

Wireless LANs - IEEE 802.11

Fac. Informática – UNLP

2020



UNIVERSIDAD
NACIONAL
DE LA PLATA

Contenidos

1 Introducción a WLAN

- Objetivos y Estándares
- Componentes Físicas de una WLAN

2 IEEE 802.11: Capa Física

- Capa Dependiente del Medio Físico: PMD
 - Frecuencias Seleccionadas

3 IEEE 802.11: Capa MAC

- Tipos de Redes Wireless
- Identificación del Basic Service Set
- Modos de Acceso al Medio
- Tramas MAC 802.11

Contenidos

1 Introducción a WLAN

- Objetivos y Estándares
- Componentes Físicas de una WLAN

2 IEEE 802.11: Capa Física

- Capa Dependiente del Medio Físico: PMD
 - Frecuencias Seleccionadas

3 IEEE 802.11: Capa MAC

- Tipos de Redes Wireless
- Identificación del Basic Service Set
- Modos de Acceso al Medio
- Tramas MAC 802.11

Contenidos

1 Introducción a WLAN

- Objetivos y Estándares
- Componentes Físicas de una WLAN

2 IEEE 802.11: Capa Física

- Capa Dependiente del Medio Físico: PMD
 - Frecuencias Seleccionadas

3 IEEE 802.11: Capa MAC

- Tipos de Redes Wireless
- Identificación del Basic Service Set
- Modos de Acceso al Medio
- Tramas MAC 802.11

Estamos en:

1 Introducción a WLAN

- Objetivos y Estándares
- Componentes Físicas de una WLAN

2 IEEE 802.11: Capa Física

- Capa Dependiente del Medio Físico: PMD
 - Frecuencias Seleccionadas

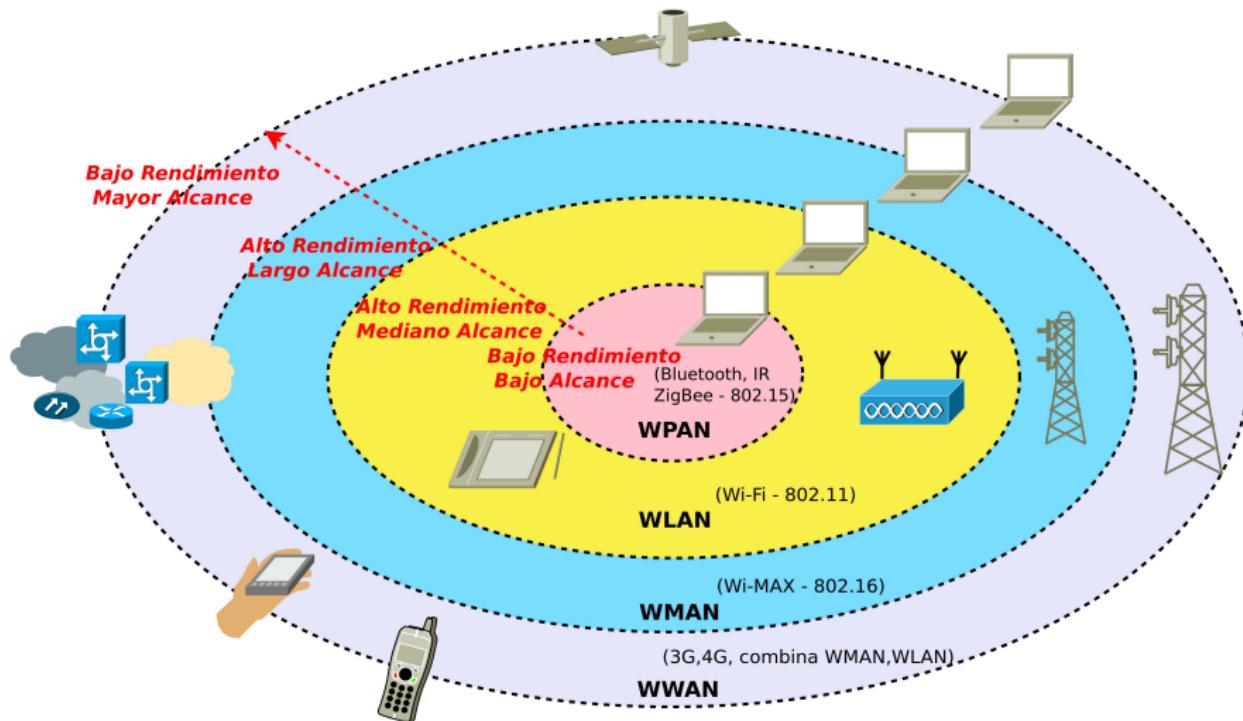
3 IEEE 802.11: Capa MAC

- Tipos de Redes Wireless
- Identificación del Basic Service Set
- Modos de Acceso al Medio
- Tramas MAC 802.11

Tecnologías Wireless

- Las redes wireless han tenido un importante crecimiento.
- Se han llevado a todos los ámbitos, a todos los alcances, con diferentes prestaciones.
- Continuamente se van renovando acorde a la evolución y necesidades.
- Surgen estándares y tecnologías apropiadas para cada requerimiento.
- Una de las organizaciones encargada de generar los estándares WLAN es la IEEE.
- En estos “slides” se cubren redes WLAN, en particular el conjunto de estándares IEEE 802.11.

WLAN dentro de Tecnologías Wireless



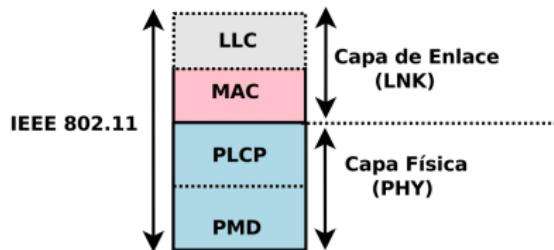
Objetivos y Características

- El conjunto 802.11 **NO** es un reemplazo de las redes cableadas.
- Es una alternativa a evaluar ante la necesidad de conectividad local.
- Funcionalidad similar a 802.3/Ethernet (llamada Wireless Ethernet).
- Funcionan sobre medios no guiados, mayormente Radio-Frecuencias (RF) en bandas “No Licenciadas”.
- Permitir la movilidad de los usuarios y alcance a lugares de difícil acceso para una instalación.
- Permiten un tiempo de puesta en marcha más corto que una LAN cableada.
- Hoy en día el rendimiento es inferior al de una LAN cableada:

$200Mbps(max) < 1Gbps, 10Gbps$

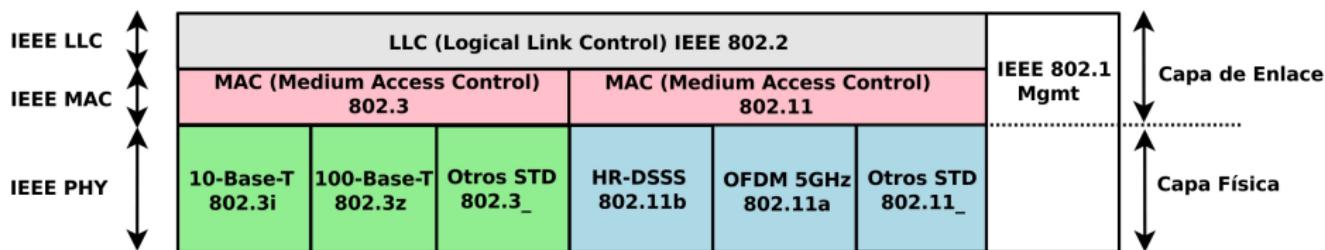
Estándares y Modelo OSI

- Protocolos estandarizados por IEEE 802.11, abarcan las dos primeras capas del modelo OSI.
- Las capas se sub-dividen en sub-capas:
 - 2.2) Sub-capa de Control Lógico de Enlace (LLC - Logical Link Control).
 - 2.1) Sub-capa de Acceso al Medio (MAC - Medium Access Control).
 - 1.2) Sub-capa Física de Procedimientos de Convergencia (PLCP - Physical Layer Convergence Procedure).
 - 1.1) Sub-capa Asociada al Medio (PMD - Physical Media Dependent).



