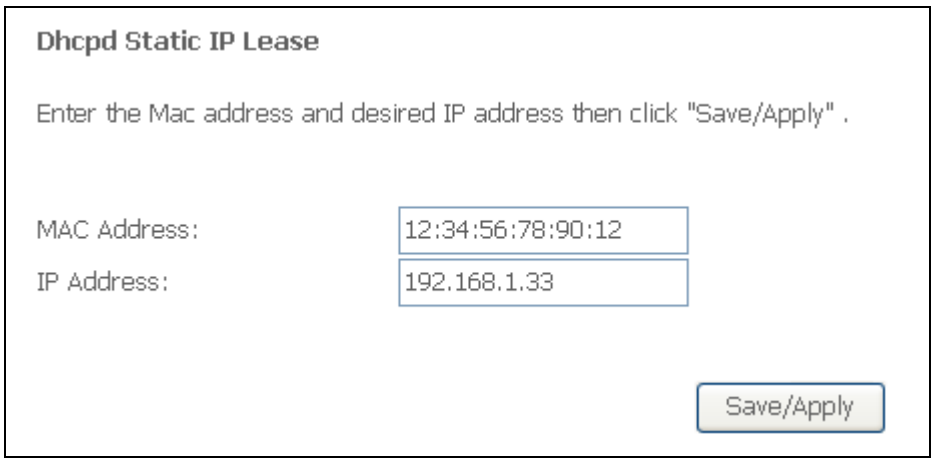
cuando no haya clientes suscritos a un grupo multicast

Enable LAN side firewall: Marque la casilla de verificación para activarlo☑.

DHCP Server: para activar el DHCP, seleccione **Enable DHCP server** e introduzca la dirección IP de inicio y de final del rango y el tiempo de préstamo de dirección IP (Leased Time). Estos parámetros configuran el router para asignar automáticamente dirección IP, puerta de enlace por defecto y servidores DNS a cada PC de la LAN.

Static IP Lease List: Pueden ser configuradas un máximo de 32 entradas.

Para añadir una entrada, introduzca la dirección MAC y la dirección IP estática y posteriormente haga clic en el botón "**Save/Apply**".

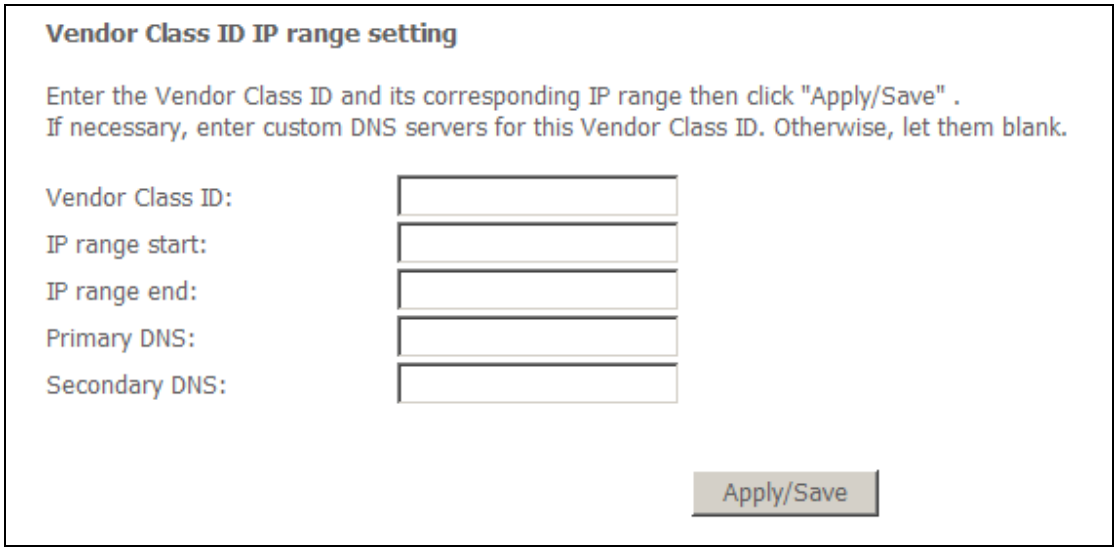


Para eliminar una entrada, marque la casilla de verificación correspondiente ☑ en la columna "**Remove**" y haga clic en el botón "**Remove Entries**", como se muestra a continuación.

DHCP Server Relay: Activado con la casilla de verificación marcada ☑ e introduzca la dirección IP del servidor DHCP. Esto permite al router retransmitir los paquetes DHCP del servidor DHCP remoto. El servidor DHCP remoto facilitará la dirección IP. *Esta opción estará oculta si el NAT está habilitado o cuando el router esté configurado con un solo PVC en modo Bridge.*

Vendor Class ID: Pueden ser configuradas un máximo de 32 entradas. Para eliminar una entrada, marque la casilla de verificación correspondiente ☑ en la columna "**Remove**" y haga clic en el botón "**Remove Entries**".

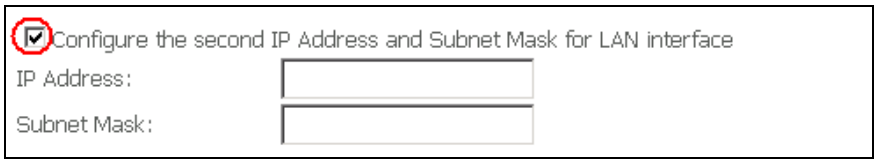
Para añadir una entrada, haga clic en el botón "**Add Entries**". La siguiente imagen muestra lo que se visualizará en pantalla.



Introduzca los parámetros correspondientes en cada uno de los campos de configuración y haga clic en el botón "**Apply/Save**".

2ND LAN INTERFACE

Para configurar una IP secundaria, marque la casilla de verificación ☑ marcada en rojo como se muestra a continuación.



IP Address: Introduzca la IP secundaria para la LAN.

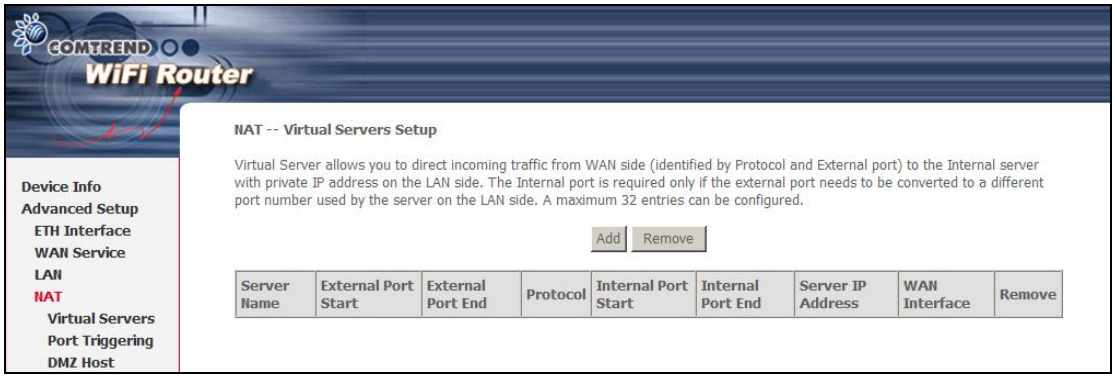
Subnet Mask: Introduzca la máscara de subred secundaria para la LAN.

5.4 NAT

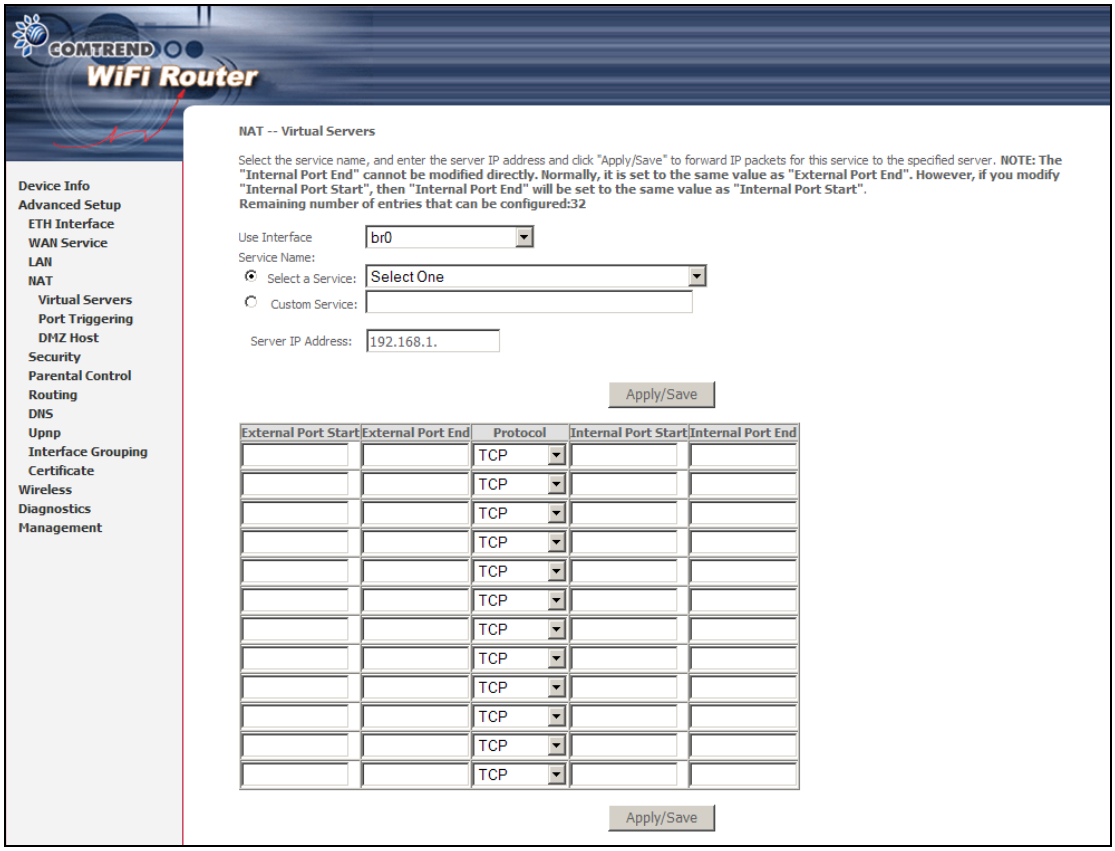
Nota: Para seleccionar esta opción, el NAT debe estar habilitado en al menos un PVCT. (La opción *NAT no está disponible en modo bridge)*

5.4.1 Virtual Servers

Virtual Servers o servidores virtuales permiten redirigir el tráfico entrante desde la WAN (identificando Protocolo y Puerto externo) a un servidor interno con dirección privada en el lado de la LAN. Los puertos internos son requeridos solo si el Puerto externo necesita ser convertido a un Puerto interno diferente para ser usado por el servidor interno del lado de la LAN.
Pueden ser configuradas un máximo de 32 entradas.



Para añadir un "**Virtual Server"**, haga clic en el botón "**Add**". Se mostrará la siguiente pantalla:



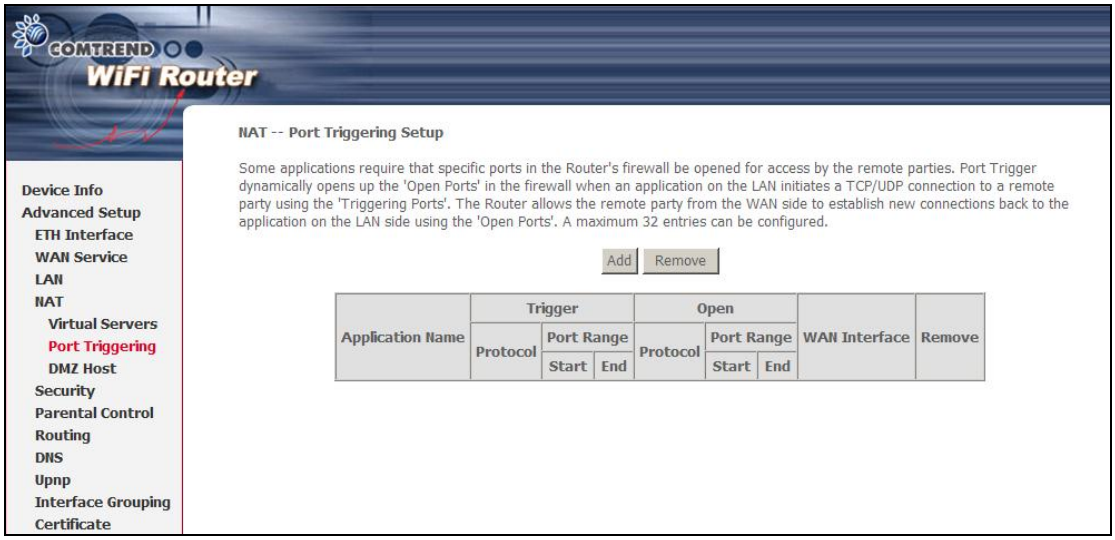
Consulte la siguiente tabla para la descripción de cada campo.

Campo/Título	Descripción
Use Interface	Seleccione el interfaz WAN de la lista desplegable.
Select a Service **Or** Custom Server	Seleccione un servicio de la lista desplegable **O** Cree un servicio personalizado introduciendo el nombre.
Server IP Address	Introduzca la dirección IP del servidor interno
External Port Start	Introduzca el puerto externo de inicio de rango (cuando seleccione un servicio personalizado o "**Custom Server"**). Cuando un servicio es seleccionado, el rango de puertos se configura automáticamente.

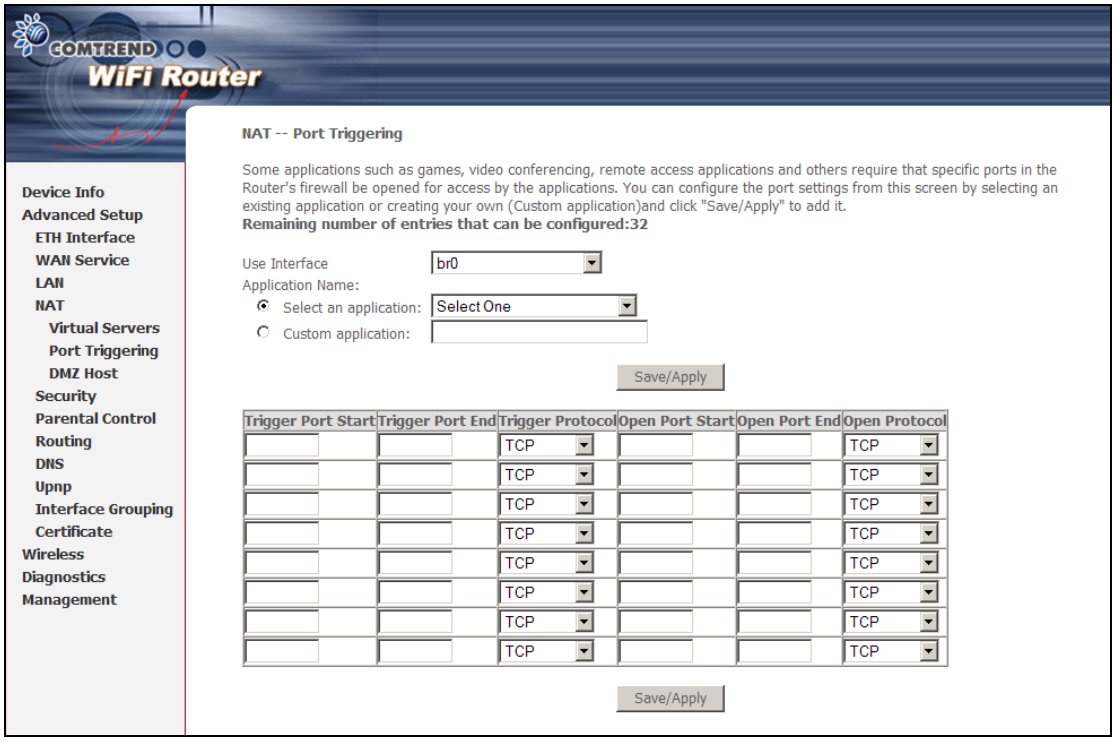
Campo/Título	Descripción
External Port End	Introduzca el puerto externo de fin de rango (cuando seleccione un servicio personalizado o "**Custom Server**"). Cuando un servicio es seleccionado, el rango de puertos se configura automáticamente.
Protocol	TCP, TCP/UDP, o UDP.
Internal Port Start	Introduzca el puerto interno de inicio de rango (cuando seleccione un servicio personalizado o "**Custom Server**"). Cuando un servicio es seleccionado, el rango de puertos se configura automáticamente.
Internal Port End	Introduzca el puerto interno de fin de rango (cuando seleccione un servicio personalizado o "**Custom Server**"). Cuando un servicio es seleccionado, el rango de puertos se configura automáticamente.

5.4.2 Port Triggering

Algunas aplicaciones requieren que los puertos cuenten con acceso permitido en el firewall. Port Triggers dinámicamente "abre los puertos" en el firewall sólo cuando la aplicación del lado de la LAN inicia la conexión TCP/UDP a un sitio remoto usando "triggering Ports". El router permite al sitio remoto desde el lado de la WAN establecer nuevas conexiones a la aplicación del lado de la LAN usando los "puertos abiertos".
Pueden ser configuradas un máximo de 32 entradas.



Para añadir un "**Trigger Port**", haga clic en el botón "**Add**". Se mostrará la siguiente pantalla:



Consulte la siguiente tabla para la descripción de cada campo.

Campo/Titulo	Descripción
Use Interface	Seleccione el interfaz WAN de la lista desplegable.
Select an Application **Or** Custom Application	Seleccione un servicio de la lista desplegable **O** Cree un servicio personalizado introduciendo el nombre.
Trigger Port Start	Introduzca el número de Puerto Trigger de inicio de rango (cuando seleccione un servicio personalizado o "**Custom Server"**). Cuando un servicio es seleccionado, el rango de puertos se configura automáticamente.
Trigger Port End	Introduzca el número de Puerto Trigger de fin de rango (cuando seleccione un servicio personalizado o "**Custom Server"**). Cuando un servicio es seleccionado, el rango de puertos se configura automáticamente.
Trigger Protocol	TCP, TCP/UDP, o UDP.
Open Port Start	Introduzca el número de Puerto "abierto" de inicio de rango (cuando seleccione un servicio personalizado o "**Custom Server"**). Cuando un servicio es seleccionado, el rango de puertos se configura automáticamente.
Open Port End	Introduzca el número de Puerto "abierto" de fin de rango (cuando seleccione un servicio personalizado o "**Custom Server"**). Cuando un servicio es seleccionado, el rango de puertos se configura automáticamente.
Open Protocol	TCP, TCP/UDP, o UDP.

5.4.3 DMZ Host

El router permitirá del lado WAN hacia el Host DMZ a aquellos paquetes que no pertenezcan a aplicaciones configuradas en la tabla de "**Virtual Server**".

Para activar el Host DMZ, introduzca la dirección IP y haga clic en el botón "**Save/Apply**".

Para desactivar el host DMZ, borre la dirección IP y haga clic en el botón "**Save/Apply**".

5.5 Security

Para que esta opción esté disponible, debe estar habilitado el firewall en la configuración WAN.
Para descripción de detalles, con ejemplos, por favor consulte el 0 Apéndice A – Firewall.

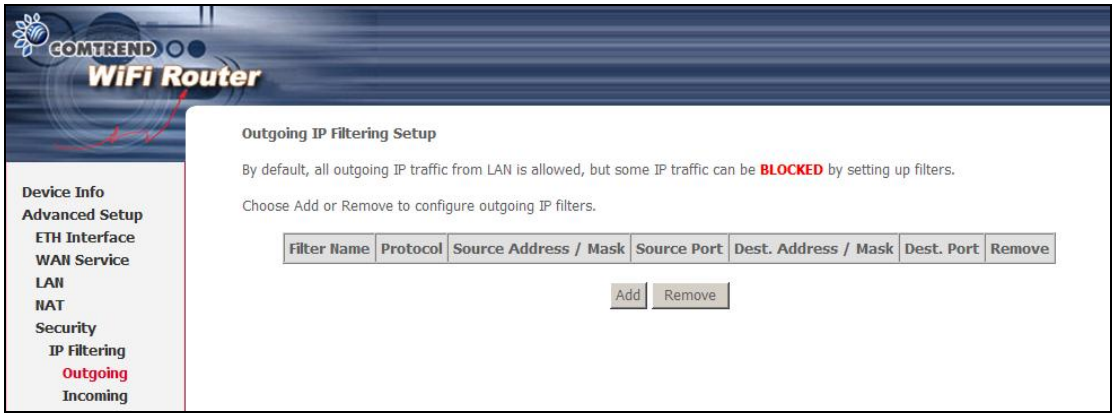
5.5.1 IP Filtering

Esta opción permite configurar filtros o reglas que limitan el tráfico IP de entrada o de salida (Outgoing/Incoming). Múltiples reglas de filtrado pueden ser configuradas y aplicadas en cada una al menos con una condición de limitación. Para paquetes IP individuales para pasar el filtro debe cumplir cada una de las condiciones.

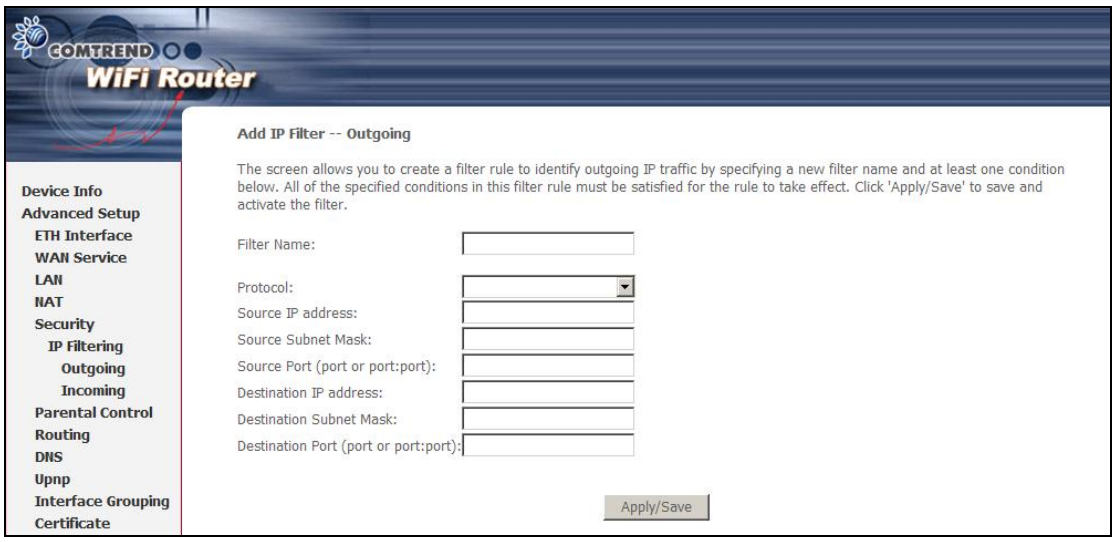
NOTA:	Esta función no estará disponible en modo Bridge. This function is not available when in bridge mode. En cambio, MAC Filtering , desempeña una función similar.

OUTGOING IP FILTER

Por defecto, todo el tráfico IP saliente está permitido, pero este tráfico IP puede ser bloqueado con filtros.



Para añadir un filtro (para bloquear tráfico IP saliente), haga clic en el botón "**Add**". En la siguiente pantalla, introduzca los criterios de filtrado y haga clic en el botón "**Apply/Save**".

