**UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO.**

**FACULTAD DE ESTUDIOS SUPERIORES ARAGON.**

# REDES INALAMBRICAS, COMUNICACIÓN Y NORMATIVIDAD.

**TESIS.**

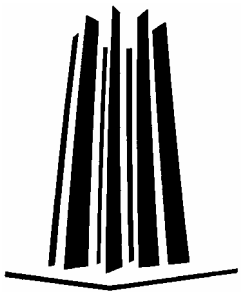
**PARA OBTENER EL TITULO DE:**

**INGENIERO MECANICO ELECTRICISTA.**
**AREA.- ELECTRICA ELECTRONICA.**

**PRESENTAN.**

**GALICIA LONA JUAN ROBERTO.**
**QUINTAS MORALES ISAIAS.**

**ASESOR. ING. BENITO BARRANCO CASTELLANOS**



**San Juan de Aragón, Edo. De México** **2006.**

**TESIS.**

**Redes Inalámbricas, Comunicación y Normatividad.**



**Asesor: Ing. Benito Barranco Castellanos**

**Introducción**

Una de las tecnologías más interesantes en la actualidad son las redes de área local inalámbricas. El gran lugar que esta ocupando esta tecnología se debe en gran parte al hecho de que es una gran tecnología que ha permanecido en un estado de receso durante los dos últimos años. Otra medida seria la de los miles de millones de dólares en ventas anuales que esta tecnología genera en todo el mundo. El estándar predominante de esta tecnología era, y sigue siendo, recopilado por el IEEE que cuenta con una gran variedad de grupos de trabajo realizando tareas alrededor de 802.11. Estos grupos de trabajo se avocan a una multitud de aspectos que constituyen un reto.

Los conocimientos técnicos en esta materia, las aplicaciones prácticas que se desprenden de ellos, y un entendimiento del amplio conjunto de aspectos son tan importantes en la actualidad como el entendimiento de ethernet. Mientras que la gran cantidad de discusiones que lleva a cabo los administradores de la red, fabricantes de tecnología se centraban en la rapidez en la que se desempeñaba un radio, hoy en día las discusiones se enfocan en la seguridad y en la movilidad en general.

Aunque la tecnología se le conoce como redes de área local inalámbricas en realidad se trata de tecnología de radio. Por tanto, no obstante que la historia de WI-FI u 802.11 sólo existe a partir de mediados de la década de los ochentas, en realidad esta tecnología comenzó 100 años atrás.

La conexión de computadoras mediante Ondas de Radio 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, como en almacenes o en oficinas que se encuentren en varios pisos.

También es útil para hacer posibles sistemas basados en plumas. Pero la realidad es que esta tecnología está todavía en pañales y se deben de resolver varios obstáculos técnicos y de regulación antes de que las redes inalámbricas sean utilizadas de una manera general en los sistemas de cómputo de la actualidad.

No se espera que las redes inalámbricas lleguen a remplazar a las redes cableadas. Estas ofrecen velocidades de transmisión mayores que las logradas con la tecnología inalámbrica. Mientras que las redes inalámbricas actuales ofrecen velocidades de 2 Mbps, las redes cableadas ofrecen velocidades de 10 Mbps y se espera que alcancen velocidades de hasta 100 Mbps. Los

sistemas de Cable de Fibra Optica logran velocidades aún mayores, y pensando futuristamente se espera que las redes inalámbricas alcancen velocidades de solo 10 Mbps.

Sin embargo 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 y el operador se pueda desplazar con facilidad dentro de un almacén o una oficina.

En este trabajote tesis se abordara lo siguiente.-

En e capitulo uno de manera general se menciona como esta estructurada una red inalámbrica en cuanto a su historia y los organismos que la conforman y se hace una descripción de cómo se conecta una WLAN.

En el capitulo dos se basa en la normatividad de la red y como la norma 802.11 es la que rige el diseño de la misma, se enumeran sus diferentes variables y se sugiere el planteamiento y la arquitectura para implementar una red Wi-Fi.

En capitulo III se implementa ya la red

# Capitulo I.

# Redes WLAN

# REDES INALÁMBRICAS DE ÁREA LOCAL

La comunicación inalámbrica puede dividirse en dos categorías: La comunicación inalámbrica en una red de área local, que trataremos aquí, y la comunicación móvil inalámbrica. La diferencia fundamental entre ambas radica en los modos de transmisión. Las LAN inalámbricas emplean transmisores y receptores que se encuentran en los edificios en que se usan mientras que las comunicaciones móviles inalámbricas usan las compañías de telecomunicaciones telefónicas u otros servicios públicos en la transmisión y recepción de las señales.

***Definición:*** Una red de área local inalámbrica o WLAN (Wireless LAN) puede definirse como una red local (Red de comunicación con una cobertura geográfica limitada, relativamente alta velocidad de transmisión, baja tasa de errores y administrada de forma privada) que utiliza ondas electromagnéticas para enlazar los equipos conectados a la red en lugar de los cables coaxiales, de par trenzado o de fibra óptica que se utilizan en las LAN convencionales cableadas. Estos enlaces se implementan básicamente a través de tecnología de microondas y -en menor medida- de infrarrojos.

Las redes locales inalámbricas, (WLANs o Wireless LANs, en inglés), han sido utilizadas tanto en la industria y la oficina como en centros de investigación desde hace más de 15 años. Su atractivo viene dado por las prestaciones en cuanto a la facilidad de instalación y renunciación (y el ahorro consiguiente) que pueden ofrecer una red sin hilos frente a una red de cable y que la convierten en una opción interesante no tanto para sustituirlas -pues sus prestaciones son menores- como para constituirse en su complemento ideal. Por otro lado permiten también implementar redes en situaciones en las que el cableado, o bien no es viable, o bien no es la solución óptima.

Entre las múltiples aplicaciones que en la actualidad se les esta dando a este tipo de redes, estacan estas:

- Entornos de difícil cableado, como edificios históricos, instalaciones con asbesto, ...
- Entornos cambiantes, como los de algunos minoristas, fabricantes, bancos ...
- Redes locales para situaciones de emergencia, como respaldo para reactivar partes críticas de una red en contingencias o siniestros.
- Para proporcionar acceso a la red a ordenadores portátiles, en algunos trabajos (enfermeras, médicos, minoristas, oficinistas ...) se requiere acceso a la información mientras se esta en movimiento. Por ejemplo : un centro de salud donde los médicos pueden examinar la hoja clínica de un paciente mientras se desplazan de la sala de urgencias a la de recuperación, ...
- En lugares o sedes temporales donde podría no compensar la instalación de cableado. Por ejemplo para establecer reuniones " ad hoc" y grupos de trabajo de corto plazo.
- Para interconectar dispositivos en ambientes industriales con severas condiciones ambientales.
- Para interconectar redes locales entre dos edificios,

## HISTORIA

El origen de las LAN inalámbricas (WLAN) se remonta a la publicación en 1979 de los resultados de un experimento realizado por ingenieros de IBM en Suiza, consistente en utilizar enlaces infrarrojos para crear una red local en una fábrica. Estos resultados, publicados en el volumen 67 de los Proceeding del IEEE, puede considerarse como el punto de partida en la línea evolutiva de esta tecnología.
Las investigaciones siguieron adelante tanto con infrarrojos como con microondas, donde se utilizaba el esquema del spread spectrum, siempre a nivel de laboratorio. En mayo de 1985, y tras cuatro años de estudios, el FCC (Federal Communications Comission), la agencia federal del Gobierno de Estados Unidos encargada de regular y administrar en materia de telecomunicaciones, asignó las bandas IMS (Industrial, Scientific and Medical) 902-928 MHz, 2,400-2,4835 GHz, 5,725-5,850 GHz a las redes inalámbricas basadas en spread spectrum. (IMS es una banda para uso comercial sin licencia).
La asignación de una banda de frecuencias propició una mayor actividad en el seno de la industria: ese respaldo hizo que las WLAN empezaran a dejar ya el laboratorio para iniciar el camino hacia el mercado. Desde 1985 hasta 1990 se siguió trabajando ya más en la fase de desarrollo, hasta que en mayo de 1991 se publicaron varios trabajos referentes a WLAN operativas que superaban la velocidad de 1 Mbps, el mínimo establecido por el IEEE 802 para que la red sea considerada realmente una LAN.

Hasta entonces, estas redes habían tenido una aceptación marginal en el mercado. Las razones eran varias:

- Gran cantidad de técnicas, tecnologías y normas existentes en el ámbito de las comunicaciones móviles debido a que los diferentes fabricantes han ido desarrollando sus propias soluciones, utilizando frecuencias y tecnologías muy distintas y normalmente incompatibles. No existía una norma ...
- Altos precios que reflejan los costes de investigación para desarrollar soluciones tecnológicas propietarias.
- Reducidas prestaciones si las comparamos con sus homologas cableadas: las redes inalámbricas únicamente permiten el soporte de datos, mientras que por una red de cableado podemos llevar multitud de aplicaciones tanto de voz, como de datos, vídeo, etcétera, y además, velocidades de transmisión significativamente menores

### Normalización

En 1990, en el seno de IEEE 802, se forma el comité IEEE 802.11, que empieza a trabajar para tratar de generar una norma para las WLAN. Pero no es hasta 1994 cuando aparece el primer borrador, y habrá que esperar a junio de 1997 para dar por finalizada la norma.
En 1992 se crea Winforum, consorcio liderado por Apple y formado por empresas del sector de las telecomunicaciones y de la informática para conseguir bandas de frecuencia para los sistemas PCS (Personal Communications Systems). En ese mismo año, la ETSI (European Telecommunications Standards Institute), a través del comité ETSI-RES 10, inicia actuaciones para crear una norma a la que denomina HiperLAN (High Performance LAN) para, en 1993, asignar las bandas de 5,2 y 17,1 GHz.
En 1993 también se constituye la IRDA (Infrared Data Association) para promover el desarrollo de las WLAN basadas en enlaces por infrarrojos.
En 1996, finalmente, un grupo de empresas del sector de informática móvil y de servicios forman el Wireless LAN Interoperability Forum (WLI Forum) para potenciar este mercado mediante la creación de un amplio abanico de productos y servicios interoperativos. Entre los miembros

fundadores de WLI Forum se encuentran empresas como ALPS Electronic, AMP, Data General, Contron, Seiko, Epson y Zenith Data Systems.
En un futuro no lejano, el previsible aumento del ancho de banda asociado a las redes inalámbricas y, consecuentemente, la posibilidad del multimedia móvil, permitirá atraer a mercados de carácter horizontal que surgirán en nuevos sectores, al mismo tiempo que se reforzarán los mercados verticales ya existentes. La aparición de estos nuevos mercados horizontales está fuertemente ligada a la evolución de los sistemas PCS (Personal Communications systems), en el sentido de que la base instalada de sistemas PCS ha creado una infraestructura de usuarios con una cultura tecnológica y hábito de utilización de equipos de comunicaciones móviles en prácticamente todos los sectores de la industria y de la sociedad.
Esa cultura constituye el caldo de cultivo para generar una demanda de más y más sofisticados servicios y prestaciones, muchos de los cuales han de ser proporcionados por las WLAN.

**Organismos**

Existen algunos organismos europeos que colaboran en la definición de normas y recomendaciones en materia de telecomunicaciones y radiofrecuencia. A continuación, una descripción rápida de los más destacados.

**CEPT.**

Acrónimo de European Conference of Postal and Telecommunications Admi-nistrations, es la organización de referencia para Europa en materia de telecomunicaciones. Las diferentes Administraciones nacionales de correos y telecomunicaciones participan en la definición de Recomendaciones y Decisiones a nivel general acerca de problemáticas de telecomunicaciones que tendrían que facilitar la integración entre los Países miembros.

**ERC y ERO.**

El ERC (European Radiocommunications Committee) es el foro específico donde las Administraciones nacionales de correos y telecomunicaciones coordinan e implementan los procesos de normalización de las comunicaciones radio en Europa, dentro de la CEPT.
Además de las actividades diarias y los Grupos de Trabajo específicos, el ERC tiene también una oficina permanente, el ERO (European Radiocommunications Office), que representa el punto de referencia para los contactos y el intercambio de la información entre expertos.
Los objetivos principales del ERC son los de coordinar, con los demás órganos dentro de la CEPT, el tema de la comunicación radio en relación con el aspecto más general de las telecomunicaciones, además de desarrollar políticas comunes y coordinar normativas y directrices para las comunicaciones radio en los Países miembros.

**ETSI**

El ETSI (European Telecommunica-tions Standard Institute) desarrolla las normas europeas de telecomunicaciones y trabaja en colaboración estrecha con las demás organizaciones. El Instituto, merced a la autofinanciación de sus miembros, es autónomo y libre de decidir las políticas y las prioridades en materia de normas.
El ETSI produce documentos llamados ETS (European Telecommunication Standard) que contienen las especificaciones técnicas, las características de los productos para telecomunicaciones y la información técnica necesaria que describe los métodos de ensayo a efectuar para conseguir las homologaciones de los productos respecto de la normativa ETS específica.

Un documento ETS puede utilizarlo como base técnica la Unión Europea cuando aborda temas relacionados con las telecomunicaciones.
Otros documentos producidos por el ETSI son: I-ETS (ETS interino), que presentan soluciones provisionales que requieren estudios ulteriores; TBR (Technical Bases for Regulation) que forman el conjunto de las especificaciones que podría utilizar la Comisión Europea a objetos de normativa; ETR (ETSI Technical Report) que proporcionan comentarios y directrices acerca de temas no abordados por los ETS o los I-ETS; además, se producen otros documentos interiores de contenido básicamente técnico.

El aspecto de la gestión de las frecuencias en el territorio, la normativa para los usuarios, las modalidades de autorización para el uso (homologación) de los productos son temas que corresponden a cada País europeo. El Gobierno Español, a través de la Secretaría General de Telecomunicaciones del Ministerio de Fomento, tiene el exclusivo derecho a decidir la aproximación relativa a estos aspectos a través de Decretos válidos en el territorio español.

A los diferentes Países europeos se les pide que acepten, dentro de lo posible, las recomendaciones y las Decisiones de la CEPT, con el objeto de facilitar la integración de las telecomunicaciones a nivel europeo. Como se ha visto, a través de su ERC y con el apoyo del ERO, la CEPT tiene por objetivo la armonización de los procedimientos de reglamentación y la adopción de las normas en todos los 43 Países miembros, que mantienen el derecho de decidir a nivel interior.

**Ets 300 328**

Otro ejemplo de como las Administraciones locales desempeñan un papel decisorio interno es Francia y España que adoptaron normas diferentes en tema de ensayos de autorización aplicables con arreglo a ETS 300 328.
Esta norma indica las características técnicas de los productos para transmisión de datos a 2,4 GHz con tecnologías Spread Spectrum y las condiciones de los ensayos de homologación correspondientes.
Para matizar la importancia internacional de la norma ETS 300 328 cabe recordar la reciente Decisión del ERC, llamada ERC/DEC(96)17, en la que la misma se indicó como referencia a nivel europeo para las telecomunicaciones en la banda 2,4 GHz de los sistemas Spread Spectrum.
A pesar de todo, Francia ha asignado sólo la banda 2,4465-2,4835 GHz para estos productos, mientras que España ha asignado la banda 2,445-2,475 GHz.
Cabe destacar que, a parte esta diferencia, España se ha ajustado completamente a la recomendación CEPT en materia de licencias. A parte la homologación de los equipos, que tiene que efectuarse en España (para ello, puede hacerse referencia a los ensayos realizados en otros países miembros de la Unión Europea), no es obligatorio tener una licencia para el uso de los equipos.

El IEEE (Institute of Electrical and Electronic Engineers) integra en el capítulo 802 las normas concernientes a las redes locales o Lan: la 802.3 marca los criterios para Ethernet, la .4 para Token ring, etc. En 1990 se constituyó una comisión con el objeto de definir las normas para las redes locales en radiofrecuencia o Wireless Lan, marcando el proyecto con el código 802.11, que contenía tan sólo la parte relacionada con la comunicación por aire. La intención era dar la oportunidad de conectar dos sistemas diferentes y de marcas diferentes de manera que pudieran intercambiar datos, sin preocuparse por definir otros elementos, como por ejemplo los protocolos de transmisión o de red.
Se ha trabajado, por consiguiente, tan sólo en las dos primeras de las siete capas del modelo de comunicación ISO/OSI (véase la tabla de referencia), haciendo hincapié, en cuanto a la segunda, en el Medium Access Control y no en el Logical Link Control.

Pero el tema es más complejo, porque las necesidades de una W-Lan van más allá de la mera conexión "estable" de un transmisor a un receptor: los terminales necesitan también conexiones múltiples al mismo punto de acceso y tienen que poder seguir transmitiendo, incluso pasando de una célula a otra (roaming).

**IEEE 802.11: reglas (y libertades) para las W-Lan**

**OPCIONES DE CAPA FÍSICA.**

Como en Ethernet 802.3 (IEEE) y en estándares del token ring (802.5), la especificación de IEEE 802.11 involucra tanto la capa física (PHY) y la de Media Access Control (MAC). En la capa de PHY, IEEE 802.11 define tres características físicas para las redes de área local inalámbricas: el infrarrojo difundido, amplio espectro de secuencia directa (DSSS), y amplio espectro de salto de frecuencia (FHSS).
Mientras que el PHY infrarrojo funciona en la banda base, los otros dos PHYs basadas en radio funcionan en la banda de 2,4 GHz. Esta última banda de frecuencia es parte de qué se conoce como la banda de ISM, una banda global primordialmente para el uso industrial, científico y médico, pero se puede utilizar para operar los dispositivos inalámbricos del LAN sin la necesidad de licencias de usuario final. Para que los dispositivos inalámbricos sean compatibles tienen que establecerse con el mismo estándar de PHY. Las tres PHYs especifican soporte para el data rate de 1 Mbps y 2 Mbps.

IEEE 802.11 define tres posibles opciones para la elección de la capa física:

- Espectro expandido por secuencia directa o DSSS (Direct Sequence Spread Spectrum),
- Espectro expandido por salto de frecuencias o FHSS (Frecuency Hopping Spread Spectrum)
  ambas en la banda de frecuencia 2.4 GHz ISM-
- y luz infrarroja en banda base -o sea sin modular-.

Para algunos, el hecho de que existan varias posibilidades en cuanto a elección de capa física proporciona una mayor flexibilidad de diseño. Para otros, sin embargo, la adopción de distintas capas físicas obligará a utilizar especificaciones adicionales para conseguir la necesaria interoperatividad.
En cualquier caso, la definición de tres capas físicas distintas se debe a las sugerencias realizadas por los distintos miembros del comité de normalización, que han manifestado la necesidad de dar a los usuarios la posibilidad de elegir en función de la relación entre costes y complejidad de implementación, por un lado, y prestaciones y fiabilidad, por otra. No obstante, es previsible que, al cabo de un cierto tiempo, alguna de las opciones acabe obteniendo una clara preponderancia en el mercado. Entretanto, los usuarios se verán obligados a examinar de forma pormenorizada la capa física de cada producto hasta que sea el mercado el que actúe como árbitro final.

