IEEE 802.11b High Rate Wireless Local Area Networks

Networks as Mobile as the People Who Use Them

Preparado por:

Victor Cea M.

Sven Gysling B.

Temario

1. Introducción al protocolo 802.11
2. Descripción de la capa física.
3. Descripción de la capa MAC
4. Medidas de desempeño.
5. Administración de potencia.
6. Seguridad en 802.11b

1. Introducción

- Una WLAN (Wireless Local Area Network) es un sistema flexible de comunicaciones de datos que reemplaza o extiende a una LAN cableada.
- Usando RF, las WLAN transmiten y reciben datos por el aire a través de paredes, techos e incluso estructuras de cemento.
- Poseen todas las cualidades que ofrecen las LAN convencionales (Ethernet, Token Ring).

Introducción

- La importancia de esta tecnología va más allá de la ausencia de cables.
- Da lugar a una nueva definición de qué es una infraestructura de red, la cual ya no tiene que ser sólida y fija, sino que puede cambiar según los requerimientos de la empresa.

Introducción

- ¿Cómo pueden múltiples usuarios operar al mismo tiempo sin confundir los mensajes?
- Igual que las radio emisoras. Las portadoras se transmiten en frecuencias distintas.
- La mayoría de las WLANs usan la banda de 2.4 GHz debido a que casi todos los países ha reservado esta banda (ISM) para ser usada por dispositivos no licenciados.

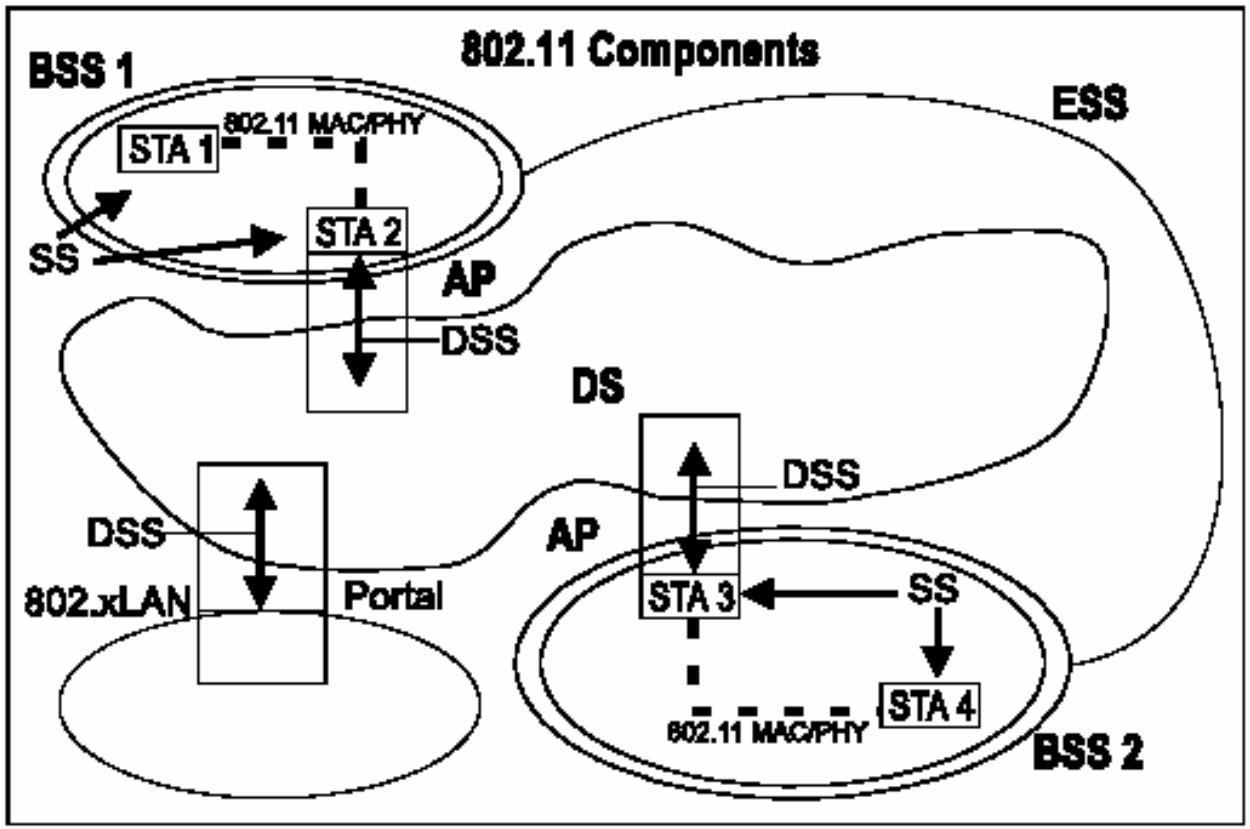
El Medio Impacta al Diseño

- La PHY usada en 802.11 difiere fundamentalmente del medio cableado en:
  - Desprotegida de señales exteriores.
  - Comunicación sobre un medio significativamente menos confiable.
  - Tiene propiedades de propagación variantes en el tiempo y asimétricas.
  - Carencia de conectividad completa.

Componentes de la arquitectura

- **Basic Service Set (BSS):** Pieza básica de una WLAN formada por STAs.
- **Distribution System (DS):** Sistema usado para interconectar BSSs.
- **Access Point (AP):** STA que provee acceso al DS.
- **Portal:** Componente lógico usado para integrar arquitecturas IEEE 802.11 y LANs tradicionales.

Componentes de la arquitectura



Complete IEEE 802.11 architecture

Configuración

- Una WLAN se puede configurar en dos modos:
  - *Peer to peer (ad hoc mode, IBSS), tipo más básico de WLAN.*
  - *Client/Server (infraestructure networking)*

Configuración Ad-hoc

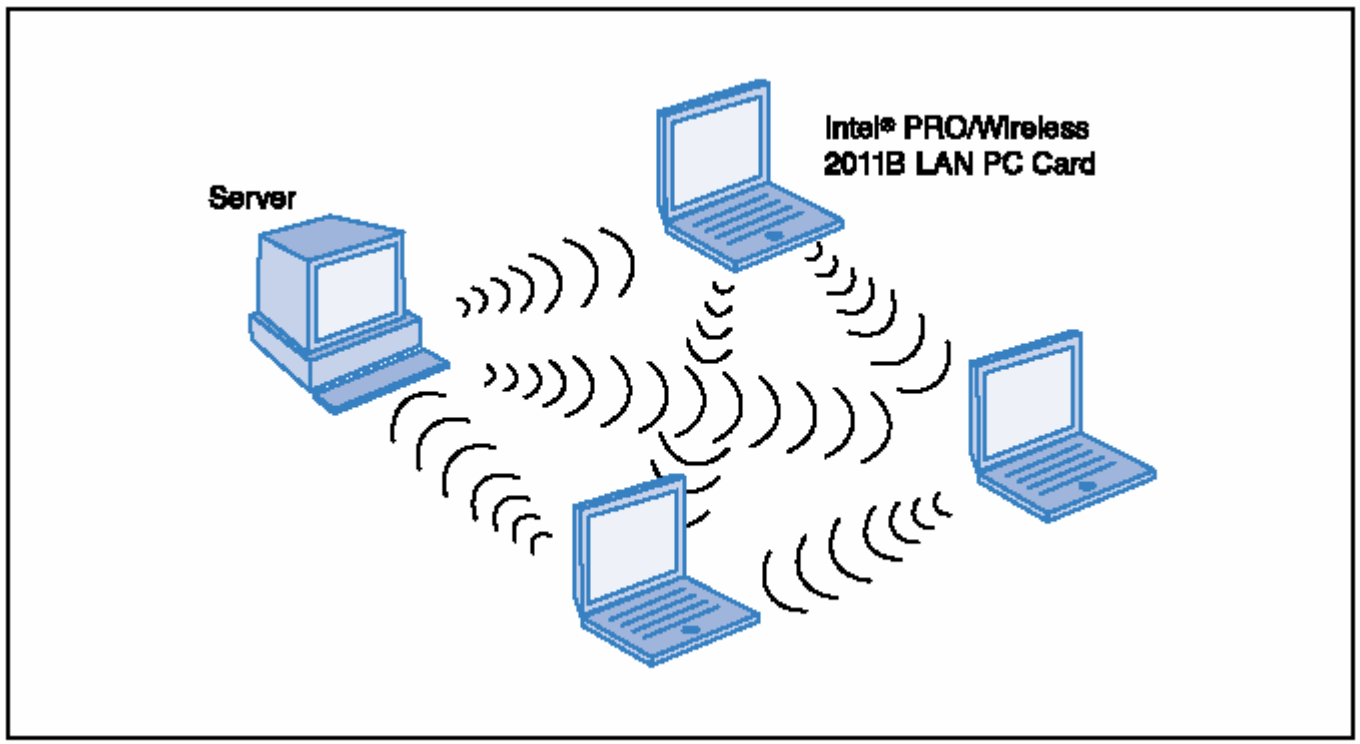


Figure A, Peer-to-Peer Wireless Configuration.

Configuración Ad-hoc

- Todas las estaciones se reconocen entre sí y se comunican directamente.
- No hay intermediación de un AP.
- Esta configuración se forma por pequeños lapsos.

