Universidad Zaragoza
1542

Trabajo Fin de Grado

Diseño, planificación y despliegue de una red Wifi pública en el municipio de Alustante (Guadalajara).

Autor

Daniel López Isarría

Director

Fernando Gutiérrez Soler

Escuela de Ingeniería y Arquitectura
Grado en Ingeniería y servicios de telecomunicación

2015

TRABAJOS DE FIN DE GRADO / FIN DE MÁSTER

Escuela de Ingeniería y Arquitectura Universidad Zaragoza

DECLARACIÓN DE AUTORÍA Y ORIGINALIDAD

(Este documento debe acompañar al Trabajo Fin de Grado (TFG)/Trabajo Fin de Máster (TFM) cuando sea depositado para su evaluación).

D./Dª. Daniel López Isarría,

con nº de DNI 73003890G en aplicación de lo dispuesto en el art. 14 (Derechos de autor) del Acuerdo de 11 de septiembre de 2014, del Consejo de Gobierno, por el que se aprueba el Reglamento de los TFG y TFM de la Universidad de Zaragoza,

Declaro que el presente Trabajo de Fin de (Grado/Máster) Grado, (Título del Trabajo) Diseño, planificación y despliegue de una red Wifi pública en el municipio de Alustante (Guadalajara).

es de mi autoría y es original, no habiéndose utilizado fuente sin ser citada debidamente.

Zaragoza, 23 de septiembre de 2015

Fdo:

RESUMEN DEL TRABAJO DE FIN DE GRADO

Diseño, planificación y despliegue de una red Wifi pública en el municipio de Alustante (Guadalajara).

Autor: Daniel López Isarría.

Director: Fernando Gutiérrez Soler.

En este trabajo de fin de grado se ha dado solución al problema actual de un municipio de Guadalajara, por la falta de cobertura 3G en la zona, mediante la incorporación de una red Wifi.
Partiendo de las bases legales y las capacidades físicas de la red, se ha diseñado un sistema capaz de dar servicio Wifi para que los usuarios puedan disponer de conexión a internet.

Para el correcto cumplimiento de la legalidad, ha sido necesario el análisis, la configuración y la instalación de dos servidores que hacen de portal cautivo, servidor web y base de datos y que permiten el registro y el control de los usuarios por parte del personal del consistorio. Además, se ha llevado a cabo el desarrollo web de las páginas que el servidor web ofrece.

La señal se transmite vía aire, mediante tecnología Wifi, por lo que han sido necesarios equipos con características específicas, para realizar una conexión correcta entre equipos y usuarios de la red. Se han estudiado las limitaciones físicas de los equipos tanto teórica como empíricamente y se ha llevado a cabo la instalación de la red, con la colaboración de operarios cualificados.

Una vez desplegado el sistema, se han hecho pruebas y se ha solicitado información a clientes y usuarios para mejorar este en la medida de lo posible, también, se ha enseñado al cliente a hacer un uso efectivo del sistema y se han puesto en marcha las medidas necesarias para un mantenimiento correcto del sistema, además de analizar las posibles líneas futuras para proyectos similares.

Se han calculado los costes que una red de este tipo conlleva y se han calculado las horas de trabajo necesarias para llevarla a cabo.

Por último, concluye con los beneficios que este TFG ha aportado al estudiante, valorando lo aprendido a lo largo del trabajo.

Índice de contenido

Capítulo 1: Introducción **5**

1.1 Motivación 5
1.2 Objetivos 6
1.3 Organización de la memoria 7

Capítulo 2: Análisis y diseño de la red **8**

2.1 Situación geográfica 8
2.2 Aspectos administrativos y legales 8
2.2.1 Boletín Oficial del Estado 9
2.2.2 Ley Orgánica de Protección de Datos 9
2.2.3 Real Decreto Legislativo 3/2011 10
2.3 Estándar IEEE 802.11 10
2.4 Parámetros radio teóricos 11
2.4.1 Enlaces punto a punto 11
2.4.2 Enlaces punto a zona 12
2.5 Ethernet 15
2.6 Elección de emplazamientos 15
2.7 Elección de equipos Wifi 17
2.7.1 Antenas omnidireccionales 17
2.7.2 Antenas sectoriales 18
2.7.3 Antenas parabólicas 18
2.8 Diseño del sistema a desarrollar 19
2.8.1 Portal Cautivo 19
2.8.2 Elección del Servidor Web 20
2.8.3 Elección de la Base de Datos 20
2.8.4 Sistema Operativo 20
2.8.5 Entorno de desarrollo integrado 21

Capítulo 3: Despliegue y configuración **22**

3.1 Características técnicas reales 22
3.2 Topología de la red 24
3.3 Configuración de las antenas 24
3.4 Instalación de las antenas 28
3.5 Configuración del portal cautivo pfSense 32
3.5.1 Dinamic Host Configuration Protocol (DHCP) 33
3.5.2 Routing 34
3.5.3 Firewall 35
3.5.4 Portal cautivo 36
3.5.5 FreeRadius 37
3.5.6 Cron 37
3.6 Configuración del servidor web y base de datos 38
3.6.1 Tomcat7 38
3.6.2 PostgreSQL y pgAdmin 40
3.7 Desarrollo web 42
3.7.1 Maven 42
3.7.2 Bootstrap 43
3.7.3 Diseño final de la Web 44

Capítulo 4: Pruebas, mantenimiento y líneas futuras **46**

4.1 Pruebas 46
4.1.1 Medidas de cobertura 46
4.1.2 Pruebas del sistema 46
4.1.3 Feedback 46
4.2 Mantenimiento 47
4.2.1 Formación y ayuda al cliente 47
4.2.2 Control remoto: TeamViewer 47
4.2.3 Control remoto: PuTTY 47
4.2.4 Copias de seguridad 48
4.2.5 Afluencia de usuarios 48
4.3 Líneas futuras 48

Capítulo 5: Cálculo de costes **49**

5.1 Coste en recursos humanos 49

5.2 Coste de equipos y cableado 49

5.3 Coste de otros materiales 50

Capítulo 6: Conclusión **51**

Beneficios personales del TFG 51

Bibliografía **52**

Capítulo 1.

Introducción.

El actual despliegue de redes inalámbricas es muy importante para el desarrollo de las tecnologías de la información y de la comunicación, sin embargo, sigue habiendo gran parte de la población a la que el acceso a estas redes se le hace imposible por su situación geográfica.

Así, Alustante, un pequeño municipio de la provincia de Guadalajara, en un intento por satisfacer las necesidades de acceso a la red por parte de sus habitantes, ha decidido consultar la posibilidad de instalar una red Wifi con la que dar un servicio de acceso a internet.

La problemática surge por la falta de cobertura 3G en el municipio y la falta de voluntad por parte de las operadoras para ofrecer este servicio a poblaciones pequeñas en los que no están obligadas a dar este tipo de cobertura si ya llega banda ancha u otro tipo de conexión, como WiMAX o conexión por satélite.
Por lo que la población acaba pagando una cuota muy alta por una conexión de mala calidad, si lo comparamos con las conexiones que se pueden contratar en municipios con un mayor número de habitantes.

Esto supone que en Alustante y Motos, pedanía de Alustante, haya que desplazarse a la biblioteca o al bar, para poder tener acceso a internet gratuitamente desde su dispositivo portátil, lo que para los vecinos de Motos supone un gasto en desplazamiento añadido, ya que esta pedanía se encuentra a 6 km de distancia y no dispone de cobertura 2G, 3G, ni banda ancha, por lo que están prácticamente incomunicados en cuanto a servicios de internet y cobertura telefónica se refiere.

El ayuntamiento de Alustante dispone de conexión a internet de banda ancha, y se pretende prestar parte de esta para el uso público. Es por ello que se van a buscar y desarrollar las soluciones que mejor se adapten al servicio actual, a la situación del consistorio y a la problemática actual, siguiendo siempre ciertas condiciones y requisitos.

1.1 Motivación.

Este TFG se dirige a dar soluciones prácticas a la hora de intentar solventar la carencia de cobertura 3G mediante una conexión inalámbrica en una población determinada. También es una oportunidad para abordar un primer trabajo de ingeniería fuera del ámbito académico.

Variables como la topografía, la población, el servicio que se pretende prestar, el ámbito legal a respetar, los recursos económicos disponibles y otros factores marcarán las pautas a seguir a la hora de gestionar el despliegue de la red.

Para llevar a cabo este trabajo se ha contado con la colaboración del ayuntamiento de Alustante, que ha sido el solicitante del servicio y el que debe valorar las soluciones aportadas y que ha prestado su ayuda de manera desinteresada colaborando y dándonos libertad para desplegar los distintos dispositivos del sistema.

1.2 Objetivos.

El objetivo general del presente trabajo es diseñar una red basada en la tecnología IEEE 802.11 (Wifi) que de solución a las necesidades planteadas por el municipio.
Comenzando por definir los servicios que se pueden prestar en estas frecuencias de manera legal, así como gestionar los procesos y notificaciones a la CNMC.
Se seleccionarán los emplazamientos más oportunos para colocar las estaciones emisoras, las necesidades reales de los alustantinos y la forma de gestionarlas con un servidor central, además, hay que llevarlas a cabo de manera efectiva y con los menores costes para el ayuntamiento, que al tratarse de un municipio pequeño, cuenta con pocos recursos para financiarla.

Para conseguir el objetivo final ya comentado el estudio ha de seguir una serie de fases, consecutivas en el tiempo, que se van a describir a continuación.

- Establecer el alcance de nuestro proyecto, que además de las limitaciones físicas, también tendrá limitaciones legales y hacer un presupuesto aproximado de las obras a realizar.

- En base a la legalidad, informar a la CNMC de los cambios que realizara el ayuntamiento de Alustante como operador. Explicar el servicio que se va a prestar y las limitaciones que va a tener.

- Valorar y seleccionar los equipos a instalar y software a desarrollar, calcular costes en función de los dispositivos seleccionados.

- Configurar dichos dispositivos y probar su correcto funcionamiento, realizando distintas pruebas. Podemos diferenciar por un lado las antenas que se encargarán de repartir la señal y por el otro, el servidor central, que hará las labores de gestión del tráfico.

- Instalar las antenas en sus correspondientes emplazamientos con la configuración establecida, con sus correspondientes pruebas y modificar lo que se crea necesario.

- El servidor central deberá ser configurado para gestionar el tráfico de la red, para ello se seleccionará un software que realizará diversas tareas:

    - Dará servicio Dinamic Host Configuration Protocol (DHCP) a los usuarios dentro de una red local para gestionar el nivel de IP.

    - Deberá incorporar un portal cautivo que permita la validación de usuarios por parte del personal del consistorio, debiendo configurar una entrada sencilla para la indexación de clientes.

    - A su vez, se deberá crear una interfaz de usuario para el inicio de sesión y el registro, para que el servidor pueda darle los servicios que le correspondan.

    - Además, deberá guardar un registro con los datos de los usuarios y las conexiones realizadas.

- Se realizarán pruebas para comprobar el correcto funcionamiento de los dispositivos y para comprobar que hay una señal suficientemente valida dentro del municipio.

- Por otro lado, se explicará a las personas encargadas del registro como hacerlo, haciendo la interfaz lo más amigable posible para evitar problemas futuros.

- Se hará una valoración del mantenimiento que hay que llevar a cabo.

- Servicios futuros que se podrán prestar a los habitantes del municipio.

1.3 Estructura de la memoria.

La memoria es un único bloque, que a su vez está dividido en los siguientes capítulos:

- **Introducción y objetivos:**
  En esta primera parte se explica la problemática y necesidades de la que ha surgido la motivación que ha llevado a la elaboración de este TFG y los objetivos que pretende abordar.

- **Análisis y diseño**
  Justifica el camino seguido para la elaboración de este TFG, también se describe el diseño del sistema.

- **Despliegue y configuración**
  Describe de forma detallada todo el trabajo realizado para la implementación del sistema.

- **Pruebas, mantenimiento y líneas futuras:**
  Analiza la comprobación del funcionamiento de la red, así como el mantenimiento que conlleva y las posibles mejoras que podría tener el sistema realizado.

- **Cálculo de costes:**
  Se calcula, de forma aproximada, el coste total, tanto humano como material.

- **Conclusión:**
  Se realiza una reflexión sobre lo aprendido durante la elaboración de este TFG.

Capítulo 2: Análisis y diseño.

Este capítulo engloba todo lo relacionado con la estructura física y lógica del sistema que se va a desarrollar. Una vez considerado el entorno y el ámbito de nuestro proyecto, se establecerán los requisitos necesarios de la red y los medios necesarios para llevar a cabo el proyecto, exponiendo los motivos de las elecciones de los distintos elementos del sistema.

2.1 Situación geográfica.

Alustante (40°36’59”N 1°39’27”O) es un municipio de la provincia de Guadalajara con un censo de 186 habitantes en 2014.
Desde 1970, Motos (40°35’32”N 1°36’45”O) es pedanía de Alustante y por ley, las pedanías deben tener el mismo tipo de servicios y de la misma calidad que el municipio del que dependen. Motos se encuentra a 6 km de Alustante por carretera. Por lo tanto, tendremos que enfocar nuestro proyecto en dar cobertura Wifi de la manera más eficiente a ambas poblaciones.

Figura 1: Mapa geográfico con la situación de Alustante y Motos.

2.2 Aspectos administrativos y legales.

Antes de comenzar a buscar las mejores soluciones para el proyecto que se va a llevar a cabo, es de suma importancia informarse acerca de la situación legal de la tecnología Wifi en España, ya que esta determinará las limitaciones de la red. La Agencia Estatal Boletín Oficial del Estado es la encargada de la edición, impresión, publicación y difusión del Boletín Oficial del Estado. En el cual se publican las nuevas normativas y leyes, así como las modificaciones de estas.

2.2.1 Boletín Oficial del Estado.

Como podemos leer en el BOE de septiembre de 2010 [1], que es el que nos afecta en este caso, hay unas normas a seguir cuando llevamos a cabo el despliegue de redes de telecomunicaciones. Aunque cada vez surgen nuevas redes de este tipo y cada una enfocada a dar distintos servicios por lo que la CNMC intenta ajustar esos casos a la legalidad, ya que existen intereses cruzados entre proveedores de internet, administraciones y usuarios.

En este caso y de manera provisional, el ayuntamiento de Alustante quiere dar un servicio de internet gratuito para sus convecinos y que por lo tanto no afecte a la libre competencia.

Para este tipo de redes, el BOE de septiembre de 2010, resuelve que la operadora, en este caso, la administración pública debe:

- Notificar a la CNMC del servicio que se va a prestar e inscribirse en el registro de operadores.
- Limitar la velocidad máxima del acceso a internet a 256 kbps.
- Restringir el acceso al servicio dentro de las viviendas y al sector terciario.
- Conservar los datos de comunicación electrónica durante al menos un año.
- Respetar la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal (LOPD), así como respetar el secreto de las comunicaciones.

La documentación necesaria que hay que rellenar y enviar a la CNMC se encuentra en su web[2]. El ayuntamiento de Alustante ya está dado de alta como operador, por lo que solo habrá que modificar su situación.

El resto de condiciones afectarán a la configuración final del sistema y deberemos tenerlas en cuenta a la hora de configurar ciertos parámetros de la red.

2.2.2 Ley Orgánica de Protección de Datos [3].

Esta ley, compuesta por 26 artículos, tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas.

Esto lo lleva a cabo regulando el tratamiento de los ficheros con datos de carácter personal, también se incluyen los ficheros ordenados en papel. Quedan excluidas de esta normativa aquellos datos recogidos para uso doméstico o a los ficheros que solo contengan datos de empresa.

Como responsables del sistema la LOPD nos obliga a tener por escrito todas las medidas de seguridad del sistema, indicando las funciones y obligaciones del personal y los usuarios, así como el personal autorizado. También debemos especificar qué permisos de acceso tiene cada usuario.

Además, la LOPD obliga a evitar en la mayor medida posible las pérdidas de información llevando a cabo copias de seguridad una vez a la semana como mínimo, así como a llevar un

registro con los accesos de cada usuario con fecha, hora y si el usuario a tenido éxito o no al iniciar sesión. Ambos ficheros, deberán tener además una copia de seguridad en otra localización.