**Elección de la capa física.**

La norma IEEE 802.11, la norma de las WLAN, contempla tres capas físicas: infrarroja, DSSS y FHSS. La elección entre infrarrojos y microondas aparece realmente clara en base a la aplicación.
Sin embargo, en lo que respecta a la elección entre DSSS y FHSS existe cierta controversia. La filosofía de los miembros del comité de IEEE al permitir la elección entre dos capas ha sido la de posibilitar que los usuarios exploten las ventajas/características de cada una en determinados aspectos para tratar de optimizar cada solución. Esto añade un factor más de complicación al tema general de interoperatividad de productos, al mismo tiempo que impone la necesidad de evaluar

cuidadosamente cada tecnología, dado que se plantea la necesidad de escoger la tecnología. Este problema de elección entre las dos tecnologías requiere un análisis pormenorizado que, por razones de tiempo fundamentalmente, no se ha podido llevar a cabo, por lo cual nos limitaremos a indicar las líneas principales, que constituyen el estado de la controversia, en el proyecto de instalación.

En resumen para la capa fisica se define:

- Frecuencia de trabajo: 2,4 GHz Spread Spectrum con ancho de banda de 83 MHz (excepto en Francia que son 40 MHz y España que son 30 MHz);
- - Velocidad de transmisión: 1 Mbit/s para FH (con 2 Mbit/s opcional) y 1 ó 2 Mbit/s para DS;
- - Modalidad de transmisión: Direct Sequence y Frequency Hopping;
- - Direct Sequence: 1 Mbit/s con modulación DBPSK (Differential Phase Shift Keying) y 2 Mbit/s con DQPSK (Differential Quadrature Phase Shift Keying). Utiliza 5 sub-bandas de 26 MHz centradas en las frecuencias: 2,412, 2,427, 2,442, 2,457 y 2,470. En España, dada la restricción de banda que existe de 30 MHz, sólo se puede usar una banda centrada en la frecuencia 2,460 GHz;
  - Frequency Hopping: emplea la modulación GFSK (Gaussian Frequency Shift Keying) de 2 ó 4 niveles. La banda ancha está dividida en 79 bandas de 1 MHz excepto en Francia que son 35 bandas y España que está dividida en 27 bandas. Cada banda está sujeta a un mínimo de 2,5 saltos por segundo, utilizando uno cualquiera de los tres esquemas posibles (22 saltos por cada dato esquema). Ello asegura que cada paquete enviado pueda transmitirse en un sólo salto de manera que la información destruida pueda recuperarse en otro salto.

**OPCIONES DE LA CAPA DE ENLACE O CAPA MAC.**

La capa de MAC del 802.11, soportada por una capa subyacente de PHY, se refiere sobre todo a las reglas para tener acceso al medio inalámbrico. Se definen dos arquitecturas de red: la red de infraestructura y la red ad hoc. Una red de infraestructura es una configuración de red para proporcionar comunicación entre clientes inalámbricos y los recursos de la red alámbrica. La transición de datos del medio inalámbrico al alámbrico se hace mediante un Punto de Acceso. El área de cobertura está definida por el Punto de Acceso (AP) y sus clientes inalámbricos asociados, y juntos todos los dispositivos forman un Conjunto de Servicio Básico.
Una red Ad Hoc es una arquitectura que se utiliza para soportar la comunicación mutua entre clientes inalámbricos. Creada típicamente espontáneamente, una red Ad Hoc no soporta el acceso a redes alámbricas, y no necesita un AP para ser parte de la red.

**Los servicios primarios proporcionaron por la capa del MAC son como sigue:**

- **Transferencia de Datos**
  Los clientes inalámbricos utilizan un acceso múltiple con sensor de colisión con algoritmo para evitar colisión (CSMA/CA) como el esquema de acceso de medios.

- **Asociación**
  Este servicio permite el establecimiento de conexiones inalámbricas entre los clientes sin y AP's en redes de infraestructura.

- **Reasociación**
  Esto ocurre además de la asociación cuando un cliente inalámbrico se mueve de un Conjunto de Servicio Básico (BSS) a otro. Dos Conjuntos de Servicios Básicos adjuntos forman un Conjunto de Servicio Extendido (ESS) si son definidos por un ESSID común. Si

se define un ESSID común, un cliente inalámbrico tendrá "roaming" de un área a otra. Aunque la reasociación se especifica en 802,11, el mecanismo que permite que la coordinación de AP-to-AP que maneja el "roaming" no se especifica.

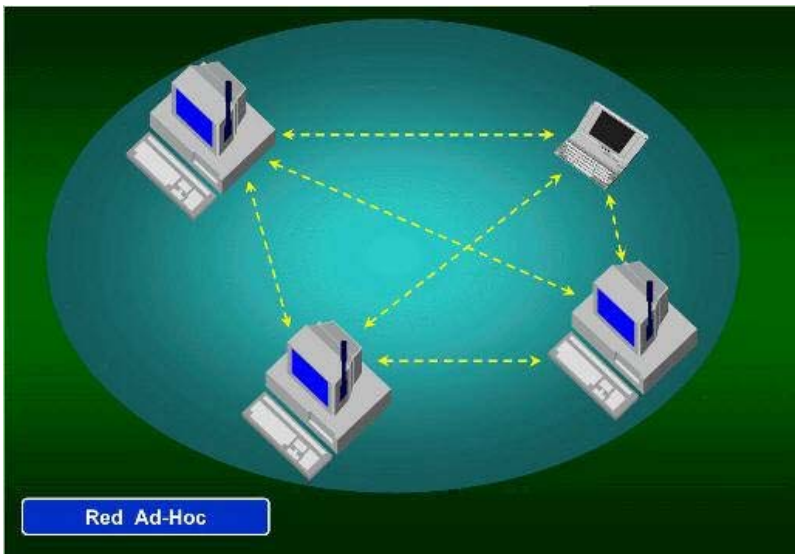
- **Autentificación**
  La autentificación es el proceso de probar la identidad del cliente, y en IEEE 802.11 este proceso ocurre antes de que un cliente inalámbrico se asocie a un AP. Por defecto, los dispositivos IEEE 802.11 funcionan en un sistema abierto, donde esencialmente cualquier cliente inalámbrico puede asociarse a un AP sin control de permisos. La autentificación verdadera es posible con el uso de la opción 802,11 conocida como privacía equivalente alámbrica o WEP, en donde una clave compartida se configura en el AP y sus clientes. Solamente esos dispositivos con clave compartida válida se podrán asociar al AP.

- **Privacidad**
  Por defecto, los datos se transmiten "al aire"; cualquier dispositivo que cumpla con la norma 802.11 puede, potencialmente "escuchar" como en el tráfico de PHY 802.11 que está dentro de rango. La opción WEP cifra los datos antes de que se envíe inalámbricamente, usando un algoritmo de cifrado de 40-bit conocido como RC4. La misma Clave Compartida usada en la autentificación se utiliza para cifrar o para desencriptar los datos; así solamente los clientes inalámbricos con la Clave Compartida exacta pueden descifrar correctamente los datos.

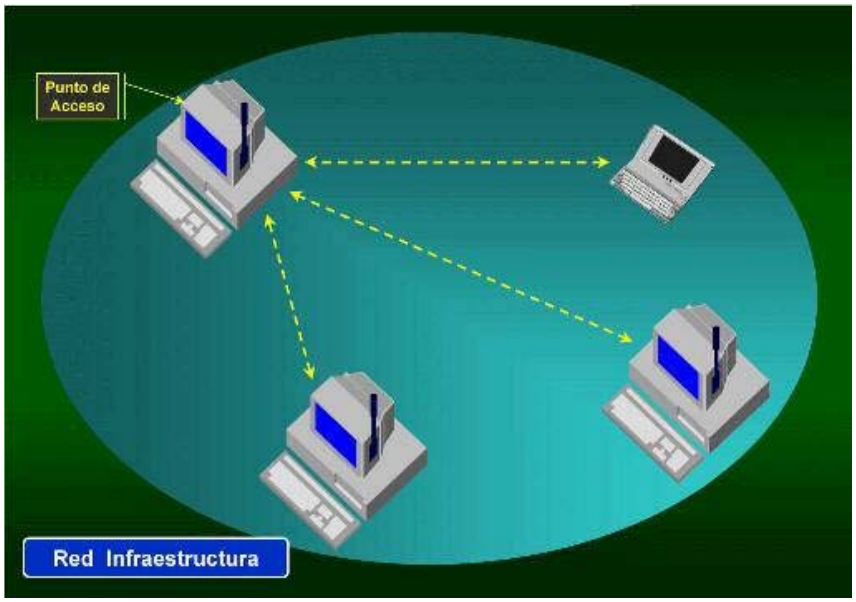
- **Manejo de Potencia**
  IEEE 802,11 define dos modos de potencia, un Modo Activo, donde un cliente inalámbrico es habilitado para transmitir y recibir y un modo Economizador, donde un cliente no es capaz de transmitir o de recibir, pero consume menos potencia. El consumo de energía real no se define y es dependiente sobre la puesta en práctica.

**El estándar establece dos topologias o configuraciones básicas:**

- En la primera –**RED AD-HOC-**, también llamadas redes entre pares, varios equipos conforman una red para intercambiar información sin contar con el apoyo de elementos auxiliares. Este tipo de red es muy conveniente para conformar grupos de trabajo ( work groups) temporales en reuniones, conferencias, etc.



- En la segunda configuración –**RED BASADA EN INFRAESTRUCTURA**- (mucho más popular en la actualidad), las WLANs se constituyen como una extensión a la infraestructura de red preexistente basada en cable . En este modelo los nodos inalámbricos se encuentran conectados a la red alambrica a través de un PC bridge o a través de un punto de acceso -un transceptor-. Los puntos de acceso controlan el trafico de las transmisiones entre las estaciones inalámbricas -que constituyen la celula o BSS-, o de ellas hacia la red alambrica -y viceversa-.
  Es aquella en la que todos los ordenadores (de sobremesa y/o portátiles) provistos de tarjetas de red inalámbrica trabajan en orden jerárquico, por el que uno de los ordenadores de la red es el punto de enlace entre todos los PCs de la misma red. Desde ese ordenador se lleva el control de acceso, como medida de seguridad del resto de los equipos que forman parte de la red.




Diseñar un protocolo de acceso para WLANs resulta mucho más complejo que hacerlo para redes locales basadas en cable por varias razones: se deben considerar distintas configuraciones como redes ad-hoc y aquellas basadas en infraestructura; perturbaciones ambientales como interferencias y variaciones en la potencia de la señal, introducen variaciones severas en el tiempo de acceso y en la tasa de errores de transmisión; al contar con equipos móviles se pueden presentar conexiones y desconexiones repentinas en la red; debe contarse con un mecanismo de relevo entre celdas para atender a nodos móviles que pasan del área de cobertura de una celda a otra ( roaming), etc.
A pesar de todo esto, la norma IEEE 802.11 define una única capa MAC -dividida en dos subcapas- para todas las capas físicas, a fin de conseguir importantes volúmenes de producción de chips con la consiguiente reducción en precios.

**Los diversos mecanismos de acceso que se han propuesto e implantado para WLANs caen en dos categorías:**

- Protocolos con arbitraje (FDMA, TDMA)

- y protocolos por contención -por detección de portadora- (CDMA/CD, CDMA/CA -usado por 802.11-), aunque también se han diseñado protocolos que son una combinación de estas dos categorías.

La multiplexación en frecuencia (FDM) divide todo el ancho de banda asignado en distintos canales individuales. Es un mecanismo simple que permite el acceso inmediato al canal, pero muy ineficiente para utilizarse en sistemas informáticos, los cuales presentan un comportamiento típico de transmisión de información por breves períodos de tiempo (ráfagas).
Una alternativa sería asignar todo el ancho de banda disponible a cada nodo en la red durante un breve intervalo de tiempo de manera cíclica. Este mecanismo, llamado multiplexación en el tiempo (TDM), requiere mecanismos muy precisos de sincronización entre los nodos participantes para evitar interferencias. Este esquema ha sido utilizado con cierto éxito sobre todo en las redes inalámbricas basadas en infraestructura, donde el punto de acceso puede realizar las funciones de coordinación entre los nodos remotos.
El protocolo de acceso múltiple por división de código (CDMA), es el mecanismo de acceso por excelencia para que puedan coexistir diferentes redes basadas en espectro disperso.
Las WLANs que emplean mecanismos de contención como acceso al medio, están basadas en el modelo de detección de "portadora" utilizado por la tecnología de red local más difundida en la actualidad, Ethernet / IEEE 802.3.
Varias de las primeras redes utilizaban exactamente el mismo algoritmo de acceso al medio, (CSMA/CD) detección de portadora con detección de colisiones: Cuando una estación desea transmitir, primero verifica que el medio de comunicación esté libre (es decir, detecta la portadora). Si éste está libre, transmite su información y si no, espera a que se libere el medio y transmite. Como existe la posibilidad de que dos estaciones transmitan información simultáneamente, este mecanismo exige que al transmitir se siga evaluando el canal, y si se detecta alguna perturbación en la transmisión (detección de colisión), se supone que ha ocurrido un conflicto, por lo que la transmisión se suspende y las estaciones involucradas en el conflicto esperan un tiempo aleatorio antes de repetir nuevamente el algoritmo.
El modelo de acceso por contención que más se utiliza en la actualidad, y que ha sido incorporado al standard 802.11 como 1ª subcapa MAC es el llamado de detección de portadora con evicción de colisión (CSMA/CA), introduce una variante en el algoritmo anterior: La mayor probabilidad de tener una colisión en CSMA/CD se da precisamente al terminar una transmisión pues puede haber más de una estación esperando que la transmisión termine, tras lo cual estas estaciones comenzarán a enviar información provocando una colisión en el medio. En CSMA/CA, cuando una estación identifica el fin de una transmisión, espera un tiempo aleatorio antes de transmitir, disminuyendo así la probabilidad de colisión.

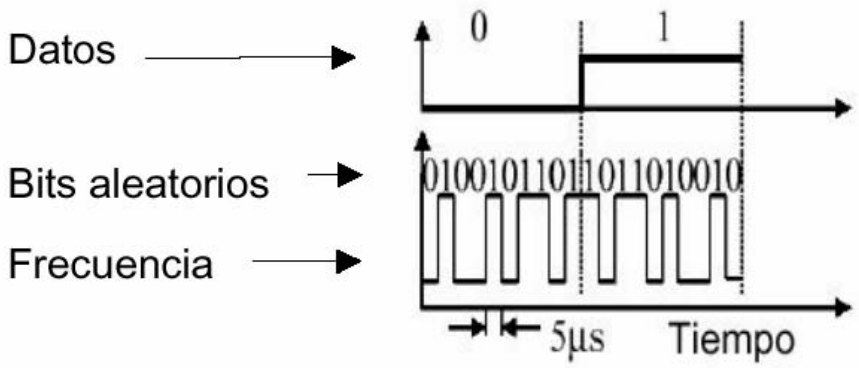
En comunicaciones inalámbricas, este modelo presenta todavía una deficiencia debida al problema conocido como de la terminal oculta (o nodo escondido): Un dispositivo inalámbrico puede transmitir con la potencia suficiente para que sea escuchado por un nodo receptor, pero no por otra estación que también desea transmitir y que por tanto no detecta la transmisión. Para resolver este problema, la norma 802.11 ha añadido al protocolo de acceso CSMA/CA un mecanismo de intercambio de mensajes con reconocimiento positivo, al que denomina Reservation-Based Protocol, que es la 2ª subcapa MAC.

Cuando una estación está lista para transmitir, primero envía una solicitud al punto de acceso (RTS) quien difunde el NAV (Network Allocation Vector) -un tiempo de retardo basado en el tamaño de la trama contenido en la trama RTS de solicitud- a todos los demás nodos para que queden informados de que se va a transmitir (y que por lo tanto no transmitan) y cuál va a ser la duración de la transmisión. Estos nodos dejarán de transmitir durante el tiempo indicado por el NAV más un intervalo extra de backoff (tiempo de retroceso) aleatorio. Si no encuentra problemas, responde con una autorización (CTS) que permite al solicitante enviar su trama (datos). Cuando el punto de acceso ha recibido correctamente la información, envía una trama de reconocimiento (ACK) notificando al transmisor.

**SEGURIDAD**

Para evitar la detección de señales por personas no deseadas en redes inalámbricas se pueden utilizar varios métodos:

1. **Espectro expandido con secuencia directa(DSSS: Direct Séquence Spread Spectrum).**
   Este método combina una cadena de dígitos con otra de bits pseudo- aleatorios mediante una XOR. Con esto conseguimos que la señal resultante tenga la misma frecuencia que la secuencia de bits.




Permite hasta 7 canales de 1 y 2Mbps.
Expandir la información de la señal sobre un ancho de banda mayor, para dificultar las interferencias.

2. **Espectro expandido con salto en frecuencias (FHSS: Frecuency Hopping Spread Spectrum).**

   Este método consiste en emitir la señal sobre una secuencia de radio frecuencias aparentemente aleatoria. En cada fracción de segundo se salta de frecuencia. El receptor capta el mensaje saltando de forma sincrona sobre la misma secuencia de frecuencias.

   Con esta técnica se transmite de forma segura, aunque depende el algoritmo de generación de números aleatorios y la semilla escogida. Este método prácticamente ya no se utiliza.

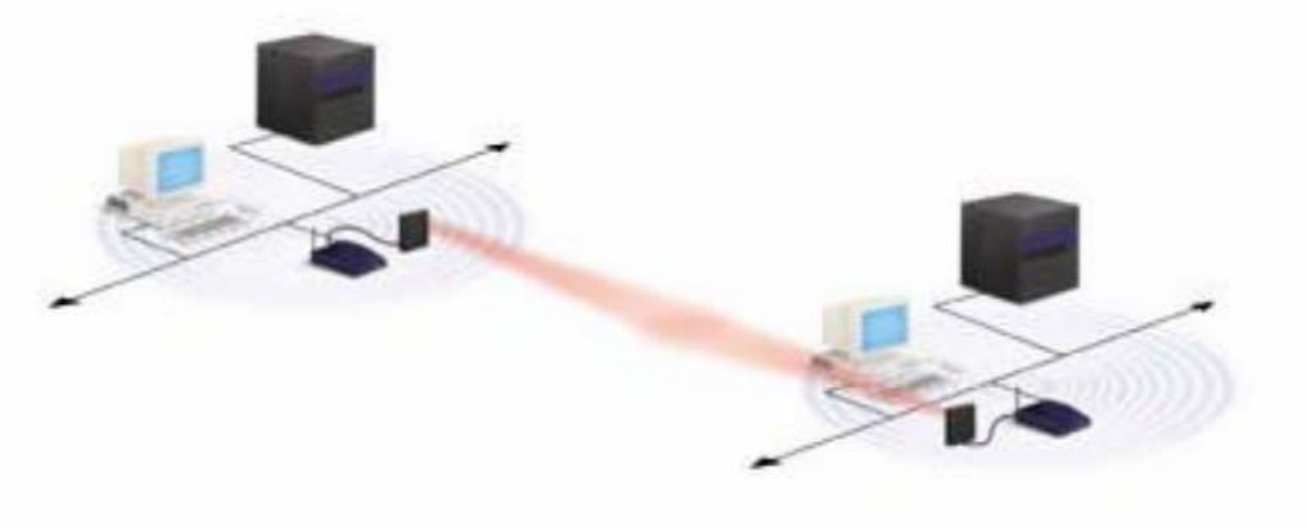
## TIPOS DE REDES INALÁMBRICAS

Existen dos amplias categorías de redes inalámbricas:

- **De Larga Distancia**

  Estas son utilizadas para transmitir la información en espacios que pueden variar desde una misma ciudad o hasta varios pases circunvecinos (mejor conocido como Redes de Area Metropolitana MAN o también Redes de Area Extensa WAN); sus velocidades de transmisión son relativamente bajas(por supuesto debido a la distancia), de 4.8 a 19.2 Kbps.

