



# Wireless LANs

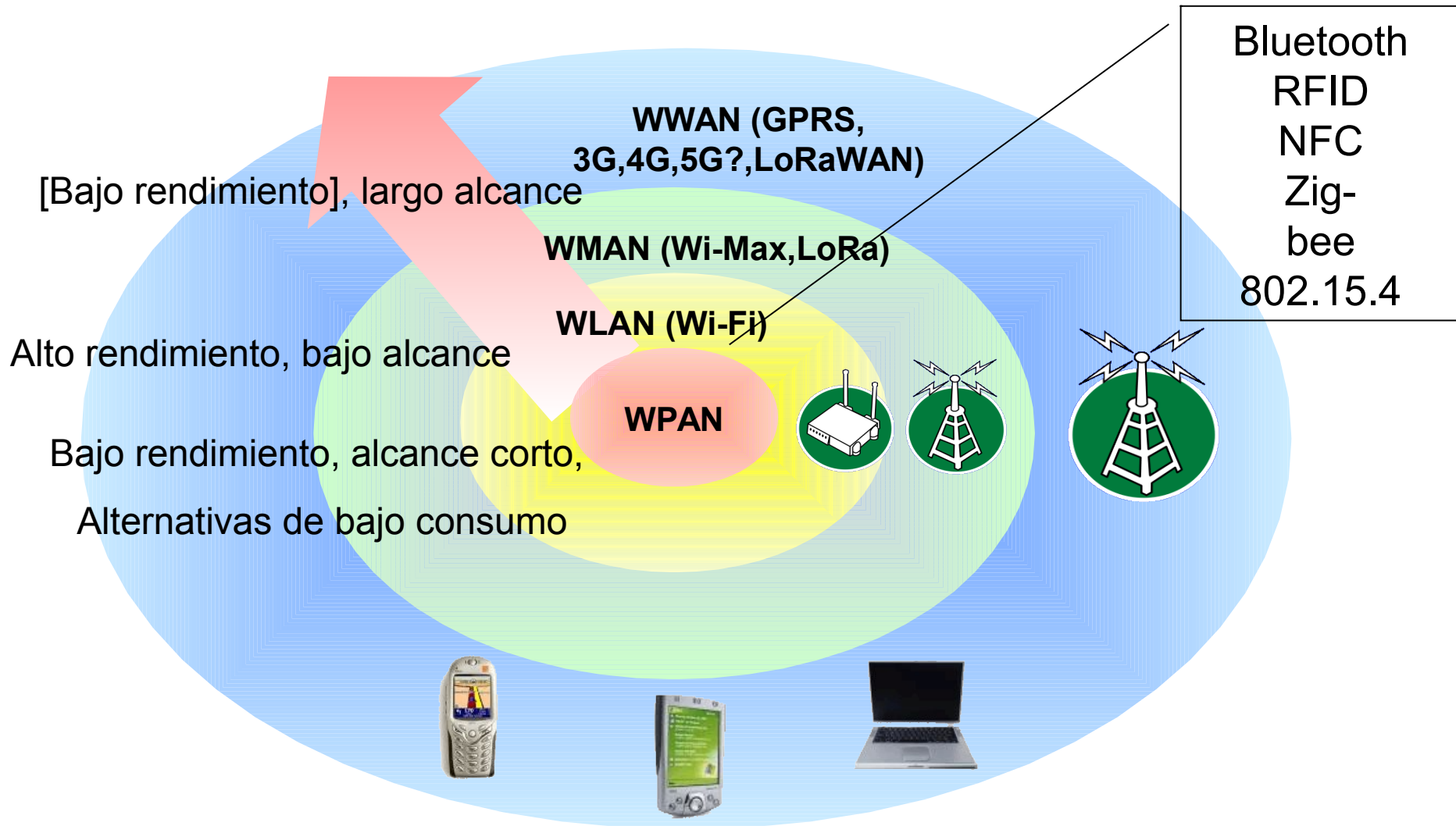
M. Robles, A. Barbieri



# Sistema Wireless LAN

- Sistema de cobertura local (del punto de vista geográfico) en el cual las estaciones se comunican sin estar conectadas directamente mediante un medio físico “cableado/guiado”.
- La información se transmite de forma inalámbrica como ondas electromagnéticas a través del espacio.
- Las ondas electromagnéticas utilizadas se ubican en el espectro de las RF (Radio frecuencias).

# Tecnologías Wireless



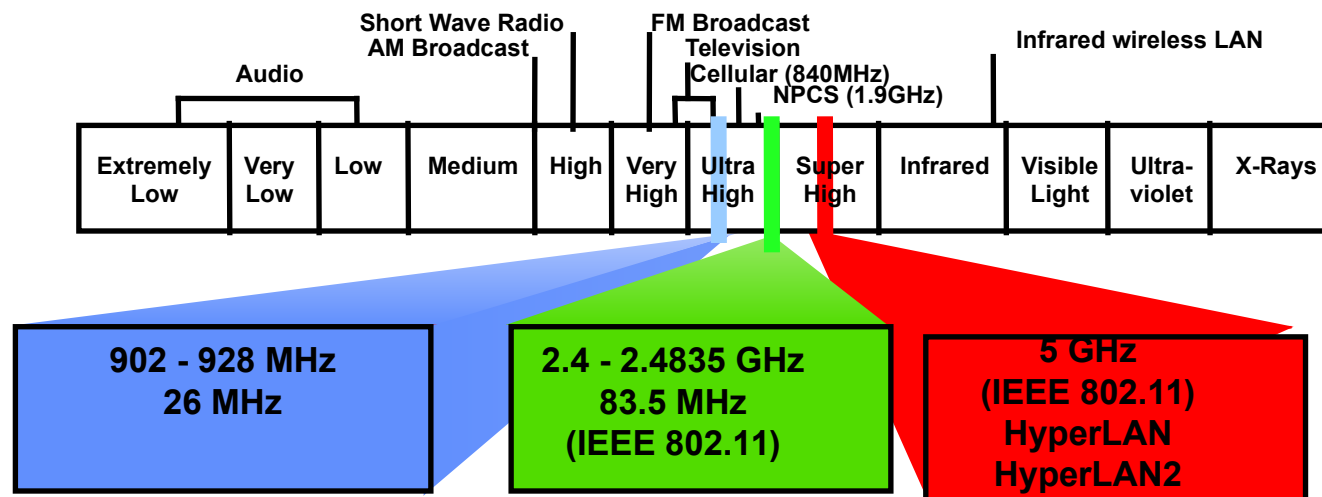


# Historia / Evolución

- 1997 - 802.11 (legacy) - 1 a 2 Mbps – 2,4Ghz e IR.
- 1999 - 802.11a - 54Mbps – 5Ghz. OFDM.
- 1999 - 802.11b - 11Mbps – 2,4Ghz. DSSS.
- 2003 - 802.11g - 54Mbps – 2,4Ghz. OFDM.
- 2004- 802.11i - Seguridad.
- 2005 – 802.11e - QoS.
- 2005 - 802.16 (Wi-MAX).
- 2009 – 802.11n – 300/600Mbps – 2,4-5GHz. OFDM/SMX.
- 2013 – 802.11ac – 500Mbps / 1Gbps - 5GHz.

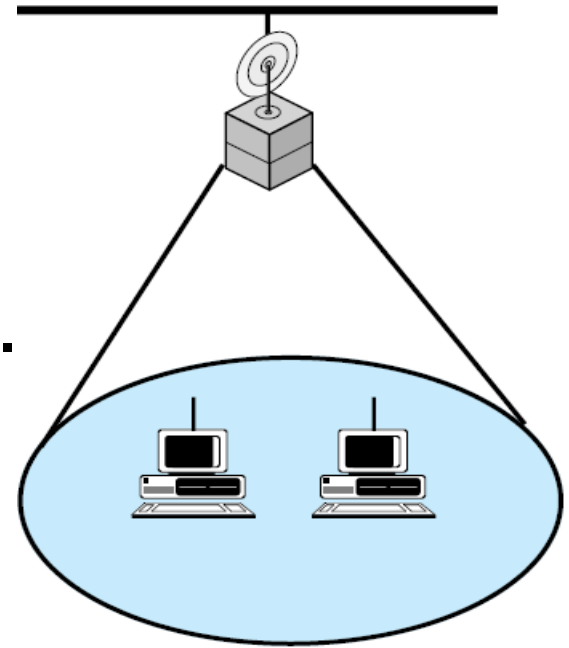
# Fundamentos RF

- 1985: Federal Communications Commission (FCC) habilita la modulación libre spread-spectrum (SS) en ciertas bandas.
- Tres cuerpos regulatorios:
  - FCC: América, Australia, Nueva Zelandia.
  - ETSI: Europa, Africa, partes de Asia.
  - TELEC: Japan.
- Tres bandas no licenciadas: 900MHz, 2,4GHz (conocida como ISM: Industrial, Scientific and Medical) y 5GHz (5.8GHz).



# Componentes WLAN

- Estaciones (terminal stations).
- Transeivers inalámbricos (Placas de red wireless).
- Antenas.
- Espacio por donde se propagan las señales.
- Transeivers concentradores - base stations (Access Points).
- Backbone cableado.





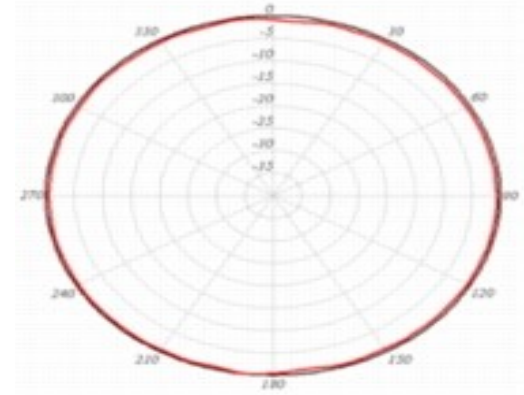
# Antenas

- Convierten la energía eléctrica en ondas de RF (Radio Frecuencia) cuando transmiten, y la operación inversa cuando reciben.
- Dimensión depende de la long. de onda.
- Proveen 3 propiedades a un sistema wireless:
  - Polarización.
  - Ganancia (medida en dBi).
  - Dirección.
- Existen 2 categorías de antenas de acuerdo a dirección:
  - Omni-direccionales.
  - Bidireccionales, Direccionales.

