



La universidad
virtual

www.uoc.edu

Estudios de Informática y Multimedia

Proyecto Fin de Carrera
Estudio del despliegue de redes inalámbricas en
el ámbito de un hospital universitario
multicéntrico y de alta complejidad.

Apellidos: *Sánchez Fernández*

Nombre: *Luis Santiago*

A mi madre, mi mujer, mis familiares y amigos.

Por la comprensión y apoyo que han sabido darme en todos estos momentos de labor, robados muchas veces del tiempo que ellos se merecían.

Junio de 2006.

Determinación del procedimiento de estudio.

Objetivos

Determinar el procedimiento que se deberá llevar a cabo para realizar las medidas de campo del alcance y, en caso de que se den las circunstancias, llevar a cabo la medición de la interacción con el resto del equipamiento médico de determinadas zonas críticas.

Tareas realizadas.

- Recopilación de planos de los edificios.
- Estudio superficial de dichos planos.
- Recopilación de información técnica y normativa sobre Wireless.
- Búsqueda de equipamiento hardware para realización de medidas.
- Estudio de los procedimientos posibles.

• Estudio de los planos de los edificios.

El hospital está situado en una finca de unas 2 hectáreas. Consta de 13 edificios que, según su funcionalidad, podemos clasificar según en: edificios hospitalarios, edificios de gestión y otros edificios. También existen varios espacios al aire libre pero que no serán considerados del proyecto de cobertura Wireless, pues el alcance de éste se limita principalmente al ámbito de aplicación del entorno clínico y de gestión. Simplemente se analizarán las distancias entre edificios de cara a posibles enlaces troncales inalámbricos.

Todos los edificios se encuentran distribuidos de forma más o menos uniforme a lo largo del terreno cubierto, con unas distancias medias entre ellos de unos 100 metros lineales, sin contar las diferencias de alturas de cada edificio.

Descripción de los edificios:

- H1 (Caseta de Seguridad)
Estructura: 1 planta cuadrangular de 20m. x 10m.
Uso: Centro de control de Vigilancia.
- CDCA (Centro de Documentación Clínica)
Estructura: 1 planta de forma rectangular de 130m. x 24m.
Uso: Archivo de historias clínicas y dependencias de administración.
- H.G. (Hospital General)
Estructura: 10 plantas en forma de X irregular de unos 180m. x 150m.
Uso: Hospitalario.
- E.L. (Edificio de Laboratorios)
Estructura: 8 plantas en forma rectangular de unos 100m. x 20m.
Uso: Laboratorio, Investigación y Consultas.
- H.R.T. (Hospital de Rehabilitación y Traumatología)
Estructura: 7 plantas en forma de Y de unos 100m. x 120m.
Uso: Hospitalario.
- H.M (Hospital de la Mujer)
Estructura: 8 plantas en forma de D de unos 80m. x 60m.
Uso: Hospitalario.

- H.I. (Hospital Infantil)
Estructura: 5 plantas de forma irregular de unos 95m. x 80m.
Uso: Hospitalario
- Lav. (Lavandería)
Estructura: 2 plantas de forma rectangular de unos 30m. x 50m.
Uso: Lavandería Industrial.
- E.G.R. (Edificio de Gestión de Recursos).
Estructura: 1 planta rectangular de 90m. x 63m.
Uso: Administrativo y Almacén.
- U.A. (Unidad Alimentaria)
Estructura: 2 plantas de forma rectangular de unos 56m. x 40m.
Uso: Almacén y cocina.
- Q.E. (Quirófano Experimental)
Estructura: 2 edificios rectangulares de 1 planta y unos 12m. x 10m.
Uso: Investigación
- A.P. (Anatomía Patológica)
Estructura: 2 plantas rectangulares de unos 42m. x 32m.
Uso: Laboratorios, Aula y Tanatorio.
- C.D.T. (Centro de Diagnóstico y Tratamiento)
Estructura: 5 plantas rectangulares de 75m. x 25m.
Uso: Consultas.
- E.G. (Edificio de Gobierno).
Estructura: 2 plantas rectangulares de 86m. x 30m.
Uso: Biblioteca, Escuela Universitaria y Dirección Gerencia.

Disposición geográfica y planos.



Ilustración 1: Disposición geográfica de los edificios

En el anexo 2 se pueden encontrar planos más detallados de cada edificio.

Procedimiento de estudio.

Documentación de cada edificio.

El primer paso será crear documentación de cada edificio donde se recoja la siguiente información:

- Datos de estructura del edificio: número de plantas y medidas de superficie, longitud y anchura de cada planta o de cada una de sus partes.
- Reunión con el responsable de mantenimiento de cada edificio para que nos indique qué posibles puntos conflictivos pueden existir (elementos emisores de ondas, posibles zonas libres de radiofrecuencias, muros especiales, etc.) y la estructura física de los edificios a nivel de paredes y suelo (tabiques de ladrillo, pladur, muros de carga, etc.)
- Análisis de distancias según los planos: De estos datos extraeremos una estimación aproximada del patrón de medidas de alcance por cada edificio y planta.

Con la información recopilada para cada edificio se procederá a realizar un estudio sobre el terreno que cubra los siguientes aspectos:

- Búsqueda de redes inalámbricas ya existentes.
- Medidas de alcance en los puntos identificados en el primer paso del procedimiento de estudio.
- Medidas de interferencias en los puntos más críticos.

Búsqueda de redes inalámbricas ya existentes.

En este apartado trataremos de identificar posibles redes ya existentes.

A día de hoy el Servicio de Tecnologías de la Información (STI) no dispone de despliegue de redes inalámbricas, sin embargo esto no es una garantía para poder asegurar que ningún usuario haya desplegado su propia red inalámbrica para su zona de trabajo. Como dichas redes podrían entrar en conflicto con la futura red a implantar, se realizará un búsqueda e identificación de posibles redes en funcionamiento.

Equipamiento:

- Un dispositivo ligero capaz de identificar redes Wireless (en concreto el Kensington WiFi Finder Plus), capaz de identificar tanto redes inalámbricas como dispositivos bluetooth. Ambos pueden causar interferencias con nuestra futura red por trabajar en la misma banda de frecuencias, como veremos en el estudio tecnológico.
- Un ordenador portátil con tarjeta de red inalámbrica y S.O. Linux y Windows XP.
- Software de identificación de redes inalámbricas. iwconfig y Kermit en Linux, Netstumbler en Windows.
- Sonda de análisis espectral Wi-Spy de la empresa MetaGeek¹.
- Sonda Fluke OptiView.
- Software de monitorización y análisis de red: nmap, ethereal, tcpdump, etc.

Procedimiento:

Primero se realizará una búsqueda de redes con el dispositivo ligero, recorriendo las plantas y pasillos de los edificios. Conviene hacer este recorrido durante las horas de trabajo habituales (de 8 a 15h) pues puede que algunas de las redes sean

¹ Wi-Spy is wireless LAN RF analysis (<http://www.metageek.net/>)

desactivadas cuando nadie las usa. En los puntos donde se identifiquen fuentes wireless o bluetooth se marcarán sobre los planos.

En un segundo recorrido se usará el ordenador portátil para acudir a los puntos identificados y tratar de analizar la información recogida sobre la red existente.

Usando el programa netStumbler registraremos los siguientes datos:

- Identificación del lugar: Si se dispone de un GPS mediante la localización y la planta. En caso contrario la identificación más cercana según la terminología usada en el edificio (puerta 4-b pasillo impares, consulta 3 de respiratorio, etc.)
- Tecnología (Bluetooth, 802.11a/b/g, otras)
- [SSID](#) y [MAC](#) del punto de acceso.
- Medidas de la señal recogida.
- Protocolos de encriptación identificados (Ninguno, [WEP](#), [WPA](#), [WPA2](#), etc).
- Dirección IP y rango que ofrece si es posible identificarlos.
- En caso de poder localizar el punto de acceso físicamente: su ubicación, marca, modelo, revisión de [firmware](#), etc.

En los puntos donde se llegue a identificar la MAC del punto de acceso se realizará una búsqueda del dispositivo en la LAN usando el Fluke para localizar su conexión y posteriormente con los programas de análisis tratar de comprobar sus restricciones de acceso a la configuración.

Con toda esta información se realizará una hoja de descripción de la infraestructura wireless detectada para dejar registro de la misma.

Medidas de alcance en los puntos identificados en el 1^{er} paso.

Equipamiento:

- Punto de acceso Cisco Aironet 1100.
- Tarjeta de red Intel Pro/Wireless 2200BG.
- Equipo PC portátil.
- Software. Un script propio que utiliza la información del iwconfig de Linux que se acompaña en el anexo 1.

Procedimiento:

Para realizar estas mediciones, primero se realizará una fase de pruebas de “calibración” de los elementos donde se tomen muestras de nivel de señal, ruido, ancho de banda y alcance entre los puntos de acceso y el portátil en un entorno libre de obstáculos y lo más libre posible de otras fuentes de interferencia.

A partir de dicha calibración se realizarán pruebas de campo en los puntos identificados en el paso de “documentación de cada edificio”, con al menos uno de los puntos de acceso y el ordenador portátil.

En las pruebas de campo se realizará previamente un plano de la zona donde se van a realizar las medidas indicando la situación de los puntos de acceso y el recorrido a realizar. También se debe solicitar un permiso adecuado a los responsables de los lugares a visitar, informándoles mediante el circuito establecido para comunicarse con dicho responsable (telefónicamente, circular interior, correo electrónico, etc.) que se va acudir para realizar unas pruebas de campo de redes inalámbricas. Convendrá tener redactado un pequeño documento sobre las pruebas a realizar.

Posteriormente se realizará una agenda de visitas en función de los permisos obtenidos, reservando al menos una media hora por visita.

El proceso de medida consistirá en:

- Realizar un croquis en papel del lugar a analizar. Dada la cantidad de obras que se realizan en las instalaciones a veces los planos no reflejan la realidad. En el croquis es importante apuntar los obstáculos que se encuentren así como la naturaleza de los mismos.
- Colocación del punto de acceso en el lugar elegido, si es posible conectado a la LAN.
- En el equipo portátil, a corta distancia del punto de acceso, nos aseguraremos de disponer de un buen nivel de señal, es decir de tener acceso a la red. Para las pruebas el equipo se configurará sin DHCP para evitar retrasos en la recuperación de la conectividad en caso de que se pierda la señal.
- A partir de aquí se realizarán tres tipos de medidas:
 - Medidas estáticas durante 5 segundos en al menos 8 localizaciones a diferentes distancias del punto de acceso y, si es posible, interponiendo algunos obstáculos entre ambos.
 - Partiendo del punto de acceso activaremos el programa realizado, cuyo código se encuentra en el anexo 1, y comenzaremos a realizar el recorrido tomando las medidas en los puntos indicados.
 - En los casos donde se disponga de acceso LAN. Realizar una medida de la tasa de transferencia con la descarga mediante ftp de un fichero muestra en al menos dos de los puntos más alejados con cobertura [WLAN](#) y comprobar el ancho de banda real obtenido.
- Por último se registrarán cuales son los puntos más lejanos donde se dispone de cobertura.

Por cada punto se realizará una ficha con la siguiente información:

- Plano teórico con recorrido.
- Croquis real.
- Número de medidas estáticas realizadas.
- Gráfico de los valores de la señal y el ancho de banda a lo largo del recorrido realizado.
- Situación de los puntos de medida de tasa de transferencia, el ancho de banda máximo, medio y mínimo obtenidos, así como los valores de la señal y el ancho de banda teórico.

Medidas de interferencias.

Existen algunos puntos en la infraestructura del hospital que son especialmente propensos a las perturbaciones electromagnéticas dentro del rango de los 2.4 Ghz. Según el [\[CNAF\]](#) dicha banda puede ser utilizada para fines Industrial, Científico o Médico ([ICM](#)) y en concreto además de para redes WLAN se utiliza para señales [RF](#) de: teléfonos inalámbricos, emisores de video, conexiones bluetooth, etc.

En concreto, en el estudio [\[ETGF-ES\]](#) especializado en entornos sanitarios encontramos en la página 39 varias normativas sobre equipamiento sanitario que opera en rangos de frecuencia que se solapan con WLAN:

- EN 300 440-1 de Dispositivos de Corto Alcance en banda de frecuencias de 1Ghz a 40Ghz.
- ETS 300 328 de Equipos y Sistemas Radio para Transmisión de Banda Ancha en la banda ICM de 2,4 Ghz con técnicas de modulación de amplitud de espectro.
- ETS 300 440 de Equipos y Sistemas Radio para Dispositivos de Corto Alcance en la banda de 1 Ghz a 25 Ghz.

También comenta un uso cada vez mayor de elementos de telemetría que usan también la banda de ICM 5 de 2,4Ghz.

Para este apartado se deben mantener reuniones con el personal responsable del equipamiento de telemetría (área de Electromedicina) y comprobar los puntos donde se estén utilizando y su espectro de frecuencia.

También se van a analizar las diferentes interferencias de elementos comunes en el entorno y su impacto en el espectro de frecuencias usado por la red Wireless (2.4 Ghz). Para ello se contará con la ayuda de un pequeño analizador especializado en dicho rango y el software que le acompaña.

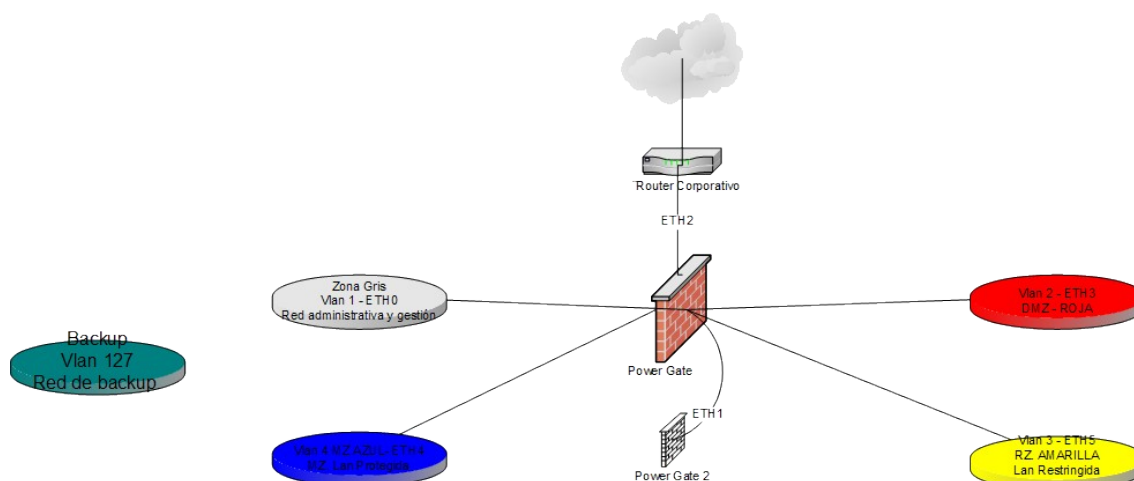
Estudio Tecnológico.

Análisis de objetivos del estudio.

Ámbito de trabajo.

Tipo de red actual.

La distribución actual de la red corporativa consiste principalmente en un único dominio en las capas física y de enlace, dividido en diferentes Vlanes en la capa de enlace. El 70 % de los puestos clientes dispone de conexiones a 100Mbits mientras que el 30% restante está conectado a 10 Mbits. La electrónica de red es Cisco en esa misma proporción, generalmente el modelo 2950 con diferentes versiones de Firmware.



Distribución en VLANs. El color identifica la VLAN.

Estamos conectados a una red mayor organizada por una entidad de la que depende el hospital y a través de ellos nos mantenemos conectados a los Servicios Centrales de dicha organización y a Internet.

La mayoría de los equipos cliente se encuentran instalados a lo largo de los diferentes edificios en la VLAN 1 (zona gris) y constituyen un único dominio de colisión. Algunos equipos dedicados a labores como la consulta de Internet de alumnos o uso por parte de entidades o personal externos (empresas, salas de conferencias o congresos, etc.) están aislados del resto de equipos y servicios a través del cortafuegos que les ofrece unos servicios mínimos de conectividad (acceso a Internet básicamente).

Respecto a las medidas de seguridad, se dispone de un DHCP corporativo que asigna direcciones a las máquinas conocidas. A niveles OSI superiores se dispone de una validación de usuario centralizada para permitir el acceso de los usuarios.

Además cada aplicación suele disponer de su sistema propio de validación de usuario, a menudo apoyado en un servicio de directorio interno basado en tecnologías Microsoft, pero mejorado en la integración con otros entornos heterogéneos mediante un desarrollo propio.

La red actual consta de unos 2000 equipos PC en red en un 99% con sistema operativo Microsoft Windows, pero de múltiples versiones (98, nt, 2000, xp), de ellos un 10% pueden ser equipos portátiles dotados de tarjetas wifi sólo los más recientes. Asimismo existen unos 30 servidores también de diferentes tecnologías, que se

encuentran repartidos entre la zona gris, la zona azul y el exterior ([SS.CC.](#)).

Tipos de clientes de red actuales.

En nuestra red actualmente podemos distinguir los siguientes perfiles de usuario:

- Profesionales de medicina y enfermería.
- Administrativos de las zonas asistenciales.
- Administrativos de las zonas de gestión.
- Directivos.
- Personal de investigación.
- Pacientes y estudiantes.

A continuación haremos un pequeño repaso de las necesidades de conectividad que tienen a día de hoy estos usuarios en función de las aplicaciones que generalmente usan:

- Profesionales de medicina y enfermería.
Utilizan principalmente aplicaciones de registro de información de los pacientes, algunas veces departamentales, la historia clínica electrónica y algunas aplicaciones de diagnóstico.
- Las aplicaciones de registro de información suelen ser aplicaciones cliente/servidor, las departamentales están basadas en numerosas ocasiones en [BBDD Access](#), y su consumo de ancho de banda suele ser bajo o medio en el caso de aplicaciones corporativas que generalmente están basadas en motores de BBDD como Sybase u Oracle, y alto cuando usan Access, pues este gestor mantiene una conexión constante con un fichero albergado en algún servidor de ficheros de la red.
- La [Historia Clínica Digital \(HCD\)](#) usa un cliente Web y su consumo de ancho de banda es pequeño, pues generalmente lo único que transfiere son los datos (texto) de los diferentes episodios del paciente y sus informes. En algunos casos se utiliza para consultar analíticas que se presentan como diagramas de barras sencillos. En algunas ocasiones se accede a través de la HCD a imágenes (radiográficas generalmente) lo cual conlleva un consumo de ancho de banda mucho mayor en momentos puntuales.
- Aplicaciones de diagnóstico. Generalmente basadas en el estándar de intercambio de información médica [DICOM](#), suelen consistir en el envío de imágenes diagnósticas para que el facultativo las evalúe y realice un informe del estudio realizado. En estos casos generalmente el trasiego de la imagen suele realizarse sin compresión, por lo que se necesitan anchos de banda altos y poca latencia en la comunicación.
- Administrativos de las zonas asistenciales.
Utilizan la aplicación de gestión hospitalaria, basada en el paradigma cliente/servidor, siendo bastante sensible a las desconexiones de red, debido principalmente a su acceso a datos a través de [ODBC](#), y a la forma en la que se construyó.
En algunos casos ha sido necesaria una auditoría de red por fallos sucesivos de la aplicación que finalmente han sido diagnosticados como una conexión deficiente a red (Incongruencia half/full duplex entre cliente y switch por errores en la negociación ha sido de las más comunes), que no impedía trabajar con otros recursos de red pero si afectaba a dicho aplicativo.
Su dependencia pues se ha comprobado que no es tanto respecto al ancho de

banda necesario (10 o 100 Mbits) sino a la pérdida de conexión.

