XEiLL: Xarxa Educativa i Lliure

Tedi Roca Domínguez
tedi.roca@gmail.com
1ª Revisión (01/02/2005)

A los que ya no están aquí,
por el pasado brindado,
el presente acontecido
y el futuro que me han enseñado a vivir.

Gracias a mis amigos y familia por el soporte ofrecido todo este tiempo,
a Victor Carceler por la orientación y el soporte sobre la XEiLL,
a Léonard Janer por su asesoramiento en el proyecto,
a Pedro Carrasco por ayudarme en todo esto,

y sin duda, mi mayor agradecimiento a mi madre por su apoyo incondicional en esto y algunos otros cientos de cosas.

Resumen

Este documento refleja el diseño e implementación de una red inalámbrica de ámbito educativo. Se realiza un recorrido sobre el estado actual y su desarrollo futuro.

Con el propósito de proporcionar una amplia visión sobre las comunicaciones inalámbricas actuales, se muestra la estructura y funcionamiento general de una red telemática extendida que haga uso del espacio aéreo como principal canal de transmisión. No obstante, nos centraremos en la definición de la XEiLL *(Xarxa Educativa i Lliure)*, donde detallaremos los materiales y las aplicaciones necesarias para su funcionamiento, así como la instalación y configuración de los equipos.

Aunque las expectativas de crecimiento apuntan hacia una expansión geográfica mucho mayor, el presente documento refleja la implementación de la red educativa en el ámbito de Santa Coloma de Gramenet. Es por esto, que durante el desarrollo del proyecto consideraremos la red como una WMAN (*Wireless Metropolitan Area Network*).

Tanto el funcionamiento como la filosofía de la XEiLL se basan en la utilización de software libre para su puesta en marcha y la garantía de un acceso abierto para los usuarios. La instalación y mantenimiento de la red se basan en la colaboración desinteresada de varias personas y entidades.

Resum

Aquest document reflexa el disseny i l'implementació d'una xarxa sense fils d'àmbit educatiu. Es realitza un recorregut sobre l'estat actual i el seu futur desenvolupament.

Amb el propòsit de proporcionar una amplia visió sobre les comunicacions sense fils actuals, es mostra l'estructura i funcionament general d'una xarxa telemàtica estesa que fa faci us de l'espai aeri com a principal canal de transmissió. No obstant, ens centrarem en la definició de la XEiLL (*Xarxa Educativa i Lliure)*, on detallarem els materials i aplicacions necessàries per al seu funcionament, així com l'instal·lació i configuració dels equips.

Encara que les expectatives de creixement apunten cap a una expansió geogràfica molt major, el present document reflexa l'implementació de la xarxa educativa en l'àmbit de Santa Coloma de Gramenet. Es per això, que durant el desenvolupament del projecte considerarem la xarxa com una WMAN *(Wireless Metropolitan Area Network)*.

El funcionament i la filosofia de la XEiLL es basen en l'utilització de software lliure per la seva posada en marxa i la garantia d'un accés obert pels usuaris. L'instalació i manteniment de la xarxa es basen en la col·laboració de varies persones i entitats.

Abstract

This document shows an educational wireless network design and implementation. It's done an actual state and future implementation review.

With the purpose of giving a wide wireless communications view, is showed structure and general working of an extended telematic network using air as main transmission channel. Anyway, we'll be centered on XEiLL (*Xarxa Educativa i Lliure)* definition, where we'll detail the necessary materials and applications to made it work, as needed hosts installation and configuration.

XEiLL's working and philosophy are based on the use of free software to make it work and open access to users. Installation and network maintenance are based on various persons and entities collaborations.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

1. Introducción

1.1. Justificación del proyecto

Hoy en día es indiscutible la gran utilidad de las redes de comunicaciones y la revolución que éstas comportaron en el entorno de los computadores tras su aparición. La capacidad de transportar datos entre largas distancias sin necesidad de desplazamientos físicos y con costes relativamente bajos sitúa las redes como un elemento indispensable para el desarrollo de servicios, negocios, investigación, desarrollo y educación.

1.1.1. Redes inalámbricas

Si a todo esto sumamos la posibilidad de utilizar los recursos disponibles con una cierta movilidad que nos permita estar conectados a la red sin necesidad de realizar costosas instalaciones físicas, contamos con la solución perfecta para utilizar dispositivos clientes, tales como ordenadores portátiles o agendas de bolsillo, de forma cómoda, eficiente y económica. En base a estas necesidades, a lo largo de la historia se han ido desarrollando diferentes sistemas de comunicaciones que permiten el enlace de terminales o computadores sin utilizar cables.
Actualmente contamos con un elevado número de medios para transmitir datos, audio y vídeo; desde el casi obsoleto *packet radio*[1], que utilizó en sus orígenes enlaces de radio a 27 MHz, hasta el actual sistema de telefonía celular o las comunicaciones vía satélite.

Entre todos estos mecanismos, nos encontramos con los sistemas de comunicaciones WiFi. Aparecido a finales de los años 80, tuvo que luchar en su primer intento de despegue ya que el rápido crecimiento de las redes de área local (en adelante *LAN: Local Area Network*), hizo que se precablearan los edificios, lo que comportó un importante desembolso económico. Por otro lado, se mejoró la seguridad y calidad del par trenzado en las instalaciones existentes. Invertir en una nueva tecnología de elevado coste no era viable en aquel momento.

[1] *Sistema de comunicaciones en el que se emplean las bandas de radioaficionado como medio de transmisión. En su máximo auge se utilizaban velocidades de 9600bps.*

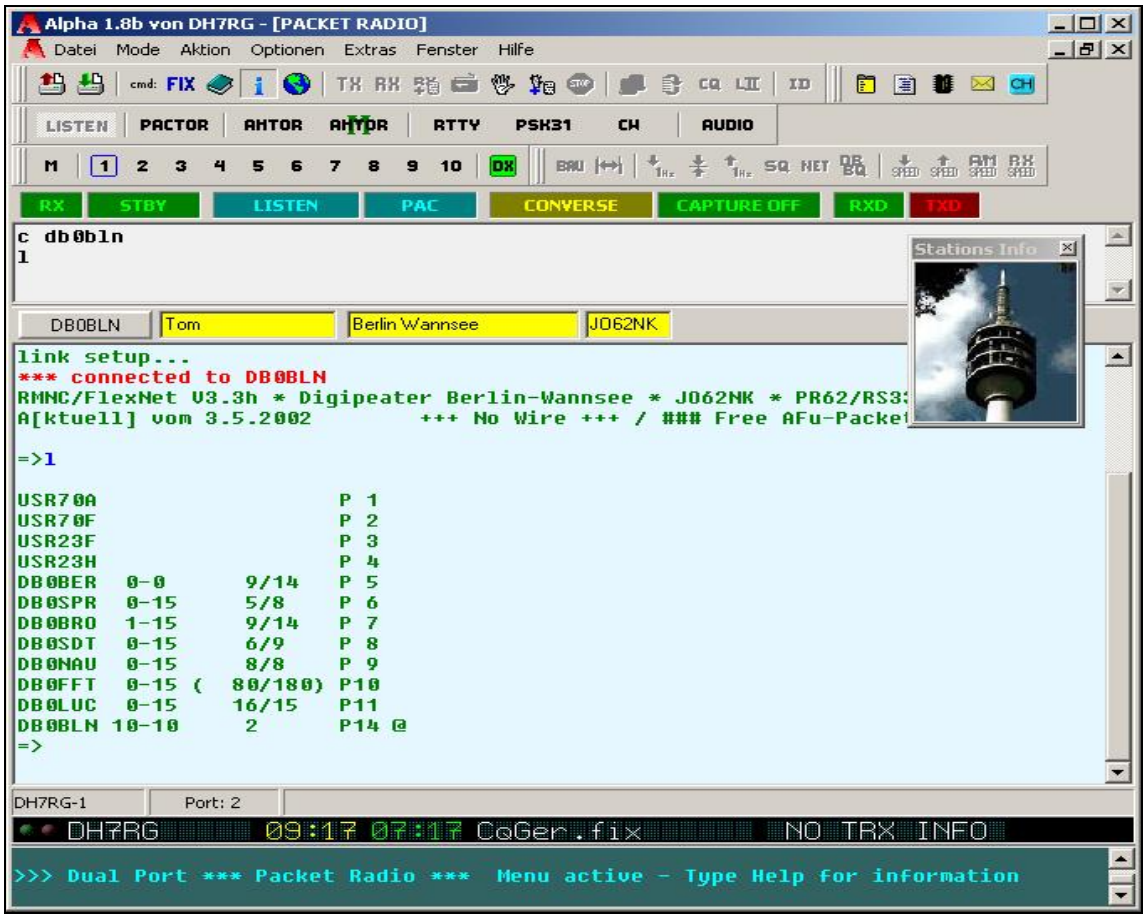


Figura 1: Pantalla del casi extinto *Packet Radio,* donde incluso se podía transmitir vídeo.

Sin embargo, pasado un tiempo se estableció como un medio económico y fácil de instalar, lo que comportó la reconsideración del sistema por parte de fabricantes y empresas. Se encontró en la tecnología WiFi[2] la solución perfecta a problemas que aparecían con el cableado convencional, como la cobertura en edificios de gran superficie, estructuras históricas y otros lugares donde no es posible realizar cableado o pequeñas oficinas donde no es rentable la instalación y mantenimiento de una *LAN* cableada.

La gran aceptación de esta tecnología y proliferación de nuevos productos, comporta actualmente un gran abanico de posibilidades de sencilla implementación y un bajo coste, al alcance de los usuarios, como podremos ver en el apartado 3.3 de este documento

[2] *Acrónimo de Wireless Fidelity. Hace referencia a las redes inalámbrica que utilizan los standards 802.11a/b/d/g.*

1.1.2. Red educativa libre

La idea de proporcionar acceso a una red educativa donde alumnos y profesores tienen acceso a contenidos y servicios potencialmente valiosos para la enseñanza, recibe especial importancia cuando ésta se encuentra disponible para cualquier usuario. De ésta forma, mediante el uso de tecnología WiFi, es posible ofrecer un gran abanico de medios que facilitan el desarrollo de la educación, introduciendo a alumnos y profesores en el vanguardista mundo de la tecnología.

En la actualidad existen numerosos proyectos sobre comunicaciones inalámbricas. A menudo éstos fracasan por su amplia abundancia y falta de asociación, lo que significa una dispersión del potencial que proporcionan este tipo de redes.
Por este motivo, la XEiLL[3] *(Xarxa Educativa i Lliure)* pretende ser un único punto de encuentro y asociación en el ámbito educativo, dejando al lado fronteras geográficas.

La posibilidad de poder colaborar en el desarrollo de una actividad que me entusiasma, como son las telecomunicaciones, respaldada por el ámbito educativo del proyecto, genera en mi un gran interés, por lo que personalmente me considero afortunado de poder plasmar todo ello en mi proyecto de fin de carrera. A todo esto, cabe destacar la fortuna de poder trabajar junto a la persona que hizo nacer la XEiLL y a la vez su principal impulsor, del que he adquirido numerosos conocimientos.

Por todo esto y muchas otras razones, me gusta considerar este proyecto como la introducción de lo que quisiera realizar durante mucho tiempo: aportar mis conocimientos y entusiasmo para el crecimiento de esta red.

[3] *Red inalámbrica libre de ámbito educativo.*

1.2. Enfoque y método de desarrollo del proyecto

Tras tomar la decisión sobre el proyecto a desarrollar, en primer lugar, se fijan los objetivos que se esperan conseguir con el proyecto.

Posteriormente se ha desarrollado un planteamiento general sobre las comunicaciones inalámbricas, con el fin de facilitar el entendimiento del resto de secciones.

En el siguiente apartado se describe qué es la XEiLL: su historia, su funcionamiento, los valores que transmite y su puesta en marcha. Este apartado ayuda a entender cómo y porqué apareció la red educativa inalámbrica. Se muestra el día a día de ésta y se realiza un recorrido sobre las figuras y sistemas necesarios para que sea posible.

A partir de este punto se separan 3 rasgos generales del desarrollo:

- Estado actual de la red: Generación de conocimiento sobre la estructura inicial, rasgos generales y especificaciones técnicas.

- Implementaciones derivadas del proyecto: Se detallan las mejoras y nuevas implementaciones, su desarrollo y el estado final de éstas.

- Propuestas futuras: Dado que tratamos con un proyecto en evolución constante, seguramente uno de los puntos más importantes de este documento es la propuesta y modo de poner en marcha nuevas implantaciones de éste.

Se cierra el trabajo con un estudio de viabilidad económica y una reflexión sobre el impacto social.

2. Objetivos

2.1. Optimización

Actualmente la XEiLL cuenta con una estructura operativa en pleno funcionamiento. Mediante el despliegue de varios nodos que ofrecen cobertura a gran parte de las ciudades de Santa Coloma de Gramenet y Badalona, proporciona diferentes servicios a los usuarios. Uno de los objetivos de este proyecto, es la optimización y mejora de la red existente mediante nuevas soluciones que garanticen una mejor estabilidad y fluidez de comunicación.

2.2. Expansión de la red

Tal como se avanzaba en la introducción de este trabajo, a día de hoy la XEiLL presenta una progresiva expansión en la ciudad que nació. Sin embargo, no debemos olvidar que la proyección de esta red no está limitada por fronteras geográficas, si no que pretende ser un nexo de unión entre educación y tecnología.
Podremos comprobar el importante papel que juegan la organización y planificación de la estructura física y lógica de la red a la hora de asegurar una firme estabilidad en su expansión.

2.3. Nuevas implementaciones

Sin lugar a dudas, podemos asegurar que esta red educativa presenta unas posibilidades de crecimiento realmente ambiciosas. Tal como se ha comentado en el punto anterior, es de suma importancia prever la expansión y asegurar la estabilidad. A la capacidad de crecimiento sumaremos un importante factor: la implementación de nuevas tecnologías.
Para comprender de mejor manera la importancia de este factor, podemos recurrir sin vacile a la vertiente social del proyecto y ponernos en lugar del usuario. Tiene suma importancia ofrecer servicios novedosos, actualizados y de valía para el usuario, de forma que se sienta interesado por formar parte de la comunidad.

2.4. Propuestas futuras

Cuando hablamos de tecnología, es inevitable que ideas como la innovación o el progreso recorran nuestra mente. Es por ello, que en el campo de las telecomunicaciones utilizamos el mismo baremo tiempo/progreso.
Estructurar una red de amplias dimensiones implica una serie de riesgos y contratiempos que hay que tener en cuenta. Hace falta estudiar con detenimiento los planes de futuro y asegurar una correcta implementación de nuevas tecnologías.
Por la naturaleza de este proyecto y sus restricciones de tiempo, no será posible mostrar todas las posibilidades que admite y mucho menos entrar en explicaciones minuciosas. Sin embargo, considerando de gran interés e importancia muchas de estas nuevas ideas, y sin olvidar el cometido en sí de un proyecto, gran parte de este trabajo se basa en la generación de conocimiento específico para llevar a cabo estas acciones.

2.5. Conexión de clientes

Actualmente la red educativa libre cuenta con gran número de personas interesadas en hacer uso de los recursos que ésta proporciona. Sin embargo, en muchos casos, el usuario no conoce los elementos precisos para llevar a cabo las conexiones o la forma óptima de hacerlo. Por ello, en este trabajo se hace énfasis en la conexión de los clientes.

No debemos olvidar que gran parte de una infraestructura de comunicaciones la forman los clientes. Son los usuarios quienes van a hacer uso de los recursos de la XEiLL y por lo tanto, parte de este proyecto está destinada a éstos.

Parte de este proyecto pretende ser una guía hacia los usuarios finales, guiándoles así en la utilización de los recursos y la configuración de sus equipos clientes para un acceso óptimo a la red. Entre otros aspectos, se detalla el material necesario y la construcción de elementos adicionales para una mejor recepción de la señal.

Figura 2: Comunicación en infraestructura.

3. Redes WiFi

Este trabajo no pretende tratar en profundidad el modo de funcionamiento de las comunicaciones inalámbricas ni su naturaleza. Sin embargo, es de vital importancia el conocimiento de algunos conceptos para comprender el desarrollo del proyecto.

3.1. Principios básicos

Tal como se explicaba en el capítulo de introducción, desde hace varios años contamos con diferentes formas para enviar información a través de la atmósfera y el espacio exterior. Éstos son métodos que proporcionan un medio de transmisión de las señales sin confinarlas, lo que conocemos como transmisiones inalámbrica.
En los medios no guiados el ancho de banda de la señal emitida por la antena es más importante que el propio medio a la hora de determinar las características de las transmisiones. Sin embargo, hay una serie de factores que influyen de forma notable en las comunicaciones:

- Ancho de banda utilizado.
- Dificultades en la transmisión (atenuación, obstáculos, etc.).
- Interferencias (presencia de señales en bandas próximas).
- Número de receptores.

Dependiendo de su uso y modo de funcionamiento, nos encontramos con los siguientes tipos de comunicaciones *WiFI*:

- *Adhoc*: Los clientes se comunican entre ellos. No precisa de un sistema de red distribuido, son los propios clientes quienes crean la red.

- Infraestructura: Los clientes se conectan a un punto central. No se envía información entre ellos.

- Escucha (pasivo): El cliente únicamente recibe datos, no envía ningún tipo de señal. Este modo es comúnmente utilizado por los programas utilizados para descubrir redes inalámbricas (*Stumblers*[4]).

Comúnmente el modo escucha es utilizado con fines de control. Para la comunicación entre un número reducido de estaciones pueden utilizarse los modos *Adhoc* o infraestructura. Sin embargo, dependerá de las necesidades individual.

- *Adhoc:* uso eventual sin necesidad de un gran rendimiento y conexión en red de un número de equipos reducido.

- Infraestructura: uso habitual y/o redes formadas por un número elevado de equipos. Elevado rendimiento (más de 5 estaciones).

3.2. Funcionamiento

3.2.1. *CSMA/CA y MACA*

Para transmitir datos a través del medio aéreo es necesario realizar un control sobre las estaciones, de forma que no haya colisión entre ellas. Para ello se utilizan protocolos de acceso al medio (*CSMA/CA*[5] *y MACA*[6]).

El funcionamiento se resume en 3 fases:

- Antes de transmitir, la estación escucha al medio para determinar si está libre u ocupado.
- Si no está ocupado, la estación ejecuta una espera entre tramas.
- Si en el tiempo de esperas continua ocupado, espera y ejecuta el algoritmo de *Backoff* hasta que quede libre.

[4] *Programas como AirStumbler, ayudan a descubrir redes* WiFi *de forma rápida y sencilla*
[5] *Carrier Sense Multiple Access/Collision Avoidance. Es un protocolo para la transmisión de portadora en redes 802.11. Previene colisiones antes de que ocurran.*
[6] *Multiple Access with Collision Avoidance. Proporciona acceso múltiple evitando lsa colisiones.*

Es de suma importancia este algoritmo porque reduce la probabilidad de colisión cuando varias estaciones quieren transmitir y todas esperan que el medio quede libre.

