Free Europe WiFi

Justel Pizarro, Ignacio Alberto

Curs 2012-2013

Director: Albert Domingo Vilar

GRAU EN ENGINYERIA EN TELEMÀTICA

upf. Universitat Pompeu Fabra Barcelona
Escola Superior Politècnica

Treball de Fi de Grau

Agradecimientos

Son muchas las personas a las que debo palabras de agradecimiento por todo lo que me han aportado. No tan sólo en el aspecto más académico, sino también en lo más personal.

A mi familia, con los que puedo contar pase lo que pase. Son ellos los que me dan valor para seguir día a día, demostrando que trabajando con esfuerzo y sacrificio, todo es posible.

A Sandra, mi novia y compañera en la vida, por darme alas y hacerme disfrutar de cada momento. Por toda la confianza que ha depositado en mí desde siempre. Sin ella no sería lo que soy.

Al equipo de Provincia WiFi, ya que en el mes de octubre de 2012, llevamos a cabo una reunión con ellos en Bolonia, Italia. En ella se acordó y puso en común los términos para llevar a cabo el proyecto. Además, me aportaron información técnica del mismo para facilitar mi tarea de replicación. Al equipo de CINECA, con los cuales se realizó una reunión en el mes de abril de 2013, en Roma, para revisar el estado del proyecto, teniendo la suerte de presenciar un curso, sobre la arquitectura técnica e instrucciones para desplegar la solución OpenWISP, que se utilizó para llevar a cabo este piloto.

Al equipo del proyecto “Commons for Europe”, en especial a la rama “Bottom-up Broadband”, sin los que hubiese sido imposible vivir tantas experiencias enriquecedoras y confiaron en mí desde el primer momento. Este trabajo ha sido parcialmente financiado por la Comisión Europea, mediante el proyecto Commons for Europe (CIP-ICT-PSP-2011-5-297191).

Una mención especial para mis amigos y compañeros de laboratorio, dónde he podido desarrollar en buena compañía este trabajo. Sin duda, hemos vivido muy buenos e inolvidables momentos juntos.

Por último, y no por ello menos importante, a mi tutor Albert. Sin titubear, puedo afirmar que no es posible pedir un mejor mentor y guía. No sé qué hubiese sido de éste trabajo sin sus comentarios constantes, en muchos casos irónico-sarcásticos, con los que además de aprender un poco más, lograban que las horas dedicadas a este trabajo fuesen más entretenidas.

A todos ellos, **GRACIAS**.

Eternamente agradecido,

Nacho.

Resumen

En una sociedad cada vez más interconectada, y con una necesidad cada vez más latente de tener acceso a la información sin importar la ubicación del usuario, se propone ofrecer una red sin cables de acceso a Internet de manera gratuita para todos los ciudadanos de todos los países que conforman la Comunidad Europea.

Se llevó a cabo una comparativa entre diversas soluciones, tanto públicas como privadas, que ofrezcan un servicio similar. Además, se realizó un estudio sobre las implicaciones legales que tendría el despliegue en España respecto a las telecomunicaciones, y su relación con los requerimientos de libre mercado.

Para su utilización, se realizó un breve estudio del espectro radioeléctrico destinado al uso de WiFi en canales ISM en Barcelona.

La solución resultante del proyecto se ha obtenido al implementar una solución ofrecida por OpenWISP. El fin de este piloto es el de su futuro despliegue.

Palabras Clave: WiFi, hotspots, OpenWISP, regulación de espectro, gratuito, BuB “Bottom-up Broadband”, Commons for Europe

Abstract

Societies are increasingly interconnected, and globalization is bringing a need to access real-time information regardless of the user's location. A wireless network that provides Internet access, free of charge, to citizens of all countries of the European Community is offered in the framework of this project.

An analysis between different solutions that are offering a similar service has been carried out to both public and private initiatives. Furthermore, it has been conducted a study about the legal implications that the deployment has inside the Spanish telecommunications market, and its direct links to achieve the free-market requirements.

Besides the analysis, a brief study on the use of radio channel spectrum devoted to WiFi under designated use of ISM band, in the city of Barcelona, has been performed.

As a result, it was chosen a solution offered by OpenWISP for implementation. Test results were obtained in order to finally deploy the main idea of the project.

Keywords: WiFi network, access, hotspots, OpenWISP, spectrum regulation, free, BuB "Bottom-up Broadband", Commons for Europe

Introducción

A medida que la sociedad avanza, surge la necesidad de albergar unos mayores y estrechos lazos de comunicación. Ya no sólo en determinados momentos, sino que estar continuamente conectado con otras personas resulta imprescindible en la sociedad actual.

Es debido a este motivo que existen diferentes implementaciones (ya sea en cuanto a aspectos tecnológicos, como a motivos legales) en diversos ámbitos geográficos, por ejemplo municipios, ciudades o incluso países. Todas ellas buscan ofrecer una solución directa a estas nuevas necesidades sociales.

Surge entonces, la idea de crear una red que proporcione acceso a Internet de manera inalámbrica, abierta y gratuita para todos los ciudadanos que lo deseen. Además, y no menos importante, otra característica es que esta conexión será totalmente ubicua, es decir, independiente del lugar geográfico en dónde el usuario se encuentre o del cual provenga dentro del marco europeo. De esta manera, se provee de una nueva solución, a la necesidad continua de estar conectado.

Esta idea no sólo representa el ideal de un acceso libre y gratuito a la información y la tecnología, sino que también se presenta como un vínculo más para estrechar las relaciones entre los diferentes países, y por lo tanto, ciudadanos de la comunidad europea.

El proyecto no se diseñará desde una visión de "red libre y neutral", sino que basándose en el principio de los WISP[1], el proyecto diseñará una red gratuita inalámbrica "WiFi" [1] (de tipo B, G o N) que proporcione interconexión con otras redes de ámbito europeo. Este sistema se ofrecerá en dos ámbitos diferenciados: en establecimientos comerciales (bares, hoteles, restaurantes, etc.) y en el dominio público.

Está estrechamente relacionado, con un trabajo de implementación llevado a cabo como parte de un proyecto europeo denominado Commons for Europe [2]. Bajo el modelo Bottom-Up Broadband [3]. Un modelo que pretende establecer un nuevo punto de vista desde el cual la oferta de servicios de telecomunicaciones no parte desde las compañías, sino desde los propios ciudadanos.

La implementación del mismo se llevará a cabo a partir de OpenWISP[4]. Este es un software de libre distribución y modificación, que ofrece la capacidad de crear soluciones que den abasto a un completo servicio de acceso a Internet sin cables. Este software ha sido desarrollado y llevado a cabo dentro de un proyecto, Provincia WiFi[5], impulsado por el ayuntamiento de Roma, con el objetivo de dar soporte, abasto y acceso a Internet a todos sus ciudadanos. Este proyecto, se distribuye actualmente bajo licencia y filosofía de

[1] Ver capítulo 1

código abierto, de manera que cualquier interesado en él, puede modificar y/o mejorarlo con el objetivo de seguir creciendo.

La finalidad u objetivo de este sistema, es ofrecer una solución completa y estable para compartir conexiones privadas a Internet, al resto de la ciudadanía. Es entonces cuando cualquier usuario que desee compartir su conexión (ya sea para ofrecerlo como un valor añadido a su negocio, o por simple altruismo), puede hacerlo sin dificultad ninguna.

No obstante, existen en marcha otras alternativas a este sistema, que han sido analizadas y propuestas como posibles modelos a seguir. Estas soluciones se encuentran ya desplegadas en diferentes ciudades europeas como son Barcelona o París entre otras muchas como solución pública, y otras tantas de carácter propietario.

Si bien muchas de estas alternativas no han sido escogidas como el modelo a continuar en este proyecto, serán analizadas y comentadas más adelante.

El alcance de este proyecto, pretende establecer un nexo común a todas las soluciones de conectividad pública de acceso a Internet sin cables, ofrecida por cualquier Estado dentro de la Unión Europea.

Por lo tanto, y a modo de resumen final, podríamos decir que el objetivo final del proyecto es:

- Analizar, comprender y documentar la elección de la mejor tecnología o producto que provea una solución abierta, global y sensata a nivel europeo, para lograr ofrecer acceso gratuito a Internet a todos los ciudadanos de la misma, dentro del territorio comunitario.

- Comprender e interpretar de manera correcta los términos y aspectos legales que requiere un despliegue tecnológico de las Tecnologías de la Información y Comunicación "*TIC*" de semejantes características.

Índice

Índice de Ilustraciones

Índice de Tablas

CAPÍTULO 1: FASE INICIAL: INTRODUCCIÓN A LOS WISP, LEGISLACIÓN, DEMANDA DE MERCADO Y ELECCIÓN DE LA SOLUCIÓN A IMPLEMENTAR

1.1 Introducción a los WISP (Wireless Internet Service Provider).

Un WISP o "Wireless Internet Service Provider", es un proveedor de servicio de acceso a Internet con la particularidad de que sus conexiones son efectuadas mediante el uso del radioespectro en frecuencias libres o no, pero en ningún caso mediante conexiones cableadas.

Estos proveedores son comunes en zonas rurales dónde el número de clientes no es suficiente para amortizar una inversión del despliegue de las infraestructuras. No obstante, en los entornos urbanos, son idóneas para proporcionar cobertura en zonas de gran superficie y que requieran poco volumen de tráfico de datos. De esta manera, se puede dar cobertura de servicio a una gran parte de la ciudad, desplegando una infraestructura siempre menor que la necesaria por parte de un proveedor tradicional.

El objetivo de los WISP no suele ser el de competir con los proveedores tradicionales, sino complementar a los mismos en las zonas comentadas anteriormente. Debido a su relación inversión/cliente, su escalabilidad de crecimiento, su bajo mantenimiento y en resumen, su rentabilidad a corto-medio plazo, han hecho que este tipo de compañías aumenten considerablemente en los últimos tiempos.

1.2 Requerimientos legales. Legislación vigente.

En este apartado hablaremos sobre la legislación vigente de las telecomunicaciones, tanto a nivel Europeo, como en España, y como todo ello afecta al desarrollo de este proyecto.

Será revisada la documentación legislativa existente para dos posibles casos de uso distintos del objetivo de este proyecto. El primero, para ofrecer el servicio de conexión y acceso a Internet mediante tecnología inalámbrica WiFi, en frecuencias de dominio público (2,4Ghz y 5Ghz), en espacios abiertos. El segundo caso, se basa en ofrecer el mismo servicio, a establecimientos comerciales (hoteles, bares, restaurantes, etc…) para que estos lo oferten como un servicio extra y gratuito a sus clientes.

1.2.1 Europa

En lo que a la toma de decisiones en la jurisdicción dentro del territorio europeo se refiere, el encargado de regir el ámbito de las telecomunicaciones es el "Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (ORECE, también conocido como BEREC)".

La principal función de este organismo, es la de asesorar y asistir a la Comisión Europea, en el desarrollo de un mercado interno, haciendo de vínculo entre las diferentes ANR (Autoridades Nacionales de Reglamentación) y la Comisión. Por lo tanto, podemos decir que el ORECE contribuye al correcto funcionamiento del mercado europeo de redes y servicios de comunicaciones electrónicas.

Según estipula su reglamento **(CE 1211/2009)**, sus objetivos primordiales son:

- Desarrollar y difundir entre las ANR, buenas prácticas reguladoras, tales como planteamientos, metodologías o directrices comunes en relación con la aplicación del marco regulador de la UE;
- Ayudar a las ANR en cuestiones de reglamentación.
- Emitir dictámenes sobre los proyectos de decisiones, recomendaciones y directrices.
- Elaborar informes y proporcionar asesoramiento en relación con el sector de las telecomunicaciones.
- Asistir al Parlamento Europeo, el Consejo, la Comisión y las ANR en la difusión de buenas prácticas.

En lo relativo a este proyecto, ORECE otorga poder a las Autoridades Nacionales de Regulación en materia de regulación local. Obviamente, esta condición tendrá validez siempre y cuando, las políticas regidas por estos ANR se encuentren bajo la misma línea de regulación que el organismo europeo.

Respecto a lo que nos atañe, **la Directiva de la Unión Europea 2006/24/CE** exige que todos los establecimientos o lugares que ofrezcan acceso a Internet al público, mantengan registros detallados de sus usuarios durante al menos un año. Este registro detallado, se explica posteriormente, ya que la directiva de la Comisión del Mercado de las Telecomunicaciones, CMT, de España, adopta también esta directriz. En cualquier caso, la falta de cumplimiento de cualquiera de estas leyes, acarrea la clausura de la conexión y acciones judiciales.

De modo más genérico, cabe destacar el rumbo político que está adquiriendo la Unión Europea en materia de legislación de telecomunicaciones. Éste mismo año, la vicepresidenta de la Comunidad Europea y comisaria de la Agenda Digital, Neelie Kroes, ha instado a los parlamentarios europeos a establecer un mercado único europeo en materia de telecomunicaciones. Entre las medidas propuestas, se encuentra la eliminación de las tarifas de "Roaming" o "Itinerancia" de telefonía móvil, entre los países de la UE, o

salvaguardar el “derecho de acceder a un Internet abierto, garantizando la neutralidad de la red”.

Con estas directivas, se marca un rumbo claro en la que se propicia el crecimiento de la comunidad, eliminando barreras artificiales y unificando el mercado. Se estipula que de este modo, se fomentarán las inversiones de las empresas, propiciando el crecimiento económico, y se resguardará un derecho de la ciudadanía que cada vez más se presenta como fundamental.

1.2.2 España

En el territorio español, las telecomunicaciones están regidas por la Ley General de Telecomunicaciones del año 2003, bajo la tutela de la Secretaria de Estado de Telecomunicaciones y para la Sociedad de la Información, “SETSI”, perteneciente al Ministerio de Industria, Energía y Turismo.

En lo referente a la regulación de los operadores del mercado de telecomunicaciones, el encargado de regular el mercado, así como las reglas de competición, es la Comisión del Mercado de Telecomunicaciones, CMT[6].

1.2.3 Referente a la Comisión del Mercado de Telecomunicaciones, o CMT

Según reza su estatuto, la Comisión del Mercado de Telecomunicaciones se define como: “La Comisión del Mercado de Telecomunicaciones, Organismo Público regulador independiente de los mercados nacionales de comunicaciones electrónicas y de servicios audiovisuales, fue creada por el Real Decreto-Ley 6/1996, de 7 de junio, de Liberalización de las Telecomunicaciones. Dicho Real Decreto-Ley fue convalidado mediante la Ley 12/1997, de 24 de abril, de Liberalización de las Telecomunicaciones, a través de la cual se ampliaron y perfilaron las funciones que fueron inicialmente atribuidas a la Comisión del Mercado de las Telecomunicaciones y se definió una nueva composición del Consejo que ejercita dichas funciones.”

La Comisión del Mercado de Telecomunicaciones es un Organismo Público dotado de personalidad jurídica y plena capacidad pública y privada, así como de patrimonio propio, independiente del patrimonio del Estado.

Tiene por objetivo el establecimiento y supervisión de las obligaciones específicas que hayan de cumplir los operadores en los mercados de telecomunicaciones y el fomento de la competencia en los mercados de los servicios audiovisuales, conforme a lo previsto por su normativa reguladora, la resolución de los conflictos entre los operadores y, en su caso, el ejercicio como órgano arbitral de las controversias entre los mismos.

El día 15 de junio de 2010, el Consejo de la Comisión del Mercado de las Telecomunicaciones se reúne y se aprueba un documento llamado: "**Circular 1/2010, de la Comisión del Mercado de las Telecomunicaciones, por la que se regulan las condiciones de explotación de redes y la prestación de servicios de comunicaciones electrónicas por las Administraciones Públicas (MTZ 2010/203).**"

En esta circular, se comenta que el 25 de junio de 2009, se aprobó llevar a cabo a consulta pública, el "Informe sobre determinadas propuestas regulatorias en relación con la explotación de redes públicas inalámbricas basadas en la utilización de dominio público radioeléctrico a través de frecuencias de uso común (WiFi) y la prestación de servicios de comunicaciones electrónicas sobre las mismas por las Administraciones Públicas".

En ella, se estudian diversos temas relacionados con la explotación de redes y la prestación de servicios de comunicaciones electrónicas. Entre ellos, se detalla las condiciones a cumplir para la explotación de redes y prestación de servicios de comunicaciones electrónicas, que NO afectan a la competencia. Es decir, nuestro caso, el de este proyecto, ya que se desea ofrecer servicio gratuito para los usuarios y, por lo tanto, afectaría a la competencia.

Por lo tanto, se entiende que no afectan a la competencia, los siguientes servicios:

1. "El servicio de acceso a Internet limitado a páginas web de las Administraciones que tengan competencias en el ámbito territorial en que se preste el servicio."
2. "Servicio general de acceso a Internet en bibliotecas en tanto que resulte indispensable para cumplir sus fines y siempre que los usuarios acrediten su vinculación con el servicio mediante algún documento que permita su identificación."
3. "Servicio general de acceso a Internet en centro de fomentos de actividades docentes o educativo-culturales no incluidos en el artículo tercero de esta circular, en tanto que resulte imprescindible para cumplir sus fines y siempre que los usuarios acrediten su vinculación con el servicio mediante algún documento que permita su identificación."
4. "La explotación de redes inalámbricas que utilizan bandas de uso común y la prestación de servicios de comunicaciones electrónicas disponibles para el público a través de las mismas siempre que la cobertura de la red excluya los edificios y conjuntos de edificios de uso residencial o mixto***** y se limite la velocidad red-usuario a 256kbps."

*****En términos generales se entiende por edificio o vivienda de uso residencial aquél cuyos bienes de dominio particular se encuentren destinados a la vivienda de personas y por edificio de uso mixto aquel cuyos bienes se destinan a actividades de diversa naturaleza, tales como oficina, comercio o vivienda.

Por lo tanto, y a modo de resumen funcional, nos hemos de centrar en los puntos 1 y 4 de la lista comentada. No obstante, existen otras implicaciones legales a tener en cuenta. Estas están relacionadas con la conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicación.

La Ley 27/2007, de 18 de octubre, "**de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicación**", pone de manifiesto, las obligaciones de los operadores de telecomunicaciones de retener determinados datos generados o tratados por los mismos, con el fin de posibilitar que dispongan de ellos los agentes facultados (Cuerpos Policiales, Centro Nacional de Inteligencia o Dirección Adjunta de Vigilancia Aduanera en marco de una investigación criminal o de seguridad).

Por la misma, se destaca que los datos que deben conservarse por los operadores especificados en esta Ley, respecto al acceso a Internet, son los siguientes:

a. Datos necesarios para rastrear e identificar el origen de una comunicación:
    i. La identificación del usuario asignada.
    ii. La identificación del usuario y el número de teléfono asignados a toda la comunicación que acceda a la red pública de telefonía.
    iii. El nombre y dirección del abonado o del usuario registrado al que se le ha asignado en el momento de la comunicación una dirección del protocolo de Internet (IP), una identificación de usuario o un número de teléfono.
b. Datos necesarios para identificar el destino de una comunicación:
    i. La identificación del usuario o el número de teléfono del destinatario o de los destinatarios de una llamada telefónica por Internet.
    ii. Los nombres y direcciones de los abonados o usuarios registrados y la identificación de usuario del destinatario de la comunicación.
c. Datos necesarios para determinar la fecha, hora y duración de una comunicación:
    i. La fecha y hora de conexión y desconexión del servicio de acceso a Internet registradas, basadas en un determinado huso horario, así como la dirección del Protocolo Internet, ya sea dinámica o estática, asignada por el proveedor de acceso a Internet a una comunicación, y la identificación de usuario o del abonado o del usuario registrado.

ii. La fecha y hora de la conexión y desconexión del servicio de correo electrónico por Internet o del servicio de telefonía por Internet, basadas en un determinado huso horario.

d. Datos necesarios para identificar el tipo de comunicación
    i. El servicio de Internet utilizado.
e. Datos necesarios para identificar el equipo de comunicación de los usuarios o lo que se considera ser el equipo de comunicación:
    i. El número de teléfono de origen en caso de acceso mediante marcado de números.
    ii. La línea digital de abonado (DSL) u otro punto terminal identificador del autor de la comunicación.
f. Datos necesarios para identificar la localización del equipo de comunicación móvil:
    1. La etiqueta de localización (identificador de la celda) al inicio de la comunicación.
    2. Los datos que permiten fijar la localización geográfica de la celda, mediante referencia a la etiqueta de localización, durante el periodo en el que se conservan los datos de las comunicaciones.
    3. Ningún dato que revele el contenido de la comunicación podrá conservarse en virtud de esta Ley.

En el caso de la conservación de datos, en lo relativo al tiempo o periodo de conservación, la Ley estipula lo siguiente:

1. La obligación de conservación de datos impuesta cesa a los doce meses computados desde la fecha en que se haya producido la comunicación. Reglamentariamente, previa consulta a los operadores, se podrá ampliar o reducir el plazo de conservación para determinados datos o una categoría de datos hasta un máximo de dos años o un mínimo de seis meses, tomando en consideración el coste del almacenamiento y conservación de datos, así como el interés de los mismos para los fines de investigación, detección y enjuiciamiento de un delito grave, previa consulta a los operadores.
2. Lo dispuesto en el apartado anterior se entiende sin perjuicio de lo previsto en el artículo 16.3 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, sobre la obligación de conservar datos bloqueados en los supuestos legales de cancelación.

No obstante, en el caso que las comunicaciones ofrecidas por el sistema propuesto durante este proyecto, se llevasen a cabo dentro de algún local comercial, y por tanto, fuesen ofrecidos por los mismos, las directrices a la cual ha de regirse son diferentes.

En este último caso, la Comisión del Mercado de Telecomunicaciones, llevó a cabo un informe llamado "Informe sobre la consideración como inscribibles en el registro de operadores de actividades de comunicaciones electrónicas realizadas por establecimientos comerciales (como hoteles, restaurantes, cafeterías, centros comerciales)" (de 26 de julio de 2010) para determinar la necesidad de inscripción, o no, de los proveedores de servicios de comunicaciones electrónicas dentro de establecimientos comerciales.

En el citado documento, y para proponer una solución, primero la CMT tomó en consideración el tratamiento de estos casos en diversos países de la comunidad europea. Para ello, se contemplaron los criterios y el tratamiento regulatorio llevado a cabo por algunas "Autoridades Nacionales de Reglamentación" (ANRs), para calificar el servicio ofrecido por los locales comerciales a sus clientes:

- Chipre
    - Tras el análisis del mercado de acceso a banda ancha al por mayor, de la Recomendación sobre Mercados de 17 de diciembre de 2007 de la Comisión Europea (Relativa a los mercados pertinentes de productos y servicios dentro del sector de las comunicaciones electrónicas), su ANR ha concluido que los servicios de banda ancha prestados vía puntos de acceso Wi-Fi en aeropuertos, hoteles y cafeterías no entran en el ámbito de dicho mercado, ya que:
        - Los clientes que gozan del servicio es esas ubicaciones, se encuentran de paso, y no de manera fija.
        - No se proporciona una velocidad constante de conexión, sino que depende del número de usuarios conectados en ese momento.

- Finlandia
    - Si bien, la Ley finlandesa ("**Application of the communicactions market legislation to the provision of wireless broadband connections", FICORA**[2]) no define explícitamente el concepto de "servicios de comunicaciones electrónicas", regula estos servicios cuando se encuentran disponibles al público en general. Por lo tanto, el servicio ofrecido en locales comerciales de poder acceder a comunicaciones electrónicas de cualquier tipo, no se consideran como un servicio disponible al público en general, ya que están destinados a los clientes del propio local.

- Francia

[2] Finnish Communications Regulatory Authority. 2013. FICORA. Consultado 12/03/2013. http://www.ficoria.fi/en/

- Se obliga a todos los operadores de redes que utilizan tecnología WiFi, a declarar su actividad al ANR. Se entiende como operador, a toda persona física o jurídica que explote una red de comunicaciones electrónicas abierta al público, o preste servicios de la misma. No obstante, existen casos en los que no se exige la notificación:
  - Redes reservadas a un uso privado
  - Establecimiento y explotación de "redes internas abiertas al público", así como la prestación al público de servicios sobre estas redes. Por "red interna abierta al público", se considera que son todas las redes que están establecidas sobre una misma propiedad y no se extienden ni al dominio público, ni a la propiedad de terceros (por ejemplo hoteles, aeropuertos…).
  - Las redes independientes reservadas al uso de una o más personas que conformen un grupo cerrado de usuarios (por ejemplo redes de empresas).

- Grecia
  - Según la legislación griega de telecomunicaciones, sólo en el caso de que el local comercial crease su propia marca para ofrecer a sus clientes servicios de banda ancha, entonces sería considerado operador de comunicaciones electrónicas, estaría obligado a notificar a la ANR su intención de prestar ese servicio.

- Lituania
  - Todo local comercial que preste servicio de banda ancha a sus clientes, no debe notificar a la ANR, ya que se considera que simplemente presta un servicio extra a sus clientes.

- Malta
  - Si la prestación de servicios de comunicaciones electrónicas se lleva a cabo dentro del límite de la edificación del local comercial, la ANR la califica como una prestación interna o privada, y por lo tanto, queda exenta de ser considerado como operador de comunicaciones electrónicas.

- Polonia
  - Al igual que en Malta, los servicios que los locales comerciales ofrezcan a sus clientes, son considerados servicios adicionales o complementarios, y por lo tanto no es necesario notificar a la ANR.

- Reino Unido

- El regulador independiente y autoridad de competencia para la industria de comunicaciones del Reino Unido (OFCOM[3]), no considera como operadores de redes abiertas ni prestadores de servicios de comunicaciones electrónicas para el público en general, a los locales comerciales que ofrezcan el servicio de banda ancha. El organismo considera, que este servicio es ofrecido en exclusiva a los clientes del local comercial, y por lo tanto, no existe ningún motivo para llevar a cabo una notificación oficial al respecto por parte de los establecimientos. No obstante, según la Ley de Economía Digital de 2010, "**Digital Economic Act 2010**", si la conexión WiFi se ofrece totalmente gratuita, toda responsabilidad recae sobre el abonado a esta conexión. Esto se debe a que entonces, la red ofrecida por el abonado se considera una "red de comunicaciones electrónicas públicas" (Public Electronic Communications Network, PECN) según la Ley de Comunicaciones, "Communications Act".

- Suiza
  - Al igual que en el resto de casos, la prestación de servicios de banda ancha en locales comerciales, no constituye una oferta al público en general ya que se encuentran destinadas a los clientes de dichos establecimientos. Por lo tanto, se trataría de una explotación de una red privada, y de prestación interna, y no existe exigencia de notificar a la ANR.

- Croacia, Eslovenia, Hungría, República Checa y Rumanía
  - En todos estos países, los establecimientos comerciales son considerados como clientes de algún ISP "Internet Service Provider", y por lo tanto, no son considerados como operadores de servicios de comunicaciones electrónicas. En definitiva, no existe obligación ni motivo alguno para notificar a sus respectivas ANR sobre la prestación del servicio.

Aquí concluye el contenido del informe de la CMT, anteriormente comentado. A modo de resumen de lo anteriormente citado, los titulares de los locales comerciales que ofrezcan servicios de comunicaciones electrónicas a sus clientes, no tienen en ningún caso la obligación de notificar su intención de prestar estos servicios. Esto se debe a que este tipo de explotación se considera explotación de redes privadas, de prestación interna o auto-prestación.

[3] Independent regulator and competition authority for the UK communication industries. 2013. OFCOM. Consultado 12/03/2013. http://www.ofcom.org.uk/

Por lo tanto, y después de que la CMT realizase un informe teniendo en cuenta el resto de países europeos, se llega a la siguiente conclusión, en la que hay que diferencias dos casos:

1. El proveedor de acceso a Internet o ISP, presta directamente el servicio en el interior de hoteles, cafeterías, etc. a los clientes de dichos establecimientos.

   En este supuesto, el ISP preste en su propio nombre y representación el servicio de acceso a Internet a los clientes del local. Por lo tanto, se entiende que existe una relación contractual directa entre los clientes del local comercial y el ISP (que es el responsable del transporte de la señal y de establecer las condiciones de uso del servicio).

   En estos casos, el titular o dueño del local comercial, no interviene en dicha relación, y en caso de intervenir, no oculta que el verdadero prestador es el ISP.

   El prestador del servicio, ISP, se responsabilizará del transporte de la señal y de salvaguardar los derechos de los usuarios receptores del servicio.

2. El establecimiento comercial facilita el servicio de acceso a Internet a sus clientes, sin existir relación directa entre el proveedor del mismo, ISP, y los consumidores finales.

   En este supuesto, el titular del establecimiento comercial, contrata con un ISP, la prestación del servicio de acceso a Internet, y lo pone a disposición de sus clientes. Lo que en realidad hace pues, es dejar abierto su acceso a Internet, y cobrar una pequeña cantidad por el servicio, facturándolo a sus clientes con el resto de servicios ofrecidos por el establecimiento. Además, instala el equipamiento requerido por una conexión inalámbrica, para que sus clientes puedan disfrutar de él.

Se concluye entonces, que el titular del establecimiento comercial no debe ser considerado como prestador de servicios de comunicaciones electrónicas, ni revendedor del mismo por los siguientes motivos:

- El titular del establecimiento no se responsabiliza frente a los usuarios finales en lo que a la señal se refiere.
- El servicio de comunicaciones electrónicas ofrecido no representa la actividad principal que presta el establecimiento a sus usuarios, aun cuando factura por ello.

- Los destinatarios del servicio ofrecido son únicamente las personas que tengan la condición de clientes de los establecimientos, estando restringido la cobertura del servicio al interior de las instalaciones del establecimiento.

Por lo tanto, y velando por los objetivos de este proyecto, no existe necesidad de darse de alta como operador, y por lo tanto, notificar a la CMT. Esto se debe a que el servicio, tal y como se ha comentado en puntos anteriores, se ofrecerá en dos ámbitos bien diferenciados:

1. En locales comerciales: se ofrecerá el servicio a bares, restaurantes, hoteles, etc… En ningún caso, se considerará a este proyecto como operador de redes de comunicación, por lo que no es necesario notificar a la Comisión del Mercado de Telecomunicaciones.

2. En ámbitos públicos: tal y como hemos visto, las comunicaciones tendrán que estar restringidas bajo las directrices que ha puesto la CMT, tanto en materia de velocidad de transmisión, como en horario de utilización o identificación de usuarios, para no ser considerado como servicio sustitutivo. En otro caso, la Ley consideraría al operador de servicio, operador de redes de comunicación, y por lo tanto, es necesario notificar a la CMT sobre esta actividad.

1.2.4 Italia

Debido a que este proyecto, tal y como veremos más adelante, se encuentra relacionado con su homónimo Italiano, se llevará a cabo una pequeña reseña sobre la legislación relativa a las telecomunicaciones en ese país.

El organismo regulador (o ANR) en el país transalpino se denomina “Autorità per le Garanzie nelle Comunicazione, AGCOM”, y se encuentra sujeto bajo el Ministerio de Comunicaciones, “MINISTERO DELLE COMUNICAZIONI”.

Éste determina bajo el Decreto del Ministro de Comunicaciones, de 28 de mayo de 2003 sobre "las condiciones para la concesión de autorizaciones generales para la prestación al público de la red LAN de radio y servicios de telecomunicaciones", publicado en la Gaceta Oficial no. 126, de 3 de junio de 2003; la normativa necesaria para poder prestar servicio de conexión a Internet al público de manera inalámbrica.

De manera sintética, decreta en su artículo tercero, que la prestación del servicio estará supeditada a una autorización general, en las condiciones establecidas en el artículo sexto del mismo documento. Para conseguir dicha autorización, las partes que deseen prestar el servicio mencionado, han de tener su domicilio social en el propio país, en uno de los países del Espacio Económico Europeo, en uno de los países pertenecientes a la Organización Mundial del Comercio "OMC", u otros países con los que existen acuerdos de reciprocidad en el ámbito regulado por éste documento. Todos éstos, tienen la obligación de presentar al Ministerio de Comunicaciones, una declaración incluyendo toda la información necesaria para verificar el cumplimiento de las condiciones previstas en el artículo sexto. Se extrae por ende, que **todo interesado en ofrecer este servicio, se encuentra obligado a inscribirse en el registro de operadores de comunicación**.

Respecto a la conservación de datos en relación a los usuarios, queda supeditado al decreto legislativo n. 109, "Aplicación de la Directiva 2006/24/CE sobre la conservación de datos generados o tratados en relación a la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y modificación de la Directiva 2002/58/CE" de 30 de mayo de 2008, publicada en la Gaceta Oficial no. 141 de 18 de junio de 2008.

En el artículo segundo de ésta, se estipula que el periodo de conservación de datos del tipo electrónico será de 12 meses en condiciones normales, siendo reemplazado los 6 meses estipulados anteriormente, y 2 años como máximo. Además, en el artículo tercero, se definen e indica el tipo de dato que debe retenerse, en cuanto a patrones de tráfico de datos. Las categorías son las siguientes:

- Nombre y dirección del abonado o del usuario registrado al que se le asignó una dirección IP única.
- La dirección IP utilizada, la dirección de correo electrónico y la identidad de la dirección IP del remitente, así como el nombre completo del dominio del host de intercambio de correos para el envío o recepción de e-mail.
- La dirección IP utilizada, número de teléfono y los datos personales del remitente en el caso de los servicios de telefonía a través de Internet.

Además, y extendiendo la Directiva Europea 2006/24/CE "sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas", de 15 de marzo de 2006, publicada en el Boletín Oficial de ' Unión Europea no. L 105/54, de 13 de abril 2006, se indica que deben ser retenidos los siguientes datos:

- La fecha y hora de la conexión y desconexión del servicio de acceso a Internet, basadas en un determinado huso horario.

1.2.5 Tabla Comparativa Legislación Europa - España – Italia

Tabla 1: Comparativa Legislación Europa-España-Italia

	España	Italia	Europa (BEREC)
Periodo de retención de datos personales	Mínimo de 6 meses, máximo de 2 años.	Mínimo de 12 meses, máximo de 2 años.	Mínimo de 6 meses, máximo de 2 años.
Conservación de datos personales	• Identificación (nombre y dirección), número de teléfono, línea digital de abonado (DSL) u otro punto terminal identificador y dirección IP (dinámica o estática, asignada por el ISP) del usuario o abonado. • Identificación (nombre y dirección) del usuario y/o el número de teléfono del/los destinatarios de una llamada sea por Internet o no, incluyendo aquellos casos en los que intervengan otros servicios, como desvíos de llamada o transferencia de llamada. • Fecha y hora de conexión y desconexión de la comunicación, del servicio de acceso a Internet, así como del servicio de correo electrónico por Internet o de telefonía por Internet. El servicio de Internet utilizado. • La etiqueta de localización (identificador de la celda) al inicio de la comunicación. • Los datos que permiten fijar la localización geográfica de la celda, mediante referencia a la etiqueta de localización, durante el periodo en el que se conservan los datos de las comunicaciones. • Ningún dato que revele el contenido de la comunicación podrá conservarse en virtud	• Nombre y dirección del abonado o del usuario registrado al que se le asignó una dirección IP única. • La dirección IP utilizada, la dirección de correo electrónico y la identidad de la dirección IP del remitente, así como el nombre completo del dominio del host de intercambio de correos para el envío o recepción de e-mail. • La dirección IP utilizada, número de teléfono y los datos personales del remitente en el caso de los servicios de telefonía a través de Internet. • La fecha y hora de la conexión y desconexión del servicio de acceso a Internet, basadas en un determinado huso horario.	• Identificación (nombre y dirección), número de teléfono, línea digital de abonado (DSL) u otro punto terminal identificador y dirección IP (dinámica o estática, asignada por el ISP) del usuario o abonado. • Identificación (nombre y dirección) del usuario y/o el número de teléfono del/los destinatarios de una llamada sea por Internet o no, incluyendo aquellos casos en los que intervengan otros servicios, como desvíos de llamada o transferencia de llamada. • Fecha y hora de conexión y desconexión de la comunicación, del servicio de acceso a Internet, así como del servicio de correo electrónico por Internet o de telefonía por Internet. El servicio de Internet utilizado. • La etiqueta de localización (identificador de la celda) al inicio de la comunicación. • Los datos que permiten fijar la localización geográfica de la celda, mediante referencia a la etiqueta de localización, durante el periodo en el que se conservan los datos de las comunicaciones. • La identidad internacional (IMSI, IMEI) de ambas

	de esta Ley.		partes de la comunicación. En el caso de servicios prepago anónimos, fecha y hora de la primera activación del servicio y la etiqueta de localización de la celda de la que se haya activado. • Ningún dato que revele el contenido de la comunicación podrá conservarse en virtud de esta Ley.
Obligatoriedad de notificación a la ANR	Dependiendo del área de cobertura del servicio: 1. <u>En locales comerciales:</u> No es necesario notificar a la Comisión del Mercado de Telecomunicaciones. 2. <u>En ámbitos públicos:</u> las comunicaciones tendrán que estar restringidas bajo las directrices impuestas por la CMT, tanto en materia de velocidad de transmisión, como en horario de uso o identificación de usuarios, para no ser considerado como servicio sustitutivo. En otro caso, es necesario notificar a la CMT sobre esta actividad.	Todo interesado en ofrecer este servicio, se encuentra obligado a inscribirse en el registro de operadores de comunicación.	Bajo la normativa de cada ANR
Restricciones del servicio	Dependiendo de si existe notificación y registro en la CMT: <u>Si existe notificación y registro:</u> No existen limitaciones legales sobre el servicio ofrecido. <u>Si no existe notificación y registro:</u> El servicio de acceso a Internet ha de estar limitado a páginas web de las Administraciones que tengan competéncias en el ámbito territorial. Podrá ser ofrecido en bibliotecas, centros de actividad docente, fomento cultural o actividades educativo-culturales, siempre y cuando los usuarios acrediten su vinculación con el servicio mediante algún documento que permita su identificación, y que el servicio sea primordial para ofrecer la actividad objetivo del	No existen limitaciones legales sobre el servicio ofrecido.	Bajo la normativa de cada ANR

	centro. En dominios públicos mediante las bandas ISM comúnes, podrá ofrecerse el servicio siempre que la cobertura del mismo excluya edificios y conjuntos de edificios residenciales o mixto (oficina – vivienda - comercio) y su velocidad máxima de transmisión se limite a 256 kbps.		

1.3 Estadísticas de uso de WiFi en España

El Instituto Nacional de Tecnologías de la Comunicación, INTECO, lleva a cabo cuatrimestralmente un estudio sobre la seguridad de las redes inalámbricas WiFi en los hogares españoles. Del estudio llevado a cabo en el primer cuatrimestre de 2012, podemos observar ciertos datos de relevancia para la realización de este proyecto.

De acuerdo a la figura 1, prácticamente el 80% de los encuestados utilizan una conexión a Internet sin cables, WiFi. En España, existen ya más de 11,52 millones de líneas de banda ancha, según la nota mensual de noviembre de 2012, de la CMT sobre las "Líneas de Banda Ancha en España". Estos datos, sumados a que es el 5º país europeo con mayor penetración de conexiones WiFi en casa, según el estudio "Broadband and Wi-Fi Households Global Forecast 2012"[7], llevado a cabo por Strategy Analytics Connected Home Devices; nos muestra la existencia un enorme mercado potencial de usuarios de conexiones WiFi al que apuntar con esta solución.