Debemos seguir los principios de confidencialidad y consentimiento por parte de los usuarios, que nos deberán ceder los datos de forma voluntaria Los usuarios tienen derecho a la consulta, rectificación y cancelación de sus datos, pudiendo impugnar y solicitar indemnizaciones si estos son usados de forma indebida.

2.2.3 Real Decreto Legislativo 3/2011 [4].

Es el decreto a tener en cuenta a la hora de realizar contratos por parte de la administración pública. La contratación del sector público debe ajustarse a los principios de libertad de acceso a las licitaciones, publicidad y transparencia de los procedimientos, no discriminación e igualdad de trato entre los candidatos. En el contrato hay dos partes: el órgano de contratación y el contratista.

El órgano de contratación es el órgano unipersonal o colegiado que tiene la necesidad de seleccionar a una persona física o jurídica para que ejecute una obra, preste un servicio o suministre un bien y que, con esta finalidad, inicia el procedimiento de contratación y adjudica el contrato.

Mientras que el contratista pueden ser las personas naturales o jurídicas, que tengan plena capacidad de obrar, que no estén incursas en prohibición de contratar. Asimismo, los empresarios deben contar con la habilitación empresarial o profesional que sea exigible para realizar la actividad.

Los contratos menores pueden adjudicarse directamente a cualquier persona con capacidad de obrar y que cuente con la habilitación profesional necesaria para realizar la prestación. Por eso, en este caso pueden licitar un proyecto sin sacar este a concurso ya que su presupuesto es inferior a 12000 €, así que este proyecto es licito y por lo tanto viable.

2.3 Estándar IEEE 802.11

Para conseguir los objetivos planteados en el proyecto, se ha decidido usar el IEEE 802.11 como tecnología para el acceso radio de los usuarios. Se trata de un estándar del Institute of Electrical and Electronics Engineers (IEEE), que es una asociación mundial de técnicos e ingenieros dedicada a la estandarización y el desarrollo en áreas técnicas. Es la asociación internacional, sin ánimo de lucro, más grande del mundo formada por profesionales de las nuevas tecnologías. El estándar IEEE 802.11 define los dos niveles inferiores de la capa OSI, es decir, la capa física y la de enlace de datos, siendo el aíre, el medio de propagación para el nivel físico.

La versión original del IEEE 802.11 fue publicada en 1997. A día de hoy, son tres las versiones del 802.11 más aceptadas entre fabricantes y las más relevantes para nuestro servicio, estas son la IEEE 802.11 b, IEEE 802.11 g y la IEEE 802.11 n.

El IEEE 802.11 b fue ratificado en 1999, esta tiene una velocidad máxima de transmisión de 11 Mbit/s, funciona en la banda de 2,4 GHz y utiliza el método de acceso original en el primer

estándar, CSMA/CD. En 2003 fue publicado el tercer estándar de modulación: 802.11g, funciona en la misma banda pero opera a una velocidad teórica máxima de 54 Mbit/s. Es compatible y puede coexistir con la versión IEEE 802.11 b aunque la presencia de nodos que operan con la IEEE 802.11 b ralentizan el funcionamiento de esta.

El estándar IEEE 802.11 n es el más reciente, siendo ratificado en 2009 con una velocidad de hasta 600 Mbit/s en capa física. En esta versión se hace uso simultaneo de la banda de 2,4 GHz y la de 5 GHz además de contar con la tecnología MIMO (Multiple Input – Multiple Output), que permite enviar y recibir datos con varias antenas a la vez y sin crear interferencias ni colisiones. A diferencia de otras versiones de Wi-Fi, 802.11n es compatible con dispositivos basados en todas las ediciones anteriores de Wi-Fi.

Por lo tanto, procuraremos que los equipos instalemos cumplan estos estándares, que son los más utilizados hoy en día para redes sin cables en áreas pequeñas.

2.4 Parámetros radio teóricos.

Podemos comprobar mediante modelos teóricos los límites físicos de nuestra red a partir de los parámetros establecidos en el estándar IEEE 802.11. El factor determinante a la hora de seleccionar las distintas antenas es la atenuación en el medio, que la calcularemos en función de la potencia recibida.

$$P_r = P_e + G_e + G_r - L_M \quad [1]$$

Siendo:
P_r: Potencia recibida (dB).
P_e: Potencia emitida (dB).
G_e: Ganancia del emisor (dBi).
G_r: Ganancia del receptor (dBi).
L_M: Perdidas en el medio (dBi).

Actualmente la Potencia Isotrópica Radiada Equivalente PIRE máximo en España está limitada a 100 mW, esto es debido a las posibles interferencias que puedan crear entre las propias señales, por lo que:

$$P_e + G_e = PIRE = 20\ dBm \quad [2]$$

Mientras que la ganancia de las antenas receptoras variará en función de la antena receptora. Para una ganancia constante, será la potencia recibida mínima necesaria la que limite las perdidas en el medio.

$$L_M = PIRE + G_r - P_r = 20dBm - P_{r\,min} \quad [3]$$

Para las perdidas en el medio, podemos diferenciar los enlaces punto a punto de los enlaces punto a zona. En ambos casos habrá pérdidas al transmitir por el aire, pero en los enlaces punto a zona tendremos que añadir otras pérdidas debidas al entorno.

2.4.1 Enlaces punto a punto.

Teniendo en cuenta que las pérdidas en espacio libre se pueden expresar como:

$$L_{EL} = 20\log\left(\frac{4\pi d}{\lambda}\right) = 20\log\left(\frac{4\pi}{\lambda}\right) + 20\log d = 20\log d + 40\ dB \quad [4]$$

Siendo:
λ: Longitud de onda (m).
d: Distancia (m).

Para frecuencias de 2.4 GHz: $$\lambda = \frac{c}{f} = 0.125\ m$$ [5]

f:Frecuencia (Hz).

Por lo que podemos calcular la distancia máxima en función de la sensibilidad de la antena receptora.

$$d = 10^{\left(\frac{-P_r - 20}{20}\right)}$$ [6]

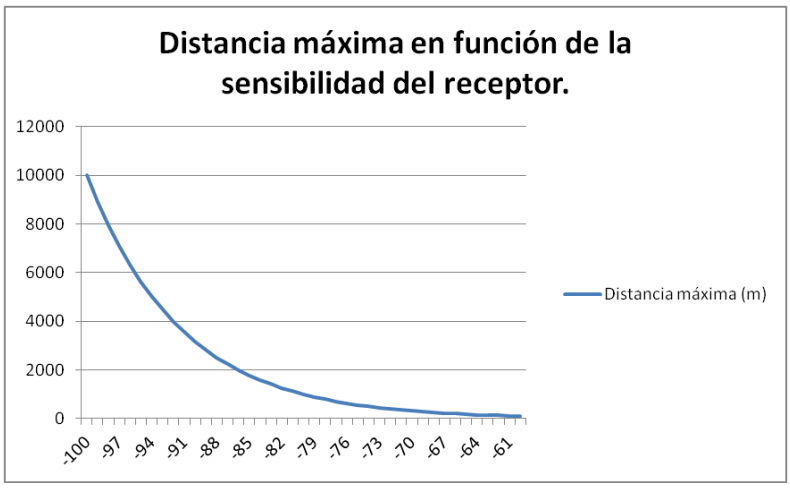

Figura 2: Gráfica de la distancia máxima en función del receptor.

2.4.2 Enlaces punto a zona.

Para este tipo de enlaces tendremos que tener en cuenta otros factores además de las pérdidas en el espacio libre. Aunque dependiendo de las posiciones de los equipos, cada conexión tendrá unas pérdidas distintas, estas se pueden aproximar a un valor medio determinado por el método elegido.

El modelo SUI (Stanford University Interim). Este modelo añade factores de corrección a las pérdidas en espacio libre para zonas con terrenos sin edificios, es el recomendado por el IEEE 802.16 para el cálculo de la perdida básica de propagación en sistemas WiMAX:

$$L_M = L_{EL} + 10\gamma \log\left(\frac{d}{d_0}\right) + S$$ [7]

para $d > d_0$

Donde:
d: Distancia entre estación base y antena receptora (m).
d_0: 100m.
γ: es exponente del factor de pérdidas.
S: factor de corrección de sombra, representado por una distribución longnormal. Toma valores entre 8.2 y 10.6 dB

$$\gamma = a - b * h_b + \frac{c}{h_b}$$ [8]

Con:
h_b: la altura de la estación base (m). Entre 10m y 80m.
Las constantes a, b, y c dependen del tipo de terreno.

Los terrenos se clasifican en 3 tipos:

- Tipo A: "urbano" con densidad de arbolado moderada a densa.
  Pérdidas de propagación altas
- Tipo B: "suburbano" con densidad de arbolado baja o "flat terrain" con densidad de arbolado moderada a densa . Pérdidas de propagación intermedias.
- Tipo C: "rural" con densidad de arbolado baja. Pérdidas de propagación bajas.

Parámetro	Tipo A	Tipo B	Tipo C
a	4.6	4	3.6
b	0.0075	0.0065	0.005
c	12.6	17.1	20

Tabla 1: Tipos de terrenos y las constantes de cada uno.

Este es un modelo válido para f ~ 2GHz y hRx ~ 2 m., para otras frecuencias y otras alturas, se añaden factores de corrección:

$$L_{M,mod} = L_M + X_f + X_h \quad [9]$$

X_f : corrección para frec > 2GHz: $$X_f = 6\log_{10}\left(\frac{f}{2000}\right) \quad [10]$$

X_h : corrección para altura Rx: $$X_h = \begin{cases} -10.8\log_{10}\left(\frac{h_r}{2000}\right) & para\ tipo\ A\ y\ B \\ -20\log_{10}\left(\frac{h_r}{2000}\right) & para\ tipo\ C \end{cases} \quad [11]$$

En nuestro caso, supondremos un terreno del tipo B y calcularemos las perdidas en función de la distancia:

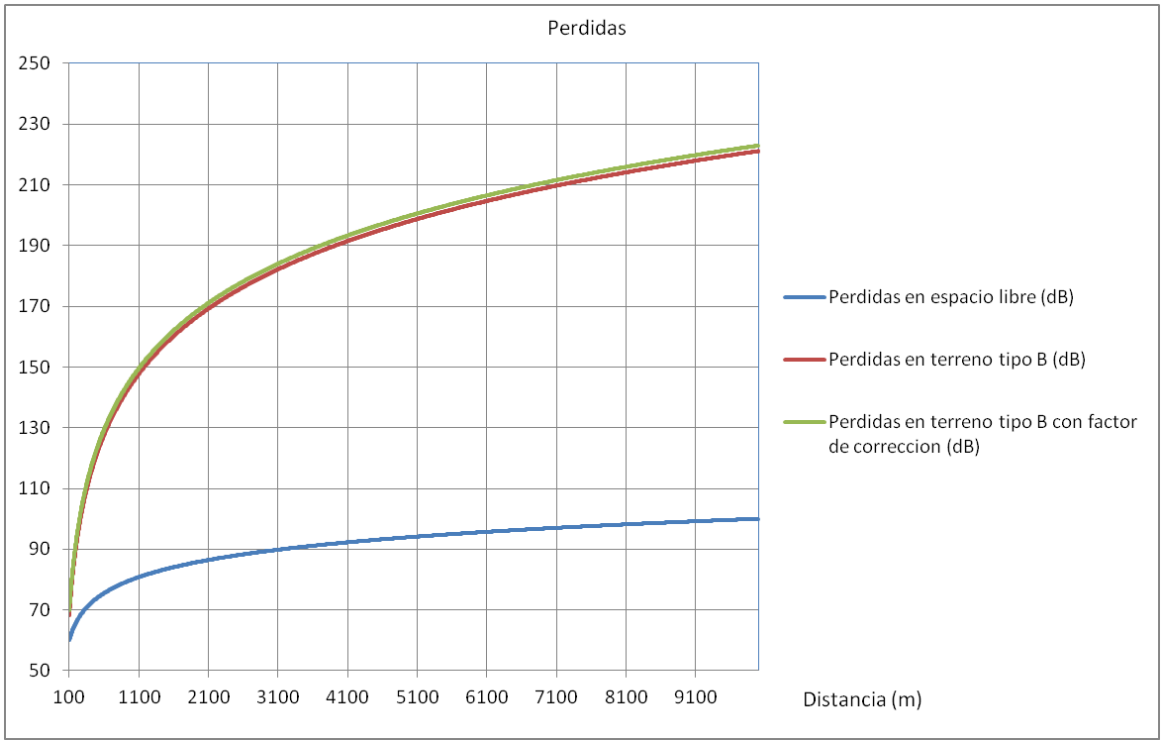

Figura 3: Comparativa de las pérdidas en función de la distancia, hasta 10000 metros.

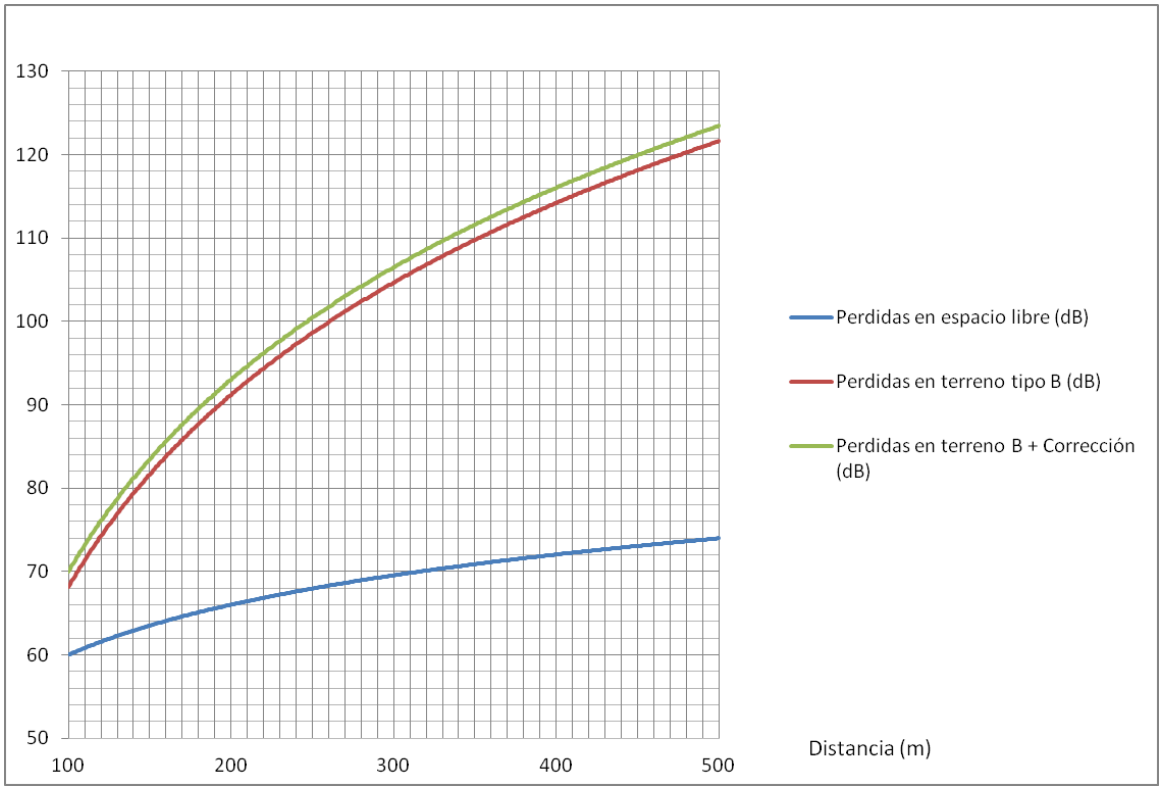

Figura 4: Comparativa de las pérdidas en función de la distancia, hasta 500 metros.

2.5 Ethernet.

Es el estándar referencia de redes de área local mediante acceso con escucha de portadora y detección de colisiones (CSMA/CD).
Ethernet define las características de cableado y los formatos de tramas de datos, el nivel físico y el de enlace del modelo OSI establecido por ISO, por lo que será el protocolo por defecto en las conexiones que realicemos mediante vía cobre.

