Nº5 | NUEVAS TECNOLOGÍAS | JULIO 2008

TECNOLOGÍA Wi-Fi

Autores: Ing. Ricardo Alberto ANDRADE
Ing. Pablo Hernán SALAS
Ing. Daniel SANTOS PAREDES

COORDINACION DE LAS PUBLICACIONES:
Ing. Guillermo Clemente | Ing. Guillermo Montenegro

DISEÑO Y DIAGRAMACIÓN:
Aixa Sacco | Área de Comunicaciones e Imagen Corporativa

ISBN 978-987-24110-6-0
Hecho el depósito que marca la Ley Nº 11.723
Primera Edición: 2000 ejemplares
Buenos Aires, Julio de 2008

NÓMINA DE AUTORIDADES

PRESIDENTA DE LA NACIÓN
Dra. Cristina Fernández

MINISTRO DE PLANIFICACIÓN FEDERAL, INVERSIÓN PÚBLICA Y SERVICIOS
Arq. Julio Miguel De Vido

SECRETARIO DE COMUNICACIONES
Arq. Carlos Lisandro Salas

COMISIÓN NACIONAL DE COMUNICACIONES

INTERVENTOR
Ing. Ceferino Alberto Namuncurá

UNIDAD DE AUDITORÍA INTERNA
Cr. Carlos Alberto Bonomi

GERENCIA DE CONTROL
Dr. Silvio De Diego

GERENCIA DE INGENIERÍA
Ing. Guillermo Clemente | Ing. Carlos Gainza

GERENCIA DE SERVICIOS POSTALES
Dr. Alfredo Javier Pérez

GERENCIA DE RELACIONES INTERNACIONALES E INSTITUCIONALES
Lic. Sergio Scarabino | Lic. Néstor Chumbita

GERENCIA DE ADMINISTRACIÓN DE RECURSOS
Lic. Horacio José Trucco

GERENCIA DE ASUNTOS JURÍDICOS Y NORMAS REGULATORIAS
Dra. Juvina Inés Intelángelo de Ten

COORDINACIÓN DE CENTROS DE COMPROBACIÓN TÉCNICA DE EMISIONES
Ing. Victor Daniel Frizzera

ÍNDICE

PRÓLOGO

En consonancia con los lineamientos trazados desde el Gobierno Nacional y el Ministerio de Planificación Federal, Inversión Pública y Servicios, tendientes a promover una política social estratégica que posibilite recuperar la participación del Estado en la formulación de políticas e instrumentos de crecimiento, inclusión y desarrollo social, desde que comenzó nuestra gestión, en la CNC hemos ido desarrollando una serie de prácticas y actividades tendientes a construir un nuevo paradigma en cuanto al rol del Organismo en su relación con la sociedad.

Durante estos años hemos implementado diversos proyectos con el objetivo de mejorar los sistemas de información y comunicación, habilitar mecanismos de participación ciudadana, hacer más eficientes los procedimientos administrativos y de resolución de reclamos y diseñar nuevas estrategias de control en materia de Telecomunicaciones, Espectro Radioeléctrico y Postales, demostrando que es posible lograr una gestión pública con altos niveles de calidad y eficiencia, generando una mayor capacidad de control, optimizando recursos, desarrollando investigaciones, innovando tecnológicamente y redefiniendo las relaciones con los distintos actores sociales involucrados.

Dentro de este marco de mejores prácticas encaradas durante la actual gestión, una de las acciones fundamentales que nos hemos propuesto fue la generación y transferencia de conocimientos, impulsando, entre otros proyectos: Convenios de Cooperación para el desarrollo de nuevas tecnologías y aplicaciones con la Comisión Nacional de Actividades Espaciales, CONAE;

PRÓLOGO

un Proyecto de Indicadores del Mercado de Telecomunicaciones, a efectos de disponer de información actualizada, consistente y confiable que permita reflejar el estado del sector, así como configurar un instrumento de gran valor estratégico para la gestión, planificación y control del mercado; la implementación de un Programa Federal de Capacitación a Cooperativas que prestan servicios de telecomunicaciones, informando acerca de los requerimientos, condiciones y posibilidades regulatorias y técnicas existentes, contribuyendo a mejorar la calidad de los servicios que prestan y a promover la competencia; y el desarrollo de una serie de investigaciones con el objetivo de aportar información sobre la materia en función de ciertas preocupaciones detectadas en distintos sectores sociales, tal el tema de las radiaciones no ionizantes, el emplazamiento de antenas y el reciclado y tratamiento de residuos electrónicos.

Es dentro de este contexto donde se encuadra la presente colección sobre nuevas tecnologías en el ámbito de las telecomunicaciones, conformada por 10 investigaciones realizadas por un grupo de estudio interdisciplinario, con el objetivo de brindar información actualizada a distintos actores acerca de los diversos avances tecnológicos y sus posibilidades de implementación, dotándolos de nuevas herramientas y conocimientos a fin de poder mejorar y ampliar los variados servicios de telecomunicaciones.

PRÓLOGO

El desarrollo de estas investigaciones es posible gracias al formidable capital humano con que contamos en nuestro Organismo, altamente capacitado, en constante formación y con amplia predisposición y voluntad para compartir y transmitir sus conocimientos y experiencias en la materia.

La conformación de grupos de estudio se prevé que sea extendida a otras áreas del Organismo, a fin de investigar y divulgar sobre diversas temáticas de interés tanto particular, para el mercado de telecomunicaciones, como general, para la sociedad en su conjunto, pues consideramos que el desarrollo de investigaciones propias constituye una obligación y una responsabilidad para el Estado en tanto es un instrumento para mejorar las condiciones sociales de nuestra población, y, en particular para nuestro Organismo, con el propósito de facilitar y promover el acceso a las telecomunicaciones, a la información y al conocimiento.

Ing. Ceferino Namuncurá
INTERVENTOR
COMISIÓN NACIONAL DE COMUNICACIONES

INTRODUCCIÓN

Wi-Fi es un conjunto de estándares para redes inalámbricas (WLAN) basadas en las especificaciones IEEE 802.11 del Instituto de Ingenieros en Electricidad y Electrónica (IEEE).

El estándar IEEE 802.11 fue diseñado para sustituir a las capas: físicas (PHY) y de acceso al medio (MAC) del estándar IEEE 802.3 (Ethernet). En lo único que se diferencia una red Wi-Fi de una red Ethernet es en la forma en que los terminales acceden a la red, siendo totalmente compatibles en todos los demás servicios.

Existen tres tipos de redes Wi-Fi, cada una de ellas basadas en un estándar 802.11 aprobadas por el IEEE. Un cuarto estándar, el 802.11n, está siendo elaborado y se esperaba su aprobación final para la segunda mitad del año 2008, mas viene demorada.

Los estándares IEEE 802.11b e IEEE 802.11g poseen una aceptación internacional debido a que la banda de 2,4 GHz está disponible casi universalmente, con una velocidad de hasta 11 Mbps y 54 Mbps, respectivamente. Existe también un primer borrador del estándar IEEE 802.11n que trabaja en la banda de 2,4 GHz a una velocidad de 108 Mbps, que bien puede alcanzarse ya con el estándar 802.11g gracias a técnicas propietarias de aceleramiento que consiguen duplicar la velocidad de transferencia de datos teórica. Actualmente existen ciertos dispositivos que permiten utilizar esta tecnología, denominados Pre-N, sin embargo, no se sabe si serán compatibles, ya que el estándar no está completamente revisado y aprobado.

INTRODUCCIÓN

También existe el estándar IEEE 802.11a, conocido como Wi-Fi 5, que opera en la banda de 5 GHz donde existen canales relativamente limpios. En dicha banda no existen otras tecnologías (*Bluetooth*, microondas, *ZigBee*, etc.) que la estén utilizando, por lo tanto hay muy pocas interferencias.

Las redes inalámbricas son un excelente complemento a las redes fijas, las cuales no representan un reemplazo de tecnología, sino que las mismas complementan a las redes fijas proveyendo movilidad a los usuarios, mientras servidores y equipamientos de centros de datos se encuentran cableados y en lugares fijos.

En definitiva el grupo de trabajo del 802.11 intenta crear un estándar que permitirá la interconexión a alta velocidad de dispositivos electrónicos de consumo masivo por medio inalámbrico.

CAPÍTULO I
REDES INALÁMBRICAS Wi-Fi

I.1 LA FAMILIA IEEE 802

El estándar IEEE 802.11 es miembro de la familia IEEE 802, el cual es una serie de especificaciones para tecnología de redes de área local (LAN). La figura I.1 muestra la relación entre los varios componentes de la familia 802 y su lugar en el modelo OSI.

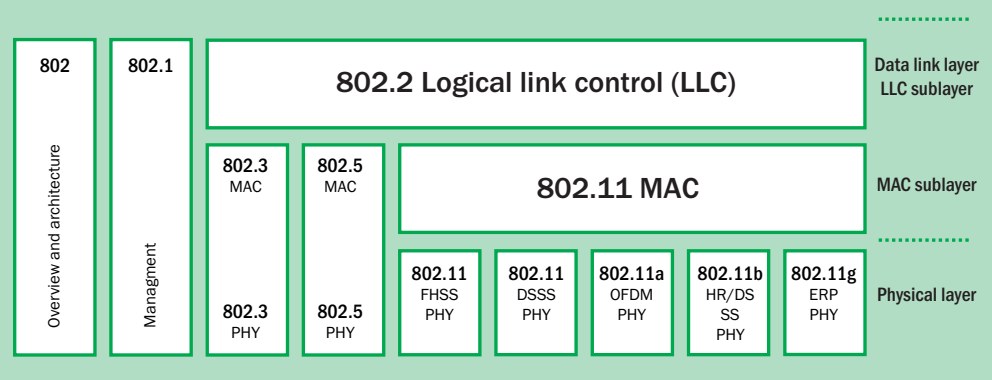


Figura I.1

Las especificaciones IEEE 802 son enfocadas sobre las dos capas inferiores del modelo OSI: capa física (PHY) y capa de enlace de datos, en particular la subcapa de acceso al medio (MAC). La capa MAC es el conjunto de reglas que determinan cómo acceder al medio y enviar datos, pero detalles de transmisión y recepción son llevados por la capa PHY.

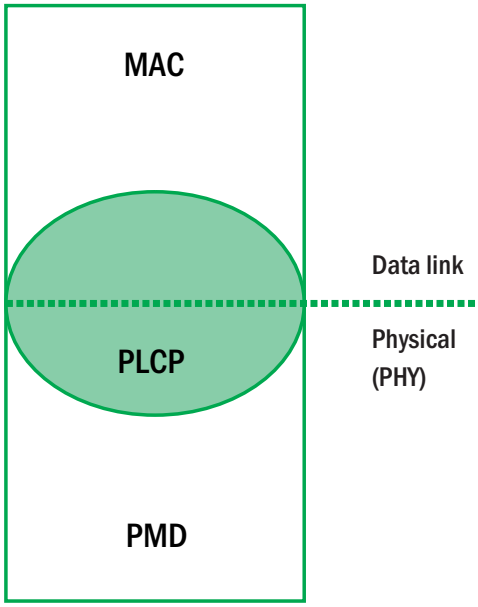
De la figura I.1 puede observarse que las especificaciones 802.11 incluyen las capas MAC y dos capas PHY: espectro ensanchado por salto de frecuencia (FHSS) y espectro ensanchado por secuencia

CAPÍTULO I

directa (DSSS). Las revisiones posteriores al 802.11 han variado la capa física: solamente así tenemos 802.11b con espectro ensanchado por secuencia directa de alta tasa (HR/DSSS), 802.11a y 802.11g con una capa física basada en la técnica de multiplexación por división de frecuencias ortogonales (OFDM), pero utilizando distintas porciones del espectro radioeléctrico.

Debido a la complejidad de la capa PHY, el estándar 802.11 la divide en dos componentes: Procedimiento de convergencia de la capa física - *Physical Layer Convergence Procedure* (PLCP) para mapear las tramas MAC sobre el medio, y un sistema dependiente del medio físico - *Physical Medium Dependent* (PMD) para transmitir estas tramas. La figura I.2 muestra un esquema de los componentes de la capa física.

Figura I.2



CAPÍTULO I

I.2 ESTRUCTURA DE RED

I.2.1 ARQUITECTURA

Las redes Wi-Fi están compuestas por cuatros elementos (figura I.3). Estos son:

ESTACIONES

Las redes son construidas para transferir datos entre estaciones. Las estaciones son dispositivos de computación con interfaces de redes inalámbricas. Típicamente son *laptops* o computadoras de mano operadas con baterías permitiendo movilidad. En general, una estación es cualquier dispositivo electrónico de consumo que pueda hablar el estándar 802.11.

PUNTO DE ACCESO (*ACCESS POINT* - AP)

Es el dispositivo puente que permite la interconexión entre los dispositivos inalámbricos y las redes fijas o de distribución.

MEDIO INALÁMBRICO

Para la transmisión de datos los estándares utilizan el medio inalámbrico y definen diferentes métodos de modulación para lograrlo. Entre ellos se encuentran las señales de radio y las emisiones por infrarrojo.

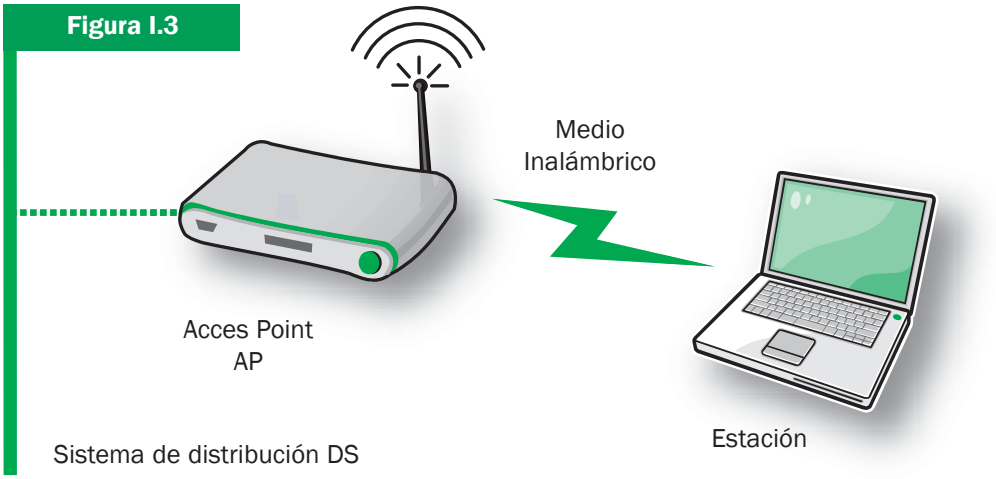
SISTEMA DE DISTRIBUCIÓN

Los Puntos de Accesos (APs) son conectados a sistemas de distribución que permiten una mayor área de cobertura, en consecuencia le

CAPÍTULO I

da mayor movilidad a las estaciones. Cabe aclarar que el estándar 802.11 no específica una tecnología en particular para el sistema de distribución. En productos comerciales el sistema de distribución es implementado de manera de interconectar los distintos APs configurando el *backbone* de la red. Ethernet es la tecnología usada mayormente para la red de *backbone*.

Figura I.3



I.2.2 TIPOS DE REDES

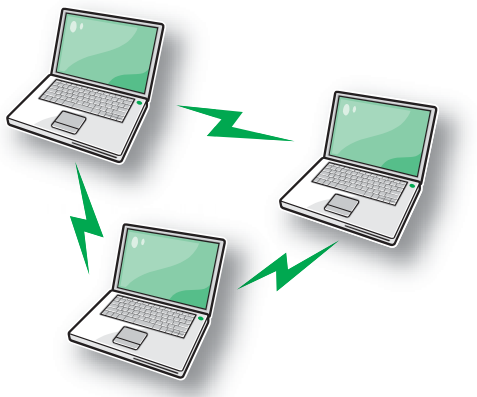
El Conjunto de Servicios Básicos de una red 802.11 es simplemente un grupo de estaciones que se comunican unas con otras, la comunicación toma lugar en un área difusa, llamada área de servicio básico (BSS), definida por la característica de propagación del medio inalámbrico. Cuando una estación está en un área de servicio básica, ésta puede comunicarse con los otros miembros de la BSS.

CAPÍTULO I

Las BSSs pueden darse de dos maneras: independientes o de infraestructura.

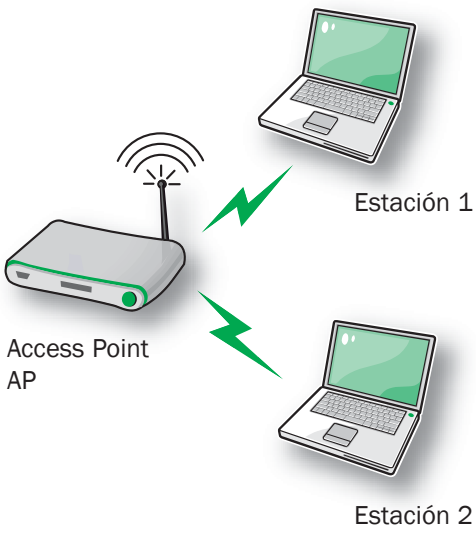
En las *BSSs independientes o ad hoc* (IBSSs) cada estación se comunica directamente con cualquier otra. La menor red posible es un IBSS con dos estaciones. Generalmente, las IBSSs están formadas de un número pequeño de estaciones para un propósito dado y para un corto período de tiempo. Un ejemplo de red IBSS puede observarse en la figura I.4.

Figura I.4



Las redes de infraestructura de BSS, son distinguidas por el uso de un Punto de Acceso (AP). Los APs son usados para todas las comunicaciones incluyendo las comunicaciones entre nodos móviles en la misma área de servicio. Si una estación móvil necesita comunicarse con otra estación móvil la comunicación debe pasar por el AP produciéndose dos saltos en la misma, como se muestra en la figura I.5.

Figura I.5



CAPÍTULO I

En una *red de infraestructura,* las estaciones deben asociarse con un AP para obtener los servicios de red. La asociación no es un proceso simétrico, las estaciones móviles siempre inicializan el proceso de asociación, y el AP acepta o deniega basándose en el contenido del requerimiento de asociación.

Las BSSs pueden crear cobertura en pequeñas oficinas y hogares, pero éstas no pueden proveer cobertura a grandes áreas. Para poder lograr coberturas importantes el 802.11 permite el enlazado de varias BSS a través de una red *backbone*, extendiendo el conjunto de servicios a un área de servicio extendida (ESS). Todos los AP dentro de un ESS tienen el mismo identificador de conjuntos de servicios [*service set identifier* - SSID] sirviendo como un nombre de red para los usuarios. En la figura I.6 se muestra un ejemplo de ESS.

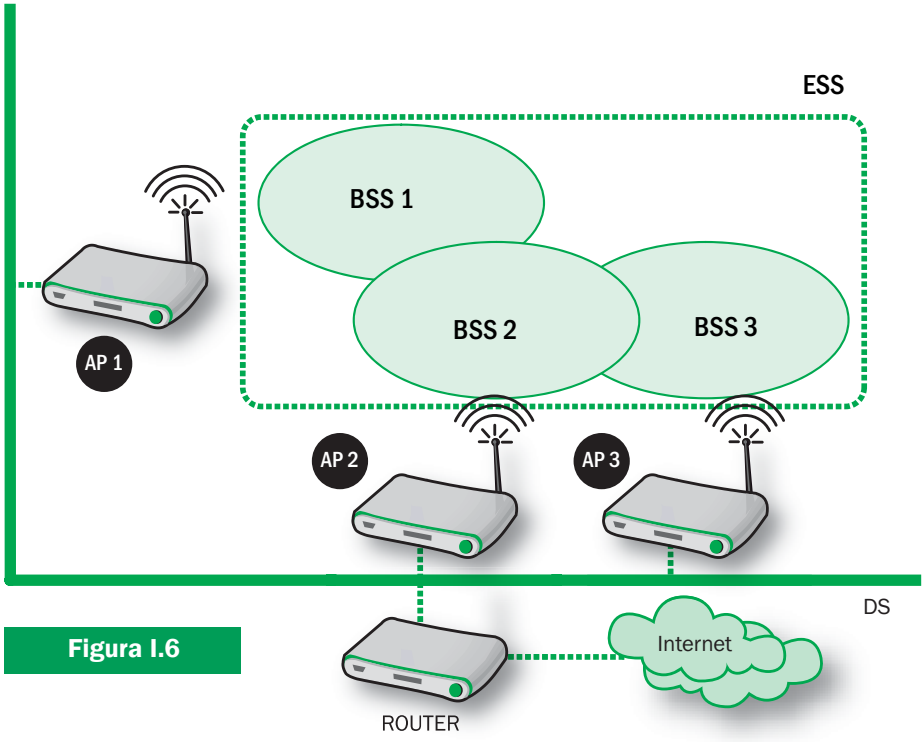


Figura I.6

CAPÍTULO I

802.11 no específica una tecnología de *backbone* en especial, solamente requiere que la misma maneje un conjunto de servicios específicos.

I.2.3 SERVICIOS DE RED

Una forma de definir una tecnología de red es definir los servicios que ésta ofrece y que permita que equipos de distintos fabricantes puedan implementarlos. Estos servicios son descriptos a continuación:

DISTRIBUCIÓN

Este servicio es usado por las estaciones móviles en una red de infraestructura cada vez que se envían datos. Una vez que una trama ha sido aceptada por un AP, éste usa el sistema de distribución para despachar la trama al destino. Cualquier comunicación que use un AP viaja a través del servicio de distribución, incluyendo comunicaciones entre dos estaciones móviles asociadas con el mismo AP.

INTEGRACIÓN

Es un servicio provisto por el sistema de distribución. Permite la conexión del sistema de distribución a una red que no sea IEEE 802. 11.

ASOCIACIÓN

Es el servicio por el cual una estación pide ser reconocida por un AP. El envío de tramas a las estaciones móviles es posible porque las estaciones se registran, o asocian, con el AP. Una estación sólo puede estar asociada a un AP por vez.

CAPÍTULO I

REASOCIACIÓN

Cuando una estación móvil se mueve entre BSSs dentro de un ESS evalúa la intensidad de señal recibida y pide la asociación a otro AP. Las reasociaciones son iniciadas por la estación móvil cuando las condiciones de señal recibida indican que una asociación diferente puede beneficiarla. Luego que la reasociación es completada, el sistema de distribución actualiza su registro de localización reflejando la accesibilidad de las estaciones móviles a través de diferentes APs.

DESASOCIACIÓN

Este servicio, como su nombre lo indica, permite terminar una asociación existente por parte de una estación móvil. Cuando una estación móvil invoca el servicio de desasociación cualquier dato cargado en el sistema de distribución es removido.