- Administrativos de las zonas de gestión.
Estos usuarios generalmente se dividen según sus competencias en:
 - contabilidad, suministros y almacén que utilizan una aplicación del propio hospital basada en emulación de [terminal VT](#). Su consumo de ancho de banda es mínimo y poco sensible a las desconexiones.
 - RR.HH. que usan algunas aplicaciones corporativas más complejas (conexiones ftp, [emulación 3270](#) o Citrix, impresión remota por LPD).

Estos cuatro grupos de usuarios son los que se encuentran actualmente en el EGR, analizado en el apartado de medidas de alcance.

- Directivos.
Generalmente su conexión suele ser a las mismas aplicaciones que usa el personal a su cargo. Sin embargo también utilizan otras aplicaciones de análisis cruzado de datos e intercambio de ficheros de gran tamaño que recogen diferentes aspectos de gestión. También generalmente necesitan un mayor nivel de movilidad y puntualmente poder sincronizar información desde [PDA](#)s (tales como su agenda o la lista de llamadas), sin necesidad de ir a su despacho.
- Personal de Investigación.
A menudo intercambian con el exterior grandes ficheros de muestras de datos y de publicaciones (pósters, conferencias, etc.) Son los que más utilizan las conexiones a Internet, por motivos profesionales. Generalmente utilizan equipos Macintosh de diferentes generaciones.
- Pacientes y Estudiantes.
A día de hoy las prestaciones que se dan a los pacientes son muy reducidas. Sólo a determinados pacientes con estancias prolongadas (varios meses) se les da acceso a Internet a través de la línea telefónica de la habitación. Respecto a los estudiantes, se dispone de una sala en la biblioteca donde pueden realizar consultas en Internet, como un cibercafé.

Necesidades generales:

A nivel general el acceso a Internet y el uso del correo interno y externo vía web para consultas, investigación y ocio está cada vez más extendido entre los usuarios. Sin embargo no se considera una aplicación crítica. A esta regla existe una excepción para algunos casos tales como aplicaciones del: Ministerio de Salud, la Tesorería de la Seguridad Social o el Ministerio de Hacienda, que sí son utilizados de forma extensiva en algunas áreas como parte de su trabajo diario.

Teniendo en cuenta que el personal suele moverse entre diferentes ubicaciones de los diferentes centros (consultas en el CDT, despachos en alguno de los hospitales o incluso en varios), también se da mucho la compartición de ficheros entre los diferentes PCs de la red.

Por último, también se usan métodos de impresión distribuida donde un equipo cliente imprime a través de impresoras conectadas a otro cliente..

Objetivos del estudio.

Tipos de clientes de red futuros.

Al plantearnos este proyecto se han tenido en mente las necesidades futuras informadas por la dirección del hospital. Los ámbitos tecnológicos con más innovación se plantean en los siguientes puntos:

- **Internet para pacientes.**
Cada vez está siendo más común disponer de acceso a Internet desde la cama del paciente como mejora de la calidad de la estancia del paciente. Esto en Hospitales como el Infantil o Traumatología donde el índice de adolescentes es mayor, podría acometerse como proyecto piloto dentro del propio centro.
- **Diagnóstico digital.**
Las técnicas de exploración y las pruebas que se realizan a los pacientes cada vez se registran con mayor frecuencia en elementos digitales susceptibles de enviar dicha información a través de una red desde el punto de origen a un almacenamiento indexado donde el médico pueda consultarla.

De momento los sectores donde más se está avanzando en este sentido son en el diagnóstico por imagen y en las analíticas. Sin embargo especialidades como Cardiología, Radioterapia o Cirugía Plástica están comenzando a solicitar también conexión a la red del hospital para la transmisión de información.

- **Informes por voz.**
Otro de los proyectos más innovadores es dotar a la historia clínica digital de "oído" para que así los médicos puedan realizar sus informes directamente por voz sin tener que transcribirlos al ordenador de forma manual.
- **Movilidad e informe desde la cama del paciente.**
Disponer de la información desde el punto más cercano posible al paciente ayuda mucho a la labor médica, al disponer en todo momento de la historia del paciente, sus informes y analíticas y diagnósticos anteriores que pueden estar relacionados con el episodio actual que lo mantiene ingresado.
- **Mejoras en la red LAN.**
Con motivo de la gran cantidad de cambios tecnológicos producidos en los últimos años y dado que la red actual está basada en un cableado de fibra óptica en estrella del año 1994, se va a acometer en breve una renovación completa del cableado.

A pesar de disponer en el nuevo diseño de sistemas de alta disponibilidad, no se cuenta con redundancia en el camino entre los edificios. Por ello otro de los objetivos sería contemplar la posibilidad de usar conexiones inalámbricas como líneas de respaldo en caso de rotura de las líneas principales de comunicación.

Interferencias con otros equipamientos.

La banda de frecuencias de 2.4 Ghz, usada por las redes inalámbricas tipo b y g que son las más extendidas, también está ocupada por otros muchos equipos de transmisión de datos, dado que es un espectro de frecuencia de uso libre. También a veces se pueden producir interferencias por otros equipos como por ejemplo los microondas o los de transmisión de imágenes de video por radiofrecuencia.

Hemos usado una sonda especializada para dicho rango para medir interferencias de algunos elementos que pueden estar presentes en nuestras instalaciones y sacar de ello algunas conclusiones de cara al despliegue de puntos de acceso.

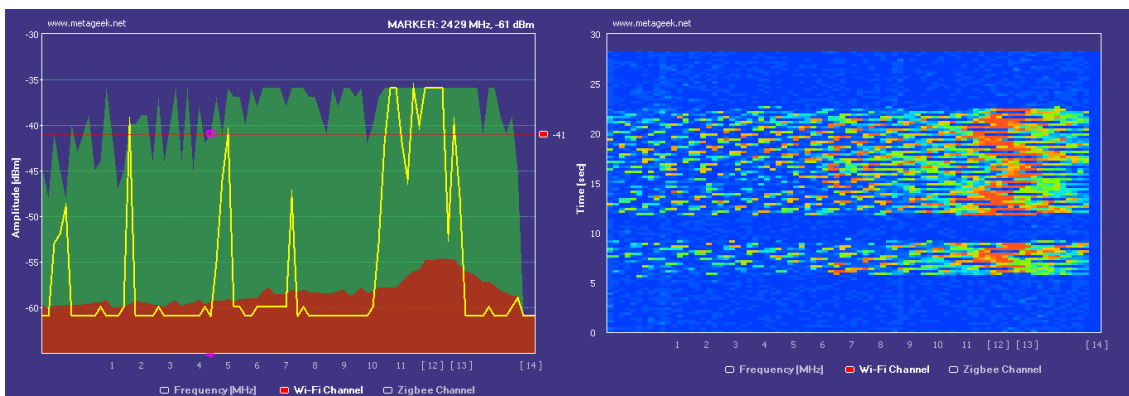
El programa que acompaña a la sonda dispone de una escala en el dominio de la frecuencia mostrando tres informaciones diferentes a lo largo del tiempo:

- Un eje de coordenadas que indica en el eje de abscisa los canales wireless y en el ordenadas la amplitud en **dBm** de la señal medida.
- Las líneas amarillas marcan la amplitud instantánea registrada para cada frecuencia.
- Las zonas rojas marcan la intensidad acumulada en cada frecuencia durante el tiempo de la medida.
- Las zonas verdes marcan los máximos medidos.

El programa también dispone de otro modo de visualización “3D” que cambia en el eje de ordenadas la amplitud por el tiempo, y va registrando la amplitud mediante códigos de color siendo el azul el mínimo y el rojo el máximo.

A continuación acompañamos un pequeño estudio de elementos que producen interferencias y que suelen encontrarse en un entorno de trabajo tan heterogéneo como este:

- **Microondas.**
Este tipo de elementos es común en las salas de descanso del personal. El registro se realizó con el equipo a unos dos metros de distancia mientras se usaba el horno microondas a plena potencia. Como vemos provocan gran distorsión a lo largo de todo el espectro (zonas verdes que marcan los máximos alcanzados), aunque más centrado en una parte de éste. Si montáramos un punto de acceso en un lugar cercano a este elemento, las interferencias serían más acusadas en los canales superiores, aunque probablemente este efecto dependerá realmente del modelo. Lo más importante de este efecto es lo difícil que resultaría diagnosticar una incidencia de usuario provocada por este equipo, ya que la desconexión duraría escasos minutos y sólo durante el tiempo de uso.

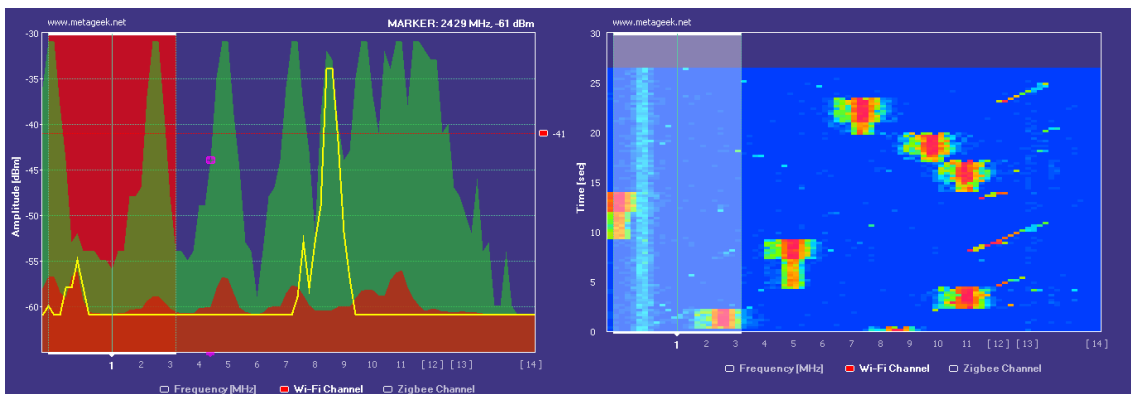


Interferencias de un horno microondas casero

- Teléfono inalámbrico.
Aunque la mayoría de los teléfonos usados en el hospital son terminales fijos hay algunos despachos y salas de reuniones que pueden contar con equipamiento inalámbrico.

Su efecto es más aleatorio que el anterior y vemos como la interferencia va cambiando de banda. En sumatorio (zona roja) no parece afectar demasiado a una comunicación fluida.

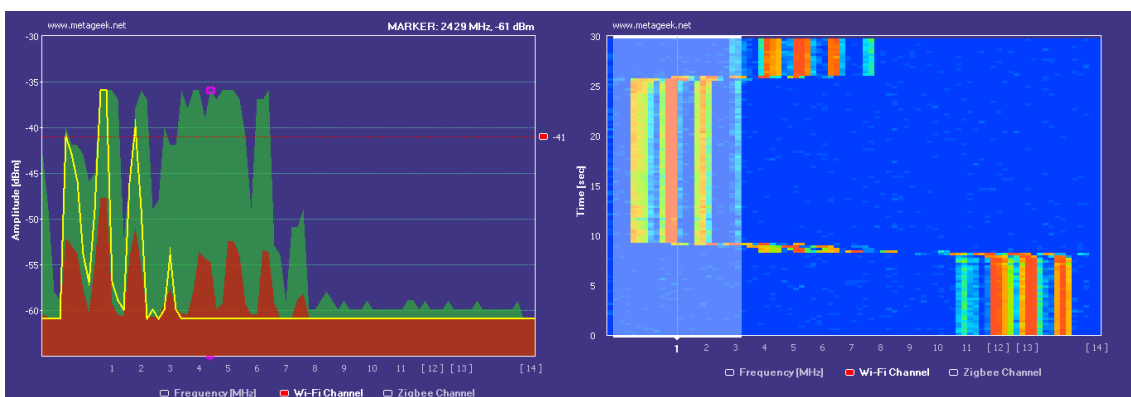
De todas formas conviene informar al personal de Mantenimiento, responsables del despliegue de telefonía, de que nos avisen cuando vayan a montar alguno de estos teléfonos cerca de alguna zona de servicio inalámbrico.



Interferencias de un teléfono inalámbrico

- Emisora de vídeo.
Menos habitual, pero mucho más distorsionadoras son las emisoras de video que usan el rango de los 2.4 Ghz.
Como vemos el efecto es enorme y sostenido. En los gráficos que se acompañan hemos cambiado la frecuencia base de trabajo del aparato (tiene 4 posibles) para ver cómo afecta en diferentes canales. Como podemos ver puede interferir en cualquiera de los canales wireless, dependiendo de su posición.

En caso de encontrarnos con uno de ellos en algún punto será fácil de detectar con la sonda. La solución más rápida pasa por configurar los puntos de acceso afectados en otros canales lejos de los que esté usando la emisora. Este mismo efecto se ha detectado con algunas emisoras de audio, como por ejemplo las de las ambulancias.



Interferencias de una emisora de video por radiofrecuencia

Interferencias con equipamiento médico.

Actualmente hay ciertas normas internas que desaconsejan el uso de dispositivos de emisión de radiofrecuencias en zonas como la Unidad de Cuidados Intensivos.

En entrevista con el personal de Electromedicina del hospital, nos indican que a día de hoy sólo existe una implantación de sensores inalámbricos en la zona de Cardiología del HG, en la unidad de cuidados intermedios, 4ª planta.

Su cometido es recoger constantemente los signos vitales de los pacientes ingresados en dicha unidad, que disponen de libertad de movimiento por la zona. Estos pacientes llevan un emisor de radiofrecuencia que envía la señal a través de varias antenas dispuestas en el techo practicable de la zona, llevando las lecturas a través de esta red a un monitor que se encuentra en el control de enfermería de la unidad. En caso de que un paciente sufra algún síntoma extraño, el sistema avisa al personal de atención que localiza al paciente y lo trata.

Analizando la información disponible del implantador de dicha red vemos que su espectro de trabajo es el de los 405 Mhz. Generalmente los equipos de medida usados en medicina trabajan en esa banda de frecuencias, o entre los 9 Khz y los 315 Khz.

También nos hacen conocedores de que existen normativas técnicas asociadas a los equipos médicos que afectan a la compatibilidad electromagnética con otros elementos emisores: EN 301 839-1, EN 302 195-1, UNE-EN 55011 y UNE-EN 60601-1-2.

Repasando documentación sobre estas normativas, que podemos encontrar en el anexo B de ETGF-ES, sólo encontramos una simple nota que pueda afectar al rango de frecuencias de la red wireless y es de investigaciones sobre la "Aceleración de los análisis químicos usando señales de 2450Mhz" (2,4 Ghz). El resto de documentación hace referencias a los espectros mencionados anteriormente, pero no a 2,4Ghz.

Datos a tener en cuenta para la implementación.

Aspectos tecnológicos.

Entre los aspectos tecnológicos, el primer punto será centrar el ámbito de estudio.

Hoy en día, las tecnologías de comunicación de dispositivos electrónicos a través de radiofrecuencia están adquiriendo cada vez mayor presencia. Hoy en día ya se dispone masivamente de este tipo de tecnologías en dispositivos digitales de mano, (calculadoras, ordenadores de bolsillo, teléfonos móviles, auriculares), pero se prevé que en unos pocos años esto llegue a otros elementos como electrodomésticos de uso cotidiano (lavadoras, televisiones, vídeos, aparatos domóticos), como una forma de sustitución de cables de comunicación.

En estos momentos se están imponiendo dos tipos de tecnologías para este propósito. La primera de ellas, 802.11, está dedicada a la comunicación de datos a alta velocidad entre dispositivos “inteligentes” (ordenadores de sobremesa, ordenadores portátiles) que están esparcidos en un área considerable (por ejemplo, cada uno de los diferentes edificios que componen este complejo). La segunda, Bluetooth, está dedicada a la sustitución de cables entre dispositivos “de mano” (teléfonos móviles, PDAs, auriculares, e incluso ordenadores portátiles). Hasta el momento, parece que Bluetooth es más apropiada para dispositivos pequeños, que funcionan dentro de un radio de unos pocos metros (red de área personal [PAN](#)), debido a las restricciones de potencia que les imponen sus baterías.

Existen también otros estándares inalámbricos (algunos de ellos en fase de aprobación) como por ejemplo WiMAX¹ o WiBRO. Este tipo de tecnologías van encaminadas a interconectar redes a varios kilómetros de distancia.

Dado el ámbito de aplicación del presente proyecto, no consideraremos ni la tecnología Bluetooth, por tratarse de una comunicación de menor distancia y orientada a otros propósitos, ni la tecnología WiMAX, dado que los centros que debemos interconectar se encuentran distanciados tan sólo varios cientos de metros en el peor de los casos. Nos centraremos en las tecnologías alrededor del estándar 802.11.

Actualmente existen 3 normativas diferentes del IEEE respecto a 802.11:

- 802.11a, que trabaja en la banda de 5Ghz y hasta 54 Mbits.
- 802.11b, que trabaja en la banda de 2.4 Ghz, pero sólo hasta los 11 Mbits.
- 802.11g, compatible con la 802.11b, también usa la banda de 2.4 Ghz pero hasta los 54Mbits.

Asimismo, hoy en día existen también varias propuestas para romper la barrera de los 54Mbits como son: 802.11n, WWiSE, MITMOT, etc. De momento de algunas de ellas sólo hay prototipos. Por otra parte tecnologías propietarias de fabricantes como Mesh de Nortel² aún no creemos que cuenten con el respaldo suficiente.

Dado que actualmente la mayoría de los equipos cliente que vienen dotados de red inalámbrica traen conexiones 802.11b y/o 802.11g y además el estándar 802.11g es capaz de soportar clientes 802.11b en sus redes, el proyecto se ha centrado en estudios sobre 802.11g, aunque la mayoría de las técnicas comentadas son de aplicación a cualquiera de las demás implementaciones con pequeñas modificaciones.

1 IEEE 802.16/WiMAX (<http://www.comsoc.org/vancouver/WiMAX-Intro.pdf>)

2 Wireless Mesh Network Solution (http://www2.nortel.com/go/solution_content.jsp?segId=0&catId=0&parId=0&prod_id=47160&locale=en-US)

Centrándonos en la tecnología 802.11g, procederemos a comentar diferentes cuestiones, haciendo una aproximación según las diferentes capas del modelo OSI.

- Nivel físico.

Aunque este aspecto está tratado en otros apartados del presente proyecto tanto desde el punto de vista de alcance como de interacción con otros elementos del entorno, incluiremos aquí algunas reseñas.

Tecnológicamente hablando, los elementos de mayor impacto en este nivel son las antenas de emisión de los puntos de acceso y los clientes. Cada antena polariza la señal según su construcción en un determinado eje y, por lo tanto, su efecto será mayor cuando la antena receptora se encuentra alineada correctamente con la antena emisora (más adelante veremos una muestra en el apartado de estudio físico).

