

# **WiFi / IEEE 802.11 - WLAN y adaptación a redes rurales extensas**

**Profesor: Francisco Javier Simó Reigadas <javier.simo@urjc.es>**

**MÁSTER OFICIAL EN REDES DE TELECOMUNICACIÓN  
PARA PAÍSES EN DESARROLLO (COMPAD)**

**UNIVERSIDAD REY JUAN CARLOS**

**Madrid, 19 de Octubre de 2009**



# MOTIVACIÓN (I)

- **i IEEE 802.11 = WLAN !**

- Gran éxito del estándar. Omnipresente a escala mundial
- Barato, bueno y eficaz
- Sigue en expansión: subgrupos N,S, ...

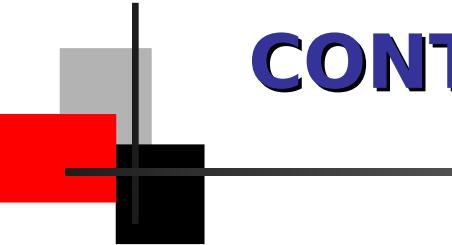
- **En distancias cortas y medias, apto para:**

- Redes inalámbricas de área local en interiores
- Puentes inalámbricos entre edificios
- Hot-Spots
- WISPS: Acceso inalámbrico a servicios de proveedores de servicios de Internet



## MOTIVACIÓN (II)

- Grandes zonas rurales del mundo habitado carecen de sistemas de comunicación con el exterior debido fundamentalmente a:
  - Dificultades de acceso y de electrificación
  - Tecnologías disponibles demasiado caras y restrictivas
- WiFi (IEEE 802.11) ha sido identificada por expertos en TIC para zonas emergentes como una posible solución estratégica porque:
  - Es muy barata
  - Ya se han hecho pequeñas experiencias con éxito
  - Con el complemento de la VoIP se pueden lograr soluciones de comunicaciones de voz y datos sencillas y asequibles
  - Alternativas (WiMAX, ...) son demasiado caras y restrictivas



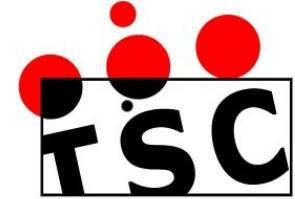
# CONTENIDOS

---

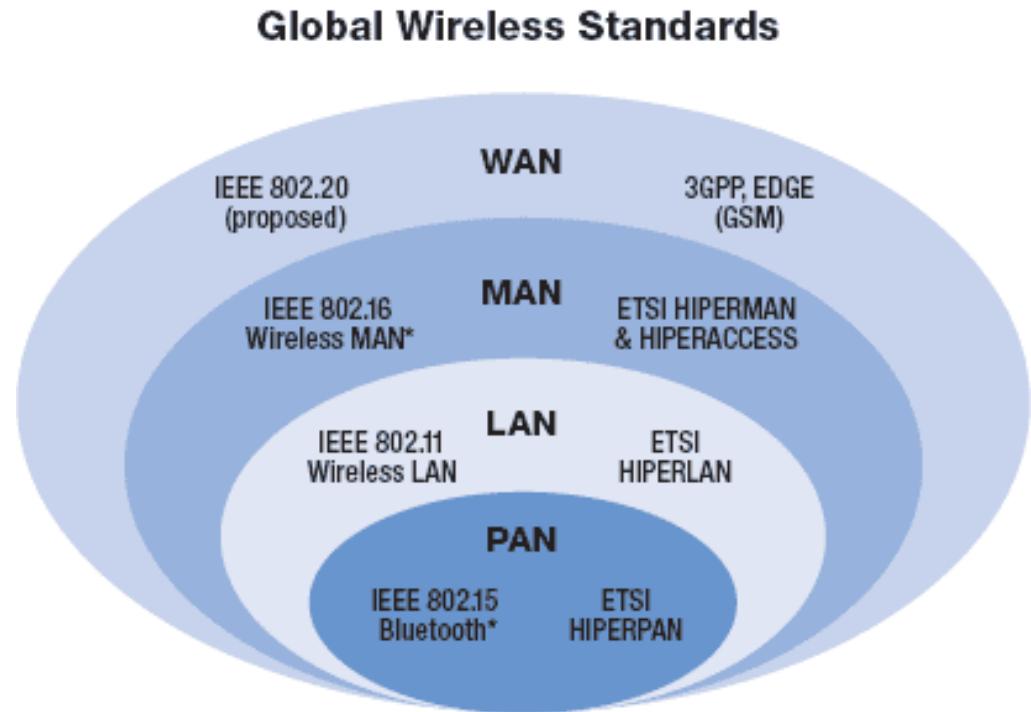


- **Introducción: WLAN, justificación y arquitectura**
- Los estándares de la familia IEEE 802.11
- La capa PHY
- La capa MAC
- Soporte de QoS (calidad de servicio)
- Redes WiFi con grandes distancias
- MAC de WiFi adaptado
- WiLDMAC: Un nuevo MAC TDMA sobre el PHY estándar
- Protocolos propietarios: nstreme, Canopy, Tsunami y otros.

# *Introducción a WiFi*



- WLAN = LAN inalámbricas
- 802.11 es la propuesta WLAN del IEEE
- Distancias entre nodos de decenas o centenares de metros



# Introducción a WiFi

## Necesidades a que responden las WLAN

- Demanda de conectar estaciones de tres tipos: fijas, portátiles y móviles
- Disminuir costes/tiempo de despliegue de red y reubicación de terminales
- Permitir despliegue instantáneo de redes (reuniones, emergencias)
- Servicios a clientes (centros de congresos, hoteles)
- Conexión de bajo coste de edificios cercanos (barcos)
- Imagen corporativa

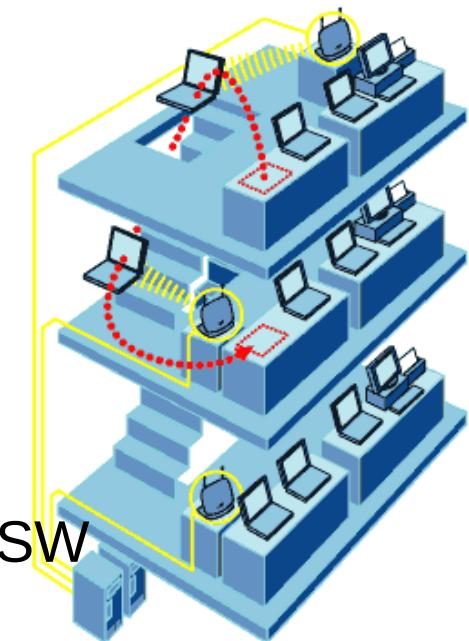


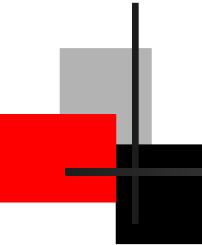
# *Introducción a WiFi*



## Aportaciones de las WLAN

- Eliminación de cables: flexibilidad, movilidad e imagen
- Despliegue de redes en casos con imposibilidad de uso de cables
- Extensión de las LAN convencionales
- Movilidad sin perder conectividad
- Facilidad de instalación y reducción de costes
- Extensión de cobertura de red en exteriores
- Conexión de bajo coste entre edificios
- Transparencia al usuario, sistema operativo y SW
- Facilidad para la extensión y la actualización





# *Introducción a WiFi*



- 1979: primer experimento de WLAN en Suiza, por IBM
- 1985: Regulación de bandas ISM por FCC
- 1991: Primeros trabajos sobre WLAN superando 1Mbps
- **1997: Publicación del estándar IEEE 802.11**
- **1999: Publicación de los estándares IEEE 802.11b y 802.11a**
- **2003: Publicación del estándar 802.11g**
- **2005: Publicación del estándar 802.11e**
- **2008: Primeros productos 802.11n draft 2 en el mercado**
- **2009: En Octubre sale el estándar 802.11n**



# Introducción a WiFi

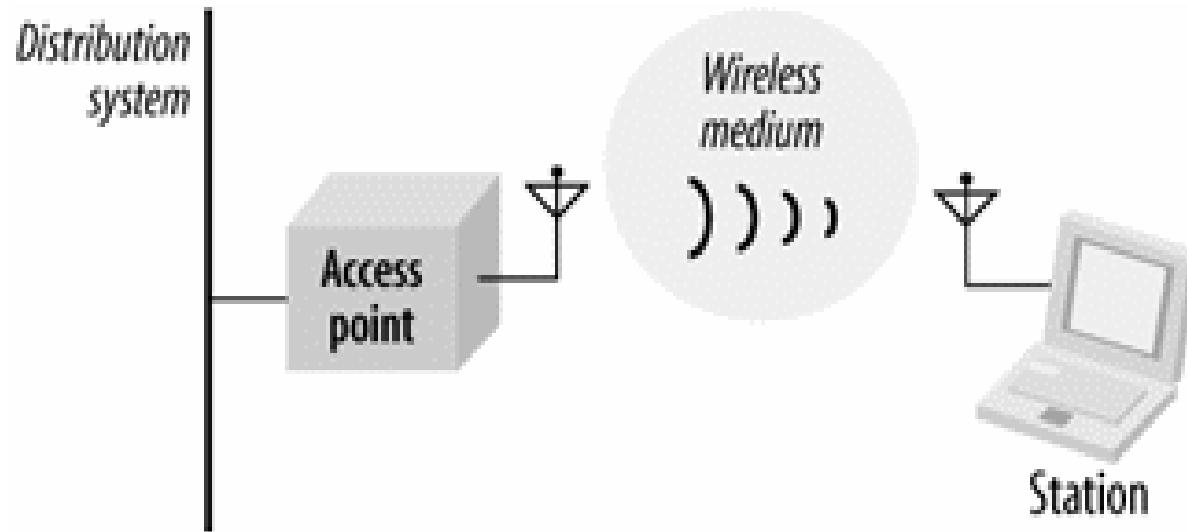
## Elementos básicos de una red Wi-Fi

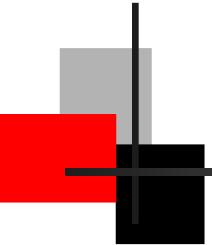
- **Estación (STA)**: cualquier portátil, PDA, etc. dotado de las funcionalidades de 802.11.
- **Punto de acceso (AP)**: nodo Wi-Fi que proporciona conectividad entre las estaciones conectadas a él y entre éstas y el resto de la red.
- **Medio inalámbrico**: se definen distintos medios (PHY) alternativos que difieren en frecuencias, modulaciones, velocidades, etc.
- **Sistema de distribución (DS)**: componente lógico para la conmutación de tramas en sistemas con varios APs unidos por una red troncal

# *Introducción a WiFi*



## Elementos básicos de una red Wi-Fi





# *Introducción a WiFi*



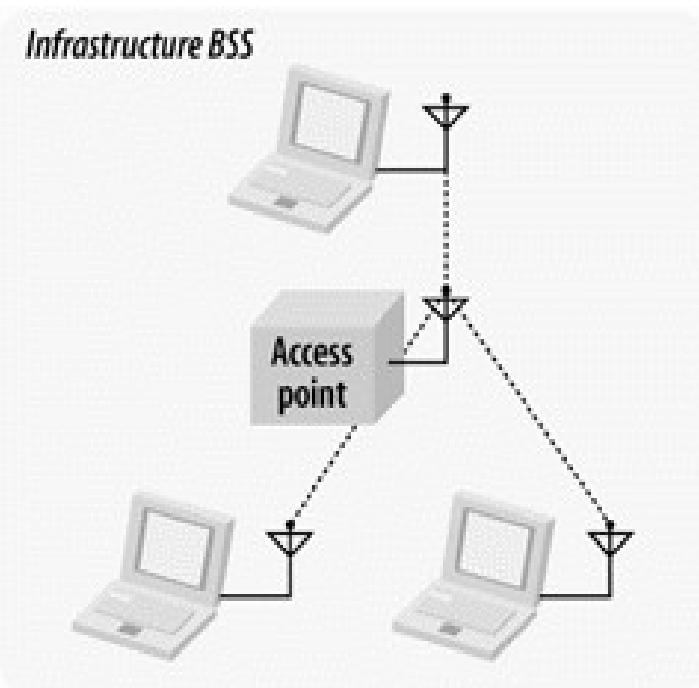
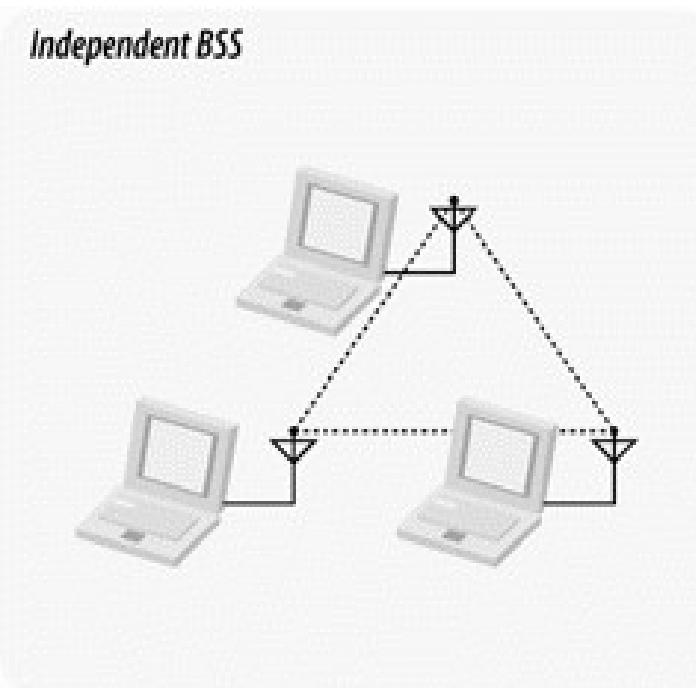
## Bloques constructivos de una red

- **BSS** (Conjunto de servicio básico): STAs que se comunican directamente entre sí. Dos tipos:
  - **IBSS** (BSS independiente): las estaciones se comunican todas con todas directamente. Se habla también de “modo Ad-Hoc”.
  - **BSS con infraestructura**: las estaciones se comunican a través de un AP. Se habla también de “modo Infraestructura”.
- Un BSS se caracteriza por un nombre de red o SSID (Identificador de conjunto de servicio)
- Pueden asociarse varios BSS en un conjunto extendido o **ESS**

# *Introducción a WiFi*



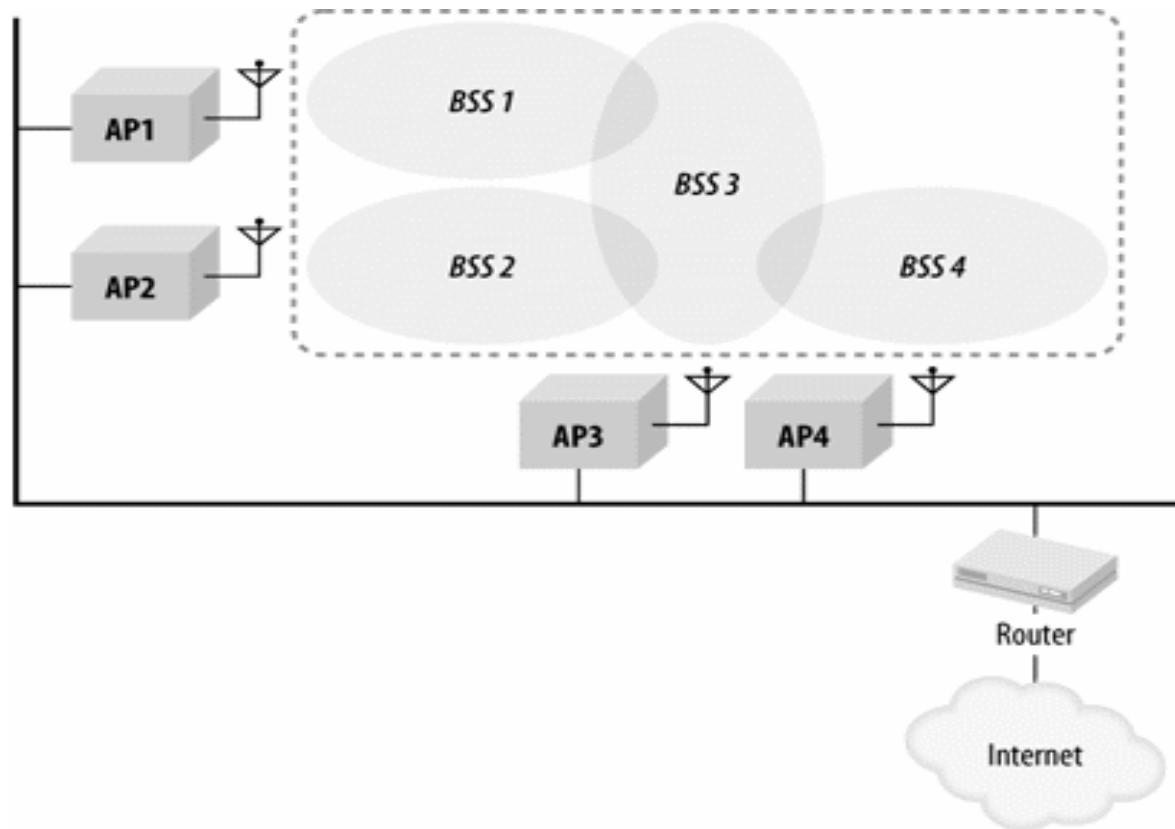
## Tipos de BSS:



# *Introducción a WiFi*

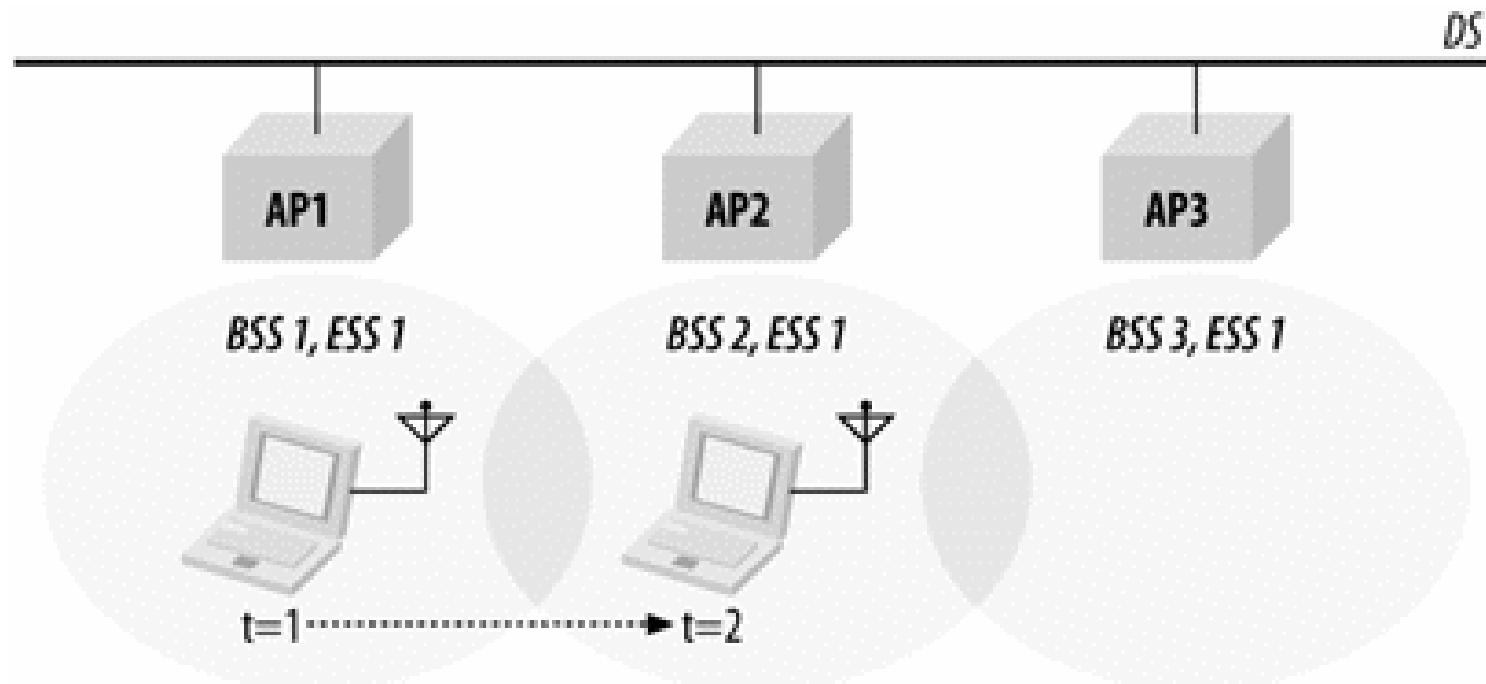


ESS



# Introducción a WiFi

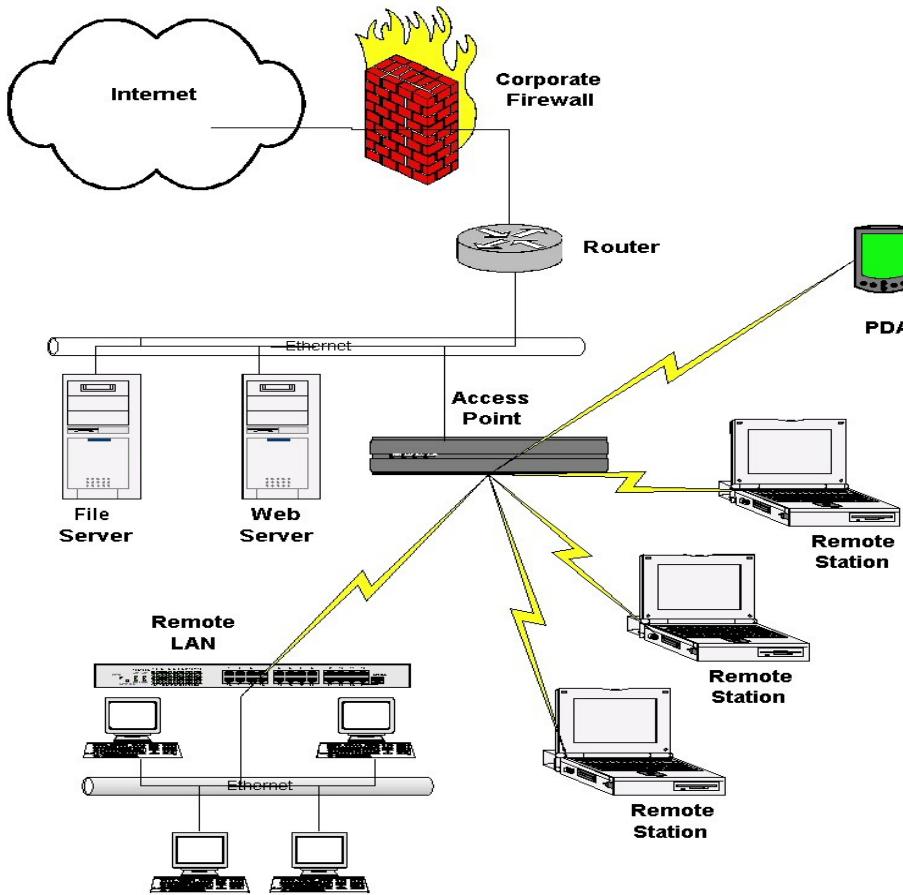
Transición entre BSS de un mismo ESS



# Introducción a WiFi



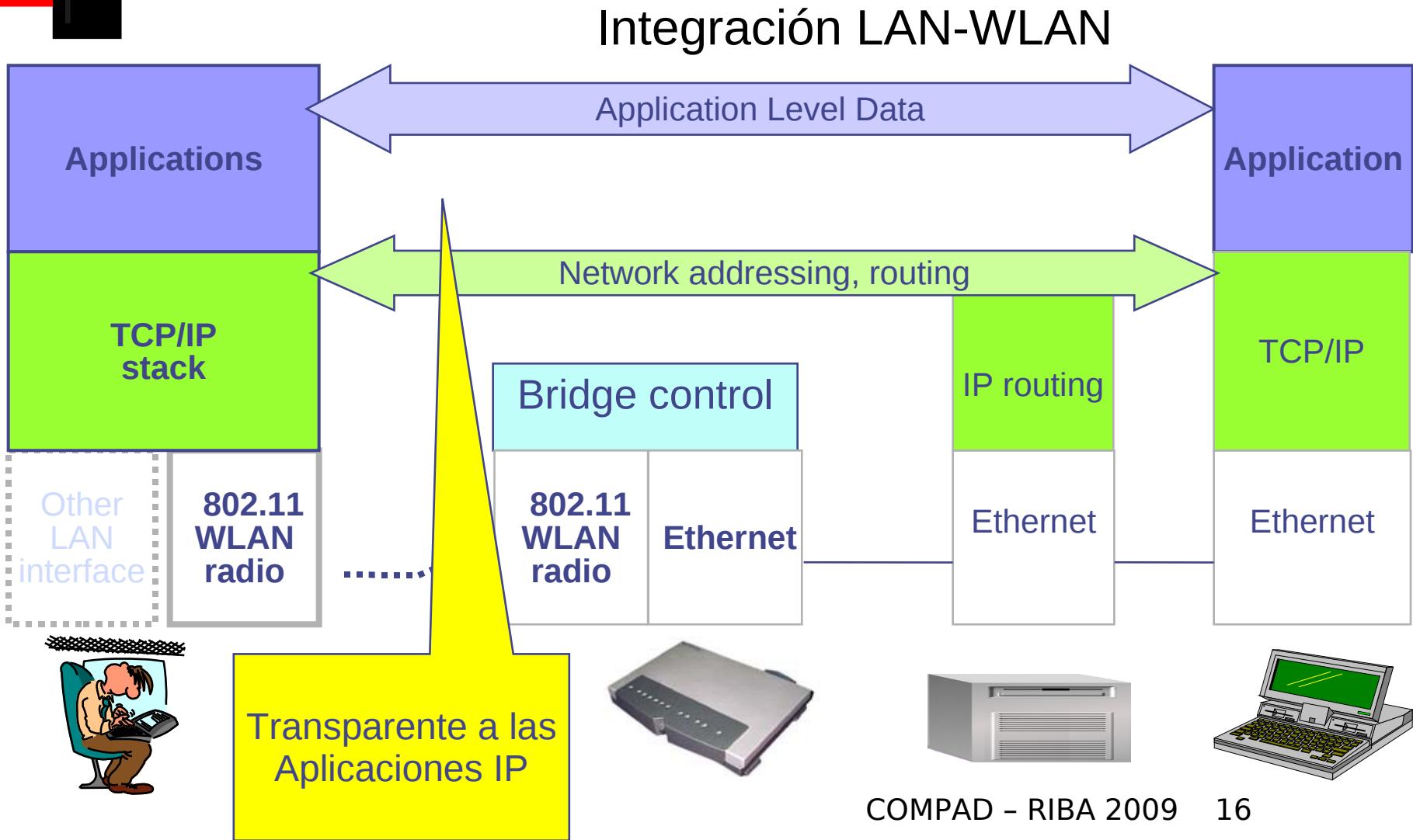
## Configuración genérica WLAN



Extensión inalámbrica para

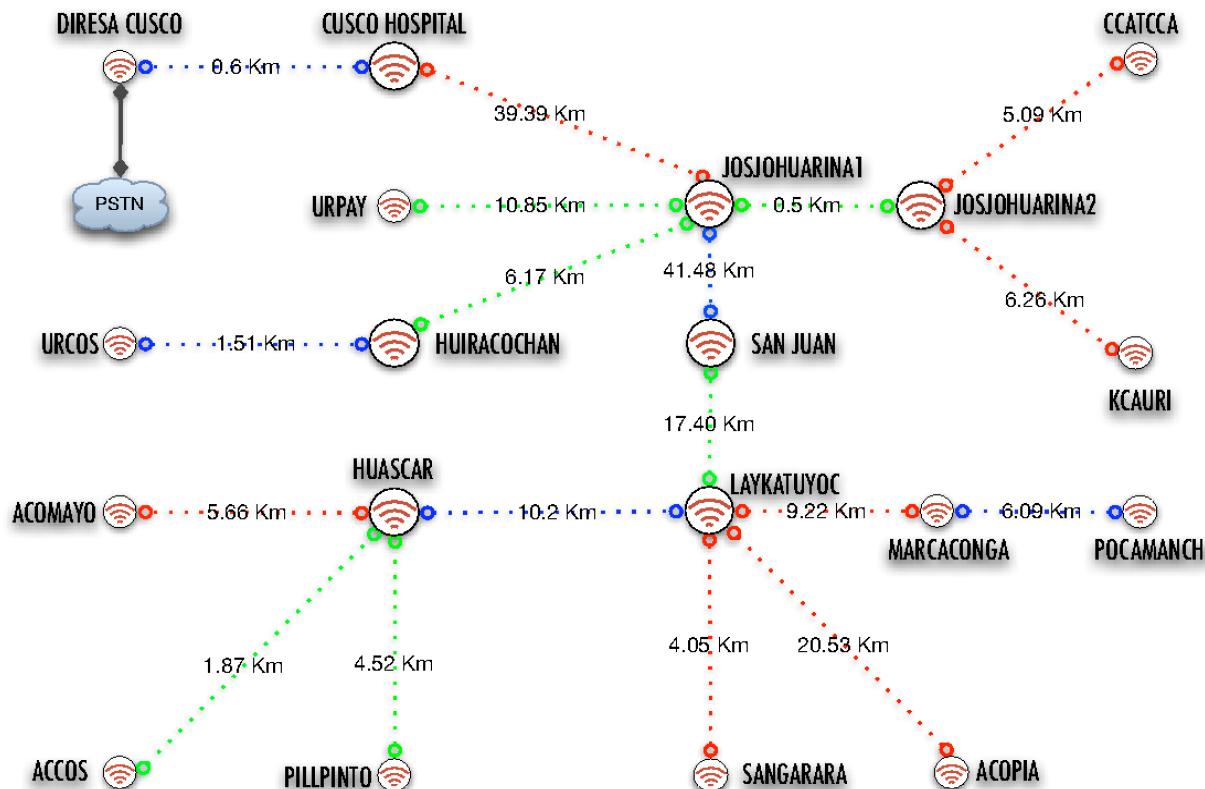
- Portátiles
- Desktops
- PDAs
- Redes remotas (bridging)

# Introducción a WiFi



# Introducción a WiFi. WiLD

WiLD = WiFi for Long Distances



# *Introducción a WiFi. WiLD*



## **Enlaces PtP largos experimentales:**

- SSC (Suecia): ~ 300Km. ULA(Venezuela): ~ 289Km. WUU (USA): ~ 132Km. EHAS (Colombia): ~ 87Km
- En los reportes de enlaces ajenos se informa de su factibilidad, pero no de las prestaciones alcanzadas.
- En nuestro enlace de 87 Km de EHAS en Colombia se analizan problemas con largas distancias: primera publicación científica sobre el tema en CITA'06.
- Mérida, Venezuela (2007): E. Pietrosémoli logra un enlace terrestre de 382 Km



# ***Introducción a WiFi. WiLD***

## **Algunas experiencias reales de aplicación en red:**

- Redes EHAS en Amazonía y en Los Andes (Perú, Colombia)
- Airjaldi, en el Himalaya (India)
- Reciente red de telemedicina en Malawi
- Red académica de Mérida (Venezuela)
- Digital Gangetic Plains (India)
- Guifinet, en Cataluña (España)
- Testbeds experimentales (TIER, RoofNET-MIT, ...)

# *Introducción a WiFi.*

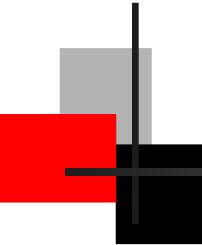
## **WiLD - Airjaldi**



*airJaldi*

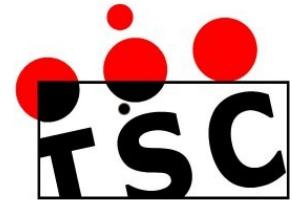
*Empowering communities through wireless networks*





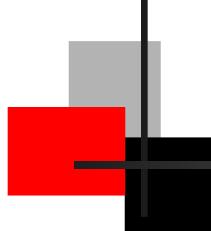
# **Introducción a WiFi.**

## **WiLD - Airjaldi**



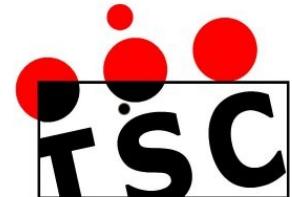
### **Dharamsala Wireless-Mesh Community Network (Feb 2005)**

- Backbone mesh de más de 30 nodos compartiendo mismo canal.
- Unos 2,000 ordenadores conectados compartiendo 6Mbps.
- Cada nodo mesh es un Himalayan-Mesh-Router (<4W)
- Antenas 8 - 11dBi omni, 12 – 24dBi directional, sectoriales, ...
- Acceso a Internet, intranet y telefonía VoIP (entrante).
- Canal mesh encriptado WPA, escondido y reservado para el backbone. Acceso por APs seleccionados.