  Existen dos tipos de redes de larga distancia (las cuales no trataremos por pertenecer a otro tema): Redes de Conmutación de Paquetes (publicas y privadas) y Redes Telefónicas Celulares .



- **De Corta Distancia** Estas son utilizadas principalmente en redes corporativas (conocidas como Redes de Area Local RAL, pero integrando datos y voz) cuyas oficinas se encuentran en uno o varios edificios que no se encuentran muy separados entre s, con velocidades del orden de 280Kbps hasta los 2 Mbps.

**VENTAJAS E INCONVENIENTES**

Las principales ventajas de la utilización de redes inalámbricas son:

- Movilidad de los nodos de emisión y recepción de la señal.
- Proporcionan cierto grado de portabilidad.
- Evita el coste de instalación del cableado entre nodos.
- Ayudan a proporcionar backup a una red existente.
- Además, son especialmente utiles en edificios históricos o áreas aisladas, donde la instalación del cableado pueda ser especialmente difícil. También es muy útil para personas que estén en constante movimiento, como médicos y enfermeras en un hospital.
-

Las desventajas que podemos encontrar son:

- Alto precio en los componentes utilizados.
- La velocidad de transmisión es menor en comparación con las redes cableadas.
- La seguridad deja mucho que desear, ya que las conexiones en redes inalámbricas son fácilmente interceptables. Para evitar esto se utilizan varios métodos, como veremos a continuación.

Los inconvenientes que tienen las redes de este tipo se derivan fundamentalmente de encontrarnos en un periodo transitorio de introducción, donde faltan estándares, hay dudas que algunos sistemas pueden llegar a afectar a la salud de los usuarios, no está clara la obtención de licencias para las que utilizan el espectro radioeléctrico y son muy pocas las que presentan compatibilidad con los estándares de las redes fijas.

Lenta evolución

A pesar de su importancia, desde un punto de vista tecnológico y estratégico (el paso de la telefonía movil a la computación movil, las perspectivas de un multimedia movil o la banda ancha en el contexto movil), el mercado de WLAN ha evolucionado muy lentamente, sin obedecer a las expectativas generadas en los últimos años, que hablaban de importantes crecimientos de negocio. Esto se ha debido, entre otros motivos, a los propios problemas que siempre conlleva el nacimiento de una tecnología: los desequilibrios entre la oferta y la demanda y la debilidad del modelo de relaciones, asociado, los problemas de excelencia de la propia tecnología (las prestaciones de los productos o servicios), los precios, normalmente elevados, y la ausencia de normas.

## ESTANDARES

Hay que hacer notar que diseñar un protocolo de acceso para WLAN resulta mucho más complejo que hacerlo para redes locales basadas en cable. En el caso que nos ocupa, se deben considerar otros factores que influyen enormemente en el funcionamiento de estos sistema, tales como perturbaciones ambientales, interferencias y variaciones en la potencia de la señal, que introducen importantes variaciones en el tiempo de acceso y en la tasa de errores de transmisión. Igualmente, al contar con equipos móviles se pueden presentar conexiones y desconexiones repentinas en la red, como también deben tenerse en cuenta mecanismos de relevo entre puntos de acceso para atender a nodos móviles que pasan de un área a otra de cobertura.

## ESTÁNDAR IEEE 802.11

El 802.11 es el estándar proporcionado por IEEE para la utilización de redes inalámbricas, la norma no especifica tecnologías ni aplicaciones, sino simplemente las especificaciones para la capa física y la capa de control de acceso al medio (MAC). Utiliza un modelo de referencia multicapas, en el que las capas más bajas corresponden a las especificaciones de capa física y aspectos dependientes del medio particular utilizado. La siguiente capa corresponde al protocolo de acceso al medio y es común a todas las redes independientemente del medio fisco utilizado, presentando as una visión unificada a las capas superiores.

## BLUETOOTH

Bluetooth, tecnología inalámbrica de corto alcance, usa una radiofrecuencia de bajo poder para conectar una gama de dispositivos con objeto de compartir archivos y conectarse en situaciones específicas a distancias de hasta 10 metros (90 m con un amplificador).
Bluetooth, una norma abierta que tiene el respaldo de un consorcio cuyos 2.000 miembros incluyen a Ericsson, IBM, Intel, Motorola y Nokia, ha sido durante varios años la más anunciada tecnología "inminente" para posibilitar la conexión instantánea inalámbrica a una red. Pero aparte de un par de portátiles con puertos de Bluetooth, los productos han tardado en aparecer. Examinamos un par de tarjetas de redes para PC de Toshiba. Nuestra conclusión: Bluetooth trabaja, pero tiene sus defectos.
Los protocolos inalámbricos para redes como HomeRF y 802.11B se usan ampliamente para conectar las PCs de escritorio con las portátiles, pero Bluetooth ofrece algunos beneficios adicionales. Como su consumo de energía de la batería es mínimo, puede utilizarse en dispositivos pequeños. Por ejemplo, puede conectar un teléfono móvil a un PDA o a una portátil para que el teléfono pueda actuar como un módem inalámbrico.
Los auriculares con Bluetooth permiten hacer llamadas sin tener que usar las manos y sin las limitaciones de un receptor con alambres. En una portátil, Bluetooth permite el intercambio inalámbrico de archivos y el acceso a redes.
Bluetooth paga un precio en el desempeño por su ahorro de energía. Con una velocidad subyacente de sólo 1 Mbps, el rendimiento real de Bluetooth es de 725 Kbps. Que es suficientemente rápido para voz y datos, pero no para el vídeo de movimiento completo que la próxima revisión del 802.11 admite. La versión 802.11A tiene una velocidad de 54 Mbps pero no estará disponible antes de mediados del 2001. Se espera que el HomeRF, que actualmente tiene un límite de 2 Mbps, llegue a 10 Mbps casi al mismo tiempo.
Es improbable que Bluetooth suplante al 802.11B, pero sí debe tornar obsoletos los puertos infrarrojos, ya que elimina el requisito de mantener la línea visual que es típico de esa tecnología. Como funciona en la misma frecuencia de 2,4 GHz que el 802.11B, HomeRF y algunas microondas, puede encontrar interferencias en lugares donde se usen otras tecnologías inalámbricas.

## LA TECNOLOGÍA HOMERF

Con una finalidad muy similar, la tecnologia HomeRF, basada en el protocolo de acceso compartido (Shared Wireless Access Protocol - SWAP), encamina sus pasos hacia la colectividad sin cables dentro del hogar. Los principales valedores de estos sistemas, se agrupan en torno al Consorcio que lleva su mismo nombre HomeRF, teniendo Próxima (una filial de Intel) como el miembro que más empeño esta realizando en la implantación de dicho estándar. Además de la sombra de Intel, Compaq es otra de las firmas relevantes que apoya el desarrollo de producto HomeRF. El soporte a esta tecnología se materializa en que actualmente ambas significativas firmas poseen cada una de ellas un producto bajo esta novedosa configuración.
Al igual que Bluetooth SIG (Bluetooth Special Interest Group), el HomeRF Working Group (HRFWG) es un grupo de compañias encargadas de proporcionar y establecer un cierto orden en este océano tecnológico, obligando que los productos fabricados por las empresas integrantes de este grupo tengan una plena interoperatividad.

Por si toda esta competitividad no fuera suficiente, el Instituto de Estándares de Telecomunicaciones Europeo (ETSI) es otra de las reconocidas organizaciones de estandarización, culpable, entre otros, de haber desarrollado el estándar GSM para la telefonía celular digital. También son responsables de haber llevado a cabo durante los años 1991 y 1996 el proyecto HyperLAN, en el cual su objetivo primordial este conseguir una tasa de transferencia mayor que la ofrecida por la especificación IEEE 802.11. Según los estudios realizados, HyperLAN incluía cuatro estándares diferentes, de los cuales el denominado Tipo 1, es el que verdaderamente se ajusta a las necesidades futuras de las WLAN, estimándose una velocidad de transmisión de 23,5 Mbps, notablemente superior a los 1 2 Mbps de la normativa IEEE 802.11b. Actualmente, el ETSI dispone de la especificación HyperLAN2 , que mejora notablemente las características de sus antecesoras, ofreciendo una mayor velocidad de transmisión en la capa física de 54Mbps para lo cual emplea el método de modulación OFDM (Orthogonal Frequency Digital Multiplexing) y ofrece soporte QoS. Bajo esta especificación se ha formado un grupo de reconocidas firmas el HiperLAN2 Global Forum (H2GF), con la intención de sacar al mercado productos basados en ese competitivo estándar. Pero volviendo a la realidad más cercana, tanto las WLAN basadas en el protocolo 820.11b, como los dispositivos BlueTooth y HomeRF, competirán por la misma franja del espectro, los famosos 2,4 GHz, con lo cual, y a pesar de la utilización de diversas técnicas para la disminución de las posibles interferencias, como espectro disperso en sus variantes de salto de frecuencia (FHSS - Frecuency-Hopping Spread Spectrum) y secuencia directa (DSSS - Direct Sequence Spread Spectrum), o la limitación de la potencia de emisión, la paulatina profusión de dispositivos inalámbricos irá incrementando las interferencias entre unos y otros.
Además, hay otro abundante conjunto de aparatos y electrodomésticos que también hacen uso de esta banda de frecuencias, como pueden ser los microondas o los teléfonos móviles, entre los más notables, agravando todavía más si cabe el problema de las interferencias que, a la postre, se traduce en la funcionalidad o no de esta clase de conexión sin hilos.
No obstante, la realidad de los productos IEEE 802.11b y la prometedora e inminente llegada de los equipos BlueTooth, son dos importantes hitos que marcarán un antes y después en el sector de las redes inalámbricas. Asimismo, y viendo las deficiencias de la actual normativa IEEE 802.11, ya se está trabajando en una futura especificación que trabaja realmente a 10 Mbps en un rango de 20 MHz dentro de la franja de 8,2 GHz, pero este estudio está todavía en una fase muy temprana.

## WAP: un nuevo estándar para las comunicaciones inalámbricas

Protocolo abierto para aplicaciones interactivas e inalámbricas
WAP: opción de estandarizar los dispositivos inalámbricos
Servicios de Valor agregado en puerta

Las telecomunicaciones son el principal factor para determinar la globalización de un país. De manera que su infraestructura se convierte en el indicador del desarrollo tecnológico, económico y político de éste.
Algunas de las nuevas tecnologías que más se han visto desarrolladas son sin duda alguna, la telefonía celular e Internet.
Internet, hoy por hoy, es una de las herramientas principales para muchas empresas y hogares. Por su parte el correo electrónico cada día es más indispensable, hasta podría decirse que aquellas empresas que no cuentan con estos medios están en desventaja competitiva ante las que si lo tienen. En general Internet es uno de los medios más completos, y de fácil acceso al mundo de la información global.
Asimismo, la telefonía celular en los últimos cinco años ha creado no solo una nueva forma de comunicación, sino se ha convertido en una necesidad. Los servicios celulares se encuentran hasta en los lugares más alejados de la civilización, y al mismo tiempo los beneficios que éstos ofrecen son diversos y económicos.
Por ejemplo, actualmente en un solo teléfono celular digital se puede tener, además del servicio telefónico, el servicio de radiolocalización, envío de correo electrónico, y el servicio de roaming global, entre otros.
Algunas compañías de telecomunicaciones como Ericsson, Motorola, Nokia y Unwired Planet han definido un nuevo protocolo para la comunicación de datos inalámbricos. Este protocolo de aplicación inalámbrica (WAP) provee a los usuarios nuevos servicios en un amplio rango de aplicaciones, tales como acceso a la información de Internet, comercio electrónico y aplicaciones telefónicas. Al mismo tiempo está diseñado para economizar la utilización de los recursos disponibles de las redes de telecomunicaciones.

## ¿Qué es WAP?

WAP (Wireless Application Protocol; Protocolo de aplicaciones inalámbricas) es una especificación para un ambiente de aplicación y un conjunto de protocolos de comunicación para estandarizar la forma en que los dispositivos inalámbricos, tales como teléfonos portátiles y asistentes digitales personales (PDAs), se puedan utilizar para el acceso a Internet, incluyendo correo electrónico, World Wide Web (WWW), los newsgroup, y el Internet Relay Chat (IRC).
En el futuro, los dispositivos y los sistemas del servicio que utilizarán WAP podrán funcionar sin importar el fabricante, el estándar de la red, el operador o la tecnología que es utilizada, es decir, con WAP se supera el problema de la compatibilidad.
WAP hace posible una amplia gama de servicios inalámbricos que son independientes de la tecnología de red inalámbrica digital subyacente. De igual forma permite a los usuarios de los teléfonos móviles tener acceso a la información de hoteles y restaurantes, servicios bancarios, servicios de directorio, tarifas de cambio, horario del vuelos, trenes y camiones, entre otros.

**Propósito y objetivo de WAP**

El propósito de WAP es proveer un ambiente común que permita desarrollar servicios de valor agregado a la telefonía móvil. Mientras que su objetivo es brindar servicios avanzados de contenidos de Internet a teléfonos celulares digitales y otras terminales.

**Algunas aplicaciones de WAP**

**Acceso de información de Internet.** El WAP puede ser utilizado para accesar información en Internet. Sin embargo, los motores de búsqueda WAP no pueden ser utilizados de la misma forma que alguna "herramienta para navegar", por las limitaciones de entrada y salida que presenta un teléfono móvil como el tamaño de memoria.
**Comercio electrónico móvil.** Los usuarios pueden tener acceso a pagos de servicios de boletos de transportes, así como también a los sistemas de bolsa de valores, etcétera.
**Aplicaciones telefónicas.** Un usuario puede tener acceso a servicios de llamadas, en combinación con otros servicios que otorgan las operadoras de servicios inalámbricos. Un ejemplo típico sería un menú definido por el usuario, que es desplegado cada vez que entra una llamada. Este menú permite al usuario decidir a contestar o rechazar la llamada, o bien retransmitirla a otra extensión o al servicio de correo de voz.

Con WAP los usuarios pueden tener acceso a los siguientes servicios:
- Servicios de la banca
- - Noticias
- - Deportes
- - Clima
- - Balance de inventarios
- - Teleservicios
- - Juegos
- - Información geográfica, etcétera.

**Beneficios del operador**

- Los operadores de las redes pueden ofrecer categorías de servicios a los usuarios.
- Pueden crear nuevos y únicos servicios y proveer accesos a servicios disponibles en Internet.
- Los operadores pueden reducir costos de servicios al cliente y Help Desk proporcionando acceso a información residente en su red.

Asimismo con la introducción de WAP, los operadores pueden remotamente ser capaces de personalizar los menús y las interfases de los teléfonos de los clientes para posteriormente diferenciar sus servicios.
Se estima que el incremento de los usuarios de WAP será parecido al que se tiene pronosticado para Internet, debido a que el WAP está orientado hacia éste.
La siguiente figura nos muestra el incremento estimado de suscriptores de servicios inalámbricos en los siguientes años.
Como se puede observar WAP motiva a los operadores de redes, a alcanzar un mercado masivo. En el caso de México, gracias a la privatización de Telmex y con la nueva competencia de empresas internacionales en el ramo de las telecomunicaciones, es muy probable que este tipo de tecnologías se adopten en un futuro no muy lejano, ya que esto creará competencia en los servicios que ofrecen las compañías telefónicas.

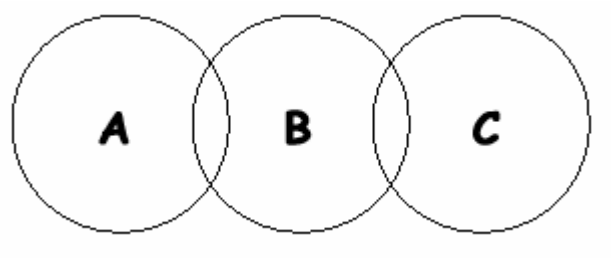
## COMPARACION DE ESTANDARES INALAMBRICOS

| | IEEE 802.11b | HomeRF | Bluetooth |
|---|---|---|---|
| Velocidad | 11 Mbps | 1,2,10 Mbps | 30-400Kbps |
| Uso | LAN de oficina o campus | Oficina casera, casa, patio | Red de área personal |
| Tipo de Terminales | Agregadas a notebook, PC de escritorio, dispositivos de bolsillo, compuerta de internet | Agregadas a notebook, PC de escritorio, modem, teléfono, dispositivo portátil, compuerta de internet | Integradas en notebook, teléfono celular, dispositivo de bolsillo, localizador, aparatos, automóvil |
| Configuración Típica | Múltiples clientes por punto de acceso. | Punto a punto o múltiples dispositivos por punto de acceso. | Punto a punto o múltiples dispositivos por punto de acceso. |
| Alcance | 50 a 300 pies | 150 pies | 30 pies |
| Uso compartido de frecuencia | Espectro de expansión de secuencia directa | Salto de frecuencia de banda ancha. | Salto de frecuencia de banda angosta |
| Compañías y grupos que lo respaldan | Cisco, Lucent, 3Com, WECA consorcio | Apple, compaq, Dell, Home RF working group, Intel, Motorola, Proxim | Bluetooth Special Interest Group, ericcson, Motorola, Nokia |
| Estado | En distribución | En desarrollo | En desarrollo |

**COLISIONES**

Al igual que en las redes cableadas, en las redes inalámbricas también se producen colisiones en el flujo normal de los datos (las primeras por cable y las segundas por medios inalámbricos).