La red Ethernet de 1973 ya tenía todas las características esenciales de la Ethernet actual. Robert Metcalfe presentó en ese año su tesis doctoral, donde exponía un protocolo que mejoraba sustancialmente el rendimiento Aloha.
Empleaba CSMA/CD para minimizar la probabilidad de colisión y activaba un mecanismo denominado retroceso exponencial binario para reducir la "agresividad" del emisor por acceder al medio. Tenía topología de bus y funcionaba a 2,94 Mb/s sobre un segmento de cable coaxial de 1,6 km de longitud. Las direcciones eran de 8 bits y el CRC de las tramas de 16 bits.

Actualmente se define en el estándar IEEE 802.3 y sus versiones han sido mejoradas, siendo 10-gigabit Ethernet (XGbE o 10GbE) el más reciente (año 2002) y más rápido de los estándares Ethernet. IEEE 802.3ae define una versión de Ethernet con una velocidad nominal de 10 Gbit/s, diez veces más rápido que gigabit Ethernet.
Los equipos utilizados para la realización del proyecto son todos compatibles con la versión Ethernet 100BaseT o superiores.

2.6 Elección de emplazamientos.

Se han seguido ciertos criterios para la elección de los emplazamientos, así, se ha elegido la colocación de las antenas en lugares públicos, con electricidad, separados una distancia razonable y con una altura suficiente para que tengan visión directa entre ellos y a su vez, la señal de cobertura lo mejor posible a las calles de los municipios. Además, se diferencia entre dos tipos de enlace:

- Punto a zona: para la accesibilidad de los usuarios.
- Punto a punto: para enlazar entre distintas zonas, repitiendo la señal necesaria para que la comunicación se lleve a cabo satisfactoriamente.

Dado que los municipios son pequeños y que son pocos emplazamientos, se decidió la posición de las antenas en base a una visita física, debido a la falta de lugares públicos, en algún caso se decidió colocarlas en casas de particulares. En Alustante los emplazamientos están en la Tabla 2 y en la Figura 5.

Nº Estación	Nombre	X(UTM)	Y(UTM)	Tipo de enlace	Altura
1	Ayuntamiento	613472	4496998	Punto a zona	10
1	Ayuntamiento	613472	4496998	Punto a punto	10
2	Plaza del Capricho	613364	4496899	Punto a zona	10
3	Frontón	613616	4496836	Punto a zona	15
4	Casa Particular	613400	4496776	Punto a zona	12
5	Guardia Civil	613735	4496530	Punto a zona	12

Tabla 2: Información referente a la localización de los emplazamientos elegidos.

En el siguiente plano se muestra de forma precisa la localización que tendrán las antenas, así como las conexiones que establecen entre ellas para llegar hasta el servidor central:

Figura 5: Mapa con los emplazamientos de las antenas y sus conexiones en Alustante.

La información sobre los emplazamientos en Motos puede verse en la Tabla 2 y la Figura 6.

Nº Estación	Nombre	X(UTM)	Y(UTM)	Radiación	Altura
1	Ermita	617115	4494296	Punto a zona	8
1	Ermita	617115	4494296	Punto a punto	8
2	Casa Particular II	617304	4494329	Punto a zona	10

Tabla 2: Información referente a la localización de los emplazamientos elegidos en Motos.

Figura 6: Mapa con los emplazamientos y las conexiones realizadas en Motos.

Las parabólicas se han situado de manera que tengan visión directa entre ellas, para eso, ha sido necesaria la instalación de la parabólica de Motos en lo alto de la ermita, situada en una loma colindante al pueblo, ya que es el punto más cercano a Motos con visión directa a Alustante.

Para comprobar la visibilidad, además de confirmarlo visualmente, se ha utilizado la herramienta de Google Earth [5](véase figura 7).

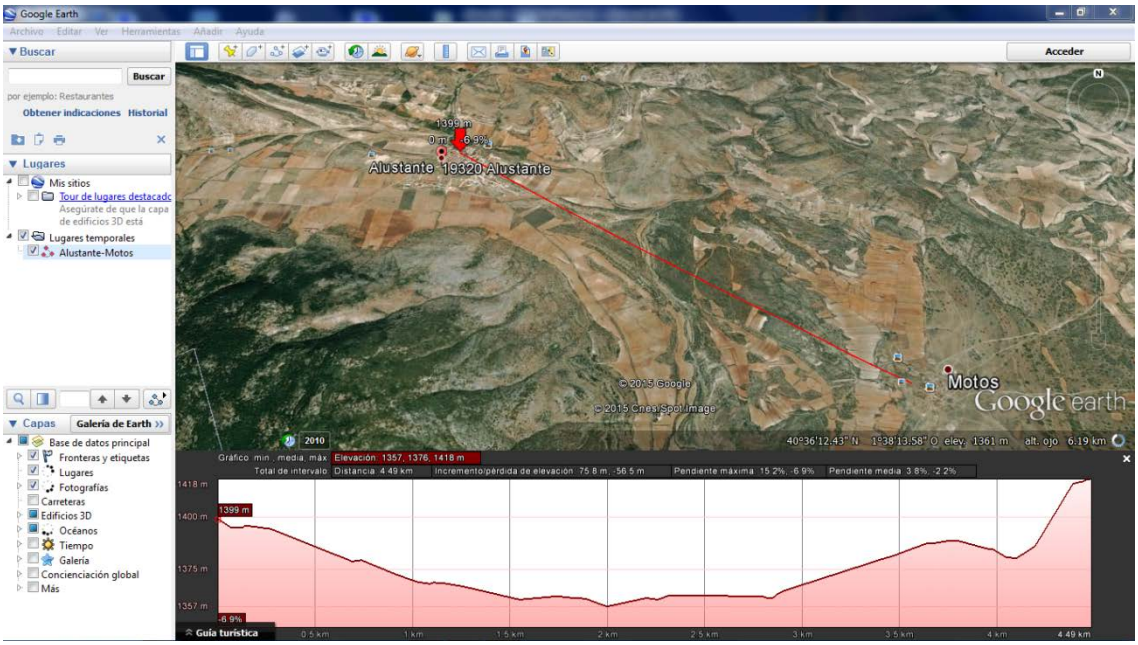

Figura 7: Distancia y elevación del terreno entre las antenas parabólicas de Alustante y Motos.

Como se puede ver en la imagen, las parabólicas no tendrán problemas en cuanto a difracción o anchos de Fresnel, porque se garantiza una visión directa. Además nos da la distancia aproximada de nuestro enlace, siendo esta de 4.5 km.

La instalación de la parabólica en la ermita ha llevado a colocar una antena sectorial en el mismo emplazamiento, así podremos conectar ambas directamente, sin apenas cableado intermedio.

2.7 Elección de equipos Wifi.

Dentro de la infinidad de fabricantes de este tipo de equipos, hay que buscar los que mejor se adapten a las necesidades reales del trabajo. Tienen que ser versátiles, potentes y económicos. Tras un proceso de búsqueda y debido a conocimientos previos de estos equipos, se ha elegido Ubiquiti como fabricante. Los equipos Ubiquiti responden perfectamente a las exigencias, tanto para las antenas omnidireccionales como las sectoriales y las parabólicas.

2.7.1 Antenas Omnidireccionales.

Las antenas omnidireccionales de Ubiquiti que trabajan a 2,4 GHz son las PicoStation M [6], son los equipos más utilizados a la hora de radiar, ya que son ideales para los enlaces punto a zona con los que se desea emitir señal constante en todas direcciones.

Pueden trabajar como Access Point o en modo puente, en cuyo caso, habrá que configurar con que MACs se pueden comunicar a la hora de repetir la señal. Son pequeñas y fáciles de instalar y configurar. Utilizadas principalmente para comunicaciones punto a zona.

Figura 8: Imagen de la PicoStation M de Ubiquiti.

2.7.2 Antenas sectoriales

Se trata de antenas con una amplitud angular relativa, en este caso, de unos 120º y están especialmente diseñadas para enlaces punto a zona ya que pueden comunicarse con una amplia zona espacial pero fijada en un sector concreto.
Para llevar a cabo el trabajo hemos seleccionado las NanoStationLoco M2 [7].

Figura 9: Imagen de la NanoStationLoco M2 de Ubiquiti.

2.7.3 Antenas parabólicas

Estas antenas son específicas para realizar comunicaciones punto a punto y poseen la ganancia suficiente para comunicar dos puntos alejados entre sí, ya que poseen una gran directividad y una apertura angular pequeña.
Se ha seleccionado las AirGrid M [8] para el trabajo, entre otros motivos, porque ofrecen una resistencia menor al viento, en comparación con las parabólicas de tipo plato.

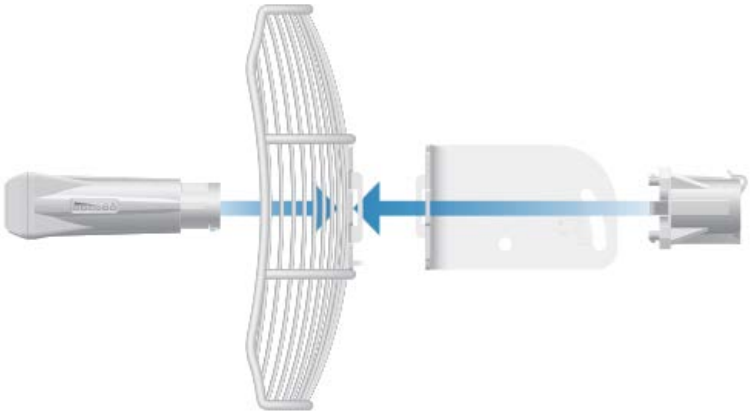

Figura 10: Imagen de la antena parábolica AirGrid M de Ubiquiti.

2.8 Diseño del sistema a desarrollar.

Además de proporcionar un servicio Wifi y de dar servicio a internet a través de la línea del ayuntamiento, se deben establecer las normas de uso y el funcionamiento que el sistema obedecerá. Para regular el acceso de los usuarios a la red será necesario un portal cautivo, pero además, será fundamental una base de datos en la que almacenar los distintos usuarios y su situación, la cual se tendrá que gestionar a su vez mediante queries o consultas, las cuales integraremos dentro de aplicaciones java, a las que se proporciona accesibilidad web, por lo que se agregará un servidor web.

Tanto la base de datos como el servidor web pueden residir en la misma máquina, pero el portal cautivo tendrá que estar en una máquina aparte por motivos de seguridad. Además, el portal cautivo será el equipo encargado del routing, por lo que tendrá que estar conectado a las tres redes del sistema.
En los siguientes apartados se analizarán las decisiones por las que se ha elegido cada software para resolver las necesidades de cada parte del proyecto.

2.8.1 Portal Cautivo.

El portal cautivo se encarga de vigilar el tráfico HTTP y fuerza a los usuarios a verificar su identidad si quieren navegar por internet. También debe permitir acceder al servidor web local y hacer registros en la base de datos, así como proporcionar servicio de servidor DHCP y DNS. Otras de sus funciones necesarias son el firewall y el NAT o la posibilidad de tener tareas programadas que se ejecuten cada cierto tiempo con Cron.

Por ello se ha elegido pfSense [9] como software para el portal cautivo. Se trata de una distribución personalizada de FreeBSD adaptado para las funciones de router, firewall y portal cautivo. Es de código abierto y fácil instalación y se puede configurar a través de consola o por vía web.

En este caso, la máquina que soporte este sistema operativo, contará con tres tarjetas de red. Estas se han denominado WAN o externa y que está conectada al router de salida de la red, LAN o interna, conectada a un switch, que a su vez, está conectado a la primera antena repetidora y a la parabólica de Alustante y BD que estará conectada a la otra máquina que hará de base de datos, de servidor web y de gestión.

2.8.2 Elección del Servidor Web.

El Servidor Web es el programa encargado de gestionar los sitios web, servicios y aplicaciones en el lado del servidor, así como de realizar conexiones con el cliente u otros servidores web para generar la respuesta adecuada ante la petición del usuario.

Generalmente se utiliza el protocolo HTTP para establecer conexiones a través del navegador web, aunque además pueden proporcionar recursos extra como seguridad HTTPS o certificados SSH. En este caso bastará con un servidor sencillo que pueda ejecutar y almacenar código HTTP, CSS y JSP.

Para ello se ha seleccionado Tomcat7, escrito en Java, por lo que funciona en cualquier sistema operativo que disponga de la máquina virtual Java, es un servidor capaz de realizar las acciones que necesita en nuestro servidor, además de funcionar sobre Ubuntu, sistema operativo sobre el que trabajarán el servidor y la base de datos.

2.8.3 Elección de la Base de Datos.

Las bases de datos son bancos de información que contienen datos relativos a ciertos temas y que tienen distintas categorizaciones, almacenados sistemáticamente para su posterior uso. En este caso, existe la necesidad de almacenar cierta información sobre los usuarios que van a hacer uso de la red Wifi, por lo que necesitaremos una base de datos. Además, tiene que ser compatible con pfSense y con el servidor web.

Se ha elegido el lenguaje de consulta estructurado SQL que permite realizar consultas con un lenguaje declarativo y que permite realizar operaciones en las propias consultas, ya sea algebra o calculo relacional.

Para ello se optado por PostgreSQL como servidor encargado de almacenar las tablas requeridas, debido a que es uno de los sistemas de gestión de bases de datos más potentes, además de ser de código abierto y compatible con pfSense.

PostgreSQL tiene una aplicación cliente con un puerto abierto y escuchando las peticiones que realizan los usuarios, pero para diseñar y gestionar las tablas, los usuarios y sus permisos, se utilizará pgAdmin III. También disponible en Ubuntu y de código abierto.

2.8.4 Sistema Operativo.

Tanto el servidor web como la base de datos estarán integrados en la misma máquina, en la que se instalará un Sistema Operativo valido.

Dentro de las posibles opciones, Linux proporciona sistemas operativos estables ,gratuitos y con buen rendimiento a la hora de trabajar como servidores. Ya que es necesario un software demasiado complicado, se ha elegido Ubuntu 12.04 a 32 bits para el equipo de gestión, y sobre el cual se instalará Tomcat7 y PostgreSQL, así como todos los programas necesarios para la gestión del equipo y de la red.

2.8.5 Entorno de desarrollo integrado.

El entorno de desarrollo integrado (IDE) debe proporcionar servicios integrales que faciliten el desarrollo del software. Estos suelen ofrecer muchas características para la creación, modificación, compilación, implementación y depuración del software.

Ya que la estructura web que se ha de llevar a cabo es sencilla y al contar con conocimientos previos, se elegido Eclipse como IDE del trabajo. Eclipse es de código abierto multiplataforma ampliamente utilizado para proyectos similares y entre sus características principales se encuentra la herramienta Maven.

Maven es una herramienta de software para la gestión y construcción de proyectos Java, que permite desarrollar y probar el proyecto de forma sencilla y creando distintos directorios para las distintas etapas del proyecto.

Maven utiliza un Project Object Model (POM) para describir el proyecto de software a construir, sus dependencias de otros módulos y componentes externos y el orden de construcción de los elementos.

Una característica clave de Maven es que está listo para usar en red. El motor incluido en su núcleo puede dinámicamente descargar plugins de un repositorio, el mismo repositorio que provee acceso a muchas versiones de diferentes proyectos Open Source en Java, de Apache y otras organizaciones y desarrolladores.

Capitulo 3: Despliegue y configuración.

Una vez seleccionados las tecnologías, los componentes y el software que mejor pueden cumplir las funciones requeridas, hay que desarrollar el despliegue y en consecuencia ajustar las configuraciones telemáticas a la topología prevista, además de desarrollar las distintas necesidades en cuanto a programación de la web.

