

# Introducción a las Redes Inalámbricas 802.11

Javier Cañas R. <jcanas@inf.utfsm.cl>

13 de marzo de 2003

## 1. Visión general

### 1.1. Arquitectura

802.11 es un estándar que forma parte de la familia IEEE 802, que consiste en un conjunto de especificaciones para tecnologías de redes LAN. La Figura 1 muestra los distintos componentes y su relación con el modelo OSI.

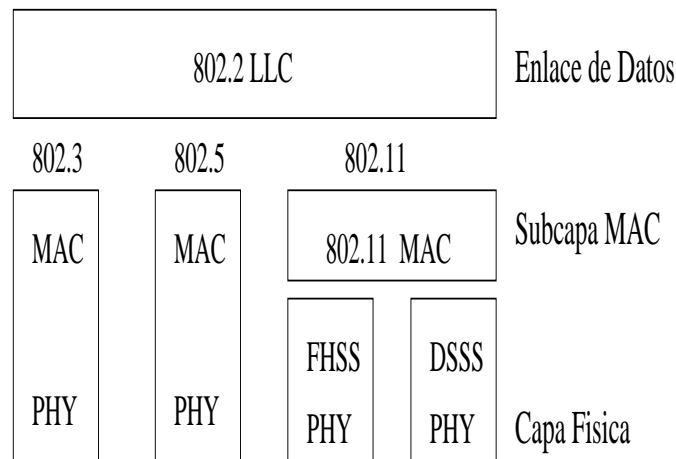


Figura 1: Arquitectura 802.11

La subcapa MAC contiene el conjunto de reglas que determinan la forma de acceder el medio y enviar datos. La subcapa PHY se ocupa de los detalles de transmisión y recepción.

En la base de la especificación 802.11 se encuentran dos capas físicas:

**FHSS** Frequency–Hopping Spread–Spectrum.

**DSSS** Direct–Sequence Spread–Spectrum.

El uso de ondas de radio en la capa física requiere una relativamente compleja capa PHY, 802.11 separa la capa física en 2 componentes genéricas:

**PLCP** Physical Layer Convergence Procedure, que mapea los frames MAC sobre el medio.

**PMD** Physical Medium Dependent, que permite la transmisión de los frames.

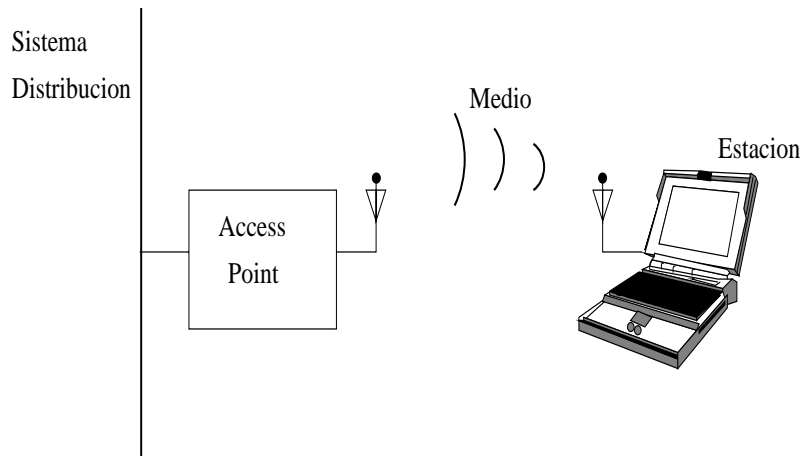


Figura 2: Componentes LAN 802.11

## 1.2. Estructura Física de una red 802.11

**Componentes** Una red 802.11 está formada por cuatro componentes principales: el sistema de distribución, el access point, el medio físico y las estaciones. La Figura 2 muestra la relación entre estos componentes.

**Tipos de red** El bloque constructivo básico de una red 802.11 es el llamado *conjunto básico de servicios* (BSS) que consiste en un grupo de estaciones que se comunican unas con otras. La comunicación tiene lugar dentro de un área, de límites difusos, llamada área básica de servicio. Si una estación está en dentro de una área básica de servicios, puede comunicarse con otros miembros del BSS.

El conjunto básico de servicios puede ser de dos tipos: ad-hoc o redes independientes y redes de infraestructura.

**Redes independientes** Se utilizan para propósitos específicos, un tarreo, una reunión, etc. . . . Como se aprecia en la Figura 3 no hay access point.

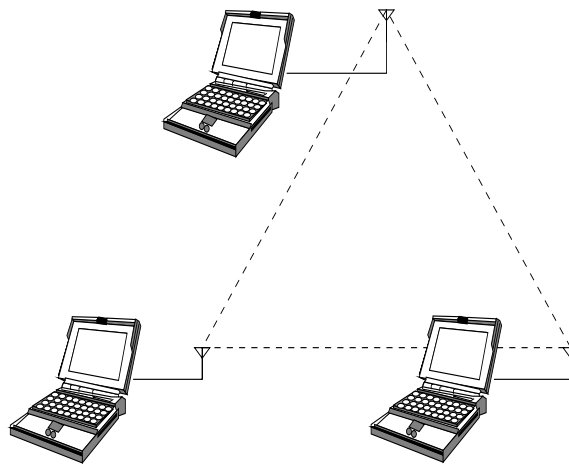


Figura 3: Redes independientes

**Redes de infraestructura** Se distinguen por la utilización de Access Point.

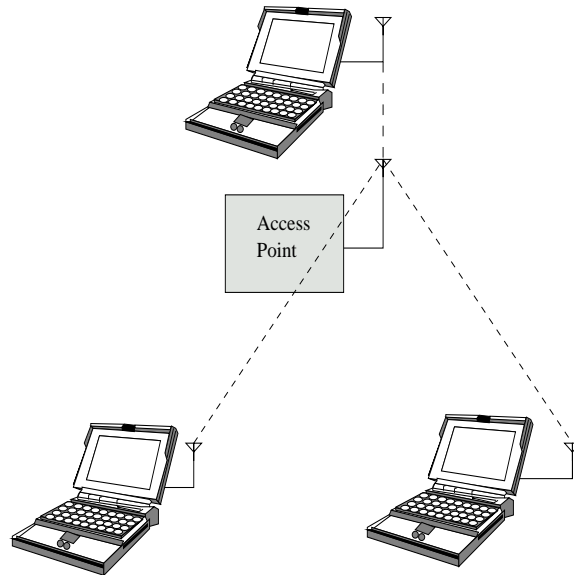


Figura 4: Redes de infraestructura

La comunicación entre dos estaciones dentro de una misma área de servicio necesita 2 saltos, lo cual resta capacidad, pero proporciona dos grandes ventajas:

1. El BSS se define por la distancia del Access Point, pero no hay restricciones respecto a distancia entre estaciones.
2. Los Access Point están en condiciones de asistir a las estaciones cuando tratan de ahorrar energía, utilizando su capacidad de buffers. Estaciones que utilizan baterías pueden apagar el transceiver y encenderlo sólo para transmitir y recuperar frames del buffer del Access Point.

En una red de infraestructura, las estaciones deben **asociarse** con un AP para obtener servicios de red (ver Figura 4). La asociación es un proceso en el cual la estación móvil queda ligada a la red 802.11 (equivale a enchufar un PC a un HUB 802.3)

### 1.3. Áreas de Servicio Extendidas

El BSS puede cubrir sólo áreas limitadas. 802.11 permite extender el área de cobertura enlazando BSS dentro de un **conjunto extendido de servicios (ESS)**.

La Figura 5 muestra la unión de 4 BSS.

Dentro de una misma ESS, las estaciones pueden comunicarse unas con otras, aún cuando estén en diferentes áreas. Los Access Point actúan como bridges, de forma tal que la comunicación directa entre estaciones necesitan que el backbone sea también una conexión de capa 2.

*Muchos access points en un área simple pueden conectarse a un mismo hub o switch.*

Las áreas de servicio extendido son el nivel abstracto más alto soportado por 802.11.

