Redes y Comunicaciones Avanzadas

Curso para la obtención del Diploma de Informática Militar

Universidad Rey Juan Carlos

César Cáceres Taladriz (cesar.caceres@urjc.es)
Escuela Técnica Superior de Ingeniería Informática

Contenidos

Universidad Rey Juan Carlos

1. Redes y enlaces inalámbricos
   - Redes LAN inalámbricas 802.11 (Wifi)
   - Redes inalámbricas personales 802.15 (Bluetooth o Zigbee)
   - Redes móviles
   - Redes vía satélite
2. Redes definidas por software (Software Defined Networks)

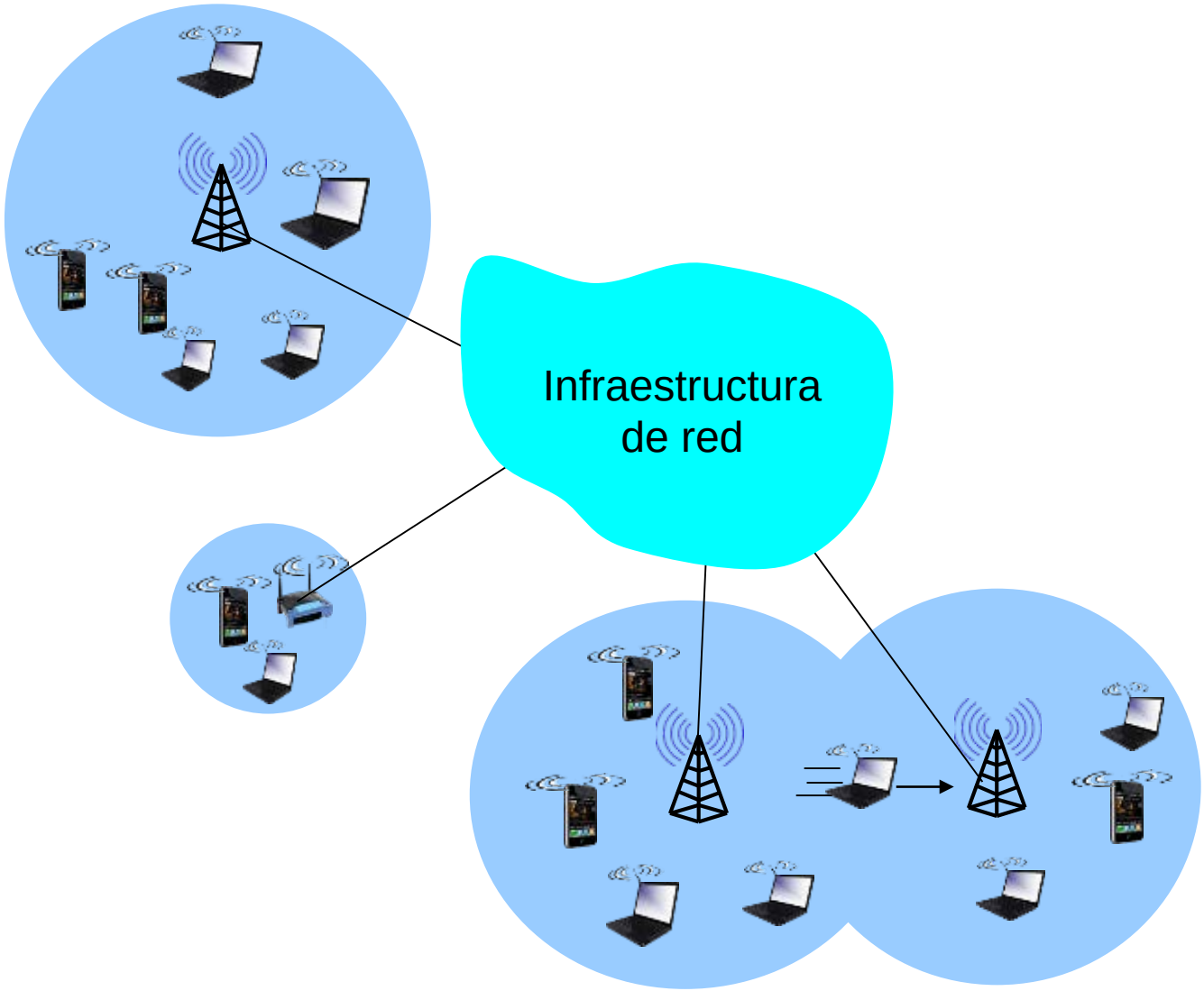
Materiales basados principalmente en:

- Kurose-Ross. Redes de Computadoras. 7ª ed. 2017. ©

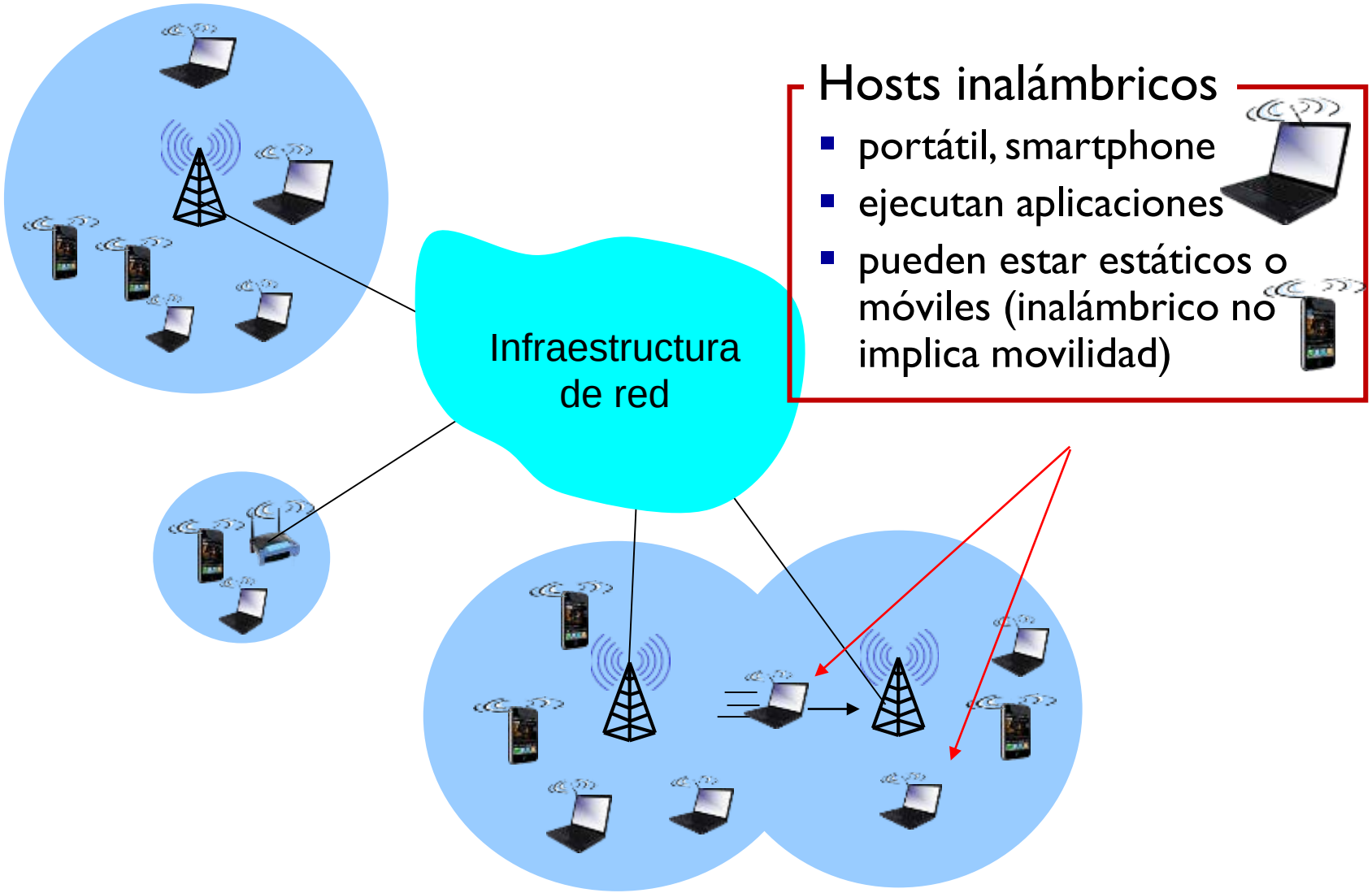
Motivación

Universidad Rey Juan Carlos

- Evolución de las comunicaciones inalámbricas y móviles
- Aumento del número de líneas y dispositivos
- Dispositivos personales (Body Area Network)
- Movilidad en la comunicación es una commodity
- Movilidad extrema (satélite) para situaciones extremas
- Flexibilidad en la configuración de las redes (Software Defined Networks)


Infraestructura
de red

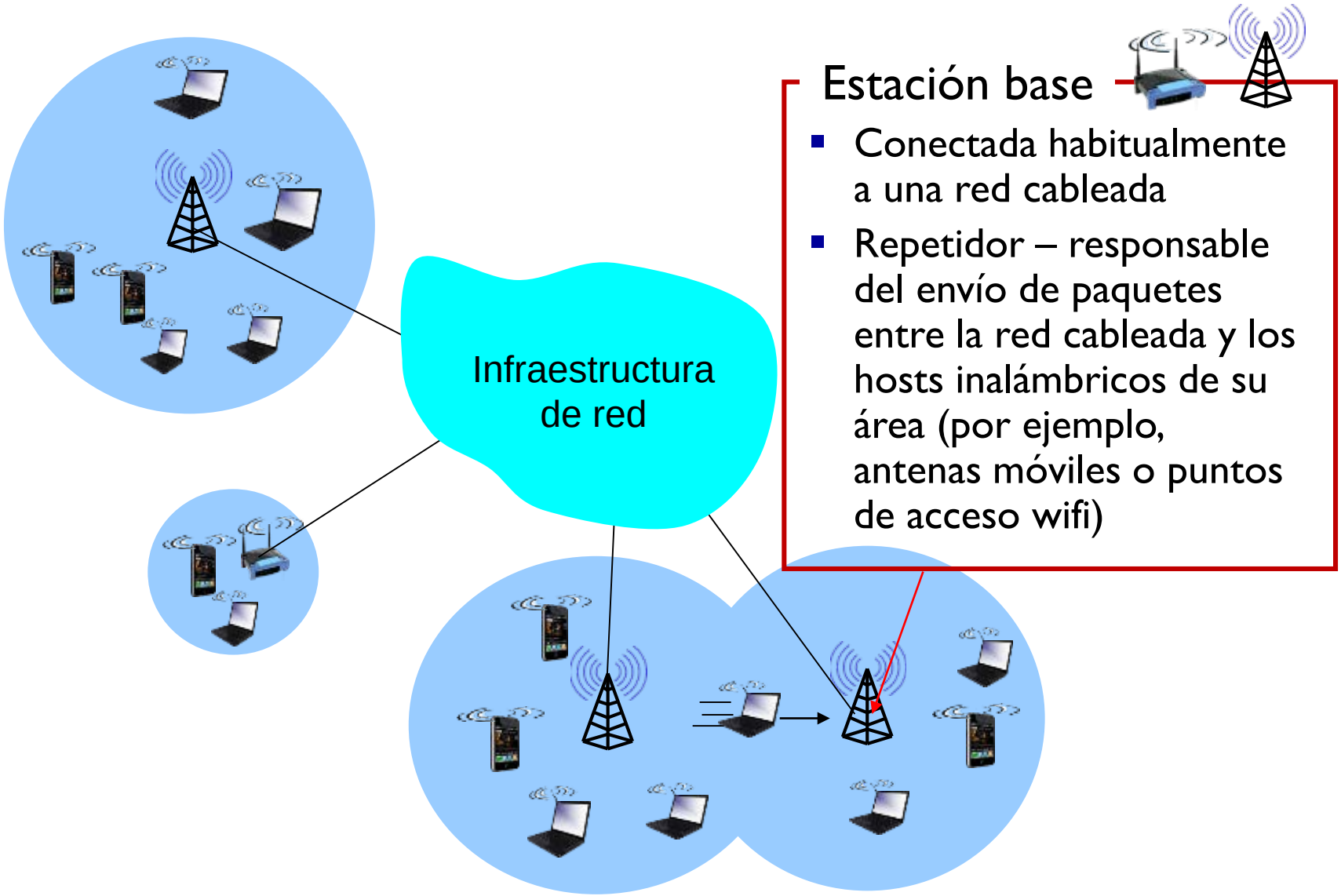
Elementos de una red inalámbrica



Hosts inalámbricos

- portátil, smartphone
- ejecutan aplicaciones
- pueden estar estáticos o móviles (inalámbrico no implica movilidad)

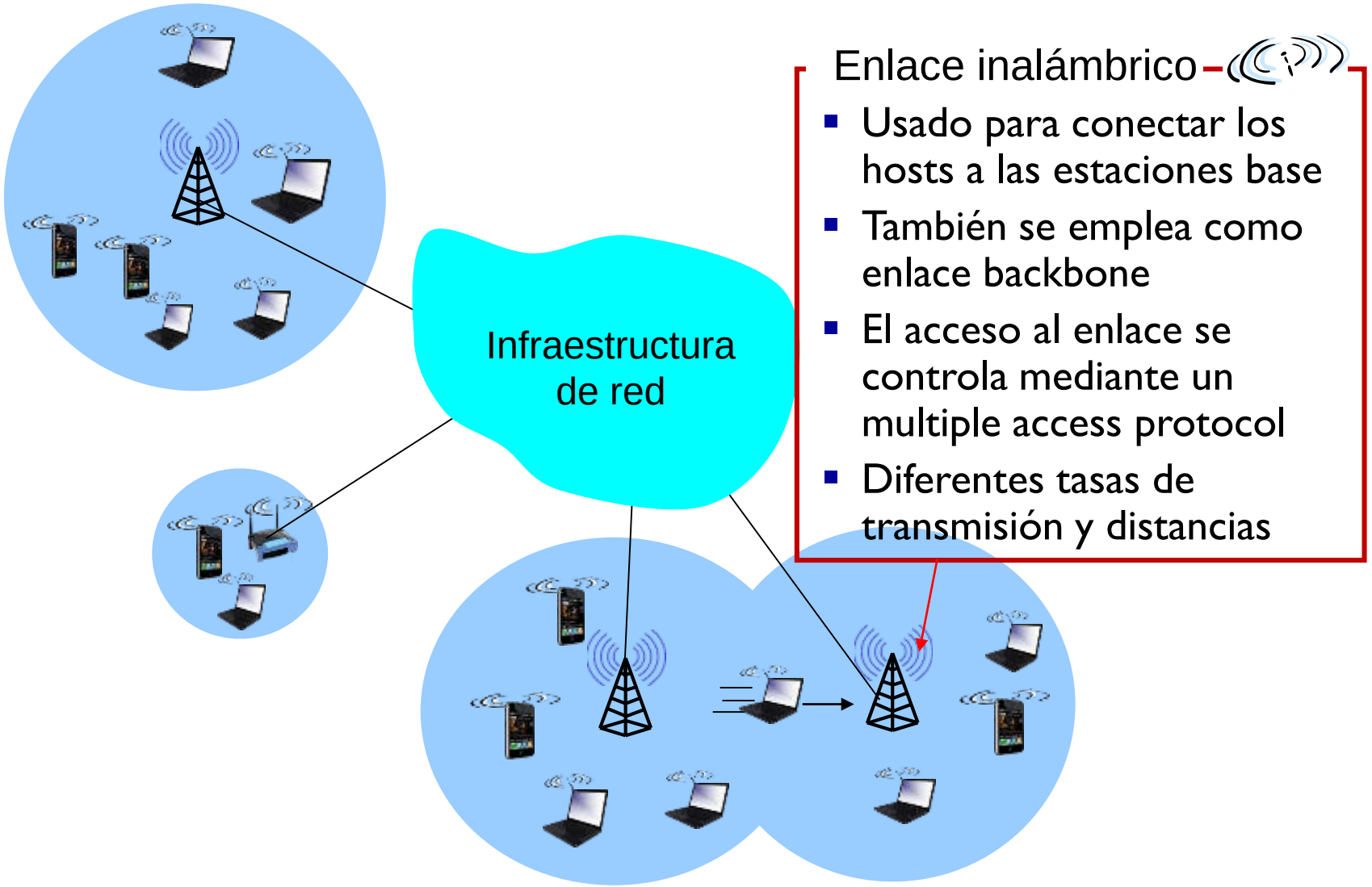
Elementos de una red inalámbrica



Estación base

- Conectada habitualmente a una red cableada
- Repetidor – responsable del envío de paquetes entre la red cableada y los hosts inalámbricos de su área (por ejemplo, antenas móviles o puntos de acceso wifi)

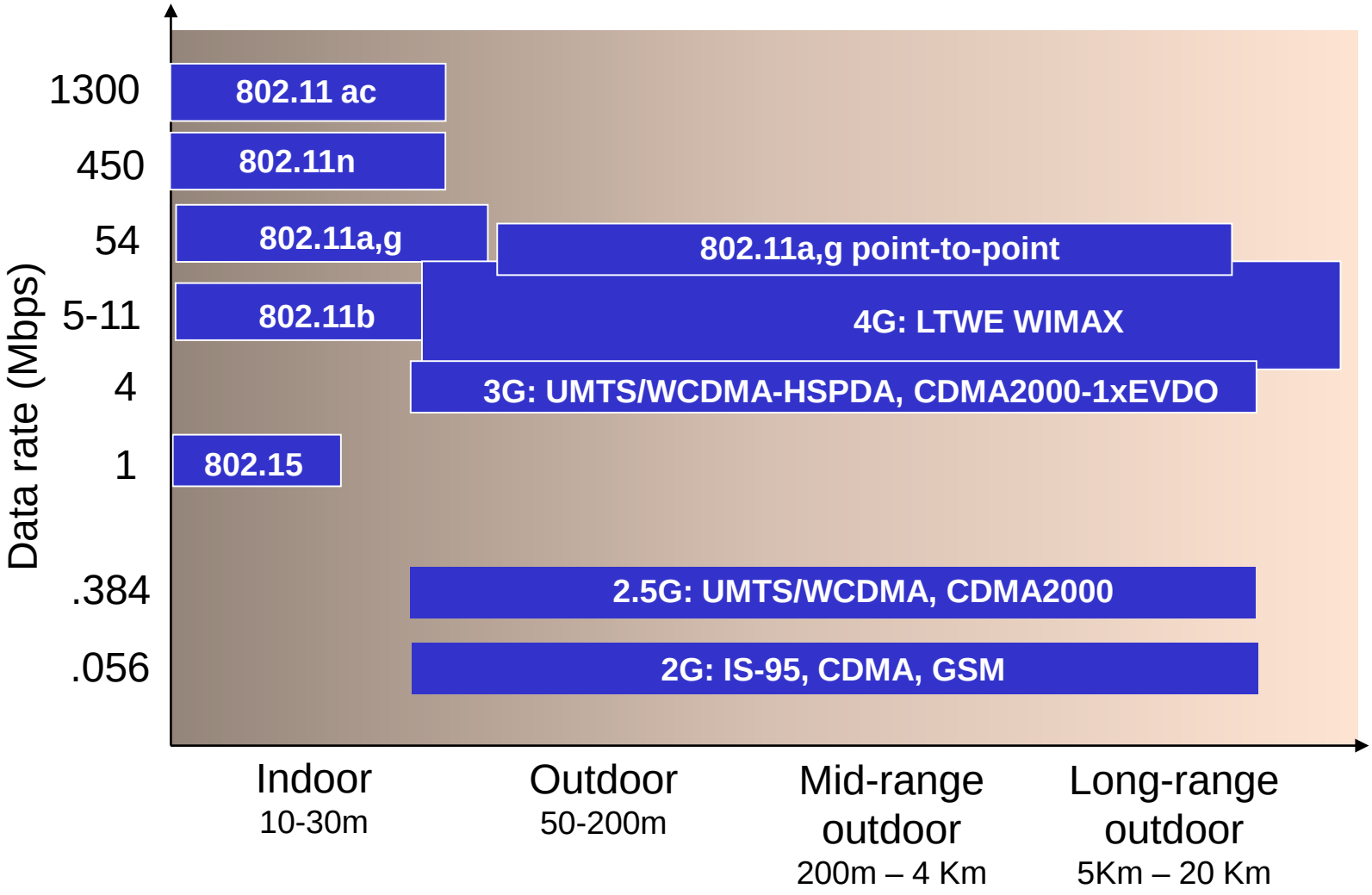
Elementos de una red inalámbrica



Enlace inalámbrico

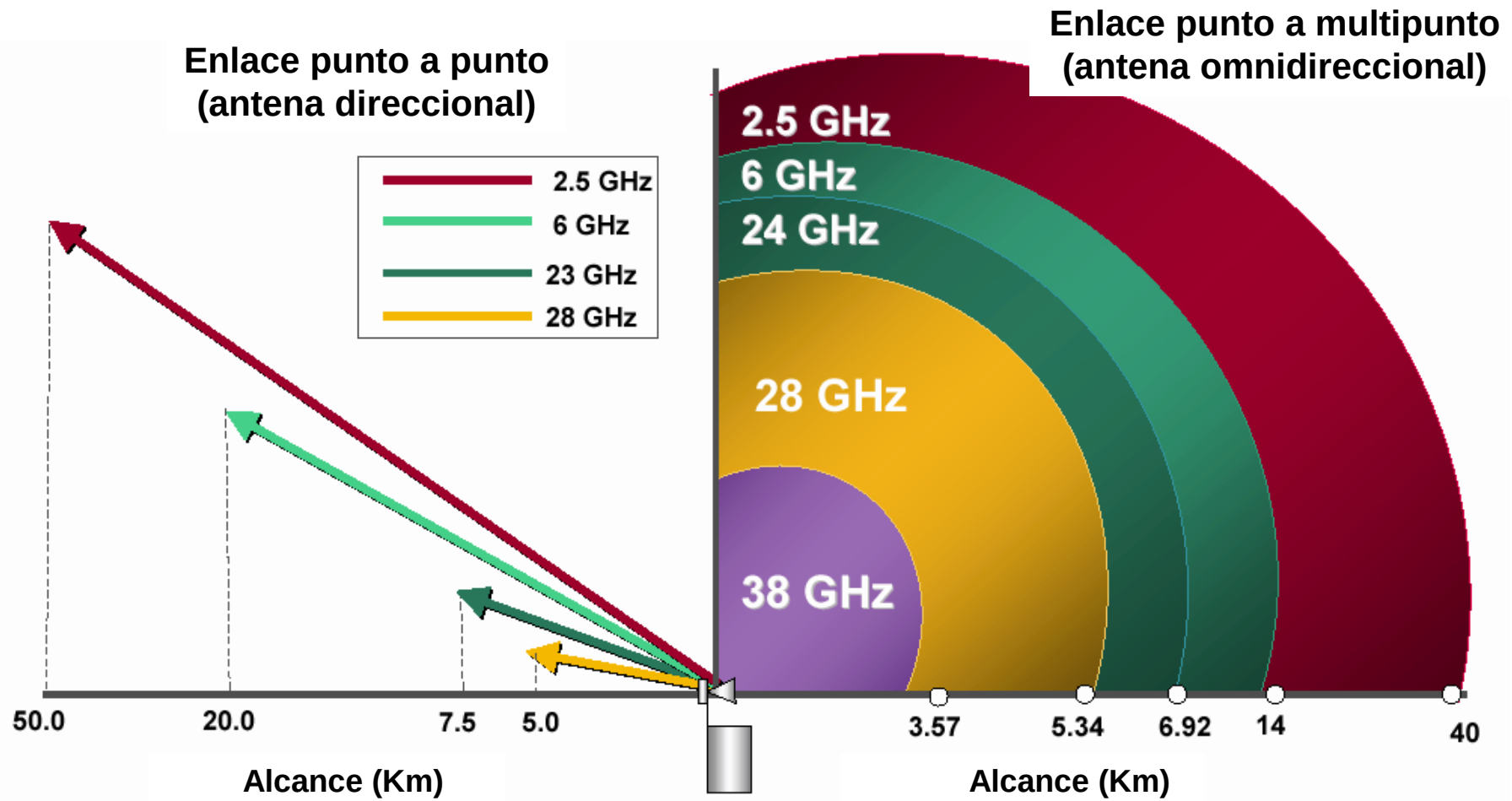
- Usado para conectar los hosts a las estaciones base
- También se emplea como enlace backbone
- El acceso al enlace se controla mediante un multiple access protocol
- Diferentes tasas de transmisión y distancias

Características de los enlaces inalámbricos



Características de los enlaces inalámbricos

Universidad Rey Juan Carlos

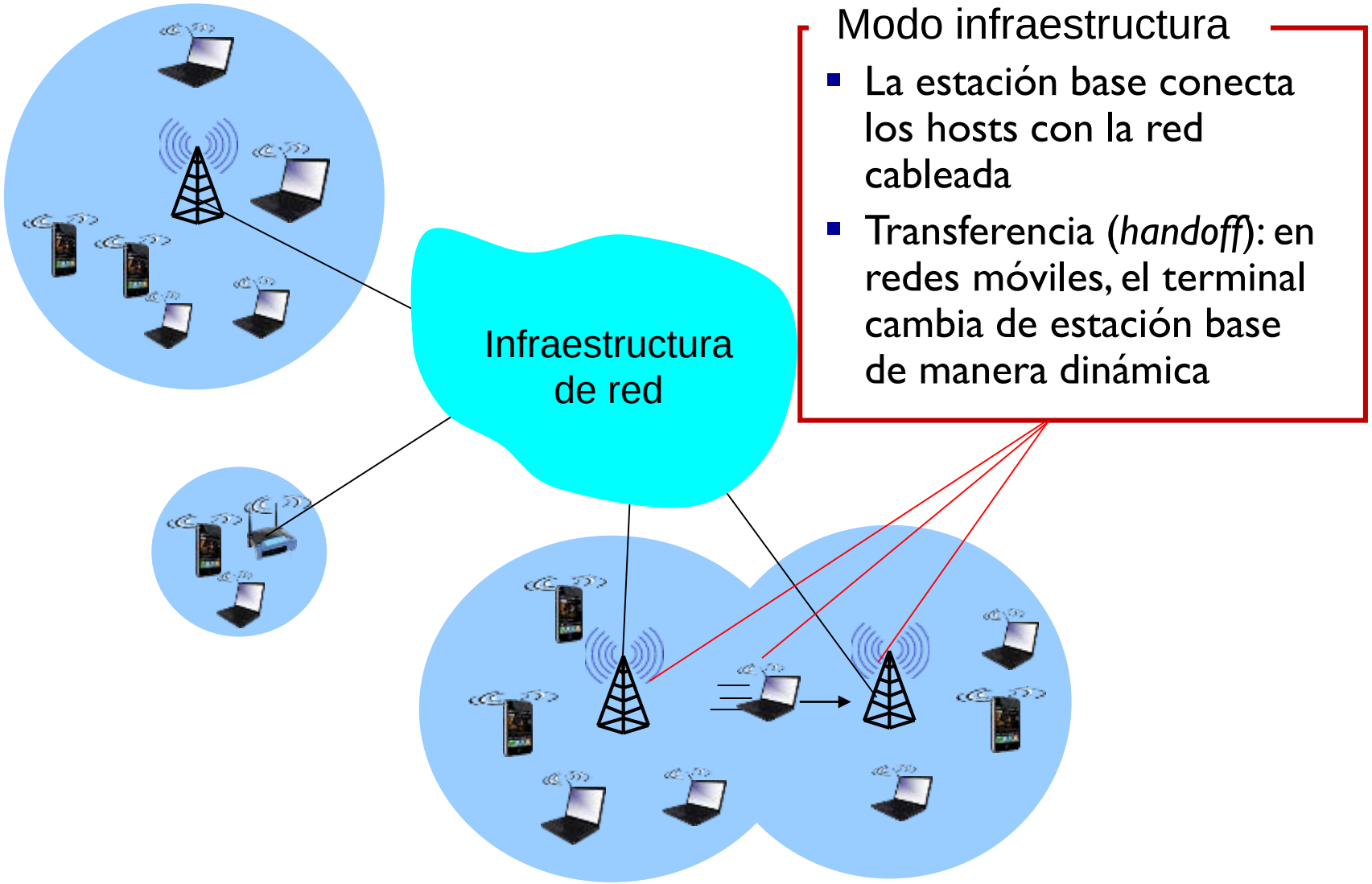


Características de los enlaces inalámbricos

Tipo de red	WWAN (Wireless WAN)	WLAN (Wireless LAN)	WPAN (Wireless Personal Area Network)
Estándar	GSM/GPRS/UMTS HSPA/LTE	IEEE 802.11	IEEE 802.15 (Bluetooth)
Velocidad	9,6/170/2000 7200/75000 Kb/s	1-2-11-54-600-9600 Mb/s(*)	721-2000 Kb/s
Frecuencia	0,9/1,8/2,1/1,5/1,8/ 2,6 GHz	2,4 y 5 GHz Infrarrojos	2,4 GHz
Rango	35 Km	70 - 150 m	10-40 m
Técnica radio	Varias	FHSS, DSSS, OFDM	FHSS
Itinerancia (roaming)	Sí	Sí	No
Equivalente a:	Conexión telef. (módem)	LAN	Cables de conexión

(*) Las velocidades bajas (1-2-11 Mb/s) corresponden a las norma 802.11 antiguas

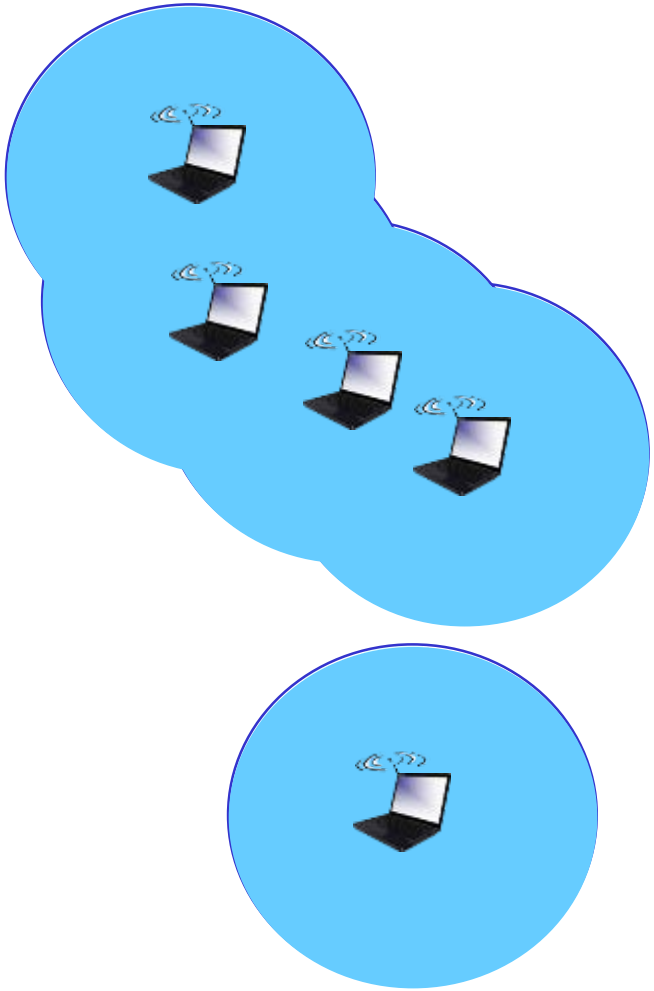
Modos en una red inalámbrica



Modo infraestructura

- La estación base conecta los hosts con la red cableada
- Transferencia (*handoff*): en redes móviles, el terminal cambia de estación base de manera dinámica