3.2.2. Envío de tramas

Las estaciones que se comunican mediante redes WiFi envían una serie de tramas para controlar su situación respecto al resto de estaciones:

- Tramas de administración:
    - Solicitud.
    - Respuesta.
    - Solicitud de prueba.
    - Respuesta de prueba.
    - *Beacon*[7].

- Tramas de control:
    - Solicitud para enviar (RTS: *Request To Send*).
    - Listo para enviar (CTS: *Clear To Send*).
    - Acuse de recibo.

- Tramas de datos

Tal como veremos en el capítulo sobre recomendaciones de seguridad, los atacantes pueden utilizar algunas de estas tramas para conseguir información sobre las estaciones y utilizarla para realizar ataques.

[7] *Tramas de información de presencia que envían continuamente los dispositivos WiFi*

3.2.3. Antenas

Se utilizan antenas exteriores para hacer llegar la señal a distancias lejanas, sin perder calidad de señal. La ganancia de estos dispositivos está expresada en dBi[8] (decibelios isotrópicos).

Siguiendo la ecuación de la energía radiada,

Energía radiada = Energía transmisión – pérdida cable + ganancia antena

podemos apreciar la importancia de utilizar una antena acorde con las distancias que queremos cubrir, además de la importancia de no rebasar la potencia máxima de transmisión permitida: 100 mW (20 dBm).

Dependiendo del modo de expansión de la señal, distinguiremos básicamente entre 2 tipos de antenas:

- Direccionales: radiación de frecuencias altas. Es posible concentrar la señal en un haz direccional y alcanzar largas distancias.

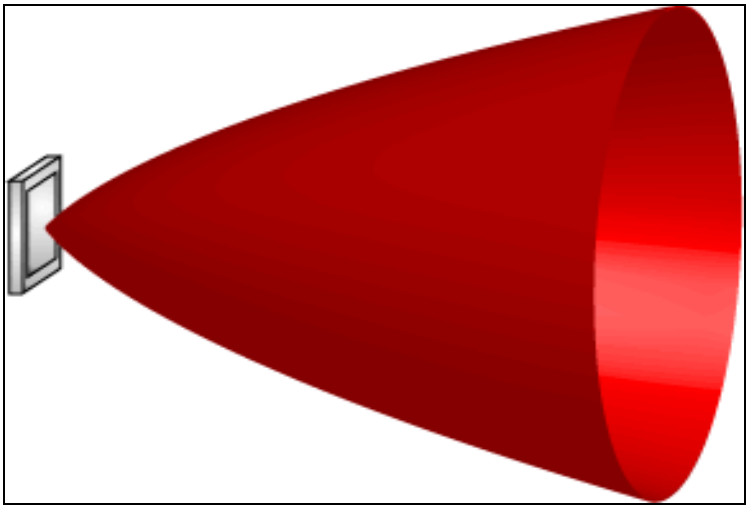


Figura 3: Radiación de una antena direccional

[8] *Decibelios relativos a una hipotética antena isotrópica.*

- *Pacific Wireless 16 dBi Yagi Series Directional antenna*
  - Ganancia: 16 dBi
  - Rango de frecuencias: 1,7Ghz-2,7Ghz
  - Utilizada para enlaces punto a punto de larga distancia

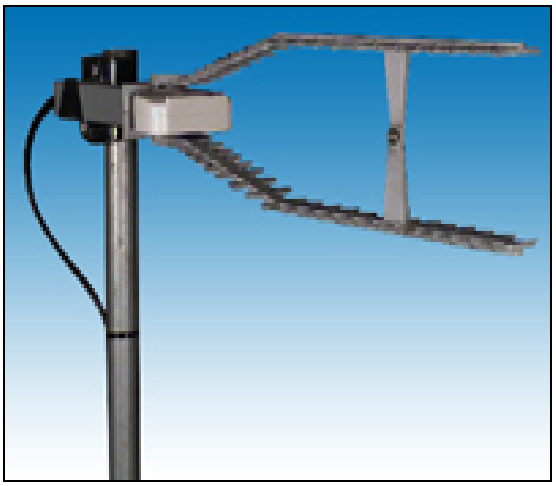


Figura 4: Yagi Direccional

Pacific Wireless Flat Panel PAA24

- Ganancia: 13 o 19 dBi
- Utilizada para situarse en paredes de edificios

Figura 5: *Flat Panel*

- *Pacific Wireless antenna PMANT*
  - Ganancia: 15,19 y 24 dBi
  - Utilizada para enlaces punto a punto de larga distancia

Figura 6: PMANT

- Omnidireccionales: radiación de frecuencias bajas. La señal se expande desde el interior de la antea, radialmente hacia el exterior. Las distancias alcanzadas son menores que en el caso de antenas direccionales.

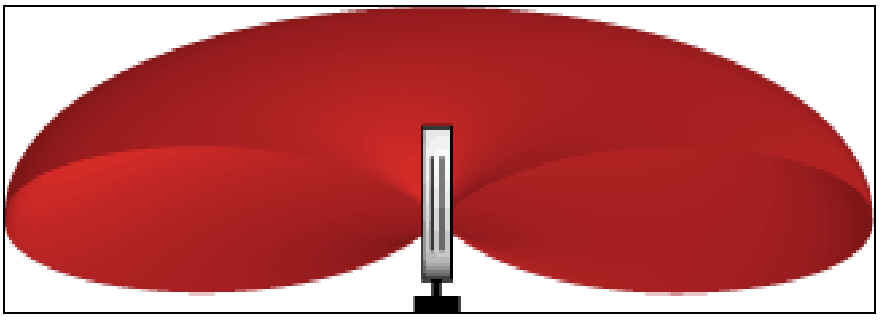


Figura 7: Radiación de una antenas omnidireccional.

- *Pacific Wireless Vertically Polarized Omnidirectional*
  - Ganancia: 7, 9 o 12 dBi
  - Antena omnidirecional de tipo colineal
  - Utilizadas como antena base para distribuir la señal en un conjunto de clientes
  - Conector N hembra integrado

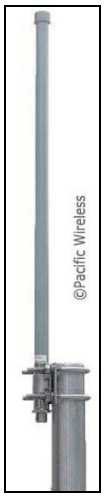


Figura 8: Vertically Polarized Omnidirectional

- *Pacific Wireless SA24*
  - Ganancia: 9 o 17 dBi
  - Dispone de subjecciones móviles para poder orientarla adecuadamente
  - Utilizada como antena base para distribuir la señal a un conjunto de clientes
  - Dispone de conector N hembra integrado

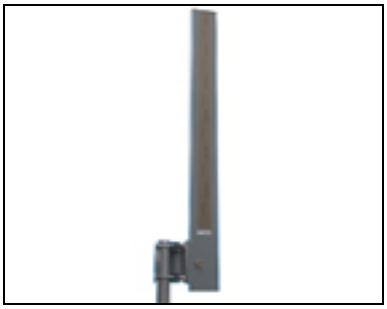


Figura 9: SA24

3.3. Aplicaciones.

Dentro de las múltiples utilidades de las redes WiFi, podemos distinguir 3 aplicaciones básicas:

- Ampliación de *LAN* cableada
    - Lugares donde ya existe una red cablead y por motivos económicos o dificultad de instalación, resulta adecuado utilizar redes inalámbricas.

- Puesta en marcha de redes donde el cableado no es posible
    - Edificios históricos
    - Lugares donde no es posible realizar agujeros o pasar cable

- Interconexión de edificios
    - Conexión de edificios cercanos, tales como sedes de una empresa

- *LAN* de reducidas dimensiones
    - Casos en los que el despliegue de una red cableada supone un importante desembolso económico, pueden ser solventados mediante la utilización de dispositivos inalámbricos de bajo coste. Por ejemplo, pequeñas oficinas o redes domésticas.

- Acceso nómada
    - Aquellas situaciones en las que se pretende dar acceso a varios usuarios. Implementar una solución inalámbrica proporciona movilidad y comodidad a los usuarios a la vez que evita tener que desplegar cableado y tomas hasta multitud de puntos.

- Redes *adhoc*
    - Redes de igual a igual. De gran utilidad para asociaciones eventuales de equipos, donde no es necesario disponer de una gran infraestructura.

3.4. Requisitos

Para garantizar una cierta calidad de comunicaciones, debemos contar con una serie de requisitos, además de los que se utilizan en las *LAN* cableadas:

- Rendimiento: el protocolo de acceso al medio debe haces uso eficiente del medio no guiado para maximizar la capacidad de la red.

- Número de nodos: uso de varias celdas para dar cobertura total en un área.

- Conexión a la *LAN* troncal: adaptación a la *LAN* cableada.

- Área de servicio típico: 100 a 300 metros

- Consumo de baterías: es inapropiado el uso de protocolo MAC que precise de nodos móviles para supervisar constantemente los puntos de acceso o realizar comunicaciones frecuentes con una estación base.

- Robustez en la transmisión y seguridad: se debe garantizar el aislamiento respecto a interferencias y escuchas.

- Funcionamiento de red ordenada: es inadecuada la superposición de redes y el uso indebido de éstas.

- Funcionamiento sin licencia: entre los usuarios prima la utilización de servicios libres.

- Sin intervención: el protocolo MAC de las *LAN* inalámbricas debe permitir al cliente desplazarse de una celda a otra.

- Configuración dinámica: permitir modificaciones, traslado y ampliación sin afectar a otros usuarios.

3.5. Seguridad

Cuando hablamos de una red inalámbrica en la que los datos se transfieren a través del espacio radioeléctrico, nos encontramos con un medio accesible por cualquier persona, por lo tanto deberemos tener en cuenta la necesidad de implementar una serie de medidas y directivas de seguridad con el fin de garantizar la integridad de los datos que viajan por la red.

En primer lugar cabe reflejar la idea de que un medio compartido se traduce en un recurso con ciertos riesgos de vulnerabilidad. Así como en las redes cableadas se ve comprometida la seguridad de las redes mediante *sniffers*[9], en las redes sin cables nos encontramos con este mismo problema, agravado por la naturaleza del enlace, ya que en éstas el atacante no precisa de una conexión física a la red para descubrir, alterar o borrar datos.

Para evitar este tipo de intrusiones en la red se han creado una serie de medidas protectoras que garantizan la seguridad de los datos que enviamos. Estas medidas consisten en la autenticación de usuarios para acceder a los recursos o la encriptación de la información transmitida.

Veremos que no todos las protecciones son tan seguras como se puede pensar de buenas a primeras. Para demostrarlo, realizamos una serie de pruebas que reflejan la vulnerabilidad de estos sistemas. Esto nos ayudará a proteger la red de forma más eficiente y a la vez entender los puntos débiles que presentan los medios.

3.5.1. Sistemas vulnerables

Se listan sistemas de seguridad de los cuales ha sido demostrada su vulnerabilidad. Es decir, pueden ser atacados para lograr intrusiones y así desestabilizar la integridad de los datos.

[9] *Analizadores de protocolos. Programas como Etherpeek o Ethereal son capaces de mostrar el contenido de las tramas generadas en una red.*

- *Service Set Identifier (SSID):*
  - Se utiliza para segmentar redes inalámbricas.
  - Para que los equipos puedan comunicarse con los servidores, puntos de acceso y otos dispositivos deben compartir el mismo SSID.
  - Es vulnerable, ya que cualquiera puede obtener el identificador SSID de una red escuchando el medio.
  - Especialmente vulnerable por los *stumblers*.
    - Se escucha el medio.
    - Se obtiene identificador SSID.
    - Atacante se identifica con el SSID.
  - Solución: deshabilitar las tramas de broadcast con el SSID de la red.

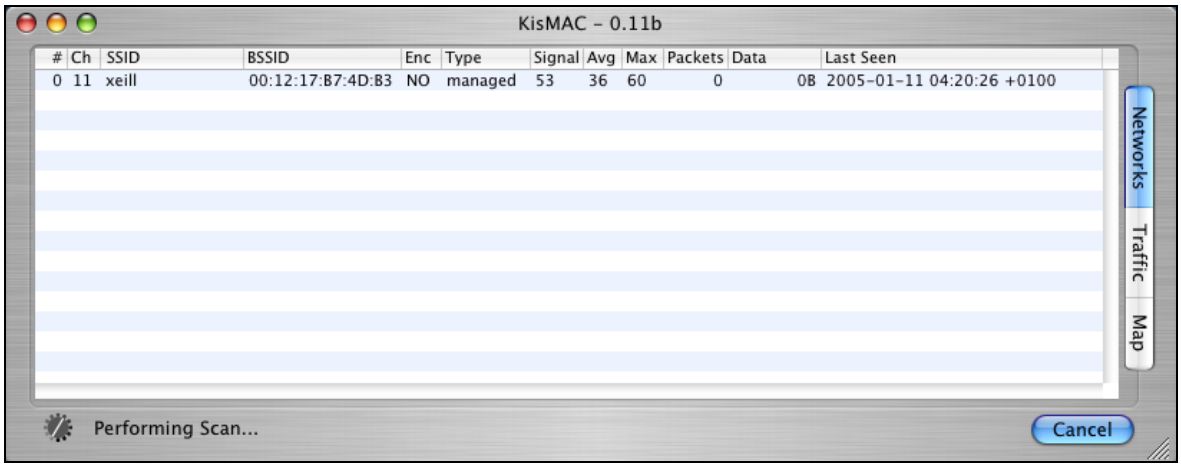


Figura 10: Utilización de un *stumbler* para descubrir el SSID de la red y conecarnos a ella

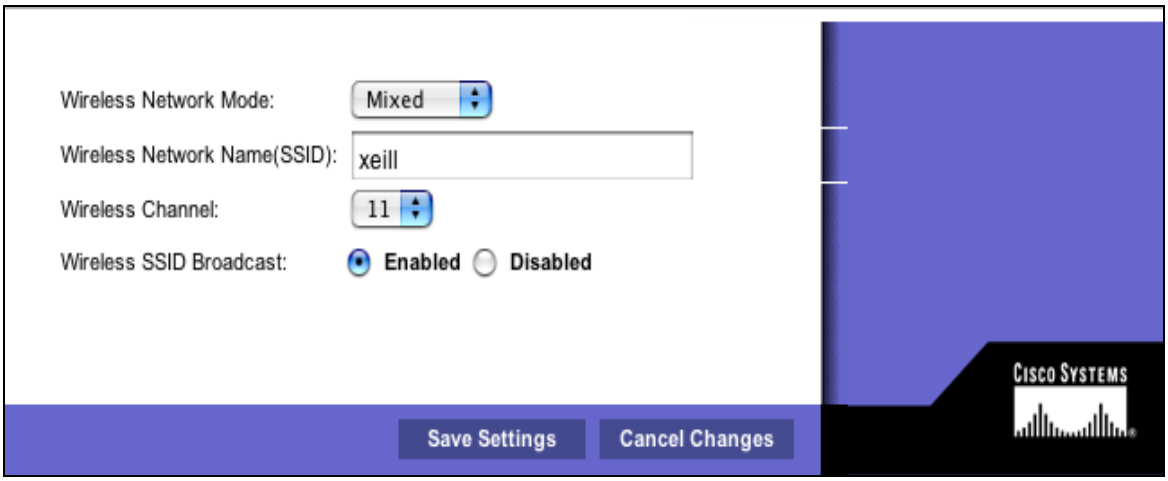


Figura 11: Deshabilitación del *broadcast* SSID

- Filtrado de direcciones MAC (dirección física del equipo):
  - El punto de acceso dispone de una lista de direcciones MAC con las que aceptar la comunicación. Rechaza la conexión de equipos con direcciones física no listadas.
  - Fácilmente vulnerable:
    - El atacante escucha el medio.
    - Mediante un *sniffer* consigue la dirección MAC del cliente.
    - El atacante cambia su propia dirección MAC por la del cliente.
    - El punto de acceso acepta la conexión.
  - Solución: utilizar algoritmos de encriptación entre cliente y punto de acceso.

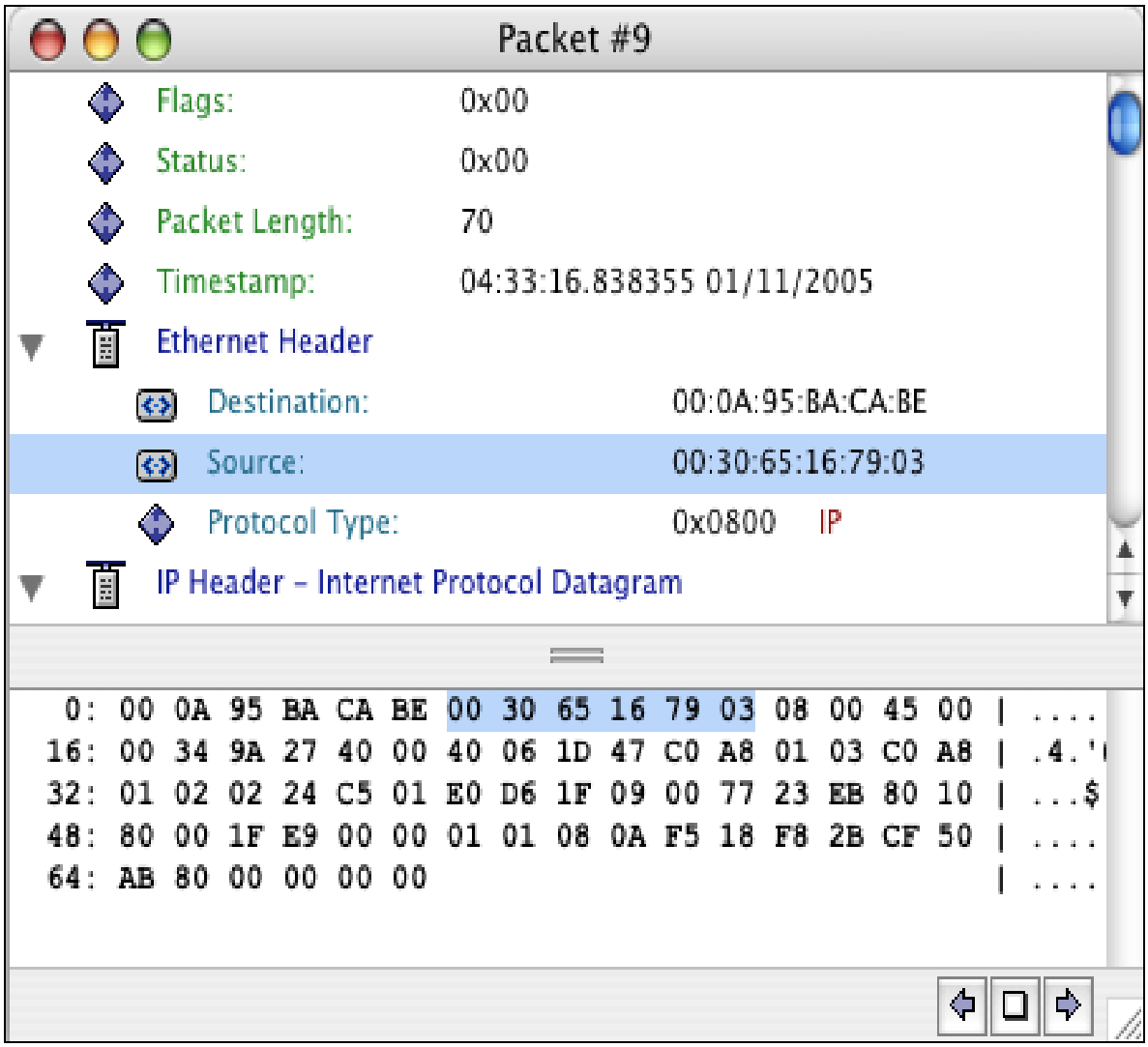


Figura 12: Obtención de la MAC de un cliente para ser clonada posteiormente

- *Wired Equivalent Privacy (WEP)*
  - Proporciona encriptación i autenticación en el estándar 802.11.
  - Utiliza un algoritmo de encriptación como clave o una secuencia de números que proporciona el usuario.
  - Cliente y servidor se configuran con la misma clave.
  - Longitud de la clave: 40 a 128 bits.
  - Vulnerable:
    - Atacante escucha las transmisiones de una red.
    - Utiliza herramientas como AirSnort que pueden llegar a descubrir las claves de encriptación en unas cuantas horas o días.
  - Solución: utilizar sistemas de seguridad adicionales.