Los puntos de acceso en un ESS operan en forma concertada para permitir que el mundo exterior utilice una dirección MAC simple para despachar frames a una estación móvil, en cuyo caso, el access point con el cual la estación móvil está asociada despacha el frame. El router ignora la ubicación de la estación móvil y delega el despacho en el access point.

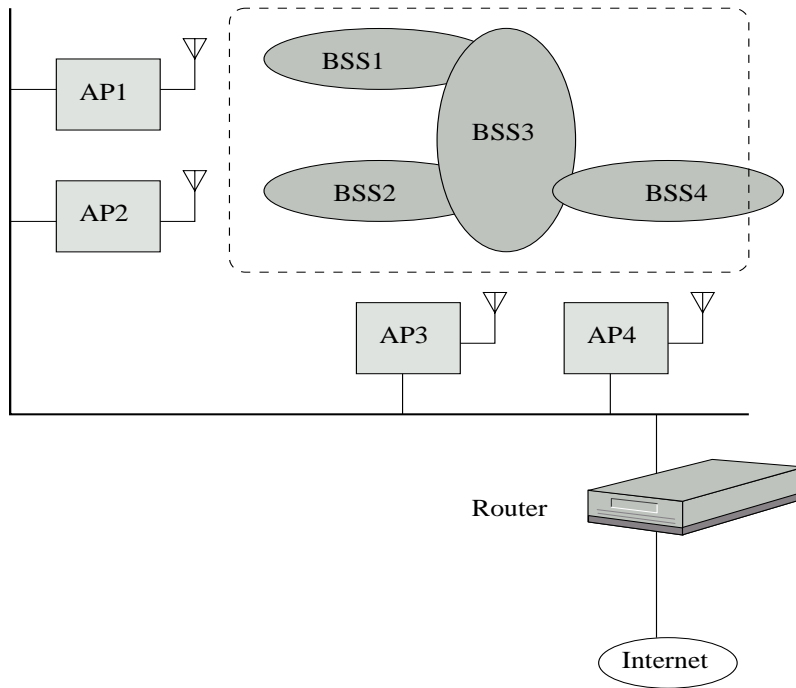


Figura 5: Conjunto de servicio extendido ESS

#### 1.4. Sistema de Distribución

802.11 describe el sistema de distribución en términos de los servicios que ofrece a las estaciones móviles.

El sistema de distribución es responsable de actualizar la ubicación física de las estaciones y despachar correctamente. El backbone Ethernet es el medio del sistema de distribución, la otra parte reside en los puntos de acceso. La mayoría de los AP actúan como bridges y en el núcleo de su software contienen un “motor de bridge” tal como se muestra en la Figura 6

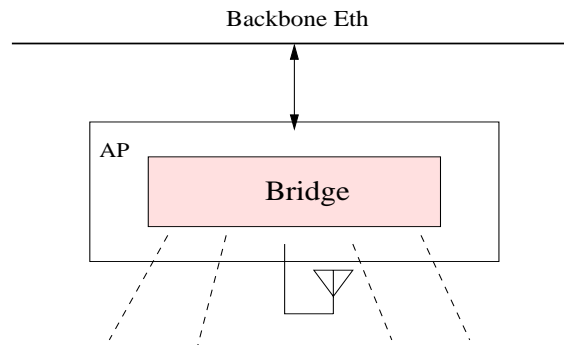


Figura 6: Sistema de distribución en Punto de Acceso 802.11

Las estaciones en una red de infraestructura depende del sistema de distribución para comunicarse unas con otras.

**Asociaciones** Una estación se asocia sólo con un AP por vez. Esto significa que en un ESS, todos los access point necesitan aprender las asociaciones de todas las estaciones.

En la Figura 5, AP4 conoce todas las estaciones asociadas con AP1. Es el bridge dentro del access point quien determina el correcto despacho del frame.

Existe un protocolo propietario llamado inter-access point protocol (IAPP) disponible en el mercado.

## 1.5. Soporte para movilidad

Las estaciones se pueden mover mientras están conectadas a la red inalámbrica. La movilidad puede generar 3 tipos de transiciones:

**Sin transición** La estación permanece dentro de su área de servicio determinada por su AP.

**Transición BSS** Las estaciones monitorean la potencia y calidad de las señales. Dentro de un área de servicio extendida, las estaciones asociadas al sistema de distribución pueden enviar frames direccionados a una MAC address de una estación móvil y dejar que el AP maneje el salto final a la estación móvil. Una estación no necesita saber la ubicación de las demás estaciones.

La Figura 7 muestra una transición BSS.

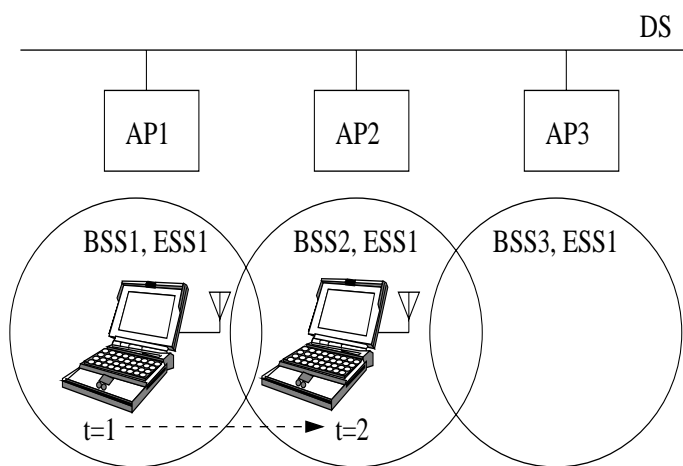


Figura 7: Transición BSS

**Transición ESS** 802.11 no soporta la transición de una estación de un ESS a otro, excepto para permitir a una estación asociarse con un AP en el segundo ESS al abandonar el primero.

## 2. La Subcapa MAC

### 2.1. Introducción

Al igual que Ethernet, 802.11 usa CSMA para control de acceso al medio de transmisión. Debido a la pérdida de capacidad que originan las colisiones, en vez de utilizar detección de colisiones (CSMA/CD), 802.11 utiliza un esquema que evita colisiones, llamado CSMA/CA, utilizando un esquema de control de acceso distribuido.

### 2.2. Restricciones para el diseño del MAC

La transmisión inalámbrica, y sobre todo, en bandas de frecuencia sin licencia (banda ISM), es altamente susceptible al ruido e interferencias.

Debido a estas restricciones, 802.11 incorpora un ACK para todo frame transmitido.

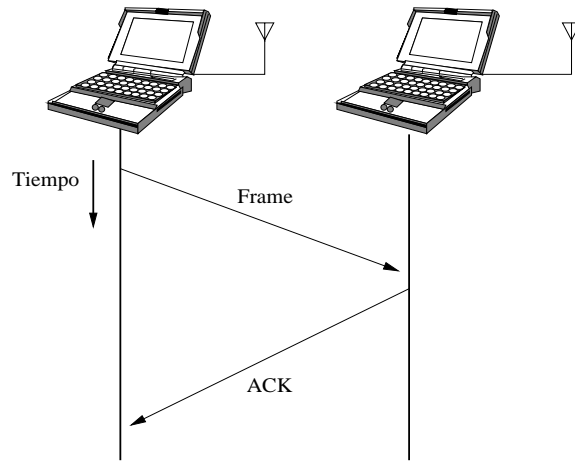


Figura 8: Reconocimiento positivo

La secuencia mostrada en la Figura 8 se denomina operación atómica. Las estaciones que participen de una operación atómica no permiten interrupción por otras estaciones que traten de utilizar el medio.

### 2.3. El problema del nodo oculto

En una red Eth, las estaciones utilizan la recepción de los frames transmitidos para implementar la función CSMA/CD.

A diferencia de Eth, las redes wireless tienen fronteras difusas donde pueden existir nodos que no se pueden comunicar con otros.