# ***Introducción a WiFi.***

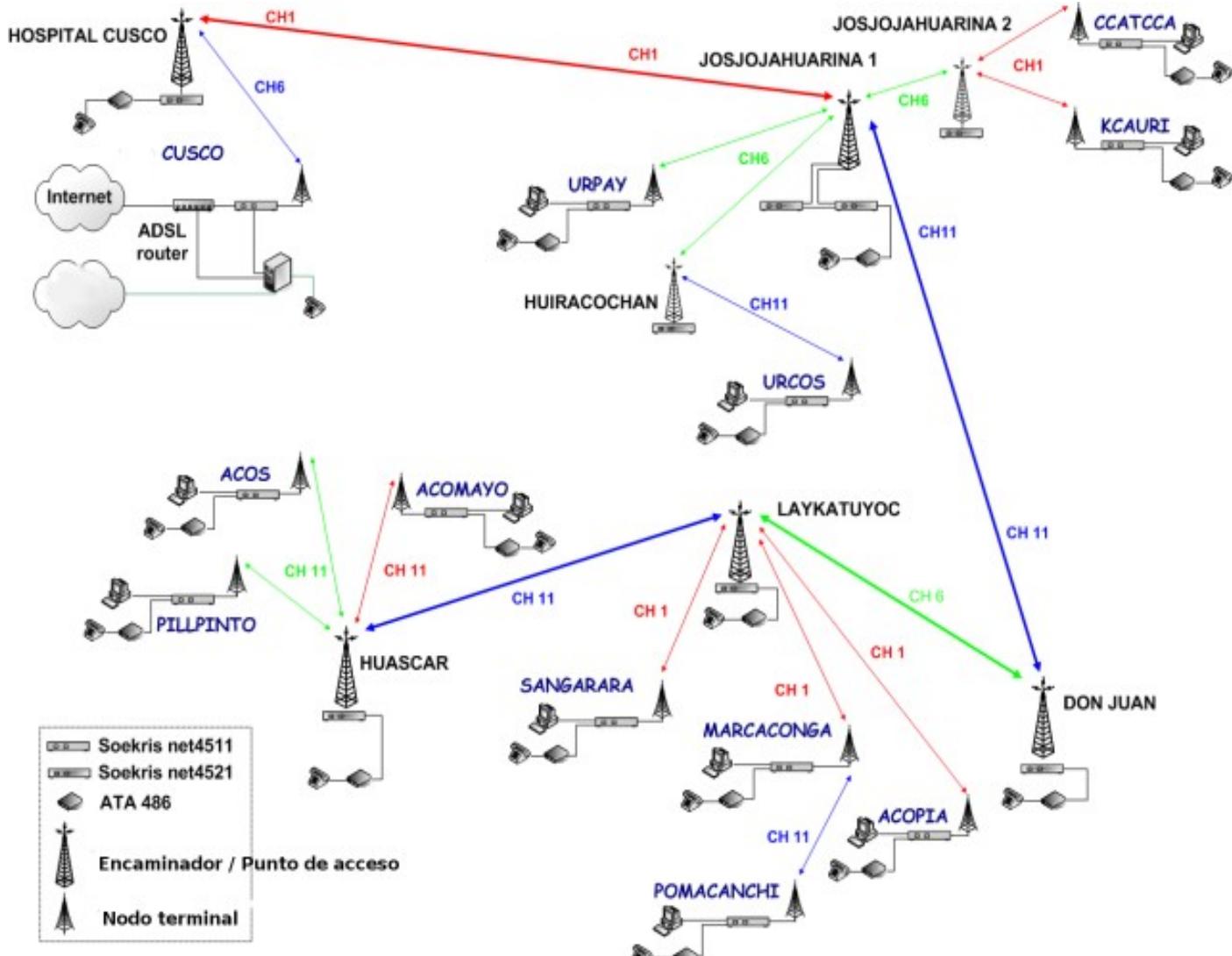
## **WiLD - CuzcoSur**



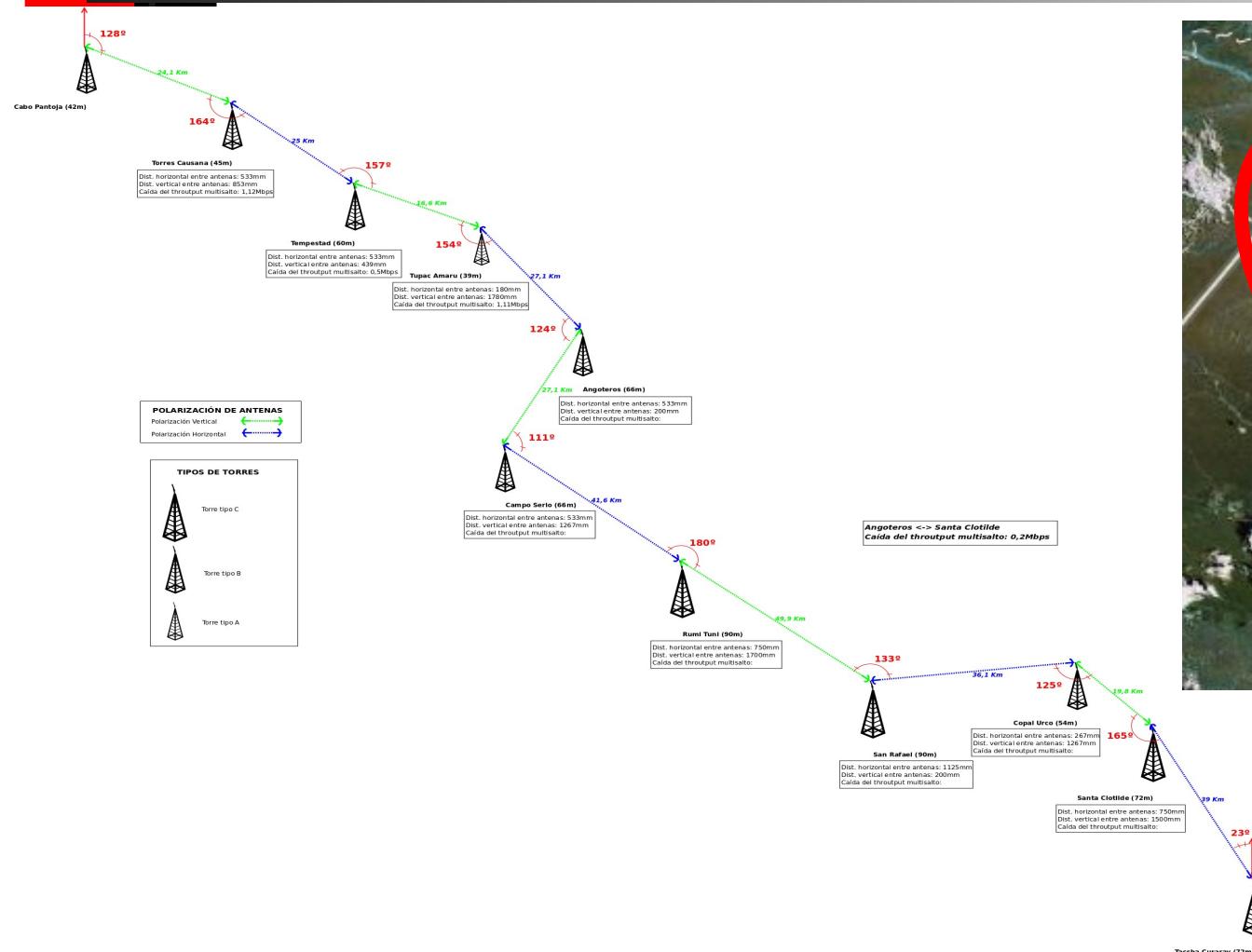
### **Red CuzcoSur (Feb 2006)**

- 18 nodos entre backbone + puestos. Canales no solapados para enlaces del backbone
- Puestos con ordenador y teléfono IP
- Cada nodo mesh es un EHAS-Router (<8W)
- Antenas 12 – 24dBi direccionales, sectoriales, ...
- Acceso a Internet, intranet y telefonía VoIP (entrante).
- Canal mesh encriptado WEP.

# Introducción a WiFi. WiLD - CuzcoSur

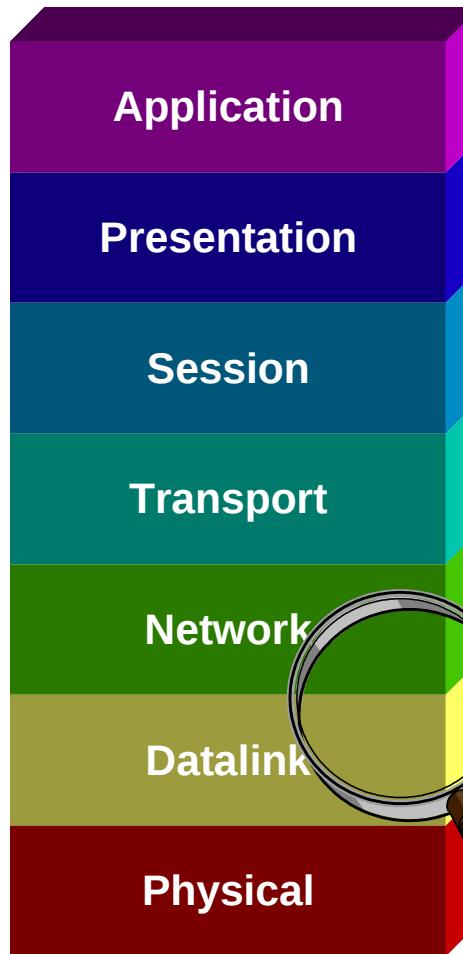


# Introducción a WiFi. WiLD - Pamafro/Napo



# Estándares IEEE 802.11

## El modelo OSI y WLAN



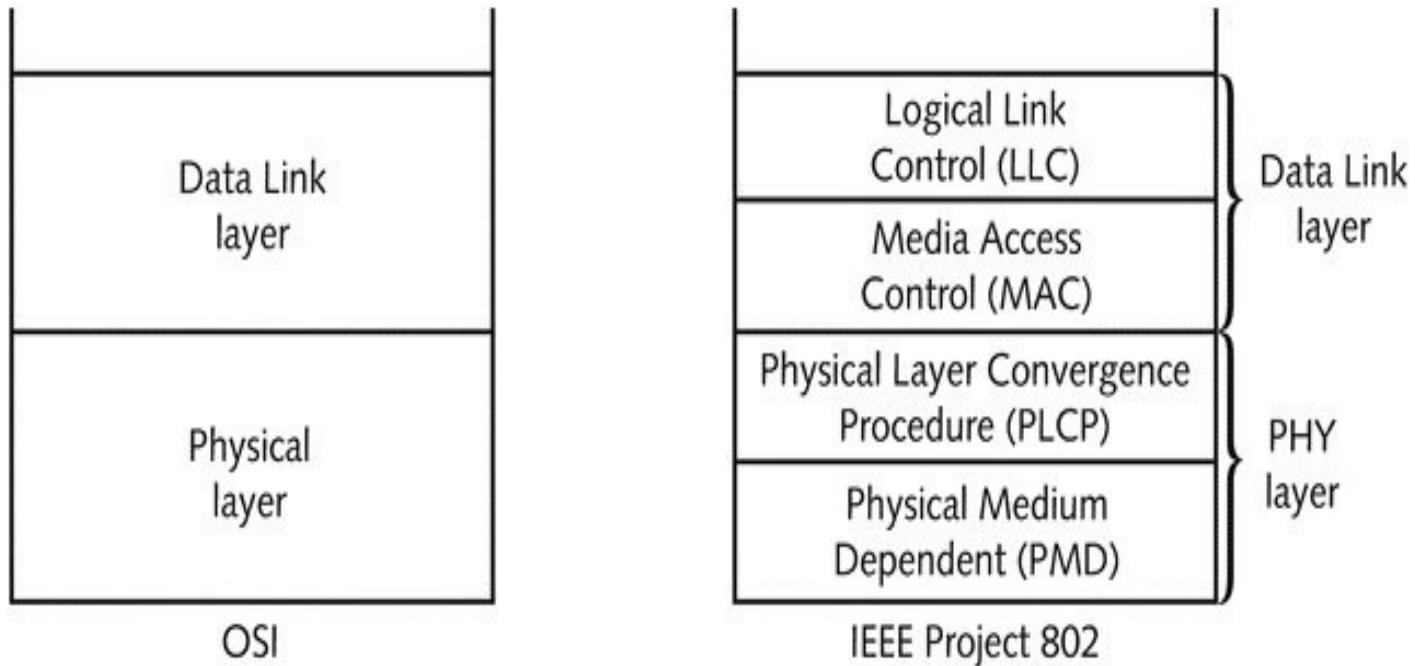
**Características principales de enlaces radio**

- El enlace radio tiene errores
- El enlace radio no siempre está disponible
- Problemas de seguridad
- Encaminamiento del tráfico a través del AP



# Estándares IEEE 802.11

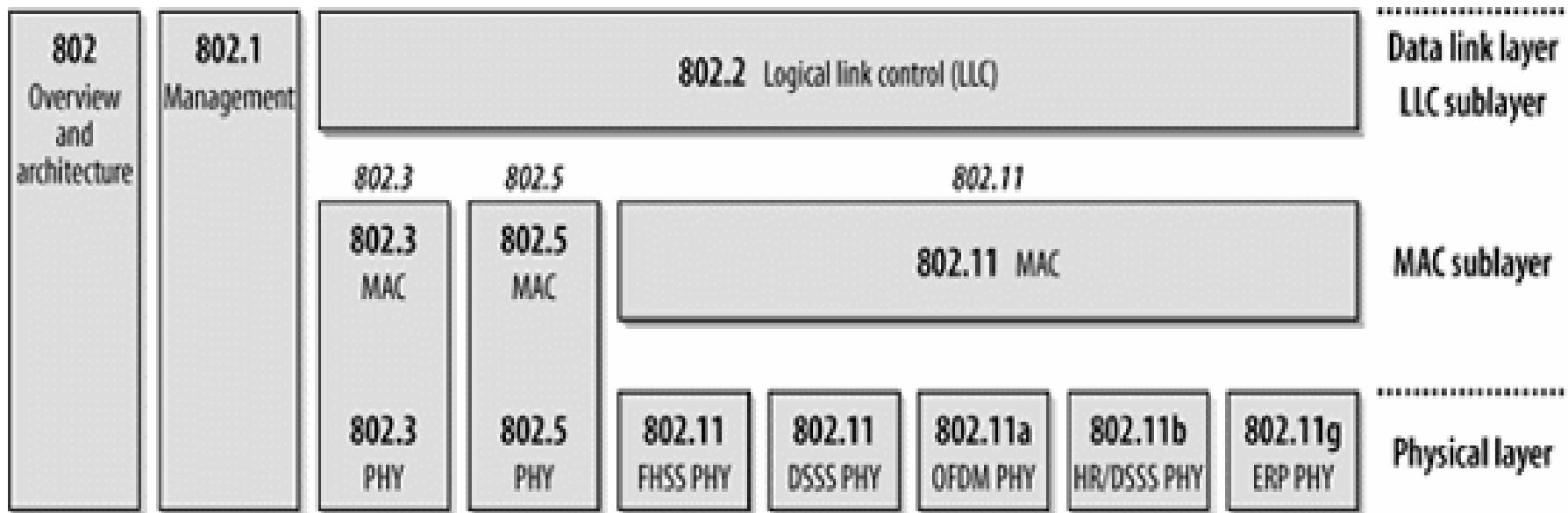
## El modelo OSI y WLAN





# Estándares IEEE 802.11

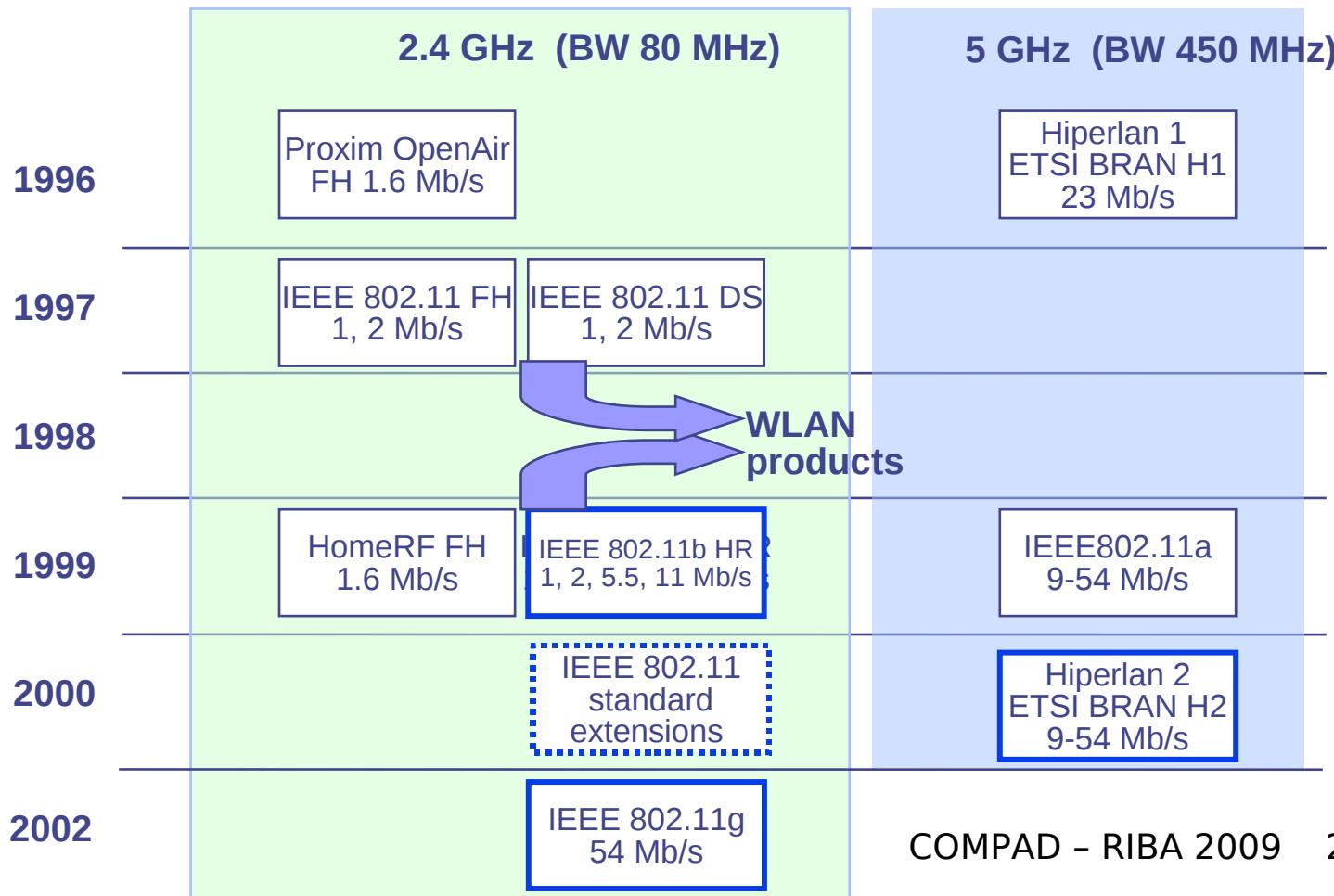
## Estándares IEEE 802



# Estándares IEEE 802.11



## Evolución de Estándares WLAN





# Estándares IEEE 802.11

## Evolución de estándares WLAN

- 1997 : se publica IEEE 802.11 para especificar WLAN
  - 1 capa MAC basada en CSMA/CA
  - 3 posibles capas físicas, velocidades 1 y 2 Mbps:
    - Infrarrojos (IR)
    - Espectro ensanchado por salto de frecuencia (FHSS)
    - Espectro ensanchado por secuencia directa (DSSS)  
y velocidades de 1 y 2 Mbps.
- Desde 1997 hasta hoy: extensiones y recomendaciones para aumentar velocidad, seguridad, alcance y prestaciones



# Estándares IEEE 802.11

## Evolución de Estándares WLAN

- IEEE802.11a – Banda de 5GHz, hasta 54 Mbps
- IEEE802.11b – Banda de 2,4GHz, hasta 11 Mbps.
- IEEE802.11c – Puentes inalámbricos con 802.11.
- IEEE802.11d – Armonización de 802.11 en los distintos países.
- IEEE802.11e – Soporte de QoS.
- IEEE802.11f – Interoperabilidad de AP. Define el protocolo IAPP.
- IEEE802.11g – Banda de 2,4GHz, hasta los 54 Mbps.
- IEEE802.11h – Adaptación de 11a a regulación europea.
- IEEE802.11i – Seguridad en las redes Wi-Fi.
- IEEE802.11j – Extensiones para Japón.



# Estándares IEEE 802.11

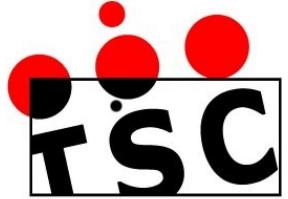
- IEEE802.11k (e.d.) – Intercambio de información de capacidad
- IEEE802.11m (e.d.) – Mantenimiento, actualizaciones.
- IEEE802.11n (e.d.) – MIMO, más de 100 Mbps.
- IEEE802.11p (e.d.) – Para ambulancias y coches de pasajeros.
- IEEE802.11r (e.d.) – “Roaming” rápido.
- IEEE802.11s (e.d.) – Redes Mesh.
- IEEE802.11T (e.d.) – WPP (métodos de testeo y métricas).
- IEEE802.11u (e.d.) – Interconexión con redes no-802.
- IEEE802.11v (e.d.) – Gestión de redes inalámbricas.
- IEEE802.11w (e.d.) – Tramas de gestión protegidas.
- IEEE802.11y (e.d.) – Extensión para USA.



# *La capa física. Introducción*

## Funciones

- Proporciona servicios a la capa MAC para intercambiar tramas
- Intercambia tramas con el PHY remoto empleando diversos mecanismos de modulación y codificación
- Da a la capa MAC un servicio de detección de canal ocupado



# *La capa física. Introducción*

## Arquitectura

- PMD (Physical Medium Dependent): Medios reales para Tx/Rx en medio físico. Detección de canal libre (CCA)
- PLCP (Physical Layer Convergence Procedure): Proporciona al MAC una interfaz única e independiente del PMD concreto.



# *La capa física. Enlace radio*

## Evolución

- 802.11 (1997) especificó 3 PHYs, a 1 o 2 Mbps:
  - IR: Infrarrojos (en desuso).
  - DSSS: Espectro ensanchado por secuencia directa (la opción ganadora), 2.4 GHz.
  - FHSS: E. E. por salto de frecuencia. 2.4 GHz (obsoleto).
- 802.11a (1999) añade otro PHY: OFDM en 5 GHz. 6 – 54 Mbps.
- 802.11b (1999) especifica HR/DSSS en 2.4 GHz; 5.5 u 11 Mbps.
- 802.11g (2003) describe ERP (Extended Rate PHY), incluye anteriores, todo en 2.4 GHz
- 802.11n (2010) introduce MIMO y velocidades de cientos de Mbps



# *La capa física. Enlace radio*

## Resumen PHY “activos”

<i>Estándar</i>	<i>Frecuencia</i>	<i>Canales no interferentes</i>	<i>Modulaciones</i>	<i>Velocidad de transmisión</i>
802.11	2,4 GHz	3	DSSS	1 y 2 Mbps
802.11b	2,4 GHz	3	HR/DSSS	5,5 y 11 Mbps
802.11g	2,4 GHz	3	DSSS/OFDM	54 Mbps
802.11a	5,8 GHz	8	OFDM	54 Mbps

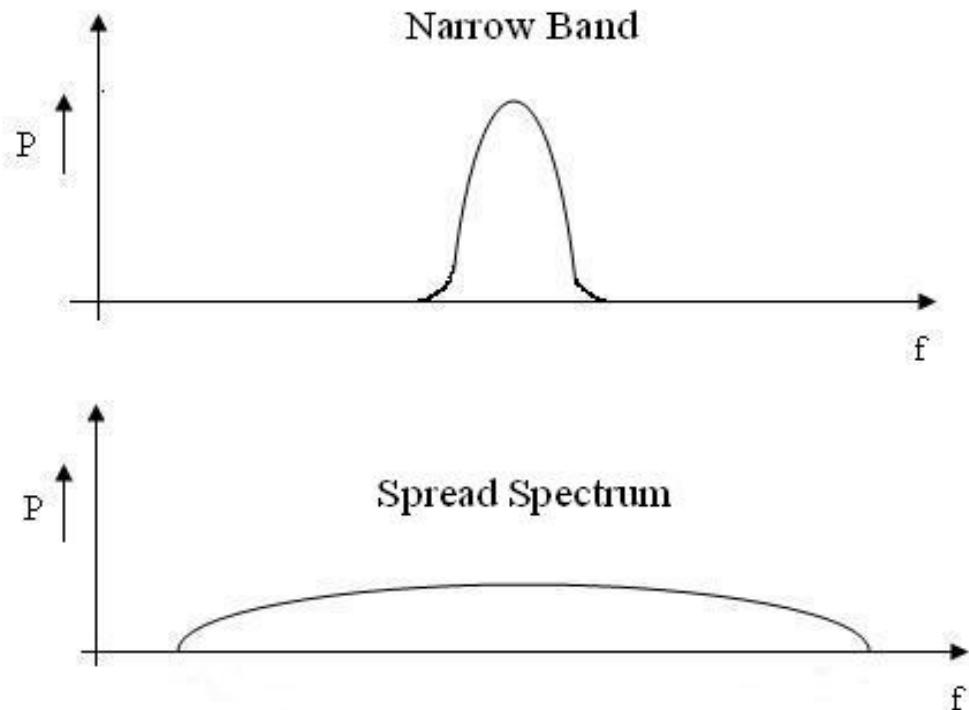
# *La capa física. Espectro ensanchado*

## Fundamentos

- Utiliza todo el ancho de banda disponible
- Ventajas
  - Inmunidad ante interferencias
  - Encriptación
- Dos clases de tecnología
  - FHSS: Espectro ensanchado por salto en frecuencia
  - DSSS: Espectro ensanchado de secuencia directa

## Fundamentos

- Difumina la señal en un espectro muy ancho mediante funciones matemáticas
- El receptor realiza la operación inversa, lo que ensalza la señal y reduce el efecto del ruido de banda estrecha
- Cualquier receptor de banda estrecha oiría ruido de baja intensidad



## *La capa física. Espectro ensanchado*

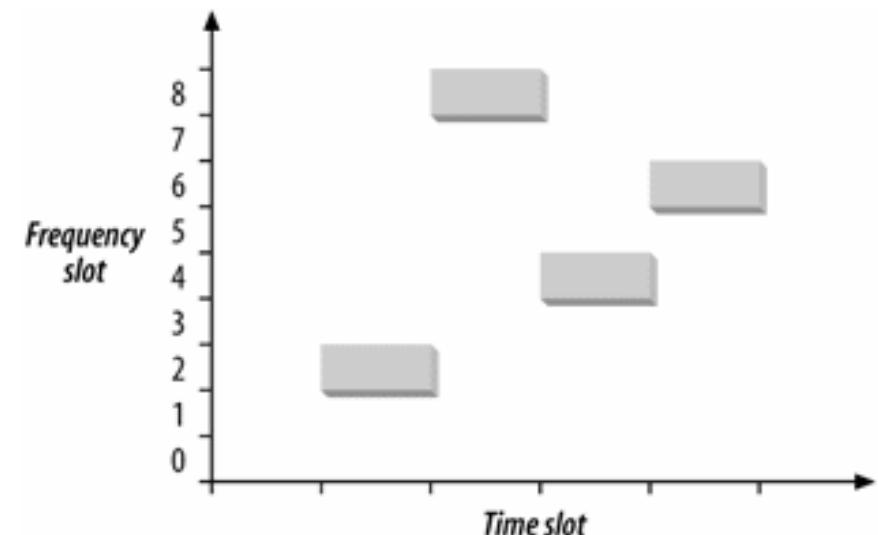
- Los atípicos inventores del espectro ensanchado y el salto de frecuencias (la actriz Hedy Lamarr y el músico George Antheil)



# *La capa física. Distintos PHY*

## FHSS

- Tx en una frecuencia durante un intervalo de tiempo.
- Pasado este tiempo se cambia la frecuencia y se sigue transmitiendo en otra.
- Orden de saltos según secuencia pseudoaleatoria conocida por el emisor y el receptor.
- Banda ISM 2.4GHz (ISM):
  - 79 canales de 1MHz cada uno.
  - Modulación GFSK
  - Velocidades de 1Mbps (2-GFSK) ó 2 Mbps (4-GFSK)

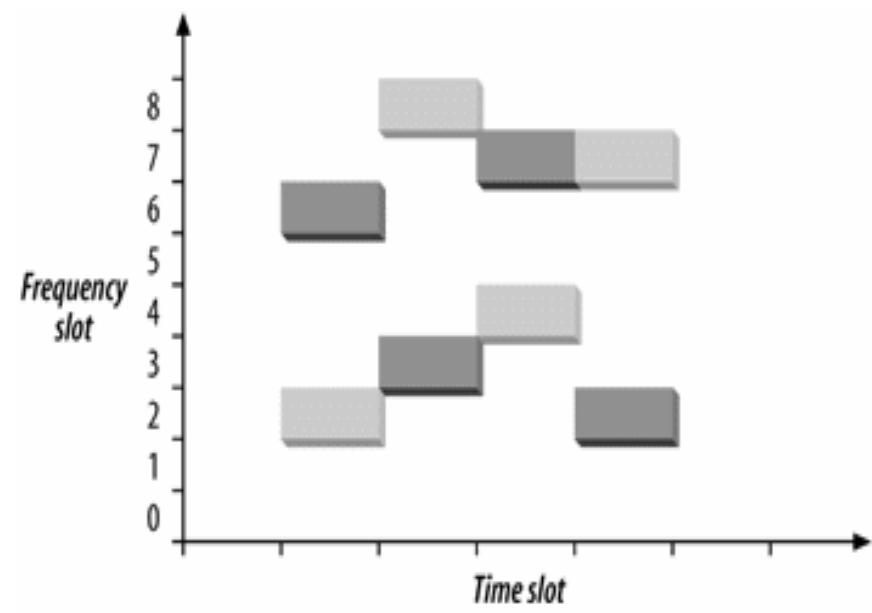
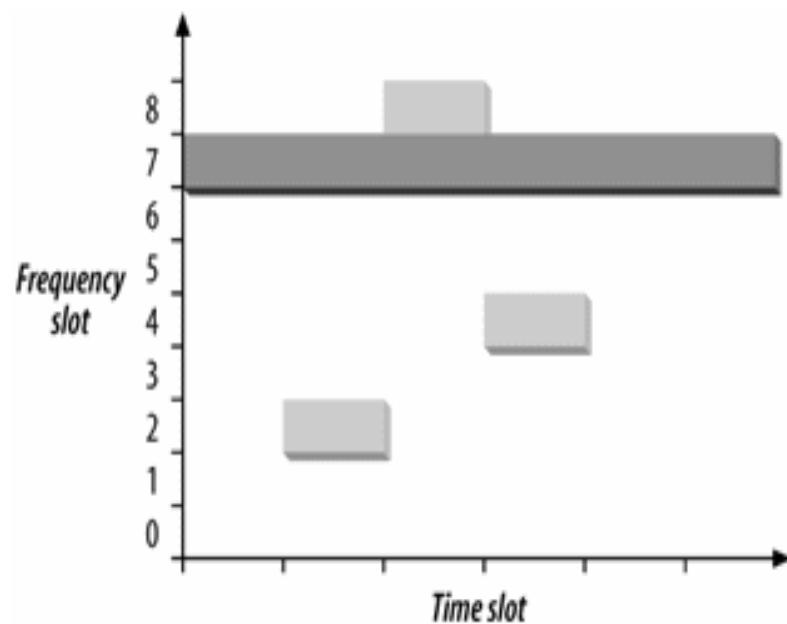


## *La capa física. Distintos PHY*

FHSS

Ruido de banda estrecha

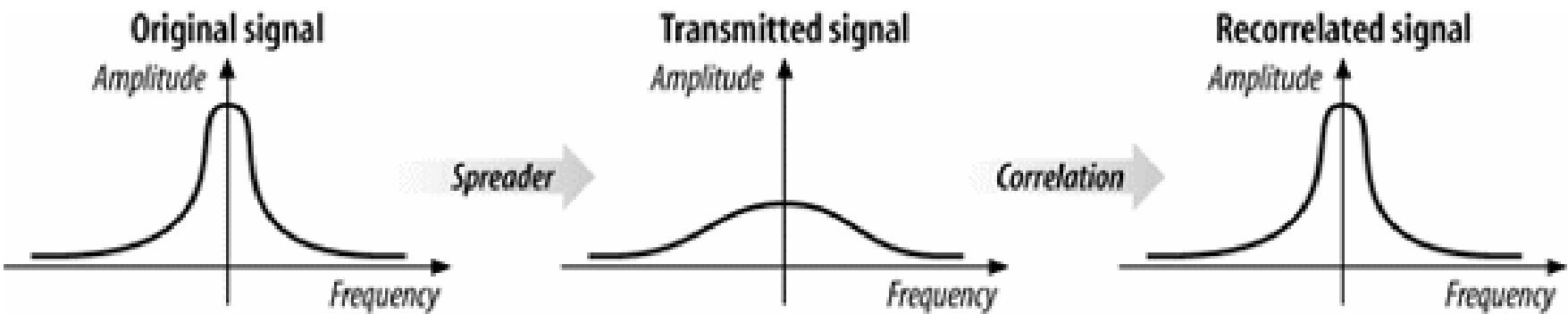
Secuencias de salto ortogonales



# La capa física. Distintos PHY

## DSSS

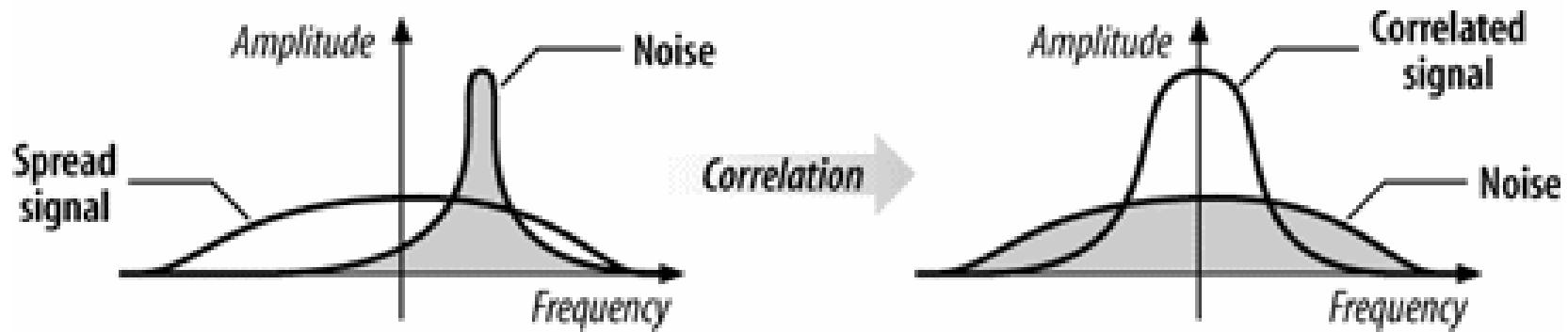
- En transmisión se reparte la potencia RF sobre una banda ancha mediante transformación matemática.
- En recepción, una función de correlación permite recuperar la señal



## *La capa física. Distintos PHY*

### DSSS

- La correlación en recepción logra eliminar interferencias y minimizar el efecto del ruido.