Modos en una red inalámbrica



Modo ad hoc

- Sin estaciones base
- Los nodos sólo pueden transmitir a otros nodos dentro de la cobertura del enlace
- Los nodos se organizan en una red y se enrutan entre ellos

Tipos de red inalámbrica

Universidad Rey Juan Carlos

	único salto	múltiples saltos
infrastructura (como APs)	host conectados a una estación base (WiFi, WiMAX, móviles) que los conecta a una red mayor (Internet)	hosts tienen que retransmitir sus mensajes por varios nodos inalámbricos hasta llegar a la red cableada (por ejemplo, redes de sensores o mallas inalámbricas)
sin infrastructura	sin estación base, ni conexión a una red mayor como Internet (Bluetooth o redes ad hoc)	Sin estación base, ni conexión a una red mayor como Internet, pero tienen que retransmitir los mensajes por distintos nodos hasta destino (ejemplos: redes móviles o vehiculares ad hoc, MANET o VANET)

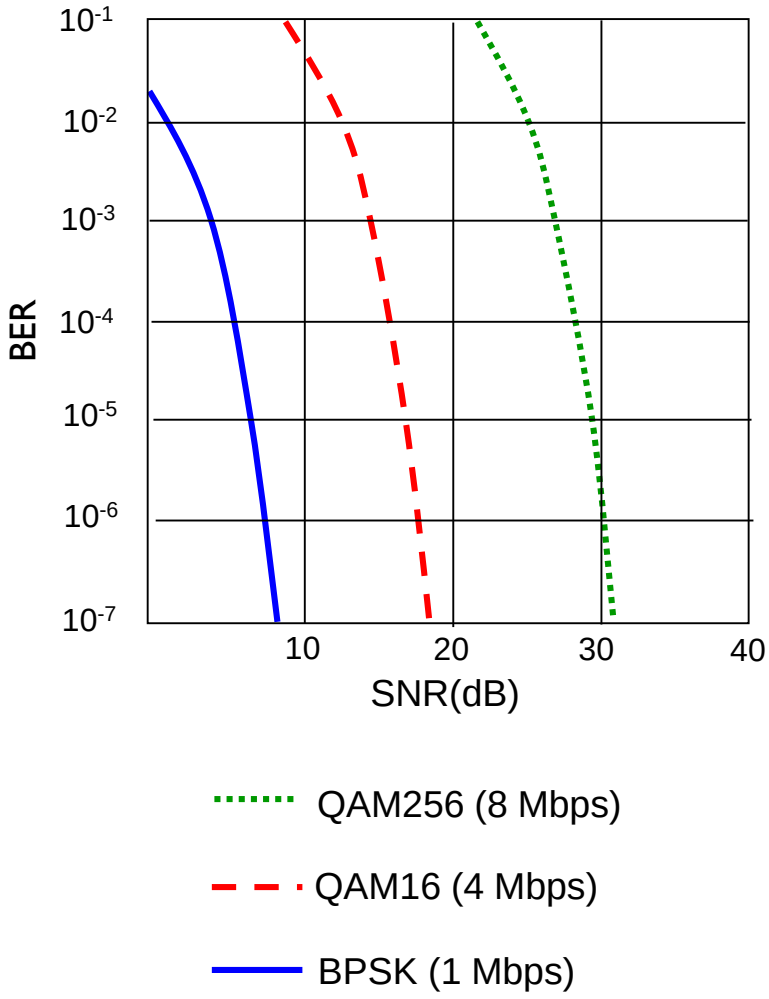
Características de enlaces inalámbricos

Universidad Rey Juan Carlos

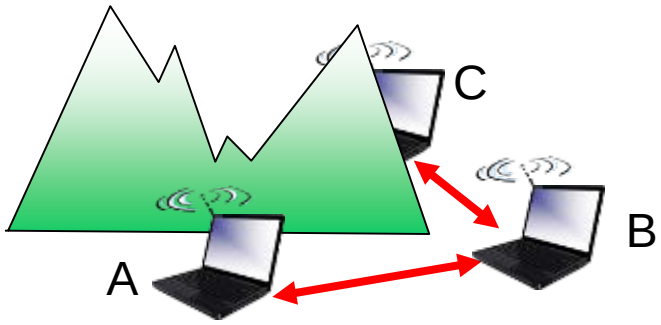
- Atenuación de la señal: la señal electromagnética se atenúa por el medio con la distancia (pérdida de propagación, path loss, o desvanecimiento)
- Interferencias de otras fuentes: distintos dispositivos transmiten en la misma banda de frecuencias y se interfieren (por ejemplo, teléfonos inalámbricos a 2,4GHz y wifi 802.11b, o señales de motores o microondas)
- Propagación multicamino: por rebotes, la señal no llega “limpia” a destino

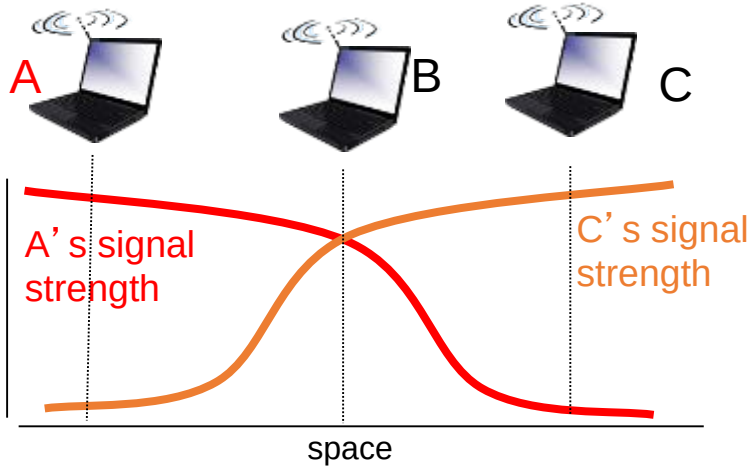
Características de enlaces inalámbricos

- SNR: Signal-to-Noise Ratio (dB)
  - Mejor a mayor SNR, pues es más fácil extraer la señal del ruido
- *BER: Bit Error Rate (probabilidad)*
- *SNR versus BER*
  - *Dada una modulación, a mayor SNR menor BER:* aumento potencia → aumento SNR → disminuyo BER
  - *Dada una SNR:* a mayor velocidad de transmisión, mayor BER. BER es un requisito.
    - Como la SNR cambia con la movilidad, hay que adaptar dinámicamente la técnica de modulación y la velocidad



Problemas añadidos en escenarios inalámbricos por el acceso simultáneo de múltiples emisores y receptores





Problema del terminal oculto

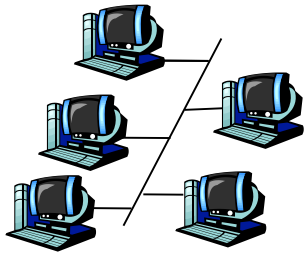
- B y A se escuchan mutuamente
- B y C se escuchan mutuamente
- A y C no se escuchan mutuamente, lo que implica que A y C no sean conscientes de su interferencia en B

Atenuación de la señal

- B y A se escuchan mutuamente
- B y C se escuchan mutuamente
- A y C no se escuchan mutuamente, interfiriendo en B

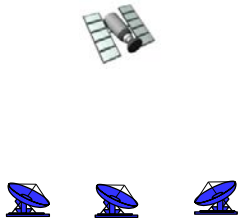
Enlace de acceso múltiple y protocolos

- Dos tipos de enlaces:
- Punto a punto
  - PPP para acceso por marcado (dial-up)
  - Enlace punto a punto entre switch Ethernet y host
- Difusión (broadcast) (medio compartido)
  - Ethernet antiguo
  - HFC de subida
  - 802.11 wireless LAN



cable compartido
(e.g., Ethernet)

RF compartido
(e.g., 802.11 WiFi)



RF compartido
(satélite)

Personas en una fiesta
(comparten el aire)

Protocolos de acceso múltiple

- Un solo canal de difusión compartida
- Dos o más transmisiones simultáneas entre nodos: interferencias
  - colisión: si el nodo recibe dos o más señales al mismo tiempo
- Se desperdicia ancho de banda del canal (durante el intervalo de colisión)
- Un algoritmo distribuido determina cómo los nodos comparten el canal y cuándo un nodo debe transmitir

Protocolo de acceso múltiple ideal

Universidad Rey Juan Carlos

Canal de difusión de tasa de transferencia R bps

1. Cuando sólo un nodo quiere transmitir, puede hacerlo a una tasa R
2. Cuando M nodos quieren transmitir, cada uno puede enviar a una tasa media R/M
3. Totalmente descentralizado:
   - no es necesario un nodo dedicado para coordinar la transmisión
   - No hay relojes de sincronización
4. Simple

Protocolos Media Access Control (MAC)

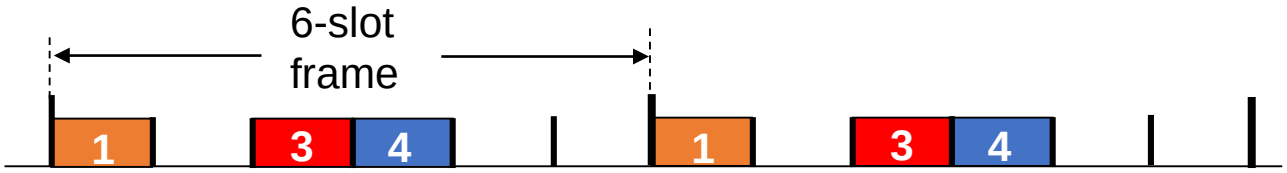
Tres clases de protocolos:

- Particionamiento del canal
  - Divide el canal en partes pequeñas denominadas slots de tiempo, frecuencia, etc.
  - Asigna partes a un nodo de forma exclusiva
- Acceso aleatorio
  - El canal no se divide, permite colisiones y forma de recuperarse de ellas
- Toma de turnos
  - Los nodos toman turnos, pero aquellos con más información que enviar pueden tomar turnos más largos

Partición de canal: TDMA

TDMA: Time Division Multiple Access

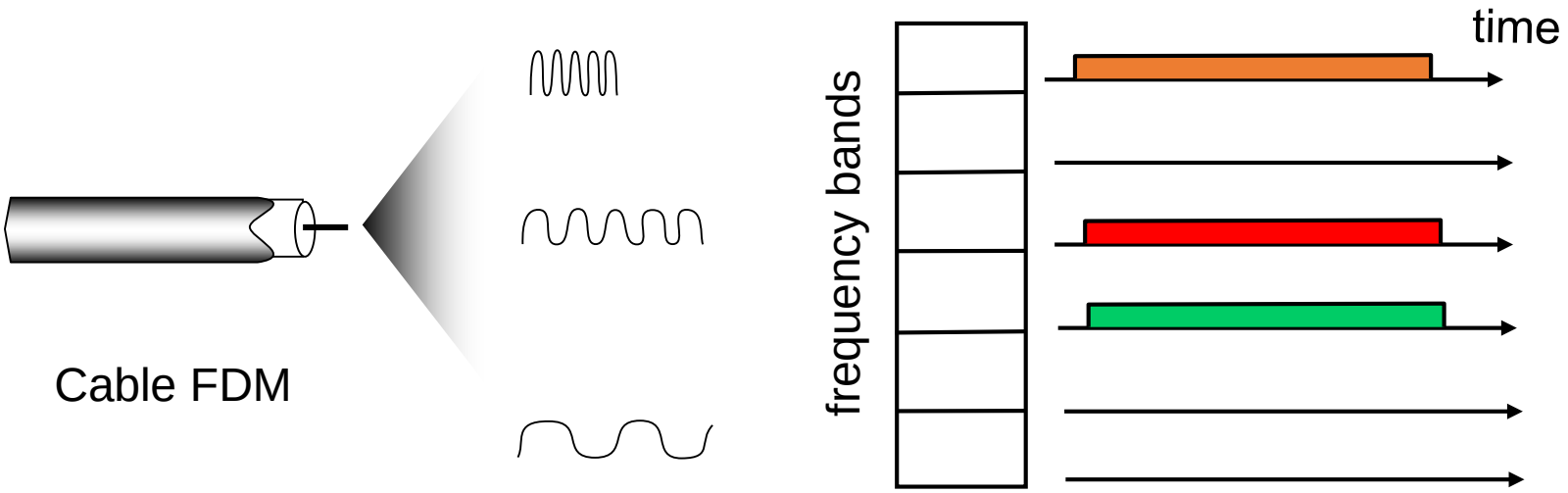
- Acceso al canal por “rondas”
- Cada estación dispone de un slot de longitud fija para transmitir sus paquetes en cada ronda
- Los slots no utilizados están inactivos
- ejemplo: LAN con 6 estaciones, 1,3,4 tienen paquetes, slots 2,5,6 inactivos



Partición de canal: FDMA

FDMA: Frequency Division Multiple Access

- El espectro del canal se divide en frecuencias
- Cada estación tiene asignada una banda concreta
- El tiempo de transmisión no utilizado hace que las frecuencias estén inactivas
- ejemplo: LAN con 6 estaciones, 1,3,4 tienen paquetes mientras que las bandas 2,5,6 están inactivas

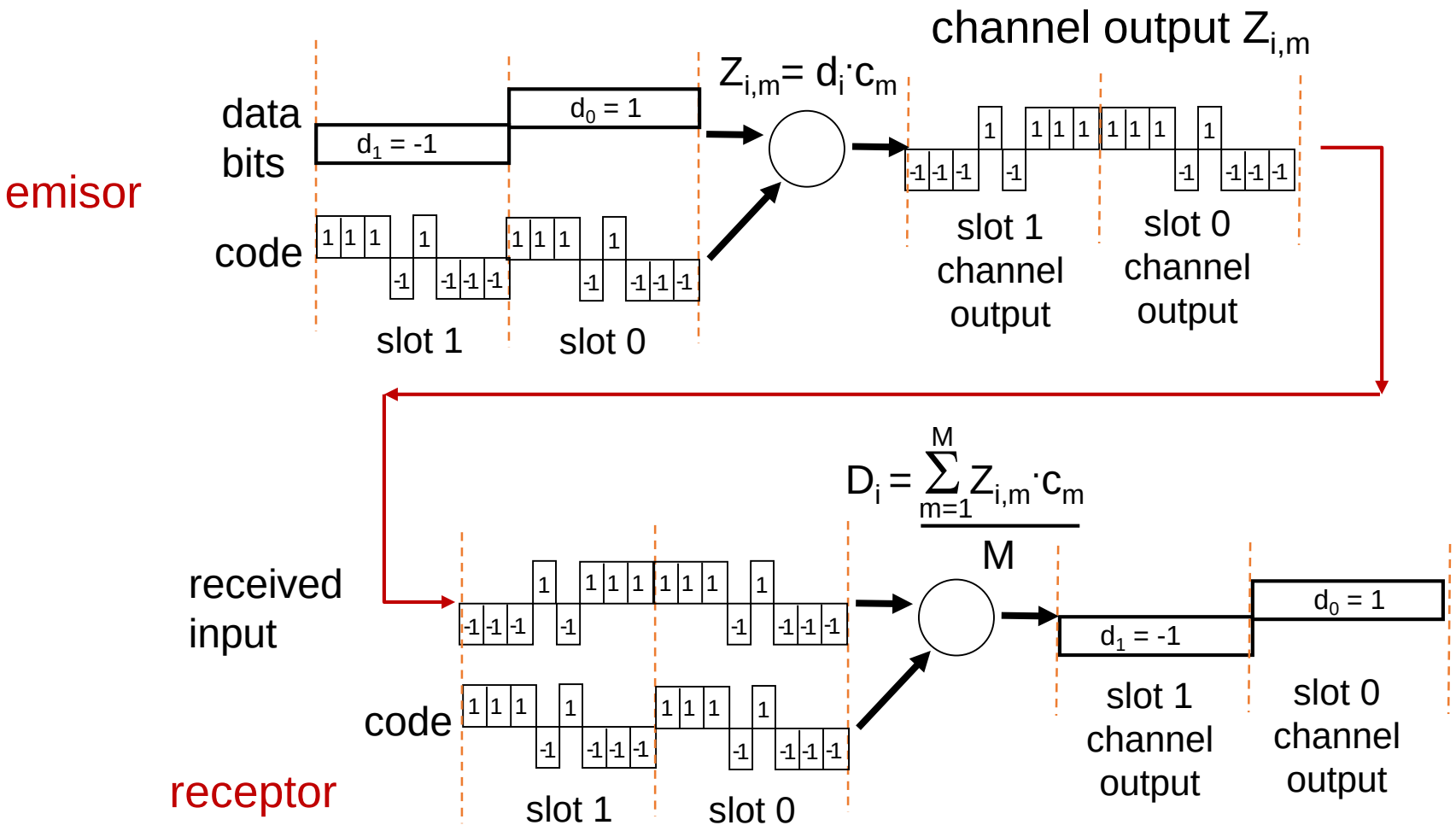


Partición de canal: CDMA

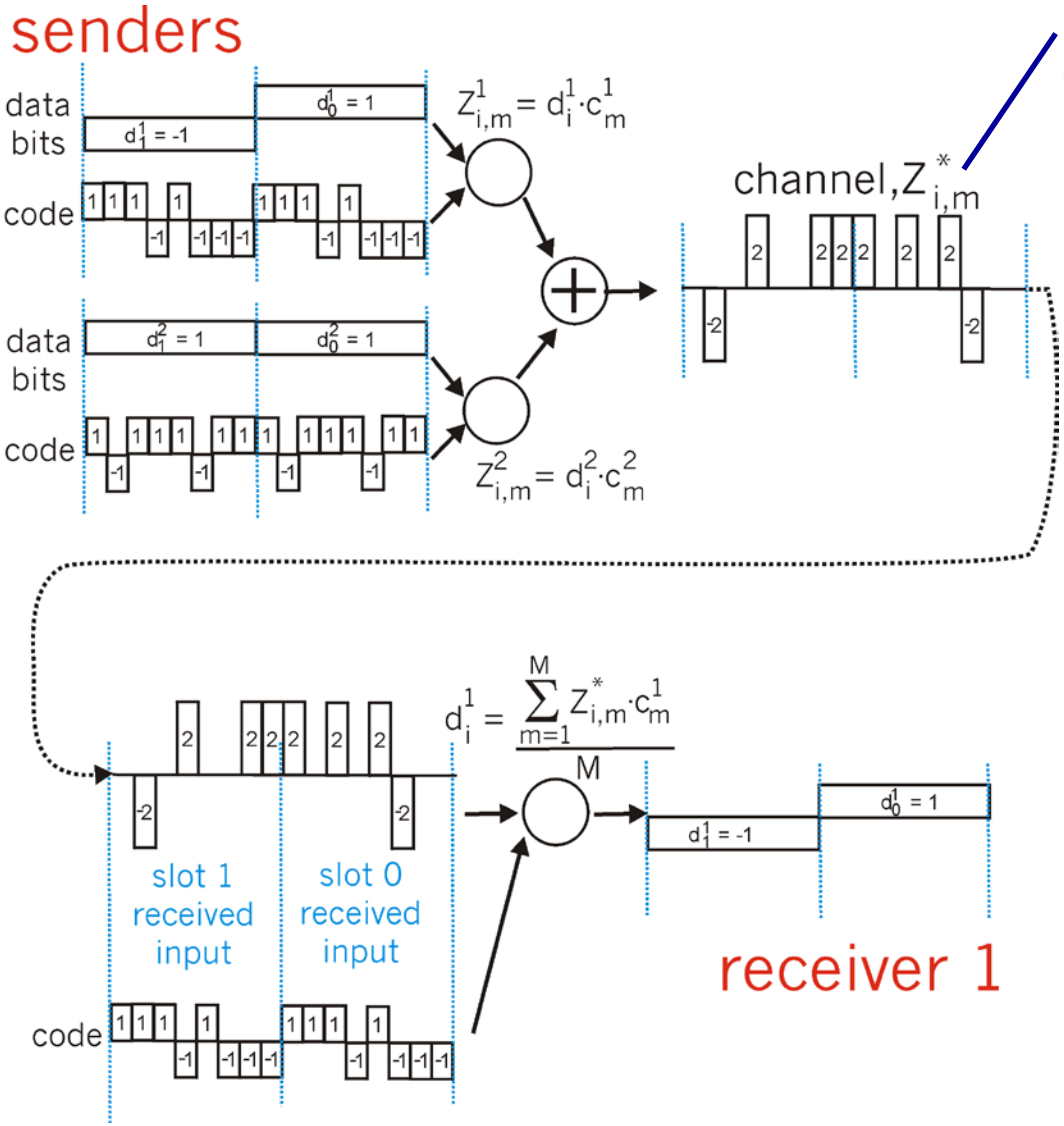
CDMA: Code Division Multiple Access

- Se asigna un código único a cada usuario
- Cada bit se codifica multiplicándolo por una señal (código) que varía a una velocidad mayor que la de bit (velocidad de chipping)
- Todos los usuarios emplean la misma frecuencia, pero cada uno tiene su propia secuencia de chipping (código)
- Se permite así la transmisión simultánea de múltiples usuarios con mínima interferencia (si los códigos se eligen bien y son “ortogonales”)

Partición de canal: CDMA



Partición de canal: CDMA



El canal suma las transmisiones de los emisores 1 y 2

Empleando el mismo código del emisor 1, el receptor recupera los datos enviados por 1 del canal donde se encuentran agregados

Protocolos de acceso aleatorio

- Cuando un nodo tiene un paquete que enviar
  - Transmite a la velocidad máxima del canal (R).
  - No hay coordinación de nodos a priori
- Dos o más nodos transmitiendo → "colisión"
- Protocolo MAC de acceso aleatorio especifica:
  - Cómo detectar colisiones
  - Cómo recuperarse de una colisión (e.g., mediante retransmisión retardada esperando un tiempo aleatorio)
- Ejemplos de protocolos MAC de acceso aleatorio:
  - ALOHA con particiones (slotted ALOHA)
  - ALOHA
  - CSMA, CSMA/CD, CSMA/CA

CSMA (Carrier Sense Multiple Access)

CSMA: Acceso múltiple con sondeo de portadora

- Sondeo = escucha antes de transmitir:
  - Si el canal parece desocupado: transmite toda la trama
  - Si el canal parece ocupado, retrasa la transmisión esperando un tiempo aleatorio
- Analogía humana: ¡no interrumpas a otros!
- ¿Hay colisiones entonces?

Colisiones en CSMA

Colisiones pueden ocurrir:

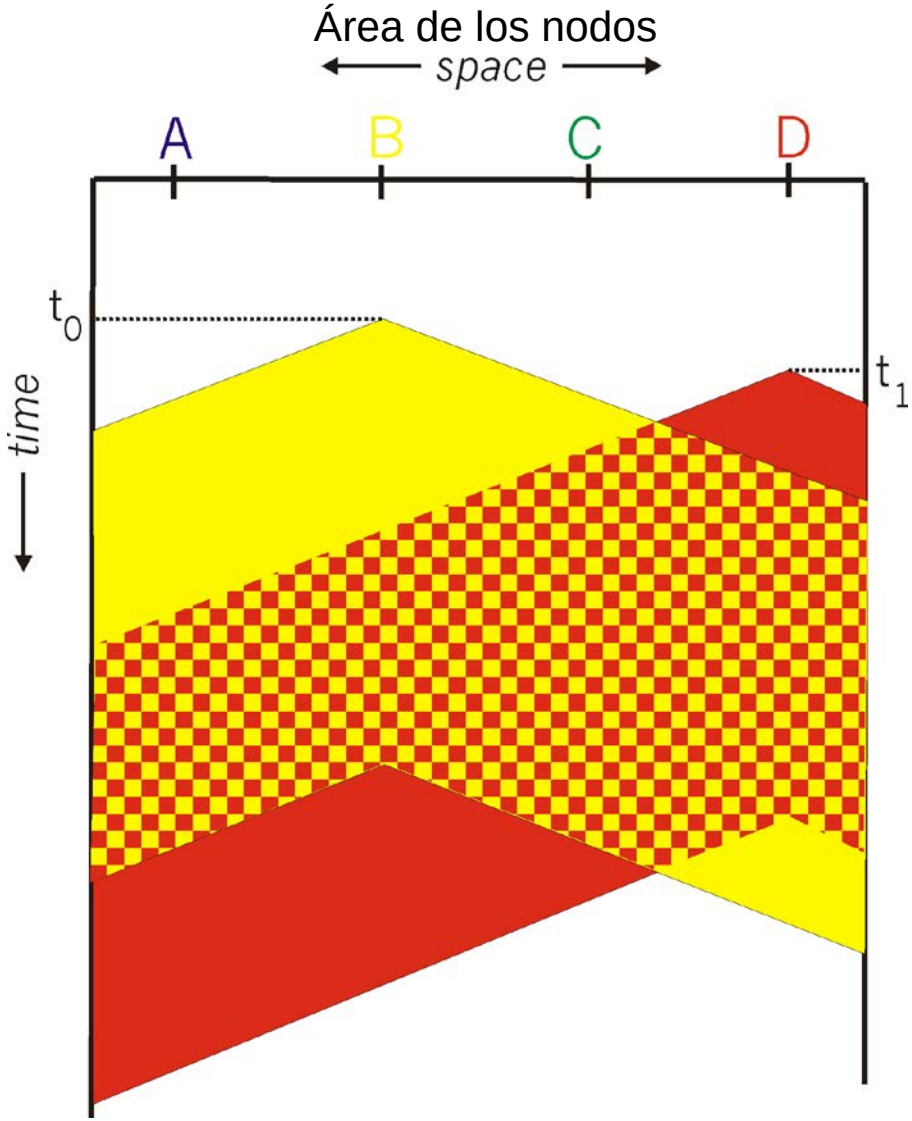
- Retraso en la propagación significa que los nodos pueden no escucharse en la transmisión

Colisión:

- La transmisión completa del paquete se pierde

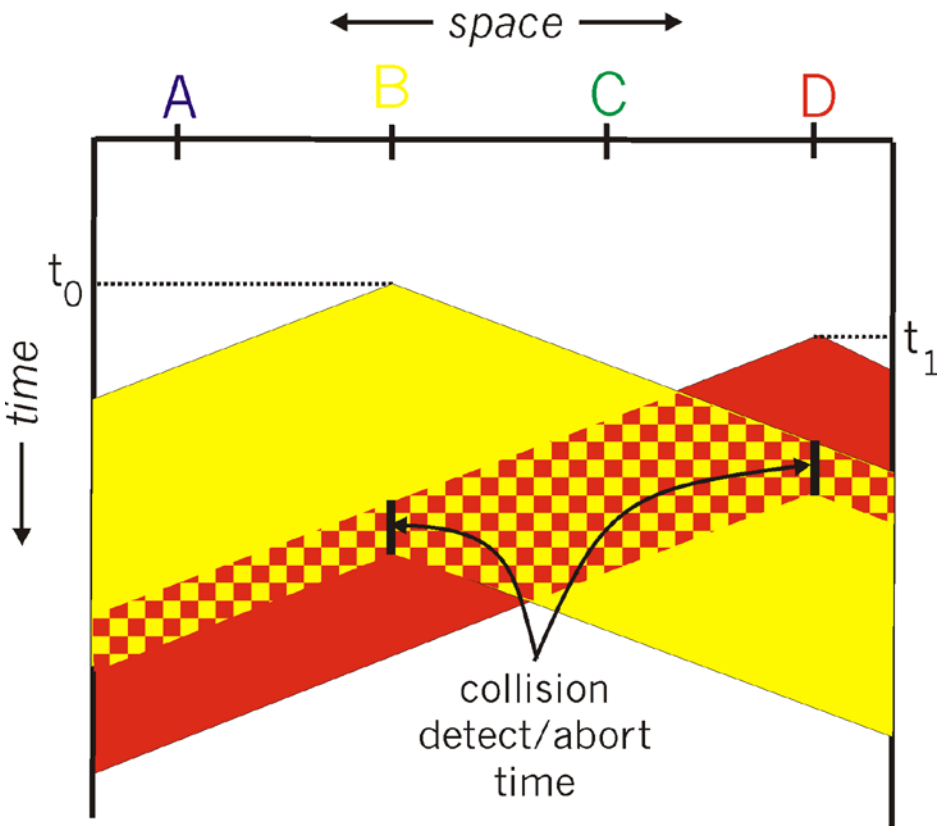
Nota:

- El papel de la distancia y el retraso en la propagación determinan la probabilidad de la colisión



CSMA/CD (Detección de Colisiones)

- Colisiones detectadas dentro de un tiempo corto
- Transmisiones en conflicto abortadas para reducir la pérdida del canal
- Detección de colisión:
  - Fácil en redes cableadas: medir la fuerza de la señal, comparar señales enviadas y recibidas
  - Difícil en redes inalámbricas: la fuerza de la señal recibida es abrumada por la fuerza de transmisiones locales



Protocolos MAC de “toma de turnos”

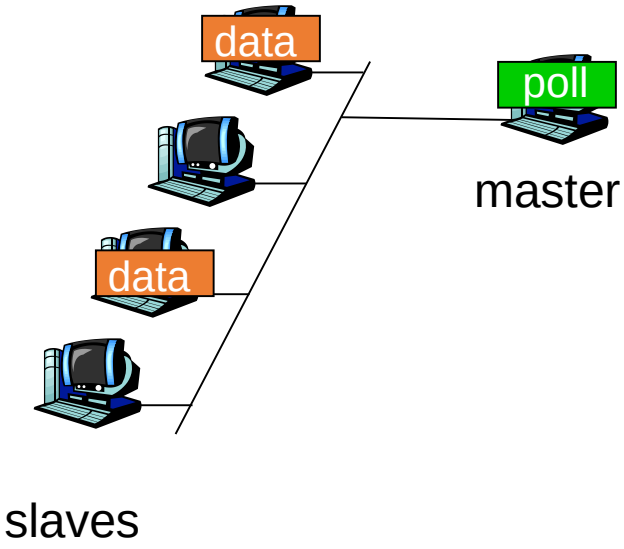
Universidad Rey Juan Carlos

- Protocolos MAC que particionan el canal
  - Alta carga del canal compartido de manera eficiente y justa
  - Ineficiente con carga baja debido al retraso en el acceso al canal, ancho de banda asignado 1/N sólo si hay 1 nodo activo!
- Protocolos MAC de acceso aleatorio
  - Eficiente con carga baja ya que un único nodo puede utilizar el canal completo
  - Con carga alta sobrecarga de colisiones
- Protocolos MAC de “toma de turnos”
  - Buscan lo mejor de ambas aproximaciones!