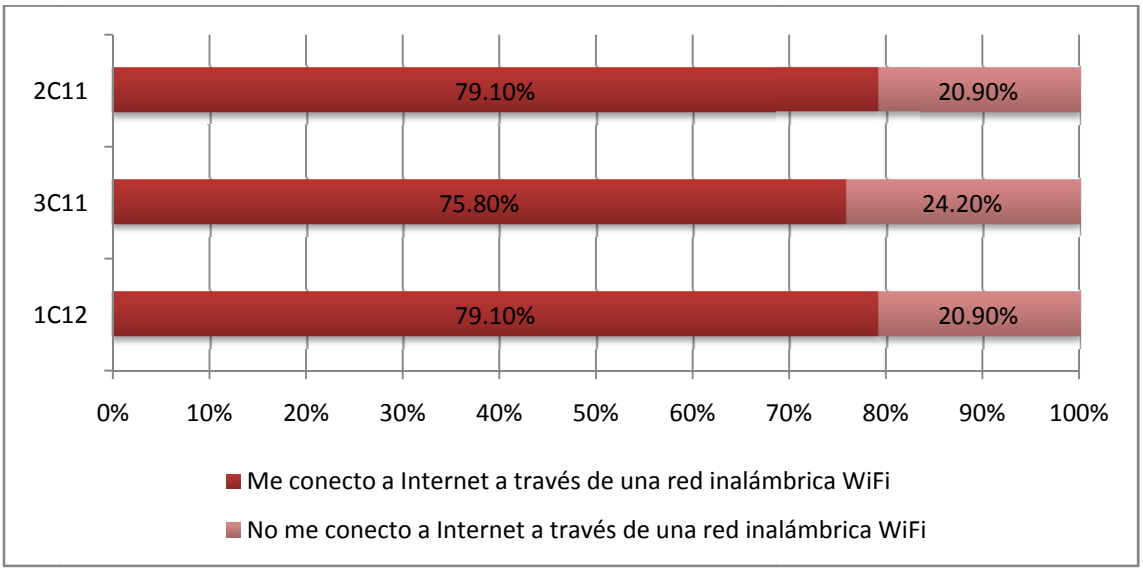


Figura 1: Evolución del nivel de utilización de redes inalámbricas WiFi (%)[4]

[4] Base: Total Usuarios (n=3.646 en 1er cuatrimestre 2012). Fuente: INTECO

Como observamos en la figura 2, poco más del 20% de los usuarios de Internet encuestados, se conectan frecuentemente a redes públicas, como pueden ser las provenientes de ayuntamientos, cafeterías o restaurantes. Teniendo en cuenta el número de usuarios habituales de Internet en España, y que esta solución pretende no sólo dar abasto local, sino pretende servir más allá de fronteras geográficas, obtenemos un inmenso número de potenciales consumidores. Este hecho alienta aún más la creación de una solución de este tipo, que ayude a aunar esfuerzos de comunicación entre diferentes países.

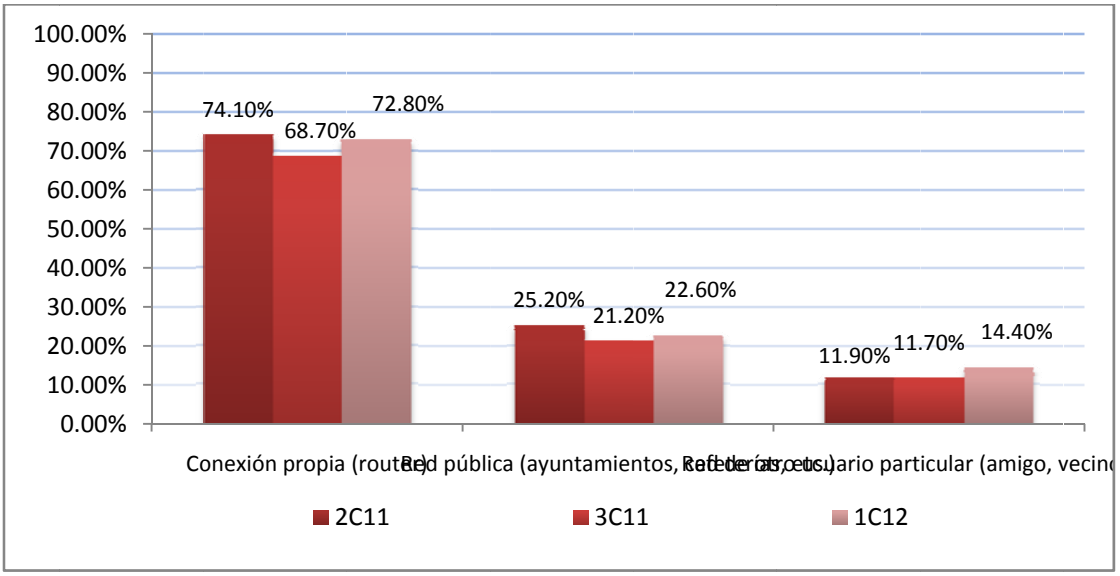


Figura 2: Evolución del punto de conexión a Internet a través de redes inalámbricas WiFi (posibilidad de respuesta múltiple) (%)[5]

De acuerdo con los datos extraídos en el informe económico sectorial de carácter anual de 2011, en la nota mensual de enero del 2013 de la CMT, resaltamos los siguientes datos reflejados en la figura 3. Vemos que el número de dispositivos móviles en el primer mes del año 2013, alcanza más de 52 millones de líneas móviles.

[5] Base: Total Usuarios (n=3.646 en 1er cuatrimestre 2012). Fuente: INTECO

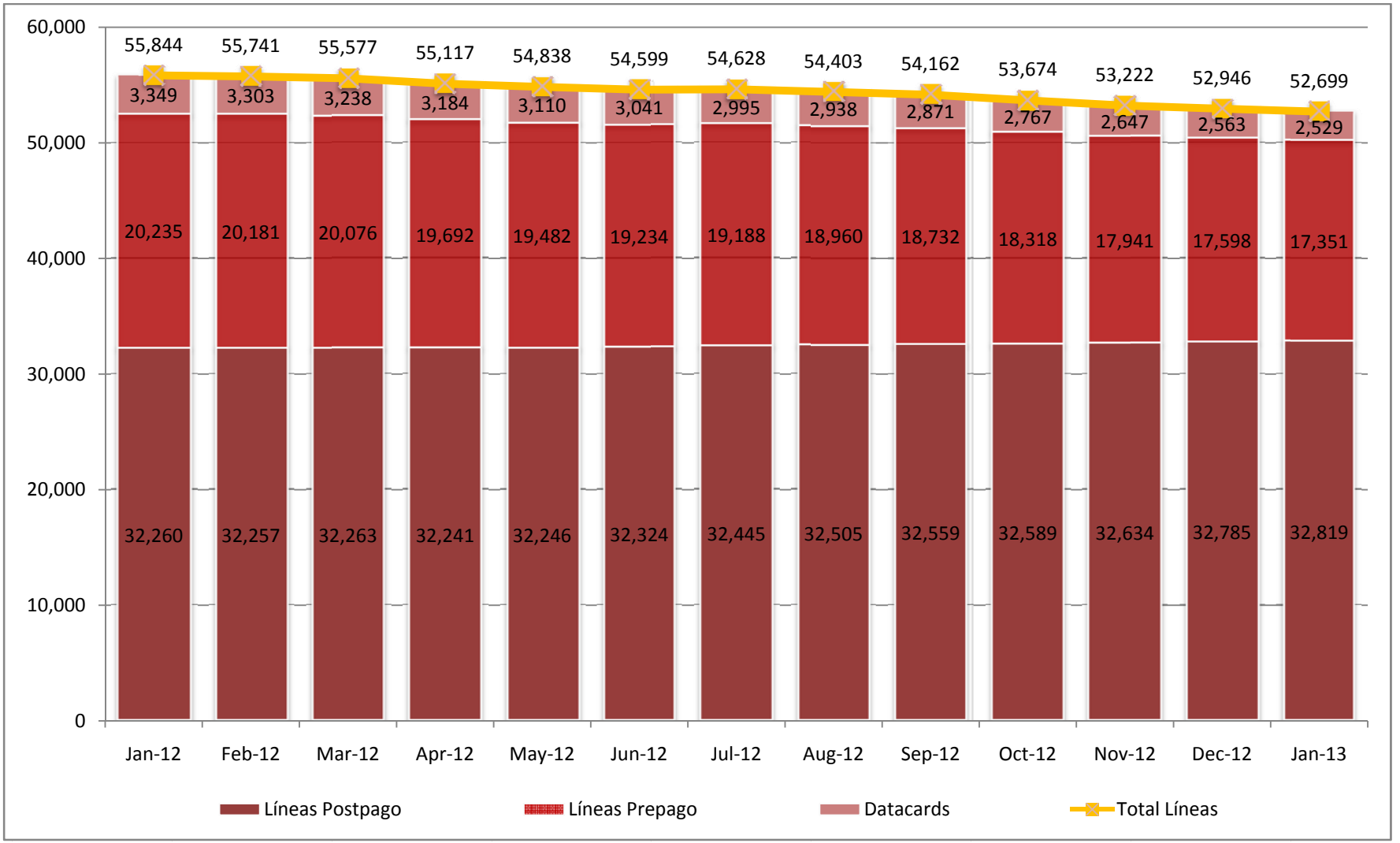


Figura 3: Evolución del parque de líneas móviles (en miles)

Según la 13º edición del informe anual "La sociedad de la información en España"[6] correspondiente al año 2012, elaborado por Telefónica, estipula que el 63% de los usuarios de dispositivos móviles en España, utiliza un teléfono inteligente, tal y como observamos en la figura 4. Según la definición extraída del diccionario Oxford, consultada el 29 de mayo de 2013: "*Un teléfono inteligente (Smartphone en inglés) es un teléfono móvil capaz de realizar muchas de las funciones de un ordenador, teniendo típicamente una pantalla relativamente grande y un sistema operativo capaz de ejecutar diversas aplicaciones"*. Este hecho puede ser ocasionado entre otros motivos, por la subvención por parte de las operadoras de telecomunicaciones, de los terminales. De esta manera, la mayor parte de usuarios, contrae un compromiso de permanencia, y por tanto, de pago con la operadora.

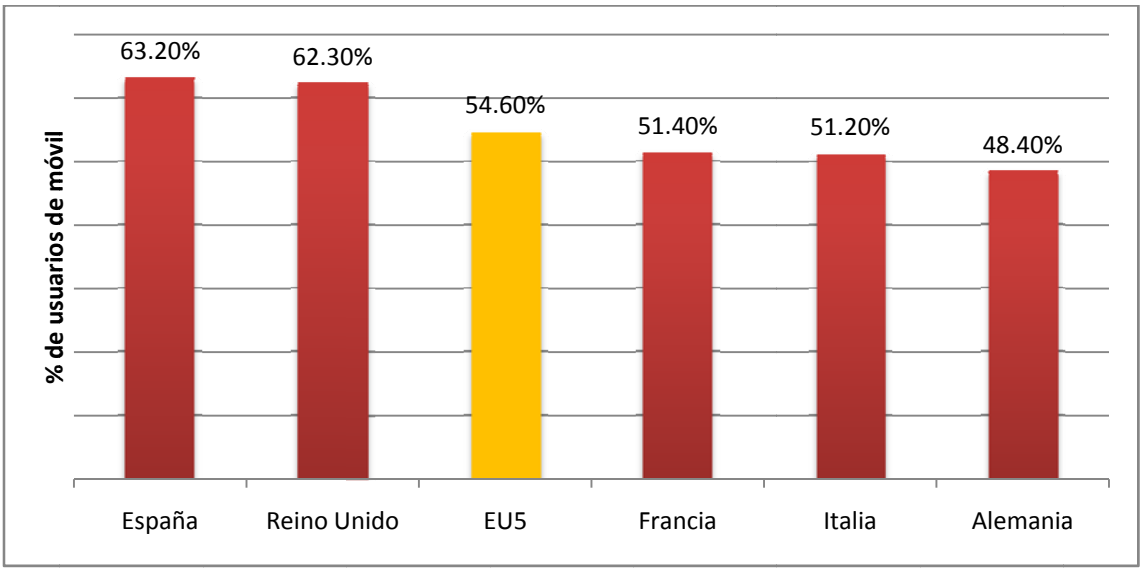


Figura 4: Porcentaje de usuarios de teléfono móvil que usan Smartphone[7]

Observamos también que la media del número de usuarios de teléfonos móviles que utilizan teléfonos inteligentes, de algunos países europeos (Alemania, España, Francia, Italia y Reino Unido), supera el 50%.

A mediados del año 2011, Google encargó un estudio a la consultora Ipsos MediaCT Germany, llamado "Think Mobile"[8], para analizar 30 países, entre ellos España, respecto al uso de Internet en los smartphones. Incidiendo sobre todo, en el momento y los lugares

[6] "La Sociedad de la Información en España", Fundación Telefónica. http://e-libros.fundacion.telefonica.com/sie12/aplicacion_sie/ParteA/pdf/SIE_2012.pdf

[7] Fuente: Comscore, datos de octubre de 2012.

[8] "Think Mobile", Ipsos MediaCT Germany. http://www.gstatic.com/ads/research/en/2011_TheMobileMovement.pdf

de acceso a Internet mediante su teléfono. De él, extraemos la figura 5, de dónde destacamos que un 76% de los encuestados, se conecta a Internet mediante su móvil cuando está fuera de casa.

Vemos además, como una gran parte de los encuestados se conectan en establecimientos comerciales, como pueden ser bares, restaurantes o aeropuertos, entre otros.

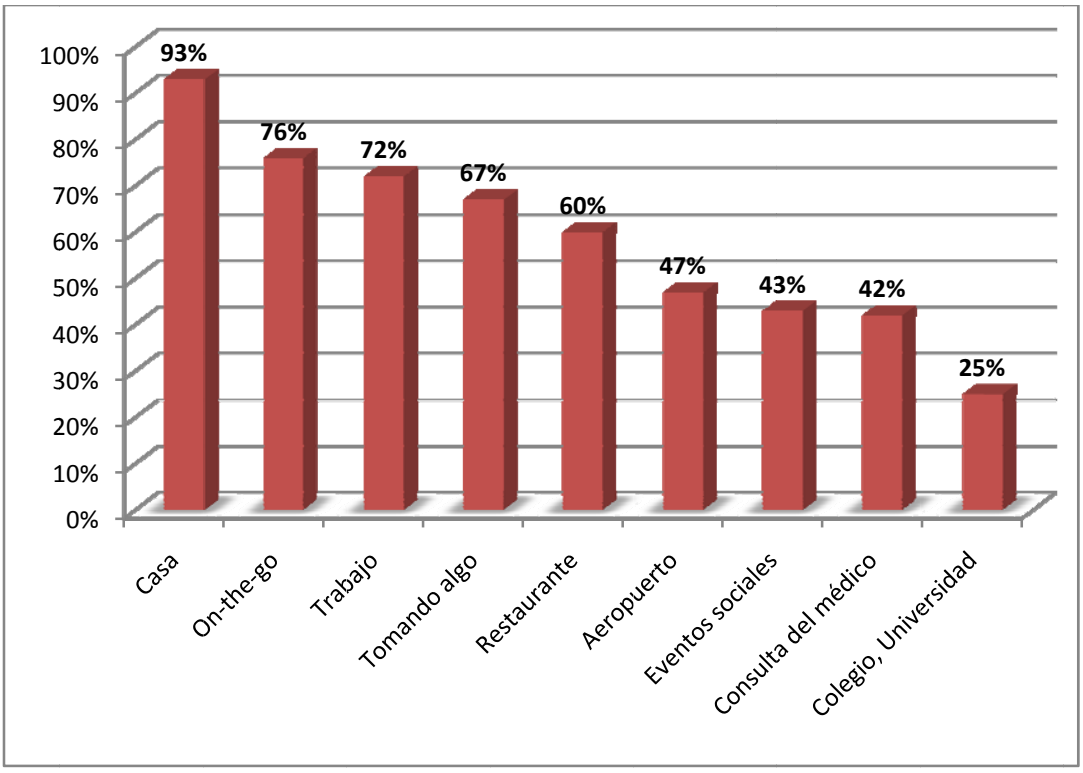


Figura 5: Dónde se conectan a Internet los usuarios con smartphone[9]

Hay que tener en cuenta también el resto de dispositivos con conexión a Internet. Estos son ordenadores portátiles y, cada vez más, tabletas. Éstas últimas, se han consolidado como el boom tecnológico del momento, y miles de personas suspiran por tener uno. Pero más allá de puras habladurías, la firma de investigaciones de mercado, TNS, llevó a cabo un informe denominado "Mobile Life"[10] en el que se concluye que las tabletas digitales tienen ya una penetración del 14% en la población española. Esta cifra prácticamente duplica a la media europea, y triplica a la media mundial. Pero yendo más allá, el 21% de los encuestados en España, planea hacerse con uno de estos dispositivos durante este año. Otro dato interesante de este estudio, en relación al proyecto que se describe en esta memoria, es que el 88% de los encuestados, afirma utilizar acceso a Internet mediante

[9] Fuente: Mobile Internet Insights. Report Spain. Ipsos MediaCT Germany. The Media. Content and Technology Research Specialists. July 2011

[10] "Mobile Life", TNS. http://discovermobilelife.com/

WiFi. En este caso también, una de las causas probables sea la subvención de dispositivos por parte de las teleoperadoras.

Según un estudio llevado a cabo por las compañías ComScore y Telefónica Alemania, el 8,8% de los usuarios españoles de Smartphone, tienen y utilizan frecuentemente, una tableta digital. Podemos observar en la figura 6, que los datos en España, son muy superiores al resto de algunos países europeos como Alemania, Reino Unido, Francia o Italia.

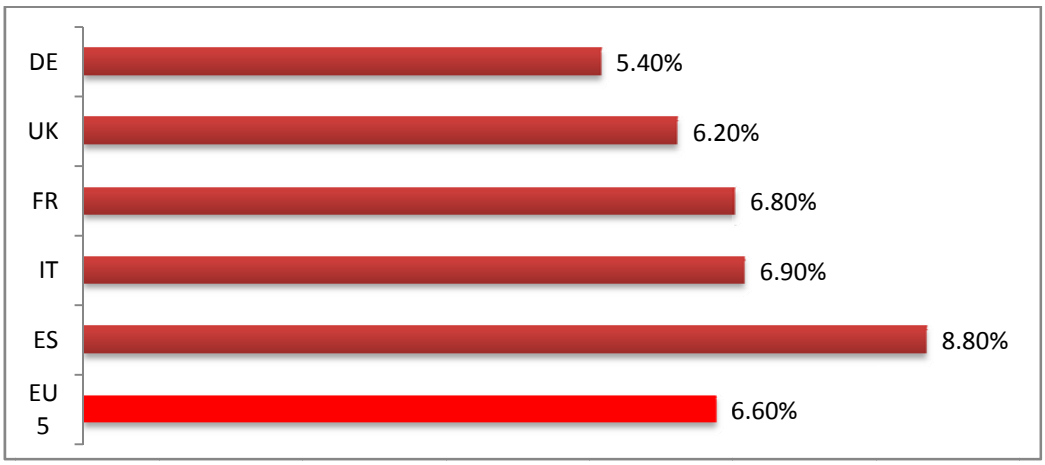


Figura 6: Porcentaje de usuarios que tienen smartphones y tablet[11]

Se estima que hacia el año 2016, el tráfico cursado mediante el uso de tabletas inteligentes, superará casi en el doble al cursado mediante teléfonos inteligentes. Según la figura 7, extraída del informe anual 2011 de la CMT, nota mensual de noviembre 2012. Por lo tanto, y de manera clara, resultaría un grave error, el no contar con estos dispositivos como medios de comunicación.

No obstante, vemos que sin lugar a dudas, el rey del tráfico móvil, seguirá siendo indiscutiblemente según las aproximaciones, los ordenadores portátiles o "laptops". De estos últimos dispositivos, absolutamente todos los modelos disponibles a la venta, sea cual sea su nivel de calidad o rendimiento, constan con la tecnología necesaria para efectuar una conexión a Internet mediante WiFi. Este hecho probablemente se vea condicionado debido a diversas causas. Una de ellas, probablemente sea, que no todos los sitios web actuales, se encuentran acondicionados o preparados para su correcta visualización en un dispositivo móvil. De esta manera, resulta tedioso y propicia, el uso de ordenadores portátiles para llevar a cabo estas tareas.

[11] Fuente: ComScore MobiLens, 3 mon. avg. ending Oct 2011. http://www.comscore.com/Insights/Press_Releases/2012/1/comScore_and_Telefonica_Germany_Announce_Results_of_Connected_Europe_Study

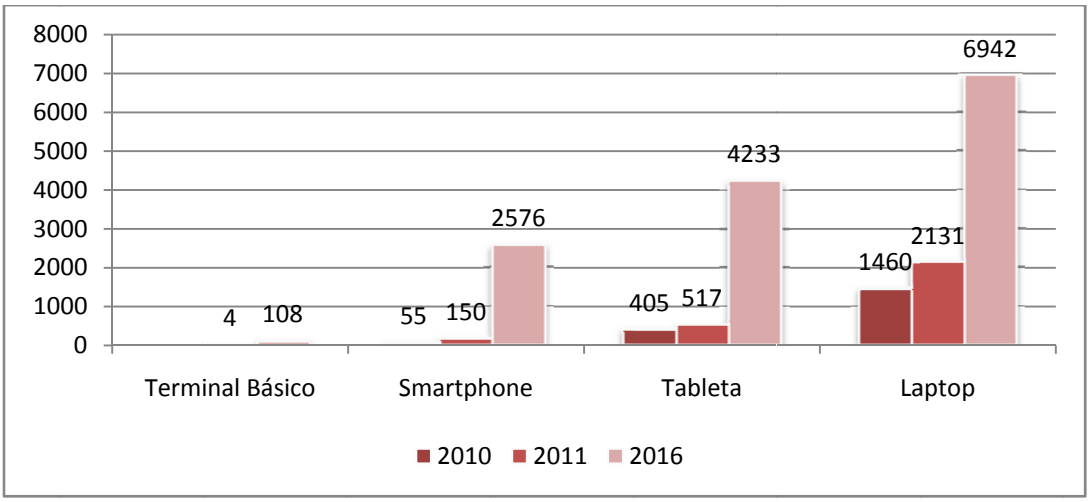


Figura 7: Tráfico medio estimado de banda ancha móvil por tipo de dispositivo (MB/mes)[12]

No olvidemos que, prácticamente todos los dispositivos comentados hasta el momento (teléfonos inteligentes, tabletas digitales y ordenadores portátiles), traen de fábrica los componentes necesarios para llevar a cabo conexiones inalámbricas sin cables WiFi.

1.4 Estudio de la utilización del rango de frecuencias WiFi

Para llevar a cabo la implementación de este proyecto, y por lo tanto, para poder decidir que dispositivos utilizar, fue llevado a cabo un breve estudio a pie de calle, sobre el rango de frecuencias que usan normalmente las redes WiFi en Barcelona.

Se realizaron dos recorridos por zonas céntricas de la ciudad. Durante los cuales se recopiló información pública relativa a las redes WiFi disponibles en cada momento. Entre dicha información, se encuentran: SSID[8], Tipo de red, BSSID[9], Hora en la que se descubrió la red, SNR[10] con la que se recibió la señal, Tasa de transmisión y Canal.

Podemos observar en la figura 8, los recorridos efectuados para recopilar datos sobre el uso de los canales de radiofrecuencia destinados a la tecnología WiFi.

[12] Fuente: Cisco 2011

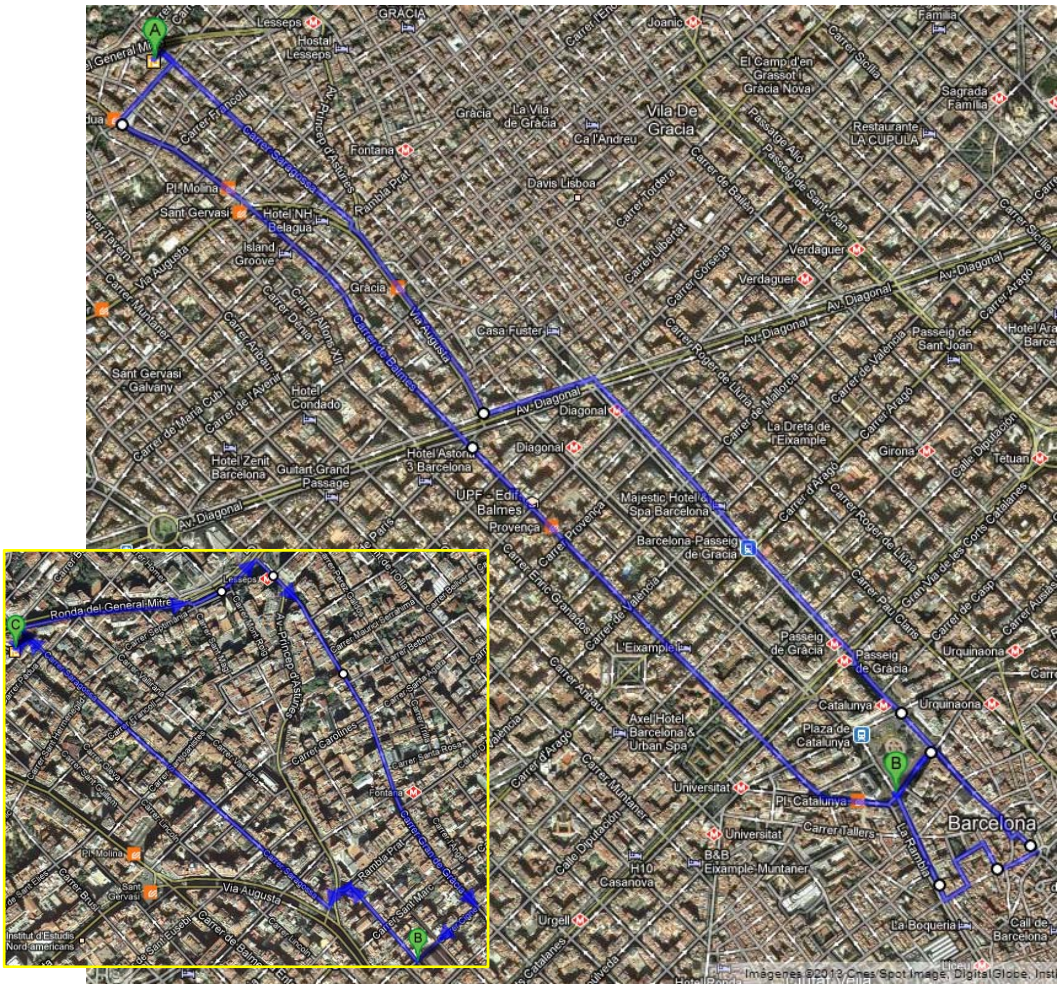


Figura 8: Recorridos llevados a cabo para la adquisición de datos.[13]

De este estudio, se sacan conclusiones tajantes respecto a la utilización del espectro de frecuencia WiFi en la ciudad de Barcelona. Se descubrieron en total 5463 redes WiFi diferentes a lo largo de estos recorridos. De éstos, más de un 97% transmiten y reciben información en el rango de frecuencia de 2,4GHz, mientras que menos del 3% lo hacen en los canales pertenecientes al rango de 5GHz. Podemos observar en la tabla 1 y figura 9, los datos obtenidos.

[13] Imágenes extraídas de: Google Maps

Tabla 2: Datos obtenidos durante el estudio del rango de frecuencias WiFi utilizados en Barcelona

# Redes 2.4GHz	# Redes 5GHz	Canal
1145	-	1
242	-	2
406	-	3
192	-	4
214	-	5
1045	-	6
165	-	7
154	-	8
368	-	9
146	-	10
864	-	11
120	-	12
214	-	13
-	52	36
-	23	40
-	35	44
-	29	48
-	12	52
-	7	56
-	8	60
-	19	64
-	2	149
-	1	153
Total	**5275**	**188**
Porcentaje	**96,56%**	**3,44%**

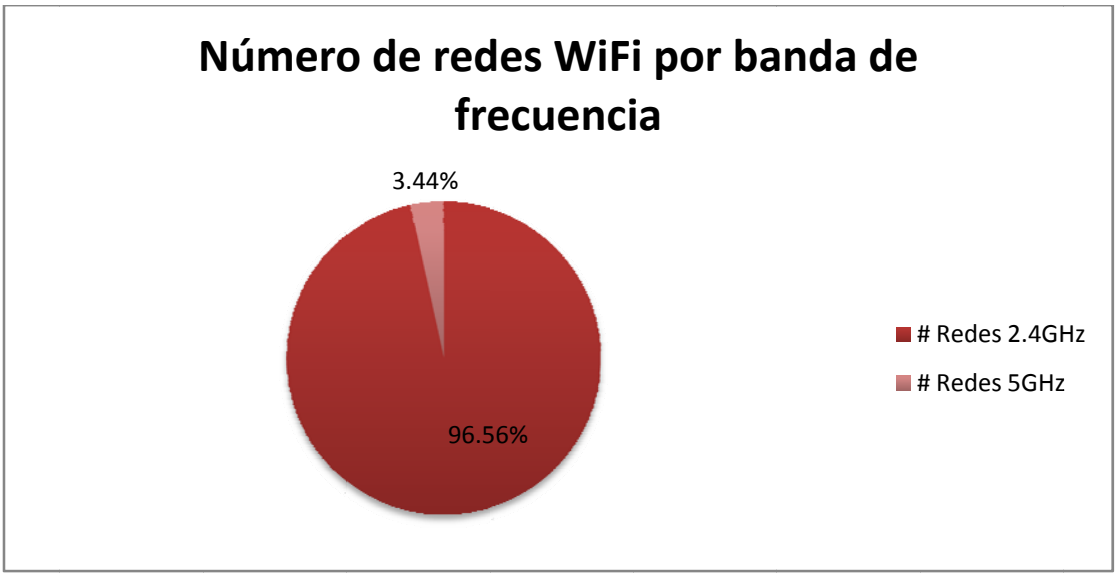


Figura 9: Porcentaje de redes WiFi según el rango de frecuencias utilizado, en Barcelona

Diversas conclusiones pueden ser extraídas de la tabla 1. Es remarcable la gran diferencia entre la utilización de un rango de frecuencias y el otro. Este hecho, va estrechamente relacionado con la adopción por parte de los usuarios de los equipos entregados por defecto por las operadoras de telecomunicaciones. Actualmente, la inmensa mayoría de los equipos que un usuario final recibe al contratar los servicios de un operador, trabajan a la banda de frecuencia de 2,4GHz.

Como consecuencia directa de este hecho, vemos una sobrepoblación de los canales 1y 6. Esto se debe a que estos canales, no se interfieren entre sí en el espectro radioeléctrico, tal como vemos en la siguiente figura 10. Dado el ancho de banda destinado a cada canal, la manera de que estos no se sobrepongan unos a otros, es escogiendo canales que estén lo suficientemente separados uno del otro. Es por esto, que se suele tomar como referencia los canales 1, 6 y 13 del rango de 2,4GHz. Este hecho explicaría la saturación de redes WiFi en estos canales.

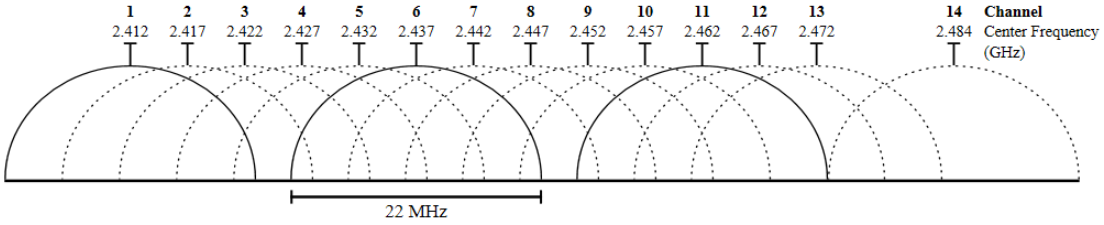


Figura 10: Disposición gráfica de los canales a 2,4GHz utilizados por WiFi. [14]

Podemos observar en la figura 11 la utilización de los canales de radiofrecuencia WiFi de uso público. En este gráfico, queda más que visible la enorme diferencia entre la utilización de redes WiFi a 2,4GHz y a 5GHz. Vemos claramente que los más utilizados son los canales 1, 6 y en menor medida el 11. Todos ellos se tratan de canales a 2,4GHz. En cuanto al rango de 5GHz, podemos concluir que los más ocupados son el 36, 44 y 48. Resulta llamativo, el hecho que un 56% de las redes encontradas utilizaban los canales: 1,6 u 11.

[14] Fuente: Wikipedia. http://en.wikipedia.org/wiki/802.11

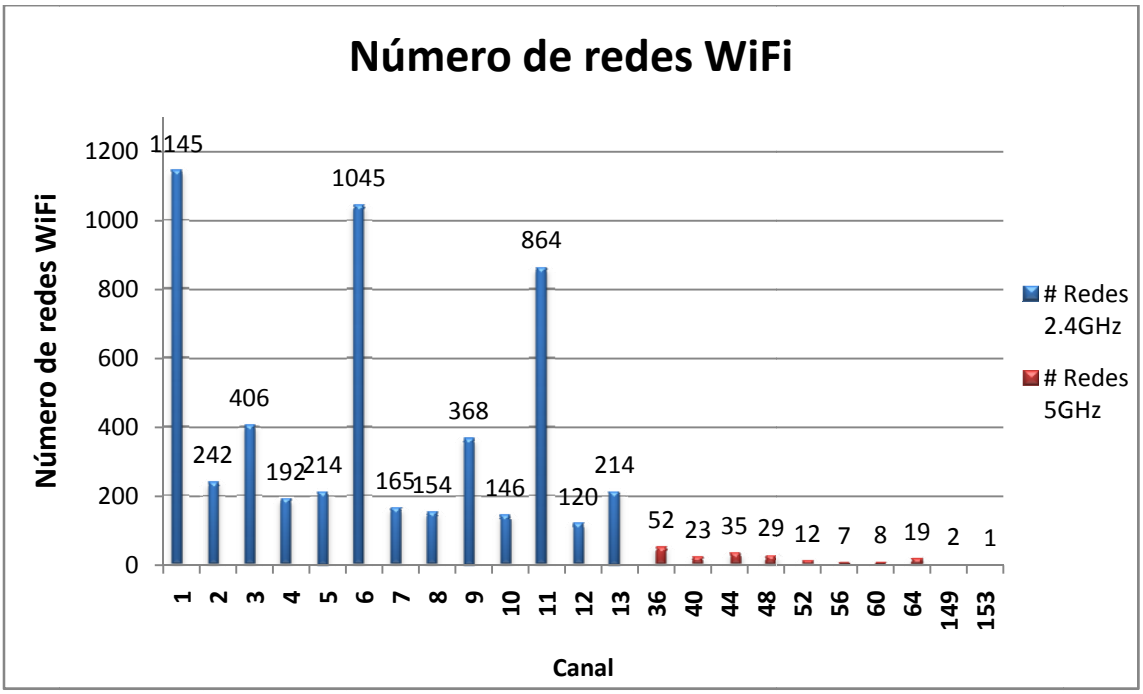


Figura 11: Utilización de los canales de radiofrecuencia WiFi

Respecto al tipo de redes WiFi descubiertas, observamos también una minoría absoluta de redes ad-hoc[11] o punto a punto. Este hecho no resulta sorprendente, ya que este tipo de redes se utilizan principalmente para llevar a cabo conexiones punto a punto. La ventaja es que no presentan necesidad de integrar en la comunicación ningún dispositivo de red, como pueden ser enrutadores o puntos de acceso. Podemos observar los datos en la figura 12.

Tabla 3: Porcentaje tipos de red. Datos obtenidos durante el estudio del rango de frecuencias WiFi utilizados en Barcelona

	# Redes	Tipo de Red	Porcentaje
	5410	BSS	99,03%
	53	Ad-HOC	0,97%
Total	5463		

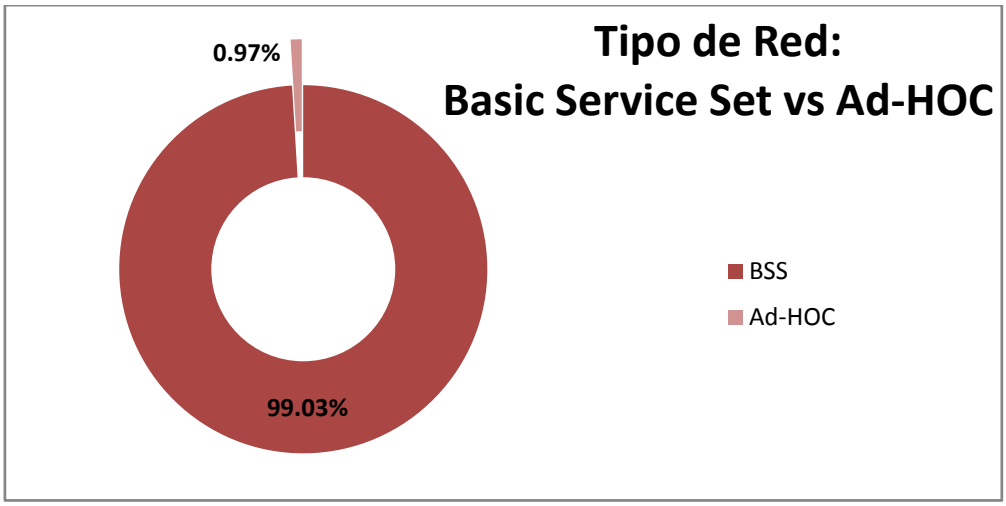


Figura 12: Comparación porcentual entre tipo de redes WiFi descubiertas

Por último, se realizó un estudio de la tasa de transmisión teórica de las redes WiFi descubiertas, según el canal en el que transmitían. Los motivos por los que la tasa de transmisión teórica pueda variar de un canal a otro, son diversas. Algunos de ellos son la ocupación o saturación de los mismos, los protocolos de transmisión utilizados o las posibles interferencias que puedan haber en ese momento dado, fruto de diversas causas. Podemos observar los resultados en la tabla 3.

Tabla 4: Tasa media de trasmisión teórica, por canal, de las redes WiFi descubiertas

# Redes	Canal	Tasa Media [Mbps]
1145	1	118,45
242	2	124,39
406	3	95,96
192	4	122,48
214	5	129,36
1045	6	149,06
165	7	129,65
154	8	135,31
368	9	106,94
146	10	121,19
864	11	130,74
120	12	122,21
214	13	124,36
52	36	285,42
23	40	267,91
35	44	267,94
29	48	211,86
12	52	218,00
7	56	124,29
8	60	306,75
19	64	287,05
2	149	252,00
1	153	130,00
Media 2,4 GHz		123,85
Media 5 GHz		235,12
Media Total		172,23

Se puede observar en la figura 13, la abismal diferencia entre las tasas de transmisión calculadas durante los recorridos del estudio, en la ciudad de Barcelona. Resalta un incremento considerable en la mayoría de los canales pertenecientes al rango de 5GHz, llegando a duplicar prácticamente la media perteneciente a los canales de 2,4GHz.