## *La capa física. Distintos PHY*

### DSSS

- El ensanchamiento en Tx se realiza con un flujo de chips ≡ bits producidos según una secuencia llamada código pseudo-aleatorio de ruido (código PN).
- El número de chips usados para transmitir un solo bit se llama “tasa de ensanchamiento”.
- 802.11 usa como código PN una palabra Barker de 11 bits por sus propiedades de autocorrelación.
- Modulación DBPSK (1Mbps) o DQPSK (2Mbps) con velocidad de chip de 1 Millón de palabras Barker por segundo (11Mchips/s)

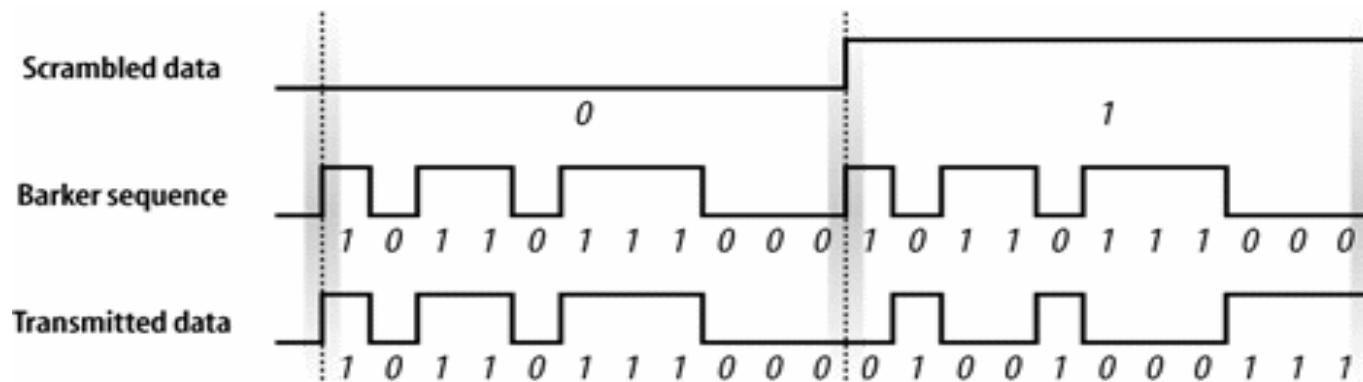
# *La capa física. Distintos PHY*

## DSSS

- Chipping:



- Codificación con palabra Barker



# *La capa física. Distintos PHY*

DSSS

*Dominio regulatorio*

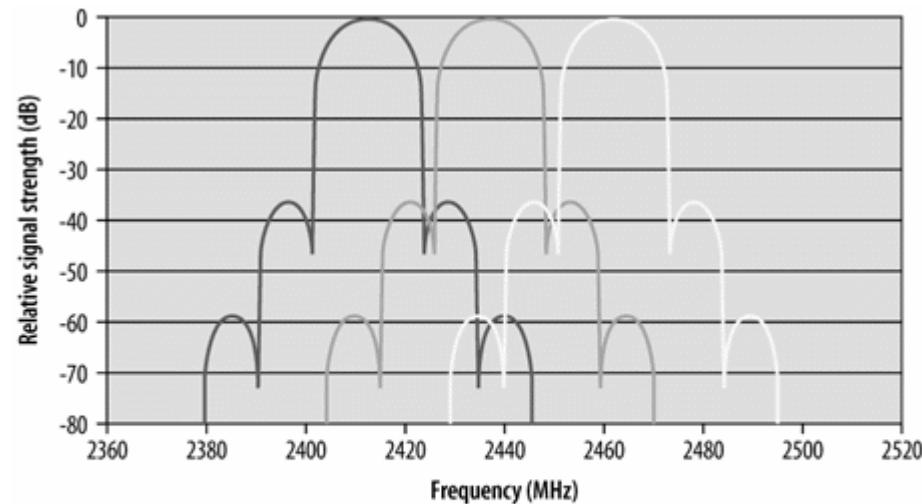
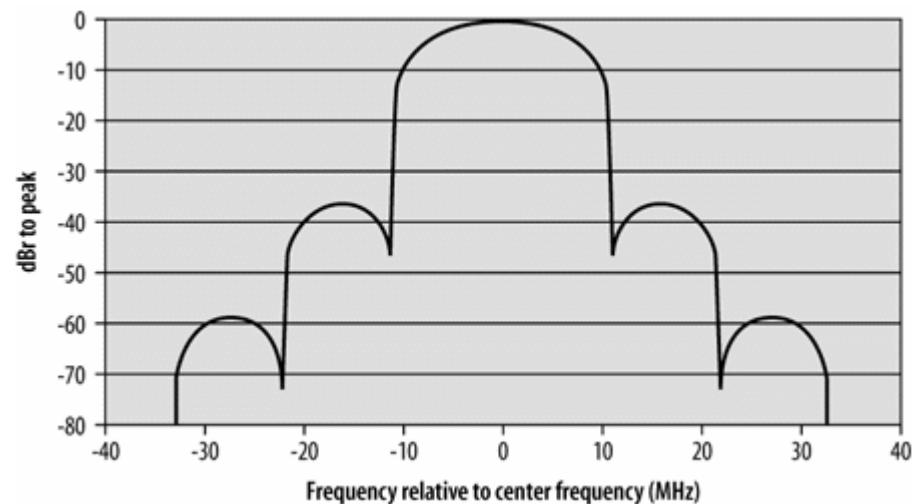
U.S. (FCC)/Canadá (IC)

Europa (ETSI)

*Canales permitidos*

1 a 11 (2.412-2.462 GHz)

1 a 13 (2.412-2.472 GHz)



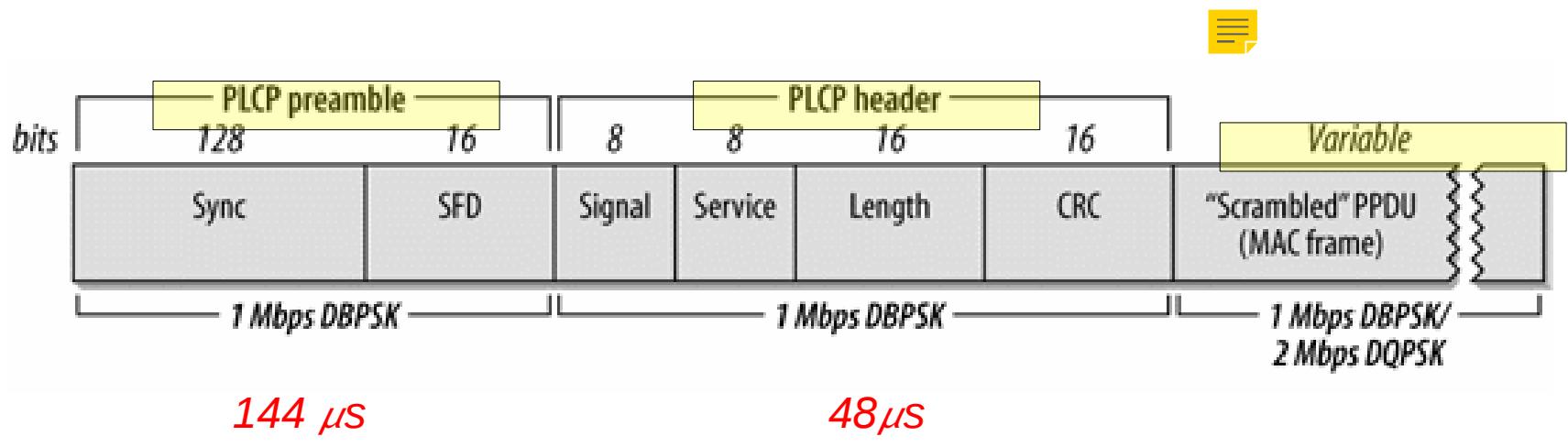
**KEY**

—	Channel 1	—	Channel 11
—	Channel 6	—	

# *La capa física. Distintos PHY*

DSSS: PHY triunfante del estándar original.

Formato de trama PLCP:

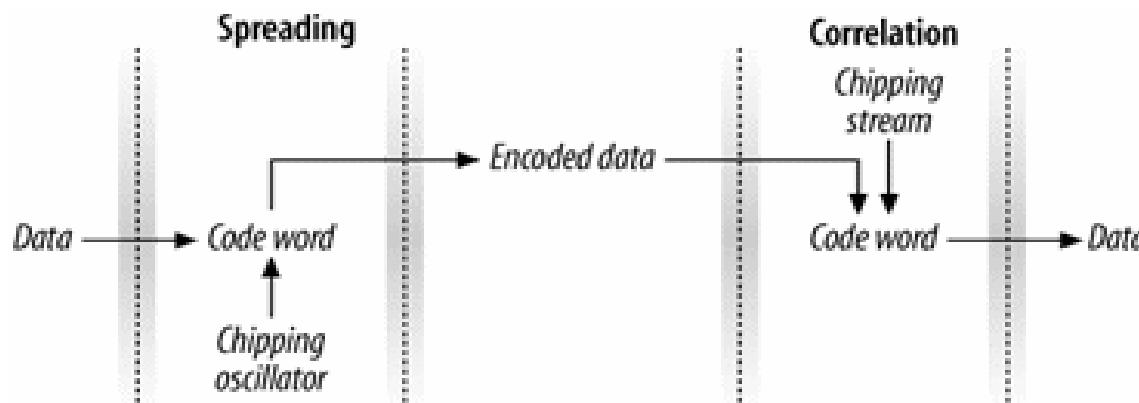


*Overhead PLCP total: 192  $\mu$ s*

# La capa física. Distintos PHY

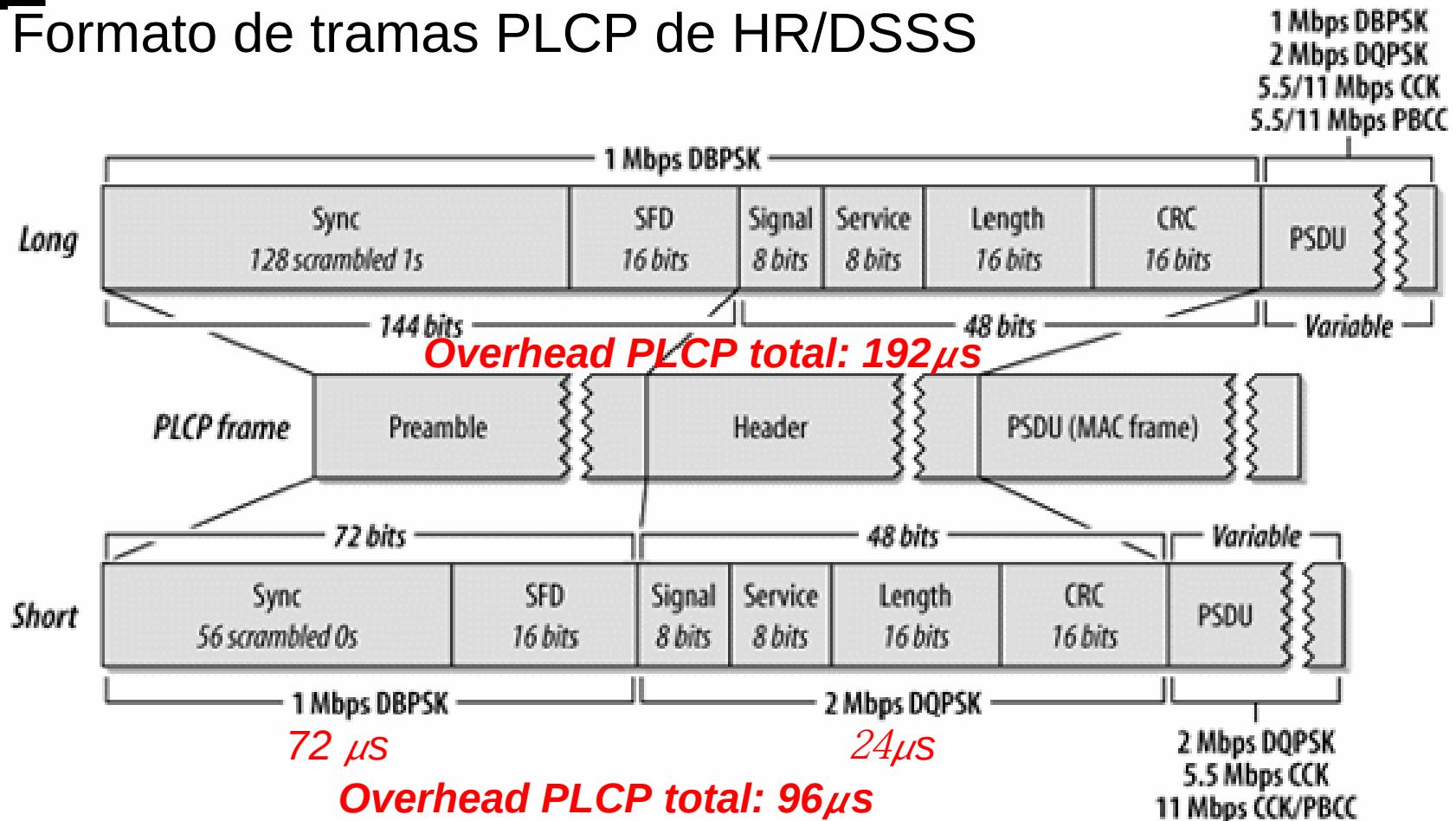
## HR/DSSS (introducido en IEEE 802.11b)

- Añade a DSSS nuevas modulaciones mediante CCK (Complementary Code Keying), logrando velocidades mayores.
- Aplicando transformaciones matemáticas logra codificar 4 u 8 por símbolo.



# La capa física. Distintos PHY

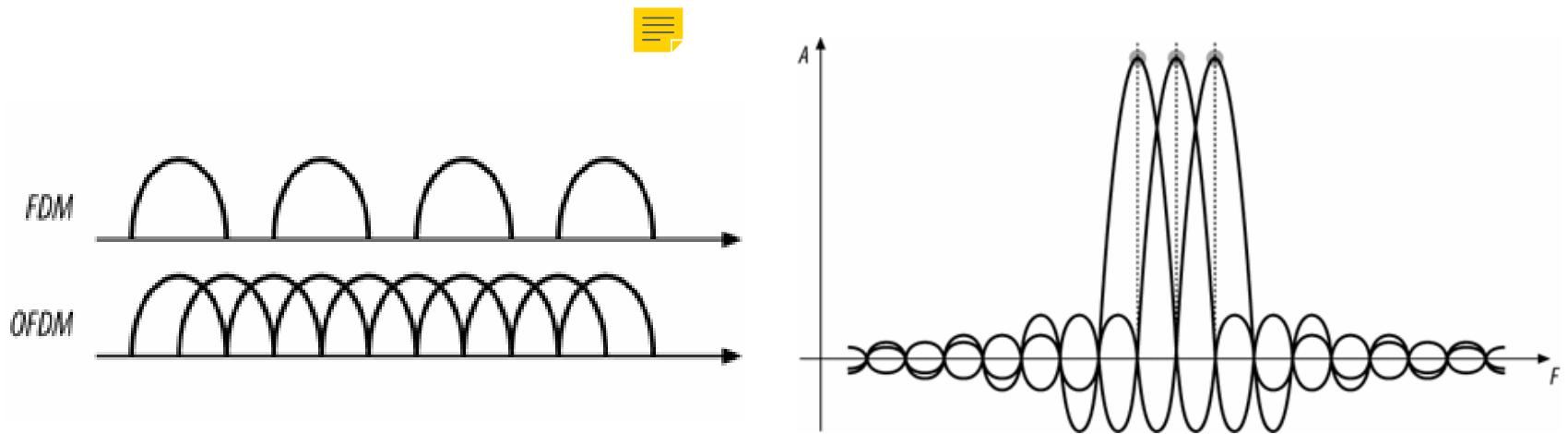
## Formato de tramas PLCP de HR/DSSS



# *La capa física. Distintos PHY*

## OFDM

- OFDM = Modulación por División en Frecuencias Ortogonales
- FDM en que se hace un uso más eficiente del espectro escogiendo frecuencias de portadoras contiguas ortogonales.
- En transmisión se usa IFFT, en recepción FFT





## *La capa física. Distintos PHY*

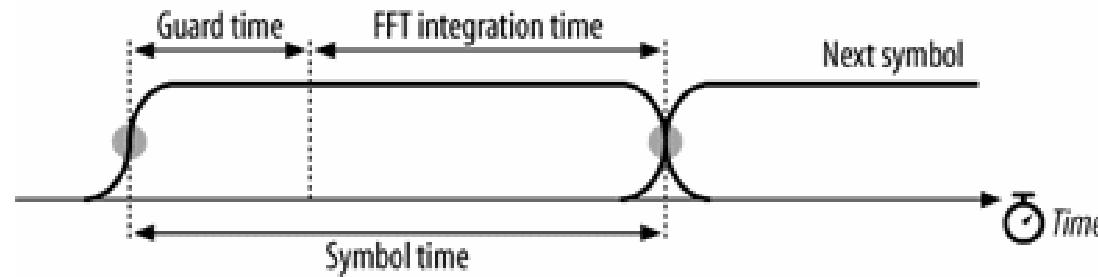
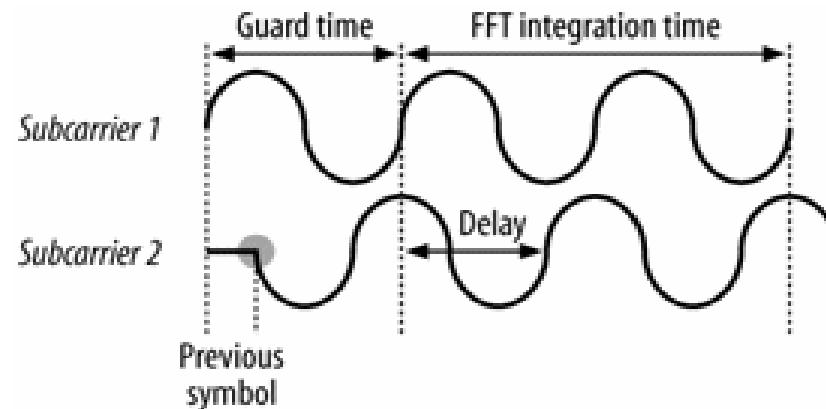
### OFDM

- Problemas de propagación
  - Debidos al multirayecto: ISI (interferencia intersimbólica)  
= interferencia entre copias del mismo símbolo que llegan con retardos distintos por haber seguido caminos diferentes.
  - Debidos al efecto Doppler o a la mala sincronización de relojes: ICI (interferencia interportadora) = invasión de la banda de una portadora por parte de portadoras vecinas.
- Solución: tiempo de guarda en cada símbolo, rellenado con prefijo cíclico.

# *La capa física. Distintos PHY*

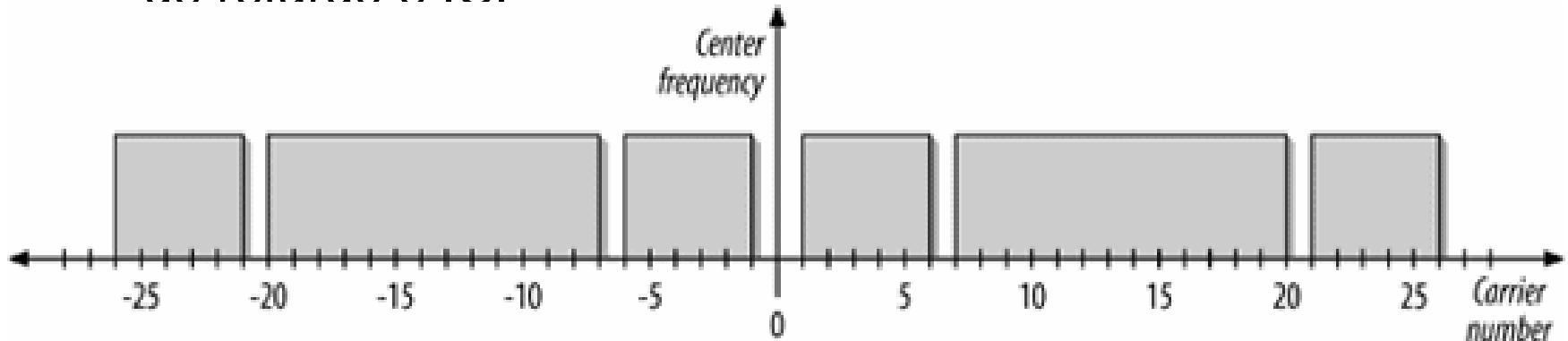
## OFDM (introducido en IEEE 802.11a)

- Tiempo de guarda



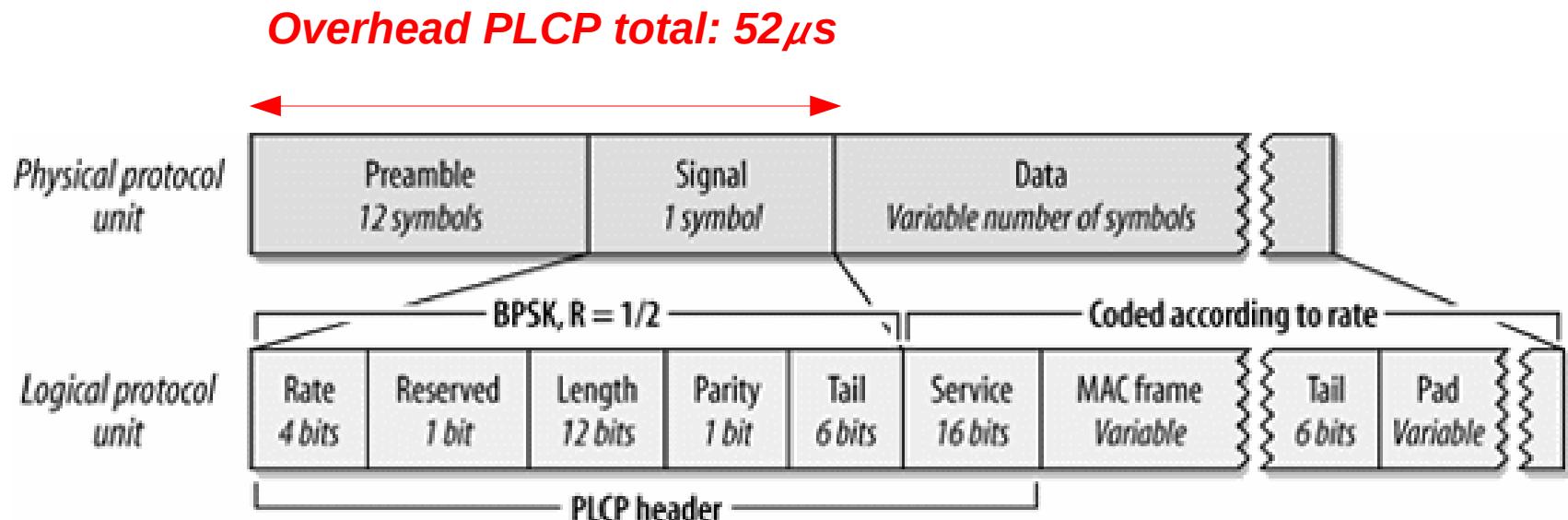
## ***La capa física. Distintos PHY***

- En 802.11a, el tiempo de guarda es de 800ns para soportar dispersión del retardo alta.
- Tiempo de símbolo  $4\mu s$  , tiempo de integración  $3.2\mu s$
- Canales de 20MHz, cada uno con 52 subportadoras
  - 48 son de datos. Entrelazado: bits consecutivos en portadoras separadas ampliamente y símbolos distintos en constelación
  - 4 (-21, -7, 7, 21) son pilotos para monitorizar desplazamientos de retardo e ICI



## *La capa física. Distintos PHY*

- ◆ Formato de tramas PLCP OFDM 5GHz (802.11a)



## *La capa física. Distintos PHY*

### ERP

- Incorpora compatibilidad hacia atrás con 11b con DSSS, y las velocidades de 11a con OFDM, todo ello en 2.4 GHz 
- El PHY ERP (Extended Rate PHY) es en realidad un paraguas que incluye:
  - **ERP-DSSS y ERP-CCK:** Modos de 802.11 y (1 Mbps y 2 Mbps) y de 802.11b (5.5 Mbps y 11 Mbps).
  - **ERP-OFDM:** Redefinición de 802.11a en 2.4 GHz (6, 9, 12, 18, 24, 36, 48 y 54 Mbps, siendo obligatorias 6, 12 y 24 Mbps).
  - **ERP-PBCC:** Opcional y poco usado. 22 Mbps y 33 Mbps.
  - **DSSS-OFDM:** Opcional y poco usado. Cabeceras DSSS + Datos OFDM.



## *La capa física. Distintos PHY*

### ERP. Convivencia con 802.11b

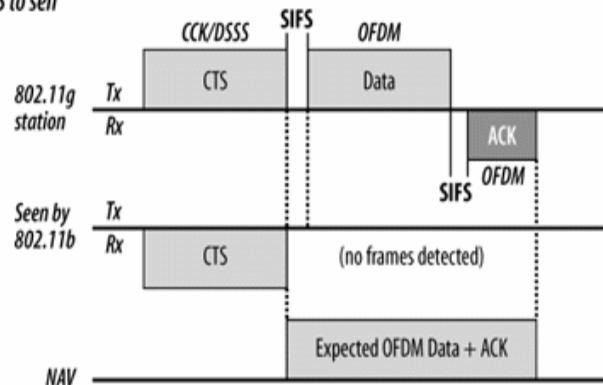
- Si en una red hay dispositivos 11b y 11g deben entenderse.
- Dos soluciones:
  - Los dispositivos 11g deben transmitir a la mayor tasa posible común a TODAS las estaciones aquellas tramas que deban ser entendidas por todas.
  - Protección: Uso de RTS/CTS o CTS-to-self para activar la detección de portadora virtual de estaciones 11b antes de transmitir en OFDM (reduce las prestaciones).
  - DSSS-OFDM y ERP-PBCC no requieren protección, es implícita.

# *La capa física. Distintos PHY*

## ERP. Convivencia con 802.11b

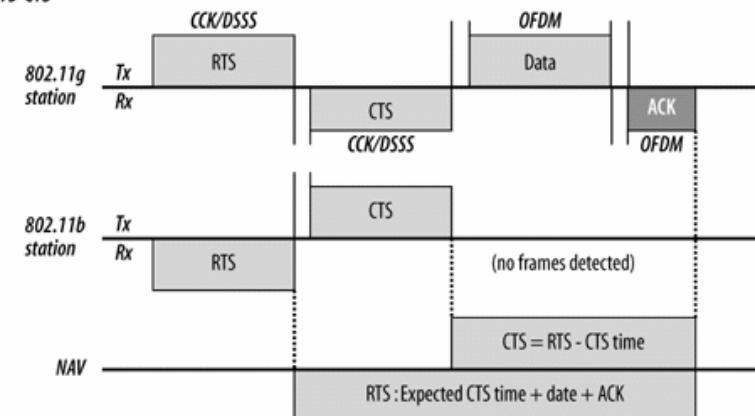
Protección con CTS-to-self

a) CTS to self



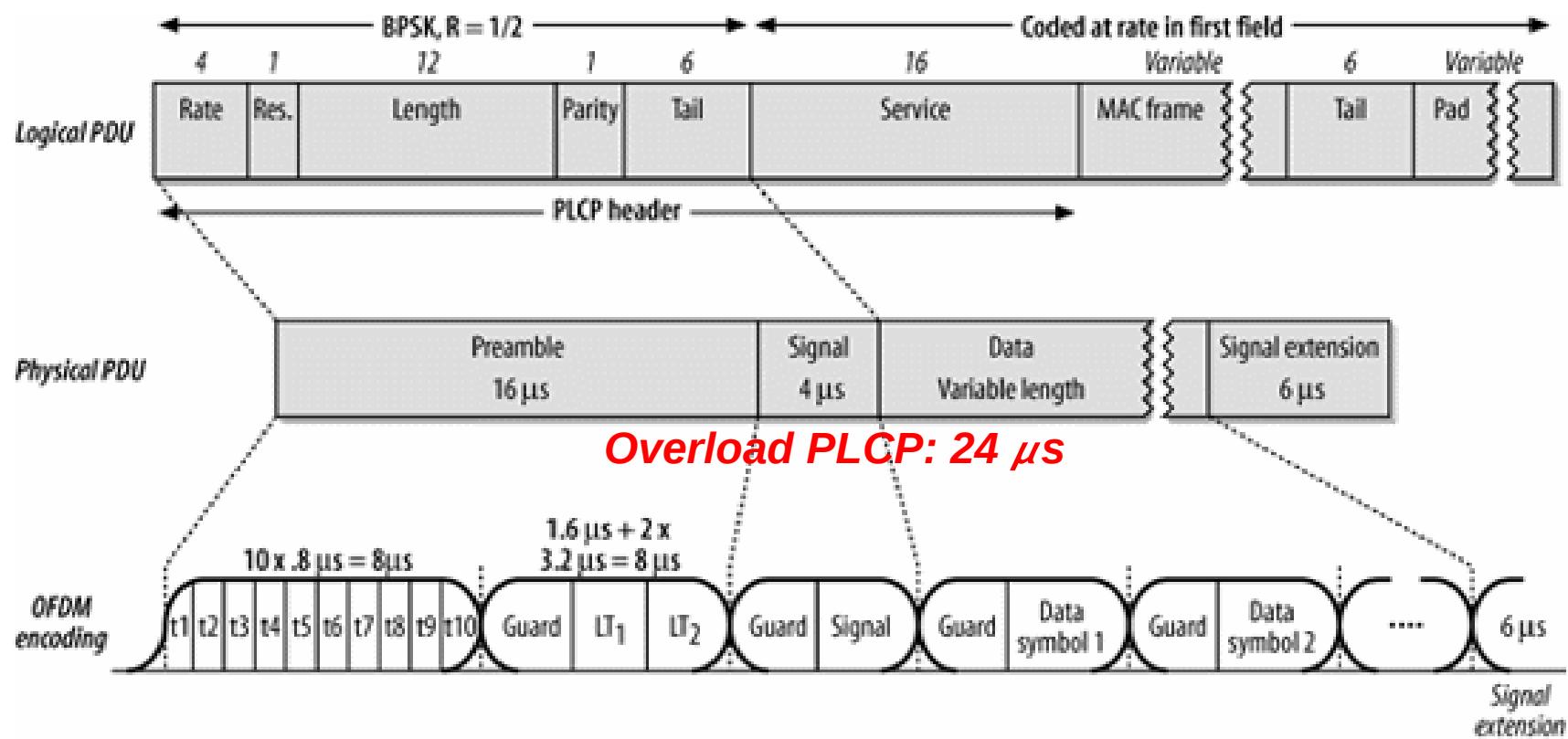
Protección con RTS/CTS

b) RTS-CTS



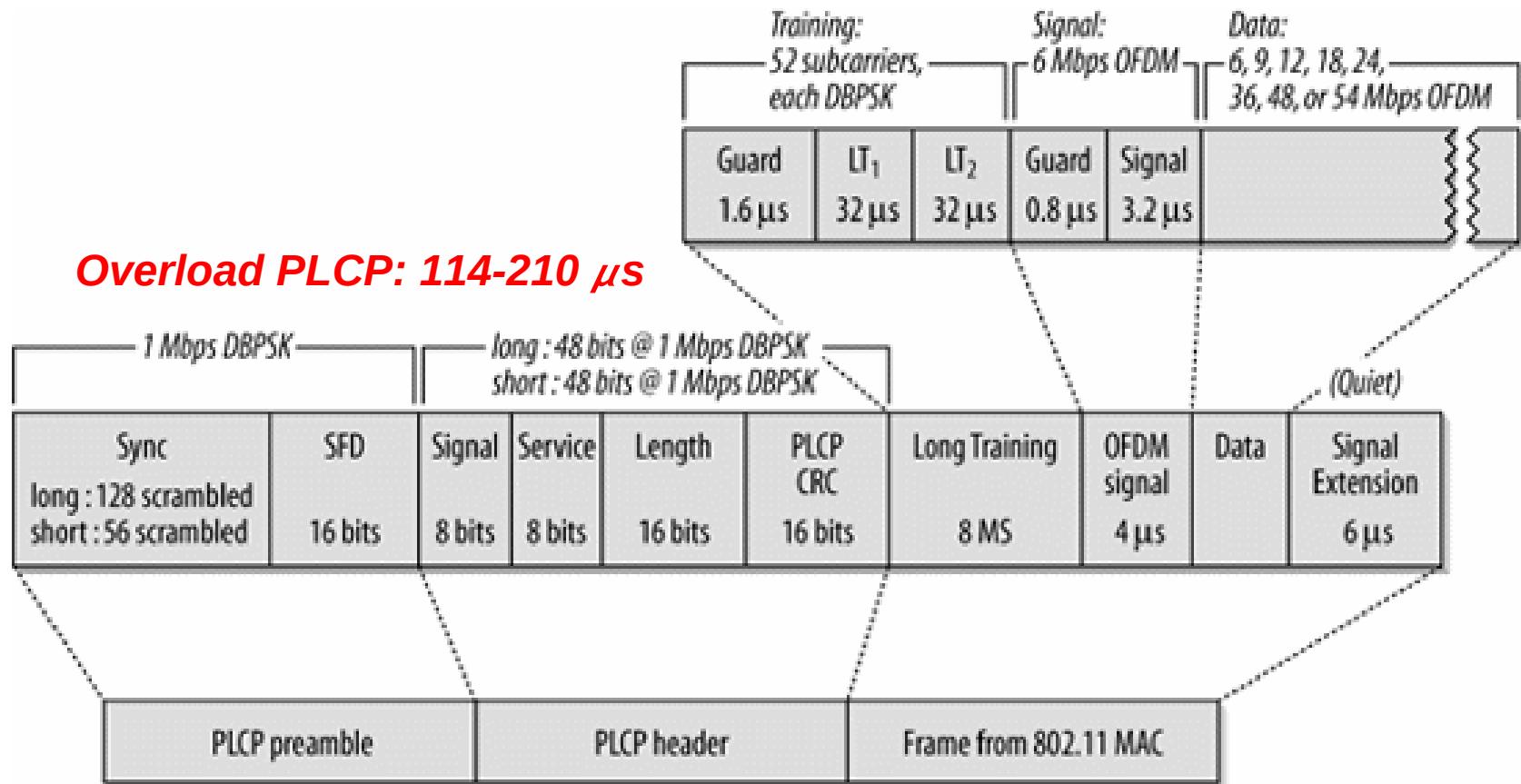
# La capa física. Distintos PHY

## Tramas PLCP ERP-OFDM



# La capa física. Distintos PHY

## Tramas PLCP DSSS-OFDM



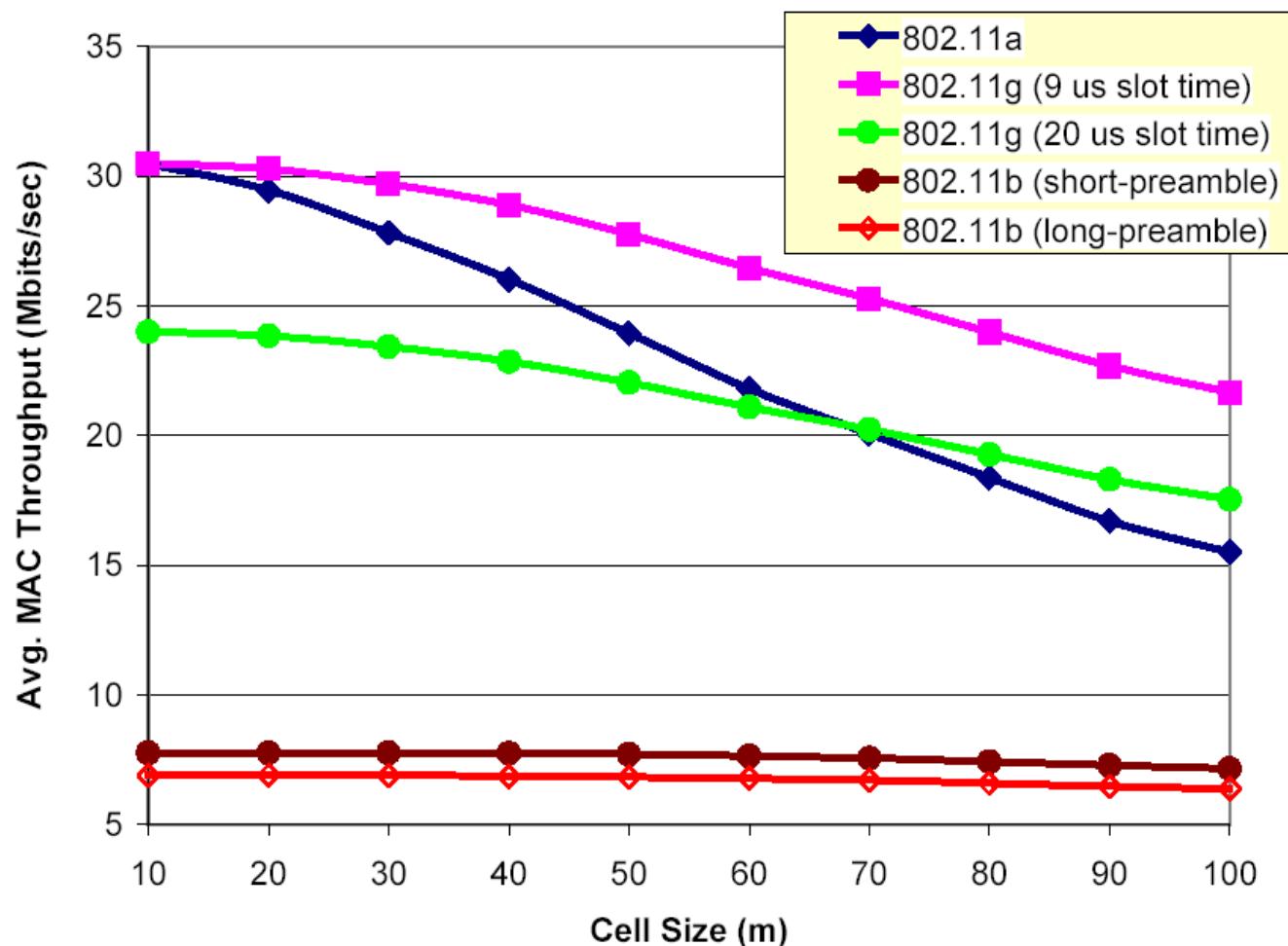


## *La capa física. Distintos PHY*

### 802.11n

- Objetivo: superar (con creces) 100Mbps de throughput neto.
- Se retrasó por la disputa entre dos grupos antagónicos, el WWISE y el Tgn-Sync. Finalmente constituyeron un único grupo EWC que sacó el Draft 2 en Enero de 2007. ~100 Mbps
- Estándar definitivo para 2010. Se esperan hasta 600 Mbps
- Se usa
  - MIMO (multiple-input multiple-output)
  - Bandas de 5 GHz y 2.4GHz simultáneamente.
  - Canales de 20MHz y 40 MHz.