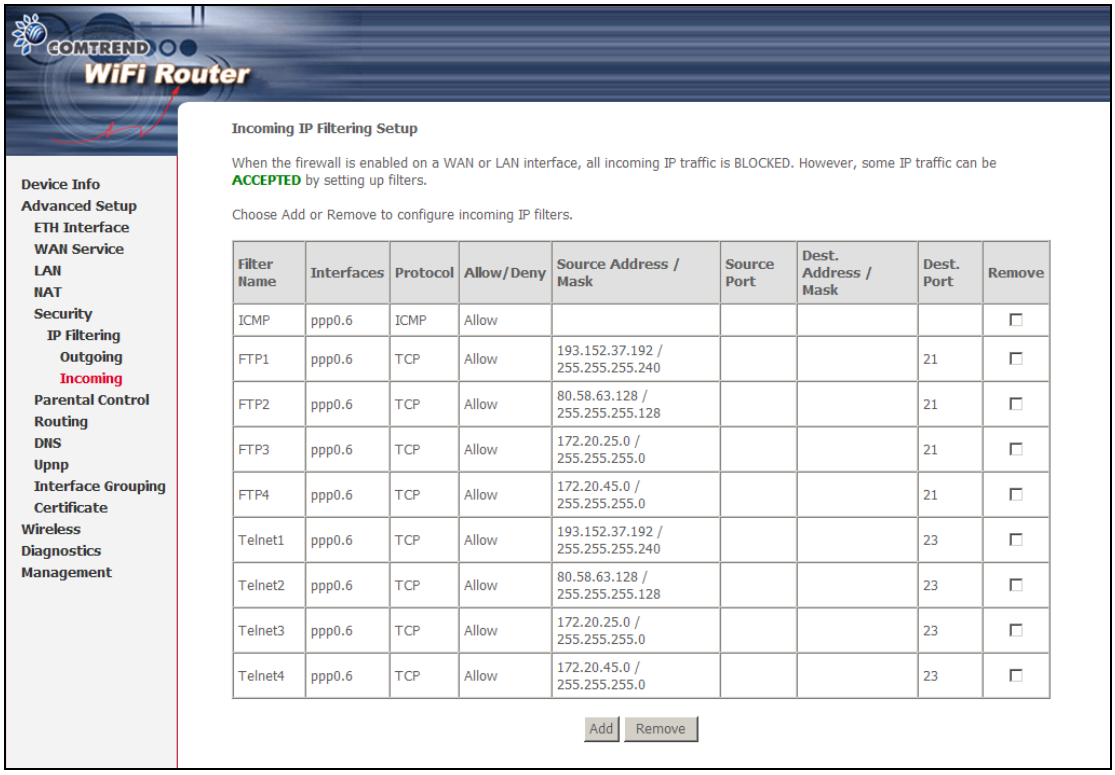


Consulte la siguiente tabla para la descripción de cada campo.

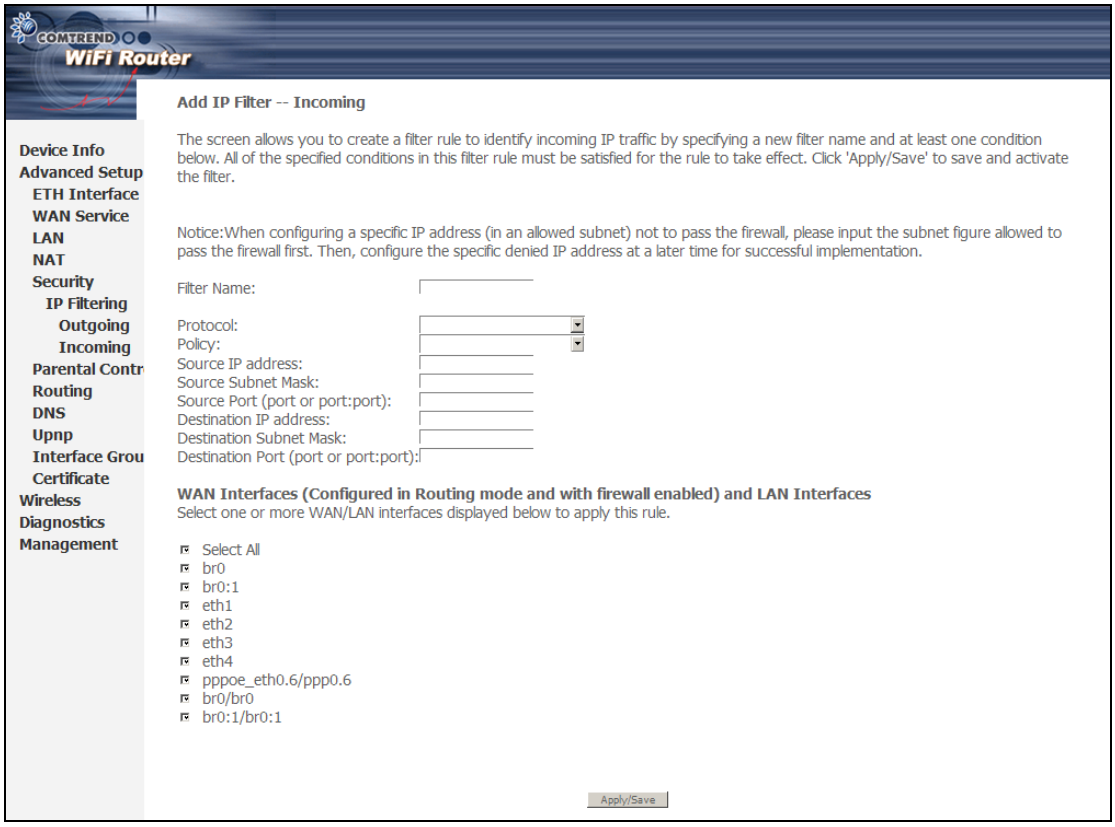
Campo	Descripción
Filter Name	Etiqueta de regla de filtrado
Protocol	TCP, TCP/UDP, UDP, o ICMP.
Source IP address	Introduzca la dirección IP origen.
Source Subnet Mask	Introduzca la máscara de sub red origen.
Source Port (port or port: port)	Introduzca el número de Puerto origen del rango.
Destination IP address	Introduzca la dirección IP de destino.
Destination Subnet Mask	Introduzca la máscara de subred de destino.
Destination Port (port or port: port)	Introduzca el número de puerto destino del rango

INCOMING IP FILTER

Por defecto, todo el tráfico entrante está bloqueado, pero puede ser permitido creando filtros.



Para nadir un filtro (para permitir tráfico entrante), haga clic en el botón "**Add**" En la siguiente pantalla, introduzca los criterios de filtrado y haga clic en el botón " **Apply/Save**".



Consulte la siguiente tabla para la descripción de cada campo.

Campo	Descripción
Filter Name	Etiqueta de regla de filtrado
Protocol	TCP, TCP/UDP, UDP, o ICMP.
Policy	Permite o deniega el tráfico IP
Source IP address	Introduzca la dirección IP origen.
Source Subnet Mask	Introduzca la máscara de subred de destino.
Source Port (port or port: port)	Introduzca Puerto o rango de origen.
Destination IP address	Introduzca la dirección IP de destino.
Destination Subnet Mask	Introduzca la máscara de subred de destino.
Destination Port (port or port: port)	Introduzca Puerto o rango de destino.

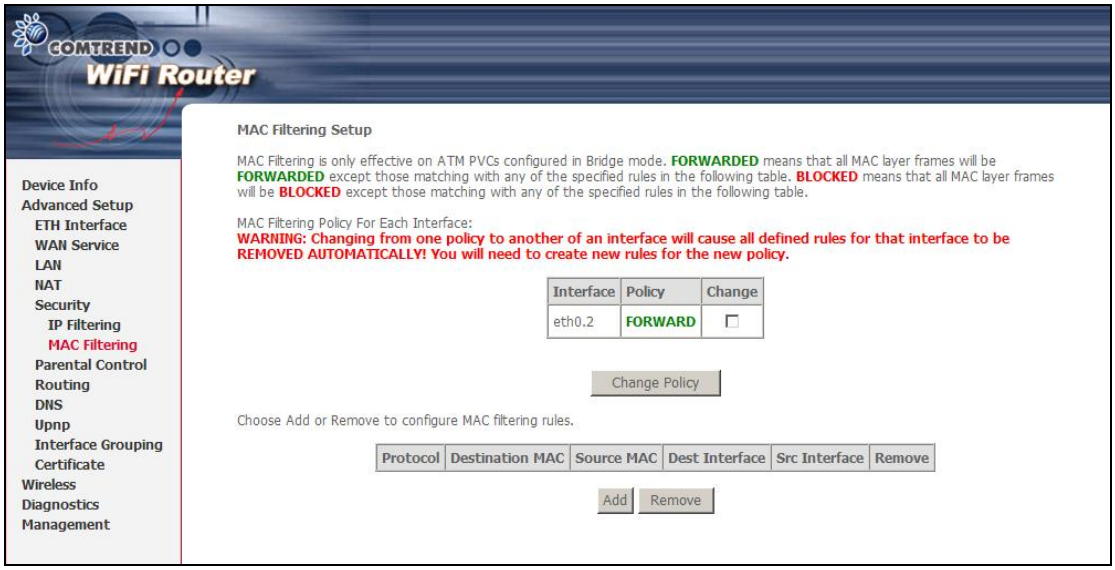
En la imagen superior, seleccione el interfaz WAN y LAN en los que serán aplicados las reglas de filtrado. Debe seleccionar todos o solo un subconjunto. Con interfaces WAN en modo bridge o sin firewall activado no estará disponible.

5.5.2 MAC Filtering

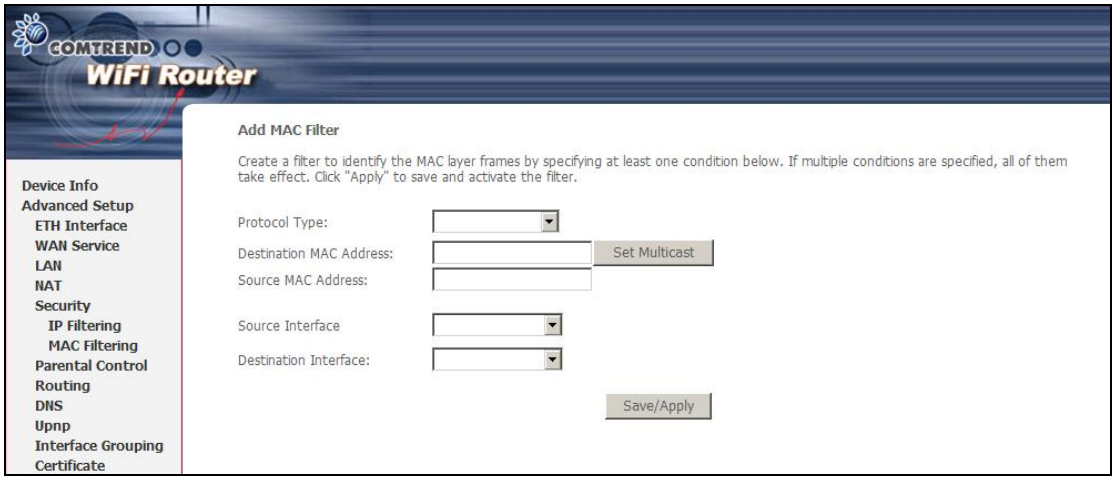
NOTA:	Esta opción solo está disponible en modo Bridge. Para otros modos usar IP Filtering para conseguir una funcionalidad similar.

Cada dispositivo de red tiene una única dirección MAC de 48 bit. Esta puede ser usada para filtrar (bloquear o permitir) paquetes basándose en el dispositivo origen. Las políticas o reglas de filtrado MAC para el WAP-5813n pueden ser configuradas de acuerdo al siguiente procedimiento.

El "**MAC Filtering Global Policy**" está definido como se indica a continuación. **FORWARDED** indica que todos los frames en la capa MAC serán **FORWARDED** (permitidos) excepto aquellos que coincidan con las reglas de filtrado MAC. **BLOCKED** indica que los frames de la capa MAC serán **BLOCKED** (bloqueados) excepto aquellos que coincidan con las reglas de filtrado MAC. Por defecto la regla "**MAC Filtering Global**" está configurado como **FORWARDED**. Para cambiar su valor, haga clic en el botón "**Change Policy**".



Haga clic en el botón "**Add**" o en el botón "**Remove**" para configurar las reglas de filtrado MAC. La siguiente imagen aparecerá al hacer clic en el botón "**Add**". Crear un filtro para identificar frames en la capa MAC puede especificar al menos una condición. Si especifica más condiciones, todas ellas deben cumplirse. Haga clic en el botón "**Save/Apply**" para salvar y activar la regla de filtrado.



Consulte la siguiente tabla para la descripción de cada campo.

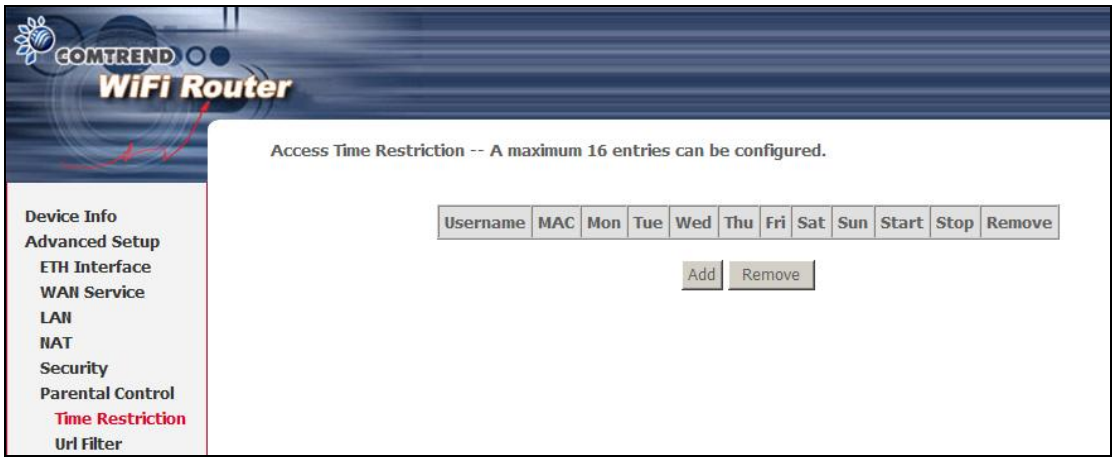
Campo	Descripción
Protocol Type	PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI, IGMP
Destination MAC Address	Define la dirección MAC de destino
Source MAC Address	Define la dirección MAC de origen
Source/Destination Interfaces	Aplica el filtro a las interfaces WAN seleccionadas.

5.6 Parental Control

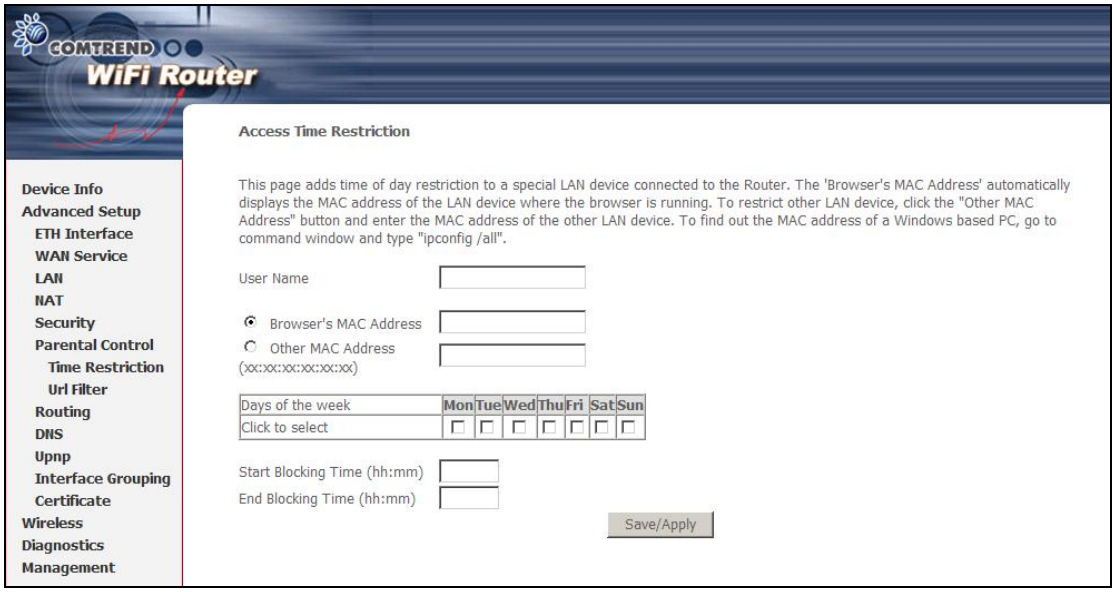
Esta sección proporciona información de la funcionalidad "**Control Paterno**", "**Parental control**" en inglés.

5.6.1 Time Restriction

Esta característica restringe el acceso desde un dispositivo LAN a un lugar en el exterior de la red a determinadas horas en los días seleccionados. Para asegurar que esta funcionalidad está activa, la sincronización "Internet Time server" o NTP debe estar activado como indica el apartado 8.4, de modo que los periodos de tiempo seleccionados coincida con su hora local.



Haga clic en el botón "**Add**" para mostrar la siguiente pantalla.



Haga clic en el botón "**Save/Apply**" para añadir un periodo de restricción.

Ver la descripción de campos a continuación.

User Name: una etiqueta definida de usuario para la restricción.

Browser's MAC Address: Dirección MAC del PC que inicia su navegador.

Other MAC Address: Dirección MAC de otro dispositivo LAN.

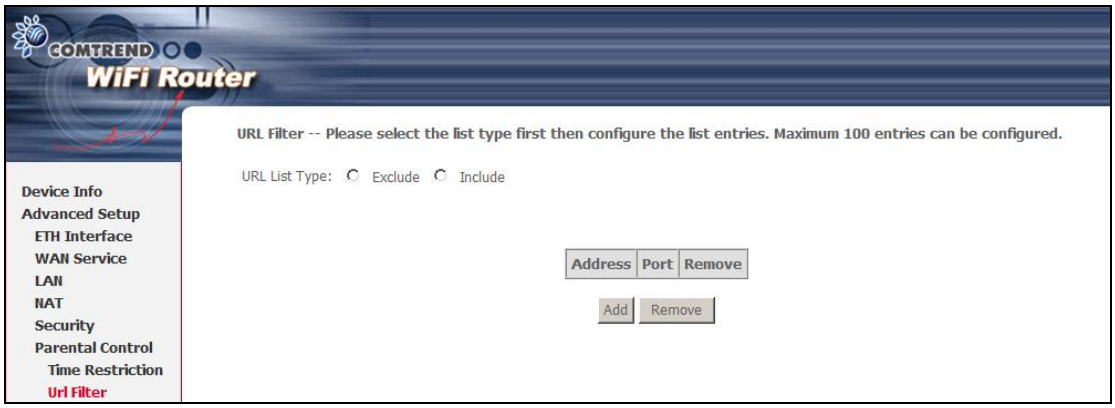
Days of the Week: Los días en que la restricción será aplicada.

Start Blocking Time: El tiempo en el que se inicia la restricción.

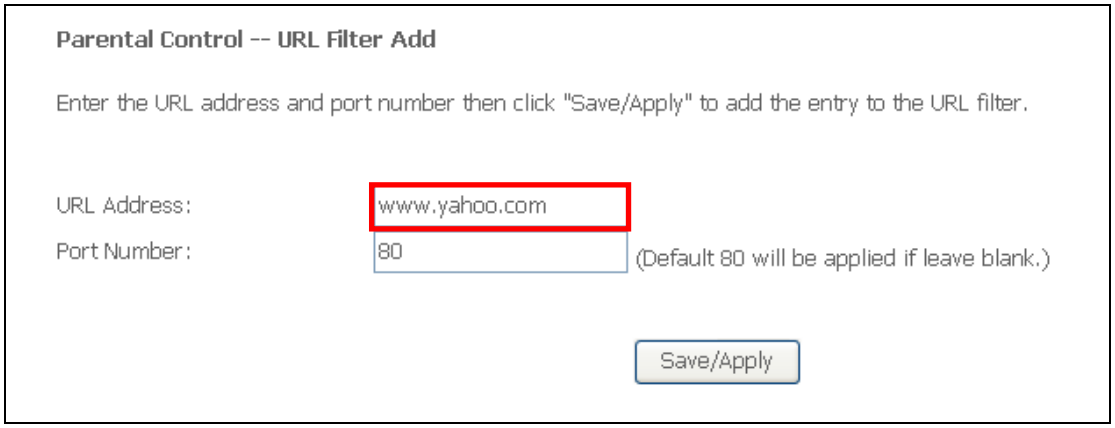
End Blocking Time: El tiempo en el que se finaliza la restricción.

5.6.2 URL Filter

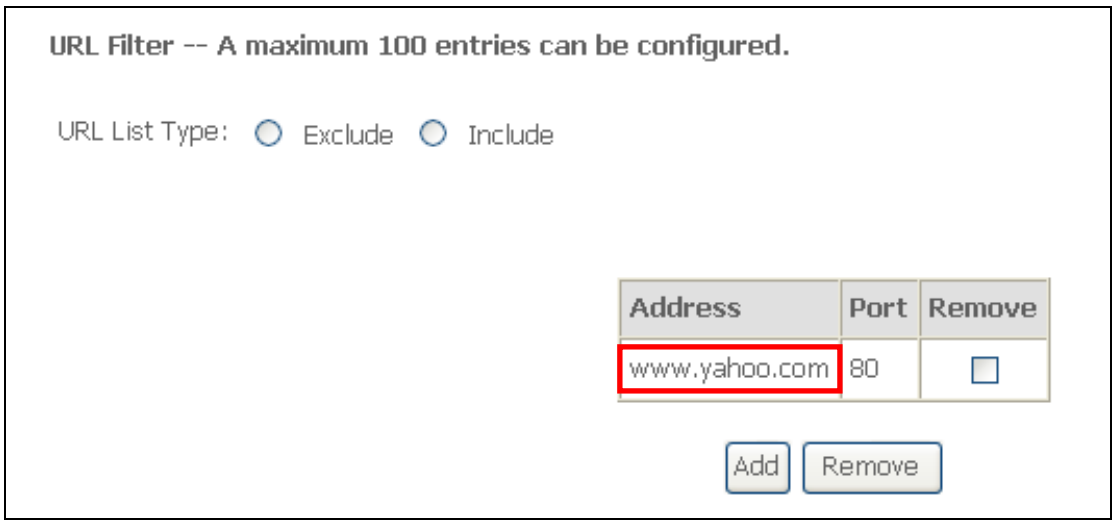
Este menú permite la creación de reglas de filtrado basado en direcciones web o URL y el número de puerto para tener derechos de acceso.



Haga clic en el botón "**Add**" para mostrar la siguiente pantalla.



Introduzca la dirección URL y número de puerto y posteriormente haga clic en el botón "**Save/Apply**" para añadir la entrada al filtro URL. La dirección URL comienza por "www", como se muestra en este ejemplo:



Se pueden añadir un máximo de 100 entradas a la lista de filtrado URL.

Marque "**Exclude**" para denegar el acceso a los sitios de Internet enumerados.
Marque "**Include"** para restringir el acceso únicamente a los sitios de internet enumerados.