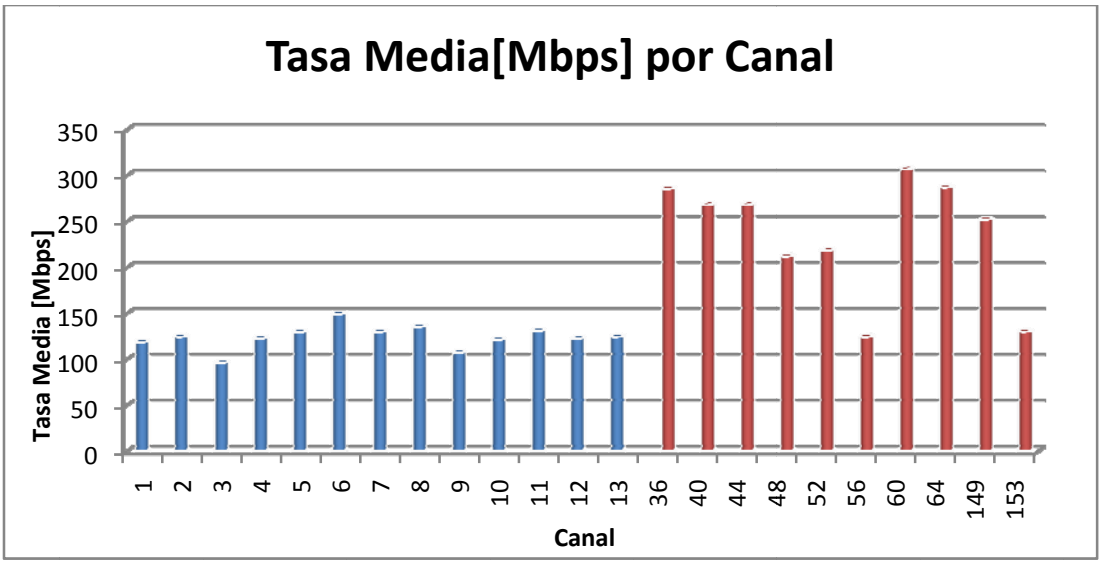


Figura 13: Tasa media de transmisión teórica de las muestras tomadas

Por lo tanto, y a modo de conclusión, podemos determinar con total certeza que los canales de la banda de frecuencias de 2,4GHz, se encuentran saturados en relación a los que trabajan a 5GHz. Debido a este motivo, la decisión habría de tomarse rotundamente a utilizar los canales que se encuentren menos utilizados, en la banda menos ocupada. No obstante, y debido a la poca utilización de éstos, nos vemos obligados a determinar que el parque tecnológico desplegado actualmente en la ciudad de Barcelona, no se encuentra completamente preparado para la utilización de estos canales. El proyecto intenta acercar las tecnologías WiFi a todos los ciudadanos, otorgándoles conectividad a Internet gratuita. Entonces el proyecto se ve obligado a utilizar la tecnología que se presente como mayoritaria para cumplir su objetivo final.

Es por este motivo que se ha decidido utilizar la frecuencia de 2,4Ghz para llevar a cabo las conexiones. Entonces el siguiente paso es decidir qué equipo se utilizará para dar abasto a los usuarios finales de la red.

1.5 Usuarios potenciales del sistema

Uno de los puntos fuertes de este sistema, es que al ser flexible, la escalabilidad no representa un problema. Si la demanda del número de usuarios resulta elevada, puede desplegarse un nuevo servidor para paliar este problema. Como se ha comentado anteriormente, el diseño final del sistema, no influenciará en gran medida al funcionamiento del mismo, por lo que resulta de gran facilidad e independencia.

En un primer momento, se estaría dando servicio a todos los usuarios que se conectan desde Italia, y los usuarios que se registrarían en España. Se calcula aproximadamente que "Free Italia WiFi" tiene 4 millones de usuarios, esto sumado a los potenciales usuarios españoles, hacen un total de aproximadamente más de 12 millones de usuarios.

Tabla 5: Usuarios potenciales en España del piloto "Free Europe WiFi"

55.669.000 líneas móviles	**47.190.493 millones de habitantes**	**55.669.000 líneas móviles**
63% penetración smartphones vs móviles	14% penetración tablets vs población	0,88 % penetración tablet + smartphone vs móviles
22,6% usuarios usan redes públicas	22,6% usuarios usan redes públicas	22,6% usuarios usan redes públicas
[55.669.000*(0.63+0.088) + 47.190.493*(0.14-0.088)] * 0.226 = 9.587.879,97		**[55.669.000*(0.63) + 47.190.493*(0.14-0.088)] * 0.226 = 8.057.545,65**
Usuarios potenciales del sistema (sin tener en cuenta número laptops)		**Usuarios potenciales del sistema (sin tener en cuenta # laptops y suponiendo NO móvil y tablet a la vez)**

Este sistema, tal y como hemos observado durante el apartado legal, no tiene como objetivo, llevar a cabo ningún tipo de afectación a los operadores de telecomunicaciones de los territorios en los que se desplegaría. Dadas las restricciones impuestas por la

normativa vigente decretada por la Comisión del Mercado de Telecomunicaciones, no se consideraría a este proyecto como competencia a los operadores, siempre que se cumpliesen las restricciones comentadas en el apartado legal de esta memoria.

Más lejos que esto, parte como una alternativa para solventar problemas y acercar las nuevas tecnologías a la sociedad, y para la sociedad. Se trata por lo tanto de un proyecto sin fines de lucro.

Por lo tanto, el tema más complicado de la realización del proyecto "Free Europe WiFi" pasa por la implicación de las administraciones públicas, o bien de buscar nuevas donaciones por parte de terceros.

Este proyecto nace como una iniciativa bajo la filosofía "Bottom-up-Broadband". Esta rompe con el paradigma clásico de las operadoras llevando las comunicaciones hacia los usuarios. En esta filosofía, son los usuarios los que ponen la primera piedra para llevar a cabo la comunicación. Es decir, nace desde los usuarios y para los usuarios, siempre respetando el mercado.

1.6 Elección de la solución a implementar

En este apartado comentaremos la elección de OpenWISP, y por lo tanto de la utilización de Ruby on Rails para el desarrollo del mismo.

Actualmente existen diversas implementaciones de proveedores de Internet, no obstante, no existen diversos que cumplan las siguientes dos condiciones. La primera, que ofrezcan servicio sin cables o WiFi, y la segunda y más importante, que sea un servicio totalmente gratuito y abierto a todos los potenciales usuarios.

Se calcula que en el año 2015 se alcanzará la friolera de 5.8 millones de puntos de acceso a Internet libres o "hotspots"[15]. Desde el año 2011, se estipula que habrá crecido en un 350%. Este número además, no incluye aquellos en los que se comparte una conexión privada, para dar acceso al resto de usuarios. Si tenemos en cuenta estos últimos, hay que sumar 4,5 millones de dispositivos más, según un estudio [16]realizado por la "Wireless Broadband Alliance"[12] (WBA).

[15] Entendemos por "HotSpots" aquellas zonas que ofrecen acceso a Internet a través de una red inalámbrica, ubicado en un lugar público.

[16] Estudio extraído de :
http://www.informa.com/Media-centre/Press-releases--news/Latest-News/Wifi-hotspots-set-to-more-than-triple-by-2015/

1.6.1 Comparativa con otros sistemas

No solamente han sido tenidos en cuenta, operadores privados, sino también posibles soluciones públicas o gubernamentales. Algunas de las implementaciones públicas, de acceso a Internet de forma gratuita, son las siguientes:

- Barcelona WiFi[13]:

  Es un servicio promovido por el ayuntamiento de la ciudad de Barcelona, y ofrecido por British Telecom[14] que permite acceder a una conexión a Internet, a través de diversos puntos de acceso ubicados en diversos puntos de la ciudad. Se define, según su web oficial, como "…un servicio que permite a los usuarios la navegación simple por Internet y, a dicho efecto, se encuentra habilitado el acceso a contenidos solo a través de un navegador de web…".
  Se pueden encontrar dispositivos para utilizar esta red, en diversos puntos de la ciudad. Tanto en edificios públicos (bibliotecas, mercados, centros cívicos, salas de estudio, etc…) como a plena intemperie. Actualmente, existen más de 430 puntos de acceso (WiFi 802.11 B/G/N) desplegados por toda la ciudad. Todas las localizaciones desde las cuales se puede acceder al servicio, están identificadas con los siguientes logotipos:

Figura 14: Barcelona WiFi. [17]

  El único requerimiento físico para poder acceder a este servicio, es contar con un dispositivo (ordenador portátil, tableta o teléfono móvil) con conexión WiFi B,G o N.
  Antes de poder acceder a la conectividad, se deben cumplir y aceptar explícitamente las condiciones generales de utilización del servicio. Estas condiciones vienen estipuladas por la Comisión del Mercado de las Telecomunicaciones -CMT-, entre otras son: la limitación de la velocidad de transmisión (máximo 256kbps), el horario de uso de la red, se permitirá

[17] Imágenes extraídas de: http://www.bcn.cat/barcelonawifi/es/welcome.html

únicamente el tráfico http/https, están prohibidas las aplicaciones de voz sobre IP -VoIP- o video llamada, etc…

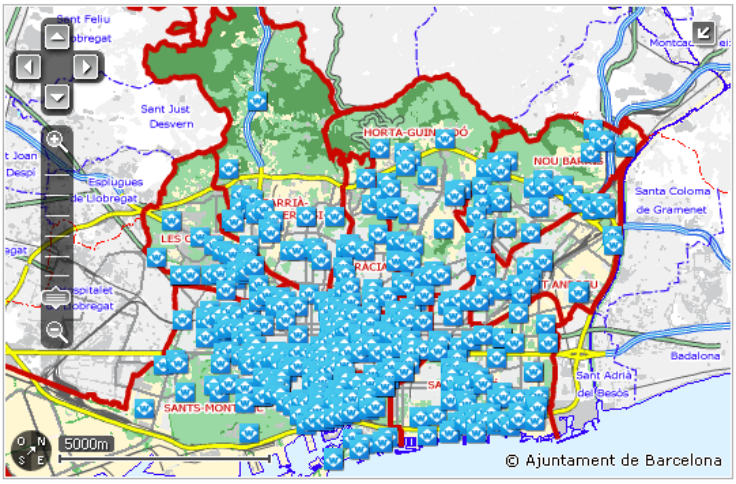


Figura 15: Mapa puntos de acceso Barcelona WiFi.[17]

- Malta "MCAfreeWiFi"[15]:

  Se trata de un servicio ofrecido por la autoridad de telecomunicaciones de Malta, "MCA". Existen más de 170 dispositivos de acceso distribuidos a lo largo de las dos islas que conforman el país.

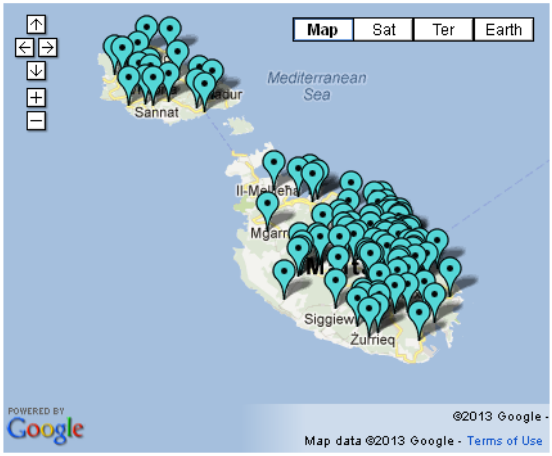


Figura 16: Mapa puntos de acceso MCAFreeWiFi. [18]

[18] Imagen extraída de: http://www.mca.org.mt/wifi-hotspots

- Oulu, Finlandia[16]:

  Es un servicio llamado PanOULU ofrecido por el ayuntamiento de la ciudad de Oulu, en compañía de la universidad de Oulu, la universidad de ciencias aplicadas de Oulu, y otras organizaciones locales. Se ofrece conexión gratuita e inalámbrica a todos los usuarios que deseen conectarse a su red. Actualmente no requiere ni registro ni identificación de nuevos usuarios. No tiene restricción alguna respecto a horarios de uso, uso de aplicaciones o ancho de banda. Existen más de 400 puntos de acceso (aproximadamente 340 en exteriores, y 110 en interiores) desplegados a lo largo de la ciudad, que utilizan el estándar WiFi 802.11 B/G/N, y aproximadamente unos 50 que utilizan el novedoso WiFi 802.11AC.
  Cada vez que un nuevo usuario se conecta a uno de los puntos de acceso, se crea una red virtual privada VPN[17], para dar mayor seguridad y confidencialidad a los datos enviados o recibidos por el usuario.

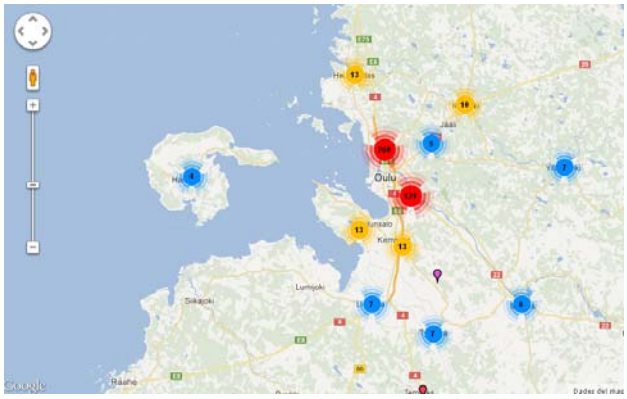


Figura 17: Mapa densidad puntos de acceso PanOULU. [19]

- Paris WiFi[18]:

  Es un servicio ofrecido por el ayuntamiento de París, conjuntamente con la operadora del mismo origen, Orange Telecom. Actualmente cuenta con más de 400 puntos de acceso distribuidos a lo largo de la ciudad. No tan sólo en edificios públicos (museos, ayuntamiento, bibliotecas, etc…) sino que también se encuentran ubicados en jardines, parques u otros lugares expuestos a la intemperie.

[19] Imagen extraída de: http://www.panoulu.net/

Figura 18: Mapa puntos de acceso Paris WiFi.[20]

Para disfrutar de la conexión, es necesario registrarse como usuario, identificándose mediante nombre, apellido y una dirección de correo válida.
El servicio ofrece de 2 horas ininterrumpidas de conexión gratuita a Internet de manera inalámbrica. Al cabo de este tiempo, si se desea seguir utilizando la conexión, es necesario un nuevo registro como usuario. Están prohibidas cualquier tipo de conexión de voz IP -VoIP-, o que utilicen la tecnología "Peer-2-Peer" o P2P[19].

Figura 19: Logo Paris WiFi.[20]

- Guifi.NET[20] :

  Guifi.net se define como una red abierta, donde los participantes (particulares, empresas, administraciones, etc.) pueden unirse a la red para extenderla y obtener conectividad. Actualmente hay más de 20.000 nodos inalámbricos operativos, todos ellos con una configuración pública para que cualquier interesado sea capaz de mejorar, mantener y ampliar la red.

[20] Imagen extraída de:
http://www.paris.fr/pratique/paris-wi-fi/localisation-des-points-wi-fi/rub_7799_stand_29274_port_17981

Figura 20: Logo de Guifi.Net

Si bien no sigue el mismo modelo que las opciones comentadas anteriormente, ha de ser considerada como una alternativa. Guifi.net ofrece conectividad a diversos ayuntamientos, que a su vez, utilizan este acuerdo para dar abastecimiento y conexión gratuita a Internet a sus habitantes de manera inalámbrica. Como pueden ser los casos de: Fuentes de Ayódar y Vallibona en Castellón, Sant Andreu de Llavaneres, Caldes de Estrac y Sant Vicenç de Montalt en Cataluña, entre otros.

No obstante, lo que Guifi.net proporciona, es acceso a las infraestructuras y redes, pero en ningún caso, se oferta el servicio de acceso Internet, como ISP. Por lo tanto, si algún organismo, ya sea público (ayuntamientos, bibliotecas, etc.) o privado (bares, restaurantes, hoteles, etc.) necesitan contratar a un ISP para poder utilizar la red de Guifi.net.

A continuación se exponen otros posibles sistemas propietarios que se plantearon como probables modelos a seguir para el desarrollo del proyecto:

- KUBI Wireless [21]

KUBI Wireless es una de las empresas de mayor presencia nacional en lo que a oferta de Internet de banda ancha sin cables se refiere. Actúa como operador de de servicios de conexión a Internet WiFi. Actualmente tiene más de 250 hotspots[15] desplegados en diversos países del mundo, tales como España, Estados Unidos, Jamaica o Croacia, entre otros.

Figura 21: Logo de KUBI Wireless

El sistema que ofrecen está destinado primordialmente a establecimientos comerciales (hoteles, bares, restaurantes, aeropuertos, etc...), y permite disfrutar de una conexión inalámbrica WiFi con acceso a Internet a los clientes de dicho establecimiento. Este servicio tiene un coste tarificado para los usuarios finales, que varía dependiendo el tiempo y las condiciones de que se haga uso del servicio. Si algún establecimiento está interesado, KUBI Wireless se hace cargo íntegramente del mantenimiento, soporte y atención al cliente, y comparte los gastos de la inversión inicial y los de explotación, a cambio de un porcentaje de los ingresos generados con este servicio.

Existe interconectividad total entre todos los hotspots de la compañía, por lo que los usuarios finales de esta red, pueden utilizar de su bono de acceso a Internet en cualquier punto de acceso de la compañía.

- ZonaWiFiGratis[22]

  Compañía con sede en Palencia, España, que ofrece soluciones para la gestión, administración y proporción de conexiones a Internet, mediante tecnologías inalámbricas WiFi, para el público.

Figura 22: Logo ZonaWifiGratis.es

Para poner en marcha su sistema, piden una cuota inicial de 200€ por parte de los establecimientos que quieran adherirse, en concepto de hardware y puesta en marcha.

- GOWEX[23]

  GOWEX es una compañía que ofrece diversas soluciones relacionadas con el acceso a Internet mediante conexión sin cables WiFi. No tan solo se dirige a establecimientos comerciales, sino que también oferta soluciones a organizaciones gubernamentales, como ayuntamientos o administraciones públicas, o incluso para flotas de vehículos.

Figura 23: Logo Gowex

  - Solución para Administraciones Públicas: ofrecen soluciones orientadas a la creación, gestión y explotación de redes inalámbricas WiFi, tanto a nivel municipal como provincial. El modelo de GOWEX, permite recuperar la inversión e incluso rentabilizarla, mediante ingresos generados por diferentes modelos de negocio a adoptar, como publicidad o servicios Premium de pago. De esta manera, buscan ofrecer un servicio auto sostenible y rentable. Básicamente, se entrega a las administraciones públicas, una plataforma técnica que permite automatizar la gestión, registro y validación de usuarios, operadores o asociaciones, dentro de la red WiFi.

- Solución para Establecimientos Comerciales: se ofrece la instalación y mantenimiento de una red de acceso a Internet WiFi, para los usuarios del local comercial. El establecimiento, puede controlar y llevar a cabo una gestión de los usuarios, mediante el uso de la plataforma WILOC de GOWEX. Además, la inversión puede rentabilizarse mediante diversas técnicas o modelos de negocio como la publicidad, contenidos o aplicaciones ofertadas a través de la red.

- FON [24]

Fon es una compañía fundada en el año 2006, en Madrid, España. Su objetivo es crear una comunidad de usuarios basados en puntos de acceso WiFi. Los usuarios, si quieren formar parte de la comunidad, han de comprar un dispositivo de enrutamiento, llamado "fonera". Este dispositivo utiliza un firmware[25] propio basado en OpenWRT.

Figura 24: Logo Fon

Cuando los usuarios conectan este dispositivo a su línea, comparten parte de su conexión a Internet a otros usuarios de Fon. A cambio, pueden acceder al resto de puntos de acceso de la comunidad. Esto es posible debido a que se crean dos redes inalámbricas diferentes. Una para uso propio del usuario dueño de la línea, y el segundo para compartir.
El tráfico cursado por la red "personal" del usuario, tiene prioridad frente al tráfico cursado por la otra red. De esta manera, se garantiza que Fon no influirá en la velocidad de la red contratada por el usuario a su ISP. Además, estas conexiones se encuentran separadas entre sí mediante un firewall implementado en el propio enrutador, por lo que Fon, garantiza la seguridad de las conexiones.
No obstante, también se puede acceder a este servicio sin ser parte de la comunidad. En este caso, se ha de ejecutar un previo pago electrónico, por el tiempo de conexión privado. Parte de los ingresos por este tipo de conexiones, es destinado directamente al dueño del punto de acceso, o hotspot. De esta manera, los usuarios que comparten su conexión, además de gozar de acceso gratuito al resto de conexiones Fon, perciben un beneficio económico.
Actualmente, Fon, cuenta con aproximadamente 7.726.831 puntos de acceso distribuidos alrededor del mundo. Un detalle curioso, es que ofrece la posibilidad a los usuarios que se conecten a alguna de sus redes, de identificarse mediante su cuenta de Facebook o Twitter.
Fon, ofrece también soluciones para negocios, tanto pequeños como grandes compañías. Además, consta de relaciones con varias operadoras de redes de reconocimiento mundial, como Telekom, British Telecom, Belgacom o KPN. Los

usuarios de algunos de estos operadores, pueden incluso comenzar a formar parte de la comunidad Fon, sin necesidad de una “fonera”. Esto se debe, a que el firmware necesario viene ya incorporado en los dispositivos de estas compañías.

- SwissCOM Eurospot [26]

La operadora de telecomunicaciones de origen Suizo, provee soluciones tanto de acceso a Internet inalámbrico privado como público. En su oferta pública, su modelo de negocio difiere en gran parte con el resto**, ya que ninguna de sus conexiones es gratuita.**

Figura 25: Logo SwissCom

Actualmente tiene más de 65.000 hotspots desplegados por todo el mundo, centrándose en restaurantes, hoteles y transportes públicos.

Se pueden adquirir paquetes de tiempo de conexión, que van desde un periodo de 5 minutos, hasta un número ilimitado de minutos al mes. Además, y de manera opcional, permite a los clientes conectarse a una red privada virtual, para proteger sus datos durante las comunicaciones.

- LinSpot[27]

LinSpot es una iniciativa proveniente de Bélgica, que ofrece un software de descarga gratuita, que permite administrar y gestionar conexiones inalámbricas a Internet. De esta manera, sus clientes son capaces de desplegar “fácilmente” un sistema de cobros, para ofrecer a los usuarios de estos, un servicio de conexión a Internet.

Figura 26: Logo LinSpot

Su modelo de negocio está basado en cobrar una comisión del 15% sobre el volumen de facturación que su cliente haya obtenido, de la utilización de LinSpot. Alguna de sus características principales son:

  - Es software de descarga gratuita, no obstante su uso no lo es. El establecimiento ha de pagar una cuota en relación al volumen del servicio facturado a sus clientes, por este servicio.

- Funciona con prácticamente todos los dispositivos de red del mercado: enrutadores, puntos de acceso, NAT, etc…
- Reporte de facturación transparente y automático.
- Actualizaciones automáticas de servicio.
- Trabaja sobre cualquier sistema operativo.

Después de realizar una descripción sobre diversas alternativas, comprobamos que algunas de ellas, técnicamente hablando, son capaces de ofrecer una solución funcional al objetivo de este piloto. Es decir, ofrecen un sistema ubicuo que no dependa del lugar de uso del sistema. Por lo tanto, permitiría el desplazamiento de los usuarios entre los diferentes países integrantes del proyecto.

No obstante, al tratarse la inmensa mayoría de soluciones y software propietario, quedan excluidos como modelo a seguir, debido a que no se encuentran en comunión con la idea final del proyecto. Observamos que, no cumple una de las condiciones básicas de la filosofía "Bottom-Up-Broadband" al no ser totalmente abierto y gratuito.

1.6.2 Sistema escogido a implementar

Como consecuencia, debido a los servicios que se ofrecen en cada uno de ellos, y teniendo en cuenta otros factores como el precio, la facilidad de la puesta en marcha o la interoperabilidad entre sistemas; se decide tomar OpenWISP como modelo a seguir, dado su **carácter plenamente abierto**, su escalabilidad y gratuidad.

Frente al resto de sistemas o soluciones comentadas antes, destacaremos las ventajas que hacen de OpenWISP la solución idónea para lograr el objetivo deseado.

En primer lugar, y probablemente la más importante, OpenWISP esta licenciado bajo GNU GPL[28], por lo que es totalmente abierto y gratuito. Esto significa que cualquier persona interesada, puede estudiar, compartir, modificar y usar su código. De hecho, su código íntegro se encuentra disponible en la plataforma online GitHub[21]. Además, OpenWISP es un proyecto o iniciativa sin fines de lucro.

Este sistema es fácilmente escalable. Es decir, pueden añadirse tantos puntos de acceso como se desee, apuntando todos al mismo servidor. O por el contrario, agregar más servidores para distribuir el sistema, si así se desea. No existe límite práctico al número de usuarios o al número de dispositivos de red, que quieran conectarse.

OpenWISP fue creado con la intención de desplegar una red abierta a la ciudadanía, que ofreciese acceso libre a internet en Roma, Italia. Este proyecto llamado "ProvinciaWiFi", ha sido desplegado con éxito en esta ciudad, y se está expandiendo por toda Italia.

[21] GitHub. 2013. GitHub, Inc. Consultado 11/04/2013. https://github.com

Actualmente tiene presencia en diversas administraciones públicas, cómo en Roma, Génova, Turín, Lamezia Terme, Cerdeña, Rosignano, Prato, Gorizia, Grosseto Pistoia y Frosinone. No obstante, hay desplegados más de 1058 puntos de acceso en estas ciudades, no sólo ubicados en zonas pertenecientes a las administraciones públicas, sino también en establecimientos y locales comerciales.

El proyecto está siendo sufragado mediante aportaciones de los ayuntamientos en los que se extiende. El sistema es totalmente gratuito, por lo tanto, no existen cuotas ni mantenimiento por parte de los usuarios finales. Además, si un establecimiento comercial quiere comenzar a ofrecer esta solución como un servicio extra para sus clientes, puede hacerlo también. Para ello, sólo hará de hacerse cargo de los gastos del dispositivo de red, el punto de acceso, que se instalará y pasará a ser de su propiedad.

En el capítulo 2, se tratará en detalle las características y ventajas del sistema finalmente escogido.

La siguiente pregunta es entonces: ¿por qué Ruby on Rails[29]? La respuesta es sencilla, OpenWISP se encuentra escrito casi en su totalidad en este lenguaje. No obstante, llevaremos a cabo una introducción para comentar las virtudes, que no son pocas, de Ruby[30].

Ruby se trata de un lenguaje de programación, de código abierto y orientado a objetos, relativamente nuevo, ya que fue creado en 1994 por Yukihiro Matsumot. Este lenguaje sigue el modelo “MVC”, o lo que es lo mismo “Modelo-Vista-Controlador”[31]. No obstante, lo que más nos interesó en este sentido, fue la puesta en marcha de un nuevo marco de trabajo, o “framework”, basado en este nuevo lenguaje. Este es el conocido como “Ruby On Rails”, llevado a cabo por David Heinemeier Hansson, y se centra en la creación y mantenimiento de aplicaciones web.

La gran ventaja de utilizar Ruby on Rails frente a otros lenguajes de programación, viene dado por los propios estandartes de este lenguaje. Utilizar la menor cantidad de código posible, y “convención” sobre “configuración”, es decir, utilizar un lenguaje más humano y natural, y menos técnico. El sistema está previsto para ser utilizado en aplicaciones web que requieran tratamiento de base de datos (prácticamente todas en la actualidad), y por lo tanto, ofrece soluciones rápidas y directas para ello. Como referencia, este lenguaje se utiliza en sitios web reconocidos a nivel mundial [22] como GitHub[21], Scribd [23], SlideShare[24] o Hulu[25], entre muchos otros.

---

[22] Extraído: http://www.developerdrive.com/2011/09/20-best-sites-built-with-ruby-on-rails/

[23] Scribd. 2013. Scribd. Consultado 11/04/2013. http://es.scribd.com/

[24] Slide Share. 2013. SlideShare. Consutlado 11/04/2013. http://www.slideshare.net

[25] Hulu. 2013. Hulu. Consultado 11/04/2013. http://www.hulu.com

CAPÍTULO 2: ESTUDIO DE OPENWISP

A continuación se explicará una breve descripción, y el funcionamiento del sistema OpenWISP, así como su arquitectura y módulos que lo componen.

OpenWISP es un sistema abierto o "Open Source"[26], que posibilita crear servicios completos para ofrecer internet de manera inalámbrica. Permite de manera sencilla, crear la infraestructura digital necesaria, para un proveedor de internet sin cables.

OpenWISP está escrito en Ruby on Rails[14] en su mayoría. Una de sus grandes ventajas, es su arquitectura modular. Cada uno de estos módulos se implementa de manera diferenciada, y por lo tanto, la complejidad/prestación del sistema final depende de los objetivos del proyecto, pudiendo ser agregadas funcionalidades paulatinamente.

Algunas de las ventajas básicas de OpenWISP son:

- Es "fácil" de poner en marcha y configurar: Gracias a que configura automáticamente redes privadas virtuales, tanto la conectividad de los usuarios, como los puntos de acceso, pueden ser administrados desde un punto central. Esto permite hacer uso de conexiones preexistentes y un monitoreo central, haciendo al sistema granular y efectivo.
- Auto-registro de los usuarios: Los usuarios pueden registrarse mediante una simple verificación telefónica, utilizando sus teléfonos móviles.
- Múltiples eSSID[32]: Esto permite que existan diferentes redes con distintos perfiles de seguridad (dependiendo del uso o el entorno en el que se despliegue la red, puede filtrarse cierto tipo de tráfico o usuarios). Todas estas redes, pueden ser multiplexadas en una única VPN, o distribuida para llegar a diferentes destinos.
- Portal Captivo personalizable: Permite personalizar y configurar el portal captivo, según las necesidades actuales, con una posible granularidad de un sólo punto de acceso.

Como anteriormente se comentaba, OpenWISP está desarrollado de forma modular. Se divide principalmente en cinco grandes bloques de funcionamiento:

[26] The Open Source Definition. 2013. Open Source Iniciative. Consultado 01/05/2013. http://opensource.org/docs/osd

2.1 OpenWISP

2.1.1 OpenWISP User Management

Este módulo se trata de un servicio web para poder administrar y manipular la creación de nuevos usuarios del servicio. Además, estos pueden acceder por su propia cuenta, para modificar y/o actualizar sus datos personales o contraseñas, Figura 27.

Este módulo es integrable con software de terceras partes, como un servidor Radius[33][33A] para efectuar la autenticación de usuarios, o uso de una base de datos, como MySQL[34] o PostgreSQL[35].

Cuando un usuario desea conectarse a internet, o se registra como nuevo usuario, el sistema le pedirá que se identifique. Algunas de sus características principales son:

- Registro de usuarios mediante su número de teléfono móvil, DNI o tarjeta de crédito (existe la posibilidad de utilizar la plataforma de pagos PayPal[36], para llevar a cabo el registro).
- Interfaz de usuario, GUI, soportada por la mayoría de navegadores web móviles.
- Recuperación, en caso de olvido, de contraseñas, mediante el teléfono móvil o correo electrónico.
- Se generan estadísticas del tráfico generado por cada usuario.
- Interfaz administrativa, para llevar a cabo la organización y mantenimiento de usuarios. Soporta diferentes roles según el usuario (operador, administrador o súper-administrador).
- Traducido al inglés e italiano, de momento.

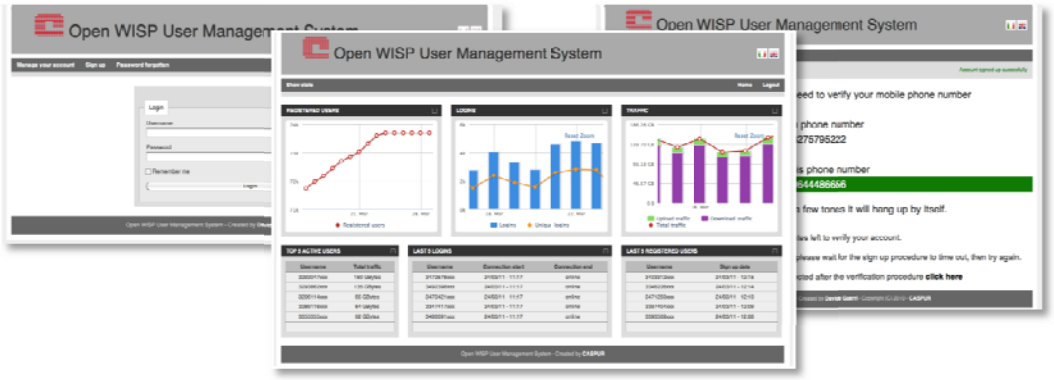


Figura 27: OpenWISP User Management

2.1.2 OpenWISP Manager

Este módulo es el encargado de administrar y crear, las diferentes configuraciones de los puntos de acceso. Estos, cuando tengan conectividad, se descargarán de manera automática, la configuración establecida para ellos. De esta manera, se consigue un punto de control centralizado de toda la red. En él, se modifica todo lo relativo a la configuración más técnica del sistema. Es posible llevar a cabo la creación de los operadores, otorgando roles (tales como administrador total, permisos para crear nuevas configuraciones, permisos para eliminar configuraciones, simple observador, etc...) que podrán llevar a cabo, figura 28.

Además, en este módulo, se guarda información útil sobre la red. Esta información puede ser entre otras: la cantidad de tráfico generado por cada VPN[17] (recordemos que cada punto de acceso puede tener varias conexiones VPN), direcciones MAC, localización geográfica, configuración de red, etc…

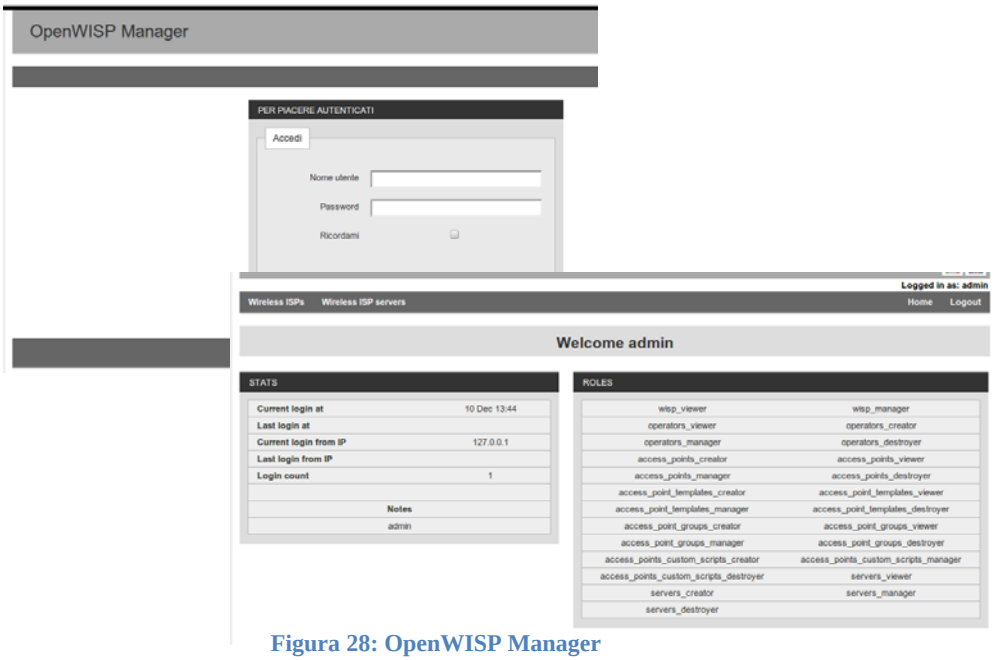


Figura 28: OpenWISP Manager

2.1.3 OpenWISP Firmware

Se trata de la configuración de los puntos de acceso utilizados para abastecer la red. Al reconfigurar y grabar en la memoria flash de estos dispositivos, la configuración necesaria para conectarse con OpenWISP Manager, obtenemos un sistema de control cerrado. Cada vez que un nuevo punto de acceso[27], se conecta a la red, éste descarga la configuración pertinente, es decir su firmware, desde OpenWISP Manager. Por lo tanto, este módulo no es una parte visible del sistema, no obstante es uno de los pilares del mismo. Figura 29

Otra de las ventajas que ofrece este módulo, es la de contar con una interfaz gráfica web. En ella, el administrador de la red puede configurar tanto los parámetros básicos de la red, como llevar a cabo pruebas de funcionamiento o rendimiento.

Este módulo está basado en OpenWRT* [37]. Éste, es un sistema operativo para dispositivos de red, basado en una distribución Linux. Proporciona un sistema de escritura de archivos completo, además de un gestor de paquetes. Este sistema permite personalizar una gran variedad de dispositivos, sin necesidad de utilizar el software original del proveedor. Ver apartado: OpenWRT.

Hasta el momento, han sido testeados algunos puntos de acceso comunes en el mercado, para que su funcionamiento con este firmware sea el esperado. Más adelante, en el capítulo 3, apartado 5 serán analizados con detenimiento.

Figura 29: OpenWISP Firmware

[27] Entendemos por “punto de acceso” a un dispositivo que interconecta diversos dispositivos de comunicación, tanto de red cableada como inalámbricos, con la finalidad de ofrecer un servicio mayor.

2.1.4 OpenWISP Captive Portal Manager

Este módulo es básicamente un portal captivo. Todo el tráfico de la red, y por lo tanto, de los diferentes usuarios ha de pasar a través de él. Su funcionamiento está basado en habilitar reglas en el cortafuego del servidor.

De esta manera, es capaz de controlar el movimiento de datos, y finalmente cumplir con los requisitos legales vigentes, vistos en el punto anterior. OpenWISP es capaz de mantener desplegado de manera simultánea, varios portales captivos en un mismo servidor.

Algunas de sus características más importantes son:

- Permite establecer múltiples instancias (una por cada interface física o virtual).
- Autenticación local o mediante un servidor RADIUS.
- Multiplataforma, permite ser desplegado en diversos sistemas operativos.
- Soporta IPv6.
- Catalogación de tráfico por usuario (versión Beta)

2.1.5 OpenWISP Geographic Monitoring

Por último, este módulo provee de una herramienta para poder establecer la localización geográfica de los puntos de acceso funcionales. Se encuentra escrito bajo Ruby on Rails y HTML5[38]. Se trata básicamente de una herramienta extra de administración. Figura 30.

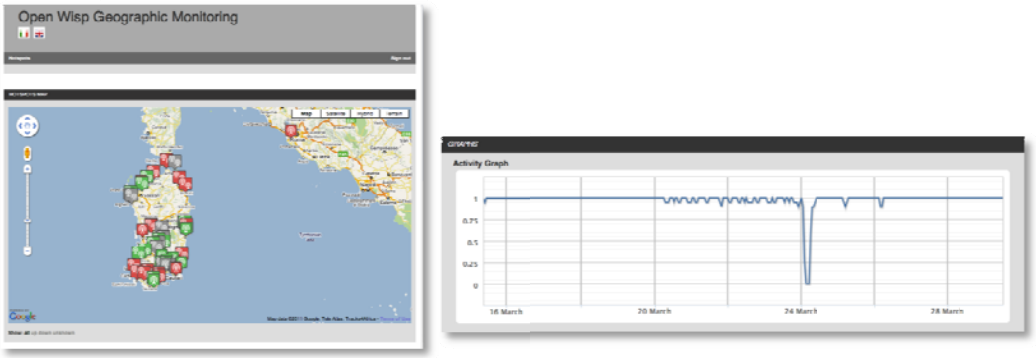


Figura 30: OpenWISP Geographic Monitoring

Además, consta de otros módulos que si bien no son imprescindibles para el funcionamiento del sistema, le aportan mayor usabilidad y nuevas características:

- OpenWISP Middleware: Este módulo, provee de comunicación entre el resto de ellos, mediante la utilización de la arquitectura REST[39].

- OpenWISP Website: Este módulo, y tal como su nombre indica, provee el sitio web oficial ya listo para desplegar.

Otra gran característica del sistema OpenWISP, reside en la flexibilidad del mismo. Este sistema puede ser desplegado y funcionar correctamente, detrás de un corta fuegos o "Firewall" [40], e incluso si un NAT[41] es utilizado, figura 31.

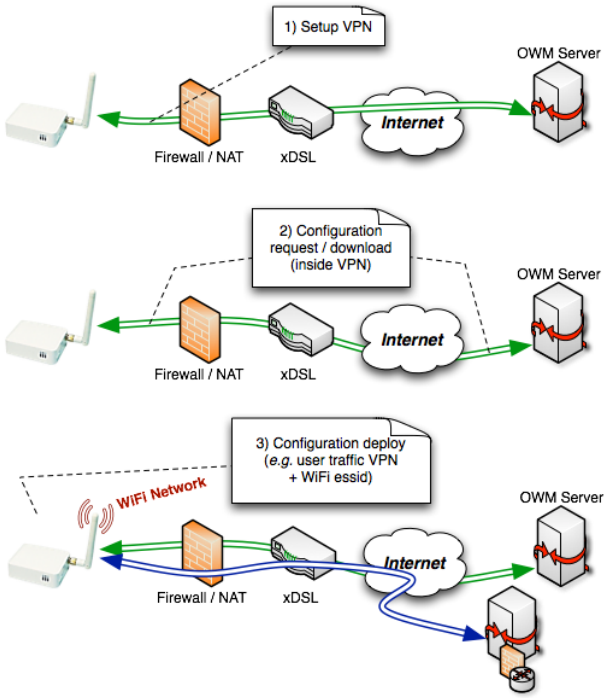


Figura 31: Arquitectura descarga configuración

Cada vez que un dispositivo de red, o punto de acceso en nuestro caso, tiene conectividad con la red; éste crea un túnel mediante la utilización de VPN, o redes virtuales privadas, con el servidor OpenWISP Manager. Esta conexión se lleva a cabo con el objetivo de descargarse automáticamente la última configuración establecida, para ese dispositivo en concreto. Periódicamente, el punto de acceso pregunta al servidor si existe una nueva configuración para estar siempre actualizado.