Estándares y Modelo OSI (Cont.)

- A nivel de enlace, la capa superior, LLC (Logical Link Control), es 802.2 de forma idéntica como 802.3 u 802.5.



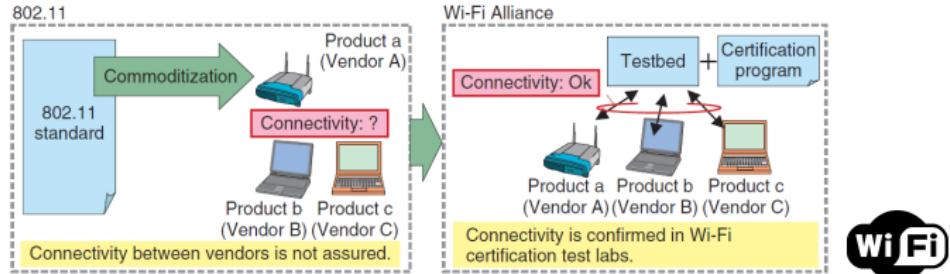
Historia de WLAN-802.11

- Evolución de acuerdo a los años:

- 1997: 802.11 - 1 a 2 Mbps - 2,4Ghz, IR
- 1999: 802.11a - 54Mbps - 5Ghz
- 1999: 802.11b - 11Mbps - 2,4Ghz
- 2003: 802.11g - 54Mbps - 2,4Ghz
- 2004: 802.11i - Seguridad (implementada como WPA2)
- 2005: 802.11e - QoS
- 2005: 802.16 - WiMAX
- 2007: 802.11-2007 (agrupa: 802.11a, b, d, e, g, h, i, j) (d: World-Mode, h: DFS, TPC, j: 5GHz en Japón)
- 2009: 802.11n (Wi-Fi4, 2.4GHz, 5GHz, 300Mbps, 600Mbps)
- 2013,2014: 802.11ac (Wi-Fi5, 5GHz, 1.3Gbps)
- 2016: 802.11ad (60GHz, 7Gbps)
- 201?: 802.11ax (Wi-Fi6, 2.4GHz, 5GHz y otras, 10Gbps)

Certificaciones Wi-Fi Alliance

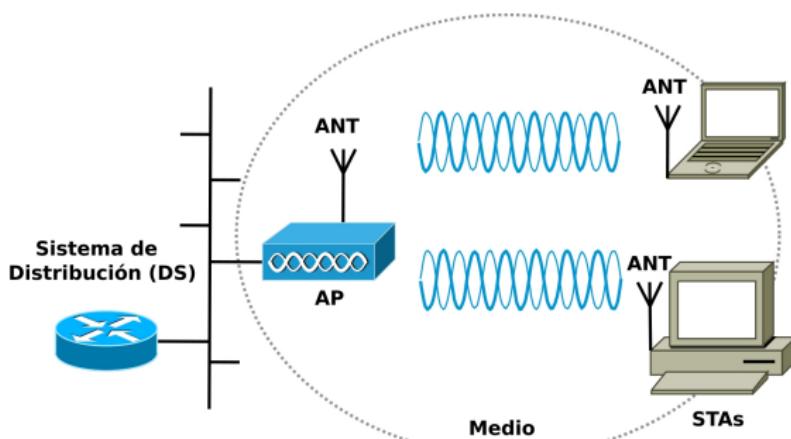
- La IEEE genera los estándares y propicia su renovación acorde las demandas.
- Los fabricantes implementan los estándares, pero quedan cuestiones abiertas.
- No está asegurada la inter-operabilidad, compatibilidad.
- Wi-Fi Alliance es una organización sin fines de lucro que certifica inter-operabilidad y promueve el desarrollo de nuevas tecnologías asociadas.



Fuente del gráfico: <https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201004gls.html>

Componentes de una WLAN

- Estaciones Terminales (STA).
- Dispositivos Concentradores, Access Point (AP).
- Espacio por donde se propagan las señales (WM).
- Sistema de Distribución (DS).
- Las STA y los AP contienen:
 - Antenas (ANT), WNICs, pigtails, y otras componentes auxiliares.



Antenas

- La funcionalidad es convertir la energía eléctrica en ondas de RF (ondas electromagnéticas) al Tx y viceversa al Rx.
- WLAN IEEE 802.11 frecuencias 2GHz y 5GHz → tamaño de antena pequeño.
- Diferentes antenas a diferentes bandas (frecuencias).
- Las antenas proveen 4 propiedades básicas a un sistema Wireless:
 - Polarización.
 - Dirección.
 - Patrón de radiación.
 - Ganancia (Gain) (dBi).

Patrón de Radiación

- Las antenas se pueden clasificar básicamente en 2 categorías de acuerdo a la direccionalidad o patrón de radiación:
 - Omni-direccionales.
 - Direccionales
- Las antenas **Omni-direccionales** irradian de una forma más homogénea.
- Las antenas **Direccionales** cubren una región particular aumentando la ganancia.

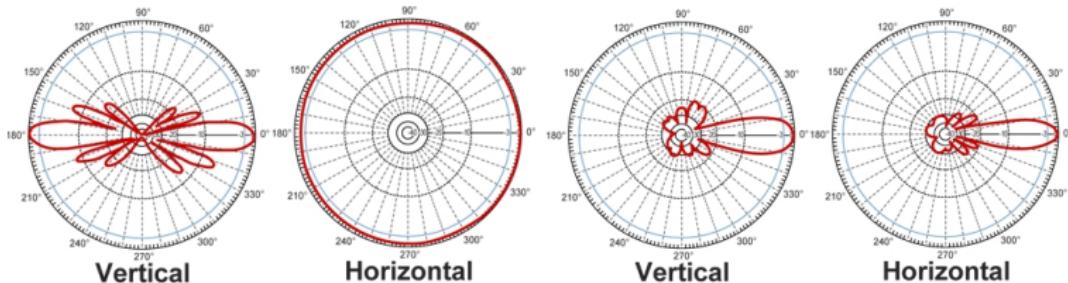


Figura: Patrones de radiación de una antena tipo dipolo (8dBi) y de otra tipo grid direccional (19dBi) en 2,4GHz

Ilustraciones de Antenas



Estamos en:

1 Introducción a WLAN

- Objetivos y Estándares
- Componentes Físicas de una WLAN

2 IEEE 802.11: Capa Física

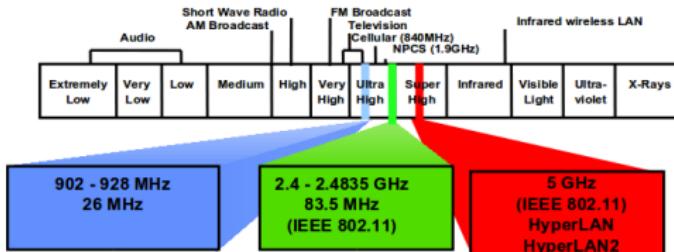
- Capa Dependiente del Medio Físico: PMD
 - Frecuencias Seleccionadas

3 IEEE 802.11: Capa MAC

- Tipos de Redes Wireless
- Identificación del Basic Service Set
- Modos de Acceso al Medio
- Tramas MAC 802.11

Capa Física: Selección de la Frecuencias

- En 1985 la Federal Communications Commission (FCC) libera banda de ISM (Industrial Scientific Medical).
- Otras organizaciones adoptaron medidas similares.
- Cada país tiene sus propias organizaciones:
 - FCC: América, Australia, Nueva Zelanda.
 - ETSI: Europa, África, partes de Asia.
 - TELEC: Japón.
 - CNC: Argentina.
- Frecuencias ISM con Spread Spectrum (SS) 900MHz - 2,4GHz - 5,8GHz.