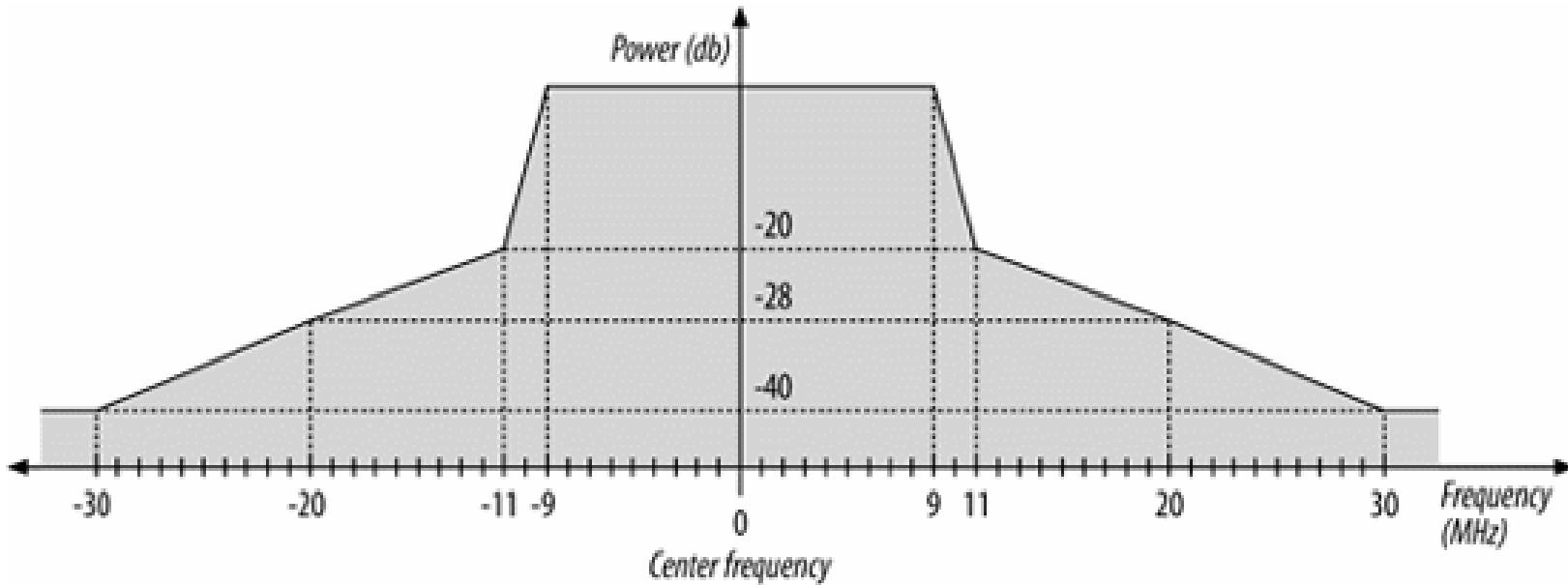
# *La capa física. Distintos PHY*



# ***La capa física. Distintos PHY***

## Observación sobre la especificación del canal

- El estándar impone una máscara
- Los transmisores están obligados a atenuar la señal fuera de banda según la máscara, pero algo de señal hay:  
**INTERFERENCIA POSIBLE CON CANALES ADJACENTES**

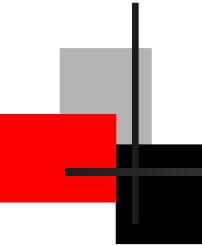




# ***La capa MAC. Introducción***

## Generalidades

- El objetivo del MAC es controlar el acceso al medio físico de la forma más eficiente posible
- Funciones:
  - Generación de trama MAC
  - Encaminamiento
  - Fragmentación / Reensamblado
  - Verificación de errores (por CRC)
  - Acceso al medio (CSMA / CA)
  - Movilidad de estaciones



# **La capa MAC. Introducción**



## Fundamento de CSMA/CA

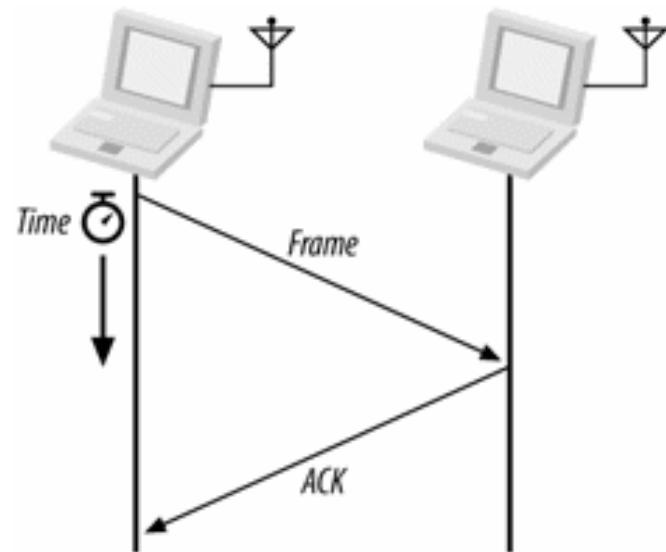


- CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance).
- Se escucha el canal para saber cuándo está libre.
- Al quedar libre el canal, se espera un tiempo aleatorio. Este tiempo es un número entero de *ranuras*.
- La ranura es una unidad de tiempo cuya duración está definida en el estándar para cada PHY (SlotTime).

# *La capa MAC. Introducción*

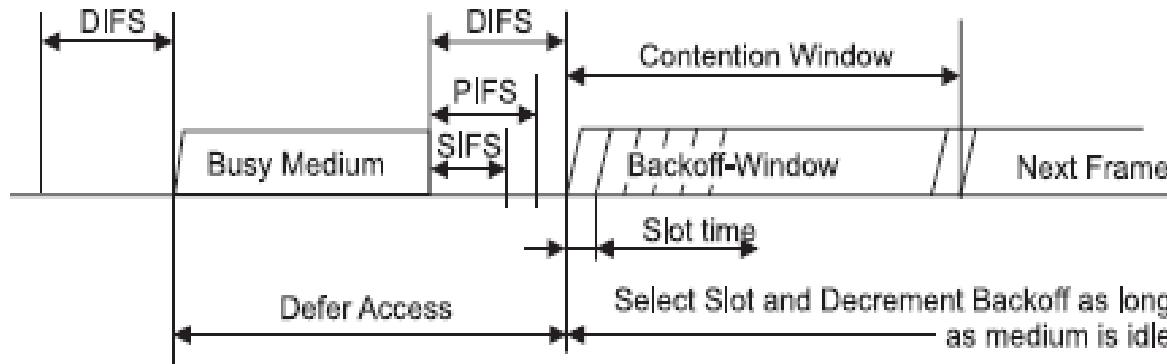
## Desafíos del MAC 802.11

- La calidad del enlace RF, fluctuante (ruido, interferencias, multirayecto...) requiere tramas de datos unicast confirmadas
- Los nodos ocultos, problema que se resuelve con un mecanismo llamado RTS/CTS



# La capa MAC. Temporización

## Definiciones



- **SlotTime**: tiempo de ranura. Las ranuras son intervalos de tiempo discretos en que se fracciona el tiempo de la ventana de contienda.
- **ACKTimeout**: tiempo que se espera por un ACK tras el envío de una trama de datos. Transcurrido ese tiempo, se retransmite o se abandona.

# ***La capa MAC. Temporización***

## Definiciones

- IFS (Inter Frame Space): tiempos de separación entre tramas
  - SIFS (Short IFS): separación entre el fin de la recepción de una trama de datos y su confirmación.
  - PIFS (PCF IFS): usado en el modo PCF (se verá más tarde). Es igual a SIFS+SlotTime.
  - DIFS (DCF IFS): usado en el modo DCF (se verá más tarde). Es igual a PIFS+SlotTime.
  - EIFS (Extended IFS): usado cuando se recibe una trama corrupta. Es igual al tiempo de transmisión de un ACK+SIFS+DIFS.



# La capa MAC. CSMA/CA

## Operación

- Se escucha el canal hasta que se escuche libre (detección de portadora real o virtual).
- Cuando el canal quede libre, se espera DIFS sin hacer nada.
- Si una vez transcurrido este tiempo el canal sigue libre, la STA inicia una nueva espera llamada ventana de contienda (**CW**, Contention Window), cuyo valor será un número aleatorio de veces el SlotTime.



## **La capa MAC. CSMA/CA**

### Operación

- Si durante la espera por la ventana de contención se detecta otra trama en el medio, se congela el temporizador y no se transmite ni se sigue la cuenta atrás.
- Una vez que el medio vuelve a quedar libre se espera nuevamente el tiempo DIFS y se reanuda la cuenta atrás de la CW donde se detuvo.
- Cuando la CW alcanza el valor cero, se transmite la trama.



# **La capa MAC. CSMA/CA**

## Operación

- Si dicha trama tenía un solo destinatario (unicast), la estación transmisora queda a la espera de recibir la correspondiente confirmación (ACK).
- El receptor recibe la trama y comprueba su CRC mientras espera un tiempo SIFS y luego envía la trama ACK para confirmar. Las tramas broadcast no se confirman en IEEE802.11, al igual que las multicast.
- Si el ACK se recibe correctamente y antes de ACKTimeout (y de que se reciba otra trama), se acaba.



# La capa MAC. CSMA/CA

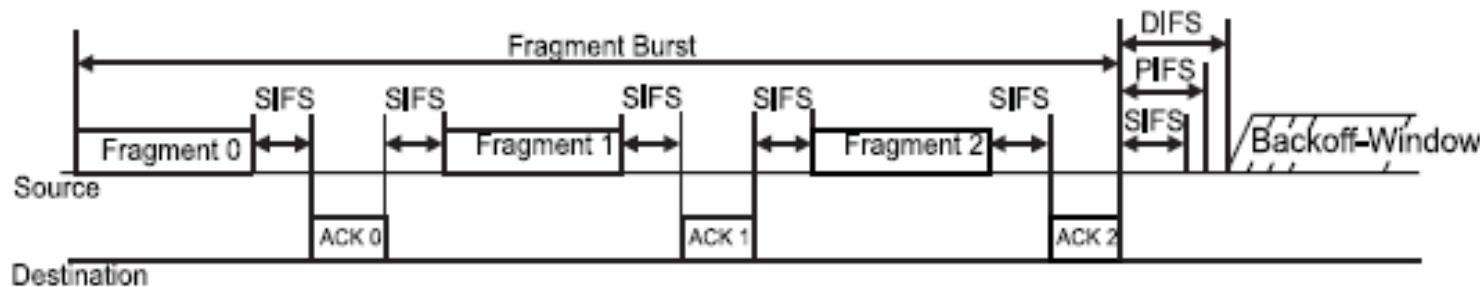
## Operación

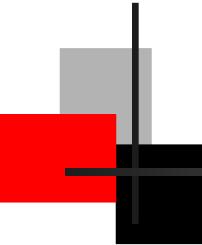
- Si el ACK no llega o llega tarde, se duplica el tamaño máximo de ventana de contienda, se calcula un tamaño de ventana entre cero y el máximo, y se inicia el procedimiento de (re)transmisión.
- Si se alcanza sin éxito un número máximo de retransmisiones (por defecto 7, ó 4 para tramas grandes en modo RTS/CTS), se descarta la trama y se reinicializa el tamaño máximo de ventana.

# La capa MAC. CSMA/CA

## Fragmentación

- Si una trama es demasiado larga, se puede fragmentar y transmitir secuencialmente (cada fragmento se confirma individualmente) separados por SIFS para que ninguna otra estación gane el canal.





# ***La capa MAC. Función de coordinación***



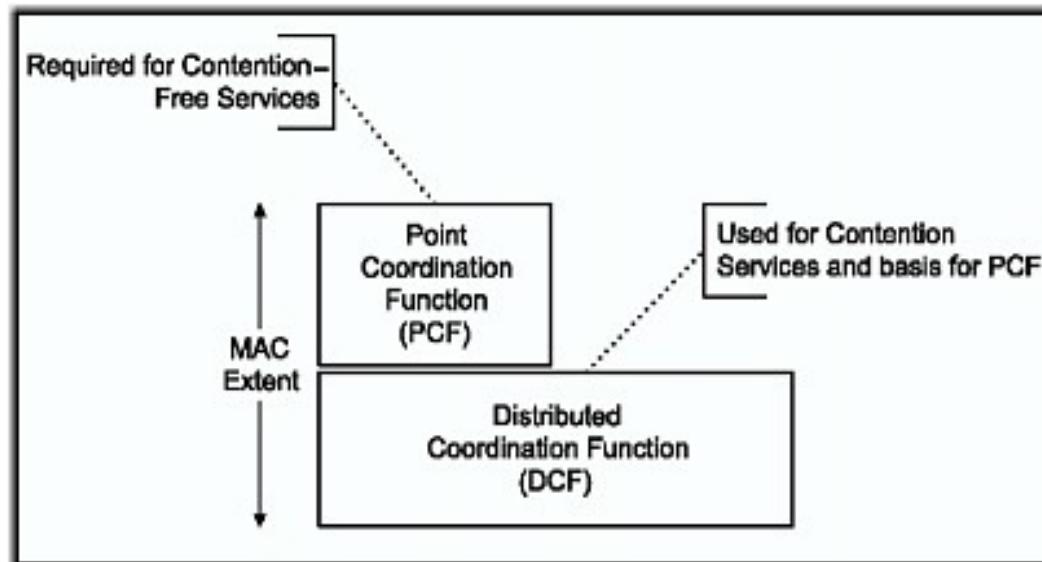
## Tipos

- PCF (Point Coordination Function). Centralizada. El PC (punto coordinador) reserva periódicamente el canal para fases libres de contienda, durante las cuales sondea por orden a todas las estaciones para que transmitan si lo necesitan, sin colisiones.
- DCF (Distributed Coordination Function). Distribuida. Cada estación usa CSMA/CA y, opcionalmente, RTS/CTS para acceder al canal; todas, incluidos APs, tienen iguales derechos.

# *La capa MAC. Función de coordinación*



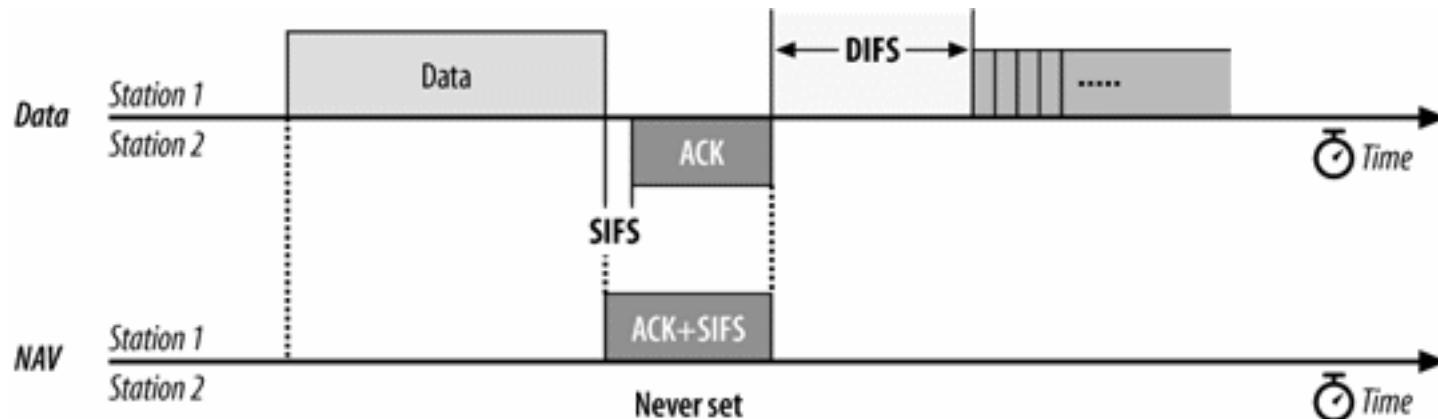
## Relación entre PCF y DCF



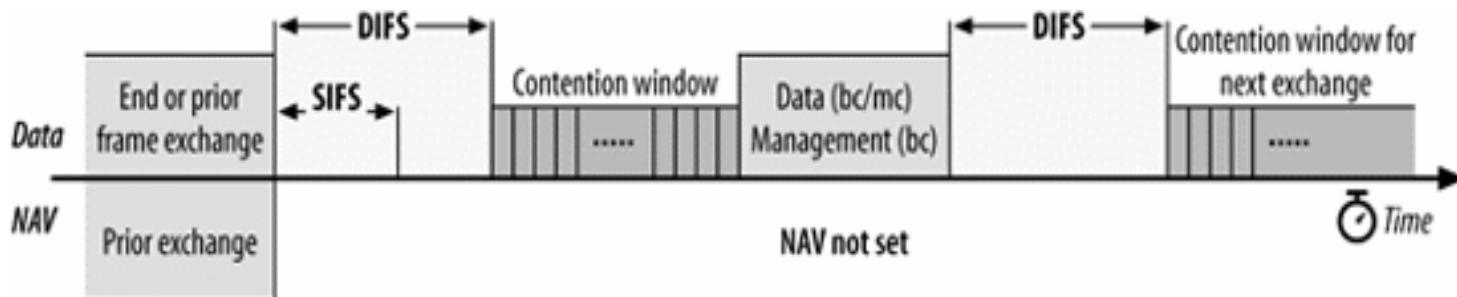
# *La capa MAC. Función de coordinación*



Trama unicast en DCF



Trama multicast o broadcast en DCF

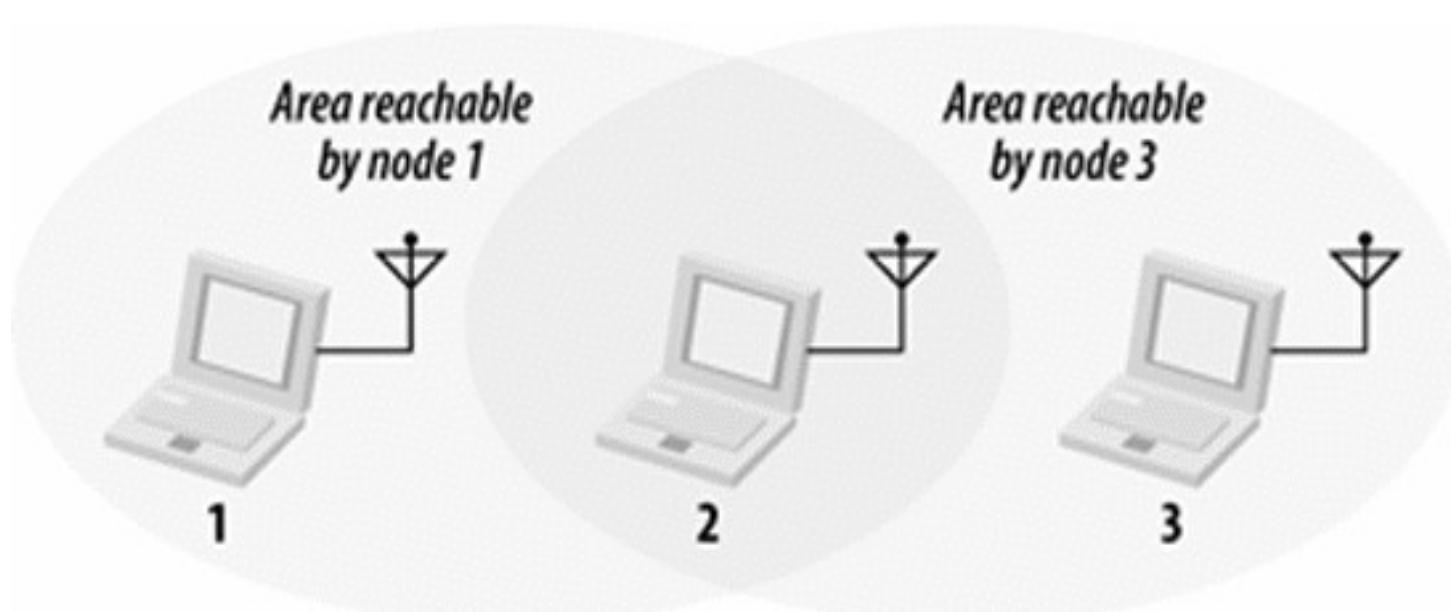


# **La capa MAC. Problema de nodo oculto**



## Planteamiento

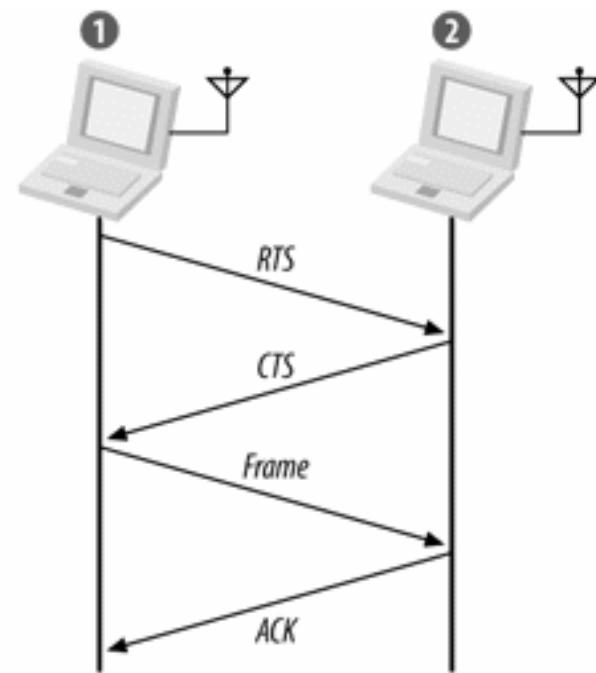
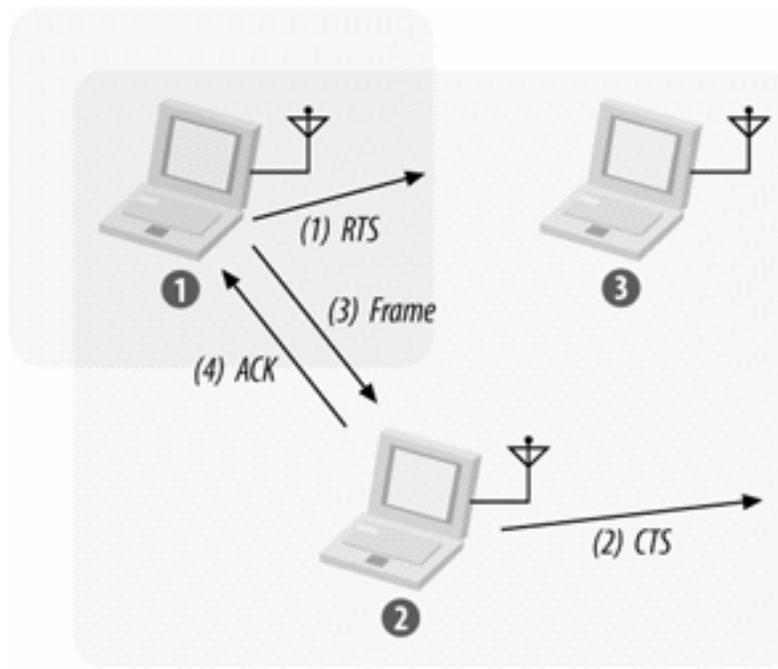
- El problema del nodo oculto: en el ejemplo, 1 y 3 no se ven por lo que no detectan la transmisión del otro hacia 2 y colisionan.
- El modo básico de CSMA/CA no funciona.



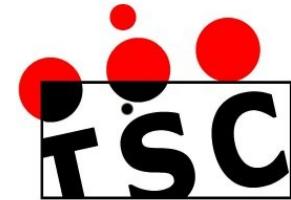
# **La capa MAC. Problema de nodo oculto**



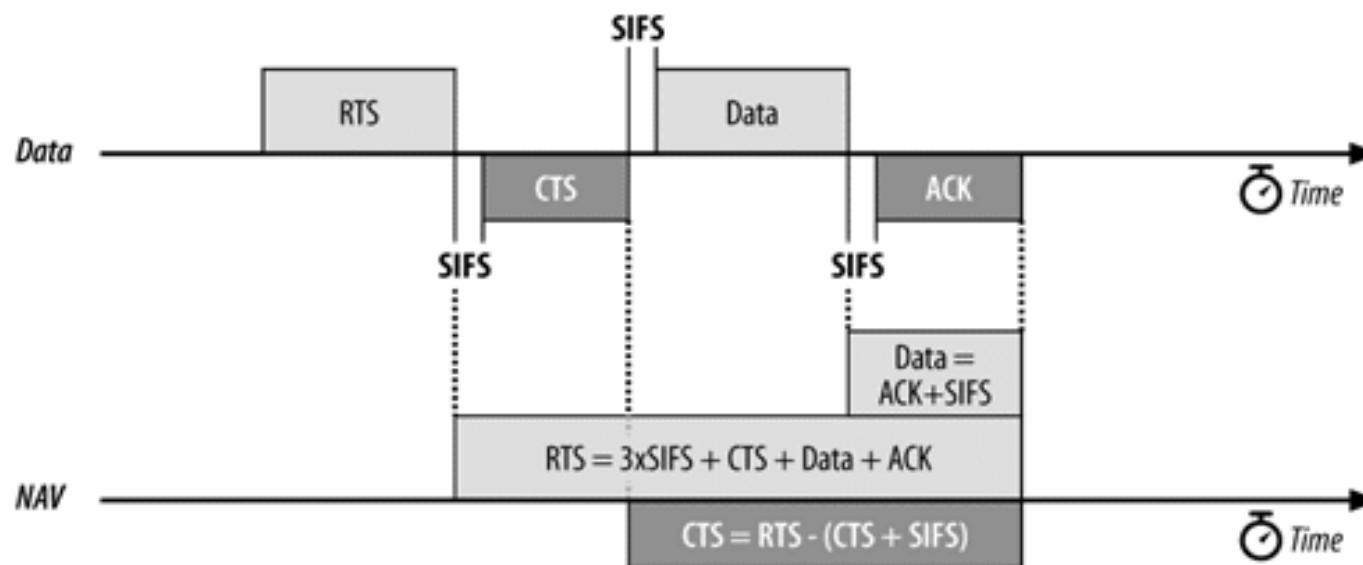
Solución: RTS/CTS



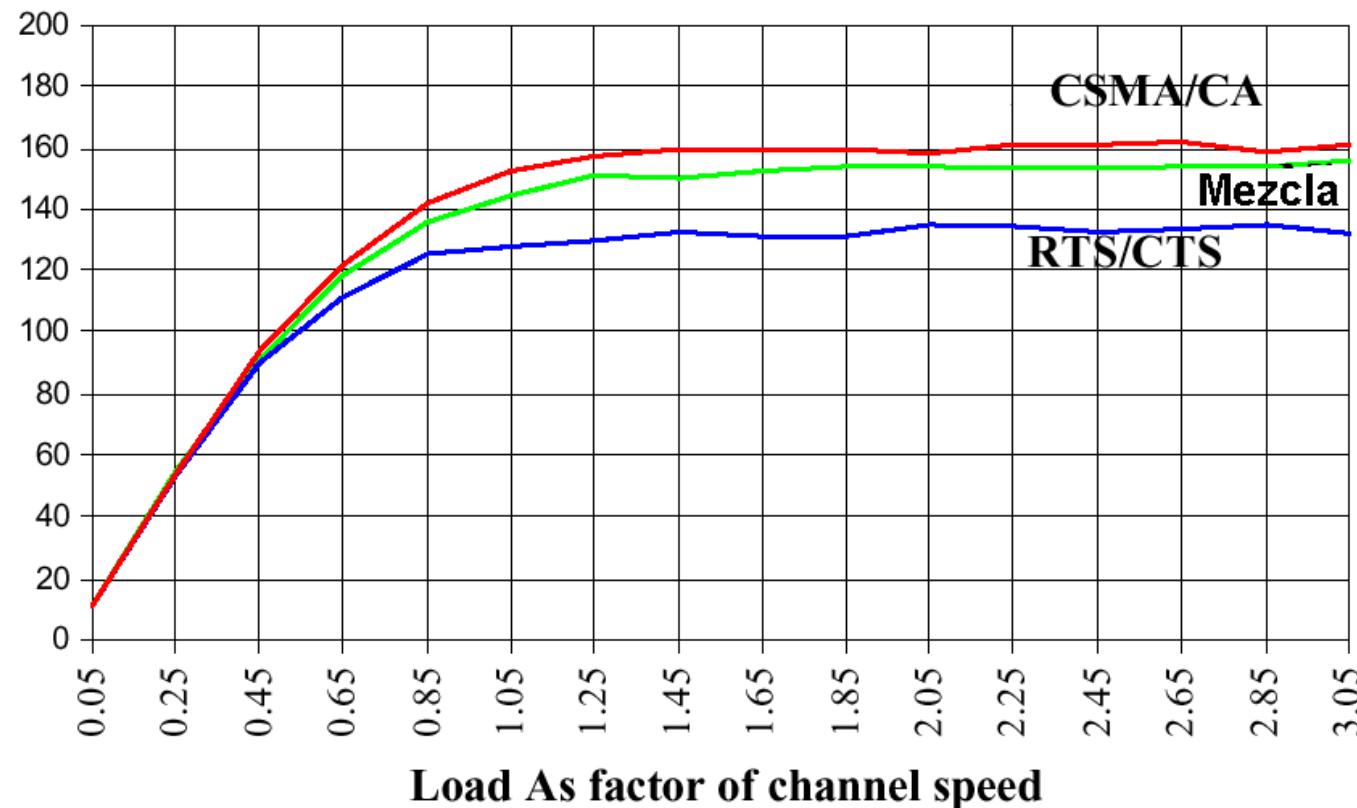
# **La capa MAC. Problema de nodo oculto**

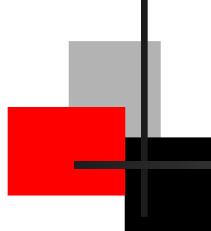


- RTS y CTS contienen información sobre la duración del total.
- Detección de portadora virtual: toda estación que puede interferir oye o bien el RTS o bien el CTS, actualiza el NAV (network allocation vector) y evita transmitir durante toda la transacción aunque no oiga nada.