- **Nodos ocultos :**




La estación C no escucha a la estación A entonces C puede empezar a transmitir mientras A está transmitiendo, en este caso A y C no pueden detectar la colisión y solamente el receptor puede detectar la colisión. La solución a estos problemas, al igual que en las redes cableadas, pasa por la utilización del protocolo CSMA/CA

- **Nodos expuestos:**

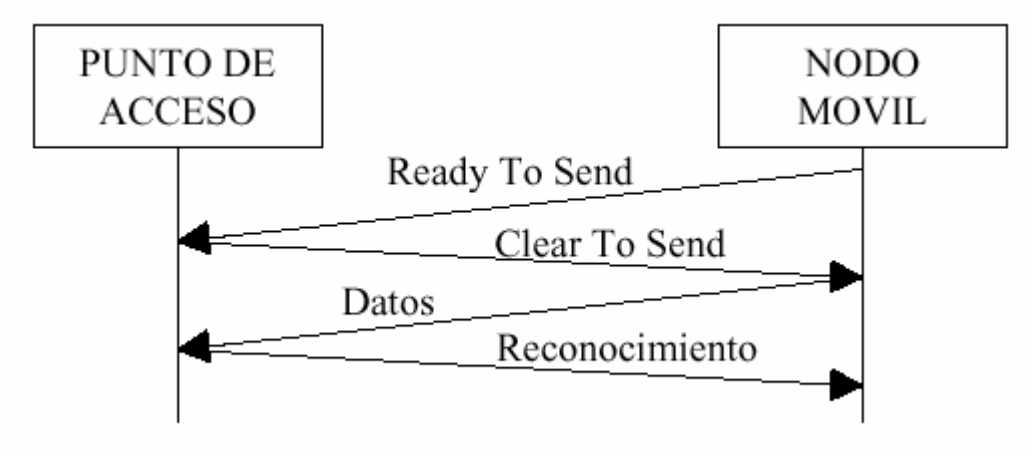
Si el Nodo B transmite a A y el nodo C quiere transmitir al D se tiene que esperar a que termine A (No muy deseable por la variabilidad del tiempo de espera que ello conlleva). En este caso la solución consiste en que los terminales expuestos escuchen el RTS (petición de envío) pero no el CTS (podemos enviar) y ante esta situación se les da permiso de enviar paquetes.

**EL PROTOCOLO CSMA/CA**

Este protocolo se encarga de evitar las colisiones durante las transmisiones inalámbricas en vez de descubrir una colisión debido a que es difícil descubrir colisiones en una red de transmisión RF.
El funcionamiento es el siguiente:

La estación fuente envía el mensaje Ready To Send (RTS), el cual contiene la estación destino y la duración del mensaje. Después de esto, las estaciones esperan a recibir un mensaje Clear To Send (CTS) o el temporizador.

En caso de recibir CTS, todas las estaciones esperarán la duración indicada.
En caso de que la estación destino esté lista para recibir, lo que hace es enviar un mensaje CTS.
Cada paquete enviado necesita ser reconocido, lo cual permite una recuperación eficiente ante las colisiones y también el envío continuo de paquetes multitrama.




**MAC**

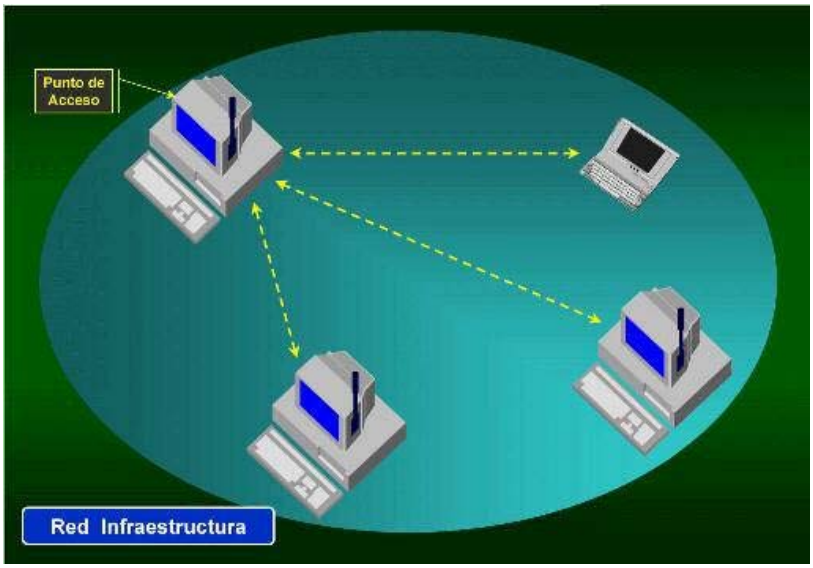
La capa de Mac del 802.11, se refiere sobre todo a las reglas para tener acceso al medio inalámbrico.
La capa de acceso al medio se divide en dos subcapas. En el nivel más bajo se define la llamada Función de Coordinación Distribuida (DCF), que proporciona una comunicación asnicrona entre estaciones que utilizan el protocolo CSMA/CA. Los servicios de transferencia de datos sin restricciones de tiempo, utilizan directamente este protocolo para intercambiar información.
Para aquellas aplicaciones con restricciones de tiempo, como conversaciones de voz o control de procesos, se propone el uso opcional de la Función de Coordinación en el Punto (PCF), que se utiliza para otorgar prioridades en el acceso al canal.

Reconocimiento

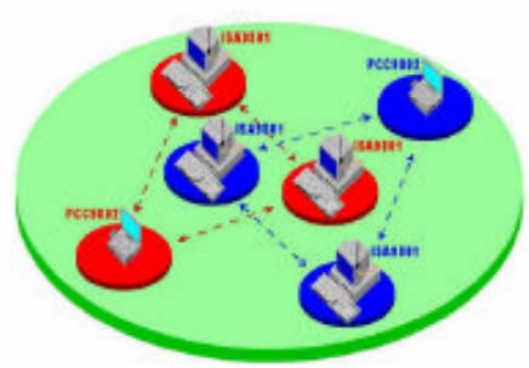
También, se define el concepto de superara, un periodo de tiempo en el que durante cierto intervalo la estación puede transmitir información critica con restricciones de tiempo en base a las reglas de PCF, y tras el cual queda un intervalo donde participa DCF para acceder al canal por contención.

Se definen dos arquitecturas de red: la red de infraestructura (cliente /servidor) y la ad hoc.

. Las redes **cliente / servidor** utilizan un punto de acceso (estaciones base) que controla la asignación del tiempo de transmisión para todas la estaciones y permite que estaciones móviles deambulen por la columna vertebral de la red cliente / servidor. El punto de acceso se usa para manejar el tráfico desde la radio movil hasta las redes C / S cableadas o inalámbricas. Esta configuración permite coordinación puntual de todas las estaciones en el área de servicios base y asegura un manejo apropiado del tráfico de datos.
El punto de acceso dirige datos entre las estaciones y otras estaciones inalámbricas y/o el servidor de la red. Típicamente las WLAN controladas por un punto de acceso central proporcionará un rendimiento mucho mayor.
Utilizan el Protocolo de acceso centralizado que es especialmente útil cuando se quieren transmitir datos sensibles al tiempo y prioritarios también.

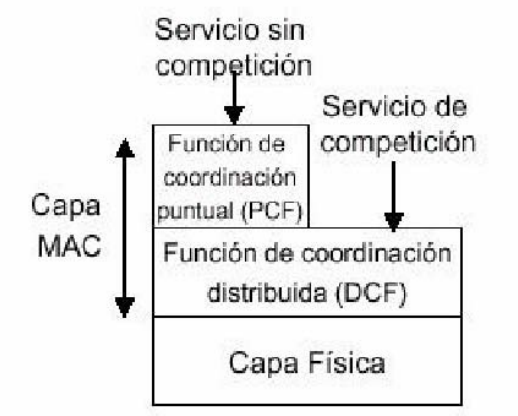



Una red **Ad-hoc** es una red simple donde se establecen comunicaciones entre las múltiples estaciones en un área dada sin el uso de un punto de acceso o servidor. La norma especifica la etiqueta que cada estación debe observar para que todas ellas tengan un acceso justo a los medios de comunicación inalámbricos por eso el protocolo empleado es el protocolo de acceso distribuido el cual posee mecanismos de detección de portadora tales como CSMA. Proporciona métodos de petición de arbitraje para utilizar el medio para asegurarse de que el rendimiento se maximiza para todos los usuarios del conjunto de servicios base.



RED AD-HOC

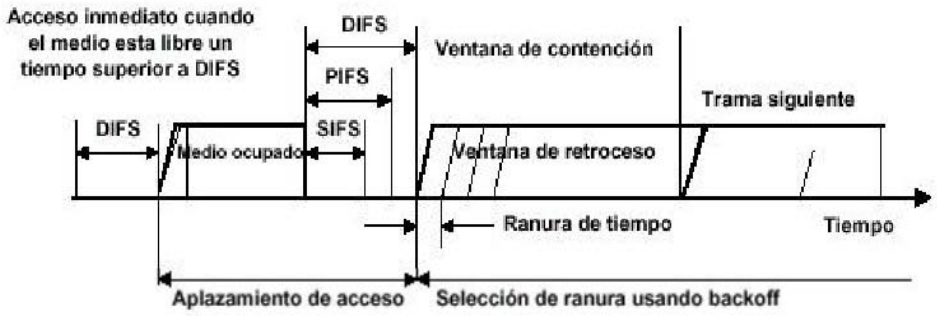
El MAC, del 802.11 proporciona un mecanismo (en consonancia con los protocolos comentados anteriormente) de acceso distribuido con un control centralizado implementado sobre el anterior.



Para el acceso se tienen dos tipos de funciones de coordinación

- **Función de coordinación distribuida (DCF)**
  - **Reglas de acceso CSMA**

    Utiliza un servicio de competición. Si una estación desea transmitir, escucha el medio. Si éste se encuentra libre, espera un tiempo igual a IFS, para ver si el medio continúa libre, y si es as la estación transmite.
    En caso que el canal se encuentre ocupado, ya sea inicialmente o tras esperar el IFS se actúa de la siguiente forma:




1. Se sigue escuchando el canal hasta que finalice la transmisión en curso.
2. Se espera IFS.
3. Si el canal está libre, se espera según el algoritmo de backoff especificado en el estándar IEEE 802.3
4. Si el canal está libre se transmite.

- **Esquema de prioridades. Tres valores de IFS**

  - SIFS ⇒ Es el IFS más corto, utilizado por todas las acciones de respuesta inmediata. Además es el más prioritario.
  - PIFS ⇒ Es empleado por el controlador centralizado cuando realiza sondeos.
  - DIPS ⇒ Es el IFS mayor, utilizado como retardo mínimo para tramas asincronas que compiten por el medio.

- **Función de coordinación puntual (PCF)**

  - Utiliza un servicio sin competición.

## MEDIOS DE TRANSMISION

En medios no guiados, tanto la transmisión como la recepción se lleva a cabo mediante antenas. En la transmisión, la antena radia energía electromagnética en el medio (normalmente el aire), y en la recepción la antena capta las ondas electromagnéticas del medio que las rodea. Básicamente hay dos tipos de
configuraciones para las transmisiones inalámbricas: direccional y omnidireccional. En la primera la antena de transmisión emite la energía electromagnética concentrándola en un haz; por tanto en este caso las antenas de emisión y recepción deben estar perfectamente alineadas. En el caso omnidireccional, por el contrario, el diagrama de radiación de la antena es disperso, emitiendo en todas direcciones, pudiendo la señal ser recibida por varias antenas. En general, cuanto mayor es la frecuencia de la señal transmitida es más factible confinar la energía en un haz direccional.

### Microondas

Suelen utilizarse antenas parabólicas para la transmisión . En conexiones a larga distancia , se utilizan conexiones intermedias punto a punto entre antenas parabólicas. Los enlaces de microondas se utilizan mucho como enlaces allí donde los cables coaxiales o de fibra óptica no son prácticos. Se necesita una linea de visión para transmitir en la banda de SHF, de modo que es necesario disponer de antenas de microondas en torres elevadas en las cimas de las colinas o accidentes del terreno para asegurar un camino directo con la intervención de pocos repetidores.
Las bandas de frecuencias más comunes para comunicaciones mediante microondas hasta 6 GHz. Además, con microondas se puede alcanzar un ancho de banda de hasta 15Mbps.
Los enlaces de microondas presentan unas tasas de error en el rango de 1 en 10 5 a 1 en 10 11 dependiendo de la relación señal/ruido en los receptores. La principal causa de pérdidas es la atenuación, debido a que las pérdidas aumentan con el cuadrado de la distancia ( con cable coaxial y par trenzado son logarítmicas ). También pueden presentarse problemas de propagación en los enlaces de microondas, incluyendo los debidos a lluvias intensas que provocan atenuaciones que incrementan la tasa de errores. Pueden producirse pequeños cortes en la señal recibida cuando una bandada de pájaros atraviesa el haz de microondas, pero es poco frecuente que ocurra.

### Infrarrojos.

Permite la transmisión de información a velocidades muy altas : 100 Mbits/seg.

Consiste en la emisión/recepción de un haz de luz ; debido a esto, el emisor y receptor deben tener contacto visual (la luz viaja en linea recta). Por esta limitación pueden usarse espejos para modificar la dirección de la luz transmitida.

En infrarrojos no existen problemas de seguridad ni de interferencias ya que estos rayos no pueden atravesar los objetos ( paredes por ejemplo ) .

Tampoco es necesario permiso para su utilización ( en microondas y ondas de radio si es necesario un permiso para asignar una frecuencia de uso ) .

Hay 3 tipos de redes de infrarrojos:

- Redes en linea de vista. (Line-of-sight) Como implica su nombre, esta versión transmite solo si el transmisor y el receptor se ven limpiamente.

- Redes por dispersión de infrarrojos. (Scatter) Esta tecnología emite transmisiones para que reboten en las paredes y techos y eventualmente contacten con el receptor. Tiene un área efectiva de unos 100 pies y tiene una señal lenta para el rebote.

- Redes por reflexión. (Reflective) En esta versión de redes por infrarrojos, los tranceptores ópticos situados cerca de los ordenadores transmiten hacia un punto común que redirige las transmisiones al ordenador apropiado. Mientras la velocidad de los infrarrojos y su conveniencia están generando interés, el infrarrojo tiene dificultad transmitiendo a distancias más largas de 200 metros. Está sujeto también a interferencias por la fuerte luz ambiental que se encuentra en muchos entornos de trabajo.

**Enlaces opticos.**

El principio de funcionamiento de un enlace óptico al aire libre es similar al de un enlace de fibra óptica, sin embargo el medio de transmisión no es un polímero o fibra de vidrio sino el aire.

El emisor óptico produce un haz estrecho que se detecta en un sensor que puede estar situado a varios kilómetros en la linea de visión. Las aplicaciones típicas para estos enlaces se encuentran en los campus de la universidades, donde las carreteras no permiten tender cables, o entre los edificios de una compañia en una ciudad en la que resulte caro utilizar los cables telefónicos.

Las comunicaciones ópticas al aire libre son una alternativa de gran ancho de banda a los enlaces de fibra óptica o a los cables eléctricos. Las prestaciones de este tipo de enlace pueden verse empobrecidas por la lluvia fuerte o niebla intensa, pero son inmunes a las interferencias eléctricas y no necesitan permiso de las autoridades responsables de las telecomunicaciones.

Las mejoras en los emisores y detectores ópticos han incrementado el rango y el ancho de banda de los enlaces ópticos al aire libre, al tiempo que reducen los costos. Se puede permitir voz o datos sobre estos enlaces a velocidades de hasta 45 Mbits/s.

El limite para comunicaciones fiables se encuentra sobre los dos kilómetros. Para distancias de más de dos kilómetros son preferibles los enlaces de microondas.

Existen dos efectos atmosféricos importantes a tener en cuenta con los enlaces ópticos al aire libre:

- La dispersión de la luz que atenúa la señal óptica en proporción al número y al tamaño de las partículas en suspensión en la atmósfera. Las partículas pequeñas, como la niebla, polvo o humo, tienen un efecto que es función de su densidad y de la relación existente entre su tamaño y de la longitud de onda de la radiación infrarroja utilizada. La niebla, con una elevada densidad de partículas, de 1 a 10µm de diámetro, tienen un efecto más acusado sobre el haz de luz. Las partículas de humo, más grandes, tienen menor densidad y, por tanto, menor efecto.

- Las brisas ascensionales (originadas por movimientos del aire como consecuencia de las variaciones en la temperatura) provocan variaciones en la densidad del aire y, por tanto, variaciones en el índice de refracción a lo largo del haz. Esto da lugar a la dispersión de parte de la luz a lo largo del haz. Este efecto puede reducirse elevando el haz de luz lo bastante con respecto a cualquier superficie caliente o utilizando emisores múltiples. La luz de cada emisor se ve afectada de diferente forma por las brisas, y los haces se promedian en el receptor.

Estos sistemas suelen emplearse para transmisiones digital de alta velocidad en banda base. En Estados Unidos, todos los fabricantes de productos láser deben poseer obligatoriamente una certificación que garantice la seguridad de todos sus productos.

Tecnología de Infrarrojos.

La verdad es que IEEE 802.11 no ha desarrollado todavía en profundidad esta área y solo menciona las características principales de la misma, a saber:

- Transmisión infrarroja difusa,
- El receptor y el transmisor no tienen que ser dirigidos uno contra el otro y no necesitan una línea de vista (line-of-sight) limpia.
- Rango de unos 10 metros.
- Solo en edificios.
- 1 y 2 Mbps de transmisión, 16-PPM y 4-PPM.
- 850 a 950 nanometros de rango. (Frente al 850 a 900 nm que establece el IrDA).
- También indica que el IrDA ha estado desarrollando standards para conexiones basadas en infrarrojo.

Por todo ello tomare como referencia de esta capa y de las siguientes -que expondré en este mismo punto- en esta tecnología las especificaciones del IrDA.
Las WLAN por infrarrojos son aquellas que usan el rango infrarrojo del espectro electromagnético para transmitir información mediante ondas por el espacio libre.

***Clasificación.***

De acuerdo al ángulo de apertura con que se emite la información en el transmisor, los sistemas infrarrojo pueden clasificarse en sistemas de corta apertura, también llamados de rayo dirigido o de línea de vista ( line of sight,LOS) y en sistemas de gran apertura, reflejados o difusos ( diffused) - recogidos por la norma 802.11.

- Los sistemas infrarrojo de corta apertura, están constituidos por un cono de haz infrarrojo altamente direccional y funcionan de manera similar a los controles remotos de los televisores y otros equipos de consumo: el emisor debe orientarse hacia el receptor antes de transferir información, lo que limita un tanto su funcionalidad. Por ejemplo, resulta muy complicado utilizar esta tecnología en dispositivos móviles, pues el emisor debe reorientarse constantemente. Resumiendo, este mecanismo solo es operativo en enlaces punto a punto exclusivamente. Por ello se considera que es un sistema inalámbrico pero no móvil, o sea que esta mas orientado a la portabilidad que a la movilidad.

- Los sistemas de gran apertura permiten la información en ángulo mucho más amplio por lo que el transmisor no tiene que estar alineado con el receptor. Una topología muy común para redes locales inalámbricas basadas en esta tecnología, consiste en colocar en el techo de la oficina un nodo central llamado punto de acceso, hacia el cual dirigen los dispositivos inalámbricos su información, y desde el cual ésta es difundida hacia esos mismos dispositivos.

Desgraciadamente la dispersión utilizada en este tipo de red hace que la señal transmitida rebote en techos y paredes, introduciendo un efecto de interferencia en el receptor, que limita la velocidad de transmisión (la trayectoria reflejada llega con un retraso al receptor). Esta es una de las dificultades que han retrasado el desarrollo de el sistema infrarrojo en la norma 802.11.

