DESPLIEGUE DE UNA WLAN EN LA EPSC

Rafael Vidal Ferré y Xavier Bordoy Rodríguez

rafael.vidal@entel.upc.es: Departamento de Ingeniería Telemática
Universitat Politècnica de Catalunya;
xavier.bordoy@upc.es: Becario investigación i2CAT - Mediacat (tecnologías multimedia)
Universitat Politècnica de Catalunya

1. INTRODUCCIÓN

Durante el pasado curso 2001/02, a iniciativa del grupo de comunicaciones inalámbricas del Departamento de Ingeniería Telemática y como parte del proyecto I2Cat (Internet 2 a Catalunya), se llevo a cabo el despliegue de una red WLAN con tecnología IEEE 802.11b a la EPSC (Escuela Politécnica Superior de Castelldefels).

El objetivo del despliegue era doble. Por un lado ofrecer una plataforma sobre la que desarrollar y probar soluciones para el suporte de la movilidad, como por ejemplo Mobile IP y Cellular IP, y aplicaciones que sacaran provecho de ella, como teléfonos sin hilos utilizando VoIP, SIP i PDAs o servicios de localización. Por otro, se pensaba en ofrecer a toda la comunidad que forma la EPSC la posibilidad de un de acceso sin hilos de calidad a su red y por extensión a la de la UPC y a Internet.

El presente artículo se centra en explicar como se ha llevado a cabo este segundo propósito. En primer lugar haremos un breve resumen de las principales características de la tecnología WLAN utilizada, el estándar IEEE 802.11b, como paso previo a la descripción de los equipos de esta tecnología que se probaron y de los criterios seguidos para seleccionar los que finalmente se utilizaron. A continuación se definirán los criterios y objetivos que guiaron el despliegue de la red y posteriormente el proceso seguido para realizarlo. Se seguirá, comentando la integración de este acceso sin hilos a la red de la EPSC indicando los problemas más significativos que esta suponía, en especial de seguridad, y como se resolvieron. Para acabar se detallará las conclusiones.

2. EL PROTOCOLO 802.11B

El protocolo 802.11b pertenece a la família de protocolos 802.11 desarrollado por el IEEE. Puede considerarse una adaptación del estándar Ethernet al medio rádio. El cambio de medio de transmisión nos introduce dos modos de funcionamiento: Managed i Ad-Hoc. La diferencia radica en el hecho en que en una red Ad-Hoc la comunicación se realiza entre los terminales directamente y en una red en modo Managed hay un elemento llamdo Access Point (AP) que es el que gestiona todas les comunicaciones, y haciendo un símil con las redes cableadas tendria, inicialmente, un papel similar al de un hub. La red desarrollada en la EPSC se corresponde con este segundo tipo.

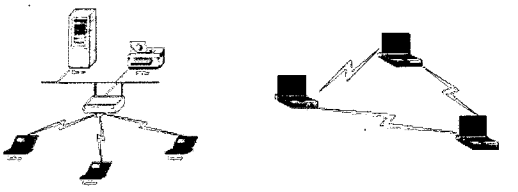

Figura 1. Sistema Managed y Ad-Hoc

Como en el caso del 802.3, el 802.11b sólo especifica el funcionamiento de las capas física y de control de acceso al medio (dentro del esquema OSI).

2.1. Capa física

La capa física se encarga de la codificación y de la modulación, básicamente. Cada AP utilitza una banda de frecuencias y las distribuye entre los usuarios. Este reparto se puede llevar a cabode dos maneras, dependiendo de la tecnología usada. La primera es el FHSS (Frequency Hopping Spread Spectrum) donde se divide el medio en 75 canales no solapados que van saltando según un patrón definido que coneicen los AP y los dispositivos conectados a ellos y permite tener diversas redes en una misma área. En segundo lugar tenemos el DSSS (Direct Sequence Spread Spectrum) donde la división se produce por código y no por frecuencia. El estándard define un total de 14 canales con un ancho de banda de 30 MHz por canal y una separación entre ellos de 5 MHz que tal y como se observa en la figura 2 se traduce en un solapamiento. Debido a esto es recomendable, y siempre que sea posible, dejar un espacio libre de cinco canales. Esta tecnología es actualmente la más usada, ya que permite llegar a tasas de hasta 11Mbps, mientras que con el FHSS no se pasa de 2Mbps.