3.1 Características técnicas reales.

Una vez seleccionados los emplazamientos, se comprueba que la potencia que recibirán las antenas es suficiente para transmitir la señal correctamente, para ello, se verifica que la distancia entre las antenas no supera la distancia máxima permitida para que la potencia recibida por las antenas sea inferior a la sensibilidad del receptor.

$$P_r = P_e + G_e + G_r - L_{EL} \quad [1]$$

La potencia mínima necesaria para la recepción correcta de las antenas se encuentra en el Datasheet de cada antena. Se puede observar tanto para las antenas PicoStation M como para la airGrid M2HP que la potencia mínima depende a su vez de la velocidad máxima de trasmisión:

-Para una velocidad máxima de 54 Mbps la potencia recibida debe ser de -75 dBm.
-Para una velocidad de 48 Mbps la potencia recibida debe ser de -77 dBm.
-Para una velocidad de 36 Mbps la potencia recibida debe ser de -80 dBm.
-Para una velocidad de 1 a 24 Mbps la potencia recibida debe ser de -97 dBm.

Mientras que la antena NanoStationM2 tendrá los mismos valores excepto para velocidades máximas de 1 a 24 Mbps en cuyo caso, la potencia recibida debe ser de -83 dBm.

La PicoStation M incluye una antena omnidireccional que mejora su ganancia en 2 dBi.
La ganancia de la airGrid M2HP modelo AG-HP-2G20 es de 20 dBi.
La ganancia de la NanoStationM2 es de 11 dBi.

Además, para este tipo de tecnologías en España, el PIRE máximo está limitado a 100 mW, 20 dBm.

$$P_e + G_e = PIRE = 20\ dBm \quad [2]$$

Además, se puede comprobar que para una determinada señal de entrada, la potencia radiada es distinta en función de la velocidad de transmisión, por otro lado, todas las antenas tienen una tolerancia de +/- 2 dB, tanto en emisión como en recepción, se supondrá el peor de los casos.

La ecuación inicial pasará a tener dos nuevos factores:

$$P_r = P_e - L_{VT} + G_e + G_r - L_{EL} - (L_{Tolerancia} * 2) \quad [13]$$

En el Datasheet de las antenas, hay pérdidas variables en función de la velocidad de transmisión, teniendo unas pérdidas comunes de:

$$L_{VT54M} = 5\ dB$$
$$L_{VT48M} = 4\ dB$$
$$L_{VT36M} = 2\ dB$$
$$L_{VT24M} = 0\ dB$$

Una vez obtenidas las pérdidas máximas posibles, se puede obtener la distancia máxima entre antenas en función de las distintas velocidades de transmisión mediante:

$$L_{EL} = 20\log\left(\frac{4\pi d}{\lambda}\right) = 20\log\left(\frac{4\pi}{\lambda}\right) + 20\log d = 20\log d + 40\ dB \qquad [4]$$

Para frecuencias de 2.4 GHz: $$\lambda = \frac{c}{f} = 0.125\ m \qquad [5]$$

Con estos valores, se pueden calcular las distancias máximas alcanzables a partir de las perdidas en espacio libre y a partir de estas, se puede obtener, en consecuencia, la distancia máxima, para la PicoStation M quedan estos resultados:

Velocidad de transmisión (Mbps)	Potencia mínima recibida (dBm)	Perdidas máximas en espacio libre (dB)	Distancia máxima (m)
54	-75	88	251.2
48	-77	91	354.8
36	-80	96	631.0
1-24	-97	115	5623.4

Tabla 3: Valores de distancia máxima de los equipos PicoStation M.

Para la antena airGrid M2HP:

Velocidad de transmisión (Mbps)	Potencia mínima recibida (dBm)	Perdidas máximas en espacio libre (dB)	Distancia máxima (m)
54	-75	106	1995.3
48	-77	109	2818.4
36	-80	114	5011.9
1-24	-97	133	44668.4

Tabla 4: Valores de distancia máxima de los equipos airGrid M2HP.

Y para la antena NanoStationM2:

Velocidad de transmisión (Mbps)	Potencia mínima recibida (dBm)	Perdidas máximas en espacio libre (dB)	Distancia máxima (m)
54	-75	97	707.9
48	-77	100	1000
36	-80	105	1778.3
1-24	-83	110	3162.3

Tabla 5: Valores de distancia máxima de los equipos NanoStationM2.

Con estos resultados se puede afirmar que las conexiones reales que se deben realizar entre antenas no tendrán en ningún caso distancias superiores a las máximas longitudes posibles alcanzables.

3.2 Topología de la red.

Para llevar a cabo una instalación de los equipos con éxito, hay que plantearse previamente la topología que la red va a utilizar, en este caso, se han separado las direcciones IP en distintos rangos, en función de su situación física, así se pueden distinguir tres redes:

-WAN o exterior: Se considera que es la parte exterior, a través de la cual llega la conexión con el proveedor de servicios de internet, Telefónica, concretamente.

-LAN o interior: Es la red a la que se conectarán los usuarios, las antenas y en la que se situará el portal cautivo. A los usuarios se les asignará la IP dinámicamente mediante DHCP, mientras que las antenas tendrán direcciones fijas introducidas manualmente.

-BD: En esta red se encuentran los dos servidores utilizados, estará protegida de entradas exteriores y solo tendrán acceso algunas peticiones interiores.

Para que funcionen correctamente y se puedan cubrir las posibles vulnerabilidades de la red, se debe configurar correctamente el firewall del portal cautivo, así como restringir los puertos accesibles a este y al servidor web.

Con todo esto, y atendiendo a las antenas instaladas quedará una red con una estructura similar a la siguiente:

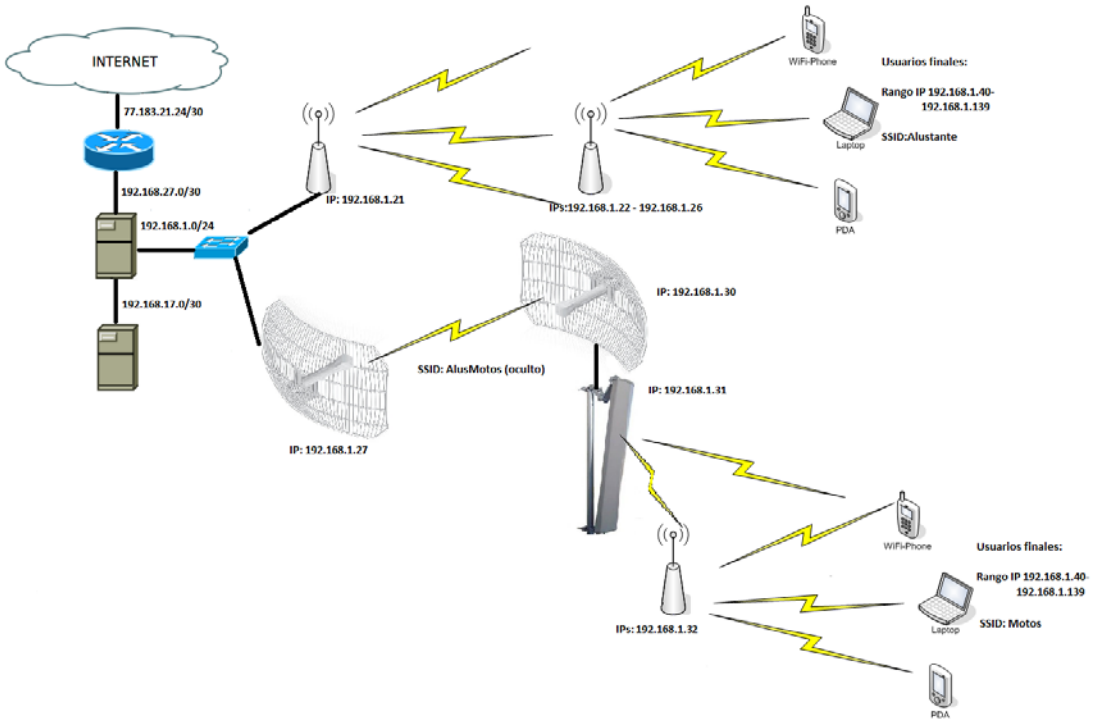

Figura 11: Esquema de la topología de la red.

3.3 Configuración de las antenas.

La configuración de las antenas se puede realizar de forma sencilla a través de su interfaz web, accesible a través de la IP que tienen por defecto y el usuario y contraseña, estos son 192.168.1.20, ubnt y ubnt.

Para llevar a cabo la correcta configuración de las antenas, se debe comenzar por el apartado del sistema, donde se le da un nombre a la antena, se cambia el usuario y la contraseña y selección de la zona horaria.

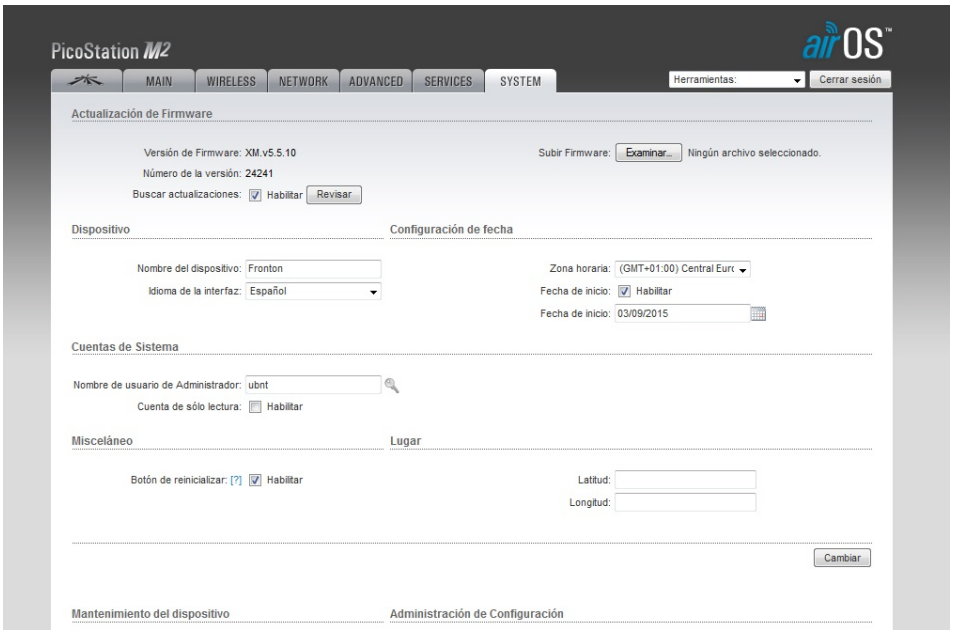

Figura 12: En esta pestaña se pueden modificar algunos parámetros básicos de la antena.

Las opciones de servicios se configuran en la Figura 13.

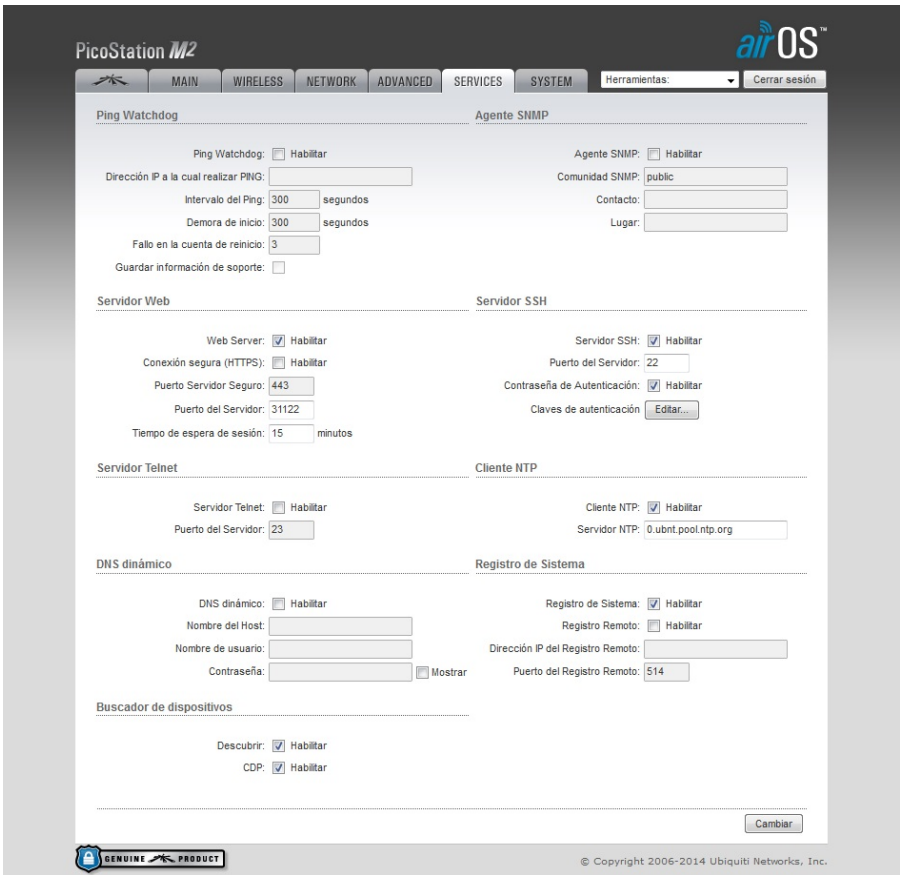

Figura 13: Pestaña de servicios de una antena Ubiquiti.

En esta pestaña, se ha de habilitar el servidor web asi como asignar el puerto por el que recibirá la antena, coincidiendo este con el puerto que le asignará el portal cautivo al hacer el NAT.

También se habilita la pestaña NTP para tener la fecha y hora correctas y el puerto 22 para acceder mediante SSH.

Despues en la pestaña de opciones avanzadas, hay que activar la pestaña que permite el control de la potencia isotrópica radiada equivalente o equivalent isotropically radiated power (EIRP).

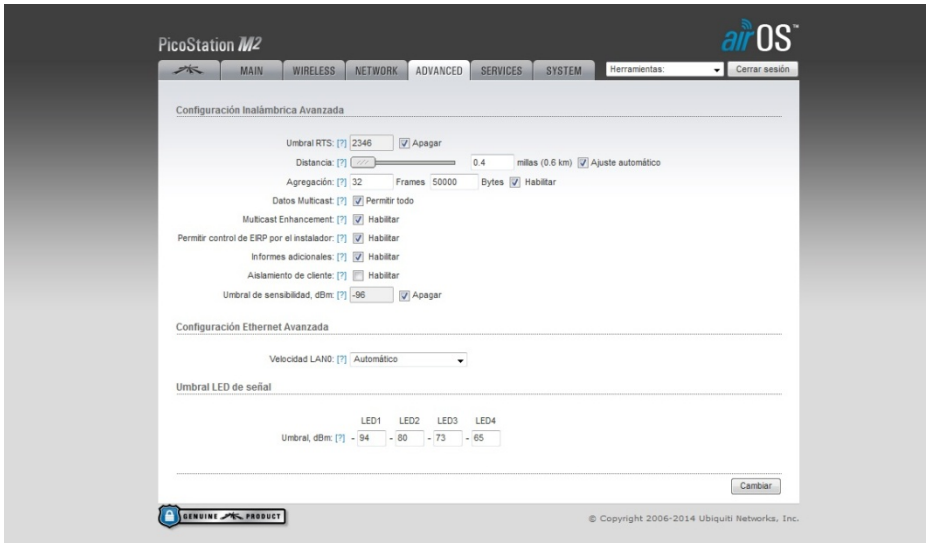

Figura 14: Parámetros avanzados de la antena.

