Redes Inteligentes

Equipo Integrado Fibra Óptica

TriWave

Manual de Fabricante

Índice

Control de Versiones

Versión	Cambio realizado por	Descripción del cambio	Fecha
1.0		1ª Edición	30/09/2014

Introducción

Este manual proporciona información relativa al diseño, instalación y configuración del equipo TriWave y va dirigido a usuarios con conocimientos básicos de la terminología y conceptos en telecomunicaciones.

Si el equipo no funciona correctamente, puede contactar con el soporte técnico de Telnet Redes Inteligentes S.A. en la siguiente dirección de correo: operaciones@telnet-ri.es.

Para la descarga de nuevas actualizaciones, productos, manuales o actualizaciones de software, puede visitar nuestra página web: http://www.telnet-ri.es

Advertencias

El equipo TriWave está diseñado para su uso exclusivo en interiores. A continuación, se describen una serie de recomendaciones que debería tener en cuenta el usuario:

- Evita la humedad y acumulación de polvo.
- No instales este este producto cerca del agua. Por ejemplo, evitar instalaciones cerca de una bañera, lavadora,…
- Deja espacio a cada lado del equipo para la disipación de calor y no pongas objetos pesados sobre ella.
- No conectes la fuente de alimentación eléctrica en superficies elevadas. Evita conectarlas al aire libre. No se deben colocar objetos pesados sobre el cable eléctrico. Se debe evitar que el cable este en zona de tránsito para impedir pisar, caminar sobre él.
- Use únicamente la fuente de alimentación eléctrica suministrada con el equipo.
- En caso de tormenta de fuerte aparato eléctrico es recomendable la desconexión del cable de alimentación para evitar descargas.
- Desconecte siempre todos los cables y conexiones de corriente eléctrica antes de realizar un mantenimiento o reparación del producto.
- La conexión a la red de fibra óptica es sensible a torsiones, por lo que se recomienda no manipular dicho cable, ni conectarlo y desconectarlo sin indicación previa de un operador especializado.
- Dentro de la fibra viaja una señal óptica. Por favor, evita mirar el haz de luz que circula por la fibra pues puede dañar su visión. Evita manipular el cable sobre el que está adherida la etiqueta “Láser de clase 1”.

PRODUCTO LASER CLASE 1

No mirar por la salida de la Fibra Óptica

Descripción del equipo

El equipo TriWave es un terminal diseñado para el uso en entornos de hogar y de negocio. Como equipo integrado de fibra óptica, tiene las propiedades de un equipo integrado, multipuerto y con capacidades inalámbricas que te permitirá la conexión de varios terminales de usuario a la línea FTTH de fibra óptica, basada en la tecnología GPON (Redes Ópticas Pasivas de Alta Capacidad), que proporciona canales de datos de alta velocidad.

Este equipo permite el acceso a la red IP, proporcionando servicios de alta calidad como la conexión a Internet, el servicio telefónico de Voz sobre IP, y el servicio de TV por Internet sin necesidad de ningún equipo adicional.

Características Técnicas

Características Hardware

- 1 puerto óptico SC/APC con acceso GPON (ITU-T G.984.x)

Interfaz G.984.2	Transmisión		Recepción		
	Longitud de onda	Potencia de Transmisión	Longitud de onda	Sensibilidad	Potencia Saturación
B+	1260-1360nm	+0,5/ +5 dBm	1480-1500nm	-28 dBm	> -8 dBm
C+	1290-1320nm	+0,5/ +5 dBm	1480-1500nm	-30 dBm	> -8 dBm

- 3 puertos LAN RJ45 IEEE 802.3ab 10/100/1000 Base-T

- 1 puertos de telefonía RJ11 (Interfaz POTs: G.711 A/u, T.38, RTP/RTCP, SIP). Interfaces FXS

Interfaz FXS (RJ11). Puertos Telf 1-2. Características de transmisión	Valores
Nivel de la señal portadora a la salida	-16 dBm
Banda de frecuencias	300-3400 Hz
Frecuencia de referencia de niveles relativos	1020 Hz
Impedancia nominal	600 Ohms resistivos
Nivel de ruido	< -60dBm
Nivel medio máximo de TX (entrada PTR)	< -10dBm (10s)
Nivel de pico máximo	< 1,5V

- Punto de acceso WIFI 802.11b/g/n con dos antenas de 3dBi (IEEE802.11n, compatible con clientes IEEE802.11b/g. Autenticación: IEEE 802.1x, a través EAP. Seguridad: IEEE 802.11i/e)

Funcionalidades LAN

- 3 puertos 10/100/1000BaseT Ethernet RJ-45 IEEE 802.3
- Autodetección de cable ethernet cruzado (Auto-MDI/MDI-X)
- Implementación bridge IEEE 802.1d
- Configuración de VLANs según el estándar 802.1Q
- Priorización de tráfico a nivel 2 mediante 802.1p
- Servidor DHCP

Características Wifi

- Punto de acceso IEEE 802.11b/g/n
- Soporte WEP, WPA, WPA2
- Soporte WPS/WPS 2.0

Routing

- Encapsulación IPoE según RFC2684 (evolución de la RFC 1483)
- Encapsulación PPPoE según RFC 2516
- Soporte de protocolo RIP v1 y v2
- IP multicast, IGMP snooping, IGMP proxy
- ICMP según RFC 1256
- NAT/PAT
- Soporte FullCone NAT
- DHCP client/relay
- DNS proxy
- Calidad de Servicio:
- Clasificación de tráfico por puerto, dirección IP, protocolo IP, 802.1p, DSCP o rango de puertos TCP/UDP
- Hasta 8 colas de salida
- Gestión de colas mediante WRR o SP
- Traffic shaping

Capacidades Firewall

- Filtrado por dirección origen, dirección destino, puerto origen y puerto destino
- Stateful Packet Inspection
- Redirección de puertos

Telefonía

- Cliente VoIP
- Ofrece dos puertos FXS
- Provisión mediante OMCI o TR-104

Gestión

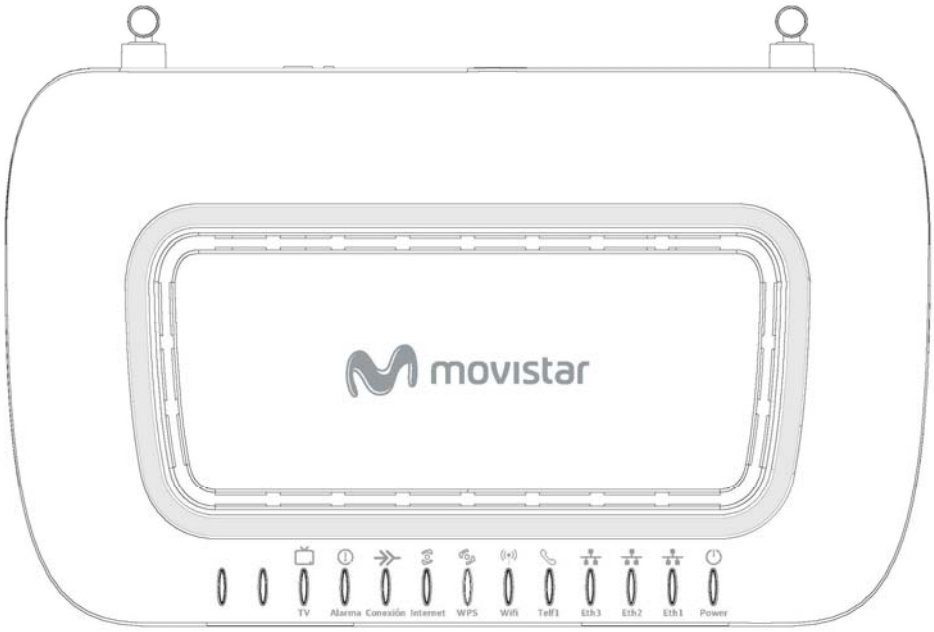
- Gestión mediante interfaz web
- Gestión remota mediante TR-069
- Provisión de canal GPON mediante OMCI
- FTP o HTTP para descargas de configuración y actualización de software

Alimentación y Normativas

- Alimentación 12VDC-2,5A. ETSI ES 202 874-1 V1.2.1 (2012-05).
- Condiciones Ambientales: ETSI 300 019 –1-1/1-2/1-3.
- Resistencia: EN 60068-2-31:2008/-2-32
- Compatibilidad Electromagnética: EN 300 328 V1.7.1 (2006-10); EN 301-489-1 V1.8.1 + EN 301-489-17 V2.1.1
- Emisiones: EN 50385: 2002. Seguridad e Inmunidad: EN 60950-1:2006 + A11:2009 + A1:2010 + A12:2011; EN 62311 (2008-11); IEC 60825-1

Diseño

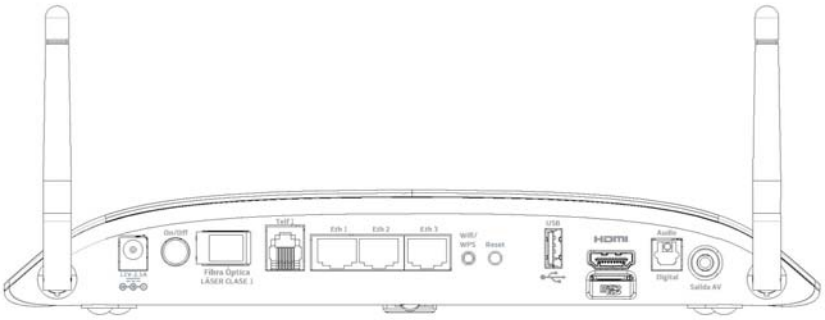
Vista Superior



Indicador	Estado Actual	Significado
Power	**Verde fijo**	El "Equipo Integrado Fibra Óptica" está alimentado.
	Verde intermitente (lento)	El "Equipo Integrado Fibra Óptica" está arrancando.
	Rojo fijo (20 segundos)	Fallo en el equipo durante el Post (Power On Self Test).
	Rojo intermitente (lento)	Fallo en el equipo durante el Post (Power On Self Test).
	Apagado	El "Equipo Integrado Fibra Óptica" no está encendido.
Eth 1-3	**Verde fijo**	Dispositivo conectado al puerto Ethernet. Enlace Ethernet establecido.
	Verde intermitente (lento)	Tráfico de datos en el puerto Ethernet.
	Apagado	No hay dispositivo conectado en puerto Ethernet.
Telf 1	**Verde fijo**	Servicio de voz disponible
	Verde intermitente (lento)	En proceso de registro con la red.
	Rojo fijo	Fallo de registro con la red.
	Apagado	No se dispone del servicio VoIP. No provisionado.
Wifi	**Verde fijo**	Interfaz Wifi habilitado.
	Verde intermitente (lento)	Hay tráfico de datos en la interfaz Wifi.
	Apagado	Interfaz Wifi deshabilitado.

WPS	**Verde fijo (120 segundos)**	Ventana WPS activa
	Rojo fijo	Problemas WPS.
	Apagado	WPS habilitado pero ventana WPS inactiva.
Internet	**Verde fijo**	Hay conexión PPPoE.
	Verde Intermitente (lento)	Negociación sesión PPPoE.
	Verde Intermitente (rápido)	Hay tráfico de datos.
	Rojo fijo	Fallo en la autenticación.
	Apagado	No hay conexión a Internet.
Conexión	**Verde fijo**	Enlace fibra óptica establecido. PON sincronizada.
	Apagado	Enlace de fibra óptica no establecida. PON no sincronizada
Alarma	**Rojo fijo**	Nivel de potencia de señal óptica no adecuado
	Apagado	Nivel de señal óptica adecuado

Vista Trasera



Conector	Descripción
12V-2.5A	Conector de cable de alimentación de corriente.
On/ Off	Pulsando interruptor se enciende/ apaga el equipo.
Fibra Óptica	Conector Fibra Óptica SC/APC.
Telf 1	Puerto RJ11 que permite conectar terminales telefónicos.
Eth 1-3	Conector hembra RJ45. Switch de conectores para LAN.
Wifi/ WPS	Activación / Desactivación de Wifi con pulsación corta. WPS con pulsación larga.
Reset	Con pulsación corta, reinicio TV MOVISTAR. Con pulsación larga, se restablece la configuración de fábrica.

Puesta en Marcha

En las siguientes figuras le indicamos la conexión entre el equipo TriWave y los dispositivos asociados.

- El cable de alimentación se conecta al conector macho de alimentación del equipo indicado con 12V-2.5A
- El cable de fibra óptica se conecta en el conector correspondiente durante la instalación del servicio de Fibra Óptica.
- El botón de la parte trasera ha de estar en posición de encendido (ON).

Nota: *La puesta en marcha será realizada por un operador especializado, por lo que se recomienda se manipule lo menos posible a este equipo.*
Para cualquier incidencia o duda con el funcionamiento del equipo, contacta con el servicio técnico a través de los números de atención al cliente.

Nota: *Debes tener en cuenta que para que el equipo esté completamente operativo, el indicador luminoso "Conexión" debe estar encendido en verde fijo. Este indicador en verde muestra que la conexión se ha realizado de manera correcta y se ha llevado a cabo la identificación y registro del dispositivo en la plataforma óptica.*

- Se deberá introducir el ONU ID para que el equipo integrado de fibra óptica, TriWave se registre en la plataforma de fibra óptica. Operación a realizar por el instalador a través del portal web de Instalación y Mantenimiento (uso restringido a personal cualificado).
- Conexión de terminales según servicios (datos/ IPTV, teléfono, TV).

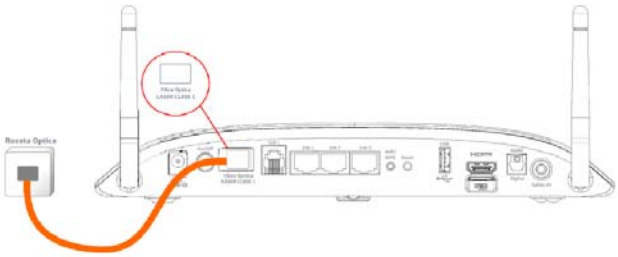


Fig. A

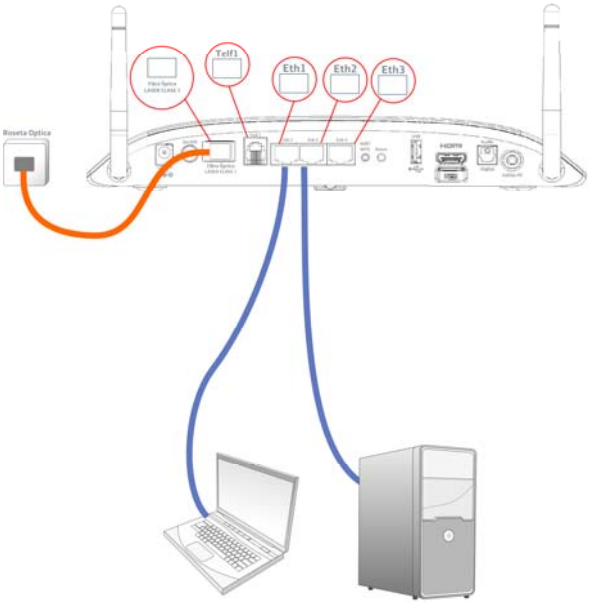


Fig. B

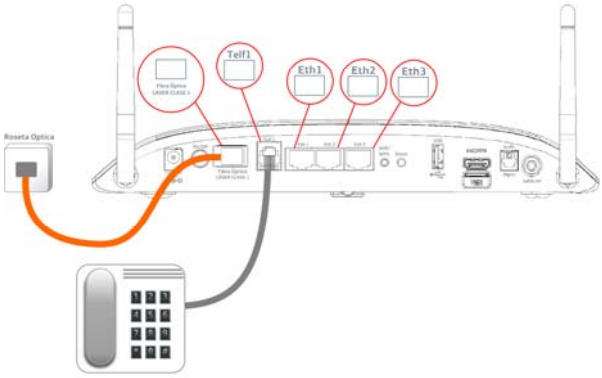


Fig. C

Fig. A. Conexión TriWave a roseta fibra óptica.

Fig. B. Conexión TriWave a equipos de usuario a través de conexión Ethernet (servicios datos/ IPTV/ VoIP).

Fig. C. Conexión TriWave a teléfono (servicio de voz).

Interfaz de Usuario Web

Este apartado describe cómo acceder al dispositivo mediante el interfaz web. Exploradores compatibles: Internet Explorer 9.0+, Chrome, Firefox,… (Ver "*Guía de Navegadores.pdf*").

Parámetros por defecto

Los parámetros de fábrica del dispositivo son:

Parámetro	Valor
Dirección IP LAN	192.168.1.1
Máscara de subred LAN	255.255.255.0
Acceso administrativo	Usuario: 1234, Contraseña: 1234
Acceso usuario	Usuario: 1234, Contraseña: 1234
Dirección IP en la WAN	Ninguna
Acceso remoto vía WAN	Desactivado
Punto de acceso inalámbrico (Wifi)	Activado
Nombre de red inalámbrica o Service Set IDentifier (SSID)	Ejemplo: MOVISTAR_XXXX

Configuración IP

MODO DHCP

Una vez el equipo TriWave esté encendido y en funcionamiento, el servidor DHCP estará activo. El servidor DHCP, asigna direcciones IP a los dispositivos conectados a la LAN.

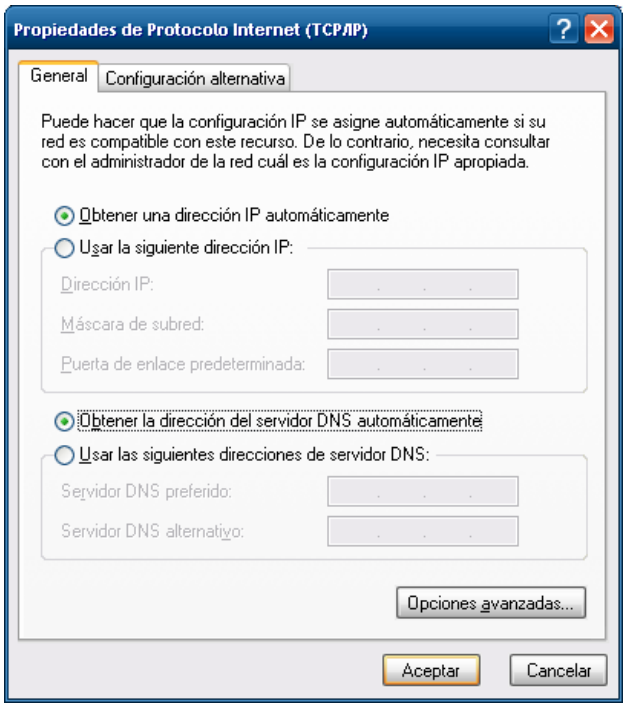
Para obtener una dirección IP del servidor DHCP, se deben seguir los siguientes pasos:

> **Nota:** *Se indican los pasos a seguir en un ordenador con sistema operativo Windows XP. Los pasos a seguir en la mayoría de los sistemas operativos son similares. En caso de duda, consulte la documentación de su sistema operativo y el documento "Guía de Navegadores.pdf".*

Paso 1: Desde la ventana de “Conexiones de Red”, abra la conexión de área local. También se puede acceder a esta ventana haciendo 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: Seleccione “Obtener una IP automáticamente” como se muestra a continuación.



Paso 4: Haga clic en el botón “OK” para aplicar los cambios.

Si encuentra dificultades al usar el modo DHCP, puede configurar el modo de direccionamiento IP estático.

MODO DE DIRECCIONAMIENTO DE IP ESTÁTICO

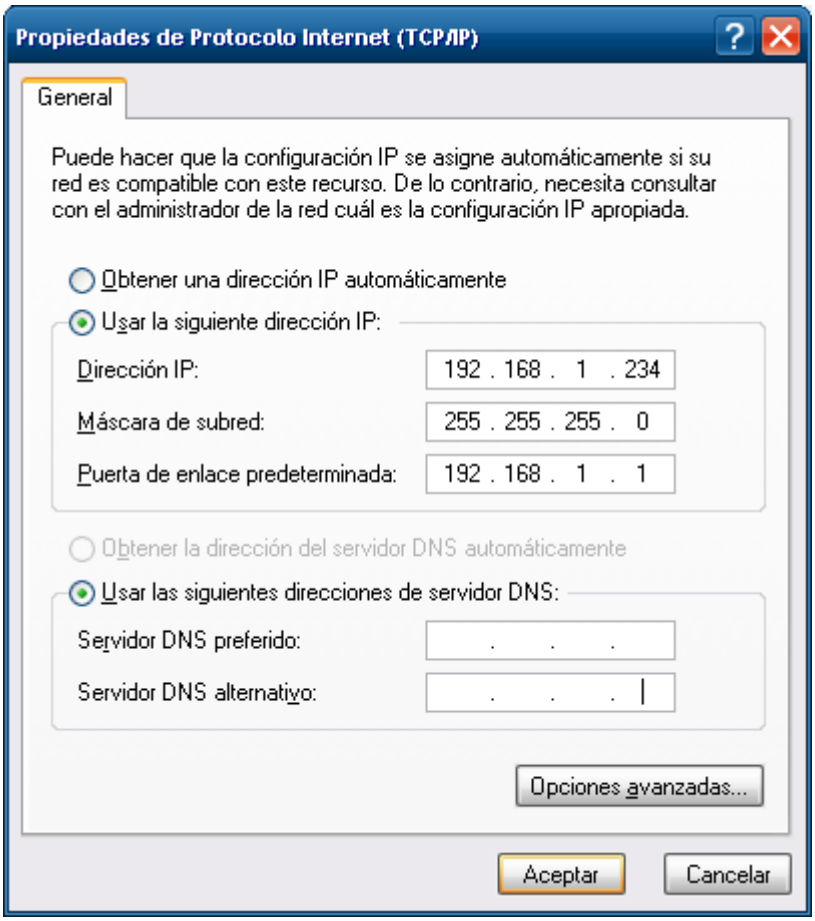
En este modo de funcionamiento, el direccionamiento IP del dispositivo no es asignado automáticamente por el equipo TriWave, sino que se establece directamente en el dispositivo terminal de usuario. Para ello, debe seguir las siguientes instrucciones.

> **Nota:** *Se indican los pasos a seguir en un ordenador con sistema operativo Windows XP. Los pasos a seguir en la mayoría de los sistemas operativos son similares. En caso de duda, consulte la documentación de su sistema operativo y el documento “Guía de Navegadores.pdf”.*

Paso 1: Desde la ventana de “Conexiones de Red”, abra la conexión de área local (también se puede acceder 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 (2<x<255) con máscara de subred 255.255.255.0 y puerta de enlace: 192.168.1.1 como se muestra a continuación:



Paso 4: Haga clic en el botón “OK” para aplicar los cambios.

Procedimiento de inicio de sesión

Para acceder a la interfaz de usuario web, debe realizar los siguientes pasos:

Paso 1: Inicie el navegador de Internet e introduzca la dirección IP del dispositivo en la barra de direcciones web. Por ejemplo: http://192.168.1.1:8080.

> **Nota:** *Para administración LOCAL (por ejemplo acceso LAN), el PC que ejecuta el navegador de Internet debe estar conectado al Puerto Ethernet del equipo TriWave.*

Paso 2: El siguiente cuadro de diálogo aparecerá, como se indica a continuación. Introduzca el nombre de usuario y contraseña (**user**: 1234/ **password**: 1234)

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.

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.

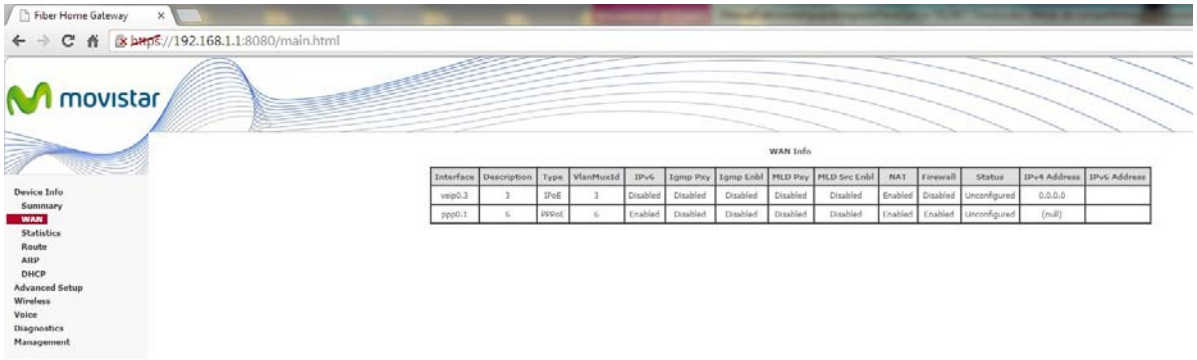
"Device Info" es la primera selección del menú principal y la primera en mostrarse. Posteriormente se mostrará una introducción.