Protocolos MAC de "toma de turnos"

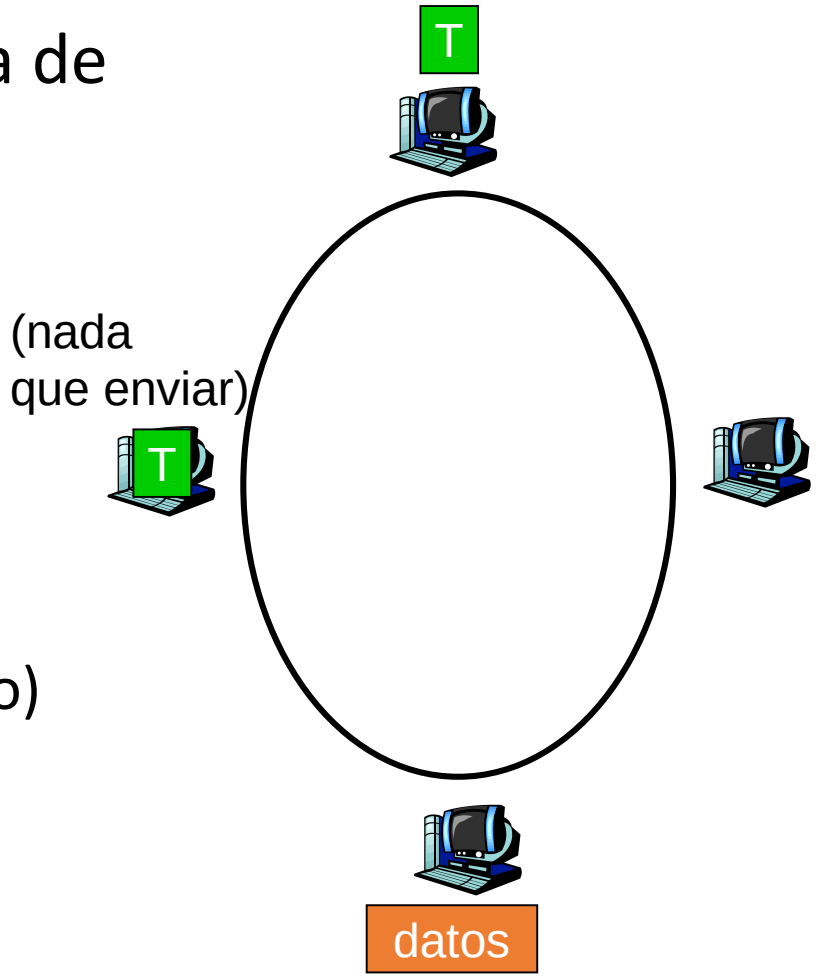
Sondeo (polling):

- Nodo maestro invita a los nodos esclavos a transmitir por turno
- Típicamente utilizado con dispositivos esclavos "tontos"
- Inquietudes:
  - Sobrecarga del sondeo
  - Latencia (si sólo 1 activo, tiene que esperar…)
  - Único punto de fallo (maestro)



Paso de testigo (token):

- El control del token se pasa de un nodo a otro de forma secuencial.
- Mensaje del token
- Inquietudes:
  - Sobrecarga del token
  - Latencia
  - Único punto de fallo (testigo)



Resumen de protocolos MAC

- Particionamiento del canal
  - División en tiempo, división en frecuencia, división en código…
- Acceso aleatorio (dinámico)
  - ALOHA, S-ALOHA, CSMA, CSMA/CD, CSMA/CA
  - Sondeo de portadora: fácil con tecnologías de cable y difícil con inalámbricas
  - CSMA/CD utilizado en Ethernet
  - CSMA/CA utilizado en 802.11
- Toma de turnos
  - Sondeo desde un lugar centralizado y paso de testigo
  - Bluetooth, FDDI, IBM Token Ring (IEEE 802.5)


Wi Fi
TM

Historia de las WLAN

Fecha	Evento
1986	Primeras WLANs. 900 MHz (860 Kb/s). No disponible en Europa.
1993	WLANs de 1 y 2 Mb/s en banda de 2,4 GHz. Primeras disponibles en Europa
7/1997	IEEE aprueba 802.11. 1 y 2 Mb/s. Banda de 2,4 GHz e infrarrojos.
1998	Primeros sistemas de11 Mb/s a 2,4 GHz. Preestándar 802.11b.
9/1999	IEEE aprueba 802.11b (hasta 11 Mb/s, 2,4 GHz) y 802.11a (hasta 54 Mb/s, 5 GHz, no disp. en Europa)
12/2001	Primeros productos comerciales 802.11a
12/2001	Borrador 802.11e (QoS en WLANs)
2003	IEEE aprueba 802.11g (hasta 54 Mb/s, 2,4 GHz)

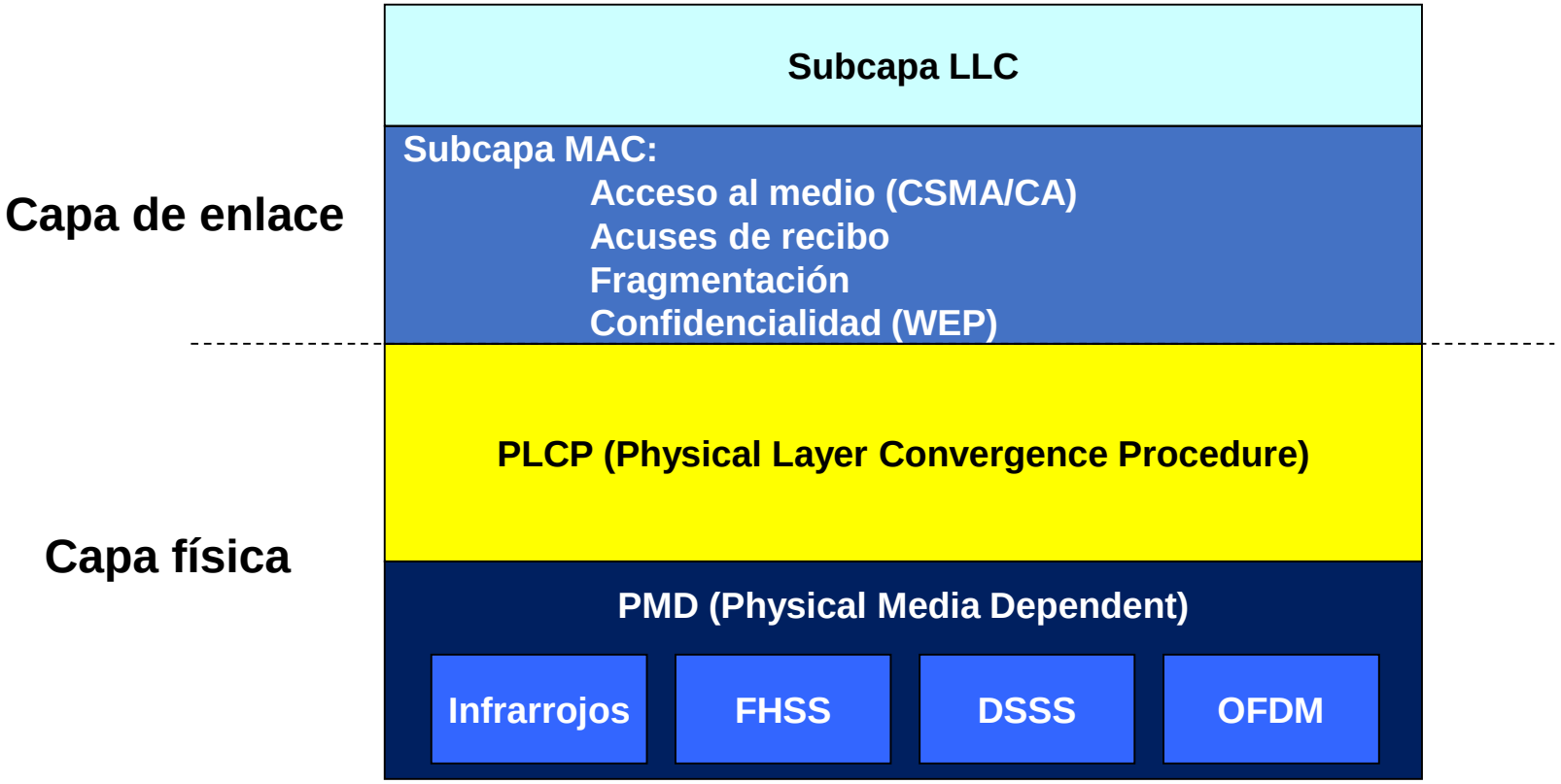
Historia de las WLAN

Generation/IEEE Standard	Maximum Linkrate	Adopted	Frequency
Wi-Fi 6 (802.11ax)	600–9608 Mbit/s	2019	2.4/5 GHz 1–6 GHz ISM
Wi-Fi 5 (802.11ac)	433–6933 Mbit/s	2014	5 GHz
Wi-Fi 4 (802.11n)	72–600 Mbit/s	2009	2.4/5 GHz
Wi-Fi 3 (802.11g)	3–54 Mbit/s	2003	2.4 GHz
Wi-Fi 2 (802.11a)	1.5 to 54 Mbit/s	1999	5 GHz
Wi-Fi 1 (802.11b)	1 to 11 Mbit/s	1999	2.4 GHz

Source: Wikipedia

- 802.11b: DSSS con todos los host usando el mismo código de chipping
- Todos emplean CSMA/CA para el acceso múltiple
- Todos soportan los modos infraestructura y ad-hoc

Modelo de Referencia de IEEE802.11



Nivel físico en 802.11

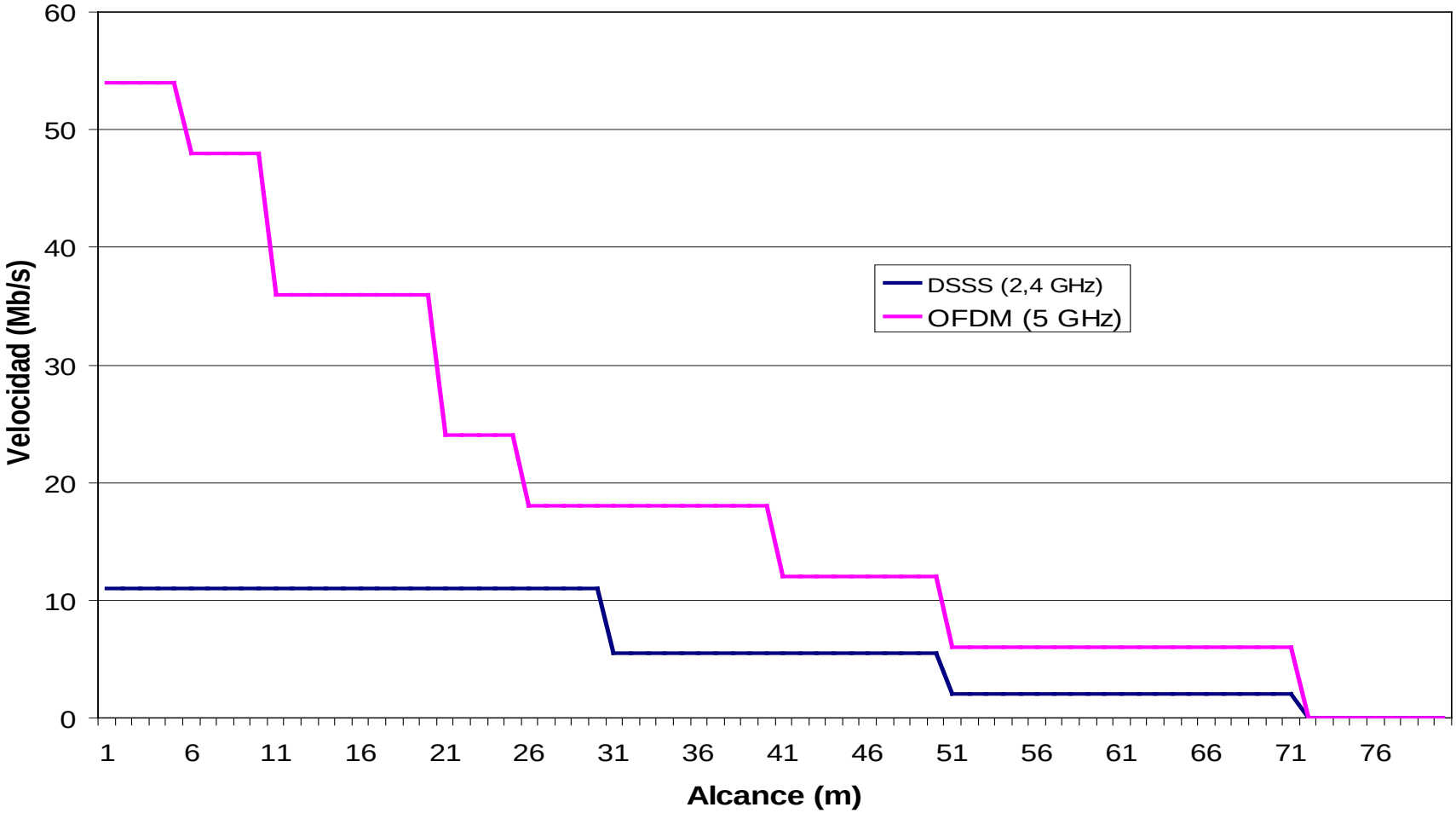
- Infrarrojos: sólo válido en distancias muy cortas y en la misma habitación
- Radio:
  - FHSS (Frequency Hopping Spread Spectrum): Sistema de bajo rendimiento, poco utilizado actualmente.
  - DSSS (Direct Sequence Spread Spectrum): Buen rendimiento y alcance.
  - OFDM (Orthogonal Frequency Division Multiplexing): Usa banda de 5 GHz (menor alcance que 2,4 GHz).
- La comunicación es Half-Duplex (no puedo enviar y recibir al mismo tiempo)

Medios del nivel físico en 802.11

Medio físico	Infrarrojos	FHSS	DSSS	OFDM
Banda	850 – 950 nm	2,4 GHz	2,4 GHz	5 GHz
Velocidades* **(Mb/s)**	**1** y 2 (802.11)	**1** y 2 (802.11)	**1**, **2** (802.11) **5.5**, **11** (802.11b) **6**, 9, **12**, 18, 22, **24**, 33, 36, 48 y 54 (802.11g)	**6**, 9, **12**, **18**, 24, 36, 48 y 54 (802.11a) 600 (802.11n) 1300 (802.11ac)
Alcance (a vel. Max.)	20 m	150 m	30 m (802.11b)	5 m
Utilización	Muy rara	Muy poca	Mucha	Mucha
Características	No atraviesa paredes	Interferencias Bluetooth y hornos microondas	Buen rendimiento y alcance	Actualmente las más modernas

* **Las velocidades en negrita son obligatorias, las demás son opcionales**

Velocidad en función del alcance



- Valores medios para interior en ambientes de oficina.
- En exteriores los alcances pueden ser hasta cinco veces mayores.
- El alcance real depende del entorno.
- Los equipos se adaptan automáticamente a la máxima velocidad posible en cada caso

Espectro electromagnético

- La mayor parte del espectro radioeléctrico está regulada por la ITU-R y se requiere licencia para emitir
- La ITU-R divide el mundo en tres regiones, Europa es la región 1. Cada una tiene una regulación diferente de las frecuencias. Algunos países tienen normativas propias más restrictivas.
- Como no sería práctico pedir licencia para cada WLAN el IEEE decidió asignar para esto algunas de las bandas ISM (designadas para aplicaciones de tipo Industrial-Scientific-Medical).
- Las frecuencias exactas de la banda ISM difieren para cada región, e incluso para algunos países.

Bandas designadas por la ITU para aplicaciones ISM

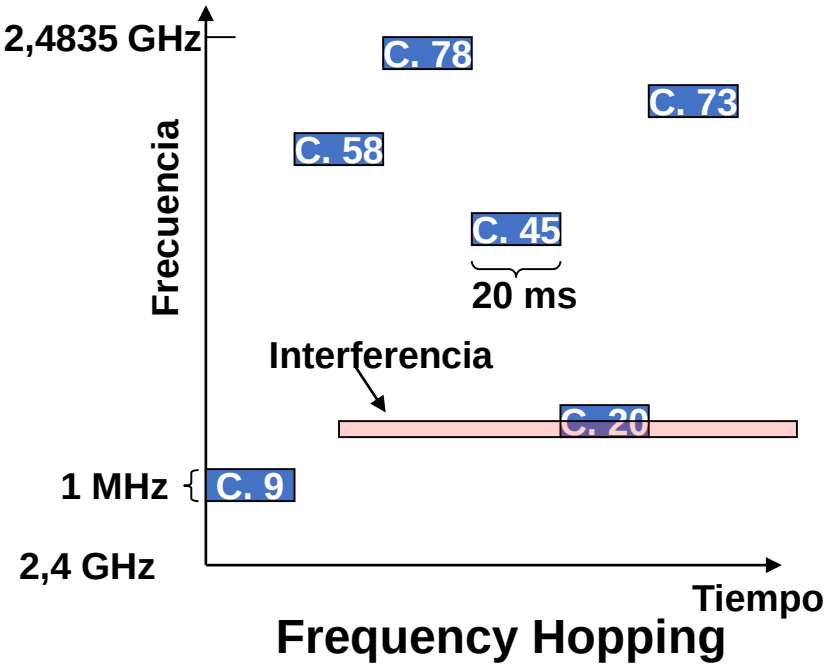
Banda	Anchura	Uso en WLAN
13 553 – 13 567 kHz	14 kHz	No
26 957 – 27 283 kHz	326 kHz	No
40.66 – 40.7 MHz	40 kHz	No
902 – 928 MHz*	26 MHz	Sistemas propietarios antiguos (solo en EEUU y Canadá)
2 400 – 2 500 MHz	100 MHz	802.11b, 802.11g, 802.11n
5 725 – 5 875 MHz	150 MHz	802.11a, 802.11n, 802.11ac
24 – 24.25 GHz	250 MHz	No

* Solo autorizada en región 2 (EEUU y Canadá)

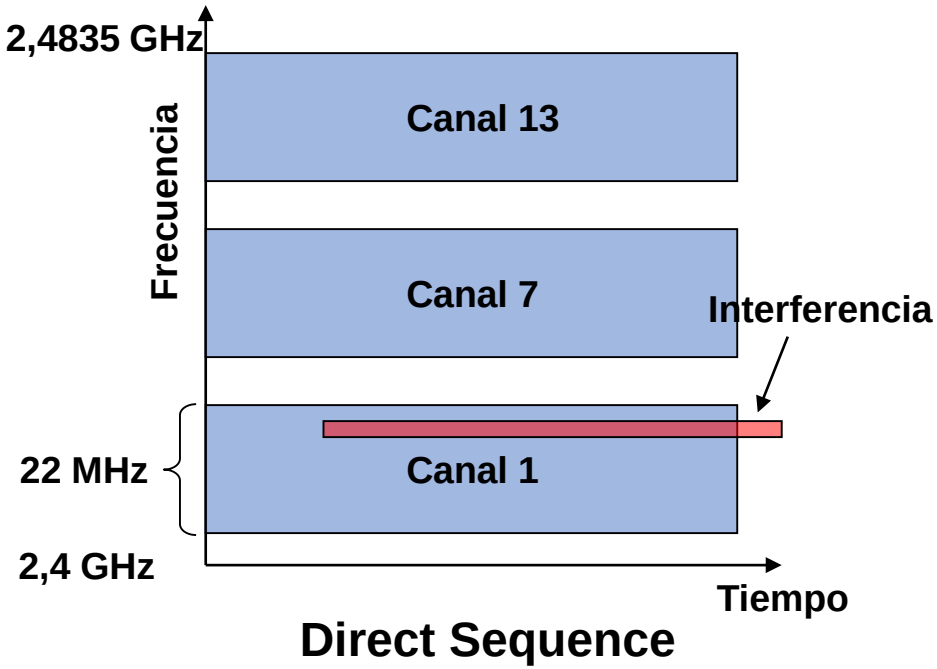
Espectro Disperso

- Para reducir la interferencia en la banda de 2,4 GHz las emisiones de más de 1 mW se han de hacer en espectro disperso
- Hay dos formas de hacer una emisión de espectro disperso:
  - Frecuency Hopping (salto de frecuencia). El emisor va cambiando continuamente de canal. El receptor ha de seguirlo.
  - Direct Sequence (secuencia directa). El emisor emplea un canal muy ancho. La potencia de emisión es similar al caso anterior, pero al repartirse en una banda mucho más ancha la señal es de baja intensidad (poca potencia por Hz).

Frequency Hopping vs Direct Sequence



Frequency Hopping



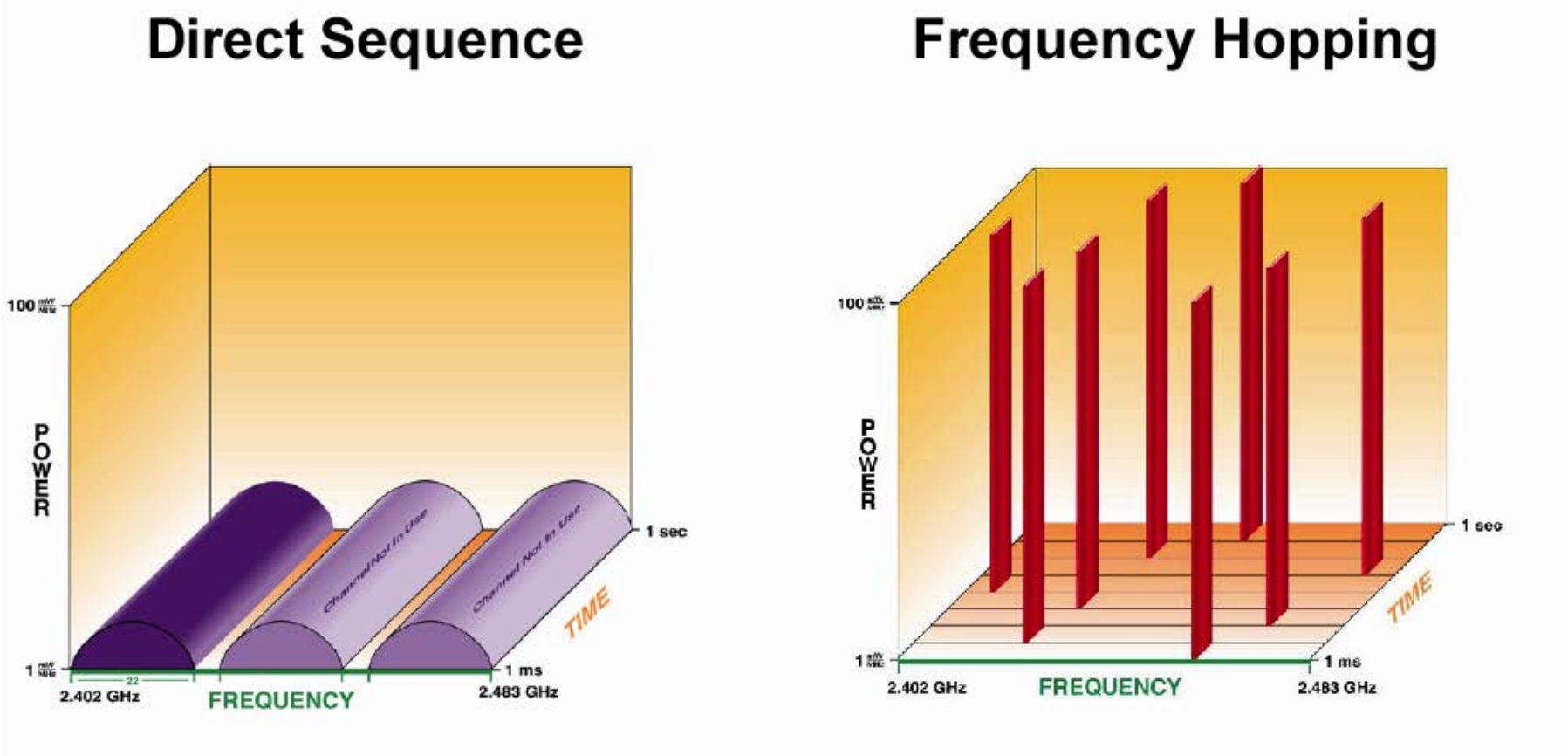
Direct Sequence

- El emisor cambia de canal continuamente (unas 50 veces por segundo)
- Cuando el canal coincide con la interferencia la señal no se recibe; la trama se retransmite en el siguiente salto

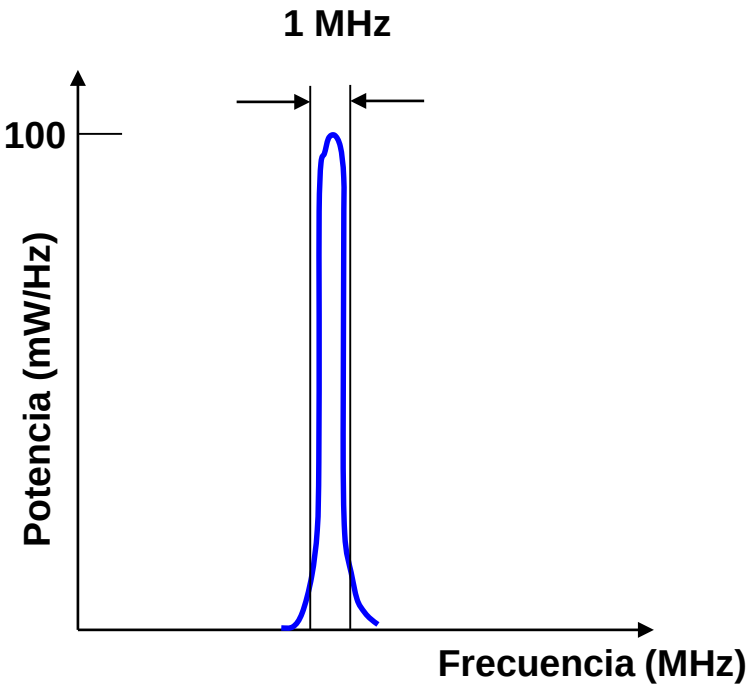
- El canal es muy ancho; la señal contiene mucha información redundante
- Aunque haya interferencia el receptor puede extraer los datos de la señal

Frequency Hopping vs Direct Sequence

Universidad Rey Juan Carlos

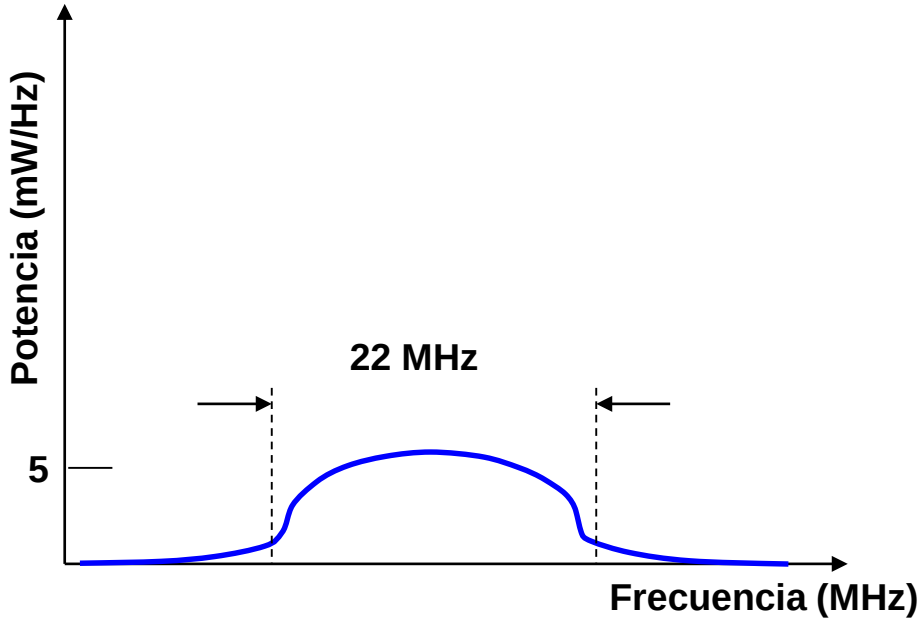


Frequency Hopping vs Direct Sequence



Frequency Hopping

Señal concentrada, gran intensidad
Elevada relación S/R
Área bajo la curva: 100 mW



Direct Sequence

Señal dispersa, baja intensidad
Reducida relación S/R
Área bajo la curva: 100 mW

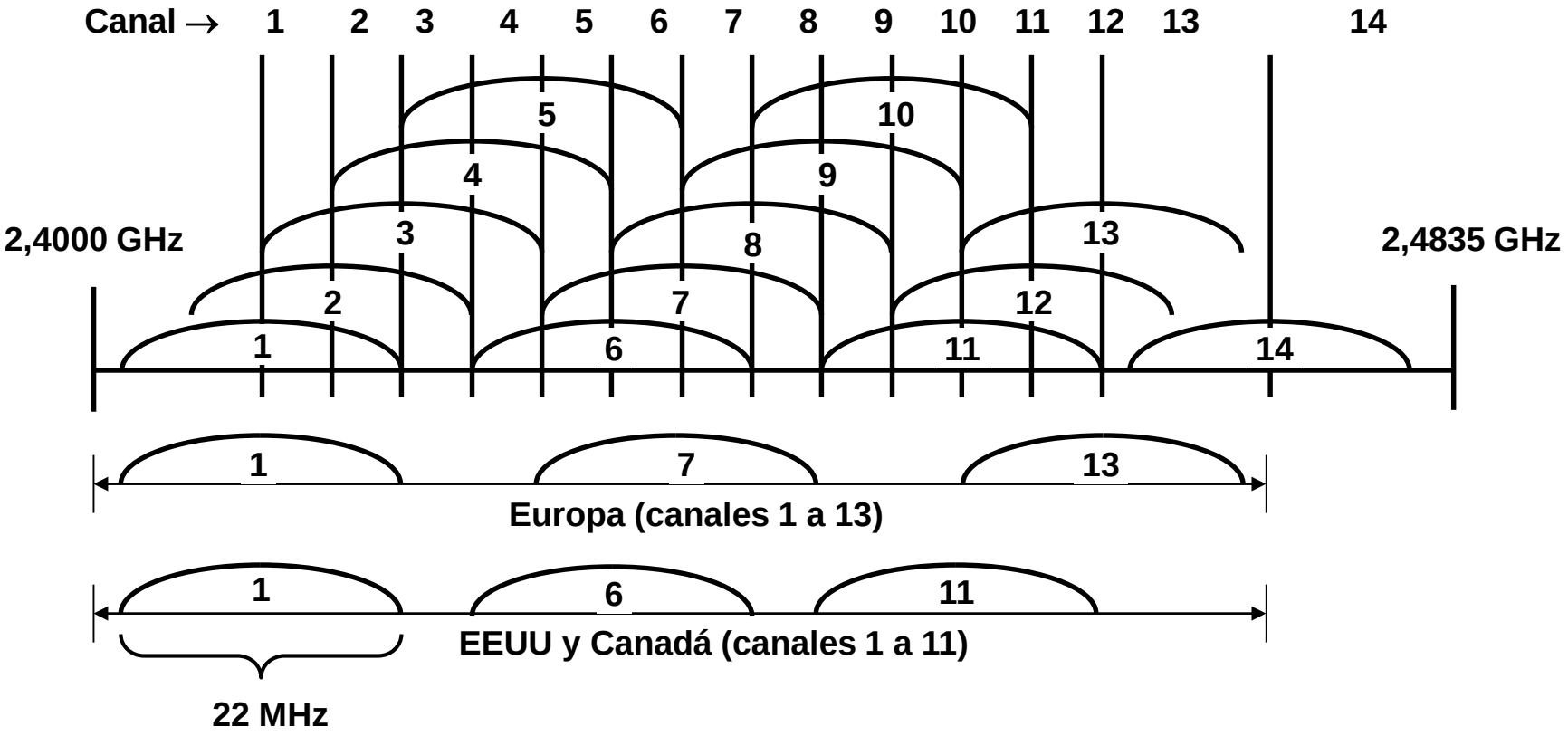
Canales 802.11b DSSS a 2,4 GHz

Canal	Frecuencia central (MHz)	Región ITU-R o país				
		América	EMEA	Japón	Israel	China
1	2412	X	X	X	-	X
2	2417	X	X	X	-	X
3	2422	X	X	X	X	X
4	2427	X	X	X	X	X
5	2432	X	X	X	X	X
6	2437	X	X	X	X	X
7	2442	X	X	X	X	X
8	2447	X	X	X	X	X
9	2452	X	X	X	X	X
10	2457	X	X	X	-	X
11	2462	X	X	X	-	X
12	2467	-	X	X	-	-
13	2472	-	X	X	-	-
14	2484	-	-	X	-	-

Anchura de canal: 22 MHz

EMEA: Europa, Medio Oriente y África

Reparto de canales DSSS a 2,4GHz



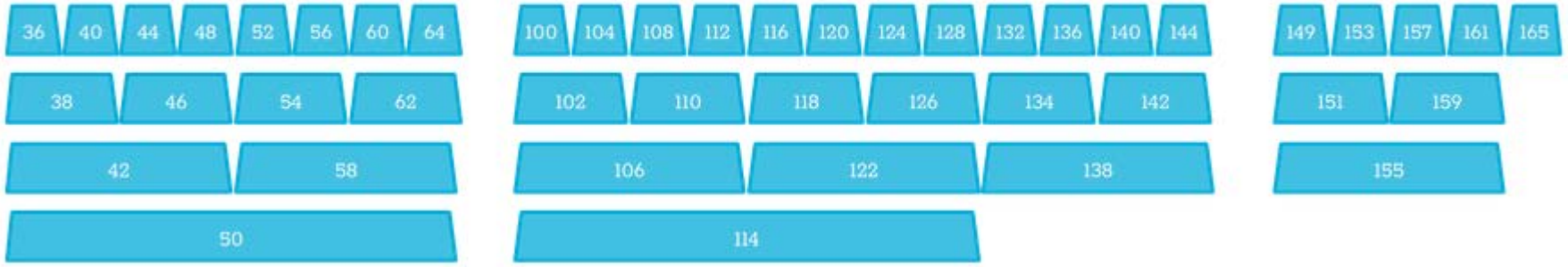
Canales DSSS simultáneos

- Si se quiere utilizar más de un canal en una misma zona hay que elegir frecuencias que no se solapen. El máximo es de tres canales:
  - EEUU y Canadá: canales 1, 6 y 11
  - Europa: canales 1, 7 y 13
  - Japón: solo se puede utilizar el canal 14
- Francia y España antes (2001) tenían normativas más restrictivas en frecuencias, que no permitían más que un canal no solapado
- Con diferentes canales se pueden constituir LANs inalámbricas independientes en una misma zona

Banda de 5 GHz (802.11a)

- Para 802.11a el IEEE ha elegido la banda de 5 GHz, que permite canales de mayor ancho de banda, o mayor número de canales
- Se divide en 24 canales no solapados
- Un equipo 802.11a no puede interoperar con uno 802.11b. La parte de radio es completamente diferente

802.11ac channels can be 20 MHz, 40 MHz, 80 MHz, and 160 MHz wide.