AUTENTICACIÓN

La seguridad es uno de los componentes más importantes de una solución basada en una LAN inalámbrica (WLAN) donde cualquiera podría inferir en los datos que se transmiten por el medio inalámbrico. Por su concepción las redes inalámbricas no pueden ofrecer el mismo nivel de seguridad que una red LAN cableada, y por lo tanto debe depender de rutinas de autenticación adicionales para asegurar que los usuarios que acceden se encuentren autorizados. La autenticación es un prerrequisito necesario para la asociación porque solamente usuarios autenticados son autorizados a usar la red. La misma puede ocurrir varias veces durante la conexión de un cliente a una WLAN.

CAPÍTULO I

DEAUTENTICACIÓN

Este servicio permite terminar una autenticación. Un efecto de la deautenticación es terminar con cualquier asociación.

PRIVACIDAD

Este servicio permite tener la confidencialidad de los datos, evitando que estaciones no habilitadas ingresen a la WLAN.

CONTROL DE POTENCIA EN TRANSMISIÓN (*TRANSMIT POWER CONTROL* - TPC)

TPC es un servicio nuevo que fue definido por 802.11h para la banda de 5 GHz requiriendo control de potencia para evitar interferencia con otros usuarios en dicha banda y también permitiendo el ahorro de energía en las estaciones móviles, obteniéndose una mayor duración de la batería.

SELECCIÓN DINÁMICA DE FRECUENCIA (*DYNAMIC FREQUENCY SELECTION* - DFS)

Algunos sistemas de radares operan en el rango de 5 GHz principalmente en países de Europa. Como resultado, algunas autoridades regulatorias han encomendado que estas WLAN deben detectar los sistemas de radar y mover sus frecuencias a otras no usadas por los mismos.

CAPÍTULO I

I.2.4 SOPORTE DE MOVILIDAD

La movilidad es la primera motivación para el desarrollo de las redes 802.11. Este estándar provee movilidad entre áreas de servicios básicas en la capa de enlace de datos. Existen tres tipos de transiciones entre puntos de accesos (APs).

NO TRANSICIÓN

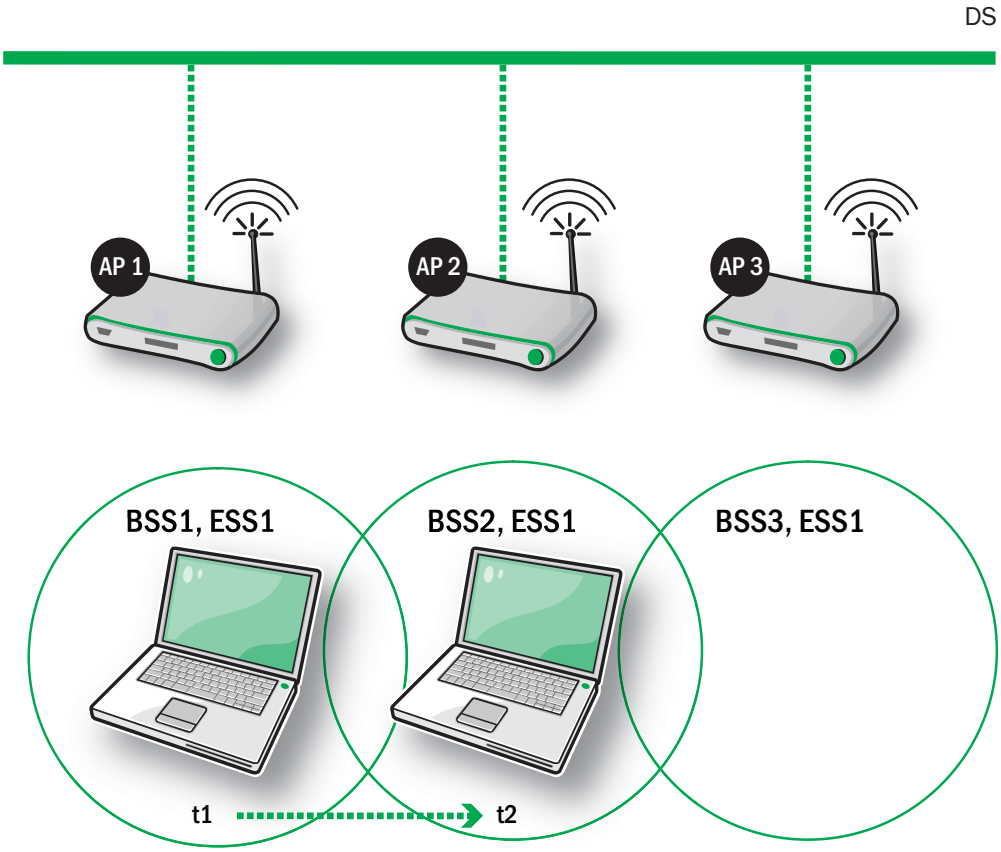
Cuando la estación no se mueve del área de servicio de su AP no es necesaria una transición, esto ocurre porque la estación se encuentra dentro del área de servicio de su AP.

TRANSICIÓN BSS

Este proceso es ilustrado en la figura I.7, los tres APs están asignados al mismo ESS. En el tiempo t1, la estación móvil se encuentra asociados al AP1 y un tiempo posterior, t2, se produce la transición de BSS y la estación móvil se reasocia con el AP2. Cabe aclarar que 802.11 no especifica los detalles de la comunicación entre los APs durante una transición de BSS.

CAPÍTULO I

Figura I.7

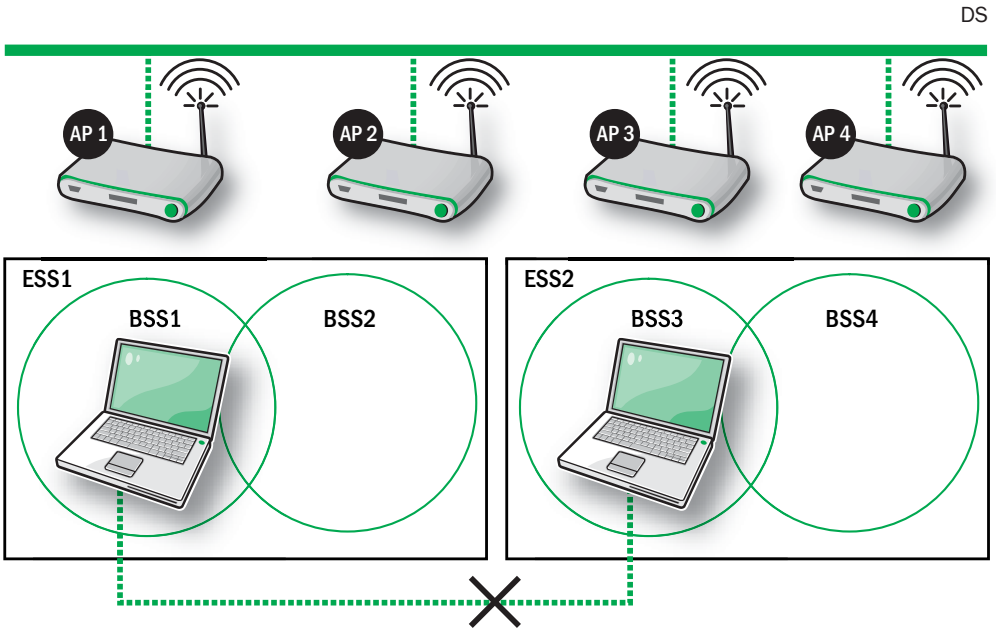


CAPÍTULO I

TRANSICIÓN ESS

Este proceso se refiere al movimiento desde un ESS a otro distinto. Las redes 802.11 no soportan este tipo de transiciones. La figura I.8 ilustra una transición de ESS. Cuatro BSSs están organizadas en dos ESSs. La continuidad de la conexión en la transición no es soportada por el estándar, por lo que la estación móvil no podrá reasociarse a la ESS2 rápidamente. Para el mantenimiento de la comunicación es necesario de protocolos de capas superiores como puede ser el caso de Mobile IP para la *suite* de protocolos de TCP/IP.

Figura I.8



Transición no soportada

CAPÍTULO II
CAPA DE ACCESO AL MEDIO (MAC) Y FÍSICA (PHY)

II.1 CONTROL DE ACCESO AL MEDIO (MAC)

De acuerdo con la familia de estándares IEEE 802 la subcapa de Control de Acceso al Medio (*Media Access Control* - MAC) se sitúa en la parte inferior de la capa de enlace de datos (Capa 2 del Modelo de Referencia OSI). La subcapa MAC puede variar dependiendo de los requerimientos de la capa física (por ejemplo: Ethernet, Token Ring, WLAN).

Algunas de las funciones de la subcapa MAC incluyen:

- Agregar la dirección MAC del nodo fuente y del nodo destino en cada una de las tramas que se transmiten.
- Al transmitir el origen debe delimitar las tramas agregando bits de bandera (*flag*s) para que el receptor pueda reconocer el inicio y fin de cada trama.
- Al recibir en destino debe determinar el inicio y el final de una trama de datos dentro de una cadena de bits recibidos por la capa física.
- Efectuar detección (y corrección si corresponde) de errores de transmisión.
- Descartar tramas duplicadas o erróneas.
- Controlar el acceso al medio físico de transmisión por parte de los dispositivos que comparten el mismo canal de comunicación.

El estándar 802.11 adapta el control de acceso al medio cableado utilizado por Ethernet al medio inalámbrico. Para el caso de Ethernet el control de acceso al medio es realizado a través de la técnica CSMA/CD (Acceso Múltiple por Sensado de Portadora con Detección

CAPÍTULO II

de Colisiones, *carrier sense multiple access / collision detect*) y dado que el medio de trasmisión de la WLAN no están confinadas a un medio cableado, la técnica empleada se denomina CSMA/CA (Acceso Múltiple por Sensado de Portadora con Anulación de Colisiones, *carrier sense multiple access / collision avoidance*). El método de CSMA/CA usa un algoritmo basado en evitar colisiones en lugar de descubrirlas, como el algoritmo usado en Ethernet. 802.11 usa un esquema de acceso distribuido con control no centralizado. Cada estación 802.11 utiliza los mismos métodos para acceder al medio. La mayor diferencia entre 802.11 y Ethernet subyace en el medio.

En Ethernet, se transmite la trama y se asume que el destino lo recibe correctamente. En los enlaces de radio esto es diferente, especialmente cuando las frecuencias usadas pertenecen a las bandas de ICM (industrial, científica y médica, en inglés ISM) que están sujetas al ruido y a la interferencia. Es por esta razón que toda transmisión en 802.11 debe ser reconocida a través de un acuse de recibo (*acknowledgement* - ACK): si cualquiera de las partes falla, la trama se considera perdida. Este proceso se puede observar en la figura II.1.

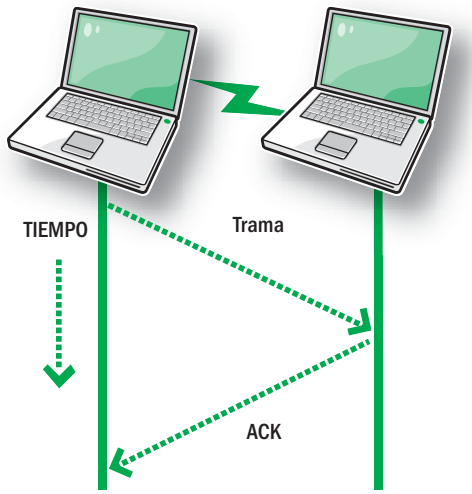


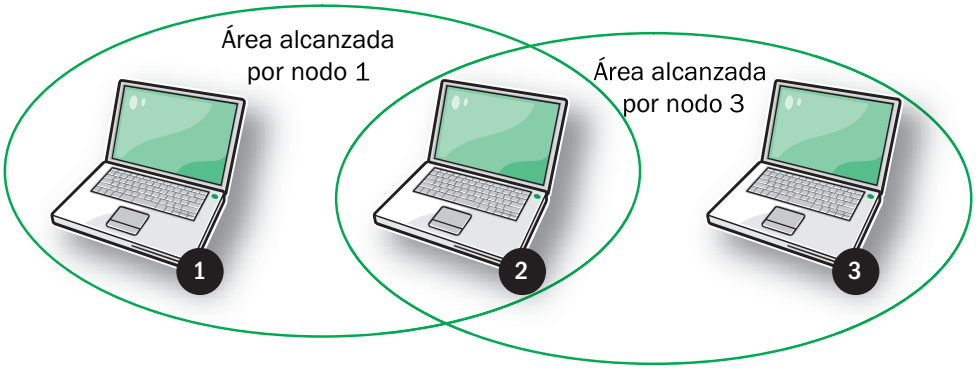
Figura II.1

CAPÍTULO II

En este tipo de redes puede ocurrir la situación ilustrada en la figura II.2: la estación 1 y la estación 3 no pueden comunicarse directamente, pero podría suceder que ambas transmitan al mismo tiempo y se produzca una colisión que no sería detectada por dichas estaciones, pues la colisión se produce localmente en la estación 2. Esta situación recibe el nombre del problema de la estación oculta.

Para prevenir colisiones, 802.11 permite que las estaciones usen señales de requerimiento y aceptación para el envío de datos con el propósito de reservar el enlace de radio (*request to send* - RTS y *clear to send* - CTS).

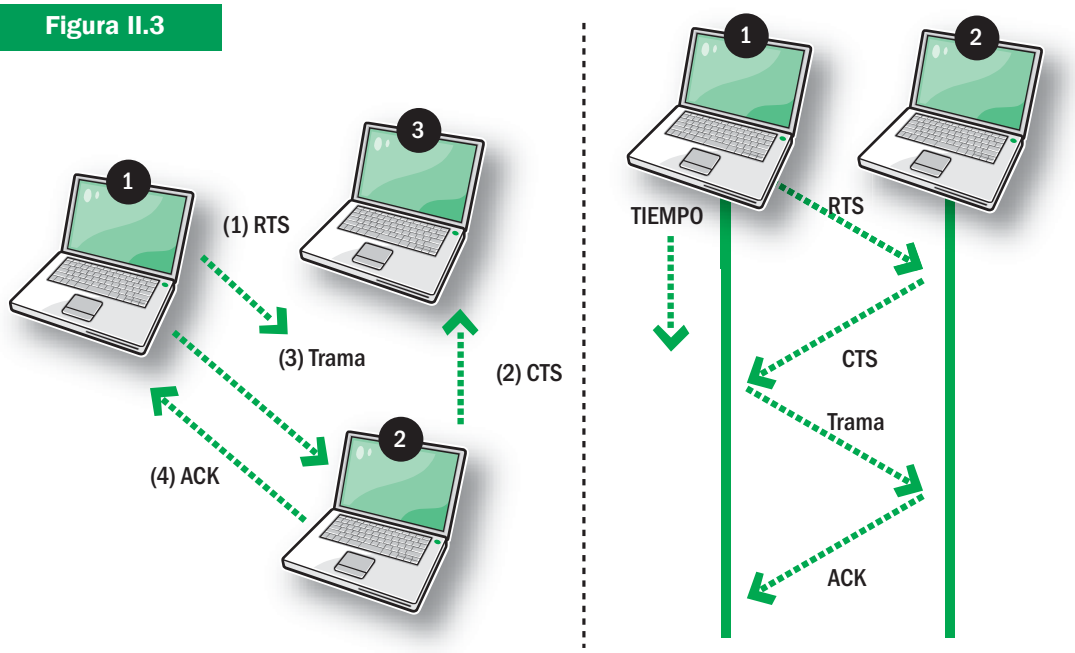
Figura II.2



Un proceso de transmisión de datos puede observarse en la figura II.3. En este caso la estación 1 tiene una trama para transmitir, por lo que inicia el proceso enviando una trama RTS. Al llegar al destino éste responde con una trama CTS produciendo el silencio de las estaciones vecinas. Luego la trama es enviada por la estación 1 y la estación 2 al recibirla envía una trama de ACK.

CAPÍTULO II

Figura II.3



II.1.1 MODOS DE ACCESO

El acceso al medio inalámbrico es controlado por funciones de coordinación, las cuales son descriptas a continuación y esquematizadas en la figura II.4:

DCF (*DISTRIBUTED COORDINATION FUNCTION*)

La DCF es el mecanismo de acceso básico del estándar CSMA/CA. En este caso, antes de transmitir, primero se verifica que el enlace de radio se encuentre limpio. Para evitar colisiones, las estaciones retardan aleatoriamente el envío de tramas y luego escuchan el canal para poder transmitir. En algunas circunstancias, la DCF puede usar la técnica de RTS/CTS para reducir la posibilidad de colisiones.

CAPÍTULO II

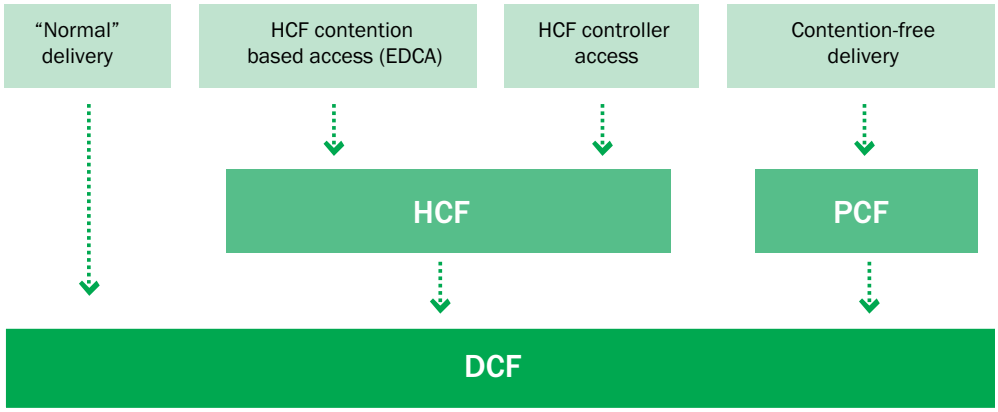
PCF (*POINT COORDINATION FUNCTION*)

La PCF provee servicios libres de contienda. Estaciones especiales llamadas puntos coordinadores son usados para asegurar que el medio sea provisto sin contienda. Los puntos coordinadores residen en los APs, por lo que la PCF está restringida a redes de infraestructura. Para ganar prioridad sobre servicios basados en la contienda estándar, la PCF permite que las estaciones transmitan tramas luego de un intervalo de tiempo corto.

HCF (*HYBRID COORDINATION FUNCTION*)

Algunas aplicaciones necesitan tener calidad de servicio (es decir, dar prioridad a cierto tipo de transmisiones) sobre envíos de mejor esfuerzo (que no garantizan despacho inmediato) y sin la rigurosidad de los tiempos requerido por la PCF. La HCF permite a las estaciones mantener colas de múltiples servicios y balancear el acceso al medio a favor de aplicaciones que requieren mayor calidad de servicio. La HCF no está totalmente estandarizada y es parte de las eventuales especificaciones 802.11e.

Figura II.4



CAPÍTULO II

Si un servicio libre de contienda es requerido, éste puede ser provisto por la Point Coordination Function (PCF) la cual se encuentra por encima de la DCF.

II.1.2 FUNCIONES DE DETECCIÓN DE PORTADORAS

La detección de la portadora es usada para determinar si el medio se encuentra disponible. Dos tipos de funciones de detección son manejadas por el estándar 802.11: la detección de portadora por parte de la capa física y las funciones de detección de portadoras virtuales.

Las funciones de detección de portadoras indican que el medio se encuentra ocupado. La MAC es la encargada de reportar esta situación a las capas superiores.

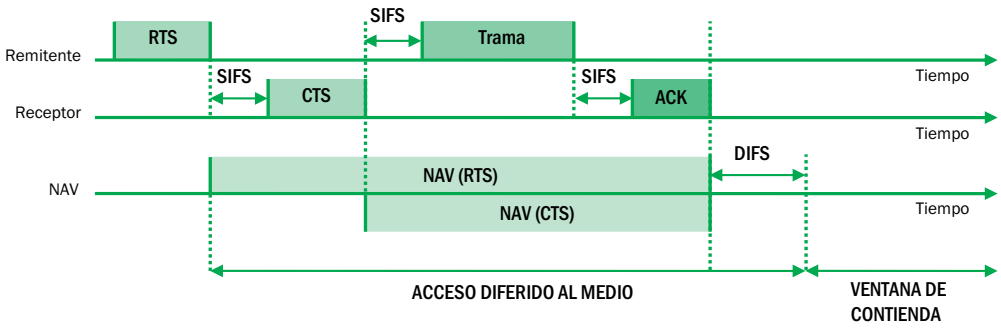
Las funciones de detección de portadora son provistas por la capa física y dependen del medio y de la modulación utilizada.

Las funciones de detección de portadoras virtuales son provistas por el Vector de Asignación de Red (NAV - *Network Allocation Vector*). El NAV es un temporizador que indica la cantidad de tiempo que el medio será reservado, expresado en microsegundos. La estación coloca el NAV con el tiempo que espera ocupar el medio, incluyendo otras tramas necesarias para completar la operación. Las otras estaciones realizan una cuenta regresiva desde el NAV hasta llegar a cero. Cuando el NAV es distinto de cero, la función de detección de portadora virtual indica que el medio está ocupado y cuando llega a cero,

CAPÍTULO II

indica que está disponible. La figura II.5 esquematiza este proceso.

Figura II.5



Cuando una estación está lista para transmitir, primero envía una solicitud de RTS (*request to send*) al AP, la cual contiene el destino y la longitud del mensaje. El AP difunde el NAV a todos los demás nodos para que todos queden informados que se va a ocupar el canal y cuál va a ser la duración de la transmisión. Dicho tiempo se encuentra basado en el tamaño de la trama a transmitir informada en la solicitud de RTS. Los nodos dejarán de transmitir durante el tiempo indicado por el NAV más un intervalo extra aleatorio (*backoff*). Si no encuentran problemas, el AP responde con una autorización (CTS) que permite al solicitante enviar su trama de datos. Si no se recibe la trama CTS, se supone que ocurrió una colisión y los procesos RTS empiezan nuevamente.

Luego de recibida la trama de datos se devuelve una trama de acuse de recibo (*Acknowledgement* - ACK) notificando al transmisor que se ha recibido correctamente la información (sin colisiones).

CAPÍTULO II

Aún así permanece el problema de que las tramas RTS sean enviadas por varias estaciones a la vez, sin embargo estas colisiones son menos dañinas, ya que el tiempo de duración de estas tramas es relativamente corto.

II.1.3 ESPACIAMIENTO INTERTRAMA

El estándar 802.11 usa cuatro diferentes espaciamientos entre tramas. Tres de ellos son usados para determinar el acceso al medio; la relación entre ellos es mostrada en la figura II.6.

