REDES INALÁMBRICAS

Redes de Datos I

Facultad de Ingeniería
Universidad Nacional de La Plata

REDES INALÁMBRICAS

- Introducción
- Nivel físico
- Topología
- Nivel MAC
- Conectividad en redes 802,11

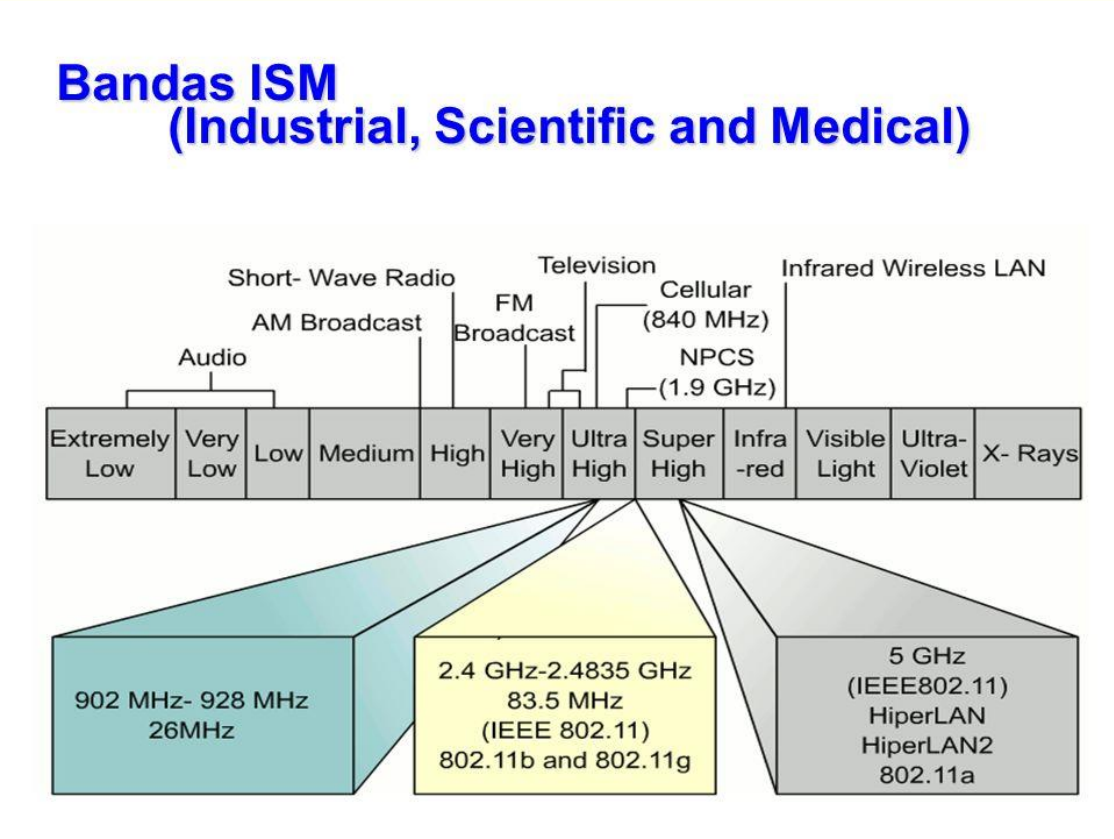
Redes inalámbricas

- Wi-Fi (Wireless Fidelity): conjunto de tecnologías WLAN (Wireless Local Area Network)
- WiFi Alliance (Apple, Cisco, Broadcom, Intel, Qualcomm, Nokia, Alibaba, ASUSteK etc).
- Estándares IEEE 802.11

REDES INALÁMBRICAS

- Introducción
- **Nivel físico**
- Topología
- Nivel MAC
- Conectividad en redes 802,11

Redes inalámbricas



ITU-R regula el uso del espacio radioeléctrico

- Región 1: EMEA (Europa, Medio Oriente, África)
- Región 2: América
- Región 3: Asia y Oceanía

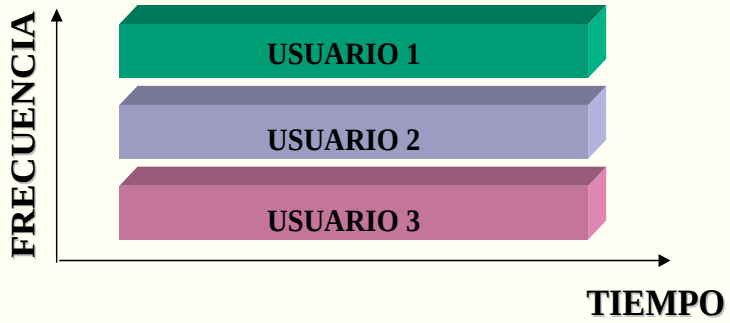
Bandas ISM

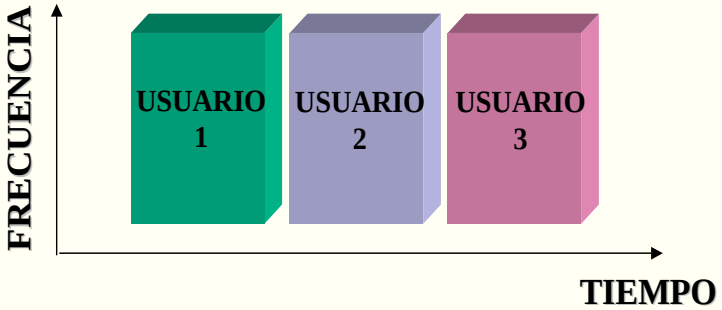
Banda	Ancho de banda	¿Se utiliza para Wi-Fi?
13.553-13.567 MHz	14 KHz	No
26.957-27.283 MHz	326 KHz	No
40.66 – 40.7 MHz	40 KHz	No
902 – 928 MHz	26 MHz	ZigBee/802.15.4 802.11ah
2.4 – 2.5 GHz	100 MHz	802.11, 802.11b. 802.11g, 802.11n, Bluetooth, ZigBee
5.725 – 5.875 GHz	150 MHz	802.11a, 802.11n, 802.11ac
24 – 24.25 GHz	250 MHz	No
61-61.5 GHz	500MHz	802.11ad

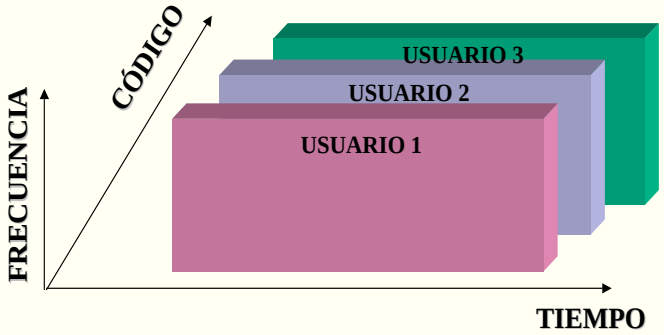
Redes inalámbricas

Técnicas de acceso múltiple: permitir a varios usuarios compartir el medio físico de transmisión

Multiplexación
- Frecuencia (FDMA)
- Tiempo (TDMA)
- Código (CDMA)







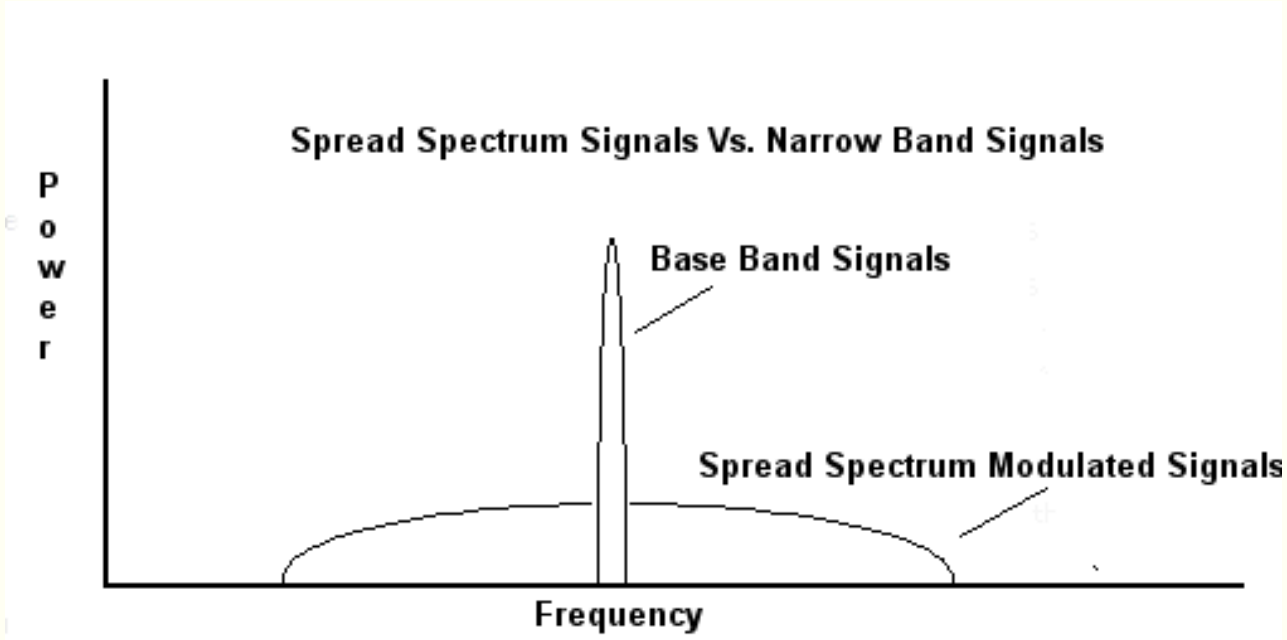
Redes inalámbricas – Spread Spectrum

Spread Spectrum (espectro expandido)

- Inmunidad frente al ruido y distorsión multitrayectoria
- Esparcir los datos sobre un gran ancho de banda
- Puede ocultar / encriptar señales
- Los usuarios pueden compartir ancho de banda con muy poca interferencia
- Tres implementaciones:
  - Salto de frecuencia (FHSS)
  - Secuencia directa (DSSS)
  - Multiplexación por división en frecuencia ortogonal (OFDM)

Redes inalámbricas – Spread Spectrum

Spread Spectrum: la señal se expande (su espectro) a través de un ancho de banda mayor que el mínimo requerido para transmitir con éxito.



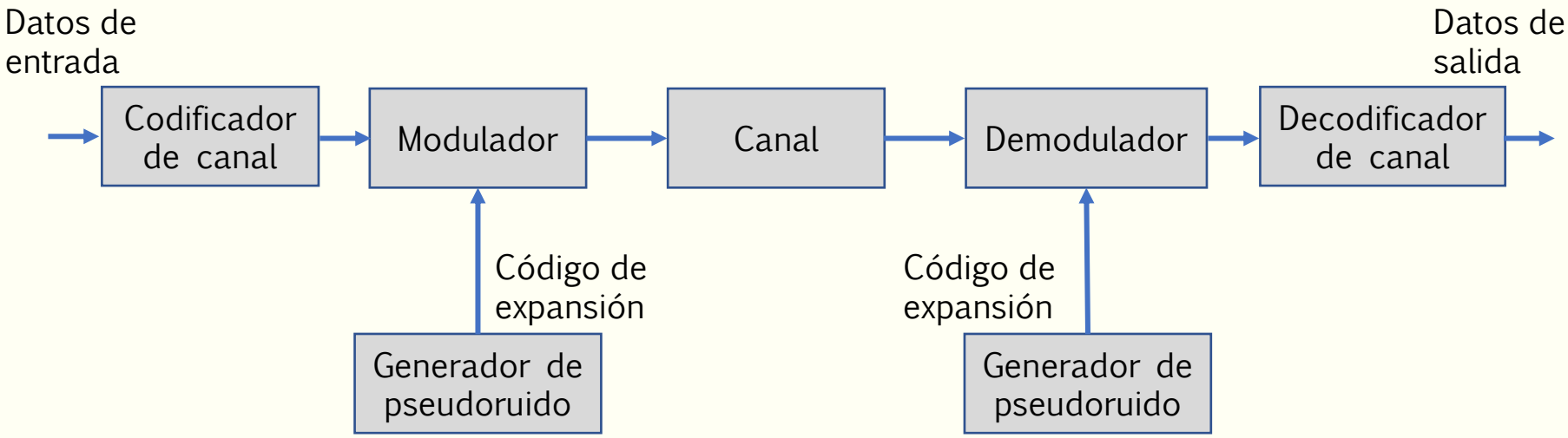
Redes inalámbricas – Spread Spectrum

Números pseudo aleatorios

- Generados por un algoritmo determinístico
  - No son exactamente aleatorios
  - Pero si el algoritmo es bueno, las secuencias pueden verse como aleatorios y pueden ser periódicas
- Comienzan a partir de una “semilla” (valor) inicial
- Debo conocer el algoritmo y la “semilla” para decodificar las secuencias

Redes inalámbricas – Spread Spectrum

Modelo general de Spread Spectrum



Redes inalámbricas – Spread Spectrum

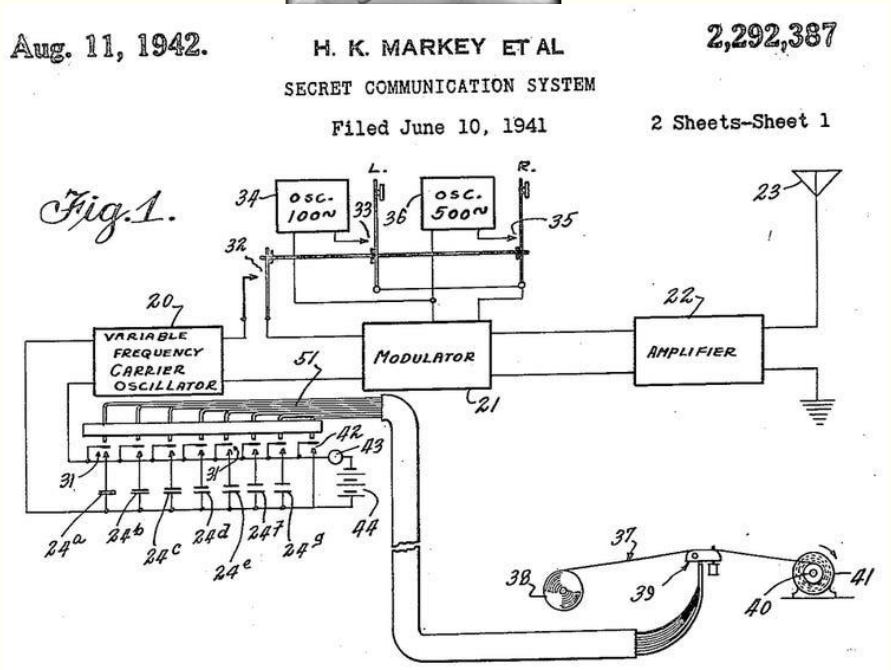
HEDY LAMARR INVENTOR

Actress Devises 'Red-Hot' Apparatus for Use in Defense

Special to THE NEW YORK TIMES.

HOLLYWOOD, Calif., Sept. 30—Hedy Lamarr, screen actress, was revealed today in a new role, that of an inventor. So vital is her discovery to national defense that government officials will not allow publication of its details.

Colonel L. B. Lent, chief engineer of the National Inventors Council, classed Miss Lamarr's invention as in the "red hot" category. The only inkling of what it might be was the announcement that it was related to remote control of apparatus employed in warfare.



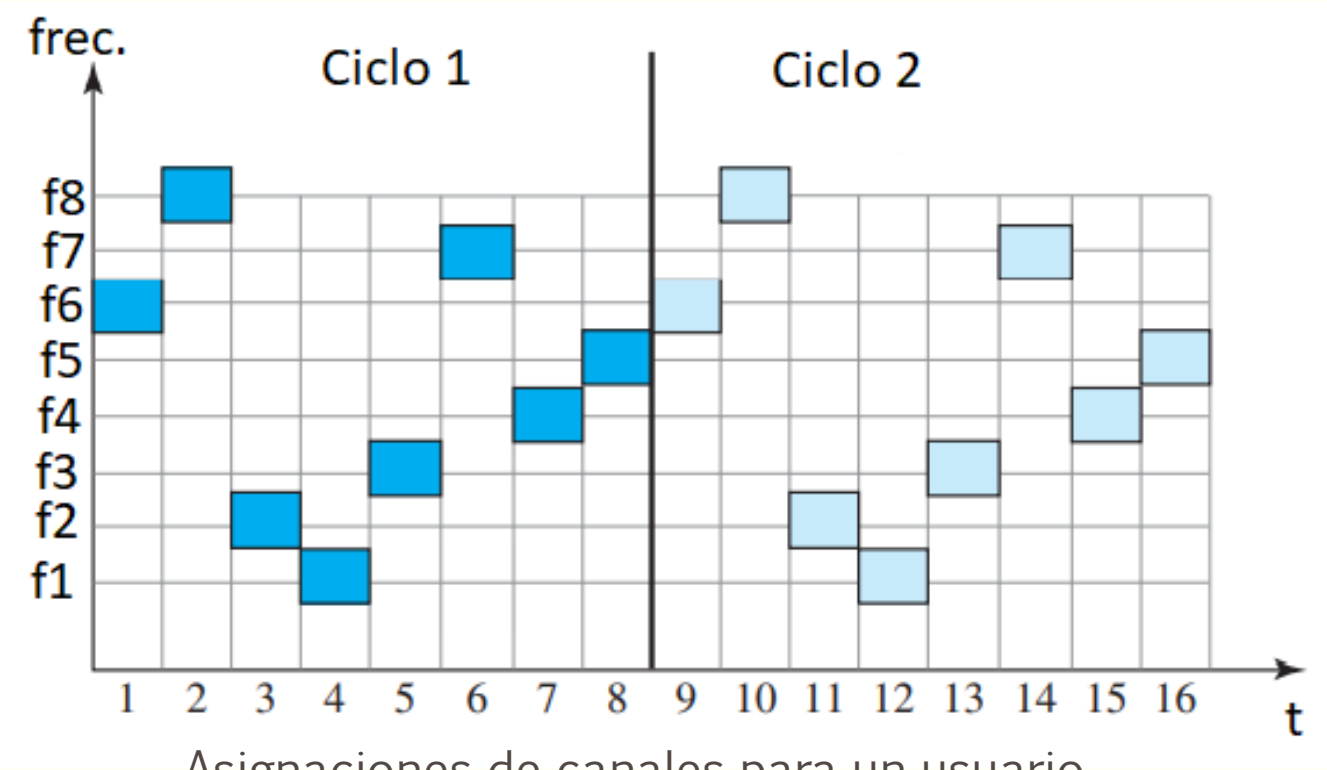
Redes inalámbricas – Spread Spectrum - FHSS

Frecuency Hoping Spread Spectrum (FHSS)

- La señal se transmite a través de una serie aparentemente aleatoria de frecuencias de radio
- El receptor salta entre las frecuencias sincronizado con el transmisor
- Interferencia en una frecuencia afecta solo unos pocos bits

Redes inalámbricas – Spread Spectrum - FHSS

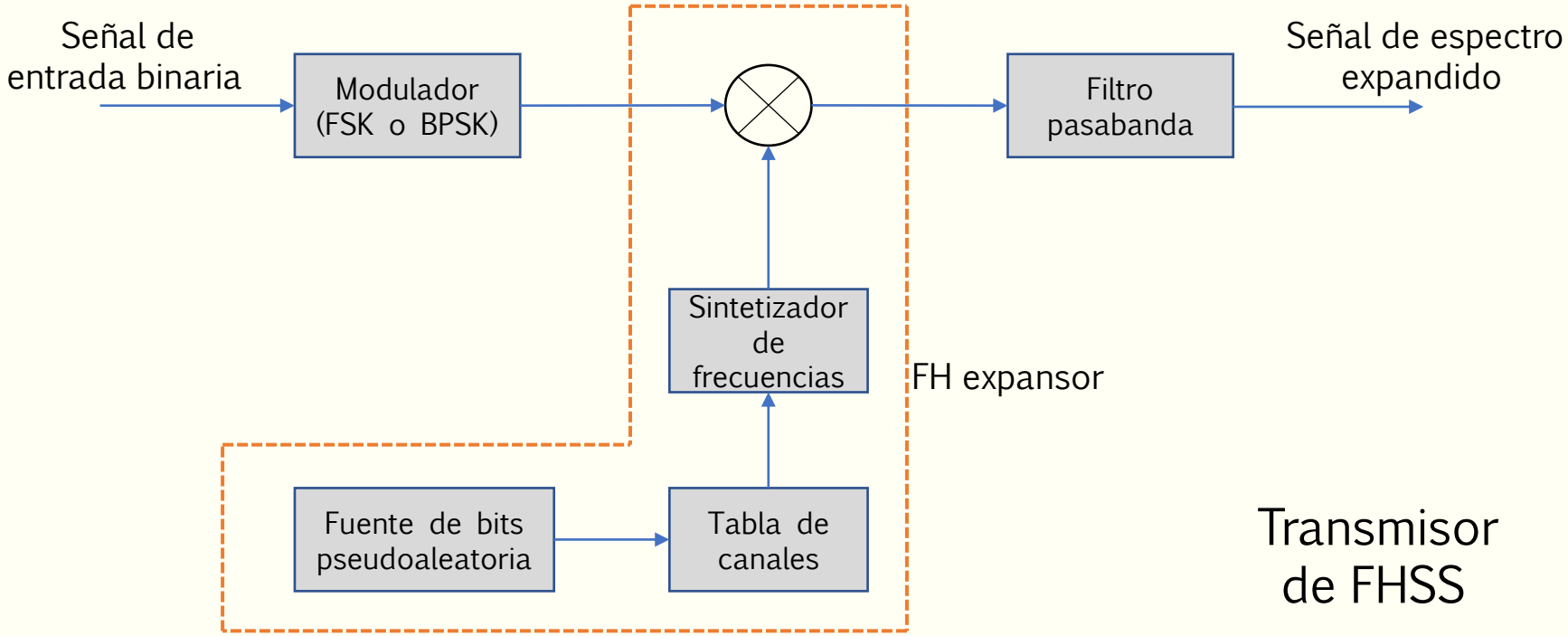
Frecuency Hoping Spread Spectrum (FHSS)



Asignaciones de canales para un usuario

Redes inalámbricas – Spread Spectrum - FHSS

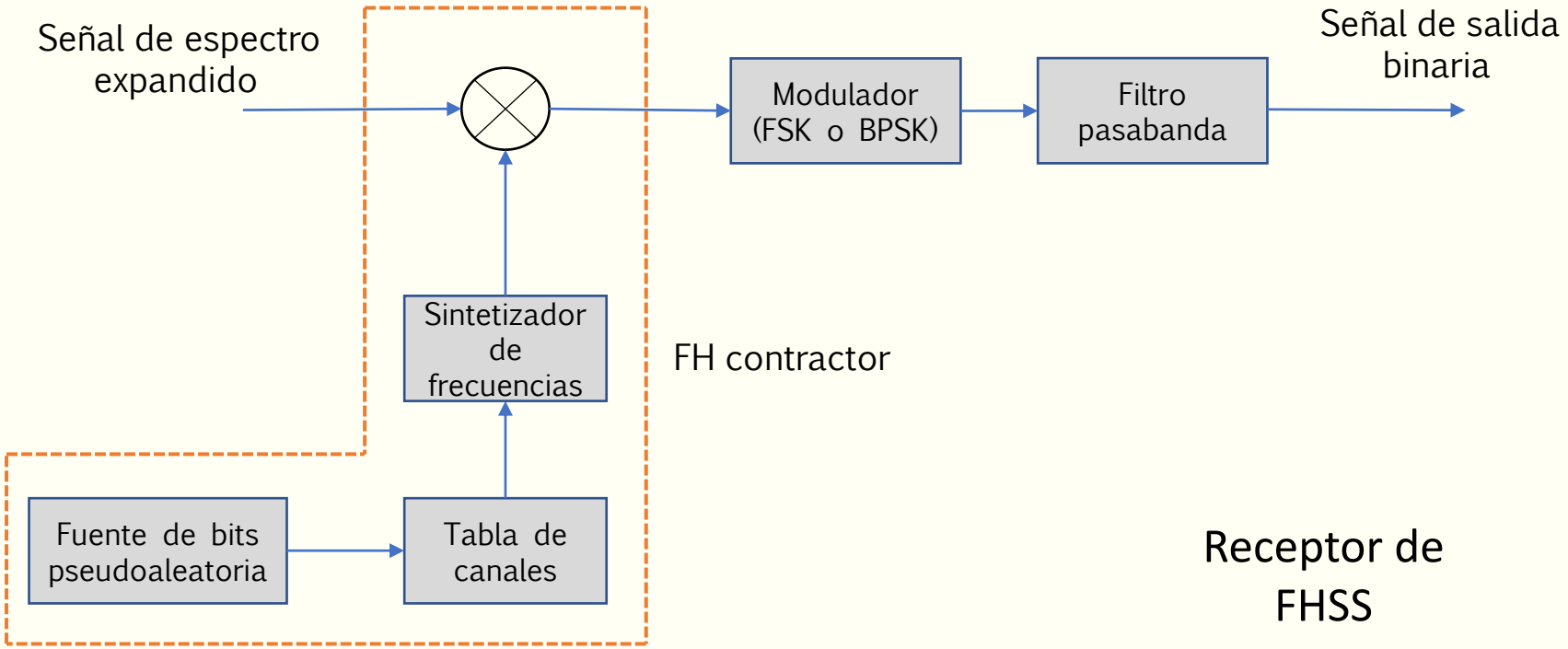
Frecuency Hoping Spread Spectrum (FHSS)