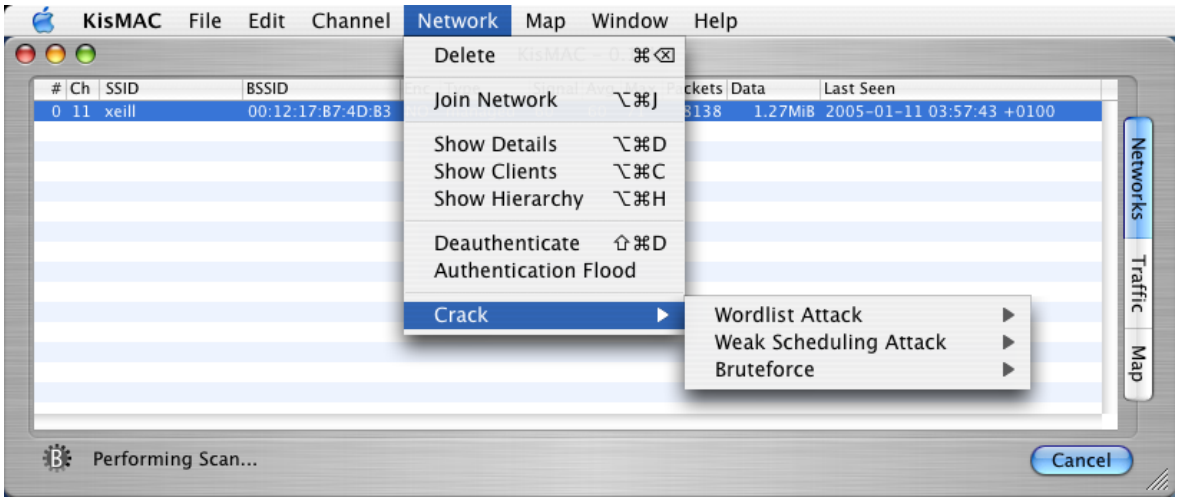


Figura 13: Métodos para conseguir contraseñas encriptadas.

3.5.2. Sistemas seguros

Nunca podemos hablar de un sistema totalmente seguro. Sin embargo, existen métodos con alto nivel de seguridad, cuya vulnerabilidad no ha sido demostrada o queda lejos de ser descubierta y/o utilizada por la gran mayoría de usuarios. Es el caso, por ejemplo, de los sistemas que se listan a continuación.

- 802.1x
  - Acceso controlado por puerto.
  - Utiliza características de la capa física de la infraestructura de la red para autenticar los dispositivos que se conectan a un puerto y no permitir el acceso al puerto cuando falla la autenticación
  - Utiliza claves dinámicas, en lugar de las claves estáticas de WEP.
  - Funcionamiento:
    - El cliente contacta con el punto de acceso (en adelante AP: *Access Point*).
    - El AP contacta con el servidor *RADIUS*[10].
    - El servidor *RADIUS* verifica los credenciales del cliente para verificar si está autorizado a acceder a la red.
    - El AP y el servidor *RADIUS* se comunican mediante el Protocolo Extensible de Autorización (*EAP*)[11]. Un protocolo punto a punto que soporta múltiples métodos de autenticación.

- WiFi *Protected Access (WPA)*
  - Mejoras de seguridad establecidas por el IEEE, identificándolo como 802.11i
  - Se implementa como avance del futuro del 802.11i.
  - Es una actualización de software para los equipos que usan WiFi.
  - Corrige las vulnerabilidades conocidas de WEP.
  - Combina la funcionalidad de 802.1x con el Protocolo de Integridad de Clave Temporal (TKIP). Éste último corrige las vulnerabilidades de las claves estáticas WEP:
    - Genera rápidamente claves utilizando una nueva encriptación cada 1000 paquetes.
    - Utiliza una función de mezcla para criptografiar los vectores de inicialización de los paquetes de datos con la clave compartida
    - Incorpora integridad de los mensajes comprobando la identificación alterada de los paquetes

[10] *Remote Authentication Dial-In Service. Más adelante veremos con más detalle su funcionamiento.*
[11] *Extensible Authentication Protocol. Permite establecer pasarelas de autenticación entre RADIUS y un punto de acceso.*

  - Basado en el mismo algoritmo RC4[12] con claves de 40 bits utilizando WEP.

- 802.1x + TKIP permite implementar redes WiFi con privacidad e integridad en las transmisiones de datos

- VPN *(Virtual Private Network)*
  - Permite a los usuarios de redes públicas y/o no protegidas establecer una conexión segura a una red privada.
  - Protege la red WiFi creando un túnel que protege los datos impidiendo el acceso a posibles usuarios no autorizados.
  - Muy utilizado en intranets corporativas por su seguridad.
  - Muy alto nivel de seguridad utilizando mecanismos como IPSec[13] *(Internet Protocol Security)*.
  - Utiliza algoritmos de encriptación fuerte como DES[14] *(Data Encryption Standard)* i 3DES[15] *(Triple DES)* para encriptar datos, con otros algoritmos para autenticar los paquetes de datos.
  - Utiliza certificados digitales para validar claves públicas
  - En las comunicaciones inalámbricas, las redes privadas virtuales se encargan de la autenticación, la encapsulación y la encriptación.
  - La utilización de IPSec, 802.11 y WEP de forma conjunta ofrece una solución práctica, escalable y fiable para una red WiFi.
  - El uso de *VPN* y cortafuegos proporciona aislamiento efectivo entre redes inalámbricas y corporativas.

[12] *Llave de cifrado con longitud variable orientada a operaciones de byte. Se utiliza un algoritmo de permutación al azar.*
[13] *Conjunto de protocolos que soportan intercambio seguro de paquetes en la capa IP.*
[14] *Método de cifrado ampliamente utilizado. Utiliza una llave privada.*
[15] *Modo del método DES que aplica la encriptación 3 veces.*

4. XEiLL

4.1. ¿Qué es?

La XEiLL, acrónimo de *Xarxa Educativa i Lliure* (en castellano, Red Educativa y Libre), se basa en un medio de comunicación telemático, integrado principalmente por la comunidad de instituciones y personas relacionadas con la enseñanza. La red está basada en el acceso gratuito y libre para los usuarios.

Actualmente, la XEiLL es un proyecto en constante expansión que cuenta con la colaboración y participación de importantes entidades como Toshiba y varios centros educativos de Santa Coloma de Gramenet y Badalona.

Gracias a este importante soporte, el énfasis de su impulsor y el soporte de muchas otras personas, la señal de esta red se extiende casi en la totalidad de la ciudad e interconecta la mayoría de instituciones educativas.

4.2. ¿Cómo nació?

Esta red nace en el año 2003 de la mano de Víctor Carceler, profesor titulado del Instituto de Enseñanza Secundaria Puig Castellar, creador e impulsor de ésta.

4.3. Objetivos

Los objetivos de la XEiLL son:

- Constituir una red telemática de libre acceso y con fines educativos.
    - A diferencia de otras redes inalámbricas, la XEiLL no se centra en la cobertura y expansión de un territorio concreto. La red fue creada para ofrecer contenidos educativos libres mediante tecnología inalámbrica, sin pensar en barreras geográficas.

- Explorar el uso de las tecnologías de la información y comunicación en la educación.
    - La implementación de un sistema abierto como este permite experimentar las posibilidades que ofrece el mundo tecnológico, enseñando así a profesores y alumnos la utilidad de éste.

- Fomentar la colaboración entre centros educativos.
    - La unión de centros para el desarrollo continuo de esta tecnología proporciona un vínculo de desarrollo común, fomentando así las relaciones entre las diferentes instituciones educativas.

- Acercar los centros educativos a su entorno social.
    - El desarrollo de actividades conjuntas propicia un beneficioso acercamiento de la población al ámbito educativo. Actualmente, este proyecto hace real un acercamiento de la sociedad al ámbito educativo.

- Divulgar el uso de las nuevas tecnologías.
    - Contando siempre con la más novedosa tecnología, el desarrollo de actividades sociales como esta, hace conocedoras a muchas personas de las posibilidades que ofrece el uso de las comunicaciones y los sistemas.

- Evitar situaciones de exclusión social.
    - Cuando hablamos de una red libre, hacemos alusión a un sistema de comunicaciones utilizable por cualquier usuario que lo pretenda, sin dejar fuera de este conjunto a ningún colectivo. El objetivo es poner al alcance de cualquier persona el uso de nuevas tecnologías.

- Servir como experiencia didáctica motivadora para los alumnos de ciclos formativos de familias relacionadas con las tecnologías de la información y la comunicación.
    - La red es sinónimo de innovación tecnológica, permitiendo a los estudiantes poder formar parte de su desarrollo y con ello recibir una formación práctica y agradable.

4.4. Personas y organizaciones que forman la red

4.4.1. Mantenedores

Como se comenta en el apartado anterior, uno de los principales objetivos de la XEiLL es ofrecer una estimulación educativa para que los alumnos que cursan ciclos formativos trabajen y aprendan con las nuevas tecnologías. Es por ello que la instalación y adecuación de la infraestructura de red la realizan éstos.
Entre otras tareas, son los encargados de realizar la instalación de nuevos nodos y sus servicios, utilizando los conocimientos adquiridos en las clases teóricas.

Tanto el planteamiento inicial como la proyección de nuevas implementaciones son dirigidas por su fundador. Éste vela por el correcto desarrollo del cometido de la red y vela por su correcto mantenimiento.

4.4.2. Centros adheridos

Actualmente colaboran voluntariamente 5 centros educativos, que mantienen los nodos instalados en sus dependencias y gestionan los servicios que éstos proporcionan.

- CEIP Torre Balldovina
- CEIP Rafael Casanova
- IES La Bastida
- IES Puig Castellar
- IES Terra Roja
-

4.4.3. Entidades

Afortunadamente, el proyecto cuenta con la colaboración de Toshiba®. Dicha empresa proporciona el material necesario para realizar las instalaciones de los nodos.
Con esta participación se sufragan los gastos económicos derivados de la puesta en marcha y mantenimiento de la red.

4.5. Características

La red telemática se basa en la utilización de tecnología inalámbrica para su implantación. Esto supone un gran abanico de posibilidades libres de ataduras físicas como el cableado, pero cuenta con ciertas limitaciones de alcance.

En la construcción de la red se utilizan dispositivos de ámbito doméstico, tales como *routers* WiFi de gama media. No por ello se restringe la utilidad y fiabilidad de éstos, ya que en la actualidad existen elementos de red con elevadas prestaciones a un coste aceptable por el usuario doméstico.

Los nodos se instalan en equipos PC habituales, sin características y ampliaciones especiales, a excepción de los servidores *proxy* que disponen de 2 tarjetas de red para enlutar el tráfico en 2 interfaces.
El sistema operativo elegido es la distribución *Mandrake Linux 10.1*. Se utiliza éste por tratarse de una versión libre de *Linux* que ofrece soporte gratuito a los usuarios.

Para la expansión de la señal se emplean antenas directivas (en el caso de enlaces WDS) y omnidireccionales (para implementar el modo infraestructura). Podemos encontrar los dispositivos empleados en comercios de electrónica e informática, o incluso construir nuestra propia antena comprando los materiales en una tienda de bricolaje.

Las instalaciones, siempre que sea posible, se realizan en centros educativos, fomentando así la divulgación tecnológica en la educación y el aprendizaje de los alumnos.

En un futuro está prevista la instalación de nodos en centros sociales con el fin de propiciar una mayor expansión de la señal y un útil aprovechamiento de los equipamientos públicos, sin generar ningún tipo de costes a éstos.

Para el acceso a la red, únicamente es necesario disponer de un equipo cliente con capacidad de comunicación inalámbrica. Por ejemplo, una PDA WiFi o un ordenador portátil con una interficie de red inalámbrica (tarjeta PCMCIA, USB, …).
El usuario debe situarse en una zona de cobertura, donde llegue la señal de la XEiLL. Cuando más cerca de un nodo se sitúe mejor será la calidad de la conexión, ya que se recibirá la señal con más potencia, traduciéndose en una ancho de banda mayor.

El propósito de esta red radica en poner la tecnología al alcance de cualquier usuario. Sin embargo, en muchas ocasiones nos encontraremos con zonas donde la densidad de población es mínima. En estos casos cabe esperar una puesta en marcha ligeramente más tardía respecto a las zonas más pobladas.

4.5.1. Estructura física

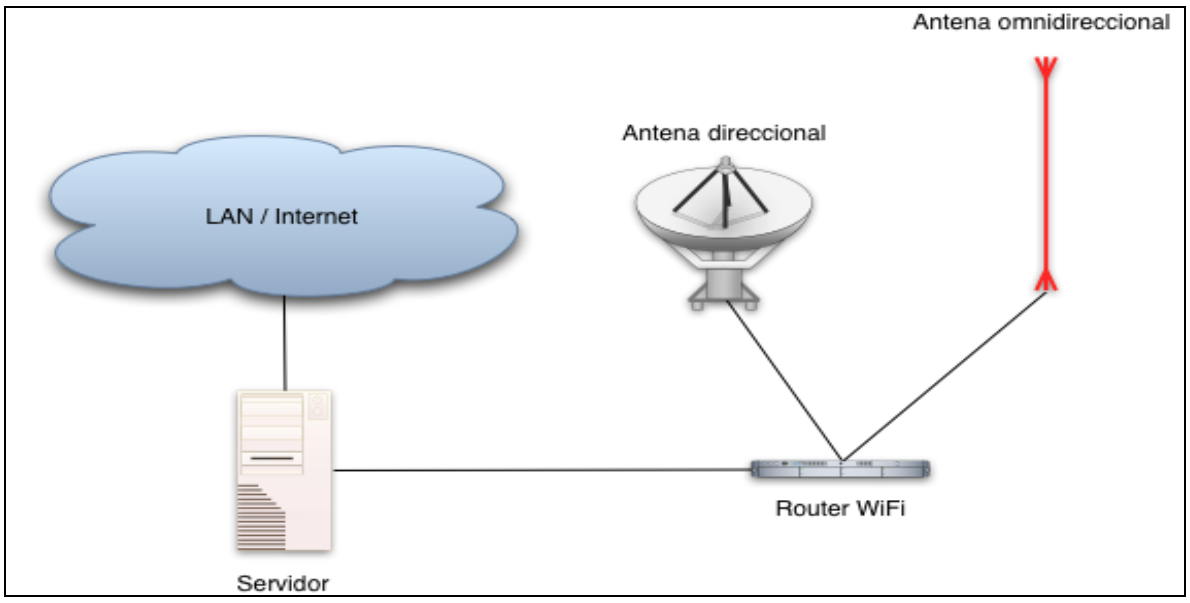


Figura 14: Estructura de básica de los nodos

Como se puede apreciar en la figura superior, los nodos están formados de forma muy simple, utilizando los siguientes elementos:

- Servidor:
  - Equipo PC doméstico.
    - Funciones implementadas:
      - Proxy
      - Servidor de contenidos / servicios
      - Otros
    - Incorpora 2 interfaces de red
      - Enlace a red de área local y/o Internet
      - Enlace al Router WiFi
- Router WiFi
- Antena omnidireccional
- Antena direccional (aquellos casos en los que exista enlace WDS)

4.5.2. Topología de red

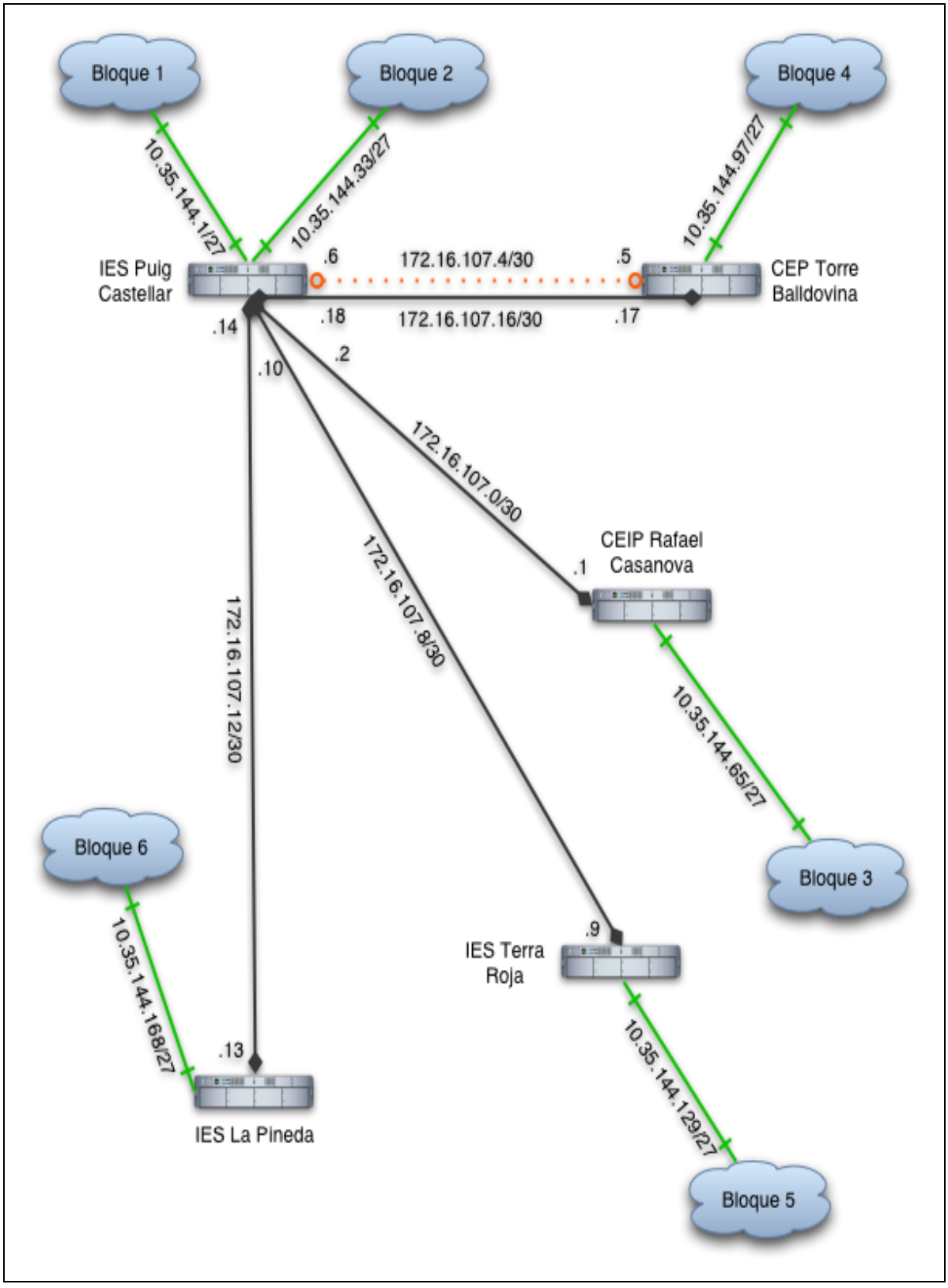


Figura 15: Topología actual de la XEiLL

4.5.3. Dimensionado IP

- IPs PUBLICAS:

  Direcciones estáticas. Utilizadas para crear los enlaces entre los diferentes centros.