# Antenas Omnidireccionales

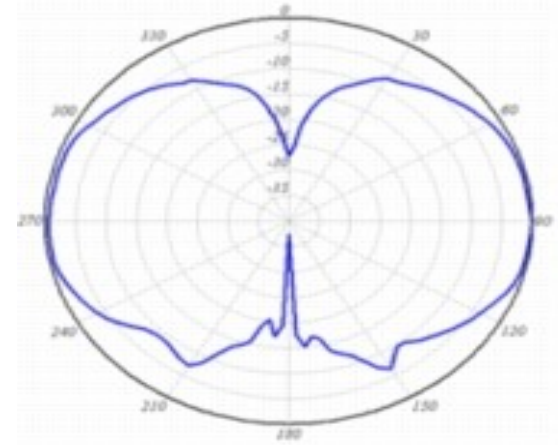
- Plano Horizontal (Patrón Azimuth)

- H-Plane: Y,X.



- Plano Vertical (Patrón de elevación)

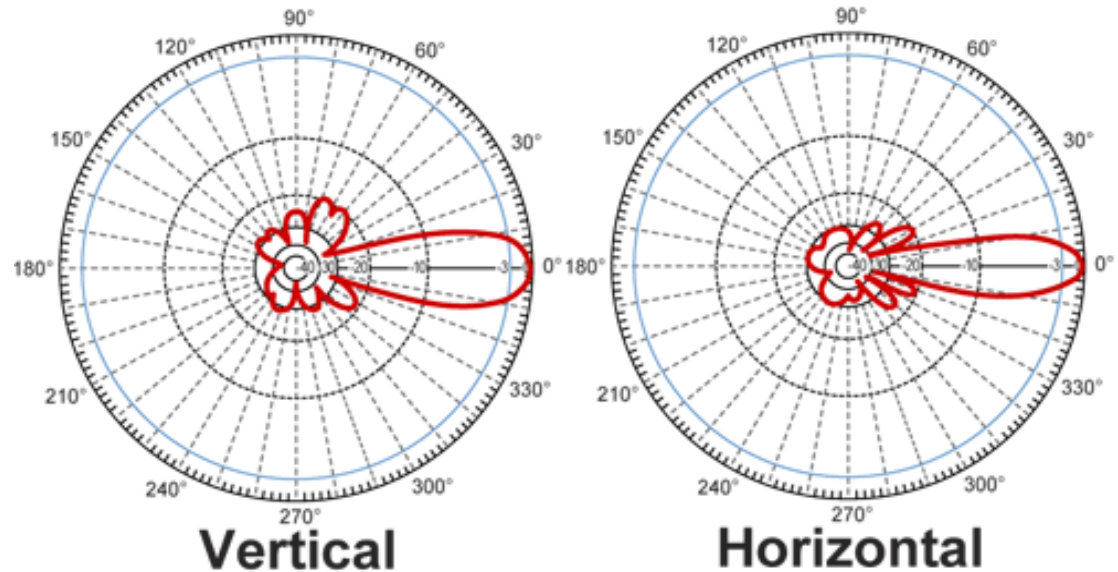
- E-Plane: Z,X Z,Y.





# Antenas Direccionales






- Plano Horizontal (Patrón Azimut)
  - Y,X.
- Plano Vertical (Patrón de elevación)
  - Z,X Z,Y.



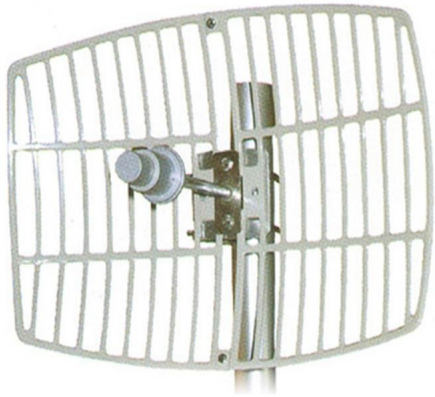
# Antenas Interiores

					
	<b>Rubber dipole</b>	<b>Pillar Mount</b>	<b>Patch Wall</b>	<b>Ceiling Mount</b>	<b>Ceiling Mount High Gain</b>
Type	omni	omni	Directional	omni	omni
Gain	2.15 dBi	5.2 dBi	8.5 dBi	2.2 dBi	5.2 dBi
Beamwidth	360° H 75° V	360° H 75° V	60° H 55° V	360° H 75° V	360° H 75° V
Indoor Range at 1Mbps	300' 91.4 m	497' 151.5 m	700' 213.4 m	350' 106.7 m	497' 151.5 m
Indoor Range at 11Mbps	100' 30.5 m	142' 43.3 m	200' 61 m	100' 30.5 m	142' 43.3 m
Cable Length	N/A	3' 0.9 m	3' 0.9 m	9' 2.7 m	3' 0.9 m

# Antenas Exteriores

					
	<b>Patch Wall</b>	<b>Mast Mount</b>	<b>High Gain Mast Mount</b>	<b>Yagi Mast</b>	<b>Solid Dish</b>
<b>Type</b>	Directional	omni	omni	Directional	Directional
<b>Gain</b>	8 dBi	5.2 dBi	12 dBi	13.5 dBi	21 dBi
<b>Beamwidth</b>	60° H 55° V	360° H 75° V	360° H 7° V	30° H 25° V	12.4° H 12.4° V
Approximate Range at 1Mbps	2.0 Miles 3.2 km	5000' 1.5 km	4.6 Miles 7.4 km	6.5 Miles 10.5 km	25 Miles 40.2 km
Approximate Range at 11Mbps	3390' 1 km	1580' 0.5 km	1.4 Miles 2.3 km	2.0 Miles 3.2 km	11.5 Miles 18.5 km
<b>Cable Length</b>	3' 0.9 m	3' 0.9 m	1' 0.3 m	1.5' 0.5 m	2' 0.6 m

# Antenas Exteriores



Grid (parrilla)

omni



yagui

dish (plato)

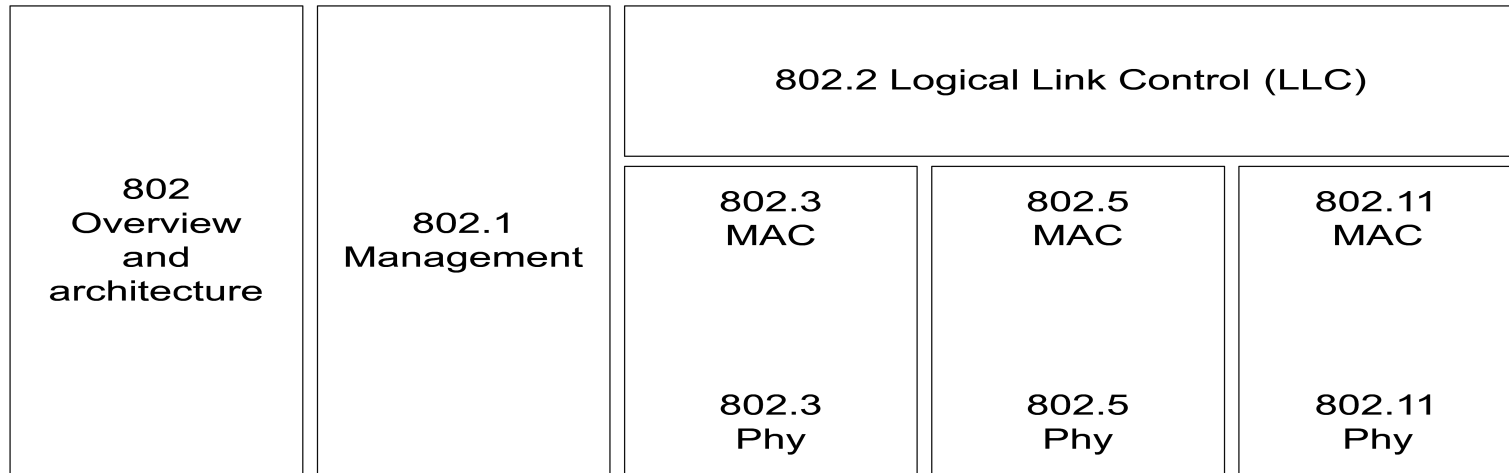




# Características de IEEE 802.11

- 802.11 es una familia de estándares.
- No es un reemplazo de las redes cableadas.
- Similar a 802.3 (Ethernet).
- Usan radio frecuencias e infrarrojos (luego eliminados de implementaciones del estándar).
- Funcionan en bandas no licenciadas (depende del país).
- Permite la movilidad de los usuarios.
- De rápida implementación.

# Características, Modelo en Capas



- Ocupa las dos capas inferiores del modelo OSI
- 802.2 LLC igual que para 802.3/803.5



# Identificación de la Red - SSID

- Service Set Identifier.
- Indica el nombre de la red.
- De 2 a 32 caracteres, sensitivo a mayúsculas.
- Obligatorio. Por seguridad, se los suele ocultar.
- Se lo suele llamar ESSID.
- No confundir con el BSSID (MAC del AP).

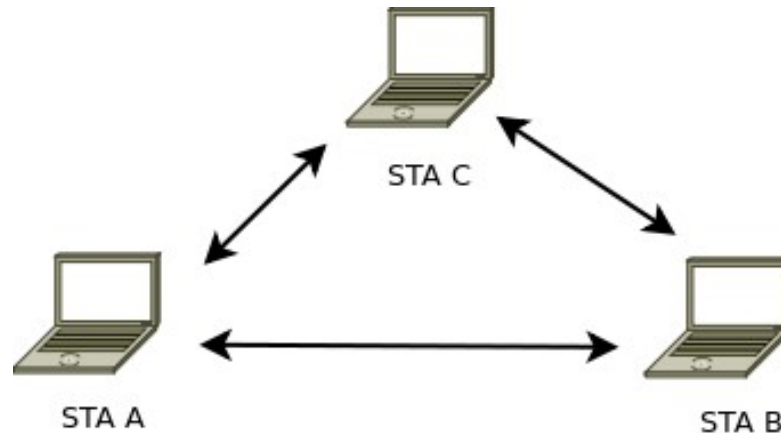


# Topologías de Red

- BSS – Basic Service Set:
  - Independent BSS. IBSS.
  - Infrastructure BSS. BSS.
  - Extended Service Set. ESS.