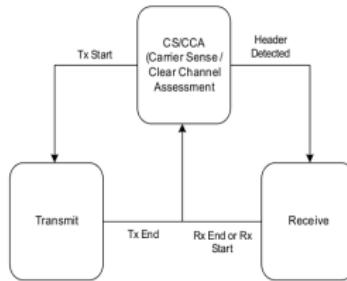


Capa Física: Selección de la Frecuencias (Cont.)

- No se van a ver los detalles.
- Básicamente: tecnología sobre “Bandas de Frecuencias no Licenciadas”, operación de RF sin planificación de autoridad competente.
- Frecuencias con poco uso a nivel mundial y de bajo costo para implementar equipos.
- No se utiliza sub-división de canales por usuario.
- Sin asignación de canal en forma exclusiva.
- Límites de Potencia Radiada, controlados por autoridades competentes.
- Consenso casi mundial en algunos puntos.

Funciones de la Capa Física: PMD

- Determina las frecuencias físicas.
- Define las Modulaciones y Codificaciones (M & C) : técnicas que permitan lidiar con la interferencia: Spread Spectrum, OFDM, otras.
- Convierte Bits en Símbolos.
- Máquinas de estado:
 - Transmite (Tx) y Recibe (Rx) los Símbolos (Sym).
 - Rx, **CS**: detecta el inicio de una señal de red que puede ser recibida.
 - Tx, **CS/CCA**: previamente debe determinar el estado del medio.

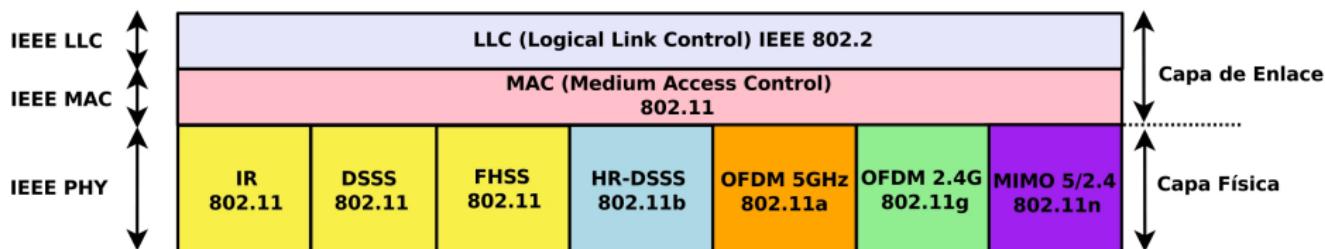


Capa Física: PMD 802.11-1997

- 802.11-1997: Frequency-Hopping (FH) Spread-Spectrum (**FHSS**).
- 802.11-1997: Direct-Sequence (DS) Spread-Spectrum (**DSSS**).
- 802.11-1997: InfraRed Light (**IR**).
- Orthogonal Frequency Division Multiplexing (**OFDM**) **5GHz 802.11a/j.**
- High-Rate Direct-Sequence Spread-Spectrum (**HR/DSSS**) **2,4GHz 802.11b.**
- Orthogonal Frequency Division Multiplexing (**OFDM-ERP** **2,4GHz 802.11g**)
- OFDM con MIMO (Multiple-Input Multiple-Output) **OFDM-MIMO 2,4/5GHz 802.11n.**
- OFDM con MU-MIMO **OFDM-MU-MIMO 2,4/5GH, 802.11ac, 60GHz en 802.11ad**

Implementaciones WLAN 802.11

- Varios estándares 802.11 difieren principalmente en los aspectos físicos.



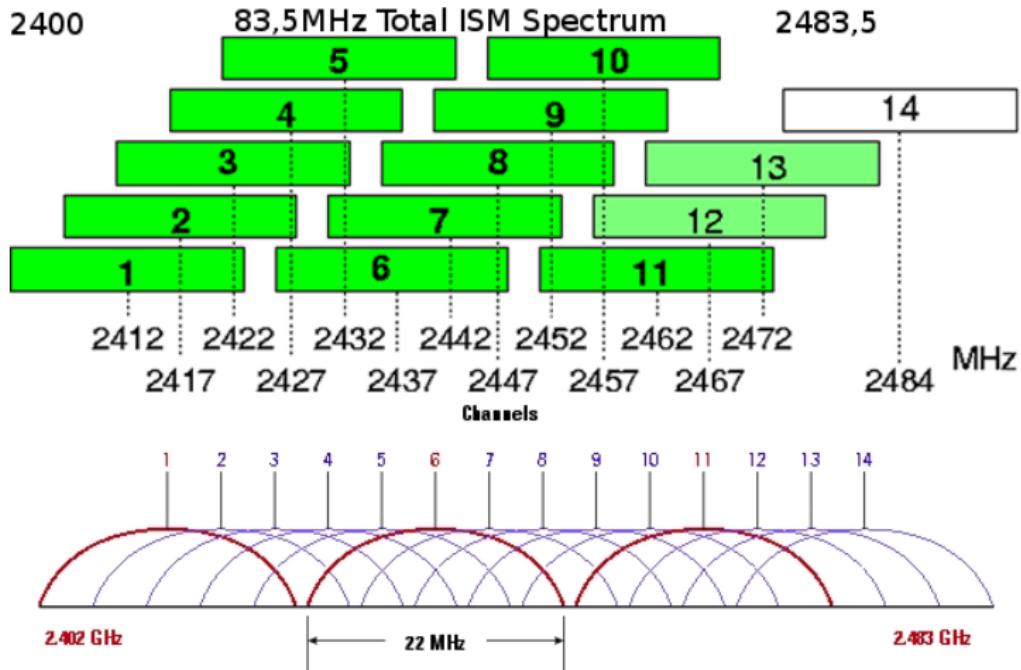
M & C IEEE 802.11-1997

- La cantidad de canales y la ubicación depende de las regulaciones de c/país.

Región	Canales	Rango de Frec.
EE.UU. (FCC)/Canada (IC)	1 .. 11	2,412-2,462 GHz
Europa, sin España (ETSI)	1 .. 13	2,412-2,472 GHz
Japón (MIC)	1 .. 14	2,412-2,462 GHz y 14
España	10 .. 11	2,457-2,462 GHz
Argentina (CNC)	1 .. 13	2,412-2,472 GHz

- Solo no se superponen 3 canales 1:2412MHz ; 6:2437MHz ; 11:2462MHz (ó 4), 802.11h (World Mode).

M & C IEEE 802.11-1997 (Cont.)



Fuente del gráfico: http://www.air-stream.org.au/channel_802_11b

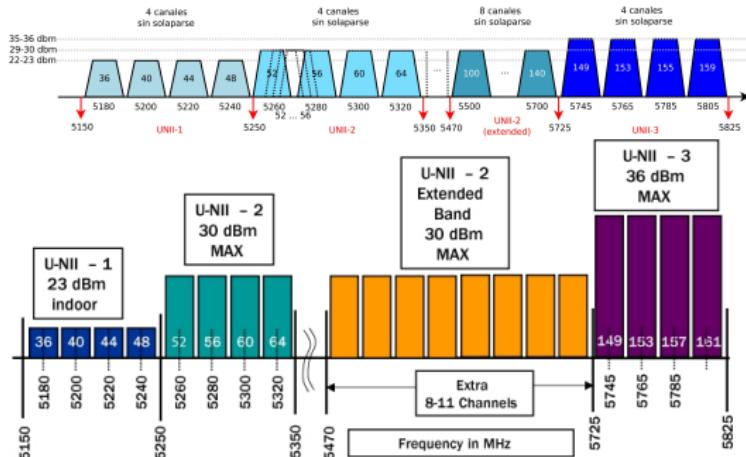
M & C IEEE 802.11a 1999

Tabla de Codificaciones y Modulaciones en 802.11a:

Speed (Mbps)	Modulation and coding rate (R)	Coded bits per carrier	Coded bits per symbol	Data bits per symbol
6	BPSK, R=1/2	1	48	24
9	BPSK, R=3/4	1	48	36
12	QPSK, R=1/2	2	96	48
18	QPSK, R=3/4	2	96	72
24	16-QAM, R=1/2	4	192	96
36	16-QAM, R=3/4	4	192	144
48	64-QAM, R=2/3	6	288	192
54	64-QAM, R=3/4	6	288	216

M & C IEEE 802.11a 1999 (Cont.)

