Televes®



wave DATA

Refs. 769001, 769002

Art. Nr. WAVEDATAP, WAVEDATAS

WaveData AP MyNETWiFi

Guía de usuario

Televes

Contenido

Importantes instrucciones de seguridad 4
Introducción 4
- Características WaveData 4
- Contenido del paquete WaveData 5

Consideraciones de seguridad 5
Consideraciones en la instalación 5
Dispositivo WaveData 5
- Conexiones del dispositivo 5
- Botones del dispositivo 6
- Leds del dispositivo 6

Instalando WaveData 7
- Ejemplo instalación Ref. 769001 7
- Ejemplo instalación Ref. 769002 7

Conectándose a WaveData 8
- Acceso WaveData vía SSH 8
- Acceso WaveData vía Web 8
- Acceso interfaz Web 8

Configurando WaveData 9
- Estado del dispositivo 9
- Configuración del sistema 9
- Configuración de Red 10
- Configurando las interfaces Wi-Fi 14
- Interfaces VLAN en el Switch 16
- Configuración del Firewall 17
- Actualización de Firmware y Configuración 19

Lista de acrónimos 21
Características WaveData 22

Importantes instrucciones de seguridad

Antes de manipular o conectar este equipo, por favor lea este manual !

Instalación segura

- Lea las instrucciones antes de manipular o conectar el equipo. Conserve estas instrucciones. Preste atención a todas las advertencias. Siga todas las instrucciones.
- Limpie la unidad sólo con un paño seco.
- No utilice este aparato cerca del agua. El aparato no debe ser expuesto a caídas o salpicaduras de agua, no situar objetos llenos de líquidos sobre o cerca del aparato tales como vasos si no tiene la suficiente protección.
- No bloquee las aberturas de ventilación. Realizar la instalación de acuerdo con las instrucciones del fabricante. Dejar un espacio libre alrededor del aparato para proporcionar una ventilación adecuada.
- No situar el equipo en ambientes de humedad elevada.
- No instalar cerca de fuentes de calor tales como radiadores, registros de calor, estufas u otros aparatos (incluyendo amplificadores) que produzcan calor. No situar sobre el aparato fuentes de llama desnuda, tales como velas encendidas.
- No situar el equipo donde pueda estar sometido a fuertes vibraciones o sacudidas.
- Utilice solamente los aditamentos/accesorios especificados por el fabricante.

Utilización segura de equipos conectados a la red eléctrica

- La temperatura ambiente no debe superar los 45°C.
- La tensión de red de este producto ha de ser de: 220-230V~ 50/60Hz.
- No enchufe el equipo a la red eléctrica hasta que todas las demás conexiones hayan sido realizadas.
- La toma de red eléctrica debe estar cerca del equipo y ser fácilmente accesible.
- Para desenchufar el equipo de la red eléctrica, tire siempre de la clavija, nunca del cable.
- No pise ni pellizque el cable de red, tenga especial cuidado con las clavijas, tomas de corriente y en el punto del cual salen del aparato.
- Desenchufe este aparato durante las tormentas eléctricas o cuando no lo utilice durante largos períodos de tiempo.
- Solicite todas las reparaciones a personal de servicio cualificado. Solicite una reparación cuando el aparato se haya dañado de cualquier forma, como cuando el cable de red o el enchufe están dañados, se ha derramado líquido o han caído objetos dentro del aparato, el aparato ha sido expuesto a la lluvia o humedad, no funciona normalmente, o haya sufrido una caída.

Advertencia

- Para reducir el riesgo de fuego o choque eléctrico, no exponer el equipo a la lluvia o a la humedad.



Este símbolo indica que el equipo cumple los requerimientos de seguridad para equipos de clase II.



Este símbolo indica total cumplimiento con el marcado CE.



Este símbolo indica que el equipo es para uso en interior.



Tratamiento de los equipos eléctricos y electrónicos al final de su vida útil (Aplicable en la Unión Europea y en países europeos con sistemas de recogida selectiva de residuos).

Introducción

Ref. 769001/769002 **WaveData AP** es la siguiente generación de productos de acceso Wi-Fi, basado en un potente chipset incluye los últimos desarrollos tecnológicos del standard IEEE 802.11/b/g/n 2,4GHz e IEEE 802.11/n/ac 5GHz.

Características WaveData

IEEE 802.11ac es la siguiente evolución del estándar Wi-Fi que puede alcanzar tasas superiores al gigabit por segundo. La especificación 802.11ac opera en la banda de 5GHz, donde hay más canales disponibles y menor probabilidad de interferencia y mayor disponibilidad por la presencia de AP cercanos, comparado con la banda 2,4GHz. El IEEE 802.11ac alcanza un rendimiento superior a 802.11n usando más streams, mayor ancho de bando, modulaciones más altas y unas técnicas de gestión del ancho de banda mejoradas.

Multi-user MIMO (MU-MIMO) es una característica avanzada definida en el standard 802.11ac que permite que varios usuarios Wi-Fi (STA) recibir transmisiones simultáneamente desde el punto de acceso (AP) en subcanales del canal de transmisión de 5GHz; Esto mejora notablemente el rendimiento de la red Wi-Fi disminuyendo la latencia puesto que la transmisión se realiza simultáneamente. MU-MIMO también incrementa el rendimiento cuando el cliente (STA) no dispone de múltiples antenas.

Características Wi-Fi

- 2,4GHz IEEE 802.11/b/g/n con 2 Streams MIMO (2x2).
- 5GHz IEEE 802.11/n/ac Wave2 con 2 Streams MIMO (2x2)
- Hasta 16 SSIDs y 124 clientes por SSID.
- Modulaciones OFDM BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM y anchos de banda de canal de 20/40/80MHz que permiten alcanzar hasta 1.73 Gbps: 867 Mbps en la interfaz 802.11ac 2x2 5GHz y 300Mbps en la interfaz 802.11n 2x2 2,4GHz.
- **4xDual Band Antenna** con +4dBi of ganancia. Potencia de transmisión 2,4GHz: 23.5dBm@MCS0 HT20 y 16.5dBm@MCS9 HT40. Potencia Transmisión 5GHz: 22dBm@MCS0 HT20, 15.5dBm@MCS9 HT40 y 14.5dBm@MCS9 HT80.
- **Modos de Seguridad Wi-Fi** Open/WEP/WPA-PSK/WPA-EAP (WPA Enterprise). Soporta cifrados WPA-TKIP/WPA-AES.
- **Aislamiento de clientes AP**: Permite aislar los clientes de un AP y evitar la comunicación STA a STA.
- **Multi-user MIMO (MU-MIMO)**: esta característica avanzada definida en el estándar 802.11ac permite comunicaciones simultánea de múltiples clientes del punto de acceso (AP) hasta cuatro clientes (STAs).
- **Load Band Steering**: soporte simultaneo de doble banda (2,4GHz and 5GHz) con la habilidad de guía activa de los clientes hacia el mejor ancho de banda disponible.
- **QoS**: WMM e IEEE 802.11e para QoS sobre Wi-Fi. Voz, Video y otros protocolos sobre Wi-Fi que requieren de QoS y/o baja latencia.
- **Wi-Fi Roaming:** autentificación rápida de clientes móviles al mejor AP disponible mediante el uso de los estándares IEEE 802.11k para Radio Resource Management (RRM) e IEEE 802.11r Fast BSS transition (FT-BSS).

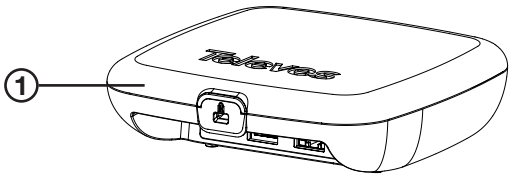
Características de Red

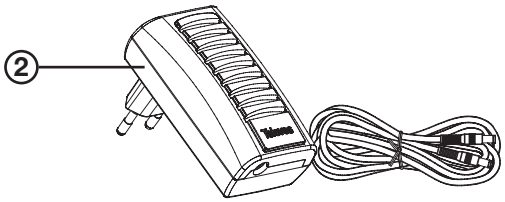
- El dispositivo puede operar en modos Bridge y Router.
- Soporte IEEE 802.1Q VLAN sobre interfaces Ethernet y Wi-Fi.
- Soporte de protocolos de red: DCHP, PPPoE, L2TP para permitir una integración sencilla con el servicio del proveedor de la red.
- Soporte de tráfico Multicast e IGMP/MLD Snooping.
- Firewall para proteger el acceso al dispositivo.
- **OpenVPN** para crear conexiones seguras con redes externas.
- **IEEE 802.1X** port-based authentication y servidor Radius externo. Permite la autentificación de dispositivos Wi-Fi mediante el servidor Radius del proveedor, evitando accesos no autorizados si la autentificacion falla.
- Posibilidad de alimentar el dispositivo a traves de un switch PoE IEEE802.3af o bien de una fuente de alimentacion externa de 12Vdc.

Requerimientos del sistema

- El sistema es Plug and Play y no requiere de ningún software o driver adicional.
- El dispositivo se configura a través de una interfaz Web y requiere de un PC con conexión Ethernet o Wi-Fi. Se recomienda el uso de las últimas versiones disponibles de los navegadores Firefox o Google Chrome.

Contenido del paquete WaveData





1	WaveData
2	Adaptador 12Vdc 1A (sólo ref. 769002)

Consideraciones de seguridad

Tenga en cuenta que el servicio SSH y la Web de acceso del WaveData siempre están accesibles en el dispositivo, tanto en la interfaz LAN como en la interfaz WAN.

- La cuenta de acceso a SSH/Web root/76Wave90Data01 es pública, como este manual. Cambiar la contraseña de acceso en el dispositivo debería ser realizado antes que ninguna otra consideración de seguridad.
- El firewall ha sido habilitado en la interfaz WAN mediante la zona WAN. Esta zona firewall admite únicamente peticiones DHCP, protocolo UPNP, SSH y Web como servicios abiertos a un acceso externo.
- El firewal ha sido habilitado en la interfaz LAN, mediante la zona LAN. Todo las peticiones de acceso desde la LAN serán aceptadas.

En algunas instalaciones considere cambiar la configuración del firewall para restringir el acceso al dispositivo desde la LAN (en hoteles o ámbitos de dominio público dónde se quiere evitar la conexión del usuario al dispositivo) o desde la WAN (si el dispositivo obtiene una IP pública y la interfaz WAN es expuesta a ataques externos)

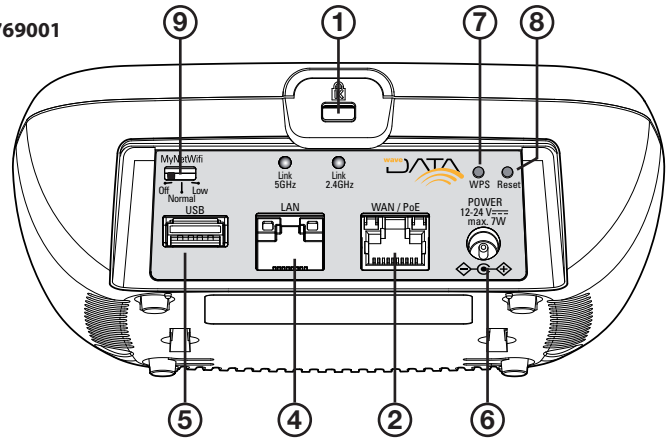
Consideraciones en la instalación

Considere las siguientes notas acerca de la instalación del WaveData:

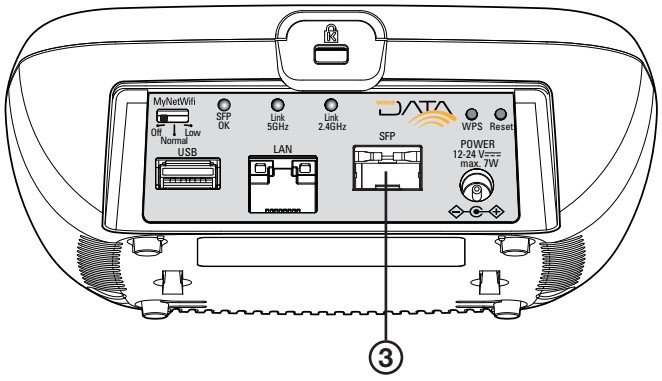
- No cubra el dispositivo, sitúelo en un lugar en dónde no puedan darse problemas térmicos; dónde las ranuras de disipación del chasis plástico estén lo suficientemente ventiladas y se garantice un correcto flujo del aire a través del dispositivo.
- Sitúe el dispositivo en un sitio despejado para garantizar la cobertura Wi-Fi. Instale el dispositivo en una pared, en sitios elevados o en un lugar dónde la cobertura Wi-Fi sea la mayor posible.

Dispositivo WaveData

769001



769002



Conexiones del dispositivo

① Slot de seguridad Kensington

En la parte dorsal del dispositivo hay un Slot Kensington para fijar el dispositivo durante el montaje e impedir que el dispositivo sea robado cuando es instalado en espacios públicos.

② 1xEthernet RJ-45 WAN (PoE) - (sólo ref. 769002)

Soporta IEEE 802.3af/at y PoE pasivo 36-56V hasta 24Watts (max). Conector Ethernet 100BASE-TX/1000BASE-T con Auto-MDIX auto negociación.

③ 1xSFP 1000BASE-X

Conector SFP (small form-factor pluggable transceptor) 1000BASE-X. Para conexión a fibra óptica.

④ 1xEthernet RJ-45 LAN

Ethernet 100BASE-TX/1000BASE-T con Auto-MDIX. Proporciona acceso por cable a la red local.

⑤ Conector USB

Conector USB 3.0 para conectar un dispositivo de almacenamiento o modem USB (GPRS, 3G, 4G, etc...) para el acceso a redes móviles.

