UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

ANÁLISIS DE LA CAPA FÍSICA EN UNA RED INALÁMBRICA COMPATIBLE CON EL ESTANDAR IEEE 802.11

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

ALEX FRANCIS BARRERA ANDIA

PROMOCIÓN
1996–I

LIMA – PERÚ
2003

A mi familia que son el motivo
de mi superación.
A mi ratoncita.

ANÁLISIS DE LA CAPA FÍSICA EN UNA RED INALÁMBRICA COMPATIBLE CON EL ESTANDAR IEEE 802.11

SUMARIO

Este trabajo pretende ser un breve estudio, no extensiva ni profunda, sobre las nuevas técnicas de modulación para redes inalámbricas o WLANs que ha estandarizando el Working Group 802.11 del IEEE así como las que todavía están en proceso de estandarización. En concreto el estudio se centra en la banda de 2.4GHz y en las técnicas de modulación DSSS que son las que mayor aceptación ha tenido en el mercado.

ÍNDICE

CAPÍTULO II

CAPÍTULO III

CAPÍTULO IV

PRÓLOGO

En los últimos años, las comunicaciones inalámbricas han tenido un crecimiento sorprendente debido a la necesidad de mantener comunicadas a las personas aun estando en movimiento, así como a las recientes tecnologías en computadoras portátiles, y dispositivos para computadoras de escritorio, tales como módems inalámbricos y las mismas redes inalámbricas. Dicha necesidad se expande no solo a la transmisión de datos, sino también a la transmisión de voz y video, o en otras palabras una comunicación multimedia. Para satisfacer las necesidades de las redes inalámbricas,el grupo de estudio 802.11 fue formado bajo el proyecto de IEEE 802 para recomendar un estándar internacional para Redes de Área Local Inalámbricas (WLAN). Se tiene el Acceso Múltiple con Detección de Portadora con Evasión de Colisiones (CSMA/CA) como la base del Control de Acceso al Medio (MAC) para WLAN del estándar IEEE 802.11. Una parte importante del estándar son los protocolos MAC necesarios para soportar una transmisión asíncrona y limitada en tiempo. El desempeño de la subcapa MAC, el cual consiste de la Función de Coordinación Distribuida (DCF) y la Función de Coordinación de Punto (PCF) se crearon para la transmisión asíncrona y limitada en tiempo (voz y video) respectivamente en una red de infraestructura a 2 Mbps.

CAPÍTULO I

REDES ALÁMBRICAS

Una red consiste en dos o más computadoras unidas que comparten recursos (ya sea archivos, CD-ROM´s o impresoras) y que son capaces de realizar comunicaciones electrónicas. Las redes pueden estar unidas por cable, líneas de teléfono, ondas de radio, satélites, etc.

La clasificación básica de redes es:

- Red de Área Local / Local Área Network (LAN)
- Red de Área Metropolitana / Metropolitan Area Network (MAN)
- Red de Área Extensa / Wide Area Network (WAN)

1.1 Red de Área Local / Local Área Network (LAN)

Se trata de una red que cubre una extensión reducida como una empresa, una universidad, un colegio, etc. No habrá por lo general dos ordenadores que disten entre sí más de un kilómetro. Una configuración típica en una red de área local es tener una computadora llamada servidor de ficheros en la que se almacena todo el

software de control de la red así como el software que se comparte con los demás ordenadores de la red. Los ordenadores que no son servidores de ficheros reciben el nombre de estaciones de trabajo. Estos suelen ser menos potentes y suelen tener software personalizado por cada usuario. La mayoría de las redes LAN están conectadas por medio de cables y tarjetas de red, una en cada equipo.

1.2 Red de Área Metropolitana / Metropolitan Area Network (MAN)

Las redes de área metropolitana cubren extensiones mayores como puede ser una ciudad o un distrito. Mediante la interconexión de redes LAN se distribuye la información a los diferentes puntos del distrito. Bibliotecas, universidades u organismos oficiales suelen interconectarse mediante este tipo de redes.

1.3 Redes de Área Extensa / Wide Area Network (WAN)

Las redes de área extensa cubren grandes regiones geográficas como un país, un continente o incluso el mundo. Cable transoceánico o satélites se utilizan para enlazar puntos que distan grandes distancias entre sí. Con el uso de una WAN se puede contactar desde España con Japón sin tener que pagar enormes cantidades de teléfono. La implementación de una red de área extensa es muy complicada. Se

utilizan multiplexadores para conectar las redes metropolitanas a redes globales utilizando técnicas que permiten que redes de diferentes características puedan comunicarse sin problemas. El mejor ejemplo de una red de área extensa es Internet.

1.4 Principales tipos de topologías físicas

1.4.1 Topología de Bus / Linear Bus

Consiste en un cable con un terminador en cada extremo del que se "cuelgan" todos los elementos de una red. Todos los Nodos de la Red están unidos a este cable. Este cable recibe el nombre de "Backbone Cable". Tanto Ethernet como LocalTalk pueden utilizar esta topología. Ver Figura 1.1

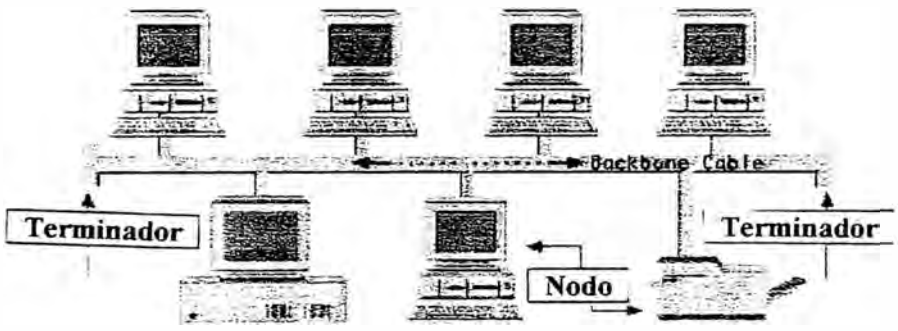


Figura 1.1: Topología de Bus

Las ventajas de la topología de Bus es que es fácil conectar nuevos nodos a la red. Requiere menos cable que una topología estrella. Las desventajas de la topología de Bus es que toda la red se caería si hubiera una ruptura en el cable principal. Se requieren terminadores. Es difícil detectar el origen de un problema cuando toda la red "cae". No se debe utilizar como única solución en un gran edificio.

1.4.2 Topología de estrella / Star

En una topología estrella todos y cada uno de los nodos de la red se conectan a un concentrador o hub. Los datos en estas redes fluyen del emisor hasta el concentrador. Este controla realiza todas las funciones de red además de actuar como amplificador de los datos. Esta configuración se suele utilizar con cables de par trenzado aunque también es posible llevarla a cabo con cable coaxial o fibra óptica. Tanto Ethernet como LocalTalk utilizan este tipo de tipología. Ver Figura 1.2

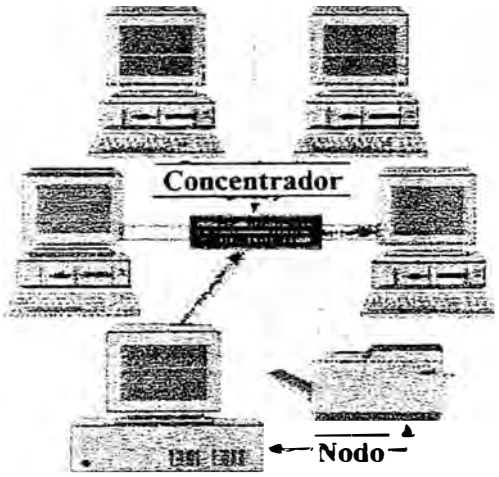


Figura 1.2: Topología estrella

La ventaja de la topología de estrella es que es de gran facilidad de instalación. Posibilidad de desconectar elementos de red sin causar problemas. Facilidad para la detección de fallo y su reparación. Los inconvenientes de la topología de estrella son que Requiere más cable que la topología de bus. Un fallo en el concentrador provoca el aislamiento de todos los nodos a él conectados. Se han de comprar hubs o concentradores.

1.4.3 Topología de Estrella cableada / Star-Wired Ring

Físicamente parece una topología estrella pero el tipo de concentrador utilizado, la MAU se encarga de interconectar internamente la red en forma de anillo. Esta topología es la que se utiliza en redes Token-Ring. Ver Figura 1.3

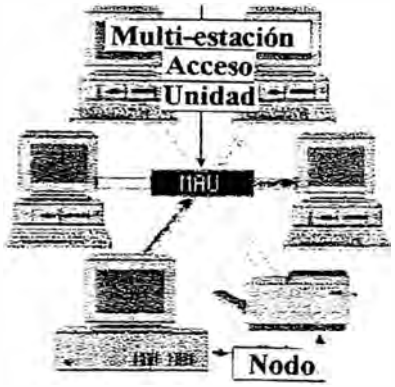


Figura 1.3: Topología de estrella cableada

1.4.4 Topología de Arbol / Tree

La topología de árbol combina características de la topología de estrella con la de bus. Consiste en un conjunto de subredes estrella conectadas a un bus. Esta topología facilita el crecimiento de la red. Ver Figura 1.4

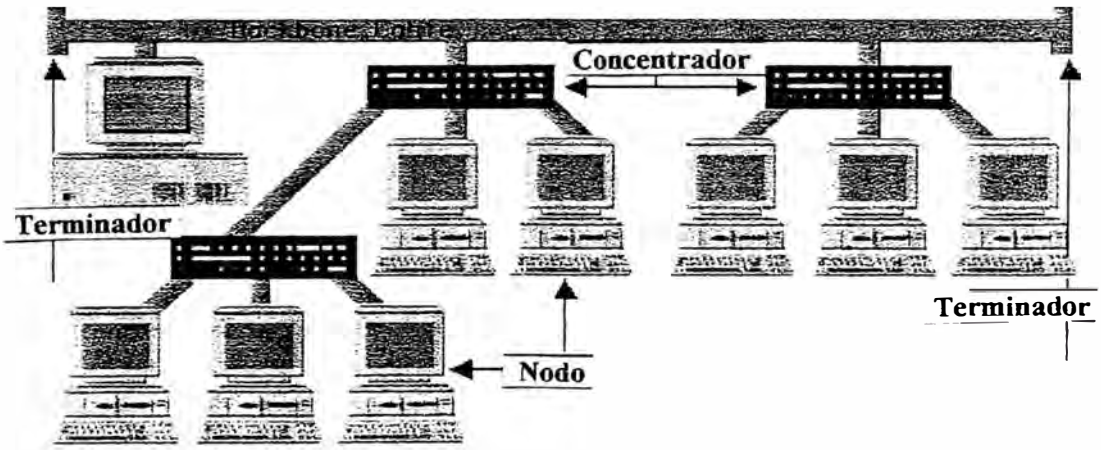


Figura 1.4: Topología de árbol.

Las ventajas de la topología de árbol es que el cableado punto a punto para segmentos individuales. Soportado por multitud de vendedores de software y de hardware. Los inconvenientes de la topología de árbol son: la medida de cada segmento viene determinada por el tipo de cable utilizado. Si se viene abajo el segmento principal todo el segmento se viene abajo. Es más difícil la configuración.

1.5 Protocolos LAN (Red de Area Local)

Un protocolo es un conjunto de normas que rigen la comunicación entre las computadoras de una red. Estas normas especifican que tipo de cables se utilizarán, que topología tendrá la red, que velocidad tendrán las comunicaciones y de que forma se accederá al cana de transmisión. Los estándares más populares son: Ethernet, LocalTalk , Token Ring FDDI.

1.5.1 Ethernet

Ethernet es hoy en día el Standard para la redes de área local. Tanto Ethernet (Versión 2) como el muy similar estándar IEEE802.3 definen un modo de acceso múltiple y de detección de colisiones, es el conocido carrier sense multiple access/collision detection (CSMA/CD). Cuando una estación quiere acceder a la red escucha si hay alguna transmisión en curso y si no es así transmite. En el caso de que dos redes detecten probabilidad de emitir y emitan al mismo tiempo se producirá una colisión pero esto queda resuelto con los sensores de colisión que detectan esto y fuerzan una retransmisión de la información.

- **Cableados**

Tipo de Ethernet	Velocidad (Mbps)	Distancia (m)	Media
10Base5 (IEEE 802.3)	10	500	Coaxial Grueso
10Base2 (IEEE 802.3)	10	185	Coaxial Fino
10BaseT (IEEE 802.3)	10	100	UTP
10BaseF(IEEE 802.3)	10	2000	Fibra Optica

Tabla 1.1: Cableados

- **Topología**

El protocolo Ethernet permite tres tipos de topología: Bus, Estrella y Arbol. (Linear Bus, star y Tree).

- **Formatos de Trama IEEE 802.3 (Figura 1.5)**

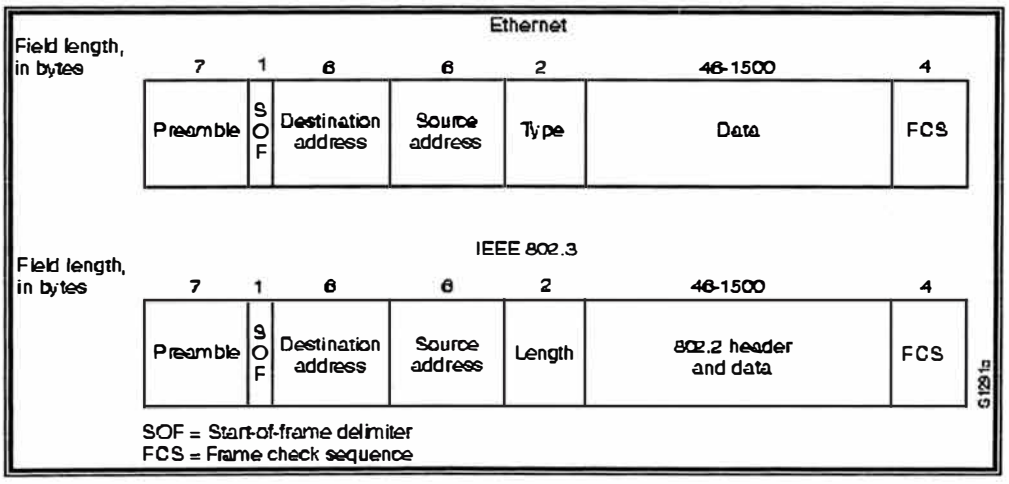


Figura 1.5: Trama IEEE 802.3

Ethernet define de qué manera se introducirán los datos en la red. Donde se indicará el receptor, el emisor donde irán los datos, donde irá el checksum, etc. Esto

se define en la trama Ethernet. En la figura superior se puede ver la distribución de la información en cada paquete enviado. Se comienza con un preámbulo que termina al que sigue la trama en sí. El inicio de la trama es la información de la dirección de destino seguido de la dirección de procedencia a lo que sigue el tipo o la longitud de la información los datos y el checksun de la trama. El checksun (FCS) se comprueba en la llegada para asegurarse de la correcta recepción de la información.

- **Fast Ethernet**

Para aumentar la velocidad de la red de 10Mbs a 100Mbs se han definido nuevos estándares de Ethernet denominados en conjunto FastEthernet (IEE802.3u). Tres nuevos tipos de redes Ethernet han visto la luz. Las topologías posibles quedan reducidas a la topología estrella.

1.5.2 LocalTalk

El protocolo LocalTalk fue desarrollado por Apple Computer, Inc. para ordenadores Macintosh. El método de acceso al medio es el CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). Este método, similar al de Ethernet (CSMA/CD) se diferencia en que el ordenador anuncia su transmisión antes de realizarla. Mediante el uso de adaptadores LocalTalk y cables UTP especiales se puede crear una red de ordenadores Mac a través del puerto serie. El sistema operativo de estos establece relaciones punto a punto sin necesidad de software adicional aunque se puede crear una red cliente servidor con el sofware AppleShare. Con el protocolo LocalTalk se pueden utilizar topologías bus, estrella o árbol usando cable UTP pero la velocidad de transmisión es muy inferior a la de Ethernet.

1.5.3 Token Ring

El protocolo Token Ring fue desarrollado por IBM a mediados de los 80. El modo de acceso al medio esta basado en el traspaso del testigo (token passing). En una red Token Ring los ordenadores se conectan formando un anillo. Un testigo (token) electrónico pasa de un ordenador a otro. Cuando se recibe este testigo se está en disposición de emitir datos. Estos viajan por el anillo hasta llegar a la estación receptora. Las redes Token Ring se montan sobre una tipología estrella cableada (star-wired) con par trenzado o fibra óptica. Se puede transmitir información a 4 o 16 Mbs. Cabe decir que el auge de Ethernet está causando un descenso cada vez mayor del uso de esta tecnología.

- **Formatos de trama tramas en Token Ring (Figura 1.6)**

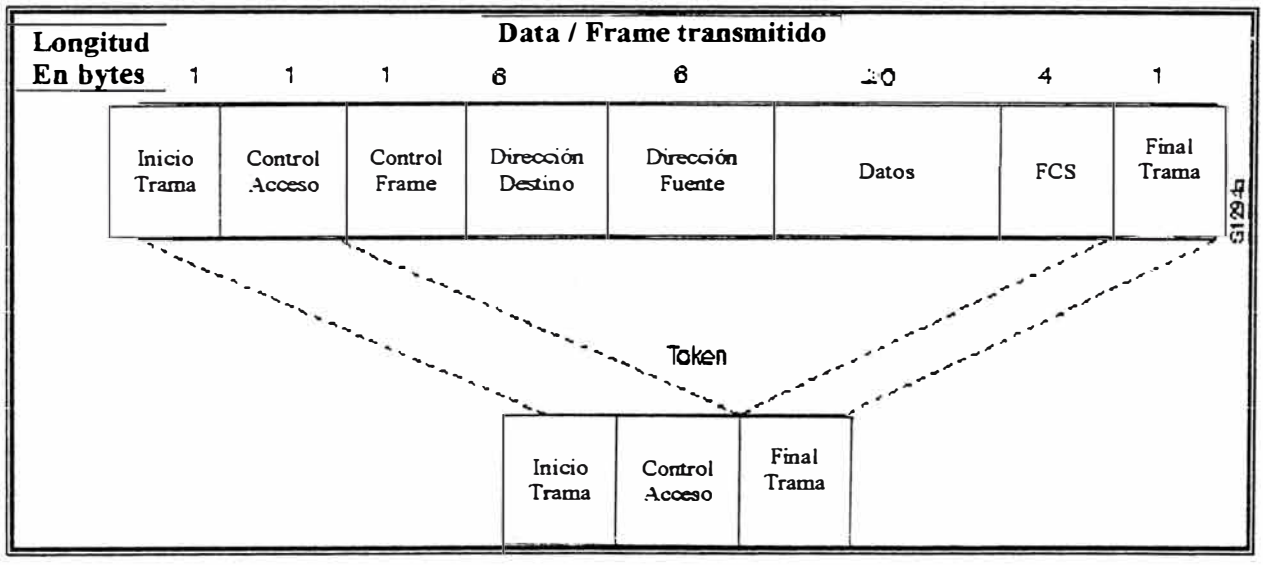


Figura 1.6: Tramas Token Ring

Como se puede ver, la trama de Token Ring es similar a la de Ethernet, la principal diferencia consiste en que a los datos se le agrega un Token, que es el que marca la prioridad de transmisión.

1.5.4 FDDI (Interfaz de Datos sobre Fibra Distribuida)

FDDI son las siglas de Fiber Distributed Data Interface. Este protocolo de red se utiliza principalmente para interconectar dos o más redes locales que con frecuencia distan grandes distancias. Ver Figura 1.7.

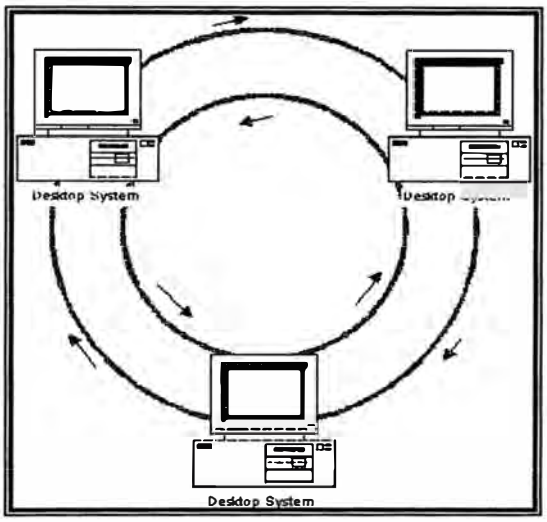


Figura 1.7: Anillo Lógico FDDI

El método de acceso al medio utilizado por FDDI está basado también en el paso de testigo. La diferencia es que en este tipo de redes la topología es de anillo dual. La transmisión se da en uno de los anillos pero si tiene lugar un error en la transmisión el sistema es capaz de utilizar una parte del segundo anillo para cerrar el anillo de transmisión. Se monta sobre cables de fibra óptica y se pueden alcanzar velocidades de 100Mbps. Ver Figura 1.8

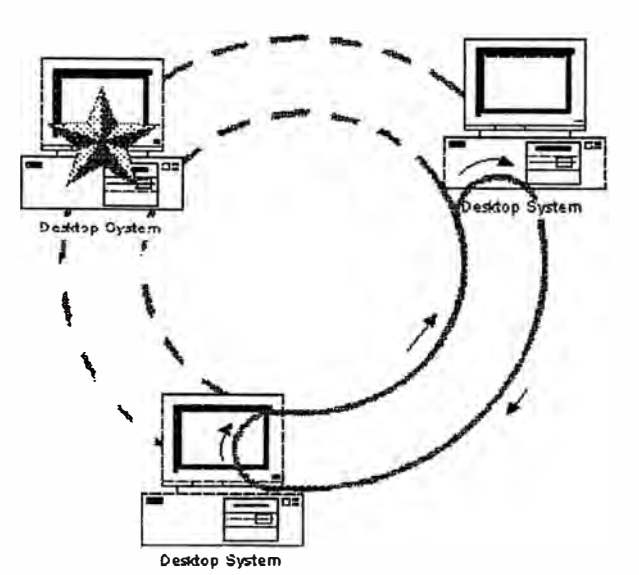


Figura 1.8: Anillo dual FDDI

1.6 Componentes de las redes LAN

Las redes de ordenadores se montan con una serie de componentes de uso común y que en mayor o menor medida siempre aparecerán en cualquier instalación. Comentaremos brevemente los siguientes: Servidores o File servers, Estaciones de trabajo o Workstations, Tarjetas de Red (NIC), Concentradores y Hubs, Repetidores, Puentes o Bridges, Routers, Cortafuegos o Firewalls.

- **Servidores**

Los servidores de ficheros conforman el corazón de la mayoría de las redes. Se trata de ordenadores con mucha memoria RAM, un enorme disco duro (o varios) y una rápida tarjeta de red. El sistema operativo de red se ejecuta sobre estos servidores así como las aplicaciones compartidas. Un servidor de impresión se encargará de controlar gran parte del tráfico de red ya que será el que acceda a las demandas de las estaciones de trabajo, y el que les proporciones los servicios que pidan, impresión,

ficheros, Internet, etc. Está claro que necesitamos un ordenador con capacidad de guardar información de forma muy rápida y de compartirla con la misma celeridad.

- **Estaciones de trabajo**

Son los ordenadores conectados al servidor. Las estaciones de trabajo no han de ser tan potentes como el servidor, simplemente necesitan una tarjeta de red, el cableado pertinente y el software necesario para comunicarse con el servidor. Una estación de trabajo puede carecer de disquetera y de disco duro y trabajar directamente sobre el servidor. Prácticamente cualquier ordenador puede actuar como una estación de trabajo.

- **Tarjeta de red**

La tarjeta de red (NIC) es la que conecta físicamente al ordenador a la red. Son tarjetas que se pinchan en el ordenador como si de una tarjeta de video se tratase o cualquier otra tarjeta. Puesto que todos los accesos a red se realizan a través de ellas se deben utilizar tarjetas rápidas si queremos comunicaciones fluidas.

Las tarjetas de red más populares son por supuesto las tarjetas Ethernet, existen también conectores LocalTalk así como tarjetas TokenRing.

- **Concentradores o Hubs**

Un concentrador o Hub es un elemento que provee una conexión central para todos los cables de la red. Los hubs son "cajas" con un número determinado de conectores, habitualmente RJ45 más otro conector adicional de tipo diferente para

enlazar con otro tipo de red. Los hay de tipo inteligente que envían la información solo a quien ha de llegar mientras que los normales envían la información a todos los puntos de la red siendo las estaciones de trabajo las que decidirán si se quedan o no con esa información. Están provistos de salidas especiales para conectar otro Hub a uno de los conectores permitiendo así ampliaciones de la red.

- **Repetidores**

Cuando una señal viaja a lo largo de un cable va perdiendo "fuerza" a medida que avanza. Esta pérdida de fuerza puede desembocar en una pérdida de información. Los repetidores amplifican la señal que reciben permitiendo así que la distancia entre dos puntos de la red sea mayor que la que un cable solo permite.

- **Bridges**

Los bridges se utilizan para segmentar redes grandes en redes más pequeñas. De esta forma solo saldrá de la red pequeña el tráfico destinado a otra red pequeña diferente mientras que todo el tráfico interno seguirá en la misma red. Con esto se consigue una reducción del tráfico de red.

- **Routers**

Un router dirige tráfico de una red a otra, se podría decir que es un bridge superinteligente ya que es capaz de calcular cual será el destino más rápido para hacer llegar la información de un punto a otro. Es capaz también de asignar diferentes preferencias a los mensajes que fluyen por la red y enrutar unos por caminos más cortos que otros así como de buscar soluciones alternativas cuando un

camino está muy cargado. Mientras un bridge conoce la dirección de las computadoras a cada uno de sus extremos un router conoce la dirección tanto de las computadoras como de otros routers y bridges y es capaz de "escanear" toda la red para encontrar el camino menos congestionado.

- **Cortafuegos o Firewalls**

Un firewall es un elemento de seguridad que filtra el tráfico de red que a él llega. Con un cortafuegos podemos aislar un ordenador de todos los otros ordenadores de la red excepto de uno o varios que son los que nos interesa que puedan comunicarse con él. En la figura se ve como el cortafuegos aisla al ordenador de la izquierda del ordenador "Foe" mientras que permite la comunicación con el ordenador "Friend".

