UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES
ARAGÓN

REDES INALÁMBRICAS
(Wi-Fi)

T E S I S

QUE PARA OBTENER EL TÍTULO DE:
INGENIERO MECÁNICO ELECTRICISTA
ÁREA: ELÉCTRICO - ELECTRÓNICO
P R S E N T A N:
SAÚL MARTÍNEZ ALCIBAR
MARCELO GERARDO ROSAS FLORES

ASESOR: ING. JUAN GASTALDI PÉREZ

MÉXICO 2005

Dedicatorias

A mi padres:
Marcelo Rosas L y Ma. Luisa Flores B

Por haberme apoyado en todo dándome
Siempre su cariño, amor y comprensión.
Gracias por encausarme en el camino del
bien para alcanzar el objetivo deseado.

A mi amiga especial:

A la persona que Me dio su Apoyo
Tanto En los momentos felices como en
los momentos tristes, le doy grAcias por
acompañarMe en el caminO del éxito y
del triunfo por eso Mil gracias...

Quería decirte que te quiero.
Lo feliz que soy
por haberte conocido,
lo mucho que significas para mí
y lo maravillosa que es la vida
junto a vos.....
Porque .....
me aceptas como soy,
Porque me amás,
y porque compartís conmigo,
los momentos más hermosos de mi vida

A mi amigo:

Gracias por brindarme tu amistad y
estar hoy, mañana y siempre Gracias.

Pbo Sergio J Garcia Ll y Jorge Marin.

A mis padres,

Gloria Alcibar González
Heriberto Martínez Cerón

Qué puedo decirles, sino mil gracias por ser el mejor ejemplo que he podido tener.

Hay padres que simplemente no deberían serlo, ustedes son una muestra de toda esta gama de sentimientos y conceptos que encierra el poder decir esta palabra "Padres", no puedo expresar aquí mismo todo lo que siento por ustedes, tan solo me resta decirles gracias por serlo y por seguir aun aquí.

Les dedico este pequeño paso en mi vida, ya que fue gracias a ustedes que pude lograrlo. No se que venga después, pero esto, esto es para ustedes.

Perdón por no saber ser el hijo que ustedes merecen.

Saúl Martínez Alcibar.

INDICE

INTRODUCCIÓN

Se llama comunicación inalámbrica a aquélla que se lleva a cabo sin el uso de cables de interconexión entre los participantes; por ejemplo, una comunicación con teléfono móvil es inalámbrica, mientras que una comunicación con teléfono fijo tradicional no lo es.

Una de las tecnologías más prometedoras y discutidas en estos tiempos es la de poder comunicar computadoras mediante tecnología inalámbrica. La conexión de computadoras mediante Radio Frecuencias o Luz Infrarroja, actualmente está siendo ampliamente investigada. Las Redes Inalámbricas facilitan la operación en lugares donde la computadora no puede permanecer en un solo lugar. Una red de área local (LAN) convencional envía paquetes de datos de un equipo a otro a través de cables o hilos. Una red de área local inalámbrica (WLAN) utiliza ondas de radio para transmitir los datos. Los datos se sobreponen a una onda de radio mediante un proceso denominado modulación, y esta onda portadora actúa como medio de transmisión, desempeñando la función del cable.

Desde el principio de los años 70 hemos tenido una red, la red Ethernet, que ha supuesto una estandarización a la hora de transmitir datos, con un gran éxito en todo el mundo. Aunque no es el único, si es el que más ha influenciado el uso habitual de las redes de área local (LAN). Nos hemos acostumbrado a tener redes de computadores de bajo coste, altas velocidades y una relativamente fácil instalación, más que apto para la mayoría de las aplicaciones. Pero el hecho de tener una infraestructura nos limita a ésas líneas preinstaladas, y los costes ante fallos, mantenimiento y reestructuración se disparan. La flexibilidad es muy baja e incluso no resulta factible la instalación de éstas líneas en algunos edificios, antiguos de valor histórico o peligrosos con asbestos u otros materiales. Todo esto puede ser solucionado con las nuevas tecnologías inalámbricas, puesto que ya no es necesaria la instalación de cables. E incluso algunos usuarios de la red inalámbrica puede verse afectado por un aumento de productividad:

- Médicos con acceso instantáneo al historial clínico de sus pacientes desde la habitación del mismo, registrando nuevos datos. O viendo constantes vitales de forma remota.

- Empresarios, que llevan consigo su portátil a distintas reuniones podrán intercomunicarse fácilmente con sus colegas, intercambiando información, diapositivas, ideas....

- En fábricas, dónde un ingeniero puede acceder a especificaciones y manuales de aparatos desde su portátil, para mantenimiento o reparación incluso en ambientes hostiles, dónde resulta imposible la instalación de una red cableada.

- Inventario de almacenes con el uso de etiquetas inteligentes, que permiten registrar productos en la base de datos, y modificarlos cuando son vendidos.

- Para emergencias, dónde no hay tiempo para desplegar una red cableada.

- Conexiones entre edificios de una misma empresa y evitar excesivo gasto en tiempo y dinero.

- O tan sólo de eliminar los tediosos cables que a todos nos molesta.

Es por eso que el siguiente trabajo de tesis tiene como objetivo principal realizar un análisis de las redes inalámbricas de área local que se han consolidado durante los últimos años, la cuales presentan distintos avances tecnológicos que pueden influir en la forma en la que se puede implementar una red. Actualmente, existen varias soluciones de redes LAN inalámbricas, con distintos niveles de estandardización e interoperabilidad. Así mismo, en este trabajo nos adentraremos en el estándar IEEE 802.11 y en su certificación Wi-Fi, ya que es la solución que cuenta con una mayor aceptación en el mercado y es la mejor respaldada por los principales fabricantes de equipos para redes de computadora.

El proceso de realización para llevar a cabo el análisis de las redes inalámbricas de área local fue: obteniendo información de diversas páginas de Internet de las principales organizaciones y comunidades Wi-Fi que existen en el mundo, así como, de los principales fabricantes y empresas desarrolladoras de esta tecnología; también se obtuvo información de los pocos libros que tratan este tipo de redes y algunos otros relacionados con los diversos temas aquí tratados; la base principal de la investigación fue recopilada del estándar IEEE 802.11 distribuido por la IEEE Wireless LAN Edition.

Con la información recopilada se desarrollo el capitulado del temario propuesto para este trabajo tesis.

En el Capitulo 1 mencionamos las distintas tecnologías existentes y competitivas en el mercado para las redes inalámbricas de área local para comprender mejor el por que se eligió Wi-Fi para la realización de esta tesis.

Ya en el Capitulo 2 nos adentramos en el estándar IEEE 802.11, para describir de manera muy técnica los principios generales en los que se basa su funcionamiento, así como, los distintos miembros de esta familia que están dedicados a mejorar cada uno de ellos el estándar en diversos aspectos.

Para que cualquier tipo de red funcione correctamente, es vital saber como realizar una buena elección del tipo de arquitectura y equipo de conexión a utilizar, logrando así que cubran nuestras necesidades; lo anterior se trata en el Capítulo 3.

Finalmente en el Capitulo 4 tratamos un tema muy importante y uno de los dos puntos por el cual las redes inalámbricas se dice que todavía no están a la altura de las redes cableadas, este punto es la seguridad; en este capitulo también se muestran los escenarios idóneos para la implementación de las redes inalámbricas, así como, sus principales aplicaciones en el mundo de las redes de computadoras.

El resultado final de este trabajo de tesis fue el de tener un estudio sobre las redes inalámbricas resaltando la tecnología existente que hoy por hoy predomina y que es causa de una gran popularidad, así también para que sirva como apoyo para la realización de otras tesis o como material de consulta para generaciones futuras de estudiantes de esta gran casa de estudios que es la UNAM o de otras instituciones.

Este trabajo de tesis tiene como segundo resultado servir de apoyo didáctico para la implementación de una red inalámbrica, dar las bases necesarias para su comprensión y su implementación, y de ninguna forma pretende ser una receta de cocina para redes, ya que las necesidades e implementación para cada escenario son distintas.

CAPÍTULO 1

LOS ESTANDARES WLAN COMPETIDORES

Una red inalámbrica de datos no es más que un conjunto de ordenadores, o de cualquier otro dispositivo informático, comunicados entre sí mediante soluciones que no requieran el uso de cables de interconexión, estas soluciones pueden ser por radiofrecuencia, microondas o infrarrojos.

En este capitulo se va a definir una clasificación para las diferentes redes inalámbricas que existen, y se mencionarán de manera breve, para después adentrarnos en el tipo de red del la que es objeto este trabajo de tesis, así como, sus principales competidores en el mercado.

CLASIFICACIÓN DE LAS REDES INALÁMBRICAS

Las comunicaciones inalámbricas, como cualquier otra cosa en esta vida, pueden clasificarse de distintas formas dependiendo del criterio al que se atienda. En este caso, vamos a clasificar a los sistemas de comunicaciones inalámbricas de acuerdo con su alcance.

Se llama alcance a la distancia máxima a la que pueden situarse las dos partes de la comunicación inalámbrica.

Existen dos amplias categorías de Redes Inalámbricas:

- *De Largo Alcance*.- Estas son utilizadas para transmitir la información en espacios que pueden variar desde una misma ciudad o hasta varios países circunvecinos (mejor conocido como Redes de Área Metropolitana MAN); sus velocidades de transmisión son relativamente bajas, de 4.8 a 19.2 Kbps.

- *De Corto Alcance* .- Estas son utilizadas principalmente en redes corporativas cuyas oficinas se encuentran en uno o varios edificios que no se encuentran muy retirados entre sí(que son las LANs Redes de Área Local), con velocidades del orden de 280 Kbps hasta los 100Mbps con soluciones propietarias.

La redes que se van a tratar en este trabajo de tesis son las de corto alcance ya que Wi.Fi pertenece a ésta , por esa razón solo se va a mencionar de manera muy superficial las redes de largo alcance.

Redes de Área Metropolitana MAN

La mayor revolución en las comunicaciones sin cables empezó con los teléfonos móviles. Los teléfonos móviles han sido el producto electrónico con más éxito de todos los tiempos, con más de 264 millones de unidades vendidas en 1999, un número que se espera que para el año 2004 se haya multiplicado por tres.

Cuando se dieron a conocer por primera vez, los teléfonos móviles tenían una función principal ofrecer comunicación por voz pero esto ha cambiado. Los sistemas de telefonía actuales cada vez utilizan más recursos de las tecnologías informáticas. Y con baterías de mayor duración, interfaces inteligentes, reconocimiento de voz y mayor velocidad, el uso del teléfono móvil está destinado a dispararse aún más en un futuro próximo, aunque utilizando cada vez más sus nuevos servicios inalámbricos y cada vez menos sus tradicionales servicios de teléfono estándar.

Para dar cobertura de transmisiones inalámbricas a un área geográfica determinada formando una red de área extensa (WAN), ésta se divide en zonas más pequeñas, denominadas células. Cada célula es la zona cubierta por una estación base radio de baja potencia con sus correspondientes antenas, y operando a frecuencias de radio individuales, que se repiten una y otra vez en otras células no adyacentes. Las llamadas realizadas en estas células se gestionan en las estaciones base o en conmutadores móviles. Estos últimos están conectados a bases de datos que hacen de interfaz entre la red inalámbrica y la red de telefonía cableada.

Cuando un teléfono móvil cruza los límites entre dos células, detecta que la señal de la célula que abandona es cada vez más débil, transfiriéndose automáticamente la llamada a la antena de la célula a la que se dirige cuando su señal sea la más potente. Y como el sistema funciona con un nivel de potencia muy bajo, las frecuencias utilizadas en una célula determinada no producen ningún tipo de interferencia en células adyacentes.

Los usuarios que ocupan un área geográfica dada deben disputarse un número limitado de canales y existen varios modos de dividir el espectro para proporcionar acceso de forma organizada:

- El FDMA (Frequency Division Multiple Access) divide un espectro disponible en franjas no solapadas en la dimensión o dominio de la frecuencia. El FDMA es el modo más familiar de dividir un espectro y tradicionalmente ha sido utilizado por los sistemas análogicos.

- El TDMA (Time Division Multiple Access) divide un espectro disponible en franjas no solapadas en la dimensión o dominio del tiempo. Los sistemas digitales son típicamente una combinación de FDMA y TDMA, donde la capacidad disponible se divide tanto en dimensiones de frecuencia como de tiempo, asignando a los usuarios canales de distintas frecuencias que utilizan en distintas franjas de tiempo.

- El GSM (Global System for Mobile Communications) es un tipo de red digital inalámbrica TDMA con características de cifrado y usada ampliamente por toda Europa a 900 MHz.

- El CDAM (Code Division Multiple Access) está basado en el concepto de espectro ensanchado, lo que significa que múltiples conversaciones comparten simultáneamente un espectro disponible y se distinguen entre sí mediante codificación en vez de usar canales de frecuencia o de tiempo.

Una compañía de telefonía inalámbrica que opera en un área geográfica definida ofrece este acceso WAN al usuario móvil en la forma de diversos planes y opciones de llamadas mensuales. Cuando sus abonados viajan fuera del área geográfica cubierta por la compañía, se les considera en roaming. Su compañía local transfiere el servicio a la compañía que opera esa área, con un coste de llamada mayor.

Existen dos tipos básicos de señales: analógica y digital. Una señal análógica puede tomar cualquier valor intermedio entre un máximo y un mínimo. Un ejemplo de señal analógica es la voz humana. Una señal digital no puede tomar cualquier valor, sino sólo un conjunto limitado de valores llamados símbolos, que pueden representar números o caracteres alfabéticos. Ejemplos de señal digital son un impulso de corriente en un cable o un impulso de luz en un cable de fibra óptica. Los sistemas inalámbricos tienden cada vez más hacia los sistemas digitales y el uso de formas avanzadas de modulación digital. Esto es debido a que la señal digital es más inmune al ruido y su manipulación o procesamiento es más sencillo que el de una señal analógica.

Existen dos tipos de redes de larga distancia: Redes de Conmutación de Paquetes (públicas y privadas) y Redes Telefónicas Celulares. Estas últimas son un medio para transmitir información de alto precio. Debido a que los módems celulares actualmente son más caros y delicados que los convencionales, ya que requieren circuiteria especial, que permite mantener la pérdida de señal cuando el circuito se alterna entre una célula y otra.

La otra opción que existe en redes de larga distancia son las denominadas: *Red Pública De Conmutación De Paquetes Por Radio*. Estas redes no tienen problemas de pérdida de señal debido a que su arquitectura está diseñada para soportar paquetes de datos en lugar de comunicaciones de voz. Las redes privadas de conmutación de paquetes utilizan la misma tecnología que las públicas, pero bajo bandas de radio frecuencia restringidas por la propia organización de sus sistemas de cómputo.

Redes Inalámbricas De Área Local WLANs

WLAN son las siglas en inglés de Wireless Local Area Networks (Redes Inalámbricas de Área Local).

Una red WLAN de datos no es más que un conjunto de ordenadores, o de cualquier otro dispositivo informático, comunicados entre sí mediante soluciones que no requieran el uso de cables de interconexión.

Aunque se puede llegar a pensar que las redes inalámbricas están orientadas a dar solución a las necesidades de comunicaciones de las empresas, dado su bajo costo, cada vez más forman parte del equipamiento de comunicaciones de los hogares.

Para disponer de una red inalámbrica, sólo hace falta instalar una tarjeta de red inalámbrica en los ordenadores involucrados, hacer una pequeña configuración y listo. Esto quiere decir que instalar una red inalámbrica es un proceso mucho más rápido y flexible que instalar una red cableada. Piense lo que supone tener que instalar cables por los suelos y paredes de la oficina o la casa. Además, las redes inalámbricas le permiten a sus usuarios moverse libremente sin perder la comunicación.

Una vez instalada la red inalámbrica, su utilización es prácticamente idéntica a la de una red cableada. Los ordenadores que forman parte de la red pueden comunicarse entre sí y compartir toda clase de recursos. Se pueden compartir archivos, directorios, impresoras, disqueteras o, incluso el acceso a otras redes. como puede ser Internet. Para el usuario, en general, no hay diferencia entre estar conectado a una red cableada o a una red inalámbrica. De la misma forma, al igual que ocurre con las redes cableadas, una red inalámbrica puede estar formada por tan sólo dos ordenadores o por miles de ellos.

Por todo lo anterior, las soluciones inalámbricas están poco a poco ocupando un lugar más destacado dentro del panorama de las posibilidades que tienen dos equipos informáticos de intercomunicarse.

Es clara la alta dependencia en los negocios de la redes de comunicación. Por ello la posibilidad de compartir información sin que sea necesario buscar una conexión física permite mayor movilidad y comodidad. Así mismo la red puede ser más extensa sin tener que mover o instalar cables.

Respecto a la red tradicional la red sin cable ofrece las siguientes ventajas:

- Movilidad: Información en tiempo real en cualquier lugar de la organización o empresa para todo usuario de la red. El que se obtenga en tiempo real supone mayor productividad y posibilidades de servicio.
- Facilidad de instalación: Evita obras para tirar cable por muros y techos.
- Flexibilidad: Permite llegar donde el cable no puede.
- Reducción de costes: Cuando se dan cambios frecuentes o el entorno es muy dinámico el coste inicialmente más alto de la red sin cable es significativamente más bajo, además de tener mayor tiempo de vida y menor gasto de instalación.
- Escalabilidad: El cambio de topología de red es sencillo y trata igual pequeñas y grandes redes.

El uso más frecuente de las WLAN es como extensión de la redes cableadas de modo que se da una conexión a un usuario final móvil.

- En hospitales: datos del paciente transmitidos de forma instantánea.
- En pequeños grupos de trabajo que necesiten una puesta en marcha rápida de una red (por ejemplo, grupos de revisión del estado de cuentas).
- En entornos dinámicos: se minimiza la sobrecarga causada por extensiones de redes cableadas, movimientos de éstas u otros cambios instalando red sin cable.
- En centros de formación, universidades, corporaciones, etc., donde se usa red sin cable para tener fácil acceso a la información, intercambiar ésta y aprender.
- En viejos edificios es también la más adecuada.
- Los trabajadores de almacenes intercambian información con una base de datos central mediante red sin cable de modo que aumenta la productividad. También para funciones críticas que requieren rapidez.

No obstante, hoy por hoy, las soluciones inalámbricas tienen también algunos inconvenientes: tienen un menor ancho de banda (velocidad de transmisión) y, en general, son más caras que las soluciones con cable. El ancho de banda de las soluciones inalámbricas actuales se encuentra entre los 11 y los 54 Mbps (aunque ya existen algunas soluciones propietarias a 100 Mbps), mientras que las redes de cable alcanzan los 1 a 5Gbps. En cuanto al precio, aunque, en general, son algo

más caras, en muchas ocasiones resultan no sólo más baratas que su alternativa cableada, sino que se muestran como la solución más conveniente.

TIPOS DE REDES INALÁMBRICAS LAN DE DATOS

Cuando anteriormente hemos hablado de las redes inalámbricas, realmente nos hemos estado refiriendo a las redes de área local inalámbricas de datos que son las de nuestro interés, como son: Wi-Fi, Bluetooth, Home RF, etc. Estas siglas, al igual que otras existentes, hacen referencia a distintos tipos de redes o de tecnologías para WLANs. Estas redes están pensadas para crear un entorno de red local entre ordenadores o terminales situados en un mismo edificio o grupo de edificios. **También existen redes inalámbricas de voz, pero éstas no son el objeto de este trabajo de tesis y, salvo mención expresa, siempre nos referiremos a las redes inalámbricas de datos.**

Para saber bien por dónde nos movemos, vamos a parar un momento a diferenciar los distintos tipos de redes LAN inalámbricas que existen.

Según el diseño requerido se tienen distintas tecnologías aplicables:

- **Banda estrecha.** Se transmite y recibe en una específica banda de frecuencia lo más estrecha posible para el paso de información. Los usuarios tienen distintas frecuencias de comunicación de modo que se evitan las interferencias. Así mismo un filtro en el receptor de radio se encarga de dejar pasar únicamente la señal esperada en la frecuencia asignada.

- **Banda ancha.** Es el usado por la mayor parte de los sistemas sin cable. Fue desarrollado por los militares para una comunicación segura, fiable y en misiones críticas. Se consume más ancho de banda pero la señal es más fácil de detectar. El receptor conoce los parámetros de la señal que se ha difundido. En caso de no estar en la correcta frecuencia el receptor, la señal aparece como ruido de fondo.

  Hay dos tipos de tecnología en banda ancha:

  a) **Espectro Expandido por Salto de Frecuencia** (FHSS: Frecuency-Hopping Spread Spectrum): utiliza una portadora de banda estrecha que cambia la frecuencia a un patrón conocido por transmisor y receptor. Convenientemente sincronizado es como tener un único canal lógico. Para un receptor no sincronizado FHSS es como un ruido de impulsos de corta duración.

  b) **Espectro Expandido por Secuencia Directa** (DSSS: Direct-Sequence Spread Spectrum): se genera un bit redundante por cada bit transmitido. Estos bits redundantes son llamados "chipping code". Cuanto mayor sea esta secuencia mayor es la probabilidad de reconstruir los datos originales (también se requiere mayor ancho de banda). Incluso si uno o más bits son perturbados en la transmisión las técnicas implementadas en radio pueden reconstruir los datos originales sin necesidad de retransmitir. Para un receptor cualquiera DSSS es un ruido de baja potencia y es ignorado.

- **Infrarrojos.** No es una técnica muy usada. Se usan frecuencias muy altas para el transporte de datos. Como la luz, los infrarrojos no pueden traspasar objetos opacos. Por lo

que o bien se utiliza una comunicación con línea de visión directa o bien es una difusión. Los Sistemas directos baratos se utilizan en redes personales de área reducida y ocasionalmente en LAN's específicas. No es práctico para redes de usuarios móviles por lo que únicamente se implementa en subredes fijas. Los sistemas de difusión IR no requieren línea de visión pero las células están limitadas a habitaciones individuales.

En cuanto a los estándares WLAN competidores en el mercado mundial existen tres principales que son los que se listan en seguida, se ha creado un poco de confusión e información inexacta en el mercado en cuanto los aspectos relacionados con un estándar WLAN.

- Home RF
- BlueTooth
- WI FI

Una de las razones principales para obtener un estándar es la compatibilidad, esto es, que el equipo que proporcione un proveedor A funcione con el equipo del proveedor B. Otra razón importante para obtener un equipo estandarizado es debido a que proporcionan estabilidad a los diseños de productos básicos y aseguran la interoperabilidad a medida que sus redes crecen y migran.

Wi-Fi

Durante bastantes años, las redes inalámbricas de ordenadores se llevaban a cabo utilizando soluciones particulares de cada fabricante. Estas soluciones, llamadas propietarias, tenían el gran inconveniente de no permitir interconectar equipos de distintos fabricantes. Cada fabricante desarrollaba su propia solución y la comercializaba por su cuenta. Para el cliente, esto suponía tener que trabajar siempre con el mismo fabricante, y, por tanto, estar sometido siempre a las limitadas soluciones que un solo fabricante puede ofrecer.

La única forma de resolver este problema es desarrollar un sistema normalizado que acepten los fabricantes como sistema común. Idealmente, son los organismos internacionales de normalización quienes realizan este trabajo con la ayuda de los propios interesados. No obstante, en muchas ocasiones una de las empresas o asociación de empresas ha sido la que ha logrado imponer su sistema en el increado. Éste es el caso, por ejemplo, del sistema VHS de vídeo o del sistema GSM de comunicaciones móviles.

En 1997 el IEEE añadió un nuevo miembro a la familia 802 que se ocupa de definir las redes de área local inalámbricas. Este nuevo miembro es el 802.11.

La primera norma 802.11 utilizaba infrarrojos como medio de transmisión. Esta norma nunca tuvo una buena aceptación en el mercado. Posteriormente, salieron otras dos normas 802.11 basadas en el uso de radiofrecuencia en la banda de 2,4 GHz. Ambas se diferencian en el método de transmisión de radio utilizado. Una utiliza el sistema FHSS (Frequency Hopping Spread Spectrum, 'Difúsión por Salto de Frecuencia') y la otra, el sistema DSSS (Direct Sequence Spread Spectrum, 'Difúsión por Secuencia Directa').

Más adelante y como consecuencia de la incorporación de las investigaciones de los grupos de trabajo 11b y 11a se ha conseguido mejorar las tasas máximas de transmisión. Más concretamente con 11b se ha podido conseguir 11Mbps en la banda de 2.4Ghz, usando técnicas de espectro ensanchado y secuencia directa, cambiando además la modulación, clave para mayores tasas de transferencia.

Por otra parte el grupo de trabajo 11a, ha conseguido acercar las redes inalámbricas a las cableadas, con una velocidad máxima de 54Mbps. Esta revisión, promovido fuertemente desde empresas estadounidenses en aras de las mejores prestaciones, trae de cabeza a todo aquel que quiera usarlo en Europa o Japón, por el tema de las licencias.

Otros grupos definidos trabajan, entre otras cosas, en:

- Grupo 11c: Añadir soporte MAC en 802.1 para operaciones de puente para el estándar 802.11.

- Grupo 11d: Definir nuevos requerimientos para la capa física, como puede ser canales, secuencias de saltos y otros requerimientos para hacer funcionar 802.11 en otros países, dónde no es posible implementar 802.11, puesto que no tienen 2.4Ghz libre o es más corto. Entre ellos España por tener parte de la banda destinada a usos Militares.

- Grupo 11e: Mejorar el MAC del 802.11 para que pueda manejar de forma adecuada la Calidad de servicio(QoS), poder tener clases de servicio y mejorar los mecanismos de seguridad y autentificación. Mejorar el PCF y DCF de manera que se mejore la eficiencia.

- Grupo 11f: Ayudar la interoperabilidad entre puntos de acceso.

- Grupo 11g: Conseguir mejorar la tasa de transmisión, manejando alrededor de 54 Mbps en la banda de 2.4Ghz, usando otras codificaciones

- Grupo 11h: Mejorar la capa física (PHY) en la banda de 5Ghz para países europeos. Por tema de las licencias es imposible transmitir en esta banda en Europa, de ahí que estas investigaciones se centren en elaborar mecanismos de selección entre interiores y exteriores.

- Grupo 11i: Desarrollar nuevos mecanismos en el nivel MAC para obtener mayores prestaciones en cuanto a seguridad.

En el caso de las redes locales inalámbricas, el sistema que se está imponiendo es el normalizado por IEEE con el nombre 802.11b. A esta norma se la conoce más habitualmente como Wi-Fi o Wireless Fidelity (Fidelidad Inalámbrica).

Con el sistema Wi-Fi se pueden establecer comunicaciones a una velocidad máxima de 11 Mbps, alcanzándose distancias de hasta varios cientos de metros. No obstante, versiones más recientes de esta tecnología permiten alcanzar los 22, 54 y hasta los 100 Mbps.

La tabla 1.1proporciona un resumen de las versiones más comunes de este estándar, así como una descripción breve de cada una de ellas.

Estandar	Frecuencia Portadora	Velocidad de Datos	Resumen
802.11 a	5.1-5.2GHz 5.2-5.3 GHZ 5.7-5.8 GHZ	54 Mbps	La potencia máxima es 40 mW en la banda 5.1, 250 mW en la banda 5.2 y 800 mW en la banda 5.7 (en Estados Unidos)
802.11 b	2.4-2.485 GHz	11 Mbps	Es el estándar que se vende más
802.11 d	NID		Múltiples dominios reguladores
802.11 e	NID	NID	Calidad de servicio QoS
802.11 f	NID		Protocolo de conexión entre puntos de acceso(Inter-Access Point Protocol, IAPP, por sus siglas en inglés)
802.11 g	2.4-2.485 GHz	36 o 54 Mbps	Compatibilidad con 802.11b y 802.11a
802.11 h	NID	NID	Selección dinámica de frecuencia (Dynamic Frequency Selection, DFS, por sus siglas en inglés)
802.11 I	NID	NID	Seguridad

Tabla 1.1 de estándares IEEE

El IEEE adoptó el estándar 802.11 IEEE en 1997 y se convirtió en el primer estándar WLAN. De acuerdo con el IEEE, 802.11 IEEE principalmente controla las Capas 1 y 2 de la pila de referencia OSI, las cuales son la capa física y la capa de enlace de datos (que con frecuencia se conoce como la capa de enlace), respectivamente.

Esto debe permitir y facilitar la interoperabilidad entre fabricantes de dispositivos IEEE802.11 y para asegurarse de ello se ha creado una alianza denominada WECA para crear y definir procedimientos para conseguir certificados de interoperabilidad y de cumplir las especificaciones, todo dentro de un estándar llamado Wi-Fi o también llamado "Wireless Fidelity". El nombre además es un indicativo del enfoque doméstico y muy enfilado hacia el usuario final.

La capa de Control de acceso al medio de 802.11

La capa MAC es un subconjunto de la capa de enlace, que a su vez es adyacente a la capa física en una red basada en IP. La Capa 1 en una red 802.11 realiza por lo menos tres funciones esenciales:

- Funciona como la interfaz entre la capa MAC en dos o más ubicaciones geográficas. Estas ubicaciones normalmente sólo están a pocos cientos de pies o menos de distancia.
- Realizan la detección real de los sucesos CSMA/CA, mismos que ocurren dentro de la capa MAC.
- Efectúan la modulación y demodulación de la señal entre dos puntos geográficos en los que residen equipos 802.11. Este esquema de modulación puede ser DSSS o FHSS.

Más aún, el estándar 802.11 define una *técnica de cambio de velocidad* que permite a las redes reducir las velocidades de datos a medida que ocurren cambios en la distancia, calidad y fuerza de la señal. Las velocidades de datos de 802.11b IEEE pueden ser tan altas como 11 Mbps o tan bajas como 1 Mbps con modulación DSSS, en tanto que las velocidades de datos moduladas con FHSS pueden ser 1 o 2 Mbps. El estándar también permite la compatibilidad entre los radios 802.11a y 802.11b. La parte de una red 802.11a que usa equipos 802.11 b dará como resultado velocidades de datos más lentas que las del estándar más viejo

La capa MAC es una subcapa de la Capa 2 de la pila OSI y controla la conectividad de dos o mas puntos a través de un esquema de direcciones. Cada computadora portátil o punto de acceso tiene una dirección MAC. El estándar 802.11 IEEE define la forma en que funciona esta asignación de direcciones además de la manera en que operan algunos aspectos de la Capa 1. Este estándar es parecido en muchos aspectos al estándar Ethernet que fue establecido por la misma entidad de estándares. De hecho, define lo siguiente:

- Las funciones que se requieren en un dispositivo compatible con 802.11 para operar en una red de igual a igual o integrado en una WLAN existente.
- La operación del dispositivo 802.11 dentro del rango de otros dispositivos 802.11 y la forma en que la tarjeta cliente migraría físicamente de un punto de acceso al otro.
- Servicios de control de acceso y entrega de datos al nivel MAC para las capas superiores de la pila de protocolos de red.
- Varias técnicas de interfaz de señalamiento en la capa física.
- Privacidad y seguridad en los datos del usuario que se transfieren a través del medio inalámbrico.

Lo que hace que una WLAN sea diferente de una LAN Ethernet es, obviamente, la capacidad de los usuarios de trasladarse de un punto de la red a otro y seguir conectados. Ésta es la característica más importante de una WLAN y es la que representa la mayor diferencia con una LAN Ethernet. La forma en la que opera MAC en 802.11 bajo este estándar es lo que permite que los niveles más altos de la pila OSI funcionen normalmente. En otras palabras, la capa MAC es la que controla los aspectos de movilidad de una red 802.11.

Es por esta razón que una capa MAC 802.11 está obligada a hacerse cargo de ciertas funcionalidades que normalmente son responsabilidad de capas más altas de la pila OSI, por ejemplo, la capa de sesión (Capa 5), que controla el inicio y la terminación de sesiones. En el estándar MAC 802.11, el flujo d información se realiza mediante un método del mejor esfuerzo, que también se conoce como *sin conexión.* Los enlaces sin conexión son en los que el extremo receptor del enlace no verifica la recepción de los datos con el enlace transmisor. La técnica que usa la capa MAC se conoce como Accesos múltiples de sensor de portadora con detección de colisiones (Carrier Sense Multiple Access with Collision Detection, CSMA/CD, por sus siglas en inglés) que es una técnica que requiere que el transmisor "escuche" lo que ocurre en el entorno local, para asegurarse de que no existen otras transmisiones en la frecuencia que tiene asignada. La detección real se efectúa en la Capa 1, pero el control del tiempo para las transmisiones se controla en la capa MAC.

CSMA/CD es un protocolo que tiene como propósito resolver los conflictos de transmisión. Como afirmamos, el transmisor determinará si existe una transmisión en la frecuencia asignada de un punto de acceso o adaptador cliente. Cuando una transmisión está en progreso, el punto de

acceso o puente esperará un periodo especifico, después del cual determinará si el canal de radio está desocupado o no. Los radios están programados de manera que es aleatorio el tiempo entre los intentos para determinar si un canal de radio en particular está disponible. Se emplearon algunas estadísticas simples para establecer que la probabilidad más alta de que un canal esté en uso, es justo después de que un intento de transmisión fue detenido debido a que el canal de radio estaba siendo usado por otro transmisor. Es por esta razón que el tiempo entre los intentos para transmitir tiene un ritmo aleatorio. La cantidad de tiempo entre la repetición de intentos con frecuencia se conoce como *tiempo de retroceso.*

Sin embargo, en la mayor parte de los sistemas 802.11 el tiempo de retroceso disminuye de manera uniforme hasta que el transmisor determina que existe un canal abierto. Al hacer que el tiempo disminuya uniformemente con periodos distintos, una WLAN obtiene eficiencia. Es fácil entender que la eficiencia de una red resultará afectada cuando todos los radios en un canal común tengan que esperar un periodo que cada vez es más largo. Al provocar que los radios intenten detectar el canal durante un tiempo que cada vez es más extenso, aunque estén seleccionados en forma aleatoria, los radios que esperan iniciar el tráfico de transmisión tendrán que esperar la menor cantidad de tiempo.

En una arquitectura del mejor esfuerzo, es posible que no exista alguna garantía de que los datos que se envían podrán recibirse de manera exitosa. Algo que hace el sistema 802.11 para ayudar a asegurar la recepción exitosa de información es enviar la información de manera repetida, lo que se conoce como *repiqueteo.*

Otra función que proporciona una capa MAC 802.11 es la de seguridad, la que normalmente se controla en la capa de presentación (Capa 6). La medida de seguridad compatible con este estándar es la Privacidad equivalente al cableado (WEP, por sus siglas en inglés) que es un método para manejar claves y cifrar los datos. Se tratará más a fondo las información acerca de WEP en el capitulo 4.

802.11a Vs. 802.11b

En la actualidad, existen tres tipos de productos RF de velocidad alta que cubren las especificaciones 802.11, de acuerdo con la ratificación del IEEE. Éstos son 802.11b, 802.11a y 802.11g.. En tanto que las especificaciones 802.11a y 802.11b fueron ratificadas por el IEEE el mismo día en septiembre de 1999, la tecnología 802.11g no fue ratificada sino hasta el segundo trimestre de 2003, los productos que usan la tecnología 802.11b aparecieron en el mercado muchos años antes de las especificaciones 802.11a y la 802.11g. La tabla 1.2 ilustra las principales diferencias entre las tres tecnologías.

	802.11 b	802.11 g	80.11 a
Frecuencia	2.4 GHz	2.4GHZ	5.7 GHZ
OFDM	No	Sí	Si
Ninguna línea de transmisión	No	No	No
Velocidades de datos	11 Mbps	54 Mbps	54 Mbps
Número de canales que no se traslapan	3	3	8

Tabla 1.2. Comparación breve entre las especificaciones

HomeRF

En 19911 se creó un grupo de trabajo bajo el nombre HomeRF (*Home Radio Frecuency,* "Radiofrecuencia del Hogar") con el objetivo de desarrollar y promover un sistema de red inalámbrica para el hogar. Aunque el grupo de trabajo lo formaron inicialmente Compaq, HP, IBM, Intel y Microsoft, posteriormente se le han ido uniendo más miembros hasta casi alcanzar los 100 a finales de 2000. Actualmente cuentan con menos miembros debido a la proliferación de otras tecnologías.

A principios de 1999, HomeRF sacó la versión 1.0 de su protocolo SWAP (*Shared Wireless Access Protocol,* "Protocolo de Acceso Compartido Inalámbrico"). La versión 2.0 de este protocolo salió en mayo de 2001.

SWAP trabaja en la banda de frecuencias de 2.4 GHz y permite configuraciones de comunicaciones punto a punto y comunicaciones con punto de comunicación central

La versión 1.0 permite transmitir datos a 1,6Mbps y mantener hasta cuatro comunicaciones dúplex de voz. Tiene un alcance de unos 50m y una potencia de transmisión de 100mW. Utiliza un protocolo similar a 802.1 para datos y otro similar a DECT para voz. L a versión 2.0 alcanza los 10 Mbps y se espera que la versión 3.0 alcance los 40 Mbps para llegar a los 100 Mbps en versiones posteriores.

Por cierto, HomeRF, como Bluetooth, utiliza el sistema FHSS

El estándar HomeRF tiene sus raíces en el Teléfono inalámbrico digital mejorado *(Digital Enhanced Cordless Telephone, DECT* por sus siglas en inglés), y es posible que para bien, debido a que existen más de 200 millones de aparatos telefónicos provenientes de más de 100 fabricantes en todo el mundo que cumplen con este estándar. Esto también explica la razón por la que el estándar HomeRF es el único que hoy día puede transportar el tráfico de voz con la calidad de llamadas telefónicas normales, y de hecho está tomando un camino opuesto al de los estándares 802.11 y BlueTooth, lo que significa ir de voz a datos.

Parece ser obvio que la intención del grupo HomeRF es la de proporcionar un aparato que adapte una base de clientes muy grande de usuarios telefónicos inalámbricos. Al parecer, intentan proporcionar un aparato central que conecte los dispositivos dentro de un hogar al teléfono inalámbrico para permitir las llamadas desde la residencia y hacia ella, y luego proporcionar un ancho de banda alto a la computadora personal al crear una interfaz de conexión de banda ancha dentro del hogar.

Esto se consigue mediante un enfoque parecido al de 802.11, el cual consiste en hacer que las capas MAC y física de la pila OSI cumplan con este estándar. El estándar HomeRF utiliza una combinación de CSMA/CD para los datos en paquetes y TDMA para el tráfico de voz y video, con el fin de optimizar el flujo del tráfico sobre una base de prioridad.

La capa física utiliza la Manipulación por frecuencia *(Frequency Shift Keying, FSK,* por sus siglas en inglés) para proporcionar velocidades en bits variables de entre 800 Kbps y 1.6 Mbps en una banda de 2.4 6Hz. Se hizo un intento de impulsar un segundo estándar HomeRF denominado HomeRF2, que permite velocidades de datos de 5 y 10 Mbps pero, además de Proxim, ninguna otra compañía ha invertido en esta tecnología. En HomeRF la disminución del ancho de banda se efectúa a través del uso de 75 canales de 1 MHz para voz y canales de datos a 1.6 Mbps. El

estándar HomeRF2 usa 15 canales de 5 MHz para canales de datos a 5 y 10 Mbps. La capa física también incluye el salto de frecuencia inteligente para evitar la residencia de transmisiones en canales que están muy congestionados debido a la interferencia.

Los medios más importantes consideran que la prioridad principal es la transmisión y se identifica por los encabezados de la aplicación, mientras que el tráfico de voz y datos hacen un balance del ancho de banda, que también está identificado y se basa en los encabezados de la aplicación. Los medios principales usan buffer de tiempo y físicos para permitir el tráfico de voz y luego el de datos.

Es muy interesante observar que el estándar HomeRF incluye un conjunto impresionante de capacidades de voz, por ejemplo, el identificador de llamadas, llamadas en espera, regreso de llamadas e intercomunicación dentro del hogar. Esto se atribuye directamente a que el origen del estándar se basa en un estándar de voz desarrollado por las compañías telefónicas.

Para la seguridad, HomeRF usa un cifrado de 128 bits aumentado por medio de la mejora en la seguridad original de la modulación FHSS en la capa física. Esta combinación debe proporcionar un nivel alto de resistencia a los ataques de denegación de servicio, a pesar de que nosotros no pudimos determinar si las claves son estáticas o dinámicas.

EL ESTÁNDAR BLUETOOTH

Bluetooth es una de las tecnologías de redes inalámbricas de área personal más conocidas. Al contrario que otras tecnologías como Wi-Fi, la tecnología Bluetooth no está pensada para soportar redes de ordenadores, sino, más bien, para comunicar un ordenador o cualquier otro dispositivo con sus periféricos: un teléfono móvil con su auricular, un PDA con su ordenador, un ordenador con su impresora, etc.