Device Info

El primer submenú "Device Info Summary" muestra la información relativa al hardware, software, configuración IP,…

WAN

Se muestran los circuitos virtuales permanentes (PVCs) configurados.



Título	Descripción
Interface	Nombre del interfaz WAN
Description	Nombre de la conexión WAN
Type	Muestra los tipos de conexión
VlanMuxId	Muestra el ID 802.1q de la VLAN
IPv6	Direccionamiento IPv6 habilitado/ deshabilitado
IGMP Proxy	Muestra el estado de *Internet Group Management Protocol* (IGMP)
IGMP Source Enabled	
MLD Proxy	
MLD Source Enabled	
NAT	Muestra el estado de *Network Address Translation* (NAT)
Firewall	Muestra el estado del Firewall
Status	Muestra el estado de conexión PON
IPv4 Address	Muestra la dirección IPv4 para el interfaz WAN
IPv6 Address	Muestra la dirección IPv6 para el interfaz WAN

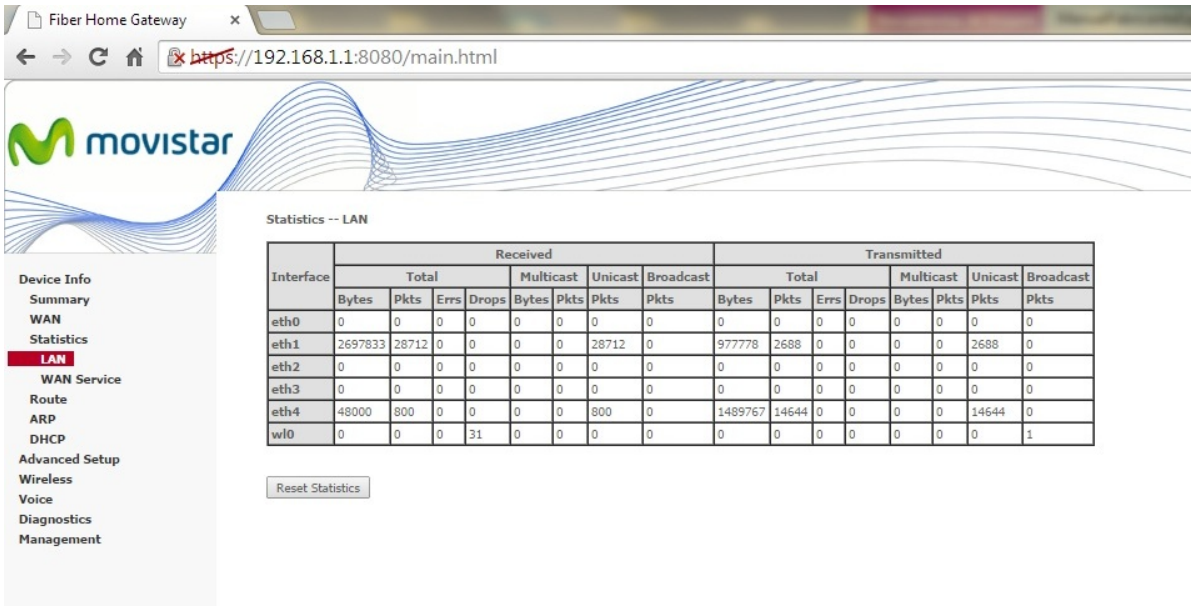
Statistics

Estadísticas. En esta sección se muestran las estadísticas facilitadas por los diferentes interfaces LAN, WAN e interfaz óptico (GPON). En cada uno de los interfaces se mostrarán los siguientes campos:

Título	Descripción
Interfaz	Nombre del interfaz
Recibidos	
Total	
- Bytes	Nº Bytes recibidos
- Pkts	Nº de paquetes recibidos
- Errs	Nº de paquetes recibidos con errores
- Drops	Nº de paquetes recibidos descartados
Multicast	
- Bytes	Nº Bytes multicast recibidos
- Pkts	Nº de paquetes multicast recibidos
Unicast	
- Pkts	Nº de paquetes unicast recibidos
Broadcast	
- Pkts	Nº de paquetes broadcast recibidos
Transmitidos	
Total	
- Bytes	Nº Bytes transmitidos
- Pkts	Nº de paquetes transmitidos
- Errs	Nº de paquetes transmitidos con errores
- Drops	Nº de paquetes transmitidos descartados
Multicast	
- Bytes	Nº Bytes multicast transmitidos
- Pkts	Nº de paquetes multicast transmitidos
Unicast	
- Pkts	Nº de paquetes unicast transmitidos
Broadcast	
- Pkts	Nº de paquetes broadcast transmitidos

LAN

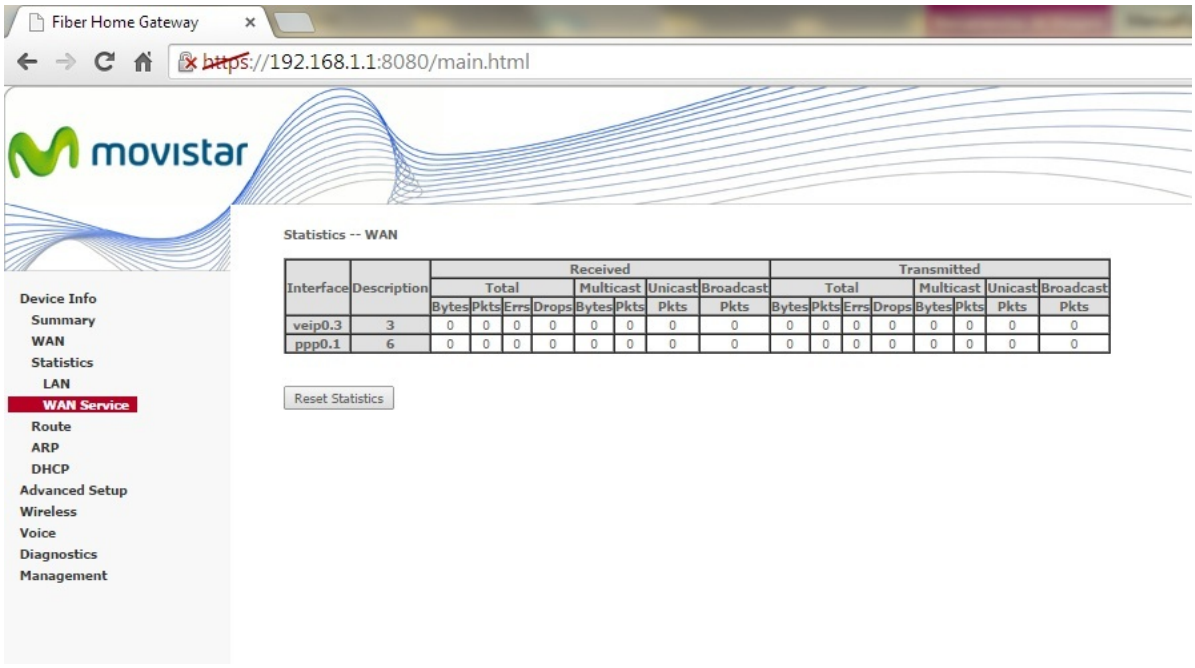
Estadísticas interfaces LAN.



Interface	Received								Transmitted							
	Total				Multicast		Unicast	Broadcast	Total				Multicast		Unicast	Broadcast
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts
eth0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
eth1	2697833	28712	0	0	0	0	28712	0	977778	2688	0	0	0	0	2688	0
eth2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
eth3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
eth4	48000	800	0	0	0	0	800	0	1489767	14644	0	0	0	0	14644	0
wl0	0	0	0	31	0	0	0	0	0	0	0	0	0	0	0	1

WAN

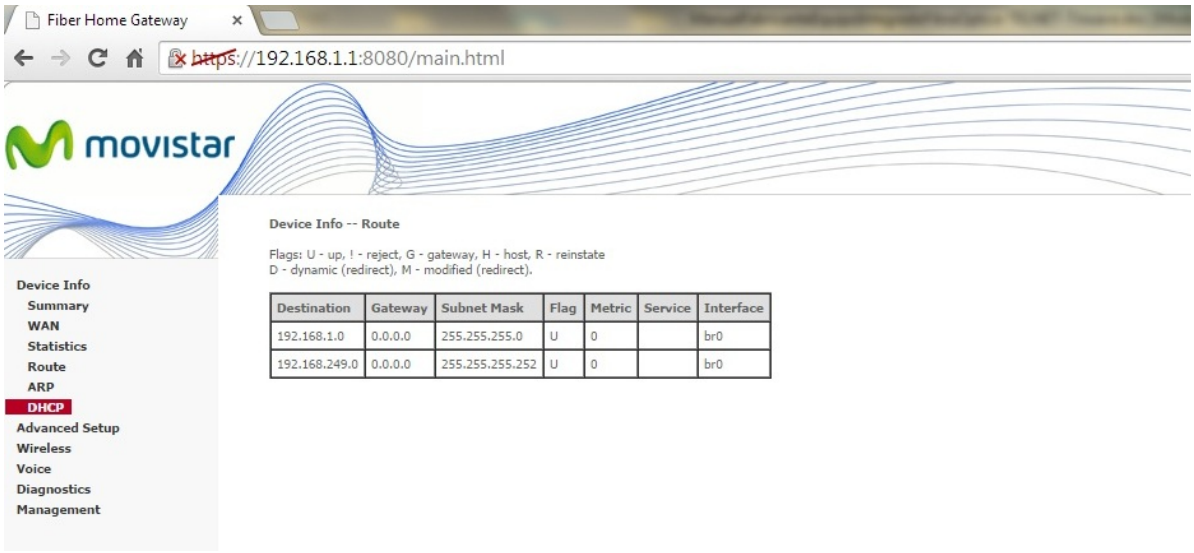
Estadísticas interfaces WAN.



Interface	Description	Received								Transmitted							
		Total				Multicast		Unicast	Broadcast	Total				Multicast		Unicast	Broadcast
		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts
veip0.3	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ppp0.1	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

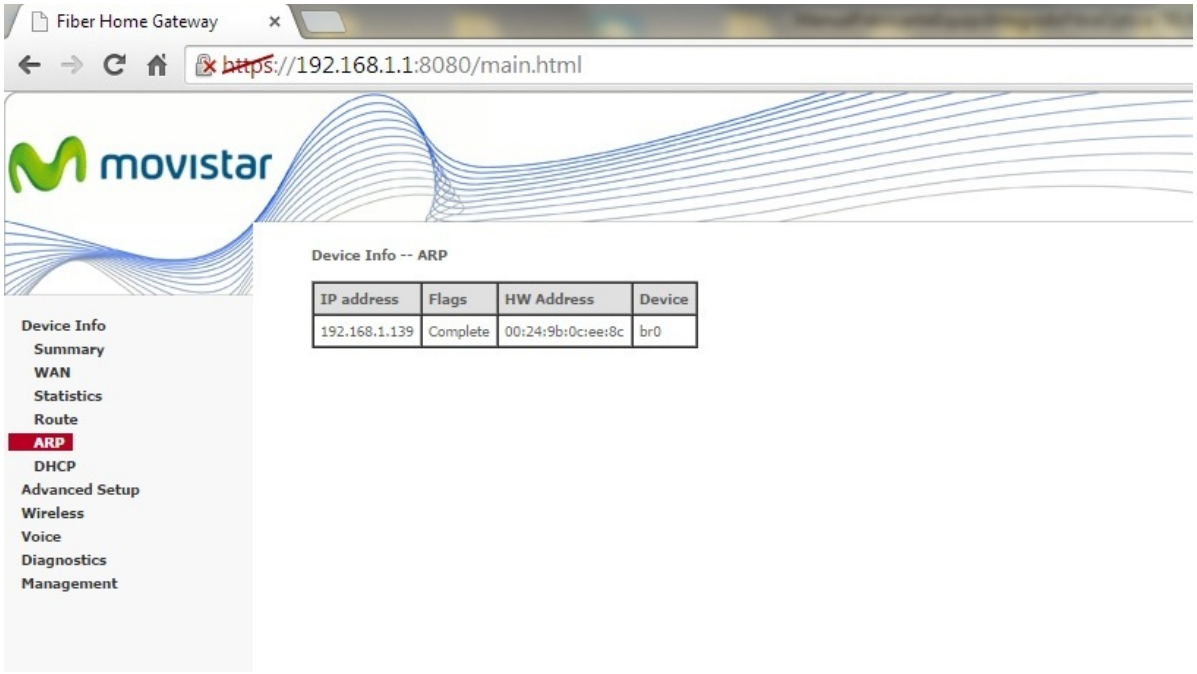
Route

Tabla de enrutamiento. Rutas dadas de alta en la generación de los diferentes servicios (datos, IPTV, voz,…).



Título	Descripción
Destination	Red/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	Muestra el estado de Internet Group Management Protocol (IGMP)
Service	Muestra el estado de Network Address Translation (NAT)
Interface	Muestra el interfaz de salida hacia la red

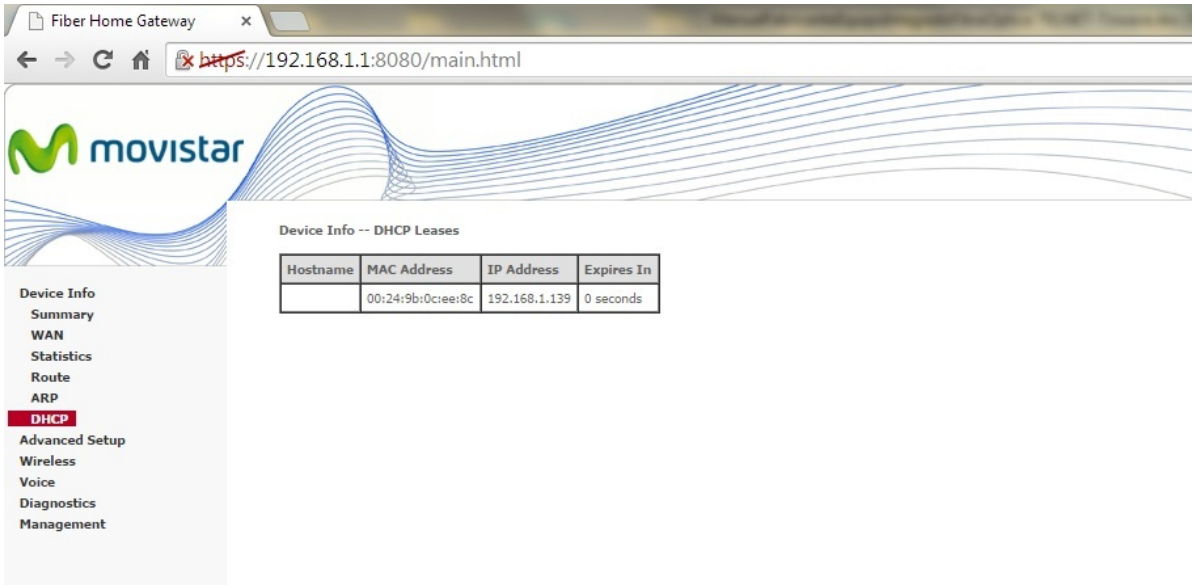
ARP



Campo	Descripción
IP Address	Dirección IP del host
Flags	Complete, Incomplete, Permanent o Publish
HW Address	Dirección MAC del host
Device	Interfaz de conexión

DHCP

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



Campo	Descripción
Hostname	Nombre del dispositivo/host en la red
MAC Address	Dirección MAC del dispositivo/host
IP Address	Dirección IP del dispositivo/host
Expires in	Tiempo que queda para la reasignación de la dirección IP del dispositivo/host a través de DHCP

Configuración Avanzada

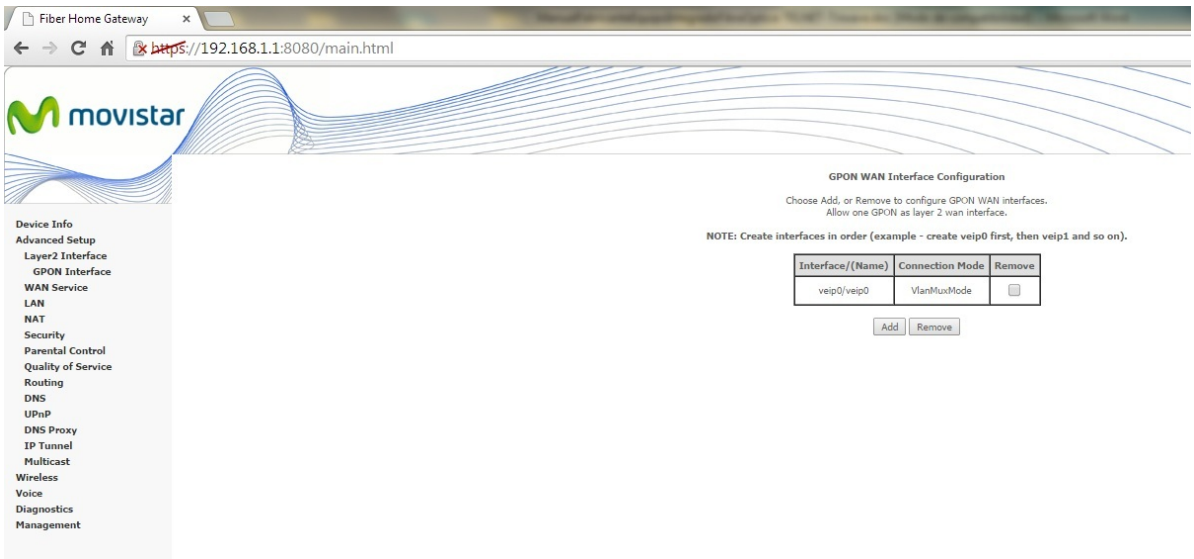
En este capítulo detallaremos las opciones avanzadas configurables a través de la web.

Layer2 Interface

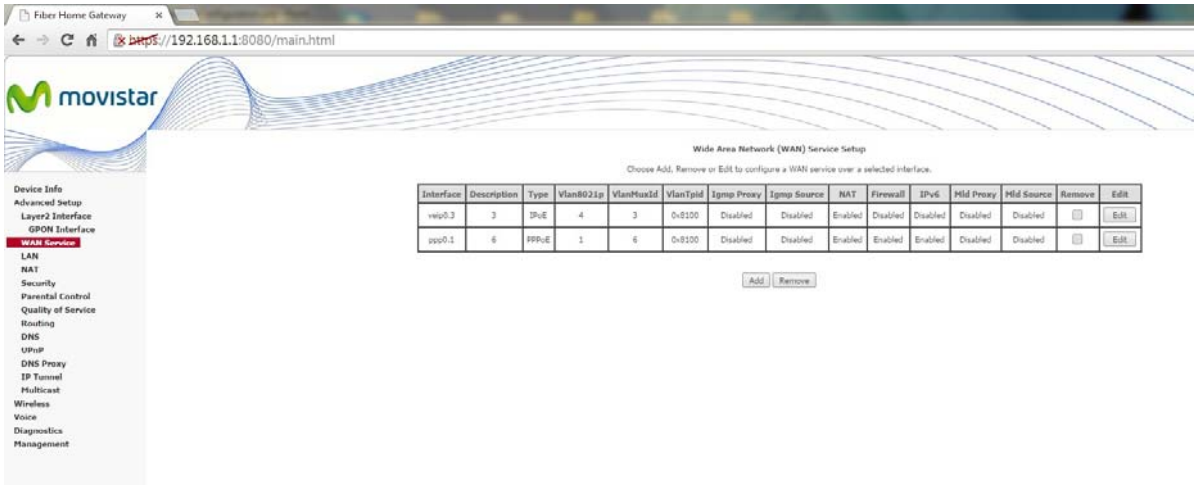
En esta pantalla podremos modificar la configuración de capa 2 de los interfaces WAN del equipo, tanto GPON como Ethernet:

Campo	Descripción
Interface	ETH WAN ó GPON WAN
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.

GPON interface



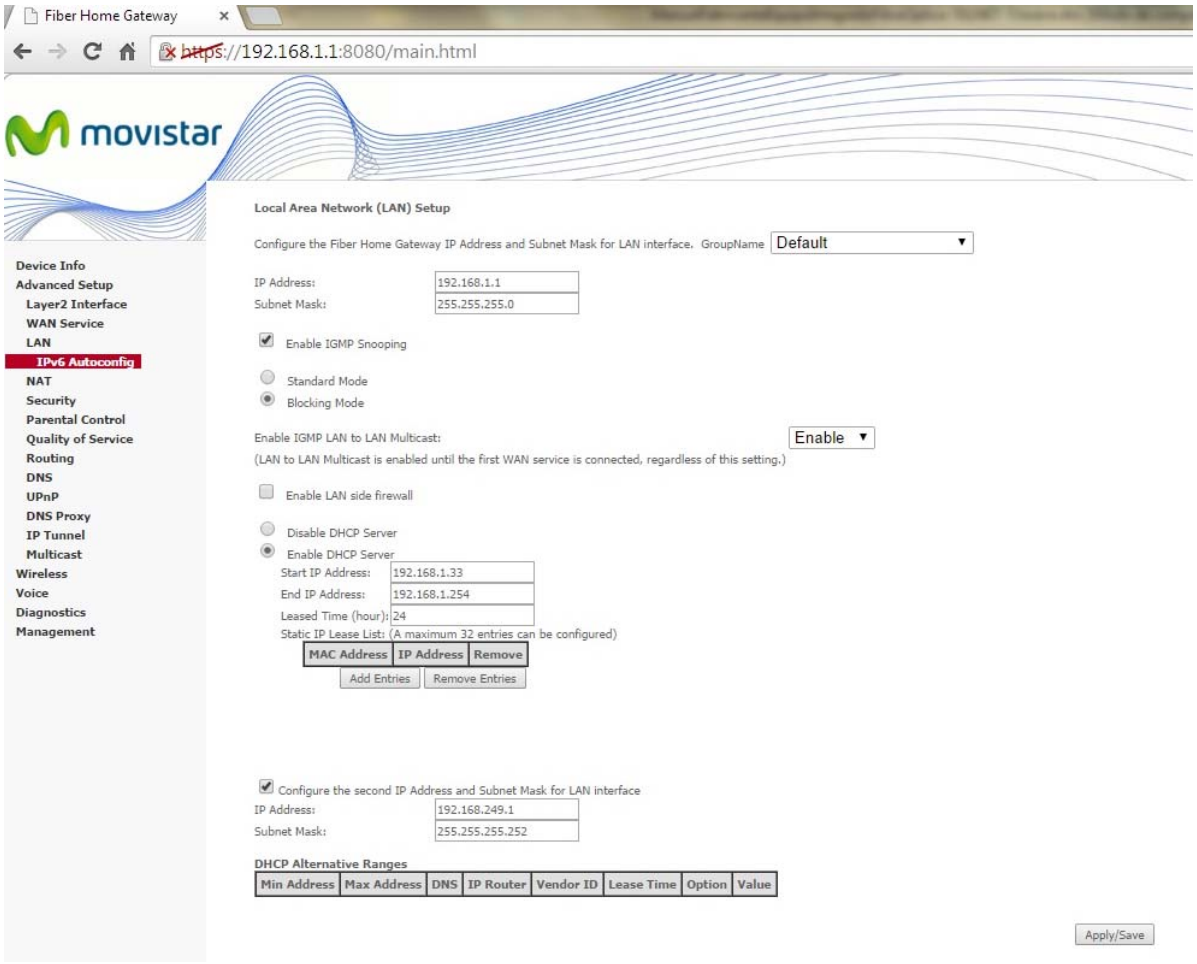
WAN Service



Título	Descripción
Interface	Nombre del interfaz WAN
Description	Nombre de la conexión WAN
Type	Muestra los tipos de conexión
Vlan8021p	Muestra la prioridad 802.1p
VlanMuxId	Muestra el ID 802.1q de la VLAN
IGMP Proxy	Muestra el estado de *Internet Group Management Protocol Proxy* (IGMP Proxy)
IGMP Source	Muestra el estado de *Internet Group Management Protocol Source* (IGMP Source)
NAT	Muestra el estado de *Network Address Translation* (NAT)
Firewall	Muestra el estado del Firewall
IPv6	Muestra si tiene habilitada la funcionalidad IPv6
MLD Proxy	Muestra si tiene habilitada la funcionalidad de IPv6 *Multicast Listener Discovery Proxy* (MLD Proxy)
MLD Source	Muestra si tiene habilitada la funcionalidad de IPv6 *Multicast Listener Discovery Source* (MLD Source)
Remove	Seleccionar la casilla de verificación y haga clic para eliminar la conexión.
Edit	Hacer clic sobre el botón para modificar los valores de los campos

LAN

Local Area Network (LAN) Setup. Esta sección permite la visualización y modificación de valores del interfaz LAN. A continuación se muestra la pantalla que aparece, así como una pequeña descripción de los parámetros.

