

# T2 – Redes Locales Inalámbricas

WLAN (Wireless Local Area Network)  
(Red de Área local inalámbrica)

"Red que permite conectar dispositivos entre sí y a Internet sin cables, utilizando señales de radio frecuencia (Ej: WiFi - Bluetooth, etc.)

Redes de Comunicaciones Móviles

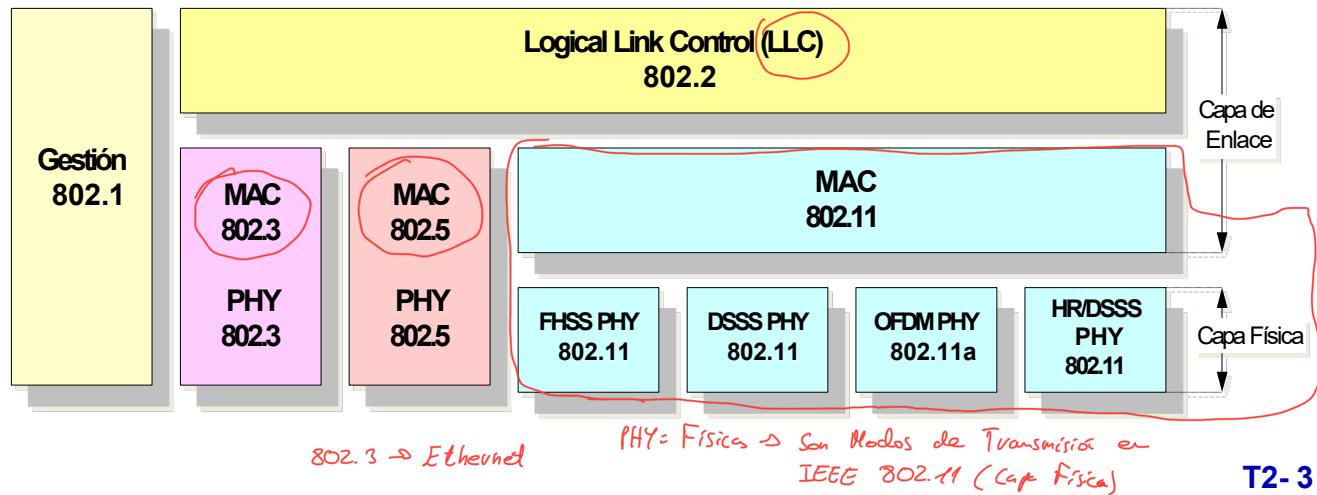
# Índice

- *Introducción a las WLAN*
- *Arquitectura IEEE 802.11*
  - *Capa física*
  - *Capa MAC*
- *Seguridad en IEEE 802.11*
- *Calidad de servicio IEEE 802.11*
- *Redes mesh*

# Introducción a las WLAN

IEEE802 → se encarga de las redes inalámbricas

- IEEE802.11 pertenece a la familia IEEE802, que especifica tecnologías de redes locales inalámbricas
  - <http://standards.ieee.org/about/get/802/802.11.html>
  - [http://www.ieee802.org/11/Reports/802.11\\_Timelines.htm](http://www.ieee802.org/11/Reports/802.11_Timelines.htm)
- Todas las redes 802 tienen elementos físicos y MAC



# Introducción a las WLAN

## Futuro de WiFi

- *Según estimaciones de Wi-Fi Alliance, en 2022 se utilizarán casi 18.000 millones de dispositivos con Wi-Fi*
- *El valor económico global de Wi-Fi está estimado en 3,3 billones de dólares en 2021 y se espera que para 2025 sea de 4,9 billones de dólares.*
- *Wifi también está convirtiendo a sus usuarios en enérgicos demandantes de una conexión más eficiente, confiable y segura, ante escenarios de trabajo híbrido o remoto, de sistemas de conectividad complejos en el hogar y las empresas y de la Internet de las cosas (IoT).*

# Introducción a las WLAN

## Futuro de WiFi

- *Existen mercados donde la tecnología WiFi no se ha desplegado ampliamente:*
  - *Se estima que 244 millones de personas en América Latina, un tercio de la población, no tienen acceso a Internet, según un estudio de 2021 del Instituto Interamericano de Cooperación para la Agricultura (IICA), Banco Interamericano de Desarrollo (BID) y Microsoft.*
  - *Habrá un crecimiento diez veces mayor en la demanda de fuentes wifi en los próximos 10 años, por lo que estamos viendo un despliegue creciente de wifi"*

# Introducción a las WLAN

## Ventajas

- No reemplazan soluciones “cableadas”, LAS COMPLEMENTAN
  - Proporcionan conectividad de red en áreas en las que es complicado establecer una red cableada (lugares de trabajo temporales, zonas de ocio, ...)
- Las redes de área local inalámbricas suponen una valiosa oportunidad de negocio para distintos sectores (aumento de productividad en servicios turísticos, museos, hoteles, ...)
- Aportan un mercado sustancial para aplicaciones de interiores (audio guías, hostelería, ...)
- Flexibilidad y facilidad de instalación

# Introducción a las WLAN

## Desventajas

- *Tasas de transmisión no son muy elevadas → Mejoran con el desarrollo de nuevos estándares*
- *Área de cobertura limitada*
- ***Bandas no licenciadas***
  - 2400 a 2500 MHz (*frecuencia central 2450 MHz*) *Microwands, Bluetooth, WiFi, etc.*
  - 5725 a 5875 MHz (*frecuencia central 5800 MHz*) *wi-fi 6E*
  - 5945 a 6425 Mhz (*frecuencia central 6185 Mhz*) *BOE 24/12/2021*
  - 24,00 a 24,25 GHz (*frecuencia central 24,125 GHz*)
  - 61,00 a 61,50 GHz (*frecuencia central 61,250 GHz*)
- *Seguridad → protocolos débiles*

# Introducción a las WLAN

Estandarización IEEE 802.11

Año	Estándar	Certificado	Bandas			Velocidad			
			2,4	5	6	Modulación	Ancho canal	Flujos MIMO	Máximo
1997	802.11		✓			DQPSK	22MHz	1	2Mb
1999	802.11a			✓		64-QAM	20MHz	1	54Mb
→ 1999	802.11b		✓			QPSK	22MHz	1	11Mb
→ 2003	802.11g		✓			64-QAM	20MHz	1	54Mb
→ 2007	802.11n	WiFi 4	✓	✓		64-QAM	40MHz	4	600Mb
→ 2013	802.11ac	WiFi 5, Wave 2	✓			256-QAM	160MHz	8	6,9Gb
→ 2021	802.11ax	WiFi 6, E, Release 2	✓	✓	✓	1024-QAM	160MHz	8	9,6Gb
→ 2024	802.11be	WiFi 7	✓	✓	✓	4096-QAM	320MHz	16	46Gb

WiFi 6 → 2,4 y 5GHz } Release 2  
 WiFi 6E → 2,4, 5 y 6 GHz }

# Introducción a las WLAN

Estandarización IEEE 802.11

	WiFi 4	WiFi 5	WiFi 6	WiFi 6E	WiFi 7
<b>Lanzamiento</b>	2007	2013	2019	2021	2024
<b>Estándar IEEE 802.11</b>	n	ac	ax		be
<b>Bandas</b>	2,4 y 5GHz	5GHz	2,4 y 5GHz	6GHz	2,4; 5 y 6GHz
<b>Ancho de canal</b>	40MHz	160MHz			320MHz
<b>Antenas MIMO</b>	4		8		16
<b>Modulación</b>	64-QAM	256-QAM	1024-QAM		4096-QAM
<b>Velocidad</b>	1,2Gb	3,5Gb	9,6Gb		46,1Gb
<b>Seguridad</b>	WPA2		WPA3		

Comparativa de características de WiFi 6 vs. WiFi 7

# Introducción a las WLAN

Estandarización IEEE 802.11



Banda 2,4 GHz → 2400 MHz - 2500 MHz

Banda 5 GHz → 5150 MHz - 5850 MHz

Banda 6 GHz → 5925 MHz - 6425 MHz

# Introducción a las WLAN

Estandarización IEEE 802.11

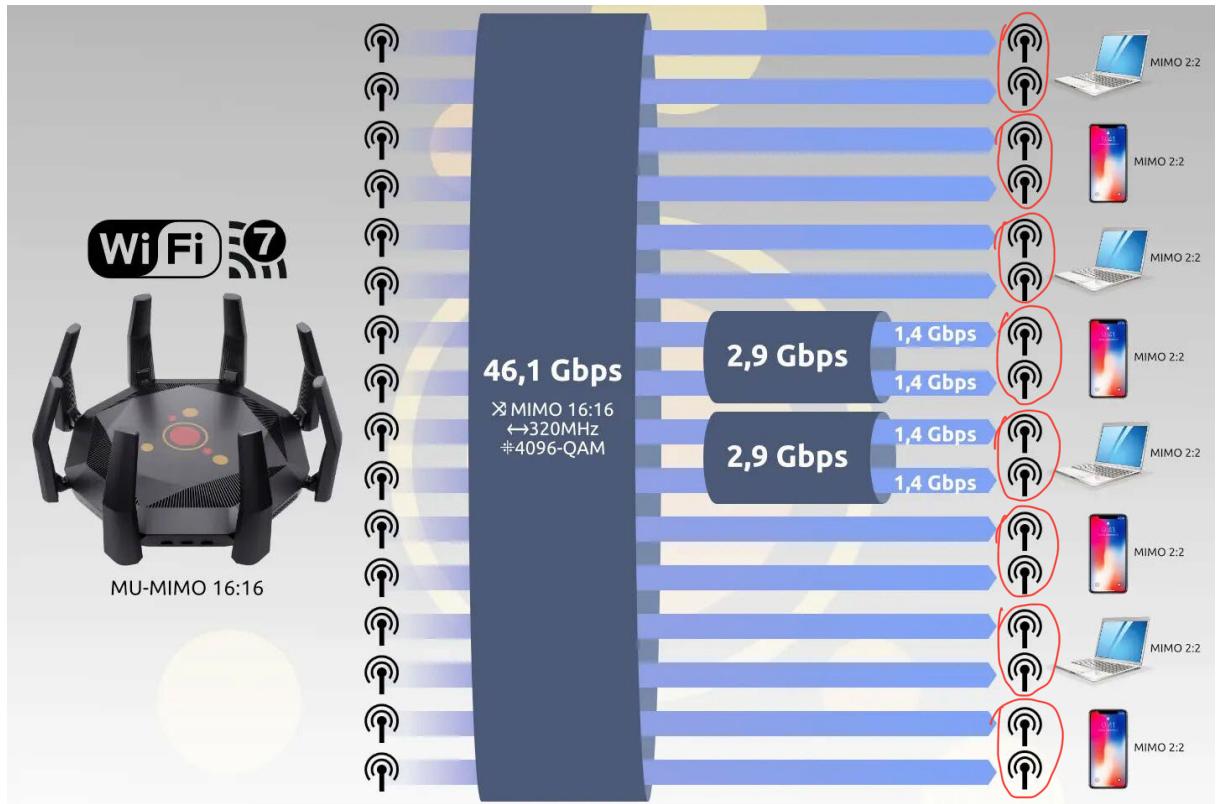
MIMO, sistema que utiliza varias antenas para enviar en paralelo varios flujos de datos utilizando el mismo espectro. En WiFi 7 duplica la cantidad máxima a 16, lo que directamente duplica el caudal respecto a las 8 antenas de WiFi 6. Aunque los clientes usan habitualmente solo dos flujos, podremos ver routers WiFi 7 con nada menos que 16 antenas en cada banda.

MIMO (Multiple Entrada, Multiple Salida) → En lugar de usar una sola antena transmisora y otra receptora, se usan varias.

MIMO = más antenas, más velocidad, más estabilidad

# Introducción a las WLAN

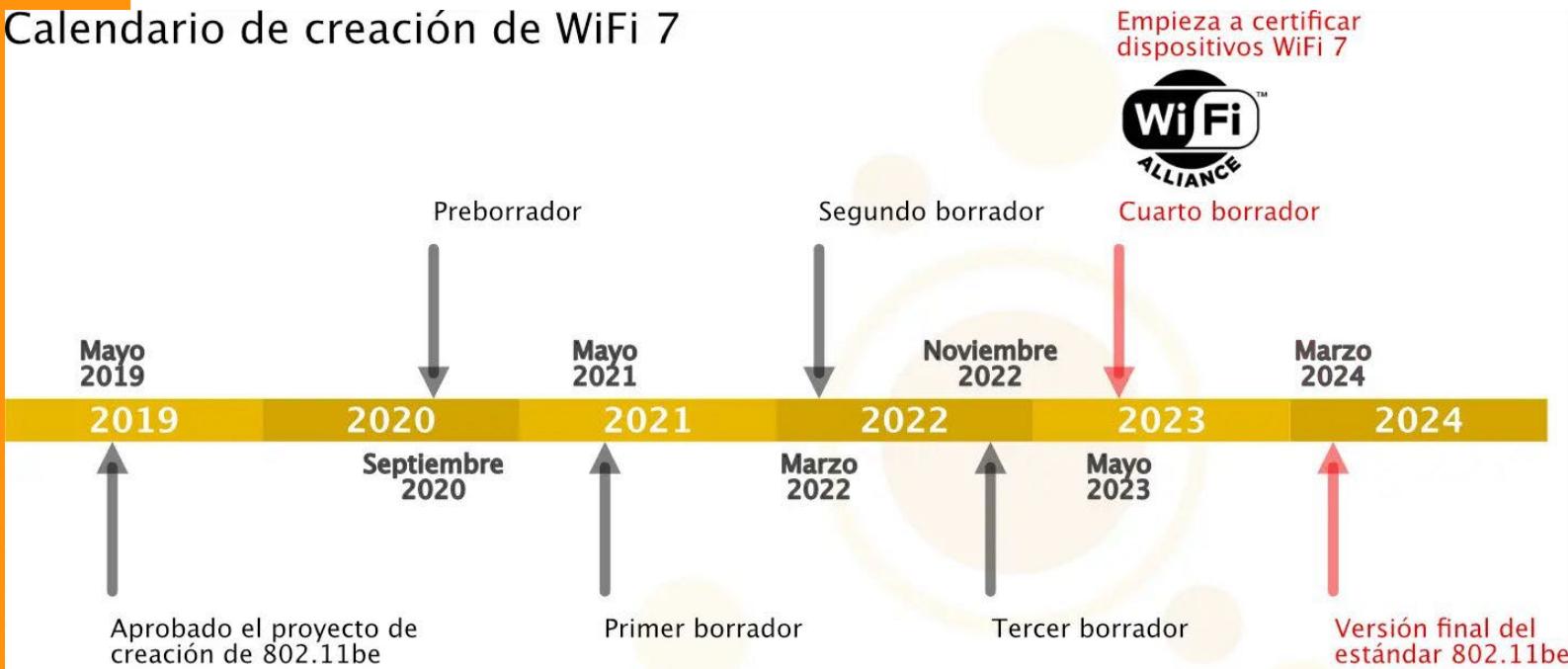
Estandarización IEEE 802.11



# Introducción a las WLAN

Estandarización IEEE 802.11

## Calendario de creación de WiFi 7



# Introducción a las WLAN

WiFi

- *En 1999 existía un estándar pero...*
  - *existían productos de diferentes fabricantes que no trabajaban correctamente juntos*
- *Wi-Fi Alliance es una organización sin ánimo de lucro para certificar la interoperabilidad de productos IEEE 802.11 fundada en 1999*
- *Actualmente, se ofrecen más de 15000 productos certificados Wi-Fi y alrededor de 450 compañías forman parte de Wi-Fi Alliance ([www.wi-fi.org](http://www.wi-fi.org))*



# Introducción a las WLAN

## Certificado WiFi



### Wi-Fi CERTIFIED™ Interoperability Certificate

This certificate lists the features that have successfully completed Wi-Fi Alliance interoperability testing.  
 Learn more: [www.wi-fi.org/certification/programs](http://www.wi-fi.org/certification/programs)



**Certification ID: WFA71644**

**Page 1 of 2**

Date of Last Certification	April 27, 2017
Company	Samsung Electronics ↗
Product	SM-G9508 ↗
Model Number	SM-G9508 ↗
Product Identifier(s)	
Category	Smartphone, multi-mode (Wi-Fi and other) —
Hardware Version	Product: REV0.2, Wi-Fi Component: N/A
Firmware Version	Product: G9508.001, Wi-Fi Component: 13.35.42
Operating System	Android, version: 7.0
Frequency Band(s)	2.4 GHz, 5 GHz ↗

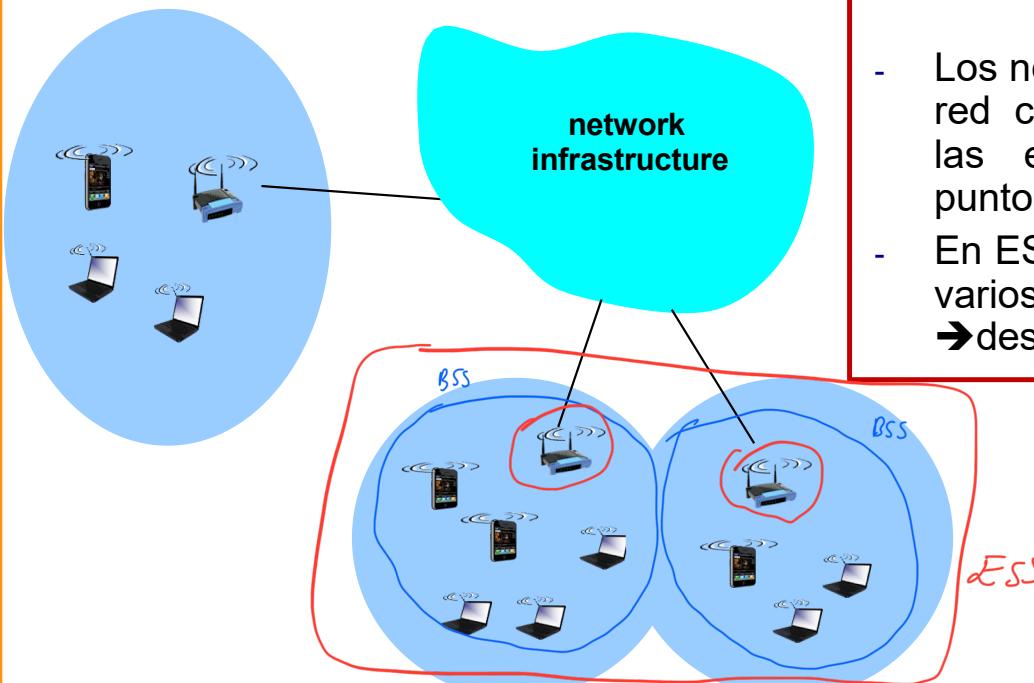
### Summary of Certifications

CLASSIFICATION	PROGRAM
Connectivity	Wi-Fi CERTIFIED™ [a, b, g, n, ac]
	WPA™ – Enterprise, Personal —
	WPA2™ – Enterprise, Personal —
	Wi-Fi Direct® ↗