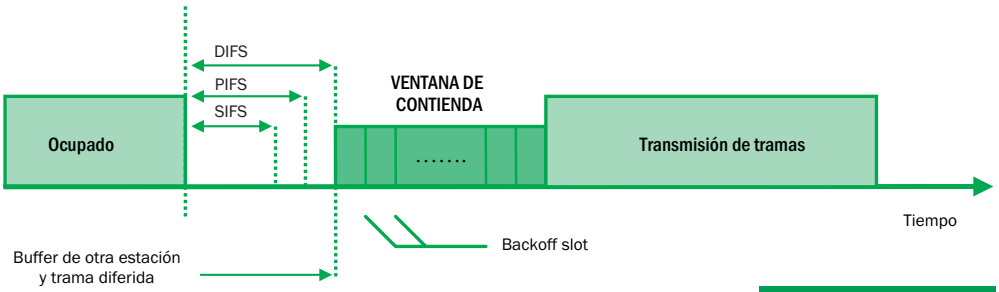


Figura II.6

Variando el espaciamiento intertrama el estándar 802.11 crea diferentes niveles de prioridad para distintos tipos de tráficos. Debido a las distintas capas físicas que el estándar 802.11 puede adoptar, éstas pueden especificar diferentes tiempos de intertramas.

- **SIFS (*Short interframe space*)**
  El SIFS es usado para transmisiones de alta prioridad, tales como tramas RTS/CTS y ACK positivas.

CAPÍTULO II

- **PIFS (*PCF interframe space*)**
  El PIFS es usado por la PCF durante una operación libre de contienda. Las estaciones con datos para transmitir pueden hacerlo luego del PIFS.

- **DIFS (*DCF interframe space*)**
  Es el tiempo mínimo para servicios basados en contienda en el cual el medio debe estar libre para que una estación pueda acceder. Las estaciones pueden tener inmediatamente acceso al medio si ha estado libre por un tiempo mayor que el DIFS.

- **EIFS (*Extended interframe space*)**
  El EIFS no fue ilustrado en la figura II.6 porque no es un intervalo fijo. Es usado solamente cuando hay un error en la transmisión de una trama.

II.1.4 TIPOS DE TRAMAS

Existen tres tipos de tramas las cuales son:

- **Tramas de datos:** usadas para la transmisión de datos.
- **Tramas de control:** usadas para el control del acceso al medio (Por ejemplo: RTS, CTS y ACK).
- **Tramas de gestión:** son transmitidas de la misma manera que las tramas de datos para intercambiar información de administración, pero no son transportadas a las capas superiores (por ejemplo: *Beacon*).

Cada tipo de trama es subdividida en diferentes subtipos de acuerdo a su función específica.

CAPÍTULO II

II.1.5 FORMATO DE TRAMA

Figura II.7

En el estándar 802.11 las tramas están compuestas de la siguiente manera, tal como se muestra en la figura II.7:

PREÁMBULO: Es dependiente de la capa PHY, e incluye:

- *Synch:* Una secuencia de bits alternada de ceros y unos, la cual es usada para la sincronización del receptor, para la selección de la antena apropiada (en caso de usarse diversidad) y para corregir el desvío en frecuencia del receptor.
- *SFD:* patrón de bits usados para delimitar el comienzo de trama.

PLCP *HEADER*: Contiene información usada por la capa PHY para decodificar la trama y es siempre transmitida a 1 Mbps.

Ésta consiste de:

- *PLCP PDU Length Word (PLW):* representa el número de bytes contenido en el paquete. Es usado por la capa PHY para detectar correctamente el fin del paquete.
- *PLCP Signaling Field (PSF):* contiene información de velocidades de información.
- *Header Error Check Field (HEC):* utiliza un código de redundancia cíclica (CRC) de 16 bits para detección de errores en el PLCP *Header*.

CAPÍTULO II

II.1.5.1 TRAMA MAC

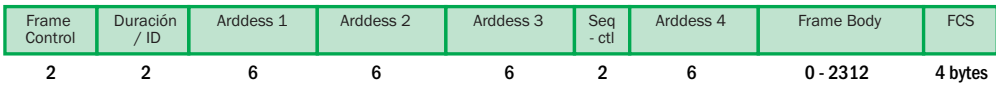


Figura II.8

El estándar 802.11 posee la trama MAC que se muestra en la figura II.8. En ella se detallan los siguientes campos:

Control de trama (*Frame Control*): Corresponde al comienzo de trama compuesto por 2 bytes:

Versión de protocolo: Estos 2 bits indican cuál es la versión de 802.11 MAC que se encuentra contenida en la trama. Hasta el presente solamente se ha desarrollado una versión de 802.11 y el número de protocolo asignado es el 0.

Tipo: Este campo de 2 bits indica el tipo de trama utilizado, pudiendo ser de: gestión, control o datos.

Subtipo: Este campo de 4 bits asociados con el de tipo detallan las acciones de cada una de las tramas, entre las cuales se encuentran las de: asociación, reasociación, prueba, *Beacon*, disasociación, autenticación, desautenticación, RTS, CTS, ACK, Datos, etc..

To DS y From DS: Estos bits indican si una trama es destinada al sistema de distribución. Todas las tramas sobre la red de infraestructura tienen estos bits activados. La Tabla 1 muestra como se interpretan estos bits.

CAPÍTULO II

TABLA 1

	To DS = 0	*To DS* = 1
From DS = 0	Todas tramas de control y gestión Tramas de datos sin un IBSS	Trama de datos transmitidas desde una estación inalámbrica en una red de infraestructura
From DS = 1	Tramas de datos recibidas para una estación inalámbrica en una red de infraestructura	Tramas de datos sobre un *brigde* inalámbrica.

More fragments: Este bit indica si la trama sufre alguna fragmentación. Cuando un paquete es fragmentado por la MAC, el fragmento inicial y los siguientes, salvo el último, contienen este bit activado en 1.

***Retry*:** Cualquier trama retransmitida tiene este bit en 1 para ayudar a la estación que la recibe en la eliminación de tramas duplicadas.

***Power management*:** Para conservar la vida de la batería, muchos dispositivos pequeños tiene la capacidad para eliminar la energización a la parte de la interface de red. Un 1 indica que la estación entró en modo de ahorro de energía y un 0 indica que la estación ha sido activada. Los Access Points poseen una importante función de administración y no pueden pasar al modo de ahorro de energía, por lo que todas las tramas transmitidas poseen este bit siempre en 0.

***More data*:** Este bit es usado por el AP para indicar que hay más fragmentos para esa estación.

CAPÍTULO II

***Protected Frame* - WEP:** Si la trama está protegida por un protocolo de seguridad de la capa de enlace de datos este bit esta activado (en 1).

***Order*:** Este bit al ser activado (estar en 1) indica que las tramas y fragmentos van a ser transmitidas en un estricto orden. Esto produce el adicionamiento de un costo en el procesamiento del envío y la recepción de las tramas MAC.

***Duration/ID*:** Este campo tiene dos significados dependientes del tipo de trama:

- Para el mensaje de *Power-Save* (ahorro de energía) éste corresponde al ID de la estación.
- En todas las otras tramas es la duración calculada, usada por el NAV.

Campos de direcciones: Una trama puede contener hasta 4 direcciones dependiendo de los bits *ToDS* y *FromDS* definidos en el campo de control, como sigue:

***Address-1*:** es siempre la dirección del receptor. Si *ToDS* está activado representa la dirección del AP y desactivado es la dirección de la estación.

***Address-2*:** es siempre la dirección del transmisor. Si *FromDS* está activado representa la dirección del AP y desactivado es la dirección de la estación.

***Address-3*:** sobre una trama con *FromDS* en 1 representa la dirección de la fuente de origen. Si la trama tiene *ToDS*

CAPÍTULO II

activado entonces corresponde a la dirección de destino.
***Address-4*:** es usado en casos especiales cuando un sistema de distribución inalámbrico es usado, y las tramas son transmitidas desde un AP a otro. En este caso los bits *ToDS* y *FromDS* están activados.

La siguiente tabla resume el uso de las diferentes direcciones de acuerdo a los bits *ToDS* y *FromDS*:

TABLA 2

To DS	FromDS	Address-1	Address-2	Address-3	Address-4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

Control de Secuencias (Seq-ctl):

Este campo es usado para representar el orden de diferentes fragmentos dentro de una misma trama y para el reconocimiento de paquetes duplicados. Está constituido por el número de fragmento y el número de secuencia, los cuales definen la trama y el número de fragmento en la trama.

FCS:

Es un campo de 32 bits conteniendo un CRC (*Cyclic Redundancy Check*) para la detección de errores de la trama MAC.

CAPÍTULO II

II.2 CAPA FÍSICA (PHY)

Tres capas físicas fueron estandarizadas en la revisión inicial del estándar 802.11, las cuales fueron publicadas en 1997. Ellas son:

- Espectro Expandido por Salto de Frecuencia (FHSS).
- Espectro Expandido por Secuencia Directa (DSSS).
- Infrarrojo (IR).

Luego fueron desarrolladas otras capas físicas basadas en tecnologías de radio:

- 802.11a: Multiplexación por División de Frecuencias Ortogonales (OFDM).
- 802.11b: Espectro Expandido por Secuencia Directa de Alta Tasa (HR/DSSS).
- 802.11g: Multiplexación por División de Frecuencias Ortogonales (OFDM).
- La futura 802.11n, la cual es también llamada MIMO-OFDM.

II.2.1 SALTO DE FRECUENCIA (FHSS)

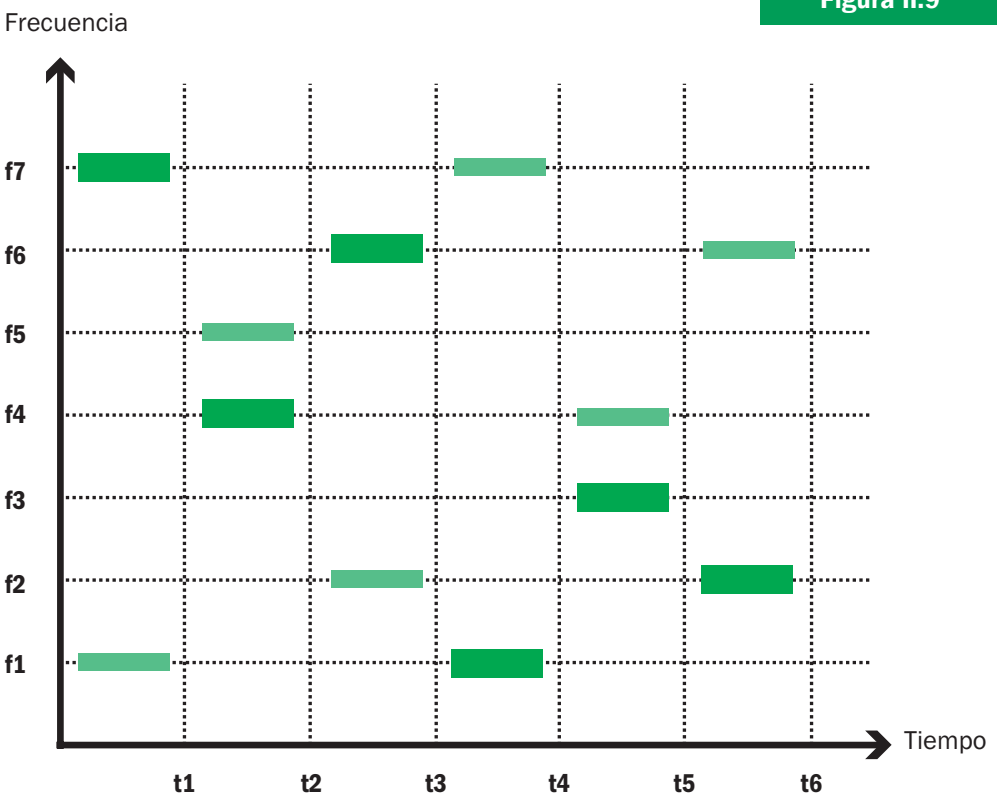
La tecnología de espectro ensanchado por salto de frecuencia (FHSS) consiste en transmitir una parte de la información en una determinada frecuencia durante un intervalo de tiempo llamado tiempo de permanencia (*dwell time*). Pasado este tiempo se cambia la frecuencia de emisión y se sigue transmitiendo en otra frecuencia. De esta manera cada tramo de información se va transmitiendo en una frecuencia distinta durante un intervalo muy corto de tiempo.

CAPÍTULO II

El orden en los saltos de frecuencia se determina según una secuencia pseudoaleatoria que el emisor y el receptor deben conocer.

Si se mantiene la sincronización en los saltos de frecuencias se consigue que, aunque en el tiempo se cambie de canal físico (frecuencia), a nivel lógico se mantenga un solo canal por el que se realiza la comunicación (el enlace es único). La figura II.9 muestra dos sistemas operando sobre el mismo espectro de frecuencias con diferentes secuencias de saltos.

Figura II.9



CAPÍTULO II

Para la banda de 2,4 GHz, el estándar 802.11 define el orden de los saltos en 3 conjuntos, con 26 secuencias cada uno. Las secuencias cubren 79 canales a lo largo de la banda, con secuencias ortogonales, es decir independientes, unas de otras en cada conjunto.

Las transmisiones son GFSK (*Gaussian Frequency Shift Keying*) modulada en 2, 4 u 8 niveles para lograr 1, 2 ó 3 Mbps, respectivamente. La velocidad de salto puede ser de 8 a 32 veces por segundo. La potencia de transmisión es concentrada en un ancho de banda de 1 MHz para cada salto.

La tabla 3 muestra los parámetros para Capa Física (PHY) FHSS.

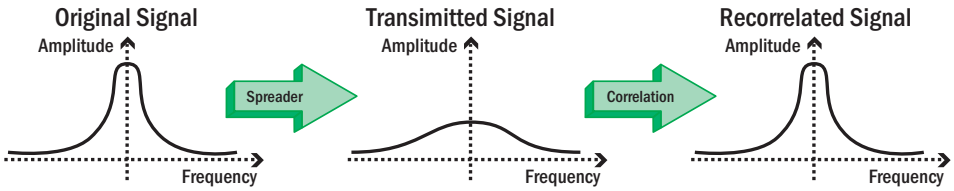
TABLA 3

Parámetro	Valor	Notas
Slot time	50 µs	
SIFS time	28 µs	Del valor del SIFS se derivan los valores de los espacios intertrama (DIFS, PIFS y EIFS)
Tamaño de la ventana de contienda	15 - 1023 slots	
Duración del preámbulo	96 µs	Los símbolos del preámbulo son transmitidos a 1 MHz. Como un símbolo tarda 1 µs en ser transmitido, 96 bits requieren 96 µs
Duración del PLCP header	32 µs	32 bits del PLCP *header*
Máxima trama MAC	4095 bytes	802.11 recomienda un máximo de 400 símbolos (400 bytes en 1 Mbps, 800 bytes en 2 Mbps) para mantener una *performance* a lo largo de diferentes tipos de medios
Sensibilidad mínima	-80 dBm	

CAPÍTULO II

II.2.2 802.11 y 802.11b SECUENCIA DIRECTA (DSSS y HR/DSSS)

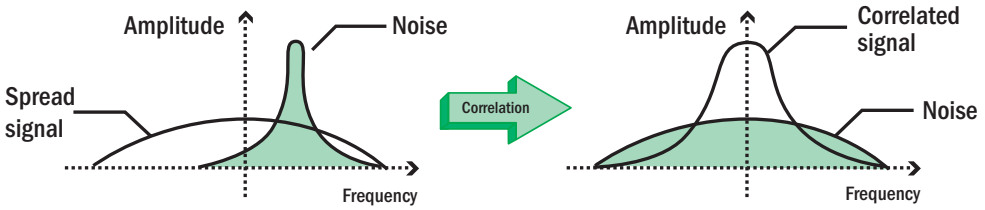
La tecnología de espectro ensanchado por secuencia directa (DSSS) consiste en modular la señal a transmitir con una secuencia de bits de alta velocidad, denominados en este caso *chips* y conocida como Secuencia de Barker, Código de Dispersión o Ruido Pseudoaleatorio (Código PN), que da como resultado una expansión de la señal.



Si bien la relación Potencia a Anchura de Banda se mantiene después del ensanchamiento de la señal (con lo cual la Potencia baja considerablemente), se obtiene una señal más inmune al ruido, ya que la interferencia afecta sólo unos pocos bits de la señal original (la Secuencia de Barker recomendada es de 11 *chips*, aunque puede llegar a 100, pero a mayor número de *chips*, mayor es el costo de los osciladores de radiofrecuencia necesarios para su manejo y mayor es la Anchura de Banda requerida).

Para recuperar la señal original, el receptor deberá conocer el Código de Ruido Pseudoaleatorio utilizado. Además, al ser aplicado el proceso inverso sobre una eventual interferencia (que por definición es de banda angosta), esta correlación produce la dispersión del ruido.

CAPÍTULO II



El mayor problema se presenta con otro usuario utilizando esta misma tecnología DSSS en la zona, como se verá más adelante.

Se conoce como Ganancia de Procesamiento (Gp) a la relación entre la Anchura de Banda de la señal de Espectro Ensanchado (AB_{PN}) respecto de la Anchura de Banda de la señal Original (AB_O). La misma debe ser mayor que 10. En particular, para una Secuencia de Barker de 11 *chips*, Gp=10,4.

La Anchura de Banda típica (para una velocidad de *chip* de 11 MHz) es de 22 MHz, siendo la canalización cada 5 MHz (desde el Canal 1, centrado en 2412 MHz, hasta el Canal 13, centrado en 2472 MHz). Sólo en Japón se utiliza el Canal 14, centrado en 2484 MHz.

En particular, IEEE 802.11 utiliza espectro ensanchado por secuencia directa (DSSS) y tiene tasas de transferencia de 1 y 2 Mbps, mientras que para IEEE 802.11b, denominada espectro ensanchado por secuencia directa de alta tasa (HR/DSSS), son de 5,5 y 11 Mbps. A pesar de poseer distintas especificaciones y puesto que las 4 velocidades de transmisión se encuentran generalmente presentes en una única interfaz, se las conoce como IEEE 802.11b, o directamente 802.11b.

CAPÍTULO II

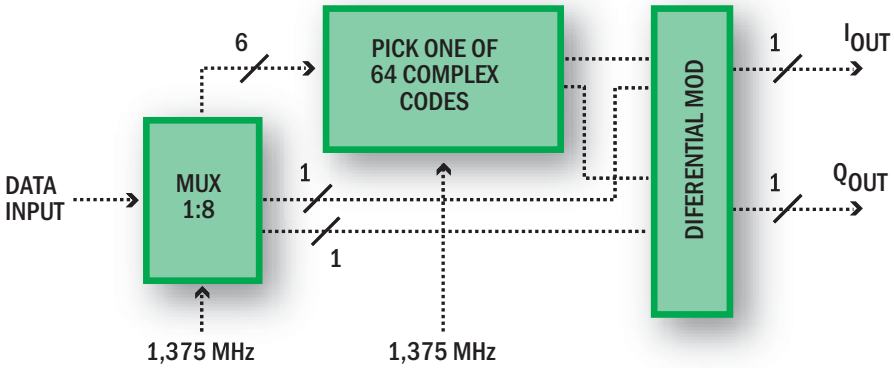
Para prevenir interferencias deben utilizarse canales espaciados 25 MHz, es decir, cada 5 canales. Así, los canales a utilizar son: 1, 6 y 11. No obstante, en ciertas circunstancias es aceptable utilizar canales más solapados (por ejemplo: 1, 4, 7 y 11 o 1, 5, 9 y 13), a expensas de bajar la velocidad de transferencia de datos (o *throughput*: cantidad de datos transferidos por unidad de tiempo [medido en bps]).

La Modulación varía de acuerdo a la tasa de transferencia alcanzada, a saber:

- **1 Mbps:** se logra con DBPSK (por corrimiento de fase binaria diferencial), explicado y graficado en el Nº 2 de la Publicación Nuevas Tecnologías de Diciembre de 2007, en el Apéndice A, página 53.
- **2 Mbps:** se logra con DQPSK (por corrimiento de fase en cuadratura diferencial). Aquí se envían 2 bits por símbolo con un salto de 90º (PI/2) por cada cambio de bit. Esta modulación es más vulnerable a interferencia por multicamino, si bien tiene una *throughput* mayor.
- **Tanto 5,5 como 11 Mbps** se logran utilizando CCK (por códigos complementarios). Las modulaciones PSK no son aplicables porque habría que aumentar considerablemente la cantidad de bits por símbolo, con las consiguientes vulnerabilidades y costos asociados. Entonces, en lugar de usar una Secuencia de Barker se utiliza una Secuencia Complementaria de 8 bits, obtenida a partir de los mismos datos a transmitir. Así, con 6 bits (2^6) se obtienen 64 palabras de código y los 2 bits restantes son

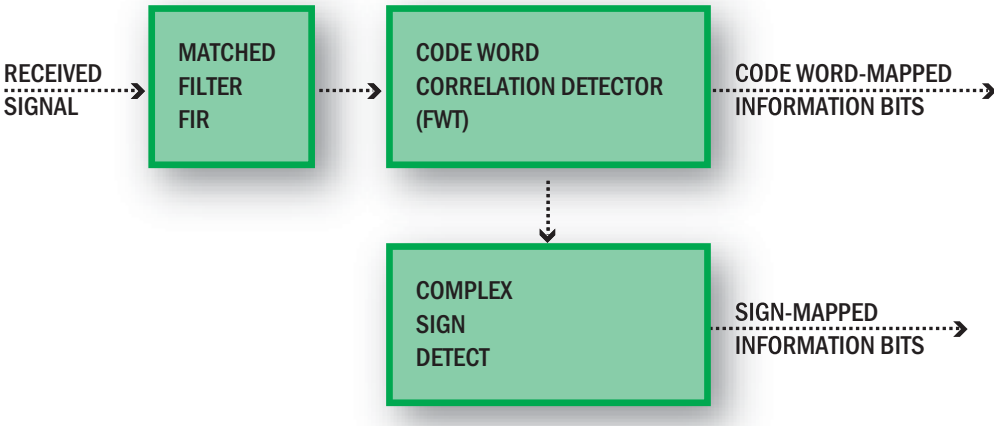
CAPÍTULO II

usados para modular en DQPSK. Estos Códigos cumplen, entre otras propiedades, que: un par de secuencias de longitud finita tienen la propiedad de que el número de pares de elementos iguales con una separación dada en una serie es igual al número de pares de elementos distintos con la misma separación en otra. Es decir: la suma del vector de autocorrelación es siempre 0, excepto en el corrimiento cero (en el mismo código). Los Códigos Complementarios utilizados en HR/DSSS son aún mas: ¢omplejos! Digamos entonces que tienen una longitud de código de 8 y una velocidad de *chip* de 11 Mcps. Los 8 complejos conforman un único símbolo y para una tasa de transferencia de símbolo de 1,375 MSps se logran 11 Mbps con la misma Anchura de Banda que para 2 Mbps con DQPSK. En particular, para 5,5 Mbps se usa un subconjunto de los códigos utilizados en 11 Mbps y en vez de cada símbolo estar constituido por 8 bits, se transmiten 4 bits por símbolo. A continuación se ilustra un Diagrama en Bloques del circuito modulador:



CAPÍTULO II

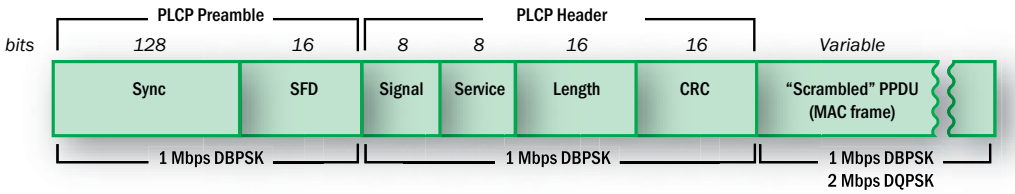
A su vez, para mejorar el rendimiento en cuanto a la tasa de error de paquetes en presencia de multicamino, se implementa un receptor de tipo *Rake* (rastrillo: se consigue con varios receptores en paralelo, levemente desfasados, donde cada componente se decodifica de forma independiente, pero en una última etapa se suman constructivamente con objeto de sacar el máximo provecho de cada camino). A continuación se ilustra un Diagrama en Bloques de dicho receptor:



La Capa Física (PHY) consta de dos componentes: Procedimiento de Convergencia de Capa Física, PLCP (*Physical Layer Convergence Procedure*) y la Dependiente del Medio Físico, PMD (*Physical Medium Dependent*). Las especificaciones son distintas, según se trate de DSSS o HR/DSSS.