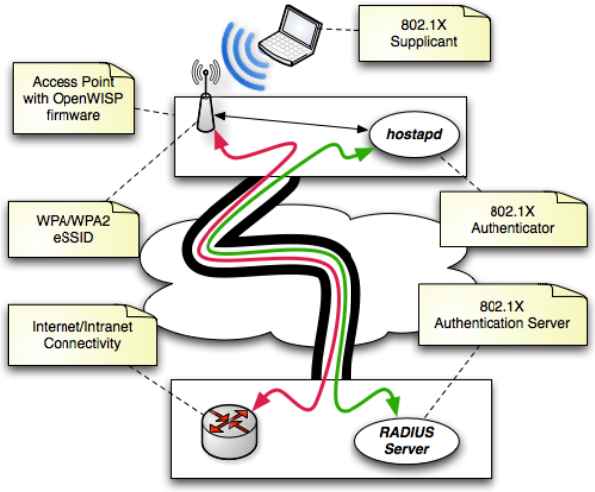


Figura 32: Esquema tunelado VPN de OpenWISP

En la figura 32, observamos cómo el sistema tiene la habilidad de encapsular dos conexiones diferentes sobre un mismo túnel. De esta manera es posible crear y distinguir diferentes tipos de redes, otorgándoles políticas de uso diferenciadas.

A continuación, se muestra en la figura 33 un esquema de funcionamiento de la arquitectura completa del sistema, y la interacción que existe entre los diferentes módulos.

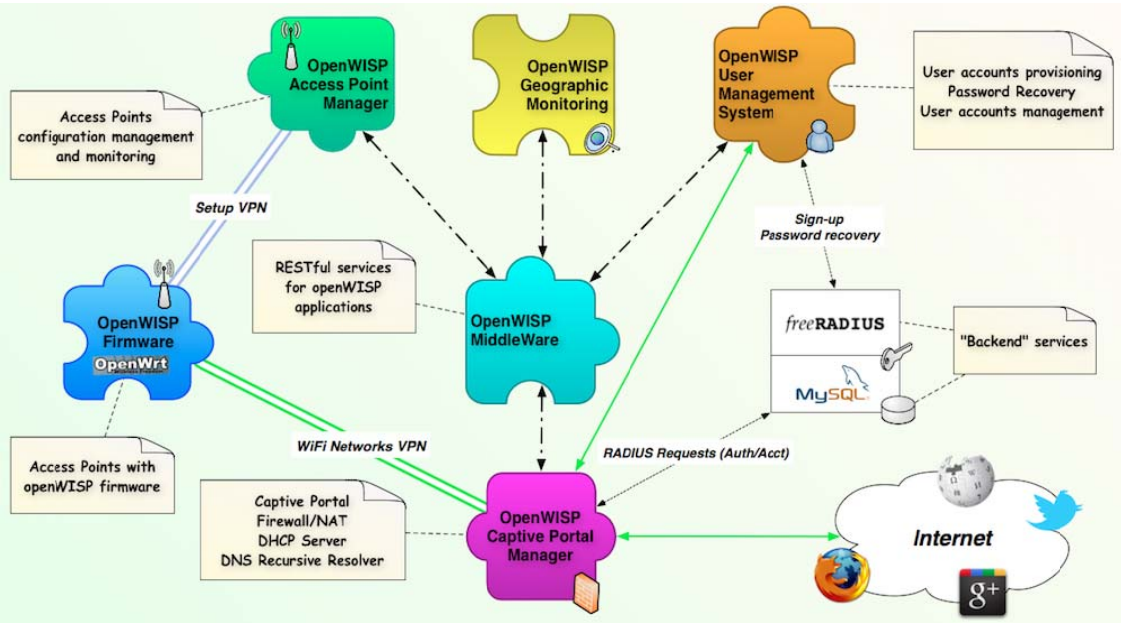


Figura 33: Arquitectura OpenWISP

2.2 Fases de la implementación de OpenWISP

El sistema OpenWISP, tal y como anteriormente se ha comentado, no necesita tener desplegado todos sus módulos para comenzar el funcionamiento. Una de sus ventajas, es que estos pueden ser añadidos a posteriori de la puesta en marcha del sistema. A continuación, se enseñarán diversos bloques de funcionamiento del sistema:

- **Despliegue 1**: el despliegue más básico del sistema (solamente dos módulos). Tendría la siguiente arquitectura, como observamos en la figura 34:

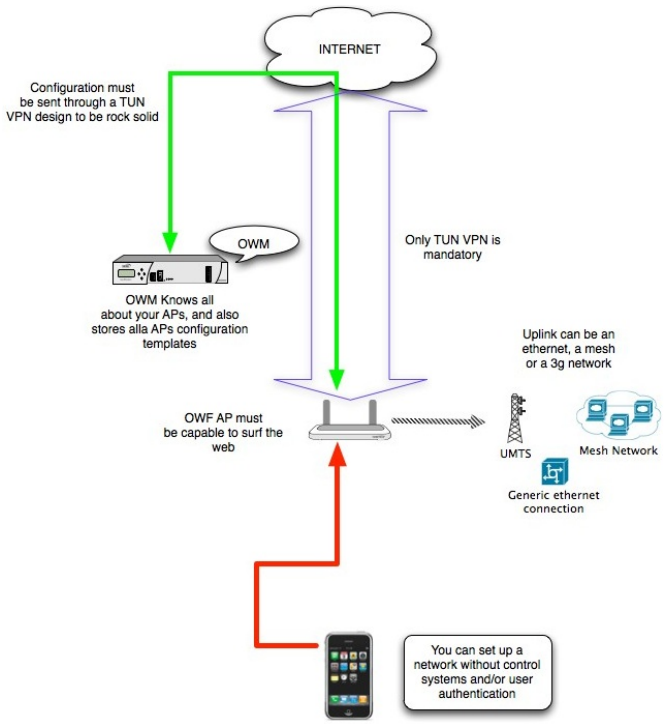


Figura 34: Primer despliegue del sistema OpenWISP.[28]

En ella podemos observar el funcionamiento del sistema, utilizando únicamente dos módulos: OpenWISP Firmware y OpenWISP Manager. El primero se introduce en los dispositivos de red, puntos de acceso, para dotarlos de la configuración inicial necesaria para su funcionamiento; mientras que el segundo se ejecuta de manera virtual en un servidor.

Una vez que los dispositivos de red tienen conectividad a Internet, se conectan de manera automática al servidor en que se encuentra alojado OpenWISP Manager. De esta manera, puede descargarse la configuración que el administrador ha establecido para ese

[28]Imagen extraída de https://spider.caspur.it/wiki/ow/How_it_works

dispositivo en concreto (pudiendo distinguir o dotar de una configuración diferente a cada punto de acceso).

Una vez recibida la configuración, el sistema está listo para funcionar según lo estipulado. Cada usuario que se conecte al punto de acceso, gozará de acceso libre y gratuito a Internet.

Para dotar de seguridad y dar robustez al sistema, todas las comunicaciones entre el punto de acceso, y el servidor OpenWISP Manager, se llevan a cabo mediante el uso de una red virtual privada.

- **Despliegue 2:** a la configuración anterior, se le añade el módulo geográfico, OpenWISP Geographic Monitoring. Tendría la siguiente arquitectura, figura 35:

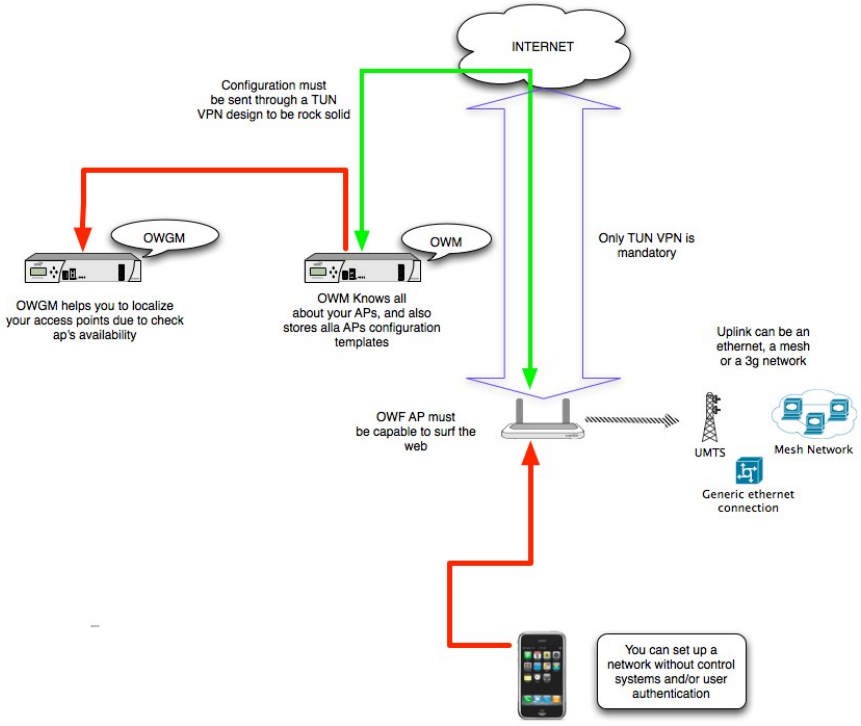


Figura 35: Segundo despliegue del sistema OpenWISP. [28]

En este tipo de despliegues, podemos observar cómo es añadido el módulo geográfico. Recordemos que este módulo, permite al administrador del sistema, obtener información sobre la localización geográfica del dispositivo de red o punto de acceso. Esta información permitirá una mayor flexibilidad, y dotará al administrador de la red, de la posibilidad de filtrar configuraciones por localización. Este nuevo módulo no es visible de cara al usuario final, y solo resulta de utilidad al administrador de la misma.

- **Despliegue 3:** en esta configuración, se añaden los módulos relacionados con la administración de usuarios: OpenWISP Captive Portal Manager y OpenWISP User Management. Tendría la siguiente arquitectura, tal y como observamos en la figura 36:

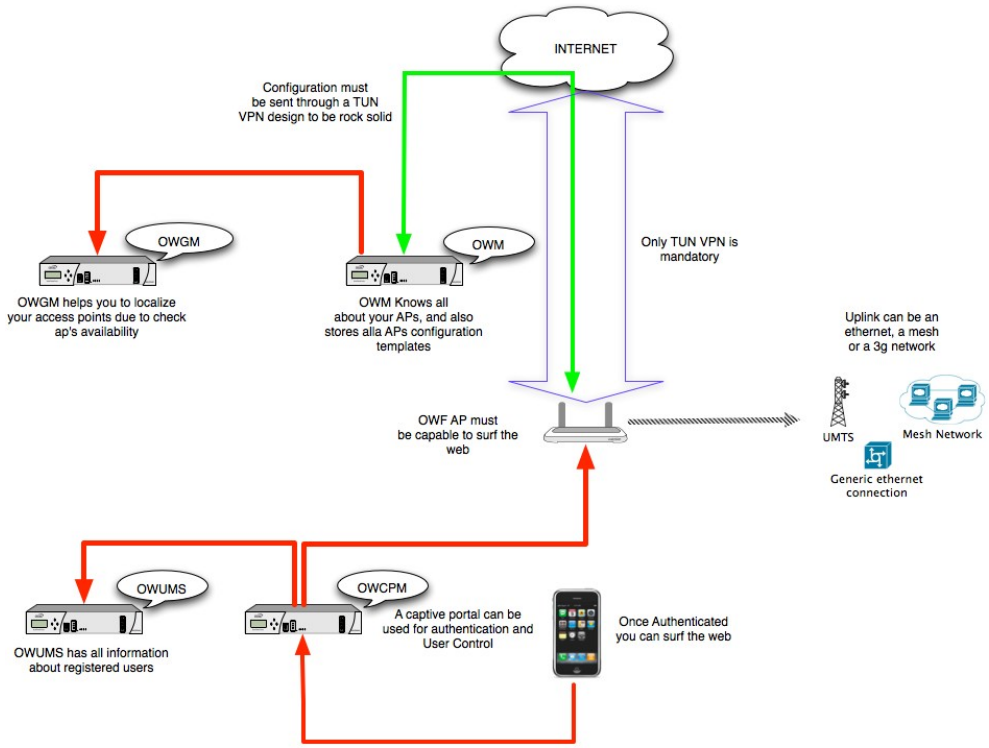


Figura 36: Tercer despliegue del sistema OpenWISP.[28]

Este tipo de despliegues, resultan interesantes debido a que proporciona un sistema para la administración y gestión de usuarios de la red.

Mediante el módulo de OpenWISP User Management, los usuarios al conectarse al sistema, pueden crear una cuenta para comenzar a disfrutar de la red. Además, pueden guardar o modificar sus datos personales y contraseñas. Tal y como se comenta anteriormente, para llevar a cabo esta tarea, este módulo se despliega junto a un servidor FreeRadius y una base de datos SQL.

El módulo OpenWISP Captive Portal Manager, ofrece una solución para cubrir los requerimientos legales según la vigente legislación. A través de él, puede llevarse a cabo un control sobre los usuarios, el uso que estos están haciendo de la red, o retener información sobre ellos, necesaria debido a requerimientos legales.

- **Despliegue 4:** en esta última configuración, el valor añadido es la encapsulación del tráfico generado por cada uno de los usuarios, mediante redes virtuales privadas. Tendría la siguiente arquitectura como observamos en la figura 37:

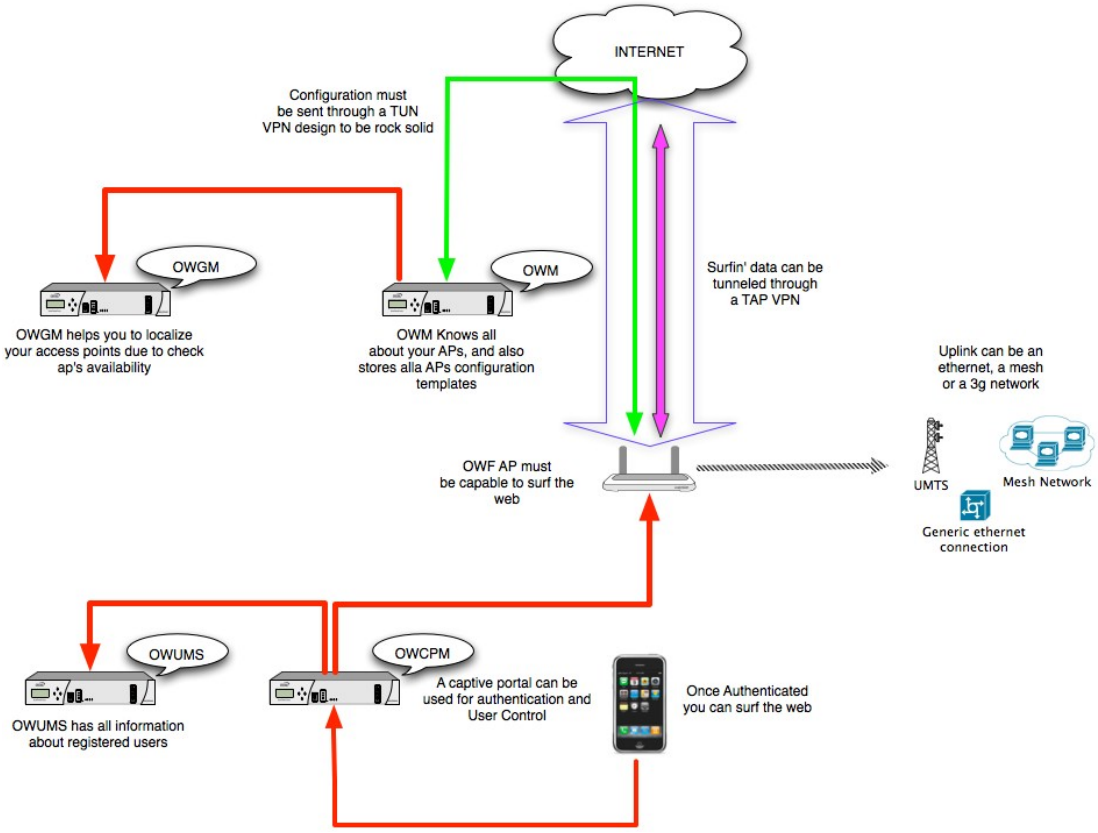


Figura 37: Cuarto despliegue del sistema OpenWISP. [28]

Observamos que resulta idéntica al último despliegue visto, pero como se comenta justo sobre la imagen, en este caso, todo el tráfico de los usuarios viaja encapsulado bajo una red privada virtual, VPN. Cada usuario, al conectarse y comunicarse a través de este sistema, genera un tráfico de datos que se encapsula de manera única. De este modo, se obtiene una nueva VPN por cada cliente que esté generando tráfico.

El objetivo de esta acción, es dotar de robustez y mayor seguridad, a la información personal del usuario conectado a la red.

2.3 OpenWRT

OpenWRT es un sistema operativo para dispositivos de red, basado en una distribución Linux, creado en 2004. Proporciona un sistema de escritura de archivos completo, además de un gestor de paquetes. Este sistema permite personalizar una gran variedad de dispositivos, sin necesidad de utilizar el software original del proveedor.

Una gran variedad de dispositivos de red son soportados por este sistema, lo que hace relativamente fácil crear una configuración predeterminada, cerrada y funcional para poner en marcha una red.

Para los desarrolladores, OpenWRT provee de un paquete de trabajo que permite crear una aplicación, sin necesidad de compilar o crear un firmware desde cero. Para los usuarios, permite alcanzar un nivel de personalización completa, permitiendo utilizar toda la capacidad disponible de los dispositivos.

Algunas de sus características más importantes son:

- Software libre: El proyecto entero es de libre uso, modificación, compartición y distribución, ya que se encuentra licenciado bajo GNU GPL[28].
- Abierto a nuevas contribuciones: El proyecto se encuentra siempre abierto a nuevas contribuciones, y no pone barreras para que cualquier interesado pueda participar en él.
- Gran comunidad: Existe un gran número de personas involucradas en este proyecto, y trabajando colaborativamente en él. Aproximadamente consta de 40 programadores a tiempo completo, con miles de usuarios en todo el mundo.

Es por estos motivos que OpenWRT, sea probablemente la solución más completa en su categoría. Dados sus niveles de rendimiento, estabilidad, flexibilidad, robusteza y diseño, se ha convertido en el firmware más extendido para dispositivos embebidos. No obstante, hay que remarcar, que no se trata de un firmware orientado al usuario final, ya que requiere un cierto conocimiento de sistemas Linux y de operaciones bajo línea de comandos, figura 38.

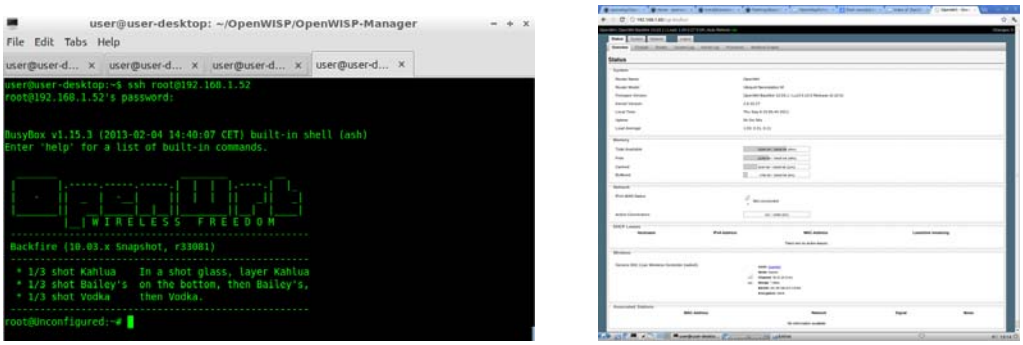


Figura 38: OpenWRT

CAPÍTULO 3: ARQUITECTURA, NORMATIVA Y MODELO DE VIDA DEL PROYECTO.

3.1 Normativa para federarse a Free Italia WiFi

Actualmente, el sistema que ya se encuentra desplegado en Italia, bajo el seudónimo de Provincia WiFi y Free Italia WiFi, es la mayor red mundial ofrecida por parte de una administración pública de acceso a Internet gratuito sin cables, WiFi. En un principio se está dando servicio a más de 4 millones de personas, en más de 100 municipios, y creciendo día a día. Podemos apreciar en el mapa de la figura 39, que aún queda mucho territorio por ser abastecido con esta solución.

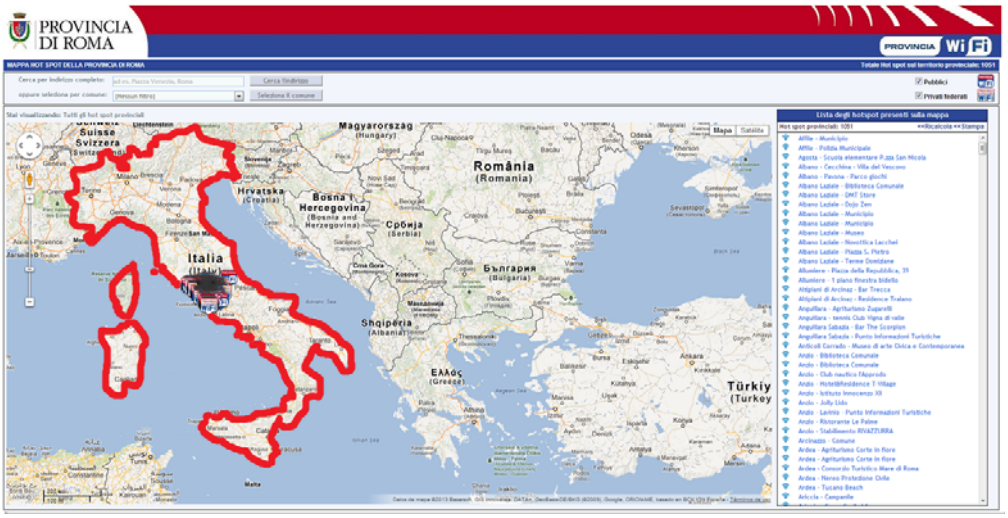


Figura 39: Mapa con el territorio ofrecido por Provincia WiFi

Para aclarecer un poco más sobre este proyecto, "Free Italia WiFi" es un proyecto llevado a cabo por la Provincia de Roma, la región autónoma de Cerdeña y el ayuntamiento de Venecia, dirigida a las administraciones públicas. Su objetivo es el de ofrecer e implementar la primera red federada[29] de acceso gratuito a internet sin cables, para todos los ciudadanos. Por lo tanto, busca incentivar y promover la colaboración dentro del

[29] Entendemos por red federada, el hecho de que ésta, está formada por diversas redes independientes unas de otras. De esta manera, convergen en un punto central, teniendo completa interconexión entre ellas, y por lo tanto, de sus usuarios, pero sin renunciar a su funcionalidad individual.

sector público, para contribuir a la alfabetización digital y velar por el derecho de la ciudadanía, a acceder libremente a Internet.

Otro de los puntos interesantes de este proyecto, es que está basado en software y código abierto y de libre distribución, permitiendo así, que se innove desde la sociedad.

Actualmente, todas las comunidades, gobiernos o ayuntamientos que deseen adherirse a "Free Italia WiFi" han de cumplir con ciertas normas establecidas para el buen funcionamiento del mismo. Estas son entre otras:

1. La administración y/o control de la red por las autoridades. Se permite la participación privada en la gestión de la misma, siempre y cuando, se haga en nombre de la administración y cumpla la normativa.
2. El acceso abierto y sin discriminación a todos los ciudadanos que conformen la administración. La capacidad de registrarse y utilizar la red, ha de ser garantizado para todos los ciudadanos.
3. Uso gratuito. El uso de la red debe de ser libre para todos los usuarios.
4. Carácter no lucrativo de la red. Esta red no tiene fines de lucro, y por lo tanto, no ha de ser explotada comercialmente por cualquier persona, objeto o entidad, aún con el consentimiento de la administración. Incluso, los datos del usuario y los relacionados con el uso de la red, no pueden ser transferidos a terceros ni utilizados para fines distintos de los previstos en la gestión propia de la red.
5. Neutralidad de la red. No existen restricciones arbitrarias respecto al acceso a Internet y sus servicios, ni a los dispositivos utilizados por el usuario final para conectarse a la misma.
6. Operar dentro del marco legal. La gestión de la red debe llevarse a cabo de acuerdo con las regulaciones nacionales y locales.
7. Publicidad del servicio. El servicio debe ser garantizado y promovido, mediante las administraciones. Éstas deben ofrecer una lista de los servicios que se ofrecen, e indicaciones sobre cualquier restricción de uso o registro, y una referencia a la ley sobre la información requerida por ésta.
8. Garantía del uso de red para todos los usuarios. Cada administración garantizará el cumplimiento de los principios enumerados anteriormente para los usuarios registrados de otras redes federadas a "Free Italia WiFi". Además, ha de garantizar los niveles mínimos de servicio, ya sea horario o de tráfico. Éstos mínimos son de dos horas de conexión, no necesariamente continua al día, y un mínimo de subida y descarga de datos, de no menos de 300MB durante esta franja temporal.

3.2 Normativa técnica

No obstante, las administraciones que quieran adherirse al proyecto “Free Italia WiFi”, también han de cumplir la siguiente normativa técnica.

Las administraciones públicas y las instituciones que se asocien con la red federada “Free Italia WiFi” han de compartir y acoger las disposiciones contenidas en el reglamento técnico que rige y define la infraestructura tecnológica para la interconexión de redes WiFi. Este reglamento ha sido elaborado por el Comité Técnico, integrado por representantes de los tres promotores (Provincia de Roma, Región Autónoma de Cerdeña y Ciudad de Venecia) y el Consorcio Interuniversitario CINECA[42]. Este último es el operador técnico del proyecto.

La característica técnica principal que presenta este proyecto, se basa en compartir un único punto de interconexión, denominado IX-WiFi, a nivel de infraestructuras como de regulación, a través del cual se unen los sistemas de autenticación de las diversas entidades que componen el sistema.

El reglamento técnico contiene todas las normas técnicas de admisión a la red, y los acuerdos de interconexión dentro de la estructura IX-WiFi. El cumplimiento de estas reglas, son una condición necesaria para poder solicitar el ingreso en el proyecto. La versión completa del documento original se adjunta al proyecto como anexo. No obstante, se ha traducido el aspecto normativo técnico para la instalación y configuración:

[…]

“Las normas técnicas para la instalación y configuración”

La entidad que desee participar en la federación de redes Wi-Fi, se conectará a “IX-WiFi” usando un proxy[43] RADIUS.

La “IX-WiFi” procederá a la configuración apropiada de su proxy RADIUS, para reenviar las solicitudes de autenticación del servidor RADIUS de la nueva entidad federada, al resto de servidores RADIUS de las entidades restantes.

Modo Federación[29]

La federación se logra mediante el uso de un proxy RADIUS puesto a disposición por "IX-WiFi", que permite al afiliado, mediante roaming (“itinerancia”), utilizar la infraestructura Wi-Fi de otras entidades federativas.

A cada afiliado le será asignado por "IX-WiFi", un "realm" que, a través del atributo "User-Realm" (de tipo “string” y el código diccionario de RADIUS, “223”) se identificará a sus usuarios, cuando sea requerido, en otras entidades federativas.

El afiliado se compromete a:

-implementar y mantener un servidor RADIUS, que pueda ponerse en contacto (en la forma que se establece a continuación) con el proxy RADIUS del “IX-WiFi”;

- dirigir las peticiones de autenticación relativa a los usuarios de otras entidades federativas, hacer "roaming" de la entidad al proxy RADIUS del “IX-WiFi”, especificando en ella el atributo User-Realm, con valor igual al código de federación, correspondiente a las entidades a las que pertenece el usuario, asignado por “IX-WiFi”;

-utilizar los paquetes de tipo “Access-Request” dirigido al proxy RADIUS del “IX-WiFi”, y en relación a los usuarios que no pertenecen a su dominio, el atributo “User-name” de RADIUS de la siguiente forma: <usuario> @ <realm entidad federada >.

-implementar y mantener un servidor RADIUS conectado (en la forma que se establece a continuación) desde el proxy RADIUS del “IX-WiFi”;

-únicamente se utilizará PAP como esquema de autenticación RADIUS para las solicitudes dirigidas a la “IX-WiFi”;

-aceptar y procesar adecuadamente las solicitudes de autenticación de proxy RADIUS del “IX-WiFi”, de usuarios de otras entidades federativas.

La conectividad entre el servidor RADIUS y el servidor proxy RADIUS de la entidad federada a “IX-WiFi”, debe asegurar la integridad y confidencialidad de la información en tránsito, mediante al menos una de las siguientes maneras: VPN Layer2, Layer3 VPN, circuitos dedicados.

Es responsabilidad del afiliado, el proporcionar los materiales necesarios y la instalación de los equipos en la sede de su punto de interconexión. Además de la aplicación de la infraestructura necesaria para la protección de las comunicaciones relativas a la autenticación RADIUS.

Están disponibles para la conexión al proxy RADIUS puertos Ethernet 10/100 Mbps RJ45.

El afiliado también tendrá que adoptar las medidas necesarias para:

-adoptar la autenticación RADIUS sólo en los puertos UDP asignados por “IX-WiFi”;

-adoptar el direccionamiento IP privado asignado por “IX-WiFi” (en este caso) por la cual, llegarán las peticiones de autentificación de los usuarios de otras entidades federadas, en cualidad de "roaming", o por la cual llegarán las solicitudes de autenticación de sus usuarios mediante otras entidades federativas, en cualidad de "roaming".

[…]

El no cumplimiento de este reglamento, comportará un aviso al contacto técnico del ente que lo haya violado. En el caso de que este comportamiento sea repetido o frecuente, el comité técnico se reserva el derecho de efectuar o llevar a cabo medidas de actuación según estime conveniente para remediar el problema.

3.3 Modelo de vida del proyecto

El proyecto, como se comentó anteriormente, se basa en la filosofía “Bottom-up”, y por lo tanto, cabe destacar que su objetivo final no es meramente lucrativo. De hecho la iniciativa de nuestros colegas italianos, “Free Italia WiFi”, basa su actividad económica en aportaciones de los ayuntamientos que se encuentran afiliados al proyecto. Además, obtienen ingreso por cada nuevo cliente (y entendemos por cliente, a aquel que pone al alcance de los usuarios, un nuevo punto de acceso a la red) que adquiere un dispositivo para conectarse. En este caso, el cliente abona al proyecto el coste íntegro del dispositivo, para así, sufragar su gasto.

Es por este motivo, que se podría decir que el punto más débil del proyecto es su sostenimiento económico. En este ámbito, además del modelo de mantenimiento por medio de las organizaciones o ayuntamientos públicos que se adhieran, se pueden proponer nuevos modelos. Si bien, en alguno de los casos, no son compatibles entre ellos o con la basa de la financiación pública, a continuación se proponen algunos.

Uno de ellos, podría ser el incluir publicidad o anuncios en los portales captivos. Así, cuando los usuarios se conectasen a la red, visualizarían estos anuncios, aportando beneficios económicos para el sistema. A su vez, utilizando el módulo geográfico de OpenWISP, podría personalizarse la publicidad según la situación geográfica del punto de acceso. De este modo, se lograría involucrar también a comerciantes locales que encontrarían en este sistema, un nuevo método para anunciarse y aumentar su segmento de mercado. No obstante, es necesario para el desarrollo del proyecto, contar con el apoyo de los comerciantes locales desde el inicio del proyecto, por motivos de viabilidad. Cualquiera de estas opciones, resultaría incompatible con el modelo de financiación pública, debido a que se estarían quebrantando las leyes de libre mercado al tener ventaja sobre las iniciativas privadas.

Podría establecerse también un nivel de usuario “Premium”, el cual pagando una cuota, tuviese acceso a Internet sin algunas de las restricciones que algunos países establecen, para la libre e igualitaria actividad de sus mercados. En este caso, esto es posible, debido a que al cobrar por la actividad profesional, no se incumplen las normas de libre mercado, pudiendo así dar los máximos servicios que se puedan ofrecer. Si esta es la opción escogida, consecuentemente, el proyecto ha de darse de alta como operador de telecomunicaciones en España.

Otra posible solución al esquema de financiamiento de la misma, es utilizar métodos modernos de financiación que envuelvan al usuario final y lo hagan partícipe del proyecto. Hacemos referencia a "crowdfunding" o "verkami". En este sistema, los usuarios finales son participes del proyecto y no meros consumidores, ya que pueden aportar una cantidad de dinero que ellos deseen. A cambio, con su pequeña aportación, el proyecto puede continuar adelante. Existen diversas plataformas como Goteo[30] o KickStarter[31] en los que han surgido casos de éxito utilizando éste método de financiación, como pueden ser: el famoso videojuego "Minecraft"[32], la consola de videojuegos basada en un sistema operativo libre "Ouya"[33] o una película sobre la serie de televisión "Veronica Mars"[34] entre muchas otras.

Sobre el mantenimiento y la sostenibilidad de la red a medio/largo plazo, al tratarse de una red compuesta por diversas redes federadas, cada red se encargará de su propio mantenimiento y sostenibilidad. De esta manera, la arquitectura de la red se mantiene en consonancia con la filosofía de apertura y federación.

3.4 Arquitectura

Pasando al apartado más técnico de nuestro proyecto, la base necesaria para el funcionamiento total del sistema, no es muy amplia y esto favorece al desarrollo del mismo.

En primer lugar, se necesita un servidor con acceso a Internet mediante una dirección IP pública estática. Éste será el encargado de ejecutar OpenWISP Manager para poner en marcha el sistema de gestión de configuraciones de los puntos de acceso. Por lo tanto, necesitaremos también desplegar aquí un servidor OpenVPN, para establecer las redes virtuales privadas, desde dónde los puntos de acceso descargarán sus configuraciones de manera segura.

Luego es necesario, y como resulta evidente, puntos de acceso correctamente configurados con el firmware de OpenWISP. De esta manera, podremos controlar su funcionamiento y configuración de manera remota, y totalmente centralizada.

---

[30] Goteo. 2013. Goteo. Consultado 10/05/2013. http://goteo.org/

[31] KickStarter. 2013. KickStarter Inc. Consultado 10/05/2013. http://www.kickstarter.com/

[32] Minecraft. 2013. Notch Development AB. Consultado 01/05/2013. http://minecraft.net/

[33] Ouya. 2013. Ouya Inc. Consultado 01/05/2013. http://www.ouya.tv/

[34] Veronica Mars. 2013. Rob Thomas. Consultado 01/05/2013. http://www.imdb.com/title/tt0412253/

Por motivos de transparencia, seguridad y robustez del sistema, se establecería un segundo servidor que llevase a cabo todo lo relacionado con los usuarios. Este servidor necesita también de una Gateway (o salida a Internet) mediante una IP pública estática, para ser accedido remotamente. De esta manera, correría OpenWISP User Management y OpenWISP Captive Portal Manager. Aquí, también se pondrá en marcha un servidor FreeRADIUS, para utilizar el protocolo RADIUS como medio para llevar a cabo la autenticación y autorización de usuarios.

RADIUS, es un protocolo de arquitectura cliente/servidor, que permite llevar a cabo la autenticación de usuarios, y así otorgarles autorización para efectuar ciertas funciones. Tiene la característica funcional, de permitir conexiones a servidores remotos, los cuales se comunicarán con un central o de mayor jerarquía. De esta manera, se logra una división y flexibilidad en el sistema. Este es un punto indispensable para llevar a cabo este proyecto, ya que no olvidemos, que la mayor ventaja competitiva de OpenWISP frente a otros sistemas, es la ubicuidad de sus usuarios.

Supongamos entonces, que un usuario del sistema en Barcelona (registrado en el servidor de Barcelona), ha de viajar a Roma. En el caso de que quiera conectarse a OpenWISP, podrá hacerlo con sus mismas credenciales de origen. Esto es posible debido a que el sistema, al intentar verificar el usuario, comprobará el servidor local (en nuestro ejemplo Roma). Al no encontrarse el usuario allí, enviará las credenciales del usuario, a un servidor de más alto nivel que llevará a cabo una función de intermediario. Técnicamente éste recibe el nombre de “proxy”. Este entonces lo pondrá en contacto con otro servidor que podría contener estos datos. De esta manera, el servidor de Roma, se pondría en contacto con el de Barcelona para verificar que los datos introducidos por el usuario, fuesen correctos. Podemos observar un ejemplo visual en la figura 40.

El diseño del sistema, no obstante, puede variar fuera de los límites de cada país. Esto significa, que cada país integrante del sistema, puede por lo tanto, tener tantas capas de servidores RADIUS, como crea conveniente. Esta regla es válida, siempre y cuando exista interoperabilidad entre su o sus servidores de más alto nivel, con los del resto de integrantes del proyecto.

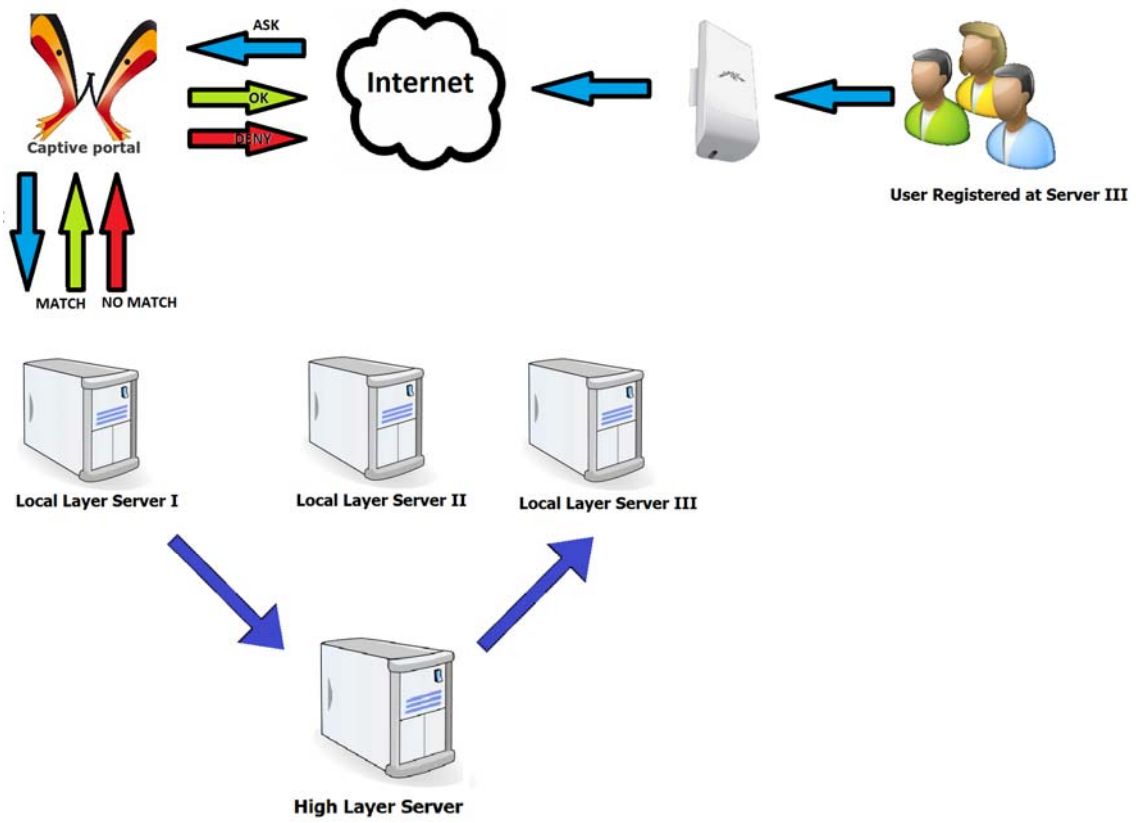


Figura 40: Ejemplo de arquitectura Radius a diferentes niveles

En la figura 41 observamos la arquitectura completa del sistema OpenWISP. Podemos observar como el usuario final puede conectarse a cualquier punto. Simplemente, ha de identificarse o registrarse en el sistema. En el último de los casos, la ventaja de este sistema respecto a todos los demás, es que tiene la característica de ser ubicuo, cosa que hace posible el uso de las credenciales del usuario, en cualquier país europeo que forme parte del proyecto. A partir de aquí, todo lo que ocurre por detrás, resulta totalmente transparente al usuario, y por lo tanto, en ningún momento se ve involucrado.