Hay que remarcar que todos estos canales no estan disponibles en todos los paises, y dependiendo de la legislació vigente en cada país serán distintos para cada uno de ellos. En España, y según consta en la norma UN-115, dentro de la banda de los 2.4 GHz disponemos de los canals 1 al 13. Además, para su uso libre dentro de esta banda de frecuencias los dispositivos deben estar limitados a una poténcia máxima de radiación de 100 mW EIRP en toda la UE.

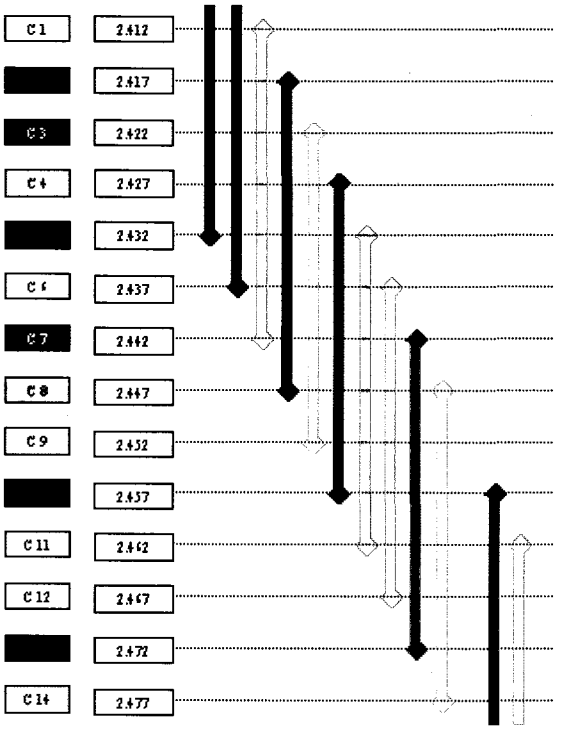

Figura 2. Canales DSSS

2.2. Capa de control de acceso al medio

La capa de control de acceso al medio, como su nombre indica, aparte de controlar el acceso al medio, realiza el control del roaming (cambio de AP de los usuarios), control de autenticación y finalmente también realiza el control de energía. No debemos olvidar que estamos hablando de una tecnología desrrollada para dispositivos móbiles alimentados porr baterías y consecuentemente, la conservación de la energía es un elemento básico para estos dispositivos.

En referencia a la capa de control de acceso al medio, como ya hemos dicho, efectúa diversas tareas. La primera es la de evitar las colisiones. Por eso ha de coordinar todas las comunicaciones y ha de establecer métodos de detección de medio ocupado. El que se ha definido como sistema obligatorio es el CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance). Con este sistema, tal y como se indica en su nombre, lo que se hace es escuchar el medio para ver si está ocupado (detector de portadora) y en caso de que lo esté no se transmite para evitar colisiones. Junto a esta tecnología se ha añadido la extensión RTS-CTS (Ready To Send - Clear To Send) que evita el problema de los terminales ocultos y sobreexpuestos.

En segundo lugar, junto al señal de sincronización se envía información del área (BSSID) para poder localizar la red wireless y poderse asociar. Esta señal de sincronización lo que hace es regular las comunicaciones, ya que dependiendo de la prioridad de las comunicaciones a realizar se asignan tiempos de contención distintos a la espera de que se libere el medio. Cada dispositivo genera un tiempo de contención aleatorio para evitar que se lleguen a producir colisiones en el nuevo intento de entrada, ya que si hubiese dos dispositivos que esperasen el mismo tiempo para acceder, al volver ha escuchar el medio ambos lo verian libre y empezarian la comunicación colisionando.