A continuación, en la pestaña de red, a las antenas se les asigna una dirección estática y se configuran en modo puente, de modo que su función sea encaminar los paquetes en la dirección correcta, la puerta de salida por defecto será el router principal:

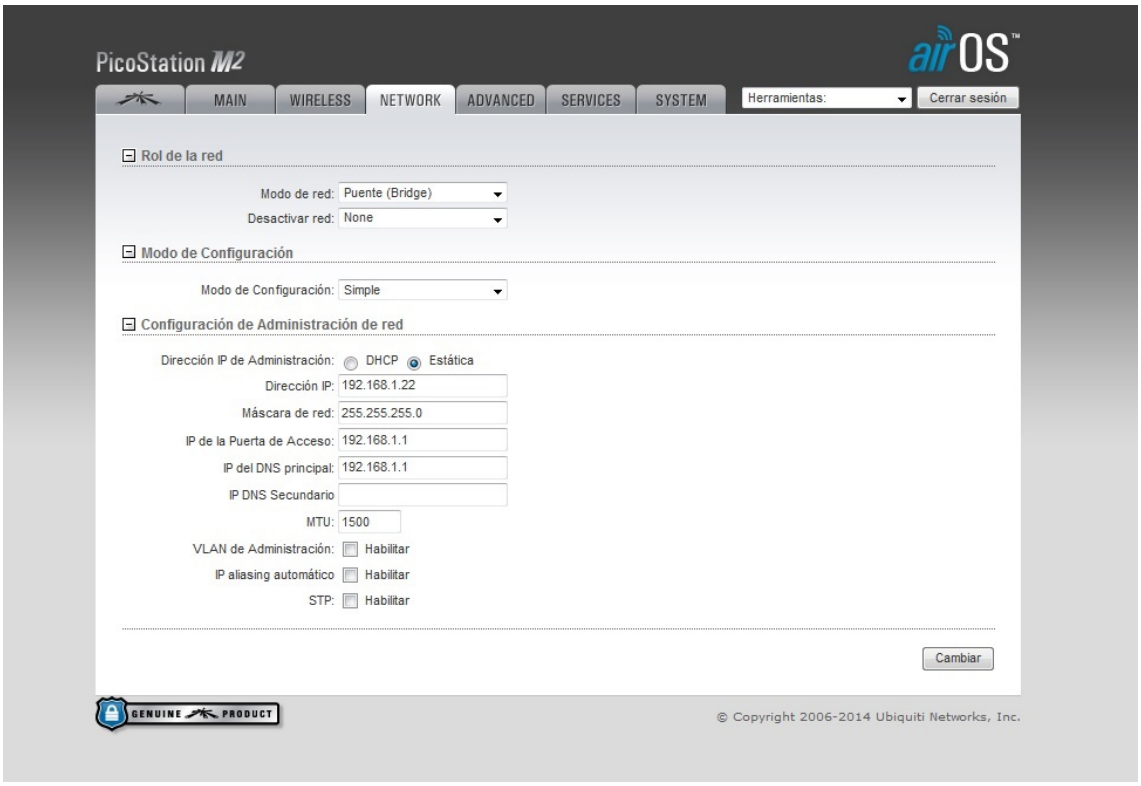

Figura 15: Configuración de la red en la que estarán las antenas.

Finalmente, se modifica la parte de red inalámbrica, donde se indica a la antena las MACs de las otras antenas con las que tendrá que comunicarse una vez esté instalada, también es posible ajustar la potencia emitida, el canal y su ancho de banda.

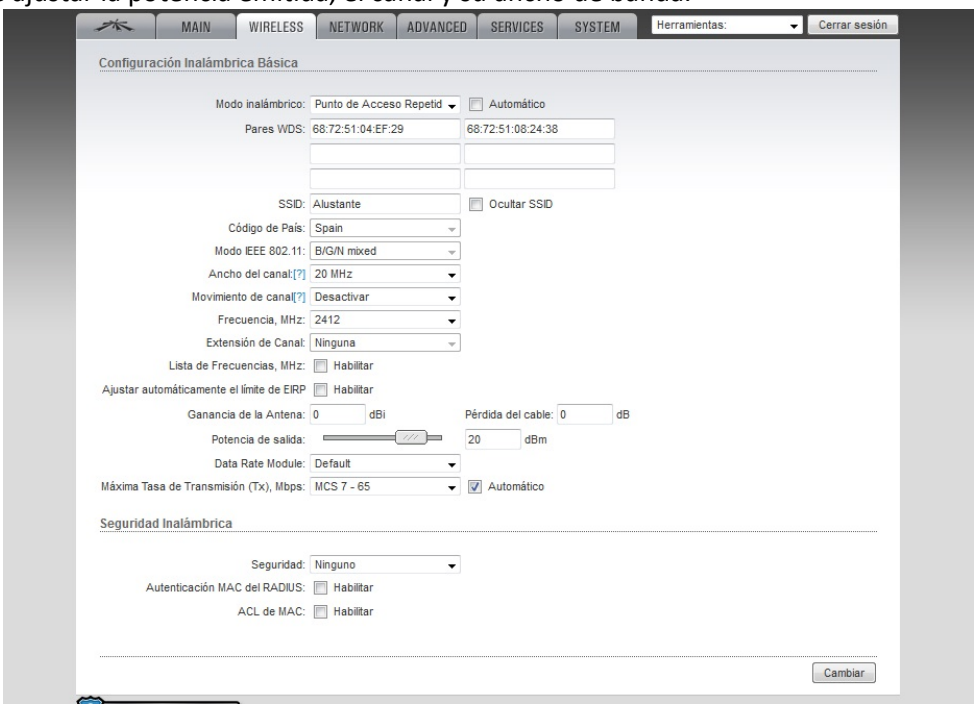

Figura 16: Configuración de los equipos Ubiquiti.

3.4 Instalación de las antenas.

Una vez que se ha decidido la situación física y se han configurado las antenas, se pasa a instalarlas. Estas instalaciones han sido llevadas a cabo gracias a la ayuda de operarios cualificados que se prestaron a colocar los mástiles debidamente, en otros casos, se aprovecharon mástiles ya instalados para la colocación de las antenas.

Figura 17: Antenas PicoStation M y AirGrid M2HP situadas en el Ayuntamiento de Alustante.

Figura 18: Antena PicoStation M instalada en el tejado del frontón de Alustante.

Figura 19: Antena PicoStation M en la plaza del Capricho.

Figura 20: Antena PicoStation M de Ubiquiti en el emplazamiento de la Guardia Civil.

Figura 21: Antena PicoStation M en la Casa Particular.

Figura 22: Antena NanoStation M2 y AirGrid M2HP en la ermita de Motos.

Figura 23: PicoStation M de Ubiquiti en el emplazamiento Casa Particular 2.

3.5 Configuración del portal cautivo pfSense.

El portal cautivo va a ser el punto que deberá atravesar cada conexión que se quiera realizar, por lo que también será el punto central de la red creada y el que gestione las comunicaciones.

Su instalación es sencilla y se puede dejar en su CD de instalación para arrancar o se puede instalar en el PC como sistema operativo residente, esta segunda opción es la que más nos interesa.

Una vez instalado, se identificaran las distintas tarjetas de red, en este caso, el servidor va a tener 3 tarjetas de red a las que se asignarán distintas redes:

-WAN o exterior: Esta irá conectada a la red LAN del router de Telefónica que a su vez proporcionara la conexión a internet. Su IP será la 192.168.27.0/30 ya que es una conexión punto a punto.

-LAN o interior: En esta red estarán tantos las antenas como los usuarios de la red, las primeras tendrán dirección estática, mientras que los usuarios la obtendrán dinámicamente mediante DHCP. La IP de la red será la 192.168.1.0/24.

-BD: Es la conexión con el servidor web y la base de datos que se encuentran en el PC con SO Ubuntu, La IP será la 192.168.17.0/30.

Una vez asignadas las tarjetas de red a las distintas redes, ya no es necesaria la interfaz por consola, la interfaz por http es más cómoda y sencilla. Aún así, se podrá seguir accediendo a la interfaz de consola mediante el programa PuTTY [10] que puede establecer una conexión SSH con el servidor.

Para configurar las IPs, se ha de clicar en la pestaña Interfaces -> (assign), donde se puede asociar las MACs de las tarjetas de red con las IPs deseadas.

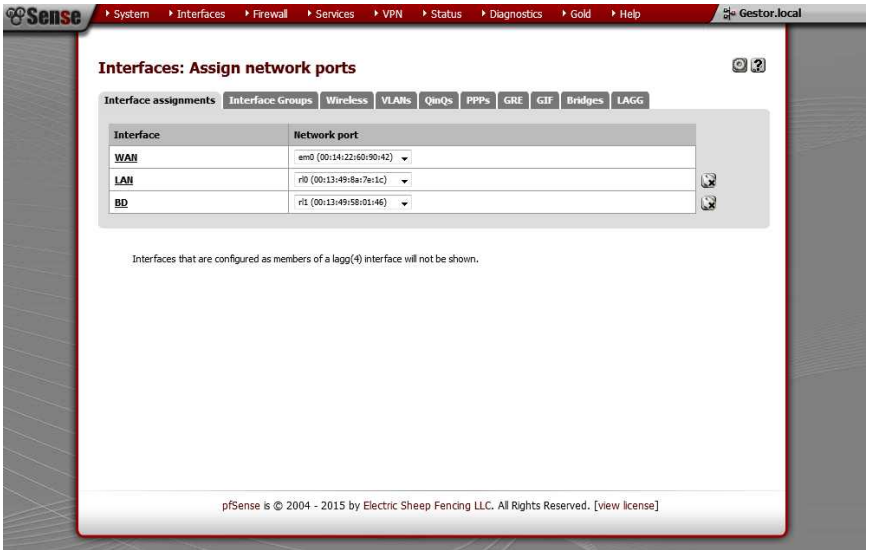

Figura 24: Pagina en la que se asocian MACs e interfaces.

Una vez asociada cada MAC con la interfaz correspondiente, se puede configurar y ponerle la IP que corresponda a cada interfaz:

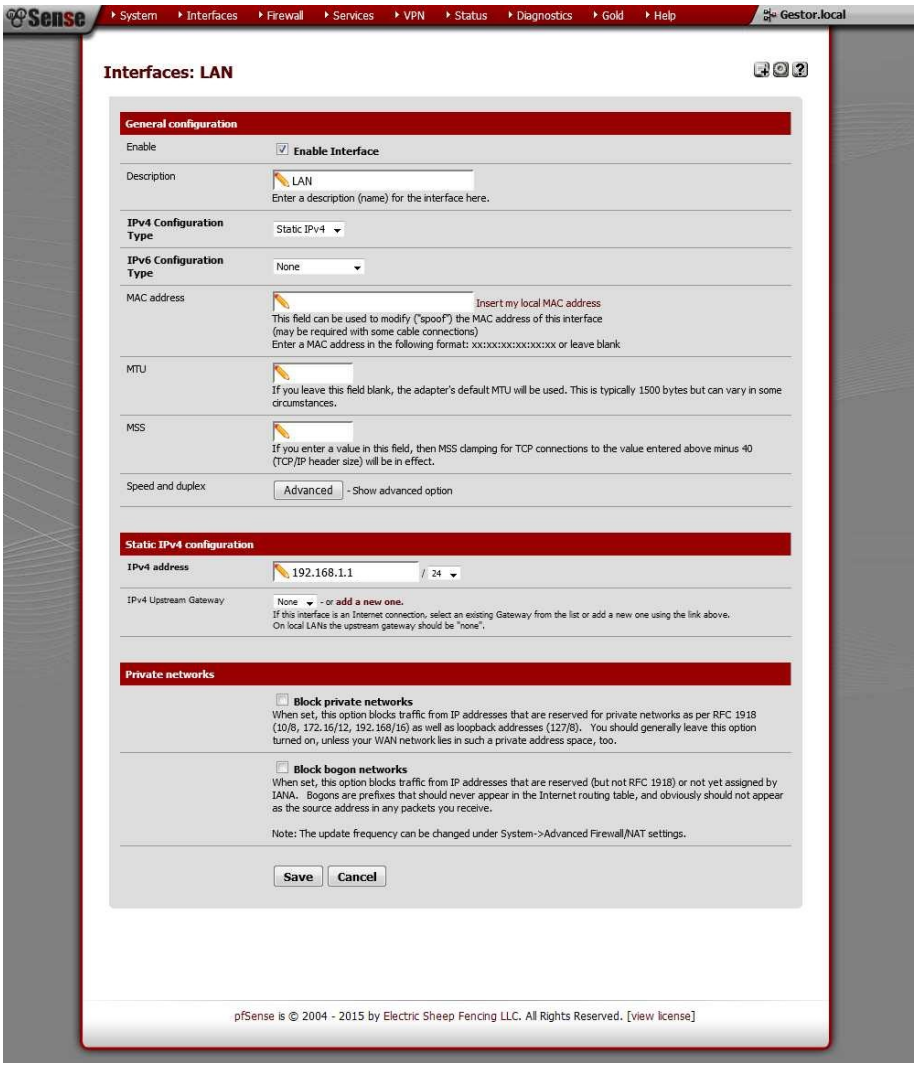

Figura 25: pfSense muestra las opciones de configuración de cada interfaz.

El portal cautivo tiene cantidad de herramientas, de las cuales, se usan y configuran las que se exponen a continuación.

3.5.1 Dinamic Host Configuration Protocol (DHCP).

Para que todos los usuarios se puedan conectar de forma automática a la red, se ha de proporcionar un servicio de DHCP en la red LAN, para configurarlo, se clica sobre Services -> DHCP server y en la pestaña de la red LAN, y se activa el servidor de DHCP.

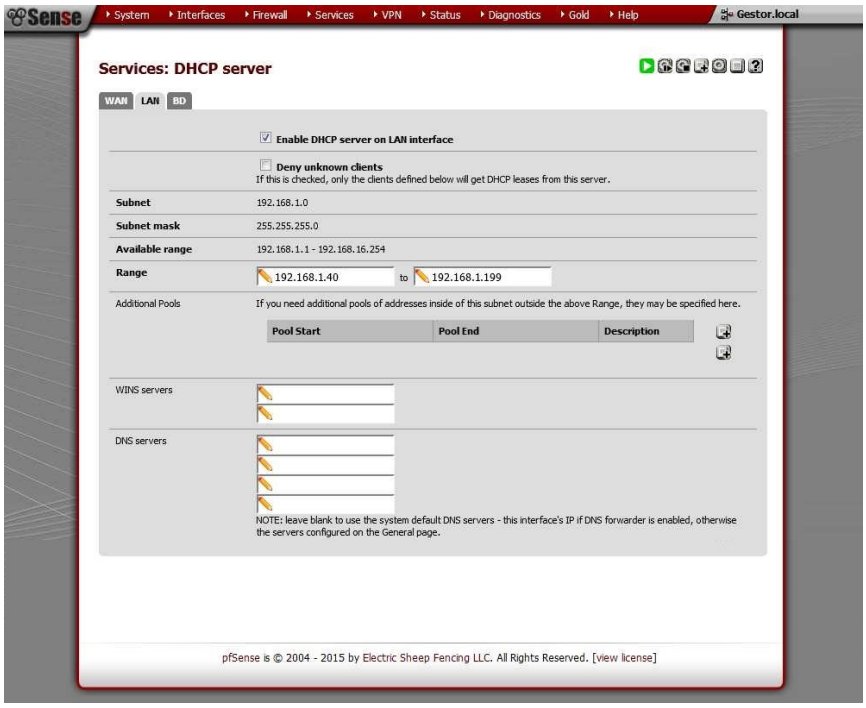

Figura 26: Pagina de configuración del servidor DHCP.

En este caso, se permite la posibilidad de que hasta 160 usuarios estén identificados mediante DHCP.

3.5.2 Routing.

Es la principal actividad que debe realizar el portal cautivo una vez que haya usuarios conectados y haciendo uso de la red. Esta labor la desarrolla de forma autónoma pfSense, aunque siempre se puede indicar cuál es el gateway de salida y las rutas por defecto.

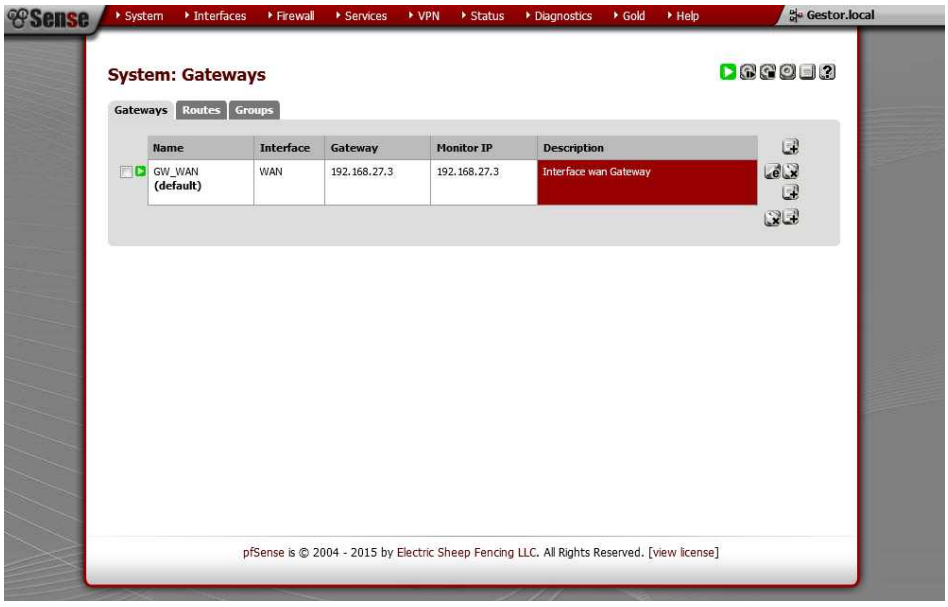

Figura 27: Puerta de salida de pfSense para conectarse a Internet.