Canales 802.11a a 5 GHz

Universidad Rey Juan Carlos

Canal	Frecuencia central (MHz)	Región ITU-R o país			
		América	Japón	Singapur	Taiwan
34	5170	-	I	-	-
36	5180	I	-	I	-
38	5190	-	I	-	-
40	5200	I	-	I	-
42	5210	-	I	-	-
44	5220	I	-	I	-
46	5230	-	I	-	-
48	5240	I	-	I	-
52	5260	I/E	-	-	I
56	5280	I/E	-	-	I
60	5300	I/E	-	-	I
64	5320	I/E	-	-	I
149	5745	-	-	-	-
153	5765	-	-	-	-
157	5785	-	-	-	-
161	5805	-	-	-	-

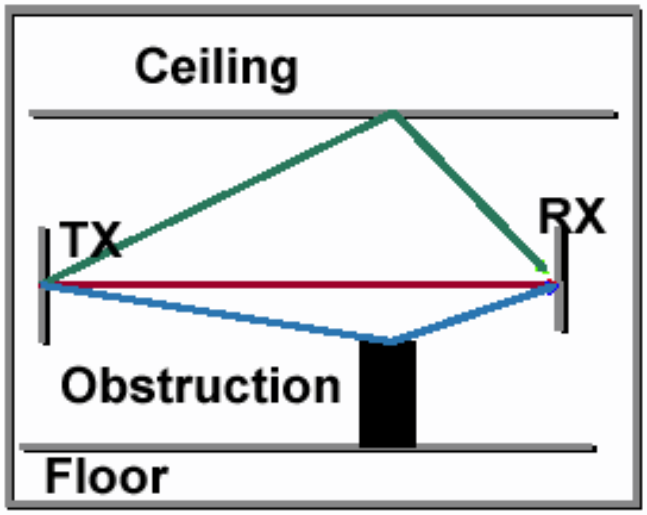
I: Uso interiores
E: Uso exteriores

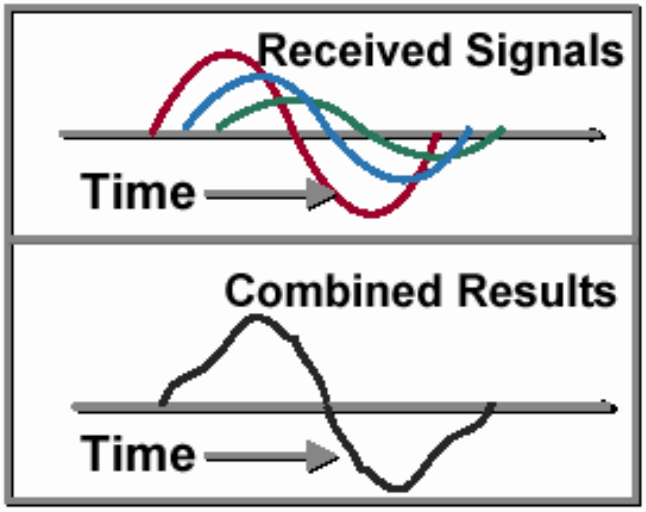
Anchura de canal: 20 MHz

Interferencias

- Externas:
  - Bluetooth interfiere con FHSS (usan la misma banda). Interfiere menos con DSSS.
  - Los hornos de microondas (funcionan a 2,4 GHz) interfieren con FHSS. También hay reportadas interferencias entre hornos de microondas y 802.11 FHSS (misma banda). A DSSS no le afectan.
  - Otros dispositivos que funciona en 2,4 GHz (teléfonos inalámbricos, mandos a distancia de puertas de garaje, etc.) tienen una potencia demasiado baja para interferir con las WLANs
  - En los sistemas por infrarrojos la luz solar puede afectar la transmisión
- Internas (de la propia señal):
  - Debidas a multitrayectoria (rebotes)

Interferencia por multicamino





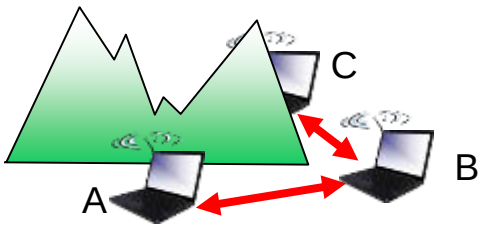
- Se produce interferencia debido a la diferencia de tiempo entre la señal que llega directamente y la que llega reflejada por diversos obstáculos.
- La señal puede llegar a anularse por completo si el retraso de la onda reflejada coincide con media longitud de onda. En estos casos un leve movimiento de la antena resuelve el problema.
- FHSS y OFDM son más resistentes a la interferencia multitrayectoria que DSSS. Pero este problema se resuelve con antenas diversidad.

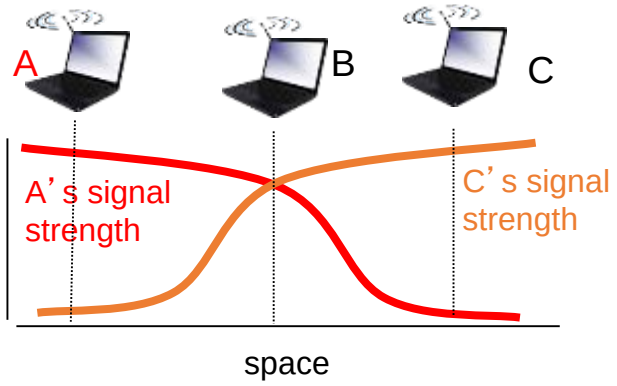
Antenas diversidad

- El equipo (normalmente un punto de acceso) tiene dos antenas. El proceso es el siguiente:
  - El equipo recibe la señal por las dos antenas y compara, eligiendo la que le da mejor calidad de señal. El proceso se realiza de forma independiente para cada trama recibida, utilizando el preámbulo (128 bits en DSSS) para hacer la medida
  - Para emitir a esa estación se usa la antena que dio mejor señal en recepción la última vez
  - Si la emisión falla (no se recibe el ACK) cambia a la otra antena y reintenta
- Las dos antenas cubren la misma zona
- Al resolver el problema de la interferencia multitrayectoria de DSSS el uso de FHSS ha caído en desuso

IEEE 802.11: Control del acceso múltiple

- Evitar colisiones: 2 o más nodos transmitiendo al mismo tiempo
- 802.11: CSMA – sondear antes de transmitir
  - Para no colisionar con la transmisión de otro nodo
- 802.11: sin detección de colisiones
  - Dificil recibir (señal débil) y transmitir (señal fuerte) al mismo tiempo
  - Hay casos imposibles de detector (terminal oculto o atenuación)
  - Objetivo: evitar las colisiones con CSMA/C(ollision)A(voidance)





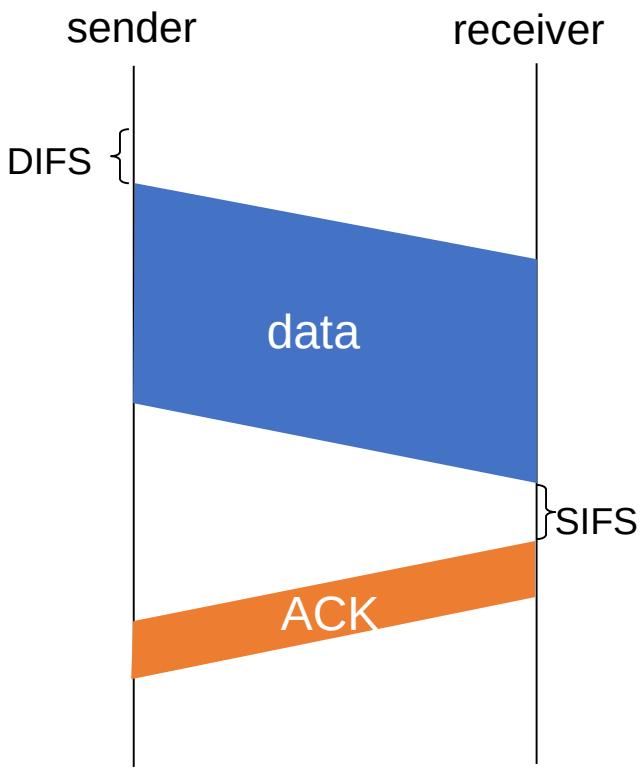
IEEE 802.11: CSMA/CA

Emisor 802.11

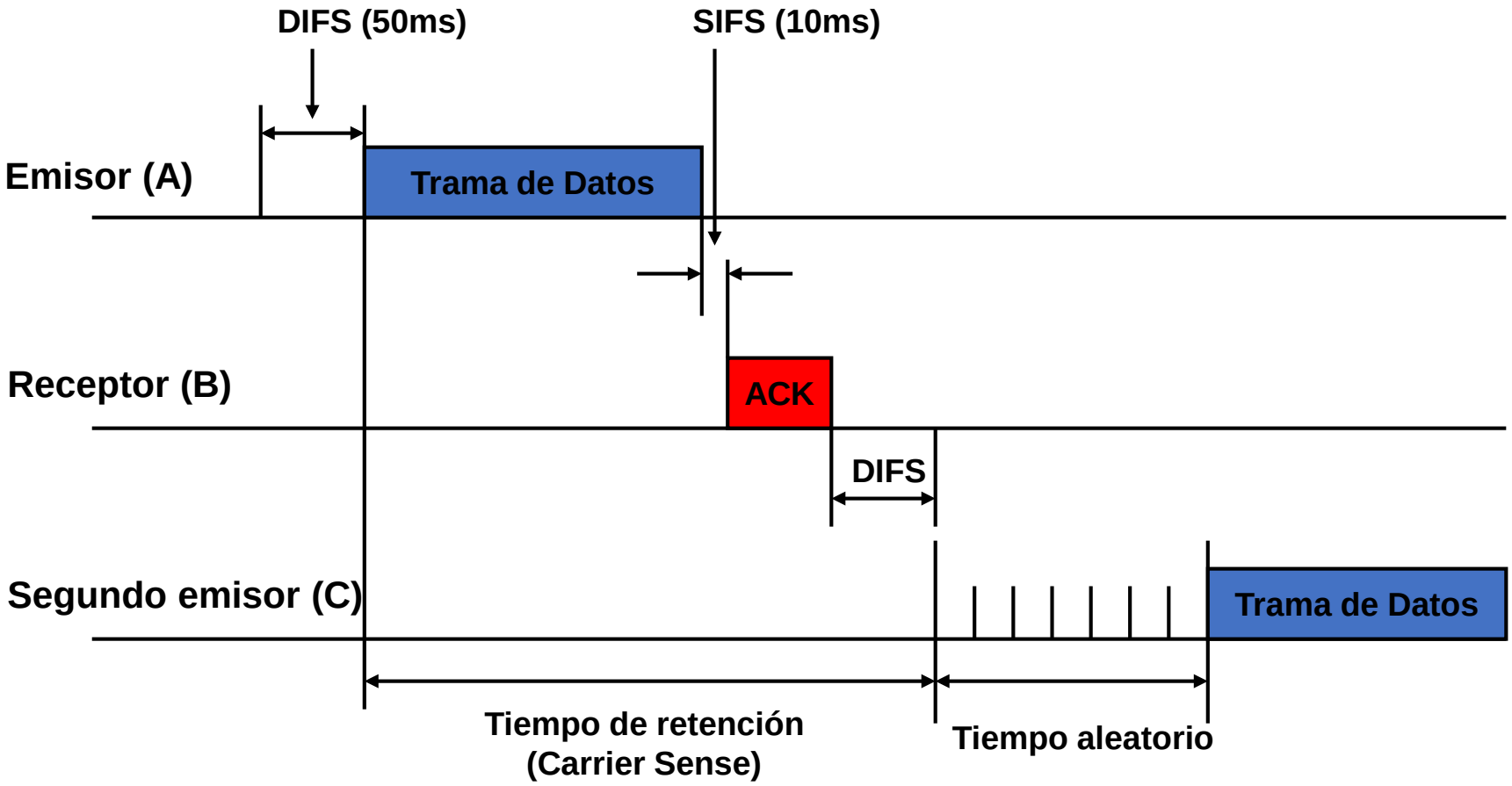
1. Si ve el canal libre durante DIFS, transmite el frame entero (sin CD)
2. Si ve el canal ocupado
   - Inicia un contador aleatorio de espera
   - El contador avanza mientras el canal esté libre
   - Transmite cuando el contador termine
   - Si no hay ACK, aumenta el contador de forma aleatoria y vuelve a empezar

Receptor 802.11

- Si recibe el frame correctamente, devuelve ACK tras SIFS (el ACK soluciona el problema de terminal oculto)



IEEE 802.11: CSMA/CA



DIFS: DCF (Distributed Coordination Function) Inter Frame Space
SIFS: Short Inter Frame Space

Colisiones

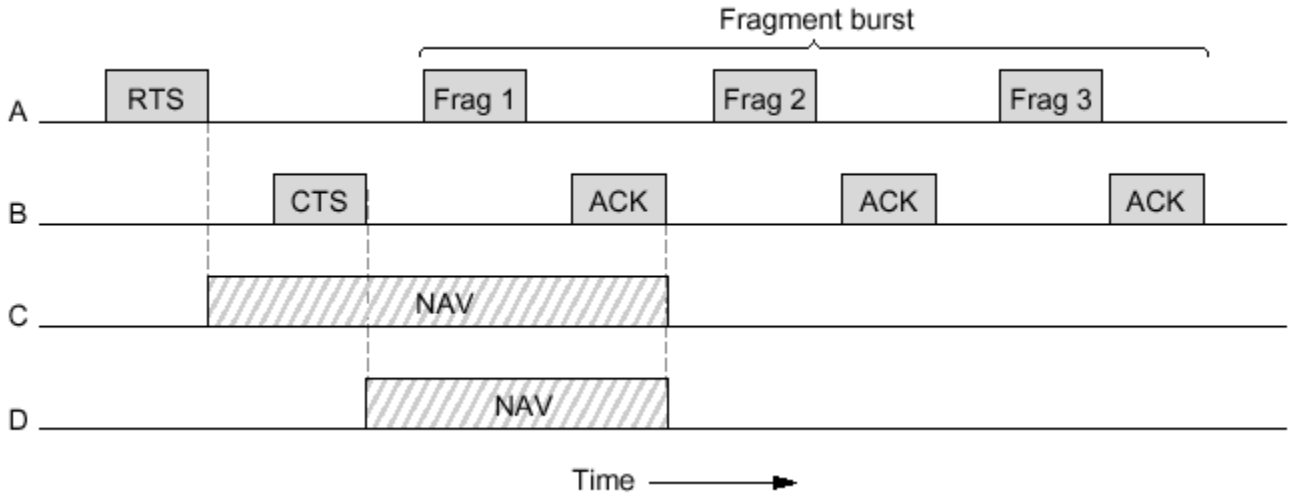
- Pueden producirse porque dos estaciones a la espera elijan el mismo número de intervalos (mismo tiempo aleatorio) para transmitir después de la emisión en curso.
- En ese caso reintentan ampliando exponencialmente el rango de intervalos y vuelven a elegir. Es similar a Ethernet salvo que las estaciones no detectan la colisión, infieren que se ha producido cuando no reciben el ACK esperado
- También se produce una colisión cuando dos estaciones deciden transmitir a la vez, o casi a la vez. Pero este riesgo es mínimo. Para una distancia entre estaciones de 70m el tiempo que tarda en llegar la señal es de 0,23 μs

Fragmentación

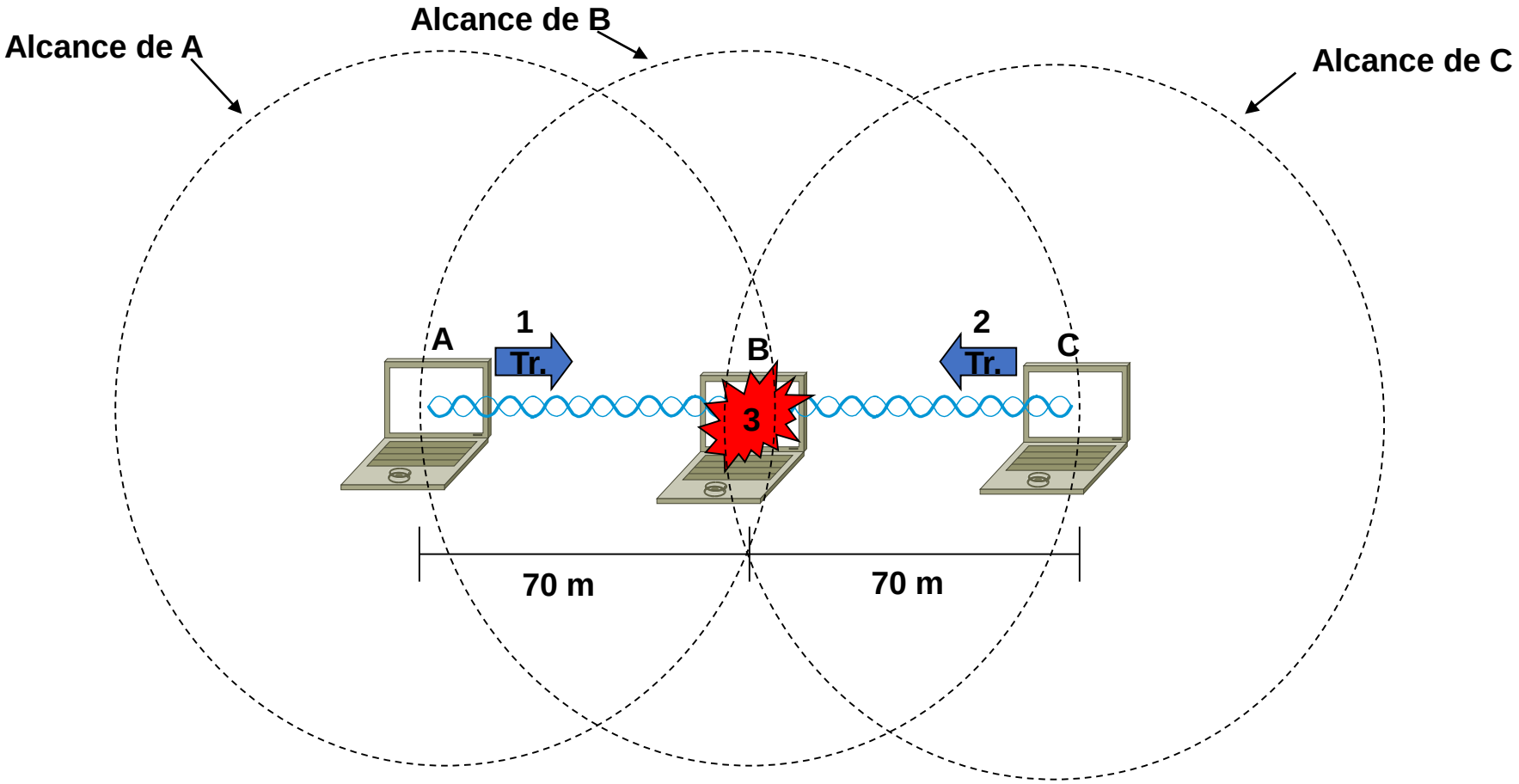
- Cuando se comienza a transmitir no hay vuelta atrás, por lo que si las tramas son largas el rendimiento puede bajar mucho
- En el nivel MAC de 802.11 se prevé la posibilidad de que el emisor fragmente una trama para evitar eso
- Por cada fragmento se devuelve un ACK por lo que en caso necesario es retransmitido por separado.
- Si el emisor ve que las tramas no están llegando bien puede decidir fragmentar las tramas grandes para que tengan mas probabilidad de llegar al receptor
- La fragmentación permite enviar datos en entornos con mucho ruido, aun a costa de aumentar el overhead
- Todas las estaciones están obligadas a soportar la fragmentación en recepción, pero no en transmisión

Envío de una trama fragmentada

La separación entre 'Frag n' y ACK es de 10 ms (SIFS).
De esta forma las demás estaciones (C y D) no pueden interrumpir el envío.



Problema de la estación oculta



1: A quiere transmitir una trama a B. Detecta el medio libre y transmite

3. Se produce una colisión en la intersección por lo que B no recibe ninguna de las dos tramas

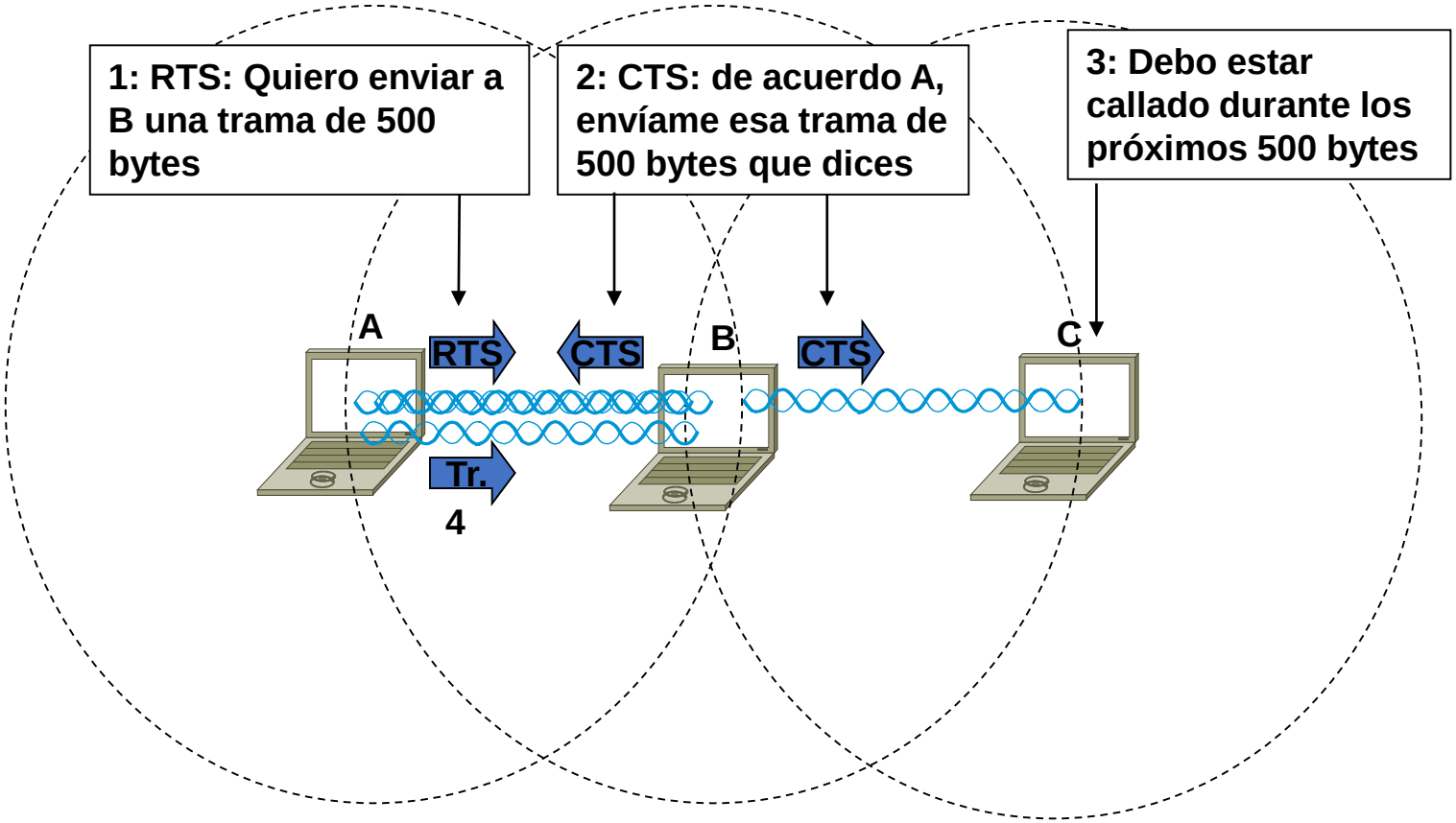
2: Mientras A está transmitiendo C quiere enviar una trama a B. Detecta el medio libre (pues no capta la emisión de A) y transmite

Solución al problema de la estación oculta

Idea: permitir al emisor reservar el canal

- El emisor hace una solicitud de envío (RTS) con un pequeño paquete al AP usando CSMA (los RTS pueden colisionar, pero son pequeños)
- El AP difunde un Clear-to-send (CTS) como respuesta al RTS, y es escuchado por todos los nodos
- El emisor del RTS puede ahora transmitir, pues tiene permiso del AP
- Si todas las estaciones se 'escuchan' directamente entre sí el uso de RTS/CTS no aporta nada y supone un overhead importante, sobre todo en tramas pequeñas
- El uso de mensajes RTS/CTS se denomina a veces *Virtual Carrier Sense*, y es **opcional**

Solución al problema de la estación oculta



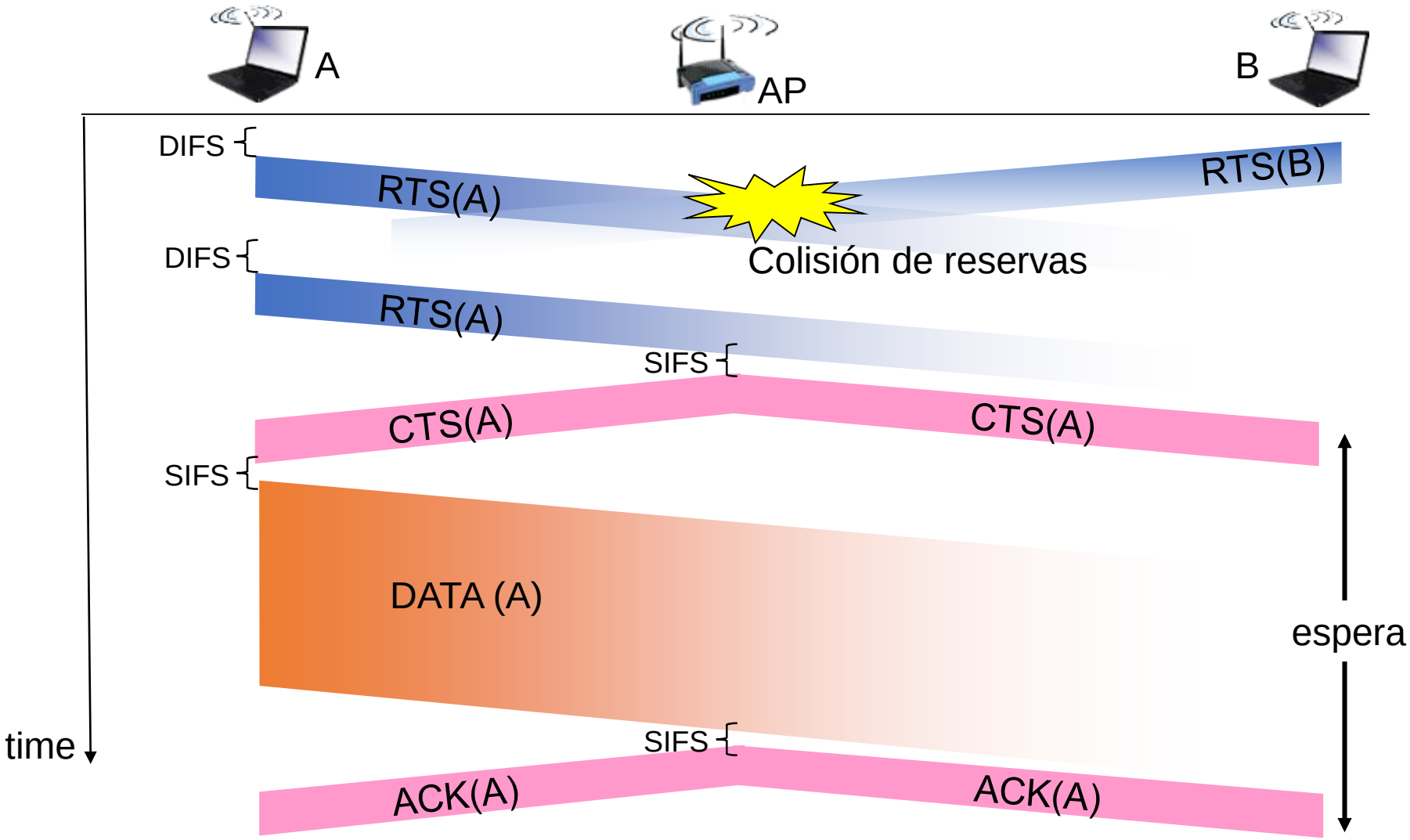
1: Antes de transmitir la trama A envía un mensaje RTS (Request To Send)