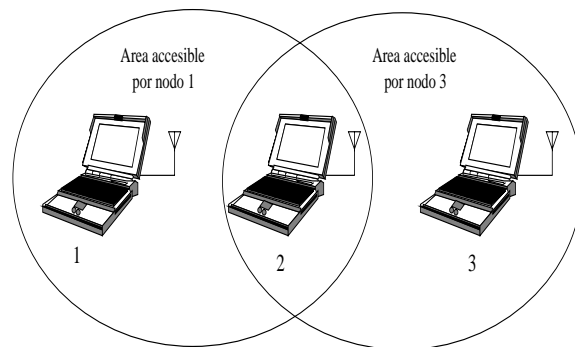


Figura 9: Los Nodos 1 y 3 están mutuamente ocultos

En la Figura 9, el nodo 2 se puede comunicar con el nodo 1 y 3, pero los nodos 1 y 3 no pueden hacerlo directamente.

Desde la perspectiva del nodo 1, el nodo 3 está "oculto" y por lo tanto es posible que ambos transmitan simultáneamente, en cuyo caso el nodo 2 no entiende nada. Aún más, la colisión es local al nodo 2.

La colisión que provocan los nodos ocultos son difíciles de detectar en redes inalámbricas debido a que los transeivers son HDX.

Para prevenir colisiones despejando un área, se utilizan señales RTS y CTS.

RTS permite reservar un enlace de radio para transmisión y también silenciar la estación que lo escucha. La estación receptora al recibir RTS, responde con un CTS. Al igual que un RTS, el frame

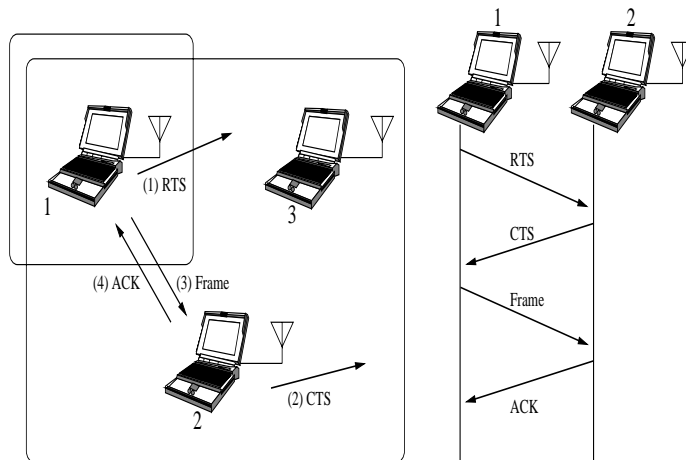


Figura 10: Despeje RTS/CTS

CTS silencia las estaciones en la vecindad inmediata. En la Figura 10 se muestra la interacción de los distintos frames.

Una vez que se ha completado el intercambio RTS/CTS, el nodo 1 puede transmitir sin preocuparse de la interferencia desde nodos ocultos.

Los nodos ocultos que están fuera del rango de la estación que transmite, son silenciados por el CTS que genera el receptor.

El intercambio RTS/CTS consume una parte de la capacidad del canal, por esta razón se usa sólo en ambientes que tienen una contención significativa en la transmisión.

El procedimiento RTS/CTS se puede configurar a través de la variable llamada *RTS threshold* (si el driver lo permite). En este caso el intercambio RTS/CTS sólo se realiza para frames cuyo largo supera el umbral *RTS threshold*. Si los frames son cortos, se envían sin intercambio de RTS/CTS.

## 2.4. Modos de Acceso y Diagramas de Tiempo

El acceso al medio inalámbrico es controlado por funciones de coordinación. La función llamada Función de Coordinación Distribuida (DCF), provee un acceso al medio similar a Ethernet. DCF es la base del estándar CSMA/CA, y al igual que Ethernet, antes de transmitir verifica que el medio esté silencioso. Para evitar colisiones, DCF utiliza backoff aleatorio después de cada frame. También en algunas circunstancias, DCF puede utilizar CTS/RTS para reducir aún más la probabilidad de colisión.

## 2.5. Detección de portadora

Para determinar la disponibilidad del medio, se utilizan dos tipos de detección de portadora: detección física y detección virtual. En ambos casos, si el medio está ocupado, el MAC lo reporta a las capas superiores.

La detección física es provista por la capa física (PHL) y depende del medio y del tipo de modulación. En general este hardware es caro, ya que por su naturaleza, los tranceptores de RF son HDX. Aún más, debido al problema de los nodos ocultos, la función de detección de portadora en forma física no puede entregar la información completa.

La detección virtual es provista por el NAV (Network Allocation Vector). El NAV es un campo del frame y representa un timer que indica un tiempo reserva. Cuando el NAV llega a cero, el medio está disponible.

El NAV asegura que las operaciones atómicas no serán interrumpidas. Por ejemplo, la secuencia RTS/CTS de la Figura 10 es atómica.

La Figura 11 muestra la acción del NAV para garantizar la atomicidad de los intercambios de frames. Se aprecia que cuando la barra NAV está presente, las estaciones, deben diferir el acceso al medio.

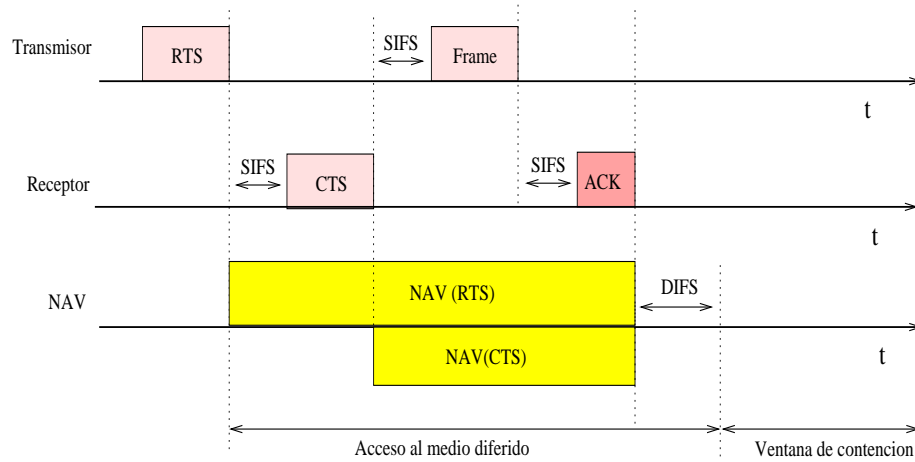


Figura 11: Uso de NAV para detección virtual de portadora

Observar que como no todas las estaciones escuchan RTS, el CTS incluye NAV más corto que previene que otras estaciones accesen el medio antes que la transmisión se complete.

Al terminar el tiempo DIFS, el medio puede ser usado por cualquier estación.

## 2.6. Espaciamento Interframe

El espaciamento interframe juega un rol clave en la coordinación del acceso al medio de transmisión.

La figura 12 muestra la relación entre estos distintos tiempos.

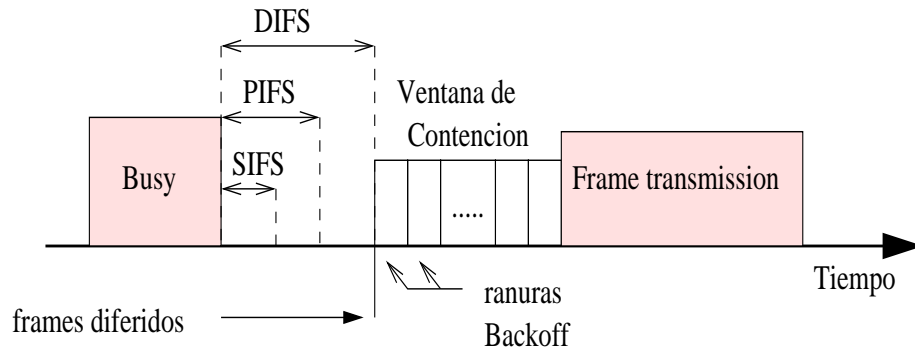


Figura 12: Espaciamento interframe

Para que las distintas estaciones puedan interoperar, independientemente de las velocidades de transmisión, estos tiempos son fijos.