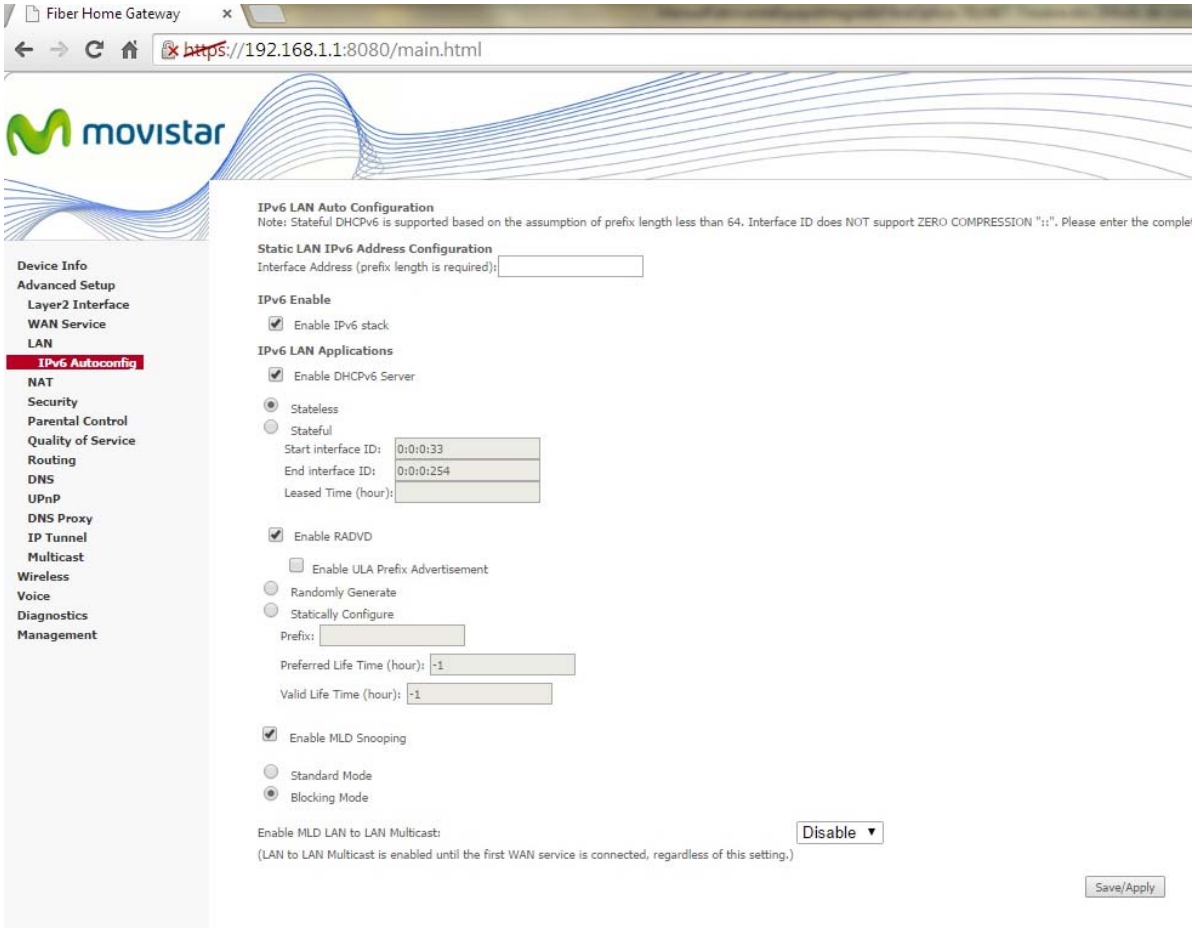


Título	Descripción
IP Address	Introduzca la dirección IP para el interfaz LAN
Subnet Mask	Introduzca la máscara de subred del interfaz LAN
Enable IGMP Snooping	Si el *check* está activado, habilita la funcionalidad *IGMP Snooping*

Standard Mode	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	El tráfico de datos multicast será bloqueado y no inundará todos los puertos
Enable IGMP LAN to LAN Multicast	Si está chequeado se habilita esta opción.
Enable LAN side firewall	Marcar esta casilla para activarlo.
Disable/Enable 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. Haciendo clic sobre el botón "*Add Entries*". En la siguiente pantalla se deberá asignar a la dirección MAC correspondiente la dirección IP deseada. Con el Botón "*Remove Entries*" se eliminarán las entradas con el *check Remove* habilitado.
Configure the second IP Address	Si se desea una segunda dirección IP en el interfaz WAN se debe habilitar esta opción
IP Address	Introduzca la dirección IP secundaria de la LAN.
Subnet Mask	Introduzca la máscara de red para la IP secundaria de la LAN.

IPv6 AutoConfig

DHCPv6 está soportado bajo la premisa de un longitud del prefijo menor que 64. Interface ID no soporta comprensión de ceros "::". Introduce la información completo. Ejemplo: "0:0:0:2" en lugar de "::2"



Título	Descripción
Interface Address	Dirección IPv6 del interfaz. Es necesario indicar la longitud del prefijo
IPv6 LAN Applications	
Enable DHCPv6 Server	.Seleccionar está opcion habilita la funcionalidad de servidor DHCPv6, permitiendo seleccionar el modo stateless o stateful.
Stateless	En esta configuración, el host utiliza el prefijo (la dirección de red y la máscara de subred), el cual es "publicado" por los dispositivos de red como parte de la creación de la dirección. Posteriormente los clientes pueden utilizar su dirección física (*MAC address*) para completar la identificación del dispositivo y así asignar la dirección IPv6.

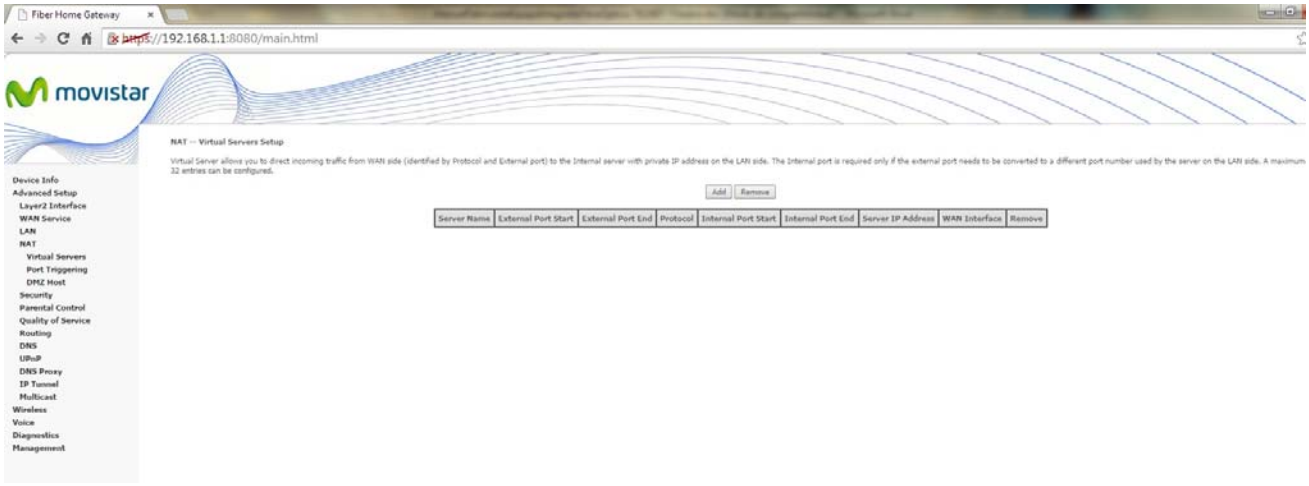
Stateful	Es un metodo similar al DHCP en IPv4, en este modo se deben definir los IDs de inicio y fin así como el tiempo en horas que se mantendrá la dirección IPv6 generada hasta una nueva actualización de la dirección (*leased time*)
Enable RADVD	Habilita el Router Adversitement Daemon
Enable ULA Prefix Advertisement	Habilita/deshabilita el anuncio de prefijos ULA. Pueden ser generado aleatoria o estáticamente.
Randomly Generate	El anuncio de prefijos será aleatorio
Statically Configure	Los prefijos serán configurados estáticamente. Habrá que configurar los siguientes parámetros: "*Prefix*", "*Preferred Life Time*" y "*Valid Life Time*".
Prefix	Valor del prefijo
Preferred Life Time (hour)	Tiempo de vida favorito en horas
Valid Life Time (hour)	Tiempo de vida valido en horas
Enable MLD Snooping	Si está chequeado, habilita el protocolo MLD
Standard Mode	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	El tráfico de datos multicast será bloqueado y no inundará todos los puertos

NAT

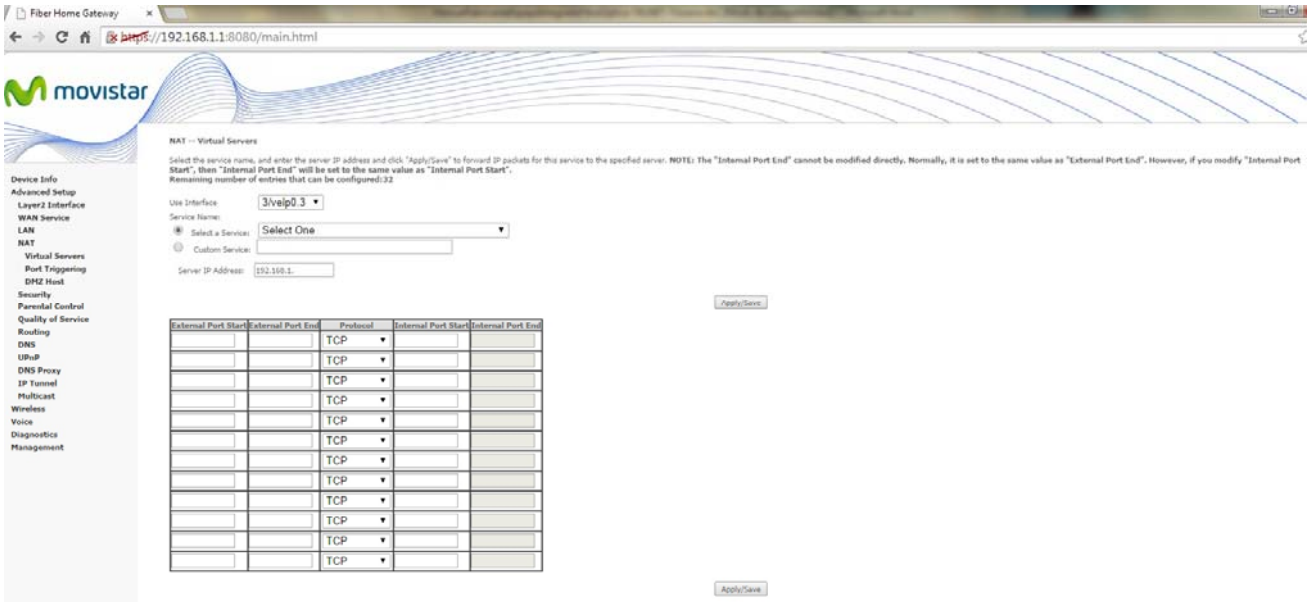
Virtual Servers

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:

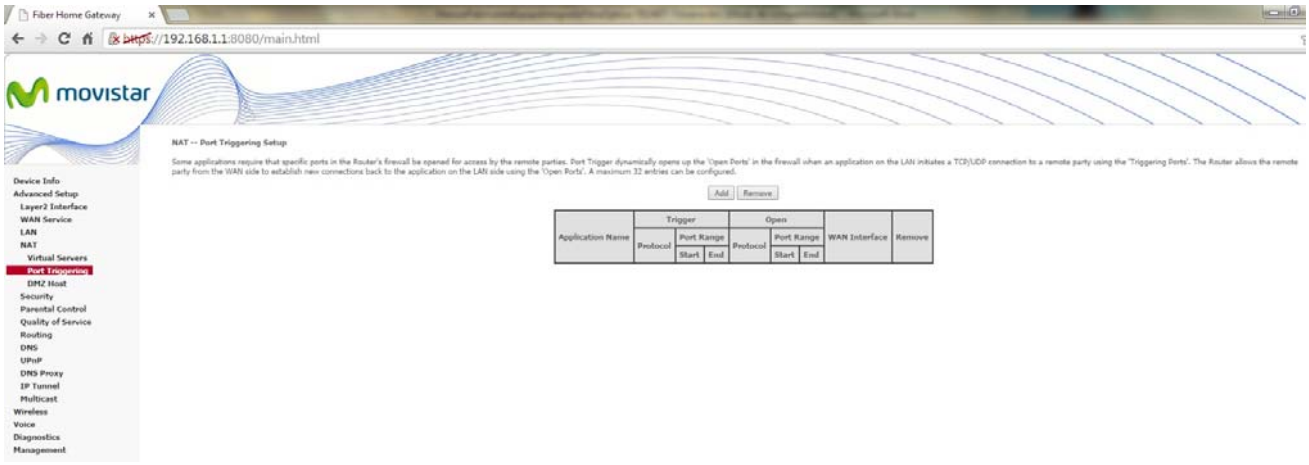


Título	Descripción
Use Interface	Seleccione el interfaz WAN de la lista desplegable
Select a service/ Custom Server	Seleccione un servicio de la lista desplegable o cree un servicio personalizado introduciendo un nombre
Server IP Address	Introduzca la dirección IP del servidor interno
External Port Start	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.
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, UDP, TCP/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.

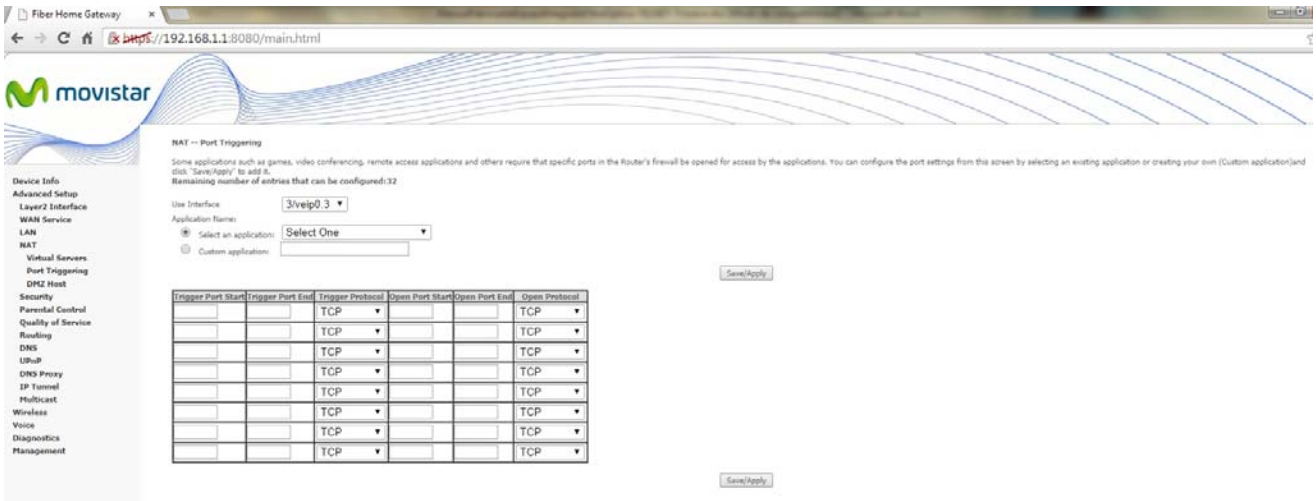
Port Triggering

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.



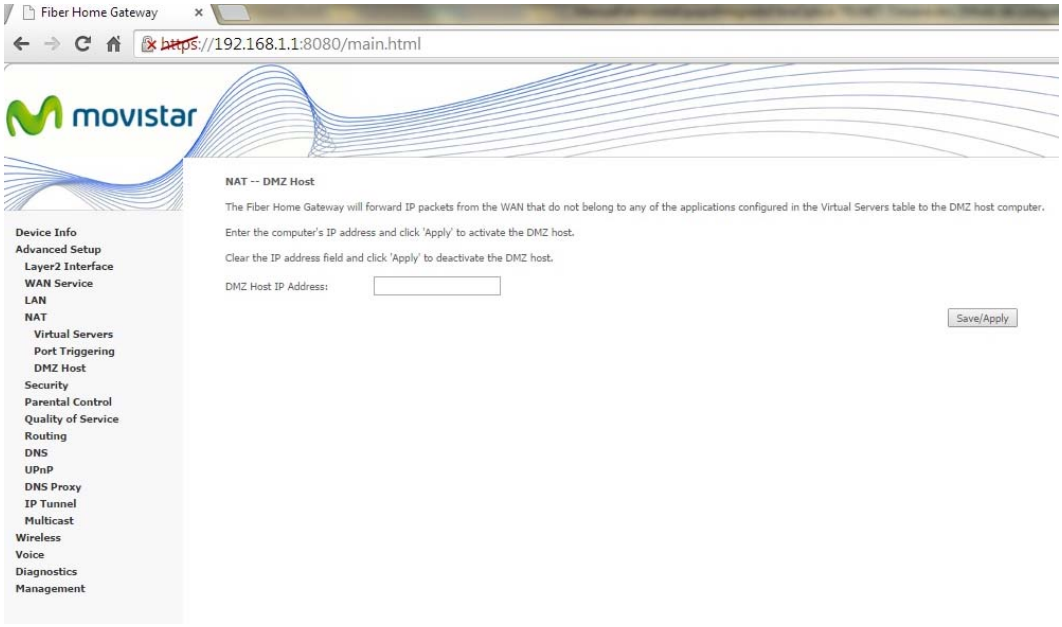
Para añadir un “Trigger Port”, haga clic en el botón “Add”. Se mostrará la siguiente pantalla:



Título	Descripción
Use Interface	Seleccione el interfaz WAN de la lista desplegable
Select an Application/ Custom Application	Seleccione una aplicación de la lista desplegable o cree una aplicación personalizada introduciendo un nombre
Trigger Port Start	Introduzca el puerto Trigger de inicio de rango (cuando seleccione una aplicación personalizada o “Custom Server”). Cuando una aplicación es seleccionada, el rango de puertos se configura automáticamente.
Trigger Port End	Introduzca el puerto Trigger de fin de rango (cuando seleccione una aplicación personalizada o “Custom Server”). Cuando una aplicación es seleccionada, el rango de puertos se configura automáticamente.
Trigger Protocol	TCP, UDP, TCP/UDP
Open Port Start	Introduzca el puerto abierto de inicio de rango (cuando seleccione una aplicación personalizada o “Custom Server”). Cuando una aplicación es seleccionada, el rango de puertos se configura automáticamente.
Open Port End	Introduzca el puerto abierto de fin de rango (cuando seleccione una aplicación personalizada o “Custom Server”). Cuando una aplicación es seleccionada, el rango de puertos se configura automáticamente.
Open Protocol	TCP, UDP, TCP/UDP

DMZ Host

TriWave permite el paso 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*”.

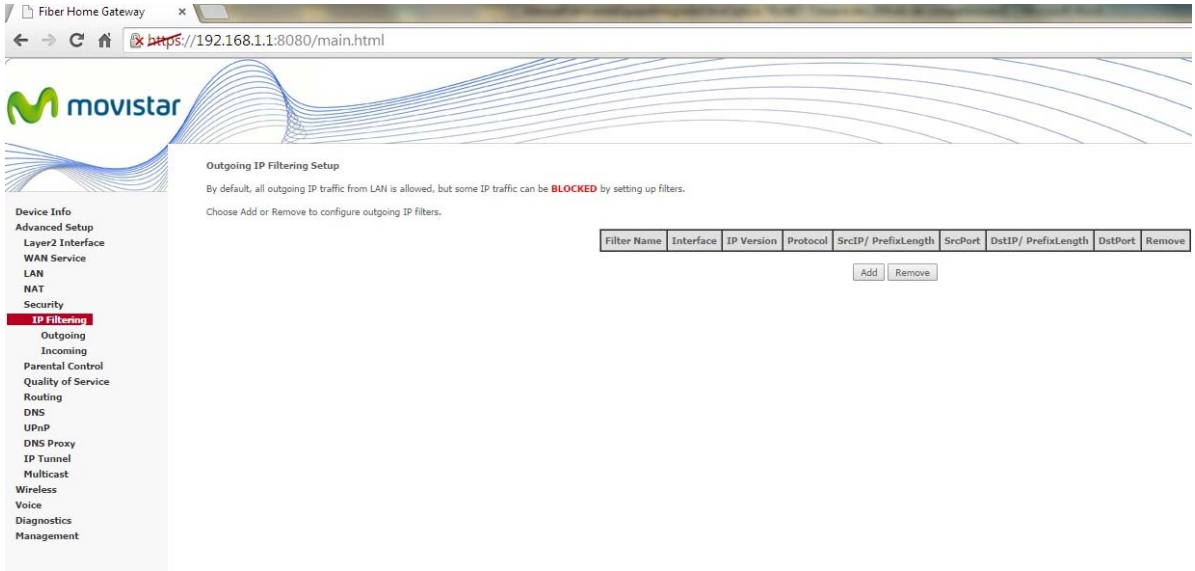
Security

Para que esta opción esté disponible, debe estar habilitado el firewall en la configuración WAN.

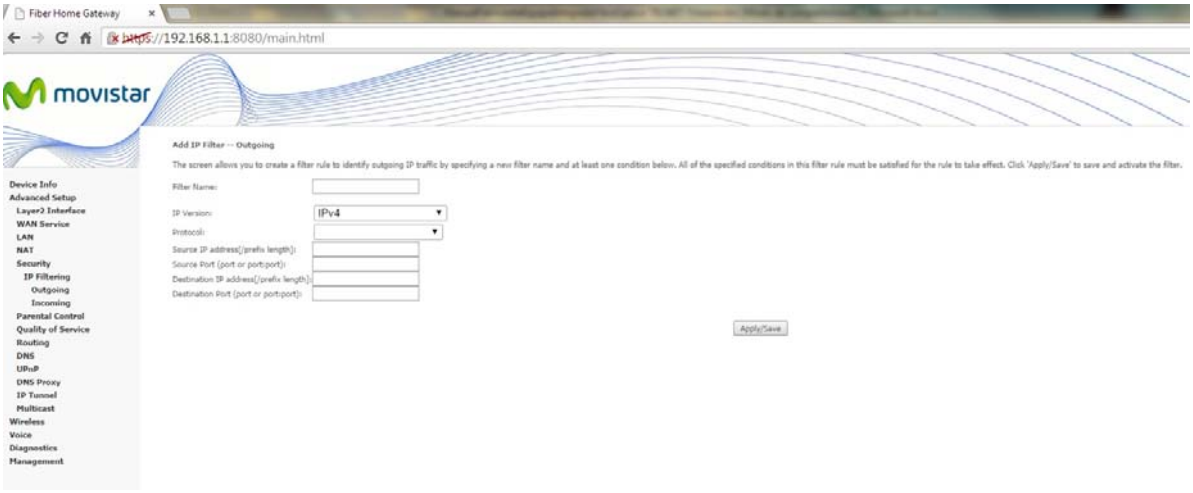
IP Filtering Outgoing

Esta opción permite configurar filtros o reglas que limitan el tráfico IP de salida. 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.

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



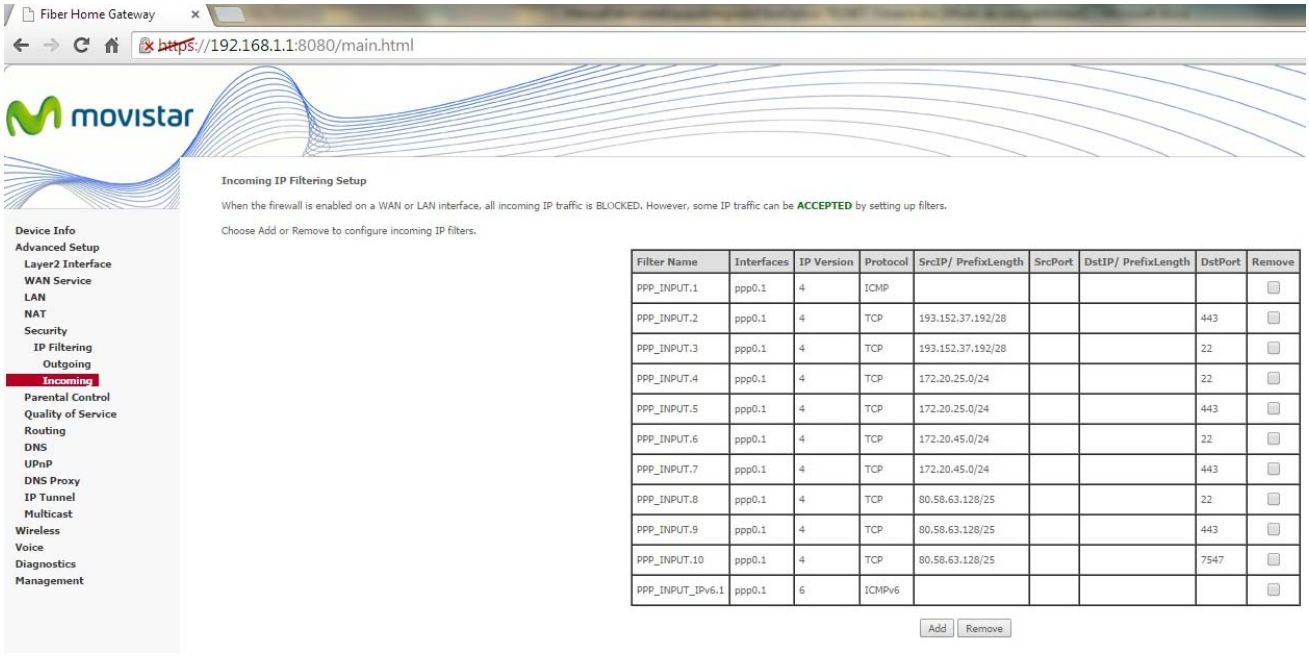
Para añadir un filtro (para bloquear tráfico IP saliente), haga clic en el botón "*Add*". En la siguiente pantalla, introduzca los criterios de filtrado y haga clic en el botón "*Apply/Save*".



