Trabajo Fin de Grado
Grado en Ingeniería de las Tecnologías de Telecomunicación

Diseño de una red Mesh de UAVs para proporcionar servicios de comunicaciones

Autor: Santiago Limón de la Rosa

Tutor: Daniel Gutiérrez Reina

Departamento de Ingeniería electrónica
Escuela Técnica Superior de Ingeniería
Universidad de Sevilla

Sevilla, 2017

Trabajo Fin de Grado
Grado en Ingeniería de las Teconlogías de Telecomunicación

Diseño de una red Mesh de UAVs para proporcionar servicios de comunicaciones

Autor:
Santiago Limón de la Rosa

Tutor:
Daniel Gutiérrez Reina
Doctor Ingeniero en Electrónica

Departamento de Ingeniería Electrónica
Escuela Técnica Superior de Ingeniería
Universidad de Sevilla
Sevilla, 2017

Trabajo Fin de Grado: Diseño de una red Mesh de UAVs para proporcionar servicios de comunicaciones

Autor: Santiago Limón de la Rosa

Tutor: Daniel Gutiérrez Reina

El tribunal nombrado para juzgar el Proyecto arriba indicado, compuesto por los siguientes miembros:

Presidente:

Vocales:

Secretario:

Acuerdan otorgarle la calificación de:

Sevilla, 2017

El Secretario del Tribunal

A mi familia

A mis compañeros

Agradecimientos

A mis padres, por su apoyo incondicional.

A mi hermana María José, por animarme en los peores momentos.

A mi hermano Manuel Jesús, por no dudar nunca de mí y recordarme siempre lo que valgo.

A todos aquellos Rafas, Migues, Diegos… que el pasar de los años me obligó a quitarles su sobrenombre "etsi" de mi agenda del móvil, para ser solo Rafa, Migue o Diego; pues sin ellos el camino no hubiese sido igual.

A mi tutor, Daniel Gutierrez, por confiar en mí y por facilitarme todos los recursos necesarios para la realización de este trabajo.

Santiago Limón de la Rosa

Sevilla, 2017

Resumen

En este proyecto, se ha trabajado en el despliegue de una red mesh, compuesta por UAVs que acturán como nodos de la propia red y a su vez, como puntos de accesos, capaces de proporcionar servicios de comunicaciones vía IP a los clientes que se conecten a ellos.

Al estar formada por UAVS que cambiarán de localización física constantemente, esta red tiene la peculiaridad de que poder adoptar distintas topologías de red de forma automática.

Con esta labor de investigación se ha creado una infraestructura que posibilite a los nodos de la red la capacidad de autoenrutar dinámicamente su tráfico y de manera trasparente a los clientes.

Abstract

In this project, we have worked on the deployment of a mesh network, composed of UAVs that act as nodes of the network itself and as access points, capable of providing IP communications services to the clients that connect to them.

Being formed by UAVS that will constantly change physical location, this network has the peculiarity of being able to adopt different network topologies automatically.

This research has created an infrastructure that enables the nodes of the network the ability to dynamically route their traffic and transparently to customers.

Índice

Índice de Figuras

1. MOTIVACIÓN Y OBJETIVOS

1.1 Motivación

Existen muchas motivaciones para realizar el presente trabajo fin de grado tanto personal como técnicas. Entre ellas se destacan las siguientes:

- Se prevé que el número de aplicaciones comerciales basadas en UAV aumente de forma vertiginosa en los próximos años. Entre las aplicaciones posibles, parece lógico pensar en aplicaciones cooperativas entre distintos UAVs que formen una red de comunicaciones.
- Poder evaluar la viabilidad y utilidad de una red comunicaciones móvil basada en dispositivos UAVs para proporcionar servicio de comunicaciones a dispositivos en tierra.

La revolución de los drones está transformando a empresas de todos los sectores de actividad, desde sectores como el del transporte y la agricultura, hasta la industria cinematográfica. El incipiente mercado relacionado con el uso de los drones está generando grandes oportunidades de negocio, y cada vez son más los que buscan beneficiarse de la implantación de este tipo de tecnología. Cada día encontramos más aplicaciones y nuevas funcionalidades que pueden satisfacer estos drones.

Llegados a este punto, podemos plantearnos la necesidad de operar no sólo con un único dron, sino con un conjunto de ellos formando una red de comunicaciones, para acometer una tarea cooperativa de forma más rápida o más eficaz. En este trabajo queremos servirnos de un conjunto de drones para llevar a cabo la tarea de proporcionar un servicio de comunicación inalámbrico a los equipos que se encuentren a su alcance. Para ello será necesario la implementación de una red que interconecte nuestros drones y los sincronice para lograr cumplir su tarea.

Con esta labor de investigación, pretendemos considerar y evaluar la utilidad que pueda tener una red móvil integrada por UAVs, capaz de proporcionar servicios de comunicaciones de forma inalámbrica a los diversos equipos que se sitúen en la superficie terrestre. Con lo de red móvil nos referimos, a una red en movilidad, cuyos nodos sean los propios drones que estarán en el aire y en constante movimiento. Esta red contará con múltiples puntos de accesos que se encargarán de dar cobertura inalámbrica a la zona que sobrevuelen en ese instante.

La idea es que la red de comunicaciones formada por los drones funcione de forma parecida a la red celular de telefonía móvil. Los drones funcionarían como torres de comunicaciones y la comunicación entre las distintas torres (drones en nuestro caso), debe ser transparente para los usuarios.

1.2 Objetivos

Como principales objetivos de este trabajo fin de grado se plantean los siguientes puntos:

- Diseño y evaluación de una red mesh para UAVs basado en dispositivos raspberry PI.
- Comparar distintos tipos de diseño de red.
- Elección y puesta en marcha de los sistemas operativos y distintos procedimientos que nos permitan la implementación de la red propuesta.

El objetivo primordial será el diseño y posterior evaluación de una red Mesh compuesta por un conjunto dispositivos raspberry PI que funcionarán como routers y puntos de acceso conectados entre sí, con el

propósito de proporcionar un servicio de comunicaciones inalámbrico a los distintos equipos que se encuentren a su alcance. Estos dispositivos raspberrys PI serán los que se sitúen sobre los UAVs.

Como objetivo previo al diseño e implementación de nuestra red, tenemos también el de comparar los distintos tipos de redes, así como las topologías que estos pueden adoptar, buscando la que más se adecue a nuestro escenario de investigación. Para ello, discutiremos entre los distintos tipos de redes existentes, profundizando en el tipo de red escogido para proporcionar los servicios de comunicaciones de nuestra red móvil, por las ventajas y beneficios que nos puede aportar: La red mesh.

Otro punto importante será el de cómo implementar esta red sobre nuestros dispositivos raspberry Pi. Deberemos buscar y estudiar las distintas opciones que nos permitan llevar a cabo nuestro trabajo. En este apartado deberemos seleccionar el sistema operativo sobre el que vamos a operar, así como los procedimientos y la lógica necesaria para llegar a la viabilidad de nuestro objetivo.

2. INTRODUCCIÓN: REDES DE COMUNICACIÓN PARA UAVS

2.1 Estado actual de las redes Mesh para ofercer servicios de comunicaciones

La integración de las redes de comunicaciones libres en lugares o edificios públicos, se ha convertido en una necesidad prioritaria en el mundo actual. Ya no solo encontramos este tipo de redes en instituciones públicas o gubernamentales, o en oficinas y lugares de trabajo. Cada vez son más las ciudades que deciden incorporar redes WiFi libres en el centro, en los parques, en las playas, en lugares de ocio… para mejorar la calidad de vida de la ciudadanía.

De aquí parte una de las iniciativas más interesante que ofrece el mercado de las redes mesh: **LibreMesh** [1].

LibreMesh es una iniciativa llevada adelante por miembros de redes comunitarias de diferentes continentes que se organizan para unificar esfuerzos en el desarrollo de herramientas útiles para facilitar el despliegue de Redes Libres para cualquier comunidad del mundo.

La herramienta principal es el firmware LibreMesh: basado en **OpenWrt** [2] y **LEDE** [3] estandariza la creación de comunidades WiFi y provee de roaming a las comunidades ya existentes.

Esta herramienta ha marcado el punto de partida del camino a seguir en la elaboración de este trabajo de fin de grado.

Otras herramientas son:

- Librenet6: un mesh tunnel broker para proveer IPv6 globales a las redes libres
- Chef: creador de firmwares a medida para comunidades
- Libremap (en colaboración con Freifunk): representación de nodos según su ubicación geográfica con actualización de calidades de enlace a tiempo real.

Las herramientas se pueden utilizar por separado o todas juntas, actualmente se está trabajando en la integración automatizada del uso de todas ellas.

Este proyecto nació como un esfuezo para fusionar algunos proyectos de firmware preexistentes:

- AlterMesh (de AlterMundi, Argentina)
- qMp (de guifi.net, Catalunya)
- eigenNet (de eigenLab, Ninux, Italia)

Algunas de las organizaciones que apoyan están apoyando estos proyectos son: the Free Network Foundation (de USA) y the Guifi.net Foundation (de Catalunya). Cualquier persona puede colaborar poniendose en contacto con los desarrolladores.

Lo habitual cuando hablamos del despliegue en un entorno al aire libre de este tipo de rede, es utilizar edificios o inmuebles públicos, torretas de comunicaciones, señales de tráfico e incluso árboles, para ubicar los puntos de acceso que da cobertura a este tipo de redes.

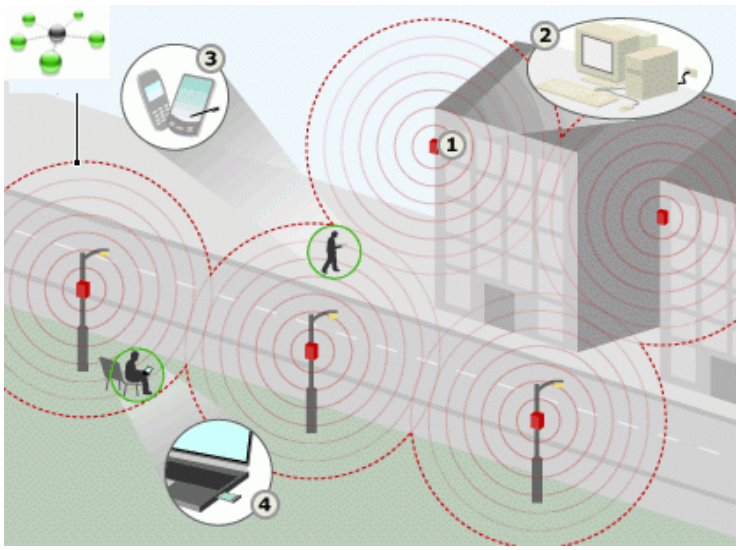


Figura 1. Red mesh en una ciudad

En este trabajo, nos hemos planteado la posibilidad de llevar a cabo este despliegue, pero con la diferencia de que no ubicaremos nuestros puntos de acceso en un emplazamiento fijo como viene siendo habitual, sino que los ubicaremos sobre vehiculos aéreos no tripulados, de aquí en adelante UAV.

2.2 Estado actual de las redes de comunicación para UAVs

En el mundo de las comuniaciones entre UAVS, la mayoría de las redes que se utilizan sirven para realizar tareas de sincronización para lograr maniobrar de forma conjunta, tareas que situado en tierra, tareas designadas habitualmente desde un equipo externo a la red de UAVs.

Podemos encontrar algunas publicaciones sobre estudios que se han realizado sobre la idea de ofercer una red de comunicaciones por medio de UAVs.

Una de estas investigaciones que puede resultarnos interesante es la siguiente investigación del Advanced Mobile Network Lab [4], dónde se considera una red ad-hoc inalámbrica de múltiples saltos que consiste en nodos (URIs) fijos (móviles o estacionarios) para los cuales el movimiento puede ser controlado. Gracias a la movilidad controlable de UAVs, la red puede lograr una mejor conectividad y rendimiento de red. Por ejemplo, los UAV pueden reubicarse en una determinada posición para minimizar el consumo de energía o aumentar el rendimiento de la red.

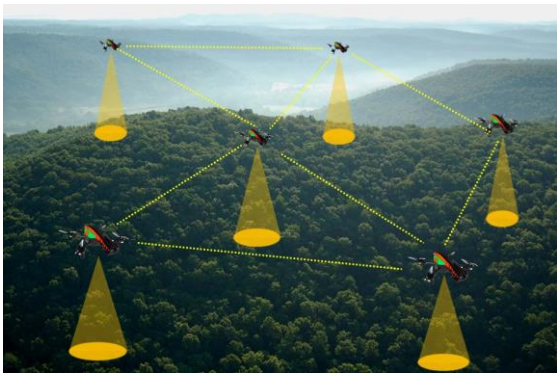


Figura 2. Red ad-hoc inalámbrica de multiples UAVs

3. TECNOLOGÍAS UTILIZADAS

3.1 Redes

En el contexto informático, una red es un conjunto de computadoras (nodos) conectadas para que se comuniquen entre sí. Según la configuración y uso que se les dé, las redes informáticas se pueden clasificar de muchas maneras. La interconexión entre millones de redes abiertas, cerradas, públicas, privadas, locales, educativas, científicas, militares, bancarias, comerciales, personales, y un largo etcétera, dan vida a lo que hoy en día conocemos como la red de redes, Internet.

La forma más habitual de clasificar las redes informáticas se basa en el alcance que estas tengan. Es decir, qué tan amplio es el conjunto de nodos que las conforman. Entre ellas, las más comunes son las redes LAN, MAN y WAN. Veremos en qué consisten cada una de ellas.

3.1.1 LAN - Local Area Network

Están restringidas en tamaño, lo cual significa que el tiempo de transmisión, en el peor de los casos, se conoce, lo que permite cierto tipo de diseños (deterministas) que de otro modo podrían resultar ineficientes. Además, simplifica la administración de la red.

Las redes de área local LAN (Local Area Network) son las de uso más frecuente. Son conjuntos de máquinas interconectadas, ubicadas en extensiones relativamente pequeñas. Son redes de propiedad privada que se usan para conectar computadoras personales o estaciones de trabajo, con objeto de compartir recursos e intercambiar información.

Desde nuestros hogares hasta grandes edificios de oficinas, pasando por entidades gubernamentales e instituciones académicas. En todos los lugares con más de una computadora interconectada, existe seguramente una LAN activa.

Las LAN permiten la interacción entre múltiples equipos para compartir datos y recursos. Muchas computadoras accediendo a la misma impresora, al mismo servidor, a la misma conexión a Internet. Todas ellas compartiendo datos a gran velocidad.

En las redes de área local la distancia entre una máquina y otra no suele ser muy grande. Por debajo de los 100 metros es lo normal. Sin embargo, con configuraciones especiales, pueden existir redes LAN con computadoras a 5 km de distancia entre sí.

3.1.2 WLAN - Wireless Local Area Network

Una LAN con sus nodos interconectados con tecnología WiFi se conoce como red inalámbrica de área local WLAN (Wireless Local Area Network). Con una WLAN no hay que tender engorrosos cables para lograr la interconexión entre las máquinas de nuestra red. Esta se realiza mediante ondas de radio de alta frecuencia.

Una desventaja es que estas redes son menos seguras que sus versiones conectadas físicamente. La señal podría ser interceptada y desencriptada por personas indeseadas.

3.1.3 MAM - Metropolitan Area Network

Una red de área metropolitana MAN (Metropolitan Area Network) consiste en computadoras compartiendo recursos entre sí en áreas de cobertura de mayor tamaño que una LAN, pero menor que una WAN. Funcionan

de forma muy parecida a una red de área local, pero cumplen estándares tecnológicos diferentes. Estas mejoras son necesarias para subsanar los problemas de latencia (retardo en la entrega de información) y pérdida de calidad de la señal en interconexiones que abarcan largas distancias.

Generalmente usan un bus doble, ida y vuelta, con fibra óptica, para interconectar las diferentes LAN a la red. También se consiguen redes MAN usando pares de cobre o microondas. Por la mayor estabilidad y menor latencia que ofrecen, son ideales para ofrecer servicios multimedia y videovigilancia en grandes ciudades, entre otras ventajas.

Como el resto de las redes cableadas, tiene su versión inalámbrica llamada WMAN (Wireless Metropolitan Area Network). Esta red utiliza tecnologías de telefonía celular como LTE y WiMax para interconectar sus miembros.

3.1.4 WAN - Wide Area Network

Las redes de área amplia WAN (Wide Area Network), son redes informáticas LAN y MAN interconectadas entre sí. Sus nodos están separados por distancias que pueden abarcar continentes enteros. Los integrantes de esas redes no necesariamente están conectados físicamente. Hacen uso de servicios de microondas y satelitales para integrar sus diferentes nodos.

Son muy usadas por grandes empresas que abarcan mucho territorio. Generalmente necesitan usar redes privadas virtuales (VPN) para conseguir la privacidad necesaria en el intercambio de datos. Otro uso muy frecuente es para ofrecer conexión web a clientes de grandes proveedores de Internet, conocidos también como ISP (Internet Service Provider).

Debido a la amplitud de su cobertura necesitan atravesar redes públicas, como las telefónicas, así como rentar servicios de transporte a otras redes privadas y usar conexiones satelitales para poder llevar la información de un lado a otro.

Su versión inalámbrica es una WWAN. Esta interconecta al resto de los nodos mediante el uso de redes de telefonía celular con tecnología LTE, WiMax, GSM, CDMA2000, UMTS, entre otras.

3.2 WiFi - IEEE 802.11

Es una tecnología de comunicación inalámbrica que permite conectar distintos equipos electrónicos, como computadoras, tablets, smartphones o celulares, etc., a una determinada red mediante el uso de radiofrecuencias o infrarrojos para la trasmisión de la información.

WiFi o Wi-Fi es originalmente una abreviación de la marca comercial Wireless Fidelity impulsada por la WiFi Alliance, que en inglés significa ‘fidelidad sin cables o inalámbrica’.

La tecnología WiFi es una solución informática que comprende un conjunto de estándares para redes inalámbricas basados en las especificaciones IEEE 802.11, lo cual asegura la compatibilidad e interoperabilidad en los equipos certificados bajo esta denominación. Existen diversos tipos de WiFi, basado cada uno de ellos en una estándar IEEE 802.11 aprobado. Son los siguientes:

- Los estándares IEEE 802.11b, IEEE 802.11g e IEEE 802.11n disfrutan de una aceptación internacional debido a que la banda de 2,4 GHz está disponible casi universalmente, con una velocidad de hasta 11 Mbit/s, 54 Mbit/s y 300 Mbit/s, respectivamente.