Aunque BlueTooth en realidad es un estándar WLAN, existe una confusión considerable en cuanto al hecho de que compite o no directamente con 802.11 y HomeRF o con ambos. En resumen, BlueTooth no compite directamente con 802.11 y compite sólo de una manera superficial con HomeRF La principal razón de esto es que BlueTooth tiene como propósito ser un estándar con un rango nominal de aproximadamente 1 a 3 metros. Su intención es conectar computadoras portátiles con teléfonos celulares, PDA con computadoras portátiles y teléfonos celulares, además de otros dispositivos similares. La segunda razón es que está relativamente limitado en la velocidad con aproximadamente 1.5 Mbps lo que es aproximadamente una décima parte de la velocidad del estándar 802.11b, y sólo una pequeña fracción de la velocidad que ofrecerán los estándares 802.11 a y 802.11 g.

Bluetooth fue desarrollado en 1994 por la empresa sueca Ericsson con el objetivo de conseguir un sistema de comunicación de los teléfonos móviles con sus accesorios (auriculares, ordenadores, etc.). En 1998 se creó el Grupo de Interés Especial Bluetooth, *(Bluetooth Special Interest Group,* SIG), *www.bluetooth.com,* formado por la propia Ericsson, IBM, Intel, Nokia y Toshiba. Esto le dio un gran empuje comercial a esta tecnología.

Bluetooth es un estándar que describe como se pueden interconectar dispositivos, que no necesitan de visión directa entre ellos, utilizando una conexión inalámbrica de corto alcance.

El nombre de este estándar viene del apodo que se le daba a Harald II, un rey vikingo. Debido a la enfermedad que tenía este hombre, los dientes se le ponían de color azul y comenzaron a llamarle Bluetooth (diente-azul). Este rey lo que hizo fue unificar bajo su reinado a numerosos reinos pequeños que funcionan con normas distintas, que es más o menos lo que hace Bluetooth: intenta que comunicar diferentes unidades donde cada una es independiente de la otra.

Las primeras versiones de la especificación BlueTooth se emitieron a principios de 1999 y se esperaba que la versión 2 fuera lanzada en 2002. Este lapso entre la publicación original de la especificación y la segunda versión puede acarrear problemas al estándar, en especial debido a que BlueTooth 1 ha estado expuesto a una considerable cobertura por parte de los medios, mismo que fue publicado a mediados de los noventa. En otras palabras, la versión 1 necesitó aproximadamente cuatro años para que se publicara la especificación, por lo que un retraso excesivo en la publicación de BlueTooth 2 podría debilitar la base de apoyo, debido a que el grupo de apoyo de ingenieros y compañías puede dedicarse a otros estándares que están más próximos a su publicación o ya están en el mercado. En la actualidad, existen cerca de 2 500 miembros de BlueTooth listados en el Grupo de interés especial.

No obstante que en realidad se acerca a la tendencia de los dispositivos que realmente son de banda ancha, de acuerdo con su página web principal, la velocidad de datos máxima es de 1 Mbps y se aclara que es una velocidad de datos aproximada. Se debe esperar que la capacidad de salida real esté alrededor de 750 Kbps, dependiendo de la carga que se use para la administración de la seguridad y el salto de frecuencia.

Las comunicaciones de Bluetooth se llevan a cabo mediante el modelo maestro/esclavo. Un terminal maestro puede comunicarse hasta con siete esclavos simultáneamente. No obstante, el maestro siempre puede suspender las comunicaciones con un esclavo (mediante una técnica conocida como *parking)* y activar la comunicación con un nuevo dispositivo esclavo. Con este sistema un maestro puede establecer comunicación con un máximo de 256 esclavos, donde sólo siete comunicaciones pueden permanecer activas simultáneamente. A este conjunto de relaciones maestro/esclavo se le llama *piconet.* En este entorno un dispositivo puede ser a la vez maestro de un *piconet* y esclavo de otro *piconet.* Cuando ocurre esto, al conjunto resultante se le conoce como *scatternet* (red dispersa).

El estándar BlueTooth tiene dos puntos fuertes:

- **Tamaño** El factor de la forma (tamaño) que ofrece BlueTooth le permite conectarse en relojes de mano, PDA y otros dispositivos electrónicos pequeños en los que el tamaño es un criterio de diseño importante.

- **Ahorro de energía** BlueTooth usa 30 microamperes, lo que es una cantidad muy pequeña de energía. Usa una fracción de la energía que emplea un reloj de mano normal y utiliza órdenes de magnitudes más bajas que las que usan los teléfonos celulares. Esta característica también juega un buen papel en la industria, la cual con frecuencia crea dispositivos, como auriculares inalámbricos, basándose en la cantidad de energía que se requiere de una batería para proporcionar un ciclo de trabajo significativo (periodo de operación continua).

En términos de seguridad, BlueTooth cuenta con un método de cifrado, pero no se especifica en la página web. Se debe mencionar que un esquema de saltos FHSS de 1 600 saltos por segundo,

además de un rango muy limitado, de 1 a 3 metros, ocasionará que sea muy difícil interferir la comunicación a distancia.

Si existe algún aspecto negativo en el estándar BlueTooth, es que ha sido fuente de una cantidad enorme de discusión. El Grupo de interés especial de BlueTooth predijo a mediados de los noventa que habría cerca de 200 millones de PC con dispositivos BlueTooth integrados en su fabricación original alrededor del año 2000. Resulta ser que los fabricantes de PC están adoptando conexiones de velocidades que exceden mucho a las que puede proporcionar BlueTooth, además de que los rangos de transmisión y recepción rebasan por mucho los ofrecimientos de BlueTooth. Ésta es la razón por la que la mayoría de los fabricantes de computadoras portátiles hoy día proporcionan productos que integran una opción 802.11.

Para ser justos con los patrocinadores de BlueTooth, algunos productos basados en BlueTooth se encuentran en la actualidad en el mercado, principalmente en el área de la conexión de teléfonos celulares con PDA, teclados y mouse con PC, cámaras con PC y conexiones similares.

Promix, a través de su constelación de compañías colaboradoras, estableció el estándar HomeRF y seleccionó al mercado residencial como su objetivo principal, en tanto que el estándar 802.11 ha optado por los mercados SMB, empresariales y SOHO. IBM, mediante el mercado BlueTooth, ha perseguido esencialmente el mercado comercial/ventas. HomeRF ha ofrecido productos en el mercado con precios tan bajos como 80 dólares en Buy.com, mientras que el equipo 802.11 se vendió y en la actualidad funciona en más de 60 países en todo el mundo con precios que fluctúan entre 79 y 300 dólares (precios de lista) por una tarjeta PCMCIA, hasta 150 a 1 000 dólares por un punto de acceso.

Esta diferencia enorme en el precio generalmente refleja la orientación a los mercados; en otras palabras, el equipo de costo muy bajo por lo común incluye características de seguridad mínimas, desempeño bajo y niveles muy inferiores de interoperabilidad y se avocan al despliegue donde no se requiere que el radio opere como un elemento de red sofisticado, como es el caso de las empresas comerciales, mercados financieros y otros negocios.

Es posible que BlueTooth haya tenido la cobertura más grande por parte de la prensa pero es, por mucho, el que menor número de dispositivos tiene en el mercado y casi siempre está integrado dentro de otro dispositivo, como un PDA o teléfono celular. El precio propuesto durante mucho tiempo para los circuitos integrados de BlueTooth es de 20 dólares para los fabricantes que ofrecen sus productos a los consumidores.

Tanto HomeRF como BlueTooth son estándares que se conocen como *cerrados.* Esto significa que las compañías que proporcionan soporte para el estándar están encerradas en torno a las compañías de desarrollo principales. En el caso de HomeRF, la compañía más importante es Proxim, en tanto que IBM es el patrocinador principal de BlueTooth. Las constelaciones de empresas alrededor de estas compañías incluyen canales distribuidores, mismos que representan grupos que venden los productos que usan estos estándares, además de Silicon y otros proveedores electrónicos más pequeños.

Bluetooth utiliza la técnica FHSS *(Frequency Hopping Spread Spectrum,* "Espectro Expandido por Salto de Frecuencia") en la banda de frecuencias de 2,4 GHz. Puede establecer comunicaciones asimétricas donde la velocidad máxima en una dirección es de 721 Kbps y 57,6 Kbps en la otra o comunicaciones simétricas de 432,6 Kbps en ambas direcciones. Por otro lado, puede transmitir tanto voz como datos.

Actualmente se está definiendo la versión 2.0 de Bluetooth. Esta versión seguirá trabajando en alcances de 10 metros y se espera que llegue a velocidades de transmisión de hasta 12 Mbps.

A pesar de la aparente complementariedad de bluetooth con Wi-Fi, lo cierto es que esta última tecnología está evolucionando mucho más rápidamente que la primera. Teniendo en cuenta que Wi-Fi tiene un ancho de banda mucho mayor que Bluetooth, que goza de un alcance bastante mayor y que poco a poco está consiguiendo equipararse en precios, existe una cierta incertidumbre en cuanto al futuro de Bluetooth.

RESUMEN DE LOS TRES ESTÁNDARES COMPETIDORES

Los tres estándares WLAN competidores están representados en el resumen de la tabla siguiente.

	Home RF	BlueTooth	802.11b
Capa física	FHSS	FHSS	FHSS, DSSS, IR
Saltos de frecuencia	50 saltos por segundo	1,600 saltos por seg	2.5 saltos por segundo
Potencia de transmisión Máxima	100 mW	100 mW	800 mW
Velocidades de datos	1 o 2 Mbps	1 Mbps	11Mbps
Número máximo de dispositivos	Hasta 127	Hasta 26	Hasta 256
Seguridad	150 pies	0, 40 y 64 bits	40 y 28 bits RC4 JKIP MIC, SSN
Rango	V1.0	30 pies	400 pies en exteriores, 1000 pies
Versión actual	Ni más ni menos	V1.0	V1.0
Costo	costoso	Menos costoso	Más costoso
Tamaño físico	Ni mayor ni menor	El más pequeño	El más grande
Alcance exterior al hogar	No	No	Sí

Tabla 1..3 Estándares competidores RF para interiores

A continuación tenemos algunas notas que se relacionan con la tabla:

- RC4 de 40 y 128 bits no se consideran algoritmos de seguridad de datos extensos.
- El rango de 1 000 pies de 802.11 se refiere a condiciones externas y tiene más posibilidades de ser una indicación del estándar 802.11 b. Las condiciones internas son

más difíciles para este tipo de sistemas RE Mediante el uso de un puente 802.11 podrán alcanzarse distancias mucho más grandes que cuando se emplea un punto de acceso.

- La potencia de salida de 802.11 en 800 mW es sustancial.
- El número máximo de dispositivos que se pueden soportar depende de la velocidad de datos por dispositivo.

En la actualidad, BlueTooth está restringido de manera estricta por la FCC en cuanto a la potencia debido a las pérdidas excesivas en las máscaras del espectro. El rango óptimo para la versión revisada se estima que será de 300 pies aproximadamente 5 metros.

Es importante observar que sólo uno de los tres estándares soporta lo que en realidad se puede llamar banda ancha, y ése es el estándar 802.11. Se hace esta afirmación debido a que el estándar 802.11 rebasa, por mucho, el desempeño de los otros dos. Los estándares 802.11 futuros aumentarán aún más la diferencia en el desempeño al ofrecer 54 Mbps en los equipos 802.11g y 802.11a.

Existen otras dos diferencias importantes entre los estándares:

- Rango
- Velocidad de adopción en el mercado

En resumen, los estándares 802.11 a y 802.11g prometen 54 Mbps de velocidad y gozan del apoyo casi unánime de todos los proveedores WLAN principales y de menor importancia. Estos estándares emergentes se crearán sobre la base de un mercado impulsado, en este momento, por las ventas mundiales de 802.11b que rebasan los 100 mil millones de dólares. Se piensa que el estándar HomeRF seguirá el camino de Betamax como competidor de 802.11. Bluetooth no compite con 802.11 debido a que tiene como objetivo un tipo de conectividad diferente, que se podría resumir como "red de área personal", lo cual en general está limitado a un rango de aproximadamente 5 metros con velocidades de datos lentas. Por tanto, se convertirá en un estándar auxiliar de 802.11a/b/g debido a que proporcionará conectividad entre los usuarios y sus dispositivos, en tanto que los estándares 802.11 conectarán a los dispositivos con las redes.

Como hemos visto anteriormente, existen muchas tecnologías distintas de comunicaciones inalámbricas. Muchas de estas tecnologías son complementarias, pero otras dan respuesta a una misma necesidad y, por tanto, compiten entre ellas por ser las preferidas del mercado. En el caso de las tecnologías de redes de área local inalámbricas, la competencia se centra en Wi-Fi, HiperLAN, HomeRF y las nuevas versiones tecnológicas de cada una de ellas.

Para que una tecnología esté lista para ser adoptada por el mercado, es necesario que tenga suficientemente desarrolladas estas cinco características:

- Normalización
- Regulación
- Tecnología

- Servicios
- Precios

En el caso de las redes locales inalámbricas, la tecnología que tiene mejor posicionamiento en estos cinco puntos es Wi-Fi. Sobre todo, tiene el mejor posicionamiento en el apartado precios, lo cual está resultando determinante para que el mercado acepte esta tecnología frente a sus competidores.

Claro que el mercado de las comunicaciones inalámbricas de datos se acaba de despertar ahora, por lo que Wi-Fi sólo lleva ganada la primera batalla de lo que, seguro, será una dura guerra.

CAPÍTULO 2

ARQUITECTURA Y FUNCIONAMIENTO DE IEEE 802.11

Ciertamente, se puede construir una red Wi-Fi sin saber cómo funciona; no obstante, si se comprende su funcionamiento, se estará en una mejor disposición para entender qué está pasando cuando algo no va como se espera. Por otro lado, también ayuda a entender mejor las características de los distintos equipos Wi-Fi y cuáles son las posibilidades reales.

En este capitulo vamos a describir los principios generales en los que se basa el funcionamiento del estándar IEEE 802.11. Como ya sabemos, esta familia de estándares tiene miembros diversos con diferencias tecnológicas. Por ello, vamos a empezar por presentar a la familia para luego centramos en su funcionamiento interno.

Wi-Fi hace referencia al estándar IEEE 802.11b. Las redes inalámbricas Wi-Fi que se instalan hoy en día son de este tipo por lo que, aunque muchos de los principios de funcionamiento que vamos a describir aquí son válidos para distintos miembros de la familia IEEE 802.11.

IEEE 802.11

Como mencionamos antes en este capítulo, el estándar 802.11 IEEE debe ser observado con un grado adicional de detalle debido a que el estándar general 802.11 tiene un conjunto de variantes y, quizá más importante, porque es el estándar que ha capturado la atención de los proveedores principales de esta tecnología y disfruta por un amplio margen la mayor parte del mercado.

IEEE802.11 es un estándar para redes inalámbricas definido por la organización Institute of Electrical and Electronics Engineers (IEEE), instituto de investigación y desarrollo, de gran reconocimiento y prestigio, cuyos miembros pertenecen a decenas de países entre profesores y profesionales de las nuevas tecnologías.

El estándar IEEE802.11 es un estándar en continua evolución, debido a que existen cantidad de grupos de investigación, trabajando en paralelo para mejorar el estándar, a partir de las especificaciones originales.

La primera versión del estándar fue definida en 1997. Aunque el comité evaluador fue creado en 1990, muestra del gran desarrollo que ha sido la primera versión. Esta versión trata de ofrecer varias formas para poder interconectar computadores y otros dispositivos sin la necesidad de cables. Esta primera versión, visto hoy está obsoleta, pero ha marcado un principio para una tecnología prometedora.

Se nos ofrece tres alternativas en cuanto a tecnología subyacente para poder realizar nuestra red. Ofrece entre otras cosas tres capas físicas, por la cual enviaríamos los datos, infrarrojos (IR), por la banda ISM 2.4Ghz con técnicas de espectro ensanchado, ya sea con salto en frecuencias FHSS como por secuencia directa DSSS. Más adelante mostraremos las diferencias de una y de otra. Con el estándar original se consiguen velocidades hasta un máximo de 2Mbps tanto por radiofrecuencia como por infrarrojos.

El mayor inconveniente de los sistemas inalámbricos definidos originalmente por 802.11 es que trabajaban a velocidades de 1 y 2 Mbps. Esto, unido al alto coste inicial de los equipos, hizo que la tecnología inalámbrica no se desarrollase hasta 1999. En ese año aparecieron semiconductores de tecnología de radio de 2,4 GHz mucho más baratos (principalmente liderados por empresas como Lucent y Harris).

Por otro lado, aparecieron tres nuevas versiones de la norma 802.11:

- **IEEE 802.11 b,** que subía la velocidad de transmisión a los 11 Mbps. Por este motivo se la conoció también como 802.11 HR *(High Rate,* 'Alta Velocidad').

- **IEEE 802.11 a.** Esta norma se diferencia de 802.11b en el hecho de que no utiliza la banda de los 2,4 GHz, sino la de los 5 GHz y que utiliza una técnica de transmisión conocida como OFDM *(Orthogonal Frequency Division Multiplexing,* 'Multiplexación Ortogonal por División de Frecuencia'). La gran ventaja es que se consiguen velocidades de 54 Mbps; llegándose a alcanzar los 72 y 108 Mbps con versiones propietarias de esta tecnología (p.e. Netgear). El mayor inconveniente es que la tecnología de semiconductores para 5 GHz no esta suficientemente desarrollada todavía.

- **IEEE 802.11 g**. Esta norma surgió en el año 2001 con la idea de aumentar la velocidad sin renunciar a las ventajas de la banda de los 2,4 Ghz. Esta norma permite transmitir datos a 54 Mbps. En cualquier caso, existen versiones propietarias de esta tecnología que llega a los 100 Mbps.

Las Mejoras

En el interés de disponer de unos estándares inalámbricos lo antes posible, al desarrollar sus normas, el IEEE no se paró a considerar determinadas características (como la calidad de servicio, seguridad, utilización del espectro, etc.) que hubiesen producido un estándar más robusto. Para resolver este problema, el IEEE ha creado posteriormente unos grupos de trabajo para desarrollar estándares que resuelvan estos problemas y que puedan ser añadidos fácilmente al protocolo principal.

Estos grupos son los siguientes:

- **IEEE 802.11 e (Calidad de servicio)**. Este grupo trabaja en los aspectos relacionados con la calidad de servicio (QoS o *Quality of Services,* en inglés). En el mundo de las redes de datos, calidad de servicio significa poder dar más prioridad de transmisión a unos paquetes de datos que a otros, dependiendo de la naturaleza de la información (voz, vídeo, imágenes, etc.). Por ejemplo, la información de voz necesita ser transmitida en tiempo real, mientras que la información de datos originada por una transferencia de archivo da igual que llegue medio segundo antes o después.

- **IEEE 80211 h (Gestión del espectro)**. Este grupo de trabajo pretende conseguir una mejora de la norma 802.11a en cuanto a la gestión del espectro radioeléctrico. Este punto es una de las desventajas que tiene IEEE 802.11 a frente a su competidor europeo HiperLAN/2 (que también opera en la banda de 5GHz).

- **IEEE 802.11 i (Seguridad)**. El sistema de seguridad que utiliza 802.11 esta basado en el sistema WEP. Este sistema ha sido fuertemente criticado debido a su debilidad. Este grupo de trabajo pretende sacar un nuevo sistema mucho más seguro que sustituya a WEP. El sistema sobre el que se está trabajando se conoce como TKIP *(Temporal Key Inlegrity Protocol,* 'Protocolo de Integridad de Clave Temporal').

ESTANDAR	GRUPOS DE TRABAJO	ESTADO
802.11 (1997)	Especificaciones de la capa física y MAC de las redes de área local inalámbricas infrarrojo radio 2,4 GHz	Completo
802.11a (1999)	Especificaciones de la capa física y MAC de las redes de área local inalámbricas radio 5GHz	Completo
802.11 b (1999)	Especificaciones de la capa física y MAC de las redes de área local inalámbricas de rango de velocidad de 5,5 a 11 Mbps radio 2,4 GHz	Completo
802.11 c	Pasarela MAC entre redes	Completo
802.11 e	Calidad de servicio para aplicaciones avanzadas (voz, vídeo, etc.)	Activo
802.11 f (2000)	Interoperatividad entre puntos de acceso de distintos fabricates (Interaccess Point Protocol, IAPP	Activo
802.11 g (2002)	Especificaciones para redes inalámbricas de alta velocidad 54 Mb s en la banda de 2,4 GHz	Activo
802.11 h	Mejoras para la selección dinámica de canal y control de potencia de transmisión	Activo
802.11 i	Mejoras para seguridad autentificación	Activo
5GSG	Globalización de los 5 GHz Grupo de estudio junto con ETSI/BRAN (European Telecommunications Standards institute(Broadband Radio Area Network, 'Instituto Europeo de Normalización en Telecomunicaciones/Redes Vía Radio de Banda Ancha') y MMAC (Mobile Multimedia Access Communication, 'Comunicaciones Multimedia de Acceso Móvil') de Japón para promover la interoperatividad entre 802.11a, ETSI Hiper LAN/2 MMAC	Activo

Tabla 2.1. Grupos de trabajo y de estudio relacionados con IEEE 802.11

Hay cantidad de grupos de trabajo, hoy día trabajando en paralelo, con el objetivo común de mejorar el estándar en diversos aspectos. De ahí que se puede concluir que se trate de una especificación en continua evolución con posibilidad de adaptarse a nuevos requerimientos y demandas de usuario en un futuro.

Como ya se ha explicado, el estándar permite el uso de varios medios y técnicas para establecer conexiones. El estándar original permite usar infrarrojos, espectro expandido tanto en salto en frecuencias como secuencia directa. Todo ello con la ventaja de usar una capa de acceso al medio (MAC) común. Ello da mucha flexibilidad a los desarrolladores e investigadores, que pueden olvidarse de ciertos aspectos ya que no existe dependencia directa entre ellos.

Existe multitud de aspectos técnicos, en la que se nos sería imposible de citar y tratar todas, de forma que se ha optado por incluir las más importantes de cara a la comprensión de la tecnología y para poder encarar más tarde la comparativa final entre las distintas tecnologías.

Los estándares de IEEE802.11 son de libre distribución y cualquier persona puede ir a la página Web del IEEE y descargarlos. Estos estándares sólo definen especificaciones para las capas físicas y de acceso al medio y para nada tratan modos o tecnologías a usar para la implementación final

TECNOLOGÍA Wi-FI.

El problema principal que pretende resolver la normalización es la compatibilidad. No obstante, como hemos visto, existen distintos estándares que definen distintos tipos de redes inalámbricas. Esta variedad produce confusión en el mercado y descoordinación en los fabricantes. Para resolver este problema, los principales vendedores de soluciones inalámbricas (3Com, Aironet, Intersil, Lucent Technologies, Nokia y Symbol Technologies) crearon en 1999 una asociación conocida como WECA (Wireless Ethernet Compability Alliance, 'Alianza de Compatibilidad Ethernet Inalámbrica'). El objetivo de esta asociación fue crear una marca que permitiese fomentar más fácilmente la tecnología inalámbrica y asegurase la compatibilidad de equipos.

De esta forma, desde abril de 2000, WECA certifica la interoperatividad de equipos según la norma IEFE 802.11b bajo la marca Wi-Fi *(Wireless Fidelity,* 'Fidelidad Inalámbrica'). Esto quiere decir que el usuario tiene la garantía de que todos los equipos que tengan el sello Wi-Fi pueden trabajar juntos sin problemas independientemente del fabricante de cada uno de ellos. Se puede conseguir un listado completo de equipos que tienen la certificación Wi-Fi en www.*wirelessethernet.org*

Como la norma 802.11b ofrece una velocidad máxima de transferencia de 11 Mbps y ya existen estándares que permiten velocidades superiores, WECA no se ha querido quedar atrás. Por este motivo, WECA anunció que empezaría a certificar también los equipos IEEE 802.11a de la banda de 5 GHz mediante la marca Wi-Fi5 y 802.11g de la banda 2.4GHz estos dos con velocidad de datos máxima de 54 Mbps.

ARQUITECTURA DEL PROTOCOLO IEEE 802.11

Qué es un Protocolo

Cuando una persona pretende comunicarse con otra, lo primero que hace es llamar su atención ("disculpe", "oye, Paco", etc.); luego, comprueba que la otra persona le atiende, para, a continuación, transmitirle la información que desea. Durante la comunicación, lo normal es que la persona que habla se asegure de que la que escucha está entendiendo lo que le dice. Para ello, espera recibir gestos de asentimiento o palabras de asimilación. Si el que habla no recibe estos mensajes, interpretará que lo que dice no es entendido y lo volverá a repetir. Finalmente, mediante mensajes preestablecidos, se da por concluida la comunicación("adiós", "hasta luego", etc.).

Pues bien, la transmisión de datos entre ordenadores también requiere llevar a cabo estos mismos procedimientos. En cualquier comunicación, bien sea entre personas o entre máquinas, siempre hacen falta una serie de normas que regulen dicho proceso. En el caso de las comunicaciones entre personas, las normas las establece la sociedad y son aplicadas por cada persona de acuerdo con la educación que haya recibido; en el caso de las máquinas, las normas las establecen los organismos de normalización (IEEE, ETSI, UIT, etc.) y son aplicadas por los ordenadores de acuerdo con el protocolo o conjunto de protocolos que se está utilizando.

Obviamente, aunque existen grandes similitudes de procedimientos, la diferencia fundamental entre personas y máquinas es que las personas están dotadas de inteligencia y pueden adaptarse fácilmente a situaciones imprevistas, además de tener inventiva y capacidad de resolver situaciones nuevas. Los ordenadores, sin embargo, deben tener protocolos muy estrictos, que tengan previstos todos los posibles casos que se puedan presentar en una comunicación, sin dejar nada al azar.

En definitiva, un protocolo no es más que un conjunto de reglas que emplean dos equipos informáticos para dialogar entre sí, de forma que puedan establecer y mantener una comunicación sin errores.

Para que los protocolos puedan llevar a cabo sus objetivos, necesitan añadir ciertos datos de control a la información original a transmitir. Estos datos adicionales son incluidos por el terminal emisor y suprimidos por el terminal receptor antes de entregar la información al destino.

En un principio, cada fabricante establecía los procedimientos de comunicación de sus propios equipos, siendo casi imposible conectar equipos de fabricantes distintos. Con la expansión de la informática, se hizo evidente que era necesario disponer de protocolos normalizados que permitiesen la interconexión de equipos independientemente de quién los fabricase. Con esta idea, a lo largo de los años han ido apareciendo distintos protocolos normalizados, cada uno de ellos dedicados a distintas aplicaciones o cubriendo distintas necesidades. Muchos de estos protocolos normalizados han surgido a partir de los protocolos desarrollados por empresas u organismos concretos (caso de TCP/IP para interconexión de redes Internet), mientras que otros han sido desarrollados por los organismos de normalización (Wi-Fi).

De forma práctica, los protocolos de comunicación son unos programas que se instalan tanto en el terminal origen, como en el destino de la comunicación. Parte de estos programas residen en el propio *hardware* del equipo, otra parte puede venir incorporada en el sistema operativo y la restante debe ser instalada por el usuario en el momento de configurar el equipo.

El modelo OSI

Una característica común a todas las comunicaciones actuales de ordenadores es el hecho de que todas ellas estructuran el proceso de comunicación en distintos niveles o capas. Cada capa se encarga de realizar una tarea distinta y perfectamente coordinada con el resto de capas. Por ejemplo, hay capas que se encargan de poner en contacto dos terminales (nivel de enlace), otras se encargan de detectar posibles bloqueos o fallos en la línea (nivel de transporte) y otras, de identificar al terminal llamante, pedir las claves de acceso, etc. (nivel de sesión).

La ventaja de hacer una división por capas es que cada una de ellas puede ser normalizada de forma independiente. No obstante, finalmente, la comunicación se lleva a cabo gracias al buen funcionamiento de todas las capas.

La Organización Internacional de Normalización, ISO *(International Standards Organization)*, propuso un modelo de referencia que permitiese estructurar las comunicaciones en siete capas. A este modelo lo llamó OSI *(Open Systems Interconnection,* 'Interconexión de Sistemas Abiertos').

Las capas del modelo OSI son las siguientes:

1. **Capa física.** Esta capa define las propiedades físicas de los componentes (frecuencias de radio utilizadas, cómo se transmiten las señales, etc.).

2. **Capa de enlace.** Esta capa define cómo se organizan los datos que se transmiten, cómo se forman los grupos de datos (paquetes, tramas, etc.) y cómo se asegura que los datos llegan al destino sin errores.

3. **Capa de red.** Esta capa define cómo organizar las cosas para que distintas comunicaciones puedan hacer uso de una infraestructura común, una red. Por ejemplo, aquí están definidos cómo se identifican los terminales (numeración) o cómo se enrutan los datos.

4. **Capa de transporte.** Esta capa define las características de la entrega de los datos.

5. **Capa de sesión.** Aquí se describe cómo se agrupan los datos relacionados con una misma función.

6. **Capa de presentación.** Nos define cómo es representada la información transmitida.

7. **Capa de aplicación.** Define cómo interactúan los datos con las aplicaciones específicas.

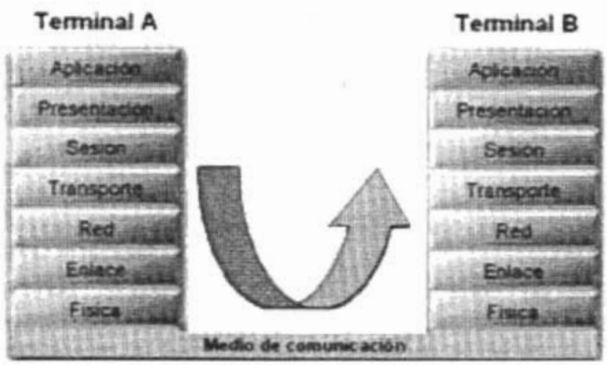


Fig.2.1 Esquema de comunicación del modelo OSI

Los modelos como OSI pretenden definir todos y cada uno de los factores que intervienen en una comunicación de una red abierta; sin embargo, no todas las comunicaciones de datos son iguales; por ejemplo, existen comunicaciones en las que no hace falta definir una determinada capa (por ejemplo, en las comunicaciones directas entre dos ordenadores no es necesario que exista un nivel de red). En cualquier caso, de todos los procedimientos definidos por OSI, los que siempre están presentes en cualquier tipo de comunicación son aquellos que están incluidos dentro de las capas física y de enlace.

Como funciona IEEE 802.11

Una red Wi-Fi puede estar formada por dos ordenadores o por miles de ellos. Para que un ordenador pueda comunicarse de forma inalámbrica, necesita que se le instale un adaptador de red.

Un **adaptador de** red es un equipo de radio (con transmisor, receptor y antena) que puede ser insertado o conectado a un ordenador, PDA o cualquier otro equipo susceptible de formar parte de la red (impresoras, etc.).

De forma general, a los equipos que forman parte de una red inalámbrica se les conoce como **terminales.**

Aparte de los adaptadores de red, las redes Wi-Fi pueden disponer también de unos equipos que reciben el nombre de puntos de acceso (AP o *Access Points,* en inglés). Un punto de acceso es como una estación base utilizada para gestionar las comunicaciones entre los distintos terminales. Los puntos de acceso funcionan de forma autónoma, sin necesidad de ser conectados directamente a ningún ordenador.

Tanto a los terminales como a los puntos de acceso se les conoce por el nombre general de estación.

Las estaciones se comunican entre sí gracias a que utilizan la misma banda de frecuencias y a que internamente tienen instalados el mismo conjunto de protocolos. Aunque los protocolos que utiliza Wi-Fi están basados en las siete capas del modelo de referencia OSI, el estándar IEEE 802.1 l sólo define las dos primeras capas (física y enlace); el resto de las capas son idénticas a las empleadas en las redes locales cableadas e Internet y se conoce con el nombre de conjuntos de protocolos IP *(Internet Protocol* o 'Protocolo Internet').

MODELO OSI			PROTOCOLOS
7	Aplicación		HTTP , FTP,SMTP
6	Presentación		
5	Sesión	IP	DNS,LDAP
4	Transporte		UDP, TCP
3	Red		ICPM, RSVP
2	Enlace	IEEE 802	LLC,MAC
1	Fisico		Fisico

Tabla2. 2 Relación de los protocolos de red local

Los diferentes estándar, incluido IEEE 802.11, permiten que aparezcan nuevas versiones de ese mismo estándar simplemente modificando una de las capas. Esto facilita no sólo la evolución de los estándares, sino que un mismo equipo pueda ser compatible con distintas versiones de un estándar. Por ejemplo, IEEE 802.1lb sólo se diferencia de IEEL 802.11 en que su capa física permite transmitir datos a alta velocidad.

Capas de IEEE 802

La norma IEEE 802 define exclusivamente los temas relacionados con las dos primeras capas del sistema OSI: las capas física y la de enlace. De hecho, a la capa de enlace la divide en dos, por lo que el resultado son tres capas:

- **PHY** *(Physical Layer,* 'Capa Física') es la capa que se ocupa de definir los métodos por los que se difunde la señal.
- **MAC** *(Medium Access Control,* 'Control de Acceso al Medio') es la capa que se ocupa del

control de acceso al medio físico. En el caso de Wi-Fi el medio físico es el espectro radioeléctrico. La capa MAC es un conjunto de protocolos que controlan cómo los distintos dispositivos comparten el uso de este espectro radioeléctrico.

- **LLC** *(Logical Link Control)* es la capa que se ocupa del control del enlace lógico. Define cómo pueden acceder múltiples usuarios a la capa MAC.

LAS CAPAS DE IEEE802.11

La Capa Física

Como hemos visto, la capa física se ocupa de definir los métodos por los que se difunde la señal. Para hacer esto, la capa física de IEEE 802.11 se divide en dos subcapas: lo que se conoce como PLCP *(Physical Layer Convergence Procedure,* 'Procedimiento de Convergencia de la Capa Física') y PMD *(Physical Medium Dependent,* 'Dependiente del Medio Físico'). PLCP se encarga de convertir los datos a un formato compatible con el medio físico. Por ejemplo, este formato es distinto si se trata de un medio físico de infrarrojos o de radio, mientras que PMD es el que se encarga de la difusión de la señal.

Por cierto, aunque las especificaciones originales de IEEE 802.11 contemplan la opción de utilizar infrarrojos como medio de transmisión, no obstante, nunca ha llegado a desarrollarse este sistema debido principalmente al corto alcance que ofrece y a que no es utilizable en el exterior debido a las interferencias producidas por agentes naturales como la lluvia o la niebla.

Espectro expandido DSSS y FHSS

En cuanto a la utilización del medio radioeléctrico, la tecnología básica en la que se basa el funcionamiento de los sistemas inalámbricas es el sistema conocido como espectro expandido *(spread spectrum* en inglés). Este sistema consiste en que el ancho de banda real utilizado en la transmisión es superior al estrictamente necesario para la transmisión de la información. Lo que se consigue con esto es un sistema muy resistente a las interferencias de otras fuentes de radio, resistente a los efectos de eco *(muitipath)* y que puede coexistir con otros sistemas de radiofrecuencia sin verse afectado y sin influir en su actividad Estas ventajas hacen que la tecnología de espectro expandido sea la más adecuada en las bandas de frecuencia para las que no se necesita licencia.

IEEE 802.11 contempla sólo dos técnicas distintas de espectro expandido para la capa física:

- FHSS *(Frecuency Hopping Spread Spectrum,* 'Espectro Expandido por salto de frecuencia', con la que se consiguen velocidades de transmisión de 1 Mbps.

- DSSS *(Direct Sequence Spread Spectrum,* 'Espectro Expandido por Secuencia Directa'), con la que se consiguen velocidades de transmisión de 2 Mbps. En versiones posteriores de este sistema se han conseguido velocidades superiores.

Dependiendo de la velocidad a la que se van a transmitir los datos, la norma IEEE 802.11. utiliza una técnica u otra.

En 1999 el IEEE sacó una nueva versión de DSSS que permite transmitir datos a 11 Mbps. Esta nueva DSSS está recogida en la norma IEEE 802.11b. Por esta razón, al 802.11b también se le conoce como 802.11 DSSSo 802.11 HR *(High Rate,* 'Alta Velocidad').

A pesar de esto, en la práctica, la velocidad de 11 Mbps no es totalmente real debido a distintas razones:

- Las interferencias y ruidos hacen que la velocidad real baje
- El propio protocolo consigue menos rendimiento que en sistemas cableados
- Las conexiones a los puntos de acceso son un cuello de botella

MODELO OSI	MODELO 802.11	TÉCNICAS DE DIFUSIÓN DE 802.11				
Capa de enlace	LLC					
	MAC					
Capa física	PLCP	DSSS 802.11	FHSS 802.11	Infrarrojos 802.11	DSSS-HR 802.11b	OFMD 802.11a
	PMD					

Tabla 2 .3 Capas física y de enlace del estándar IEEE 802.11

Estos estándares pueden conseguirse en *http://standards.ieee.org*

Además de las técnicas de difusión comentadas anteriormente, con la nueva versión IEEE 802.11 a salió una nueva técnica conocida como OFDM *(Orthogonal Frequency Division Multiplexing,* 'Multipiexación Ortogonal por División de Frecuencias') con la que se consigue velocidades de transmisión de hasta 54 y 100 Mbp, aunque OFMD es una técnica para propagar la señal a través de un ancho de banda determinado, no es, por definición, una técnica de espectro extendido, 802.11a y g usan OFMD como su técnica de propagación.

FHSS

La técnica FHSS *(Frequency Hopping Spread Specfrum,* 'Espectro Expandido por Salto de Frecuencia') consiste en dividir la banda de frecuencias en una serie de canales e ir transmitiendo la información saltando de un canal a otro de acuerdo con un patrón de saltos *(spreading code* o *hopping code)* conocido tanto por el emisor como por el receptor. El tiempo máximo que se debe permanecer en cada frecuencia está regulado en 400 mseg.

El inconveniente de FHSS es que tiene la necesidad de sincronizar el emisor y el receptor en la frecuencia a utilizar en cada momento. Este problema fue resuelto por los ingenieros de Sylvania Electronic Systems a finales de los años cincuenta.

El estándar IEEE 802.11 definió en 1997 que cada canal de FHSS tuviera un ancho de banda de 1 MHz dentro de la banda de frecuencias de 2,4 GHz. El ancho de banda total disponible y, por

tanto, el número total de canales disponibles varia de acuerdo con el marco regulatorio de cada país o área geográfica. En cualquier caso, siempre existen tres juegos de secuencias de saltos.

La técnica FHSS reduce las interferencias porque, en el peor de los casos, la interferencia afectará exclusivamente a uno de los saltos de frecuencia, liberándose a continuación de la interferencia al saltar a otra frecuencia distinta. El resultado es que el número de bits erróneos es extremadamente bajo.

Otra de las ventajas de FHSS es que permite que coexistan varias comunicaciones en la misma banda de frecuencias. Para ello, cada comunicación debe tener un patrón de saltos con distinta secuencia.

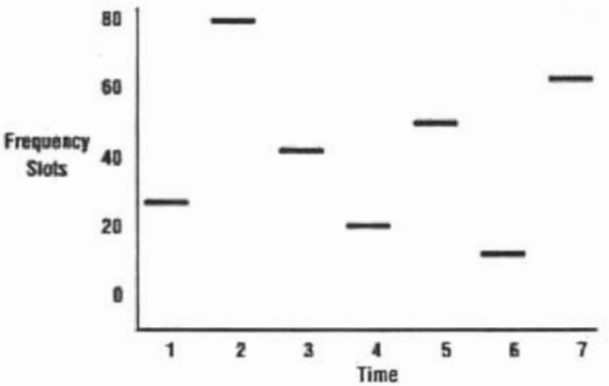


Fig. 2. 2 sistema FHSS

A pesar de que el estándar original IEEE 802.11 incluía el sistema FHSS, no existe ninguna instalación real que utilice este sistema. La razón es que la velocidad máxima que se consigue con la tecnica FHSS es de unos 3 Mbps (aunque sólo está normalizada la velocidad de lMbps). No obstante, es posible que en un futuro se consigan velocidades superiores. Se habla de hasta 15 Mbps.

DSSS

La técnica DSSS se basa en sustituir cada bit de información por una secuencia de bits conocida como *chip* o código de *chips (chipping code,* en inglés). Estos códigos de chips permiten a los receptores eliminar por filtrado las señales que no utilizan la misma secuencia de bits. Entre las señales que son eliminadas se encuentra el ruido y las interferencias.

El código de *chips* permite al receptor identificar los datos como pertenecientes a un emisor determinado. El emisor genera el código de *chips* y, sólo los receptores que conocen dicho código pueden descifrar los datos. Por tanto, en teoría, DSSS permite que varios sistemas puedan funcionar en paralelo; cada receptor filtrará exclusivamente los datos que se corresponden con su código de *chi4>s.* Por otro lado, cuanto más largo es el código de *chips,* más resistente será el sistema a las interferencias y mayor número de sistemas podrán coexistir simultáneamente. La norma IEEE 802.11 recoge que la longitud mínima del código de *chips* debe ser de 11.