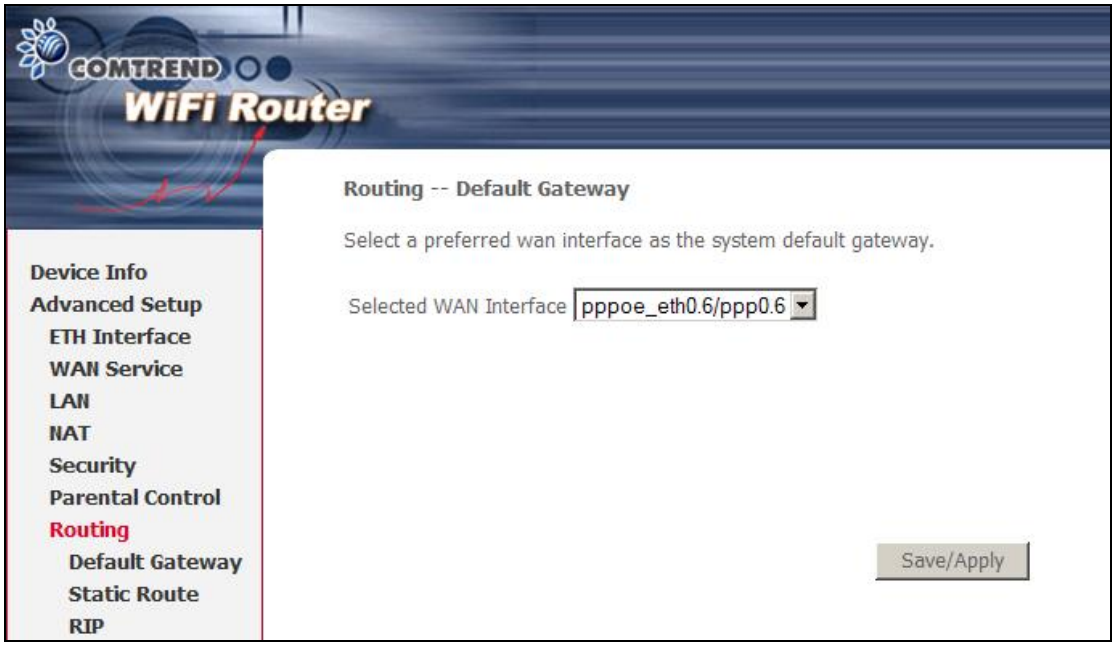
5.7 Routing

Esta opción permite realizar la configuración de **Default Gateway, Static Route,** y **RIP**.

NOTA:	En modo Bridge, El submenú **RIP** estará oculto, mientras que **Default Gateway** y **Static Route** serán mostradas pero inoperantes.

5.7.1 Default Gateway

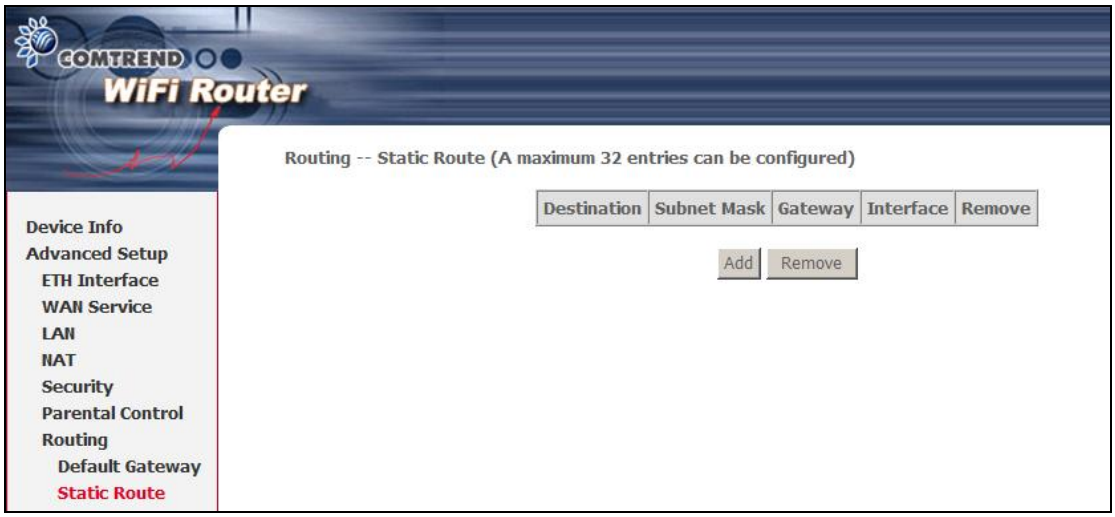
Seleccione el interfaz WAN como la puerta de enlace por defecto o default Gateway y haga clic en el botón "**Save/Apply**".



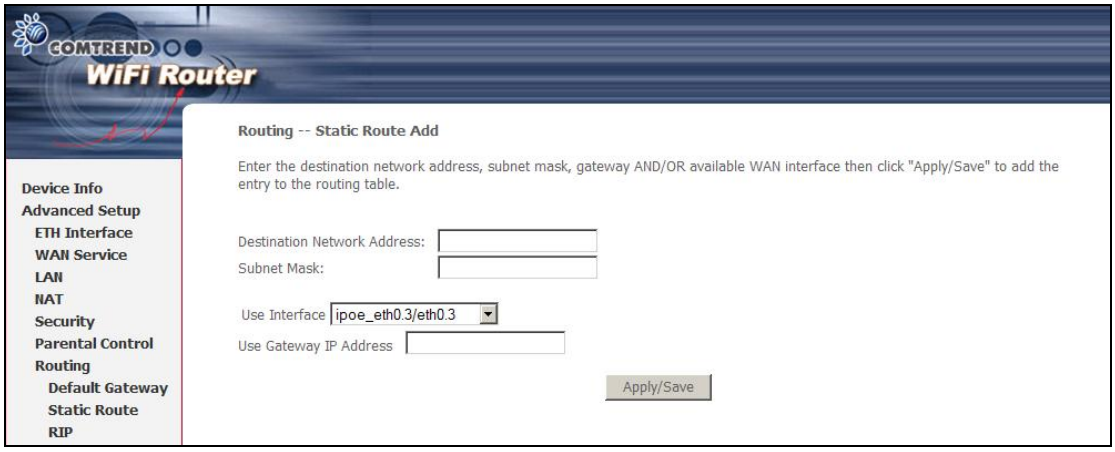
NOTA: Después de activar "**Automatic Assigned Default Gateway**", el WAP-5813n debe ser reiniciado para activar el default Gateway seleccionado.

5.7.2 Static Route

Esta opción permite configurar rutas estáticas. Haga clic en el botón "**Add**" para añadir una nueva ruta estática. Haga clic en el botón "**Remove**" para eliminar una ruta estática.



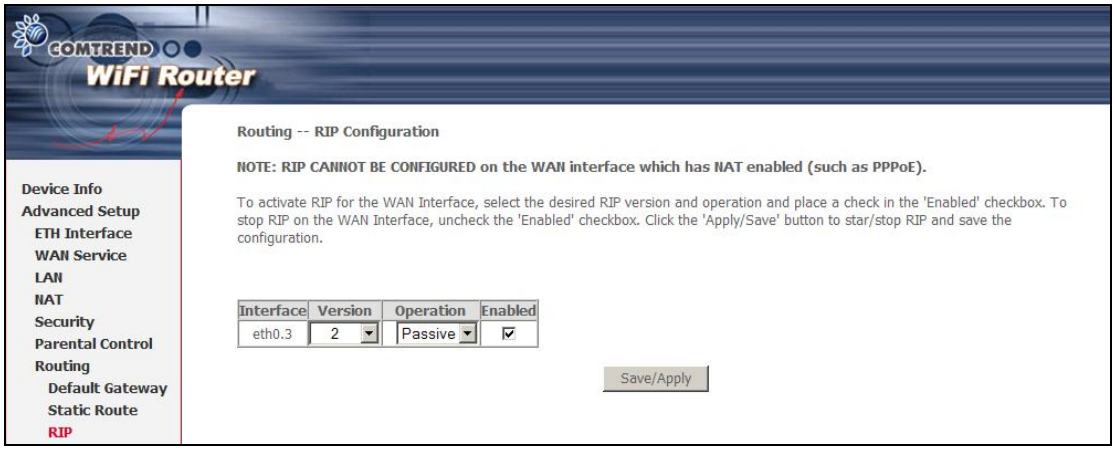
Haga clic en el botón "**Add**" para mostrar la siguiente pantalla.



Introduzca la dirección de red de destino, Submáscara, dirección IP del Gateway, y/o Interfaz WAN. Haga clic en el botón "**Save/Apply**" para salvar la ruta introducida en la tabla de enrutamiento.

5.7.3 RIP

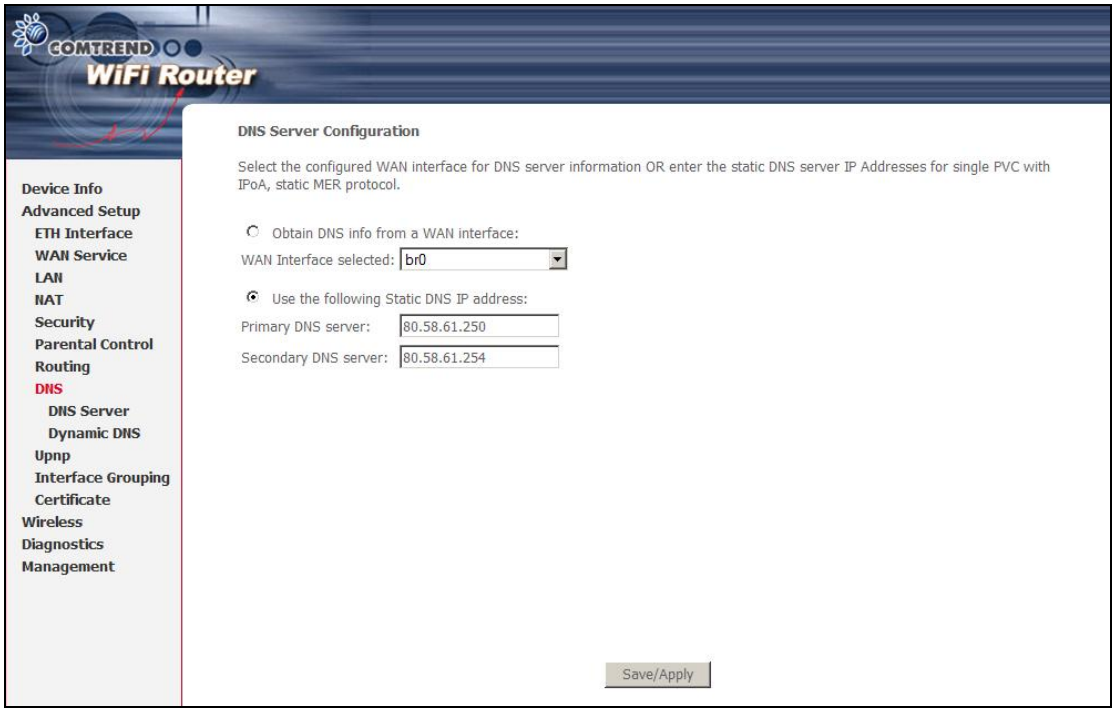
Para activar RIP, configurar la versión y modo e operación de RIP maque la casilla ve verificación ☑ "**Enabled**" para activarlo para al menos un interfaz WAN. Haga clic en el botón "**Save/Apply**".



5.8 DNS

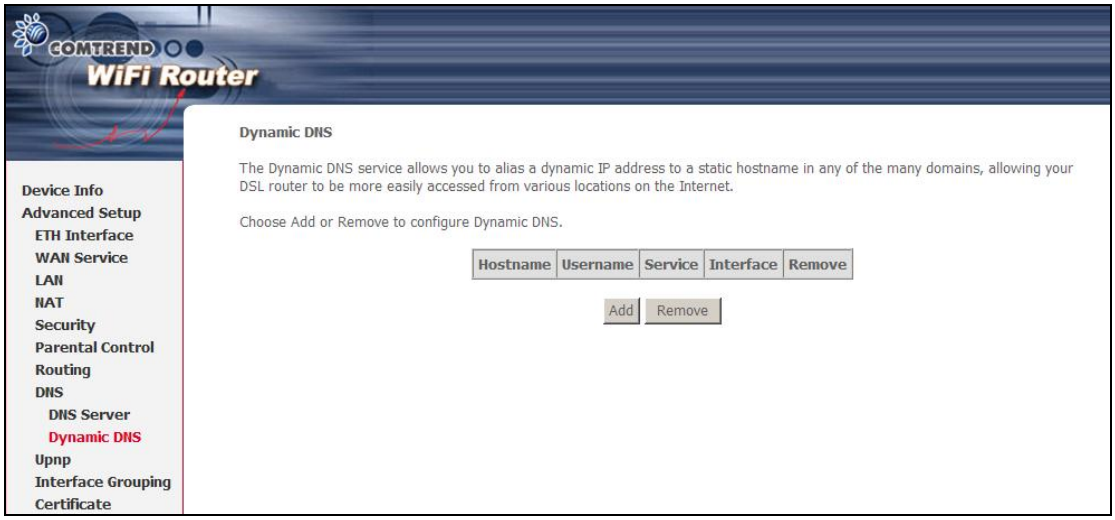
5.8.1 DNS Server

Para obtener información DNS de un interfaz WAN, marque "**Obtein DNS info from a WAN interface**", seleccione un interfaz WAN de la lista desplegable. Para DNS estático, marque "**Use the following static DNS IP address**", e introduzca la dirección IP del DNS primario y la dirección IP del DNS secundario. Haga clic en el botón "**Save/Apply"** para guardar la configuración.

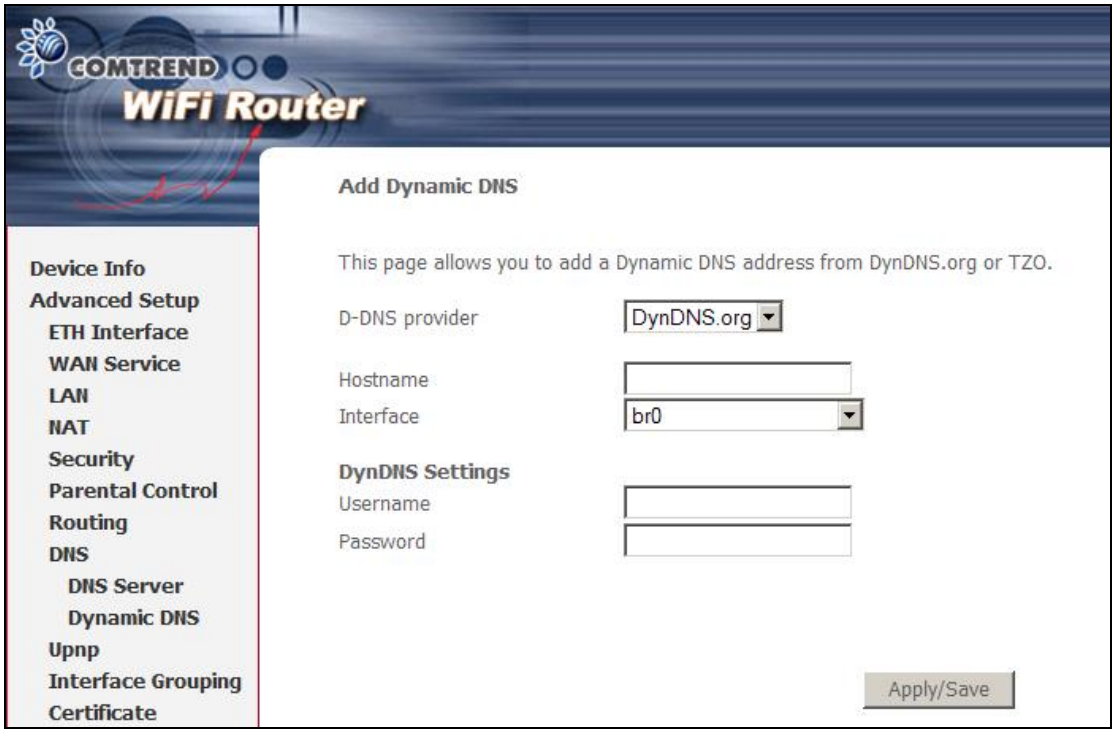


5.8.2 Dynamic DNS

El servicio Dynamic DNS (DNS dinámico) permite a la dirección IP de su router comportarse como un hostname o nombre de dominio, permitiendo al WAP-5813n ser localizado y accedido más fácilmente desde otros sitios de Internet.



Para añadir un servicio Dynamic DNS, haga clic en el botón "**Add**". La siguiente pantalla será mostrada.

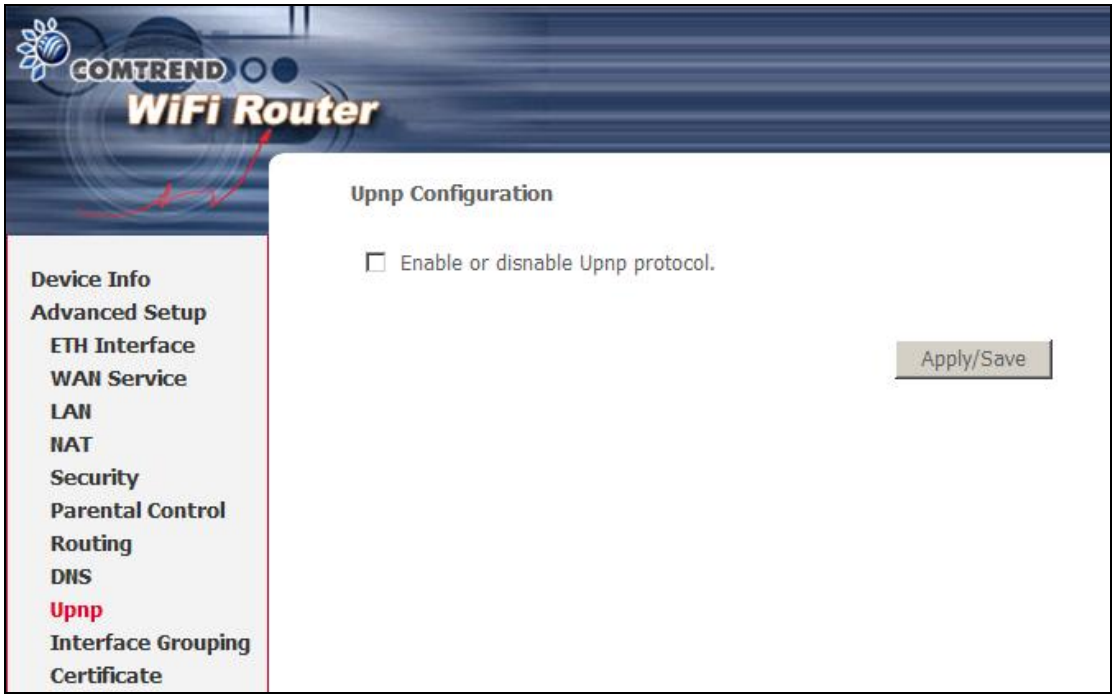


Consulte la siguiente tabla para la descripción de cada campo.

Campo	Descripción
D-DNS provider	Seleccione el proveedor Dynanic DNS de la lista desplegable.
Hostname	Introduzca el nombre del servidor DNS dinámico
Interface	Seleccione el interfaz de la lista
Username	Introduzca el usuario del servidor DNS dinámico
Password	Introduzca la contraseña del servidor DNS dinámico

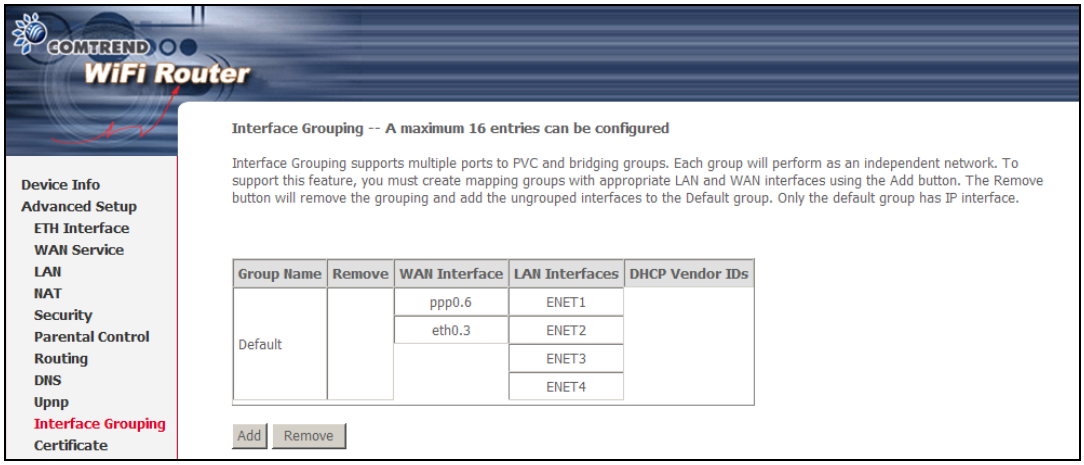
5.9 UPnP

Marque la casilla de verificación ☑ y haga clic en el botón "**Apply/Save**" para activar el protocolo UPnP.

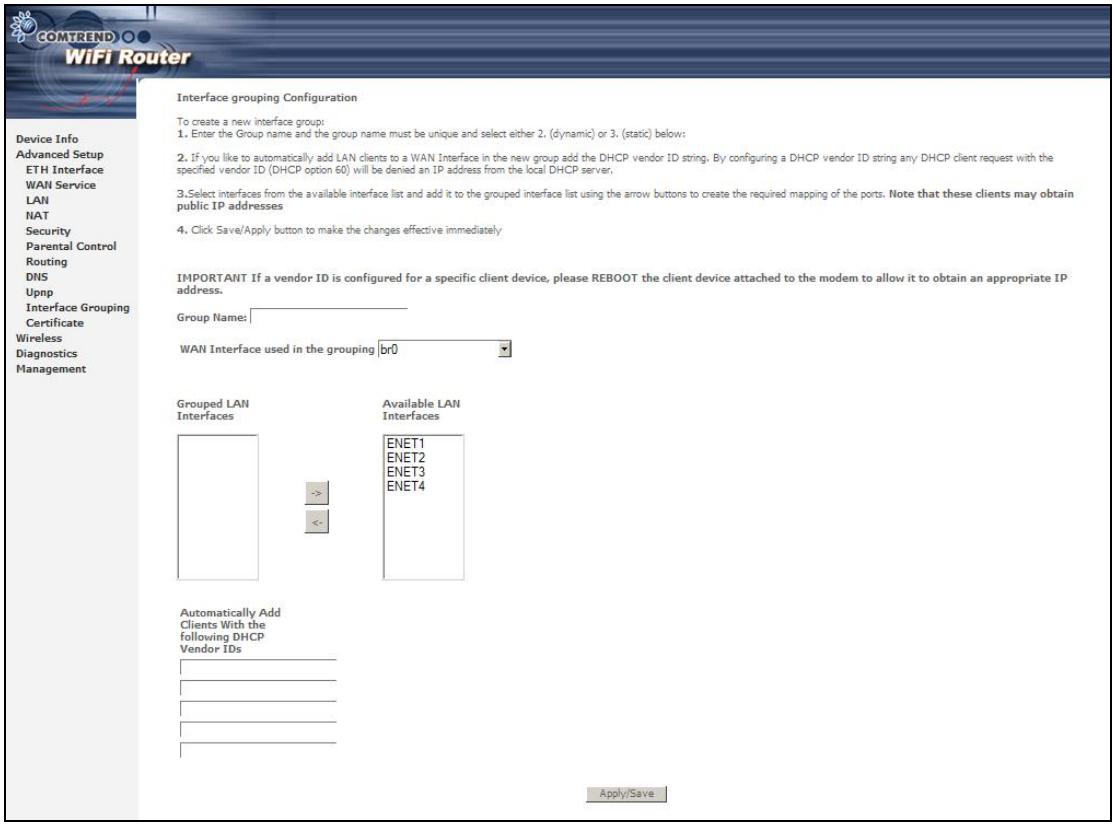


5.10 Interface Grouping

Interface Grouping soporta grupos de múltiples puertos por PVC o bridging. Cada grupo funciona como una red independiente. Para usar esta funcionalidad, debe crear "**mapping groups**" con su LAN y WAN apropiadas usando el botón "**Add**".



Para añadir un grupo de interfaces o "**Interface Group**", haga clic en el botón "**Add**". Se mostrará la siguiente pantalla. Enumera las interfaces disponibles y agrupadas. Siga las instrucciones mostradas a continuación.



Automáticamente añadir clientes con el siguiente DHCP Vendor IDs:
Añada soporte automáticamente al mapeo de interfaces LAN por cada PVC utilizando DHCP Vendor ID (opción 60). El servidor DHCP local declinará y reenviará las solicitudes al servidor DHCP remoto por el interfaz LAN apropiadamente mapeado. Este se activará cuando el Interface Grouping esté habilitado.

Por ejemplo, imagine que existen 4 PVCs (0/33, 0/36, 0/37, 0/38). VPI/VCI=0/33 es para PPPoE y los otros para IP set-top box (video). Las interfaces LAN son ENET1, ENET2, ENET3, and ENET4.