⑥ Conector alimentación Jack 12-24 Vdc

Conector jack como alternativa a la alimentación por PoE. Admite rango 12–24Vdc.

Botones del dispositivo

⑦ Botón WPS

Este botón tiene una doble funcionalidad

- **Inicio de sesión WPS**: Para iniciar una sesión WPS pulse el botón en el AP para autorizar a los dispositivos. Pulse también el botón WPS en una estación Wi-Fi para completar la sesión WPS. La sesión estará activa durante un máximo de 120 segundos, tras lo cual se desactivará.
- **Valores de Fábrica**: Pulse el botón durante al menos tres segundos para restaurar la configuración por defecto. Esto borrará la configuración actual del dispositivo y restaurará la configuración de fábrica.

⑧ Botón de Reset

Pulse el botón para realizar un reset hardware del dispositivo. Una alternativa es realizar un reset software mediante una operación de reboot vía la interfaz Web o comando SSH. El software reset es un método más adecuado puesto que garantiza que la integridad y seguridad de la configuración.

⑨ Conmutador MyNETWi-Fi

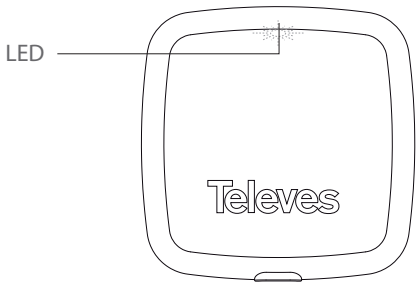
Este conmutador de tres estados permite configurar la potencia de transmisión de las interfaces Wi-Fi en las dos radios: 2,4GHz y 5GHz.

Posición	Función
Off	Wi-Fi Apagado
Normal	Potencia Wi-Fi controlada por Software. (max. 23dBm)
Low	Modo MyNETWi-Fi (max. 10dBm)

Leds del dispositivo

Led RGB Frontal

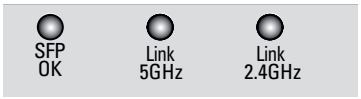
El dispositivo tiene un led RGB frontal para indicar su estado.



Funciones Led RGB	
Actividad del dispositivo	Patrón del LED
Inicio del sistema (kernel)	Parpadeo Naranja
AP emitiendo SSIDs	Verde
myNETWi-Fi	Naranja
Wi-Fi Apagado/Todos los VAPS desactivados.	Azul
Actualización del sistema (firmware o configuración)	Parpadeo Azul
Fallo del dispositivo	Rojo o Parpadeo Rojo
Sistema apagado o Fuente de alimentación desconectada	Led Apagado

Leds del dispositivo (posteriores)

El dispositivo tiene varios leds posteriores:



- **2,4GHz Link**: Parpadeo indica que el Radio Wi-Fi 2,4G está activado y funcionando. Fijo o Apagado que la Radio Wi-Fi 2,4G está apagada.
- **5G Link**: Parpadeo indica que el Radio Wi-Fi 5G está activado y funcionando. Fijo o Apagado que la Radio Wi-Fi 5G está apagada.
- **SFP OK** (sólo en ref. 769002): indica lo que se conoce como "LOS LED (SFP)". Es decir, indica que el SFP está instalado y que hay enlace óptico.

  LOS: *Loss Of Signal*. Led de pérdida de señal. Indica si existe algún problema con la red de fibra.

  LED "LOS" ACTIVO (LED en ROJO), si la recepción del interfaz (RX) detecta pérdida de señal (LOS). LED "LOS" estará APAGADO si detecta presencia de señal (LINK).

Instalando WaveData

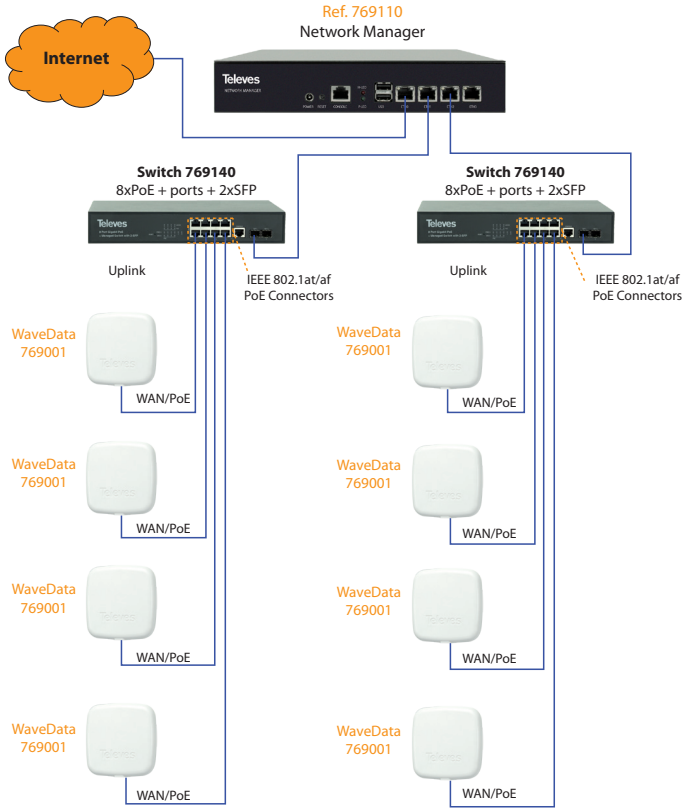
Ejemplo instalación Ref. 769001

La siguiente figura muestra una instalación de referencia de la Ref. 769001 WaveData PoE.

En la instalación mostrada se utilizan dos switches PoE 769140 con 8 puertos PoE IEEE 802.3af/at para la conexión y alimentación de la Ref. 769001.

El conector Ethernet proporciona alimentación y datos simultáneamente.

La Ref. 769110 Network Manager se utiliza como Router de Salida a Internet.

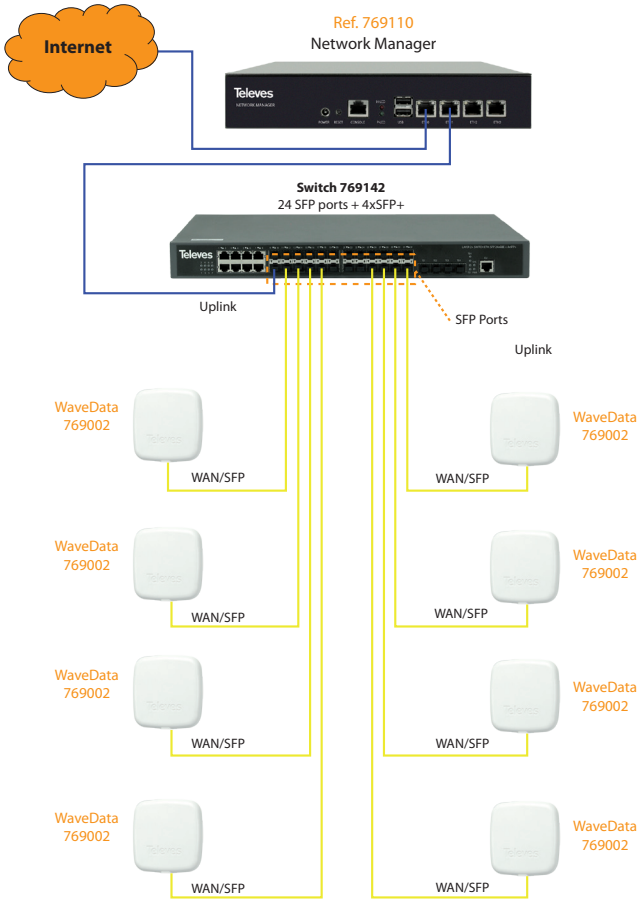


Ejemplo instalación Ref. 769002

En la instalación mostrada se utilizan un Switch 769142 con 24xSFP ports + 4xSFP+ para la conexión con la Ref. 769002 WaveData SFP.

Los enlaces de fibra óptica monomodo se pueden realizar con SFP's 769210 0 769212.

La Ref. 769110 Network Manager se utiliza como Router de Salida a Internet.



Conectándose a WaveData

Para facilitar la instalación del producto, el dispositivo viene configurado en modo bridge y predefinido con dos interfaces.

- **LAN**: IP estática 169.254.1.254. La interfaz LAN incluye todos los puertos Ethernet y las interfaces Wi-Fi.
- **LAN_DHCP**: Interfaz LAN configurada como cliente DHCP.

De esta forma sobre la interfaz LAN tendremos dos IP:

- Una dirección IP fija 169.254.1.254: disponible para la conexión local al dispositivo cuando no exista un servidor DHCP en la instalación.
- Una dirección IP obtenida por cliente DHCP cuando el dispositivo sea instalado un red en donde el Router asigne direcciones a los dispositivos de la red con un servidor DHCP.

Para acceder al dispositivo utilice las siguientes credenciales:

- IP por defecto: LAN => 169.254.1.254, LAN_DHCP => cliente DHCP.
- Usuario: **root**
- Contraseña: **76Wave90Data01**

Acceso WaveData vía SSH

El terminal SSH puede ejecutar cualquier comando en el WaveData como la instalación de nuevos paquetes, añadir/eliminar/reiniciar un servicio o un cambio de configuración. El servicio SSH se ejecuta en el puerto TCP 22.

El siguiente ejemplo muestra como conectarse vía SSH:

```
$ sshpass -p 76Wave90Data01 ssh root@192.168.1.1
BusyBox v1.25.1 (2018-06-25 18:51:51 CEST) built-in shell (ash)
     MM           NM                   MMMMMMM          M       M
    $MMMMM        MMMMM               MMMMMMMMMMM      MMM     MMM
  MMMMMMMMM     MM MMMMM.             MMMMM:MMMMMM:    MMMM   MMMMM
MMMM= MMMMMM   MMM    MMMM       MMMMM   MMMM  MMMMMM   MMMM  MMMM'
MMMM=   MMMMM MMMM     MM        MMMMM    MMMM    MMMM   MMMMNMMMMM
MMMM=    MMMM  MMMMM             MMMMM    MMMM    MMMM   MMMMMMMM
MMMM=    MMMM   MMMMMM         MMMMM     MMMM    MMMM   MMMMMMMM
MMMM=    MMMM     MMMMM,     NMMMMMMMM    MMMM    MMMM   MMMMMMMMMM
MMMM=    MMMM       MMMMMM   MMMMMMMM     MMMM    MMMM   MMMM  MMMMMM
MMMM=    MMMM   MM    MMMM    MMMM       MMMM    MMMM   MMMM    MMMM
MMMM$ ,MMMMM  MMMMM  MMMM     MMM        MMMM    MMMM   MMMM    MMMM
  MMMMMMM:      MMMMMMM     M          MMMMMMMMMMM  MMMMMMM MMMMMMM
    MMMMMM       MMMMN     M            MMMMMMMM      MMMM    MMMM
     MMMM           M                    MMMMMM        M       M
       M
 ------------------------------------------------------------
   For those about to rock... (Chaos Calmer, r47828)
 ------------------------------------------------------------
root@OpenWrt:~#
```

Acceso WaveData vía Web

El dispositivo dispone de una interfaz Web en el puerto 80. El objetivo de la interfaz Web es configurar el dispositivo y realizar tareas de administración

Use las siguientes credenciales para el acceso.

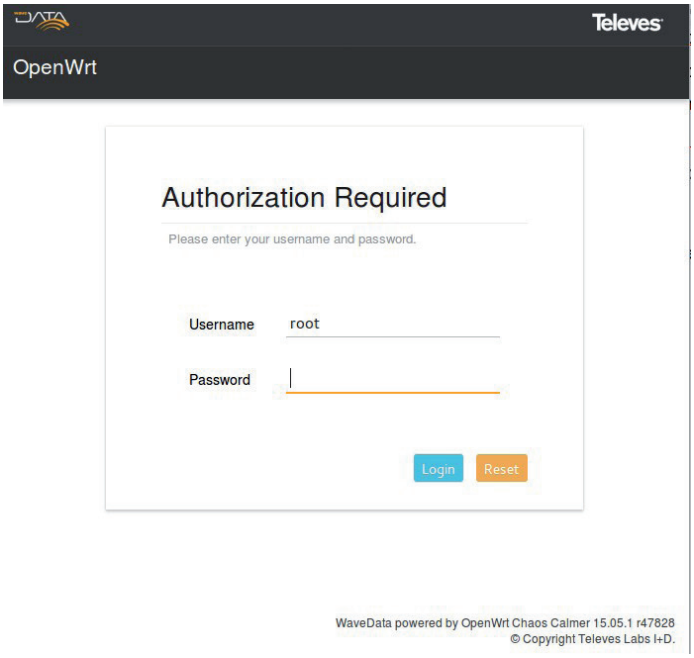
- Usuario: **root**
- Contraseña: **76Wave90Data01**

Acceso interfaz Web

Utilice la ultima versión del navegador Firefox o Google Chrome para dirigirse a la interfaz Web del dispositivo: http://169.254.1.254.

La captura muestra el login de la interfaz Web.

Introduzca las credenciales.