- Espectro más amplio, más cantidad de sub-bandas, inicio 5.8GHz.



Note: Twelve non-overlapping channels within U-NII-1, UNII 2 and UNII 3.

Fuente del segundo gráfico: <http://www.cable360.net/ct/strategy/emergingtech/25375.html>

Resumen Capa Física (Ejemplo)

- Acorde a los niveles de “calidad” de la señal y conf. será la M & C usadas:
 - 1.3Gbps: 802.11ac OFDM + 256QAM y MU-MIMO.
 - 300,600Mbps: 802.11n OFDM + 256QAM con -73dBm o mejor.
 - 54Mbps: 802.11a/802.11g OFDM + 64QAM con -73dBm Rx Sensity.
 - 36Mbps: 802.11a/802.11g OFDM + 16QAM con -80dBm Rx Sensity.
 - 22Mbps: 802.11b+/802.11g podría usar PBCC (Convolutional Coding).
 - 18Mbps: 802.11b+/802.11g podría usar PBCC + QPSK.
 - 18Mbps: 802.11a/802.11g OFDM + QPSK con -87dBm Rx Sensity.
 - 11Mbps: 802.11g/802.11b CCK + DQPSK con -88dBm.
 - 5,5Mbps: 802.11b CCK, DBPSK con -91dBm.
 - 1-2Mbps: 802.11b Barker 11, DBPSK con -94dBm.

Estamos en:

1 Introducción a WLAN

- Objetivos y Estándares
- Componentes Físicas de una WLAN

2 IEEE 802.11: Capa Física

- Capa Dependiente del Medio Físico: PMD
 - Frecuencias Seleccionadas

3 IEEE 802.11: Capa MAC

- Tipos de Redes Wireless
- Identificación del Basic Service Set
- Modos de Acceso al Medio
- Tramas MAC 802.11

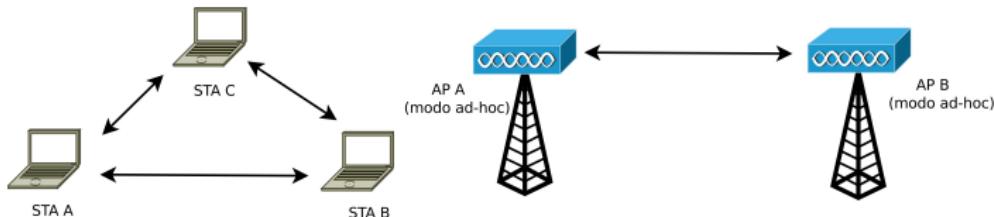
Capa MAC (Medium Access Control)

- Características de la capa MAC 802.11:
 - Se encuentra sobre la capa Física y controla la transmisión de los datos del usuario.
 - Soporta Broadcast y Multicast.
 - Mismo formato de dir. MAC que Ethernet.
 - El encapsulamiento diferente al de Ethernet, usa 802.2.
 - Utiliza ACK positivos. Operaciones atómicas, Broadcast y multicast no.
 - Tramas de diferente tipos: datos, administración y control.
 - Formato de la trama más complejo (comparado con Ethernet).
 - Unicast contempla fragmentación.

Topologías de Red 802.11

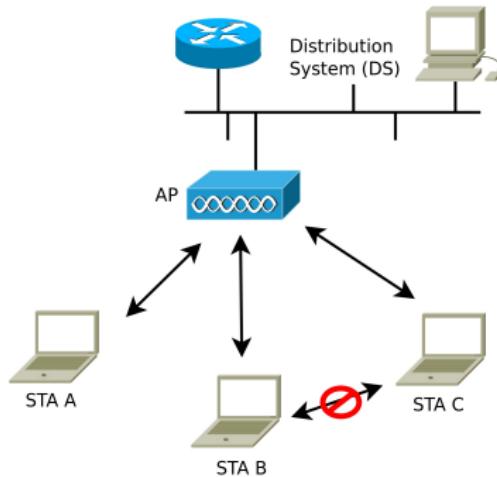
- BSS - Basic Service Set:
 - Independent BSS (IBSS) - Independiente.
 - Infrastructure BSS - Infraestructura.
 - Extended Service Set (ESS) - Extendido.

Topologías de Red - IBSS



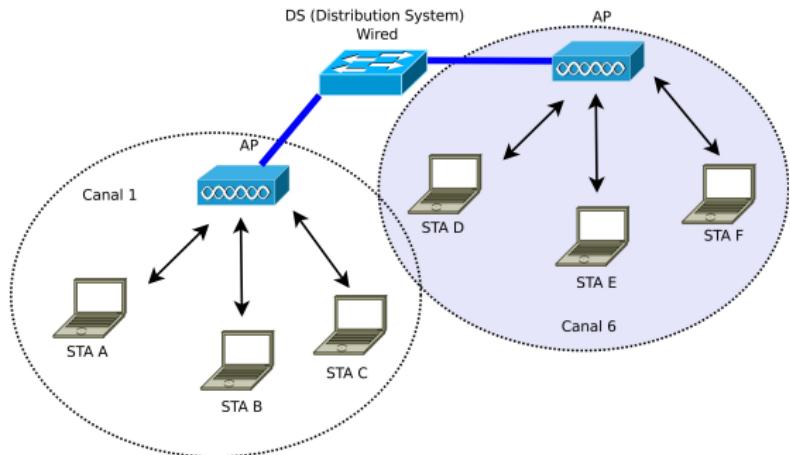
- No se utilizan Access Points.
- Conocidas como redes Ad-Hoc.
- Tiempo de vida limitado, o caso especial de redes punto a punto, modo bridge.

Topologías de Red - BSS de Infraestructura



- Requieren el uso de un dispositivo concentrador: Access Point (AP).
- El AP es una STA especial, AP rol de hub/switch wireless.
- Las estaciones deben asociarse al AP.
- Las estaciones solo se comunican a través del AP.
- Algunos AP presentan conexión a la red cableada.

Topologías de Red - ESS

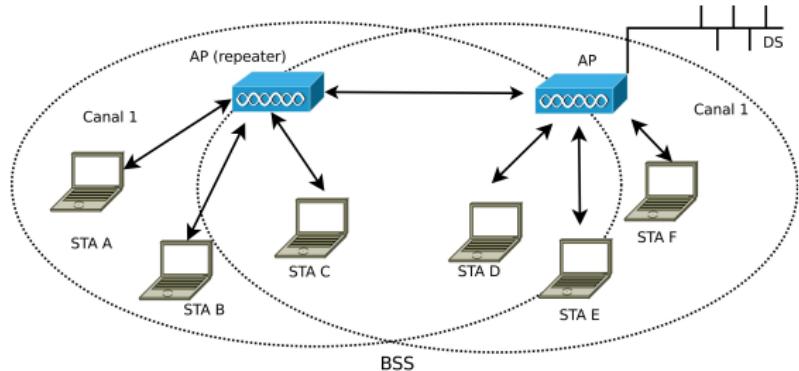


- Se unen varios BSS (varios APs) a través de un backbone, conocido como Distribution System (DS).
- Estaciones se unen a un solo AP.
- APs se comunican entre ellos, lo pueden hacer vía red cableada o WDS (Wireless Dist. System).