Desglosándola por partes, podemos decir que existen dos partes independientes una de otra. El sistema de gestión y tratamiento de configuración, y el sistema relativo a los usuarios.

El sistema de gestión de las configuraciones, está basado por el dispositivo de red, y el módulo OpenWISP manager, tal y como se explica en el apartado relativo a OpenWISP. Para llevar a cabo las comunicaciones entre estas dos partes, se utiliza una red virtual privada, o VPN, para asegurar las comunicaciones entre ambos. Todo esta parte del sistema, resulta totalmente invisible al usuario final.

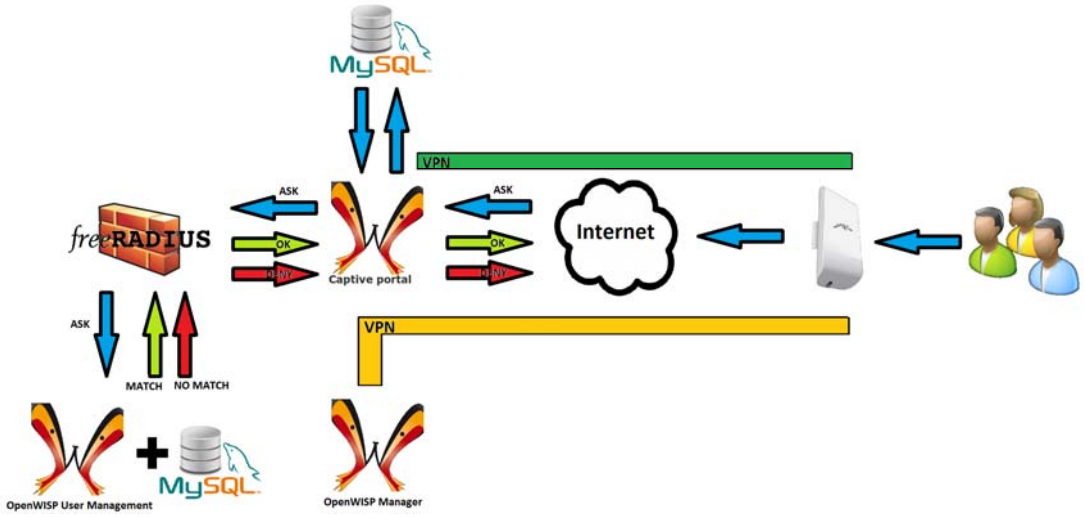


Figura 41: Arquitectura del sistema OpenWISP

Por otro lado, nos encontramos con la parte del sistema relativo al tratamiento del usuario, y todo lo referente a él. Por lo tanto, cuando un usuario se conecta a un dispositivo de este sistema, se requiere una autenticación por su parte. Si este se ha conectado por primera vez, será necesario un registro, si no este caso, entonces simplemente identificarse. Una vez llevado a cabo este paso, el usuario podrá navegar por Internet, siendo totalmente ajeno al trabajo que lleva a cabo el sistema.

Cuando un usuario accede al sistema, éste comprueba los datos introducidos por el usuario. Dependiendo entonces, desde que punto de acceso esté conectado el usuario, se lo reenviará a un portal captivo predeterminado. Como se ha comentado anteriormente, OpenWISP permite establecer diversos portales captivos y asignar grupos de dispositivos a estos portales. Éstos, se utilizan para limitar el tráfico de los usuarios, de acuerdo a la legislación de cada país, de esta manera se consigue que el sistema sea completamente legal.

3.5 Equipos

De entre todos los equipos soportados, y testeados, por OpenWISP, nos encontramos con cuatro fabricantes diferentes pero muy reconocidos. Sin embargo, la solución podría funcionar en un mayor número de dispositivos. El motivo por el que se no han añadido a la lista, es que no han sido testeados correctamente, y podrían no presentar el efecto deseado.

La lista de los dispositivos de red, probados y que funcionan correctamente bajo OpenWISP son:

- D-Link DIR 825[35]
- Abocom WAP 2102[36]
- Alix[37]
- UBNT[38]
    - NanoStation / NanoStation Loco
    - NanoStation M2/M5 / NanoStation Loco M2/M5
    - PicoStation / PicoStation M
    - UniFi – Cualquier modelo de la gama
    - Airwire - Descatalogado
    - PowerAPN - Descatalogado
    - Routerstation - Descatalogado

A continuación se expondrán los motivos por los que se ha escogido el modelo NanoStation M2, para llevar a cabo este piloto y no el resto. No obstante, y cabe comentar, que cualquiera de los anteriormente expuestos, serviría para esta función, teniendo en cuenta obvias diferencias técnicas.

De todos los modelos anteriormente expuestos, se descartaron todos los descatalogados por razones evidentes. Entonces pasaremos a exponer brevemente las cualidades de cada uno de estos equipos.

- D-Link DIR 825

Se trata de un dispositivo enrutador, más conocido como “router”, diseñado para interiores. Necesita el uso de alimentación externa.

Figura 42: D-Link DIR 825

Soporta el uso de ambas bandas de frecuencia WiFi sin licencia, esto es 2,4GHz y 5GHz. Una de las ventajas que presenta, es que consta de dos interfaces de radio diferenciadas,

[35] http://www.dlink.com/es/es/

[36] http://www.abocom.com.tw/

[37] http://pcengines.ch/alix.htm

[38] http://www.ubnt.com/

por lo que puede trabajar en ambas frecuencias de manera simultánea. Ha sido diseñado para uso casero, y para usuarios de exigencia media-baja. Permite además, compartir otros dispositivos conectados a la red, como discos duros externos o impresoras. Trae integrado un sistema que implementa QoS[44] según las necesidades del usuario en tiempo real.

En cuanto a su aspecto más técnico, soporta los estándares IEEE 802.11n[45], IEEE 802.11b[46], IEEE 802.11g[47], IEEE 802.11a[48], IEEE 802.3[49] y IEEE 802.3u[50]. Como se comentaba, consta de dos interfaces radio diferenciadas, de cuatro puertos LAN[51] y un puerto WAN[52], además de puerto USB[53] extra.

Precio medio final: 98,33€. Ver tabla 5 Anexo IV.

- Abocom WAP 2102

Este dispositivo se trata de un punto de acceso. Necesita el uso de alimentación externa. Tiene un diseño minimalista y portátil, que lo hacen interesante por el poco espacio que ocuparía una posible instalación del mismo. Está pensado para trabajar en interiores, y por lo tanto, no soporta condiciones altas de humedad o frío.

Figura 43: Abocom WAP 2102

En el apartado técnico, no destaca por sus prestaciones. Trabaja en la banda de frecuencias de 2,4GHz únicamente. Por lo tanto, se basa en los protocolos 802.11b y 802.11g. Consta además de un puerto LAN.

Precio medio: Bajo demanda, entre 10€ y 20€.

- Alix

De todos los dispositivos presentados, es quizás el más diferente. A diferencia del resto, se trata de una placa de sistema, fabricada y vendida por la empresa PC Engines. Esta placa, es una versión básica, y no trae incorporada ningún tipo de tarjetas de red, o de memoria. Todos estos módulos han de adquirirse de manera separada.

Como observamos en la figura 44, no se trata de un producto cerrado y listo para utilizar, por lo que requiere de un mayor trabajo extra, para ponerlo en marcha.

Figura 44: Alix

La ventaja de este producto, respecto a los demás que hemos visto, es sin duda la flexibilidad y granularidad del mismo. Al ser básicamente modular, se puede adaptar para hacer frente a todo tipo de necesidades.

Precio medio final: 152,78€. Ver tabla 6 Anexo IV.

- UBNT NanoStation 2/5 - NanoStation M2/M5

Estos dispositivos se tratan de puntos de acceso. Han sido diseñados para trabajar tanto en interiores, como en exteriores. Cada modelo trabaja en un respectivo rango de frecuencias WiFi (2/M2 a 2,4GHz, 5/M5 a 5GHz). Una de las ventajas de estos dispositivos, es que se alimentan mediante POE[54], “Powered-over-ethernet”. Por lo que no requiere hacerles llegar un cable de alimentación externa, de manera directa, sino que se transmite por el mismo cable de red.

Figura 45: NanoStation 2/5 / M2/M5

En cuanto a su aspecto más técnico, soporta los estándares IEEE 802.11n, IEEE 802.11b, IEEE 802.11g, IEEE 802.11a, IEEE 802.3 y IEEE 802.3u.
La diferencia entre los modelos M y los demás, es que estos tienen soporte MIMO, “Multiple In-Multiple Out”[55]. Esta tecnología aprovecha fenómenos físicos como la propagación multi-camino de las ondas para incrementar la tasa de transmisión, y reducir errores. Esta tecnología se comenzó a utilizar en el estándar IEEE 802.11n y, básicamente, utiliza múltiples antenas para recibir y transmitir información.

La ventaja de todos los dispositivos de la compañía UBNT, es la gran comunidad de usuarios y desarrolladores que hay detrás de estos dispositivos. Traen como firmware de fábrica, un software propietario de la propia compañía, llamado AirOS[56], pero deja la opción de borrarlo e instalar el nuevo firmware al antojo del usuario.
Se adjunta la ficha técnica de estos dispositivos. Ver anexo.

Precio medio final: 79,42€. Ver tabla 7 Anexo IV.

- UBNT NanoStation Loco 2/5 – NanoStation Loco M2/M5

Estos dispositivos son muy similares a los anteriormente comentados. Son también puntos de acceso, que trabajan a las bandas de frecuencias de 2,4GHz o 5GHz, dependiendo del modelo.

Figura 46: NanoStation Loco 2/5 / M2/M5

Están diseñados tanto para su uso en entornos interiores, como exteriores. Se podría decir que estos modelos, son la versión menos potente y más barata de la gama NanoStation.).
También se alimentan mediante POE, “Powered-over-ethernet”. Por lo que no requiere hacerles llegar un cable de alimentación externa, de manera directa, sino que se transmite por el mismo cable de red.
En cuanto a su aspecto más técnico, soporta los estándares IEEE 802.11n, IEEE 802.11b, IEEE 802.11g, IEEE 802.11a, IEEE 802.3 y IEEE 802.3u
Como en la gama de dispositivos anteriores, estos modelos se diferencian por utilizar la tecnología MIMO o no.

Precio medio final: 54,01€. Ver tabla 8 Anexo IV.

- UBNT PicoStation – PicoStation M

Estos dispositivos son muy similares a los anteriormente comentados. Son también puntos de acceso, que trabajan a las bandas de frecuencias de 2,4GHz, y en su modelo ya descatalogado, a 5GHz. Están diseñados principalmente para su uso en espacios exteriores.

Su principal ventaja reside en su reducido tamaño. Además, la antena incorporada por defecto, es extraíble, habiendo la posibilidad de cambiarla por una que se adapte a las necesidades del usuario.

Figura 47: PicoStation / PicoStation M

También se alimentan mediante POE, "Powered-over-ethernet". Por lo que no requiere hacerles llegar un cable de alimentación externa, de manera directa, sino que se transmite por el mismo cable de red.
En cuanto a su aspecto más técnico, soporta los estándares IEEE 802.11n, IEEE 802.11g, IEEE 802.3 y IEEE 802.3u. Como en la gama de dispositivos anteriores, estos modelos se diferencian por utilizar la tecnología MIMO o no.

Precio medio final: 68,11€. Ver tabla 9 Anexo IV.

- UBNT UniFi

Esta última gama de la marca Ubiquiti, se trata de un nuevo punto de acceso. Dependiendo del modelo, trabaja en los rangos de frecuencia de 2,4GHz o 2,4GHz y 5GHz de manera dual.

Se trata de un diseño de interiores, pensado para dar soporte y cobertura WiFi en grandes superficies. Llegando a dar cobertura, de manera teórica, en un radio de 120m, en su modelo más básico, y 185m en su modelo más potente. No obstante, existe un modelo de exteriores, aunque con un diseño exterior totalmente diferente.

Figura 48: UniFi

Se alimenta también mediante un puerto POE, por lo que no requiere de conexión eléctrica directa, sino que se transporta mediante un cable de red Ethernet.

En cuanto a su aspecto más técnico, y dependiendo del modelo, soporta los estándares IEEE 802.11b, IEEE 802.11a, IEEE 802.11n, IEEE 802.11g, IEEE 802.3 y IEEE 802.3u.

Precio medio final: 113,04€. Ver tabla 10 Anexo IV.

Como podemos observar en la comparativa superior, la mayoría de estos dispositivos tienen características similares. Por lo que en definitiva, la elección de uno u otro, se verá condicionada al uso que se le pretende dar dentro del proyecto.

Además, hemos tenido en cuenta las estadísticas del uso del espectro de frecuencia sin licencia de WiFi. En ellas, observamos que si bien, el rango de 2,4GHz está muy ocupado, es el más utilizado con diferencia frente a la banda de 5GHz. Esto es debido principalmente, a las restricciones tecnológicas de los componentes extendidos entre la población. Es decir, a una falta de implementación de nuevas tecnologías compatibles con el estándar 802.11n, y que por lo tanto, pueda trabajar a una banda de frecuencias más altas. En un futuro no muy lejano, puede ser interesante barajar la opción de trabajar en 5GHz, ya que una gran parte del parque tecnológico de la población, soportará estas frecuencias.

En un primer momento se decidió por utilizar el equipo fabricado por la compañía taiwanesa Abocom. Su principal basa reside en su reducido precio, entre 10€ y 20€, y de esta manera, los costes de despliegue de la red, serían muy acotados. Desgraciadamente, ya no se fabrica este modelo de punto de acceso, habiendo de escoger una alternativa como dispositivo a utilizar.

Por lo tanto, y debido a sus cualidades, sus características técnicas, y su diseño tanto para uso exterior como interior, se ha decidido utilizar la UBNT NanoStation M2 para llevar a cabo el despliegue inicial del proyecto. Su relación calidad/precio es más que llamativa, haciendo de este producto una elección sin duda interesante para proyectos de esta característica. Recordemos además, que trabaja en la banda de frecuencias de 2,4GHz, y lleva incorporada la tecnología MIMO. Se adjuntan las especificaciones técnicas de este modelo como anexo.

Uno de los puntos importantes, por el cual se tomó esta decisión, es que esta marca, permite que todos sus productos sean modificados según el criterio del usuario. Tanto a nivel de hardware, como a nivel de firmware. Por este motivo, un gran número de usuarios conforman su comunidad, y por lo tanto, representan una posible ayuda, o

ventaja, en relación a los aspectos más técnicos. Por otro lado, la implementación de este piloto ha sido llevada a cabo en el departamento de investigación NETS de la Universidad Pompeu Fabra. Es por ello que se escogió este modelo con motivo de su posible reutilización en otros pilotos, proyectos u investigaciones que se lleven a cabo.

En un primer momento, servirá para llevar a cabo las pruebas necesarias para comprobar la robustez y funcionalidad total del sistema. No obstante, en un futuro despliegue de este proyecto a gran escala, otros modelos de puntos de acceso se tendrán en cuenta. Esta decisión estará basada sobre todo en un aspecto financiero, para abaratar costes respecto a las necesidades puntuales de cada implementación.

CAPÍTULO 4: DESPLIEGUE DE LA RED

En este apartado describiremos el trabajo llevado a cabo hasta el momento, como implementación de este sistema.

Esta implementación se lleva a cabo en el laboratorio de redes del departamento NETS (Network Technologies and Strategies) de la Universidad Pompeu Fabra de Barcelona. El equipo utilizado se detalla a continuación:

- Lubuntu 12.04
- Pentium 4 @3.00Ghz
- AsusTek Computer Inc. P4S800D-X
- 512+256 MB SDRAM DDR2
- Disco Duro Seagate ATA 80 GB
- NVIDIA GeForce4 MX 4000 512 MB
- Ubiquiti NanoStation M2

Figura 49: Equipo Laboratorio

4.1 Etapas

4.1.1 Primera Etapa de Implementación

La implementación se llevará a cabo en diversas etapas, en las que se añadirán progresivamente nuevas características. Esto es posible, debido a la granularidad y robustez de OpenWISP.

Podemos definir entonces las siguientes iteraciones en las que la implementación fue llevada a cabo:

1. En la primera etapa, se implementarán los componentes básicos y necesarios del sistema, es decir, OpenWISP Firmware y OpenWISP Manager.

   De esta manera, conseguiremos tener un dispositivo configurado bajo nuestras necesidades, y un sistema de gestión de configuraciones. Además, podremos

modificar la configuración del dispositivo, o grupo de dispositivos, de manera remota.
Esto es posible gracias a que cada vez que un nuevo dispositivo es conectado a Internet, OpenWISP firmware busca automáticamente actualizaciones en el servidor de configuraciones, OpenWISP manager. Todas las comunicaciones entre ambos son llevadas a cabo mediante una red virtual privada, o VPN. Si existiese alguna actualización, se descargaría y configuraría automáticamente.
El despliegue final, quedaría definido de la manera que podemos observar en la siguiente figura 50:

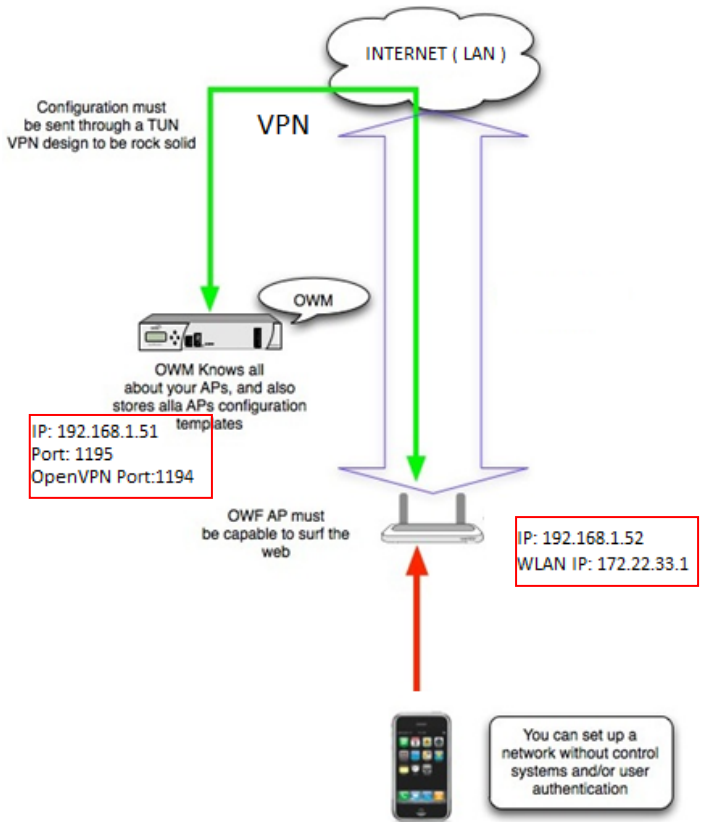


Figura 50: Despliegue primera etapa

No obstante, ésta primera iteración de despliegue es muy básica y no tiene en cuenta ningún tipo de identificación de usuarios, ni ninguna opción extra.
Cómo además se trata de un despliegue de pruebas, utilizaremos direcciones IP locales, por lo que sólo podrá haber conexión si se encuentran los dispositivos en la misma red interna. El servidor, tiene la IP 192.168.1.51, y en los puertos 1195 se encuentra corriendo OpenWISP Manager, y en el 1194 el servidor OpenVPN.

Antes de ponernos manos a la obra con el firmware, es necesario montar el servidor VPN. Para ello utilizamos la herramienta libre “OpenVPN”[57]. Podemos observar en la figura 51, el fichero de configuración utilizado en el servidor OpenVPN.

server.conf ×

```
dev tun
proto tcp
port 1194
ca ca.crt
cert server.crt
key server.key
dh dh1024.pem
tls-auth ta.key 0
duplicate-cn
user nobody
group nogroup
server 10.8.0.0 255.255.255.0
ifconfig-pool-persist /etc/openvpn/clients.txt
status /etc/openvpn/status.txt
persist-key
persist-tun
#push "redirect-gateway def1"
#push "route 192.168.0.0 255.255.255.0"
keepalive 10 120
verb 6
comp-lzo
max-clients 10
```

Figura 51: Fichero de configuración del servidor OpenVPN

Como servidor web, para dar soporte a OpenWISP Manager, se utiliza Phusion Passenger[58], que a su vez utiliza librerías de Apache[59], al que se le han añadido las siguientes líneas a los módulos de configuración.
Para ello, se han añadido dos ficheros de configuración, o lo que es lo mismo dos módulos, y se han activado correctamente. Estos, sirven básicamente para enseñarle a Apache dónde se encuentran los archivos necesarios para poner en marcha el plug-in Passenger, para trabajar con Ruby on Rails. A continuación, podemos observar en la figura 52, los ficheros añadidos a la configuración:

<passenger.conf>

File Edit Search Options Help

```
PassengerRoot /var/lib/gems/1.8/gems/passenger-3.0.18
PassengerRuby /usr/bin/ruby
```

<passenger.load>

File Edit Search Options Help

```
LoadModule passenger_module /var/lib/gems/1.8/gems/passenger-3.0.18/ext/apache2/mod_passenger.so
```

Figura 52: Ficheros de configuración de los módulos de Apache.

Además, se ha configurado un fichero indicando a Apache el sitio web de OpenWISP Manager, como se observa en la figura 53. De esta manera, se pueden tener varios sitios web en un mismo servidor.

```
<VirtualHost _default_:443>
    SSLEngine On
    SSLCertificateFile /etc/ssl/certs/ssl-cert-snakeoil.pem
    SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key

    # Possible values include: debug, info, notice, warn, error, crit, alert, emerg.
    LogLevel warn
    CustomLog /var/log/apache2/access-owm.log combined
    ErrorLog /var/log/apache2/error-owm.log
    ServerSignature On

    DocumentRoot /var/www/
    PassengerDefaultUser www-data

    <Files "favicon.ico">
        Options FollowSymLinks MultiViews
        Order Allow,Deny
        Allow from All
    </Files>
    <Directory /var/www>
        Options FollowSymLinks MultiViews
        AllowOverride Limit
        Order Deny,Allow
        Deny from All
        Allow from 127.0.0.1
    </Directory>

## This is needed cause the baseuri is hardcoded on openwisp
    Alias /owm "/home/user/OpenWISP/OpenWISP-Manager/public/"
    <Directory /home/user/OpenWISP/OpenWISP-Manager/public/>
        Options ExecCGI FollowSymLinks
        AllowOverride all
        Order allow,deny
        Allow from all
        RailsEnv production
        RailsBaseURI "/owm"
    </Directory>
    RewriteEngine on
    RewriteRule ^/get_config(.+)/$ /owm/get_config$1 [L]

    <Location "/get_config">
        Order Deny,Allow
        Deny from all
        Allow from 10.8.0.0/16
    </Location>

    <Location "/owm/get_config">
        Order Deny,Allow
        Deny from all
        Allow from 10.8.0.0/16
    </Location>
</VirtualHost>
```

Le indicamos que al buscar "/owm" en nuestro servidor, se dirija a la ruta deseada para cargar los archivos correspondientes.

De esta manera, hacemos accesible a este sitio web, únicamente desde la VPN que hemos configurado.

Figura 53: Fichero de configuración del sitio web de OpenWISP Manager para Apache

Esta modificación se lleva a cabo, para especificarle al servidor que las imágenes de configuración sólo se puedan descargar desde la red virtual privada. Una vez acabada la configuración del servidor, nos disponemos a realizar el despliegue del mismo, como observamos en la figura 54.

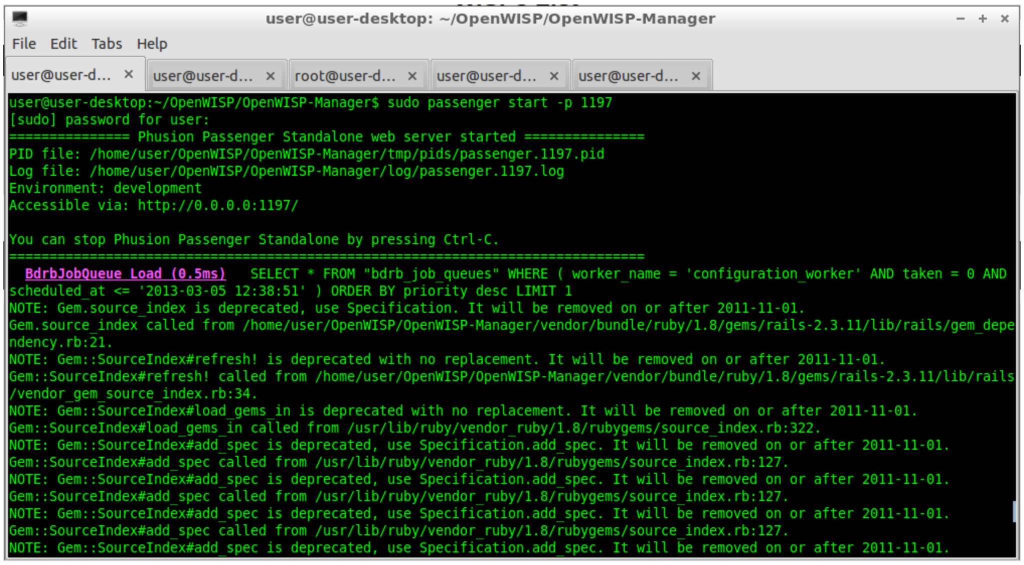


Figura 54: Puesta en marcha del servidor OpenWISP Manager

Podemos observar en la siguiente figura 55, como se encuentra funcionando OpenWISP Manager, en el servidor. Nótese que se accede a él mediante la dirección IP de la red virtual privada, y no mediante la red local.

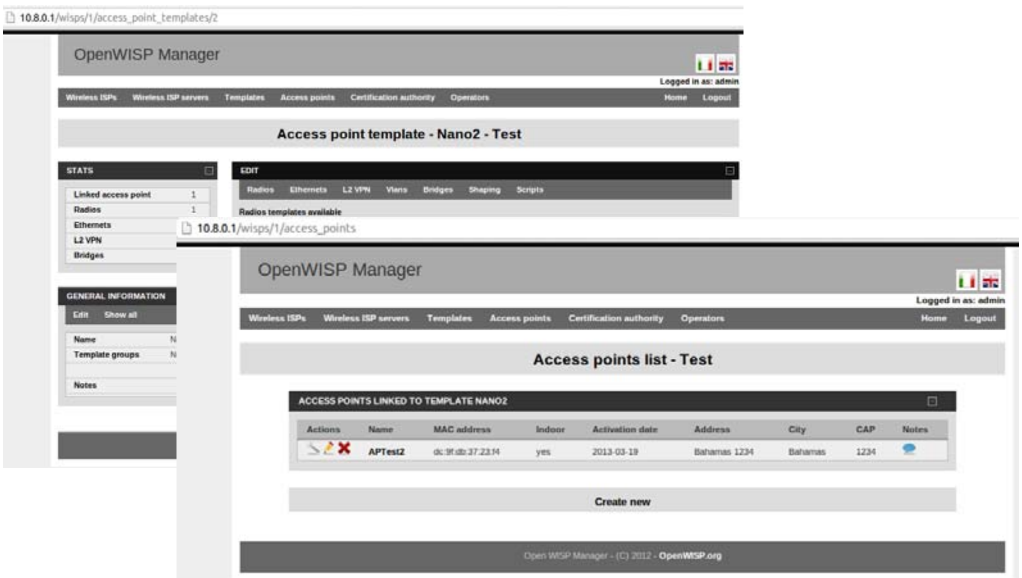


Figura 55: Comprobación funcionamiento OpenWISP Manager

Para finalizar la parte del servidor propiamente dicho, se define un script de inicio, también llamado demonio o "daemon", para que cada vez que se inicie el servidor, se lance automáticamente una instancia de OpenWISP Manager.

Instalación firmware en el dispositivo

El paso siguiente será llevar a cabo la grabación del firmware de OpenWISP, correctamente configurado a nuestras necesidades. Para ello, será necesario obtener el código fuente, tanto de OpenWISP como de OpenWRT, y luego compilarlo.

El primer paso llevado a cabo fue descargar el código fuente de OpenWISP firmware, y OpenWRT, de sus respectivas páginas. Luego, la compilación de este código, para obtener la imagen final, lista para grabar en la memoria del dispositivo.

Para esto, hemos de acceder al bloque de memoria escribible del dispositivo. Por lo tanto, nos disponemos a apagar el dispositivo, desconectando el cable Ethernet principal. Una vez se encuentra apagado, presionamos el botón de reseteo mientras volvemos a conectar el cable de corriente. Transcurridos unos diez segundos desde la puesta en marcha del dispositivo, éste se encuentra preparado para instalarle un nuevo firmware. Figura 56

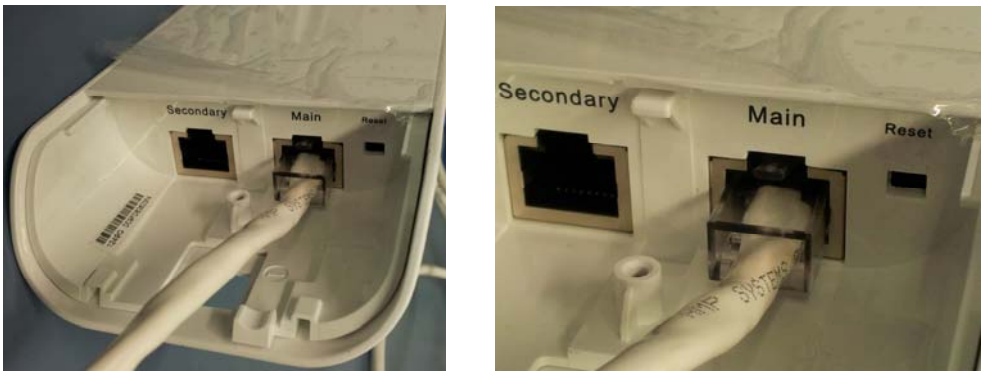


Figura 56: NanoStation M2

Por defecto, cuando accedemos al modo de escritura de la memoria del dispositivo, éste es accesible desde la dirección IP privada 192.168.1.20.

Como observamos en la figura 57, las opciones de configuración del firmware son muy extensas, y permiten que se adapte a las necesidades puntuales de cada implementación.

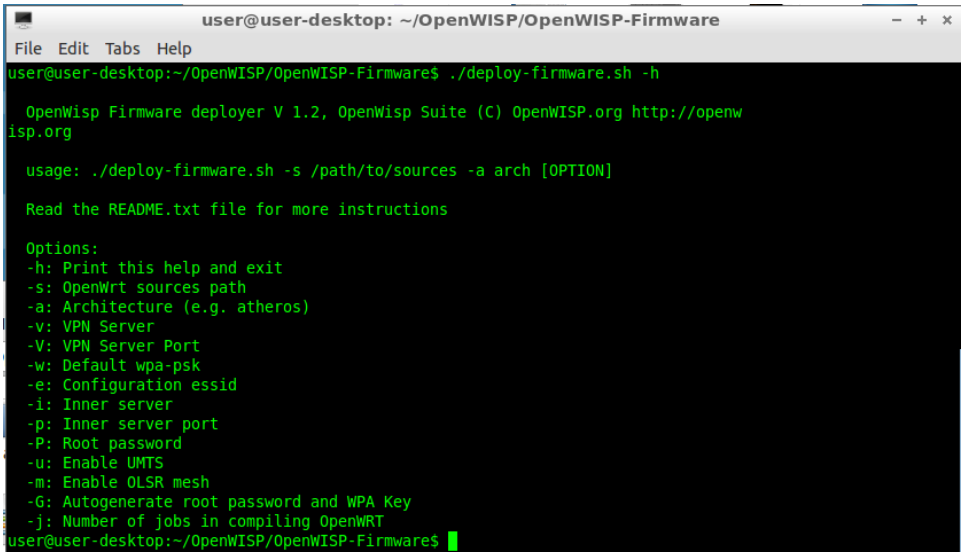


Figura 57: Opciones de configuración de OpenWISP

En nuestro caso, diversas de estas opciones no nos interesan actualmente, ya que el primer despliegue será un prototipo de pruebas. Por lo tanto, el comando utilizado quedaría definido de la siguiente manera:

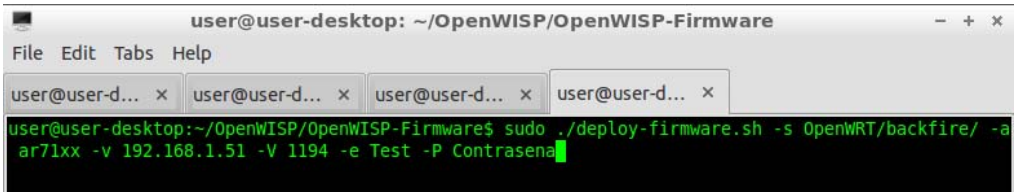


Figura 58: Comando finalmente utilizado para compilar el firmware

Como hechos a destacar, observamos que el chipset que lleva incorporado nuestro punto de acceso es de la compañía Atheros, perteneciente al modelo "ar71xx"[60].

Además, se declara el servidor VPN, es decir, el servidor desplegado en el laboratorio, que se encuentra en la dirección IP privada 192.168.1.51, y escucha en el puerto 1194. En este caso, definimos en una IP privada al servidor VPN, debido a que se trata de un primer prototipo. En el caso de una implementación final, el servidor VPN debería de ser accesible desde una dirección IP pública, es decir, ha de ser accesible desde cualquier punto de Internet, sin necesidad de estar físicamente en la misma red.

Para acabar de explicar las opciones escogidas sobre la compilación del firmware, sólo queda destacar dos puntos. El primero está relacionado con la contraseña que se le será otorgada al dispositivo, para acceder a todas las opciones de configuración del mismo como superusuario[61], también llamado “root”. La segunda, pertenece al nombre que se le da por defecto al SSID de la red inalámbrica que emitirá el dispositivo. Este nombre, no obstante, como todo el resto de opciones, son modificables desde OpenWISP Manager.

Una vez ya obtenemos la imagen del firmware de OpenWISP para nuestro modelo de punto de acceso, obtendremos un resumen similar al de la figura 59, y pasamos a la grabación en el mismo.

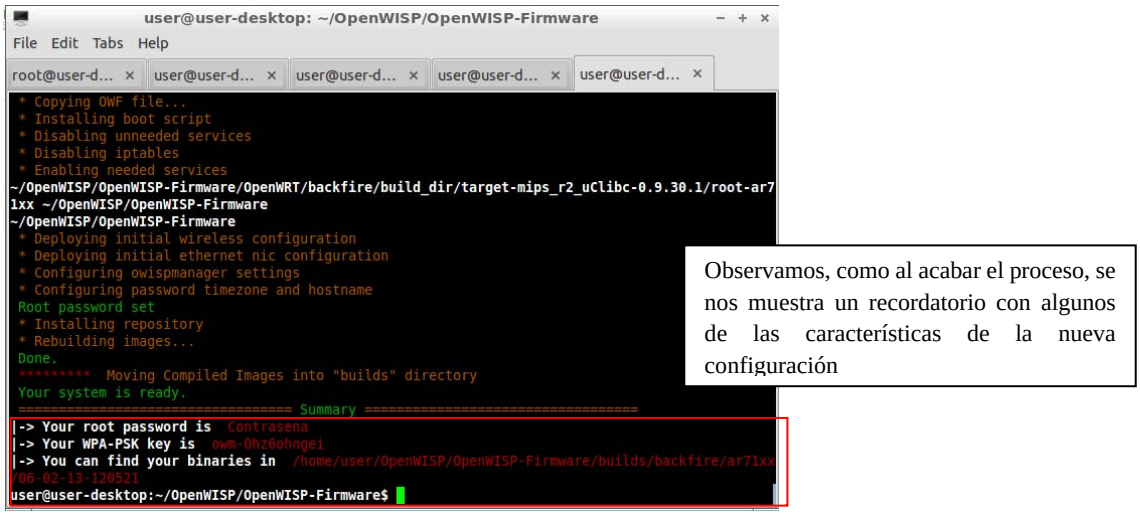


Figura 59: Finalización del proceso de compilación del firmware

Cuando la compilación acaba, se inserta la nueva imagen del firmware en el dispositivo. Para ello, utilizamos la herramienta TFTP[62]. Esta, nos permite transferir archivos al dispositivo a través de una conexión Ethernet.

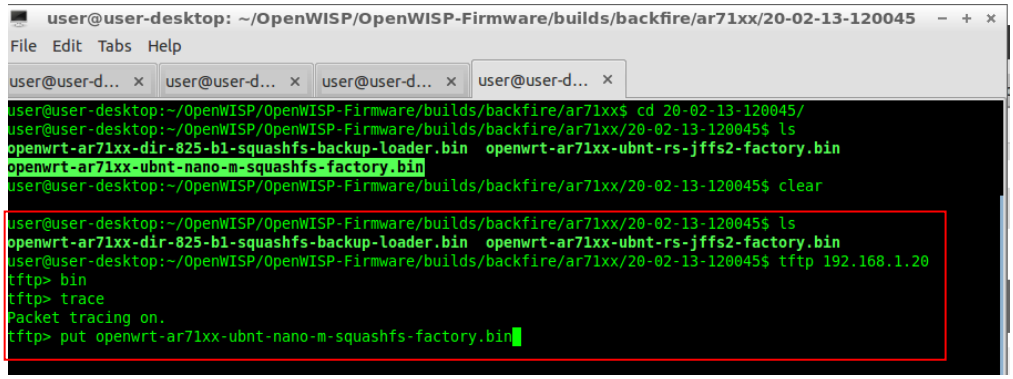


Figura 60: Proceso de grabación de la imagen mediante TFTP

Comprobación del funcionamiento del dispositivo

En este punto, cuando la transferencia del nuevo firmware ha acabado, somos ya capaces de conectarnos al dispositivo, mediante la herramienta “Telnet”[63]. En este caso, tal como le habíamos asignado anteriormente, accedemos a la dirección IP local, 192.168.1.52, como podemos observar en la siguiente figura 61.

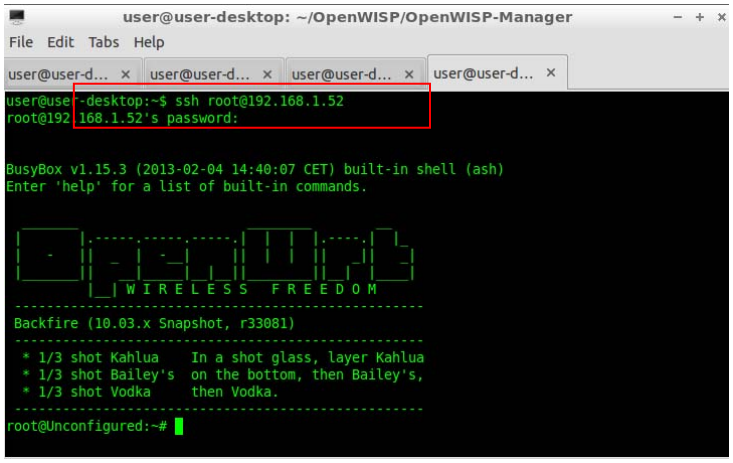


Figura 61: Conexión telnet a dispositivo

El siguiente punto, es el de comprobar que la conectividad entre dispositivo y servidor existe mediante la red virtual. Para ello, y como observamos en la figura 62, en la configuración de red del servidor, buscamos la dirección IP virtual que este ha adquirido. Una vez conocemos su dirección, llevamos a cabo un simple test de conectividad utilizando la herramienta “Ping”[64]. Observamos que desde el dispositivo, se lleva a cabo una transacción de paquetes hacia la dirección virtual del servidor. Como puede verse, esta transacción se efectúa correctamente.