LA configuración de "**The Interface Grouping**" será:

1. Default: ENET1, ENET2, ENET3, and ENET4.
2. Video: nas_0_36, nas_0_37, y nas_0_38. El DHCP Vendor ID será "Video".

Si el servidor DHCP local está funcionando en 2l grupo "Default" y el Servidor DHCP del proveedor de acceso a internet (ISP) está funcionado en el PVC 0/36. Este será usado únicamente por los STB. En la parte LAN, el PC puede conseguir una dirección IP del servidor DHCP local del CPE y acceder a Internet a través del PVC del PPPoE (0/33).

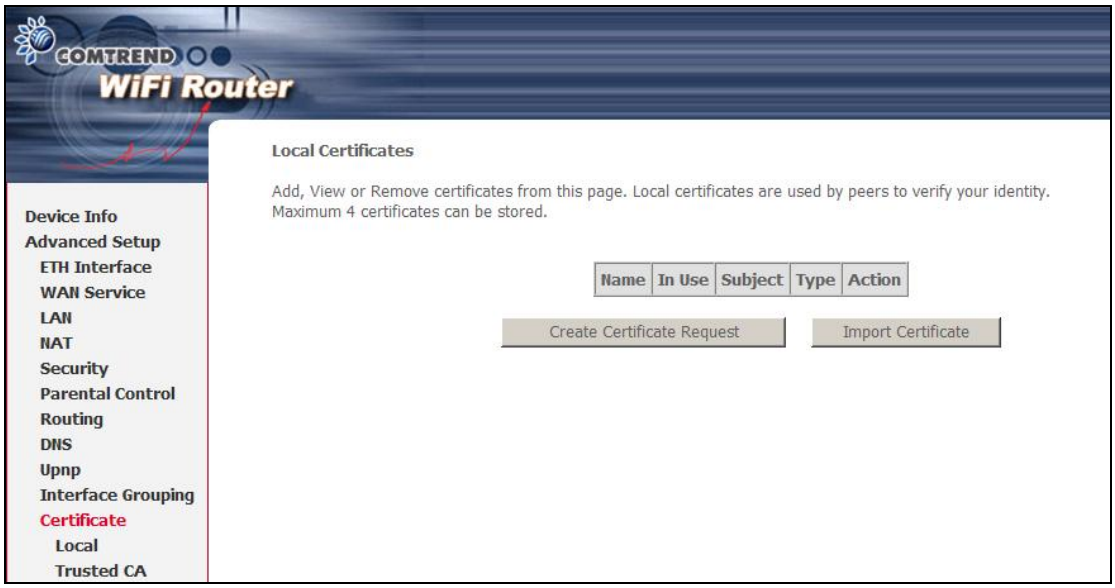
Si el set-top box está conectado al interfaz "ENET1 "y envía solicitudes DHCP won al Vendor id "Video", el servidor DHCP del WAP-5813n enviará estas solicitudes al servidor DHCP del ISP. Entonces el CPE cambiará la configuración port-mapping automáticamente. La configuración port-mapping se convertirá en:

1. Default: ENET2, ENET3, and ENET4.
2. Video: nas_0_36, nas_0_37, nas_0_38, y ENET1.

5.11 Certificate

Un certificado es como una clave pública, adjuntada a su propia información (nombre de empresa, nombre de servidor, nombre de persona real, contacto de correo electrónico, dirección postal, etc.) y firma digital.
Habrá una o más firmas digitales adjuntas al certificado, indicando que entidades certificadoras han comprobado la validez del certificado.

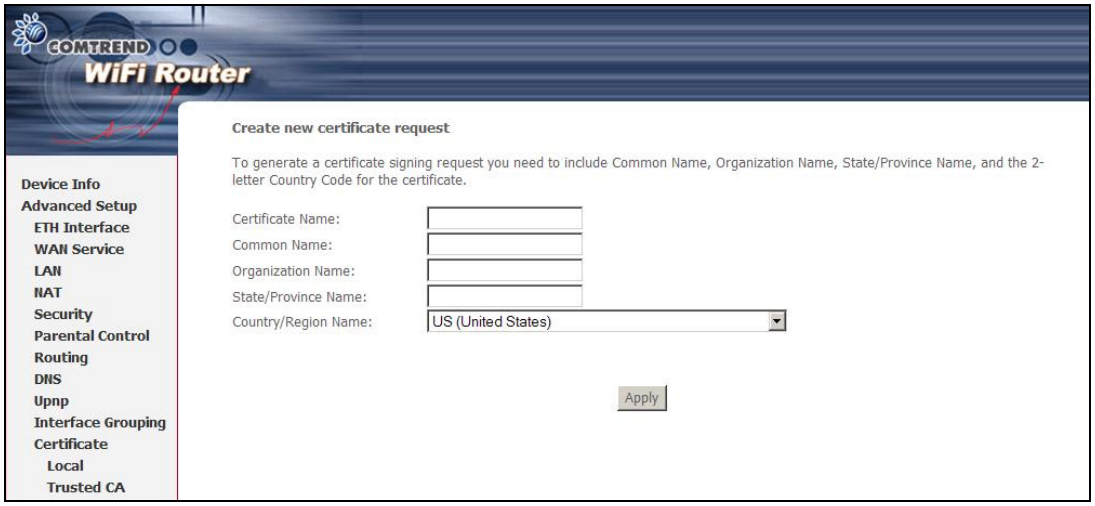
5.11.1 Local



CREATE CERTIFICATE REQUEST

Haga clic en el botón "**Create Certificate Request**" para generar una solicitud de certificado digital. Parte de la información debe ser incluida en la solicitud del certificado digital.

La solicitud de certificado digital puede ser presentada los Vendor/ISP/ITSP para aplicar un certificado. Su Vendor/ISP/ITSP pedirá que proporcione la información requerida y facilite la información en el formato regulado. Introduzca la información requerida y haga clic en el botón "**Apply**" para generar una clave privada y una solicitud de certificado digital.

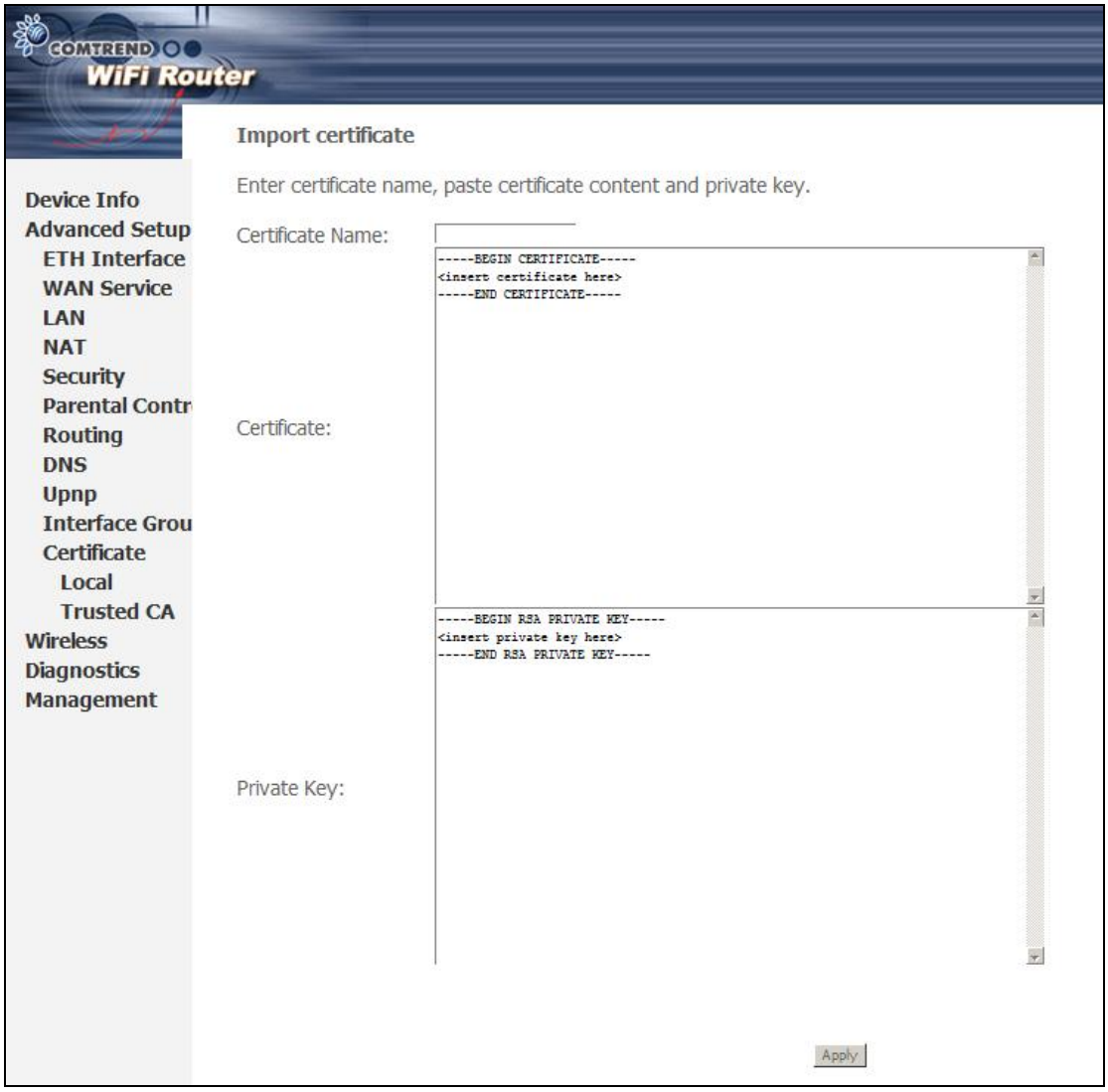


Consulte la siguiente tabla para la descripción de cada campo

Campo	Descripción
Certificate Name	Un nombre definido por el usuario para el certificado.
Common Name	Normalmente, el nombre complete de la máquina.
Organization Name	El nombre legal exacto de la organización o empresa. Sin abreviaturas.
State/Province Name	Localidad, Estado o provincial donde está situada su organización. No puede ser abreviada.
Country/Region Name	Las dos letras ISO de la abreviatura del país.

IMPORT CERTIFICATE

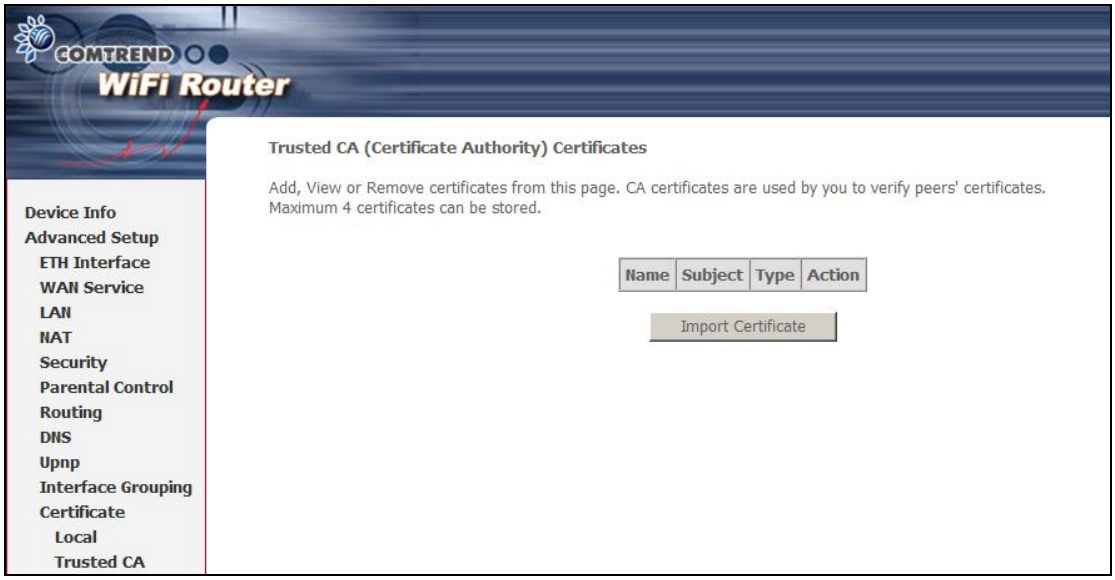
Haga clic en el botón "**Import Certificate**" para pegar el contenido del certificado y clave privada facilitada por su Vendor/ISP/ITSP dentro de los correspondientes campos mostrados a continuación.



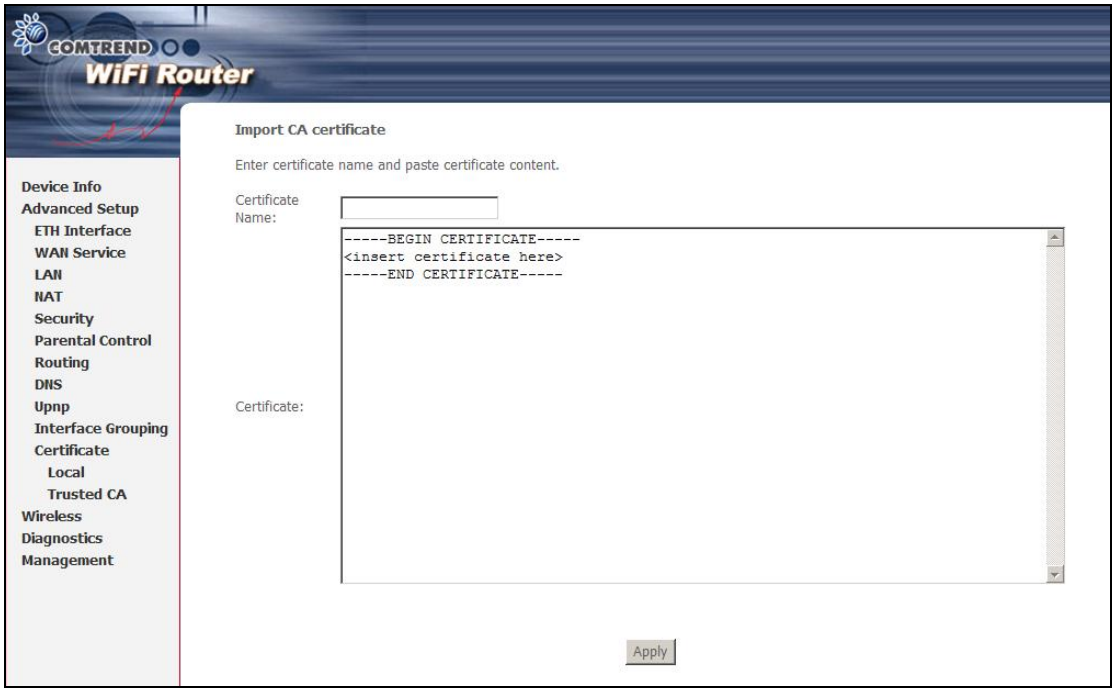
Introduzca un nombre de certificado y haga clic en el botón "**Apply**" para importar el certificado local.

5.11.2 Trusted CA

CA es la abreviatura de Autoridad Certificadora (en inglés), la cual es parte del sistema X.509. Es en sí misma un certificado, adjuntado con información del propietario de ese CA, pero su propósito no es la encriptación/ des encriptación. Su propósito e señalar la expedición del certificado, a fin de demostrar que el certificado es válido



Haga clic en el botón "**Import Certificate**" para pegar el contenido del certificado y su propio Trusted CA. El certificado CA contenido será facilitado por el Vendor/ISP/ITSP y es usado para autenticar al Auto-Configuration Server (ACS) al que el CPE estará conectado.



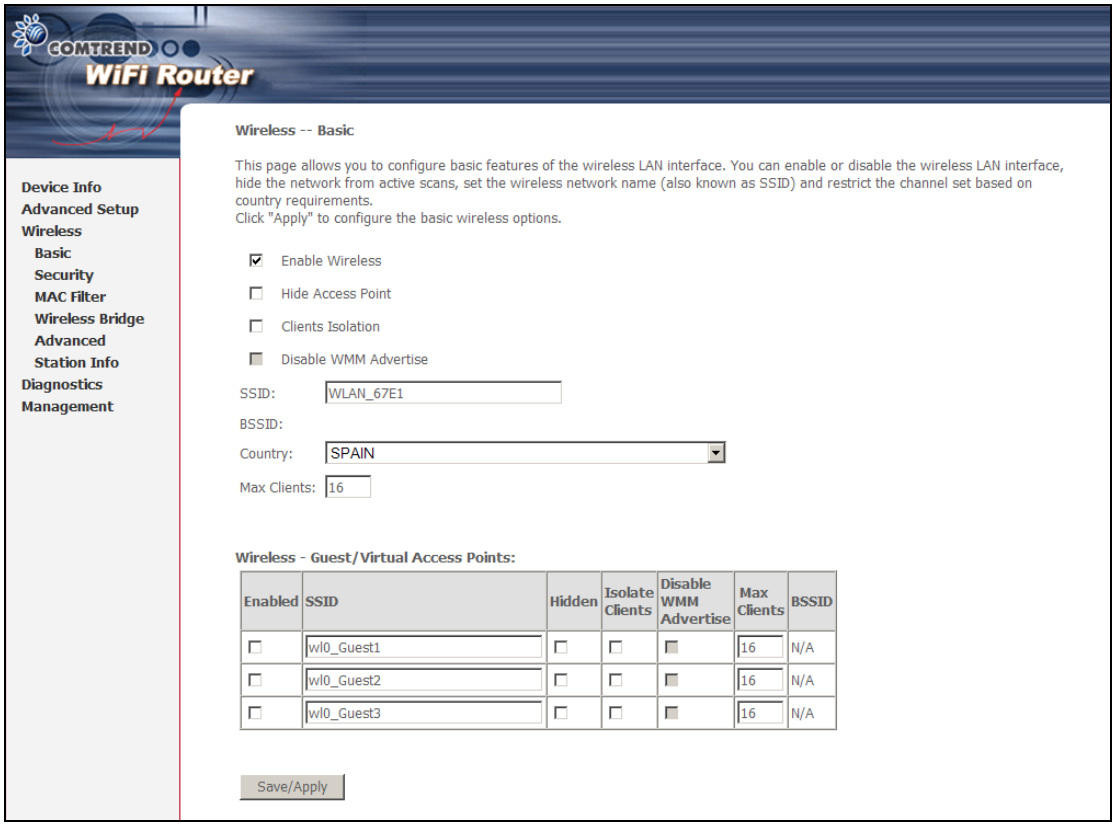
Introduzca el nombre del certificado y haga clic en el botón "**Apply**" para importar el certificado CA.

6. Wireless

El menú Wireless facilita acceso a las opciones de configuración del enlace inalámbrico, como se muestra a continuación.

6.1 Basic

La opción Basic permite configurar los parámetros básicos del interfaz inalámbrico (WLAN). Puede activar o desactivar el interfaz inalámbrico, ocultar la red a escaneos actives, configurar el nombre de red inalámbrica (también conocido como SSID) y restringir el canal a los requerimientos de configuración de País.



Haga clic en el botón "**Save/Apply**" para aplicar las opciones inalámbricas seleccionadas.

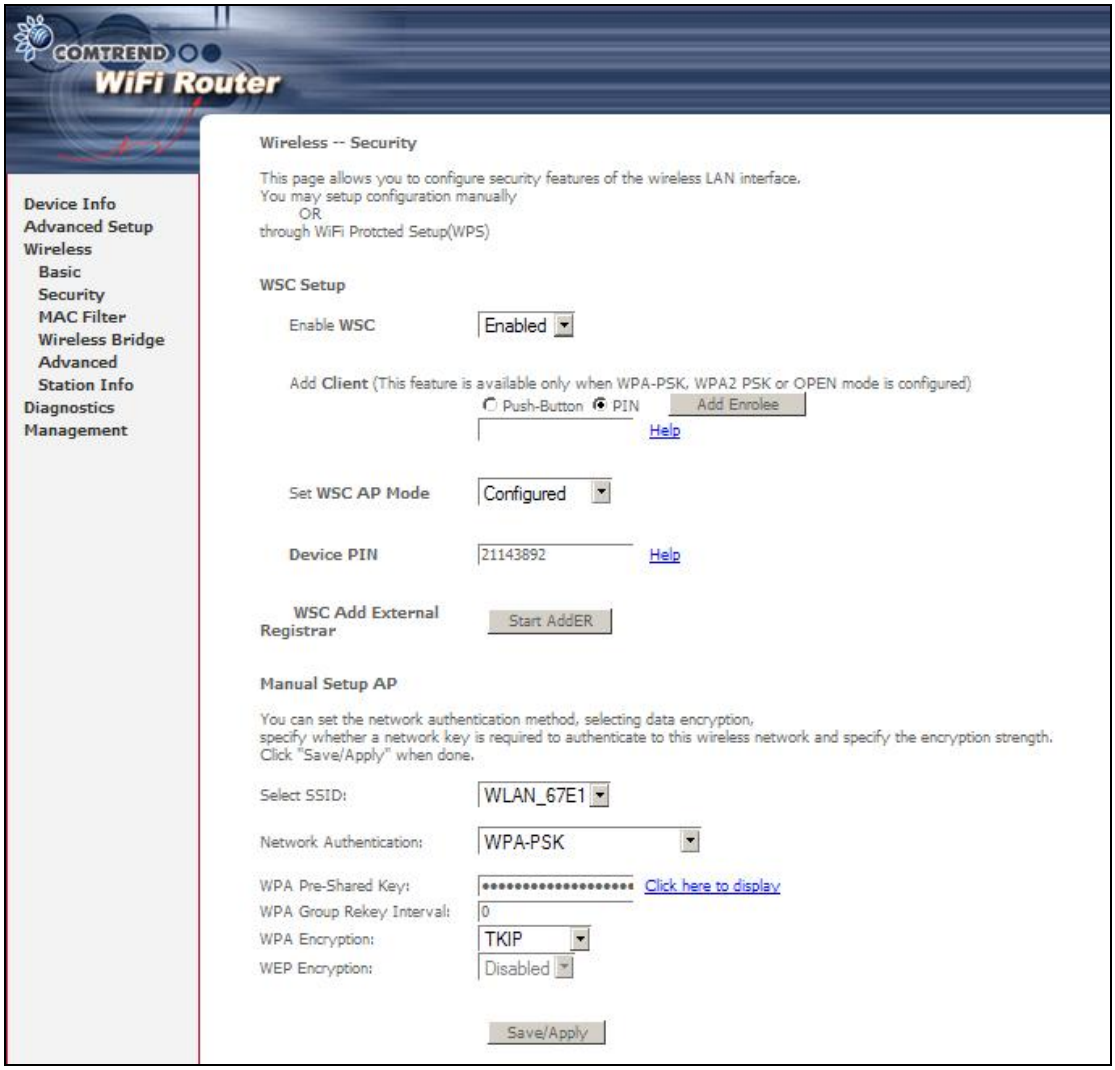
Consulte la siguiente tabla para la descripción de cada opción.

Opción	Descripción
Enable Wireless	Una casilla de verificación ☑ que active o desactiva el interfaz inalámbrico. Cuando está marcada, las opciones de configuración básicas serán mostradas.