1.7 El cableado de la red

El cable es el medio a través del cual fluye la información a través de la red. Hay distintos tipos de cable de uso común en redes LAN. Una red puede utilizar uno o más tipos de cable, aunque el tipo de cable utilizado siempre estará sujeto a la topología de la red, el tipo de red que utiliza y el tamaño de esta. Estos son los tipos de cable más utilizados en redes LAN: Cable de par trenzado sin apantallar / UTP, Unshielded twisted pair, Cable de par trenzado apantallado / STP Shielded twisted pair, Cable coaxial, Cable de fibra óptica

- **Cable de par trenzado sin apantallar / Unshielded Twisted Pair (UTP) Cable**

Este tipo de cable es el más utilizado. Tiene una variante con apantallamiento pero la variante sin apantallamiento suele ser la mejor opción para una PYME. La calidad del cable y consecuentemente la cantidad de datos que es capaz de transmitir varían en función de la categoría del cable. Las gradaciones van desde el cable de teléfono, que solo transmite la voz humana a el cable de categoría 5 capaz de transferir 100Megabytes por segundo.

Categorías UTP

Tipo	Uso
Categoría1	Voz (Cable de teléfono)
Categoría 2	Datos a 4 Mbps (LocalTalk)
Categoría 3	Datos a10 Mbps (Ethernet)
Categoría 4	Datos a 20 Mbps/16 Mbps Token Ring
Categoría 5	Datos a 100 Mbps (Fast Ethernet)

Tabla 2: Categorías UTP

La diferencia entre las distintas categorías es la tirantez. A mayor tirantez mayor capacidad de transmisión de datos. Se recomienda el uso de cables de Categoría 3 o 5 para la implementación de redes en PYMES (pequeñas y medianas empresas). Es conveniente sin embargo utilizar cables de categoría 5 ya que estos permitirán migraciones de tecnologías 10Mb a tecnología 100Mb. EL Conector UTP

es el estándar para conectores de cable UTP es el RJ-45. Se trata de un conector de plástico similar al conector del cable telefónico. Las siglas RJ se refieren al estándar Registerd Jack, creado por la industria telefónica. Este estándar define la colocación de los cables en su pin correspondiente.

- **Cable de par trenzado Apantallado / Shielded Twisted Pair (STP) Cable**

Una de las desventajas del cable UTP es que es susceptible a las interferencias eléctricas. Para entornos con este problema existe un tipo de cable UTP que lleva apantallamiento, esto es, protección contra interferencias eléctricas. Este tipo de cable se utiliza con frecuencia en redes con topología Token Ring.

- **Cable Coaxial**

El cable coaxial contiene un conductor de cobre en su interior. Este va envuelto en un aislante para separarlo de un apantallado metálico con forma de rejilla que aisla el cable de posibles interferencias externas. Aunque la instalación del cable coaxial es más complicada que la del UTP, este tiene un alto grado de resistencia a las interferencias. Por otra parte también es posible conectar distancias mayores que con los cables de par trenzado. Existen dos tipos de cable coaxial, el fino y el grueso conocidos como thin coaxial y thick coaxial. Con frecuencia se pueden escuchar referencias al cable coaxial fino como thinnet o 10Base2. Esto hace referencia a una red de tipo Ethernet con un cableado coaxial fino, donde el 2 significa que el mayor segmento posible es de 200 metros, siendo en la práctica reducido a 185 m. El cable coaxial es muy popular en las redes con topología de BUS. Con frecuencia se pueden

escuchar referencias al cable coaxial grueso como thicknet o 10Base5. Esto hace referencia a una red de tipo Ethernet con un cableado coaxial grueso, donde el 5 significa que el mayor segmento posible es de 500 metros. El cable coaxial es muy popular en las redes con topología de BUS. El cable coaxial grueso tiene una capa plástica adicional que protege de la humedad al conductor de cobre. Esto hace de este tipo de cable una gran opción para redes de BUS extensas, aunque hay que tener en cuenta que este cable es difícil de doblar. El Conector para cable coaxial más usado es el conector BNC. BNC son las siglas de Bayone-Neill-Concelman. Los conectores BNC pueden ser de tres tipos: normal, terminadores y conectores en T.

- **Cable de fibra óptica**

El cable de fibra óptica consiste en un centro de cristal rodeado de varias capas de material protector. Lo que se transmite no son señales eléctricas sino luz con lo que se elimina la problemática de las interferencias. Esto lo hace ideal para entornos en los que haya gran cantidad de interferencias eléctricas. También se utiliza mucho en la conexión de redes entre edificios debido a su inmunidad a la humedad y a la exposición solar. Con un cable de fibra óptica se pueden transmitir señales a distancias mucho mayores que con cables coaxiales o de par trenzado. Además, la cantidad de información capaz de transmitir es mayor por lo que es ideal para redes a través de las cuales se desee llevar a cabo videoconferencia o servicios interactivos. El coste es similar al cable coaxial o al cable UPT pero las dificultades de instalación y modificación son mayores. En algunas ocasiones escucharemos 10BaseF como referencia a este tipo de cableado. En realidad estas siglas hablan de una red Ethernet con cableado de fibra óptica. Las características generales son el

aislante exterior está hecho de teflón o PVC, Fibras Kevlar ayudan a dar fuerza al cable y hacer más difícil su ruptura, se utiliza un recubrimiento de plástico para albergar a la fibra central, el centro del cable está hecho de cristal o de fibras plásticas. Los Conectores para fibra óptica más utilizada es el conector ST. Tiene una apariencia similar a los conectores BNC. También se utilizan, cada vez con más frecuencia conectores SC, de uso más fácil.

CAPÍTULO II

REDES INALÁMBRICAS LOCALES (WLAN)

2.1 Introducción

Uno de los grandes avances dentro del mundo de la informática nació en 1970, momento en que la red ethernet fue desarrollada: un conjunto de máquinas podía intercambiar información de forma efectiva. Lentamente, esta opción iba a llegar a estar al alcance de todo el mundo. Actualmente, es el tipo de red más extendida. De todos modos, la idea básica no era tan nueva en aquel momento, ya que la comunicación por cable puede remontarse a inventos como el telégrafo o el teléfono, aunque sí que era innovadora la manera de resolver el problema de dividir un medio compartido. De todas maneras, a medida que la implantación de redes locales se extendió, también se hizo evidente que, aparte de la idea básica, también compartía algunos de los inconvenientes principales: la necesidad forzosa de crear una infraestructura previa a su implantación, o sea, el hecho de tener que perforar las paredes o el suelo para introducir los cables, así como la limitación de la movilidad de los extremos a comunicar. Este problema no sólo se da en el diseño inicial, sino que surge cada vez que quiere ampliarse la red; la única solución posible es sobredimensionarla durante su diseño, a partir de estimaciones de crecimiento. O se hace esto o se empieza a optar por soluciones temporales que acaban siendo permanentes, con cables y hubs (concentradores) escondidos detrás de los

ordenadores o debajo de las mesas, fuera de los armarios de los cables contemplados inicialmente. De todos modos, incluso acertando a la primera, podemos encontrarnos con el problema de que puede no ser sencillo hacer llegar el cable a todas partes en condiciones.

Dado este factor limitador, era lógico pensar que la tecnología de redes locales acabaría siguiendo los pasos de sus predecesores, y de la misma forma que el telégrafo pasó a ser sin hilos y aparecieron los teléfonos celulares (y actualmente sobran los comentarios sobre el fenómeno de la telefonía móvil), surgió la idea de crear redes locales inalámbricas (WLAN, Wireless Local Area Network). Otra vez nos encontramos ante un concepto básico que de ninguna manera es nuevo —las primeras comunicaciones sin hilos datan de principios del siglo pasado— aplicado finalmente a tecnologías modernas.

2.2 Descripción general de las WLAN

Las redes LAN inalámbricas de alta velocidad ofrecen las ventajas de la conectividad de red sin las limitaciones que supone estar atado a una ubicación o por cables. Existen numerosos escenarios en los que este hecho puede ser de interés; entre ellos, se pueden citar los siguientes.

Las conexiones inalámbricas pueden ampliar o sustituir una infraestructura con cables cuando es costoso o está prohibido tender cables. Las instalaciones temporales son un ejemplo de una situación en la que la red inalámbrica tiene sentido

o incluso es necesaria. Algunos tipos de construcciones o algunas normativas de construcción pueden prohibir el uso de cableado, lo que convierte a las redes inalámbricas en una importante alternativa.

Y, por supuesto, el fenómeno asociado al término "inalámbrico", es decir, no tener que instalar más cables además de los de la red de telefonía y la red de alimentación eléctrica, ha pasado a ser el principal catalizador para las redes domésticas y la experiencia de conexión desde el hogar.

Los usuarios móviles, cuyo número crece día a día, son indudables candidatos a las redes LAN inalámbricas. El acceso portátil a las redes inalámbricas se realiza a través de equipos portátiles y NIC inalámbricas. Esto permite al usuario viajar a distintos lugares (salas de reunión, vestíbulos, salas de espera, cafeterías, aulas, etc.) sin perder el acceso a los datos de la red. Sin el acceso inalámbrico, el usuario tendría que llevar consigo pesados cables y disponer de conexiones de red.

Más allá del campo empresarial, el acceso a Internet e incluso a sitios corporativos podría estar disponible a través de zonas activas de redes inalámbricas públicas. Los aeropuertos, los restaurantes, las estaciones de tren y otras áreas comunes de las ciudades se pueden dotar del equipo necesario para ofrecer este servicio. Cuando un trabajador que está de viaje llega a su destino, quizás una reunión con un cliente en su oficina, se puede proporcionar acceso limitado al usuario a través de la red inalámbrica local. La red reconoce al usuario de la otra organización y crea una conexión que, a pesar de estar aislada de la red local de la empresa, proporciona acceso a Internet al visitante.

En todos estos escenarios, vale la pena destacar que las redes LAN inalámbricas actuales basadas en estándares funcionan a alta velocidad, la misma velocidad que se consideraba vanguardista para las redes con cable hace tan solo unos años. El acceso del usuario normalmente supera los 11 MB por segundo, de 30 a 100 veces más rápido que las tecnologías de acceso telefónico o de las redes WAN inalámbricas estándar. Este ancho de banda es sin duda adecuado para que el usuario obtenga una gran experiencia con varias aplicaciones o servicios a través de PC o dispositivos móviles. Además, los avances en curso de estos estándares inalámbricos continúa aumentando el ancho de banda, con velocidades de 22 MB.

Muchos proveedores de infraestructura están dotando de cable zonas públicas de todo el mundo. En los próximos 12 meses, la mayoría de los aeropuertos, centros de conferencias y muchos hoteles proporcionarán acceso de 802.11b a sus visitantes.

La tecnología WLAN viene regida por el estándar 802.11, especificado por el Institute of Electrical and Electronics Engineers (IEEE), el mismo organismo encargado de especificar el resto de tecnologías de red (como la ethernet, la 802.3). Mediante este proceso, se garantiza inicialmente la interoperabilidad entre diferentes fabricantes y un funcionamiento dentro de las capas del modelo de comunicaciones igual que cualquier otra tecnología de LAN. Por tanto, su interacción con protocolos de comunicación, como TCP/IP, es totalmente transparente. Desde el punto de vista del sistema operativo, usar un adaptador de WLAN es lo mismo que utilizar uno de LAN tradicional. Actualmente, existen 4 estándares básicos para comunicación inalámbrica en redes locales:

- **802.11**: Es el primero que apareció; contempla la comunicación hasta 2Mbps y emite en la banda de 2.4GHz ISM (Industrial, Scientific and Medical, una frecuencia donde no hace falta licencia para operar) o dentro del espectro infrarrojo.
- **802.11b**: Surgió casi inmediatamente después del anterior; llega hasta 11Mbps dentro de la misma banda. Actualmente es el sistema más extendido.
- **802.11a**: Aprobado a la vez que el 802.11b; emite hasta 54Mbps dentro de la banda de los 5GHz UNII.
- **802.11g**: Es el último que apareció y bastante reciente (en el mes de noviembre de 2001); es una extensión para permitir anchos de banda superiores a los 20Mbps en la banda de 2.4GHz.

2.3 Tecnología inalámbrica LAN

Actualmente, destaca la implementación de dos soluciones LAN inalámbricas. Se trata de los estándares IEEE 802.11, principalmente 802.11b, y la solución propuesta por el grupo de trabajo HomeRF. Ambas soluciones no son interoperables entre sí ni con otras soluciones de redes LAN inalámbricas. Mientras que HomeRF está diseñado exclusivamente para el entorno doméstico, 802.11b se está implementando en hogares, en la pequeña y mediana empresa, en grandes organizaciones y en un número cada vez mayor de zonas activas de redes inalámbricas públicas. Algunos de los principales distribuidores de portátiles los equipa o tiene previsto equiparlos con tarjetas NIC 802.11b internas. A continuación se ofrece una comparación de las dos soluciones:

	IEEE 802.11B	HOMERF
Principales fabricantes que lo han admitido	Cisco, Lucent, 3Com WECA	Apple, Compaq, HomeRF Working Group
Estado	Se incluye	Se incluye (baja velocidad)
Extensión	50-300 pies (15,24-91,44 cm)	150 pies (45,72 cm)
Velocidad	11 Mbps	1, 2, 10 Mbps
Aplicación	Hogares, oficinas pequeñas, campus, empresas	Hogar
Costo	75-150 dólares por tarjeta	85-129 dólares
Seguridad	WEP/802.1x	NWID/cifrado
Distribuidores	Más de 75	Menos de 30
Puntos de acceso públicos	Más de 350	Ninguno
Cuota de mercado de las tarjetas NIC inalámbricas	72%	21%

Tabla 2.1: Diferencias entre IEEE 802.11b y HomeRF

Grandes empresas entre ellas Microsoft considera que 802.11 es la solución más sólida y prometedora que se puede aplicar a múltiples entornos.

2.4 Topologías de las WLAN

Las redes LAN inalámbricas se construyen utilizando dos topologías básicas. Para estas topologías se utilizan distintos términos, como administradas y no

administradas, alojadas y par a par, e infraestructura y "ad hoc". En este documento se utilizarán los términos "infraestructura" y "ad hoc". Estos términos están relacionados, esencialmente, con las mismas distinciones básicas de topología.

2.4.1 WLAN tipo infraestructura.

Una topología de infraestructura es aquella que extiende una red LAN con cable existente para incorporar dispositivos inalámbricos mediante una estación base, denominada punto de acceso. El punto de acceso une la red LAN inalámbrica y la red LAN con cable y sirve de controlador central de la red LAN inalámbrica.

El punto de acceso coordina la transmisión y recepción de múltiples dispositivos inalámbricos dentro de una extensión específica; la extensión y el número de dispositivos dependen del estándar de conexión inalámbrica que se utilice y del producto. En la modalidad de infraestructura, puede haber varios puntos de acceso para dar cobertura a una zona grande o un único punto de acceso para una zona pequeña, ya sea un hogar o un edificio pequeño. Ver Figura 2.1.

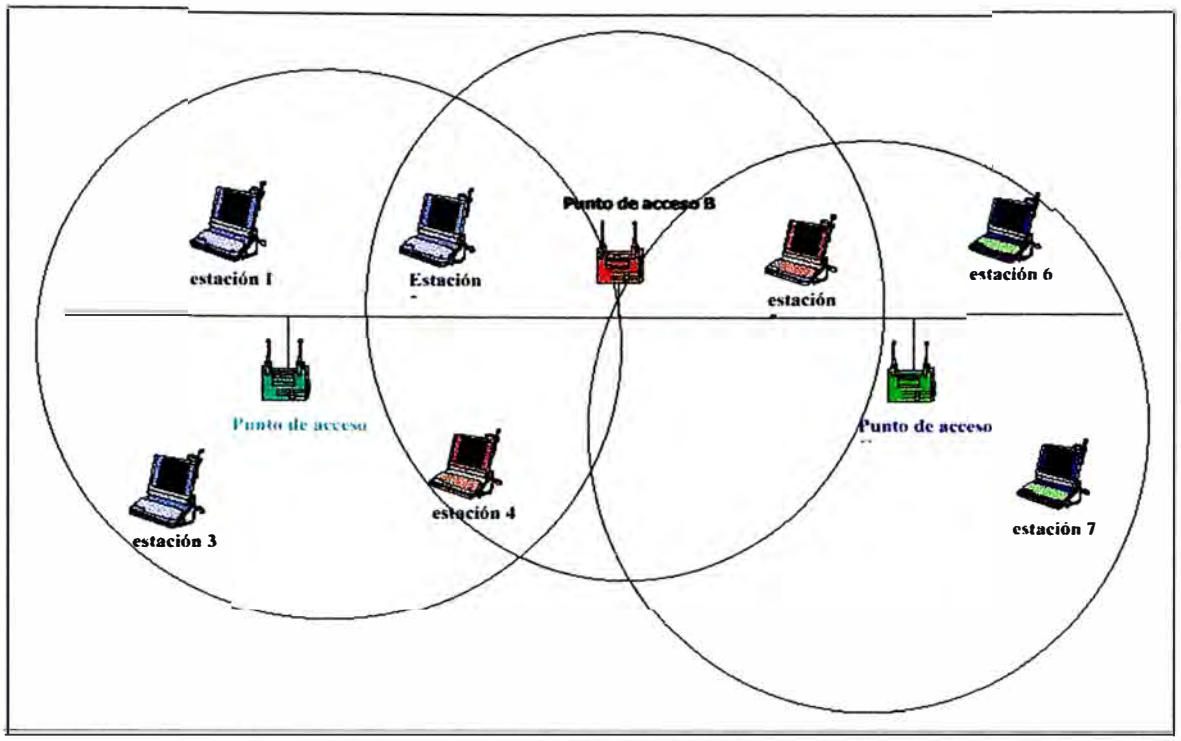


Figura 2.1: Red de tipo infraestructura

Descripción general del funcionamiento de la modalidad de infraestructura:

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

La estación elige una red entre las que están disponibles e inicia un proceso de autenticación con el punto de acceso. Una vez que el punto de acceso y la estación se han verificado mutuamente, comienza el proceso de asociación.

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

En la modalidad de infraestructura, todo el tráfico de red procedente de las estaciones inalámbricas pasa por un punto de acceso para poder llegar a su destino en la red LAN con cable o inalámbrica.

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

Dado que es posible que algunas estaciones no se escuchen mutuamente, aunque ambas estén dentro del alcance del punto de acceso, se toman medidas especiales para evitar las colisiones. Entre ellas, se incluye una clase de intercambio de reserva que puede tener lugar antes de transmitir un paquete mediante un intercambio de tramas "petición para emitir" y "listo para emitir", y un vector de

asignación de red que se mantiene en cada estación de la red. Incluso aunque una estación no pueda oír la transmisión de la otra estación, oirá la transmisión de "listo para emitir" desde el punto de acceso y puede evitar transmitir durante ese intervalo.

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

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

En las WLANs del tipo infraestructura, se incluyen nodos especiales llamados puntos de acceso, los cuales se interconectan por medio de un sistema de distribución que permite a una red de estaciones inalámbricas abarcar la mayor área posible, y tener acceso a las redes fijas existentes. Por lo tanto, se puede dividir el tráfico típico de la red en dos direcciones: enlace de subida (hacia la dorsal) y enlace de bajada (de la dorsal).

- **Tráfico de enlace de bajada:** Debido al ancho de banda limitado de las WLAN, típicamente se utiliza un canal común para la comunicación entre

puntos de acceso y los nodos móviles. La comunicación de enlace de bajada se logra transmitiendo en este canal común. Más preciso, el punto de acceso transmite a todos los nodos móviles aún si es un solo destino. La actividad del enlace de bajada constituye casi el 75 u 80% del total del tráfico en redes inalámbricas [Chen, 1994].

- **Tráfico de enlace de subida:** El enlace de subida es una consideración importante de la subcapa MAC en el diseño de redes inalámbricas, puesto que es necesario reconocer y registrar a los usuarios nuevos que entran a la red, y aquellos que la dejan, a cualquier hora, y en cualquier lugar. Generalmente se necesita un protocolo de acceso múltiple para organizar las transmisiones de nodos móviles [Chen, 1994].

2.4.2 WLAN de Propósito específico (Ad-hoc).

Redes Ad-hoc es un concepto en comunicaciones computacionales, el cual significa que los usuarios desean comunicarse con otros usuarios en una red temporal, sin ninguna forma de administración centralizada (como sucede en las redes de infraestructura), sin la ayuda de una dorsal, ya sea inalámbrica o fija. Cada nodo participante en este tipo de red (ad-hoc) actúa tanto como un servidor (host), así como un enrutador (router).

Los nodos en una red ad-hoc pueden consistir en computadoras personales tipo laptops, como asistentes digitales personales. Una de las características importantes de las redes Ad-hoc, es la topología dinámica con la que se cuenta, lo

cual es a consecuencia de la movilidad de los nodos, donde los nodos pueden cambiar de posición frecuentemente. Ver Figura 2.2

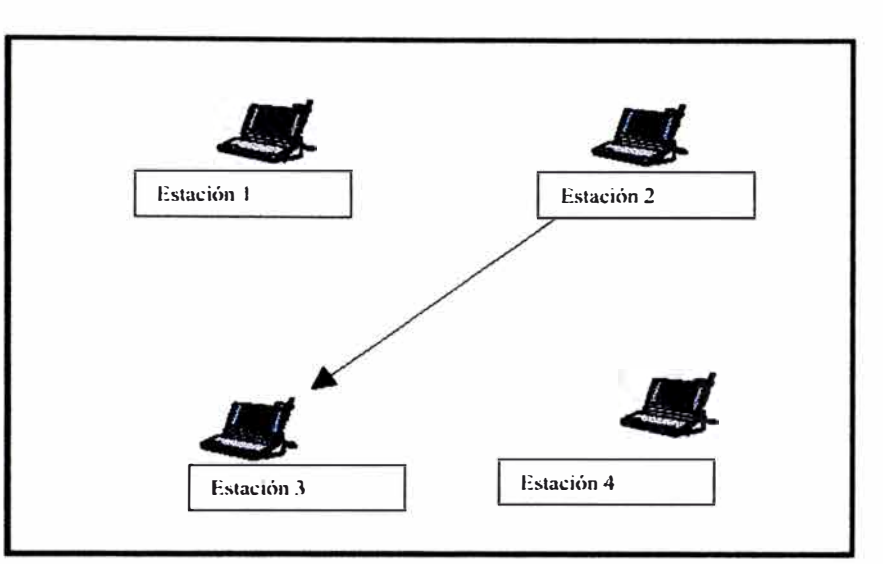


Figura 2.2: Red de propósito específico (Ad-hoc)

Descripción general del funcionamiento de la modalidad ad hoc:

Después de explicar el funcionamiento básico de la modalidad de infraestructura, del modo ad hoc se puede decir que no tiene punto de acceso. En esta red sólo hay dispositivos inalámbricos presentes. Muchas de las operaciones que controlaba el punto de acceso, como la señalización y la sincronización, son controladas por una estación. La red ad hoc no disfruta todavía de algunos avances como retransmitir tramas entre dos estaciones que no se oyen mutuamente.

2.5 Estándares actuales para WLAN

Existen dos estándares para redes inalámbricas. Uno es el estándar IEEE 802.11 [IEEE 802.11, 1998], y el segundo es el HIPERLAN (High Performance European Radio LAN por sus siglas en inglés) el cual fue propuesto por el Instituto Europeo de Estándares en Telecomunicaciones (ETSI por sus siglas en inglés) [HIPERLAN, 1995]. Ambos estándares limitan su trabajo a la capa física y a la subcapa MAC. También, los dos estándares emplean esquemas de acceso aleatorios, debido a las ventajas que representa sobre los protocolos fijos o sobre aquellos en función de la demanda. Los accesos aleatorios permiten la movilidad de una estación dentro y fuera del radio de la celda. Sin embargo, el precio para este comportamiento no determinístico tiene sus consecuencias para garantizar una QoS.

HIPERLAN es totalmente opuesto al estándar IEEE 802.11. Este estándar fue diseñado por un comité de investigadores dentro del ETSI, sin la fuerte influencia de los fabricantes de equipo y vendedores y es considerablemente diferente a los productos existentes. El estándar es bastante simple, y a la fecha sólo se están esperando productos que salgan al mercado [Pahlavan et al., 1997; LaMaire et al., 1996].

Existen diferencias considerables entre ambos estándares. Mientras que HIPERLAN puede soportar servicios limitados en tiempo asignando prioridad de acceso al canal dinámicamente, el IEEE 802.11 soporta este servicio también, pero utilizando un punto de coordinación para garantizar una parte fija de los recursos de la red. Otra de las diferencias es la frecuencia a la que trabajan ambos estándares. Mientras que HIPERLAN trabaja en las frecuencias de los 5.15 - 5.30GHz y 17.1

17.2GHz, el IEEE emplea la frecuencia de los 2.4GHz [LaMaire et al., 1996]. HIPERLAN transmite a una velocidad de 23.529Mbps, mientras que el IEEE 802.11 a 2Mbps [IEEE 802.11, 1998]. El protocolo utilizado por HIPERLAN es una variante de CSMA/CA basado en el tiempo de vida y la prioridad para el tiempo del paquete, y las retransmisiones en el nivel de la subcapa MAC [Wolisz et al., 1996]. El protocolo incluye una encriptación opcional y ahorro de energía. Otra característica de HIPERLAN aparte de la alta velocidad, es el enrutamiento de redes de tipo específico: si el destino está fuera de alcance, nodos intermedios darán la ruta óptima dentro de la red HIPERLAN. HIPERLAN es totalmente de tipo específico, no necesitando así un controlador central, como su contraparte IEEE 802.11.

2.6 Servicios de las WLAN

Como se ha visto, la necesidad de una red local inalámbrica no se basa en la búsqueda de la mejora del ancho de banda, o de la fiabilidad o eficiencia dentro de las comunicaciones, sino única y exclusivamente en la comodidad para el usuario final (y en el caso de los trabajadores, en el aumento de su productividad) y en hacer más sencillo tanto su despliegue como su crecimiento posterior. Como siempre, la aplicabilidad depende de cada caso concreto: no hace falta una red inalámbrica para unir dos o tres PC para jugar en línea (o sí, si están en lugares separados de la casa), pero existen entornos concretos que se ven muy favorecidos por esta tecnología.

- **Entornos corporativos**: Los empleados pueden beneficiarse de una conexión móvil en la red para consultar el correo o compartir ficheros sin que importe

su ubicación. Se tiene acceso total tanto durante una reunión como en la cafetería (¿por qué no?).

- **Educación**: Los estudiantes y los profesores pueden sacar provecho a un nivel parecido a los entornos corporativos, pero en el ámbito del campus y a la hora de impartir la docencia, o en la biblioteca. Permite tener una red dentro de escuelas, en edificios posiblemente antiguos, sin necesidad de recablear o fijar los ordenadores a ubicaciones concretas.
- **Finanzas**: Información económica en tiempo real en la bolsa simplemente conectando el portátil. Los equipos de auditoria pueden compartir información con un tiempo mínimo de overhead administrativo.
- **Salud**: Es parecido al anterior, pero con información sobre pacientes. Hay una necesidad menor de reproducir información sobre papel, al poder acceder a todo su conjunto en línea desde cualquier lugar.
- **Almacenes y manufacturas**: Significa mayor facilidad para mantener inventarios directamente en línea, sin tener que fijar el punto de entrada de la información en un lugar fijo o tener que pasar cables por superficies grandes y no siempre suficientemente bien adaptadas.