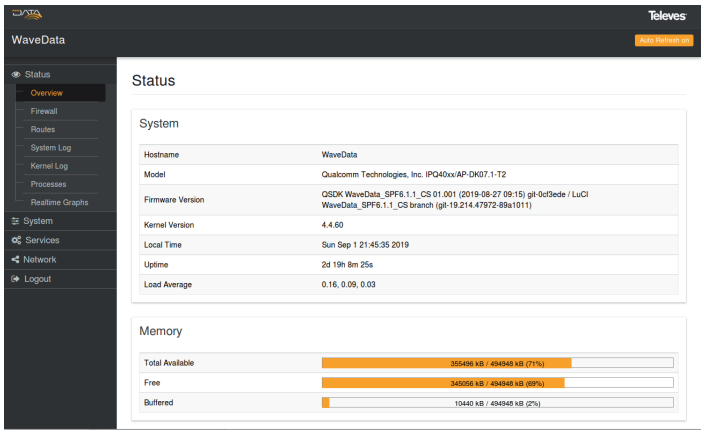


ES

Configurando WaveData

Estado del dispositivo

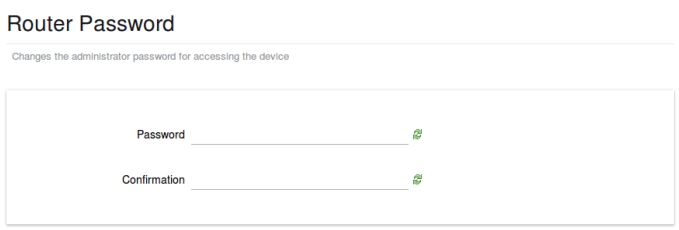
Vaya a ***Status***>***Overview*** para ver el estado del dispositivo



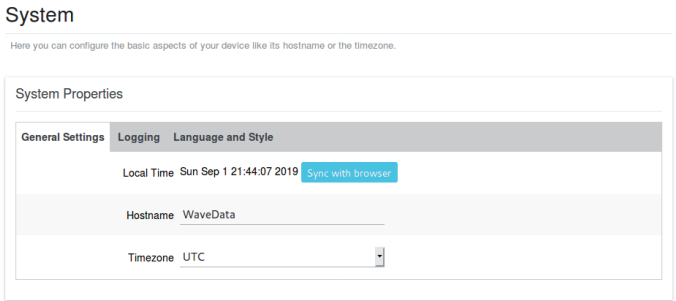
Configuración del sistema

Cambio de Contraseña

Vaya a ***System***>***Administration*** para cambiar la Contraseña de la cuenta de administración utilizada durante el acceso.



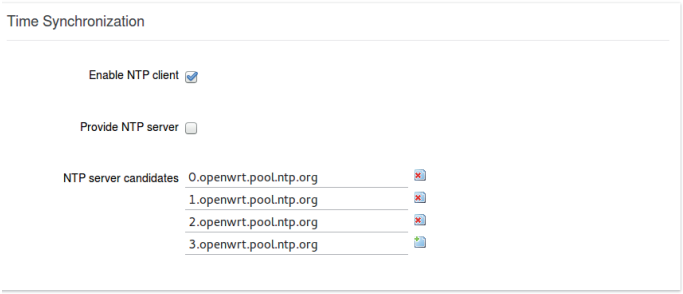
Nombre del Anfitrión y Zona horaria



- **Sync with browser**: Establece la fecha actual del dispositivo a la hora utilizada por el navegador.
- **Hostname**: Nombre del dispositivo
- **Timezone**: Timezone del dispositivo. Por defecto es UTC.

Sincronización de tiempo

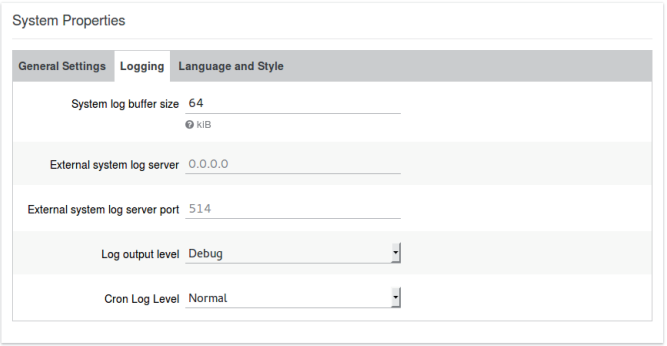
El WaveData permite sincronizar la fecha del sistema a través de un servidor NTP (Network time protocol).



- **Enable NTP Client**: Permite configurar el tiempo del sistema a través de los candidatos de servidores NTP definidos.
- **Provide NTP Server**: Permite al WaveData convertirse en un servidor NTP para proveer tiempo/fecha.
- **NTP Server Candidates**: Candidatos de servidores NTP. Introduzca servidores NTP válidos para configurar el tiempo del sistema.

Registro del sistema

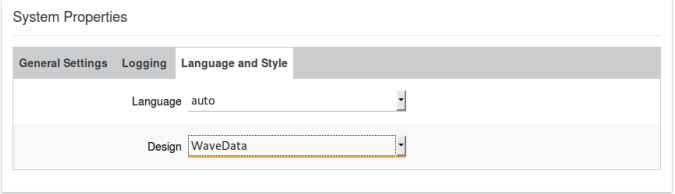
El WaveData guarda un registro de eventos. Por defecto el registro no es almacenado en un fichero, es almacenado en un buffer circular. A medida que se introducen nuevas entradas en el registro, las más antiguas son borradas. La siguiente web configura el registro del sistema.



- **System log buffer size**: Tamaño del buffer del registro del sistema. Por defecto 64KiB.
- **System Log server**: Servidor de registro del sistema. Introduzca una dirección IP del servidor de registro del sistema. La especificación vía hostname no es válida. Establezca el puerto de destino, por defecto 514.
- **Log output Level**: Nivel de salida del registro. Cambie el nivel de los mensajes añadidos al registro del sistema. Por defecto Debug (depuración).
- **Cron Log level**: Introduzca el nivel de los mensajes registrados por el servidor cron.

Estilo e Idioma del sistema

Cambie el idioma y el estilo de la interfaz Web.



- **Language**: Cambie el idioma de la interfaz Web.
- **Design**: Cambie el estilo de la interfaz Web.

Configuración de Red

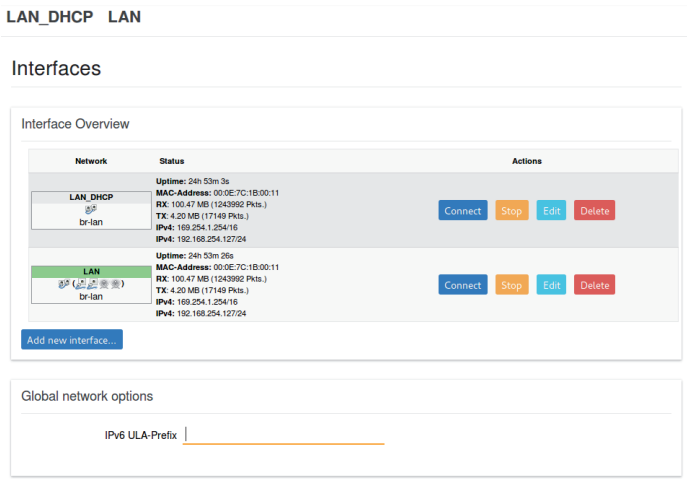
El sistema tiene dos interfaces predefinidas:

- **LAN**: Esta es una interfaz bridge, llamada br-lan: como miembros tiene todas las interfaces físicas del sistema, esto es, los Wi-Fi VAP (Virtual access point) de 2,4G (ath0) y 5G (ath1) y las interfaces ethernet eth0 y eth1. Tiene asignada de forma estática la IP 169.254.1.254.
- **LAN_DHCP**: Esta interfaz añade un cliente DHCP a la interfaz LAN. El objeto de esta interfaz es permitir que el dispositivo obtenga una dirección IP adicional por DHCP, a expensas de la dirección IP 169.254.1.254 asignada estáticamente.

Esta configuración por defecto permite que el tráfico recibido por las interfaces sea automáticamente propagado en función de dónde esté situado el host de destino, minimizando las necesidades de configuración y facilitando la propagación de tráfico. Si necesita habilitar el modo Router en el dispositivo consulte la sección Configuración en modo Router.

Lista de interfaces

Para listar las interfaces del sistema vaya a ***Network*>*Interfaces***



Opciones de interfaz:

- **Delete Interface**: Elimina la interfaz en el dispositivo. La configuración asociada será eliminada.
- **Connect/Stop Interface**: Activa o desactiva la interfaz. Cuando desactiva una interfaz a través de la que se conecta al dispositivo, se pierde la conectividad con el dispositivo.
- **Add New Interface**: Añade una nueva interfaz al dispositivo.
- **Edit Interface**: Edita la configuración de la interfaz.

Cuando se realizan cambios en la configuración de varias interfaces, conviene guardar primero los cambios en la configuración, para posteriormente aplicarlos de forma conjunta en el sistema. Esto evita perdidas de conexión innecesarias. p.e. cuando una interfaz física como eth0 se desasigna de la interfaz LAN para asignarla a otra WAN.

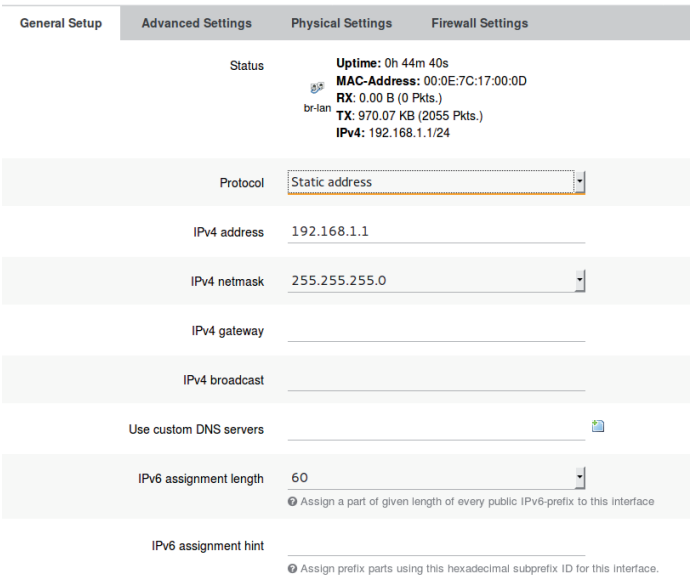
Para realizar este tipo de operaciones se proporción una serie de opciones globales que gestionan los cambios en la configuración antes de su aplicación:

- **Save&Apply**: Salva y Aplica todos los cambios de configuración realizados.
- **Save**: Salva los cambios realizados en la configuración, previamente a su aplicación. Guarda los cambios en la configuración en una lista antes de aplicarlos. Estos cambios pueden deshacerse con Reset.
- **Reset**: Elimina todos los cambios previamente realizados.

Interfaz: Configuración General

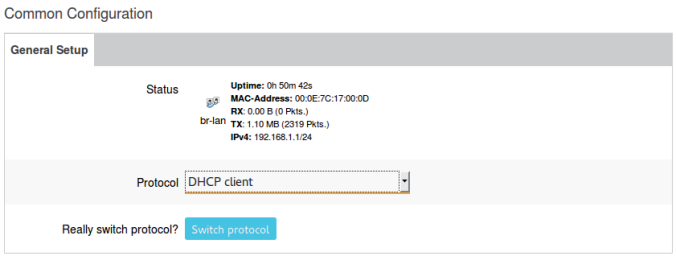
Vaya a Edit ***Interface*** > ***General Setup*** para configurar una interfaz y seleccionar el protocolo de operación.

La siguiente captura muestra la interfaz para configurar una interfaz con IP estática.



- **Protocol**: Selecciona el protocolo de la interfaz. Puede seleccionar DHCP, Static, PPPoE o LT2P. Al seleccionar un protocolo, la interfaz Web muestra las opciones disponibles para el mismo. Los protocolos soportados pueden ser extendidos instalando nuevos paquetes software.

  Haga click en el botón "Switch Protocol" para cambiar de protocolo en la interfaz.

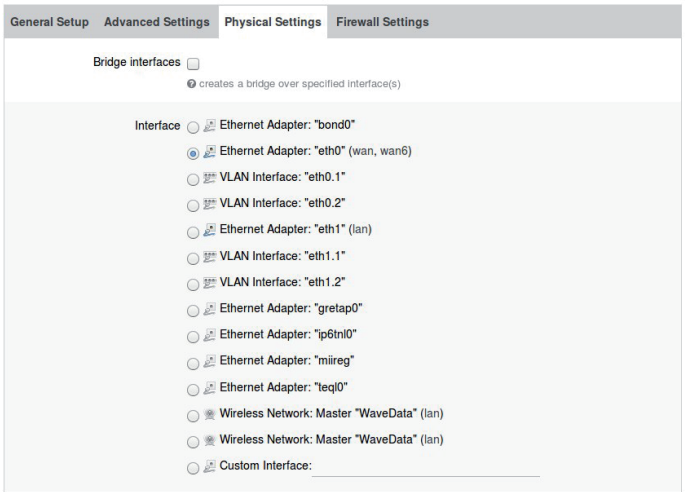


Interfaz: Seleccionando interfaces físicas

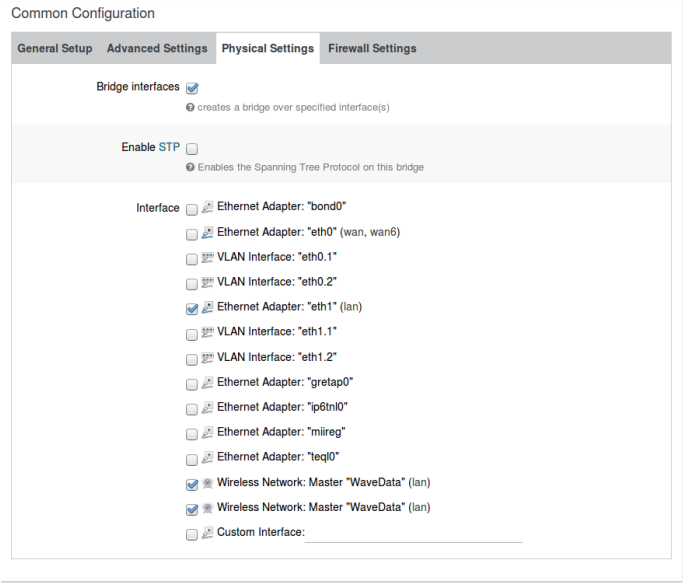
Vaya a ***Edit Interface*** > ***Physical Settings*** para configurar qué interfaces físicas serán gestionadas por la interfaz.