Wireless Distribution System (WDS)

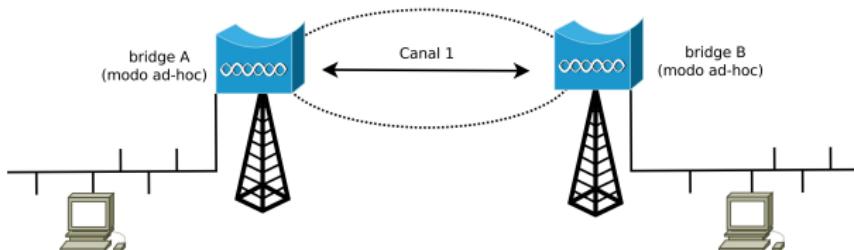
- El estándar solo define el formato de las tramas, pero no el mecanismo (STD:IEEE-802.11-2007-3.170).
- Conexión APs entre sí de forma wireless.
- Se puede realizar utilizando un segundo RADIO.
- Se puede hacer utilizando el mismo RADIO, mediante **WDS**.
- El WDS permite interconectar APs mediante una red inalámbrica usando la misma frecuencia.
- APs rol de Cliente y APs al mismo tiempo.
- Permite:
 - Enlace entre AP para construir un **bridge** entre 2 redes.
 - Cubrir grandes áreas con varios AP, si necesidad de cablear, **repetidores**.
 - Roaming.

Topologías de Red - AP-AP Repetidor



- **Repetidor:** AP **NO** conectado a una red cableada. **Range Extender.**
- Los APs deben comunicarse entre ellos, Repetidor hace de AP y Cliente a la vez.
- Se pueden encadenar varios APs. No se recomienda más de 2 por rendimiento.
- No está contemplado de esta forma en el estándar IEEE.

Topologías de Red - AP-AP Bridges



- **Bridge:** AP que conecta una red cableada (Ethernet) con otra vinculándose a partir de un segundo AP.
- Los APs solo se comunican entre ellos de forma Wireless, modo ad-hoc.
- Extensión de fabricantes, no está contemplado de esta forma en el estándar IEEE.

Service Set IDentifier (SSID)

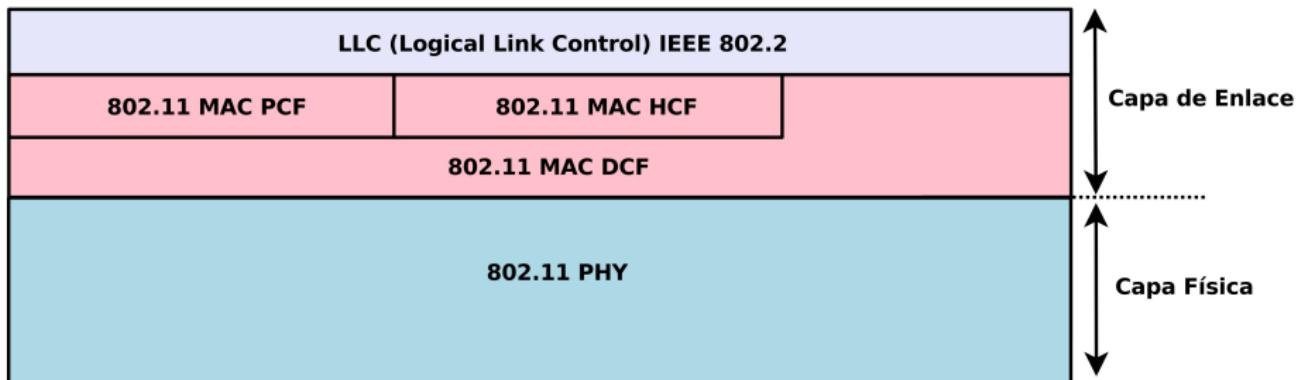
- el SSID le da un nombre distintivo a la red.
- Usado en el momento de la asociación a la WLAN por un nombre.
- De 2 a 32 caracteres, sensitivo a mayúsculas (2 restringido por fabricantes).
- IEEE 802.11 define 0 - 32, (0 length) NULL SSID, llamado broadcast/wildcard.
- Obligatorio. Por seguridad se los suele ocultar aunque no es efectivo.
- Se lo suele llamar ESSID.
- Un AP podría tener múltiples SSID: **MSSID**.
- El mismo SSID podría estar repetido en varios AP.
- No confundir con el BSSID (MAC del AP).
- si el AP lo manda de forma broadcast en los Beacons se dice que es: **Guest Mode** o **Broadcast SSID**.

Basic Service Set Identifier (BSSID)

- el BSSID identifica únicamente una celda física wireless.
- Es la dir. MAC del AP que cubre la celda.
- Es una dirección otorgada por la IEEE grabada en la WNIC (salvo modo ad-hoc).
- El cliente al conectarse a la WLAN selecciona qué AP a través del BSSID.
- En el caso de MSSID, se requieren Multiple Basic Set Service Id (**MBSSID**).
- MBSSID: una dirección MAC base +1 cada nuevo SSID.
- En general cada MBSSID asociado con una VLAN diferente mediante 802.1Q.
- Las WNIC de las estaciones también se identifican con una MAC.

Capa MAC - Acceso al medio

- Tres mecanismos de acceso al medio:
 - **DCF:** Distributed Coordination Function (Obligatorio, NO determinístico)
 - **PCF:** Point Coordination Function (determinístico).
 - **HCF:** Hybrid Coordination Function (para QoS).



Acceso al Medio: CSMA/CA

- El acceso al medio con DCF se implementa con CSMA/CA (vs. CSMA/CD de Ethernet).
- No existen estaciones con privilegios, incluso el AP debe competir para acceder al medio.
- Antes de Tx se debe verificar que el medio este libre: **CS (Carrier Sense)**.
- Medio compartido implica varias estaciones intentando acceder: **MA (Multiple Access)**.
- Detección de colisiones dificultosa: **CD (Collision Detect)**, se cambia por **CA (Collision Avoidance)**.
- Método de Tx y Rx no simultáneo HDX.
- **CA** no significa que no existen colisiones, se tratan de evitar, difícil de detectar.

Acceso al Medio: Sensado

Sensado Físico/Physical Carrier-Sense: capa física, módulo **Carrier Sense/Clear Channel Assessment (CS/CCA)**.

Sensado Virtual/Virtual Carrier-Sense (VCS): observación de los encabezados de tramas. Utilizan temporizador: **Network Allocation Vector (NAV)** e inspecciona tramas en curso (campo “Duration”) del encabezado.

- Detecta la duración y actualiza el NAV.
- NAV se decrementa de forma automática.
- NAV=0, VCS indica medio libre.

Extensión de Virtual Carrier-Sense (VCS): cuando no se pueden ver entre dos nodos (nodo oculo) se requiere solicitar acceso mediante RTS/CTS al AP(todos lo deben ver).

Algoritmo, CA: Collision Avoidance

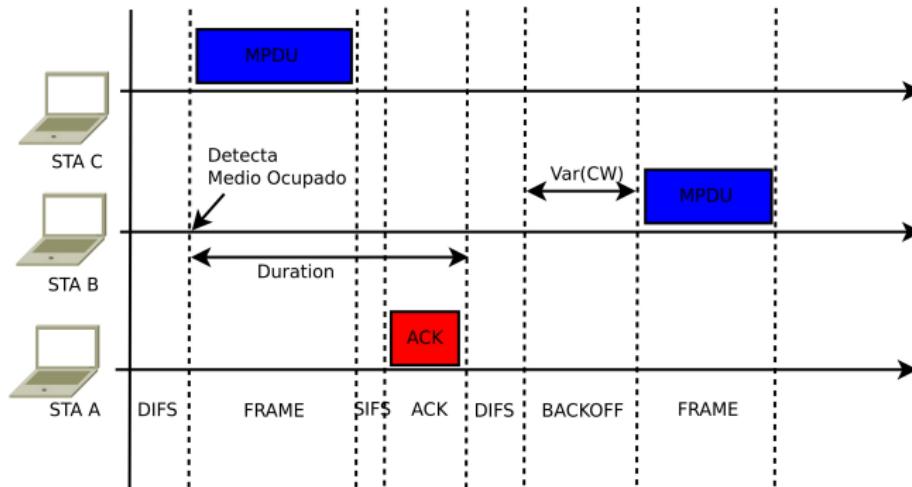
- Antes de enviar espera IFS: DIFS/EIFS (en modo DCF).
- NO se envía si el medio esta ocupado.
- Corre Backoff recién cuando detecta el medio libre en caso de:
 - ① El evento anterior inmediato fue “Medio Ocupado” (Deferred Access).
 - ② Es una re-transmisión.
 - ③ Luego de un envío unicast exitoso inmediato (Deja posibilidad de Tx a otras STA).
- No corre Backoff:
 - Es un nuevo paquete, luego de DIFS, “Medio Libre” y no viene de una Tx previa.