Transmisor de FHSS

Redes inalámbricas – Spread Spectrum - FHSS

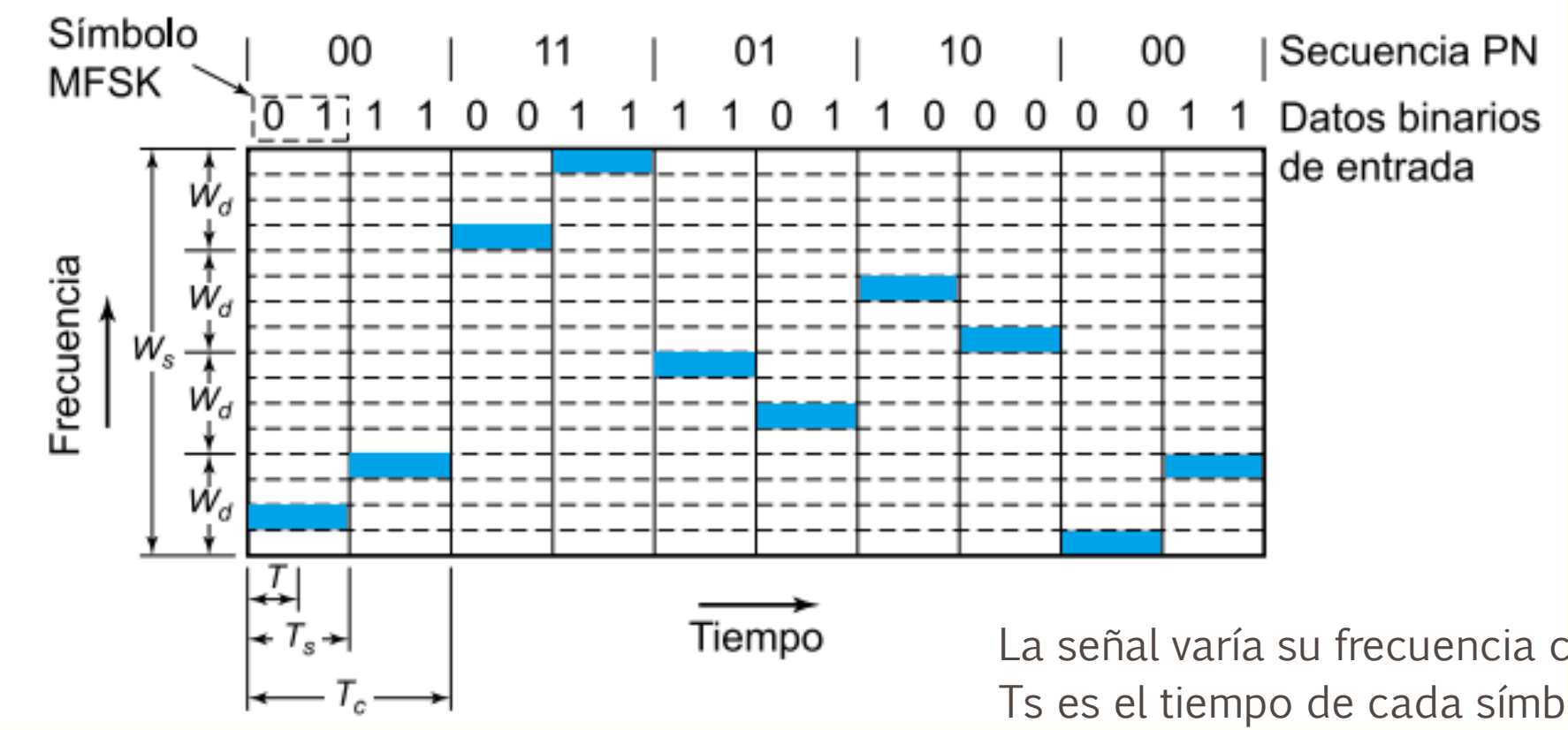
Frecuency Hoping Spread Spectrum (FHSS)



Receptor de FHSS

Redes inalámbricas – Spread Spectrum - FHSS

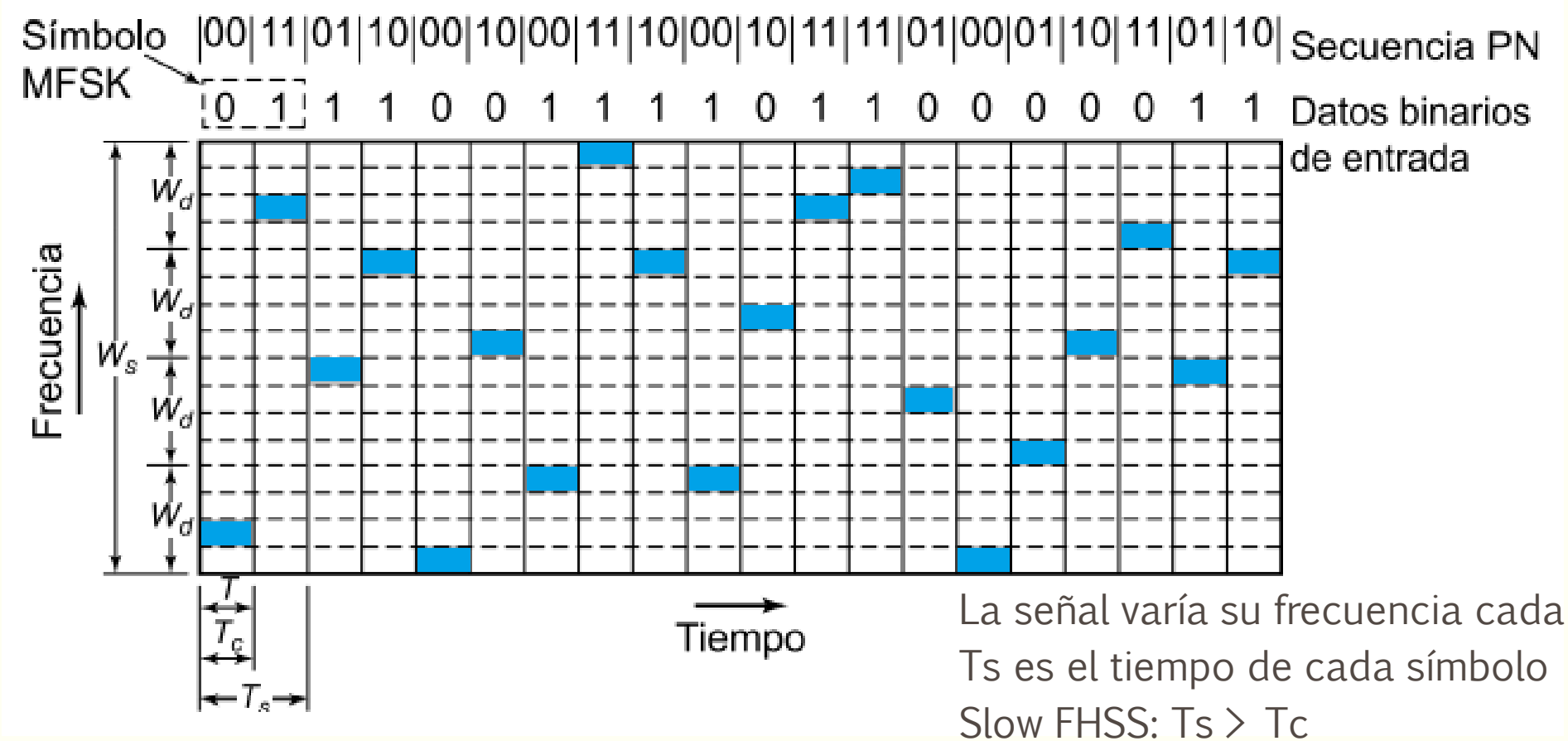
Slow FHSS



La señal varía su frecuencia cada Tc
Ts es el tiempo de cada símbolo
Slow FHSS: Ts < Tc

Redes inalámbricas – Spread Spectrum - FHSS

Fast FHSS



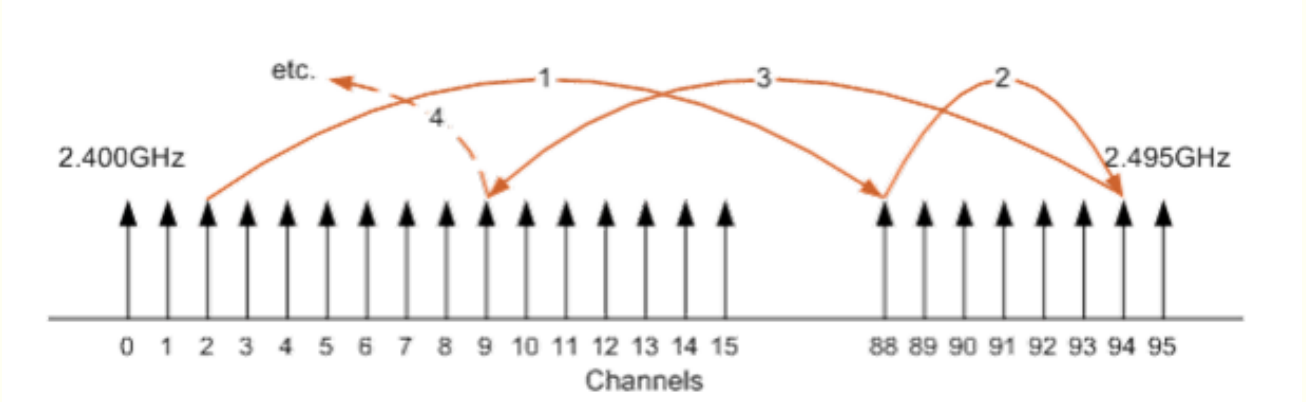
La señal varía su frecuencia cada Tc

Ts es el tiempo de cada símbolo

Slow FHSS: Ts > Tc

Redes inalámbricas – Spread Spectrum - FHSS

Frecuency Hoping Spread Spectrum (FHSS)



Región	Canales
US & Canada	2 – 79 (2.402 – 2.479 GHz)
Europa (ETSI)	2 – 79 (2.402 – 2.479 GHz)
Francia	48 – 82 (2.448 – 2.482 GHz)
España	47 – 73 (2.447 – 2.473 GHz)
Japón	73 – 95 (2.473 – 2.495 GHz)

Dwell time: tiempo en que transmite en una frecuencia específica

Hop time: tiempo para reajustar los circuitos a una nueva frecuencia

Redes inalámbricas – Spread Spectrum - FHSS

Frecuency Hoping Spread Spectrum (FHSS)

IEEE 802.11 define:

- 1 MHz de ancho de banda para la señal a transmitir
- Modulación GFSK o 4GFSK
- Dwell time = 400 ms
- Salto mínimo de frecuencia igual a 6 MHz
- Ejemplo de secuencia de saltos :3, 26, 65, 11, 46, 19, 74, 50, 22 ...
- El número máximo de saltos de cada secuencia está definido por las autoridades regulatorias. Por ej.: EE.UU y Europa 26, Japón 23.
- Dos velocidades soportadas: 1Mbps y 2Mbps

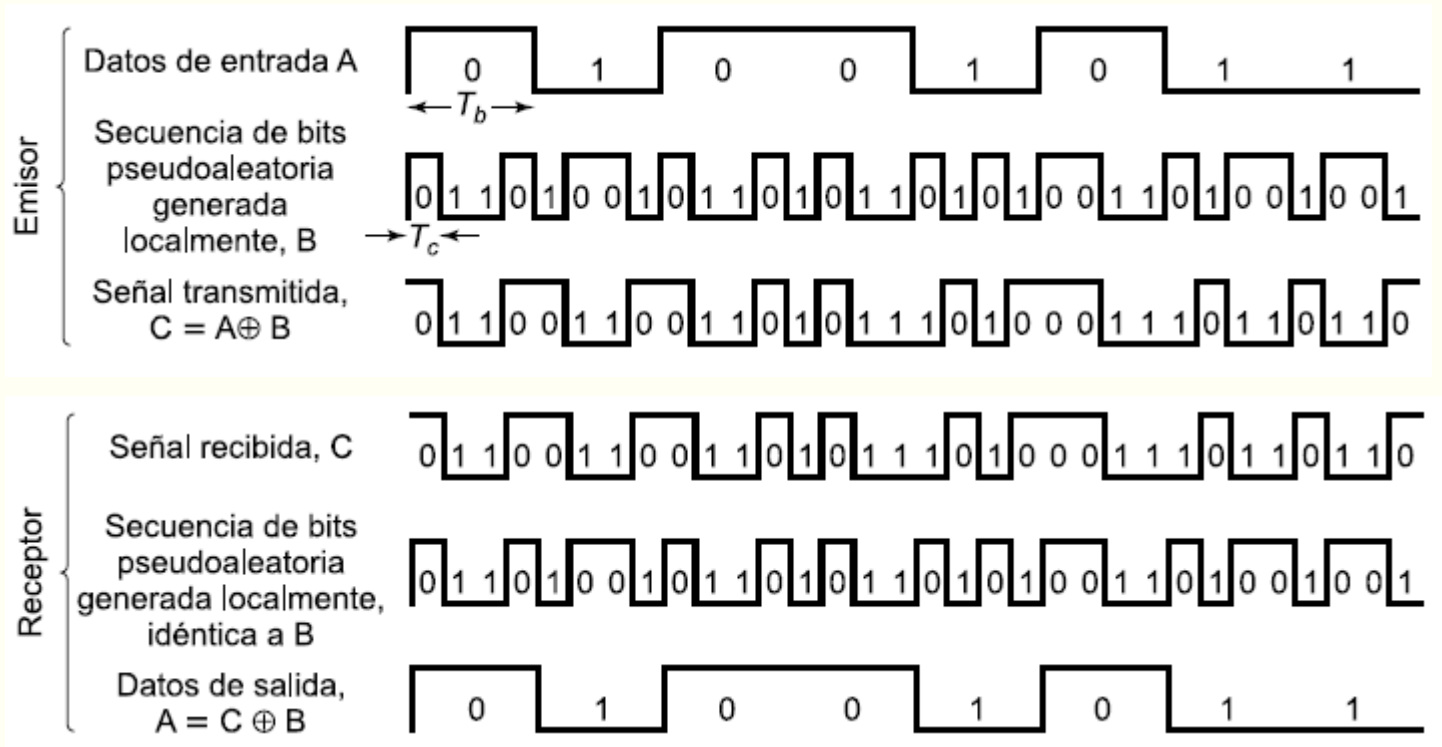
IEEE 802.11

Redes inalámbricas – Spread Spectrum - DSSS

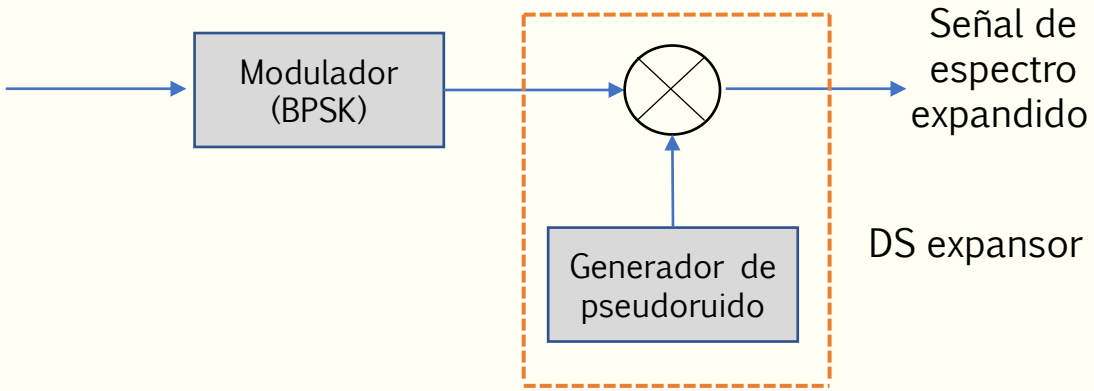
Direct Secuence Spread Spectrum (DDSS)

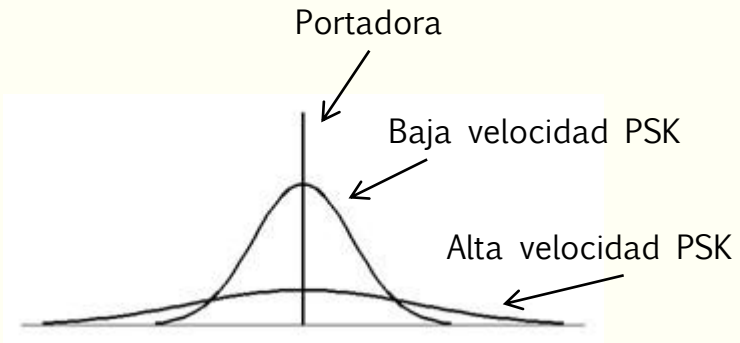
- Cada bit se representa como múltiples bits (llamados chips), utilizando un código de expansión
- Combina la secuencia de entrada con el código expansor, mediante un X-OR
- Performance similar a FHSS

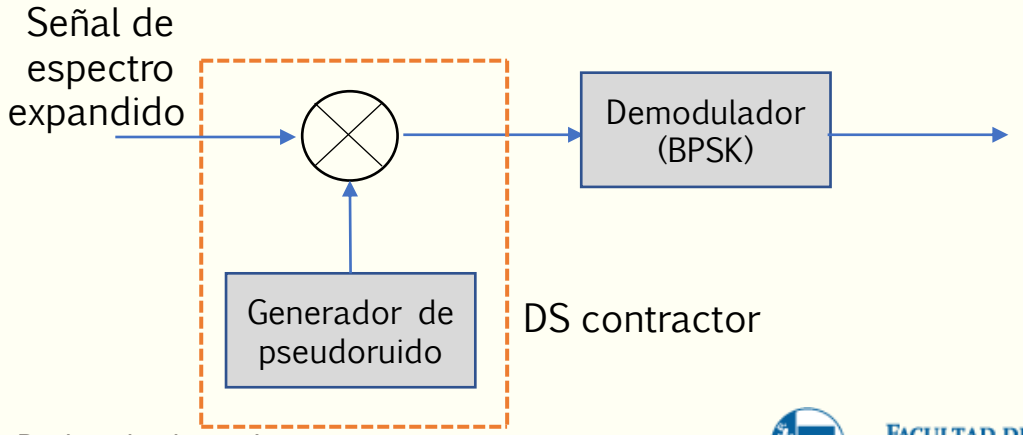
Direct Secuence Spread Spectrum (DDSS)



Direct Secuence Spread Spectrum (DDSS)





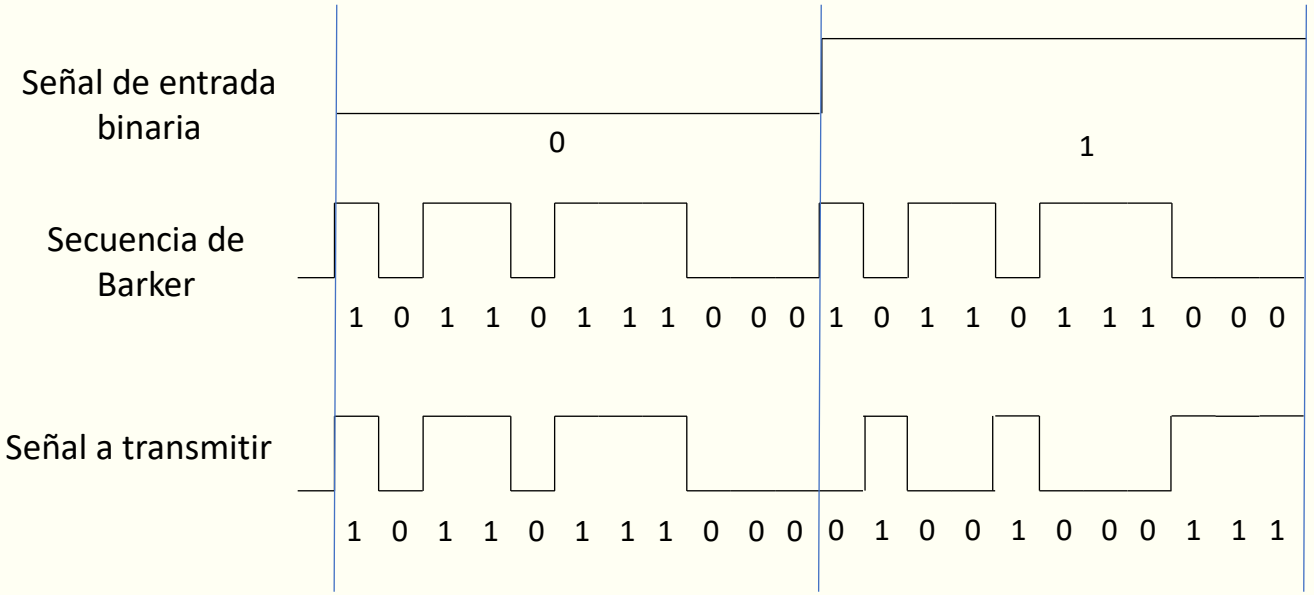


Direct Secuence Spread Spectrum (DDSS)

Secuencia de Barker de chips (ruido pseudo aleatorio)

1 bit ---> secuencia de 11 chips

1 Mbps ---> 11 Megachip/s ---> 22 MHz de BW



IEEE 802.11

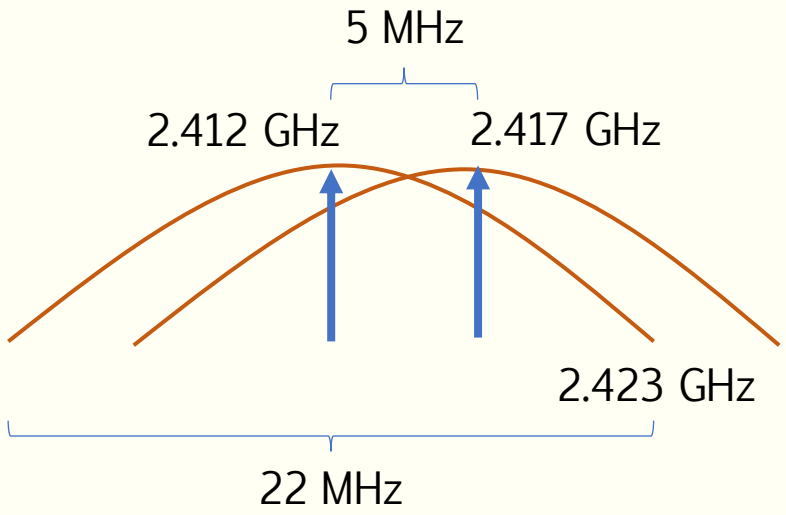
1 Mbps (DBPSK)
2 Mbps (DQPSK)

Direct Secuence Spread Spectrum (DDSS)

El espectro de la banda de 2.4 GHz se divide en 14 canales

Cada canal utiliza 22 MHz

La separación entre canales es de 5 MHz



Direct Secuence Spread Spectrum (DDSS)

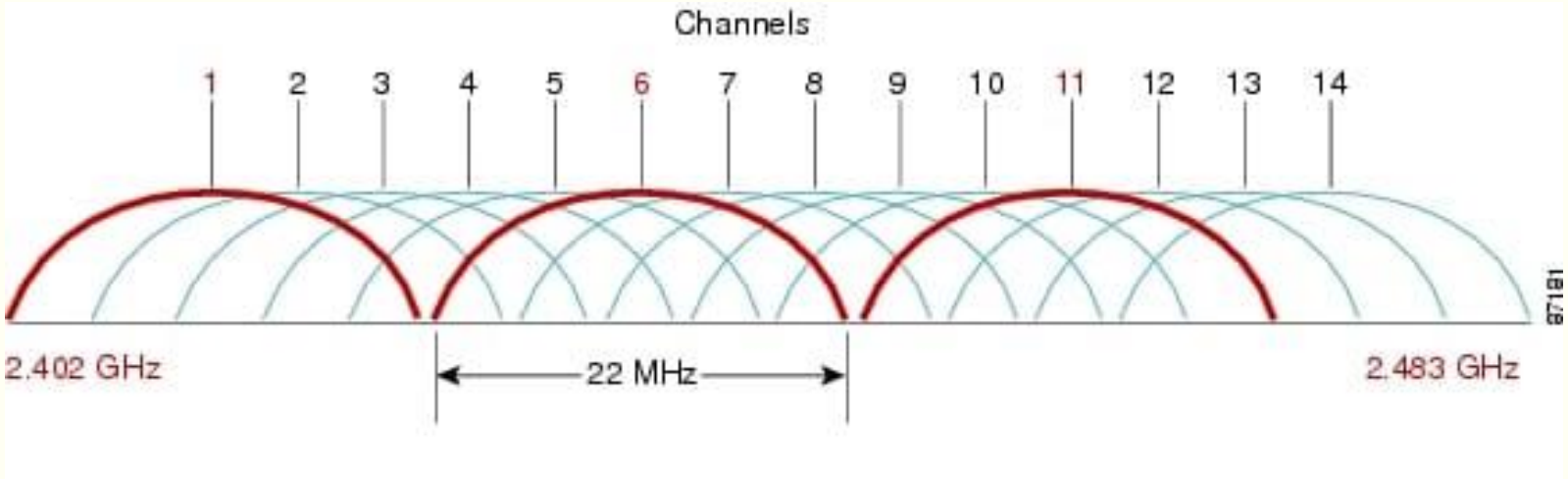
Canal	Frecuencia central (MHz)	Región ITU-R o país				
		América	EMEA	Japón	Israel	China
1	2412	✓	✓	✓	X	✓
2	2417	✓	✓	✓	X	✓
3	2422	✓	✓	✓	✓	✓
4	2427	✓	✓	✓	✓	✓
5	2432	✓	✓	✓	✓	✓
6	2437	✓	✓	✓	✓	✓
7	2442	✓	✓	✓	✓	✓
8	2447	✓	✓	✓	✓	✓
9	2452	✓	✓	✓	✓	✓
10	2457	✓	✓	✓	X	✓
11	2462	✓	✓	✓	X	✓
12	2467	X	✓	✓	X	X
13	2472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

Anchura de canal: 22 MHz

EMEA: Europa, Medio Oriente y África

Redes inalámbricas

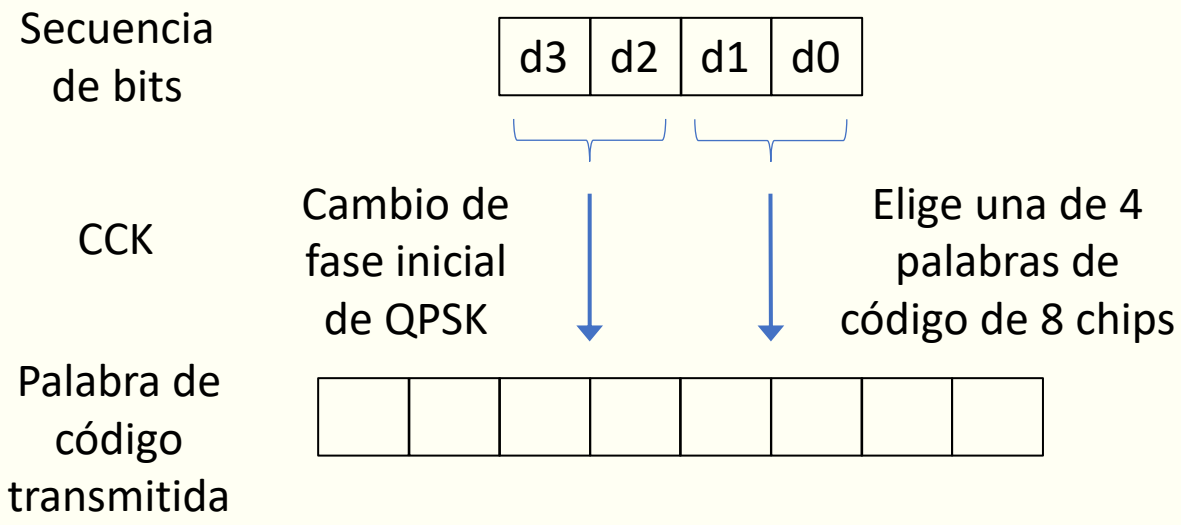
Direct Secuence Spread Spectrum (DDSS)



La separación entre canales implica que en un área donde se utilizan redes inalámbricas adyacentes existen 3 canales que no se superponen.

Direct Secuence Spread Spectrum (DDSS)

Para aumentar la velocidad se utiliza la técnica de CCK (Complementary Code Keying)
4 (u 8) bits se codifican en secuencias de 8 chips.