  - 172.16.107.0/30: Enlace VPN IES Puig Castellar - CEIP Rafael Casanova
    - 172.16.107.1: CEIP Rafael Casanova
    - 172.16.107.2: IES Puig Castellar
  - 172.16.107.4/30: Enlace WDS IES Puig Castellar - CEP Torre Balldovina
    - 172.16.107.5: CEP Torre Balldovina
    - 172.16.107.6: IES Puig Castellar
  - 172.16.107.8/30: Enlace VPN IES Puig Castellar - IES Terra Roja
    - 172.16.107.9: IES Terra Roja
    - 172.16.107.10: IES Puig Castellar
  - 172.16.107.12/30: Enlace VPN IES Puig Castellar - IES La Pineda
    - 172.16.107.13: IES La Pineda
    - 172.16.107.14: IES Puig Castellar
  - 172.16.107.16/30: Enlace VPN IES Puig Castellar - CEP Torre Balldovina
    - 172.16.107.17: CEP Torre Balldovina
    - 172.16.108.18: IES Puig Castellar

- IPs PRIVADAS:

  Direcciones dinámicas. Asignadas a los equipos clientes que conectan con la XEiLL.

  - 10.35.144.1/27: Bloque Clientes 1: IES Puig Castellar
  - 10.35.144.33/27: Bloque Clientes 2: IES Puig Castellar
  - 10.35.144.65/27: Bloque Clientes 3: CEIP Rafael Casanova

- 10.35.144.97/27: Bloque Clientes 4: CEP Torre Balldovina
- 10.35.144.129/27: Bloque Clientes 5: IES Terra Roja
- 10.25.144.168/27: Bloque Clientes6: La Pineda

4.6. Implementación

4.6.1. OSPF

En primer lugar, a la hora de interconectar los diferentes equipos, debemos tener en cuenta la utilización de un protocolo de encaminamiento. Esto permitirá hacer llegar los datos desde un punto de la red hasta otro extremo.

Una posibilidad es la utilización de RIP[16] (*Routing Information Protocol*) para encaminar los datos. Este protocolo fue descartado ya que transmite su tabla de encaminamiento completa y a medida que crece la red, se genera más tráfico.

OSPF (*Open Shortest Path First*) utiliza un algoritmo de encaminamiento de estado del enlace, en el cual cada dispositivo mantiene las descripciones del estado de sus enlaces locales a las redes y periódicamente transmite información de estado actualizada a todos los dispositivos de encaminamiento de los que tiene conocimiento.

El tráfico que se genera es mínimo ya que las descripciones de los enlaces son pequeñas y raramente se tienen que enviar. Cuando un dispositivo de encaminamiento recibe un paquete de actualización lo confirma al emisor.

Para trazar la ruta de envío, OSPF calcula una ruta a través del conjunto de redes que suponga el menor coste de acuerdo a una métrica configurable por el usuario.

[16] *Protocolo de encaminamiento que envía mensajes de actualización de ruta a intervalos regulares y cuando la red cambia..*

4.6.2. VPN *(Virtual Private Networks)*

La utilización de redes privadas virtuales permite establecer una red entre clientes que se encuentran geográficamente separados, de manera que para el usuario final sea transparente y pueda tener la percepción de una topología local.

De este modo, es posible interconectar los nodos que forman la XEiLL como si de una única *LAN* se tratase, adquiriendo una serie de valores que respaldan su seguridad y desarrollo:

- Privacidad en las aplicaciones TCP/IP. Acceso seguro a clientes remotos.
- Encriptación de datos. Transparente hacia el usuario final.
- Ofrece movilidad a los clientes.
- Permite ampliar y escalar las redes.

A continuación podemos ver los protocolos más utilizados para crear VPNs:

- *Point-to-Point Tunneling Protocol* (PPTP)[17]
    - Permite que el tráfico IP, IPX o NetBEUI sea encriptado y encapsulado en encabezados IP como Internet.
    - Fue creado por Microsoft pero existen versiones para Linux.

- *Layer 2 Tunneling Protocol (L2TP)*[18]
    - Proporciona encriptación y envío de tráfico IP e IPX sobre cualquier medio que soporte entrega de datagramas punto-a-punto (IP, X.25, FrameRelay, ATM, etc.)

- *IP Security (IPSec) Tunel Mode*[19]
    - Los paquetes IP son encriptados y encapsulados en encabezados IP para ser enviados a través de una red pública IP.

[17] *Protocolo de tunelado punto a punto.*
[18] *Protocolo de tunelado de capa 2.*
[19] *Modo tunelado de seguridad IP.*

4.6.3. WDS *(Wireless Distribution System)*

Podemos interconectar varios puntos de acceso inalámbricos en la misma red mediante la tecnología WDS. Para ello se ha definido un formato especial de paquete que implementado por el sistema de distribución inalámbrico.

Para crear los enlaces haremos lo siguiente:

- Crear una interfaz wds (en ambos casos serán wlan0wds0) enlazándola con la MAC del otro punto de acceso.

```
iwpriv wlan0 wds_add xx:00:00:00:00:00
```

- Configurarla la IP en 0.0.0.0

```
ifconfig wlan0wds0 0.0.0.0
```

- Agregar dicha interfaz al bridge.

```
brctl addif br0 wlan0wds0
```

Una vez hecho esto, podemos comprobar la actualización del puente en cada equipo:

```
wlan0     IEEE 802.11-b  ESSID:"xeill"
          Mode:Master  Frequency:2.437GHz  Access Point: 00:50:C3:04:72:21
          Bit Rate:11Mb/s   Tx-Power:7 dBm   Sensitivity=1/3
          Retry min limit:8   RTS thr:off   Fragment thr:off
          Encryption key:XXXXXXXXXXXXXXXXXX   Encryption mode:restricted
          Power Management:off
          Link Quality:0  Signal level:0  Noise level:0
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
```

```
        Tx excessive retries:1907  Invalid misc:1540   Missed beacon:0

wlan0wds  IEEE 802.11-b  ESSID:"xeill"
        Mode:Master  Frequency:2.437GHz  Access Point: 00:50:C3:04:72:21
        Bit Rate:11Mb/s   Tx-Power:7 dBm   Sensitivity=1/3
        Retry min limit:8   RTS thr:off   Fragment thr:off
        Encryption key: XXXXXXXXXXXXXXXXXX   Encryption mode:restricted
        Power Management:off
```

4.7. Servicios activos

4.7.1. Web

El servidor web más estable y extendido es *Apache* ya que ofrece una herramienta potente, flexible y ajustado a los nuevos estándares.

Se ejecuta en diversas plataformas operativas tales como: Windows 9x/NT/2000/ME, Macintosh, Novell NetWare, OS/2, Linux y la mayoría de los Unix existentes: IRIX, Solaris, HPUX, SCO, FreeBSD, NetBSD, AIX, Digital Unix, etc.

Para la instalación en los servidores Linux de la XEiLL podemos instalar el paquete de forma simple utilizando apt-get.

```
apt-get apache apache-manual
```

Esto nos instalará el servidor y la documentación.

A partir de aquí, tenemos el servidor instalado con la configuración por defecto. Para iniciar el demonio de *apache* simplemente hay que lanzar el script *httpd.* A continuación podemos ver su funcinalidad:

```
# service httpd stop
   Stopping httpd:                    [  OK  ]

# service httpd start
   Starting httpd:                    [  OK  ]

# service httpd status
   httpd (pid 6973 6972 6971 6970 6969 6968 6967 6966 6963) is running...

# service httpd reload
   Reloading httpd:                   [  OK  ]
```

Se pueden cambiar las diferentes opciones de configuración y activar módulos nuevos editando el fichero /etc/httpd/httpd.conf

El acceso a cada directorio del servidor se puede regular en un fichero, contenido en el mismo directorio o en sus antecesores, cuyo nombre por defecto es `.htaccess.`

4.7.2. *Jabber*

Más conocido como "el cliente de mensajeria instantanea de *Linux*", es un proyecto de código abierto que permite incluir otras alternativas como AIM, ICQ, MSN o Yahoo. Formado por un conjunto de protocolos XML y tecnologías que permiten a dos entidades de Internet intercambiar mensajes, presencia y otra información estructurada en tiempo real.

Para instalar el servicio hay que seguir los siguientes pasos:

- Descargar Jabberd 2 en http://www.jabberstudio.org/projects/jabberd2/releases/download.php?file=jabberd-2.0s6.tar.gz.

- Descomprimir el fichero.

```
tar -zxvf jabberd-2.0s3.tar.gz
```

- Configurar la instalación con soporte para MySQL (por defecto).

```
cd jabberd-2.0s3
./configure
```

- Construir Jabberd.

```
make
```

- Instalar Jabberd.

```
su
make install
```

Una vez completada la instalación, nos encontramos con la siguiente estructura:

/usr/local/etc/jabberd	Ficheros de configuración de Jabberd
/usr/local/bin	Ficheros binarios (jabberd, c2s, resolver, router, s2s, sm)

- Cambiar permisos de los ficheros creados.

```
chown -R root:jabber /usr/local/etc/jabberd/*
chmod -R 640 /usr/local/etc/jabberd/*
```

- Añadimos el nombre del *host* servidor en el fichero de configuración sm.xm1.

```
<!-- Session manager configuration -->
    <sm>
    <id>nodo1.xeill.net</id>
```

- Añadimos el identificador local en el fichero de configuración c2s.xm1.

```
<!-- Local network configuration -->
    <id>nodo1.xeill.net</id>
```

- Configurar la base de datos.

```
mysql -u root -p
mysql>\. db-setup.mysql
```

- Dar permisos a la base de datos, cambiando la contraseña por defecto por la elegida.

```
GRANT select,insert,delete,update ON jabberd2.*
    to jabberd2@localhost IDENTIFIED by 'contraseña';
```

- Crear link simbólico al socket utilizado por Jabberd2.

```
ln -s /var/lib/mysql/mysql.sock /tmp/mysql.sock
```

- Incluir el *driver* para el almacenamiento y la configuración de acceso a MySQL en sm.xml.

```
<!-- Storage database configuration -->
 <storage>
<driver>mysql</driver>
<!-- MySQL driver configuration -->
    <mysql>
      <!-- Database server host and port -->
      <host>localhost</host>
      <port>3306</port>

      <!-- Database name -->
      <dbname>jabberd2</dbname>

      <!-- Database username and password -->
      <user>jabberd2</user>
      <pass>contraseña</pass>

      <!-- Transaction support. If this is commented out, transactions
           will be disabled. This might make database accesses faster,
           but data may be lost if jabberd crashes.

           This will need to be disabled if you are using a MySQL
           earlier than v3.23.xx, as transaction support did not appear
           until this version. -->
      <transactions/>
    </mysql>
```

4.7.3. Mirror FTP

Un *mirror* FTP nos permitirá poner al alcance los usuarios ficheros que distribuyen otros servidores, expandiendo así la capacidad de localización.

Para realizar la instalación seguiremos los siguientes pasos:

- Descargar la última versión de *mirror* en ftp://sunsite.org.uk/packages/mirror/mirror.tar.gz.

- Descomprimir el fichero.

```
tar –xzvf mirror.tar.gz
```

- Ejecutar la instalación.

```
perl install.pl here
```

- Editar el fichero mirror.defaults con nuestra configuración.

```
hostname: nodo1.xeill.net
local_dir: /
remote_password: PFC
mail_to: tedi.roca@gmail.com
```

- Crear un fichero con el nombre del sitio FTP a replicar, dentro del directorio *packages*.

```
pico packages/ftp.ejemplo_pfc.com
```

- Editar el fichero con la configuración para cada sitio FTP.

```
package=<ejemplo_PFC>
        comment=<ejemplo de mirror para el PFC>
        site=ftp.ejemplo_PFC.com
        remote_dir=/pub
        local_dir=/public/Mirrors/ftp.ejemplo_PFC.com/pub
```

- Lanzar el demonio.

```
mirror -d packages/ftp.ejemplo_pfc.com
```

4.7.4. DNS

El servidor DNS *(Domain Name Service)* se utiliza para resolver direcciones de Internet. Su función es transformar los nombres de *hosts* en direcciones IP cuando se envía una solicitud.

El servicio está instalado en una máquina central de la red, donde el resto de *hosts* solicitan la resolución de direcciones. Si éste no es capaz de resolver la dirección con su propia lista, lo solicita a otros servidores externos. Con este servicio, dotamos de capacidad propia a la red para asignar y resolver los nombres de los *hosts* que la forman sin necesidad de recurrir a elementos externos.

Se detalla brevemente los pasos a seguir para implementar el servicio:

Nota: se da por supuesto que el lector conoce los métodos de descarga e instalación de paquetes, así como su compilación y otras tareas de mantenimiento del sistema.

- Descargar el paquete correspondiente a la distribución de *Linux* utilizada, en nuestro caso *Mandrake Linux 10.1*.

- Instalar el paquete.

- Modificamos el archivo */etc/named.conf* con la configuración para nuestra instalación.

- Cambiamos los permisos de lectura y escritura para el archivo */etc/rndc.key* y el directorio */var/named.* Únicamente el usuario *named* deberá tener acceso a ellos.

- Modificamos el archivo de definición para las zonas: */var/named/named.root*. En él se listan los principales servidores de DNS de Internet, a los que recurrirá nuestro servidor en caso de no encontrar ninguna entrada en la lista interna que definiremos.

- En el directorio */var/named* creamos los archivos de zonas que hemos definido previamente en la configuración. El nombre de estos ficheros debe coincidir con los especificados anteriormente.

- Incluimos el demonio */etc/named* para que se ejecute al iniciar el sistema.

5. Servicios y otras implementaciones propuestas

El futuro de la XEiLL depende en gran medida de los servicios que ésta ofrezca. Se listan una serie de servicios e implementaciones propuestas, con el fin de ofrecer al usuario un abanico de posibilidades tecnológicas.

5.1. Streaming: VideoLan Server

Para llevar a cabo la futura implantación de este servicio se han realizado numerosas pruebas con diferentes tipos de hardware y software. El motivo de tan laboriosa tarea de investigación es la sobrecarga en la red que puede conllevar una incorrecta instalación del servicio, ya que como bien es sabido, éste consume gran ancho de banda.

Ante las posibles alternativas, nos encontramos con Darwin Streaming Server, el que ha sido software por excelencia para streaming durante mucho tiempo. A la hora de utilizarlo se plantearon una serie de contrapuntos, entre los que cabe destacar la dificultat de gestión del servicio, fallos de seguridad o necesidad de utilizar software propietario para "adaptar" los clips, que hicieron tomar el paquete VideoLan Server como la alternativa perfecta. Las razones que llevaron a elegir este software frente a otros son:

- Sencillez en la instalación y administración del servidor.
- Posibilidad de realizar streaming de todos los formatos de vídeo actuales.
- Varias fuentes de entrada: dvd, archivos, cámara de vídeo, TV, …
- Se puede enviar la información mediante UDP, RTP u otros.

Se propone la instalación de un servidor autónomo e independiente en cada centro de la XEiLL, ya que se augura un uso local para transmitir eventos del propio centro. Sin embargo también se contempla la utilización de servidores únicos para transmitir streaming a toda la red.

Los pasos seguidos para realizar la instalación en el nodo de pruebas son:

- Accedemos al sitio *http://www.videolan.org/streaming/download-vls-sources.html* y descargamos los suiguientes archivos:

  - Fuentes del servidor:
    - vls-0.5.6.tar.gz

  - Librerias necesarias:
    - libdvbpsi3-0.1.4.tar.gz (librería de tablas MPEG TS y DVB PSI)
    - libdvdcss-1.2.8.tar.gz (librería de desciframiento de DVD)
    - libdvdread-0.9.4.tar.gz (libería para lectura de DVD)
    - libdvb-0.2.2.tar.gz (Librería DVB)

- Descomprimimos todos los ficheros:

```
tar –zxvf vls-0.5.6.tar.gz
tar –zxvf libdvpsi3-0.1.4.tar.gz
tar –zxvf libdvdcss-1.2.8.tar.gz
tar –zxvf libdvdread-0.9.4.tar.gz
tar –zxvf libdvb-0.2.2.tar.gz
```

- Copiamos las fuentes al directorio /usr/local/src/

```
mv vls-0.5.6 /usr/local/src/
mv libdvpsi3-0.1.4 /usr/local/src/
mv libdvdcss-1.2.8 /usr/local/src/
mv libdvdread-0.9.4 /usr/local/src/
mv libdvb-0.2.2 /usr/local/src/
```

- Dentro de cada una de las carpetas que hemos movido, realizaremos la compilación de las fuentes de la siguiente manera:

```
./configure
make
```

- Ahora que tenemos el servidor de streaming y las librerias instaladas, procederemos a configurar VideoLan Server, ediando el fichero vls.cfg. Para ello haremos lo siguiente:

```
pico /usr/local/etc/videolan/vls/vls.cfg
```

- Básicamente utilizaremos la configuración por defecto, ya que las opciones que nos interesan vienen activadas por defecto:

- Log de actividad almacenado en el fichero vls.log.
- Puerto 9999 abierto para la administración mediante telnet.
- Declaración de fuentes.