La tecnología infrarrojo cuenta con muchas características sumamente atractivas para utilizarse en WLANs: el infrarrojo ofrece una amplio ancho de banda que transmite señales a velocidades muy altas (alcanza los 10 Mbps); tiene una longitud de onda cercana a la de la luz y se comporta como ésta (no puede atravesar objetos sólidos como paredes, por lo que es inherentemente seguro contra receptores no deseados); debido a su alta frecuencia, presenta una fuerte resistencia a las interferencias electromagnéticas artificiales radiadas por dispositivos hechos por el hombre (motores, luces ambientales, etc.); la transmisión infrarrojo con láser o con diodos no requiere autorización especial en ningún país (excepto por los organismos de salud que limitan la potencia de la señal transmitida); utiliza un protocolo simple y componentes sumamente económicos y de bajo consumo de potencia, una característica importante en dispositivos móviles portátiles (laptops, pdas).

Entre las limitaciones principales que se encuentran en esta tecnología se pueden señalar las siguientes: es sumamente sensible a objetos móviles que interfieren y perturban la comunicación entre emisor y receptor; las restricciones en la potencia de transmisión limitan la cobertura de estas redes a unas cuantas decenas de metros; la luz solar directa, las lámparas incandescentes y otras fuentes de luz brillante pueden interferir seriamente la señal.


Conexiones posibles actualmente usando tecnologia de infrarrojos.

Las velocidades de transmisión de datos no son suficientemente elevadas y solo se han conseguido en enlaces punto a punto. Por ello, lejos de poder competir globalmente con las LAN de microondas, su uso está indicado más bien como apoyo y complemento a las LAN ya instaladas, cableadas o por radio (microondas), cuando en la aplicación sea suficiente un enlace de corta longitud punto a punto que, mediante la tecnología de infrarrojos, se consigue con mucho menor coste y potencia que con las tecnologías convencionales de microondas.

**Capas y protocolos**.

El principio de funcionamiento en la capa física es muy simple y proviene del ámbito de las comunicaciones ópticas por cable: un LED (Light Emitting Diode), que constituye el dispositivo emisor, emite luz que se propaga en el espacio libre en lugar de hacerlo en una fibra óptica, como ocurre en una red cableada. En el otro extremo, el receptor, un fotodiodo PIN recibe los pulsos de luz y los convierte en señales eléctricas que, tras su manipulación (amplificación, conversión a formato bit -mediante un comparador- y retemporización) pasan a la UART (Universal Asynchronous Receiver Transmitter) del ordenador, de forma que para la CPU todo el proceso luminoso es absolutamente transparente. En el proceso de transmisión los bits viajan mediante haces de pulsos, donde el cero lógico se representa por existencia de luz y el uno lógico por su ausencia. Debido a que el enlace es punto a punto, el cono de apertura visual es de 30 y la transmisión es half duplex, esto es, cada extremo del enlace emite por separado.

- Tras la capa física se encuentra la capa de enlace, conocida como IrLAP, (Infrared Link Access Protocol) que se encarga de gestionar las tareas relacionadas con el establecimiento, mantenimiento y finalización del enlace entre los dos dispositivos que se comunican. IrLAP constituye una variante del protocolo de transmisiones asincronas HDLC (Half Duplex Line Control) adaptada para resolver los problemas que plantea el entorno radio. El enlace establece dos tipos de estaciones participantes, una actúa como maestro y otra como esclavo. El enlace puede ser punto a punto o punto a multipunto, pero en cualquier caso la responsabilidad del enlace recae en el maestro, todas las transmisiones van a o desde ella.

- La capa de red esta definida por el protocolo IrLMP (Infrared Link Management Protocol), la capa inmediatamente superior a IrLAP, se encarga del seguimiento de los servicios (como impresión, fax y módem), así como de los recursos disponibles por otros equipos, es decir, disponibles para el enlace.

- Finalmente, la capa de transporte, IrTP (Infrared Transport Protocol) se ocupa de permitir que un dispositivo pueda establecer múltiples haces de datos en un solo enlace, cada uno con su propio flujo de control. Se trata, pues, de multiplexar el flujo de datos, lo cual permite, por ejemplo, el spool de un documento a la impresora mientras se carga el correo electrónico del servidor. Este software, de carácter opcional -dado que no es necesario para la transferencia básica de ficheros- resulta útil cuando se ha de establecer un enlace, por ejemplo, entre un PDA (Personal Digital Assistant) y la LAN.

Definiciones.

*HiperLAN*. Es un sistema de radiocomunicacion de corto alcance al margen de IEEE 802.11, pero que utiliza esta norma como borrador y la tecnología spread spectrum en el rango de frecuencias de los 2.4Ghz. Sus orígenes se remontan a 1991, año en que empezó el proceso de especificación pero sin el bagaje de productos ya existentes del que disponía desde un principio IEEE 802.11.. Se encuentra actualmente en el Proyecto BRAN -Broadband Radio Access Networks-, el cual esta en desarrollo en el seno de ETSI, que no facilita el acceso a su documentación, salvo a los miembros. Entre los objetivos del proyecto están los siguientes : producir especificaciones para accesos por radio de alta calidad a redes fijas, también para accesos de negocios, residenciales, o públicos. Para ello se pretende implementar ATM, lo que permitirá un ancho de banda de 20Mbps, y soporte para multimedia.

*IrDA*. Organización internacional no lucrativa que tiene como objetivo la creación y promoción de standards de interconexión mediante infrarrojos interoperativos, de bajo costo y que soporten modelos punto a punto de corto alcance. Constituida en 1993 y con sede en Walnut Creek (California), IrDA representa el punto de referencia en comunicaciones ópticas por infrarrojos inalámbricas.

En la actualidad cuenta con más de 160 miembros que pertenecen a la industria de comunicaciones, componentes, ordenadores y periféricos, cable y telefonía, software, hardware y proveedores de servicios.

De sus actividades cabe destacar la especificación en septiembre de 1993 de las bases para las normas de enlace de datos SIR (Serial InfraRed) y el establecimiento, en junio de 1994, de los protocolos SIR (Serial infrared Link), IrLAP (protocol stack Link Access Protocol), y IrLMP (InfraRed
Link Management Protocol).

Más tarde, en octubre de 1995, lanza una serie de extensiones de la norma SIR incluyendo los 4 Mbps. Un mes después, Microsoft anuncia su apoyo a IrDA respecto a las conexiones a Windows 95 mediante un sistema de conexión infrarrojo inalámbrico entre PC basados en su sistema operativo y los periféricos.

Posteriormente, en octubre de 1996 se establece la iniciativa bidireccional para cámaras de vídeo, y en abril de 1997 se anuncia la propuesta de unas especificaciones de telecomunicaciones basadas en infrarrojos para soluciones en la transmisión de información.

En julio de 1997, se establece una iniciativa de estandarización para infrarrojo bidireccional. En octubre de ese mismo año surgen las especificaciones del estandard para el intercambio de imágenes capturadas mediante dispositivos/cámaras (IrTran-P o Infrared Picture Transfer). En ese mismo mes surge otra iniciativa para establecer un estandard para la conectividad inalámbrica por infrarrojos entre ordenadores de mesa y dispositivos periféricos como cámaras, teléfonos celulares y pcs portátiles. En noviembre establece un nuevo estandard para interoperatibilidad entre dispositivos de comunicación movibles.

Finalmente, en febrero de este año publica IrDa Control, un nuevo estandard para dispositivos inalámbricos de entrada (por ejemplo, ratones, teclados, joysticks, ...).

El trabajo actual se centra en introducción de puertos infrarrojos para sustituir los cables serie/paralelo punto a punto que conectan los ordenadores a los periféricos, para continuar próximamente con desarrollos en el área de los protocolos multipunto que se utilizan en los sistemas LAN.

## SEÑALES DE RADIO

Existen dos técnicas de transmisión de radio, dependiendo del espectro utilizado:

- Espectro sencillo de radio

  Es similar a transmitir desde una emisora de radio. El usuario sintoniza el emisor y el transmisor a una cierta frecuencia. Esto no requiere una linea de visión porque el rango de difusión es 5000. Sin embargo, debido a que la señal es de alta frecuencia, no puede traspasar acero o paredes gruesas. Además es relativamente lento, en un rango de 4,8 Mbps. Los clientes se suscriben a este método desde un servicio proporcionado por Motorola.

- Radio de amplio espectro.

  La radio de amplio espectro emite señales en un rango de frecuencias. Esto ayuda a evitar los problemas de comunicación de espectro sencillo. Las frecuencias disponibles están divididas en canales. Los adaptadores de amplio espectro sintonizan en un canal especifico por una determinada longitud de tiempo y entonces cambian a un canal diferente.

  Una secuencia de saltos determina el timing, y los ordenadores en la red están todos sincronizados al salto de tiempo. Para evitar que usuarios no autorizados escuchen la transmisión, el emisor y el transmisor utilizan un código.

  La típica velocidad de 250Kbps hace este método mucho más lento que los otros. Sin embargo, algunas implementaciones pueden ofrecer velocidades de hasta 2 Mbps sobre distancias de 2 millas al exterior y 400 pies en interior.

  Esta es un área donde la tecnología actualmente proporciona una verdadera red sin hilos. Por ejemplo, 2 más ordenadores equipados con tarjetas Xircom Credit Card Netware y un sistema operativo como Windows 95 o Windows NT pueden actuar como una red peer-to-peer sin cables que los conecten. Sin embargo, si tienes una red existente basada en servidor NT puede enlazar la red de más arriba en ésta añadiendo un punto de acceso (Netware Access Point) a uno de los ordenadores en la red de NT.

Tecnología de radiofrecuencia.

Las redes inalámbricas que utilizan radio frecuencia pueden clasificarse atendiendo a su capa física, en sistemas de banda estrecha ( narrow band) o de frecuencia dedicada -no recogido por IEEE 802.11-, y en sistemas basados en espectro disperso o extendido (spread spectrum) -elegido por IEEE 802.11-

Frecuencia dedicada

Esta técnica trabaja de modo similar a la forma en que se difunden las ondas desde una estación de radio. Hay que sintonizar en una frecuencia muy precisa tanto el emisor como el receptor. La señal puede atravesar paredes y se expande sobre un área muy amplia, así que no se hace necesario enfocarla. Sin embargo, estas transmisiones tienen problemas debido a las reflexiones que experimentan las ondas de radio (fantasmas); para evitarlas en lo posible, estas transmisiones están reguladas (en EUA) por la FCC. Hay que sintonizar muy precisamente para prevenir las posibles interferencias.

En octubre de 1990, Motorola introdujo un concepto de WLAN al que llamó WIN, Wireless In-building Network. Es la primera de únicamente dos WLANs que operan en una frecuencia dedicada y que requieren de autorización de las autoridades gubernamentales para operar (la otra es el sistema MR-23VX-LAN de Microwave Radio). El sistema de Motorola, llamado Altair, opera en la banda de 18 GHz del espectro radioeléctrico y -para los Estados Unidos- le han sido asignados 5 canales con dos bandas de frecuencia de 10 MHz cada uno, con lo que Altair puede transmitir información a velocidades de hasta 10 Mbps, aunque su media son los 5 Mbps.

Desde sus orígenes, Altair fue diseñado para coexistir y complementar la infraestructura de red basada en cable que muy probablemente ya se tiene en las organizaciones donde se piensa utilizar. La configuración de red está basada en áreas de 450 a 5,000 m2 llamadas micro celdas y coordinadas por un módulo de control (CM). Los dispositivos inalámbricos en el área de la micro celda, llamados Módulo de Usuario (UM), no se comunican directamente entre sí, sino a través del CM. Cada UM puede además estar conectado a un segmento de red local no inalámbrica y controlar hasta 6 dispositivos. Además, diferentes micro celdas pueden interconectarse a través de sus CMs para así aumentar la cobertura total de la red inalámbrica.

Spread spectrum o espectro expandido.

Los productos comerciales que utilizan infrarrojo o frecuencias dedicadas, aportan únicamente un tercio del mercado de WLANs. Las otras dos terceras partes transmiten información en bandas del espectro que no requieren autorización para su uso. Estas son las llamadas bandas para aplicaciones industriales, científicas y médicas (ICM o IMS).

En mayo de 1985, y tras cuatro años de estudios, el FCC (Federal Communications Comission), la agencia Federal del Gobierno de Estados Unidos encargada de regular y administrar en materia de telecomunicaciones, asignó las bandas IMS (Industrial, Scientific and Medical) 902-928 MHz, 2,400-2,4835 GHz, 5,725-5,850 GHz a las redes inalámbricas basadas en spread spectrum. Entre ellas, el IEEE 802.11 incluyo en su especificacion las frecuencias en torno a 2,4 GHz que se habían convertido ya en el punto de referencia a nivel mundial, la industria se había volcado en ella y está disponible a nivel mundial (debido a que distintas agencias reguladoras del mundo la asignaron para el uso de spread spectrum).

La banda IMS es "unlicensed", es decir, se asigna sin licencia en el sentido de que FCC simplemente asigna la banda y establece las directrices de utilización, pero no decide sobre quién debe transmitir en esa banda usando determinadas zonas de frecuencia. De hecho algunas de estas frecuencias están siendo extensamente utilizadas por otros dispositivos como teléfonos inalámbricos, puertas de garaje automáticas, sensores remotos, etc...

Es por esto por lo que las autoridades reguladoras exigen que los productos se desarrollen dentro de algún esquema que permita controlar las interferencias.

- Existe para esto una alternativa teórica que consiste en utilizar una potencia de salida muy baja, pero no resulta una alternativa práctica debido a que afecta a otros factores como, por ejemplo, la velocidad,que es crucial en este tipo de aplicaciones.
- Las técnicas tradicionales de modulación maximizan la potencia en el centro de la frecuencia asignada para solventar el problema del ruido, pero resulta fácil su detección e interceptación. Además existen limitaciones establecidas.

- Otras alternativas que han sido globalmente aceptadas por la industria y adoptadas por IEEE 802.11 se refieren a los esquemas DSSS (Direct Sequence Spread Spectrum) y FHSS (Frecuency Hopping Spread Spectrum), ambos dentro de la órbita de la tecnología conocida como "spread spectrum" o "espectro expandido". Esta tecnología se ha impuesto frente a las tecnologías tradicionales, por su excelencia y por sus mejoras en cuanto a complejidad y costes.

El spread spectrum, que podría traducirse como espectro expandido, es una técnica que ha sido generada y ampliamente utilizada en el sector de la defensa por sus excelentes propiedades en cuanto a inmunidad a interferencias y a sus posibilidades de encriptación. Hace sólo unos diez años que se produjo el spin-off (la extensión de programas gubernamentales, orientados a una misión específica, sobre todo de defensa, al sector civil) hacia el sector civil comercial en lo que respecta a los esquemas de modulación DSSS y FHSS. Los otros dos esquemas de spread spectrum siguen utilizándose en el sector de defensa, en particular en aspectos de radar y aplicaciones especiales.

**Definición:**

**Modulación - Proceso por el que se transforma una señal digital en una señal analógica que pueda ser enviada a través del canal hasta el receptor, que realizara el proceso inverso.**

Para ello se añade la información de la señal digital (en forma de función temporal) a alguno de los parámetros de la portadora (señal ideal, pura -sin información-, y de alta frecuencia)

A grandes rasgos, spread spectrum consiste en un esquema de modulación que consiste en lo siguiente: como su nombre indica, la señal se expande (su espectro) a través de un ancho de banda mayor que el mínimo requerido para transmitir con éxito. Mediante un sistema de codificación se desplaza la frecuencia o la fase de la señal de forma que ésta quede expandida, con lo cual se consigue un efecto de camuflaje.

Posteriormente, en el receptor la señal se recompone para obtener la información inicial que se deseaba transmitir. En definitiva, se esparce la señal a lo largo de un amplio margen del espectro evitando concentrar la potencia sobre una única y estrecha banda de frecuencia como ocurre con las técnicas convencionales de este modo puede usar un rango de frecuencias que este ocupado ya por otras señales.

Todos los elementos de cada red local inalámbrica basadas en espectro expandido utilizan el mismo código de expansión, lo cual permite la diferenciación y que esa red coexista con otras redes o con otros sistemas en la misma banda de frecuencias.

Los modos de implementación de DSSS y FHSS son sensiblemente diferentes a pesar de que comparten la misma filosofía.

A. La técnica de espectro expandido por secuencia directa (DSSS), se basa en desplazar la fase de una portadora mediante una secuencia de bits muy rápida, diseñada de forma que aparezcan aproximadamente el mismo número de ceros que de unos. Esta secuencia –un código Barker también llamado código de dispersión o PseudoNoise- se introduce sustituyendo a cada bit de datos; puede ser de dos tipos, según sustituya al cero o al uno lógico.

B. Tan solo aquellos receptores a los que el emisor envíe dicho código podrán recomponer la señal original -filtrando señales indeseables-, previa sincronización. Aquellos que no posean el código creerán que se trata de ruido. Por otro lado al sustituir cada cada bit de datos a transmitir, por una secuencia de 11 bits equivalente, aunque parte de la señal de trasmisión se vea afectada por interferencias, el receptor aún puede reconstruir fácilmente la información a partir de la señal recibida.

C. A cada bit de código en PN se le denomina chip. Una mayor cantidad de chips indica una mayor resistencia a la interferencia. El IEEE 802.11 establece una secuencia de 11 chips, siendo 100 el optimo.

D. En la técnica de espectro expandido por salto de frecuencia o FHSS (Frecuency Hopping Spread Spectrum) la señal se mueve de una frecuencia a otra, es decir, la expansión de la señal se produce transmitiendo una ráfaga en una frecuencia, saltando luego a otra frecuencia para transmitir otra ráfaga, y así sucesivamente.

Las frecuencias utilizadas para los saltos y el orden de utilización se denomina modelo de hopping (hopping pattern). El ser tiempo de permanencia en cada frecuencia es lo que se conoce como dwell time, que debe muy corto, pattern menor que milisegundos, para evitar interferencias; tanto el dwell time como el hopping están sujetos a restricciones por parte de los organismos de regulación.

## USO EFICIENTE DE ESPACIO, ESPECTRO Y TIEMPO EN REDES DE RADIO FRECUENCIA

El método de acceso, tal como la modulación de radio y el ancho de banda disponible, es importante para determinar la eficiencia y la capacidad de un sistema de radio. Los factores que permiten optimizar la capacidad de comunicación dentro de una área geográfica y del espectro de ancho de banda, son considerados más importantes que la forma de como son implementadas.

Los diseñadores de sistemas únicamente pueden definir la utilización del espacio y del tiempo, y una aproximación de la eficiencia de la tecnología de transmisión por radio. Los diseños de alta eficiencia han sido evitados en sistemas de radio y redes porque su utilización no es muy obvia en cuanto a rapidez y conveniencia.
Uno de los aspectos más importantes de la eficiencia del tiempo es la asignación de frecuencia consolidada y el tráfico de cargas de usuarios no relacionados entre si. Por lo menos, el punto alto y el promedio de circulación de cada grupo deben de tener diferentes patrones; esto es muy difícil porque los canales incompartibles pueden ser vistos como viables, aunque su capacidad puede llegar a ser insuficiente para las necesidades máximas.
Independientemente del rango, un conjunto de enlaces puede únicamente dar servicio a un fracción del área total.
Para una cobertura total del área, se debe de usar canales independientes, derivados por frecuencia, código o tiempo. No es fácil minimizar el número de canales independientes o conjunto de enlaces para una cobertura total. Mientras la distancia incrementa, la señal de radio disminuye, debido a la curvatura de la Tierra o a obstáculos fiscos naturales existentes .
Este diseño es muy utilizado en interferencia limitada. Existe una trayectoria normal cuando en el nivel de transferencia, de estaciones simultáneamente activas, no prevén la transferencia actual de datos.