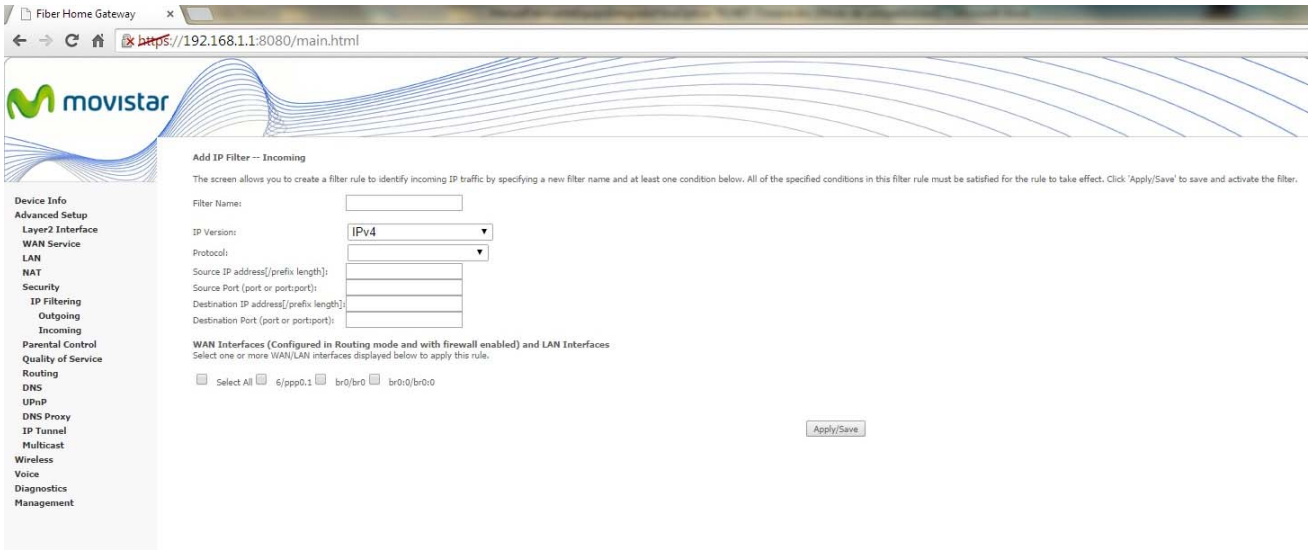
Campo	Descripción
Filter Name	Introduzca el nombre del filtro
IP Version	IPv4, IPv6
Protocol	TCP, UDP, TCP/UDP, ICMP
Source IP Address[/prefix length]	Introduzca la dirección IP origen. Si se trata de una red se puede añadir la máscara.
Source Port (port or port:port)	Introduzca el número de puerto origen o el rango de puertos origen.
Destination IP Address[/prefix length]	Introduzca la dirección IP destino. Si se trata de una red se puede añadir la máscara.
Destination Port (port or port:port)	Introduzca el número de puerto destino o el rango de puertos destino.

IP Filtering Incoming

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



Para añadir 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*".



Campo	Descripción
Filter Name	Introduzca el nombre del filtro
IP Version	IPv4, IPv6
Protocol	TCP, UDP, TCP/UDP, ICMP
Source IP Address[/prefix length]	Introduzca la dirección IP origen. Si se trata de una red se puede añadir la máscara.
Source Port (port or port:port)	Introduzca el número de puerto origen o el rango de puertos origen.
Destination IP Address[/prefix length]	Introduzca la dirección IP destino. Si se trata de una red se puede añadir la máscara.
Destination Port (port or port:port)	Introduzca el número de puerto destino o el rango de puertos destino.

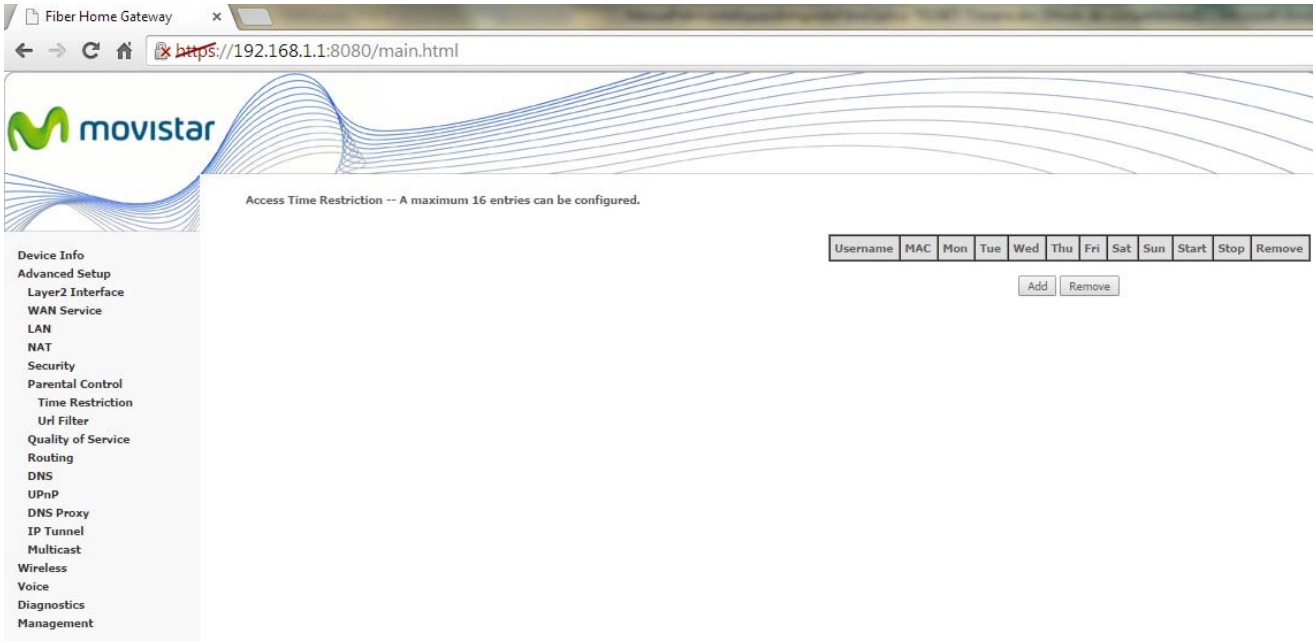
En la imagen superior, seleccione el interfaz WAN y LAN en los que serán aplicados las reglas de filtrado. Debe seleccionar todos o solo un subconjunto. Con interfaces WAN en modo bridge o sin firewall activado no estará disponible.

Parental Control

Esta sección permite establecer determinadas restricciones a determinados horarios y determinadas webs. A continuación detallamos estas funcionalidades.

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 se indica en el apartado correspondiente, 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.

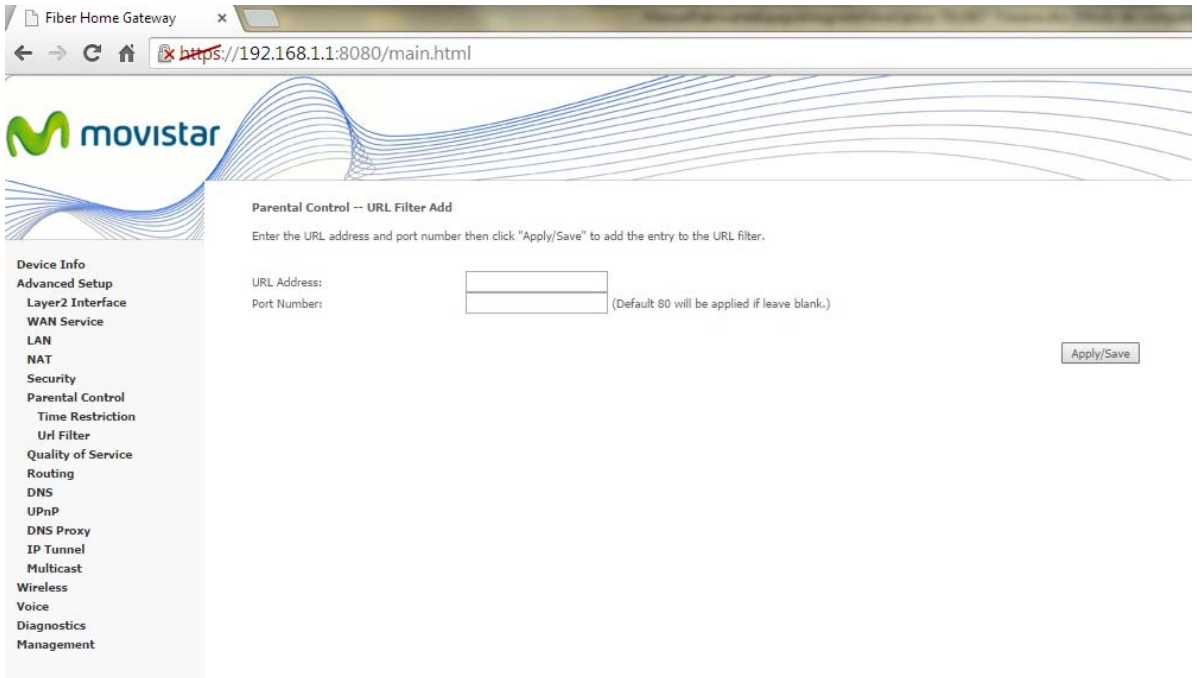
Ver la descripción de campos a continuación.

Campo	Descripción
User Name	Nombre definido por el 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 de inicio la restricción
End Blocking Time	El tiempo de finalización de la restricción

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.



Para la creación de un filtro a una URL, seguir los siguientes pasos:

Paso 1: 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.

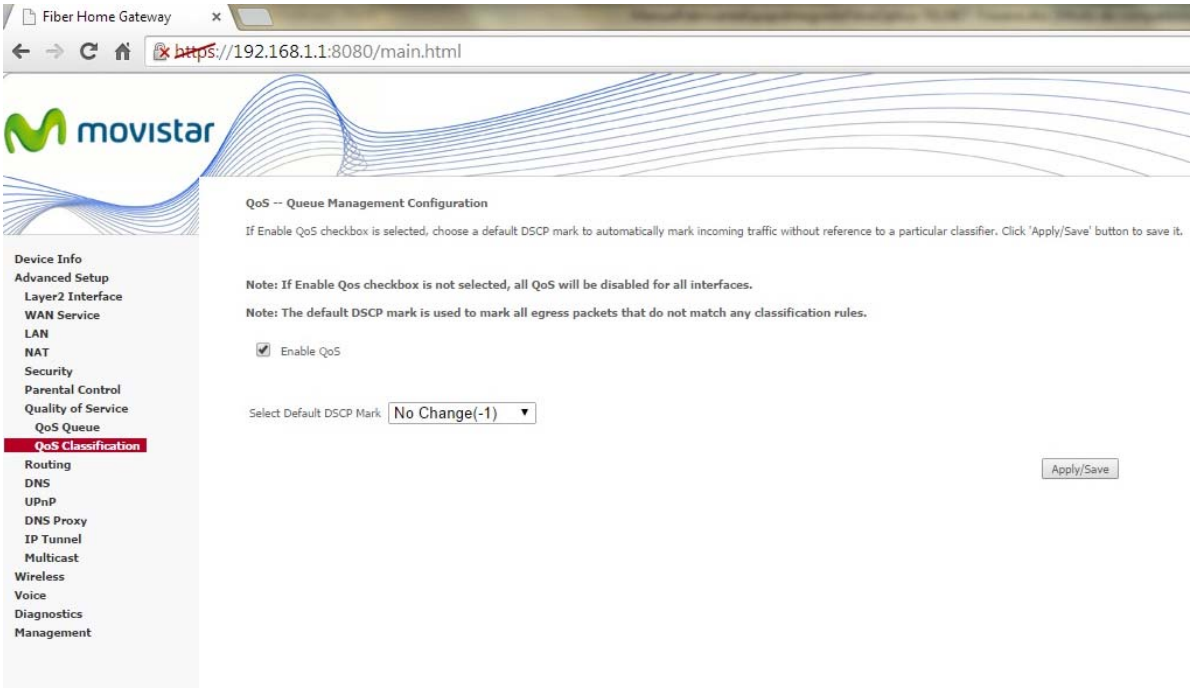
Paso 2: Especificar tipo de filtro. Marque "*Exclude*" para sólo permitir el acceso a los sitios de internet enumerados. Marque "*Include*" para restringir el acceso únicamente a los sitios de internet enumerados.

Quality of Service

Si el check “Enable QoS” está seleccionado, elige una etiqueta DSCP por defecto para marcar el tráfico entrante sin referencia a una clasificación particular. Haz clic sobre el botón “Apply/Save” para guardar los cambios.

> **Nota:** Si el *check* “Enable QoS” no está seleccionado, QoS será deshabilitado en todos los interfaces.

> **Nota:** La etiqueta DSCP por defecto se utiliza para marcar todo el tráfico saliente que no ha pasado por ninguna regla de clasificación.

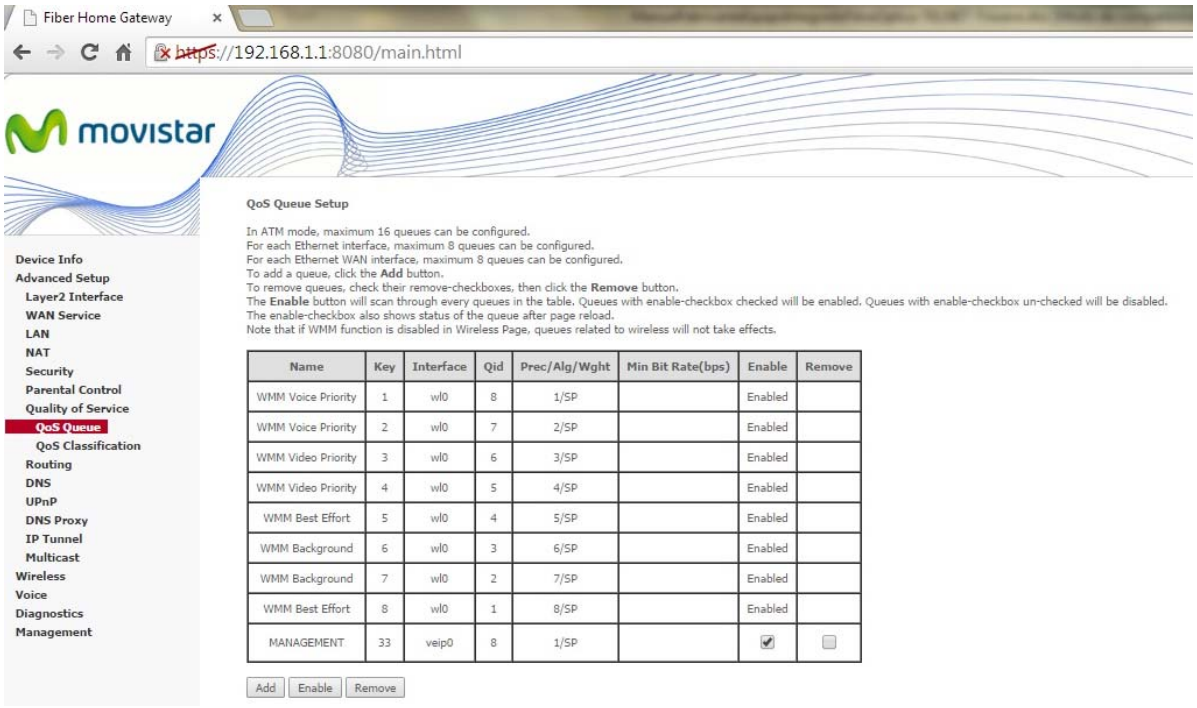


QoS Queue

En modo ATM, un máximo de 16 colas de prioridad se pueden configurar.

En cada interfaz Ethernet, hasta un máximo de 8 colas pueden configurarse, igual que en los interfaces WAN Ethernet.

En la imagen mostrada a continuación están las colas de prioridad que están generadas en el equipo por defecto. Estas colas no pueden ser eliminadas (no tiene habilitada la opción “*Remove*”) y siempre están habilitadas, salvo que la función WMM está deshabilitada en la página “Wireless”, entonces las colas relativas al interfaz *wireless* no tomarán efecto.

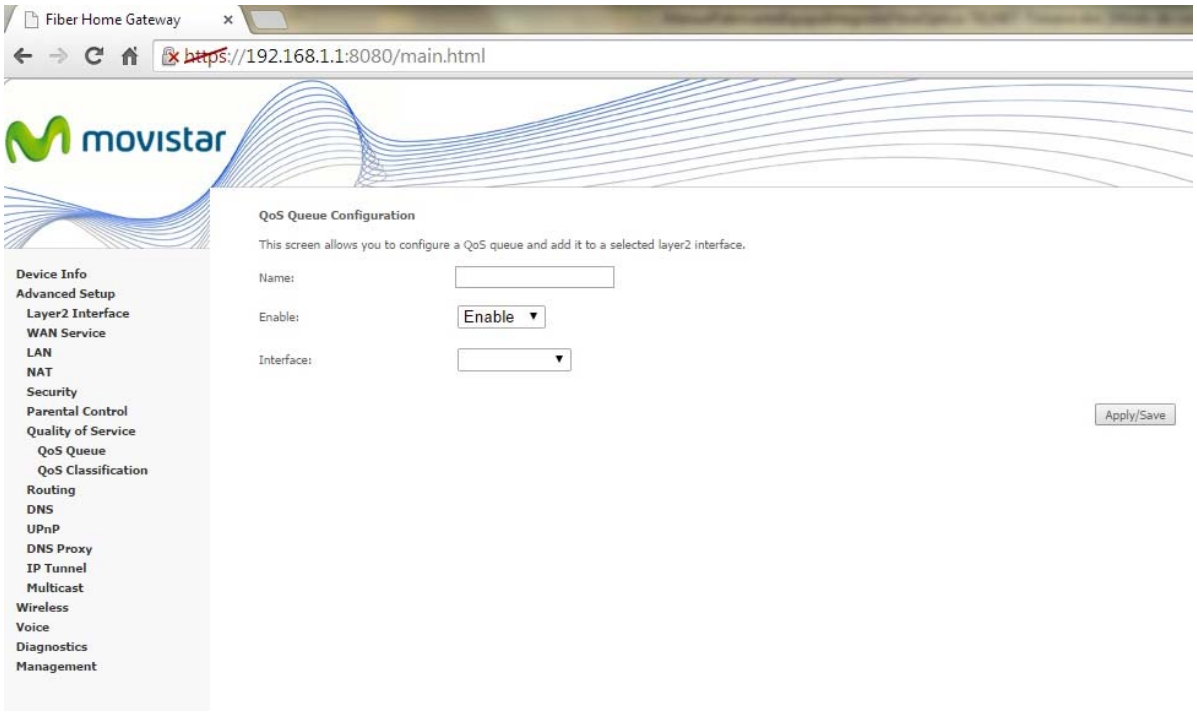


Para añadir una cola, clic en botón "*Add*".

Para eliminar colas, selecciona los *checks* "*Remove*" correspondientes y haz clic sobre el botón "*Remove*" de la parte inferior.

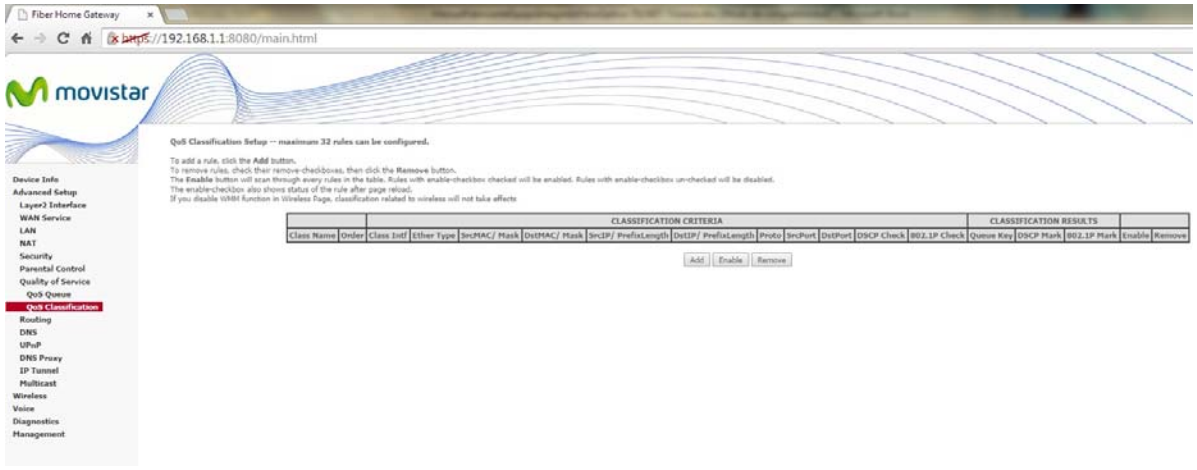
El botón "*Enable*" actualiza las colas. Habilita las colas que tienen el *check* "*Enable*" habilitado y deshabilita las colas con este *check* deshabilitado. Por tanto, para que los cambios en los *checks* "*Enable*" tengan efecto es necesario pulsar el botón "*Enable*" de la parte inferior.

Campo	Descripción
Name	Nombre identificativo de la cola
Key	Número identificativo de la cola
Interface	Interfaz de la cola
Qid	Número de cola del interfaz
Prec/Alg/Wght	Valores para la priorización de las colas.
Min Bit Rate (bps)	Bps garantizado en los casos que sea necesario.
Enable	Habilitación/deshabilitación de la cola
Remove	Eliminación de la cola



QoS Classification

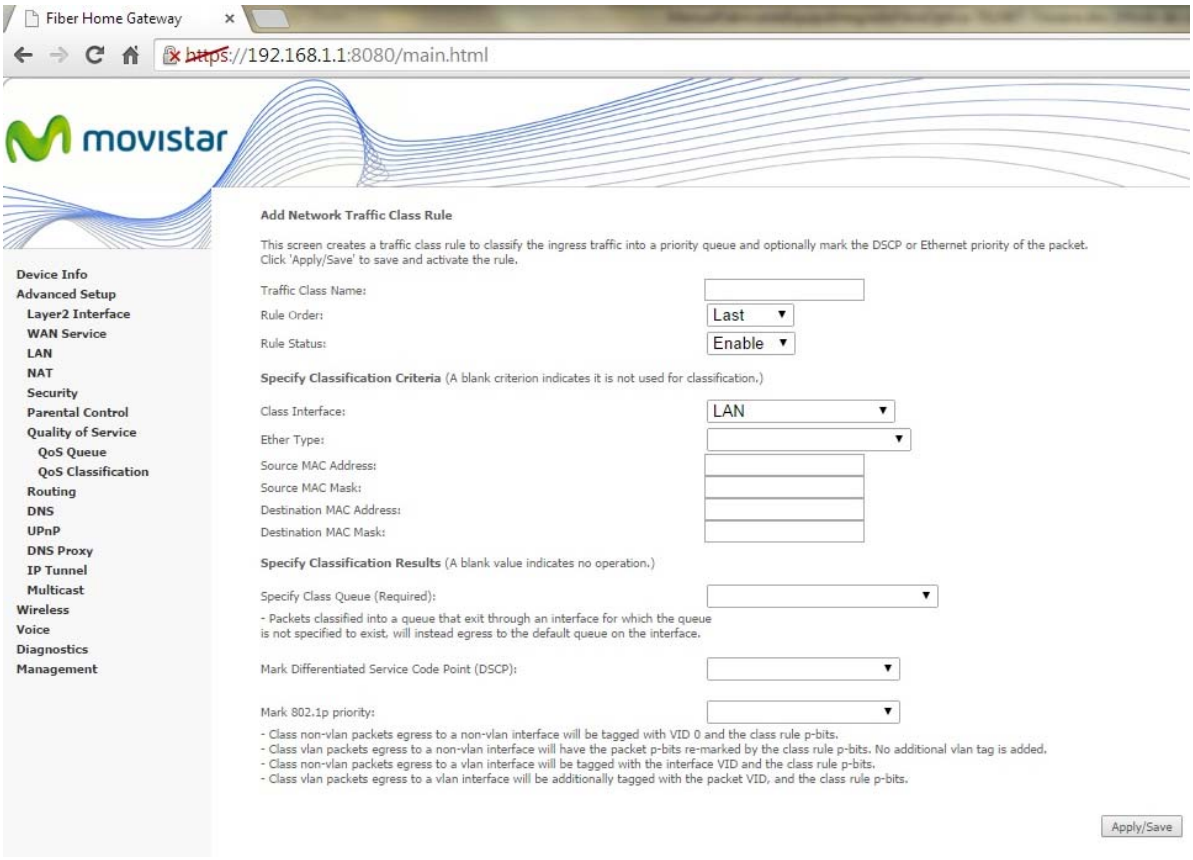
Para clasificar el tráfico entrante se pueden configurar hasta un total de 32 reglas.