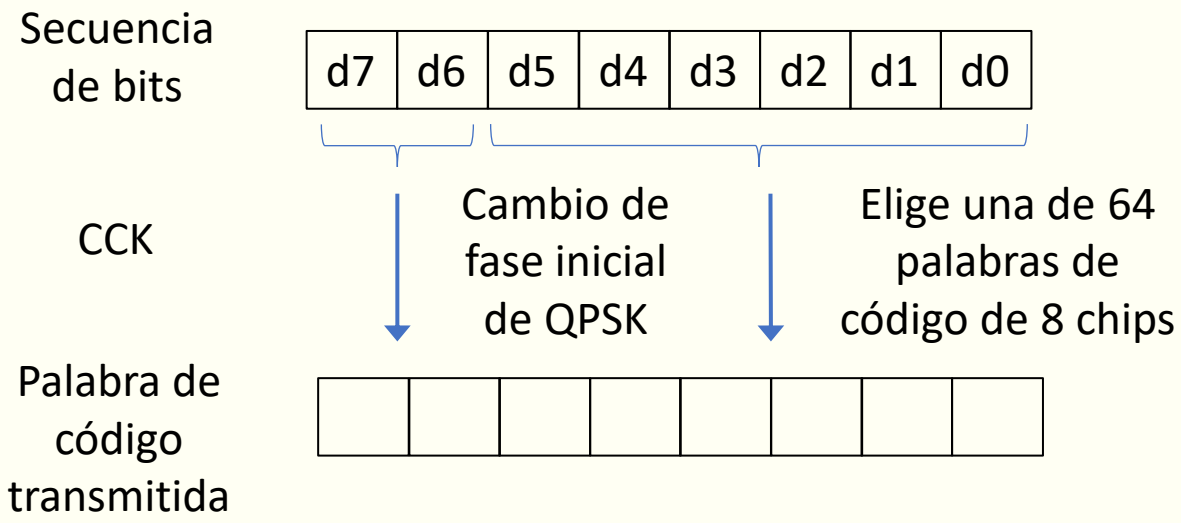


Se transmite a 11 Mchip/s
4 bits = 8 chips
Velocidad = 5,5 Mbps

IEEE 802.11b

Direct Secuence Spread Spectrum (DDSS)

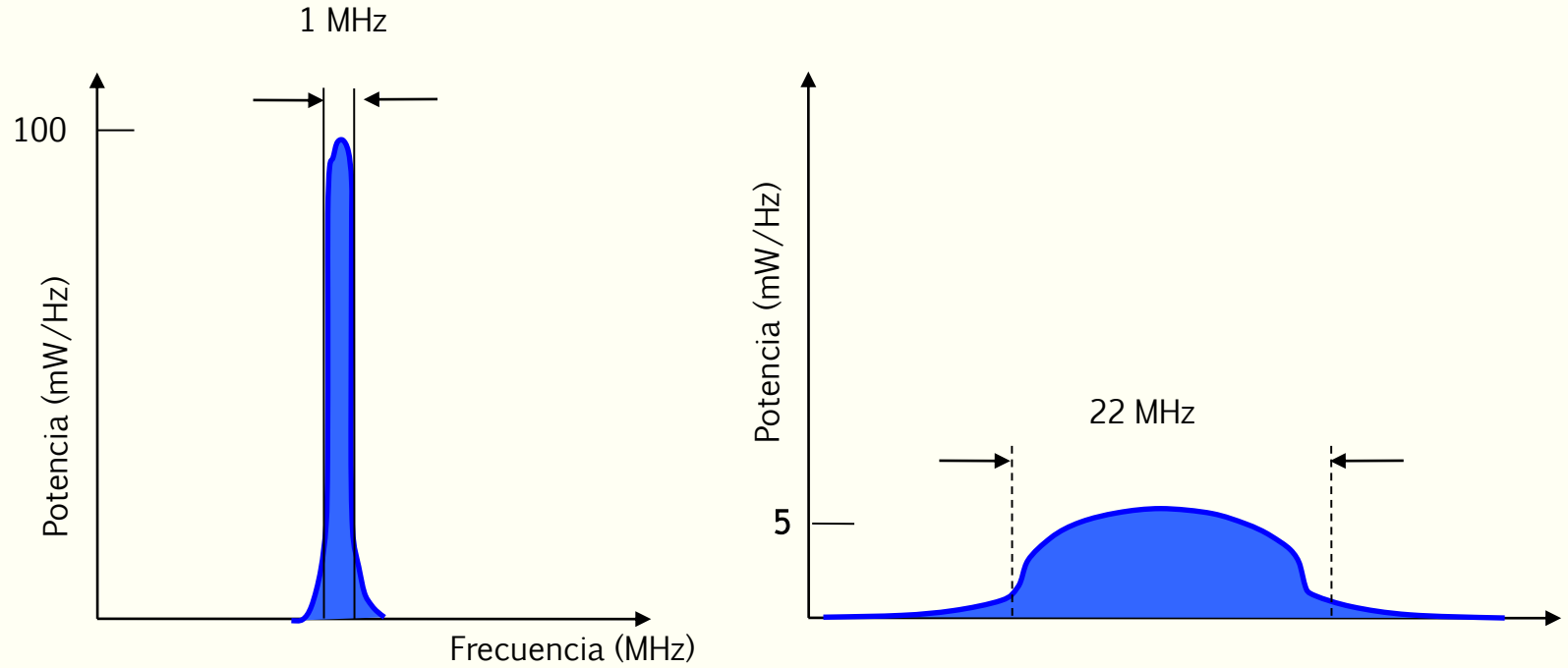
Para aumentar la velocidad se utiliza la técnica de CCK (Complementary Code Keying) 4 (u 8) bits se codifican en secuencias de 8 chips.



Se transmite a 11 Mchip/s
8 bits = 8 chips
Velocidad = 11 Mbps

IEEE 802.11b

Comparación de canales de FHSS y DSSS



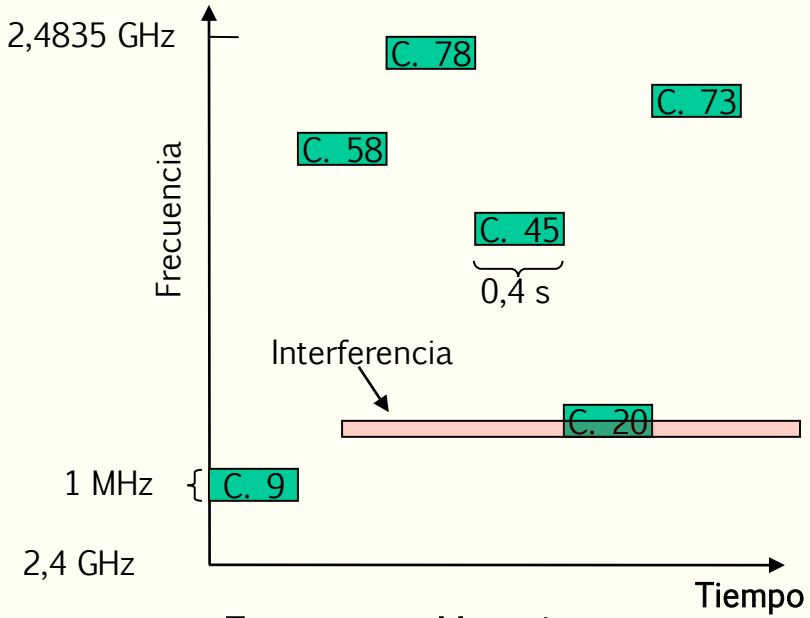
Frequency Hopping

Señal concentrada, alta intensidad
Elevada S/N
Pot. Transmitida: 100mW

Direct Sequence

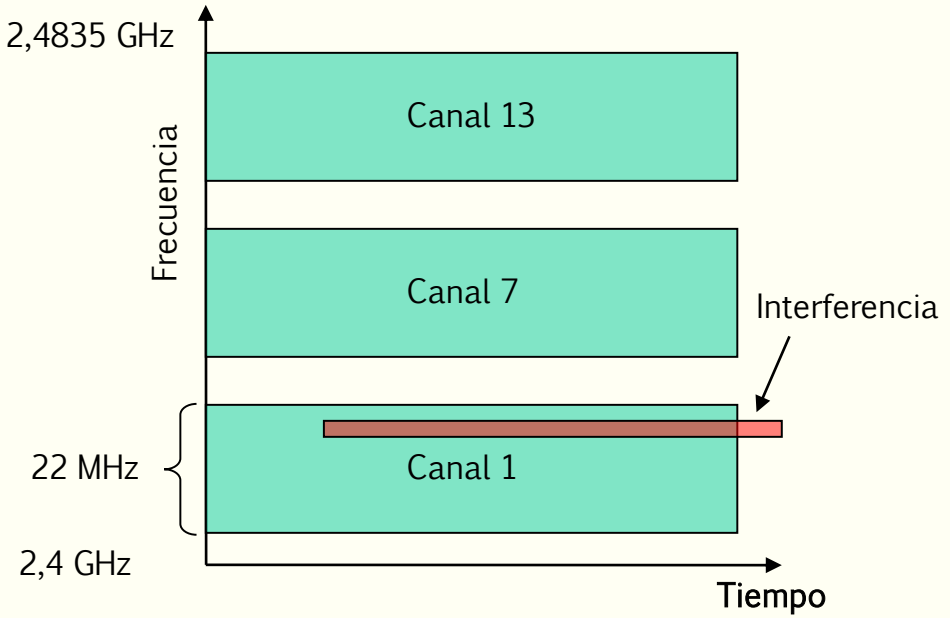
Señal dispersa, baja intensidad
Baja S/N
Pot. Transmitida: 100mW

Comparación de interferencia entre FHSS y DSSS



Frequency Hopping

El transmisor cambia de canal continuamente. En caso de interferencia, se retransmite



Direct Sequence

El canal es más ancho, y proclive a interferencias. Pero la señal lleva mucha redundancia. En caso de interferencia, se pueden llegar a extraer los datos.

Comparación entre FHSS y DSSS

- FH permite mayor número de emisores simultáneos y soporta mejor la interferencia por multitrayectoria (rebotes)
- DS permite mayor capacidad (802.11b). La interferencia multitrayectoria se resuelve con antenas diversidad
- Hoy en día FH no se utiliza en 802.11, solo en Bluetooth (802.15)

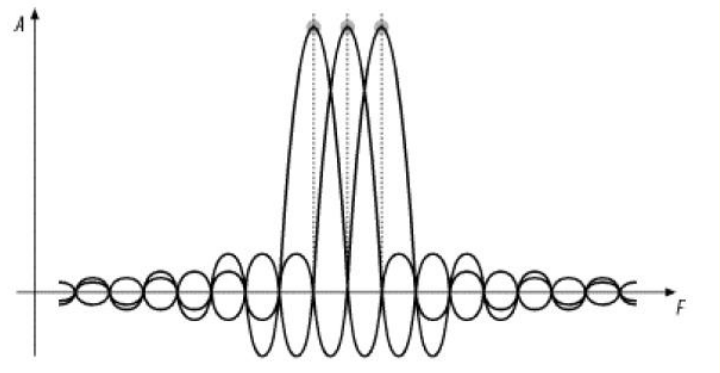
Antenas diversidad: el AP recibe la señal por las dos antenas y elige la de mejor calidad de señal.

Orthogonal Frecuency Division Multiplexing (OFDM)

Flujo de bits se divide en N trenes de bits que modulan N portadoras (subcanales) ortogonales, que se transmiten en paralelo.

Tasa de símbolos/s por canal: 250ksps; reduce IIS.

1 canal de 20 MHz ---> 52 subcanales (solapados) de 312.5 KHz: 48 para datos y 4 para corrección de errores.



Cada subportadora se modula mediante BPSK, QPSK, 16-QAM o 64-QAM, y se codifican con códigos convolucionales (R=1/2, 2/3 y 3/4)

Orthogonal Frecuency Division Multiplexing (OFDM)

Por ejemplo:

Tasa de símbolos: 250 ksps

Duración de un símbolo: 4 us

Subportadoras de datos: 48

Modulación: 64-QAM (6 bits codificados/ subportadora)

Cantidad de bits codificados por símbolo: 6 x 48 = 288

Bits de datos por símbolo: 3/4 x 288 = 216 bits/símbolo

Velocidad: 216 bits / 4 us = 54 Mbit/s

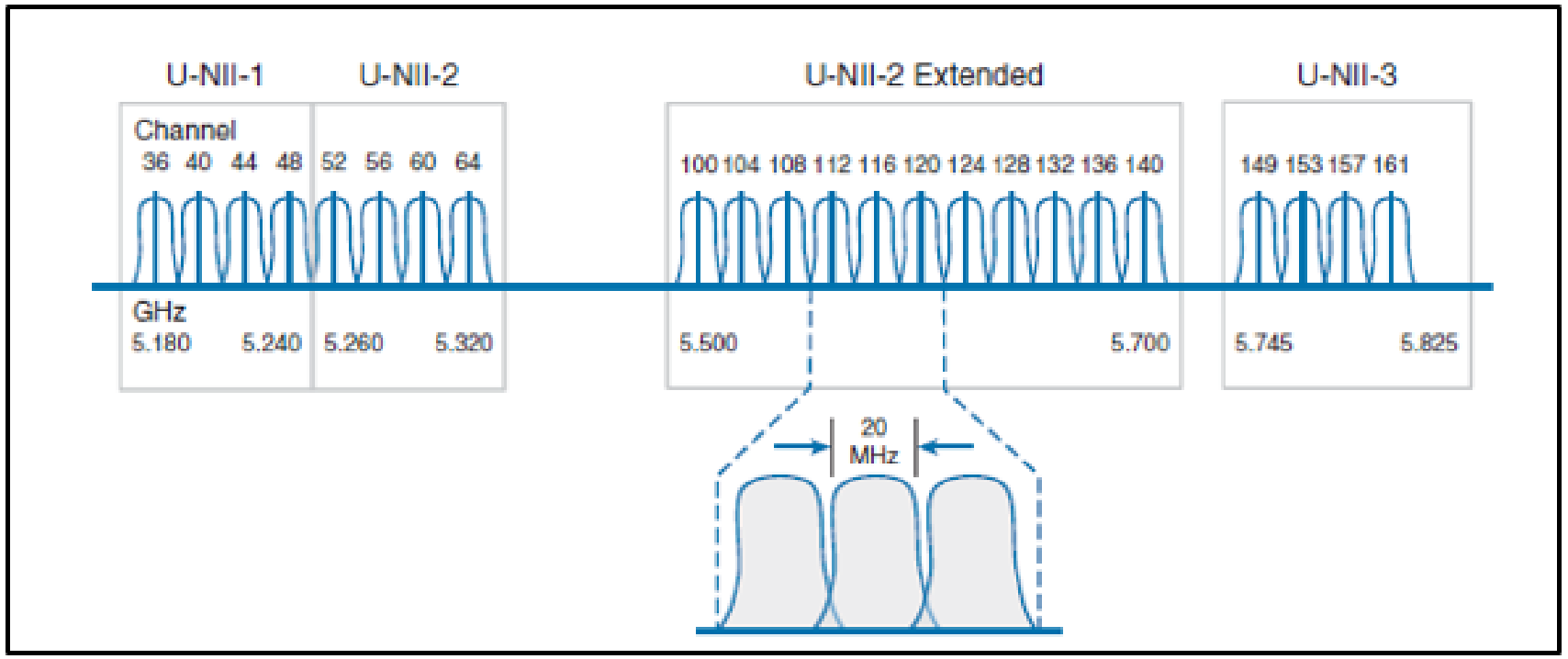
Orthogonal Frecuency Division Multiplexing (OFDM)

Modulación	Tasa de codificación	Bits codificados / portadora	Bits codificados / símbolo	Bits de datos / símbolo	Velocidad
BPSK	1/2	1	48	24	* 6 Mbps
BPSK	3/4	1	48	36	9 Mbps
QPSK	1/2	2	96	48	* 12 Mbps
QPSK	3/4	2	96	72	18 Mbps
16-QAM	1/2	4	192	96	* 24 Mbps
16-QAM	3/4	4	192	144	36 Mbps
64-QAM	2/3	6	288	192	48 Mbps
64-QAM	3/4	6	288	216	54 Mbps

MCS: Modulation Codification Scheme

IEEE 802.11a (5 GHz)

Orthogonal Frecuency Division Multiplexing (OFDM)



U-NII (Infraestructura Nacional de Información No Licenciada)

En la banda de 5 GHz los canales están separados 5 MHz. Hay un máximo de 23 canales sin superposición

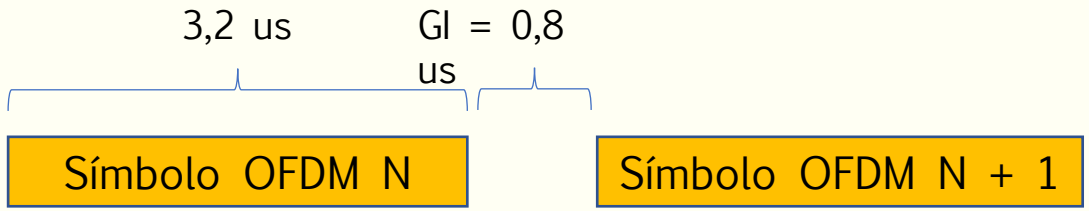
Orthogonal Frecuency Division Multiplexing (OFDM)

- OFDM también es aplicado en la banda de 2.4 GHz
- Definido en IEEE 802.11g
- Soporta las mismas velocidades que 802.11a
- El estándar es compatible con 802.11b, por lo que soporta las velocidades de este estándar

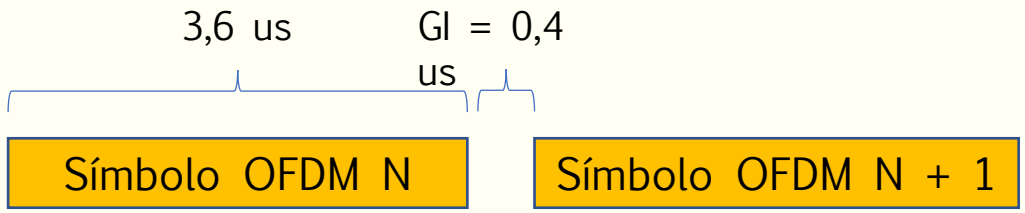
IEEE 802.11g (2.4 GHz)

Mejoras (1)

Intervalo de guarda: es la separación entre dos símbolos OFDM



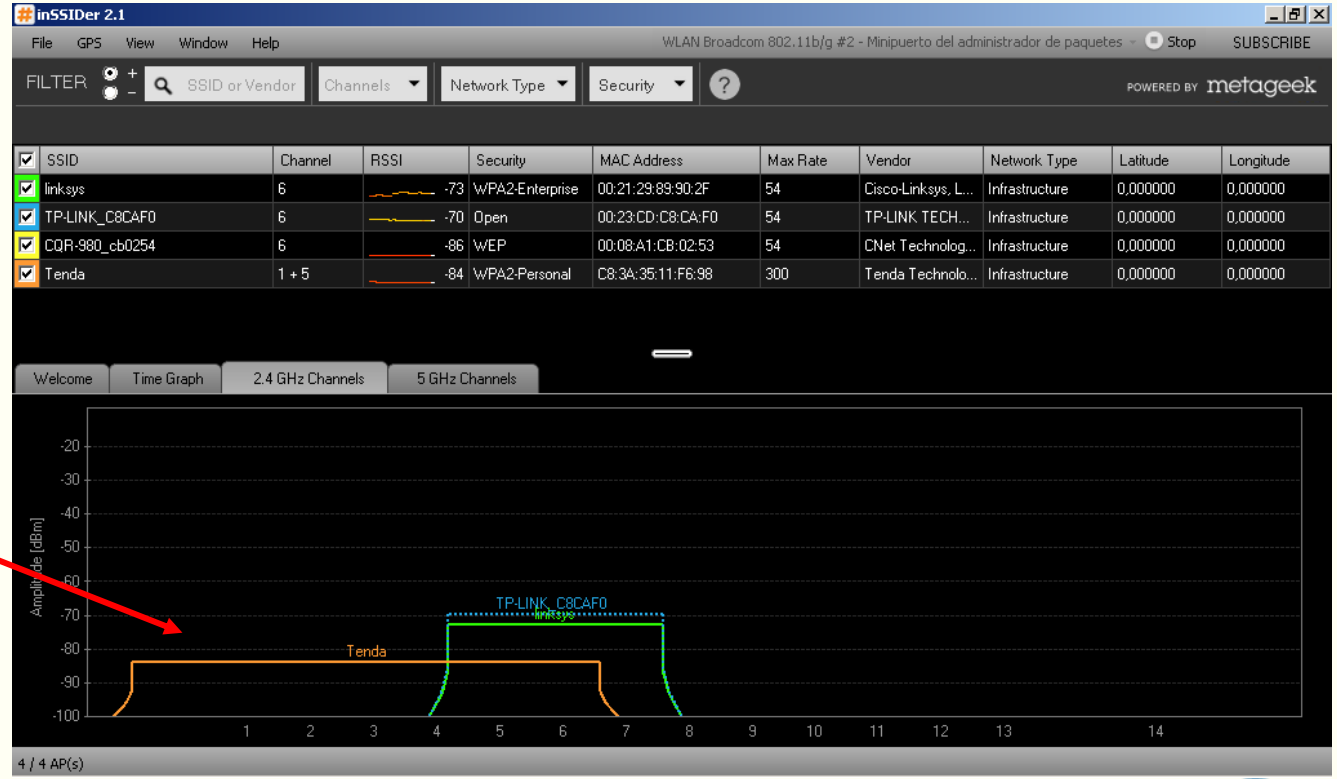
Si el retardo multi trayectoria es bajo, se puede utilizar un intervalo de guarda menor



Mejoras (2)

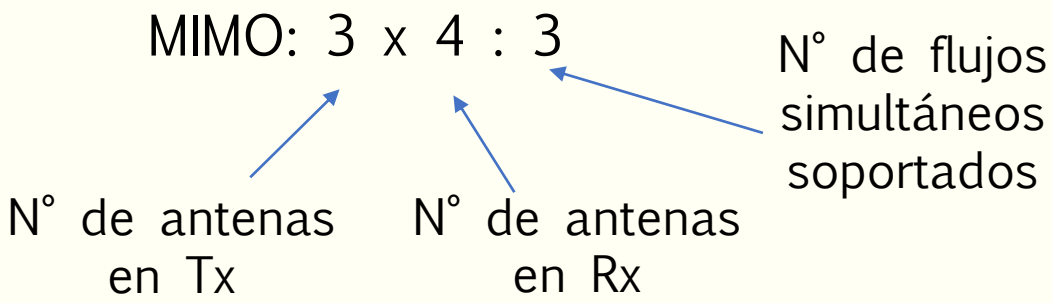
Unión de canales (channel bonding): se pueden utilizar para aumentar la velocidad de la transmisión

Utiliza un bonding de 2 canales

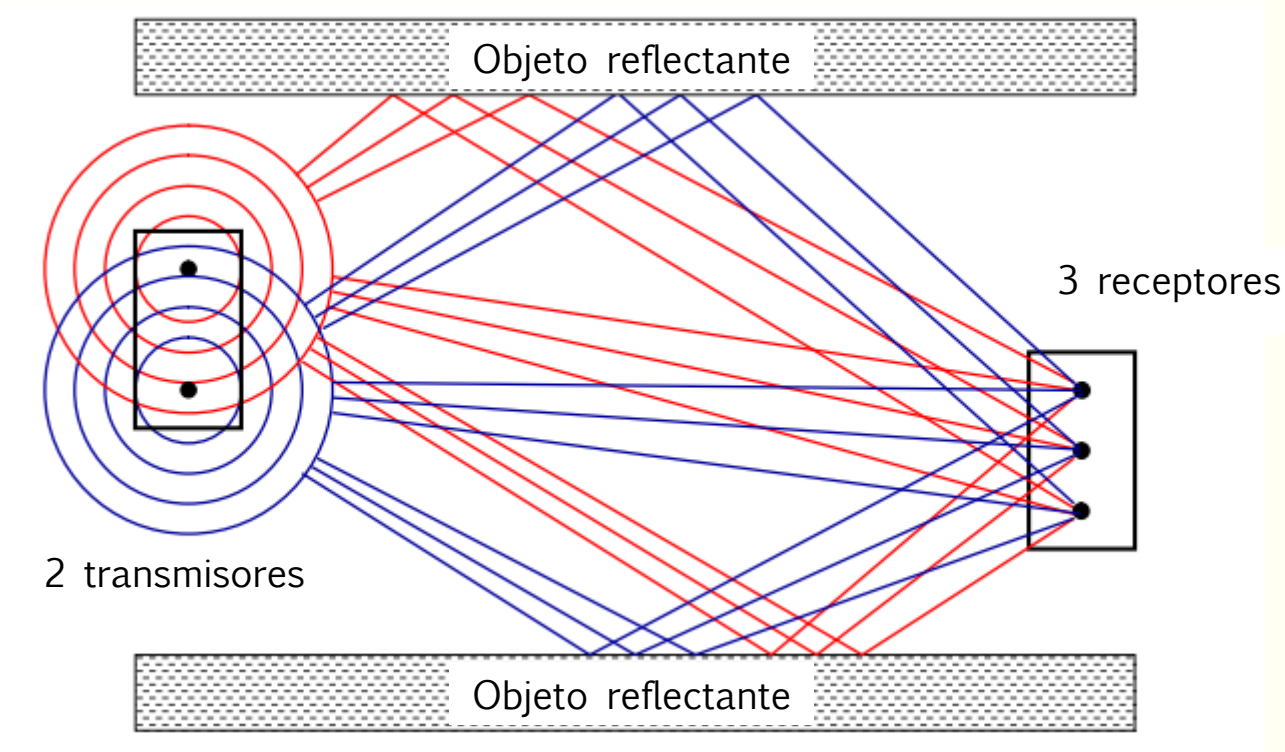


Mejoras (3)

- MIMO: Multiple Input Multiple Output
- Realiza un multiplexado espacial para enviar y recibir varios flujos (streams) en paralelo por el mismo canal. Se utilizan varias antenas en transmisión y en recepción.
- Terminología:



Mejoras (3)

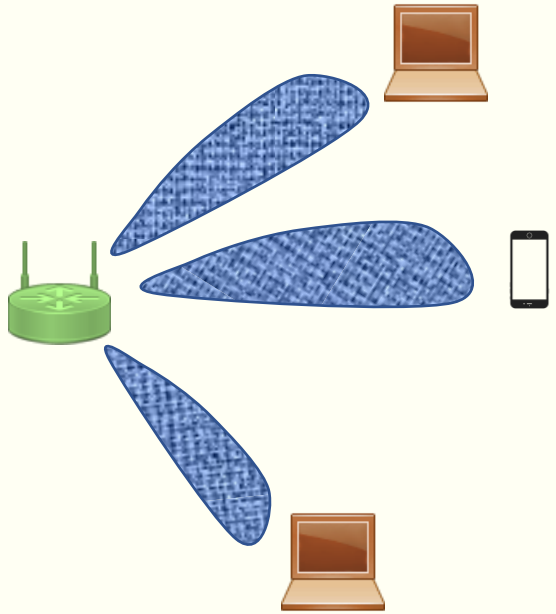


El flujo de señal es dividido en múltiples flujos, donde cada uno se transmite por una antena. Cada uno de estos flujos arriba al receptor con diferentes amplitudes (nivel de señal) y fase.