**Short interframe space (SIFS)** Se usa para transmisiones de alta prioridad como RTS/CTS y ACK.

**DCF interframe space (DIFS)** Es el tiempo mínimo que el medio debe estar desocupado. Pasado este tiempo, las estaciones pueden ocupar el medio.

Operaciones atómicas comienzan igual que transmisiones regulares, o sea, deben esperar que concluyan el DIFS antes de comenzar. Sin embargo, los demás pasos de una operación atómica utilizan el SIFS. Con esto se logra que las estaciones puedan retener el medio sin ser interrumpidas.

En resumen, usando SIFS y NAV las estaciones pueden apropiarse del medio por el tiempo que estimen necesario.

## 2.7. Acceso basado en contención

La mayor parte del tráfico 802.11 utiliza la función DCF que proporciona un servicio de acceso al medio basado en contención que permite a las estaciones interactuar sin necesidad de un control central y por lo tanto puede ser utilizado ya sea por redes IBSS o por redes de infraestructura.

El algoritmo de acceso es el siguiente:

- Antes de intentar transmitir, cada estación verifica si el medio está desocupado. Si está ocupado utiliza el algoritmo de backoff exponencial para evitar colisiones.
- Si el medio está desocupado por un tiempo mayor que DIFS, la transmisión puede comenzar inmediatamente. La detección de portadora se puede hacer en forma física o virtual.
  - Si el frame anterior fue recibido sin errores, el medio estará libre por al menos el DIFS.
  - Si la transmisión previa contiene errores, el medio estará libre por un tiempo EIFS.
- Si el medio está ocupado, la estación debe esperar que el canal se desocupe. Esta espera se denomina **acceso diferido**. Si el acceso es diferido, la estación espera que el canal se desocupe el tiempo DIFS y se prepara para el procedimiento de backoff exponencial.

Reglas adicionales se aplican en determinadas circunstancias:

1. La recuperación de errores es responsabilidad de la estación que envía el frame. El ACK es la única indicación de éxito en la transmisión. Si no llega ACK, la fuente de la información retransmite el frame.
  2. Todo frame unicast debe ser reconocido por ACK.
  3. Cualquier falla incrementa un contador llamado contador de reintento y la transmisión se repite. Una falla puede deberse en una falla para obtener acceso al medio o una pérdida de ACK.
- Secuencias multiframe, pueden actualizar el NAV en cada paso del procedimiento de transmisión.
  - Los siguientes frames pueden ser transmitidas después de un SIFS, y por lo tanto con máxima prioridad: CTS y fragmentos en una secuencia de fragmentos.
  - Secuencias extendidas de frames se requieren por paquetes de capas de alto nivel más largas que los umbrales de configuración.
    - Paquetes más largos que el umbral RTS deben tener un intercambio RTS/CTS.
    - Paquetes más largos que el umbral de fragmentación se deben fragmentar.

## 2.8. Recuperación de errores con DCF

La estación que inicia un intercambio atómico de frames es responsable de la detección y corrección de errores en los frames. En se puede inferir pérdidas de frames por falta de ACK. Cada vez que se retransmite un frame se incrementa el contador de reintentos.

Cada frame o fragmentos de frame tiene asociado un contador de reintento. Una estación maneja dos tipos de contadores de reintento: el contador corto, y el contador largo.

Los frames cuyo largo es menor que el umbral RTS se consideran cortos.

El contador corto vuelve a cero cuando:

- Se recibe un CTS en respuesta de un RTS.
- Se recibe un ACK después de una transmisión sin fragmentos.
- Se recibe un frame broadcast o multicast.

El contador largo vuelve a cero cuando:

- Se recibe un ACK para un frame más largo que el umbral RTS.
- Se recibe un frame broadcast o multicast.

Además del contador de reintento, los fragmentos tienen asociado un “tiempo de vida” por el MAC. Al iniciar la transmisión del primer fragmento, comienza a correr el tiempo de vida. Al expirar, el frame se descarta y no se hace un nuevo intento de retransmitir los fragmentos restantes.

## 2.9. Backoff en DCF

Después que la transmisión de un frame se completa y ha transcurrido el DIFS, las estaciones pueden intentar transmitir datos. El tiempo que sigue después del DIFS se denomina *ventana de contención*.

La *ventana de contención* se divide en ranuras. El largo de un ranura es dependiente de la velocidad de transmisión. La estación selecciona al azar una ranura y la espera antes de intentar acceso al medio. Al existir competencia entre varias estaciones, gana la que tiene el número menor.

Al igual que Ethernet, el tiempo de backoff se selecciona de un rango, cada vez mayor, toda vez que la transmisión falla. Cada vez que el contador de reintento se incrementa, la ventana de contención se mueve a la siguiente potencia de dos mayor. La figura 13 muestra los tamaños de la ventana de contención cuando la capa física es DSSS.

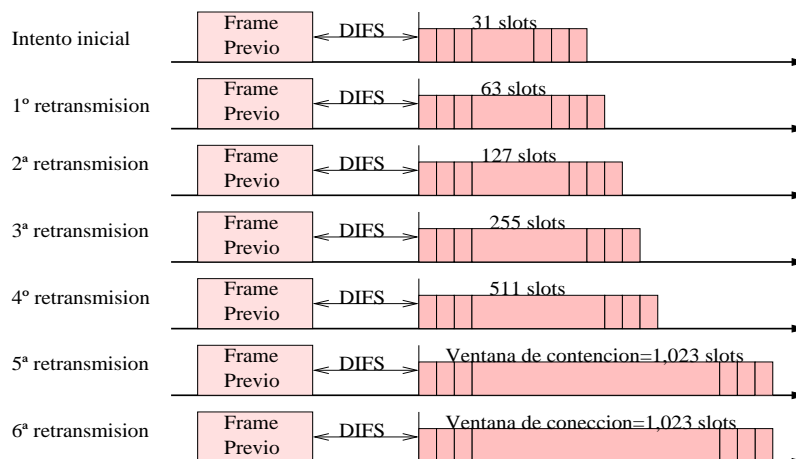


Figura 13: Ventana de contención DSSS

Al llegar la ventana a su máximo tamaño, permanece hasta que vuelve a cero. El permitir tamaños grandes de ventanas de contención cuando hay muchas estaciones compitiendo, hacen que los algoritmos MAC sean estables aún a máxima carga.

La ventana de contención vuelve a su tamaño mínimo cuando los frames se transmiten exitosamente o cuando el contador de reintento llega a su máximo y se descarta la transmisión del frame.

## 2.10. Fragmentación y reensamblado

Paquetes provenientes de protocolos de alto nivel necesitan fragmentarse para entrar a los canales inalámbricos. Adicionalmente la fragmentación ayuda a mejorar la confiabilidad en presencia de interferencias de radiofrecuencia.

Un paquete de alto nivel se fragmenta cuando su tamaño excede el umbral de fragmentación configurado por el administrador de la red. Todos los fragmentos comparten el mismo número de secuencia de frame y adicionalmente cada fragmento se numera en forma ascendente para permitir su reensamblado. La figura 14 muestra la transmisión de una descomposición en 3 fragmentos.

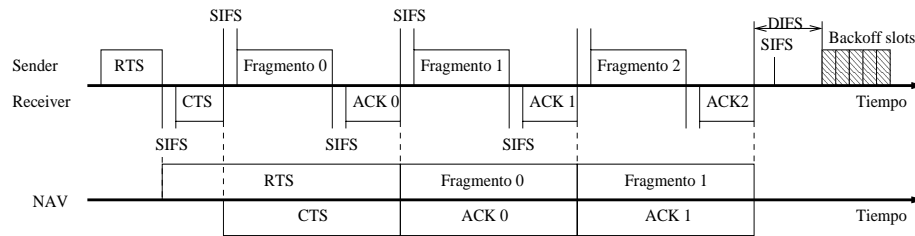


Figura 14: Ciclo de fragmentación

Se observa la incorporación de RTS/CTS porque es común que el umbral de fragmentación tenga el mismo valor de *umbral RTS/CTS*. En la figura 14 se observan también los NAV.