Configuración Cliente-Servidor

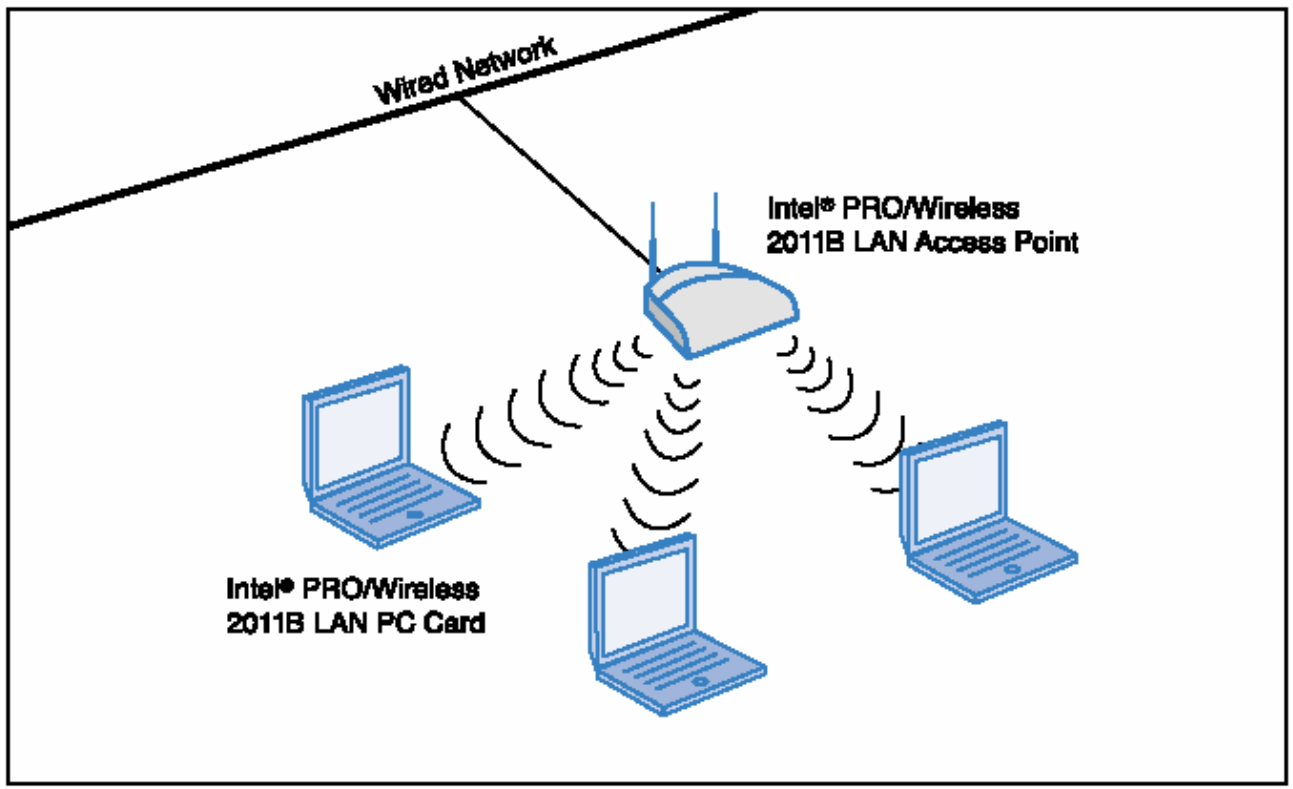


Figure B, Client/Server Wireless Configuration.

Configuración Cliente-Servidor

- Todas las comunicaciones pasan a través del AP.
- El AP es fijo y también forma parte de la red cableada.

Equipamiento WLAN

USA Canadá y Europa: 2.4-2.4835 GHz

Japón: 2.471-2.497 GHz

Existen tres dispositivos que forman la base de una WLAN:

- *Adaptadores WLAN*

  Similares a los adaptadores LAN, permiten a los usuarios acceder a la red, son la interfaz entre el sistema operativo de red y la antena.

Equipamiento WLAN (APs)

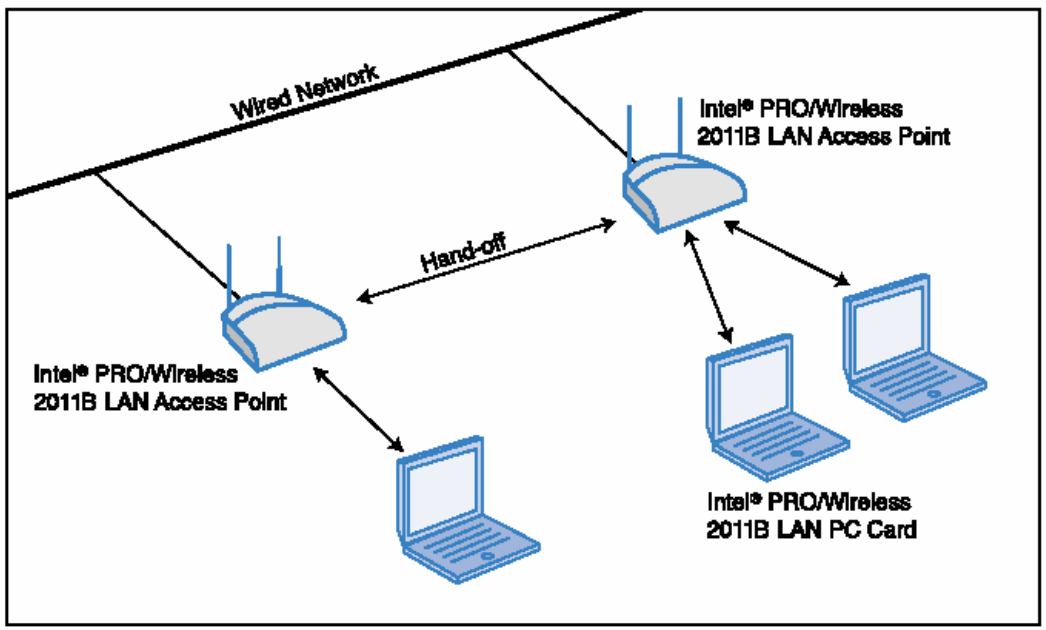
- *Access Point*

  Es el equivalente a un hub. Su función es recibir, encolar y transmitir datos entre la WLAN y la red cableada. Típicamente se conecta a la LAN con un cable Ethernet convencional y se comunica con los terminales móviles por medio de antenas.

  Generalmente se sitúan en el cielo raso.

Equipamiento WLAN (APs)

Varios AP son capaces de realizar handoff entre ellos si el usuario se cambia de área.



Equipamiento WLAN (APs)

- Los AP funcionan en rangos de 20 a 500 metros.
- Cada AP soporta entre 15 y 250 usuarios.
- Un AP puede rastrear el movimiento de un usuario y permitir o denegar clientes o tráfico específico. (control por MAC)

Equipamiento WLAN (APs)

- Es fácil escalar WLANs agregando APs.
- Disminuye la congestión y aumenta el área de cobertura.

  Los AP pueden usarse como bridges entre edificios cercanos.

Equipamiento WLAN

- *Outdoor LAN bridges*

  Se usan para conectar LANs en edificios distintos. Cuando los costos de instalar un cable son altos, un *WLAN bridge* es una buena alternativa.

  Soportan altas tasa de transmisión y varios kilómetros de alcance si se utilizan antenas direccionales en presencia de LOS.

Capas del protocolo IEEE 802.11

Capas del protocolo

- Las especificaciones definen dos capas:
  - Capa 1 o capa física (PHY)
  - Capa 2 o capa MAC (MAC)

Capas del protocolo

La capa física específica las técnicas de modulación usadas y las características de señalización para la transmisión en radio frecuencia.

La capa 2 define la forma de acceder a la capa 1.