3.5.3 Firewall.

El cortafuegos es fundamental a la hora de cubrir posibles vulnerabilidades ya que restringe el tráfico mediante la comprobación de los paquetes, si las cabeceras IP de los paquetes se ajustan a las normas establecidas, estos pasan, en caso contrario, bloquean ese tráfico. En la figura 28 se pueden observar algunas de estas reglas.

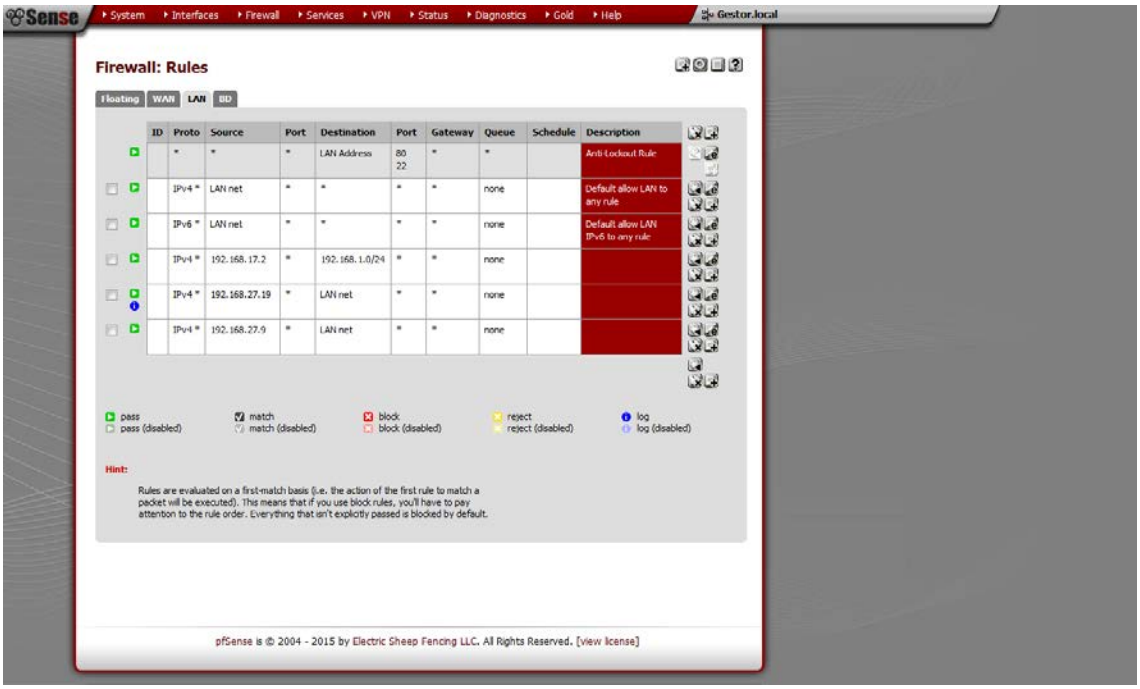

Figura 28: Reglas del firewall para los paquetes entrantes o salientes de la red LAN.

Además, dentro de esta herramienta es posible definir un traductor de direcciones de red (NAT) que permita la comunicación con algunos equipos desde el exterior. Para cada antena definiremos un puerto especifico por si hubiera que comprobar el estado de estas en algún momento, así no sería necesario estar dentro de la red para poder hacerlo.

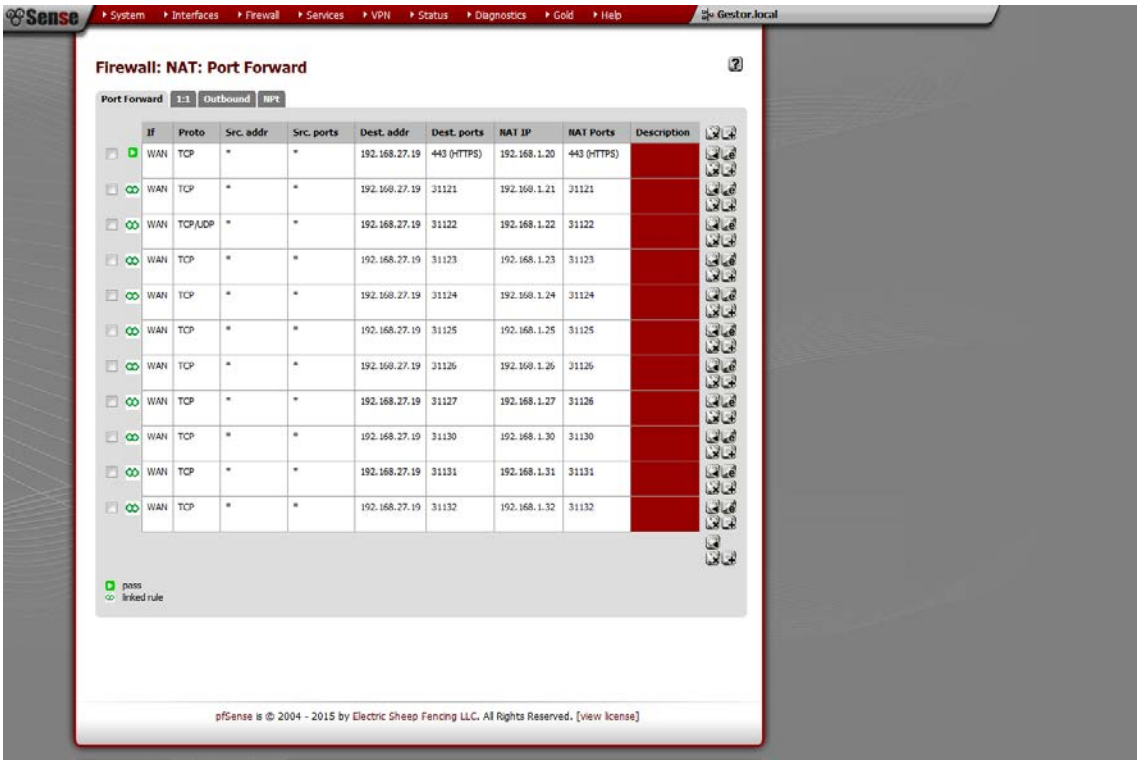

Figura 29: Reglas NAT para la conexión con las antenas.

3.5.4 Portal cautivo.

El portal cautivo obliga a los usuarios a validarse para poder conectarse a la red, esta validación la realizará mediante la comprobación de un usuario y contraseña. En caso de que los usuarios no tengan cuenta, tendrán la opción de registrarse para obtenerla una vez que la administración del ayuntamiento haya validado el perfil del usuario.

Para ello se crea una zona en la red LAN. Una vez creada, se modifican los atributos del portal cautivo, clicando en edit se verá la página que contiene todos sus atributos.

En esta página se indica a pfSense en que interfaz va a estar el portal cautivo. La primera opción permite definir la zona desde la que se conectarán los usuarios, es decir, desde la red LAN. Definiendo el tiempo que tardará en desconectar pfSense a los usuarios que no estén activos y a los que sí. También, se limitará la velocidad permitida de los usuarios, fijando esta a 256 kbps para cumplir la legalidad.

Además, hay que especificar el tipo de autenticación que se desea, en este caso, la entidad que autentica la validez de los usuarios será FreeRadius, que por defecto usa el protocolo PAP, por lo que se seleccionan estas opciones. La dirección de red de FreeRadius es la misma que la del servidor pfSense y tiene habilitado el puerto 1812 por defecto, que no se modifica. Se añade el secreto compartido entre FreeRadius y el portal cautivo para evitar posibles vulnerabilidades en el intercambio de información.

Finalmente, esta ventana permite enviar al portal cautivo la página principal que se desea mostrar cuando los usuarios se conecten y la página de errores que se abrirá cuando los usuario introduzcan incorrectamente sus datos de registro.

Para las páginas de inicio y errores hay que adjuntar algunos ficheros CSS y fotos que dan forma a estas, esto se puede hacer a través de la pestaña de File Manager (Figura 30). El puerto por defecto en el que escucha el servidor web de pfSense es el 8002.

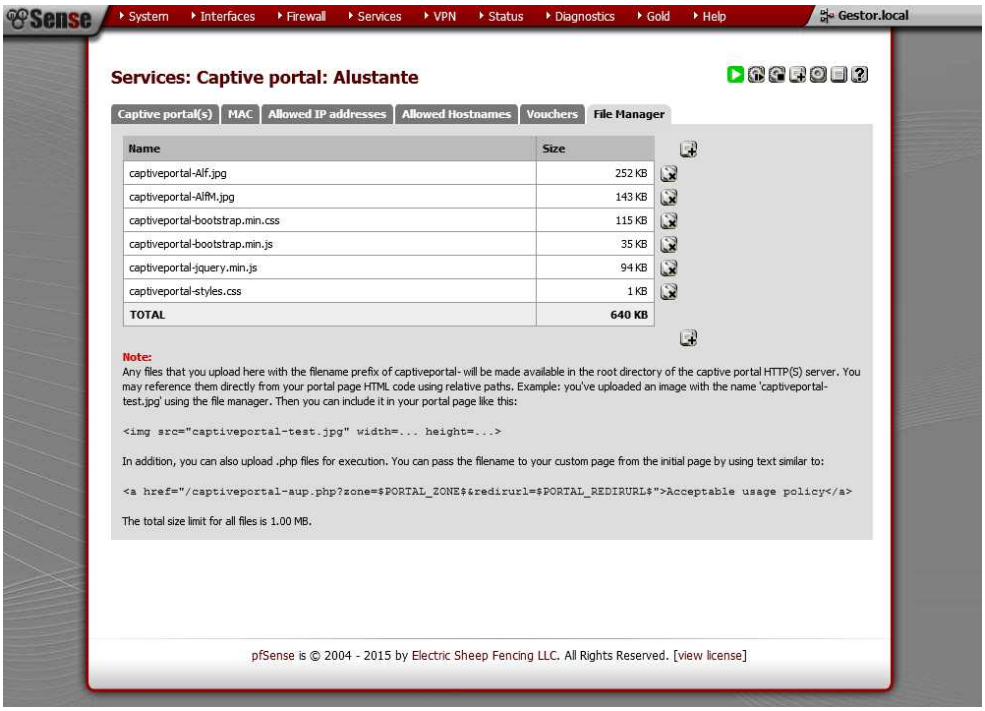

Figura 30: Ficheros dentro de pfSense a los que recurre la página principal.

Por último, en Allowed IP addresses hay que escribir una regla que de permiso a los usuarios para acceder al servidor de Tomcat, para lo que los usuarios situados en la LAN se puedan comunicar con la dirección 192.168.17.2:8090.

3.5.5 FreeRadius.

FreeRadius es el servicio que se encarga de la correcta validación del usuario, FreeRadius se apoya en el protocolo RADIUS. Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1812 UDP para establecer sus conexiones por defecto, que se mantendrá. Además, el servidor RADIUS comprueba que la información es correcta utilizando esquemas de autenticación como PAP, CHAP o EAP.

La información referente a la validación se la envía el portal cautivo, y FreeRadius consultará en la base de datos que tenemos en PostgreSQL, en el otro servidor. Para que FreeRadius realice correctamente la validación, solicita unas tablas de la base de datos con un formato concreto a PostgreSQL, estas tablas serán necesarias para la correcta configuración de la base de datos.

3.5.6 Cron.

Cron es una herramienta de que se encarga de ejecutar procesos a intervalos regulares, va a ser muy útil para ejecutar rutinas de mantenimiento de manera automática. Puede crear y

enviar copias de los usuarios y los registros o buscar actualizaciones. Se ajusta la periodicidad de los eventos en las medidas de tiempo deseadas de forma sencilla.

Cron es impulsado por un *crond*, un archivo de configuración que específica las ordenes y el orden en que tienen que ejecutarse ordenándolas temporalmente.

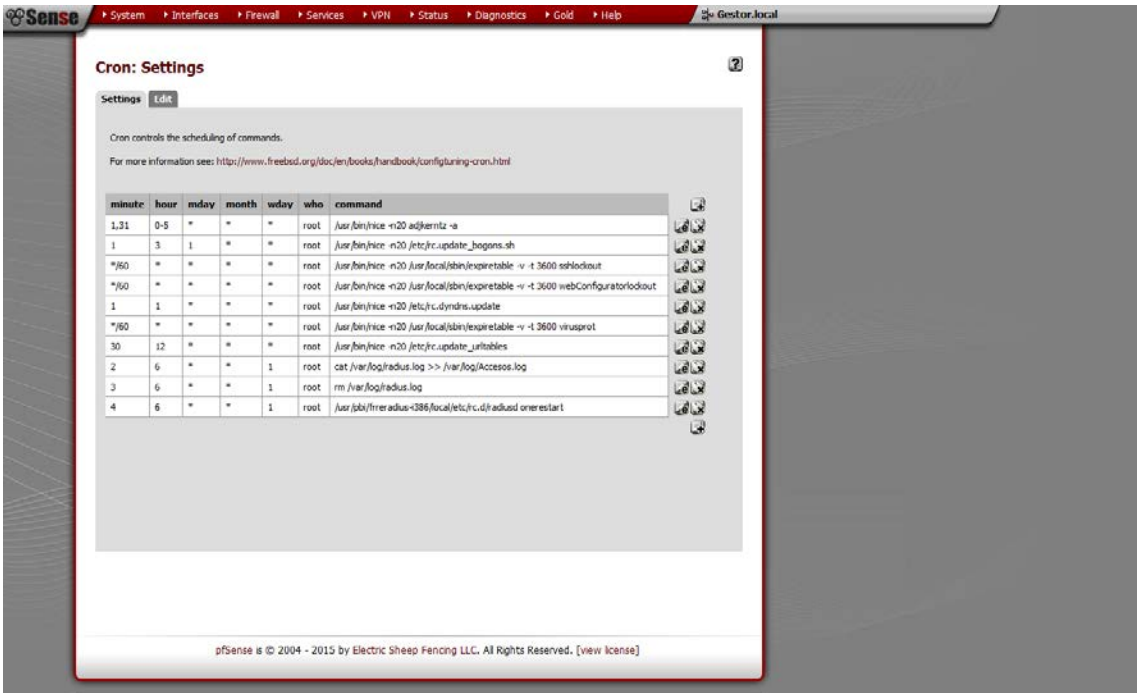

Figura 31: Lista de tareas que el cron ejecuta rutinariamente.

3.6 Configuración del servidor web y base de datos.

El servidor web y la base de datos pueden convivir alojadas en la misma máquina, por ello, instalaremos ambos en nuestro sistema operativo, que será Ubuntu 12.04 de 32 bits [11].

Ubuntu es un sistema operativo basado en GNU/Linux y se distribuye como software libre, está orientado para ser fácil de usar y con un nivel de usuario medio, este puede hacer un uso efectivo de él. Cuenta con cantidad de repositorios y librerías al ser uno de los sistemas de Linux más usados y desarrollados.

Se puede descargar el CDLive de su página web oficial y su instalación es sencilla e intuitiva.
Se instalará en un Pentium IV de 2.6GHz y 2Gbits de RAM. Una vez instalado y configurado, pasaremos a instalar los programas necesarios para la realización del proyecto.