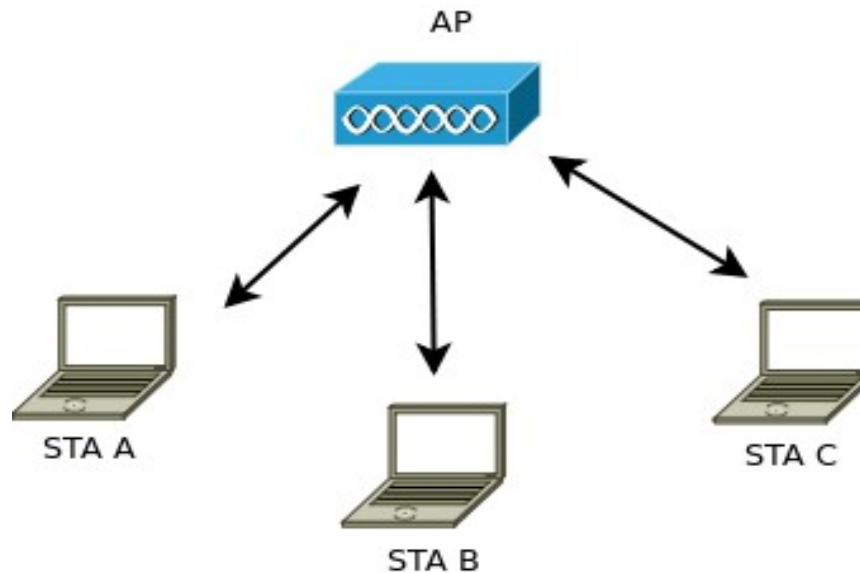


# Topologías de Red - IBSS



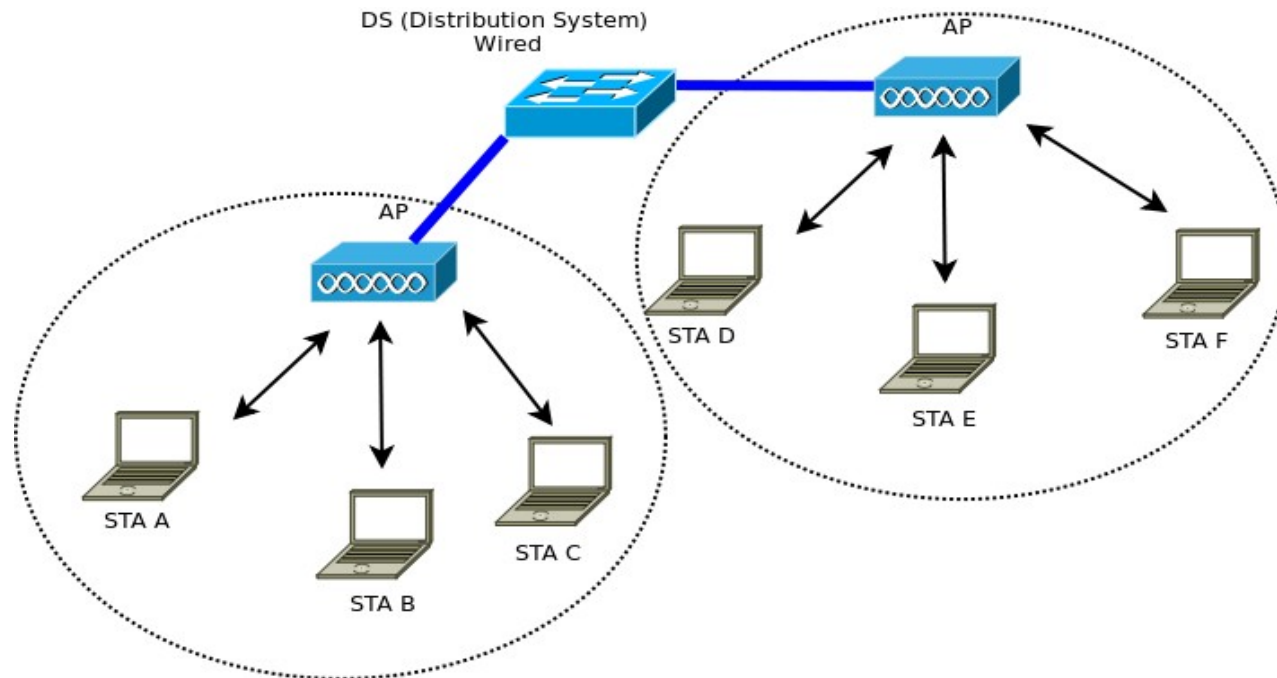
- No se utilizan Access Points.
- También conocidas como redes Ad-Hoc.
- Tiempo de vida limitado o caso especial de redes punto a punto, modo bridge.

# Topologías de Red - Infraestructura BSS



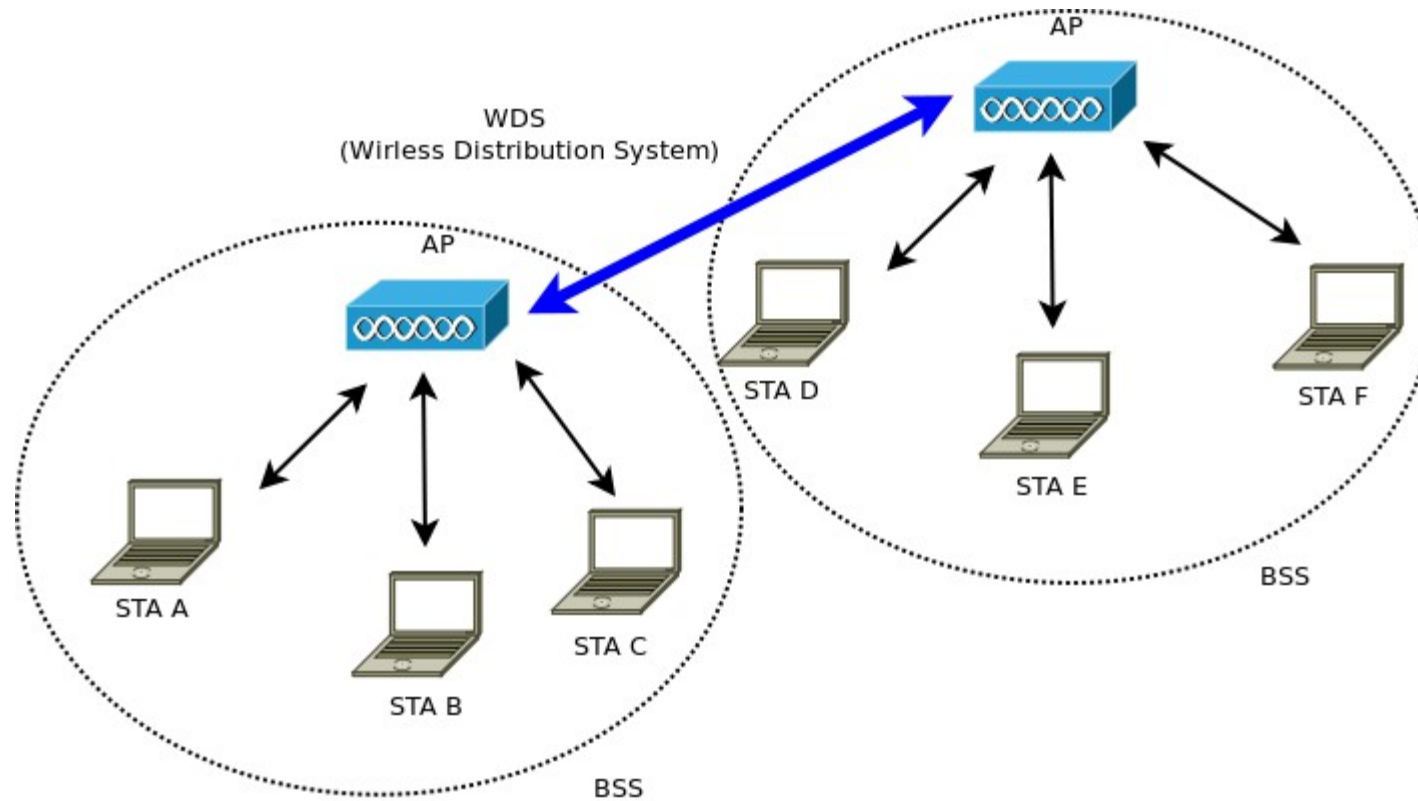
- Requieren el uso de un AP (Access Point).
- AP: hub/switch wireless.
- Algunos AP presentan conexión a la red cableada.
- Las estaciones deben asociarse al Access Point.
- Las estaciones se comunican a través del AP.

