



• Redes LAN y wireless

# T4: Redes Wireless

## Introducción

### Características WLAN

- Redes locales inalámbricas utilizan medios de transmisión no guiados (ondas electromagnéticas)
- Para conectar los dispositivos de usuario de la red
- Alternativa / complemento → LAN cableada
- Justificación → Cobertura lugares difíciles de cablear  
Facilitar movilidad de los usuarios

### Espectro Radioeléctrico WLAN

- WLAN utiliza bandas de f:
  - { ISM (Industrial, Scientific and Medical)  
    UNII (Unlicensed National Info. Infrastructure)}
  - Reservadas internacionalmente para uso sin licencia → siempre tiene mayor potencia max emisión
- 
- 902-928 MHz  
2.5 GHz (2500-2540 MHz)  
100-1000 MHz (5250-5490 MHz)  
2.2 GHz (5710-5735 MHz)  
2.4 GHz (2400-2484 MHz)  
5 GHz (5150-5835 MHz)
- 802.11 / 802.11b  
802.11g / 802.11n  
802.11a / 802.11n / 802.11ac

### Condicionantes Wireless

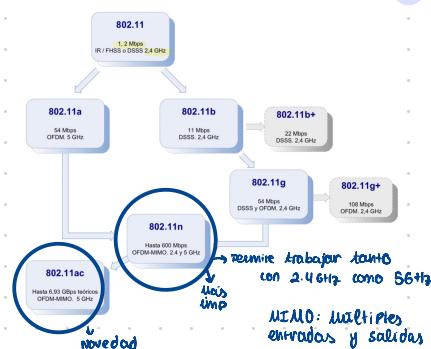
- Redes inalámbricas → el medio siempre es compartido
- No es posible utilizar protocolos MAC tradicionales  
→ no se escuchan colisiones, nodos ocultos, itinerancia,...

Atenución Variable:  
(cobertura limitada  $1/d^2$ )  
Recepción bidimensional  
Interferencias con otras fuentes  
Propagación Multirayos

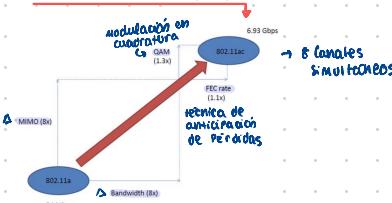


- "nodo oculto": A → no detecta envíos → C (falta CS, carrier sense)  
B: C si; → colisión entre A y C  
ni A ni C → no detectan (falta CD, collision detection)

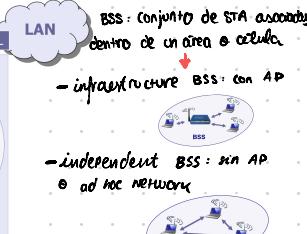
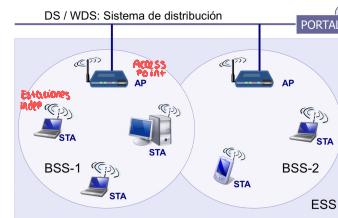
### WLAN: Evolución de los estándares 802.11



### Factores de la evolución



### Componentes de la WLAN



+ ESS, Extended Service Set → Agrupación 2 o más BSS con = SSID

↳ BSS se enlazan mediante una red backbone "sist de Distrib." (DS o WDS)

+ Service Set Identifier, SSID → ESSID → identif/rótulo red, 82 octetos

+ Basic Service Set Identifier, BSSID → identif de célula, 6 octetos  
+ Gener de nombre, en forma de MAC (formato 48C)

+ Portal → Puente hacia la red fija (implementado por los APs)

### Operación en modo Infraestructura

#### ① Localizar APs

Escaneo Pasivo: → todos los canales hasta recibir tramas Baliza (beacons)

Escaneo Activo: estación intenta localizar AP → a cada canal una trama de prueba (probe request)

② Estación decide a qué AP asociarse → en función de potencia serial recibida

③ Inicia proceso autenticación → control Acceso WLAN → estación debe identificarse → AP

