IEEE 802.11

Departamento de Sistemas Telemáticos y Computación (GSyC)

gsyc-profes (arroba) gsyc.es

Octubre de 2013

La familia 802.11

Banda ICM (Industrial, Científica y Médica)
Nivel Físico y MAC. No incluye nivel de red

- IEEE 802.11:
  - Año 1997. Ahora a vece se llama 802.11 *legacy*
  - 1-2 Mbps en 2.4 GHz (la misma de Bluetooth)
  - Salto de frecuencias (FHSS) o secuencia directa (DSSS)
- IEEE 802.11b: Extensión de 802.11, 11 Mbps, DSSS
  - Año 1999. Muy extendido (en su día)
  - 14 canales de 22 MHz (parcialmente solapados)
- IEEE 802.11a: Extensión de 802.11
  - Año 1999
  - 54 Mbps, OFDM, 5 GHz
    Mayor frecuencia implica menor alcance, pero es una banda menos congestionada. Incompatible con 802.11b. No ICM en europa

- IEEE 802.11g: Extensión de 802.11
  - Año 2003 (norma) 2005 (mercado)
  - 20-54 Mbps, DSSS y OFDM
  - Compatible hacia atrás con 802.11b
  - Muy similar a 802.11a, pero en 2.4 GHz. Más alcance y menos consumo que 802.11a
- IEEE 802.11n
  - Unos 450Mbps, hasta 600Mbps. Unos 40MByte/s
  - Borrador año 2007, aprobado en 2009
  - OFDM
  - Multiple-input multiple-output (MIMO)
    aka *smart antennas*. Multiplexación por división en el espacio. Conjunto de antenas con diferente orientacion. Algoritmos que tienen en cuenta dónde está el emisor y la dirección por la que entra la señal
  - Canales de 40Mhz (frente a 20Mhz)
  - Mejor rendimiento en 5 GHz, se puede usar en 2.4 GHz si las frecuencias están libres

(Existe 802.11G+, 125Mbps, propietario de Atheros)

- IEEE 802.11p
  - *Wireless Access in Vehicular Environments*
    Aprobado el año 2010
  - 5,9 GHz (EEUU), 5.8 GHz (Europa)
  - Comunicación entre vehículos, seguridad vial, señalización, alertas de emergencia, prevención de colisiones en intersecciones, pago de peajes (E-Tolls, *electronic toll collection*), parking, etc
- IEEE 802.11ac
  Actualmente en desarrollo, se espera que se apruebe en 2014. En 2013 hay algunos equipos en el mercado con 802.11ac draft. Banda de 5 Ghz, tasa de transferencia de 1 Gbps, canales de hasta 160 Mhz, *beamforming*, hasta 8 flujos MIMO

Wi-Fi

- Wi-Fi: Wireless Fidelity
- Marca registrado, Wi-Fi Alliance
- Certificación de productos IEEE 802.11{abgn} que interoperan

http://en.wikibooks.org/wiki/Wireless_Home_Network_Basics

Nivel de enlace en redes corporativas actuales

802.11 trabaja en nivel de enlace.

- Normalmente el paquete contenido dentro de una trama viajará por diferentes segmentos de red (distintos niveles de enlace), que podrán ser cableados o inalámbrico
- Las LAN cableadas (típicamente ethernet) modernas en entornos corporativos suelen ser bastante compleja, incluyendo funcionalidad no prevista en el diseño original de los niveles ISO/OSI.
  Aunque esta funcionalidad permanece oculta dentro de este nivel de abstracción, invisible a niveles superiores e inferiores

El modelo conceptual de las LAN de cable se corresponde con las LAN de los años 80, pero en la actualidad:

- El cable no es coaxial, sino fast ethernet o gigabit ethernet sobre par trenzado
- Los conmutadores (*switches*) ofrecen topología en estrella, la topología de bus ha desaparecido.
- Es frecuente unir varios segmentos físicos en un mismo segmento lógico mediante VPN (*Virtual Private Networks*)
- También es habitual el caso inverso: Un mismo segmento de red físico se presenta al nivel de red como varios segmentos distintos (VLAN).
  Metáfora: coloreado de tramas y de bocas del conmutador
- Puede haber topologías complicadas, enlaces redundantes y necesidad de encaminamiento
- Puede ser necesario combatir los bucles

Aunque el nivel de enlace se haya complicado, sigue siendo un nivel de enlace, sigue demandando lo mismo del nivel inferior y ofreciendo lo mismo al nivel superior

- Está por encima del nivel físico, del que utiliza sus servicios: El nivel físico transmite bits entre máquinas contiguas, el nivel de enlace forma con ellos tramas, detecta errores y opcionalmente los corrige.
- Está por debajo del nivel de red, al que ofrece la abstracción de que dos máquinas se comuniquen como si estuvieran en el mismo segmento de red (lo estén o no).

Elementos de una red 802.11

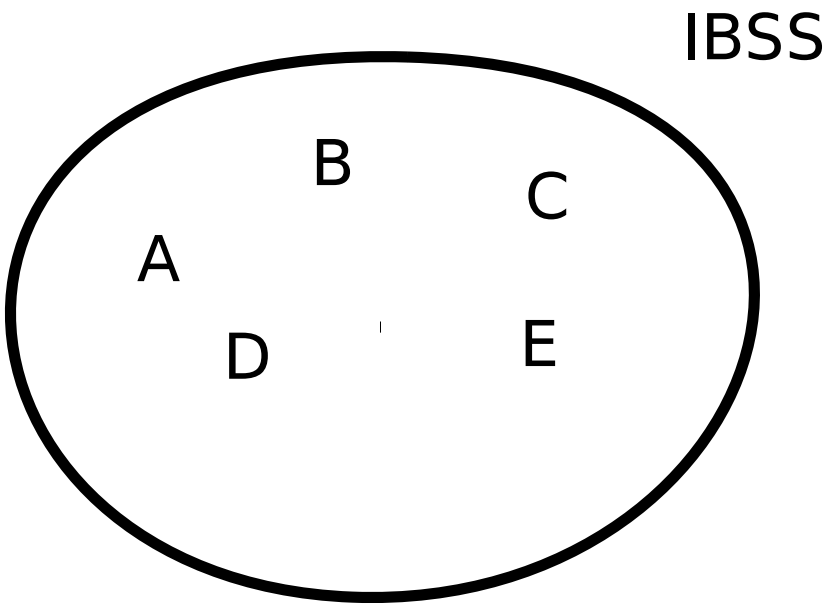
- *Wireless Station*. WSTA. Estación inalámbrica, Nodo móvil
- *Access Point*. AP. Punto de acceso
- *Distribution System*. DS. Sistema de Distribución. Troncal (típicamente cableado) y servicios que conectan varios AP de la misma red 802.11 (siempre en nivel de enlace)

Acceso al medio

- *Distributed Coordination Function*, DCF. Función de coordinación distribuida. Con contienda. CSMA/CA y MACA
- *Puntual Coordination Function*. PCF. Función de coordinación puntual. Sin contienda. Opcional, poco usada