- En la actualidad ya se maneja también el estándar IEEE 802.11ac, conocido como WIFI 5, que opera en la banda de 5 GHz y que disfruta de una operatividad con canales relativamente limpios. La banda de 5 GHz ha sido recientemente habilitada y, además, no existen otras tecnologías (Bluetooth, microondas, ZigBee, WUSB) que la estén utilizando, por lo tanto, existen muy pocas interferencias. Su alcance es algo menor que el de los estándares que trabajan a 2,4 GHz (aproximadamente un 10 %), debido a que la frecuencia es mayor (a mayor frecuencia, menor alcance).

3.3 Punto de acceso inalámbrico

Un punto de acceso inalámbrico, más conocido por sus siglas en inglés WAP o AP (wireless access point), es un dispositivo de red que interconecta equipos de comunicación de forma inalámbrica, formando así una red inalámbrica que interconecta dispositivos móviles o tarjetas de red inalámbricas.

Estos dispositivos suelen configurarse en las redes inalámbricas como intermediarios, permitiendo la conexión inalámbrica de un dispositivo móvil de cómputo (computadora, tableta, Smartphone) con una red (Internet o local). Estos facilitan la conexión de varias máquinas cliente sin la necesidad de un cable, lo que les aporta a estos clientes una mayor portabilidad del equipo, y que estos posean una conexión sin limitárseles tanto su ancho de banda.

Normalmente, un WAP también puede conectarse a una red cableada, y puede transmitir datos entre los dispositivos conectados a la red cableada y los dispositivos inalámbricos. Además de esto, podemos conectar a muchos WAP entre sí, formando una red aún mayor y permitiendo realizar roaming a los clientes de la red.

Para configurar estos puntos de acceso inalámbricos lo habitual es asignarles direcciones IP de manera fija o dinámica, al tratarse de un equipo de red más, y así poder acceder a ellos.

3.4 Sistemas de distribución

Un conjunto de routers y puntos de acceso que interconectados componen una red se denomina **sistema de distribución** o **DS** (de sus siglas en inglés Distribution System). Hay diferentes tipos de sistemas de distribución que se pueden configurar de acuerdo a las necesidades y posibilidades que tengamos. Cada uno de ellos tiene sus ventajas e inconvenientes. Si el coste no es un problema y es posible instalar cables de red a través de las áreas de cobertura, la mejor opción será un sistema de distribución cableado en malla.

El sistema de distribución más básico, consiste en un sistema interconectado por cables de red. Como podemos ver en la siguiente figura, todos los puntos de acceso están conectados al router con su propio cable de red dedicado. Por tanto, la señal de Internet entrante a todos los APs (Puntos de Acceso) será a través de esta conexión por cable. Esto permite proporcionar a los APs una señal muy buena. Si es posible, así es como debe configurarse una red para asegurarse de que nuestros dispositivos inalámbricos obtengan la mejor señal posible. Si contamos con múltiples routers inalámbricos y queremos que estos actúen como APs, en general, sólo deberíamos tener un dispositivo que actúe como un enrutador, viéndonos obligados a desactivar la función de enrutamiento en el resto de dispositivos, de lo contrario podríamos llegar a provocar graves problemas de convergencia en nuestra red.

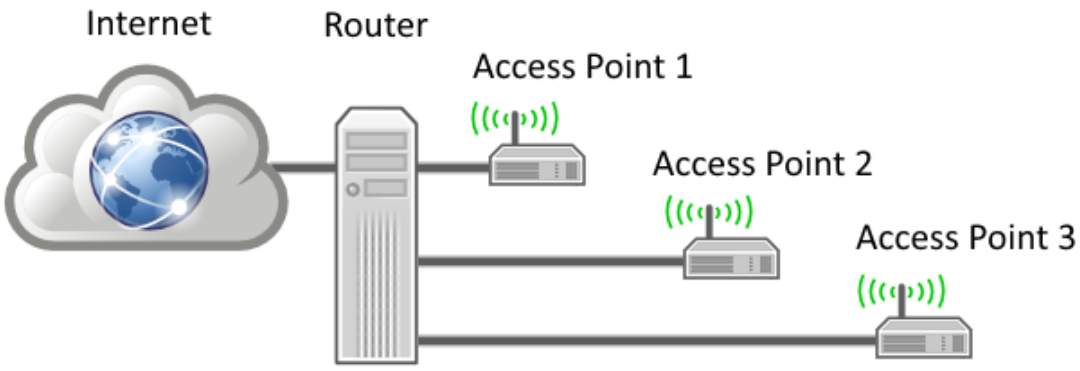


Figura 3. Sistema de Distribución

Otra posiblidad de sistema de distribución cableado es aquella em la que cada uno de los APs tiene dos interfaces de red cableadas. Tal como podemos ver e la figurade a continuación, el AP1 obtiene su señal de entrada directamente del router, transmitiendo esta señal a través de su segunda interfaz cableada hacia el AP2

por medio del cable de red. De la misma forma el AP2 transmite su señal al AP3. Este sistema de distribución es diferente al anterior aún contando con los mismos dispositivos de red y con una interconexión cableada entre ellos, pero funcionalmente, cada AP proporcionaría una señal de gran calidad.

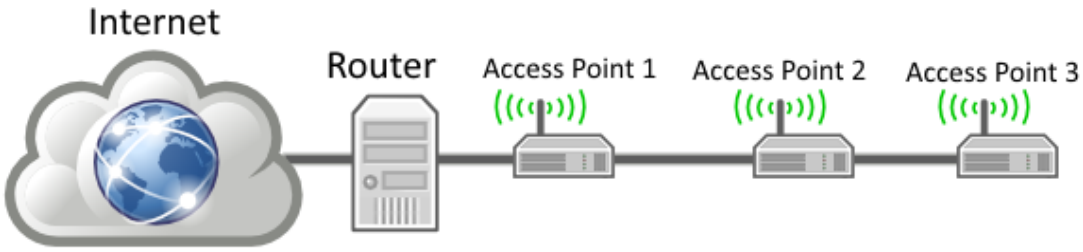


Figura 4. Sistemade Distribución de tipo Bus

A veces no es posible la instalación de cables de red para interconectar los distintos APs. Por esta razón la señal a transmitir debe viajar por el aire. Cuando esto ocurre, hablamos de un sistema de distribución inalámbrico, tal como el representado en la Figura 5, dónde las líneas de puntos representan la comunicación inalámbrica entre los APs. También podemos observar que tiene un esquema semejante al de la Figura 4, en el cual el AP2 se comunica directamente con el AP1, y el AP3 se comunica con el AP2 de forma directa e indirectamente a su vez con el AP1. En este caso el esquema planteado será el de **un sistema de distribución inalámbrico** o **WDS** (de sus siglas en inglés: Wireless Distribution System). Configurar un WDS es un poco más complejo, ya que cada AP tiene que estar programado para aceptar solamente la señal entrante del AP que corresponda. Por lo tanto, el AP2 sólo deberá aceptar la señal de AP1, y el AP3 sólo aceptará la señal del AP2. Esto significa que, si por algún motivo el AP2 quedara inhabilitado, el AP3 no podría obtener ninguna señal a su entrada; lo que desembocaría en que los equipos conectados al AP3 quedarían fuera de línea al no tener acceso a la señal de comunicación aportada por el router.

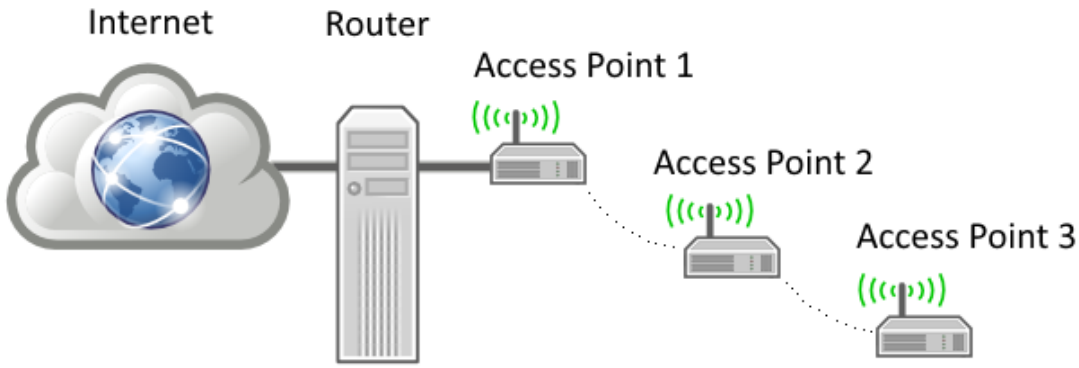


Figura 5. Sistema de Distribución Inalámbrico

WDS no tiene redundancia entre los APs participantes. Esto quiere decir que cuando uno de los APs falla, el sistema de distribución se corta. Para poder solucionar esta situación el AP que queda fuera de línea, debe ser reparado o debe reemplazarse lo antes posible dado que ha dejado sin conexión a todos los APs y equipos involucrados, que dependían de éste para obtener la señal de comunicación proporcionada por nuestro router.

Este problema de redundancia de APs podemos corregirlo utilizando una topología de **red WDS de malla** o **red Mesh**, en la que todos los APs se comunican entre sí. Uno de los principales beneficios de este tipo de redes es que pueden prescindir de enrutamiento manual, o apenas requerir atención para el mantenimiento de éste. Sí se implementan protocolos de enrutamiento dinámicos, podrían considerarse “autoenrutables”, de esta

manera cuando un AP se cae, otro tomará su papel enrutando a los APs que dependían del AP caído. Esta es la razón por la que una red WDS de malla es más robusta, pero también es más cara debido a la mayor complejidad de esta red. Cuando un AP está desconectado, el flujo de la señal de comunicación se desvía. Por ejemplo, fijándonos en la siguiente figura, si AP2 se cae, AP1 se comunicará con AP3 y será el encargado de enrutar a través de su conexión inalámbrica. De esta forma, los nodos adyacentes a un nodo o enlace fallido propagarán un cambio en la tabla de rutas, notificando a nodos contiguos del cambio en la red, y así sucesivamente. En consecuencia, una red en malla resulta muy confiable.

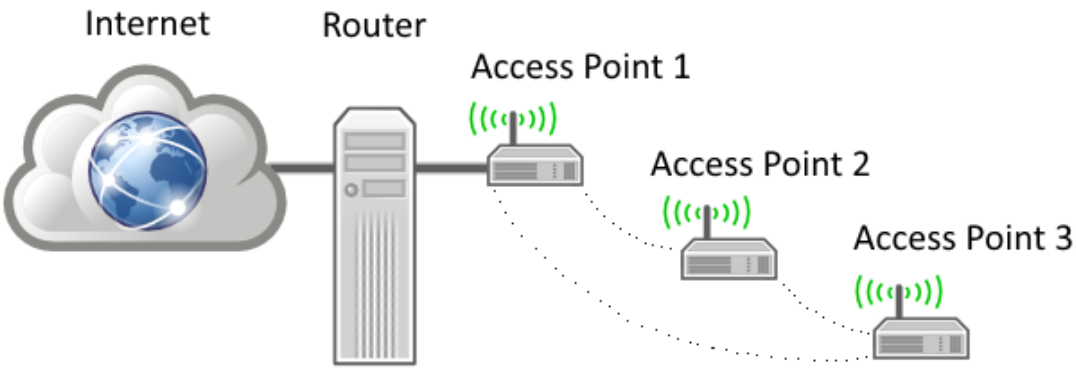


Figura 6. Sistema de Distribución Mesh

3.5 STP - Spanning Tree Protocol

Es un protocolo de red de nivel 2 del modelo OSI (capa de enlace de datos). Su propósito es el de gestionar la presencia de bucles. Este protocolo nos garantiza que no existan tales bucles en aquellas topologías de red en las que existan enlaces redundantes (necesarios en muchos casos para garantizar la disponibilidad de las conexiones), evitando así que se puedan ocasionar problemas que pueden inhabilitar la operatividad de la red.

Este protocolo permite a los dispositivos de interconexión activar o desactivar automáticamente los enlaces de conexión en trayectorias redundantes, de forma que se garantice la eliminación de bucles. STP es transparente a las estaciones de usuario.

3.6 DHCP - Dynamic Host Configuration Protocol

El protocolo de configuración dinámica de host DHCP es un estándar TCP/IP diseñado para simplificar la administración de la configuración IP de los equipos de nuestra red.

Si disponemos de un servidor DHCP, la configuración IP de los equipos de una red puede hacerse de forma automática, evitando así la necesidad de tener que realizar manualmente uno por uno la configuración TCP/IP de cada equipo.

Un servidor DHCP es un servidor que recibe peticiones de los equipos de red solicitando una configuración de red IP. El servidor responderá a dichas peticiones proporcionando los parámetros que permitan a los equipos autoconfigurarse. Para que un equipo solicite la configuración de red a un servidor, será preciso que en su configuración de red tengan habilitada la opción que permita obtener dirección IP de forma automática.

El servidor DHCP proporcionará al cliente al menos los siguientes parámetros:

- Dirección IP
- Máscara de subred

Opcionalmente, el servidor DHCP podrá proporcionar además de estos anteriores otros parámetros de configuración tales como:

- Puerta de enlace
- Servidores DNS
- Muchos otros parámetros más

El servidor DHCP proporciona una configuración de red TCP/IP segura y evita conflictos de direcciones repetidas. Utiliza un modelo cliente-servidor en el que el servidor DHCP mantiene una administración centralizada de las direcciones IP utilizadas en la red. Los clientes podrán solicitar al servidor una dirección IP y así poder integrarse en la red.

3.7 Encriptación WPA2 PSK

Se trata de un protocolo de autenticación y cifrado para redes WiFi:

- WPA2 (Wi-Fi Protected Access 2 o Acceso Protegido Wi-Fi 2) es un sistema para proteger las redes inalámbricas (Wi-Fi), creado para corregir las deficiencias del sistema previo en el nuevo estándar 802.11i – WPA, contando con un algoritmo más robusto y difícil de vulnerar.
- PSK (Pre-shared key o Clave pre-compartida) es una clave secreta compartida con anterioridad entre las dos partes de una canal de comunicaciones inalámbrico antes de que se utilice. Para crear una clave de secreto compartido, se debe utilizar la función de derivación de claves. Estos sistemas utilizan casi siempre algoritmos criptográficos de clave simétrica. Se utiliza en cifrado Wi-Fi como WEP o WPA, donde tanto el punto de acceso inalámbrico (AP) como todos los clientes comparten la misma clave.

4. DISEÑO DEL SISTEMA

4.1 Hardware

Para llevar a cabo este trabajo hemos utilizado varios dispositivos Raspberry Pi así como otros tantos módulos Wipi, cedidos por el departamento de electrónica de la Escuela Superior de Ingenieros de la US.

4.1.1 Raspberry Pi

Raspberry Pi es un computador de placa reducida o de placa única (SBC) de bajo costo desarrollado en Reino Unido por la Fundación Raspberry Pi [5], con el objetivo de estimular la enseñanza de ciencias de la computación en las escuelas.

El software para la raspberry Pi es open source, siendo su sistema operativo oficial una versión adaptada de Debian, denominada Raspbian, aunque permite usar otros sistemas operativos, incluido una versión de Windows 10. En todas sus versiones incluye un procesador Broadcom, una memoria RAM, una GPU, puertos USB, HDMI, Ethernet (El primer modelo no lo tenía), 40 pines GPIO y un conector para cámara. Ninguna de sus ediciones incluye memoria, siendo esta en su primera versión una tarjeta SD y en ediciones posteriores una tarjeta MicroSD.

Se han utilizado varias versiones de dispositivos Raspberry Pi buscando la viabilidad de este proyecto. En la implementación final de este proyecto y en los que a las simulaciones se refiere, hemos utilizado únicamente la Raspberry Pi 3 Modelo B, esta elección se debe principalmente a que en adición a su mayor capacidad de trabajo cuenta con un módulo para soportar conexiones inalámbricas integrado.

Figura 7. Raspberry Pi 3-B

4.1.2 WiPi

Se trata del módulo oficial de la Raspberry Pi para soportar conexiones inalámbricas. Es compatible con los estándares: IEEE 802.11n, IEEE 802.11g y IEEE 802.11b; y es capaz de operar con las siguientes velocidades de transmisión:

- 11b: 1/2/5.5/11Mbps.
- 11g: 6/9/12/18/24/36/48/54 Mbps.
- 11n: up to 150 Mbps.

Su rango de frecuencias es de los 2.4 a los 2.4835 GHz, y se puede configurar para trabajar sobre los canales del 1 al 13, soportando una potencia de transmisión de 20dBm como máximo. En cuanto a las características de seguridad soporta las encriptaciones: WPA/WPA2, WPA-PSK/WPA2-PSK y WEP de 64/128/152 bits.

Debido a las diversas redes de conexión inalámbrica requeridas para implementar nuestra red de comunicaciones se ha optado por hacer uso de este módulo extra, además del módulo integrado en la propia Raspberry, dado que una vez se configura una interfaz de red en un canal de frecuencias concreto, no se puede configurar otra interfaz de red en el mismo módulo que opere en un canal de frecuencias distinto a la interfaz anteriormente configurada. Trabajar en distintos canales de frecuencias nos minimizará el ruido y la pérdida de paquetes de nuestra red, aportando un mejor funcionamiento.

Figura 8. Módulo Wipi

4.2 Software

Como comentamos anteriormente el software para la raspberry Pi es open source lo que nos brinda la oportunidad de poder usar una gran diversidad de sistemas operativos. En vistas del propósito de este TFG, la distribución elegida para implementar nuestra red de comunicaciones conformada por dispositivos Raspberry Pi es una distribución de Linux conocida como LEDE, basada en OpenWRT.

4.2.1 OpenWRT

OpenWrt es una distribución GNU/Linux altamente extensible para dispositivos embebidos (generalmente enrutadores inalámbricos). A diferencia de muchas otras distribuciones para routers, OpenWrt está construido desde sus cimientos como una plataforma totalmente funcional, y un sistema operativo fácilmente modificable. En la práctica, esto significa que usted puede tener justo la funcionalidad que requiera, sin funciones o características innecesarias para el objetivo de su plataforma. OpenWrt es impulsado por un núcleo Linux, más reciente que la mayoría de otras distribuciones de finalidad equivalente.

Figura 9. OpenWRT

Para los desarrolladores, OpenWrt proporciona un marco para construir una plataforma empotrada sin tener que crear una distribución e imagen de firmware completa alrededor de ese objetivo. Para los usuarios, significa la libertad completa de adaptar la funcionalidad y configuración, posibilitando el uso de un dispositivo embebido en formas que el fabricante o vendedor nunca imaginó.