2. Capa Física PHY

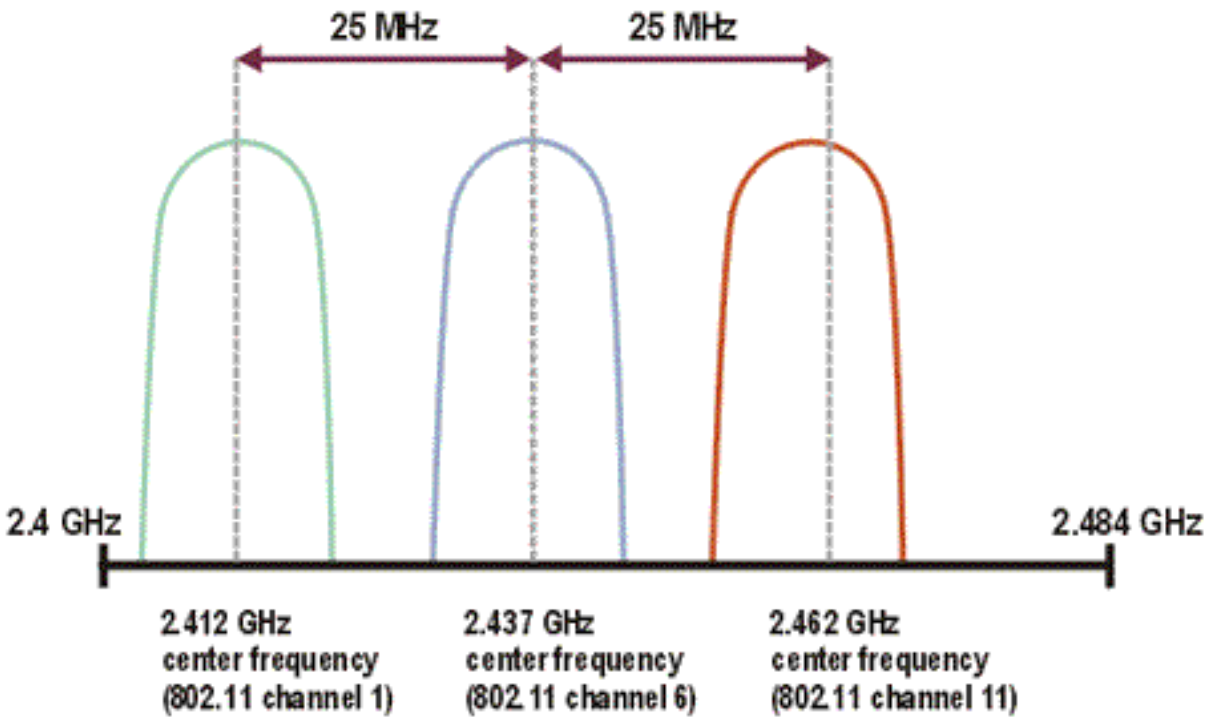
Capa Física PHY

- Originalmente se definieron 3 capas físicas (PHY) para 802.11, dos de SS y una infrarrojo.
- Las técnicas de SS aumentan la confiabilidad, y permiten que productos diferentes compartan el espectro con mínima interferencia.
- El estándar original define tasas de 1 Mbps y 2 Mbps usando FHSS o DSSS.

Canales

- Cuando se utiliza DS, se divide la banda de 2.4 GHz en 14 canales de 22 MHz.
- Sólo existen 3 canales que no se traslapan, pero no son únicos.
- Los canales 1, 6 y 11 son usados comúnmente para minimizar la complejidad en la configuración y administración de los canales

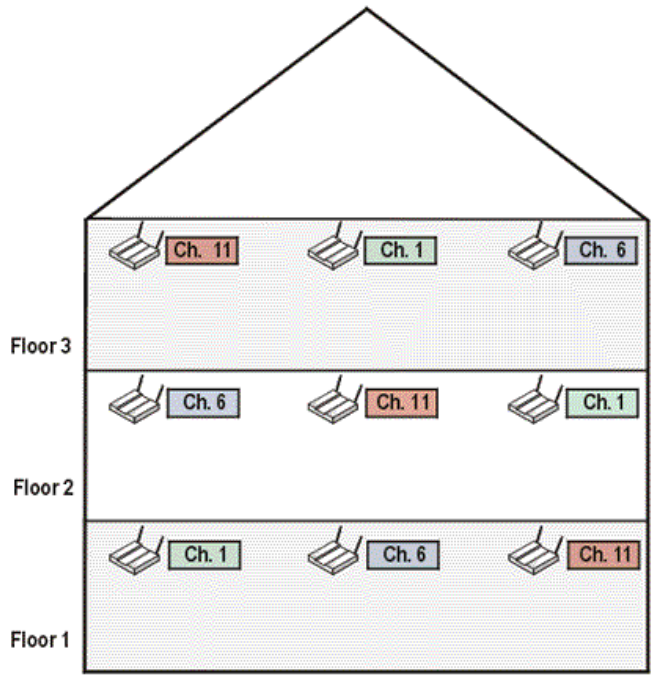
Canales



Source: *The IEEE 802.11 Handbook: A Designer's Companion*

Ejemplo

- Se muestra un edificio con 9 APs.
- Se minimiza la interferencia entre APs.
- Si se producen contiendas entre dos APs configurados en el mismo canal, el mecanismo CSMA/CA asegura que ambos usuarios accederán a la red.



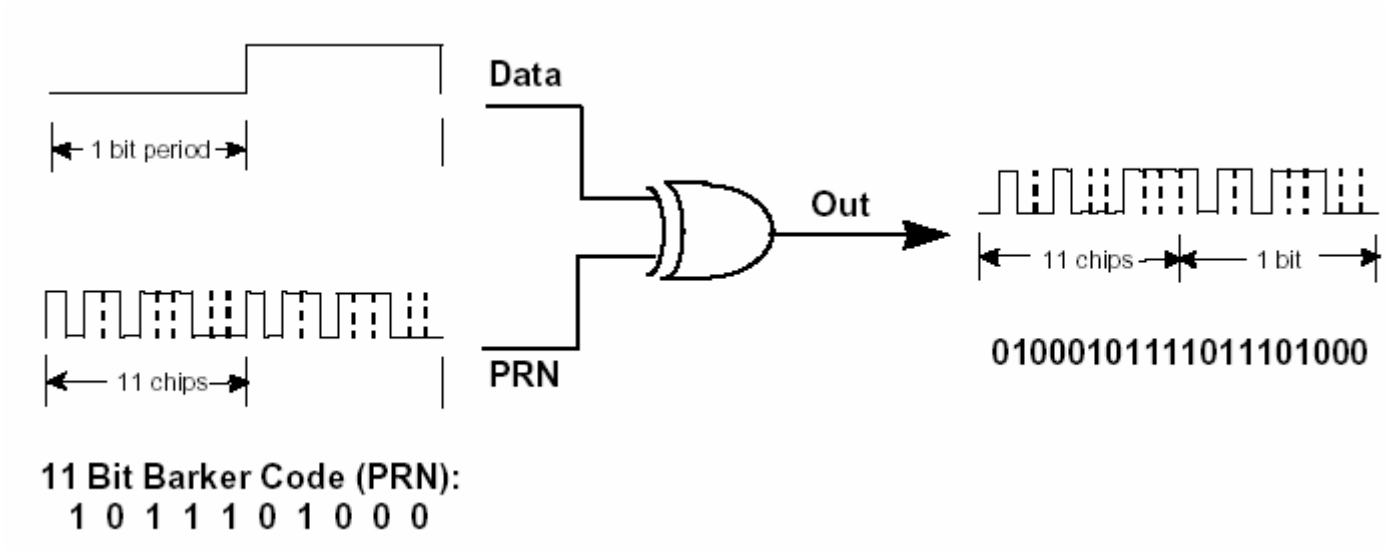
Capa Física PHY

- Para compensar el ruido en un canal dado se usa una técnica llamada “chipping”. Cada bit de datos se convierte en una serie de un patron de bits redundantes llamados “chip”.

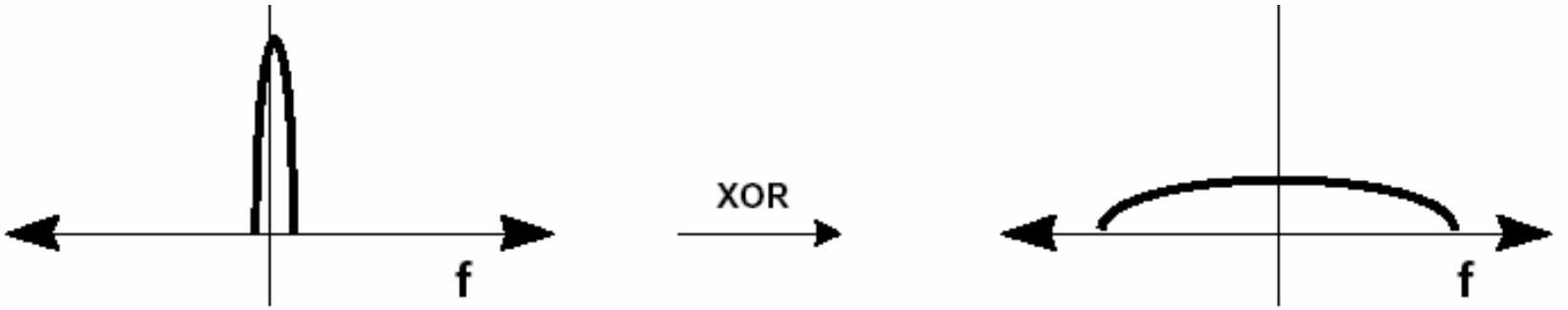
Capa Física PHY

- La contribución clave por parte del 802.11b fue estandarizar el soporte de dos nuevas velocidades: 5.5 Mbps y 11 Mbps. (obliga a usar DS).
- El estándar original especifica un chip de 11 bits, llamado “Barker sequence”. Para codificar los datos (1s o 0s)

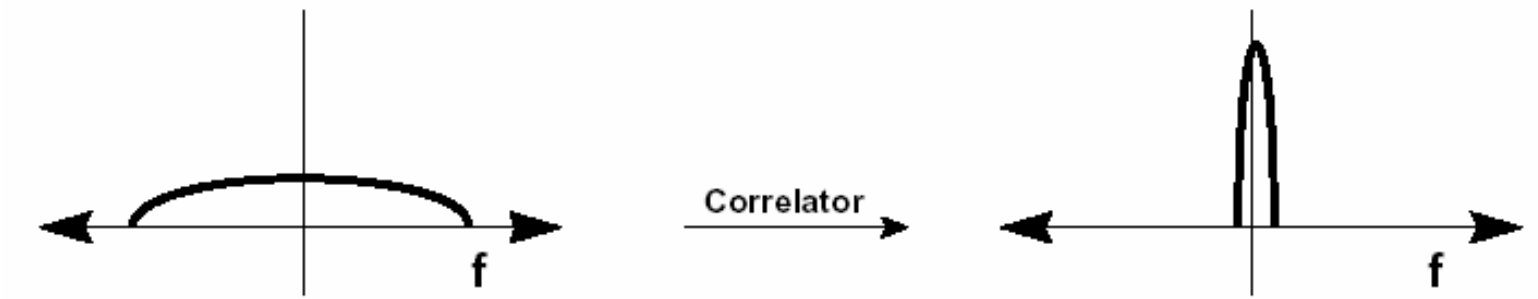
Espectro Ensanchado



Espectro Ensanchado



Efecto de la secuencia PN sobre el espectro transmitido



Señal recibida se correlaciona con PN para recuperar los datos

Espectro Ensanchado

- En vez de la Barker sequence se codifica usando una palabra (de 64 disponibles) de 8 bits (Complementary Code Keying).