Mejoras (4)

Beamforming:

- El transmisor transmite las señales con mayor intensidad en dirección a la ubicación del receptor.
- Mejora la S/N, y por lo tanto la velocidad.
- La mejora se percibe a distancias medias.
- Se utiliza sólo cuando el receptor tiene una sola antena.



Integrando todas las mejoras

- Aumento de portadoras de datos, de 48 a 52
  Mejora de velocidad: de 54 a 58.5 Mbps
- Aumento de la tasa de codificación, de 3/4 a 5/6
  Mejora de velocidad: de : 58.5 a 65 Mbps
- Reducción del intervalo de guarda, de 0.8 a 0.4 us
  Mejora de velocidad: de 65 a 72.2 Mbps
- Duplicación del BW mediante channel bonding
  Mejora de velocidad: de 72,2 a 150 Mbps
- Hasta 4 flujos espaciales (MIMO)
  Mejora de velocidad: de 150 a 600 Mbps

IEEE 802.11n

Velocidades soportadas en 802.11n (algunas)

MCS index	Spatial streams	Modulation type	Coding rate	Data rate (Mbit/s)			
				20 MHz channel		40 MHz channel	
				800 ns GI	400 ns GI	800 ns GI	400 ns GI
0	1	BPSK	1/2	6.50	7.20	13.50	15.00
1	1	QPSK	1/2	13.00	14.40	27.00	30.00
2	1	QPSK	3/4	19.50	21.70	40.50	45.00
3	1	16-QAM	1/2	26.00	28.90	54.00	60.00
4	1	16-QAM	3/4	39.00	43.30	81.00	90.00
5	1	64-QAM	2/3	52.00	57.80	108.00	120.00
6	1	64-QAM	3/4	58.50	65.00	121.50	135.00
7	1	64-QAM	5/6	65.00	72.20	135.00	150.00
8	2	BPSK	1/2	13.00	14.40	27.00	30.00
9	2	QPSK	1/2	26.00	28.90	54.00	60.00
10	2	QPSK	3/4	39.00	43.30	81.00	90.00
11	2	16-QAM	1/2	52.00	57.80	108.00	120.00
12	2	16-QAM	3/4	78.00	86.70	162.00	180.00
13	2	64-QAM	2/3	104.00	115.60	216.00	240.00
14	2	64-QAM	3/4	117.00	130.00	243.00	270.00
15	2	64-QAM	5/6	130.00	144.40	270.00	300.00

Redes inalámbricas

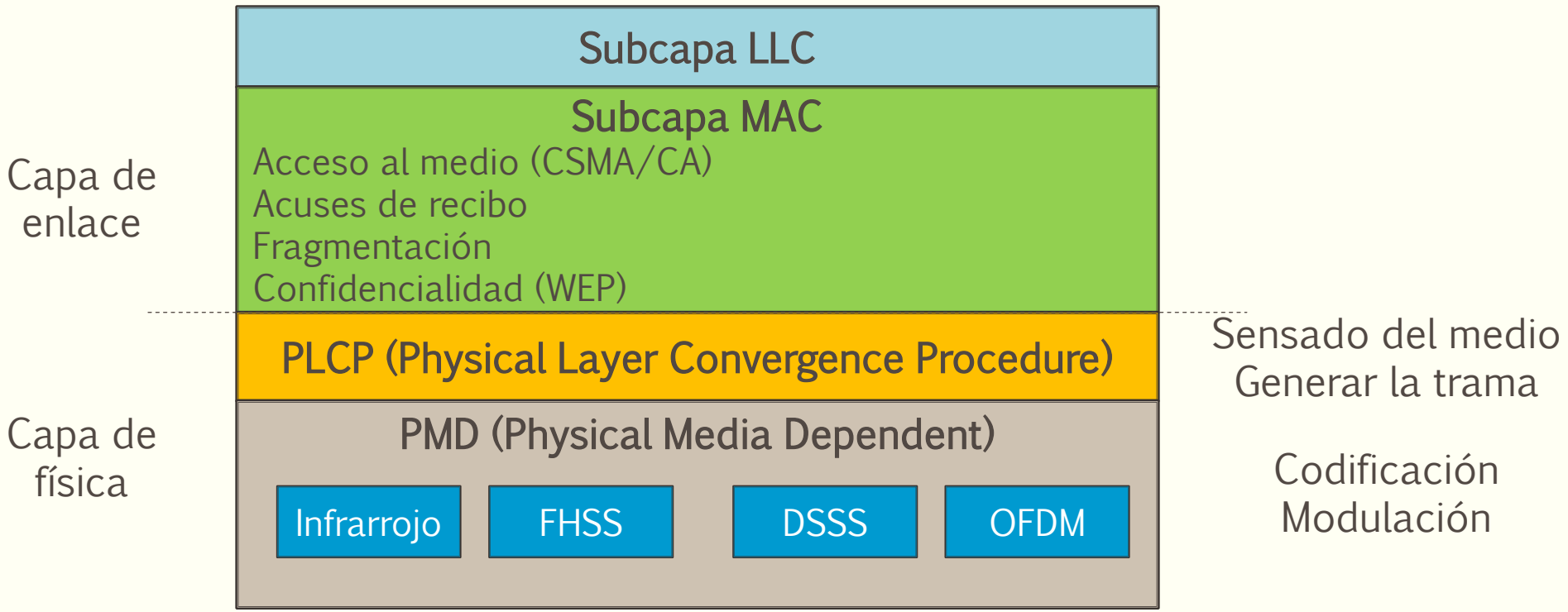
Estándar	Año	Esquema	Modulación	Banda	BW	MIMO	Velocidades
802.11	1997	DSSS, FHSS	BPSK	2.4 GHz	22 MHz	ND	1, 2 Mbps
802.11a	1999	OFDM	BPSK, QPSK, 16-QAM o 64-QAM	5 GHz	22 MHz	ND	6 – 54 Mbps
802.11b	1999	DSSS	BPSK, QPSK	2.4 GHz	22 MHz	ND	1, 2, 5.5, 11 Mbps
802.11g	2003	OFDM	BPSK, QPSK, 16-QAM o 64-QAM	5 GHz	20 MHz	ND	6 – 54 Mbps
802.11n (WiFi-4)	2009	OFDM	BPSK, QPSK, 16-QAM o 64-QAM	2.4 GHz	20 MHz 40 MHz	4x4	6.5 - 600 Mbps
802.11ac (WiFi-5)	2013	OFDM	BPSK, QPSK, 16-QAM, 64-QAM, 128-QAM o 256-QAM	5 GHz	20 MHz 40 MHz 80 MHz 160 MHz	8x8	6.5 Mbps – 6.93 Gbps
802.11ax (WiFi-6)	2019	OFDM	h/1024-QAM	2.4 GHz 5 GHz	Idem 802.11ac	8x8	h/ 9.6 Gbps

Redes inalámbricas

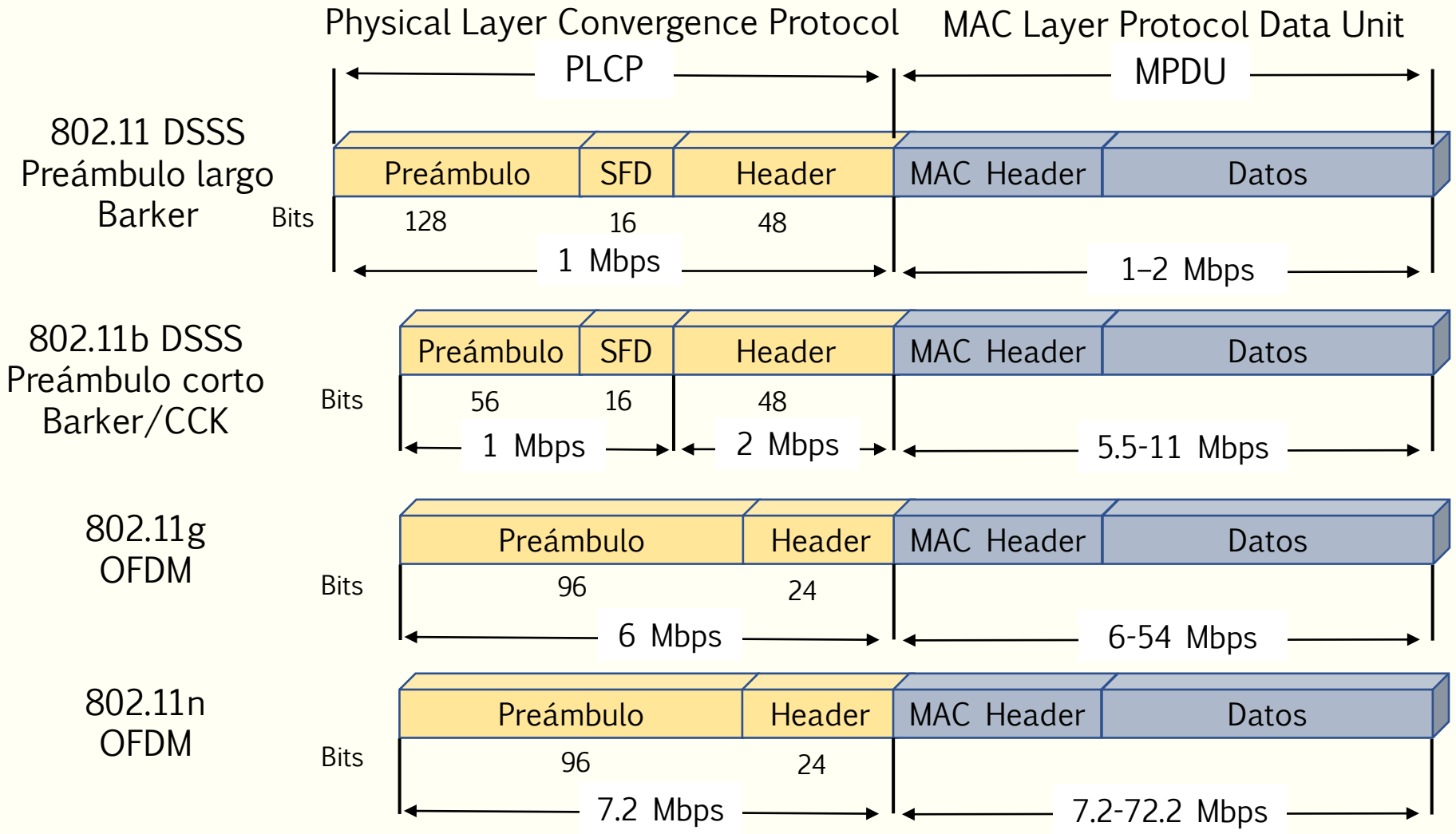
NanoStation®M NanoStation®locoM

OPERATING FREQUENCY 2412-2462MHz							
2GHz TX POWER SPECIFICATIONS				2GHz RX SPECIFICATIONS			
	DataRate	Avg. TX	Tolerance		DataRate	Sensitivity	Tolerance
11b/g	1-24Mbps	23 dBm	+/-2dB	11b/g	24Mbps	-83 dBm	+/-2dB
	36Mbps	21 dBm	+/-2dB		36Mbps	-80 dBm	+/-2dB
	48Mbps	19 dBm	+/-2dB		48Mbps	-77 dBm	+/-2dB
	54Mbps	18 dBm	+/-2dB		54Mbps	-75 dBm	+/-2dB
11n / AirMax	MCS0	23 dBm	+/-2dB	11n / AirMax	MCS0	-96 dBm	+/-2dB
	MCS1	23 dBm	+/-2dB		MCS1	-95 dBm	+/-2dB
	MCS2	23 dBm	+/-2dB		MCS2	-92 dBm	+/-2dB
	MCS3	23 dBm	+/-2dB		MCS3	-90 dBm	+/-2dB
	MCS4	22 dBm	+/-2dB		MCS4	-86 dBm	+/-2dB
	MCS5	20 dBm	+/-2dB		MCS5	-83 dBm	+/-2dB
	MCS6	18 dBm	+/-2dB		MCS6	-77 dBm	+/-2dB
	MCS7	17 dBm	+/-2dB		MCS7	-74 dBm	+/-2dB
	MCS8	23 dBm	+/-2dB		MCS8	-95 dBm	+/-2dB
	MCS9	23 dBm	+/-2dB		MCS9	-93 dBm	+/-2dB
	MCS10	23 dBm	+/-2dB		MCS10	-90 dBm	+/-2dB
	MCS11	23 dBm	+/-2dB		MCS11	-87 dBm	+/-2dB
	MCS12	22 dBm	+/-2dB		MCS12	-84 dBm	+/-2dB
	MCS13	20 dBm	+/-2dB		MCS13	-79 dBm	+/-2dB
	MCS14	18 dBm	+/-2dB		MCS14	-78 dBm	+/-2dB
	MCS15	17 dBm	+/-2dB		MCS15	-75 dBm	+/-2dB

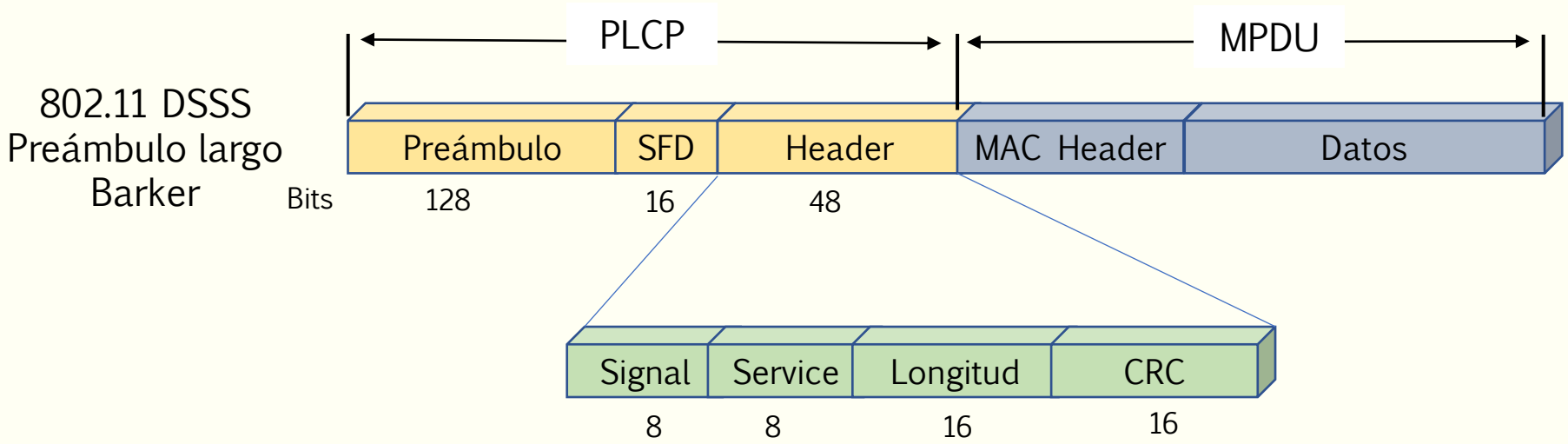
Modelo de referencia de 802.11



Redes inalámbricas



Redes inalámbricas



- Preámbulo: 128 “1” para sincronizar transmisor – receptor, y elegir antena
- SFD: delimitador de comienzo, 0000 0101 1100 1111
- Signal: identifica la velocidad de transmisión (1-2 Mbps)
- Service: Reservado
- Longitud: indica la cantidad de microsegundos que dura la trama
- CRC: 16-CRC aplicado al Header

REDES INALÁMBRICAS

- Introducción
- Nivel físico
- **Topología**
- Nivel MAC
- Conectividad en redes 802,11

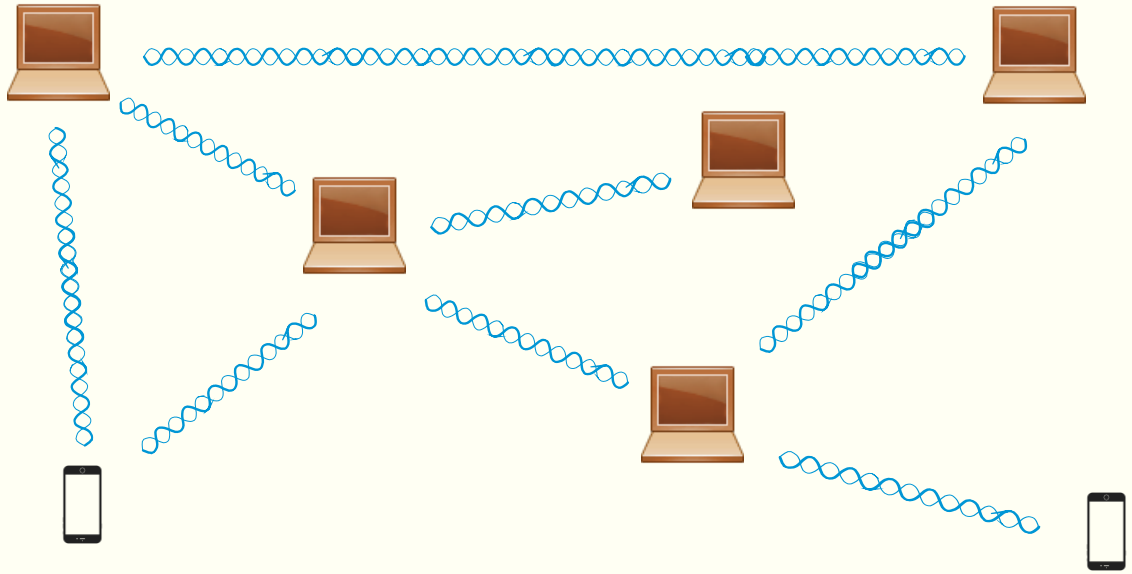
BSS Basic Service Set

- BSS es el conjunto de dispositivos inalámbricos (fijos o móviles) que pueden comunicarse entre sí, a través de un medio en común, dentro de una red 802.11
- Un BSS puede incluir o no un punto de acceso (Access Point, AP), para proveer conectividad a una red cableada (Ethernet) o a otra red inalámbrica mediante un AP.
- BSA (Basic Service Area) es el área de cobertura de una BSS.

- Ad-hoc
  - BSS
- Infraestructura
  - BSS
  - EBSS (Extended)
  - MBSS (Mesh)

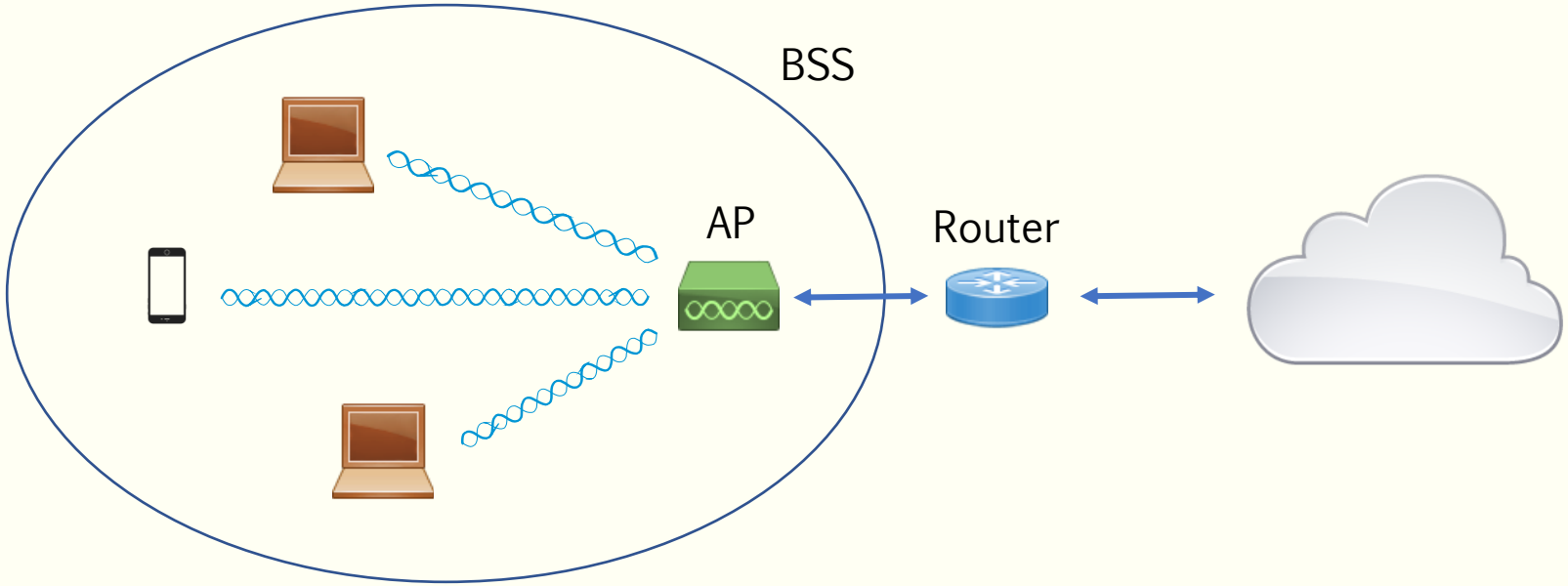
Ad-hoc: IBSS

Independant Basic Service Set (IBSS) - Las estaciones inalámbricas se comunican directamente entre sí. Cada estación puede no ser capaz de comunicarse con cualquier otra estación



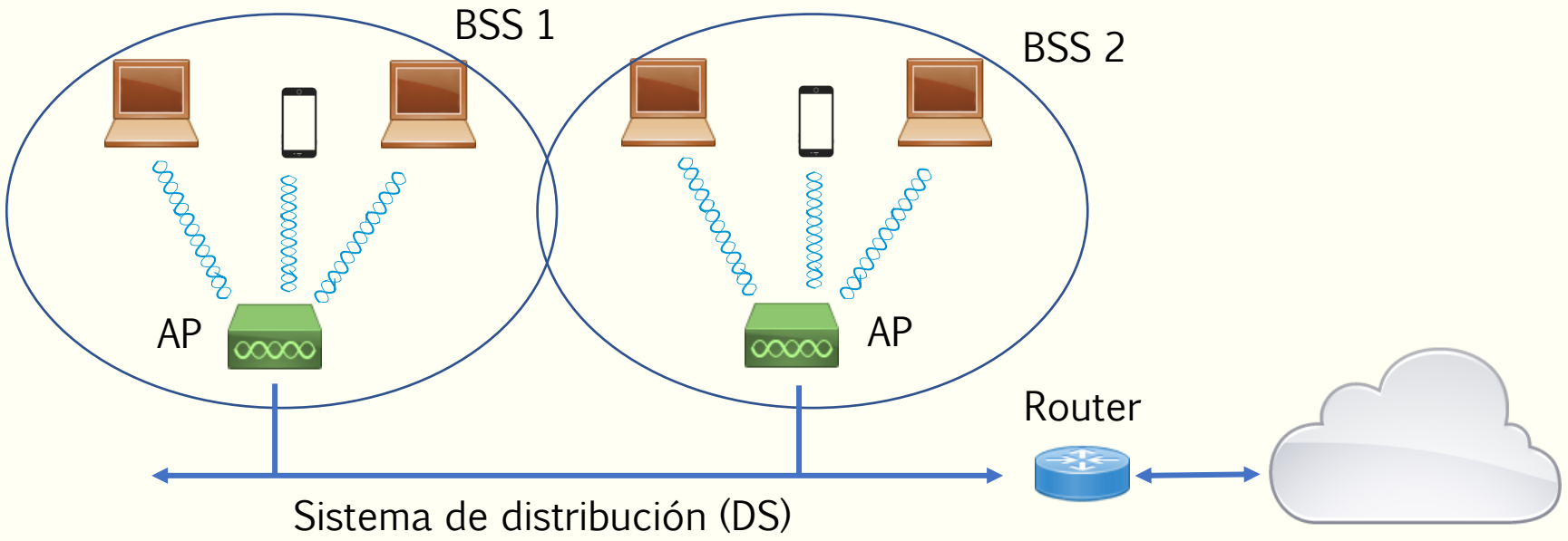
Infraestructura: BSS

Basic Service Set (BSS) – Un punto de acceso (AP) provee la función de puente(bridge) local para BSS. Todas las estaciones se comunican con el AP y no directamente entre ellas.



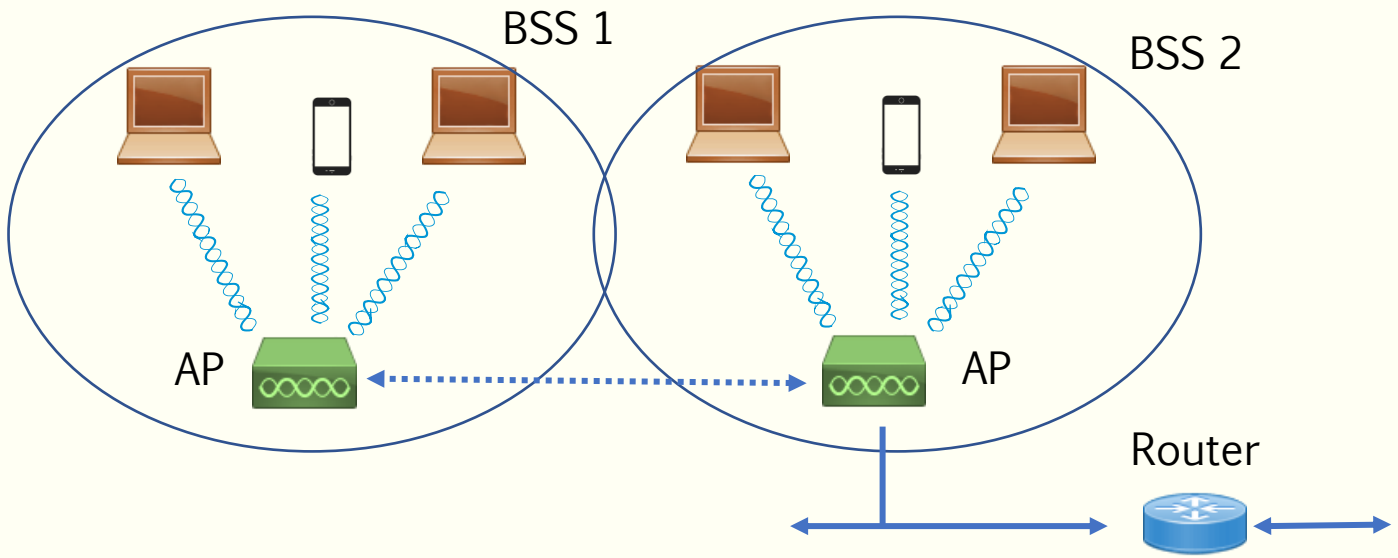
Infraestructura: ESS

Extended Service Set (ESS) – Un ESS es un conjunto de BSSs, donde los APs se comunican entre ellos para intercambiar tráfico desde una BSS a otra.