De todos modos, por el tipo de aplicaciones descritas se hace evidente que una red inalámbrica no es el único factor indispensable para conseguir sus ventajas; también es necesario que las herramientas de trabajo sean móviles: portátiles o PDA. Ahora bien, mediante esta tecnología puede darse un valor añadido a estos dispositivos.

En un estudio relativamente reciente realizado por la empresa Cisco Systems (Wireless LAN benefits study) se analizan los puntos mencionados anteriormente una vez llevados a la práctica, no sólo como posibles ventajas teóricas. En general, donde se ha producido mayor implantación de la tecnología de redes locales inalámbricas actualmente es en la educación y la salud (Figura 2.3). Además, dentro de este estudio se analizan cuáles son las principales utilidades de la red en el entorno implantado y se llega a la conclusión de que el aspecto mejor valorado no es tanto la facilidad de tareas administrativas o el hecho de compartir contenidos, sino la mera posibilidad de tener acceso a la red a cualquier hora desde cualquier lugar en el entorno de trabajo, para poder acceder al correo electrónico o Internet (Figura 2.4).

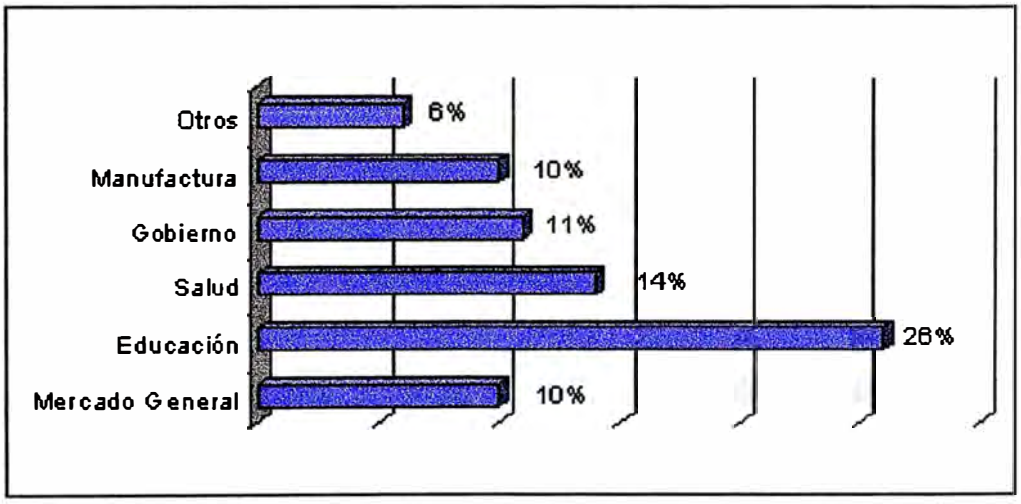


Figura 2.3: Penetración del mercado de WLAN por sectores

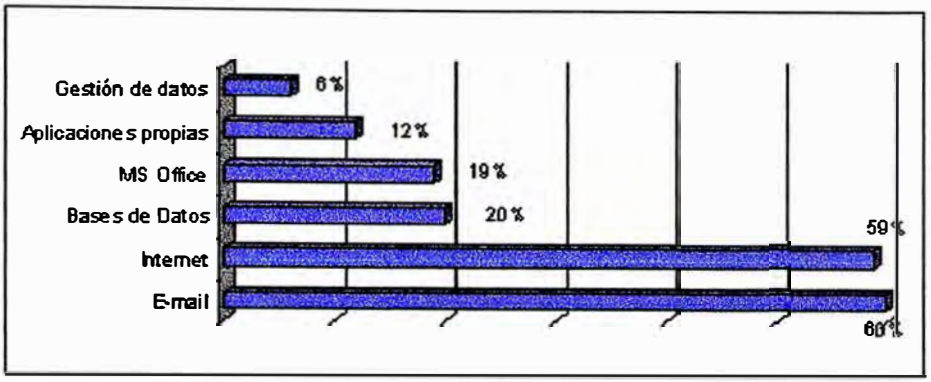


Figura 2.4: Aplicaciones clave en las WLAN

Todo gira siempre alrededor de lo mismo: comodidad, facilidad de uso y menor necesidad de overhead administrativo para obtener disponibilidad de acceso a la red (y, por lo tanto, más eficiencia e, incluso, según los estudios, calidad de vida). Aunque inicialmente la inversión necesaria es superior a una LAN cableada, a la larga, y midiendo el ciclo de vida completo de la red, también resulta más económica.

El uso de LANs inalámbricas genera aumentos en productividad. Cisco Systems anunció los resultados de un estudio independiente realizado por NOP World-Technology, el primero en confirmar los aumentos que se obtienen en productividad en las organizaciones que utilizan tecnología LAN inalámbrica.

El estudio, titulado "Estudio de los beneficios de las LANs inalámbricas", muestra mejoras en la productividad de los empleados, ahorros en costos y otros beneficios obtenidos por los usuarios finales y administradores IT de redes, en más de 300 organizaciones basadas en Estados Unidos con 100 o más empleados que

utilizan LANs inalámbricas. Uno de los resultados más significativos revelado por los clientes finales es que al utilizar LANs inalámbricas, pueden estar conectados una y hasta tres cuartos de hora más cada día, obteniendo un ahorro de 70 minutos promedio por usuario y aumentando su productividad en un 22%.

"Las condiciones económicas actuales han hecho que la productividad y la rentabilidad sean las nuevas claves para el éxito en los negocios," dijo Charles Giancarlo, Vicepresidente Senior de Cisco Systems. "La conectividad inalámbrica ha sido vista como una de las tecnologías que prometen un mayor impacto en productividad, pero hasta el momento no había estudios formales que confirmaran los beneficios de las LANs inalámbricas. Los resultados de esta investigación muestran que las LANs inalámbricas pueden tener un impacto directo en la productividad, y que los beneficios son aún más importantes de lo que se pensó".

Los encuestados para el estudio NOP World, estimaron que la conectividad inalámbrica tiene un impacto grande en el retorno de la inversión (ROI), con un ahorro para las organizaciones de $164.000 dólares anuales en costos de cableado, más de 3.5 veces lo que anticipó el equipo de IT. Estos ahorros no incluyeron los beneficios financieros de una mejora en productividad, que puede incrementar en una organización el retorno de la inversión en las LANs inalámbricas por cientos o millones de dólares más.

El ROI anual estimado por empleado fue de US $7.550 dólares, a través de una combinación de ahorro en costos y ganancias en productividad. Ben Rogers, Gerente del estudio NOP World-Technology, dijo que "las ganancias

en la eficiencia por empleado, de US $7.000 dólares por usuario por año, demuestra las posibles mejoras en la productividad a través del uso de LANs inalámbricas. Considerando un nivel de compañía general, las mejoras en la productividad fueron de US $6.3 millones de dólares anuales para las organizaciones participantes en el estudio. En la medida en que las LANs inalámbricas se implementan en las organizaciones, las ganancias en productividad pueden incrementarse aún más".

Otro beneficio de utilizar LANs inalámbricas, revelado por el estudio, fue una mayor efectividad en las tareas diarias. Cerca de dos tercios de usuarios finales encuestados respondieron que su efectividad se mejoró. La ganancia promedio en efectividad de aquellos que sintieron que hubo un incremento, fue del 38%. Para quienes respondieron por parte de organizaciones de salud, un 51% sintió que el incremento en la efectividad fue significativo. El hecho de "cualquier día, en cualquier lugar" de las comunicaciones inalámbricas permite acceso incrementado para corregir la información cuando más se necesita. En el ámbito de la salud, esta podría ser la diferencia entre vida o la muerte.

Además de las ganancias en los negocios, el 87% de los encuestados estuvieron de acuerdo en que hay un impacto positivo en su calidad de vida, ya que las LANs inalámbricas incrementan la flexibilidad, la productividad y ahorran tiempo. Los empleados que tienen una conexión LAN inalámbrica pueden obtener resultados en menor tiempo, trabajando por lo general desde locaciones fuera de sus oficinas, logrando un tipo de trabajo y de vida balanceada e incrementando la satisfacción, lo que permite una mayor lealtad y retención de los empleados. El estudio fue liderado por el Cisco Thought Leadership Network (TLN), que se

dedica a entregar investigaciones e ideas innovadoras sobre cómo pueden las compañías triunfar en la economía de Internet. TLN trabaja directamente con líderes fuera de Cisco para entender el mercado en evolución y desarrollar modelos y marcos para aumentar las tendencias emergentes. Entre sus programas, el TLN publica mensualmente investigaciones, estudios y presentaciones en conjunto con el newsletter IQ de John Chambers, subrayando el pensamiento de líderes, conceptos, e investigaciones que TLN patrocina.

2.7 Requerimientos del protocolo MAC en LANs inalámbricas

Teóricamente, las redes inalámbricas deberían de proveer los mismos servicios y capacidades que se tienen en las redes alámbricas, sin embargo, esto no ocurre. Esto se debe a la naturaleza del medio inalámbrico, el cual es muy diferente al cable de cobre o la fibra óptica. Así, muchas de las funciones que se implementan fácilmente en un medio alámbrico, no son tan fáciles o no son posibles de implementar en un medio inalámbrico. Estas diferencias hacen que el diseño de los protocolos MAC para redes inalámbricas sea una tarea muy complicada. Aquí se discutirán algunas cuestiones de ese tipo.

2.7.1 Confiabilidad.

El medio inalámbrico tiene que ser tan confiable como el sistema alámbrico. Los errores no se pueden prevenir totalmente. El aire es uno de los medios menos

confiables, dependiendo principalmente del ambiente donde está operando. Pueden existir interferencias de otras fuentes eléctricas o electrónicas, y se deben de tomar precauciones en ello para que el nivel de errores sea bajo. Esta es una tarea difícil de lograr puesto que los sistemas inalámbricos emplean relaciones señal-ruido más pequeña que los sistemas alámbricos.

2.7.2 Transparencia.

Dado que las redes inalámbricas no reemplazarán a las redes alámbricas, tendrán que compartir el mismo ambiente. De tal manera que el software tendrá que ser compatible para ambos casos. El modelo OSI contempla que sólo las dos primeras capas serán diferentes. Existen interfaces que son totalmente transparentes al usuario.

2.7.3 Caudal eficaz

Dado que el espectro es un recurso escaso, el caudal eficaz es una de las consideraciones más críticas en el protocolo MAC. Las redes inalámbricas deberían de ser capaces de transmitir a las mismas velocidades que las redes alámbricas. Dichas velocidades están aún demasiado lejos de las posibilidades tecnológicas para los medios inalámbricos. Por ejemplo, las terminales interactivas, donde la movilidad es un objetivo, pueden trabajar adecuadamente en el intervalo de los 64Kbps (texto), y hasta 20Mbps para aplicaciones gráficas [Chen, 1994].

2.7.4 Seguridad

La encriptación de la información es necesaria en medios inalámbricos. Para evitar degradar el desempeño de la red, esto puede efectuarse en el hardware utilizando códigos de encriptación, o por el mismo método de transmisión (empleando técnicas de espectro esparcido, por ejemplo). Si no se tiene un control de seguridad, se podrían tener accesos no deseados en la red [Chen, 1994].

No todo podía ser perfecto. Una de las preocupaciones principales en cuanto a la utilización de redes locales inalámbricas recae en la seguridad de la información que viaja por la red y los equipos que forman parte de ella. En un medio cableado, para poder acceder a las transmisiones es necesario "pinchar" el cable o bien encontrar un punto de conexión para que el atacante pueda entrar a la red y formar parte de ella. Esta opción no es sencilla (a menos que el ataque lo lleve a cabo alguien desde dentro, claro). Dentro de una red local cableada existen mecanismos para poder evitar escuchas no autorizadas incluso por parte de sus propios integrantes (por ejemplo, con la utilización de switches, conmutadores), pero en una red inalámbrica, las comunicaciones viajan por el aire y, por lo tanto, todo el mundo dentro del área de alcance de la red puede escucharlas. Por este motivo, el uso de mecanismos criptográficos es algo más que opcional e, incluso así, no puede evitarse la captura del tráfico de datos, aunque sea encriptado.

El problema principal, sin embargo, no se encuentra sólo en la escucha de las comunicaciones de terceros y la consiguiente obtención de información útil, sino

también en la accesibilidad a las máquinas que forman parte de la red por parte de los intrusos. El cable obliga a las comunicaciones de la red a pasar por un camino predeterminado, sobre el que pueden aplicarse medidas concretas (como la aplicación de firewalls, cortafuegos), pero en el entorno inalámbrico, cualquier persona puede acceder a cualquier otra máquina de la red desde cualquier lugar, incluyendo a los intrusos. Ello posibilita lo que se denomina "ataque del aparcamiento" (parking lot attack): conceptualmente, el intruso se sienta en el aparcamiento de la empresa (fuera del edificio, pero dentro del alcance de la red) y ataca a las máquinas desde allí (Figura 2.5). Si el peso de la seguridad de la red se ha delegado en el firewall, y entonces es más laxa en el resto de máquinas, ello puede provocar que, de hecho, todavía sea más fácil entrar en las máquinas internas.

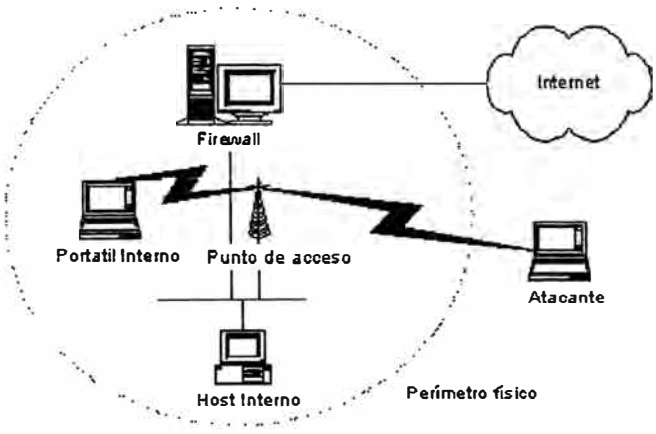


Figura 2.5: Ataque del aparcamiento

El estándar 802.11, que gobierna la especificación de redes inalámbricas, contempla este hecho y establece mecanismos para encriptar la información y autenticar los componentes de la red mediante el protocolo WEP (Wired Equivalent Protocol), basado en la distribución de claves criptográficas. Por desgracia, existen

indicios claros de que se trata de un sistema que se puede llegar a romper y, por lo tanto, es inseguro, y el propio estándar no va mucho más allá en temas de seguridad, ya que deja en manos de las compañías la tarea de implementar sus propios mecanismos de seguridad, lo que puede llegar a provocar que diferentes sistemas no sean interoperables, como efecto secundario. Toda una contradicción teniendo en cuenta que ello viene dado por la decisión de un comité de estandarización. Actualmente ya hay herramientas de libre distribución que permiten descifrar las claves WEP únicamente basándose en la cantidad de información capturada en la red, no en el poder computacional del asaltante.

Una de las debilidades principales del mecanismo básico de seguridad es su naturaleza estática: una vez se configura una clave para una red, no cambia nunca, lo que significa que cuando se consigue romper, ya puede accederse libremente a la red para siempre (a menos que la intrusión sea detectada y se cambie la clave, lo que implica únicamente que el intruso tendrá que volver a empezar de cero). Esta distribución de claves se hace de forma estática, y esto significa que mantener una red segura puede suponer una carga administrativa adicional importante. Un punto hacia la solución recae en el uso de claves dinámicas que cambien automáticamente.

La conclusión a la que se llega es que si bien una red local inalámbrica facilita tareas administrativas y de infraestructura, también implica un conjunto de premisas que hay que considerar muy seriamente desde el punto de vista de la seguridad durante su concepción, por lo que se tendrá que estudiar a fondo qué recursos adicionales ofrece cada fabricante sobre este tema y sus implicaciones.

Tomarse a la ligera estos hechos puede facilitar el acceso de intrusos dentro de la red local.

Otro aspecto que últimamente está en boca de los medios de comunicación no es la seguridad de las comunicaciones o la red en sí, sino la seguridad de sus usuarios desde el punto de vista de las emisiones de radiaciones en el entorno. Las emisiones de los dispositivos de redes locales inalámbricas son, de hecho, muy inferiores con respecto a las de los propios teléfonos móviles, y su tipo de radiación se degrada muy rápidamente con la distancia (dada su área de alcance relativamente limitada). Sin embargo, todos los equipos tienen que pasar los requisitos de seguridad impuestos por las regulaciones de la industria. En este aspecto todavía no se ha atribuido nunca ningún efecto adverso a una red local inalámbrica.

2.7.5 Movilidad

La aplicación primaria de las redes inalámbricas es para servir a usuarios móviles. Sin embargo, tal movilidad puede ser muy dinámica, ocurriendo en pocos milisegundos. El protocolo debe permitir dicha movilidad [Chen, 1994].

Cuando un usuario o una estación se desplazan de un punto de acceso a otro punto de acceso, se debe mantener una asociación entre la tarjeta NIC y un punto de acceso para poder mantener la conectividad de la red. Esto puede plantear un problema especialmente complicado si la red es grande y el usuario debe cruzar límites de subredes o dominios de control administrativo. Si el usuario cruza un límite de subred, la dirección IP asignada originalmente a la estación puede dejar de

ser adecuada para la nueva subred. Si la transición supone cruzar dominios administrativos, es posible que la estación ya no tenga permiso de acceso a la red en el nuevo dominio basándose en sus credenciales.

Más allá del simple desplazamiento dentro de un campus corporativo, otros escenarios de usuarios móviles son muy reales. Los aeropuertos y restaurantes agregan conectividad inalámbrica con Internet y las redes inalámbricas se convierten en soluciones de red populares para el hogar.

Ahora es más probable que el usuario pueda abandonar la oficina para reunirse con alguien de otra compañía que también disponga de una red inalámbrica compatible. De camino a esta reunión, el usuario necesita recuperar archivos desde la oficina principal y podría encontrarse en una estación de tren, un restaurante o un aeropuerto con acceso inalámbrico. Para este usuario sería de mucha utilidad poder autenticarse y utilizar esta conexión para obtener acceso a la red de la empresa. Cuando el usuario llegue a su destino, puede que no tenga permiso de acceso a la red local de la empresa que va a visitar. Sin embargo, sería fortuito que el usuario pudiera obtener acceso a Internet en este entorno extraño. Entonces, dicho acceso podría utilizarse para crear una conexión de red privada virtual con la red de su empresa. Después, el usuario podría irse a casa y desear conectarse a la red doméstica para descargar o imprimir archivos para trabajar esa tarde. Ahora, el usuario se ha desplazado a una nueva red inalámbrica, que posiblemente incluso puede ser de la modalidad ad hoc.

Para este ejemplo, la movilidad es una situación que debe pensarse muy detenidamente. La configuración puede ser un problema para el usuario móvil, ya que las distintas configuraciones de red pueden suponer un reto si la estación inalámbrica del usuario no tiene capacidad para configurarse automáticamente.

2.7.6 Consumo de energía (batería)

Dado que el servicio primordial de las redes inalámbricas es dar servicio a usuarios móviles y la fuente de alimentación para dichos usuarios típicamente es por medio de una batería, la utilización eficiente de la transmisión y recepción es otra importante consideración para el protocolo MAC. La recepción puede consumir más energía que la transmisión, dado que las señales modernas de comunicación digital necesitan una potencia de alrededor de 100mW, y considerando que el tiempo de recepción es mucho mayor que el de transmisión, pero necesita de 100 mA para soportar el proceso de la señal digital en el receptor. Si no se tiene el ahorro de energía, el receptor tiene que mantenerse escuchando el canal todo el tiempo y decodificar cada paquete recibido [Chen, 1994].

2.7.7 Retraso

El retraso de los paquetes es una característica importante para todas las aplicaciones, pero especialmente para los servicios limitados en tiempo y aplicaciones multimedia, tales como voz y video [Chen, 1994].

2.7.8 Acceso equitativo

El desvanecimiento del canal puede causar una recepción de potencia diferente a la normal. Tal situación puede resultar en un acceso no equitativo hacia la red [Chen, 1994]. Esto es, que una estación puede recibir mucho menos potencia en la señal que otro usuario. Cuando el protocolo está operando en el período de contienda, la estación que tenga poca señal de recepción estará en desventaja de accesar al medio. El protocolo MAC deberá de poder resolver esta situación dado que la captura se puede realizar con potencias tan pequeñas que pueden tener una diferencia de hasta 9dB [Chen, 1994].

2.7.9 Detección de colisiones

Las terminales móviles en las redes inalámbricas, no tienen la capacidad de sensar el medio mientras mandan su información, dado que tienen solamente una antena para transmitir y recibir. Por consiguiente, existirá un tiempo en el cual se cambiará del medio de emisor al de receptor. Esto hace que la detección de colisiones sea más difícil, ya que se necesita estar monitoreando el medio continuamente, otro problema que se tiene en la detección de colisiones es aquel causado por el "problema de terminal oculta".

2.7.10 Terminal oculta

Un par de terminales en la misma red pueden no escucharse entre ellas, esto puede ocasionar que si una está transmitiendo, la otra sense el medio libre e inicie la transmisión, repercutiendo esto en colisiones [Hadzi-Velkov y Gavrilovska, 1999].

2.7.11 Transferencia entre celda

La función que permite a los nodos móviles comunicarse con el punto de acceso en una celda, y poder cambiar a otro punto de acceso en otra celda, es llamado "handoff" o "handover". El propósito de esto, es mantener el servicio para los nodos móviles a través de diferentes celdas [Chen, 1994].

Se utilizan los términos handoff y handover en el idioma inglés debido a que en esta área de las telecomunicaciones no existe una traducción literal al español que indique su significado en forma precisa.

2.8 El futuro de la WLAN

Según las estimaciones de Venture Development, el mercado estadounidense de redes inalámbricas crecerá desde los 706 millones de dólares de 2001 hasta los 1.716 millones de 2004, con un crecimiento anual en torno al 40%. La predicción de Info Tech para el mercado mundial de redes inalámbricas es de 4,200 millones de dólares en 2005. Ver Figura 2.6.

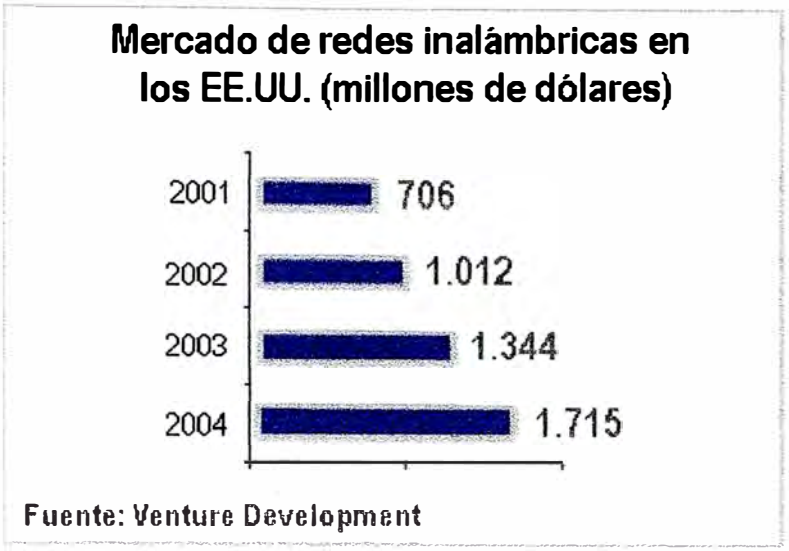


Figura 2.6: Proyección de inversiones

Poco a poco, el IEEE pone en marcha nuevas iniciativas sobre sus diferentes aspectos. El número de iniciativas que están en funcionamiento actualmente indica el esfuerzo que se le está dedicando y la apuesta importante que se lleva a cabo sobre ellas. Algunos de los aspectos sobre los cuales se está trabajando incluyen:

- Calidad de servicio
- Operación de bridges (puentes)
- Interoperabilidad entre puntos de acceso
- Extensiones a mayores anchos de banda
- Mejoras de seguridad

Aparte de las necesarias mejoras en cuanto a la seguridad, uno de los puntos más esperados es el estándar sobre calidad de servicio (QoS), que será el 802.11e, de carácter esencial para aplicaciones multimedia (como la videoconferencia o el vídeo bajo demanda).

Como se ha mencionado, el estándar 802.11b es el más extendido en la actualidad; sin embargo, existe otro problema importante aparte de la seguridad: la banda de frecuencias en las que se mueve se está saturando lentamente y su velocidad no es muy elevada (lo equivalente a una ethernet a 10Mbps que opera sobre un hub). De momento ya actúa en la misma frecuencia que los hornos microondas y los teléfonos inalámbricos (por lo que estos aparatos pueden afectar al funcionamiento de una WLAN 802.11b) y dentro de poco parece que empezará el auge de las redes WPAN (Wireless Personal Area Networks) para comunicaciones a corta distancia, que se mueven en el mismo espectro. Dado que el medio de transmisión es el aire, no existe tampoco la posibilidad de que un dispositivo adicional distribuya mejor el ancho de banda, como un switch ethernet. Por lo tanto, puede llegar el caso de que la red inalámbrica muera de éxito y quede totalmente saturada, de forma que se relegue su aplicación a situaciones en las que no se tenga más remedio que hacerlo.

Para solucionar estas problemáticas está disponible el estándar 802.11a, con la apariencia de Tierra Prometida, moviéndose en una banda todavía sin saturación y a mayores velocidades. Evidentemente, tampoco está exento de problemas, ya que su banda no es libre en todo el mundo: en Japón cuenta con la mitad del ancho de banda y en Europa está restringida, aunque el IEEE está trabajando para poder adaptarlo. A un nivel práctico todavía tiene que verse qué sucederá, ya que actualmente el 802.11b está mucho más implantado y es difícil que las empresas sencillamente tiren su inversión en la red por un producto totalmente nuevo, con menos apoyo y más caro. Todas las miradas están puestas en aquellos productos que permitan la

adaptación entre los dos estándares, pero si realmente llega el punto en el que la banda de 2.4GHz queda totalmente saturada, no habrá mucho que pensar.

De momento quizás aún es pronto para hacer el gran cambio, aunque este año parece que es clave para ver si la WLAN llegará a un nuevo peldaño con el progresivo paso al estándar 802.11a o si se quedará anclada en el 802.11b, que todavía funciona muy bien. La clave estará seguramente en la aparición de componentes que permitan el uso dual de las dos tecnologías, de la misma forma que en la ethernet las redes a 100Mbps no empezaron a despegar hasta la aparición de componentes 10/100. En medio de todo ello surge un nuevo estándar para WLAN, el 802.11g, que ofrece compatibilidad con el 802.11b, pero altas velocidades como el 802.11a. De todos modos, actualmente sólo es una especificación sobre papel; cuando exista sobre silicio se verá qué puede ofrecer.