Para añadir una regla, se debe hacer clic sobre el botón "*Add*". Más adelante se detalla los campos a configurar en las reglas de clasificación.

Para eliminar reglas, selecciona los *checks* "*Remove*" correspondientes y haz *click* sobre el botón "*Remove*" de la parte inferior.

El botón "*Enable*" actualiza las colas. Habilita las reglas que tienen el *check* "*Enable*" habilitado y deshabilita las reglas con este *check* deshabilitado. Por tanto, para que los cambios en los *checks* "*Enable*" tengan efecto es necesario pulsar el botón "*Enable*" de la parte inferior.



Para la generación de una nueva regla de clasificación de tráfico, se deben especificar los siguientes campos:

Campo	Descripción
Traffic Class Name	Nombre definido por el usuario para la regla de clasificación.
Rule Order	Establecer el número de orden de la regla.
Rule Status	Para crear la regla habilitada o deshabilitada
Class Interface	Interfaz seleccionado
Criterio de la regla de clasificación (En blanco indica que ese filtro no se utiliza para la clasificación)	
Ethertype	IP (0x0800) ARP (0x0806) IPv6 (0x86DD) PPPoE_DISC (0x8863) PPPoE_SES (0x8864) 8865 (0x8865) 8866 (0x8866) 8021Q (0x8100)
Source MAC Address	Dirección de host/red origen

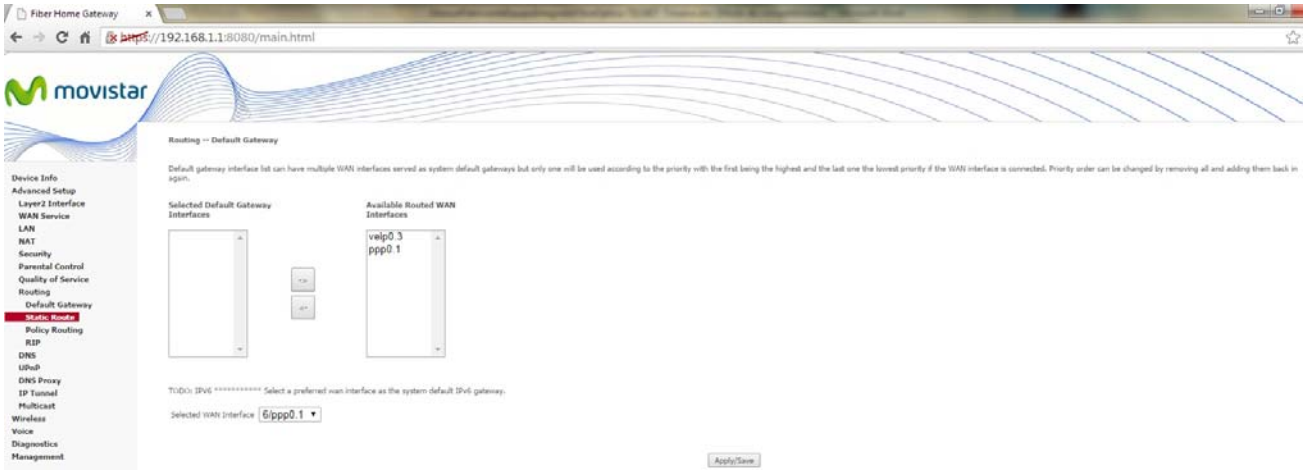
Source MAC Mask	Máscara de red origen
Destination MAC Address	Dirección de host/red destino
Destination MAC Mask	Máscara de red destino
Resultados de la regla de clasificación (Campo en blanco indica que no se realiza ningún cambio)	
Specify Class Queue	Cola de salida especificada - Paquetes que se clasifican en una cola de salida no especificada en el interfaz de salida de la trama, se reasigna a la cola por defecto de dicho interfaz
Mark Differentiated Service Code Point (DSCP)	Valor DSCP establecido en las tramas IP
Mark 802.1p priority	Prioridad establecida en la tramas con etiqueta VLAN - Paquetes salientes sin VLAN por un interfaz sin VLAN serán etiquetados con VLAN 0 y la prioridad correspondiente. - Paquetes salientes con VLAN por un interfaz sin VLAN tendrán la prioridad reestablecida por la regla de clasificación, no se añade ninguna etiqueta adicional. - Paquetes salientes sin VLAN hacia un interfaz con VLAN será etiquetados con la VLAN del interfaz y con la prioridad de la regla de clasificación correspondiente. - Paquetes salientes con VLAN hacia un interfaz con VLAN, se añadirá al paquete la VLAN del interfaz y la prioridad de la regla de clasificación

Routing

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

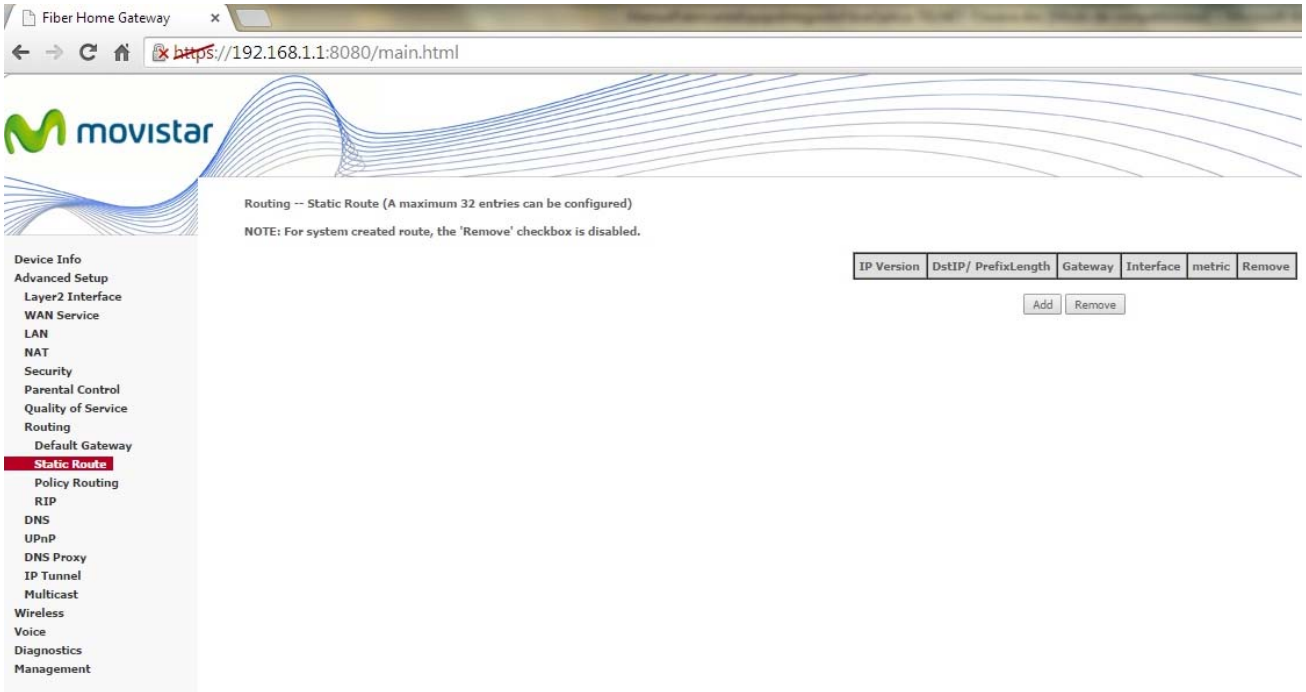
Default Gateway

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

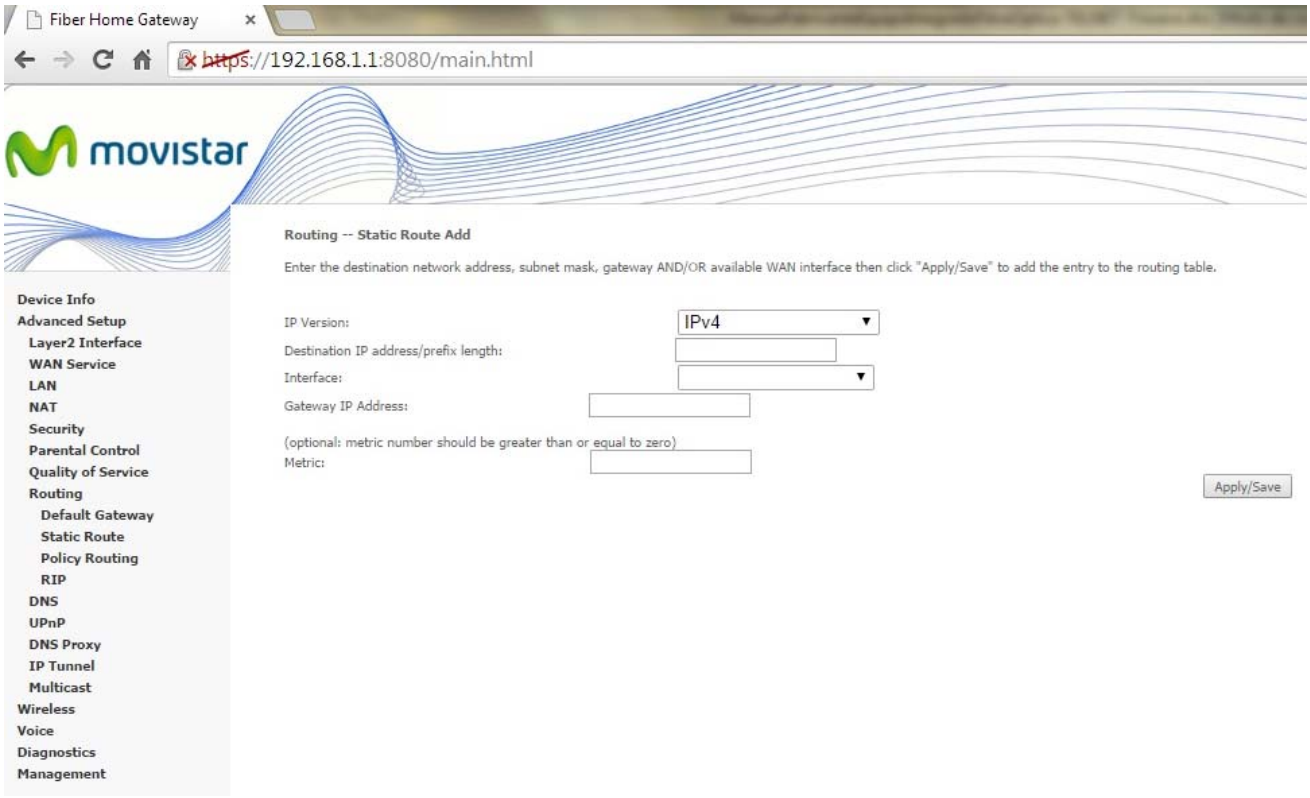


Static Route

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.



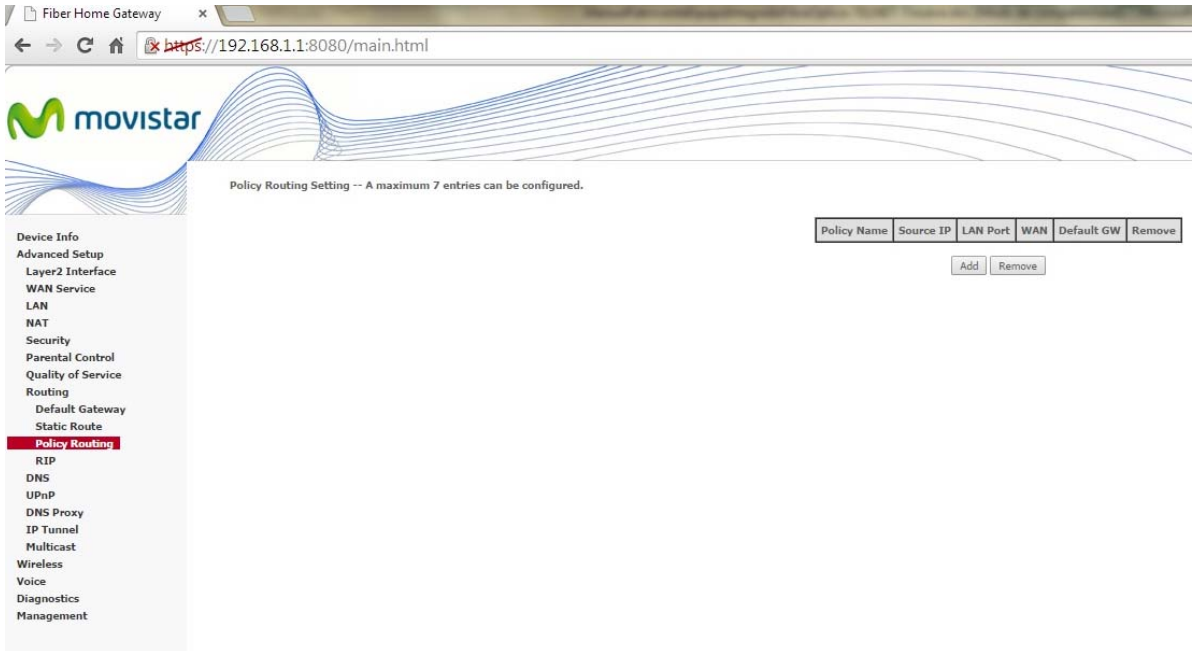
Al pulsar el botón "*Add*" aparece la siguiente imagen:



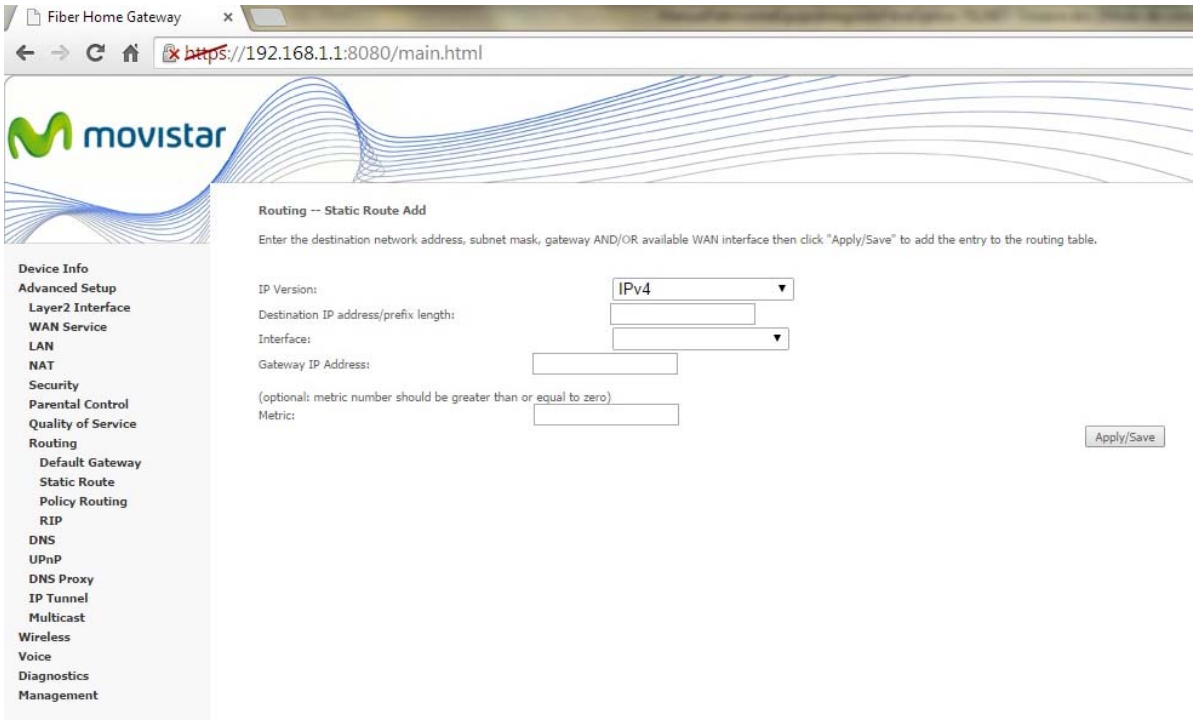
Introduzca la dirección de red de destino, máscara, dirección IP del Gateway, interfaz destino y métrica de la ruta creada. Haga clic en el botón "*Save/Apply*" para salvar la ruta introducida en la tabla de enrutamiento.

Policy Routing

En este apartado se pueden generar políticas de enrutamiento.



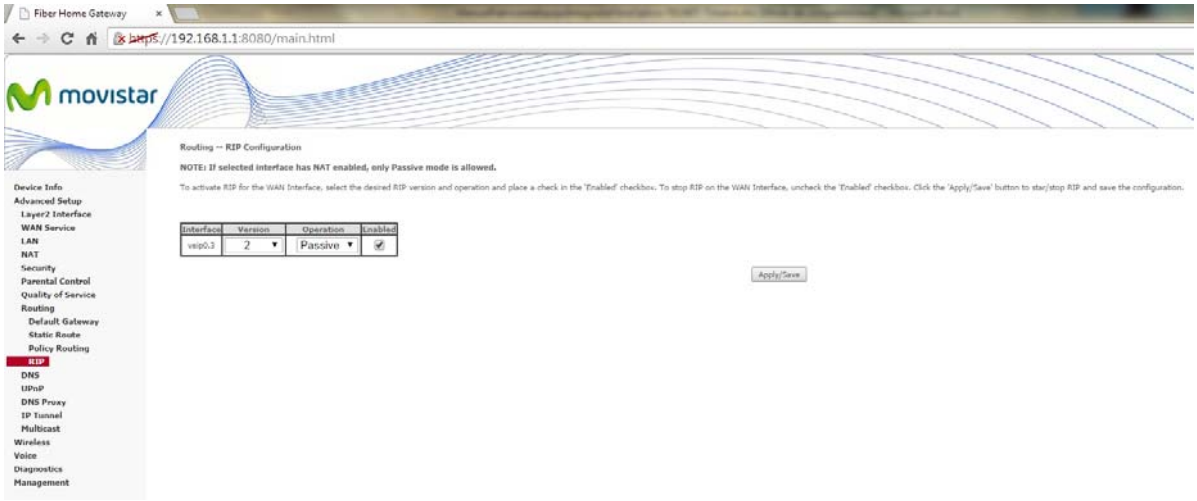
Al pulsar el botón "*Add*" aparece la siguiente pantalla:



Para la creación de la política se debe establecer el nombre, puerto físico LAN, dirección IP, interfaz WAN y gateway.

RIP

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



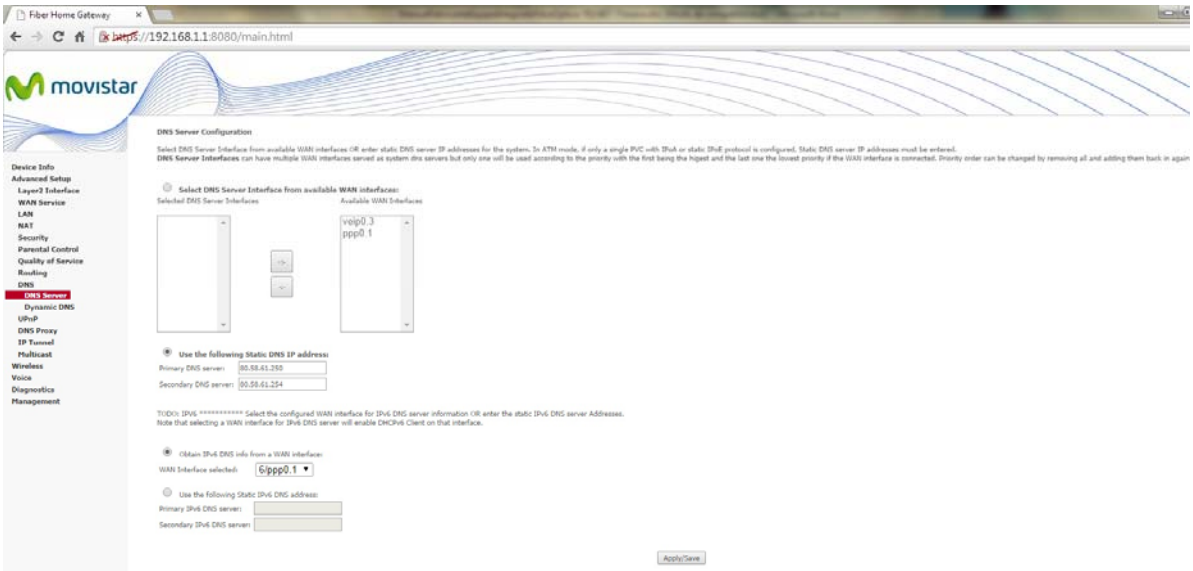
DNS

DNS Server

Selecciona el interfaz para acceder a los servidores DNS de los interfaces WAN disponibles o configura estáticamente las direcciones IP de los servidores DNS para el sistema. En modo ATM, si se configura un único PVC con IPoA o IPoE, se debe configurar direcciones IP estáticas.

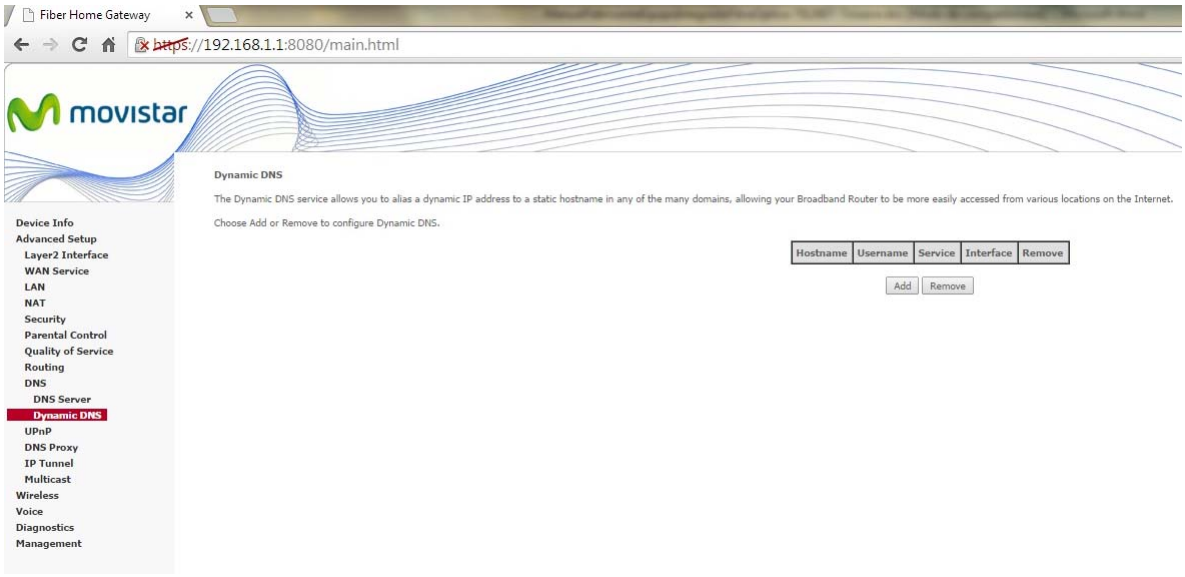
Los interfaces para acceder a los servidores DNS pueden ser múltiples pero sólo se accederá por el interfaz con mayor prioridad.

Para obtener información DNS de un interfaz WAN, marque *"Obtain 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.