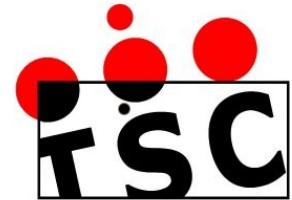


# *La capa MAC. Problema de nodo oculto*





# ***La capa MAC. Formato de trama***

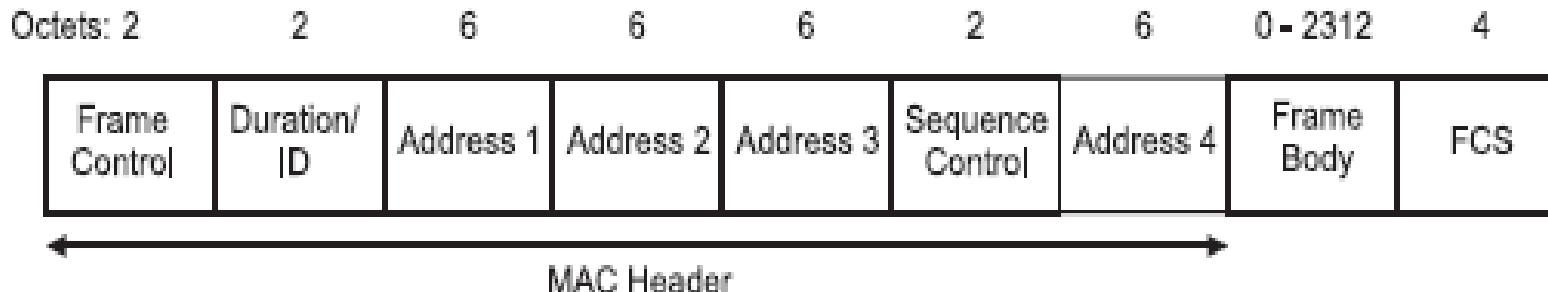


- ♦ Tipos de tramas de datos:
  - Data
  - Null
  - Data+CF-Ack
  - Data+CF-Poll
  - Data+CF-Ack+CF-Poll
  - CF-Ack
  - CF-Poll
  - CF-Ack+CF-Poll

# **La capa MAC. Formato de trama**



## Trama de datos



- ◆ Campo de control de trama: información de control MAC
- ◆ Duration ID: duración de la transacción, para actualizar NAV.
- ◆ Direcciones: para encaminar la trama a través del DS.
- ◆ Control de secuencia: en fragmentación, para saber último
- ◆ FCS: detección de errores
- ◆ Cuerpo de la trama: ahí se encapsulan datos a transmitir.

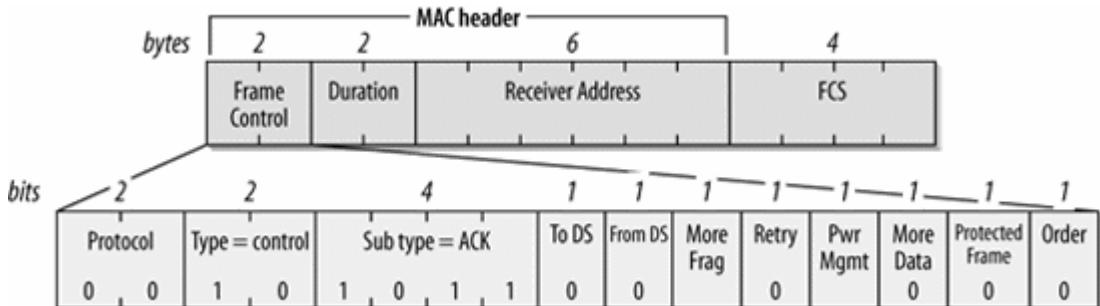
# La capa MAC. Formato de trama



## ◆ Trama ACK

14 bytes @ máxima tasa común.

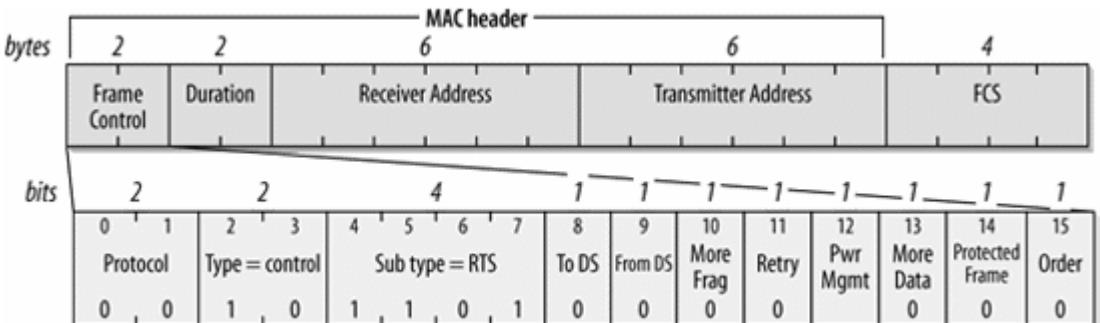
Caso peor: 112  $\mu$ s



## ◆ Trama RTS o CTS

20 bytes @ máxima tasa común.

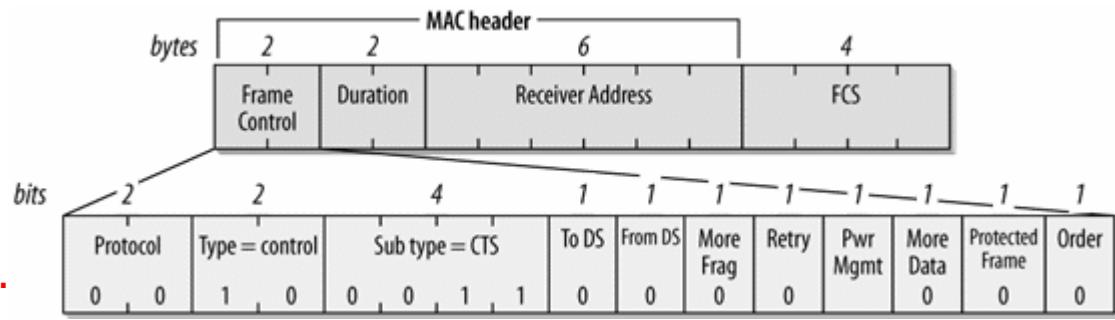
Caso peor: 160  $\mu$ s

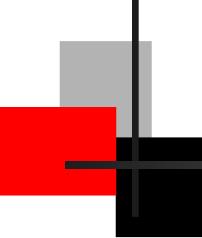


## ◆ Trama PS-Poll

14 bytes @ máxima tasa común.

Caso peor: 112  $\mu$ s

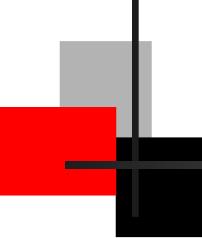




# **La capa MAC. IEEE 802.11e**



- Antes de 802.11e:
  - El MAC trataba a todos los tipos de tráfico por igual
  - Sin soporte a requerimientos de QoS (Quality of Service)
  - IEEE 802.11e define los mecanismos para proporcionar QoS a aplicaciones en tiempo real como voz y vídeo.
- Se distinguen estaciones que no utilizan los servicios QoS (nQSTA) aquellas que si los utilizan (QSTA).
- Para soportar QoS, IEEE 802.11e introduce una tercera función de coordinación, llamada HCF (Hybrid Coordination Function).

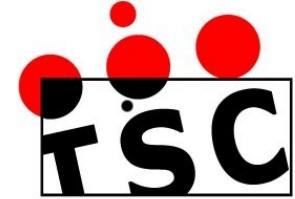


# **La capa MAC. IEEE 802.11e**

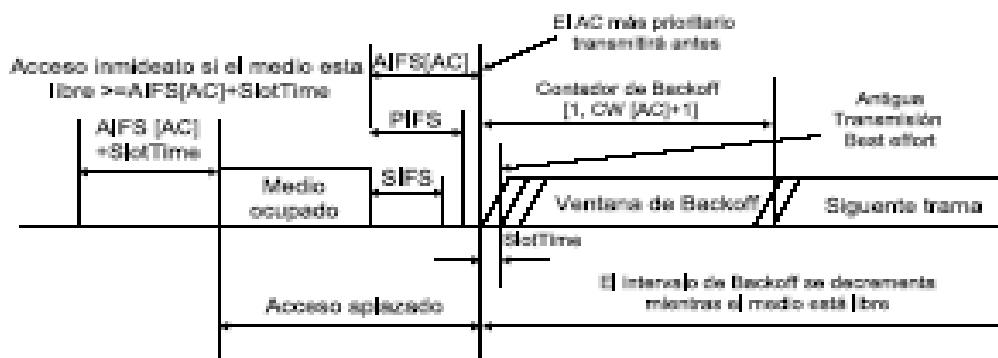


- HCF define dos nuevos mecanismos de acceso al canal:
  - **EDCA** (Enhanced Distributed Channel Access)
  - **HCCA** (HCF Controlled Channel Access).
- 4 categorías de acceso (AC) y 8 flujos de tráfico (TS)
- Las tramas que llegan se etiquetan con un identificador de prioridad de usuario (TID) según necesidad de QoS.
  - TID entre 0 y 7: mapeo a 4 AC EDCA
  - TID entre 8 y 15: HCCA; en cola correspondiente a TS
- TXOP (Transmission Opportunity): Intervalo de tiempo durante el que una estación puede enviar sus tramas.

# La capa MAC. IEEE 802.11e



- EDCA
  - Mejora DCF priorizando tráficos. Dos formas de hacerlo:
    - Asignar distintos IFS a las diferentes AC
    - Asignar distintos CW a las diferentes AC
  - Para el primero, se define AIFS (Arbitration IFS)  
$$AIFS[AC] = AIFSN[AC] \times aSlotTime + SIFS$$

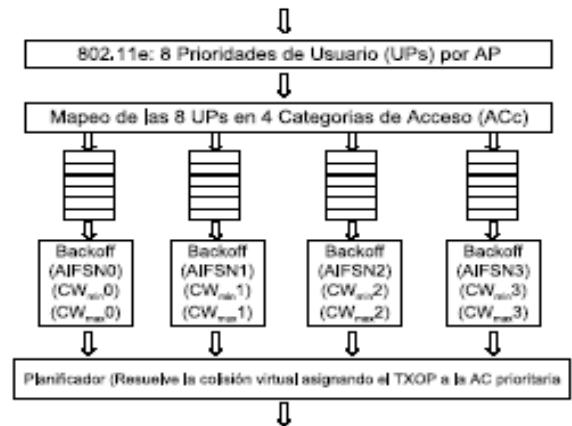


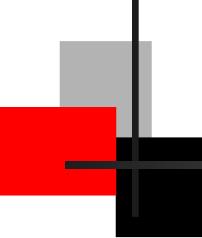
# **La capa MAC. IEEE 802.11e**



## Clases AC definidas en 802.11e

- Dos o más AC dentro de una misma QSTA pueden poner a 0 su contador de Backoff en el mismo instante. Si esto ocurre, se produce una **colisión interna**.
- Siempre que esto se produzca, la capa MAC ofrecerá la oportunidad de transmisión al flujo más prioritario, tratando el de menor prioridad igual que si se hubiera producido una colisión real.





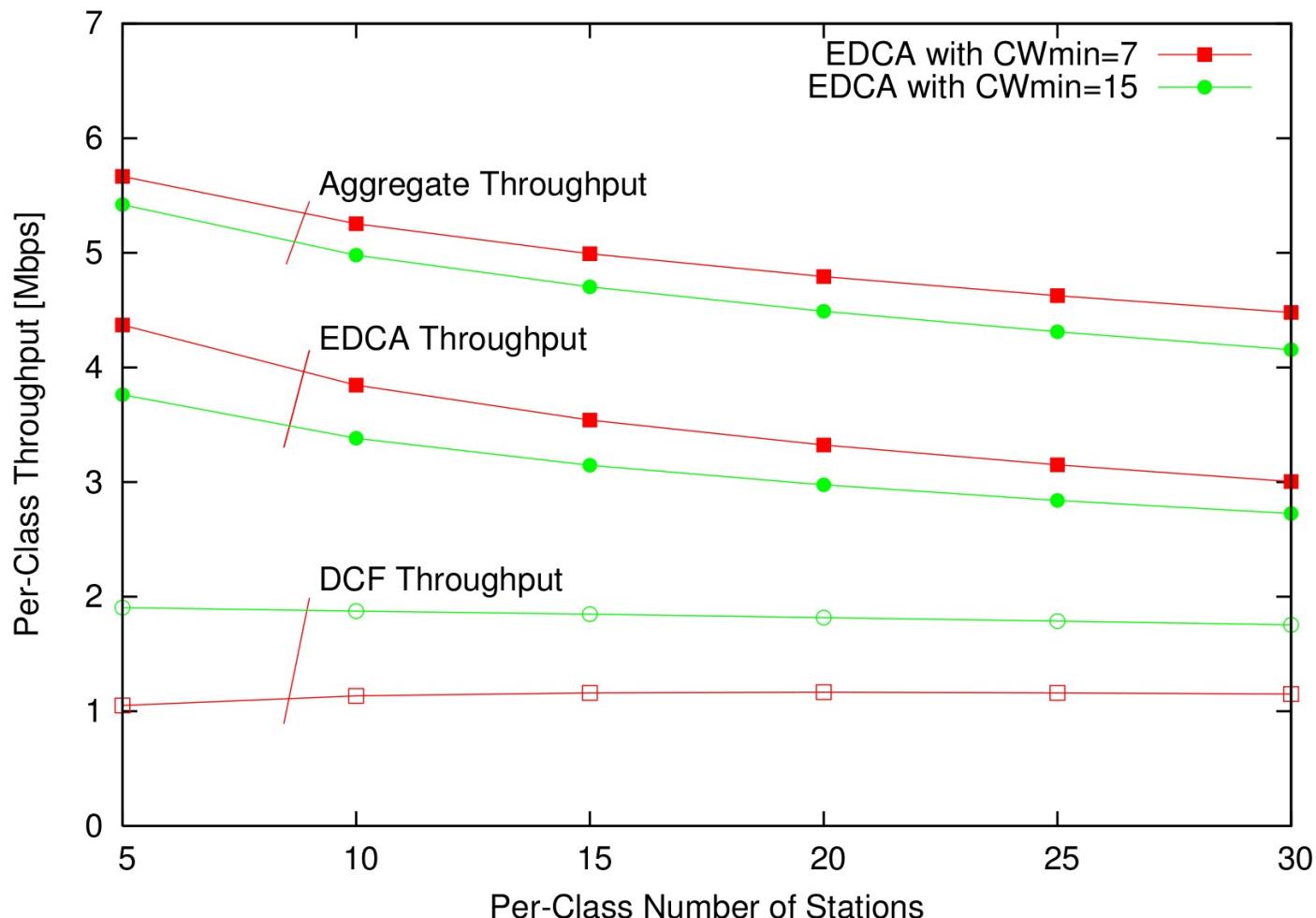
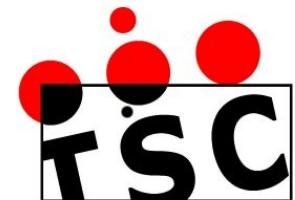
# **La capa MAC. IEEE 802.11e**



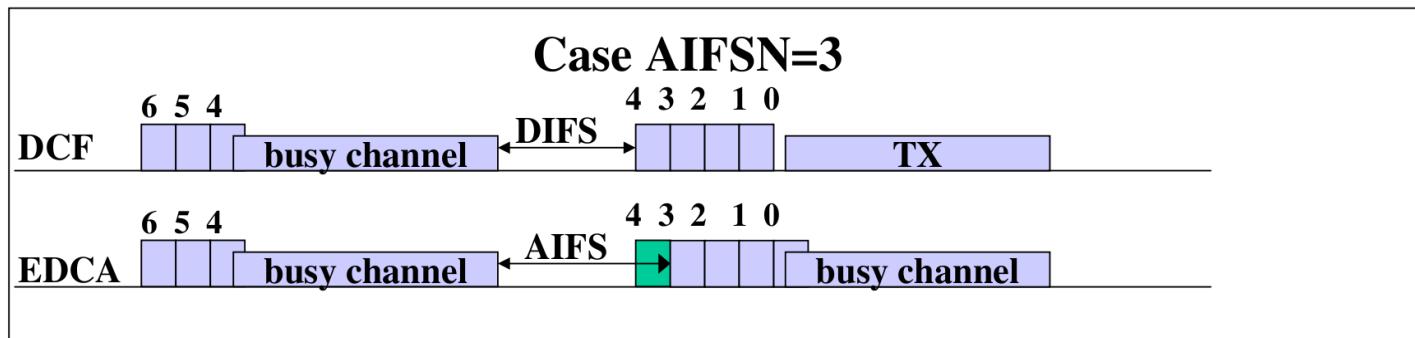
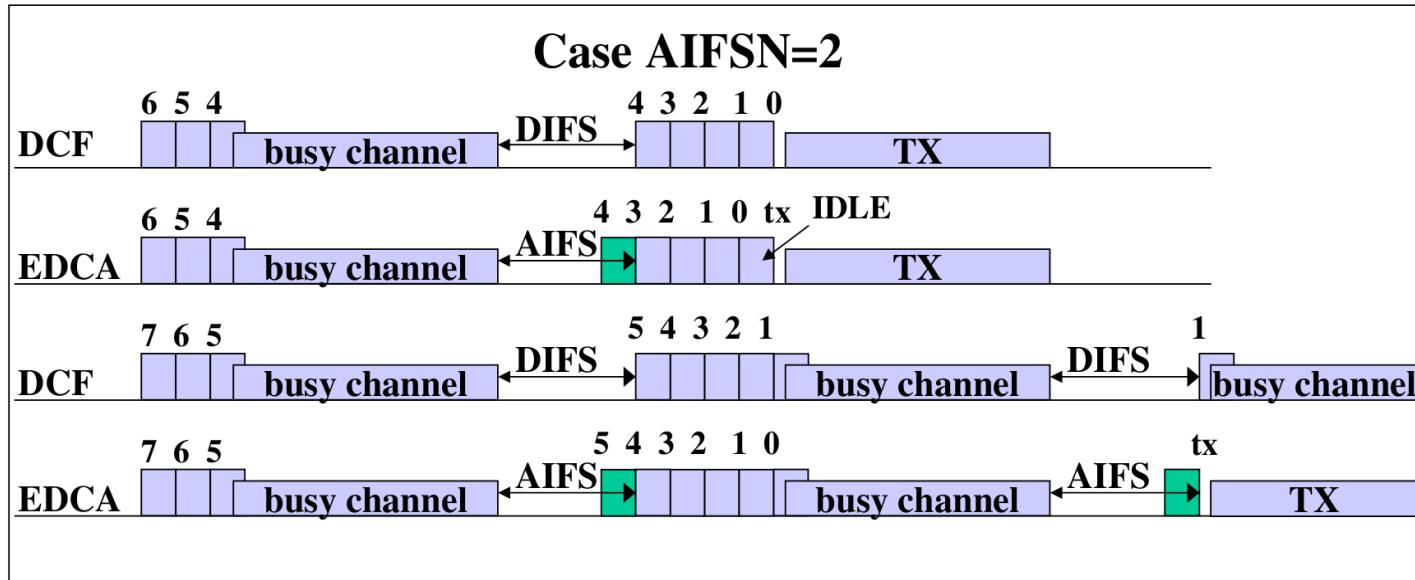
Access Category	$CW_{min}$	$CW_{max}$	AIFSN
$AC\_BK$	$aCW_{min}$	$aCW_{max}$	7
$AC\_BE$	$aCW_{min}$	$aCW_{max}$	3
$AC\_VI$	$aCW_{min}/2$	$aCW_{min}$	2
$AC\_VO$	$aCW_{min}/4$	$aCW_{min}/2$	2

## EDCA DEFAULT SETTINGS

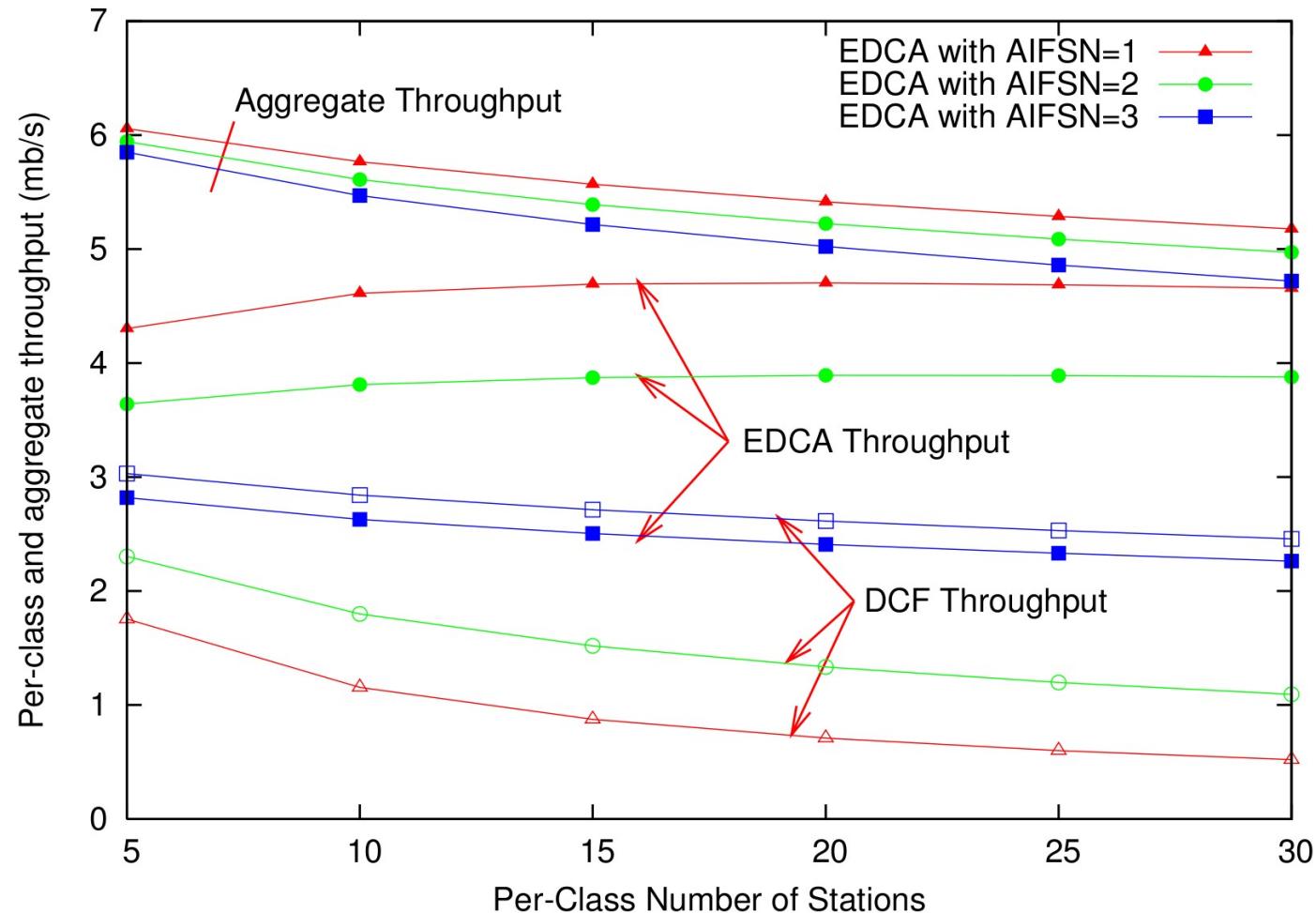
# *La capa MAC. IEEE 802.11e*



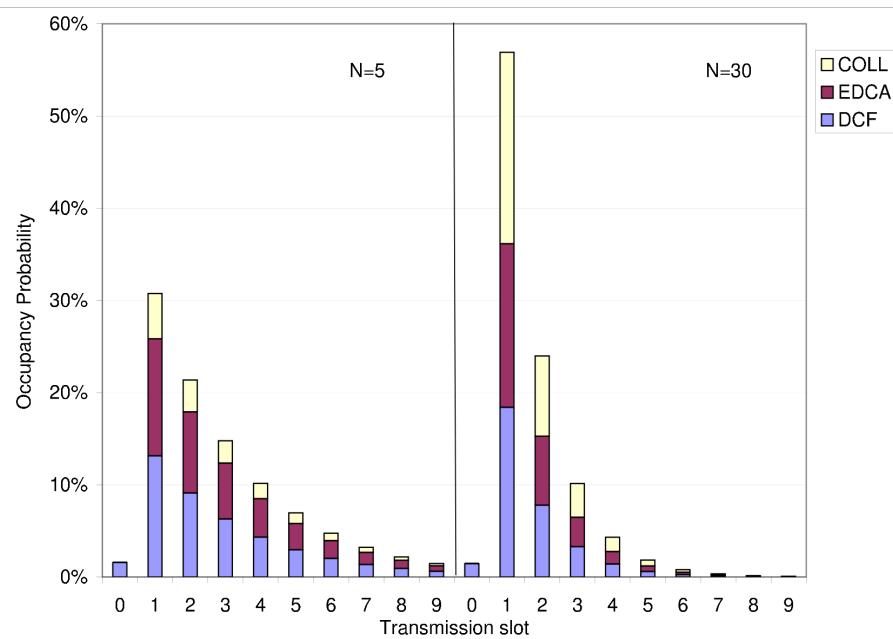
# La capa MAC. IEEE 802.11e



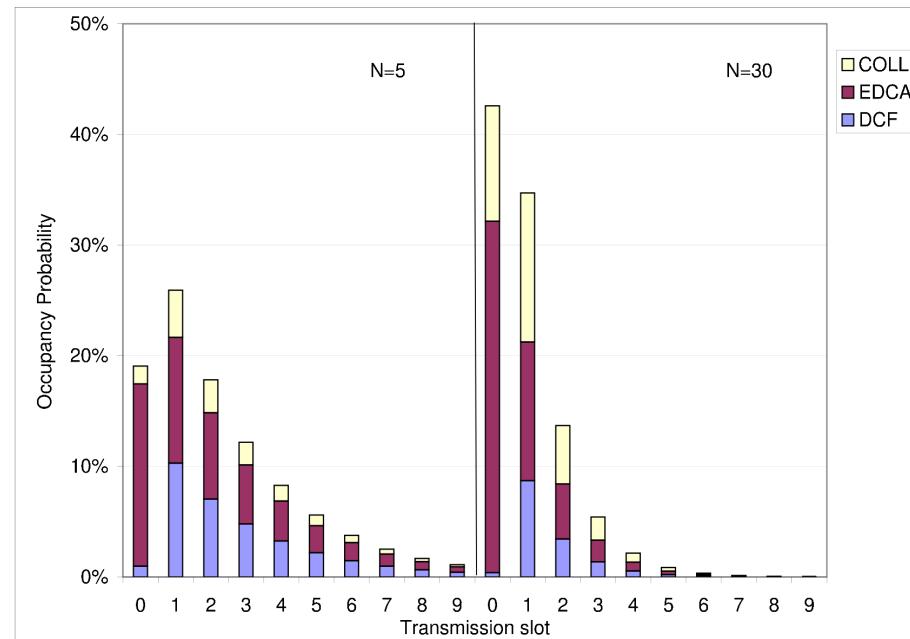
# *La capa MAC.* IEEE 802.11e



# La capa MAC. IEEE 802.11e

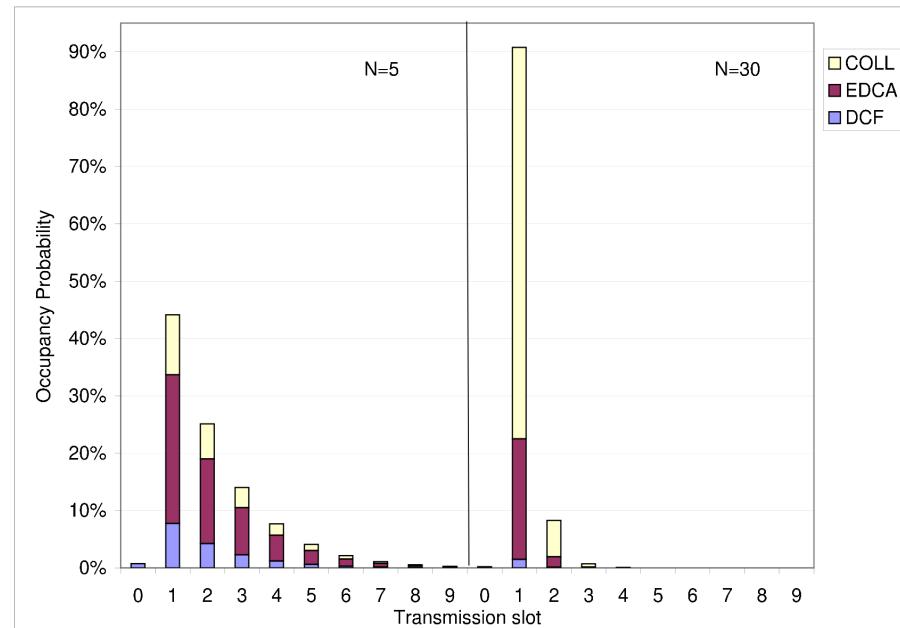
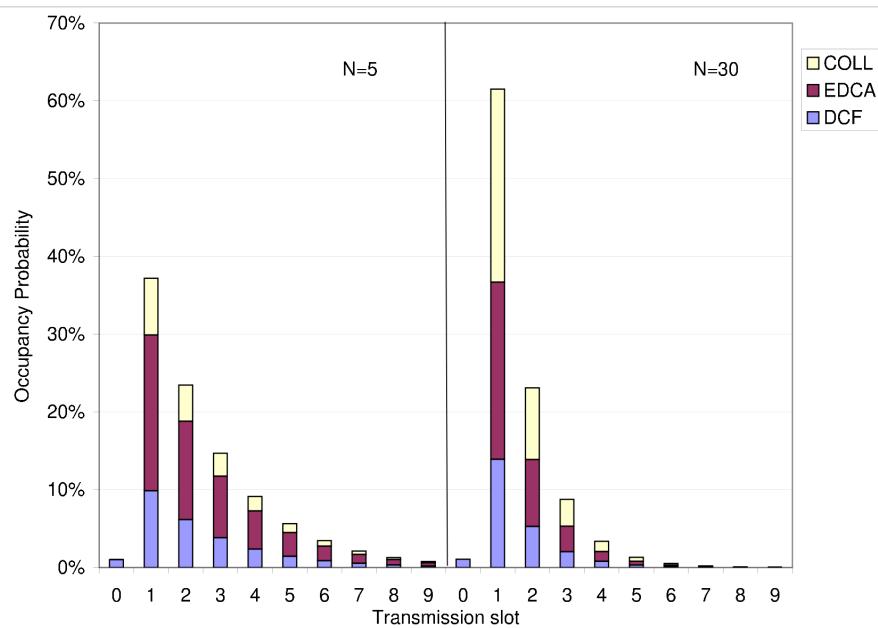


BE vs DCF (5/30 STA's de cada)



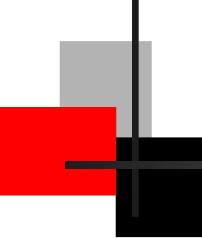
Diferenciación con AIFSN  
(5/30 STA's de cada)

# La capa MAC. IEEE 802.11e



BE vs DCF (5/30 STA's de cada)

Diferenciación con CWmin y CWmax  
(5/30 STA's de cada)

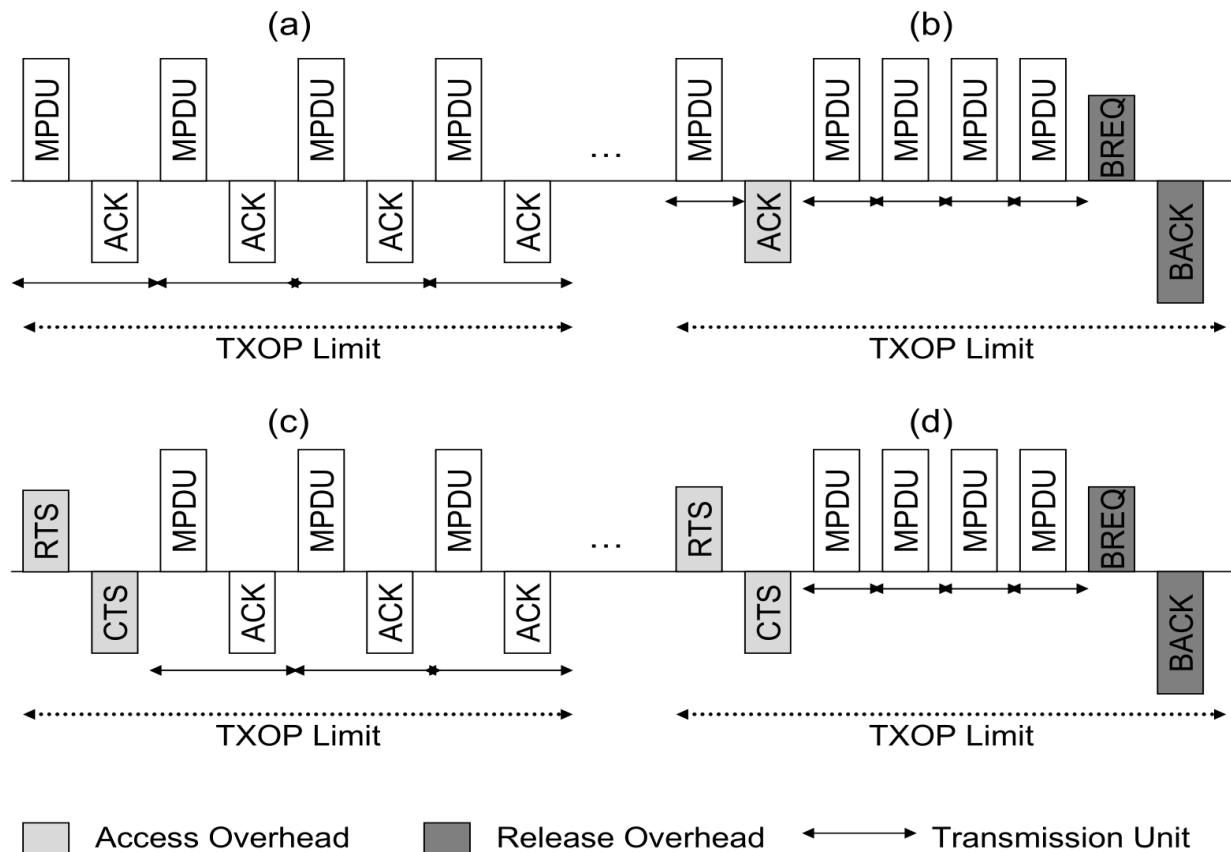


# **La capa MAC. IEEE 802.11e**



- Otros dos recursos nuevos en el MAC de 11e:
  - TXOP: Retener el canal durante más de una trama.  
Límite: el marcado por TXOP\_Limit [ms] 
  - Block ACK: Mandar varias tramas seguidas que se confirman todas a la vez al final, para ahorrarse los ACKs en la mayoría.
- Estos y los otros parámetros de 11e, los fija el AP y los transmite a las STA's en una trama beacon.
- El AP puede tener valores distintos a los de las STA's.