# Introducción a las WLAN

## Topologías

Consumo de Servicios Básicos (BSS)



### Modo infraestructura

BSS (Basic Service Set)

ESS (Extended Service Set)

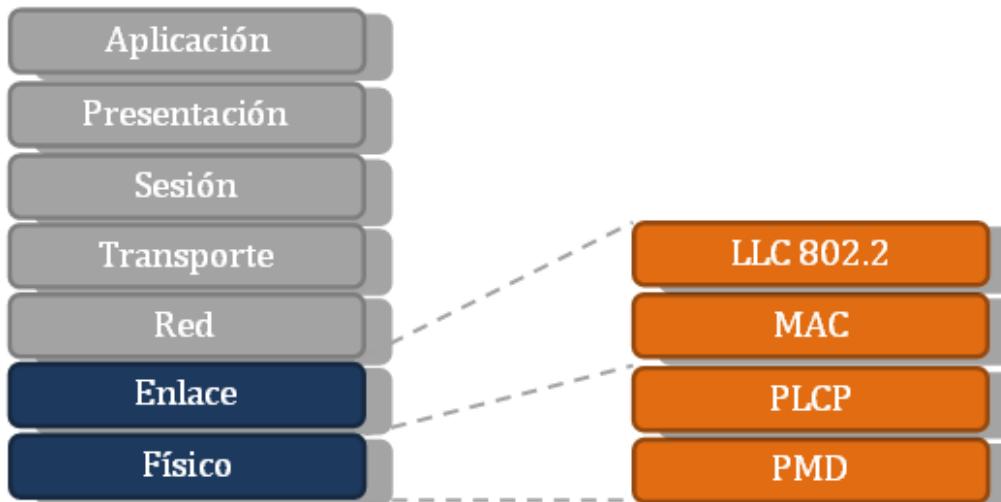
- Los nodos se conectan a la red cableada a través de las estaciones bases o puntos de acceso
- En ESS se superponen varios BSS  
→desplazamiento

"El entorno está compuesto por 2 básicos"

ESS

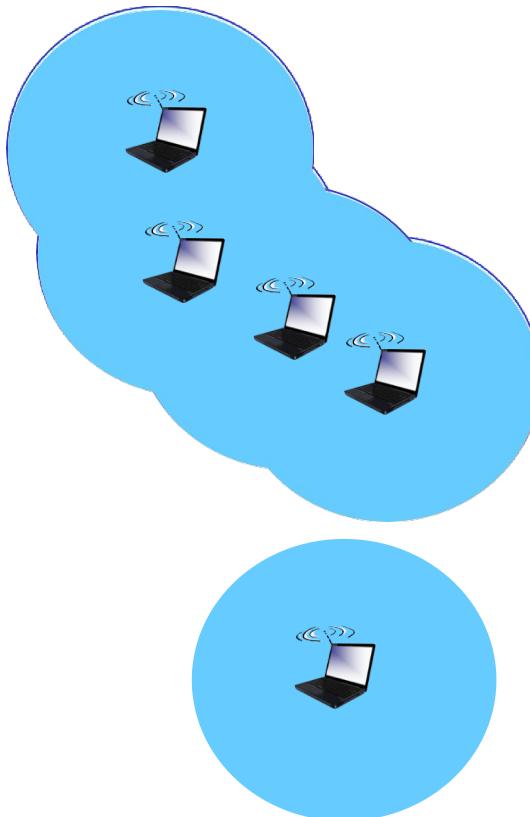
# Introducción a las WLAN

Modelo OSI



# Introducción a las WLAN

## Topologías



### Modo adhoc

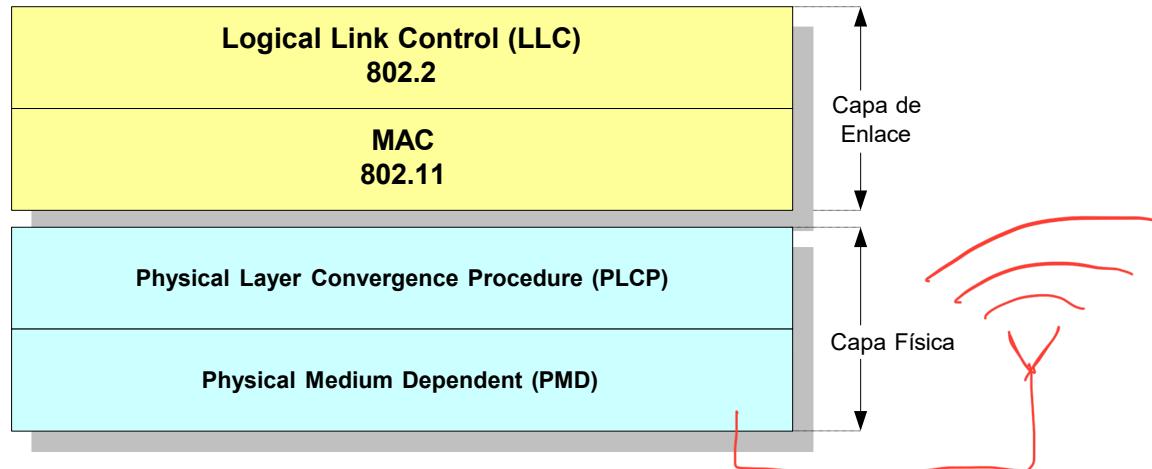
#### IBSS (Independent Basic Service Set)

- No hay estaciones base
- Los nodos sólo transmiten a los nodos que están dentro del área de cobertura
- Los nodos organizan su propia red

# Arquitectura IEEE 802.11

Capa física

- Dividida en dos subcapas: **PLCP** y **PMD**
  - Physical Layer Convergence Procedure (PLCP)**
  - Physical Medium Dependent (PMD)**



# Arquitectura IEEE 802.11

## Capa física

- **Physical Layer Convergence Procedure (PLCP):**
  - Gestiona las tramas de la MAC y las pone en el formato adecuado para la PMD
  - Preámbulos y cabeceras de la capa física (varían según estándar)
  - Carrier sensing para la capa MAC
    - ↳ Detección de portadora
- **Physical Medium Dependent (PMD)**
  - Gestiona las características particulares del medio inalámbrico
  - Define los métodos para transmitir y recibir datos en el medio (modulación y codificación)

# Arquitectura IEEE 802.11

## Capa física

- *Tecnologías de transmisión*
  - *Mientras más eficientemente se codifiquen los datos, mayores tasas o flujos de bits se consiguen dentro del mismo ancho de banda*
  - *En IEEE 802.11 se utiliza más ancho de banda del mínimo necesario para mandar un bit a fin de conseguir protección contra las interferencias*
  - Varias técnicas para ensanchar el ancho de banda:
    - FHSS (*Espectro ensanchado por salto de frecuencia*)
    - DSSS (*Espectro ensanchado por secuencia directa*)
    - OFDM (*Multiplexación por división de frecuencia ortogonal*)

Ya no se  
usan

- {
- FHSS (*Espectro ensanchado por salto de frecuencia*)
  - DSSS (*Espectro ensanchado por secuencia directa*)
  - OFDM (*Multiplexación por división de frecuencia ortogonal*)

↑  
Esto se usa hoy en día

# Arquitectura IEEE 802.11

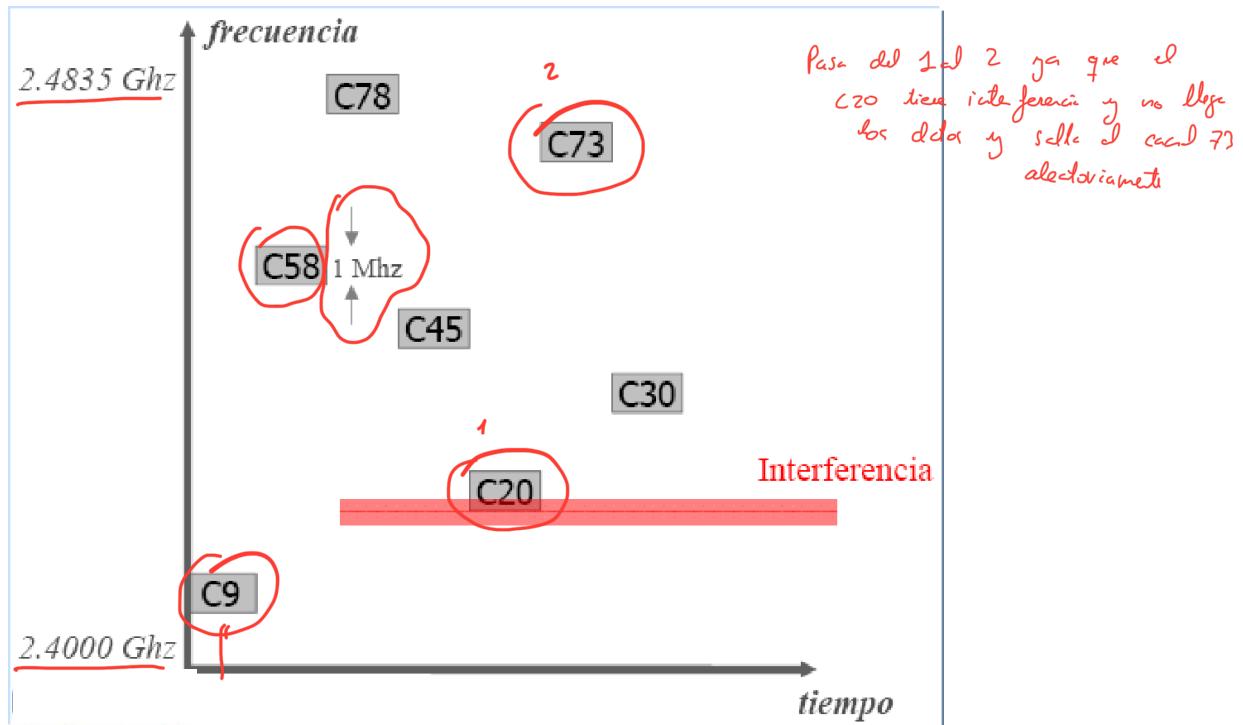
## Capa física

- **Frecuency Hopping (salto de frecuencia): FHSS**
  - La señal (banda estrecha) se transmite a diferentes frecuencias de manera alternativa
  - El transmisor cambia de canal continuamente y aleatoriamente
  - El tiempo de transmisión en cada frecuencia < 400 ms (dwell time)
  - El transmisor debe enviar al receptor señales de sincronización para la secuencia y duración de los saltos
  - Se utiliza la banda de frecuencia 2,400 → 2,4835 GHz, la cual se divide en 79 canales de 1 MHz de ancho c/u “cada uno”
  - Cuando el canal coincide con una interferencia, la señal no se recibe; la trama se retransmite en el siguiente salto

# Arquitectura IEEE 802.11

## Capa física

- FHSS



# Arquitectura IEEE 802.11

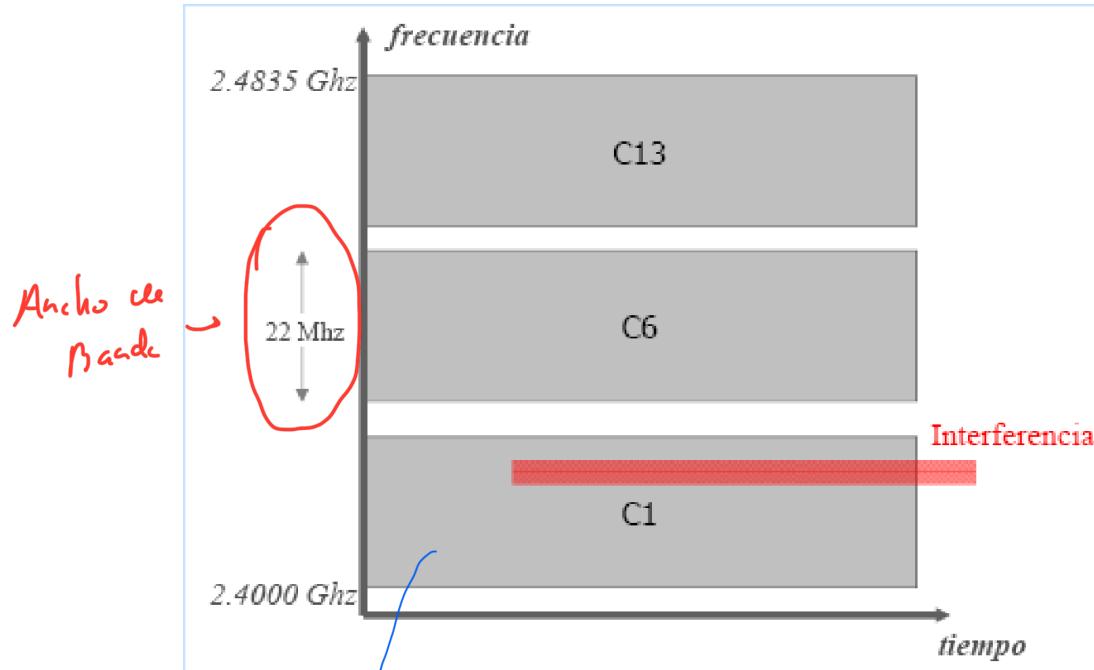
## Capa física

- Direct Sequence (Secuencia directa): DS~~SS~~
  - Cada bit correspondiente a un 1 es sustituido por una secuencia de bits específica y el bit 0 por su complemento
  - En lugar de ensanchar el espectro usando diferentes frecuencias, cada bit se codifica en una secuencia de impulsos más cortos (chips) → normalmente cada bit
  - Más rápida que FHSS, pero más vulnerable a interferencias  
*DSSS < eficiencia cada bit transmitidos por cada bit de datos*

# Arquitectura IEEE 802.11

Capa física

- DSSS



Con 2 bits adicionales, de los 11 bits, se recuperan señal sin necesidad de transmisión

# Arquitectura IEEE 802.11

## Capa física

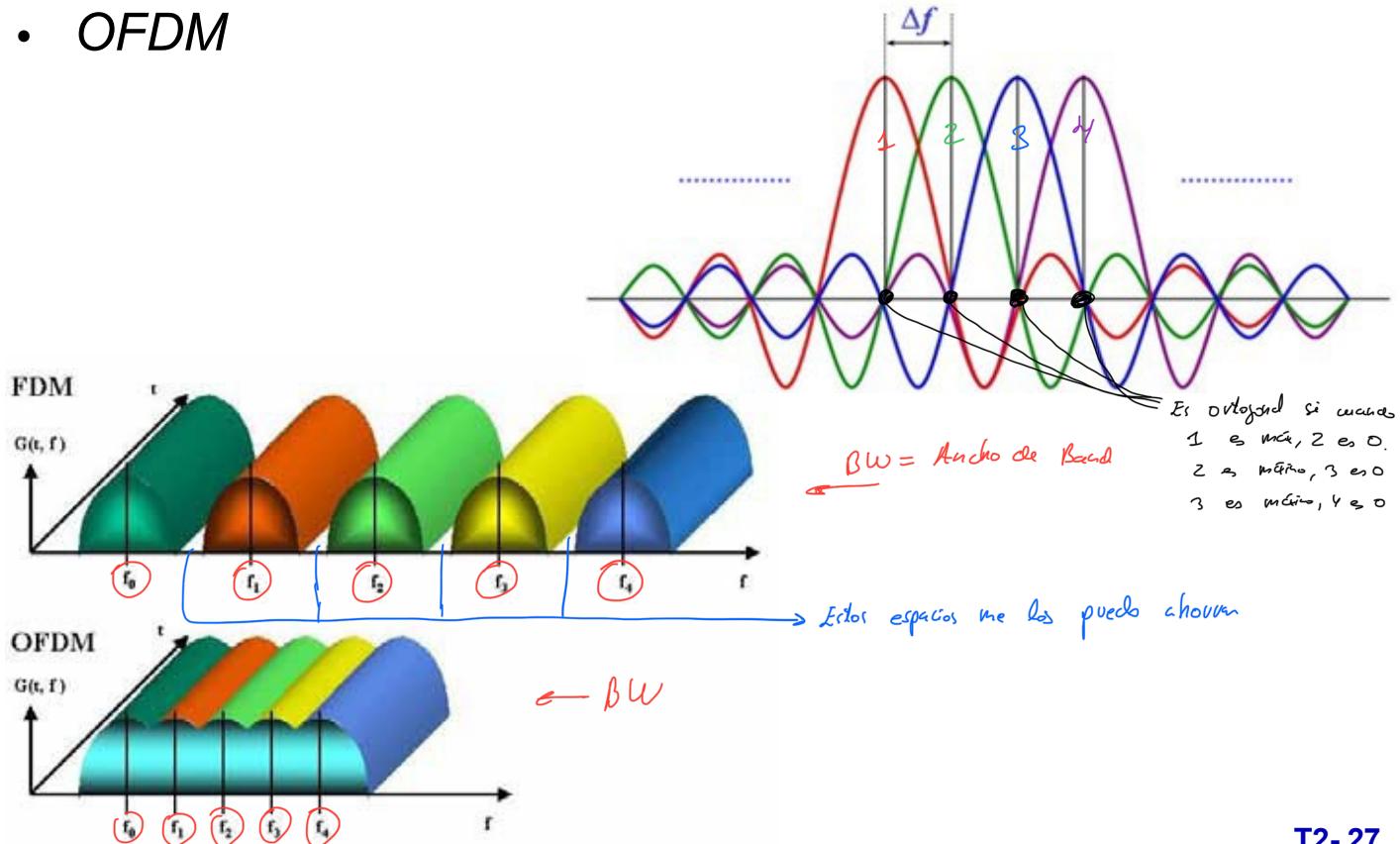
- **Orthogonal Frequency (Frecuencia ortogonal):** OFDM
  - Basada en la idea de la multiplexión por división de frecuencia (FDM)
  - La banda se divide en canales ortogonales y cada uno se usa para transmitir una portadora (modulada con diferentes técnicas)
  - Un sólo transmisor transmite en muchas (desde decenas a millares) frecuencias ortogonales
  - Esta técnica de modulación es la más común a partir del 2005, debido a que es muy robusta respecto a la recepción de señales con distintos retardos y amplitudes
    - WiFi, WiMax, ADSL, LTE