3.6.1 Tomcat7 [12].

Además de instalar Tomcat es necesario tener instalado el JDK y configuradas las variables de entorno JAVA_HOME, CLASSPATH y PATH, ya que si no, el equipo no podrá interpretar código Java.

Para ello, se ejecutan los siguientes comandos en la terminal:

```
sudo apt-get install default-jdk
sudo apt-get install tomcat7
```

Será necesario editar el archivo de configuración bash:

```
sudo nano ~/.bashrc
```

Y añadir las siguientes líneas al fichero:

```
export JAVA_HOME=/usr/lib/jvm/default-java
export CATALINA_HOME=/var/lib/tomcat7
```

Se reinicia bash para que aplique los cambios:

```
~/.bashrc
```

También hay que modificar el fichero:

```
sudo nano /var/lib/tomcat7/conf/tomcat-users.xml
```

En el que hay que añadir un usuario con todos los roles necesarios para configurar y modificar Tomcat, los roles que podrán acceder a la zona restringida del proyecto y el usuario con ese rol.
También hay que crear otro usuario, que será el que tenga permisos para acceder a la validación de usuarios, que se encontrará en el mismo servidor.
Esto se consigue añadiendo al fichero:

```
<tomcat-users>
  <role rolename="admin-gui"/>
  <role rolename="admin-script"/>
  <role rolename="manager-gui"/>
  <role rolename="manager-status"/>
  <role rolename="manager-script"/>
  <role rolename="manager-jmx"/>
  <role rolename="validador"/>
  <user username="admin" password="1234" roles="standard,manager-
gui,manager-status,manager-script,manager-jmx,admin-gui,admin-script"
/>
  <user username="alcalde" password="almanaque" roles="validador" />
</tomcat-users>
```

Mientras que en el fichero `web.xml` se definen los ficheros a los que solo tendrá acceso el administrador del sistema, además se puede definir el tiempo de la sesión y el mensaje que aparecerá al solicitar las paginas indicadas, en este caso, las que validan a los usuarios.

```
<session-config>
  <session-timeout>30</session-timeout>
</session-config>
<security-constraint>
  <web-resource-collection>
    <web-resource-name> ALUSTANTE </web-resource-name>
    <url-pattern>/validateUsers.jsp</url-pattern>
    <url-pattern>/managePendingUsers.jsp</url-pattern>
  </web-resource-collection>
  <auth-constraint>
    <role-name>administrador</role-name>
```

```
  </auth-constraint>
</security-constraint>

<!-- Define the Login Configuration for this Application -->
<login-config>
  <auth-method>BASIC</auth-method>
  <realm-name>Acceso restringido</realm-name>
</login-config>
```

Además, por motivos de seguridad y porque hay otras aplicaciones que usan el mismo puerto, se debe asignar otro puerto al servidor modificando el fichero `server.xml`, dentro de `/conf` y cambiando las líneas que indican el puerto de conexión:

```
<Connector port="8090" protocol="HTTP/1.1"
connectionTimeout="20000"    redirectPort="8443" />
```

Con esta configuración se podrá desplegar la web de forma sencilla. Una vez diseñada, se tiene que desplegar y dejar accesible desde el exterior, para ello, una vez arrancado Tomcat, hay que conectarse a `http://localhost:8090/manage/html`, seleccionar el fichero `war` donde está guardado el contenido de la web y desplegarlo.

A continuación, se reinicia Tomcat para que aplique los cambios, mediante la orden en el bash:

```
sudo service tomcat7 restart
```

3.6.2 PostgreSQL [13] y pgAdmin

PostgreSQL es un sistema de administración de bases de datos relacionales orientadas a objetos, es capaz de gestionar bases de datos y se define un puerto (5432) por el que transmitir y recibir información.
Se puede usar pgAdmin para gestionar la información de PostgreSQL. Es una herramienta de código abierto para la administración de bases de datos PostgreSQL y derivados.

Para llevar a cabo la instalación de PostgreSQL habrá que seguir unos sencillos pasos:

Actualizar el sistema:

```
sudo apt-get update
sudo apt-get upgrade
```

Instalar PostgreSQL y pgAdmin:

```
sudo apt-get install postgresql pgadmin3
```

A través de pgAdmin se puede crear el servidor que trabajará con PostgreSQL. Desde pgAdmin se pueden crear y modificar los distintos parámetros de los servidores de PostgreSQL.

PostgreSQL crea un usuario por defecto, pero se creara otro que se encargue de gestionar las bases y tablas que necesita FreeRadius.
FreeRadius especifica que la conexión debe realizarse con unas determinadas tablas, el formato de estas se ha podido encontrar en internet [14]. Una vez creadas ya están listas para

usar, en ellas se guardan los usuarios y los logs que generan los propios usuarios, además de otras opciones y configuraciones que no se van a utilizar.

Además, se tiene que crear una base de datos en la que insertar los usuarios que se registren en el sistema y que todavía no estén validados, la tabla tendrá la siguiente forma:

```
CREATE TABLE pending_users(
id bigint NOT NULL,
username character varying(300),
name character varying(300),
first_surname character varying(300),
second_surname character varying(300),
birth_date date,
address character varying(2000),
telephone bigint,
password character varying(300),
validated boolean DEFAULT false,
CONSTRAINT pending_users_pkey PRIMARY KEY (id ),
CONSTRAINT pending_users_username_key UNIQUE (username )
)
WITH (
  OIDS=FALSE
);
ALTER TABLE pending_users
  OWNER TO radius;
```

Se podrán indexar usuarios fácilmente siguiendo algunos ejemplos [15], se puede configurar para que tenga IP dinámica o estática y se puede hacer un hash de las contraseñas de los usuarios y codificarlas con el protocolo deseado, en este caso se usará codificación md5.
Esto garantiza que no se puedan leer las contraseñas una vez introducidas, protegiendo a los usuarios y al sistema.

Para poder usar el protocolo md5 hay que configurar el archivo pg_hba.conf, que se encuentra dentro de la carpeta de postgresql, en este fichero se establecen los paquetes que va a aceptar en función del emisor y de la codificación, por lo que tendremos que añadir:

```
# TYPE  DATABASE      USER        ADDRESS           METHOD
host    radius        radius      192.168.17.0/24   md5
```

Con esta línea, le especificamos que la base de datos radius, de la que es propietario el usuario radius, será receptiva en la red 192.168.17.0 y usara md5 como codificación de passwords.

Después se reinicia PostgreSQL:

```
sudo service postgresql restart
```

Una vez realizadas estas modificaciones, se verifica que FreeRadius es capaz de conectarse con PostgreSQL. FreeRadius se intenta conectar con la base de datos al arrancar y en caso de que no lo consiga, se queda inactivo, cuando se den estas situaciones será por una configuración incorrecta.

3.7 Desarrollo web.

Hay que desarrollar la web de acceso que los usuarios van a utilizar para conectarse a la red, así como la de registro y validación. Además, para darle cierta imagen y cuerpo a la web se usarán distintas herramientas de diseño. Se utilizará Eclipse [16] como entorno de desarrollo, ya que es de código abierto y admite multitud de ampliaciones.

3.7.1 Maven.

Una vez instalado eclipse, se creará un proyecto Maven, estos proyectos están compuesto por:

- Un fichero POM.xml (Project Object Model), que es la unidad fundamental de trabajo en Maven, en este fichero se encuentra la información acerca del proyecto y los detalles de configuración. Se especifican, por ejemplo, las dependencias o los plugins que van a ser ejecutados y Maven se encarga de descargarlos y añadirlos al classpath.

- La carpeta de recursos: Se encuentran los ficheros desarrollados, clasificados en carpetas en función de su lenguaje y situación en el proyecto.
    - Los ficheros Java se encuentran dentro de los Recursos Java y a su vez aparece como recurso del dentro de las carpetas database y domain del proyecto.
    - Se pueden guardar dentro del proyecto recursos para otros usos, pero que sean útiles a la hora de programar, create.sql contiene el código que crea las tablas de PostgreSQL.
    - Dentro de /webapp se almacenan los ficheros que dan forma a la web.
        - En su raíz, los jsp serán las páginas accesibles.
        - /Css, /fonts y /js contienen los ficheros de Bootstrap que dan forma a la web.
        - En /img estarán las imágenes del proyecto.
    - La carpeta test permite testear los distintos ficheros java, es una opción interesante a la hora de probar nuevos métodos Java, ya que una vez ejecutado y obtenido el resultado, volvemos al estado anterior de la máquina, sin que se guarde nada.

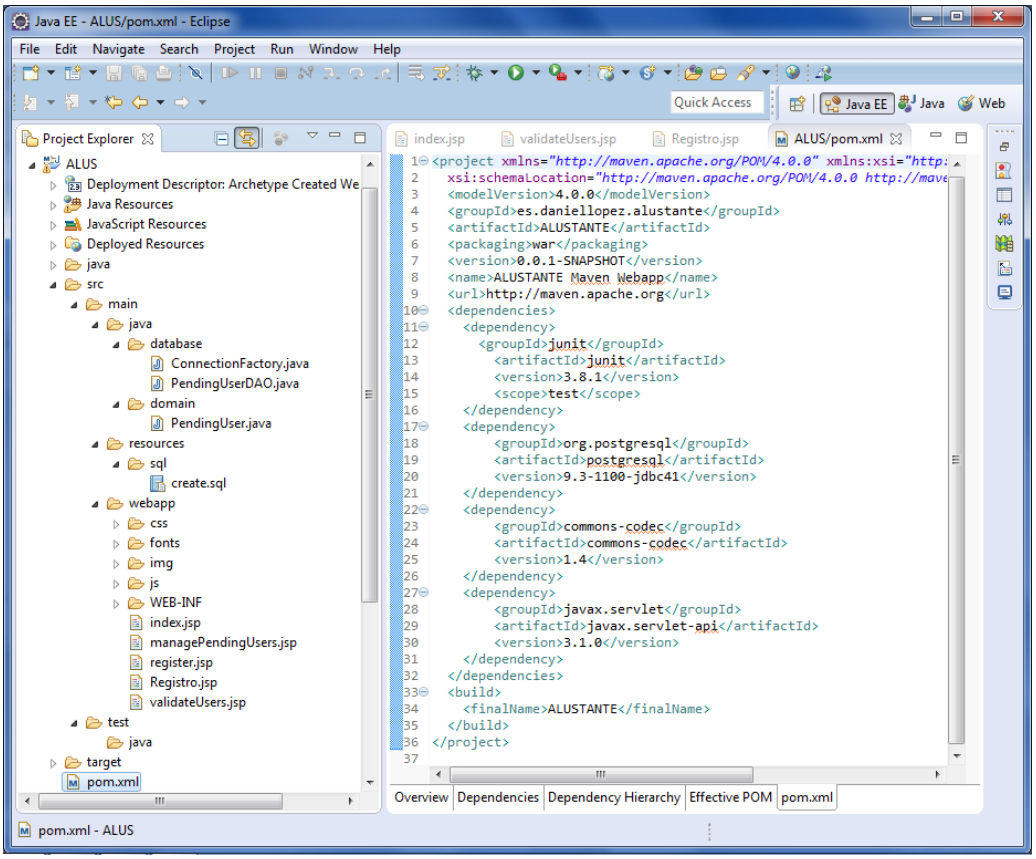

Figura 32: Programa Eclipse con un proyecto Maven en construcción.

- Para comprobar el resultado, se compila el proyecto como una construcción Maven y si el resultado es exitoso, creará dentro de la carpeta `/target`:
  - La carpeta del proyecto con la forma de una carpeta preparada para guardar en un fichero war.
  - El fichero war en sí, preparado para desplegarse en un servidor web.
    Una vez realizado el proyecto, este será el fichero que se desplegará en el servidor Tomcat del equipo Ubuntu.
  - La carpeta /m2e-wtp con información relativa a la carpeta /META-INF de la web. Es decir, a los metadatos relacionados con la web.

3.7.2 Bootstrap.

La finalidad de la web es permitir una validación y un registro rápidos y sencillos, para ello habrá que darle forma con el archivo styles.css, donde se almacena esta información, pero además se va a incluir Bootstrap para el diseño de la web.

Bootstrap es un framework de software libre para diseño de sitios y aplicaciones web. Desde su página [17] permite descargar la última versión e implantarlo en el proyecto directamente de forma sencilla. Además, contiene ejemplos y paginas con plantillas de los distintos elementos que puede representar.
Gracias a la sencillez de las reglas que sigue para encuadrar la página, es fácil ajustar cabeceras, textos, casillas y botones a las filas y columnas que permite definir.

3.7.3 Diseño final de la Web.

La web que se ha presentado en el ayuntamiento de Alustante y que permite las labores de gestión de la red creada se compone de 4 páginas: inicio de sesión, registro, validación y eliminación de usuarios.

Se ha utilizado un fichero CSS de referencia para que puedan ser visualizadas en todo tipo de dispositivos, tanto móviles como tablets u ordenadores. Así, la imagen y el texto se ajustan mediante Bootstrap a cada pantalla y en función de su tamaño, se situarán de una forma u otra.

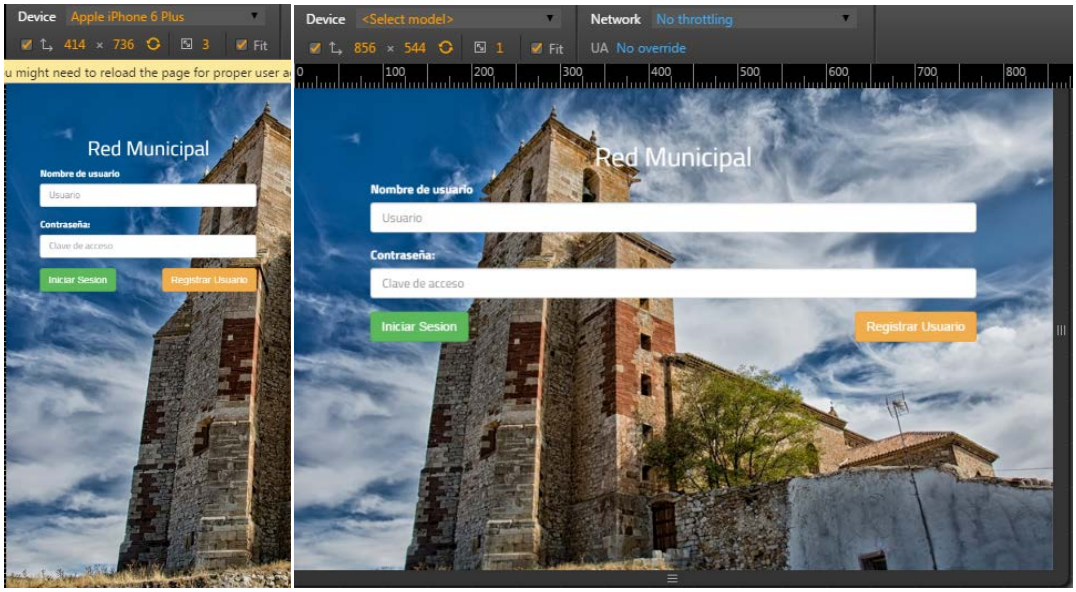

Figura 33: Interfaces de inicio para móvil y tablet.

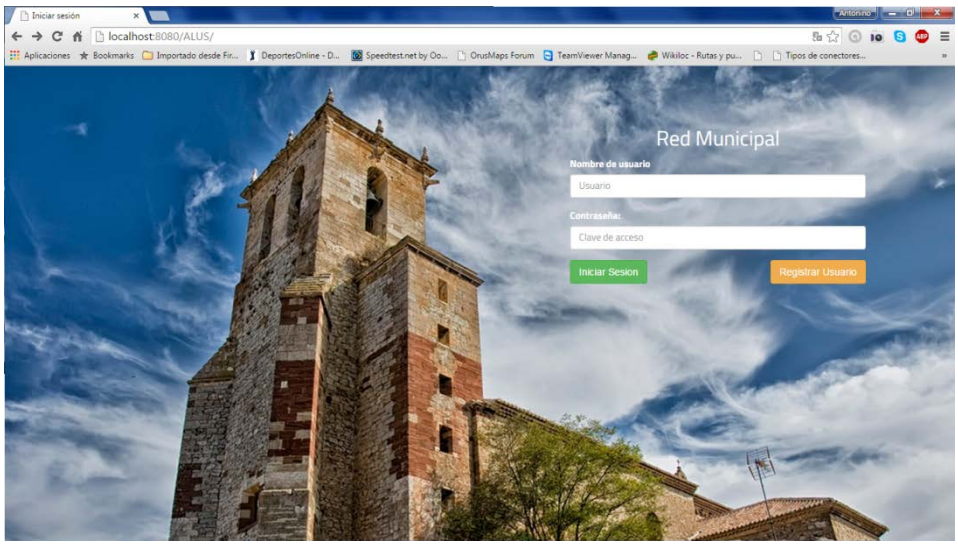

Figura 34: Página de inicio para los usuarios que se conectan a través del PC.