Por ello será importante elegir la antena a utilizar no sólo en función de su ganancia y espectro de difusión, sino también de su ángulo de polarización respecto a los equipos cliente.

Existen antenas en el mercado específicamente diseñadas para interconectar edificios, con un espectro de difusión muy lineal. Esto nos permitiría conectar edificios mediante bridges inalámbricos utilizando esta conexión como línea de backup para la conexión principal. Si bien el caudal que se podría conseguir es mucho menor que el de una fibra, se podrían dar servicios críticos de conexión con dicha configuración.

- Nivel de acceso al medio.

Hay mucha bibliografía sobre la vulnerabilidad de los actuales protocolos de control de acceso al medio que existen en el entorno wireless. Técnicas como el filtrado por MAC o la encriptación WEP pueden no resistir adecuadamente ataques intensos o pueden terminar dejando el punto de acceso sin servicio debido a denegaciones de servicio. Sin embargo, ello no debe disuadirnos de implantar todas las políticas posibles, pues con ello al menos evitaremos la mayoría de los intentos de acceso no autorizado que muchas veces simplemente buscan poder navegar de forma gratuita por Internet.

Si el parque de clientes es acotado y fácilmente inventariable conviene adoptar una política de filtrado de MAC, si es posible basada en RADIUS.

Respecto a la encriptación de la información, es conveniente adoptar como mínimo, siempre que los equipos cliente a utilizar lo permitan, WPA con una contraseña suficientemente robusta. WEP no es conveniente dado que es un cifrado de clave simétrica bastante ligero y sobre el que hay multitud de herramientas que consiguen capturar la clave inicial en el momento de establecer la conexión, capturando tramas de los equipos cliente o inyectando tráfico malintencionado hacia el punto de acceso. Existen mejoras de diferentes fabricantes, pero adoptar una de ellas haría que nuestros equipos cliente necesitaran también equipamiento de dicho fabricante.

Otro de los puntos desfavorables para WEP es que nos obliga a disponer de una única clave para todos los clientes asociada al equipo, no al usuario. Por ello un cambio de la clave WEP (lo cual es una técnica bastante usual de protección de contraseñas) conllevaría reconfigurar todos los equipos clientes.

Con WPA existe la opción de usar una clave compartida para todos los clientes o trabajar con certificados (EAP-TLS), de la cual hablaremos en el siguiente apartado.

Respecto a la red de acceso para los pacientes, podríamos no plantearnos aplicar ninguna de estas medidas de seguridad, sin embargo hacerlo nos ayudaría a mantener un mejor control sobre lo que ocurre en nuestra red y quienes están accediendo a ella.

Una vez conectado el cliente a la red, después de haber superado correctamente tanto el filtrado de MAC como la encriptación WPA, es aconsejable que este usuario se encuentre conectado a una red virtual VLAN diferente la de los demás equipos de la LAN (Zona Gris). Si el despliegue de la red inalámbrica se realiza con el objetivo de poder acceder a la historia clínica digital, que es una aplicación web, el cliente no necesita llegar a acceder a los servidores de BBDD corporativos ni a otros clientes de la red. Esto se consigue conectando los puntos de acceso a conexiones en el switch asociadas a dicha VLAN. En la estructura actual de conexiones podemos plantearnos que esta red virtual pueda ser la red restringida (Zona Amarilla) o crear una nueva conexión en el cortafuegos para diferenciar las reglas que apliquemos a los usuarios de la red inalámbrica. El objetivo de esta topología es minimizar los riesgos de accesos indebidos y reducir el ancho de banda consumido por los clientes, por ejemplo, aplicando en el cortafuegos políticas de QoS a dichas conexiones.

Algunas técnicas más depuradas contra accesos no permitidos aconsejan limitar el número de MACs permitidas por puerta en los switches a los que se encuentren conectados los AP's. También incluir entradas ARP estáticas en los cortafuegos para los puntos de acceso. Con estas técnicas se evitan ataques del tipo "[Man-in-the-Middle](#)" o de [DoS](#).

- Capas de red y transporte.

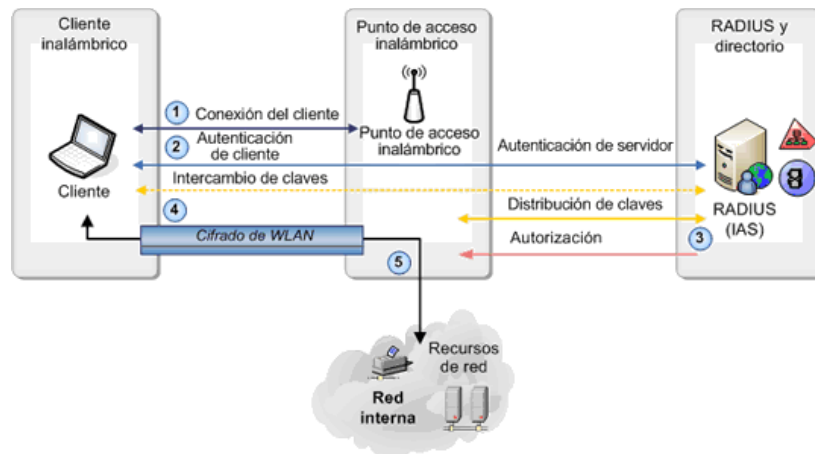
En este apartado, enlazado con el nivel de enlace, las técnicas más útiles son dos:

- Utilización de un servidor de RADIUS, una entidad certificadora y un servicio de directorio junto con EAP-TLS.

Esta combinación de técnicas nos da un alto nivel de seguridad incluso en el caso de que alguien consiguiera pasar alguno de los filtros de niveles inferiores. Su robustez se basa en que a través de los certificados generados por la entidad tanto para el cliente como para el punto de acceso la clave que se utiliza en cada sesión es diferente y generada dinámicamente.

Una vez establecida la conexión entre el cliente y el punto de acceso, éste valida el "Common Name" del certificado del usuario contra el servidor RADIUS. Finalmente el servidor de RADIUS se encuentra conectado con el servicio de directorio pudiendo autenticar que el usuario pertenece a la corporación y autorizando o no el paso del cliente a la red.

Toda la comunicación se encuentra protegida por TLS mediante los certificados de cliente y servidor.



Funcionamiento de EAP-TLS. Fuente [SLPEAP]

Esta solución es razonablemente fácil de implementar, nos proporciona un alto nivel de seguridad, permite autenticar tanto al equipo como al usuario, soporta contraseñas de un solo uso y es escalable.

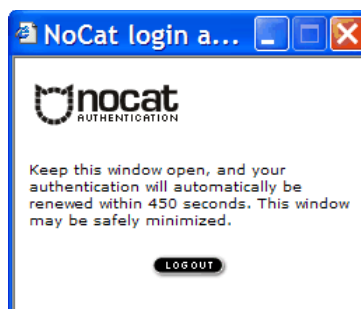
La única desventaja respecto a nuestra instalación es que para equipos cliente Microsoft sólo Windows XP lo soporta de forma nativa, los clientes W2000 necesitan un parche y equipos anteriores no lo soportan.

- Otra solución adoptada por grandes redes de acceso wireless libre es la denominada “NoCat¹” o de portal cautivo [NPSRWI-FI], también implementada por Red-IRIS.

Para implementarla se necesitan puntos de acceso en modo bridge y un router/firewall Linux.

La técnica consiste en que un cliente recién conectado recibe una dirección DHCP que suministra el router Linux. Este mismo router hace que cualquier acceso del usuario a Internet es cortado y se le redirige a un portal donde debe validarse mediante un usuario y una contraseña. Cuando el usuario se valida se genera un token que se le envía al router para que este reconfigure sus reglas de cortafuegos y le permite navegar libremente mientras tenga validez dicho token.

En el equipo cliente queda una ventana parecida a la que se acompaña renovando periódicamente el token.



1 “NoCat's goal is to bring you Infinite Bandwidth Everywhere for Free” (<http://nocat.net/>)

Si el periodo del validez de un token pasa y no ha llegado una actualización, el cortafuegos desactiva las reglas para dicha conexión que pasa a quedar desactivada hasta que se realice una nueva autenticación.

Una de las ventajas de este sistema es que no necesita que el usuario pertenezca a la organización o disponga de un certificado digital, sino que se puede permitir un acceso limitado a internet a usuarios no autenticados, y un acceso mayor a usuarios autenticados.

También nos permite un establecer políticas de aprovisionamiento automático de usuarios en el propio portal, como por ejemplo:

- Un usuario nuevo pueda registrarse directamente en el mismo momento de la conexión, obteniendo su usuario y contraseña. Esto hace que a la vez dispongamos de un control sobre quién se ha registrado y nos aseguremos de que cada usuario haya aceptado un acuerdo de servicio.
- Un usuario nuevo registra una petición para acceder a la red. Esta petición queda registrada en el portal de aprovisionamiento, a la espera de que alguno de los profesionales responsables de la zona de hospitalización valide la petición. Al hacerlo, éste aprueba la solicitud para que el usuario pueda usar el servicio. Esta política nos da mayor control sobre intentos fraudulentos de uso de la red inalámbrica por parte de personas ajenas al sistema.

Políticas válidas y políticas no recomendables.

En este apartado iremos haciendo una relación de buenas prácticas, y otras no tan buenas, que se deben tener en cuenta de cara a configurar una red inalámbrica fiable. Muchas de estas reglas están basadas en la lógica, sin embargo no por ello muchas veces se obvian, por no dedicarle el tiempo suficiente a la reflexión previamente de la ejecución.

Comenzaremos con los aspectos de seguridad de los elementos:

- Seguridad física.
Tanto los clientes como los puntos de acceso contienen información valiosa sobre la configuración de nuestra red (aparte de toda la información del usuario que suelen tener los equipos). Alguien que consiga acceder a alguno de ellos podría averiguar lo suficiente como para comportarse como uno más de nuestros usuarios o suplantar a alguno.

Los equipos clientes deben estar configurados de tal forma que se necesite algún tipo de autenticación para acceder a ellos.

Los puntos de acceso deberían colocarse en zonas lejos del alcance del público en general (un Hospital suele estar lleno de gente que entra y sale), e incluso fuera del alcance de los propios usuarios. Aquí encontramos razones de seguridad de acceso y de seguridad personal. Los puntos de acceso están pensados para colocarse a cierta distancia de las personas y así cumplir con los márgenes de seguridad a los que la ley obliga respecto a la densidad de potencia máxima permitida, así como la distancia de referencia según el “Reglamento de medidas de protección sanitaria frente a emisiones radioeléctricas” [RD 1066/2001] (10 W/m² para 2,4 Ghz). También evitar que un usuario pueda manipular el punto de acceso nos garantiza la continuidad en el servicio del mismo.

- Limitar el alcance de la red a las áreas deseadas.
El principio de “seguridad por la oscuridad” en este caso sí nos sirve. Debemos escoger las antenas adecuadas según su patrón de emisión y ganancia, la orientación de los puntos de acceso adecuadas, y los niveles de señal necesarios para llegar hasta donde deseamos dar cobertura pero no más allá de lo necesario. Así evitaremos confusión entre los usuarios respecto a las zonas donde pueden y donde no pueden trabajar, así como dejar zonas en las que alguien pueda intentar ganar acceso a la red sin permiso.
- WLAN en un dominio de broadcast diferente a la LAN.
Los usuarios con acceso a la red inalámbrica son menos controlables que los usuarios conectados a la LAN, pues estos últimos deben conseguir acceso físico a un punto de la red mientras que los primeros pueden estar en cualquier lugar con cobertura. Por ello es una buena política colocar las redes wireless en una VLAN diferente al resto y que un sistema cortafuegos diferencie el tráfico seguro del que no lo es. Esta política también facilita la implantación de determinadas políticas de autorización de acceso y encriptación de la información.
- Implementación de sistemas de autenticación robustos.
No basta con limitar el acceso físico a las zonas de cobertura, también es necesario aplicar políticas adecuadas que, por ejemplo, nos ayude a diferenciar los usuarios de la red de pacientes que necesitan sólo acceso a Internet, de los médicos intentando consultar una historia clínica.

Políticas como el filtrado de MAC o la ocultación del SSID no terminan siendo válidas por sí solas, pues son fácilmente evasibles.

- La información visible de los puntos de acceso (SSID) no debería contener información sobre la organización ni sobre su ubicación.
- Las contraseñas elegidas deben ser suficientemente robustas.
La mayoría de los algoritmos de encriptación actuales basan su robustez en la imposibilidad de conseguir averiguar la contraseña encriptada en un tiempo computable. La mayoría de las técnicas de ataque se basan en conseguir romper alguna contraseña en base a algoritmos de prueba y error utilizando diccionarios de palabras. Las garantías de éxito de éstas se basan en encontrar una contraseña que no cumpla ciertos mínimos de robustez (mezclar números y letras, incluir algún carácter extraño, no utilizar palabras conocidas o relacionadas con el entorno, etc.)
- Autenticación de dispositivo y de usuario.
Algunas de los sistemas de acceso de las redes wireless están pensados para autenticar al equipo cliente, pero no al usuario. Es conveniente poder autenticar ambos para poder asegurar que el usuario que solicita autorización está usando un equipo adecuado, y no encontrarse con casos en los que un login de usuario perdido intenta acceder desde un equipo no autorizado o un equipo robado o extraviado con un usuario no autorizado.
- Políticas interna de cobertura para los usuarios internos y los externos.
Los usuarios de nuestra red ya firman un documento de conformidad respecto a sus obligaciones dentro del marco legal de la LOPD. A dicho documento deberíamos añadir las cláusulas necesarias que impliquen el uso de accesos inalámbricos (por ejemplo custodia de la contraseña de acceso WEP).

Si nos planteamos dar cobertura de red inalámbrica a los pacientes convendría publicar la información sobre las condiciones de dicho servicio antes de que el usuario pueda comenzar a utilizarlo (por ejemplo: el PC debería disponer de un antivirus, el hospital no se hace responsable de las páginas que se visiten, que dicha navegación puede ser registrada por motivos legales, que no deben realizarse tareas ilícitas usando esta conexión, que no hay garantías de calidad de la conexión, etc.)

- Formación al usuario y transparencia.
Preparar una documentación clara y sencilla para proporcionar a los usuarios tanto internos (profesionales del hospital) como externos (pacientes), ayudará a mejorar la eficacia de la red y a obtener un uso más óptimo de la misma.

Si la implantación se va a llevar a cabo finalmente en condiciones donde los usuarios no la utilicen habitualmente (salas de formación o de reuniones, por ejemplo) quizás fuera interesante organizar algunos seminarios para los usuarios más interesados en los que se expliquen la utilidad y forma de uso de estos elementos.

- Monitorización y auditorías periódicas.
Por último sería interesante, si la implantación de redes wireless llega a hacerse a gran escala, disponer de sistemas de detección de intrusos (IDS) y de monitorización del rendimiento de los equipos. También convendría planificar auditorías internas periódicas que revisen el correcto estado y funcionamiento de la instalación.

También puede ser una buena política para asegurar la calidad de la instalación contratar auditorías externas que intenten romper las políticas de seguridad, igual que lo haría un atacante externo, y luego genere un informe de cómo ha sido posible. Con esto también podemos comprobar la fiabilidad de los sistemas IDS.

Estudio físico.


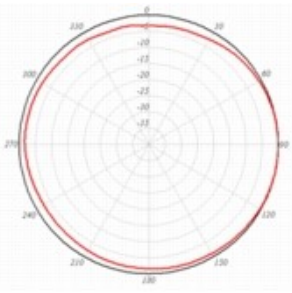
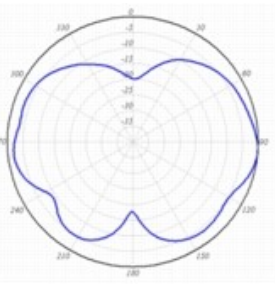
Medidas de alcance y rendimiento.

Equipamiento.

El equipo que finalmente hemos utilizado para las medidas de alcance ha sido:

- Cisco Aironet 1100 Series con antena integrada
- Equipo portátil dotado de una tarjeta inalámbrica Intel PRO Wireless 2200BG y con el software Windows XP
- Programa "Network Stumbler"
- Un servidor ftp.
- Un cliente ftp que mide la tasa de transferencia de datos.

Las características técnicas del punto de acceso recogidas por el fabricante¹ son:

	Azimuth Plane Radiation Pattern		Elevation Plane Radiation Pattern	
	Rango de frecuencia	2.4 a 2.5 Ghz		
	Ganancia	2 dBi		
	Polarización	Lineal		
	Azimuth 3dB BW	Omni		
	Elevations 3dB BW	50 grados		
	Antenna Connector	Integrado		
	Montaje	Integrado		
	Tipo de Antena	Omnidireccional		

En estas gráficas vemos que este punto de acceso está concebido para trabajar en el ámbito horizontal en los 360 grados (omnidireccional) y que verticalmente su ámbito de trabajo resta 50 grados respecto a la vertical.

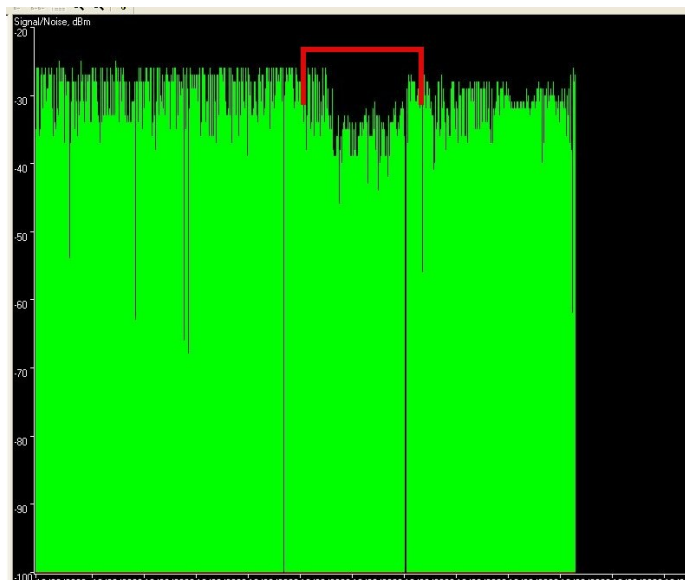
El Azimuth no es más que el corte XY, es decir, indica como radia la antena si la viéramos desde arriba. La elevación es el corte ZX, es decir, indica como radia la antena vista desde un lateral tomando en ambos como origen de coordenadas la antena.²

1 http://www.cisco.com/en/US/products/hw/wireless/ps469/products_data_sheet09186a008008883b.html

2 <http://usuarios.lycos.es/natasab/dev/online.php?code=0&id=6>

Hemos realizado unas pruebas empíricas de dichas medidas según la posición y hemos obtenido el gráfico siguiente, donde se remarca una pérdida de entre 5 y 10 dBms colocándolo horizontalmente.

Por ello, en el momento de tomar las mediciones, y consecuentemente en el montaje definitivo de los elementos, debemos asegurar la verticalidad del elemento para no disminuir su eficiencia y provocar falsas medidas y que su altura respecto a los clientes sea la indicada para que dicho ángulo de 50 grados no se llegue a tener con ningún cliente.