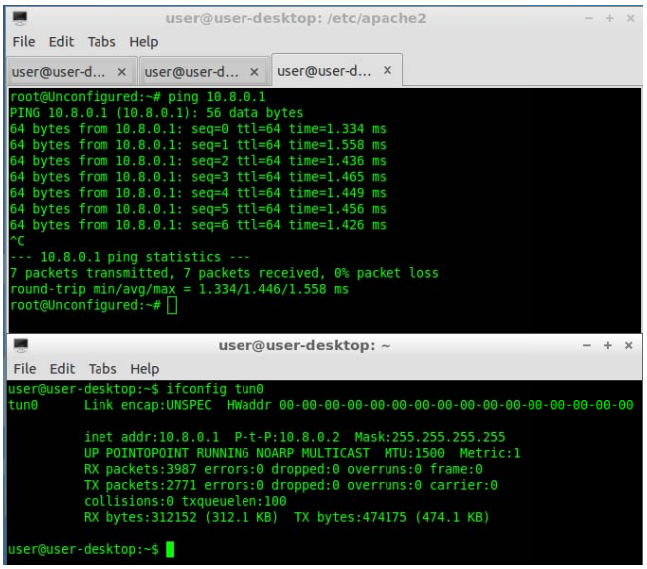


Figura 62: Comprobación conectividad VPN entre dispositivo y servidor

Podemos acceder también a la configuración del dispositivo, mediante su interfaz de usuario. Para ello, hemos de conectar nuestro ordenador a la red WiFi abastecida por el punto de acceso. Una vez conectado, por defecto la dirección del punto de acceso, mediante el cual nos conectamos a internet, es 172.22.33.1. Dentro de la interfaz gráfica, podemos modificar la configuración de red local del dispositivo, tal como vemos en la figura 63.

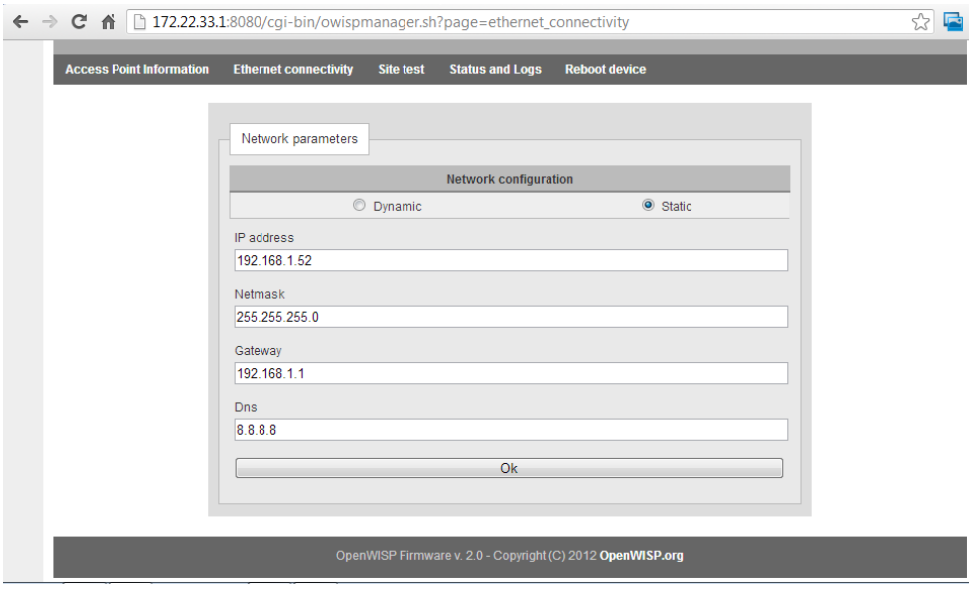


Figura 63: Interfaz de configuración de OpenWISP en el punto de acceso

Además de poder modificar los parámetros de configuración del dispositivo de red, la interfaz gráfica de OpenWISP, nos permite observar información propia

del dispositivo: figura 64, o monitorizar la configuración actual, la tabla de enrutamiento que guarda, o el log de debug: figura 65.

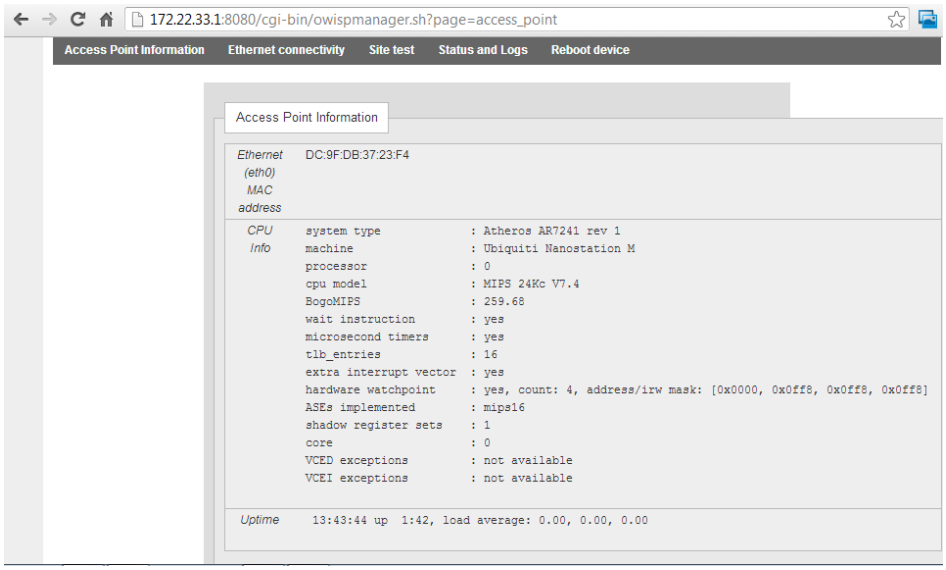


Figura 64: Información del dispositivo mediante la interfaz de OpenWISP

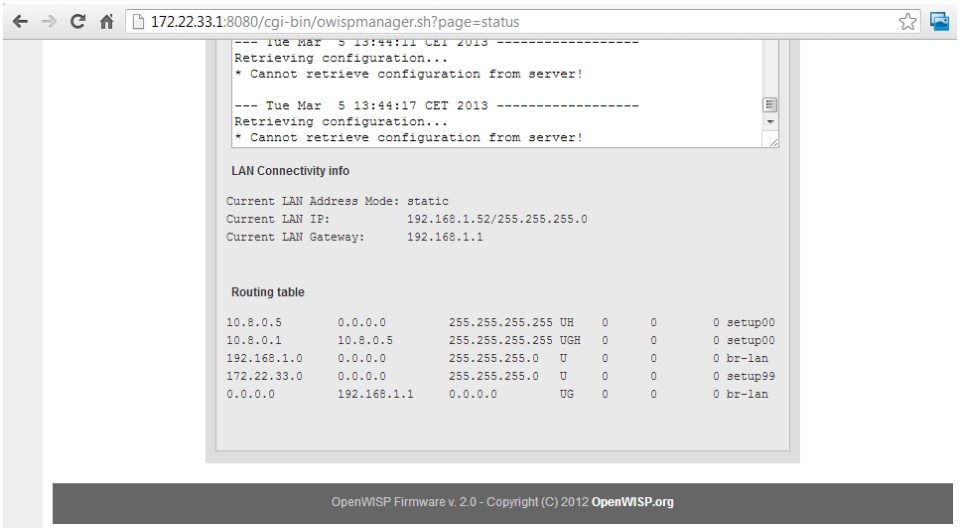


Figura 65: Información del estado del dispositivo mediante la interfaz de OpenWISP

Por último y no menos importante, mediante la interfaz gráfica, se nos permite llevar a cabo un test para comprobar de manera automática el correcto funcionamiento del sistema, Figura 66.

Entre otras cosas, nos da información de:

1. Si se encuentra presente la puerta de enlace o si es accesible por el dispositivo.
2. Si el servidor DNS[65] se encuentra en funcionamiento.

3. Si el servidor NTP[66] se encuentra en funcionamiento.
4. Si ha sido posible descargar el fichero de configuración desde OpenWISP Manager, de manera automática.
5. Lleva a cabo un test llamado “Traceroute” mediante el cual se permite seguir la pista a los paquetes que vienen desde un host de la red. Además, otorga estadísticas sobre el tiempo de latencia de la red, entre otra información. Este test se lleva a cabo utilizando en primer lugar, paquetes de poco tamaño, y luego con paquetes de tamaño más considerable.

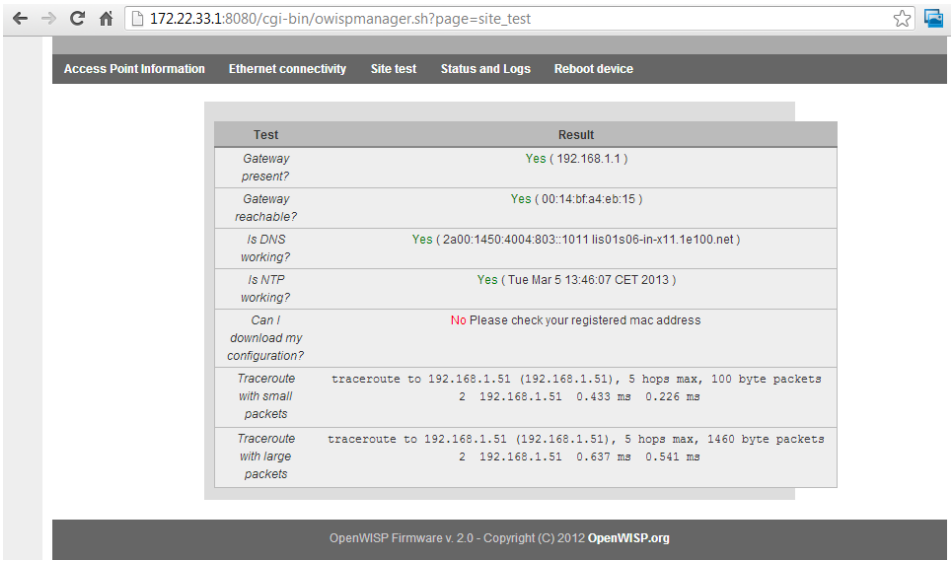


Figura 66: Test de funcionamiento llevado a cabo por el dispositivo de red mediante OpenWISP

Por último, y para dar por finalizada esta etapa de la implementación, observamos en la figura 67, que el sistema funciona correctamente. Se muestra un pantallazo del log del punto de acceso, en dónde vemos que la puesta a punto del sistema, la creación de la red virtual privada, y la descarga automática de la nueva configuración estipulada, han sido llevadas a cabo correctamente.

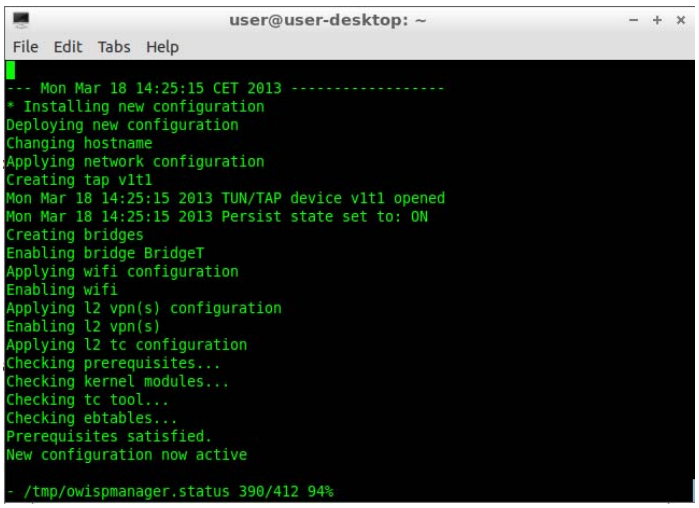


Figura 67: Pantallazo del log del dispositivo de acceso

Conclusiones

A lo largo de este proyecto he llevado a cabo una propuesta de solución para ofrecer, a todos los ciudadanos europeos, acceso a Internet inalámbrico WiFi. No sólo he elaborado una comparativa técnica de diferentes soluciones o implementaciones, sino también, he realizado un estudio sobre la legislación pertinente a este proyecto en España, y en el ámbito europeo.

- Propusimos una solución abierta y gratuita, para que todos los ciudadanos europeos puedan gozar de este servicio.
- Hemos planteado un método para que el sistema no tenga limitaciones territoriales. Llegando al resultado que cualquier ciudadano europeo en cuyo país se haya implementado este servicio, podrá acceder a la red en cualquier otra parte de Europa que también lo disponga.
- Mediante el estudio a pie de calle sobre la utilización y ocupación de los canales del espectro radioeléctrico libres para la utilización del estándar 802.11 concluimos que la banda de 2,4GHz se encuentra saturada, justo lo contrario que su homónima a 5GHz en la ciudad de Barcelona.
- En el esquema más técnico, comparamos diversas alternativas tanto públicas como privadas, decantándonos al final por utilizar OpenWISP como la solución más relevante y que mejor se adapta al objetivo y filosofía de este proyecto.
- En este trabajo demostramos cómo se ejecuta la implementación de éste sistema. Si bien, fue llevada a cabo en un entorno controlado y cerrado, su posible apertura a los usuarios finales es más que posible. Este despliegue fue realizado en varias etapas gracias a la modularidad de OpenWISP. Cada una de estas fases es independiente de la anterior, y añade nuevas funcionalidades al sistema.
- Una de las conclusiones más relevantes de este proyecto, más allá de querer brindar una solución para ofrecer conexión a Internet gratuita, es que éste aboga por reclamar a las autoridades de regulación de telecomunicaciones, unas leyes unificadas para el territorio europeo[39], en especial, para aquellos países que componen la Unión Europea.

[39] No olvidemos que las leyes están al servicio de la ciudadanía, y por lo tanto, dentro del contexto europeo de unidad, resulta un sin sentido que las regulaciones sobre telecomunicaciones no estén unificadas. Básicamente, esta falta de unanimidad legislativa, dificulta las tareas de los operadores de telecomunicaciones y que puedan surgir nuevos productos en materia de telecomunicaciones usando una pequeña parte del espectro de manera gratuita y unificada en el territorio.

Trabajo Futuro

Los resultados del despliegue han sido satisfactorios, no obstante aún queda trabajo por realizar para acabar de desplegar este sistema.

Recordemos que en la primera etapa, se implementó el módulo de administración de dispositivos, OpenWISP Manager, y se instaló el nuevo firmware al punto de acceso. Satisfactoriamente, cuando se modifica la configuración pertinente al dispositivo desde el servidor, en cuestión de minutos (ya que el dispositivo busca si existen nuevas configuraciones cada cinco minutos) éste se descarga la última versión disponible de su configuración y la instala, de manera automática. Los resultados y capturas de pantalla, pueden observarse al final de dicho capítulo de esta memoria.

A modo de resumen, podemos concluir entonces, que la primera etapa del despliegue de la solución ha sido totalmente satisfactoria.

Los pasos más inmediatos, son los de implementar los módulos del sistema relativos a los usuarios. Sin estos módulos, el despliegue actual no tiene sentido de cara a obtener un producto plenamente funcional y listo para su distribución.

Una vez se dé por finalizado el despliegue del sistema en Barcelona, la siguiente etapa es la de interconectar los proxy RADIUS con el servidor RADIUS “IX-WiFi” que tiene sede en Roma, Italia. De esta manera, se podrá gozar de la total ubicuidad de éste sistema. No obstante, no se da por finalizado el proyecto llegados a este punto. Queda mucho trabajo por delante, sobre todo en labores de expansión y difusión.

Un punto positivo de este proyecto, es como se ha comentado anteriormente, su flexibilidad e independencia dentro de los integrantes del mismo. Es por ello, que de la misma manera que se busca implementar la iniciativa en Europa, la posibilidad queda más que abierta hacia otros países.

Fuentes Bibliográficas

[1] **Wireless Fidelity *"WiFi"***
IEEE Standard for Information Technology. "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications". IEEE. Revisión 2007. Consultado 12/04/2012
http://standards.ieee.org/getieee802/download/802.11-2012.pdf

[2] **Commons for Europe**
Commons for Europe. 2012. Commons for Europe. Consultado 12/04/2012
http://commonsforeurope.net/

[3] **Bottom Up Broadband**
Jaume Barceló, Boris Bellalta, Roger Baig, Ramon Roca, Albert Domingo, Luis Sanabria, Cristina Cano and Miquel Oliver; (2012) "Bottom-up Broadband Initiatives in the Commons for Europe Project".

[4] **Open WISP**
Open WISP Project. 2012. Open WISP. Consultado 12/04/2012
http://openwisp.caspur.it/

[5] **Provincia WiFi**
Provincia WiFi. 2011. Provincia di Roma. Consultado 12/04/2012
http://www.provincia.roma.it/percorsitematici/innovazione-tecnologica/progetti/4035

[6] **Comisión del Mercado de las Telecomunicaciones de España *"CMT"***
Comisión del Mercado de las Telecomunicaciones de España.
http://www.cmt.es/vigentes_norm

[7] **Broadband and Wi-Fi Households Global Forecast 2012**
"Broadband and Wi-Fi Households Global Forecast 2012" Strategy Analytics Connected Home Devices. 2012. Kantideep Thota.
http://www.strategyanalytics.com/default.aspx?mod=reportabstractviewer&a0=7215

[8] **SSID**
IEEE Standard for Information Technology. "IEEE 802. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications". IEEE. Revisión 2007. Consultado 12/04/2012
http://standards.ieee.org/getieee802/download/802.11-2012.pdf

[9] **BSSID**
IEEE Standard for Information Technology. "IEEE 802. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications". IEEE. Revisión 2007. Consultado 12/04/2012
http://standards.ieee.org/getieee802/download/802.11-2012.pdf

[10] **SNR**
Signal-to-Noise Ratio. 2013. Wikipedia Foundation. Consultado 02/05/2013
http://en.wikipedia.org/wiki/Signal-to-noise_ratio

[11] **Ad-hoc**
IEEE Standard for Information Technology. “Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications”. IEEE. Revisión 2007. Consultado 12/04/2012
http://standards.ieee.org/getieee802/download/802.11-2012.pdf

[12] **WBA**
Wireless Broadband Alliance. 2013. Wireless Broadband Alliance. Consultado 20/12/2012
http://www.wballiance.com/

[13] **Barcelona WiFi**
Barcelona WiFi. 2009. Ajuntament de Barcelona. Consultado 12/04/2012
http://www.bcn.cat/barcelonawifi/es/

[14] **British Telecom**
British Telecom. 2013. British Telecom. Consultado: 12/06/2012
http://www.bt.com/

[15] **Malta MCAfreeWiFi**
Malta Communicactions Authority. 2013. Malta Communicactions Authority. Consultado: 12/03/2013
http://www.mca.org.mt/wifi-hotspots

[16] **PanOULU**
Public Access Network OULU. 2013. Public Access Network OULU. Consultado: 25/12/2012
http://www.panoulu.net/

[17] **Virtual Private Network “*VPN*”**
Virtual Private Network Technologies: Definition and Requirements. 2008. Virtual Private Network Consortium. Consultado 12/04/2012
http://www.vpnc.org/vpn-technologies.html

[18] **París WiFi**
París WiFi. 2009. Ville de Paris. Consultado 12/04/2012
http://www.paris.fr/wifi

[19] **P2P**
G. Camarillo, “Peer-to-Peer (P2P) Architecture: Definition, Taxonomies, Examples, and Applicability” IAB, RFC 5694, Nov. 2009. [Online]. Available:
http://tools.ietf.org/html/rfc5694

[20] **Guifi.Net**
Guifi.Net. 2013. Guifi.Net. Consultado 01/05/2013
http://guifi.net/

[21] **KUBI Wireless**
Kubi Wireless. 2013. Kubi Wireless. Consultado 23/11/2012

http://www.kubiwireless.com/

[22] **ZonaWiFiGratis**
Zona WiFi Gratis. 2012. Zona WiFi Gratis. Consultado 20/11/2012
http://www.zonawifigratis.es

[23] **GOWEX**
GOWEX. 2013. GOWEX. Consultado 20/12/2012
http://www.gowex.com/

[24] **FON**
Fon. 2013. Fon. Consultado 11/04/2013
http://www.fon.com/es

[25] **Firmware**
IEEE Standard for Boot (Initialization Configuration) Firmware: Bus Supplement for IEEE 896 (Futurebus+)
E-ISBN : 0-7381-2772-8
Print ISBN: 1-55937-580-9
INSPEC Accession Number: 5261314
Digital Object Identifier : 10.1109/IEEESTD.1996.80827
Persistent Link: http://ieeexplore.ieee.org/servlet/opac?punumber=3696
Year : 1996
Date of Current Version : 06 august 2002
Issue Date :1996

[26] **SwissCOM Eurospot**
Public Wireless LAN, SwissCOM Eurospot. 2013. SwissCOM. Consultado 20/12/2012
http://www.swisscom.ch/en/residential/internet/internet-on-the-move/pwlan.html

[27] **LinSpot**
LinSpot. 2013. LinSpot. Consultado 20/12/2012
http://www.linspot.com/

[28] **GNU GPL**
GNU General Public License. 2013. GNU Project. Consultado 11/04/2013
http://www.gnu.org/licenses/gpl.html

[29] **Ruby for Rails**
“Ruby techniques for Rails Developers”
David A. Black
Editorial Manning
ISBN: 1-932394-69-9
Printed in USA, 2006

[30] **Ruby on Rails**
Ruby on Rails. 2003. Ruby on Rails. Consultado 12/04/2012
http://rubyonrails.org/

[31] **“Modelo-Vista-Controlador”**
“MVC, Model-view-controller”
Jesse Russell, Ronald Cohn
Editorial Book on Demand
ISBN-10: 5513484684
ISBN-13: 978-5513484684

[32] **eSSID**
IEEE Standard for Information Technology. “IEEE 802. Part 11: Wireless LAN Medium Access Control (MAC) nd Physical Layer (PHY) Specifications”. IEEE. Revisión 2007. Consultado 12/04/2012
http://standards.ieee.org/getieee802/download/802.11-2012.pdf

[33] **RADIUS**
C. Rigney, S. Willens, Livingston, A. Rubens, Merit, W. Simpson, “Remote Authentication Dial In User Service (RADIUS)”, Daydreamer, June 2000. [Online]. Available: http://tools.ietf.org/html/rfc2865

[33A] **RADIUS**
Securing Public Access to Private Resources
Jonathan Hassell
Editorial O’Reilly Media
ISBN: 978-1-4493-8686-3
E-ISBN 1-4493-8686-5

[34] **MySQL**
MySQL. 2013. MySQL. Consultado 11/04/2013
http://www.mysql.com /

[35] **PostgreSQL**
PostgreSQL. 2013. PostgreSQL. Consultado 11/04/2013
http://www.postgresql.org/

[36] **PayPal**
PayPal. 2013. PayPal Inc. Consultado 11/04/2013
https://www.paypal.com/

[37] **OpenWRT**
OpenWRT. 2013. OpenWRT. Consultado 10/10/2012
https://openwrt.org/

[38] **HTML5**
HyperText Markup Language 5. 2013. The World Wide Web Consortium. Consultado 02/05/2013
http://www.w3.org/TR/html5/

[39] **REST**
“REST in Practice: Hypermedia and Systems Architecture”
Jim Webber, Savas Parastatidis, Ian Robinson

Editorial O'Reilly Media
ISBN-10: 0596805829
ISBN-13: 978-0596805821

[40] **Firewall**
N. Freed, "Behavior of and Requirements for Internet Firewalls", SUN, RFC 2979, Oct. 2000. [Online]. Available: http://www.ietf.org/rfc/rfc2979.txt

[41] **NAT**
K. Egevang, Cray Communications, P.Francis, "The IP Network Address Translator (NAT)", NTT, RFC 1631, May 1994. [Online]. Available: http://www.ietf.org/rfc/rfc1631.txt

[42] **CINECA**
CINECA Consorzio Interuniversitario. 2013. CINECA Consorzio Interuniversitario. Consultado 11/04/2013
http://www.cineca.it/

[43] **Proxy**
C. Rigney, S. Willens, Livingston, A. Rubens, Merit, W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", Daydreamer, June 2000. [Online]. Available: http://tools.ietf.org/html/rfc2865#section-2.3

[44] **QoS**
Seitz, N., "ITU-T QoS standards for IP-based networks," *Communications Magazine, IEEE*, vol.41, no.6, pp.82,89, June 2003
ISSN: 0163-6804
INSPEC Accession Number: 7655562
Digital Object Identifier: 10.1109/MCOM.2003.1204752
Date of Current Version: 20 June 2003
Issue Date: June 2003
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1204752&isnumber=27123

[45] **IEEE 802.11n**
IEEE Standard for Information Technology. "IEEE 802. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications". IEEE. Revisión 2007. Consultado 12/04/2012
http://standards.ieee.org/getieee802/download/802.11-2012.pdf

[46] **IEEE 802.11b**
IEEE Standard for Information Technology. "IEEE 802. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications". IEEE. Revisión 2007. Consultado 12/04/2012
http://standards.ieee.org/getieee802/download/802.11-2012.pdf

[47] **IEEE 802.11g**
IEEE Standard for Information Technology. "IEEE 802. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications". IEEE. Revisión 2007. Consultado 12/04/2012

http://standards.ieee.org/getieee802/download/802.11-2012.pdf

[48] **IEEE 802.11a**
IEEE Standard for Information Technology. “IEEE 802. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications”. IEEE. Revisión 2007. Consultado 12/04/2012
http://standards.ieee.org/getieee802/download/802.11-2012.pdf

[49] **IEEE 802.3**
IEEE Standard for Information Technology. “IEEE 802. Part 3: Carrier sense multiple access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications ”. IEEE. Revisión 2008. Consultado 01/05/2013
http://standards.ieee.org/getieee802/download/802.3-2008_section1.pdf

[50] **IEEE 802.3u**
IEEE Standard for Information Technology. “IEEE 802. Part 3: Carrier sense multiple access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications ”. IEEE. Revisión 2008. Consultado 01/05/2013
http://standards.ieee.org/getieee802/download/802.3-2008_section1.pdf

[51] **LAN**
IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture. Revisión 2001. IEEE. Consultado 12/04/2012
http://standards.ieee.org/getieee802/download/802-2001.pdf

[52] **WAN**
IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture. Revisión 2001. IEEE. Consultado 12/04/2012
http://standards.ieee.org/getieee802/download/802-2001.pdf

[53] **USB**
Universal Serial Bus, USB. 2013. Universal Serial Bus Implementers Forum, Inc. Consultado 02/05/2013
http://www.usb.org/developers/docs/usb_20_040413.zip

[54] **POE**
IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements," *IEEE Std 802.3af-2003 (Amendment to IEEE Std 802.3-2002, including IEEE Std 802.3ae-2002)* , vol., no., pp.0_1,121, 2003
E-ISBN: 0-7381-3697-4
Print ISBN: 0-7381-3697-2
Digital Object Identifier: 10.1109/IEEESTD.2003.94284
Persistent Link: http://ieeexplore.ieee.org/servlet/opac?punumber=8612
Date of Current Version: 22 July 2003
Issue Date: 2003
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1213877&isnumber=27294

[55] **MIMO**
Sanayei, S.; Nosratinia, A., "Antenna selection in MIMO systems," *Communications Magazine, IEEE*, vol.42, no.10, pp.68,73, Oct. 2004
ISSN: 0163-6804
INSPEC Accession Number: 8155625
Digital Object Identifier: 10.1109/MCOM.2004.1341263
Date of Current Version: 08 octubre 2004
Issue Date: Oct. 2004
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1341263&isnumber=29548

[56] **AirOS**
AirOS V. 2013. Ubiquiti Networks. Consultado 15/04/2013
http://www.ubnt.com/airos

[57] **OpenVPN**
OpenVPN. 2013. OpenVPN. Consultado 01/05/2013
http://openvpn.net/

[58] **Phusion Passenger**
Phusion Passenger. 2013. Phusion. Consultado 12/04/2013
https://www.phusionpassenger.com/

[59] **Apache**
Apache. 2013.The Apache Software Foundation. Consultado 12/04/2013
http://www.apache.org/

[60] **Atheros Ar71xx**
Qualcomm Atheros. 2013. Qualcomm. Consultado 01/05/2013
http://www.qca.qualcomm.com/media/product/product_68_file1.pdf

[61] **Superusuario ("Root")**
"root" Definition. 2007. The Linux Information Project. Consultado 02/05/2013
http://www.linfo.org/root.html

[62] **TFTP**
K. Sollins, "The TFTP Protocol (Revision 2)" MIT, RFC 1350, July 1992. [Online]. Available: http://tools.ietf.org/html/rfc1350

[63] **Telnet**
J. Postel, J. Reynolds, "TELNET Protocol Specification" ISI, RFC 854, May 1983. [Online]. Available: http://tools.ietf.org/html/rfc854

[64] **Ping**
J. Quittek, NEC, K. White, "Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations", IBM Corp., RFC 4560, June 2006. [Online]. Available: http://tools.ietf.org/html/rfc4560#section-1.1

[65] **DNS**
P. Mockapetris, “Domain Names – Implementation and Specification”, ISI, RFC 1035, Nov. 1987. [Online]. Available: http://www.ietf.org/rfc/rfc1035.txt

[66] **NTP**
D.L. Mills, “Network Time Protocol (NTP)”, M/A-COM Linkabit, RFC 958, Sept. 1985. [Online]. Available: http://tools.ietf.org/html/rfc958

Anexos

Anexo I: Project Charter

Free Europe WiFi Pilot

Project Charter

1. OPPORTUNITY / IDEA

This opportunity arose from the actual tendency that cities along the whole world are working on. They are trying to provide free WiFi internet connection to all citizens. The real opportunity is the need to create a community network to communicate freely anywhere in the EU. Born as a tie, to strengthen the communication of citizens of different countries within a common block, as is Europe.
There is already an open system for getting free wireless internet distribution deployed in Italy, and the goal is to implement this system in Spain always keeping full interoperability. Also lay the foundation regarding documentation, to give rise to other countries to also do it.

2. DESCRIPTION / PURPOSE

A complete description of all the cases that are running at the moment in different European cities will be made in order to understand the main need that feeds this project.
Achieve the implementation of OpenWISP system in Spain and their overall diffusion alternatively, to the extent possible.
To achieve the correct and complete documentation on both cases, the first is currently in operation, Italian case, and about the case to be implemented, the Spanish one. Always keeping in mind writing technical information for future implementations.

3. GOAL

Implement and maintenance of a free wireless internet connection.
Create a prototype/demonstration module to offer new cities to support the project.
Document all the technical aspects of the system and its implementation.

4. OBJECTIVES / RESULTS

- Be able to understand, modify according to our case and deploy OpenWISP system.
- Create, complete and correct technical documentation about the project for future implementations.

5. SCOPE

The scope of the project is the public WiFi internet connection solutions offered by any European city.

6. STAKEHOLDERS AND SPONSORS OF THE PROJECT

- Project Team
- Universitat Pompeu Fabra
- CINECA
- Provincia di Roma
- Guifi.net
- DOTOpen
- Linx
- ESADE
- Fraunhofer FOKUS
- Forum Virium
- City of Amsterdam
- Waag Society
- NESTA
- Ajuntament de Barcelona

7. RISK

- Issues in disseminating this connectivity solution. Exists other solutions owned by public administration.
- Possible future problem with the FreeItalia WiFi project, in which this project is based, because of politic elections and no continuity future managers.

8. SCHEDULE

WBS	Nombre	Inicio	Fin	Trabajo
1	Warm-up session	Dec 5	Dec 5	1d
2	Kick-off meeting	Dec 6	Dec 6	1d
3	**Initial design phase**	Dec 7	Apr 2	123d
3.1	Legistlation approach	Dec 7	Dec 20	10d
3.2	Spanish legislation initial solution	Dec 7	Dec 20	10d
3.3	Network design	Dec 21	Jan 24	25d
3.4	Studing OpenWisp	Dec 21	Apr 2	73d
3.5	Documentation	Jan 25	Jan 31	5d
4	**Early implementation**	Jan 25	Mar 7	80d
4.1	Server setup	Jan 25	Feb 21	20d
4.2	Firmware modification	Jan 25	Feb 21	20d
4.3	Router configuration	Jan 25	Feb 21	20d
4.4	Lab deployment	Feb 22	Mar 1	6d
4.5	Testing	Feb 22	Mar 1	6d
4.6	Project Re-analysis	Mar 4	Mar 7	4d
4.7	Documentation	Mar 4	Mar 7	4d
5	**Final implementation**	Mar 8	Apr 22	64d
5.1	Network deployment	Mar 8	Apr 2	18d
5.2	Troubleshooting	Mar 8	Apr 2	18d
5.3	Project final analysis	Apr 3	Apr 22	14d
5.4	Documentation	Apr 3	Apr 22	14d
6	Full documentation	Dec 10	Apr 30	102d
7	**Project defense**	May 1	Jun 12	31d
7.1	Presentation preparation	May 1	Jun 11	30d
7.2	Final presentation	Jun 12	Jun 12	1d

Anexo II: Distribución temporal del proyecto

Free Europe Wi-Fi Project

Definición del proyecto.

- Oportunidad/Idea:

A medida que la sociedad avanza, surge la necesidad de albergar unos mayores y estrechos lazos de comunicación. Ya no sólo en determinados momentos, sino que estar continuamente conectado con otras personas, resulta imprescindible en la sociedad actual. Es por esto que el acceso a la información y comunicación se presenta cada vez más como una necesidad básica de la ciudadanía.

Existen diferentes implementaciones (ya sea debido a aspectos tecnológicos, como a motivos legales) en diversos ámbitos geográficos, por ejemplo municipios, ciudades o incluso países. Todas ellas buscan ofrecer una solución directa a las nuevas necesidades sociales.

Dada la tecnología actual y la gran necesidad de intercomunicación existente entre las personas, surge la idea de crear una red que proporcione acceso a Internet de manera inalámbrica, abierta y gratuita para todos los ciudadanos que lo deseen. Además, y no menos importante, otra característica es que esta conexión será totalmente ubicua, es decir, independiente del lugar geográfico en dónde el usuario se encuentre o provenga. De esta manera, se provee de una nueva solución, a la necesidad continua de estar conectado.

Esta idea no sólo representa el ideal de un acceso libre y gratuito a la información y la tecnología, sino que también se presenta como un vínculo más para estrechar las relaciones entre los diferentes países, y por lo tanto ciudadanos, de la comunidad europea.

- Descripción/Propósito:

El proyecto se basa en diseñar tanto una red inalámbrica *"WiFi"* [1] (de tipo B, G o N), que proporcione acceso a Internet a todos los ciudadanos de manera libre y gratuita, sino también su interconexión con la implementación en diferentes países que se sumen a la causa, con el objetivo de lograr la interoperabilidad entre ellas.

Está estrechamente relacionado, con un trabajo de implementación llevado a cabo como parte de un proyecto europeo denominado Commons for Europe [2]. Bajo el modelo Bottom-Up Broadband [3]. Un modelo que pretende establecer un nuevo punto de vista desde el cual la oferta de servicios de telecomunicaciones no parte desde las compañías, sino desde los propios ciudadanos.

La implementación del mismo se llevará a cabo a partir de OpenWISP[4]. Este es un software de libre distribución y modificación, que ofrece la capacidad de crear soluciones que den abasto a un completo servicio de acceso a Internet sin cables. Este software ha sido desarrollado y llevado a cabo dentro de un proyecto, Provincia WiFi[5], impulsado por el ayuntamiento de Roma, con el objetivo de dar soporte, abasto y acceso a Internet a todos sus ciudadanos. Este proyecto, se distribuye actualmente bajo licencia y filosofía de código abierto, de manera que cualquier interesado en él, puede modificar y/o mejorarlo con el objetivo de seguir creciendo.

El pasado mes de octubre, fue llevada a cabo una reunión con los responsables de Provincia WiFi en Bolonia, Italia. En ella se acordó y puso en común los términos para llevar a cabo el proyecto. Además, se aportó información técnica del mismo para facilitar la tarea de réplica que se llevará a cabo.

La finalidad u objetivo de este sistema, es ofrecer una solución completa y estable para compartir conexiones privadas a Internet, al resto de la ciudadanía. Es entonces cuando cualquier usuario que desee compartir su conexión (ya sea para ofrecerlo como un valor añadido a su negocio, o por simple altruismo), puede hacerlo sin dificultad ninguna.

La gran ventaja de este sistema frente a otros similares es la seguridad que se proporciona a sus usuarios. Tanto, aquellos que comparten su conexión, como los que se beneficiarán de ella, no se encuentran en ningún momento en riesgo de sufrir ataques de

seguridad y/o privacidad. Esto es posible, debido a que el sistema se basa en la creación de redes privadas virtuales [17], o VPN. Este tipo de redes crean virtualmente un enlace seguro entre dos puntos, que pueden no encontrarse en la misma red local.

- Problema/Antecedentes:

Tal y como se ha comentado anteriormente, este proyecto está basado en uno de similar características llevado a cabo por la provincia de Roma, Italia. Se denomina Provincia WiFi, empezado en 2008, con el objetivo de dar acceso y conexión libre a Internet a todos los ciudadanos. El servicio ofrece cobertura a todo el territorio de la provincia, aproximadamente unos 5352 kilómetros cuadrados, que incluyen tanto a la ciudad de Roma, como a otras 120 ciudades diferentes. En total busca ofrecer sus ventajas a 4,5 millones de habitantes de esta región. Actualmente más de doce administraciones públicas italianas están distribuyendo e implementando este sistema para ofrecer sus servicios a sus ciudadanos.

No obstante, existen en marcha otras alternativas a este sistema, que han sido analizadas, estudiadas y propuestas como posibles modelos a seguir. Estas soluciones se encuentran desplegadas en diferentes ciudades europeas como son Barcelona, Londres o París entre otras muchas. Más adelante se analizarán a fondo algunas de estas soluciones. A continuación se enseña una breve reseña de una selección de ellas:

- Barcelona[13]: es un servicio ofrecido por el ayuntamiento, llamado Barcelona WiFi. Permite conectarse a Internet a través de diversos puntos de acceso ubicados a lo largo de la ciudad, tanto en edificios municipales, como en puntos en la vía pública. Este servicio está sujeto a la aceptación del usuario final de las condiciones de uso del servicio, establecidas para cumplir con la normativa vigente por la Comisión del Mercado de Telecomunicaciones, "*CMT*"[6] y la ley de Telecomunicaciones de España[11] . Además las condiciones de velocidad de la conexión y el horario de uso, dependerá de la ubicación de los puntos de acceso a la red.

- París[18]: este servicio es ofrecido por el ayuntamiento de París, pero desplegado y mantenido por una operadora de telecomunicaciones, France Telecom, para ofrecer conexión gratuita a Internet en diversos puntos de la

ciudad. Los puntos de acceso se encuentran en zonas municipales como bibliotecas, parques o los ayuntamientos o edificios públicos.

Si bien todas estas alternativas no han sido escogidas como el modelo a continuar en este proyecto, serán analizadas y comentadas más adelante.

- Alcance

El alcance de este proyecto, pretende establecer un nexo común a todas las soluciones de conectividad pública de acceso a Internet sin cables, ofrecida por cualquier Estado dentro de la Unión Europea.