- **Libre y de código abierto**. El proyecto es completamente libre y de código abierto, licenciado bajo los términos de la GPL. El proyecto pretende siempre estar alojado en un sitio Internet de fácil acceso, con su código fuente completo, y disponible para crear los ejecutables correspondientes.
- **Fácil y de libre acceso**. El proyecto siempre estará abierto a nuevos contribuyentes y tiene una baja barrera para la participación. Cualquier persona podrá aportar. Nosotros, los desarrolladores actuales, activamente otorgamos acceso de escritura a cualquier persona interesada en obtenerlo. Creemos que las personas son responsables cuando se les da la responsabilidad. Únicamente solicítelo y será capaz de adquirir los privilegios de acceso que necesite.
- **Impulsada por la Comunidad**. A través del esfuerzo y trabajo de "todos" colaborando para alcanzar un objetivo común.

OpenWrt desde hace mucho tiempo se estableció como la mejor solución de firmware en su clase, superando a otras soluciones de firmware para dispositivos embebidos en términos de rendimiento, estabilidad, extensibilidad, robustez y diseño.

4.2.2 LEDE

El proyecto LEDE ("Linux Embedded Development Environment") es un sistema operativo Linux basado en OpenWrt. Se trata de un reemplazo completo del firmware suministrado por el proveedor de una amplia gama de enrutadores inalámbricos y otros muchos dispositivos no destinados para este propósito. Puede consultar la tabla de hardware de los dispositivos compatibles: Table of Hardware.

Figura 10. LEDE

La mayoría de la gente se decanta por instalar LEDE porque cree que le puede ofrecer un mejor funcionamiento que el firmware de stock que le ofrece su proveedor. Entre otros motivos, ellos encuentran que es más estable, ofrece más características, es más seguro y tiene un mejor soporte. A continuación, se detallan algunas de las características por las que nos hemos decidido por esta opción:

- **Extensibilidad**: LEDE proporciona muchas capacidades que sólo se encuentran en dispositivos de gama alta. Sus 3000 paquetes de aplicaciones están estandarizados, por lo que puede replicar fácilmente la misma configuración en cualquier dispositivo compatible, incluidos dos (o incluso cinco) años de edad, enrutadores.
- **Seguridad**: La instalación estándar de LEDE es segura por defecto, con Wi-Fi deshabilitado, sin contraseñas pobres o puertas traseras. Los componentes de software de LEDE se mantienen al día, por lo que las vulnerabilidades se cierran poco después de que se descubran.
- **Rendimiento y Estabilidad**: El firmware de LEDE está hecho de módulos estandarizados usados en todos los dispositivos soportados. Esto significa que cada módulo probablemente recibirá más pruebas y corrección de errores que el firmware de stock que puede ser modificado para cada línea de productos y nunca se ha vuelto a tocar.
- **Fuerte apoyo de la comunidad**: Los miembros del equipo de LEDE son participantes regulares en las listas de correo LEDE Forum, LEDE Developer y LEDE Admin y los canales IRC de LEDE. Puede interactuar directamente con los desarrolladores, los voluntarios que gestionan los módulos de software y con otros usuarios de larga data, aumentando drásticamente las posibilidades de resolver el problema.
- **Investigación**: Muchos equipos utilizan LEDE como una plataforma para su investigación sobre el

rendimiento de la red. Esto significa que las mejoras de sus exitosos experimentos estarán disponibles en LEDE en primer lugar, mucho antes de que se incorpore al mainline, el firmware del proveedor.

- **Open Source / Sin coste adicional**: LEDE se proporciona sin ningún costo monetario. Ha sido creado por un equipo de voluntarios: desarrolladores y mantenedores, individuos y empresas. Cualquier persona de la comunidad puede contribuir con algún esfuerzo para ayudar a mejorarlo. Todo lo anterior es posible dado que LEDE es parte de la comunidad de código abierto, y alimentado por el kernel de Linux.

5. CONFIGURACIÓN DE LA RED

5.1 Descripción de la red de comunicaciones

La red que nos diponemos a configurar, debido a su complejidad, podemos dividirla en tres partes. Estas partes o secciones de red de nuestra red global, son a su vez tres redes inalámbricas distintas:

- **Red de conexión a la nube**. Será la red que utilicemos para poder conectarnos al exterior (WAN). Conectaremos nuestro router principal como cliente de dicha red, que será la que nos proporcionara los servicios de comunicación, como puede ser acceso a Internet por ejemplo.
- **Red de distribución**. Será la encargada de enlazar todos los nodos de nuestra red. Servirá para enrutar la comunicación entre la red de acceso de los clientes y nuestro router principal. Esta red cumplirá funciones de comunicación sincronización entre todos nodos o routers que la conforman.
- **Red de acceso**. Esta es la red a la que los clientes o usuarios finales se podrán conectar para poder servirse de nuestros servicios de comunicaciones.

Pasaremos a ver cada una de ellas con mayor detalle en los siguientes apartados.

5.2 Red de conexión a la nube

En primer lugar, conectaremos uno de los routers que conforman nuetsra red a una red que disponga de conexión a Internet, en nuestro caso el router seleccionado será el que corresponde a la Raspberry Pi A, al que nos referiremos de aquí en adelante como el router principal.

Para realizar esta configuración en nuestro router principal será necesario crear una nueva interfaz inalámbrica a la que denominaremos WAN. Una vez hemos creado esta interfaz, será preciso que escaneemos los canales de radiofrecuencia WiFi disponibles y seleccionemos la señal WiFi que nos proporcione el servicio de internet requerido para el funcionamiento de nuestra red. En el caso que nos acontece la señal que nos proveerá de acceso a Internet se denomina “LaNube”.

Una vez escogida esta señal configuraremos esta interfaz como **Cliente DHCP**, para que se nos asignen los parámetros de red de forma automática.

La interfaz especificada quedará cnofigurada del siguiente modo:

- **Raspberry Pi A:** Interfaz WAN.
    - Una señal WiFi que recibirá la que hemos decidido llamar “LaNube” con las siguientes características:
        - Tipo de señal: Client
        - SSID: LaNube
        - BSSID: E8:B4:C8:12:46:BC
        - Canal de radiofrecuencia: 6
        - Encriptación: WPA2 PSK

Realizada esta configuración, nuestro router principal ya dispondrá de la conexión a Internet necesaria para proveer al resto de nodos y clientes conectados.

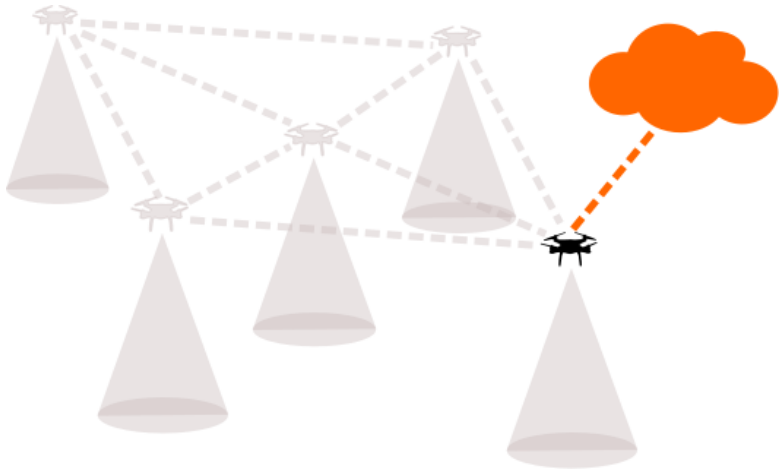


Figura 11. Red de conexión a “LaNube”

5.3 Red de distribución

La red de distribución nos permitirá conectar a todos los dispositivos Raspberry que actuarán como **nodos** de nuestra red, entre sí, para que puedan comunicarse y sincronizarse. A su vez, también nos permitirá conectar a todos los putnos de accso de los clientes que de esta forma podrán ampliar su cobertura de manera que cubra la mayor extensión posible.

Por las características que tiene nuestra red, que estará soportada por dispositivos raspberry Pi ubicados “a bordo” de distintos UAVs, su localización geográfica podrá variar, de hecho, será lo habitual pues estarán sobrevolando una zona en cuestión. Dicho esto, no es difícil entender que el dibujo de nuestra red será algo dinámico, pues la disposición de sus nodos irá variando en todo momento. Debido a esta peculiaridad resultará de gran interés poder construir una red de tipo **Mesh** o **mallada**, en la que sus nodos vayan adaptándose a distintas topologías de red de forma automática.

Para conseguir armar esta red mesh nos serviremos de la función **WDS** que nos ofrece el LEDE. Esta función configurada debidamente nos proporcionará un protocolo de enrutamiento dinámico, y redundancia en los canales de conexión inalámbrica de nuestra red de distribución.

Conviene señalar que no todos los routers soportan esta tecnología, que hace que un dispositivo cliente conectado a nuestra red de acceso cambie de un punto de acceso a otro sin notarlo, conservando la dirección MAC en la información enviada.

Para esta red de distribución nos hemos decantado por un direccionamiento IP estático que nos permita tener localizados a todos los nodos y asi poder configurar mas tarde las conexiones entre ellos. Las direcciones IP y máscaras escogidas para la configuración de los dispositivos Raspberry PI que conforman esta red son las siguientes:

- **Raspberry Pi A**: 192.168.10.1 / 255.255.255.0
- **Raspberry Pi B**: 192.168.10.2 / 255.255.255.0
- **Raspberry Pi C**: 192.168.10.3 / 255.255.255.0

Además, dado que se utilizará únicamente para conectar los nodos que actuarán como routers entre sí, se ha optado por dotarla de seguridad, cifrando sus enlaces de comunicación con una encriptación WPA2-PSK; pues no queremos que ningún dispositivo que forme parte de nuestra red de distribución se conecte.

Para conseguir el enrutamiento dinámico de esta red, así como la redundancia entre sus enlaces de

comunicación característicos de las redes Mesh, será necesario conectar cada una de nuestras Raspberry con todas las demás en caso de no ser un número muy elevado, o al menos con todas las posibles; y además activar el protocolo **STP**, que será el encargado de enrutar dinámicamente la red en todo momento. De esta forma nuestra red será lo más robusta posible, y en caso de que algún nodo caiga por alguna circunstancia o se aleje dejando sin cobertura su zona de trabajo, otro nodo cercano será el encargado de autoenrutar su flujo de comunicación y de gestionar a sus clientes manera transparante a ellos, así como de enrutar al resto de nodos que dependían de éste para acceder al nodo principal.

Por tanto, cada nodo de nuestra red deberá disponer de una señal master que proporcione la señal de conexión hacia el nodo principal, y tantas señales clientes como nodos vecinos tenga.

En nuestras pruebas se han utilizado 3 dispositivos Raspberry Pi, con lo que disponemos de 3 nodos de red. Uno es el denominado nodo principal, con interfaz WAN, que suministrará la conexión a internet; y otros dos nodos que se encargarán de distribuir la señal del nodo principal.

Todos los nodos de nuestra red contarán con una interfaz a la que hemos denominado **LAN** que deberemos configurar en modo **Bridge**, para que nos cree un puente entre todas las interfaces inalámbricas "WDS" ya sean de tipo master o cliente.

Las interfaces y conexiones inalámbricas de nuestros nodos de red para cumplir con las especificaciones planteadas de nuestra red de distribución quedarán de la siguiente manera:

- **Raspberry Pi A:** Interfaz LAN en modo Bridge con las siguientes señales inalámbricas:
    - Una señal WiFi que emitirá la que hemos decidido llamar "WDS" con las siguientes características:
        - Tipo de señal: Master WDS
        - SSID: WDS
        - BSSID: 00:C1:41:32:0E:61
        - Canal de radiofrecuencia: 1
        - Encriptación: WPA2 PSK

- **Raspberry Pi B:** Interfaz LAN en modo Bridge con las siguientes señales:
    - Una señal WiFi que emitirá la señal "WDS" con las siguientes características:
        - Tipo de señal: Master WDS
        - SSID: WDS
        - BSSID: 00:C1:41:32:09:BC
        - Canal de radiofrecuencia: 1.
        - Encriptación: WPA2 PSK
    - Una señal WiFi cliente que recibirá la señal que provee la Raspberry Pi A con las siguientes características:
        - Tipo de señal: Client WDS
        - SSID: WDS.
        - BSSID: 00:C1:41:32:0E:61
        - Canal de radiofrecuencia: 1.
        - Encriptación: WPA2 PSK
    - Una señal WiFi cliente que recibirá la señal que provee la Raspberry Pi C con las siguientes características:
        - Tipo de señal: Client WDS

        - SSID: WDS.
        - BSSID: 00:C1:41:32:01:A3
        - Canal de radiofrecuencia: 1
        - Encriptación: WPA2 PSK

- **Raspberry Pi C:** Interfaz LAN en modo Bridge con las siguientes señales:
    - Una señal WiFi que emitirá la señal "WDS" con las siguientes características:
        - Tipo de señal: Master WDS
        - SSID: WDS
        - BSSID: 00:C1:41:32:01:A3
        - Canal de radiofrecuencia: 1
        - Encriptación: WPA2 PSK
    - Una señal WiFi cliente que recibirá la señal que provee la Raspberry Pi A con las siguientes características:
        - Tipo de señal: Client WDS
        - SSID: WDS.
        - BSSID: 00:C1:41:32:0E:61
        - Canal de radiofrecuencia: 1
        - Encriptación: WPA2 PSK
    - Una señal WiFi cliente que recibirá la señal que provee la Raspberry Pi B con las siguientes características:
        - Tipo de señal: Client WDS
        - SSID: WDS.
        - BSSID: 00:C1:41:32:09:BC
        - Canal de radiofrecuencia: 1
        - Encriptación: WPA2 PSK

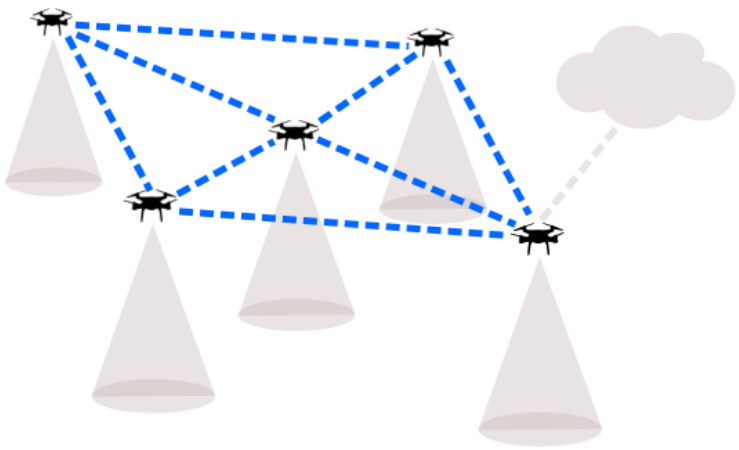


Figura 12. Red de distribución WDS

5.4 Red de acceso

Esta será la parte de la red encargada de permitir el acceso a las conexiones de los clientes o usuarios finales. Esta red estará compuesta por la suma de todos los puntos de acceso desplegados por cada uno de nuestros nodos de red.

Cada nodo de red actuará como punto de acceso para servir a los clientes de nuestra red de comunicaciones, permitiendo que estos se conecten y suministrandoles una conexión a internet a través de la ya explicada anteriormente red de distribución.

A la de acceso la hemos denominado “SOS” en nuestras simulaciones. Esta red queremos que sea una red pública, a la que pueda acceder cualquier persona, por lo que no hemos visto conveniente usar ningun tipo de encriptación.

Los nodos de red proporcionarán cobertura de red “SOS” a su zona de influencia, es decir, a la zona que este sobrevolando en ese preciso momento el UAV en el que esten localizados cada uno de ellos.

La configuracción de la red inalámbrica “SOS” será la misma en cada uno de los nodos de nuestra red y se detalla a continuación:

- **Raspberry Pi A:** Interfaz LAN en modo Bridge.
    - Una red inalámbrica con las siguientes características:
        - Tipo de señal: Master
        - ESSID: SOS
        - BSSID: 00:C1:41:16:11:37
        - Canal de radiofrecuencia: 3

- **Raspberry Pi B:** Interfaz LAN en modo Bridge.
    - Una señal WiFi que emitirá la señal “SOS” con las siguientes características:
        - Tipo de señal: Master
        - ESSID: SOS
        - BSSID: B8:27:EB:2B:5A:CD
        - Canal de radiofrecuencia: 6

- **Raspberry Pi C:** Interfaz LAN en modo Bridge.
    - Una señal WiFi que emitirá la señal “SOS” con las siguientes características:
        - Tipo de señal: Master
        - ESSID: SOS
        - BSSID: B8:27:EB:90:89:98
        - Canal de radiofrecuencia: 11

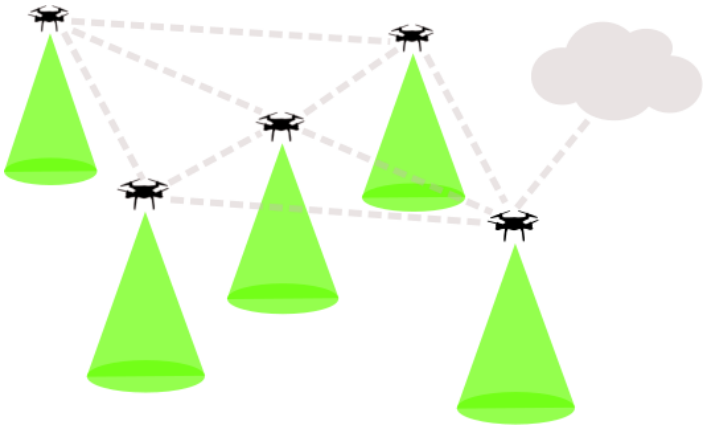


Figura 13. Red de acceso SOS

5.5 Servidor DHCP

Para gestionar la configuración de red de los clientes o usuarios que se conecten a nuestra red de comunicaciones de forma automatica, será imprescindible hacer uso de un servidor DHCP. Este servidor lo ideal es que sea un único servidor en toda la red, pues la existencia de mas de un servidor DHCP en una misma red puede ocasionar problemas que pongan en grave peligro la funcionalidad de la toda la red.

Nuestro servidor DHCP lo activaremos en el nodo principal de nuestra red, es decir en la Raspberry Pi A. Este será el encargado de configurar el direccionamiento IP, no solo de los clientes conectados directamente a su red de acceso, sino de todos los clientes conectados a cualquiera de los nodos que participen en nuestra red. Para ello será obligatorio descactivar toda funcionalidad de DHCP en el resto de los nodos.