- 802.11b usa modulación QPSK y una tasa de 1.375 MSps. Así se obtienen las tasas de transmisión mayores.

Cuadro Resumen

Table 1. *802.11b Data Rate Specifications*

Data Rate	Code Length	Modulation	Symbol Rate	Bits/Symbol
1 Mbps	11 (Barker Sequence)	BPSK	1 MSps	1
2 Mbps	11 (Barker Sequence)	QPSK	1 MSps	2
5.5 Mbps	8 (CCK)	QPSK	1.375 MSps	4
11 Mbps	8 (CCK)	QPSK	1.375 MSps	8

Tasas de Transmisión

- Para soportar ambientes ruidosos y amplia cobertura, 802.11b usa una técnica llamada *dynamic rate shifting,* lo cual permite cambiar automáticamente la tasa de datos para adecuarse a la naturaleza errática de los canales inalámbricos.
- Idealmente los usuarios se conectan a 11 Mbps, pero si se mueven fuera del rango de trabajo de esta tasa, o si hay mucha interferencia, los dispositivos bajan la tasa a 5.5, 2 y 1 Mbps y viceversa.

Tasas de Transmisión

- Este mecanismo está implementado en la capa física y es transparente para el usuario y para las capas superiores.

3. Capa MAC

Acceso al medio DCF

- El método fundamental de acceso al medio para 802.11b es un DCF (Distributed Coordination Function) conocido como CSMA/CA con tiempo de backoff aleatorio.
- El método funciona de la siguiente manera:

Diagrama de flujo CSMA

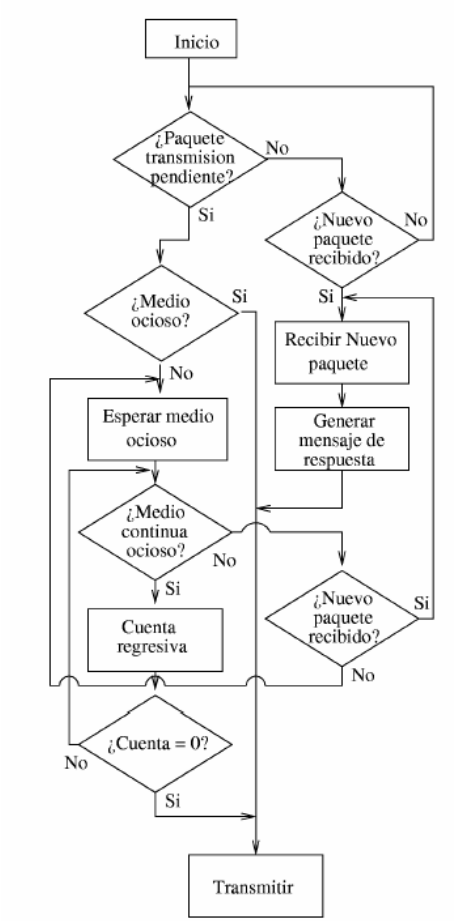


Diagrama de Flujo Estaciones.

Acceso al medio

- El protocolo CSMA/CA está diseñado para reducir la probabilidad de colisión cuando muchas estaciones tratan de acceder al medio.
- Esto ocurre cuando el medio se desocupa luego de una transmisión.
- Para entender el funcionamiento, es necesario introducir los siguientes términos temporales:

Acceso al medio

- **SIFS:** Short Inter Frame Space. Se usa para separar transmisiones de un mismo diálogo (fragm, ack). Sólo hay una estación autorizada para transmitir después de este tiempo. El valor de este tiempo se calcula considerando que la estación transmisora pueda cambiara a modo recepción y decodificar el paquete devuelto. SIFS=28 μs
- **PIFS:** Point Coordination Frame Space. Usado por el AP para tener prioridad sobre las demás estaciones. PIFS=SIFS+1 slot = 78 μs

Acceso al medio

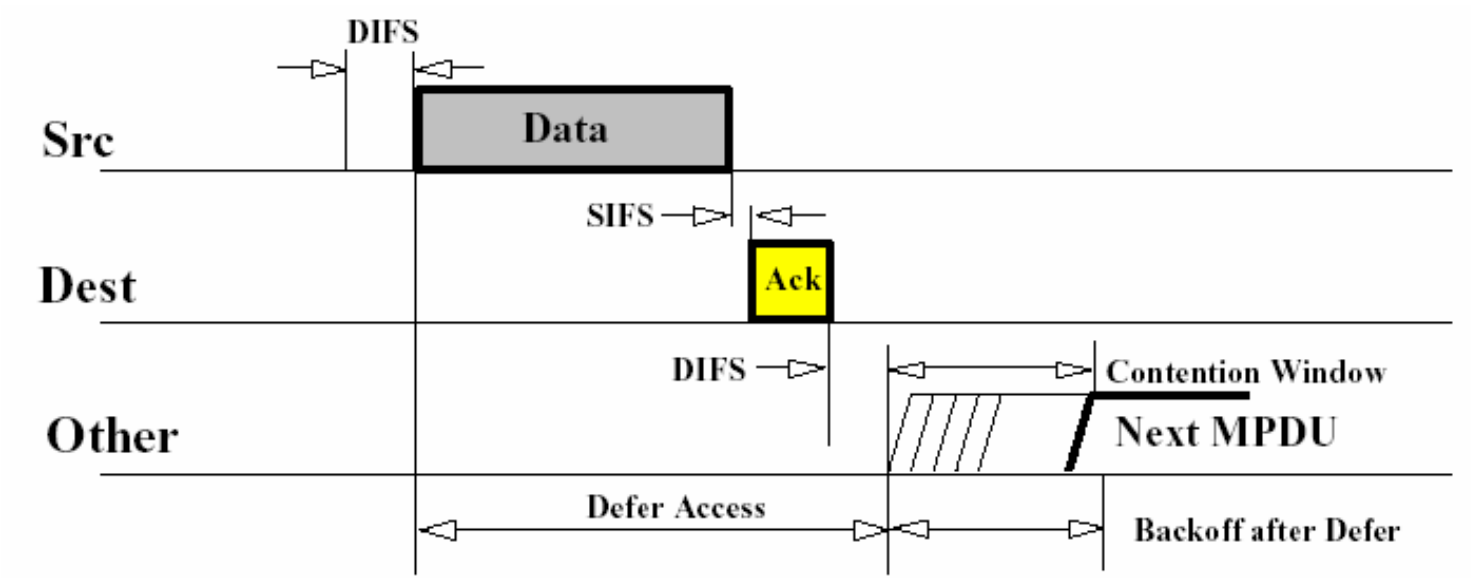
- **DIFS:** Distributed Inter Frame Space. Se usa para la estaciones que desean comenzar una transmisión. DIFS = PIFS+ 1 slot = 128 μs
- **EIFS:** Extended Inter Frame Space. Se usa para estaciones que reciben un paquete que no pueden entender. Se usa para prevenir colisiones de una estación que no comprendió la información de duración.

Acceso al medio

- Si un transmisor detecta que el canal está ocupado, espera un tiempo de back-off aleatorio (ranurado) a partir del término de un DIFS.
- Si otra estación toma el canal en el intertanto, el timer se detiene en el valor actual.

Acceso al medio

- Luego, utilizarán esa información más el protocolo CSMA para sensar el medio.



Acceso al medio

Este mecanismo funciona muy bien en redes LAN, pero presentan problema en un sistema inalámbrico por dos razones:

- Implementar un sistema con CD requiere implementar un enlace Full Duplex (demasiado caro).
- En un ambiente inalámbrico no se puede garantizar que todas las estaciones “se ven”. Por lo tanto, si una estación tx sensa el medio libre, no significa que el medio esté libre en el extremo receptor.