En tercer lugar hay el tema de la mobilidat de los usuarios. En efecto, los usuarios estarán en movimento y consecuentemente, no estarán siempre cubiertos por el mismo AP. Así que es necesario algún mecanismo de control que notifique que un usuario ha cambiado de nodo de control (AP) y por tanto, todos sus paquetes ahora irán por otro camino. Para poder llevar a cabo est e control cada AP tiene una base de datos donde estan registrados todos los usuarios y puede ser consultado por los AP's vecinos para poder realizar el envío de paquetes más eficiente posible. El cambio de zona se produce cuando el terminal no tiene suficiente poténcia para continuar estableciendo una comunicación de calidad (rápida) y entonces escanea el medio en busca de un nuevo punto de conexión más potente.

En cuarto lugar hay el control de potencia. Como que la energía es limitada (duración limitada de las baterias) los dispositivos entran en reposo cuando no se estan usando, y miran el medio periódicamente para saber si hay algun paquete en espera de ser entregado. Por este motivo la sincronización es básica, ya que si un AP recibe un paquete para un dispositivo que está en reposo sabe el tiempo que tardará este en volver a mirar el medio y por tanto podrá entregarlo. En caso contrario, si no estuviesen sincronizados, el paquete podría demorarse excesivamente, y inclusive podría llegar a ser eliminado del buffer por acumulación de paquetes en cola.

Finalment, hablar del protocolo de cifrado, llamado WEP, Wired Equivalent Privacity es decir, nivel de privacidad equivalente a una red cableada. Puede ser de 64 o 128 bits y en principio parecia un sistema bastante robusto, pero se ha demostrado que romperlo es muy fácil, y que el paso de 64 a 128 bits simplemente aumenta linealmente el tiempo necesario para hallar el código. Además, este sistema obliga al usuario y al personal de administración de la red a gestionar las claves de cifrado que se usarán, cosa que añade inconvenietes a su correcta utilización.

2.3. El certificado Wi-Fi

Para concluir este apartado, comentaremos qué es Wi-Fi (Wireless Fidelity) y cual es su relación con el IEEE 802.11.
Wi-Fi no es nada mas que un certificado que acredita que los dispositivos de distintos fabricantes podran interactuar entre ellos sins ningún tipo de problema. Esta certificación se originó debido al hecho de que en sus inicios, el protocol del IEEE 802.11b no estaba totalmente definido

y dejaba mucha libertad a los fabricantes, de modo que si no comprabas todos los dispositivos a un mismo fabricante te podías encontrar con el problema de que no se comunicasen todos los dispositivos debido a errores en el formato de las transmisiones. Esto se traducía en un freno en la expansión del 802.11b. Para superar este problema se creó una asociación de fabricants, la WECA (Wireless Ethernet Compatibility Alliance), con el objectivo de crear un certificado de interoperabilidad, el certificado Wi-Fi.
El éxito de Wi-Fi y el hecho que el término Wireless Ethernet no fuese usado demasiado, normalmente se utiliza el término WLAN, ha hecho que la WECA pasase a denominarse Wi-Fi Alliance y que utilizase Wi-Fi como sinónimo de todas las redes 802.11 y no solamente de las 802.11b. Así actualmente oímos hablar de redes Wi-Fi, es decir 802.11, formadas por productos con o sin certificación Wi-Fi. Para consultar una lista de productos con certificado Wi-Fi se puede visitar la web de la Wi-Fi Alliance, www.wi-fi.org <http://www.wi-fi.org/>.

A dia de hoy esta certificación aún tiene sentido debido a que los protocolos dejan a los fabricantes posibilidades para que incluyan mejoras, algunas en fase de estandarización, pero también han definido muy claramente cuales han de ser las funcionalidades básicas que se han de cumplir para que las comunicaciones se puedan llevar a cabo. I estos mínimos son los que asegura el certificado Wi-Fi. El posible soporte de cualquier función adicional queda fuera del ámbito de garantía de Wi-Fi.

3. EQUIPOS PROBADOS PARA EL DESPLIEGUE

Para poder llevar a cabo el despliegue de la infraestructura wireless de la EPSC se provaron diversos equipos para poder ver su rendimiento , así como las opciones que los diferenciaban del resto.