Infraestructura: MBSS

Mesh Basic Service Set (MBSS) – Un MBSS es un conjunto de BSSs, donde los APs se comunican entre ellos a través de un medio inalámbrico

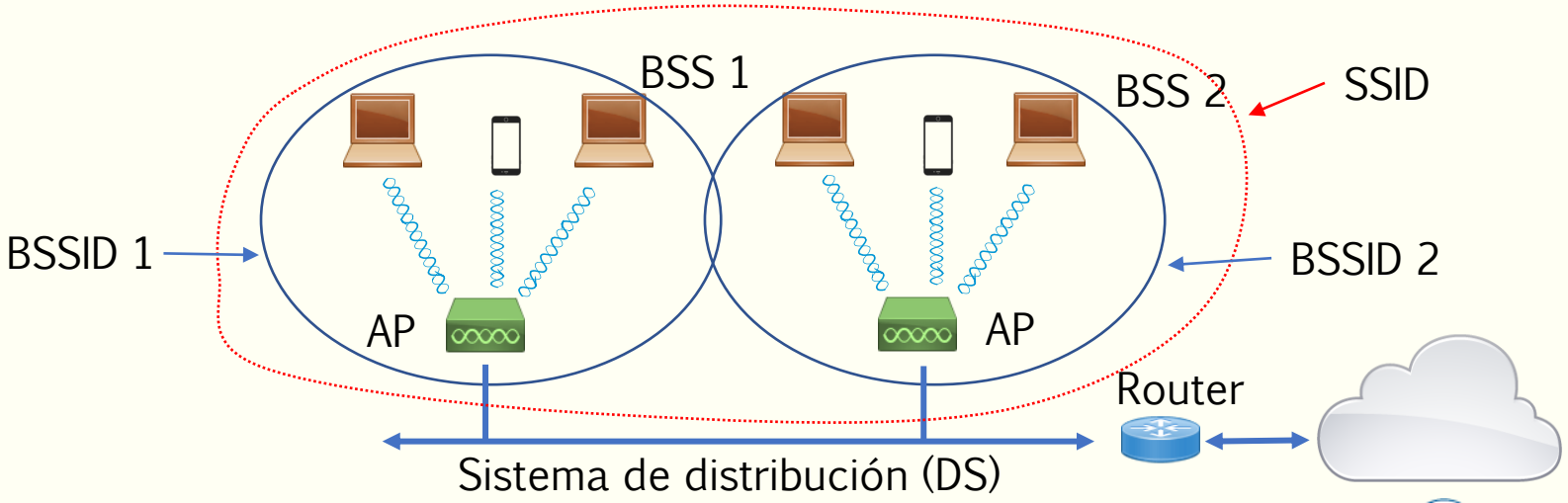


Identificadores: BSSID y SSID

Cada BSS se identifica por una cadena de seis dígitos hexadecimales llamada **BSSID**, que se corresponde con su dirección MAC o un derivado.

Los IBSS (redes ad-hoc, sin AP) se identifican por un **BSSID** generado al azar por quien crea el IBSS, y no tiene relación con la MAC

Cada red inalámbrica se identifica por un **SSID** (Service Set Identifier), que es una cadena de hasta 32 caracteres alfanuméricos (por ej.: WiFi-Ingeniería).



Direcciones MAC en los AP

Cada AP tiene al menos dos direcciones MAC:

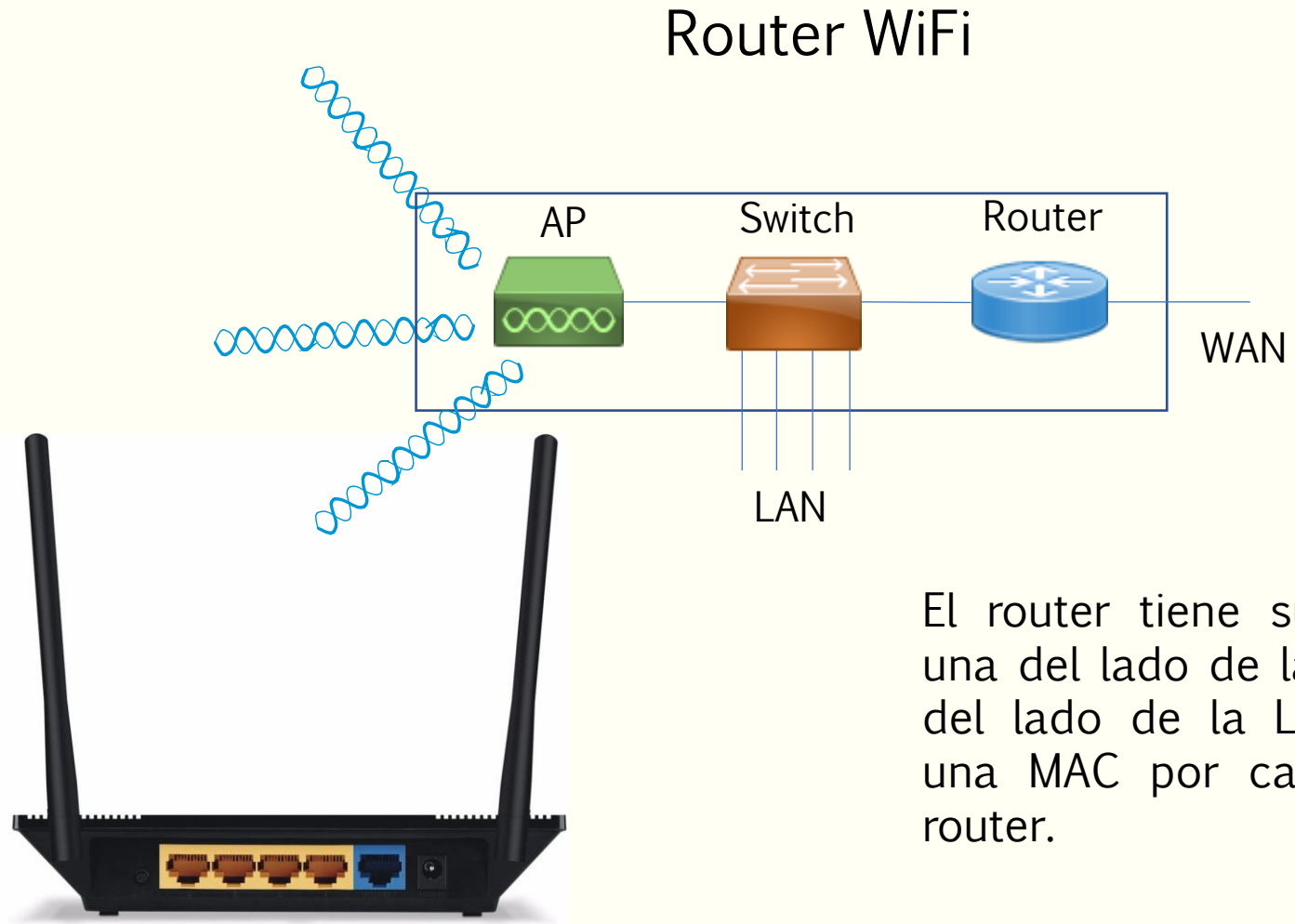
- una en su interfaz inalámbrica
- una en su interfaz del sistema de distribución (DS), típicamente en la interfaz Ethernet

Dirección MAC asociada la interfaz inalámbrica: BSSID

Si el AP tiene mas de un radio, cada uno tendrá una MAC diferente

Dirección MAC asociada la interfaz Ethernet: se utiliza para gestión

Redes inalámbricas

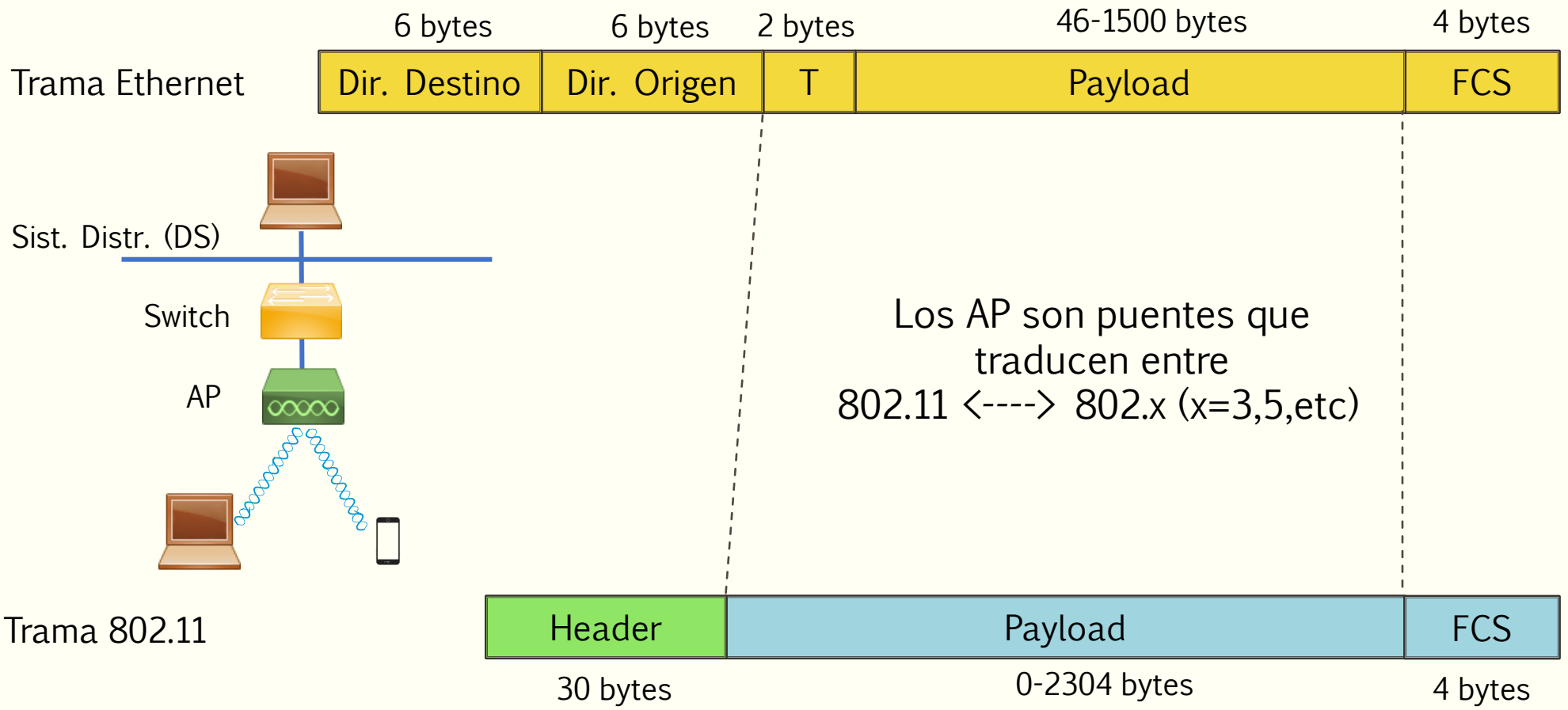


El router tiene sus dos MAC, una del lado de la WAN y otra del lado de la LAN. Además, una MAC por cada radio del router.

REDES INALÁMBRICAS

- Introducción
- Nivel físico
- Topología
- **Nivel MAC**
- Conectividad en redes 802,11

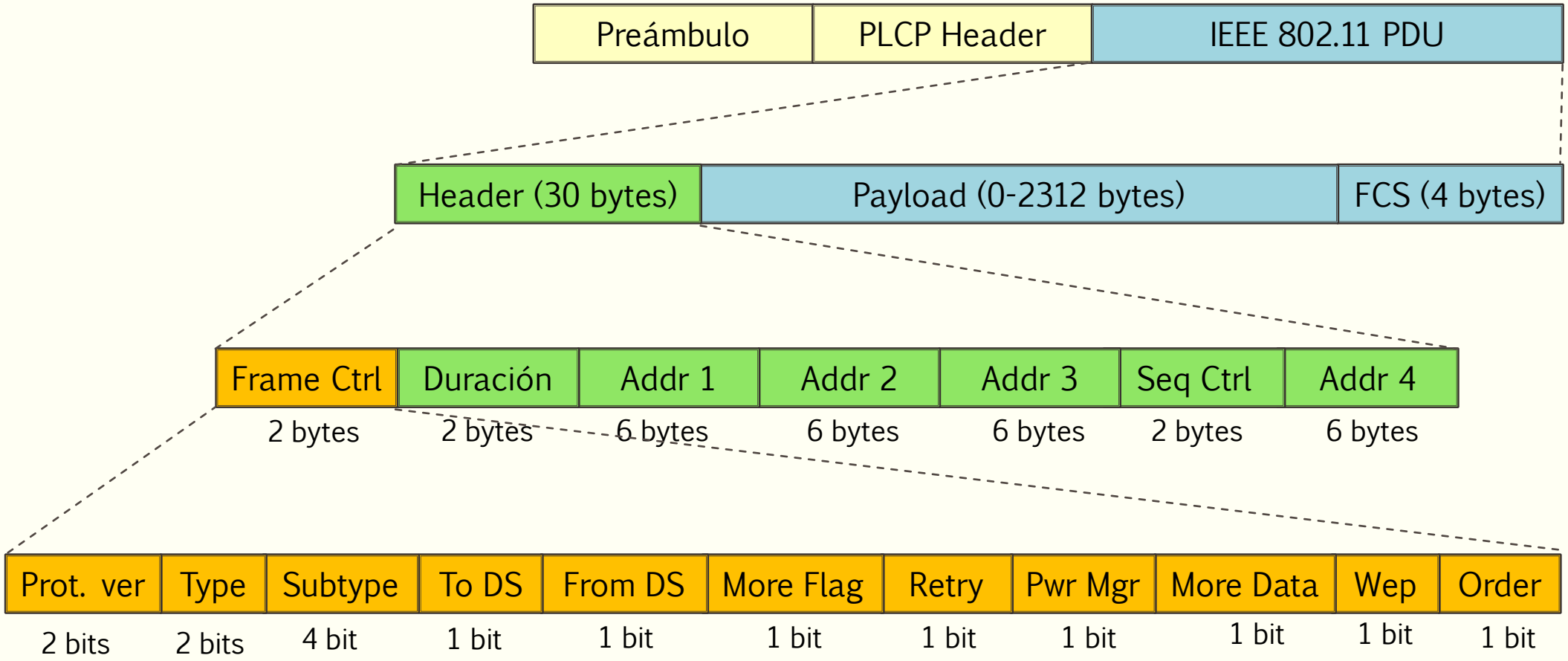
Redes inalámbricas



Tipos de tramas 802.11

- De **gestión**: se utilizan para administrar un BSS. Por ejemplo. sondeo, asociación, roaming y desconexión de estaciones en el BSS.
  - Tramas baliza (beacon)
  - Tramas de sonda petición/respuesta (probe)
  - Tramas de autenticación/desautenticación
  - Tramas de asociación/reasociación/desasociación
- De **control**: sirven para controlar el acceso al medio. Deben escucharlas todas las estaciones. Contienen sólo la cabecera.
  - Tramas RTS (Request To Send) y CTS (Clear To Send)
  - Tramas ACK (Acknowledgement, acuse de recibo)
  - PS-Poll (Power Save Poll, solicitud de tramas al encender el radio)
- De **datos** (paquetes IP, ARP, STP, etc.)

Trama 802.11


Preámbulo
PLCP Header
IEEE 802.11 PDU
Header (30 bytes)
Payload (0-2312 bytes)
FCS (4 bytes)
Frame Ctrl
Duración
Addr 1
Addr 2
Addr 3
Seq Ctrl
Addr 4
2 bytes
2 bytes
6 bytes
6 bytes
6 bytes
2 bytes
6 bytes
Prot. ver
Type
Subtype
To DS
From DS
More Flag
Retry
Pwr Mgr
More Data
Wep
Order
2 bits
2 bits
4 bit
1 bit
1 bit
1 bit
1 bit
1 bit
1 bit
1 bit
1 bit

Campo control de trama 802.11

Prot. ver	Type	Subtype	To DS	From DS	More Flag	Retry	Pwr Mgr	More Data	Wep	Order
2 bits	2 bits	4 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit

- Protocol Version: versión de protocolo utilizado. Las estaciones receptoras verifican si lo soportan.
- Tipo y Sub tipo: determina la función de la trama (control, datos, y gestión). Hay muchos sub tipos para cada tipo de trama. Cada subtipo determina una función específica a realizar con el tipo de trama asociada.
- To DS and From DS: indica si la trama está saliendo o entrando al sistema de distribución; solo se utiliza en tramas de datos de estaciones asociadas a un Access Point.

Campo control de trama 802.11

Prot. ver	Type	Subtype	To DS	From DS	More Flag	Retry	Pwr Mgr	More Data	Wep	Order
2 bits	2 bits	4 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit

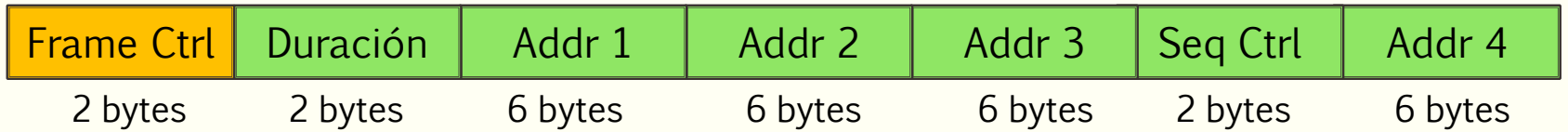
- More Fragments: indica si a continuación existen más fragmentos en la trama de datos o gestión.
- Retry: indica si la trama de datos o gestión está siendo retransmitida.
- Power Management: indica si la estación emisora está en modo activo o en modo de ahorro de energía.
- More Data: indica a una estación que está en modo de ahorro de energía que el Access Point tiene más tramas para enviarle. También es utilizado por un Access Point para indicar que va a enviar tramas broadcast o multicast.

Campo control de trama 802.11

Prot. ver	Type	Subtype	To DS	From DS	More Flag	Retry	Pwr Mgr	More Data	Wep	Order
2 bits	2 bits	4 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit

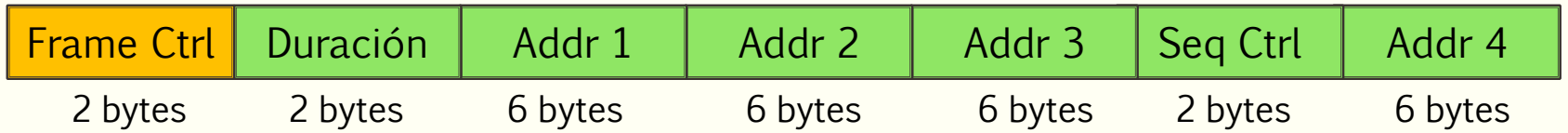
- WEP: indica si en la trama se utiliza encriptación y/o autenticación. Puede ser activado en tramas de datos o gestión que tengan activado el subtipo autenticación.
- Order: indica que todas las tramas recibidas deben ser procesadas en orden.

Trama 802.11

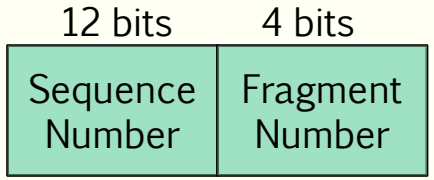


- Duration/ID Field: Es utilizado por todas las tramas de control para indicar el tiempo remanente necesario para recibir la próxima trama. Cuando el subtipo es Power Save PS Poll, el campo contiene la identidad de asociación de la estación transmisora.

Trama 802.11



- **Sequence Control field:** número de fragmento y el número de secuencia.



Sequence Number indica el Nº de secuencia de cada trama. Este Nº es el mismo para todos los fragmentos de una trama fragmentada. Si la trama no es fragmentada el Nº se incrementa en 1 para cada trama hasta 4095, cuando se resetea a cero.

Fragment Number indica el número de fragmento de una trama fragmentada enviada. El valor inicial es 0 y se va incrementando en 1 para cada fragmento subsecuente.

Trama 802.11

Address:

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

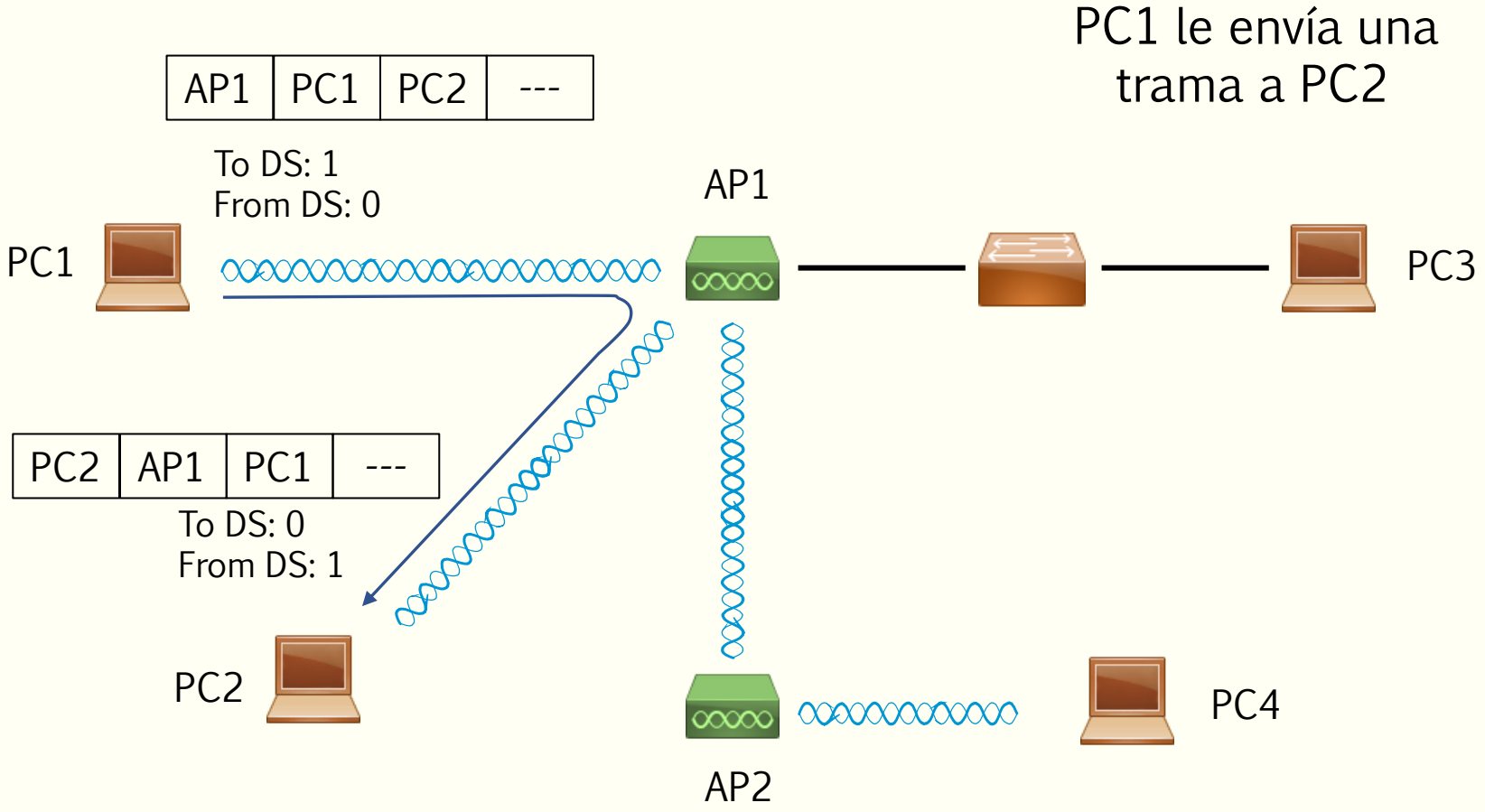
Destination Address (DA): dirección MAC del destino final de la trama.

Source Address (SA): dirección MAC de la estación que inició la trama

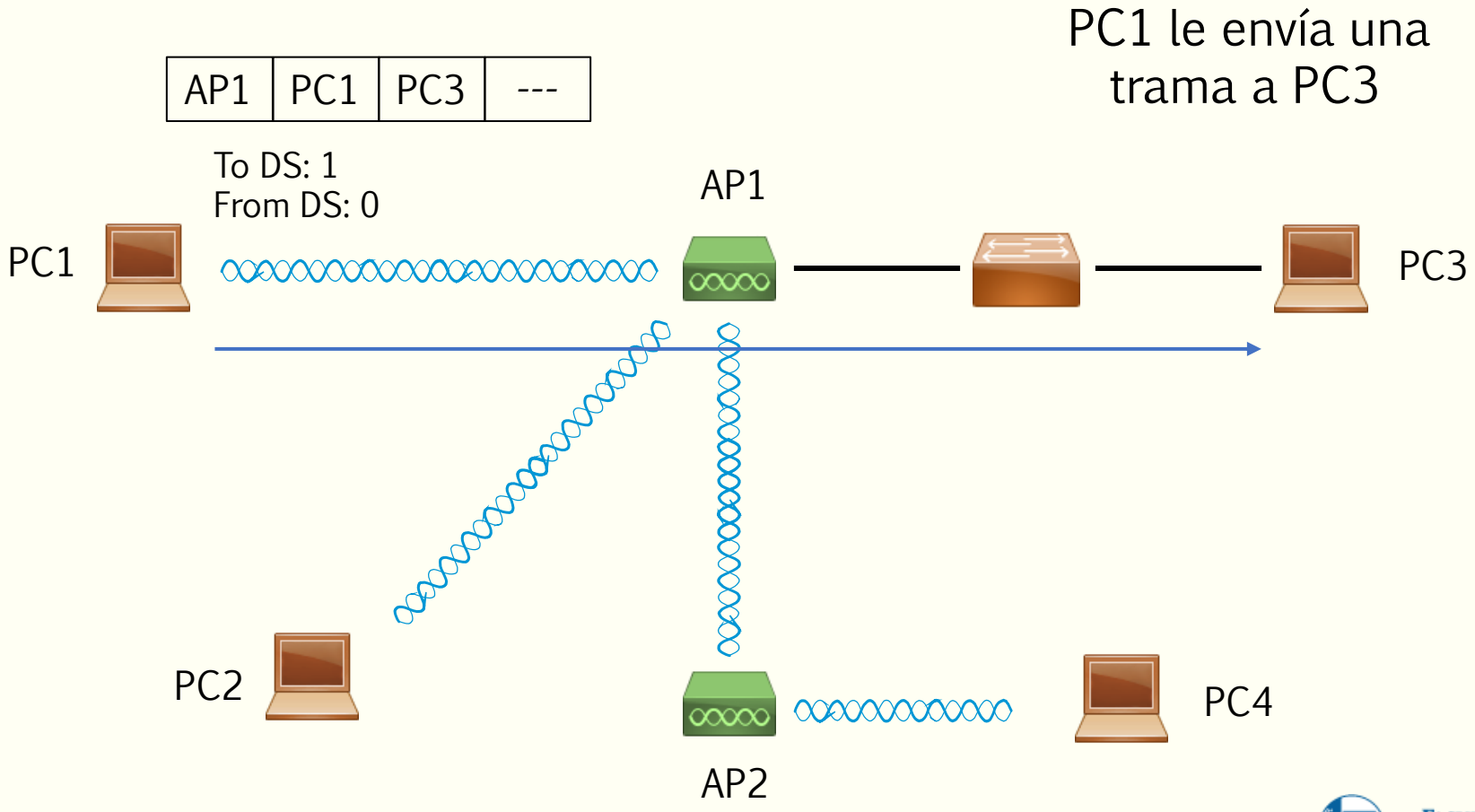
Transmitter Address (TA): la dirección MAC de la estación que transmite la trama al medio inalámbrico

Receiver Address (RA): dirección MAC de la estación inmediatamente próxima del medio inalámbrico que recibirá la trama.