Opción	Descripción
Hide Access Point	Seleccionar "**Select Hide Access Point**" para proteger el punto de acceso de detección por escaneo inalámbrico active. Para chequear el estado del punto de acceso e Windows XP, abra "**Conexiones de Red**" desde el menú Inicio y selecciones "**Ver conexiones de red disponibles**". Si el punto de acceso está oculto, no será mostrado en la lista. Para conectar con un punto de acceso oculto, la estación debe añadir el punto de acceso de forma manual a la configuración inalámbrica.
Clients Isolation	Cuando está activado, impide que los PCs asociados a la red inalámbrica sean vistos desde "Mis sitios de Red" o desde redes vecinas. También, impide que un cliente inalámbrico pueda comunicarse con otro cliente inalámbrico.
Disable WMM Advertise	Detiene al router de publicar la funcionalidad WMM o Wireless Multimedia, la cual facilita la calidad de servicio básica para aplicaciones en tiempo real (ej. VoIP, Video).
SSID [1-32 characters]	Configura el nombre de la red inalámbrica. El SSID significa Service Set Identifier. Todas las estaciones deben configurado correctamente el SSID para accede a la WLAN. Si el SSID no es correcto, el usuario no tiene garantizado el acceso.
BSSID	El BSSID es un identificado de 48 bit usado para identificar un BBS en particular (Basic Service Set) dentro de un área. En infraestructuras de redes BSS, el BSSID es la dirección MAC del punto de acceso; y en BSS independientes o red ad hoc, el BSSID es generado aleatoriamente.
Country	Una lista desplegable permite seleccionar la configuración específica del país seleccionado. Leyes locales regulan el límite y rango de canales, como por ejemplo: US= worldwide, Japan=1-14, Jordan= 10-13, Israel= 1-13
Max Clients	El número máximos de clientes que pueden accede al router.
Wireless - Guest / Virtual Access Points	El WAP-5813n soporta múltiples SSID llamados Guest SSIDs o Virtual Access Points (punto de accesos virtuales). Para activar uno o más de un Guest SSIDs marque la casilla de verificación ☑ en la columna "**Enabled**". Para ocultar un SSID marque la casilla de verificación ☑ en la columna "**Hidden**". Haga lo mismo para "**Isolate Clients**" y "**Disable WMM Advertise**". Para una descripción de estas dos funcionalidades, consulte las filas anteriores de los campos "Clients Isolation" y "Disable WMM Advertise". De igual modo, para "**Max Clients**" y "**BSSID**", consulte las entradas coincidentes en esta tabla. **NOTA:** Host inalámbrico remotos no pueden escanear Guest SSIDs.

6.2 Security

La siguiente pantalla aparecerá cuando es seleccionado "**Wireless Security**". Las opciones mostradas aquí permiten configurar los parámetros de seguridad del interfaz inalámbrico.



Haga clic en el botón "**Save/Apply**" para implementar los nuevos parámetros de configuración.

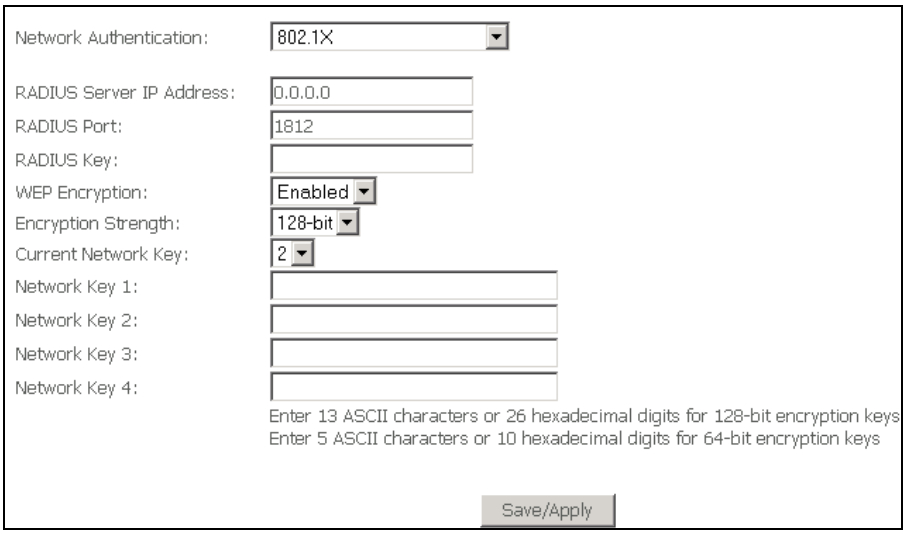
WIRELESS SECURITY

Los parámetros de seguridad inalámbrica pueden ser configurados manualmente o a través de WI-FI Protected Setup (WPS). El método WPS configura los parámetros de seguridad automáticamente (consultar apartado 6.2.1) mientras que el método Manual Setup requiere que el usuario configures estos parámetros usando el interfaz de usuario Web. Ver siguiente tabla.

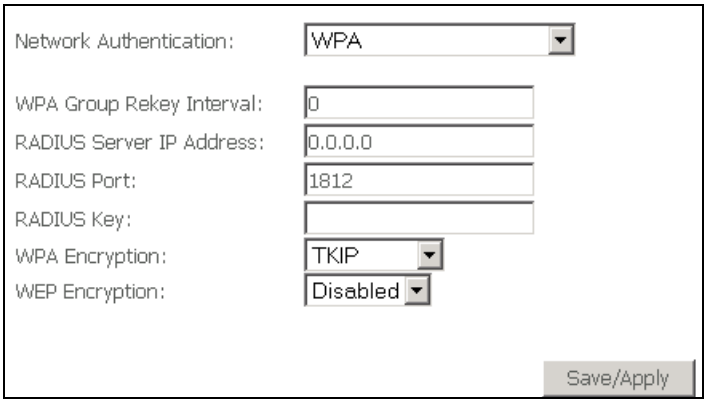
Seleccionar SSID
Seleccionar el nombre de red inalámbrica de la lista desplegable. Todas las estaciones deben configurado correctamente el SSID para accede a la WLAN. Si el SSID no es correcto, el usuario no tiene garantizado el acceso.

Network Authentication
Esta opción especifica si una cave red esta usada para autenticación de la red inalámbrica. Si la autenticación de red está configurada como Open, entonces no existe autenticación. A pesar de ello, la identidad del cliente es todavía verificada. Cada tipo de autenticación tiene sus propios parámetros. Por ejemplo, seleccionando autenticación 802.1X revelará la dirección IP del servidor Radius, puerto y campo clave. La encriptación WEP también estará disponible como se

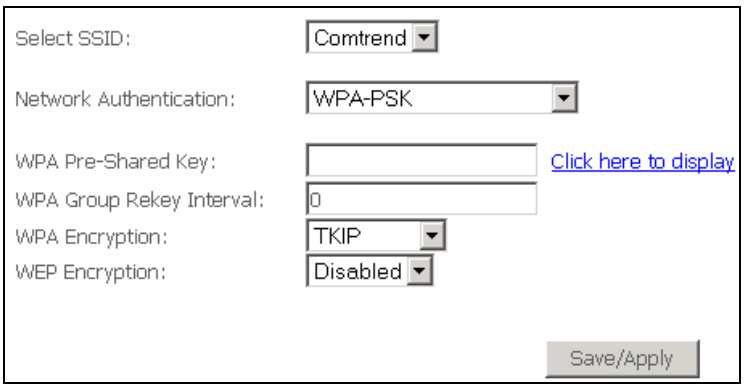
muestra a continuación.



La autenticación WPA estará disponible como se muestra a continuación.



La autenticación WPA-PSK estará disponible como se muestra a continuación.



WEP Encryption

Esta opción especifica si los datos enviados en una red están encriptados. La misma clave de red es usada para la encriptación de datos y autenticación de red. Cuatro claves de red pueden ser definidas aunque una única puede ser usada al mismo tiempo. Use la lista desplegable "**Current Network Key**" para seleccionar la clave red adecuada.

Las opciones de seguridad incluye autenticación y encriptación basada en el algoritmo wired equivalent privacy (WEP). WEP es un servicio de seguridad

configurable usado para proteger redes 802.11 de accesos no autorizados, tales como escucha; en este caso, la captura de tráfico inalámbrico. Cuando la encriptación de datos está activada, la clave secreta compartida de encriptación es generada y usada por la estación origen y la estación destino para modificar a otro rango de bits, evitando así la divulgación a espías. Bajo autenticación de clave compartida, cada estación inalámbrica asume tener un receptor de clave compartido sobre un canal seguro que es independiente del calan de comunicaciones de red inalámbrica.
Encryption Strength
Esta lista desplegable se mostrará cuando la encriptación WEP este habilitada. La longitud de la clave es proporcional al número de bits binarios que componen la clave. Esto significa que las claves con mayor número de bit tienen un mayor grado de seguridad y son considerablemente más difíciles de averiguar. El tamaño de encriptación puede ser configurado a 64 bit o a 128 bits. Una clave de 64 bit es equivalente a 5 caracteres ASCII o diez números hexadecimales. Una clave de 128 bits contiene 13 caracteres ASCII o 26 números hexadecimales. Cada clave contiene una cabecera de 24 bits (un iniciador de vector) que permite la decodificación de múltiples cadenas de datos encriptados.

6.3 WPS

Wi-Fi Protected Setup (WPS) es un estándar que simplifica la configuración de la seguridad inalámbrica para dispositivos de red certificados. Los dispositivos certificados WPS tienen implementados dos métodos; a través de un número PIN y usando push button, localizado en el dispositivo o accesible a través del software del dispositivo. El WAP-5813 tiene ambos implementados un botón WPS en el panel frontal y un botón virtual accesible desde el interfaz web de usuario.

Los dispositivos con el logo WPS (mostrado aquí) soportan WPS. Si el logo WPS no está presente en el dispositivo, todavía puede soportar WPS, consulte la documentación del fabricante para el apartado "Wi-Fi Protected Setup".

NOTA:	WPS está únicamente disponible en los modos de autenticación Open, WPA-PSK, WPA2-PSK y modo mixto WPA2/WPA-PSK. Otros modos de autenticación que no usen WPS pueden ser configurados manualmente.

Para configurar los parámetros de seguridad con WPS, siga el procedimiento descripto a continuación.
Debe elegir entre el método de configuración Push-Button o PIN para los pasos 6 y 7.

I. Configuración

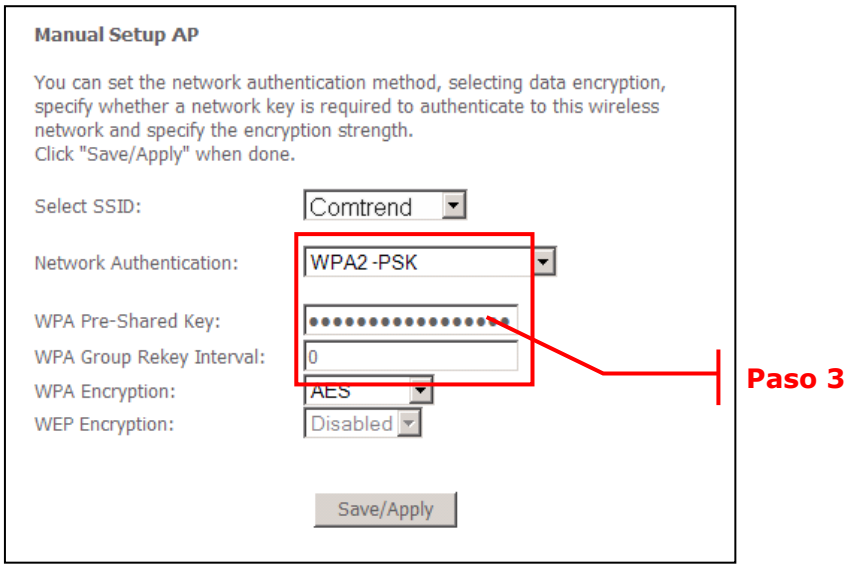
Paso 1: Active WPS seleccionando "**Enabled**" de la lista desplegable.

Paso 2: Seleccione "**configured**" en el campo "**Set WSC AP Mode**". "**Configured**" es utilizado cuando el WAP-5813 asignará la seguridad a los clientes. "**Unconfigured**" es usado cuando un cliente externo asigna los parámetros de seguridad al WAP-5813n.

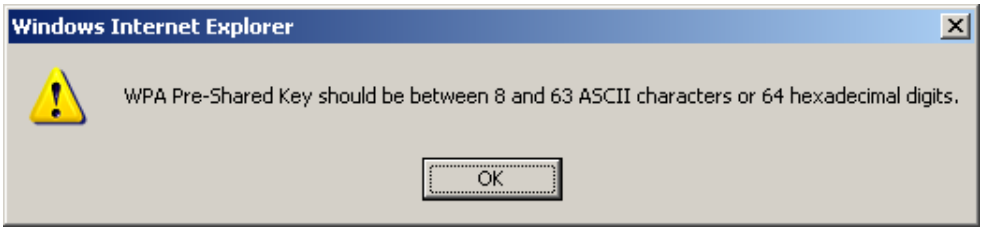
NOTA:	El cliente inalámbrico puede tener o no tener posibilidad de asignar los parámetros de seguridad al WAP-5813n. Si no tiene esta posibilidad, el usuario debe configurar "**WSC AP Mode**" como "**Configured**". En Windows Vista, se puede añadir un registrador externo utilizando el botón "**StartAddER**". Consultar Apéndice E para obtener más detalles

II. NETWORK AUTHENTICATION

Paso 3: Seleccione Open, WPA-PSK, WPA2-PSK, o Mixed WPA2/WPA-PSK como modo de autenticación de red desde el submenú "**Manual Setup AP**" del menú "**Wireless Security screen**". El ejemplo mostrado a continuación muestra el modo WPA2-PSK.



Paso 4: Para los modos Pre-Shared Key (PSK), introduzca la clave o contraseña en el campo "**WPA Pre-Shared Key**". Puede ver el siguiente cuadro de diálogo si la clave es demasiado corta o demasiado larga.



Paso 5: Haga clic en el botón "**Save/Apply**".

IIIa. CONFIGURACIÓN PUSH-BUTTON

El modo de configuración WPS Push-Button facilita un modo de configuración semiautomático. El botón WPS situado en el panel frontal del Router puede ser usado para este propósito. El interfaz de usuario Web (WUI) también facilita esta posibilidad a través de un botón software.

El procedimiento de configuración WPS Push-Button se describe a continuación. Se asume que la funcionalidad de punto de acceso inalámbrico está activada y que el router está configurado como punto de acceso de la red inalámbrica. Además, el cliente inalámbrico debe estar también configurado correctamente y disponible, con la funcionalidad WPS activada.

NOTA:	El punto de acceso inalámbrico del router buscará clientes WPS durante un periodo de 2 minutos. Si el router finaliza la búsqueda antes de completar el paso 7, por favor, vuelva a realizar el paso 6.

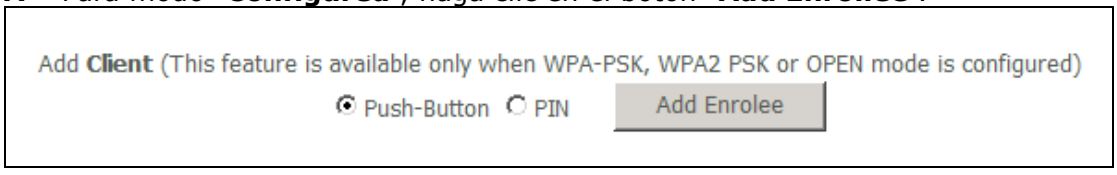
Paso 6: Primer método: WPS button

Pulse el botón WPS del panel frontal del router. El indicador luminoso WPS pardeará mostrando que el router está realizando una búsqueda de clientes WPS.

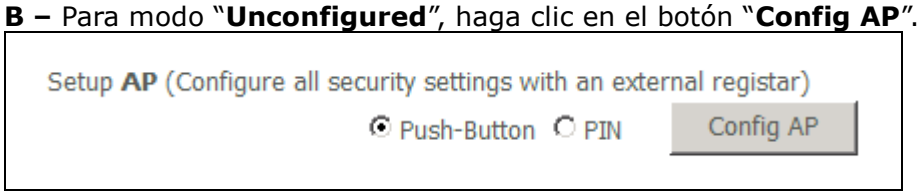
Segundo método: Botón virtual en el interfaz Web (WUI)

Seleccione y marque "**Push-Button**" en el submenú "**WSC Setup**" del menú "**Wireless Security**", como se muestra en el punto **A** y **B** de la siguiente figura, haga clic en el botón apropiado para seleccionar el modo correcto en el paso 2.

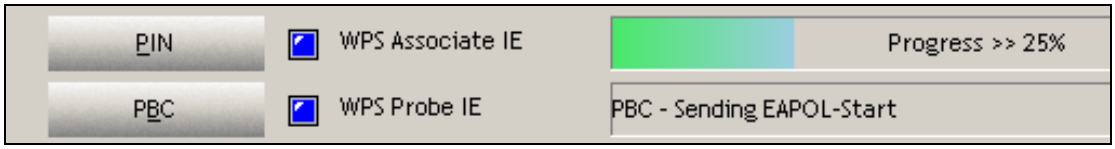
A – Para modo "**Configured**", haga clic en el botón "**Add Enrollee**".



B – Para modo "**Unconfigured**", haga clic en el botón "**Config AP**".



Paso 7: En el cliente WPS active la función push-button.
La siguiente imagen muestra un ejemplo de pantalla típica de un cliente WPS.



Vaya al paso 8 (Parte IV. Chequeo de la conexión) para comprobar el estado de la conexión WPS.

IIIb. CONFIGURACIÓN WPS - PIN

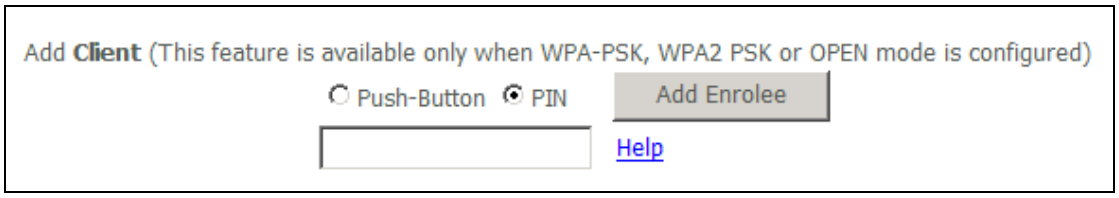
Utilizando este método, los parámetros de seguridad son configurados con un número de identificación personal (PIN). El PIN puede ser facilitado por el propio dispositivo o la herramienta de software. El PIN también puede ser generado aleatoriamente. Para obtener un número PIN para el cliente inalámbrico WPS, consulte la documentación de fabricante para más detalles.

El procedimiento de configuración WPS PIN se describe a continuación. Se asume que la funcionalidad de punto de acceso inalámbrico está activada y que el router está configurado como punto de acceso de la red inalámbrica. Además, el cliente inalámbrico debe estar también configurado correctamente y disponible, con la funcionalidad WPS activada.

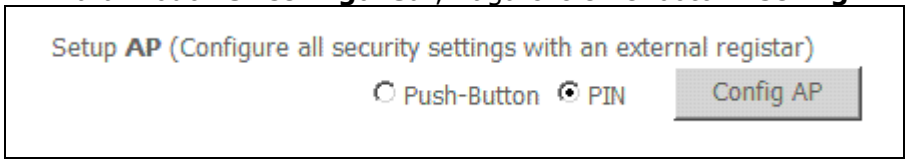
NOTA:	A diferencia del método push-button, el método PIN no tiene límite de tiempo. Esto significa que el router estará buscando continuamente clientes hasta a encontrar uno.

Paso 6: Seleccione "**PIN**" en el submenú "**WSC Setup**" de menú "**Wireless Security**", como se muestra en el punto **A** y **B** de la siguiente figura, haga clic en el botón apropiado para seleccionar el modo correcto en el paso 2.

A – Para modo "**Configured**", introduzca el número PIN en el campo facilitado para ello y haga clic en el botón "**Add Enrollee**", como se muestra a continuación.



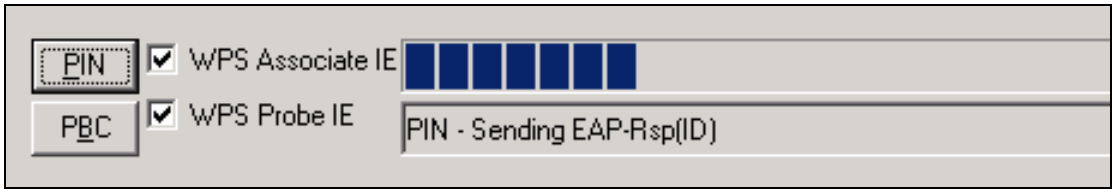
B – Para modo "**Unconfigured**", haga clic en el botón "**Config AP**".



Paso 7: Active la funcionalidad PIN en el cliente inalámbrico. Para modo "**Configured**", el cliente debe estar configurado como un "**Enrollee**". Para modo "**Unconfigured**", el cliente debe estar configurado como el "**Registrar**". Este es diferente a la funcionalidad External Registrar incorporada en Windows Vista.

La siguiente imagen muestra un ejemplo de cliente WPS con la

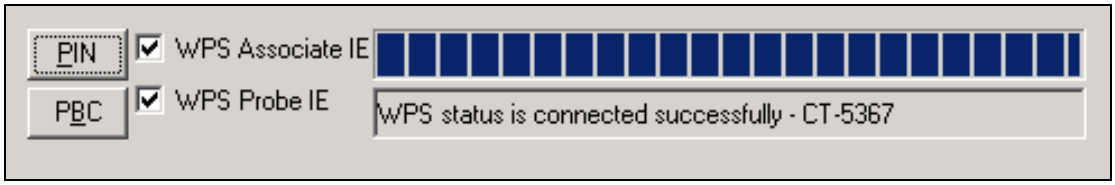
funcionalidad PIN en progreso.



Vaya al paso 8 (Parte IV. Chequeo de la conexión) para comprobar el estado de la conexión WPS.

IV. CHECK CONNECTION

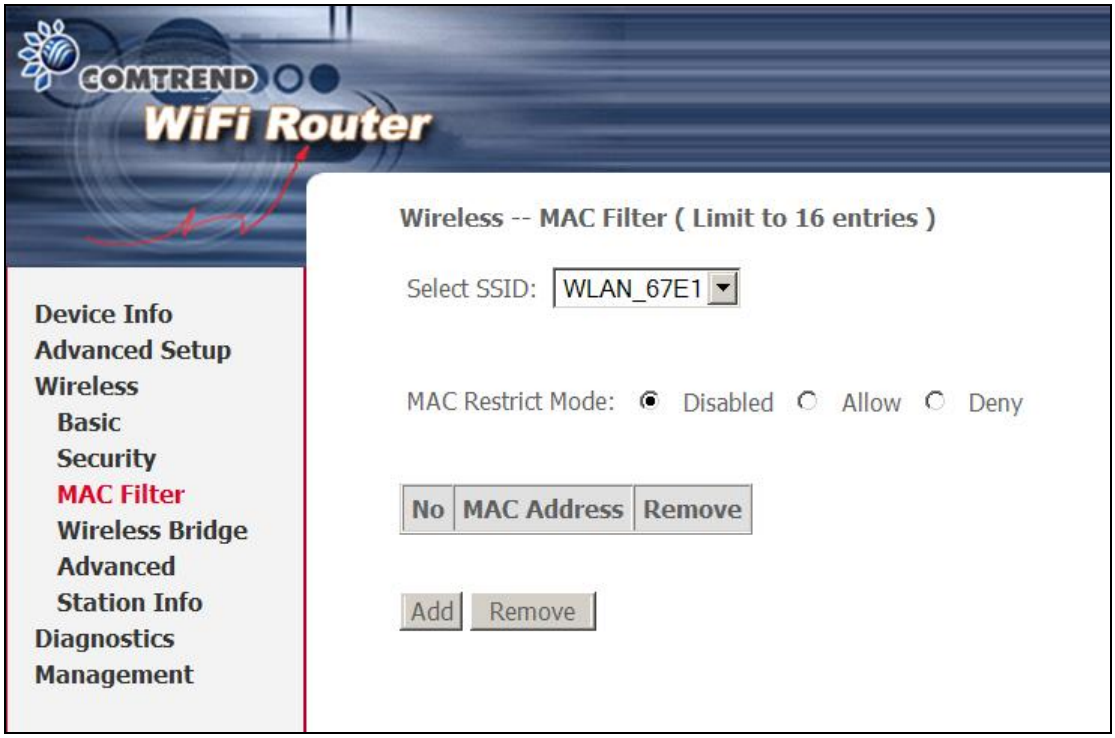
Paso 8: Si el método de configuración WPS se realice con éxito, el cliente inalámbrico tundra acceso a la red inalámbrica. El cliente software debe mostrar el estado. El siguiente ejemplo muestra una conexión establecida satisfactoriamente.