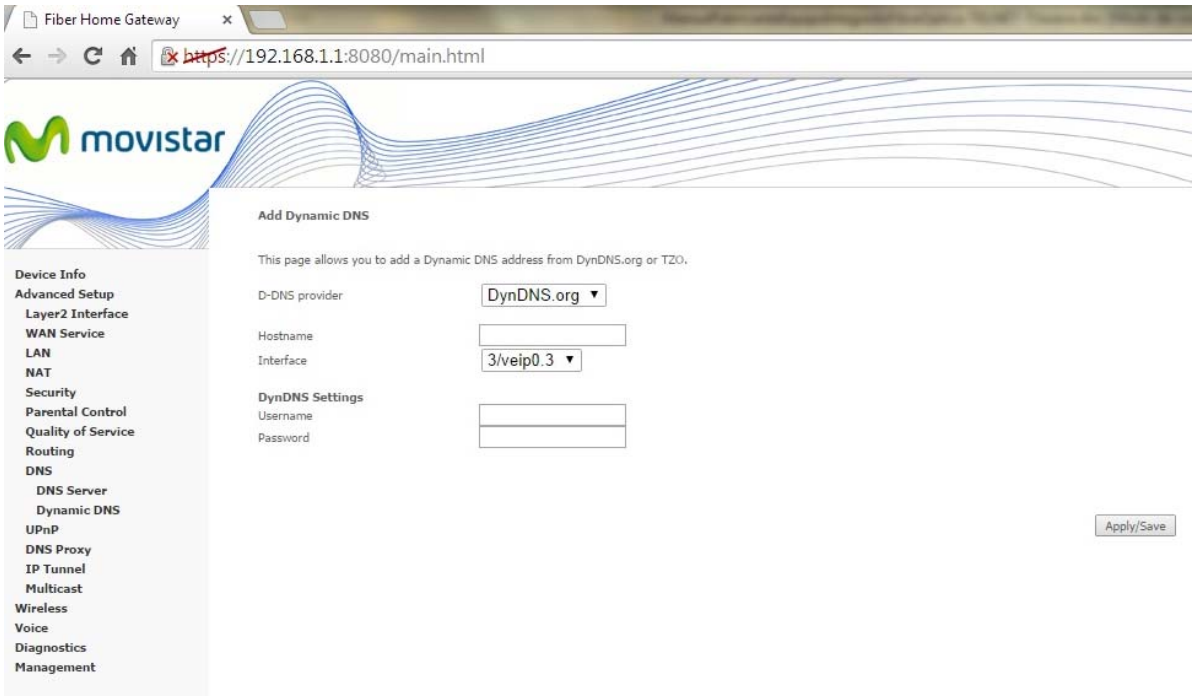


Dynamic DNS

El servicio *Dynamic DNS* (DNS dinámico) permite a la dirección IP de su router comportarse como un *hostname* o nombre de dominio, permitiendo al TriWave el acceso desde otros sitios de Internet más fácilmente.



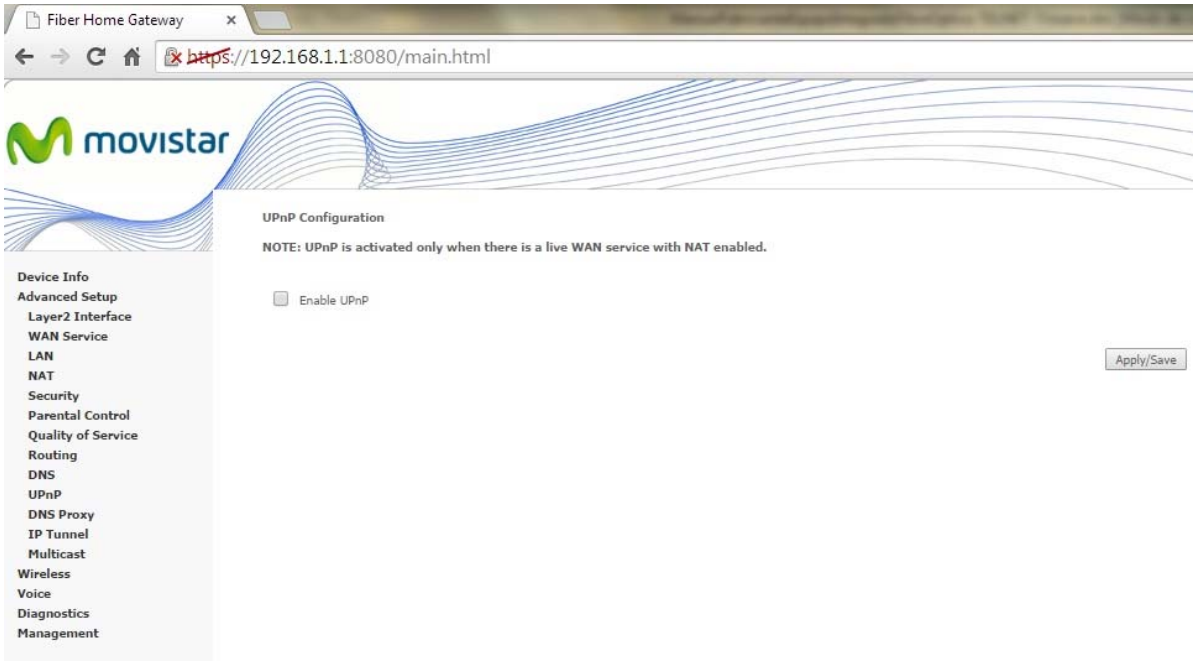
Para añadir un servicio *Dynamic DNS*, haga clic en el botón "*Add*"**.** La siguiente pantalla será mostrada:



Campo	Descripción
D-DNS Provider	Seleccione el proveedor Dynamic DNS de la lista desplegable
Hostname	Introduzca el nombre del servidor DNS dinámico
Interface	Seleccione el interface del desplegable
Username	Introduzca el usuario del servidor DNS dinámico
Password	Introduzca la contraseña del servidor DNS dinámico

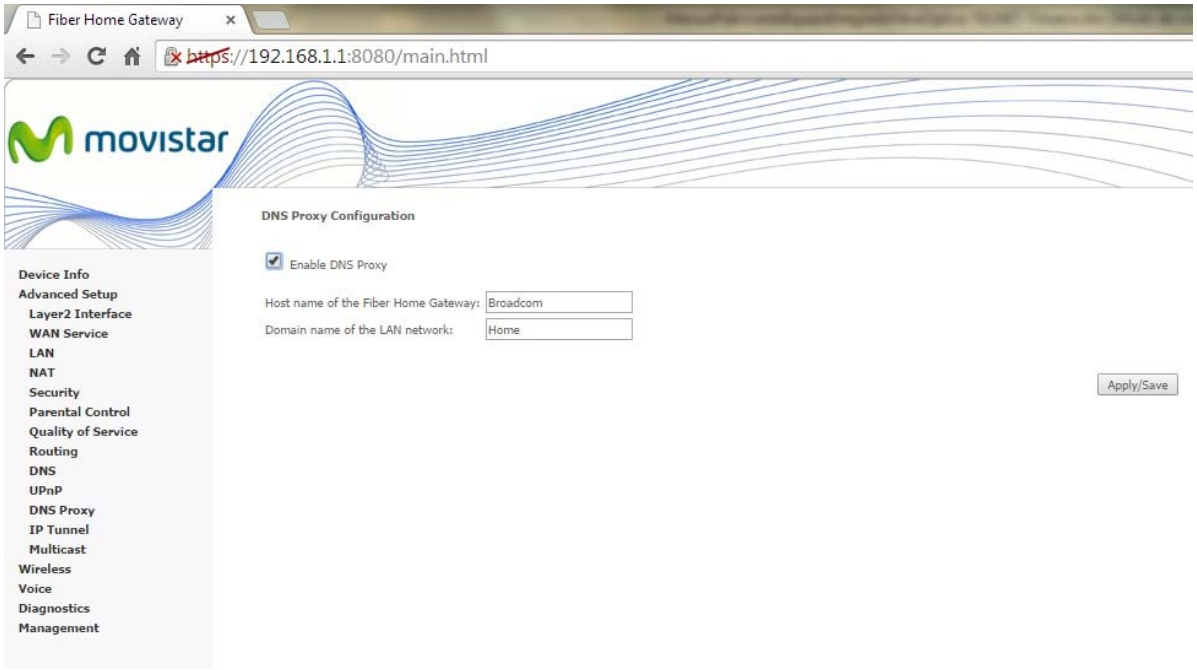
UPnP

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



DNS Proxy

Marque la casilla de verificación "*Enable DNS Proxy*" y haga clic en el botón "*Apply/Save*" para activar el protocolo *DNS Proxy*. Después hay que establecer el nombre del equipo TriWave y nombre del dominio de la red LAN.



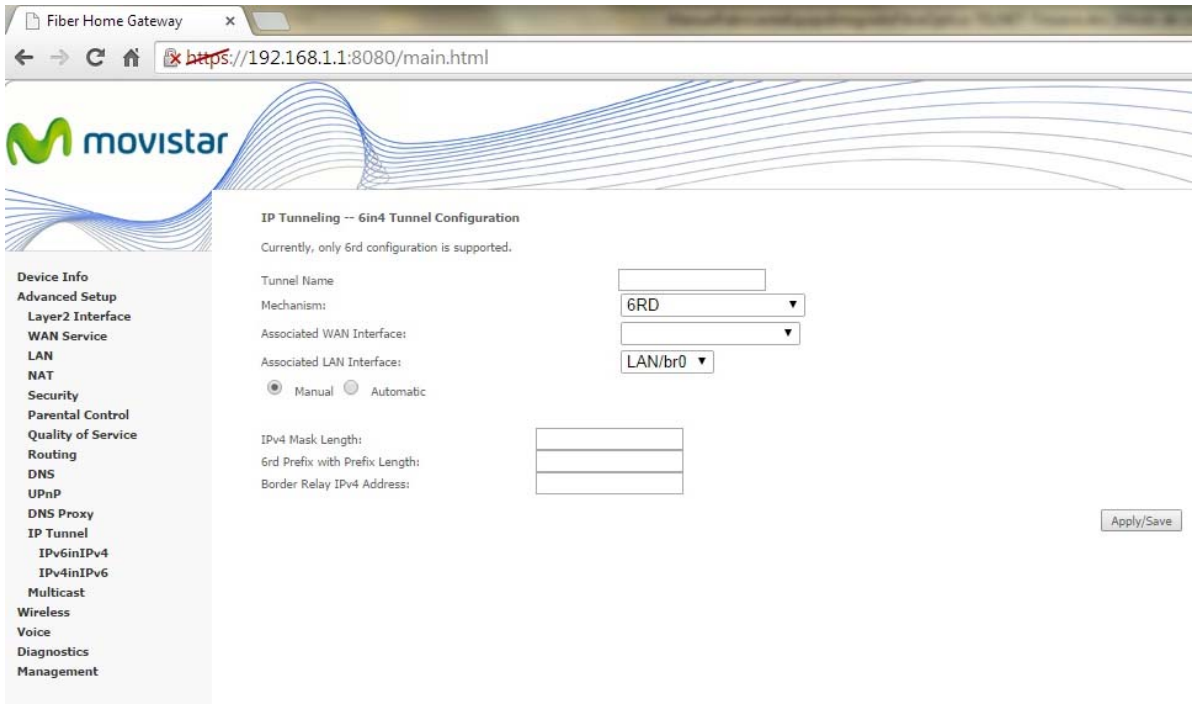
IP Tunnel

En este apartado podremos configurar los parámetros para permitir a hosts conectados únicamente a IPv4 ó IPv6 acceder a recursos sólo disponibles utilizando el otro protocolo.

IPv6inIPv4

Aquí podemos configurar un túnel IPv4 para dispositivos IPv6.

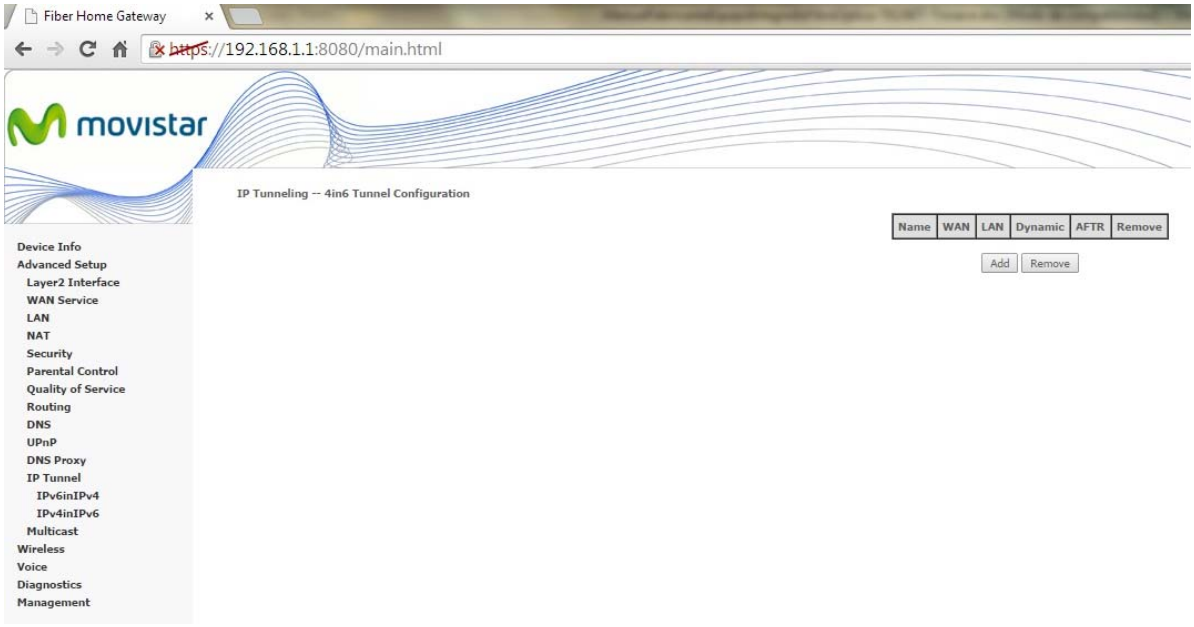
Actualmente, TriWave sólo soporta la configuración 6rd:



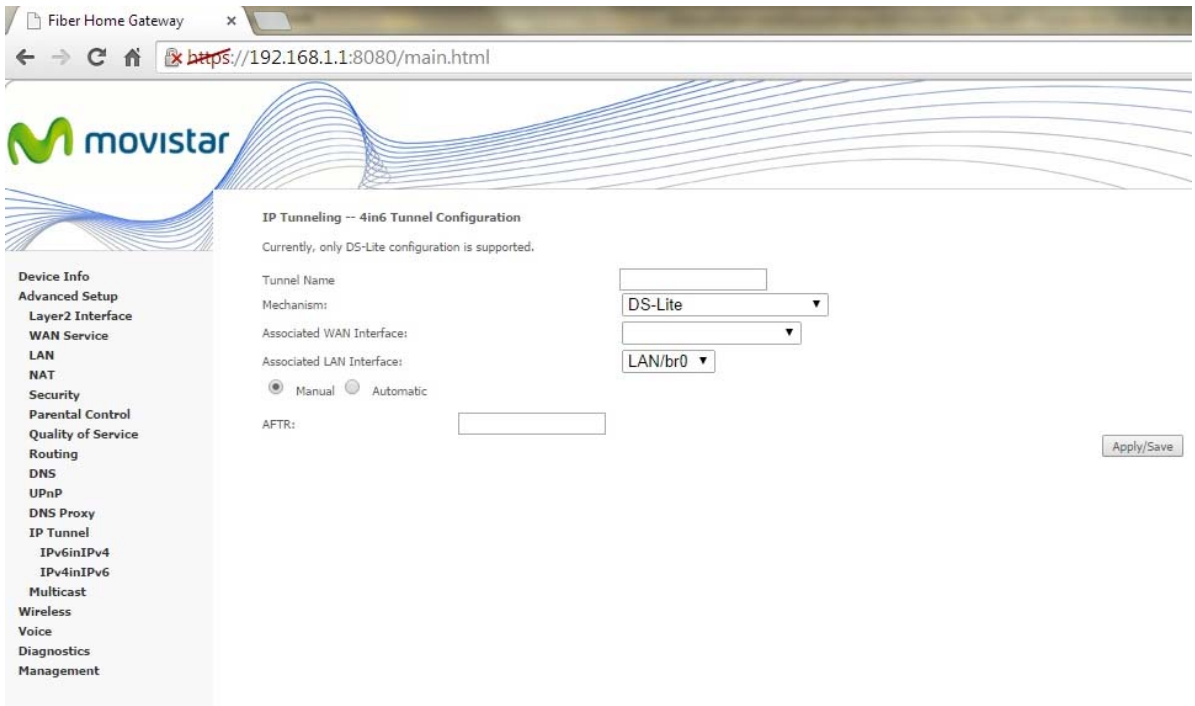
Para la configuración hay que establecer el nombre de tunel, y los interfaces WAN y LAN que se van a asociar. Si se opta por configuración manual hay que establcer adicionalmente la longitud de la máscara IPv4, longitud del prefijo 6rd y la dirección IPv4 Relay a la que hay que conectarse.

IPv4inIPv6

Aquí podemos configurar un túnel IPv6 para dispositivos IPv4.



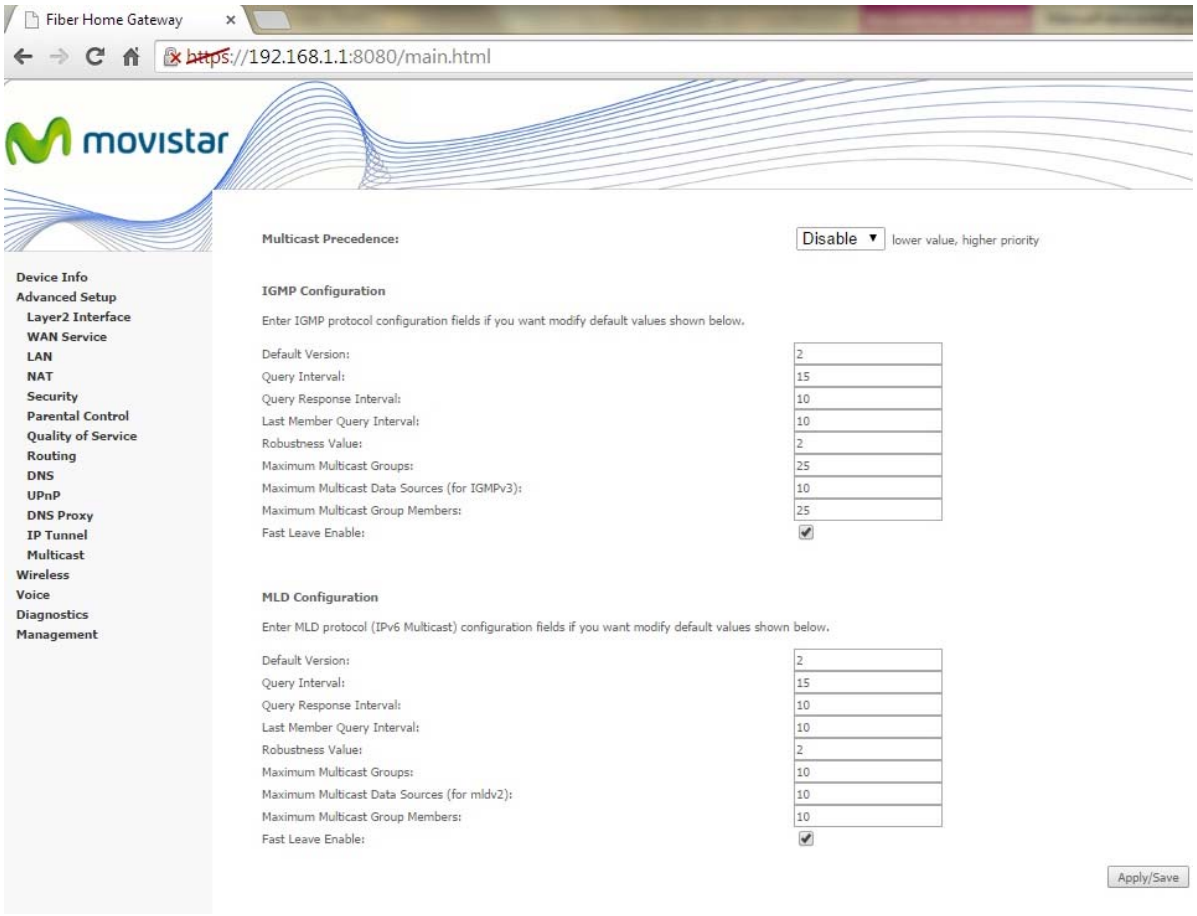
Actualmente, TriWave sólo soporta la configuración DS-Lite:



Para la configuración hay que establecer el nombre de tunel, y los interfaces WAN y LAN que se van a asociar. Si se opta por configuración manual hay que establecer adicionalmente el AFTR (*Address Family Translation Router*).

Multicast

En este apartado se configura los parámetros del protocolo IGMP:



Campo	Descripción
Multicast Precedence	Valor del campo "*Precedence*" que se establecerá en las tramas Multicast
IGMP Configuration	
Default Version	Versión por defecto del protocolo IGMP
Query Interval	Tiempo que ha de transcurrir entre cada *Query* del equipo. Por defecto, 125 segundos.

Query Response Interval	Tiempo que se inserta en el campo de Tiempo de Respuesta Máximo de los mensajes de tipo *General Query*. Por defecto, 10 segundos.
Last Member Query Interval	Tiempo que se inserta en el campo de Tiempo de Respuesta Máximo de los mensajes de tipo *Group-Specific Query*. Por defecto, 1 segundo, e indica además el intervalo entre cada una de las *Group-Specific Queries*.
Robustness Value	Número de veces que un paquete es reenviado. Es útil en redes congestionadas. De 1 a 7. Por defecto, 2.
Maximum Multicast Groups	Número máximo de grupos multicast que se pueden establecer (Por defecto = 25).
Maximum Multicast Data Sources (for IGMPv3)	Número máximo de fuente de datos. Por defecto, 10.
Maximum Multicast Group Members	Número Máximo de miembros en un grupo Multicast: Por defecto, 25.
Fast Leave Enable	Opción que minimiza el tiempo de finalización de un grupo multicast. Si está habilitada esta opción cuando llegue un "*Leave*" el equipo borra el grupo inmediatamente.
MLD Configuration (IPv6)	
Default Version	Versión por defecto del protocolo IGMP
Query Interval	Tiempo que ha de transcurrir entre cada "*Query*" del equipo. Por defecto 125 segundos.
Query Response Interval	Tiempo que se inserta en el campo de Tiempo de Respuesta Máximo de los mensajes de tipo General Query. Por defecto, 10 segundos.
Last Member Query Interval	Tiempo que se inserta en el campo de Tiempo de Respuesta Máximo de los mensajes de tipo Group-Specific Query. Por defecto, 1 segundo, e indica además el intervalo entre cada una de las Group-Specific Queries.
Robustness Value	Número de veces que un paquete es reenviado. Es útil en redes congestionadas. De 1 a 7. Por defecto, 2.
Maximum Multicast Groups	Número máximo de grupos multicast que se pueden establecer. Por defecto, 25.
Maximum Multicast Data Sources (for IGMPv3)	Número máximo de fuente de datos. Por defecto, 10.
Maximum Multicast Group	Número Máximo de miembros en un grupo Multicast. Por defecto, 25.