En primer lugar, se probaron dos AP's. Un Cisco Aironet 340 y un 3Com AirConnect. En todas las medidas que se hicieron, no se apreciaron grandes diferencias ni en lo referente a cobertura como a la calidad de las comunicaciones. Primero, hay que recordar que estamos en la banda ISM y que estamos limitados en poténcia, y que por tanto no eran de esperar muchas diferencias en las areas de cobertura debido a que los dos AP's trabajavan a la poténcia máxima permitida y con un diagrama de radiación omnidireccional. Sí que habría habido diferencias si se hubiesen usado antenas exteriores adicionales , pero este no era nuestro caso de interés, ya que lo que buscábamos era una radiación isotrópica que nos cubriera el máximo volumen posible. Así que la elección del AP se hizo más por cuestiones de adaptación a nuestras necesidades más que por cuestiones de rendimiento.

En segundo lugar se evaluaron tres tarjetas PCMCIA, Lucent WaveLAN Silver, Cisco Aironet 340 y 3Com AirConnect. Aquí sí que apreciaron diferencias de calidad entre ellas. En primer lugar, las tarjetas 3Com son las que obtuvieron el peor resultado en les pruebas que se realizaron, ya que eran las que peor negociaban la velocidad de comunicación con el AP, y en segundo lugar porque eran las que menos potencia recibian en igualdad de condiciones. Las otras dos tarjetas probades demostraron una alta calidad de funcionamento, ya que se mantenian en los 11 Mbps casi hasta las zones límite de cobertura. I para destacar una diferencia tenemos que la Lucent permite acoplarle una antena exterior que mejoraría las prestaciones, ya que con una antena de mayor calidad mmejoramos la calidad de la señal recibida, aumentando el área de cobertura o la calidad de la señal, cosa que con la tarjeta Cisco no es posible. El siguiente aspecte que se evalua és el soporto que tienen las tarjetas para los diferentes sistemas operativos. Aquí 3Com vuelve a quedar en último lugar, ya que sólo ofrece drivers para Windows, mientras que Cisco y Lucent, a parte del ya mencionado, ofrecen drivers y software para Linux, Unix y un largo etcétera de sistemas operativos. Este es un aspecto bastante importante, ya que las redes wireless són bastante heterogéneas en cuanto a los usuaris y es importante que no esten obligados a cambiar sus sistemas operativos tan solo para poder un hardware determinado.

Una vez finalizadas las pruebas, se decidió el AP usado sería el 3Com AirConnect y que la tarjeta PCMCIA que se usaría para las mediciones sería la Lucent. La decisión se tomó por los siguientes motivos. En primer lugar, el rendimiento que mostraron los dos AP's era muy similar, así que descartar alguno por este motivo no era fácil. Así que el elemento determinante fue la adaptación del AP al que sería nuestro entorno. Los AP's estarían conectados directamente a la red de la escuela para poder acceder a los recursos que esta nos ofrece, y por tanto detrás habría un conjunto de servidores que se encaregarían del control de acceso a los recursos, así que en este sentido lo que se necesitaba era un punto de access que no tuviese demasiadas herramientas adicionales, y en esto el AP de 3Com se presentaba como un equipo másacorde a lo requerido, ya que el AP Cisco presentaba un conjunto de funcionalidades que en nuestro entorno no eran necesarias (com por ejemplo servidores DHCP, BOOTP y opciones de filtrado avanzado entre otras, que en nuestra infraestructura no eren requeridas).

En lo referente a la tarjeta de acceso, la elección entre la Lucent y la Cisco fue bastante a gusto personal, ya que ambas presentaban unas características de funcionamiento muy similares y softwares de medición muy completos.

4. DISEÑO DE LAS COBERTURAS

4.1. Requerimientos

En primer lugar, hay los requerimientos de lo que hay que cubrir. Este despliegue representaba la primera fase de lo que se espera sea la red en un futuro, y por tanto no se quería cubrir todo el edificio en el que se ubica la Escuela.