- Objetivo

El objetivo final del proyecto es:

- Analizar, comprender y documentar la elección de la mejor tecnología o producto que provea una solución abierta, global y sensata a nivel europeo, para lograr ofrecer acceso libre y gratuito a Internet a todos los ciudadanos de la misma, dentro del territorio comunitario.

- Comprender e interpretar de manera correcta los términos y aspectos legales que requiere un despliegue tecnológico de las Tecnologías de la Información y Comunicación "*TIC*" de semejantes características.

Esquema de trabajo. Tareas a efectuar.

Planificación del Proyecto

El proyecto ha sido planificado para ser realizado y llevado a cabo en una duración aproximada de 9 meses, desde la realización de la reunión de comienzo. Más adelante se enseñará y definirá a fondo las tareas a realizar y su aproximada duración temporal. Se ha de tener en cuenta además, los días festivos y no laborables dado el calendario oficial de la universidad.

No obstante y a modo introductorio, el proyecto se basa primordialmente en tres grandes etapas: la fase inicial del diseño, la primera implementación, también denominada versión Beta[40] en software, y por último la implementación y despliegue final de la solución.

Tan importante como la realización del proyecto, es la documentación del mismo. Este hecho resulta imprescindible debido a diversos motivos, algunos de los cuales son los siguientes:

- Ayuda a revisar y corregir todo el trabajo realizado, plantear nuevas preguntas y desafíos en el proyecto.
- Otorga la posibilidad de que la experiencia adquirida durante la realización del proyecto, pueda ser compartida y socializada, dando la ventaja a otras personas interesadas, de adquirir información, ya sean problemas experimentados o logros realizados, para su futuro uso o re-implantación. Este último punto es uno de los grandes objetivos en el marco en que se encuentra envuelto el proyecto.

Al finalizar el proyecto, éste habrá de ser presentado y juzgado en un tribunal compuesto por el tutor del alumno que lo realizará, y dos profesores de corte académico similar al del proyecto. Se juzgará el trabajo realizado durante la implementación del mismo, y la calidad tanto de la información como su fiabilidad. Además, al acabarlo, el alumno ha de haber adquirido ciertas competencias tanto específicas como transversales que han de ser demostradas durante la presentación del proyecto.

[40] Entendemos por versión “Beta” a la segunda fase de desarrollo en la que eliminan activamente errores que puedan existir, dando lugar a una versión estable del software.

Explicación de las tareas a realizar

- Sesión informativa pre-inicio

Esta reunión es plenamente de carácter informativo, y busca dar una visión más completa sobre el proyecto a realizar y su viabilidad tanto a nivel del estudiante que lo llevará a cabo, como de la dirección del mismo. Básicamente se presenta la idea básica detrás del proyecto al estudiante, y se le enseñan los objetivos que este ha de conseguir al final del mismo.

Duración estimada de esta etapa: 1 día

- Reunión de comienzo

Reunión informativa en la que se dará a conocer la decisión inicial de comenzar con este proyecto. Además serán puestos los cimientos que darán el pistoletazo de salida a la puesta en marcha de este proyecto.

Duración estimada de esta etapa: 1 día

- Fase de diseño inicial

En esta fase, se llevará a cabo de manera exhaustiva un diseño viable y factible del este proyecto. Este diseño será de carácter inicial, y pasará a revisión del mismo en futuras fases. No sólo se tendrá en cuenta el aspecto más técnico de la misma, sino que también desde un punto de vista económico, teniendo en cuenta el costo de los materiales necesarios para su desarrollo.

A continuación se enseñarán y explicarán las sub-fases con las que contará la etapa de diseño inicial:

    - Legislación

En este apartado serán estudiados, analizados y comprendidos los aspectos legislativos y legales, que tengan relación alguna con este proyecto. Desde la ley de telecomunicaciones, hasta los boletines ofrecidos por la Comisión del Mercado de las Telecomunicaciones. Debido a que en los últimos tiempos el desarrollo del sector de las telecomunicaciones ha experimentado, considerablemente, un avance tecnológico, ha implicado un crecimiento paralelo de la normativa reguladora del sector; A partir de

este estudio, será posible ofrecer una solución tecnológica que pueda ser implementada en territorio español, y por lo tanto sea viable desde este punto de vista.

Duración estimada de esta etapa: 10 días

- Solución inicial respecto a la legislación española.

En este apartado llevaremos a cabo un análisis en profundidad de la legislación española en materia de telecomunicaciones, para poder llevar a cabo un proyecto cuya viabilidad sea factible en cualquier parte del territorio español, tanto peninsular como insular. La joven liberación de las telecomunicaciones en España (Ley 12/1997, de 24 de abril, de Liberalización de las Telecomunicaciones), y los compromisos adquiridos por la misma con la Unión Europea, han obligado la creación de un amplio cuerpo legislativo, dinámico y ágil debido a los constantes cambios vividos por este sector estratégico, para cada una de las áreas que conforman el sector de las telecomunicaciones.

Duración estimada de esta etapa: 10 días

- Diseño inicial y teórico de la red

En esta sub-etapa se realizará el diseño inicial y teórico de la red Wi-Fi a desplegar. Teniendo no sólo en cuenta el aspecto tecnológico de la misma, sino también el lado legislativo o legal de la futura solución a ser implementada.

Este diseño ha de estar en consonancia con la viabilidad y factibilidad de su realización futura.

Duración estimada de esta etapa: 25 días

- Estudio de OpenWISP

Tal y como veremos con mayor extensión más adelante, durante el desarrollo del proyecto, se escogerá OpenWISP como la solución más viable y de mayor encaje en la idea de este proyecto.

Este módulo tecnológico se encuentra escrito en el lenguaje *Ruby on Rails*[29] orientado a plataformas web. Por lo tanto, es una parte importante del proyecto, el adquirir conocimientos técnicos suficientes en este lenguaje de programación.

Duración estimada de esta etapa: 73 días

- Documentación de esta etapa

En esta etapa, se describirá y documentará todo el trabajo realizado durante esta fase del proyecto.

Duración estimada de esta etapa: 5 días

- Primera implementación

En esta fase se llevará a cabo un desarrollo inicial del diseño estipulado en la fase anterior, y por lo tanto una primera implementación, también llamada versión beta, de la solución escogida.

Más adelante, este proceso finalizará con una nueva iteración de diseño, corrigiendo y mejorando la versión actual de la solución prevista.

- Configuración del Servidor

Se realizará la configuración de los módulos de OpenWISP, en especial del servidor necesario para poner en marcha el sistema. Más adelante se analizará a fondo la tecnología OpenWISP y sus diferentes módulos y utilidades.

Duración estimada de esta etapa: 20 días

- Modificación del Firmware[25]

Es esta sub-etapa se modificará el firmware que será implementado en los puntos de acceso, que servirán para que los usuarios finales puedan disfrutar de este servicio. Esta modificación viene dada por las características del proyecto a desplegar, adaptando el firmware a la solución adecuada al caso de este trabajo. La tecnología adoptada por OpenWISP, y por lo tanto la que implantaremos en este proyecto, es llamada OpenWRT. Esta será analizada y enseñada más adelante durante el desarrollo de este trabajo.

Duración estimada de esta etapa: 20 días

- Configuración de enrutamiento y puntos de acceso

Una vez acabado, diseñado y desarrollado el firmware necesario para los dispositivos, se pasará a realizar la tarea de implementarles el nuevo código necesario para llevar a cabo nuestro proyecto.

Duración estimada de esta etapa: 20 días

- Desarrollo y puesta en marcha en un entorno controlado (laboratorio)

Esta sub-etapa es la primera gran demostración de la versión beta o de pruebas de nuestra solución. Aquí llevaremos a cabo la puesta en marcha del sistema en un entorno controlado como es en un laboratorio para observar las bondades y problemas que aún presente nuestra solución.

Duración estimada de esta etapa: 6 días

- Testeo y búsqueda de errores

Como resulta habitual en estos procedimientos, es imprescindible dedicar ciertos recursos del proyecto al testeo y corrección de posibles errores. Comúnmente, los errores suelen ser de diseño, o de funcionamiento. Esta tarea tiene el objetivo final de mejorar el producto final.

Duración estimada de esta etapa: 6 días

- Re-análisis del proyecto

La evolución y procedimiento natural de la sub-etapa anterior, es la de modificar la solución propuesta para corregir o mejorar aspectos que alcancen el mínimo de calidad y funcionamiento deseados.

Duración estimada de esta etapa: 4 días

- Documentación de esta etapa

En esta etapa, se describirá y documentará todo el trabajo realizado durante esta fase del proyecto.

Duración estimada de esta etapa: 4 días

- Implementación Final

En esta etapa, tal y como su nombre indica, será llevada a cabo la implementación y puesta a punto final del proceso. Se ejecutará y demostrará que la solución adoptada y desarrollada es viable y efectiva.

  - Despliegue de la red

Se llevará a cabo el despliegue e implementación del sistema desarrollado a lo largo del proyecto, y por lo tanto de la red. Aquí podremos observar ya los primeros frutos que ha dado el trabajo en sí. No obstante, en la siguiente etapa se corregirán o modificarán posibles contratiempos o imprevistos que hayan surgido.

Duración estimada de esta etapa: 18 días

  - Solución de problemas

Se resolverán los problemas que puedan surgir durante la primera implementación del prototipo. Dada la naturaleza del despliegue del proyecto, es probable que surjan diversos problemas al pasar de la propuesta teórica a la implantación real.

Duración estimada de esta etapa: 18 días

  - Análisis final del proyecto

En esta sub-etapa se llevará a cabo el análisis del proyecto en su versión final, su relación con la solución inicial, y toda la información pertinente para la correcta y debida explicación de los detalles de la solución finalmente adoptada.

Duración estimada de esta etapa: 14 días

  - Documentación de esta etapa

En esta etapa, se describirá y documentará todo el trabajo realizado durante esta fase del proyecto.

Duración estimada de esta etapa: 14 días

- Documentación total del proyecto

Llegado a este punto será llevada a cabo una recopilación de toda la información obtenida, a lo largo del desarrollo del proyecto.

Podemos observar también, cómo se lleva a cabo un proceso de documentación, al acabar cada una de las etapas del desarrollo de este proyecto.

Es vital llevar a cabo un registro documental del proceso, porque nos ayudará a identificar los aspectos más importantes del proyecto, aportándole identidad y personalidad. Además, ello permite reconocer e identificar: las ventajas y desventajas, los costos y beneficios, etc. del mismo.

La correcta documentación del proyecto se caracteriza por resaltar sus ventajas, a través de una adecuada estructura y lenguaje, de acuerdo al nivel del trabajo. Ésta debe destacar los objetivos, y ser útil como soporte para el desarrollo del proyecto, al contemplar todos los aspectos relevantes del mismo.

A través de la documentación final, será posible llevar a cabo una defensa del trabajo científico realizado, y podrá ser utilizado para ampliar los conocimientos científicos de la comunidad.

Duración estimada de esta etapa: 102 días

- Defensa del proyecto

    - Presentación Final del proyecto frente a un tribunal

Una vez finalizado el proyecto y reunida toda la documentación correspondiente, es necesario preparar la defensa del proyecto, para demostrar la viabilidad y validez del mismo. Para preparar una buena defensa del proyecto, el alumno debe tener en cuenta no sólo los puntos fuertes del mismo, sino saber responder al porqué de los puntos débiles que se hayan presentado. Además, ha de poder proporcionar soluciones para contrarrestar los efectos de dichas debilidades.

Debido a las características del proyecto desarrollado, el tribunal será minucioso con sus preguntas y análisis.

Debido a un tribunal compuesto por profesores de diferentes campos o áreas de estudio, se ha de describir el proyecto en un lenguaje menos especializado y comprensible para la mayoría de público, haciendo uso de la aportación de detalles técnicos cuando sea necesario.

Duración estimada de esta etapa: 30 días

Diagrama de Gantt. Planificación temporal del proyecto

A continuación, se enseña el diagrama de Gantt, que fue llevado a cabo como primera guía temporal de las tareas a realizar en este trabajo final de grado.

Tareas

WBS	Nombre	Inicio	Fin	Trabajo
1	Warm-up session	Jul 18	Jul 18	1d
2	Kick-off meeting	Jul 19	Jul 19	1d
3	**Initial design phase**	Jul 20	Sep 25	81d
3.1	Legistlation approach	Jul 20	Aug 2	10d
3.2	Spanish legislation initial solution	Jul 20	Jul 31	8d
3.3	Network design	Aug 3	Sep 6	25d
3.4	Studing OpenWisp	Aug 3	Sep 11	28d
3.5	Documentation	Sep 12	Sep 25	10d
4	**Early implementation**	Sep 26	Jan 21	121d
4.1	Firmware modification	Sep 26	Dec 4	50d
4.2	Server setup	Sep 26	Nov 6	30d
4.3	Router configuration	Dec 5	Dec 13	7d
4.4	Lab deployment	Dec 14	Dec 27	10d
4.5	Testing	Dec 28	Jan 10	10d
4.6	Project Re-analysis	Jan 11	Jan 21	7d
4.7	Documentation	Jan 11	Jan 21	7d
5	**Final implementation**	Jan 22	Mar 18	80d
5.1	Network deployment	Jan 22	Mar 4	30d
5.2	Troubleshooting	Jan 22	Mar 4	30d
5.3	Project final analysis	Mar 5	Mar 18	10d
5.4	Documentation	Mar 5	Mar 18	10d
6	Full documentation	Mar 19	May 13	40d
7	**Project defense**	May 14	May 14	1d
7.1	Final presentation	May 14	May 14	1d

En este momento, nos encontramos en una situación de retraso respecto a la planificación inicial. Para definir con mayor exactitud, nos encontraríamos en la primera fase, o “Initial Design Phase”, en dónde serán puestas las bases para el desarrollo del proyecto. No obstante, aún falta documentar de manera correcta esta etapa.

Más allá de todos los problemas tenidos con el calendario inicial, existe ahora la ventaja de poder dedicarse a la realización del proyecto a tiempo completo.

Es por este motivo, y tal como podemos observar, el calendario inicial establecido para el proyecto, no podrá ser llevado a cabo en el tiempo previsto. Por ello, es necesario un replanteo de la planificación, para dotar al proyecto de un calendario factible.

A continuación se enseña el nuevo planteamiento temporal:

Tareas

WBS	Nombre	Inicio	Fin	Trabajo
1	Warm-up session	Dec 5	Dec 5	1d
2	Kick-off meeting	Dec 6	Dec 6	1d
3	**Initial design phase**	Dec 7	Jan 10	43d
3.1	Legistlation approach	Dec 7	Dec 13	5d
3.2	Spanish legislation initial solution	Dec 7	Dec 13	5d
3.3	Network design	Dec 14	Jan 1	13d
3.4	Studing OpenWisp	Dec 14	Jan 3	15d
3.5	Documentation	Jan 4	Jan 10	5d
4	**Early implementation**	Jan 11	Mar 13	68d
4.1	Firmware modification	Jan 11	Feb 7	20d
4.2	Server setup	Jan 11	Feb 7	20d
4.3	Router configuration	Feb 8	Feb 20	9d
4.4	Lab deployment	Feb 21	Feb 27	5d
4.5	Testing	Feb 28	Mar 7	6d
4.6	Project Re-analysis	Mar 8	Mar 13	4d
4.7	Documentation	Mar 8	Mar 13	4d
5	**Final implementation**	Mar 14	Apr 12	44d
5.1	Network deployment	Mar 14	Apr 3	15d
5.2	Troubleshooting	Mar 14	Apr 3	15d
5.3	Project final analysis	Apr 4	Apr 12	7d
5.4	Documentation	Apr 4	Apr 12	7d
6	Full documentation	Apr 15	May 10	20d
7	**Project defense**	May 13	Jun 24	31d
7.1	Presentation preparation	May 13	Jun 21	30d
7.2	Final presentation	Jun 24	Jun 24	1d

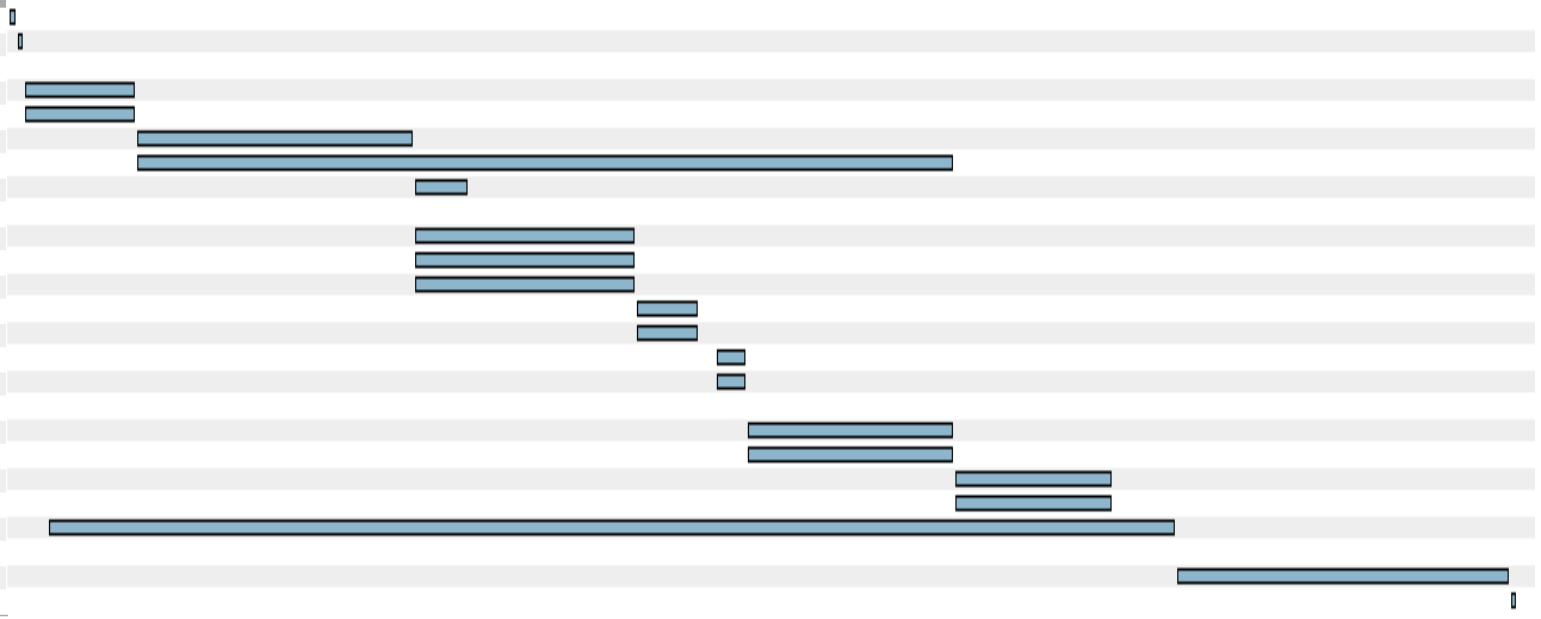
No obstante, a mediados de marzo, el calendario previsto del proyecto, ha de ser re-estipulado y corregido, para lograr los objetivos previstos en el tiempo establecido. Por ello, se rehace un calendario que se represente de manera más acertada, la duración temporal de las tareas a realizar.

WBS	Nombre	Inicio	Fin	Trabajo
1	Warm-up session	Dec 5	Dec 5	1d
2	Kick-off meeting	Dec 6	Dec 6	1d
3	**Initial design phase**	Dec 7	Apr 2	123d
3.1	Legistlation approach	Dec 7	Dec 20	10d
3.2	Spanish legislation initial solution	Dec 7	Dec 20	10d
3.3	Network design	Dec 21	Jan 24	25d
3.4	Studing OpenWisp	Dec 21	Apr 2	73d
3.5	Documentation	Jan 25	Jan 31	5d
4	**Early implementation**	Jan 25	Mar 7	80d
4.1	Server setup	Jan 25	Feb 21	20d
4.2	Firmware modification	Jan 25	Feb 21	20d
4.3	Router configuration	Jan 25	Feb 21	20d
4.4	Lab deployment	Feb 22	Mar 1	6d
4.5	Testing	Feb 22	Mar 1	6d
4.6	Project Re-analysis	Mar 4	Mar 7	4d
4.7	Documentation	Mar 4	Mar 7	4d
5	**Final implementation**	Mar 8	Apr 22	64d
5.1	Network deployment	Mar 8	Apr 2	18d
5.2	Troubleshooting	Mar 8	Apr 2	18d
5.3	Project final analysis	Apr 3	Apr 22	14d
5.4	Documentation	Apr 3	Apr 22	14d
6	Full documentation	Dec 10	Apr 30	102d
7	**Project defense**	May 1	Jun 12	31d
7.1	Presentation preparation	May 1	Jun 11	30d
7.2	Final presentation	Jun 12	Jun 12	1d

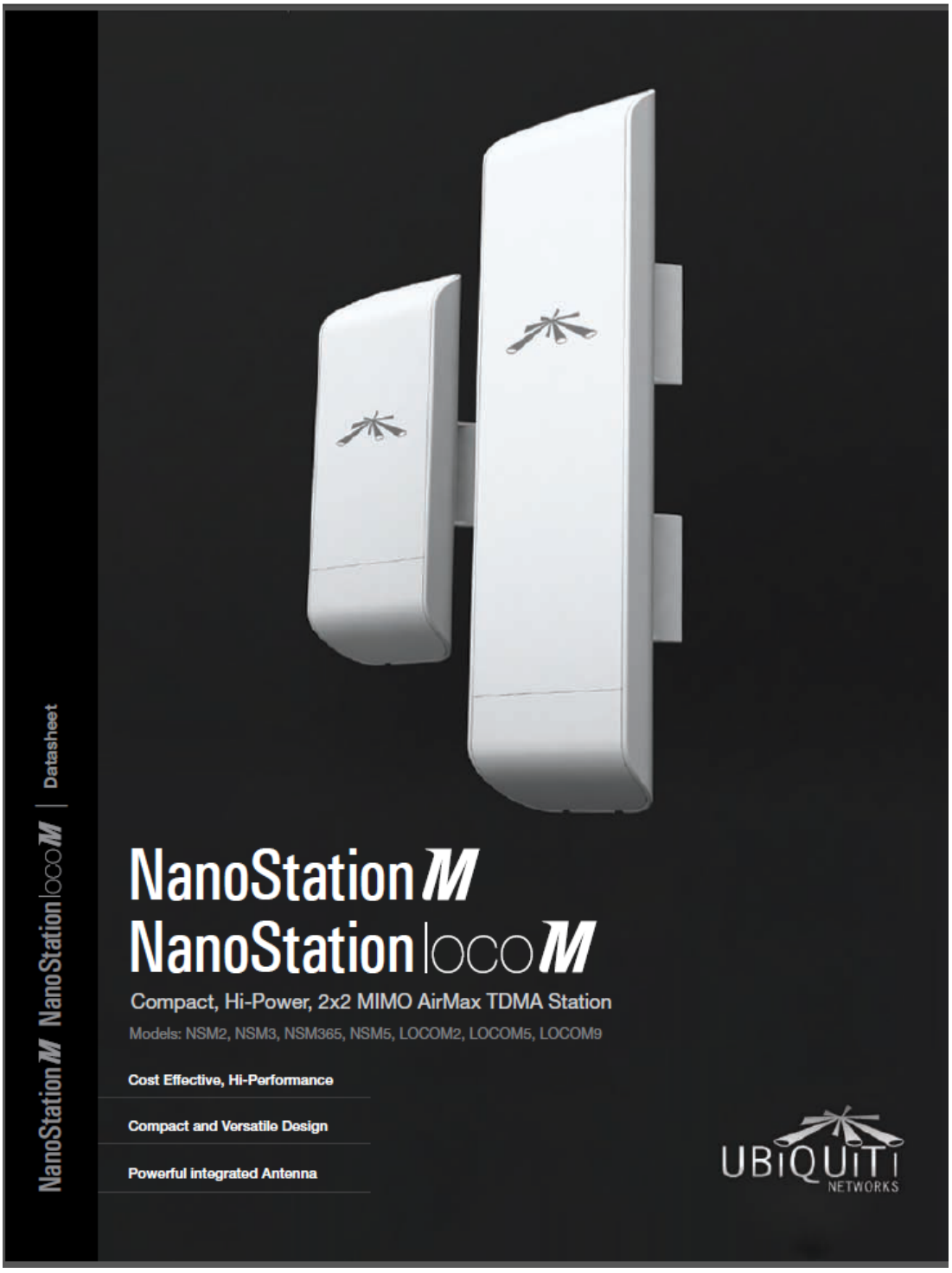
A continuación se detalla el diagrama de Gantt que finalmente siguió finalmente el proyecto.

Gráfica Gantt

WBS	Nombre	Trabajo
1	Warm-up session	1d
2	Kick-off meeting	1d
3	**Initial design phase**	**123d**
3.1	Legistlation approach	10d
3.2	Spanish legislation initial solution	10d
3.3	Network design	25d
3.4	Studing OpenWisp	73d
3.5	Documentation	5d
4	**Early implementation**	**80d**
4.1	Server setup	20d
4.2	Firmware modification	20d
4.3	Router configuration	20d
4.4	Lab deployment	6d
4.5	Testing	6d
4.6	Project Re-analysis	4d
4.7	Documentation	4d
5	**Final implementation**	**64d**
5.1	Network deployment	18d
5.2	Troubleshooting	18d
5.3	Project final analysis	14d
5.4	Documentation	14d
6	Full documentation	102d
7	**Project defense**	**31d**
7.1	Presentation preparation	30d
7.2	Final presentation	1d



Anexo III: UBNT NanoStation Datasheet



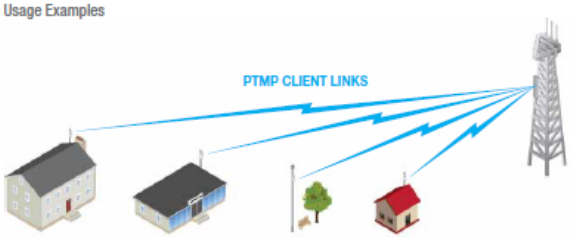
Overview

Leading Edge Industrial Design

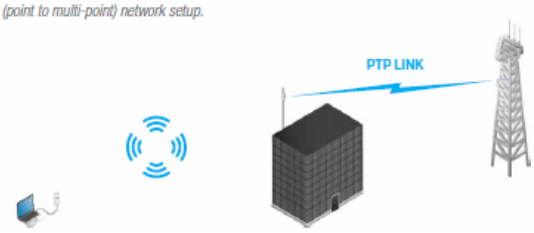
The original NanoStation set the bar for the world's first low-cost and efficiently designed outdoor broadband CPE. The new NanoStation M and NanoStation Loco M take the same concept to the future with new redesigned sleek and elegant form-factors along with integrated AirMax (MIMO TDMA Protocol) Technology.

The low cost, hi-performance, and small form factor of NanoStation M and NanoStation Loco M make them extremely versatile and ideal in several different applications (see diagrams on right for some usage examples).

Usage Examples



NanoStation M as powerful clients in an AirMax PTMP (point to multi-point) network setup.



NanoStation M as a powerful wireless client.

Use two NanoStation M to create a PTP link.

Integrated AirMax Technology

Unlike standard WiFi protocol, Ubiquiti's Time Division Multiple Access (TDMA) AirMax protocol allows each client to send & receive data using pre-designated time slots scheduled by an intelligent AP controller.

This "time slot" method eliminates hidden node collisions & maximizes air time efficiency. It provides many magnitudes of performance improvements in latency, throughput, & scalability compared to all other outdoor systems in its class.

Intelligent QoS Priority is given to voice/video for seamless access.

Scalability High capacity and scalability.

Long Distance Capable of high speed 50km+ links

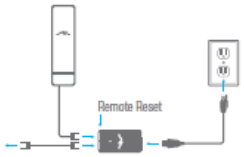
Latency Multiple features dramatically reduce noise.

Dual Ethernet Connectivity *

The New NanoStation M provides a secondary ethernet port with software enabled POE output for seamless IP Video integration.

Intelligent POE **

Remote hardware reset circuitry of NanoStation M allows for device to be reset remotely from power supply location. In addition, any NanoStation can easily become 802.3af 48V compliant through use of Ubiquiti's Instant 802.3af adapter (sold separately).



* Only NanoStation M models.
** Remote reset is an additional option. Nanostation M comes standard as 24V without remote reset.

Ubiquiti Networks, Inc. Copyright © 2011, All Rights Reserved

Models

[top] **NSM2** (2.4GHz, 10.4-11.2dBi), **NSM3** (3.4-3.7GHz, 12.2-13.7dBi), **NSM365** (3.65GHz, 12.2-13.7dBi), **NSM5** (5GHz, 14.6-16.1dBi)
[bottom left] **LOCOM9** (900MHz, 8dBi) [bottom right] **LOCOM2** (2.4GHz, 8.5dBi), **LOCOM5** (5GHz, 13dBi)

Ubiquiti Networks, Inc. Copyright © 2011, All Rights Reserved

Software

airOS

AirOS is an intuitive, versatile, highly developed Ubiquiti firmware technology. It is exceptionally intuitive and was designed to require no training to operate. Behind the user interface is a powerful firmware architecture which enables hi-performance outdoor multipoint networking.

Protocol Support

Ubiquiti Channelization

Spectral Width Adjust

ACK Auto-Timing

AAP Technology

Multi-Language Support

airView

Integrated on all Ubiquiti M products, AirView provides Advanced Spectrum Analyzer Functionality: Waterfall, waveform, and real-time spectral views allow operators to identify noise signatures and plan their networks to minimize noise interference.

Waterfall Aggregate energy over time for each frequency.

Waveform Aggregate energy collected.

Real-time Energy is shown real-time as a function of frequency.

Recording Automize AirView to record and report results.

airControl

AirControl is a powerful and intuitive web based server network management application which allows operators to centrally manage entire networks of Ubiquitii devices.

Network Map

Monitor Device Status

Mass Firmware Upgrade

Web UI Access

Manage Groups of Devices

Task Scheduling

Ubiquiti Networks, Inc. Copyright © 2011, All Rights Reserved

Specifications

System Information		
Processor Specs		Atheros MIPS 24KC, 400MHz
	LOCOM9	LOCOM, NSM
Memory Information	64MB SDRAM, 8MB Flash	32MB SDRAM, 8MB Flash
	LOCOM	NSM
Networking Interface	1 X 10/100 BASE-TX (Cat. 5, RJ-45) Ethernet	2 X 10/100 BASE-TX (Cat. 5, RJ-45) Ethernet

Regulatory / Compliance Information				
	LOCOM9	M2, M5**	NSM3	NSM365
Wireless Approvals	FCC Part 15.247, IC RS210	FCC Part 15.247, IC RS210, CE	-	FCC Part 90Z
RoHS Compliance	YES			

Physical / Electrical / Environmental / Antenna			
Enclosure Characteristics	Outdoor UV Stabilized Plastic		
Mounting Kit	Pole Mounting Kit included		
Power Method	Passive Power over Ethernet (pairs 4, 5+; 7, 8 return)		
Operating Temperature	-30C to 75C		
Operating Humidity	5 to 95% Condensing		
Shock and Vibration	ETSI300-019-1.4		
	LOCOM9	LOCOM	NSM
Dimensions	164 x 72 x 199 mm	163 x 31 x 80 mm	294 x 31 x 80 mm
Weight	0.9 kg	0.18 kg	0.4 kg 0.5 kg (M3/M365)
Power Supply (included)	24V, 1A POE	24V, 0.5A POE	24V, 0.5A POE 24V, 1A POE (M3/M365)
Max Power Consumption	6.5 Watts	5.5 Watts	8 Watts
Antenna Gain	8 dBi	8 dBi (M2) 13 dBi (M5)	11 dBi (M2) 13.7 dBi (M3/M365) 16 dBi (M5)
Polarization	Dual Linear		
RF Connector	External RP-SMA	-	-

Operating Frequency Summary (MHz)				
LOCOM9	M2**	NSM3	NSM365	M5**
902-928	2412-2462	3400-3700	3650-3675	5470-5825*

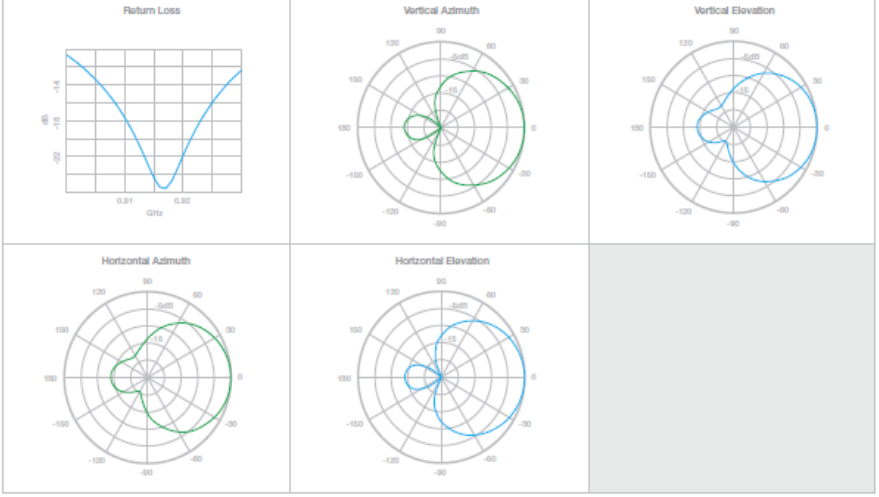
* Only 5745 - 5825 MHz is supported in the USA
** Applies to both NanoStation M and NanoStation Loco M models

Ubiquiti Networks, Inc. Copyright © 2011, All Rights Reserved

Specifications (cont.) - LOCOM9

NanoStation Loco M9 - Operating Frequency 902-928 MHz							
OUTPUT POWER: 28 dBm							
900 MHz TX POWER SPECIFICATIONS				900 MHz RX POWER SPECIFICATIONS			
AirMax	MCS0	28 dBm	+/- 2 dB	AirMax	MCS0	-96 dBm	+/- 2 dB
	MCS1	28 dBm	+/- 2 dB		MCS1	-95 dBm	+/- 2 dB
	MCS2	28 dBm	+/- 2 dB		MCS2	-92 dBm	+/- 2 dB
	MCS3	28 dBm	+/- 2 dB		MCS3	-90 dBm	+/- 2 dB
	MCS4	28 dBm	+/- 2 dB		MCS4	-86 dBm	+/- 2 dB
	MCS5	24 dBm	+/- 2 dB		MCS5	-83 dBm	+/- 2 dB
	MCS6	22 dBm	+/- 2 dB		MCS6	-77 dBm	+/- 2 dB
	MCS7	21 dBm	+/- 2 dB		MCS7	-74 dBm	+/- 2 dB
	MCS8	28 dBm	+/- 2 dB		MCS8	-95 dBm	+/- 2 dB
	MCS9	28 dBm	+/- 2 dB		MCS9	-93 dBm	+/- 2 dB
	MCS10	28 dBm	+/- 2 dB		MCS10	-90 dBm	+/- 2 dB
	MCS11	28 dBm	+/- 2 dB		MCS11	-87 dBm	+/- 2 dB
	MCS12	28 dBm	+/- 2 dB		MCS12	-84 dBm	+/- 2 dB
	MCS13	24 dBm	+/- 2 dB		MCS13	-79 dBm	+/- 2 dB
	MCS14	22 dBm	+/- 2 dB		MCS14	-78 dBm	+/- 2 dB
	MCS15	21 dBm	+/- 2 dB		MCS15	-75 dBm	+/- 2 dB

NanoStation Loco M9 - Antenna Information (for integrated 2x2 MIMO Antenna)	
NanoStation Loco M9 also features a RP-SMA connector for a higher gain external antenna	
Gain	7.5 dBi
Cross-pol Isolation	28 dB minimum
Max VSWR	1.3:1
Beamwidth	60 deg. (H-pol) / 60 deg (V-pol) / 60 deg (Elevation)

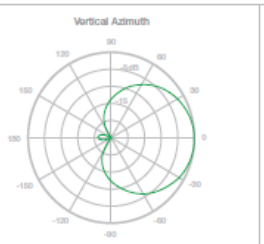


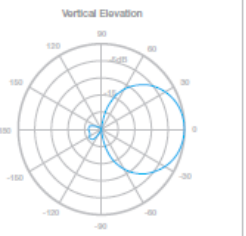
Ubiquiti Networks, Inc. Copyright © 2011, All Rights Reserved

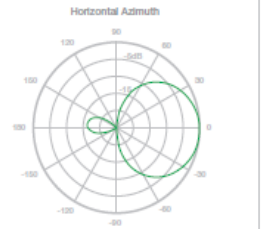
Specifications (cont.) - LOCOM2

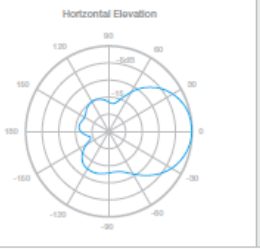
NanoStation Loco M2 - Operating Frequency 2412-2462 MHz							
OUTPUT POWER: 23 dBm							
2.4 GHz TX POWER SPECIFICATIONS				2.4 GHz RX POWER SPECIFICATIONS			
	DataRate	Avg. TX	Tolerance		DataRate	Avg. TX	Tolerance
11b / g	1-24 Mbps	23 dBm	+/- 2 dB	11b / g	1-24 Mbps	-83 dBm	+/- 2 dB
	36 Mbps	21 dBm	+/- 2 dB		36 Mbps	-80 dBm	+/- 2 dB
	48 Mbps	19 dBm	+/- 2 dB		48 Mbps	-77 dBm	+/- 2 dB
	54 Mbps	18 dBm	+/- 2 dB		54 Mbps	-75 dBm	+/- 2 dB
11n / AirMax	MCS0	23 dBm	+/- 2 dB	11n / AirMax	MCS0	-96 dBm	+/- 2 dB
	MCS1	23 dBm	+/- 2 dB		MCS1	-95 dBm	+/- 2 dB
	MCS2	23 dBm	+/- 2 dB		MCS2	-92 dBm	+/- 2 dB
	MCS3	23 dBm	+/- 2 dB		MCS3	-90 dBm	+/- 2 dB
	MCS4	22 dBm	+/- 2 dB		MCS4	-86 dBm	+/- 2 dB
	MCS5	20 dBm	+/- 2 dB		MCS5	-83 dBm	+/- 2 dB
	MCS6	18 dBm	+/- 2 dB		MCS6	-77 dBm	+/- 2 dB
	MCS7	17 dBm	+/- 2 dB		MCS7	-74 dBm	+/- 2 dB
	MCS8	23 dBm	+/- 2 dB		MCS8	-95 dBm	+/- 2 dB
	MCS9	23 dBm	+/- 2 dB		MCS9	-93 dBm	+/- 2 dB
	MCS10	23 dBm	+/- 2 dB		MCS10	-90 dBm	+/- 2 dB
	MCS11	23 dBm	+/- 2 dB		MCS11	-87 dBm	+/- 2 dB
	MCS12	22 dBm	+/- 2 dB		MCS12	-84 dBm	+/- 2 dB
	MCS13	20 dBm	+/- 2 dB		MCS13	-79 dBm	+/- 2 dB
	MCS14	18 dBm	+/- 2 dB		MCS14	-78 dBm	+/- 2 dB
	MCS15	17 dBm	+/- 2 dB		MCS15	-75 dBm	+/- 2 dB

NanoStation Loco M2 - Antenna Information	
Gain	8.5 dBi
Cross-pol Isolation	20 dB minimum
Max VSWR	1.4:1
Beamwidth	60 deg. (H-pol) / 60 deg (V-pol) / 60 deg (Elevation)