Perdida de señal por orientación incorrecta del AP

La tarjeta de red tiene las siguientes características de alcance¹: “Alcance normal en interiores de 30 m a 54 Mbps y 91 m a 1 M bps para 802.11g y de 30 m a 11 Mbps y 90 m a 1 Mbps para 802.11b”

Para las mediciones, hemos utilizado la configuración del punto de acceso en configuración de fábrica, sin ningún tipo de encriptación ni procedimientos de validación.

Con esta configuración intentamos recoger las medidas máximas de alcance y rendimiento posibles, no perdiendo parte del ancho de banda disponibles en la encriptación. A partir de estas medidas base podremos en tomar decisiones respecto a la distancia máxima que debe existir entre puntos de acceso y clientes, tal y como se verá en los siguientes apartados.

Datos de estructura de los edificios.

Como referencia para la reunión con el responsable de mantenimiento del complejo consultamos la tabla de “Perdida de señal por tipo de Obstáculo” que aparece en el Apéndice E, pág. 503 de [WI-FOO].

¹ <http://www.intel.com/cd/products/services/emea/spa/234997.htm>

Elemento	Perdida (dB)	Rango Efectivo
Espacio abierto	0	100%
Ventanas (cristales no tintados)	3	70%
Ventanas con cristales tintados	5-8	50%
Muro ligero (Pladur, muros secos, etc.)	5-8	50%
Muro medio (mamparas, aglomerado, etc.)	10	30%
Muro sólido (Ladrillo o similar, aprox. 15 cms.)	15-20	15%
Muro de carga (aprox. 30 cms.)	20-25	10%
Techo/Suelo	15-20	15%
Techo/Suelo muy denso	20-25	10%

Tabla de Pérdidas de señal por tipo de Obstáculo

Reunión de toma de datos.

Con estas referencias establecemos una reunión con D. Diego Sánchez, responsable del área de Mantenimiento del área hospitalaria y conocedor de la estructura de los edificios.

Después de exponerle los motivos de la reunión y los puntos donde estábamos más interesados en recabar información, procedemos a repasar los edificios principales del entorno y a analizar sus características. Su disposición física y el número de plantas lo podemos encontrar en el apartado "[Descripción de los edificios](#)" correspondiente al punto "Estudio de los planos de los edificios".

La estructura principal de los edificios es de dos tipos: estructura de hormigón, o bien una estructura mixta de zonas de hormigón con armazón metálico.

Generalmente los edificios más antiguos (HG, HRT y CDT) están dotados con estructura de Hormigón que suele ser más pesada y compleja y, por lo tanto, más difícil de penetrar por las ondas electromagnéticas.

Los edificios más modernos o las ampliaciones (por ejemplo, la zona de quirófanos, urgencias y radiología del HG), ya están fabricados utilizando una estructura más ligera con armazón metálico.

Sin embargo, teniendo en cuenta que la mayoría de los edificios tiene una superficie de planta bastante grande, esto hace pensar que el espesor de los techos/suelos necesarios para sostener la infraestructura sea un gran obstáculo para la transmisión por radiofrecuencia.

Respecto a su estructura interna, volvemos a diferenciar entre estructuras más antiguas y las nuevas construcciones.

Las construcciones antiguas están hechas de tabiques de ladrillo con grosores entre los 10 y los 30 centímetros aprox. En muchos de los pasillos y estancias se puede también encontrar una cobertura de azulejos de material cerámico. Las ventanas suelen ser de materiales férreos y los cristales sin ninguna característica especial reseñable.

Las construcciones más modernas (ampliaciones o reformas) ya se hacen con materiales mucho más ligeros. Muros secos o pladur, tabiques de ladrillo en algunos casos, pero más ligeros. Los recubrimientos de azulejos tienden a sustituirse por materiales basados en compuestos de madera con lacados plásticos, generalmente resistentes en algunos casos a productos químicos abrasivos. Respecto a los cerramientos, ahora se suelen realizar con ventanales de aluminio con doble acristalamiento.

Con respecto a los techos, de cara a poder ubicar los puntos de acceso en ellos, para reducir la accesibilidad por parte de personal no autorizado, en la mayoría de los casos existentes encontramos techos de escayola practicables con una “zona de luz” de entre 20 y 80 centímetros de altura. En ellos existen multitud de canalizaciones de todo tipo (diversas canalizaciones de agua, gases, electricidad, cableado estructurado informático).

En resumen estos son los datos para los edificios más representativos:

- HG, Mixto.
 - Hospitalización: Estructuras de hormigón. Muros y techos robustos. Recubrimientos de azulejos.
 - Radioterapia y quirófanos: Hierros y con hormigón. Muros y techos robustos. Recubrimientos de azulejos.
- HRT
 - En general: Estructura de hormigón. Muros y techos robustos.
 - Zonas reacondicionadas (algunas alas de hospitalización y las urgencias) Estructura de hormigón. Muros menos robustos o de Pladur o mamparas de aglomerado. Recubrimientos plásticos.
- HM
 - Hormigón con armazón metálico. Muros de ladrillo.
- HI
 - Hormigón con armazón metálico. Muros de ladrillo.
- CDT
 - Estructuras de hormigón. Muros y techos robustos. Recubrimientos de azulejos.
- EGR
 - Una sola nave. Techos de escayola practicables el primero con cobertura de uralita a unos 6 a 9 metros de altura. Muros de ladrillo en algunos casos y mamparas de Pladur o aglomerado.
- EG
 - Zona de Gestión. Metálica. Muros de ladrillo ligeros. Sólo dos plantas con lo que el techo es más ligero.
 - Ampliación. Salón de actos y Escuela de Enfermería. Hormigón. Pocos muros.

Decisiones de puntos de medida tras la reunión.

Tras analizar la información recabada, tomamos la decisión de analizar in-situ sólo dos de los edificios, ya que prácticamente las características de todos los demás se encontrarían englobadas en éstos y las decisiones de implantación que adoptemos podríamos basarlas en estas medidas sin demasiado margen de error.

Las medidas serán realizadas en:

- Edificio de Gestión de Recursos. Como modelo de las construcciones más modernas, por ser el que cuenta con una estructura más ligera y con mayores zonas abiertas.
- Hospital General, zona antigua. Es el edificio más antiguo (50 años aproximadamente) y con las medidas más desfavorables para la transmisión de la señal: Techos/suelos muy robustos. Muros grandes, compleja estructura, muchas zonas de “sombra” como los huecos de los ascensores (cuenta al menos con 5 zonas de ascensores diferentes).

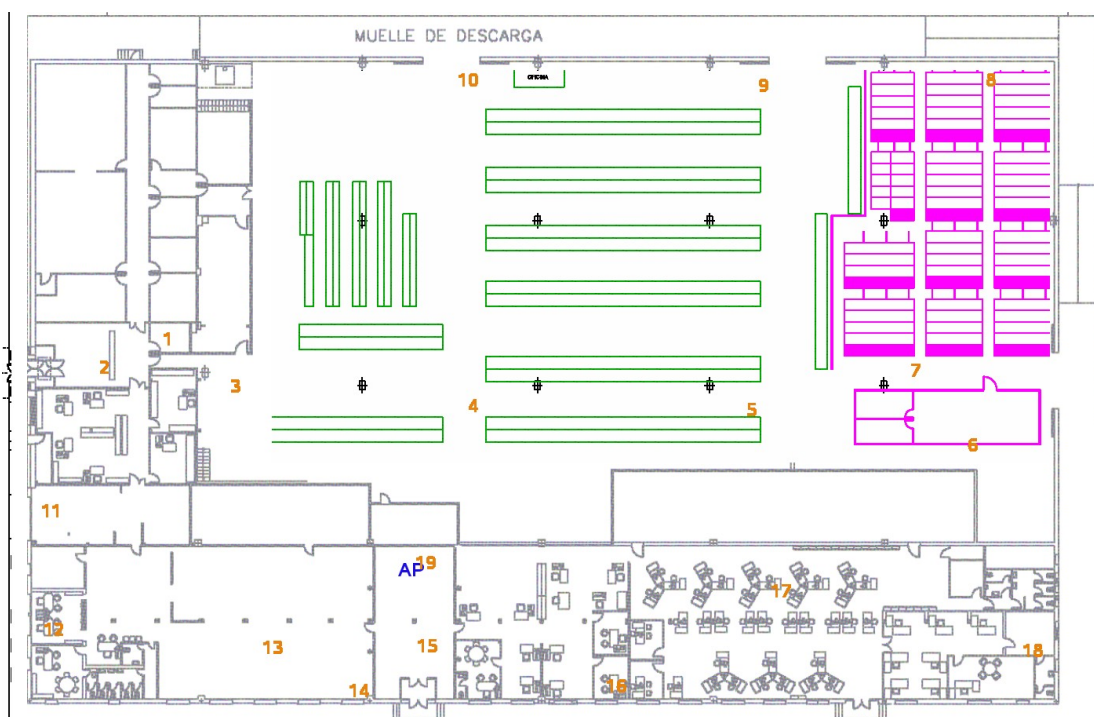
Medidas en el EGR.

Equipados con el punto de acceso, el medidor de interferencias, y el PC portátil se accede al recinto en una hora de poco trabajo, para facilitar el acceso a las diferentes zonas de mediciones.

Este edificio consta de las siguientes partes, según vemos en el plano.

- La zona rosa corresponde con un antiguo archivo de historias clínicas que consta de estanterías metálicas de unos 2 metros de altura. No dispone de techo de escayola, su techo es la cubierta de la nave.
- La zona verde corresponde con un almacén con estanterías de estructura metálica y de madera de unos 6 metros de altura. Como en el caso anterior, tampoco dispone de techo de escayola y también su techo es la cubierta.
- La zona gris es una zona de oficinas con pequeñas divisiones que generalmente son de ladrillo o mamparas de aglomerado. El techo es de escayola practicable.

El punto de acceso se colocó en la marca “AP”(en azul), y los puntos de medición son los que aparecen numerados del 1 al 19 (en naranja).



Plano de medidas en el EGR

El procedimiento de medición en cada punto consistió en ejecutar el script de recogida de datos durante 5 segundos al menos, y durante un tiempo superior cuando las medidas fluctuaban demasiado. Después se procedía a descargar un fichero por ftp desde uno de los servidores de la LAN y apuntar la tasa de transferencia. Ambos resultados se registraban en dos ficheros llamados puntox.log y puntox.ftp.log.

Los puntos se encuentran distribuidos en varios conjuntos:

- Puntos en espacios abiertos o con pocos obstáculos: 3, 4, 5, 6, 7, 8, 9 y 10.
El único obstáculo entre ellos y el AP es un muro de ladrillo y alguna estantería metálica.
- Puntos en despachos: 1, 2, 16 y 18.
Atravesan varias paredes, generalmente de pladur o ladrillo.
- Puntos en zonas amplias: 11, 12, 13, 14, 15 y 17.
Atravesan alguna pared o mampara, pero de poco espesor.
- El 19 es el punto de referencia medido a escasa distancia.

Colocación del AP y Medidas de interferencias.

La posición donde se colocó el punto de acceso fue la misma en la que se encontraban los armarios de comunicaciones utilizados para la red local.

El lugar está situado en un archivo de documentación de unos 7x3,5 metros que, curiosamente, no viene reflejado en el plano. Está delimitado por tres paredes de pladur y un muro de ladrillo. El muro y las dos paredes laterales si aparecen reflejadas en el plano.

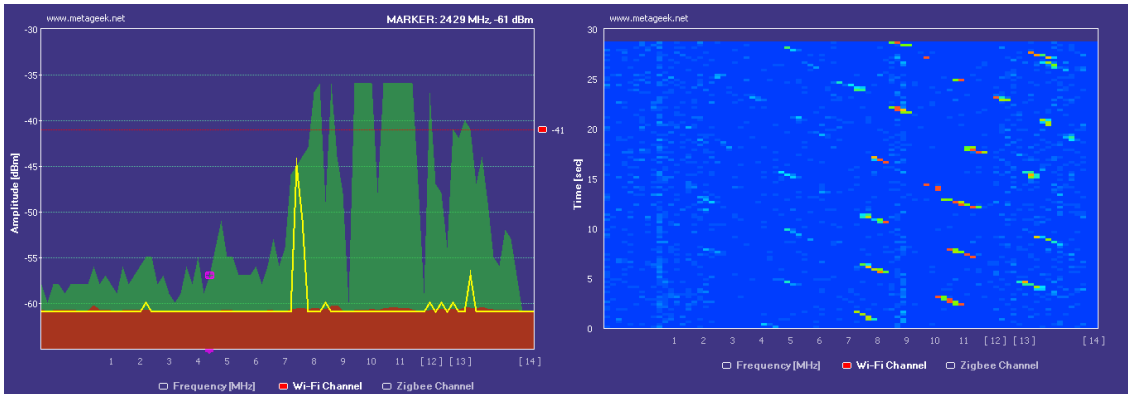
El AP se colocó en un archivo de papel donde se encuentran los armarios de comunicaciones de la LAN. Se colocó a unos 2 metros de altura orientado según el eje longitudinal del edificio. En la zona no se observaban elementos generadores de interferencias como microondas (bastante frecuente en salas de descanso), o teléfonos inalámbricos.



Imágenes de la colocación del punto de acceso en EGR

Antes de la puesta en marcha del punto de acceso se tomó una muestra de un minuto del ruido electromagnético existente en la zona donde se iba a colocar. Como vemos es mínimo y probablemente provocado por algún portátil que estuviera buscando conexiones.

Esto nos indica que en este edificio se podría implantar una red inalámbrica sin tener en cuenta los canales a usar para evitar interferencias.



Medidas de Interferencia en EGR

Medidas y primeras conclusiones

Usando una hoja de cálculo se realizaron la media aritmética de los valores recogidos para poder comparar las medidas obtenidas en los diferentes puntos independientemente del número de muestras recogidas.

Punto	Ftp Tx	Valores Promedio				Distancia al AP (m)
		Bit Rate Mb/s	Link Quality	Signal level dBm	Noise level dBm	
P1	53,69	1,42	37,67	-77,75	-86,75	29
P2	4,3	54	35,07	-81,64	-87,21	33
P3	1020	54	56,4	-66,4	-86,8	23
P4	956,79	54	67	-59,2	-86,4	18
P5	708,03	11	58	-64,6	-86,4	31
P6	764,82	5,5	54,4	-68,4	-87	52
P7	440,66	11	42,8	-74	-85,8	47
P8	82	1	36,6	-77,8	-86,6	67
P9	66,54	1,4	40,2	-76,2	-86,6	54
P10	507,12	11	55,2	-68,6	-87	43
P11	113,31	1	44,4	-74,2	-86,8	34
P12	1250	24	69,6	-59	-86,6	35
P13	1080	36	70,4	-57,2	-86,4	15
P14	1350	50,4	77,8	-50,2	-87,6	13
P15	1320	54	88,6	-41	-87,2	7
P16	1060	36	69,2	-57,6	-87,2	22
P17	1080	36	48,2	-65	-86	33
P18	31,43	1	33	-80,2	-86,8	60
P19	1640	54	60	-28,4	-86,8	1,5

Tabla de valores obtenidos

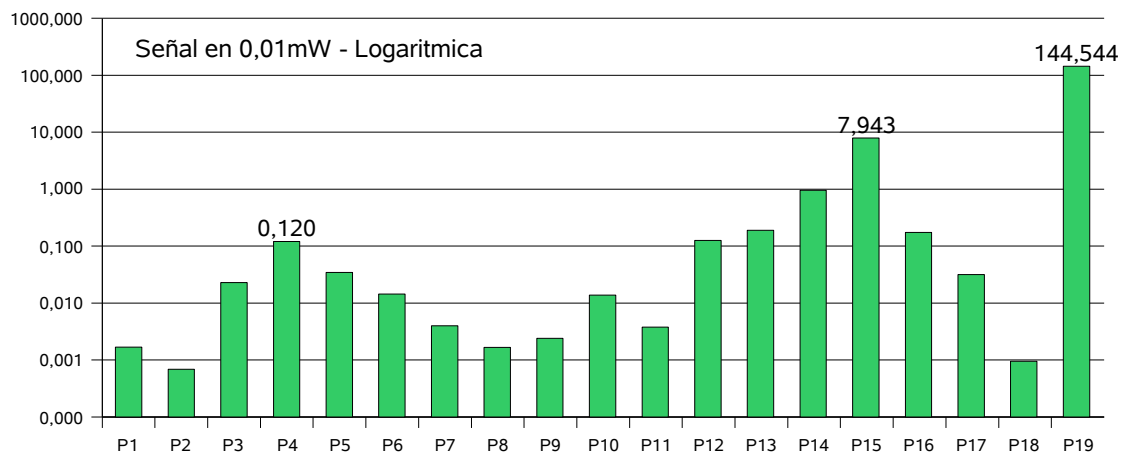
Podemos observar en la tabla de medidas y en los gráficos siguientes algunos aspectos a destacar:

- Dadas las características estructurales del edificio, el punto de acceso era visible desde todos los lugares de medición, aunque sólo en espacios abiertos se conseguía llegar a tasas de trabajo razonables en distancias de unos 50 metros máximo.
- La distancia media de trabajo parece rondar en torno a los 30 metros. A mayores distancias vemos que el ancho de banda obtenido en las zonas con más obstáculos se reduce en extremo, siendo poco recomendable para aplicaciones con un consumo medio de recursos de red (navegación por internet, trabajo con acceso a BBDD, trabajo con ficheros de ofimática centralizados). Sí es una opción planteable para clientes ligeros o aplicaciones para PDAs (por ejemplo, un control de stocks).
- Curiosamente obtenemos mejores niveles de calidad de señal a distancias del orden de los 10 metros que en el punto más cercano. Esto probablemente sea debido a la saturación de los componentes, al recibir demasiada potencia.

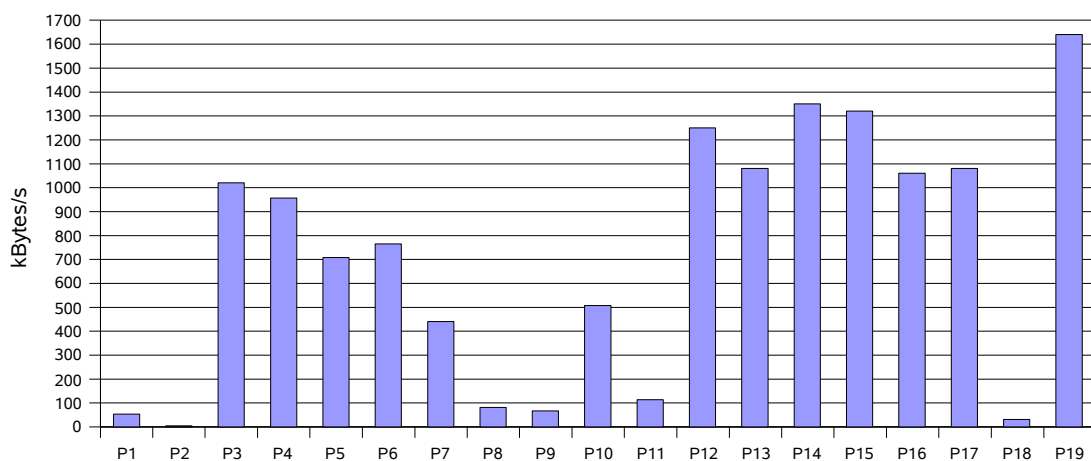
Gráficos comparativos.