Pase lo que pase, lo que resulta evidente es que las redes locales inalámbricas continuarán en auge en los mercados que pueden beneficiarse enormemente de ellas. Si así sucede, será indispensable incluirlas dentro de los programas de formación en tecnología de redes, de igual modo que en la actualidad todo gira alrededor de la ethernet como punto de partida de una red local. Si realmente se convertirán en un punto de referencia, sólo el tiempo lo dirá.

CAPÍTULO III

ARQUITECTURA DEL ESTANDAR IEEE 802.11

3.1 Capa física

El estándar 802.11 que trata sobre las técnicas de acceso al medio bosqueja tres diferentes capas posibles que se utilizarán: Infrarrojo (IR por sus siglas en inglés), Secuencia Directa mediante Espectro Esparcido (DSSS por sus siglas en inglés) y Saltos en Frecuencia mediante Espectro Esparcido (FHSS por sus siglas en inglés). En la siguiente sección se describen brevemente las tres diferentes capas físicas mencionadas.

3.1.1 Infrarrojo (IR):

Para transmitir en infrarrojo, se emplean longitudes de onda de 850 nm a 950 nm, similar a su utilización en enlaces de fibra óptica, los sistemas IR detectan solo la amplitud de la señal, reduciendo así grandemente la interferencia. Estos sistemas no están limitados en su ancho de banda. Por lo tanto, se puede transmitir a muy altas velocidades, a diferencia de otros sistemas. Dado que opera en el espectro de luz no se requiere licencia de uso de la FCC en Estados Unidos [IEEE 802.11, 1998]. Existen dos formas de implementar un sistema con este tipo de transmisión:

- Tener una línea de vista, con una buena distancia de transmisión (algunos kilómetros), ofreciendo gran ancho de banda y altas velocidades.
- Esparcir la señal en todas direcciones, reduciendo la cobertura a 1 o 2 metros.

3.1.2 Secuencia Directa mediante Espectro Esparcido (DSSS)

El proceso de DSSS se realiza multiplicando una portadora de Radio Frecuencia (RF por sus siglas en inglés) y una señal digital (pseudo-ruido (PN por sus siglas en inglés)). Primero el código del PN se modula sobre la señal de información apoyándose en alguna técnica de modulación (BPSK, QPSK, etc.), después se multiplica la portadora de RF con la señal de información modulada PN. Las señales generadas aparecen como ruido en el dominio de la frecuencia. El ancho de banda que tiene dicha señal permite que la potencia caiga por debajo del umbral de ruido sin la pérdida de información. Para este propósito se emplean secuencias de código binario tan pequeñas como 11 bits o tan grandes como $[2*10^{89} - 1]$ bits, teniendo tasas de transmisión desde un bit por segundo hasta cientos de megabits por segundo.

En DSSS, la energía de RF es esparcida a través de todo el ancho de banda sustituyendo cada bit de datos por múltiples sub bits, llamados chips que ocupan el mismo intervalo de tiempo. La longitud de la secuencia de chips se conoce como ganancia de procesamiento. En Estados Unidos y Europa, DSSS opera en el intervalo de frecuencias de 2.4GHz a 2.4835GHz. En Japón, opera en el intervalo de frecuencias de 2.471GHz a 2.497GHz. La velocidad de 1Mbps es codificada

utilizando DBPSK (differential binary phase shift keying). El 0 se codifica con fase 0 y el 1 se codifica con fase π. La velocidad de 2Mbps se logra empleando codificación DQPSK (differential quadrature phase shift keying). Los símbolos 00, 01, 10, 11 son codificados en 0, $\pi/2$, π, $3\pi/2$ respectivamente [Taylor *et al.*, 1991; Viterbi, 1995].

3.1.3 Saltos en Frecuencia mediante Espectro Esparcido (FHSS):

En sistemas de FHSS, los saltos del radiotransmisor a partir de una frecuencia portadora a otra, es un modelo específico que parece ser al azar. La interferencia se limita, acotando el tiempo que se tiene en cada frecuencia, disminuyendo así la posibilidad de que dos transmisores intenten utilizar la misma frecuencia al mismo tiempo. FHSS trabaja en la banda de los 2.4GHz (banda Industrial, científica y médica por sus siglas en inglés ISM). En Estados Unidos y Europa. Se tienen 79 canales en el grupo de saltos. El primer canal está centrado en 2.402GHz y los canales subsecuentes están espaciados 1MHz, dichos saltos de frecuencia no deben de estar demasiado tiempo en cualquiera de los canales. En Japón, el espectro se divide en 23 canales, en donde el primer canal está centrado en 2.473GHz y todos los canales subsecuentes están separados a 1MHz. La razón mínima de salto permitida es 2.5 saltos por segundo. El acceso básico de 1 Mbps utiliza dos niveles GFSK (gaussian frequency shift keying). Para el acceso a 2Mbps, se emplean 4 niveles de GSFK además de limitar la interferencia de fuentes externas, esta tecnología puede ayudar a evitar que dos redes instaladas en el mismo edificio interfieran entre ellas. En muchos casos, todos los puntos de acceso en una LAN se programan con el mismo código de salto de frecuencia. Cuando un solo código no puede manejar a

todos los usuarios, una solución es dividir la red en varias más pequeñas, cada uno con su propio código. Con los sistemas de secuencia directa, los códigos son diseñados para ser mutuamente ortogonales, de tal manera que las transmisiones de una red aparezcan como ruido en las otras y reduciendo al mínimo la interferencia de la red [Taylor *et a*l., 1991; Viterbi, 1995; IEEE 802.11, 1998].

3.2 Subcapa de Control de Acceso al Medio (MAC)

La parte MAC del protocolo 802.11, define un mecanismo de acceso llamado DFWMAC (MAC inalámbrica con Fundación Distribuida, por sus siglas en inglés). DFWMAC incorpora un método básico de acceso distribuido y un método de acceso centralizado opcional. Estos dos métodos de acceso pueden coexistir, y de hecho el método de acceso distribuido forma la base para el método centralizado. Estos dos métodos (o "coordinación de funciones") se utilizan para soportar dos tipos de tráfico: asíncrono y limitado en tiempo [IEEE 802.11, 1998].

3.2.1 Funciones distribuidas y puntos de coordinación.

Una función de coordinación en una LAN inalámbrica es un mecanismo que determina cuando una estación en particular puede transmitir. Con una función de coordinación distribuida, esta determinación es responsabilidad de los nodos individualmente y puede dar lugar a transmisiones simultáneas múltiples, mientras una función de punto de coordinación centraliza esta decisión en cualquier momento dado y por lo tanto se asegura que solamente un solo nodo puede transmitir.

El método de acceso fundamental con DFWMAC es una función de coordinación distribuida conocida como Acceso Múltiple con Detección de Portadora Evitando Colisiones, o CSMA/CA. El empleo de este método de acceso es obligatorio para todos los puntos de acceso, y se utiliza dentro de las dos configuraciones mencionadas anteriormente, como son la de tipo específico y la de infraestructura [IEEE 802.11, 1998].

DFWMAC incorpora una función de punto de coordinación, implementada encima del protocolo básico de CSMA/CA. Como se muestra en la Figura 3.1, el PCF se estructura arriba del DCF basado en CSMA/CA, utilizando la prioridad de acceso proporcionadas por este esquema. Este método de acceso utiliza un punto de coordinación (típicamente el punto de acceso) para determinar cual estación tiene derecho de transmitir. La operación es esencialmente una encuesta del punto de coordinación.

El empleo de la función del punto de coordinación DFWMAC es opcional, y de hecho, requiere que la configuración de la red no permita traslapes de puntos coordinados en un Grupo de Servicio Básico (BSS por sus siglas en inglés) en el mismo canal. Un BSS que funcione bajo una Función de Coordinación Distribuida (DCF por sus siglas en inglés) puede traslaparse con otro BSS.

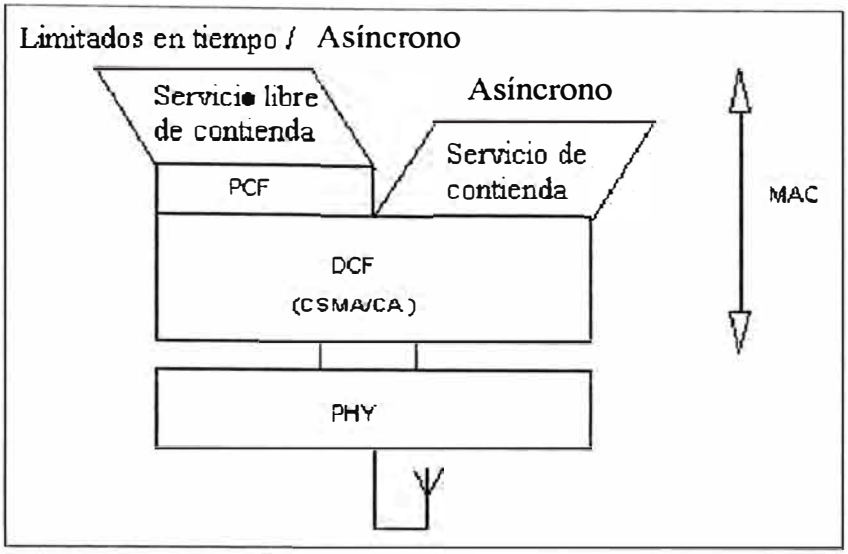


Figura 3.1: Modelo del servicio MAC

Los dos métodos de acceso están integrados en un concepto de supermarco, en el cual un inicio libre de contienda ocurre al iniciar el supermarco, seguido por un período de contienda. La Figura 3.2 muestra la estructura del supermarco [IEEE 802.11, 1998].

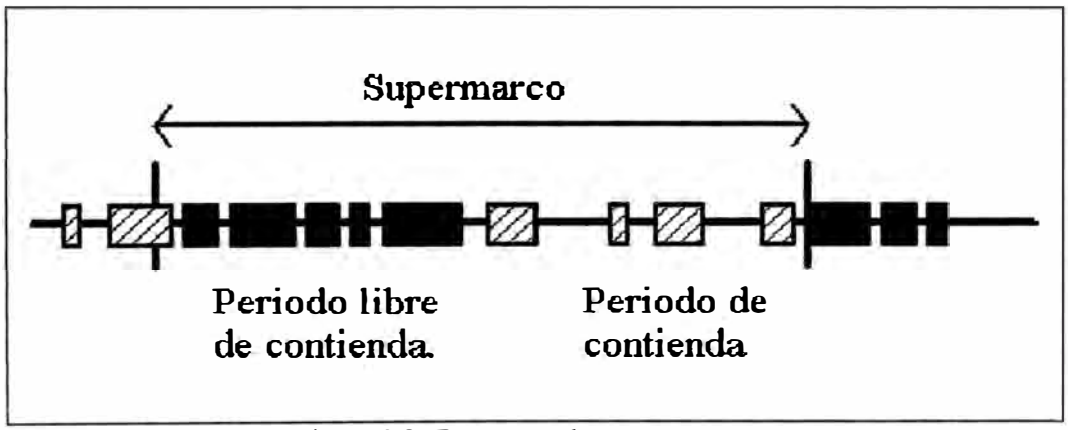


Figura 3.2: Estructura de un supermarco.

3.2.2 Función de Coordinación Distribuida (DCF)

La detección de colisiones no es posible en los medios inalámbricos, dado que las estaciones son incapaces de escuchar el canal para sensar el medio que no

tenga colisiones mientras transmite. Para superar este problema, el protocolo MAC evita las colisiones utilizando CSMA/CA. Cuando el medio está libre después de un período de estar ocupado, estaciones múltiples podrían estar esperando por el medio para iniciar su transmisión. El sensado de portadora se puede efectuar por mecanismos físicos o virtuales. El sensado de portadora físicamente detecta la actividad en el canal, observando la potencia de la señal de los otros usuarios. En el sensado de portadora virtual, la estación fuente establece la duración en un campo del encabezado del marco de datos, o se emplean marcos de control (RTS y CTS petición de envío / permiso para enviar, por sus siglas en inglés respectivamente). La duración del campo indica el período de tiempo después del marco actual, que el medio estará reservando para completar con éxito su transmisión y recibir el acuse de recibo. Al detectar las estaciones el campo de duración para la transmisión, estas ajustan su vector de asignación de red (NAV por sus siglas en inglés) el cual define el período de tiempo hasta que se completa la transmisión actual. El intervalo de tiempo entre marcos es llamado espacio entre marcos (IFS por sus siglas en inglés). Una estación determinará que el medio está inactivo a través de la función de sensado de portadora por el intervalo IFS especificado. Existen tres intervalos diferentes IFS para definir diferentes prioridades de acceso al medio inalámbrico; espacio entre marco corto (SIFS por sus siglas en inglés), espacio entre marco en la Función de Punto de Coordinación (PCF por sus siglas en inglés) (PIFS), y espacio entre marco en la Función de Coordinación Distribuida (DCF por sus siglas en inglés) (DIFS) [IEEE 802.11, 1998]. La descripción de los diferentes tiempos IFS se describen a continuación:

3.2.2.1 SIFS (Espacio entre marco corto)

El período SIFS se utiliza para acciones de respuesta inmediata. Por ejemplo: se envía un marco CTS en respuesta a un marco RTS recibido correctamente. Además, durante el período libre de contienda (CFP por sus siglas en inglés), el punto de coordinación PC esperará un período SIFS antes de mandar cualquier marco a las estaciones y las estaciones que estén bajo este esquema, responderán después de esperar un período SIFS [IEEE 802.11, 1998].

3.2.2.2 PIFS (Espacio entre marco en la Función de Punto de Coordinación)

El período PIFS es más grande que el período SIFS. El período PIFS se emplea solamente en PCF en el Punto de Acceso (AP por sus siglas en inglés) para ganar el acceso al medio al inicio del período libre de contienda (CFP) [IEEE 802.11, 1998].

3.2.2.3 DIFS (Espacio entre marco en la Función de Función Distribuida)

El período DIFS es más grande que el período PIFS. El período DIFS se utiliza en estaciones que operan bajo el esquema DCF para transmitir marcos de datos (MPDUs) y manejo de marcos (MMPDUs). Una estación que emplea el esquema DCF, y que desea iniciar la transmisión de un marco RTS, o marco de datos (sin la opción RTS/CTS), estará autorizado a transmitir si su mecanismo de sensado

de portadora determina que el medio estuvo ocioso por un período de tiempo DIFS [IEEE 802.11, 1998].

A continuación se hará una descripción del mecanismo de acceso básico:

Una estación antes de iniciar con su transmisión sensa el canal por un período para determinar si otra estación está transmitiendo. Si el medio se encuentra ocioso por un intervalo que excede el período DIFS, la estación iniciará un tiempo aleatorio para al final de éste, iniciar la transmisión. Las colisiones pueden ocurrir al final de este tiempo, en el caso de que dos estaciones tengan el mismo tiempo aleatorio de espera. Si antes de que termine el tiempo de espera para intentar iniciar la transmisión (backoff) de una estación, otra inició la transmisión, en el instante en que se detecte el canal ocupado, el tiempo de backoff se detiene, para cuando el medio se detecte libre nuevamente, la estación esperará por el tiempo de backoff restante de cuando este se detuvo, e iniciará su transmisión cuando este tiempo de backoff sea cero [IEEE 802.11, 1998].El método básico de acceso se ilustra a continuación en la Figura 3.3

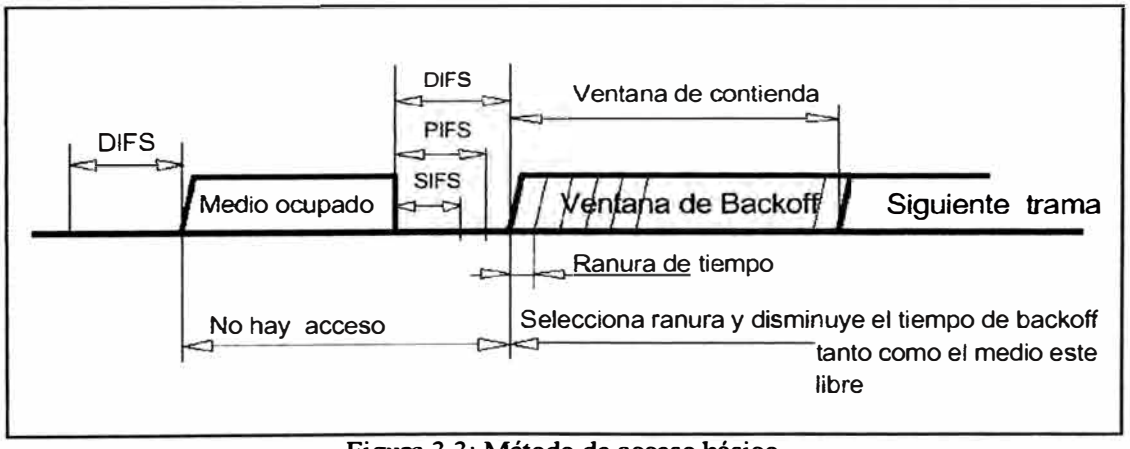


Figura 3.3: Método de acceso básico.

Puesto que una estación que está transmitiendo no puede escuchar su propia transmisión, cuando ocurre una colisión la estación transmisora continúa mandando la trama de datos hasta completarlo. Si la trama de datos es grande, entonces se desperdiciará bastante ancho de banda del canal por la trama corrupta. Los marcos de control RTS y CTS pueden ser empleados por una estación para reservar el ancho de banda antes de la transmisión de una trama de datos, con el propósito de minimizar el ancho de banda desperdiciado cuando una colisión ocurre. RTS y CTS son tramas de control relativamente pequeñas (RTS es de 20 octetos y CTS es de 14) comparados con la longitud máxima de una trama (2346 octetos). La estación que utiliza este mecanismo sigue el esquema de acceso básico para contender por el medio. La estación fuente manda un marco RTS después de que el canal a estado libre por el período DIFS. La estación destino responde al paquete RTS con un paquete CTS después de un período SIFS. Después de que el intercambio de paquetes RTS/CTS ha sucedido, ahora sí se pueden mandar los paquetes de datos. En dado caso que el marco CTS no se reciba dentro de un cierto intervalo de tiempo, el RTS se retransmite, siguiendo las reglas del tiempo aleatorio especificadas en el procedimiento de acceso básico. Los marcos RTS y CTS contienen un campo de duración que indica el período por el cual estará reservado el canal para la transmisión de información. Si una estación captura un paquete RTS y no es para ella, lee del campo de duración el período que el canal estará ocupado, y actualiza su vector de asignación de red a esta duración y se abstiene de mandar información en este tiempo. Lo mismo ocurre si solamente se recibe un paquete CTS por una estación que no le corresponda recibir este paquete, pero que si está dentro del BSS, actualizará su NAV. Una estación no está permitida a iniciar una transmisión si su

NAV no es cero. Esto garantiza que todas las estaciones dentro del intervalo de la fuente o destino tienen conocimiento acerca de la transmisión y su duración [IEEE 802.11, 1998].

Sin embargo, para una carga que no es muy grande, emplear RTS/CTS implica incrementar el retraso por el encabezado de estos. Por esta razón, el RTS/CTS se utiliza para paquetes de tamaño grande. En la Figura 3.4 se ilustra como trabaja el RTS/CTS [IEEE 802.11, 1998].

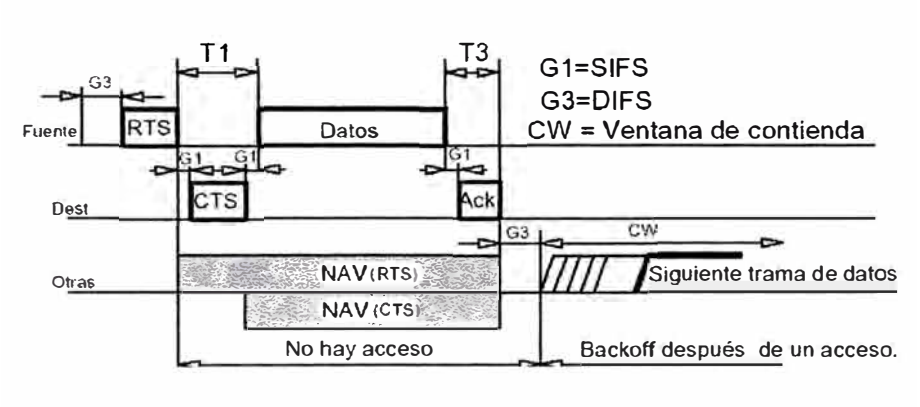


Figura 3.4 Diagrama del mecanismo de tiempo del empleo de RTS/CTS

El tiempo aleatorio de espera se selecciona de acuerdo a la siguiente ecuación:

Backoff Time = Random() * aSlotTime

Donde:

aSlotTime = al tiempo estimado en que el medio se encuentre libre más el tiempo que tarda el viaje completo de transmisión y recepción más el tiempo de propagación en el aire.

aSlotTime = Clear channel assessment time + RX-TX turnaround time + Air propagation time

y

Random() = entero pseudo aleatorio extraído de una distribución uniforme sobre el intervalo [0,CW], donde CW es un entero dentro del intervalo de los valores característicos de la capa física CWmin ≤ CW ≤ CWmax. Es importante la necesidad de una independencia estadística entre el flujo del número aleatorio entre estaciones [IEEE 802.11, 1998].

El parámetro de la ventana de contienda (CW) tomará un valor inicial CWmin. La CW se incrementa al doble cada vez que un intento de transmisión de una trama de datos fracasa, hasta que la CW alcanza el valor máximo. Una vez que ha sido alcanzado el valor máximo, se mantiene hasta que se reinicia nuevamente. Esto mejora la estabilidad del protocolo de acceso bajo condiciones de grandes cargas. La CW se reiniciará después de que cada intento por transmitir una trama de datos se logre con éxito. El grupo de valores de CW será ascendente en potencias de $(2^n) - 1$ iniciando con un CWmin y continuando hasta alcanzar un CWmax [IEEE 802.11, 1998], como se ilustra en la Figura 3.5

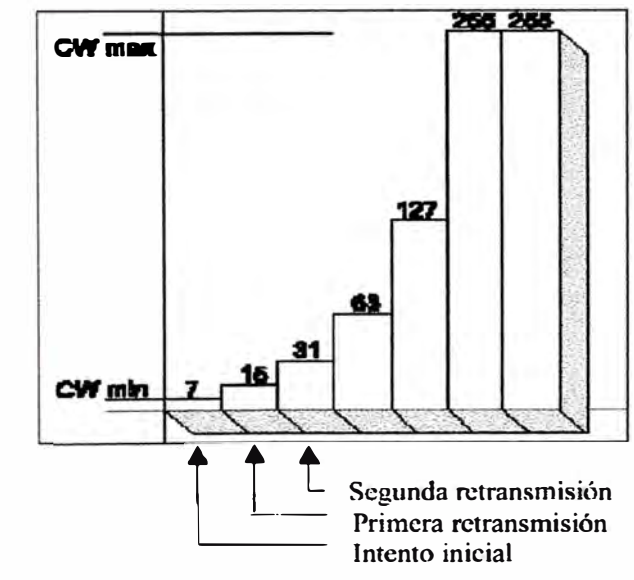


Figura 3.5: Incremento exponencial de CW

3.2.2.4 Servicio Asíncrono.

El servicio asíncrono ocurre en las configuraciones ad-hoc y de infraestructura, empleando CSMA/CA y funciones de puntos de coordinación. DFWMAC mejora la robustez de CSMA/CA para un tráfico asíncrono empleando un acuse de recibo del nivel MAC. La parte de CSMA/CA se diseña para compartir el medio de una manera espectralmente eficiente. El acuse de recibo del nivel MAC permite la detección de una trama perdida y su recuperación por la retransmisión en el nivel MAC. Esta es la manera en que el tráfico asíncrono se maneja dentro de una configuración pura de Función de Distribución Coordinado (DCF por sus siglas en inglés) (ejemplo, una red ad-hoc o una red de infraestructura que utiliza solamente el DCF). De igual manera, CSMA/CA junto con el acuse de recibo se utilizan dentro del período de contienda de un supermarco cuando una función de punto de coordinación está presente. Todas las transmisiones asíncronas del marco utilizan el CSMA/CA+Ack, a excepción de los marcos de Broadcast/Multicast dirigidos a las estaciones, las cuales no las reconocen. Los marcos de Broadcast/multicast que se generan por las estaciones y deben ser remitidos por un punto de acceso serán reconocidos por el punto de acceso [IEEE 802.11, 1998].

Para mejorar la robustez del mecanismo básico CSMA en situaciones de estaciones ocultas, se transmite un marco particular utilizando el mecanismo RTS/CTS en el cual tanto el remitente como el receptor hacen saber su intento por transmitir en una duración específica a otras estaciones. Puesto que este mecanismo es particularmente apropiado para proteger marcos largos de transmisión, su empleo

se controla por un parámetro que la estación determina de acuerdo al tamaño, es decir se determina que marco será transmitido con RTS/CTS y cual será transmitido sin este [IEEE 802.11, 1998].

Las transmisiones asíncronas libres de contienda se pueden administrar por la función del punto de coordinación. Aquí el punto de coordinación puede permitir a la estación que participe en el inicio libre de contienda, durante el cual transmite sus marcos asíncronos. Una estación que participa en tal servicio puede utilizar también el período de contienda para sus marcos asíncronos, y las oportunidades de transmisión libres de contienda se pueden apreciar como desempeño del funcionamiento para la estación dada. El empleo del período libre de contienda para las transmisiones asíncronas es posible con un superbarco solamente si las estaciones limitadas en tiempo han tenido ya sus requerimientos resueltos [IEEE 802.11, 1998].

3.2.3 Función de Punto de Coordinación (PCF)

3.2.3.1 Servicios de tiempo limitado.

Las estaciones que requieren una variación limitada de retardo en sus transmisiones, pueden utilizar el servicio de tiempo limitado DFWMAC. Este se establece en el período libre de contienda (punto de coordinación) de un supermarco. Cada estación realiza una conexión con el punto de coordinación, cuando este les haga la petición a cada estación que trabaje bajo el protocolo PCF. El punto de coordinación (típicamente el punto de acceso) se asegurará que la estación reciba

tales oportunidades en intervalos regulares (al menos una vez dentro de cada supermarco). Como el servicio limitado en tiempo se basa en la función de punto de coordinación, es posible solamente en las configuraciones en las cuales el punto de coordinación BSS no se traslapa con ningún otro punto de coordinación BSS. Cada BSS es el que se encarga de controlar el sistema de petición para cada estación. La implementación del mecanismo de acuse de recibo es algo diferente para el servicio limitado en tiempo [IEEE 802.11, 1998].