*“Si hay 2 frecuencias ortogonales, se pueden mandar datos simultáneamente”*

# Arquitectura IEEE 802.11

Capa física

- OFDM

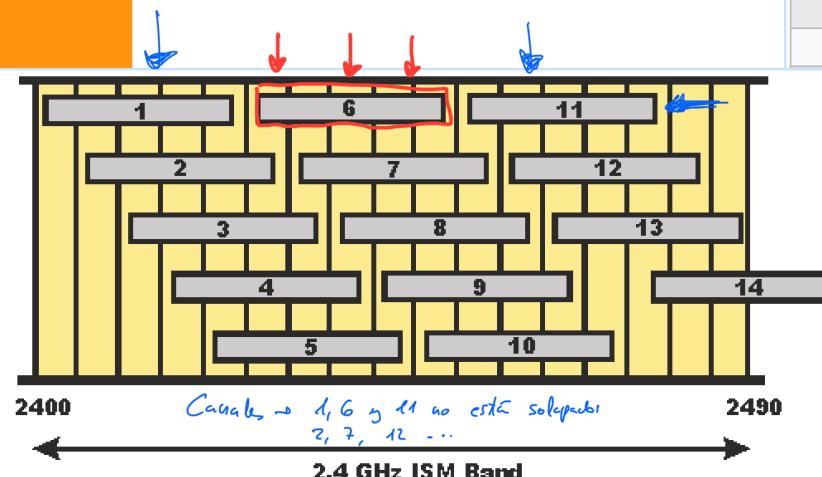


# Arquitectura IEEE 802.11

## Capa física

- Canales 802.11 en 2.4 Ghz
  - Espaciados cada 5 Mhz, excepto el último (12 Mhz)
  - Ancho banda: 22 Mhz
  - Separación: 25 Mhz

En esta banda, los canales están solapados porque hay poco ancho de banda.



CHANNEL NUMBER	LOWER FREQUENCY MHZ	CENTER FREQUENCY MHZ	UPPER FREQUENCY MHZ
1	2401	2412	2423
2	2404	2417	2428
3	2411	2422	2433
4	2416	2427	2438
5	2421	2432	2443
6	2426	2437	2448
7	2431	2442	2453
8	2436	2447	2458
9	2441	2452	2463
10	2451	2457	2468
11	2451	2462	2473
12	2456	2467	2478
13	2461	2472	2483
14	2473	2484	2495

# Arquitectura IEEE 802.11

Capa física

- Canales 802.11 en 2.4 Ghz

CHANNEL NUMBER	EUROPE (ETSI)	NORTH AMERICA (FCC)	JAPAN
1	✓	✓	✓
2	✓	✓	✓
3	✓	✓	✓
4	✓	✓	✓
5	✓	✓	✓
6	✓	✓	✓
7	✓	✓	✓
8	✓	✓	✓
9	✓	✓	✓
10	✓	✓	✓
11	✓	✓	✓
12	✓	No	✓
13	✓	No	✓
14	No	No	802.11b only



# Arquitectura IEEE 802.11

## Capa física

- Canales 802.11 en 5 Ghz
  - 25 canales no solapados (canal de 20 Mhz)

CHANNEL NUMBER	FREQUENCY MHZ	EUROPE (ETSI)	NORTH AMERICA (FCC)	JAPAN
36	5180	Indoors	✓	✓
40	5200	Indoors	✓	✓
44	5220	Indoors	✓	✓
48	5240	Indoors	✓	✓
52	5260	Indoors / DFS / TPC	DFS	DFS / TPC
56	5280	Indoors / DFS / TPC	DFS	DFS / TPC
60	5300	Indoors / DFS / TPC	DFS	DFS / TPC
64	5320	Indoors / DFS / TPC	DFS	DFS / TPC
100	5500	DFS / TPC	DFS	DFS / TPC
104	5520	DFS / TPC	DFS	DFS / TPC
108	5540	DFS / TPC	DFS	DFS / TPC
112	5560	DFS / TPC	DFS	DFS / TPC
116	5580	DFS / TPC	DFS	DFS / TPC
120	5600	DFS / TPC	No Access	DFS / TPC
124	5620	DFS / TPC	No Access	DFS / TPC
128	5640	DFS / TPC	No Access	DFS / TPC
132	5660	DFS / TPC	DFS	DFS / TPC
136	5680	DFS / TPC	DFS	DFS / TPC
140	5700	DFS / TPC	DFS	DFS / TPC
149	5745	SRD	✓	No Access
153	5765	SRD	✓	No Access
157	5785	SRD	✓	No Access
161	5805	SRD	✓	No Access
165	5825	SRD	✓	No Access

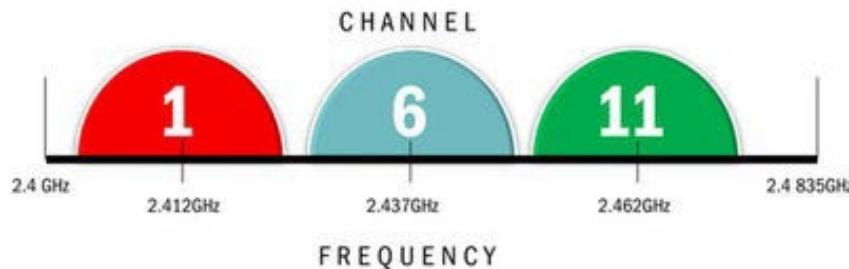
- DFS = Dynamic Frequency Selection
- TPC = Transmit Power Control
- SRD = Short Range Devices 25 mW  
max power

# Arquitectura IEEE 802.11

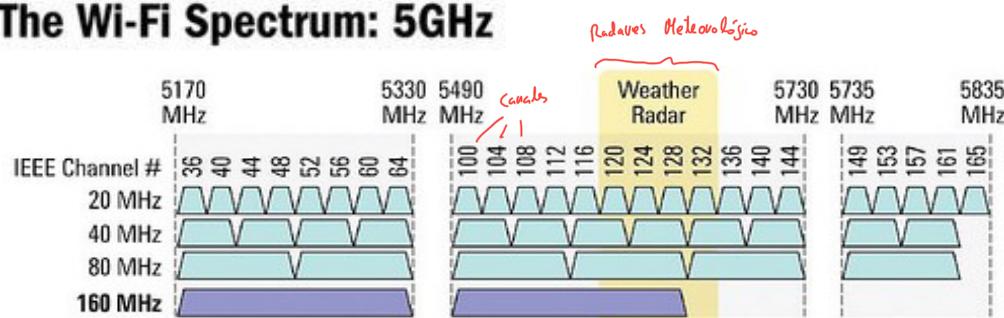
Capa física

- Canales 2.4 /5 Ghz

## The Wi-Fi Spectrum: 2.4GHz



## The Wi-Fi Spectrum: 5GHz



# Arquitectura IEEE 802.11

## Capa física

- *Otras bandas de frecuencias*

WI-FI TECHNOLOGY	STANDARD	FREQUENCIES BANDS
White-Fi	802.11af	470 - 710MHz 
Microwave Wi-Fi	802.11ad	57.0 - 64.0 GHz ISM band (Regional variations apply) Channels: 58,32, 60.48, 62.64, and 64.80 GHz

# Arquitectura IEEE 802.11

Capa física

- **802.11b (11Mbps banda de 2,4Ghz)**
  - Técnica DSSS
    - Para 1 Mbps: DBPSK
    - Para 2 Mbps: DQPSK
    - Para 5.5 y 11 Mbps: CCK
  - Formato encabezado físico
    - • SYNC = bits de sincronismo (todo 1s)
    - • SFD = delimitador de trama (0x05CF)
    - • SIGNAL = tasa binaria que se tiene que emplear: 11, 5.5, 2, 1 Mbps
    - • SERVICE = información adicional sobre la modulación (CCK vs. PBCC), reloj interno
    - • LENGTH = microsegundos requeridos para transmitir la trama
    - • CRC = detección errores

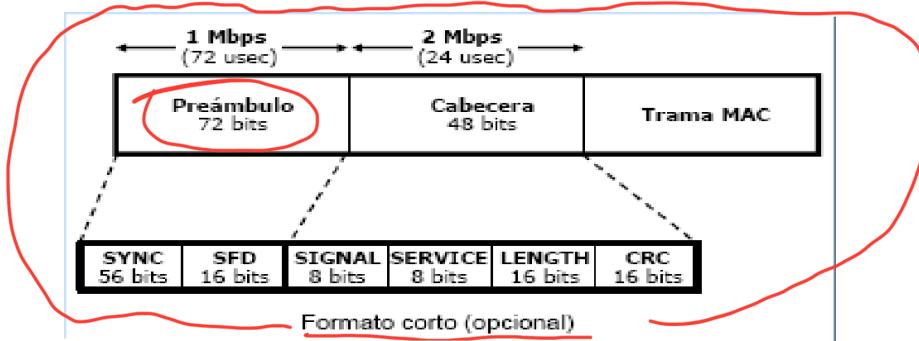
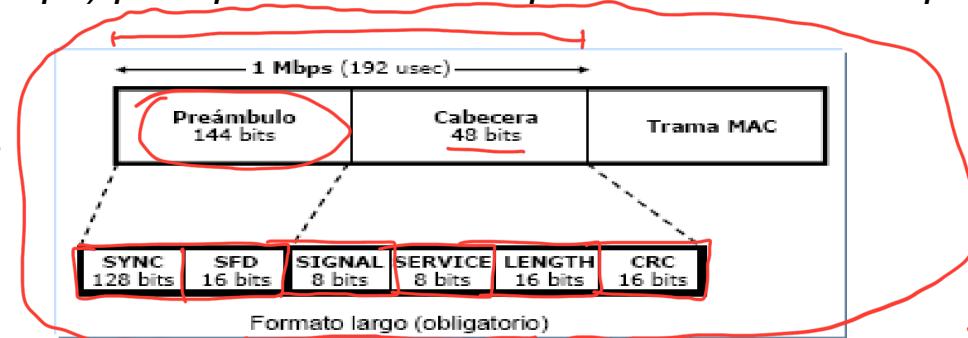
# Arquitectura IEEE 802.11

Capa física

- Formato encabezado físico 802.11b

*Examen*

- Los preámbulos y cabeceras son transmitidos a baja velocidad (1/2 Mbps) para permitir la interoperabilidad entre dispositivos



# Arquitectura IEEE 802.11

## Capa física

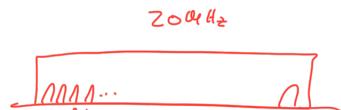
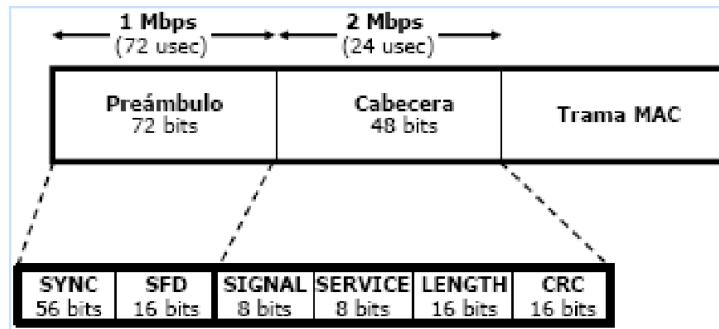
- 802.11g (54Mbps banda 2,4Ghz)

- Extensión de 802.11b, DSSS y OFDM

IEEE 802.11G WI-FI PHYSICAL LAYER SUMMARY		
PHYSICAL LAYER	USE	DATA RATES (MBPS)
ERP-DSSS	Mandatory	1, 2, 5.5, 11
ERP-OFDM	Mandatory	6, 9, 12, 18, 24, 36, 48, 54
ERP-PBCC	Optional	1, 2, 5.5, 11, 22, 33
DSSS-OFDM	Optional	6, 9, 12, 18, 24, 36, 48, 54

Total = 82 portadoras

- Se utiliza el formato corto del encabezado 802.11b



En cada canal puede haber más de 1 persona gracias a los subportadores.

# Arquitectura IEEE 802.11

## Capa física

- **802.11n (WiFi 4 por Wi-Fi Alliance. Max 600Mbps banda 2,4 Ghz y 5 Ghz)**
  - **MIMO (Multiple Input Multiple Output)**
    - Se trata de enviar por múltiples antenas, y recibir también por múltiples antenas de manera simultánea
    - Uso de varios “flujos” espaciales (spatial stream): flujo de bits por una de las dimensiones espaciales que aparecen (varias antenas en los dos extremos del enlace)
    - Incremento del rendimiento y disminución de la influencia del multi-camino
    - El uso de 3 y 4 spatial streams es opcional, 2 spatial streams es obligatorio en los AP
      - Mínimo (2x2), Máximo (4 x 4)



52 subportadoras  
de datos

# Arquitectura IEEE 802.11

## Capa física

- **802.11n**
  - Utilización opcional de canales de 40 Mhz → aumenta la tasa binaria
  - 56 subportadoras en OFDM →  $52 \text{ datos} + 4 \text{ piloto} = 56$
  - Compatibilidad con 802.11a/g (legacy o Mixto)
    - Preámbulo compatible con el empleado por 802.11a/g
    - Después se añade un segundo preámbulo, necesario para MIMO
    - En canales de 40 Mhz se repite el preámbulo en los dos canales de 20 Mhz
  - Situaciones sin dispositivos 802.11a/g (Greenfield)
    - Definición de un preámbulo exclusivo para 802.11n

Alto Rendimiento

# Arquitectura IEEE 802.11

## Capa física

- **802.11n**

*Curiosidad*

$$P_{\text{R}} = \frac{16}{N} = \frac{\text{Lat de Envio}}{\text{Lat de Salida}}$$

*Modo de Funcionamiento*

Index MCS	Modul.	Codif.	Spatial Streams	Canales 20 Mhz		Canales 40 Mhz	
				800 ns	400 ns	800 ns	400 ns
0	BPSK	1/2	1	6.5	7.2	13.5	15.0
1	QPSK	1/2	1	13.0	14.4	27.0	30.0
2	QPSK	3/4	1	19.5	21.7	40.5	45.0
3	16-QAM	1/2	1	26.0	28.9	54.0	60.0
4	16-QAM	3/4	1	39.0	43.3	81.0	90.0
5	64-QAM	2/3	1	52.0	57.8	108.0	120.0
6	64-QAM	3/4	1	58.5	65.0	121.5	135.0
7	64-QAM	5/6	1	65.0	72.2	135.0	150.0
8	BPSK	1/2	2	13.0	14.4	27.0	30.0
9	QPSK	1/2	2	26.0	28.9	54.0	60.0
10	QPSK	3/4	2	39.0	43.3	81.0	90.0
11	16-QAM	1/2	2	52.0	57.8	108.0	120.0
12	16-QAM	3/4	2	78.0	86.7	162.0	180.0
13	64-QAM	2/3	2	104.0	115.6	216.0	240.0
14	64-QAM	3/4	2	117.0	130.0	243.0	270.0
15	64-QAM	5/6	2	130.0	144.4	270.0	300.0

*Velocidad Mbps*

# Arquitectura IEEE 802.11

## Capa física

- **802.11n**

*Curiosidad*

Index MCS	Modul.	Codif.	Spatial Streams	Canales 20 Mhz		Canales 40 Mhz	
				800 ns	400 ns	800 ns	400 ns
16	BPSK	1/2	3	19.5	21.7	40.5	45.0
17	QPSK	1/2	3	39.0	43.3	81.0	90.0
18	QPSK	3/4	3	58.5	65.0	121.5	135.0
19	16-QAM	1/2	3	78.0	86.7	162.0	180.0
20	16-QAM	3/4	3	117.0	130.0	243.0	270.0
21	64-QAM	2/3	3	156.0	173.3	324.0	360.0
22	64-QAM	3/4	3	175.5	195.0	364.5	405.0
23	64-QAM	5/6	3	195.0	216.7	405.0	450.0
24	BPSK	1/2	4	26.0	28.9	54.0	60.0
25	QPSK	1/2	4	52.0	57.8	108.0	120.0
26	QPSK	3/4	4	78.0	86.7	162.0	180.0
27	16-QAM	1/2	4	104.0	115.6	216.0	240.0
28	16-QAM	3/4	4	156.0	173.3	324.0	360.0
29	64-QAM	2/3	4	208.0	231.1	432.0	480.0
30	64-QAM	3/4	4	234.0	260.0	486.0	540.0
31	64-QAM	5/6	4	260.0	288.9	540.0	600.0

ts de cod. 6 bits que envio , 5 son útiles.