## 2.11. Formato de Frame

Un enlace de datos inalámbricos impone condiciones de borde diferentes a la capa MAC Ethernet. Una de estas diferencias son 4 campos de dirección, cuya interpretación y uso depende del tipo de frame MAC que se transmitirá.

La figura 15 muestra el frame MAC genérico. Cada campo es transmitido de izquierda a derecha, y el bit más significativo de cada campo aparece al final.

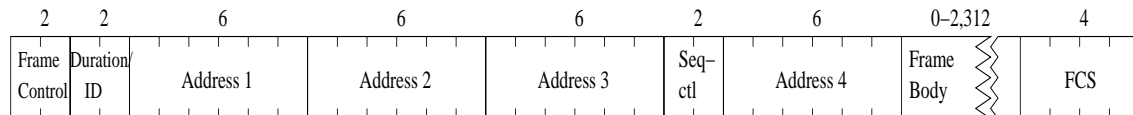


Figura 15: Frame MAC genérico 802.11

Se puede apreciar algunas diferencias con el MAC Ethernet: el preámbulo es parte de la capa física, y el campo tipo/largo está contenido en el encabezamiento de los datos del frame 802.11.

Breve descripción de campos:

**Frame Control** El frame comienza con dos bytes que se subdividen en los siguientes subcampos:

**Versión de Protocolo**

**Tipos y Subtipos** Identifica funciones que se incorporan a 802.11 como RTS, CTS, ACK, Frame de Datos, etc.

**ToDS y FromDS** Estos bits indican cuando un frame está destinado a un sistema de distribución.

	ToDS=0	ToDS=1
From DS=0	Frame de administración y control Frames de datos redes ad-hoc	Frame de datos transmitido desde una estación inalámbrica en una red de infraestructura
From DS=1	Frame de dato recibido desde una estación inalámbrica en una red de infraestructura	Frame de Datos en un bridge inalámbrico

**Más fragmentos** Similar al bit de IP.

**Retry** El bit es 1 si es un frame retransmitido.

**Manejo de Fuente de Poder**

**More data** Para estaciones que entran en un modo de ahorro de batería.

**WEP** Si el frame ha sido procesado por WEP.

**Orden bit** Cuando se requiere preservar el orden de transmisión en forma estricta.

**Duration/IP** Este campo tiene diferentes usos y dependiendo de una combinación de bits toma 3 formas diferentes:

**Duración** Se establece el NAV. El valor numérico representa el número de microsegundos que el medio debe estar ocupado. El bit 15 está en cero.

**Periodo libre de contención** Bit 14 en cero y bit 15 en uno. Todos los demás bits están en cero, lo cual significa un valor de 32768 interpretado como NAV.

**PS-Poll** Usado para ahorro de batería.

**Dirección** Los 4 campos de dirección se rotulan como Address 1, Address 2, . . . , Address 4. La regla es que Address 1 se usa para el receptor, Address 2 para el transmisor, Address 3 para filtrado por parte del receptor.

Se sigue la misma regla que en Ethernet para direcciones MAC. Tipos de dirección:

**Destino** Receptor final, es decir la estación que pasará el frame a las capas superiores.

**Fuente** Identifica la fuente de transmisión.

**Receptor** Indica cual estación inalámbrica debe procesar el frame. Si es una estación inalámbrica, la dirección receptor es la dirección destino. En el caso de frames destinados a un nodo de una red Ethernet conectada a un Access Point, la dirección receptor es la interfaz inalámbrica en el Access Point y la dirección destino puede ser un router conectado a la red.

**Transmisor** Identifica la interfaz inalámbrica que transmite el frame sobre el medio inalámbrico. Sólo usa en bridges inalámbricos.

**Basic Service Set ID** Para identificar diferentes redes inalámbricas en la misma área, las estaciones pueden ser asignadas a un BSS. En redes de infraestructura, el BSSID es la dirección MAC usada por la interfaz inalámbrica en el Access Point. Redes “ad hoc” generan un BSSID aleatorio.

La tabla muestra los campos de dirección de un frame de datos en distintas situaciones:

<i>Función</i>	<i>ToDS</i>	<i>FromDS</i>	<i>Add1</i>	<i>Add2</i>	<i>Add3</i>	<i>Add4</i>
IBSS	0	0	destino	fuelle	BSSid	–
A un AP	1	0	BSSid	fuelle	destino	–
Desde un AP	0	1	destino	BSSid	fuelle	–
En bridge	1	1	receptor	transmisor	destino	fuelle

El número de campos de dirección utilizados dependen del tipo de frame. La mayoría de los frames de datos utilizan 3: Fuente, destino y BSSID. Como la mayoría de las transmisiones utiliza 3 direcciones, esta es la razón por la cual aparecen en forma contigua.

**Control de Secuencia** Este campo de 16 bytes se utiliza para reensamblar y descartar duplicados. Se descompone de 4 bytes que indica el número de fragmento y un campo de 12 bytes para número de secuencia.

Las capas superiores asignan números de secuencia a los frames cuando son pasados al MAC para transmisión. Estos números de secuencia se generan con un contador módulo-4096 comenzando desde cero e incrementando en uno por cada frame pasado al MAC. Si es necesario fragmentar, todos los fragmentos conservan el mismo número de secuencia.

**Carga útil** El largo máximo de la carga útil es de 2312 bytes.

**Frame Check Sequence** Corresponde al código de integridad CRC. Este código se calcula sobre todos los campos de header y de la carga útil.

### 3. La Capa Física

La capa física de la arquitectura 802.11, se abrevia PHY.

#### 3.1. Arquitectura de la Capa Física

La capa física se divide en dos subcapas: Procedimiento de convergencia de la capa física (PLCP) y la subcapa dependiente del medio (PMD):

La figura 16 muestra la arquitectura lógica y permite apreciar que la subcapa PLCP actúa como un verdadero “pegamento” entre los frames del MAC y la radio transmisión en el éter. Esta subcapa añade sus propios encabezamientos al frame y en particular los preámbulos de sincronización. La subcapa PMD es responsable de transmitir cualquier bit que recibe desde PLCP al éter usando la antena. La capa física también incorpora una función llamada CCA (Clear Channel Assessment) que permite indicar al MAC cuando se detecta una señal.

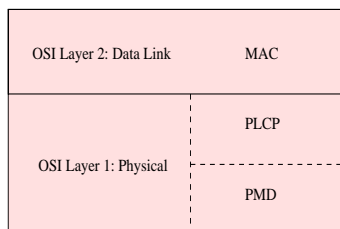


Figura 16: Arquitectura de la capa Física

### 3.2. Enlaces de radiofrecuencia

El estándar 802.11 establece 3 capas físicas:

- Frequency-hopping spread-spectrum FH PHY
- Direct-Sequence spread-spectrum DS PHY
- Luz infrarroja IP PHY

En 1999 se agregaron 2 nuevas capas:

**802.11a** Orthogonal Frequency Division Multiplexing: OFDM PHY

**802.11b** High-Rate Direct Sequence: HR/DSSS PHY

El espectro de radio frecuencia está asignado en bandas dedicadas a propósitos particulares. Existen bandas de frecuencia que han sido reservadas para usos que no requieren licencias, por ejemplo los hornos de micro-hondas operan a 2.45GHz. En los Estados Unidos, la Federal Communications Commission (FCC) es responsable de las regulaciones en el uso del espectro de radiofrecuencia. (En Chile es la Subtel). Tanto en los Estados Unidos como otros países, los organismos reguladores designan ciertas bandas para uso “industrial, científico y médico” y se denominan bandas ISM. Por esta razón los componentes 802.11 no requieren licencias. Cada tarjeta vendida en el mercado norteamericano contiene un número de identificación FCC que permite obtener toda la información disponible en forma abierta y pública.