Existen dos formas de asociar una interfaz a una interfaz física:

- **Single interface**: La interfaz es formada únicamente por una interfaz física. La interfaz WAN, que se mostrará en el modo Router, es un ejemplo de una interfaz formada por una única interfaz física.



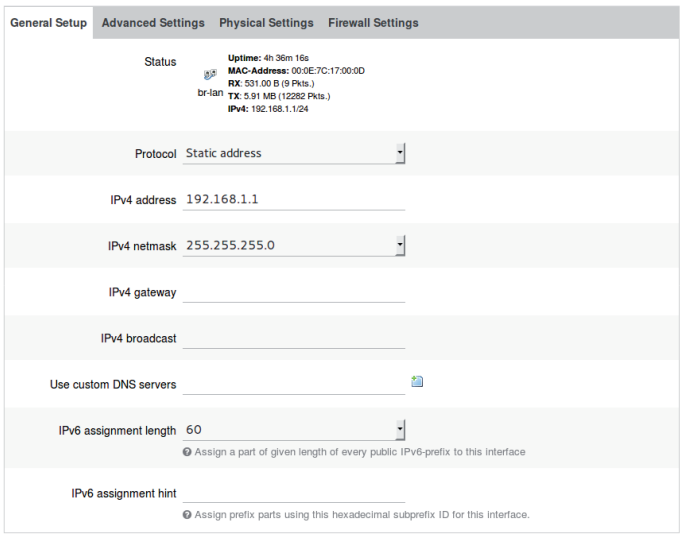
- **Bridged interface**: La interfaz es un bridge en dónde las interfaces físicas son miembros del mismo. La interfaz LAN es un ejemplo de este tipo interfaz, en dónde se crea un bridge, llamado br-lan, cuyos miembros son las dos interfaces radio (para 2,4GHz y 5GHz) y las interfaces ethernet, eth1 y eth0.



Interfaz: Seleccionando el protocolo

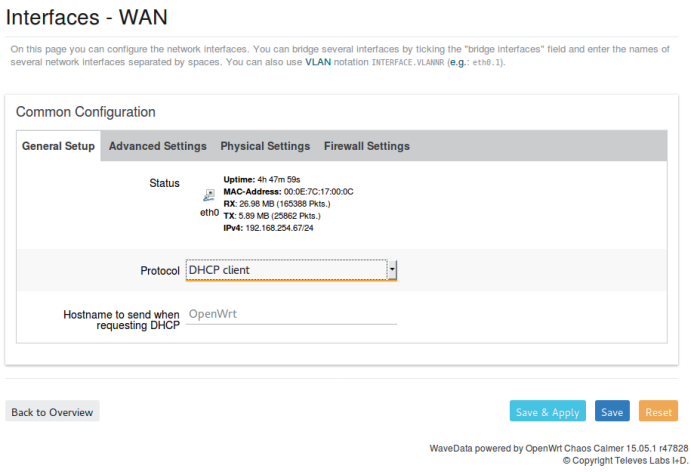
En ***Edit Interface*** > ***General Setup*** seleccione el protocolo de la interfaz entre: Static IP Address, DHCP client, PPPoE o L2TP. Cada protocolo tiene su propia configuración de acuerdo a parámetros específicos.

Dirección IP estática



- **IPv4 Address**: Dirección IP de la interfaz.
- **IPv4 netmask**: Mascara de red de la interfaz.
- **IPv4 gateway**: Gateway de la interfaz.
- **IPv4 broadcast**: Dirección broadcast de la interfaz.
- **DNS Servers**: Servidor DNS de la interfaz. Puede incluir múltiples DNS.

Cliente DHCP

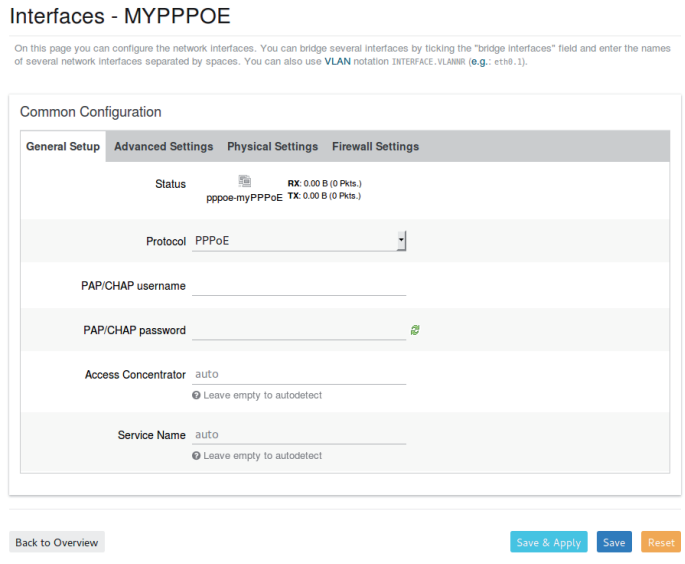


- **Hostname**: Establece un hostname especifico en la petición DHCP diferente del hostname del dispositivo.

Cliente PPPoE

Crea una conexión PPPoE con el servidor PPPoE del proveedor.

PPPoE (Point-to-Point Protocol over Ethernet o Protocolo Punto a Punto sobre Ethernet) es un protocolo de red para la encapsulación PPP sobre una capa de Ethernet. Es un protocolo de acceso a Internet punto a punto que permite al WaveData establecer una conexión con un servidor ofreciendo autenticación, cifrado, mantención y compresión. Consulte con su proveedor para verificar si ofrece este servicio.



Por favor, use los siguientes parámetros PPP para configurar el tunnel PPPoE con el servidor:

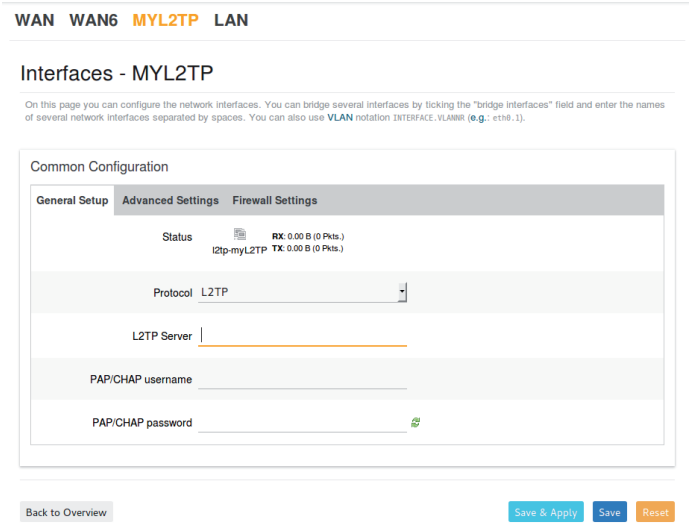
- **PAP/CHAP username**: Usuario de la cuenta PPP.
- **PAP/CHAP password**: Contraseña de la cuenta PPP.
- **Access Concentrator**: Especifica el servidor PPP al que conectarse. Normalmente este campo es el hostname de la maquina ejecutando el servicio, aunque puede ser diferente. Si no se indica, el cliente PPPoE se conectará con el primer servidor PPPoE que descubra.
- **Service Name**: Especifica el nombre de servicio del servidor PPP al que conectarse y debe coincidir con la configuración del servidor PPP. Este campo se utiliza para diferenciar entre servidores PPPoE instalados en

la misma red. Si no se indica, el cliente PPPoE se conectará con el primer servidor PPPoE que descubra.

Túnel L2TP

El protocolo L2TP (Layer 2 Tunneling Protocol) es un protocolo utilizado para soportar VPN (virtual private networks) como parte de los servicios prestados por los proveedores de Internet (ISP). Este protocolo no proporciona encriptación o confidencialidad sino que confía en otros protocolos de encriptación como IPSEC para proporcionar encriptación y seguridad.

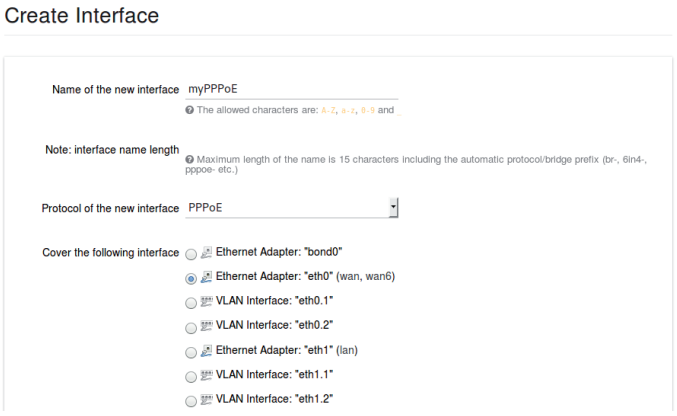
Publicado en 1999 como el estándar RFC 2661, L2TP ha sido desarrollado sobre la base de os antiguos protocolos de tunes para comunicaciones punto a punto: Cisco's Layer 2 Forwarding Protocol (L2F) y Microsoft Point-to-Point Tunneling Protocol (PPTP).



- **L2TP Server**: Servidor L2TP al que conectarse. Valores validos son un valor de hostname o una dirección IP.
- **PAP/CHAP username**: Usuario de la cuenta L2TP.
- **PAP/CHAP password**: Contraseña de la cuenta L2TP.

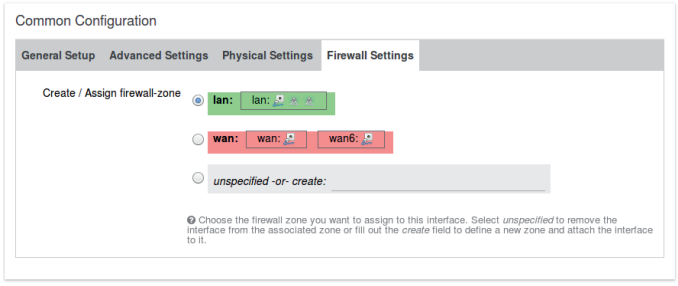
Añadiendo una nueva interfaz

Haga Click en el botón para crear una nueva interfaz. Puede seleccionar el protocolo de la interfaz y la interfaz/ces físicas. Puede añadir múltiples interfaces con diferentes protocolos sobre una misma interfaz física.



Interfaz: Configuración de Firewall

Vaya a ***Edit Interface*** > ***Firewall Settings*** para cambiar la zona firewall sobre la que opera la interfaz.

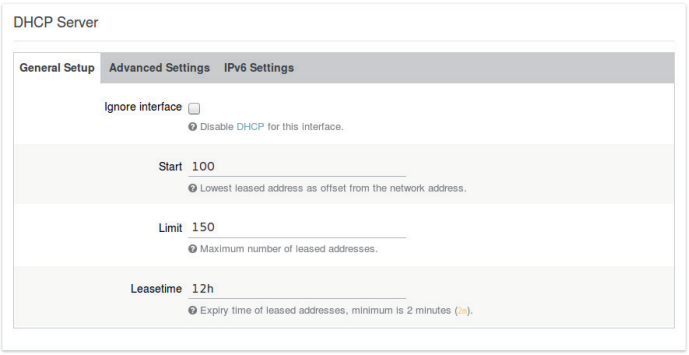


La interfaz puede ser asignada a una zona firewall. El firewall divide la red en varias zonas y cada zona tiene sus propias reglas de filtrado. Vaya a ***Network*** > ***Firewall*** para añadir o cambiar las reglas de cada una de las zonas del Firewall.

Interfaz: DHCP Server

Vaya a ***Edit Interface*** > ***DHCP server*** para habilitar el servidor DHCP server en la interfaz.

- **Ignore interface**: Seleccione esta opción si no quiere que el servidor DHCP asigne direcciones IP en esta interfaz.
- **Start**: Primera dirección IP valida para su asignación por DHCP. Este valor es tomado como un offset calculado sobre la dirección IP de la interfaz.
- **Limit**: Numero máximo de direcciones DHCP asignadas.
- **Lease Time**: Tiempo de expiración de las direcciones IP asignadas por DHCP. Introduzca un numero seguido de un prefijo ("s" para segundos, "h" para horas). Por ejemplo 120s o 24h.



Configuración en modo Router

El dispositivo viene preconfigurado para operar como bridge sobre todas las interfaces. Para cambiar el modo de configuración, de modo Bridge a modo Router, es necesario crear una nueva interfaz, llamada WAN:

- **WAN**: Esta interfaz tendrá asignada la interfaz física eth0 y utilizará el conector externo WAN/PoE (769001) o WAN/SFP (769002). Por defecto será configurada como cliente DHCP.
- **WAN6**: Esta interfaz tendrá asignada la interfaz física eth0 y utilizará el conector externo WAN/PoE (769001) o WAN/SFP (769002). Por defecto será configurada como cliente DHCPv6.

En modo router el dispositivo todavía conservará una interfaz local:

- **LAN**: esta interfaz crea un bridge, llamado br-lan, y tiene como miembros las interfaces Wi-Fi VAP (Virtual access point) de 2,4G (ath0) y 5G (ath1) y la interfaz ethernet local (eth1). Se configurará con IP 192.168.1.1 y un servidor DHCP para los clientes locales.
- **LAN_DHCP**: esta interfaz no será necesaria y será eliminada.

Con la creación de la interfaz WAN el dispositivo operará en modo router; la interfaz WAN se conectará a la red del proveedor y será configurada vía DHCP. La interfaz LAN es un bridge con la interfaz ethernet local (eth1) y las interfaces Wi-Fi como miembros.

El tráfico de la LAN será enrutado hacia la WAN utilizando NAT (Network Address Translation).