# Topologías de Red – ESS



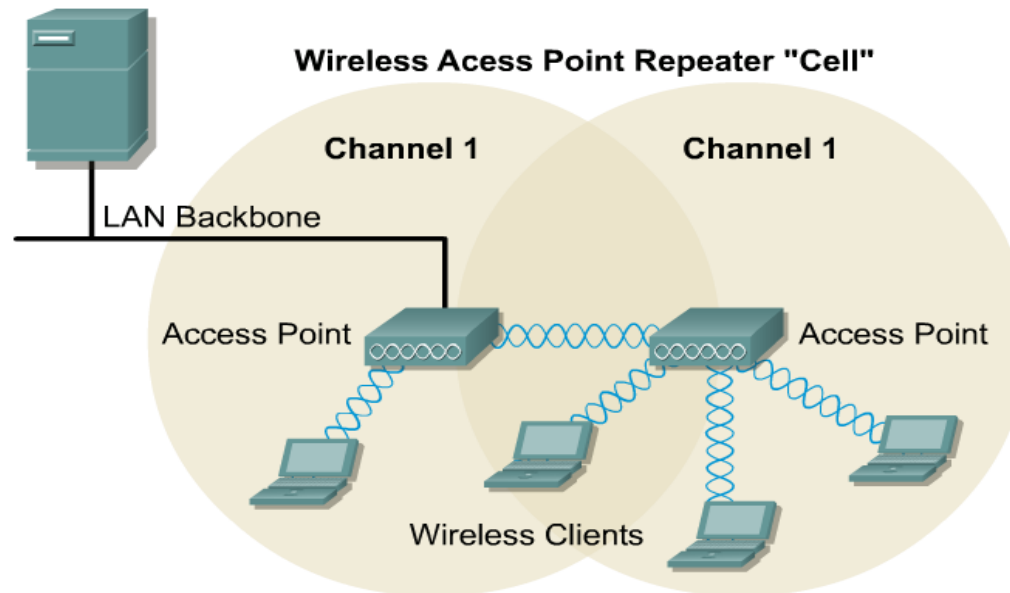
- Se unen varios BSS a través de un backbone, conocido como Distribution System.
- Estaciones se unen a un solo AP.
- AP debe comunicarse entre ellos. Lo pueden hacer vía red cableada o WDS (Wireless Dist. System).

# Topologías de Red – ESS



## ■ WDS

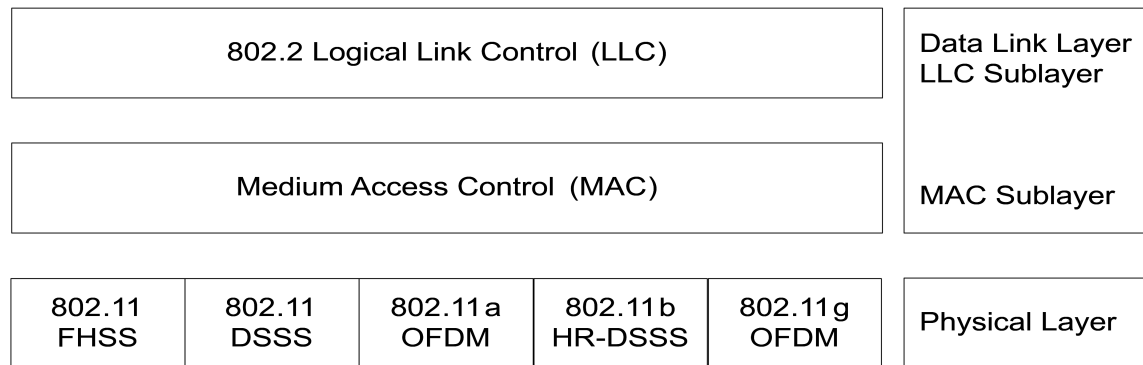
# Topologías de Red - Repetidores



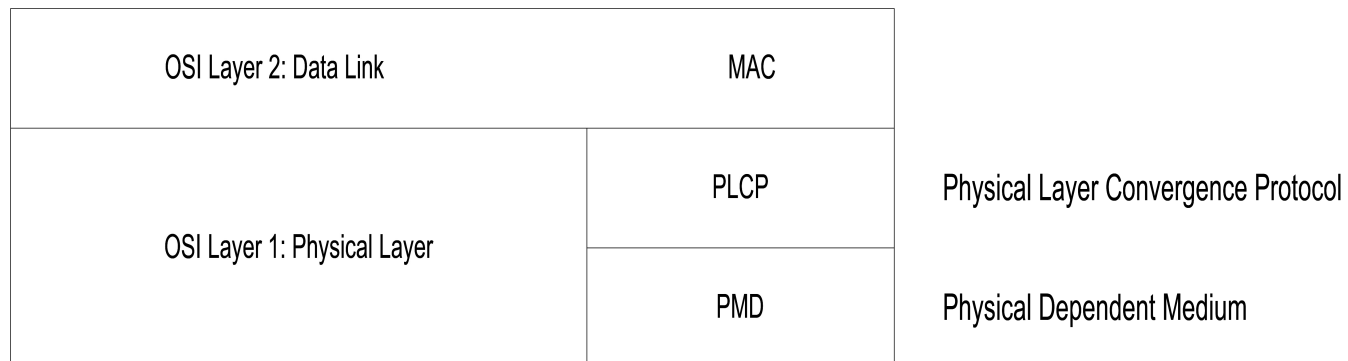
- Repetidor: Access Point no conectado a una red cableada.
- Extiende la red, combate atenuación de la señal.
- AP debe comunicarse entre ellos.
- Se pueden encadenar varios AP. No se recomienda más de 2.

# Capa Física

## ■ 802.11 y sus enmiendas hasta 2003



## ■ Arquitectura



# Capa Física - Canales

2.4 GHz Spectrum	
Channel Number	Channel in GHz
1	2.412
2	2.417
3	2.422
4	2.427
5	2.432
6	2.437
7	2.442
8	2.447
9	2.452
10	2.457
11	2.462

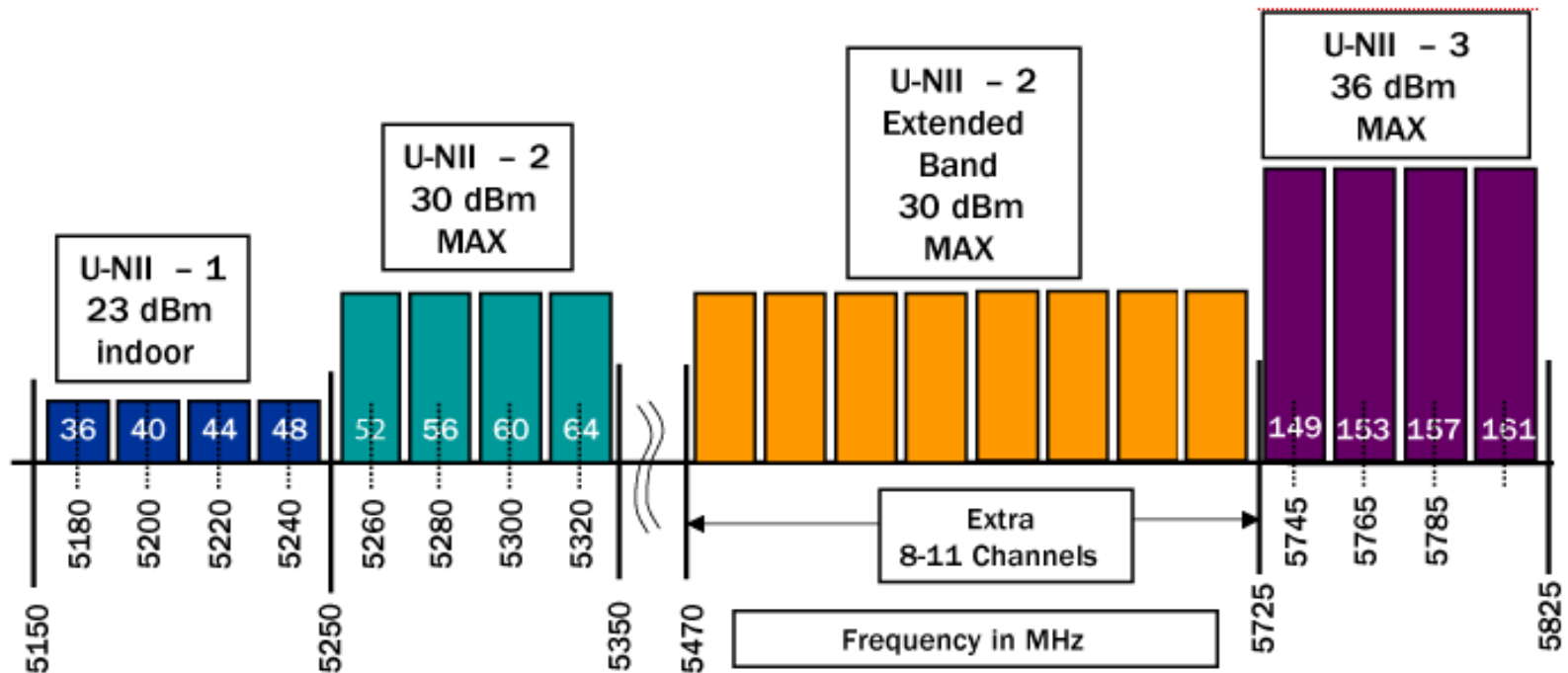
2.4GHz - has 3 non-overlapping channels separated by 20MHz (1, 6 and 11). Using 40MHz channel bonding would require using two of the three available channels.

5 GHz Spectrum	
Channel Number	Channel in GHz
34	5.170
36	5.180
38	5.190
40	5.200
42	5.210
44	5.220
46	5.230
48	5.240
52	5.260
56	5.280
60	5.300
64	5.320
100	5.500
104	5.520
108	5.540
112	5.560
116	5.580
120	5.600
124	5.620
128	5.640
132	5.660
136	5.680
140	5.700
149	5.745
153	5.765
157	5.785
161	5.805
165	5.825

5GHz - has 24 non-overlapping channels separated by 20MHz. This allows up to 12 non-overlapping 40MHz channels.