También puede hacer doble clic en el icono de Conexión Inalámbrica de la ventana "Conexiones de red" para confirmar el estado de la nueva conexión.

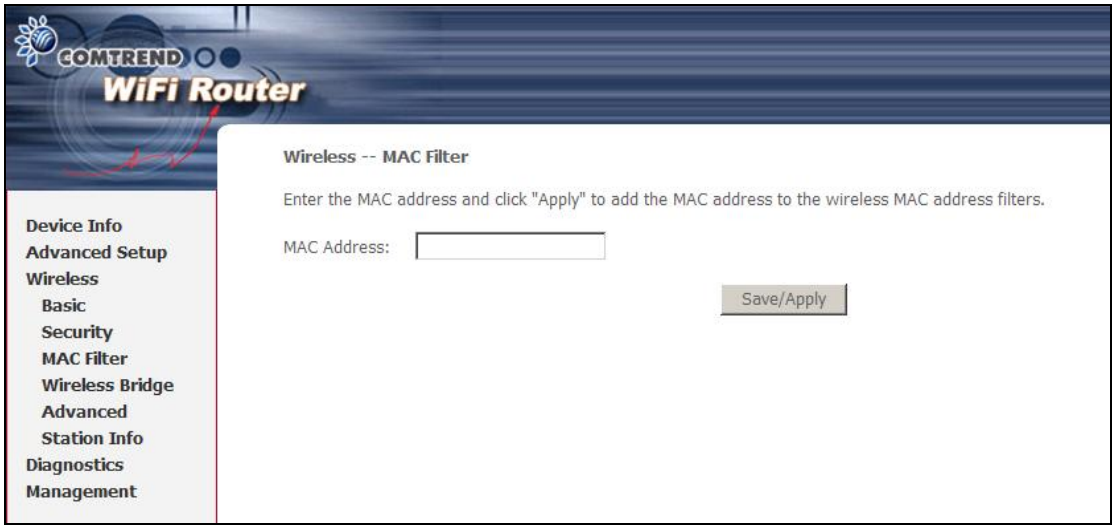
6.4 MAC Filter

Esta opción permite acceder al router realizar una gestión de restricciones basada en direcciones MAC. Para añadir un filtro de dirección MAC, haga clic en el botón "**Add**" mostrado a continuación. Para eliminar un filtro, seleccione la dirección MAC de la tabla de direcciones MAC mostrada a continuación y haga clic en el botón "**Remove**".



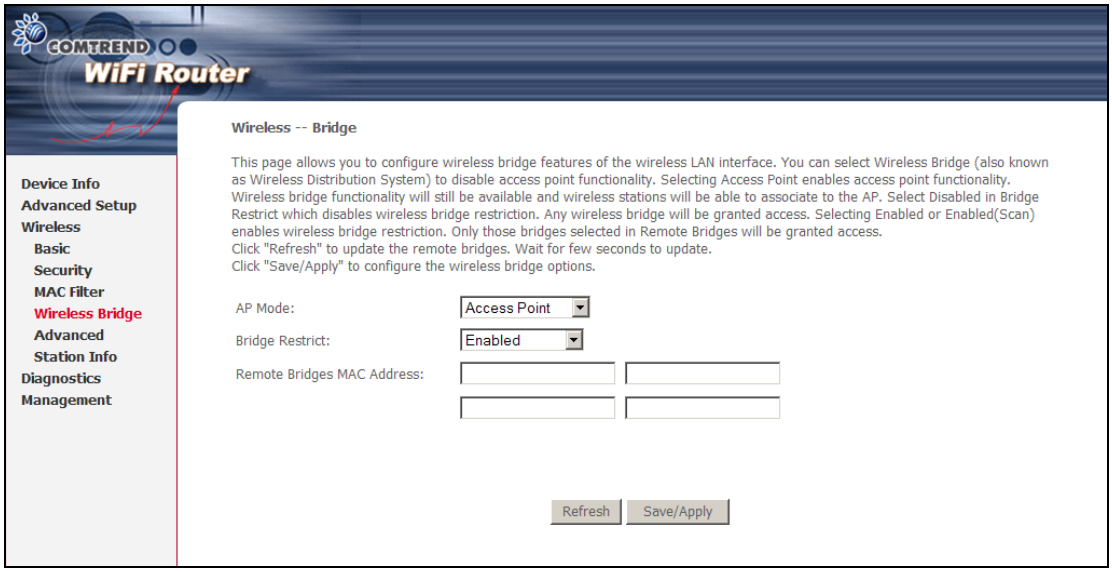
Opción	Descripción
Select SSID	Selecciona el nombre de red inalámbrico de la lista desplegable. SSID significa Service Set Identifier. Todas las estaciones deben estar configuradas con el SSID correcto para acceder a la WLA. Si el SSID no es correcto, el cliente no tiene garantizado el acceso.
MAC Restrict Mode	Disabled: Filtrado MAC desactivado. Allow: Acceso permitido a las direcciones MAC especificadas. Deny: Acceso restringido a las direcciones MAC especificadas.
MAC Address	Enumera las direcciones MAC sujetas al modo de restricciones MAC. Lists the MAC addresses subject to the MAC Restrict Mode. Se puede añadir un máximo de 60 direcciones MAC. Cada dispositivo de RED tienen una única dirección MAC de 48 bit. Normalmente mostrada como xx.xx.xx.xx.xx.xx, donde xx es un número hexadecimal.

Después de pulsar sobre el botón "**Add**", la siguiente pantalla aparecerá.
Introduzca la dirección MAC en el campo facilitado y haga clic en el botón "**Save/Apply**".



6.5 Wireless Bridge

Esta opción permite la configuración de la funcionalidad Bridge inalámbrico del interfaz WLAN. Consulte la tabla inferior para conocer más detalles de las distintas opciones.



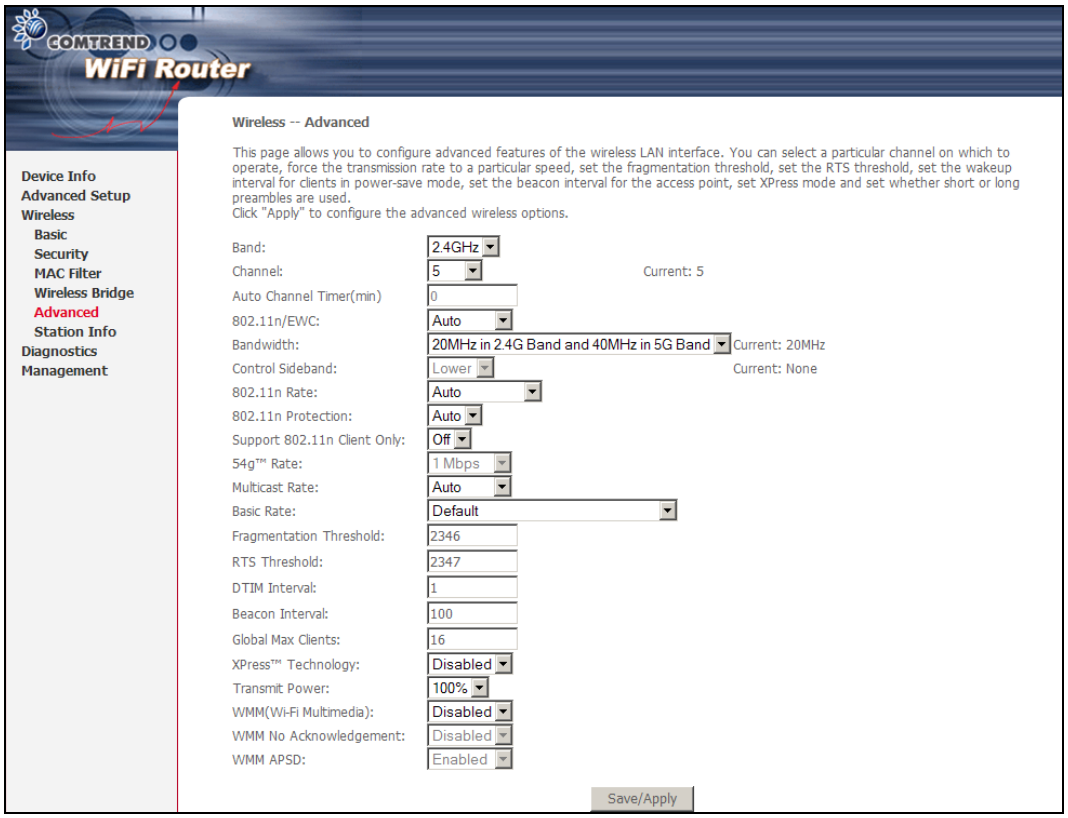
Haga clic en el botón "**Save/Apply**" para salvar y aplicar los parámetros de la nueva configuración.

Funcionalidad	Descripción
AP Mode	Seleccionando "**Wireless Bridge**" (alias de Sistema de distribución inalámbrico) desactiva la funcionalidad de punto de acceso, mientras que seleccionando "**Access Point**" activa la funcionalidad de punto de acceso. En modo "**Access Point**", la funcionalidad "**wireless bridge**" estará disponible y las estaciones inalámbricas deben estar asociadas al punto de acceso.

Funcionalidad	Descripción
Bridge Restrict	Seleccionando "**Disabled**" desactiva la restricción wireless bridge, lo que indica que cualquier wireless bridge tendrá acceso garantizado. Seleccionando "**Enabled**" o "**Enabled (Scan)**" active la restricción wireless bridge. Sólo los bridges seleccionados en la lista de Bridge remotos ("**Remote Bridges**") tendrán acceso garantizado. Haga clic en el botón "**Refresh**" para actualizar la lista de estaciones con Bridge Restrict activado.

6.6 Advanced

El submenú "**Advanced"** permite configurar las prestaciones avanzadas del interfaz inalámbrico. Puede seleccionar un canal en particular con el que operar, aplicar una velocidad en particular para forzar el rango de transmisión, configurar el umbral de fragmentación, configurar el umbral RTS, configurar wake interval para clientes en modo ahorro de energía o power-save, configurar el beacon interval para el punto de acceso, configurar el modo XPress y configurar si el preámbulo usado es corto o largo. Haga clic en el botón "**Save/Apply**" para configurar las nuevas opciones inalámbricas avanzadas.



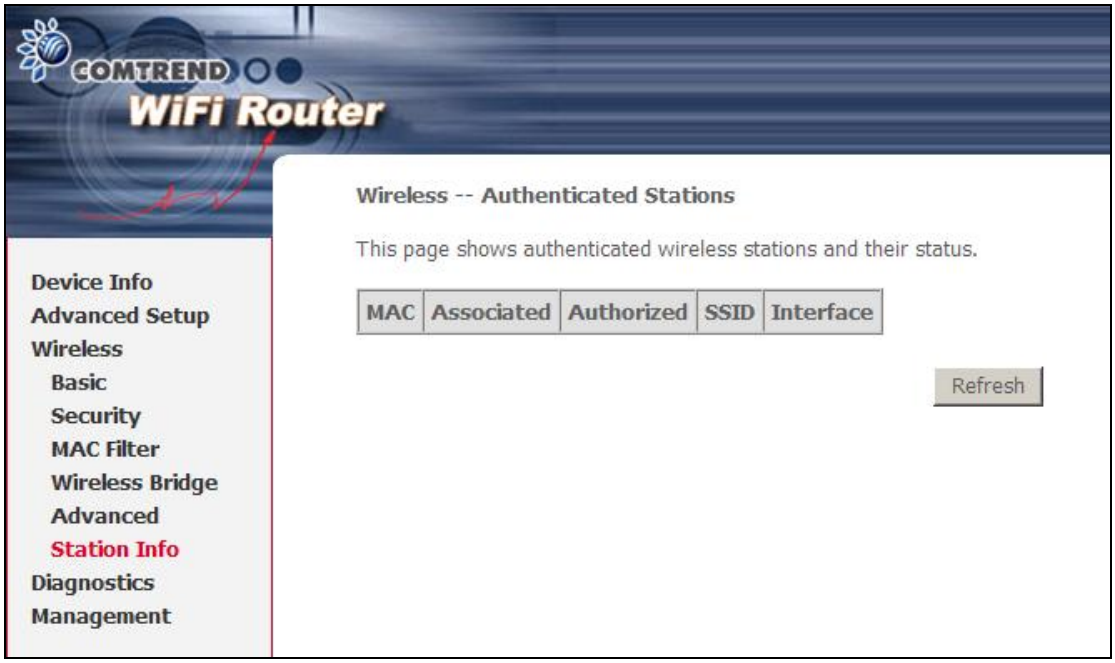
Campo	Descripción

Campo	Descripción
Band	Configure 2.4 GHz para compatibilidad con dispositivos IEEE 802.11x estándar. La nueva enmienda permite a los dispositivos 802.11n ser compatibles y coexistir en la misma red inalámbrica con dispositivos de velocidades 802.11x inferiores. IEEE 802.11g iguala el rango de datos en la frecuencia 2,4 GHz con dispositivos 802.11a, los cuales tienen un rango de 54Mbps en la frecuencia de 5GHz. (IEEE 802.11a tiene otras diferencias comparadas con IEEE 802.11b y g, como la cantidad de canales ofrecidos).
Channel	La lista desplegable permite seleccionar un canal específico.
Auto Channel Timer (min)	La auto búsqueda de canales temporizado en minutes. (0 to disable)
802.11n/EWC	Un equipo configurado con los parámetros de estándar de interoperabilidad en IEEE 802.11n Draft 2.0 y Enhanced Wireless Consortium (EWC)
Bandwidth	Seleccione la banda de frecuencia de 20GHz o 40GHz. La banda de frecuencia de 40GHz usa dos bandas adyacentes de 20 GHz para incrementar el Throughput de datos.
Control Sideband	Seleccionar sideband alta o baja cuando está en modo 40GHz.
802.11n Rate	Configurar el rango de transmisión físico (PHY).
802.11n Protection	Turn Off Para throughput maximizado. Turn On para mayor seguridad.
Support 802.11n Client Only	Turn Off para permitir a clientes 802.11b/g acceder al router. Turn On para prohibir a clientes 802.11b/g acceder al router.
54g Rate	La lista desplegable especifica los siguientes rangos fijos: Auto: Default. Usa el rango de datos de 11 Mbps cuando es necesario. Rangos fijos de 1 Mbps, 2Mbps, 5.5Mbps, o 11Mbps. Los parámetros apropiados dependen de la calidad de la señal inalámbrica.
Multicast Rate	Parámetros para el rango de paquetes multicast transmitidos (1 -54 Mbps)
Basic Rate	Configuración de rango básico de transmisión.
Fragmentation Threshold	Un umbral, especificado en bytes, que determina qué paquetes se fragmentarán y a qué tamaño. En una WLAN 802.11, los paquetes que exceden el umbral de fragmentación serán fragmentados, por ejemplo, divididos en, unidades más pequeñas adecuadas al tamaño del circuito. Lo paquetes más pequeños que el umbral de fragmentación especificado no serán fragmentados. Introduzca el valor entre 256 y 2346. Si tiene un alto índice de error de paquetes, trate de aumentar ligeramente el umbral de fragmentación. La configuración del valor debe permanecer entre los parámetros por defecto configurados a 2346. Configurar los parámetros de fragmentación demasiado bajos puede crear problemas de prestaciones.

Campo	Descripción
RTS Threshold	Solicitud a enviar, cuando está configurado en bytes, especifica el tamaño de paquete más allá del que la tarjeta inalámbrica invoca en su mecanismo RTS/CTS. Los paquetes que excedan el umbral RTS especificado hacen funcionar el mecanismo RTS/CTS. La tarjeta transmite paquetes más pequeños sin utilizar RTS/CTS. El valor por defecto es 2347 (longitud máxima) desactiva el umbral RTS.
DTIM Interval	Delivery Traffic Indication Message (DTIM) es también conocido como el Beacon Rate. El rango permitido es un valor entre 1 y 65536. Un DTIM es un contador que informa a los clientes de la próxima ventana para escuchar los mensajes broadcast y multicast. Cuando el AP ha amortiguado el impacto de los mensajes broadcast y multicast para los clientes asociados, envía el próximo DTIM con un valor de intervalo de un 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 entre transmisiones de beacon en milisegundos. Por defecto es 100ms y el rango permitido es de 1 a 65535. La transmisión de beacon identifica la presencia del punto de acceso. Por defecto, los dispositivos de red pasivos escanean todas las frecuencias de canales escuchando los siguientes puntos desde donde acceder. Antes de que una estación entre en modo de ahorro de energía o power-saving, la estación necesita el interval de beacon para conocer cuando debe volver a escuchar para recibir el beacon (y aprender si existe frames en el buffer del punto de acceso)
Global Max Clients	El número máximo número de clientes que pueden conectarse al router.
Xpress ™ Technology	Xpress Technology cumple con el borrador de especificaciones de los estándares planteados por los fabricantes inalámbricos.
Transmit Power	Fija la potencia de salida (por porcentaje) deseado.
WMM (Wi-Fi Multimedia)	La tecnología para mantener la prioridad de aplicaciones de voz, audio y video en redes inalámbricas. Permite a los servicios multimedia tener mayor prioridad.
WMM No Acknowledgement	Referido a la política de conocimiento a nivel MAC. Activando un "no acuse" de recibo que puede resultar en una transferencia de datos más eficiente pero más propenso a errores en entornos con ruido en radio frecuencia.
WMM APSD	Entrega de power save automático. Este método permite ahorrar energía.

6.7 Station Info

Esta sección muestra el modo de autenticación de las estaciones inalámbricas y su estado. Haga clic en el botón **Refresh** para actualizar la lista de estaciones asociadas a la WLAN.



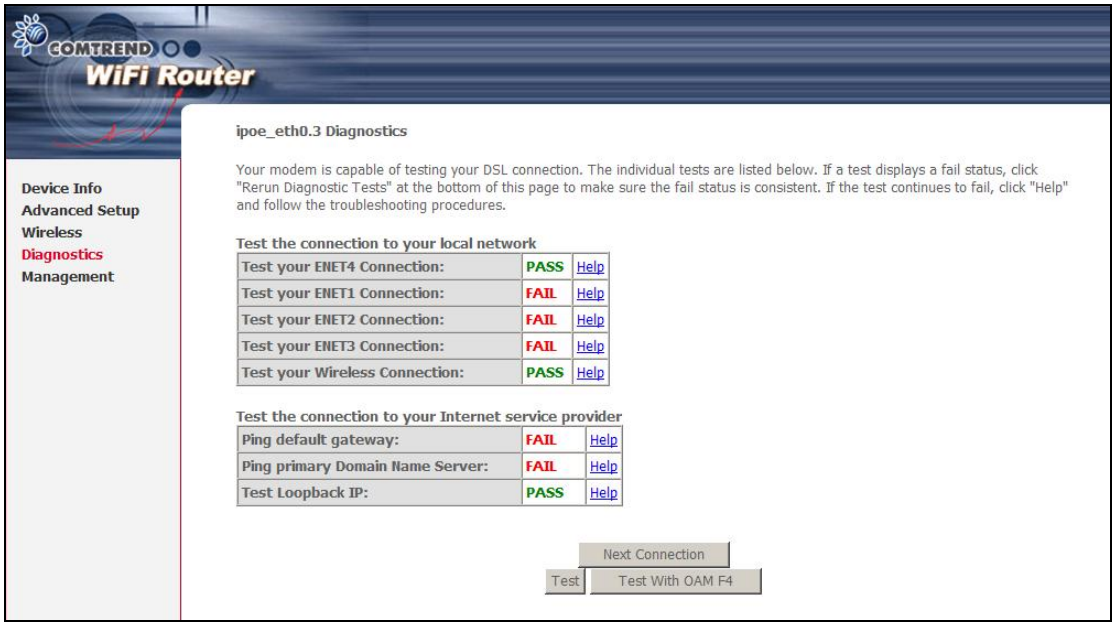
Consulte la siguiente tabla para la descripción de cada columna.

Denominación	Descripción
MAC	Lista de direcciones MAC de todas las estaciones.
Associated	Lista de todas las estaciones que están asociadas al punto de acceso, mostrando el tiempo de conexión y paquetes emitidos y recibidos por cada una de las estaciones. Si la estación es parada durante mucho tiempo, es eliminada de la lista.
Authorized	Lista los dispositivos con acceso autorizado.
SSID	Muestra los SSID del router a los que las estaciones están conectados.
Interface	Muestra las interfaces del router a las que las estaciones están conectadas.

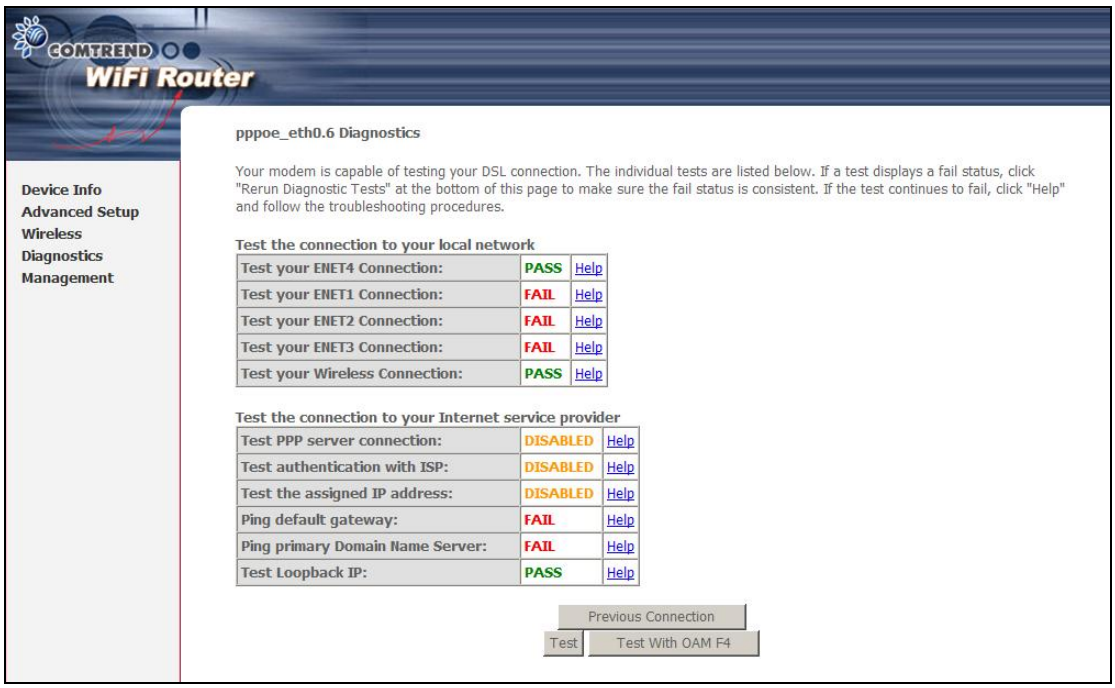
7. Diagnostics

La sección Diagnostics para los tipos de conexiones IPoW y PPPoE se muestra a continuación

Conexión IPoW



Conexión PPPoE



El menú Diagnostics facilita el estado de la conexión para el WAP-5813n. Si un test muestra un fallo, haga clic en el botón Test para resetear y confirmar el error. Si el error continúa, haga clic en Help y siga las instrucciones del proceso de troubleshooting.