3.2.3.2 Función de Punto de Coordinación.

DFWMAC utiliza opcionalmente una función del punto de coordinación (PCF), que puede proporcionar servicios libres de contienda. El empleo de este PCF está restringido, porque puede ser utilizado solamente en ciertos ambientes. La restricción básica es que un PCF no puede traslaparse con otro PCF en el mismo canal, así que debe haber suficiente aislamiento entre múltiples PCF's. Esto se debe a que la contienda entre múltiples traslapes de PCF's no se pueden resolver por el protocolo. Esto limita la utilidad del PCF a operar donde existe un solo BSS de un ESS, o donde los ambientes múltiples del canal puedan asegurar el suficiente aislamiento entre PCF's vecinos. El PCF no se puede emplear en redes Ad-Hoc debido a que el PCF requiere de un punto de coordinación, el cual se representa por el punto de acceso (AP), y las redes Ad-Hoc no cuentan con él [IEEE 802.11, 1998]. El PCF permite servicios libres de contienda, los cuales pueden ser utilizados por servicios limitados en tiempo así como con servicios asíncronos. Los servicios libres de contienda se utilizan solamente en el modo de infraestructura. Estaciones y AP's

tienen la opción de implementar el PCF. Pueden ser utilizadas solamente cuando una estación y un AP tienen esta opción implementada, permitiendo al AP controlar la comunicación utilizando métodos de encuesta [IEEE 802.11, 1998].

3.2.3.3 Estructura del Supermarco.

El PCF utiliza un concepto de supermarco como se muestra en la Figura 3.6 Dentro de un período dado de supermarco, el PCF será activado en el período libre de contienda, mientras que el DCF se utiliza en el período de contienda.

El período libre de contienda puede ser variable en un supermarco, sin ningún encabezado adicional. Al principio del supermarco, el PCF ganará control sobre el medio con la condición de que el medio se detecte libre. Si el medio se detecta ocupado, entonces el PCF se esperará hasta el extremo del marco, y ganará control sobre el medio tan pronto como detecte que se encuentra disponible por un período de tiempo utilizado por el protocolo de acceso PCF que es el que le asigna la prioridad de tener acceso al medio sobre el protocolo DCF [IEEE 802.11, 1998].

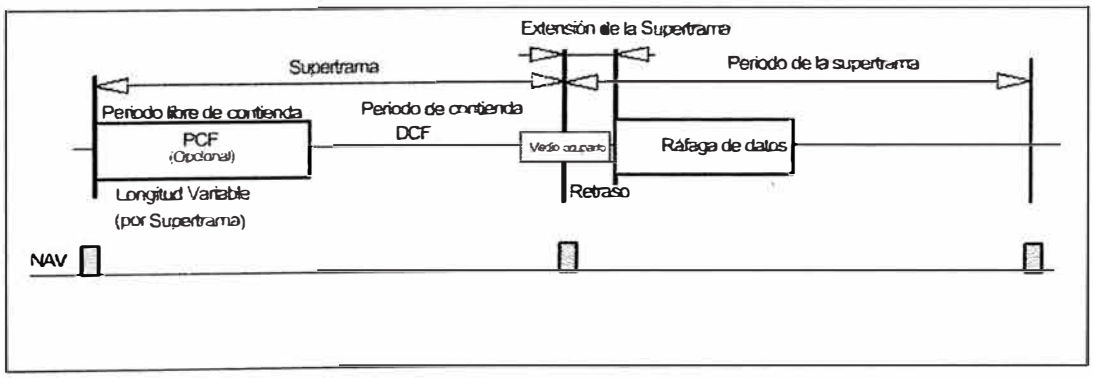


Figura 3.6 Construcción de un supermarco PCF

El tráfico asíncrono que utiliza el DCF, se esperará automáticamente hasta después del período libre de contienda, porque utiliza el nivel de prioridad PCF del protocolo de acceso CSMA/CA, que causa una ráfaga de tráfico con las intertramas que son más pequeñas que el período mínimo DIFS necesario por el protocolo CSMA/CA [IEEE 802.11, 1998].

Para evitar la contienda al inicio del período de supermarco entre el tráfico de contienda y el PCF, se puede emplear una función Tx-Blackout. Esto se puede ver como un programa de NAV de la primera ranura al inicio de cada supermarco. La longitud de un superbarco podría ser un parámetro manejable, la cual puede depender de los servicios proporcionados, y quizás del tipo de PHY utilizado. En una PHY con saltos en frecuencia se requiere que el tiempo que dure el salto sea un múltiplo de un número entero del período del superbarco [IEEE 802.11, 1998].

3.2.3.4 Protocolo PCF (Función de Punto de Coordinación)

Cada Período Libre de Contienda (CFP por sus siglas en inglés) iniciará con una trama llamada Beacon que contiene un "Mensaje de Indicación de entrega de Tráfico" DTIM. La trama beacon se emplea para efectuar la sincronización y para actualizar relojes. El Punto de Coordinación (PC por sus siglas en inglés) genera períodos libres de contienda a una razón de repetición libre de contienda (CFPRate) el cual se define como un número de intervalos [IEEE 802.11, 1998], como se ilustra en la Figura 3.7

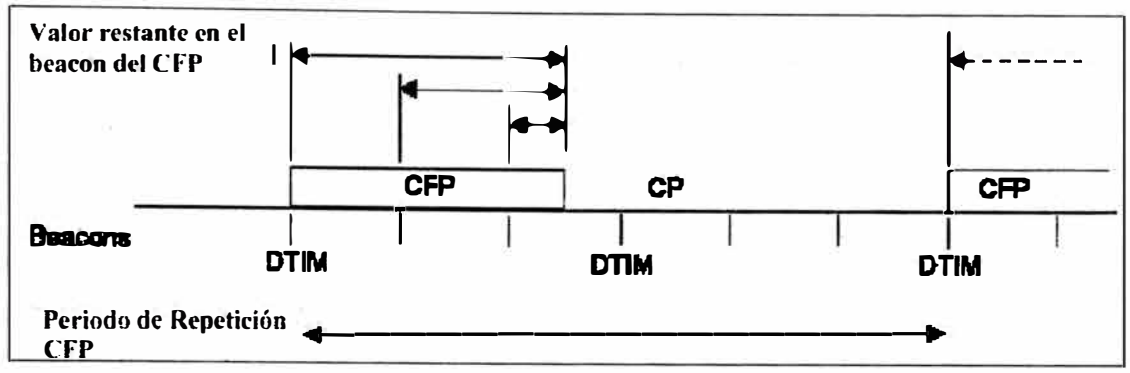


Figura 3.7: Beacons y CPPS

La longitud del período libre de contienda se controla por el punto de coordinación, con un valor máximo especificado por el parámetro de Duración Máxima del Período Libre de Contienda (CFP-MaxDuration por sus siglas en inglés) en el parámetro libre de contienda, colocado en el punto de coordinación. El valor mínimo para CFP-MaxDuration es el tiempo requerido para transmitir dos tramas de datos con la longitud máxima cada una (2346 octetos) incluyendo el encabezado, el marco de beacon inicial y el marco de Fin de Período Libre de Contienda (CF-End por sus siglas en inglés). Este tiempo será suficiente para mandar un marco de datos a la estación vía el punto de acceso, mientras le manda el marco de encuesta, y la estación responda con un marco de datos. El valor máximo para CFPMaxDuration es el período libre de contienda menos el tiempo requerido para transmitir una trama de datos con la longitud máxima durante el Período de Contienda (CP por sus siglas en inglés), expresado en microsegundos [IEEE 802.11, 1998].

El protocolo de Función de Punto de Coordinación se basa en un esquema de encuesta. Las estaciones necesitan solicitar el servicio libre de contienda, el cual cuando se concede puede ser utilizado hasta que el servicio se cierra. Si el servicio se

concede por AP, después el protocolo de PCF pondrá esa estación en la lista de encuesta, de tal manera que pueda participar en el servicio [IEEE 802.11, 1998].

El punto de acceso enviará el tráfico de la cola (CF-down) para estaciones libres de contienda con una prioridad específica PCF. Un bit de encuesta en el encabezado de estos marcos revisará las estaciones para enviar sus datos (CF-up). Las estaciones reaccionarán a la encuesta inmediatamente cuando tengan un marco en la cola para transmitir en el período libre de contienda, para enviar este marco después del intervalo de tiempo SIFS. Esto resulta en una ráfaga de tráfico libre de contienda [IEEE 802.11, 1998].

Al inicio de cada período libre de contienda, el punto de coordinación (normalmente es el punto de acceso) sensará el medio. Cuando el medio este libre por un período PIFS, el PC transmitirá un marco beacon, después de transmitir el marco inicial, el punto de coordinación esperará un período SIFS para iniciar la transmisión. Después del beacon, iniciará mandando un paquete, ya sea de encuesta únicamente, o de encuesta incluyendo los datos, para la primera estación que se encuentra en la lista de encuesta. Para los servicios que requieren el acuse de recibo de MAC, como es el caso en el empleo de la función de punto de coordinación, este se hace a través de un bit en el encabezado de la respuesta o en marcos subsecuentes. Este es el bit de Ack_Previous_Frame (marco previamente recibido, APF por sus siglas en inglés). El marco U1 en la Figura 3.8 tiene el bit APF para el acuse de recibo del marco anterior D1. También el marco D2 contendrá el bit APF para el acuse de recibo de U1, esto, con la finalidad de optimizar el sistema de encuesta, ya

que así, se evita tener que mandar el acuse de recibo en un paquete, o los datos en otro, dado que el sistema realiza una transmisión a las estaciones cuando transmite, todas reciben el paquete, y si tiene información para alguna de ellas lo toma, de lo contrario lo desecha. La información que puede contener un paquete para cada estación puede ser datos, de acuse de recibo o bien de petición de envío de información [IEEE 802.11, 1998].

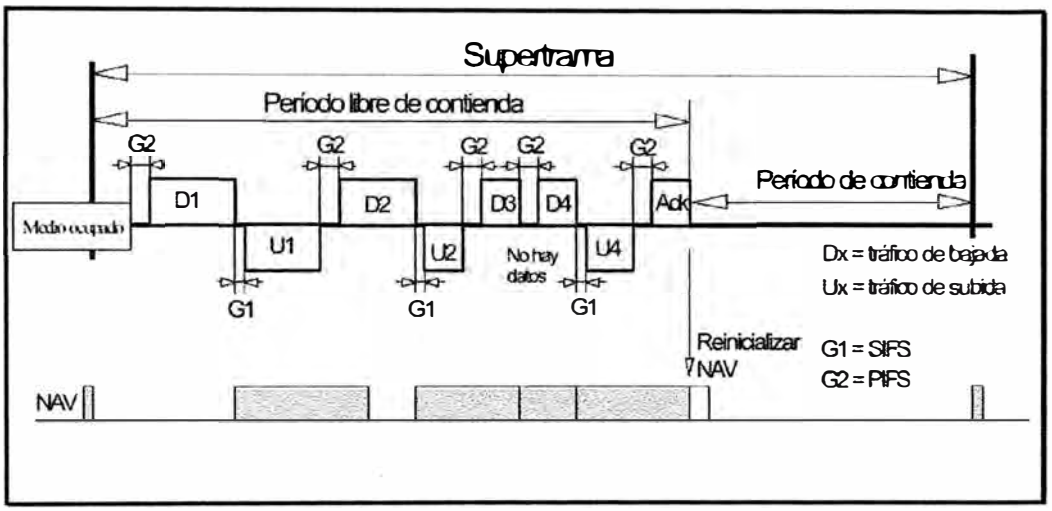


Figura 3.8: Mecanismo del protocolo PCF

La duración de los marcos puede ser variable, sólo está limitada por una longitud máxima negociada durante el servicio libre de contienda. Si una estación no reacciona dentro del tiempo de retardo de PIFS, entonces la función de punto de coordinación en el punto de acceso tomará control y transmitirá el siguiente marco que se encuentre en la cola. Obsérvese que una estación no responderá en la siguiente situación: cuando la estación no tiene tráfico CF-up para mandar, y no se requiere ningún acuse de recibo para ser regresado por el marco precedente CF-down. Por

ejemplo, cuando el marco CF-down tiene una longitud de zona de datos de 0, es decir, que el PC no mandó datos a dicha estación [IEEE 802.11, 1998].

En el encabezado de todos los marcos libres de contienda que vienen del punto de acceso (CF-down) se proporciona una indicación para actualizar a NAV en cada estación, que difiere para el inicio del período libre de contienda. Esto evitará que las estaciones que no escuchan a la estación que responde (oculta), comiencen inadvertidamente su transmisión durante el inicio de período libre de contienda, y esperen al período de contienda para poder transmitir [IEEE 802.11, 1998].

Obsérvese que se asume que todas las estaciones escucharán al punto de acceso, de modo que la información que se reciba por cada estación, puede entonces proteger el marco CF-up, el cual puede no ser escuchado por todas las estaciones en el BSS. La función de punto de coordinación generará un marco al final del período libre de contienda que tiene las siguientes funciones:

- Mandar acuse de recibo al último marco de CF-Up recibido si necesitó el bit de APF.
- Reajustar el NAV en todas las estaciones que estén escuchando.

Esto se puede hacer por ejemplo en un acuse de recibo o marco de aviso. Es importante actualizar el NAV, debido a la medida variable del marco de respuesta de la estación. El NAV se fija a una longitud prevista máxima del marco de respuesta. Una función de Reset_NAV (reinicializar el vector de asignación de red) es necesaria

para permitir a todas las estaciones asíncronas, utilizar el período de contienda inmediatamente después de que termine el período libre de contienda.

Cuando el punto de coordinación no tiene más marcos para transmitir, o estaciones que encuestar, este mandará un marco CF-End para marcar el final de la transmisión del CFP. Si se recibe un acuse de recibo al tiempo que se transmite el CF-End, el punto de coordinación transmitirá un marco CF-End+ACK (marco de fin de periodo de contienda incluyendo el acuse de recibo). Todas las estaciones que reciban dicho marco, actualizarán sus NAV y podrán intentar transmitir durante el período de contienda.

CAPÍTULO IV

TÉCNICAS DE MODULACIÓN

4.1 Introducción

El estándar IEEE 802.11 (Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications), a pesar de su reciente aparición, está penetrando en el mercado rápidamente. El secreto del éxito de esta técnica se basa principalmente en que trabaja en bandas de frecuencia que no necesitan de licencia para su utilización: ISM (Industrial, Scientific and Medical; 2,4GHz) y U-NII (Unlicensed National Information Infrastructure; 5GHz). El caso opuesto es lo que le ha sucedido a la tecnología UMTS (Universal Mobile Telecomunications System). El elevado precio a pagar por las licencias ha sido la causa principal del fracaso de esta tecnología. El mercado ve en el 802.11 el candidato ideal para reemplazar el hueco dejado por el UMTS.

Inicialmente el 802.11 se pensó para redes locales inalámbricas (WLAN) de corto alcance pensadas para entornos SOHO (Small Office – Home Office), pero la necesidad de comunicar dispositivos portátiles a velocidad de transmisión elevada ha llevado a plantear e incluso llevar a la práctica la creación de redes inalámbricas de mayor envergadura. Ejemplo de esto son las redes de este tipo que ya están instaladas

en aeropuertos, campus universitarios o incluso en barrios de distintas ciudades, como ya antes se ha detallado en el capitulo III del presente informe.

El estándar IEEE 802.11 se divide en dos capas principales: la capa MAC (Media Access Control) y la capa física o PHY. Estas dos capas permiten hacer una separación funcional del estándar y, lo que es más importante, permite que un único protocolo de datos pueda usarse con distintos métodos de transmisión en radiofrecuencia (RF).

El estándar IEEE 802.11 [IEEE802.11] fue aprobado por el IEEE en 1997 y posteriormente, en 1999, fue adoptado como estándar internacional conjuntamente por la ISO (International Organization for Standardization) y el IEC (International Electrotechnical Commission) [ISO/IEC 8802.11].

El interés suscitado en este campo de las redes inalámbricas ha posibilitado una rápida evolución del estándar inicial (802.11 es el primero que apareció; contempla la comunicación hasta 2Mbps y emite en la banda de 2.4GHz ISM - Industrial, Scientific and Medical, una frecuencia donde no hace falta licencia para operar - o dentro del espectro infrarrojo) y actualmente existen tres extensiones del estándar inicial:

- 802.11b "Higher-Speed Physical Layer Extension in the 2.4 GHz Band" [IEEE802.11b].
- 802.11a "High-speed Physical Layer in the 5 GHZ Band" [IEEE802.11a]

- 802.11g "Further Higher-Speed Physical Layer Extension in the 2.4 GHz Band" [IEEE802.11g]

Dentro del mercado el que más aceptación ha tenido es el 802.11b, aunque la velocidad de transmisión máxima (11Mbps) es inferior a la del 802.11a (54Mbps). La razón es que debido a que se trabaja a una banda de mayor frecuencia (5GHz) el alcance es justo la mitad que en el 802.11b que trabaja en la banda de 2,4GHz. El nuevo estándar 802.11g, que todavía está en fase de borrador, trata de llegar a velocidades de transmisión similares al 802.11a, pero en la frecuencia de 2,4GHz.

Este estudio se va a centrar en la capa física del 802.11 y en la extensión 802.11b por ser el más extendido. En el último apartado se analizará la nueva extensión 802.11g.

4.2 Técnicas de transmisión

La capa física del estándar 802.11 define diferentes técnicas de transmisión. En concreto tres:

- FHSS (Frecuency Hopping Spread Spectrum) Espectro extendido de salto de frecuencias. En este sistema el emisor va saltando de frecuencia en un patrón conocido por el receptor. Mediante una correcta sincronización, puede mantenerse un único canal lógico.
- DSSS (Direct Spread Spectrum) Espectro extendido de secuencia directa. Se genera un patrón redundante por cada bit que debe ser transmitido, llamado

chip, de manera que en caso de pérdida de información ésta pueda ser recuperada; con ello se consigue que sea más resistente a cualquier interferencia.

- Infrarrojo Difuso no ha recibido ninguna aceptación en el mercado y por eso quedará fuera de este estudio.

Las otras dos tecnologías no son compatibles y, por lo tanto, es preciso estudiar para cada caso concreto qué emisor/receptor es más conveniente. En términos generales, los aparatos basados en el FHSS son más baratos y consumen menos, pero también tienen una zona de alcance menor que los de DSSS y están más limitados en el ancho de banda que pueden ofrecer. Si bien este último aspecto actualmente no importa demasiado, ya que el estándar prefija cuál es la velocidad máxima que puede alcanzarse independientemente de cuál sea la tecnología utilizada, se prevé que los estándares más nuevos contemplarán esta posibilidad de mayor velocidad para los mecanismos que utilicen el DSSS.

4.2.1 FHSS (Saltos en Frecuencia mediante Espectro Esparcido)

La técnica de espectro ensanchado mediante saltos de frecuencia o FHSS propuesta por el IEEE, consiste en dividir la banda ISM en 79 canales de 1MHz sin superposición y realizar saltos periódicos de un canal a otro siguiendo una secuencia pseudoaleatoria que sirve de pauta. Si se eligen bien las pautas y se sincronizan los distintos transmisores perfectamente pueden estar emitiendo a la vez 78 dispositivos sin interferirse entre ellos. Las técnicas de modulación que se aplican a estos canales

en el estándar 802.11 son 2GFSK y 4GFSK. GFSK significa Gaussian Frecuency Shift Keying y consiste en un filtro Gaussiano paso bajo de 500KHz (500Ksímbolos/s) para conformar la señal (NRZ- Not Return to Zero) de forma que no interfiera con canales adyacentes y una simple modulación en frecuencia (FSK). Las velocidades de transmisión que se alcanzan son:

- 2GFSK: Utiliza dos niveles de amplitud (2 símbolos) para obtener 1Mbps.
- 4GFSK: Utiliza cuatro niveles de amplitud (4 símbolos) para obtener 2Mbps

Como podemos apreciar en la Figura 4.1

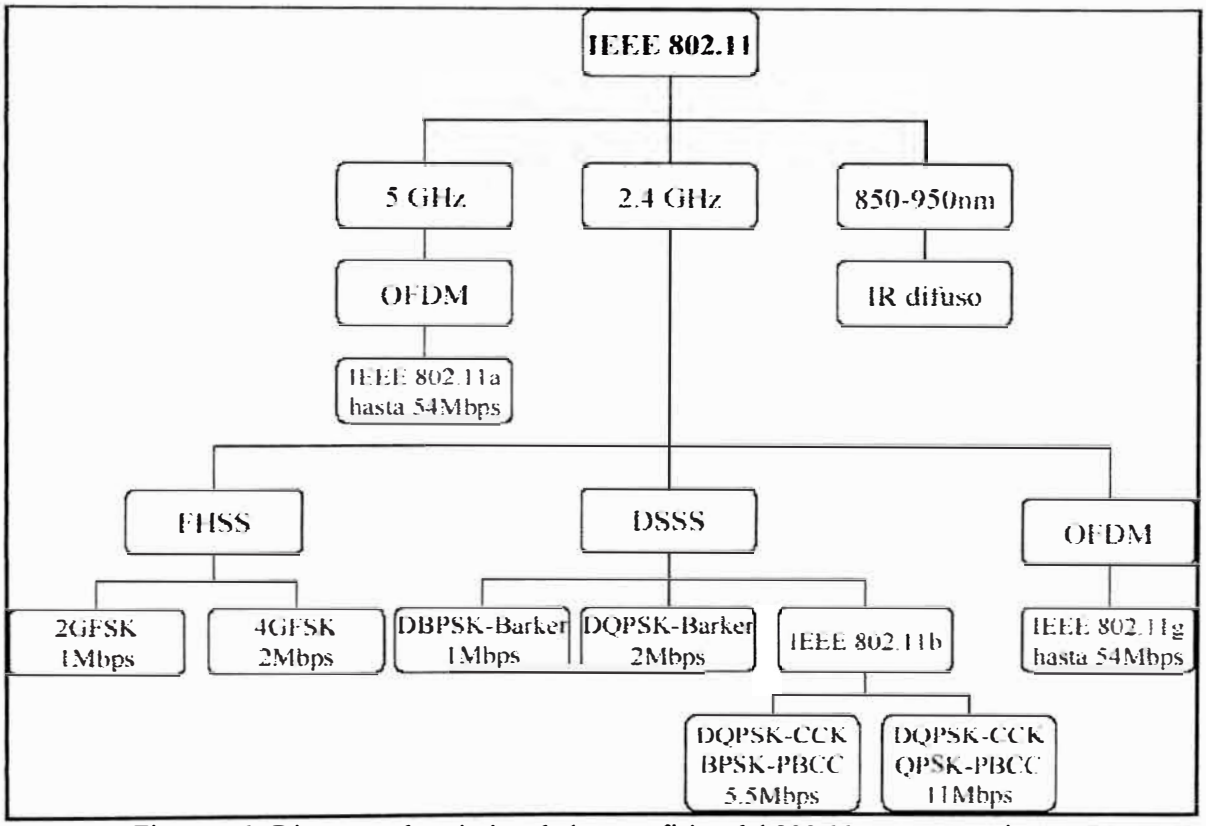


Figura 4.1: Diagrama descriptivo de la capa física del 802.11 y sus extensiones.

En la Figura 4.2 se muestra un ejemplo simple de cómo funciona esta técnica. En este ejemplo se supone que hay dos dispositivos FHSS emitiendo simultáneamente. Uno de ellos aparece marcado con línea fina y el otro con línea

gruesa. En cada instante de tiempo cada uno de ellos está trabajando a una frecuencia distinta al otro. Debido a que se utiliza un rango de frecuencias bastante amplio esta técnica se considera dentro del conjunto de técnicas de espectro ensanchado.

El esquema de FHSS/802.11 es muy parecido al de BlueTooth. Sin embargo este ha calado más hondo en el mercado relegando al FHSS/802.11 a un segundo plano. Aún así el Bluetooth no ha podido con la popularidad del DSSS/802.11. Esto se debe a que el mercado demanda redes inalámbricas de alta velocidades de transmisión y el Bluetooth se pensó para interconectar periféricos a cortas distancias y a baja velocidad.

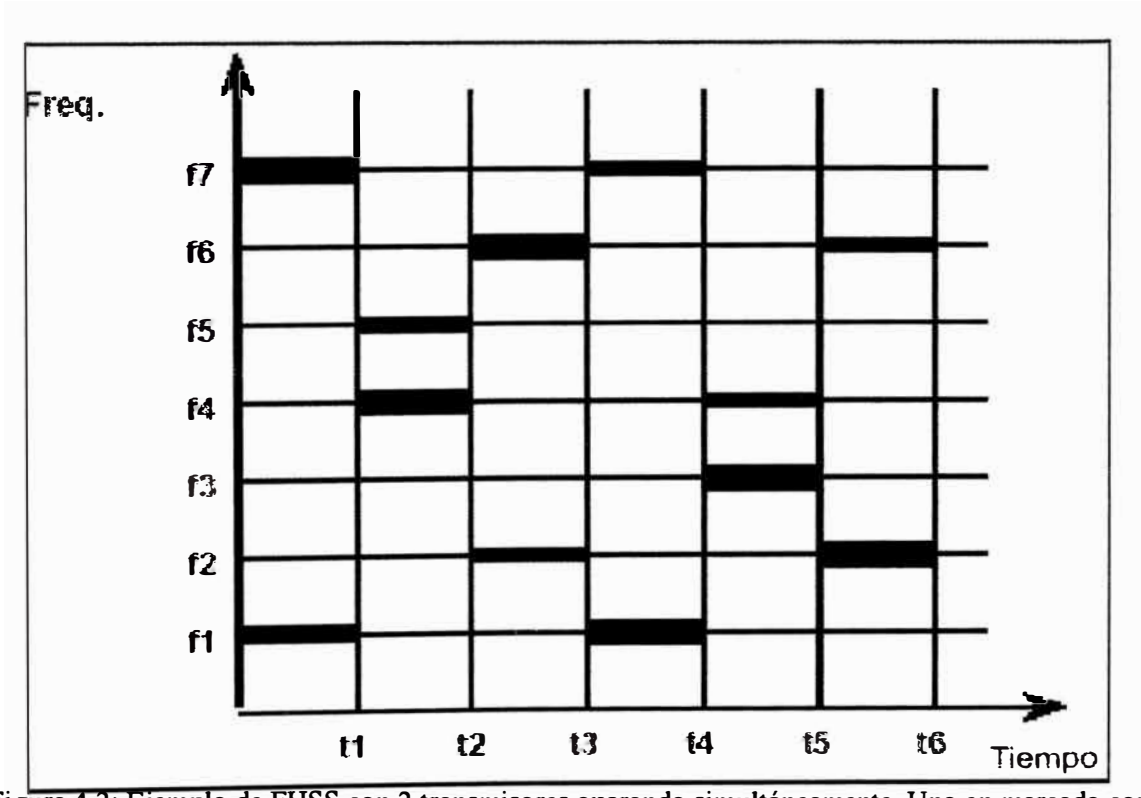


Figura 4.2: Ejemplo de FHSS con 2 transmisores operando simultáneamente. Uno en marcado con línea gruesa y otro con línea fina.