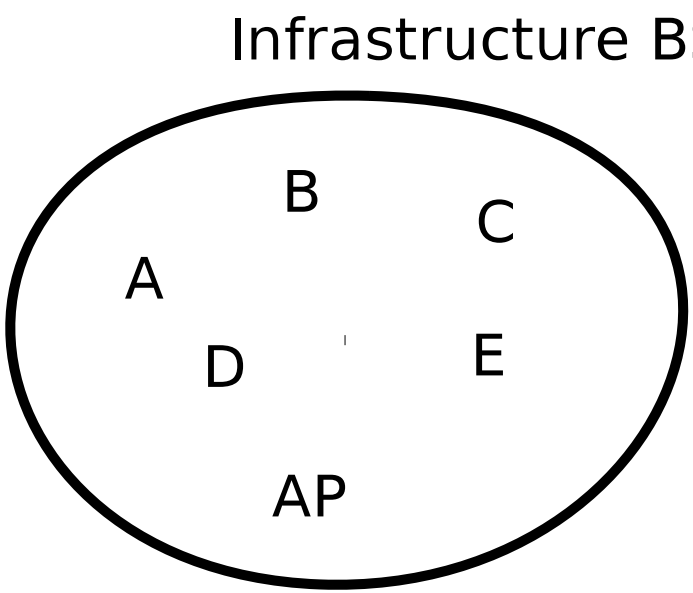
Celda independiente

- Sin AP.
  Independent Basic Service Set. IBSS. Modo *ad-hoc*. Emplea DCF. Tráfico directamente entre los WSTA



Celda con infraestructura

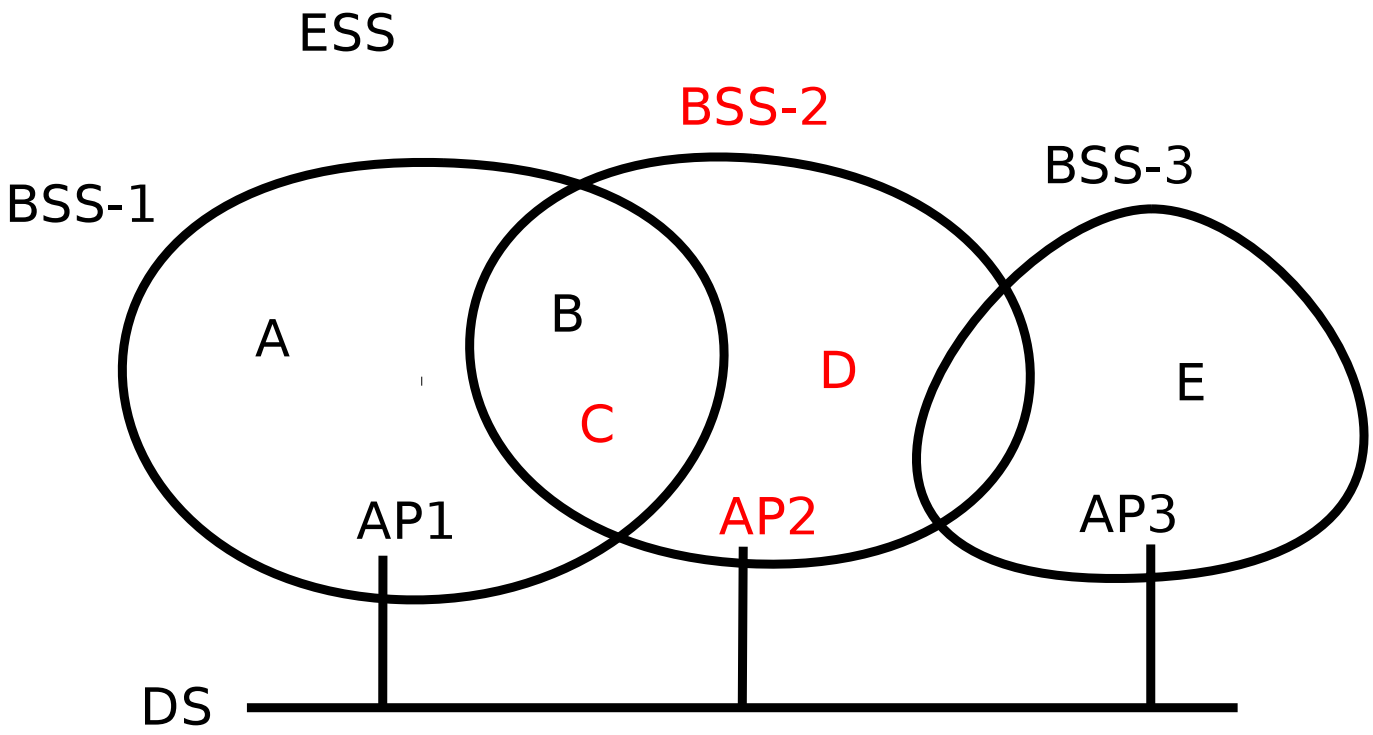
- Un AP.
  Infrastructure Basic Service Set . [1] *Infrastructure BSS*.
  Emplea DCF y opcionalmente PCF. Cada trama siempre pasa por el AP