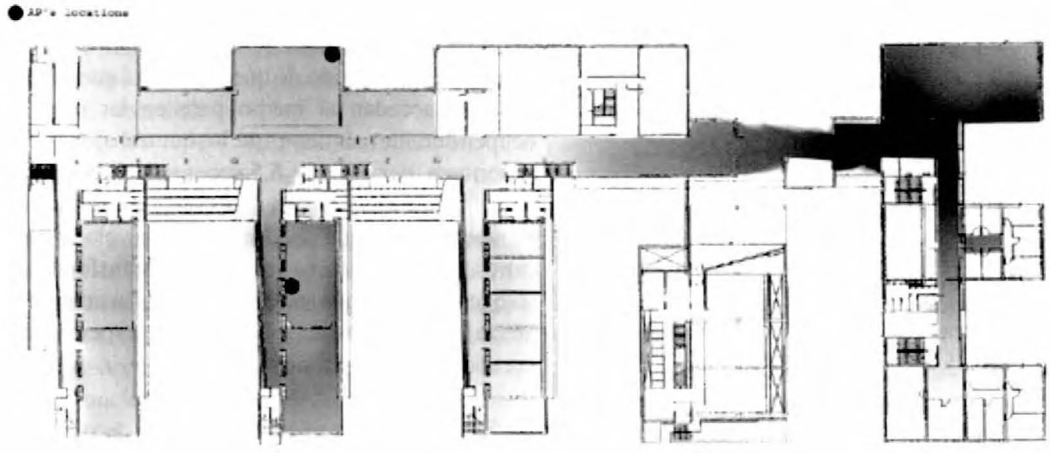

Figura 3. Plano coberturas y localización de los AP's

Las areas que se teniean que cubrir eren todas zonas comunes de la planta baja del edifici, que son salas de estudio, salones de actos y sala de reuniones, la biblioteca y el bar. En segundo lugar, se deseaba ofrecer una continuidad en el servicio, osea, que los usuarios que se moviesen entre las areas comentadas antes no perdiesen la comunicación en ningún momento. El tercer requisito era el de minimizar el número de AP's, por dos motivos. El primero y más obvio, es el factor económico. Quantos más dispositivos se usen, más caro será el despliegue. El segundo , y no menos importante, es el tema de la ocupación de canales, ya que a más puntos de acceso, más canales ocupados, y debemos recordar que los canals se solapen y por tanto no todos los canales son útiles en todos los lugares, ya que si uasmos canales cercanos deberemos mantener una distancia física suficiente para que no se creen interferencias, o deberemos reducir la potencia de transmisión.

Y como última condicióa al despliegue habia que garantizar la calidad de la comunicación, entendiendo com tal la máxima velocidad de acceso posible, osea garantizar los 11 Mbps en todas las zonas a cubrir. Y con estas premisas se inició el despliegue.

4.2. Proceso de ubicación de los AP's

Lo primero que se hizo fue un cálculo estimativo de las atenuaciones que se originaban por distancia i por los distintos materiales que constituian la estructura del edificio a partir de medidas hechas con el AP y la tarjeta seleccionada. Estos valores servirán de orientación para realizar una primera estimación de cual podría ser la ubicación ideal de los equipos.

En cuanto a las medidas previas destacar la importancia que en el desarrollo de este proyecto han jugado las zonas acristaladas del edificio. Los vidrios no suponen ningún tipo de atenuación adicional para la señal y por tanto es conveniente aprovechar dichas superfícies el máximo posible con tal de mejorar la calidad de la señal en las areas a cubrir.

Una vez decididas las ubicaciones, se situan los AP's de forma provisional en la que sería su ubicación definitiva y se miden las coberturas ofrecidas. Si són satisfactorias, es decir, cumplen con los requisitos de SNR y cobertura, se decide que esa serà su ubicación. Entonces se pasa a determinar la localización del siguiente AP, y así se va reiterando el proceso, hasta obtener el resultado definitivo. Para minimizar el númenro de movimientos es muy importante que las mediciones iniciales, a pesar de ser ser aproximadas, sean lo mas correctas posibles, ya que un mal cálculo nos puede hacer esperar unos resultados que posteriormente será imposible obtener, y como consecuencia, esto nos llevará a un número elevado de mediciones y cálculos que nunca coincidirán con lo esperado.