- Cambiaremos el password de los usuarios en:

```
BEGIN "Users"
        Admin.      =      3BcKWoiQn0vi6:PFC
END
```

De esta forma especificaoms el usuario "admin" con password "PFC" (previamente encriptado con *mkpasswd*. Junto al password se adjunta el grupo.

Una vez configurado comprobaremos el correcto funcionamiento. Para ello realizamos los siguientes pasos:

- Copiamos un clip al disco local del servidor y lo llamamos "prueba.mpg". Estará ubicado en: /var/streaming/movies/

- Lanzamos el servidor VLS, especificando el archivo a reproducir, la dirección destino y especificando la conexión UDP.

```
root@powerbuntu:/var/streaming/movies # vls -d udp:192.168.1.2
file:prueba.mpg
VideoLAN Server v 0.5.6 (Dec 31 2004) - (c)1999-2003 VideoLAN
Synchronised with PS stream
New Pid assigned: 80
PMT Add, PID : 0x80 , Type : 0x5
Synchronised with PS stream
New Pid assigned: 81
PMT Add, PID : 0x81 , Type : 0x5
New Pid assigned: 82
Video: 0x82 , 130
PMT Add, PID : 0x82 , Type : 0x1
updating PCR_PID to value 130 (current pid = 0)
New Pid assigned: 83
Audio: 0x83 , 131
PMT Add, PID : 0x83 , Type : 0x3
```

- Desde un equipo cliente de la red probamos el servicio:

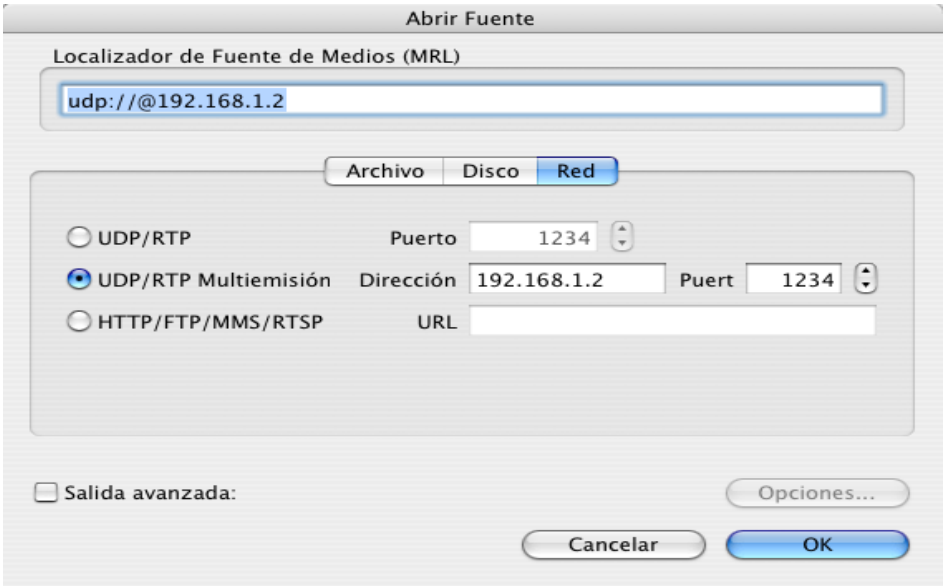


Ilustración 16: Cliente de *streaming*.

Figura 17: *Streaming* recibido por el cliente

5.2. IRC: ircd

5.3.
El servicio de IRC (Internet Relay Chat) ofrece comunicaciones de texto entre usuarios individuales o salas de chat. Con la implantación de este servicio se pretende dotar de un espacio de debate donde los usuarios puedan comunicarse en tiempo real.

Antes de probar esta aplicación en la red educativa se ha creído conveniente estudiar su comportamiento en una reproducción local con varios nodos interconectados.

A continuación se detallan los pasos seguidos en la instalación de cada nodo.

- Descargar las fuentes de ircd en:

http://www.irc101.org/files/?download=ircd/irc2.11.0.tgz

- Descomprimimos el archivo:

```
tar -zxvf ircd2.11.0.tgz
```

- Movemos la carpeta al directorio de fuentes:

```
mv ircd2.11.0 /usr/local/src
```

- Ejecutamos la configuración:

```
cd /usr/src/local/ ircd2.11.0/ppc-pc-linux-gnuoldld
./configure
```

- Compilamos el paquete:

```
make all
```

- Copiamos el fichero de ejemplo de configuración /usr/src/irc2.10.3/doc/example.conf a /usr/local/etc/ircd.conf

```
cp  /usr/local/ircd.conf.example /usr/local/etc/ircd.conf
```

- Editamos el archivo ircd.conf para introducir la configuración referente a nuestro servidor:

```
cd /usr/local/etc/
pico ircd.conf
```

Modificaremos las siguientes líneas:

M:<Server NAME>:<YOUR Internet IP#>:<Geographic Location>:<Port>:<SID>

En esta línea especificamos la descripción de la máquina, indicando el nombre del host donde está instalado el demonio, la dirección por donde se realizaran las conexiones (muy útil si tenemos varias interfaces), la situación geográfica y el SID (identificador único del nodo).

```
M:<nombre_nodo>:<ip_nodo>:<XEiLL - Xarxa Educativa i Lliure>:<6667>:SID
```

A:<Your Name/Location>:<Your Electronic Mailing Addr>:<other>::Network Name

A continuación incluimos la información administrativa de la red.

```
A:<XEiLL Spain>:IRC admin. XEiLL<tedi.roca@gmail.com>:::XEiLL
```

P:<Internet IP#>:<>:<Internet IP Mask>:<Port>:*

En esta línea incluimos el socket a utilizar para realizar la conexión al servidor. En nuestro caso, especificamos únicamente el puerto por defecto 6667. Otros detalles como la IP ya han sido especificados en líneas anteriores. Podríamos especificar diferentes puertos para diferentes interficies.
Comentaremos todas las líneas con parámetros de puertos y añadimos la siguiente:

```
P::::6667:
```

Y:<Class>:<Ping Frequency>:<Connect freq>:<Max Links>:<SendQ>::

Podemos definir los rangos en conexión. Debemos ajustar al máximo las frecuencias de control para no ser vulnerables a los ataques y detectar las sesiones fantasmas, sin llegar a exigir una elevada respuesta del cliente y servidor, ya que en momentos en los que la red estuviese ligeramente colapsada, podría romperse la conexión fácilmente. Utilizaremos los siguientes valores (optimizados):

```
Y:2:90:300:1:8000000
Y:10:90::100:512000:10:32
Y:11:90::100.51200:0.1:0.2
Y;12:90::100:512000:1:3
Y:13:90::100:512000:1:1
```

I:<TARGET Host Addr>:<Password>:<TARGET Hosts NAME>:<Port>:<Class>

El servidor admite autenticación de los clientes, de tal manera, que solo permitirá la conexión de éstos si se encuentran dentro del rango declarado, pudiendo especificar parámetros como los puertos utilizados, la dirección del host, contraseña, etc.
Ya que precisamos formar una red libre, permitiremos el acceso desde cualquier cliente añadiendo la línea que se muestra a continuación y comentando todas aquellas que comiencen por I:.

```
I:*@*::::
```

O:<TARGET Host NAME>:<Password>:<Nickname>:<Port>:<Class>

Tenemos la posibilidad de definir operadores locales, asignando los *hosts* y contraseñas a los que pertenecen, así como los puertos y clases.
Definimos el nick “troca” con password PFC para acceder como operador. La identificación se realizará al iniciar el cliente o bien escribiendo /oper troca PFC en la línea de comandos del cliente de IRC.

```
O:*@*:PFC:troca:::10
```

H:<servers witch are permitted entry:sid mask:hub server::

Especificamos que servidores serán designados HUBS y por lo tanto permitiran conexiones de otros servidores. En nuestro caso realizará esta función el nodo1

```
H:*::nodo1.XEiLL.net
```

** A partir de aquí la configuración del nodo variará dependiendo de si está configurado como hub o como cliente. A continuación se detallan ambas **

HUB:

C:<TARGET Host Addr>:<Password>:<TARGET Server NAME>:<TARGET PORT>:<Class>

Definimos los servidores a los que intentaremos conectar, de forma que creemos una red con varios nodos.
Añadiremos el resto de *hosts* que albergan servidores de IRC excepto el propio nodo.

```
C:192.168.1.4:PFC:nodo2.XEiLL.net::50
```

N:<TARGET Host Addr>:<Password>:<TARGET Server NAME>:<Domain Mask>:<Class>

Esta línea define que servidores permitiremos conectar a nuestro nodo.
Añadiremos el resto de *hosts* que albergan servidores de IRC excepto el propio nodo.

```
N:192.168.2.4:PFC:nodo2.XEiLL.net::50
```

LEAF:

```
C:192.168.2.3:PFC:nodo1.XEiLL.net:6667:30
N:192.168.2.3:PFC:nodo1.XEiLL.net::30
```

Finalmente ya solo nos queda comprobar el correcto funcionamiento del servicio. Para ello, desde un cliente de irc, nos conectamos a unos de los nodos. Se recibe la siguiente respuesta:

```
[22:15]     -!-   Looking up 192.168.1.4..
[22:15]     -!-   Connecting to 192.168.1.4 (192.168.1.4) port 6667..
[22:15]     -!-   Connected. Now logging in..
[22:15]     -!-   Please wait while we process your connection.
[22:15]     -!-   Welcome     to     the     Internet     Relay     Network
troca!~troca@192.168.1.2
[22:15]     -!-   Your host is nodo2.XEiLL.net, running version 2.11.0
[22:15]     -!-   This server was created jue dic 30 2004 at 21:16:22 CET
[22:15]     -!-   nodo2.XEiLL.net 2.11.0 aoOirw abeiIklmnoOpqrRstv
[22:15]     -!-   RFC2812     PREFIX=(ov)@+     CHANTYPES=#&!+     MODES=3
CHANLIMIT=#&!+:21   NICKLEN=9   TOPICLEN=160   KICKLEN=160   MAXLIST=beIR:42
CHANNELLEN=50  IDCHAN=!:5  CHANMODES=beIR,k,l,imnpstaqr  :are  supported  by
this server
[22:15]     -!-   PENALTY   FNC   EXCEPTS=e   INVEX=I   CASEMAPPING=ascii
NETWORK=XEiLL :are supported by this server
[22:15]     -!-   000BAAAAA :your unique ID
[22:15]     -!-   There are 3 users and 0 services on 2 servers
[22:15]     -!-   14 :channels formed
[22:15]     -!-   I have 2 users, 0 services and 0 servers
[22:15]     -!-   1 1 :Current local users 1, max 1
[22:15]     -!-   1 1 :Current global users 1, max 1
[22:15]     -!-   - nodo2.XEiLL.net Message of the Day -
[22:15]     -!-   - 30/12/2004 23:25
[22:15]     -!-   -  .=============================================.
[22:15]     -!-   -  :  Bievenid@ al servidor IRC de la XEiLL        :
[22:15]     -!-   -  :  Este servicio se encuentr en pruebas         :
[22:15]     -!-   -  :  Contacte con admin en tedi.roca@gmail.com    :
[22:15]     -!-   -  `=============================================='
```

```
[22:15]     -!-   End of MOTD command.
[22:15]     -!-   Server is currently in split-mode.
[22:15]     -!-   Found your IP: [192.168.1.2]
[22:15]     -!-   troca sets mode +w troca
```

Nos autenticamos como operadores mediante la sentencia */oper troca PFC*

```
[22:20]     ---   troca sets mode +o troca
[22:20]     ---   You are now an IRC Operator
```

5.4. Servidor de autenticación: *FreeRADIUS*

RADIUS (*Remote Authentication Dial-In Service*) ofrece autenticación y autorización centralizada para el acceso a redes. Inicialmente fue desarrollado para su uso en el acceso telefónico remoto pero en la actualidad se implementa en múltiples sistemas para validar accesos a diferentes tipos de conexión como ADSL o WiFI.

La topología de los sistemas RADIUS se basa generalmente en uno o varios servidores centrales que validan el acceso a los múltiples clientes. Estos servidores cuentan con una base de datos de usuarios a la que recurren para cotejar la validación.
En el caso que nos ocupa, la implementación de un sistema de autenticación, vamos a ver como la utilización de este sistema permite una conexión segura entre los usuarios y la red.

Como podemos apreciar, los usuarios actúan como clientes del punto de acceso (servidor). Éste a su vez es cliente de un servidor RADIUS instalado en otra máquina.

Para la instalación del servicio en los nodos de la XEiLL, utilizaremos FreeRADIUS, la versión libre de RADIUS, típicamente utilizada en entornos *Linux*. Necesitaremos los siguientes elementos:

- 1 PC. En nuestro caso, utilizaremos el servidor ubicado en cada nodo.
- Paquete LDAP instalado.
- 1 Punto de acceso inalámbrico.

Para la instalación y configuración del servidor se han seguido los pasos de Jorge Luque Alcalá incluidos en el documento "*Diseño e implementación de un sistema de autenticación, autorización y acceso a una red inalámbrica vía FreeRADIUS y Active Directory*".

Realizaremos la instalación de la siguiente manera:

- Descargamos el paquete desde:

  ftp://ftp.freeradius.org/pub/radius/CVS-snapshots/freeradius-snapshot-20040520.tar.gz

- Configuramos la instalación:

```
tar zxvf freeradius-snapshot-20040520.tar.gz
cd freeradius-snapthos-20040520
./configure –sysconfigdir=/etc
```

- Nos deplazamos al directorio */etc/raddb* donde se encuentran los archivos de configuración y editamos el archivo *clients.conf* añadiendo las siguientes líneas:

```
client 192.168.1.10 {
        secret = password_para_enviar_al_AP
        shortname = descripción_AP
}
```

- Editamos el archivo *radius.conf* modificando los modos de autorización y autenticación para utilizar:

```
authorize {
        preprocess
        eap
        suffix
```

```
        files
        ldap
}

authenticate {
        unix
        authtype LDAP {
                ldap
        }
}
```

- Dentro del mismo fichero configuramos el módulo LDAP, indicando la identidad del usuario con permisos de consulta, los certificados y la identidad certificadora.

- Modificamos el archivo *users* añadiendo el tipo de autenticación para cada usuario y el método por defecto:

```
“usuario”       Auth-Type := tipo_autenticacion

DEFAULT     Auth-Type := tipo_autenticacion_por_defecto
```

- Incluimos la ejecución de */usr/local/radius/sbin/radiusd* en la rutina de inicio de sistema para que se ejecute al arrancar.

- Ya sólo nos queda entrar en la configuración del punto de acceso y habilitar la autenticación mediante servidor RADIUS, especificando la dirección del servidor.

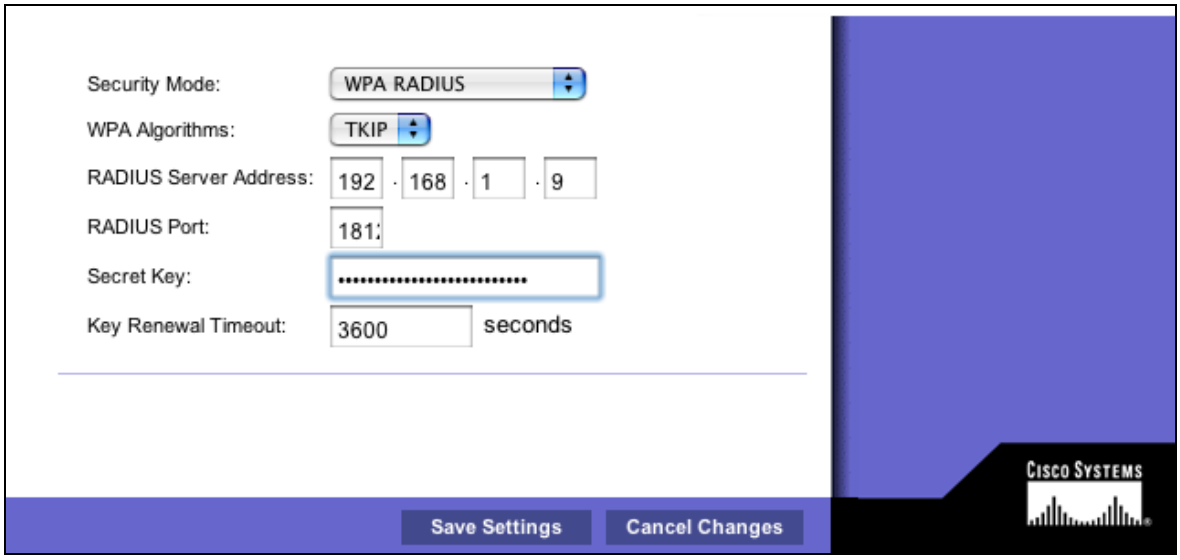


Figura 18: Configuración del servidor RADIUS en el punto de acceso

6. Legislatura aplicable

Un factor muy importante a la hora de establecer sistemas de comunicaciones es el cumplimento de las legislatura actual concerniente. Evitar estas normas puede conducir a importantes sanciones y cancelaciones de proyectos.
Es por ello que nos referimos en el siguiente capitulo a la normativa actual sobre utilización de frecuencias y potencia de transmisión.

Para las comunicaciones WiFi se utilizan 2 bandas libres del espacio radioeléctrico: 2,4 Ghz y 5 Ghz. La regulación de éstas corresponden a los siguientes organismos:

- Ministerio de Ciencia y Tecnología[20]
    - Regula el espacio radioeléctrico a través de la Secretaría de Estado de Telecomunicaciones.

- Comisión de Mercado de Telecomunicaciones[21]
    - Asegura el cumplimiento de la normativa vigente. Es un organismo regulador sectorial independiente. Entidad con personalidad jurídica y plena capacidad pública y privada. Sus principales funciones son:
        - Concede títulos necesarios que permiten prestar servicios de telecomunicaciones.
        - Resuelve dudas que formulan operadores, asociaciones de consumidores y usuarios.
        - Marca instrucciones vinculantes para las entidades que operan en el sector, dirigidas a mantener la libre competencia de mercado.
        - Asesora el Gobierno en relación a la política de telecomunicaciones.
        - Tiene potestad sancionadora respecto a los incumplimientos de las Instrucciones o Resoluciones que dicte en el ejercicio de sus competencias.