4.2.2 DSSS (Secuencia directa mediante espectro esparcido)

El DSSS consiste en técnicas de espectro ensanchado mediante secuencia directa. Para ser tolerantes al ruido e interferencias, en vez de saltar de una frecuencia a otra como el FHSS, utilizan códigos pseudoaleatorios (PN) que distribuyen la potencia de los datos a transmitir en un amplio ancho de banda. Los datos a transmitir se convolucionan con códigos pseudoaleatorios. Estos códigos poseen componentes frecuenciales que se distribuyen en un amplio ancho de banda. La propiedad fundamental es que, aunque el canal de transmisión introduzca ruido No, un simple proceso de correlación en la detección permite recuperar la señal. El estándar 802.11 propone utilizar como código pseudoaleatorio el Código Barker de 11 bits.

Para aclarar este concepto, supongamos que la señal modulada que se va a transmitir (s(t), de potencia S), antes de ser "ensanchada", tiene un ancho de banda de Bs Hz y una densidad espectral de potencia aproximadamente constante e igual a So W/Hz, tal como se muestra en la Figura 4.3. Su potencia será aproximadamente igual a S=BsSo.(La potencia es el área encerrada por la curva). Antes de ser transmitida se efectúa una convolución con una señal pseudoaleatoria de un ancho de banda de W Hz. El resultado es una señal de aproximadamente W Hz de ancho de banda (con W >> Bs), y que al conservar su energía tendrá una densidad espectral de potencia de So' W/Hz:

$$S = S_0' W \Rightarrow S_0' = \frac{S}{W} = \frac{B_S}{W} S_0$$

Durante la transmisión se suma a la señal un ruido n(t) de ancho de banda B_N y densidad espectral de potencia I_0 W/Hz. Resultando una potencia $N=B_N I_0$. Esta interferencia tiene una potencia significativa frente a la de la señal modulada, y en condiciones normales sería suficiente para provocar una pérdida total de la comunicación.

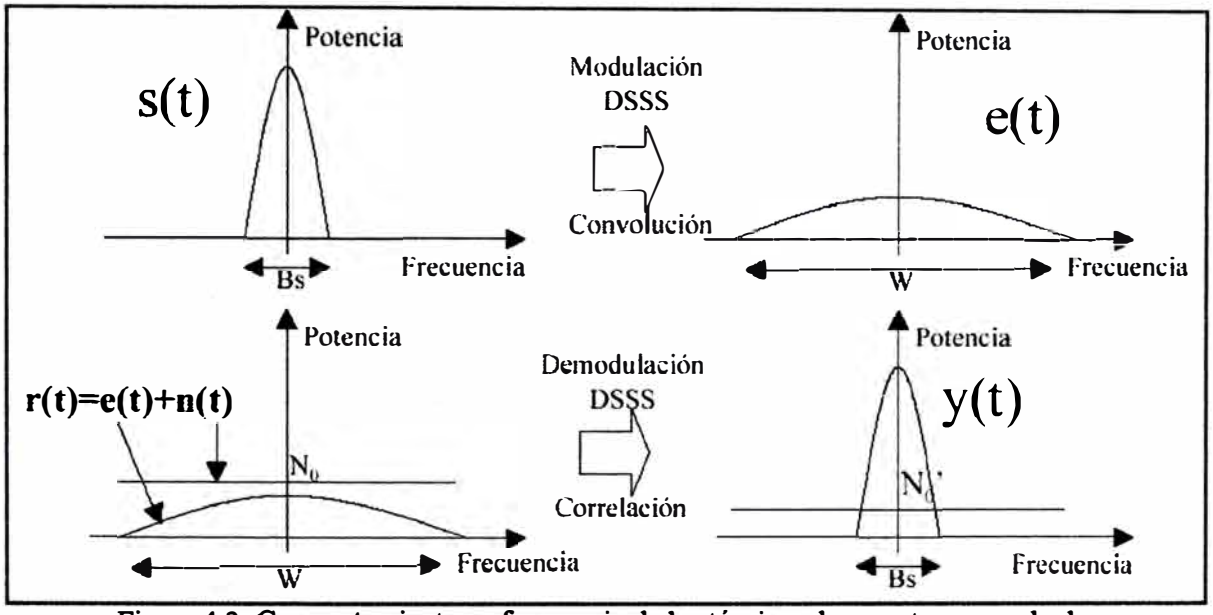


Figura 4.3: Comportamiento en frecuencia de las técnicas de espectro ensanchado.

En el receptor, se realiza la operación de correlación, dando como resultado la señal modulada en su forma original más el ruido. Este proceso es justo el inverso del de convolución. Ambos procesos actúan como filtros FIR (Finite Impulse Response), pero con los coeficientes invertidos. En este caso, los coeficientes son las muestras de la señal pseudoaleatoria utilizada con ancho de banda W. Debido a que la densidad espectral de potencia debe mantenerse constante:

$$N = N_0' W \Rightarrow N_0' = \frac{N}{W} = \frac{B_N}{W} N_0$$

Antes de demodular la señal S, se realiza un filtrado pasa-banda que elimina las secuencias que están fuera de banda de detección Bs. De esta forma, la energía del ruido queda reducida a:

$$N' = N_0' B_S = \frac{B_S}{W} N = \frac{N}{GP}$$

Es decir, la potencia del ruido queda dividida por un factor W/Bs, que es igual a la relación entre el ancho de banda de la señal después y antes del ensanchado, mientras que la señal S conserva su potencia original. Este factor se llama Ganancia de Proceso (GP). Por lo tanto puede concluirse que la relación señal a ruido después de todo el proceso es:

$$SNR(dB) = 10 \log \frac{S}{N'} = 10 \log \left(GP \cdot \frac{S}{N} \right)$$

El proceso realizado puede resumirse en la siguiente figura:

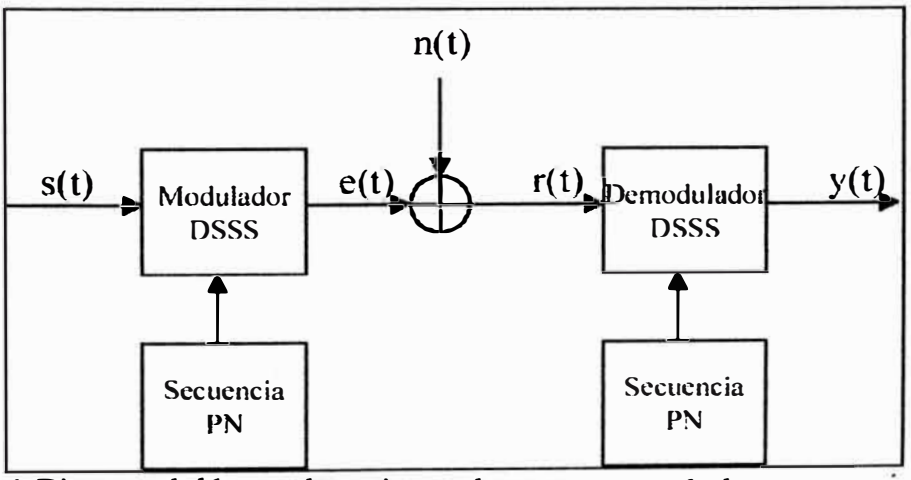


Figura 4.4: Diagrama de bloques de un sistema de espectro ensanchado por secuencia directa.

A pesar del interés que posee esta técnica, no todo son ventajas. Unos de los principales inconvenientes consisten en que la mejora de la SNR tiene por

contrapartida una reducción directamente proporcional de la velocidad de transmisión. En el apartado 4.4.1 se verá con más detalle.

El concepto de DSSS se ha ido ampliando. Ese es el caso de las modulaciones CCK (Complementary Code Keying) y PBCC (Packet Binary Convolutional Coding) que se han incluido en la extensión 802.11b del estándar. El concepto es parecido al que se acaba de describir pero con ciertas peculiaridades que permiten obtener un mejor rendimiento del canal de transmisión. A cada una de ellas se dedican sendos apartados (4.4.2 y 4.4.3).

El proceso DSSS descrito anteriormente es un proceso en banda base, pero para transmitirlo hace falta modular la señal resultante del mismo para desplazarla hasta una frecuencia que esté dentro de la banda ISM. La modulación adoptada por el estándar es la DPSK (Diferential Phase Shift Keying) en sus variantes binaria: DBPSK y en cuadratura: DQPSK. En el apartado 4.4.1 se explican ambas.

Dentro de la banda hay que seleccionar un canal y conformar la señal para que no interfiera en los canales adyacentes. El siguiente apartado versa sobre este tema. Por último, en el apartado 4.4.5 se explicará brevemente cuales son las propuestas para la siguiente extensión del estándar: 802.11g, cuya aprobación está pensada para principios del 2003. Básicamente consiste en aplicar las técnicas del 802.11a a la banda de 2,4GHz. O lo que es lo mismo técnicas OFDM (Orthogonal Frecuency División Multiplexing), que se explicarán brevemente en el apartado 4.4.6.

4.3 Canales de transmisión

Antes de pasar a un estudio más profundo se hace necesario definir exactamente la banda de frecuencias y los distintos canales. El estándar 802.11 está pensado para operar en la banda de frecuencias entre 2,4 y 2,497GHz. Ésta banda tiene la peculiaridad de que su uso es libre y por lo tanto no hay que tener un permiso especial, ni pagar cuota alguna.

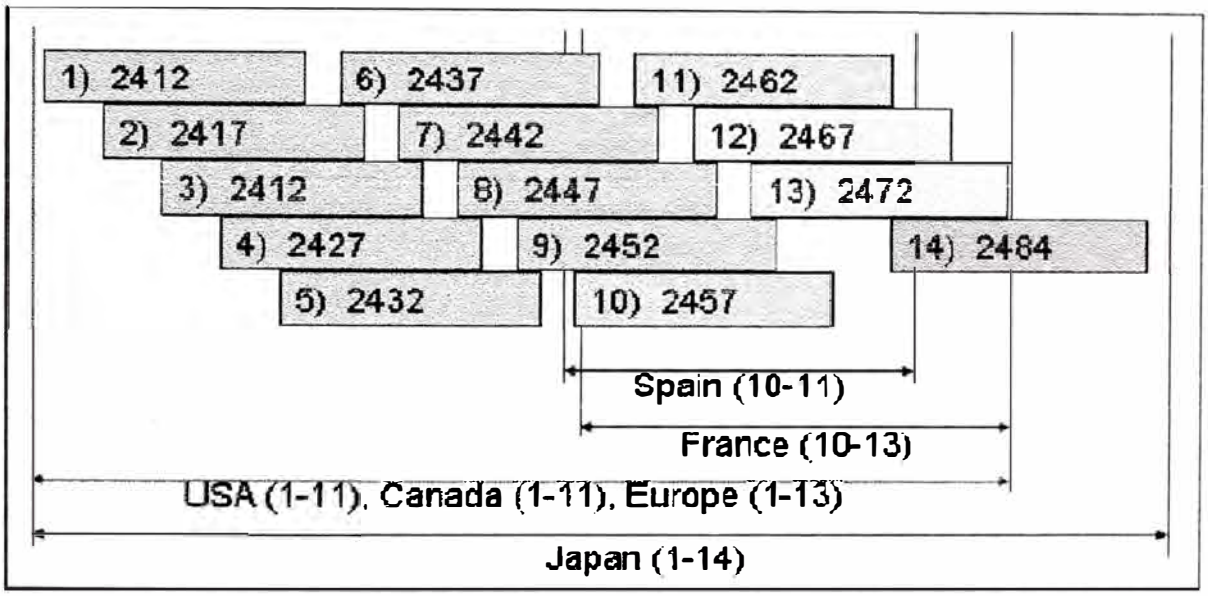


Figura 4.5: Distribución en frecuencia de los canales DSSS del 802.11 según las normativas de distintos países. Los canales están etiquetados con el número de cada canal y la frecuencia central.

En la Figura 4.5 se muestra los canales específicos disponibles en distintos países según sus respectivas agencias de regulación del espectro radioeléctrico. Ésta distribución es la que aparece en el documento definitivo del estándar 802.11 (Tabla 4.1) y se basa en la regulación que existía en el momento en que se redactó.

País	Agencia Reguladora	Rango de Frecuencia Disponible	Canales Disponibles en DSSS	Canales Disponibles en FHSS
USA	FCC	2.4 a 2.483 GHz	1 entre 11	2 entre 80
CANADA	IC	2.4 a 2.4835 GHZ	1 entre 11	2 entre 80
JAPON	MKK	2.4 a 2.497 GHZ	1 entre 14	2 entre 95
FRANCIA	-	2.4465 a 2.4835 GHZ	10 entre 13	48 entre 82
ESPAÑA	-	2.445 a 2.475	10 a 11	47 entre 73
RESTO DE EUROPA	ETSI	2.4 to 2.835	1 entre 13	2 entre 80

Tabla 4.1: Distribución en frecuencia de los canales del 802.11

4.4 Técnicas de modulación

4.4.1 DPSK (Codificación de Fase Diferencial Desplazada)

En el estándar 802.11 y en su extensión 802.11b la señal en banda base se modula con DPSK (Diferential Phase Shift Keying) para llevarla al canal del espectro que corresponda. En concreto con las variantes binarias DBPSK y en cuadratura DQPSK. En este capítulo se hace una descripción general de este tipo de modulación.

La codificación diferencial permite una detección no del todo óptima, pero que no requiere un control de la fase de la portadora. Ésta técnica es muy popular en aplicaciones de comunicaciones móviles donde la variación de la fase de la portadora impuesta por las condiciones del canal es mucho más lenta que la velocidad de símbolo, pero demasiado rápida para hacer un control óptimo de la misma.

El nombre PSK diferencial (DPSK) a veces necesita ser clarificado ya que se refiere a dos aspectos separados del formato modulación/demodulación: el procedimiento de codificación y el procedimiento de detección. El término codificación diferencial se refiere al procedimiento de codificar los datos diferencialmente; esto es, la presencia de un cero o uno binario se manifiesta por la similitud o la diferencia del símbolo cuando es comparado con el símbolo precedente. El término detección diferencial coherente de una PSK codificada diferencialmente, el significado usual de DPSK, se refiere al esquema de detección frecuentemente clasificado como no coherente debido a que este no requiere una fase de referencia con la portadora recibida. Algunas veces, las señales PSK codificadas diferencialmente se detectan coherentemente.

Con sistemas no coherentes, no se tiene intención en determinar el valor real de la fase en la señal de llegada. Por lo tanto, si la forma de onda transmitida en DBPSK es:

$$s_i(t) = \sqrt{\frac{2E}{T}} \cos\left[w_0 t + \theta_i(t)\right] \begin{matrix} i = 1,2,\ldots, M \\ 0 \le t \le T \end{matrix}$$

En donde E es el contenido de energía de $S_i(t)$ en cada duración del símbolo T y $\theta\, i(t)$ la información binaria d_i (M bits) transmitida codificada en cambios de fase de π radianes si el bit es 1 y 0 radianes si el bit es 0 según la constelación de la Figura 4.6

$$\theta_i = \theta_{i-1} + \Delta\theta(d_i)$$

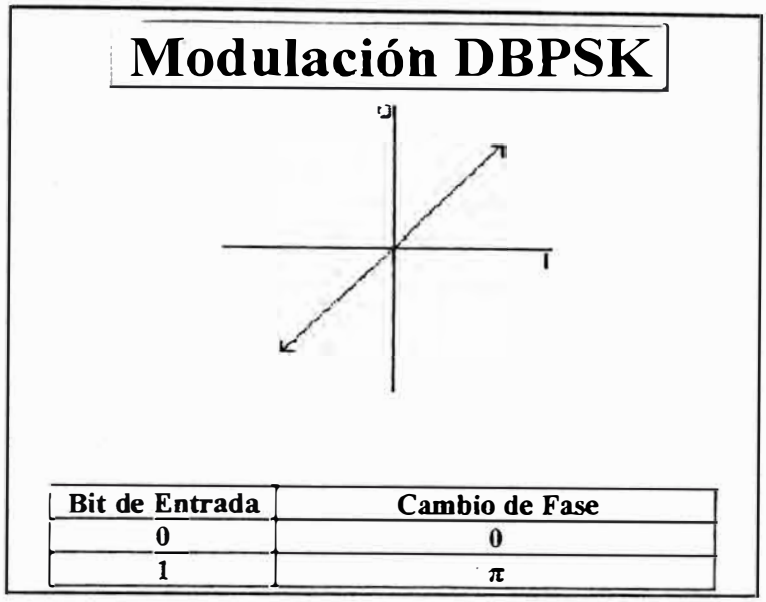


Figura 4.6: Constelación DBPSK.

La señal recibida puede caracterizarse por:

$$r(t) = \sqrt{\frac{2E}{T}}\cos[w_0 t + q_i(t) + a] + n(t) \qquad \begin{matrix} i = 1.2..... M \\ 0 \le t \le T \end{matrix}$$

En donde a es una constante arbitraria y típicamente se asume como una variable aleatoria uniformemente distribuida entre 0 y 2π radianes, y n(t) es ruido.

Para detección coherente, se utilizan filtros acoplados en fase; para detección no coherente, esto no es posible debido a que la salida del filtro acoplado es una función del ángulo desconocido a. Sin embargo, si se asume que a varia lentamente en relación con dos periodos (2T), como se muestra en la Figura 4.7, la diferencia de fase entre dos formas de onda sucesivas, $q_j(T1)$ y $q_k(T2)$ es independiente de a, es decir:

$$[q_k(T_2) + a_1] - [q_j(T_1) + a_2] = q_k(T_2) - q_j(T_1) = f_i(T_2) : a_1 \cong a_2$$

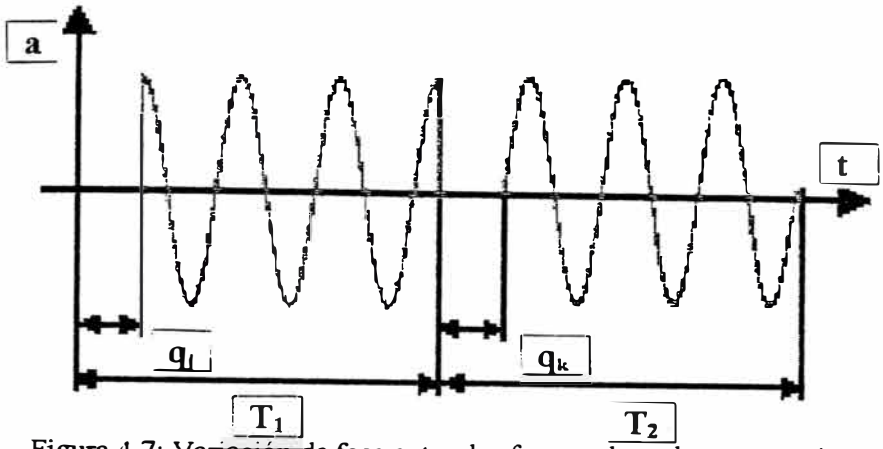
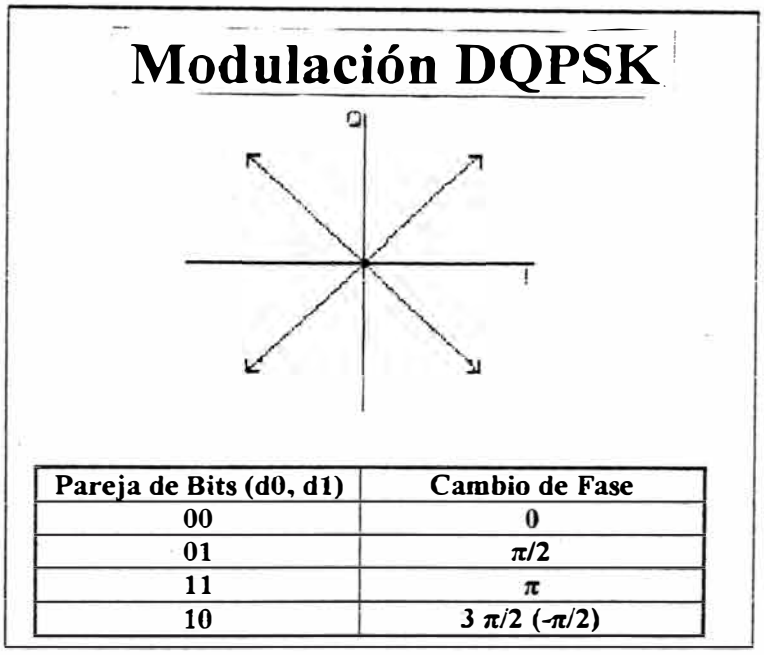


Figura 4.7: Variación de fase entre dos formas de ondas consecutivas.

Para DQPSK el proceso es similar, pero con una constelación con cuatro fases distintas:



Pareja de Bits (d0, d1)	Cambio de Fase
00	0
01	$\pi/2$
11	π
10	$3\pi/2$ ($-\pi/2$)

Figura 4.8: Constelación DQPSK.

La base para la detección diferencial coherente de PSK con codificación diferencial (DPSK) es la siguiente. La fase de la portadora de la forma de onda en el intervalo previo puede ser usada como fase de referencia para la demodulación. Su uso requiere de codificación diferencial del mensaje en el transmisor desde que la

información es portada por la diferencia entre dos formas de onda sucesivas. Para enviar el i-ésimo mensaje (i =1, 2,..., M), la forma de onda actual debe tener su fase adelantada $\Delta\theta(di)$ radianes sobre la forma de onda previa. El detector, en general, calcula las coordenadas de la señal de llegada al correlacionarla con formas de onda localmente generadas tales como $2\cos w_o t$ y $2\text{sen}w_o t$.

El detector entonces mide el ángulo entre el vector actual de señal recibido y el vector de señal previamente recibido, como se muestra en la Figura 4.9

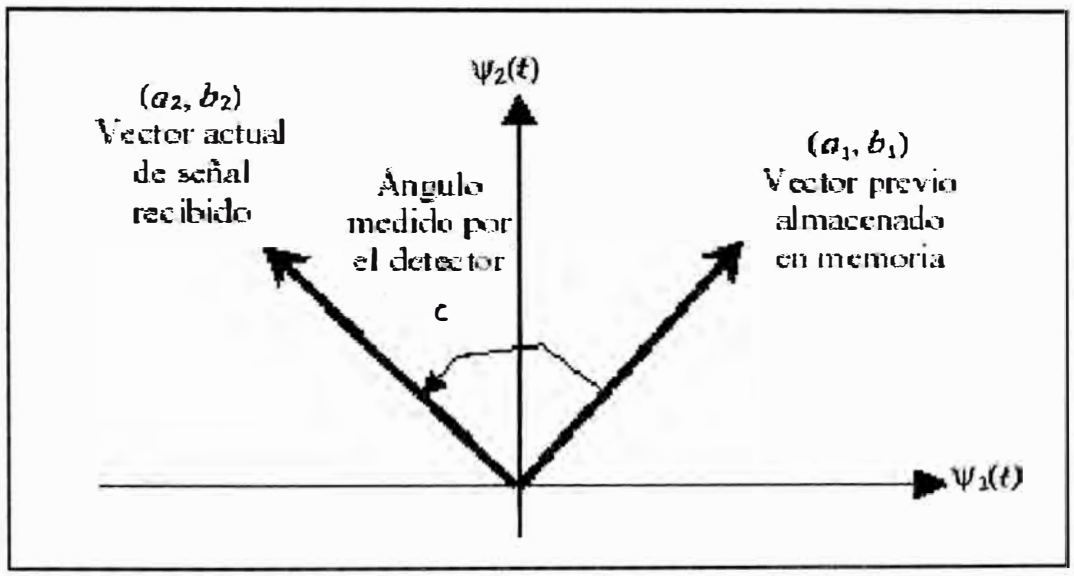


Figura 4.9: Espacio de señales para DPSK.

En general, el formato DPSK se desempeña menos eficientemente que PSK, debido a que los errores en DPSK tienden a propagarse (en intervalos de símbolo adyacentes) debido a la correlación entre formas de onda. Una forma de ver la diferencia entre PSK y DPSK es que en el inicio se compara la señal recibida con una referencia limpia; en los siguientes, no obstante, dos señales ruidosas son comparadas entre sí. Podemos decir que existe dos veces más ruido asociado con el formato DPSK comparado con PSK. En consecuencia, como un primer indicio,

podemos estimar que DPSK manifiesta una degradación de aproximadamente 3dB comparada con PSK; esta degradación decrece rápidamente con el incremento en la SNR. El compromiso para esta pérdida en el desempeño es reducir la complejidad del sistema. Las expresiones de la Probabilidad de bit erróneo (P_o) para los esquemas de modulación BPSK, DBPSK, QPSK y DQPSK son listados en la Tabla 4.2 y su gráfica se muestra en la Figura 4.10. En esta gráfica puede observarse las diferencias que existen entre utilizar un tipo de modulación u otro. Las variantes diferenciales de PSK tiene la ventaja de que los sistemas de detección son más simples de implementar, pero como puede observarse, para una misma E_b/N_o la probabilidad de error aumenta. También se observa que las variantes en cuadratura (mayor eficiencia espectral que las binarias) tienen una probabilidad de error mayor.