### 3.3. Spread Spectrum

La tecnología Spread Spectrum es utilizada en las bandas ISM para transmisión de datos.

Tradicionalmente las comunicaciones de radiofrecuencia buscan inyectar la máxima cantidad de energía de señal en bandas de frecuencia lo más angostas posibles.

La técnica de Spread Spectrum utiliza una función matemática para diseminar la potencia de señal sobre un amplio rango de frecuencias. Esta técnica permite atenuar el efecto del ruido sobre los datos transmitidos.

Para limitar las interferencias entre dispositivos en la banda ISM, los organismos reguladores establecen limitaciones sobre la potencia en las transmisiones. El límite legal es de un watt de potencia en la salida del transmisor y cuatro watts de potencia efectiva irradiada (ERP). Cuatro watts de ERP equivalen a 1 watt con una antena que tiene 6db de ganancia. ( $6db = 3db + 3db = 2*2$ ).

### 3.4. Tipos de Spread Spectrum

802.11 usa tres técnicas diferentes de Spread Spectrum:

**FHSS** Salta de una frecuencia a otra usando patrones aleatorios. En cada subcanal transmite una porción de los datos.

**DSSS** Disemina la potencia de la señal sobre una banda amplia de frecuencia usando funciones matemáticas de codificación.

**OFDM** Orthogonal Frequency Division Multiplexing. Divide un canal en muchos subcanales y codifica una porción de señal en cada subcanal en paralelo.

El sistema más barato es el FHSS. DSSS requiere un sistema más sofisticado de procesamiento de señal, lo cual significa mayor costo y mayor consumo de energía.

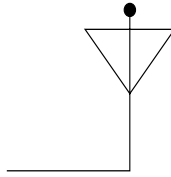


Figura 17: Representación esquemática de una antena

### 3.5. Antenas

Las antenas son un componente crítico de un sistema de RF. Convierten señales eléctricas en ondas y vice-versa. La figura 17 muestra la representación esquemática de una antena.

El tamaño de una antena depende de la frecuencia: a mayor frecuencia, menor tamaño. El tamaño mínimo a cualquier frecuencia es  $\frac{1}{2}$  de la longitud de onda (usando técnicas de ingeniería de comunicaciones, se puede reducir más).

Las antenas se diseñan considerando la direccionalidad. Una antena omnidireccional, envía y recibe señales desde cualquier dirección. Una antena direccional, irradia y recibe sobre una porción más angosta del espacio.

En redes 802.11 se usan normalmente antenas omnidireccionales en ambos extremos del enlace, aunque también es posible utilizar antenas direccionales cuando se desean cubrir distancias mayores.

Los adaptadores 802.11 incorporan antenas interiores. Utilizando dispositivos opcionales es posible tener una cobertura mayor.

### 3.6. 802.11 FH PHY

La técnica de transmisión llamada Frequency hopping consiste en un cambio rápido en la frecuencia de transmisión de una manera predeterminada y pseudo aleatoria como se muestra en la figura 18.

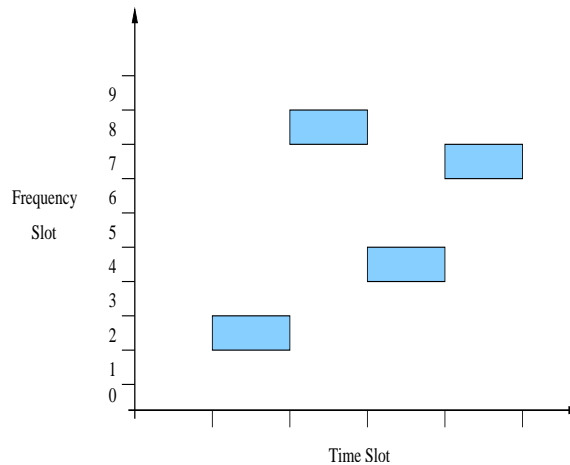


Figura 18: Frequency hopping

El patrón de saltos establece la forma como se utilizan las ranuras de tiempo. Por ejemplo, en la figura 18 la secuencia es  $\{2, 8, 4, 7\}$ . Tanto el transmisor como el receptor deben estar sincronizados, de forma tal que el receptor esté permanentemente atendiendo la frecuencia del transmisor. Como se aprecia en la figura 18, cada frecuencia es usada un pequeño tiempo denominado *dwell time*.

Si dos sistemas FH necesitan compartir la misma banda, se pueden configurar con diferentes secuencias de forma de evitar interferencias mutuas. Secuencias que no traslapan se denominan secuencias *ortogonales*.

Ahora, en el detalle, 802.11 divide la banda ISM en canales de 1 MHz, asignando el canal 0 en 2400 GHz. Diferentes regulaciones limitan el número de canales. En los Estados Unidos los canales permitidos son del 2 al 79. El dwell time es de 0.4 segundos.

### 3.7. 802.11 DS PHY

La modulación de secuencia directa (DS PHY), ha sido la técnica más exitosa de modulación usada en 802.11, sin embargo, el hardware requiere mayor potencia para lograr el mismo desempeño que FH PHY; por otro lado, se puede adaptar a tasas mayores de transmisión que redes que operan en FH PHY.

DS es una técnica spread-spectrum que permite transmitir una señal sobre una banda de frecuencia más ancha. La figura 19 muestra la técnica básica.

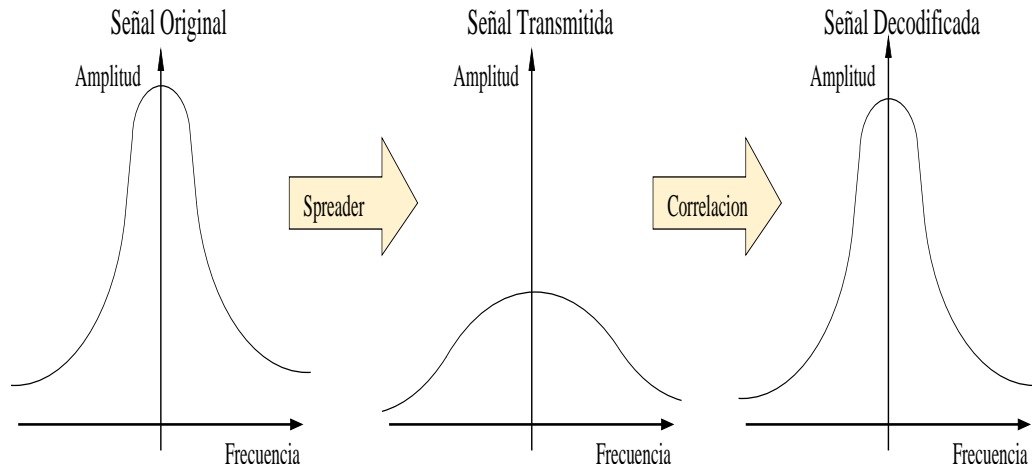


Figura 19: Técnica Básica DSSS

En la figura 19 se aprecia a la izquierda, la banda angosta de una señal. Ésta es procesada por un “spreader” que, a través de una transformación matemática, aplana la amplitud diseminándola en una banda más ancha. Frente a un receptor convencional, la señal es percibida sólo como ruido, pero el receptor DS monitorea una porción más ancha del espectro de frecuencia y le aplica una transformación de correlación la cual invierte el proceso inicial.

La correlación busca cambios de la señal de radio frecuencia que ocurren a través de la banda completa. Lo que se logra es una excelente protección frente a la interferencia, tal como se aprecia en la figura 20.

La modulación de secuencia directa se genera aplicando una secuencia llamada “chipping sequence”. Se denomina *chip* a un bit utilizado en el proceso; matemáticamente un chip es un bit y se hace la diferencia porque el chip sólo se utiliza en el proceso de codificación.