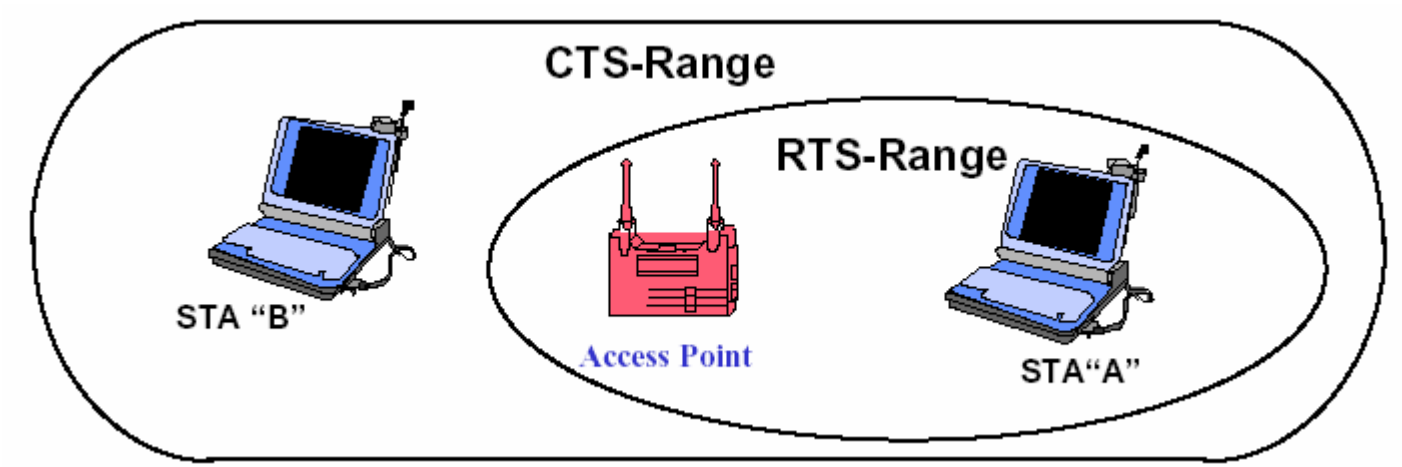
Acceso al medio

- El estándar implementa un sistema adicional (CA) para solucionar este problema mediante paquetes de control. (Virtual Carrier Sense)
- Cuando una estación desea transmitir, envía un paquete de control llamado RTS al AP.
- Luego espera por una paquete de respuesta llamado CTS.
- Las demás estaciones actualizan la información de reserva del medio.

Acceso al medio

- Dado que el AP tiene alcance hacia todas las estaciones, éstas recibirán el CTS y sabrán que el canal se encuentra reservado (soluciona el problema de nodo oculto).
- Luego de recibir el CTS, la estación habilitada transmitirá los datos y esperará por el ACK correspondiente.
- Este esquema puede no utilizarse siempre. (RTS Threshold)

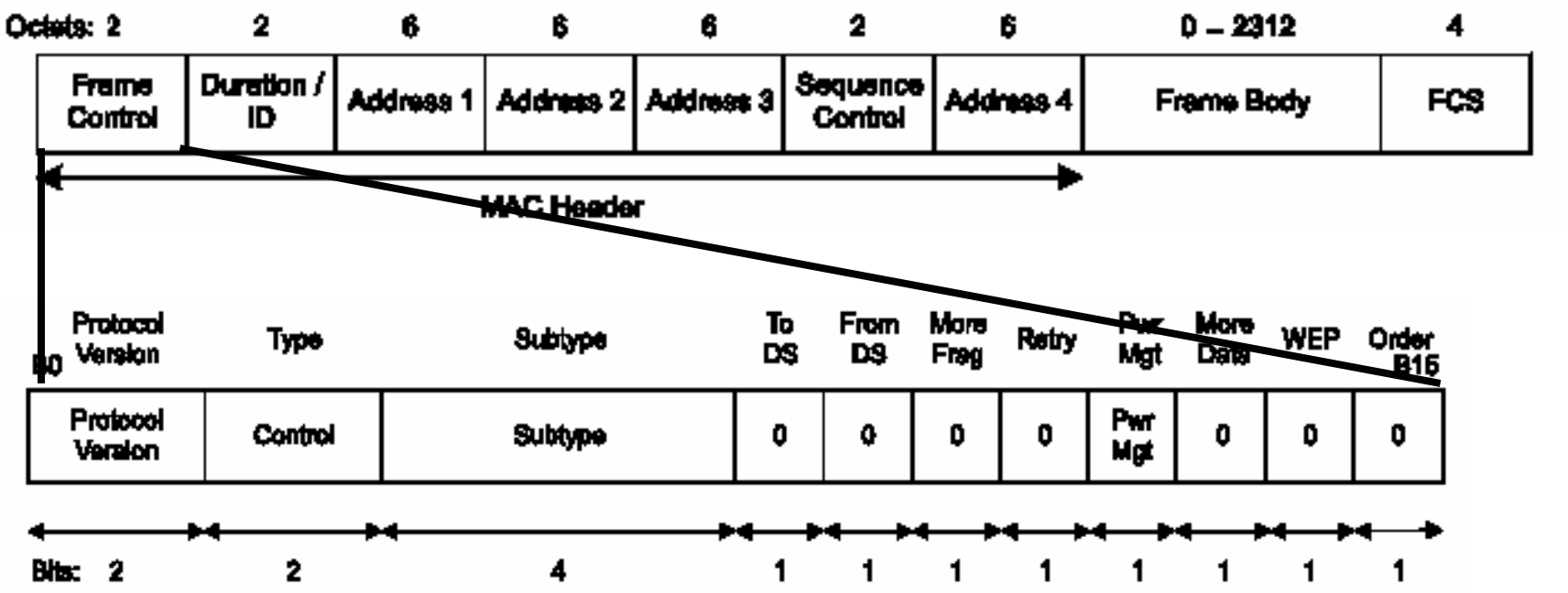
Acceso al medio



Este mecanismo soluciona el problema de nodo oculto.

Formato de Tramas

MAC Data Frame



Formato de Tramas

- Frame Control:
  - Type: Tipo de trama (control, data, management, reserved). 2 bits.
  - En la tabla se definen algunas combinaciones de tipo y subtipo.

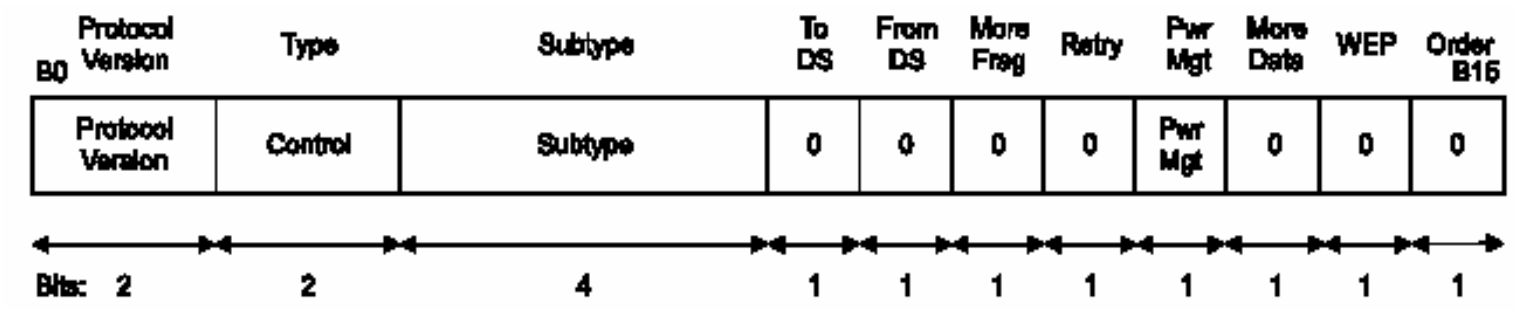
Formato de Tramas

Type value b3 b2	Type description	Subtype value b7 b6 b5 b4	Subtype description
00	Management	0000	Association request
00	Management	0001	Association response
00	Management	0010	Reassociation request
00	Management	0011	Reassociation response
00	Management	0100	Probe request
00	Management	0101	Probe response
00	Management	0110–0111	Reserved
00	Management	1000	Beacon
00	Management	1001	Announcement traffic indication message (ATIM)
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication
00	Management	1101–1111	Reserved
01	Control	0000–1001	Reserved
01	Control	1010	Power Save (PS)-Poll
01	Control	1011	Request To Send (RTS)

Formato de Tramas

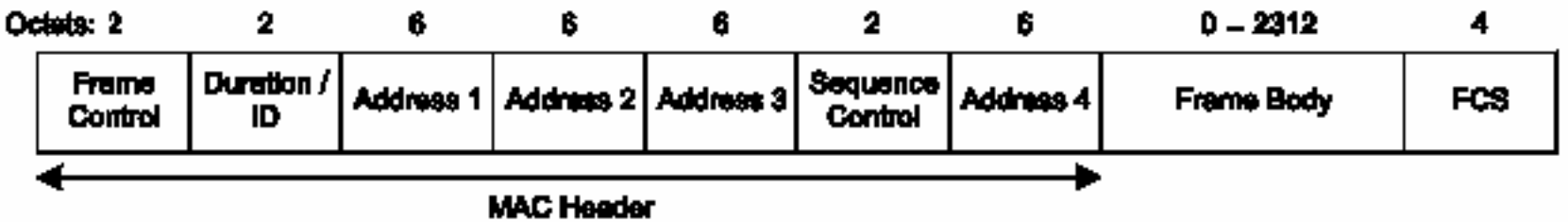
Valores To/From DS	Significado
To DS=0 From DS=0	Datos desde una estación a otra dentro de la IBSS. Datos de control
To DS=1 From DS=0	Datos destinados a la DS
To DS=0 From DS=1	Datos provenientes de la DS
To DS=1 From DS=1	Tramas que van de un AP a otro AP

Formato de Tramas



- Retry: Si es un 1, la trama es una retransmisión.
- Pwr Mng: Indica el modo de manejo de potencia. Un 1 indica modo power save.
- More Data: Indica si hay más datos encolados para una estación que está en modo power save.
- WEP: Indica si los datos han sido encriptados.