Modo Router: Creando la interfaz WAN

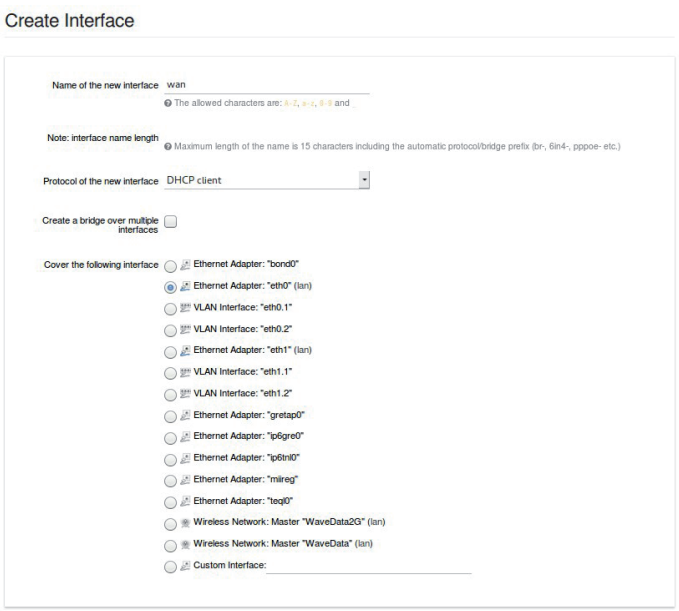
Es necesario:

- Crear una interfaz WAN con protocolo cliente DHCP.
- Asignar la interfaz física eth0 a la interfaz WAN.
- Asignar la zona WAN del firewall a la interfaz WAN.
- Activar NAT masquerading en la zona WAN.

Vaya a ***Interfaces*** > ***Add new Interface*** para crear una nueva interfaz llamada wan.

Seleccione DHCP client como protocolo de la interfaz y la interfaz física eth0.

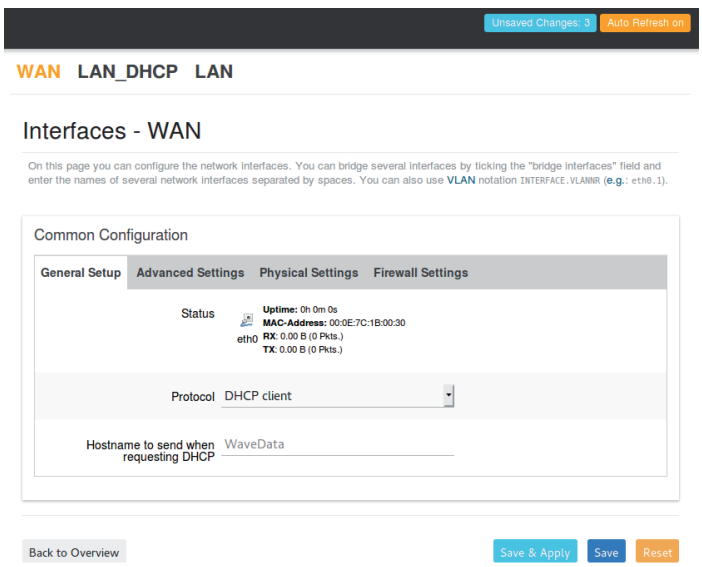
Para finalizar el proceso haga click en **Submit**. Este botón tan sólo realizará cambios en la configuración pero no los aplicará.



Los cambios realizados se indican en la parte superior izquierda: 

Al cambiar la configuración pero no aplicarla, nos permite seguir configurando el dispositivo hasta completar el cambio de configuración.

De otro modo, si aplicamos la modificación de la configuración sobre la interfaz con la que nos conectamos, el cambio puede suponer una perdida de conexión.



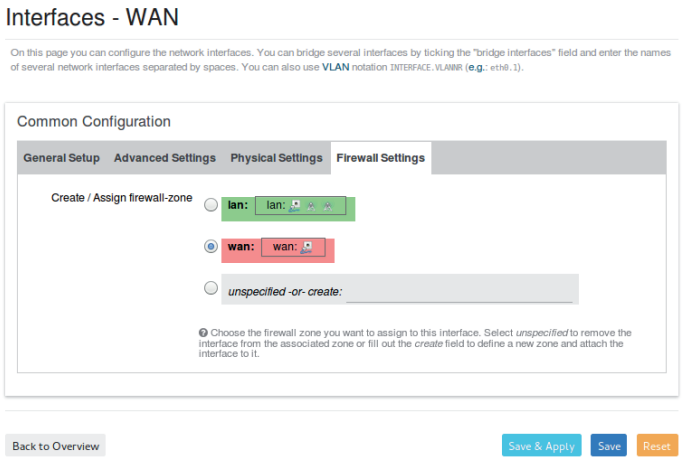
Modo Router: Zona firewall para la WAN

Si la red WAN sobre la que opera el dispositivo no es confiable es necesario activar el firewall. Por defecto el WaveData viene con una zona predefinida y configurada denominada zona WAN.

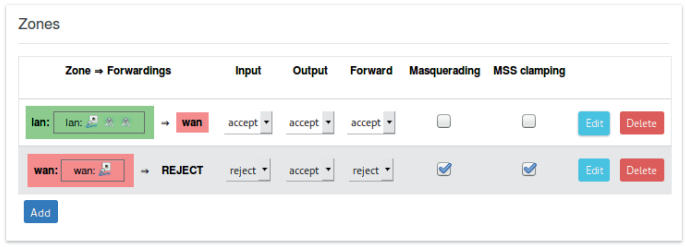
En el modo Router necesitamos también activar NAT masquerading para el tráfico de salida de la WAN.

Para asignar la interfaz WAN a dicha zona vaya a ***Interfaces*** > ***WAN*** > ***Firewall Settings*** y seleccione WAN como la zona a utilizar por la interfaz.

Pulse **Save** para guardar los cambios.



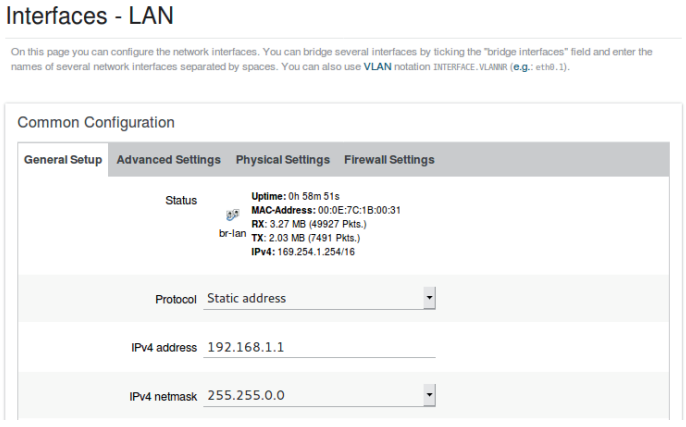
Vaya a ***Firewall*** > ***Zones*** y verifique que la zona WAN tiene activado el *masquerading*.



Modo Router: Configurando la interfaz LAN

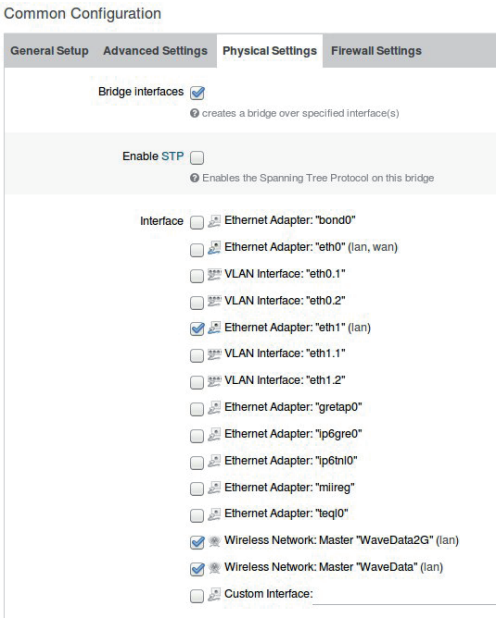
Se muestran los pasos para la configuración de la interfaz LAN en modo Router:

Vaya a ***Interfaces*** > ***LAN*** > ***IPV4 Address*** y configure la dirección IP: 192.168.1.1.

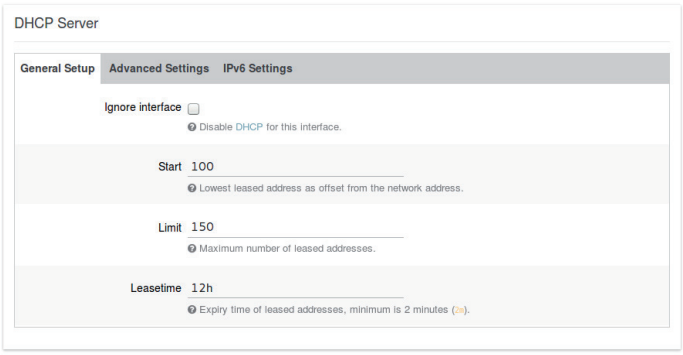


Desasignar la interfaz física eth0 de la interfaz LAN (está asignada por defecto).

Vaya a ***Interfaces*** > ***LAN*** > ***Physical Settings*** y elimine eth0 de la lista.

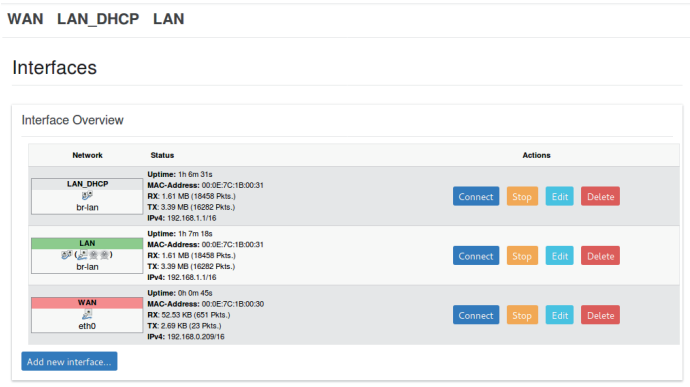


Vaya a ***Interfaces*** > ***LAN*** > ***DHCP Server*** y active el servidor DHCP.

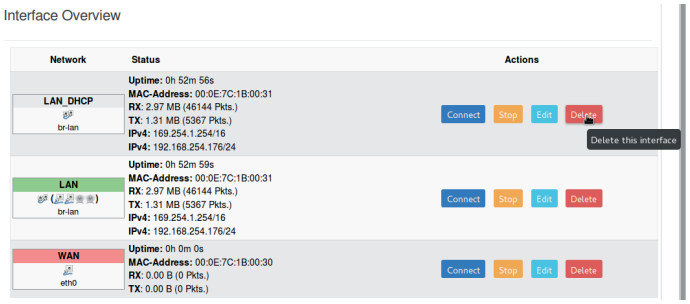


Finalmente, realizados los cambios, pulse en Save & Apply para aplicar la nueva configuración.

Se muestran la lista de interfaces, con la nueva interfaz WAN en la lista y con IP asignada por DHCP.

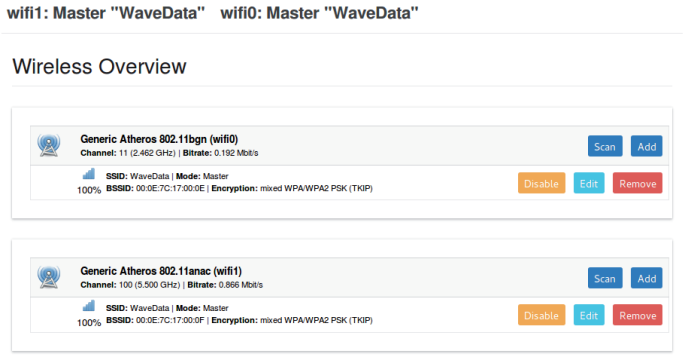


Para el modo router la interfaz LAN_DHCP ya no es necesaria. Vaya a ***Interfaces*** y haga click en el botón **Delete** de la interfaz LAN_DHCP para eliminarla.



Configurando las interfaces Wi-Fi

Vaya a ***System*** > ***Wi-Fi*** para ver la lista de interfaces Wi-Fi.



La Web ofrece los siguientes botones para cada interfaz Radio:

- **Scan**: Escanea la red para encontrar los AP disponibles.
- **Add**. Añade un nuevo VAP.

Y los siguientes botones por VAP (Virtual Access Point)

- **Disable/Enable** VAP.
- **Edit**: Configura las opciones del VAP.
- **Remove**: Elimina este VAP de la interfaz Wi-Fi.

Lista de clientes asociados

Muestra la lista de clientes conectados con las interfaces Wi-Fi.

Para cada cliente, muestra el SSID con el que esta conectado, su MAC y las tasas y niveles de señal de la conexión Wi-Fi.

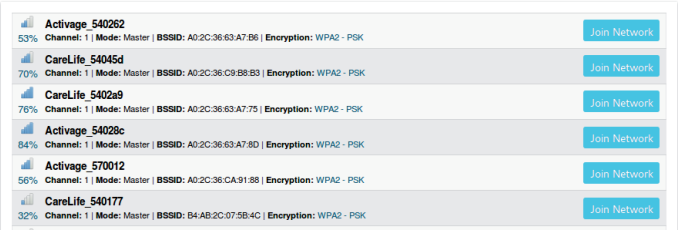


Escaneo de las redes Wi-Fi

Al escanear se muestran todos los AP disponibles.