En la práctica, la coexistencia de sistemas no se consigue por el uso de distintos códigos de *chips*, sino por el uso de distintas bandas de frecuencias. Un sistema DSSS de 11 Mbps (IEEE 802.11 b) necesita un ancho de banda de 22 MHz, siendo la distancia mínima entre portadoras de 30 MHz. Como el ancho de banda disponible en la banda de2,4 GHz (en el área regulada por el FCC) es de *83,5* MHz, sólo es posible la coexistencia de tres sistemas DSSS en el mismo lugar.

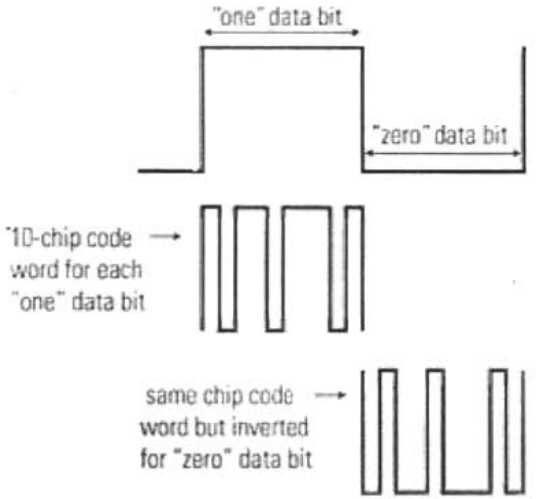


Fig. 2. .3 Principios del sistema DSSS

OFDM

OFDM *(Orihogonal Frequency Division Multiplexing,* 'Multiplexación Ortogonal por División de Frecuencias') es la técnica de gestión de frecuencias utilizada por IEEE 802.11a y 802.11g. Esta técnica divide el ancho de banda en suhcanales más pequeños que operan en paralelo. De esta forma se consigue llegar a velocidades de transmisión de hasta 54 Mbps (100 Mbps con soluciones propietarias).

La técnica OFDM fue patentada por Bell Labs en 1970 y está basada en un proceso matemático llamado FFT *(Fast Fourier Trans}o¡in,* 'Transformada Rápida de Fourier'). OFDM divide la frecuencia portadora en 52 subportadoras solapadas. 48 de estas subportadoras son utilizadas para transmitir datos y las otras cuatro para poder alinear las frecuencias en el receptor. Este sistema consigue un uso muy eficiente del espectro radioeléctrico.

OFDM puede transmitir datos a distintas velocidades, utilizando distintas técnicas de modulación en cada una de ellas. Las velocidades normalizadas que admite OFDM son 6, 9, 12, 18, 24, 36, 48 y 54 Mbps.

Una de las ventajas de OFDM es que consigue una alta resistencia a las interferencias producidas por las ondas reflejadas en los objetos del entorno (eco o *multipath).* Estas ondas llegan al receptor con distinta amplitud y a distinto tiempo que la señal principal produciendo interferencias. Estas interferencias son un problema a velocidades superiores a 4 Mbps; por este motivo, se utilizan técnicas (como OFDM) que mitiguen este efecto.

VELOCIDAD	TÉCNICAS DE MODULACIÓN	BITS POR SEÑAL
6Mbps	BPSK	1
9Mbs	BPSK	1
12Mbps	QPSK	2
18Mb s	QPSK	2
24 Mbps	QAM-16 (BPSK	4
36Mbps	QAM-16 BPSK)	4
48Mb s	QAM-64 QPSK	6
54 Mbps	QAM-64 (QPSK)	6

Tabla 2 .4 Técnicas de modulación utilizadas por IEEE 802 11a

Modulación de la señal

Para poder transmitir la señal vía radio, hace falta definir un método de difusión de la señal y un método de modulación de la señal. La modulación consiste en modificar una señal pura de radio para incorporarle la información a transmitir. La señal base a modular recibe el nombre de portadora *(carrier* en inglés). Lo que se le cambia a la portadora para modularía es su amplitud, frecuencia, fase o una combinación de éstas. Mientras mayor es la velocidad de transmisión, mas complejo es el sistema de modulación.

Las técnicas de modulación utilizadas en IEEE 802.11 son las siguientes:

- BPSK *(Binary Phase-Shift Keying,* 'Modulación Binaria por Salto de Fase')
- QPSK *(Quadrature Phase-Shifi Keying,* 'Modulación por Salto de Fase en Cuadratura')
- GFSP *(Gaussian Frecuency-Shifi Keying,* 'Modulación Gausiana por Salto de Frecuencia')
- CCK *(Comp/ementary Code Keying,* 'Modulación de Código Complementario')

Una vez emitida la señal modulada, el receptor tiene que recibir la señal, sincronizar el código de difusión y demodular la información. Los sistemas FHSS son más complicados de sincronizar que los sistemas DSSS. En el primer caso hay que sincronizar tiempo y frecuencia y en el segundo, sólo el tiempo.

CAPA MAC. EL CONTROL DE ACCESO AL MEDIO

La capa MAC define los procedimientos que hacen posible que los distintos dispositivos compartan el uso de este espectro radioeléctrico. Mientras que las distintas versiones del estándar 802.11 utilizan distintos sistemas para difundir su señal (su capa física es distinta), la capa MAC es la misma para todas ellas.

Es interesante también el hecho de que la capa MAC sea muy similar a la utilizada por la red Ethernet. Ambas utilizan la técnica conocida como CSMA *(Carrier Sense Multiple Aceess,* 'Acceso Múltiple por Detección de Portadora'). No obstante, la versión cableada (Ethernet) utiliza la tecnología CD *(Collision Detection,* 'Detección de Colisión'), mientras que la versión inalámbrica utiliza la tecnología CA *(Collision Avoidance,* 'Evitación de Colisión'). Una colisión se produce cuando dos terminales intentan hacer uso del medio físico simultáneamente. La tecnología CD detecta que se ha producido una colisión y retransmite los datos, mientras que la tecnología CA dispone de procedimientos para evitar que se produzcan colisiones.

La razón de que haya dos sistemas es que, cuando el medio es un cable, un terminal puede transmitir y recibir al mismo tiempo, por lo qué puede detectar las colisiones. Por el contrario, en el medio radioeléctrico un terminal no puede transmitir y recibir al mismo tiempo por el mismo canal (la transmisión dejaría opaca a la recepción), por lo que, al no poder detectar las posibles colisiones, no hay mas remedio que disponer de una técnica que las evite.

Evitar las colisiones

Entre la capa MAC y la capa física se intercambian tres tipos de paquetes de datos: de control, de gestión y de información.

MAC tiene dos funciones distintas para coordinar la transferencia de datos:

- **PCF** *(Point Coordination Function,* 'Función de Coordinación del Punto') facilita un sistema para poder transmitir el tráfico que es sensible a los retardos y que requiere un tratamiento especial evitando las demoras. A la estación que hace uso de esta función se le llama coordinador del punto, PC *(Point Coordinator).* El PC emite una señal guía con la duración del periodo de tiempo que necesita disponer del medio. Las estaciones que reciben esta señal no emiten durante ese tiempo.

- **DCF** *(Distributed Coordination Function,* 'Función de Coordinación Distribuida') facilita un sistema que permite compartir el medio físico (radioeléctrico, infrarrojos, etc.) entre todas las estaciones de la red. Para ello, DCF define los mecanismos que le permiten a las estaciones negociar el acceso al medio físico, así como los mecanismos que aseguran la entrega de los datos a las estaciones. A través de DCF se transmiten los datos que no son sensibles a los retardos.

La función DCF se encuentra con un problema y es que una de las diferencias de los medios cableados frente a los inalámbricos es que en estos últimos es mucho más complicado detectar las

colisiones. Dos estaciones que no se ven entre sí pueden iniciar una comunicación simultáneamente sin percatarse de la colisión. DFC dispone de una función para impedir la colisión que evita este problema.

Los mecanismos CSMA/CA de detección de la colisión consisten en comprobar si el medio está en uso antes de empezar a transmitir. Sí el medio está en uso, se espera un tiempo antes de volver a hacer la comprobación. El tiempo que espera cada estación tiene una duración aleatoria (generada por cada estación entre un tiempo mínimo y un máximo) para evitar que haya colisiones sucesivas indefinidas.

La función DCF contempla un mecanismo físico y otro lógico de detección de colisión. Al mecanismo físico se le conoce como CCA *(Clear Channel Assessment,* 'Valoración de la Disponibilidad del Canal'). Por ejemplo, cuando hablamos de un medio radioeléctrico, este mecanismo puede consistir en comprobar si en el medio existe cualquier señal DSSS o cualquier otra señal con un nivel de energía superior a un umbral.

El mecanismo físico de detección de colisión es muy eficiente, pero no es eficaz cuando dos estaciones de una misma red que no se ven entre ellas emiten al mismo tiempo. Esto se conoce con el nombre de problema del nodo oculto. Para evitar estos casos, se dispone del sistema lógico de detección de colisión. Este sistema consiste en intercambiar la información del uso del medio a través de tramas de control. A estas tramas de control se las conoce corno RTS *(Request to Send),* Solicitud para Enviar') y CTS *(Clear to Send'* Listo para Enviar'). Como esta información de control añade mas datos de control a la transmisión en detrimento de los datos de información (baja el rendimiento del protocolo), en aquellos casos en los que se disponga de un medio tisico con poca probabilidad de colisiones se puede deshabilitar el mecanismo de detección de colisión, o habilitarlo exclusivamente para aquellos paquetes de datos que tengan un tamaño superior a uno determinado.

Cuando una estación de una red va a transmitir información, primero envía una trama RTS al punto de acceso donde facilita información del destinatario de la transmisión, el remitente y el tiempo que ocupará dicha transmisión. El punto de acceso responde con una trama CTS que reciben todas las estaciones que están en el área de cobertura del punto de acceso. En esta trama CTS se incluye el tiempo de ocupación del medio; por tanto, las estaciones saben el tiempo que estará ocupado el medio y no intentarán hacer ninguna transmisión hasta que dicho tiempo no haya pasado

Por cierto, cuando el destinatario ha recibido toda la información, emite una trama *ACK (Acknowledgment,* 'Cocimiento') para indicarle al emisor que todo está bien. Si el emisor no recibe la trama ACK que espera, aguardará un tiempo antes de dar la transmisión por errónea y volver a hacer el envió.

Trama de IEEE8O2.11

Las tramas MAC contienen los siguientes componentes básicos.

- una cabecera MAC, que comprende campos de control, duración, direccionamiento y control de secuencia.

- un cuerpo de trama de longitud variable, que contiene información específica del tipo de trama
- un secuencia checksum (FCS) que contiene un código de redundancia CRC de 32 bits.

Las tramas MAC se pueden clasificar según tres tipos;

1) Tramas de datos.
2) Tramas de control. Los ejemplos de tramas de este tipo son los reconocimientos o ACKs, las tramas para multiacceso RTS y CTS, y las tramas libres de contienda.
3) Tramas de gestión. Como ejemplo podemos citar los diferentes servicios de distribución, como el servicio de Asociación, las tramas de Beacon o portadora y las tramas TIM o de tráfico pendiente en el punto de acceso.

La trama, por otra parte, es muy parecida a las demás de la familia IEEE8O2, siendo de 48bits de longitud y con muchos campos comunes a la trama de Ethemet. A continuación se muestra un ejemplo:

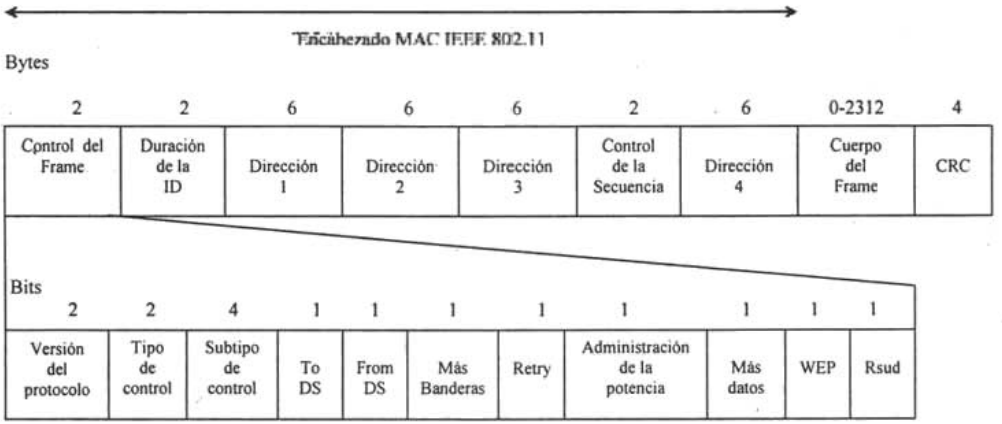


Fig. 2.4 Trama MAC IEEE 802.11

Los campos que componen esta trama son:

- Campo de control. Merece examinar aparte. Lo haremos más abajo.
- Duration/ID. En tramas del tipo PS o Power-Save para dispositivos con limitaciones de potencia, contiene el identificador o AID de estación. En el resto, se utiliza para indicar la duración del periodo que se ha reservado una estación.
- Campos address14. Contiene direcciones de 48 bits donde se incluirán las direcciones de la

estación que transmite, la que recibe, el punto de acceso origen y el punto de acceso destino.

- Campo de control de secuencia. Contiene tanto el número de secuencia como el número de fragmento en la trama que se está enviando.
- Cuerpo de la trama. Varia según el tipo de trama que se quiere enviar.
- FCS. Contiene el checksum.

Los campos de control de trama tienen el formato siguiente:

- Versión.
- Type/Subtype. Mientras el campo tipo identifica si la trama es de datos, control o gestión. el campo subtipo nos identifica cada uno de los tipos de tramas de cada uno de estos tipos.
- ToDS/FromDS. Identifica si la trama se envía o se recibe al/del sistema de distribución. En redes ad-hoc, tanto ToDS como FromDS están a cero. El caso más complejo contempla el envio entre dos estaciones a través del sistema de distribución Para ello situamos a uno tanto ToDS como FromDS
- Más fragmentos. Se activa si se usa fragmentación
- Retry Se activa si la trama es una retransmisión
- Power Management Se activa si la estación utiliza el modo de economía de potencia.
- More Data. Se activa si la estación tiene tramas pendientes en un punto de acceso.
- WEP. Se activa si se usa el mecanismo de autenticación y encriptado.
- Order. Se utiliza con el servicio de ordenamiento estricto, en el cual no nos detendremos.

Se puede ver lo mucho que se parece a una trama Ethemet con algunas excepciones, por ejemplo, como incorporar 4 campos de direcciones. Esto se hace para facilitar el tráfico desde y hacia nodos al otro lado de los puntos de acceso. Además se incorpora muchos mecanismos de control para ahorro de energía, seguridad, etc.

ARQUITECTURA DE IEEE 802.11

La topología de una red es la arquitectura de la red, la estructura jerárquica que hace posible la interconexión de los equipos. IEEE 802.11 y, por tanto, Wi-Fi, contempla tres arquitecturas distintas:

- IBSS *(Independent Basic Service Set,* 'Conjunto de Servicios Básicos Independientes')
- **BSS** *(Basic Service Set,* 'Conjunto de Servicios Básicos')
- ESS *(Extended Service Set,* 'Conjunto de Servicios Extendido')

Componentes de la arquitectura IEEE 802.11

IEEE establece que la arquitectura de IEEE 802.11 consiste en varios componentes que actúan recíprocamente para proporcionar una red inalámbrica LAN que apoya la movilidad de la estación transparentemente a las capas superiores.

A continuación se explican las diferentes arquitecturas basadas en la norma IEEE Wireless LAN Edition.

El BSS independiente (IBSS)

El IBSS(conjunto de servicios básicos Independientes) es el tipo más básico de IEEE 802.11 LAN. Una red IEEE802.11 LAN mínimo sólo puede consistir de dos estaciones(STA). Figura 1 muestra un IBSS. Este modo de funcionamiento de IEEE 802.11 es posible cuando las estaciones pueden comunicar directamente y no existen ninguna estación que coordine el enlace.

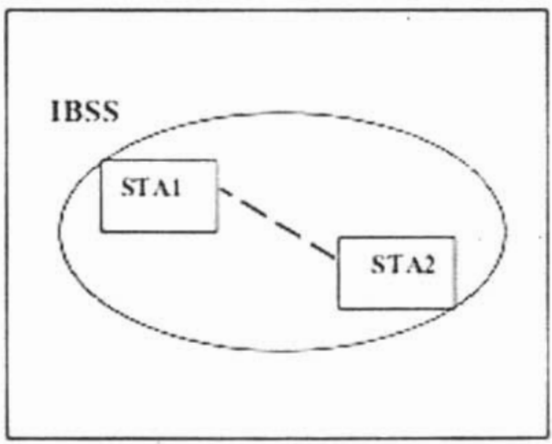


Fig2. 5 IBSS

El BSS

Conjunto básico de servicio (BSS) es la forma principal de un IEEE 802.11 LAN. La figura 2..6 muestra dos BSSs cada uno de los cuales tienen dos estaciones(STA) que son miembros del BSS.

Es útil pensar en los óvalos usados para representar un BSS, en cuanto las estaciones miembro permanezcan dentro del área del fondo del BSS pueden permanecer en comunicación. (El concepto de área, mientras que no es preciso, es a menudo bastante bueno.)

Si una estación se va de su BSS, esta no puede comunicarse más directamente con otros miembros del BSS.

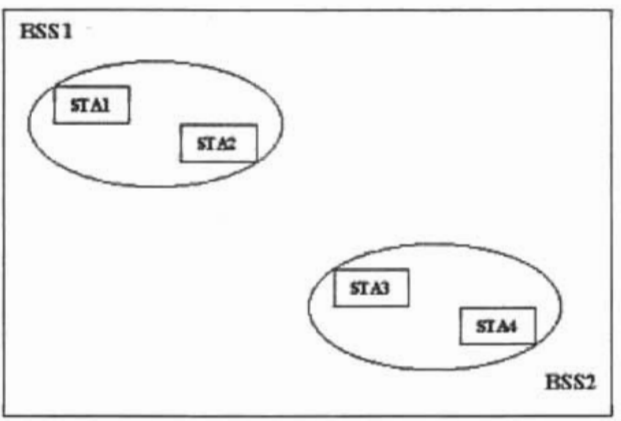


Figura 2 .6 BSSs

La asociación entre un STA(estaciones) y un BSS es dinámica (STAs enciende, apaga, dentro del rango, y sale de rango). Para volverse un miembro de una infraestructura BSS, una estación se volverá asociada. Estas asociaciones son dinámicas e involucran el uso del servicio del sistema de distribución (DSS) que se describe mas adelante.

Los conceptos del sistema de distribución (DS)

Las limitaciones de la capa física determinan la distancia directa de estación-a-estación que puede ser soportada. Para algunas redes esta distancia es suficiente; para otras redes, se requiere aumentar el alcance.

En lugar de existir independientemente, un BSS puede formar también un componente de una forma extendida de red que se construye con múltiples BSSs. Los BSSs son conectados por una capa de distribución de red o DS.

Cada BSS está conformado por estaciones móviles o estaciones que se encuentran controlados por una Función Coordinada Distribuida (DFC) que determina que nodo tiene derecho a transmitir o recibir información en el medio inalámbrico de radio de propagación.

Un punto de acceso (AP) es un STA que proporciona el acceso al DS proporcionando los servicios de DS además de actuar como un STA.

La Figure 2.7 agrega los DS y componentes de AP al cuadro de la arquitectura. IEEE 802.11

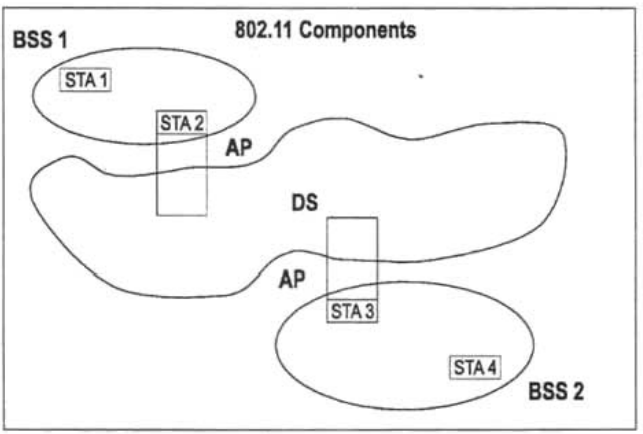


Figura 2. 7.DSs y APs

Los datos se mueven entre un BSS y el DS vía un AP, es decir, las estaciones den un BSS obtienen acceso a la capa DS y por lo tanto a otros nodos inalámbricos fuera de su área de cobertura a través de un AP, así ellos son las entidades del direccionamiento.

Conjunto de Servicio Extendido (ESS): La Red de Mayor Alcance

El DS y BSSs le permiten a IEEE 802.11 crear una red inalámbrica de tamaño arbitrario y complejo. IEEE 802.11 se refieren a este tipo de red como la red de ESS.

El conjunto de servicio extendido ESS permite crear una red inalámbrica formada por más de un punto de acceso AP o así logrando así una mayor área de cobertura.

La STA1 y la STA4 se pueden conectar a través de ESS que cubre los BSS1 y BSS2.

La comunicación entre las estaciones que componen un BSS se realiza mediante la Función Coordinada Distribuida DFC involucrando la capa MAC y la capa Física. El mensaje original de STA1 pasa por AP1 a través de STA2 mediante los Servicios del Sistema de Distribución DSS y de ahí al DS en donde se realiza el enrutamiento óptimo de la dirección de STA4 este se hace a través del AP2 y de STA3 en el BSS2.

En la Fig.2.8 las estaciones dentro de un ESS pueden comunicar y las estaciones móviles se pueden mover de un BSS a otro (dentro del mismo ESS) transparentemente a DS.

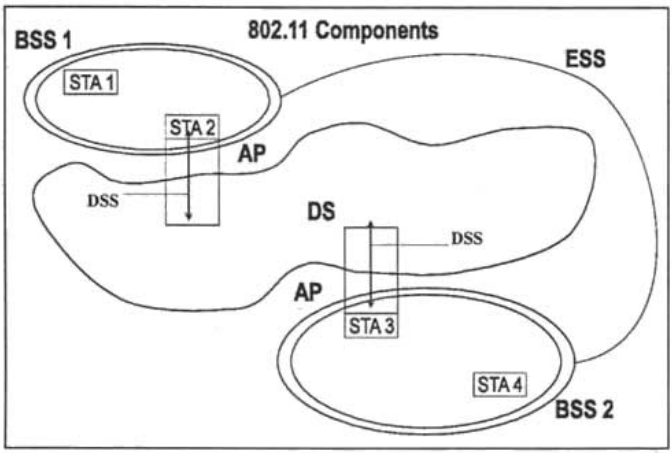


Fig. 2 .8ESS

Integración con LANs alámbricas

Para integrar la arquitectura de IEEE 802.11 con un alambrado tradicional LAN, al final es introducido en la arquitectura un componente lógico – un portal

Por ejemplo, un portal se muestra en Figura 2.9 que conecta a un IEEE alambrado 802 LAN.

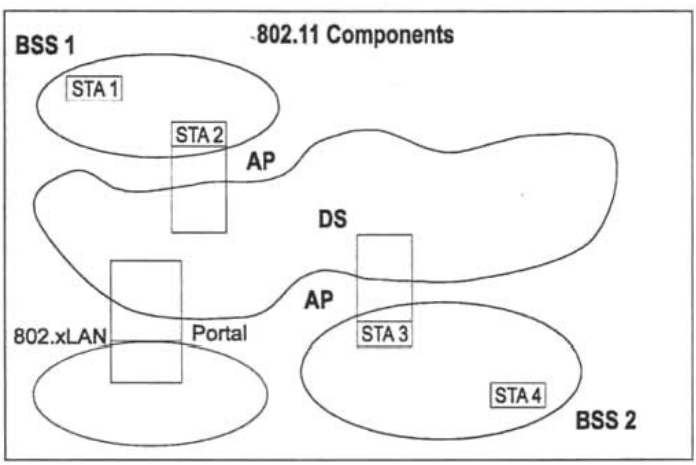


Figure 2.9Conexión de una LAN inalámbrica con IEEE 802 LANs

Todos los datos de la IEEE 802.LANs entran en la arquitectura IEEE 802.11 vía un portal. El portal proporciona la integración lógica entre la arquitectura IEEE 802.11 y el LANs alambrado. Es posible para un dispositivo ofrecer ambas funciones de un AP y un portal; éste podría ser el caso cuando un DS es aplicado en componentes IEEE 802 LAN.

En IEEE 802.11, la arquitectura ESS (APs y el DS) proporciona segmentación de tráfico y extensión del rango. Las conexiones lógicas entre IEEE 802.11 y otro LANs son vía el portal. Los portales se conectan entre el DSM y el medio LAN que serán integrados.

Los Servicios

La arquitectura IEEE 802.11 permite la posibilidad que el DS no puede ser idéntico a un existiendo alambrados LAN. Un DS puede crearse de muchas tecnologías diferentes incluso la actual IEEE802 LANs. IEEE 802.11 no obliga al DS para ser el enlace de los datos o la capa de la red.. IEEE 802.11 no especifica los detalles de aplicaciones de DS explícitamente. En cambio, IEEE 802.11 especifica los *servicios*. Los servicios son asociados con los componentes diferentes de la arquitectura. Hay dos categorías de servicios IEEE 802.11. el servicio de estación (SS) y el DS. Ambas categorías de servicio son usadas por la subcapa 802.11 MAC.

El conjunto completo de servicios para la arquitectura IEEE802.11 son como sigue:

a) Autentificación

b) Asociación

c) Desautentificación

d) Desasociación

e) Distribución

f) Integración

g) Privacidad

h) Reasociación

i) entrega de MSDU

Este conjunto de servicios es dividido en dos grupos: aquellos que son parte de cada STA, y aquellos que son parte de un DS.

SS (servicio de estación)

El servicio proporcionado por las estaciones es conocido como el SS. El SS está presente en cada estación IEEE 802.11(incluyendo APs, cuando los Aps incluyen la función de la estación). El SS se especifica para el uso de las entidades de las capas MAC.

El SS de la capa MAC es como sigue:

a) Autenticación

b) Desautentificación

c) Privacidad

d) entrega de MSDU

DSS

El servicio proporcionado por el DS(sistema de distribución) es conocido como el DSS. Estos servicios se representan en la arquitectura de IEEE 802.11 por las flechas dentro de los APs, indicando que los servicios de limites lógicos se usan para cruzar medios y espacios de dirección. La incorporación física de varios servicios puede o no estar dentro de un AP físico.

Los DSSs son proporcionados por el DS. Ellos son accedidos vía un STA que también proporciona DSSs. Un STA que está proporcionando el acceso a DSS es un AP.

Los DSSs son como sigue:

a) Asociación

b) Desasociación

b) Distribución

d) Integración

e) Reasociación

EL DSSs es especificado para el uso por las entidades de subcapas MAC.

La figura 2.10 muestra la arquitectura completa de IEEE 802.11 combinando los componentes de las figuras anteriores con ambos tipos de servicios.

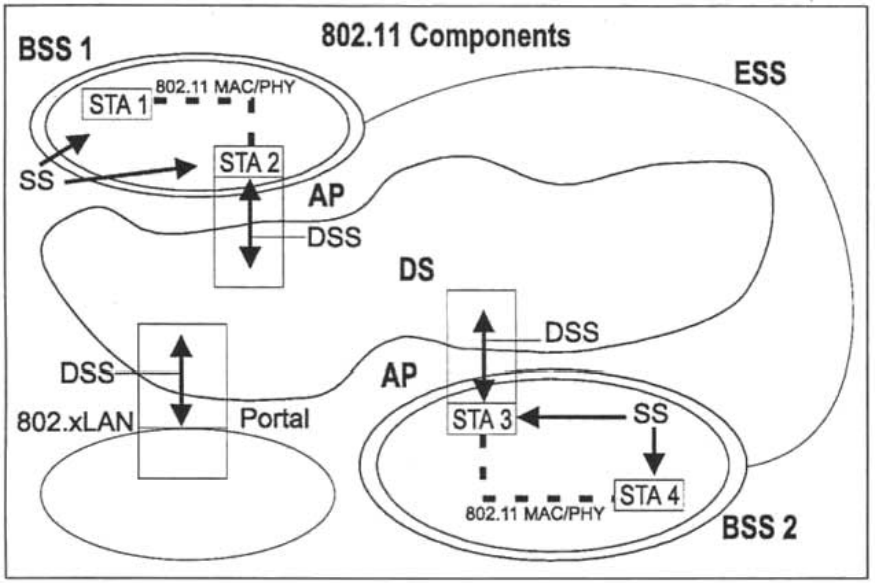


Figure 2. 10.arquitectura completa de IEEE 802.11
IEEE Wireless LAN Edition

APRECIACIÓN GLOBAL DE LOS SERVICIOS

Hay nueve servicios especificados por IEEE 802.11. Se usan seis de los servicios para apoyar la entrega de MSDU entre STAs. Se usan tres de los servicios para controlar en IEEE 802.11LAN el acceso y confidencialidad.

Distribución del mensajes dentro de un DS

Distribución

Éste es el servicio primario usado por las STAs de IEEE 802.11. Se invoca conceptualmente por cada mensaje de los datos a una STA IEEE 802.11 que operan en un ESS (cuando el frame se envía por el DS). La distribución es vía un DSS.

Refiérase a la red ESS en Figura 6 y considere un mensaje de datos enviándose de STA 1 a STA 4. STA1 envía el mensaje y es recibido por STA 2 (la entrada AP). El AP da el mensaje al servicio de distribución de el DS. El trabajo del servicio de distribución es entregar el mensaje dentro del DS de tal manera que este llegue al destino DS apropiado para el destinatario

intencional. En este ejemplo, el mensaje se distribuye a STA 3 (la salida AP) y STA 3 acceda al WM para enviar el mensaje a STA 4 (el destino intencional).

Cómo el mensaje es distribuido dentro del DS no se especifica por IEEE 802.11. Todo el IEEE 802.11 se requiere hacer es proporcionar al DS con bastante información para el DS para poder determinar el punto de salida que corresponde al destinatario deseado. La información necesaria se proporciona al DS por las tres asociaciones de servicio (la asociación, reasociación, y disociación).

El ejemplo anterior era un caso en que el AP que invocó el servicio de la distribución era diferente del AP que recibió el mensaje distribuido. Si el mensaje se hubiera pensado para una estación que era un miembro del mismo BSS como la estación enviante, entonces la entrada y salida APs para el mensaje habría sido el mismo.

Entonces, cuando se transfiere datos de un terminal a otro que pertenecen a diferentes puntos de acceso, el servicio.de distribución se asegura de que los datos alcancen su destino.

Integración

Si el servicio de distribución determina que el destinatario intencional de un mensaje es un miembro integrado de un LAN alámbrica, el punto de salida del DS sería un portal en lugar de un AP.

Los Mensajes que son distribuidos a un portal causa el DS invocan a la función de la Integración (conceptualmente después del servicio de la distribución). La función Integración es responsable de ejecutar todo lo que se necesite entregar de un cierto mensaje DSM al medio integrado LAN(incluyendo cualquier medio requerido o dirección de espacio de retransmisión). La integración es vía un DSS.

Los mensajes que se recibieron de un LAN (vía un portal) por el DS para una STA IEEE 802.11 invocarán la función de la Integración antes que el mensaje sea distribuido por el servicio de distribución.

Entonces, el servicio de integración facilita la transferencia de datos entre la red inalámbrica IEEE802.11 y cualquier otra red (por ejemplo, Internet o Ethernet).

Servicios que apoyan al servicio de distribución

La información requerida por el servicio de distribución para operar es proporcionada por los servicios de la asociación. Antes de que de un mensaje del datos pueda ocuparse por el servicio de distribución, un STA será asociado. Para entender el concepto de asociación, es primero necesario entender el concepto de movilidad.

Tipos de movilidad

Los tres tipos de transición de importancia a esta norma que describen la movilidad de estaciones dentro de una red es como sigue:

a) No-transición: En este tipo, se identifican dos subclases que son normalmente indistinguibles:

   1) static-no movimiento

   2) local movement - movimiento dentro del rango PHY de comunicación del STAs [es decir, movimiento dentro de una área de servicio básico (BSS)].

b) BSS-transición: Este tipo se define como un movimiento de la estación de un BSS a otro BSS dentro del mismo ESS.

c) ESS-transición: Este tipo se define como el movimiento de la estación de un BSS en un ESS a un BSS en un ESS diferente. Este caso sólo se apoya en el sentido que el STA puede mover. El mantenimiento de conexiones de las capas superiores no puede garantizarse por IEEE 802.11; de hecho, la ruptura de servicio es probable que ocurra.

Asociación

Para entregar un mensaje dentro de un DS, el servicio de la distribución necesita saber a qué AP accesó para una determinada STA IEEE 802.11. Esta información se proporciona al DS por el concepto de asociación. La asociación es necesaria, pero no suficiente, para apoyar la movilidad de la BSS-transición.La asociación es suficiente para mantener la movilidad de no-transición. La asociación es un DSS.

Antes de que un STA se permita enviar un mensaje del datos vía un AP, se asociará primero con el AP. El acto de volverse asociado invoca el servicio de la asociación que proporciona la STA a AP que traza al DS. El DS aprovecha esta información para lograr su servicio de distribución de mensaje. Cómo la información prevista por el servicio de asociación se guarda y maneja dentro del DS no es especificada por esta norma.

En cualquier momento dado, un STA puede asociarse con no más de un AP. Esto asegura que el DS puede determinar una única respuesta a la pregunta, ¿Qué AP está sirviendo a una X STA?.

Una vez que una asociación es completada, un STA puede hacer uso lleno de un DS (vía el AP) para comunicar. La asociación siempre se comienza por el STA móvil, no por el AP.

Un AP puede asociarse en un tiempo con muchos STAs. Un STA sabe que APs están presentes y entonces piden establecer una asociación invocando el servicio de asociación.

Entonces, Para que un terminal pueda comunicarse con otros terminales a través de un punto de acceso, debe primero estar asociado a dicho punto de acceso. Asociación significa asignación del terminal al punto de acceso haciendo que éste sea el responsable de la distribución de datos a, y desde, dicho terminal. En las redes con más de un punto de acceso, un terminal sólo puede estar asociada a un punto de acceso simultáneamente.

Reasociación

La asociación es suficiente para la entrega de mensaje de no-transición entre estaciones IEEE 802.11. La funcionalidad adicional se necesita apoyar la movilidad de la BSS-transición. La funcionalidad requerida adicional se proporciona por los servicios de reasociación. La Reasociación es un DSS.

El servicio del reasociación se invoca para cambiar de una asociación actual de un AP a otra. Estos no dejan de informar al DS de la cartografía actual entre AP y STA de como la estación se mueve de BSS a BSS dentro de un ESS. La Reasociación también habilita atributos de las asociación cambiantes de una asociación establecida mientras los restos de STA se asociaron con el mismo AP. La Reasociación siempre se comienza por el STA móvil.

El servicio de reasociación transfiere una asociación entre dos puntos de acceso. Cuando un terminal se mueve del área de cobertura de un punto de acceso a la de otro, su asociación pasa a depender de este último.

Disociación

El servicio del disociación se invoca cuando una asociación existente será terminada. La disociación es vía un DSS.

En un ESS, este le dice al DS que anule la información de la asociación existente. Los esfuerzos por enviar los mensajes vía el DS a un disociación STA serán infructuosos.

El servicio de disociación puede invocarse por cualquier parte en una asociación (no-APSTA o AP). La Disociación es una notificación, no una demanda.

La disociación Cancela una asociación existente, bien porque el terminal sale del área de cobertura del punto de acceso, o porque el punto de acceso termina la conexión.

Servicios de control de acceso y confidencialidad

Se requieren dos servicios para IEEE 802.11 para proporcionar la funcionalidad equivalente a lo que es inherente a LANs alambrado. El diseño de LANs alambrado asume los atributos físicos del alambre. En particular, el diseño de LAN alambrado se asume físicamente cerrado y controla la naturaleza de medios alambrados. La naturaleza del medio físicamente abierto de un IEEE 802.11 LAN viola esas suposiciones.

Se proporcionan dos servicios para traer a IEEE 802.11 funcionalidad en la línea con las suposiciones de LAN alambradas; la autentificación y privacidad. La autentificación se usa en lugar de los medios alambrados de conexión física. La privacidad se usa para proporcionar los aspectos confidenciales de medios alambrados cerrados.

Autenticación

En LANs alambrado, la seguridad física puede usarse para prevenir el acceso desautorizado. Esto es poco práctico en LANs inalámbricas porque ellas tienen un medio sin los límites precisos.

IEEE 802.11 proporciona la capacidad de controlar el acceso LAN vía el servicio de la autentificación. Este servicio se usa por todas las estaciones para establecer su identidad a estaciones con las que se comunicarán. Esto es para ambas redes ESS y IBSS. Si un nivel mutuamente aceptable de autentificación no se ha establecido entre dos estaciones, la asociación no se establecerá. La autentificación pertenece a un SS.

El servicio de autentificación entonces comprueba la identidad de una estación y la autoriza para asociarse En una red cableada lo que identifica a un terminal como parte de la red es el hecho de estar conectado físicamente a ella. En una red inalámbrica no existe la conexión física, por lo que, para saber si un terminal forma o no parte de la red, hay que comprobar su identidad antes de autorizar su asociación con el resto de la red.

Desautentificación

El servicio del desautentificación se invoca cuando una autenticación existente será terminada. La desautentificación pertenece a un SS.

Porque en un ESS, la autenticación es un requisito previo para la asociación, el acto de desautentificación causará que la estación pueda ser desasociada. El servicio del desautentificación puede invocarse por cualquiera parte de autentificación (no - APSTA o AP). La desautentificación no es una solicitud; es una notificación. La desautentificación no se negará por cualquier parte. Cuando un AP envía un aviso del desautentificación a un STA asociado, la asociación también se terminará.

Entonces, el servicio de desautentificación cancela una autentificación existente Este servicio da por concluida la conexión cuando una estación pretende desconectarse de la red.

Privacidad

Plantear la funcionalidad de las LAN inalámbricas hasta el nivel implícito de diseño en LAN alambrado, IEEE 802.11 proporciona la habilidad de encriptación de contenidos de mensajes. Esta funcionalidad se proporciona por el servicio de privacidad. La privacidad pertenece a un SS.

El servicio de privacidad Evita el acceso no autorizado a los datos gracias al uso del algoritmo WEP *(Wired Equivalency Protocol,* 'Protocolo de Equivalencia con Red Cableada'). Este algoritmo pretende emular el nivel de seguridad que se tiene en las redes cableadas

Los puntos de acceso utilizan tanto los servicios de estaciones como los servicios de distribución, mientras que los terminales sólo utilizan los servicios de estaciones.

SERVICIO MAC	DEFINICIÓN	TIPO DE ESTACION
Autentificación	Comprueba la identidad de una estación Y la autoriza para asociarse	Terminales y puntos de acceso
Desautentificación	Cancela una autentificación existente	Terminales y puntos de acceso
Asociación	Asigna el terminal al punto de acceso	Puntos de acceso
Desasociación	Cancela una asociación existente	Puntos de acceso
Reasociación	Transfiere una asociación entre dos puntos de acceso	Puntos de acceso
Privacidad	Evita el acceso no autorizado a los datos gracias al uso del algoritmo WEP	Terminales y puntos de acceso
Distribución	Asegura la transferencia de datos entre estaciones de distintos puntos de acceso	Puntos de acceso
Entrega de datos	Facilita la transferencia de datos entre estaciones	Terminales y puntos de acceso
Integración	Facilita la transferencia de datos entre redes Wi-Fi y no Wi-Fi	Puntos de acceso

Tabla 2.5. Servicios de la capa MAC

LA GESTIÓN

Tanto la capa física como la capa MAC están divididas en capacidades de gestión y de transferencia de datos. Lo que se conoce como PLME *(PHY Layer Management Entity,* 'Entidad de Gestión de la Capa Física') es quien se encarga de la gestión de la capa física, mientras que lo que se conoce como MILME (MAC *Layer Management Entity,* 'Entidad de Gestión de la Capa MAC') es quien se encarga de la gestión de la capa MAC. PLME y MLME intercambian información a través de MIB *(Management Information Base,* 'Base de Datos de la Información de Gestión'). Ésta es una base de datos de las características físicas (velocidad de transmisión, niveles de potencia, tipo de antena, etc.) de las estaciones.

EL FLUJO DE DATOS

Los datos que se van a transmitir por el medio radioeléctrico proceden de las capas superiores (formato IP) y se pasan a la capa **LLC** *(Logical Link Control,* 'Control Lógico del Enlace'). La capa LLC le pasa estos datos a la capa MAC, quien, a su vez, se los pasa a la capa física para su emisión.