# La capa MAC. IEEE 802.11e

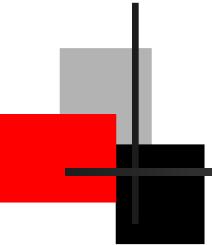


Data burst illustration with different access modes and ACK policies:  
(a) BI, (b) BB, (c), RI, and (d) RB

# **La capa MAC. IEEE 802.11e**

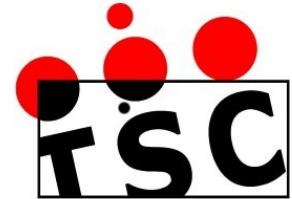


- HCCA:
  - Similar a PCF; el coordinador se llama HC (Hybrid Coordinator) y es siempre el AP. Los periodos CP se realizan con EDCA.
  - Se definen clases de tráfico (TC). El HC puede coordinar el tráfico como prefiera, sabiendo las clases de tráfico y la longitud de las correspondientes colas.
  - Cuando HC sondea a una QSTA con CF-Poll, ésta puede mandar tramas durante TXOP.
- La WiFi-Alliance certifica el soporte HCCA (opcional) como “WMM Scheduled Access”



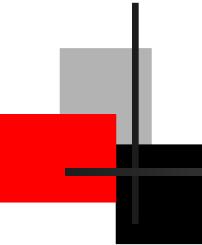
# ***Seguridad y control de acceso.***

## ***Seguridad básica***



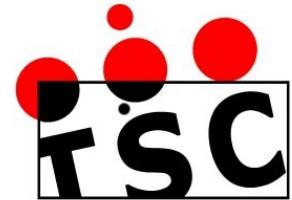
### Problemas de seguridad en WLAN

- Las señales de Wireless LAN no se limitan a los edificios en los que se utilizan.
- Existe un riesgo potencial de acceso no autorizado por parte de personal fuera del área de cobertura.
- Posibilidad de riesgo potencial para el acceso no autorizado a los recursos de red a través del medio radio.
- “Espionaje” de la señalización wireless.



# ***Seguridad y control de acceso.***

## ***Seguridad básica***

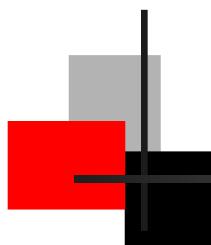


### Service Set ID (SSID)

- Cadena utilizada como identificación de un conjunto de servicio.
- Puede actuar como palabra clave básica para acceder al sistema.
- Fácilmente superada. El AP difunde el SSID; fácil de conocer.

### Wired Equivalent Privacy (WEP)

- Define un método de autentificación y encriptación.
- La autentificación se utiliza para protegerse de usos no autorizados de la red.
- La encriptación se utiliza para prevenir que “espías” decodifiquen transmisiones capturadas.



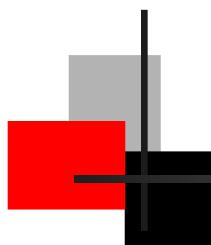
# **Seguridad y control de acceso.**

## **WEP**



### **WEP (Wireless Equivalent Privacy)**

- Cifrado mediante codificación XOR a partir de una clave.
- Esta clave se utiliza para generar una secuencia de números aleatorios, RC4 en el caso de WEP.
- Para recuperar la secuencia enviada, a partir de la clave inicial, se genera la misma secuencia de números aleatorios y se realiza un XOR a la secuencia recibida.
- La clave generadora de WEP es de 40 bits más 24 bits de un vector de inicialización (IV).
- Esto lleva a decir que la clave de WEP es de 64 bits.



# **Seguridad y control de acceso.**

## **WEP**



### Fallos

- Relacionados con la gestión de claves
  - Gestión manual de claves, problemática.
  - Clave de 40 bits, muy pequeña.
  - Si se reutiliza el “keystream”, susceptible de análisis (vulnerabilidad de IV).
  - Si no se cambian, las claves pueden compilarse en “diccionarios”.
  - WEP utiliza CRC para chequeos de integridad, que no es “fuerte” criptográficamente.
  - El AP es un punto de desencriptación privilegiado

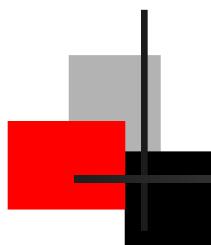
# **Seguridad y control de acceso.**

## **WEP**

### **Fallos**

- Hay una serie de IVs “débiles” de los que se conocen los 2 primeros bytes (RC4). En una red WEP hay 1280 IVs débiles.
- Si en vez de utilizarse una llave estándar de 40 bits, se utiliza una de 128 bits, se cuadriplica el número de IVs débiles.
- Con este conocimiento y utilizando teoría de probabilidad, se demostró que con 6-8 millones de paquetes se recuperaba la llave completa.
- A finales de agosto de 2001 se publicó AirSnort, un programa que era la implementación del ataque teórico.
- Desde entonces se admite que las redes WEP son completamente vulnerables.





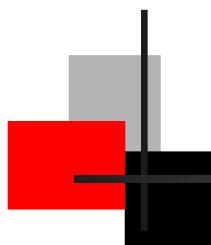
# ***Seguridad y control de acceso.***

## **WEP**



### Soluciones

- Múltiple autentificación
- Generación y gestión de certificados
- Encriptación a diferentes niveles de la capa OSI.
  - IPSEC
  - OpenSSH
- Filtrado HMAC (débil)
- Todas estas soluciones combinadas son una mejora enorme respecto a WEP pero no son infalibles.

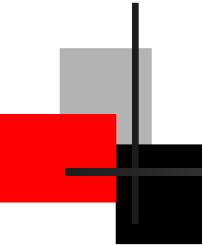


# **Seguridad y control de acceso. WPA/WPA2**



## **WPA: Wi-Fi Protected Access**

- WPA: propuesta por la Wi-Fi Alliance en 2003
  - Emplea RC4 como algoritmo de cifrado.
  - Usa TKIP (Temporary Key Integrity Protocol) como algoritmo de gestión de claves.
- WPA2: estandarizado por el IEEE 802.11i
  - Utiliza AES (Advanced Encryption Standard) como algoritmo de cifrado.
  - Toma CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) como encriptación.



# ***Seguridad y control de acceso.***

## **WPA/WPA2**



### Fundamentos

- Tanto TKIP como AES garantizan que las claves de encriptación utilizadas son distintas para cada paquete, eliminando una importante vulnerabilidad de WEP.
- Se calcula el MIC (Message Integrity Check)
  - Incrementado en cada trama (evita ataque por retransmisión)
  - Garantiza integridad generando un hash de IV y claves y transmitiendo el hash en lugar de IV
- Dos entornos posibles: Enterprise y Doméstico o personal



# **Gestión de red. Introducción**

## Objetivos

- Minimizar efectos de no fiabilidad y fácil accesibilidad del medio físico.
- Reducir problemas de excesivo consumo de energía.
- Mejorar el uso eficiente de los recursos.

# Gestión de red. Introducción

## Generalidades

- Tanto la capa física como la capa MAC tienen acceso a una base de información de gestión (MIB), que tiene objetos para obtener información y otros para emprender ciertas acciones.
- Hay tres interfaces entre los componentes de gestión: la entidad de gestión del sistema (SME) puede acceder a ambos MIBs, y adicionalmente el MIB del MAC puede acceder al del PHY.

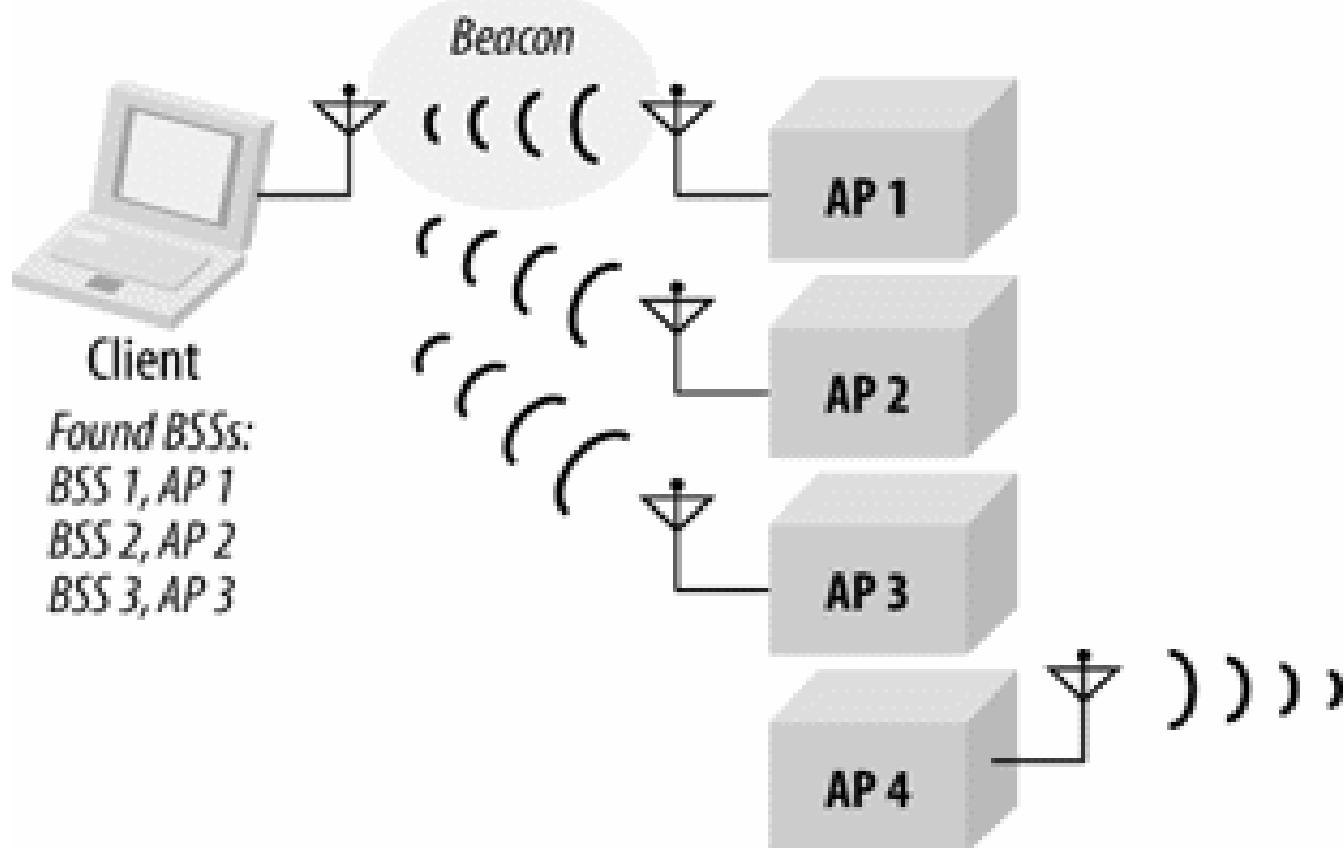
# Gestión de red. Introducción

## Funciones

- **Escaneo:** buscar redes y sistemas en la zona de cobertura
  - Activo (Enviando Probe-Request)
  - Pasivo (Escuchando Beacons)
- **Asociación:** se incluye en esta función toda tarea necesaria para establecer un nexo de unión entre un AP y una STA determinados .
- **Ahorro de energía:** desconexión de STAs conservando la conectividad.
- **Gestión del espectro:** gestión de potencia y frecuencia para uso óptimo de canal compartido.

# Gestión de red. Escaneo

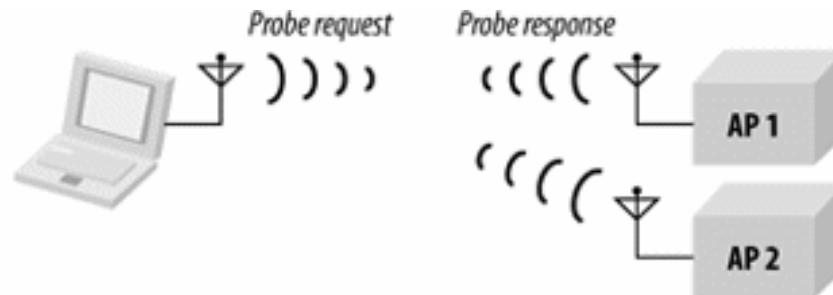
Pasivo



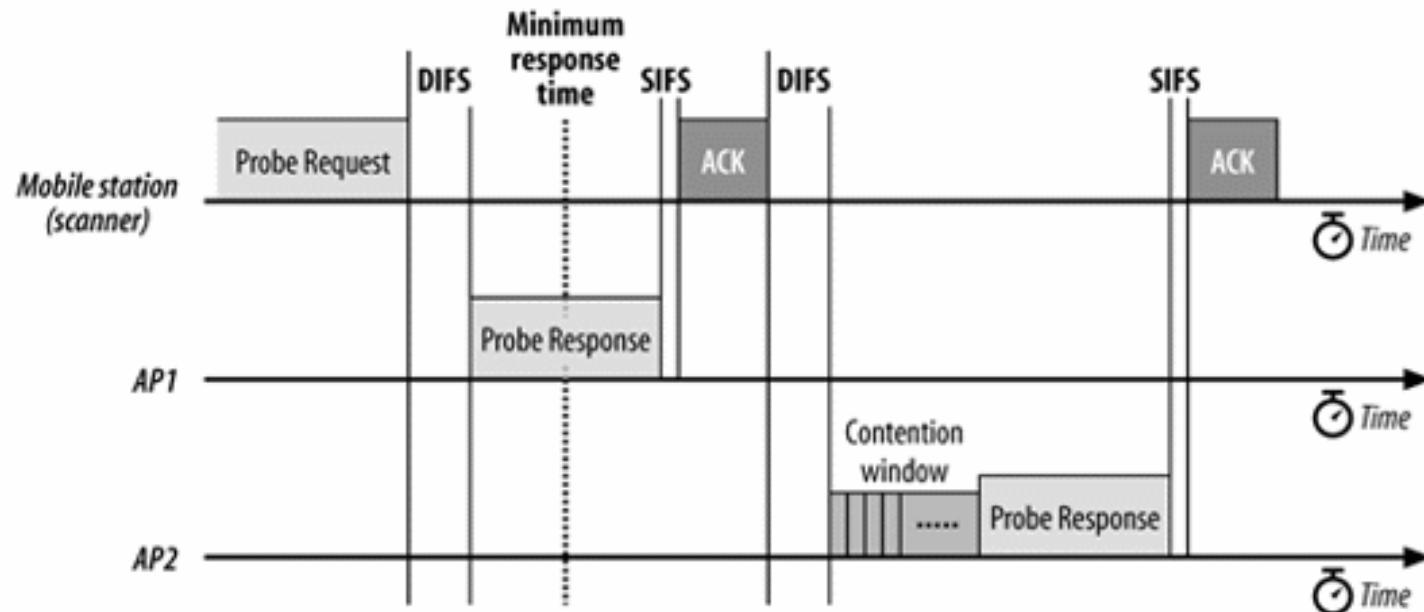
# Gestión de red. Escaneo

Activo

(a)



(b)





# Gestión de red. Asociación

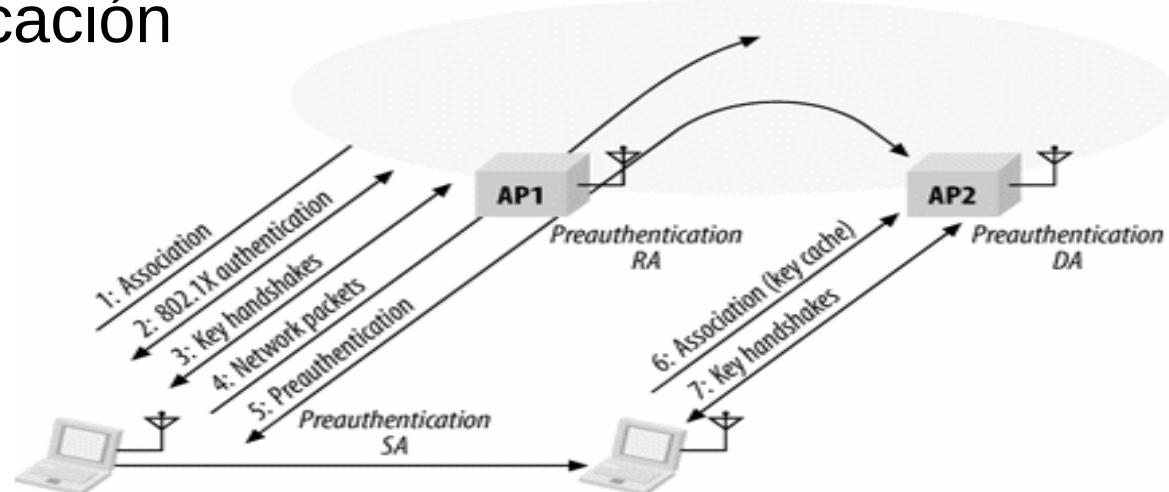
## Tareas

- **Adhesión (joining):** operación interna a la STA consistente en identificar parámetros asociados a SSID escogido y compararse con ellos. Si hay varios BSS accesibles, elección del mejor. También sincronización de tiempo y frecuencia.
- **Autentificación:** identificación unilateral de STA a AP por sistema abierto o WEP
- **Preatentificación:** permite ahorrar tiempo en caso de posible transición entre BSS. La STA se preautentica en los BSS accesibles, y si transita a otro, sólo se tiene que asociar.

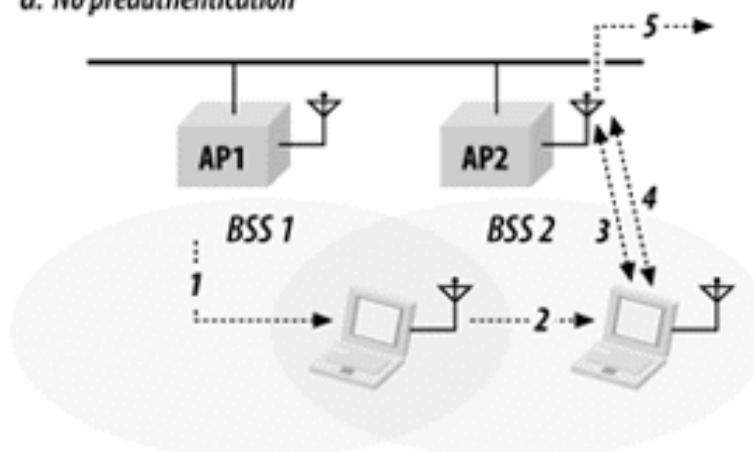
# Gestión de red. Asociación



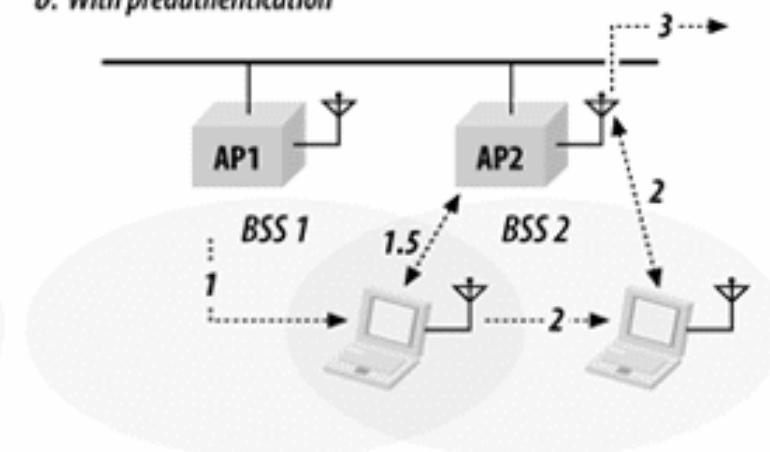
## Preatentificación



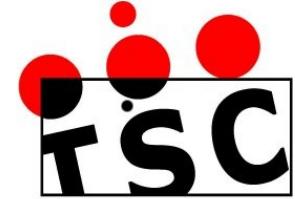
a: No preauthentication



b: With preauthentication

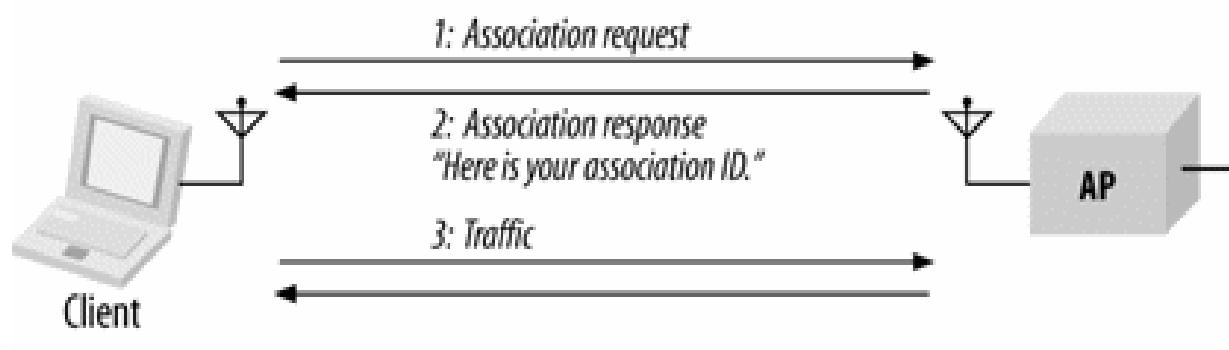


# Gestión de red. Asociación



## Tareas

- **Asociación:** operación de registro para que el DS sepa a través de qué AP está accesible la STA.



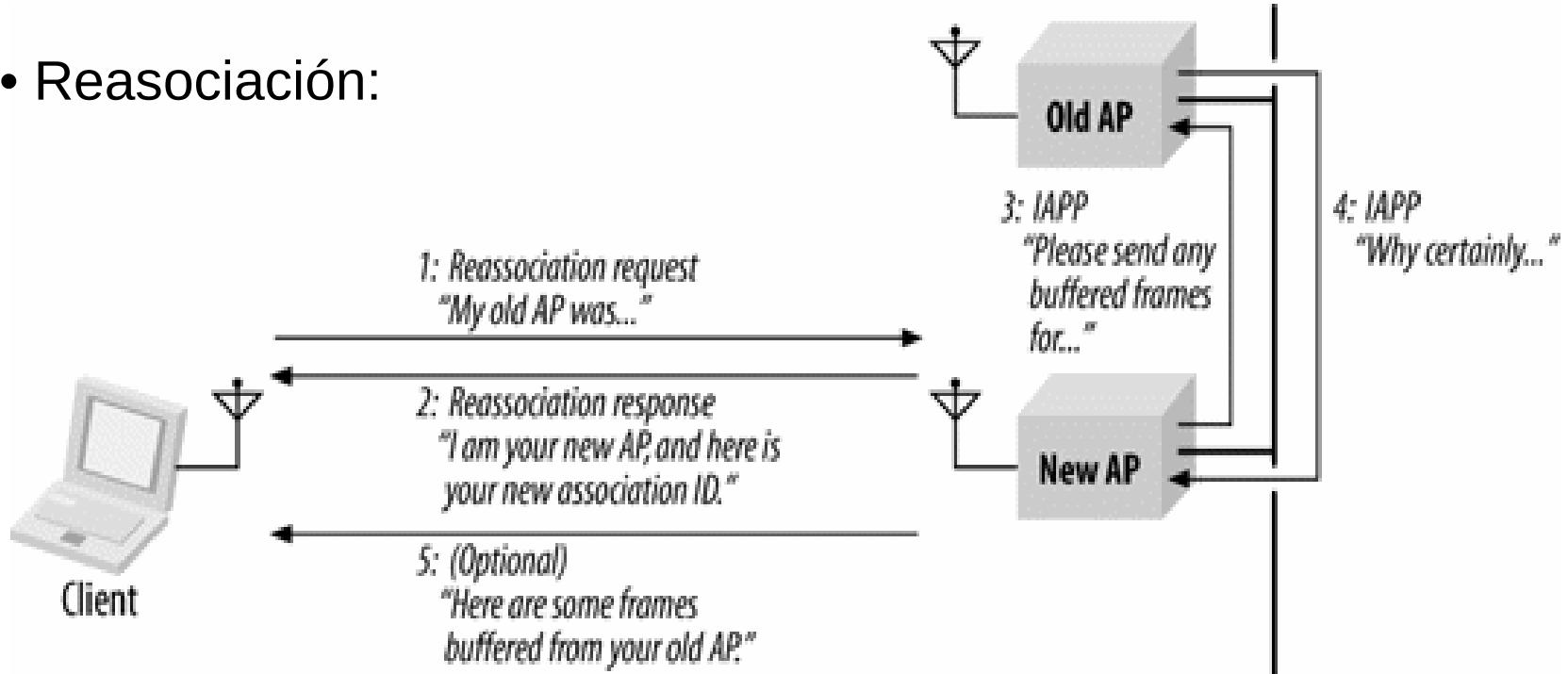
- **Reasociación:** igual pero cuando la STA ya estaba asociada a otro BSS del ESS. El nuevo AP informa al antiguo y le requiere las tramas destinadas a la STA y pendientes de entrega.

# Gestión de red. Asociación



## Tareas

- Reasociación:



## Fundamentos

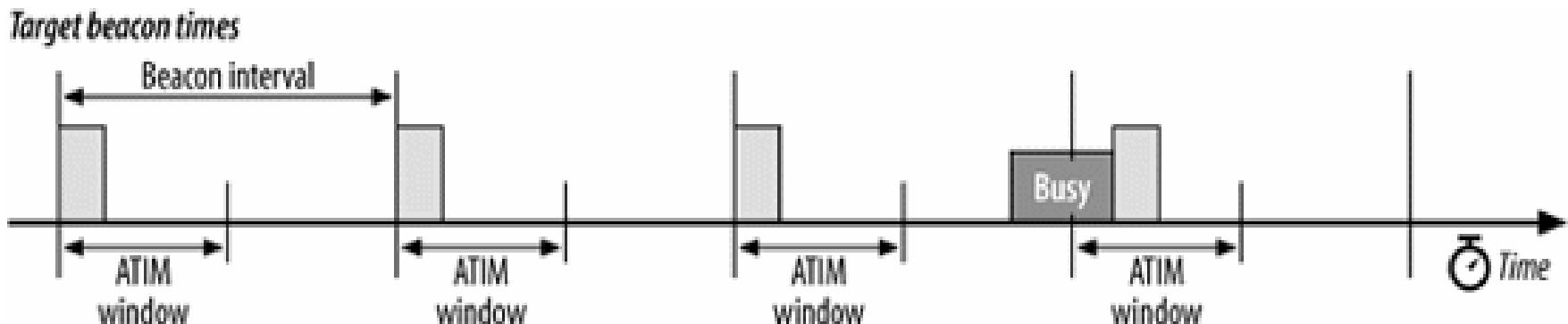
- STAs suspendidas todo el tiempo posible sin sacrificar conectividad.
- El AP se mantiene informado del estado de STAs y distribuye periódicamente un mapa de indicación de tráfico (TIM) en las tramas beacon para avisar a las estaciones que tienen tráfico pendiente.
- El intervalo de escucha se negocia con el AP en la asociación.
- La estación con tramas pendientes las pide con PS-Poll.
- Cada varios beacons, uno con DTIM para avisar de posibles tramas broadcast/multicast

# Gestión de red. Ahorro de energía



## Fundamentos

- Ahorro de energía en IBSS: tras la trama beacon se abre una ventana ATIM durante la que cualquier estación puede mandar tramas ATIM.
- Todas las estaciones deben estar despiertas durante beacon y ventana ATIM.



## Fundamentos

- Función: lograr la maximización de la capacidad agregada mediante el uso eficiente del espectro y la potencia.
- **Control de potencia de transmisión (TPC)**: en base a la información de potencia máxima y mínima y niveles de recepción, se ajusta automáticamente la potencia al mínimo que asegura una buena recepción.
- **Selección dinámica de frecuencia (DFS)**: en la asociación se informa de los canales soportados al AP. En todo momento el AP puede ordenar un periodo silencioso para escuchar el canal en búsqueda de interferencias.



# Análisis de prestaciones

› Modelos de DCF: Hay cientos. Algunos más relevantes:

- › Chhaya y Gupta (1997): primer modelo publicado (anterior al estándar).
- › Cali, Conti y Gregori (2000): simplifica el MAC reduciendo toda la complejidad de la ventana de contención; aproxima el mecanismo de contienda por un p-persistente.
- › Tay y Chua (2001). Modelo simplificado basado en la sustitución de varias variables aleatorias por sus valores medios.
- › Ziouva y Antonakopoulos (2002). Mejora del modelo de Cali et al. en que contempla poblaciones finitas y tráfico no saturado.



# Análisis de prestaciones

- **Primer modelo de Bianchi (2000):**
  - Modelo analítico del DCF (Distributed Coordination Function) basado en una cadena bidimensional de Markov
  - Hace algunas simplificaciones y aproximaciones críticas:
    - Tráfico saturado
    - Número ilimitado de retransmisiones
    - Canal ideal
    - La probabilidad de colisión es cte. e independiente de la retransmisión

# Análisis de prestaciones. Bianchi



- $b(t)$  = proc. estocástico de retroceso binario exponencial en STA
- $s(t)$  = proc. estocástico de número de retransmisión en una STA
- $\{b(t), s(t)\}$  = proc. estocástico bidimensional que se puede modelar por una cadena de Markov de distribución estacionaria:

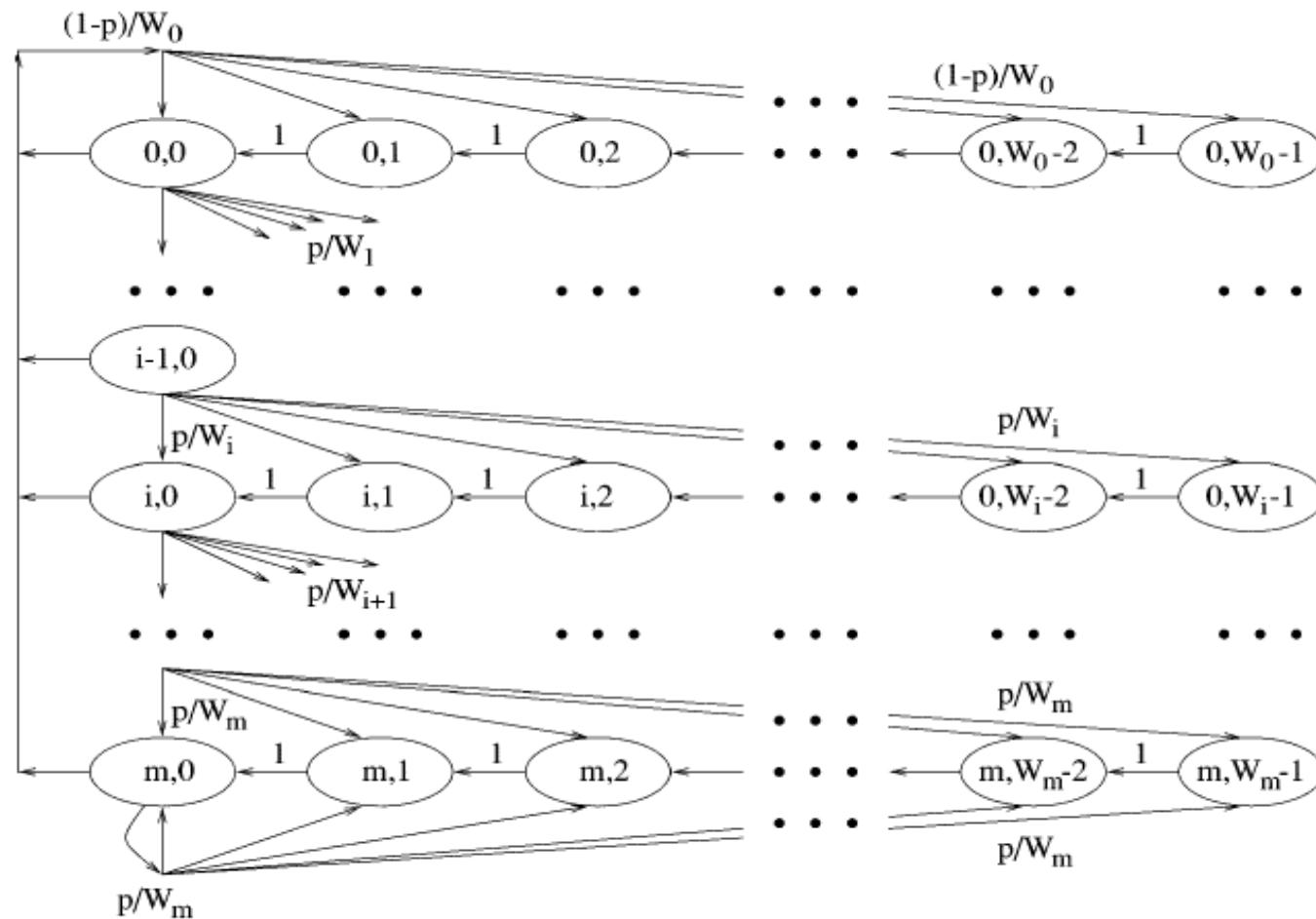
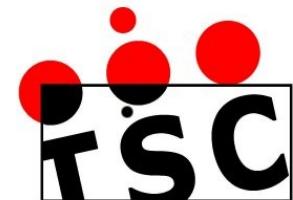


- $W_0 = CW_{min} = \text{nº mínimo de posibles valores de la ventana de contención para la primera transmisión de una trama.}$
- $m = \text{máximo número de retransmisiones}$

$$W_m = 2^m W_0, \text{ y } W_i = 2^i W_0 \text{ para } i \in (0, m)$$

- $\tau = \text{Prob. incondicional de TX de una STA en cualquier ranura}$
- $p = \text{Prob. condicional de colisión de una STA que TX}$

# Análisis de prestaciones. Bianchi



# Análisis de prestaciones. Bianchi



- La solución de la cadena de Markov permite obtener:

$$\tau = \frac{\varepsilon}{(1 - 2p)(w - \varepsilon)}$$

- Ahí tenemos dos incógnitas, hace falta otra ecuación que las relacione. Puesto que una estación colisionará si alguna de las demás transmite en la misma ranura:

$$p = 1 - (1 - \tau)^n$$

- Dos ecuaciones con dos incógnitas, resolución por métodos numéricos.