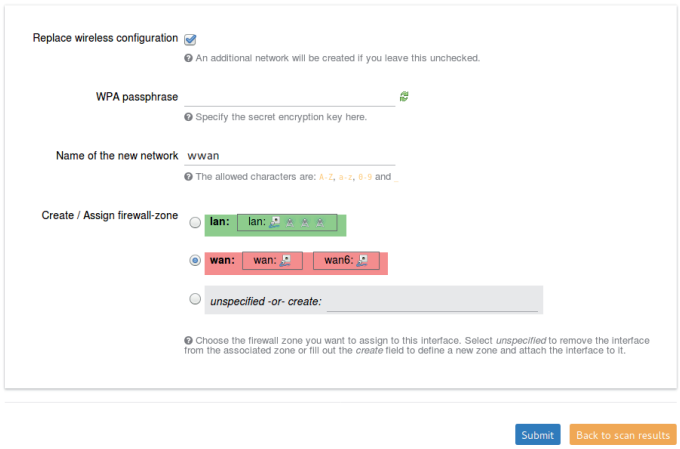
ES

Join Network: Wireless Scan



- **Join network**: Este botón permite conectarse a la red seleccionada.

Join Network: Settings

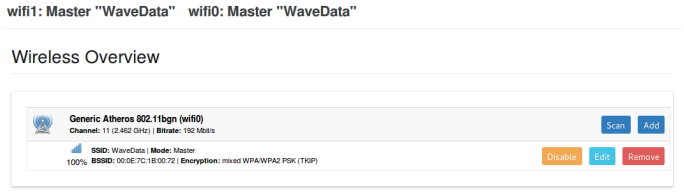


Cuando se crea un nuevo VAP para unirse a una red Wi-Fi, por defecto se crea una nueva red llamada **wwan**. La red **wwan** está preconfigurada como una interfaz bridge y creará un bridge llamado br-wwan, con el nuevo VAP como única interfaz física.

El VAP creado en modo STA se unirá al AP seleccionado:

- **Replace wireless configuration**: Cuando crea el VAP, en modo STA VAP, se borran todos los VAP creados en el dispositivo y el nuevo VAP será el único VAP disponible. Utilice esta opción con cuidado puesto que todos los VAPs en modo AP creados por defecto serán eliminados.
- **Create/Assign Firewall zone**: Asigna una zona del firewall a la red **wwan** creada.

Un método alternativo para crear un nuevo VAP en modo STA, al margen del proceso de escaneo, es utilizar el botón **Add** disponible en cada uno de los interfaces Radio especificando los parámetros adecuados: SSID, WPA Key, etc...

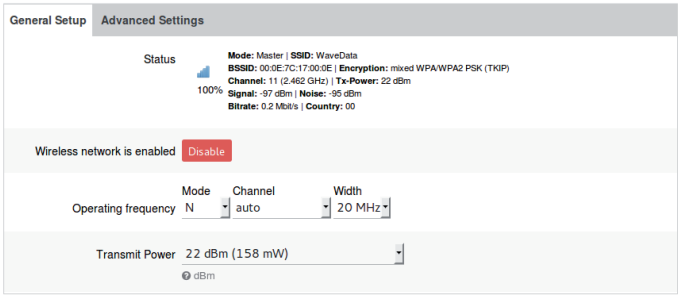


Editando la configuración de la interfaz Wi-Fi

Haga click en el botón **Edit** para configurar la interfaz VAP.

La sección **Device Configuration** configura el dispositivo radio (2,4G o 5G) y afecta a todos los VAPs del dispositivo radio.

Device Configuration

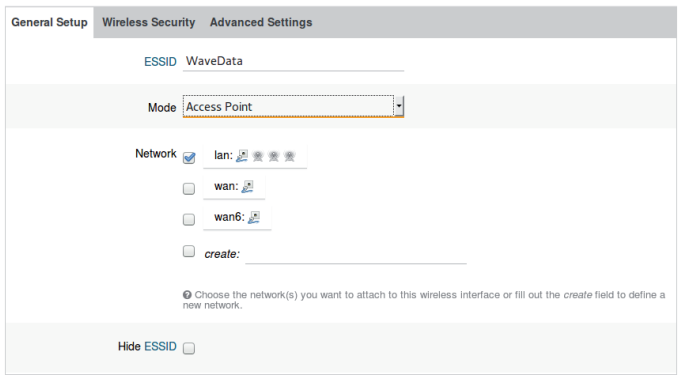


- **Mode**: Seleccione el modo 802.11/a/b/g/n/ac
- **Channel**: Canal del dispositivo Wi-Fi. auto permite que el driver escoja el mejor canal disponible.
- **Width**: Ancho de banda del canal Wi-Fi 20/40/80 MHz.
- **Power**: Potencia de transmisión del canal Wi-Fi.

La sección **Interface Configuration** configura los parámetros especificos del VAP para lo cual proporciona tres pestañas.

VAP General Setup

Interface Configuration

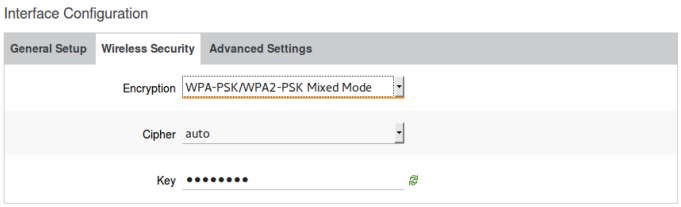


- **ESSID**: En el modo AP, el SSID identifica al AP en una red Wi-Fi y será emitido por el dispositivo radio. Para el modo STA la SSID indica la red Wi-Fi a la que nos queremos conectar.
- **Network**: Seleccione la interfaz a la que el VAP pertenecerá. Este network debe ser siempre una interfaz en modo bridge.

Modos de un VAP

- **Access Point**: El modo del VAP es AP. El dispositivo Wi-Fi emite el SSID en el aire y espera por conexiones de estaciones Wi-Fi.
- **Access Point (WDS)**: El modo del VAP es AP con WDS (Wireless distribution System) habilitado. WDS habilita Ethernet sobre Wi-Fi, es una extensión del protocolo 802.11 que permite la propagación de paquetes Wi-Fi sobre ethernet, insertando en el paquete la MAC de origen y destino del paquete ethernet. Esto permite que un VAP sea miembro de un bridge y propague tráfico por otros miembros del bridge que son puertos ethernet. Es el modo por defecto. Para que funcione adecuadamente el STA tiene que tener esta capacidad también.
- **Client**: El modo VAP es STA (Managed mode) e intenta conectarse con el mejor AP que se corresponda con el SSID.
- **Client (WDS)**: El modo VAP es STA con WDS habilitado e intenta conectarse con el mejor AP que se corresponda con el SSID. WDS habilita Ethernet sobre Wi-Fi. Si un VAP es miembro de un bridge y necesita propagar tráfico sobre una red Ethernet habilite esta opción.

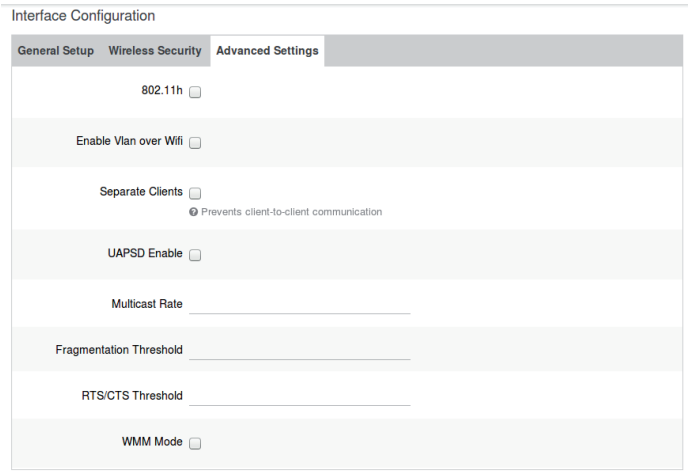
Configuración de Seguridad en un VAP



- **Encryption**: Los siguientes modos están disponibles: Open, WEP, WPA/WPA2-PSK o WPA-EAP (802.1X).
- **Cipher**: Establece el cifrado del VAP: WPA-TKIP, WPA-AES o auto para soportar ambos.
- **Key**: Contraseña para la encriptación WEP o WPA. Las contraseñas WEP deben tener una longitud ascii de 6 o 13 caracteres.

Opciones Avanzadas de un VAP

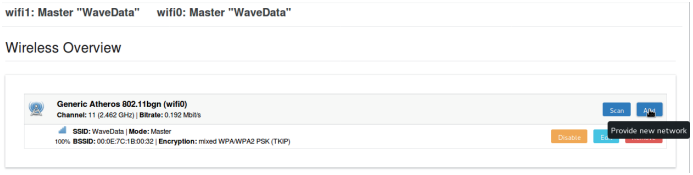
Para cada VAP se proporcionan una serie de opciones avanzadas que habilitan características adicionales:



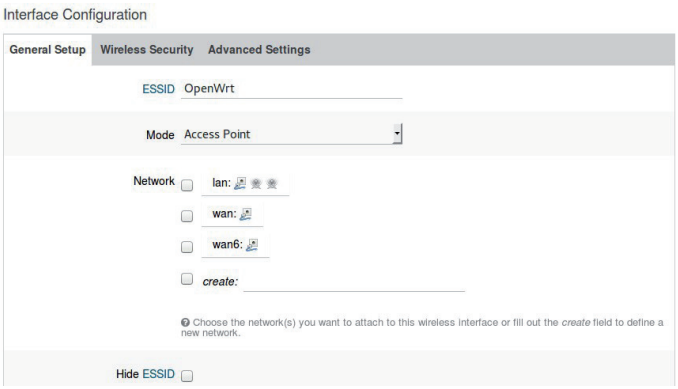
- **802.1h**: Habilita la extensión IEEE 802.1h incluida en el estándar IEEE 802.11 (Spectrum and Transmit Power Management Extensions). Estas extensiones que sólo aplican a la interfaz 5G permiten detectar y resolver problemas de interferencia con las emisiones de satélites o de radares cercanos en la banda de 5GHz. El estándar define dos mecanismos denominados Dynamic Frequency Selection (DFS) y Transmit Power Control (TPC) para los modos IEEE 802.11a. Esta extensión ha sido integrada el estándar IEEE 802.11-2007.
- **Enable VLAN over Wi-Fi**: Habilita el soporte para transmitir tags VLAN sobre la Wi-Fi. Los clientes (STA) conectados al AP también deben tener soporte para la recepción/emisión de tags VLAN sobre Wi-Fi, de forma que el tag se conserve para su recepción en una interfaz VLAN en el dispositivo cliente.
- **Separate Clients**: Impide la comunicación entre clientes en un AP. Por defecto esta opción está desactivada.
- **UAPSD**: Esta opción está basada en el estándar IEEE 802.11e que define un nuevo mecanismo que permite reducir el consumo energético. APSD (automatic power save delivery) proporciona dos mecanismos para este ahorro energético: 'scheduled APSD' (S-APSD) y 'unscheduled APSD' (U-APSD). Básicamente APSD habilita en un AP la acumulación y transmisión del múltiples tramas a un STA de forma conjunta, estableciendo periodos de servicio (service) y periodos de baja actividad (standby). Esto permite que los STA conectados ahorren batería puesto que reciben todos los datos de una sola vez, además conocen de antemano cuando el AP enviará los datos.
- **WMM Mode**: Habilita la extensión WMM (Wi-Fi Multimedia) basado en el estándar IEEE 802.11e. Esta extensión proporciona parámetros de QoS (Quality of service) para las redes IEEE 802.11. WMM prioriza el trafico de acuerdo a cuatro categorías (Access Categories, AC): Voz (AC_VO), Video (AC_VI), best effort (AC_BE), y background (AC_BK). Sin embargo WMM, no soporta un tasa garantizada. Esta opción de WMM es adecuada para aplicaciones que tengan como requisitos ciertos parámetros de QoS como Voz sobre IP (VoIP) o Voz sobre Wi-Fi (VoWLAN).

Añadiendo interfaces VAP

Haga click en el Botón ***Add*** para añadir un nuevo VAP a la interfaz Wi-Fi.



La Web ofrece la misma interfaz que cuando se edita un VAP, pero las opciones son rellenadas con valores predefinidos. Configure el nuevo VAP según sus necesidades.



Interfaces VLAN en el Switch

El WaveData dispone de un switch interno conectado a los puertos ethernet. Vaya a ***Network*** > ***Switch*** para configurar las interfaces VLAN en el switch interno del dispositivo.

Por defecto, el switch tiene las siguientes asignaciones a puertos externos:

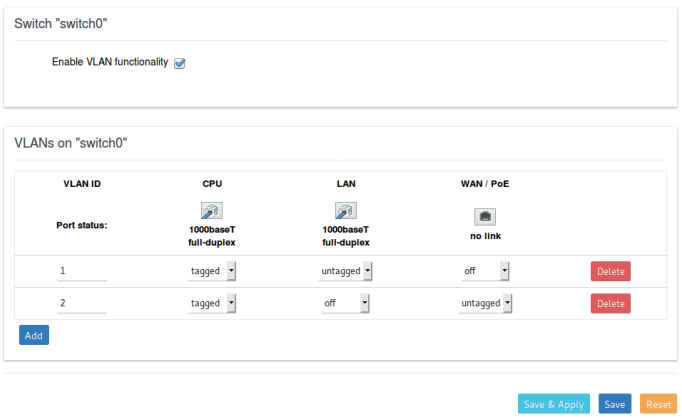
- La interfaz WAN/SFP es el Puerto 5.
- La interfaz LAN es el Puerto 4.
- El puerto CPU conectado directamente al SoC es el puerto 0. El switch envía/recibe todo el trafico del SoC a través de este puerto.

La configuración por defecto del dispositivo crea dos VLAN en el Switch:

VLAN2: Untagged para el puerto 5 (WAN) y tagged para el puerto 0 (CPU). El switch recibe trafico untagged del puerto WAN y lo envía con VLAN2 al SoC.

VLAN1: Untagged para el Puerto 4 (LAN) y tagged para el puerto 0 (CPU). El switch recibe trafico untagged del puerto LAN y lo envía con VLAN1 al SoC.