Para este tipo de diseño, los siguientes factores son importantes:

- Es necesaria una relación señal-interferencia, para una comunicación correcta.

- Se requiere de un margen expresado en estadísticas para generar esta relación, aun en niveles de señal variables.

- La posición de las antenas que realizan la transmisión. La cual puede ser limitada por las estaciones y perfectamente controlada por puntos de acceso fijos.

- La función de la distancia para el nivel de la señal. Esta dada por el valor promedio de la señal, considerando las diferencias en la altura de la antena de la terminales y los impedimentos naturales en la trayectoria.

### Factor de reuso

El número de conjuntos de canales requeridos es comúnmente llamado Factor de Reuso o Valor N, para el sistema de planos celulares. El sistema de planos celulares original contempla 7 grupos de canales de comunicación y 21 grupos de canales de configuración basados en una estructura celular hexagonal. (Un patrón de un hexágono con 6 hexágonos alrededor, da el valor de 7, y un segundo anillo de 14 da el valor de 21.)
Estos valores se calcularon asumiendo la Modulación de indexamiento 2 FM, previendo un valor de captura de cerca de 12 dB y un margen de cerca de 6 dB. En los sistemas digitales el factor de reuso es de 3 4, ofreciendo menor captura y menor margen.

**Factor de distancia**

El promedio de inclinación de curvatura es reconocido por tener un exponente correspondiente a 35-40 dB/Decena para una extensión lejana y de propagación no óptica. Para distancias cortas el exponente es más cerca al espacio libre o 20 dB/Década. El aislamiento de estaciones simultáneamente activas con antenas omnidireccionales pueden requerir factores de Reuso de 49 o más en espacio libre. La distancia de aislamiento trabaja muy bien con altos porcentajes de atenuación media. Dependiendo de lo disperso del ambiente, la distancia de aislamiento en sistemas pequeños resulta ser en algunos casos la interferencia inesperada y por lo tanto una menor cobertura.

**Puntos de acceso**

La infraestructura de un punto de acceso es simple: Guardar y Repetir, son dispositivos que validan y retransmiten los mensajes recibidos. Estos dispositivos pueden colocarse en un punto en el cual puedan abarcar toda el área donde se encuentren las estaciones.

Las características a considerar son :

- La antena del repetidor debe de estar a la altura del techo, esto producirá una mejor cobertura que si la antena estuviera a la altura de la mesa.

- La antena receptora debe de ser más compleja que la repetidora, as aunque la señal de la transmisión sea baja, ésta podrá ser recibida correctamente. Un punto de acceso compartido es un repetidor, al cual se le agrega la capacidad de seleccionar diferentes puntos de acceso para la retransmisión (esto no es posible en un sistema de estacion-a-estacion, en el cual no se aprovechara el espectro y la eficiencia de poder, de un sistema basado en puntos de acceso).

La diferencia entre el techo y la mesa para algunas de las antenas puede ser considerable cuando existe en esta trayectoria un obstáculo o una obstrucción. En dos antenas iguales, el rango de una antena alta es 2x-4x, más que las antenas bajas, pero el nivel de interferencia es igual, por esto es posible proyectar un sistema basado en coberturas de punto de acceso, ignorando estaciones que no tengan rutas de propagación bien definidas entre si.

Los ángulos para que una antena de patrón vertical incremente su poder direccional de 1 a 6 están entre los 0° y los 30° bajo el nivel horizontal, y cuando el punto de acceso sea colocado en una esquina, su poder se podrá incrementar de 1 a 4 en su cobertura cuadral. El patrón horizontal se puede incrementar de 1 hasta 24 dependiendo del medio en que se propague la onda.

En una estación, con antena no dirigida, el poder total de dirección no puede ser mucho mayor de 2 a 1 que en la de patrón vertical. Aparte de la distancia y la altura, el punto de acceso tiene una ventaja de hasta 10 Db en la recepción de transmisión de una estación sobre otra estación . Estos 10 Db son considerados como una reducción en la transmisión de una estación, al momento de proyectar un sistema de estacion-a-estacion.

**Aislamiento de sistemas vecinos**

Con un proyecto basado en Puntos de Acceso, la cobertura de cada punto de acceso es definible y puede ser instalado para que las paredes sean una ayuda en lugar de un obstáculo. Las estaciones están recibiendo o transmitiendo activamente muy poco tiempo y una fracción de las estaciones asociadas, con un punto de acceso, están al final de una área de servicio; entonces el potencial de interferencia entre estaciones es mínimo comparado con las fallas en otros mecanismos de transmisión de gran escala.

De lo anterior podemos definir que tendremos dos beneficios del punto de acceso:

- El tamaño del grupo de reuso puede ser pequeño ( 4 es el valor usado, y 2 es el deseado).

- La operación asincrona de grupos de Reuso contiguos puede ser poca perdida, permitiendo as que el uso del tiempo de cada punto de acceso sea aprovechado totalmente.

Estos detalles incrementan materialmente el uso del tiempo.

**Eficiencia del tiempo .-**

El tiempo es importante para poder maximizar el servicio, al momento de diseñar la frecuencia en el espacio. El uso del tiempo está determinado por los protocolos y por los métodos de acceso que regularmente usen los canales de transmisión de la estación.

Las características del método de acceso para que se considere que tiene un tiempo eficiente, pueden estar limitada por los métodos que sean utilizados.

Algunas de estas características son:

- Después de completar una transmisión/ recepción, la comunicación debe de estar disponible para su siguiente uso.

    - No debe de haber tiempos fijos entre la transmision-recepcion.
    - Rellenar la longitud de un mensaje para complementar el espacio, es desperdiciarlo.

- La densidad de distribución geográfica y tiempo irregular de la demanda del tráfico deben ser conocidas.

    - Un factor de Reuso, es más eficiente por un uso secuencial del tiempo que por una división geográfica del área.

    - Para la comunicación en una área, se debe de considerar la posibilidad de que en áreas cercanas existan otras comunicaciones.
    -
    - La dirección del tráfico desde y hacia la estación no es igual, el uso de un canal simple de transmisión y recepción da una ventaja en el uso del tiempo.

- Para tráfico abundante, se debe de tener una lista de espera en la que se manejen por prioridades: El primero en llegar, es el primero en salir, además de poder modificar las prioridades.

- Establecer funciones para usar todo el ancho de banda del canal de comunicación, para que el tiempo que exista entre el comienzo de la transmisión y la disponibilidad de la comunicación, sea lo más corto posible.

- El uso de un saludo inicial minimiza tiempos perdidos, en el caso de que los paquetes transferidos no lleguen correctamente; cuando los paquetes traen consigo una descripción del servicio que requieren, hacen posible que se mejore su organización.

- La conexión para mensajes debe ser más eficiente que la selección, particularmente al primer intento, sin embargo la selección puede ser eficiente en un segundo intento cuando la lista de las estaciones a seleccionar sea corta.

Para transacciones de tipo asincrona, es deseable completar la transacción inicial antes de comenzar la siguiente. Deben completarse en el menor tiempo posible.

El tiempo requerido para una transacción de gran tamaño es un parámetro importante para el sistema, que afecta la capacidad del administrador de control para encontrar tiempos reservados con retardos, como hay un tiempo fijo permitido para la propagación, el siguiente paso debe comenzar cuando termina el actual. El control del tráfico de datos en ambas direcciones, se realiza en el administrador de control.

**Limite del tiempo y de la longitud del paquete**

Cuando el paquete es más pequeño, la proporción del tiempo usado al acceder al canal es mayor.

Aunque la carga pueda ser pequeña para algunas funciones, la transferencia y descarga de archivos son mejor administrados cuando la longitud del paquete tiene un buen tamaño, minimizandose el tiempo de transferencia.

En paquetes grandes, se incrementa la posibilidad de que el paquete tenga errores en el envío. En sistemas de radio el tamaño aproximado ideal es de 512 octetos o menos; un paquete con una longitud de 100-600 octetos puede permitir la salida oportuna de respuestas y datagramas prioritarios junto con los datagramas normales.

Es necesario proveer formas para dividir los paquetes en segmentos dentro de las redes inalámbricas. Para un protocolo propuesto, el promedio de mensajes transferidos es mayor para el tráfico originado por el saludo inicial que el originado por el punto de acceso. En este promedio se incluyen campos de dirección de red y otras funciones que son agregadas por el protocolo usado y no por el sistema de radio.

El mensaje más largo permitido para poder superar un retardo de acceso de 1.8 µseg. y un factor de reuso de 4, utiliza menos de 600 µseg. Un mensaje de 600 octetos utiliza 400 µseg. a una velocidad de transmisión de 12 Mbs; los 200 µseg. que sobran pueden ser usados para solicitar requerimientos pendientes. El tiempo marcado para un grupo de reuso de 4 puede ser de 2.400 µseg. Este tiempo total puede ser uniforme, entre grupos comunes y juntos, con 4 puntos de acceso. Sin embargo, la repartición del tiempo entre ellos será según la demanda.

Las computadoras necesitan varios anchos de banda, dependiendo del servicio a utilizar, ya sea este de transmisiones de datos, de video y voz, de voz, etc. La opción elegida dependerá de si:

- El medio fisco puede multiplexar de tal manera que un paquete sea un conjunto de servicios.
- El tiempo y prioridad es reservado para el paquete y los paquetes relacionados con el, la parte alta de la capa MAC es multiplexada.

La capacidad de compartir el tiempo de estos dos tipos de servicios ha incrementado la ventaja de optimizar la frecuencia en el espacio y los requerimientos para armar un sistema.

# CAPÍTULO II

## Normatividad 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 802.1l 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.ll 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 |
| 802.1l a (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 |
| 802.1l c | Pasarela MAC entre redes | Completo |
| 802.1l e | Calidad de servicio para aplicaciones avanzadas (voz, vídeo, etc.) | Activo |
| 802.1l f (2000) | Interoperatividad entre puntos de acceso de distintos fabricates (lnteraccess Point Protocol, IAPP | Activo |
| 802.1l 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 802.1la, 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.w*irelessethernet.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 Organízation),* 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.

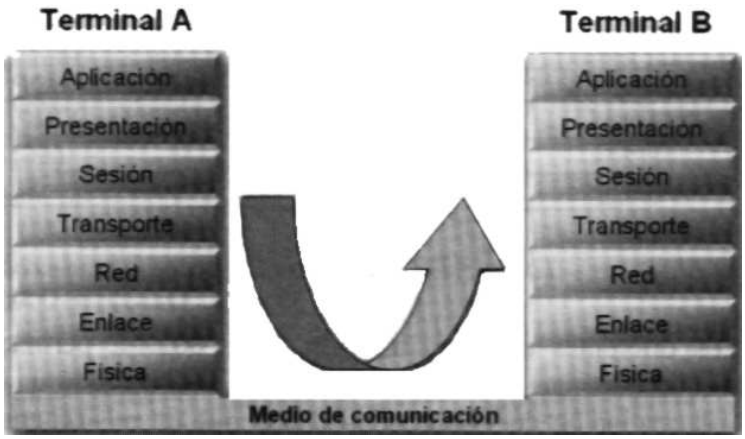



Fig.2.1 Esquema de comunicación del modelo OSI

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 | IP | HTTP , FTP,SMTP |
| 6 | Presentación | | |
| 5 | Sesión | | DNS,LDAP |
| 4 | Transporte | | UDP, TCP |
| 3 | Red | | ICPM, RSVP |
| 2 | Enlace | IEEE 802 | LLC,MAC |
| 1 | Físico | | Físico |

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.

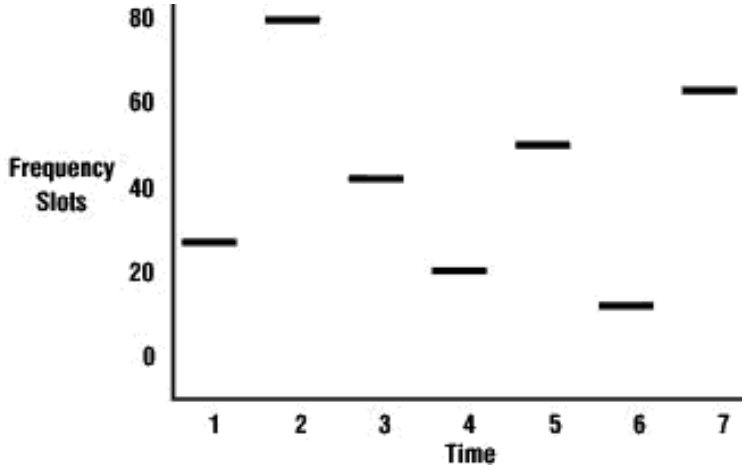



Fig. 2. 2 sistema FHSS

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.

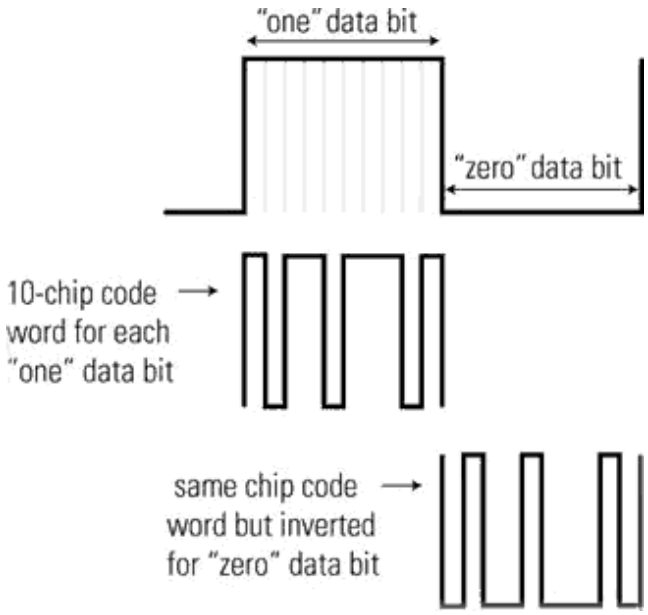



Fig. 2. .3 Principios del sistema DSSS

**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 Mu/tiple 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 que 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:

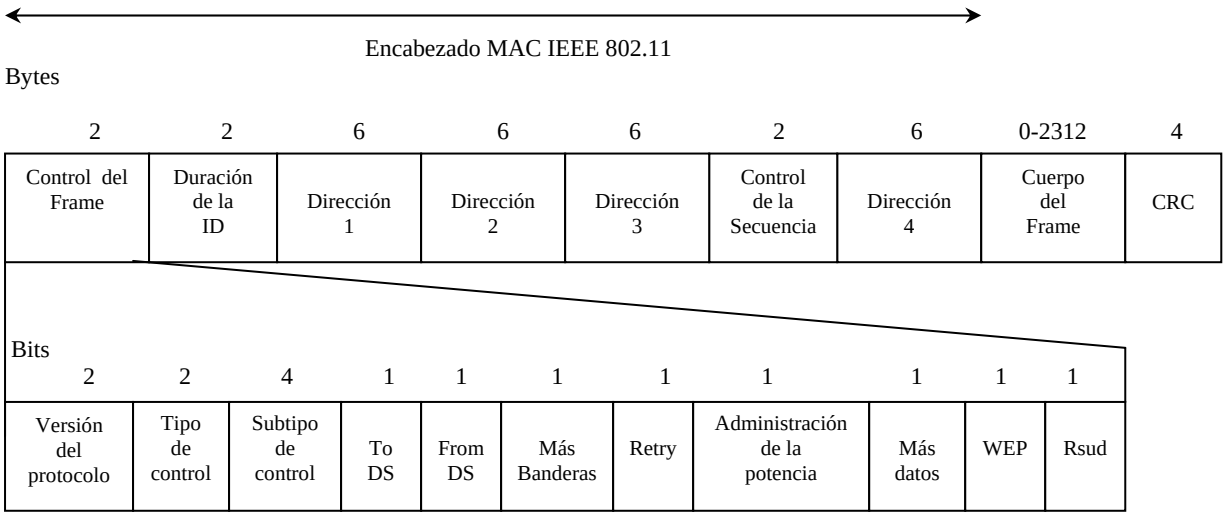



Fig. 2.4 Trama MAC IEEE 802.11

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 addressl4. 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.

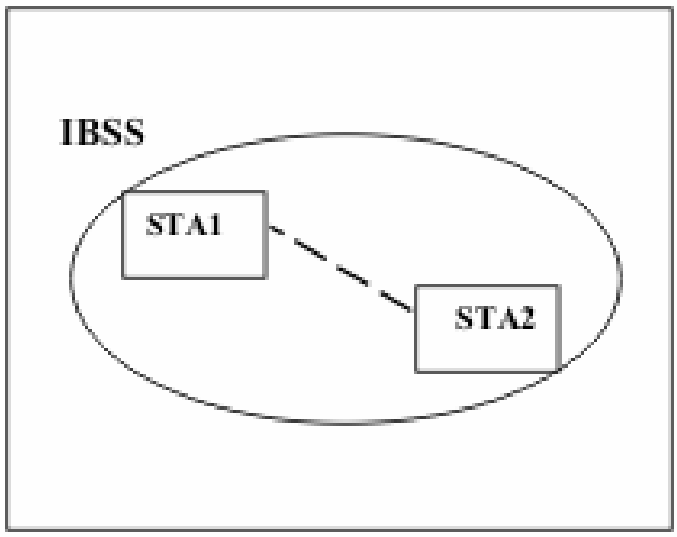



Fig2. 5 IBSS

**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.

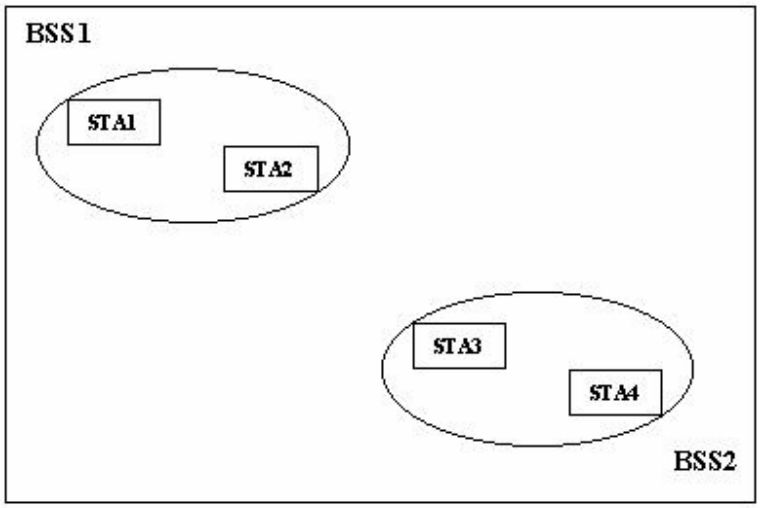



Figura 2 .6 BSSs

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

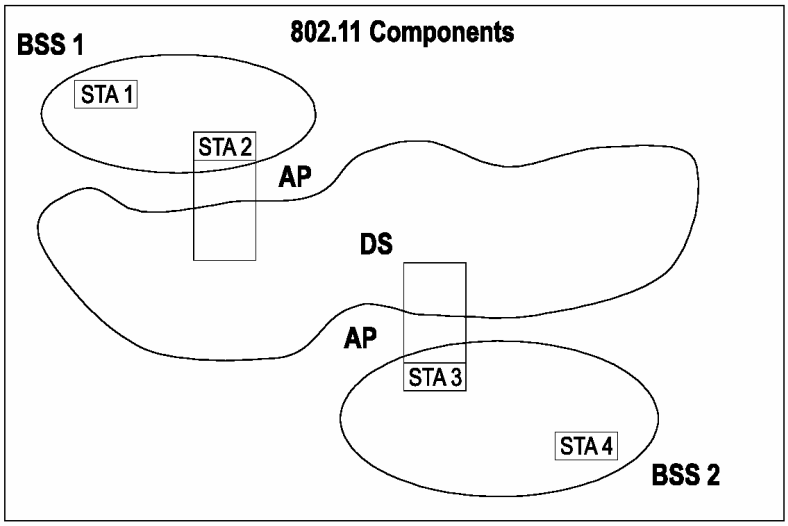



Figura 2. 7.DSs y APs

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.