PLCP|DSSS: agrega un encabezado de 6 campos a las tramas recibidas de la Capa de Acceso al Medio (MAC), como se muestra a continuación en la Figura.

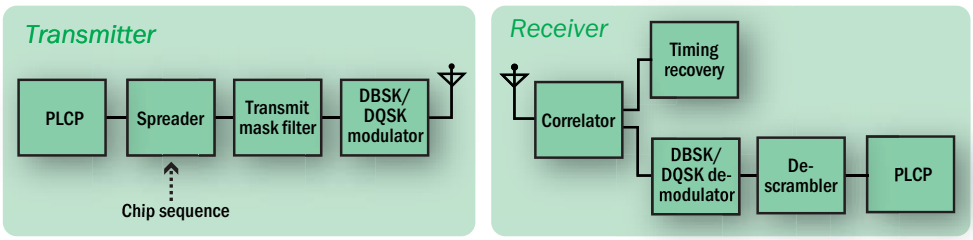
CAPÍTULO II



Dado que no existen restricciones para el contenido del campo de datos, se aplica un Encriptador para eliminar secuencias largas de 1's y 0's, tal que la señal a transmitir se asemeje más al ruido. Este encriptador se denomina *Scrambler* y es aplicado a toda la trama DSSS, incluidos encabezado y preámbulo PLCP. (En FHSS, en cambio, se denomina *Data Whitener* y se aplica solamente sobre la trama MAC que sigue al encabezado PLCP.)

PMD|DSSS: es una especificación larga y compleja que incorpora provisiones para dos tasas de datos (1 y 2 Mbps). Para 1 Mbps se encripta el encabezado PLCP más las tramas MAC y se transmite utilizando DBPSK a 1 Mbps, mientras que para 2 Mbps se transmite preámbulo y encabezado PLCP utilizando también DBPSK a 1 Mbps (para hacerlos más robustos) y conmuta a DQPSK a 2 Mbps para transmitir las tramas MAC (aunque puede bajar esta velocidad también en casos de interferencia).

En la siguiente Figura se ilustra el Diagrama en Bloques de un transceptor (transmisor+receptor) DSSS:



CAPÍTULO II

El Control de Acceso al Medio (MAC) se hace mediante la función CS/CCA de Sensado de Portadora/Evaluación de Canal Libre (*Carrier Sense/Clear Channel Assessment*), que puede reportar si el medio se encuentra ocupado de tres modos, a saber:

1. Si se supera el umbral de detección de energía.
2. Si encuentra una señal DSSS, aunque no se cumpla el modo 1.
3. La combinación de los modos 1 y 2.

Estos reportes deben ser muy rápidos, a fin de evitar colisiones.

La siguiente tabla muestra los parámetros para Capa Física (PHY) DSSS.

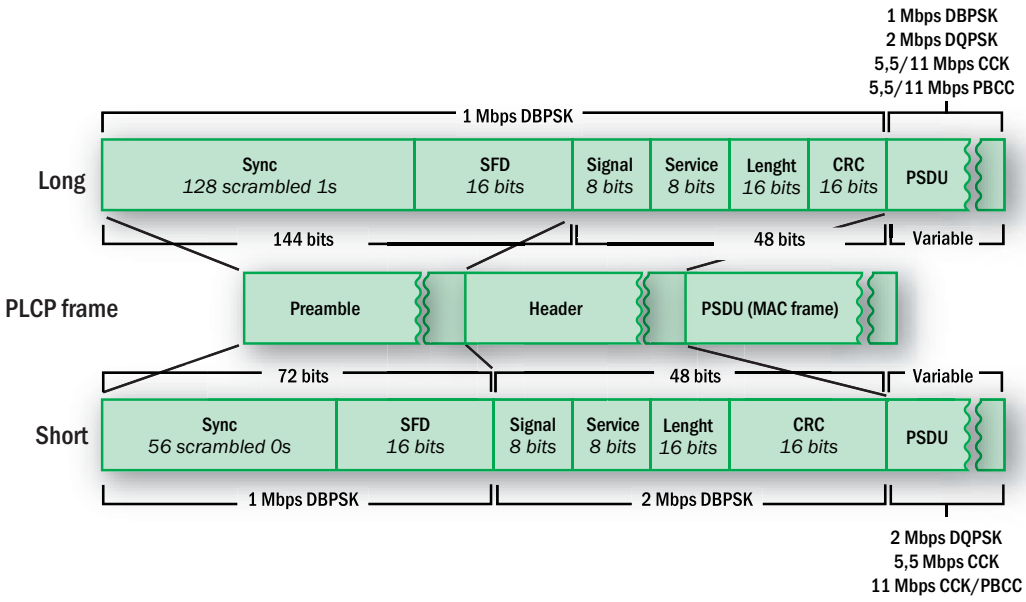
TABLA 4

Parámetro	Valor	Notas
Slot time	20 µs	
SIFS time	10 µs	Del valor del SIFS se derivan los valores de los espacios intertrama (DIFS, PIFS y EIFS)
Tamaño de la ventana de contienda	31 - 1023 slots	
Duración del preámbulo	144 µs	Los símbolos del preámbulo son transmitidos a 1 MHz. Como un símbolo tarda 1 µs en ser transmitido, 144 bits requieren 144 µs
Duración del encabezado PLCP	48 µs	El encabezado PLCP es de 48 bits
Máxima trama MAC	4 - 8191 bytes	
Sensibilidad mínima	-80 dBm	
Rechazo de canal adyacente	35 dB	

CAPÍTULO II

La Capa Física (PHY) de HR/DSSS consta también de los mismos dos componentes: Procedimiento de Convergencia de Capa Física, PLCP (*Physical Layer Convergence Procedure)* y la Dependiente del Medio Físico, PMD (*Physical Medium Dependent*), pero con diferentes especificaciones, tal como se dijera antes. A saber:

PLCP|$_{HR/DSSS}$: los largos encabezados de la PHY original (o sea, para DSSS), transmitidos a 1 Mbps utilizando DBPSK, reducen el rendimiento hasta un 25%. La nueva PHY (para HR/DSSS) emplea encabezados más cortos, transmitidos a 2 Mbps usando DQPSK, que si bien recortan sólo un 14% el preámbulo PLCP|$_{DSSS}$, mejoran el rendimiento drásticamente. En un principio no todos los equipos aceptaban los encabezados cortos, por eso se los interrogaba y en función a cuál respondían era el encabezado a enviar. A continuación se muestran ambos encabezados.

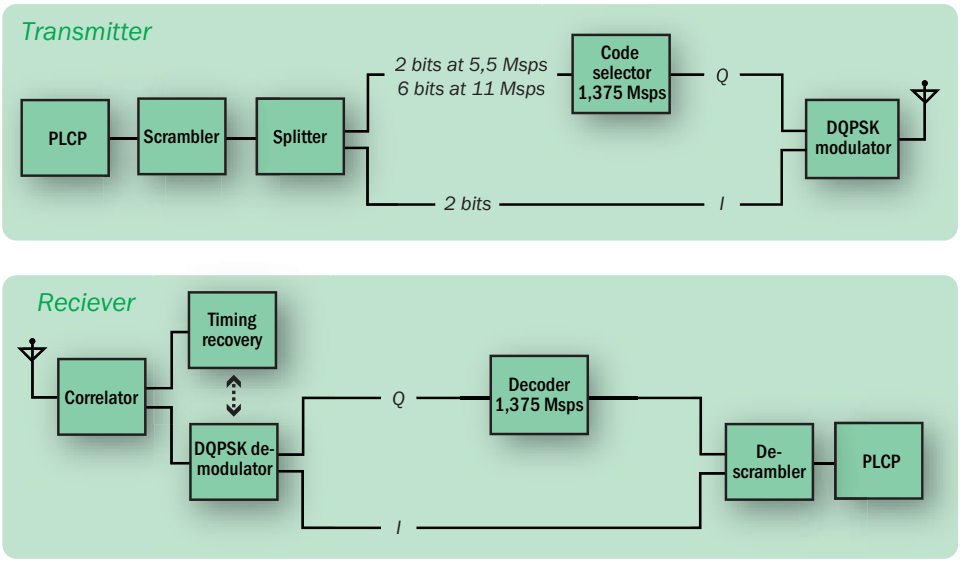


CAPÍTULO II

El encriptado es similar en ambos casos, sólo que se utilizan distintos valores específicos para HR/DSSS.

PMD|$_{HR/DSSS}$: para hacerla compatible con la de IEEE 802.11 original (es decir, DSSS), transmite las dos tasas de transferencia más bajas (1 y 2 Mbps) del mismo modo (o sea, con encabezados largos). Las dos tasas más altas (5,5 y 11 Mbps) son transmitidas utilizando CCK, tal como se explicara previamente.

En la siguiente Figura se ilustra el Diagrama en Bloques de un transceptor (transmisor+receptor) HR/DSSS:



CAPÍTULO II

El Control de Acceso al Medio (MAC) de HR/DSSS también utiliza la función CS/CCA de Sensado de Portadora/Evaluación de Canal Libre (*Carrier Sense/Clear Channel Assessment*), que puede reportar si el medio se encuentra ocupado también de tres modos, aunque no todos son los mismos que los de DSSS:

1. Es idéntico, o sea reporta ocupado si se supera el umbral de detección de energía.

Los modos 2 y 3 son para DSSS, quedando para HR/DSSS los modos 4 y 5.

4. Escucha durante 3,65 ms (tiempo correspondiente a la trama más larga transmitida a 5,5 Mbps) la presencia de una señal HR/DSSS válida. De no existir, se reporta como libre.
5. Es la combinación de los modos 1 y 4.

La siguiente tabla muestra los parámetros para Capa Física (PHY) HR/DSSS.

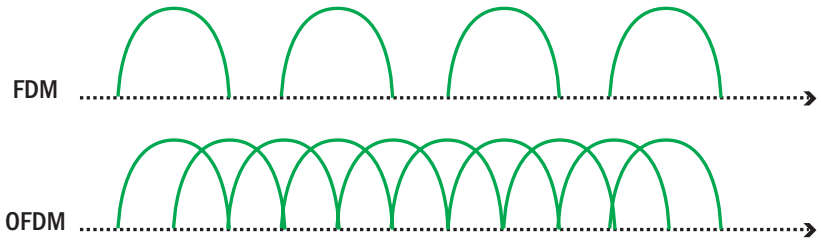
Parámetro		Valor	Notas
Slot time		20 µs	
SIFS time		10 µs	Del valor del SIFS se derivan los valores de los espacios intertrama (DIFS, PIFS y EIFS)
Tamaño de la ventana de contienda		31 - 1023 slots	
Duración del preámbulo	Largo	144 µs	Los símbolos del preámbulo son transmitidos a 1 MHz. Como un símbolo tarda 1 µs en ser transmitido, 144 bits requieren 144 µs y 72 bits, 72 µs
	Corto	72 µs	
Duración del encabezado PLCP		48 µs	El tiempo de transmisión del encabezado PLCP depende de qué preámbulo haya sido utilizado
Máxima trama MAC		4095 bytes	
Sensibilidad mínima		-76 dBm	
Rechazo de canal adyacente		35 dB	

CAPÍTULO II

II.2.3 802.11a y 802.11j u 802.11h (OFDM)

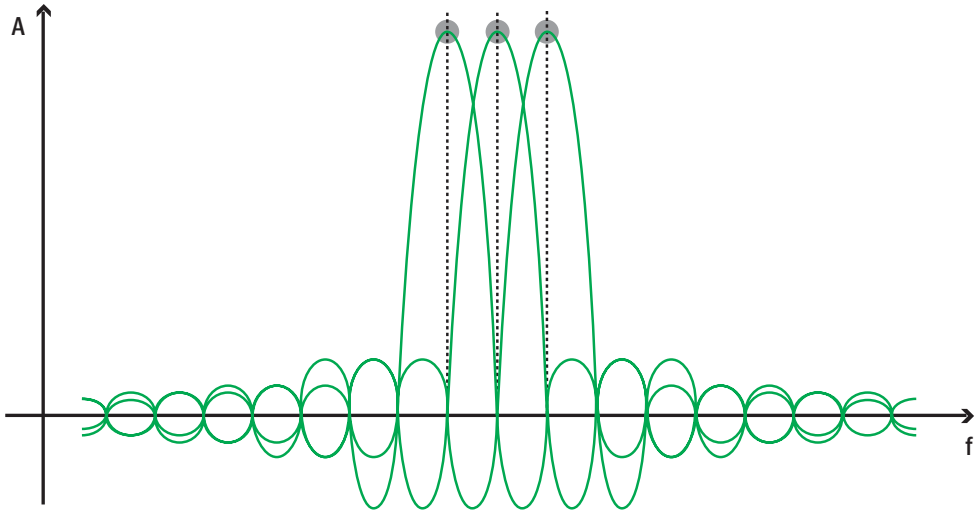
La tecnología de multiplexación por división de frecuencias ortogonales (OFDM) consiste en fraccionar un canal de frecuencia largo (gran anchura de banda) en un número de subcanales ortogonales, los cuales serán usados en paralelo para aumentar la velocidad de transferencia de datos (*throughput*).

Esta multiplexación está relacionada de cerca con la multiplexación por división de frecuencias (FDM). El problema con la FDM tradicional es el gasto que implican las bandas de guarda (utilizadas para evitar interferencia entre los usuarios), que reducen la capacidad. Con OFDM en cambio se seleccionan canales que se solapan pero no se interfieren (denominados Ortogonales).



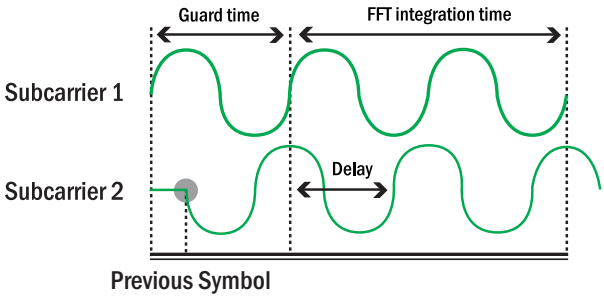
Es decir, que a cada frecuencia de subportadora, las restantes no contribuyen a la forma de onda total, como puede observarse en la siguiente Figura, que para cada amplitud pico de una subportadora las otras dos valen cero.

CAPÍTULO II

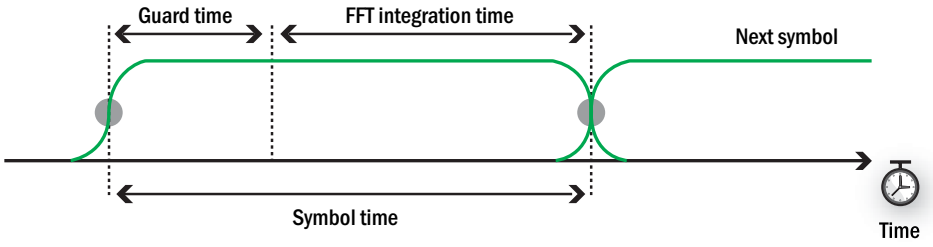


OFDM es bastante robusta ante una interferencia entre símbolo (ISI), producida por multicaminos. En cambio, se presenta el problema de interferencia entre portadoras (ICI), producida por pequeños corrimientos en las frecuencias de subportadoras. Para solucionarlo, se agrega un tiempo de guarda (t_G), de modo tal que demoras menores a t_G no ocasionan dicha interferencia. Como era de esperarse, este t_G también reduce la *throughput*, por eso es importante su adecuada elección (ya que t_G bajos no previenen la ICI y t_G altos bajan la *throughput* innecesariamente). Transmitir silencios en las bandas de guarda no es factible, ya que destruye la ortogonalidad en presencia de retardos expandidos. Como OFDM depende de tener un número entero de longitudes de onda entre subportadoras, lo que se hace es extender ciclos de las portadoras (demoradas distintos tiempos) durante dicho t_G, tal que cuando se empiezan a procesar no se interfieren.

CAPÍTULO II



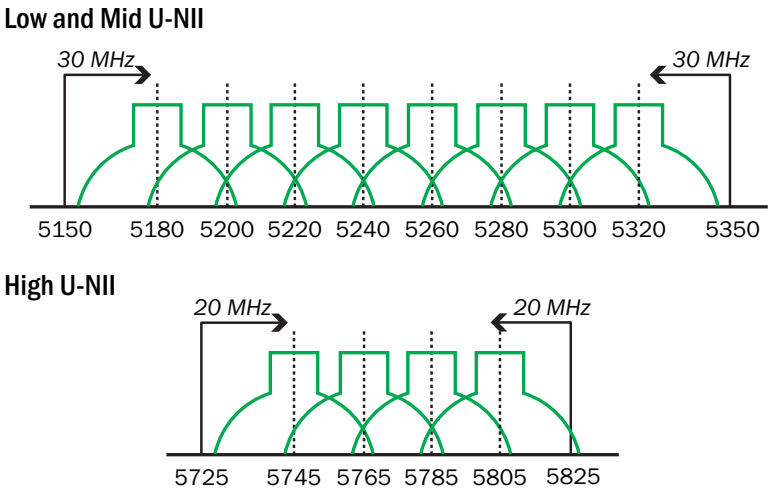
A su vez, para evitar transiciones abruptas (que causarían ruido de alta frecuencia), lo que se hace es agregar bits de relleno al principio y al final de las transmisiones, para permitir al transmisor subir y bajar la potencia y procesar una vez alcanzado el nivel.



En particular, IEEE 802.11a utiliza un tiempo de guarda t_G =800 ns (obtenido en función de los retardos típicos de los ambientes en que se utilizan), con 4 µs de tiempo de símbolo y espaciamiento de sub-portadoras de 0,3125 MHz. La Anchura de Banda requerida de 20 MHz es una solución de compromiso entre una *throughput* razonable (hasta 54 Mbps) y el número de canales operando simultáneamente por distintos usuarios (máximo 4) en el espectro asignado. La

CAPÍTULO II

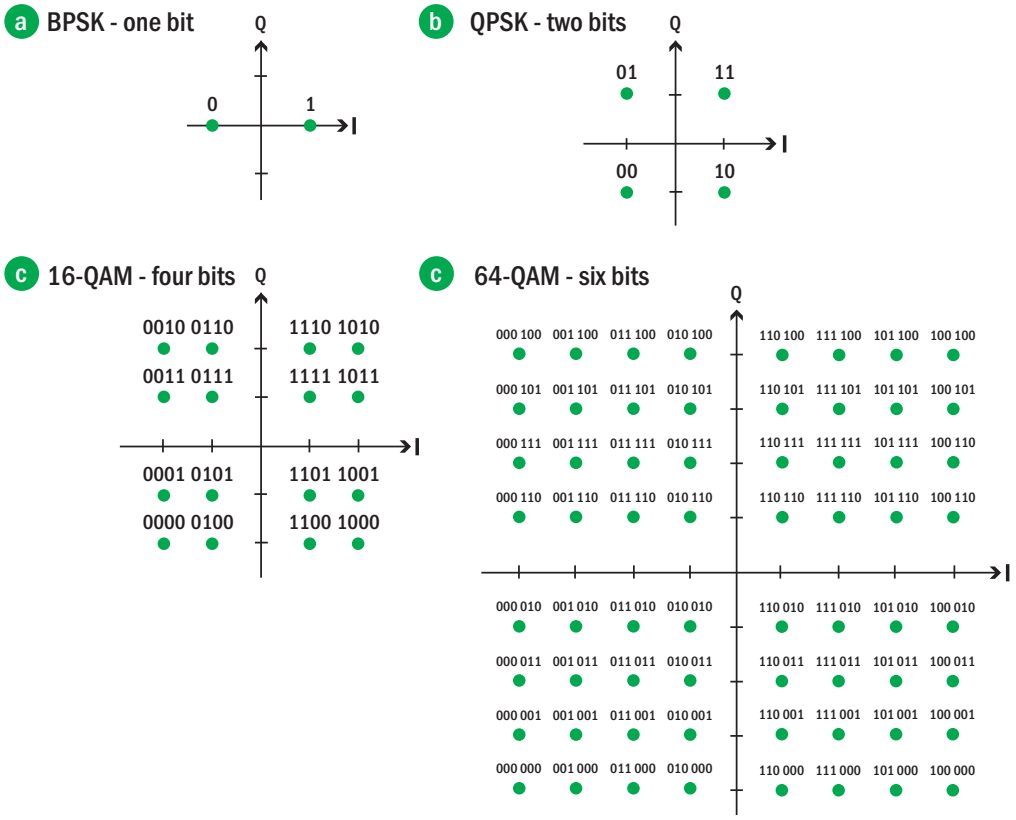
Modulación depende de la velocidad de transmisión (para el mejor caso: 64-QAM, como se verá más adelante).



Cada canal del 20 MHz posee 52 subportadoras, 4 de ellas usadas únicamente para monitorear la interferencia entre portadoras (ICI), denominadas portadoras piloto, o sea que son 48 las que transmiten datos.

QAM (modulación de amplitud en cuadratura): consiste en modular en amplitud las 2 componentes [denominadas (y abreviadas): en fase (I) y en cuadratura (Q)] que forman la portadora, es decir: varía el tamaño (amplitud) de la portadora en función de la entrada. Existen distintos niveles (o constelaciones) de modulación (siempre potencias pares de 2), a saber: 16-QAM o 64-QAM. Si bien existen superiores (por ejemplo: 256-QAM), a medida que el nivel aumenta, el receptor debe ser más complejo para poder distinguir entre todos los estados posibles.