Trama 802.11


PC1 le envía una trama a PC2
AP1 | PC1 | PC2 | ---
To DS: 1
From DS: 0
AP1
PC1
PC3
PC2 | AP1 | PC1 | ---
To DS: 0
From DS: 1
PC2
PC4
AP2

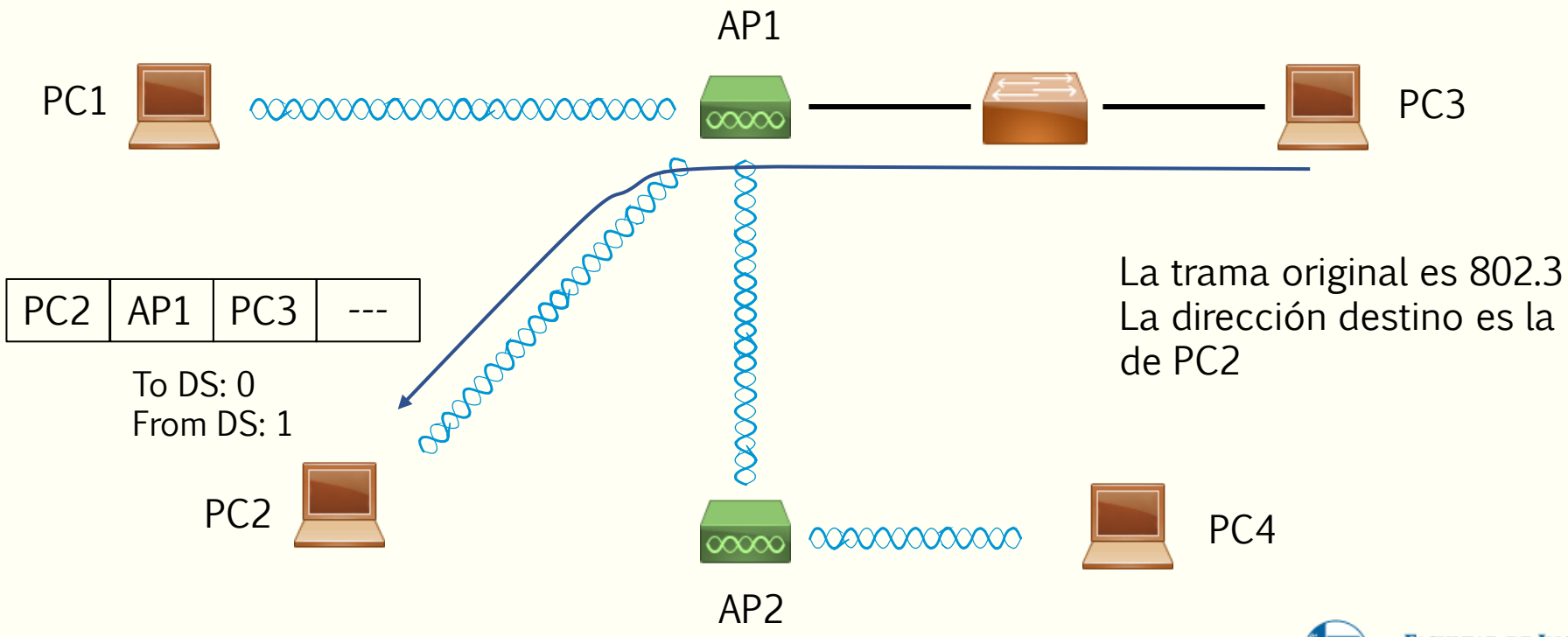
Trama 802.11


PC1 le envía una trama a PC3
AP1
PC1
PC3

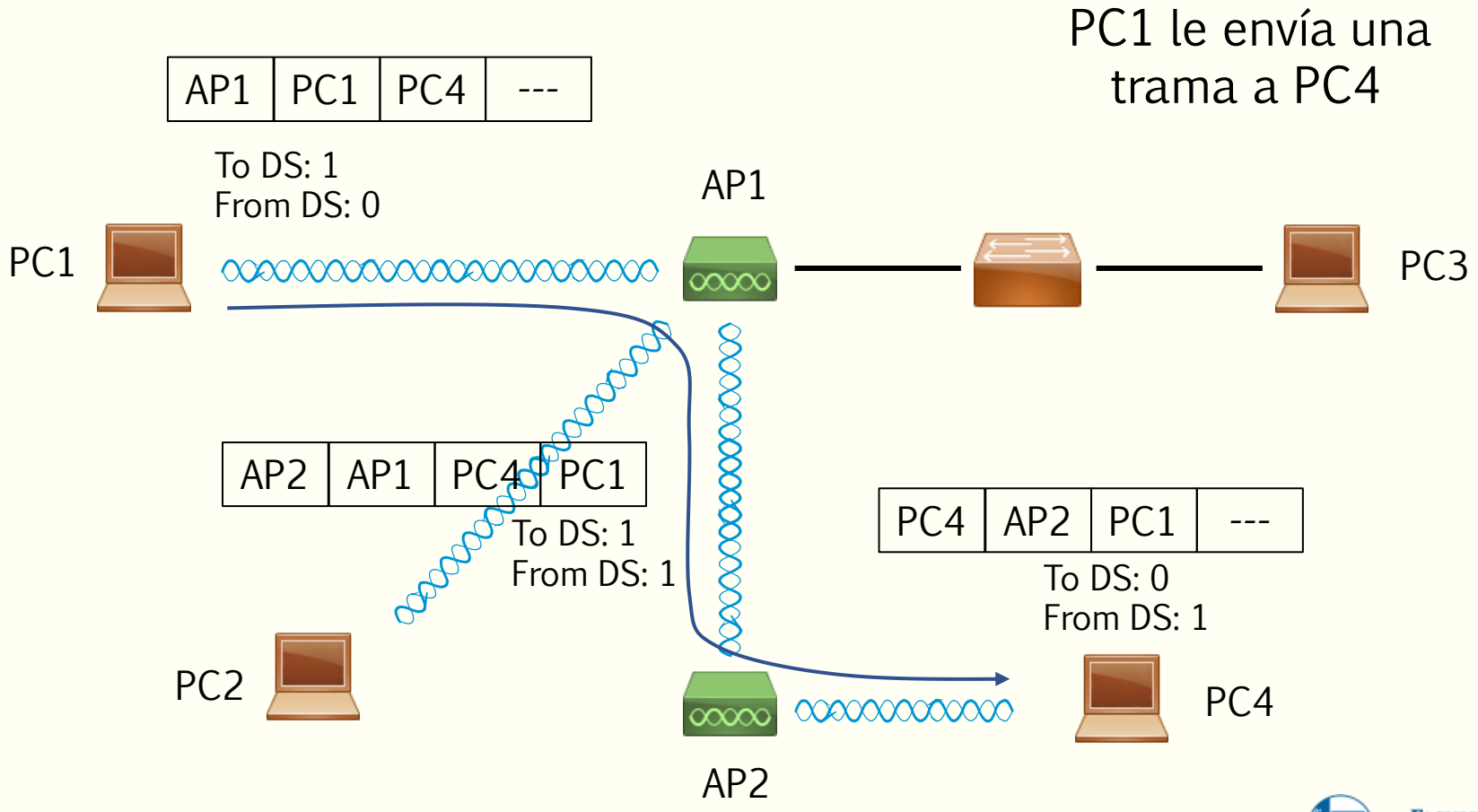
To DS: 1
From DS: 0
AP1
PC1
PC3
PC2
PC4
AP2

Trama 802.11

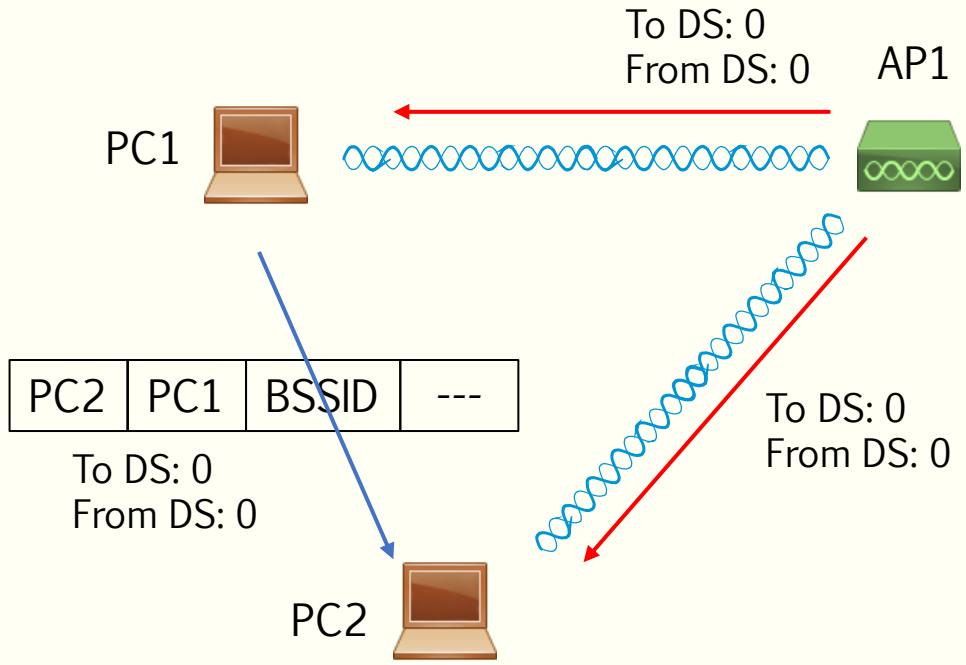
PC3 le envía una trama a PC2



Trama 802.11


PC1 le envía una trama a PC4
AP1 PC1 PC4 ---
To DS: 1
From DS: 0
AP1
PC1
PC3
AP2 AP1 PC4 PC1
To DS: 1
From DS: 1
PC4 AP2 PC1 ---
To DS: 0
From DS: 1
PC2
PC4
AP2

Trama 802.11



En casos especiales, tanto el To como el From son = 0. Por ej.:

- Un AP envía una trama de gestión o control, la cual es un broadcast.
- Una estación envía una trama de gestión a un AP
- Una estación se comunica con otra estación, en modo ad-hoc

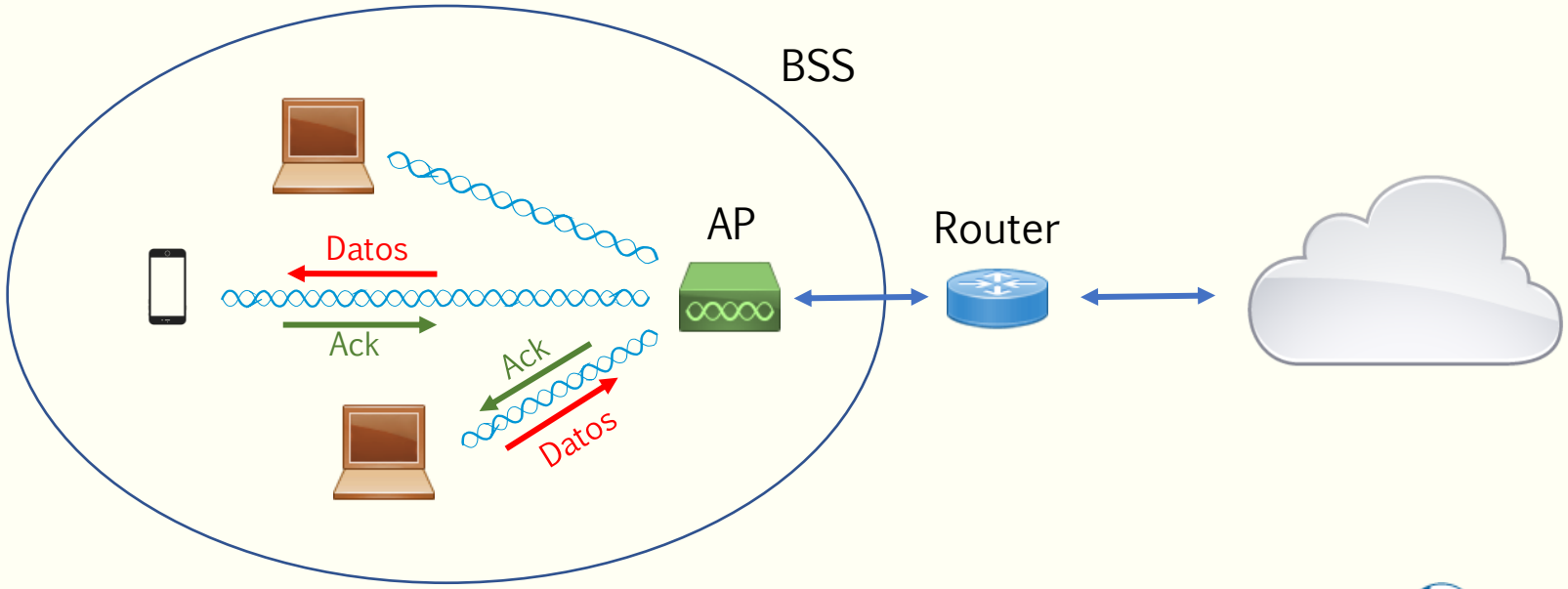
Protocolo MAC en redes 802.11

Se definen tres modos de operación:

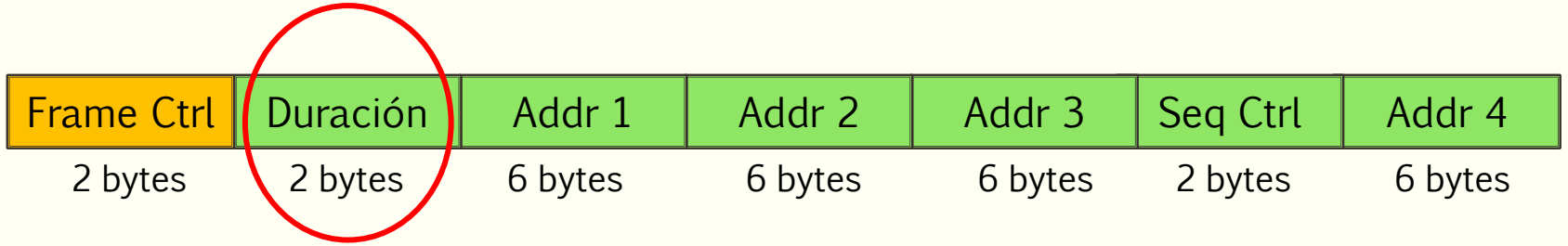
- **DCF (Distributed Coordination Function):** similar a 802.3, no hay un control centralizado de la red. Las estaciones y el AP en el BSS comparten el medio utilizando "CCA – Clear Channel Assesment), en donde para comprobar si el canal está libre utiliza:
  - Detección de energía
  - Carrier Sense o detección de preámbulo
- **PCF (Point Coordination Function)**: se utiliza sólo cuando hay APs. El AP sondea a las estaciones para saber si tienen algo para transmitir. Es opcional en 802.11 y no es muy utilizado.
- **HCF (Hybrid Coordination Function):** agrega funciones de calidad de servicio (QoS). Está establecido en 802.11e

Envío de tramas de datos en 802.11

- Todos los envíos se confirman mediante una trama de ACK.
- Si no reciben el ACK, suponen que hubo colisión.
- Los datos pasan siempre por el AP.
- La celda siempre funciona mediante half-duplex.



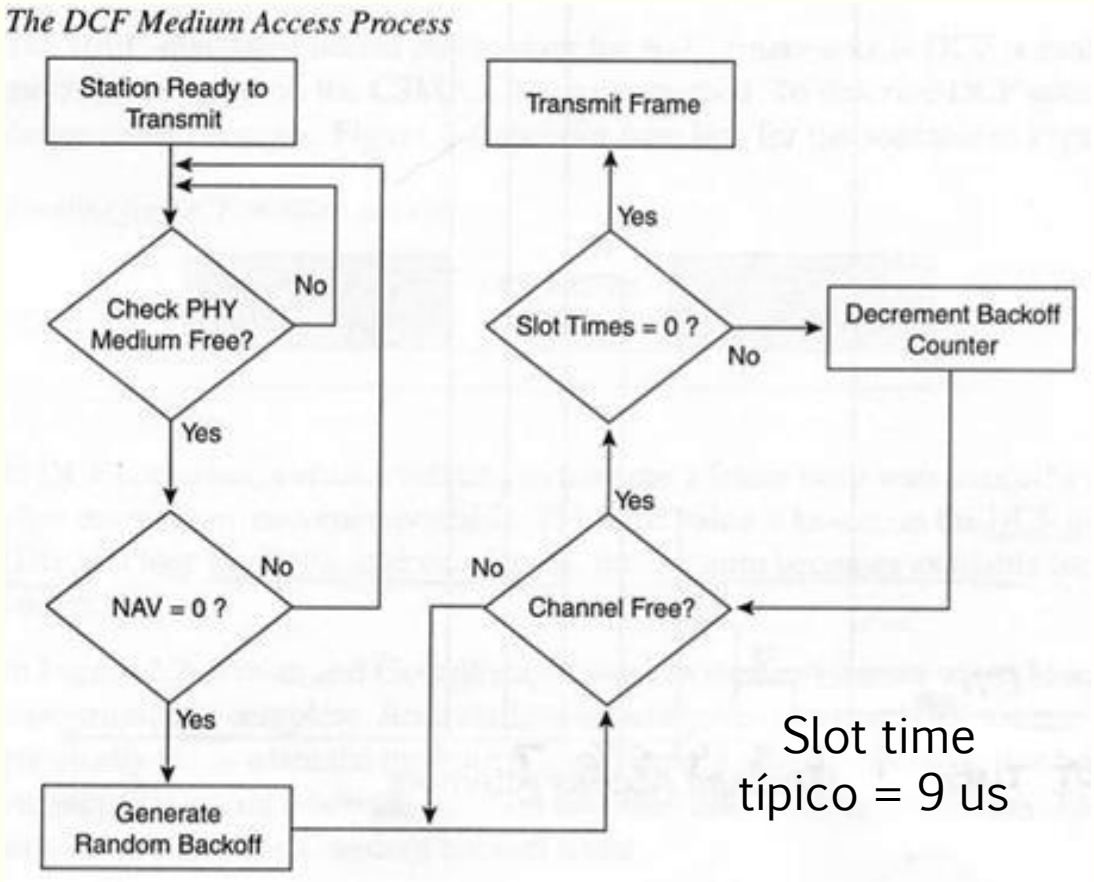
Envío de tramas de datos en 802.11



- El campo Duración indica el tiempo en que estará ocupado el canal transmitiendo la trama.
- Se calcula a partir de la velocidad de transmisión y la longitud de la trama. Se incluye el tiempo aproximado en recibir el ACK.
- Cada estación en la celda mantiene un contador de tiempo, llamado NAV (Network Allocation Vector) que indica el tiempo que falta para que el canal esté libre. Si NAV > 0 , la estación no transmite.

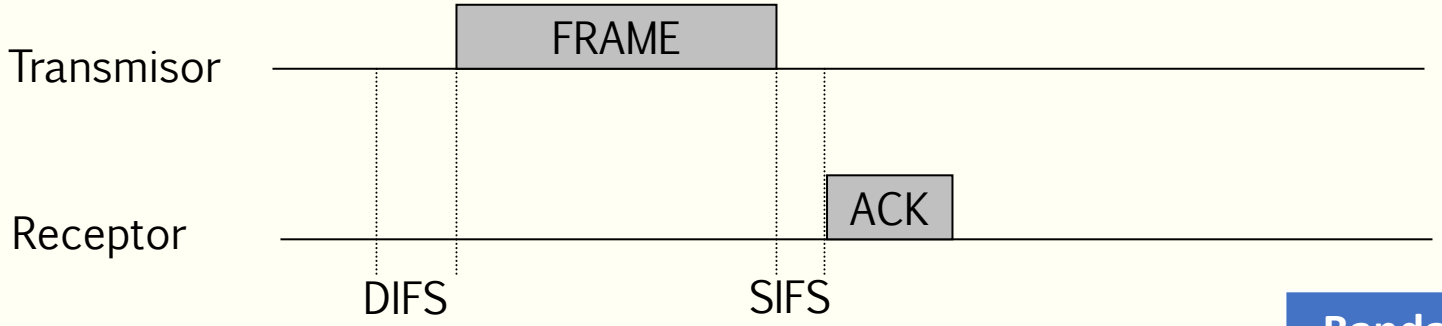
CSMA/CA (CSMA Collision Avoidance)

1) Esperar a que el canal esté libre y el NAV = 0
2) Elegir un número de intervalos aleatorios (Backoff counter) entre 0 y n (n = 31 en 802.11n)
3) Si el canal está libre, esperar un número de intervalos igual a backoff counter. Si está ocupado, se pausa el reloj.
4) Enviar la trama
5) Aguardar el ACK. Si no llega, supone colisión, repite desde el inicio duplicando n (hasta 1023)



CSMA/CA con ACK

- DIFS (DCF Inter Frame Space): tiempo mínimo entre una trama de datos y la siguiente
- SIFS (Short Inter Frame Space): tiempo que separa una trama de datos de su ACK
- Si el emisor no recibe el ACK, considera que no hubo éxito en la transmisión, aguarda EIFS (Extended Interframe Space) y activa el algoritmo de backoff.

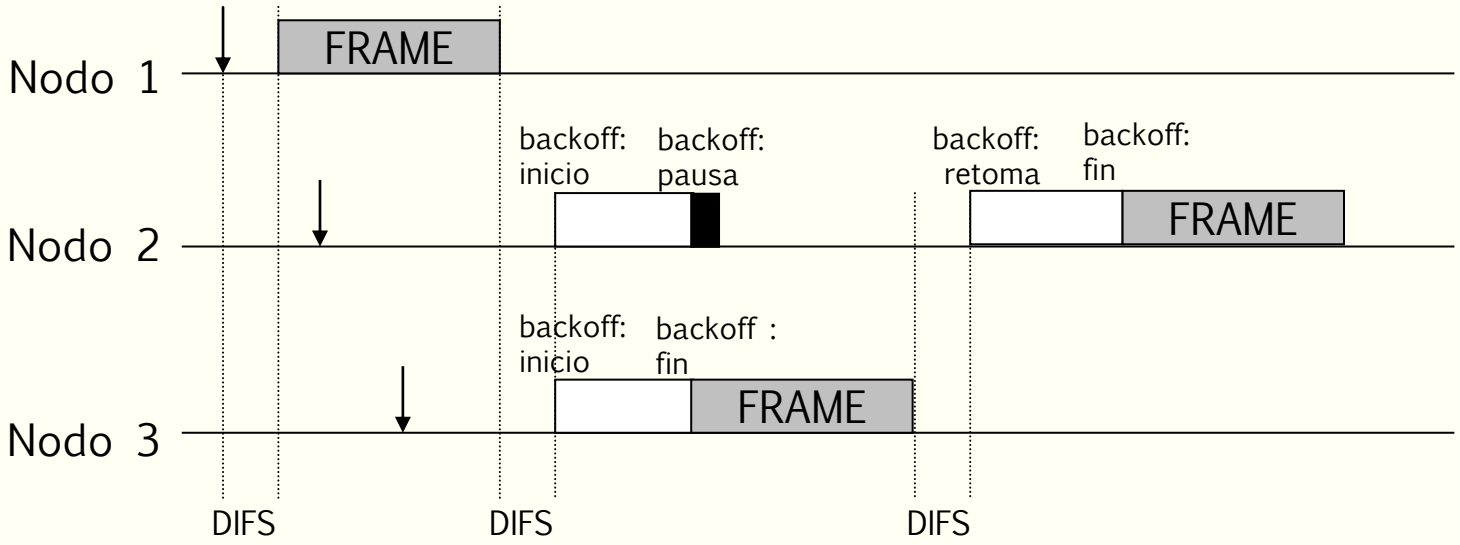


Banda	SIFS	DIFS
2.4 GHz	10 us	50 us
5 GHz	16 us	34 us

Implementación de CSMA/CA - Backoff

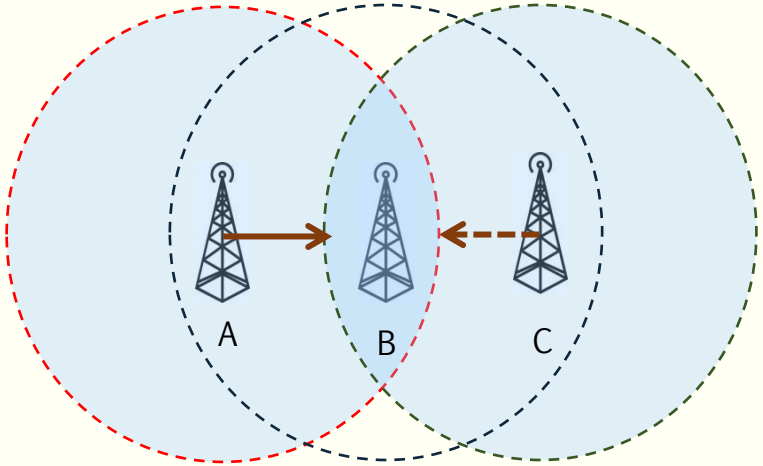
- Un intervalo aleatorio (Backoff time) se selecciona y activa el temporizador

- El temporizador:
  - Decrece mientras el canal está libre
  - Entra en pausa al detectar una transmisión
  - Se reactiva al liberarse el canal

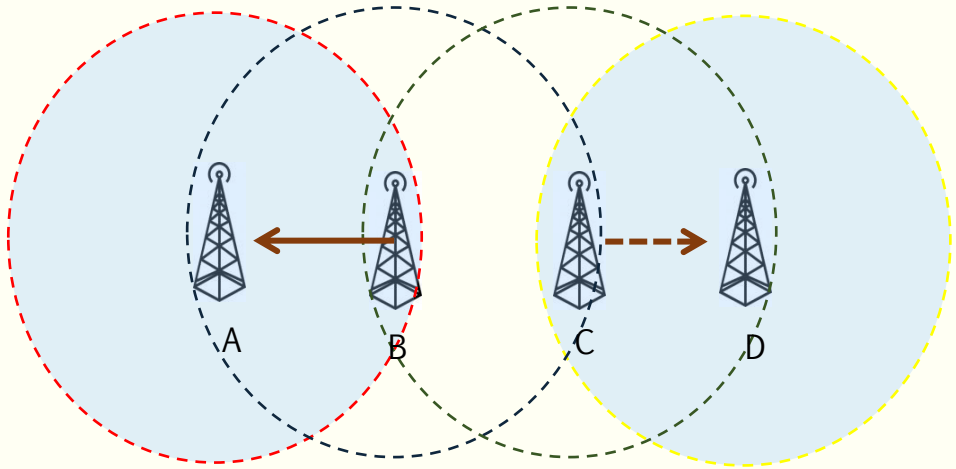


- Cuando el temporizador llega a 0, intenta transmitir

Nodo oculto / expuesto



La estación A transmite a B.
La estación C no escucha a A, por lo que empieza a transmitir, y genera colisión.