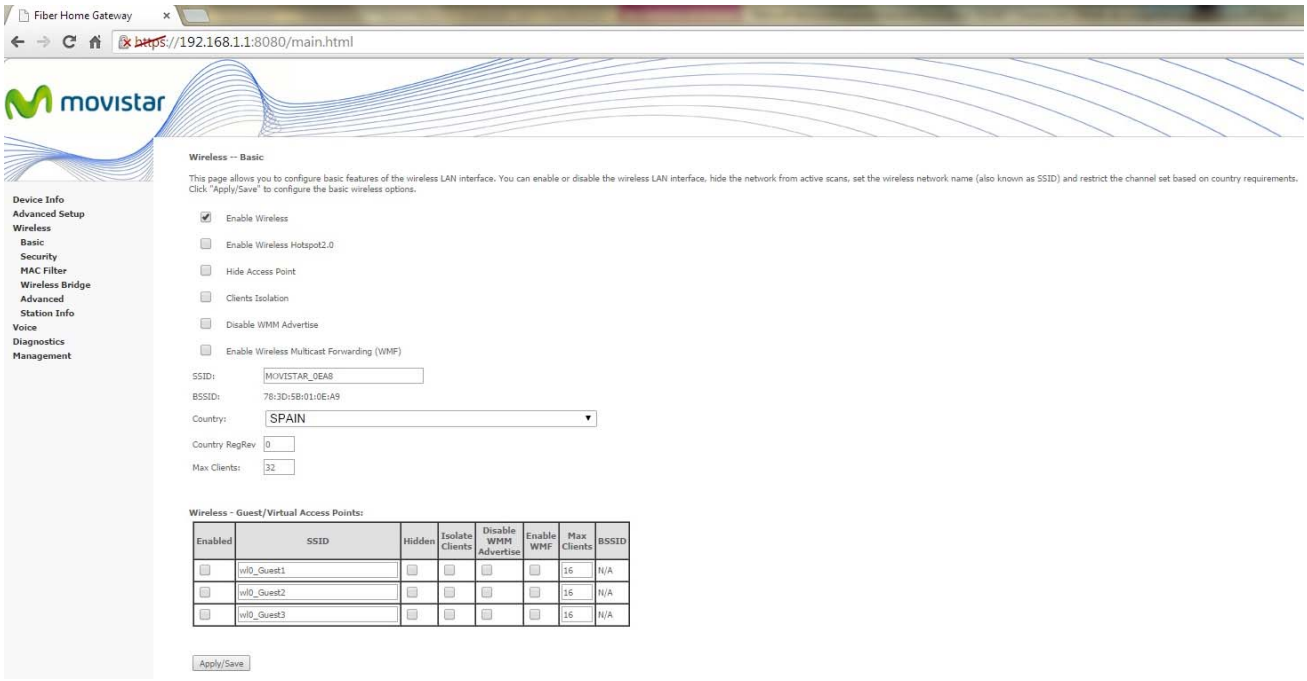
Members	
Fast Leave Enable	Opción que minimiza el tiempo de finalización de un grupo multicast. Si está habilitada esta opción cuando llegue un "*Leave*" el equipo borra el grupo inmediatamente.

Wireless

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

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.

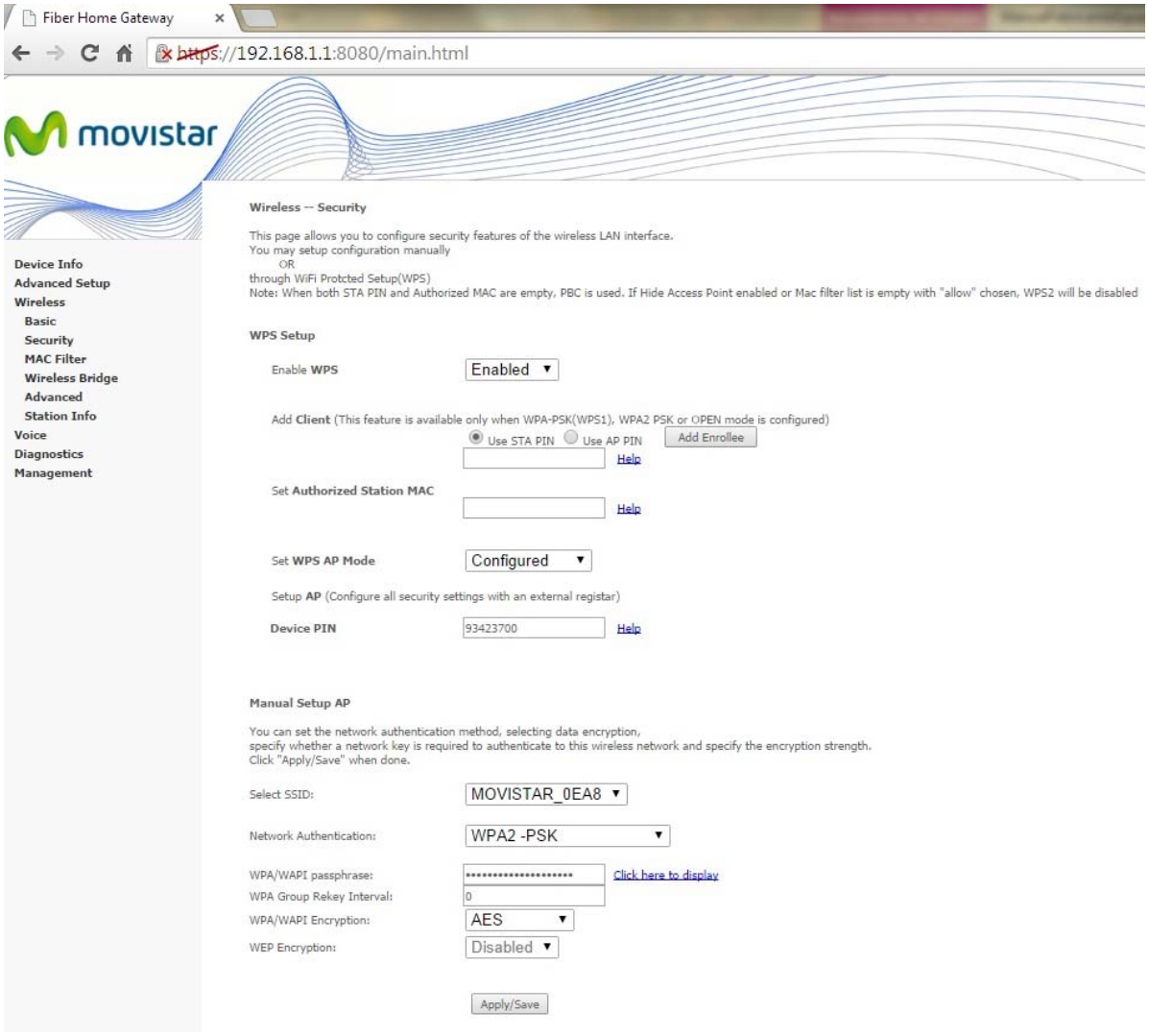
Campo	Descripción
Enable Wireless	Activa o desactiva el interfaz inalámbrico. Cuando está marcada, las opciones de configuración básicas serán mostradas.
Enable Wireless Hotspot2.0	Si está activo mejora las prestaciones de los dispositivos Wi-Fi para descubrir y conectarse a nuestro equipo.
Hide Access Point	Si está activo, protege el punto de acceso de la detección por escaneo inalámbrico. Por ejemplo: Para chequear el estado del punto de acceso en Windows XP, abra “Conexiones de Red” desde el menú Inicio y seleccione “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).
Enable Wireless Multicast Forwarding (WMF)	Si está activado permite al router reencaminar paquetes a otras redes dónde otros dispositivos multicast están activos y escuchando.
SSID (1-32 caracteres)	Configura el nombre de la red inalámbrica. El SSID significa *Service Set IDentifier*. Todas las estaciones deben configurado correctamente el SSID para acceder 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 acceder al equipo.

Wireless - Guest / Virtual Access Points	El TriWave 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 remoto no puede escanear *Guest SSIDs*.

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:

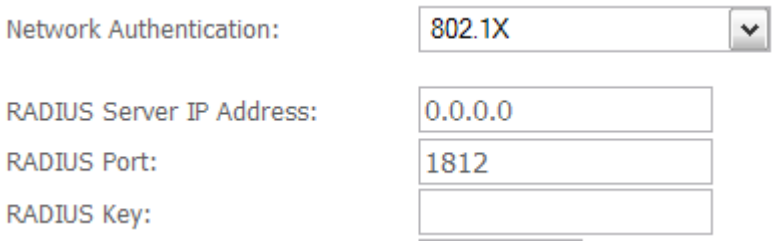
Seleccionar el nombre de red inalámbrica de la lista desplegable. Todas las estaciones deben tener configurado correctamente el SSID para acceder a la WLAN. Si el SSID no es correcto, el usuario no tiene garantizado el acceso.

Network Authentication:

Esta opción especifica si algún protocolo se utiliza para la 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.

Los posibles métodos de autenticación son: *Open* (sin autenticación), *Shared, 802.1x*, *WPA*, *WPA-PSK*, *WPA2*, *WPA2-PSK*, *Mixed WPA2/WPA*, *Mixed WPA2/WPA-PSK*.

Cada tipo de autenticación tiene sus propios parámetros. Por ejemplo, seleccionando autenticación 802.1X se deberá especificar la dirección IP del servidor Radius, puerto y campo clave.



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

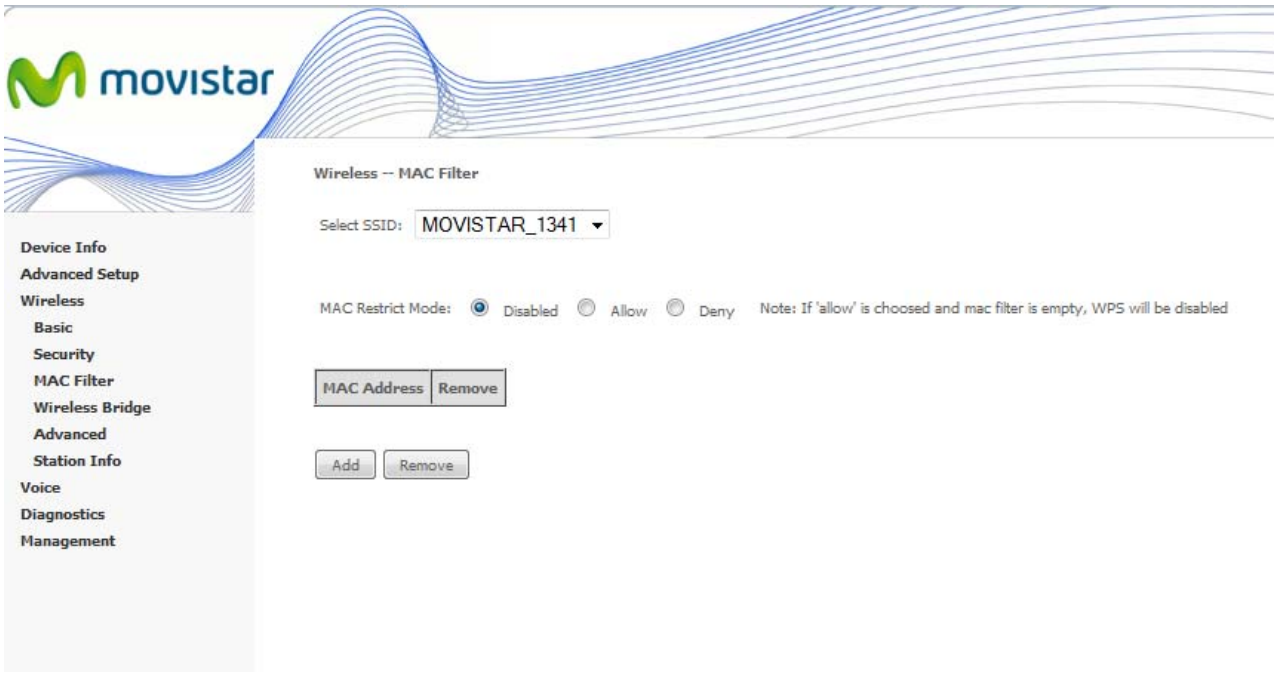
Esta lista desplegable se mostrará cuando la encriptación WEP este habilitada. La longitud de la clave es proporcional al número de bits binarios que componen la clave.

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.

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**".



Campo	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. 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*".

Wireless Bridge

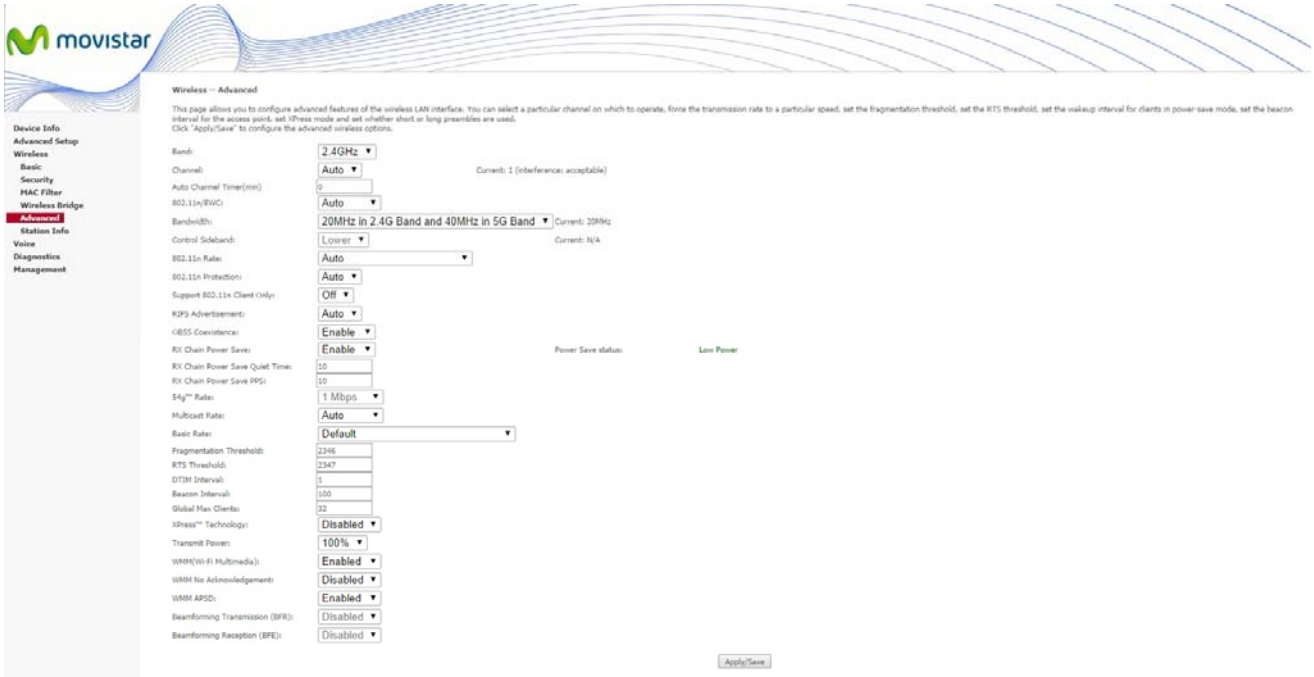
Esta opción permite la configuración de la funcionalidad Bridge inalámbrico del interfaz WLAN. Consulte la tabla inferior para conocer más detalles de las distintas opciones.

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

Campo	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.

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
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	Seleccione un canal de la lista
Auto Channel Timer (min)	La auto búsqueda de canales temporizado en minutes. (“0”, para deshabilitar)

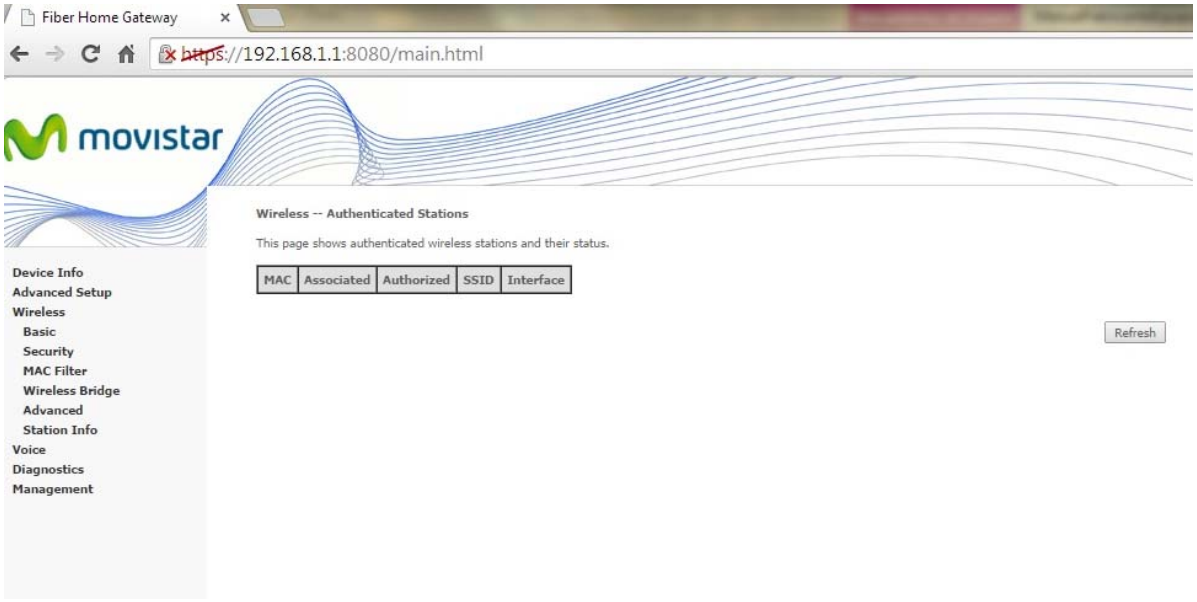
802.11n/EWC	Un equipo configurado con los parámetros de estándar de interoperabilidad en IEEE 802.11n Draft 2.0 y *Enhanced Wireless Consortium* (EWC)
Bandwidth	Seleccione la banda de frecuencia de 20GHz o 40GHz. La banda de frecuencia de 40GHz usa dos bandas adyacentes de 20 GHz para incrementar el 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	**Off** para *throughput* maximizado. **Auto** para mayor seguridad.
Support 802.11n Client Only	**Off** para permitir a clientes 802.11b/g acceder al router. **On** para prohibir a clientes 802.11b/g acceder al router.
RIFS Advertisement	Es una característica del 802.11n que mejora las prestaciones reduciendo los intervalos entre transmisiones OFDM. **Off** para deshabilitarlo. **Auto** para activarlo.
OBSS Coexistence	Activa o desactiva la coexistencia entre 20-40MHz en redes de área local inalámbricas.
Rx Chain Power Save	Si habilitas está característica, apagas una de las cadenas de recepción y de esta manera ahorrar potencia.
Rx Chain Power Save Quiet Time	Número de segundos que el tráfico debe estar por debajo del valor PPS antes de activar la característica "*Rx Chain Power Save*"
Rx Chain Power Save PPS	Número máximo de paquetes por segundo que puede procesar el interfaz WLAN durante el "*Quiet Time*" descrito en el campo previo, antes que el "*Rx Chain PowerSave*" se active.
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.
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 intervalo de *beacon* para conocer cuándo debe volver a escuchar para recibir el *beacon* (y aprender si existen tramas 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.

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.



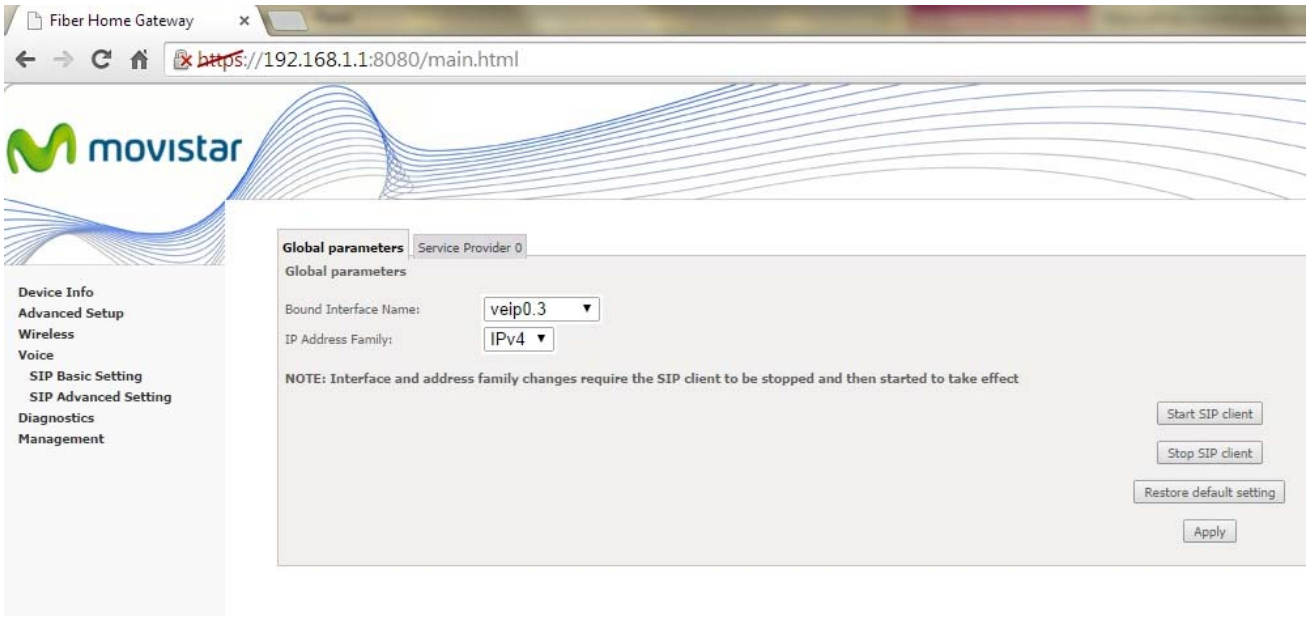
Campo	Descripción
MAC	Lista de direcciones MAC de todas las estaciones
Associated	Lista de todas las estaciones que están asociadas al punto de acceso, mostrando el tiempo de conexión y paquetes emitidos y recibidos por cada una de las estaciones. Si la estación es parada durante mucho tiempo, es eliminada 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.

Voice

En este apartado se podrá visualizar y configurar todos parámetros relativos a la voz del TriWave

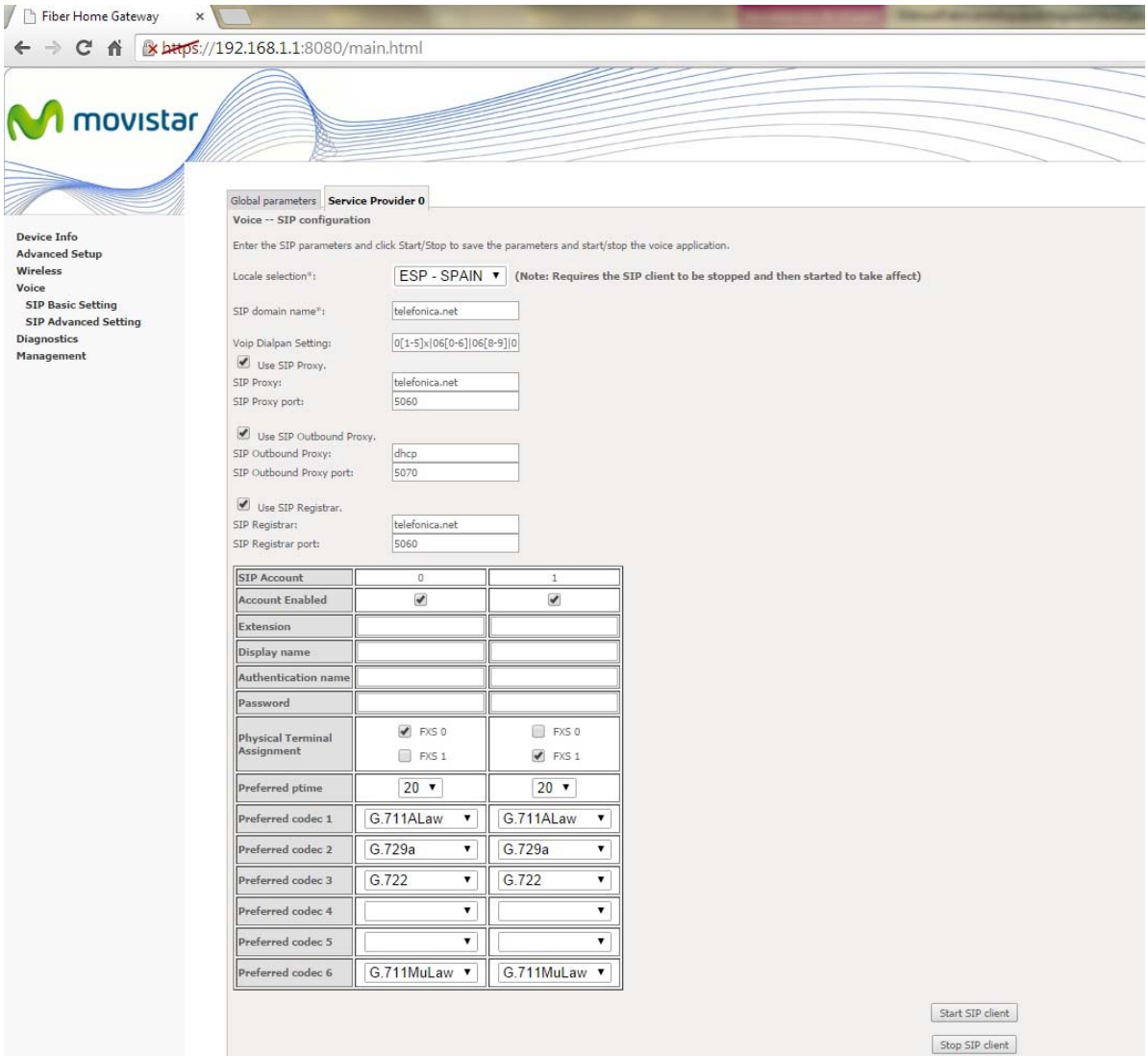
SIP Basic Setting

En la pestaña de parámetros globales aparece la siguiente figura dónde debemos elegir el interfaz, IPv4 o IPv6, iniciar o detener el cliente SIP y poder restaurar los valores por defecto.