Hay 30 modos

# Arquitectura IEEE 802.11

Capa física

- 802.11ac WiFi 5
  - Sólo en la banda de 5 Ghz
  - Canales de 40, 80 y 160 Mhz
  - Hasta 8 spatial streams
  - Todos los dispositivos AC deben soportar canales de 20, 40 y 80 Mhz y 1 spatial stream
  - Multi User (MU) MIMO
  - Intervalo de guarda de 400 ns
  - Modulación: hasta 256 QAM

# Arquitectura IEEE 802.11

## Capa física

- 802.11ac WIFI 5

*fijo de reproducción*

- 325 Mbps → canal 80 MHz, 1 spatial stream y 64-QAM 5/6
- 7 Gbps → canal 160 Mhz, 8 spatial streams y 256-QAM 5/6 con intervalo de guarda corto

# Arquitectura IEEE 802.11

## Capa física

- 802.11ac – Tasas con 1 spatial stream

Modulation Coding Scheme and Forward Error Correction Rate for 802.11ac						
MCS	Modulation	FEC Rate	Data Rate			
			20 MHz (Mbps)	40 MHz (Mbps)	80 MHz (Mbps)	160 MHz (Mbps)
0	BPSK	1/2	7.2	15.0	32.5	65.0
1	QPSK	1/2	14.4	30.0	65.0	130.0
2	QPSK	3/4	21.7	45.0	97.5	195.0
3	16QAM	1/2	28.9	60.0	130.0	260.0
4	16QAM	3/4	43.3	90.0	195.0	390.0
5	64QAM	2/3	57.8	120.0	260.0	525.0
6	64QAM	3/4	65.0	135.0	292.5	585.0
7	64QAM	5/6	72.2	150.0	325.0	650.0
8	256QAM	3/4	86.7	180.0	390.0	780.0
9	256QAM	5/6	N/A	200.0	433.3	866.7

# Arquitectura IEEE 802.11

## Capa física

- 802.11ax WiFi 6
  - Bandas de 2,4 y 5 Ghz
  - Canales de 40, 80, 80+80 y 160 Mhz
  - Hasta 8 spatial streams Ax
  - Todos los dispositivos AC deben soportar canales de 20, 40 y 80 Mhz y 1 spatial stream
  - Multi User (MU) MIMO
  - Intervalo de guarda de 400 ns
  - Modulación: hasta 1024 QAM

# Arquitectura IEEE 802.11

## Capa física

- **802.11ax**
  - Coloración BSS
    - Cuando hay muchos dispositivos conectados simultáneamente, se usa la técnica de utilización de colores (marcas) para identificar cada red.
    - Los puntos de acceso utilizan estos colores para tomar decisiones sobre si está permitido el uso simultáneo del medio o no.
    - Reducción de las interferencias
  - 9,6 Gbps → canal 160 Mhz, 8 spatial streams y 1024-QAM con intervalo de guarda corto
  - Menor consumo energético (TWT, Target Wake Time)
    - Se negocian con el AP los tiempos de actividad de los dispositivos

# Arquitectura IEEE 802.11

**Capa física**

- *Resumen estándares*

**IEEE 802.11 PHY Standards**

Release Date	Standard	Frequency Band (GHz)	Bandwidth (MHz)	Modulation	Advanced Antenna Technologies	Maximum Data Rate
1997	802.11	2.4 GHz	20 MHz	DSSS, FHSS	N/A	2 Mbits/s
1999	802.11b	2.4 GHz	20 MHz	DSSS	N/A	11 Mbits/s
1999	802.11a	5 GHz	20 MHz	OFDM	N/A	54 Mbits/s
2003	802.11g	2.4 GHz	20 MHz	DSSS, OFDM	N/A	542 Mbits/s
2009	802.11n	2.4 GHz, 5 GHz	20 MHz, 40 MHz	OFDM	MIMO, up to 4 spatial streams	600 Mbits/s
2013	802.11ac	5 GHz	40 MHz, 80 MHz, 160 MHz	OFDM 256 QAM	MIMO, MU-MIMO, up to 8 spatial streams	6.93 Gbits/s
2019	802.11ax WiFi 6	2.4 y 5 GHz	40, 80+80, 160 MHz	OFDM 1024 QAM	MU-MIMO, Spatial streams	9,6 Gbits/s
2024	wifi 7	2.4 , 5 y 6 GHz	320 MHz	4096 QAM	16 Spatial Streams	T2- 45

# Arquitectura IEEE 802.11

## Capa MAC

- Necesidad de arbitrar el acceso al medio compartido
- Se basa en el mecanismo Carrier Sense Multiple Access (CSMA) con la variante Collision Avoidance (CA) → DCF (Distributed Coordination Function)
  - 802.3 → CSMA/CD (Cableado)  
↓  
Detección de Colisiones
  - 802.11 → CSMA/CA (Inalámbrico)  
↓  
"Evitar Colisiones"

← Función que utiliza el mecanismo CSMA/CA
- En el medio inalámbrico, no se puede emplear detección de colisión, como en Ethernet, porque las estaciones no pueden escuchar el medio mientras transmiten
- Además pueden existir nodos ocultos

# Arquitectura IEEE 802.11

## Capa MAC

### • Funcionamiento Básico DCF

- Una estación que quiere transmitir comprueba el medio
- Si el medio está libre espera un tiempo denominado DIFS. Si al finalizar DIFS el medio sigue libre la estación transmite la trama
  - Para asegurar un acceso equilibrado al canal, si una estación acaba de transmitir una trama y tiene otra lista para ser transmitida deberá esperar un periodo aleatorio
- Si está ocupado, se espera a que vuelva a estar libre durante un tiempo DIFS tras el cual espera un tiempo aleatorio y transmite (si sigue libre)
- Cuando una estación recibe correctamente una trama de datos, espera un tiempo SIFS y le manda la confirmación pertinente (ACK)

Libre

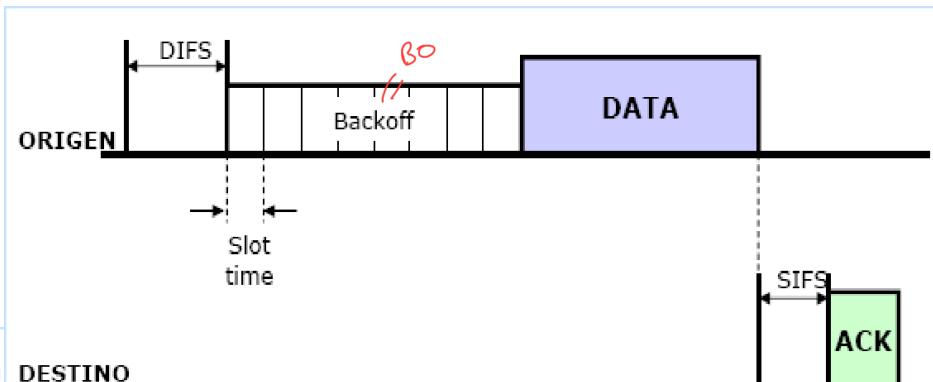
Ocupado

# Arquitectura IEEE 802.11

Capa MAC

- *Funcionamiento Básico DCF*

- Si una estación transmite una trama y no recibe confirmación en un tiempo determinado, dará la trama por perdida, procediendo a su retransmisión



802.11 b

- Slot Time = 20 us
- SIFS = 10 us
- DIFS = 50 us (2 x Slot\_Time + SIFS)
- Tiempo de Backoff = Número aleatorio entre 0 y CW – 1 (CW<sub>min</sub>=32; CW<sub>max</sub>=1024)

slot time 9μs 802.11 a/g/n /ac

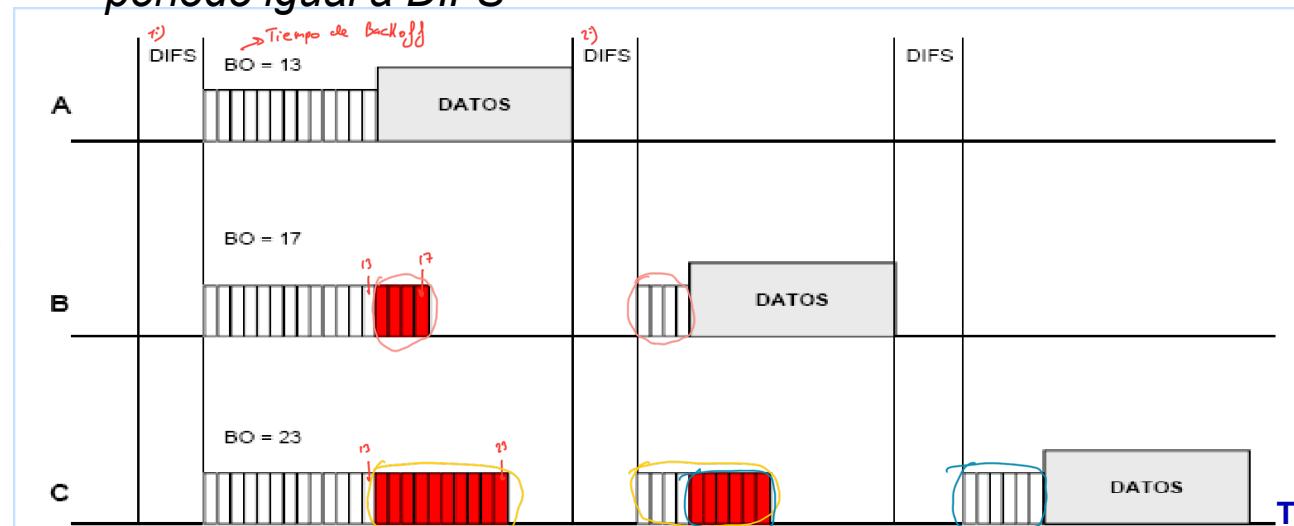
# Arquitectura IEEE 802.11

Capa MAC

- *Funcionamiento Básico DCF*

- Durante cada slot las estaciones revisan el medio, si está libre continúan disminuyendo el temporizador
- Si el medio se ocupa durante un slot se detiene el temporizador y sólo se reinicia cuando el medio vuelve a estar libre por un periodo igual a DIFS