# Capa Física - Canales

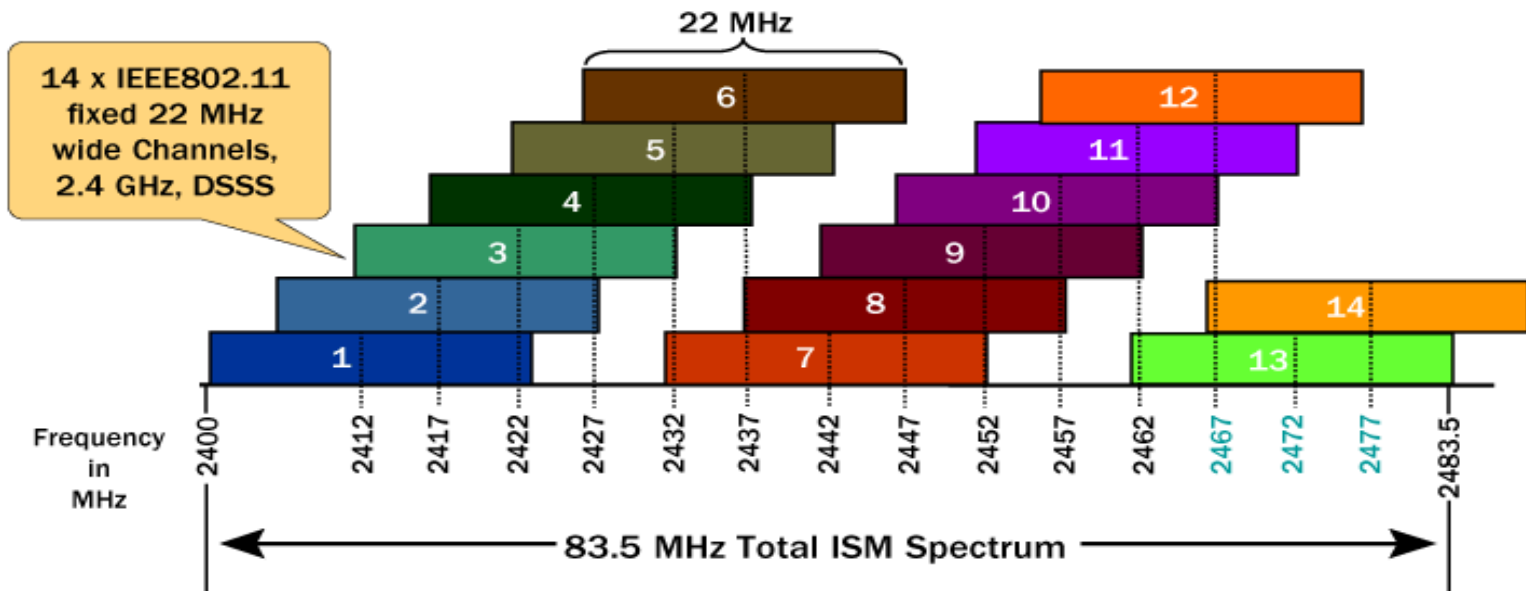
## ■ 802.11a/n/ac





# Capa Física - Canales

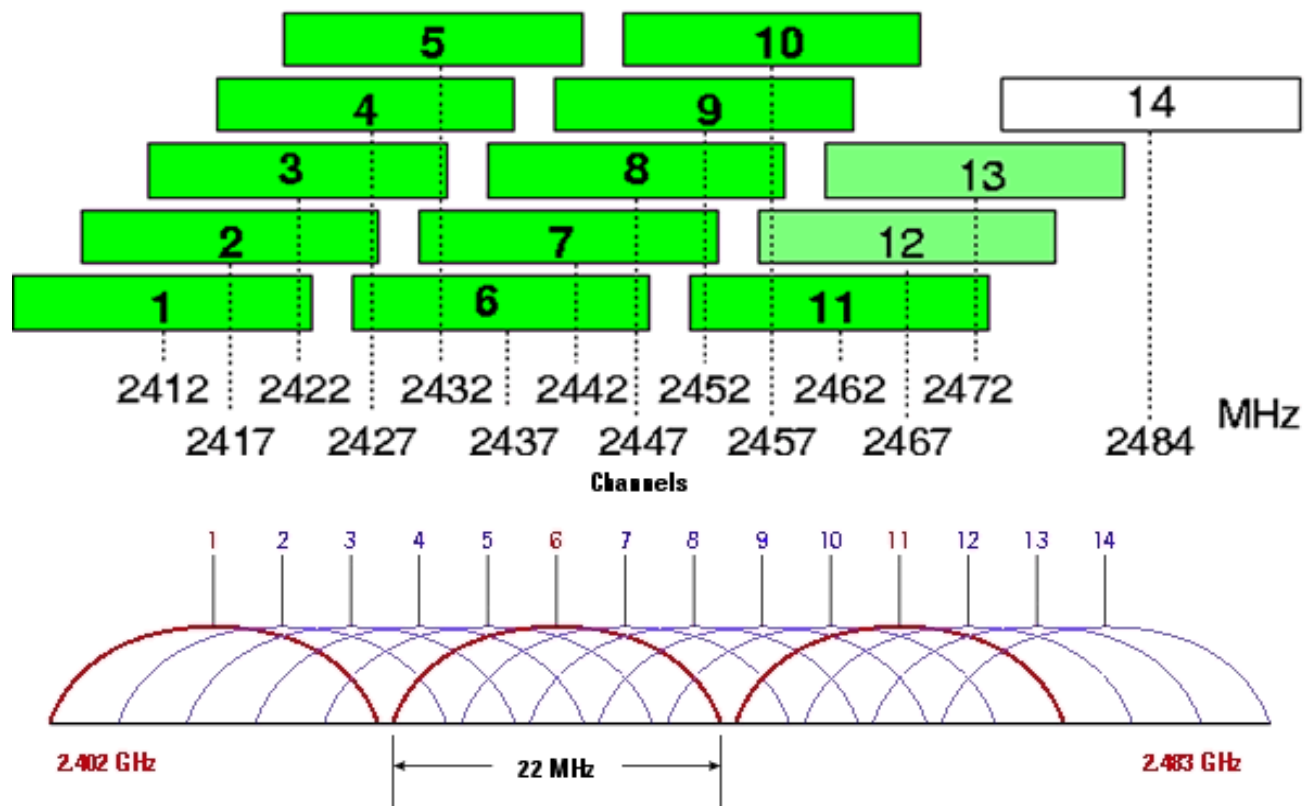
## ■ 802.11b/g/n



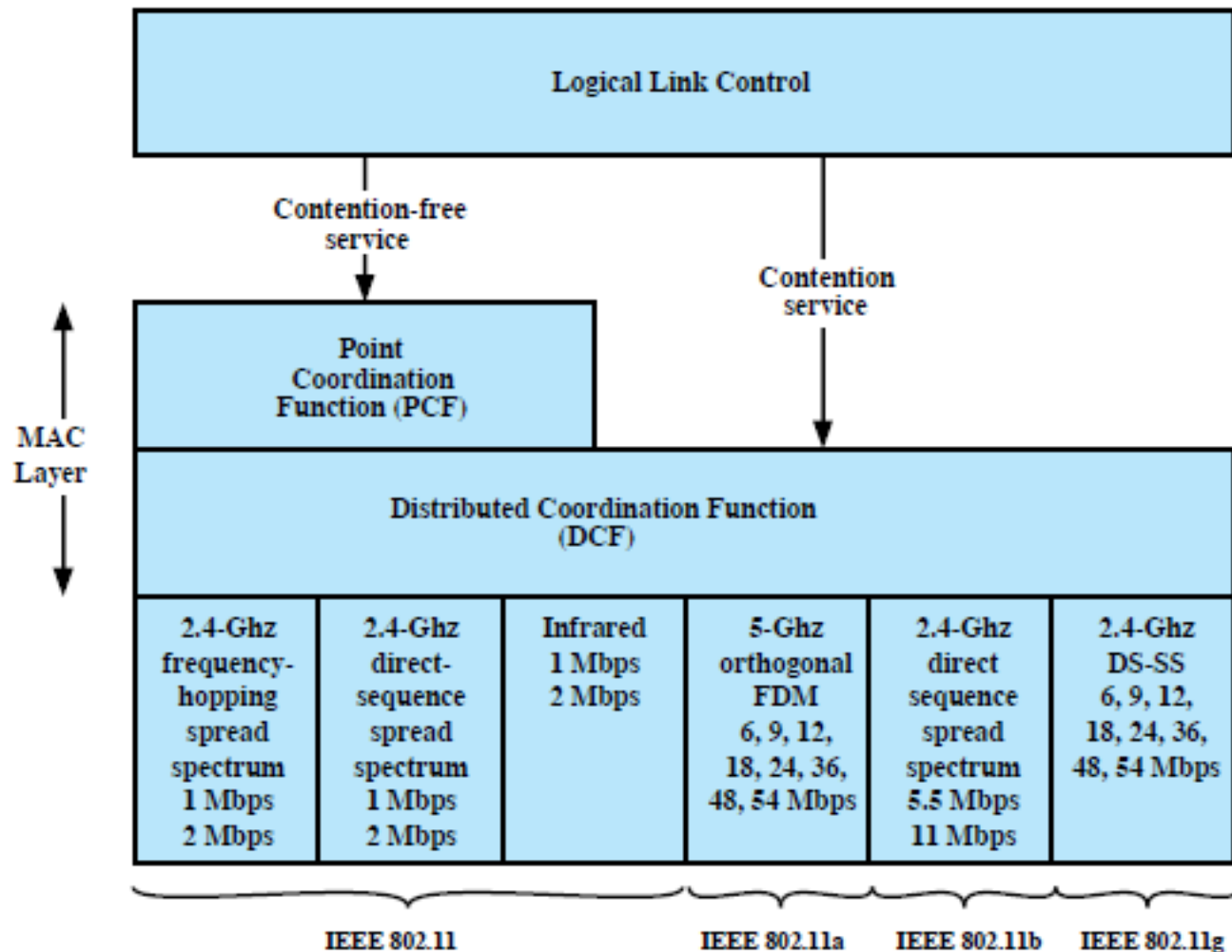
- FCC: 11 canales.
- ETSI: 13 canales.
- TELEC: 14 canales.