En la figura 3 se puede obserbar el plano de la planta baja del edificio y la ubicación de los AP's y el área que cubre cada uno donde están garantizados los 11Mbps.

5. EXPLOTACIÓN DE LA RED

Actualmente la WLAN actua como una extensión de la red de la EPSC y en concreto de una de sus VLANs (Virtual LAN). Un usuario cualquiera con un sistema operativo plug&paly tan solo necesita insertar la tarjeta WLAN en su ordenador y mediante DHCP obttiene todos los parámetros de configuración TCP/IP necesarios para comunicarse con la red. Esta situación que en un principio puede parecer la idonea puede provocar gran cantidad de problemas, algunos asociados a la seguridad y otros de escalabilidad, derivados principalmente de las particularidades de la tecnología 802.11b. A continuación pasamos a comentar los más importantes y cuales han sido las soluciones aplicadas.

5.1. Problemas que se plantean

La VLAN en la que se encuentran los APs está asociada a una subred IP con un total de 254 IPs públicas libres a repartir entre los diferents equipos que la participan, algunos de ellos usuarios de la WLAN. Esta situación

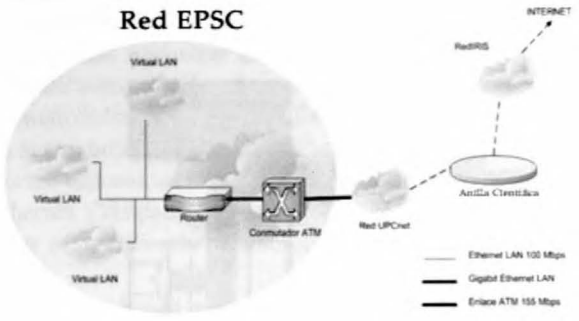

Figura 4. Esquema simplificado de la de de la EPSC y su salida a Internet

puede provocar la aparición de dos problemas. El primero una posible insuficiencia de direcciones IP que actuará como limitador del número de usuarios posibles de la WLAN. El segundo viene dado por el hecho de que el access rádio es más inseguro por naturaleza, y en concreto la tecnología 802.11 se ha demostrado bastante vulnerable. Esto podría suponer un agujero de seguridad potencial para todos los equipos que forman parte de la VLAN, ya sean usuarios de la WLAN o no. Anteriormente ya se ha comentado que el cifrado WEP no es una buena solución para garantizar la confidencialidad de los datos de los usuarios de la WLAN. Además el suyo presenta algunos inconvenientes prácticos associados: necesidad de tarjetas y AP's compatibles, distribución de claves y caida de la velocidad de transmisión.

Per otro lado el mecanismo de acceso del 802.11b puede ofrecer como mucho 11Mbps que se pueden convertir en el mejor de los casos en poco más de 6Mpbs de datos de aplicación. Estos recursos són a repartir para todos los usuarios conectados a un mismo AP, y si su número es muy elevado se ha comprovado que la velocidad que obtiene cada usuario está por debajo del resultado de dividir la velocidad total de acceso por el número de usuarios activos.

Otra situación que puede degradar las prestaciones de la res es el hecho que algunos usuarios accedan a baja velocidad (por ejemplo 2Mbps) debido a que se encuentren en zonas límite de cobertura. A menor velocidad, más tiempo de transmisióo, lo que provocará que cuando estos usuarios accedan al medio para enviar una trama lo ocupen durante más tiemp que los que trabajen a velocidads superiores, por ejemple 5,5 veces más que los que van a 11Mbps. La coexisencia de estos dos tipos de usuarios provoca que los que pueden trabajar a velocidades superiores vean reducida su velocidad de transferéncia global ya que a pesar de que su velocidad de transmisión no se ve afecta sí que aumenta el tiempo de espera para poder acceder al medio y transmitir.