CAPÍTULO II



Utiliza la técnica de corrección de errores progresiva (FEC), que permite al receptor detectar bits corruptos y repararlos. Para ello, agrega bits de redundancia (7) dependientes de los datos que están siendo transmitidos y los codifica con códigos convolucionales, que dependen fuertemente de los bits ya transmitidos. Una vez en el receptor, se decodifica y aplica el algoritmo de Viterbi, que permite encontrar la secuencia de

CAPÍTULO II

bits transmitida más probable. A su vez, definida la tasa de código R como la cantidad de bits de datos que se envían respecto de los totales, ésta puede ser de 1/2, 2/3 o 3/4 (a medida que R disminuye, se dice que el código es más robusto, pero disminuye la *throughput*).

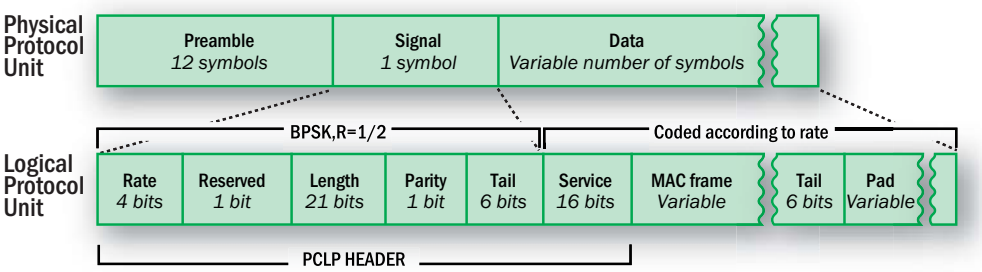
Además, hace el entrelazado (*interleaving*) de las subportadoras que constituyen cada canal operativo. Las secuencias de bits deben ser transmitidas en subportadoras separadas y en distintas constelaciones, luego cada flujo de datos debe ser asociado a la subportadora correspondiente.

Existe también las variantes europea (IEEE 802.11h) y japonesa (IEEE 802.11j), que intentan resolver los problemas derivados de la coexistencia de estas redes (IEEE 802.11a) con sistemas de Radares y Satélites en esta banda, utilizada generalmente por sistemas militares. Con tal fin, estas variantes proporcionan a las redes existentes la capacidad de seleccionar dinámicamente la frecuencia (*Dynamic Frequency Selection* - DFS) a fin de evitar interferencias co-canal con sistemas de radares y para asegurar una utilización uniforme de los canales disponibles y controlar la potencia de transmisión (*Transmitter Power Control* - TPC) para asegurar que se respetan las limitaciones de potencia transmitida que puede haber para diferentes canales en una determinada región, de manera que se minimiza la interferencia con sistemas de satélites.

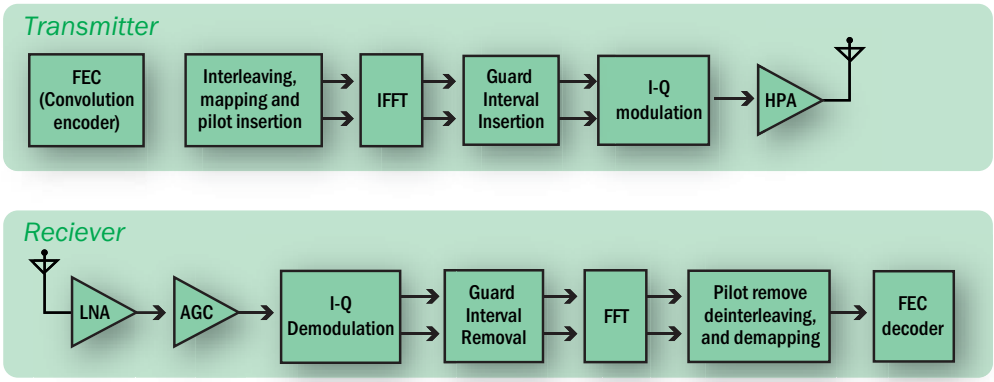
CAPÍTULO II

La Capa Física (PHY) consta también de los dos componentes: Procedimiento de Convergencia de Capa Física, PLCP (*Physical Layer Convergence Procedure*) y la Dependiente del Medio Físico, PMD (*Physical Medium Dependent*).

La trama PLCP se ilustra a continuación:



En la siguiente Figura se ilustra el Diagrama en Bloques de un transceptor (transmisor+receptor) OFDM:



CAPÍTULO II

Mientras que PMD usa un cóctel de distintos esquemas de modulación para ir desde 6 hasta 54 Mbps. Para todos los casos la tasa de símbolo es de 0,250 MSps sobre los 48 subcanales, siendo lo que varía el número de bits por símbolo. A continuación se resumirán los distintos parámetros para cada una de las velocidades:

Speed (Mbps)	Modulation and coding rate (R)	Coded bits per carrier [a]	Coded bits per symbol	Data bits per symbol [b]
6	BPSK, R=1/2	1	48	24
9	BPSK, R=3/4	1	48	36
12	QPSK, R=1/2	2	96	48
18	QPSK, R=3/4	2	96	72
24	16-QAM, R=1/2	4	192	96
36	16-QAM, R=3/4	4	192	144
48	64-QAM, R=2/3	6	288	192
54	64-QAM, R=3/4	6	288	216
72[c]	64-QAM	6	288	288

a) Los bits codificados por Subcanal son una función de la modulación (BPSK, QPSK, 16-QAM o 64-QAM)
b) Los bits de datos por símbolo son una función de la tasa de código convolucional.
c) A pesar que no ha sido normalizada una tasa sin un código convolucional, muchos productos ofrecen un modo donde ha sido bajada para una *throughput* adicional.

La implementación de la función CCA de Evaluación de Canal Libre (*Clear Channel Assessment*), que puede reportar si el medio se encuentra ocupado, queda librada a los fabricantes (aunque siguiendo una extensa serie de lineamientos). No obstante, también se requiere de un acuse de recibo (*Acknowledgement*) para ver la velocidad a la que se va a transmitir.

CAPÍTULO II

La siguiente tabla muestra los parámetros para Capa Física (PHY) OFDM.

Parámetro	Valor	Notas
Slot time	9 µs	
SIFS time	16 µs	Del valor del SIFS se derivan los valores de los espacios intertrama (DIFS, PIFS y EIFS)
Tamaño de la ventana de contienda	15 - 1023 slots	
Duración del preámbulo	20 µs	
Duración del encabezado PLCP	4 µs	
Sensibilidad del receptor	-65 a -82 dBm	Depende de la velocidad de transmisión de los datos
Máxima trama MAC	4095 bytes	

II.2.4 802.11g (ERP)

IEEE 802.11g utiliza la misma tecnología OFDM que IEEE 802.11a, pero en las mismas frecuencias de IEEE 802.11b, es decir de 2400 MHz a 2484 MHz (aunque en realidad en Japón no utilizan el Canal 14 para esta tecnología). Con ello, opera a una velocidad teórica máxima de 54 Mbps, o cerca de 24,7 Mbps de velocidad real de transferencia, similar a la de IEEE 802.11a y es compatible con IEEE 802.11b, ya que utiliza las mismas frecuencias. Por este motivo se la denomina ERP (capa física de tasa extendida, *Extended Rate PHY*), ya que la capa física no varía (respecto de IEEE 802.11b, o sea pueden coexistir 3 canales), pero además de las velocidades de transmisión de 1, 2, 5,5 y

CAPÍTULO II

11 Mbps, se suman las correspondientes a IEEE 802.11a (6, 9, 12, 18, 24, 36, 48 y 54 Mbps, siendo las obligatorias a implementar 6, 12 y 24 Mbps).

Buena parte del proceso de diseño lo tomó el hacer compatibles los dos estándares. Sin embargo, en redes bajo IEEE 802.11g la presencia de nodos IEEE 802.11b reduce significativamente la *throughput*, ya que al igual que HR/DSSS, emplea además encabezados cortos y largos, para que pueda ser compatible también con DSSS. Asimismo, debe implementar un sistema de protección para que, en caso de que haya una estación operando en IEEE 802.11b, ésta entienda que hay otra (operando en IEEE 802.11g) que quiere utilizar el medio y no se interfieran, debido que al tener distintas modulaciones no se entienden (el PMD es distinto). Esta protección puede implementarse de dos maneras:

CTS (libre para transmitir): es un mecanismo de autoprotección en el cual la estación IEEE 802.11g se envía a sí misma un pedido de transmisión, que es escuchado por todos y de esta manera se reserva el medio por el tiempo necesario para transmitir los datos más el acuse de recibo (ACK: *Acknowledgement*).

RTS/CTS (requerimiento para transmitir/libre para transmitir): en este caso la estación IEEE 802.11g envía al destinatario un pedido de transmisión y espera que la estación le responda que el medio se encuentra libre para hacerlo. Recién ahí envía los datos y al terminar, el ACK.

CAPÍTULO II

En ambos casos, los pedidos de transmisión se envían a tasas de transmisión correspondientes a IEEE 802.11b, para asegurarse que todos los entiendan. No obstante, una vez que dispone del medio, los datos los puede transmitir a velocidades mayores. Es por esta razón que si bien las tasas son iguales a IEEE 802.11a, la *throughput* puede llegar a reducirse a la mitad.

La implementación de la función CCA de Evaluación de Canal Libre (*Clear Channel Assessment*), que puede reportar si el medio se encuentra ocupado, se define de un único modo, que combina un umbral de energía mínimo con la habilidad de decodificar la señal (que consiste en detectar la presencia de una señal IEEE 802.11g válida). Sería equivalente al modo 3 de DSSS o al modo 5 de HR/DSSS, donde se evalúan las dos condiciones anteriores respectivas de cada caso (superar un umbral de energía mínimo y detectar una señal correspondiente a la tecnología en cuestión válida).

Los equipos que operan bajo IEEE 802.11g llegaron al mercado muy rápidamente, incluso antes de su ratificación. Esto se debió en parte a que para construir estos equipos se podían adaptar los ya diseñados para IEEE 802.11b. Los que se venden actualmente, con potencias de hasta medio Watt, prometen establecer comunicaciones de hasta 15 km con antenas parabólicas apropiadas.

Una variante propietaria es el IEEE 802.11 Super G, que alcanza una velocidad de transferencia de 108 Mbps.

CAPÍTULO II

La siguiente tabla muestra los parámetros para Capa Física (PHY) ERP.

Parámetro	Valor	Notas
Slot time	20 µs 9 µs	Si la red consiste sólo de estaciones IEEE 802.11g, este valor es menor que el de IEEE 802.11b y compatible con el de IEEE 802.11a.
SIFS time	10 µs	Del valor del SIFS se derivan los valores de los espacios intertrama (DIFS, PIFS y EIFS)
Tiempo de extensión de la señal	6 µs	Cada paquete IEEE 802.11g es seguido por este tiempo.
Tamaño de la ventana de contienda	15 o 31 - 1023 slots	Si la estación soporta sólo IEEE 802.11b, habrá 31 slots para compatibilidad. Caso contrario, será más corta.
Duración del preámbulo	20 µs	
Máxima trama MAC	4095 bytes	

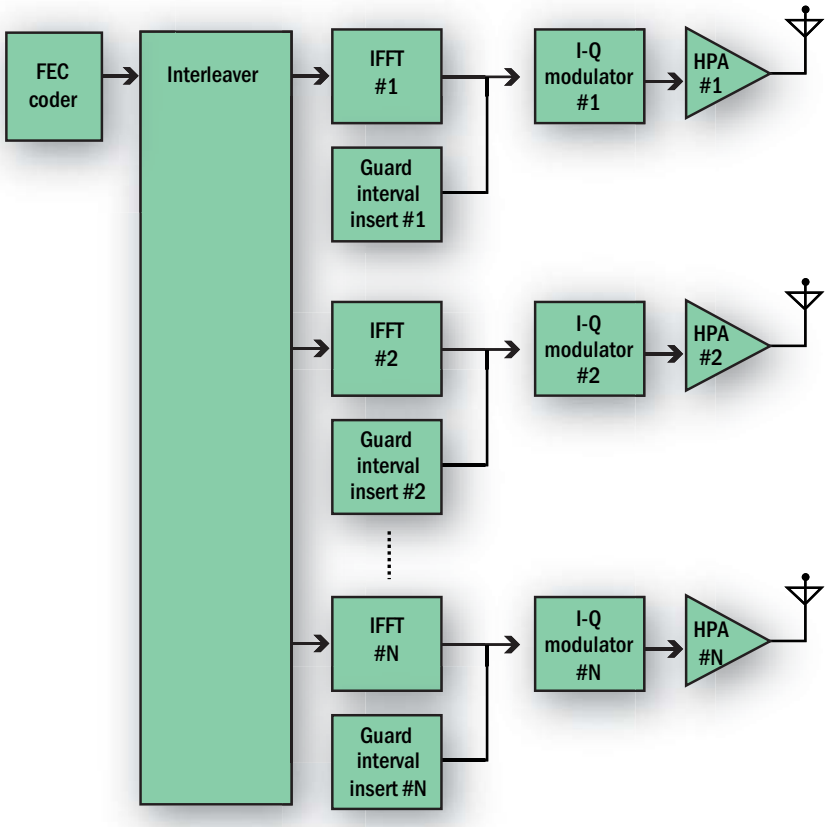
II.2.5 802.11n (MIMO-OFDM)

La velocidad real de transmisión podría llegar a los 600 Mbps (lo que significa que las velocidades teóricas de transmisión serían aún mayores), y debería ser hasta 10 veces más rápida que una red bajo IEEE 802.11a e IEEE 802.11g, y cerca de 40 veces más rápida que una red bajo IEEE 802.11b. También se espera que el alcance de operación de las redes sea mayor con este nuevo estándar gracias a la tecnología Múltiples Entradas - Múltiples Salidas (MIMO, *Multiple Input - Multiple Output*), que permite utilizar varios canales a la vez para enviar y recibir datos, gracias a la incorporación de varias antenas.

CAPÍTULO II

Existen también otras propuestas alternativas que podrán ser consideradas y se espera que el estándar, que debía ser completado hacia finales de 2006, se promulgue hacia 2008. No obstante, ya hay dispositivos que se han adelantado al protocolo y lo ofrecen de forma no oficial (con la promesa de actualizaciones para cumplir el estándar cuando el definitivo haya sido aprobado).

En la siguiente Figura se ilustra el Diagrama en Bloques de un transceptor (transmisor+receptor):



CAPÍTULO III
SEGURIDAD EN REDES Wi-Fi

III.1 SEGURIDAD Y AUTENTICACIÓN

Uno de los problemas más graves a los cuales se enfrenta actualmente la tecnología Wi-Fi es la seguridad. Un muy elevado porcentaje de redes son instaladas por administradores de sistemas y redes por su simplicidad de implementación sin tener en consideración la seguridad y, por tanto, convirtiendo sus redes en redes abiertas, sin proteger la información que por ellas circulan.

Para poder considerar una red inalámbrica como segura, debería garantizar los siguientes requisitos:

- Las ondas de radio deben confinarse tanto como sea posible, lo cual resulta de difícil implementación pero se puede llegar una solución de compromiso con antenas direccionales y configurando adecuadamente la potencia de transmisión de los APs.

- Debe implementarse algún mecanismo de autenticación de doble vía, que permita al cliente verificar que se está conectando a la red correcta, y a la red constatar que el cliente está autorizado para acceder a ella.

- Los datos deben viajar cifrados por el aire, para evitar que equipos ajenos a la red puedan interpretar la información.

CAPÍTULO III

Existen varios métodos para lograr la configuración segura de una red inalámbrica: filtrado de direcciones MAC, WEP, VPN, 802.1x y WPA; cada método logra un nivel diferente de seguridad y presenta ciertas ventajas y desventajas.

III.1.1 FILTRADO DE DIRECCIONES MAC

Este método consiste en la creación de una tabla de datos en cada uno de los APs. Dicha tabla contiene las direcciones MAC de las tarjetas de red inalámbricas que se pueden conectar al AP. Como cada tarjeta de red posee una dirección MAC única, se logra autenticar el equipo.

Este método tiene como ventaja su sencillez, pero posee desventajas en no ser perfectamente escalable, las direcciones MAC no son amigables lo que puede llevar a cometer errores en la manipulación de las listas y no garantiza la confidencialidad de la información transmitida al no proveer un mecanismo de cifrado.

III.1.2 WEP: *WIRED EQUIVALENT PRIVACY*

El algoritmo WEP, acrónimo de *Wired Equivalent Privacy*, forma parte de la especificación 802.11 y se diseñó con el fin de proteger los datos que se transmiten en una conexión inalámbrica mediante el cifrado. Está basado en el algoritmo de cifrado RC4, y utiliza claves de 64 bits o de 128 bits y el algoritmo de chequeo de integridad CRC.

CAPÍTULO III

El algoritmo WEP resuelve aparentemente el problema del cifrado de datos entre emisor y receptor. Sin embargo, existen dos situaciones que hacen que WEP no sea seguro en la manera que es empleado en la mayoría de las aplicaciones:

1. La mayoría de las instalaciones emplea WEP con claves de cifrado estáticas (se configura una clave en el AP y no se cambia nunca, o muy de vez en cuando). Esto hace posible que un atacante acumule grandes cantidades de texto cifrado con la misma clave y pueda intentar un ataque por fuerza bruta.

2. Existen en la actualidad distintas herramientas gratuitas para romper la clave secreta en enlaces protegidos con WEP. A pesar de estas vulnerabilidades el protocolo WEP sigue siendo popular debido a que es fácil de configurar y cualquier sistema con el estándar 802.11 lo soporta.

III.1.3 VPN: *VIRTUAL PRIVATE NETWORK*

Una red privada virtual (VPN) emplea tecnologías de cifrado para crear un canal virtual privado sobre una red de uso público. Estas redes han sido utilizadas desde 1990 en redes cableadas para asegurar las comunicaciones entre usuarios remotos y sus redes corporativas a través de Internet. Su funcionalidad puede ser adaptada a las WLAN.

CAPÍTULO III

Esta técnica provee una especie de túnel donde los datos viajan totalmente encriptados desde un sitio hasta otro. Un esquema básico de una VPN se muestra en la figura III.1. Los servidores de VPN se encargan de autenticar y autorizar a los clientes inalámbricos y de cifrar todo tráfico desde y hacia dichos clientes.

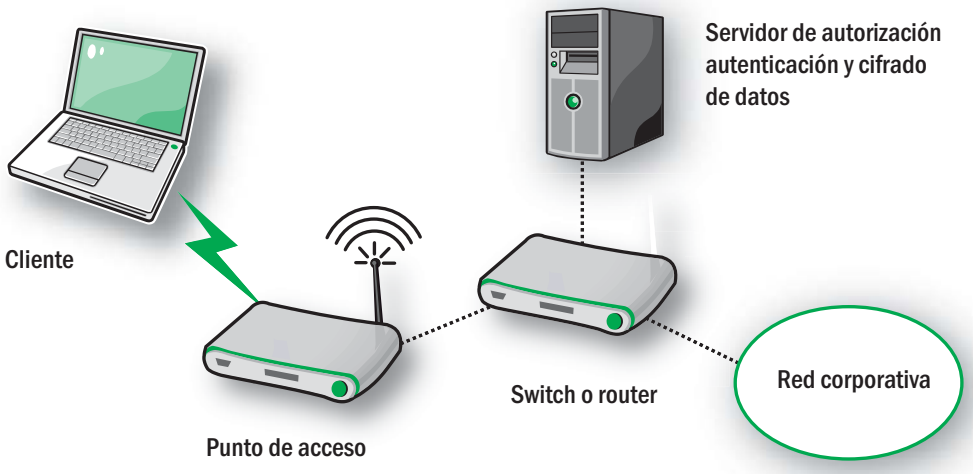


Figura III.1

III.1.4 AUTENTICACIÓN DE USUARIOS CON 802.1X

802.1x es un protocolo de control de acceso y autenticación basado en la arquitectura cliente/servidor, que restringe la conexión de equipos no autorizados a una red. El protocolo fue inicialmente creado por la IEEE para uso en redes de área local cableadas, pero se ha extendido también a las redes inalámbricas.

CAPÍTULO III

El protocolo 802.1x involucra tres participantes (figura III.2):

1. El equipo cliente que desea conectarse con la red.
2. El servidor de autorización/autenticación, que contiene toda la información necesaria para saber cuales equipos y/o usuarios están autorizados para acceder a la red. 802.1x fue diseñado para emplear servidores RADIUS (*Remote Authentication Dial-In User Service*), cuya especificación se puede consultar en el RFC 2058, del IETF.
3. El autenticador, que es el equipo de red (*switch, router*, servidor de acceso remoto, etc.) que recibe la conexión del cliente. El autenticador actúa como intermediario entre el cliente y el servidor de autenticación, y solamente permite el acceso del cliente a la red cuando el servidor de autenticación así lo autoriza.

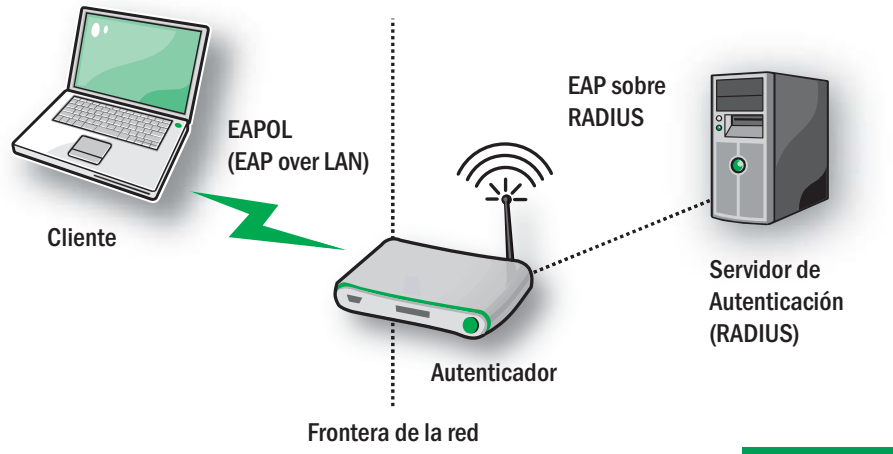


Figura III.2

CAPÍTULO III

La autenticación del cliente se lleva a cabo mediante el protocolo EAP (*Extensible Authentication Protocol*) y el servicio RADIUS.

Existen diversas variantes del protocolo EAP, según la modalidad de autenticación que se emplee. Se puede hablar de dos grupos de variantes: las que emplean certificados de seguridad, y las que utilizan contraseñas.