Los paquetes de datos que se intercambian entre las capas LLC y MAC se conocen como MSDU *(MAC Service Data Unit,* 'Unidad de Datos del Servicio MAC'), mientras que los paquetes de datos que se intercambian entre las capas MAC y física reciben el nombre de **MPDU** *(MAC protocol data unit,* 'Unidad de Datos del Protocolo MAC'). En la capa física, quien recibe estos datos es PLCP, quien es responsable de convertir los datos MPDU a un formato compatible con el medio físico.

Fig.2.11 Interfaces de la capa MAC y Fisica

DOMINIOS REGULADORES PARA WI-FI

Unos de los principales atractivos de Wi-Fi es que no se requiere de una licencia para operar los dispositivos en la banda de 2.4 GHz o, en Estados Unidos y una cantidad cada vez mayor de países, la banda de 5 GHz. Sin embargo, "libre de licencia" no significa "sin regulación". De hecho, en distintos grados dependiendo de cada país, Wi-Fi está sujeto a una variedad de regulaciones que impactan el rango, escalabilidad, portabilidad, protección del producto y una variedad de factores adicionales que impactan la capacidad de uso en general de la tecnología.

Varias instituciones reguladoras han desarrollado un papel principal en el desarrollo de la popularidad de Wi-Fi. Las agencias reguladoras han tenido la visión de permitir la operación libre de licencia y, al coordinar sus esfuerzos, han proporcionado cierto nivel de integración en todo el mundo. Han aplicado e implementado regulaciones que han promovido, en lugar de retraer, el uso de estas bandas; en pocas palabras, sin la cooperación e incluso liderazgo que han proporcionado algunas instituciones reguladoras, no sería posible el Wi-Fi que conocemos actualmente.

Dominios reguladores

Hoy en día existen aproximadamente 200 paises en el mundo. Como estados soberanos, cada uno de ellos tiene la autoridad de crear e implementar regulaciones que sea únicas para su país. De hecho, unos cuantos países (por fortuna sólo algunos pocos) han impulsado regulaciones sobre Wi-Fi que sólo son especificas para esos países. La gran mayoría de los países opta por acoger un conjunto común de regulaciones de otro país (normalmente más grande). Un conjunto de países que por lo regular son colindantes y comparten un conjunto común de regulaciones se conoce

dentro de la especificación 802.11 como un *dominio regulador.* La tabla 2.6 define los dominios de regulación actuales para los productos Wi-Fi.

Dominio Regulador	Área Geográfica
América o FCC (Comisión Federal de Comunicaciones)	Norte, Sur y Centro d e América, Australia y Nueva Zelanda, distintas partes de Asia y Oceanía
Europa o ETSI (Instituto Europeo de Estándares de Telecomunicaciones)	Europa, Medio Oriente, Arica, distintas partes de Asia y Oceanía
Japón	Japón
China	Republica popular China
Israel	Israel
Singapur	Singapur
Taiwán	Republica de China
*Las regulaciones del dominio regulador de Singapur y Taiwán para las WLANs son especificadas por estos paises solo en la operación de la banda de 5 GHz; para la oeración de la banda de 2.4GHz entran en los dominios de ETSI y FCC respectivamente.	

Tabla 2.6 Dominios reguladores actuales para los productos Wi-Fi

Hay que observar que en la tabla 2.6 que la gran mayoría del mundo está dentro de los dos dominios reguladores principales, los dominios FCC y el ETSI. Otros países que tienen una tradición gubernamental de "hacer las cosas por sus propios medios" normalmente también tienden a presentar aspectos defensivos particularmente profundos y colocar estas consideraciones por arriba de la conveniencia y ahorros en costo que están asociados con la adopción de las regulaciones que desarrolló otro país (como es el caso de la adopción de FCC) o un instituto que establece estándares internacionales (como ETSI).

Debido a que ser un 'miembro" de un dominio regulador es completamente voluntario, las membresías pueden cambiar, y así lo hacen, en periodos bastante frecuentes.

Como se sugiere en el pie de nota de la tabla 2.6, los países tienen distintas operaciones sobre la operación de 2.4 GHz y 5 GHz, lo cual conduce a dominios reguladores distintos para cada banda Singapur y Taiwán son dominios reguladores únicos para la operación de 5 GHz, no existe un dominio regulador para 5 GHz en China y el dominio ETSI de 5 GHz se encuentra en un enorme estado de cambio en términos de membresías además de las regulaciones mismas-. Por estas y otras razones, es mejor discutir las reglas y requerimientos para los dominios reguladores para las bandas de 2.4 y 5 GHz como temas separados.

El dominio regulador FCC

La Comisión federal de comunicaciones fue establecida mediante el Acto de comunicaciones de 1934, los tiempos del Pacto nuevo que establecieron al gobierno federal como comisario del espectro de la frecuencia de radio en Estados Unidos. El espectro de frecuencia fue visto, y se sigue viendo así, como un bien público, cuyo uso debe estar sujeto a la regulación gubernamental.

La gran mayoría del espectro de frecuencia está asignada al uso con licencia -la operación en las *hondas con licencia* está restringida para el uso exclusivo del portador de la licencia-. Como compensación por el uso exclusivo de una banda en particular, el portador de la licencia está obligado a seguir las regulaciones FCC (aunque los requerimientos del ejército tienden a

sobreponerse a los de la FCC), pagar una cuota y, en muchos casos, 'actuar a favor del interés público". Ésta es la razón por la cual una emisora de televisión local puede, por ejemplo, emitir con exclusividad en el Canal 4 pero está obligado a incluir anuncios públicos de manera gratuita (normalmente en las primeras horas de las mañanas entre semana). A pesar de que la operación en las bandas libres de licencia no requiere de ningún proceso de licenciamiento formal, sí obliga al usuario seguir algunas regulaciones.

El conjunto de regulaciones FCC que se aplica a la operación Wi-Fi en la banda de 2.4 GHz y la de 5 GHz, es un subconjunto de las regulaciones de la Parte 15 de la FCC, el cual se aplica a una amplia variedad de dispositivos, incluyendo computadoras personales además de receptores de televisión y radio. La comunidad de fabricantes y proveedores, incluyendo las redes de televisión y radio, fabricantes de PC y aparatos electrónicos para el consumidor además de los fabricantes de dispositivos Wi-Fi, tienen un papel activo en la definición y propuesta de regulaciones FCC nuevas o modificaciones a las existentes. La mayor parte del público (y las industrias que están afectadas en particular) tienen la oportunidad de proporcionar comentarios a la FCC antes de que las reglas nuevas tomen efecto al responder a la Noticia de crear reglas propuestas *(Notice of Proposed Rule Making, NPRM,* por sus siglas en inglés). Es a través de las NPRM y otros procesos menos formales que las proposiciones de reglas nuevas se detallan para balancear las necesidades de los participantes que a menudo tienen perspectivas distintas. Dentro de las regulaciones de la Parte 15 se definen tres bandas de frecuencia separadas, 900 MHz, 2.4 GHz e Infraestructura de información nacional libre de licencia *(Unlicensed National Information Infrastructure, UNII,* por sus siglas en inglés) como disponibles para las aplicaciones industriales, científicas y médicas libres de licencia. La tabla 2.7 describe las características de estas bandas de frecuencia.

Banda	Rango de frecuencia	Uso común
900 MHz	902 – 928 MHz	Primeras WLANs, teléfonos inalámbricos.
2.4 GHz	2.400 – 2.4834 GHz (amplitud de 83.5 MHz)	WLANs Wi-Fi 802.11b y 802.11g, Bluetooth, teléfonos inalámbricos
UNII-1	5.15 – 5.25 GHz (amplitud de 100 MHz)	WLANs de uso interno
UNII-2	5.25 – 5.35 GHz (amplitud de 100 MHz)	WLANs de uso interno y externo
UNII-3	5.725 – 5.825 GHz (amplitud de 100 MHz)	Puentes inalámbricos de uso externo de rango amplio

Tabla 2.7 La FCC designa distintas posiciones del espectro de la frecuencia de radio para la operación libre de licencias y algunas veces sugiere, o especifica, los usos de estas bandas.

A pesar de que se encuentran dentro de las regulaciones de la Parte 15, se aplican distintas reglas para cada una de las bandas. La banda de 900 MHz es usada principalmente por los teléfonos inalámbricos, LAN inalámbricas que no cumplen con los estándares y otros dispositivos que no son Wi-Fi. Debido a esto, nos basaremos en las bandas de 2.4 y 5 GHz.

Las bandas de 2.4 GHz

El principal atractivo de la banda de 2.4 GHz es que está reservada para la operación libre de licencia no sólo por la FCC sino que también por otras agencias reguladoras, lo que significa que está libre de licencias a lo largo de la mayor parte del mundo. En relación a las regulaciones para la banda de 2.4 GHz en otras partes del mundo y en relación a otras regulaciones de la FCC para las bandas de 5 GHz, las reglas de operación en la banda 2.4 GHz de la FCC son bastante liberales.

Las regulaciones definen la operación para los sistemas de Espectro extendido de saltos de frecuencia (FHSS) como, por ejemplo, los productos heredados de LAN inalámbricas, teléfonos inalámbricos y dispositivos BlueTooth, además de definir con mayor detalle la operación para los sistemas de Espectro extendido de secuencia directa (DSSS) como, por ejemplo, Wi-Fi. Originalmente, esto representaba la exclusión de los sistemas basados en OFDM, como Wi-Fi de 802.11g. pero esto ha sido modificado para permitir estos sistemas de alto desempeño que operan en la banda de 2.4 GHz. La compatibilidad con la gran mayoría de estas regulaciones es principalmente la responsabilidad de la comunidad de fabricantes que la de los usuarios -los fabricantes deben proporcionar sistemas compatibles y el usuario simplemente debe usarlos como es debido.

Hay que observar que los fabricantes tienen la responsabilidad de proporcionar un *sistema* compatible en lugar de simplemente ofrecer un producto *compatible.* Por ejemplo, cuando un punto de acceso o un adaptador de un cliente incorpora antenas y el usuario no puede conectar un tipo diferente de antena, entonces el sistema representa al producto. Por otro lado, si un punto de acceso tiene un conector de antena, el fabricante debe certificar no sólo el punto de acceso sino el punto de acceso con todas las combinaciones posibles de antenas. Entonces el usuario podrá escoger algunas de estas antenas posibles y poder desplegar un sistema compatible.

La regulación siguiente que está dentro de las reglas de la Parte 15 de la FCC, Subparte C, Subsección 15.203, tienen como fin definir de mejor manera lo que significa 'todas las antenas posibles":

"Un radiador intencional (recuerde que esto quiere decir un radio en términos gubernamentales) debe estar diseñado para asegurar que no se debe usar ningún otro tipo de antena que no haya sido elaborada por la parte responsable (el fabricante, por ejemplo) con este dispositivo. El uso de una antena permanentemente conectada o una antena que usa un dispositivo de acoplamiento único para el radiador intencional debe considerarse adecuado para cumplir con las provisiones de esta sección".

Para cumplir con esta regulación, los fabricantes normalmente modifican un conector estándar en la industria de forma que se convierta en 'exclusivo" para ellos y generalmente no está disponible en otras fuentes. Por ejemplo, Cisco Systems modifica un conector con rosca para cable coaxial *(Threaded Novel Col7nector, TNC,* por sus siglas en inglés) al invertir la polaridad del acoplamiento lo cual da como resultado un conector RP-TNC. Otros fabricantes llevan a cabo modificaciones similares que son fáciles de duplicar, lo cual lleva a la creación de una industria de conectores de distintos fabricantes que es saludable y, razonablemente, de bajo perfil. Por lo tanto, es bastante sencillo obtener antenas de otros fabricantes con conectores que se ajustarán a los puntos de acceso de los fabricantes líderes en la industria.

Conectar antenas de otros fabricantes a un dispositivo Wi-Fi no es una violación de las reglas FCC. Al trabajar en cooperación con el fabricante del radiador intencional, el fabricante de la antena ya sea el fabricante de la antena mismo o un distribuidor- puede certificar la compatibilidad FCC del sistema (todos los puntos de acceso que deseen conectar además de todas las antenas que deseen incluir), lo cual los convierte a ellos, y no al fabricante, en la "parte responsable". Esto representa una carga originada por las regulaciones grande, costosa y consumidora de tiempo, además, de hecho, es una motivación para "no incluir" algunos aspectos. Para los usuarios, la estrategia más prudente es simplemente obtener antenas del mismo fabricante que proporciona el punto de acceso. Cuando esto no es posible, si se obtiene una antena de otro fabricante, es necesario preguntar si existe una certificación de compatibilidad para los puntos de acceso o adaptadores de clientes específicos.

Una vez que está establecido que el punto de acceso y el sistema de antenas es compatible, la primera área a considerar por los usuarios debe ser la de estar dentro de las limitaciones de la potencia de transmisión. Este es un aspecto que sólo se relaciona con los productos de puentes de punto a punto y punto a multipunto, los cuales a menudo están *basados* en dispositivos Wi-Fi pero no son, estrictamente hablando, puntos de acceso o dispositivos de cliente.

La FCC limita el total de la potencia de transmisión y la ganancia de antena menos cualquier pérdida en el cable, a no más de 36 dBm o 4 watts. Esta potencia de radiación isotrópica efectiva *(Effective Isotropic Radiated power, EIRP,* por sus siglas en inglés) permite un poco más de flexibilidad en la parte del usuario y el fabricante. Pero la IFCC la ha incluido, junto con otras agencias reguladoras del resto del mundo, para asegurar que el fabricante no proporcione un equipo que irradiará una cantidad excesiva de energía dentro de un espacio determinado.

Por ejemplo, cualquiera de las siguientes situaciones de radio, antena y cable son compatibles con la FCC:

- Un dispositivo transmitiendo 20 dBm (100 mW) con una antena dipolo (conocida como "pato de hule") de 2 dBi directamente conectada; 20 + 2 = 22 dBm, <36 dBm
- Un dispositivo transmitiendo 20 dBm (100 mW) con una antena omnidireccional de 5 dBi directamente conectada; 20 + 5 = 25 dBm, < 36 dBm
- Un dispositivo transmitiendo 20 dBm (100mW) con una antena Yagi de 13 dBi directamente conectada; 20 + 13 - 2 = 31 dBm, <36 dBm
- Por otro lado, el escenario siguiente no es compatible:
- Un dispositivo transmitiendo 20 dBm (100mW) con una antena de plato de 21 dBi conectada mediante 25 pies de cable que implica cerca de 2 dBm de pérdida; 20 + 21 - 2 39 dBm, >36 dBm

Hay que observar que de acuerdo a los ejemplos anteriores, con la mayoría de los tipos de antenas diseñadas para las aplicaciones LAN inalámbricas, el usuario corre poco peligro de exceder las limitaciones EIRP de la FCC. Sólo cuando diseñe un sistema que use antenas de ganancia alta y haz angosto como, por ejemplo, las antenas parabólicas que están diseñadas para las aplicaciones de puente de punto a punto, tendrá que considerar la reducción en la potencia de transmisión o de introducción de pérdidas por cable para seguir siendo compatible. En pocas palabras. si usa dispositivos Wi-Fi que no estén modificados, mantener la compatibilidad con las limitaciones EIRP de la FCC no debe ser una preocupación grande.

A pesar de que las regulaciones de la FCC para las antenas son bastante restrictivas, son mínimas en comparación con las regulaciones de la FCC para los amplificadores externos. Un *amplificador* es un dispositivo de potencia que se conecta entre el radio y la antena para añadir potencia adicional al sistema. por lo tanto, incrementando la densidad de potencia total en un espacio determinado. A pesar de que la FCC permite la venta de antenas individuales, prohíbe, específicamente, la venta de amplificadores externos como dispositivos aislados. Los amplificadores externos se pueden comprar sólo como parte de un *kit* que incluye al radiador intencional, antena y los cables necesarios, además del amplificador externo. Estos kits deben estar certificados como para la compatibilidad con la FCC en la forma de sistema completo. Muchas

personas han observado que la FCC tiene una perspectiva cuidadosa con respecto a los amplificadores en general debido al potencial que proporcionan para él abuso.

Para la gran mayoría de aplicaciones Wi-Fi, toda la ganancia que un usuario requiere se puede obtener a través de la selección de una antena -no es necesario un amplificador externo. Con un grado ligeramente menor, se puede decir lo mismo para las aplicaciones de puente. En general, es mejor que el usuario tenga en cuenta que simplemente debe evitar los amplificadores externos, en especial cuando los amplificadores no se ofrecen como parte de un elemento certificado que sea uno de los componentes 802.11 que se han adquirido.

A pesar de que la asignación FCC para la banda ISM de 2.4 GHz está definida entre 2.4 y 2.4835 GHz, los dispositivos Wi-Fi que operan en esa banda funcionan en términos de canales.

Las especificaciones 802.11b y 802.11g definen los canales disponibles en la banda FCC para el uso en Estados Unidos de la manera siguiente:

ID de canal (MHz)	Frecuencia
1	2412
2	2417
3	2422
4	2427
5	2432
6	2437
7	2442
8	2447
9	2452
10	2457
11	2462

Tabla 2. 8

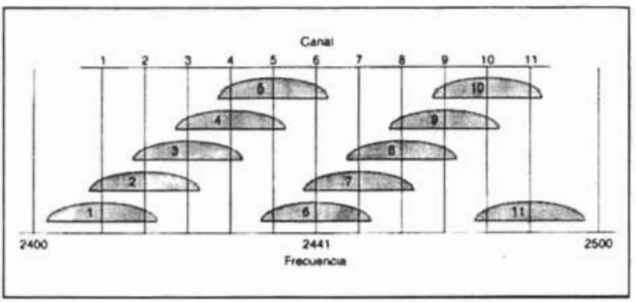


Fig. 2.12 Los 11 canales de 802.11 en la frecuencia de 2.4Ghz

Los resultados anteriores de las especificaciones 802.11 b y 802.11g sugieren, de manera errónea, que el usuario tiene once canales disponible en la banda de 2.4 GHz. Por supuesto, ése no es el caso. Como indicamos antes, el usuario en realidad no tiene más de tres canales que *no se traslapan.* Se requiere de un mínimo de 22 MHz de ancho de banda para la transmisión Wi-Fi en la banda de 2.4 GHz.

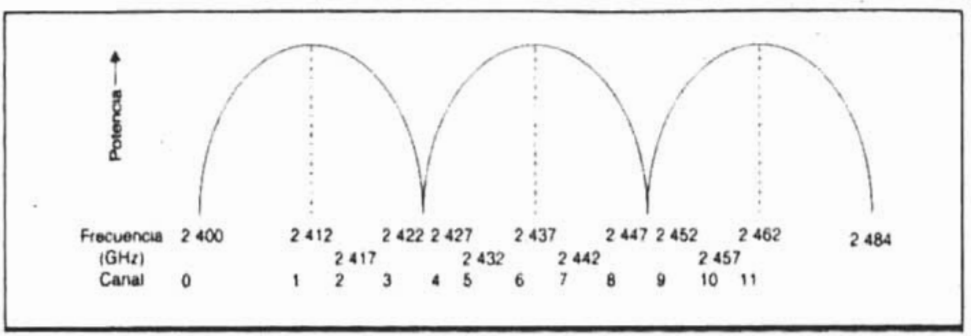


Fig. 2.13 A pesar de que las especificaciones 802.11b /g definen 11 canales en la banda ISM de 2.4 GHz de la FCC solo tres no se traslapan y por lo tanto se pueden usar

Como se muestra en la figura 2.13, estos canales de 22 MHz de amplitud se extienden 1 MHz fuera del punto central del canal en ambas direcciones. Los únicos canales disponibles de estos once que permiten la amplitud de 11 MHz en ambas direcciones sin interferir con otro canal o extenderse más allá de la frecuencia asignada (excediendo las bandas laterales) son los canales 16 y 11. A pesar de que no existe una restricción legal sobre el diseño de una LAN inalámbrica que tenga un uso menor o mayor de un canal. normalmente es recomendable usar los tres canales, ni uno más ni uno menos, para alcanzar el mejor balance entre la capacidad y la confiabilidad.

Las bandas de 5 GHz

Como se indica en la tabla 2.7, la FCC ha asignado tres bandas libres de licencia en la porción de 5 GHz del espectro de frecuencia que se conocen de manera colectiva como las bandas de Infraestructura de información nacional libre de licencia *(Unlicensed National Infórmation Infiastructure, UNI).* (Por razones que no son intuitivas, la FCC insiste en colocar un guión entre la *U* y la *N,* lo cual da como resultado U-NII, una convención que casi todas las demás partes han ignorado.) Cada una de las tres bandas tiene una amplitud de 100 MHz. La banda UNII- 1 está ubicada entre 5.15-5.25 GHz, UNII-2 en 5.25-5.35 GHz y UNII-3 en 5.725-5.825. Se observa que las bandas UNII-l y IINII-2 son contiguas y de hecho son tratadas por 802.11 a como un espacio continuo de amplitud de 200 MHz del espectro, más del doble del tamaño de la banda ISM de 2.4 GHz. Esto da como resultado un beneficio importante a 802.11a -la amplitud de 200 MHz en las bandas UNII-1 y UNII-2 están divididas hasta en ocho canales *que no se traslapan,* cada uno de ellos con una amplitud de 25 MHz.

Como se indica en la tabla 2.7, cada banda UNII está diseñada para un uso distinto. Como bandas libres de licencia, estos usos no son en sí parte de las regulaciones; en lugar de esto, las regulaciones están diseñadas para promover el uso especificado para el detrimento, o al menos inconveniencia, de otros usos. La banda UNII-3 está diseñada para funcionar como puente inalámbrico de rango amplio en sistemas de punto a punto y punto a multipunto y sólo se debe usar en entornos exteriores. A pesar de que las bandas UNII-l y UNII-2 son contiguas y se consideran como una sola banda por la mayoría de los dispositivos Wi-Fi de 5 GHz, tienen limitaciones reguladoras muy distintas.

CAPÍTULO 3

COMPONENTES DE CONECTARIZACIÓN PARA REDES WI-FI

La mayoría de las redes inalámbricas que hay en el mercado (sean Wi-Fi o de otro tipo) funcionan de una manera similar: tienen unas estaciones base (puntos de acceso) que coordinan las comunicaciones y unas tarjetas de red (adaptadores de red) que se instalan en los ordenadores y que les permiten formar parte de la red.

Adicionalmente, existen antenas que permiten aumentar el alcance de los equipos Wi-Fi, así como *software* especializado que permite facilitar la labor de gestión y mantenimiento de la red inalámbrica.

Antes de describir las distintas componentes necesarias para crear una red Wi-Fi, vamos a dedicar unas páginas para describir las características más importantes para una selección adecuada de algún tipo arquitectura Wi-Fi, así como, los parámetros a considerar para su implementación. Después en este capitulo vamos a tratar fundamèntalmente los adaptadores de red, los puntos de acceso y las antenas externas.

POR QUÉ INSTALAR UNA RED INALÁMBRICA

Las redes inalámbricas hacen exactamente el mismo trabajo que realizan las redes cableadas: interconectan ordenadores y otros dispositivos informáticos (impresoras, módem, etc.) para permitirles compartir recursos. Las redes locales permiten interconectar desde dos ordenadores hasta cientos de ellos situados en un entorno donde la distancia máxima de un extremo a otro de la red suele ser de algunos cientos de metros. Esto quiere decir que las redes de área local se limitan generalmente al ámbito de un edificio. No obstante, distintas redes locales situadas en distintos edificios (edificios que pueden estar situados en distintas ciudades) pueden interconectarse entre sí formando un único entorno de red.

En resumen, las ventajas que ofrece una red de área local, sea cableada o inalámbrica, son las siguientes:

- Permite compartir periféricos: impresoras, escáneres, etc.
- Permite compartir los servicios de comunicaciones (ADSL, módem cable, RDSI, etc.)
- Permite compartir la información contenida en cada ordenador
- Permite compartir aplicaciones

A partir de aquí, la pregunta seria si la red local que nos interesa instalar debe ser cableada o inalámbrica. Muchos usuarios responden a esta cuestión simplemente decidiéndose a instalar la última tecnología del mercado y la última tecnología es la inalámbrica. La inquietud de disponer de la tecnología más moderna es loable y no cabe duda de que las redes inalámbricas ofrecen una mayor comodidad de uso o una mayor facilidad de instalación, pero toda tecnología tiene sus

propias limitaciones. Por tanto, creo que es interesante pararse a analizar un poco las ventajas y posibles inconvenientes que tiene la tecnología inalámbrica.

Ventajas

Las principales ventajas que ofrecen las redes inalámbricas frente a las redes cableadas son las siguientes:

- **Movilidad.** La libertad de movimientos es uno de los beneficios más evidentes de las redes inalámbricas. Un ordenador o cualquier otro dispositivo (por ejemplo, una PDA o una *webcam)* pueden situarse en cualquier punto dentro del área de cobertura de la red sin tener que depender de si es posible o no hacer llegar un cable hasta ese sitio. Ya no es necesario estar atado a un cable para navegar por Internet, imprimir un documento o acceder a la información de nuestra red local corporativa o familiar. En la empresa se puede acceder a los recursos compartidos desde cualquier lugar de ella, hacer presentaciones en la sala de reuniones, acceder a archivos, etc., sin tener que tender cables por mitad de la sala o depender de si el cable de red es o no suficientemente largo.

- **Desplazamiento.** Con un ordenador portátil o PDA no sólo se puede acceder a Internet o a cualquier otro recurso de la red local desde cualquier parte de la oficina o de la casa, sino que nos podernos desplazar sin perder la comunicación. Esto no sólo da cierta comodidad, sino que facilita el trabajo en determinadas tareas, como, por ejemplo, la de aquellos empleados cuyo trabajo les lleva a moverse por todo el edificio.

- **Flexibilidad.** Las redes inalámbricas no sólo nos permiten estar conectados mientras nos desplazamos con un ordenador portátil, sino que también nos permiten colocar un ordenador de sobremesa en cualquier lugar sin tener que hacer el más mínimo cambio en la configuración de la red. A veces, extender una red cableada no es una tarea fácil ni barata. Piense en edificios antiguos o en áreas apartadas. En muchas ocasiones acabamos colocando peligrosos cables por el suelo para evitar tener que hacer la obra de poner enchufes de red más cercanos. Las redes inalámbricas evitan todos estos problemas. Resulta también especialmente indicado para aquellos lugares en los que se necesitan accesos esporádicos. Si en un momento dado existe la necesidad de que varias personas se conecten a la red en la sala de reuniones, la conexión inalámbrica evita llenar el suelo de cables. Ln sitios donde pueda haber invitados que necesiten conexión a Internet (centros de formación, hoteles, cafés, entornos de negocio o empresariales) las redes inalámbricas suponen una alternativa mucho más viable que las redes cableadas.

- **Ahorro de costes.** Diseñar e instalar una red cableada puede llegar a alcanzar un alto coste, no solamente económico, sino en tiempo y molestias. En entornos domésticos y en determinados entornos empresariales donde no se dispone de una red cableada porque su instalación presenta problemas, la instalación de una red inalámbrica permite ahorrar costes al permitir compartir recursos: acceso a Internet, impresoras, etc.

- **Escalabilidad**. Se le llama escalabilidad a la facilidad de expandir la red después de su instalación inicial. Conectar un nuevo ordenador cuando se dispone de una red inalámbrica es algo tan sencillo como instalarle una tarjeta y listo. Con las redes cableadas esto mismo

requiere instalar un nuevo cableado o, lo que es peor, esperar hasta que el nuevo cableado quede instalado.

Desventajas

Evidentemente, como todo en la vida, no todo son ventajas, las redes inalámbricas también tienen algunos puntos negativos en su comparativa con las redes de cable. Los principales inconvenientes de las redes inalámbricas son los siguientes:

- **Menor ancho de banda.** Las redes de cable actuales pueden trabajar a 1 Gbps, mientras que las redes inalámbricas Wi-Fi lo hacen a 11 Mbps. Es cierto que existen estándares que alcanzan los 54 Mbps y soluciones propietarias que llegan a 100 Mbps, pero estos estándares están en los comienzos de su comercialización y tienen un precio superior al de los actuales equipos Wi-Fi.

- **Mayor inversión inicial.** Para la mayoría de las configuraciones de red local, el coste de los equipos de red inalámbricos es superior al de los equipos de red cableada.

- **Seguridad**. Las redes inalámbricas tienen la particularidad de no necesitar un medio físico para funcionar (podría funcionar incluso en el vacío). Esto fundamentalmente es una ventaja, pero se convierte en un inconveniente cuando pensamos que cualquier persona con un ordenador portátil sólo necesita estar dentro del área de cobertura de la red para poder intentar acceder a ella. Como el área de cobertura no está definida por paredes o por ningún otro medio físico, a los posibles intrusos no les hace falta estar dentro de un edificio o estar conectado a un cable. Además, el sistema de seguridad que incorporan las redes Wi-Fi no es de los más fiables. A pesar de esto, también es cierto que ofrece una seguridad válida para la inmensa mayoría de las aplicaciones y que ya hay disponible un nuevo sistema de seguridad (WPA) que hace a Wi-Fi mucho más confiable.

- **Interferencias.** Las redes inalámbricas funcionan utilizando el medio radioeléctrico en la banda de 2,4 GHz. Esta banda de frecuencias no requiere de licencia administrativa para ser utilizada por lo que muchos equipos del mercado, como teléfonos inalámbricos, microondas, etc., utilizan esta misma banda de frecuencias. Además, todas las redes Wi-Fi funcionan en la misma banda de frecuencias, incluida la de los vecinos. Este hecho hace que no se tenga la garantía de que nuestro entorno radioeléctrico esté completamente limpio para que nuestra red inalámbrica funcione a su más alto rendimiento. Cuantos mayores sean las interferencias producidas por otros equipos, menor será el rendimiento de nuestra red. No obstante, el hecho de tener probabilidades de sufrir interferencias no quiere decir que se tengan. La mayoría de las redes inalámbricas funcionan perfectamente sin mayores problemas en este sentido.

- **Incertidumbre tecnológica**. La tecnología que actualmente se está instalando y que ha adquirido una mayor popularidad es la conocida como Wi-Fi (IEEE 802.11b). Sin embargo, ya existen tecnologías que ofrecen una mayor velocidad de transmisión y unos mayores niveles de seguridad. Es posible que, cuando se popularice esta nueva tecnología, se deje de comercializar la actual o, simplemente, se deje de prestar tanto apoyo a la actual. Lo cierto es que las leyes del mercado vienen también marcadas por las necesidades de los clientes y, aunque existe esta incógnita, los fabricantes no querrán perder el tirón que ha

supuesto Wi-Fi y harán todo lo posible para que los nuevos dispositivos sean compatibles con los actuales. La historia nos ha dado muchos ejemplos similares.

Apreciaciones

Después de ver las ventajas y los inconvenientes, cualquiera puede sacar sus propias conclusiones; no obstante, hagamos un par de apreciaciones.

La tecnología inalámbrica en los hogares es un caso especial. Es raro encontrar una casa que tenga preinstalada una red cableada de datos. Sin embargo, aun contando con una única impresora, una única conexión a Internet (vía ADSL o cable, por ejemplo), un único grabador de CD o un único escáner, cada vez es más normal disponer de más de un ordenador en casa. Para poder compartir estos recursos, se puede instalar una rígida red cableada tendiendo cables a través de las paredes o configurar una red inalámbrica. Es cierto que esta última solución es más cara que la primera, pero también es más flexible, escalable, fácil de instalar y, además, permite movilidad. ¿Por qué estar encerrado en una habitación si hace un día estupendo y se está mejor en el salón, en el patio o en el parque enfrente de casa? Por otro lado, el problema de la seguridad no es altamente preocupante en la informática del hogar.

El caso de las empresas puede ser similar al anterior, pero también nos encontramos con un punto adicional. Las redes cableadas son un problema en aquellas empresas donde existe la posibilidad de cambiar la disposición de los puestos de trabajo. Sin embargo, para una red inalámbrica no supone ningún problema el cambiar un ordenador de sitio.

El hecho de instalar una red inalámbrica no quiere decir que toda la red tenga que ser inalámbrica. Las redes Wi-Fi son completamente compatibles con las redes locales cableadas Ethernet. Por tanto, la parte inalámbrica puede ser un complemento de la parte cableada. Se puede cablear lo que sea fácil cablear y dejar a Wi-Fi que resuelva la extensión de la red a aquellas áreas más difícilmente cableables. Por otro lado, también se puede disponer de una red de cable para unos usuarios y una red inalámbrica paralela para aquellos otros que por la labor que desempeñan necesitan disfrutar de la ventaja de la movilidad.

Por ultimo, la redes inalámbricas son ideales, por ejemplo, si se necesita disponer de conexión a red en lugares abiertos (por ejemplo, un campus universitarios), en sitios públicos (centros comerciales, redes vecinales, servicios municipales, etc.) o sitios cerrados pero disponiendo de movilidad (almacenes, salas de reuniones, etc.).

LAS OPCIONES CON LAS QUE S CUENTAN

Anteriormente hemos dado los puntos más importantes para confirmar que, efectivamente, necesitamos una red inalámbrica. Ahora toca analizar qué tipo de red es la que le viene mejor a nuestras necesidades. Una red puede comunicar un par de ordenadores o a cientos de ellos, podemos tener a todos los ordenadores concentrados en una pequeña zona o dispersos por una gran área, dentro de un edificio, en varios edificios o en el exterior.

Las decisiones que hay que tomar a este respecto son las siguientes:

- Cuál será la estructura de la red, si se necesitaran instalar puntos de acceso y cuántos serán necesarios.
- Qué tarjeta o dispositivos inalámbricos instalaremos en cada ordenador, PDA o cualquier otro equipo informático que necesitemos conectar.
- Qué tipo de antenas necesitaremos para poder cubrir todo el área por la que necesitamos disponer del servicio.
- Cómo conectaremos nuestra red inalámbrica a la red local cableada y a Internet.

LAS DIFERENTES ESTRUCTURAS DE RED

Como ya se explico anteriormente la IEEE802.11 tiene 3 diferentes arquitecturas, estas arquitecturas se vieron de forma muy técnica ya que la información fue recopilada de la *IEEE Wireless LAN Edition* de la norma *IEEE Std 802.11™ - 1999 (R2003)*. A continuación se explicaran la mismas arquitecturas de una forma más digerible y comercial.

IBSS (Independent Basic Service Set, 'Conjunto de Servicios Básicos Independientes').

Esta modalidad está pensada para permitir exclusivamente comunicaciones directas entre los distintos terminales que forman la red. En este caso no existe ningún terminal principal que coordine al grupo, no existe punto de acceso. A esta modalidad también se le conoce como una red ad hoc (entre iguales) o peer to peer(punto a punto).

Ésta es una red de área local independiente que no está conectada a una infraestructura con cables y en la que todos los puestos están directamente conectados entre sí (lo que se conoce como topología de malla). Consiste simplemente en proveer a los ordenadores con una tarjeta de red inalámbrica de modo que "todos hablen con todos" como puede observarse en la figura. En este caso, no es necesario incorporar un punto de acceso. Presenta la ventaja de su sencillez pero, a cambio, tiene el inconveniente de crear una red aislada de otras redes y no ofrecer facilidades de seguridad ni gestión como cuando se dispone de una base.

La configuración de una WLAN en modo ad hoc se emplea para establecer una red cuando no exista una infraestructura inalámbrica o cuando no se requieran servicios, como en una feria comercial o cuando se trabaja con compañeros en una ubicación remota. Esta topología es práctica en lugares en los que pueden reunirse pequeños grupos de equipos que no necesitan acceso a otra red. Ejemplos de entornos en los que podrían utilizarse redes inalámbricas ad hoc serían un domicilio sin red con cable o una sala de conferencias donde los equipos se reúnen con regularidad para intercambiar ideas.

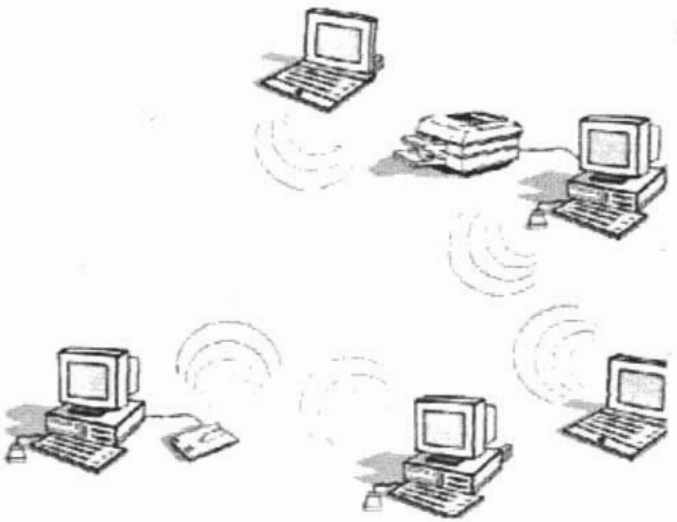


Fig 3.1 Red IBSS o ad hoc

BSS (Basic Service Set, 'Conjunto de Servicios Básicos').

En esta modalidad se añade un equipo llamado punto de acceso (AP o *Aceess Point* en inglés) que realiza las funciones de coordinación centralizada de la comunicación entre los distintos terminales de la red. Los puntos de acceso tienen funciones de *buffer* (memoria de almacenamiento intermedio) y de *gateway* (pasarela) con otras redes. A los equipos que hacen de pasarelas con otras redes externas se les conoce como *portales*. A la modalidad BSS también se la conoce como modo infraestructura.

El portátil o dispositivo inteligente, denominado "estación" en el ámbito de las redes LAN inalámbricas, primero debe identificar los puntos de acceso y las redes disponibles. Este proceso se lleva a cabo mediante el control de las tramas de señalización procedentes de los puntos de acceso que se anuncian a sí mismos o mediante el sondeo activo de una red específica con tramas de sondeo. La estación elige una red entre las que están disponibles e inicia un proceso de autenticación con el punto de acceso.

Una vez que el punto de acceso y la estación se han verificado mutuamente, comienza el proceso de asociación. La asociación permite que el punto de acceso y la estación intercambien información y datos de capacidad. El punto de acceso puede utilizar esta información y compartirla con otros puntos de acceso de la red para diseminar la información de la ubicación actual de la estación en la red. La estación sólo puede transmitir o recibir tramas en la red después de que haya finalizado la asociación.

En la modalidad de infraestructura, todo el tráfico de red procedente de las estaciones inalámbricas pasa por un punto de acceso para poder llegar a su destino en la red LAN con cable o inalámbrica. El acceso a la red se administra mediante un protocolo que detecta las portadoras y evita las colisiones. Las estaciones se mantienen a la escucha de las transmisiones de datos durante

un período de tiempo especificado antes de intentar transmitir (ésta es la parte del protocolo que detecta las portadoras). Antes de transmitir, la estación debe esperar durante un período de tiempo específico después de que la red está despejada. Esta demora, junto con la transmisión por parte de la estación receptora de una confirmación de recepción correcta, representan la parte del protocolo que evita las colisiones. Observe que, en la modalidad de infraestructura, el emisor o el receptor es siempre el punto de acceso.

Dado que es posible que algunas estaciones no se escuchen mutuamente, aunque ambas estén dentro del alcance del punto de acceso, se toman medidas especiales para evitar las colisiones. Entre ellas, se incluye una clase de intercambio de reserva que puede tener lugar antes de transmitir un paquete mediante un intercambio de tramas "petición para emitir" y "listo para emitir", y un vector de asignación de red que se mantiene en cada estación de la red. Incluso aunque una estación no pueda oír la transmisión de la otra estación, oirá la transmisión de "listo para emitir" desde el punto de acceso y puede evitar transmitir durante ese intervalo.

El proceso de movilidad de un punto de acceso a otro no está completamente definido en el estándar. Sin embargo, la señalización y el sondeo que se utilizan para buscar puntos de acceso y un proceso de reasociación que permite a la estación asociarse a un punto de acceso diferente, junto con protocolos específicos de otros fabricantes entre puntos de acceso, proporcionan una transición fluida.

La sincronización entre las estaciones de la red se controla mediante las tramas de señalización periódicas enviadas por el punto de acceso. Estas tramas contienen el valor de reloj del punto de acceso en el momento de la transmisión, por lo que sirve para comprobar la evolución en la estación receptora. La sincronización es necesaria por varias razones relacionadas con los protocolos y esquemas de modulación de las conexiones inalámbricas.