5.2. Soluciones usadas

Como primera medida para preservar la segurdad del resto de equipos de la red de la EPSC se decidió crear una nueva VLAN formada única i exclusivament por los AP's de la WLAN. Además esta VLAN se conectaria al resto de la red de la EPSC a través de un PC Linux que actuaría como Firewall. De esta manera se consigue aislar y controlar todo el tráfico de la red WLAN. Aprovechando esta arquitectura de red se decidió usar IPs privadas y que el PC Linux Firewall realizase las funciones de NAT y servidor DHCP, convertiendo el PC Linux en lo que se conoce cómo *Wireless Firewall Gateway* (WFG).

Con esta propuesta se rompía el límite impuesto por número de IP's públicas disponibles y gracias al servidor DHCP propio se podía realizar una asignación de IP's a medida en la que, por ejemplo, a diferentes colectivos (alumnos, PAC, PAS o otros) se les assignan grupos de IP's diferents que faciliten su diferenciación, incluso en términos de QoS utilitzando Diffserv, y pudiesen dar a cabo políticas de filtrado distintas en el Firewall.

Respecto al problema de la confidencialidad de los datos enviados por el medio rádio se ha desestimado la utiliza-

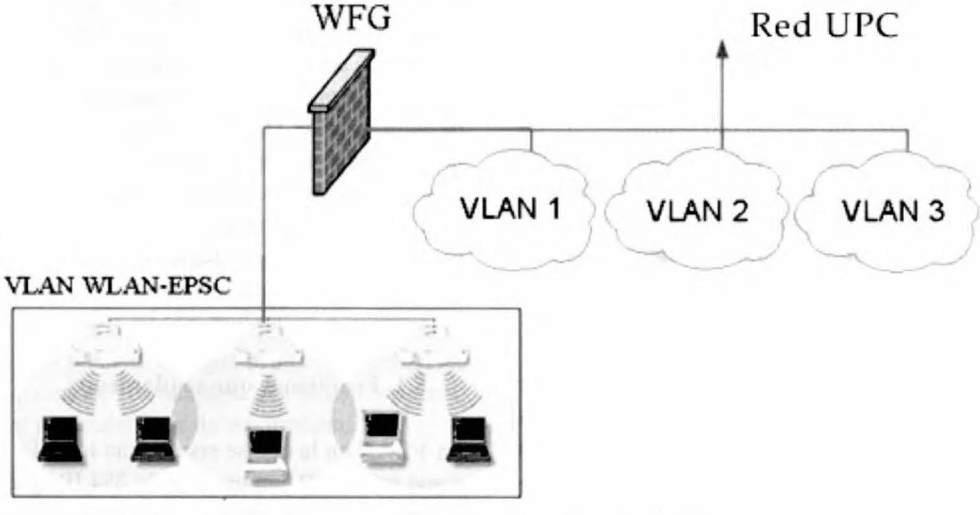

Figura 5. Integración de la WLAN en la red de la EPSC

ción de WEP porque hemos creido que sus inconvenientes pesaban más que sus virtudes. El usuario ha de ser consciente de que utiliza un canal inseguro y si lo cree convenient puede utilitzar herramientas alternativas para proteger sus datos: cifrado del correo, acceso a web o correo seguro o redes privadas virtuales.

Para evitar que usuarios no deseados utilizen la red WLAN y provoquen una degenarión del rendimiento de la red se limita el acceso a ésta usando una función presente en la mayoría de los AP's: el filtrado por dirección física (MAC). Esto tiene un inconveniente: para poder utilizar la WLAN es necessario que el usuario de de alta la MAC de su tarjeta al gestor de la red, y que este la de de alta en los AP's. Otra funcionalidad de los AP's que nos puede ayudar a evitar el efecto de los usuarios de baja velocidad es el fijar una velocidad mínima de associación por debajo de la cual un usuario no puede utilizar un AP. Esto tiene como inconveniente que se limita el área de servicio a las zones donde la calidad de la señal permite conseguir la velocidad fijada. Por lo que hay un compromiso entre ofrecer la máxima cobertura posible o limitarla para asegurar unas mejores prestaciones.