El flujo de “chips” se denomina también “códigos de ruido pseudoaleatorios” (códigos PN) y deben ser generados a tasas más altas que los datos. Un parámetro importante en el proceso de modulación es la llamada *tasa de spreading*, es decir, el número de chips que se utilizan para transmitir un bit simple. Aumentar la tasa de spreading tiene dos costos: componentes de RF más caros y el costo indirecto de un mayor ancho de banda.

Entrando en mayores detalles, 802.11 adoptó una palabra de 11 bits como código PN llamada palabra de **Barker** fundamentalmente por sus propiedades de autocorrelación.

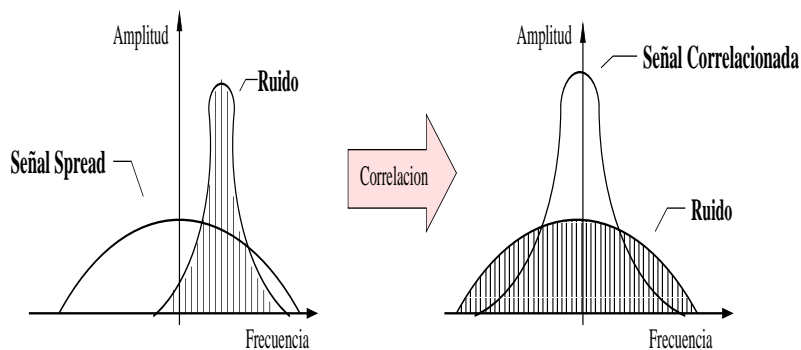


Figura 20: Técnica Básica DSSS

## 4. Administración

Las redes inalámbricas nos liberan de las rígidas restricciones de las redes de cobre, aunque por ello debemos pagar un alto precio: el medio es poco confiable, acceso más fácil por personas no autorizadas y duración limitada de baterías.

Algunos drivers 802.11 permiten una gran flexibilidad para configurar facilidades de administración. En general estas capacidades son diferentes en productos distintos.

### 4.1. Arquitectura de Administración

Los componentes de la arquitectura de administración se muestran en la figura 21.

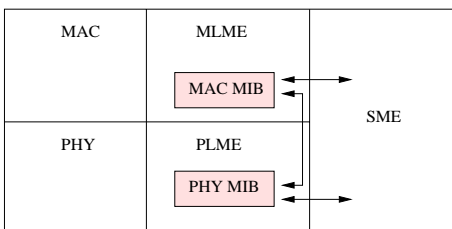


Figura 21: Arquitectura de Administración

MLME (MAC Layer Management Entity) es la entidad que administra la capa MAC, PLME administra la capa física y SME (System management entity) contiene los métodos a través de los cuales interactúan los usuarios con los drivers.

Los MIB (Management Information Base) permiten configurar, por ejemplo, a través de SNMP.

### 4.2. Scanning

Antes de utilizar una red, hay que encontrarla. En una red Ethernet, basta con encontrar un conector en la pared; en las redes inalámbricas, las estaciones deben identificar una red compatible antes de utilizarla. El proceso de identificar redes se denomina *scanning*.

En el procedimiento de scanning se utiliza un conjunto de parámetros. La mayoría de las implementaciones tienen valores asignados por defecto. Algunos de estos parámetros son:

**BSSType** Especifica si se usa redes “ad hoc”, de infraestructura o cualquiera.

**BSSID** Si se busca alguna red en particular o cualquiera (broadcast). Si el dispositivo se mueve, broadcast es la mejor opción.

**SSID** Asigna un string a un conjunto de servicios extendidos. Esta forma es más amistosa ya que utiliza nombres (strings).

**ScanType** Selecciona scan activo o pasivo. La opción pasiva ahorra baterías.

**ChannelList** Permite a las estaciones especificar una lista de canales. El significado preciso de canal depende de la capa física, si es FH, se especifica el conjunto de canales de saltos.

**ProbeDelay** Configura el retardo en microsegundos antes de comenzar la prueba en modo activo.

**MinChannelTime** y **MaxChannelTime** Configura tiempos mínimos y máximos del tiempo de scan en algún canal específico.

### 4.3. Scanning Pasivo

Ahorra batería porque no requiere transmitir. En este modo, la estación se mueve a cada canal, de la lista de canales y espera por frames tipo *Beacon*. Estos frames Beacon son almacenados en buffers donde se extrae la información del BSS que la generó.

Los frames Beacon contienen la información necesaria que necesita la estación para ajustar sus parámetros al BSS. En la figura 22 la estación móvil usa scan pasivo para encontrar un BSS en su área, escucha los frames Beacon de 3 Puntos de Acceso y reporta que sólo encontró AP 1, AP 2 y AP 3.

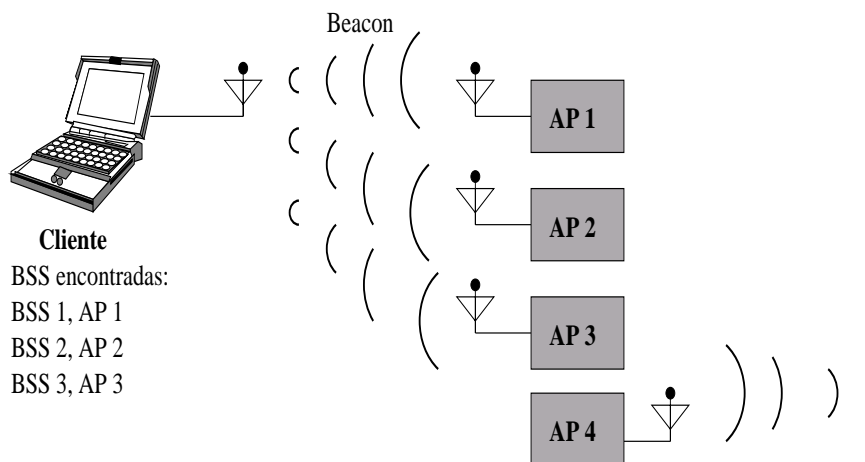


Figura 22: Scanning Pasivo

### 4.4. Scanning Activo

En esta modalidad, la estación genera frames *Probe Request* sobre cada canal para solicitar respuesta de alguna red específica.

Se usa el siguiente procedimiento:

1. Ir a un canal y esperar algún frame, o esperar timeout del timer *ProbeDelay*. Si se detecta un frame el canal está en uso y puede ser probado. El timer protege el procedimiento de una espera indefinida.
2. Obtener acceso al medio usando el procedimiento de acceso DCF (Función de Coordinación Distribuida) y enviar un frame *Probe Request*.
3. Esperar que transcurra *MinChannelTime*.

- Si el medio nunca está ocupado, no hay red. Mover al siguiente canal.
- Si el medio estaba ocupado durante el intervalo MinChannelTime, esperar hasta MaxChannelTime y procesar cualquier frame Probe Response.

En cada BSS una estación es responsable de responder los Probe Request. En redes de infraestructura el access Point transmite los Beacon y también los frames Probe Response.

La figura 23 muestra los frames y sus intervalos de tiempo.

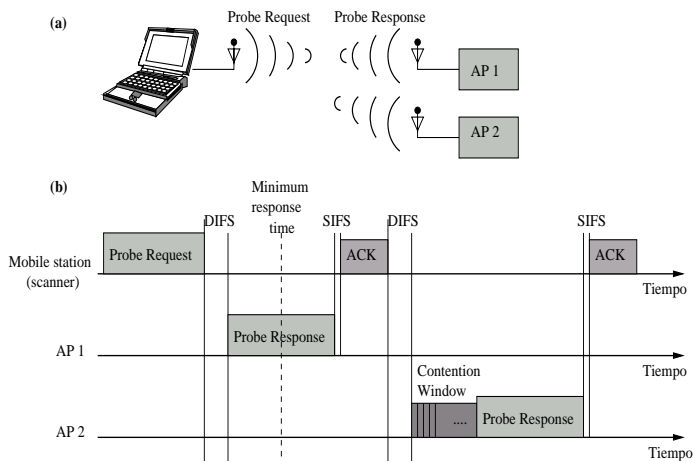


Figura 23: Procedimiento de Scanning Activo

Al finalizar el scan se genera un reporte de scan que contiene todos los BSS descubiertos, junto a sus parámetros. La estación puede elegir cualquier red descubierta.