Teniendo en cuenta las direcciones IP estáticas que hemos adjudicado a nuestros nodos, deberemos escoger un rango de direcciones IP a repartir por nuestro servidor DHCP entre los clientes que no nos pueda crear un conflicto con las direcciones IP de nuestros nodos. El rango que hemos optado por utilizar en nuestras simulaciones es el siguiente:

5.6 Clientes

Los clientes o usuarios finales de nuestra red de comunicaciones serán dispositivos capacitados de conexión inalámbrica WiFi. Para poder acceder a nuestra red será necesario que estos esten dentro del alcance de cobertura de nuestra red de acceso “SOS”, y que escaneen y se conecten a ella.

Dado que contamos con servidor DHCP en nuestra red de comunicaciones, la configuración de red de los clientes deberíamos de configurarla de forma automática por DHCP.

Lo ideal será para evitar problemas de conexión y que nuestra red funcione de la manera más trasparente possible al usuario que estos una vez conectados por primera vez a nuestra red de acceso activen la opción de union automática.

5.7 Red de servicios de comunicaciones

Como hemos descrito al comienzo de este capítulo, nuestra red final está conformada por las tres redes anteriores, y será la que en toda su extensión, logre comunicar a los clientes o usuarios finales con la conexión al exterior; proporcionando así a estos clientes el servicio de comunicaciones objeto de este studio. En la Figura 14 podemos ver como quedaría el escenario final conjunto de todas las redes.

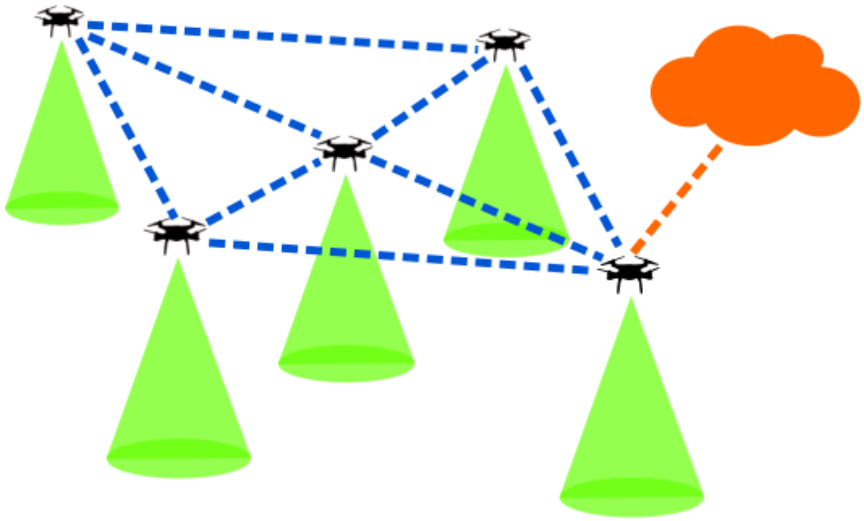


Figura 14. Red mesh de servicios de comunicaciones completa

6. RESULTADOS EXPERIMENTALES

6.1 Configuración de la red de conexión a la nube

En primer lugar añadiremos y habilitaremos una nueva conexión inalámbrica en el router principal de nuestra red, escanearemos las redes WiFi disponibles y nos uniremos a la red que nos proporcionará acceso a internet: la señal "LaNube". El modo de conexión a utilizar será Cliente DHCP.

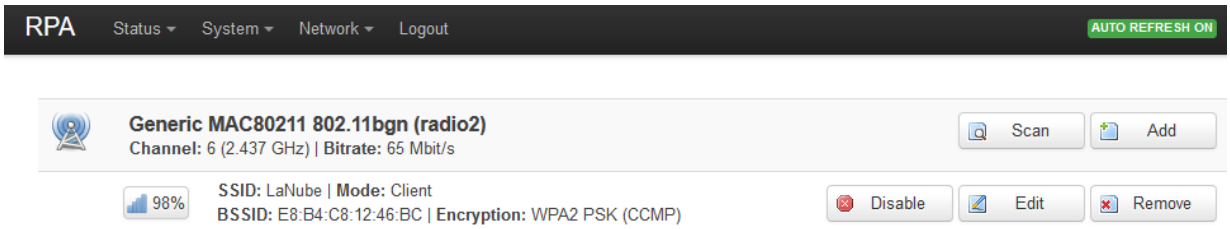


Figura 15. Conexión del router principal RPA a la red WiFi "LaNube"

Una vez hemos conectado nuestro router principal, al que denominamos RPA, pasaremos a la creación e una nueva interfaz a la que llamaremos WWAN y vincularemos a esta la red inalámbrica "LaNube". Esta interfaz podemos verla en la Figura 16.

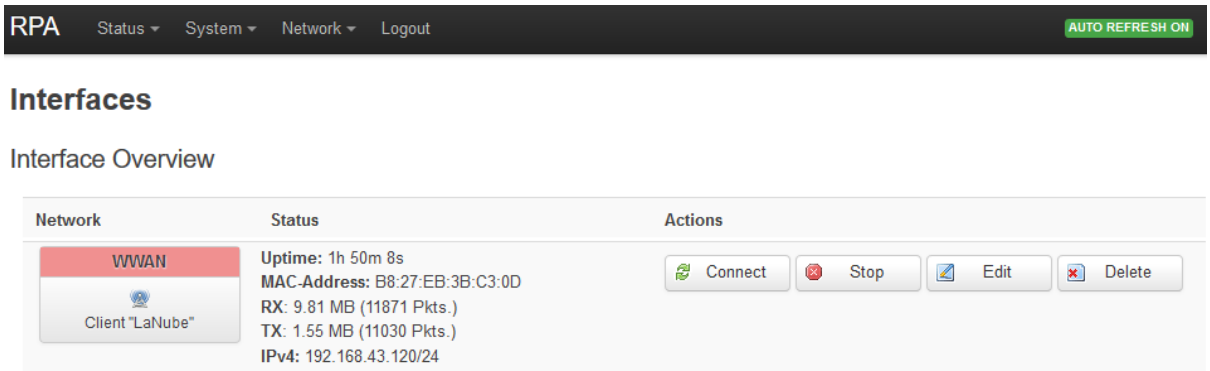


Figura 16. Creación de la interfaz WWAN en RPA

En este punto ya deberíamos tener acceso a internet a partir de esta interfaz. Podemos comprobarlo desde las herramientas de diagnosis incorporadas en nuestro firmware (LEDE).

Para ello nos iremos al menu desplegable "Network" y seleciomaremos la opción "Diagnostics". Desde esta nueva página realizaremos un ping a la dirección de prueba "lede-project.org". Podemos verlo en la

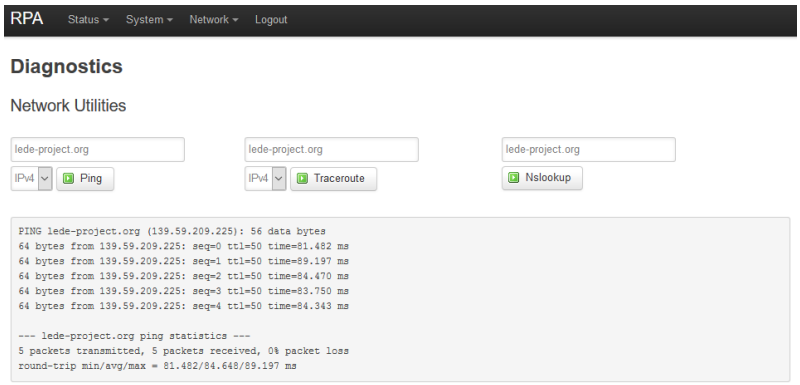


Figura 17. Ping desde RPA a una dirección de Internet

6.2 Despliegue de la red de distribución

Primero configuraremos la red de distribución en la RPA. Para ello desplegaremos una nueva red inalñambrica a la que denominaremos “WDS” configurando el modo de conexión como Access Point WDS, que emita en el canal 1 de radiofrecuencias WiFi. En este paso le configuraremos también seguridad inalámbrica desde la pestaña Wireless Security elegiremos “WPA2 PSK” aportando una clave personal que cumpla el requesito de 8 caracteres como mínimo.

Esta red la vincularemos a una nueva interfaz que llamaremos LAN, donde configuraremos de forma manual la IP estática que le hemos asignado al nodo RPA: 192.168.10.1.

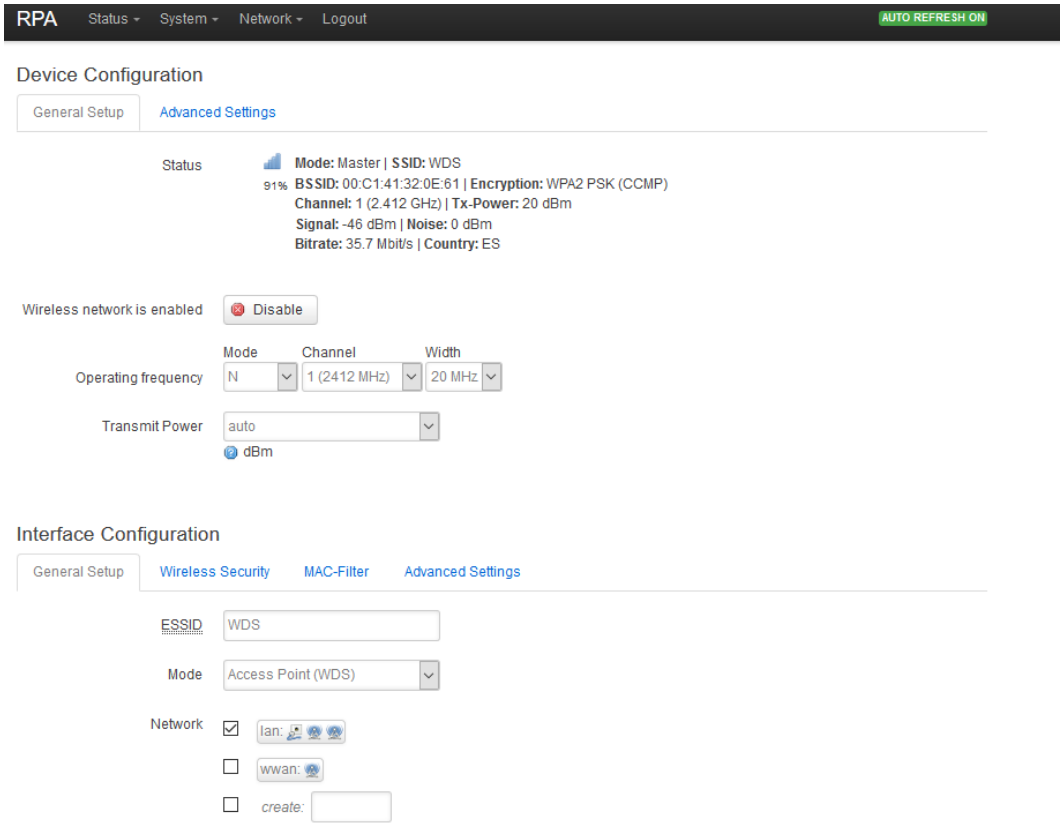


Figura 18. Configuración de la red de distribución WDS en RPA

Ya tenemos configurada la parte de la conexión de red emite la señal de comicaciones que recibirán y distribuirán el resto de nodos de la red. Pasaremos a configurar el resto de nodos, todos de la misma forma.

Desde otro nodo de la red, y así para todos, escanearemos las señales de redes inalámbricas que estén a nuestro alcance. Una vez escaneadas selecionaremos la señal WDS y nos uniremos proporcionando la clave creada en el paso anterior.

Figura 19. Escaneo de conexiones WiFi en el nodo RPC

El modo de conexión a esta red será “Client WDS”. Solo quedará asignar esta señal a una interfaz LAN la cual hayamos configurado manualmente con la IP estática que le corresponda al nodo en cuestión.

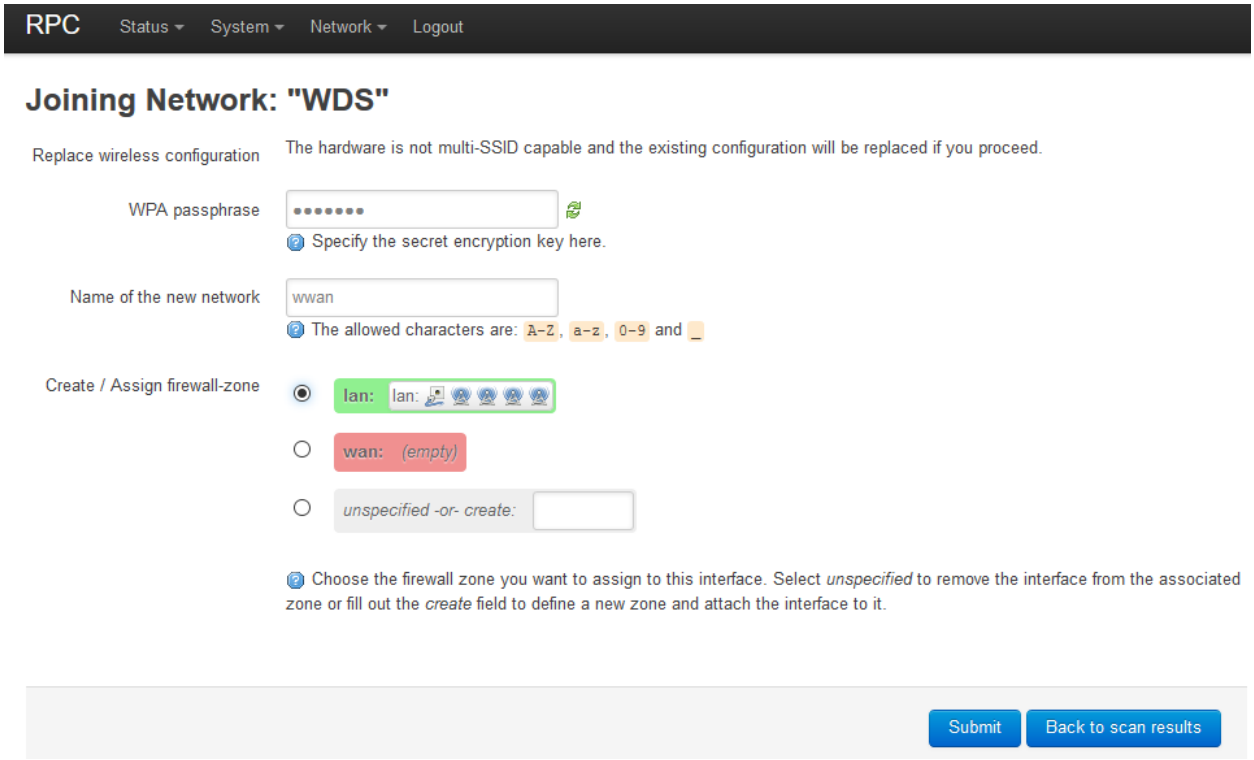


Figura 20. Configuración de un nodo de la red de distribución como cliente WDS

Haremos este proceso de configuración en todos los demás nodos, estableciendo conexión en tantas redes inalámbricas WDS como resto de nodos haya.

A su vez en cada uno de los nodos de la red será necesario desplegar una red inalámbrica en modo Access Point WDS tal como hemos hecho con el nodo principal RPA.

Todas las redes tanto en modo punto de acceso como en modo cliente desplegadas o configuradas en cada uno de nuestros nodos deberán estar vinculadas a una única interfaz LAN en modo Bridge de múltiples interfaces.

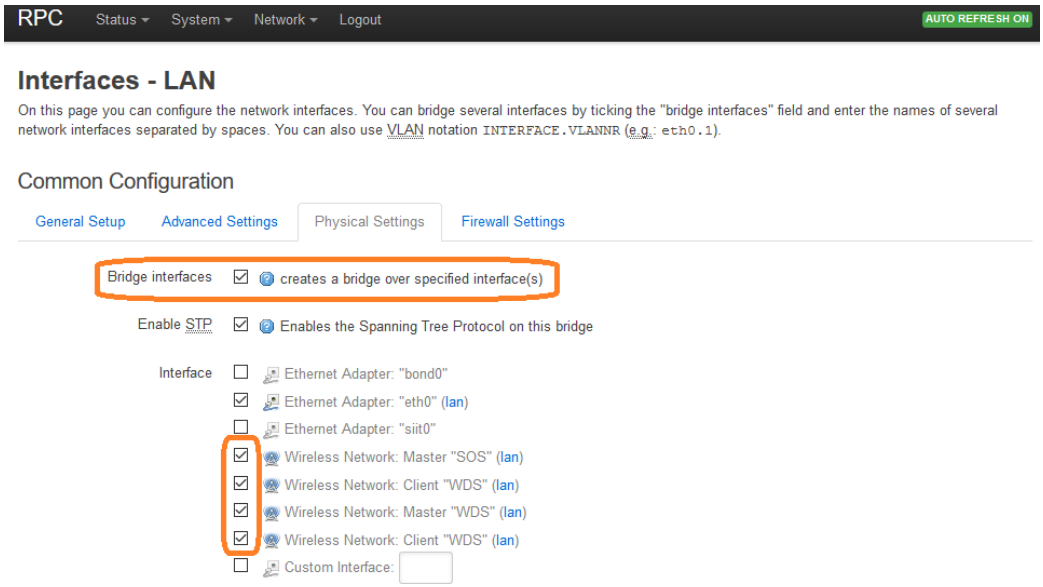


Figura 21. Configuración de un puente entre interfaces

6.3 Pruebas de conexión

Para realizar pruebas de conexión entre los nodos que forman nuestra red de distribución, podemos hacer uso de nuevo de las propias herramientas de diagnosis incorporadas en nuestro firmware. Para ello nos iremos al menu desplegable “Network” y seleciomaremos la opción “Diagnostics”. Nos mostrará un nuevo de menú con las herramientas de diagnosis.

Desde el menu de diagnosis probaremos a hacer *ping* entre nuestro nodo principal, RPA, al resto de nodos configurados en la red. Bastará con poner las direcciones IP que hemos adjudicado a nuestros nodos de forma manual.