8. Management

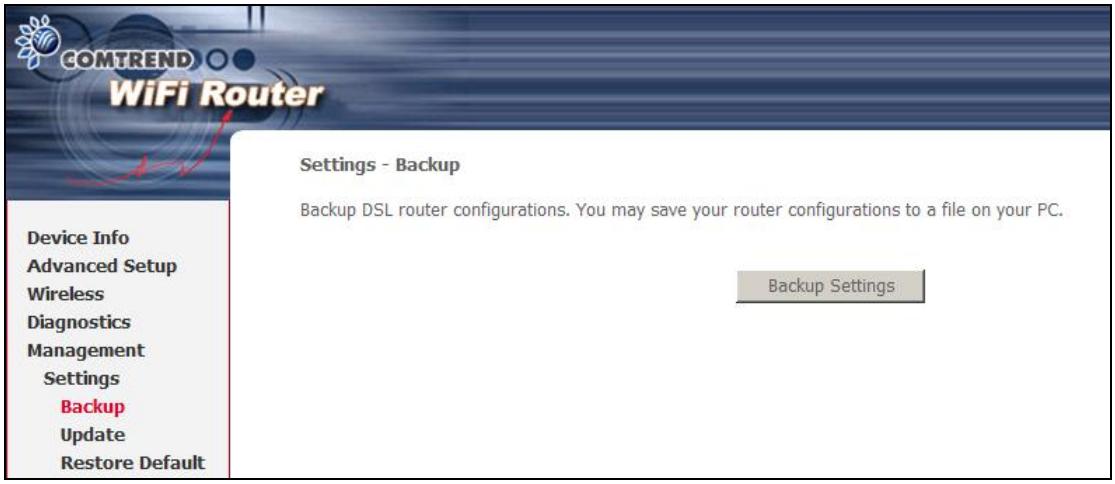
El menú Management tiene las siguientes funcionalidades y procesos:

9.1 Settings

Esta sección incluye Backup Settings, Update Settings, y Restore Default.

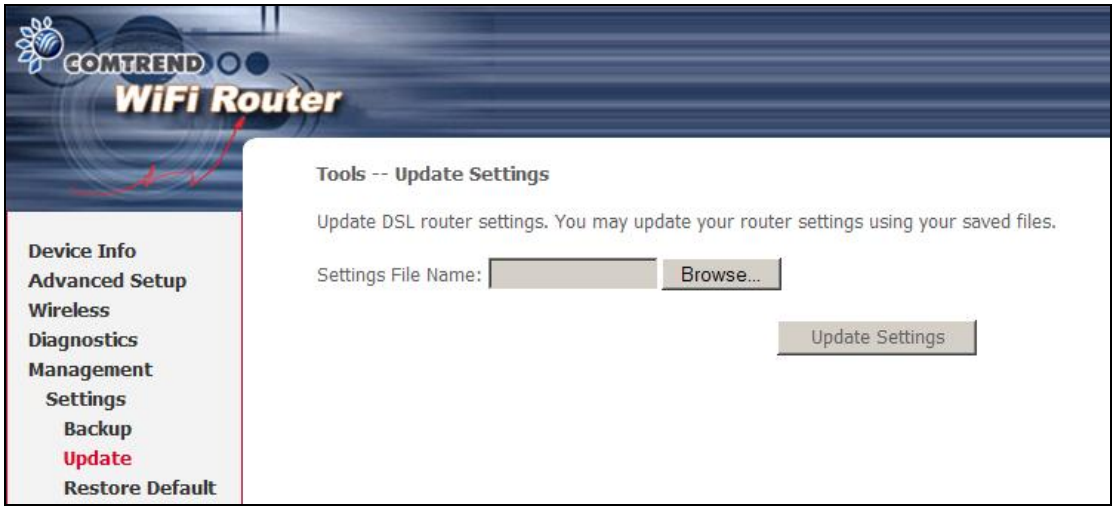
9.1.1 Backup Settings

Para salvar la configuración actual a un fichero, haga clic en el botón **Backup Settings**. Se le pedirá una localización en su PC donde guardar el fichero de seguridad. Este fichero puede ser recuperado posteriormente utilizando el botón **Update Settings** descrito a continuación.



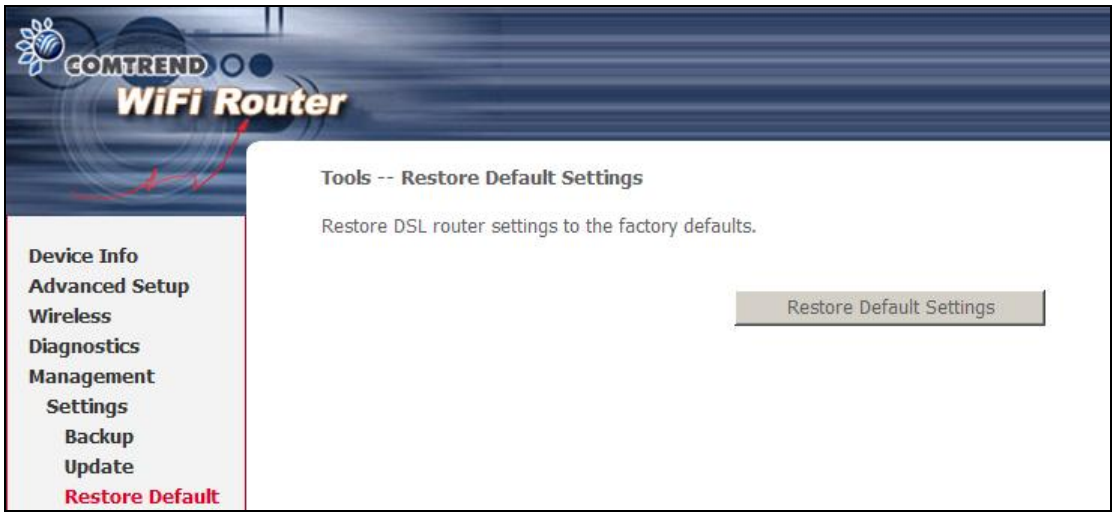
9.1.2 Update Settings

Esta opción recupera el fichero de configuración salvado anteriormente utilizando el botón **Backup Settings**. Introduzca el nombre del fichero (incluyendo su localización) en el campo **Settings File name** o haga clic en el botón **Browse...** para buscar el fichero. Haga clic en el botón **Update Settings** para recuperar la configuración.

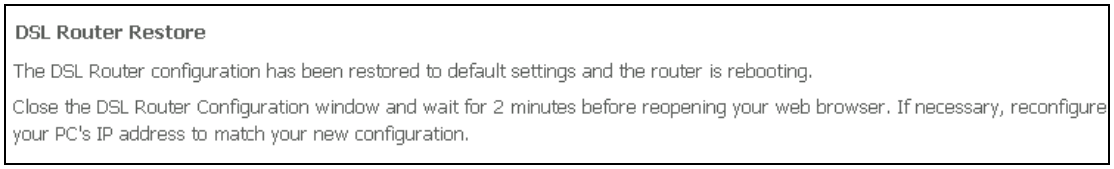


9.1.3 Restore Default

Haga Clic en el botón **Restore Default Settings** para restaurar los valores de fábrica o por defecto.



Después de cliquear el botón **Restore Default Settings**, se mostrará la siguiente pantalla.



Cierre el navegador y espere 2 minutos antes de reabrirlo. Puede ser necesario, reconfigurar la configuración IP de su PC para que coincide con la nueva configuración.

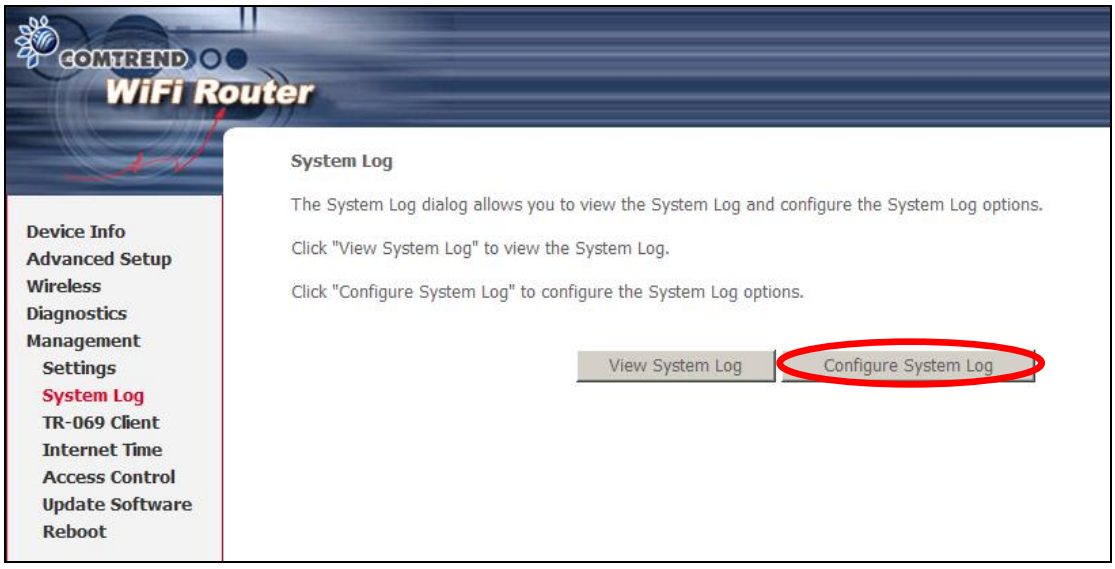
NOTA:	Esta entrada tiene el mismo efecto que el botón **Reset**. El WAP-5813n y su bootloader soportan el reseteo por defecto. Si el botón **Reset** es pulsado continuamente durante más de 5 segundos, el bootloaders borrará la configuración salvada en la memoria flash.

9.2 System Log

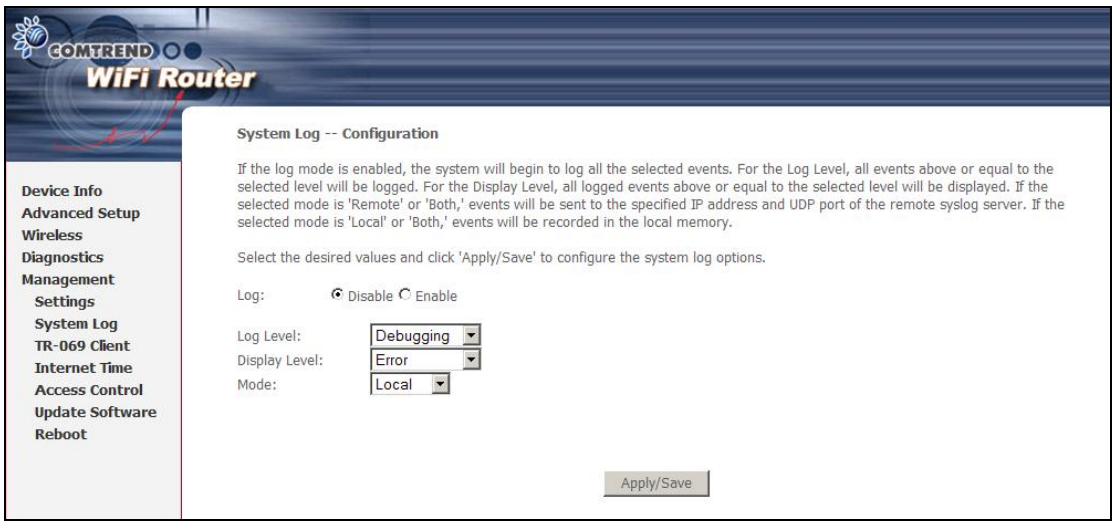
Esta función permite guardar los log del sistema solicitado.

Siga los pasos inferiores para configurar, activar y ver los log de sistema.

PASO 1: Haga clic en el botón **Configure System Log**, como se muestra a continuación (marcado en **Rojo**).



PASO 2: Seleccione las opciones deseadas y haga clic en el botón **Apply/Save**.

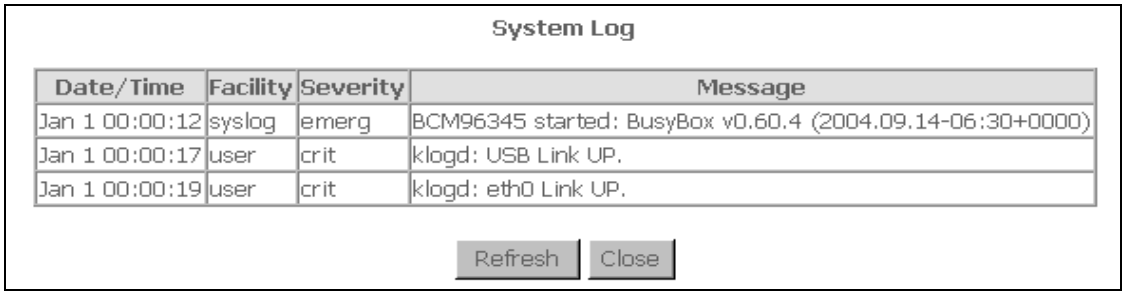


Consulte la siguiente tabla para descripción detallada de cada opción de log de sistema.

Opción	Descripción
Log	Indica si el sistema está grabando actualmente los eventos. El usuario puede activar o desactivar los eventos a loguear. Por defecto, está desactivado. Para activarlo, seleccione **Enable** en el botón de opción y haga clic en el botón **Apply/Save**.

Opción	Descripción
Log Level	Le permite configurar el nivel de evento y filtrar los eventos no deseados. El rango de eventos que van desde el nivel más crítico "Emergency" hasta el nivel configurado será grabado en el buffer de log de la SDRAM del WAP-5813n. Cuando el buffer de log esté lleno, sobrescribirá los eventos más antiguos. Por defecto, el nivel de log es "Debugging", el cual es el nivel menos crítico. Los niveles de log están definidos a continuación: • Emergency = el sistema es inutilizable • Alert = deben tomarse medidas de inmediata • Critical = Condiciones críticas • Error = Condiciones de error • Warning = condición normal pero significativa • Notice= condición normal pero insignificativa • Informational= proporciona información de referencia • Debugging = Mensajes de nivel Debug. Emergency es el nivel más serio, mientras que Debugging es el menos importante. Por ejemplo, si el nivel de registro se establece en la Debugging, todos los acontecimientos desde el nivel más bajo de depuración para el nivel más crítico a nivel de emergencia serán registrados. Si el nivel de log se fija a Error, solo el nivel de Error o superior será logueado.
Display Level	Permite al usuario seleccionar los eventos de log y mostrarlos en la ventana **View System Log** para los eventos de este nivel o superior al nivel Emergency.
Mode	Le permite que especifique los eventos que deben ser almacenados en la memoria local, o ser enviados a un sistema de log remoto como un servidor syslog, o a ambos simultáneamente. Si el modo remoto está seleccionado, la vista de log de sistema no estará disponible para mostrar los eventos salvados en el sistema remoto o servidor syslog. Cuando el modo remoto o ambos modos están configurados, el WEBGUI mostrará el usuario para introducir la dirección IP del servidor y su puerto UDP.

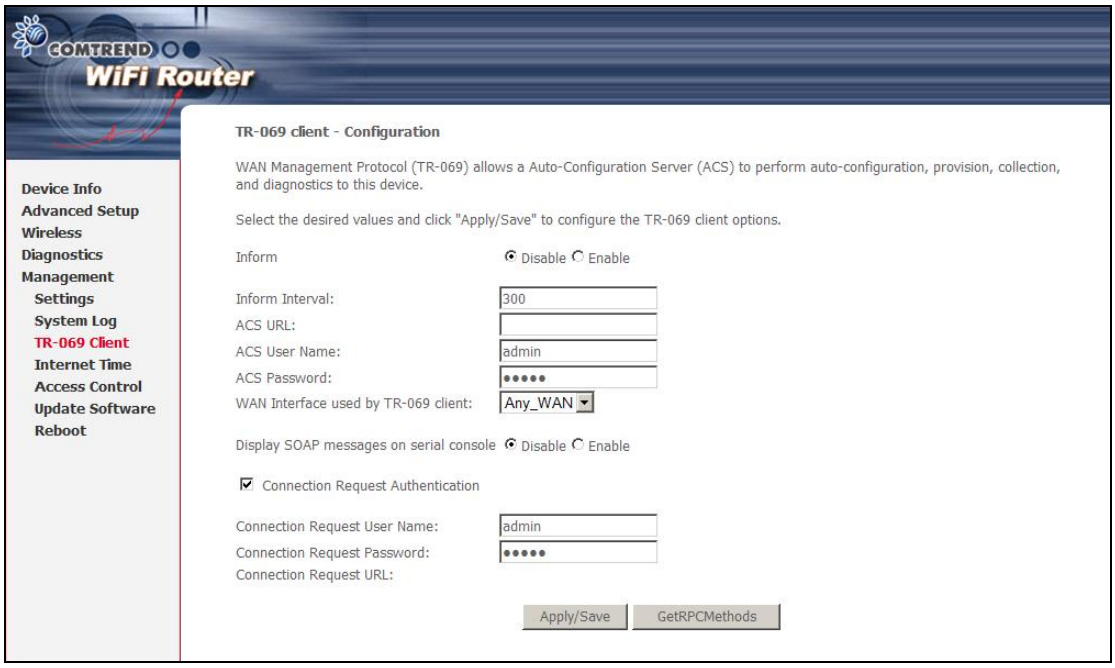
PASO 3: Haga Clic en el botón **View System Log**. Los resultados se mostraran como a continuación.



9.3 TR-069 Client

WAN Management Protocol (TR-069) permite a un Auto-Configuration Server (ACS)

llevar a cabo la autoconfiguración, provisión, colección, y diagnósticos del dispositivo. Seleccione los valores deseados y haga clic en el botón **Apply/Save** para configurar las opciones del cliente TR-069.



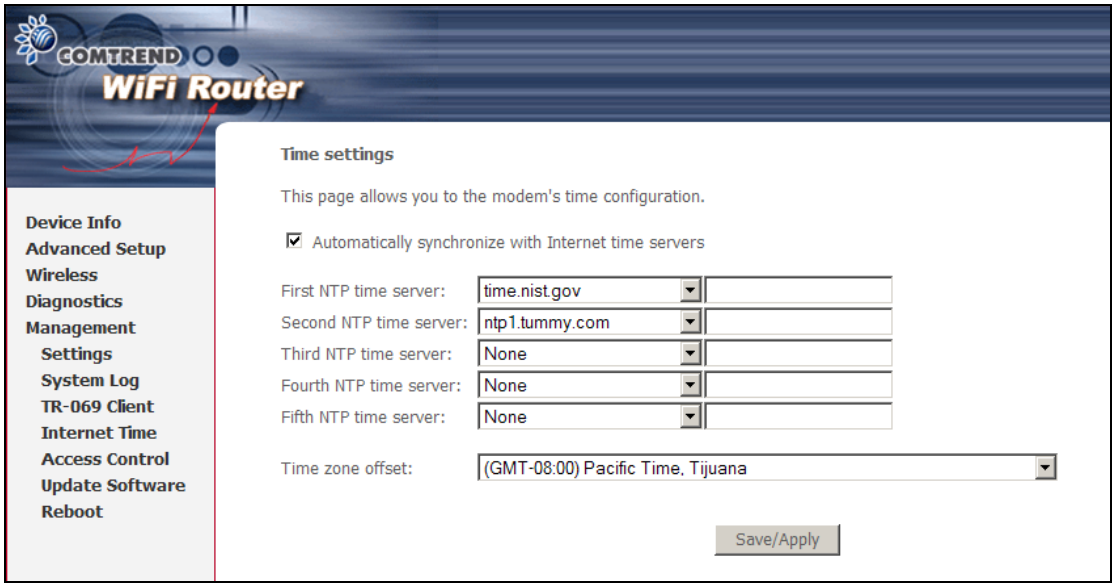
Opción	Descripción
Inform	Activa/desactiva el cliente TR-069 en el CPE.
Inform Interval	La duración del intervalo en segundos para la cual el CPE debe atender la conexión con el ACS y llamar al método Inform.
ACS URL	URL para el CPE para conectarse al ACS utilizando WAN Management Protocol. Este parámetro debe tener formato URL valido para HTTP o HTTTPS. Una URL HTTPS indica que el ACS soporta SSL. El CPE usa un certificado para validarse en al URL del ACS donde se realiza una autenticación basada en certificado.
ACS User Name	Nombre de usuario utilizado para autenticar el CPE cuando se realiza una conexión al ACS utilizando WAN Management Protocol. Este nombre de usuario es usado solo para autenticación HTTP por el CPE.
ACS Password	Contraseña utilizada para autenticar el CPE cuando se realiza una conexión al ACS utilizando WAN Management Protocol. Esta contraseña es usada solo para autenticación HTTP por el CPE.
WAN Interface used by TR-069 client	Seleccionar Any_WAN, LAN, Loopback o una conexión configurada.
Display SOAP messages on serial console	Activa/desactiva Mensajes SOAP o consola serie. Esta opción es usada para troubleshooting avanzado del CPE.
Solicitud de conexión	
Authorization	Marque la casilla de verificación para activarlo. ☑
User Name	Nombre de usuario usado para autenticar una solicitud de conexión realizada a un ACS por el CPE.

Opción	Descripción
Password	Contraseña usada para autenticar una solicitud de conexión realizada a un ACS por el CPE.
URL	Universal Resource Locator.

El botón **Get RPC Methods** fuerza que el CPE establezca una conexión inmediata al ACS. Este debe ser usado para descubrir los métodos de configuración soportados por el ACS o por el CPE. Esta lista debe incluir ambos métodos estándar TR-069 (Estas definiciones en la especificación o en versiones posteriores) y métodos específicos del proveedor. El receptor de la respuesta debe ignorar cualquier método irreconocible.

9.4 Internet Time

Esta opción sincroniza automáticamente el tiempo y hora del router con un servidor de tiempo de internet. Para habilitar la sincronización horaria, marque la correspondiente casilla de verificación, seleccionando el servidor de tiempo preferido, seleccionar la correcta zona horaria y haga clic en el botón **Save/Apply.**



NOTA:	Internet Time debe estar activado para usar el control paterno o Parental Control (página 34). Además, este menú no es mostrado en modo Bridge, ya que el router no sería capaz de conectar con el servidor NTP.

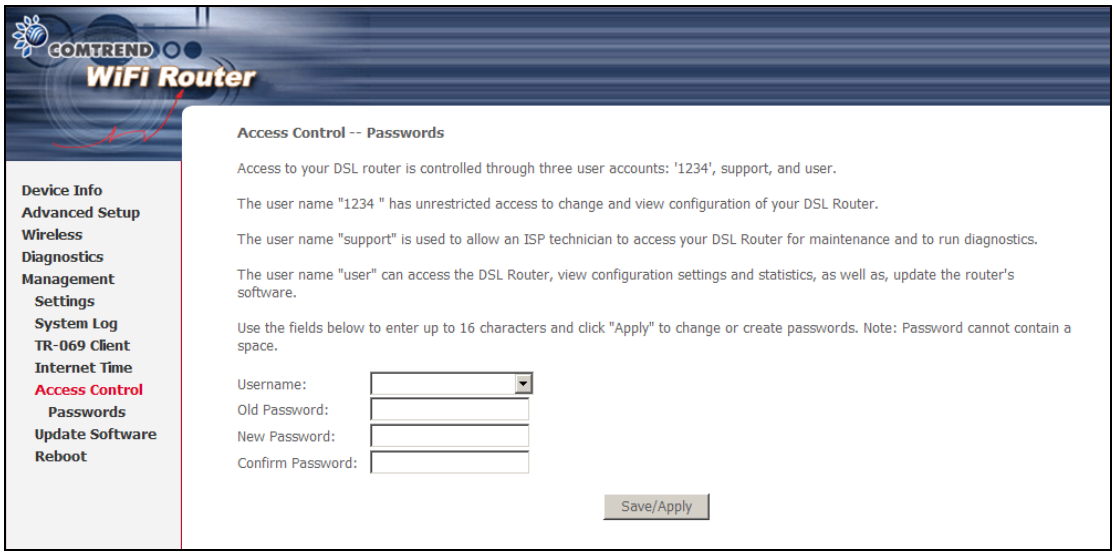
9.5 Access Control

9.5.1 Passwords

Esta pantalla es usada para configurar la contraseña de las cuentas de usuarios utilizadas para acceder el dispositivo. El acceso al WAP-5813n es controlado a través del siguiente árbol de usuarios:

- **1234** – Tiene acceso sin restricciones para cambiar y visualizar la configuración.
- **support** – Usado para mantenimiento remoto y diagnostico del router.
- **User** – Tiene acceso limitado. Esta cuenta puede ver los parámetros de configuración y estadísticas, así como, actualizar el firmware del router.