[1] BSS: Conjunto de estaciones asociadas lógicamente. BSA (Basic Service Area): Area que contiene los miembros de un BSS. Puede contener estaciones de otro BSS

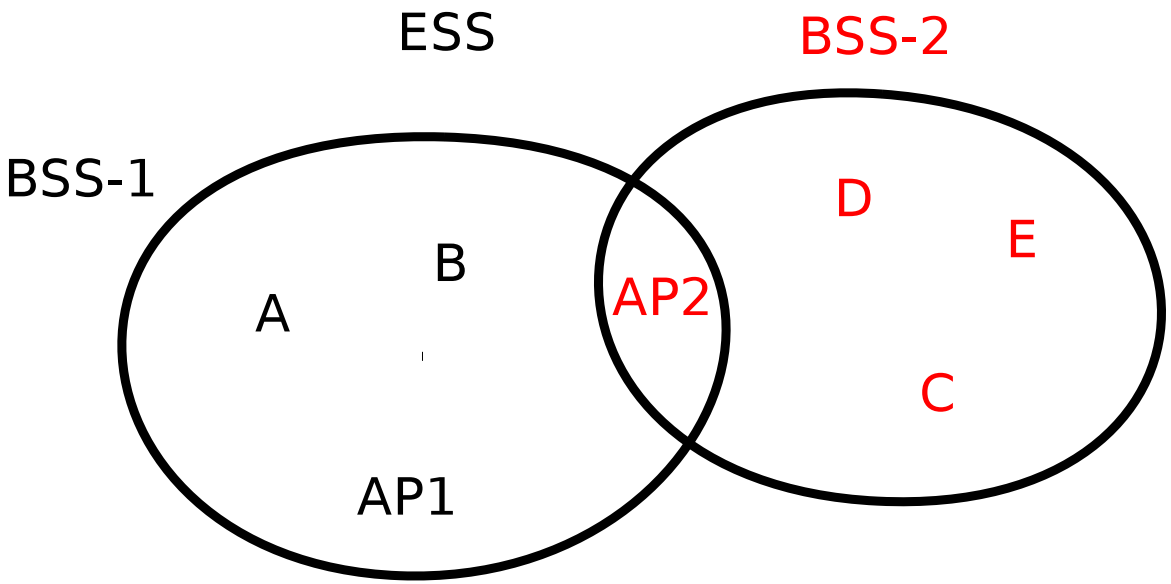
Celda extendida

- Más de un AP. *Extended Service Set*. ESS. DCF y opcionalmente PCF. Cada trama pasa por uno o más AP.