802.11 ofrece 2 métodos por defecto

↳ Autenticación abierta: solo → AP estación

Autenticación con clave compartida → algoritmo Privacidad WEP

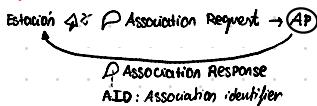
802.1x / EAP mejor

# T4 : Redes Wireless

## (INTRODUCCIÓN)

Operación en modo infraestructura, II

- ④ AP  $\xrightarrow{\text{Aceptado}}$  Authentication Response  $\xleftarrow{\text{rechazo}}$



- ⑤ (Se ha establecido conexión)  $\rightarrow$  Canal puede ser utilizado para tránsito de datos

- ⑥ Reasociación

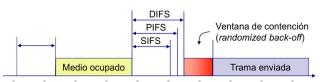
estación  $\rightarrow$  evalúa señal recibida desde APs de su SSID

cuando considera nuevo AP (B) es mejor anterior (A):

- $\rightarrow$  ST solicita Asociación  $\rightarrow$  AP<sub>B</sub>
- $\rightarrow$  AP<sub>B</sub> confirma asociación y registra estación
- $\rightarrow$  AP<sub>B</sub> informa a AP<sub>A</sub> con un P de reasociación
- $\rightarrow$  AP<sub>A</sub> realiza desasociación y si tramas pendientes de ST a la estación a AP<sub>B</sub>

## $\Rightarrow$ IFS (Inter Frame Space)

- + @ espera nuevo ST
- + consideran hasta 4 intervalos: (list. de prioridades)
  - SIFS  $\rightarrow$  ACK, CTS, respuesta sonde
  - PIFS  $\rightarrow$  inicio PCF (con prioridad)
  - DIFS  $\rightarrow$  inicio DCF (Best-effort)
  - EIFS  $\rightarrow$  considerar  $\neq$  error

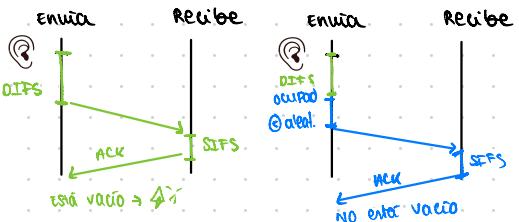


## Nivel MAC

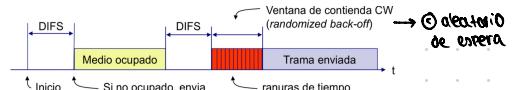
### FLXs de Coordinación CF

- DCF (Distributed CF) CSMA/CA  $\rightarrow$  obligatoria
  - Asignación del canal por contienda  $\rightarrow$  Servicio Best-effort
  - Collision Avoidance  $\rightarrow$  Prevenir colisiones en la red
  - Tramas unicau  $\rightarrow$  confirmadas con ACK
- DCF con RTS/CTS  $\rightarrow$  Distribuida, opcional
- PCF (basada en sondeo)  $\rightarrow$  opcional
- HCF (ATM con QoS)  $\rightarrow$  opcional

### CSMA/CA (Collision Avoidance)



- + La estación que quiere ST el medio (CS)
- + Si entró libre después de un intervalo IFS (Intervalo frame)
  - $\hookrightarrow$  ST DIFS, PIFS, SIFS
- + Si ocupado  $\rightarrow$  espera a que sea libre  $\rightarrow$  intervalo IFS
  - un num. aleatorio de ranuras de  $\theta$   $\Delta \rightarrow$   $\Delta$  colisiones



### NAV (Network Allocation Vector)

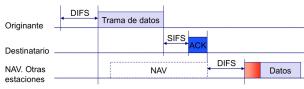
temporizador de espera  $\rightarrow$  activar estaciones cuando de teclear tramas (en medio inalámbrico)