[20] *http://www.mcyt.es/*
[21] *http://www.cmt.es/cmt/index.htm*

- ETSI (Instituto Europeo de Estándares de Telecomunicaciones)[22]
    - Establece la potencia máxima radiada: 20 dBm (100 mW)

El "Título V de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones" [23] cita:

"…Tratados y Acuerdos internacionales en los que España sea parte, atendiendo a la normativa aplicable en la Unión Europea i a las resoluciones y recomendaciones de la Unión Internacional de Telecomunicaciones y de otros organismos internacionales…"

En el artículo número 7[24]: *"Títulos habilitantes y supuestos en los que no es perceptiva su obtención"* refiriéndonos al apartado 2, letra c, podemos ver la indicación de que las instalaciones o equipos que utilicen el dominio público radioeléctrico, mediante el uso común general, no necesitan licencia para operar.

Mediante el Cuadro Nacional de Atribución de Frecuencias (CNAF)[25] podemos obtener el listado de frecuencias de uso general, privado o especial. En las notas de Utilización Nacional[26] se especifican se especifica como uso común general:

- UN 109: Enlaces de vídeo de corto alcance para aplicaciones genéricas, tanto en el interior como en el exterior de los edificios (2421MHz, 2449 MHz, 2477 MHz).

- UN 51: Aplicaciones industriales, científicas y médicas -> ICM (2403 a 2500 MHz, 5725 a 5875 MHz, 24 a 24,25 GHz, 61 a 61,50 GHz)

- UN 85: Redes de Área Local: 2445 MHz a 2475 MHz. [27]

[22] *http://www.etsi.org/*
[23] *http://www.setsi.mcyt.es/legisla/teleco/lgt/5.htm*
[24] *http://www.setsi.mcyt.es/legisla/teleco/lgt/2.htm*
[25] *http://www.setsi.mcyt.es/espectro/cnaf.htm.*
[26] *http://www.setsi.mcyt.es/espectro/notas_un02/notas_un02.htm.*
[27] *http://www.setsi.mcyt.es/espectro/notas_un02/un81_90_02.htm.*

"Estas frecuencias podrán ser utilizadas en redes de área local para la interconexión sin hilos entre ordenadores y/o terminales y dispositivos periféricos para aplicaciones en interior de edificios. La potencia total será inferior a 100 mW (PIRE)[28]. Esta utilización se considera de uso común")

"Esta banda de frecuencias también podrá utilizarse para aplicaciones generales de baja potencia en recintos cerrados y exteriores de corto alcance. La potencia radiada máxima será inferior a 100 mW (PIRE)"

"En ambos casos, las características radioeléctricas de estos equipos se ajustarán a las especificaciones ETSI ETS 300 328, ETS 300 440 o bien al estándar específico, si es el caso, lo que deberá indicarse en el correspondiente certificado de aceptación"

- UN 128: Redes de Área Local de altas prestaciones: 5150 a 5350 MHz
  "En esta banda el uso por el servicio móvil en redes de área local se restringe para su utilización únicamente en el interior de recintos..."

Por otro lado, contamos con el ETS 300 328, un Standard de la ETSI que tiene como título: *"Radio Equipment and Systems (RES); Wideband transmissions systems; Technical characteristics and test conditions for data transmission equipment operating in 2,4 GHz ISM band and using spread spectrum modulation techniques".* [29]
Se trata de un documento utilizado por laboratorios y fabricantes para garantizar el funcionamiento y calidad de sus equipos.

Adicionalmente, y en conclusión a este apartado, cabe citar que la CMT indica específicamente que no se pueden utilizar recursos económicos procedentes de fondos públicos para realizar el despliegue y explotación de una red inalámbrica. Tampoco está permitido que el acceso a Internet sea subvencionado por medio de fondos públicos municipales.

[28] *Potencia isótropa radiada equivalente.*
[29] *http://www.setsi.mcyt.es/normali/certifi/cnaf_tel.htm.*

7. Recomendaciones de seguridad

Tal como se prevé en cualquier tipo de red telemática, debemos contar con un amplio nivel de seguridad que proteja los datos que viajan a través de ésta y los servicios implementados.

Además de los requerimientos para una red cableada, se proponen una serie de medidas específicamente otorgadas a tecnologías inalámbricas. Éstas ayudaran a proteger la integridad de la XEiLL, proporcionando una red más segura.

- No basar la seguridad de la red en autenticación y encriptación WEP:
  - Tal como se comentó en la introducción de este trabajo, existe alto nivel de intrusión mediante software capaz de generar este tipo de claves, lo que supondría un gran riesgo para la red, ya que ésta ofrece cobertura WiFi en la cercanía de los lugares donde están instalados los nodos.
  - La utilización de este sistema requiere de algún otro tipo de soporte adicional que complemente la seguridad.

- Separar las redes WiFi de las redes cableadas:
  - Los centros educativos que forman la XEiLL disponen de una red cableada para el uso general. Unir estas redes a la XEiLL supone exponerse a una serie de peligros.
  - Hay que tener en cuenta que la XEiLL no es una red con finalidades administrativas, de gestión o servicios globales. Es por ello, que unir la red inalámbrica a la cableada puede suponer la aparición de cuellos de botella, ataques a redes privadas del propio centro o utilización indebida de recursos.

- Utilizar listas de control de acceso por MAC:
  - A la hora de instalar los puntos de acceso en los nodos debemos tener en cuenta el tipo de acceso permitido. Resulta interesante que los usuarios puedan conectar directamente sin necesidad de registrar la dirección física

de su interfaz de red. Sin embargo, es especialmente peligroso permitir la conexión de otros puntos de acceso en modo puente o repetidor.

- En estos dos modos, un atacante podría expandir la señal en ámbitos geográficos no deseados, incrementar la potencia radiada llegando a limites superiores a los permitidos o utilizar la red educativa con fines ajenos a los establecidos, estableciendo la conexión con un punto de acceso de su propiedad.

- Cambiar las claves WEP periódicamente:
  - Tal como hemos indicado anteriormente, este sistema no proporciona un nivel fuerte de seguridad y sus claves de acceso pueden ser descifradas mediante programas como AirSnort o MacStumbler.
  - Es recomendable cambiar estas claves a menudo. Ello no hará que la red sea invulnerable, pero endurecerá el trabajo de un posible atacante. En los casos en los que las claves utilizadas sean de 128 bits, se puede llegar a tardar varios días en descifrarla.

- Deshabilitar las tramas *beacon*:
  - Éstas son informaciones periódicas que envían los dispositivos base de infraestructura, tales como puntos de acceso o tarjetas WiFi en modo activo.
  - En estas tramas el dispositivo informa del SSID al que pertenece de forma continua.
  - En el caso de los usuarios de la XEiLL supone un inconveniente ocultar el SSID de la red, evitando así que los clientes puedan descubrirla, ya que los usuarios que deseen hacer uso de ésta deberían ser conocedores de ciertos parámetros de conexión y por lo tanto no estaríamos hablando de una red libre, si no una red de alcance limitado.
  - Sin embargo, a la hora de realizar enlaces inalámbricos (WDS) entre los nodos, evitaremos enviar el SSID en todos aquellos momentos en los que no se curse tráfico, típicamente aquellos horarios en los que una red está inactiva y por lo tanto su nivel de defensa se ve mermado en cuanto a supervisión humana.

- Cambiar las contraseñas por defecto y las direcciones IP de los puntos de acceso:
  - Indudablemente es de suma importancia variar estos datos respecto a las configuraciones de fábrica. Sería tremendamente fácil para el atacante cambiar los parámetros de los dispositivos si no tomásemos esta precaución.
  - Las direcciones IP y las contraseñas de acceso son genéricas para las configuraciones por defecto de un modelo concreto de dispositivo.

- No utilizar servidores DHCP:
  - En aquellos dispositivos en los que no estén previstos cambios de rutas ni acceso eventual de clientes, desactivaremos esta opción. De esta forma evitaremos que un posible atacante obtenga una dirección IP automáticamente, dificultando así el posible ataque.

- Utilizar servidores de autentificación segura:
  - Una de las soluciones más fiables, considerada como una solución de seguridad fuerte, consiste en la implementación de un servidor de autentificación.
  - Tal como se explicó en capítulos anteriores, la implementación de un servidor RADIUS para la generación de claves de acceso utilizadas por el punto de acceso, proporcionan un conjunto de características de seguridad de gran fiabilidad.

Cabe destacar que no es adecuado confinar la seguridad de una red telemática inalámbrica en un único sistema de seguridad. La utilización de varios de estos métodos proporcionan un nivel de seguridad aceptable. Aún así, nunca se debe confiar en la efectividad absoluta de estos sistemas, algunos son vulnerables y otros pueden llegar a serlo en un futuro.

8. Estudio geográfico de la ciudad

En la actualidad, la mayoría de nodos que integran la XEiLL se encuentran en la ciudad de Santa Coloma de Gramenet. Esta ciudad es típicamente conocida por la desastrosa organización de sus edificaciones. Tal es el desorden en la estructuración, que durante años ha sido objeto de estudio de las universidades japonesas, como modelo a evitar. Esto comporta un notable desnivel en edificios del mismo plano.

A este hecho debemos sumar las barreras naturales que genera la irregularidad del relieve. Los diferentes barrios de la ciudad se encuentran a diferentes niveles respecto el nivel del mar y en algunos casos rodeados por montañas.

Figura 19: Mapa en relieve de Santa Coloma de Gramenet

Por todo esto, resulta especialmente dificultoso hacer llegar la señal de la red al mayor número de usuarios posible.

La finalidad de este capítulo es el estudio geográfico de la ciudad, con el fin de identificar los puntos de instalación óptimos para los nodos.

En la figura X podemos identificar la estructura que formará en un futuro la XEiLL. En la actualidad algunos de estos nodos ya se encuentran instalados, el resto lo estarán breve.
Dando un vistazo al mapa en relieve anterior, podemos entender fácilmente la ubicación de los nodos.

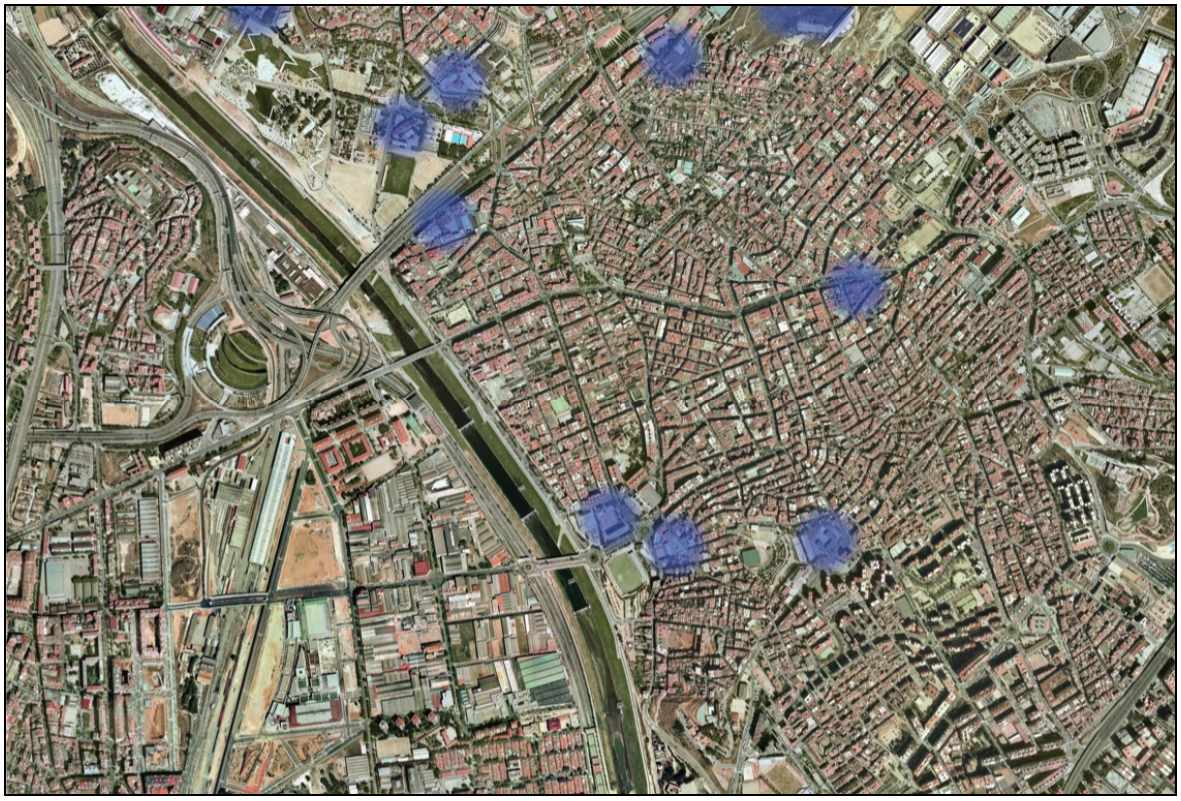


Figura 20: Ubicación de los nodos instalados

Como se aprecia en la parte central de mapa, nos encontramos con un plano regular edificado. Esta zona estará cubierta por los nodos de las zonas colindantes.

En la parte superior del mapa de relieve se encuentra una zona montañosa donde apenas no hay viviendas. Por el momento no está previsto dar cobertura a estas zonas, ya que tampoco se encuentran localizadas instituciones educativas.

Para entender las necesidades de cobertura, podemos utilizar el mapa de la Figura X, donde podemos distinguir principalmente dos tipos de zonas, las azules donde se localizan edificaciones industriales y las rojas donde están ubicadas las zonas residenciales.

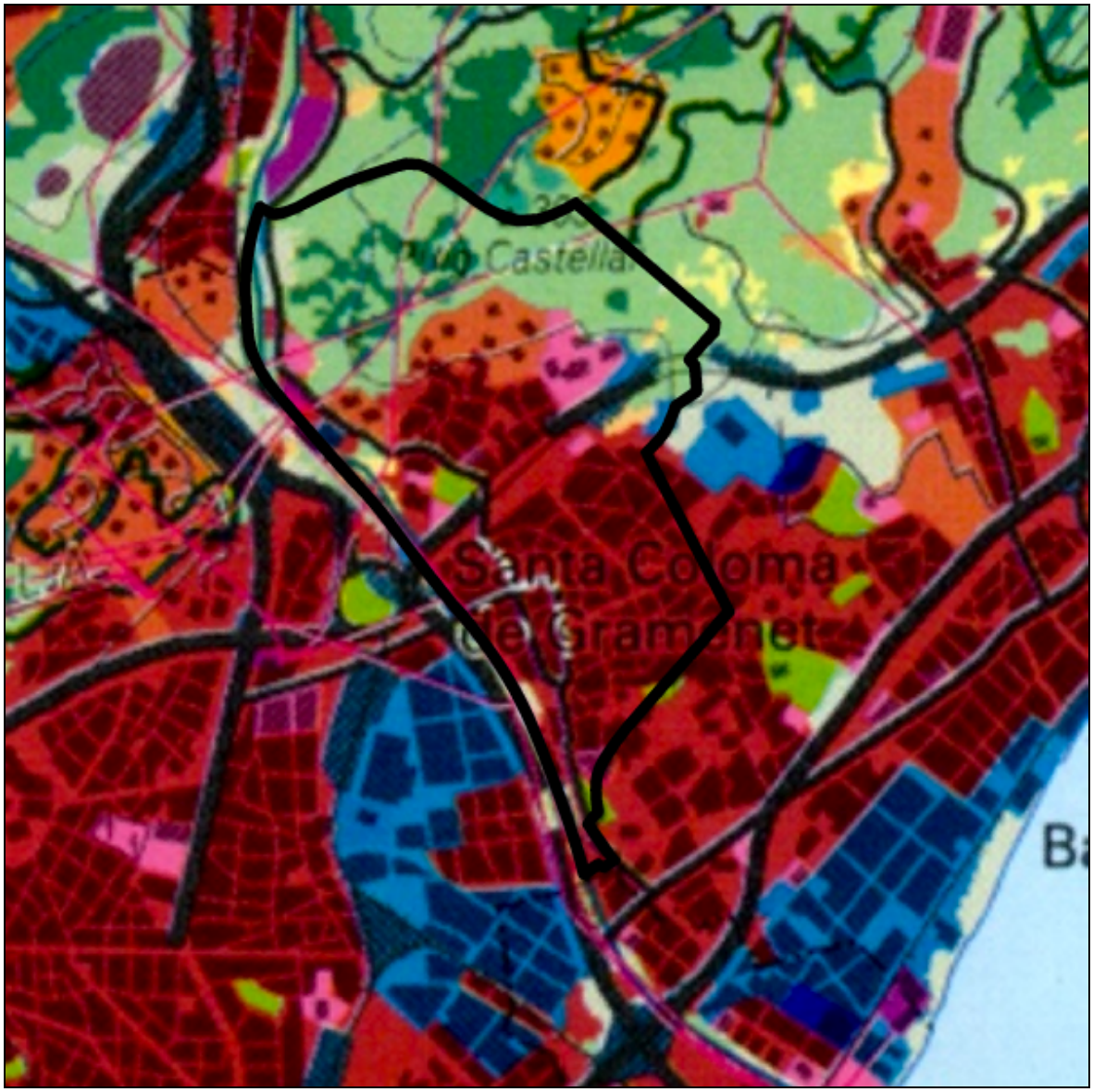


Figura 21: Mapa de utilización de los suelos de Santa Coloma de Gramenet

En cuanto a la interconexión de los nodos mediante enlace WDS, podemos utilizar el teorema sobre la Altura de *Fresnel*. Éste describe la distancia que se puede cubrir en un enlace directo, contando con la utilización de un elipse como zona a dejar libre en la altura y distancia de expansión de la señal.

Para calcular la altura que debe estar libre en todo el enlace, podemos utilizar un simulador como el hospedado en http://www.firstmilewireless.com/calc_fresnel.html o la tabla incluida en el capítulo siguiente (Tabla 1).

9. Instalación y configuración de equipos

9.1. Nodos

9.1.1. Ubicación

Es de vital importancia la correcta ubicación de los nodos en puntos donde la expansión de la señal sea óptima. Asimilando la imposibilidad de llegar a todos los puntos de la ciudad, nos centraremos en conseguir que la señal se expanda lo máximo posible.

Las ondas de radiofrecuencia superiores a los 2 GHz no atraviesan por completo los cuerpos sólidos. Por lo tanto, en las transmisiones WiFi (2,45 GHz) nos encontraremos con ciertos obstáculos, tales como como montañas y edificaciones, que impiden la expansión de la señal.

Para interconectar dos puntos mediante enlace inalámbrico debemos contar con visión directa tener en cuenta zona de *Fresnel*. Esta zona es un área elíptica alrededor del camino visual entre los puntos a enlazar. Esta zona varia en función de la longitud del camino y la frecuencia de la señal.