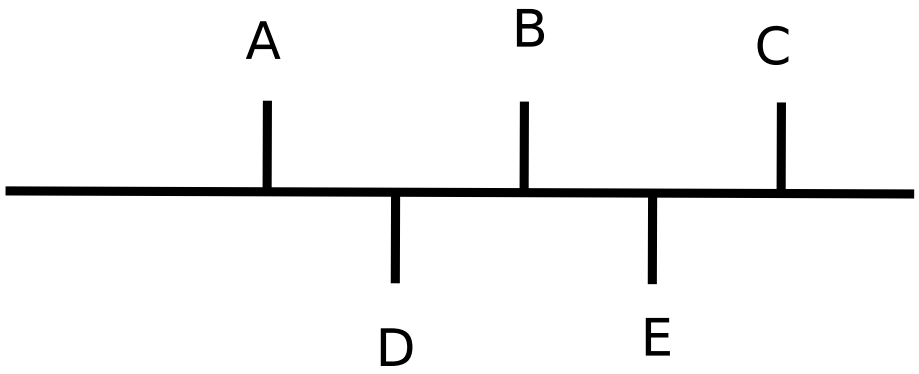
Wireless Distribution System

- Varios AP. No hay un DS independiente entre ellos
- Todos en el mismo canal. SSID común o diferente
  - Un AP actúa como *maestro*, también llamado o *WDS AP*
  - Otro AP actúa como *repetidor*, también llamado *esclavo* o *WDS Station*
- No estándar. No lo soportan todos los equipos. Cada *chipset* lo hace a su manera. Puede haber incompatibilidad incluso dentro de la misma marca
- Incompatible con varios mecanismos de seguridad



- El rendimiento en las estaciones C, D y E cae a la mitad, puesto que hay un salto adicional para cada trama
- Es posible encadenar varios AP

Importante: Las cuatro redes anteriores son percibidas de la misma manera desde el nivel de red y superiores



En la actualidad son frecuentes topologías complejas en el nivel de enlace (ESS, VPN, VLAN).
Esta complejidad debe quedar oculta en nivel de enlace, para el nivel de red las estaciones siguen siendo vecinas

- Los routers WiFi que tenemos en casa ¿son AP?

Identificadores de red y de celda

SSID: *Service Set Identifier*

- Identificador de red, identifica cada ESS
- Entre 0 y 32 bytes, no necesariamente ASCII
- Incluido en cada Beacon
- 0 bytes: broadcast SSID

BSSID: *Basic Service Set Indentifier*

- Identifica cada BSS
  - En modo Ad-Hoc, son 46 bits generados aleatoriamente
  - En modo infraestructura, son los 48 bits de la MAC del AP

Modos de un AP

Un AP puede trabajar en:

- Master mode
  Modo más habitual en un AP, Infraestructure BSS
- Managed mode
  También llamado *client mode*. El AP se comporta como un WSTA en un BSS, usa el canal fijado para la BSS, se comunica con otros a través del maestro
- Ad-Hoc mode
  IBSS
- Monitor mode
  Acepta todas las tramas para todas las estaciones de todos los SSID. No es lo mismo que el modo promiscuo (aceptar todas las tramas de su propio SSID)

Tipos de Access Point

AP típico para casa / oficina pequeña

- Equipo compacto con antena integrada
- Puede incluir cliente DHCP, servidor DHCP, NAT, interfaz WAN (ADSL, cable)
- Se administra mediante servidor web en dirección 192.168.0.1, 192.168.1.1 o 10.0.0.1
- Los equipos antiguos solo incluían WEP y filtros MAC. Los modernos también tienen WPA

AP típico para uso corporativo

- Implementa protocolo para permitir movilidad entre BSS
- Los antiguos permitían cambiar tarjetas de radio
- Soporte de protocolos futuros mediante actualización del firmware
- PoE: Power over the Ethernet (IEEE 802.3af, año 2003)
- Antena independiente, intercambiable y regulable
- Virtual Access Points. Varios SSID
- Autentificación de usuarios integrada con BD corporativa. Permite uso como HotSpot
- Integración con VLAN dinámica en función del usuario
- Herramientas de monitorización y control
- Configuración mediante scripts SNMP, centralizables
- Restricciones de seguridad eléctrica y anti-incendios (*plenum-rated*)