La pagina que permite al usuario registrarse (Figura 35) hace una llamada a una página auxiliar dentro del servidor que a su vez invoca a las clases java, si el usuario se registra correctamente, se le añade en la base de datos y se le informa de que se le ha validado correctamente. Si no, el control de errores le indicará que campos ha introducido mal.

Figura 35: Página diseñada para que los usuarios se registren.

Para que los administradores de la red puedan llevar a cabo sus funciones, se han creado otras dos ventanas que les permiten validar o eliminar a los usuarios.

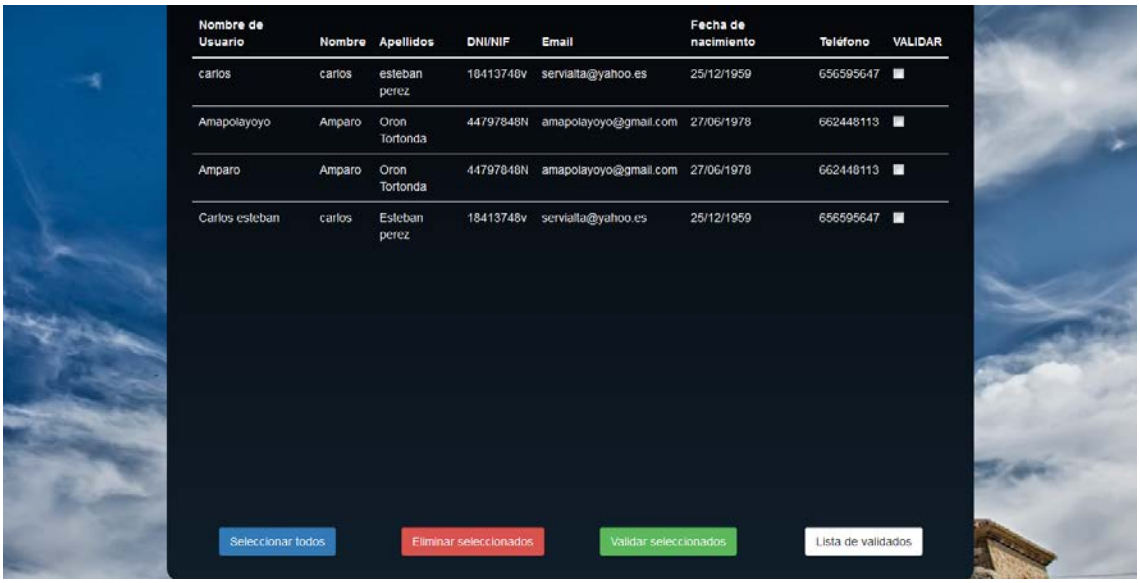

Figura 36: Imagen de la web en la que se validan o eliminan usuarios sin validar.

Capítulo 4: Pruebas, mantenimiento y líneas futuras.

Una vez realizadas todas las tareas expuestas previamente, hay que probar el correcto funcionamiento del sistema y su estabilidad, además de establecer unos medios que permitan acceder a cualquier punto de la red si fuera necesario. También es recomendable llevar un mantenimiento y seguimiento de la red, sobre todo en los primeros intervalos de tiempo después de la instalación.

Será recomendable pedir opiniones a usuarios y clientes para conseguir un feedback que nos permita mejorar en este o futuros diseños.

4.1 Pruebas.

Se comprueba que las antenas se comunican entre ellas sin problemas antes y después de instalarlas. Se han realizado mediciones de cobertura, buscando localizar puntos sin cobertura, por si hubiera que reforzar la señal en alguna zona.
También se comprueba el correcto funcionamiento del sistema una vez instalado.

4.1.1 Medidas de cobertura.

Se ha realizado un pequeño test de cobertura en el pueblo de forma rudimentaria, tomando medidas cada cierta distancia y apuntando los valores de la señal recibida en cada punto. Se tomaron unas 100 medidas y en ellas se evidencia las zonas donde la cobertura es baja o nula, por si fuera necesario ampliar la señal.

Estas zonas son las que están más alejadas de las antenas y no tienen visión directa con ellas, también, en las calles más estrechas es donde más dificultad se encuentra para recibir señal.

4.1.2 Pruebas del sistema.

Una vez instalado, se comprobó el correcto funcionamiento del sistema, así como también las posibles vulnerabilidades, corroborando que se cumplían las reglas del firewall, los NATs y que las respuestas de los servidores eran correctas. Además, se comprobó que todas las antenas transmitían correctamente.

4.1.3 Feedback.

Una vez desplegado el sistema final, se está permitiendo que los usuarios comiencen a registrarse y a hacer uso de la red. Como todo proyecto, siempre hay puntos que se pueden mejorar y se han tenido en cuenta las posibles dudas o críticas que tanto los usuarios como los clientes experimentaron.

4.2 Mantenimiento.

Este tipo de redes exigen un mantenimiento mínimo una vez puesto en marcha, pero siempre pueden aparecer problemas o situaciones inesperadas, además se podrán prever cambios en la red, como pueden ser la afluencia de usuarios en distintas épocas del año.

4.2.1 Formación y ayuda al cliente.

Por la falta de conocimiento en esta área por parte de los empleados públicos del ayuntamiento, será importante informarles y enseñarles a usar algunas funciones de la web.
Además se proporcionará un número de contacto en caso de que ocurra un error en el sistema o algún equipo se bloquee, para que llamen y el equipo técnico sea capaz de resolverlo, independientemente de la situación de este.

4.2.2 Control remoto: TeamViewer [18].

Para garantizar una gestión eficaz, es indispensable ser capaz de alcanzar y de acceder a los dispositivos en cualquier situación. Por ello, se han configurado reglas NAT que permiten acceder a cada dispositivo cuando se realiza la conexión a través puerto específico.

Esto permitirá la alcanzabilidad con todas las antenas. Sin embargo, la dificultad reside en que la IP pública del ayuntamiento es dinámica y va cambiando, la cual será necesaria para acceder via web a los distintos equipos.

Se ha elegido TeamViewer para realizar la tarea debido a su sencillez y a que es software libre. Además, es compatible con los sistemas operativos con los que se trabaja.
Cuando se inicia en un equipo, el programa genera una ID y una contraseña (también permite que el usuario establezca su propia contraseña). Para establecer una conexión entre un equipo local y otro remoto, el usuario del equipo local debe ponerse en contacto con el otro y este debe indicarle la ID y la contraseña. Una vez hecho esto, se introducen en el programa TeamViewer que se está ejecutado en el ordenador local.
Las sesiones de TeamViewer están codificadas mediante infraestructura de clave pública RSA y AES y se comunican mediante http, es decir, escuchan a través del puerto 80 o el 443.

Se dejará instalado y ejecutándose a TeamViewer tanto en el PC del ayuntamiento como en el servidor web. De esta manera se puede acceder a la red sin saber realmente la IP pública de esta. Una vez dentro, se puede hacer uso de alguna página o aplicación [19] que muestra la IP pública del ayuntamiento.

4.2.3 Control remoto: PuTTY.

PuTTY es un cliente de acceso remoto a máquinas informáticas de cualquier tipo mediante SSH, Telnet o RLogin, para plataformas Windows 32bits y UNIX.

La utilización de PuTTY será necesaria para acceder al servidor pfSense, para usarlo solo hay que ejecutar el programa que se encuentra en su web [10] e introducir la IP destino, es decir, la 192.168.17.1. El programa se conectará a pfSense mediante SSH y se podrá realizar una

sesión similar a la que se tendría en el propio servidor. Tambien estará activa su interfaz a través de http.

Con todas estas medidas, se tiene acceso al sistema en cualquier momento y lugar con conexión a internet.

4.2.4 Copias de seguridad.

Para la cumplir la LOPD, esta nos obliga a hacer una copia de la base de datos que contiene los datos de los usuarios y otra de las sesiones que intentan establecer los usuarios con la fecha de estas. Esta información debe ser almacenada durante al menos un año. Esta tarea se puede automatizar gracias a cron, añadiéndole dos instrucciones en las que se le indica los ficheros a copiar semanalmente. Se realizará tanto en el pfSense como en el Ubuntu.

Para la base de datos SQL en Ubuntu se usa pg_dump[20] , debemos instalarlo:

```
sudo apt-get install gnome-schedule
```

La instrucción a incluir en el cron[21] será:

```
01 03 * * 04 pg_dump basededatos > fichero.sql
```

4.2.5 Afluencia de usuarios.

Alustante, como casi todos los pueblos, sufre bruscas variaciones de población en ciertos momentos del año, de tal forma, que en semana santa y en las fiestas patronales, a mediados de agosto, su población se multiplica y pueden estar alrededor de 1000 personas.

En estas épocas está claro que la red se va a ver desbordada, ya que la conexión de internet del ayuntamiento es de 3 Mbps. Para intentar dar un servicio mínimo de mensajería instantánea a los usuarios de la red durante estas fechas, se reducirán los tiempos de conexión inactiva a 5 minutos y se limitarán las conexiones activas a 1 hora, para que el servidor DHCP pueda dar nuevas direcciones a otros usuarios.

4.3 Líneas futuras

Entre las distintas posibilidades de líneas futuras de este proyecto, la idea principal sería la de mejorar la cobertura de la red dentro del municipio, así como la búsqueda de municipios con la misma problemática, algo bastante común en esta zona de España.
También se podrían usar las redes Wifi municipales como redes de transito para que los usuarios se conecten a internet a través del router de sus casas, en vez de encaminarlos todos a través del internet del ayuntamiento, mejorando el servicio a ambos tipos de usuario.

Capítulo 5: Cálculo de costes.

En este proyecto van a ser necesarios varios operarios y un ingeniero, así como recursos económicos para la financiación de los equipos y los materiales empleados para llevar a cabo todo el despliegue.

5.1 Coste en recursos humanos.

Podemos dar un valor aproximado de las horas de trabajo necesarias para llevar a cabo el proyecto por parte del ingeniero y los operarios.

Por un lado, podemos valorar el trabajo del ingeniero en horas efectivas:

- Reuniones con personal del ayuntamiento y con personas especializadas en el tema: 15 h.
- Estudio del proyecto y preparación de este con casos similares: 20 h.
- Investigación sobre leyes, teoría de propagación, recursos de software y hardware a utilizar: 70 h.
- Configuración e instalación de antenas: 50 h.
- Configuración e instalación de equipos: 45 h.
- Desarrollo de software: 100 h.

En total, unas 300 horas, este es un valor aproximado y del que no se cuentan el tiempo de viaje, imprevistos, ni mejoras llevadas a cabo.

Los operarios estuvieron presentes durante la instalación de las antenas y además fueron los encargados de colocar los mástiles en las posiciones indicadas, fueron dos y entre ambos se calcula que trabajaron 100 horas.

5.2 Coste de equipos y cableado.

Aquí se incluyen los materiales que se han comprado exclusivamente para este proyecto y que ha pagado el ayuntamiento.
Para este proyecto han sido necesarias 8 antenas, 2 PCs y un switch. Además, hemos necesitado cables de par trenzado y conectores RJ-45 en todas las conexiones realizadas por cable. Las antenas y el switch han sido adquiridos en pccomponentes [22], donde se puede comprar todo tipo de material informático. Los ordenadores, al no necesitar un procesador demasiado potente han sido donados.

Artículo	Precio (€)	Und	Total (€)
Ubiquiti Networks NSM2 NanoStation M2 2.4 GHz 11 dBi	96.95	1	96.95
Ubiquiti Picostation MH2 MIMO + Antena 2 dBi	77.25	6	463.50
Ubiquiti Networks AG-HP-2G16 AirGrid M series, 2,4 GHz	61.20	2	122.40
D-Link GO-SW-8E 8-port 10/100Mbps Fast Ethernet Switch	15.25	1	15.25
Bobina Cable FTP Cat 6 Flexible 100 Mts	66.55	1	66.55
TOTAL			764.65

Tabla 6: Costes de los productos necesarios para el desarrollo del proyecto.

5.3 Coste de otros materiales.

Por otro lado, aunque sin poder valorar económicamente, cabe mencionar la inversión que ha hecho el ayuntamiento para la instalación de los soportes sobre los que se han colocado las antenas. Han sido necesarios 4 mástiles de 2, 3 y 4 metros, con sus respectivos anclajes.

Además, ha proporcionado una grúa con cesta porta personas para poder acceder a las zonas donde se llevaron a cabo las instalaciones y el material necesario para llevar a cabo estas obras.

Capitulo 6: Conclusión.

Beneficios personales de este TFG.

- Encontrarme no solo en un ámbito educativo, si no también empresarial. Experimentando los problemas, análisis de viabilidad, enfoques, ideas y soluciones prácticas que se le dan a cada proyecto.

- Toma de contacto con clientes mediante feedback durante la evolución del proyecto.

- Aprendizaje de tecnologías y habilidades poco conocidas hasta ahora, pero con gran proyección de futuro, mediante documentación y tutoriales en inglés.

- Trabajo en cooperación con personas con distintas especializaciones y conocimientos.

Bibliografía

[1] Boletín Oficial del estado del 8 de septiembre de 2010
http://www.boe.es/buscar/doc.php?id=BOE-A-2010-12831

[2] Documentos a presentar para registrarse o modificar los datos de los operadores ante la CNMC:
http://telecos.cnmc.es/documents/10138/2228218/201505_WEB_SCE.pdf/30258377-4009-4626-a11e-adaa2afdd0a5

[3] LOPD
http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/estatal/common/pdfs/2014/Ley_Organica_15-1999_de_13_de_diciembre_de_Proteccion_de_Datos_Consolidado.pdf

[4] Boletín Oficial del estado del 3 de noviembre de 2013
http://www.boe.es/diario_boe/txt.php?id=BOE-A-2011-17887

[5] Google Earth
https://www.google.es/intl/es_es/earth/

[6] Datasheet Antenas Ubiquiti Omnidireccionales
http://dl.ubnt.com/datasheets/picostationm/picom2hp_DS.pdf

[7] Datasheet Antenas Ubiquiti Sectoriales
http://dl.ubnt.com/datasheets/nanostationm/nsm_ds_web.pdf

[8] Datasheet Antenas Ubiquiti Parabólicas
http://dl.ubnt.com/datasheets/airgridm/airGrid_HP.pdf

[9] pfSense
https://www.pfsense.org/

[10]PuTTY
http://www.putty.org/

[11] Sistema Operativo Ubuntu
http://www.ubuntu.com/

[12] Servidor Web Tomcat7
http://tomcat.apache.org/download-70.cgi

[13] PostgreSQL
http://www.postgresql.org/

[14] Esquema en PostgreSQL para la conexión FreeRadius
http://wiki.freeradius.org/config/PostgreSQL-DDL-script

[15] Ejemplos de usuarios para PostgreSQL
http://wiki.freeradius.org/guide/SQL-HOWTO

[16] Eclipse
https://eclipse.org/downloads/

[17] Bootstrap
http://getbootstrap.com/

[18] TeamViewer
https://www.teamviewer.com/es/index.aspx

[19] Dirección IP pública
https://www.whatismyip.com/es/

[20] Copia seguridad postgresql
http://rm-rf.es/postgresql-como-crear-y-restaurar-backups-de-bases-de-datos/

[21]Cron en Ubuntu
https://help.ubuntu.com/community/CronHowto

[22] PcComponentes
http://www.pccomponentes.com/antenas.html