En la siguiente tabla, obtenida mediante el simulador citado anteriormente, se puede encontrar la relación entre la distancia de las antenas y la altura a vaciar de obstáculos para redes inalámbricas que trabajen a 2,4 GHz..

Distancia entre antenas (en Km)	Zona de *Fresnel* (en metros)
1	3,9
2	5,6
3	7,1
4	8,4
5	9,7
6	11,0
7	12,3
8	13,6
9	15,0
10	16,4
11	17,9
12	19,4
13	21,0
14	22,7
15	24,4

Tabla 1: Relación entre distancia y zona de *Fresnel* para señales de 2,4 GHz

A la hora de instalar un nuevo nodo se debe realizar un recorrido por los mapas del capitulo anterior, con el fin de identificar los posibles elementos que puedan irrumpir en la expansión de la señal.

9.1.2. Servidores

Para la instalación de los equipos servidores se utilizan PCs de uso doméstico como el que utiliza cualquier usuario doméstico. Únicamente se les equipa con una tarjeta Ethernet adicional.

Cada equipo está ubicado en un centro escolar y ofrece diferentes servicios. El sistema operativo instalado es *Linux* por su estabilidad, la disponibilidad de paquetes necesarios para llevar a cabo un proyecto de este tipo y el hecho de ser una distribución gratuita.

Adicionalmente, tal como se ha visto a lo largo del proyecto, se instala otro *software adicional,* siempre libre y sin coste para el usuario y la organización de la XEiLL, convirtiendo este en un proyecto "libre".

No se entra en detalle sobre la instalación de este sistema operativo ya que la intención de este proyecto no es centrarse en ello y en la actualidad las instalaciones guiadas proporcionan al usuario una visión clara y simple del progreso de ésta.

9.1.3. Puntos de acceso – *routers*

En la mayoría de los casos se instalan *routers* inalámbricos, lo que podríamos traducir en un punto de acceso + *router*. Se instalan en cajas estancas situadas cerca de las antenas, de modo que no se pierda calidad de señal por la atenuación del cable.

El modelo más adecuado para este tipo de instalaciones es el *Lnksys WRT-54G*, por los siguientes motivos:

- Precio económico.
- Calidad del fabricante *(Cisco Systems).*
- Facilidad de uso.
- *Firmware* actualizable fácilmente con soporte *Linux.*
- Incluye 2 conectores para antenas.

Figura 22: ***Linksys WRT-54G***

9.1.4. Antenas

Para la instalación de las antenas se eligen principalmente edificios de centros educativos, donde haya instalado un nodo de la red, pero no se descarta en un futuro realizar instalaciones en otros centros culturales o espacios cedidos.

Figura 23: Antena instalada en el IES Puig Castellar

9.2. Clientes

9.2.1. Equipo necesario

Para poder utilizar los servicios de la XEiLL el usuario no precisa de grandes conocimientos de informática ni adquirir costoso material. Simplemente precisa de un equipo, ya sea de sobremesa o portátil, y una interficie de red inalámbrica que permita el envío y recepción de datos.

Se contemplan 3 escenarios en los que se puede encontrar el usuario:

- Acceso desde medio fijo:
    - Se realiza la conexión desde un equipo con ubicación fija, tal como un ordenador de sobremesa.
    - Material necesario:
        - Equipo informático.
        - Tarjeta WiFi PCI o tarjeta WiFi PCMCIA y adaptador PCI-PCMCIA.

- Acceso desde medio móvil:
    - El usuario conecta desde un dispositivo portátil: PDA, ordenador portátil, ...
    - Material necesario:
        - Equipo informático portátil
        - Tarjeta WiFi PCMCIA, PDA o portátil con tecnología WiFi incorporada, USB WiFi, CompactFlash/SD WiFi

- Conexión puente:
    - En casos puntuales, cabe la posibilidad de que algunos usuarios realicen la función de puente, expandiendo así la señal de la XEiLL. De esta forma, el dispositivo WiFi del usuario recibe la señal de la XEiLL y a su vez la expande a su zona de cobertura.
    - Material necesario:
        - Punto de acceso inalámbrico con capacidad para funcionar en modo puente o repetidor.

En todos los casos, se puede hacer uso de antenas externas para mejorar la calidad de señal, transmitiendo y recibiendo datos a mayor distancia. Se pueden utilizar antenas comerciales o bien construir una.

La construcción de una antena WiFi no requiere grandes conocimientos. Vamos a ver como construir una antena direccional[30].

Material necesario:

- Lata de *Nesquik* o similar.
- Conector N hembra con tuerca.
- Cable de antena.
- Estaño.

Herramientas:

- Taladro u otra herramienta para perforar materiales metálicos.
- Cinta métrica o pie de rey.
- Soldador.

Instrucciones para la construcción:

- Elegir la frecuencia para el funcionamiento óptimo de la antena.

- Introducir el diámetro de la lata y la frecuencia en el simulador de http://www.saunalahti.fi/~elepal/antenna2calc.php, lo que proporcionará las medidas donde ubicar el conector y la longitud del vivo.

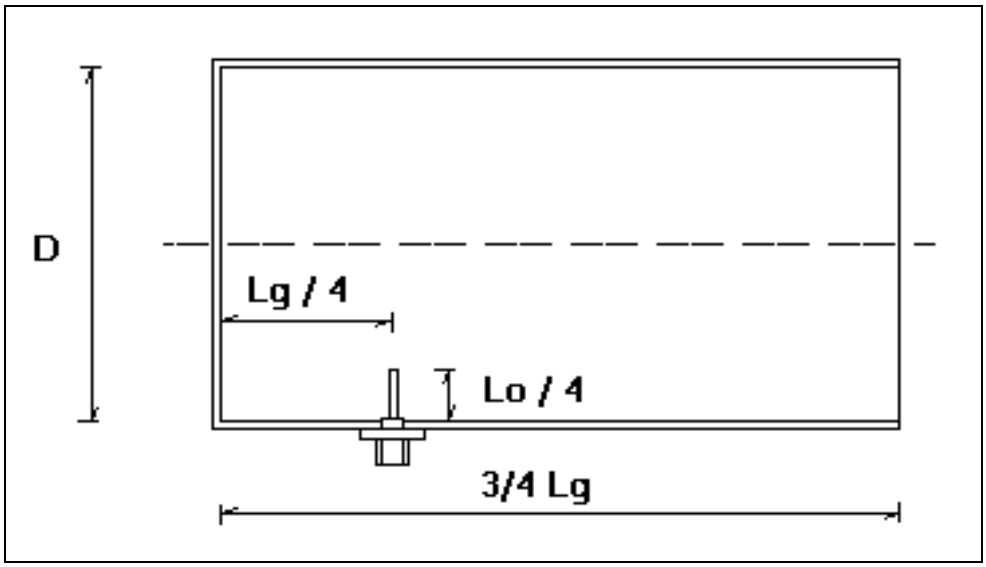


Figura 24: Medidas para la ubicación del conector y longitud del vivo.

[30] *Información extraída de http://www.saunalahti.fi/~elepal/antenna2.html.*

- Soldar al conector N la longitud de vivo obtenida.

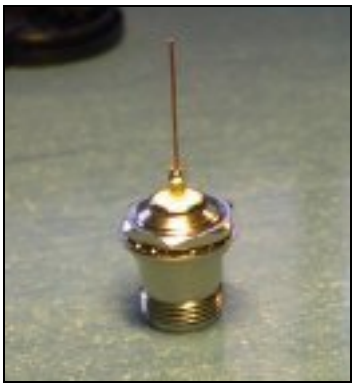


Figura 25: Conector N hembra con vivo soldado

- Perforar el bote a la distancia de la base obtenida e introducir el conector N con el vivo soldado.

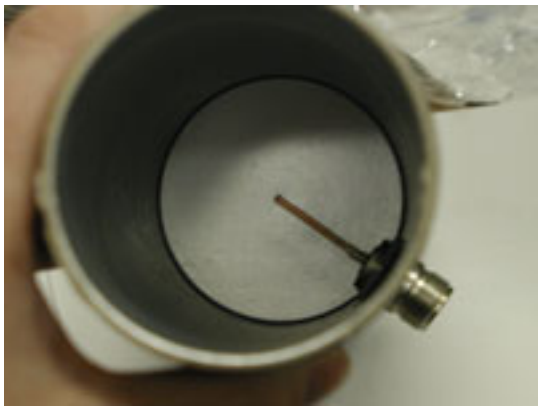


Figura 26: Antena domestica una vez finalizada

Si bien la utilización de antenas externas supone una gran mejora en las comunicaciones, en muchos casos las tarjetas PCMCIA de los clientes no disponen de conectores para éstas.

9.2.2. Configuración

Tras realizar un recorrido sobre los equipos necesarios para poder conectar con una red inalámbrica como la XEiLL, vamos a ver como se deben configurar los equipos clientes.

Se detallan instrucciones precisas para la puesta en marcha de la conexión en los sistemas operativos más utilizados. Teniendo en cuenta que en cada plataforma disponemos varias versiones de sistema operativo y considerando redundante la explicación de cada uno de ellos, explicaremos los pasos a realizar en las versiones más actuales y por lo tanto más utilizadas:

- *Windows XP Home Edition (SP2)*

    - En la barra de tareas, localizar el icono de redes inalámbricas y pulsar el botón derecho. En el menú que aparece, seleccionar "Ver redes inalámbricas disponibles".

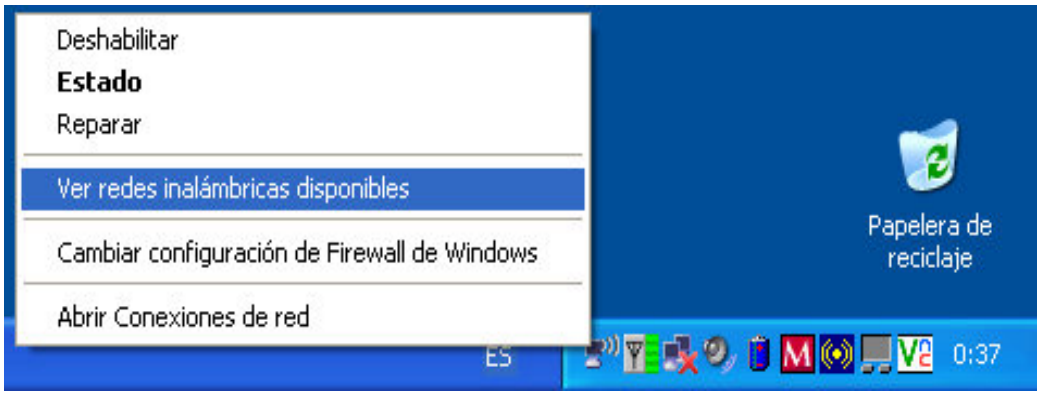


Figura 27: Acceso a redes inalámbricas en *Windows XP*

    - En la pantalla aparecerán las redes disponibles. Seleccionar "xeill" y clicar en "Conectar".

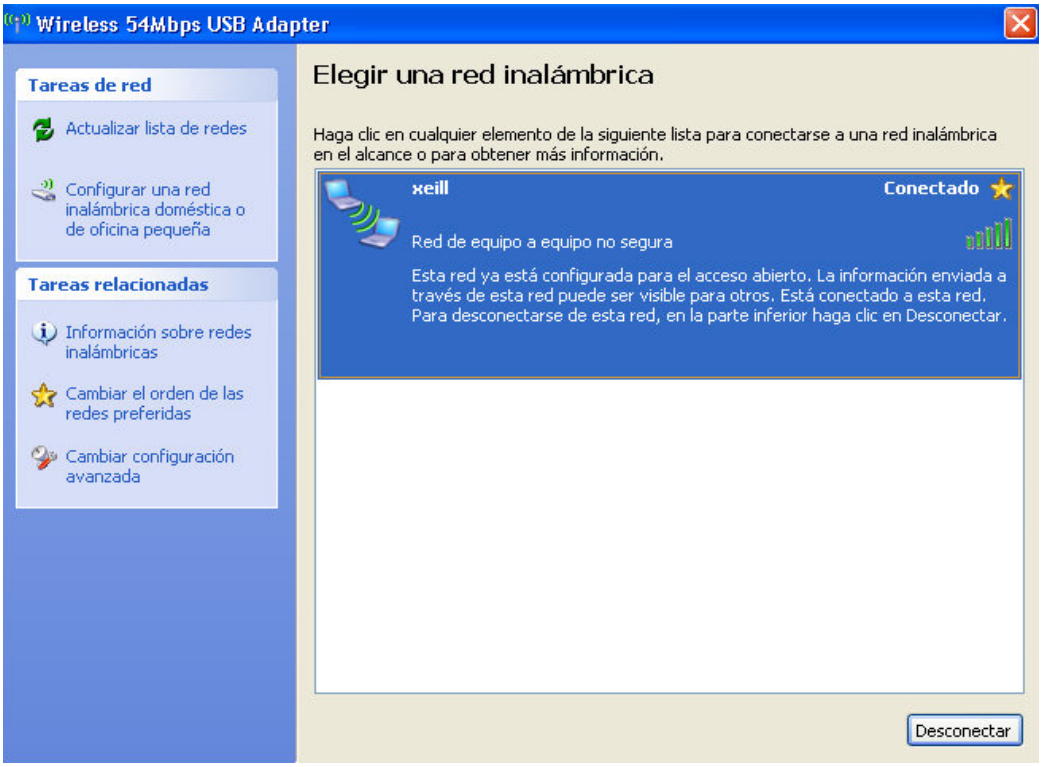


Figura 28: Conexión de un equipo cliente con *Windows XP* a la XEiLL

- Automáticamente el equipo obtendrá una dirección y nombre de red mediante DHCP.

- *Mac OS X 10.3.7*

  - En la barra del menú superior del sistema, seleccionamos el icono de *Aiport* y en el menú desplegable clicamos en donde aparece *xeill.*

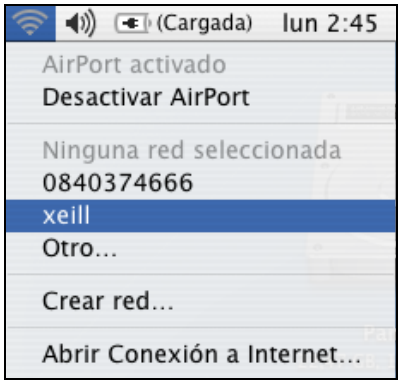


Figura 29: Conexión de un equipo cliente con *Mac OS X* a la XEiLL

- *Ubuntu Linux 4.01 (Gnome Desktop)*

    - En el menú superior entramos en el menú *Equipo* > *Configuración del Sistema* > *Red.*

Figura 30: Panel de Configuración de red en *Ubuntu Linux*

    - En el panel de configuración que nos aparece, clicamos el botón *Añadir.*

    - Cuando aparezca el asistente, clicamos el botón *Adelante* hasta que nos pregunte el tipo de conexión. Seleccionamos *Inalámbrica* y pulsamos *Adelante* nuevamente.

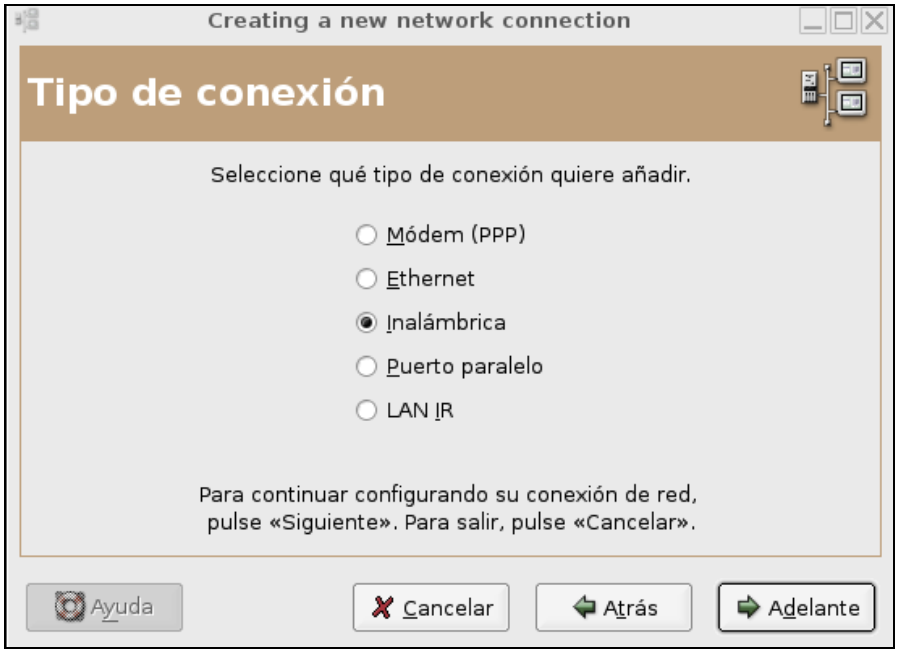


Figura 31: Crear conexión de red en *Ubuntu Linux*

- En la pantalla para configurar una nueva red, seleccionamos el dispositivo a utilizar e introducimos el identificador de la red (ESSID): xeill. No hay que introducir ninguna clave WEP.