Formato de Tramas



Addresses: Existen 4 campos de direcciones. Son usados para indicar el BSSID, dirección fuente (SA), dirección destino (DA), dirección de estación transmisora (TA) y receptora (RA). Algunas tramas pueden no contener todos estos campos.

Formato de Tramas

- Contenido Trama Address

To DS	From DS	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

Formato de Tramas

- **BSSID:** Identifica cada BSS
- **DA:** Dirección MAC del destinatario final.
- **SA:** Dirección MAC de quien inicia la transmisión.
- **RA:** Dirección MAC del destino de la información en el campo de datos.
- **TA:** Dirección MAC de la estación que transmitió la información del campo de datos.

Formato de Tramas

- Una dirección MAC puede ser de uno de estos tipos:
  - Dirección individual: Asociada a una estación particular de la red.
  - Dirección de grupo: Asociada a una o más estaciones.
    - Multicast
    - Broadcast

Formato de Tramas

Formato de la trama RTS:

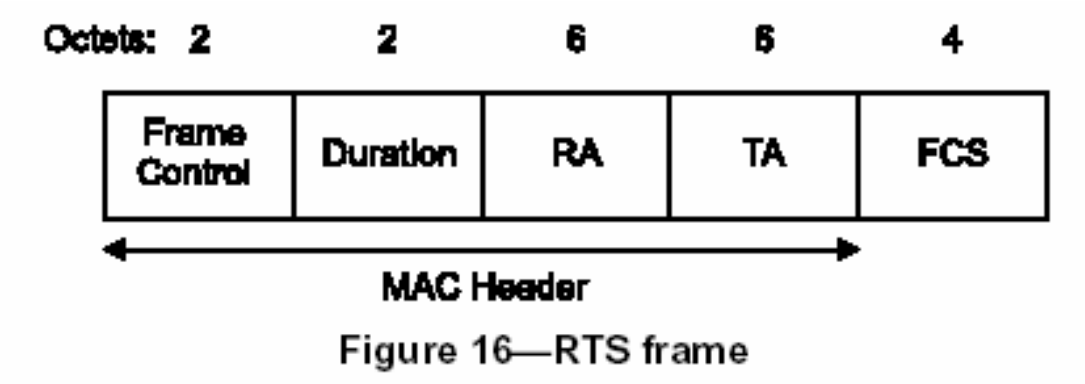
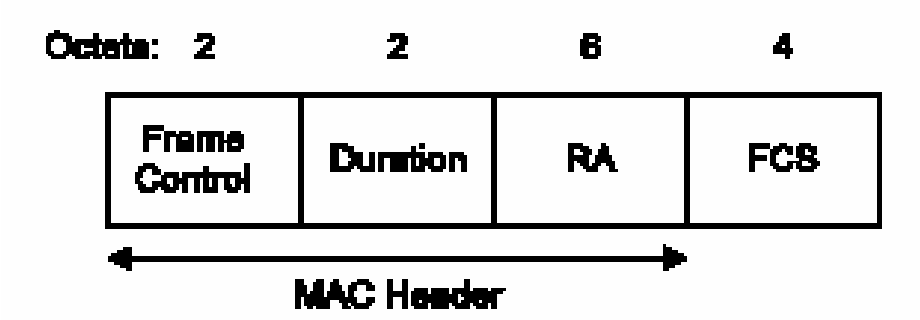


Figure 16—RTS frame

Duration:	Tiempo requerido para la tx completa
RA:	Dirección de destino
TA:	Dirección del transmisor
FCS:	Frame Check Sequence (CRC 32-bits)

Formato de Tramas

Formato de la trama CTS:



Características adicionales

- La capa MAC provee dos características importantes: CRC checksum y fragmentación de paquetes.
- A cada paquete se le calcula un CRC, que se transmite junto con el paquete para asegurar que los datos sean válidos.
- La fragmentación permite que paquetes grandes se dividan en otros más pequeños.

Características adicionales

- Muy útil en áreas congestionadas o con mucha interferencia, debido a que un paquete grande tiene es más susceptible a fallas.
- La capa MAC es responsable de rearmar los paquetes, siendo este proceso transparente para las capas superiores.

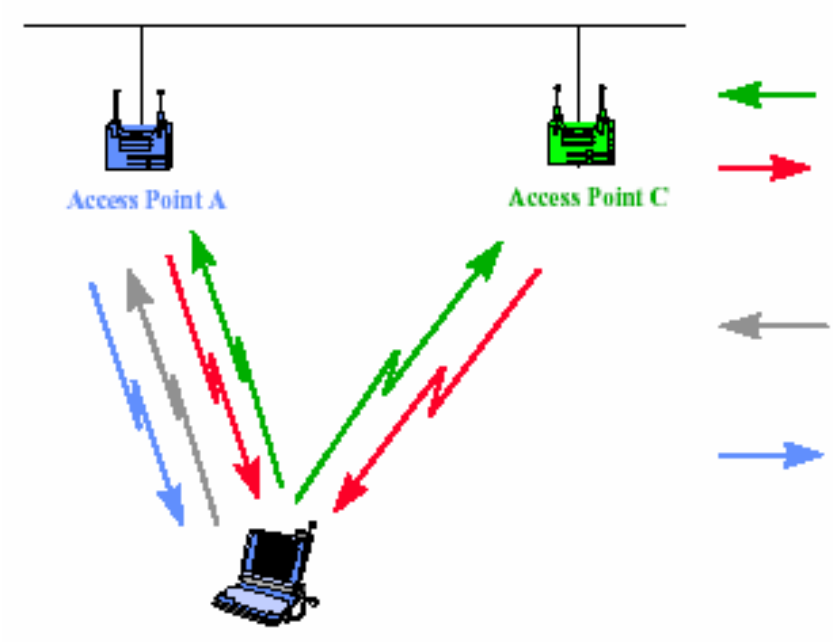
Roaming

- Estaciones pueden moverse más allá del radio de cobertura de su AP, pero dentro del rango de otro AP.
- Esta reasociación le permite continuar su operación.
- La estación decide que el enlace con su AP es débil.

Roaming

- Usa una función de scanning para buscar otro AP.
- Mandan una petición al nuevo AP.
- AP informa de la asociación al DS el cual es actualizado.
- De lo contrario, se continúa haciendo scanning.

Roaming (scanning activo)



Estación manda prueba

APs responden la prueba

Estación selecciona el mejor AP

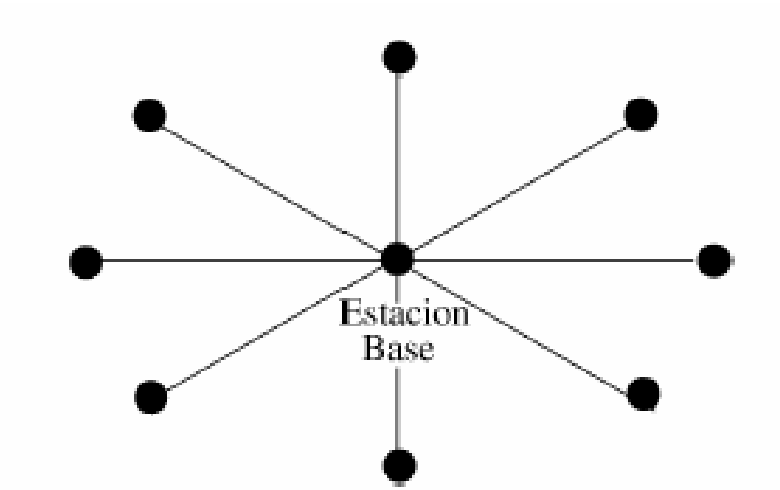
Estación manda petición de asociación

AP responde la petición

4. Medidas de Desempeño en 802.11b

Medidas de Desempeño

- Se presentarán curvas basadas en el siguiente modelo para una red WLAN:

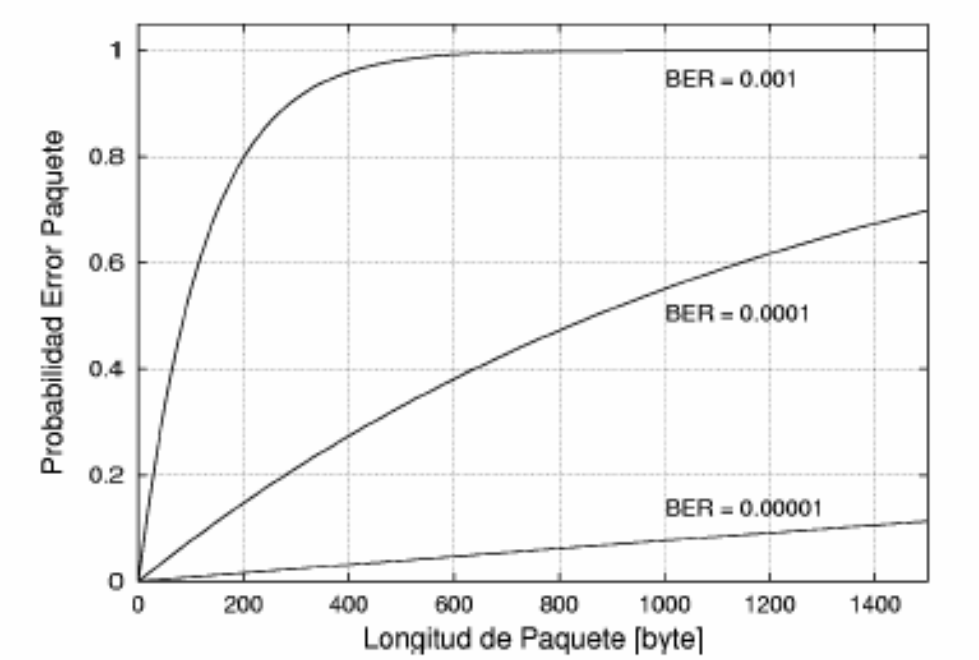


Modelo de Topología de Red

Medidas de Desempeño

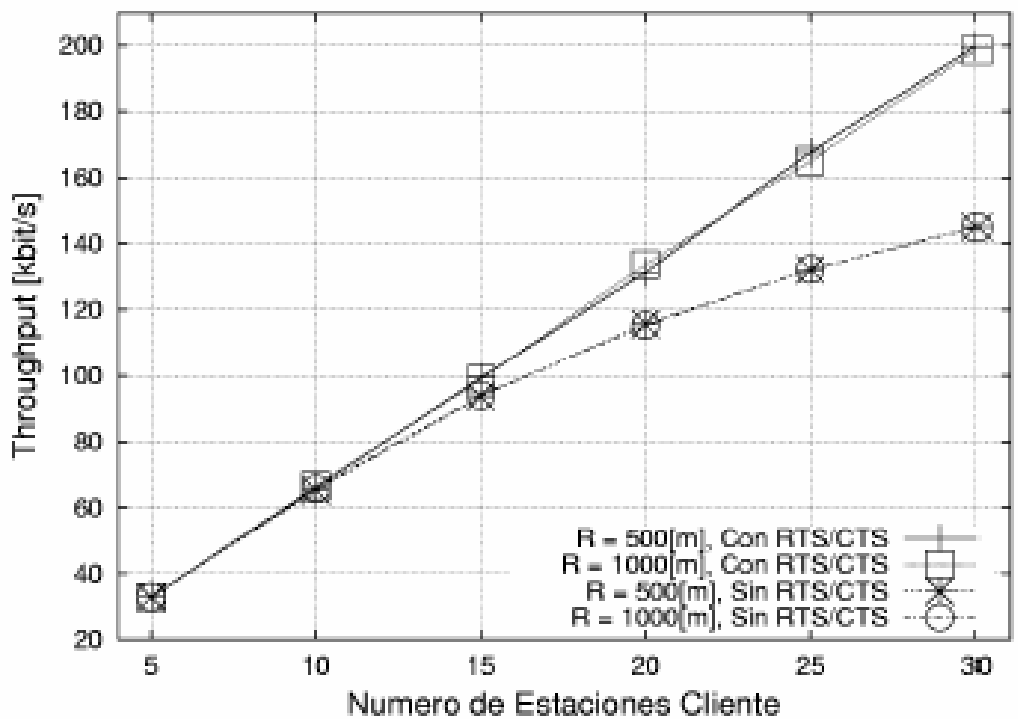
- Supuestos del modelo:
  - La estación base (AP) distribuye el tráfico de Internet.
  - La distancia entre el AP y las STAs superan los 400m.
  - Antenas altamente directivas.
  - El tráfico generado por cada cliente es independiente.
  - El tiempo entre generación de paquetes se modela mediante una distribución de Poisson.
  - No se considerarán errores de canal.

Probabilidad de Error



Probabilidad de error de paquete PER v/s longitud del paquete. Parametrizado para distintos valores de probabilidad de error de bit BER

Throughput Medio

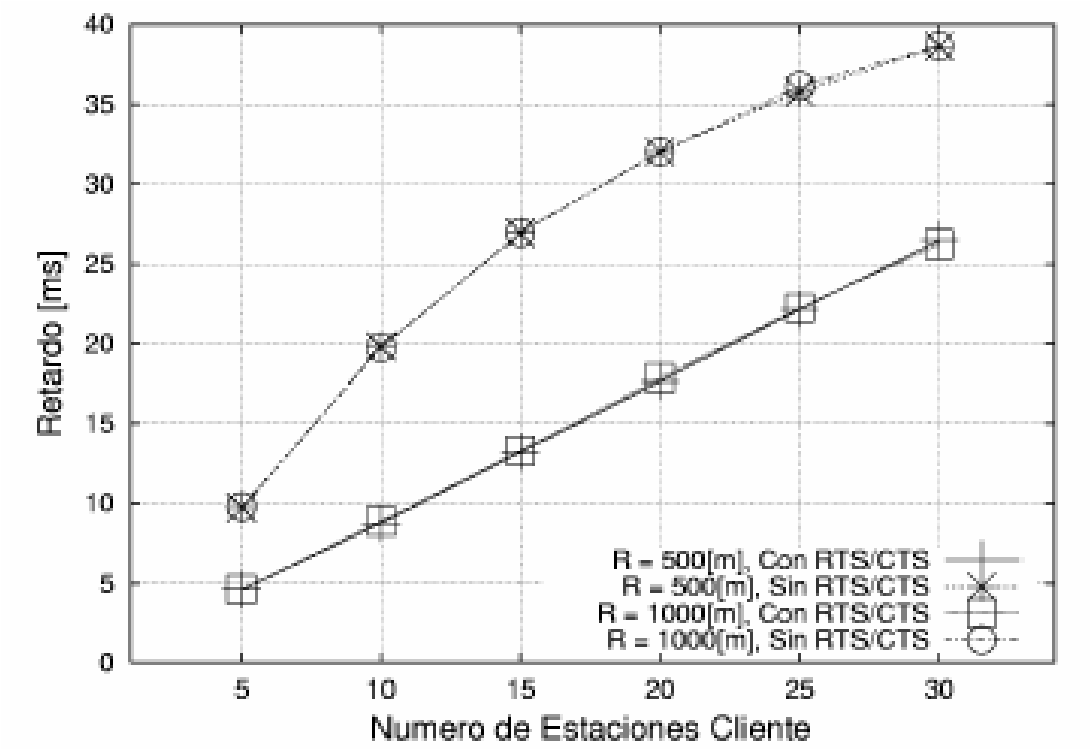


Throughput Medio Total

Throughput Medio

- Independiente del rango de cobertura.
- Mientras más usuarios mayor el throughput.
- Cuando se usa RTS/CTS no se nota un efecto de saturación.
- Desde el punto de vista del throughput, el mecanismo RTS/CTS logra mejorar el desempeño de la red.

Retardo Medio STAs



Retardo Medio Estaciones Cliente.

Retardo Medio STAs

- Aumento progresivo en el retardo a medida que se agregan más clientes.
- Si se utiliza intercambio RTS/CTS, el retardo aumenta en forma lineal.
- Si no se utilizan las tramas RTS/CTS, el retardo es mayor con cierta tendencia a estabilizarse.
- RTS/CTS contempla un menor retardo debido a que previene colisiones producidas por terminales ocultos, y por ende retransmisiones.

5. Administración de Potencia

Modos de operación

Existen dos modos de operación:

Active mode (AM): Las estaciones pueden recibir en cualquier instante.

Power Save (PS): Las estaciones escuchan a veces para ver si el AP tiene información encolada para el. El AP le transmite esta información (o ACK) sólo en respuesta de una trama PS-Poll.

Modos de operación

- Para cambiar de modo, las estaciones deben informar al AP mediante el bit disponible en la trama de control.
- El AP debe conocer el modo actual de operación de todas las estaciones en su dominio.

Modos de operación

- Las estaciones que actualmente tienen datos encolados para ellas, son mapeadas en el TIM (traffic indication map), el cual es transmitido junto con todos los beacons que genera el AP. (para sincronización)
- Las estaciones en modo PS deben estar escuchando estos beacons periódicamente.

Administración de Potencia

La potencia de transmisión de la mayoría de los AP va de 1 mW a 100 mW (en USA).

- Ésta afecta el alcance de la señal. (diseño de celdas)

6. Seguridad en 802.11b

Seguridad en 802.11b

- Como el medio es compartido, todos los datos sobre una red wireless pueden ser interceptados
- El Standard IEEE 802.11b contempla mecanismos de autenticación y encriptación.
- La meta es hacer una red wireless tan segura como una red cableada.
- El protocolo implementado en el standard es el Wired Equivalent Privacy (WEP).

Seguridad en 802.11b

- Siempre deben considerarse tres aspectos:
  - *Los clientes necesitan privacidad.*

    Cuan robustos y costosos deben ser los protocolos.
  - *Fácil de usar*.

    Si la implementación es muy difícil, entonces no se va a usar.
  - *Regulaciones Gubernamentales*.

    La encriptación es vista como municiones por muchos países. Los productos encriptados son controlados para la exportación.

Seguridad en 802.11b

- Las redes wireless irradian los datos más allá de la zona en que trabaja la organización.
- Las ondas de 2.4 GHz fácilmente pueden atravesar paredes o lograr un par de cuadras de alcance.
- Cualquier persona dentro de este radio puede interceptar la información si posee la misma NIC (Network Interface Card).