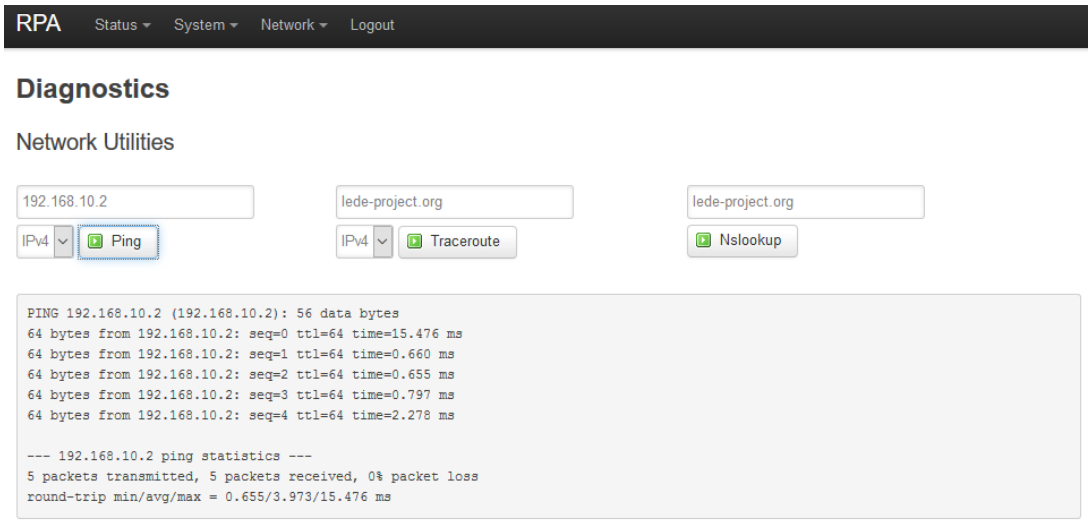


Figura 22. Ping de RPA a RPB

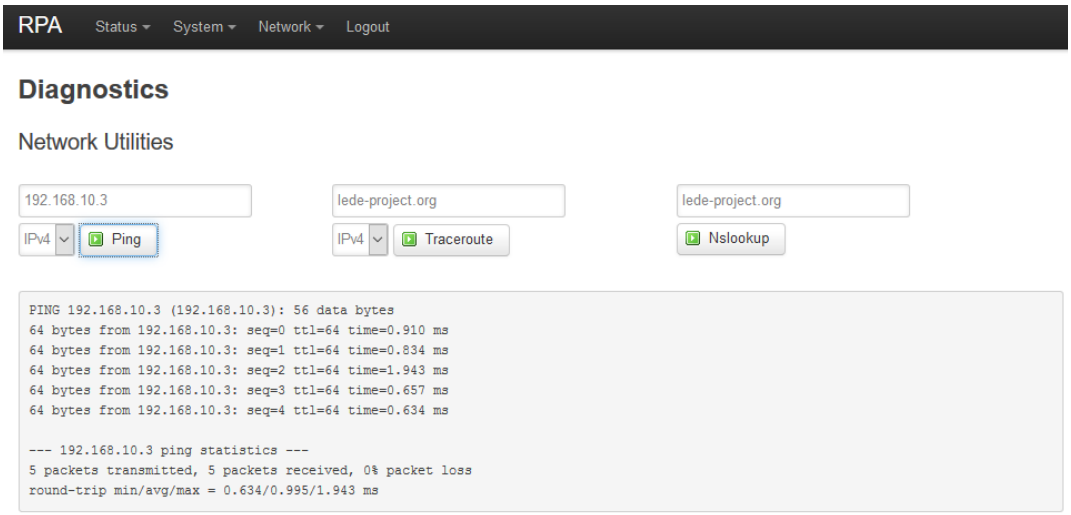


Figura 23. Ping de RPA a RPC

Tras realizar esta comprobación, podemos ver que hemos tenido una respuesta exitosa por parte de los demás nodos de la red. Llegados a este punto, ya hemos conseguido que se comuniquen nuestros nodos entre sí.

6.4 Habilitar el servidor DHCP

Configuraremos ahora el servidor DHCP. Este solo se configurará en un único nodo, el nodo principal que corresponde a la RPA. En el resto de nodos, tanto en RPB como en RPC, deberemos deshabilitar este servidor DHCP.

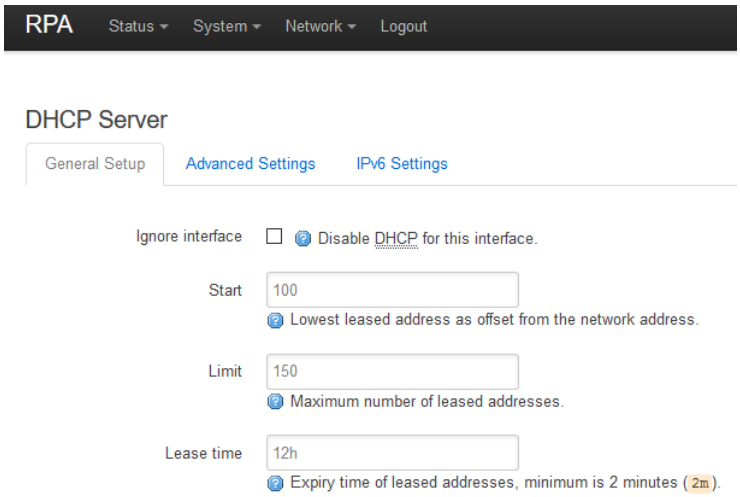


Figura 24. Configuración del servidor DHCP en RPA

6.5 Despliegue de la red de acceso

Esta red estará formada por la suma de todos los puntos acceso desplegados en cada uno de los nodos. A cada uno de las redes desplegadas por los puntos de acceso que participen en esta red se le asignará el mismo nombre, dado que se trata de armar una única red "SOS". Este despliegue lo realizaremos en distintos canales de radiofrecuencias, con la idea de evitar el ruido y las interferencias en las comunicaciones que se ocasionarían si operasen todos los puntos de acceso en el mismo canal de radiofrecuencias.

Utilizaremos un canal de radiofrecuencias WiFi para cada una de las redes inalámbricas desplegadas por cada

uno de los puntos de acceso de nuestra red. La configuración escogida es la siguiente:

- La Raspberry Pi - RPA trabajará sobre el canal 3.
- La Raspberry Pi - RPB trabajará sobre el canal 6.
- La Raspberry Pi - RPC trabajará sobre el canal 11.