En los gráficos siguientes mostramos el nivel de señal medido en una escala logarítmica según la fórmula: $nivel = 10^{\frac{valor\ dBm}{10}} * 10.000$

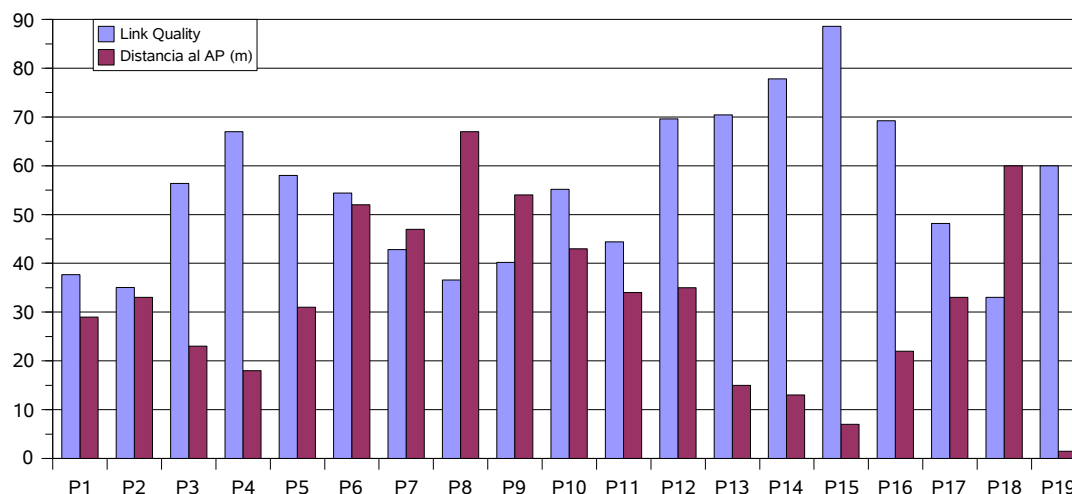
También mostramos un gráfico con la tasa de transferencia obtenida para poder compararlo, y otro que incluye una relación entre la calidad de la señal y la distancia.



Nivel de señal medido



Tasa de transferencia de un fichero mediante FTP



Calidad de la señal frente a distancia

Ejemplo de despliegue previsto en el edificio.

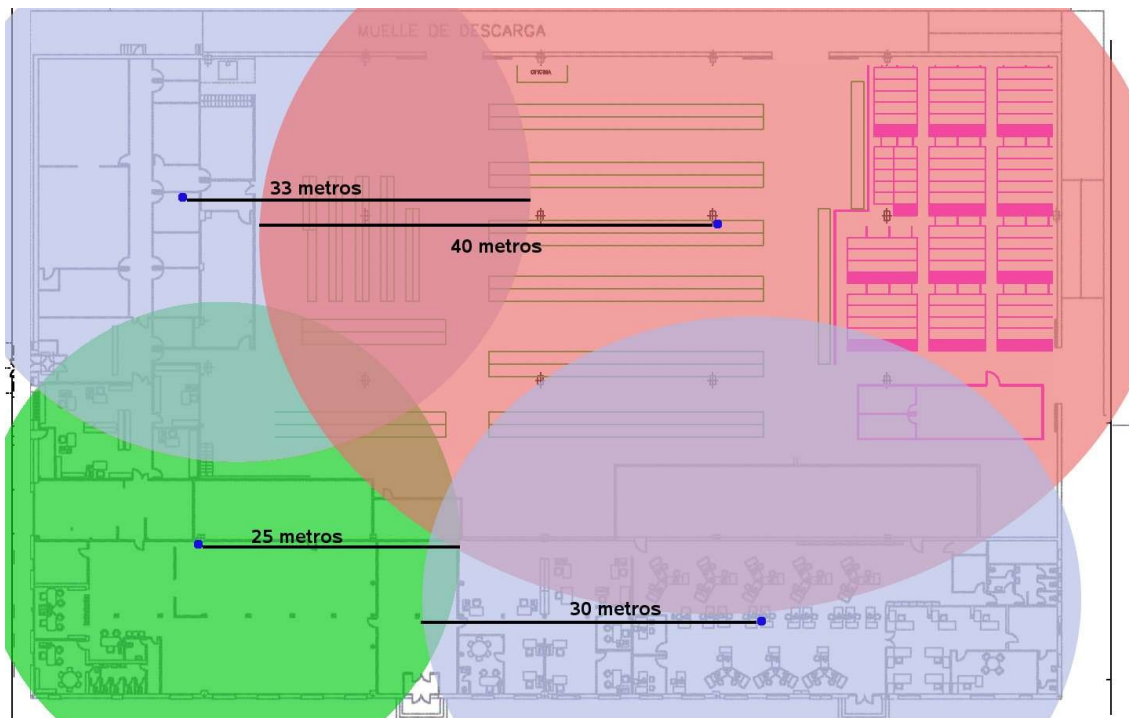
A tenor de las medidas realizadas, un ejemplo de despliegue en el centro podría realizarse con 3 o 4 puntos de acceso, dependiendo de si se quiere dar soporte de red inalámbrica al almacén o no.

De los 4 puntos de acceso posibles que se muestran en el gráfico con un punto azul, los canales a elegir serían ser sólo 3: el canal rojo, el verde y el azul.

Dado el reparto de canales de la red 802.11g, sólo existen tres canales completos. El resto presenta determinado niveles de solapamiento. Con esta usando sólo 3 canales podríamos hacer el despliegue de la red con la garantía de que ninguno de los puntos de acceso entraría en conflicto con los demás. En los puntos donde la señal de los APs del canal azul pudieran entrar en conflicto garantizamos que el usuario dispone de otro canal libre sin interferencias cuya señal se recibe con mucha mayor calidad.

Con ello conseguimos una cobertura total con una distancia máxima de 30 metros en los puntos de la zona de oficina, lo que se ha demostrado que consigue entre unos 1000 y 1300 MBytes de velocidad de transferencia sostenida, lo cual sería equiparable a aproximadamente una conexión de 10 Mbits/s de LAN, aunque esto dependerá realmente del número de clientes existentes en la red inalámbrica y del tipo de carga de red que impliquen las aplicaciones que se utilicen.

En la zona de Almacén se ha previsto un único punto de acceso puesto que es una zona libre de obstáculos y donde, llegado el caso de usar dispositivos móviles, el ancho de banda necesario sería pequeño.



Ejemplo de despliegue Wireless

Medidas en el HG.

Al igual que en el caso anterior, visitamos el HG y colocamos el punto de acceso en funcionamiento y conectado a la LAN en una zona de la planta baja donde hay cierto espacio libre de muros. El punto aparece marcado en el plano como "AP" (azul).

Procedimos con las mediciones en las plantas baja (puntos 1, b2 y b3), primera (1_1, 1_2, 1_3 y 1_4), segunda (2_1) y sótano (s_1 y s_2), con los resultados que se pueden apreciar en la tabla siguiente:

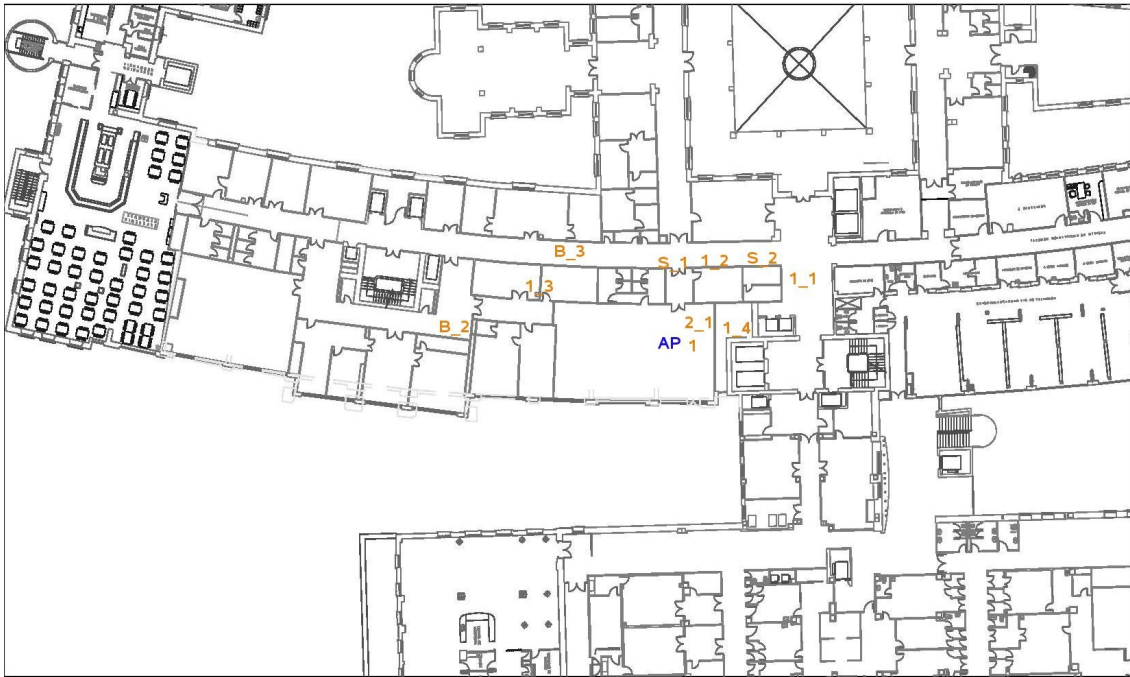
Punto	Ftp Tx	Valores Promedio				Distancia al AP (m)	Distancia Horiz.	Distancia vertical
		Bit Rate Mb/s	Link Quality	Signal level dBm	Noise level dBm			
P1	1680	48	95	-27	-85	1,5	1,5	0
P1_1	0	24	33	-80	-86,2	15,52	15	4
P1_2	494,87	54	55	-68	-85,2	10,77	10	4
P1_3	0	54	51,8	-69,8	-85,2	20,4	20	4
P1_4	858,76	54	61	-63,8	-85	8,94	8	4
P2_1	0	54	38,8	-76,8	-84,8	8,25	2	8
Ps_1	0	54	47	-71,6	-86	8,06	7	4
Ps_2	0	24	43,6	-73,2	-85,4	8,94	8	4
Pb2	0	24	44,4	-73,8	-85,8	23	23	0
Pb3	22,69	24	64,6	-61,4	-85,4	15	15	0

Medidas recogidas en el HG

En este caso, para el cálculo de la altura se han tenido en cuenta la distancia horizontal y la vertical.

Los resultados obtenidos muestran que la distancia máxima de trabajo en horizontal es de unos 15 metros, con una tasa de transferencia extremadamente baja y que en las plantas superiores e inferiores el nivel de propagación de la señal es mínimo, consiguiendo una conexión razonable sólo en algunos puntos de la primera planta estando a menos de 10 metros del punto de acceso.

El plano de los lugares de medida es el siguiente.



Puntos de mediciones en el HG

Conclusiones de las medidas obtenidas

Las características constructivas de este edificio, con muros grandes y paredes revestidas hace que la propagación de la señal de la red inalámbrica sea mínima.

En estas condiciones, la única opción viable para poder proporcionar algunos servicios de red wifi sería utilizarla en salas de conferencias, salones de actos, salas de espera y demás dependencias con gran amplitud. Cualquier otro despliegue necesitará de un número excesivo de puntos de acceso y conllevaría muchos problemas de: planificación de los canales a elegir para el despliegue, cobertura pobre y niveles de servicio pobres o nulos en cuanto el usuario tratara de usar el dispositivo inalámbrico en movimiento a lo largo de la planta.

Redes inalámbricas encontradas (warwalking).

En la inspección de redes inalámbricas existentes usamos varias herramientas para conseguir detectar y aislar las que fuéramos encontrando. Utilizamos un llavero de detección de redes inalámbricas, el portátil configurado con S.O. Windows XP con el programa Network Stumbler y una sonda de Fluke Networks conectada a la red corporativa que rastrea todos los equipos con conexión, su MAC y algunos datos más en el caso de que dispongan de SNMP configurado. Cuando usemos esta última debemos tener en cuenta que existen equipos que responden con una única MAC para la red wifi y la red LAN y otros que disponen de varias direcciones MAC, pero en este último caso al menos los 3 primeros octetos si coinciden, debido a que son los que indican el fabricante del equipo.

El primer paso fue realizar un recorrido por las dependencias del edificio con el llavero detector. Detectamos 9 puntos en diferentes edificios.

Dado que este detector es muy simple (existen otros en el mercado que nos indican en un display qué tipo de conexión es, si dispone de algún protocolo de encriptación y el SSID de la conexión), el siguiente paso fue usar el portátil para recoger más datos de la conexión. Con ello pudimos comprobar que 5 de ellos se trataban de portátiles con su conexión inalámbrica en modo adHoc (falsos positivos). Estos casos nos ayudarán más adelante a completar la redacción de la documentación que vamos a proporcionar a nuestros usuarios.

Después de esta criba nos quedamos sólo con 4 puntos que sí parecían redes inalámbricas en uso: en la 2ª planta del HG por la zona de despachos médicos, en HRT en la zona de consultas, en el Archivo de historias clínicas y en EG alrededor de los despachos.

Uno de ellos (HG) no tenían configurado ningún protocolo básico de seguridad, otro (HRT) usaba seguridad tipo WEP, el tercero (Archivo) disponía de encriptación pero por el SSID pudimos deducir que pertenecía a otra empresa cercana a nuestras instalaciones. El último estaba configurado con WPA.

Con los aparatos que si estaban dentro de nuestro entorno, procedimos a registrar las direcciones MAC de los equipos, su fabricante, su SSID y su canal. Para ello usamos el Network Stumbler y corroboramos el fabricante con una página de búsqueda por MAC¹:

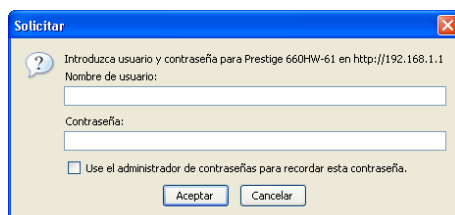
- 00:A0:C5:9C:FB:DD - Zyxel – Wireless – Canal 1 – N/A – 00A0C5 Zyxel Communication.
- 00:11:50:36:5D:9F - ??? - p140988680002 – Canal 6 – WEP - 001150 Belkin Corporation.
- 00:0F:3D:9F:F2:AA - Dlink – SIM – Canal 6 – WPA – 000F3D D-Link Corporation.

00:A0:C5:9C:FB:DD

En este equipo, que no disponía de control de acceso, el primer paso fue tratar de conectarnos directamente a Internet a través de él. Nos ofertó una dirección IP (192.168.1.33) y comprobamos que podíamos navegar sin restricciones.

Por otra parte, usamos la sonda Fluke para rastrear la MAC, y no aparecían ni esta dirección ni ninguna similar. Así pudimos deducir que no estaba conectado a la LAN.

1 Vendor/Ethernet MAC Address Lookup and Search (http://www.coffer.com/mac_find/?string=001150)



Entramos en el interfaz web de configuración del equipos y vimos en el diálogo de conexión que se trataba de un modelo Prestige 660HW-61.

Consultando en la web del fabricante el manual de dicho aparato¹ vemos que la contraseña de acceso era “1234” y accedimos a su configuración, donde comprobamos que efectivamente no se encontraba conectado a ninguna red Ethernet, y que sólo disponía de una conexión [ADSL](#) y la red inalámbrica.

Finalmente, tras varias labores de “ingeniería social”, identificamos al responsable de dicha red inalámbrica que nos confirmó que la usaba para un estudio clínico de investigación en colaboración con un laboratorio farmaceutico. El estudio recoge información de tratamientos de diferentes facultativos a través de Internet. El laboratorio presta el equipamiento necesario, coloca la red inalámbrica, una línea ADSL que permite la conexión y un portátil. Cuando termine el estudio retirarán todo el equipo.

Dado que no se trata de un equipo gestionado por nosotros, dimos por cerrado el asunto, no sin antes informar a los usuarios de los posibles problemas de accesos no deseados a su equipo en caso de no securizar un poco más su conexión. Obtuvimos de ellos la firme promesa de no conectar dicho punto de acceso a la red del hospital.

00:11:50:36:5D:9F

Este equipo no nos permitía conectarnos directamente a él, por lo que debimos realizar las pesquisas en otro sentido.

En primer lugar buscamos su MAC usando la sonda Fluke. Aunque no aparecía, sí aparecía la MAC 00-11-50-36-5d-9e, que es sospechosamente parecida. Rastreando dicha dirección a través de las tablas de direcciones de los switches de la red llegamos a uno de los armarios de HRT, lo que prácticamente confirmaba que se trataba del mismo equipo.

El llavero tiene una función para ir mostrando la calidad de la señal mientras nos desplazamos para saber si nos acercamos o alejamos de la fuente, y con ella intentamos localizar el equipo sobre el terreno, pero no nos fue posible.

Finalmente, consultándolo previamente con la dirección de STI, procedimos a deshabilitar por software la puerta del switch donde se detectó el equipo en espera de que los usuarios de éste informen de un fallo en la conexión.

De momento nadie ha llamado al servicio de soporte reclamando una falta de conexión, y por otra parte tampoco hemos vuelto a ver esa dirección MAC en inspecciones posteriores con la sonda Fluke.

¹ P-660HW Series 802.11g Wireless ADSL 2+ 4-port Gateway
(http://www.zyxel.com/web/product_family_detail.php?PC1indexflag=20040812093058&CategoryGroupNo=AC5783AE-9475-41AD-BDA5-0997187F44AA)

Probablemente se trate de otro caso similar al anterior con la diferencia de que esta vez sí que se ha conectado el equipo a la LAN, aunque luego sólo se use su función wireless.

De momento se ha dado el problema por resuelto hasta que se consiga más información, o alguno de los usuarios solicite soporte a este respecto.

00:0F:3D:9F:F2:AA

Al igual que en el caso anterior no pudimos conectarnos al equipo directamente, así que buscamos su MAC con la sonda Fluke y confirmamos que se encontraba en la primera planta del EG.

Con el llavero conseguimos localizar el punto de acceso, que se encontraba en una de las salas de reuniones aledañas a los despachos de los directivos.

Preguntando a los responsables de la sala conseguimos averiguar que el equipo había sido montado como parte de la dotación audiovisual de la sala en un proyecto “llave en mano” que se realizó hace unos 6 meses. Existen unas instrucciones de cómo conectarse disponibles para quien desee utilizar la conexión, siendo su función básicamente dar acceso al resto de la red del hospital (aplicaciones, ficheros en otros equipos, etc.).