# Capa Física - Canales

## ■ 802.11b/g/n

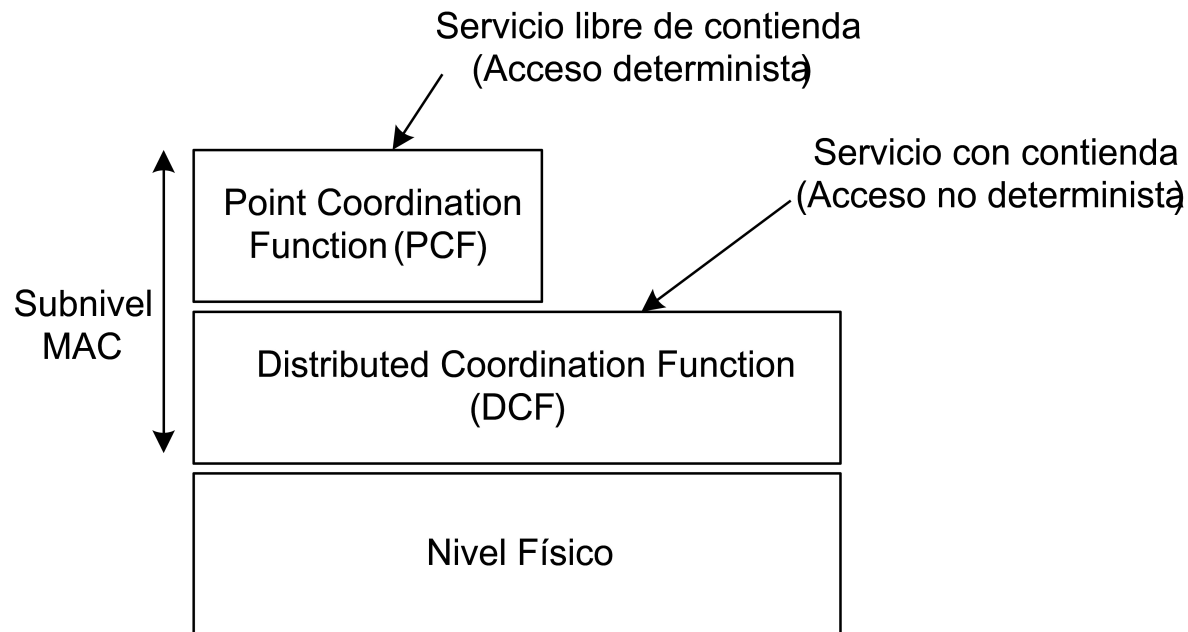


# Arquitectura 802.11



# Acceso al Medio

- Dos mecanismos de acceso al medio:
  - DCF: Distributed Coordination Function.
  - PCF: Point Coordination Function (AP master).





# Acceso al Medio PCF

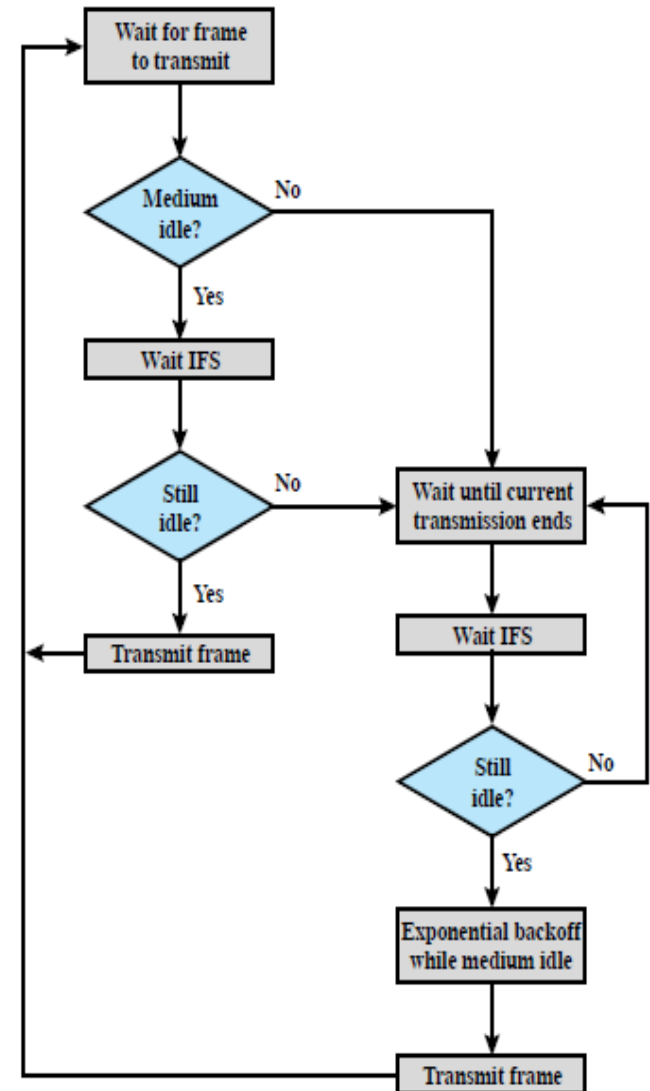
- Algoritmo centralizado.
- Manejado por un master, el AP.
- No tiene contención.
- No implementado en la mayoría de los casos.
- No debe monopolizar el medio, debe dejar lugar a DCF.

# Acceso al Medio DCF - CSMA/CA

- Carrier Sense Multiple Access / Collision Avoidance.
- Acceso al medio con contención, no determinístico, múltiples posibles accesos.
- Algoritmo Distribuido.
- Obligatorio, debe compartir con PCF.
- No detecta colisiones, CD difícil de implementar en medio wireless: HDX, no puede escuchar y enviar al mismo tiempo (la fuerza de la Tx muy superior a la de Rx).

# Acceso al Medio DCF - CSMA/[CA]

- Escucha en el canal
- Si esta libre, espera DIFS y vuelve a escuchar.
- Si sigue libre, Transmite.
- Si esta ocupado (en cualquiera de las 2 circunstancias) activa backoff.
- Luego de Transmitir, debe aplicar backoff también (luego de Ack o tmout).



# Acceso al Medio DCF - Backoff

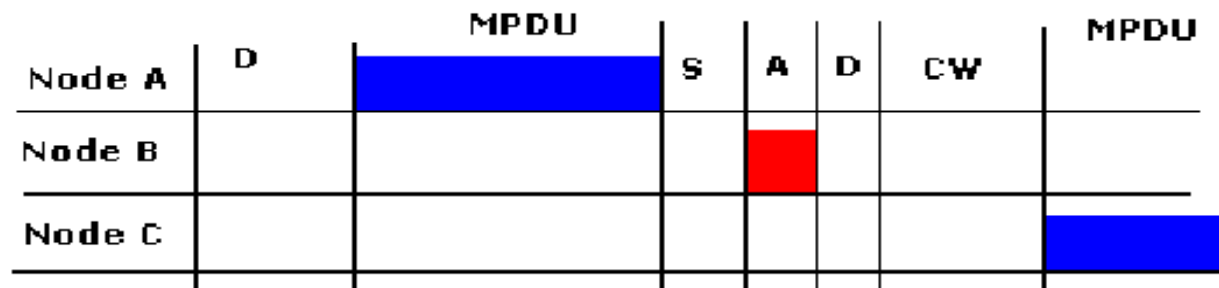
- Similar a Ethernet va aumentando la cantidad de intervalos posibles cada intento fallido (Contention Window size).
- Selecciona de forma aleatoria e incrementa de forma exponencial.
- El tamaño de los slots depende de la velocidad de la estación, más rápida → mas cortos los slots.
- El tamaño máximo de la CW depende de la capa física, para DSSS es de 1024 slots.
- Una vez que se alcanza se mantiene hasta transmitir o dar un error, Reset del CW.
- El timer se decrementa si canal libre, sino se congela.



# Acceso al Medio DCF - CSMA/CA

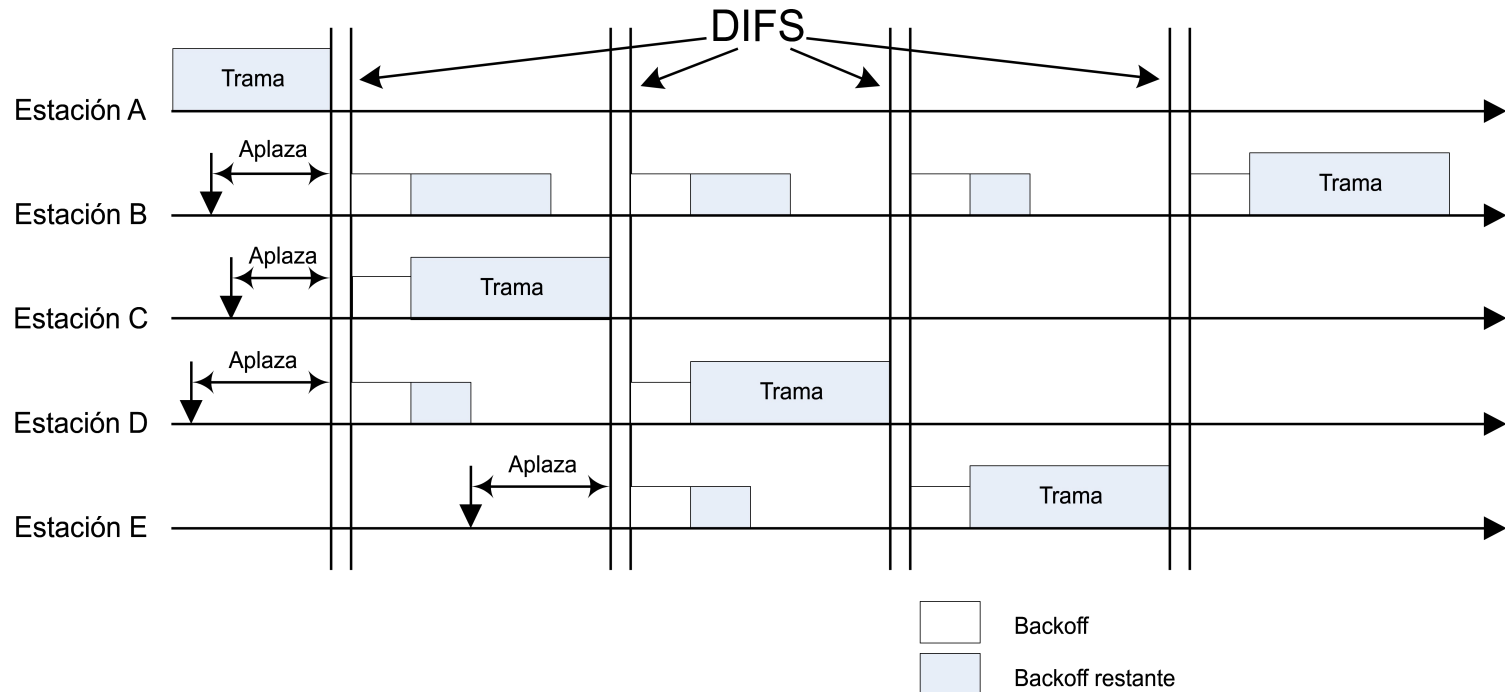
- A diferencia de CSMA/CD el backoff se ejecuta antes de enviar y no luego de detectar la colisión.
- Las colisiones igual existen, se trata de evitarlas.
- Utiliza ACKs, Si no recibe ACK asume que hubo colisión u otro problema , aumenta back-off y vuelve a intentar transmitir.