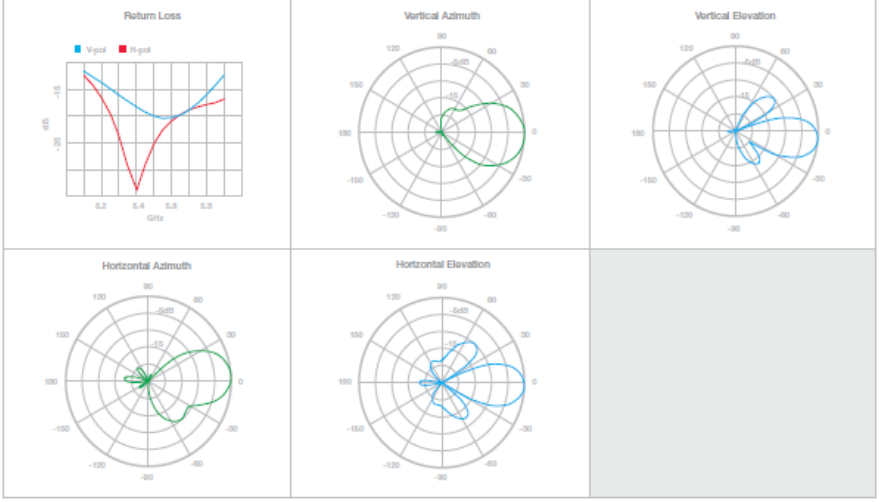


Ubiquiti Networks, Inc. Copyright © 2011, All Rights Reserved

Specifications (cont.) - LOCOM5

NanoStation Loco M5 - Operating Frequency 5470-5825 MHz*							
OUTPUT POWER: 23 dBm							
5 GHz TX POWER SPECIFICATIONS				5 GHz RX POWER SPECIFICATIONS			
	DataRate	Avg. TX	Tolerance		DataRate	Avg. TX	Tolerance
11a	6-24 Mbps	23 dBm	+/- 2 dB	11a	6-24 Mbps	-83 dBm	+/- 2 dB
	36 Mbps	21 dBm	+/- 2 dB		36 Mbps	-80 dBm	+/- 2 dB
	48 Mbps	19 dBm	+/- 2 dB		48 Mbps	-77 dBm	+/- 2 dB
	54 Mbps	18 dBm	+/- 2 dB		54 Mbps	-75 dBm	+/- 2 dB
11n / AirMax	MCS0	23 dBm	+/- 2 dB	11n / AirMax	MCS0	-96 dBm	+/- 2 dB
	MCS1	23 dBm	+/- 2 dB		MCS1	-95 dBm	+/- 2 dB
	MCS2	23 dBm	+/- 2 dB		MCS2	-92 dBm	+/- 2 dB
	MCS3	23 dBm	+/- 2 dB		MCS3	-90 dBm	+/- 2 dB
	MCS4	22 dBm	+/- 2 dB		MCS4	-86 dBm	+/- 2 dB
	MCS5	20 dBm	+/- 2 dB		MCS5	-83 dBm	+/- 2 dB
	MCS6	18 dBm	+/- 2 dB		MCS6	-77 dBm	+/- 2 dB
	MCS7	17 dBm	+/- 2 dB		MCS7	-74 dBm	+/- 2 dB
	MCS8	23 dBm	+/- 2 dB		MCS8	-95 dBm	+/- 2 dB
	MCS9	23 dBm	+/- 2 dB		MCS9	-93 dBm	+/- 2 dB
	MCS10	23 dBm	+/- 2 dB		MCS10	-90 dBm	+/- 2 dB
	MCS11	23 dBm	+/- 2 dB		MCS11	-87 dBm	+/- 2 dB
	MCS12	22 dBm	+/- 2 dB		MCS12	-84 dBm	+/- 2 dB
	MCS13	20 dBm	+/- 2 dB		MCS13	-79 dBm	+/- 2 dB
	MCS14	18 dBm	+/- 2 dB		MCS14	-78 dBm	+/- 2 dB
	MCS15	17 dBm	+/- 2 dB		MCS15	-75 dBm	+/- 2 dB

NanoStation Loco M5 - Antenna Information	
Gain	13 dBi
Cross-pol Isolation	20 dB minimum
Max VSWR	1.4:1
Beamwidth	45 deg. (H-pol) / 45 deg (V-pol) / 45 deg (Elevation)



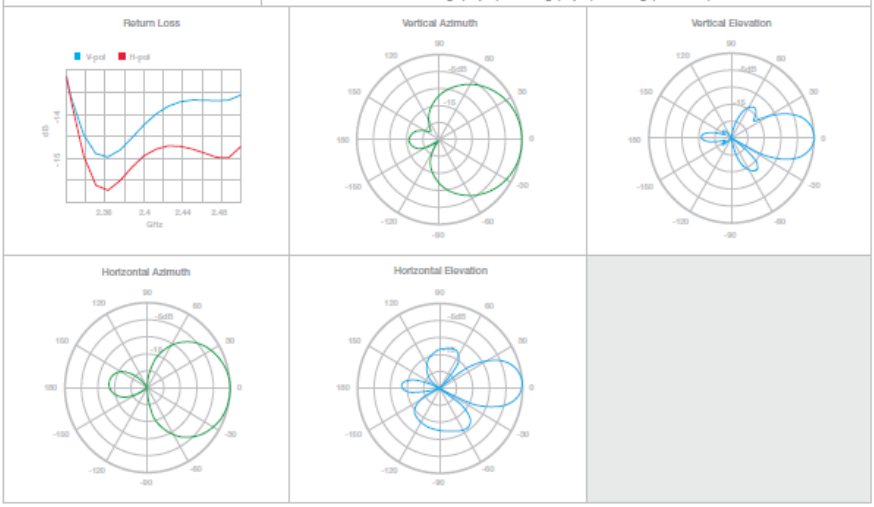
Ubiquiti Networks, Inc. Copyright © 2011, All Rights Reserved

* Only 5745 - 5825 MHz is supported in the USA

Specifications (cont.) - NSM2

NanoStation M2 - Operating Frequency 2412-2462 MHz							
OUTPUT POWER: 28 dBm							
2.4 GHz TX POWER SPECIFICATIONS					2.4 GHz RX POWER SPECIFICATIONS		
	DataRate	Avg. TX	Tolerance		DataRate	Avg. TX	Tolerance
11b / g	1-24 Mbps	28 dBm	+/- 2 dB	11b / g	1-24 Mbps	-97 dBm min	+/- 2 dB
	36 Mbps	26 dBm	+/- 2 dB		36 Mbps	-80 dBm	+/- 2 dB
	48 Mbps	25 dBm	+/- 2 dB		48 Mbps	-77 dBm	+/- 2 dB
	54 Mbps	24 dBm	+/- 2 dB		54 Mbps	-75 dBm	+/- 2 dB
11n / AirMax	MCS0	28 dBm	+/- 2 dB	11n / AirMax	MCS0	-96 dBm	+/- 2 dB
	MCS1	28 dBm	+/- 2 dB		MCS1	-95 dBm	+/- 2 dB
	MCS2	28 dBm	+/- 2 dB		MCS2	-92 dBm	+/- 2 dB
	MCS3	28 dBm	+/- 2 dB		MCS3	-90 dBm	+/- 2 dB
	MCS4	27 dBm	+/- 2 dB		MCS4	-86 dBm	+/- 2 dB
	MCS5	25 dBm	+/- 2 dB		MCS5	-83 dBm	+/- 2 dB
	MCS6	23 dBm	+/- 2 dB		MCS6	-77 dBm	+/- 2 dB
	MCS7	22 dBm	+/- 2 dB		MCS7	-74 dBm	+/- 2 dB
	MCS8	28 dBm	+/- 2 dB		MCS8	-95 dBm	+/- 2 dB
	MCS9	28 dBm	+/- 2 dB		MCS9	-93 dBm	+/- 2 dB
	MCS10	28 dBm	+/- 2 dB		MCS10	-90 dBm	+/- 2 dB
	MCS11	28 dBm	+/- 2 dB		MCS11	-87 dBm	+/- 2 dB
	MCS12	27 dBm	+/- 2 dB		MCS12	-84 dBm	+/- 2 dB
	MCS13	25 dBm	+/- 2 dB		MCS13	-79 dBm	+/- 2 dB
	MCS14	23 dBm	+/- 2 dB		MCS14	-78 dBm	+/- 2 dB
	MCS15	22 dBm	+/- 2 dB		MCS15	-75 dBm	+/- 2 dB

NanoStation M2 - Antenna Information	
Gain	10.4-11.2 dBi
Cross-pol Isolation	23 dB minimum
Max VSWR	1.6:1
Beamwidth	55 deg. (H-pol) / 53 deg (V-pol) / 27 deg (Elevation)

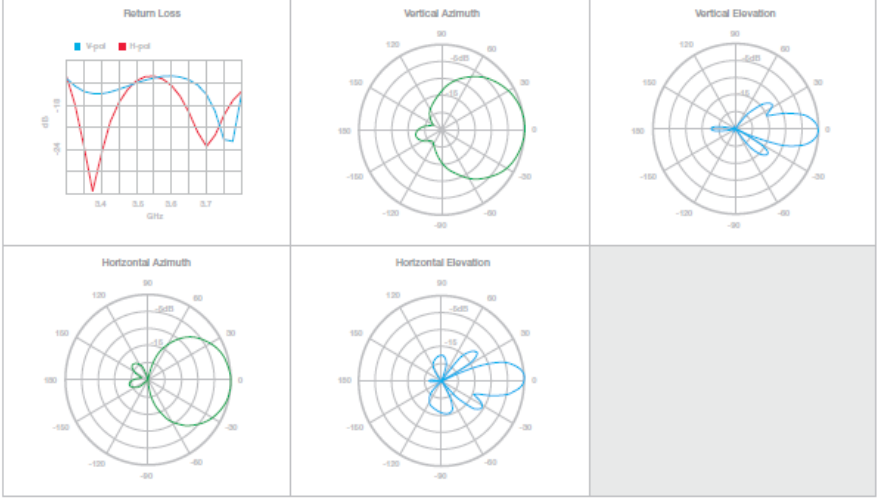


Ubiquiti Networks, Inc. Copyright © 2011, All Rights Reserved

Specifications (cont.) - NSM3/NSM365

NanoStation M3 (3400-3700 MHz) / NanoStation M365 (3650-3675 MHz)							
OUTPUT POWER: 25 dBm							
TX POWER SPECIFICATIONS				RX POWER SPECIFICATIONS			
AirMax	MCS0	25 dBm	+/- 2 dB	AirMax	MCS0	-94 dBm	+/- 2 dB
	MCS1	25 dBm	+/- 2 dB		MCS1	-93 dBm	+/- 2 dB
	MCS2	25 dBm	+/- 2 dB		MCS2	-90 dBm	+/- 2 dB
	MCS3	25 dBm	+/- 2 dB		MCS3	-89 dBm	+/- 2 dB
	MCS4	24 dBm	+/- 2 dB		MCS4	-86 dBm	+/- 2 dB
	MCS5	23 dBm	+/- 2 dB		MCS5	-83 dBm	+/- 2 dB
	MCS6	22 dBm	+/- 2 dB		MCS6	-77 dBm	+/- 2 dB
	MCS7	20 dBm	+/- 2 dB		MCS7	-74 dBm	+/- 2 dB
	MCS8	25 dBm	+/- 2 dB		MCS8	-93 dBm	+/- 2 dB
	MCS9	25 dBm	+/- 2 dB		MCS9	-91 dBm	+/- 2 dB
	MCS10	25 dBm	+/- 2 dB		MCS10	-89 dBm	+/- 2 dB
	MCS11	25 dBm	+/- 2 dB		MCS11	-87 dBm	+/- 2 dB
	MCS12	24 dBm	+/- 2 dB		MCS12	-84 dBm	+/- 2 dB
	MCS13	23 dBm	+/- 2 dB		MCS13	-79 dBm	+/- 2 dB
	MCS14	22 dBm	+/- 2 dB		MCS14	-78 dBm	+/- 2 dB
	MCS15	20 dBm	+/- 2 dB		MCS15	-75 dBm	+/- 2 dB

NanoStation M3 / M365 - Antenna Information	
Gain	12.2 - 13.7 dBi
Cross-pol Isolation	28 dB minimum
Max VSWR	1.4:1
Beamwidth	60 deg. (H-pol) / 60 deg (V-pol) / 20 deg (Elevation)

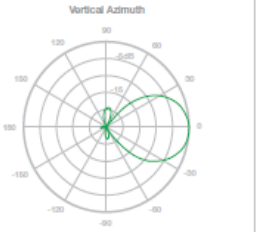


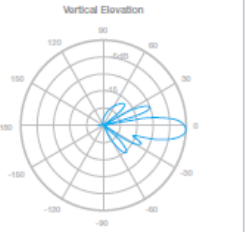
Ubiquiti Networks, Inc. Copyright © 2011, All Rights Reserved

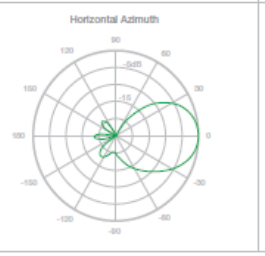
Specifications (cont.) - NSM5

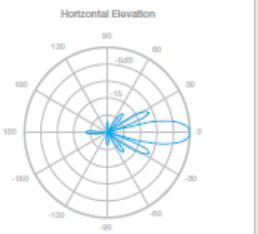
NanoStation M5 - Operating Frequency 5470-5825 MHz							
OUTPUT POWER: 27 dBm							
5 GHz TX POWER SPECIFICATIONS					5 GHz RX POWER SPECIFICATIONS		
	DataRate	Avg. TX	Tolerance		DataRate	Avg. TX	Tolerance
11a	6-24 Mbps	27 dBm	+/- 2 dB	11a	6-24 Mbps	-94 dBm min	+/- 2 dB
	36 Mbps	25 dBm	+/- 2 dB		36 Mbps	-80 dBm	+/- 2 dB
	48 Mbps	23 dBm	+/- 2 dB		48 Mbps	-77 dBm	+/- 2 dB
	54 Mbps	22 dBm	+/- 2 dB		54 Mbps	-75 dBm	+/- 2 dB
11n / AirMax	MCS0	27 dBm	+/- 2 dB	11n / AirMax	MCS0	-96 dBm	+/- 2 dB
	MCS1	27 dBm	+/- 2 dB		MCS1	-95 dBm	+/- 2 dB
	MCS2	27 dBm	+/- 2 dB		MCS2	-92 dBm	+/- 2 dB
	MCS3	27 dBm	+/- 2 dB		MCS3	-90 dBm	+/- 2 dB
	MCS4	26 dBm	+/- 2 dB		MCS4	-86 dBm	+/- 2 dB
	MCS5	24 dBm	+/- 2 dB		MCS5	-83 dBm	+/- 2 dB
	MCS6	22 dBm	+/- 2 dB		MCS6	-77 dBm	+/- 2 dB
	MCS7	21 dBm	+/- 2 dB		MCS7	-74 dBm	+/- 2 dB
	MCS8	27 dBm	+/- 2 dB		MCS8	-95 dBm	+/- 2 dB
	MCS9	27 dBm	+/- 2 dB		MCS9	-93 dBm	+/- 2 dB
	MCS10	27 dBm	+/- 2 dB		MCS10	-90 dBm	+/- 2 dB
	MCS11	27 dBm	+/- 2 dB		MCS11	-87 dBm	+/- 2 dB
	MCS12	26 dBm	+/- 2 dB		MCS12	-84 dBm	+/- 2 dB
	MCS13	24 dBm	+/- 2 dB		MCS13	-79 dBm	+/- 2 dB
	MCS14	22 dBm	+/- 2 dB		MCS14	-78 dBm	+/- 2 dB
	MCS15	21 dBm	+/- 2 dB		MCS15	-75 dBm	+/- 2 dB

NanoStation M5 - Antenna Information	
Gain	14.6 - 16.1 dBi
Cross-pol Isolation	22 dB minimum
Max VSWR	1.6:1
Beamwidth	43 deg. (H-pol) / 41 deg (V-pol) / 15 deg (Elevation)









Ubiquiti Networks, Inc. Copyright © 2011, All Rights Reserved

* Only 5745 - 5825 MHz is supported in the USA

Misc

TOUGHCable

OUTDOOR CARRIER CLASS SHIELDED

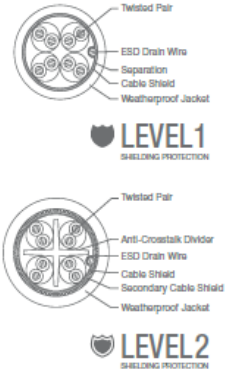
Protect your networks from the most brutal environments with Ubiquiti's industrial-grade shielded ethernet cable, TOUGHCable.

Increase Performance Dramatically improve your ethernet link states, speeds, and overall performance with Ubiquiti TOUGHCables.

Extreme Weatherproof TOUGHCables have been built to perform even in the harshest weather and environments.

Eliminate ESD Attacks Protect your networks from devastating ESD Attacks, TOUGHCables eliminate ESD attacks and ethernet hardware damage.

Extended Cable Support TOUGHCables have been developed to have increased power handling performance for extended cable run lengths.



Bulletproof your networks

TOUGHCable is currently available in two versions: Level 1 Shielding Protection and Level 2 Shielding Protection.

Level 1 is a Category 5e (Up to 1Gbps Ethernet Support) Outdoor Carrier Class Shielded Cable.

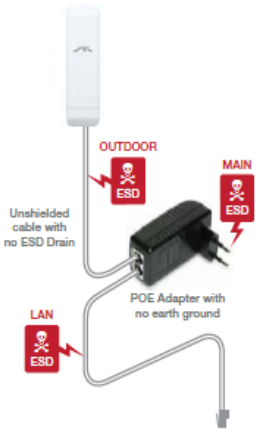
Level 2 is a Category 5e Enhanced Gigabit Performance (1Gbps Ethernet Support) Outdoor Carrier Class Shielded Cable.

Additional Information:

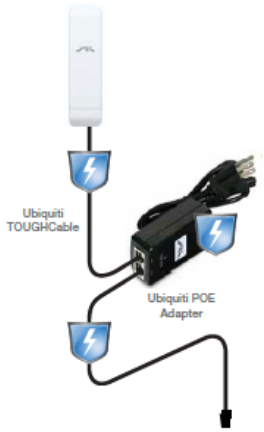
- 24 AWG copper conductor pairs
- ESD Drain Wire: 26 AWG integrated ESD Drain wire to prevent ESD attacks & damage.
- PVC outdoor rated jacket
- 0.35um foil shield
- Multi-Layered Shielding
- 1000ft (304.8m) length
- Use with TOUGHCable Connectors (sold separately) for optimal performance

Learn more:
www.ubnt.com/toughcable

ESD Attacks are overwhelmingly the leading cause for device failures. The diagram below illustrates the areas vulnerable to ESD Attacks in a defenseless network.



By using a grounded Ubiquiti POE adapter (included) along with Ubiquiti TOUGHCable (sold separately), you can effectively eliminate ESD Attacks.



Ubiquiti Networks, Inc. Copyright © 2011, All Rights Reserved

UBIQUITI NETWORKS

TERMS OF USE: The Ubiquiti radio device must be professionally installed. Shielded ethernet cable and earth grounding must be used as conditions of product warranty. It is the installers responsibility to follow local country regulations including operation within legal frequency channels, output power, and Dynamic Frequency Selection (DFS) requirements.

For further information, please visit www.ubnt.com.

All specifications in this document are subject to change without notice. NSM-DS-042911

Ubiquiti Networks, Inc. Copyright © 2011, All Rights Reserved

Anexo IV: Tablas de precios de equipos

Tabla 6: Precios D-Link DIR 825.[41]

Precio Final	Tienda	URL
78,17€	Amazon	http://www.amazon.es/D-Link-Xtreme-Gigabit-Router-Dir-825/dp/B001WAKCYQ/ref=sr_1_1?ie=UTF8&qid=1363262685&sr=8-1
120,99€	centerPConline.com	http://www.centerpconline.com/product?product_id=27161&utm_source=shopmania&utm_medium=cpc&utm_campaign=direct_link#.UUG96xyQXh4
87,90€	PixMania.com	http://www.pixmania.com/es/es/2820725/art/d-link/router-wifi-quadband-dir.html?merch=1#srcid=9650&key=ZkgNBjAdamUgLl0oDj0EWQs6QXArMSEXGRMVMXdGaEd4cUJ0GhZQWFUlDjgHVQk5RnxaXg==&CodePromo=oui
106,27€	CLS Informática	http://www.clsmarket.com/routers/4374-d-link-dir-825-0790069318122.html?utm_source=shopmania&utm_medium=cpc&utm_campaign=direct_link

Tabla 7: Precio Equipo Alix.[41]

Componente	Precio Final	Tienda	URL
ALIX 2D2	85,30€	LandaShop	http://landashop.com/catalog/pcengines-alix-lx800-mpci-p-82.html
Fuente Alimentación	5,52€	LandaShop	http://landashop.com/catalog/fuente-alimentacion-p-253.html?language=es
Interfaz Radio	27,50€	LandaShop	http://landashop.com/catalog/compex-wlm54sag23-80211agb-200mw-p-206.html
Tarjeta Memoria Flash	28,59€	Amazon	http://www.amazon.es/Sandisk-Tarjeta-memoria-Compact-Flash/dp/B0007QU6WY/ref=sr_1_1?ie=UTF8&qid=1363793513&sr=8-1
Pigtail	5,87€	LandaShop	http://landashop.com/catalog/pigtail-ufln-jack-bulkhead-p-235.html

Tabla 8: Precios NanoStation.[41]

Precio Final	Tienda	URL	Modelo
76,00€	Amazon	http://www.amazon.es/PUNTO-ACCESO-EXTERIOR-UBIQUITI-NANOSTATION/dp/B007FPRPGU/ref=sr_1_1?ie=UTF8&qid=1363276773&sr=8-1	2
85,00€	Amazon	http://www.amazon.es/PUNTO-ACCESO-EXTERIOR-UBIQUITI-NANOSTATION/dp/B007FPRP9M/ref=sr_1_5?ie=UTF8&qid=1363276773&sr=8-5	5
78,34€	LandaShop	http://landashop.com/catalog/nanostation-mimo-airmax-p-1027.html	M2
78,34€	LandaShop	http://landashop.com/catalog/nanostation-mimo-airmax-p-1026.html	M5

[41] Webs consultadas el 14 de marzo de 2013, a las 20.30 hs

Tabla 9: Precios NanoStation Loco.[41]

Precio Final	Tienda	URL	Modelo
44,49€	LandaShop	http://landashop.com/catalog/nanostation-loco2-polarizacion-dual-p-782.html	2
62,31€	MasWIFI	http://www.maswifi.com/puntos-de-acceso/nanostation-5-loco-ubiquiti-5-ghz-13dbi-punto-acceso-router-cliente	5
48,34€	MasWIFI	http://www.maswifi.com/puntos-de-acceso/ubiquiti-nanostation-loco-m2-2-4-ghz-8-dbi-mimo-airmax	M2
60,89€	LandaShop	http://landashop.com/catalog/nanostation-loco-mimo-airmax-p-1681.html	M5

Tabla 10: Precios PicoStation. [41]

Precio Componentes	Tienda	URL	Modelo
52,96€	LandaShop	http://landashop.com/catalog/picostation2-antena-omni-desmontable-rsma-p-778.html	2
73,81€	MasWIFI	http://www.maswifi.com/puntos-de-acceso/interior/ubiquiti-picostation5-802-11a-5ghz-antena-7dbi	5
71,49€	LandaShop	http://landashop.com/catalog/picostation-mimo-airmax-antena-omni-rsma-p-1718.html	M2
74,17€	MasWIFI	http://www.maswifi.com/puntos-de-acceso/interior/ubiquiti-picostation-m2h-mimo-airmax-800mw-802-11g-n-antena-6dbi	M2

Tabla 11: Precios UniFi.[41]

Precio Componentes	Tienda	URL	Modelo
48,20€	LandaShop	http://landashop.com/catalog/unifi-access-point-wifi-standard-p-1895.html?gclid=CIKepfqa_7UCFRDKtAod6R8Aew	UAP
76,02€	EuroDK	http://www.eurodk.com/en/products/indoor-%D1%81/unifi-long-range/	UAP-LR
233,17€	MasWIFI	http://www.maswifi.com/ubiquiti-unifi-uap-pro-gige-radio-dual-hasta-750mbps?gclid=CJGG4p6f_7UCFY3LtAodyCAAzw	UAP-PRO
94,79€	LandaShop	http://landashop.com/catalog/unifi-access-point-wifi-outdoor-p-2489.html?gclid=COmt35-f_7UCFUfMtAodMRIALg	UAP-Outdoor

Anexo V: Reglamento Free Italia WiFi

REGOLAMENTO TECNICO FEDERAZIONE

FreeItalia WiFi

Sommario

Premesse

La Federazione di Reti Wi-Fi istituzionali ha lo scopo di interconnettere infrastrutture d'accesso realizzate mediante la tecnologia Wi-Fi tra enti, organizzazioni ed entità in genere che intendono promuovere un servizio di accesso a Internet destinato ai propri utenti e distribuito tra gli enti partecipanti alla federazione FreeItaliaWiFi.

L'elemento caratterizzante della Federazione di Reti Wi-Fi è rappresentato dalla condivisione di un unico punto d'interconnessione, denominato nel seguito *IX-WiFi*, come struttura di collegamento e regolamentazione per i diversi partecipanti.

Attraverso il presente regolamento tecnico sono definite le regole per l'ammissione alla Rete Federata e le modalità di interconnessione all'IX-WiFi.

Il rispetto delle regole espresse all'interno del presente regolamento tecnico rappresentano condizione necessaria per poter richiedere l'adesione alla federazione di Reti Wi-Fi.

Il presente regolamento tecnico rappresenta un accordo formale tra le entità federate e l'IX-WiFi.

Comitato Tecnico

È istituito il Comitato Tecnico di IX-WiFi, composto da un rappresentante per ognuna delle seguenti entità:

- Comune di Venezia;
- Provincia di Roma;
- Regione Sardegna;
- Consorzio CINECA, operatore tecnico del punto di interconnessione IX-WiFi.

Il Comitato Tecnico ha il compito di

- Vigilare sul rispetto del Regolamento Tecnico da parte degli afferenti all'IX-WiFi e del personale tecnico dell'IX-WiFi;
- Proporre e adottare modifiche al Regolamento Tecnico;
- Supervisionare la qualità dei servizi offerti dal punto d'interconnessione, proporre innovazioni e iniziative finalizzate allo sviluppo di IX-WiFi e al miglioramento della qualità dei servizi stessi.

Prerequisiti per la federazione

Il presente accordo di federazione può essere stipulato da entità legalmente riconosciute.

La richiesta di partecipazione alla Federazione di Reti Wi-Fi può essere formalizzata attraverso la presentazione di un "accordo di federazione" stipulato seguendo le regole per l'ammissione di seguito elencate. L'entità che intende federarsi deve:

- garantire all'IX-WiFi di essere in possesso dei pieni poteri di proprietà e legali per poter rispettare i punti del seguente documento;
- essere essa stessa, o servirsi di, un operatore di comunicazioni "titolare" di un servizio per la fornitura di connettività a Internet wireless gratuita a utenti italiani e stranieri, e in regola con la normativa per la privacy e per la sicurezza (cfr. Normativa di riferimento). A mero titolo esemplificativo, il candidato deve impegnarsi a mettere a disposizione i log e l'anagrafica degli utenti in caso di accesso da parte delle autorità preposte.

L'entità candidata alla federazione è inoltre tenuta a presentare la documentazione di seguito elencata che certifichi i requisiti necessari secondo le modalità espresse dal presente regolamento:

- autorizzazione generale per la fornitura di reti o servizi di comunicazione elettronica ad uso pubblico;
- iscrizione al registro degli operatori di comunicazione dell'entità cui appartengono gli indirizzi di rete utilizzati dagli utenti finali del servizio;
- autorizzazione alla fornitura al pubblico dell'accesso RadioLAN alle reti ed ai servizi di telecomunicazioni (Wi-Fi) ai sensi del Decreto ministeriale 28/05/03 (cfr. "Normativa di riferimento").

Fermo restando il rispetto dei requisiti minimi sopraelencati, le domande di ammissione sono valutate e approvate dal Comitato Tecnico.

Tutti gli enti federati hanno stessi diritti e devono rispettare i medesimi doveri nei confronti dell'IX-WiFi.

Regole generali

- Ogni afferente è federato con tutti gli altri afferenti, e si impegna a consentire l'accesso agli utenti appartenenti a tutte le altre reti federate;
- l'afferente s'impegna a consentire l'accesso agli utenti appartenenti alle altre reti federate in maniera non discriminatoria rispetto all'accesso principale (ad esempio, in caso di accesso mediante captive portal, affiancando alla maschera di accesso principale la maschera di accesso federato, o un collegamento diretto alla maschera);
- l'afferente s'impegna a fornire il servizio di verifica delle credenziali di accesso per i soli utenti registrati al proprio servizio. Non è consentita la fornitura di autenticazione di utenti afferenti ad eventuali altre federazioni o accordi di circolarità anagrafica stipulati dall'afferente a meno di approvazione esplicita da parte comitato tecnico;
- l'afferente s'impegna a consentire l'accesso, per gli utenti che utilizzano la propria infrastruttura, al sito web dell'IX-Wi-Fi dove saranno riportate le istruzioni necessarie all'utilizzo del roaming (cfr. "Compiti del personale tecnico dell'IX-WiFi");
- l'afferente dovrà disporre di un servizio di supporto ai propri utenti (via e-mail e/o numero telefonico), e si impegnerà a rispondere a richieste di supporto da parte di utenti di altri enti federati che abbiano problemi ad autenticarsi presso la propria infrastruttura (cfr. "Procedure per il supporto utenti e la segnalazione dei guasti");

- i costi d'interconnessione tra la sede dell'IX-WiFi e la sede dell'afferente sono a totale carico dell'afferente stesso;
- l'ente afferente s'impegna ad utilizzare canali di comunicazione sicuri per la condivisione delle chiavi di cifratura o di altri dati sensibili;
- gli afferenti devono comunicare e tenere aggiornato il nominativo di un referente amministrativo, un referente tecnico ed un NOC con un numero di telefono per le emergenze. Di tali referenti dovrà essere comunicato il nome, la figura professionale all'interno dell'afferente, un telefono ed un indirizzo di e-mail. Gli afferenti dovranno inoltre comunicare un indirizzo e-mail che l'IX-WiFi userà per le comunicazioni ufficiali. Tali numeri dovranno essere considerati riservati alle comunicazioni tra afferenti e non dovranno essere comunicati agli utenti finali;
- l'afferente sarà invitato a partecipare, nella figura del referente amministrativo e/o tecnico, alle riunioni periodiche della federazione, che saranno comunicate dal comitato tecnico con un preavviso minimo di 15 gg. Tali riunioni potranno avvenire in audio/videoconferenza, secondo le modalità stabilite dal comitato tecnico;
- non è consentito all'afferente la cessione del presente accordo di federazione a terze parti a meno di un assenso specifico da parte del comitato tecnico dell' IX-WiFi;
- l'attività degli afferenti presso l'IX-WiFi non dovrà essere in contrasto con le vigenti leggi italiane o europee.

Regole tecniche per l'installazione e la configurazione

Aspetti generali

L'entità che intenda partecipare alla federazione di reti Wi-Fi dovrà collegarsi all'IX-WiFi mediante l'utilizzo del proprio proxy RADIUS.

L'IX-WiFi procederà alla configurazione opportuna del proprio proxy RADIUS, per inoltrare le richieste di autenticazione, provenienti dai RADIUS server delle altre realtà federate, verso il RADIUS server di ogni nuova entità afferente.

Modalità di Federazione

La federazione è realizzata mediante utilizzo del proxy RADIUS messo a disposizione dall'IX-WiFi che consente all'afferente l'utilizzo in "roaming" delle infrastrutture Wi-Fi delle altre entità federate.

A ogni afferente verrà assegnato dall'IX-WiFi un "realm" che permetterà, attraverso l'attributo "User-Realm" (di tipo stringa e codice dizionario RADIUS pari a 223) di identificare i suoi utenti quando richiederanno l'autenticazione presso altri enti federati. L'entità afferente è tenuta:

- a implementare e mantenere un server RADIUS in grado di contattare (secondo le modalità riportate in seguito) il proxy RADIUS dell'IX-WiFi;
- a dirigere le richieste di autenticazione relative ad utenze delle altre entità federate in "roaming" presso l'entità stessa verso il proxy RADIUS dell'IX-WiFi, specificando in esse l'attributo *User-Realm* con valore pari al **<realmente federato>, dell'entità cui l'utente appartiene, assegnato dall'IX-WiFi**;
- ad utilizzare, nei pacchetti RADIUS di tipo Access-Request diretti verso il proxy RADIUS dell'IX-WiFi e relativi ad utenze non appartenenti al proprio dominio, l'attributo RADIUS *User-Name* nella seguente forma:

  <utente>@<realm ente federato>

- ad implementare e mantenere un server RADIUS in grado di essere contattato (secondo le modalità riportate in seguito) dal proxy RADIUS dell'IX-WiFi;
- ad utilizzare **esclusivamente** PAP come schema di autenticazione per le richieste di RADIUS dirette verso l'IX-WiFi;

  ad accettare e processare opportunamente le richieste di autenticazione provenienti dal proxy RADIUS dell'IX-WiFi relative a proprie utenze in "roaming" presso altre entità federate e che utilizzeranno PAP come schema di autenticazione.

La connettività tra il server RADIUS dell'ente federato e il proxy RADIUS dell'IX-WiFi dovrà essere tale da garantire l'integrità e la riservatezza delle informazioni in transito e potrà realizzarsi almeno con le seguenti modalità:

- VPN Layer 2;
- VPN Layer 3;
- circuiti dedicati.

È compito dell'afferente provvedere al materiale necessario e all'installazione di eventuali propri apparati presso la sede del punto di interconnessione finalizzati all'implementazione dell'infrastruttura necessaria alla protezione delle comunicazioni inerenti l'autenticazione RADIUS.
Sono disponibili per il collegamento verso il proxy RADIUS porte Ethernet 10/100 Mbps RJ45.

L'entità afferente è tenuta inoltre a:

- adottare per le comunicazioni d'autenticazione RADIUS esclusivamente i port UDP assegnati dall'IX-WiFi;
- adottare l'indirizzamento IP privato assegnato dall'IX-WiFi (laddove applicabile) dal quale perverranno le richieste di autenticazione delle utenze di altre entità federate in "roaming" presso l'entità stessa ovvero al quale saranno destinate le richieste di autenticazione dei propri utenti in "roaming" presso le altre entità federate.

Compiti del personale tecnico dell'IX-WiFi

Il personale tecnico dell'IX-WiFi ha il compito di:

- mantenere nella migliore efficienza possibile il proxy RADIUS;
- intervenire nel caso di malfunzionamento del proxy RADIUS;

- apporre e tenere aggiornate le etichette relative ai cavi di connessione tra gli apparati dell'afferente e l'apparato del centro stella del punto di interconnessione (laddove applicabile);

Il personale tecnico dell'IX-WiFi ha inoltre l'obbligo di informare i referenti tecnici degli afferenti circa interventi di manutenzione ordinaria o straordinaria. La comunicazione per interventi di manutenzione programmati avverrà via e-mail almeno 7 giorni prima dell'intervento.

Il personale tecnico dell'IX-WiFi s'impegna a gestire un sito web all'interno del quale saranno tenute aggiornate alcune informazioni di carattere tecnico.

- Nella parte pubblica del sito:
    - notifiche sulla manutenzione ed eventuali interventi programmati;
    - informazioni istituzionali, copia dell'accordo e del regolamento tecnico;
    - informazioni tecniche di dettaglio, user guide, FAQ;
    - livelli minimi di servizio.
- In una parte del sito ad accesso riservato:
    - tutte le informazioni di carattere tecnico relative all'infrastruttura utilizzata per la federazione ad esclusione di quelle strettamente riservate (quali ad esempio le chiavi di cifratura);
    - informazioni statistiche e di monitoraggio di utilità per gli afferenti (quali ad esempio il volume delle autenticazioni RADIUS), e relativi grafici;
    - la lista dei referenti tecnici e NOC dei singoli afferenti.

Il sito web fornirà inoltre a ogni afferente uno spazio per la pubblicazione delle proprie politiche di accesso alla rete garantiti agli utenti in roaming. Tali politiche saranno visibili nella parte privata del sito.

Il personale tecnico dell'IX-WiFi fornirà un indirizzo e-mail e un numero telefonico per richieste di supporto da parte degli enti federati. Tali contatti dovranno ritenersi riservati e non essere comunicati agli utenti finali.

Procedure per il supporto utenti e la segnalazione dei guasti

L'utente dell'ente federato “A” che incontri dei problemi ad autenticarsi presso l'ente federato “B” dovrà rivolgersi al servizio di supporto dell'ente federato “B”.

L'ente federato “B” diventerà “owner” della chiamata di supporto e sarà l'unico ad interagire con l'utente richiedente. Ove necessario, l'ente federato “B” si rivolgerà al personale tecnico dell'IX-WiFi o dell'ente federato “A” per individuare il problema e sollecitarne la soluzione.

Violazione del presente regolamento

Il Comitato Tecnico e il personale tecnico dell’IX-WiFi si riservano il diritto di chiedere agli afferenti evidenza del rispetto del presente regolamento.

In caso di violazione del presente regolamento da parte di un afferente, l’IX-WiFi manderà dei richiami formali ai contatti tecnici dell’afferente. Al persistere o al ripetersi della situazione, l’IX-WiFi si riserva di sottoporre il caso al Comitato Tecnico che lo valuterà e deciderà se adottare ulteriori misure.

In caso di grave violazione del presente regolamento, l’IX-WiFi si riserva di intervenire nel modo che riterrà più opportuno per porvi rimedio.

Normativa di riferimento

- Delibera AGCOM 26 novembre 2008 666/08/CONS Regolamento per l’organizzazione e la tenuta del registro degli operatori di comunicazione;
- Decreto Ministeriale (Gasparri) 28 Maggio 2003 Condizioni per il rilascio delle autorizzazioni generali per la fornitura al pubblico dell'accesso Radio-LAN alle reti e ai servizi di telecomunicazioni;

- Decreto Ministeriale (Landolfi) 4 ottobre 2005, Condizioni per il rilascio delle autorizzazioni generali per la fornitura al pubblico dell'accesso radio LAN alla rete e ai servizi di telecomunicazioni;

- Decreto Legge 27 luglio 2005 n.144 Misure urgenti per il contrasto del terrorismo internazionale;

- Decreto Legislativo 30 giugno 2003 n. 196 Codice in materia di protezione dei dati personali, e s.m.i.;
- Decreto Legislativo 1 agosto 2003 n. 259/2003 Codice delle comunicazioni elettroniche, e s.m.i.;

- Decreto Legislativo 30 maggio 2008 n. 109, "Attuazione della direttiva 2006/24/CE riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE";

- Legge 31 luglio 2005, n. 155, Conversione in legge, con modificazioni, del decreto-legge 27 luglio 2005, n. 144, recante misure urgenti per il contrasto del terrorismo internazionale, e s.m.i.;

- Con riferimento alle modalità di accesso Wi-Fi in ambito pubblico e alle misure relative all'identificazione dell'utente si specifica che, con nota del 27 novembre 2007, il Ministero dell'interno – dipartimento della pubblica sicurezza ha ritenuto che per soddisfare i requisiti della norma vigente (decreto legislativo n. 144/05 convertito con modificazioni con legge n. 155/05) sia sufficiente l'utilizzo di una SIM/USIM, quale mezzo per attivare le procedure necessarie a ottenere le credenziali di accesso alla rete, in quanto consente l'identificazione seppur indiretta dell'utente. Il Ministero ha ulteriormente precisato che è comunque necessario che la messaggeria sia veicolata attraverso una carta SIM/USIM rilasciata all'utente nel rispetto delle disposizioni, relative all'identificazione dell'utente, stabilite dall'art. 55 del decreto Legislativo n. 259/03, con conseguente esclusione delle SIM/USIM rilasciate da Paesi stranieri.