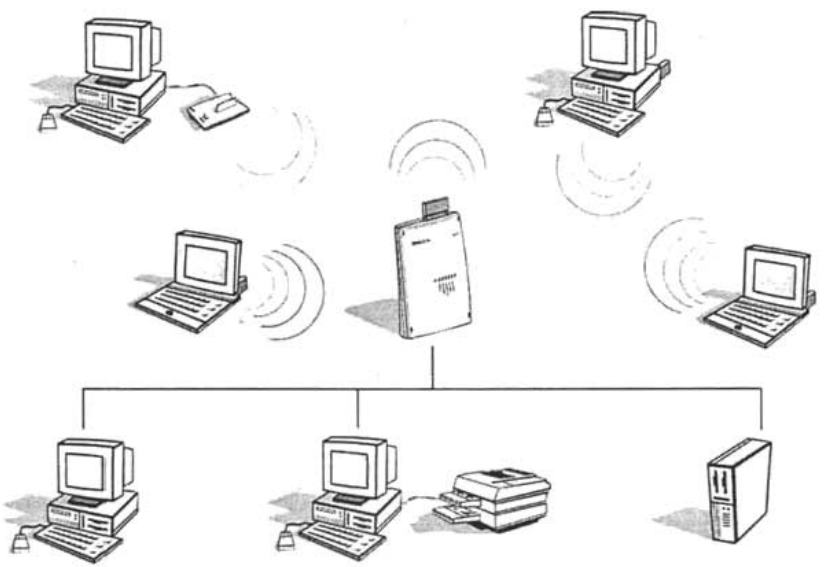


Fig.3.2 Estructura BSS o Infraestructura

ESS (Extended Service Set, 'Conjunto de Servicios Extendido')

Esta modalidad permite crear una red inalámbrica formada por más de un punto de acceso. De esta forma se puede extender el área de cobertura de la red, quedando constituida por un conjunto de celdas pegadas unas a otras. Una red ESS está formada por múltiples redes BSS.

La configuración ESS permite crear una red local inalámbrica con una extensa área de cobertura. Para cubrir todo el área, se disponen de múltiples celdas BSS, cada una de las cuales cuenta con su punto de acceso. En esta configuración, los terminales pueden desplazarse por todo el área de cobertura sin perder la comunicación.

La configuración ESS resulta interesante cuando se necesita cubrir un gran área de oficinas, oficinas localizadas en distintas plantas, un espacio público o lugares con una alta concentración de terminales donde un solo punto de acceso resulta escaso.

Los distintos puntos de acceso que forman una red ESS se interconectan entre sí a través de una red que, generalmente, suele ser una red cableada Ethemet. Esta conexión sirve también para que los terminales inalámbricos puedan comunicarse con los terminales de la red cableada.

Para que funcionen las redes ESS, deben configurarse los distintos puntos de acceso como miembros de una misma red. Esto implica que todos deben tener el mismo nombre de red y la misma configuración de seguridad, aunque funcionando en distintos canales de radio. Esto último es importante porque, de otro modo, los puntos de acceso se interferirían unos a otros impidiendo la comunicación con sus terminales.

Cuando un terminal se mueve filera del alcance del punto de acceso con el que está asociado originalmente, automáticamente se reasocia con un nuevo punto de acceso con el que tenga cobertura.

Esta reasociación la hace el terminal automáticamente, sin que el usuario tenga que hacer nada. Desde el punto de vista del usuario, la conexión a una red ESS es idéntica a la conexión a una red BSS. La única diferencia es que se dispone de una mayor cobertura.

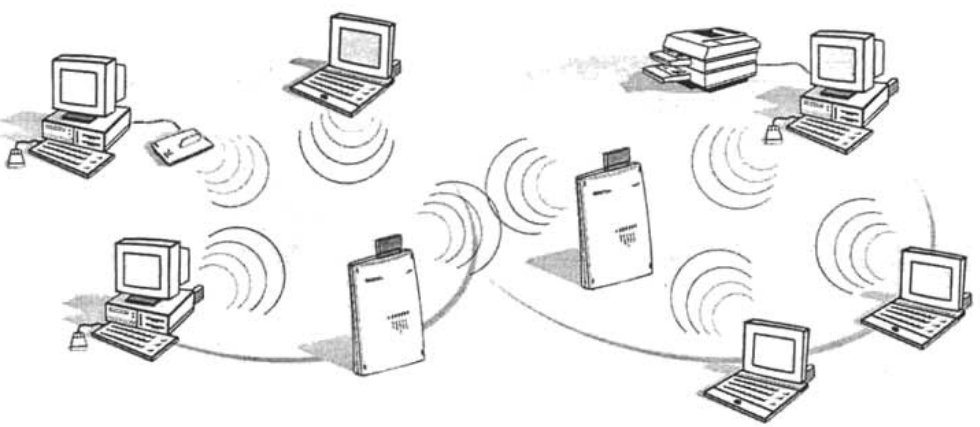


Fig.3. 3 Estructura ESS

En las modalidades BSS y ESS todas las comunicaciones pasan por los puntos de acceso. Aunque dos terminales estén situados uno junto al otro, la comunicación entre ellos pasará por el punto de acceso al que estén asociados. Esto quiere decir que un terminal no puede estar configurado para funcionar en la modalidad *ad hoc* (IBBS) y de infraestructura (BSS) a la vez.

PORQUE SE REQUIEREN LOS PUNTOS DE ACCESO

Las comunicaciones *ad hoc* son muy fáciles de configurar y resultan muy interesantes cuando se necesita establecer una comunicación temporal entre dos equipos. Por otro lado, el modo infraestructura es el más adecuado para crear redes permanentes, aunque sean de tan sólo dos terminales. Las razones que nos llevan a esta conclusión son varias:

- El modo infraestructura ofrece un mayor alcance que en la modalidad *ad hoc*. Los terminales no tienen por qué estar dentro del área de cobertura el uno del otro; al tener un punto de acceso intermedio pueden, al menos, duplicar su distancia.
- El punto de acceso permite compartir el acceso a Internet entre todos sus terminales. Esto permite compartir un acceso de banda ancha (por ejemplo, ADSL o cable) entre todos los terminales que forman la red, sean dos o cientos de ellos.
- El punto de acceso permite crear redes con un mayor número de terminales.
- El punto de acceso ofrece características de gestión de la comunicación que no ofrece el modo *ad hoc*.
- El punto de acceso, al igual que cualquier red local, permite compartir los recursos de los terminales que forman la red (archivos, impresoras, etc.)

Recientemente ha aparecido en el mercado una alternativa al modo *ad hoc* conocida como *software* de punto de acceso. Esto consiste en configurar los ordenadores en modo *ad hoc* y hacer que uno de estos ordenadores haga las funciones de punto de acceso instalándole un programa especial, el *software* de punto de acceso. Ya se han hecho programas de este tipo para distintos sistemas operativos. Se ha dado el caso de usuarios que recuperan un viejo ordenador para dedicarlo exclusivamente a trabajar como punto de acceso.

EL ALCANCE QUE SE TIENE

Cuando nos decidimos a instalar una red inalámbrica, generalmente se parte de unas necesidades de cobertura. Pretendemos tener cobertura en toda la oficina, la casa, el entorno empresarial o el pueblo completo. Quiere esto decir que uno de los factores más importante de las redes inalámbricas es la cobertura. La cobertura de la red depende tanto del alcance de los adaptadores de red (las tarjetas Wi-Fi), como del de los puntos de acceso.

Los fabricantes anuncian que un punto de acceso o una tarjeta Wi-Fi llega a tener una cobertura de cientos de metros en espacio abierto con visibilidad directa entre terminales y sin interferencias de otros equipos que trabajen en la banda de 2,4 GHz (microondas, teléfonos inalámbricos, etc.). Esto es cierto, pero, si se instala el punto de acceso en el interior de una casa u oficina, el alcance puede reducirse a unos 25 a 50 metros dependiendo de los obstáculos que haya en la habitación (armarios, mesas, etc.).

Por otro lado, la mayoría de los equipos Wi-Fi vienen equipados con un sistema que baja automáticamente la velocidad de transmisión conforme la señal de radio se va debilitando. Esto significa que, conforme se aumenta la distancia entre emisor y receptor, se puede ir disminuyendo la velocidad de transmisión de datos.

Además de la distancia, en el entorno existen otros factores que pueden afectar a la cobertura, como son las interferencias (naturales y artificiales) o las pérdidas de propagación debido a los obstáculos. De hecho, muchas de estas condiciones del entorno son cambiantes, por lo que en una posición puede haber cobertura en un momento dado y no haberla unos minutos más tarde. Por ejemplo, puede que no tenga cobertura en la cocina cuando tenga puesto el microondas, pero sí el resto del tiempo; o puede que no tenga cobertura en una zona del patio cuando en primavera los árboles la dejan completamente en sombra radioeléctrica, pero sí el resto del año.

La conclusión es que, a poco que se complique la visibilidad entre los terminales (por distancia, por los obstáculos o por las interferencias), la única manera de saber exactamente si existe cobertura entre ellos es instalando los equipos y haciendo una prueba real de cobertura.

LAS INTERFERENCIAS

Dado que 802.11b utiliza la banda de 2,4 GHz y que estas frecuencias se encuentran en una banda abierta para usos industriales, científicos y médicos para los que no se necesita licencia, existe el riesgo de coincidir en el uso de la frecuencia con otros sistemas como los microondas, teléfonos inalámbricos, sistemas de televigilancia, dispositivos bluetooth o, incluso, otras redes inalámbricas. Estos otros usos pueden producir interferencias en las señales de radio de nuestra red. Una interferencia consiste en la presencia no deseada de señales radioeléctricas que interrumpen el normal funcionamiento del sistema.

Para evitar que una interferencia pueda cortar la comunicación, cuando el equipo Wi-FI (protocolo MAC) detecta la presencia de una señal de' interferencia, automáticamente entra en un periodo de espera en la idea de que, pasado dicho periodo, habrá pasado la interferencia. Evidentemente, esto hace que el servicio se degrade, pero no se interrumpe.

Desde el punto de vista del usuario, es imposible evitar las interferencias esporádicas, pero lo que sí se puede evitar son las interferencias constantes o periódicas. El sistema consiste en hacer pruebas de recepción de señal en la zona bajo sospecha. Estas pruebas pueden realizarse a distintas horas del día. A veces ocurre que las interferencias sólo se producen a la hora de la comida (microondas). Muchas de estas interferencias pueden evitarse sencillamente situando el punto de acceso en otro lugar, o moviendo el terminal.

Debido a la naturaleza de la tecnología de radio, las señales de radio frecuencia pueden desvanecerse o bloquearse por materiales medioambientales. La inspección in situ nos ayudará a identificar los elementos que afecten negativamente a la señal inalámbrica .

La tabla siguiente muestra los materiales más comunes con los que puede existir algún tipo de dificultad para la transmisión y recepción de las radiofrecuencias, así como su nivel de interferencia.

MATERIAL	EJEMPLO	INTERFERENCIAS
Madera	Tabiques	Baja
Vidrio	Ventanas	Baja
Amianto	Techos	Baja
Yeso	Paredes interiores	Baja
Ladrillo	Paredes interiores y exteriores	Media
Hojas	Árboles y plantas	Media
Agua	Lluvia / niebla	Alta
Cerámica	Tejas	Alta
Papel	Rollos de papel	Alta
Vidrio con alto contenido en plomo	Ventanas	Alta
Metal	Vigas	Muy alta

Debido a que las redes inalámbricas operan en un espectro de frecuencias utilizado por otras tecnologías, pueden existir interferencias que pueden afectar negativamente al rendimiento.

Las tecnologías que pueden producir interferencias son las siguientes:

- Bluetooth
- Hornos Microondas
- Algunos teléfonos DECT inalámbricos
- Otras redes WLAN

EQUIPO NECESARIO PARA WI-FI

Certificación de Equipo Wi-Fi

Wi-Fi, o "Wireless Fidelity", es una asociación internacional sin ánimo de lucro formada en 1999 para asegurar la compatibilidad de los distintos productos de redes de área local inalámbrica basadas en la especificación IEEE 802.11. Esta alianza está formada actualmente por 183 miembros, y desde que comenzó la certificación de productos en marzo de 2,000,698 productos llevan el certificado Wi-Fi, asegurando la compatibilidad entre todos ellos.

La alianza Wi-Fi se estableció originalmente como WECA (Wireless Ethernet Compatibility Alliance) en agosto de 1999, por varias compañías líderes en tecnología en redes inalámbricas. Desde 1999, el número de miembros de la alianza Wi-Fi se ha incrementado dado que cada vez más compañías de productos electrónicos de consumo, proveedores de servicios de red y fabricantes de ordenadores se han dado cuenta de la necesidad de ofrecer a sus clientes compatibilidad inalámbrica entre sus productos.

Wi-Fi utiliza la tecnología de radio denominada IEEE 802.11b,802.11a, 8011g ofreciendo seguridad, fiabilidad, y conectividad tanto entre equipos inalámbricos como en redes con hilos (utilizando IEEE 802.3 o Ethernet). Las redes Wi-Fi operan en las bandas de 2.4 y 5 GHz (no es necesario disponer de licencia), con una velocidad de 11Mbps (802.11b) o 54Mbps (802. 11a,g), ofreciendo un funcionamiento similar al de una red Ethernet.

Aunque lo más probable es que los equipos de diferentes fabricantes que cumplan técnicamente los mismos estándares sean compatibles, el certificado Wi-Fi asegura que no presentan ningún tipo de incidencias al trabajar conjuntamente en una red. Los aspectos que debe cubrir un equipo para obtener el certificado Wi-Fi son:

- Diversas pruebas para comprobar que sigue el estándar Wi-Fi.
- Pruebas rigurosas de compatibilidad para asegurar la conexión con cualquier otro producto con certificado Wi-Fi y en cualquier espacio (casa, oficina, aeropuerto, etc.) equipado con un acceso Wi-Fi.

Para que un equipo reciba el logotipo Wi-Fi es necesario que sea probado y verificado en los laboratorios de pruebas de esta asociación, asegurando que los productos con el logotipo Wi-Fi trabajan perfectamente unos con otros. Una vez que el producto inalámbrico pasa el proceso de pruebas, la compañía obtiene el sello Wi-Fi que se muestra en la figura 3.4 para dicho producto y puede utilizarlo con él. Es importante resaltar que el certificado lo recibe un producto en concreto, y no una familia de productos. Cada vez que el fabricante modifique alguno de sus componentes, el producto debe pasar por todo el programa de pruebas antes de obtener de nuevo el certificado Wi-Fi.

Para asegurar la compatibilidad, la alianza Wi-Fi trabaja con grupos técnicos de estándares como IEEE, y con compañías que trabajan en el desarrollo de futuras generaciones de redes inalámbricas. Este esfuerzo de cooperación asegura que los equipos trabajen con éxito en cualquier entorno Wi-Fi.

Fig 3.4 Logotipo certificado Wi-Fi

Hoy en día es posible encontrar espacios públicos equipados con redes inalámbricas Wi-Fi como cafeterías, hoteles, aeropuertos, etc., debido a que cada vez más viajeros y profesionales reclaman un acceso a Internet allí donde se encuentren. Estas zonas Wi-Fi ofrecen acceso rápido y flexible a Internet. Básicamente sus características son:

- Acceso sencillo a Internet, sin problemas de conectividad con el equipo Wi-Fi que disponga, a través de un acceso de banda ancha.
- Una velocidad de entre 11 y 54 Mbs.
- Una conexión estable, a prueba de curiosos. Todas las zonas Wi-Fi soportan conexiones de redes privadas virtuales (VPN) que refuerzan la seguridad.

El Punto de Acceso más adecuado para nuestras necesidades

El punto de acceso es el centro de las comunicaciones de la mayoría de las redes inalámbricas. El punto de acceso no sólo es el medio de intercomunicación de todos los terminales inalámbricos, sino que también es el puente de interconexión con la red fija e Internet.

Existen dos categorías de puntos de acceso:

- Puntos de acceso profesionales, diseñados para crear redes corporativas de tamaño medio o grande. Éstos suelen ser los más caros, pero incluyen mejores características (aunque sean particulares del fabricante), como son mejoras en la seguridad y una más perfecta integración con el resto de equipos. Los líderes de este tipo de equipamiento son Cisco, 3Com, Agere/Orinoco (antiguamente conocidos como Lucent) y Nokia.
- Puntos de acceso económicos dirigidos a cubrir las necesidades de los usuarios de pequeñas oficinas o del hogar. Estos puntos de acceso ofrecen exactamente los mismos servicios que los anteriores, con la misma cobertura y las mismas velocidades. La diferencia se nota cuando se dispone de un gran número de usuarios. En estos casos, los puntos de acceso profesionales ofrecen mejores resultados, eso sí, multiplicando el precio por cuatro o cinco. Los que más puntos de acceso de tipo económico venden son Intel, 3Com, D-Link, Agere/Orinoco, NetGear Proxim y Linksys.

Aparte de lo anterior, cada equipo tiene sus propias características externas. Por ejemplo, algo que diferencia claramente a unos puntos de acceso de otros es el número y tipo de puertos exteriores que ofrece. Existen puntos de acceso que disponen hasta de un puerto de impresora (con su servidor de impresión), mientras que otros se limitan a ofrecer una conexión para red cableada o Internet.

Por otro lado, es habitual que los puntos de acceso se utilicen también como pasarela de conexión con otras redes (por ejemplo, con Internet). Desde este punto de vista, es importante que se tengan en cuenta dos cosas: la primera es que nos fijemos en las características de *router* del punto de acceso: DHCP, NAT o propiedades de *firewall* son características que nos ayudarán en la configuración y manejo de las comunicaciones con Internet o con otras redes.

En el entorno corporativo suelen coexistir una red inalámbrica, para darle movilidad a los usuarios que la necesitan, junto con una red cableada, para darle conectividad al resto de usuarios. Generalmente, las redes corporativas utilizan el protocolo TCP/IP; no obstante, hay que tener en cuenta que en el mercado existen otros protocolos como SPX/IPX, NetBIOS, LANtastic, etc. Por tanto, conviene comprobar que el punto de acceso que se va a comprar sea compatible con el protocolo de red cableada con el que se va a conectar.

Por último, los equipos Wi-Fi tienen la ventaja de que tienen la garantía de interfuncionar sin problemas de acuerdo con la norma IEEE 802.1 lb. Esto es así, sin duda, en relación con los adaptadores de red; sin embargo, existe cierta incompatibilidad en relación con los puntos de acceso. La incompatibilidad aparece a la hora de mantener en servicio una comunicación cuando un usuario pasa del área de cobertura de un punto de acceso al de otro (a esto se le llama *roaming* en inglés). En este caso, silos puntos de acceso son de distinto fabricante, es muy posible que se corte la comunicación. La comunicación se podrá volver a establecer con el nuevo punto de acceso, pero no se habrá producido una transferencia sin interrupciones, que es de lo que se trata. Para evitar este problema, es recomendable que los puntos de acceso vecinos sean del mismo fabricante. Además, cuando todos los dispositivos son del mismo fabricante, es posible utilizar alguna característica adicional propietaria del fabricante. Se puede valorar si esto merece la pena.

En cualquier caso, el IEEE esta trabajando para solucionar este problema (grupo de trabajo IEEE 802.11 f). Por cierto, esto no tiene nada que ver con las tarjetas inalámbricas que se conectan a los ordenadores; estas últimas si pueden proceder de fabricantes distintos sin problemas.

Características Principales de los Puntos de Acceso

Los puntos de acceso son realmente unas pequeñas cajas de las que sobresalen una o dos antenas. Algunos fabricantes se han preocupado incluso de darles una forma estilizada que se salga de la forma típica de caja. Aunque la estética exterior de la caja pueda parecer un hecho sin importancia, en las redes para el hogar puede ser un punto a valorar. Por otro lado, a veces la estética es algo más que las apariencias. Unos puntos de acceso incluyen útiles para poderlos soportar en la pared o en el techo, mientras que otros carecen de este tipo de accesorios.

En cualquier caso, en su interior podemos encontrar lo mismo:

- Un equipo de radio (de 2,4 GHz, en el caso de 802.11b o 5 GHz, en el caso de 802.11a,g)
- Una o dos antenas (que pueden o no apreciarse exteriormente)

- Un *software* de gestión de las comunicaciones

- Puertos para conectar el punto de acceso a Internet o a la red cableada

La radio

El objetivo principal de los puntos de acceso es comunicarse con los terminales vía radio Por tanto, lo principal de los puntos de acceso es su equipamiento de radio. Este equipamiento viene integrado en un conjunto de *chips* electrónicos conocidos como *chipsets.* Aunque en el mercado existen muchos fabricantes de puntos de acceso, son muchos menos los que fabrican *chipsets.* Dos de los principales fabricantes de *chipsets* Wi-Fi son Lucent e Intersil.

Desde el punto de vista del usuario, el funcionamiento de los distintos *chipsets* es idéntico. Además, entre ellos deben ser compatibles. No obstante, la teoría de la compatibilidad trae sorpresas a veces, por lo que resulta recomendable comprar equipos puntos de acceso y tarjetas inalámbricas) que utilicen *chipsets* del mismo fabricante. La única forma de estar seguros de esto es comprar todo el equipamiento del mismo fabricante. Esto puede ser un contrasentido desde el punto de vista de la compatibilidad de la marca Wi-Fi, pero tiene sus ventajas prácticas.

Los Puertos con que debe contar un Punto de Acceso

Los puntos de acceso necesitan disponer de puertos para poderse conectar con una red local cableada y con Intemet. Para conseguir esto, los puntos de acceso suelen traer uno o más puertos 10/100Base-T (RJ-45). No obstante, las posibilidades de conectividad de los puntos de acceso no acaban aquí; dependiendo del modelo, nos podemos encontrar con los siguientes puertos:

- Un puerto especial para conectarse a un *hub* o *switch* de red de área local Ethemet *(uplink port).*

- Disponer internamente de un *huh,* por lo que ofrecen de dos a cuatro puertos exteriores para conectarles los equipos de red Ethernet de que disponga el usuario. Esto es ideal para el hogar o la pequeña oficina ya que evita la necesidad de disponer de un *hub* o *switch* independiente. En cualquier caso, si se necesitase de más de cuatro puertos, siempre se puede comprar otro *hub* y conectarlo al punto de acceso para extender la red.

- Un puerto serie RS-232 para que se le pueda conectar un módem de red telefónica (RTB o RDSI). Esta conexión a Internet a *56* Kbps o 64 Kbps puede ser utilizada como acceso principal a Internet o como acceso de seguridad en el caso de que falle la conexión de banda ancha (ADSL o cable módem).

- Un puerto paralelo o USB para conectarle una impresora. Esto permite compartir una impresora sin la obligación de tener un ordenador encendido para poder mantener disponible la impresora. Además, la impresora no le ocuparía recursos a ningún ordenador.

- Puerto para conectarle una antena exterior que le provea de un mayor alcance. En el mercado existe una gran variedad de antenas externas que pueden dar respuesta a muchas necesidades distintas. Si se necesita que el punto de acceso ofrezca cobertura a una distancia superior a unos 100 metros, es importante contar con un punto de acceso que disponga de un conector de este tipo.

Los puntos de acceso ofrecen determinadas características que son configurables, como son las opciones de seguridad o de gestión de la red. La mayoría permiten llevar a cabo esta configuración a través de una interfaz basada en páginas *web*. Para hacer uso de esto, sólo se necesita instalar el *software* que incluye el punto de acceso.

No obstante, es importante saber que algunos puntos de acceso no utilizan una interfaz *web*, sino que requieren de la introducción directa de líneas comandos (lo que se conoce como CLI, *Command Line Interface*, 'Interfaz de Línea de Comandos') o, incluso, requieren de un sistema operativo particular. Por ejemplo, Airport Base Station de Apple requiere disponer de un ordenador con sistema operativo Mac. En cualquier caso, siempre es buena idea asegurarse de que el punto de acceso es compatible con nuestro sistema operativo.

Los punto de acceso o pasarela inalámbrica su funcionalidad básica consiste en:

- Realizar la conversión de la señal de datos Ethernet a señales de radio (IEEE 802.11 para el caso de redes Wi-Fi), pudiendo ser un punto de conexión entre ambas redes (con hilos e inalámbricas).
-
- Actúa como elemento de interconexión entre diferentes clientes inalámbricos.
- Proporcionan un área de cobertura para los clientes inalámbricos. El espacio cubierto dependerá de la capacidad del equipo y sobre todo del entorno físico que se quiera cubrir: espacios exteriores o interiores con más o menos obstáculos.
- Pueden ofrecer funciones de "firewall" que permite aumentar la seguridad de la red. También pueden ofrecer mecanismos de autenticación para los clientes inalámbricos.
- Pueden ser configurados para crear diferentes escenarios de trabajo. Ofrecen facilidades de gestión.

Si es necesario ofrecer conexión inalámbrica a áreas más extensas, se pueden utilizar varias unidades bases conectadas entre sí, cada una cubriendo una parte del área total.

A continuación se muestran algunas fotografías de puntos de accesos ofrecidos por Telefónica.

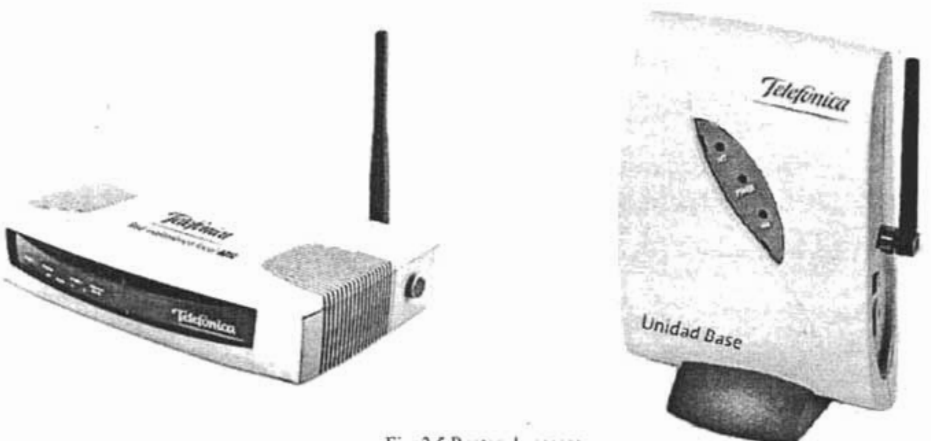


Fig. 3.5 Puntos de acceso

Adaptadores Inalámbricos de Red

Los adaptadores de red son las tarjetas o dispositivos que se conectan a los ordenadores para que puedan funcionar dentro de una red inalámbrica. Estos equipos pueden recibir también el nombre de tarjetas de red o interfaces de red. De hecho, en inglés se conoce como NIC *(Network Interface Cards,* 'Tarjetas Interfaces de Red') a cualquier tarjeta instalable o conectable a un ordenador que sirve para integrarlo en una red, sea ésta cableada o inalámbrica.

Los adaptadores de red son fundamentalmente unas estaciones de radio que se encargan de comunicarse con otros adaptadores (modo *ad hoc)* o con un punto de acceso (modo infraestructura) para mantener al ordenador al que están conectados dentro de la red inalámbrica a la que se asocie.

Como todos los equipos de radio, los adaptadores de red necesitan una antena. Esta suele venir integrada dentro del propio adaptador sin que externamente se note. Algunos adaptadores, sin embargo, permiten identificar claramente su antena. En cualquier caso, la mayoría de los adaptadores incluyen un conector para poder disponer una antena externa. Este tipo de antenas aumentan grandemente el alcance del adaptador.

Tipos de Adaptadores De Red

Al igual que desde hace tiempo viene siendo normal encontrar ordenadores que incluyen de fábrica una puerto Ethernet RJ45, recientemente están apareciendo en el mercado algunos ordenadores portátiles que ya tienen integrado un adaptador de red Wi-Fi. No obstante, éstos son todavía excepciones, lo normal es que el adaptador de red sea un equipo independiente que haya que instalar o conectar al ordenador o PDA.

Actualmente, existen los siguientes tipos de adaptadores inalámbricos de red:

- **Tarjetas PCMCIA.** Éstas son tarjetas que tienen un tamaño similar al de una tarjeta de crédito (realmente como un 30% más larga) y que se insertan en los puertos PCMCIA *(PC cara)* de tipo II que suelen incorporar la mayoría de los ordenadores portátiles. Se pueden encontrar tarjetas PCMCIA de Wi-Fi desde 30 euros (y el precio sigue bajando). Los ordenadores de sobremesa no suelen contar con puertos PCMCIA.

- **Tarjetas PCI o ISA.** Los ordenadores de sobremesa no suelen disponer de ranuras PCMCIA. De lo que sí disponen son de ranuras PCI o ISA donde se pueden instalar todo tipo de tarjetas de periféricos, entre las que están las tarjetas Wi-Fi. No obstante, lo cierto es que no es fácil encontrar en el mercado este tipo de tarjetas Wi-Fi. La solución alternativa consiste en instalar tarjetas conversoras de PCI o ISA a PCMCIA. Estos conversores son tarjetas PCI o ISA que se insertan en una ranura interna del ordenador y que ofrecen un puerto PCMCIA al exterior. El precio de estos adaptadores es de unos 40 euros. Evidentemente, adicionalmente haría falta disponer de la tarjeta PCMCIA.

- **Unidades USB.** Se trata de unidades inalámbricas que se conectan al ordenador (portátil o sobremesa) mediante un puerto USB. Estas unidades son más propias de los ordenadores de sobremesa, ya que evitan tener que instalar en su interior un adaptador de tarjeta PCMCIA. No obstante, son válidas para todo tipo de ordenadores. Si el ordenador ya tiene

ocupados todos sus puertos USB (por ejemplo, porque se está utilizando para el teclado, la impresora, etc.), en el mercado existen multiplicadores de puertos USB que permiten sacar cuatro puertos de donde había uno.

Tarjetas PCMCIA

Uno de los problemas que tenían antiguamente los ordenadores portátiles era que difícilmente podían ampliarse en sus prestaciones. Para instalarle una tarjeta de red o un módem a un ordenador de sobremesa, bastaba con añadir en su interior la tarjeta correspondiente (ISA, PCI, etc.). El interior de los portátiles, sin embargo, estuvo completamente cerrado hasta que aparecieron unos puertos especiales conocidos como PCMCIA *(Personal Computer Memory Card International Association,* 'Asociación Internacional de Tarjetas de Memoria para Ordenadores Portátiles'). En inglés se la conoce más coloquialmente como *PC Card* (tarjeta de PC).

Los puertos PCMCIA son una especie de ranura en la que se pueden insertar unas tarjetas del tamaño de una de crédito. Estas tarjetas quedan insertadas en el interior de la ranura, por lo que el ordenador portátil no pierde su integridad y fácil portabilidad. En el mercado existen muchos tipos de tarjetas PCMCIA: módem, tarjetas de red Ethernet, discos duros, etc.

Las tarjetas PCMCIA las crearon en 1989 una asociación de fabricantes de equipos con el propósito inicial de desarrollar una norma *hardware* y *sofware* para tarjetas de memoria intercambiables (de ahí su nombre). No obstante, la idea fue tan buena que se ha utilizado para todo tipo de periféricos.

Todas las tarjetas PCMCIA tienen un ancho de 54 milímetros, siendo su largo variable, pero con un mínimo de *85,6* milímetros. El hecho de ser variable se debe a que algunas tarjetas necesitan sobresalir hacía el exterior para mostrar algún tipo de conector, una antena o, simplemente, porque necesitan más espacio.

En cuanto al grosor de las tarjetas existen tres tipos: las tarjetas tipo I con un grosor de 3,3 milímetros (utilizadas, por ejemplo, para ampliaciones de memoria), las de tipo II con un grosor de 5 milímetros (son las habituales en los adaptadores de red inalámbricos) y las de tipo III con un grosor de 10,5 milímetros (utilizadas, por ejemplo, por los discos duros).

Por una razón exclusivamente de espacio, cada tarjeta requiere su propio tipo de ranura en el ordenador. Esto quiere decir que una ranura de tipo III admite cualquier tipo de tarjeta, mientras que una ranura de tipo I sólo admite tarjetas de este tipo. El tamaño más habitual de las tarjetas es el de tipo II.

Aparte del tamaño y del peso, otra de las características que aportan las tarjetas PCMCIA es su bajo consumo de energía y ser resistentes a los golpes típicos de los dispositivos móviles.

Por cierto, los adaptadores Wi-Fi PCMCIA suelen ser de tipo II (con *bus* de 32 bits tipo *CardBus) y* la mayoría de los ordenadores portátiles incluyen una o dos ranuras PCMCIA de este tipo. Si tiene un ordenador muy antiguo, será mejor que compruebe si admite este tipo de tarjetas antes de comprar el adaptador.

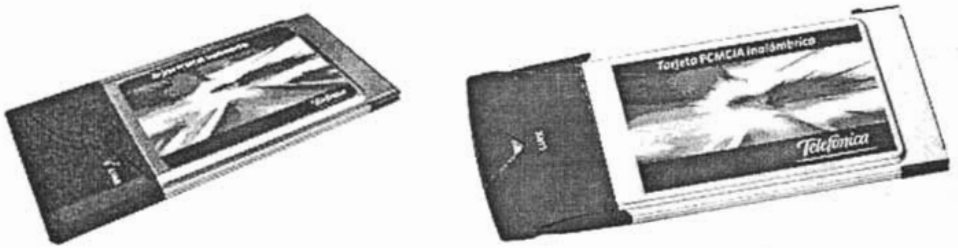


Fig 3.6 Tarjetas Wi-Fi PCMCIA

Adaptadores PCI e ISA

Los ordenadores de sobremesa no suelen incluir ranuras PCMCIA. Estos ordenadores suelen disponer de suficiente espacio interior como para admitir la instalación de nuevos periféricos a base de tarjetas tipo PCI *(Peripheral Components Interconnect,* 'Interconexión de Componentes Periféricos') o ISA *(Industry Standard Architecture,* 'Arquitectura Normalizada de la Industria'). Este tipo de tarjetas es más barata que las tarjetas PCMCIA, aunque también son mayores en tamaño y de instalación algo más compleja (entre otras cosas, hay que abrir el ordenador). Lo curioso en este caso es que difícilmente se encuentran en el mercado adaptadores inalámbricos de red de tipo PCI o ISA. El motivo quizás sea que las mayores prestaciones de las redes inalámbricas se consiguen con un ordenador portátil ("or aquello de la movilidad), así que el mayor mercado de adaptadores de red está hoy por hoy en el de las tarjetas PCMCIA, siendo relativamente pequeño el de las tarjetas PCI o ISA. ¿Cómo se conectan entonces los ordenadores de sobremesa a las redes inalámbricas? Pues con adaptadores USB o utilizando una tarjeta conversora de PCI o ISA a PCMCIA.

Una tarjeta conversora de PCI o ISA a PCMCIA es una tarjeta que se instala en el interior del ordenador en una de las ranuras PCI o ISA disponibles y que ofrece al exterior una ranura PCMCIA (generalmente de tipo II o III). Dicho de otra manera, este conversor le añade una ranura PCMCIA al ordenador.

Las tarjetas conversoras de este tipo suelen ser baratas, pero a este precio hay que añadirle el precio de la propia tarjeta PCMCIA, por lo que la conexión a la red inalámbrica del ordenador de sobremesa pasa a ser algo más cara que la del ordenador portátil.

El mayor inconveniente que presentan los dispositivos PCI e ISA es que requieren ser instalados en el interior del ordenador. Por tanto, hay que abrir el ordenador. Adicionalmente, incluso los que anuncian ser *Plug&Play* (tipo conectar y funcionar) finalmente requieren que se les instale el *software* de los controladores (por eso algunos los llaman *Plug&Pray,* conectar y rezar).

Por cierto, si se tiene un ordenador que dispone tanto de ranuras PCI como ISA, siempre es más aconsejable utilizar las de tipo PCI. Éstas suelen dar menos problemas de instalación y requieren menos recursos del sistema (una sola IRQ frente a las dos que requiere ISA). No hay más que pensar que ISA es un estándar de principios de los años ochenta, mientras que PCI es de principios de los años noventa (1993, exactamente). PCI file desarrollado por Intel como competidor al que poco antes se había convertido en el primer estándar de *bus* local, el estándar VESA *(Video Electronics Standard Association,* 'Asociación para la Normalización de la

Electrónica de Video'). La principal novedad que trajo PCI file el ser el primer sistema que permitia lo que se vino a llamar *Plug&Play* (conectar y funcionar).

Por cierto, ISA, también conocido como *bus* AT, puede transmitir información a una velocidad máxima de 16 MBps, mientras que PCI puede llegar a *528* Mbps.

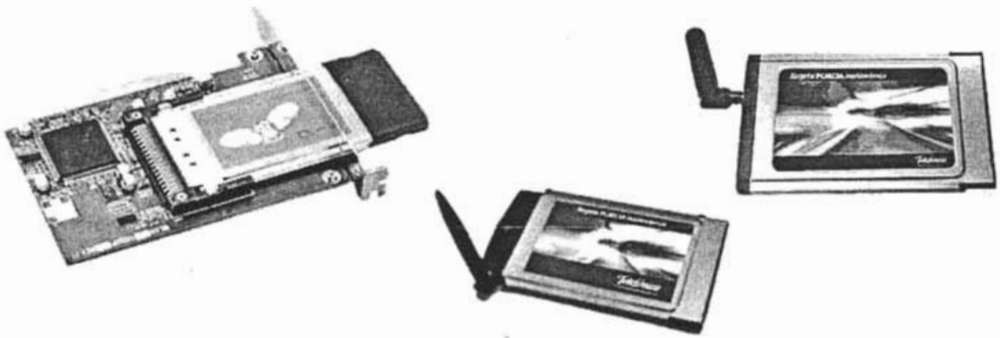


Fig 3.7 Tarjetas Wi-Fi PCI

Adaptadores USB

USB *(Universal Serial Bus,* 'Bus Serie Universal') es un nuevo puerto de comunicaciones que se diseñó para poder mejorar la forma en cómo los periféricos se conectaban a los ordenadores . Hasta que apareció USB en 1993, las únicas posibilidades de conectar un periférico a un ordenador eran mediante el puerto serie o el puerto paralelo (además del puerto del teclado/ratón y el puerto de juego). El inconveniente mayor con estos puertos es que sólo se podían conseguir velocidades de transmisión de 115 Kbps. Adicionalmente, los ordenadores sólo disponían de un puerto paralelo y dos series, con lo que el número de dispositivos a conectar se reducía a tres; además, son puertos que no le permiten al ordenador reconocer automáticamente el dispositivo que tienen conectado, ni alimentarlos a través del propio puerto

USB vino a traer las siguientes ventajas:

- No hace falta apagar el ordenador para conectar o desconectar un periférico
- USB.
- El ordenador reconoce automáticamente los periféricos que se conectan mediante USB. Si es preciso, instalan automáticamente los controladores necesarios para hacerlo funcionar adecuadamente.
- Ofrecen una alta velocidad de transferencia de datos: hasta 12 Mbps.
- Permite conectar hasta 127 dispositivos USB. Incluso, aunque el ordenador disponga de un solo puerto, basta con instalar un multiplicador de puertos (un *hub)* para disponer de más puertos USB.

- Ofrece alimentación eléctrica a los periféricos a través del propio conector USB (hasta 500 mA).

- Los periféricos USB pueden apagarse automáticamente cuando detectan que no se están utilizando.

- Los periféricos USB se instalan automáticamente, sin necesidad de abrir el ordenador.

Todo lo anterior ha hecho que los periféricos USB hayan ido desplazando poco a poco al resto de periféricos del mercado, hasta el punto de que ya existen ordenadores que no disponen de puertos serie ni paralelo, sino sólo puertos USB. Hoy en día, prácticamente todos los tipos de periféricos ofrecen la posibilidad de ser conectados al ordenador a través de un puerto USB: impresoras, módem, escáneres, cámaras, discos duros, etc. El caso de los adaptadores de red inalámbricos no iba a ser menos.

Desde el punto de vista de los adaptadores de red inalámbrica, USB ofrece la ventaja de poder compartir el adaptador entre diferentes ordenadores según se necesite. Como instalar el adaptador es tan fácil como conectarlo al puerto USB, si un ordenador necesita conectarse a la red, se le enchufa el adaptador y listo. Cuando no lo necesite, con desenchufarlo del puerto USB se tiene bastante.

Otras de las ventajas es que el adaptador puede reorientarse con respecto al punto de acceso para buscar una mejor cobertura, sin tener que mover el ordenador.

El único inconveniente de los adaptadores USB es que son dispositivos externos al ordenador. No quedan integrados dentro de él como lo hacen los adaptadores PCMCIA, PCI o ISA.