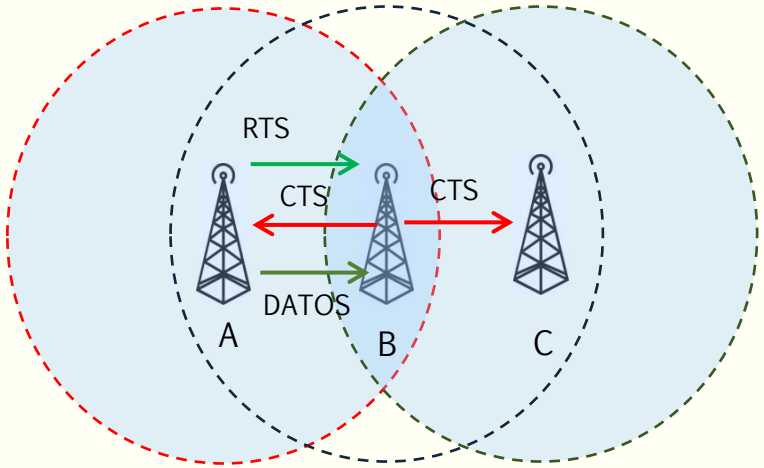
La estación B transmite a A.
La estación C necesita comunicarse con D, pero no lo hace porque ve el canal ocupado (aunque no habría interferencia ni en A ni en D).

MACA: Multiple Access Collision Avoid

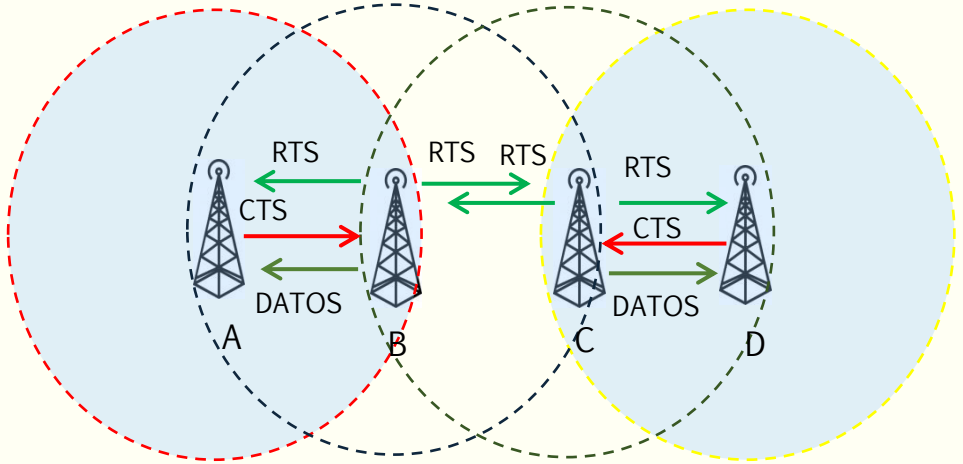
- Antes de transmitir, el emisor envía una trama RTS (Request to Send), indicando longitud de datos a enviar
- El receptor contesta con una trama CTS (Clear to Send), copiando la longitud
- Al recibir el CTS, el emisor envía sus datos

- Al ver un RTS, esperar al CTS
- Al ver un CTS, esperar según la longitud

Nodo oculto / expuesto: solución con MACA

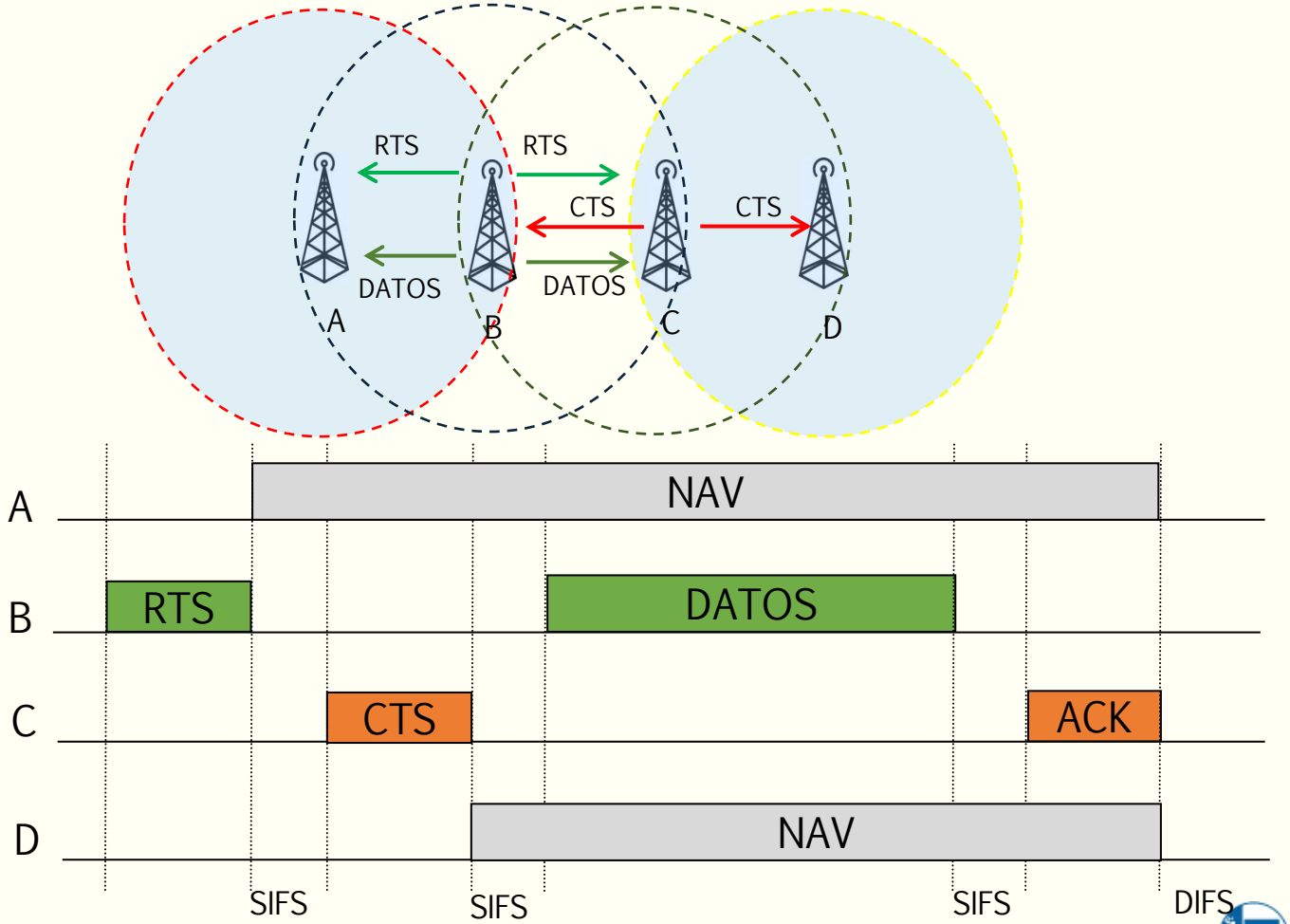


La estación A transmite a B un RTS.
La estación B responde con un CTS que escucha C, por lo que C actualiza su NAV y no transmite.



La estación B transmite a A un RTS.
La estación A responde con un CTS, pero C no lo escucha, por lo que C envía su RTS para poder comunicarse con D.

MACA: Multiple Access Collision Avoid



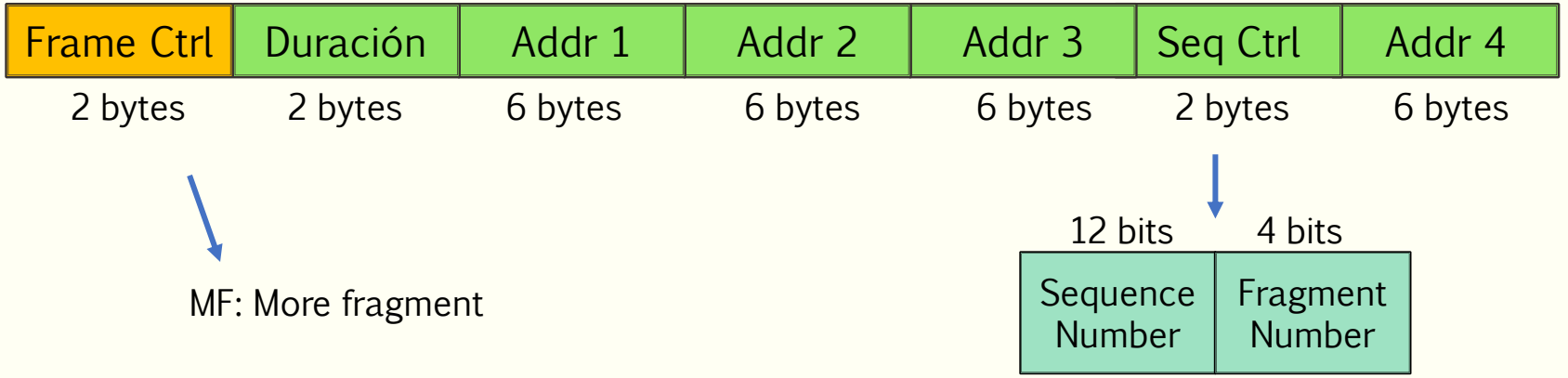
RTS/CTS: Ventajas y desventajas

- Ventajas:
  - Se reducen las colisiones en los casos de la estación (nodo) oculta
- Desventajas:
  - Aumenta la latencia (se suma el tiempo de los RTS/CTS)
  - Disminución del rendimiento (throughput): hay mas mensajes de control. Esto afecta particularmente a las tramas cortas

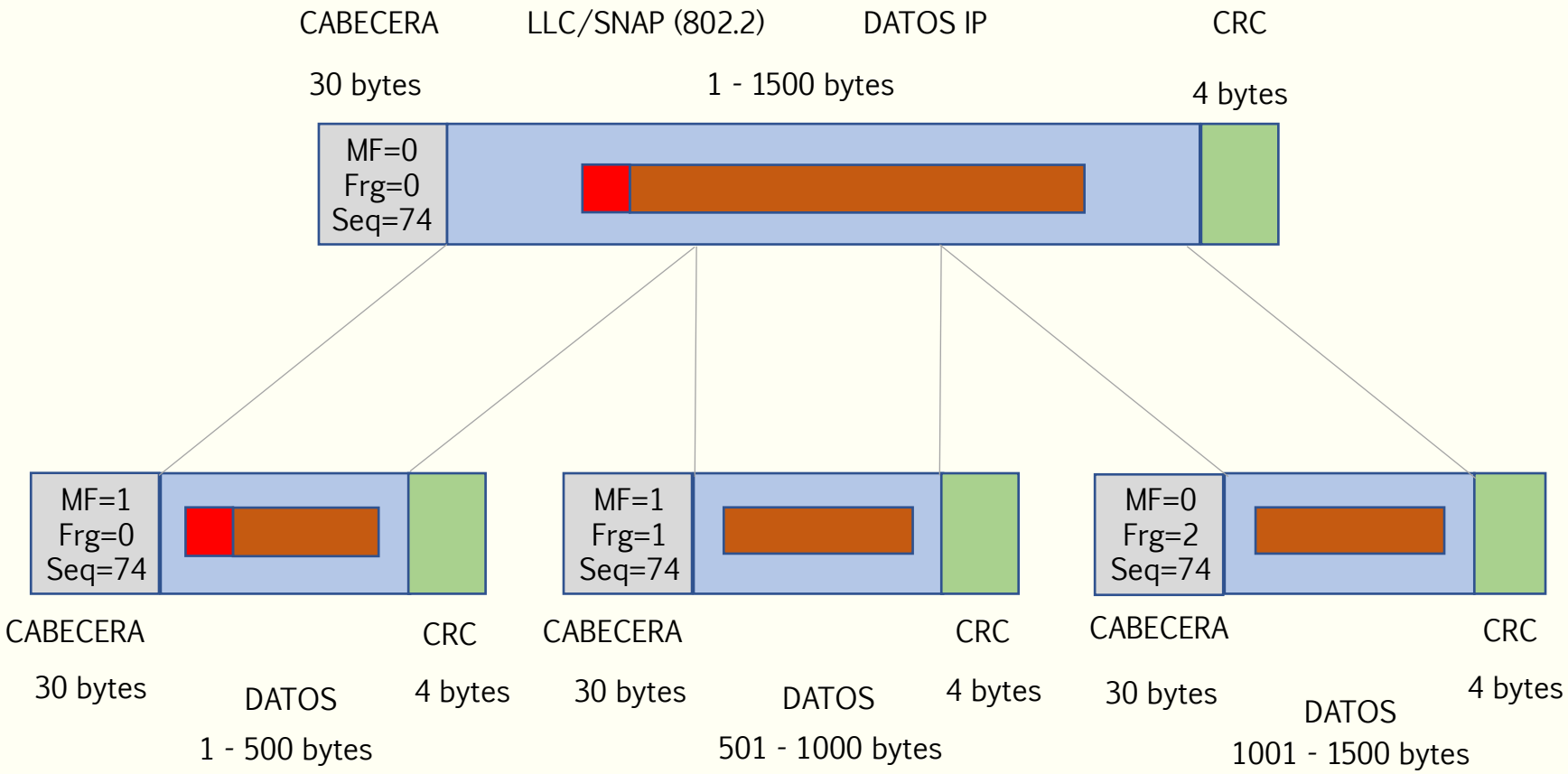
- Se puede configurar el umbral del largo de la longitud de la trama a partir del cual se utiliza RTS/CTS

Fragmentación

- Para reducir la probabilidad de error, se prevé la fragmentación.
- Por cada fragmento, existe un ACK.
- Reduce la eficiencia, pero permite enviar datos cuando hay una tasa de error elevada.
- La fragmentación se hace a nivel de enlace.
- Los paquetes multicast y broadcast no se fragmentan nunca.

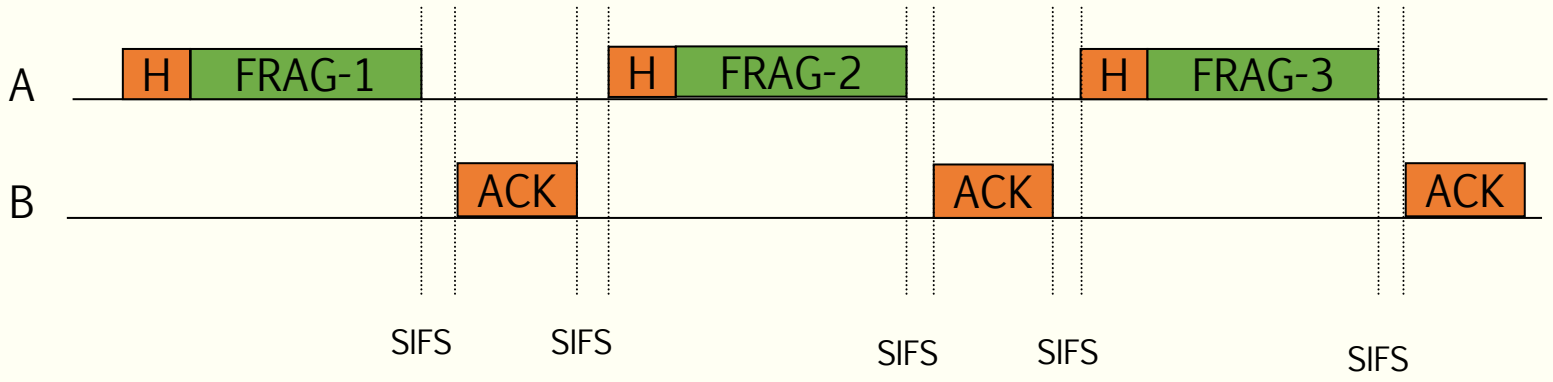


Fragmentación



Fragmentación

- Cada fragmento necesita su ACK
- La separación entre el fragmento y el ACK es de un SIFS (10 us)
- En caso de tener que reenviar un fragmento, se debe esperar un DIFS y utilizar CSMA/CA
- Puede combinarse con RTS/CTS

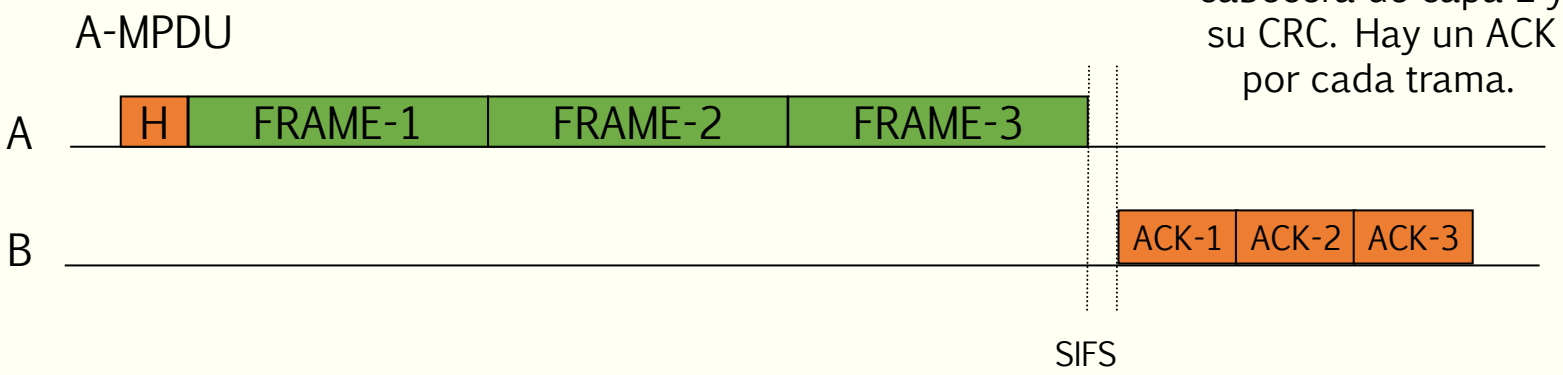


Mejoras

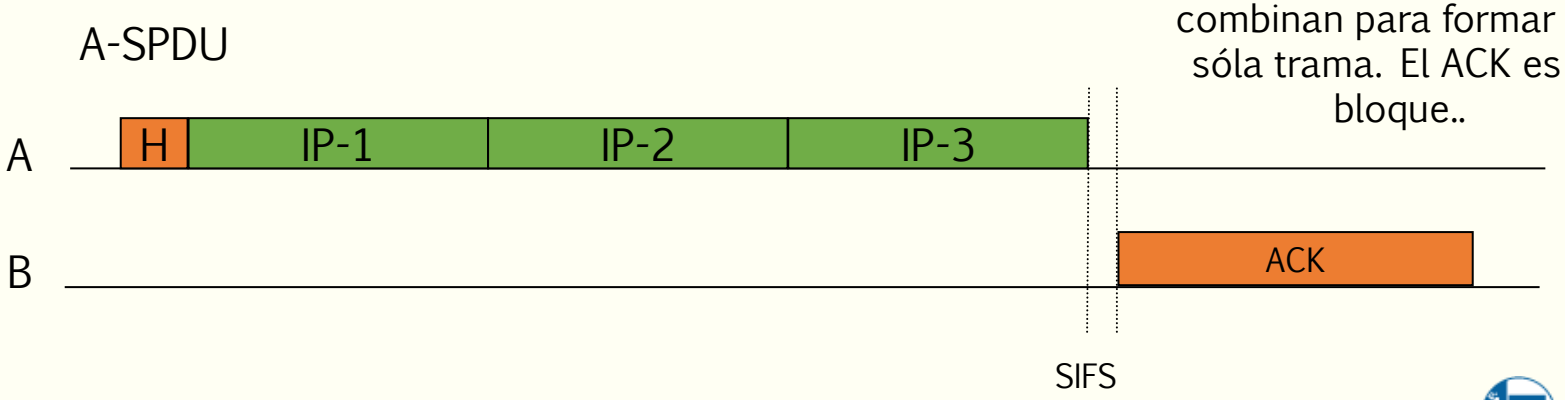
- 802.11e mejora el rendimiento incorporando:
  - Posibilidad de envío de ráfagas (tramas separadas por SIFS)
  - Posibilidad de un solo ACK para confirmar toda la ráfaga (reenvío selectivo de hasta 64 tramas)
- 802.11n mejora el rendimiento a través de agregación de tramas:
  - Envía varias tramas MAC en una misma trama (A-MPDU, Aggregate MAC Protocol Data Unit). El método permite reenvío selectivo. Soporta hasta 65.535 bytes
  - Envía varios paquetes (capa 3) en la carga útil de una trama MAC (A-MSDU, Aggregate, MAC Service Data Unit). No admite reenvó selectivo. Soporta hasta 7.935 bytes.
- 802.11ac utiliza A-MPDU

Mejoras

Cada trama lleva su cabecera de capa 2 y su CRC. Hay un ACK por cada trama.



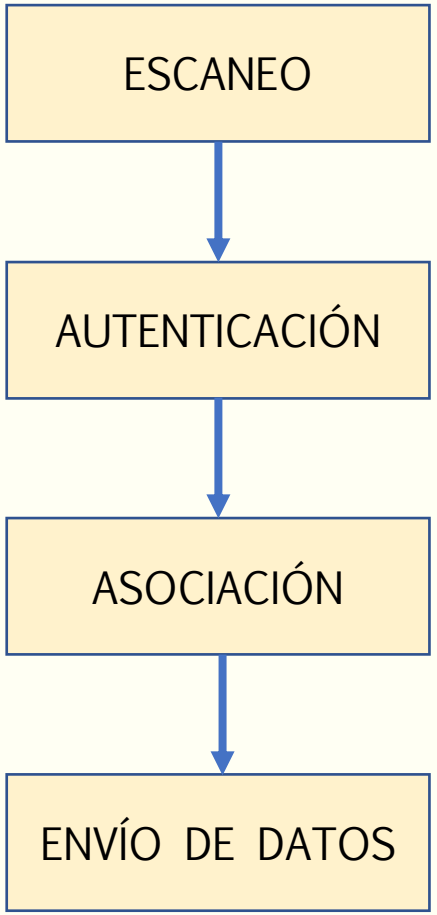
Los datos de capa 3 se combinan para formar una sóla trama. El ACK es en bloque..



REDES INALÁMBRICAS

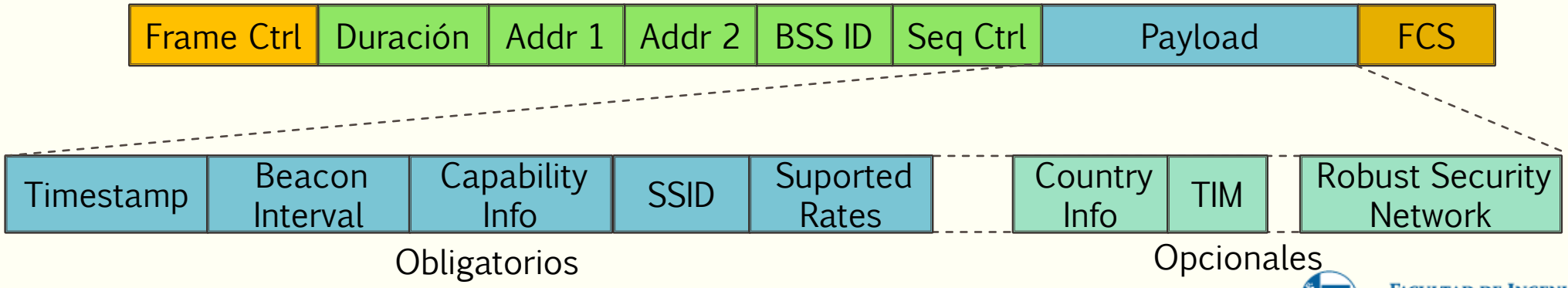
- Introducción
- Nivel físico
- Topología
- Nivel MAC
- **Conectividad en redes 802,11**

Fases de una conexión en 802.11



Escaneo

- El AP envía una trama de gestión, llamada baliza (beacon), periódicamente, típicamente 10 veces por segundo
- La baliza incluye:
  - Identificador de red ESSID o SSID
  - Tasas soportadas
  - Intervalo entre balizas
  - TIM (Traffic Indication Map)
- La baliza viaja sin encriptar, aunque se puede ocultar (SSID oculto)



Escaneo

- Búsqueda pasiva:
  - El terminal escanea canales y escucha balizas
  - Al recibir baliza con SSID intenta unirse al AP
  - Si recibe el mismo SSID de distintas balizas, elige la de mayor potencia o calidad de señal (menor tasa de error)
- Búsqueda activa:
  - El terminal envía baliza sonda (probe request). Un AP está obligado a responder con un "probe response" si:
    - El probe request corresponde con el SSID del AP
    - El probe request contiene un SSID = 0 (SSID broadcast)
  - Los AP que la oigan, responderán
  - El terminal elige a quien asociarse
  - La frecuencia de escaneo puede configurarse en la interfaz, y es útil para la itinerancia

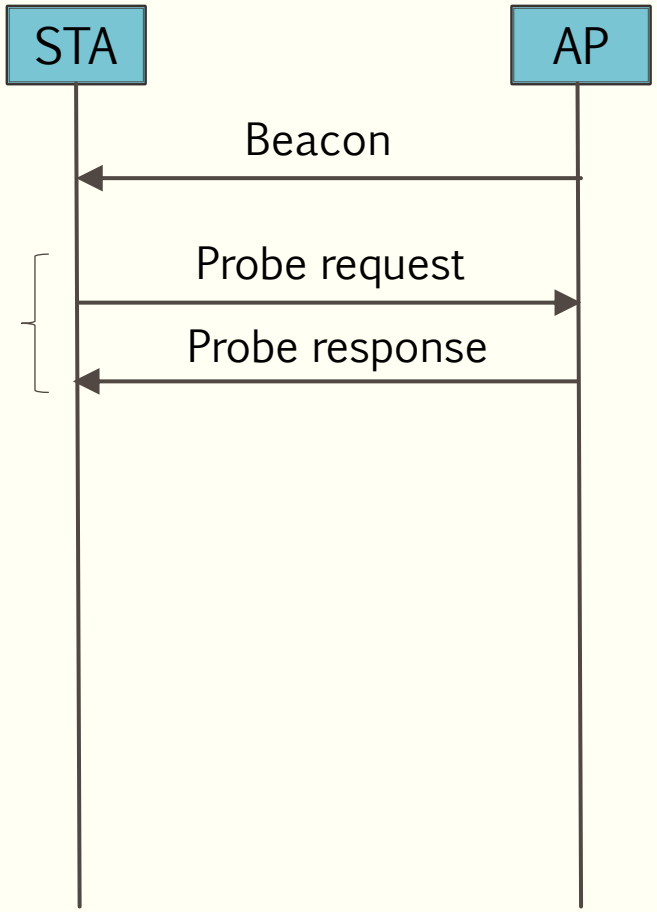


Diagrama de estados de transición

STATE 1

Desautenticado y desacociado

Tramas de clase 1: RTS, CTS, ACK, Probe Request, Probe Response, Beacon, Autenticación, Desautenticación