CSMA/CA: Acknowledgment (ACK)

- Cada trama unicast requiere una confirmación por parte del receptor.
- El emisor cada vez que Tx trama unicast inicia **Retrans-Timer**.
- Trabaja en modo Stop & Wait.
- Si el receptor detecta errores en la trama recibida (FCS error), no envía nada.
- El emisor solo considera exitoso el envío si recibe ACK.
- Los ACKs deben ser atómicos con la operación de Tx.
- Luego de una Rx exitosa se espera IFS menos: SIFS (Short IFS) para confirmar, asegura acceso.
- Broadcast y Multicast no usan ACK.

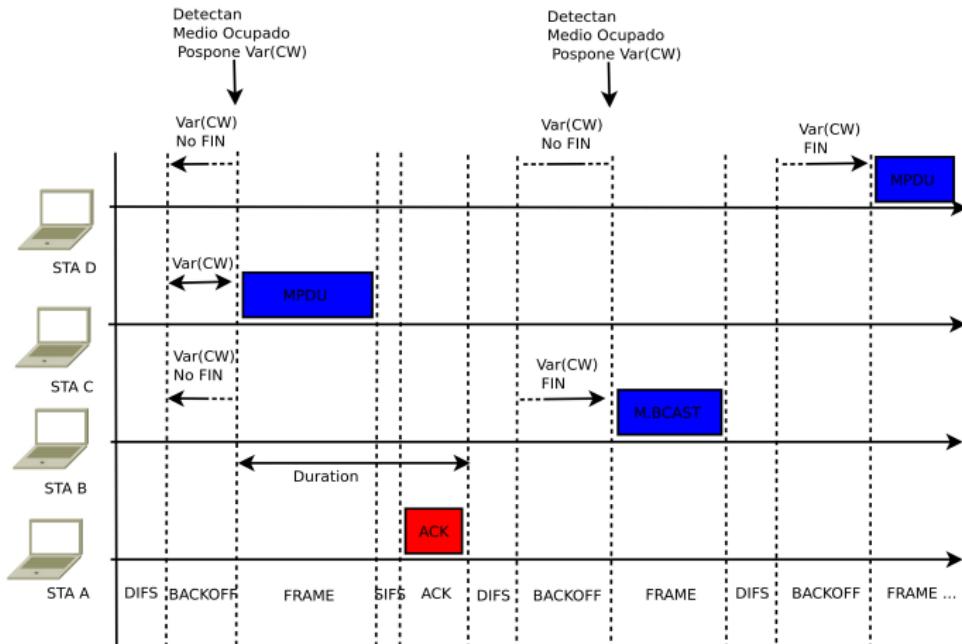
CSMA/CA: Ejemplo 1

- Primera Tx, espera DIFS, medio libre → STA “C” Tx.



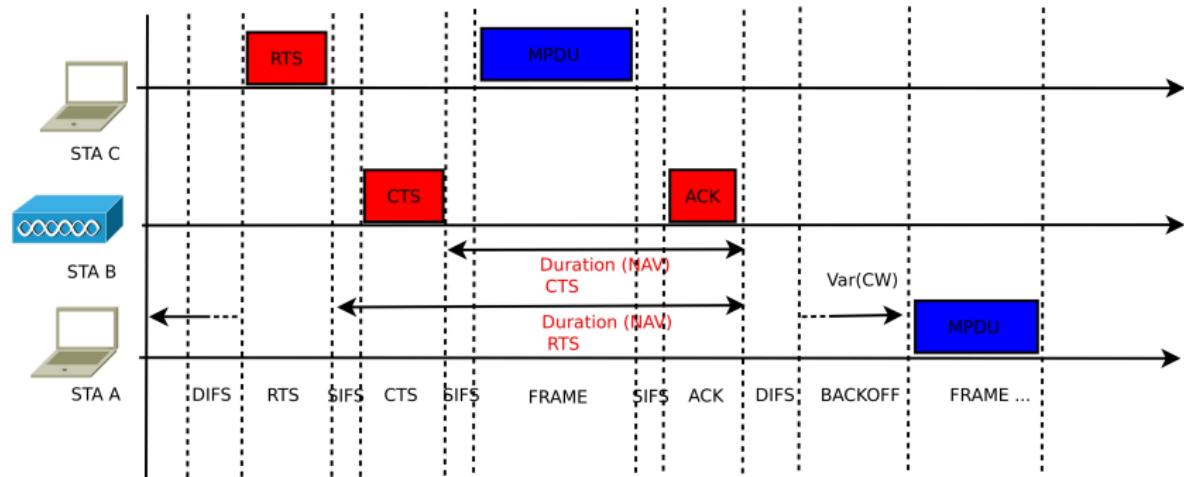
CSMA/CA: Ejemplo 2

- Todas las STA vienen de evento “Medio Ocupado”, STA “B” Tx.
- Aplican Backoff, la que selecciono el tiempo más corto, STA “C” Tx.



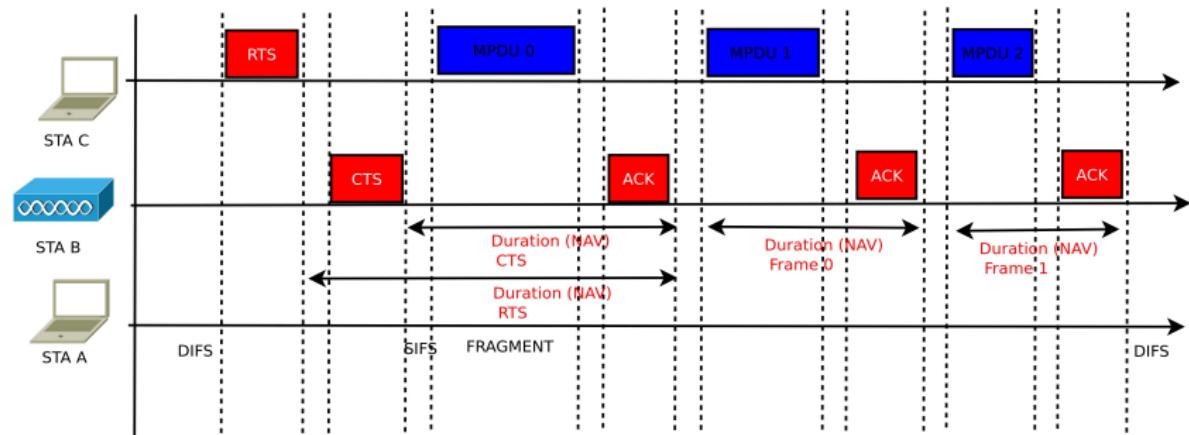
CSMA/CA: Ejemplo 3

- Extensión del Virtual Carrier-Sensing con CTS/RTS.
- Tramas largas, mayor que el valor: **dot11RTSThreshold** deben ser enviadas con el mecanismo de CTS/RTS.



CSMA/CA: Fragmentación

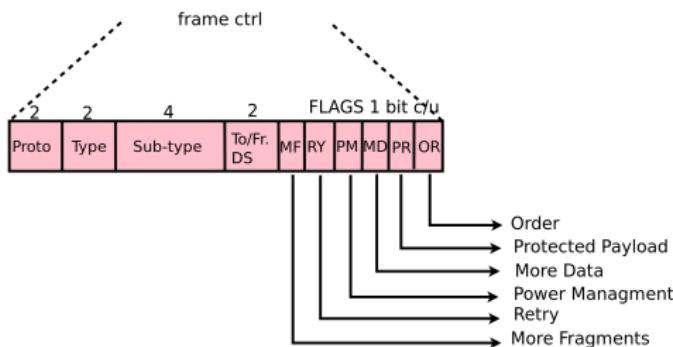
- 802.11 admite fragmentación a nivel de enlace (evita frag. a nivel IP).