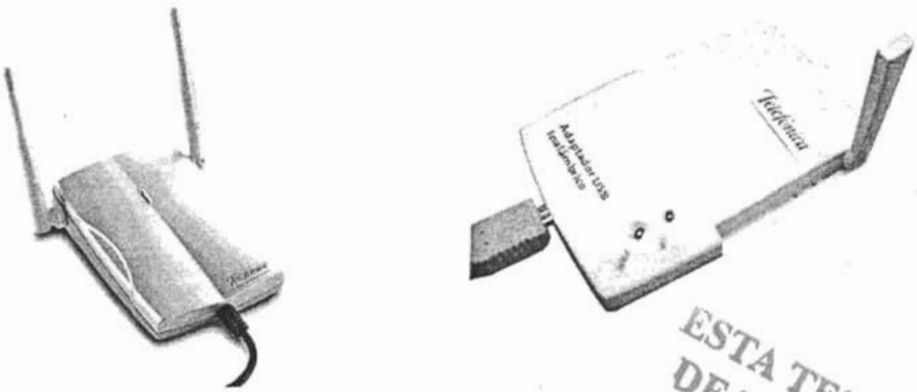


Fig. 3.8 Adaptadores USB para redes Wi-Fi

Adaptadores para PDA

Un PDA es un pequeño ordenador que cabe en la palma de la mano; de hecho, en inglés también se les conoce como *PalmFC*, literalmente, 'PC de la palma de la mano', y el PDA más vendido es el Palm Pilot de 3Com. Es cierto que también se les conoce como *PocketPC* (PC de bolsillo) o como *HandHeld PC* (PC de mano).

Debido a su pequeño tamaño, los PDA pueden llevarse siempre encima, por lo que suelen incluir aplicaciones que, de alguna manera, son asistentes personales de su usuario: agenda de direcciones, agenda de actividades, lista de tareas, juegos, etc. No obstante, un PDA puede utilizarse también como herramienta de comunicación: permite acceder a Internet, ver páginas *web*, gestionar correos electrónicos, etc. De hecho, las nuevas PDA incluyen versiones reducidas de programas de gestión tan conocidos como Microsoft Word, Excel, etc. En definitiva, un PDA es un pequeño ordenador de gran utilidad debido precisamente a su pequeño tamaño.

Habitualmente, un PDA se conecta a Internet a través de un ordenador personal. Los correos se escriben en el PDA, pero no se transmiten (o reciben) hasta que no se conectan mediante un cable (o infrarrojos) al ordenador personal con el que se ha asociado previamente. También existe la posibilidad de conectarle un módem especial al PDA y acceder directamente a Internet a través de un proveedor de acceso (vía llamada telefónica). En este sentido, han aparecido más recientemente en el mercado equipos PDA que incluyen en su interior un terminal móvil, o teléfonos móviles que incluyen en su interior las capacidades de los PDA.

Cualquiera de las soluciones anteriores tiene un inconveniente y es que no permite que el PDA esté conectado a Internet permanentemente, al menos, sin pagar unas altas tarifas por las llamadas telefónicas (del móvil o del fijo). Por otro lado, salvo en el caso del PDA con móvil (con alto coste en llamadas), el PDA siempre estará conectado por cable para intercambiar sus datos con el ordenador asociado o conectarse a Internet. Pues bien, las redes inalámbricas le ofrecen al PDA la posibilidad de liberarse de las ataduras del cable.

En el mercado existen módulos adaptadores de red inalámbrica para los principales modelos de PDA: 3Com, Compaq, HP, Casio, etc. A la hora de comprar uno de estos dispositivos, es conveniente asegurarse de que es el adecuado para el modelo concreto de PDA de que se dispone. Estos módulos suelen ser tarjetas de tipo Compact Flash con una pequeña antena exterior.

Bridges

Un *bridge* ('puente') es un dispositivo que interconecta dos redes. Una vez interconectadas, los equipos de una red pueden ver y comunicarse con los equipos de la otra red como si todos formaran parte de la misma red. La mayoría de los puntos de acceso hacen las funciones de *bridges* al poder interconectar una red local cableada con la red inalámbrica. Esto hace posible que los ordenadores de la red inalámbrica utilicen las impresoras de la red cableada o accedan a los archivos de cualquiera de sus ordenadores.

No obstante, existe un equipo conocido como *bridge* inalámbrico *(Wireless Bridge)* que es algo distinto de un punto de acceso. Un *bridge* inalámbrico interconecta dos redes remotas (cableadas o no) mediante una conexión inalámbrica. Estas dos redes pueden ser interconectadas también mediante cable, pero los *bridges* inalámbricos evitan la necesidad de tener que instalar o alquilar el cable.

La solución inalámbrica requiere de dos equipos *bridges* inalámbricos, uno en cada extremo. En cualquier caso, estos equipos pueden ser utilizados para extender el área de cobertura de una red inalámbrica, sobre todo cuando se trata de interconectar zonas localizadas en edificios distintos o que no tienen una visibilidad directa para poder utilizar antenas externas direccionales.

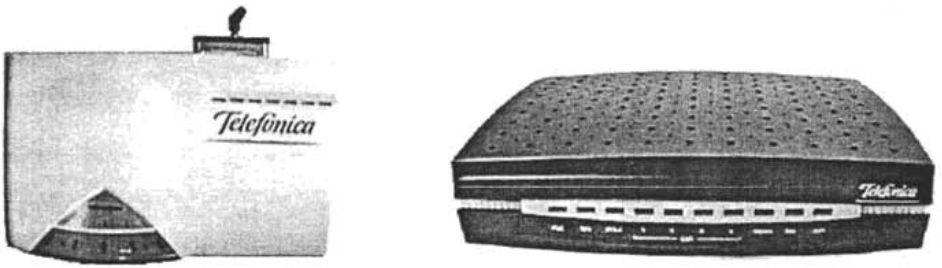


Fig. 3.11 Puentes inalámbricos

El Software

Para instalar y hacer funcionar una red inalámbrica, no hace falta más que el *software* que viene incluido con el propio equipamiento. Como mucho, es posible que haga falta acceder a la *web* del fabricante de algún adaptador de terminal para bajarse el controlador de dispositivo necesario para nuestro sistema operativo. Por tanto, la necesidad del *software* no viene por hacer funcionar la red, sino por conseguir unas características de gestión más adecuada a nuestras necesidades.

En el mercado existe una variedad de *software* muy útil para analizar y gestionar la red inalámbrica. Entre otras cosas, este *software* sirve para identificar posibles huecos en la seguridad de la red o para identificar redes activas en el entorno. Esto quiere decir que el *software* sirve tanto para piratear las redes de otros como para asegurar la nuestra.

Lo cierto es que todavía queda mucho por hacer en cuanto a *software* de análisis y gestión de redes inalámbricas; no obstante, actualmente ya se puede encontrar alguna buena herramienta, incluso de tipo *freeware* (gratuita) o *shareware* (probar antes de comprar).

Antenas

Una antena es un dispositivo que permite la emisión y recepción de ondas electromagnéticas (ondas de radio). Esto quiere decir que las antenas convierten las señales eléctricas en ondas electromagnéticas, y viceversa.

Todos los equipos Wi-Fi ya incorporan sus propias antenas. No obstante, cuando se desea disponer de una red de mayor alcance o cobertura, a veces, resulta conveniente sustituir la antena incorporada en el equipo Wi-Fi por otra exterior con mayor ganancia

La mayoría de las antenas que incorporan los equipos Wi-Fi son antenas internas. Esto quiere decir que son antenas que vienen incluidas dentro de la unidad del punto de acceso o del adaptador de red (tarjeta PCMCIA o dispositivo USB). Las antenas internas ofrecen la gran ventaja de la comodidad al formar parte del propio dispositivo, pero tienen el inconveniente del alcance. Si se necesita aumentar el alcance sin instalar nuevos puntos de acceso, la mejor solución es colocar una antena externa. Con una buena antena externa, la señal Wi-Fi de un punto de acceso puede llegar a

superar los 15 kilómetros de alcance siempre que no haya obstáculos, como edificios o árboles, y que la antena esté bien colocada.

La mayoría de los puntos de acceso y de los adaptadores de red admiten que se les conecte una antena externa. Existen antenas externas tanto para interiores como para exteriores de edificios .

Una antena es un dispositivo (generalmente formado por una o más varillas) destinado a la radiación y/o captación de ondas radioeléctricas. La antena de un equipo emisor radia las ondas radioeléctricas, mientras que la antena de un equipo receptor las capta. Un mismo equipo de radio, y su antena, puede ser utilizado tanto para transmitir como para recibir. Por cierto, a esto se le llama *transceiver (transmiter-receiver,* 'transmisor-receptor').

Una comunicación en la que la información fluye en ambas direcciones recibe el nombre de bidireccional. No obstante, cuando la transmisión y recepción no se efectúa simultáneamente, sino alternativamente, se obtiene lo que se conoce como comunicación semidúplex *(half-dupplex* en inglés). Las comunicaciones Wi-Fi son bidireccionales semidúplex.

En el mercado existen muchos tipos de antenas que pueden funcionar bien en los entornos Wi-Fi. No obstante, antes de lanzarse a comprar, conviene tener claro algunos conceptos generales que nos ayudan a comprender mejor las características de los distintos tipos de antena.

Tipos de Antenas

En el mercado existen tantos tipos de antenas como ha permitido la imaginación: yagui, de panel, parabólica de disco, parabólica de rejilla, de techo, *patch,* dipolo, planas, compactas, móviles, sectoriales, espiral, guía-onda, anular, etc. No obstante, todos estos tipos de antenas pueden agruparse en dos tipos primarios: omnidireccional y direccional.

Las antenas omnidireccionales son aquéllas que radian en todas direcciones y también pueden captar la señal procedente de todas las direcciones. Por el contrario, las antenas direccionales concentran su radiación en una dirección y sólo pueden captar la señal procedente de esa dirección. Las antenas direccionales tienen un mayor alcance (y ganancia) que las primeras a costa de concentrarse en una sola dirección.

En el caso de los equipos Wi-Fi, se suelen utilizar los tipos de antenas omnidireccionales para interiores y los tipos direccionales para exteriores.

Las antenas más habituales son las conocidas como dipolo. Un dipolo emite su señal haciendo que la energía se propague paralela al dipolo y perpendicular al suelo (polarización vertical). Si se girase la antena 90 grados, se obtendría una antena de polarización horizontal. Ambos modelos son posibles. Para cada caso particular un modelo puede funcionar mejor que el otro.

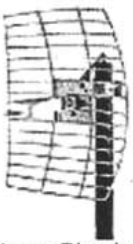
Las antenas direccionales concentran la energía en una sola dirección consiguiendo obtener incrementar el alcance. Cuanto más direccional es una antena, mayor es su alcance. Existen muy distintos modelos de antenas direccionales entre los que destacan los siguientes:

- La antena yagui es una antena direccional con una apertura de haz de entre 15 y 60 grados. Su ganancia varía entre los 6 y los 21 dBi. Estas antenas suelen venir montadas en el interior de una cobertura cilíndrica.

- La antena de panel tipo *patch* (parche) es una antena plana para ser montada en la pared. Esta antena emite energía siguiendo un modelo semiesférico. Tienen ganancias de entre 12 y 22 dBi. Su mayor inconveniente es que, al ser plana, puede sufrir por la fuerza del viento si se sitúan en el exterior.

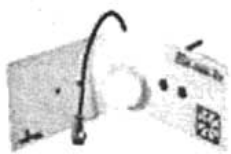
- La antena parabólica es una antena que tiene forma de disco cóncavo con la que se consigue unos haces muy direccionales. Es muy útil para comunicaciones punto a punto y se pueden conseguir ganancias de hasta 27 dBi. En el mercado existen distintas configuraciones de antenas parabólicas: redondas, mayadas, cuadradas, etc.

- Además de las anteriores, existen otros diferentes tipos de antenas (dipolos, reflectores, etc.) que pueden ser utilizadas en las instalaciones Wi-Fi. En cualquier caso, siempre es conveniente asegurarse que la antena está construida para funcionar en la banda de 2,4 GHz.



Antena Direccional

Antena Omnidireccional



Antena de panel tipo patch

Fig. 3.10 Antenas externas para Wi-Fi

La mayoría de los puntos de acceso vienen equipados con una doble antena. Esta doble antena se utiliza para obtener diversidad en la recepción. Cada antena, aunque sólo estén separadas unos centímetros, puede recibir la señal en muy distintas condiciones en cada momento. El sistema elige la mejor de las señales en cada momento evitando de esta forma muchos de los posibles problemas de mala recepción.

CAPÍTULO 4

SEGURIDAD Y APLICACIONES DE REDES Wi-Fi

No existe ningún sistema de seguridad que sea absolutamente impenetrable. Como sabemos, el objetivo de cualquier sistema de seguridad es permitir el acceso a cualquier persona autorizada e impedírselo a cualquier otra. Sin embargo, el simple hecho de que una persona puede entrar, aunque sea de forma autorizada, hace que el sistema deje de ser impenetrable. Si un intruso puede averiguar los pasos a dar para entrar legalmente, conseguirá romper la barrera.

Las comunicaciones inalámbricas tienen un inconveniente particular: carece de barreras físicas. Por tanto, cualquier persona, con unos conocimientos mínimos sobre seguridad y con una tarjeta Wi-Fi instalada en su ordenador puede, potencialmente, acceder a un punto de acceso de una red inalámbrica. No obstante, fundamentalmente, lo que hace que esto sea cierto es que muy pocos usuarios se toman en serio las medidas de seguridad. Por ejemplo, suele ser común que un usuario instale una red Wi-Fi sin modificar la configuración que trae el sistema por defecto. Si un intruso desea entrar en un sistema, lo primero que comprobará es si todavía tiene la configuración inicial.

Aparte de lo anterior, es cierto que la seguridad del sistema Wi-Fi no es de las mejores. Se le ha criticado extensivamente de ser un sistema muy débil, hasta el punto de que el IEEE ha creado un grupo de trabajo (802.11i) con el objetivo de proponer las medidas necesarias para conseguir un sistema Wi-Fi completamente seguro.

Por tanto, independientemente de que las redes inalámbricas sean más o menos seguras, lo que sí es cierto es que vienen provistas de medidas de seguridad para evitar que personas ajenas puedan hacer uso de la red. Estas medidas son lo suficientemente buenas como para que la inmensa mayoría de las personas que tenemos a nuestro alrededor no puedan entrar en la red.

SEGURIDAD EN LAS REDES INALÁMBRICAS

Como hemos visto, el riesgo de seguridad que resulta más evidente en las redes inalámbricas es el hecho de que, al estar formado por equipos que emiten los datos al entorno, cualquier receptor que, esté dentro del área de cobertura del emisor puede interceptar dichos datos e intentar interpretarlos.

Desde sus comienzos, 802.11 ha proporcionado algunos mecanismos de seguridad básicos para impedir que esta libertad mejorada sea una posible amenaza. Por ejemplo, los puntos de acceso (o conjuntos de puntos de acceso) 802.11 se pueden configurar con un identificador del conjunto de servicios (SSID). La tarjeta NIC también debe conocer este SSID para asociarlo al AP y así proceder a la transmisión y recepción de datos en la red. Esta seguridad, si se llegase a considerar como tal, es muy débil debido a estas razones:

- Todas las tarjetas NIC y todos los AP conocen perfectamente el SSID
- El SSID se envía por ondas de manera transparente (incluso es señalizado por el AP)

- La tarjeta NIC o el controlador pueden controlar localmente si se permite la asociación en caso de que el SSID no se conozca.

- No se proporciona ningún tipo de cifrado a través de este esquema.

Aunque este esquema puede plantear otros problemas, esto es suficiente para detener al intruso más despreocupado.

Las especificaciones 802.11 proporcionan seguridad adicional mediante el algoritmo WEP (Wired Equivalent Privacy). WEP proporciona a 802.11 servicios de autenticación y cifrado. El algoritmo WEP define el uso de una clave secreta de 40 bits para la autenticación y el cifrado, y muchas implementaciones de IEEE 802.11 también permiten claves secretas de 104 bits. Este algoritmo proporciona la mayor parte de la protección contra la escucha y atributos de seguridad física que son comparables a una red con cable.

Una limitación importante de este mecanismo de seguridad es que el estándar no define un protocolo de administración de claves para la distribución de las mismas. Esto supone que las claves secretas compartidas se entregan a la estación inalámbrica IEEE 802.11 a través de un canal seguro independiente del IEEE 802.11. El reto aumenta cuando están implicadas un gran número de estaciones, como es el caso de un campus corporativo.

Para proporcionar un mecanismo mejor para el control de acceso y la seguridad, es necesario incluir un protocolo de administración de claves en la especificación. Para hacer frente a este problema se creó específicamente el estándar 802.1x, que se describe más adelante en estas notas del producto.

El estándar IEEE 802.11 contempla tres mecanismos básicos de seguridad:

- SSDI *(Service Set Identifier,* 'Identificador del Conjunto de Servicios'), en ocasiones también se conocen como ESSID, en donde E quiere decir extendido. Es un código alfanumérico que se configura en cada ordenador y punto de acceso que forma parte de la red. Este código puede ser utilizado como una simple contraseña entre la estación y el punto de acceso o como un identificador del emplazamiento del emisor en una red pública. Existen puntos de acceso que permiten que se les deshabilite el sistema SSID. Lo cierto es que este sistema no garantiza excesivamente la seguridad, ya que los códigos SSID son emitidos en forma de texto sin codificar. Cualquier receptor con el *software* adecuado puede averiguar estos datos. De hecho, Windows XP incluye un programa que es capaz de detectar automáticamente estos códigos y mostrarle al usuario la lista de redes (lista de SSID) detectadas para que el usuario elija a cuál desea conectarse.

- Se puede generar una **lista de direcciones MAC** y limitar el acceso a la red a aquellos ordenadores contemplados en la lista. Las direcciones MAC están formadas por 12 caracteres alfanuméricos (por ejemplo, 12-AB-56-78-90-FE) e identifican a la tarjeta de los adaptadores de red. Las direcciones MAC no son modificables por el usuario. No obstante, es cierto que estas direcciones se transmiten en forma de texto sin codificar y, por tanto, son fácilmente leíbles con un receptor adecuado. Un intruso experimentado podría leer una dirección correcta, configurársela a su estación y acceder a la red sin problemas. Por cierto, las direcciones MAC no tienen nada que ver con la capa MAC del protocolo.

- La última medida de seguridad de Wi-Fi consiste en el algoritmo de cifrado WEP *(Wired Equivalency Protocol,* 'Protocolo de Equivalencia con Red Cableada'). Con este sistema se cifran todos los datos que se intercambian entre los ordenadores y los puntos de acceso. WEP utiliza el algoritmo de cifrado PRNG *(Pseudorandom Number Generation,* 'Generación de Números Pseudoaleatorios') RC4 desarrollado en 1987 por RSA Data Security. La utilización de la técnica de cifrado WEP es opcional.

Cifrado

De forma muy parecida en la que la industria WLAN ha adoptado el concepto de autenticación de una variedad de fuentes, también ha imitado el proceso de cifrado. La noción de usar un código para ocultar el significado de un mensaje que se envía a personas no intencionadas, o entrometidas, es casi tan vieja como la noción de enviar mensajes. El cifrado es la práctica de cambiar la información de forma que esté tan cerca como sea posible de ser imposible de leer sin la información necesaria para descifraría. Esta información puede ser una clave, secreto o código, además puede tomar la forma de un anillo decodificador de secretos o un libro de códigos. Generalmente, mientras más complicado sea el código, será más difícil descifrarlo. Además, mientras más complicado sea el código, codificar o decodificar la información normalmente consumirá más tiempo (o uso del procesador).

El tema del cifrado es bastante complicado y extenso por lo que no se trata a fondo en este trabajo de tesis. Sin embargo, existen algunos conceptos importantes que se deben conocer para desplegar una LAN Wi-Fi.

Un *cifrado* o *algoritmo* es una fórmula que se usa para generar un flujo de datos cifrados basado en una clave de cifrado. Estas claves de cifrado se pueden medir en términos de longitud; en general, mientras más grande sea la clave, será más complicado y robusto el código. En el mundo digital, la unidad de medida que se usa para las longitudes de claves son los bits. Por lo tanto, por ejemplo, una clave de 40 bits es menos robusta que una de 128 bits. Una clave de cifrado de 40 bits da como resultado 2^{40} (más de un billón) de combinaciones posibles. Una clave de 128 bits ofrece2^{128} combinaciones. Suponiendo que se usa el mismo algoritmo, una clave de 128 bits es 2^{88} veces más difíciles de romper que una clave de 40 bits. El Departamento de Comercio de los Estados Unidos, trabajando en conjunto con la Agencia Nacional de Seguridad, ha impuesto restricciones en las exportaciones a las tecnologías de cifrado basadas en la longitud de la clave, prohibiendo las exportaciones de mucho productos que usan claves de cifrado mayores a 64 bits de longitud, el famoso 'cifrado robusto". (Los productos Wi-Fi, los cuales están clasificados como productos de venta al público por el gobierno, están exentos de esta restricción y se pueden exportar incluso cuando proporcionen un cifrado sólido.)

Para crear el mensaje codificado, denominado *texto codificado,* se combina la clave de cifrado con el mensaje original, o *texto simple.* Existen dos tipos principales de cifrado. El *cifrado de flujo* que codifica el texto simple usando 1 bit a la vez. Y el *cifrado de bloque* que fragmenta el texto simple en bloques y luego los cifra bloque por bloque. Los cifrados de flujo se consideran más eficientes y rápidos, debido a que los cifrados de bloque introducen un paso extra al proceso, el cual impacta el desempeño pero incrementa la robustez. La combinación de la clave del cifrado y el texto simple se conoce como una función *OR exclusiva* (o, con mayor frecuencia, *XOR)* (vea la figura 4.1). Entonces, el texto de cifrado que se obtiene queda, en teoria, tan fuertemente cifrado como el número posible de combinaciones que la longitud de la clave supone.

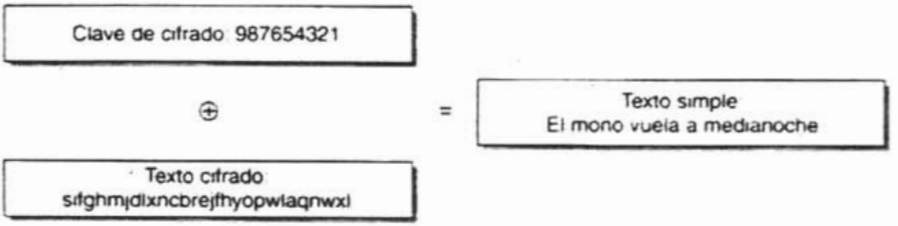


Fig. 4.1 Creación del mensaje codificado

En la figura 4.1 la combinación de la clave de cifrado y el texto simple a través de una función da como resultado el texto cifrado

Es razonable pensar que si el mismo mensaje se codifica con el mismo código, se obtendrá el mismo mensaje secreto (el mismo texto simple pasa a través de la función XOR con la misma clave que da como resultado el mismo texto cifrado). En términos de redes, este texto simple es un solo paquete, el cual a menudo se repite debido a los errores en la transmisión y a los envíos que esto implica. Esta representación frecuente de paquetes y la repetición resultante de texto cifrado proporcionan a los piratas informáticos mejores oportunidades de descubrir el código.

Una manera de resolver este problema es mediante el uso de un *vector de inicialización* el cual es un valor numérico de una longitud en bits determinada que se adjunta a la clave de cifrado (vea la figura 4.2). A diferencia de la clave de cifrado, el vector de inicialización sufre modificaciones frecuentemente(tan a menudo como el envío de cada paquete) y se envía en forma de texto simple de forma tal que pueda ser reconocido tanto en las estaciones emisoras como las receptoras. La modificación en el vector de inicialización produce los cambios en el flujo cifrado, lo cual da como resultado un texto cifrado distinto aún cuando el texto simple, o el paquete, sea exactamente el mismo.

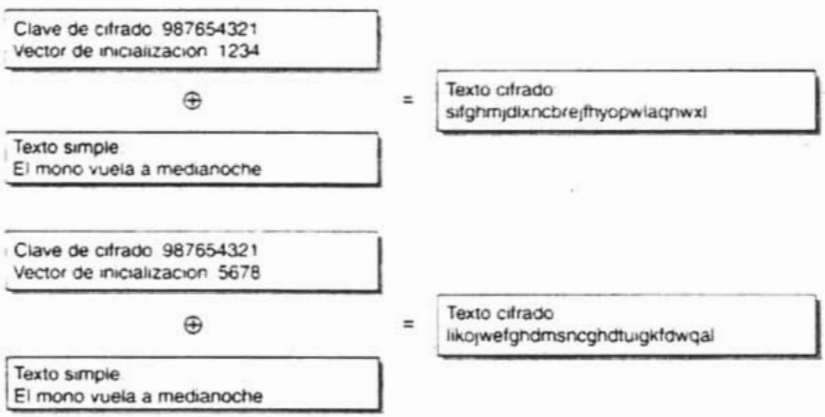


Fig 4.2 Vector de inicialización

En la figura 4.2 al adjuntar un vector de inicialización de texto simple al flujo cifrado, incluso el mismo flujo cifrado y mismo mensaje de texto simple da como resultado un texto cifrado distinto, lo cual disminuye la posibilidad de que se pueda descifrar el código.

Para la seguridad de redes inalámbricas, se utilizan 2 tipos de encriptación de llaves, basadas en claves de constante rotación. Estas son:

- WEP
- WPA.

WEP

El sistema de cifrado WEP consiste en aplicar a los datos originales la operación lógica XOR (O exclusiva) utilizando una clave generada de forma pseudoaleatoria. Los datos cifrados resultantes son los que se transmiten al medio.

Para generar la clave pseudoaleatoria, se utiliza una clave secreta definida por el propio usuario y un vector de inicialización (IV, *Initialization Vector).* La clave secreta es única y debe estar configurada en todos los ordenadores y puntos de acceso.

La longitud de los datos cifrados excede en cuatro caracteres a la longitud de los datos originales. Estos cuatro caracteres reciben el nombre de ICV *(Integrity Check Value,* 'Valor de Comprobación de Integridad') y se utilizan para que el receptor pueda comprobar la integridad de la información recibida..

Una vez que llegan al destino los datos cifrados, se combina el IV con la clave secreta (distribuida a todas las estaciones) para generar la semilla que permitirá descifrar los datos mediante el algoritmo PRNG.

Uno de los inconvenientes que tiene este sistema de cifrado es que la clave secreta es estática. Una vez asignada, se configura en cada estación (por el administrador o por cada usuario) y permanece invariable hasta que se vuelva a repetir este proceso manualmente. Si se perdiese una de las estaciones de la red, habría que volver a configurar una nueva clave en todas las estaciones para garantizar la seguridad.

Por otro lado, el IV se transmite en abierto a todas las estaciones. El IV sí cambia periódicamente.

Las claves de cifrado que usa WEP están basadas en el algoritmo de cifrado RC4, un cifrado de flujo diseñado por Ron Rivest (quien representa a la *R* en el acrónimo Seguridad RSA, una compañía de seguridad de datos con buena reputación y muy respetada). RC4 (cifrado 4 de Rivest) es un cifrado de flujo y se puede implementar usando varias longitudes de clave.

La implementación en WEP del algoritmo RC4 ofrece claves de cifrado que son de 40 bits de largo y tienen un vector de inicialización de 24 bits, lo cual da como resultado una clave de 64 bits de longitud en total. Muchos fabricantes han ido más allá del estándar para proporcionar claves que sean de 104 bits de longitud. lo que da como resultado una longitud de clave total de 128 bits cuando se añade el vector de inicialización. Para generar una clave WEP. se debe introducir una cadena alfanumérica -para los productos de algunos vendedores, en formato hexadecimal (número del cero al nueve, además de las letras de la A a la F), mientras que otros pueden usar cualquier cadena alfanumérica. Cuando la función WEP está activada, a cada estación (cliente o punto de acceso) se le asigna una clave común. Esta clave desordena los datos y se mezcla entre la información antes de ser transmitida, de tal modo que si una estación recibe un paquete que no está mezclado con la clave correcta, la estación descartará el paquete.

A la hora de la verdad, la instalación de esta función es opcional, aunque sumamente sencilla de poner en marcha. Simplemente habrá que seleccionar el tipo de encriptación WEP que se desea implementar, 40 o 128 bits, y a continuación elegir la clave que se utilizará. Obviamente, si la función WEP está activada en uno o más puntos de acceso, todos los dispositivos inalámbricos de la red deberán tener el mismo código WEP, que se establece fácilmente mediante las utilidades de software suministradas.

No obstante, existe la posibilidad de establecer una comunicación con células combinadas. Una célula combinada es una red de radio en la que algunos dispositivos utilizan WEP y otros no. Esta opción es posible mediante la simple activación del parámetro "Allow Association To Mixed Cells".

COMO FUNCIONA WEP

WEP utiliza el algoritmo RC4 para la encriptación con llaves de 64 bits, aunque existe también la posibilidad de utilizar llaves de 128 bits. Veremos que en realidad son 40 y 104 bits, ya que los otros 24 van en el paquete como Vector de Inicialización (IV).

Llaves

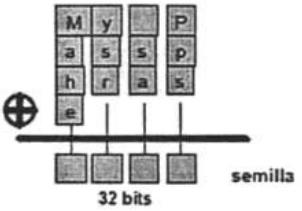
La llave de 40 ó 104 bits, se genera a partir de una clave (passphrase) estática de forma automática, aunque existe software que permite introducir esta llave manualmente.

La clave o passphrase debe ser conocida por todos los clientes que quieran conectarse a la red Wireless que utiliza WEP, esto implica que muchas veces se utilice una clave fácil de recordar y que no se cambie de forma frecuente.

A partir de la clave o passphrase se generan 4 llaves de 40 bits, sólo una de ellas se utilizará para la encriptación WEP.

Este es el proceso que se realiza para generar las llaves:

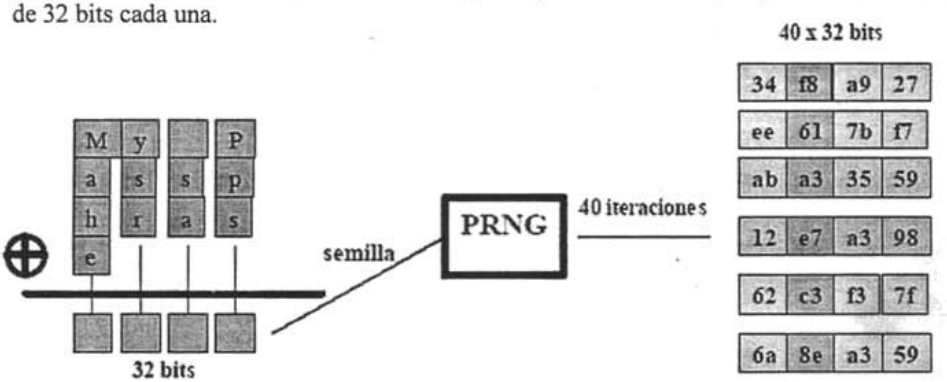
Se hace una operación XOR con la cadena ASCII (*My Passphrase*) que queda transformada en una semilla de 32 bits.



M	y		P	a	s	s	p	h	r	a	s	e
4D	79	20	50	61	73	73	70	68	72	61	73	65

```
4D XOR 61 XOR 68 XOR 65 = 21
79 XOR 73 XOR 72 XOR 0  = 78   } SEMILLA
20 XOR 73 XOR 61 XOR 0  = 32
50 XOR 70 XOR 73 XOR 0  = 53
```

El generador de números pseudoaleatorios (PRNG) utiliza la semilla para generar 40 cadenas de 32 bits cada una.



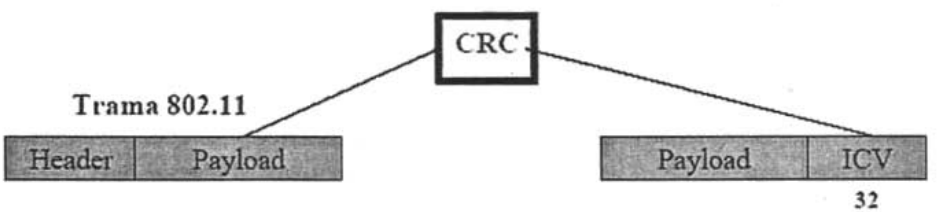
Se toma un bit de cada una de las 40 cadenas generadas por el PRNG para construir una llave y se generan 4 llaves de 40 bits.

De estas 4 llaves sólo se utilizará una para realizar la encriptación WEP como veremos a continuación.

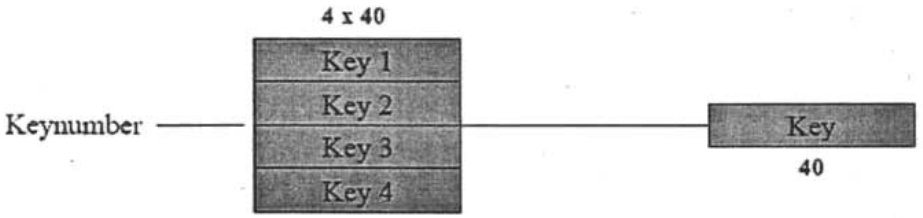
Encriptación

Para generar una trama encriptada con WEP se sigue el siguiente proceso:

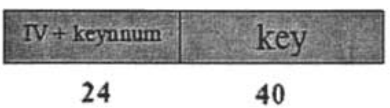
Partimos de la trama que se quiere enviar. Esta trama sin cifrar está compuesta por una cabecera (Header) y contiene unos datos (Payload). El primer paso es calcular el CRC de 32 bits del payload de la trama que se quiere enviar. El CRC es un algoritmo que genera un identificador único del payload en concreto, que nos servirá para verificar que el payload recibido es el mismo que el enviado, ya que el resultado del CRC será el mismo. Añadimos este CRC a la trama como **valor de chequeo de integridad** (ICV Integrity Check Value):



Por otra parte seleccionamos una llave de 40 bits, de las 4 llaves posibles:



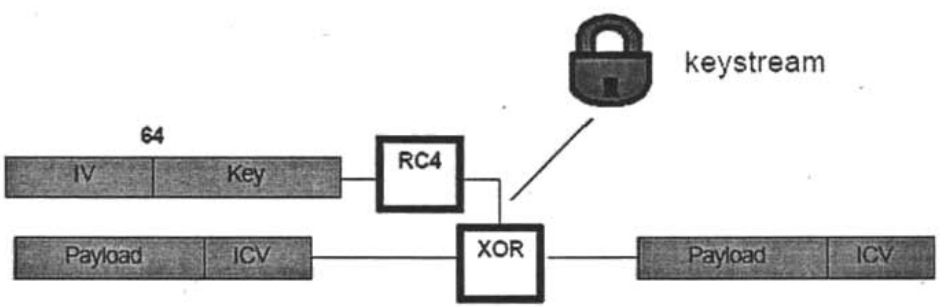
Y añadimos el **Vector de Inicialización** (IV) de 24 bits al principio de la llave seleccionada:



El IV es simplemente un contador que suele ir cambiando de valor a medida que vamos generando tramas, aunque según el estándar 802.11b también puede ser siempre cero. Con el IV de 24 bits y la llave de 40 conseguimos los 64 bits de llave total que utilizaremos para encriptar la trama. En el caso de utilizar encriptación de 128 bits tendríamos 24 bits de IV y 104 de llave.

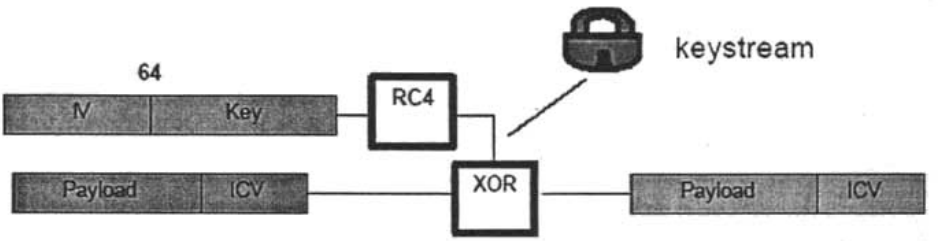
Llegado a este punto, aplicamos el algoritmo RC4 al conjunto IV+Key y conseguiremos el keystream o flujo de llave. Realizando una operación XOR con este keystream y el conjunto Payload+ICV obtendremos el Payload+ICV cifrado, este proceso puede verse en el siguiente grafico.

Se utiliza el IV y la llave para encriptar el Payload + ICV:

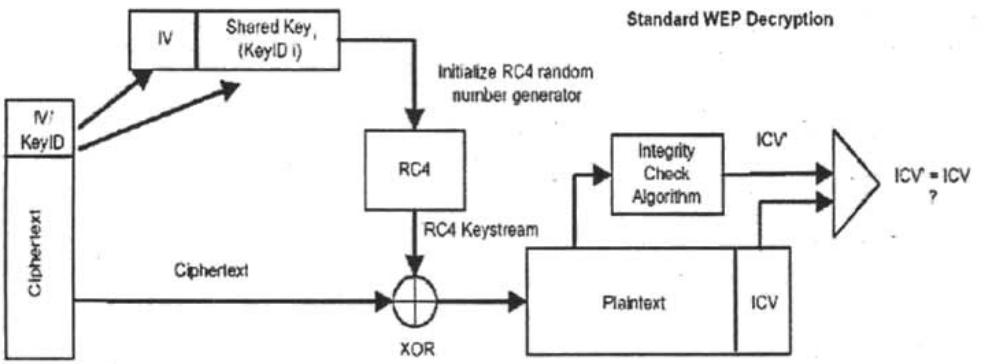


Después añadimos la cabecera y el IV+Keynumber sin cifrar. Así queda la trama definitiva lista para ser enviada:

(plaintext) realizando una XOR con el Payload+ICV cifrados y la llave completa como se describe a continuación.



Una vez obtenido el plaintext, se vuelve a calcular el ICV del payload obtenido y se compara con el original. El proceso completo puede verse en el siguiente esquema:



AUTENTICACIÓN 802.1 X

802.1X IEEE es un estándar ratificado por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) para el control de acceso a la red basado en puertos. Observe que pertenece al grupo de trabajo 802.1, y es parte de un conjunto de estándares de nivel básico que se aplican a una amplia variedad de estándares de red. De hecho, 802.1X fue diseñado originalmente para usarse con tecnologías cableadas como, por ejemplo, Ethernet. Sin embargo, debido a la confianza típica que tienen los profesionales IS en la seguridad física de los puertos cableados, como discutimos en el cuadro anterior, 802.lX fue visto por muchas personas como una solución que estaba en búsqueda de un problema.

Como hemos afirmado a lo largo de todo este libro, un tema que aparece en la historia de las WLAN es que copia tecnologías de áreas distintas con el fin de resolver problemas más rápida-

mente. Por esta razón, 802.IX fue adoptado por la industria inalámbrica como el medio principal de autenticar usuarios en la LAN.

La arquitectura 802.1X está compuesta de tres partes principales: un solicitante, un autenticador y un servidor de autenticación. Cuando se aplica a Wi-Fi, el solicitante reside en los dispositivos de cliente y el punto de acceso sirve como el autenticador. El solicitante normalmente es un fragmento pequeño de software que se ubica en el sistema operativo o el controlador de dispositivo que proporciona el fabricante del adaptador de cliente. El punto de acceso actúa como el portero de la LAN, permitiendo que el dispositivo de cliente obtenga el acceso a la LAN sólo después de que el cliente ha sido autenticado. Los servidores de Servicio de autenticación remota de usuario por medio del acceso telefónico *(RernoteAudieiitication Dial-In User Service, RADIUS,* por sus siglas en inglés), que inicial-mente fueron desarrollados para la autenticación de usuarios de red remotos que usaban una conexión telefónica hacia la red a través del sistema telefónico público inseguro, fueron mejorados para autenticar usuarios accediendo a la LAN a través de un medio igualmente inseguro -ondas de radio.

El proceso de autenticación de 802. IX cuando se aplica a las WLAN funciona de la manera siguiente:

1. El cliente obtiene el acceso al medio inalámbrico a través de CSMA/CA y crea una asociación con un punto de acceso.

2. El punto de acceso compatible con 802.IX acepta la asociación pero ubica al cliente en una "área de espera" sin estar autenticado. Para el cliente sin autenticación, el puerto virtual, es decir, la puerta de enlace, hacia la LAN está bloqueado. El punto de acceso envía una solicitud de identificación al cliente.

3. El cliente proporciona una respuesta de identificación que tiene el nombre de usuario o un identificador específico similar que no es secreto. Al recibir la respuesta de identificación, el punto de acceso reenvía esta respuesta a través del enlace cableado hacia el servidor RADIUS. Si un punto de acceso está configurado de manera que sólo acepte clientes compatibles con 802. IX y la respuesta de identificación del cliente no ha llegado, el cliente continúa asociado con el punto de acceso pero dentro del área de espera de manera indefinida sin ser autenticado (sin obtener acceso a la red).

4. El servidor RADIUS busca el ID de usuario en la base de datos. Es importante observar que los servidores RADIUS mismos no siempre incorporan una base de datos con ID de usuario y credenciales de autenticación, sino que acceden a estas credenciales que están en una base de datos separadas como, por ejemplo, Active Directory de Windows 2000 o la base de datos de los Servicios de dominio de NT. La ventaja de este enfoque es que una base de datos común, y a menudo preexistente, se puede habilitar de manera que soporte la autenticación inalámbrica además de la cableada. Esto permite la centralización de la autenticación de credenciales, y por lo mismo, la disminución de la carga administrativa.