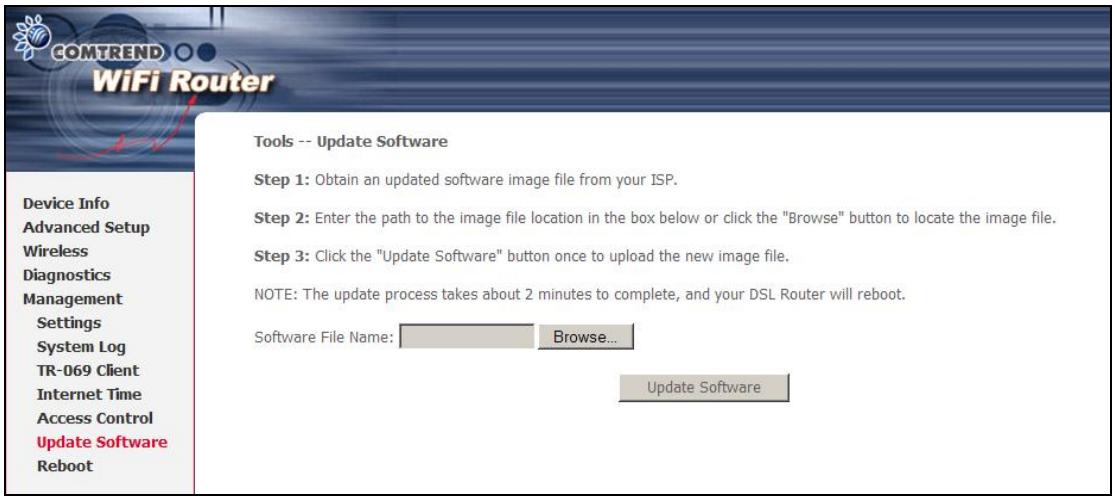
Use los siguientes campos para cambiar los parámetros de la contraseña. Haga clic en el botón **Save/Apply** para continuar.



NOTA: La contraseña o password debe tener máximo 16 caracteres.

9.6 Update Software

Esta opción permite llevar a cabo una actualización de firmware desde un fichero almacenado de forma local.



Paso 1: Obtener el fichero imagen de la versión de software a actualizar desde su ISP.

Paso 2: Introduzca la ruta y nombre de fichero de la imagen de versión de software en el campo **Software File Name** o haga clic en el botón Browse

para localizar el fichero imagen.

Paso 3: Haga clic en el botón **Update Software** una vez para actualizar e instalar el fichero.

NOTA:	El proceso de actualización durará aproximadamente 2 minutos para completarse. El dispositivo se reiniciará y la ventana del navegador se refrescará a la pantalla por defecto si la instalación ha sido satisfactoria. Es recomendable que se compare la versión de software en la parte alta de la pantalla **De vice Info** con la versión de firmware instalada, para confirmar la instalación satisfactoria.

9.7 Save and Reboot

Para salvar la configuración actual y reiniciar el router haga clic en el botón **Save/Reboot**.

NOTA: Es necesario cerrar la ventana del navegador y esperar 2 minutos antes de reabrirla. Es necesaria también para resetear la configuración IP de su PC.

Apéndice A – Firewall

STATEFUL PACKET INSPECTION

Referido a una arquitectura, donde el firewall o cortafuegos realiza un seguimiento de los paquetes en cada conexión que atraviesa todas las interfaces y asegurando que son validas. Este es un contraste un filtrado de paquetes estático, donde sólo se examina el paquete basándose en la información de encabezado de cada paquete.

Es un incidente en el cual el usuario u organización se ve privado de los servicios o recursos que normalmente espera usar o tener. Varios Ataques DoS (Denial of service o Denegación de servicio) de los que el CPE puede resistir son ARP Attack Ping Attack Ping of Death Land, SYN Attack, Smurf Attack, and Tear Drop.

FILTRADO DE TCP/IP/PUERTO/INTERFAZ

Estas reglas ayudan en el filtrado de tráfico en la capa de red (capa 3). Cuando un interfaz de Routing es creado, se debe chequear que el firewall o cortafuegos debe estar activo.
Navegue hasta Advanced Setup → Security → IP Filtering.

Filtrado IP de salida.

Ayuda en el establecimiento de reglas para cortar paquetes desde las interfaces LAN. Por defecto, si el cortafuego está activado, todo el tráfico desde la LAN es permitido. Para configurar una o más reglas, se debe especificar los tipos de paquetes provenientes desde la LAN que pueden ser cortados.

Ejemplo 1:	Filter Name	: Out_Filter1
	Protocol	: TCP
	Source IP address	: 192.168.1.45
	Source Subnet Mask	: 255.255.255.0
	Source Port	: 80
	Dest. IP Address	: NA
	Dest. Subnet Mask	: NA
	Dest. Port	: NA

Este filtro tirará o cortará todos los paquetes provenientes de la LAN con la dirección IP y mascara de red 192.168.1.45/24 teniendo como origen el Puerto 80 independiente mente del destino. Los otros paquetes serán aceptados.

Ejemplo 2:	Filter Name	: Out_Filter2
	Protocol	: UDP
	Source IP Address	: 192.168.1.45
	Source Subnet Mask	: 255.255.255.0
	Source Port	: 5060:6060
	Dest. IP Address	: 172.16.13.4
	Dest. Subnet Mask	: 255.255.255.0
	Dest. Port	: 6060:7070

Este filtro tirará o cortará todos los paquetes UDP provenientes desde la LAN con dirección IP y mascara de red 192.168.1.45/24 y origen el rango de puertos desde el 5060 al 6060, destino a 172.16.13.4/24 y destino el rango de puertos desde el 6060 al 7070.

Filtrado IP de entrada

Ayuda a configurar reglas de aceptación o denegación de paquetes provenientes desde el interfaz WAN. Por defecto, todo el tráfico IP entrante desde la WAN es bloqueado, si el firewall está activado. Para configurar uno o más filtros, se debe especificar los tipos de paquetes provenientes de la WAN que pueden ser aceptados.

Ejemplo 1:

Filter Name	: In_Filter1
Protocol	: TCP
Policy	: Allow
Source IP Address	: 210.168.219.45
Source Subnet Mask	: 255.255.0.0
Source Port	: 80
Dest. IP Address	: NA
Dest. Subnet Mask	: NA
Dest. Port	: NA
Selected WAN interface	: br0

Este filtro acepta todos los paquetes provenientes del interfaz WAN "br0" con IP y mascara de red 210.168.219.45/16 con origen el Puerto 80, independientemente el destino. El resto de paquetes provenientes de esta interfaz serán tirados o cortados.

Ejemplo 2:

Filter Name	: In_Filter2
Protocol	: UDP
Policy	: Allow
Source IP Address	: 210.168.219.45
Source Subnet Mask	: 255.255.0.0
Source Port	: 5060:6060
Dest. IP Address	: 192.168.1.45
Dest. Sub. Mask	: 255.255.255.0
Dest. Port	: 6060:7070
Selected WAN interface	: br0

Esta regla aceptará todos los paquetes UDP provenientes del interfaz WAN "br0" con IP y máscara de red 210.168.219.45/16 y origen el rango de puertos desde el 5060 al 6060, destino 192.168.1.45/24 y destino el rango de puertos desde el 6060 al 7070. El resto de paquetes provenientes de este interfaz serán tirados o cortados.

Filtrado en capa MAC

Estas reglas ayudan en el filtrado de tráfico a nivel 2. El filtrado MAC es solo efectivo en modo Bridge. Después de que una conexión de tipo Bridge es creada, seleccione Advanced Setup → Security → MAC Filtering en el menú WEBGUI.

Ejemplo 1:

Global Policy	: Forwarded
Protocol Type	: PPPoE
Dest. MAC Address	: 00:12:34:56:78:90
Source MAC Address	: NA
Src. Interface	: eth1
Dest. Interface	: eth2

Añadiendo esta regla se tirarán o cortarán todos los frames PPPoE provenientes de eth1 a eth2 con destino la dirección MAC 00:12:34:56:78:90 independientemente de la dirección MAC origen. El resto de frames de este interfaz serán permitidos.

Ejemplo 2:

Global Policy	: Blocked
Protocol Type	: PPPoE

Dest. MAC Address : 00:12:34:56:78:90
Source MAC Address : 00:34:12:78:90:56
Src. Interface : eth1
Dest. Interface : eth2

Añadiendo esta regla permite que todos los frames PPPoE con dirección eth1 a eth2 con destina la dirección MAC 00:12:34:56:78 y origen la dirección MAC 00:34:12:78:90:56. El resto de frames de este interfaz serán tirados o cortados.

Configuración de día y hora del Control Parental.

Esta funcionalidad restringe el acceso al exterior a través del WAP-5813n a un dispositivo LAN seleccionado, así como elegir los días de la semana y horas.

Ejemplo:
User Name : FilterJohn
Browser's MAC Address : 00:25:46:78:63:21
Days of the Week : Mon, Wed, Fri
Start Blocking Time : 14:00
End Blocking Time : 18:00

Con esta regla, un dispositivo LAN con la dirección 00:25:46:78:63:21 no tundra acceso a la WAN los Lunes, Miércoles y viernes, de 2 p.m. a 6 p.m. En otros horarios y días, el dispositivo tendrá acceso al exterior.

Apéndice B – designación de Pin.

Puertos ETHERNET (RJ45)

Pin	Definición	Pin	Definición
1	Transmit data+	5	NC
2	Transmit data-	6	Receive data-
3	Receive data+	7	NC
4	NC	8	NC

Apéndice C – Especificaciones

Interfaces Hardware

RJ-45 X 1 para WAN (Giga Ethernet), RJ-45 X 4 para LAN (Giga Ethernet), Botón WPS X 1, Interruptor de encendido/Apagado X 1, Botón Wi-Fi On/Off X 1, Botón Reset X 1

Interfaz LAN

Standard.....IEEE 802.3, IEEE 802.3u
10/100 BaseT .....Auto-sense
MDI/MDX support.....Yes

Interfaz WLAN

Standard .....IEEE802.11n (IEEE802.11b/g compatible)
Encryption.....64/128-bit Wired Equivalent Privacy (WEP)
Channels.....11 (US, Canada)/ 13 (Europe)/ 14 (Japan)
Data Rate.....Up to 300Mbps
WPA/WPA2 .....Yes
IEEE 802.1x .....Yes
WMM .....Yes
WPS .....Yes
MAC Filtering .....Yes
Optional.....Afterburner mode (Turbo mode)***

Gestión

Cumple con los protocolos de gestión remota TR-069/TR-098/TR-111, Telnet, Gestión basada en Web, backup y restauración de la configuración, actualización de software por via servidor HTTP / TFTP / FTP

Funciones de enrutamiento:

PPPoE, IPoA, Static route, RIP v1/v2, NAT/PAT, DMZ, DHCP Server/Relay/Client, DNS Proxy, ARP, IGMP Proxy

Funciones de seguridad:

Protocolos de autenticación: PAP, CHAP
Port Triggering/Forwarding, Packet and MAC address filtering, DoS Protection, SSH, VPN

Passthrough de aplicaciones

PPTP, L2TP, IPSec, VoIP, Yahoo messenger, ICQ, RealPlayer, NetMeeting, MSN, X-box

Fuente de alimentación .....Input: 100 - 240 Vac
Output: 12 Vdc / 1.0 A

Condiciones medioambientales

Temperatura de operaciones.....0 ~ 50º C
Humedad relativa.....5 ~ 95% (no-condensado)

Dimensiones..... 205 mm (largo) x 48 mm (alto) x 145 mm (ancho)

Peso del kit

(1*WAP-5813n, 2*RJ45 cable, 1*fuente de alimentación, 1*CD-ROM) = 1.0 kg

Certificaciones ..... CE 0197, CE

NOTA:	Las especificaciones están sujetas a cambios sin previo aviso.

Apéndice D – Cliente SSH

A diferencia de Microsoft Windows, el sistema operativo Linux tiene un cliente incluido. Para los usuarios de Windows, pueden usar un software de dominio público llamado "putty" que puede ser descargado del siguiente enlace:

http://www.chiark.Verdeend.org.uk/~sgtatham/putty/download.html

Para acceder utilizando el cliente SSH debe primero activar el acceso SSG por la LAN, por la WAN o por ambas desde el menú Management → Access Control → Services en el interfaz WEBGUI.

Para acceder al router usando el cliente SSH de Linux

Para acceso LAN, teclee: ssh -l root 192.168.1.1

Para acceso WAN, teclee: ssh -l support *Dirección IP de la WAN*

Para accede al router utilizando el cliente ssh "putty" para Windows

Para acceso LAN, teclee: putty -ssh -l root 192.168.1.1

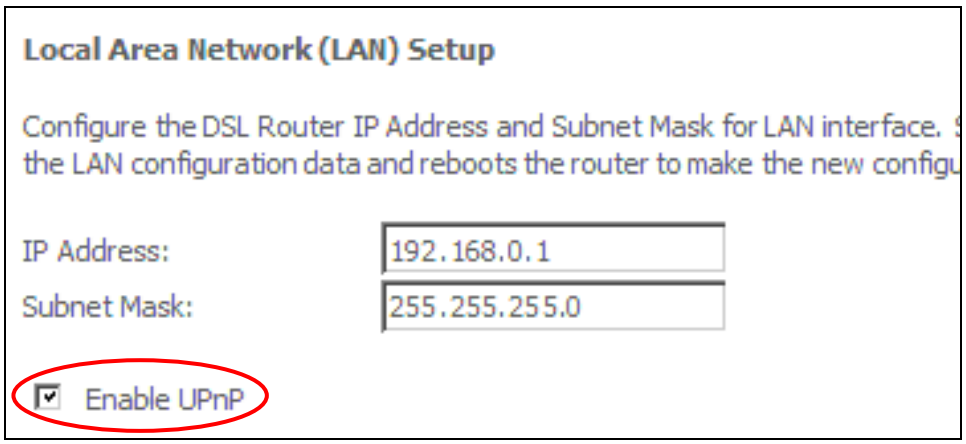
Para acceso WAN, teclee: putty -ssh -l support *Dirección IP de la WAN*

NOTA: La *Dirección IP de la WAN* puede ser encontrada en el menú Device Info → WAN

Apéndice E – Registrador externo WSC

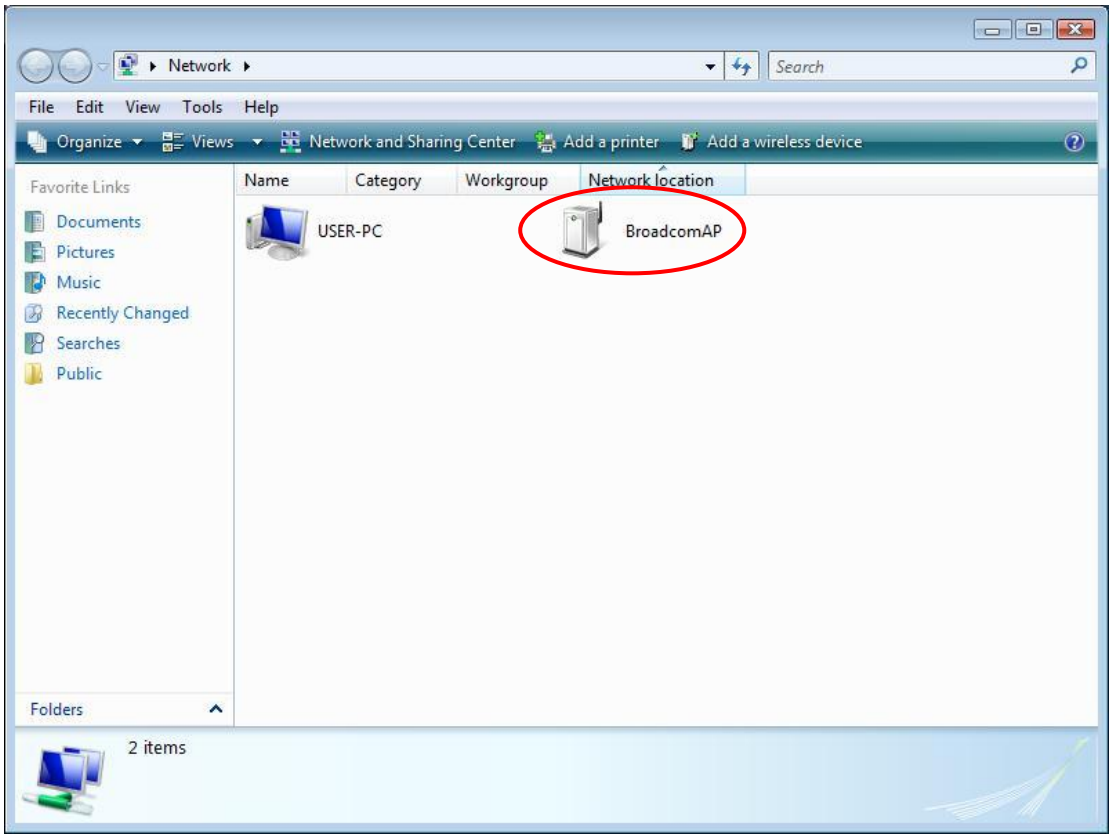
Siga estos pasos para añadir un registrador externo utilizando el interfaz WEBGUI en un PC con sistema operativo Microsoft Windows Vista:

Paso 1: Activar UPnP en el menú Advanced Setup → LAN del interfaz WEBGUI.

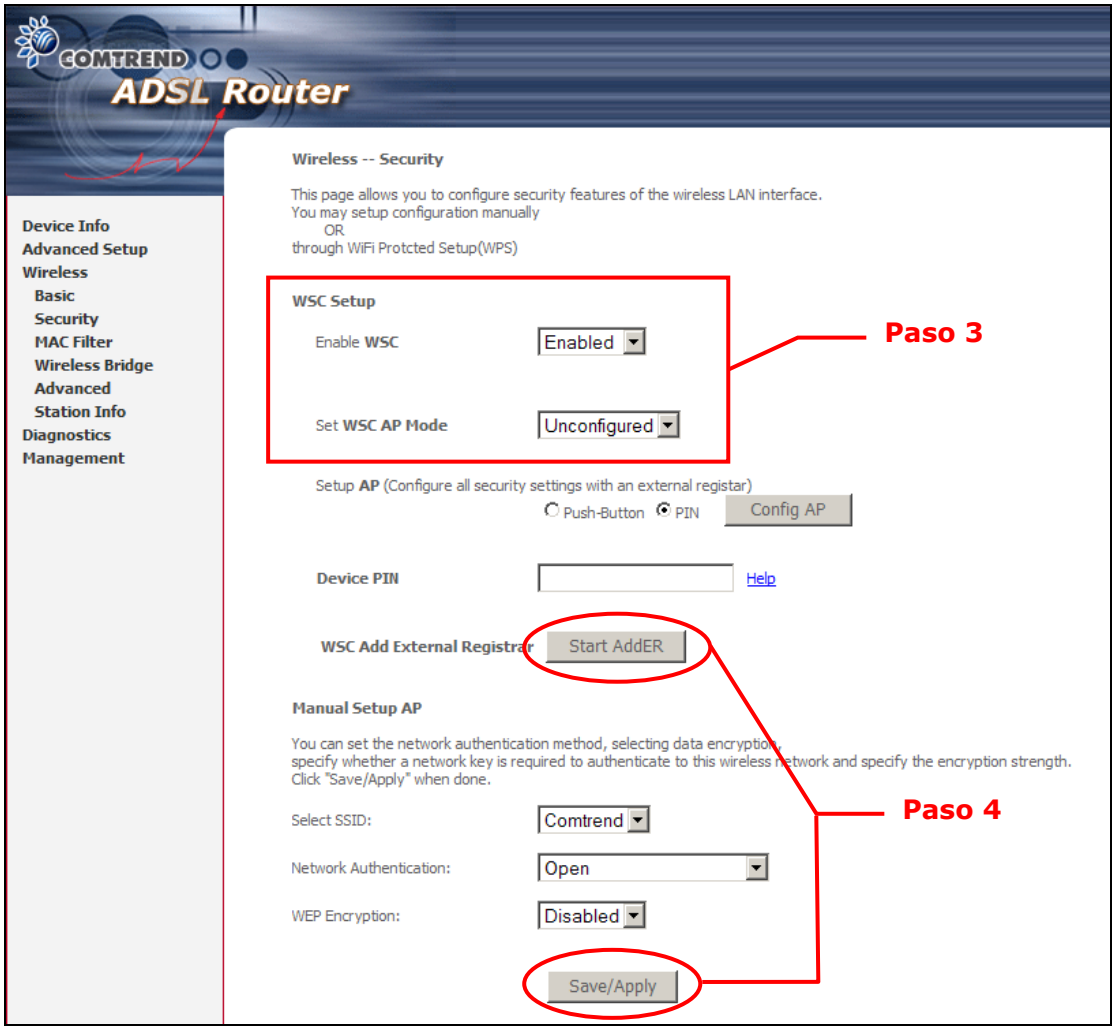


NOTA: Debe existir un PVC para ver esta opción.

Paso 2: Abrir una carpeta de red y buscar el icono BroadcomAP.

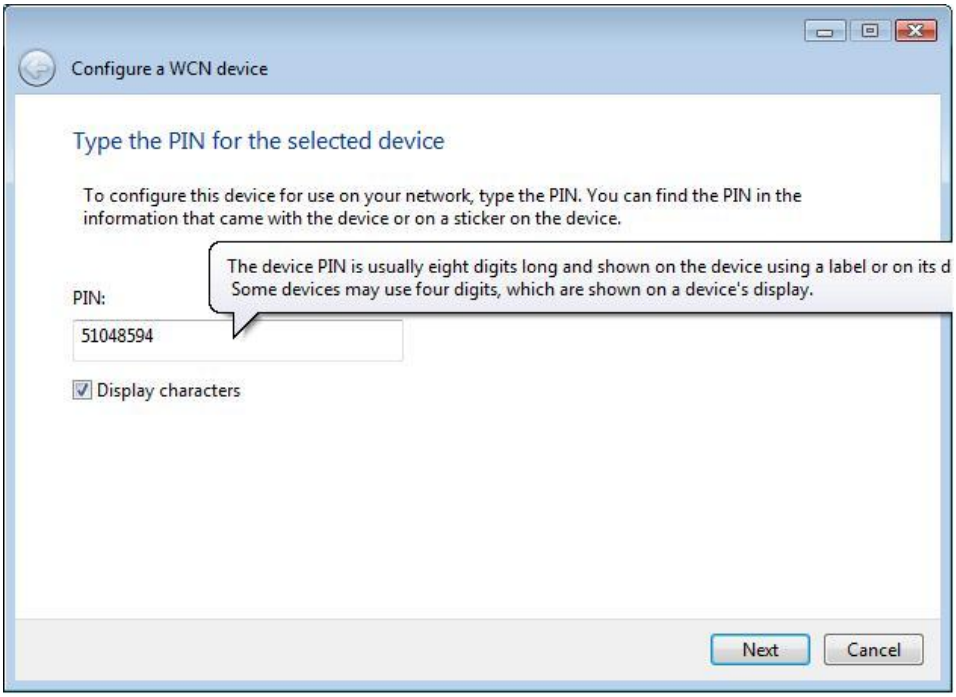


Paso 3: En el menú WEBGUI en la pantalla Wireless → Security, active WSC seleccionando **Enabled** de la lista desplegable y establezca WSC AP Mode como Unconfigured.



Paso 4: Haga clic en el botón **Save/Apply** de la pantalla. LA pantalla se pondrá en blanco mientras el router aplica la nueva configuración inalámbrica. Cuando la pantalla retorne, haga clic en el botón **Start AddER**, como se muestra a continuación.

Paso 5: Ahora retorne a la carpeta de Conexiones de red y haga clic en el icono BroadcomAP. Un cuadro de diálogo aparecerá preguntando por el número PIN del dispositivo. Introduzca el número PIN del dispositivo como es mostrado en el menú Wireless → Security. Haga clic en el botón **Next**.



Paso 6: Windows Vista intentará configurar los parámetros de seguridad la red inalámbrica.

Paso 7: Si es satisfactorio, los parámetros de seguridad coincidirán con los de Windows Vista.