- + valor no inicializa con el campo Duración
  - $\hookrightarrow$  Cabecera ? Trama
  - $\hookrightarrow$  Estaciones  $\rightarrow$  procesan campo  $\rightarrow$  inicializan NAV
  - $\hookrightarrow$  NAV > 0  $\rightarrow$  bucle  $\xrightarrow{\text{P}}$  frames
- + f(x) NAV  $\begin{cases} \text{Colisiones} \\ \text{Ahorro energía} \end{cases}$

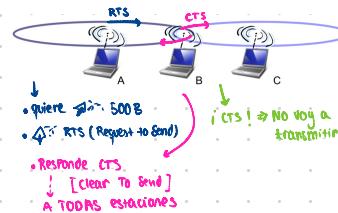
### DCF

#### Envío Unicast

- + Una vez recibida trama  $\rightarrow$  verifica su CRC
  - $\hookrightarrow$  es correcto  $\rightarrow$  ACK + Espera SIFS
  - NO se recibe ACK + enviado EIFS  $\rightarrow$  retransmisión



#### Envíos unicast con RTS/CTS



### PCF, Envío Sin Contienda

Point Coordination Function  $\rightarrow$  mecanismo optional de ST basado en sondeo sin conflicto

- + Estaciones deben solicitarlo  $\rightarrow$  fase de asociación al AP
- + Acceso al Medio  $\rightarrow$  Gant rotulado por un PC [Point Configuration]  $\rightarrow$  AP
- + Periodicamente  $\rightarrow$  PC inicia Periodo Libre de contienda: CFP [Contention-free Period]
  - $\hookrightarrow$  ST trama Beacon con duración Máx del Periodo  $\rightarrow$  Estaciones actualizan su NAV
- + Traumas de datos: CF-Ack, CF-Poll, CF-end y COMBINACIONES
- + (Reforzar el control)  $\rightarrow$  usan intervalos SIFS 2 PIFS  $\rightarrow$  Para impedir q estaciones DCF accedan al canal

# T4 : Redes Wireless

## (Nivel MAC)

### [FIC]s de Coordinación

#### HCF, Nodo Refugio (802.11e, QoS)

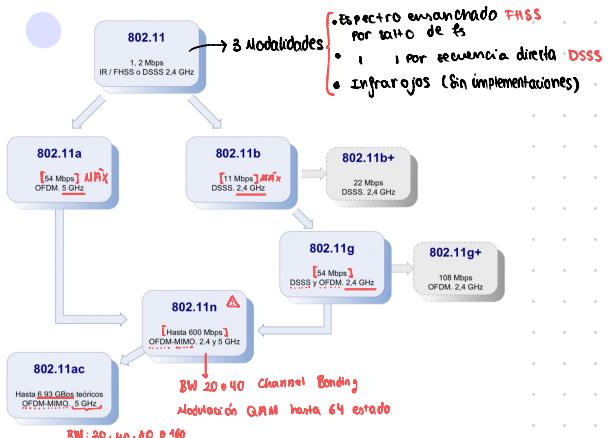
Hybrid Coordination Function → permite mejorar eficiencia en  $\Rightarrow$  en entornos con requerimientos QoS [Redes pocas estaciones & punto a punto]

- + Se basa en  $\Rightarrow$  estera no Toma del canal en transmisiones sucesivas
- + Dos modalidades
  - Distribuida: EDCA, Enhanced Channel Access
  - Por sondeo: HCCA, HCF Controlled Channel Access

#### Parámetros Configurables PAP

- Canal y BW (a partir 802.11n)
- uso RTS/CTS y fragmentación mejoramiento directo y dinámico de entornos
- Umbral RTS  $\rightarrow$  longitud trama  $\rightarrow$  a partir de la cual se activa RTS/CTS
- Umbral fragmentación  $\rightarrow$  longitud trama  $\rightarrow$  a partir de la cual se activa fragmentación
- Intervalo Beacon  $\Rightarrow$  entre baliza y baliza n+1
- Intervalo DTIM  $\Rightarrow$  cuántas balizas se incluyen  $\Rightarrow$  DTIM
- Modo de trabajo de la antena (activar diversidad MIMO)