Representación Gráficamente



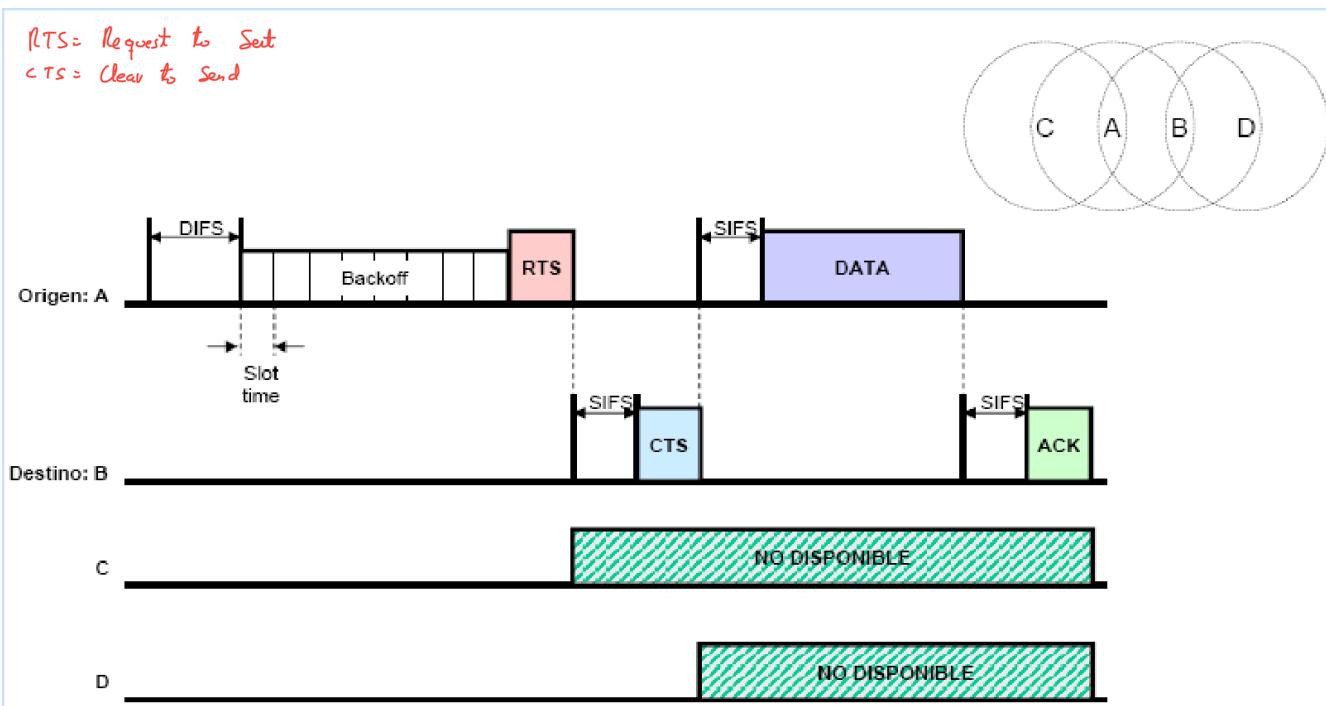
# Arquitectura IEEE 802.11

Capa MAC

- Problema terminal oculto → RTS/CTS

RTS = Request to Send

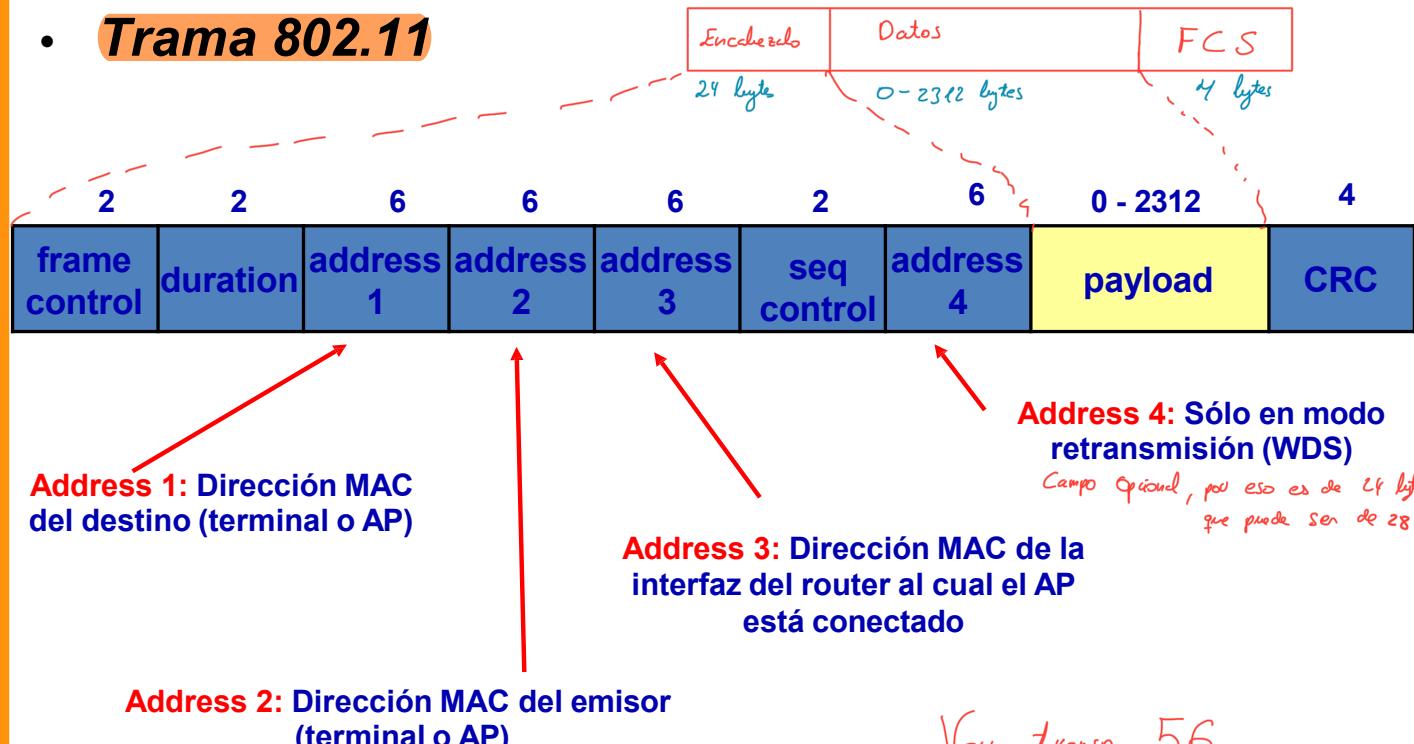
CTS = Clear to Send



# Arquitectura IEEE 802.11

Capa MAC

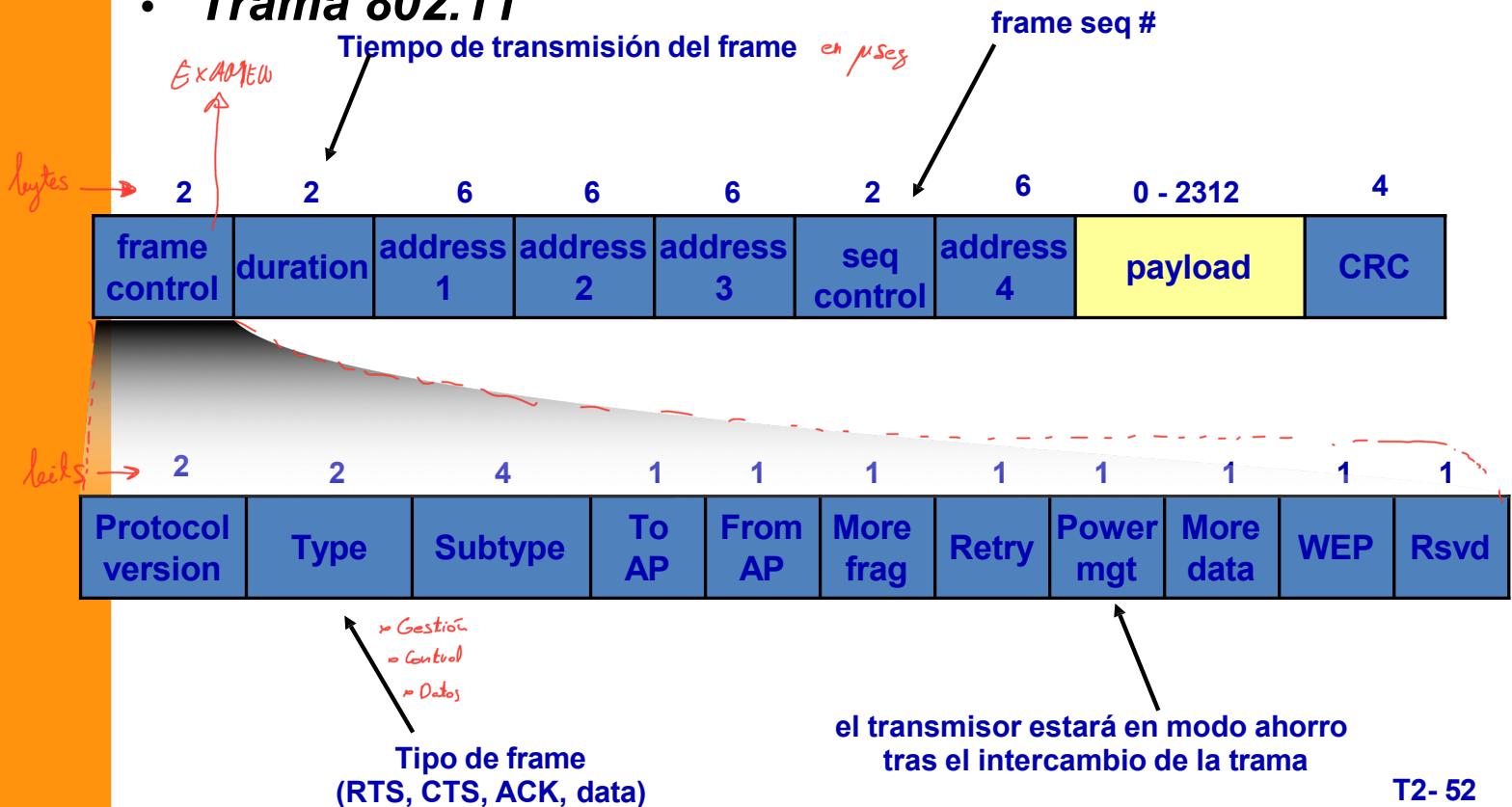
- Trama 802.11**



# Arquitectura IEEE 802.11

Capa MAC

- **Trama 802.11**



# Arquitectura IEEE 802.11

**Capa MAC**

- **Trama 802.11 – Gestión, Control y Datos**

Type value	Type description	Subtype value	Subtype description
00	Management	0000	Association Request
00	Management	0001	Association Response
00	Management	0010	Reassociation Request
00	Management	0011	Reassociation Response
00	Management	0100	Probe Request
00	Management	0101	Probe Response
00	Management	0110-0111	Reserved
00	Management	1000	Beacon
00	Management	1001	ATIM
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication
00	Management	1101	Action
00	Management	1110-1111	Reserved
<hr/>			
Type value	Type description	Subtype value	Subtype description
01	Control	0000-0111	Reserved
01	Control	1000	Block Ack Request
01	Control	1001	Block Ack
01	Control	1010	PS-Poll
01	Control	1011	RTS
01	Control	1100	CTS
01	Control	1101	ACK
01	Control	1110	CF-end
01	Control	1111	CF-end + CF-ack

# Arquitectura IEEE 802.11

Capa MAC

- **Trama 802.11 – Gestión, Control y Datos**

Type value	Type description	Subtype value	Subtype description
10	Data	0000	Data
10	Data	0001	Data + CF-ack
10	Data	0010	Data + CF-poll
10	Data	0011	Data +CF-ack +CF-poll
10	Data	0100	Null
10	Data	0101	CF-ack
10	Data	0110	CF-poll
10	Data	0111	CF-ack +CF-poll
10	Data	1000	QoS data
10	Data	1001	QoS data + CF-ack
10	Data	1010	QoS data + CF-poll
10	Data	1011	QoS data + CF-ack + CF-poll
10	Data	1100	QoS Null
10	Data	1101	Reserved
10	Data	1110	QoS + CF-poll (no data)
10	Data	1111	Qos + CF-ack (no data)
11	Reserved	0000-1111	Reserved

# Arquitectura IEEE 802.11

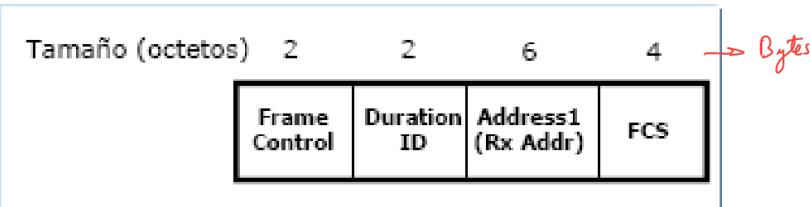
**Capa MAC**

- **Trama 802.11**

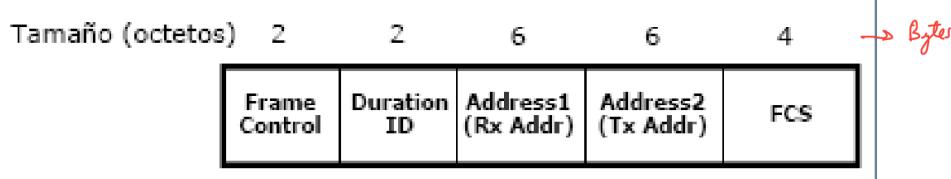
Transp Importante para los problemas

EXAMEN

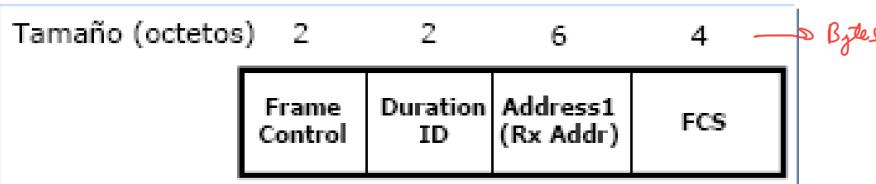
- **ACK**



- **RTS**



- **CTS**

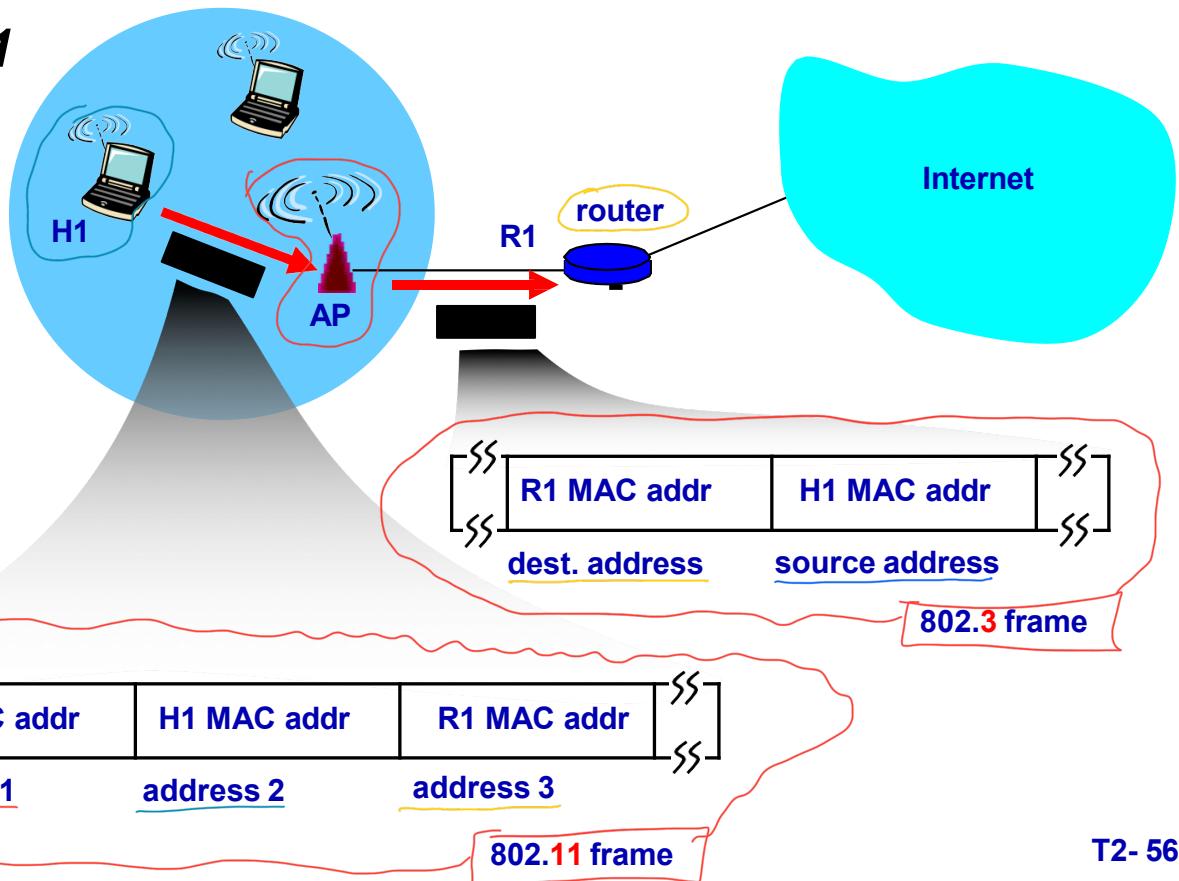


Como ves son tramas, por lo que llevan un encabezado cada una

# Arquitectura IEEE 802.11

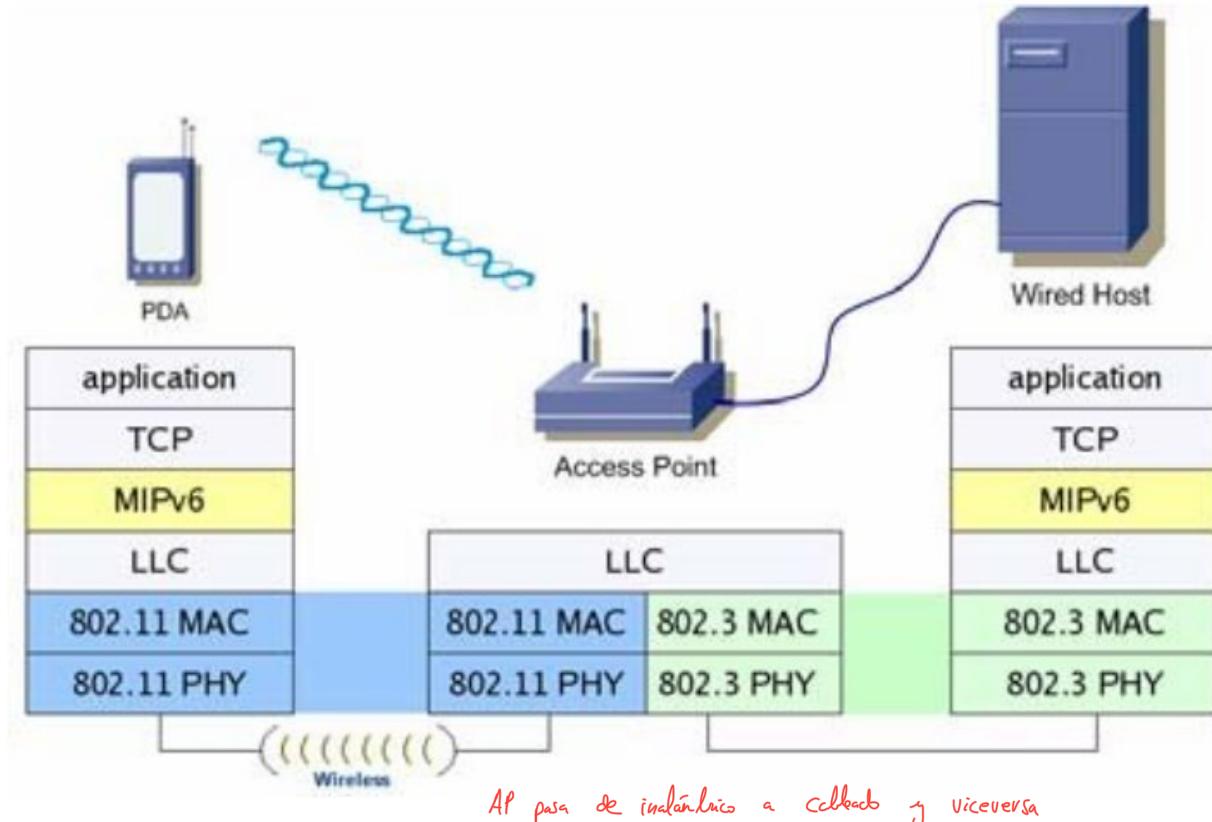
Capa MAC

- 802.11



# Arquitectura IEEE 802.11

Capa MAC



AP pasa de inalámbrico a cableado y viceversa

# Arquitectura IEEE 802.11

## Capa MAC

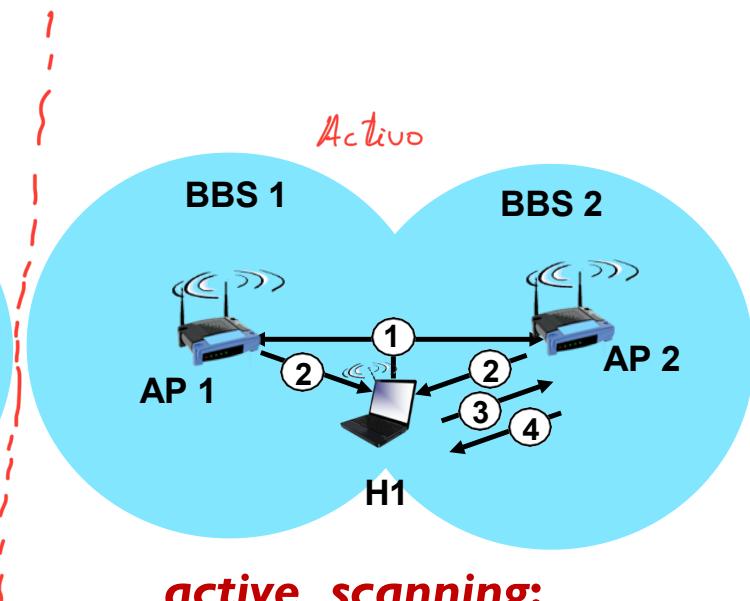
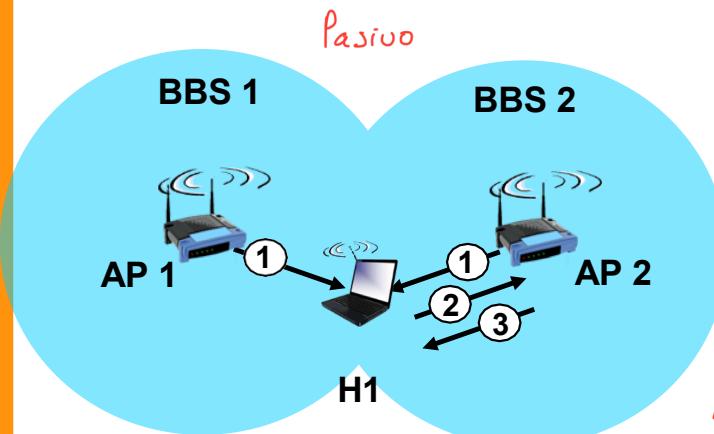
- **Operaciones de gestión**

- *Empleadas para gestionar las comunicaciones entre las estaciones y los puntos de acceso*
- *En el modo infraestructura, los AP mandan beacons (aproximadamente 10 cada segundo)*
- *Búsqueda de redes*
  - *Pasivo: la estación se sitúa en cada uno de los canales y escucha beacons*
  - *Activo: la estación manda un Probe Request en cada uno de los canales (broadcast), el punto de acceso le responde con un Probe Response*
- *Una vez completada la búsqueda, la estación debe autenticarse y asociarse con el punto de acceso antes de empezar a transmitir datos*
  - 1) Autenticación = "Poner Clave"      **A!**
  - 2) Asociarse = Aquí ya puede empezar a transmitir
- *En el modo ad-hoc, la generación de beacons es distribuida*

# Arquitectura IEEE 802.11

Capa MAC

- Operaciones de gestión



## passive scanning:

- (1) Beacon frames sent from APs
- (2) Association Request frame sent: H1 to selected AP
- (3) Association Response frame sent from selected AP to H1

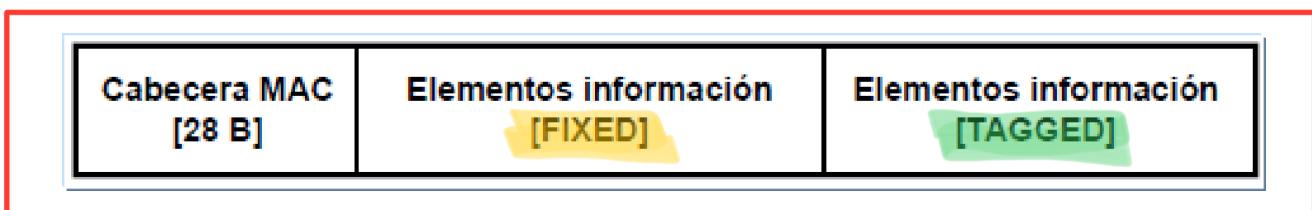
## active scanning:

- (1) Probe Request frame broadcast from H1
- (2) Probe Response frames sent from APs
- (3) Association Request frame sent: H1 to selected AP
- (4) Association Response frame sent from selected AP to H1

# Arquitectura IEEE 802.11

## Capa MAC

- **Tramas de operaciones de gestión**
  - Todas las tramas de gestión comparten un formato común
  - Los parámetros fijos (FIXED) tienen un formato específico
  - Para los etiquetados (TAGGED) se utiliza codificación TLV
  - El contenido de los elementos (FIXED o TAGGED) dependen del tipo de trama de gestión