2: B responde al RTS con un CTS (Clear To Send)

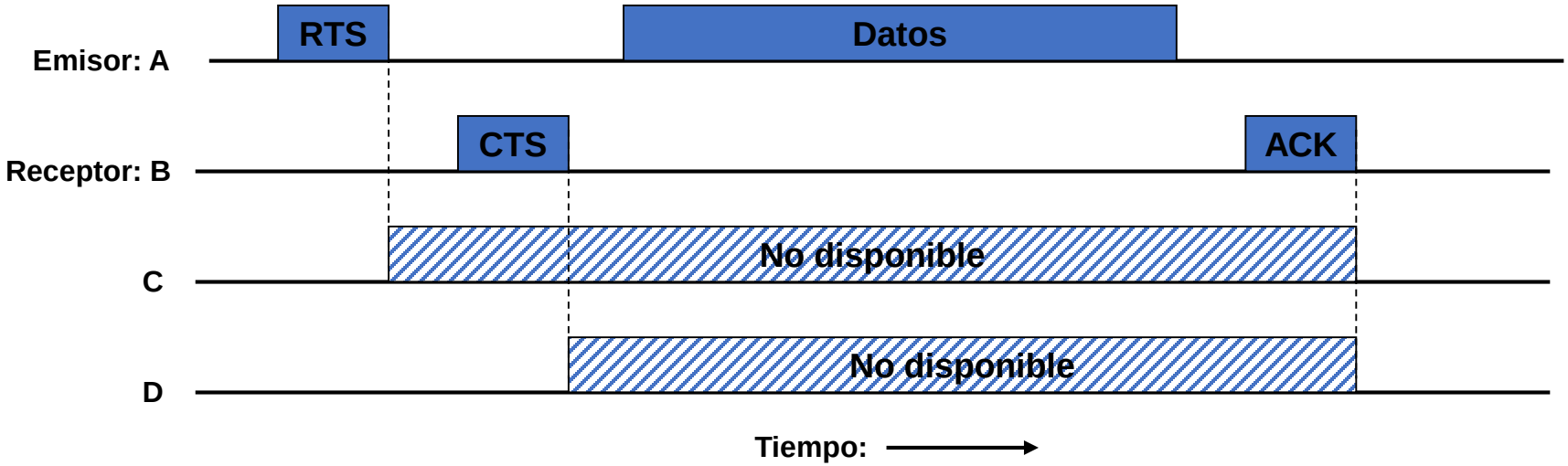
3. C no capta el RTS, pero sí el CTS. Sabe que no debe transmitir durante el tiempo equivalente a 500 bytes

4. A envía su trama seguro de no colisionar con otras estaciones

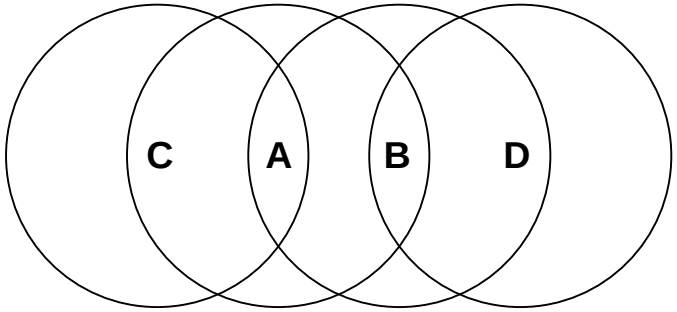
Solución al problema de la estación oculta



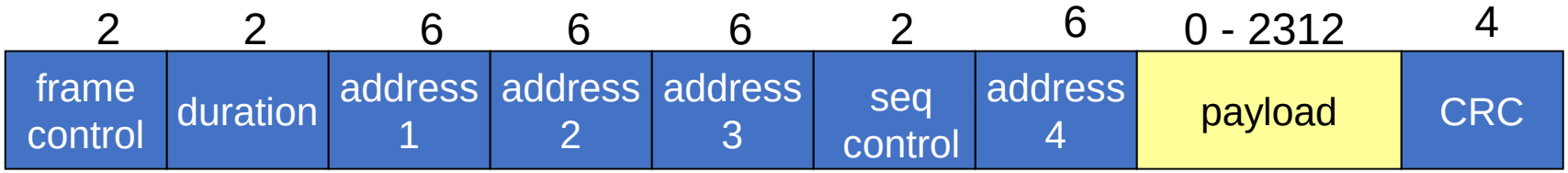
Solución al problema de la estación oculta



C y B están en el área de cobertura de A, pero D no. En cambio D está en el área de cobertura de B.



Trama 802.11



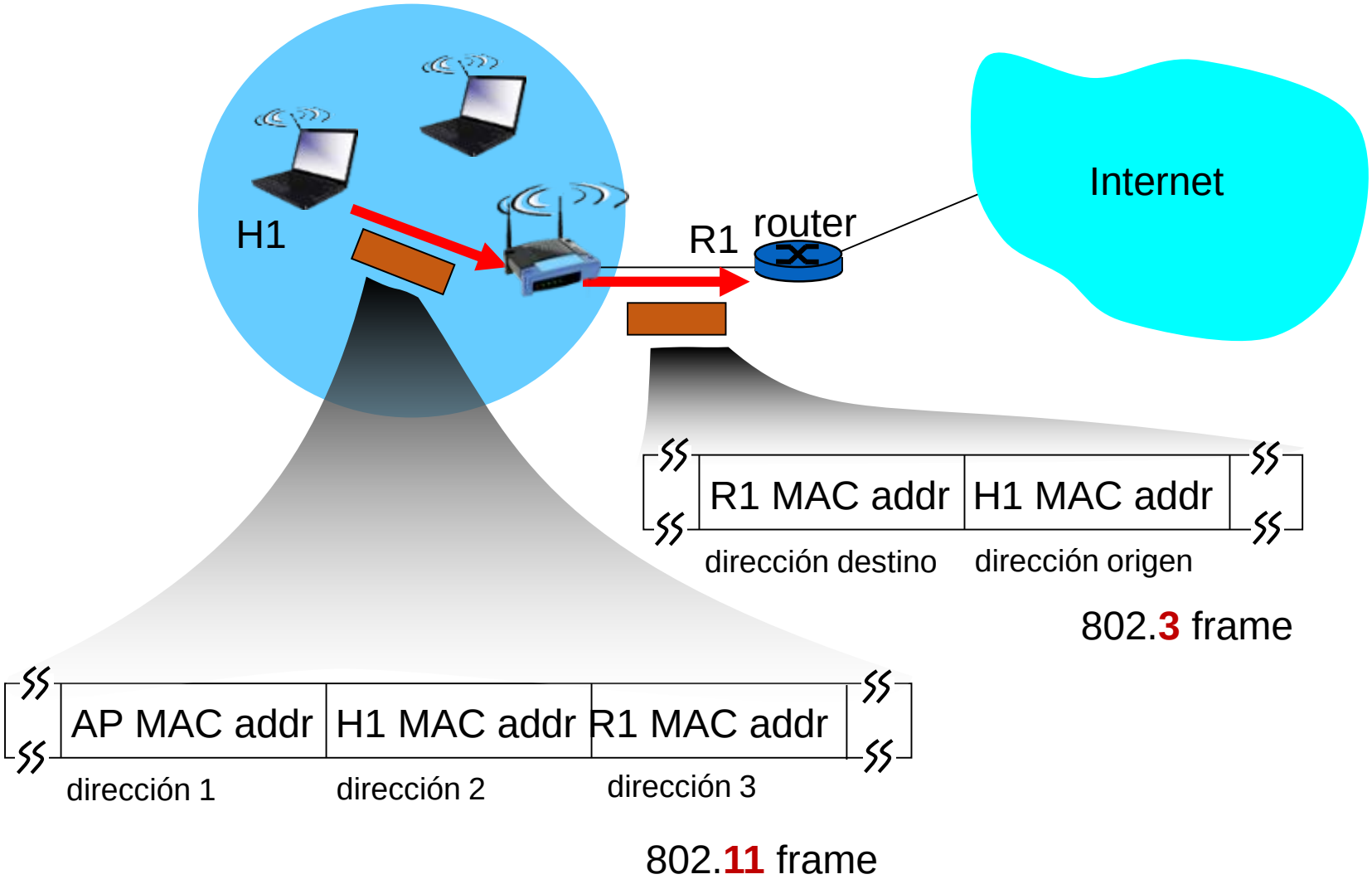
Dirección 1: dirección MAC del host inalámbrico o del AP que recibe esta trama

Dirección 2: dirección MAC del host inalámbrico o del AP que transmite esta trama

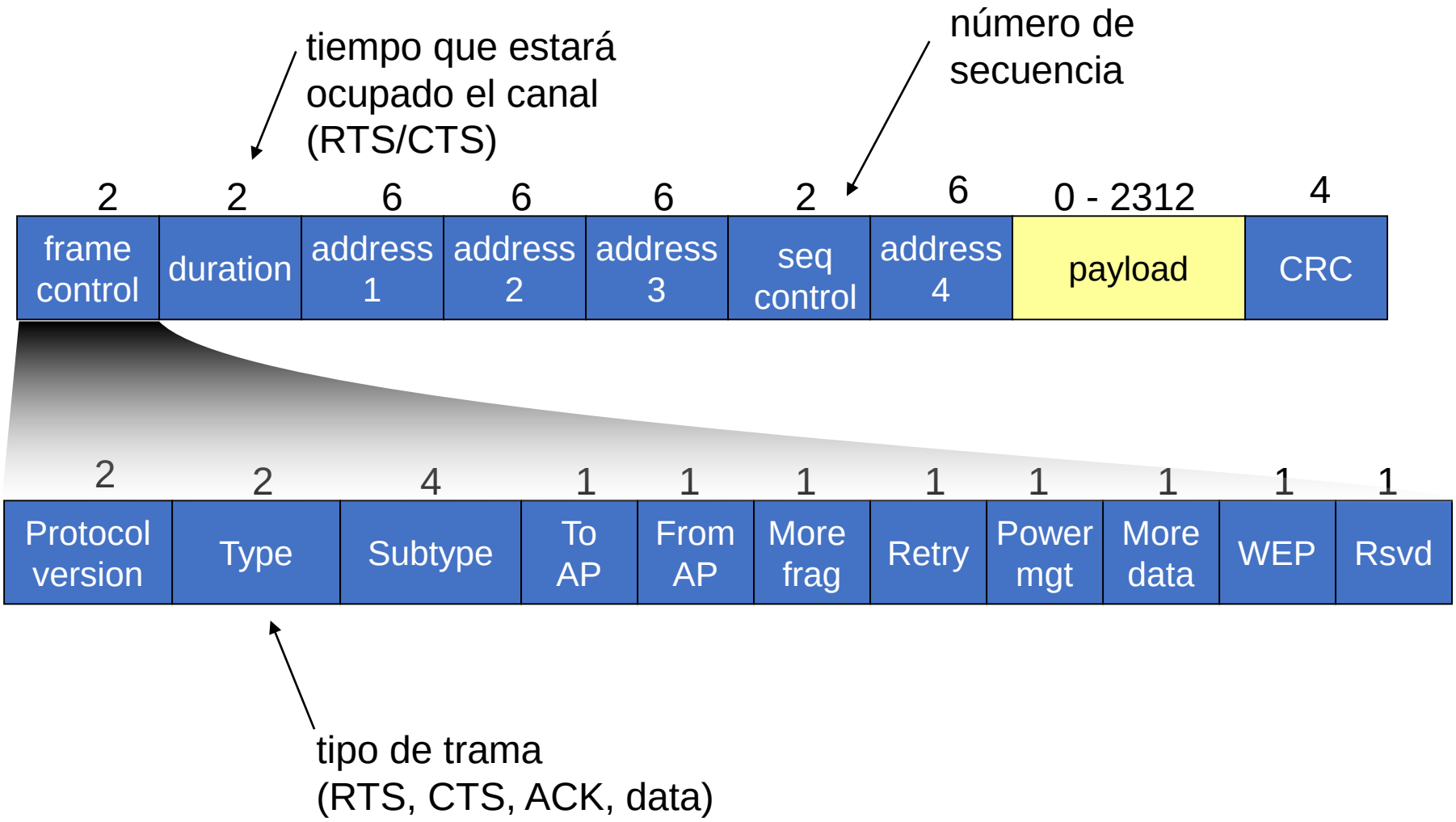
Dirección 3: dirección MAC de la interfaz del router a la que está enlazado el AP

Dirección 4: usada únicamente en modo ad hoc

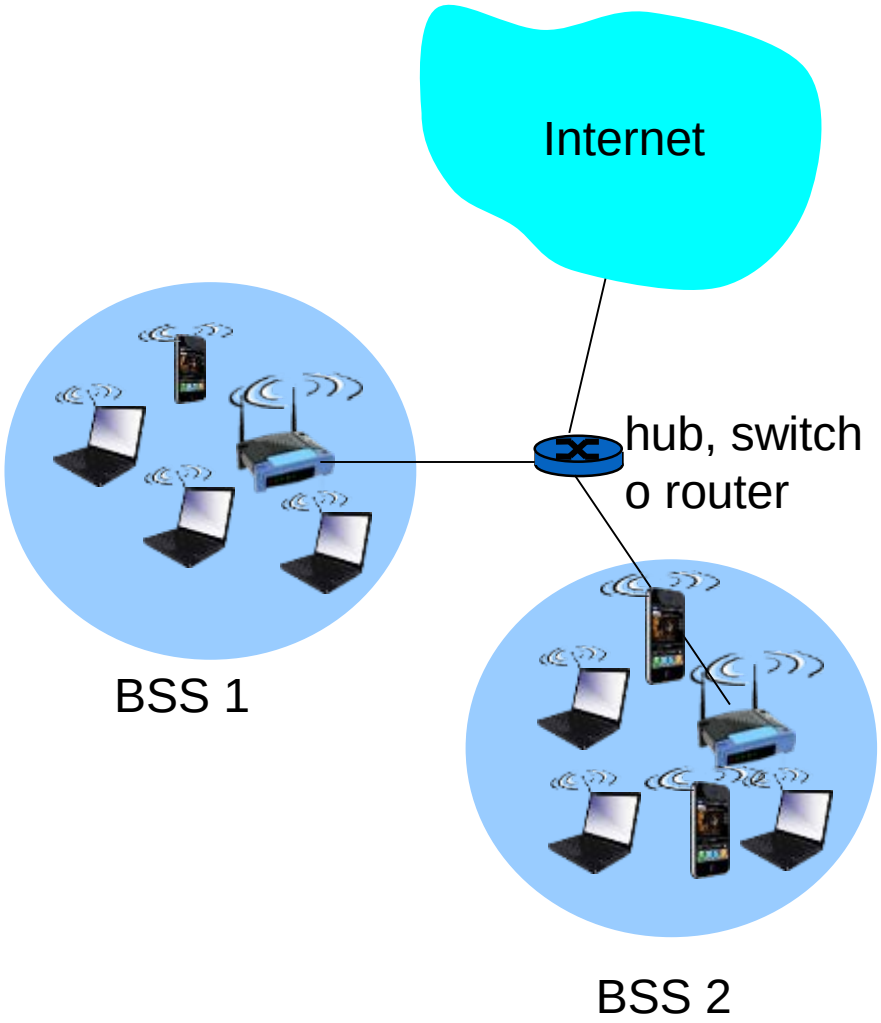
Trama 802.11


H1
R1
router
Internet
R1 MAC addr
H1 MAC addr
dirección destino
dirección origen
802.3 frame
AP MAC addr
H1 MAC addr
R1 MAC addr
dirección 1
dirección 2
dirección 3
802.11 frame

Trama 802.11

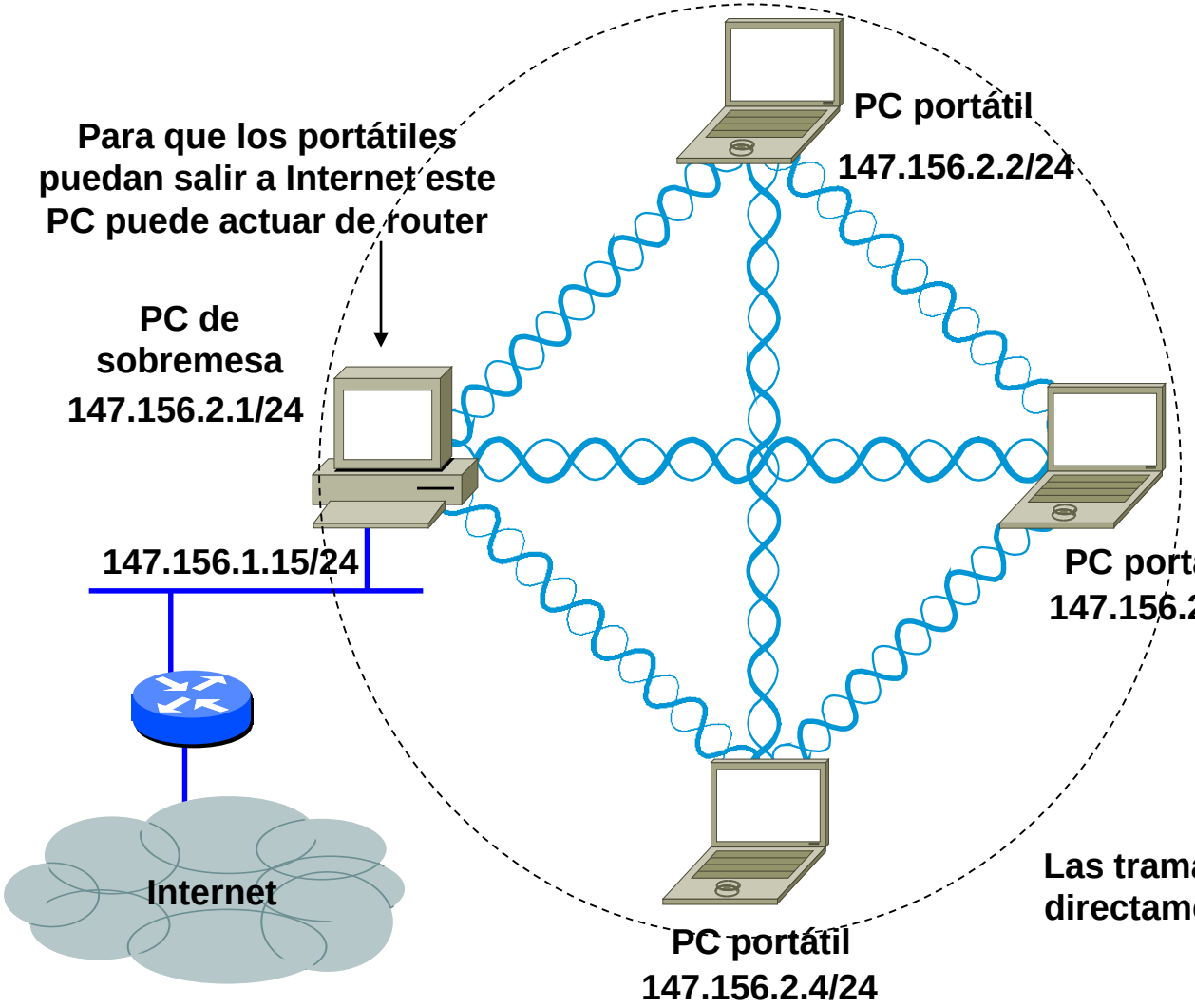

tiempo que estará ocupado el canal (RTS/CTS)
número de secuencia
2
2
6
6
6
2
6
0 - 2312
4
frame control
duration
address 1
address 2
address 3
seq control
address 4
payload
CRC
2
2
4
1
1
1
1
1
1
1
1
Protocol version
Type
Subtype
To AP
From AP
More frag
Retry
Power mgt
More data
WEP
Rsvd
tipo de trama (RTS, CTS, ACK, data)

Arquitectura 802.11



- Host inalámbrico que se comunica con una estación base
  - Estación base = punto de acceso (AP)
- Basic Service Set (BSS) (o celda) en modo infraestructura, contiene:
  - Hosts inalámbricos
  - Punto de acceso (AP): estación base
  - Modo ad hoc: sólo hosts

Red 802.11 ad hoc

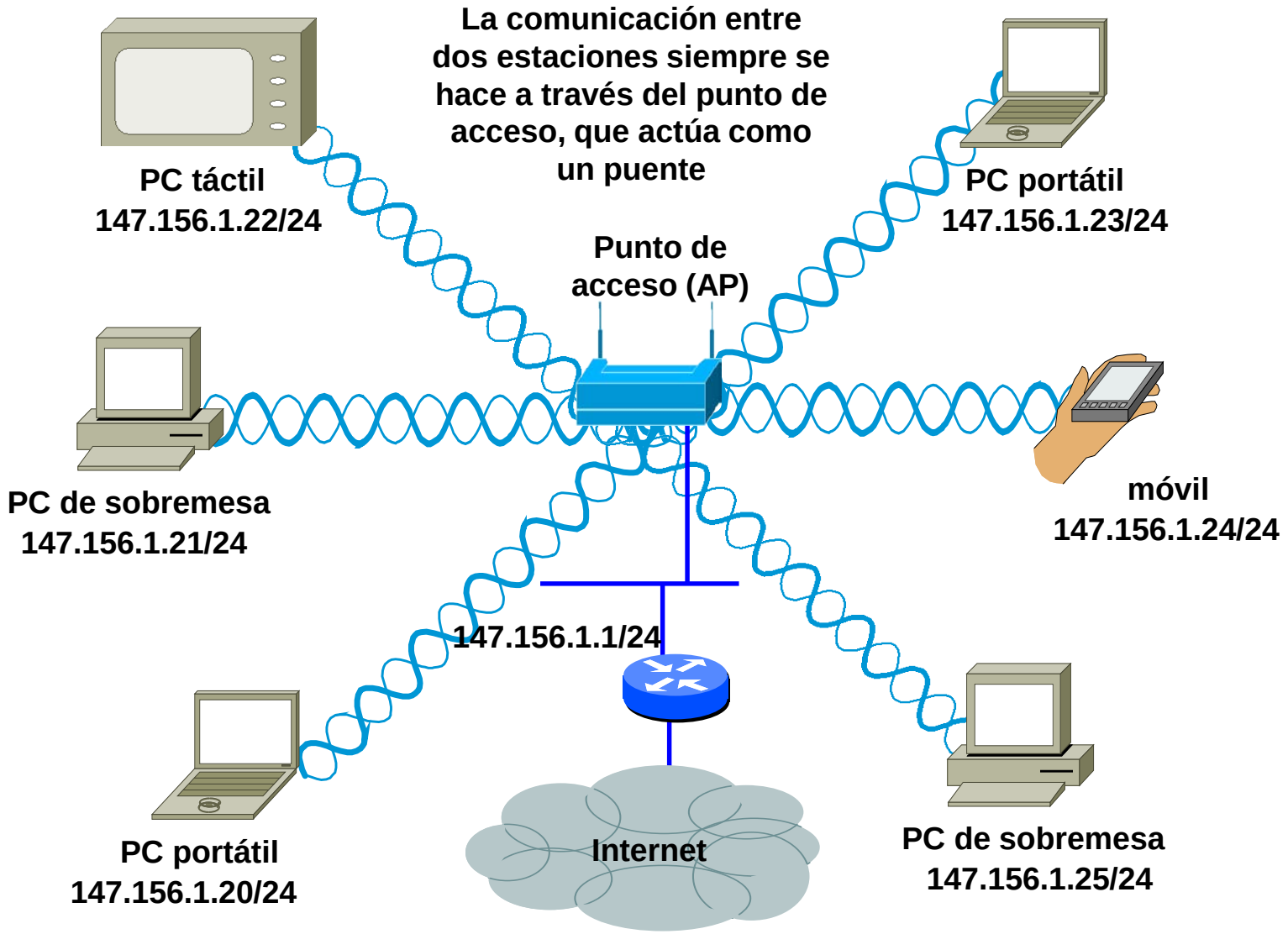


Tarjeta PCI

Adaptador USB

Las tramas se transmiten directamente de emisor a receptor

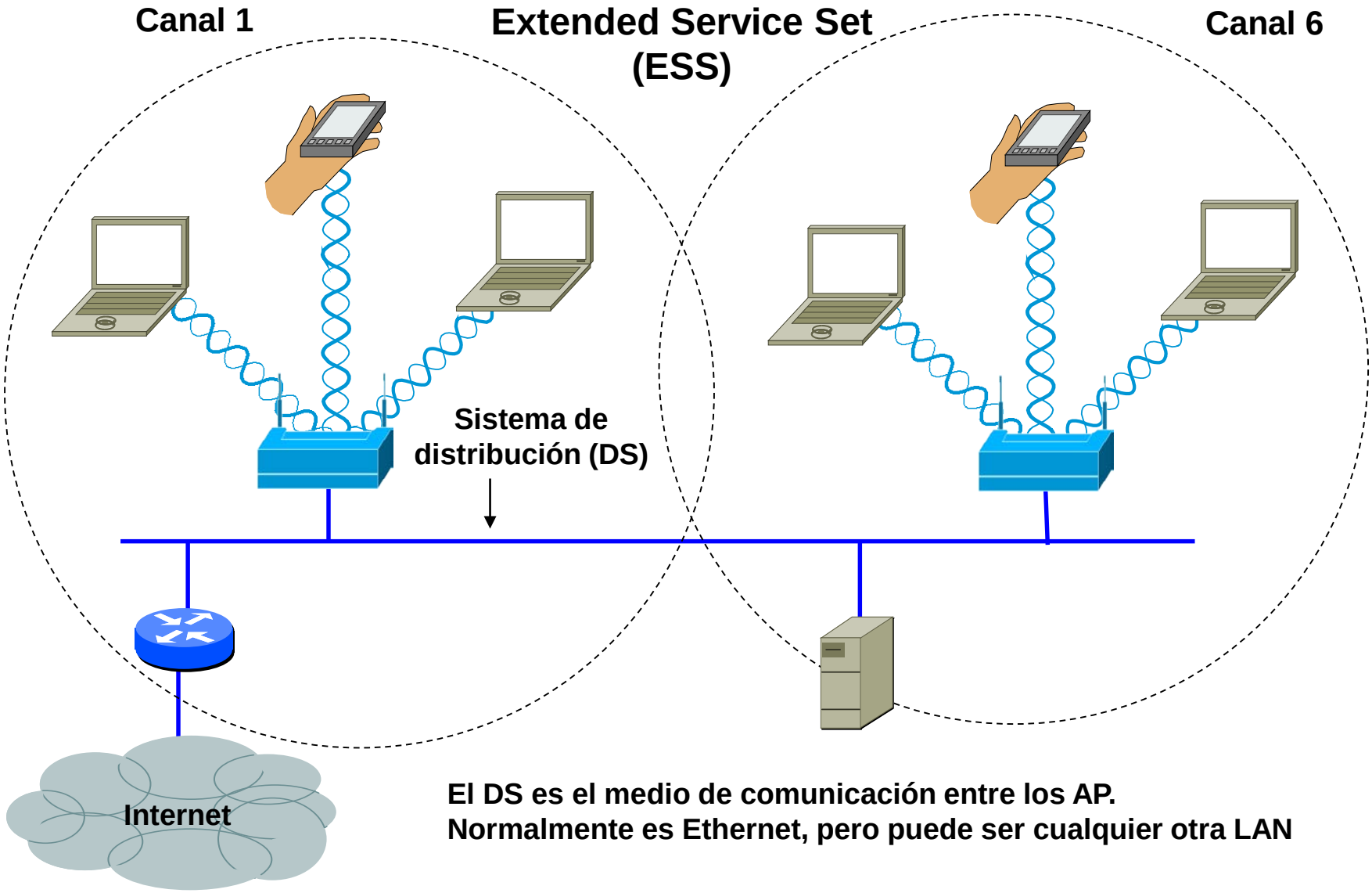
Red 802.11 infraestructura (con AP)



Red 802.11 infraestructura (con AP)

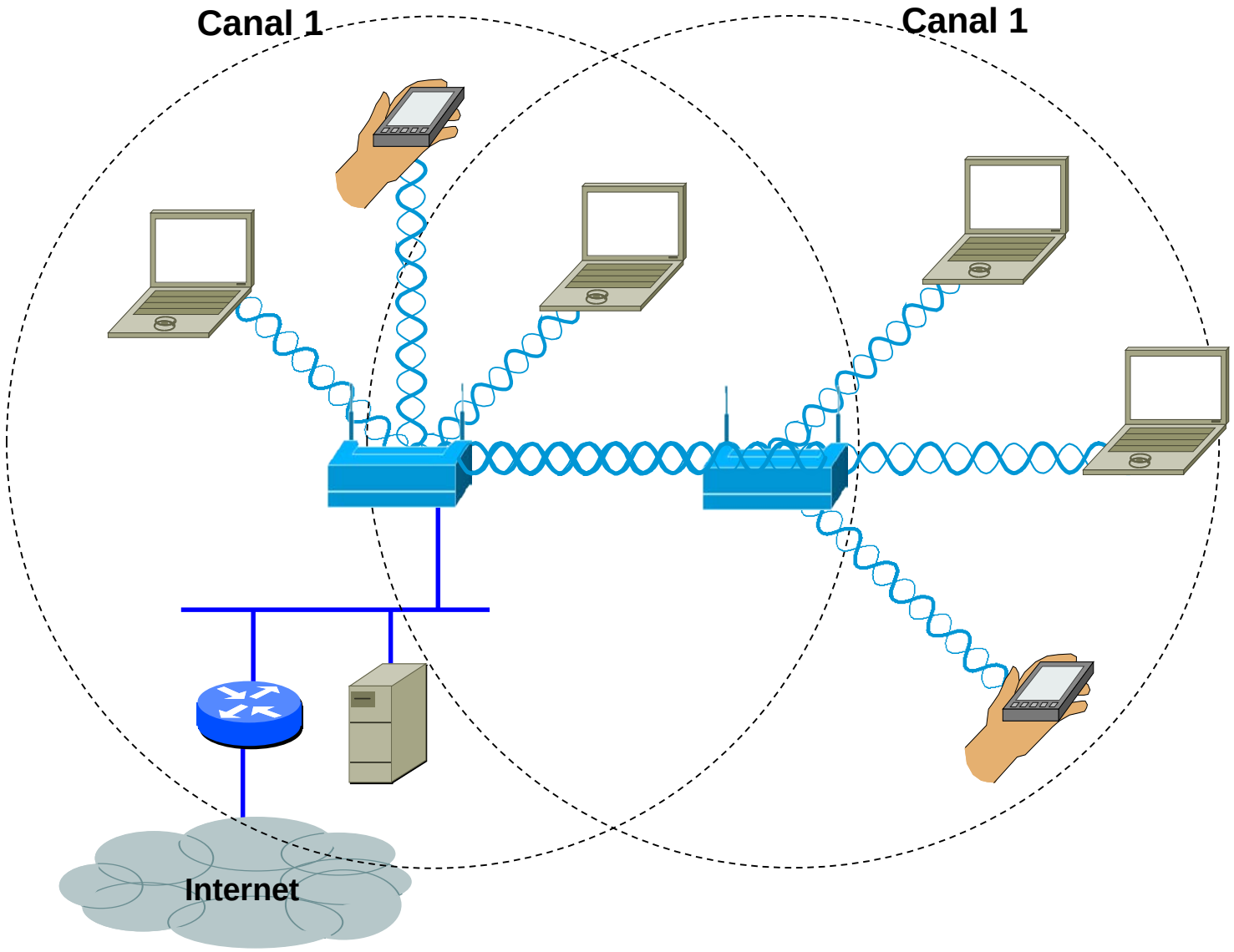
- Con puntos de acceso (AP) cada trama requiere dos emisiones de radio (salvo que el destino esté en la LAN y no en la WLAN).
- Aunque haya estaciones ocultas la comunicación siempre es posible, pues se hace a través del AP que siempre está accesible para todos
- Los AP son dispositivos fijos de la red. Por tanto:
  - Sus antenas pueden situarse en lugares estratégicos, y pueden ser de alta ganancia.
  - Se pueden dotar de antenas diversidad (para evitar los problemas de multitrayectoria)
  - No tienen requerimientos de bajo consumo (no usan baterías)