(CW) Contention Window, (MPDU) Data frame, (D) DIFS Inter Frame Spacing, (A) ACKs, SIFS (S): Short IFS. (P), PIFS (Point coord IFS).

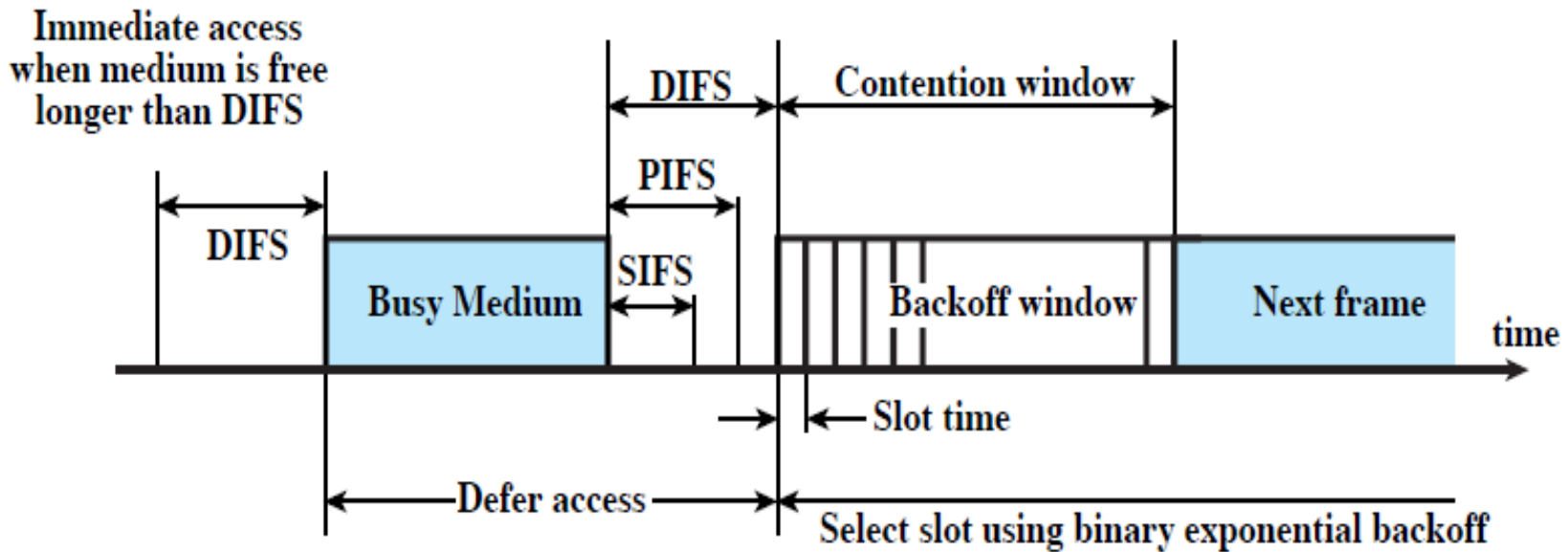


# Acceso al Medio - CSMA/CA

## ■ Ejemplo:



# Accesso al Medio DCF - CSMA/CA





# Acceso al Medio DCF – Carrier Sense

- Formas de Censar el Medio:

- Physical Carrier Sense.
- Virtual Carrier Sense.

- Physical Carrier:

- Difícil de implementar.
- Depende de los fabricantes.
- Pertenece a la capa PMD.

# Acceso al Medio DCF – VCS/NAV

## ■ Virtual Carrier Sense:

- Los frames llevan en el encabezado MAC la duración, del tiempo de: Tx+Spaces+ACKs: NAV (Network Allocation Vector).
- Las estaciones mantienen contadores de cuanto tiempo va a estar ocupado el medio.
- Al ver los NAV actualizan sus contadores.
  - Si el frame no es para la estación.
  - Si el valor es mayor que el NAV local.

## ■ El Virtual Carrier se puede implementar con mensajes de control RTS/CTS.

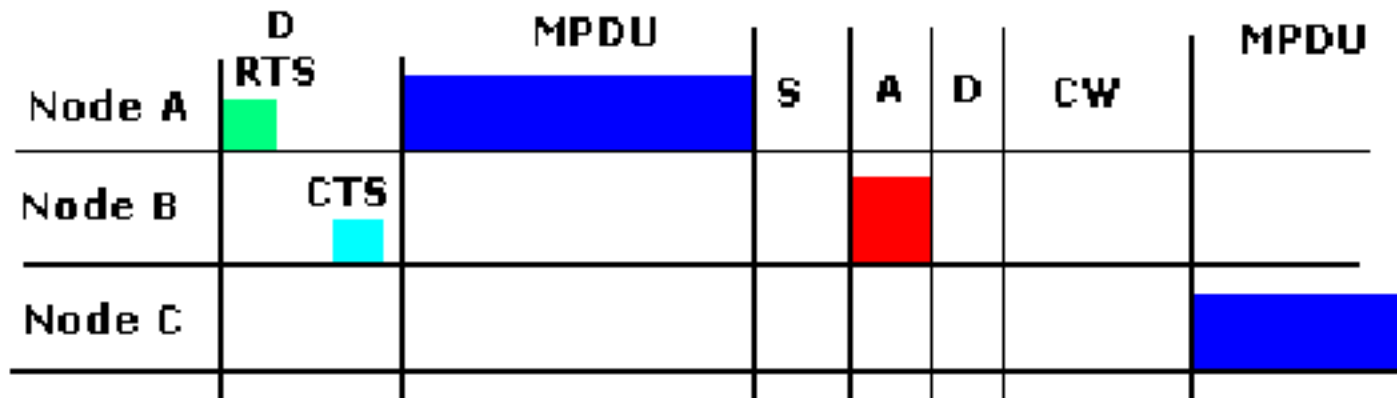


# Acceso al Medio DCF – VCS RTS/CTS

- Virtual Carrier Sense con RTS/CTS
- La estación que desea transmitir puede enviar RTS indicando el NAV.
- La receptora confirmara con CTS.
- Luego podrá enviarse.
- Las demás estaciones observando el RTS o el CTS saben el tiempo de deben esperar.

# Acceso al Medio DCF – Virtual Carrier

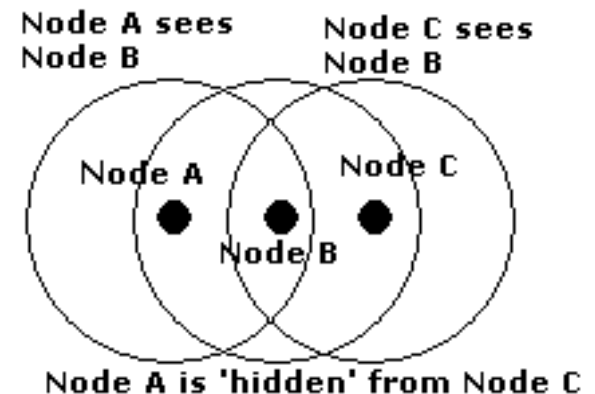
- RTS/CTS reduce las colisiones, pero agrega overhead.
- Usado antes de enviar frames mayores a 2347B.
- CTS to SELF (menor overhead).
- CTS/RTS Resuelve el problema del “hidden node”.



**CSMA/CA with RTS/CTS**

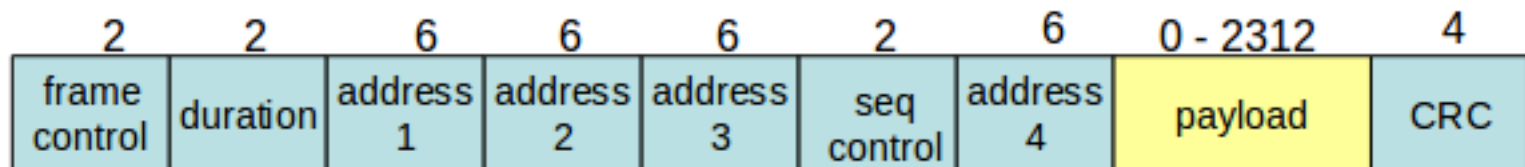
# Problema del Nodo Oculto

- El problema del “hidden node” ocurre cuando en la red hay nodos que no pueden ver las transmisiones de otros.
- “A”, “B” se ven, “C”, “B” se ven. “A”, “C” no se ven.
- CTS/RTS Resuelve el problema del “hidden node”, pues “C” no ve el RTS pero si el CTS que lleva el NAV.
- CTS to SELF no lo resuelve.