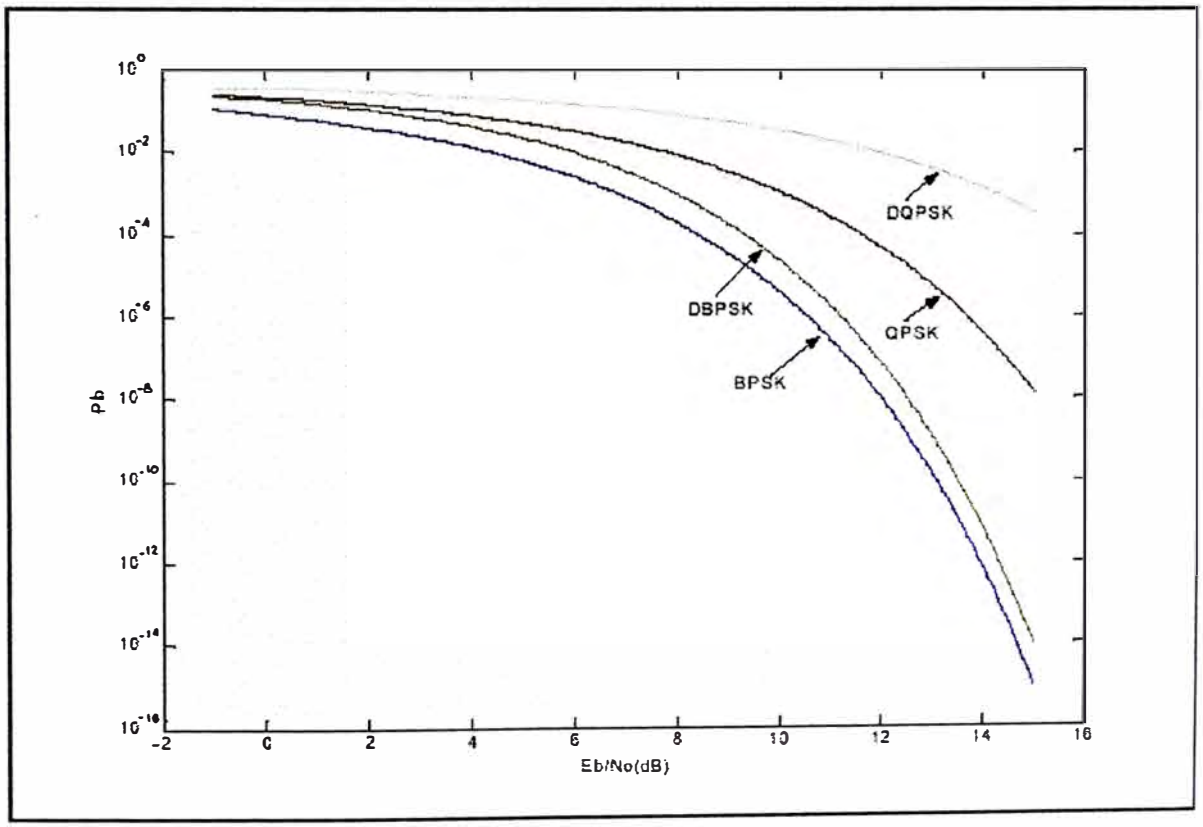


Figura 4.10: Curvas de probabilidad de bit erróneo para diferentes tipos de modulación PSK.

Modulación	Pb o Ps
BPSK	$Q\left(\sqrt{\frac{2E_b}{N_0}}\right)$
DBPSK	$\frac{1}{2}\exp\left(-\frac{E_b}{N_0}\right)$
QPSK	$2Q\left(\sqrt{\frac{2E_s}{N_0}}\operatorname{sen}\frac{\pi}{4}\right)$
DQPSK	$2Q\left(\sqrt{\frac{2E_s}{N_0}}\operatorname{sen}\frac{\pi}{4\sqrt{2}}\right)$

Tabla 4.2: Probabilidad de bit erróneo de BPSK y DBPSK y probabilidad de símbolo erróneo para QPSK y DQPSK.

Para comparar las modulaciones binarias a las en cuadratura se ha utilizado la siguiente relación entre la Probabilidad de bit erróneo (P_b) y la Probabilidad de símbolo erróneo (P_s):

$$\frac{Pb}{Ps} = \frac{M/2}{M-1} = \frac{2}{3}$$

Siendo M, el número de fases de la constelación para k bits/símbolo:

$$M = 2^k$$

En el caso de QPSK, *M* es 4. La función *Q(x)* es conocida como la función de error complementario y está definida por:

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^{\infty} e^{-\frac{u}{2}} du$$

El parámetro E_b/N_o se puede expresar como la relación de la potencia promedio de la señal a la potencia del ruido, *S/N* (o SNR). Al introducir el ancho de

banda de la señal W, se pueden escribir las siguientes igualdades, mostrando la relación entre E_b/N_o y SNR para señales binarias:

$$\frac{E_b}{N_0} = \frac{ST}{N_0} = \frac{S}{RN_0} = \frac{SW}{RN_0W} = \frac{S}{N}\left(\frac{W}{R}\right)$$

en donde S es la potencia promedio de la señal modulada, T el intervalo de duración del bit $R=1/T$ la tasa de bits y $N=N_oW$ el ruido con una potencia promedio N_o en un ancho de banda W.

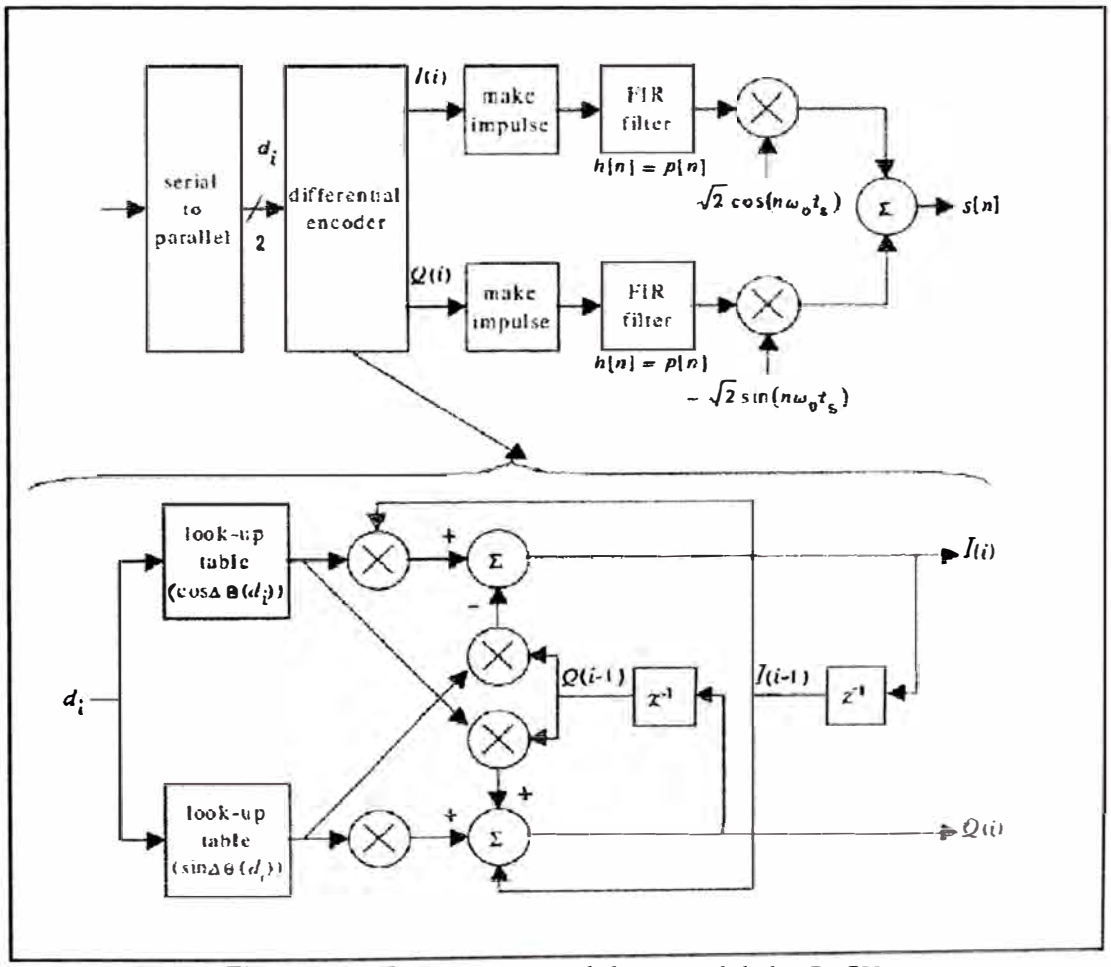


Figura 4.11: Estructura general de un modulador DPSK.

Para terminar este apartado vamos a comparar brevemente como se implementan en la práctica los moduladores y demoduladores DPSK. El estándar 802.11 impone que los equipos deben funcionar con DBPSK y DQPSK.

La estructura del modulador es la que aparece en la Figura 4.11. Este sistema permite generar las señales en banda base I (en fase) y Q (en cuadratura) para PQPSK. Para trabajar en DBPSK basta con utilizar solamente la fase I. El filtro FIR suele ser un Filtro de Coseno Alzado que permite reducir las interferencias entre símbolos (ISI).La demodulación se basa principalmente en correlar la señal recibida (r(t)) consigo misma pero retardada un periodo.

En otras palabras, durante el intervalo de símbolo, se empareja un símbolo recibido con el símbolo previo y se busca si ha habido cambio de fase. Esto queda más claro observando la Figura 4.12:

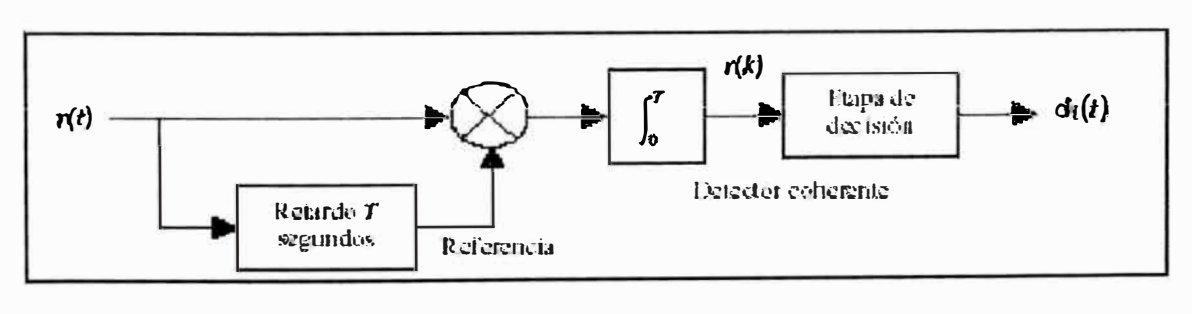


Figura 4.12: Detector coherente diferencial.

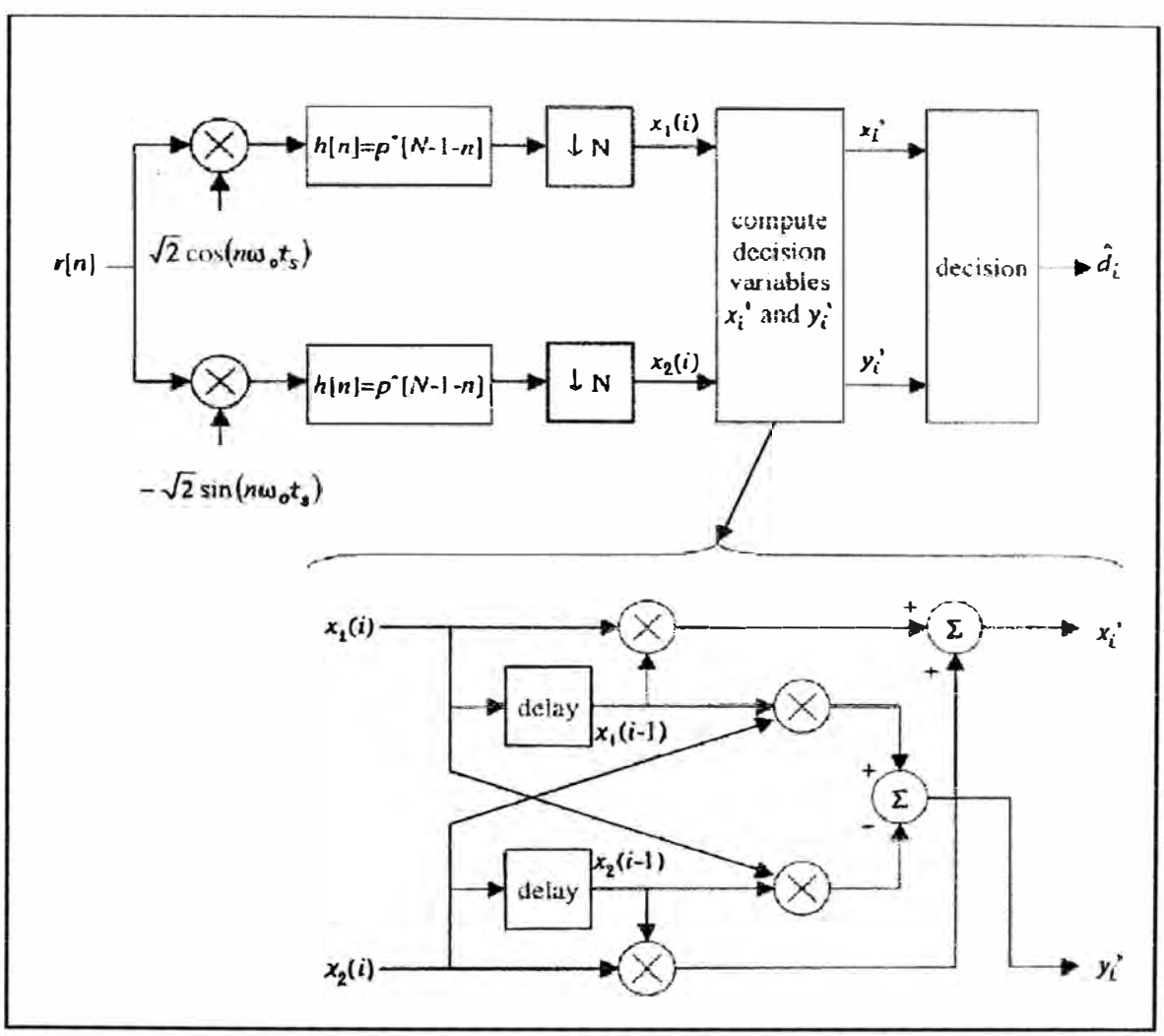


Figura 4.13: Diagrama de bloques de un demodulador DQPSK.

En la práctica se utiliza también el mismo sistema (Figura 4.13) para demodular DBPSK y DQPSK. La diferencia es que en DBPSK sólo se utiliza una de las fases. Para obtener ambas que están en cuadratura se demodula de forma no coherente con señales desfasadas π /2. El resultado de ambas se filtra con el Filtro de Coseno Alzado utilizado en el modulador, pero conjugado. Utilizando el diagrama de la Figura 4.14 se permite obtener el periodo de símbolo. Este se utiliza para realizar un diezmado por N (número de muestras por símbolo). De esta forma, la detección de las señales en fase y en cuadratura en banda base se realiza con una símple correlación digital basada e un simple registro por fase.

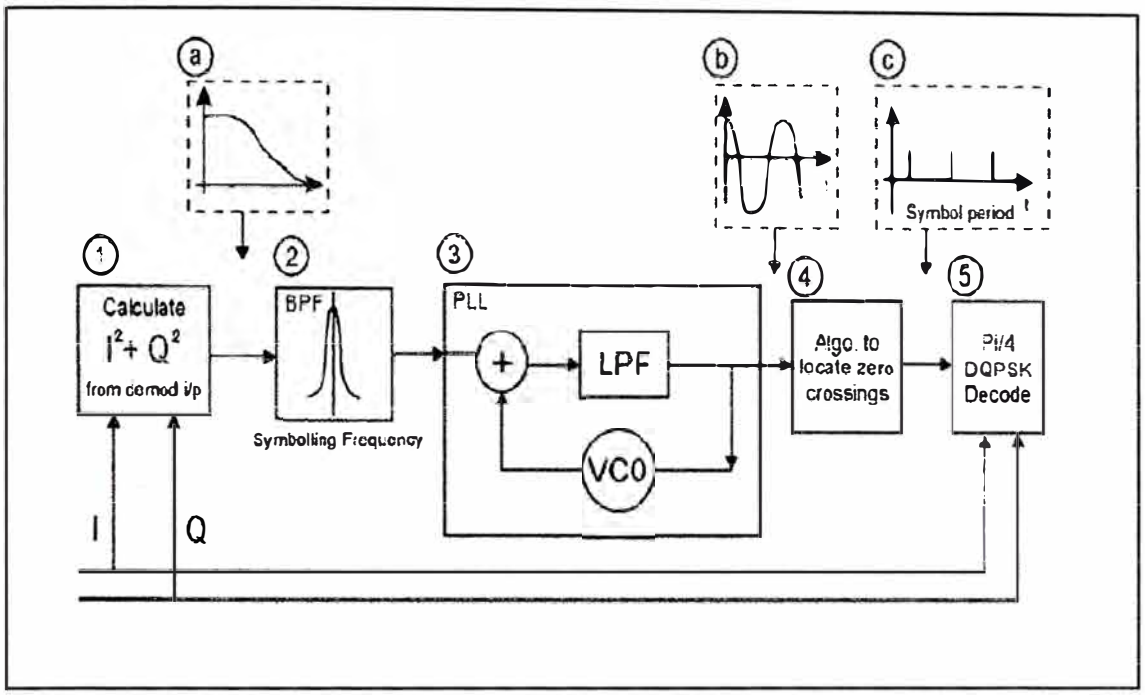


Figura 4.14: Sistema para recuperación de la señal de sincronismo del periodo de símbolo.

- **Secuencias Barker**

El estándar 802.11, además de la modulación DPSK propone la utilización de secuencias Barker de 11 bits para realizar el ensanchado del espectro. La principal ventaja de esta técnica como se comentó en el apartado 3.1 consiste en que se obtiene una alta tolerancia al ruido. En concreto, la codificación con secuencias Barker de 11 bits permite introducir una ganancia de proceso (GP) de:

$$GP = 10\log(\frac{11}{1}) = 10.4dB$$

Como se observa en la Figura 4.15 el resultado del proceso de detección de una secuencia Barker de 11 bits da como resultado picos de ±11 y lóbulos laterales de ±1.

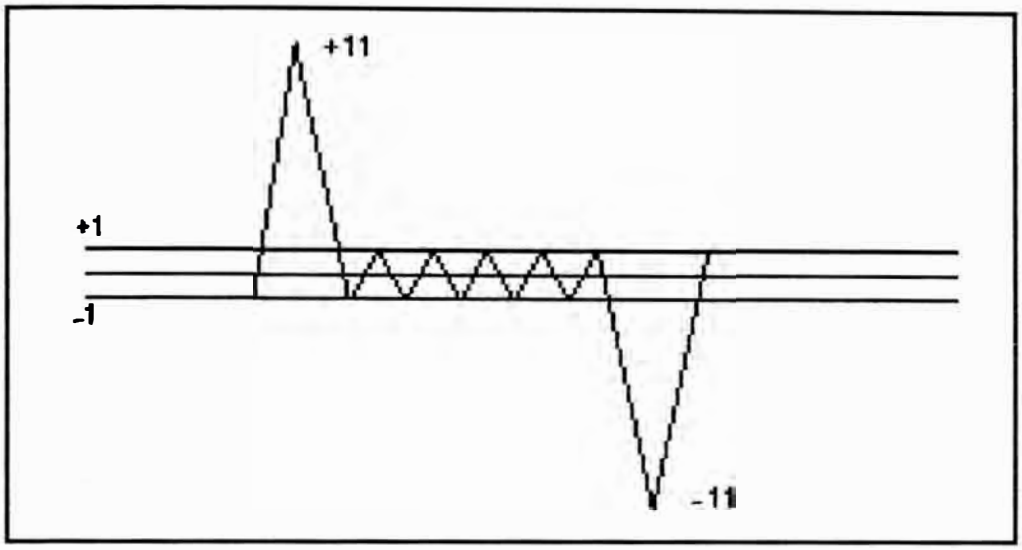


Figura 4.15: Resultado ideal del proceso da detección de secuencias Barker de 11 bits.

El proceso básicamente consiste en realizar una función XOR entre los bits a transmitir y una secuencia pseudoaleatoria Barker de 11 bits. El problema es que la secuencia resultante tiene una frecuencia 11 veces superior a la señal digital que se pretende emitir.

Esto se traduce en una eficiencia espectral 11 veces menor que si no se utilizara esta técnica (Figura 4.16)

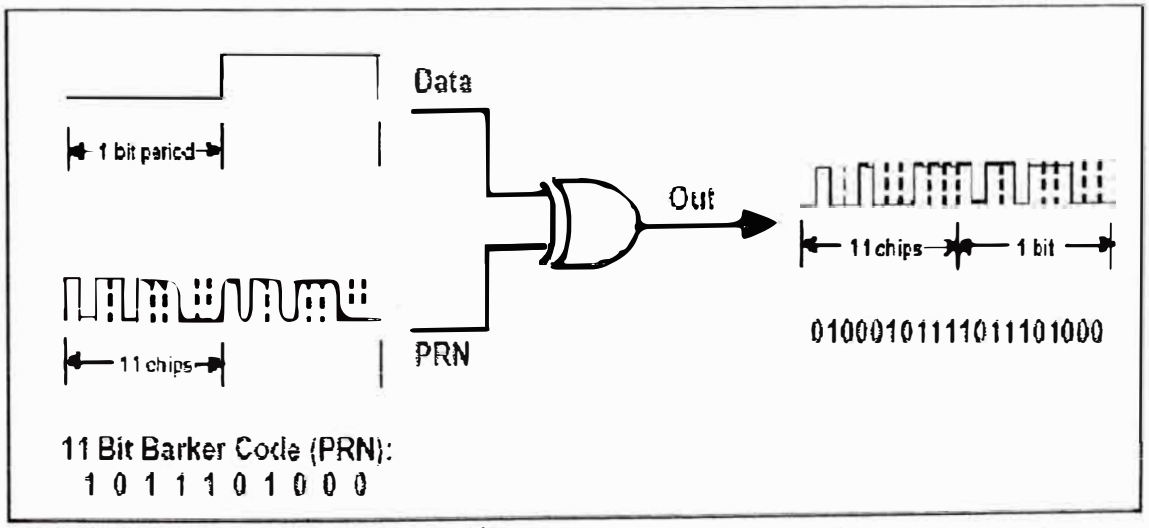


Figura 4.16: Proceso de Modulación en Banda Base con secuencias Golay de 11 bits.

En Canales de 11MHz en banda base como los propuestos en el estándar 802.11 con las dos variantes de DPSK propuestas y sus respectivas eficiencias espectrales se puede alcanzar una velocidad de transmisión de:

Modulación	Eficiencia espectral	Velocidad de transmisión
DBPSK	1símbolo/Hz	1Mbit/seg
DQPSK	2símbolos/Hz	2Mbits/seg

Tabla 4.3 Velocidades de transmisión del estándar 802.11 dependiendo de la modulación empleada.

La señal DPSK recibida y demodulada se procesa de forma digital para realizar el proceso de "desensanchado". Este proceso consiste simplemente en una correlación con la secuencia Barker de 11 bits.

4.4.2 CCK (Código de Llaveo Complementario)

Las velocidades de transmisión del estándar 802.11 resultan insuficientes para aplicaciones de comunicaciones y más cuando este estándar tiene como objetivo sustituir las redes LAN cableadas por inalámbricas WLAN. La extensión IEEE 802.11b del estándar propone sistemas de modulación que consiguen velocidades de transmisión de 5.5 y 11Mbps. Éstas técnicas también se basan en DQPSK, pero no utilizan Barker para "ensanchar" el espectro. La técnica propuesta para alcanzar 5,5 y 11 Mbps es Complementary Code Keying (CCK) o opcionalmente Packet Binary Convolutional Coding (PBCC). Ambas son tecnologías propietarias de Intersil y Texas Instruments respectivamente. En esta sección se tratará la primera de ellas (CCK) [PEARSON00] y en la siguiente PBCC.

La base de CCK son las secuencias Complementarias. Éstas secuencias fueron propuestas por primera vez por M. J. Golay en 1961[Golay61].Golay estudio pares de secuencias Complementarias. Posteriormente este concepto se generalizo a Conjuntos de Secuencias Complementarias [TSENG72] y a Conjuntos de Secuencias Complementarias Multifásicas [SIVASWAMY78]. Éstas últimas son las que utiliza la técnica propuesta por Intersil: CCK.

La principal propiedad de las secuencias empleadas es que poseen una característica de autocorrelación ideal, es decir corresponde a una delta de Krönecker perfecta de modo que cumplen:

$$\phi_{11}[n]+\phi_{22}[n]+\ldots+\phi_{MM}[n]=\sum_{i=1}^{M}\phi_{ii}[n]=\begin{cases}MN & ,n=0\\ 0 & ,n\neq 0\end{cases}$$

Siendo φ_{ii} las autocorrelaciones individuales de cada una de las M secuencias complementarias, de longitud N, elegidas. Para entender mejor este concepto se puede realizar un ejemplo con las siguientes secuencias Complementarias Multifásicas:

$$s_1=\{1,j,-1,j,1\}$$
$$s_2=\{j,1,-j,1,-j\}$$
$$s_3=\{-j,1,-j,1,j\}$$
$$s_4=\{1,j,-1,j,1\}$$

Si se realiza la suma de las autocorrelaciones de las cuatro secuencias se obtiene la siguiente gráfica:

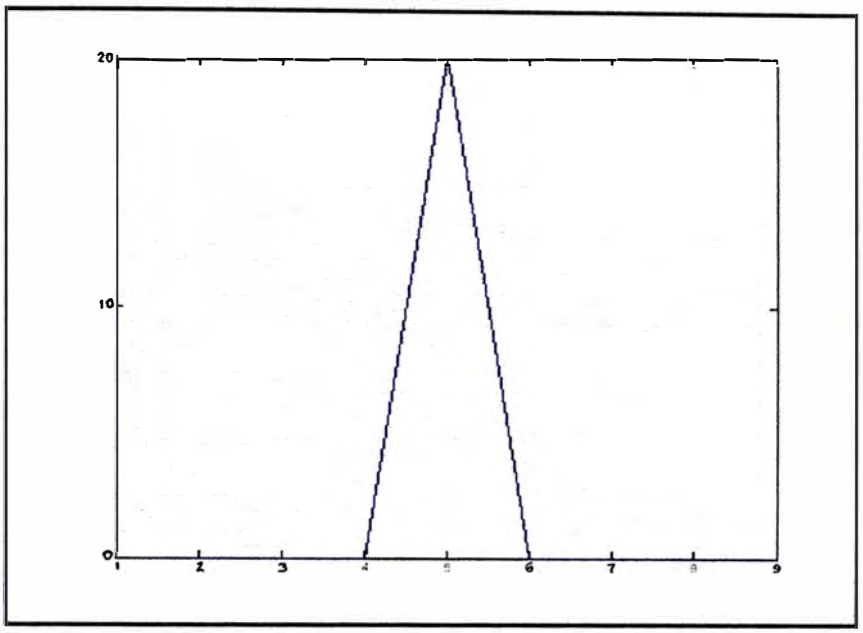


Figura 4.17: Ejemplo de detección de Secuencias Complementarias Multifásicas.