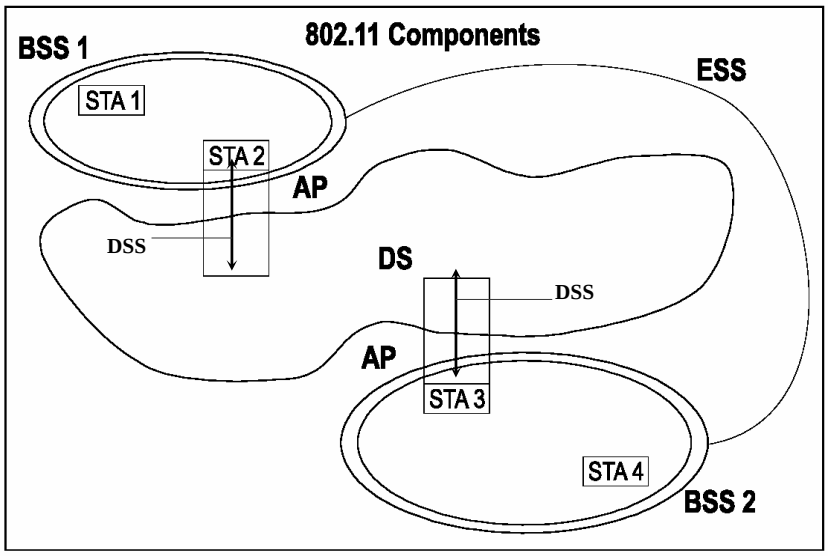



Fig. 2 .8ESS

**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.

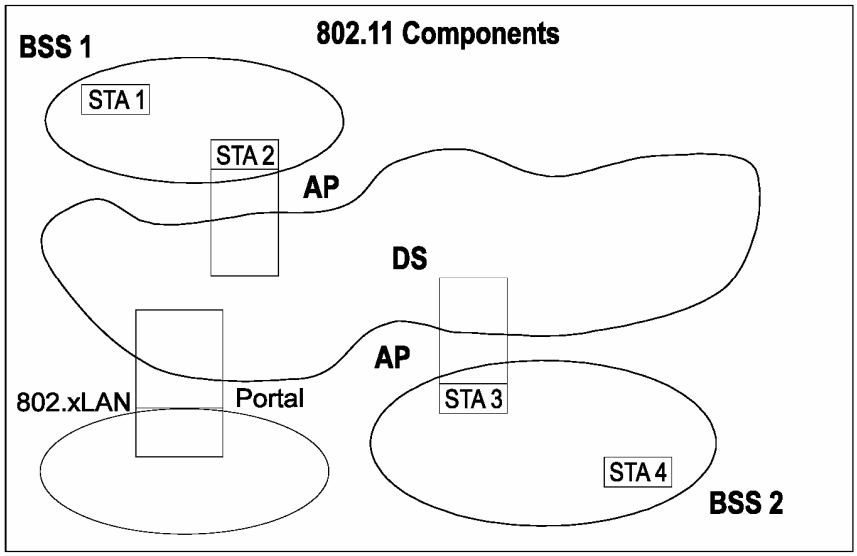



Figure 2.9Conexión de una LAN inalámbrica con IEEE 802 LANs

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.

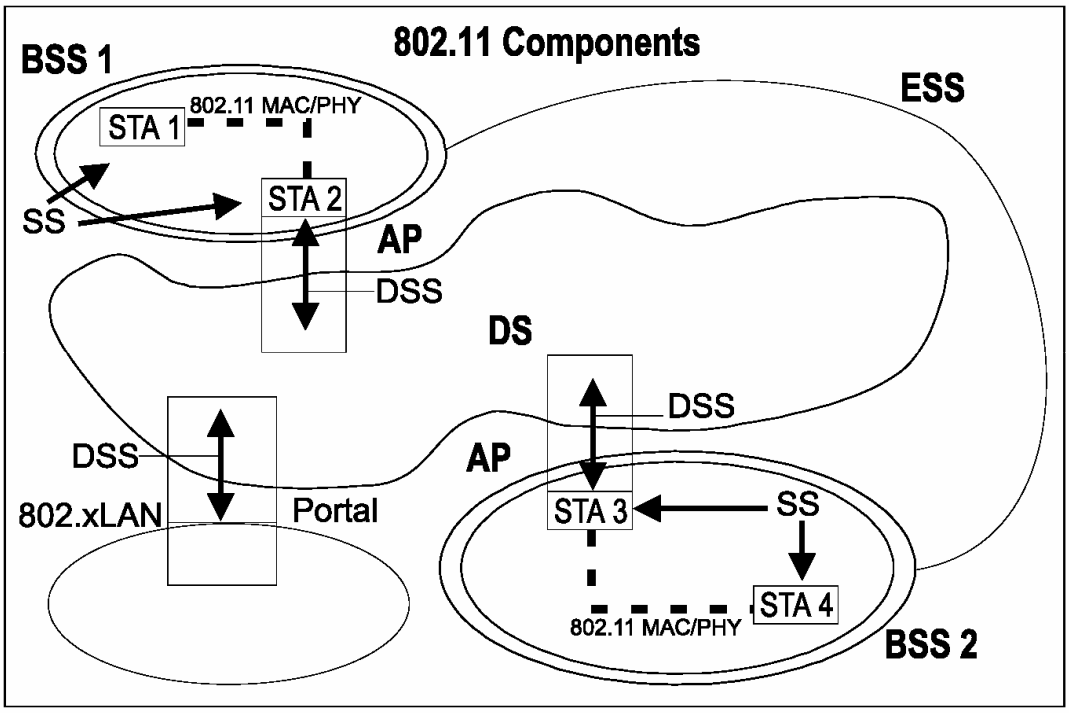



**Figure 2. 10.arquitectura completa de IEEE 802.11**
IEEE Wireless LAN Edition


## 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 tísica 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 tísica, 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 Física

**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 países 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<br>(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<br>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 países 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 específica, 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

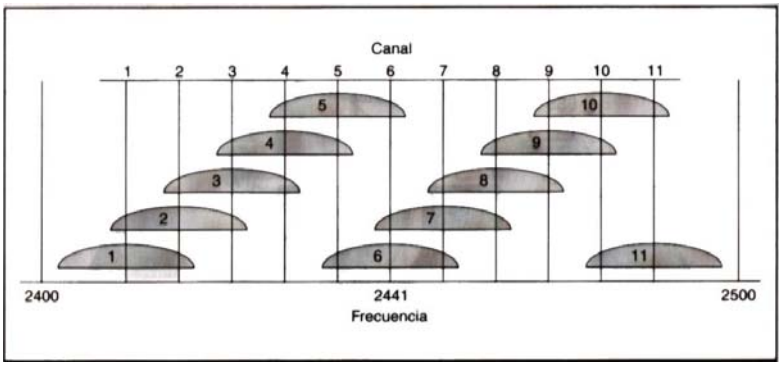



Fig. 2.12 Los 11 canales de 802.11 en la frecuencia de 2.4Ghz

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.

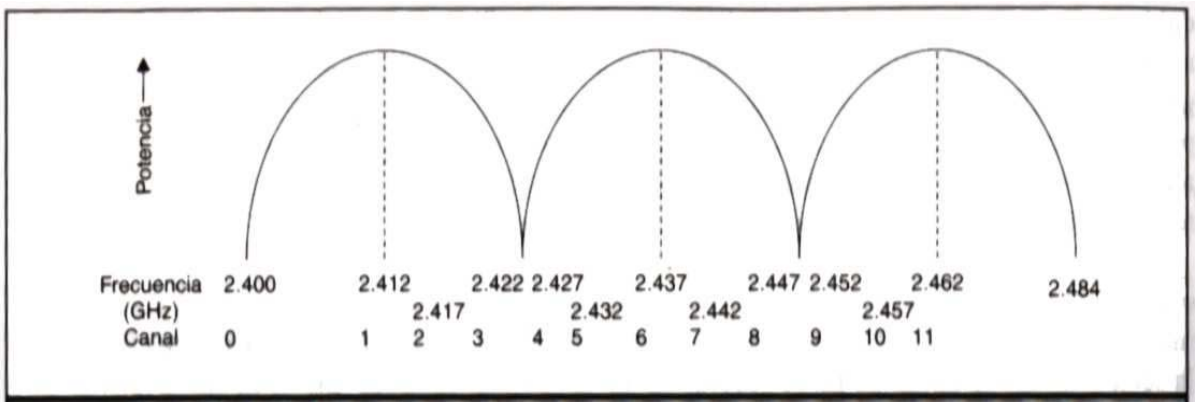



Fig. 2.13 A pesar de que las especificaciones 802.11b /g definen 11 canales en la banda ISM de 2.4 GHz de la FCC solo tres no se traslapan y por lo tanto se pueden usar

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.

# CAPITULO III. Diseño y seguridad de una red Wi–Fi.

**Diseño de la red inalámbrica.**

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 equipos 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, es necesario describir las características más importantes para una selección adecuada de algún tipo arquitectura Wi-Fi, así como, los parámetros a considerar para su implementación.

**Por qué instalar una red inalámbrica.**

Las redes inalámbricas hacen exactamente el mismo trabajo que realizan las redes cableadas: interconectan equipos y otros dispositivos para permitirles compartir recursos. Las redes locales permiten interconectar desde dos equipos 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.

Las ventajas que ofrece una red de área local, ya 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 equipo.
- Permite compartir aplicaciones.

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, es decir, la tecnología inalámbrica. El interés de disponer de la tecnología más moderna es valido 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.

**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 equipo 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 equipo 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 podemos 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 equipo portátil, sino que también nos permiten colocar un equipo 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. También es útil 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. En los 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 equipo 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.**

Claro que 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 trabajan 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**. Como las redes inalámbricas no necesitan de un medio físico para funcionar, esto se considera una ventaja, pero se convierte en un inconveniente cuando pensamos que cualquier persona con un equipo 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, descrito anteriormente) 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. Lo cierto es que las leyes del mercado vienen también marcadas por las necesidades de los clientes y 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.

**Tecnología inalámbrica.**

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), un único grabador de CD o un único escáner, cada vez es más normal disponer de más de un equipo 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.

El caso de las empresas puede ser similar al anterior, pero 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 equipo de sitio.

El hecho de instalar una red inalámbrica no significa 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 difíciles de cablear. 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.

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.).

**Opciones a considerar.**

Ya planteamos los puntos más importantes para confirmar que si necesitamos una red inalámbrica. Es hora de analizar qué tipo de red es la que le viene mejor a nuestras necesidades. Una red puede comunicar un par de equipos o a cientos de ellos, podemos tener a todos los equipos 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 equipo, PDA o cualquier otro equipo informático que necesitemos conectar.

- Qué tipo de antenas necesitaremos para poder cubrir toda el área para 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 la IEEE802.11 tiene 3 diferentes arquitecturas, estas arquitecturas se vieron de forma muy técnica en el capitulo anterior. A continuación se explicaran las mismas arquitecturas de una forma más comercial.

**IBSS (Independent Basic Service Set, “Conjunto de Servicios Básicos Independientes”).**

Esta modalidad está pensada para permitir exclusivamente comunicaciones directas entre las distintas terminales que forman la red. En este caso no existe ninguna 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 puertos están directamente conectados entre sí (lo que se conoce como topología de malla). Consiste simplemente en proveer a los equipos con una tarjeta de red inalámbrica de modo que todos hablen con todos. En este caso, no es necesario incorporar un punto de acceso. Presenta la ventaja de su sencillez pero, a cambio, crea 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 cuando se trabaja con compañeros en una ubicación remota. Esta topología es común en lugares en los que pueden reunirse pequeños grupos de equipos que no necesitan acceso a otra red; por ejemplo, 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*) que realiza las funciones de coordinación centralizada de la comunicación entre las distintas 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 separar 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, descrito anteriormente, 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.

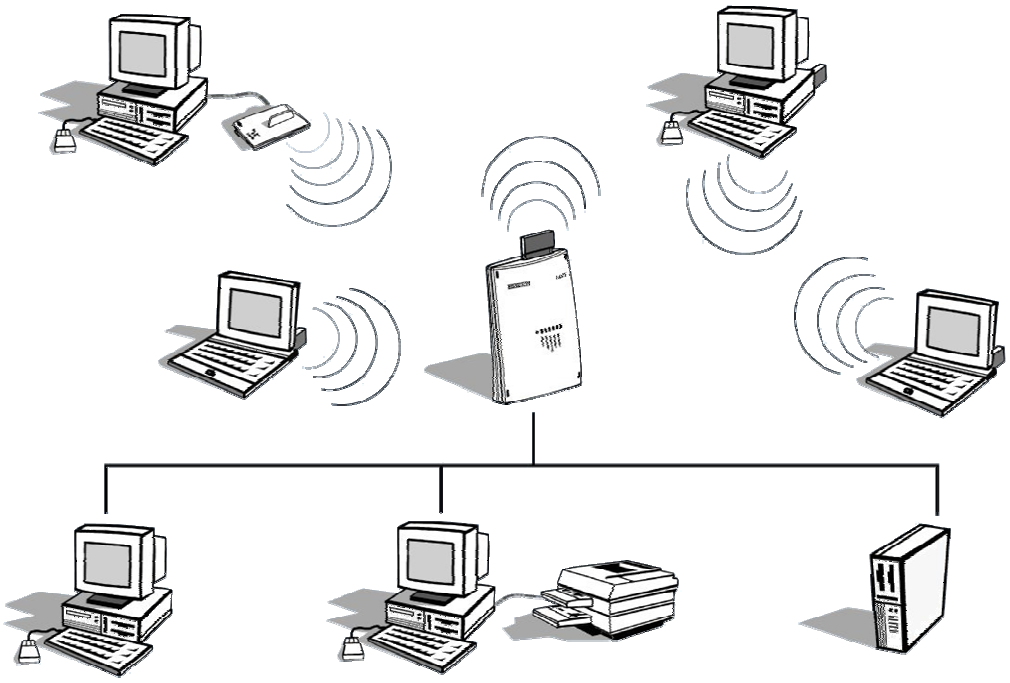


Fig.3.2 Estructura BSS o Infraestructura

**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 lograrlo se dispone de múltiples celdas BSS, cada una de las cuales cuenta con su punto de acceso. En esta configuración, las terminales pueden desplazarse por toda el área de cobertura sin perder la comunicación.

La configuración ESS resulta útil cuando es necesario cubrir una gran área de 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 las terminales inalámbricas puedan comunicarse con las 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, ya que de otro modo, los puntos de acceso se interferirían unos a otros impidiendo la comunicación con sus terminales.

Si un equipo pierde la comunicación con el AP, la reasociación con el nuevo AP se hace 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.

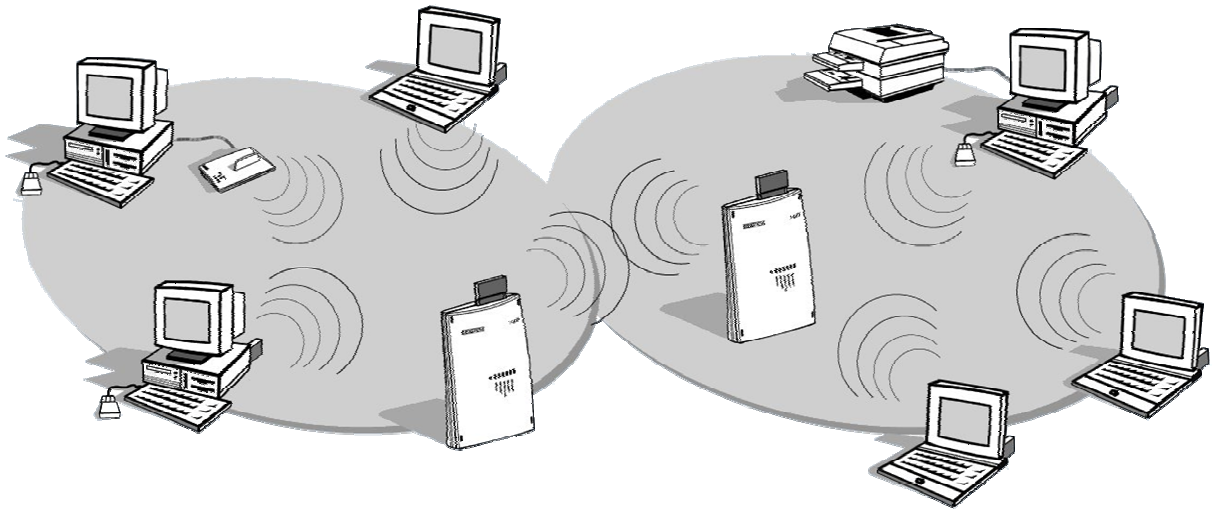


Fig.3. 3 Estructura ESS

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 una terminal no puede estar configurada para funcionar en la modalidad *ad hoc* (IBBS) y de infraestructura (BSS) a la vez.

**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 entre todas las terminales que forman la red, sean dos o más.

- 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 las terminales que forman la red como archivos, impresoras, etc.

Recientemente han aparecido en el mercado una alternativa al modo *ad hoc* conocida como *software* de punto de acceso. Esto consiste en configurar los equipos en modo *ad hoc* y hacer que uno de estos equipos haga las funciones de punto de acceso instalándole un programa especial, el *software* de punto de acceso.

**Alcance.**

Cuando nos decidimos a instalar una red inalámbrica, generalmente se parte de las necesidades de cobertura; es decir, pretendemos tener cobertura en toda la oficina, la casa, el entorno empresarial. Por lo que uno de los factores más importante de las redes inalámbricas es la cobertura. Esta depende tanto del alcance de los adaptadores de red (las tarjetas Wi-Fi), como 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. Hasta cierto punto es verdad, pero si el punto de acceso se instala 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.

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 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.