# Formato de Trama 802.11 (MAC)



**BSSID:** MAC address of the AP

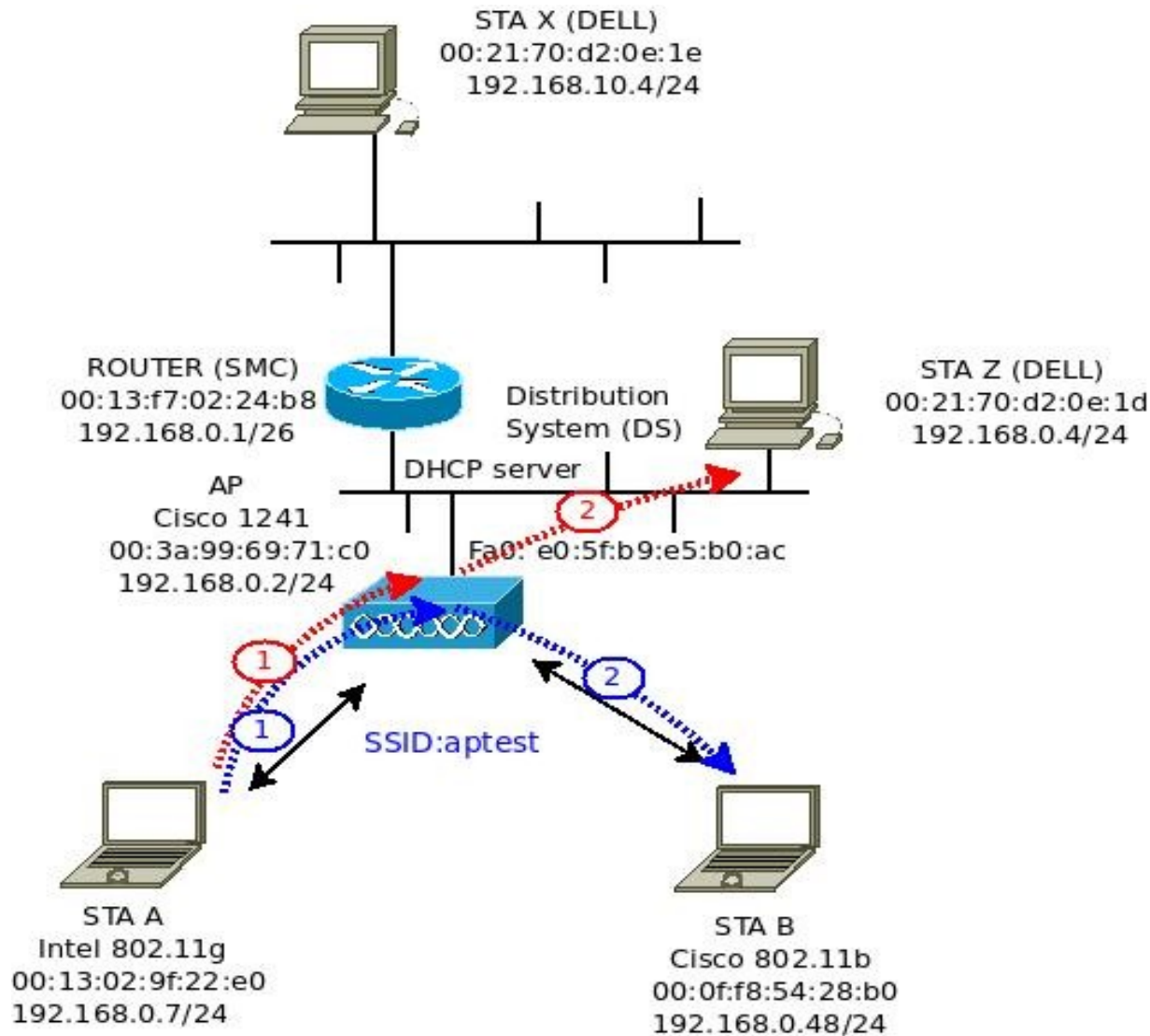
**DA:** MAC address

**SA:** MAC address of wireless host transmitting this frame

**Address 4:** used only in ad-hoc mode. Repeater addr.

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

# Formato de Trama 802.11 (MAC) (Ejemplo)



# Formato de Trama 802.11 (MAC) (Cont.)

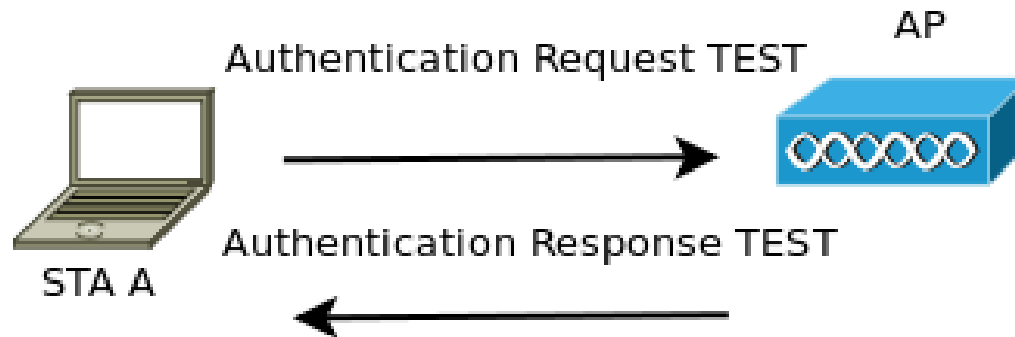
- Frame Control:
  - Versión (por ahora 00).
  - Type/Subtype:
    - Management: Auth, Beacon, Assoc, Probe (00).
    - Control: RTS, CTS, ACK (01).
    - Data: (10).
    - Reserved: (11).
  - Fragmentación.
  - Seguridad WEP.
  - Power Management.



## 802.11 - Funcionamiento

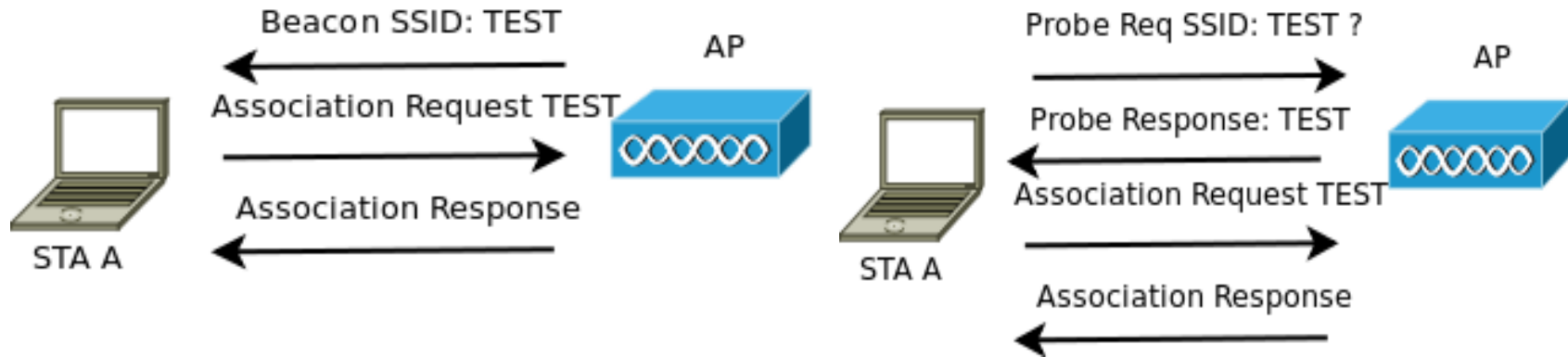
- AP envía frames Beacons continuamente.
- Probe Request/Probe Response.
- Autenticación (puede ser mutua).
- Asociación/Re-asociación.
- Intercambio de datos.
- De-autenticación.

# Seguridad Wireless: Autenticación



- 802.11 define dos tipos de autenticación:
  - Open system (sin autenticación).
  - Shared Key.
- 802.11i:
  - Pre-Shared Key. PSK (Personal Shared Key).
  - 802.1X (EAPoL, EAP, Radius).
  - Podrían usarse certificados.


# Asociación



- Proceso por el cual una estación se une a un AP.
- Solo se realiza en redes infraestructura.
- Permite saber a que AP está unida una estación.
- Previo a la asociación esta la autenticación.

# Seguridad Wireless: Cifrado

- WEP (Wired Equivalent Privacy)
  - Estándar original: WEP (Wired Equivalency Privacy).
  - Clave 40 bits. Fabricantes agregaron clave 104 bits.
  - Basado en RC4. Protocolo simétrico.
  - Crackeado en 2001.
- WPA
  - Usa: TKIP: Temporal Key Integrity Protocol.
  - Adoptado por la certificación WPA (Wi-Fi Protected Access).
  - Soluciona las debilidades de WEP.
- WPA2 802.11i.
  - Utiliza AES o TKIP.



# Seguridad - Evolución

## ■ TSN / WPA

- Diseñado alrededor de WEP.
- No requiere nuevo hardware.
- Autenticación: 802.1X y Pre-Shared Key.
- Soporta un único estándar de encriptación: TKIP.
- Integridad: algoritmo Michel.

## ■ WPA 2

- Diseñado desde el principio.
- Requiere nuevo hardware para soportar nuevos métodos de encriptación
- Autenticación: 802.1X, Pre-Shared Key y Certificados.
- Soporta opciones de encriptación: TKIP y AES.



# Características de los Estándares

- 802.11: FHSS, DSSS, 2.4GHz (1-2Mbps)
- 802.11b: DSSS, 2.4GHz, coding: Baker11, CCK, mod: DBPSK, DQPSK (diferencial) (1-2-5.5-11Mbps).
- 802.11a: OFDM, 5.0GHz, coding: conv. Mod: BPSK, QPSK, 16QAM, 64QAM (1-2-5.5-11-6-9-12..54Mbps).
- 802.11g: DSSS, OFDM, 2.4GHz, Barker11, CCK, mod: DBPSK, DQPSK (1-2-5.5-11-6-9-12..54Mbps).

# Compatibilidad 802.11b y 802.11g

- 802.11g debe soportar short preamble y long preamble.
- 802.11g puede trabajar con OFDM o HR-DSSS.
- 802.11b solo DSSS.
- Los Beacons de los AP 802.11g indican:
  - Non-ERP-Present: si NO hay equipos 802.11b.
  - Use-Protection: debe usar RTS/CTS pues algún AP vio equipo 802.11b.
- Los Beacons, RTS/CTS se envían en DSSS.



# Referencias:

Cisco CCNAv3.1.

Data & Computer Communications (6th Edition),  
William Stallings.

Computer Networks (4th. Edition), Andrew  
Tanenbaum.

<http://www.ieee802.org/>

Wikipedia.

<http://www.zytrax.com/tech/wireless>