Trama 802.11

Formato de la trama de Gestión

24 bytes	0-2312 bytes	CRC 4 bytes
----------	--------------	----------------

# Arquitectura IEEE 802.11

## Capa MAC

- *Tramas de operaciones de gestión – Codificación TLV*
  - *TLV (Type Length Value ) se emplea en varios protocolos (802.11, BGP,...)*
  - *Cada parámetro se codifica con tres campos:*
    - *Tipo: indica el argumento que se está transmitiendo*
    - *Longitud: tamaño del argumento*
    - *Valor: Parámetro a transmitir*
  - *Los dos primeros campos (Tipo, Longitud) tienen un tamaño fijo*
  - *Ventajas*
    - *Flexibilidad para incorporar nuevos parámetros*
    - *Eficiencia con campos de longitud variable*
    - *Facilidad en el procesado*

# Arquitectura IEEE 802.11

## Capa MAC

- Tramas de operaciones de gestión – **Codificación TLV**

```
☒ Tagged parameters (68 bytes)
    ☐ SSID parameter set (Nombre punto de Acceso "AP")
        Tag Number: 0 (SSID parameter set)
        Tag length: 17 → ↗ concatenar
        Tag interpretation: linksys_SES_24086: "linksys_SES_24086" ↘
    ☐ Supported Rates: 1,0(B) 2,0(B) 5,5(B) 11,0(B) → Velocidades separadas
        Tag Number: 1 (Supported Rates)
        Tag length: 4
        Tag interpretation: supported rates: 1,0(B) 2,0(B) 5,5(B) 11,0(B) [Mbit/sec]
    ☐ DS Parameter set: Current Channel: 6
        Tag Number: 3 (DS Parameter set)
        Tag length: 1
        Tag interpretation: Current channel: 6
    ☐ Traffic Indication Map (TIM): DTIM 0 of 1 bitmap empty
        Tag Number: 5 (Traffic Indication Map (TIM))
        TIM length: 4
        DTIM count: 0
        DTIM period: 1
        Bitmap Control: 0x00 (mcast:0, bitmap offset 0)
    ☐ Vendor Specific: Broadcom
        Tag Number: 221 (vendor specific)
        Tag length: 6
        Vendor: Broadcom
        Tag interpretation: Not interpreted
        ☐ Vendor Specific Microsoft WPA
```

# Arquitectura IEEE 802.11

## Capa MAC

- Tramas de operaciones de gestión – **Beacon**
    - Elementos de información FIXED *12 bytes*
    - *Timestamp [8B]* favorecen la sincronización de la red
    - *Beacon Interval [2B]* intervalo entre beacons
    - Capability [2B] *B = Bytes*
      - Infraestructura o Adhoc
      - Privacidad → Soporte WEP o no
      - Modulación DSSS-OFDM, ....
- dos APs anuncian la existencia*

*Esta trama nada*

ESS	IBSS	CF Poll	CF Poll REQ	Priv.	Short Prea.	PBCC	Chan. Agility	Spec. Mgm.	QoS	Short Slot Time	APSD	Res.	DSSS OFDM	Delay Block ACK	Inm. Block ACK
-----	------	---------	-------------	-------	-------------	------	---------------	------------	-----	-----------------	------	------	-----------	-----------------	----------------

- Varios campos se han incorporado a medida que han aparecido ampliaciones al estándar

# Arquitectura IEEE 802.11

## Capa MAC

- *Tramas de operaciones de gestión – Beacon*
  - **Elementos de información TAGGED**
    - SSID
    - Tasas binarias soportadas
    - Para cada una se usan 7 bits para la velocidad y 1 bit para indicar si es básica
    - Canal empleado
    - Tasas binarias extendidas (sólo se pueden añadir 8 al campo anterior)
    - Aspectos seguridad
    - Traffic Indication Map – Indicación de tramas para una estación

# Arquitectura IEEE 802.11

## Capa MAC

- Tramas de operaciones de gestión – Beacon
  - Adhoc Beacon 802.11b

```
IEEE 802.11
IEEE 802.11 wireless LAN management frame
Fixed parameters (12 bytes)
    Timestamp: 0x0000000000009615F
    Beacon Interval: 0.102400 [Seconds]
Capability Information: 0x0002
    .... .... .... .0 = ESS capabilities: Transmitter is a STA
    .... .... .... .1 = IBSS status: Transmitter belongs to an IBSS
    .... .... ..0.. = CFP participation capabilities: Station is not CF-Pollable (0x0000)
    .... .... ...0 .. = Privacy: AP/STA cannot support WEP
    .... .... ..0. .... = Short Preamble: Short preamble not allowed
    .... .... ..0... .. = PBCC: PBCC modulation not allowed
    .... .... .0.... .. = Channel Agility: Channel agility not in use
    .... .0. .... .... = Short Slot Time: Short slot time not in use
    ..0. .... .... .... = DSSS-OFDM: DSSS-OFDM modulation not allowed
Tagged parameters (25 bytes)
    Tag Number: 0 (SSID parameter set)
    Tag length: 6
    Tag interpretation: RedGID
    Tag Number: 1 (Supported Rates)
    Tag length: 4
    Tag interpretation: Supported rates: 1.0(B) 2.0(B) 5.5 11.0 [Mbit/sec]
    Tag Number: 3 (DS Parameter set)
    Tag length: 1
    Tag interpretation: Current Channel: 1
    Tag Number: 6 (IBSS Parameter set)
    Tag length: 2
    Tag interpretation: ATIM window 0x0
```

# Arquitectura IEEE 802.11

## Capa MAC

- Tramas de operaciones de gestión – Beacon
  - Infraestructura Beacon 802.11g

```

IEEE 802.11 Beacon frame, Flags: .....c
IEEE 802.11 wireless LAN management frame
  Fixed parameters (12 bytes)
    Timestamp: 0x000005c6f02aa196
    Beacon Interval: 0,102400 [Seconds]
  Capability Information: 0x0011
    ..... .... .... 1 = ESS capabilities: Transmitter is an AP
    ..... .... .... 0. = IBSS status: Transmitter belongs to a BSS
    .... 0. .... 00.. = CFP participation capabilities: No point coordinator at AP (0x0000)
    .... .... .... 1 .... = Privacy: AP/STA can support WEP
    .... .... .... 0. .... = Short Preamble: short preamble not allowed
    .... .... .... 0.... = PBCC: PBCC modulation not allowed
    .... .... 0. .... = Channel Agility: channel agility not in use
    .... 0. .... .... = Spectrum Management: dot11spectrumManagementRequired FALSE
    .... 0. .... .... = Short slot Time: short slot time not in use
    .... 0. .... .... = Automatic Power Save Delivery: apsd not implemented
    ..0. .... .... .... = DSSS-OFDM: DSSS-OFDM modulation not allowed
    .0. .... .... .... = Delayed Block Ack: delayed block ack not implemented
    0. .... .... .... = Immediate Block Ack: immediate block ack not implemented
  Tagged parameters (68 bytes)
    SSID parameter set
      Tag Number: 0 (SSID parameter set)
      Tag length: 17
      Tag interpretation: linksys_SES_24086: "linksys_SES_24086"
    Supported Rates: 1,0(B) 2,0(B) 5,5(B) 11,0(B)
      Tag Number: 1 (Supported Rates)
      Tag length: 4
      Tag interpretation: Supported rates: 1,0(B) 2,0(B) 5,5(B) 11,0(B) [Mbit/sec]
    DS Parameter set: Current Channel: 6
      Tag Number: 3 (DS Parameter set)
      Tag length: 1
      Tag interpretation: Current Channel: 6
    Traffic Indication Map (TIM): DTIM 0 of 1 bitmap empty
      Tag Number: 5 (Traffic Indication Map (TIM))
      TIM length: 4
      DTIM count: 0
  
```

# Arquitectura IEEE 802.11

Todo lo que estamos dando  
son Tramas [colección] ...

Capa MAC

- *Tramas de operaciones de gestión – Probe Request*
  - La estación lanza en cada canal Probe Request en busca de redes
  - *Sin elementos de información FIXED*
  - *TAGGED*
    - SSID (broadcast o almacenadas en estación)
    - *Tasas soportadas*
    - *Request Information*
    - *Extensión tasas soportadas*
    - *Información específica del fabricante*

# Arquitectura IEEE 802.11

## Capa MAC

- *Tramas de operaciones de gestión – Probe Request*

```
IEEE 802.11 Probe Request, Flags: . . . . . C
  Type/Subtype: Probe Request (0x04)
  + Frame Control: 0x0040 (Normal)
    Duration: 0
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Source address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
    Fragment number: 0
    Sequence number: 1625
  + Frame check sequence: 0xc1a4d2ca [correct]
IEEE 802.11 wireless LAN management frame
  Tagged parameters (30 bytes)
    SSID parameter set
      Tag Number: 0 (SSID parameter set)
      Tag length: 0
      Tag interpretation: : Broadcast
    Supported Rates: 1,0 2,0 5,5 11,0 6,0 9,0 12,0 18,0
    Request: Tag 10 Len 1
    Extended Supported Rates: 24,0 36,0 48,0 54,0
    Vendor Specific: Intel
```

# Arquitectura IEEE 802.11

## Capa MAC

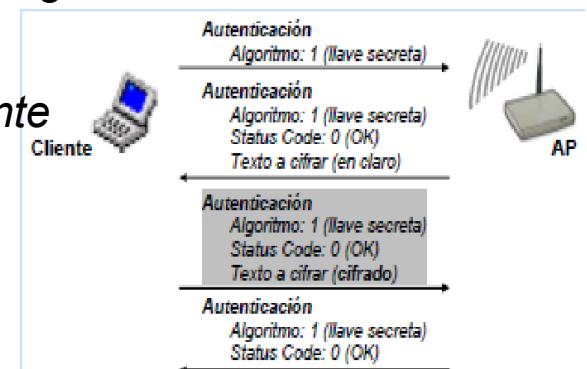
- *Tramas de operaciones de gestión – Probe Response*
  - El AP responde a los Probe Request con Probe Response
  - Similar a la trama Beacon, pero trama unicast
  - Incorpora (si fuera necesario) campos para responder a las peticiones del REQUEST

```
IEEE 802.11 Probe Response, Flags: ....R...C
  Type/Subtype: Probe Response (0x05)
  + Frame Control: 0x0850 (Normal)
    Duration: 314
    Destination address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    Source address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Fragment number: 0
    Sequence number: 3560
  + Frame check sequence: 0x6c7814c3 [correct]
IEEE 802.11 wireless LAN management frame
  + Fixed parameters (12 bytes)
    Timestamp: 0x000000289903266A
    Beacon Interval: 0,102400 [seconds]
    + Capability Information: 0x0601
  + Tagged parameters (113 bytes)
    + SSID parameter set
      Tag Number: 0 (SSID parameter set)
      Tag length: 12
      Tag interpretation: 30 Munroe St: "30 Munroe St"
  + Supported Rates: 1,0(B) 2,0(B) 5,5(B) 11,0(B)
    Tag Number: 1 (Supported Rates)
    Tag length: 4
    Tag interpretation: Supported rates: 1,0(B) 2,0(B) 5,5(B) 11,0(B) [Mbit/sec]
```

# Arquitectura IEEE 802.11

## Capa MAC

- Tramas de operaciones de gestión – **Autenticación**
  - Las estaciones se autentican contra la red
    - No se comprueba la identidad del punto de acceso
  - Abierta
    - Obligatoria para todos los AP
    - El AP acepta al terminal móvil sin comprobar su identidad
    - Filtrado MAC para mejorar la seguridad
  - Basado en clave compartida
    - Texto “reto” a cifrar por el cliente



# Arquitectura IEEE 802.11

## Capa MAC

- *Tramas de operaciones de gestión – Autenticación*
  - *Trama de autenticación*
    - *Elementos FIXED*
      - *Authentication Algorithm Number [2B] – Abierto o Llave secreta*
      - *Authentication Transaction Sequence Number [2B] – Número de trama actual*
      - *Status Code [2B] – Representa el resultado de la operación*
    - *Elementos TAGGED*
      - *Texto a encriptar – Sólo presente en el algoritmo basado en llave compartida*
      - *Información específica del fabricante*

# Arquitectura IEEE 802.11

## Capa MAC

- *Tramas de operaciones de gestión – Autenticación*

```
IEEE 802.11 Authentication, Flags: ....c
  Type/Subtype: Authentication (0x0b)
  □ Frame Control: 0x00B0 (Normal)
    Version: 0
    Type: Management frame (0)
    Subtype: 11
    □ Flags: 0x0
    Duration: 44
    Destination address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Source address: Intelcor_d1:b6:4f (00:13:02:d1:b6:4f)
    BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Fragment number: 0
    Sequence number: 1647
    □ Frame check sequence: 0xe0cbe847 [correct]
IEEE 802.11 wireless LAN management frame
  □ Fixed parameters (6 bytes)
    Authentication Algorithm: Open System (0)
    Authentication SEQ: 0x0001
    Status code: Successful (0x0000)
```

# Arquitectura IEEE 802.11

## Capa MAC

- *Tramas de operaciones de gestión – De-autenticación*
  - *Trama de de-autenticación*
    - *Se emplea para terminar una autenticación*
    - *Elementos de información FIXED*
      - *Código motivo [2B]*
    - *Elementos de información TAGGED (Opcional)*
      - *Información específica de fabricante*

# Arquitectura IEEE 802.11

## Capa MAC

- Tramas de operaciones de gestión – De-autenticación
  - Trama de de-autenticación

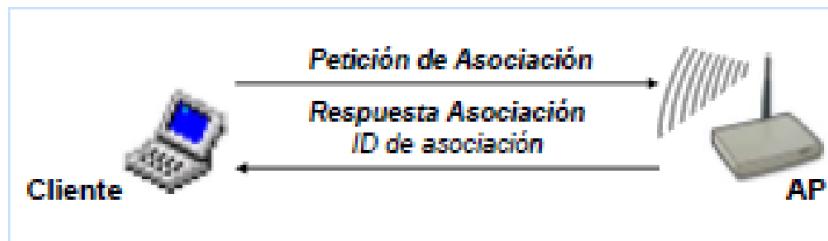
```
IEEE 802.11 Deauthentication, Flags: . . . . .  
Type/Subtype: Deauthentication (0x0c)  
Frame Control: 0x00C0 (Normal)  
Version: 0  
Type: Management frame (0)  
Subtype: 12  
Flags: 0x0  
Duration: 44  
Destination address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)  
Source address: Intelcor_d1:b6:4f (00:13:02:d1:b6:4f)  
BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)  
Fragment number: 0  
Sequence number: 1605  
Frame check sequence: 0x9c8b4a3b [correct]  
IEEE 802.11 wireless LAN management frame  
Fixed parameters (2 bytes)  
Reason code: Unspecified reason (0x0001)
```

# Arquitectura IEEE 802.11

Capa MAC

- *Tramas de operaciones de gestión – Asociación*
  - Operación necesaria para empezar a transmitir datos en la red, posterior a la autenticación
  - Si la estación no estuviera autenticada, el punto de acceso le respondería con una trama de “Desautenticación”

“Si no me asocio, no puedo transmitir”



# Arquitectura IEEE 802.11

## Capa MAC

- *Tramas de operaciones de gestión – Asociación*
  - *Trama Petición Asociación*
    - *Elementos de información FIXED*
      - *Capability [2B] – Como en el beacon*
      - *Listen Interval [2B] – Gestión potencia*
    - *Elementos de información TAGGED*
      - *SSID*
      - *Tasas soportadas*
      - *Extensión para tasas soportadas*
      - *Capacidad de gestión de espectro*
      - *Capacidad de QoS*
      - *Información de seguridad*
      - *Información específica del fabricante*

# Arquitectura IEEE 802.11

## Capa MAC

- Tramas de operaciones de gestión – Asociación
  - Trama Petición Asociación

```
[+] IEEE 802.11 Association Request, Flags: ....R...C
[+] IEEE 802.11 wireless LAN management frame
    [+] Fixed parameters (4 bytes)
        [+] Capability Information: 0x0011
            Listen Interval: 0x000a
    [+] Tagged parameters (51 bytes)
        [+] SSID parameter set
            Tag Number: 0 (SSID parameter set)
            Tag length: 17
            Tag interpretation: linksys_SES_24086: "linksys_SES_24086"
    [+] Supported Rates: 1,0(B) 2,0(B) 5,5(B) 11,0(B)
            Tag Number: 1 (Supported Rates)
            Tag length: 4
            Tag interpretation: Supported rates: 1,0(B) 2,0(B) 5,5(B) 11,0(B) [Mbit/sec]
    [+] Vendor Specific: Microsoft: WPA
            Tag Number: 221 (Vendor Specific)
            Tag length: 24
            Vendor: Microsoft
            Tag interpretation: WPA IE, type 1, version 1
            Tag interpretation: Multicast cipher suite: TKIP
            Tag interpretation: # of unicast cipher suites: 1
            Tag interpretation: Unicast cipher suite 1: TKIP
            Tag interpretation: # of auth key management suites: 1
            Tag interpretation: auth key management suite 1: PSK
            Tag interpretation: Not interpreted
```

# Arquitectura IEEE 802.11

## Capa MAC

- *Tramas de operaciones de gestión – Asociación*
  - Trama Respuesta Asociación
    - *Elementos de información FIXED* *Parámetros Fijos*
      - *Capability [2B] – como en el beacon*
      - *Código resultado asociación [2B]*
      - *ID de la asociación [2B]*
    - *Elementos de información TAGGED* *Parámetros etiquetados*
      - *Tasas soportadas*
      - *Extensión para tasas soportadas*
      - *Parámetros EDCA (Enhanced distributed channel access)*
      - *Información específica fabricante*