Aunque WPA se considera suficientemente robusta a día de hoy, ya existen procedimientos para, si la clave no es suficientemente robusta, llegar a ganar acceso a equipos con este tipo de encriptación. En la web de remote-exploit viene un tutorial en flash tremendamente gráfico y sencillo de realizar¹. Como el punto de acceso se encuentra conectado a la misma red que el resto de equipos (VLAN Gris) esto significaría que el agresor podría tener acceso a cualquiera de estos equipos.

En la conversación con dicho responsable le explicamos los peligros que puede acarrear disponer de esta conexión, y le solicitamos que se responsabilicen de comprobar que la red wireless sólo permanezca activa en los momentos en los que alguien realmente la necesite y al terminar la sesión la desconecten ellos mismos, al igual que repasan si el proyector o el PC se han apagados.

Por otra parte registramos la información de este punto de acceso para proceder a aplicar todas las restricciones necesarias cuando dispongamos de una política corporativa bien definida al respecto, si este AP las soporta.

Conclusiones

Como en otros muchos aspectos de la informática, la seguridad no está presente muchas veces en la mente del usuario con la importancia necesaria.

La mayoría de los usuarios considera que, una vez resuelto el problema del acceso físico a los equipos, están solventados muchos de los problemas de accesos indebidos, sin embargo hemos podido comprobar que no es así. Otras veces simplemente no se es consciente de los peligros que implican este tipo de tecnologías.

La formación continuada al usuario y la auditoría periódica serán dos de las herramientas que más nos puedan ayudar a minimizar la proliferación de puntos de acceso no controlados.

1 Remote-exploit - Tutorials WPA Cracking
(http://www.remote-exploit.org/index.php/Tutorials#WPA_Cracking)

Resultados del análisis conjunto y conclusiones.

En este epígrafe aplicaremos los conocimientos adquiridos en las fases anteriores y buscaremos soluciones para los diferentes ámbitos de aplicación de partida.

Dónde creemos que wifi puede ser más útil.

Después de este análisis entendemos que los principales lugares de uso de redes inalámbricas serán aquellas zonas que tengan una permeabilidad adecuada, que permita dar un servicio adecuado con pocos puntos de acceso.

La utilización de una nueva tecnología necesita dar confianza a los nuevos usuarios, que probablemente verán con recelo cualquier fallo que el nuevo sistema tenga. Experiencias en otros hospitales con malos resultados, como en el Hospital Universitario de Gante (Bélgica)[ETGF-ES], hacen reflexionar sobre el peligro de dar una herramienta en la cual el facultativo no puede llegar a confiar. Tras varios intentos de uso al final la nueva herramienta termina por abandonarse y volverse a las anteriores, menos tecnológicas pero más fiables. Sin embargo, experiencias positivas como la del Hospital de Son Llätzer en Mallorca nos indican que una tecnología bien implantada puede terminar siendo todo un éxito.

En nuestro caso particular, según los estudios que hemos realizado, la cobertura wifi debería concentrarse en una primera fase en las zonas remodeladas de los hospitales o en los edificios mas modernos, donde si puede sacarse un provecho adecuado a la tecnología sin hilos. Sin embargo, como hemos visto en el caso del HG, tratar de implantar esta solución en alas hospitalarias sin remodelar será costoso dado el corto alcance y la baja calidad de la señal, pudiendo llevar al fracaso del proyecto.

También sería aconsejable reflexionar sobre el tipo de comunicación de los clientes antes de proceder a cambiar el tipo de conexión de los puestos actuales. Como hemos comprobado, la red inalámbrica puede sufrir cortes esporádicos debidos a interferencias, y su ancho de banda es más limitado que el de una conexión actual (en la mayoría de los casos). Sustituir una conexión LAN existente por una WLAN puede significar un deterioro bastante importante en el trabajo del usuario.

Sí es muy conveniente esta red en salas de uso múltiple o conferencias. También, en el archivo de historias clínicas (tradicionales) y el almacén, permitiría disponer de equipos cliente que fueran validando directamente el contenido de las estanterías sobre una aplicación ligera desarrollada para una PDA, por ejemplo.

Respecto a la conexión para pacientes, parece aconsejable implantar puntos de acceso para los pacientes en las zonas de largas estancias donde actualmente utilizan un acceso telefónico a Internet. Con ello mejoraríamos tanto la velocidad de acceso de los pacientes como la posibilidad de que varios utilicen el acceso a la vez. Dada la naturaleza de estas zonas (aislamiento, mucho equipo médico, etc.) convendría dedicar especial atención a las posibles interferencias con el equipo clínico utilizado. Para ello aconsejamos abordar estas fases del proyecto coordinados con el área de Electromedicina, responsable del mantenimiento de este equipo.

De momento no se plantean conexiones desde los espacios abiertos entre edificios.

Decisiones de implementación.

Respecto a la implementación de la red creemos que la mejor aproximación sería una solución mixta entre las dos estudiadas:

- Para los usuarios tradicionales del hospital, que disponen de un usuario corporativo y un equipo cliente de acceso propio del hospital, la solución más interesante es permitirle un acceso a la red sin necesidad de tener que validarse ni dejar ninguna ventana abierta en el equipo. Por ello, para este tipo de usuarios lo ideal sería adoptar EAP/TLS con un servidor RADIUS y una entidad certificadora. Con un buen documento de ayuda y una sesión previa conectado a la LAN, el usuario podría generar su propio certificado digital y preparar su PC para conectarse sin intervención del STI.
- Para los pacientes que no tienen una vinculación fija con el hospital la solución de un portal cautivo les hace independientes del STI para poder acceder a Internet, y por otra parte nos asegura la conformidad del usuario con las políticas que se le hayan indicado en una cláusula que debe aceptar en el momento del registro (aunque el 99,9% de los usuarios no lee este tipo de cláusulas nunca).

Procedimiento de trabajo propuesto para el futuro.

De cara a la implantación futura de esta red conviene recordar los siguientes puntos antes de proceder a montar un nuevo punto de acceso:

- Comprobar el entorno en busca de elementos que produzcan interferencias o que se vean afectados por ellas. Realizar mediciones con la sonda.
- Realizar mediciones de alcance y calidad de la señal para asegurar que tendremos la cobertura necesaria. Elaborar un plano de implantación a partir de los datos recopilados.
- Repasar las aplicaciones que se utilizarán y, en caso de no conocerlo anteriormente, realizar medidas de consumo de ancho de banda y resistencia a desconexiones de la aplicación.
- Repasar el tipo de usuario que va a utilizar la red. Asegurarnos de que conoce sus ventajas y sus inconvenientes.
- Actualización de la documentación de despliegue de la red.
- Revisión periódica de las redes ya montadas y de los logs de acceso.

¿... Y en el futuro qué? Inteligencia Ambiental en entornos de salud pública

En la revisión y propuesta de uso de tecnologías inalámbricas que hemos realizado en este proyecto, hasta el momento hemos hecho referencia al presente más inmediato y viable de aplicación de dichas tecnologías en el escenario real de un hospital.

Sin embargo, en nuestro proyecto consideramos conveniente ampliar la visión actual del uso de las tecnologías inalámbricas a conceptos de futuro a medio y largo plazo. Esta visión enlaza con las perspectivas prospectivas propuestas en el índice del proyecto y su concreción en el ámbito de un hospital andaluz.

Para realizar este estudio se han utilizado varias fuentes bibliográficas destacando una de ella: el informe titulado “Safeguards in a World of Ambient Intelligence (SWAMI)” [SWAMI]

Introducción al concepto de Inteligencia Ambiental

El término “Ambient Intelligence” fue acuñado en Europa a partir del concepto estadounidense de “Ubiquitous Computing” (Mark Weisser 1991). Asimismo el concepto correspondiente en el ámbito japonés es “Ubiquitous Network Society”.

Weisser utilizó dicho término para describir la tercera generación de sistemas informáticos, que marcó el punto de inflexión inicial de la visión de una futura sociedad de la información.

Lo más significativo de la visión de Weiser es que mientras predecía la difusión masiva de Internet en pocos años, incluía la idea de redes generalizadas de computadores, asumiendo todo tipo de formatos y emplazamientos en escenarios no convencionales.

Fundamental en esta visión es la conexión de redes, sin la cual la habilidad de intercomunicación entre los ordenadores se vería muy limitada. En 1993, Weiser afirmó que la próxima generación de entornos de computación sería tal que “en ella una persona estaría continuamente interactuando con cientos de ordenadores de su entorno conectados de forma inalámbrica” (Weiser 1993).

En aquella época tales tipos de redes inalámbricas de computadores se encontraban en sus comienzos, sin embargo hoy en día mediante WLAN, WiMax y Bluetooth, las posibilidades de tales redes densas de área local están empezando a formar parte de la realidad.

Mientras los investigadores de los Estados Unidos trabajaban en la visión de Computación Ubicua, la Unión Europea comenzaba a promover una visión similar en su agenda de investigación y desarrollo. El término adoptado en Europa es “Ambient Intelligence”, es decir Inteligencia Ambiental, (acuñado por Emile Aarts, de Philips) que tiene mucho en común con la visión de Computación Ubicua de Weiser, aunque quizás dándole más énfasis a la “computación centrada en el usuario y con la visión de integración o convergencia de innovaciones respecto a tres tecnologías claves: computación ubicua, diseño de la interfaz de usuario y comunicación ubicua

Por tanto, el concepto de Inteligencia Ambiental hace alusión a la consideración de aspectos humanos que resultan claves tanto a la hora de tomar una decisión sobre la puesta en marcha de proyectos reales de computación ubicua, como a la hora de

llevarlos a cabo. En concreto, existen diversas cuestiones críticas, entre las que cabe destacar los siguientes:

- Usuarios bajo vigilancia
- Suplantación de la identidad
- Ataques maliciosos
- División digital o analfabetismo tecnológico
- Spamming

Escenario: Dominio de aplicaciones del sector de salud pública

En el citado documento encontramos un escenario específico de salud pública, que consideramos muy útil a la hora de prever un escenario semejante en el hospital en estudio. A continuación incluiremos la traducción del texto original descriptivo de dicho escenario, que nos servirá para pensar en las posibles futuras líneas de evolución que pudiera tener el presente proyecto.

Dominio de las aplicaciones de la salud

El ámbito de la salud conlleva dos aspectos a tener en cuenta. Por una parte, los cuidados de la salud determinan la vida y la muerte de la gente, y el acceso rápido a la información concerniente a la salud de una persona (por ejemplo, alergias y enfermedades crónicas) puede resultar muy importante en caso de emergencia.

Por otra parte, la información de la salud es muy confidencial. La gente probablemente no desea revelar sus problemas de salud, a sus superiores en el ámbito laboral, a las compañías de seguros e incluso a parientes cercanos. Por tanto, es importante (aunque quizás no sea fácil) desarrollar aplicaciones de Inteligencia Ambiental en el dominio de la salud de tal forma que los trabajadores de servicios de emergencia y los doctores puedan tener acceso a la información cuando la necesiten, pero nadie más pueda hacerlo sin autorización.

Las principales funcionalidades previstas de Inteligencia Ambiental en el dominio de la salud son las siguientes:

- Prevención de enfermedades, que incluye monitorización continua de la salud y de las actividades relacionadas con la salud (por ejemplo el ejercicio físico), promoción de estilo de vida saludable y consejos relacionados, alertas sobre productos alimenticios peligrosos (por ejemplo, aquellos que puedan causar reacciones alérgicas), y predicción de enfermedades, por ejemplo por análisis genético.
- Tratamiento de enfermedades, orientado hacia la recuperación a corto plazo. La curación comienza por el diagnóstico (que podría ser vía vídeo, o haciendo uso de los llamados “laboratorios en chips”, tecnologías para la medición de la presión sanguínea, análisis de orina, etc.) y continúa con el tratamiento en cualquier momento y lugar. Esto debería conseguirse haciendo uso de redes específicas de equipamiento médico e intercambio de información entre los doctores, así como diminutos sistemas de Inteligencia Ambiental capaces de dosificar fármacos, por ejemplo dispensadores de insulina para pacientes diabéticos. Los sistemas de Inteligencia Ambiental deberían ser capaces de realizar diagnósticos automáticos de crisis y dar la medicación necesaria, por ejemplo

en caso de problemas del corazón o epilepsia. En estos caso, la monitorización continua es también necesaria.

- Cuidados y atención domiciliaria. Es una actividad a largo plazo dirigida hacia el proceso de recuperación de pacientes y hacia el apoyo de las funciones de la vida diaria de la gente que necesita atención a largo plazo, tales como ancianos, discapacitados o enfermos crónicos.

Los cuidados también implican monitorización continua, con el objetivo de dar soporte a la vida de forma autónoma o semi-autónoma, y facilitar el proceso de recepción de los cuidados.

Los medios para conseguir este objetivo son, en primer lugar, “inteligencia incrustada” capaz de llevar el seguimiento de las actividades, detectar anomalías y dar consejo de forma inofensiva y, en segundo lugar, las “tecnologías de asistencia” tales como las ayudas a la audición, prótesis e implantes (por ejemplo, implantes del corazón).

- Optimización de la cadena de alarma en caso de emergencia (por ejemplo, ataque al corazón o un accidente), desde pedir ayuda hasta preparar el tratamiento.
- Funciones de apoyo, por ejemplo mejorar el intercambio de información, ayudar a seleccionar el especialista adecuado o hacer uso del seguro médico.

Por tanto, se prevé que las aplicaciones de la salud llegarán a ser posibles en cualquier sitio y en todo momento, con la ayuda de sofisticados sensores incrustados y/o actuadores para el seguimiento continuo de las acciones y la salud de los usuarios.

Los siguientes pasos

Para poder aplicar estos novedosos conceptos debe desarrollarse una conectividad generalizada de todos los equipos relacionados en la actividad asistencial en el propio hospital y posteriormente en el domicilio del paciente, pero siempre garantizando las medidas necesarias de acceso a la información e interoperabilidad de los diferentes elementos.

Próximos proyectos en esta línea serían la autenticación de los usuarios del sistema mediante sistemas criptográficos o biomédicos y el despliegue de estrategias de acceso único a los sistemas de información, que dejarán de estar almacenados en una plataforma monolítica para encontrarse distribuidos en forma de “grid” en diferentes entidades (bases de datos documentales, sensores en los pacientes, agentes inteligentes en otros hospitales, etc.).

Glosario.

ADSL

“Asymmetric Digital Subscriber Line”. Línea de conexión a internet económica que usa cableado telefónico. Sus velocidades de conexión varían desde los 128 Kbits a 2, 4 y 20 Mbits. Se basa en una distribución asimétrica de dicho canal de comunicación favoreciendo la descarga de contenidos del usuario frente al envío de información. Su principal reducción de coste frente a otras líneas de velocidades similares radica en que el nivel de compromiso de servicio por parte del proveedor es mucho menor que en otras tecnologías como Frame-Relay o ATM.

Ad-Hoc

Tipo de conexión inalámbrica entre iguales que se realiza entre dos equipos cliente para intercambiar información. Otra alternativa de conexión inalámbrica es usar un AP.

AP

“Access Point”. Siglas de un tipo de equipo para redes inalámbricas que ofrece servicio a varios usuarios de la red wireless conectándolos a través de un punto común, generalmente conectado mediante cable a otras redes mayores.

CNAF.

El Cuadro Nacional de Atribución de Frecuencias es la normativa española que regula el uso de frecuencias para los diferentes tipos de servicios de radiocomunicación. El cuadro vigente en la actualidad fue aprobado por la orden ITC/1998/2005, de 22 de JUNIO.

dBm

dBmW. Medida de potencia usada generalmente en transmisiones de radio que indica los miliwatios de potencia de emisión o recepción de un equipo en una escala de decibelios (logarítmica) lo cual permite utilizar la misma magnitud para transmisiones potentes y débiles.

BBDD

Sistema de gestión de Base de Datos. Programa que facilita las tareas de gestión y administración de un almacén centralizado de datos.

DICOM

Digital Imaging and COmmunications in Medicine (<http://medical.nema.org/>). Organismo que promueve diferentes formatos de intercambio de información en entornos médicos. Está muy difundido en los sistemas de imagen digital (TACs, RMNs, escáneres e impresoras de radiografías).

DoS

“Denial of Service”. Término que indica un ataque por el que un elemento deja de prestar servicio debido generalmente a un mal funcionamiento de éste en unas condiciones de trabajo para los que no fue desarrollado. Un ejemplo de este tipo de problemas es cuando se le realizan a un servidor web tantas peticiones, generalmente no válidas y ficticias, que el servicio web llega a detenerse.

Firmware

Software que se ejecuta en un equipo informático y que le confiere sus características y funciones principales. Normalmente está grabado en una memoria reescribible y es susceptible de ser cambiado por versiones mejores que el fabricante libera, con nuevas funcionalidades.

Historia Clínica Digital

Programa que recoge de forma centralizada toda la información relacionada con un paciente que se genera en las diferentes dependencias hospitalarias. Su función es concentrar en una única plataforma dichos datos, unificándolos y proporcionando a los usuarios unos criterios de acceso uniformes y una muestra jerarquizada de la información con diferentes niveles de acceso y privilegios.

ICM.

Bandas de frecuencias reservadas susceptibles de ser usadas con fines Industrial, Científico o Médico. Se encuentran divididas en 8 rangos y que van desde los 13,553 Mhz a los 61,50 Ghz. (ver CNAF).

MAC

“Media Access Control”. Capa del modelo OSI que hace referencia al acceso al medio físico. Por extensión se suele utilizar el término MAC para designar la dirección de un dispositivo para dicha capa, que en los entornos Ethernet consiste en una secuencia de seis octetos y que se suele representar como 00:00:00:00:00:00.

Man-in-the-Middle

Tipo de ataque por el cual se consigue interceptar la información que fluye entre dos elementos de una red interponiéndose en su camino. Generalmente se utiliza con otras técnicas de suplantación de la personalidad (desde el punto de vista de las comunicaciones) de forma que los implicados en la conexión creen estar enviando los datos al otro elemento aunque en realidad se la envían al atacante, que la registra y la hace llegar hasta su destinatario final para evitar ser detectado.

ODBC

“Open Database Connectivity”. Conjunto de programas que surgió en 1992 y que ofrecen una plataforma de desarrollo al programador que le aísla de muchas de las complejidades de la implementación final del motor de base de datos usado.

OSI

“Open Systems Interconnection”. Modelo de referencia generado en 1982 por ISO (“International Organization for Standardization”) e ITU-T (“ITU Telecommunication Standardization Sector”) para definir las características que deben cumplir los sistemas de red para garantizar la interoperabilidad entre los diferentes tipos de redes.

PAN

“Personal Area Network”. Adaptación de las conocidas siglas LAN o WAN para hacer referencia a los elementos que se interconectan en el entorno de una persona para proporcionarle algún servicio (auriculares bluetooth, conexión infrarrojos, etc.)

PDA

“Personal Digital Assistants”. Dispositivo electrónico de bolsillo que da al usuario funciones básicas de agenda, calendario, edición de texto, etc. La mejora de la tecnología y la miniaturización de los componentes ha facilitado que estos dispositivos sean cada vez más potentes y puedan a veces comportarse casi como un PC. Generalmente se utilizan para sincronizar determinadas tareas con otro equipo de mayores prestaciones pero más pesado. Las últimas generaciones ya llevan integradas tarjetas de acceso a redes inalámbricas.