Las variantes de EAP que emplean certificados de seguridad son las siguientes:

- **EAP-TLS:** requiere de instalación de certificados en los clientes y en el servidor. Proporciona autenticación mutua fuerte (es decir, el servidor autentica al cliente y viceversa) y soporta el uso de claves dinámicas para WEP. La sesión de autenticación entre el cliente y el autenticador se cifra empleando el protocolo TLS (*Transport Layer Security*)

- **EAP-TTLS:** proporciona servicios similares a EAP-TLS, con la diferencia de que requiere solamente la instalación de un certificado en el servidor. Esto garantiza la autenticación fuerte del servidor por parte del cliente; la autenticación del cliente por parte del servidor se efectúa una vez que se establece la sesión TLS, utilizando otro método tal como PAP, CHAP, MS-CHAP o MS-CHAP v2.

CAPÍTULO III

- **PEAP:** funciona de manera parecida a EAP-TTLS, en el sentido de que solamente requiere de certificado de seguridad en el servidor. Provee protección a métodos más antiguos de EAP, mediante el establecimiento de un túnel seguro TLS entre el cliente y el autenticador.

Las variantes de EAP que utilizan contraseñas son las siguientes:

- **EAP MD5:** emplea un nombre de usuario y una contraseña para la autenticación. La contraseña se transmite cifrada con el algoritmo MD5.

- **LEAP:** Emplea un esquema de nombre de usuario y contraseña, y soporta claves dinámicas WEP.

- **EAP-SPEKE:** Esta variante emplea el método SPEKE (*Simple Password-authenticated Exponential Key Exchange*), que permite verificar que tanto cliente como servidor comparten una información secreta (en este caso una contraseña) a través de un medio inseguro. Se ha comprobado que el método es muy seguro, aún con contraseñas cortas. Ofrece protección contra ataques de diccionario, así como el servicio de autenticación mutua sin necesidad de certificados. Muchos proveedores lo implementan por ser un método de autenticación robusto y sencillo.

CAPÍTULO III

III.1.5 WPA: *Wi-Fi PROTECTED ACCESS*

WPA es un estándar propuesto por los miembros de la Alianza Wi-Fi (que reúne a los grandes fabricantes de dispositivos WLAN) en colaboración con la IEEE. Este estándar busca subsanar los problemas de WEP, mejorando el cifrado de los datos y ofreciendo un mecanismo de autenticación.

Para solucionar el problema de cifrado de los datos, WPA propone un nuevo protocolo para cifrado, conocido como TKIP (*Temporary Key Integrity Protocol*). Este protocolo se encarga de cambiar la clave compartida entre punto de acceso y cliente cada cierto tiempo, para evitar ataques que permitan revelar la clave. Igualmente se mejoraron los algoritmos utilizados por WEP.

El mecanismo de autenticación usado en WPA emplea 802.1x y EAP, que fueron mencionados en la sección anterior.

Según la complejidad de la red, un punto de acceso compatible con WPA puede operar en dos modalidades:

- Modalidad de red empresarial: para operar en esta modalidad se requiere de la existencia de un servidor RADIUS en la red. El punto de acceso emplea entonces 802.1x y EAP para la autenticación y el servidor RADIUS suministra las claves compartidas que se usarán para cifrar los datos.

CAPÍTULO III

- Modalidad de red casera, o PSK (*Pre-Shared Key*): WPA opera en esta modalidad cuando no se dispone de un servidor RADIUS en la red. Se requiere entonces introducir una contraseña compartida en el punto de acceso y en los distintos dispositivos móviles. Solamente podrán acceder al punto de acceso los dispositivos móviles cuya contraseña coincida con la del punto de acceso. Una vez logrado el acceso, TKIP entra en funcionamiento para garantizar la seguridad de acceso. Se recomienda que las contraseñas empleadas sean largas (20 caracteres o más), porque ya se ha comprobado que WPA es vulnerable a ataques de diccionario si se utiliza una contraseña corta.

Adicionalmente a la autenticación y cifrado, WPA también mejora la integridad de la información cifrada. El chequeo de redundancia cíclica (CRC - *Cyclic Redundancy Check*) utilizado en WEP es inseguro, ya que es posible alterar la información y actualizar el CRC del mensaje sin conocer la clave WEP. WPA implementa un código de integridad del mensaje (MIC - *Message Integrity Code*), también conocido como "*Michael*". Además, WPA incluye protección contra ataques de repetición (*replay attacks*), ya que incluye un contador de tramas.

La norma WPA data de abril de 2003, y es de cumplimiento obligatorio para todos los miembros de la Alianza Wi-Fi a partir de

CAPÍTULO III

finales de 2003. Según la Alianza Wi-Fi, todo equipo de red inalámbrica que posea el sello "*Wi-Fi Ceritified*" podrá ser actualizado por *software* para que cumpla con la especificación WPA.

Existe una versión mejorada de WPA llamada versión 2 (WPA2), que se encuentra basada en el estándar 802.11i (802.1x, TKIP y AES).

CAPÍTULO IV
NORMALIZACIÓN

IV.1 NORMALIZACIÓN

El problema principal que pretende resolver la normalización es la compatibilidad. No obstante existen distintos estándares que definen distintos tipos de redes inalámbricas. Esta variedad produce confusión en el mercado y descoordinación en los fabricantes. Para resolver este problema, los principales vendedores de soluciones inalámbricas (3COM, AIRONES, ITERSIL, LUCENT TECHNOLOGIES, NOKIA y SYMBOL TECHNOLOGIES) crearon en 1999 una asociación conocida como WECA (*Wireless Ethernet Compability Aliance*, Alianza de Compatibilidad Ethernet Inalámbrica). El objetivo de esta asociación fue crear una marca que permitiese fomentar más fácilmente la tecnología inalámbrica y asegurase la compatibilidad de equipos.

De esta forma desde abril de 2000 WECA certifica la interoperabilidad de equipos según la norma 802.11 bajo la marca Wi-Fi. Esto quiere decir que el usuario tiene la garantía de que todos los equipos que tenga el sello Wi-Fi pueden trabajar juntos sin problemas, independientemente del fabricante de cada uno de ellos. A partir del año 2003 WECA cambió de nombre, pasando a denominarse Alianza Wi-Fi.

En todos los productos que cumplen con la certificación suelen aparecer los siguientes logotipos, según para las normas que fueran certificados.

CAPÍTULO IV

IV.2 PROGRAMA DE CERTIFICACIÓN

La Alianza de Wi-Fi ha trabajado con sus miembros para certificar más de 3300 productos. El programa de certificación asegura que los productos WLAN puedan funcionar entre múltiples fabricantes. Como resultado el programa de certificación ha hecho posible la rápida adopción de productos Wi-Fi en hogares, oficinas y lugares de acceso público alrededor del mundo.

El programa de certificación cubre las siguientes categorías:

PROGRAMA OBLIGATORIO

- Productos Wi-Fi basados en estándares de radio 802.11a, 802.11b, 802.11g en modo simple y dual (802.11b y 802.11g) o productos multibandas (2,4 GHz y 5 GHz)

- Seguridad de red inalámbrica: mecanismos de seguridad WPA (*Wi-Fi Protected Access*) y WPA2 (*Wi-Fi Protected Access Version 2*)

- Mecanismos de autenticación usado para validar la identidad de los dispositivos de red: EAP (*Extensible Authentication Protocol*)

CAPÍTULO IV

PROGRAMAS OPCIONALES

- Perfiles de configuración de seguridad (WPS - *Wi-Fi Protected Setup*): facilidades de seguridad usando un número de identificación personal (PIN) o un interruptor localizado sobre el dispositivo.

- Soporte de multimedia: WMM (Wi-Fi Multimedia) activado para priorizar tráfico generado por diferentes aplicaciones, usando mecanismos de calidad de servicio (QoS).

- Resguardo de energía para contenido multimedia: ayuda a conservar la vida útil de la batería mientras se usan aplicaciones de voz y multimedia de manera de administrar el momento en que el dispositivo debe ser activado.

- Convergencia de dispositivo con tecnología Wi-Fi y celular: provee información detallada acerca del rendimiento del radio Wi-Fi en un teléfono celular, mide cómo interactúan uno con el otro.

Los ensayos de certificación Wi-Fi son realizados por 11 laboratorios independientes ubicados en los países de: España, Taiwán, Japón, Alemania, China, Corea, India y Estados Unidos. Independientemente de ello, cada país es soberano y tiene derecho a realizar sus propias certificaciones y Homologaciones (permiso para comercializar los equipos en el país). En Argentina, dicho equipamiento debe someterse a ensayo bajo la Norma

CAPÍTULO IV

Técnica CNC-Q2-63.01 y cumplimentar una Carpeta Técnica para aspirar a obtener la Homologación.

IV.3 EQUIPOS CERTIFICADOS

Existen una gran variedad de equipos certificados. Entre ellos podemos mencionar, según la categoría a:

EQUIPAMIENTO DE REDES

- Puntos de acceso (APs) para pequeñas oficinas, oficinas hogareñas (SOHO)
- Puntos de acceso para empresas
- *Switchs*
- *Routers*
- *Gateways* para cable y ADSL (integrado en dispositivos de acceso para el hogar)

ELECTRÓNICA DE CONSUMO

- Cámaras Web
- Cámaras digitales
- Cámaras de video
- Audio digital portátil
- Reproductores MP3
- *Set top Box*
- Reproductores de DVD / DVR
- Televisión
- Consolas de Juegos

CAPÍTULO IV

DISPOSITIVOS DE COMPUTACIÓN

- Tarjetas adaptadoras externas
- Tarjetas adaptadoras internas
- Computadoras *Laptop*
- Agendas, PDA (*Personal Digital Assitant*)
- Impresoras o servidores de impresión (incluyendo scanner y fax)

DISPOSITIVOS DE VOZ

- Teléfonos, modo dual (Wi-Fi y celular)
- Teléfonos, modo simple (Wi-Fi solamente)
- Teléfonos inteligentes o *Smartphone*, modo dual (Wi-Fi y celular)
- Teléfonos inteligentes o *Smartphone*, modo simple (Wi-Fi solamente)

Y muchos otros dispositivos que puedan necesitar una conexión externa.

Se puede obtener un listado completo de equipos que tienen la certificación Wi-Fi en **www.wirelessethernet.org/certified_products.asp** y en nuestra página web **www.cnc.gov.ar** los equipos homologados en el país.

CAPÍTULO IV

EQUIPAMIENTO DE REDES:



ELECTRÓNICA DE CONSUMO:



DISPOSITIVOS DE COMPUTACIÓN:



DISPOSITIVOS DE VOZ:


CAPÍTULO V
USOS Y APLICACIONES

V.1 APLICACIONES

Si bien el estándar 802.11 ha sido orientado al desarrollo de redes de área local inalámbrica con aplicación dentro de espacios interiores, esto no ha sido impedimento para que existan aplicaciones Wi-Fi más allá de su concepción inicial, llegándose incluso a pensar en la posibilidad de dar cobertura inalámbrica a áreas metropolitanas, cubriendo por entero una ciudad.

Existen dos ámbitos de aplicación de la tecnología Wi-Fi. Estos pueden ser para uso privado o en aplicaciones de entornos públicos.

En las de uso privado, podemos tener aplicaciones de hogar y de empresas que incorporan a Wi-Fi como una plataforma de interconexión de dispositivos variados (*Access Points* Wi-Fi + MODEM ADSL/Cable + *Router* + Cámaras, etc.). Wi-Fi en la empresa aparece como extensión inalámbrica de las redes de área local (LAN), permitiendo principalmente el beneficio de movilidad y eliminación de cableado.

Otras aplicaciones permiten a las empresas la interconexión de edificios cercanos, para lo cual son necesarias antenas direccionales y de alta ganancia, con línea de visión directa entre los puntos de conexión. Las distancias que son alcanzables (dentro de los límites de potencia máxima permitida) superan en ocasiones los 15 km. Este tipo de enlace punto a punto o punto multipunto permite la creación de conexiones inalámbricas de bajo costo y alto ancho de banda.

CAPÍTULO V

Una red pública Wi-Fi para el acceso a Internet se denomina PWLAN (*Public Wireless LAN*). Bajo este tipo de uso están apareciendo compañías denominadas WISP (*Wireless Internet Service Provider*, Proveedor de Servicio de Internet Inalámbrico), que ofrecen servicios de acceso a Internet dentro de espacios estratégicos de uso público como pueden ser hoteles, aeropuertos, restaurantes, estaciones de subterráneos y ferrocarriles, etc.. Estos lugares donde se presta el servicio se denominan *hot spots* públicos. Su mercado objetivo es el formado por los denominados trabajadores móviles, aquellos que pasan gran tiempo fuera de su oficina y que utilizan el acceso a Internet como parte de su trabajo diario. Podemos encontrar *hot spots* gratuitos donde el gestor de espacio decide desplegar una infraestructura Wi-Fi y ofrecer el servicio como un añadido a su oferta.

V.2 BANDAS DE FRECUENCIAS

Los dispositivos inalámbricos son construidos para operar en una cierta banda de frecuencias. Cada banda de frecuencias tiene asociada un ancho de banda que se encuentra ligado en gran medida con la capacidad de transmitir datos que se puede obtener en los enlaces.

El estándar 802.11 ocupa, entre otras, las bandas de frecuencias designadas para aplicaciones industriales, científicas y médicas (ICM) en las porciones de frecuencias comprendidas entre 2400 MHz - 2500 MHz y 5725 MHz - 5875 MHz. Las bandas ICM están atribuidas a equipos relacionados con procesos industriales, científicos o médicos. Entre

CAPÍTULO V

estos dispositivos podemos encontrar los hornos microondas que operan en 2,4 GHz, teléfonos inalámbricos, dispositivos *Bluetooth*, etc.

La atribución del espectro es controlada rigurosamente por la autoridad regulatoria de cada país, la cual fija las condiciones técnicas y operativas de la misma. Resultan interesantes las distintas alternativas dadas por los distintos Organismos Mundiales y Administraciones de los países. En el próximo capítulo se analizarán las atribuciones de bandas de frecuencias para nuestro país para estos sistemas.

V.2.1 UIT: UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

La UIT en su artículo 5 referido a atribución de frecuencia para la Región 2 (en la cual está incluida América) atribuye la banda 2400 MHz a 2500 MHz con categoría primaria a los servicios fijo, móvil y de radiolocalización y la banda 5725 MHz - 5825 MHz con categoría primaria al servicio de radiolocalización.

Asimismo, en su artículo 5.150 determina que ambas bandas de frecuencias están designadas para aplicaciones industriales, científicas y médicas (ICM). Los servicios de radiocomunicaciones que funcionan en estas bandas deben aceptar la interferencia perjudicial resultante de las aplicaciones ICM.

CAPÍTULO V

V.2.2 REGULACIÓN INTERNACIONAL

Los estándares 802.11b y 802.11g comparten la misma banda de frecuencias, con lo cual están sujetos a los mismos requerimientos regulatorios y usan la misma canalización como se muestra en la tabla 5, en la cual se observa que existen 14 canales con una separación de 5 MHz, siendo el ancho de banda de 22 MHz.

TABLA 5

Número de canal	Frecuencia central (MHz)	USA/Canadá	Europa	Japón
1	2412	Si	Si	Si
2	2417	Si	Si	Si
3	2422	Si	Si	Si
4	2427	Si	Si	Si
5	2432	Si	Si	Si
6	2437	Si	Si	Si
7	2442	Si	Si	Si
8	2447	Si	Si	Si
9	2452	Si	Si	Si
10	2457	Si	Si	Si
11	2462	Si	Si	Si
12	2467	No	Si	Si
13	2472	No	Si	Si
14	2484	No	No	Si

Como puede observarse, el ancho de banda de la señal (22 MHz) es superior a la separación entre canales consecutivos (5 MHz), por

CAPÍTULO V

eso se hace necesaria una separación de al menos 5 canales con el fin de evitar interferencias entre celdas adyacentes. Tradicionalmente se utilizan los canales 1, 6 y 11, aunque se ha documentado que el uso de los canales 1, 5, 9 y 13 no es perjudicial para el rendimiento de la red.

Para el estándar 802.11a, los identificadores de canales, frecuencias centrales y regulaciones son mostrados en la tabla 6. Para este caso también el ancho de banda de la señal es de 22 MHz.

TABLA 6

Número de canal	Frecuencia central (MHz)	USA/Canadá	Europa	Japón
34	5170	No	Si	Si
36	5180	Si	No	No
38	5190	No	Si	Si
40	5200	Si	No	No
42	5210	No	Si	Si
44	5220	Si	No	No
46	5230	No	Si	Si
48	5240	Si	No	No
52	5260	Si	Si	Si
56	5280	Si	Si	Si
60	5300	Si	Si	Si
64	5320	Si	Si	Si
149	5745	Si	Si	Si
153	5765	Si	Si	Si
157	5785	Si	Si	Si
161	5805	Si	Si	Si

CAPÍTULO V

Para la compatibilidad con sistemas de radar existentes y evitar interferencias con comunicaciones por satélite, en Europa se requiere la implementación de un control dinámico de las frecuencias y un control automático de las potencias de transmisión, respectivamente. Es por eso que para su uso en Europa, las redes 802.11a deben incorporar las modificaciones del 802.11h, equivalente al 802.11j de Japón.

A parte de las frecuencias permitidas, todas las regulaciones establecen valores máximos de la potencia radiada isotrópica efectiva (PIRE), lo cual conlleva a una combinación apropiada entre el nivel de potencia y la ganancia de antena. A modo de ejemplo, para el 802.11a, Japón establece como límite máximo 10mW/MHz, USA establece 160 mW sobre los canales 36 a 48 y 800 mW sobre los canales 52 a 64. Así también para el 802.11b/g, USA establece un máximo de 4W, Europa de 100 mW y Japón 10 mW/MHz.

CAPÍTULO VI
REGLAMENTACIÓN NACIONAL

VI.1 REGLAMENTACIÓN EN ARGENTINA

Las bandas de frecuencias atribuidas en Argentina para la implementación de la tecnología Wi-Fi son las siguientes:

- 2400 MHz a 2483,5 MHz
- 5250 MHz a 5350 MHz
- 5725 MHz a 5850 MHz

Las mismas se desprenden del Cuadro de Atribución de Bandas de Frecuencias de la Republica Argentina (CABFRA).

Para la gestión de la autorización de una determinada frecuencia de operación, lo primero que se debe determinar es el uso que se dará al sistema a implementar, el cual será para uso privado o para prestar un servicio.

La modalidad de prestador, está orientada a dar un servicio a terceros, para lo cual se requiere previamente a la autorización de la frecuencia, la obtención de la licencia única de prestación de servicio de telecomunicaciones.

Cuando el sistema se utiliza para uso privado, sólo es necesario gestionar la autorización de las frecuencias a emplear.

De acuerdo a las bandas de frecuencias y a las tecnologías que se pretendan implementar, se involucrarán diferentes Resoluciones, de las cuales se enunciarán brevemente los conceptos principales.

CAPÍTULO VI

De lo enunciado en los párrafos anteriores se destaca que, independientemente de la modalidad de uso a adoptar, es necesario solicitar siempre la autorización de las frecuencias a emplear y abonar la correspondiente tasa radioeléctrica por el uso del espectro.

Asimismo, se deberá tener en cuenta el nivel de radiaciones no ionizantes (RNI), a través de las cuales se determina si una estación radioeléctrica se encuentra dentro de los niveles máximos permisibles de exposición de los seres humanos a dichas radiaciones, establecidos en la Resolución 202/95 del Ministerio de Salud, y reglamentado por la Resolución CNC 3690/2004.

La actividad de estas estaciones radioeléctricas no estará garantizada contra interferencias perjudiciales provenientes de otras estaciones autorizadas.

En todos los casos, los equipos a utilizar deberán estar homologados (independientemente de las certificaciones internacionales que dispongan) por esta Comisión Nacional. Recordemos que la Homologación es el permiso que otorga la CNC para comercializar y/o utilizar equipos de comunicaciones en el territorio nacional, como se explicara anteriormente. Todo equipo que haga uso del espectro radioeléctrico, se conecte a la Red Telefónica Pública Conmutada (RTPC) o sirva de interconexión entre prestadores, deberá estar homologado. Algunos ejemplos son: los equipos Wi-Fi bajo estudio en esta publicación, teléfonos inalámbricos y convencionales, contestadores telefónicos, identificadores de llamadas, *routers* y *gateways*.

CAPÍTULO VI

Toda la información requerida para tramitar la obtención de la licencia de prestador y la autorización de las frecuencias, se solicitará en el Centro de Atención al Usuario del Espectro Radioeléctrico (CAUER) de la Comisión Nacional de Comunicaciones. El trámite de homologación lo debe iniciar el fabricante o importador, que a su vez debe estar inscripto en los Registros de Actividades de Telecomunicaciones de esta CNC, y todos los requisitos se encuentran disponibles en nuestra página web **www.cnc.gov.ar**.

VI.2 CUADRO DE ATRIBUCIÓN DE BANDAS DE FRECUENCIAS DE LA REPÚBLICA ARGENTINA

Secciones del Cuadro de Atribución de Bandas de Frecuencias de la República Argentina correspondientes a las porciones espectrales en donde es posible la implementación de la tecnología Wi-Fi.

ATRIBUCIÓN EN LA REPÚBLICA ARGENTINA [MHz]	OBSERVACIONES
2400 - 2450	Sistemas de espectro ensanchado Resolución SC 302/1998 Resolución SC 463/2001 Resolución SC 210/2004 Resolución SC 264/2004
FIJO	Sistemas de modulación digital de banda ancha Resolución SC 213/2004 Resolución SC 261/2005
Aficionados	Sistemas Multicanales Digitales (MXD) Punto a Punto y Punto a Multipunto de 2 - 2x2 y 8 Mbps Resolución CNT 2860/1992

CAPÍTULO VI

ATRIBUCIÓN EN LA REPÚBLICA ARGENTINA [MHz]	OBSERVACIONES
2450 - 2483,5 FIJO	Sistemas de espectro ensanchado Resolución SC 302/1998 Resolución SC 463/2001 Resolución SC 210/2004 Resolución SC 264/2004 Sistemas de modulación digital de banda ancha Resolución SC 213/2004 Resolución SC 261/2005 Sistemas Multicanales Digitales (MXD) Punto a Punto y Punto a Multipunto de 2 - 2x2 y 8 Mbps Resolución CNT 2860/1992
5250 - 5255 RADIOLOCALIZACIÓN Investigación espacial.	Resolución SC 288/2002
Fijo 5255 - 5350 RADIOLOCALIZACIÓN. FIJO	Resolución SC 288/2002
5725 - 5850 RADIOLOCALIZACIÓN Fijo Aficionados	Sistemas de espectro ensanchado Resolución SC 302/1998 Resolución SC 463/2001 Resolución SC 210/2004 Resolución SC 264/2004 Digitales banda ancha Resolución SC 288/2002 Resolución SC 261/2005

CAPÍTULO VI

VI.3 DESCRIPCIÓN DE LAS PRINCIPALES RESOLUCIONES

RESOLUCIÓN SC 2102/1992

A través de la misma se aprobó el reglamento para sistemas que utilizaran técnicas de espectro ensanchado, el cual se aplicaba exclusivamente a sistemas del servicio fijo y sistemas con terminales móviles en espacios limitados.