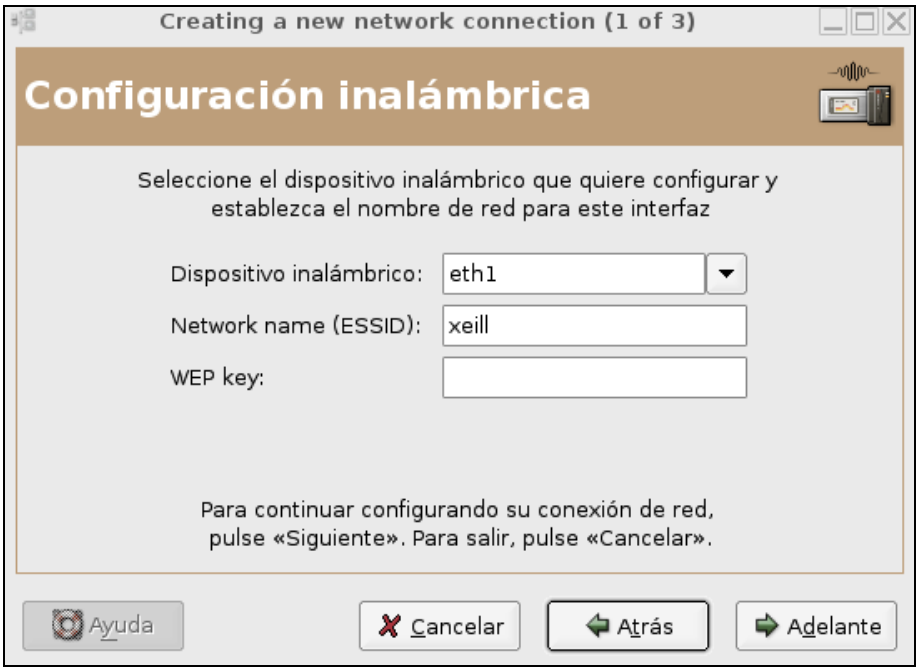


Figura 32: Configuración de una conexión de red en *Ubuntu Linux*

- Cuando aparezca el panel de configuración de la dirección, seleccionamos *Automático (DHCP)* en la pestaña *Configuración.*

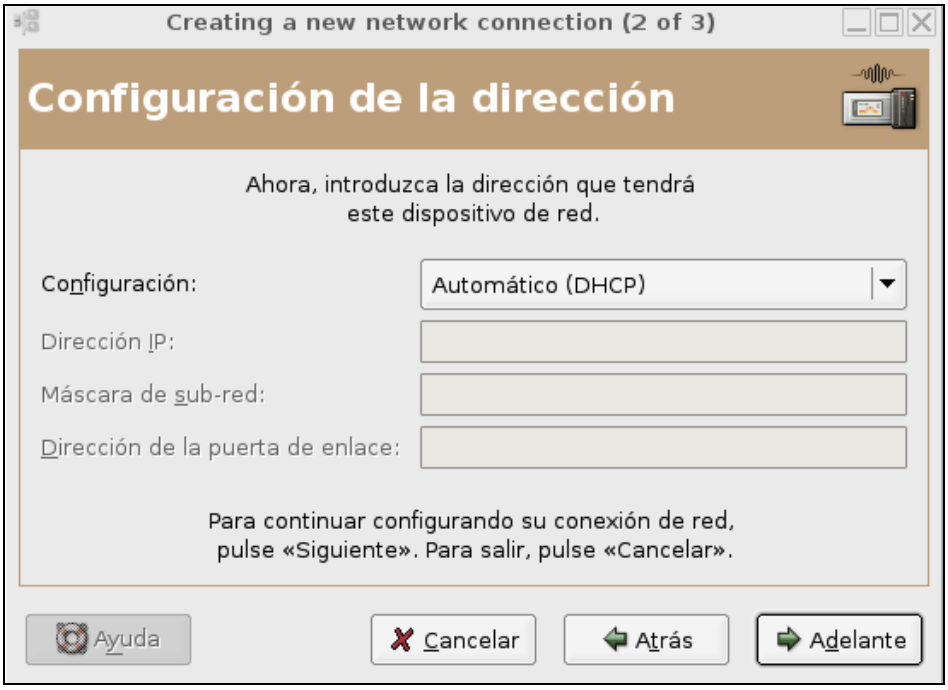


Figura 33: Congiruación de la dirección IP en *Ubuntu Linux*

- Para terminar, pulsamos adelante hasta que finalice la configuración, aceptando los siguientes pasos.

10. Viabilidad económica

Sin duda, uno de los aspectos más importantes a la hora de poner en marcha un proyecto, es su coste económico. De ello depende la viabilidad de su implantación y la elección entre varias alternativas.

En los siguientes apartados se realiza un breve recorrido sobre los materiales y dispositivos utilizados, detallando el precio orientativo de coste en el mercado.

Cabe destacar que en este proyecto no se tiene en cuenta el coste de la mano de obra y servicios proporcionados por terceros, ya que la instalación y mantenimiento de la red la realizan personas sin ánimo de lucro, bien sea para el aprendizaje propio, de terceros o como iniciativa voluntaria.

10.1. Coste de implementación.

El coste de las instalaciones se centra básicamente en los nodos de acceso, ya que al enviarse la señal a través del medio aéreo, no se generan gastos de cableado e instalaciones intermedias.
Coste de los materiales:

- Equipo informático (PC) base: 400 €
- 2 x Tarjeta de red PCI: 30 €
- 1 Router + Punto de acceso: 100 €
- Antena direccional: 150 €
- Antena omnidireccional: 100 €
- Sistema operativo: 0 € (Distribución gratuita)
- Software adicional: 0 € (Sofware libre)
- 2 x Cable antena – punto de acceso 1 m: 0,50 €
- 2 x Conector N (antena): 2 €
- 2 x Conector MC (punto de acceso): 2€
- Cable Ethernet CAT5 2m: 3 €

Total materiales: 787,5 €

El precio de la instalación de los nodos no afecta a las instalaciones realizadas en la XEiLL, ya que no se genera negocio a través de ellas, si no que se realizan de forma voluntaria por estudiantes. De todas formas, a continuación se detalla el coste de una instalación de este tipo, con el propósito de proporcionar una visión más exacta del coste real.

Se estipula el precio de 30 €/hora para los servicios generales de informática (configuración de PC, instalación de sistema, etc), 50 €/hora para los servicios de redes y 60 €/hora para los servicios especializados (instalación y configuración de software de terceras partes)

Coste de la mano de obra:

- Ensamblaje de equipo base e instalación de tarjetas de red:
    - 1h x 30€ = 30€

- Instalación del sistema operativo:
    - 1h x 30€ = 30€

- Configuración del *router* + punto de acceso:
    - 1h x 50€ = 50€

- Construcción, conexión y fijación de cables de antena y Ethernet:
    - 2h x 50€ = 100€

- Fijación de las antenas:
    - 1h x 50€ = 50€

- Instalación de software adicional:
    - Servidor web (Apache + PHP): 1h x 60€ = 60€
    - Servidor IRC (ircd): 2h x 60€ = 120€
    - Servidor Proxy: 2h x 60€ = 120€
    - VPN (openVPN): 4h x 60€ = 240€
    - Encaminamiento dinámico OSPF (zebra): 3h x 60€ = 180€

Total mano de obra: 980€

TOTAL INSTALACIÓN POR NODO: 1767,5€

10.2. Comparativa con redes cableadas

No es posible realizar un exhaustivo estudio económico sobre el coste del despliegue en similares condiciones ya que la tecnología WiFi proporciona enlaces radiales y direccionales, mientras que los enlaces físicos significan el despliegue a puntos concretos.

Podemos prever un aumento significativo del coste de despliegue respecto a las redes inalámbricas, por las siguientes razones:

- Similar coste de implementación de los servidores.
- Despliegue de cableado:
    - Elevado coste de la fibra óptica.
    - Necesidad de repetidores, *hubs* y otros dispositos de red intermedios.
    - Se precisan permisos de obra pública.
- Costosa reparación de los enlaces (elementos de red y cableado).
- Elevado gasto de planificación
- Costes de ampliación muy elevados.

Por lo tanto, comprobamos que resulta mucho más sencillo y económico el despliegue de redes inalámbricas.

11. Impacto social

Tal como se avanzó en la introducción de este trabajo, el desarrollo de esta red pretende ser un nexo de unión entre instituciones educativas, alumnos y otros ciudadanos interesados en la evolución de la cultura y la tecnología.

Actualmente existe el sitio www.xeill.net donde se puede encontrar información actualizada sobre la red. Este es el principal lugar de encuentro entre usuarios y entidades educativas. Resulta especialmente estimulante para los alumnos el foro incluido en la página web, donde los usuarios pueden incluir sus comentarios.

Desde que la XEiLL vio la luz ha crecido un notable interés por este tipo de tecnologías en la población, especialmente entre los estudiantes. Prueba de ello es su activa participación e interés por el proyecto.

Aun contando con este creciente interés, quedan muchas barreras por superar. En muchos casos los interesados en esta red desconocen este tipo de tecnología y por consiguiente no saben como acceder a los recursos. Es necesario crear un flujo de comunicación hacía la población, de forma que todo aquel que quiera pueda tener acceso a dicha información.

Es notable el especial énfasis que exhiben los jóvenes en utilizar esta red. Todo y que se trata de una red libre, debemos contar con la necesidad de disponer de equipos portatiles para sacar el máximo partido de la XEiLL. Es por ello que en la propia página web se pueden encontrar equipos ofertados por distribuidores autorizados a un precio especial.

Hasta el momento el proyecto ha tenido muy buena acogida y presenta un crecimiento exponencial día a día.

Glosario de acrónimos

AP *Access Point*
Punto de acceso

ADSL *Asymetric Digital Subscriber Line*
Línea de Subscripción Digital Asimétrica

DHCP *Dinamyc Host Configuration Protocol*
Protocolo de Configuración Dinámica de Equipos

DNS *Domain Name Service*
Servidor de Nombres de Dominio

EAP *Extensible Authentication Protocol*
Protocolo de Autenticación Extensible

IEEE *Institute of Electrical and Electronics Enginneers*
Instituto de Ingenieros Eléctricos y Electrónicos

IP *Internet Protocol*
Protocolo de Internet

IPSec *IP Security*
IP Segurizado

L2TP *Layer 2 Tunneling Protocol*
Protocolo de Capa 2 Tunelizado

LAN *Local Area Network*
Red de Área Local

LDAP *Lightweight Directory Access Protocol*
Protocolo Ligero de Acceso a Directorio

MAC *Médium Access Control*
Control de Acceso al Medio

PKI *Public Key Infrastructure*
Infraestructura de Clave Pública

RADIUS *Remote Authentication Dial-In User Service*
Servicio de Autenticación de Usuarios de Acceso Remoto

SSID *Service Set Identify*
Identificación del Bloque de Servicio

SSL *Secure Socket Layer*
Capa Conectora Segura

TCP *Transport Control Protocol*
Protocolo de Control de Transporte

TKIP *Temporal Key Integrity Protocol*
Protocolo de Integridad de Clave Temporal

VPN *Virtual Private Network*
Red Privada Virtual

WEP *Wired Equivalency Privacy*
Privacidad Equivalente al Cable

WPA WiFi *Protected Access*
Acceso WiFi Protegido

W*LAN* *Wireless Local Area Network*
Red de Área Local Inalámbrica

Bibliografía

Documentación escrita:

[1] Cisco Systems, Inc., *Academia de Networking de Cisco Systems CCNA - Tercera edición*. 2004 Pearson Educación, S.A.

[2] William Stallings, *Comunicaciones y Redes de Computadores*. 2000 Pearson Educación, S.A.

[3] Uyless D. Black, *2nd. Generation Mobile & Wireless Networks*. Ed. Prentice Hall PTR, 1999.

[4] Marcos Faúndez Zanuy, *Sistemas de Comunicaciones*. Ed. Marcombo 2001.

[5] Jonathan Leary Pejman Roshan, *Wireless Local-Area Network Fundamentals*. Ed. Ciscopress 2001.

[6] Neil Reid y Ron Seide, *802.11 (Wi-Fi). Manual de redes inalámbricas*. Editorial O'Reilly Networking 2003.

Referencias Web:

[7] http://www.xeill.net

[8] http://www.matarowireless.net

[9] http://www.barcelonawireless.net

[10] http://www.guadawireless.net

[11] http://www.antennaswireless.net

[12] http://bulma.net

[13] http://www.wikipedia.com

[14] http://www.apache.org

[15] http://www.jabber.org

[16] http://www.videolan.org

[17] http://www.irc101.org

[18] http://www.freeradius.org

[19] http://www.mcyt.es/

[20] http://www.cmt.es/

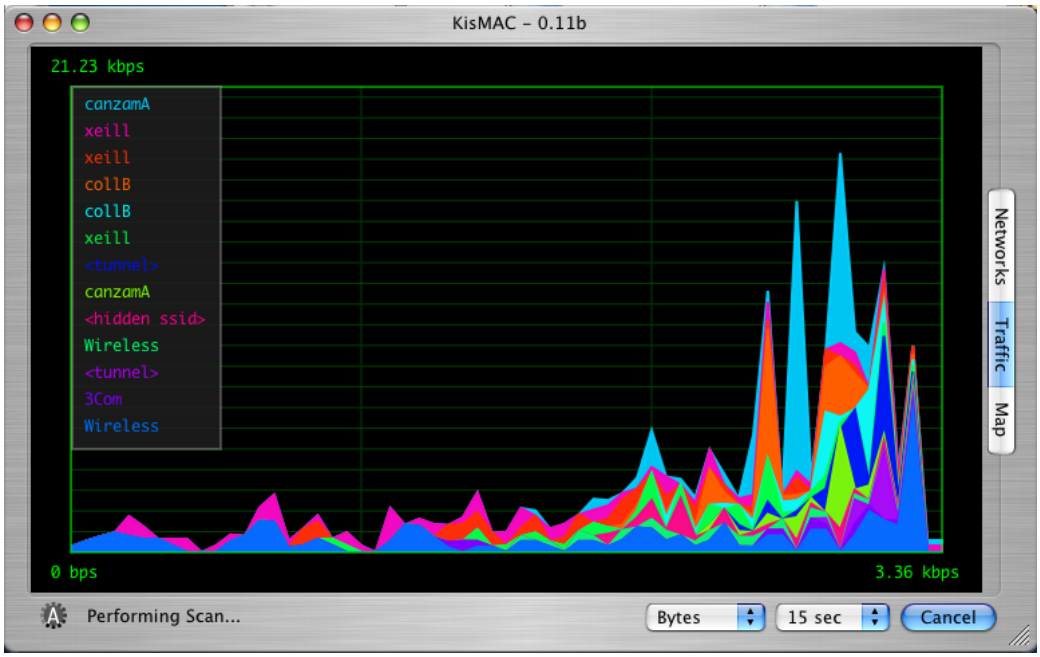
[21] http://www.etsi.org/

[22] http://www.saunalahti.fi/~elepal/

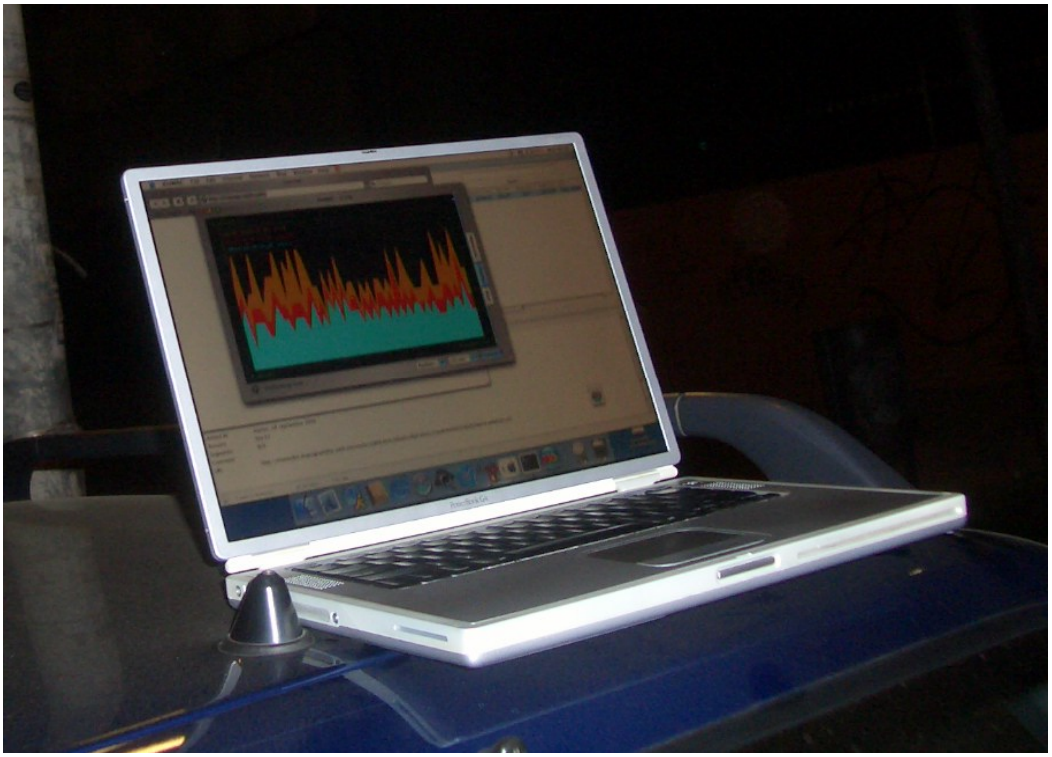
Anexo

A continuación se recogen los resultados obtenidos en las pruebas de conectividad.

En primer lugar, podemos apreciar en la gráfica de tráfico la actividad de la XEiLL y otras redes colindantes a intervalos ranurados.



Gráfica de tráfico de las redes colindantes a la XEiLL

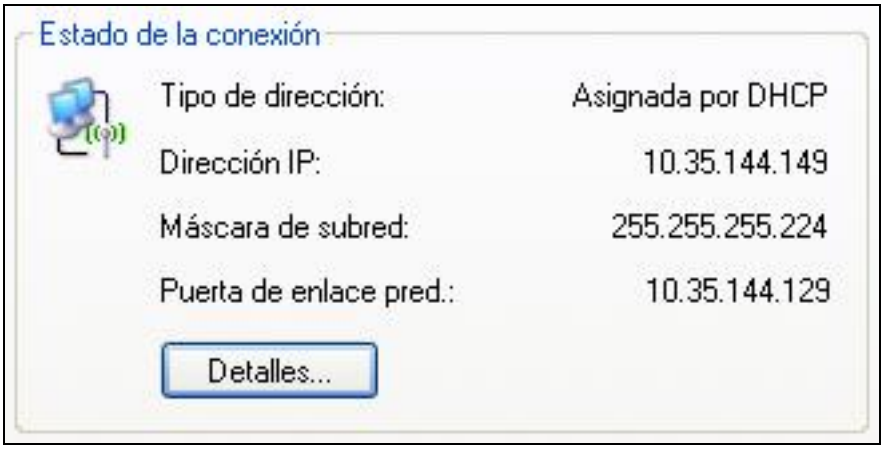


Podemos comprobar como aumenta el nivel de señal recibido al situar el equipo portátil a mayor altitud

Para realizar las pruebas se utilizaron diferentes equipos portátiles con varios sistemas operativos. Inicialmente se realizaron los tests utilizando computadoras con tecnología WiFi integrada, concluyendo con niveles de señal aceptables.
A continuación se probó a utilizar un adaptador WiFi USB, consiguiendo mejoras en la señal y sobretodo una estabilidad mayor en la conexión.
El siguiente paso fue utilizar varias tarjetas PCMCIA con antenas externas. El nível de señal recogido fue óptimo en la mayor parte de la ciudad.

Momento de la realización de las pruebas con un *PowerBook G4* con tarjeta *Airport* (PCMCIA) interna. La señal recibida mejoró notablemente al añadir una tarjeta *Orinoco Silver* con antena externa

En la siguiente imagen podemos ver como el *host* cliente obtiene una dirección IP autoasignada por el servidor del IES Terra Roja.



Cliente conectado al nodo del IES Terra Roja

Otro aspecto importante en los tests fue la utilización de antenas externas. En la imagen se puede apreciar una antena direccional *Pringles* en pleno funcionamiento. Con este tipo de antena se consiguieron excelentes resultados.

Utilización de antena externa *Pringles*