# Arquitectura IEEE 802.11

## Capa MAC

- *Tramas de operaciones de gestión – Asociación*
  - Trama Respuesta Asociación

```
IEEE 802.11 Association Response, Flags: .....c
IEEE 802.11 wireless LAN management frame
  Fixed parameters (6 bytes)
    Capability Information: 0x0601
      Status code: Successful (0x0000)
      Association ID: 0x0005
  Tagged parameters (36 bytes)
    Supported Rates: 1,0(B) 2,0(B) 5,5(B) 11,0(B)
      Tag Number: 1 (Supported Rates)
      Tag length: 4
      Tag interpretation: supported rates: 1,0(B) 2,0(B) 5,5(B) 11,0(B) [Mbit/sec]
    Extended Supported Rates: 6,0(B) 9,0 12,0(B) 18,0 24,0(B) 36,0 48,0 54,0
      Tag Number: 50 (Extended Supported Rates)
      Tag length: 8
      Tag interpretation: supported rates: 6,0(B) 9,0 12,0(B) 18,0 24,0(B) 36,0 48,0 54,0 [Mbit/sec]
    EDCA Parameter Set: Tag 12 Len 18
      Tag Number: 12 (EDCA Parameter Set)
      Tag length: 18
      Tag interpretation: Not interpreted
```

# Arquitectura IEEE 802.11

Capa MAC

- *Tramas de operaciones de gestión – Desasociación*
  - *Termina la asociación*
  - *Elementos de información FIXED*
    - Código motivo [2B]
  - *Elementos de información TAGGED*
    - *Información específica fabricante*

# Arquitectura IEEE 802.11

Capa MAC

- *Tramas de operaciones de gestión – Re-asociación*
  - *Se utiliza durante el roaming (traspaso) entre dos BSS de la misma ESS*
  - *El formato de las tramas es muy similar al del proceso de asociación, pero incluye información del AP actual*

# Arquitectura IEEE 802.11

## Capa MAC

- *Tramas de operaciones de gestión – Re-asociación*
  - Trama Petición Re-Asociación
    - Elementos de información FIXED
    - Capability [2B] – Como en el beacon
    - Listen Interval [2B] – Gestión de potencia
    - **AP actual [6B]**
  - *Elementos de información TAGGED*
    - SSID
    - Tasas soportadas
    - Extensión para tasas soportadas
    - Capacidad de gestión de espectro
    - Capacidad de QoS
    - Información de seguridad

# Arquitectura IEEE 802.11

## Capa MAC

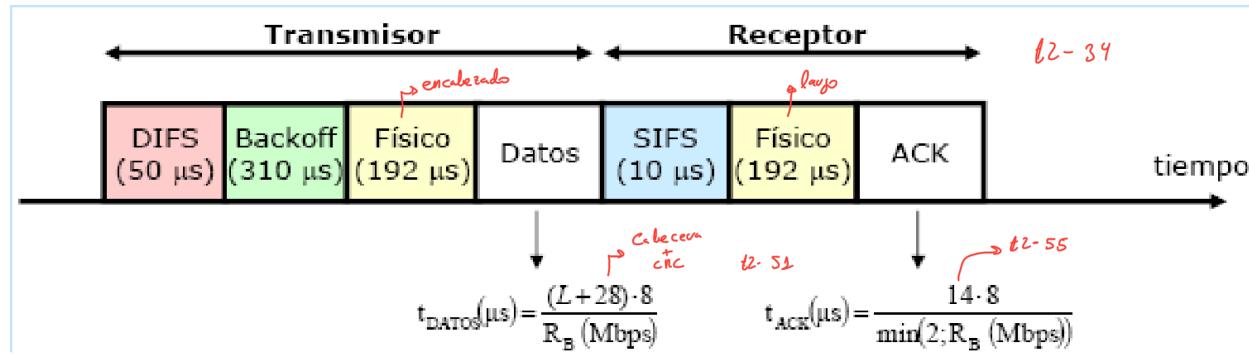
- *Tramas de operaciones de gestión – Re-asociación*
  - Trama Respuesta Re-Asociación
    - *Elementos de información FIXED*
      - *Capability [2B] – como en el beacon*
      - *Código resultado asociación [2B]*
      - *ID de la asociación [2B]*
    - *Elementos de información TAGGED*
      - *Tasas soportadas*
      - *Extensión para tasas soportadas*
      - *Parámetros EDCA*
      - *Información específica fabricante*

# Arquitectura IEEE 802.11

## Rendimiento

- Rendimiento en 802.11b**

- Las tasas de transmisión del estándar dan lugar a rendimientos efectivos más bajos, debido a la elevada sobrecarga que introducen las capas MAC y Física



- Hay que añadir el efecto RTS/CTS



$t_{2-51} = \text{Tiempo 2, transparency S1}$

Trama MAC

T2-84

# Seguridad en IEEE 802.11

## Seguridad

- *Requerimientos tradicionales de seguridad*
  - *Privacidad*
  - *Integridad de los datos*
  - *Autenticación*
- *El medio inalámbrico es intrínsecamente más vulnerable*
- *Se trató de solventar este problema, incluyendo el método WEP (Wired Equivalent Privacy) en la recomendación 802.11*
  - *Método poco eficaz, por lo que aparecen otras alternativas*

# Seguridad en IEEE 802.11

## Seguridad

- **WEP**

- Se trata de un **mecanismo de seguridad a nivel de enlace entre la estación y el AP**
- Sencillez y facilidad de *implementación*
- Controla el acceso a la red, denegando el acceso a estaciones no autenticadas
- Se basa en un algoritmo simétrico, RC4
  - Se genera una cadena de bits a partir de una llave
  - Esta se utiliza para cifrar el mensaje original, mediante la operación lógica XOR

[WEP → WPA → WPA2 → WPA3]

Evolución

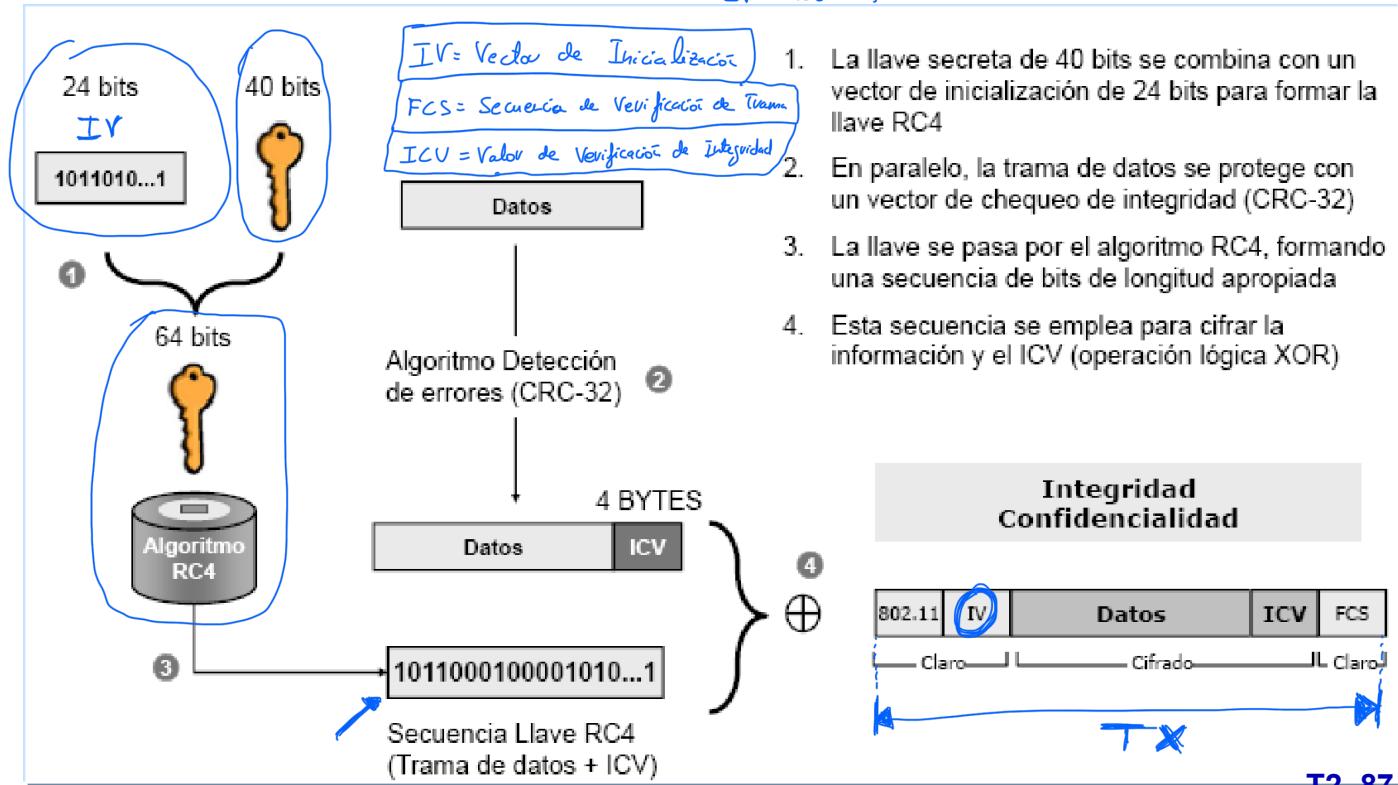
Únicamente podemos tener este

# Seguridad en IEEE 802.11

## Seguridad

- **WEP**

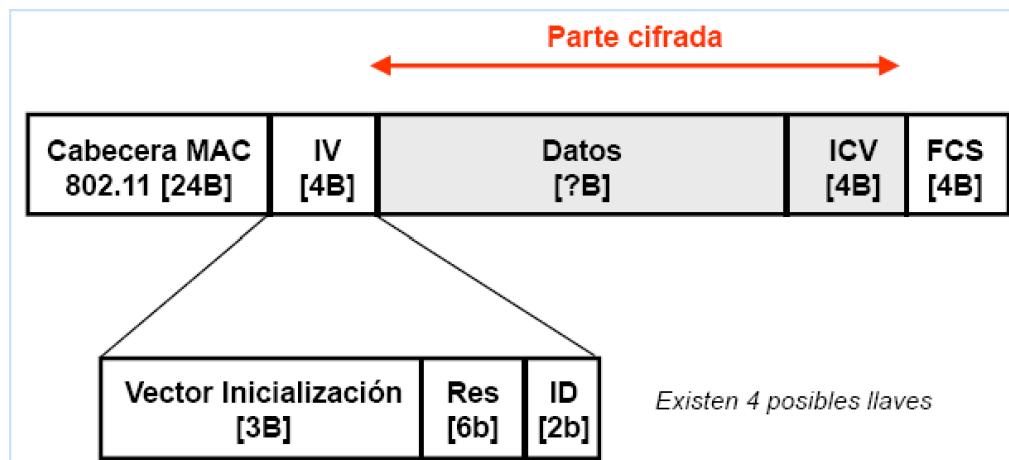
WEP extendido usa llave de 104 bits  
 $104 + 24 \text{ IV} = 128 \text{ bits}$



# Seguridad en IEEE 802.11

## Seguridad

- *Formato de trama WEP*

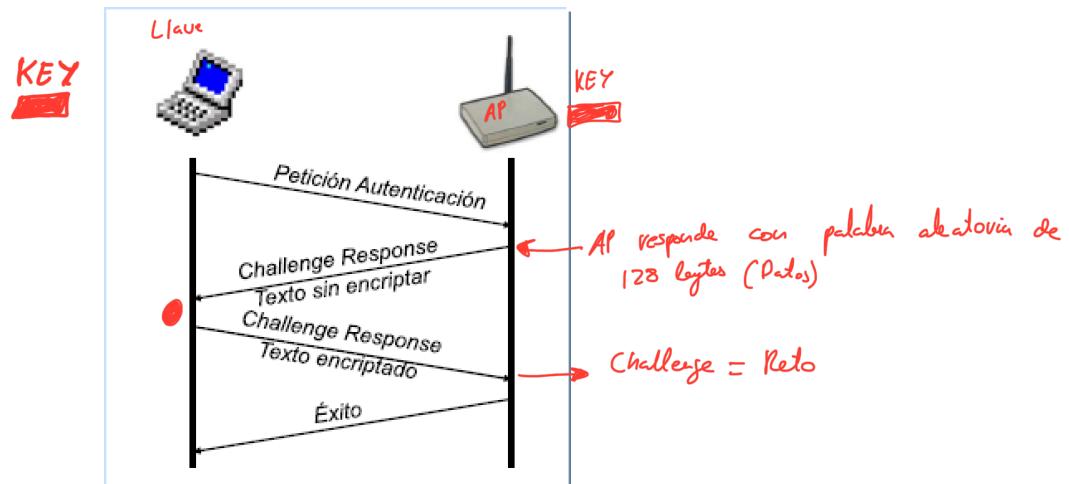


# Seguridad en IEEE 802.11

## Seguridad

- Autenticación WEP

- Las estaciones tienen que compartir una llave con el Punto de Acceso
- Esta llave se tiene que distribuir a todas las estaciones, antes de afrontar la autenticación



# Seguridad en IEEE 802.11

## Seguridad

- *Problemas con WEP*
  - *La llave cambia con el IV, pero éste se transmite en claro en el paquete*
    - Además, siendo de 24 bits, el mismo IV se usará relativamente pronto: un punto de acceso cargado, con paquetes de 1500 Bytes constantemente, utilizará todos los IV en 5 horas → “sólo” hay en torno a 17 M de IV
    - El estándar recoge que es opcional modificar el IV en cada paquete
  - *La integridad se basa en un CRC*
    - Es lineal, por lo que se pueden cambiar bits en los paquetes

# Seguridad en IEEE 802.11

## Seguridad

- Problemas con WEP
  - En la fase de autenticación, se transmite el texto claro y después el cifrado
    - $RC4(KEY, Reto) \oplus Reto = RetoCifrado$
    - $RetоСифрado \oplus Reto = RC4(KEY, Reto)$
  - No hay control de acceso especificado en el estándar, se suele basar en filtrado por dirección MAC
  - Distribución de llaves: Talón de Aquiles de los mecanismos de seguridad simétricos

Servicio de Usuario con Acceso Telefónico para Autenticación Remota.

# Seguridad en IEEE 802.11

## Seguridad

- **WPA (Wireless Protected Access)**

Autenticación →

- Servidor 802.1x para la distribución de llaves

- En entornos reducidos se suele usar clave compartida

Privacidad →

- Encriptación TKIP (Temporal Key Integrity Protocol)

- Vector de inicialización (IV) de 48 bits

- Clave de ~~104 bits~~ 128 bits

WPA - Enterprise

- Dinámicamente generada por el servidor de autenticación;

- Se cambia por trama, usuario, sesión

- Sigue usando RC4

Integridad →

- MIC (Message Integrity Check) → Michael

- Reemplaza al CRC

- Autenticación: 802.1x + EAP

CRC32 Llave 40 IW24 — WEP — RC4

MIC  
(MICHAEL)

Llave 128

IW48 — WPA { RC4/TKIP  
WPA-PSK  
WPA-Enterprise }  
WPA-Personal  
WPA-802.1x

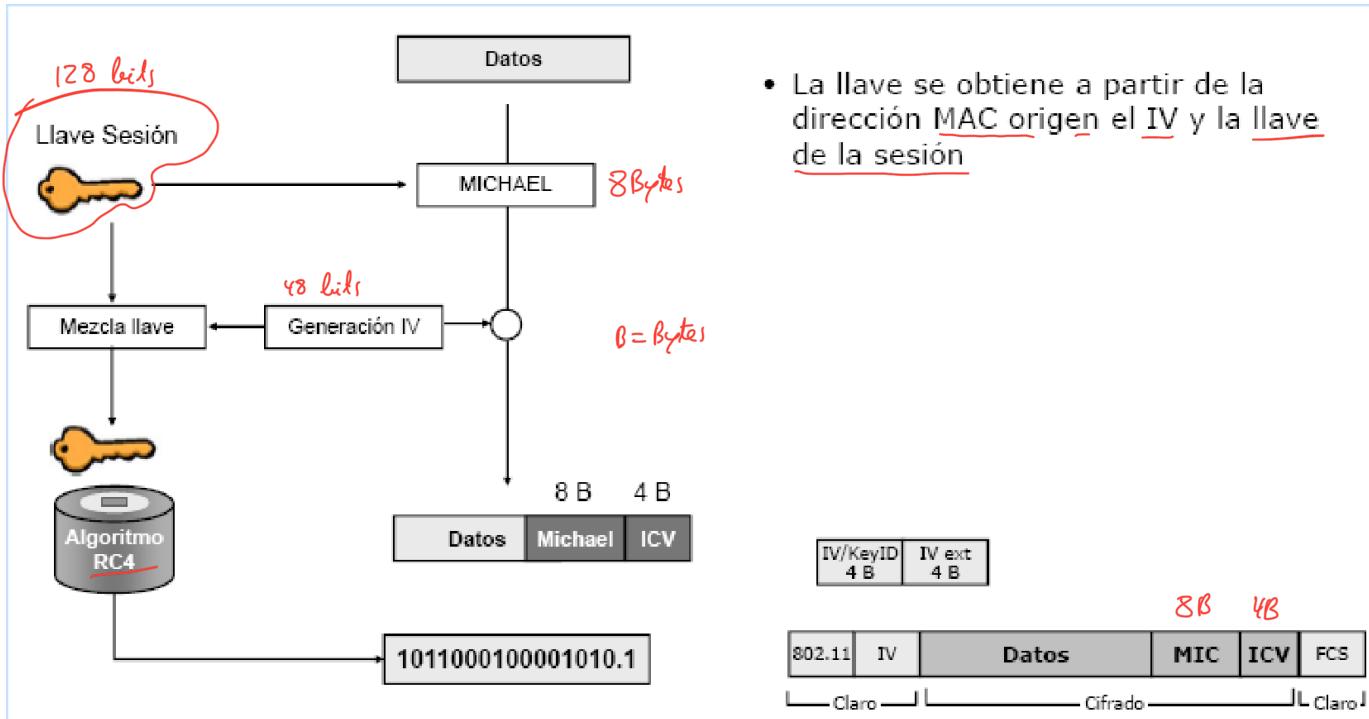
WPA2

WPA3

# Seguridad en IEEE 802.11

## Seguridad

- WPA(*Wireless Protected Access*)