## Nivel Físico



### Banda 2.4 GHz en 802.11 b/g

- 13 canales ( $\neq$  num canales según ubicación)
- Separación de 5 MHz
- 2MHz canal = 22 MHz  $\rightarrow$  produce sola paralaje
- Interferencias  $\rightarrow$  establecer plan de fs
- 802.11ac mantiene compatibilidad (hacia atrás) 802.11n
  - $\hookrightarrow$  emite un canal primario de 20MHz compatible con 802.11a

## Seguridad

### General / conceptos básicos (tabla)

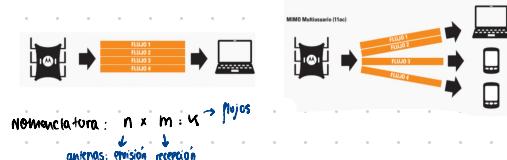
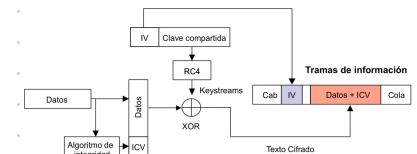
#### WEP (Wired Equivalent Privacy)

- Control de acceso
- Proporciona Confidencialidad
- Integridad

- RC4 + algoritmo de cifrado simétrico usa clave confidencial & vector sincronización (IV)
- La clave compartida  $\hookrightarrow$  única

- Control de identidad basado en CRC

#### Esquema de cifrado WEP



# T4 : Redes Wireless

## (Seguridad)

### [ WEP ]

#### Debilidades WEP

- > Clave única
  - ↳ no renovación autom. de claves
  - ↳ no identifica usuario
- > Control de identidad débil (IEV no →)
- > NO tiene o replicación →
- > IV de longitud insuficiente < 256 bits cifrar (6 veces) predecible
- > Posible ataque cifrado WEP → inter. conmutador
  - ↳ Alcance → puede identif. PAP sin conexión clave AP
  - ↳ Puede interceptar tramas viradas para añadir tráfico a la red
  - ↳ Puede obtener clave WEP mediante análisis estadístico de las tramas cifradas capturadas

#### WEP es vulnerable

#### Ataques WEP

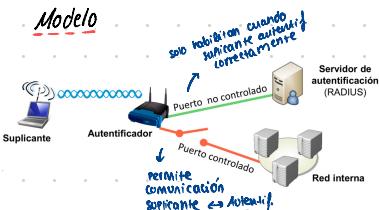
- + Ataque Fuerza bruta → mediante diccionarios
- + Ataque inductivo (Arbaigne) → Construye matriz de keystreams partiendo del tráfico capturado.
  - (Matriz) → obtiene texto claro (sin necesitar a partir del cifrado clave)
- + Ataque Estadístico → obtiene clave analizando un num. suficiente de tramas cifradas

### 802.1x / EAP

- Sist. de autenticación diseñado inicialmente para control de acceso a redes cableadas
- ↳ soporta múltiples mecanismos de autent. (certificados, one-time password, ...)

- ↳ la extensión **Wireless** incluye:
  - Estación "portante"
  - canal
  - seguro
  - switch "autentificador"

### Modelo



### Dialogo



### Arquitectura

Trabaja en 3 niveles

- Nivel de enlace: protocolo EAP / encapsulado EAP
- Nivel de aplicación: métodos autent.
- Nivel de enlace

### Métodos EAP más comunes

	Cliente	Servidor
EAP - PEAP	aut. TLS	aut. digital
EAP - TTLS	usuario, contraseña	..
EAP - TLS	aut. digital	..