Red 802.11 infraestructura extendida



El DS es el medio de comunicación entre los AP.
Normalmente es Ethernet, pero puede ser cualquier otra LAN

Red 802.11 infraestructura (AP+repetidor)



Canales y SSID del AP

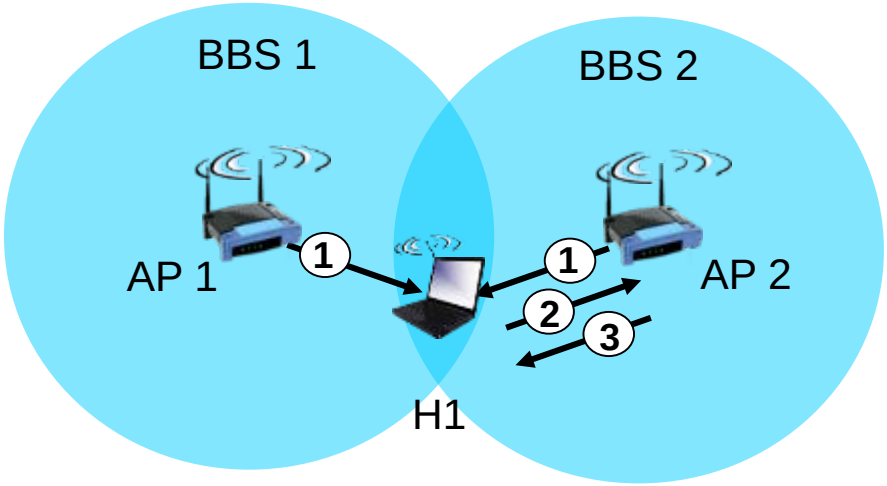
- En 802.11b se divide el espectro 2.4-2.485GHz en 11 (o 13 en Europa) canales a distintas frecuencias
- En 802.11a se divide el espectro 5.1-5.8GHz en 24 canales
- El administrador del AP escoge el canal para evitar interferencias con APs cercanos
- También puede elegir canales que no se solapen
  - En 2.4GHz son 3 (1-6-11, o 1-7-13 en Europa)
  - En 5GHz son los 24
- El administrador asigna un Service Set Identifier (SSID) para identificar el AP

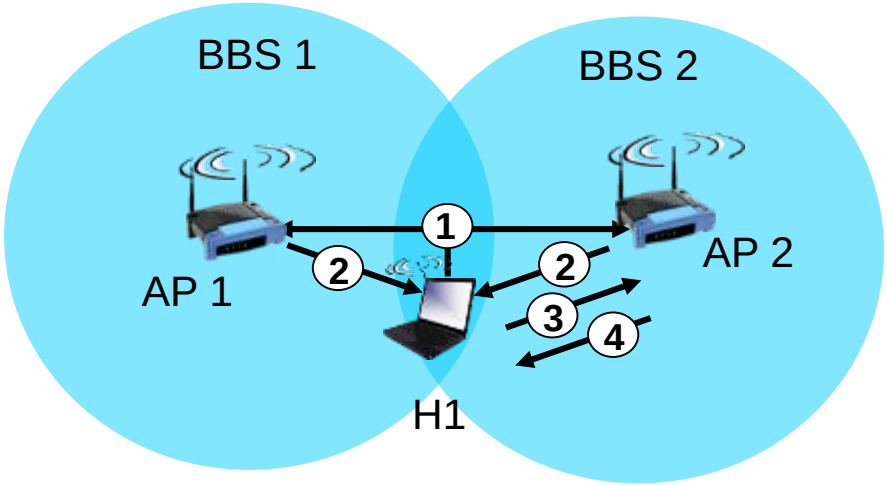
Asociación del host con el AP

Antes de enviar o recibir datos, el host se debe asociar con el AP:

1. El AP emite tramas baliza (10 beacon/seg) con su dirección MAC y su nombre (SSID)
2. Host escanea los canales buscando esos beacons
3. El usuario selecciona el AP al que asociarse (o automáticamente al de mayor intensidad de señal o al más descongestionado)
4. Se autentican host y AP si así se requiere (802.11i)
5. Habitualmente el host emplea DHCP para obtener su IP y datos de la subred

Asociación del host con el AP





Escaneo pasivo:

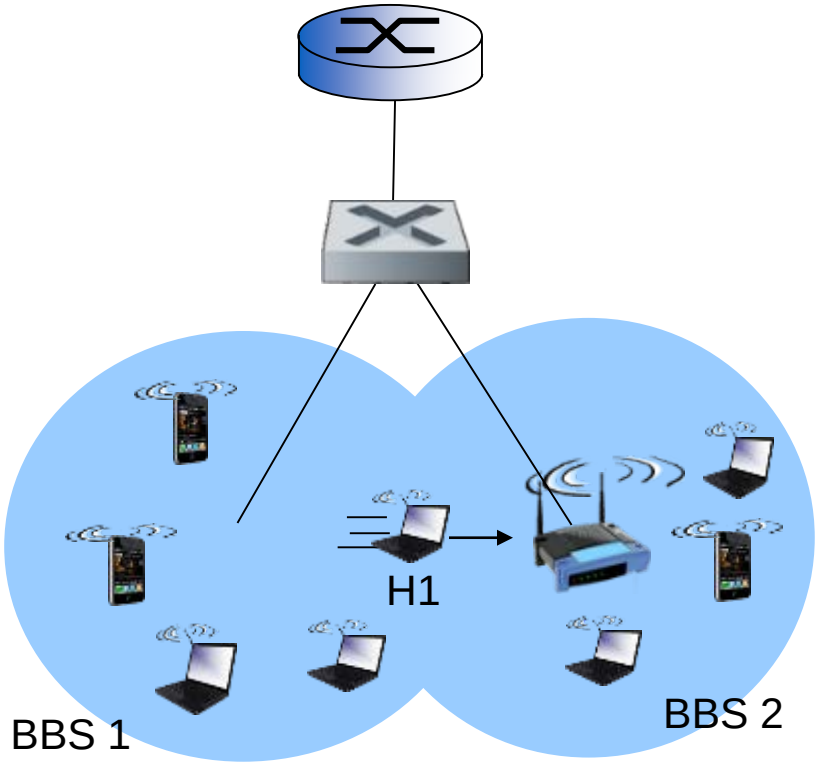
(1) Beacons enviados desde los APs
(2) Trama de solicitud de asociación enviada de H1 a un AP concreto
(3) Trama de respuesta de asociación enviada de ese AP a H1

Escaneo activo:

(1) Difusión desde H1 de una trama de solicitud de sondeo
(2) Envío de tramas de respuesta de sondeo desde los APs
(3) Envío de trama de solicitud de asociación de H1 al AP seleccionado
(4) Envío de trama de respuesta de asociación desde ese AP a H1

Movilidad dentro de la misma subred IP

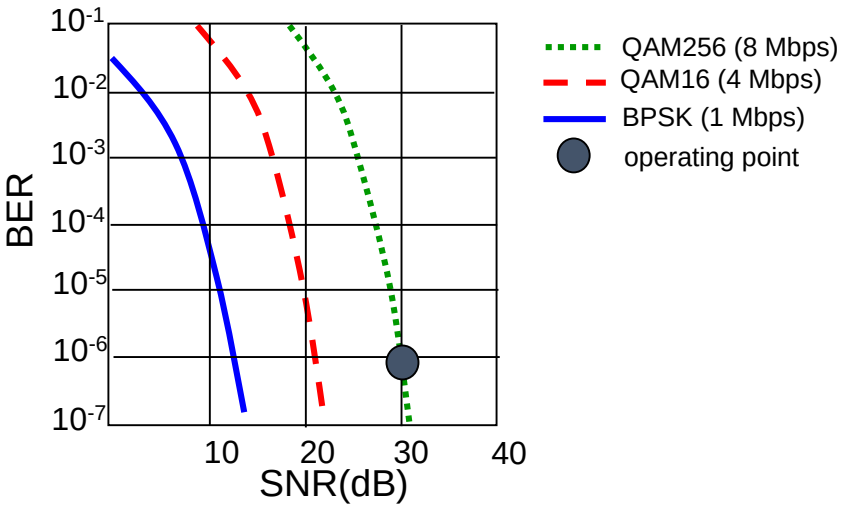
- Si un host (H1) se mueve pero se mantiene en la misma subred IP, su direccion IP puede mantenerse igual
- El switch tendrá que aprender a qué AP está asociado ahora H1, con su capacidad de auto-aprendizaje



Adaptación de velocidad

Escenario: Host que se aleja de la estación base

- Cerca de la estación base puede utilizar una técnica de modulación con alta velocidad de transmisión y mantener una baja BER
- Según se aleja, disminuye la SNR y aumenta la BER
- Debe cambiar la técnica de modulación, disminuyendo la velocidad y la BER



1. SNR disminuye, BER aumenta según se aleja el host de la estación base

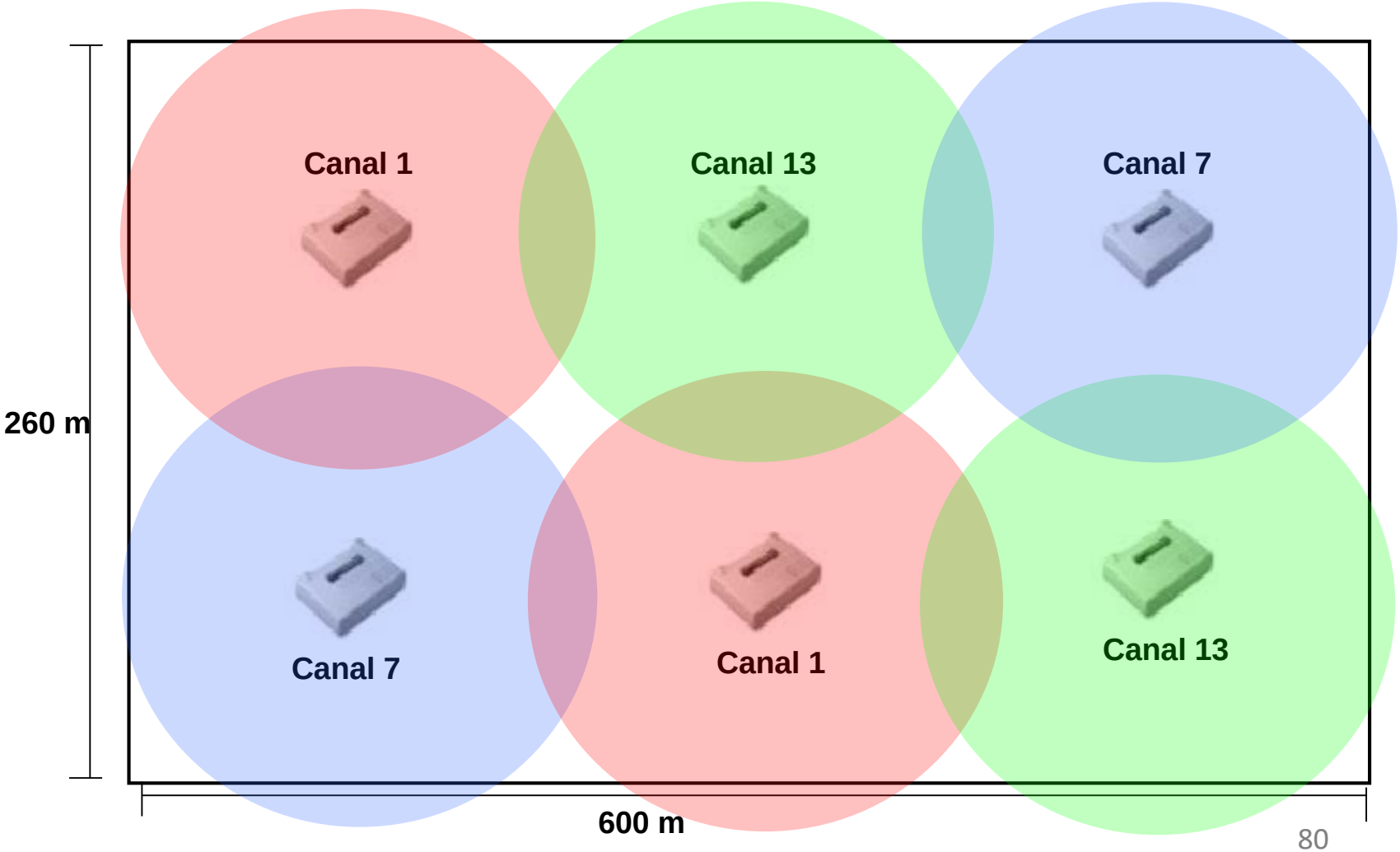
2. Cuando BER es demasiado alto se cambia a una técnica de menor velocidad pero menor BER

Gestión de la potencia

- Un host indica al AP que pasa al estado “dormido” con un bit en la trama 802.11
- Pone un temporizador para justo antes del siguiente beacon (habitualmente 100 ms)
- El AP guarda las tramas que lleguen para ese host hasta el siguiente beacon
- El host se despierta (250 microseg) y recibe del AP un beacon con la lista de hosts con tramas guardadas
- Si está entre ellos, las recibe, si no, vuelve a dormir
- Así podría estar un 99% del tiempo dormido

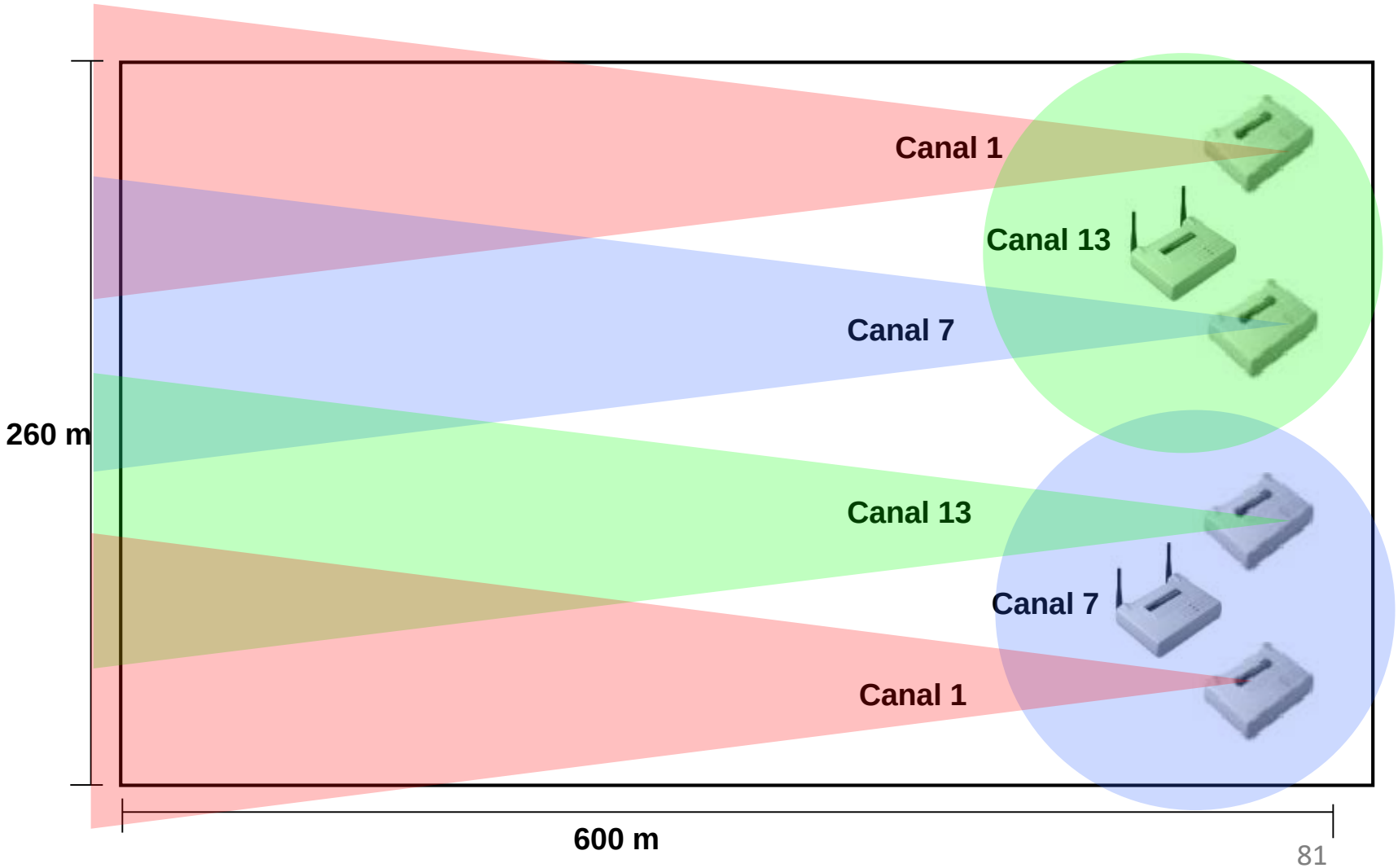
Ejemplo 1: WLAN en almacén

- **Tomas RJ45 (100BASE-TX) disponibles por todo el almacén para conexión de los AP**
- **Antenas omnidireccionales de mástil de alta ganancia (5,2 dBi)**



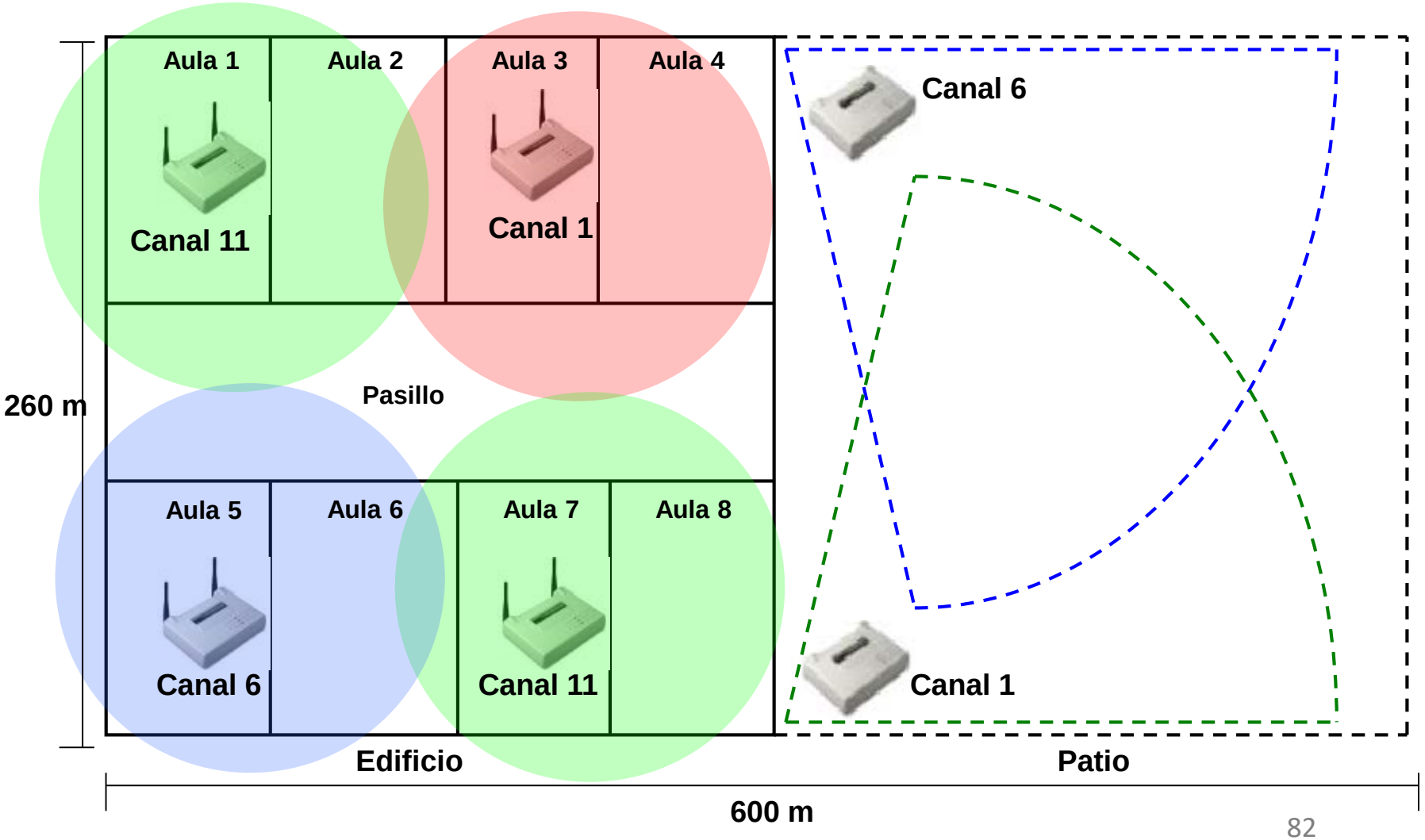
Ejemplo 2: WLAN en almacén

- **Tomas RJ45 (100BASE-TX) disponibles sólo en un lado del almacén**
- **Antenas Yagi (13,5 dBi) y Dipolo diversidad(2,14 dBi)**



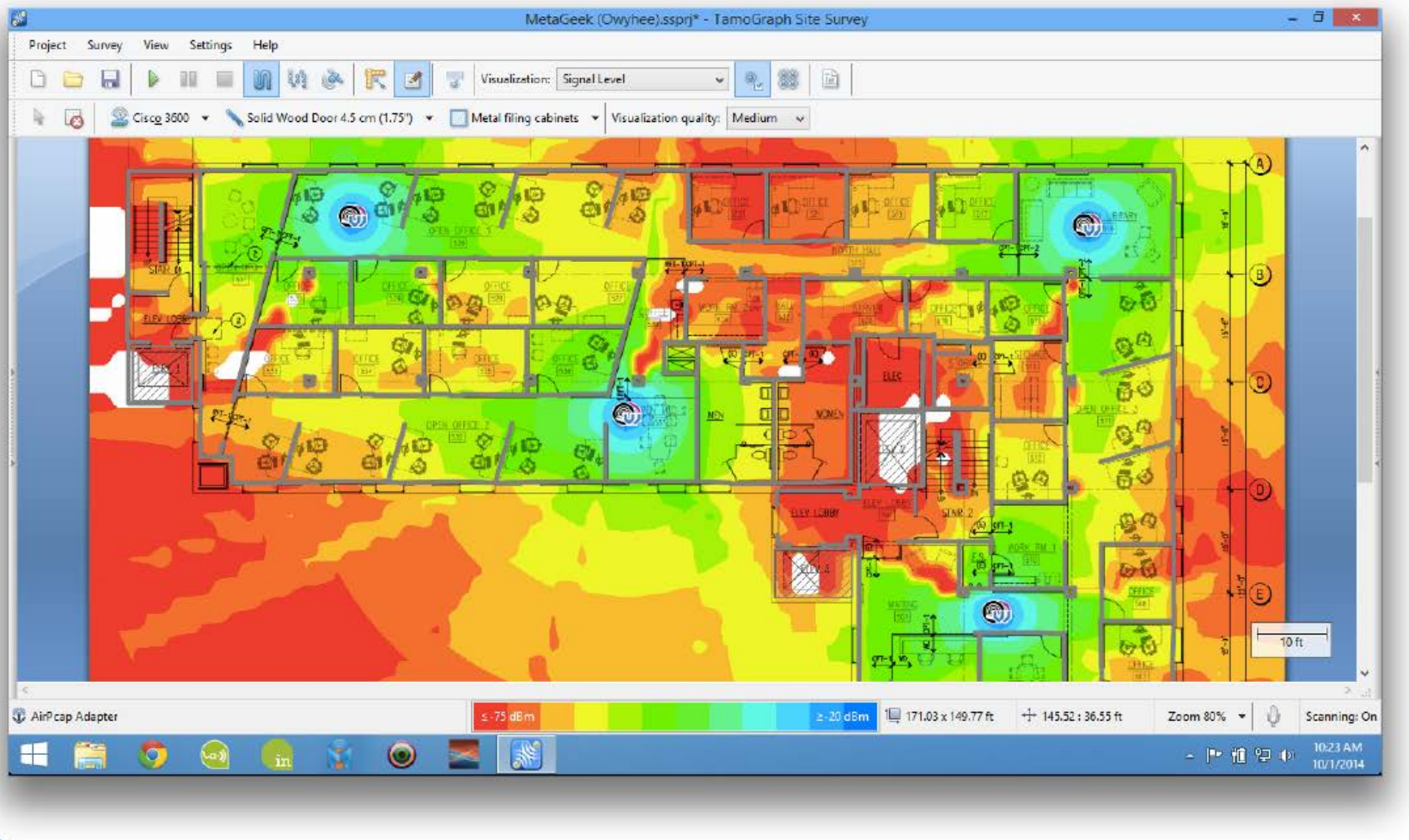
Ejemplo 3: WLAN en campus

- **Antenas dipolo diversidad (2,14dBi) en las aulas y de parche (8,5 dBi) montadas en pared para el patio**



Planificación de cobertura wifi

Universidad Rey Juan Carlos

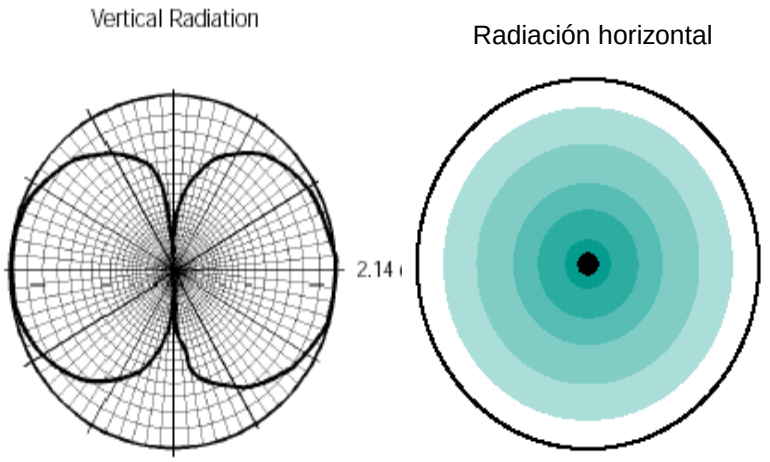


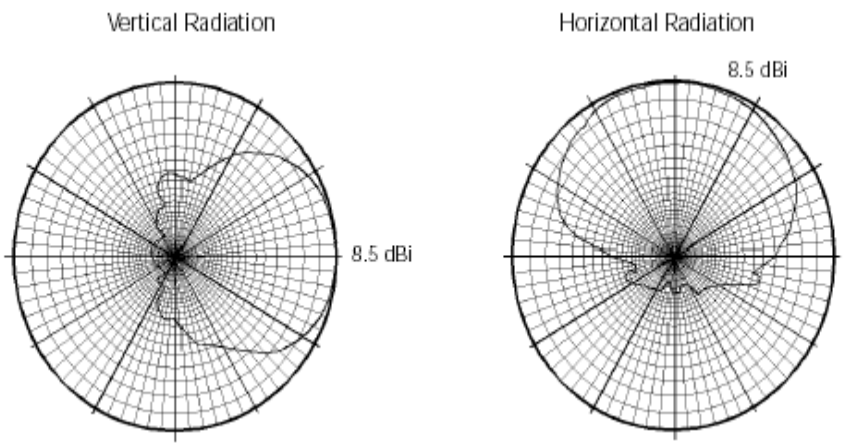
metageek

Ejemplos de antenas

Antena dipolo diversidad para contrarrestar efectos multitrayectoria (2,14 dBi)

Antena de parche para montaje en pared interior o exterior (8,5 dBi) Alcance: 3 Km a 2 Mb/s, 1 Km a 11 Mb/s





Relación antena-potencia

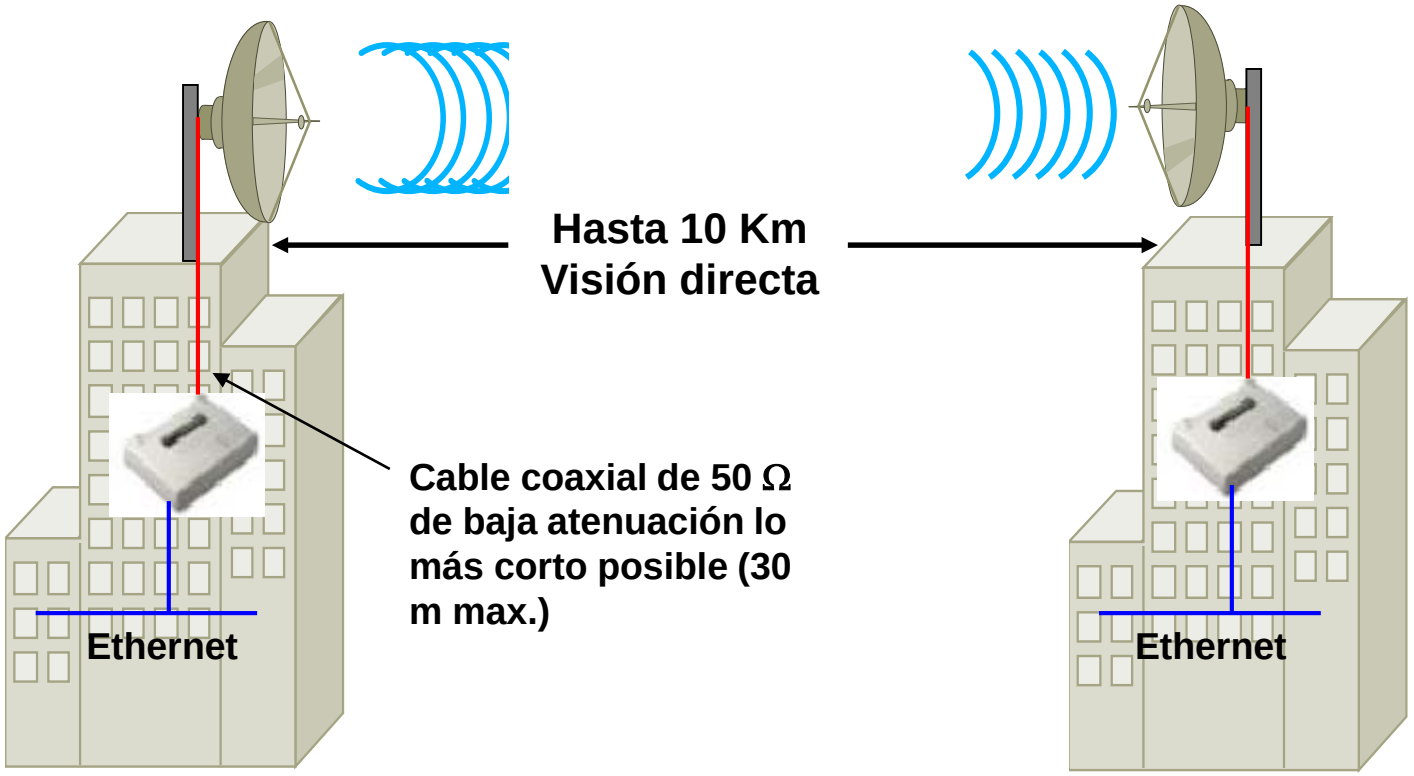
- Las normativas fijan una potencia máxima de emisión y una densidad de potencia. Por tanto con una antena de mucha ganancia es preciso reducir la potencia.
- Los límites varían según el 'dominio regulatorio'. Por ejemplo en el caso de EMEA (Europa, Medio Oriente y África) los límites son los de la tabla adjunta.