Autenticación

- La autenticación de enlace es el primer paso para conectar a una BSS
- IEEE 802.11-2012 define dos tipos de autenticación 802.11:
  - Open System: se utiliza en conjunto con otros métodos mas avanzados; intercambio de saludos
  - Shared Key: utiliza WEP (Wired Equivalent Privacy); se lo considera obsoleto

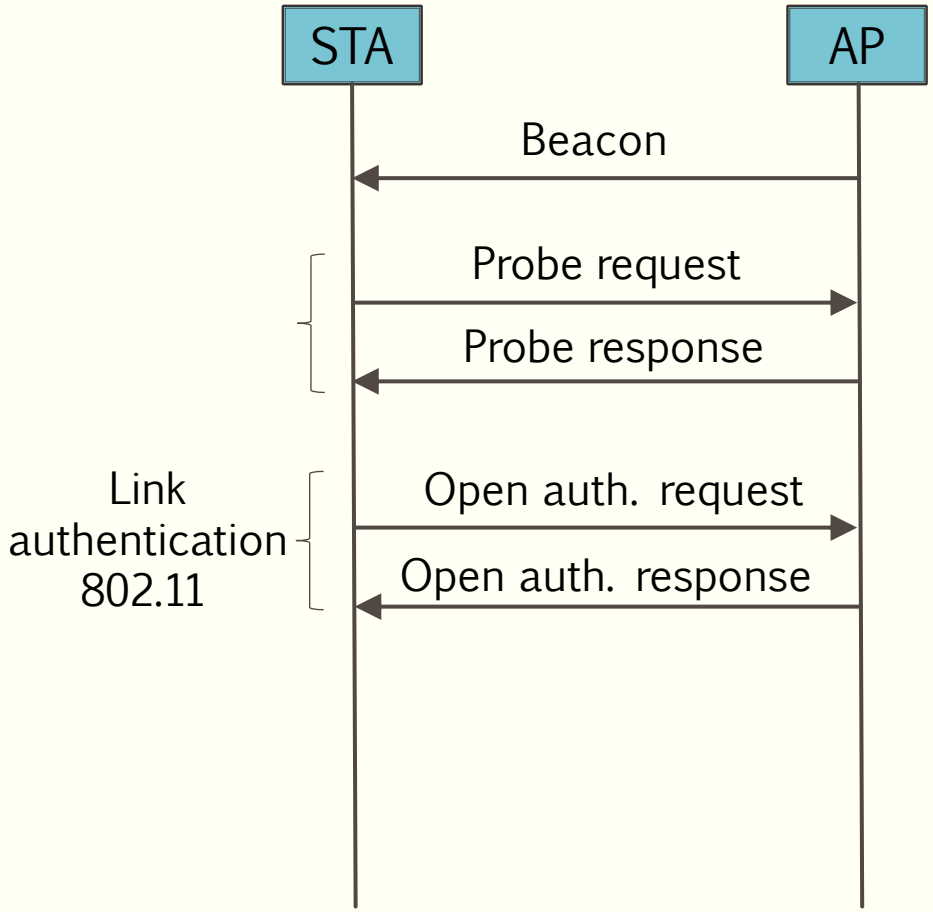
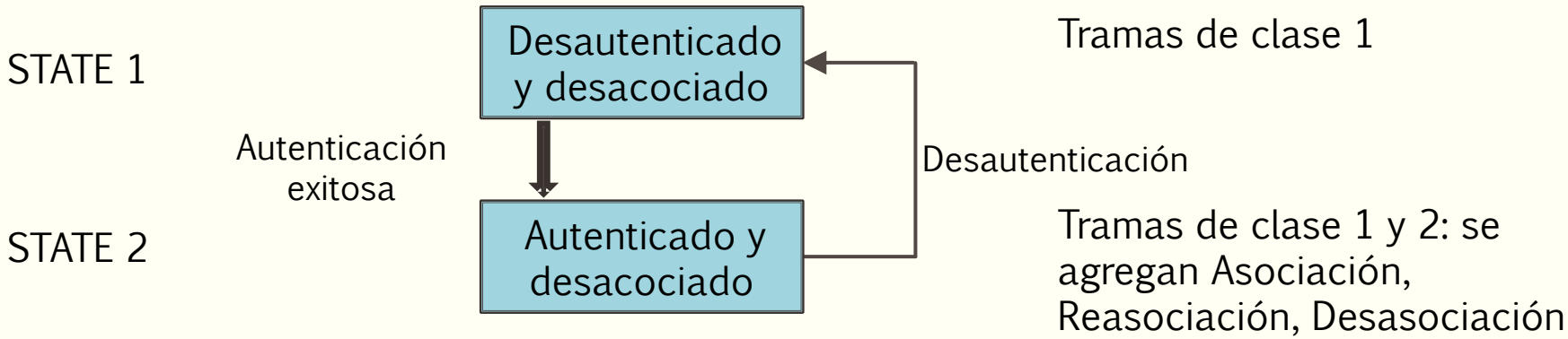


Diagrama de estados de transición



Asociación

- Cuando la estación encuentra una red compatible, intenta asociarse a ella
- La estación indica el tipo de red al que quiere asociarse, el SSID, las velocidades soportadas y el intervalo en el que escuchará las balizas
- La autenticación se hace con un SSID, la asociación con un BSSID
- Si una estación cambia de AP por itinerancia, debe reasociarse, pero no reautenticarse.

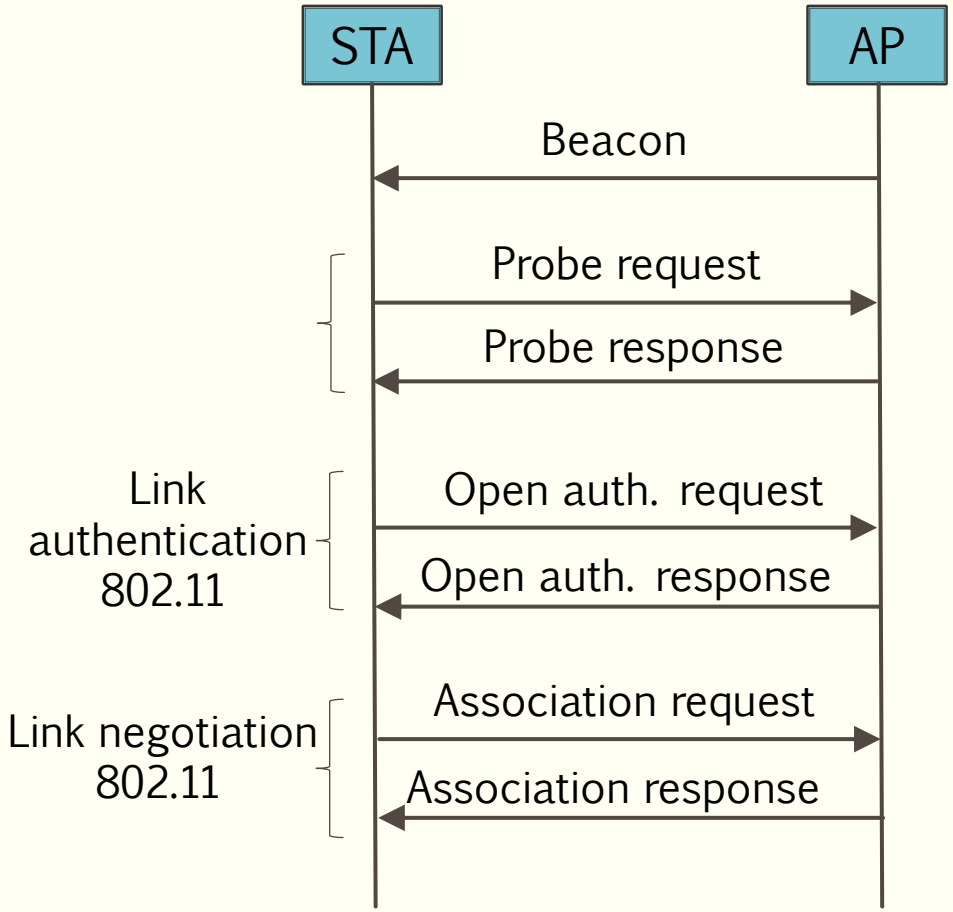
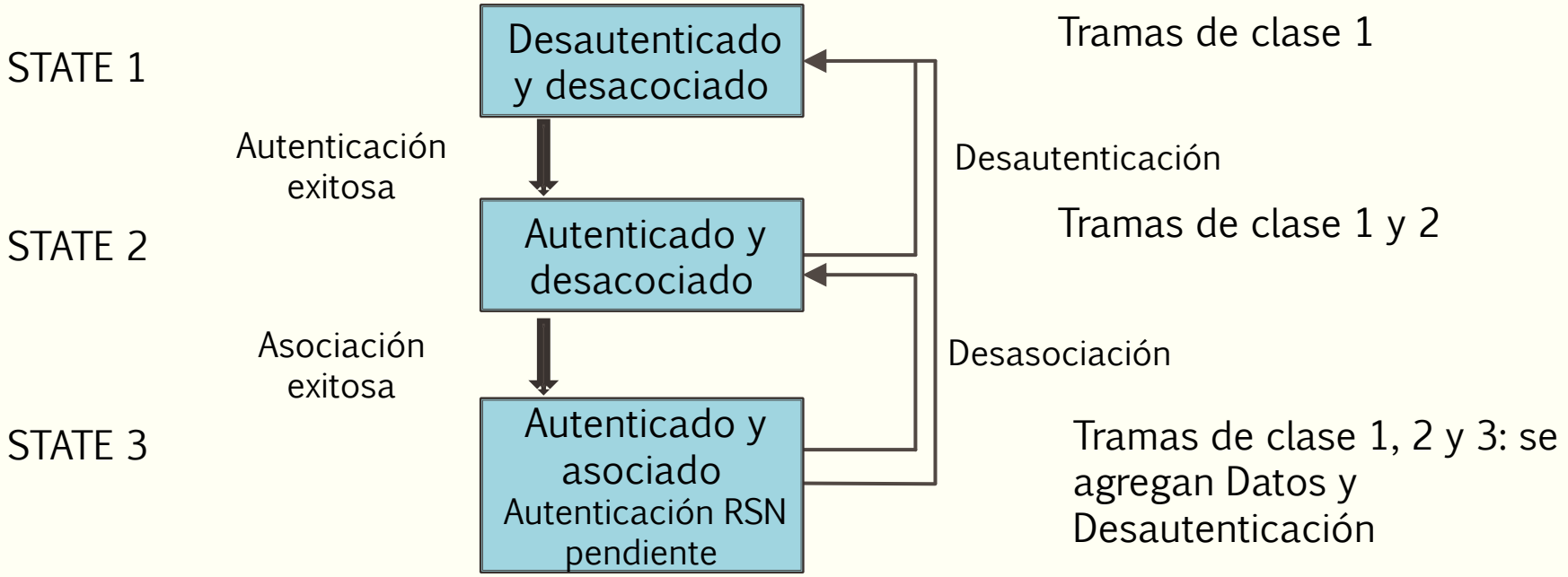


Diagrama de estados de transición



RSN: Robust Security Network

Autenticado y asociado

- Para llegar al último estado se debe cumplimentar un proceso llamado “4 Way Handshake”
- Se generan las llaves de encriptación dinámicas para proteger los datos
- En 2004 la WiFi Alliance diseñó el protocolo WAP: utiliza una clave compartida (PSK) y TKIP para encriptar
- Con 802.i surgió WAP2, utiliza AES (Advance Encryptation System) para encriptar
- A nivel empresarial: 802.1X/EAP (Extensible Authentication Protocol)

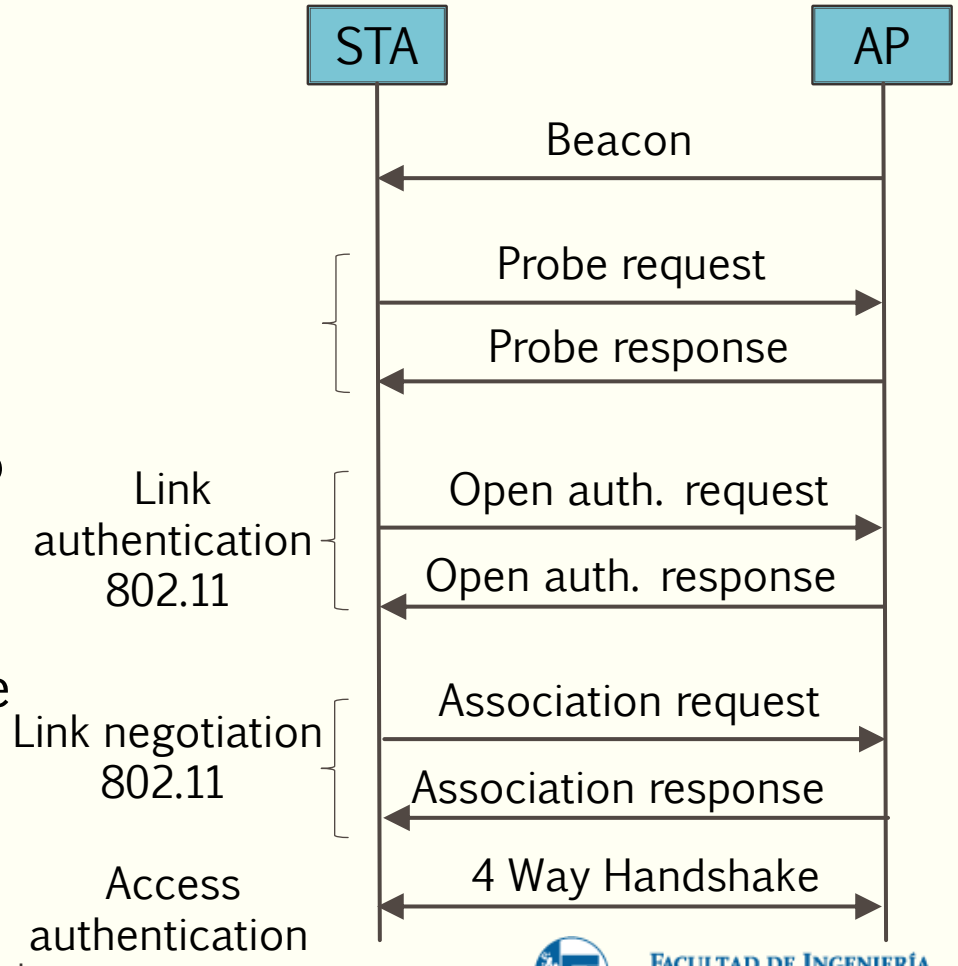
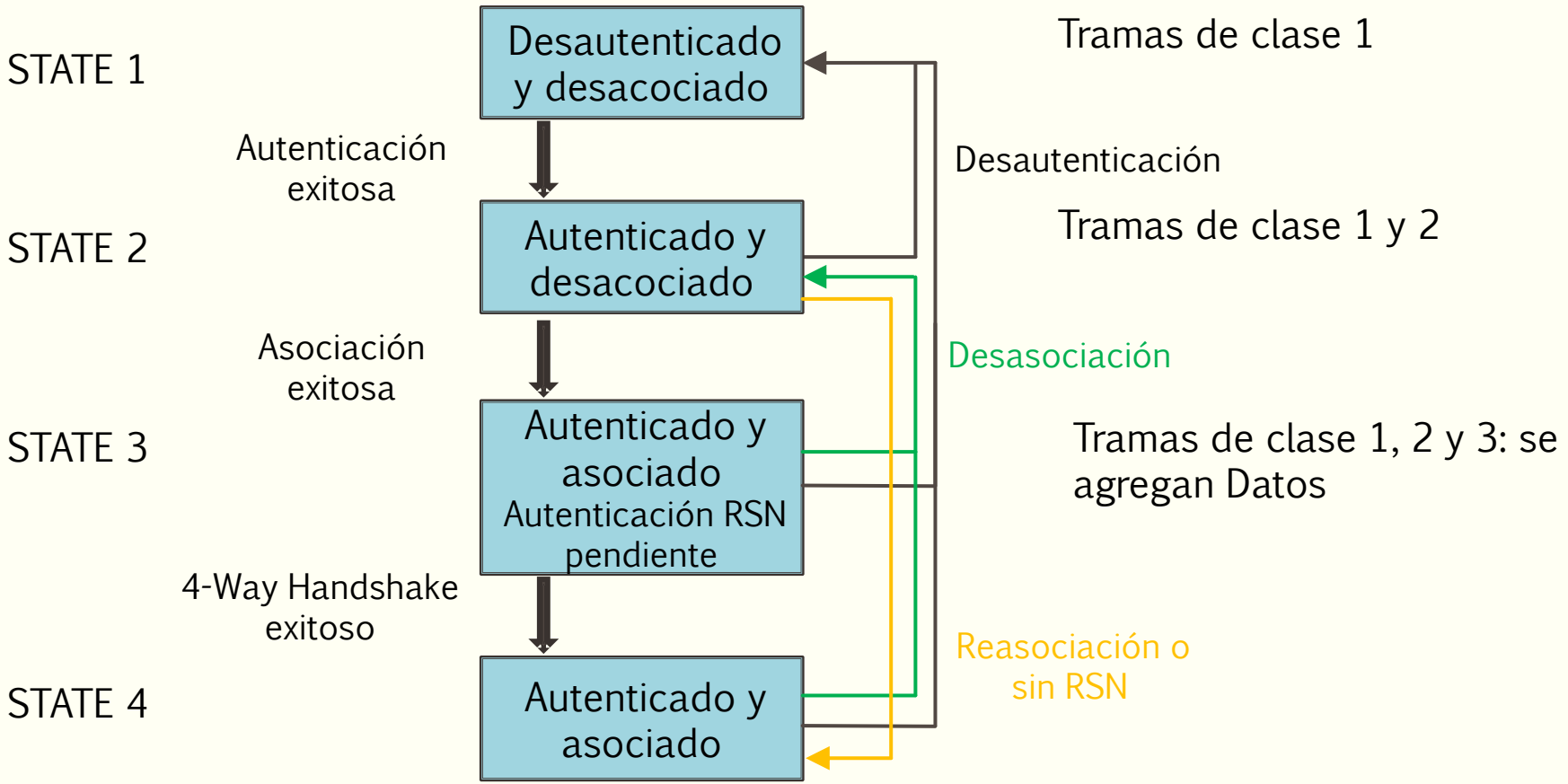


Diagrama de estados de transición

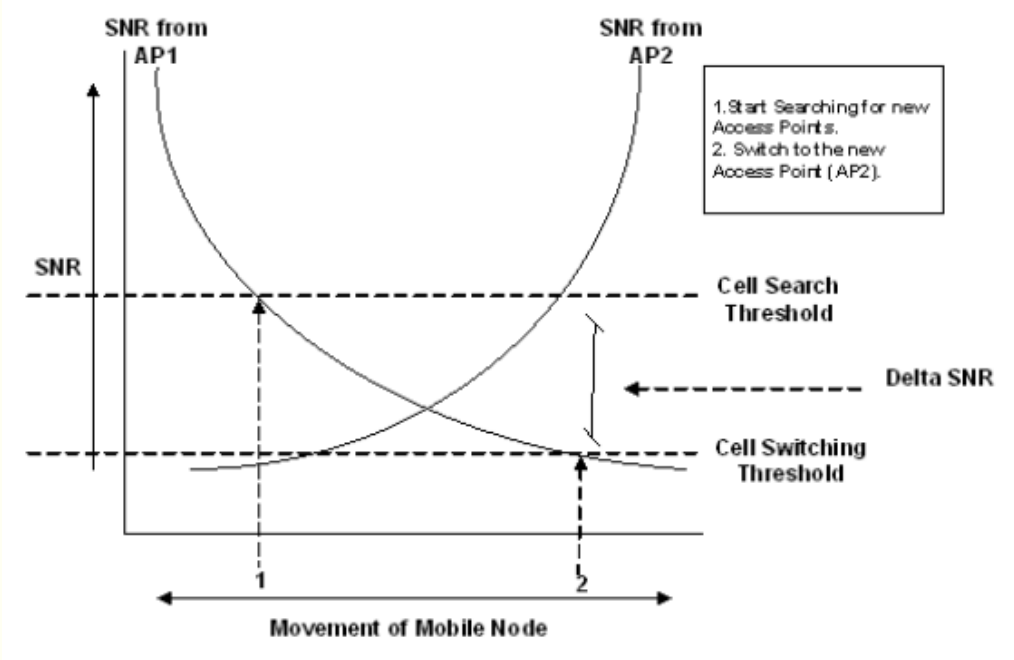


Itinerancia (roaming)

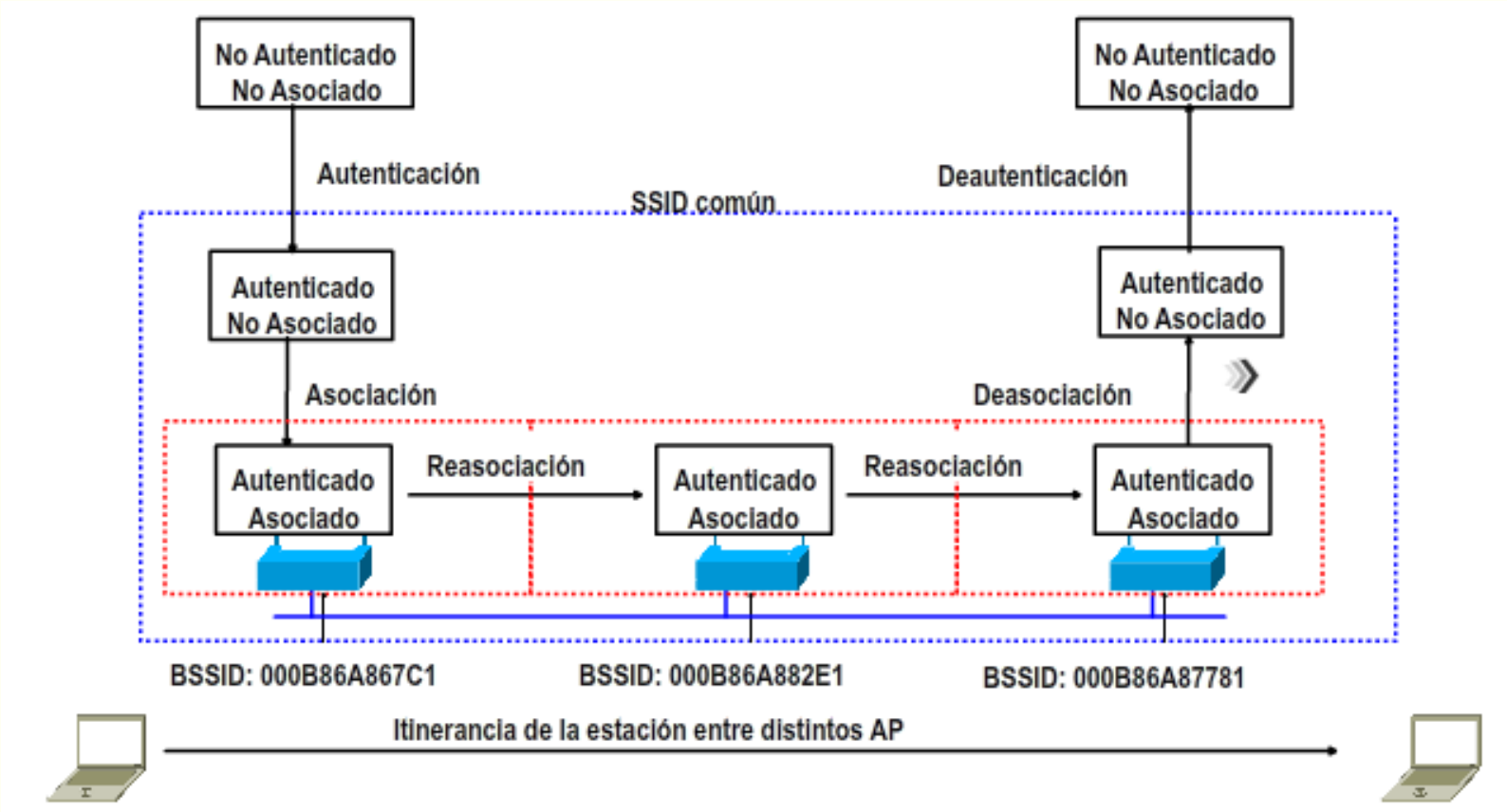
- Cada estación se conecta a un único BSS.
- Si la estación se mueve entre dos AP que tienen el mismo SSID, deberá desasociarse del primero y asociarse al segundo (reasociación).
- La decisión es de la estación, en base a:
  - Potencia recibida de cada AP
  - Tasa de error (estimada por las retransmisiones)
  - Beacons recibidos
  - Evolución de la velocidad de la conexión
  - Relación S/N (si está disponible)
- Al reasociarse, los APs se transfieren los datos pendientes de la estación

Itinerancia (roaming)

- Cuando la SNR cae por debajo de un umbral “Cell Search”, comienza a buscar otros AP
- Cuando la SNR cae por debajo del umbral “Cell Switching”, conmuta de AP



Itinerancia (roaming)



Ahorro de energía

- El objetivo es ahorrar energía en estaciones que generalmente están alimentadas por baterías.
- Las estaciones pueden adoptar un modo limitado de potencia (standby), en donde no escuchan las tramas: están “dormidas”.
- La estación le debe avisar al AP que va a trabajar de este modo.
- Periódicamente, se “despiertan” y escuchan el siguiente beacon. Hay un campo en el beacon llamado TIM (Traffic Indication Map) en el que el AP avisa acerca de que estaciones tienen tramas pendientes. Si hay algo para ella, la estación le solicitará al AP que se lo envíe (trama PS-Poll).
- Si la estación no aparece en el TIM, puede volver a “dormirse” a no ser de que tenga algo para enviar.

Redes inalámbricas

- 802.11: 1-2 Mbps
- 802.11a: 54 Mbps en la banda de 6 GHz --- WiFi 1 (no oficial)
- 802.11b: 11 Mbps en la banda de 2.4 GHz --- WiFi 2 (no oficial)
- 802.11d: Internacionalización del estándar
- 802.11e: Gestión de QoS
- 802.11f: Itinerancia en equipos de diferentes fabricantes
- 802.11g: 54Mbps en la banda de 2,4 GHz --- WiFi 3 (no oficial)
- 802.11h: Control de potencia en 5 GHz
- 802.11i: Seguridad (TKIP, AES)
- 802.11n: Hasta 600 Mbps en bandas de 2.4 y 5 GHz (MIMO) --- WiFi 4
- 802.11s: Redes malladas
- 802.11ac: hasta 1.3 Gbps en la banda de 5 GHz (256 QAM, 3 MIMO) --- WiFi 5
- 802.11ad hasta 6.9 Gpbs en bandas de 2.4, 5 y 60 GHz (WiGig)
- 802.11ah: ultra bajo consumo, en la banda de 900 MHz. IoT
- 802.11ax: hasta 9,6 Gbps en bandas de 2.4, 5 y 6 GHz (1024 QAM, 8 MIMO) --- WiFi 6