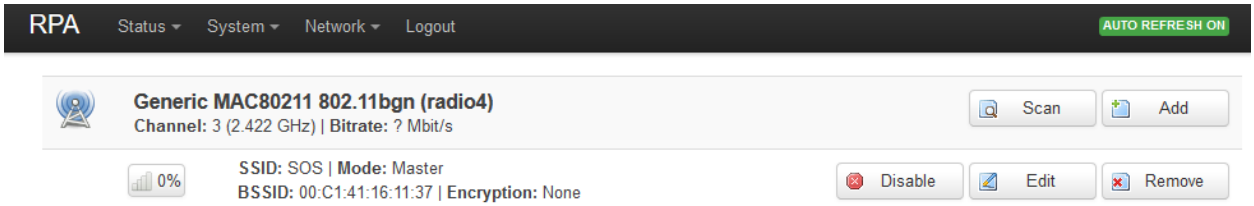


Figura 25. Master "SOS" en RPA

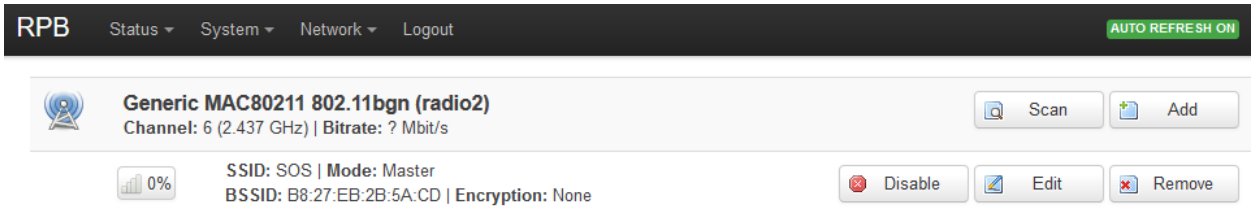


Figura 26. Master "SOS" en RPB

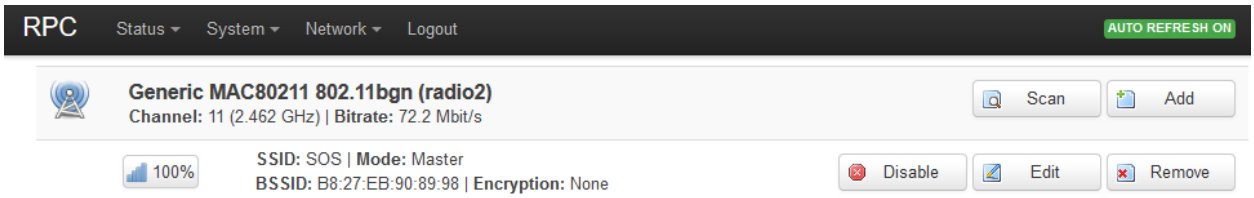


Figura 27. Master "SOS" en RPC

6.6 Despliegue final de toda red de comunicaciones

6.6.1 Vista de las redes inalámbricas configuradas en nuestros nodos

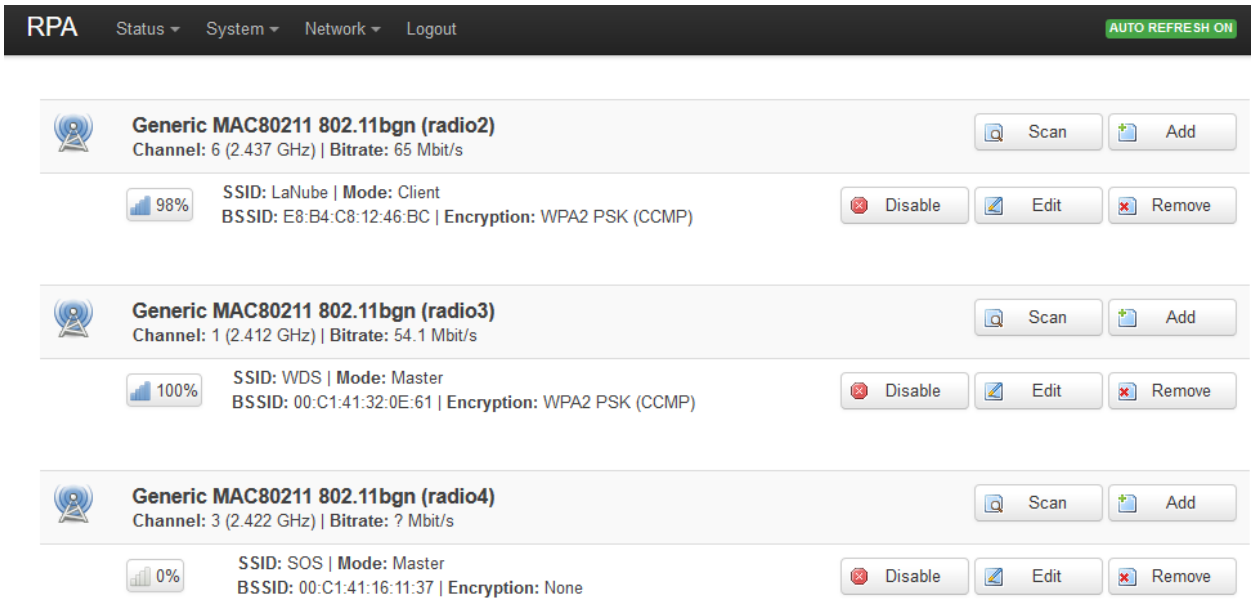


Figura 28. Conexiones de red inalámbricas de RPA

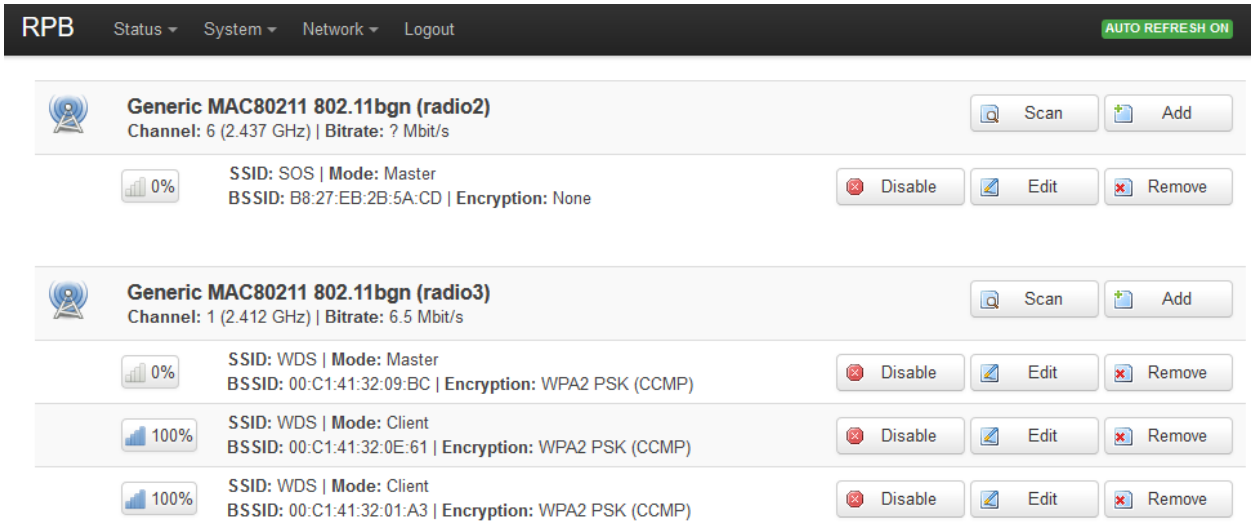


Figura 29. Conexiones de red inalámbricas de RPB

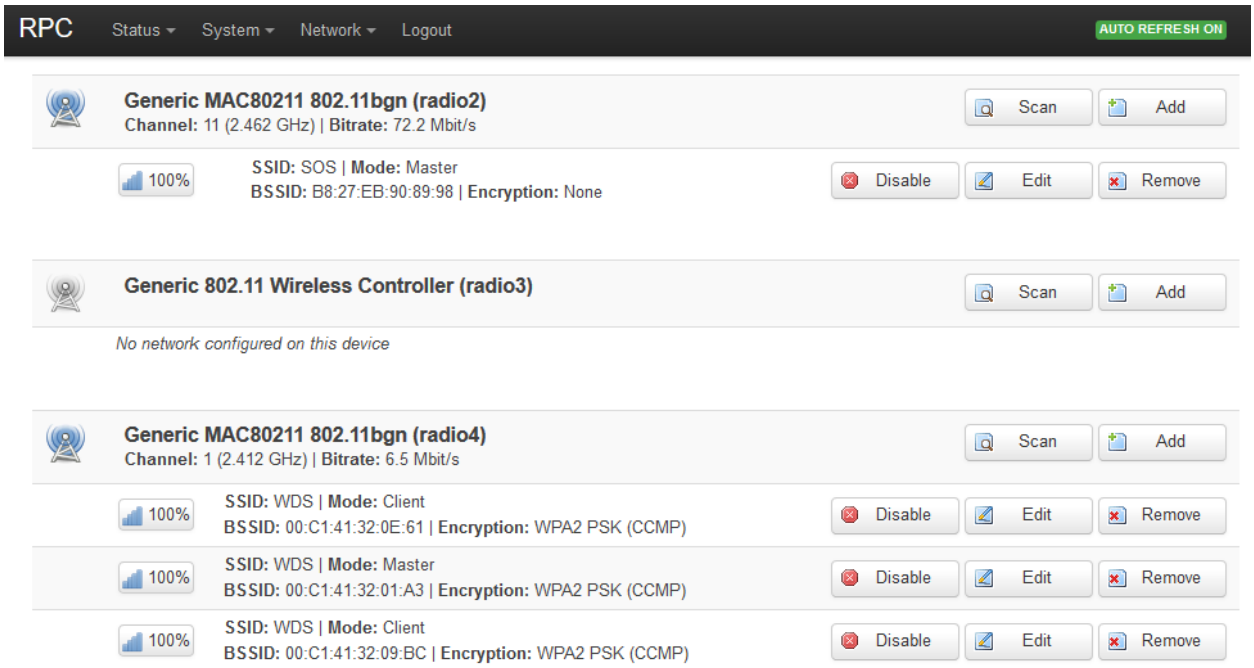


Figura 30. Conexiones de red inalámbricas de RPC

6.6.2 Vista de las interfaces configuradas en nuestros nodos

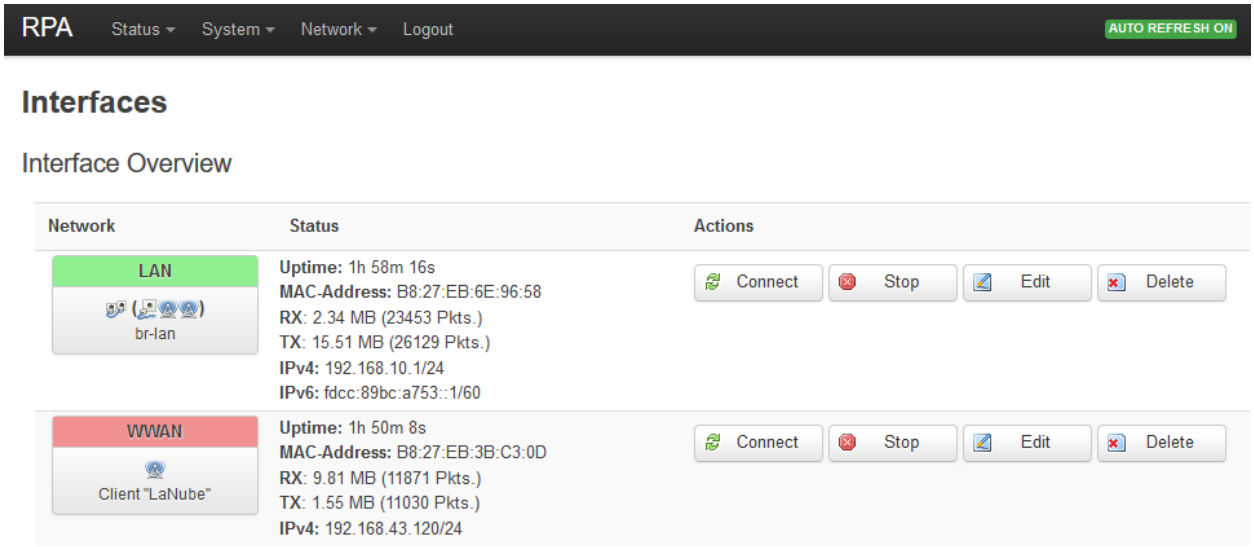


Figura 31. Interfaces configuradas en la RPA

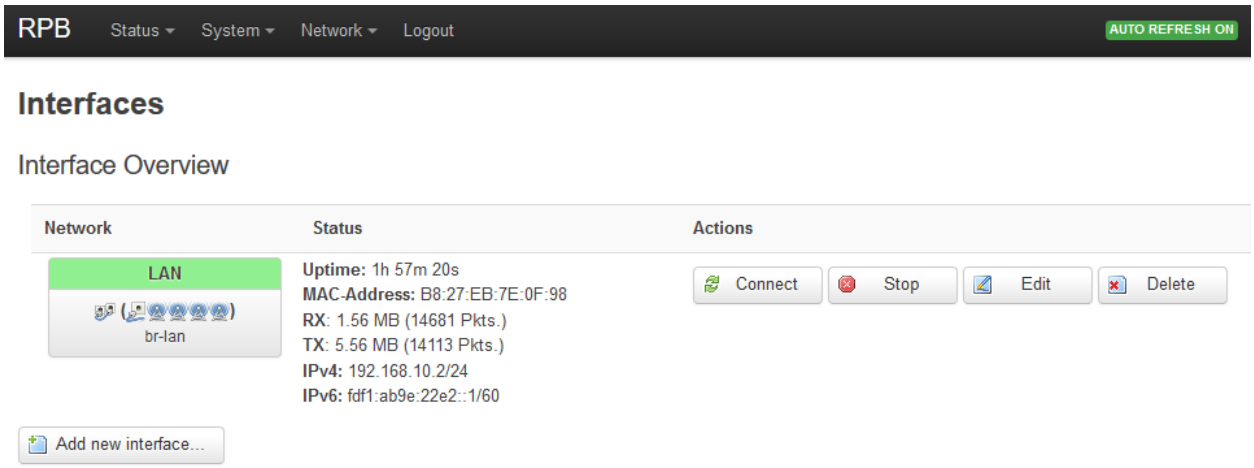


Figura 32. Interfaces configuradas en la RPB

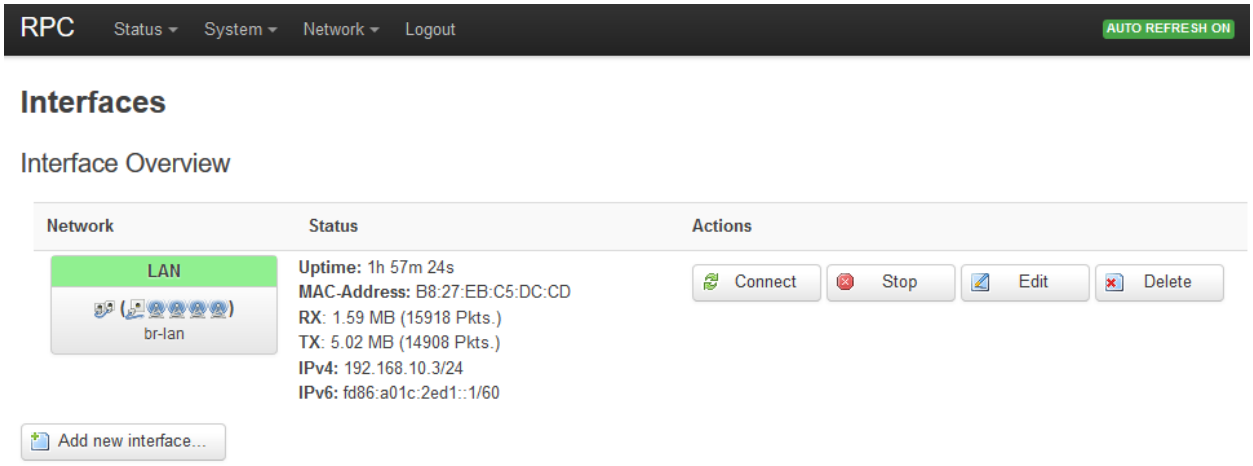


Figura 33. Interfaces configuradas en la RPC

6.7 Conexión de los clientes

Para conectarnos a la red de acceso "SOS" como cliente, será necesario utilizar algún tipo de dispositivo con conexión inalámbrica, como pueden ser un smartphone, un portátil o una tablet.

Una vez nos encontremos al alcance de la red "SOS", exploraremos las conexiones WiFi visibles desde nuestro dispositivo y nos conectaremos a ella. Para conectarnos deberemos tener habilitada la configuración de red automática en nuestro dispositivo y no será necesaria introducer ninguna clave ya que esta red es libre.

Figura 34. Conexión de un cliente a la red de acceso

Preferiblemente marcaremos la opción de union automática, para poder realizar la union de manera trasparante al usuario al migrar de un punto de acceso con cobertura "SOS" a otro. Esta migración podrá deberse aque nos desplacemos respecto al punto de acceso al que nos hayamos conectado, o bien sea el UAV en el que se localiza este punto de acceso el que se displace. También puede ocurrir que por alguna circustancia, el UAV o la raspberry a la que estemos conectado quede inoperativa, en tal nuestro dispositivo se conectará de manera automática a otro punto de acceso que se encuentre a nuestro alcance.

Figura 35. Datos de conexión del cliente

Una vez conectados a la red, nos asignarán el direccionamiento conveniente y dispondremos de acceso a nuestra red, así como a los servicios que se proporcionen como en el caso de nuestra simulación acceso a internet.

6.8 Pruebas de funcionamiento de la red

6.8.1 Prueba 1: Reinicio de la red

Una vez tenemos todos los nodos de nuestra red configurados y conectados entre sí y su funcionamiento se encuentra funcionando correctamente, pasamos a apagar todos los dispositivos Raspberry Pi.

Esperamos unos segundos y procedemos a encenderlas sin ningún orden específico.

Figura 36. Nodos de nuestra red conectados tras un reinicio forzado

Una vez encendidas todas podemos observamos que se ha desplegado de manera automñatica todas las redes inalámbricas pertienentes y que podemos conectarnos como cliente y navegar sin problemas.

6.8.2 Prueba 2: Cambio provocado de la topología de la red de distribución

Ahora nos disponemos a provocar un cambio en la topología de connexion de los nodos de nuestra red de distribución.

En la Figura 37 podemos observar la existencia de un cliente conectado en el nodo RPC y bordeado de color rojo el tráfico generado por el cliente. En azul podemos determiner que dicho cliente está conectado a la red SOS. Justo debajo podemos apreciar en color verde que nuetsra RPC está bifurcando el tráfico del cliente directamente hacia la red WDS correspondiente a la RPA, pues se trata de su MAC.

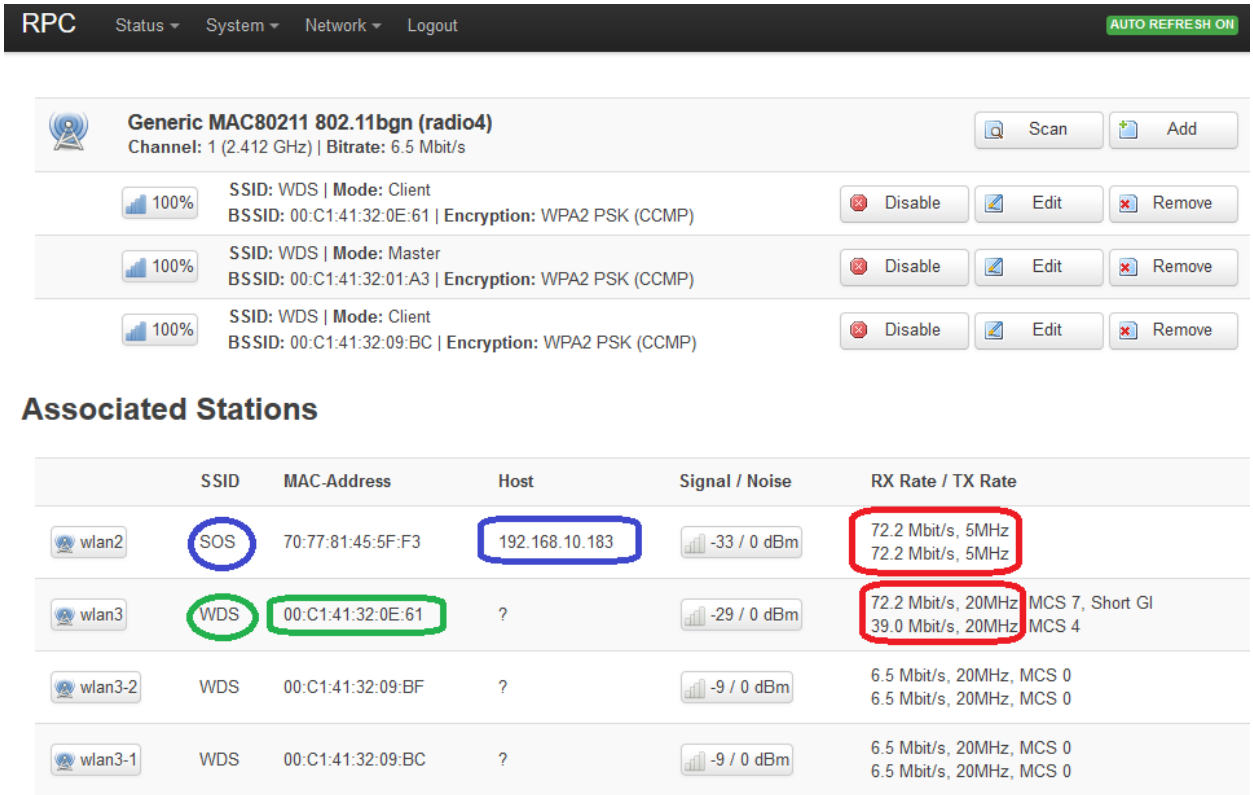


Figura 37. Nodo RPC enruta tráfico del cliente hacia RPA

A continuación vamos a proceder a deshabilitar en el nodo RPC la conexion a la red WDS desplegada por la RPA, con lo que lo dejaremos desconectado de forma directa.

Esperamos unos segundos y podemos ver al como refleja la Figura 38 como una vez desconectado de RPA (color naranja), el nodo ha comenzado a distribuir el tráfico de nuestro cliente de la red SOS (color azul) hacia el nodo con la MAC correspondiente a la de RPB.

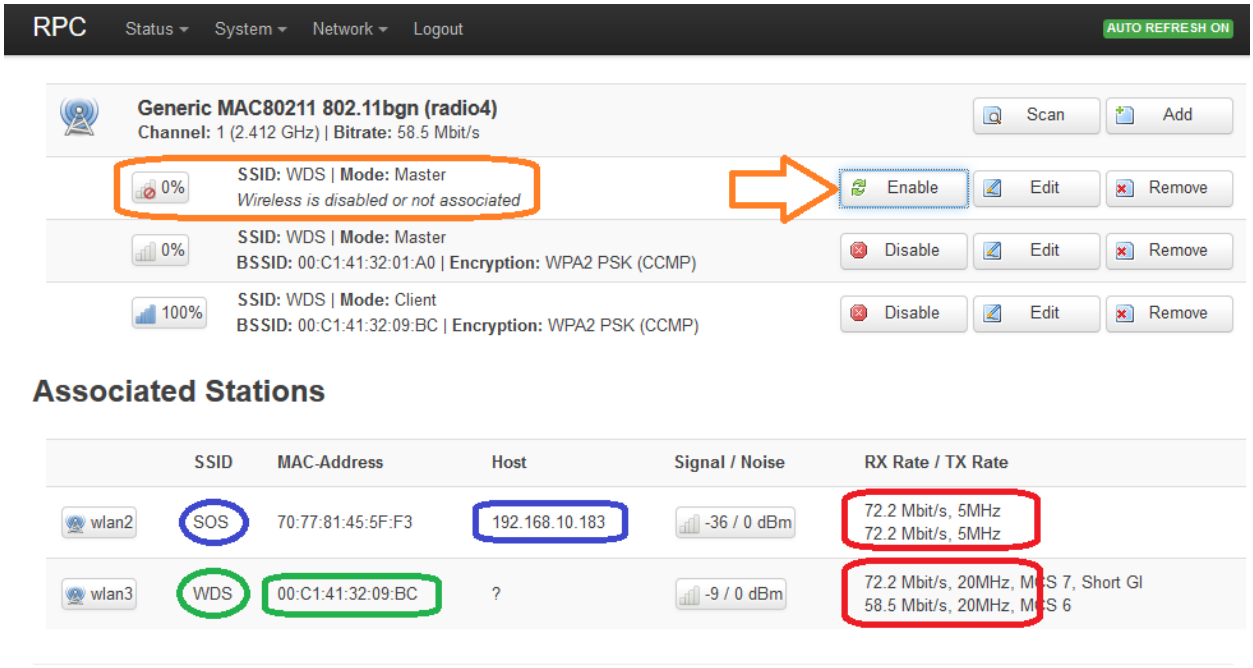


Figura 38. Nodo RPC enruta trñafico del cliente hacia RPB

6.8.3 Prueba 3: Caída de un nodo de la red

Procedemos ahora a conectarnos a la red “SOS” con un cliente. Una vez realizada la connexion, buscamos cual será el nodo de la red al que nos hemos conectado. En la Figura 39 se muestra la interfaz web del nodo RPC, y podemos observar que nos aparece como cliente asociado a la red “SOS” nuestro dispositivo.

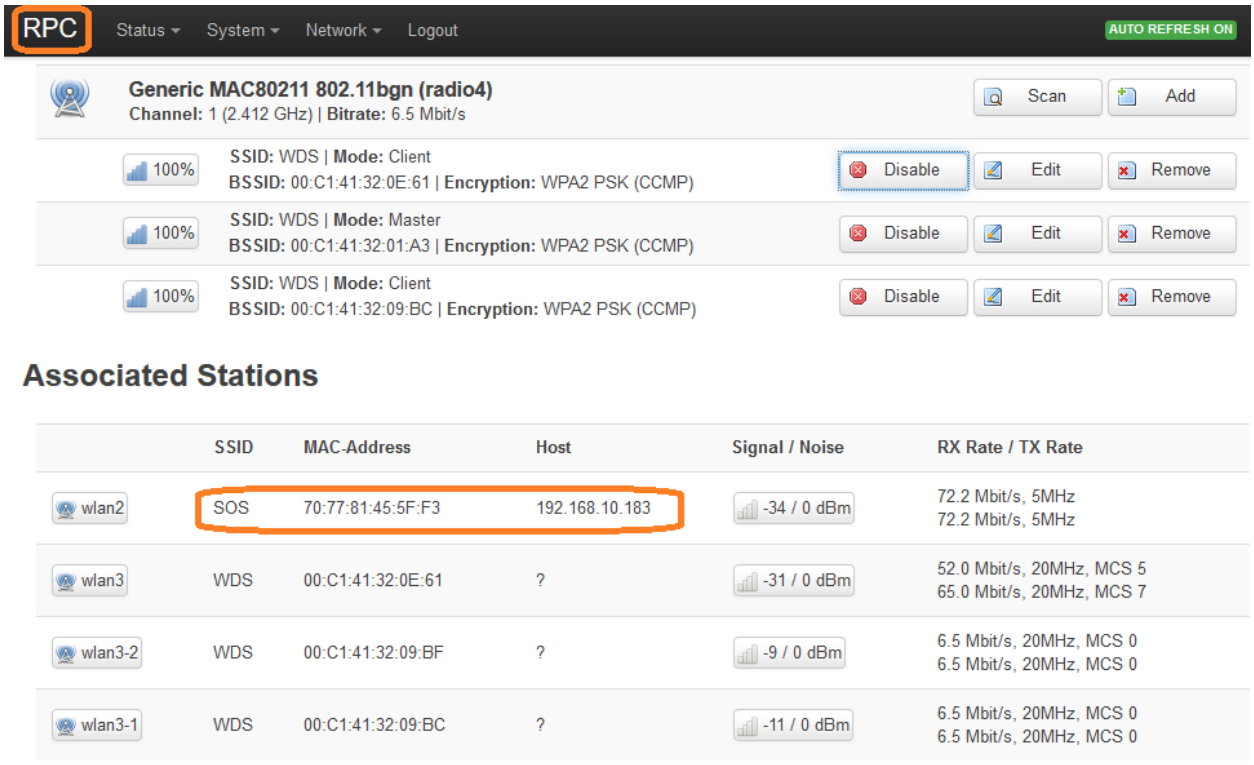


Figura 39. Cliente conectado a RPC

Pasamos ahora a desconectar de la alimentación al nodo RPC, el cual tiene vinculado al cliente. Una vez realizado esta apagado fortuito de la RPC procedemos a mostrar las estaciones asociadas al nodo RPB desde su interfaz web.

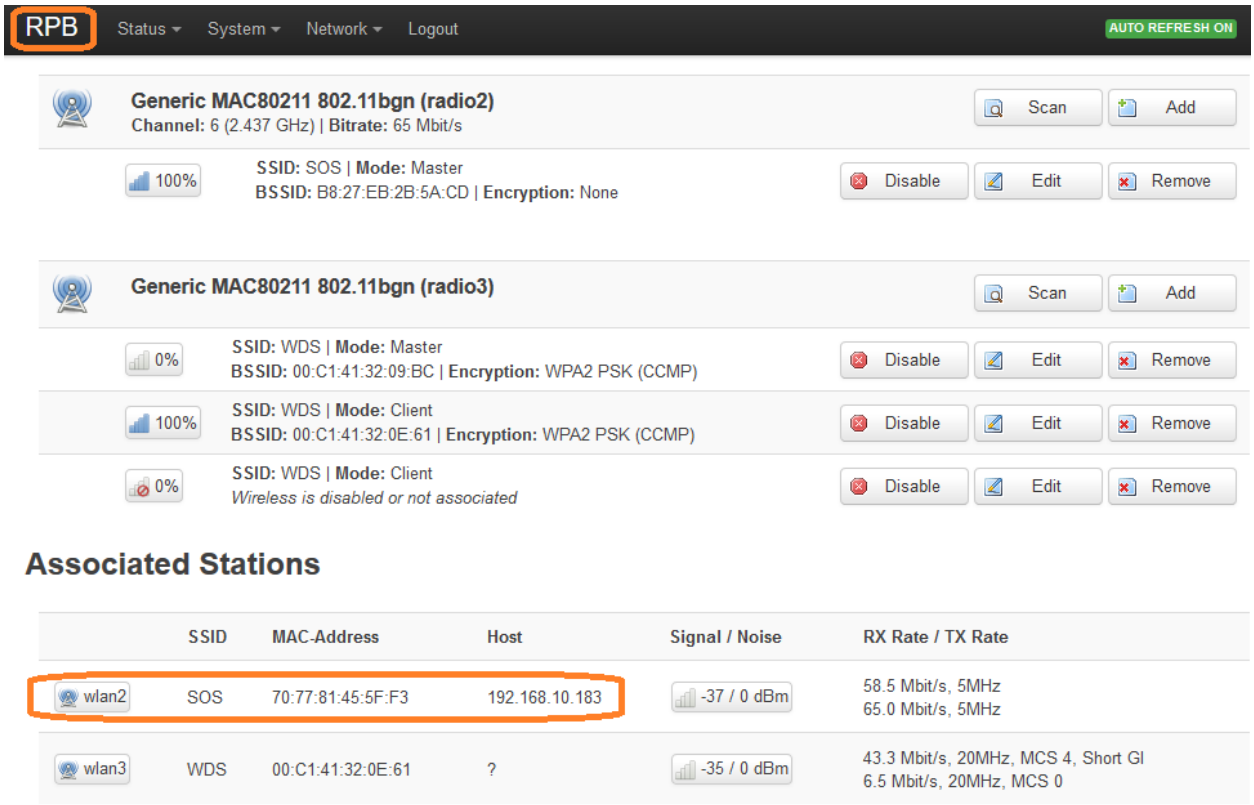


Figura 40. Cliente conectado a RPB

En la Figura 40 podemos observar como nos aparece el cliente como estación asociada al nodo RPB el cliente con IP 192.168.10.183 y la MAC 70:77:81:45:5F:F3. Si comparamos estos datos con los del cliente de la Figura 39 podemos observar que se trata del mismo.