Las bandas de frecuencias permitidas eran:

a) 902 MHz a 928 MHz
b) 2400 MHz a 2483,5 MHz
c) 5725 MHz a 5850 MHz

La operación de estos sistemas estaba condicionada a no causar interferencia perjudicial a otros sistemas autorizados, como asimismo tolerar la interferencia proveniente de esos sistemas autorizados, contra la cual no estarían protegidos.

Para obtener la pertinente autorización, los equipos a utilizar deberían estar homologados y haber realizado la declaración jurada de las estaciones a operar.

RESOLUCIÓN SC 302/1998

Ante el avance de la tecnología se debió actualizar la normativa vigente al momento del dictado de la presente, con el agregado de especificaciones técnicas a cumplir.

CAPÍTULO VI

Entre las modificaciones principales se destacan las siguientes:

a) Documentación técnica y administrativa para la homologación de los equipos.

b) Potencia máxima admisible.

En las bandas de 2400 MHz a 2483,5 MHz y de 5725 MHz a 5850 MHz la potencia máxima es de 1 Watt.

c) Ganancia de antena

En la banda de 2400 MHz a 2483,5 MHz, si la ganancia de antena supera los 6 dBi, debe reducirse 1 dB la potencia máxima del transmisor por cada 3 dB que dicha ganancia supere los 6 dBi.

RESOLUCIÓN SC 463/2001

Esta Resolución surge debido a la creciente demanda para prestar servicios públicos de telecomunicaciones en las bandas atribuidas a espectro ensanchado por parte de los prestadores, es decir aquellos que poseen una licencia única de prestación de servicios de telecomunicaciones.

Se autorizó el uso con modalidad compartida de la banda de 2400 MHz a 2483,5 MHz a los sistemas que utilizaran la técnica de espectro ensanchado comprendidos en la Resolución SC 302/1998 para la prestación de servicios de telecomunicaciones. Estos sistemas no deberían producir interferencia perjudicial sobre los sistemas multicanales digitales existentes en dicha banda. En caso de nuevas asignaciones, la Comisión Nacional de Comunicaciones se reservará el

CAPÍTULO VI

derecho de requerir los cálculos de interferencia correspondientes, aplicando el procedimiento establecido en la Directiva General N° 61.02 de este Organismo.

En esta misma Resolución también se autorizó la banda de 5725 MHz a 5850 MHz para los sistemas que utilizan la técnica de espectro ensanchado, para la prestación de servicios de telecomunicaciones.

La autorización en ambas bandas quedará sujeta al análisis de la presentación de la información técnica contenida en el Anexo de la presente Resolución.

RESOLUCIÓN SC 288/2002

Se autorizó el uso de las bandas de 5250 MHz a 5350 MHz y de 5725 MHz a 5825 MHz al servicio fijo con categoría secundaria a los sistemas radioeléctricos de acceso local de uso privado que empleen comunicaciones bidireccionales de datos con técnicas de modulación digital de banda ancha, en las cuales se incluye la técnica de multiplexación por división de frecuencias ortogonales conocido con el nombre de OFDM, que fuera explicada en el Capítulo II.2.3.

La configuración de la red para la banda de 5250 MHz a 5350 MHz será punto a multipunto. En esta banda se excluye la utilización de la técnica de espectro ensanchado. Por otro lado, la parte alta de la banda, es decir de 5725 MHz a 5825 MHz, se utilizará en configuración punto a punto.

Los equipos deberán estar homologados por esta CNC, mientras

CAPÍTULO VI

que las emisiones radioeléctricas deberán cumplir los requerimientos técnicos indicados en la presente Resolución.

La autorización de estos sistemas será de categoría secundaria.

RESOLUCIÓN SC 213/2004

Se autorizó para la prestación de servicios de telecomunicaciones, excepto los de telefonía el empleo de la banda de 2400 MHz a 2483,5 MHz en la modalidad compartida, mediante el uso de sistemas radioeléctricos de acceso local que empleen comunicaciones bidireccionales de datos con técnicas de modulación digital de banda ancha, incluyendo los que utilizan la técnica de multiplexación por división de frecuencias ortogonales OFDM.

Estos sistemas no deberán producir interferencia perjudicial sobre los sistemas multicanales digitales existentes y también podrán destinarse para uso privado.

La autorización quedará sujeta al análisis de la presentación de la información requerida en la presente Resolución.

RESOLUCIÓN SC 264/2004

Se modifica la Resolución SC 210/2004, aclarando que en las bandas de 2400 MHz a 2483,5 MHz y de 5725 MHz a 5850 MHz para sistemas que utilizan la técnica de espectro ensanchado, se pueden prestar todos los servicios de telecomunicaciones, excepto los de telefonía en el Área Múltiple Buenos Aires (AMBA) y en las Áreas correspondientes a las capitales de todos los estados provinciales, además de Bahía Blanca [provincia de Buenos Aires (BA)], Mar del Plata (BA) y Rosario [provincia de Santa Fe (SF)].

CAPÍTULO VI

RESOLUCIÓN SC 261/2005

Mediante la presente se autoriza para la prestación de servicios de telecomunicaciones el uso de las bandas de 2400 MHz a 2483,5 MHz y de 5725 MHz a 5850 MHz en la modalidad compartida, mediante el empleo de sistemas radioeléctricos de acceso local para comunicaciones bidireccionales de datos con técnicas de modulación digital de banda ancha, diferentes de espectro ensanchado, incluyendo los que utilizan la técnica OFDM.

Los sistemas comprendidos en el párrafo anterior no podrán destinarse a brindar el servicio de telefonía en el Área Múltiple Buenos Aires (AMBA) y en las Áreas correspondientes a las capitales de todos los estados provinciales, además de Bahía Blanca [provincia de Buenos Aires (BA)], Mar del Plata (BA) y Rosario [provincia de Santa Fe (SF)].

RESOLUCIÓN CNC 3690/2004

Establécese que los titulares de autorizaciones de estaciones radioeléctricas y los licenciatarios de estaciones de radiodifusión deberán demostrar que las radiaciones generadas por las antenas de sus estaciones no afectan a la población en el espacio circundante a las mismas.

Hay que tener en cuenta que las mediciones se realizarán en las horas de mayor tráfico o de mayor potencia emitida.

No obstante, por las características técnicas de estas estaciones, las mismas se encontrarían exceptuadas de realizar las mediciones. A pesar de ello, cada estación deberá contar con la Declaración Jurada.

CAPÍTULO VI

VI.4 CUADRO COMPARATIVO DE MODALIDADES DE USO, TECNOLOGÍAS, BANDAS DE FRECUENCIAS Y RESOLUCIONES ASOCIADAS

USOS	TECNOLOGíAS	BANDAS DE FRECUENCIAS		
		2400 MHz a 2483,5 MHz	5250 MHz a 5350 MHz	5725 MHz a 5850 MHz
USO PRIVADO	SEE	Res. SC 302/1998	----------	Res. SC 302/1998
	OFDM	Res. SC 213/2004	Res. SC 288/2002	Res. SC 288/2002 (5725 MHz a 5825 MHz)
USO PRESTADOR	SEE	Res. SC 463/2001 Res. SC 264/2004	----------	Res. SC 463/2001 Res. SC 264/2004
	OFDM	Res. SC 213/2004	----------	Res. SC 261/2005

VI.5 COROLARIO

Independientemente del uso que se le pretenda dar a los sistemas que utilizan estas bandas de frecuencias, siempre se debe contar con la correspondiente autorización de la Comisión Nacional de Comunicaciones, para lo cual se deberán utilizar equipos homologados por la misma.

Si se desea utilizar la banda de 2400 MHz a 2483,5 MHz en calidad de prestador, se deberán realizar cálculos de compatibilidad electromagnética, de manera de no provocar interferencias a los sistemas MXD (multicanales digitales) que comparten la misma banda.

CAPÍTULO VII
CONCLUSIONES

VII.1 RESUMEN DE TECNOLOGÍAS

En el siguiente cuadro se detallan los estándares IEEE 802.11, conocidos como Wi-Fi, entre otros:

IEEE 802.11	Estándar para LANs inalámbricas (WLANs) en la Banda de Frecuencias de 2400 MHz a 2484 MHz. Se diferencia del IEEE 802.3 en las Capas Física y de Enlace de Datos. Utiliza espectro ensanchado por secuencia directa (DSSS) y tiene tasas de transferencia de 1 y 2 Mbps. Puesto que estas 2 velocidades de transmisión se encuentran generalmente presentes en la interfaz IEEE 802.11b, es que se las conoce también como IEEE 802.11b, o directamente 802.11b (a pesar de diferir en sus especificaciones).
IEEE 802.11a	Estándar para LANs inalámbricas (WLANs) en las Bandas de Frecuencias de 5,150 GHz a 5,350 GHz y de 5,725 GHz a 5,850 GHz. Utiliza multiplexación por división de frecuencias ortogonales (OFDM), alcanzando tasas de transferencia 6, 9, 12, 18, 24, 36, 48 y 54 Mbps, siendo las obligatorias a implementar 6, 12 y 24 Mbps.
IEEE 802.11b	Estándar para LANs inalámbricas (WLANs) en la Banda de Frecuencias de 2400 MHz a 2484 MHz. Utiliza espectro ensanchado por secuencia directa de alta tasa (HR/DSSS), siendo estas de 5,5 y 11 Mbps.
IEEE 802.11g	Estándar para LANs inalámbricas (WLANs) en la Banda de Frecuencias de 2400 MHz a 2484 MHz. Utiliza la misma tecnología OFDM que IEEE 802.11a, alcanzando tasas de transferencia 6, 9, 12, 18, 24, 36, 48 y 54 Mbps, pero en las mismas frecuencias de IEEE 802.11b.
IEEE 802.11h	Estándar para LANs inalámbricas (WLANs) en las Bandas de Frecuencias de 5,150 GHz a 5,350 GHz y de 5,725 GHz a 5,850 GHz. Variante europea de IEEE 802.11a, pero con la capacidad de seleccionar dinámicamente la frecuencia (DFS) y controlar la potencia de transmisión (TPC) para resolver los problemas derivados de la coexistencia con sistemas de Radares y Satélites en estas bandas, utilizadas generalmente por sistemas militares.
IEEE 802.11j	Estándar para LANs inalámbricas (WLANs) en las Bandas de Frecuencias de 5,150 GHz a 5,350 GHz y de 5,725 GHz a 5,850 GHz. Variante japonesa de IEEE 802.11a, pero con la capacidad de seleccionar dinámicamente la frecuencia (DFS) y controlar la potencia de transmisión (TPC) para resolver los problemas derivados de la coexistencia con sistemas de Radares y Satélites en estas bandas, utilizadas generalmente por sistemas militares.
IEEE 802.11n	Estándar para LANs inalámbricas (WLANs) en las Bandas de Frecuencias de 2400 MHz a 2484 MHz, de 5,150 GHz a 5,350 GHz y de 5,725 GHz a 5,850 GHz. Utiliza la misma tecnología OFDM que IEEE 802.11a e IEEE 802.11g, más la tecnología Múltiples Entradas - Múltiples Salidas (MIMO), alcanzando tasas de transferencia de hasta 600 Mbps.

CAPÍTULO VII

IEEE 802.11e	Añade al estándar 802.11 factores como calidad de servicio (QoS), permitiendo soportar tráfico en tiempo real en todo tipo de entornos y situaciones.
IEEE 802.11i	Intenta resolver los elementos de seguridad y encriptación del estándar básico. El estándar abarca los protocolos 802.1x, TKIP y AES. Se implementa WPA2.
IEEE 802.15	Estándar para PANs (*Personal Area Network*) en la Banda de Frecuencias de 2400 MHz a 2484 MHz. Utiliza espectro ensanchado por saltos de frecuencia (FHSS) y tiene tasas de transferencia del orden de 2 Mbps. Se lo conoce como *Bluetooth*. Pueden presentar interferencias con redes Wi-Fi, aunque en las últimas versiones se han actualizado sus especificaciones para permitir la coexistencia de dichas redes.
IEEE 802.15.4	Estándar para PANs (*Personal Area Network*) en la Banda de Frecuencias de 2400 MHz a 2484 MHz. Utiliza espectro ensanchado por secuencia directa (DSSS) y tiene bajas tasas de transferencia de 250 kbps. Se lo conoce como *Zig Bee*. Permiten realizar comunicaciones seguras de corto alcance y maximizan la vida útil de la batería.

CAPÍTULO VII

VII.2 VENTAJAS Y DESVENTAJAS

Esta tecnología posee las siguientes ventajas:

- La compatibilidad entre equipos de diferentes fabricantes garantizada por la certificación de la Alianza Wi-Fi, permite que estos dispositivos puedan interoperar.

- Los precios de este tipo de equipamiento se han reducido considerablemente, determinando en muchos casos que la solución WLAN sea más interesante que una solución cableada.

- La movilidad comienza a tomarse como un valor añadido al implementarse una red local.

- Muchos fabricantes de computadoras y PDA comienzan a incluir en la producción en serie interfaces Wi-Fi, permitiendo que aparezca como una buena alternativa para la interconexión de dispositivos.

- Dispositivos de comunicaciones móviles comienzan a incluir Wi-Fi de fábrica, lo que abre una gran incógnita respecto al desarrollo que esta tecnología puede llegar a alcanzar.

CAPÍTULO VII

Con respecto a las desventajas, podemos mencionar:

- Pérdida de velocidad en comparación a una conexión cableada, debido a las interferencias y pérdidas de señal que el ambiente pueda acarrear.

- Una de las desventajas fundamentales se encuentra en el campo de la seguridad. Una red configurada con WEP puede ser vulnerada por programas capaces de descifrar las claves. Sin embargo la Alianza Wi-Fi ha sacado el estándar WPA y posteriormente WPA2, basados en el grupo de trabajo 802.11i, siendo este último el protocolo de seguridad más seguro para Wi-Fi en este momento. No obstante requiere de *hardware* y *software* compatibles, ya que los antiguos no cuentan con dicho protocolo.

VII.3 FUTURO

Son muchas las expectativas creadas en torno a Wi-Fi, apoyadas en tres variables: la reducción de costos, la movilidad y el apoyo de fabricantes de equipamiento informático que intentan el crecimiento de esta tecnología, tanto en el ámbito del hogar y la empresa, como en el negocio de las telecomunicaciones.

La potenciación del desarrollo de Wi-Fi deberá contener las características básicas requeridas de: movilidad, facilidad de conexión para el usuario, dispositivos económicos y estándares interoperables.

CAPÍTULO VII

Wi-Fi no estaba pensada para realizar un despliegue a nivel nacional, provincial ni metropolitano (es decir, de gran cobertura), sino permitir su despliegue en pequeñas zonas, generalmente *indoor*, y está muy lejos de poder cubrir una área amplia al estilo de las redes móviles 1G y 2G. Sin embargo, permite realizar cobertura en base a pequeñas celdas en espacios de uso público, denominados *hot spots*, con la debida autorización del arrendador del espacio físico.

En lo que respecta a Argentina, últimamente observamos un gran incremento de solicitudes de autorización por parte de proveedores de servicio de Internet inalámbricos (WISP) para implementar esta tecnología en diversas localidades a lo largo de todo el país, en particular en aquellas regiones donde no hay otros accesos de banda ancha.

Nuevos estándares están apareciendo en los cuales se propone una cobertura de área metropolitana, quedando Wi-Fi para un entorno local, como complemento. Entre ellos podemos mencionar a WiMAX cuyo estándar es el IEEE 802.16, el cual opera en frecuencias de uso exclusivo, soporta calidad de servicio, no necesita línea de vista y permite movilidad. El mismo lo analizaremos en próximas publicaciones.

ANEXO

GLOSARIO DE TÉRMINOS, NEOLOGISMOS Y ACRÓNIMOS

µs	Microsegundos. 0,000001 s.
802.1x	Protocolo de control de acceso y autenticación basado en la arquitectura cliente/servidor, que restringe la conexión de equipos no autorizados a una red.
Access Point	Punto de Acceso. Ver AP.
ACK	*Acknowledgement*. Acuse de recibo. Se envía de la estación destino a la origen para confirmar que una trama fue recibida.
Ad hoc	Ver IBSS.
Address	Dirección.
ADSL	*Asymmetric Digital Subscriber Line*, Línea de Abonado Digital Asimétrica. Consiste en una línea digital de alta velocidad, apoyada en la línea telefónica convencional o línea de abonado. Es una tecnología de acceso a Internet de banda ancha, lo que implica capacidad para transmitir datos a mayor velocidad.
AES	*Advanced Encryption Standard*, Estándar de Encriptado Avanzado.
AMBA	Área Múltiple Buenos Aires.
AP	*Access Point*, Punto de Acceso. Equipo que permite interconectar dispositivos inalámbricos y redes fijas o de distribución.
Asociación	Servicio por el cual una estación pide ser reconocida por un AP.
Ataque de Diccionario	Un atacante intenta obtener la clave para ingresar a la red probando con las palabras utilizadas más frecuentemente.
Ataque por Fuerza Bruta	Un atacante acumula grandes cantidades de texto cifrado con la misma clave e intenta un ataque para ingresar a la red probando distintas combinaciones.
Ataques de Repetición	Para prevenir repetidos ataques para ingresar a la red WPA incluye un contador de tramas.
Autenticación	Servicio que verifica que las estaciones que acceden a la red están autorizadas. Prerrequisito necesario para la asociación.
Autenticador	Equipo de red que recibe la conexión del cliente.

ANEXO

Backbone	Conexiones o cableado troncal de la red.
Backoff	Intervalo extra aleatorio adicionado al tiempo indicado por el NAV.
Bandas de guarda	Bandas utilizadas para evitar interferencia entre los usuarios.
Beacon	Baliza. Tramas enviadas periódicamente por un AP para difundir su presencia y la información necesaria para poder identificar la red.
bit	*Binary Digit*, Dígito Binario. Unidad de medida de información digital, con dos estados posibles: 0 o 1.
bit	Unidad de datos de Capa Física.
Bluetooth	Como se conoce al estándar IEEE 802.15.
bps	Bits por segundo. Unidad de medida de velocidad de transmisión de datos.
BSS	*Basic Service Set*, Área de Servicio Básico. Área difusa donde se comunican un grupo de estaciones. Pueden ser Independientes (IBSS o *Ad Hoc*) o de Infraestructura.
BSS de Infraestructura	Red 802.11 donde las estaciones se comunican exclusivamente a través de un punto de acceso.
BSSID	Dirección del AP.
Byte	8 bits.
CABFRA	Cuadro de Atribución de Bandas de Frecuencias de la República Argentina.
Capa 1	Ver Capa Física.
Capa 2	Ver Capa de Enlace de Datos.
Capa 3	Capa de Red del modelo de referencia OSI.
Capa 4	Capa de Transporte del modelo de referencia OSI.
Capa de Enlace de Datos	Capa 2 del modelo de referencia OSI. Constituida por las capas MAC y LLC.
Capa Física	Capa 1 del modelo de referencia OSI. Ver PHY.
CAUER	Centro de Atención al Usuario del Espectro Radioeléctrico.

ANEXO

CCA	*Clear Channel Assessment*, Evaluación de Canal Libre. Técnica empleada para reportar si el medio se encuentra ocupado.
CCK	*Complementary Code Keying*, Modulación por Códigos Complementarios.
CHAP	*Challenge Handshake Authentication Protocol*, Protocolo de Autenticación de Intercambio de Señales de Desafío. Función de seguridad soportada en líneas que usan el encapsulamiento PPP para evitar el acceso no autorizado. CHAP no evita por sí mismo el acceso no autorizado, sino que simplemente identifica el extremo remoto. El *router* o servidor de acceso entonces determina si el usuario tiene el acceso permitido.
chips	Secuencia de bits de alta velocidad utilizada para modular la señal a transmitir en espectro ensanchado.
Claves de cifrado estáticas	Se configura una clave en el AP y no se cambia nunca, o muy de vez en cuando.
CNC	Comisión Nacional de Comunicaciones. Ex CNT.
CNT	Comisión Nacional de Telecomunicaciones.
Código de Dispersión	Ver Secuencia de Barker.
Código PN	Ver Ruido Pseudoaleatorio.
CRC	*Cyclic Redundancy Check*, Comprobación de Redundancia Cíclica. Control para la detección de errores de la trama MAC.
CSMA/CA	*Carrier Sense Multiple Access with Collision Avoidance*, Acceso Múltiple por Sensado de Portadora con Anulación de Colisiones. Técnica empleada en WLANs para evitar colisiones.
CSMA/CD	*Carrier Sense Multiple Access with Collision Detection,* Acceso Múltiple por Sensado de Portadora con Detección de Colisiones. Técnica usada en redes Ethernet para mejorar sus prestaciones. Los dispositivos de red que tienen datos para transmitir funcionan en el modo "escuchar antes de transmitir". Esto significa que cuando un nodo desea enviar datos, primero debe determinar si los medios de red están ocupados o no. A su vez, la estación está a la escucha a la vez que emite, de forma que si detecta que se produce una colisión, detiene inmediatamente la transmisión.
CTS	*Clear To Send*, Libre para Transmitir. Mecanismo por medio del cual se reserva el medio para que una determinada estación transmita, a fin de evitar colisiones.
DA	*Destination Address*. Dirección Destino. Dirección del receptor.

ANEXO

Data Whitener	Blanqueador de datos. Encriptador en FHSS.
DBPSK	*Differential Binary Phase Shift Keying,* Modulación por Corrimiento de Fase Binaria Diferencial.
DCF	*Distributed Coordination Function*, Función de Coordinación Distribuida. Mecanismo de acceso básico del estándar CSMA/CA.
Deautenticación	Servicio que termina la autenticación. Implica terminar con una asociación.
Desasociación	Servicio por el cual una estación pide ser removida de un AP.
DFS	*Dinamic Frequency Selection*, Selección Dinámicamente de Frecuencia. Capacidad de seleccionar dinámicamente la frecuencia para resolver los problemas derivados de la coexistencia con sistemas de Radares en las Bandas de Frecuencias de 5,150 GHz a 5,350 GHz y de 5,725 GHz a 5,850 GHz, utilizadas generalmente por sistemas militares.
DIFS	*DCF Interframe Space*, Espaciamiento Intertrama DCF.
Distribución	Servicio de envío de una trama aceptada por un AP al destino, en una red de infraestructura.
DQPSK	*Differential Quadrature Phase Shift Keying*, Modulación por Corrimiento de Fase en Cuadratura Diferencial.
DS	*Distribution System,* Sistema de Distribución.
DSSS	*Direct Sequence Spread Spectrum*, Espectro ensanchado por secuencia directa.
Duration/ID	Duración/Identificador. Bit que indica la identificación de la estación en ahorro de energía o el tiempo del NAV.
Dwell Time	Tiempo de Permanencia. Tiempo muy breve (< 400 ms) en el que se transmite información en una determinada frecuencia en FHSS.
EAP	*Extensible Authentication Protocol*, Protocolo de Autenticación Extensible. Utilizado para la autenticación del cliente. Pueden emplear certificados de seguridad o contraseñas.
EAP MD5	EAP que emplea un nombre de usuario y una contraseña cifrada en MD5 para la autenticación.
EAP-SPEKE	*EAP-Simple Password-authenticated Exponential Key Exchange*, Intercambio de Clave Exponencial Autenticada-Contraseña Simple. Permite verificar que tanto cliente como servidor comparten una contraseña a través de un medio inseguro.