Tipos y Partes de Tramas MAC

- Tipo de Tramas MAC:
 - Management (Administración).
 - Control (Control).
 - Data (Datos).
- Partes de una Trama MAC:
 - Cabecera MAC (MAC Header): info. de control, direcciones, etc.
 - Cuerpo de la trama (Body): datos, payload.
 - Cola de la trama (Trailer): **FCS (Frame Check Sequence)** o CRC de 32 bits.

Trama MAC 802.11 y Ethernet



Capa MAC - Formato Frames

- To DS/From DS** Si la trama va desde una STA al AP, al revés, o desde un AP a otro AP, o de STA a STA.

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

2	2	6	6	6	2	6	0..2312	4
frame ctrl	Dur.	Address 1	Address 2	Address 3	seq	Address 4	Contenido/Payload	CRC

Capa MAC - Trama de Datos

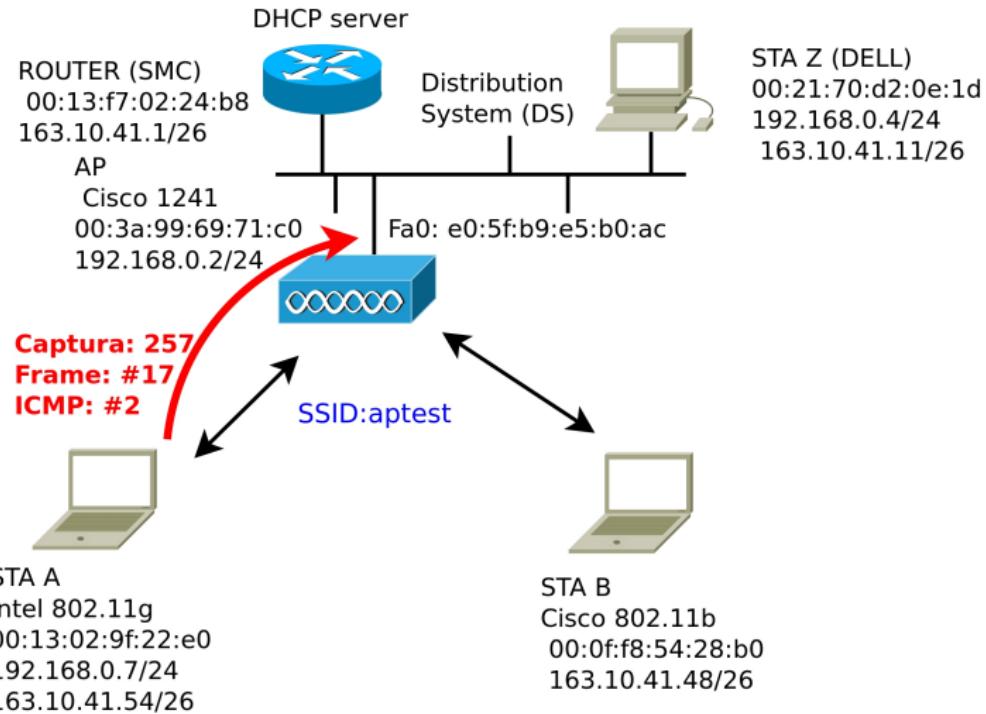
No. .	Time	Source	Destination	Protocol	Info
254	183.794168	192.168.0.2	192.168.0.7	ICMP	Echo (ping) reply
257	184.791645	192.168.0.7	192.168.0.2	ICMP	Echo (ping) request
258	184.792119	192.168.0.2	192.168.0.7	ICMP	Echo (ping) reply

Frame 257 (118 bytes on wire, 118 bytes captured)
IEEE 802.11 QoS Data, Flags:T
Type/Subtype: QoS Data (0x28)
Frame Control: 0x0188 (Normal)
Version: 0
Type: Data frame (2)
Subtype: 8
Flags: 0x1
Duration: 44
BSS Id: Cisco_09:71:c0 (00:3a:99:69:71:c0)
Source address: IntelCor 9f:22:e0 (00:13:02:9f:22:e0)
Destination address: e0:5f:b9:e5:b0:ac (e0:5f:b9:e5:b0:ac)
Fragment number: 0
Sequence number: 17
QoS Control
Logical-Link Control
Internet Protocol, Src: 192.168.0.7 (192.168.0.7), Dst: 192.168.0.2 (192.168.0.2)
Internet Control Message Protocol

Cap: 257 FILE:///CAPTURES/infr-apttest.pcap

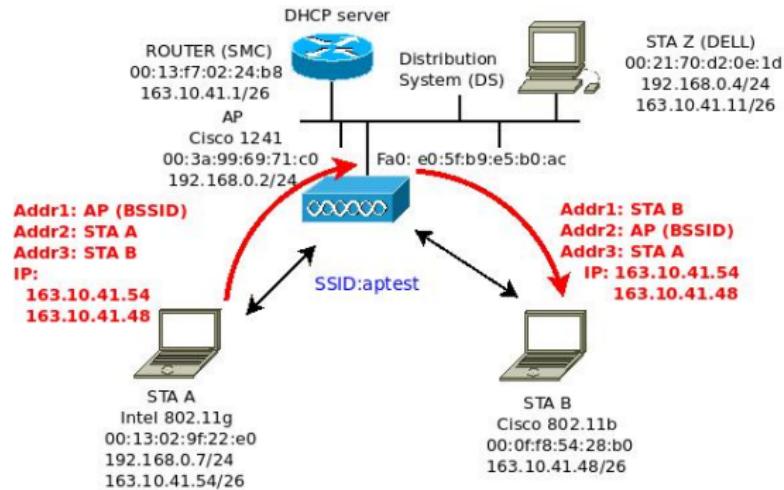
Capa MAC - Trama de Datos (Cont.)

- Escenario de envío de Trama de Datos al AP:



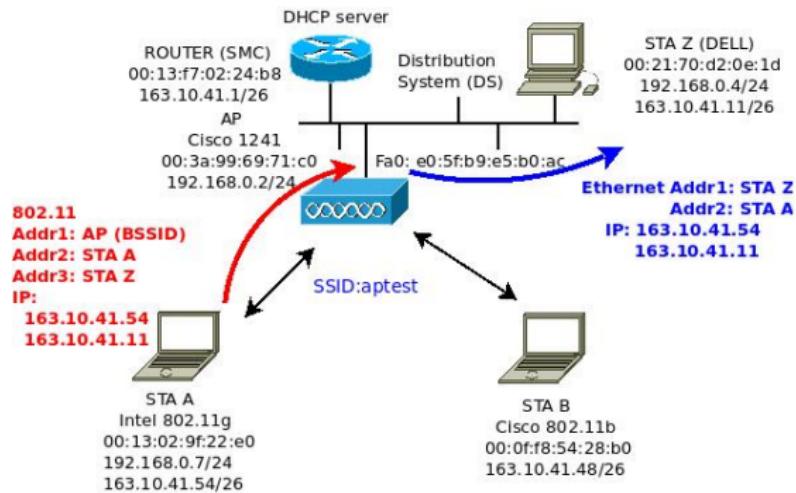
Capa MAC - Trama de Datos (Cont.)