6.8.4 Prueba 4: Traspaso de un cliente entre dos nodos de la red

Para realizar esta prueba nos ayudaremos de la aplicación WiFi Analyzer [6] instalada en un smartphone que conectaremos como cliente a nuestra red de acceso “SOS”.

Escogiendo en esta apliccaicón la opciñon de “Gráficos de canales” se mostrará en un gráfico la información sobre la potencia y los canales sobre los que operan las señales WiFi diponibles en nuestra zona. Esto podemos verlo en la Figura 41. Si analizamos la figura podemos ver que existen 3 señales con el nombre de SOS localizadas en los canales 3, 6 y 11.

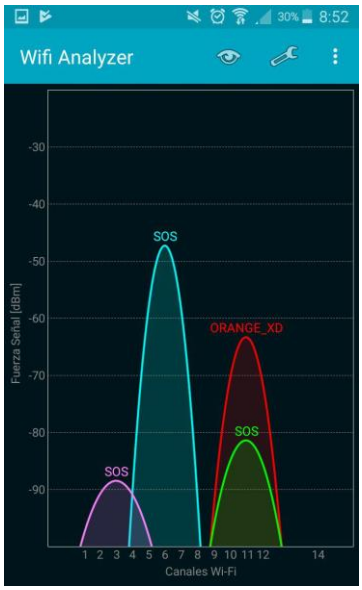


Figura 41. Gráfico de canales WiFi Analyzer

En la Figura 42 se muestra en la parte superior el nodo al que nuestro dispositivo cliente se encuantra conectado, así como el nivel de potencia de señal que recibe de los puntos de acceso de la red “SOS”.

Figura 42. Nivel de potencia recibida de la señal de red SOS

Conforme nos vamos alejando del nodo al que nos hemos conectado, nodo RPB, podemos observar como va disminuyendo la potencia de la señal correspondiente al nodo RPB.

Si a su vez nos vamos aproximando al nodo RPC, podemos apreciar también como la potencia de esta señal, correspondiente a la MAC y que trabaja sobre el canal 11, va aunmentando cada vez más. Podemos apreciar las variaciones de la potencia de ambas señales comparando la Figura 42 con la Figura 43.

Figura 43. Variaciones en la potencia de la señal de red SOS

Cuando las diferencias entre la señal de RPB y RPC son bastante notorias, nuestro dispositivo cliente abandona la connexion con el nodo RPB para conectarse al nodo RPC que presenta una major señal de red. Esta migración de un nodo a otro nodo de la red podemos evdenciarlo en la Figura 44.

Figura 44. Migración de un cliente a un nodo vecino

7. CONCLUSIONES

Con este trabajo de investigación, se ha logrado armar una infraestructura robusta capaz de proporcionar servicios de comunicaciones a los clientes que se conecten a ella, cumpliendo con las necesidades que la caracterizan por tratarse de una red móvil sobre UAVs.

El resultado de este estudio, marca el camino hacia la viabilidad de una futura red de comunicaciones libre capaz de llegar mucho más lejos en cuanto a funcionalidades y calidad del servicio de comunicaciones, dado que este estudio se ha llevado a cabo utilizando dispositivos que no han sido diseñados para operar como equipos de red.

Realizada esta tarea, quedaría por analizar la capacidad de crecimiento y escalado de nuestra red, pues en el escenario de simulación planteado solo han intervenido tres dispositivos Raspberry Pi. Habría que ver como funcionaría nuestra red cuando son muchos más los nodos que participen en su despliegue, así como las limitaciones en cuanto a ancho de banda se refiere de nuestros dispositivos inalámbrico a la hora de conectarse a más dos nodos de red y a un mayor número de clientes.

8. MEJORAS FUTURAS

Una de las posibles mejoras de nuestra red de comunicaciones, que resultaría de gran interés, es la capacidad de balanceo de carga entre nodos vecinos; de forma que si un nodo está muy congestionado en comparación con un nodo de red contiguo o vecino, puedan compartir el trabajo traspasandole algunos de los clientes que se encuentre dentro de su zona de cobertura.

Otro aporte importante, sería el de capacitar a la red de redundancia en el nodo principal, pues hemos visto cómo cualquier nodo de la red puede gestionar de forma automática a los clientes, siempre y cuando estén en su radio de cobertura, de un nodo vecino que haya quedado inhabilitado; pero sí es el nodo principal el que quedase inhabilitado, dado que es el único que tiene configurada una interfaz WAN con salida al exterior, nuestra servicio de comunicaciones quedaría inhabilitado.

En adición a esto, conforme se realizaba este studio, se echa en falta la creación de una base de datos capaz de recopilar en todo momento estadísticas sobre el tráfico y el número de usuarios actual de la red, de cada nodo, de cada enlace, de cada zona geográfica… Que nos serviría para dar un paso más, en cuanto a la mejora del servicio de nuestra red, añadiendole funcionalidades como pueden ser las de reubicar un nodo libre en una zona geográfica congestionada, concentrar más todos los nodos de la red o por el contrario expandirlos abarcando un mayor radio de cobertura.

REFERENCIAS

[1] L. Mesh, «Libre Mesh,» [En línea]. Available: http://libremesh.org/.

[2] «OpenWRT,» [En línea]. Available: https://wiki.openwrt.org/es/about/start.

[3] LEDE, «LEDE-project,» [En línea]. Available: https://lede-project.org/.

[4] A. M. N. Lab, «Advanced Mobile Network Lab,» [En línea]. Available: http://amnl.ulsan.ac.kr/research.html.

[5] R. P. Foundation, «Raspberry Pi Foundation,» [En línea]. Available: https://www.raspberrypi.org/.

[6] W. Analyzer, «WiFi Analyzer,» [En línea]. Available: https://play.google.com/store/apps/details?id=com.farproc.wifi.analyzer&hl=es.

[7] GPC, «Redes informáticas LAN, MAN y WAN: En qué se diferencian,» [En línea]. Available: https://gpcinc.mx/blog/redes-informaticas-lan-man-wan/.

[8] OpenWRT, «Client Mode Wireless,» [En línea]. Available: https://wiki.openwrt.org/doc/howto/clientmode.

9. ANEXO I – COMPILACIÓN DE LA IMAGEN DE LEDE

Para compilar una nueva imagen actualizada de LEDE, el firmware utilizado en este trabajo, se han seguido los pasos que se detallan a continuación.

Primero debemos asegurarnos de que las dependencias estén instaladas (para Debian / Ubuntu):

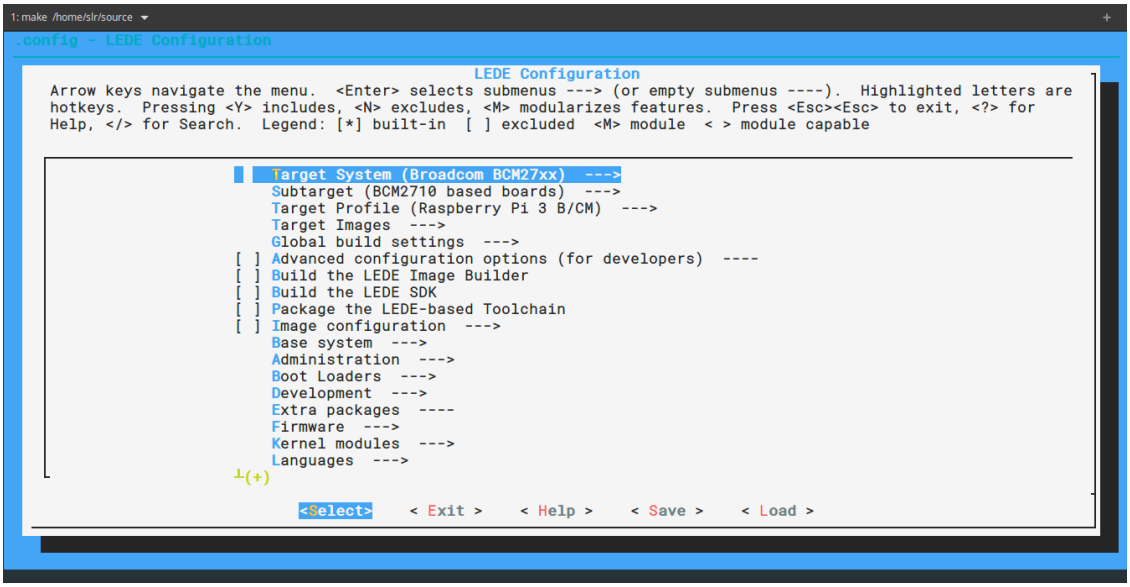
```
sudo apt-get install subversion g++ zlib1g-dev build-essential git python rsync man-db
sudo apt-get install libncurses5-dev gawk gettext unzip file libssl-dev wget
```

En segundo lugar, obtendremos el código fuente LEDE con los siguientes comandos:

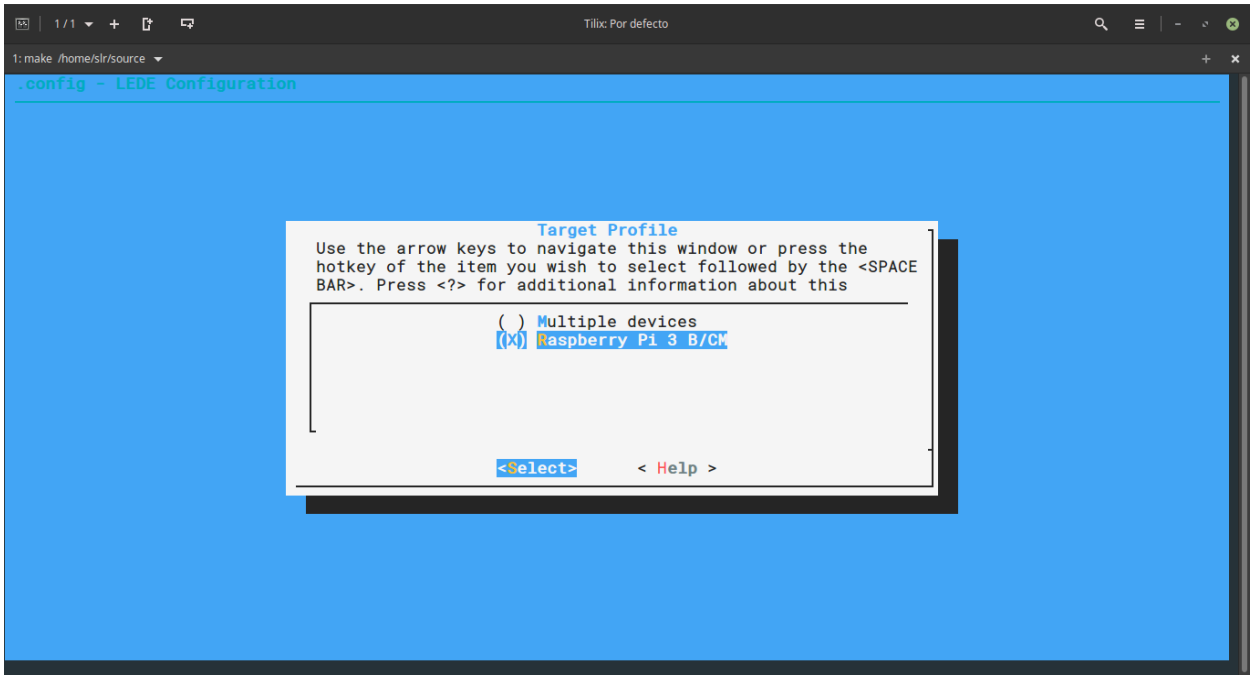
```
git clone https://git.lede-project.org/source.git lede
cd lede

./scripts/feeds update -a
./scripts/feeds install -a

make defconfig
make menuconfig
```

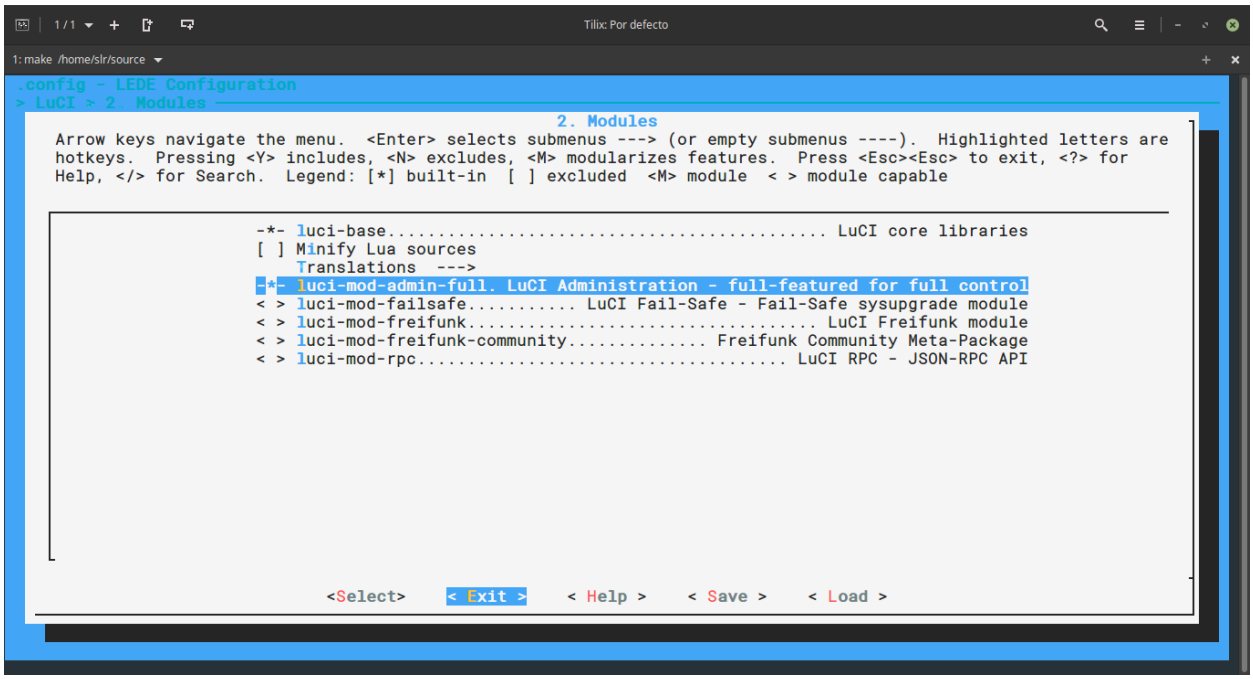
El último comando abrirá un menú.

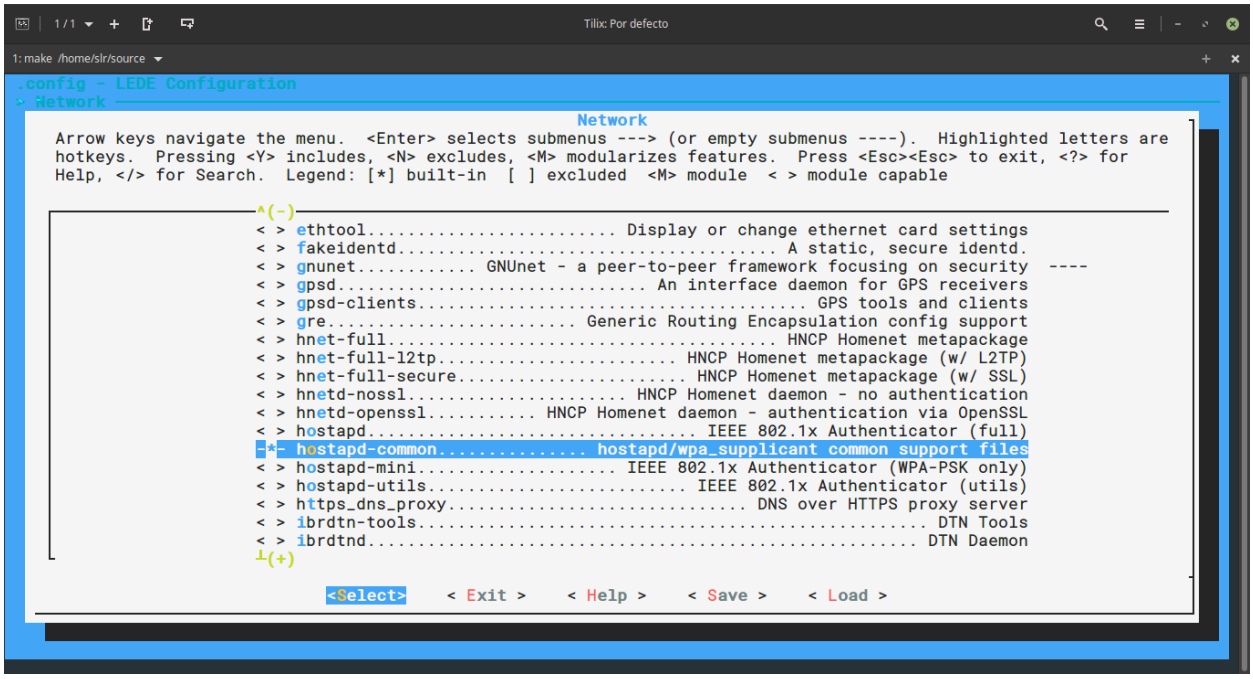
Desde este menú tendremos opción a instalar los paquetes y funcionalidades que deseamos. A continuación se muestran algunas capturas de cómo hemos configurado nuestra imagen.