En la figura anterior se puede observar que la respuesta de este proceso es una Delta de Krönecker ideal. A diferencia de la secuencia Barker no existen lóbulos laterales y la longitud de las secuencias no está limitada a 13 bits. Esto permite conseguir Ganancias de proceso elevadas. La versión de 11Mbps de CCK trabaja con una secuencia para ensanchado de 8 chips. Con una velocidad de símbolo de 1.375Msímbolos/s la señal resultante de 11Mbps ocupa aproximadamente el mismo ancho de banda que la versión DQPSK/Barker11 del 802.11. Las Secuencias Complementarias Multifase se sintetizan con la siguiente fórmula:

$$c = \left\{ e^{j(\varphi_1+\varphi_2+\varphi_3+\varphi_4)}, e^{j(\varphi_1+\varphi_3+\varphi_4)}, e^{j(\varphi_1+\varphi_2+\varphi_4)}, -e^{j(\varphi_1+\varphi_4)}, e^{j(\varphi_1+\varphi_2+\varphi_3)}, e^{j(\varphi_1+\varphi_3)}, -e^{j(\varphi_1+\varphi_2)}, e^{j(\varphi_1)} \right\}$$

La secuencia c se divide en bloques de dos bits (dibits), que sirven para codificar las cuatro fases de modulador según la Tabla 4.4.

DIBIT	FASE
db1	φ1
db2	φ2
db3	φ3
db4	φ4

Tabla 4.4: Codificación de fase en CCK. Relación entre dibits y parámetros de fase.

Los dibits db2,db3 y db4 definen la fase de la constelación DQPSK según la Tabla 4.5. El dibit db1 define 1 mediante la siguiente expresión:

$$\varphi_1(i) = \varphi_1(i-1) + offset(db1) + \pi * (\mathrm{mod}(i,2))$$

DIBIT	FASE
00	0
01	π
10	π/2
11	-π/2

Tabla 4.5: Fase de la Constelación DQPKS según los dibits.

El resultado es que ø1 es el valor de ø1 del símbolo anterior más un offset dependiendo de la Tabla 4.6, más π radianes si el símbolo actual es un símbolo impar y 0 radianes si es par.

Una vez se han obtenido las cuatro fases ø1, ø2, ø3 y ø4, éstas se utilizan para calcular los 8 chips complejos según la Tabla 4.6. Estos chips definen las fases de la

constelación QPSK. Como ø1 introduce el mismo offset a todos los chips la modulación se convierte en DQPSK.

CHIP	FÓRMULA
0	$e^{j(\varphi_1+\varphi_2+\varphi_3+\varphi_4)}$
1	$e^{j(\varphi_1+\varphi_2+\varphi_4)}$
2	$e^{j(\varphi_1+\varphi_3+\varphi_4)}$
3	$-e^{j(\varphi_1+\varphi_4)}$
4	$e^{j(\varphi_1+\varphi_2+\varphi_3)}$
5	$e^{j(\varphi_1+\varphi_3)}$
6	$-e^{j(\varphi_1+\varphi_2)}$
7	$e^{j(\varphi_1)}$

Tabla 4.6: Correspondencia entre Chips y fases en CCK.

La versión de 5.5Mbps de CCK se modula de forma parecida a la de 11Mbps. La única diferencia es que sólo se codifican 4 bits en vez de 8. Debido a esto lo valores ø se calculan de una forma diferente. En este caso, el primer dibit también se utiliza para codificar ø1. Los ø restantes se calculan mediante los bits 3 y 4. En este caso:

$$\varphi 2=(bit3)*\pi+\ \pi/2$$
$$\varphi 3=0$$
$$\varphi 4=(bit4)*\ \pi$$

4.4.3 PBCC (Codificación Convolucional de Paquete Binario)

La extensión 802.11b también soporta la técnica opcional conocida como PBCC (Packet Binary Convolutional Coding) para alcanzar velocidades de

transmisión de 5.5Mbps y 11Mbps. Esta es una Tecnología desarrollada por la empresa Allantros y que posteriormente fue comprada por Texas Instruments.

La técnica consiste en utilizar un Codificador Convolucional que genera 2 bits por cada bit que se quiera emitir. La salida del codificador se mapea en una constelación DQPSK para velocidades de transmisión de 11Mbps y en DBPSK para 5.5Mbps.

El método de ensanchado de este método se basa en modificar la constelación DPSK basándose en una secuencia de 256 bits. Por cada símbolo que se transmite la constelación se desplaza $\pi/2$ si el bit correspondiente de la secuencia es 1.

El codificador por convolución se basa en el siguiente diagrama de bloques:

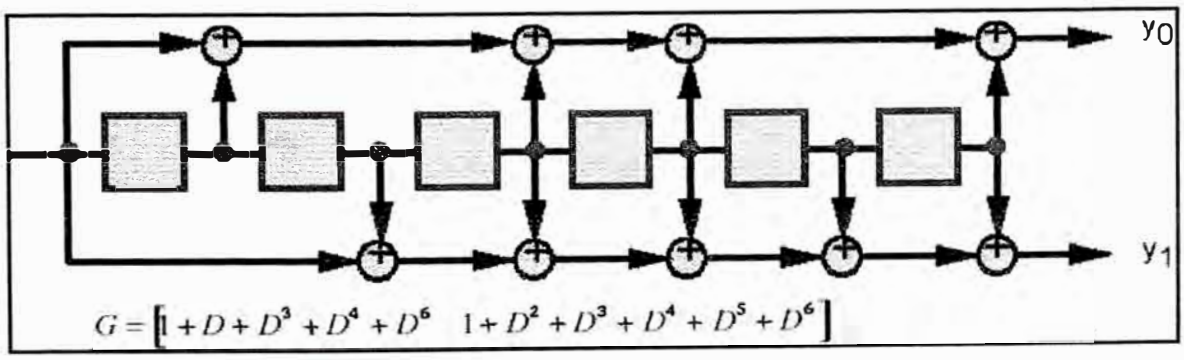


Figura 4.18: Codificador BCC.

Dependiendo del valor S(i) de la secuencia de 256 bits la constelación para transmitir cada símbolo es:

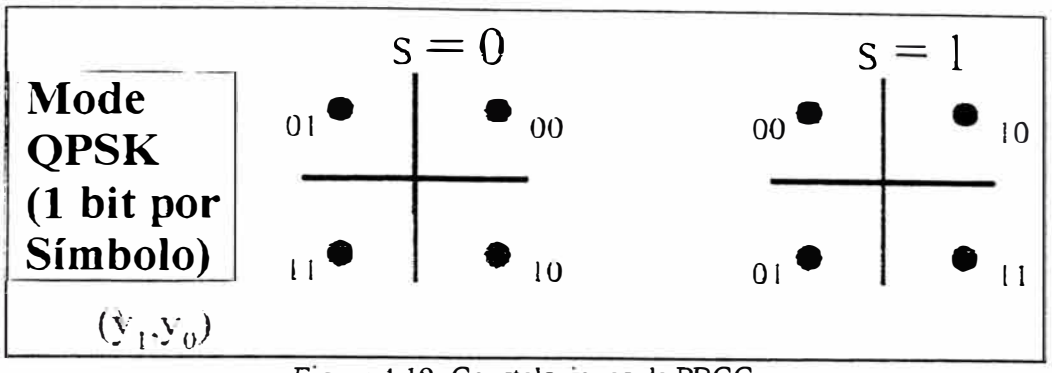


Figura 4.19: Constelaciones de PBCC.

4.5 Estado del arte del 802.11 en la actualidad

Las velocidades de transmisión en la banda de 2.4GHz propuestas por el estándar 802.11 no son suficientes para llegar a alcanzar velocidades parecidas a las de las actuales redes LAN (100Mbps). Por ello los organismos de estandarización están realizando un esfuerzo considerable por conseguir alcanzar velocidades de transmisión mayores.

El problema de alcanzar velocidades mayores es que las técnicas de modulación se vuelven más complejas. Esto influye de forma negativa sobre la relación señal ruido y por lo tanto el alcance de los radioenlaces disminuye. En la Figura 4.20, se observa como es necesaria una relación Es/No mayor para transmitir modulaciones más complejas.

Esta gráfica está sacada de la presentación del Texas Instruments al grupo WG del 802.11 [TEXAS00] y realiza una comparativa entre los métodos por el 802.11 explicados anteriormente y su nueva propuesta PBCC22 para la extensión del

estándar 802.11g que todavía está en estado de borrador y pendiente de aprobación para 2003.

Este estándar lleva por título "Further Higher-Speed Physical Layer Extension in the 2.4GHz Band" y tiene la intención de estandarizar métodos de modulación que permitan transmitir en la banda de 2.4GHz a más de 20Mbps. La idea principal se basa en utilizar la tecnología elegida para el 802.11: OFDM (Orthogonal Frecuency Division Multiplexing), pero la presión tanto de Intersil como de Texas han hecho que sus respectivas tecnologías, CCK y PBCC, también formen parte del estándar pero de modo opcional.

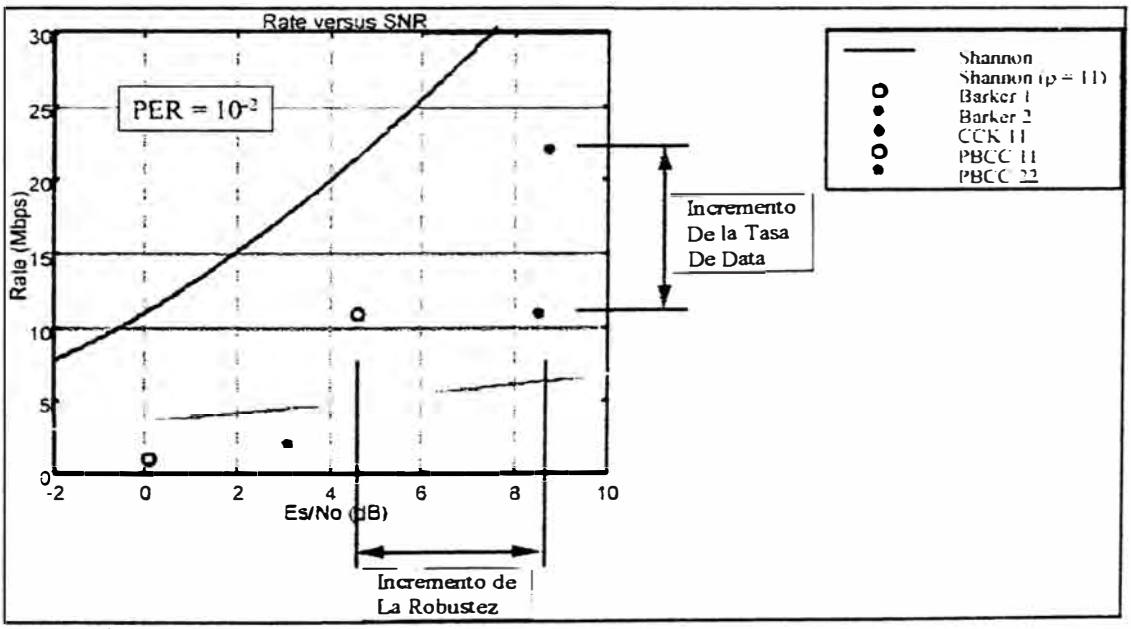


Figura 4.20: Relación entre Es/No mínima y velocidad de transmisión (Mbps).

El planteamiento es que los dispositivos que cumplan este estándar deberán implementar OFDM de manera obligatoria según el estándar 802.11a y ser

compatibles con el estándar 802.11 y su extensión 802.11b. Es decir, se podrán alcanzar velocidades de transmisión de hasta 54Mbps. Opcionalmente se podrán utilizar los siguientes métodos:

- PBCC con velocidades de transmisión de 22Mbps y 33Mbps
- CCK-OFDM con velocidades de hasta 54Mbps.

El nuevo PBCC básicamente consiste en utilizar modulaciones M-arias DMPSK. CCK- OFDM plantea utilizar un preámbulo basado en CCK antes de transmitir los datos modulados con OFDM.

4.6 Introducción al OFDM (Multiplexacion por Division de Frecuencia Ortogonal)

Para finalizar este estudio se va a hacer una breve descripción de la técnica de modulación OFDM.

OFDM consiste básicamente en dividir la banda sobre la que se trabaja en distintas sub-bandas más pequeñas (Figura 4.21). Los datos se multiplexan y se modulan en BPSK, QPSK o QASK. La ventaja es que cada sub-banda se puede tratar de forma independiente. De esta forma, se pueden realizar un tratamiento independiente en cada sub-banda.

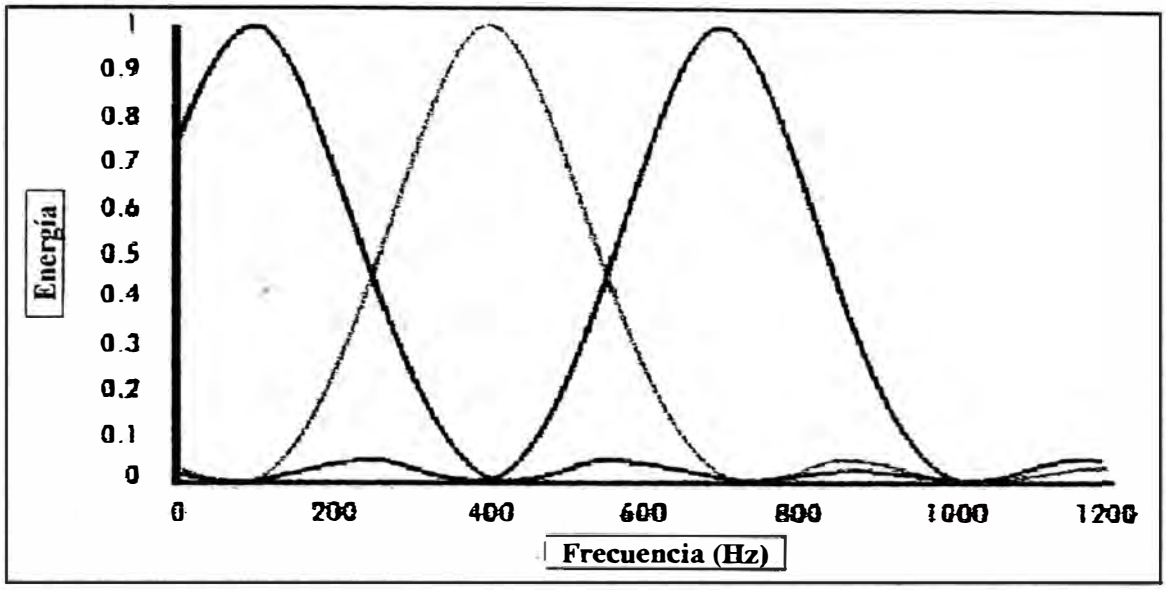


Figura 4.23: Ejemplo de OFDM.

El proceso de modulación/demodulación se basa en la transformada rápida de Fourier (FFT). Ver Figura 4.24. El sistema realiza una transformada inversa (IFFT) en el transmisor y la transformada directa (FFT) en el receptor.

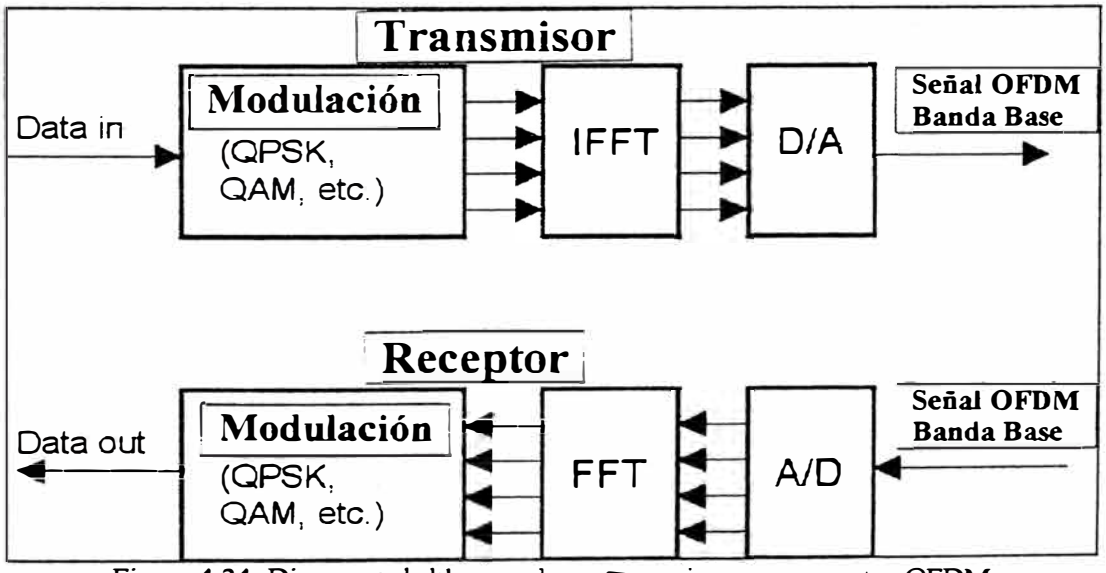


Figura 4.24: Diagrama de bloques de un transmisor y un receptor OFDM

El principal problema de esta técnica reside en que la señal resultante de la modulación tiene un factor PMEPR (Peak-to-Mean Power Power Ratio) muy elevado [DAVIS97]. Esto se debe a que si las señales que se encuentran en cada una de las sub-bandas se encuentran en fase se produce un pico de señal elevado y si se encuentran en contrafase se contrarrestan se anulan. Este efecto tiene consecuencias negativas sobre los sistemas de RF.

CONCLUSIONES

Las velocidades de transmisión en la banda de 2.4GHz propuestas por el estándar 802.11 no son suficientes para llegar a alcanzar velocidades parecidas a las de las actuales redes LAN. Por ello los organismos de estandarización están realizando un esfuerzo considerable por conseguir alcanzar velocidades de transmisión mayores.

Diferentes estudios sobre el algoritmo CSMA/CA para cada uno de los diferentes medios físicos demuestran que, si bien para carga baja se comportan de manera similar, a carga alta el medio infrarrojo se comporta mejor que el DSSS, y éste a su vez mejor que el FHSS, pero cuando nos movemos en condiciones de propagación ideales. En cambio, la introducción de un retardo sitúa a FHSS como la mejor solución, seguida de DSSS e IR.

Desde el punto de vista de la seguridad, se ha criticado mucho el algoritmo WEP de encriptación y actualmente se están utilizando otro tipo de soluciones a nivel más alto de capa. Parece ser que aunque la encriptación se haya modificado para el uso de claves de 128bits, el algoritmo utiliza cuatro claves de cifrado, lo cual hace sencillo el hacking y cracking por un intruso.

La importancia de tener una red inalámbrica totalmente comunicada entre todas las estaciones que la conforman es muy alta, ya que al no tener una buena comunicación entre ellas mismas, se generan problemas en la red, como colisiones, pérdidas y retrasos de paquetes. El análisis del lugar en que se deberá instalar la red debe de garantizar una buena comunicación entre las estaciones que conforman el BSS, evitando que dos o más estaciones pertenecientes al mismo BSS transmitan simultáneamente por no "escucharse" entre ellas mismas.

El efecto de captura en el análisis de una red LAN inalámbrica es importante, dado que de ello depende en parte el buen funcionamiento de la misma. Al no tener un efecto de captura adecuado, las pérdidas en la red se incrementan ya que una estación al recibir mas de un paquete debe de tomar solo uno y destruir el resto, o destruir ambos paquetes, ocasionando por un lado pérdidas por los paquetes destruidos y por otro lado retraso porque estos paquetes destruidos se deben de retransmitir nuevamente. El efecto que produce el considerar las estaciones ocultas es de igual importancia, debido a que contribuyen con tráfico que se introduce en la red al transmitir paquetes de información.

El problema de alcanzar velocidades mayores es que las técnicas de modulación se vuelven más complejas. Esto influye de forma negativa sobre la relación señal ruido y por lo tanto el alcance de los radio enlaces disminuye. En la figura 4.20, se observa como es necesaria una relación Es/No mayor para transmitir modulaciones más complejas.

GLOSARIO

AP	Punto de Acceso
BACKBONE	Nivel máximo de una red jerárquica
BSS	Grupo de Servicio Básico
CCK	Código de Llaveo Complementario
CF	Fin de Período Libre de Contienda
CFP	Período Libre de Contienda
CFP	Duración Máxima del Período Libre de Contienda
CHIP	Patrón redundante generado por cada bit que se transmite usando las técnicas de transmisión DSSS, de manera que en caso de pérdida de información ésta pueda ser recuperada, con ello se consigue que sea más resistente a cualquier interferencia.
CTS	Permiso para enviar
CSMA/CD	Acceso Múltiple por detección de Portadora con Detención de Colisiones

CSMA/CA	Acceso Múltiple por detección de Portadora Evitando Colisiones
DBPSK	Modulación de Fase Diferencial Binaria
DCF	Función de Coordinación Distribuida
DIBITS	Bloques de dos Bits
DIFS	Espacio entre marco en la Función de Función Distribuida
DPSK	Codificación de Fase Diferencial Desplazada
DQPSK	Modulación de Fase Diferencial en Cuadratura
DSSS	Secuencia Directa mediante Espectro Esparcido
DTIM	Mensaje de Indicación de entrega de Tráfico
ETHERNET	Red de área local con topología bus y velocidad de 10 Mbps sobre cable coaxial, que sigue la norma IEEE 802.3, utilizando el protocolo CSMA/CD.
ETSI	Instituto Europeo de Estándares en Telecomunicaciones
FDDI	Interfaz de Datos sobre Fibra Óptica
FHSS	Saltos en Frecuencia mediante Espectro Esparcido
FIFO	Primero en entrar primero en salir
GFSK	Modulación en Frecuencia con filtros Gausianos
IEEE	Instituto de Ingenieros de Electricidad y Electrónica
IFS	Espacio entre marcos
IR	Infrarrojo
MAC	Subcapa de Control de Acceso al Medio
MAN	Redes de Área Extensa

NAV	Vector de asignación de red
OFDM	Múltiplexación por División de Frecuencia Ortogonal
PBCC	Codificación Convolucional de Paquete Binario
PC	Punto de Coordinación
PCF	Función de Punto de Coordinación
PHY	Capa Física
PIFS	Espacio entre marco en la Función de Punto de Coordinación
PMEPR	Nivel de Potencia
QoS	Calidad de Servicio
RF	Radio Frecuencia
RTS	Petición de envío
SIFS	Espacio entre marco corto
STP	Cable de par Trenzado Apantallado
UTP	Cable de par Trenzado sin Apantallar
WLAN	Redes inalámbricas de Área Local
WPAN	Redes Personales Inalámbricas

BIBLIOGRAFÍA

[1] Benjamin E. Henty. "A Brief Tutorial on the PHY and MAC layers of the IEEE 802.11b Standard" July 12, 2001.

[2] "Transmisión Digital" F.J. Martínez Zaldivar, J.R. Vidal Catalá. Editorial de la universidad Politécnica de Valencia.

[3] "Digital Modulation and coding", Stephen G. Wilson. Prentice Hall.

[4] "Discrete-Time Signal Processing" Alan V. Oppenheim and Ronald W. Schafer. Prentice Hall.

[5] [ISO/IEC 8802.11] International Standard ISO/IEC 8802-11 IEEE P802.11, 1999

[6] [IEEE802.11] IEEE Std 802.11-1997

[7] [IEEE802.11b] IEEE Std 802.11b-1999 (Supplement to ISO/IEEE Std 802.11, 1999)

[8] [IEEE802.11a] IEEE Std 802.11a-1999 (Supplement to IEEE Std 802.11-1999)

[9] [IEEE802.11g] IEEE Std 802.11g/D2.1, January 2002 (Supplement to IEEE Std 802.11, 1999)

[10] [ETSI99] ETR0230002 V0.2.0 (1999-04) Broadband Radio Access Networks (BRAN); High Performance Radio Local Area Networks (HIPERLAN) Type 2; System Overview (www.etsi.org)

[11] [CNAF98] Cuadro Nacional de Atribución de Frecuencias (CNAF). Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información (SETSI). Ministerio de Ciencia y Tecnología. http://www.setsi.mcyt.es/espectro/tablas_cnaf/bandasfr.htm (según BOE Suplemento nº 193 · 13/8/98 · ORDEN de 22 de julio de 1998).

[12] [CNAF02] BOE 070-2002 (Pág. 11674 a 11842)- ORDEN CTE/630/2002, de 14 de marzo, por la que se aprueba el Cuadro Nacional de Atribución de Frecuencias (CNAF). MINISTERIO DE CIENCIA Y TECNOLOGÍA 22/03/2002

[13] [TSENG72] Tseng, C.-C. and Liu, C.L.: " Complementary Sets of Sequences" , IEEE Trans. Inform. Theory, vol. IT-18, No. 5, pp. 644-652, Sep. 1972.

[14] [GOLAY61] Golay, M.J.E.: 'Complementary series', *IRE Trans.*, 1961, IT-7, pp. 82-87.

[15] [SIVASWAMY78] Sivaswamy, R. "Multiphase Complementary Codes", IEEE Trans. On Information Theory, vol. IT-24, No.5. Sept. 1978, p.546-552

[16] [PEARSON00] Pearson, B., "Complementary Code Keying Made Simple", Intersil Application Note. AN9850.1. May 2000

[17] [TEXAS00] "Texas Instruments Proposal for IEEE 802.11g High-Rate Standard", Heegard, Rossin, Shoemake, Coffey, and Batra. doc.: IEEE 802.11-00/384

[18] [DAVIS97] Davis. A, Jedwab. J "Peak-to-Mean control in OFDM, Golay complementary Sequences and Reed-Muller Codes" HP Laboratories Bristol. HPL-97-158. December,1997

[19] **Chen** Kwang-Cheng, 1994, "Medium Access Control of Wireless LANs for Mobile Computing", IEEE Network, 50-62.

[20] **Hadzi -Velkov** Zoran and Gavrilovska Liljana, 1999, "Performance of the IEEE 802.11 Wireless LANs Under Influence of Hiden Terminals and Pareto Distributed Packet Traffic", IEEE Communication magazine, 221- 225

[21] **LaMaire** Richard O., Krishna Arvind and Bhagwat Pravin, IBM James Panian, ericson Inc., 1996, "Wireless LANs and Mobile Networking: Standards and future Directions", IEEE Communications Magazine,86-94 p.

[22] **Pahlavan** Kaveh, Zahedi Ali and Krishnamurthy Prashant, 1997, "Wideband Local Access: Wireless LAN and Wireless ATM", IEEE Communications Magazine, 34-40 p.

[23] **Taylor** Jack T., Omura Jim K., Cylink Corporation, 1991, "Spread Spectrum Technology: A Solution to the Personal Communications Services Frequency Allocation Dilemma", IEEE communications magazine, 48-51.

[24] **Viterbi** Andrew J., 1995, "CDMA Principles of Spread Spectrum Communication", Addison Wesley Wireless Communication Series, Addison Wesley Publishing Company, 3 era Edicion, Reading Massachusetts, 670 p.

[25] **Wolisz** A., Schlaeger M., Weinmiller J., Woesner H., 1996, "Wireless Access to High Speed Networks, High-Speed Networking for Multimedia Applications", W. Effelsberg, O. Spaniol, A. Danthine, D. Ferrari , Kluwer Academic Publishers, 1-21 p.