Si seleccionamos la pestaña “Service Provider 0” aparace la siguiente pantalla:

SIP Basic Setting

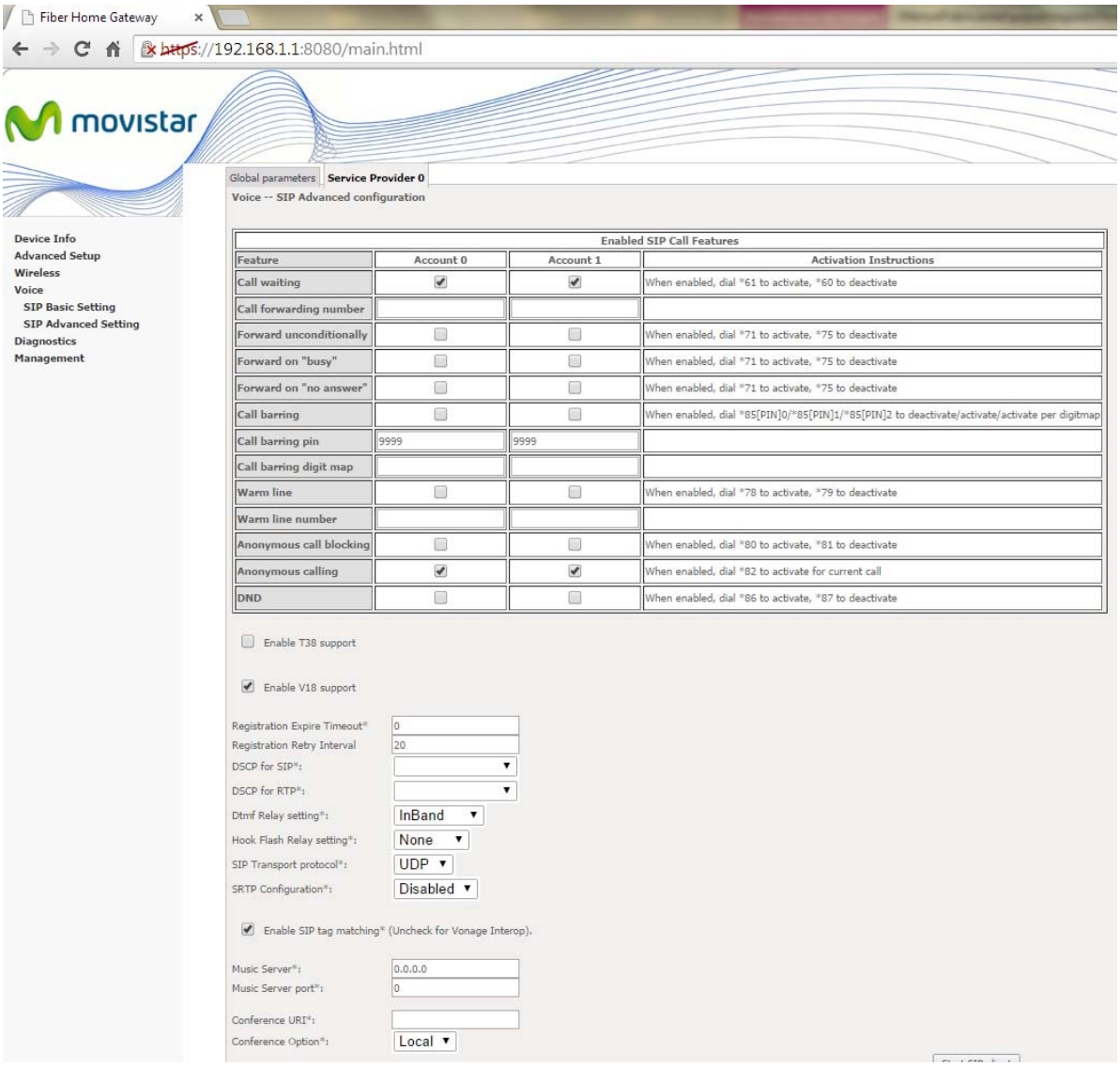


En esta pantalla tenemos los siguientes parámetros configurables:

Campo	Descripción
Locale selection	Especifica qué características locales se están usando. En esta versión del TriWave sólo está presente la opción ESP-SPAIN.
SIP domain name	Especifica el nombre de dominio utilizado para los mensajes SIP salientes.
Voip Dialplan Setting	Especifica el *DialPlan* que debe coincidir para todas las llamadas VoIP salientes.

SIP Proxy	
SIP Proxy	Nombre o dirección IP del SIP Proxy
SIP Proxy port	Puerto del servidor del SIP Proxy
SIP Outbound Proxy	
SIP Outbound Proxy	Nombre o dirección IP del SIP Outbound Proxy
SIP Outbound Proxy port	Puerto del servidor del SIP Outbound Proxy
SIP Registrar	
SIP Registrar	Nombre o dirección IP del SIP registrar
SIP Registrar port	Puerto del servidor del SIP registrar
SIP Account	
SIP Account	Número de cuenta SIP (0 y 1)
Account Enabled	Especifica si esta cuenta está habilitada o no.
Extension	Especifica la extensión o número de teléfono de esta cuenta. Este valor es el ID del usuario en un SIP URI. Por ejemplo, si la extensión es “123456”, entonces el SIP URI en la cabecera en todos los mensajes salientes será: From: “NOMBRE”<sip:123456@xxx>
Display name	Especifica el nombre para esta cuenta. Este valor es el nombre que aparecerá en el SIP URI. Por ejemplo, si el nombre es “ALICIA”, entonces la cabecera de todos los mensajes salientes será: From: “ALICIA”<sip:123456@xxx>
Authentication name	Especifica el nombre utilizado en todas las sesiones de autenticación SIP
Password	Especifica el password utilizado en todas las sesiones de autenticación SIP
Preferred ptime	Especifica el intervalo entre paquetes en ms para el códec utilizado. Valores válidos son 10, 20 y 30 ms.
Preferred codec N	Especifica el orden y tipo de códec que son anunciados en los campos SDP que son enviados en las negociaciones SIP. *Preferred codec* “1”, será el prioritario.

SIP Advanced Setting



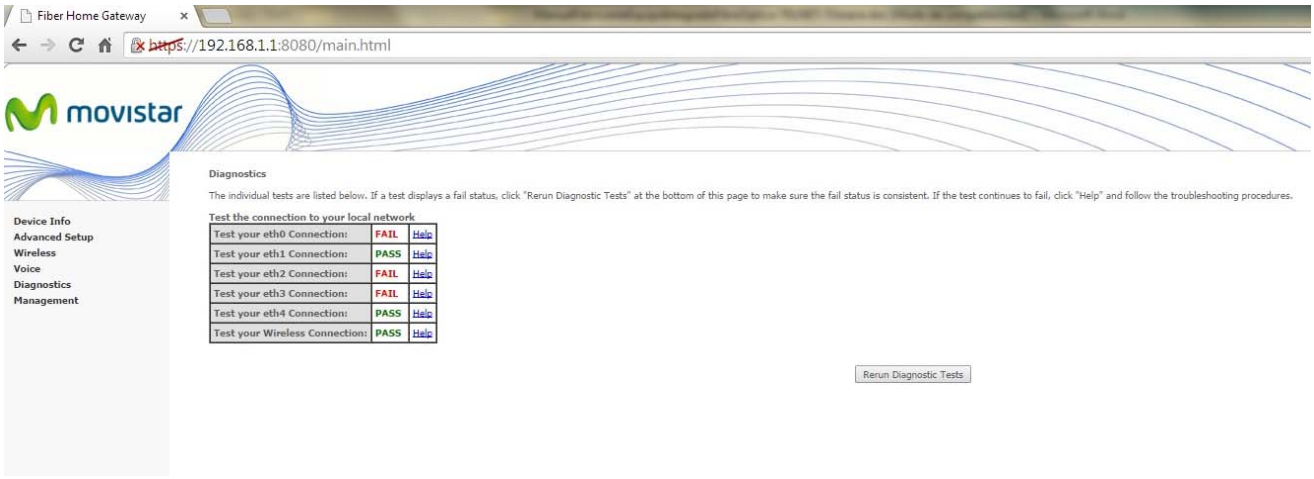
Campo	Descripción
Call waiting	Activa la llamada en espera en esta cuenta
Call forwarding number	Especifica el número de teléfono al que se desviarán las llamadas cuando el desvío de llamadas este habilitado
Forward unconditionally	Activa incondicionalmente el desvío de llamadas en esta cuenta
Forward on “busy”	Activa el desvío de llamadas cuando la cuenta está ocupada
Forward on “no answer”	Activa el desvío de llamadas cuando no hay respuesta en esta cuenta
Call barring	Activa la característica de bloqueo de llamadas salientes

Call barring pin	Especifica el PIN a utilizar cuando activamos el bloqueo de llamadas desde el terminal.
Call barring digit map	Especifica los números de teléfono que serán restringidos y serán comparados en cada ocasión para determinar si aplica el bloqueo de llamadas.
Warm line	Habilita la opción de configurar un número de teléfono para soporte
Warm line number	Especifica el número de teléfono de soporte.
Anonymous call blocking	Activa el bloqueo de llamadas entrantes anónimas.
Anomymous calling	Evita enviar información CLID (Calling Line Identification) en las llamadas salientes desde esta cuenta
DND	Activa la característica “No molestar” en esta cuenta.
Enable T38 Support	Habilita esta característica.
Enable V18 Support	Habilita esta característica.
Registration Expire Timeout	Especifica el timeout para el registro SIP
Registration Retry Interval	Especifica el intervalo de reintentos para el registro SIP
DSCP for SIP	Valor DSCP para los paquetes SIP salientes
DSCP for RTP	Valor DSCP para los paquetes RTP salientes.
Dtmf Relay Setting	Especifica el método a utilizar cuándo se transmiten los dígitos DTMF. Los posibles valores son: - **SIPInfo:** vía paquetes SIP INFO. - **In-band:** vía paquetes RTP en banda. - **RFC2833:** vía paquetes RTP RFC2833.
Hook Flash Relay setting	Especifica que evento se utiliza cuando se transmite eventos hook flash. Los posibles valores son: - **SIPInfo:** vía paquetes SIP INFO. - **None:** No trasnsmite eventos hook flash.
SIP Transport protocol	Especifica el protocolo de trasnsporte para los mensajes SIP salientes: - **UDP** - **TCP** - **TLS**

SRTP Configuration	Habilita SRTP (Secure Real-time Transport Protocol))
Enable SIP tag matching	Especifica si la etiqueta tiene que coincidir estrictamente para la confirmación de los diálogos SIP en todas las sesiones SIP.
Music Server	Nombre o dirección IP de un servidor de música
Music Server port	Puerto del servidor de música
Conference URI	URI de una conferencia.
Conference Option	Sólo es posible especificar la opción LOCAL

Diagnostics

Este apartado el resultado del test a cada interfaz de la red local. Para asegurarnos del estado actual de cada test, pulsar "*Rerun Diagnostics Tests*". Si el resultado del test es "*FAIL*", pulsa "*Help*" y sigue los procedimientos de *troubleshooting*.



Management

Settings

Esta sección incluye las siguientes opciones: "*Backup Settings*", "*Update Settings*" y "*Restore Default*".

Backup

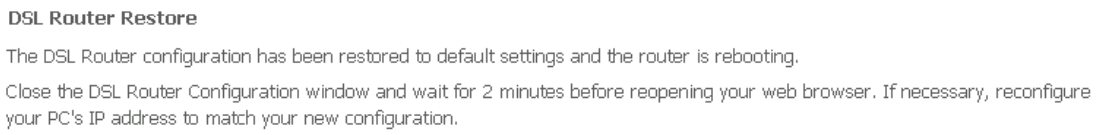
Para salvar la configuración actual a un fichero, haga clic en el botón "*Backup Settings*". Se le pedirá una localización en su PC donde guardar el fichero de seguridad. Este fichero puede ser recuperado posteriormente utilizando el botón "*Update Settings*" descrito a continuación.

Update

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 Default Settings*" para buscar el fichero. Haga clic en el botón "*Update Settings*" para recuperar la configuración.

Restore Default

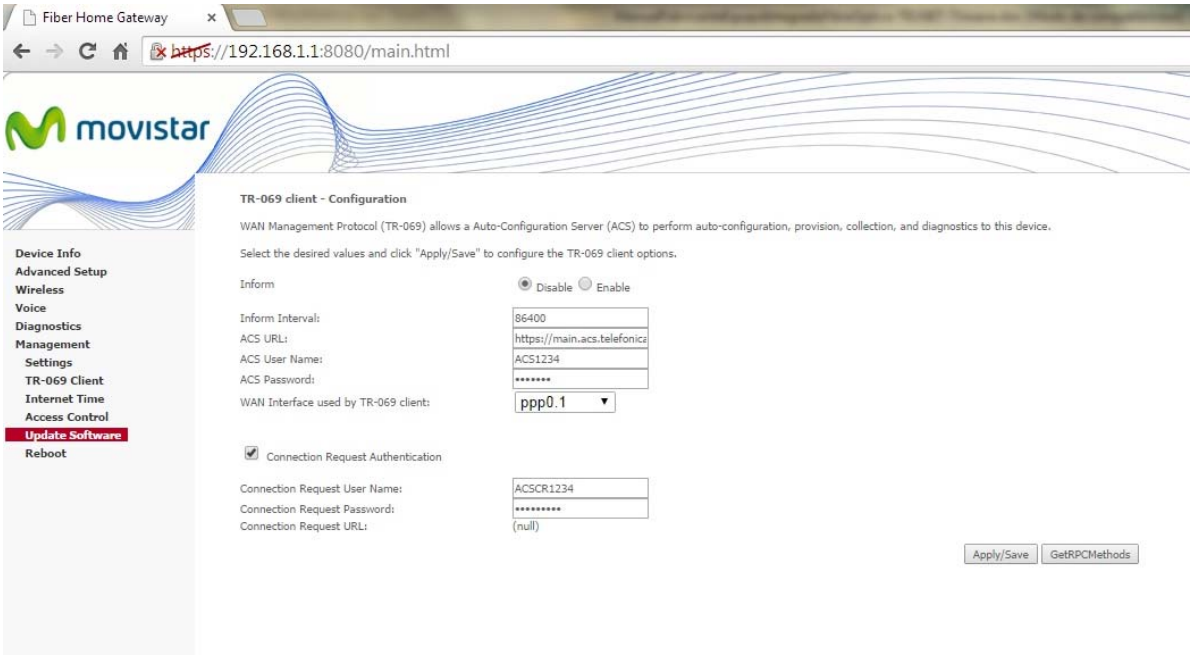
Haga Clic en el botón "*Restore Default Settings*" para restaurar los valores de fábrica o por defecto. Después de cliquear el botón "*Restore Default Settings*", se mostrará el siguiente mensaje:



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.

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.



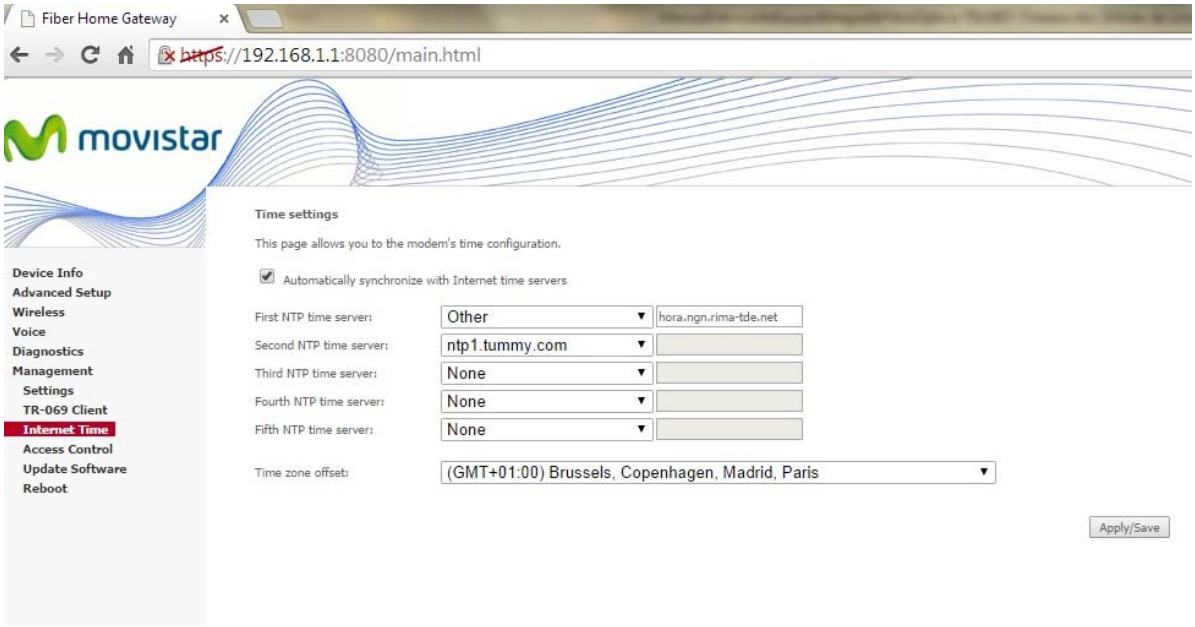
Campo	Descripción
Inform	Activa/desactiva el cliente TR-069
Inform Interval	La duración del intervalo en segundos para la cual el TriWave debe atender la conexión con el ACS y llamar al método "*Inform*".
ACS URL	URL para el CPE para conectarse al ACS utilizando *WAN Management Protocol*. Este parámetro 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 TriWave cuando se realiza una conexión al ACS utilizando *WAN Management Protocol*. Este nombre de usuario es usado solo para autenticación HTTP por el TriWave.

ACS Password	Contraseña utilizada para autenticar el TriWave cuando se realiza una conexión al ACS utilizando *WAN Management Protocol*. Esta contraseña es usada solo para autenticación HTTP por el TriWave.
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 TriWave.
Solicitud de conexión	
Authentication	Marca la casilla para activarlo
User Name	Nombre de usuario usado para autenticar una solicitud de conexión realizada a un ACS por el TriWave.
Password	Contraseña usada para autenticar una solicitud de conexión realizada a un ACS por el TriWave.
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.

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 Parental Control Además, este menú no es mostrado en modo Bridge, ya que el TriWave no sería capaz de conectar con el servidor NTP.

Access Control

Passwords

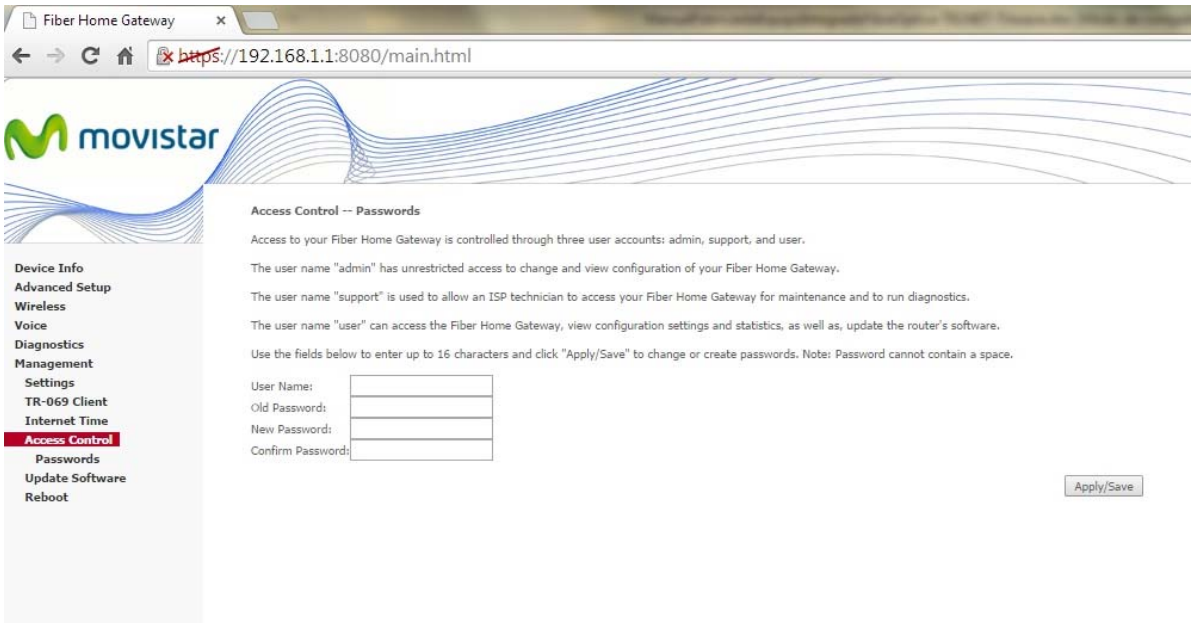
Esta pantalla es usada para configurar la contraseña de las cuentas de usuarios utilizadas para acceder el dispositivo. El acceso al TriWave es controlado a través del siguiente árbol de usuarios:

1234: Tiene acceso sin restricciones para cambiar y visualizar la configuración.

Support: Usado para mantenimiento remoto y diagnóstico del router.

User: Tiene acceso limitado. Esta cuenta puede ver los parámetros de configuración y estadísticas, así como, actualizar el firmware del router.

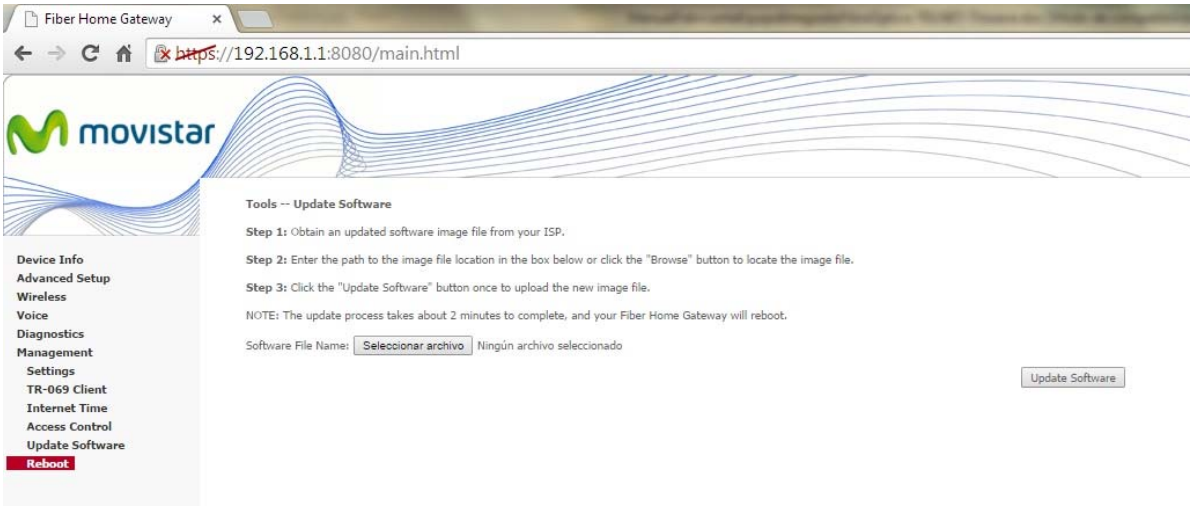
Use los siguientes campos para cambiar los parámetros de la contraseña. Haga clic en el botón "*Save/Apply*" para continuar.



Nota: La contraseña o password debe tener máximo, 16 caracteres.

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 Device Info con la versión de firmware instalada, para confirmar la instalación satisfactoria.

Reboot

Para guardar 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.

Información para el tratamiento de los equipos eléctricos y electrónicos al final de su vida útil (Aplicable en la UE y en países europeos con sistemas de recogida selectiva de residuos)

Este símbolo en el equipo, embalaje o manual de instrucciones indica que este producto, al final de su vida útil, no puede tratarse como un residuo doméstico normal, sino que debe ser recogido de forma selectiva.

Al entregar este producto para su gestión ambiental está evitando las posibles consecuencias negativas para el medio ambiente y la salud derivadas de una eliminación inadecuada. Además, mediante el reciclaje de los materiales que componen este producto se obtiene un ahorro importante de energía y recursos.

Para la recogida selectiva del producto puede contactar con el Dpto. Comercial de TELNET Redes Inteligentes S.A. en el teléfono 976.14.18.00, con su distribuidor habitual o consultar la página web www.telnet-ri.es

En cumplimiento del RD 208/2005, TELNET Redes Inteligentes S.A. participa en el Sistema Integrado de Gestión (SIG) de la Fundación ECOTIC

TELNET Redes Inteligentes S.A. se encuentra inscrito en el Registro nacional de productores de aparatos eléctricos y electrónicos (REI-RAEE) del Ministerio de Industria, Turismo y Comercio con el número 1746