Sin embargo, la única manera de saber exactamente si existe cobertura entre los equipos es instalando los equipos y haciendo una prueba real de cobertura.

**lnterferencias.**

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 televigílancia, dispositivos bluetooth o, incluso, otras redes inalámbricas. Estos 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 por el uso del microondas. Muchas de estas interferencias pueden evitarse sencillamente situando el punto de acceso en otro lugar, o moviendo la terminal.

Debido a la naturaleza de la tecnología de radio, las señales de radio frecuencia pueden desvanecerse o bloquearse por materiales medioambientales. Antes de instalar es necesario hacer una inspección que 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 |

Como se vio anteriormente, 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.

**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 equipos 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 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.

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 en el lugar 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.**

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 y con 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, como mejoras en la seguridad y una mejor 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 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.

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 tener en cuenta dos cosas: la primera es 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 a utilizar 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 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 (conocido como *roaming*). En este caso, si los 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 pretende. 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.

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

**Características Principales de los Puntos de Acceso.**

Los puntos de acceso son 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 las 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.

**Puertos del Punto de Acceso.**

Los puntos de acceso necesitan disponer de puertos para poderse conectar con una red local cableada y con Internet. Para conseguir esto, los puntos de acceso cuentan con uno o más puertos 10/100Base-T (RJ-45). No obstante, 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 *hub,* 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 equipo encendido para poder mantener disponible la impresora. Además, la impresora no le ocuparía recursos a ningún equipo.

- Puerto para conectarle una antena exterior que le provea de un mayor alcance. 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*) o, incluso, requieren de un sistema operativo particular. Por ejemplo, Airport Base Station de Apple requiere disponer de un equipo con sistema operativo Mac. En cualquier caso, siempre es buena idea asegurarse de que el punto de acceso es compatible con nuestro sistema operativo.

La funcionalidad básica de los puntos de acceso o pasarela inalámbrica 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.
- 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.

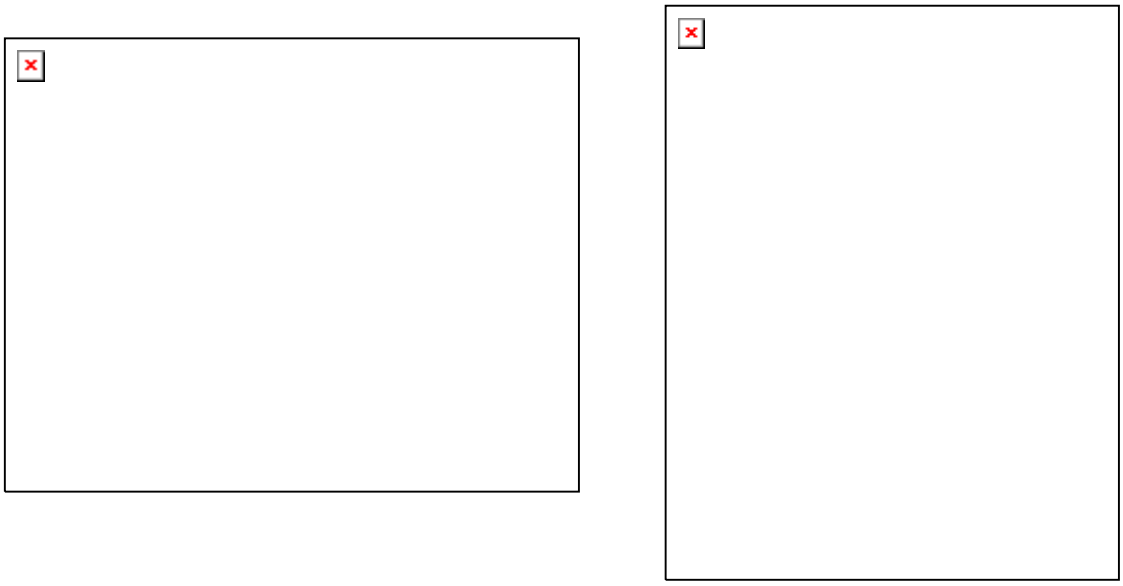


Fig. 3.5 Puntos de acceso

**Adaptadores Inalámbricos de Red.**

Los adaptadores de red son las tarjetas o dispositivos que se conectan a los equipos para que puedan funcionar dentro de una red inalámbrica. Estos equipos pueden recibir también el nombre de tarjetas de red o interfaces de red (NIC *Network Interface Cards*) es decir, cualquier tarjeta instalable o conectable a un equipo 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 equipo 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 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.**

Recientemente están apareciendo en el mercado algunos equipos portátiles que ya tienen integrado un adaptador de red Wi-Fi. No obstante, aun existe la necesidad de que el adaptador de red sea un equipo independiente que haya que instalar o conectar al equipo o PDA.

Actualmente existen los siguientes tipos de adaptadores inalámbricos de red:

- **Tarjetas PCMCIA. S**on tarjetas que tienen un tamaño similar al de una tarjeta de crédito, 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 equipos portátiles. Los equipos de sobremesa no suelen contar con puertos PCMCIA.

- **Tarjetas PCI o ISA.** Los equipos 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 también es posible instalar tarjetas conversoras de PCI o ISA a PCMCIA. Estos conversores son tarjetas PCI o ISA que se insertan en una ranura interna del equipo y que ofrecen un puerto PCMCIA al exterior. Evidentemente, adicionalmente haría falta disponer de la tarjeta PCMCIA.

- **Unidades USB.** Se trata de unidades inalámbricas que se conectan al equipo (portátil o sobremesa) mediante un puerto USB. Estas unidades son más propias de los equipos de sobremesa, ya que evitan tener que instalar en su interior un adaptador de tarjeta PCMCIA. No obstante, son válidas para todo tipo de equipos. Si el equipo ya tiene ocupados todos sus puertos USB existen multiplicadores de puertos USB que permiten sacar cuatro puertos de donde había uno.

**Tarjetas PCMCIA.**

Uno de los problemas que tenían antiguamente los equipos portátiles era que difícilmente podían ampliarse en sus prestaciones. Para instalarle una tarjeta de red o un módem a un equipo de sobremesa, bastaba con añadir en su interior la tarjeta correspondiente (ISA, PCI, etc.). Sin embargo, el interior de los portátiles, estuvo completamente cerrado hasta que aparecieron puertos especiales conocidos como PCMCIA *(Personal Computer Memory Card International Association*). Conocidas 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 equipo 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 *software* para tarjetas de memoria intercambiables. 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, usadas habitualmente en los adaptadores de red inalámbricos, y las de tipo III con un grosor de 10,5 milímetros utilizadas por los discos duros.

Por una razón exclusivamente de espacio, cada tarjeta requiere su propio tipo de ranura en el equipo. 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.

Los adaptadores Wi-Fi PCMCIA suelen ser de tipo II (con *bus* de 32 bits tipo *CardBus) y* la mayoría de los equipos portátiles incluyen una o dos ranuras PCMCIA de este tipo. Si tiene un equipo 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 equipos de sobremesa no suelen incluir ranuras PCMCIA. Estos equipos suelen disponer de suficiente espacio interior como para admitir la instalación de nuevos periféricos a base de tarjetas tipo PCI *(Peripheral Components Interconnect*) o ISA *(1ndustry Standard Architecture*). Este tipo de tarjetas es más barata que las tarjetas PCMCIA, pero son mayores en tamaño y de instalación algo más compleja. Sin embargo difícilmente se encuentran en el mercado adaptadores inalámbricos de red de tipo PCI o ISA. Para resolver este problema existen los adaptadores USB o la 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 equipo 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 equipo.

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 equipo de sobremesa pasa a ser algo más cara que la del equipo portátil.

El mayor inconveniente que presentan los dispositivos PCI e ISA es que requieren ser instalados en el interior del equipo.  Adicionalmente, incluso los que anuncian ser *Plug&Play* (tipo conectar y funcionar) finalmente requieren que se les instale el *software* de los controladores.

Si se cuenta con un equipo que dispone tanto de ranuras PCI como ISA, es más aconsejable utilizar las de tipo PCI; ya que suelen dar menos problemas de instalación y requieren menos recursos del sistema. 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 Ássociation*). La principal novedad que trajo PCI file el ser el primer sistema que permitía lo que se vino a llamar *Plug&Play* (conectar y funcionar).

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

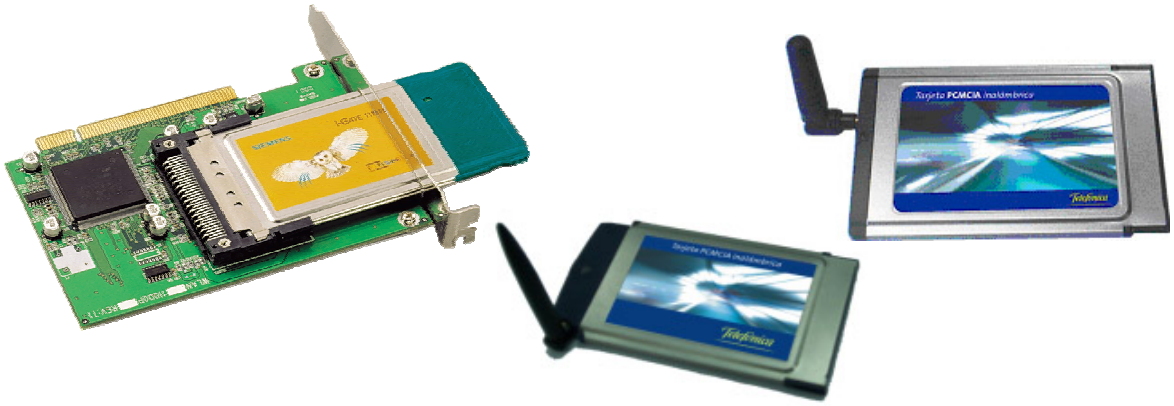


Fig 3.7 Tarjetas Wi-Fi  PCI

**Adaptadores USB.**

USB *(Universal Serial Bus*) es un nuevo puerto de comunicaciones que se diseñó para poder mejorar la forma en cómo los periféricos se conectaban a los equipos. Antes de que apareciera USB, las únicas posibilidades de conectar un periférico a un equipo eran mediante el puerto serie o el puerto paralelo. El inconveniente mayor con estos puertos es que sólo se podían conseguir velocidades de transmisión de 115 Kbps. Adicionalmente, los equipos 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 equipo reconocer automáticamente el dispositivo que tienen conectado, ni alimentarlos a través del propio puerto y el USB vino a traer las siguientes ventajas:

- No hace falta apagar el equipo para conectar o desconectar un periférico USB.
- El equipo 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 equipo 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.
- Los periféricos USB pueden apagarse automáticamente cuando detectan que no se están utilizando.
- Los periféricos USB se instalan automáticamente, sin necesidad de abrir el equipo.

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 equipos que no disponen de puertos serie ni paralelo, sino sólo puertos USB. Actualmente prácticamente todos los tipos de periféricos ofrecen la posibilidad de ser conectados al equipo a través de un puerto USB, tales como impresoras, módem, escáneres, cámaras, discos duros, etc.

Desde el punto de vista de los adaptadores de red inalámbrica, USB ofrece la ventaja de poder compartir el adaptador entre diferentes equipos según se necesite. Como instalar el adaptador es tan fácil como conectarlo al puerto USB, si un equipo 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 equipo.

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

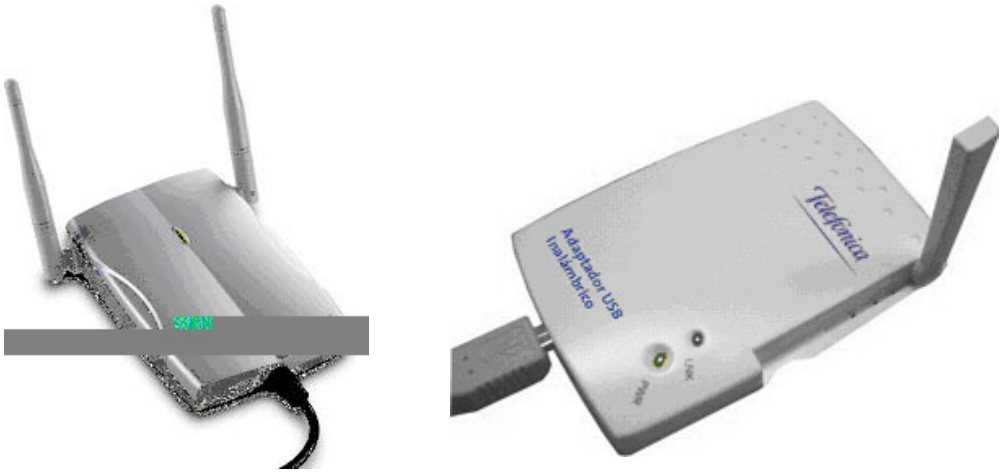



Fig. 3.8 Adaptadores USB para redes Wi-Fi

**Adaptadores para PDA.**

Un PDA es un pequeño equipo que cabe en la palma de la mano; 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, son asistentes personales de su usuario como agenda de direcciones, agenda de actividades, lista de tareas, juegos, etc. Sin embargo, un PDA puede utilizarse también como herramienta de comunicación que permite al usuario acceder a Internet, ver páginas *web*, gestionar correos electrónicos, etc. Del mismo modo, las nuevas PDA incluyen versiones reducidas de programas de gestión tan conocidos como Microsoft Word, Excel, etc. En definitiva, un PDA es un pequeño equipo de gran utilidad debido precisamente a su pequeño tamaño.

Habitualmente, un PDA se conecta a Internet a través de un equipo personal. Los correos se escriben en el PDA, pero no se transmiten hasta que no se conectan mediante un cable o infrarrojos al equipo 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. En este sentido, han aparecido 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, el PDA siempre estará conectado por cable para intercambiar sus datos con el equipo asociado o conectarse a Internet. Así, 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 equipos de la red inalámbrica utilicen las impresoras de la red cableada o accedan a los archivos de cualquiera de sus equipos.

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

**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, 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. 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*).

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

En el mercado existen muchos tipos de antenas que pueden funcionar bien en los entornos Wi-Fi. Sin embargo, es importante conocer 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. 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.

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 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 consiguen haces direccionales. Es 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 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.

**Diseño de la red.**

Una vez decidido para añadir un sistema inalámbrico necesitamos determinar como empezar y que productos son los indicados para soportar las aplicaciones, movilidad, rangos, seguridad y otras características de la red.

Para diseñar cualquier red después de haber determinado las necesidades del usuario es importante la definición del área de cobertura. Es importante contar con un diagrama adecuado de las instalaciones en donde se muestre la cobertura que necesitamos tomar en cuenta para la WLAN, así como determinar las velocidades mínimas que requieren los usuarios. Es igual de importante verificar si las instalaciones están construidas con materiales que permitan que las ondas de radio penetren en las áreas especifica. Las señales de 2.4 GHz penetran las construcciones normales de manera mas sencilla que las señales de 5 GHz; para lo que hay que realizar pruebas en las instalaciones procurando evitar la interferencia con los demás dispositivos como microodas, alarmas inalámbricas, dispositivos bluetooth, etc las cuales se pueden evitar mediante la colocación adecuada de los AP y las antenas.

Del mismo modo debemos determinar cuantos usuarios están ubicados dentro del área; por ejemplo para usuarios de aplicaciones de oficina es suficiente entre 10 y 20 usuarios por punto de acceso para tener un desempeño razonable, si lo que necesitamos son transacciones pequeñas que requiere un ancho de banda pequeño como una casa el número de usuarios por AP puede aumentar.

## Conclusiones

Actualmente, las redes locales inalámbricas (WLAN) se encuentran instaladas mayoritariamente en algunos entornos específicos, como almacenes, bancos, restaurantes, fábricas, hospitales y transporte. Las limitaciones que, de momento, presenta esta tecnología ha hecho que sus mercados iniciales hayan sido los que utilizan información tipo "bursty" (períodos cortos de transmisión de información muy intensos seguidos de períodos de baja o nula actividad) y donde la exigencia clave consiste en que los trabajadores en desplazamiento puedan acceder de forma inmediata a la información a lo largo de un área concreta, como un almacén, un hospital, la planta de una fábrica o un entorno de distribución o de comercio al por menor; en general, en mercados verticales.

Otras aplicaciones, las primeras que se vislumbraron, más bien de un carácter marginal debido a que en un principio no se captaba el potencial y la capacidad real de las WLAN, se refieren a la instalación de redes en lugares donde es difícil o compleja la instalación de una LAN cableada, como museos o edificios históricos, o bien en lugares o sedes temporales donde podría no compensar la instalación de cableado.

El previsible aumento del ancho de banda asociado a las redes inalámbricas y, consecuentemente, la posibilidad del multimedia móvil, permitirá atraer a mercados de carácter horizontal que surgirán en nuevos sectores, al mismo tiempo que se reforzarán los mercados verticales ya existentes. La aparición de estos nuevos mercados horizontales está fuertemente ligada a la evolución de los sistemas PCS (Personal Communications Systems), en el sentido de que la base instalada de sistemas PCS ha creado una infraestructura de usuarios con una cultura tecnológica y hábito de utilización de equipos de comunicaciones móviles en prácticamente todos los sectores de la industria y de la sociedad.

Esa cultura constituye el caldo de cultivo para generar una demanda de más y más sofisticados servicios y prestaciones, muchos de los cuales han de ser proporcionados por las WLAN. Soluciones propietarias

Otro de los factores que ha podido influir de forma negativa en la introducción de estas tecnologías ha sido la falta de un estándar que determine su implementación. Así, durante los últimos años los diferentes fabricantes han ido desarrollando sus propias soluciones, utilizando frecuencias y tecnologías muy distintas y normalmente incompatibles. Por último, y aunque no se deben comparar entre sí uno y otro tipo de redes dado su diferente nivel de prestaciones, es inevitable que se tienda a comparar sus precios, por lo que si a todo lo anterior unimos el mayor costo inicial de una red inalámbrica respecto al equivalente de una red de cable, tendremos una idea más clara de cuáles han

sido las principales razones por las que la introducción de este tipo de productos no ha sido tan rápida como en un principio se esperaba.

A pesar de todo esto, el crecimiento del mercado de redes inalámbricas, tanto mundial como europeo, ha sido realmente espectacular durante los últimos cuatro años, en los que ha experimentado crecimientos anuales superiores al cien por cien, tanto en volumen de facturación como en número de conexiones. Este crecimiento ha sido paralelo, y se debe, en su mayor parte, al auge experimentado por el mercado de los PC portátiles, para los que el empleo de una red inalámbrica cobra pleno sentido.

Resulta curioso observar que mientras el crecimiento en países como Francia, Reino Unido, Portugal o los países Nórdicos supera incluso los porcentajes anteriormente citados, el desarrollo de este mercado en España ha sido hasta la fecha mucho más lento. La causa habría que buscarla quizá en la falta de conocimiento de este tipo de tecnologías; quizá en que los presupuestos para tecnologías de información, al ser inferiores a la media europea, hacen al mercado español más sensible a los precios; o quizá en que en España siempre han sido más conservadores a la hora de emplear tecnologías de radio.

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 dos 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.

**Etherne**t. 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 0SI 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.

## Bibliografía.


**- 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®