ANEXO

EAP-TLS	EAP - *Transport Layer Security*, EAP-Seguridad de la Capa de Transporte. Variante de EAP que requiere de instalación de certificados en los clientes y en el servidor.
EAP-TTLS	EAP - *Tunneled TLS*, EAP-TLS Tunelizado. Similar a EAP-TLS, pero requiere la instalación de un certificado sólo en el servidor.
EIFS	*Extended Interframe Space*, Espaciamiento Intertrama Extendido.
Encriptador	Circuito que se utiliza para eliminar secuencias largas de 1's y 0's, tal que la señal a transmitir se asemeje más al ruido.
ERP	*Extended Rate PHY*, PHY de Tasa Extendida. Como se denomina a IEEE 802.11g, ya que la capa física no varía (respecto de IEEE 802.11b), pero la velocidad teórica máxima es la de IEEE 802.11a.
Escalable	Término que se utiliza para definir redes que pueden aumentar el número de usuarios.
ESS	*Extended Service Set,* Área de Servicio Extendida. Interconexión de distintas BSSs que permite extender el área de cobertura.
Ethernet	Tecnología de redes de computadoras de área local basada en tramas de datos. Define las características de cableado y señalización de nivel físico y los formatos de trama del nivel de enlace de datos del modelo OSI. Se refiere a las redes de área local y dispositivos bajo el estándar IEEE 802.3 que define el protocolo CSMA/CD, aunque actualmente se llaman así a todas las redes cableadas que usen ese formato de trama.
FCS	*Frame Check Sequence*. Secuencia de Comprobación de Trama. Campo de 32 bits conteniendo un CRC.
FDM	*Frequency Division Multiplexing,* Multiplexación por División de Frecuencias.
FEC	*Forward Error Correction*, Correción Progresiva de Errores. Técnica que permite al receptor detectar bits corruptos y repararlos.
FHSS	*Frequency Hopping Spread Spectrum*, Espectro ensanchado por saltos de frecuencia.
Gateways	Equipo para interconectar distintos tipos de redes.
GFSK	*Gaussian Frequency Shift Keying*, Modulación por Corrimiento de Frecuencia Gausiana.
GHz	GigaHertz. 1000000000 Hz.

ANEXO

Gp	Ganancia de Procesamiento. Relación entre la Anchura de Banda de la señal de Espectro Ensanchado (AB_{PN}) respecto de la Anchura de Banda de la señal Original (AB_O).
HCF	*Hybrid Coordination Function*, Función de Coordinación Híbrida. Permite a las estaciones mantener colas de múltiples servicios y balancear el acceso al medio a favor de aplicaciones que requieren mayor calidad de servicio.
Header Error Check Field	Utiliza un CRC de 16 bits para detección de errores en el encabezado PLCP.
HEC	Ver *Header Error Check Field.*
HiPeRLAN	*High Performance Radio Local Area Network*, Red de Área Local basada en Radio de Alto Rendimiento.
Homologación	Permiso que otorga el Estado Nacional para comercializar equipos de Telecomunicaciones en el País. En nuestro caso, dicha función está a cargo de la CNC y tiene como principios fundamentales velar por la seguridad del usuario, el uso eficiente del espectro radioeléctrico y la compatibilidad de las redes e interconexión entre prestadores. Este permiso se otorga previo análisis de cumplimiento con una Carpeta Técnica, que incluye también los Informes de Ensayo a los que deben ser sometidos los equipos para verificar que se ajustan a las Normas Técnicas establecidas por nuestra Administración. En el caso que los equipos sean utilizados para uso propio, este procedimiento se denomina Autorización.
Hot spot	Lugar donde se presta el servicio de Wi-Fi.
HR/DSSS	*High Rate Direct Sequence Spread Spectrum*, Espectro ensanchado por secuencia directa de alta tasa.
Hz	Hertz. Unidad de medida de frecuencia y anchura de banda. Cantidad de veces (Ciclos) por segundo que se repite una onda.
IBSS	*Independent Basic Service Set*, Área de Servicio Básico Independiente. Red 802.11 donde las estaciones se comunican directamente sin pasar por un punto de acceso. Conocidas como *ad hoc.*
ICI	*Inter Carrier Interference*, Interferencia entre Portadoras. Producida por pequeños corrimientos en las frecuencias de subportadoras.
ICM	Bandas de frecuencias atribuidas por la UIT al uso Industrial, Científico y Médico.
IEEE	*Institute of Electrical and Electronics Engineers*, Instituto de Ingenieros en Electricidad y Electrónica. Mayor asociación internacional sin fines de lucro formada por profesionales de 175 países en nuevas tecnologías, como ingenieros electrónicos, eléctricos, informáticos y en telecomunicación, dedicada a la generación de estándares, entre otras cosas.

ANEXO

IEEE 802.3	Estándar para redes de área local (LANs) Ethernet.
IEEE 802.16	Estándar para MANs. Ver WiMAX.
IETF	*Internet Engineering Task Force*, Grupo de Trabajo en Ingeniería de Internet. Organización internacional abierta de normalización, cuyo objetivo es contribuir a la ingeniería de Internet, actuando en diversas áreas, tales como transporte, enrutamiento y seguridad.
Indoor	Uso interno.
Integración	Servicio de conexión del sistema de distribución a una red distinta de IEEE 802.11.
Interleaving	Entrelazado. Las secuencias de bits deben ser transmitidas en subportadoras separadas y en distintas constelaciones, luego cada flujo de datos debe ser asociado a la subportadora correspondiente.
IR	Infrarrojo.
ISI	*Inter Symbol Interference*, Interferencia entre Símbolos. Producida por multicaminos.
ISM	*Industrial, Scientific and Medical*, Industrial, Científico y Médico. Ver ICM.
ISO	*International Standarization Organization*, Organización Internacional para la Estandarización. Compuesta por representantes de los organismos de normalización nacionales, produce normas industriales y comerciales, conocidas como normas ISO y su finalidad es la coordinación de las normas nacionales, en consonancia con el Acta Final de la Organización Mundial del Comercio, con el propósito de facilitar el comercio, facilitar el intercambio de información y contribuir con estándares comunes para el desarrollo y transferencia de tecnologías.
kbps	Kilo bits por segundo. 1000 bps.
LAN	*Local Area Network*, Red de Área Local. Es la interconexión de varias computadoras y periféricos. Su extensión está limitada físicamente a un edificio o a un entorno de hasta 100 metros.
Laptop	Computadora portátil.
LEAP	*Lightweight* EAP, EAP Liviano. Emplea un esquema de nombre de usuario y contraseña, y soporta claves dinámicas WEP.
LLC	*Logical Link Control*, Capa de Control de Enlace. Una de las subcapas de la Capa de Enlace de Datos (Capa 2) del modelo OSI, encargada del control de errores, control de flujo, tramas y direccionamiento de la otra subcapa (MAC).

ANEXO

MAC	*Media Access Control*, Control de Acceso al Medio. Subcapa de la Capa 2 (Capa de Enlace de Datos) del modelo de referencia OSI, encargada del direccionamiento físico, de la topología y del acceso a la red, de la notificación de errores, de la distribución ordenada de tramas y del control del flujo. Cualquier medio de transmisión debe ser capaz de proporcionar una transmisión sin errores, un tránsito de datos fiable a través de un enlace físico. Debe crear y reconocer los límites de las tramas, así como resolver los problemas derivados del deterioro, pérdida o duplicidad de las tramas. También puede incluir algún mecanismo de regulación del tráfico que evite la saturación de un receptor que sea más lento que el emisor.
MAN	*Metropolitan Area Network*, Red de Área Metropolitana.
Mapear	Proceso de asociación de las tramas MAC sobre el medio físico.
Mbps	Mega bits por segundo. 1000000 bps.
Mcps	Mega *chips* por segundo.
MD5	*Message-Digest Algorithm 5*, Algoritmo de Resumen del Mensaje 5. Algoritmo de reducción criptográfico.
MHz	MegaHertz. 1000000 Hz.
MIC	*Message Integrity Code*, Código de Integridad del Mensaje. Conocido como "*Michael*" y utilizado en WPA.
Michael	Ver MIC.
MIMO	*Multiple Input-Multiple Output,* Múltiples Entradas-Múltiples Salidas.
Modalidad de red casera	WPA opera en esta modalidad cuando no se dispone de un servidor RADIUS en la red. Se recomiendan claves de 20 caracteres o más.
Modalidad de red empresarial	Requiere un servidor RADIUS en la red.
More Data	Más Datos. Bit usado por el AP para indicar que hay más fragmentos para esa estación.
More Fragments	Más Fragmentos. Bit que indica si la trama MAC sufre alguna fragmentación.
ms	Milisegundos. 0,001 s.
MS-CHAP	MicroSoft-CHAP.
MS-CHAP V2	MicroSoft-CHAP Versión 2.

ANEXO

MSps	Mega Símbolos por segundo.
MXD	Sistemas Multicanales Digitales.
NAV	*Network Allocation Vector*, Vector de Asignación de Red. Temporizador que indica la cantidad de tiempo (expresado en microsegundos) que el medio será reservado.
Notebook	Computadora portátil.
OFDM	*Orthogonal Frequency Division Multiplexing,* Multiplexación por División de Frecuencias Ortogonales. Tecnología consistente en fraccionar un canal de gran anchura de banda en un número de subcanales ortogonales de banda angosta, los cuales serán usados en paralelo para aumentar la velocidad de transferencia de datos.
Order	Orden. Bit que indica que las tramas y fragmentos van a ser transmitidas en un estricto orden.
Ortogonal	Independiente.
OSI	*Open System Interconnection*, Interconexión de Sistemas Abiertos. Es un modelo de referencia de red descriptivo creado por ISO, marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones.
PAN	*Personal Area Network,* Red de Área Personal.
PAP	*Password Authentication Protocol*, Protocolo de Autenticación de Contraseña. Protocolo de autenticación que permite que los PPP iguales se autentiquen entre sí. El *router* remoto que intenta conectarse al router local debe enviar una petición de autenticación. A diferencia de CHAP, PAP pasa la contraseña y el nombre de usuario sin cifrar. PAP en sí mismo no impide el acceso no autorizado, sino que simplemente identifica el extremo remoto. Luego el *router* o servidor de acceso determina si se le concede acceso al usuario. PAP se soporta sólo en líneas PPP.
PBCC	*Packet Binary Convolution Code,* Código Convolucional Binario por Paquete.
PCF	*Point Coordination Function,* Función de Coordinación de Puntos. Provee servicios libres de contienda en redes de infraestructura.
PDA	*Personal Digital Assistant,* Asistente Digital Personal. Computadora de mano originalmente diseñada como agenda electrónica. En la actualidad corren distintos sistemas operativos.
PEAP	*Protected* EAP, EAP Protegido. Similar a EAP-TTLS (instala sólo un certificado en el servidor), pero más antiguo.

ANEXO

Performance	Rendimiento.
PHY	*Physical Layer*, Capa Física. Capa 1 del modelo de referencia OSI, encargada de las conexiones físicas de la computadora hacia la red, en lo que se refiere al medio físico (guiados: cable coaxil, cable de par trenzado, fibra óptica, etc.; no guiados: radiofrecuencias, infrarrojos, microondas, láser y otras redes inalámbricas); características del medio (tipo de cable o calidad del mismo; tipo de conectores normalizados o en su caso tipo de antena; etc.) y la forma en la que se transmite la información (codificación de señal, niveles de tensión/intensidad de corriente eléctrica, modulación, tasa binaria, etc.).
PIFS	PCF *Interframe Space*, Espaciamiento Intertrama PCF.
PIN	*Personal Identification Number*, Número de Identificación Personal.
PLCP	*Physical Layer Convergence Procedure*, Procedimiento de Convergencia de la Capa Física. Subcomponente de la Capa Física encargado de mapear las tramas MAC sobre el medio.
PLCP *Header*	Encabezado PLCP. Contiene información usada por la capa PHY para decodificar la trama.
PLCP *Signaling Field*	Campo de Señalización PLCP. Información contenida en el encabezado PLCP referente a velocidades de información.
PLCP PDU *Length Word*	Longitud de Palabra PLCP. Información contenida en el encabezado PLCP que representa el número de bytes contenido en el paquete.
PLW	Ver PLCP PDU *Length Word*.
PMD	*Physical Medium Dependent*, Dependiente del Medio Físico. Subcomponente de la Capa Física encargado de transmitir las tramas MAC.
Portadoras piloto	Utilizadas para monitorear la ICI.
Power Management	Gerenciamiento de Energía. Bit que indica si una estación entró en modo de ahorro de energía para conservar más duración de batería.
Power-Save	Ahorro de Energía. Ver *Power Management*.
PPP	*Point to Point Protocol*, Protocolo Punto a Punto. Suministra conexiones *router* a *router* y usuario a red.
Preámbulo	Parte constitutiva de una trama. Es dependiente de la capa PHY.
Privacidad	Servicio que permite tener la confidencialidad de los datos.

ANEXO

Protected Frame	Trama Protegida. Bit que indica si la trama está protegida por un protocolo de seguridad de la capa de enlace de datos.
PSF	Ver PLCP *Signaling Field.*
PSK	*Phase Shift Keying*, Modulación por Corrimiento de Fase.
PSK	*Pre-Shared Key,* Clave Pre-Compartida. En una red casera la clave se introduce en el AP y en cada computadora. Ver Modalidad de red casera.
PWLAN	*Public* WLAN. WLAN Pública.
QAM	*Quadrature Amplitud Modulation*, Modulación de Amplitud en Cuadratura.
QoS	*Quality of Service.* Calidad de Servicio. Consiste en priorizar cierto tipo de transmisiones.
R	Ver Tasa de código.
RA	Dirección del Receptor.
RADIUS	*Remote Authentication Dial-In User Service*, Servicio de Autenticación Remota de Usuario Llamante. Servidor utilizado en el protocolo 802.1x para autorización/autenticación.
Rake	Receptor rastrillo, se consigue con varios receptores en paralelo, levemente desfasados, donde cada componente se decodifica de forma independiente, pero en una última etapa se suman constructivamente con el objeto de sacar el máximo provecho de cada camino.
RC4	Algoritmo de cifrado.
Reasociación	Servicio por el cual una estación pide ser reconocida por otro AP cuando se mueve entre BSSs dentro de un ESS.
Retry	Retransmisión.
RFC 2058	*Request For Comments*, Pedido de Comentarios. En particular, 2058 especifica el uso de servidores RADIUS.
RNI	Radiaciones No Ionizantes.
Router	Enrutador. Equipo de red usado para la interconexión en Capa 3.
Replay Attacks	Ver Ataques de Repetición.
RTPC	Red Telefónica Pública Conmutada.

ANEXO

RTS	*Request To Send,* Requerimiento para Transmitir. Mecanismo por medio del cual la estación a transmitir envía al destinatario un pedido de transmisión y espera que la estación le responda que el medio se encuentra libre para hacerlo. Recién ahí envía los datos.
Ruido Pseudoaleatorio	Ver Código de Dispersión.
s	Segundo. Unidad de medida de tiempo.
SA	*Source Address*. Dirección Fuente. Dirección Origen o de transmisor.
SC	Secretaría de Comunicaciones.
Scrambler	Encriptador en DSSS.
Secuencia de Barker	Ver *chips*.
Servidor de acceso remoto	*Router* capaz de recibir llamadas de clientes remotos.
Set Top Box	Aparato que se coloca encima del televisor. Es el nombre con el que se conoce el dispositivo encargado de la recepción y opcionalmente decodificación de señal de televisión analógica o digital, para luego ser mostrada en un dispositivo de televisión.
SFD	*Start of Frame Delimiter*, Delimitador de Comienzo de Trama. Patrón de bits usados para delimitar el comienzo de trama incluido en el Preámbulo.
SIFS	*Short Interframe Space*, Espaciamiento Intertrama Corto.
Sistema de distribución	Interconexión de puntos de acceso que permite extender el área de cobertura de la red.
SOHO	*Small Office, Home Office*. Pequeña Oficina, Oficina Hogareña. Se refiere a entornos domésticos o de pequeña empresa con instalaciones y equipos informáticos de escasa potencia.
SS	*Spread Spectrum,* Espectro Ensanchado.
SSID	*Service Set Identifier,* Identificador de Conjuntos de Servicios. Nombre de red para todos los APs dentro de un ESS.
Switch	Conmutador. Equipo de red usado para la interconexión en Capa 2.
Synch	Secuencia de bits alternada de ceros y unos incluida en el Preámbulo usada para la sincronización del receptor.

ANEXO

TA	Dirección del Transmisor.
Tasa de código	Cantidad de bits de datos que se envían respecto de los totales.
t_G	Tiempo de guarda. Tiempo agregado para evitar ICI.
Throughput	Velocidad de transferencia de datos.
TKIP	*Temporary Key Integrity Protocol*, Protocolo de Integridad de Clave Temporal. Protocolo que se encarga de cambiar la clave compartida entre punto de acceso y cliente cada cierto tiempo, para evitar ataques que permitan revelar la clave.
TLS	*Transport Layer Security,* Seguridad de la Capa de Transporte. Protocolo de seguridad que cifra la sesión de autenticación entre el cliente y el autenticador.
Token Ring	Estándar de red de configuración en anillo con método de paso de testigo como control de acceso al medio.
TPC	*Transmit Power Control*, Control de Potencia de Transmisión. Capacidad de controlar la potencia de transmisión para resolver los problemas derivados de la coexistencia con sistemas de Satélites en las Bandas de Frecuencias de 5,150 GHz a 5,350 GHz y de 5,725 GHz a 5,850 GHz, utilizadas generalmente por sistemas militares.
Trama	Unidad de datos de Capa de Enlace de Datos.
Transceptor	Transmisor+Receptor.
Transición BSS	Movilidad entre BSSs. Las redes 802.11 no soportan movilidad entre ESSs.
UIT	Unión Internacional de Telecomunicaciones. Organismo de las Naciones Unidas encargado de hacer recomendaciones para el ámbito de las telecomunicaciones. Con sede en Ginebra (Suiza), está formada por 191 Estados Miembros y más de 700 Miembros del Sector y Asociados.
Viterbi	Algoritmo que permite encontrar la secuencia de bits transmitida más probable.
VPN	*Virtual Private Network*, Red Privada Virtual. Técnica que provee una especie de túnel donde los datos viajan totalmente encriptados desde un sitio hasta otro. Usada para asegurar las comunicaciones entre usuarios remotos y sus redes corporativas a través de Internet.
WECA	*Wireless Ethernet Compatibility Alliance*, Alianza para la Compatibilidad de Ethernet Inalámbrica. Cambió su denominación por Wi-Fi. Ver Wi-Fi.
WEP	*Wired Equivalent Privacy*, Privacidad Equivalente a la Cableada. Protocolo de Seguridad.

ANEXO

Wi-Fi	Alianza constituida por líderes en la industria con el objetivo de adoptar estándares reconocidos en el mundo entero para redes de área local inalámbricas de alta velocidad. Antes conocida como WECA. También se utiliza directamente este nombre para identificar dichas redes.
Wi-Fi Ceritified	Wi-Fi Certificado. Todo equipo de red inalámbrica que posea este sello podrá ser actualizado por software para que cumpla con la especificación WPA, según la Alianza Wi-Fi.
Wi-Fi Multimedia	Soporte de multimedia. Programa para priorizar tráfico generado por diferentes aplicaciones, usando mecanismos de calidad de servicio (QoS).
Wi-Fi Protected Setup	Perfiles de configuración de seguridad. Facilidades de seguridad usando un PIN o un interruptor localizado sobre el dispositivo Wi-Fi.
WiMAX	*Worldwide Interoperability for Microwave Access*, Interoperabilidad Mundial para Acceso por Microondas. Estándar del IEEE (802.16) de acceso a radio de última generación orientada a última milla que permite la transmisión inalámbrica de datos. Proporciona accesos concurrentes en áreas de hasta 48 km de radio y a velocidades de hasta 70 Mbps, utilizando tecnología que no requiere visión directa con las estaciones base. WiMax es un concepto parecido a Wi-Fi pero con mayor cobertura (MAN) y ancho de banda. Existen distintas versiones para fijo (IEEE 802.16d) y móvil (IEEE 802.16e).
WISP	*Wireless Internet Service Provider,* Proveedor de Servicio de Internet Inalámbrico.
WLAN	*Wireless Local Area Network,* Red de Área Local Inalámbrica.
WMM	Ver Wi-Fi Multimedia.
WPA	*Wi-Fi Protected Access*, Acceso Protegido Wi-Fi. Protocolo de Seguridad que busca subsanar los problemas de WEP, mejorando el cifrado de los datos y ofreciendo un mecanismo de autenticación.
WPA2	WPA Versión 2. Basada en el estándar 802.11i (802.1x, TKIP y AES).
WPAN	*Wireless Personal Area Network*, Red de Área Personal Inalámbrica.
WPS	Ver Wi-Fi *Protected Setup.*
Zig Bee	Como se conoce al estándar IEEE 802.15.4.

BIBLIOGRAFÍA

- Matthew S. Gast, 802.11 *Wireless Networks The Definitive Guide,* O'Reilly Media Inc., 2005.
- Stewart S. Miller, *Wi-Fi Security*, McGraw Hill, 2003.
- Juan Manuel Madrid Molina, Seguridad en redes inalámbricas 802.11, Universidad ICESI, 2004.
- Luís Carlos Fernández González, Las Tecnologías Wi-Fi: Aplicaciones, Modelos de Negocio y Tendencias, CEDITEC, 2003.
- *Cisco Certified Network Associate* (CCNA), Asociado de Red Cisco Certificado, 2004/2005.
- Intersil, *Application Note* AN9850.1, **www.eetasia.com/articles/2001may/2001may25_ntek_dsp_an.pdf** Mayo 2000.
- **www.cnc.gov.ar**
- **www.ieee.org**
- **www.wi-fi.org**
- **www.wikipedia.org**