### WPA (Wireless Protected Access)

- Objetivo: reemplazar WEP
- 2 Modos de trabajo
  - ↳ WPA-PSK o Personal: SOHO (small office, Home, ..)
  - ↳ WPA-Enterprise: usa 802.1x / EAP y requiere servidor autentif. externo

### Características

- ↳ Gestión de claves dinámico (clave → <sup>ultimo</sup> clave devuelta)
  - ↳ claves temporales ≠ cada sesión
- ↳ Uso RC4 256 b → algoritmo cifrado
  - ↳ Revisa tramas integridad e impide replicación
- ↳ Ataques estadísticos inviables
  - ↳ clave devuelta: no débil → ataque diccionario
  - ↳ Captura intercambio inicial
  - ↳ es posible algunas circunstancias → robar tráfico facilitando ataque inductivo para obtener clave devuelta

### WPA-2 / 802.11i

- único compatible a partir 802.11n
- = WPA
  - ↳ RC4 → AES <sup>upgrade</sup> integridad
  - ↳ reautentificación
  - ↳ más robusta

### WPS (Wi-Fi Protected Setup)

Mecanismo de config. de seguridad para los terminales (Adecuado para entornos domóticos)

- ↳ permite realizar una config. sencilla de WPA - WPA2
- Modos de uso
  - PIN (Personal Identification Number) → genera una clave para autentificar y recibir clave única PSK
  - PBC (Push Button Config.) → se establece red → usuario → AP
  - NFC (Near Field Communication) → RFID
  - USB (Universal Serial Bus)
- ↳ desaconsejado su uso → ataques ≠ bruta

### Recomendaciones de seguridad

- Cambiar contraseña de admin. y lim. acceso AP
- Usar WPA-2 (personal → clave PSK compleja)
- Aislar zona wireless del resto de la red (con VLAN o VPN)
- Aislar estaciones wireless
- No dar acceso en free profiles usuarios no Multihop SSID y VLAN
- Deshabilitar difusión SSID
- Monitorear tráfico malicioso → IDS [Best Detectar Intrusos]
- Ubicar los AP en lugares seguros
- Realizar auditorías periódicas

# T4 : Redes Wireless

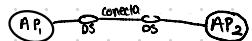
## Topologicas

### Config de los APs

AP → config de 7s modos

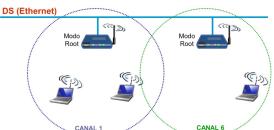
- ↳ Modo AP
- ↳ Modo Repetidor
- ↳ Modo Bridge
- ...
- ↳ Hot Standby
- ↳ Solaramiento espacial
- ↳ MultiBSSID

### Config predeterminada (Root)



y denies recursos  
de la red cableada

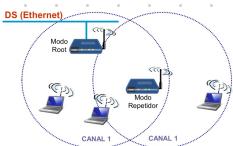
AP adyacentes → deben config. en canales no solapados



### AP en modo Repetidor

Extiende el alcance BSS → actuando como un cliente AP root  
→ ambos APs config = canal

recviendo tramas  
a la estación dest



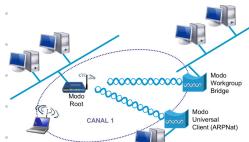
### Modo Bridges

Conectan segmentos de la LAN cableada  
a través enlaces wireless (WDS)

1 AP → "root"  
Resto → estaciones

→

Se utiliza 1 solo canal



### Hot Standby

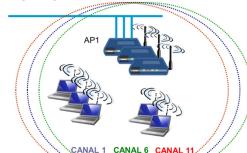
- Para ofrecer servicio de alta disponibilidad
- AP enciendo → fija como backup



### Solaramiento Espacial

Varios AP → ofrecen = cobertura inalámbrica del ESS  
operando en 7s canales

Mejora BW disponible (los estaciones se reparten  
entre los APs)



### Multi BSSID

- Es posible config. múltiples WLAN sobre = AP
- Todas comparten → canal pero pueden  
mantener ≠ config.



### Multi BSSID → VLANs

- Para ofrecer un tratamiento específico  
a cada WLAN virtual, es posible  
asociarlas a VLANs