# Análisis de prestaciones. Bianchi



- Una vez resuelto el modelo, se puede calcular el caudal de saturación:

$$S = \frac{E[P] \sigma}{(1 - P_r) \sigma + }$$

- donde:

$$P_r = 1 - (1 - \tau)^n$$

$$P_r P_s = n \tau (1 - \tau)^{n-1}$$

- $\sigma$  es el tamaño de ranura (cte.)

- $E[P]$  es el tamaño medio de paquete

- En modo básico:

$$T_c^{bas} = H + E[P] \cdot \tau$$

$$T_c^{bas} = H + E[P] \cdot \tau$$

- Con RTS/CTS:

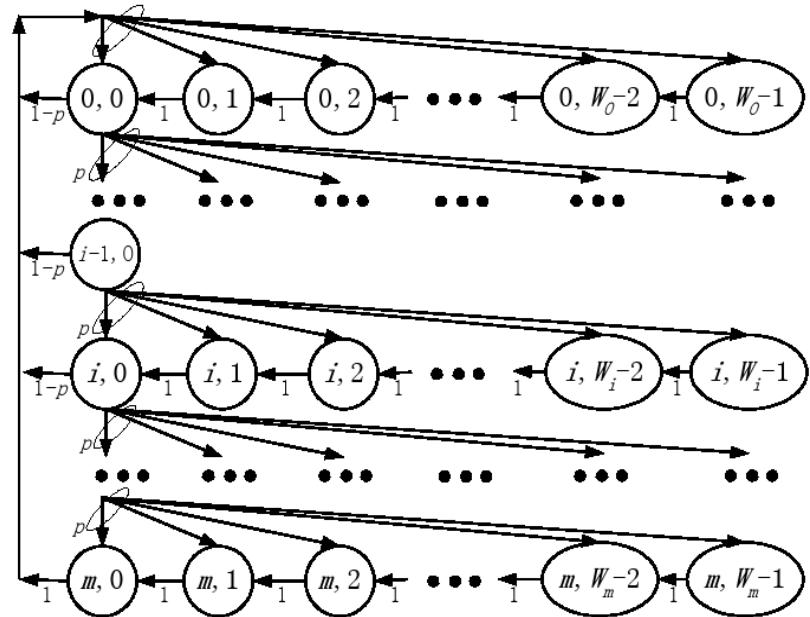
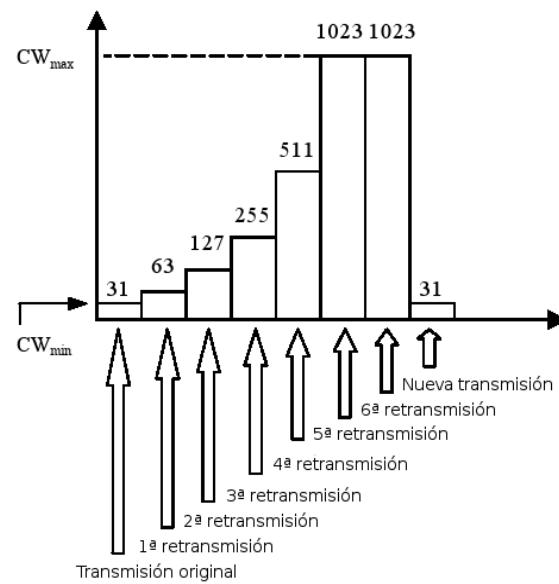
$$T_c^{cts} = RTS + R \cdot S + S \cdot S$$

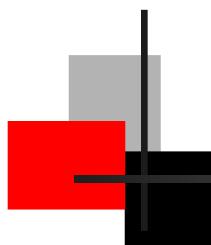
$$T_c^{cts} = RTS + Dif$$

# Análisis de prestaciones. Otros modelos basados en Bianchi



- Número de retransmisiones finito: Wu et al. (2002) y Chatzimisios et al. (2002)

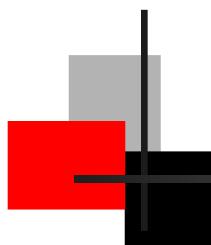




# *Análisis de prestaciones. Otros modelos basados en Bianchi*



- **Condición de medio ocupado:** Ziouva y Antonakopoulos (2002) con interpretación discutible del estándar, por mantener hipótesis de tráfico saturado, y finalmente Duffy et al. (2005) con tráfico no saturado.
- **Canal no ideal:** Chatzimisios, Boucouvalas y Vitsas (2003), sin considerar la posibilidad de corrupción de ACKs, y finalmente Dong y Varaiya (2005) incluyendo esa y otras mejoras.



# **Análisis de prestaciones. Otros modelos basados en Bianchi**



- **Tamaño de paquetes variable:** Chen y Li (2004) introducen el tamaño de paquetes como una función estadística y modelan las prestaciones para el modo mixto (RTS/CTS con RTSThreshold).
- **Redes multisalto:** Barowski y Biaz (2005) aportan un modelo tridimensional de Markov, incluyendo en los estados el número de paquetes en cola e introduciendo en el modelo la tasa de llegada de paquetes al MAC.



# *Análisis de prestaciones. Segundo modelo de Bianchi*

- En 2005, Bianchi y Tinnirello abandonan la matemática basada en cadenas bidimensionales de Markov y combinan la teoría de la probabilidad condicional con cadenas unidimensionales de Markov.
  - Recogen todas las mejoras en el modelado del MAC de otros autores, e introducen formulación matemática para calcular el retardo medio y la probabilidad de descarte de tramas por exceso de retransmisiones. **Modelo prácticamente perfecto.**
  - Corrige la notación:  ,  $i = (1, \dots, R)$
  - Redefine la ranura: es el tiempo entre dos decrementos en el retroceso binario exponencial de una estación que no transmite.

# Análisis de prestaciones. Segundo modelo de Bianchi



- › La primera fórmula del modelo queda:
- › La segunda sigue siendo la misma.
- › Se corrige el tamaño de la ventana de primera transmisión, teniendo en cuenta que sólo la estación que acaba de transmitir puede repetir en la primera ranura si obtiene una ventana de tamaño cero. Eso redefine  $E[P]'$ ,  $T_s'$  y  $T_c'$ . Esto corrige el cálculo del caudal en consecuencia.

$$S = \frac{1}{(1 - P_{rr}) \sigma + }$$

$$B_o = \frac{1}{CW_{min} + 1}$$

$$E[P]' = \frac{E[P]}{1 - B_o}$$

$$T_s' = \frac{T_s}{1 - B_o}$$

$$T_c' = T_c + \sigma$$

# Análisis de prestaciones. Segundo modelo de Bianchi

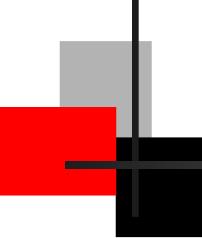


- El retardo medio se calcula empleando el resultado de Little, y la probabilidad de descarte de paquete por exceso de retransmisiones por análisis de probabilidades condicionales.

$$\tau = \frac{n[1 - P(\text{pck drop})]}{S/E}$$

$$P(\text{pck drop}) = \sum_{i=1}^n p_i$$

- La primera fórmula del modelo es directamente aplicable independientemente de la distancia. El planteamiento para el cálculo de los tres parámetros de prestaciones también lo es, aunque con modificaciones sustanciales.
- Sigue sin ser válida la suposición de que todas las estaciones perciben las ranuras igual y a la vez.



# **Análisis de prestaciones. Distancias largas. Modelo de Simó**



- *La mayor parte de los modelos hacen simplificaciones que los hacen inservibles para radios de celda de más de 3 Km.*
- *Bianchi sirve parcialmente para distancias largas:*
  - *Las hipótesis de partida no son menos ciertas por tratarse de distancias largas; alguna es incluso más cierta para un número pequeño de nodos.*
  - *El modelo de Markov no contiene nada que dependa de la distancia (necesario considerar retransmisiones finitas ( $\Delta d \Rightarrow \Delta p \Rightarrow$  probabilidad no nula de Nº retransmisiones máx.).*
  - *La segunda ecuación del sistema se hace falsa.*
  - *p y  $\tau$  no tienen porqué ser iguales para diferentes STAs.*
  - *Otros errores menores.*

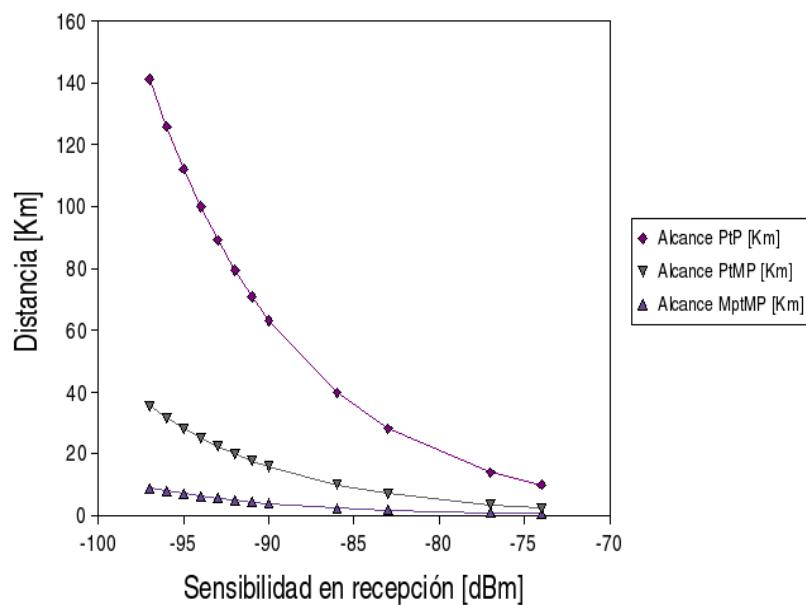
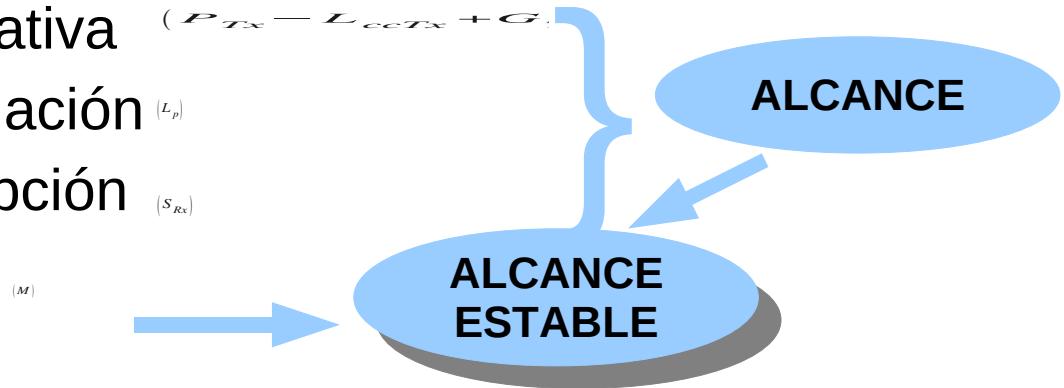


# WiFi para distancias largas



## 1. Límites impuestos por el PHY

- PIRE limitada por normativa
- Las pérdidas de propagación ( $L_p$ )
- La sensibilidad en recepción ( $S_{Rx}$ )
- Margen de estabilidad ( $M$ )



### FCC:

- PtMP:  $P_{Tx} < 30 \text{ dBm}, G_{Tx} < 6 \text{ dBi}$
- PtP:  $P_{Tx} < [30 - (G_{Tx} - 6)/3] \text{ dBm}$  (2.4 GHz)  
 $P_{Tx} < 30 \text{ dBm}$  (5.8 GHz)

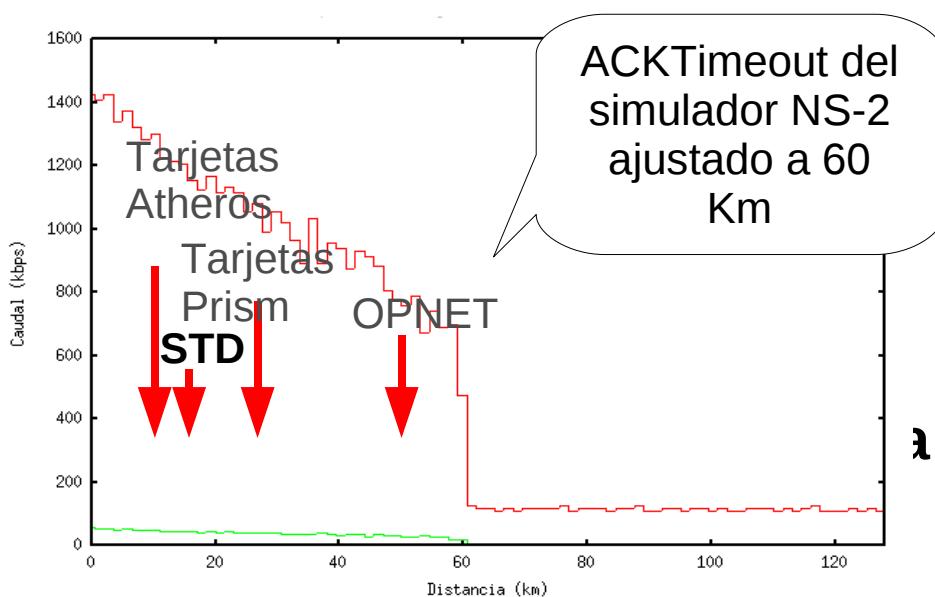
$$\frac{P_{Rx}}{P_{Tx}} = \frac{P_{Tx} - L_{ccTx}}{S_{Rx} + M}$$

# WiFi para distancias largas

## 2. Límites impuestos por el MAC

### ➤ ACKTimeout

- **Modo básico:** Si se supera, todo se retransmite “*ShortRetryLimit*” veces (caudal marginal, máximo retardo. Se puede calcular).
- **RTS/CTS:** Igual con CTSTimeout y “*LongRetryLimit*” (No funciona).



Rate [Mbps]	Max. Dist. [Km]
1	19.8
2	11.4
5,5	6.1
11	4.5
18	2.3
24	2.1
36	1.8
54	1.7

ACKTimeout =

⋮

# WiFi para distancias largas

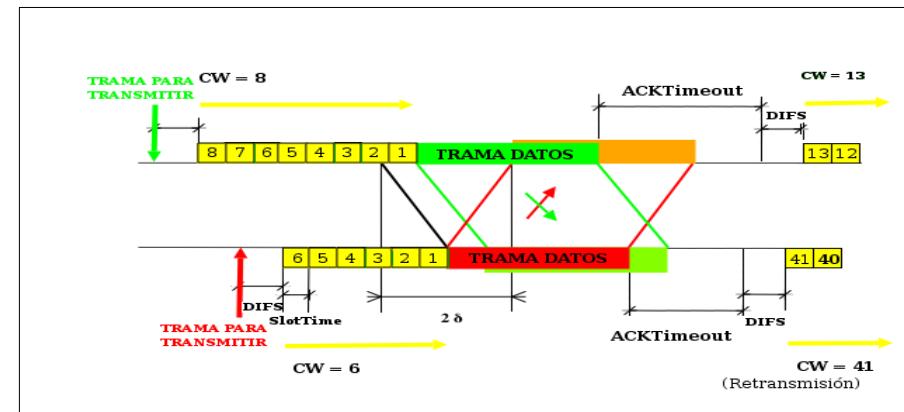
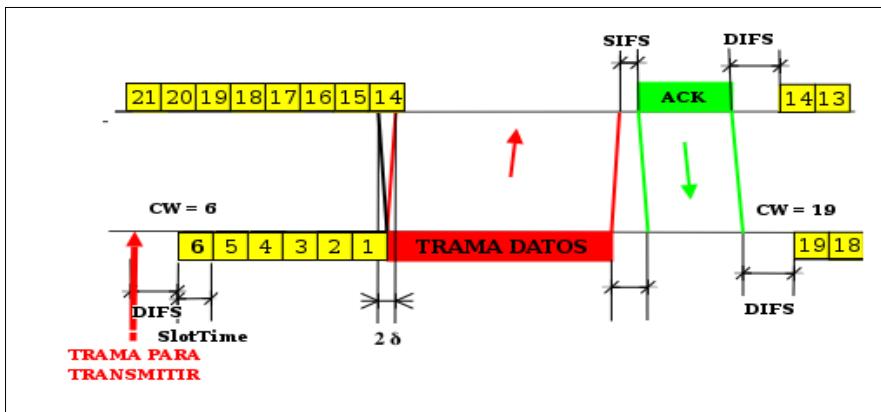
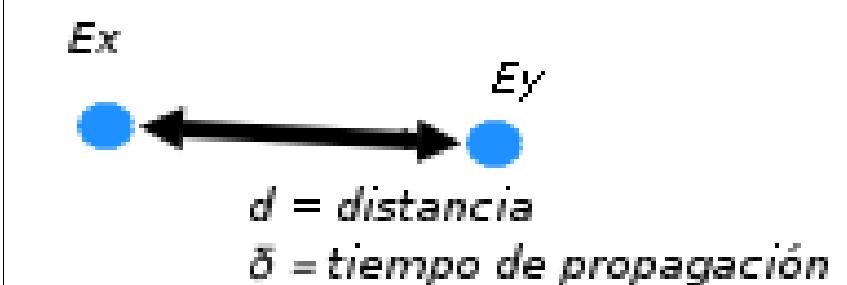


## 2. Límites impuestos por el MAC

- › **SlotTime**: STAs colisionan si TX en la misma ranura (falso si  $d>3Km$ )
- › **Intervalo de Vulnerabilidad ( $IV_{xy}$ )**
- › **IV Normalizado ( $IVN_{xy}$ )**

$$\delta < \sigma/2 : IV_{xy} = \sigma, IVN_{xy} = 1$$

$$\delta > \sigma/2 : IV_{xy} = 2\delta, IVN_{xy} = 2\delta/\sigma$$



# WiFi para distancias largas

## 2. Límites impuestos por el MAC (Nodos ocultos)

- Se dan varios intervalos de vulnerabilidad e invulnerabilidad
  - $iv(\Omega_x)$  (tiempo en que RX en  $E_x \Rightarrow$  Colisión)
  - $ii(\Omega_x)$  (tiempo en que RX en  $E_x \Rightarrow$  Inhibición de TX)
- Ejemplo: Si  $E_{Tx}$  es la STA TX,  $E_{Rx}$  es la RX, y  $E_i$  la interferente:

$$E_{Tx} \in \Omega_i \Rightarrow$$

$$iv(\Omega_{\infty}) = (-\infty, t_0]$$

$$iv(\Omega_{\infty}) = (\min(t_0 + 2\delta, \dots$$

...

Igual se definen  $iv(\Omega_{Tx})$ ,  $ii(\Omega_{Tx})$ ,  $iv(\Omega_{Rx})$ ,  $ii(\Omega_{Rx})$ ,  $iv(\Omega_{rx})$  y  $ii(\Omega_{rx})$

- Con todo ello se puede calcular el tiempo de vulnerabilidad

# Análisis de prestaciones. Distancias largas – M.S.



- Con probabilidades condicionales, para cada STA de la red se llega a:

$$\tau_Q = \frac{2(1 - p_Q)}{(1 - p_Q) \sum_{i=0}^R}$$

- Otras  $n$  ecuaciones recogen la interacción entre las estaciones:
  - Definimos  $\xi_{QDX} = \Pr\{TX(E_Q \rightarrow E_D) \text{ colisione con } TX(E_X)\}$
  - Definimos  $\mu_{QD} = \Pr\{TX(E_Q \rightarrow E_D) \mid TX(E_Q)\}$

$$p_Q = \prod_{D=1, D \neq Q}^n \mu_{Qi}$$

# Análisis de prestaciones. Distancias largas – M.S.



Prob. de que  $IV_{QX}$  se abra justamente en la ranura en que  $E_x$  empieza a TX (único término a distancias cortas)

Prob. de que  $IV_{QX}$  contenga  $j$  principios de ranura

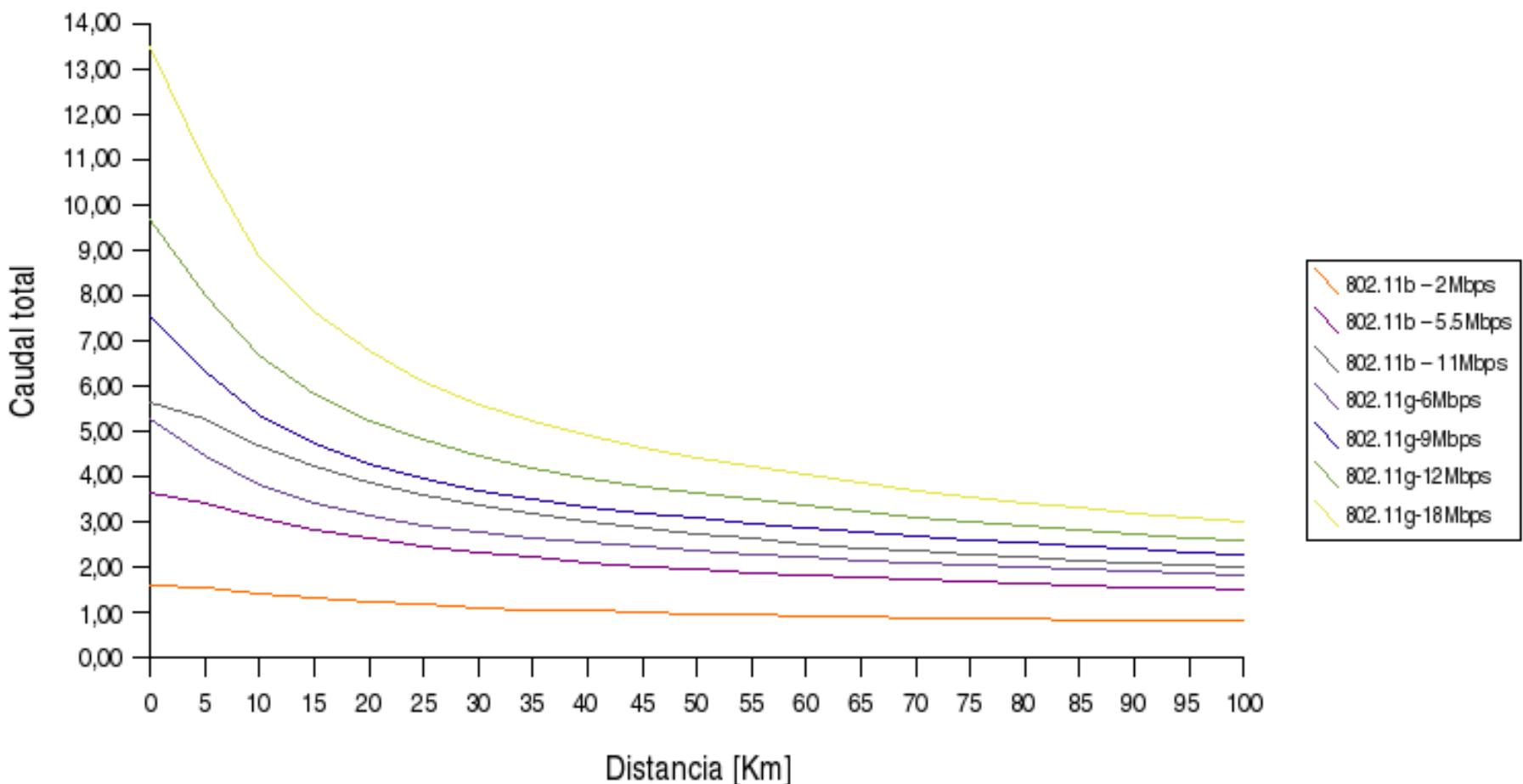
Prob. de último ACK de  $E_Q$  a  $E_x$  dentro de  $IV_{QX}$

Prob. de que ninguna STA distinta de  $E_Q$  y  $E_x$  TX en  $j$  ranuras

# Análisis de prestaciones. Distancias largas – M.S.



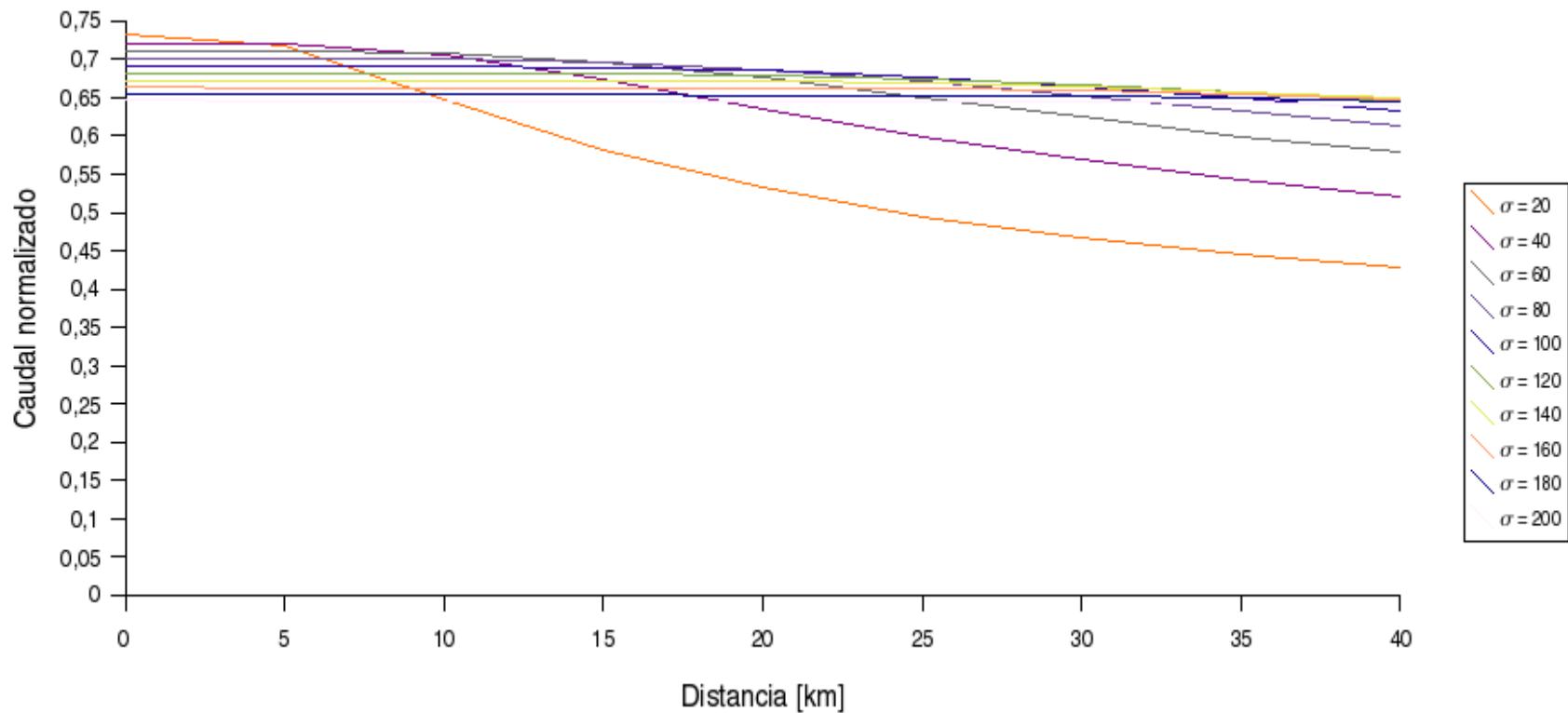
- Caudal sin optimizar para distintas velocidades en función de la distancia:



# Análisis de prestaciones. Distancias largas – M.S.



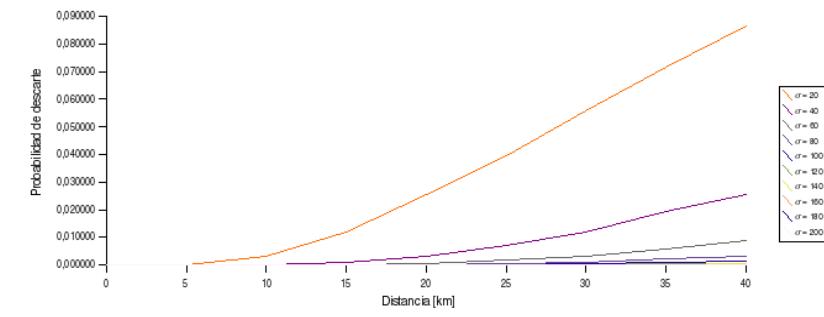
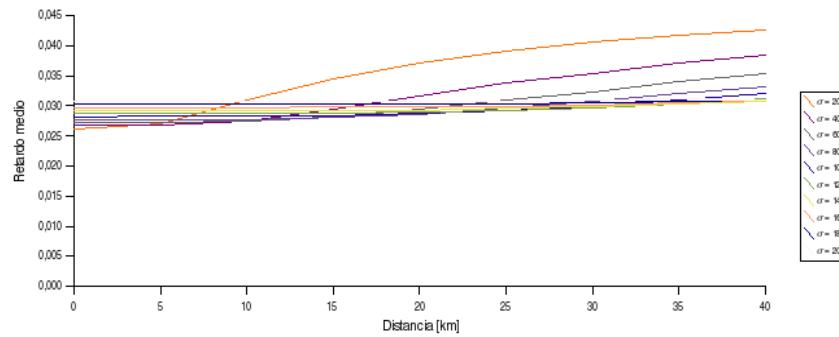
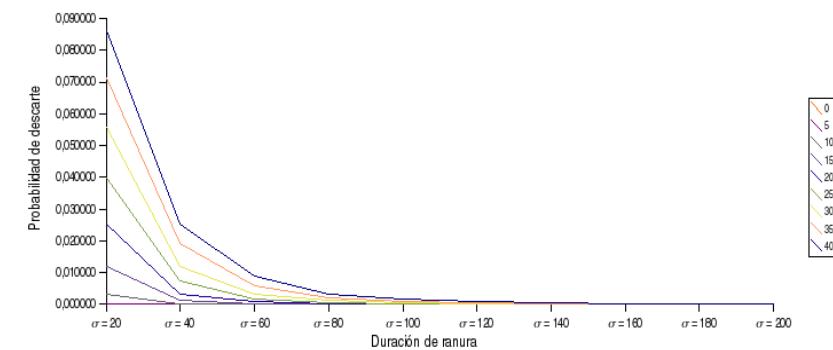
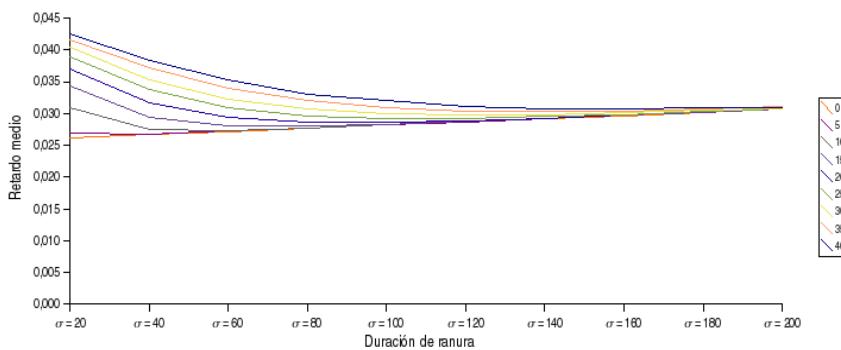
- Optimización (SlotTime):



# Análisis de prestaciones. Distancias largas – M.S.



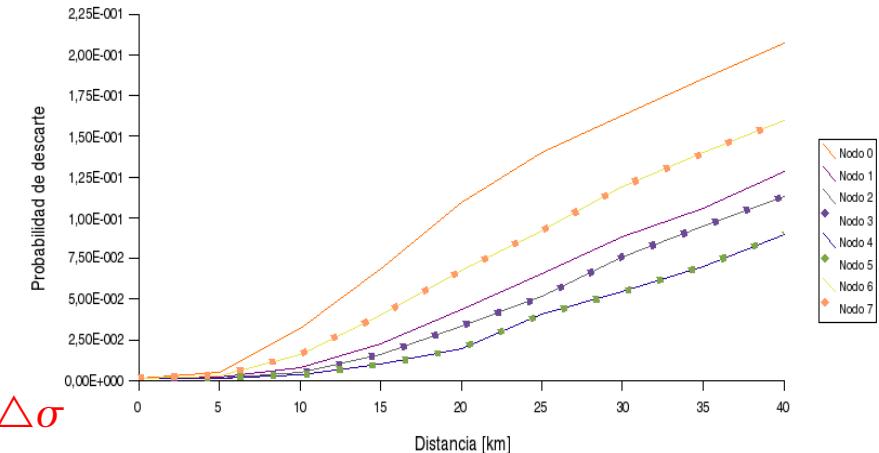
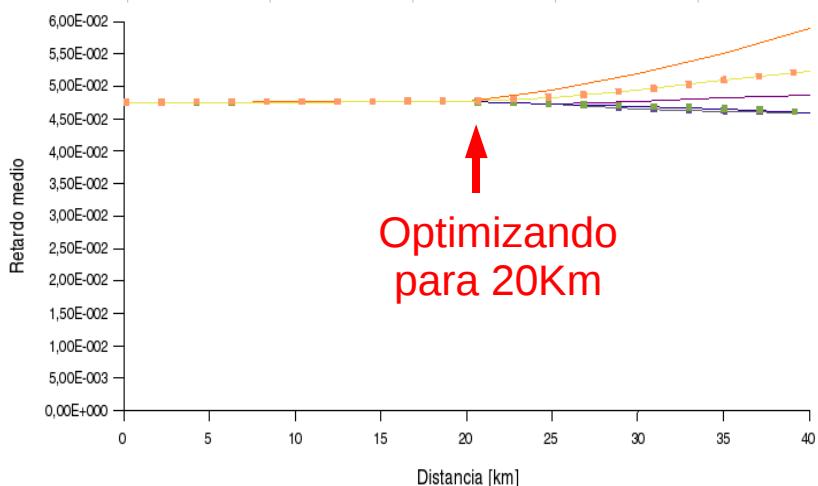
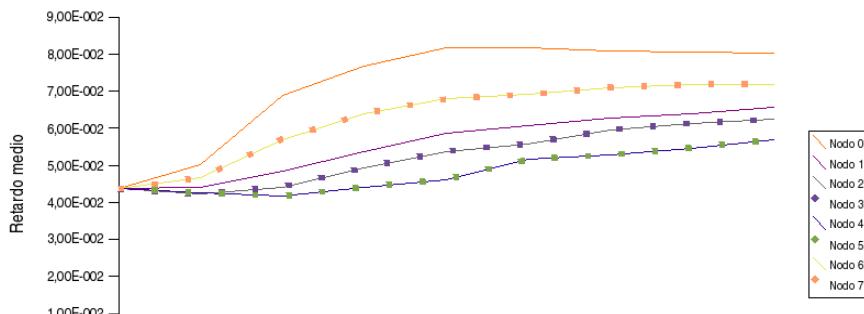
## ➤ Optimización (SlotTime):



# Análisis de prestaciones. Distancias largas – M.S.



## ➤ Optimización (SlotTime):



$\Delta\sigma$



# *WiFi para distancias largas.*

## *Conclusión*



- **Límites de distancia** de IEEE 802.11:
  - el PHY impone límites según el dominio regulatorio, el entorno y el material empleado
    - ⇒ para distancias largas, normativas permisivas como FCC
  - el MAC impone límites con el *ACKTimeout*, y funciona mal a partir de  $\sigma > \partial/2$ 
    - ⇒ Ajuste (no estándar) del parámetro ACKTimeout.
    - ⇒ Ajuste (no estándar) del parámetro SlotTime.
- **La operación eficiente a larga distancia requiere salirse levemente del estándar, pero se mantiene la compatibilidad y la interoperabilidad.**

## Factor principal de diseño

- Carga del AP: en las WLANs se comparte el ancho de banda
  - La utilización del AP se incrementa con el número de clientes asociados.
  - La cantidad de ancho de banda disponible al cliente se reduce.