Seguridad en 802.11b

- La mayoría de los adaptadores LAN poseen un modo “promiscuo” el cual permite capturar todos los paquetes en su segmento de red (con un software adecuado)

- Los ataques más comunes a una red cableada o wireless son :
  - *Amenazas a la seguridad física de la red. (DoS y sabotaje)*
  - *Acceso no autorizado.*
  - *Ataques desde dentro de la red.*

Seguridad en 802.11b

- Por lo tanto, las medidas utilizadas para asegurar la integridad de una red cableada también se aplican a una red wireless
- 802.11b ofrece un set extra de elementos de seguridad (WEP)
- Red wireless puede ser más segura que una red cableada.

Algoritmo WEP

- El algoritmo se eligió para que cumpliera con los siguientes criterios:
  - *Razonablemente robusto (clientes)*
  - *Auto sincronizable (las estaciones se salen frecuentemente del radio)*
  - *Exportable.*
  - *Opcional.*

Teoría de Operación WEP

- El proceso de ocultar la información contenida es llamado *Encriptación (E).*
- La información que no es cifrada es llamada *Texto Plano (P)* y la cifrada es llamada *Texto Cifrado (C).*
- El proceso de llevar el Texto Cifrado a Texto Plano se llama Des-encriptación *(D).*

Teoría de Operación WEP

- Un algoritmo criptográfico es una función matemática usada para cifrar o descifrar información.
- Algoritmos criptográficos modernos usan una “ k sequence” *(k)* para midificar su salida.

Teoría de Operación WEP

- La función de encriptación opera en P para generar C:

$$E_k(P) = C$$

- La función D opera en C para producir P:

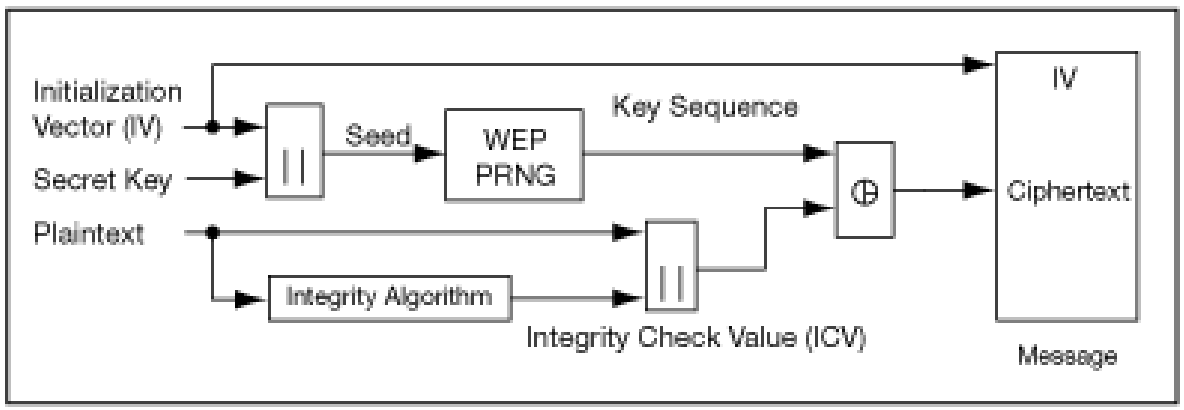
$$D_k(C) = P$$

- Si la misma llave es usada para encriptar y des-encriptar, entonces:

$$D_k(E_k(P)) = P$$

Algoritmo WEP

- Se usa la misma “llave” para encriptar y desencriptar los datos.
- Al texto plano se le aplican dos procesos: el primero encripta el texto plano; y el segundo lo protege de modificaciones no autorizadas (ICV).



Algoritmo WEP

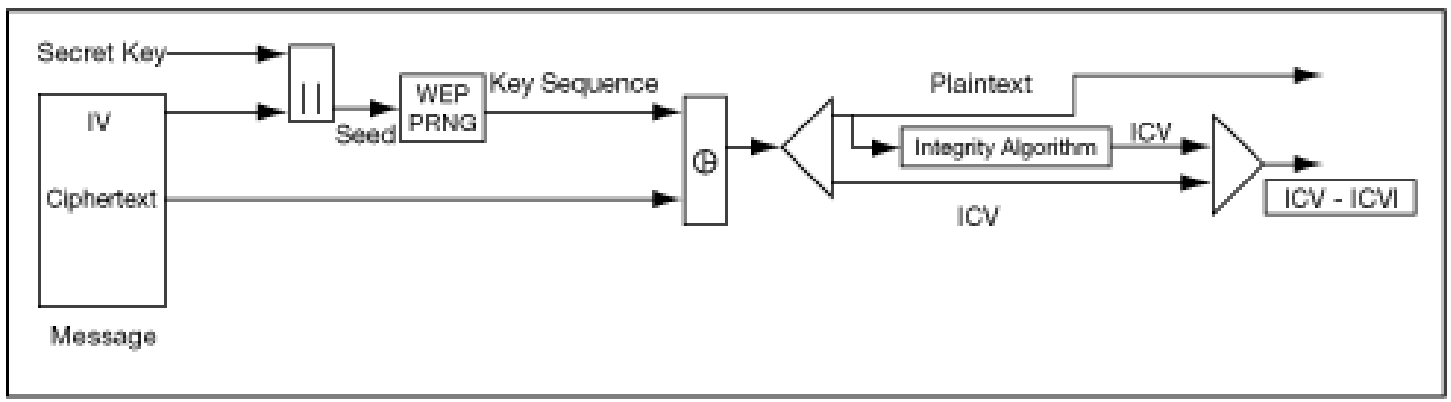
- La llave secreta (40 bits) es concatenada con un vector de iniciación (IV, 24 bits), resultando una llave de 64 bits.
- Esta llave se introduce en el generador de pseudoaleatorio de números (PRNG), el cual genera una secuencia en base a la entrada.

Algoritmo WEP

- Esta secuencia se usa para encriptar los datos haciendo un XOR bit a bit.
- Luego se envía el IV, el texto plano y el ICV.
- En el receptor se usa el IV para regenerar la llave que permita recuperar el mensaje.

Algoritmo WEP

- El mensaje recuperado es pasado por el algoritmo de integridad para generar un ICV'.
- Éste se compara con el ICV transmitido para ver si hubo errores y notificar a la estación transmisora.



Autenticación

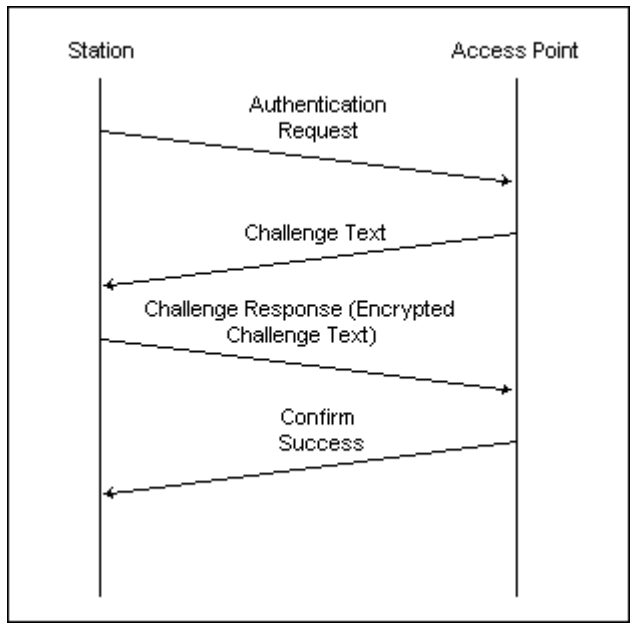
- Existen dos forma de autenticación:
  - *Open system authentication*

    No hay autenticación, la estación se puede asociar a cualquier AP y escuchar a todos los datos que se envían como texto plano.
  - *Shared key authentication*

    Se utiliza la misma llave usada para la encriptación, por lo que se debe tener implementado WEP.

Autenticación

•Una estación envía una authentication frame al AP.
•Cuando el AP la recibe, responde con otra authentication frame que contiene 128 bytes de texto aleatorio generados por el motor WEP.
•La estación encriptará este mensaje con una llave compartida y la reenviará al AP.
•El AP recupera el mensaje encriptado usando la misma llave y la compara al texto enviado anteriormente.



Referencias

- “Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications”, *ANSI/IEEE Std 802.11, 1999 Edition.*
- “Higher-Speed Physical Layer Extension in the 2.4 GHz Band”, Supplement to *ANSI/IEEE Std 802.11, 1999 Edition.*
- Hugo Araya, Walter Grote H, “Modelo de Simulación para Intefaz de Radiofrecuencias del Protocolo IEEE 802.11b”.
- Jim Zyren and Al Petrick, “IEEE 802.11 Tutorial”.
- 3Com Technical Paper, “IEEE 802.11b Wireless LANs”.
- Agilent Technologies, “IEEE 802.11 Wireless LAN PHY Layer (RF) Operation and Measurements”. *Application Note 1380-2.*

Referencias

- Dell White Paper, “Deploying 802.11b (Wi-Fi) in the Enterprise Network”
- Wim Diep Straten, Phil Belanger, “802.11 Tutorial, MAC entity”.
- Intel, “IEEE 802.11b, High Rate Wireless Area Networks”
- Pablo Brenner, “A Technical Tutorial on the IEEE 802.11 Protocol”