El comportamiento del switch es en modo estricto, esto es, tan solo las VLAN definidas en el software son reconocidas por el switch. Inicialmente VLAN1 y VLAN2. Otras VLAN no son admitidas por el switch.



Para sincronizarse con el switch, el driver Ethernet del SoC es configurado adecuadamente. El comportamiento del driver Ethernet es el siguiente:

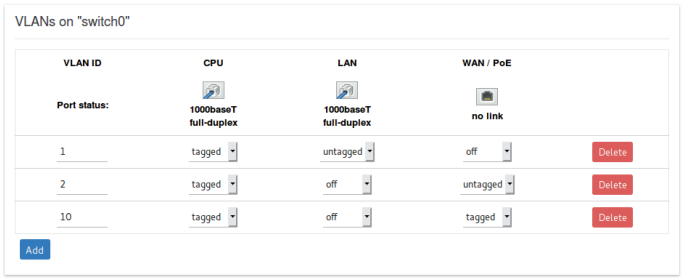
- El driver ethernet crea dos dispositivos: eth0 y eth1.
- El driver conoce, mediante una cabecera insertada por el switch, de que puerto proviene un paquete.
- Todo el trafico del switch es recibido/transmitido a través del Puerto 0 (CPU Port)
- Propaga el trafico recibido (por el puerto 0) procedente del puerto 5 (WAN) a la interfaz eth0 y viceversa.
- Propaga el trafico recibido (por el puerto 0) procedente del puerto 4 (LAN) a la interfaz eth1 y viceversa.

Creación de VLAN para tageado del trafico Wi-Fi

El usuario puede añadir más VLAN según las necesidades de la red. En el siguiente ejemplo se muestra como añadir el tag VLAN 10 al trafico procedente de las interfaces Wi-Fi antes de propagar el trafico por la WAN.

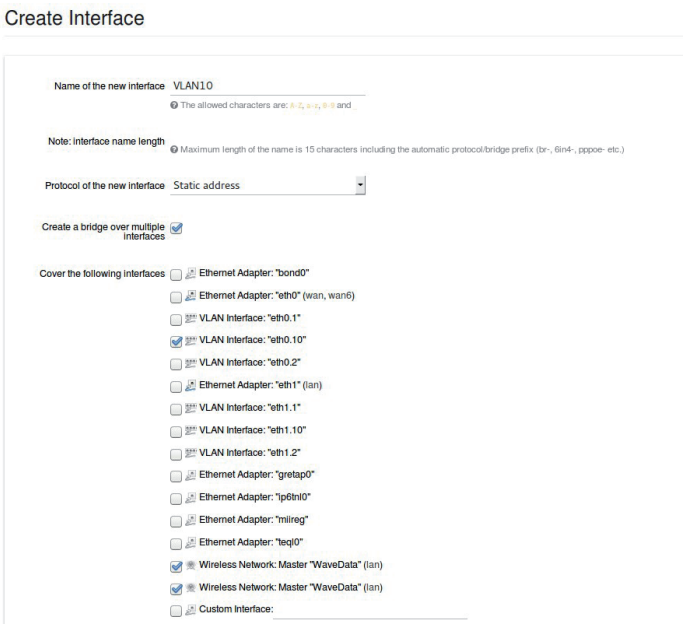
La captura muestra como crear una nueva VLAN 10 en el puerto WAN (Puerto 5) y propagar el trafico tageado a la CPU.

Esta configuración también crea una nueva interfaz VLAN, llamada eth0.10, en el sistema.

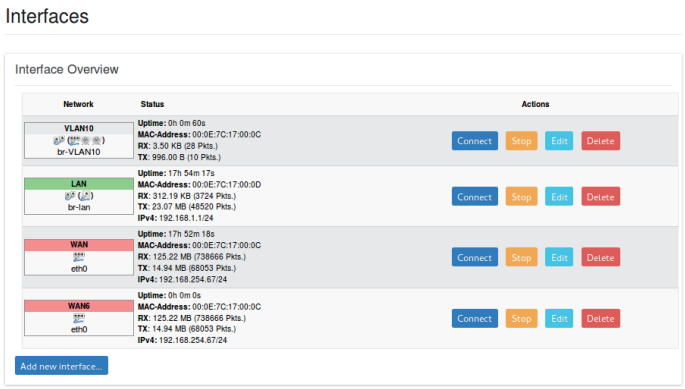


Para gestionar la interfaz VLAN eth0.10, necesita crear una nueva interfaz en el sistema, llamada VLAN10, como un bridge.

- Vaya a ***Network*** > ***Interfaces*** and haga click en el botón **Add**.
- Establezca VLAN10 como el nombre de su nueva interfaz.
- Seleccione '***Create bridge over multiple interfaces'*** y añade la interfaz VLAN eth0.10 y los Wi-Fi VAP como miembro de la nueva red VLAN10.



Ahora la interfaz VLAN10 propaga el trafico Wi-Fi desde los VAP hacia el puerto WAN insertando el tag VLAN10.

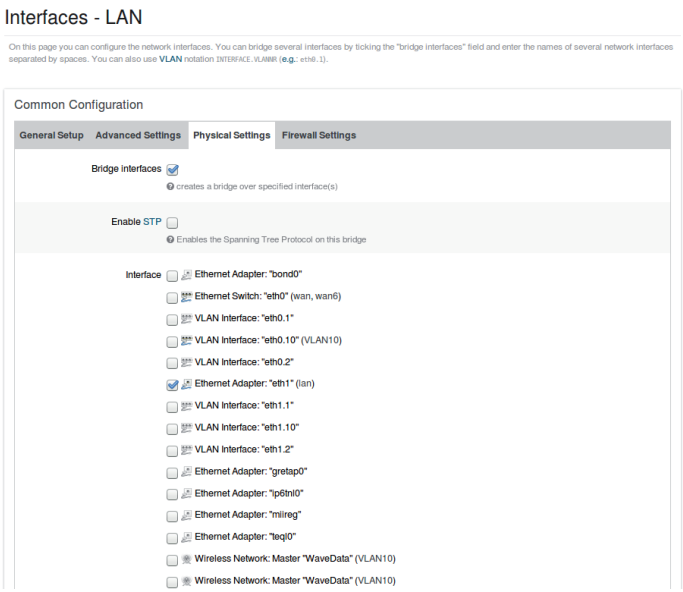


Puede utilizar los VAP por defecto del WaveData o crear nuevos VAP.

Por defecto, los VAP son miembros de la interfaz LAN. Para que la nueva configuración surta efecto es necesario eliminar los VAP de la interfaz LAN donde están asignados por defecto

Vaya a ***Network*** > ***Interfaces*** > ***LAN*** > ***Edit*** > ***Physical Interfaces*** y elimine los VAP Wi-Fi de la LAN.

Ahora, los VAP Wi-Fi está asociados sólo a la interfaz VLAN10.

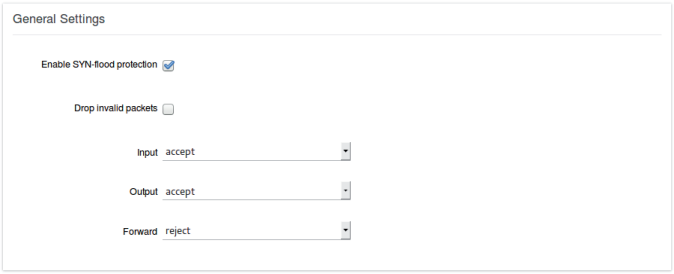


Configuración del Firewall

Vaya a ***Network*** > ***Firewall*** para configurar el firewall.

Cada zona tiene tres tipos de tráfico:

- **Input**: El tráfico recibido desde la una interfaz con destino a la CPU. El acceso local a servicios como SSH o Web pertenece a esta categoría.
- **Output**: El tráfico enviado desde la CPU. La respuesta a peticiones de servicio SSH o Web pertenece a esta categoría.
- **Forward**: El tráfico enrutado de una zona a otra. Por ejemplo, el tráfico que intercambiado entre las zonas LAN <==> WAN.



Normalmente cuando un paquete es recibido desde una interfaz esta es cubierta por la zona que tiene asignada. Si recibimos un paquete desde una interfaz que no tiene ninguna zona asignada, se aplican las políticas por defecto. Vaya a ***Firewall*** > ***Zone Settings***, para modificar dichas políticas.

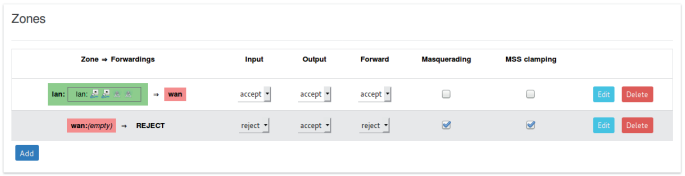
Por defecto, el firewall define dos zonas:

- **Zona LAN**: La política por defecto para esta zona es aceptar todo el trafico de la CPU (Input, Output y Forward).
- **Zona WAN**: La política por defecto de esta zona es aceptar sólo el tráfico Output. El trafico Input y forwarding es rechazado.

Sobre esta política se añaden excepciones definidas en las reglas de Trafico (Traffic Rules, como la apertura de los servicios SSH y Web), Propagación de puertos (Port Forwarding) y propagación entre zonas (interzone forwarding).

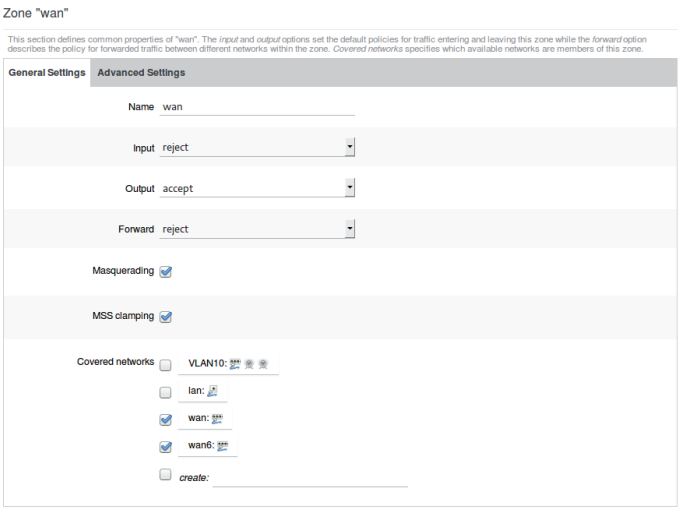
En la zona WAN, puesto que está expuesta al dominio público, se activa el Masquerading (también conocido como NAT) y MSS Clamping.

En este caso, como se muestra en la captura, está permitido la comunicación entre zonas LAN => WAN.

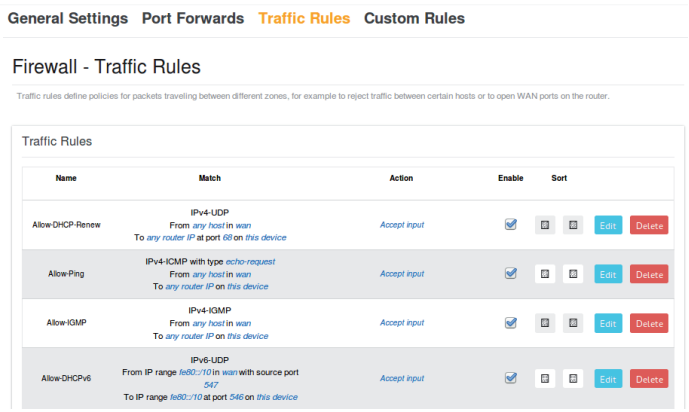


Zona WAN

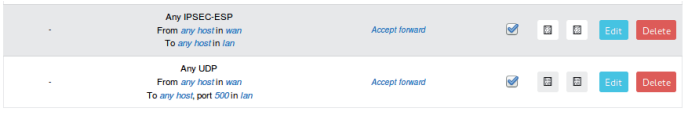
La zona WAN define la política y reglas de filtrado de las interfaces WAN y WAN6.



- La política por defecto de la WAN es rechazar el trafico de entrada (para evitar ataques de seguridad a los servicios del router).
- La propagación hacia zonas desconocidas es rechazada, pero puede usar la configuración del propagación entre zonas (Inter-Zone Forwarding) para habilitar la propagación de/hacia otras zonas.
- Aunque la política del trafico de entrada es rechazar el trafico, esta política es modificada por la definición de reglas específicas. La siguiente captura muestra la definición de reglas que afectan al trafico de entrada de la zona WAN, permitiendo la realización de peticiones ICMP y DHCP.



- Aunque la política de propagación (forward) para la zona WAN es bloquear el trafico. Existen reglas de propagación de tráfico o propagación de puertos que son excepciones al bloqueo y permite la propagación. En la captura se muestra como el trafico IPSec puede se transmitido entre las zonas WAN => LAN.



- Inter-zone forwarding: El paquete es propagado entre zonas si está habilitado para atravesar las zonas de origen => destino. Si el paquete pertenece a una conexión activa (perteneciente a una conexión válida con estados ESTABLISHED o RELATED en el gestor de conexiones, Connection tracking) no necesita ser habilitado, puesto que por defecto se admite su paso. En general el tráfico entre zonas WAN => LAN se corresponde con tráfico relacionado con una conexión activa.

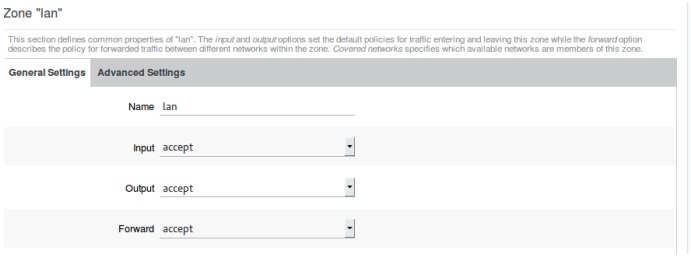
  Sin embargo, los paquetes iniciales LAN => WAN sí necesitan ser habilitados para su propagación, puesto que las conexiones son iniciadas desde la LAN y todavía no son conexiones activas.