6. CONCLUSIONES

Después de todas las pruebas, medidas y cálculos se consiguió montar la red con solo tres APs. Esto fue posible gracias a la curiosa forma del edificio, que ha permitido que grandes zonas tuviesen visión directa desde un mismo AP, pudiendo así minimizar su número. Además, todas las zonas están solapadas entre sí, y por tanto no existe pérdida de conectividad en ningún momento, y finalmente, se ha garantizado que en todos los puntos requeridos inicialmente la calidad de la conexión es tal que la comunicación sea a 11 Mbps. La integración a la red de la EPSC y su explotación como servicio se ha resuelto con creación de una nueva VLAN y la introducción de un PC Linux con las funciones de cortafuegos, NAT y servidor DHCP, y la utilización de control de acceso por MAC en los APs.

El servicio se encuentra en funcionamiento desde el cuadrimestre de otoño 2002/03 con un préstamo de tarjetas y suporte técnico a les persones interesadas en utilizar la red gestionado por Servicios Técnicos de la EPSC. Además, gracias a un acuerdo con el CRSD (Centro de Recursos de Suporte a la Docencia) enmarcado dentro de un convenio con entre l'ICE (Instituto de Ciencias de la Educación) y la EPSC para llevar a cabo experiencias de innovación docente utilizando WLAN se ha conseguido incrementar de manera considerable el número de APs y tarjetas disponibles. Esto permitirá aumentar la cobertura del acceso wireless a prácticamente la totalidad de la EPSC convirtiendo cualquier aula de teoría, reuniones o trabajo en grupo en un potencial laboratorio informático.

Como líneas futuras de este proyecto nos hemos marcado dos caminos a seguir. Por un lado se pretende extender la cobertura al exterior de la EPSC y por otro desarrollar herramientas basadas en software de código abierto y libre distribución que permitan una gestión integral de la red wireless y faciliten su utilización. Respecto a este último objetivo se está trabajando para pasar de una política de control de acceso basada en la MAC a otra basada en el login y password utilizando el software NoCatAuth.

7. BIBLIOGRAFÍA

[1] Despliegue de una red WLAN a la EPSC. Xavier Bordoy (autor), David Remondo i Rafael Vidal (director y subdirector) Trabajo fin de carrera, EPSC, julio 2002

[2] Explotación de una red WLAN a la EPSC. Daniel Martínez (autor) i Rafael Vidal (director) Trabajo fin de carrera, EPSC, julio 2002

[3] Mobile Communications. Jochen Schiller. Editorial Addison-Wesley, 2000

[4] Wireless Lans. Jim Geier. Editorial MacMillan technical publishing, 1999

[5] Weaknesses in the Key Scheduling Algorithm of RC4. Scott Fluher, Itsik Mantin, and Adi Shamir. 8th Annual Workshop Selected Areas in Cryptography, Agost 2001

[6] An Empirical Characterization of Instantaneus Throuput in 802.11b WLANs A. Vasan i A.U. Shankar. University of Maryland, report tècnic, CS-TR-4389, UMIACS-TR-2002-69. <http://www.cs.umd.edu/~shankar/Papers/802-11b-profile-1.pdf>

[7] Wireless Firewall Gateway White Paper. Nichole K. Boscia, Derek G. Shaw. NASA Advanced Supercomputing Division. <http://www.nas.nasa.gov/Groups/Networks/Projects/Wireless/>

[8] NoCatAuth. The NoCat Community Wireless Network Project. <http://nocat.net/nocatrfc.txt>

AUTORES

Rafael Vidal, Ingeniero de Telecomunicaciones por la ETSETB y profesor del Departamento de Ingeniería Telemática desde el año 2000, con docencia en la EPSC. Forma parte del grupo de investigación de comunicaciones inhalámbricas desde el año 1998, su ámbito de trabajo es el soporte a la movilidad en redes fijas.

Xavier Bordoy, Ingeniero Técnico de Telecomunicaciones por la EPSC desde el año 2002 y becario del departamento de Ingeniería Telemática de la misma facultad. Vinculado actualmente al proyecto i2CAT, investiga sobre tecnologías multimedia para las redes de Internet 2, y más específicamente en la retransmisión de televisión de alta definición sobre IP.