#### 4.5. Unión (Joining)

Una vez que la estación móvil procesa el reporte de scan, puede elegir unirse a algún BSS. Esta unión, es previa a la asociación. Antes de utilizar la red se requiere de dos etapas previas: autenticación y asociación.

El criterio de elección de algún BSS es una decisión que involucra tanto la implementación como la intervención del usuario.

Dentro del procedimiento de unión, la estación debe capturar los parámetros PHY para garantizar que cualquier transmisión con el BSS se realizará sobre los canales correctos.

#### 4.6. Asociación

Una vez completa la autenticación, las estaciones pueden asociarse con un Access Point (o reasociarse con uno nuevo) para lograr un completo acceso a la red.

La asociación es un procedimiento de registro que permite al Sistema de Distribución conocer la localización de cada estación móvil, de forma tal que cada frame destinado a una estación móvil, sea despachado al access point correcto.

La asociación sólo tiene lugar en redes de infraestructura y es lógicamente equivalente a enchufar el conector en una red Ethernet.

#### 4.7. Procedimiento de Asociación

El procedimiento básico de asociación se muestra en la figura 24.

La asociación es iniciada por la estación móvil y consiste en una secuencia de 3 pasos:

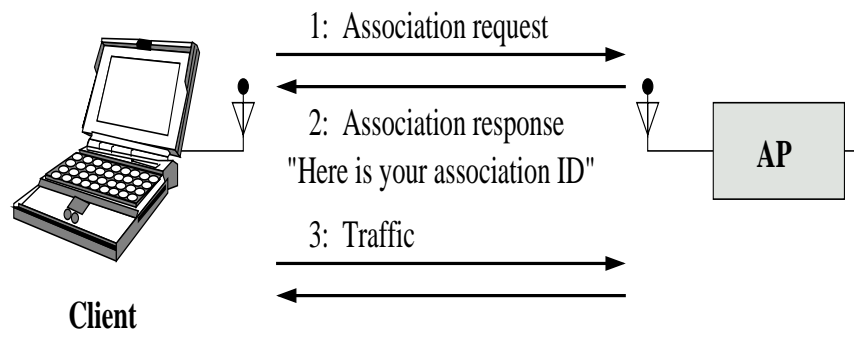


Figura 24: Procedimiento de Asociación

1. La estación emite un frame de requerimiento de asociación.
2. El access point procesa el requerimiento de asociación estableciendo una negociación, como por ejemplo, espacio en buffers.
  - Si la asociación esta OK, el access point responde con código de éxito y un identificador de asociación (AID). El AID es un identificador numérico.
  - Si la asociación no tiene éxito termina el procedimiento.
3. El access point comienza a procesar los frames de la estación móvil.

#### 4.8. Procedimiento de Reasociación

La reasociación es el proceso de mover una asociación desde un access point a uno nuevo. Cuando una estación se mueve dentro de un área de cobertura, desde un access point a otro, utiliza el procedimiento de reasociación para informar a la red 802.11 la nueva posición. Este procedimiento se ilustra en la figura 25.

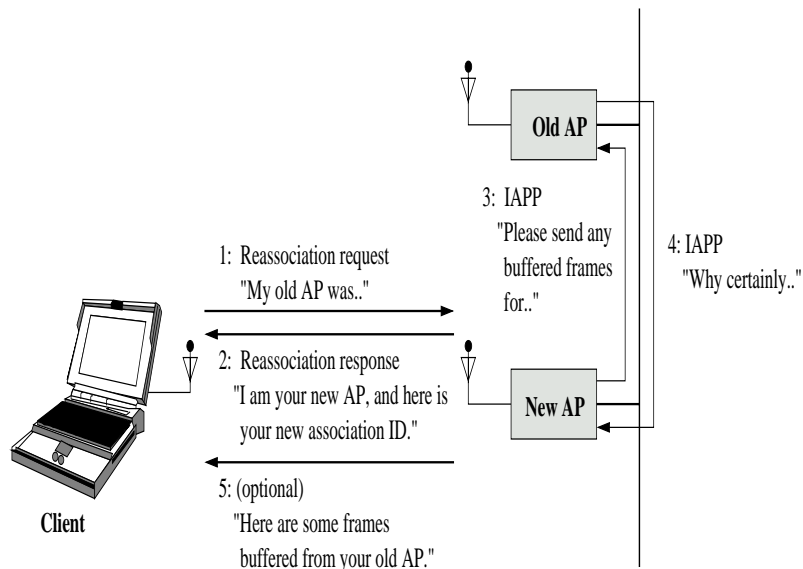


Figura 25: Procedimiento de Reasociación

La estación monitorea la calidad de la señal que recibe del access point con el cual está asociado y también desde otros access point del mismo ESS. Cuando la estación detecta una opción mejor inicia el procedimiento de reasociación que, tal como se señala en la figura 25, consta de cinco pasos:

1. La estación móvil envía una solicitud de reasociación a un nuevo access point. El frame de solicitud contiene la dirección del antiguo access point. El nuevo access point se comunica con el antiguo verificando si existe la asociación previa.
2. El nuevo access point procesa el requerimiento de una manera similar a una solicitud de asociación.
3. El nuevo access point contacta al antiguo para terminar el procedimiento de reasociación. Esta comunicación es parte del protocolo IAPP (Inter-Access Point Protocol).
4. El antiguo access point envía cualquier frame de su buffer, cuyo destino es la estación móvil, al nuevo access point.
5. El nuevo access point comienza a procesar los frames destinados a la estación móvil.

El procedimiento de reasociación también se usa para reunir una estación móvil que momentáneamente se ha alejado de la red. Esta situación se muestra en la figura 26.

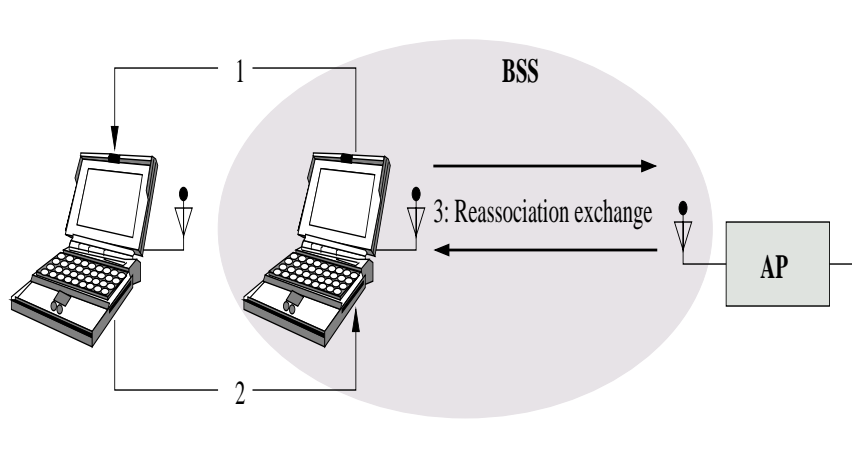


Figura 26: Reasociación con el mismo access point

## Referencias

- [1] Pablo Brenner. A technical tutorial on the ieee 802.11 protocol. [www.sss-mag.com/pdf/802\\_11tut.pdf](http://www.sss-mag.com/pdf/802_11tut.pdf).
- [2] Matthew S. Gast. *802.11 Wireless Networks*. O'Really, 2002.
- [3] Peterson L. and Davie B. *Computer Networks: A System Approach*. Morgan Kaufmann Publishers, 2000.
- [4] Jim Zyren and Petrck Al. Ieee 802.11 tutorial. [www.utdallas.edu/ir/wlans/whitepapers/80211primer.pdf](http://www.utdallas.edu/ir/wlans/whitepapers/80211primer.pdf).