5. Una vez que el ID de usuario ha sido identificado por el servidor RADIUS, comienza un proceso de interrogación al cliente (en donde el punto de acceso pasa las preguntas del servidor RADIUS al cliente). El cliente responde a estas preguntas hasta que llega el momento de que el servidor RADIUS determina que el cliente es en realidad legítimo. Debido a que 802.IX no especifica los tipos de autenticación, dejando este aspecto a los fabricantes individuales, pueden variar los medios a través de los cuales el cliente es interrogado, responde y la forma en que finalmente es autenticado en la LAN. Estas

implementaciones específicas para cada fabricante están fuera del alcance de este libro. Lo que es verdad es que en todos los casos la información que debe ser secreta como, por ejemplo, las contraseñas. no pasan a través de la WLAN en forma de texto simple. Tomando en cuenta que la información que pasa a través de la RF puede ser interceptada con relativa facilidad por los piratas informáticos, es obvio que enviar una contraseña de un cliente a un punto de acceso contradice el propósito mayor de una contraseña.

6. En las WLAN, no sólo el cliente debe estar autenticado en la LAN, la LAN también debe estar autenticada en el cliente. Es decir, existe la posibilidad de que un cliente se pueda asociar con un punto de acceso que no sea parte de la infraestructura de la empresa. De hecho, los *puntos de acceso ocultos* pueden estar instalados por el pirata informático con el propósito de interceptar la información de autenticación del cliente. Por lo tanto, cuando se aplica la autenticación 802.1 X en las WLAN, proporciona una autenticación mutua, el cliente en la red y la red en el cliente. Por lo tanto, el cliente inicia lo que es esencialmente el proceso inverso de interrogación y respuestas con el servidor RADIUS.

7. Una vez que el cliente ha sido autenticado en la red a través del punto de acceso y el servidor RADIUS, y la red ha sido autenticada en el cliente, se abre el puerto virtual en el punto de acceso y el cliente puede comenzar a acceder a la red inalámbrica y cableada.

EL ESTÁNDAR 802.11i

Reconociendo la necesidad de una arquitectura de seguridad mucho más robusta y escalable para las LAN Wi-Fi, el grupo 802.11 del IEEE votó para designar un grupo de trabajo especialmente para la seguridad, la cual ha sido parte de una tarea del grupo dedicado a la calidad de servicio. El grupo de trabajo 802.1 u (TGi en términos del IEEE) se formó en el año 2001 y, a pesar de que hasta la fecha no han entregado un estándar ratificado ha hecho mucho para proporcionar una seguridad empresarial que ofrezca *interoperabilidud.*

En pocas palabras, 802.11 i especifica a 802.1 X, junto con el Protocolo de autenticación extensible (EAP), como los medios mediante los cuales los clientes Wi-Fi y las redes se pueden autenticar mutuamente. Lo que es notable acerca del EAP es que el aspecto *extensible* del protocolo proporciona la flexibilidad de autenticar usando una variedad de maneras. Esto les ofrece a los fabricantes la libertad de ofrecer diferentes *tipos de autenticación* o *métodos de autenticoción* usando tipos distintos de credenciales. 802.1 li especifica RC4, el mismo algoritmo de cifrado que se usa para las claves WEP estáticas, como el algoritmo de cifrado para las claves dinámicas de cifrado de una sola sesión y un solo usuario.

WPA.

Después de lo visto, no es de extrañar que una de las mayores debilidades que siempre ha estado presente cuando se hablaba de Wi-Fi haya sido la seguridad. Este hecho no sólo ha preocupado a los usuarios de Wi-Fi, sino que también ha provocado la reacción de muchos

miembros de la alianza Wi-Fi (de WECA) para intensificar los trabajos que permitan crear un mecanismo que permita dotar a los productos certificados Wi-Fi de altos niveles de seguridad. El resultado es que la Alianza Wi-Fi, conjuntamente con el IEEE, ha sacado al mercado un nuevo sistema de seguridad para Wi-Fi conocido corno WPA *(Wi-Fi Protected Access,* 'Acceso Wi-Fi Protegido').

WPA son unas especificaciones basadas en el estándar IEEE 802.11 i que mejora fuertemente el nivel de protección de datos y el control de acceso de las redes inalámbricas Wi-Fi. La gran ventaja de WPA es que pueden aplicarse a las redes Wi-Fi existentes y que es completamente compatible con el futuro sistema de seguridad integrada proporcionado por IEEE 802.11 i.

WPA se puede instalar en los equipos Wi-Fi existentes de una forma tan sencilla como instalar un pequeño *software* en los equipos. Una vez instalado, el nivel de seguridad adquirido es extremadamente alto, asegurándose que sólo los usuarios autorizados pueden acceder a la red y que los datos transmitidos permanecen completamente inaccesibles para cualquier usuario que no sea el destinatario.

WPA se está empezando a implantar y se espera que a corto plazo sustituya a WEP.

El Protocolo de integridad de clave temporal *(Temporal Key Integritv Protocol, TKIP,* por sus siglas en inglés) es un medio parcial para "disminuir" las deficiencias de la implementación de RC4 en 802.11 para las claves de cifrado estáticas y, aún más importante, dinámicas. A finales del 2002, TKIP permaneció como un elemento definido de manera general en el esbozo del estándar 802.11i. TKIP también se basa en RC4 y está formado esencialmente de tres mejoras importantes en relación a la implementación inicial del algoritmo:

- Combinación de clave por paquete La clave de cifrado se combina con la dirección MAC de la estación emisora y un número de paquete secuencial para complicar aún más la clave básica, haciéndola más difícil de romper.

- Un vector de inicialización de 48 bits El doble de la longitud del vector de inicialización de 24 bits original que se especificó en el estándar WEP inicial. Recuerde que las longitudes de la clave tienen un efecto exponencial mientras que una clave de 24 bits tiene aproximadamente 16 millones de combinaciones, una clave de 48 bits proporciona cerca de 280 billones de combinaciones. La longitud más larga de esta clave, junto con la combinación de clave por paquete, hace que las claves de cifrado sean varios órdenes de magnitud más robustas que las implementaciones de generaciones anteriores.

- Comprobación de integridad de mensaje *(Message Integrity Checks, MIC,* por sus siglas en inglés) Está diseñada para frustrar los ataques inductivos o de hombre en el medio. La implementación MIC en TKIP es una versión de la siguiente generación llamada (de forma suspicaz) "Michael". Mediante un MIC, las direcciones de envío y recepción además de otra información única, se integra en la carga cifrada. Los cambios en esta información, que están asociados a la intercepción de un paquete, dan como resultado el rechazo del paquete y una alerta que indica que un ataque puede estar fraguándose.

Las mayores ventajas que aporta WPA frente a WEP son dos:

- Mejoras en el cifrado de datos mediante TKIP *(Temporal Key Integrity Protocol,* 'Protocolo Temporal de Integridad de Clave'). Este sistema asegura la confidencialidad de los datos.

- Autentificación de los usuarios mediante el estándar 802.11x y EAP *(Extensible Authentication Protocol,* 'Protocolo Extensible de Autentificación'). Este sistema permite controlar a todos y cada uno de los usuarios que se conectan a la red. No obstante, si se desea, permite el acceso de usuarios anónimos.

Actualmente el IEEE está terminando de desarrollar las especificaciones del estándar 802.11i. Como WPA salio antes que 802.11i, no puede seguir todas estas especificaciones. No obstante, lo que cubre actualmente WPA será completamente compatible con este nuevo estándar. Se puede decir que WPA es un subconjunto de 802.11i. WPA ha tomado de 802.11i aquellas características que son ya comercializables, como 802.11x y TKIP, y ha dejado aparte aquellas otras características que 802.11i no tiene aun completamente definidas.

Desafortunadamente, TKIP aún no es un estándar completo y ratificado. En un esfuerzo para ofrecer las mejoras TKIP que se necesitan con urgencia en el mercado, de manera más rápida a la típica del proceso de establecer estándares, varias organizaciones han creado un atajo al proceso mediante la publicación de soluciones anteriores al estándar. Cisco Systems ha puesto en el mercado una versión de TKIP exclusiva del fabricante antes de que aparezca el estándar. Microsoft ofrece el método Redes seguras simples *(Simple Security Networking, SSN,* por sus siglas en inglés) el cual es un subconjunto del esbozo del estándar 802.11 i y al mismo tiempo una implementación de Microsoft de TKIP. Subsecuentemente, SSN fue adoptado por la Alianza Wi-Fi como un estándar de seguridad temporal, renombrando la iniciativa WPA de Acceso protegido Wi-Fi.

A pesar de todas las mejoras que ofrecen TKIP y WAP, las arquitecturas basadas en RC4 siguen siendo consideradas por muchas personas como métodos fundamentalmente insuficientes para organizaciones que están preocupadas especialmente por la seguridad.

Uno de los inconvenientes mayores que incluyen algunas de estas características (no incluidas en WPA) es que requieren cambios en el *hardware* de los equipos Wi-Fi actuales. Por el contrario, todas las características que incluye WPA pueden ser actualizadas en los equipos Wi-Fi actuales mediante *software.* WPA necesitará que todos los dispositivos de red sean compatibles con el nuevo sistema. Si uno de los adaptadores inalámbricos no está preparado, la red entera se encriptará utilizando el antiguo WEP.

LA ALTERNATIVA: RED PRIVADA VIRTUAL

Para las personas que estén familiarizadas con las VPN, esta discusión sobre la seguridad WLAN hará que se sientan como en un lugar conocido. De hecho, muchos de los problemas inherentes a la transmisión de datos seguros a través de un medio inalámbrico que es fundamentalmente inseguro, son muy similares a los problemas inherentes a la transmisión de datos seguros a través de Internet que también es fundamentalmente inseguro. Esto conduce a la pregunta: ¿por qué no simplemente usar la tecnología VPN existente para resolver el problema de la seguridad inalámbrica? De hecho, ¿por qué no?

Muchas organizaciones han optado por ignorar los desarrollos que se han realizado en la seguridad específica para Wi-Fi y simplemente despliegan una VPN sobre la capa física Wi-Fi que es completamente insegura. Existe una variedad de ventajas en este enfoque:

- La tecnología VPN es relativamente madura. Mediante años de experiencia en la protección de datos importantes a través de Internet los fabricantes VPN han encontrado y mitigado la mayoría, sino es que todos, de los tipos de ataques que se han hecho en contra de las WLAN. Actualmente, las VPN proporcionan una variedad de métodos de autenticación que integran los cifrados DES, 3DES y AES.

- El enfoque VPN aprovecha la infraestructura de seguridad existente y el conocimiento del personal. Muchas organizaciones empresariales se han basado en las VPN para ofrecer acceso remoto en lugar de líneas contratadas costosas y que no son escalables o circuitos privados. A un nivel conceptual, sino es que técnico, estos esfuerzos se pueden aprovechar para resolver también los problemas de los clientes inalámbricos.

- Con las VPN, existe cierta capacidad de interoperabilidad. A pesar de que es cierto que no existe un estándar que realmente incluya interoperabilidad en las VPN, los fabricantes han, hasta cierto grado, solucionado esto mediante soluciones técnicas y de mercadotecnia. Las soluciones VPN están formadas por una aplicación del lado del cliente y un concentrador hardware en él otro extremo, o una aplicación de servidor basada en software. La mayoría de las aplicaciones VPN del lado del cliente operan en un rango muy amplio de sistemas operativos del lado del cliente y están disponibles por un costo muy bajo, o gratuitamente. Al hacer esto, 4os fabricantes VPN pueden resolver el problema principal de las tecnologías que aún no cuentan con un estándar -interoperabilidad-. ¿Cuál es el motivo de que exista interoperabilidad en una aplicación de cliente VPN si es una solución gratuita y opera en todos los dispositivos de cliente?

Sin embargo, existen algunas desventajas cuando se usa una solución VPN para resolver la seguridad WLAN:

- Las VPN están principalmente diseñadas sin tomar en cuenta demasiado el acceso a la red. Desde la perspectiva del usuario, normalmente la invocación del cliente VPN requiere de pasos adicionales, una inconveniencia que no es consistente con la libertad que ofrecen las WLAN. En el lado administrativo, a pesar de que es posible que el equipo específico VPN o hardware dedicado para las VPN esté instalado previamente para ofrecer el acceso remoto, es poco probable que sea capaz de controlar el tráfico asociado con las LAN Wi-Fi una tecnología que principalmente es de acceso local. El hardware de concentradores VPN soporta un número fijo de clientes sin duda existe un costo asociado con cada cliente adicional que se soporta. Es posible que los servidores VPN basados en software también tengan una 'cantidad de lugares" finita. Aprovechar la tecnología VPN para dar soporte a las WLAN requerirá, como mínimo, de una actualización significativa a la infraestructura.

- Las ventajas de "interoperabilidad" de las VPN son su desventaja. Es decir, debido a que los clientes VPN residen en el software y usan el procesador del anfitrión, su operación implicará un impacto en el desempeño mucho mayor al que ocasionan las soluciones que implementan el cifrado en el hardware. A pesar de que esto es cierto en el lado del cliente, es mucho más visible en el software de servidor VPN dentro de la infraestructura.

- Las VPN están limitadas en el sentido que no proporcionan la capacidad de priorizar el flujo de paquetes que se requiere para el tráfico sensible al tiempo, como el de voz y video. Las VPN sólo proporcionan soporte para el tráfico unidifusión IP y no soportan otros protocolos, por ejemplo, IPX y AppleTalk.

En pocas palabras, debe considerar tanto las ventajas como las desventajas de desplegar o aprovechar una VPN para satisfacer los requerimientos de seguridad de las WLAN. Se debe observar también que una VPN y las soluciones de seguridad especificas para las WLAN no se excluyen mutuamente. Para aplicaciones que incluso están dentro de la misma organización, las VPN pueden representar una solución mejor que WEP TKIP y WPA y viceversa.

FIREWALL O CORTAFUEGOS

Los cortafuegos o *firewall* son una de las más importantes medidas de seguridad para proteger un ordenador individual de los posibles ataques que pueda recibir, tanto a través de un entorno no del todo seguro como el de las redes Wi-Fi, como a través de una conexión de banda ancha a Internet.

El cortafuegos no protege las comunicaciones, sino que protege al ordenador para que ningún intruso pueda hacer uso del disco duro o de cualquier otro recurso. Un punto de acceso o un *router* puede tener también determinadas propiedades de cortafuegos para proteger los recursos de la red. Los cortafuegos llevan a cabo su protección analizando los datos de petición de acceso a los distintos recursos y bloqueando los que no estén permitidos.

Para las aplicaciones en el hogar o en pequeños negocios, es posible que sea suficiente con las características de cortafuegos incluidas en el punto de acceso normal. No obstante, existen puntos de acceso profesionales que mejoran fuertemente estas características. Aparte de lo anterior, un cortafuegos puede ser tanto un equipo *hardware* específico, como un *software* instalado en un ordenador o servidor. Los siguientes son algunos ejemplos de equipos *hardware:* Watchguard *(www.watchguard.com),* Webramp *(www.webramp.com),* Officeconnect *(www.3com.com)* o Sonicwall *(www.sonicwall.com).* Por el contrario, los siguientes son algunos ejemplos de *software:* Zonealarm*(www.zonealabs.com),* Conseal Private Desktop *(www.signa19.com),* Sybergen Secure Desktop *(www.sybergen.com)* Norton Internet Security *(www.symantec.com)* o Blackice Defender *(www.networkice.com).*

Los filtros del cortafuegos

El cortafuegos toma la decisión de qué datos deja pasar y qué otros no analizando los paquetes de información. La principal diferencia entre un buen cortafuegos y uno menos bueno es la cantidad de información que es capaz de analizar para tomar las decisiones. En la actualidad existen tres tipos de cortafuegos:

Filtrado de paquetes. Éstos facilitan un control de acceso básico basado en la información sobre el protocolo de los paquetes. Simplemente deja o no pasar los paquetes de acuerdo con el protocolo de comunicación que utiliza el paquete. Los *routers* incluidos en los puntos de acceso (o

en los *routers* ADSL o módem cable) ya suelen disponer de este tipo de filtrado. El problema es que esto supone una protección mínima para el usuario.

Servidor *proxy*. Se trata de una aplicación *software* que va más allá del simple filtrado del protocolo del paquete. Este tipo de cortafuegos puede tomar decisiones basado en el análisis completo de todo un conjunto de paquetes asociados a una sesión que tiene el mismo destinatario. Ciertamente, un *proxy* mejora la seguridad, aunque tiene el inconveniente de ralentizar la comunicación. Además, son más elaborados de configurar. Algunas de las soluciones *proxy* del mercado son las siguientes: Microsoft Proxy Server *(www.microsoft.com),* Winproxy *(www.winproxy.com),* Wingate *(www.wingate.deerfield.com)* o Sygate *(www.sybergen.com).*

Análisis completo del paquete. Éstos se basan en la misma técnica de filtrado de paquetes, pero, en vez de simplemente analizar la dirección de la cabecera del paquete, va interceptando paquetes hasta que tiene información suficiente para mantener su seguridad. Posteriormente, entrega estos paquetes al destinatario de la red interna y permite una comunicación directa entre este destinatario interno y su extremo externo. Este cortafuegos bloquea todas las comunicaciones generadas en Internet y deja pasar aquéllas iniciadas por cualquier ordenador interno. El resultado es una comunicación más fluida que con los *proxy,* pero la seguridad es menor.

Las reglas de filtrado

Las reglas de las que dependen los filtros de los cortafuegos se basan en distintos factores, condiciones o características de los paquetes de datos. Las características más comunes son las siguientes:

- **Dirección IP.** Tanto la dirección IP origen como destino pueden ser utilizadas para controlar los paquetes. Este tipo de filtros se utiliza habitualmente para bloquear la comunicación con ciertos servidores externos o para bloquear el acceso a Internet de ciertos usuarios.

- **Nombres de dominio.** Esta característica se utiliza de la misma forma que el filtrado de direcciones IP, pero basadas en los nombres de dominio en vez de en los números IP. Ya sabemos que los números IP de un servidor pueden cambiarse fácilmente, mientras que los nombres de dominio suelen ser más estables.

- **Protocolos. Los protocolos son** también una característica interesante a filtrar. Por ejemplo, se puede dejar pasar el protocolo http para permitir el acceso a páginas *web,* pero no permitir el protocolo telnet para impedir ejecutar comandos en ordenadores remotos, el protocolo ftp para impedir la bajada de archivos potencialmente infectados de virus o el protocolo smtp para impedir que desde el ordenador de un usuario se pueda crear un servidor de correo desde donde enviar correos ilegales *(spam).*

- **Puertos.** Mientras las direcciones IP se utilizan para identificar a los equipos origen y destino de la comunicación, los puertos son unos números que sirven para identificar cada una de las aplicaciones con comunicaciones simultáneas que puede tener un mismo equipo. Generalmente, cada número de puerto se utiliza para una aplicación distinta. Por ejemplo, el servicio *web* suele utilizar el puerto 80; Telnet, el 23 o el correo electrónico POP3, el 110. Por tanto, filtrar los números de puertos es una forma de filtrar los servicios a los que se puede acceder o ser accedidos.

- **Contenido.** Los cortafuegos pueden filtrar también los datos que contienen determinadas palabras o frases. En este caso, el cortafuegos analiza todo el contenido de los paquetes en busca de las palabras o frases prohibidas.

CONSIDERACIONES PARA UNA BUENA SEGURIDAD EN LAS WLANs

Mediante estas consideraciones en materia de seguridad de redes Wi-Fi se pretende resumir, de alguna manera, todo lo visto en este capítulo en 10 puntos. Estos son los 10 puntos que siempre hay que tener en cuenta a la hora de pensar en la seguridad de nuestra red Wi-Fi:

1. Cambiar los parámetros de seguridad que vienen configurados por defecto en el equipo Wi-Fi. Sobre todo, se debe cambiar la clave de acceso a las propiedades de configuración de los puntos de acceso. También es importante cambiar el nombre de red (ESSID).

2. Deshabilitar la configuración remota del punto de acceso. Muchos puntos de acceso permiten que se acceda a sus características de configuración desde una red remota (por ejemplo, Internet). Un intruso puede utilizar esta propiedad para averiguar la forma de acceder localmente a la red o para cambiar la configuración de acuerdo con sus intereses (por ejemplo, añadiendo a la red un punto de acceso falso desde donde actuar impunemente).

3. Activar siempre el cifrado WEP. Se ha visto que el cifrado WEP tiene muchas debilidades, pero, no cabe duda de que es mucho mejor que no tener activado ningún cifrado. Por otro lado, al configurar las claves WEP, no hay que elegir claves que sean extremadamente fáciles. Además, es recomendable cambiar estas claves periódicamente.

4. Configurar los puntos de acceso para que no envíen el ESSDI (nombre de red). Generalmente, los puntos de acceso publican el nombre de la red para que sus usuarios puedan conectarse a ella con toda facilidad. Esta característica es muy interesante en redes de acceso público, pero no tienen gran interés en las redes privadas. Impedir que el punto de acceso publique su nombre de red (ESSID) complica el acceso indebido.

5. Utilizar las características de cortafuegos *(firewall)* del punto de acceso o, en su defecto, instalar un equipo o *software* cortafuegos. Una característica de cortafuegos que suelen incluir la mayoría de los puntos de acceso es la posibilidad de controlar el acceso comprobando las direcciones MAC de las tarjetas adaptadoras de red de sus usuarios. Es buena idea habilitar esta opción. Ya sabemos que este sistema no es absolutamente infalible, pero una muy buena barrera para la mayoría de los intrusos.

6. Si es posible, deshabilitar la asignación dinámica de números IP (DHCP). Esto complicará un poco la configuración de los ordenadores de los usuarios, pero aumentará su seguridad.

7. Cuando se trata de compartir archivos e impresoras, compartir sólo lo necesario. No compartir nunca todo el disco duro de un ordenador, sino solamente el directorio o archivo que se necesite compartir. Además, si es posible, protegerlos con claves.

8. No dejar grabados en el equipo los datos de acceso a la red. Ni tampoco dejar estos datos escritos en papeles que están permanentemente con el equipo.

9. Sí es posible, configurar una red privada virtual (VPN).

10. La seguridad es tan débil como el más débil de sus eslabones. A veces, el eslabón más débil de esta cadena son sus propios usuarios. Por tanto, es importante informar a los usuarios de aquellas medidas mínimas de seguridad que deben tener en cuenta y recordárselas periódicamente.

APLICACIONES DE REDES WI-FI

Corno ya se pudo ver a lo largo de todo este trabajo de tesis, las LAN Wi-Fi están proliferando con rapidez en los domicilios y centros de trabajo. Wi-Fi es una manera efectiva en costo de compartir el acceso a Internet, archivos e impresoras en el hogar sin el problema de desplegar un cableado nuevo. Wi-Fi cada vez es más popular en las empresas debido a que los usuarios comienzan a exigir en sus trabajos la misma libertad inalámbrica que experimentan en sus hogares.

Pero en la sociedad actual, la distinción entre los sitios para vivir y para trabajar ya no es tan clara. Los viajeros de negocios con frecuencia pasan gran parte de su vida y tiempo de trabajo fuera de su hogar, al permanecer en hoteles. Para muchas personas de negocios, la asistencia a las ferias comerciales es una parte normal de sus trabajos. Para llegar a estos hoteles y centros de convenciones son necesarios algunos medios de transporte en Norteamérica, el medio más común es el avión, mientras que en otras partes del mundo se usan comúnmente los aviones y trenes. Pasar algún tiempo en los aeropuertos y estaciones de trenes, antes de salir o entre las conexiones, es parte de la vida de mucha gente.

La forma en que se trabaja también está cambiando. Como mencionamos antes, muchas personas están trabajando cada día más desde sus hogares, aprovechando la ventaja de las conexiones de banda ancha, teléfonos celulares y computadoras portátiles que ofrecen gran parte de la infraestructura de una oficina a las habitaciones adicionales de un hogar o en la mesa de la cocina. Pero además, las personas comienzan a considerar los espacios públicos como, por ejemplo cafeterías y restaurantes, como lugares alternativos para trabajar lo cual les permite mezclar el trabajo con interacción social y el pequeño placer de una taza de café.

Todo esto ha creado un tercer "espacio" para las LAN Wi-Fi, uno que está *en medio* de los lugares en donde las personas tradicionalmente viven y trabajan. Este famoso mercado de acceso público es el más nuevo, pequeño y especulativo de los tres, haciendo que se considere el mercado más emocionante del grupo. Debido a que Wi-Fi es una tecnología de red de área *local,* estas áreas tienden a medir miles de pies cuadrados en lugar de las coberturas de área que ofrecen los sistemas de teléfonos celulares, los cuales se miden en miles de millas cuadradas. Estas áreas de cobertura pública que son relativamente pequeñas han llegado a conocerse como *puntos de encuentro.*

A continuación describiremos los tipos de lugares públicos en donde se están desplegando las LAN Wi-Fi y los modelos de negocios que están asociados con estos despliegues hasta el punto en que se pueda decir que existen modelos de negocios.

¿Dónde se encuentra Wi-Fi?

Para que un despliegue Wi-Fi sea exitoso, se deben satisfacer algunas condiciones, a saber:

- Un número suficiente de individuos debe pasar a través de un área pública con dispositivos de cliente, por ejemplo, computadoras portátiles y PDA que tengan soporte para Wi-Fi.
- Una cantidad suficiente de estos dispositivos debe tener habilitado las capacidades Wi-Fi. Si los dispositivos no están habilitados, el usuario debe contar con una necesidad importante de que el dispositivo habilite sus capacidades Wi-Fi para el acceso público.
- Los individuos deben pasar un periodo suficiente en estas áreas públicas, tanto en términos del número de visitas como en el tiempo acumulado, de manera que surja el deseo de la conectividad inalámbrica.
- Ellos, o sus organizaciones, deben otorgar un nivel suficiente de valor al acceso inalámbrico público para justificar cualquier costo que esté asociado al acceso.

De acuerdo con la lista anterior, puede observar que muchas áreas públicas cuentan, en grados distintos, con las condiciones necesarias para el despliegue Wi-Fi público. En unos cuantos minutos, un grupo que sea razonablemente creativo podría concebir tas ideas de tipos de ubicaciones potenciales. Dicho esto, los lugares más comunes que existen actualmente para los puntos de encuentro Wi-Fi se pueden resumir de la manera siguiente:

Aeropuertos

Una cantidad sorprendente de viajeros de negocios cargan con sus computadoras portátiles a lo largo de aeropuertos en todo el mundo y todos los días. Debido a que el correo electrónico se ha convertido en una forma casi obligatoria de comunicación de negocios y con las expectativas de incremento en la capacidad de respuesta, incluso las personas de negocios que viajan necesitan descargar frecuentemente los mensajes entrantes y enviar las respuestas. Las salas de espera de viajeros frecuentes de las líneas aéreas son lugares naturales para el despliegue Wi-Fi debido a que no solamente se concentran ahí las personas de negocios sino que también los estimula a quedarse un periodo relativamente largo en estos lugares. Los despliegues Wi-Fi en las áreas públicas de los aeropuertos -terminales, puertas y en las explanadas- cumplen con todas las condiciones que describimos anteriormente excepto por, posiblemente, la idea de tener tiempo suficiente. Muchos viajeros de negocios que no tienen membresías de los lugares de descanso de las líneas aéreas hacen todo lo posible para minimizar la cantidad de tiempo que pasan por los aeropuertos. Debido a todas las razones que mencionamos, las estaciones de tren son igualmente viables como puntos de encuentro Wi-Fi especialmente en aquellas partes del mundo en que los trenes son una forma común para realizar viajes de negocios. La extensión natural de los despliegues Wi-Ei en los aeropuertos y estaciones de trenes serían los puntos de encuentro móviles en los aviones y trenes mismos. Aquí, los clientes potenciales están normalmente en las áreas de punto de encuentro por

un periodo incluso más largo y tienen mayor capacidad de atención que cuando están en los aeropuertos o estaciones de tren. Actualmente, los aspectos reguladores de la instalación de Wi-Fi en los aviones se están diseñando al mismo tiempo que se revisan los problemas técnicos de mantener un enlace de banda ancha con Internet desde aviones y trenes que se mueven.

Hoteles

Un aspecto lamentable de los viajes de negocios es que a menudo el único momento en que se puede trabajar en lo que normalmente se trabajaría durante el día es durante las noches o temprano en las mañanas. El acceso telefónico a redes en las habitaciones ha sido la forma tradicional de proporcionar la conectividad que se necesita con frecuencia. A medida que han crecido los tamaños de archivos y las expectativas de desempeño, las velocidades de acceso telefónico se están convirtiendo con rapidez en aspectos imprácticos para la adquisición de correo electrónico y navegación en la Web el ancho de banda en las habitaciones es un requerimiento cada vez más grande-. Dado el pequeño tamaño de las habitaciones de hoteles, el aspecto de movilidad de Wi-Fi no es un requerimiento tan importante. Por otro lado, Wi-Fi proporciona a los hoteleros la capacidad de proporcionar una banda ancha en las habitaciones sin tener que desplegar cable Ethernet a lo largo de todo el edificio. Debido a que en las computadoras portátiles Wi-Fi cada día es más común, al igual que Ethernet, proporcionar la banda ancha inalámbrica en la habitación es una posibilidad cada vez mayor.

Centros de convenciones

Cualquier persona que haya tenido que esperar sentada mientas transcurre un 'descanso en la sesión" en una feria comercial, apreciará el atractivo de una diversión como la de leer el correo electrónico o explorar la Web. Los operadores de los centros de convenciones, coordinadores de ferias e incluso algunos exhibidores apreciarán este hecho, haciendo que cada vez sea más común en algunas industrias la disponibilidad del acceso Wi-Fi en el piso de una feria comercial o en sus cercanías.

Cafeterías

Estos lugares populares para los puntos de encuentro Wi-Fi tienen como fin atraer a las personas que pasan una cantidad de tiempo considerable mientras consumen un costoso café con leche. Éstas pueden ser jóvenes incluyendo estudiantes, escritores, artistas y otras personas que no cuentan con lugares de trabajos más tradicionales y consideran a los cafés como lugares de trabajo, además de las personas de negocios que entran a las cafeterías para almorzar o cenar. Los puntos de encuentro Wi-Fi son considerados como la simbiosis de dos negocios principales: el lugar atrae a los usuarios y la conexión inalámbrica los mantiene en el lugar más tiempo, todo mientras toman café.

Espacios abiertos

Las áreas públicas como, por ejemplo, parques urbanos, jardines e incluso glorietas, son áreas que los trabajadores y ciudadanos visitan a menudo para disfrutar de los espacios abiertos. De la misma forma en que los estudiantes universitarios aprovechan los despliegues Wi-Fi en la universidad mediante navegar por Internet sin la necesidad de cables desde las áreas verdes, las

personas de ciudad estarán contentas de contar con el acceso inalámbrico en lugares abiertos. Las instituciones públicas como, por ejemplo, gobiernos de la ciudad y universidades urbanas más grandes, están, en gran parte, en las primeras etapas de los análisis de viabilidad de este tipo de servicio.

MODELOS DE NEGOCIOS PARA LOS PUNTOS DE ENCUENTRO

Debido a que es un fenómeno bastante reciente, nadie puede hacer conclusiones sobre cuál es el modelo de negocio o modelos que son óptimos para los puntos de encuentro Wi-Fi a corto y largo plazo. Actualmente se está llevando a cabo un poco de experimentación y se han puesto a prueba en varios modelos de negocios.

Para que alguna organización considere un despliegue Wi-Fi, la primera pregunta de negocios que se debe responder es si el punto de encuentro tiene como fin ser un generador directo de ganancias, en el cual se cobre una cuota por el uso, o un servicio, que no implique cargos por el uso pero que represente algún beneficio indirecto para la organización.

Existen dos modelos de ingresos directos; la suscripción y el pago por servicio, que se están aplicando actualmente a los puntos de encuentro Wi-Fi. Un servicio de suscripción normalmente proporciona una cantidad de minutos (o una cantidad ilimitada de minutos) o una cuota de suscripción mensual. Este modelo sigue estrechamente el modelo de los teléfonos celulares y proporciona al propietario del punto de encuentro un flujo más continuo de ganancias. Un modelo de ingresos por uso es más apto para atraer al usuario ocasional, que se conecte de manera impulsiva sin considerar ningún tipo de servicio de largo plazo, por el cual deberá pagar con una tarjeta de crédito. Estos modelos no se excluyen mutuamente de ninguna manera y a menudo se ofrecen como opciones complementarias. Por ejemplo, un proveedor grande de puntos de encuentro Wi-Fi ofrece una suscripción ilimitada mensual por 30 dólares, pero también proporciona un plan de pago por servicio en el cual se debe pagar 2.99 dólares por los primeros 15 minutos y 0.25 centavos de dólar por cada minuto adicional. Cuando se compara con las tarifas por uso, la suscripción mensual parece una ganga -lo cual es justo el objetivo.

Cuando Wi-Fi se despliega como un servicio público, el modelo es similar al de cualquier otro servicio municipal como, por ejemplo, el alumbrado público o la recolección de basura -no existe un costo directo para el usuario, sólo la contribución indirecta al proyecto por medio de los impuestos

Convenios y Pagos

Uno de los retos técnicos más grandes que enfrenta el despliegue amplio de los puntos de encuentro Wi-Fi no tiene nada que ver con las frecuencias de radio. De hecho, la instalación de un punto de acceso en un café no es más difícil que la instalación en un hogar. Sin embargo, lo difícil es establecer un sistema de contabilidad general que se acople a los modelos de negocios que discutimos antes.

Muchos sistemas se basan en una puerta de enlace en Internet, una aplicación o dispositivo que se encuentra entre el punto de acceso e Internet, que limita el tráfico a un sitio web, o una pequeña cantidad de sitios web, hasta que se introduce un número de tarjeta de crédito o contraseña de suscripción. A pesar de que este medio de autenticación es factible, otros proveedores de servicios Wi-Fi potenciales sugieren que un enfoque mejor es usar un SIM GSM, un medio de autenticación que usa un chip inteligente físico que se incrusta en el dispositivo de cliente. El SIM GSM es uno de los medios más populares para la identificación y autenticación de teléfonos portátiles en la red celular no es sorprendente que los patrocinadores principales de la autenticación SIM GSM sean los fabricantes de equipo celular y proveedores de servicios móviles. En Europa ya existen sistemas que permiten que la facturación Wi-Fi esté integrada en un solo recibo telefónico mensual.

Las personas que han comprado suscripciones de acceso Wi-Fi desearán, naturalmente, tener la posibilidad de usar sus suscripciones en tantos lugares como sea posible para maximizar el aprovechamiento de su inversión mensual. Con los teléfonos celulares esto se lleva a cabo a través de un sistema de movilidad y convenios. Sin importar que un usuario podría ser un cliente del proveedor A, es posible que acceda a la red a través de una torre celular que le pertenece a un proveedor B. A través de una serie de acuerdos y sistemas, los dos proveedores hacen un "convenio" entre sus cuentas, facturando y pagando uno al otro el acceso que proporcionan a los clientes ajenos.

Actualmente, los convenios y sistemas sólo se encuentran en las primeras etapas de uso para los puntos de encuentro Wi-Fi, pero se piensa que en general serán un requisito previo para la demanda a gran escala -como ocurrió con los teléfonos celulares-. Detrás del apoyo para el uso de la autenticación por medio de SIM GSM, se aloja la expectativa de que un sistema Wi-Fi que usa este sistema de teléfono celular pueda aprovechar los convenios y sistemas de facturación que ya existen, haciendo posible obtener lo "máximo" en cuanto a la comodidad del usuario: una sola factura integrada que contenga los cargos del teléfono celular y el acceso Wi-Fi.

La información debe ser gratuita

Existe otro tipo de modelo de punto de encuentro Wi-Fi que tiene poco que ver con los negocios. Este es un grupo pequeño pero muy llamativo de individuos que cree que el acceso inalámbrico es algo que se debe ofrecer gratuitamente o compartir en lugar de vender. En lugar de intentar limitar el acceso en las WLAN de sus hogares o lugares de trabajo a través de medidas de seguridad y autenticación, los seguidores de este modelo dejan abiertas sus conexiones, a menudo emitiendo sus SSID, con la idea de ofrecer la disponibilidad de sus redes a cualquier persona que esté dentro del rango.

Las organizaciones locales, e incluso internacionales, están haciendo esfuerzos para intentar organizar este fenómeno anarquista. Freenetworks.org (www.freenetworks.org) es una organización dedicada a implementar este "ejercicio de libertad en las telecomunicaciones". Cuenta con más de una docena de organizaciones de miembros locales en lugares como, por ejemplo, Londres, Praga, San Francisco, Toronto, Washington DC y Pittsburgh. En la ciudad de Nueva York, los miembros de la organización NYCWireless (www.nycwireless.net) tienen un sitio web que despliega un mapa con las ubicaciones y SSID de más de 170 puntos de acceso

abiertos dentro y alrededor de Manhattan. Seattle Wireless (www.seattlewireless.net) es otra organización que agrupa miembros que proporcionan la ubicación de puntos de acceso abiertos a lo largo del área de Puget Sound.

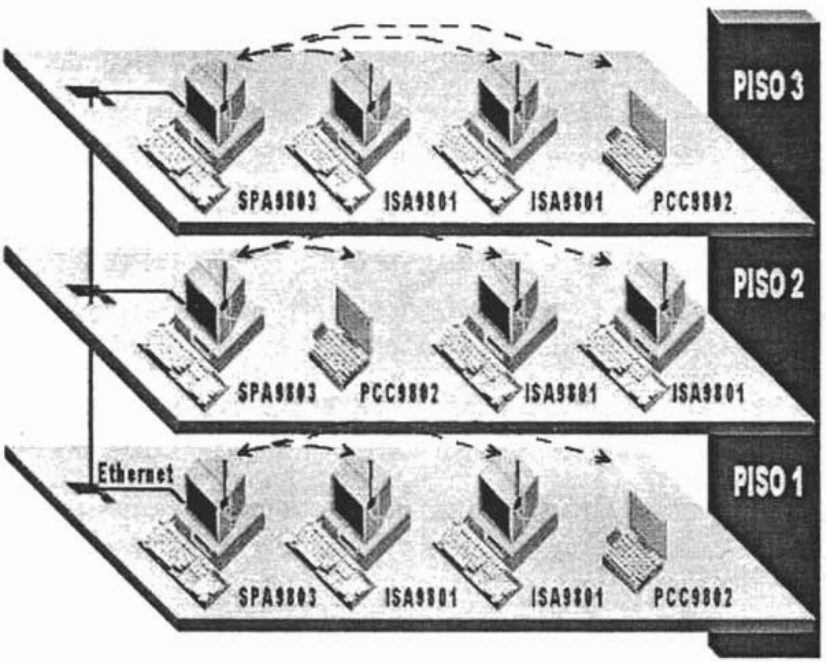
No todas las personas apoyan la idea del acceso libre. Los proveedores de servicios de banda ancha como, por ejemplo, proveedores DSL y de cable, normalmente limitan el grado hasta el cual una conexión se puede compartir entre múltiples clientes. Los modelos de aprovisionamiento para las áreas residenciales están basados en una cantidad relativamente pequeña de dispositivos por conexión y por lo tanto una cantidad de tráfico modesta. Obviamente, el hecho de compartir las conexiones existentes tiende a reducir la demanda de conexiones nuevas, lo cual afecta los ingresos del proveedor de servicios. A pesar de que los proveedores de servicios no han llevado a cabo ninguna acción concertada en contra de los grupos de comunidades inalámbricas o sus miembros, es algo que podrían hacer. Mediante el software de administración de red común, es fácil encontrar un uso demasiado alto que esté fuera de lo común para una sola conexión. La mayoría de los proveedores de servicios están tomando una perspectiva de mirar a ver qué pasa", antes de tomar medidas que potencialmente pueden ser poco populares hasta que el crecimiento de las redes gratuitas haga que sea necesario tomar una acción.

El lado más oscuro del acceso inalámbrico gratuito es la *guerra de los automóviles* que puede provocar. Una derivación del término arcaico *guerra de marcación* en donde los piratas informáticos usan frecuencias de marcación aleatorias para entrar en computadoras remotas a través del sistema telefónico, la guerra de los automóviles es la práctica de recorrer áreas buscando puntos de acceso abiertos. Estos puntos de acceso pueden estar abiertos de manera premeditada para que se puedan compartir o (con mayor frecuencia) de forma inadvertida debido a las medidas de seguridad ineficientes o inexistentes. Las guerra de los automóviles a menudo usan antenas de ganancia alta que se montan en los automóviles para maximizar el rango y efectividad de la herramienta de pirateo móvil. A pesar de que el objetivo de estas guerras no siempre es causar daño a la red o robar información de ella, su asociación con el punto de acceso normalmente no es esperada -y cuando menos es incorrecta y posiblemente ilegal-. Un problema más reciente que supera la guerra de los automóviles es la *guerra del gis*. Cuando se descubre un punto de acceso abierto, la persona que lleva a cabo la guerra de los automóviles o el gis marcará la ubicación con gis, a menudo desplegando el SSID del punto de acceso abierto. La guerra del gis evita la incomodidad de la guerra de los automóviles puesto que el trabajo ya estará hecho.