- Escenario de envío de Trama de Datos a otra estación 802.11:



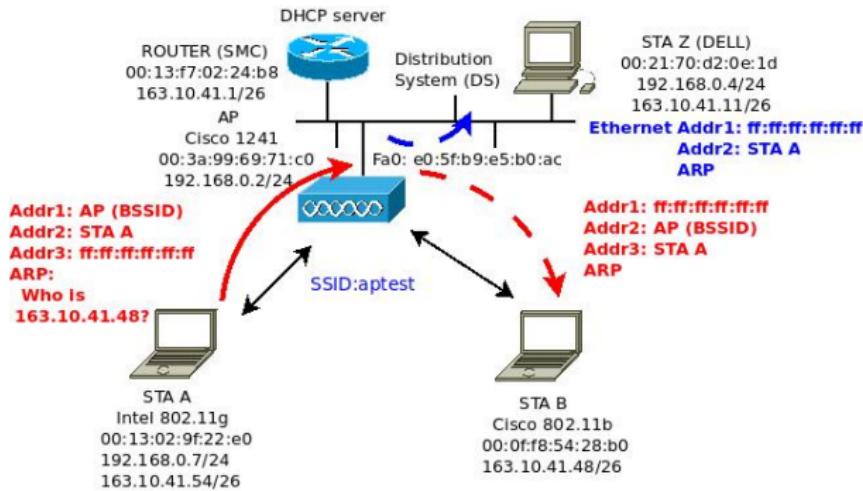
Capa MAC - Trama de Datos con Ethernet

- Escenario de envío de Trama de Datos a estación cableada:



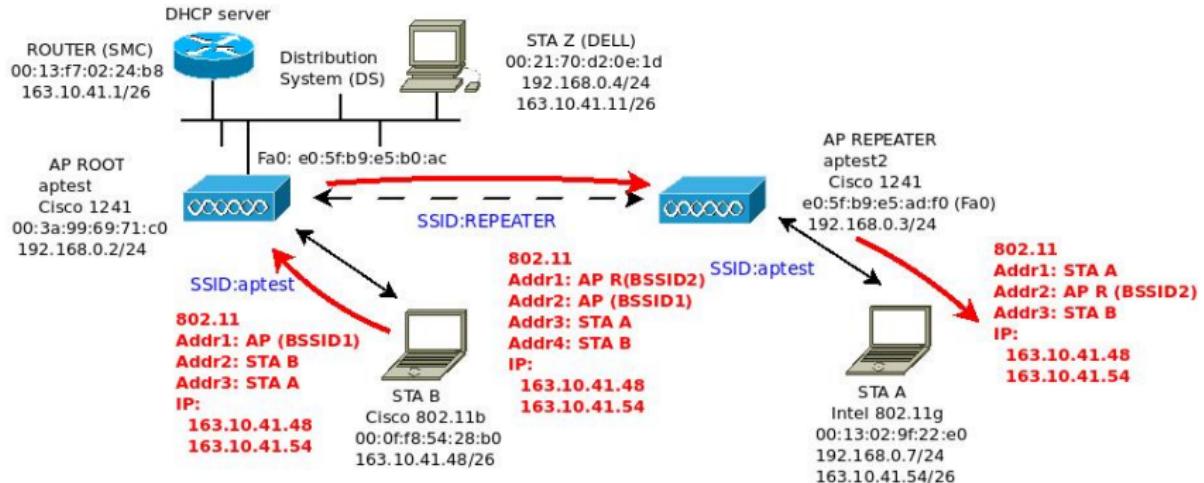
Capa MAC - Trama de Datos ARP

- Escenario de envío de Trama de Datos, ARP Request:



Capa MAC - Trama de Datos con WDS

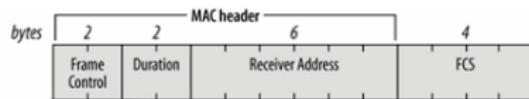
- Escenario de envío de Trama de Datos a estación en repetidor:



Capa MAC - Tramas de Control

- ACK (Acknowledgment).
- RTS (Request to Send), RTS (self).
- CTS (Clear to Send).
- PS-Poll (Power-Save Poll).

ACK



Fuente del gráfico: "Wireless Networks The Definitive Guide 2nd Ed.", Matthew Gast.

Capa MAC - Tramas de Administración

- Tramas de MGMT:

- Tramas Baliza/Guía (Beacon).
- Asociación (Association Request).
- Respuesta de Asociación (Association Response).
- Tramas de Des-asociación (Disassociate).
- Tramas de Re-asociación (Reassociation Request y Reassociation Response).
- Tramas de Sondeo (Probe Request).
- Respuesta al Sondeo (Probe Response).
- Tramas de Autenticación (Authentication y Deauthentication).

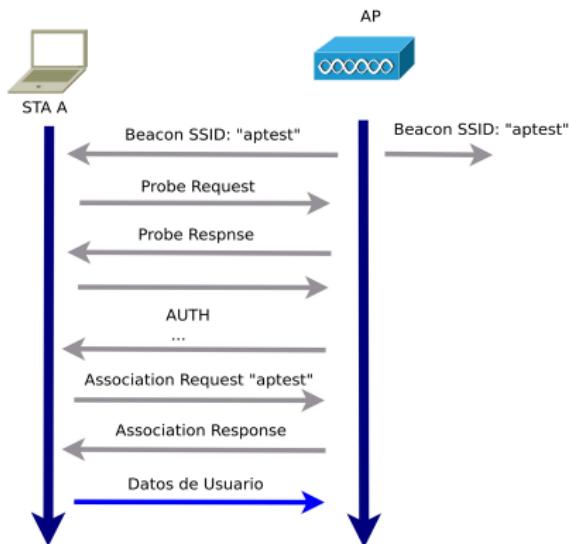
802.11 MGMT - Funcionamiento

- ① Scanning (Activo/Pasivo).
- ② Autenticación.
- ③ Asociación.
- ④ Intercambio de datos.
- ⑤ Deautenticación (opcional).

Capa MAC - Sensado/Beaconing

- Sensado/Escaneo Pasivo (Passive Scanning):
 - Saltan de canal en canal escuchando tramas **Beacon** de APs.
 - La estación no envía nada.
 - Solo inspecciona los IE (Info. Elements) de los Beacons.
- Sensado/Escaneo Activo (Active Scanning):
 - Salta de canal en canal enviando **Probe Request** y esperando **Probe Response**.
 - Debe seguir las reglas de acceso DCF.
 - **Probe Request** broadcast, a SSID=ANY o SSID="Specific Value".
 - **Probe Response** unicast.

802.11 - Scan/Autenticación/Asociación



Time	Cisco_69:71:c0	Broadcast	Comment
0.000			
39.443		Probe Response, SN=355	IEEE 802.11: Beacon frame, SN=3528, Fh=0, Flags=....., Bi=100, SSID="aptest", Name="aptest"
39.445		Probe Request, SN=1	IEEE 802.11: Probe Response, SN=3524, Fh=0, Flags=....., Bi=100, SSID="aptest", Name="aptest"
39.446		Probe Response, SN=1	IEEE 802.11: Probe Request, SN=1, Fh=1, Flags=....., SSID="aptest"
39.677		Probe Request, SN=2	IEEE 802.11: Probe Response, SN=3515, Fh=0, Flags=....., Bi=100, SSID="aptest", Name="aptest"
39.678		Probe Response, SN=2	IEEE 802.11: Probe Request, SN=2, Fh=0, Flags=....., SSID="aptest"
39.680		Authentication, SN=2	IEEE 802.11: Probe Response, SN=3518, Fh=0, Flags=....., Bi=100, SSID="aptest", Name="aptest"
39.680		Authentication, SN=2	IEEE 802.11: Authentication, SN=3919, Fh=0, Flags=.....
39.681		Association Request	IEEE 802.11: Authentication, SN=4, Fh=0, Flags=....., SSID="aptest"
39.683		Association Response	IEEE 802.11: Association Response, SN=3520, Fh=0, Flags=.....

802.11 - Funcionamiento (Cont.)

A Todo esto se le debe agregar la seguridad !!!

Referencias

[802.11-2007] IEEE Std-802.11. 2007.

[Gast05] 802.11 Wireless Networks The Definitive Guide 2nd Ed.
Matthew Gast. O'Reilly. 2005.

[CAR09] CCNA Wireless Official Exam Certification Guide (CCNA
IUWNE 640-721). Brandon James Carroll. Cisco Press. 2009.