RF.

Señales de Radio-Frecuencia.

SSID

“Service set identifier”. Código asociado a un punto de acceso por el que se identifica

la red inalámbrica a la que pertenece.

SS.CC.

Servicios Centrales. Abreviatura por la que se conoce al organismo que centraliza la gestión entre los diferentes hospitales que componen el Servicio Andaluz de Salud. Generalmente aglutina determinadas tareas de gestión y suele marcar políticas corporativas en determinados ámbitos de trabajo.

TLS

“Transport Layer Security”. Protocolo de nivel de transporte que proporciona encriptación de datos a través de redes no confiables.

Terminal VT/ emulación 3270

Terminal de conexión de texto usada para acceder a los antiguos sistemas mainframe. También conocida como terminal “tonta” debido a que su única función era mostrar la pantalla de un programa que funcionaba en el sistema central. Existían programas que emulan el comportamiento de dichas pantallas en un PC a los que por extensión se le llama programas de emulación de terminal. Las diferentes tecnologías de los mainframe hicieron aparecer varios tipos de terminales.

VLAN

“Virtual LAN”. Particionamiento de un segmento de red físico en varios segmentos lógicos gracias a un software. Permite aislar en la capa de enlace el tráfico entre los diferentes segmentos.

warwalking/wardriving

Término utilizado para nombrar a la afición de recorrer diferentes zonas en busca de redes inalámbricas para intentar hacer un uso no autorizado de ellas. El apelativo “driving” o “walking” designa cómo se hace la búsqueda, o bien desde un coche con un ordenador portátil y una antena o bien caminando con el portátil.

WLAN.

Wireless LAN. Nomenclatura usual para las redes inalámbricas.

WPA/WEP

“Wi-Fi Protected Access” o “Wired Equivalent Privacy”. Tecnologías de seguridad que intentan garantizar el acceso no fraudulento o la captura de tráfico de las redes inalámbricas mediante sistemas de encriptación. Con ellas se intenta evitar que un usuario no autorizado utilice una red inalámbrica o que pueda recoger información valiosa de los datos transmitidos para luego tratarlos (descubrir documentos, contraseñas de acceso, etc.). Este tipo de técnicas se han comenzado a desarrollar a partir del nacimiento de las redes sin cable, dado que la transmisión de información se realiza a un medio sin posibilidad de evitar quién recibe dicha transmisión. Serían el equivalente al GSM para la telefonía móvil, que anteriormente usaba transmisiones analógicas sin encriptación.

Referencias Bibliográficas

[CNAF] - Cuadro Nacional de Atribución de Frecuencias - SECRETARÍA DE ESTADO DE TELECOMUNICACIONES - Año:2005 -
url: <http://www.mityc.es/Telecomunicaciones/Secciones/Espectro/cnaf/>

[ETGF-ES] - Elementos Técnicos para la gestión de frecuencias en espacios complejos: Entornos Sanitarios - Grupo NAP - Año: 2005
ISBN: 84-934124-3-0

[SLPEAP] - Seguridad en LAN inalámbricas con PEAP y contraseñas - Microsoft - Año:2004 -
url: http://www.microsoft.com/latam/technet/seguridad/guidance/lan/peap_int.msp

[NPSRWI-FI] - Nuevos protocolos de seguridad en redes Wi-Fi - Pablo Garaizar Sagarminaga - Año:2002 – url: <http://www.e-ghost.deusto.es/docs/2005/conferencias/NuevosProtWiFi.pdf>

[RD 1066/2001] - Reglamento que establece condiciones de protección del dominio público radioeléctrico... - - Año:2001 – url: <http://www.mtas.es/insht/legislation/RD/radiofre.htm>

[WI-FOO] - WI-FOO The Secrets of Wireless Hacking - Andrew A. Vladimirov. Konstantin V. Gavrilenko. Anderi A. Mikhailovsky - Año: 2004 ISBN: 0-321-20217-1

[SWAMI] - Safeguards in a World of Ambient Intelligence (SWAMI) - Instituto de Estudios de Prospección Tecnológica - Año:2005 – url: <http://swami.jrc.es/pages/index.htm>

Anexos.

1.- Scripts de recogida de datos

captura.sh

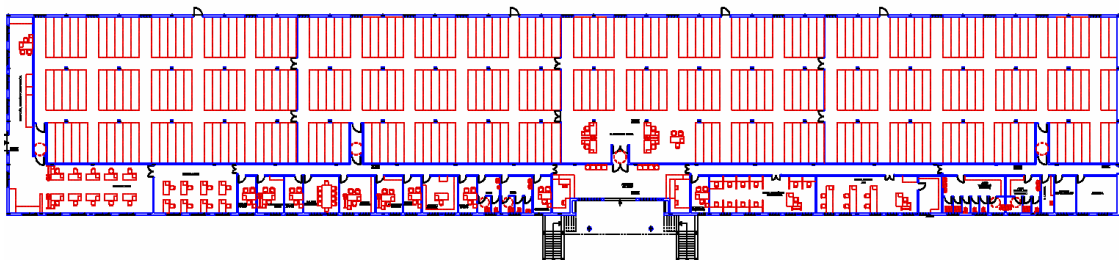
```
captura_wireless.sh eth1 punto$1 1 2 3
ncftpget ftp://10.232.0.17/bootcdv9.nrg >> punto$1.ftp.log
```

captura_wireless.sh

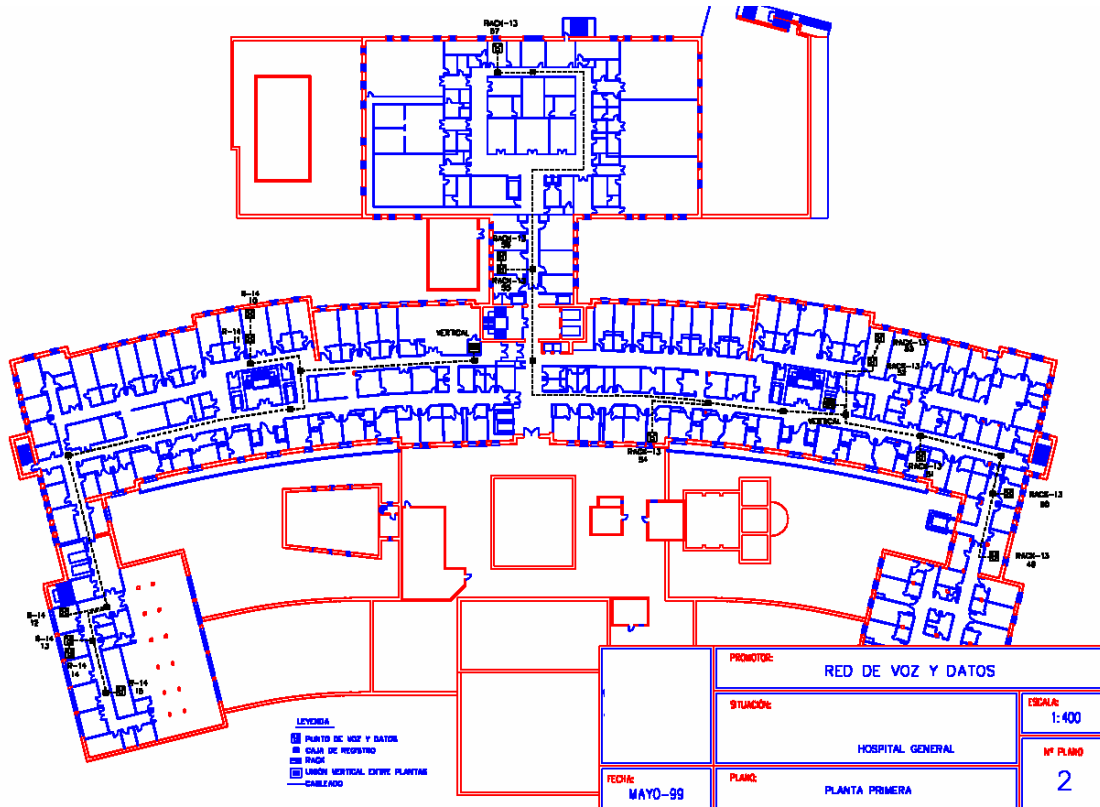
```
#!/bin/sh
if [ -z "$1" ]; then
echo "Error. Necesita indicar un interfaz de escucha"
exit
else
interf=$1
fi
if [ -z "$2" ]; then
fichero=/dev/null
else
fichero=$2.log
fi
date >> $fichero
echo ----- >> $fichero
export apoyo=/tmp/wl_meter.log
echo ESSID~Frequency GHz~Access Point~Bit Rate Mb/s~Tx-Power dBm~Retry limit~Power
Management~Link Quality~Signal level dBm~Noise level dBm~Tx excessive retries | tee -a
$fichero
echo $1
while [ ! -z "$1" ]; do
iwconfig $interf > $apoyo
ESSID=`cat /tmp/wl_meter.log | grep ESSID | cut -d ":" -f 2 | cut -d "'" -f 2`
Frequency=`cat /tmp/wl_meter.log | grep Frequency | cut -d ":" -f 3 | cut -d " " -f 1-2`
AccessPoint=`cat /tmp/wl_meter.log | grep "Access Point" | cut -d ":" -f 4-12`
BitRate=`cat /tmp/wl_meter.log | grep "Bit Rate" | cut -d "=" -f 2 | cut -d " " -f 1`
TxPower=`cat /tmp/wl_meter.log | grep "Tx-Power" | cut -d "=" -f 3 | cut -d " " -f 1`
Retrylimit=`cat /tmp/wl_meter.log | grep "Retry limit" | cut -d ":" -f 2 | cut -d " " -f
1`
PowerMgmt=`cat /tmp/wl_meter.log | grep "Power Management" | cut -d ":" -f 2`
LinkQuality=`cat /tmp/wl_meter.log | grep "Link Quality" | cut -d "=" -f 2 | cut -d " "
-f 1`
SignalLevel=`cat /tmp/wl_meter.log | grep "Signal level" | cut -d "=" -f 3 | cut -d " "
-f 1`
NoiseLevel=`cat /tmp/wl_meter.log | grep "Noise level" | cut -d "=" -f 4 | cut -d " " -f
1`
TxexRetries=`cat /tmp/wl_meter.log | grep "Tx excessive retries" | cut -d ":" -f 2 | cut
-d " " -f 1`
echo
$ESSID~$Frequency~$AccessPoint~$BitRate~$TxPower~$Retrylimit~$PowerMgmt~$LinkQuality~$Si
gnalLevel~$NoiseLevel~$TxexRetries | tee -a $fichero
sleep 1
shift
done
```

2.- Planos de los edificios.

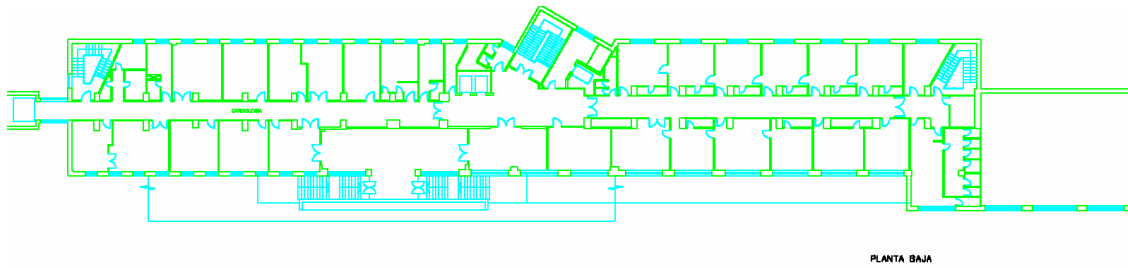
CDCA



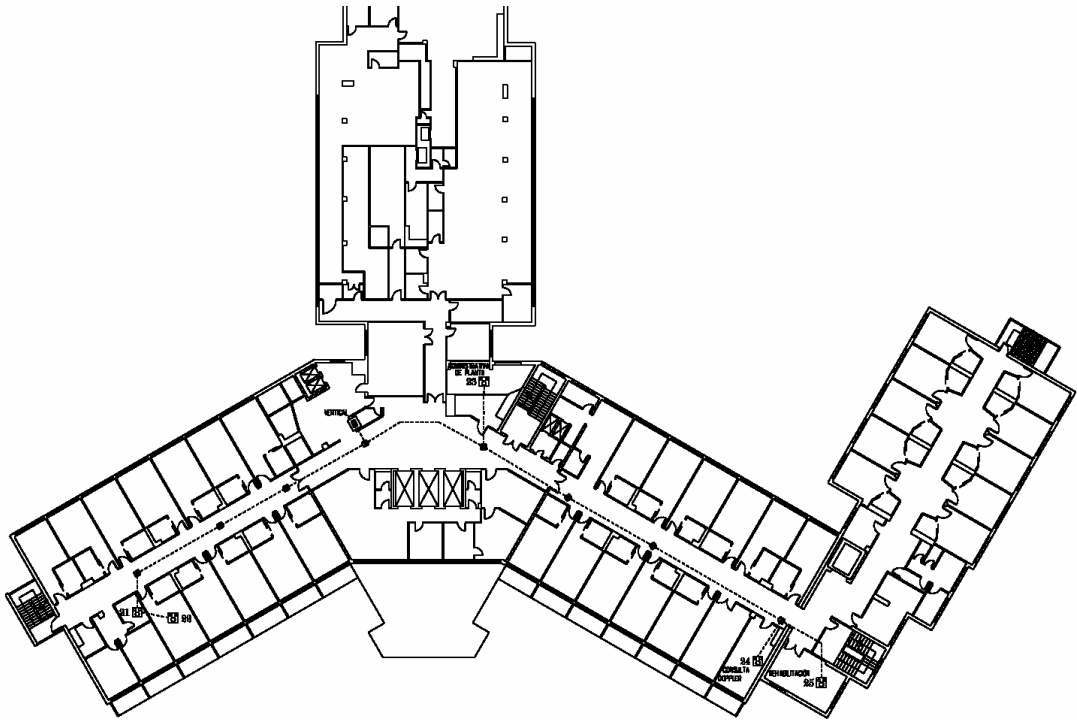
H.G.



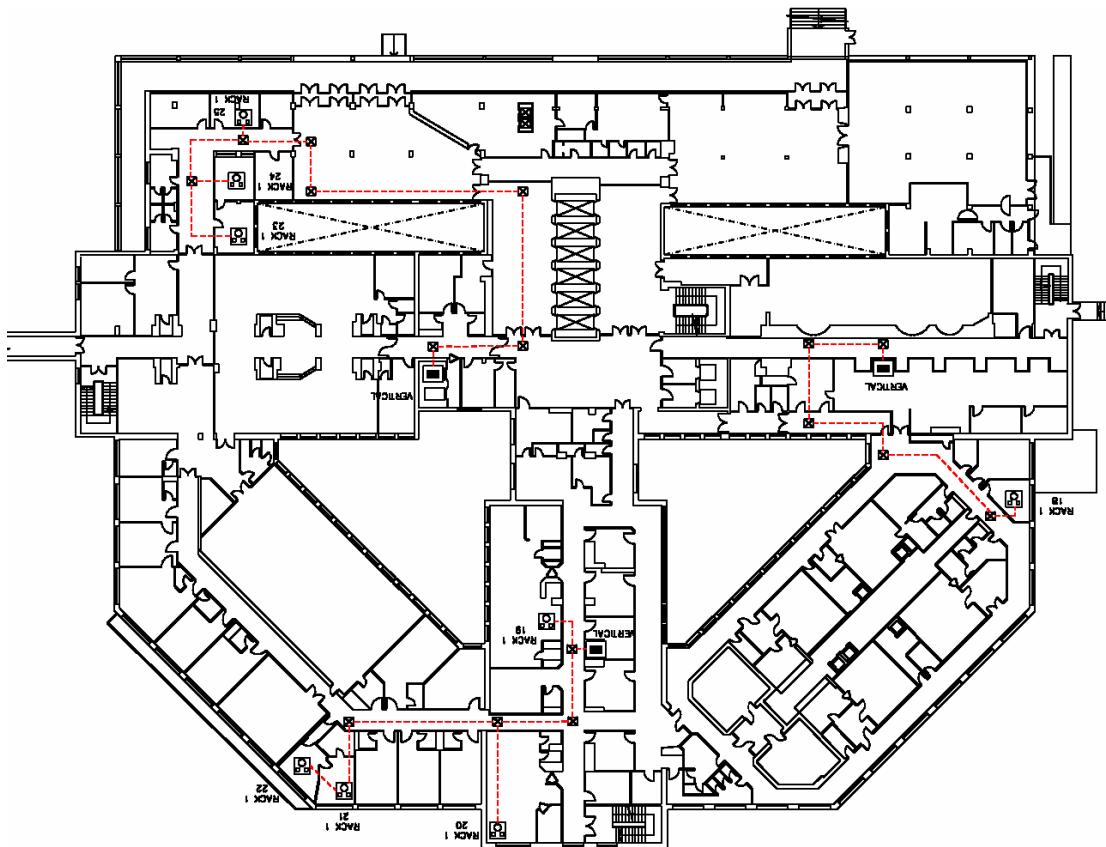
E.L.



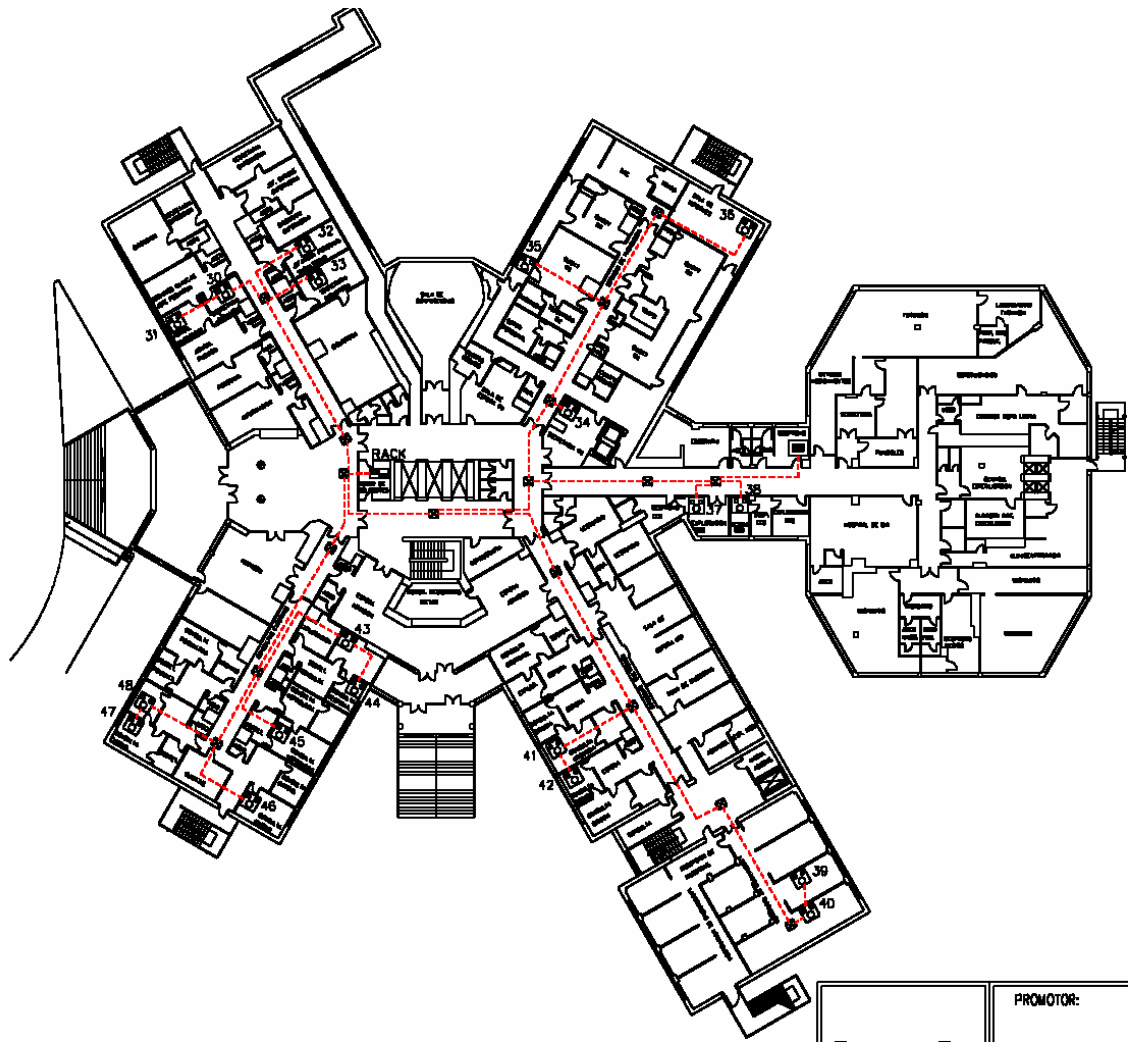
H.R.T.