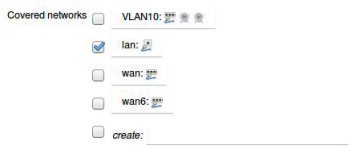
Zona LAN

La zona LAN cubre todo el tráfico desde y hacia las interfaces locales, en este caso la interfaz etiquetada como LAN en el dispositivo.

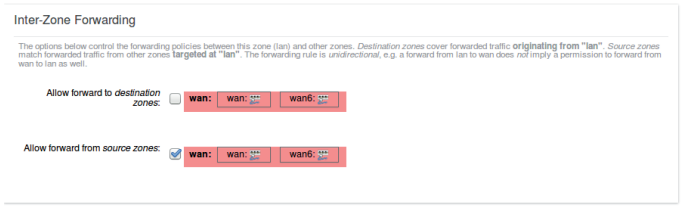
- Cuando el router recibe un paquete desde la LAN, la política por defecto es aceptar la entrada y salida de dicho paquete hacia la CPU. De esta forma los hosts locales tienen acceso a los servicios del dispositivo como SSH o Web sin restricciones.
- Cuando el router recibe un paquetes desde la LAN y con destino a otras zonas, la política por defecto es rechazar el tráfico con destino a zonas desconocidas. Use la opción Inter-zone forwarding para habilitar el tráfico desde/hacia otras zonas, o añada reglas especificas para permitir el tráfico de un determinado tipo.



- La zona LAN cubre el trafico de la red LAN.

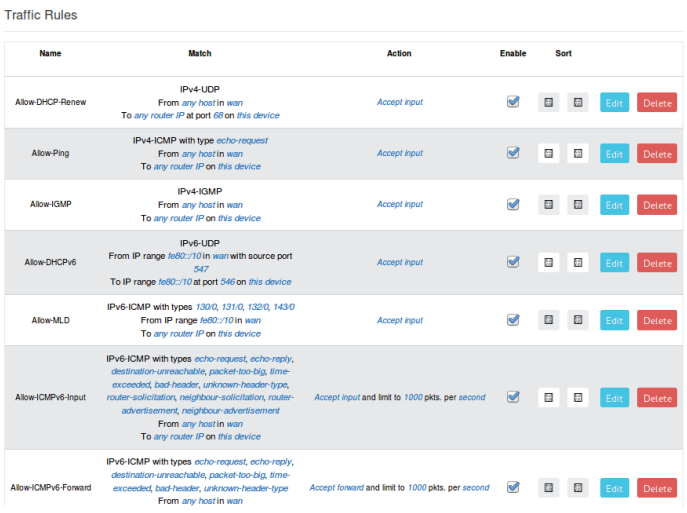


- La zona LAN acepta el trafico desde la WAN si pertenece a una conexión activa (con estados ESTABLISHED o RELATED en el gestor de conexiones, Connection tracking) o cumple alguna regla de propagación de puertos. La zona WAN tiene como política rechazar el tráfico que proviene de zonas desconocidas, por lo que tenemos que habilitar la que acepte el trafico procedente de la LAN.

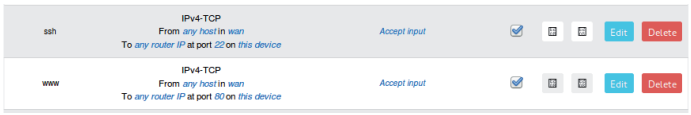


Reglas de Tráfico

Por defecto, el dispositivo viene configurado con algunas reglas predefinidas. Las siguientes reglas permiten a la WAN aceptar el trafico UpnP, DHCP e ICMP. Esto permite la detección PlugAndPlay o la realización de un ping al dispositivo.



También se añaden otras reglas para permitir la conexión hacia la interfaz Web o el servicio SSH.

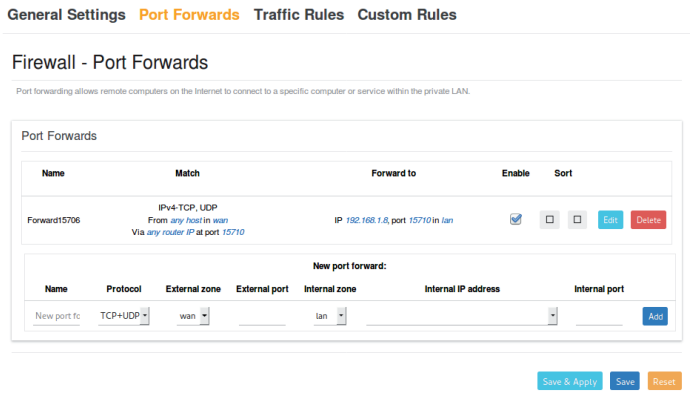


Propagación de puertos

ES

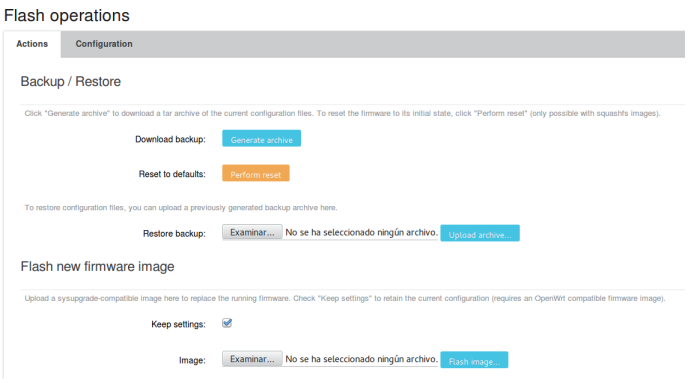
La propagación de puertos (Port forwarding) permite propagar el tráfico entre zonas cuando este cumple la condición de operar en un determinado puerto TCP o UDP. Permite propagar el tráfico desde un host en la zona WAN a un servidor local en la LAN.

El siguiente ejemplo permite que las peticiones realizadas desde la zona WAN en el puerto 15710 sean propagadas al host 192.168.1.8. Los hosts externos de la zona WAN pueden usar el puerto 15710 del router para conectarse host local 192.168.1.8:15710 en la zona LAN.



Actualización de Firmware y Configuración

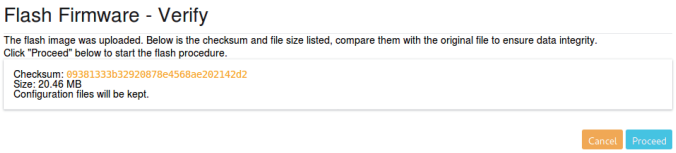
Vaya a ***System>Backup/Flash Firmware*** para actualizar el firmware y la configuración. Abajo se muestra una captura de la interfaz de actualización.



Las operaciones de actualización incluyen:

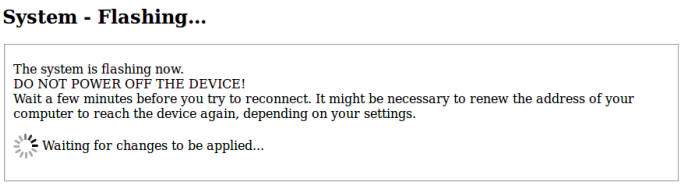
- **Download Backup:** Salva la configuración del dispositivo en un archivo comprimido.
- **Reset to Defaults**: Establece al configuración por defecto y realiza un reboot del dispositivo.
- **Restore Backup**: Actualiza la configuración del dispositivo con un backup previo.
- **Upgrade Firmware**: Actualiza el kernel y el sistema de archivos del dispositivo a la ultima versión. Las versiones de firmware son proporcionadas por Televes. Active la opción Keep Settings para conservar la configuración actual del dispositivo tras la actualización (activado por defecto).

La actualización del firmware es realizado en dos etapas, la primera verifica que el firmware es válido.



Tras verificar su validez, muestra un checksum del archivo. Verifique que dicho checksum coincide con el archivo MD5 que acompaña al firmware.

Haga click en el botón **Proceed** para actualizar el dispositivo.



Lista de acrónimos

ACRÓNIMO	SIGNIFICADO
AES-CCMP	Advanced Encryption Standard-Counter. Cipher Mode Protocol
AES-GCMP	Advanced Encryption Standard-Counter.
AP	Wireless access point, conocido por las siglas WAP o AP
Auto-MDIX	Auto Medium Dependent Interface crossover
BPSK	Binary phase-shift keying
CPU	Central Processing Unit
DCHP	Dynamic Host Configuration Protocol
DDR	Double Data Rate Synchronous Dynamic Random-Access Memory
DNS	Domain Name System
eMMC	embedded MultiMediaCard
GPRS	General Packet Radio Service
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
MIMO	Multiple-Input and Multiple-Output
MLD	Multicast Listener Discovery
MU-MIMO	Multi-user MIMO
NAT	Network Address Translation
NTP	Network time protocol
OFDM	Orthogonal Frequency Division Multiplexing
PAP/CHAP	Password Authentication Protocol /Challenge Handshake Authentication Protocol
PoE	Power over Ethernet
PPPoE	Point-to-Point Protocol over Ethernet
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
QPSK	Quadrature Phase-Shift Keying
RGB	Red Green Blue
RRM	Radio Resource Management
SFP	Small Form-factor Pluggable
SSH	Secure Shell
SSID	Service Set Identifier
STA	STATION.A client device in an 802.11 (Wi-Fi) wireless network such as a computer, laptop
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
UDP	User Datagram Protocol
UPNP	Universal Plug and Play
USB	Universal Serial Bus
VAP	Virtual Access Point
VLAN	Virtual LAN
WAN	Wide Area Network
WDS	Wireless distribution System
WEP	Wired Equivalent Privacy
WLAN	Wireless LAN
WMM	Wi-Fi Multimedia
WPA-EAP	Wi-Fi Protected Access - Protected Extensible Authentication Protocol
WPA-PSK	Wi-Fi Protected Access - Pre-Shared Key
WPS	Wi-Fi Protected Setup

Características WaveData

CPU	Procesador	QCA IPQ
Memoria	DDR, NOR, eMMC	512MB DDR, 32MB NOR, 4GBytes eMMC
Interfaces	Alimentación, Ethernet, USB	1x USB 3.0 1x Jack alimentación 12-24Vdc. 12V/2A 1x RJ45 Gigabit (10/100/1000). Auto MDI-X 1x PoE RJ45 Gigabit Ethernet 802.11af/at. Auto MDI-X (sólo ref.769001) 1x SFP IEEE 1000BASE-X (sólo ref. 769002)
Wireless	Interfaces	Interfaces 2,4G y 5G WLAN 1x 2,4G IEEE 802.11nbg 2x2 MIMO 1x 5G IEEE 802.11nac Wave2 5G 2x2 MIMO
	Potencia Transmisión	2,4GHz 23.5dBm @ MCS0 HT20 16.5dBm @ MCS9 HT40 5GHz 22 dBm @ MCS0 HT20 15.5 dBm @ MCS9 HT40 14.5 dBm @ MCS9 HT80
	Máxima Tasa física Wireless	1.73 Gbps max. 2x2 On-Board 5GHz radio, hasta 867 Mbps tasa física 2x2 On-Board 2,4GHz radio, hasta 300 Mbps tasa física
	MIMO	2,4GHz 2x2 y 5GHz 2x2
	Rango Frecuencias	2.412 - 2.472 GHz y 5.180 - 5.825GHz
	Ancho de Banda de Canal	5GHz radio: 20/40/80 MHz 2,4GHz radio: 5/10/20/40 MHz
	Modulaciones	OFDM: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM
	Antenas	4x Antenas para Doble Banda 2,4G/5G
	Ganancia Antena	2,4GHz +4dBi, 5GHz +4dBi
	Seguridad	Encriptación: Open, WEP, WPA-PSK, 802.1X WPA-EAP Cifrado: TKIP, AES-CCMP, AES-GCMP
Leds	Led RGB	Led Tri-color para indicar el estado del dispositivo. • Verde: Unidad OK y Wi-Fi funcionando. • Azul: Unidad OK y Wi-Fi apagado. • Naranja: Unidad OK y modo myNETWi-Fi (max 10dBm). • Parpadeo Azul: Actualización del sistema en curso.
Botones	Botón Reset	Botón reseteo Hardware
	Botón WPS/ Configuración	• 0-3 segundos: WPS • > 3 segundos: Configuración por defecto
	Interruptor MyNETWi-Fi	Tri-estado: Apagado, Normal (22dBm), myNETWi-Fi (10dBm).
Acceso Dispositivo	Dirección IP	IP por defecto: 169.254.1.254
	Cuenta Login	Usuario: root, Contraseña: 76Wave90Data01
Sistema Operativo	Linux/OpenWRT	Linux kernel 4.4.60, QCA QSDK basado en OpenWRT CC 15.05
Alimentación	Adaptador Jack	1x conector jack DC: 12-24 V. 12V/2A
	Alimentación sobre Ethernet	PoE Pasivo 36-56V, IEEE 802.3af/at
	Max. Consumo Alimentación	2x Wi-Fi Interfaces: max. 7W
Rango Temperatura	ºC	-5 ... +45 ° C
Dimensiones, Peso	mm, gr	146 x 146 x 43 mm 300 g

- Por la presente, Televés S.A.U. declara que el tipo de equipo radioeléctrico Wave Data es conforme con la Directiva 2014/53/UE. El texto completo de la declaración UE de conformidad está disponible en la dirección Internet siguiente: https://doc.televes.com.

European technology **Made in EUrope**

Fabricante: **Televes S.A.U.** Rúa B. de Conxo, 17 - 15706 Santiago de Compostela, A Coruña. Spain www.televes.com

769001, 769002_001_ES