Ganancia (dBi)	Pot. Máx. (mW)
0	100
2,2	50
5,2	30
6	30
8,5	5
12	5
13,5	5
21	1

Puentes inalámbricos entre LANs

- Los sistemas de transmisión vía radio de las LANs inalámbricas pueden aprovecharse para unir LANs entre sí
- Esto permite en ocasiones un ahorro considerable de costos en alquiler de circuitos telefónicos
- Los dispositivos que se utilizan son puentes inalámbricos, parecidos a los puntos de acceso
- Como los puntos a unir no son móviles se pueden usar antenas muy direccionales, con lo que el alcance puede ser considerable

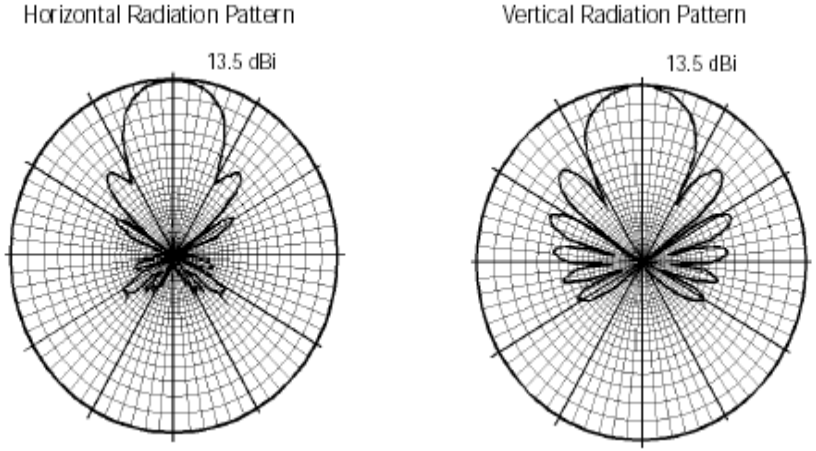
Configuración punto a punto



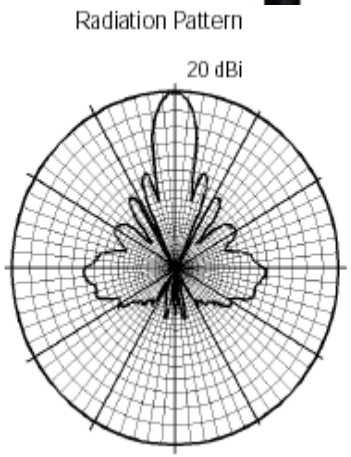
Restricciones ETSI: **Ganancia máxima: 20 dBi (antena parabólica)**
Potencia máxima: 100 mW
Alcance máximo: 10 Km (visión directa)

Antenas de largo alcance

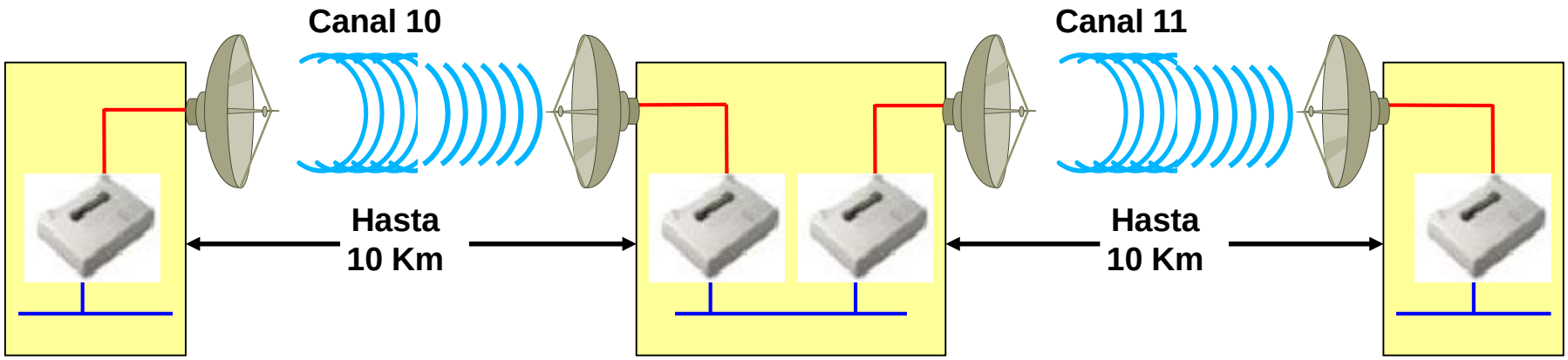
Antena Yagi exterior (13,5 dBi)
Alcance: 6 Km a 2 Mb/s, 2 Km a 11 Mb/s



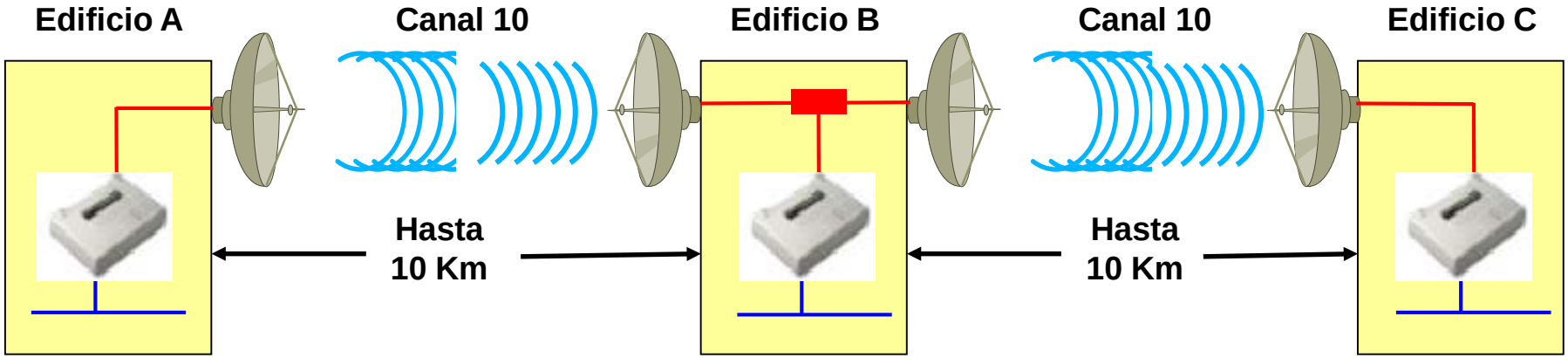
Antena Parabólica exterior (20 dBi)
Alcance: 10 Km a 2 Mb/s, 5 Km a 11 Mb/s



Técnicas para aumentar el alcance

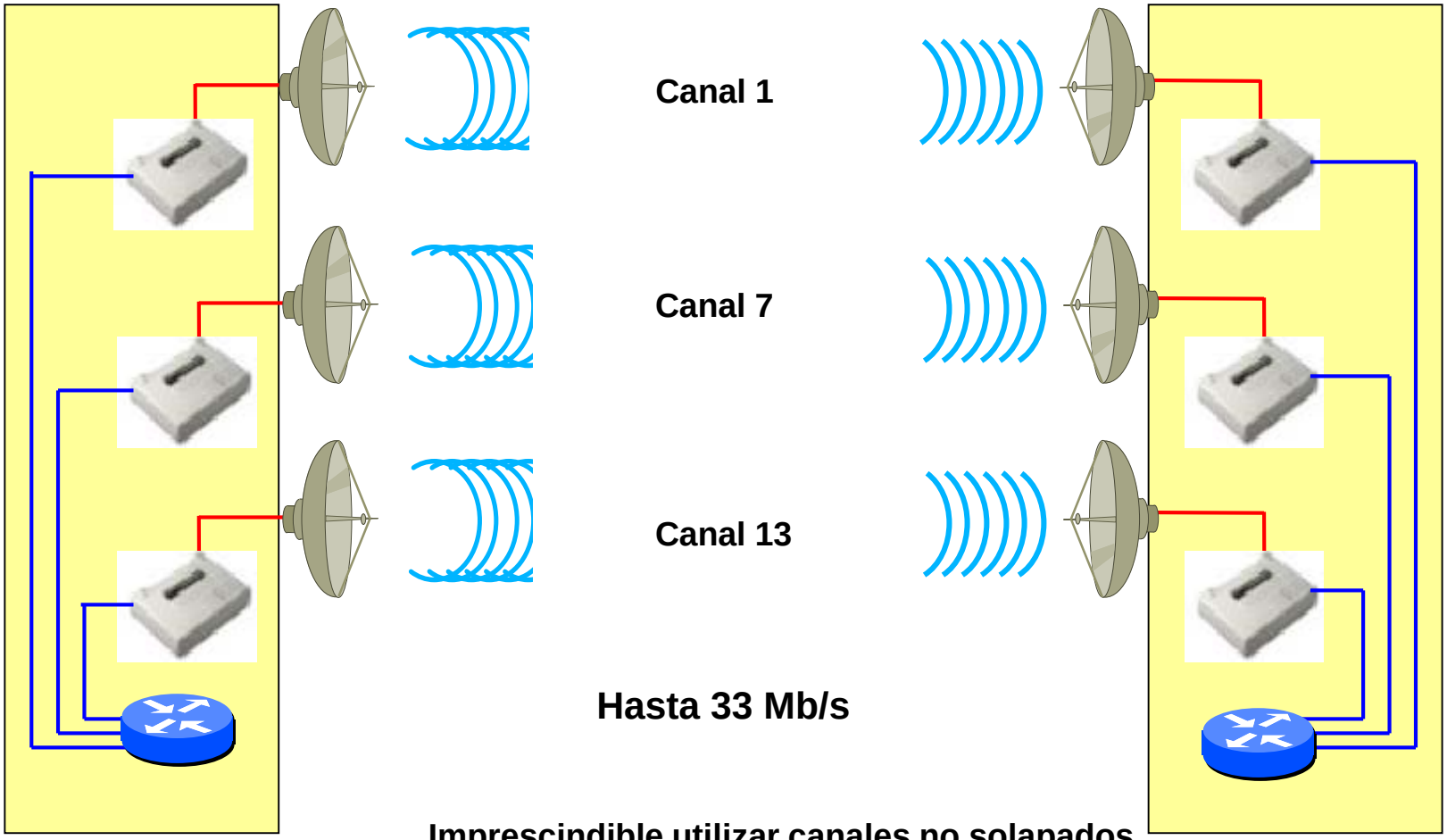


Hasta 11 Mb/s para cada enlace



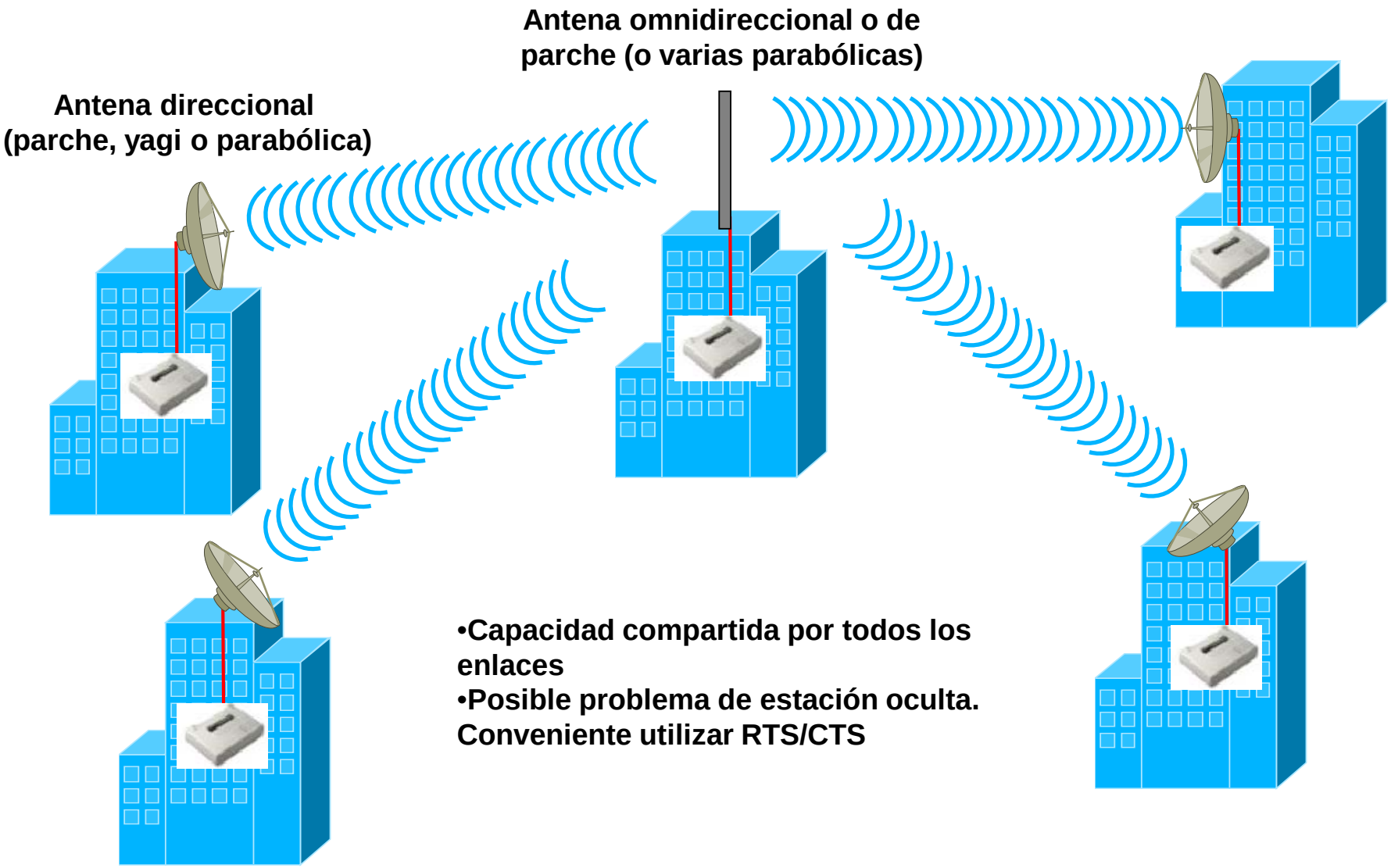
Hasta 11 Mb/s, compartidos entre ambos enlaces
Posible problema de estación oculta (entre A y C). Necesidad de utilizar mensajes RTS/CTS

Técnicas para aumentar el alcance



Imprescindible utilizar canales no solapados

Configuración multipunto



- Capacidad compartida por todos los enlaces
- Posible problema de estación oculta. Conveniente utilizar RTS/CTS

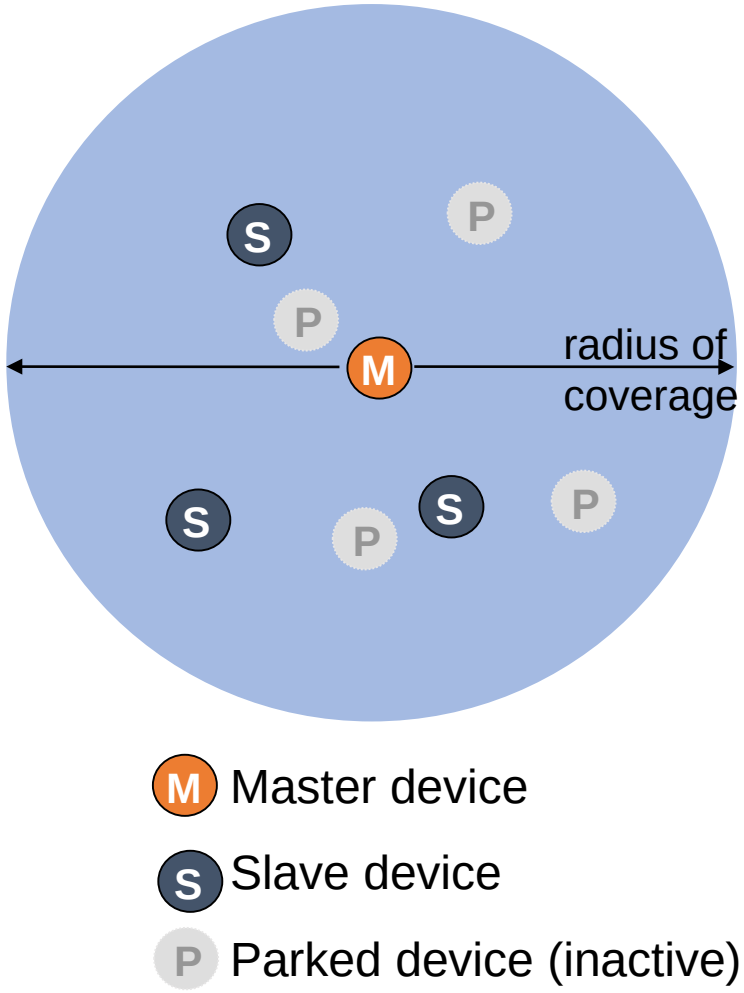
Bluetooth®

ZigBee®

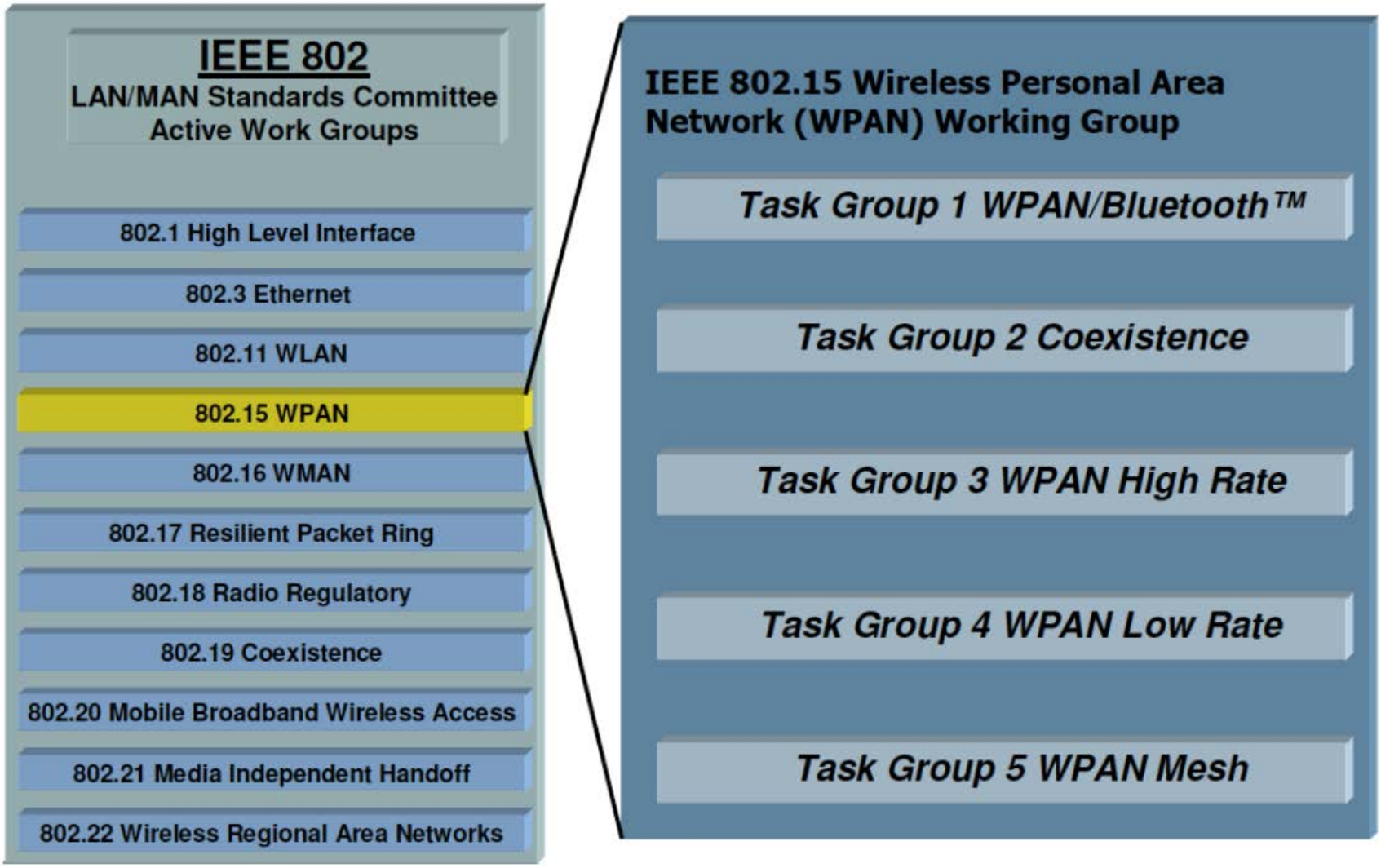
1.2. Redes inalámbricas personales 802.15

Wireless Personal Area Networks (WPAN)

- Distancia menor de 10m
- Sustituyen a los cables (ratón, teclado, auriculares…)
- Redes ad hoc, no infraestructura
- Maestro/esclavo: los esclavos piden permiso al maestro para enviar
- IEEE802.15: evolucionó de la especificación Bluetooth
- Banda 2.4-2.5GHz



Universidad Rey Juan Carlos



1.2. Redes inalámbricas personales 802.15

La IEEE ha buscado establecer una serie de estándares internacional que toman forma en las especificaciones 802.15:

- **El Grupo 802.15.1** es responsable por la estandarización del conjunto de especificaciones recopiladas por el estándar Bluetooth.
- **El Grupo 802.15.2** es responsable por los aspectos de coexistencia de dos o más tecnologías inalámbricas diferentes que compartan el mismo ambiente de operación y espectro radioeléctrico. Específicamente el grupo se dedica a dos grandes tareas, la primera cuantificar el efecto de la interferencia mutua entre dispositivos que empleen las tecnologías de WPAN y WLAN, y como segunda tarea propone el establecimiento de mecanismos de coexistencia entre dispositivos WPAN y WLAN en las capas física PHY y de accedo al medio MAC.
- **El Grupo 802.15.3** es responsable por el desarrollo de una especificación de WPAN de alta velocidad, de más de 20 Mbps. El primer borrador describe una especificación que opera en 5 canales de 15 MHz en la banda ISM de 2.4 GHz.
- **El Grupo 802.15.3a** se formó a finales del 2001 como una propuesta para desarrollar una alternativa a la especificación 802.15.3 teniendo como objetivo el desarrollar un estándar de capa física PHY, basado en UWB, para soportar tasas de transferencia de datos de 110 a 480 Mbps, en distancias inferiores a los 10 metros.
- **El Grupo 802.15.4** está enfocado en la estandarización de red WPAN de baja velocidad y muy bajo consumo de potencia (low power LP-WPAN) lo que conduce a que los dispositivos puedan operar de forma autónoma con baterías teniendo una vida útil de meses e incluso años, empleando un bajo nivel de complejidad y teniendo un muy bajo costo.

Bluetooth (IEEE 802.15.1)

- Objetivo: reemplazar cables de conexión entre periféricos
- Esta tecnología se creó en el seno de un Grupo de Trabajo creado por Nokia y Ericsson. Mas tarde lo adoptó el IEEE como el comité 802.15
- Bluetooth fue un rey danés que en el siglo X unificó Dinamarca y Noruega
- Estándar abierto aprobado por el IEEE en junio de 2002

Bluetooth: The chronicle

Bluetooth 1.0

1998.10 – 2003. 11
"Base Rate"
- 1Mbps data rate
- V1.0 - Draft
- V1.0A - published on 1999.7
- V1.0B Enhanced the Interoperability
- V1.1 - IEEE 802.15.1
- V1.2 Enhanced the compatibility

Bluetooth 2.0 + EDR

2004. 11 – 2007. 7
"Enhanced Data Rate"
- Higher ordered modulation for data payload
- 2Mbps or 3Mbps physical data rate
- V2.0
- V2.1

Bluetooth 3.0 + HS

2009. 4
"HS Mode"
- AMP Alternative MAC/PHY
- Implement high data rate by using 802.11 protocols.
- Facing the Challenge from Wi-Fi
- V3.0

Bluetooth 4.0

2010. 6 – 2014. 12
"Low Energy"
- Facing the IoT application
- Changed the protocol greatly, almost a new technology
- V4.0
- V4.1
- V4.2

- Bluetooth 5 (2016): 200m de alcance y 100Mbps.
- BLE con 2Mbits/s. Actualmente versión 5.2 (2020)

Nivel físico en Bluetooth

- Tecnología muy similar a 802.11 FHSS:
  - Misma banda (2,4 GHz)
  - Misma tecnología de radio (Frequency Hopping)
- Pero:
  - Potencias de emisión inferiores (diseñado para equipos portátiles, como móviles, con baterías de baja capacidad)
  - Alcance mucho menor (10 m)
  - Velocidad más reducida (721 Kb/s)
  - Cambio de frecuencias mucho más frecuente que en 802.11 (1600 en vez de 50 veces por segundo)
- Existe probabilidad de interferencia entre:
  - Dos redes Bluetooth próximas
  - Una red Bluetooth y una 802.11 a 2,4 GHz (sobre todo FHSS)
  - Una red Bluetooth y un horno de microondas

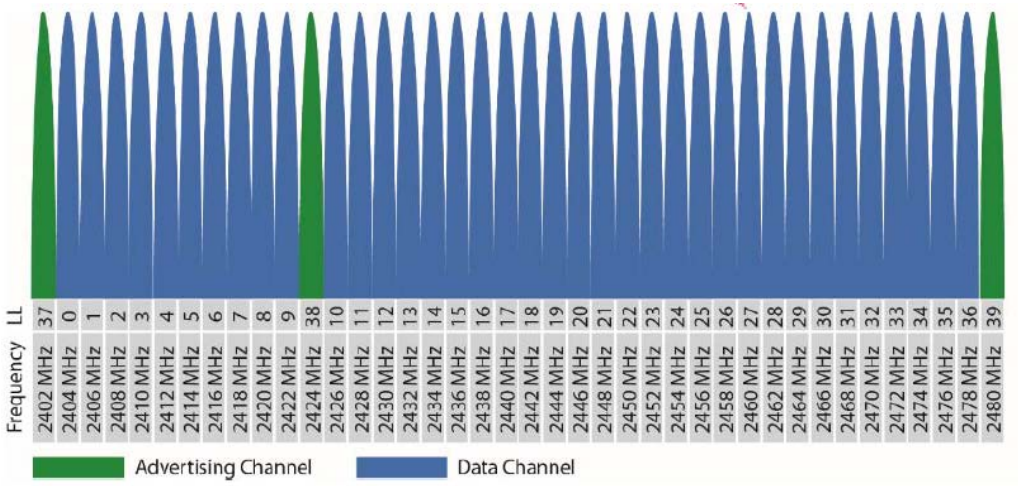
Nivel físico en Bluetooth

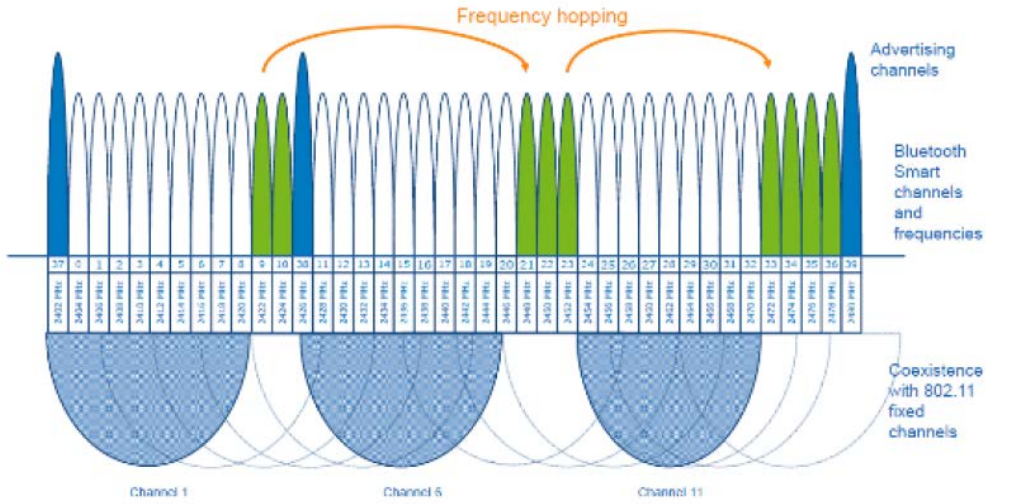
Bluetooth:

- TDM
- Particiones de 625µs
- 79 canales
- Frequency Hopping
- Hasta 4 Mbps

BLE

- 40 canales de 2MHx
- 3 canales de anuncio
- 37 canales de datos





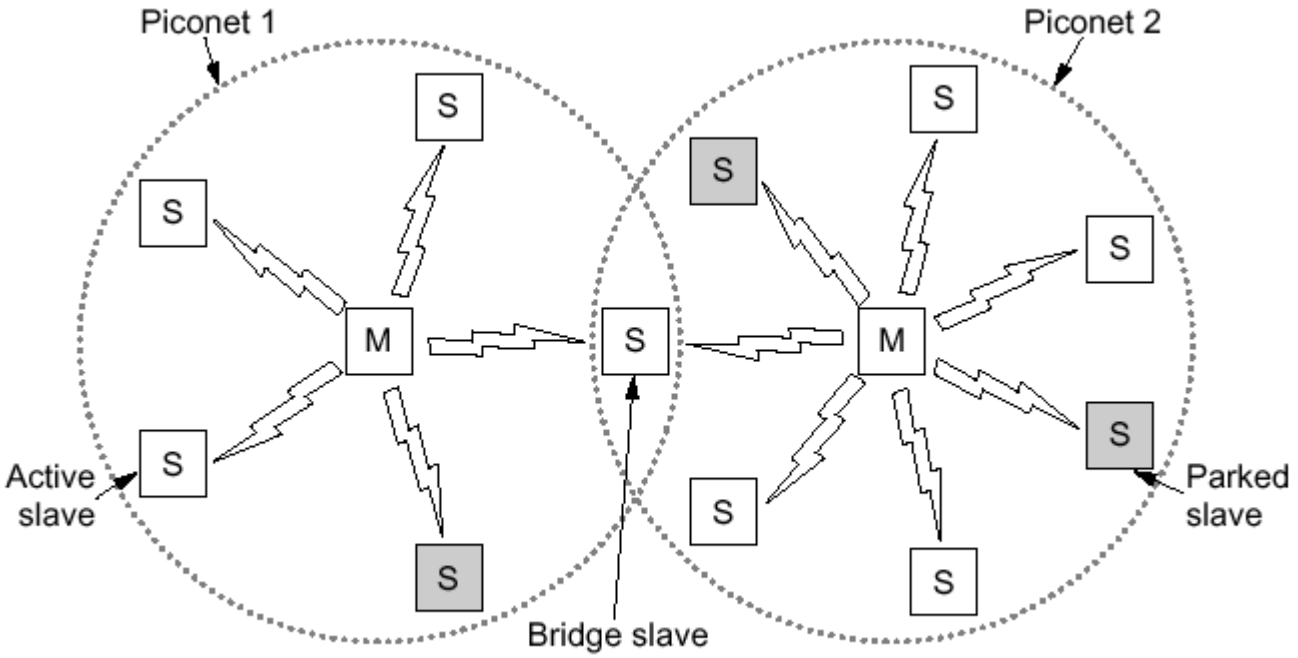
Arquitectura Bluetooth

- No hay puntos de acceso, sólo estaciones (PCs portátiles, móviles, impresoras, auriculares…)
- Se forman picoredes, con un máximo de 8 dispositivos activos
- Uno de los dispositivos de la red actúa como maestro y el resto (máximo 7) como esclavos
- El maestro fija el patrón de salto de frecuencias y da las señales de reloj para que el resto de dispositivos se sincronicen con él
- Puede haber hasta 255 dispositivos aparcados dentro de la red, que no pueden comunicarse hasta que el maestro los cambie a estado activo

Protocolo MAC en Bluetooth

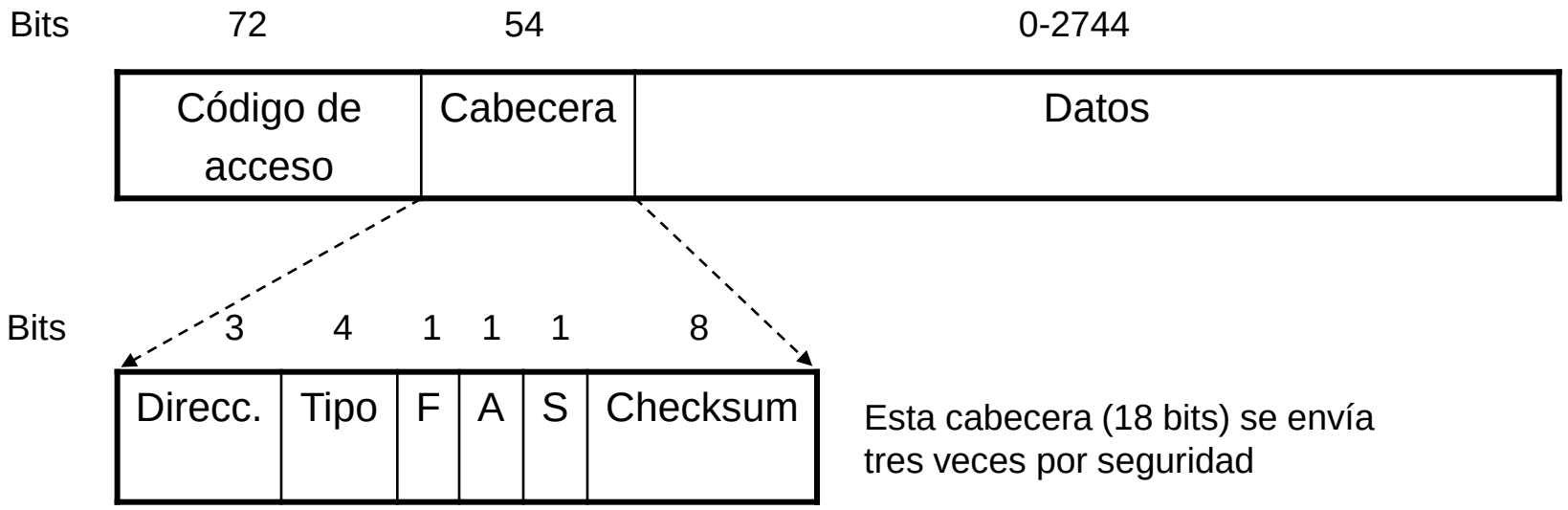
- El maestro se encarga de dar 'turno de palabra' a los esclavos
- El maestro transmite en particiones impares y un esclavo sólo puede transmitir después de que el maestro se haya comunicado con él en la partición anterior
- El esclavo se comunica únicamente con el maestro (salvo en Bluetooth mesh en versión v5)

Topología Bluetooth



Dos 'picoredes' se pueden unir para formar una 'scatternet'

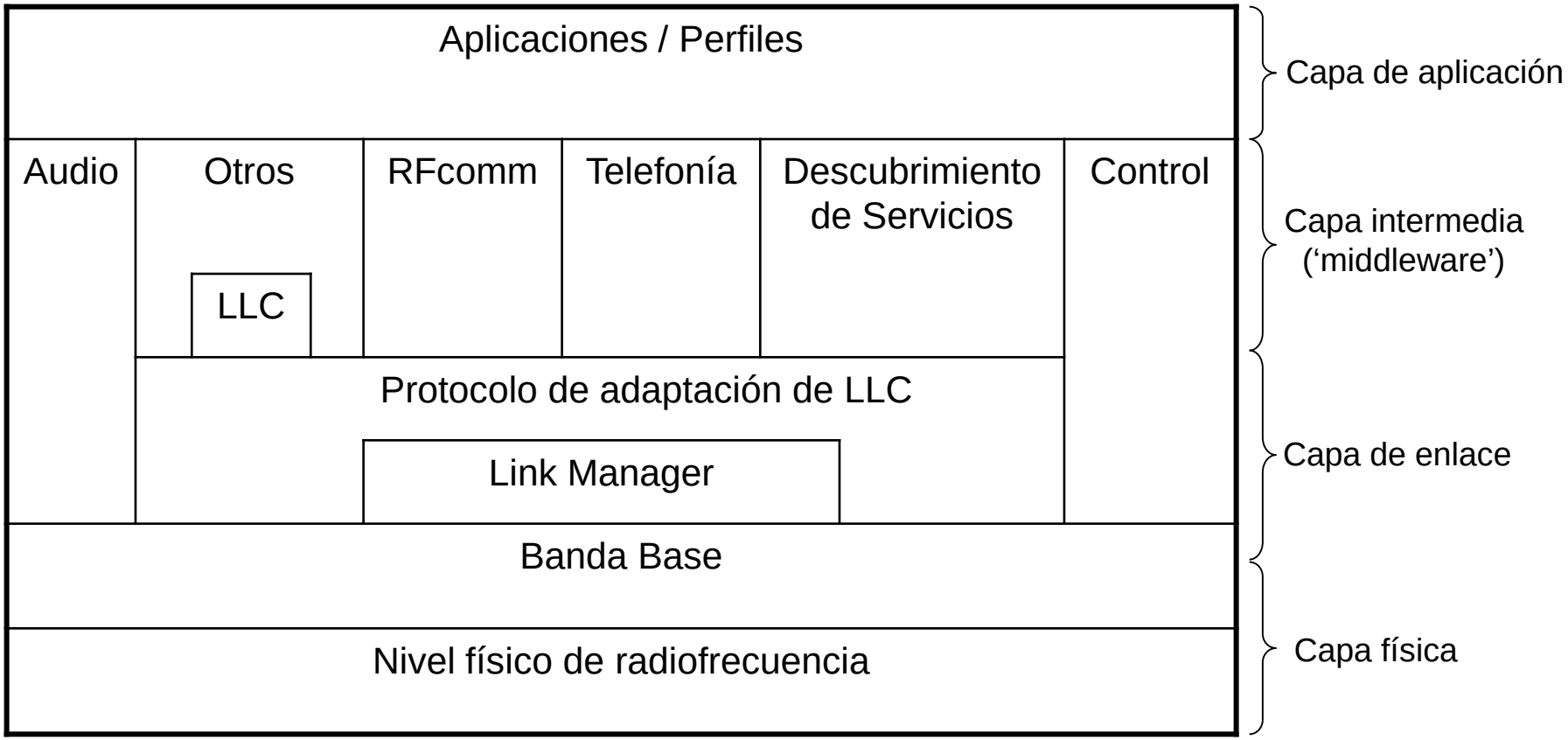
Trama Bluetooth



Access Code: identifica al maestro (puede haber más de uno accesible para el esclavo)

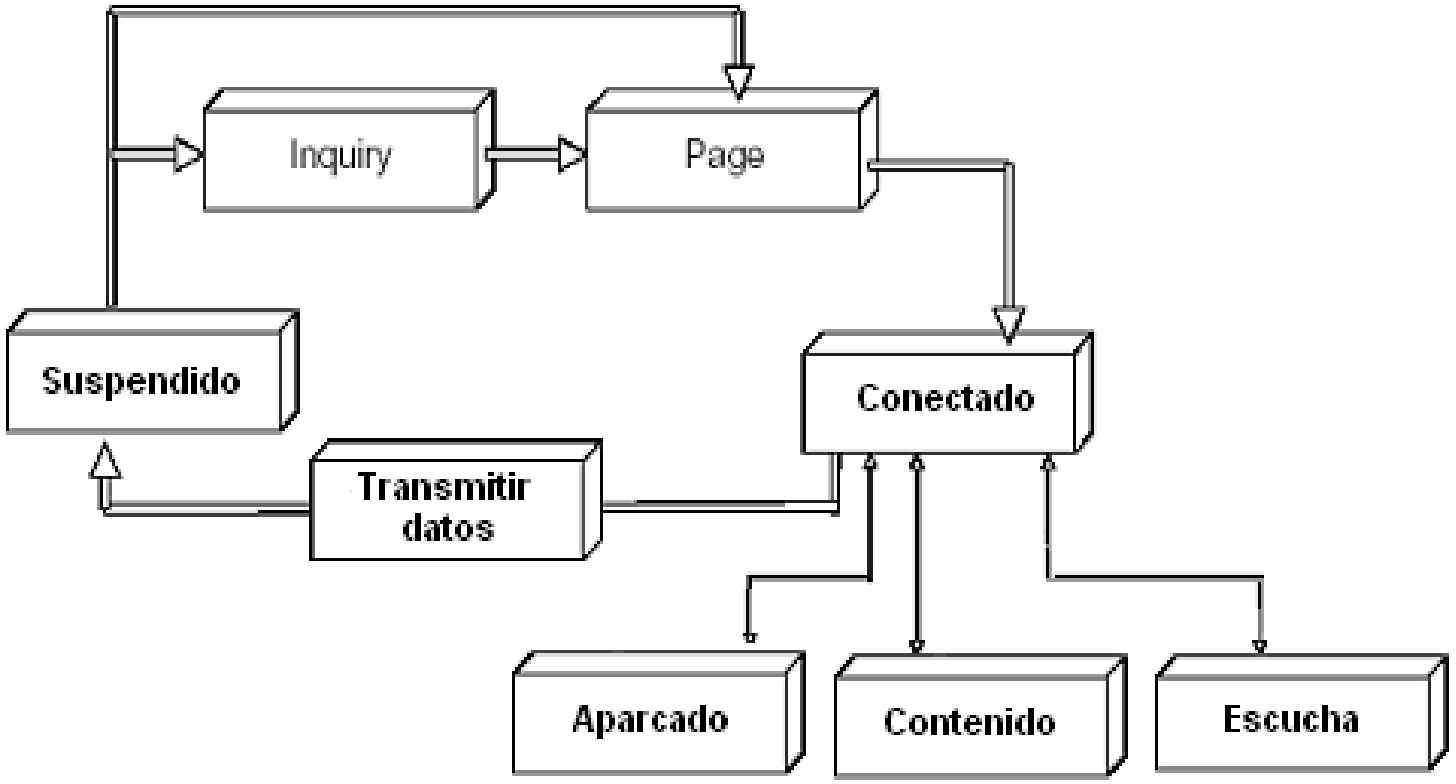
Addr: Dirección (máximo 8 estaciones)
Type: Tipo de trama, corrección de errores y longitud
F: Control de flujo
A: Acknowledgment
S: Num. Secuencia (protocolo de parada y espera)

Arquitectura Bluetooth



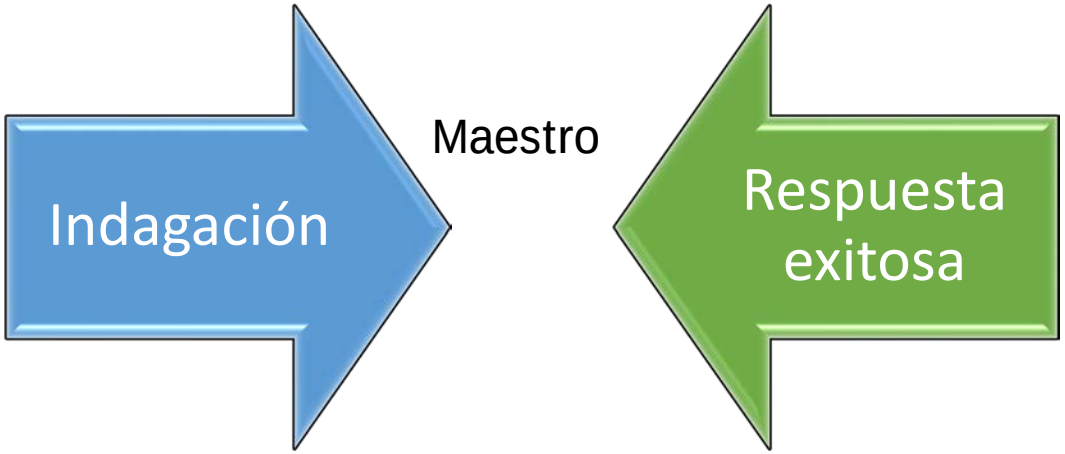
Estados dispositivos Bluetooth

- Un dispositivo bluetooth puede estar en un estado de control.



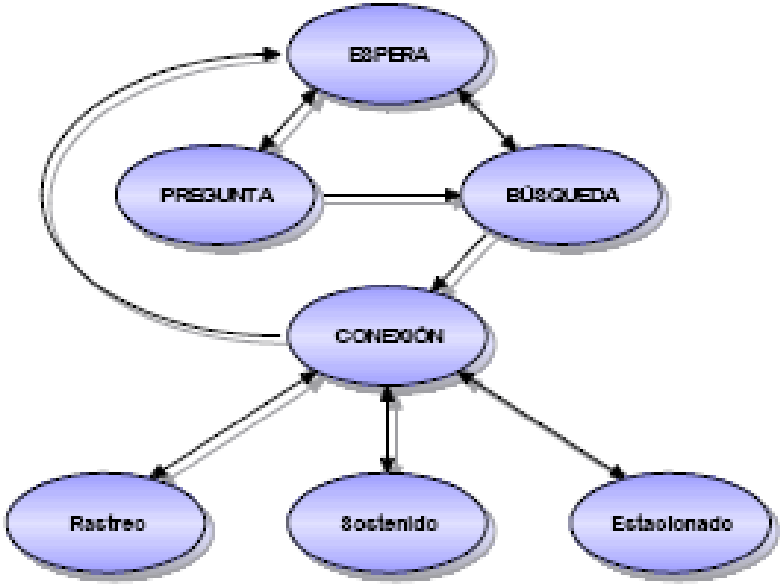
Estados (indagación)

- Se lleva a cabo entre dos dispositivos
  - Inquiry
  - Inquiry Scan
- Se utiliza cuando la dirección destino no se conoce
- Inquiry – descubrir estaciones
- Inquiry Scan – desean ser descubiertas



Procedimientos de pregunta y búsqueda

- Estos procedimientos son fundamentales para constituir una piconet, debido a que el potencial maestro necesita conocer qué dispositivos existen en la proximidad y con cuál o cuáles en particular se desea conectar.



Procedimientos de pregunta y búsqueda

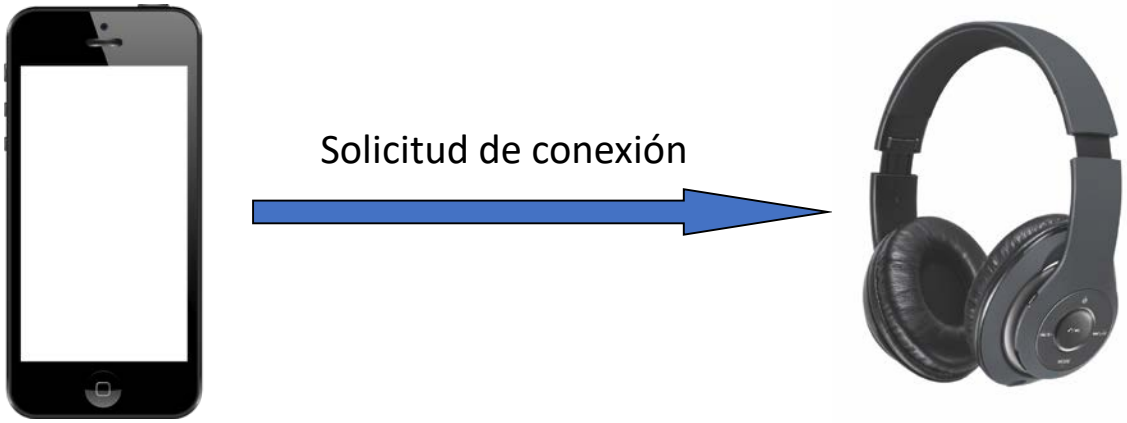
- El mecanismo de pregunta (inquiry) es utilizado cuando se requiere conocer qué dispositivos están disponibles para la conexión.

- En caso contrario, se reduce el tiempo de conexión si se conocen los dispositivos utilizando directamente el mecanismo de búsqueda para conectarse con un dispositivo en particular.

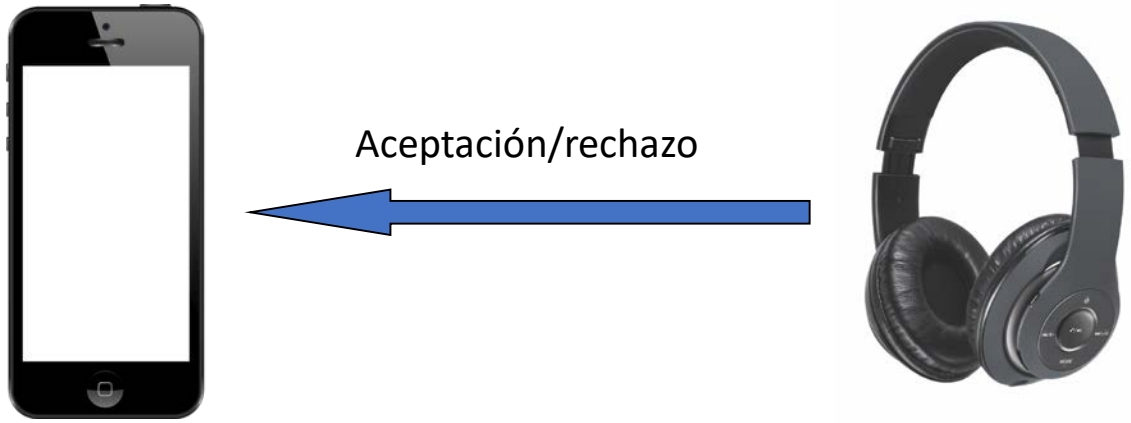
- Una vez lograda la conexión, los esclavos pueden participar activamente en la piconet o decidir entrar en alguno de los modos de ahorro de energía.

Emparejamiento de dispositivos

Tras haberse completado el procedimiento de búsqueda ya se está listo para establecer una conexión LMP. En primer lugar el dispositivo emisor envía la primitiva *LMP_host_connection_req*.

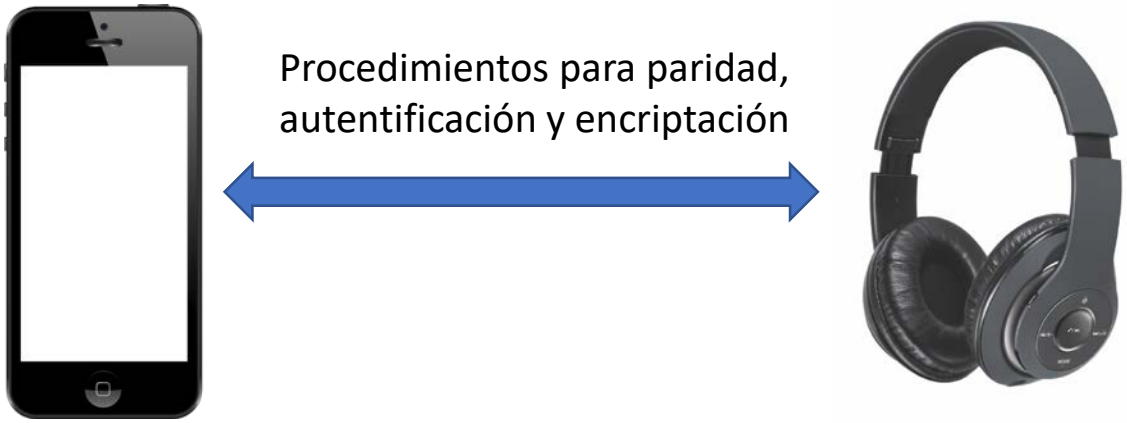


El dispositivo receptor recibe el mensaje y obtiene información sobre la conexión que se va abrir. Este dispositivo remoto puede aceptar o rechazar esa petición de conexión mediante una primitiva



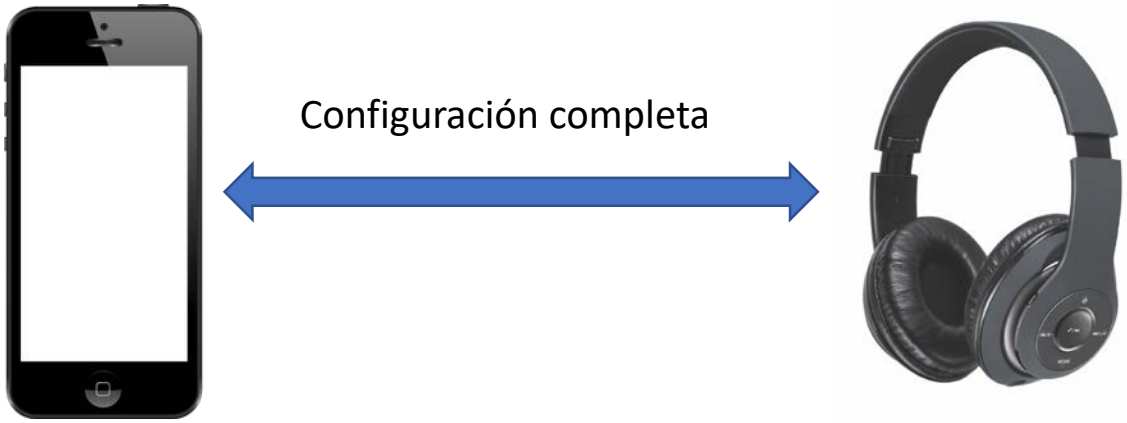
Emparejamiento de dispositivos

Ahora ambos lados de la comunicación se intercambian datos sobre paridad, autenticación y encriptación para conocerse mutuamente.



Emparejamiento de dispositivos

Una vez establecidos todas las configuraciones necesarias, los dos dispositivos se mandan *LMP_setup_complete*. Después de esto, se procederá a la transmisión de los paquetes de los diferentes canales lógicos que emplea LMP.



Emparejamiento de dispositivos

Modo pasivo

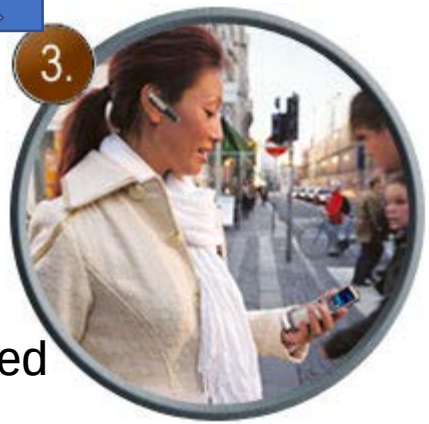
Búsqueda:

Descubrimiento del servicio del punto de acceso

Solicitud:

Emparejamiento mediante el PIN (seguridad)

Creación de un canal con el punto de acceso



Utilización de la red

Consumo de potencia

- En Bluetooth se definen cinco posibles estados, básicamente para controlar niveles de consumo de potencia
  - **Active (activo)**, activa comunicación.
  - **Hold (contención)**, conectado pero sin necesidad de transmisión.
  - **Sniff (escucha)**, el esclavo escucha sólo en algunos slots
  - **Park (aparcado)**, están registrados pero no hacen transmisión.
  - **Stand By (no conectado)**, no conectado a ninguna piconet.

Modos de ahorro de energía

- Rastreo (sniff). En este modo el esclavo conservando su dirección de miembro activo (AM_ADDR), reduce su actividad en la piconet apagando su receptor durante un tiempo prefijado (T_{sniff}), para luego encenderse una cantidad de ranuras de tiempo ($N_{sniff\_attempt}$) y esperar por paquetes del maestro.

- Sostenimiento (hold). A diferencia del modo de rastreo, el esclavo suspende su actividad normal con la piconet sólo una vez durante un tiempo predeterminado (holdTO), conservando su AM_ADDR

- Estacionado (park). En este modo el esclavo renuncia a su AM_ADDR, ya cambio, el maestro le asigna una dirección de miembro estacionado (PM_ADDR) y una dirección de solicitud de acceso (AR_ADDR).

Perfiles Bluetooth

Son un conjunto de mensajes y procedimientos de la especificación Bluetooth para una situación de uso concreta del equipo.

- Los perfiles se encuentran asociados con las aplicaciones.
- Permiten que no sea necesario implementar en un determinado dispositivo toda la pila de protocolos, sólo la parte que va a necesitar. (necesario para ratones, auriculares)
- Perfiles compartidos
- Perfil de acceso genérico mínimo.
- Perfil de acceso a descubrimiento de servicios (Service Discovery Access Profile)

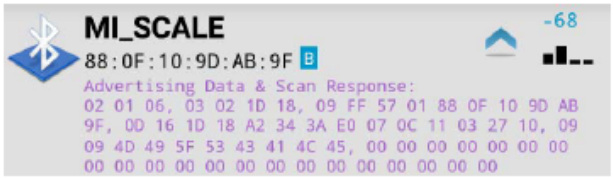
Perfiles Bluetooth

- Advanced Audio Distribution Profile (A2DP)
- Audio/Video Remote Control Profile (AVRCP)
- Basic Imaging Profile (BIP)
- Basic Printing Profile (BPP)
- Common ISDN Access Profile (CIP)
- Cordless Telephony Profile (CTP)
- Device ID Profile (DID)
- Dial-up Networking Profile (DUN)
- Fax Profile (FAX)
- File Transfer Profile (FTP)
- General Audio/Video Distribution Profile (GAVDP)
- Generic Access Profile (GAP)
- Generic Object Exchange Profile (GOEP)
- Hard Copy Cable Replacement Profile (HCRP)
- Hands-Free Profile (HFP)
- Human Interface Device Profile (HID)
- Headset Profile (HSP)
- Intercom Profile (ICP)
- Object Push Profile (OPP)
- Personal Area Networking Profile (PAN)
- Phone Book Access Profile (PBAP)
- Serial Port Profile (SPP)
- Service Discovery Profile (SDAP)
- SIM Access Profile (SAP, SIM)
- Synchronisation Profile (SYNCH)
- Video Distribution Profile (VDP)
- Wireless Application Protocol Bearer (WAPB)

Ejemplo Bluetooth Low Energy (BLE)

P.nbr.	Time (us)	Channel	Access Address	Adv PDU Type	Adv PDU Header				AdvA	AdvData	CRC	RSSI (dBm)	FCS
					Type	TxAdd	RxAdd	PDU-Length					
9	+1031101 -1031101	0x25	0x8E89BED6	ADV_IND	0	0	0	37	0x880F109DAB9F	02 01 06 03 02 1D 18 09 FF 57 01 88 0F 10 9D AB 9F 0D 16 1D 18 A2 34 3A E0 07 0C 11 03 27 10	0xC0391F	-54	OK

AD structure	Type	Content
02 01 06	01: FLAG	0x06: 00000110: Support only LE connection
03 02 1D 18	02: Service UID	0x181D: Weight Scale
09 FF 57 01 88 0F 10 9D AB 9F	FF: Vendor Spec.	0x0157: Huami co., Ltd. 880F109DAB9F: Device Address
0D 16 1D 18 A2 34 3A E0 07 0C 11 03 27 10	16: Service Data	0x181D: Weight Scale Service 0xA2: 10100010 SI units, Time stamp present, no user ID, no BMI 0x3A34: 14900 (x 0.005kg = 74.5kg) 0xE0070C11010203: 2016-12-17 03:39:16
09 09 4D 49 5F 53 43 41 4C 45	09: Local Name (short)	0x4D 49 5F 53 43 41 4C 45: 'MI_SCALE'

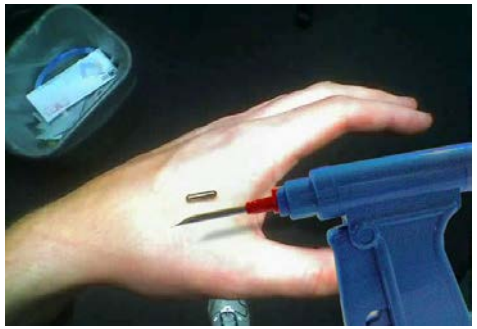


Zigbee (IEEE 802.15.4)

- Redes personales con menor consumo de potencia, menor velocidad de bit y menor ciclo de trabajo que Bluetooth
- Muy empleada en IoT: sensores de luz, temperatura, interruptores, dispositivos de seguridad…
- Bajo coste
- Velocidades de canal de 20, 40, 100 y 250 kbps
- Dos tipos de nodos: maestro (dispositivo de función completa) y esclavo (de función reducida)
- Redes en estrella, malla… con múltiples posibles protocolos MAC

Radio Frequency IDentification (RFID)

- Sistema de almacenamiento y recuperación de datos remoto que usa etiquetas o tags RFID para transmitir la identidad de un objeto (similar a un número de serie único) mediante ondas de radio.
- Un dispositivo lector o reader se comunica a través de una antena con la etiqueta, que también tiene una antena.
- Las tags RFID pueden ser activos, semipasivos (también conocidos como semiactivos o asistidos por batería) o pasivos.



Near Field Communication (NFC)

- Comunicación entre 2 dispositivos a distancia muy cercana (<4cm)
- Uso para identificación, llaves, pago contactless…
- Típicamente, como RFID, usa la frecuencia 13.56 MHz, con velocidades de 106-424 kbps
- También como RFID, dentro de los estándares ISO18000