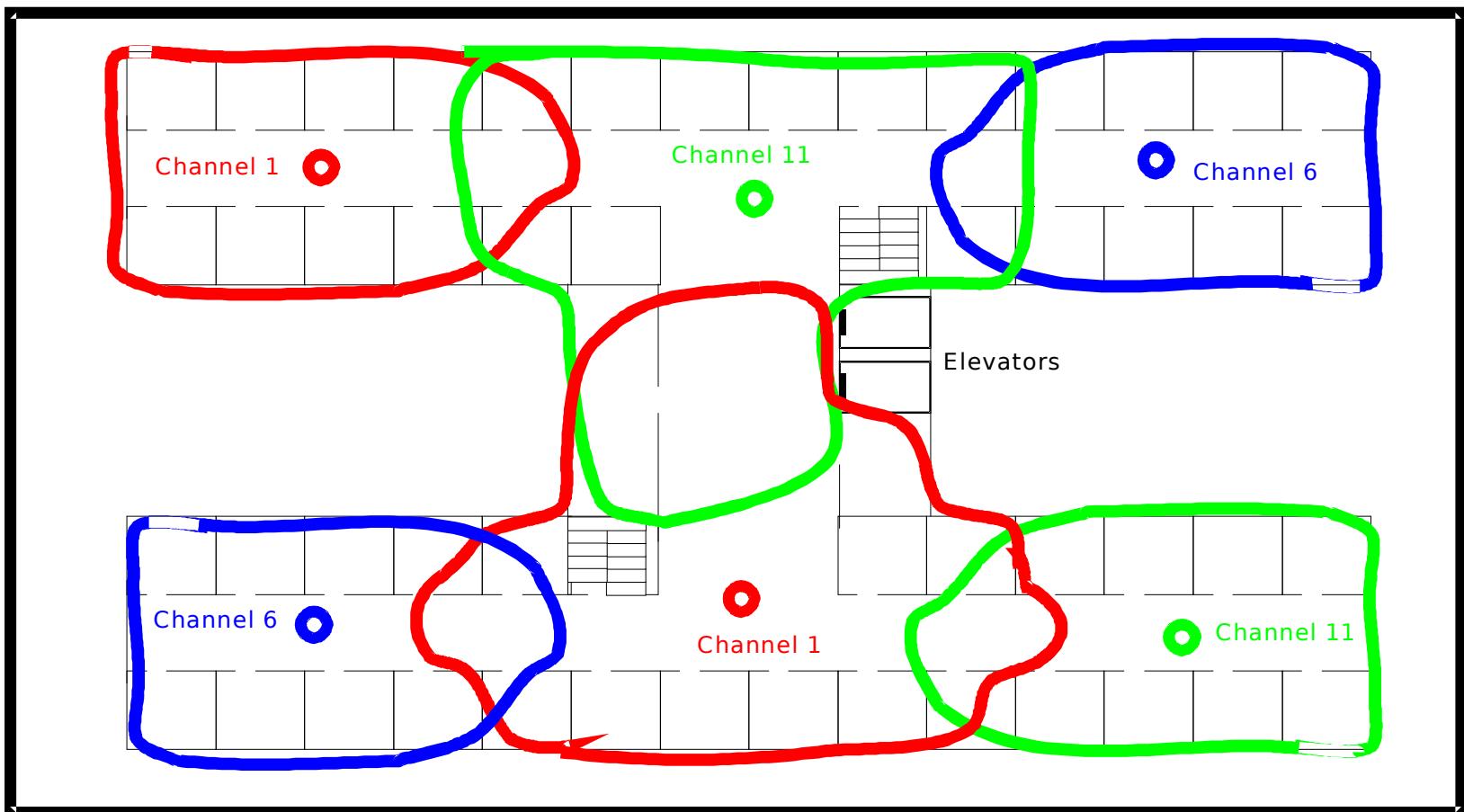
## Consideraciones

- Número de clientes potenciales a la vez.
- Clientes de voz.
- Disponible vs. concurrente.
- Segundos e incluso terceros APs superpuestos.
- Restricciones en la potencia de uso.
- Reducir tamaño de la celda, por tanto el número de clientes concurrentes.

# Diseño de redes. En interiores

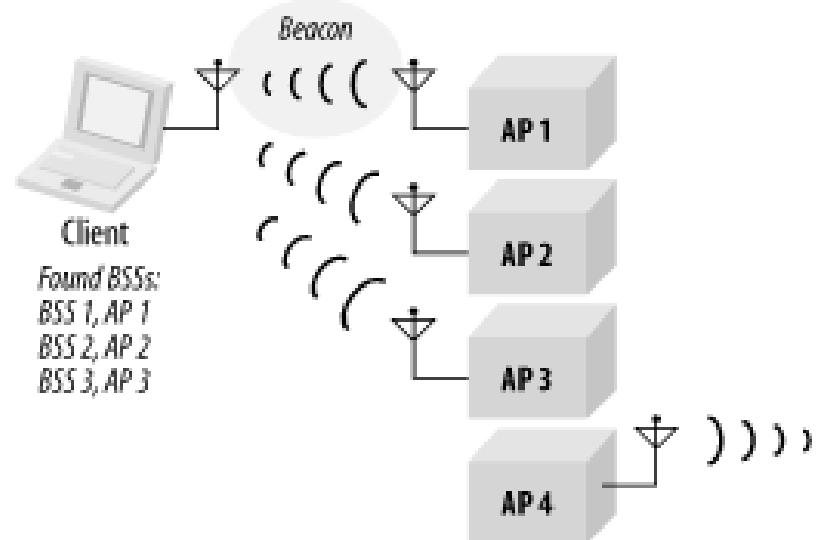


## Cobertura



## Distribución de APs

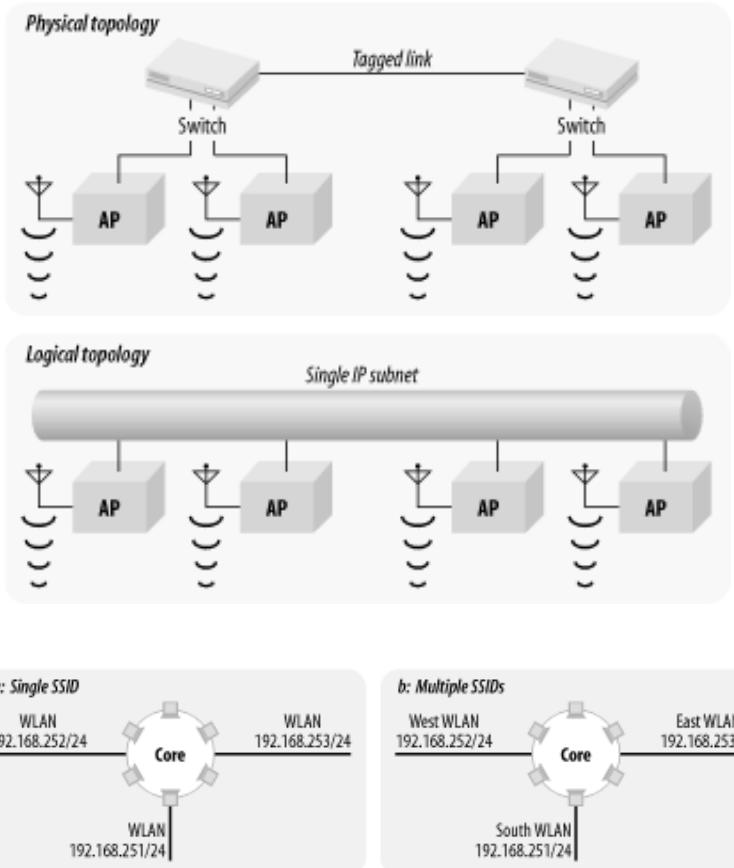
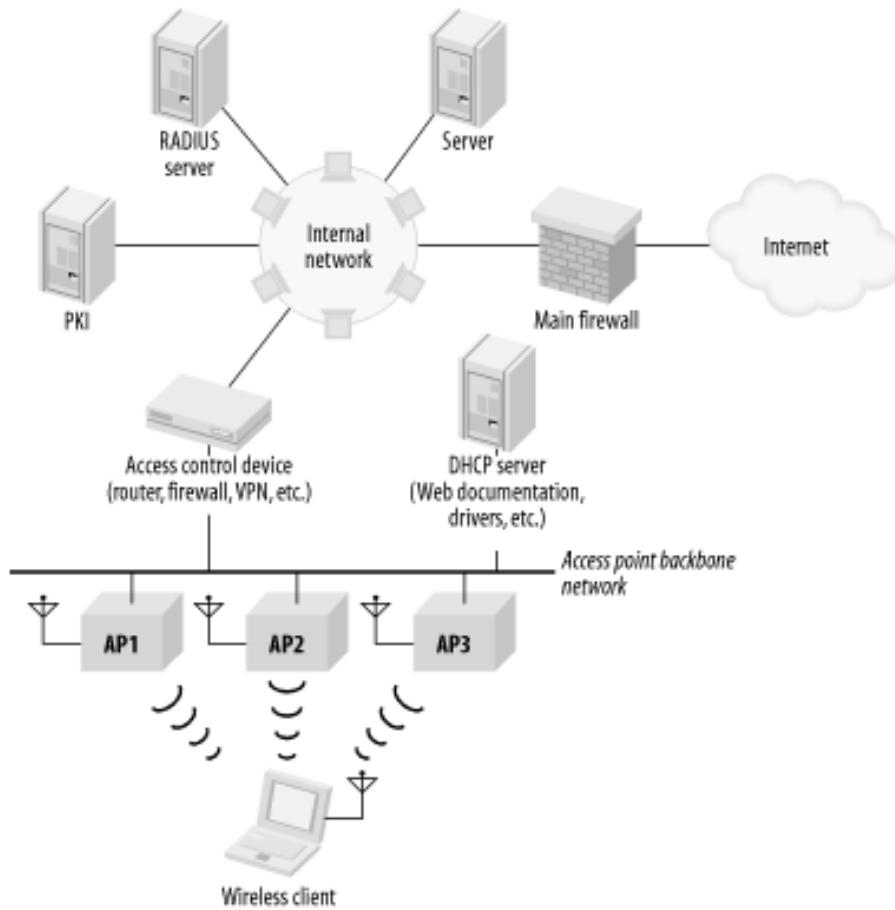
- Elección cuidadosa de los emplazamientos
- Control de superposición de celdas
- Control de potencia de emisión
- “Scan” inicial fácil de descubrir la red o redes desplegadas.



# Diseño de redes. En interiores



## Despliegue típico

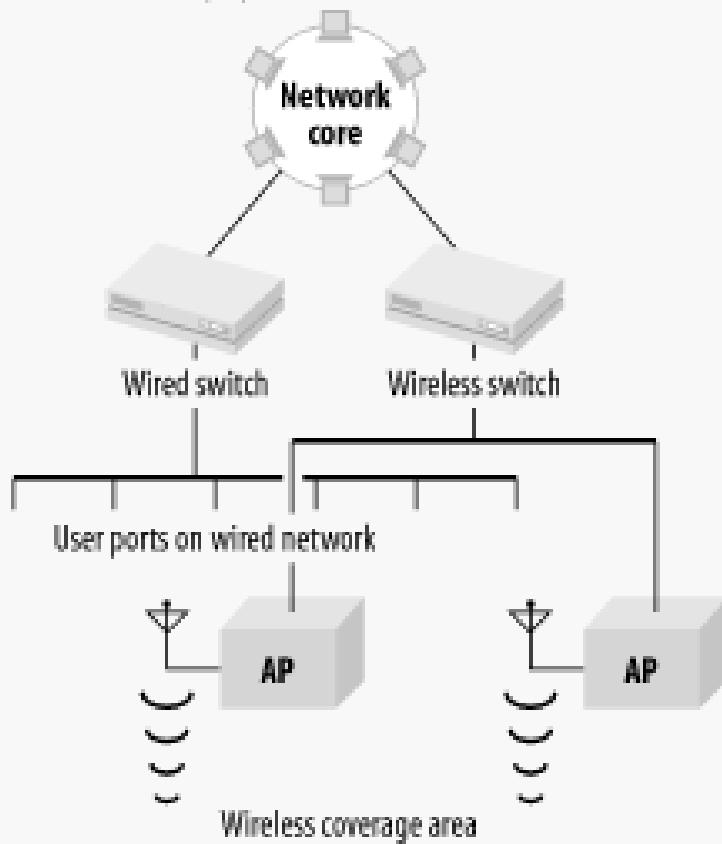


# Diseño de redes. En interiores

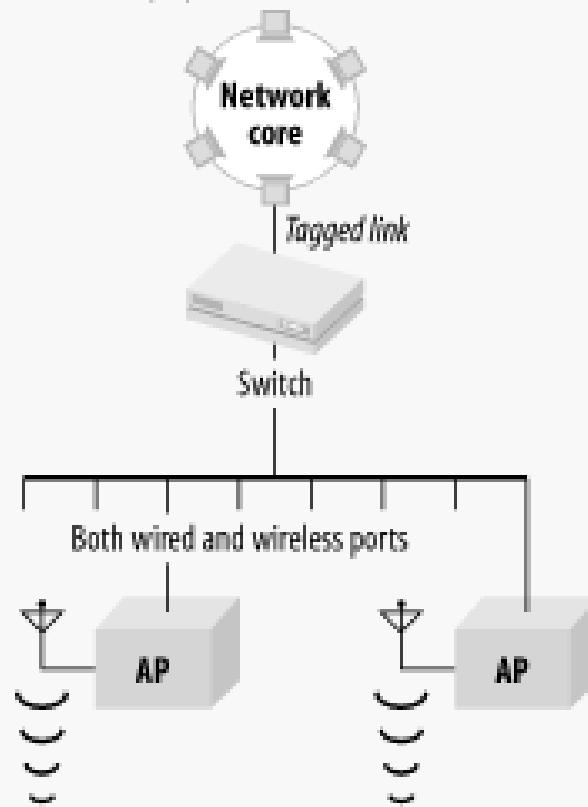


## Despliegue VLAN asociada

a: Non-VLAN deployment

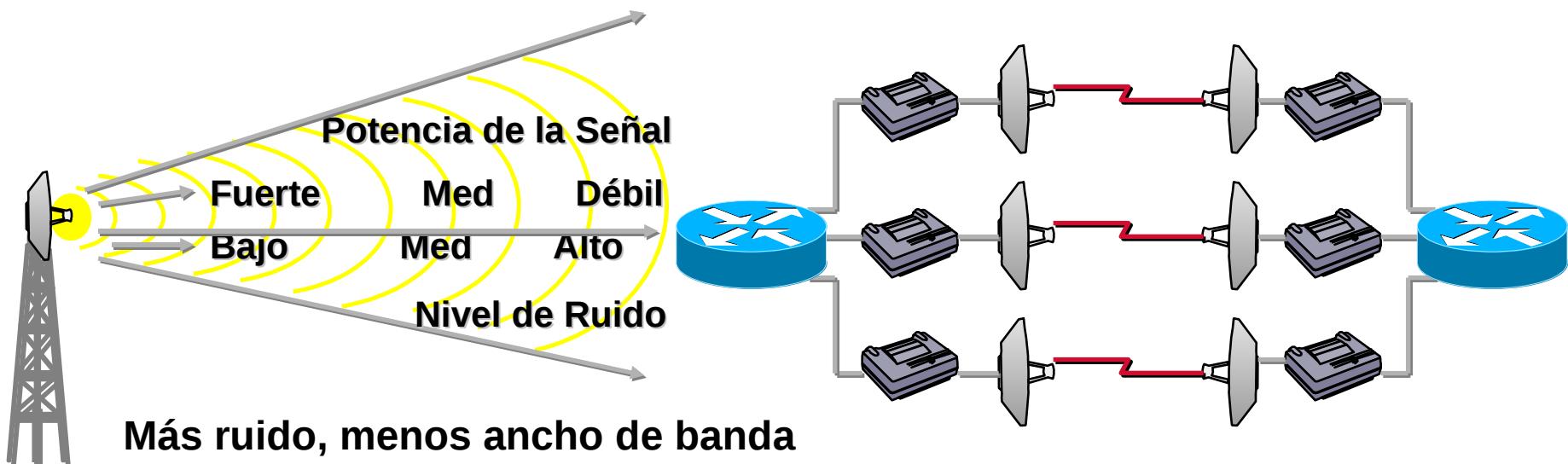


b: VLAN deployment

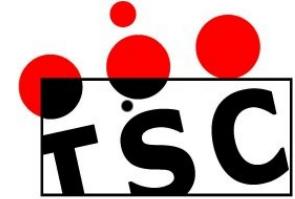


## Compromiso distancia o ancho de banda

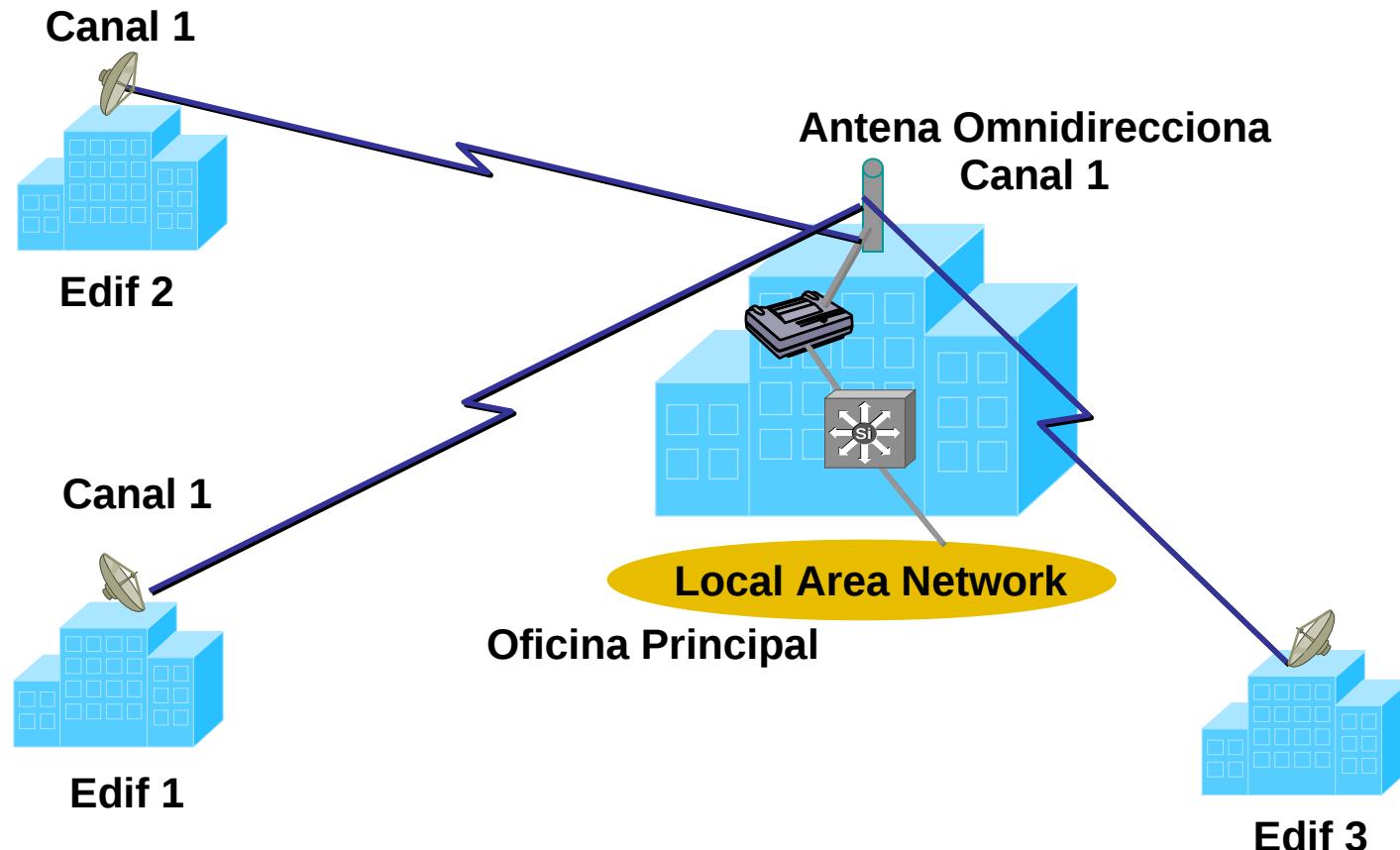
- Mayores distancias posibles a menor velocidad
- Sumando enlaces paralelos, más capacidad



# Diseño de redes. Exteriores



## Enlaces tipo Campus

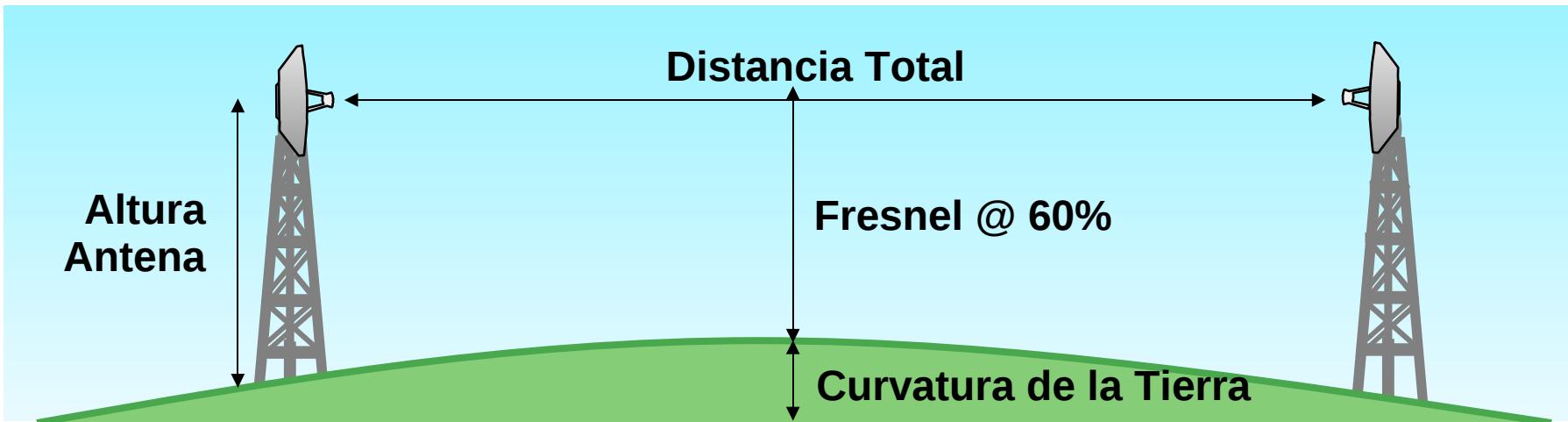


# Diseño de redes. Exteriores



## Zona de Fresnel

- Altura de la antena
  - Consideración de zonas de Fresnel (despejar  $>0.6F_1$ )
  - Enlaces de línea de visión directa de más de 40 km, difíciles sin torres altas o perfiles favorables

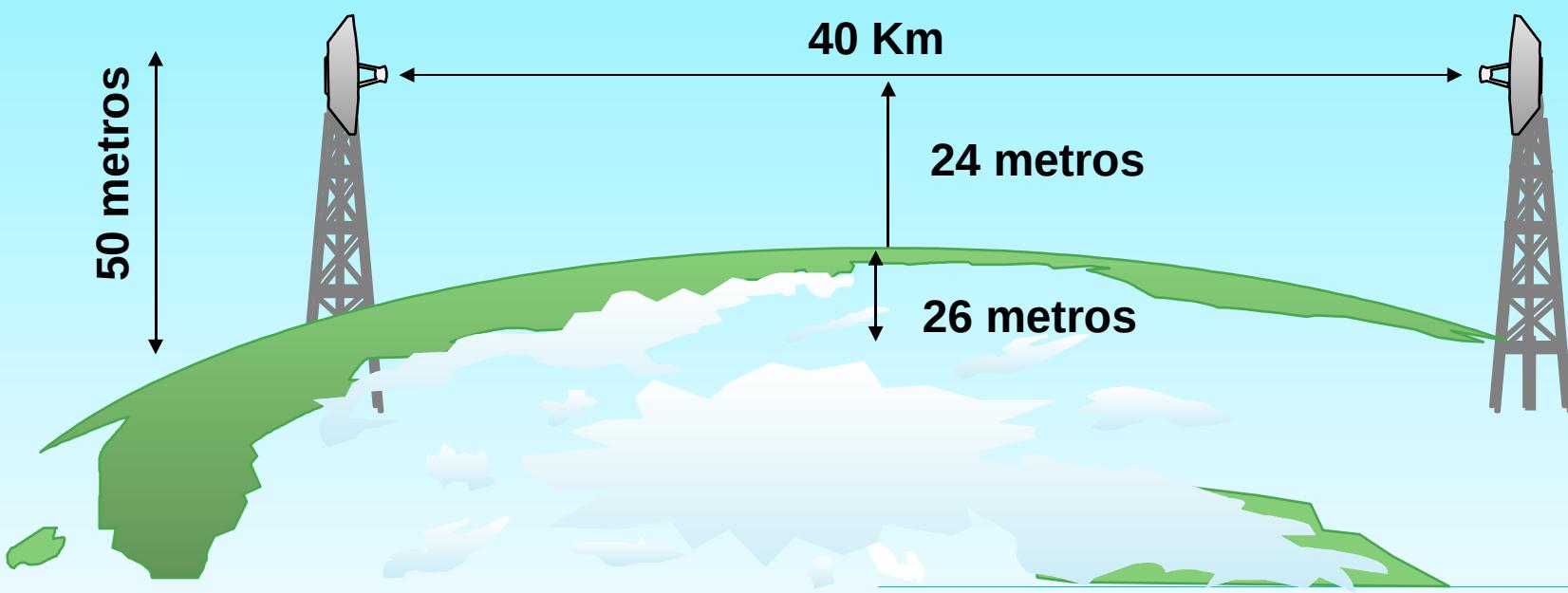


Distancia Total ? Km	Zona de Fresnel ?? m	Curvatura de la Tierra + ? m	Altura Antena ?? m
-------------------------	-------------------------	---------------------------------	-----------------------

# Diseño de redes. Exteriores

## Zona de Fresnel

- Altura de la antena (ejemplo)
  - Distancia Total 40 km
  - Zona de Fresnel 24 m
  - Curvatura Tierra 26 m
  - Altura requerida de la antena 50 m



# Redes ciudadanas



**Mesh!!**

# **Protocolos MAC alternativos sobre PHY's de IEEE 802.11**



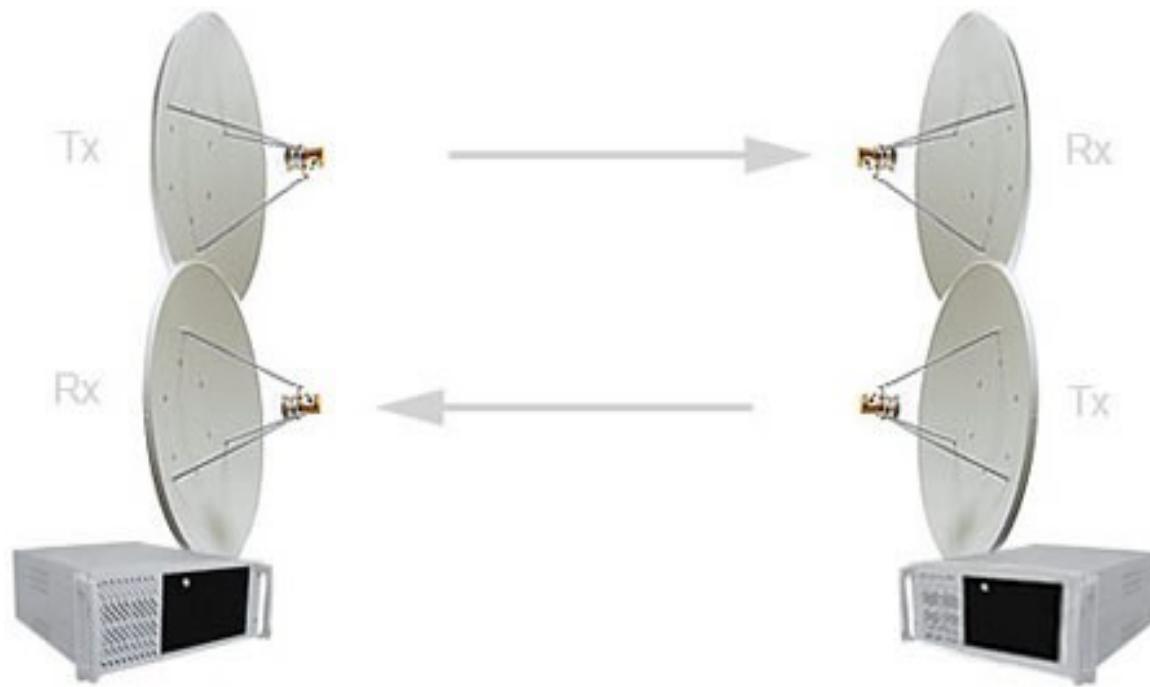
- Alternativas al estándar IEEE 802.11 para distancias largas
  - “WiFi modificado”:
    - ventajas de modos no contemplados en el estándar (e.g. el modo pseudo-IBSS evita particiones que ocurren con IBSS)
    - usos “fraudulentos” del estándar (e.g. MAC alternativo diseñado en software/firmware usando modo multicast para evitar confirmaciones de tramas)
    - asociación de varios transceptores para lograr más ancho de banda o para evitar colisiones separando Tx/Rx.
  - Protocolos totalmente diferentes
    - TDMA: WiLD-MAC, 2P
    - Otros propietarios: Nstreme, Turbocell, WORP, ...

# *Protocolos MAC alternativos... Mikrotik nstreme*



- Diseñado para uso eficiente del canal en distancias grandes
- Para PtP y PtMP
- Características:
  - Sondeo de clientes
  - Overhead de protocolo muy reducido
  - Independencia de prestaciones con la distancia
  - Ajustes dinámicos en funciónl de uso y tipo de tráfico
- Se dispone de dos interfaces en cada extremo (nstreme2), se puede separar el tráfico de ida y el de vuelta.
- Marcas: Mikrotik (barata), Lobometrics (mejor terminada)

# Protocolos MAC alternativos... *Mikrotik nstreme*



# **Protocolos MAC alternativos...**

## **TIER WiLD-MAC**



- Diseñado para uso eficiente del canal en distancias grandes, teniendo en cuenta múltiples interfaces si las hay.
- Para PtP y PtMP
- Características:
  - TDMA
  - Overhead de protocolo alto
  - Independencia de prestaciones con la distancia
  - Si hay múltiples interfaces, se sincronizan las transmisiones
    - Se evitan colisiones
    - Se facilita la planificación de canales (se usa el mismo)
  - EXPERIMENTAL! Producto derivado producido por INTEL