# Seguridad en IEEE 802.11

## Seguridad

- **WPA2 (Wireless Protected Access)** → Evolución wpa

Estándar Seguridad

- Basado en el estándar IEEE 802.11i (junio 2004)
- Utiliza AES como método de transmisión / Encriptación
  - Método de encriptación de bloque y no de flujo (RC4)
- Arquitectura 802.11i / WPA2
  - 802.1x para la autenticación → idéntica a la empleada por WPA/TKIP
  - CCMP (Counter-Mode/CBC-Mac Protocol) → integridad, confidencialidad y autenticación

→ Protocolo de Autenticación → Reemplaza al TKIP del wpa

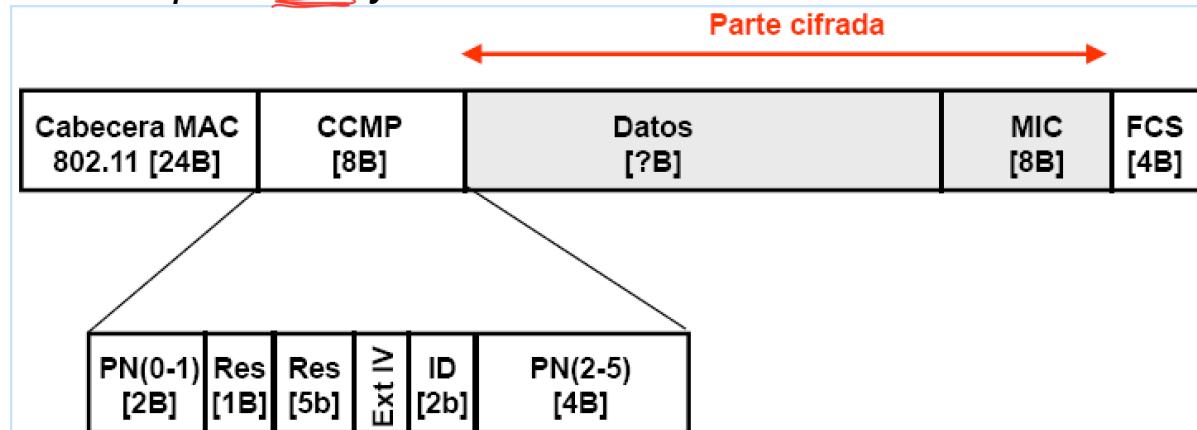
CCMP = AES

wifi

# Seguridad en IEEE 802.11

## Seguridad

- *WPA2 (Wireless Protected Access)*
  - *El formato de su trama es similar al de WPA*
    - *No incorpora ICV – Packet Number*
    - *El formato de la cabecera CCMP es similar al de TKIP (combinación IV/IV Extendido)*
    - *La principal diferencia radica en la implementación → se emplea AES y no RC4*



# Seguridad en IEEE 802.11

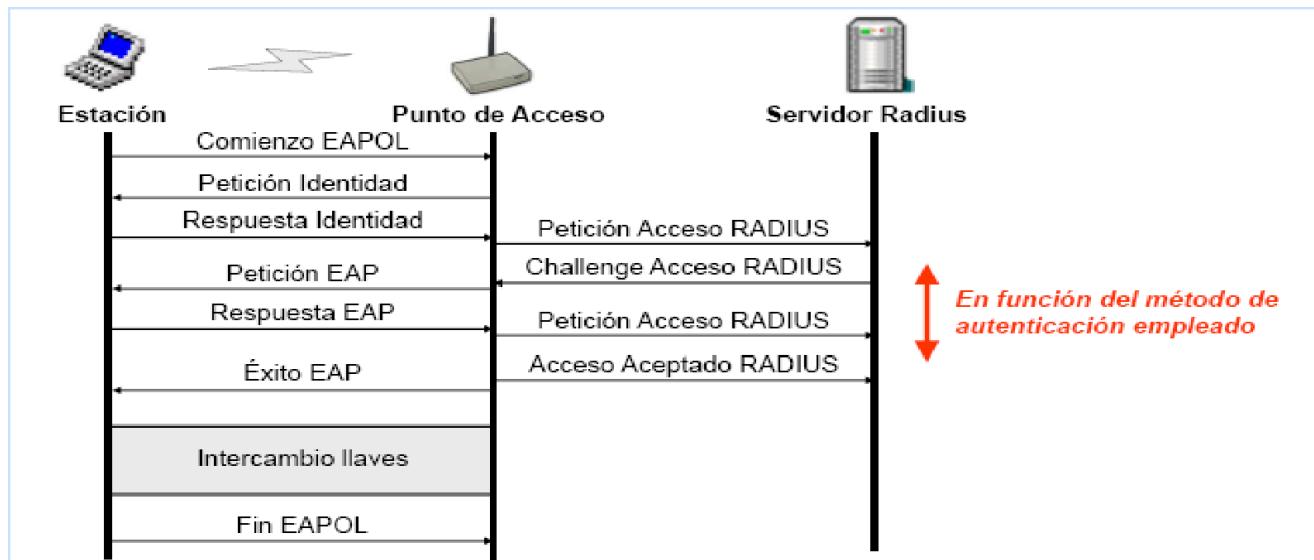
## Seguridad

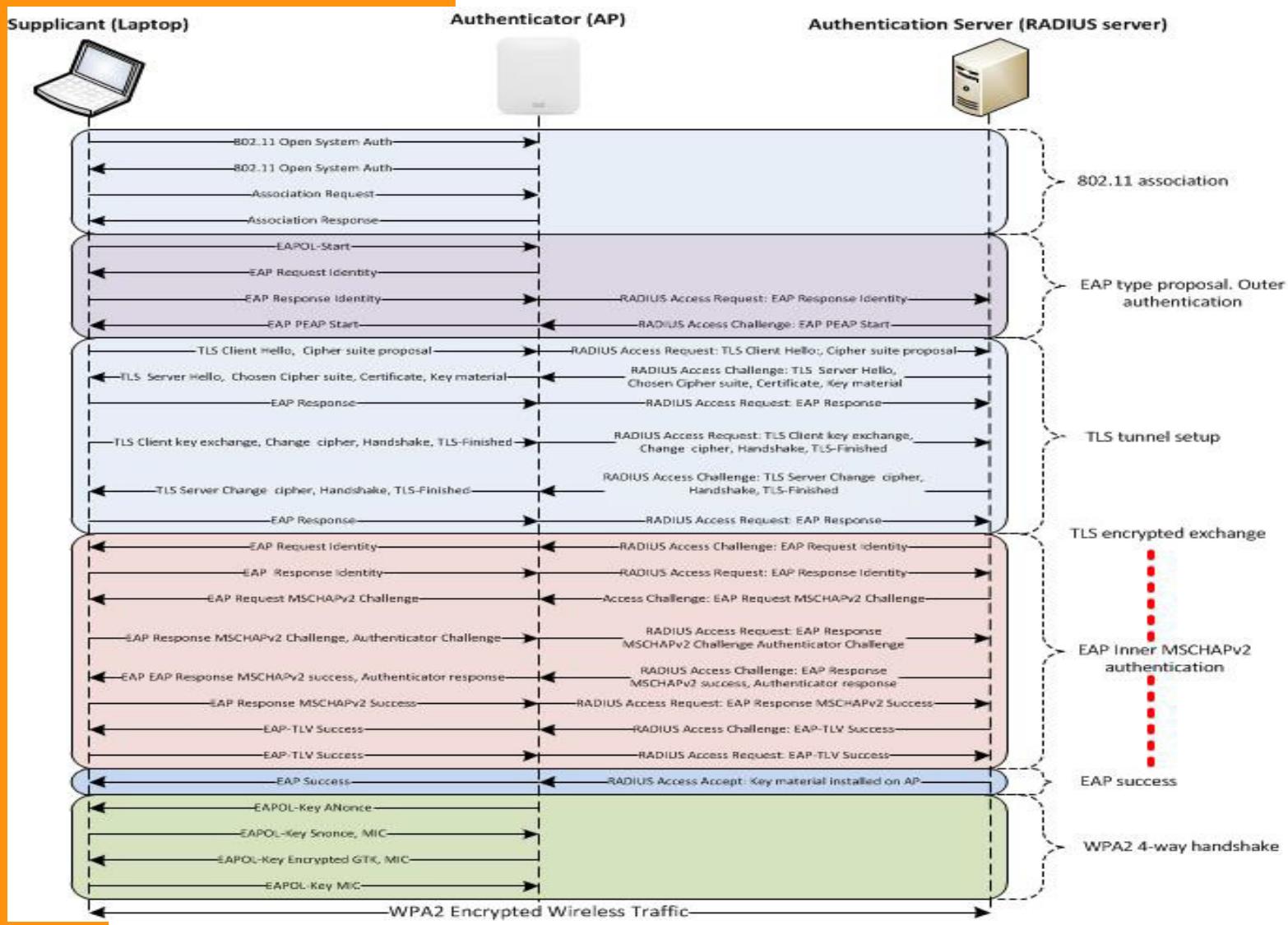
- WPA2-Personal *PSK*
  - Clave secreta compartida
- WPA2-Enterprise
  - Se basa en el Protocolo de Autenticación Extensible (EAP, RFC 2284, RFC3748)
  - Extensión EAP Over LAN (EAPOL), utilizando servidores RADIUS
  - Todas las sesiones de cada usuario se cifran con una clave distinta

# Seguridad en IEEE 802.11

## Seguridad

- *WPA2-Enterprise*





# Calidad de Servicio

802.11e

- *Uno de los principales inconvenientes para el desarrollo de servicios sobre 802.11 es la imposibilidad de fijar una determinada calidad de servicio para una aplicación particular*
- *El retardo, jitter y la pérdida de paquetes en aplicaciones como VoIP or video streaming provocan una calidad de servicio pobre.*
- *En las aplicaciones que son sensibles al tiempo (time sensitive) es necesario priorizar el tráfico (establecer un nivel de prioridad a los paquetes)*
- *IEEE 802.11e ofrece esta priorización*

# Calidad de Servicio

802.11e

- Se redefine la capa MAC

*CSMA/CA*  
*( Distributed Coordination Function )*

- Se mejora DCF y PCF a través de una nueva función de coordinación, HCF (Hybrid Coordination Function)
- HCF define dos métodos de acceso al canal:
  - Enhanced Distributed Channel Access (EDCA)
    - Basado en contención
  - HCF Controlled Channel Access (HCCA)
    - Transferencias en situaciones libres de contención
- En ambos se categoriza el tráfico

# Calidad de Servicio

802.11e

- EDCA
  - Se definen cuatro categorías de acceso (AC) (colas) y 8 prioridades de usuario (UP)
  - Cada AC es una variante de DCF con valores diferentes de la ventana de contención (CW), AIFS (arbitrary inter-frame space) y TXOP (transmission opportunity)
    - AIFS → Intervalo de tiempo entre frames bajo 802.11e
    - TXOP → Intervalo durante el cual una estación puede enviar tantos frames como sea posible
  - Cada paquete procedente de la capa superior se etiqueta con un identificador de prioridad acorde con sus necesidades de QoS

# Calidad de Servicio

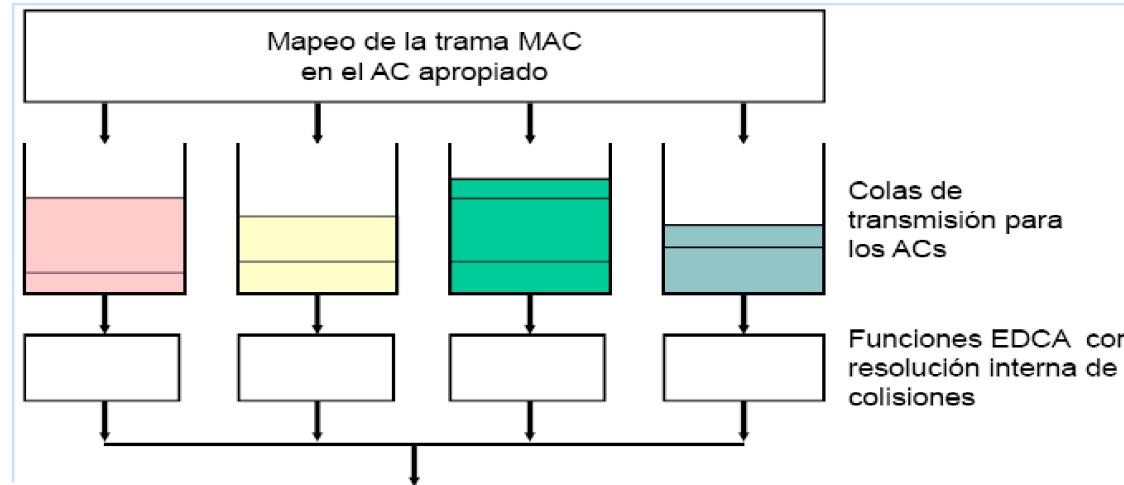
802.11e

- EDCA

BAJA →

↓  
ALTA

Prioridad	UP (como 802.1D)	802.1D	AC <small>Access Categories</small>	Designación
Más baja	1 2	BK --	AC_BK AC_BK	Background Background
	0	BE	AC_BE	Best Effort Best Effort
	3	EE	AC_BE	Video
	4	CL	AC_VI	Video
	5	VI	AC_VI	Voice
	6	VO	AC_VO	Voice
	7	NC	AC_VO	Voice



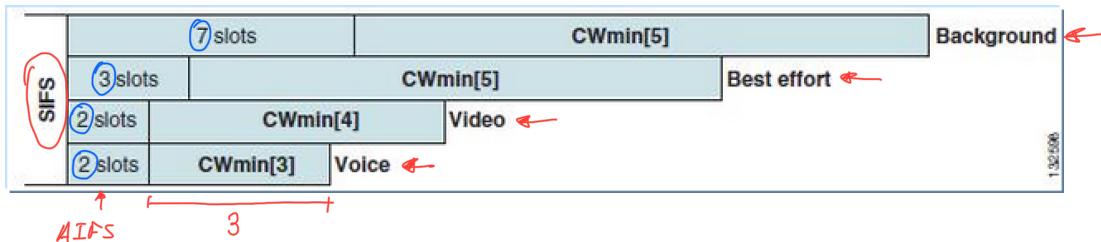
# Calidad de Servicio

802.11e

- EDCA
  - Valores por defecto de cada AC para 802.11g (OFDM)

AC	CWmin	CWmax	AIFS	Max TXOP
Background (AC_BK)	15	1023	7	0
Best Effort (AC_BE)	15	1023	3	0
Video (AC_VI)	7	15	2	3.008ms
Voice (AC_VO)	3	7	2	1.504ms

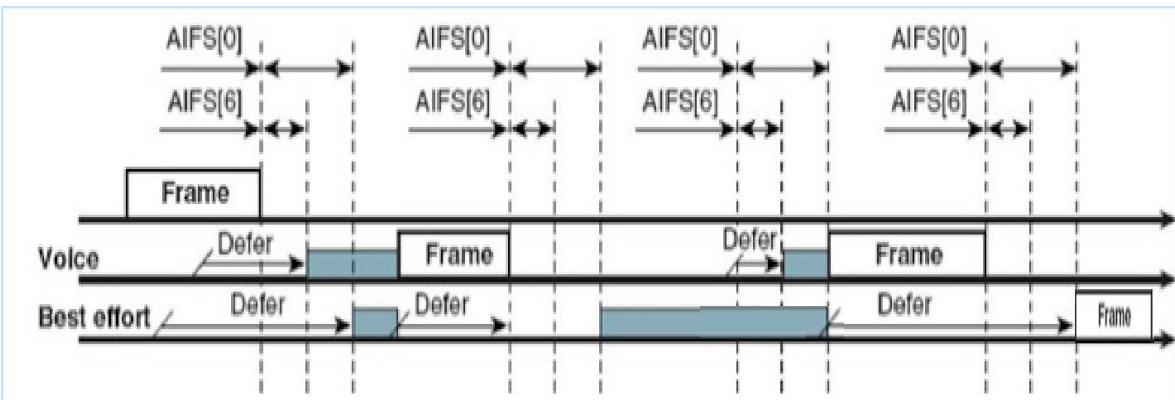
- Menores valores AIFS y de CWmin y CWmax reducen el tiempo de espera



# Calidad de Servicio

802.11e

- EDCA
  - $AIFS[0]$  representa  $UP=0 \rightarrow AC\_BE$
  - $AIFS[6]$  represeta  $UP=6 \rightarrow AC\_VO$
  - Los frames con prioridad baja esperan bastante tiempo



# Calidad de Servicio

802.11e

- *HCCA*
  - Existe un HC (*Hybrid Coordinator*) que tiene mayor prioridad que el resto de las estaciones (normalmente el AP)
  - Presenta ciertas similitudes con PCF, pero:
    - Las tramas pueden transmitirse tanto en periodo libre de contención (CFP) como en periodos de contención (CP)
  - El HC es capaz de asegurar a las estaciones un TXOP determinado
  - El HC tiene una mayor prioridad que las estaciones
    - Espera un tiempo menor para acceder al canal
  - El HC puede establecer (en un beacon) un periodo libre de contención (como en PCF)
  - El HC realiza un *polling* a las estaciones para determinar cuáles tienen datos con mayor prioridad y habilitar sus transmisiones

# Redes Mesh

- *Combinan la topología de red en infraestructura con adhoc*
- *Hay nodos que actúan como relays para los paquetes que proviene de estaciones que están fuera del rango de cobertura de un AP*
- *Necesario utilizar protocolos de enrutamiento para encaminar paquetes*
  - *AODV (Ad hoc On-Demand Distance Vector)*
  - *DSDV(Destination-Sequenced Distance-Vector Routing)*
  - *OLSR(Optimized Link State Routing protocol)*
- *IEEE 802.11s define como crear una red mesh*
  - *Hybrid Wireless Mesh Protocol*

# Redes Mesh