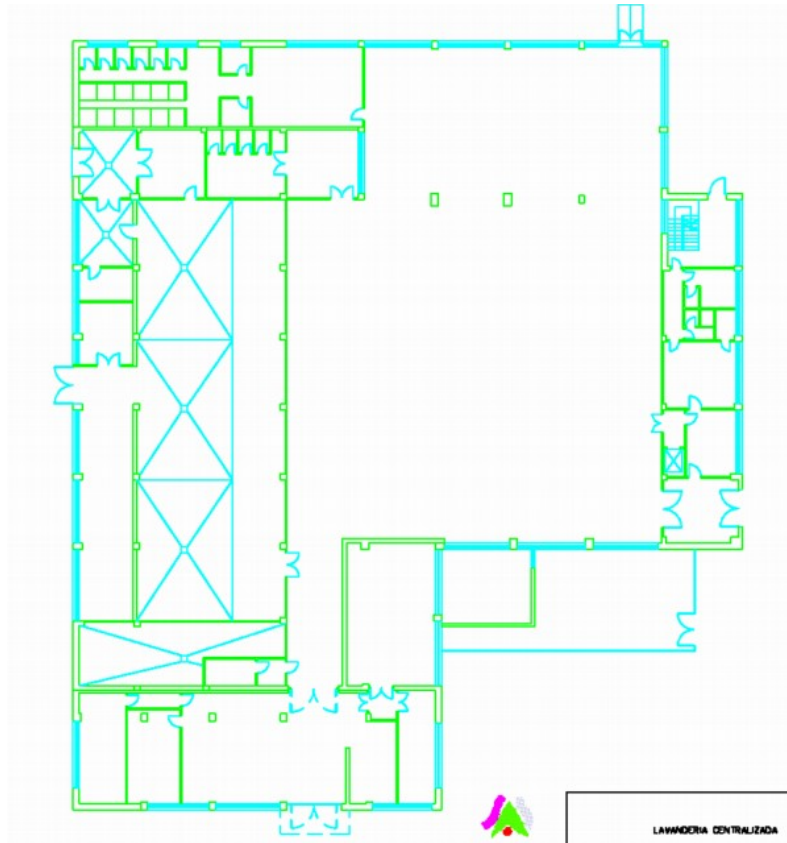
H.M.



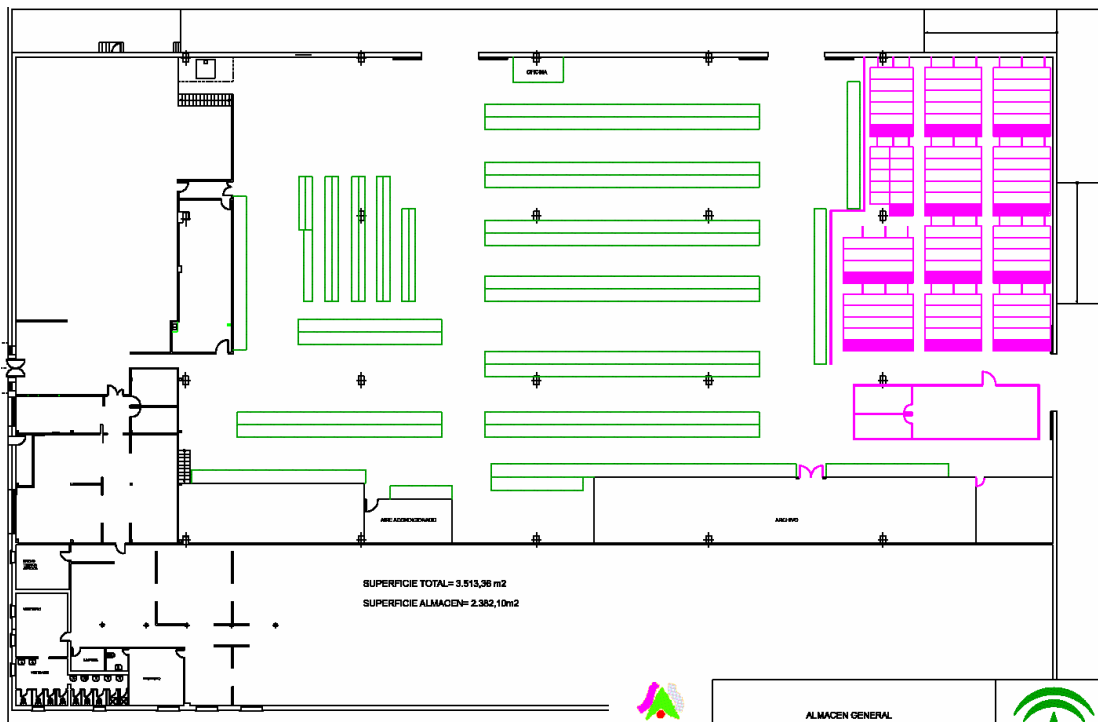
H.I.



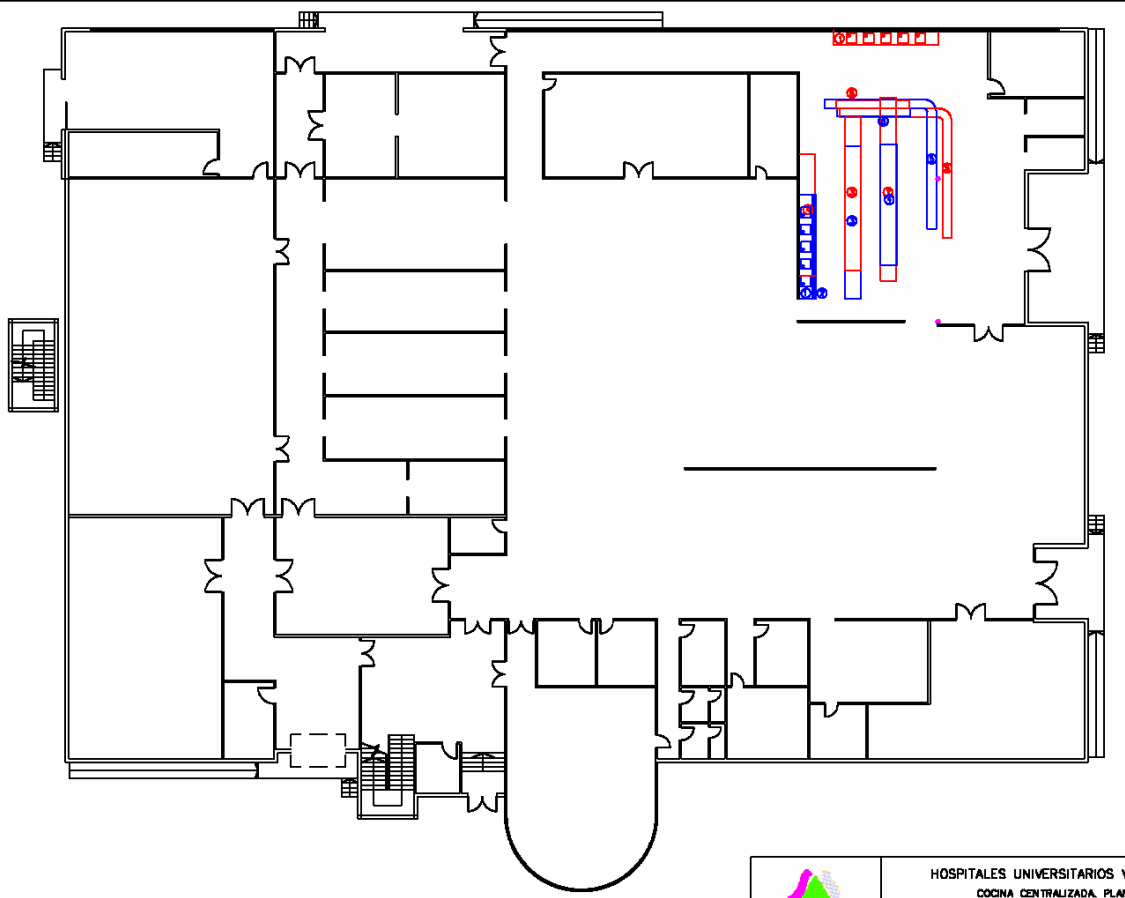
Lav.



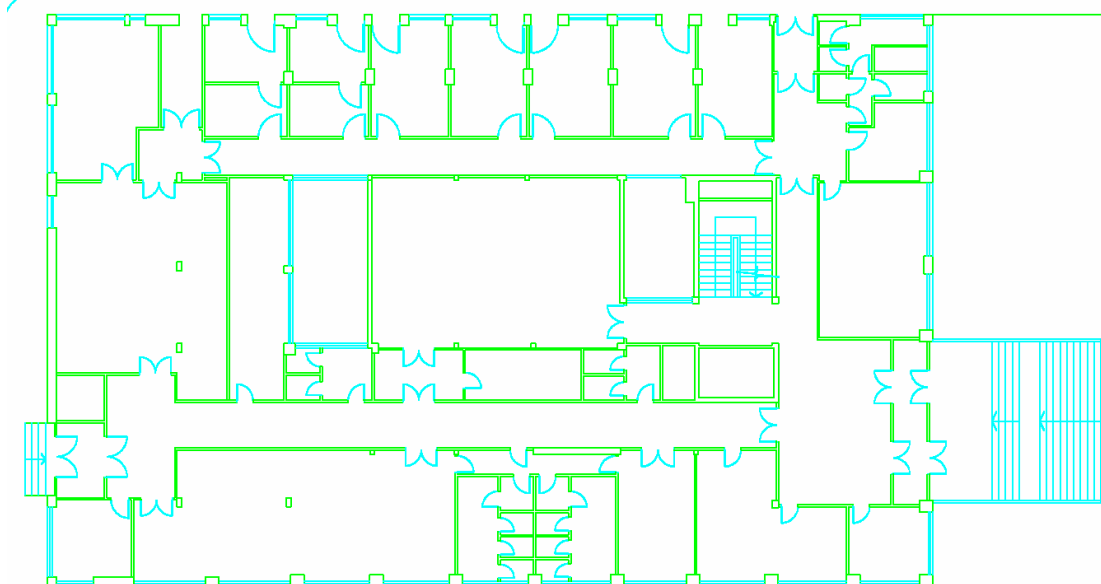
E.G.R.



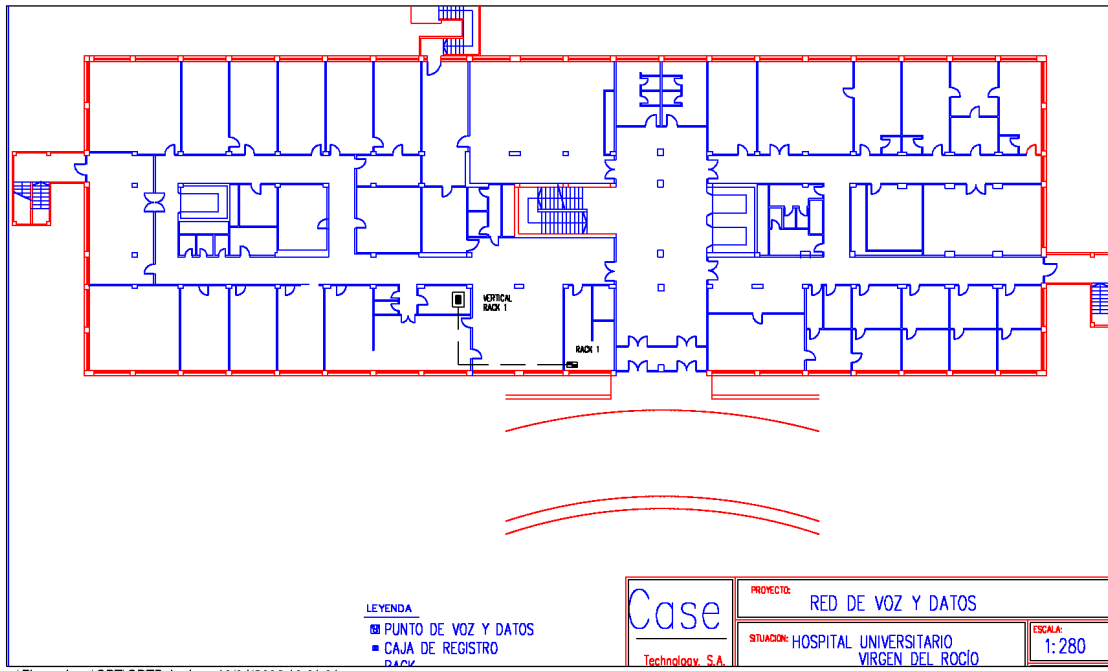
U.A.



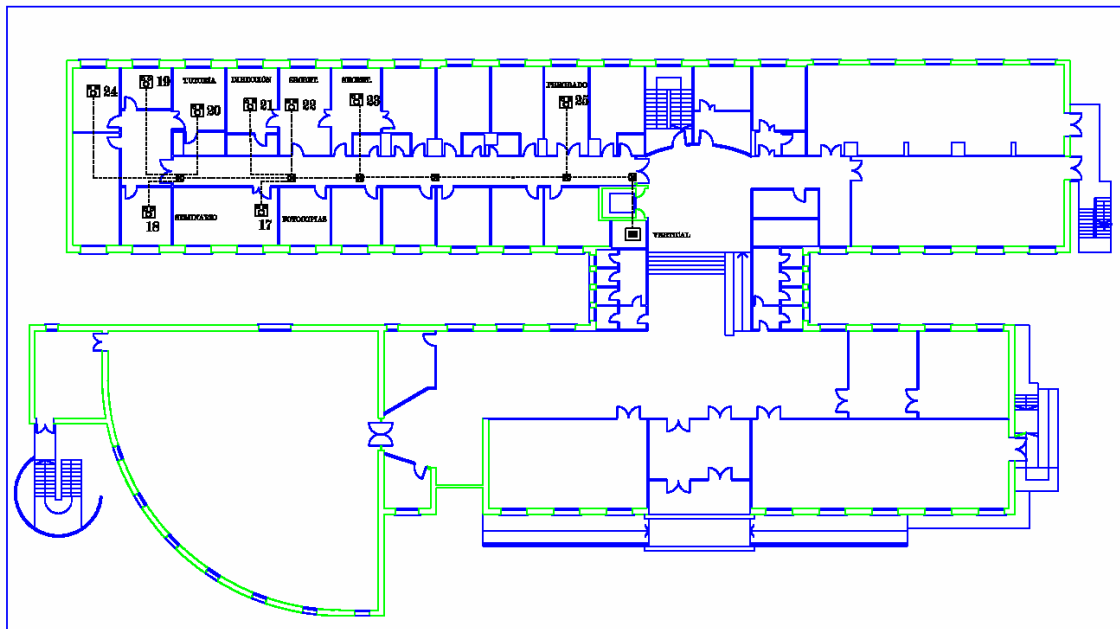
A.P.



C.D.T.



E.G.



Índice de contenido

Determinación del procedimiento de estudio.....	3
Objetivos.....	3
Tareas realizadas.....	3
Estudio de los planos de los edificios.....	3
Descripción de los edificios:.....	3
Disposición geográfica y planos.....	4
Procedimiento de estudio.....	5
Documentación de cada edificio.....	5
Búsqueda de redes inalámbricas ya existentes.....	5
Medidas de alcance en los puntos identificados en el 1er. paso.....	6
Medidas de interferencias.....	7
Estudio Tecnológico.....	9
Análisis de objetivos del estudio.....	9
Ámbito de trabajo.....	9
Objetivos del estudio.....	12
Interferencias con otros equipamientos.....	13
Interferencias con equipamiento médico.....	15
Datos a tener en cuenta para la implementación.....	16
Aspectos tecnológicos.....	16
Políticas válidas y políticas no recomendables.....	21
Estudio físico.....	24
Medidas de alcance y rendimiento.....	24
Equipamiento.....	24
Datos de estructura de los edificios.....	25
Reunión de toma de datos.....	26
Decisiones de puntos de medida tras la reunión.....	27
Medidas en el EGR.....	28
Colocación del AP y Medidas de interferencias.....	29
Medidas y primeras conclusiones.....	30
Gráficos comparativos.....	31
Ejemplo de despliegue previsto en el edificio.....	32
Medidas en el HG.....	33
Conclusiones de las medidas obtenidas.....	34
Redes inalámbricas encontradas (warwalking).....	35
00:A0:C5:9C:FB:DD.....	35
00:11:50:36:5D:9F.....	36
00:0F:3D:9F:F2:AA.....	37
Conclusiones.....	37
Resultados del análisis conjunto y conclusiones.....	38
Dónde creemos que wifi puede ser más útil.....	38
Decisiones de implementación.....	39
Procedimiento de trabajo propuesto para el futuro.....	39
¿... Y en el futuro qué? Inteligencia Ambiental en entornos de salud pública.....	40
Introducción al concepto de Inteligencia Ambiental.....	40
Escenario: Dominio de aplicaciones del sector de salud pública.....	41
Dominio de las aplicaciones de la salud.....	41
Los siguientes pasos.....	42
Glosario.....	43
Referencias Bibliográficas.....	46
Anexos.....	47
1.- Scripts de recogida de datos.....	47

2.- Planos de los edificios.....	47
CDCA.....	47
H.G.....	48
E.L.....	48
H.R. T.....	48
H.M.....	49
H.I.....	49
Lav.....	51
E.G.R.....	51
U.A.....	52
A.P.....	52
C.D.T.....	53
E.G.....	53