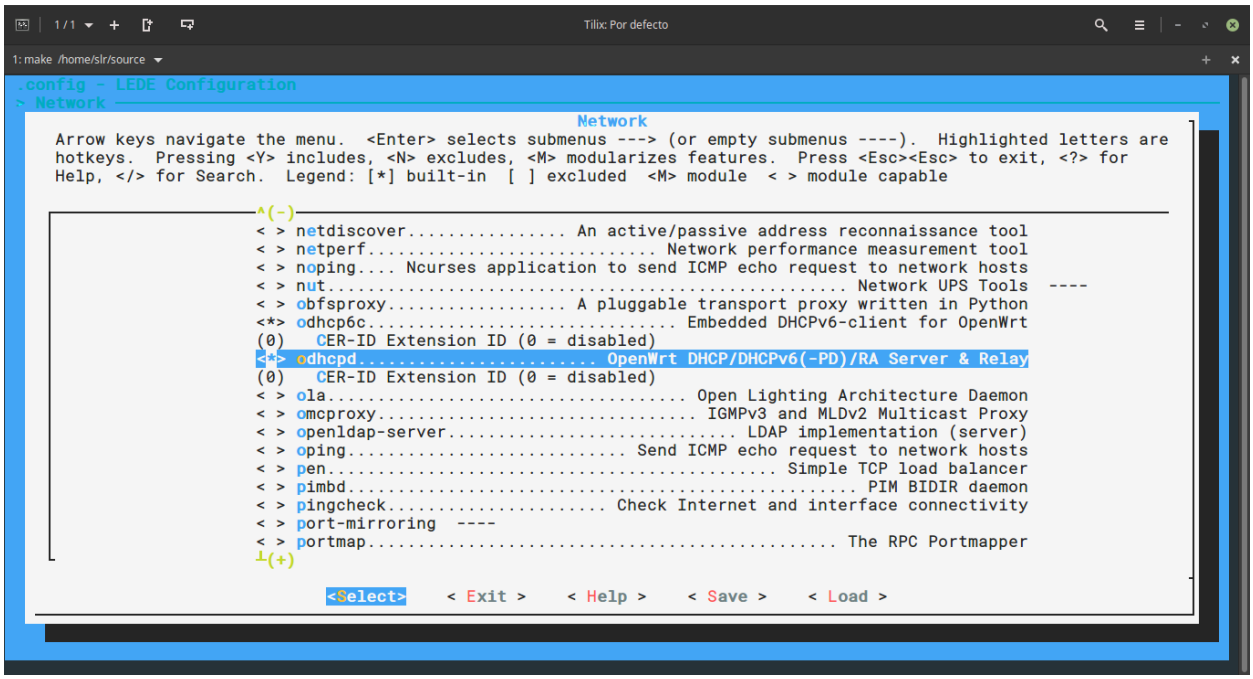


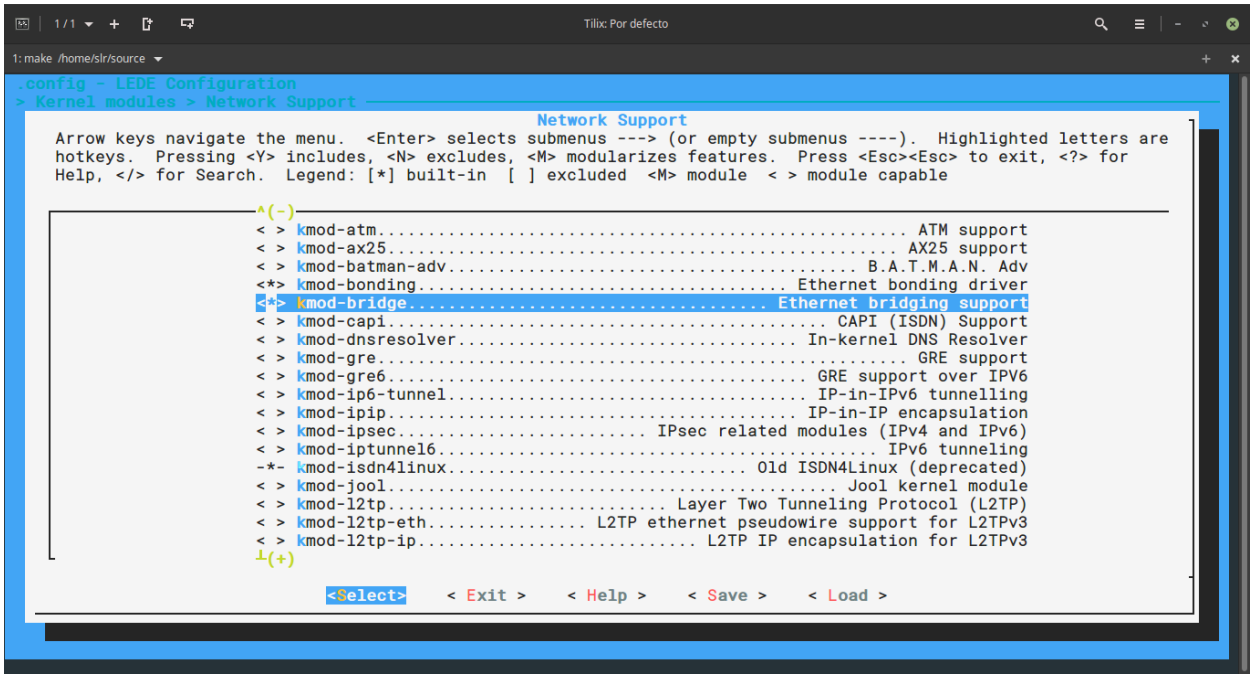

1: make /home/slr/source
.config - LEDE Configuration
Target System
Use the arrow keys to navigate this window or press the
hotkey of the item you wish to select followed by the <SPACE
BAR>. Press <?> for additional information about this
( ) Allwinner A1x/A20/A3x
( ) AppliedMicro APM821xx
( ) Atheros AR231x/AR5312
( ) Atheros AR7xxx/AR9xxx
( ) Atmel AT91
(X) Broadcom BCM27xx
<Select>
< Help >

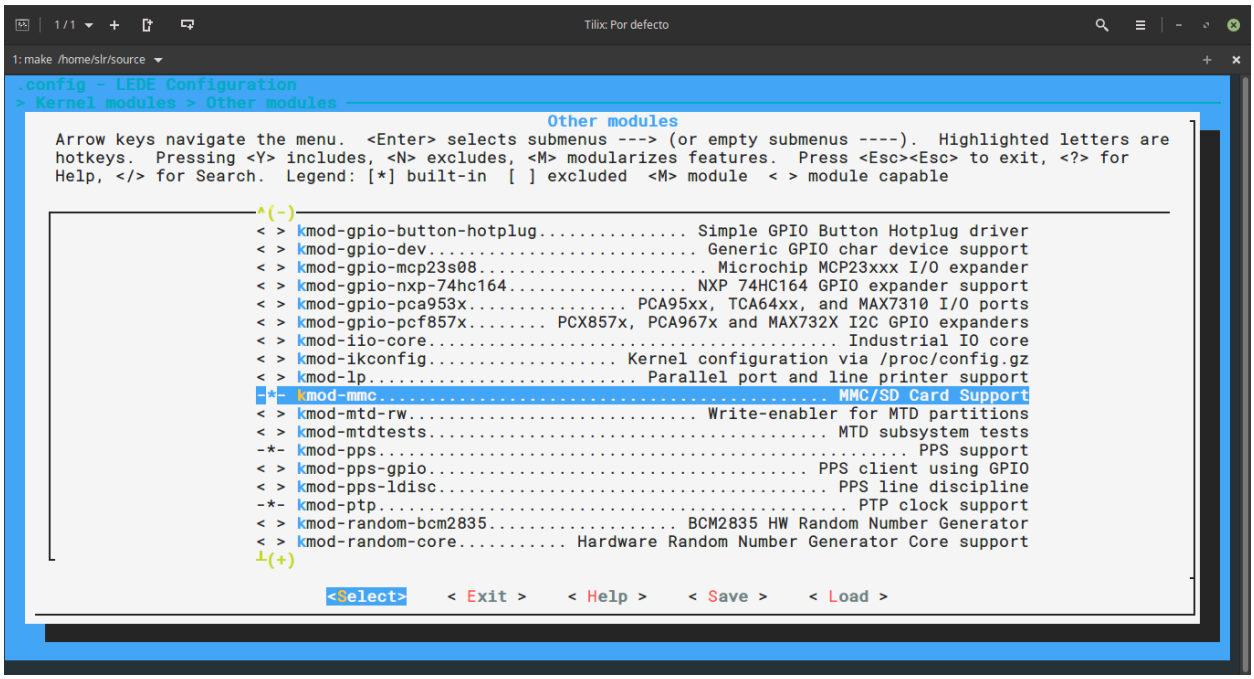

Tilix: Por defecto
1: make /home/slr/source
.config - LEDE Configuration
Target Profile
Use the arrow keys to navigate this window or press the
hotkey of the item you wish to select followed by the <SPACE
BAR>. Press <?> for additional information about this
( ) Multiple devices
(X) Raspberry Pi 3 B/CM
<Select>
< Help >

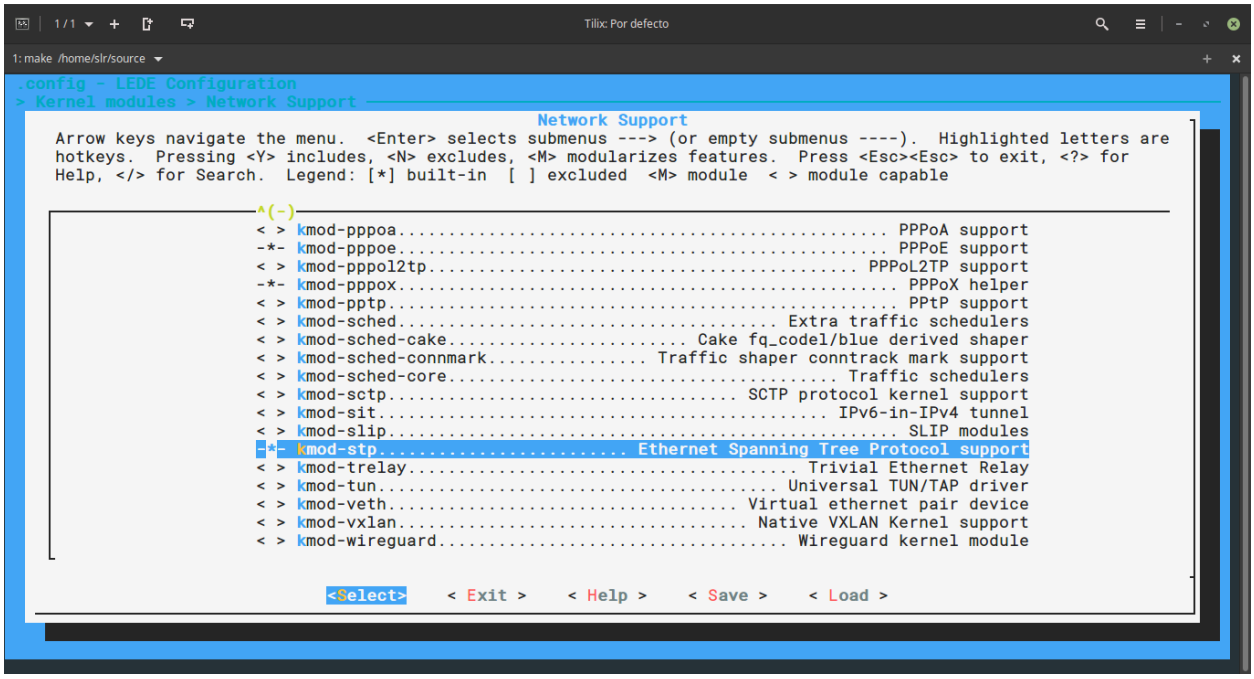

Tilix: Por defecto
1: make /home/slr/source
.config - LEDE Configuration
> LuCI > 2. Modules
2. Modules
Arrow keys navigate the menu. <Enter> selects submenus ---> (or empty submenus ----). Highlighted letters are hotkeys. Pressing <Y> includes, <N> excludes, <M> modularizes features. Press <Esc><Esc> to exit, <?> for Help, </> for Search. Legend: [*] built-in [ ] excluded <M> module < > module capable
-*- luci-base..... LuCI core libraries
[ ] Minify Lua sources
Translations --->
-*- luci-mod-admin-full. LuCI Administration - full-featured for full control
< > luci-mod-failsafe..... LuCI Fail-Safe - Fail-Safe sysupgrade module
< > luci-mod-freifunk..... LuCI Freifunk module
< > luci-mod-freifunk-community..... Freifunk Community Meta-Package
< > luci-mod-rpc..... LuCI RPC - JSON-RPC API
<Select> < Exit > < Help > < Save > < Load >


Tilix: Por defecto
1: make /home/slr/source
.config - LEDE Configuration
> Network
Network
Arrow keys navigate the menu. <Enter> selects submenus ---> (or empty submenus ----). Highlighted letters are hotkeys. Pressing <Y> includes, <N> excludes, <M> modularizes features. Press <Esc><Esc> to exit, <?> for Help, </> for Search. Legend: [*] built-in [ ] excluded <M> module < > module capable
^(-)
< > ethtool..... Display or change ethernet card settings
< > fakeidentd..... A static, secure identd.
< > gnunet..... GNUnet - a peer-to-peer framework focusing on security ----
< > gpsd..... An interface daemon for GPS receivers
< > gpsd-clients..... GPS tools and clients
< > gre..... Generic Routing Encapsulation config support
< > hnet-full..... HNCP Homenet metapackage
< > hnet-full-l2tp..... HNCP Homenet metapackage (w/ L2TP)
< > hnet-full-secure..... HNCP Homenet metapackage (w/ SSL)
< > hnetd-nossl..... HNCP Homenet daemon - no authentication
< > hnetd-openssl..... HNCP Homenet daemon - authentication via OpenSSL
< > hostapd..... IEEE 802.1x Authenticator (full)
-*- hostapd-common..... hostapd/wpa_supplicant common support files
< > hostapd-mini..... IEEE 802.1x Authenticator (WPA-PSK only)
< > hostapd-utils..... IEEE 802.1x Authenticator (utils)
< > https_dns_proxy..... DNS over HTTPS proxy server
< > ibrdtn-tools..... DTN Tools
< > ibrdtnd..... DTN Daemon
v(+)
<Select> < Exit > < Help > < Save > < Load >


Tilix: Por defecto
1: make /home/slr/source
.config - LEDE Configuration
> Network
Network
Arrow keys navigate the menu. <Enter> selects submenus ---> (or empty submenus ----). Highlighted letters are hotkeys. Pressing <Y> includes, <N> excludes, <M> modularizes features. Press <Esc><Esc> to exit, <?> for Help, </> for Search. Legend: [*] built-in [ ] excluded <M> module < > module capable
< > netdiscover..... An active/passive address reconnaissance tool
< > netperf..... Network performance measurement tool
< > noping.... Ncurses application to send ICMP echo request to network hosts
< > nut..... Network UPS Tools ----
< > obfsproxy..... A pluggable transport proxy written in Python
<*> odhcp6c..... Embedded DHCPv6-client for OpenWrt
(0) CER-ID Extension ID (0 = disabled)
<*> odhcpd..... OpenWrt DHCP/DHCPv6(-PD)/RA Server & Relay
(0) CER-ID Extension ID (0 = disabled)
< > ola..... Open Lighting Architecture Daemon
< > omcproxy..... IGMPv3 and MLDv2 Multicast Proxy
< > openldap-server..... LDAP implementation (server)
< > oping..... Send ICMP echo request to network hosts
< > pen..... Simple TCP load balancer
< > pimbd..... PIM BIDIR daemon
< > pingcheck..... Check Internet and interface connectivity
< > port-mirroring ----
< > portmap..... The RPC Portmapper
<Select> < Exit > < Help > < Save > < Load >


Tilix: Por defecto
1: make /home/slr/source
.config - LEDE Configuration
> Kernel modules > Network Support
Network Support
Arrow keys navigate the menu. <Enter> selects submenus ---> (or empty submenus ----). Highlighted letters are hotkeys. Pressing <Y> includes, <N> excludes, <M> modularizes features. Press <Esc><Esc> to exit, <?> for Help, </> for Search. Legend: [*] built-in [ ] excluded <M> module < > module capable
< > kmod-atm..... ATM support
< > kmod-ax25..... AX25 support
< > kmod-batman-adv..... B.A.T.M.A.N. Adv
<*> kmod-bonding..... Ethernet bonding driver
<*> kmod-bridge..... Ethernet bridging support
< > kmod-capi..... CAPI (ISDN) Support
< > kmod-dnsresolver..... In-kernel DNS Resolver
< > kmod-gre..... GRE support
< > kmod-gre6..... GRE support over IPV6
< > kmod-ip6-tunnel..... IP-in-IPv6 tunnelling
< > kmod-ipip..... IP-in-IP encapsulation
< > kmod-ipsec..... IPsec related modules (IPv4 and IPv6)
< > kmod-iptunnel6..... IPv6 tunneling
-*- kmod-isdn4linux..... Old ISDN4Linux (deprecated)
< > kmod-jool..... Jool kernel module
< > kmod-l2tp..... Layer Two Tunneling Protocol (L2TP)
< > kmod-l2tp-eth..... L2TP ethernet pseudowire support for L2TPv3
< > kmod-l2tp-ip..... L2TP IP encapsulation for L2TPv3
<Select> < Exit > < Help > < Save > < Load >





Una vez seleccionemos todos los paquetes que nos interesen, seleccionamos salir y guardamos la configuración. Ahora se procederá a construir una imagen. Eso puede llevar algún tiempo:

```
make
```

Si está compilando utilizando un equipo de varios núcleos, puede acelerar la compilación utilizando varios núcleos de CPU:

```
make -j N
```

donde N es su número de núcleos de la CPU + 1. Evite en la producción, ya que puede conducir a errores extraños y difíciles de detectar. Utilice la opción '-j' sólo si está familiarizado con el sistema de compilación.

Posteriormente, las imágenes se pueden encontrar en ./bin/targets/ar71xx/generic/ - done. 8-)

Las imágenes * -factory.bin son para la primera instalación. Las imágenes * -sysupgrade.bin son para la actualización de instalaciones existentes de LEDE.

Notas:

Para volver a compilar las imágenes, simplemente ejecuta make de nuevo.

Esto ahora será mucho más rápido también.

Cambia la configuración con make menuconfig y compila de nuevo.

Los archivos colocados en un directorio llamado archivos, se colocarán en el sistema de archivos raíz de las imágenes. P.ej. archivos / etc / config / my_config.