A pesar de que el fenómeno de las redes gratuitas y la guerra de los automóviles provienen de puntos de vista diametralmente opuestos, son dos lados de la misma moneda. Las redes gratuitas surgen de tipos altruistas poco comunes que toman la banda ancha de los supuestamente ricos monopolios de cable y de teléfono y la ofrecen a las personas comunes que merecen estos servicios. Ambas guerras son simples travesuras y molestias de amantes de la tecnología que tienen demasiado tiempo. Pero ambas indican el deseo incipiente de acceso de banda ancha inalámbrico poco costoso (más bien gratuito) en un área metropolitana amplia. Aunque es probable que estos movimientos disminuyan con el tiempo (a medida que los proveedores de servicios comiencen a reforzar sus acuerdos de servicio y seguridad inalámbrica para frustrar al pirata informático casual que realice la guerra de los automóviles), su confianza general podría continuar. En un futuro en donde exista un acceso inalámbrico de banda ancha poco costoso, el fenómeno de las redes libres y la guerra de los automóviles se considerarán prototipos poco aceptables.

Enlace de áreas físicas independientes mediante Puntos de Acceso.

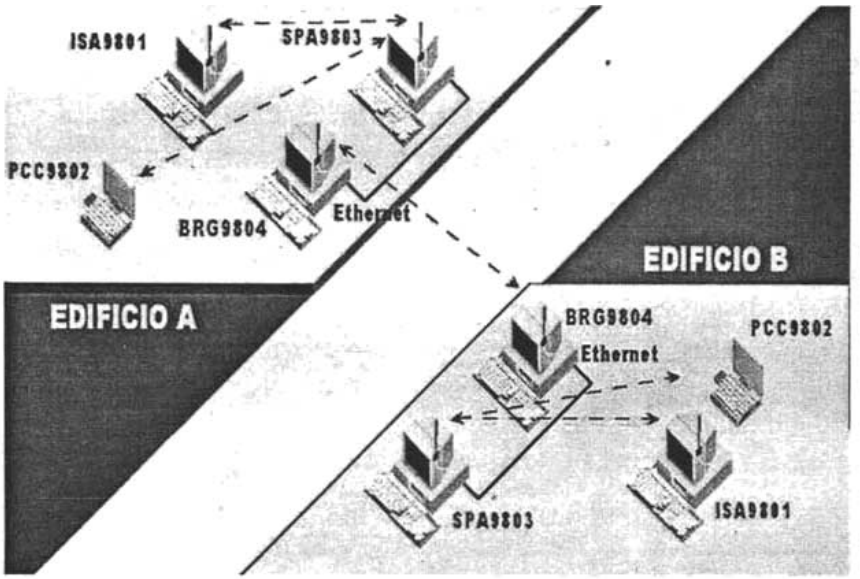
El enlace entre redes inalámbricas situadas en diferentes plantas de un mismo edificio es un perfecto ejemplo del uso del *Punto de Acceso* para realizar el enlace entre redes inalámbricas independientes, mediante un mínimo cableado Ethernet, en aquellas situaciones de cobertura límite de las antenas debido a obstáculos importantes.



Enlaces entre redes locales próximas.

La combinación del *Punto de Acceso* y el *Puente* permite llevar a cabo el enlace entre dos áreas inalámbricas, cuando resulta imposible o demasiado caro realizar esta unión mediante un cable.

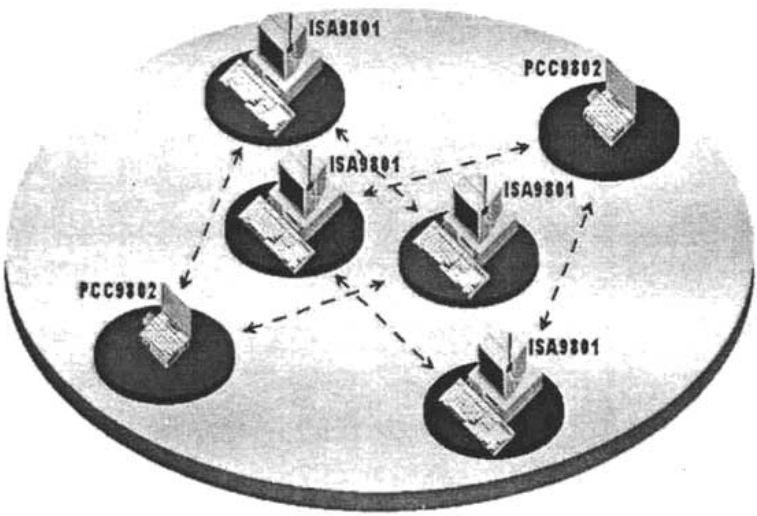
Para una situación similar entre dos redes Ethernet existentes, el *Puente* permite enlazar ambas inalámbricamente salvando vía radio los obstáculos que impedían su unión mediante un cable.



Redes Inalámbricas en el mismo área física.

Dos o más redes inalámbricas, tanto en modo Ad-Hoc como de Infraestructura, pueden coexistir simultáneamente en el mismo área física de cobertura de sus antenas, de forma totalmente transparente a los usuarios de cada una de las redes.

Además, mediante una sencilla operación de asignación de canales en su configuración, ambas redes pueden operar a pleno rendimiento de su ancho de banda.



CONCLUSIONES

Las redes inalámbricas pueden tener mucho auge en nuestro país debido a la necesidad de movimiento que se requiere en la industria. Las redes inalámbricas llevan años ofreciendo la posibilidad de unir puntos de difícil acceso, y además le permiten moverse dentro de un entorno manteniendo su conectividad. Estos servicios estaban restringidos a las grandes empresas, pero actualmente, gracias a los últimos desarrollos que mejoran en velocidad, la consolidación y madurez de los estándares que definen estas redes y la ampliación de terminales económicos, hace que se abra cada vez más el marco de usuarios finales a pequeños negocios e incluso a usuarios residenciales que ven en las tecnologías inalámbricas nuevas maneras de comunicarse.

Además es relativamente fácil el crear una red híbrida, con la cual seguiríamos teniendo las ventajas de la velocidad que nos brinda la parte cableada y expenderíamos las posibilidades con la parte inalámbrica. Una red híbrida Ethernet con radiofrecuencias y cableada, se puede considerar como una de las redes de más uso en el mundo.

La alianza Wi-Fi es una organización que ha hecho demasiado para alcanzar el objetivo de interoperabilidad de los dispositivos basados en los estándares 802.11. Si un cliente que implementa una red Wi-Fi de múltiples fabricantes puede tener la seguridad de que todos los dispositivos de WLAN han pasado las pruebas y verificaciones de interoperabilidad y por lo tanto su red funcionara sin ningún problema de compatibilidad; por esto es la mejor opción en cuanto a productos inalámbricos.

Wi-Fi, tiene un brillante futuro por delante. Va a ser el líder en comunicaciones empresariales y lo tiene todo para ser el Ethernet inalámbrico. Con la facilidad de instalación y sus considerables velocidades será el que comunique nuestros ordenadores, no sólo portátiles, en el futuro, tanto en la oficina como en nuestras casas. Y eso sin olvidarnos de las otras tecnologías que, cada una por un lado, en nichos de mercado distintos van a salir igual de triunfadores, además de que serán más bien complementarios y no tanto competidores.

La principal ventaja de las redes inalámbricas es que no necesitan licencia para su instalación, es la libertad de movimientos que permite a sus usuarios, ya que la posibilidad de conexión sin hilos entre diferentes dispositivos elimina la necesidad de compartir un espacio físico común y soluciona las necesidades de los usuarios que requieren tener disponible la información en todos los lugares por donde puedan estar trabajando. Además, a esto se añade la ventaja de que son mucho más sencillas de instalar que las redes de cable y permiten la fácil reubicación de los terminales en caso necesario.

También, presentan 2 principales desventajas contra redes cableadas, o más bien inconveniente, el primero es la seguridad, debido al medio por el que trasmiten son más propensas a ataques; el otro inconveniente es el hecho de la "baja" velocidad que alcanzan, hasta que los nuevos estándares no permitan un incremento significativo, no es de prever su uso masivo, ya que por ahora no pueden competir con las LAN basadas en cable,

Por todo lo anterior se puede observar que por unos cuantos años más las WLANs no podrán sustituir a las redes LAN cableadas, más bien, se deben ver como una alternativa o un complemento y no como un sustituto en la implementación de una red, esto es, se pueden mezclar las redes cableadas y las inalámbricas, y de esta manera generar una "Red Híbrida" y poder resolver los últimos metros hacia la estación. Se puede considerar que el sistema cableado sea la parte principal y la inalámbrica le proporcione movilidad adicional al equipo.

APÉNDICE A

GLOSARIO

802.11. Conjunto de estándares de red de área local inalámbrica definidos por el IEEE Institute of Elecirical and Electronies Engineers, 'Instituto de Ingenieros Eléctricos y Electrónicos'). Entre estos estándares se encuentra 802.11b, que es en el que se basa Wi-Fi.

acceso alámbrico. El uso de teléfonos de cobre, lineas de cable o fibra. Las ventajas del acceso alámbrico incluyen la confiabilidad alta, tolerancia a la interferencia alta y, generalmente, la posibilidad de resolver problemas en forma más sencilla. En el caso de la fibra, el acceso alámbrico cuenta con un ancho de banda excepcionalmente alto. El acceso alámbrico es el opuesto tecnológico del acceso inalámbrico.

administrador. Persona responsable del mantenimiento y/o gestión de una red corporativa, red de área local (cableada o inalámbrica) o de un servidor de red.

administración de red Término genérico que se usa para describir sistemas o acciones que ayudan a mantener y caracterizar una red o resolver problemas de la red.

ancho de banda. El rango de frecuencia necesaria para transportar una señal, medido en unidades de hertz (Hz). Por ejemplo, las señales de voz normalmente requieren aproximadamente 7 kHz de ancho de banda y el tráfico de datos por lo común requiere de aproximadamente 50 kHz de ancho de banda, pero esto depende estrechamente del esquema de modulación, velocidades de datos y la cantidad de canales del espectro de radio que se usen.

ANSI . Acrónimo del Instituto nacional de estándares de Estados Unidos. Una organizaci ón voluntaria compuesta de miembros corporativos, gubernamentales y de otros tipos que coordina las actividades relacionadas con los estándares, aprueba los estándares nacionales de Estados Unidos y desarrolla posiciones en las organizaciones de estándares internacionales. ANSI ayuda a desarrollar estándares internacionales y de la Unión Americana relacionados con, entre otras cosas, las comunicaciones y las redes.

antena. Un dispositivo para transmitir o recibir una frecuencia de radio (RU). Por lo común, las antenas están diseñadas para frecuencias específicas y definidas de manera relativamente estricta y su diseño varia mucho. Por ejemplo, una antena para un sistema de 2.5 GHz (MMDS) normalmente no funcionará para un diseño de 28 GHz (LMDS).

AP. Acrónimo de punto de acceso. Un punto de acceso es un dispositivo que normalmente conecta a los dispositivos de cliente, por ejemplo, tarjetas PCMCIA, con la porción Etbernet de una LAN. Normalmente un punto de acceso tiene un puerto Ethernet y otro de energía en la parte trasera e incluye una o dos antenas que transmiten y reciben señales RU de los dispositivos de cliente, otros puntos de acceso o puentes de grupos de trabajo.

ASCII. Acrónimo del Código estándar de Estados Unidos para el intercambio de información. Especifica un código de 8 bits para la representación de caracteres (7 bits más la paridad).

atenuación. La pérdida de energía en la señal de comunicación, ya sea por el diseño del equipo, manipulación del operador o transmisión a través de un medio, por ejemplo, la atmósfera, cobre o fibra.

autenticación . En seguridad, la verificación de la identidad de una persona o proceso.

autenticación abierta. Un tipo de autenticación donde un punto de acceso concede la autenticación a cualquier cliente, sin importar si pertenece o no a la red de ese punto de acceso en particular. Se puede decir que es más común en los dispositivos de datos sencillos, por ejemplo, los lectores del código de barras que tienen poco poder de procesamiento.

autenticación de estación El proceso de autenticar un dispositivo 802.11, por ejemplo, un puente o punto de acceso, a diferencia de autenticar un cliente, como una tarjeta PCMCIA.

banda base Característica de una tecnología de red donde sólo se usa un portador de frecuencia. Ethernet es un ejemplo de una red de banda base. También se conoce como banda angosta.

banda de paso. Las frecuencias que un radio permite que pasen desde su entrada hasta su salida. Cuando un receptor o transmisor usa filtros con bandas de paso angostas, sólo la frecuencia deseada y frecuencias adyacentes son un aspecto que debe tomar en cuenta el diseñador del sistema. Si un receptor o transmisor usa filtros con bandas de paso amplias, entonces muchas frecuencias más cercanas a la frecuencia deseada serán un problema para el diseñador del sistema. En un sistema de multiplexión por división de frecuencia (FDM), las bandas de paso de transmisión y recepción serán diferentes. En un sistema de multiplexión por división de tiempo (TDM), las bandas de paso de transmisión y recepción son las mismas.

bandas ISM. Normalmente, pero no siempre, se acuerda que las bandas industriales, científicas y médicas son las siguientes: 902 a 928 MHz, 2.4 a 2.485 GHz, 5.15 a 5.35 GHz y 5.725 a 5.825 GHz.

bit. Una contracción de dígito binario, que es la unidad más pequeña posible de información que puede controlar una computadora. Un carácter alfabético o numérico normalmente está compuesto de 8 bits, lo que a su vez forma un byte de información. Por tanto, un carácter sencillo, por ejemplo, la letra b, requiere de la combinación de ocho 1 y 0.

BLUETOOTH. Es una tecnología inalámbrica que permite intercomunicar equipos a una distancia de varios metros (menos de 10 metros). Al contrario que otras tecnologías como Wi-Fi, la tecnología Bluetooth no está pensada para soportar redes de ordenadores, sino, más bien, para comunicar un ordenador o cualquier otro dispositivo con sus periféricos: un teléfono móvil con su auricular, una PDA con su ordenador, un ordenador con su impresora, etc.

BPSK. Acrónimo de la Modulación de fase por desplazamiento binario. Una técnica de modulación de frecuencia digital que se usa para transmitir información. Este tipo de modulación es menos eficiente pero más sólido que otras técnicas de modulación parecidas, por ejemplo, QPSK y 64 QAM.

BSS. Basic Service Set, 'Conjunto de Servicios Básicos'. Es una de las modalidades de comunicación en las que se pueden configurar los terminales de una red Wi-Fi. En este caso, la red inalámbrica dispone de un equipo punto de acceso) que se encarga de gestionar las comunicaciones (internas y externas) de todos los dispositivos que forman la red. Este modo de conexión también es conocido como modo infraestructura.

CCK. Complementary Code K~ying, 'Salto de Código Complementario'. Es una técnica de modulación utilizada en Wi-Fi junto con las técnicas de espectro distribuido.

certificado Una declaración firmada en forma digital de una entidad que establece qu~ una clave pública de alguna otra entidad tiene algún valor en particular. Lo certificados son un concepto común en la sociedad moderna. Los usamos como licencias de conducir, membresías a clubes y como identificaciones Estos elementos asignan una clave pública a un individuo, posición u organización.

cifrado. Una clave que convierte el texto sencillo en texto cifrado. Esto no se deb~ confundir con algunas formas de códigos secretos en los cuales cierta' palabras o frases se reemplazan con palabras o frases de códigos secretos.

clave. Se usa para "abrir" un texto cifrado; la clave se puede considerar en lo' mismos términos relativos que un cerrojo o una llave. Una sola clave puedc generar una cantidad grande de versiones diferentes de texto cifrado desde el texto sencillo. También existen diferentes tipos de claves, por ejemplo, la clave de ejecución que cifra la frecuencia de un número de bits, y una clave de mensaje, la que es diferente para cada uno de los mensajes. En el uso de las claves como las de mensajes, obviamente tanto la fuente de la transmisión como la parte receptora deben conocer el orden y una clave específica que se usa en cada transmisión.

cortafuegos. Es un dispositivo de seguridad (hardware o software) que controla los accesos a una red local desde el exterior (típicamente, Internet).

CSMA/CA. Carrier Sense Multiple Access with Collision Avoidance, 'Acceso Múltiple por Detección de Portadora con Evitación de Colisión'. Es el sistema que emplea Wi-Fi para negociar las comunicaciones entre los distintos dispositivos. Este sistema evita que dos dispositivos puedan intentar hacer uso del medio simultáneamente (evita la colisión).

CSMA/CD. Carrier Sense Mulaple Access with Collis ion Detection, 'Acceso Múltiple por Detección de Portadora con Detección de Colisión'. Es el sistema que emplean las redes Ethernet para negociar las comunicaciones entre los distintos dispositivos. Este sistema detecta que dos dispositivos han intentado hacer uso del medio simultáneamente (detecta la colisión) y hace que cada uno lo intente de nuevo en tiempos distintos.

dirección MAC. Dirección estandarizada de la capa de enlace de datos que se requiere para cada puerto o dispositivo que se conecte a una LAN. Otros dispositivos de la red usan estas direcciones para asignar puertos específicos en la red y crear, además de actualizar, tablas de direccionamiento y estructuras de datos. Las direcciones MAC son de 6 bytes de longitud y son controladas por el IEEE. También se conocen como direcciones de hardware, direcciones de capa MAC y direcciones físicas.

DSSS. Acrónimo del Espectro extendido de secuencia directa. Una técnica de propagación en la que distintas señales de datos, voz y video, o ambas, se transmiten a través de un conjunto específico de frecuencias de manera secuencial desde la frecuencia más baja hasta la más alta, o desde la más alta hasta al más baja.

encabezado. Información de control colocada antes de los datos cuando se encapsula esa información en red.

encapsular. Envolver los datos en un encabezado de protocolo especifico, por ejemplo, los datos Ethernet se envuelven en un encabezado Ethernet específico antes de convertirse en tráfico de la red. Además, cuando se crean puentes entre redes, la trama completa de una red simplemente se coloca en el encabezado que usa el protocolo de la capa de enlace de datos de la otra red.

espectro electromagnético. El rango completo de frecuencias electromagnéticas (al igual que magnéticas); un subconjunto de este espectro se usa en los sistemas RU comerciales.

espectro extendido. Una técnica de propagación en la que se distribuyen señales de datos, video o voz a través de un rango amplio de frecuencias; luego las señales son agrupadas y recopiladas en el receptor.

Ethernet. Especificación para una LAN de banda base que inventó la compañía Xerox Corporation y que fue desarrollada en conjunto por Xerox, Intel y Digital Equipment Corporation. Las redes Ethernet usan CSMA/CD y funcionan a través de una variedad de tipos de cable a 10 Mbps. Ethernet es similar al conjunto de estándares 802.3 del IEEE.

Ethernet rápido. Alguna de las variedades de especificaciones Ethernet de 100 Mbps. Ethernet rápido ofrece un incremento en la velocidad 10 veces mayor al de la especificación Ethernet 10 Base-T y al mismo tiempo mantiene las cualidades del formato de las tramas, mecanismo MAC y MTU. Este tipo de similitudes permite el uso de aplicaciones 10 Base-T existentes y las herramientas de administración de red en las redes Ethernet rápido. Está basado en la extensión de la especificación 802.3 de la IEEE.

ETSI. Acrónimo del Instituto Europeo de estándares de comunicaciones. Una organización que crearon los PTT europeos y la Comunidad Europea para proponer estándares de telecomunicaciones para Europa.

FCC. Acrónimo de la Comisión federal de comunicaciones. Es una agencia gubernamental de Estados Unidos que supervisa, otorga licencias y controla los estándares de transmisión electrónica y electromagnética.

FHSS. Acrónimo del Espectro extendido de saltos de frecuencia. Una técnica de propagación mediante la cual distintas señales de datos, voz y video, o ambas, se transmiten a través de un conjunto especifico de frecuencias en un orden pseudoaleatorio, en lugar de usar un método secuencial que va desde la frecuencia más baja hasta la más alta, o desde la más alta a la más baja, como en el caso de DSSS. Las señales se propagan en el rango de tiempo, no en el rango de frecuencia. Vea también DSSS y espectro extendido.

f¡rewall. Direccionador o servidor de acceso, o varios direccionadores o servidores de acceso, que tienen la tarea de funcionar como un búfer entre cualquier red pública conectada y una red privada. Un direccionador firewall usa una lista de acceso y otros métodos para asegurar la protección de una red privada.

frecuencia. Número de ciclos, medidos en hertz (1 por segundo), de una señal de corriente alterna por unidad de tiempo. Por ejemplo, una frecuencia de 1 MHz tendría un ciclo completo (una onda senoidal completa) pasando por un punto determinado en el espacio a la velocidad de un millón de ciclos por segundo. Una frecuencia de 1 GHz haría que pasen ondas senoidales a través de un punto determinado en el espacio con una velocidad de mH millones de veces por segundo, y así sucesivamente.

getway. Pasarela. Es un sistema informático que transfiere datos entre dos aplicaciones o redes incompatibles entre sí. El gateway adapta el formato de los datos de una aplicación a otra o de una red a otra. Se utiliza generalmente para interconectar dos redes distintas o para hacer que una aplicación entienda los datos generados por otra aplicación distinta.

HIPERLAN. High-Perfomance Radio Local Area Network, 'Red de Area Local de Radio de Alto Rendimiento'. Es un estándar de red de área local inalámbrica definido por ETSI (Instituto Europeo de Normalización en Telecomunicaciones) que permite transmitir datos hasta 54 Mbps trabajando en la banda de 5 GHz.

HOMERF. Home Radio Frequency', 'Radio Frecuencia del Hogar'. Es una tecnología de red de área local inalámbrica que en su día fue promovida por Intel (además de otros). Existen tres versiones en el mercado que alcanzan los 1,6, 10 y 40 Mbps, respectivamente. En cualquier caso, HomeRF ha quedado hoy en día en el olvido debido al auge de Wi-Fi.

IBSS. Jndependent Basic Service Set, 'Conjunto de Servicios Básicos Independientes'. Es una de las modalidades de comunicación en las que se pueden configurar los terminales de una red Wi-Fi. En este caso, la red inalámbrica no dispone de punto de acceso, llevándose a cabo las comunicaciones de forma directa entre los distintos terminales que forman la red. Este modo de conexión también es conocido como modo ad hoc, modo independiente o de igual a igual peer-to-peer en inglés).

IEEE. Acrónimo del Instituto de ingenieros eléctricos y electrónicos.

ISO. International Standard Organization, 'Organización Internacional para la Normalización'. Esta organización ha definido los protocolos de comunicaciones conocidos como ISO/OSI, utilizado por las redes públicas de conmutación de paquetes.

ITU. Acrónimo de la Unión internacional de telecomunicaciones. Institución internacional que desarrolla estándares en todo el mundo para las tecnologías de telecomunicaciones.

IV. Acrónimo de Vector de inicialización. Un valor externo necesario para iniciar las operaciones de cifrado; en otras palabras, un valor matemático que depende del texto cifrado para su codificación. Un IV con frecuencia se puede considerar una forma de clave de mensaje. En general, un IV debe acompañar al texto cifrado, y por tanto, siempre extiende el texto con el tamaño del IV. En las redes 802.11, se recomienda que se despliegue un IV único por paquete para eliminar una secuencia predeterminada que los piratas informáticos puedan explotar. En particular, esto ocasiona que sea difícil para los piratas informáticos escribir o

realizar ataques que usen tablas matemáticas, que simplemente programan el número de combinaciones de la clave hasta que se descubre alguna o más que funcionan.

LAN. Acrónimo de Red de área local. Una red de datos de alta velocidad y pocos errores que cubre un área geográfica relativamente pequeña (por lo común, algunos miles de metros). Las LAN se conectan a estaciones de trabajo, periféricos, terminales y otros dispositivos dentro de un solo edificio u otra área limitada geográficamente. Los estándares LAN especifican el cableado y el método de señales de las capas física y de enlace de datos del modelo OSI. Ethernet, UDDI y Token Ring son tecnologías LAN que se usan ampliamente. Se compara con una MAN y una WAN.

MAC. Acrónimo del Control de acceso a medios. La inferior de las dos subcapas de la capa de enlace de datos definida por el IEEE. La subcapa MAC controla el acceso a los medios compartidos, por ejemplo, si se usará el pase de tokens o la contención.

método de acceso. Generalmente, la forma mediante la cual los dispositivos de red acceden a otras redes; en otras palabras, el medio que conecta a las LAN. Los ejemplos incluyen los sistemas inalámbricos fijos de banda ancha, DSL y módems de cable.

módem. Contracción de modulador/demodulador. Un dispositivo que convierte señales digitales y análogas. En la fuente, un módem convierte las señales digitales a una forma que se ajuste a la transmisión a través de equipo de comunicación análoga. En el punto de destino, las señales análogas se vuelven a convertir a la forma digital. Los módems permiten la transmisión de datos a través de las líneas telefónicas de voz.

modulación. El proceso mediante el cual las características de las señales eléctricas se transforman para representar información.

nodo. En general se le llama nodo a cualquier ordenador conectado a una red.

OFDM. Acrónimo de la Multiplexión por división ortogonal de frecuencia. Una técnica de modulación UDM que se usa para transmitir señales al dividir la señal de radio en varias frecuencias en las que se transmite en forma simultánea. Una de las diferencias principales entre OUDM y DHSS o UHSS es que las señales en OUDM se envían simultáneamente a través del tiempo en lugar de manera secuencial.

OSI. Abreviatura del Modelo de referencia de Interconexión de sistemas abiertos. Algunas ocasiones se conoce como Pila de referencia 081. Es el modelo de arquitectura de red desarrollado por ISO e ITU-T. El modelo consiste de siete capas, cada una de las cuales realiza funciones de red específicas, por ejemplo, asignación de direcciones, control de flujo, control de errores, encapsulado y transferencia confiable de mensajes. La capa inferior (capa física) es la que está más cercana a la tecnología de medios. Las dos capas inferiores se implementan en el hardware y software, mientras que las cinco capas superiores sólo están implementadas en el software. La capa más alta (capa de aplicación) es la más cercana al usuario. El modelo

de referencia 051 se usa de forma universal como un método para enseñar y entender la funcionalidad de una red. Es parecida en algunos aspectos a SNA. Otros términos asociados son: capa de aplicación, capa de enlace de datos, capa de red, capa física, capa de presentación, capa de sesión y capa de transporte.

paquete. Agrupamiento lógico de información que incluye un encabezado que contiene la información de control y (normalmente) los datos del usuario. Los paquetes se usan con mayor frecuencia para referirse a las unidades de datos de la capa de red. Los términos datagrama, trama, mensaje y segmento también se usan para describir los agrupamientos lógicos de información en varias capas del modelo de referencia 081 y en distintos círculos tecnológicos.

PCI. Peripheral Component Interconnect, Interconexión de Componentes Periféricos'. Son unas especificaciones creadas por Intel y que definen un sistema de bus local que permite conectar al PC hasta 10 tarjetas de periféricos. El estándar PCI ha venido a reemplazar al antiguo estándar ISA (1ndi£strv Standard Architecture).

PCMCIA. Personal Computer Memory Card International Associotion, 'Asociación Internacional de Tarjetas de Memoria para Ordenadores Personales'. Se trata de una asociación de fabricantes de equipos que en 1989 sacó al mercado un tipo de puerto y de dispositivo de pequeño tamaño que permite que se le puedan instalar todo tipo de periféricos a los ordenadores personales. En un principio se dedicaron sólo a ampliar la memoria, de ahí su nombre. Tanto el puerto como los dispositivos reciben también el nombre de PCMCIA. En inglés se la conoce más coloquialmente como PC Card (tarjeta de PC).

pila de protocolos. Conjunto de protocolos de comunicación relacionados que operan juntos y, como un grupo, resuelven la comunicación en alguna o todas las siete capas del modelo de referencia 051. No todas las pilas de protocolo cubren cada una de las capas del modelo y con frecuencia un solo protocolo de la pila incluye un número de capas a la vez. **TCP/IP** es una pila de protocolos típica.

puente. Dispositivo que conecta y pasa paquetes entre dos segmentos de red que usan el mismo protocolo de comunicación. Los puentes operan en la capa de enlace de datos (Capa 2) del modelo de referencia 051. En general, un puente filtrará, reenviará o rechazará una trama entrante basándose en la dirección MAC de esa trama.

QAM. Acrónimo de la Modulación de amplitud de cuadratura. Método de modulación de señales digitales en una señal de portadora de frecuencia de radio que se relaciona con la amplitud y el código de fase. QAM es un esquema de modulación que se usa principalmente en la dirección de flujo descendente (QAM-64, QAM-256). QAM- 16 normalmente se usa más en la dirección de flujo ascendente. Los números indican la cantidad de puntos de código por símbolo.

QoS. Acrónimo de Calidad de servicio. Una característica de algunos protocolos de red que trabajan con tipos distintos de tráfico de red en forma distinta para asegurar los niveles requeridos de confiabilidad y latencia de acuerdo con el tipo de tráfico. Algunos tipos de tráfico, por ejemplo, el de voz y video, son más sensibles a los reterasos en la transmisión y, por tanto,

tienen prioridad sobre los datos que son menos sensibles a los retrasos. Por ejemplo, los sistemas Cisco Systems PTM BBUW tradicionalmente tienen cuatro niveles de QoS, pero algunos sistemas tienen hasta 13 niveles, dependiendo de cuántos bits se usen para priorizar el tráfico. La mayor parte de los sistemas usan tres o cuatro niveles de QoS, mismos que se conocen normalmente como Servicio garantizado no solicitado (UGS, por sus siglas en inglés), Bit de velocidad constante (CBR; en ocasiones conocido como CIR o velocidad de información constante) y velocidad del mejor esfuerzo (BER). USG tiene una prioridad sobre CIR/CBR, que a su vez tiene prioridad sobre BER. Los niveles QoS se establecen en la Capa 2 (capa de enlace de datos) de la pila de referencia 051.

QPSK. Acrónimo de la Modulación de fase por desplazamiento en cuadratura. Un método de modulación de señales digitales en señales de portadora de frecuencia de radio mediante el uso de cuatro estados de fase para codificar dos bits digitales.

RC4. Un algoritmo de seguridad que usa WEP. Considerado abiertamente como un algoritmo inseguro, RC4 fue desarrollado en 1987 por Ron Rivest, para la compañía RSA Data Security y fue un algoritmo propietario hasta 1994, cuando el código fue publicado en Internet y por tanto, para el resto del mundo.

red. Conjunto de ordenadores interconectados entre sí. También puede hacer referencia a la infraestructura que permite la interconexión de estos ordenadores.

red de área local. Es una red de datos que interconecta ordenadores situados en el entorno de un edificio o de las oficinas de una empresa dentro de ese edificio. Una red local permite a sus usuarios compartir información y recursos de la red, corno impresoras o lineas de comunicaciones (acceso a Internet).

RF. Acrónimo de Frecuencia de radio. En general, se refiere a las comunicaciones inalámbricas con frecuencias por debajo de 300 GHz. El término RU se usa comúnmente también para cubrir todos los tipos de sistemas inalámbricos.

RFC. Acrónimo de Solicitud de comentarios. Conjunto de documentos que se usa como el medio principal para comunicar información acerca de Internet. Probablemente las versiones más conocidas son las del IEEE. Algunas RFC son designadas como estándares de Internet. La mayor parte de las RUC documentan especificaciones de protocolo, por ejemplo, Telnet y UTP, pero algunas son humorísticas o históricas. Las RUC están disponibles en línea desde varias fuentes.

router . Es un sistema utilizado para transferir datos entre dos redes que utilizan un mismo protocolo. Un router puede ser un dispositivo software, hardware o una combinación de ambos. Los puntos de acceso, generalmente, hacen las funciones de router. A este equipo también se le conoce en español por el nombre de enrutador.

señal análoga. La representación de información mediante una cantidad física que varía continuamente, por ejemplo, el voltaje. Debido a este cambio constante de la forma de la onda respecto a su paso a través de un punto determinado en el tiempo o espacio, una señal análoga puede tener una cantidad infinita de estados o valores. Esto contrasta con una señal digital, la que tiene un número muy limitado de estados.

servidor. Se trata de un software que permite ofrecer servicios remotos a sus usuarios. También puede recibir el nombre de servidor el propio ordenador donde está instalado el software servidor. El ordenador de los usuarios contacta con el servidor gracias a otro software llamado cliente.

SOHO . Acrónimo de Oficina pequeña/oficina del hogar.

TCP. Acrónimo del Protocolo de control de transmisión. Es un protocolo de la capa de transporte orientado a las conexiones y proporciona la transmisión de datos dúplex completa confiable. Es parte de la pila de protocolos TCP/IP.

TCP/IP. Acrónimo de Protocolo de control de transmisión/Protocolo de Internet. Es el nombre común para el conjunto de protocolos que desarrolló el Departamento de defensa (DoD, por sus siglas en inglés) en la década de los setenta para soportar la construcción de redes interconectadas en todo el mundo. TCP e IP son los dos protocolos más conocidos del conjunto.

texto cifrado. Texto que ha sido cifrado o codificado. A pesar de que el texto cifrado contiene la misma información que el texto simple, puede contener, o no, el mismo número de bits. Es posible que algunos sistemas de bajo nivel tengan dificultades para resolver el cifrado, para lo cual se usa el término cifrado de expansión de datos. El texto cifrado siempre requiere de una clave para determinar el texto sencillo.

texto sencillo. La información original que se puede leer. Normalmente es un conjunto de caracteres alfanuméricos, pero también puede tener otras formas de datos, por ejemplo, valores o símbolos matemáticos.

Trama. Agrupamiento lógico de información que se envía como una unidad de la capa de enlaces de datos a través de un medio de transmisión. Con frecuencia, se refiere al encabezado y al indicador de fin, empleado en la sincronización y control de errores, que rodea a la información de usuario contenida en la unidad. Los términos célula, datagrama, mensaje, paquete y segmento también se usan para describir agrupamientos de información lógicos en varias capas del modelo de referencia OSI y en distintos círculos tecnológicos.

transceiver. Transmiter-Receiver, 'Transmisor-Receptor'. Es un equipo de radio que puede tanto transmitir como recibir.

U-NII. Acrónimo de Infraestructura nacional de información libre de licencia. Principalmente una banda de frecuencia de Estados Unidos. Los productos inalámbricos para esta banda funcionan en la frecuencia de 5.725 a 5.825 GHz para el uso exterior. Existen otras dos bandas U-NII: 5.15 a 5.25 GHz y 5.25 a 5.35 GHz. La banda de 5.15 GHz es para el uso en interiores sólo en Estados Unidos, mientras que la banda de 5.25 a 5.35 GHz se puede usar tanto en interiores como en exteriores dentro de Estados Unidos. Los dos conjuntos inferiores de frecuencia U-NII, se transmiten con niveles de potencia más bajos que los de la banda de 5.725 a 5.825 GHz. Estas frecuencias no requieren el uso o compra de una licencia de sitio, pero el equipo requiere de una certificación de la UCC y el cumplimiento estricto con sus regulaciones. U-NII fue un término creado por los reguladores federales

para describir el acceso de ciudadanos y empresas a una red de información. Es equivalente al término "supercarretera de información", no describe la arquitectura, protocolo o topología de los sistemas.

VLAN. Acrónimo de Red de área local virtual. Un grupo de clientes que están ubicados en distintos lugares pero que se comunican entre ellos como si pertenecieran al mismo segmento LAN.

VoIP. Acrónimo de Voz sobre IP. Permite a un direccionador transportar tráfico de voz (por ejemplo, llamadas telefónicas y faxes) en una red IP. En VoIR el DSP segmenta las señales de voz en tramas, las cuales se agrupan en conjunto de dos y se almacenan en paquetes de voz. Estos paquetes de voz se transportan usando IP de acuerdo con la especificación H.323 de ITU-T.

VPN. Acrónimo de Red privada virtual. Una red privada virtual es un enlace privado que reside entre dos partes pero viaja a través de redes públicas.

WAN. Acrónimo de Red de área amplia. Red de comunicaciones de datos que da servicio a usuarios que se encuentran en un área geográfica y extensa, y con frecuencia usan dispositivos de transmisión proporcionados por las compañías de telecomunicaciones comunes.

WECA. Wireless Ethernet Compability Alliance, 'Alianza de Compatibilidad Ethernet Inalámbrica'. Es una asociación de fabricantes de equipos de red creada en 1999 con el objetivo de fomentar la tecnologia inalámbrica y asegurase la compatibilidad de equipos. WECA es la creadora de la marca Wi-Fi y es quien certifica los equipos con esta marca.

WEP. Acrónimo del Protocolo equivalente al cableado. WEP es un protocolo de seguridad que principalmente usan los radios 802.11 para proteger las comunicaciones inalámbricas de robo de información y de espionaje, además, evita el acceso no autorizado a una red inalámbrica. El sistema WEP surgió con la idea de ofrecerle a las redes inalámbricas un estado de seguridad similar al que tienen las redes cableadas.

WI-FI. Wireless Fidelity, 'Fidelidad Inalámbrica'. Es una marca creada por la asociación WECA con el objetivo de fomentar la tecnología inalámbrica y asegurarse la compatibilidad de equipos. Todos los equipos con la marca Wi-Fi son compatibles entre sí y utilizan la tecnología inalámbrica defiruda por el IEEE en su estándar 802.1 lb.

WLAN. Wireless Local Area Network, 'Red de Área Local Inalámbrica'. Es el acrónimo con el que se hace referencia a las redes de área local inalámbricas. Las redes Wi-Fi son un ejemplo de este tipo de redes.

WPA. Wi-Fi Protecied Access, 'Acceso Wi~Fi Protegido'. Son unas especificaciones de seguridad basadas en el estándar lEE 802.11 i que incrementa fuertemente el nivel de protección de datos y de control de acceso de las redes Wi-Fi. Las facilidades de seguridad ofrecidas por WPA pueden implantarse en las redes Wi-Fi existentes mediante una instalación de software.

APÉNDICE B

BIBLIOGRAFÍA

A continuación se dispone la bibliografía que fue consultada para la realización de esta tesis, la gran mayoría de esta bibliografía pertenece a Internet, ya que ésta es una inmensa biblioteca donde se encuentra todo tipo de información. A pesar de lo anterior, las direcciones consultadas fueron validas para el día de su consulta, la información contenida en Internet tiende a ser inestable, por lo que existe la posibilidad de que algunas de ellas no existan dentro de un tiempo.

www.34t.com/box-does.asp

www.3com.com

http://www.andaluciawireless.net/

www.arc.com.mx

www.arrakis.es/~sergilda/wlan

www.bluetooth.com

www.cisco.com

www.e-advento.com

http://es.wikipedia.org/wiki/Wi-Fi

www.ericsson.com

www.freenetworks.org

www.grouper.ieee.org/groups/802/11/Documents/index.html

www.homerf.org

www.ibm.com

www.ieee.org

www.intel.com

http://www.irit.fr/~Ralph.Sobek/wifi/

www.jalercom.com

www.lucent.com

www.madridwireless.net

www.microsoft.com

www.microsoft.com/latam/windowsxp/pro/biblioteca/planning/wirelesslan/default.asp

www.mobilestar.com

www.mobilian.com

www.nokia.com

www.nycwireless.et

http://www.nextec.com.ar/redes_Inalambricas/redes_inalambricas.html

www.opennetworks.org3.net

www.proxim.com

www.seattlewireless.net

www.sincables.net

www.standards.ieee.org/wireless

www.tecnotopia.com.mx

www.telefonica.net

www.telefonicaonline.com

www.toshiba.com

www.wi-fi.org

www.wirelessdevnet.com

www.wirelessunlimited.org

www.wirelessweek.com

www.wlana.com

www.zaragozawireless.org

- 802.11 (Wi-Fi)
Manual de redes Inalámbricas
Neild Reid y Ron Seide
Mc Graw Hill

-802.11Wireless Networks
The Definitiv Guide
Matthew Gast
O Reilly

-CCIE Fundamentals Network Desing an Case Studies
Cisco Systems

-Creación de Redes Cisco Escalables
Catherine Paquet y Piane Teare
Cisco Systems

-Data Computer Communications
Hura Singhal
CCR Presss

-IEEE Wireless LAN Edition
A compilation based on
IEEE Std. 802.11™ – 1999(R2003)
And its amendments

-Introducción a Redes Inalambricas
Adam Engst, Glenn Fleishman
Anaya Multimedia

-Redes de Computadora
Andrew S. Tanenbaum
Pearson

-TCP/IP Network Administration
Craighunt
O'Reilly & Asociate, Inc.

-Wi-Fi
Como construir una red inalámbrica
José A. Carballar
Alfaomega & Ra-Ma®