Distribuciones Linux para routers inalámbricos

- La mayoría de los AP domésticos son ordenadores con Linux
- Se les puede cambiar el firmware original, muy limitado, para instalar otro mucho más flexible, como OpenWRT
- El primer modelo y más popular, es el Linksys WRT54G, pero no es el único
- De esta forma, un AP doméstico ofrece buena parte de la funcionalidad de uno corporativo, como p.e.
  - Dropbear: Cliente y servidor ssh
  - TC: *Traffic Control* QoS
  - Asterisk: Centralita (PBX,*Private Branch Exchange*)
  - ChilliSpot: Autentificación de usuarios mediante web cautivo. Se integra con un servidor radius
  - Kismet. sniffer y detector de intrusiones

Nivel físico: canales en 802.11b,g

- 14 canales diferentes, cada uno con espectro expandido
- Pueden coexistir varias redes en la misma zona (cada una en un canal)
- Los canales se solapan, no siempre puede haber coexistencia
- Según los países/regiones, algunos canales no están permitidos.
- Los Access Point pueden buscar canales libres

Canales Permitidos

- Estados Unidos: 1-11
- Japón: 1-14
- Casi todo el resto del mundo: 1-13

Cada canal esta separado 5 Mhz del contiguo pero cada flujo de datos necesita 22 Mhz. Canales óptimos

- Estados Unidos: 1,6,11
- Europa: 1, 6 y 11; o bien 2, 7 y 12; o bien 3, 8 y 13
  Otra alternativa: 1, 7, 13

Formato de trama 802.11

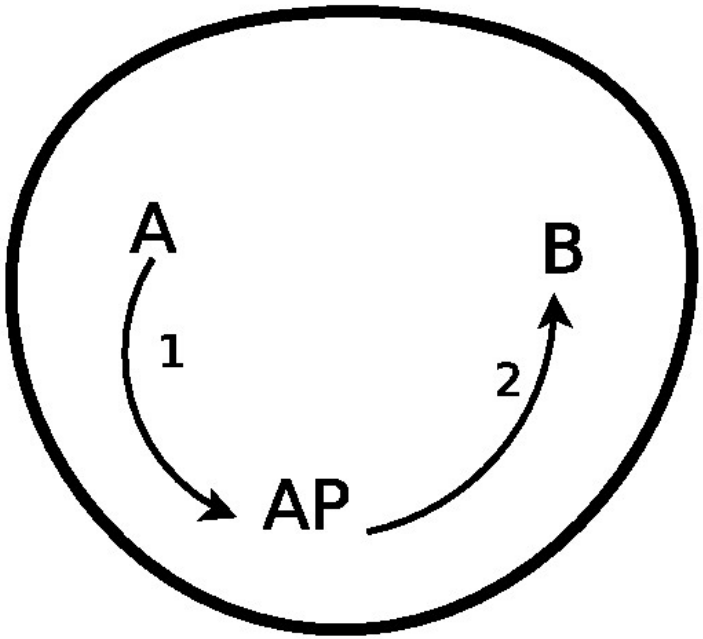
Tres tipos de trama

- Gestión. (*management frame*)
  Association request, Association response, Reassociation request, Reassociation response, Probe request, Probe response, Beacon, Authentication, Deauthentication, ...
- Control. (*control frames*)
  RTS, CTS, ACK, QoS, Power Save (PS)-Poll ...
- Datos. (*data frames*)
  Data, null data, ...

- Direcciones MAC de 48 bits, iguales a las de todas las redes IEEE 802
- Compatible con 802.3 (los AP traducen entre ambos formatos)
- Admite hasta 2304 bytes de datos, aunque en IP solo se usarán hasta 1500
- Las trama 802.11 incluye un *Frame Check Sequence* (*FCS*) *aka* CRC
- Si el CRC es correcto, se envía ACK

En una trama 802.11 hay espacio para 4 direcciones

- en modo ad-hoc sólo se usan dos
- en modo infraestructura se usan 4:
  - Origen. (*Source address*). Interfaz que crea la trama
  - Destino. (*Destination address*). Destino final
  - Transmisor. (*Transmitter address*). Estación inalámbrica que transmite
  - Receptor. (*Receiver address*). Estación inalámbrica que debe procesar la trama (AP o WSTA)

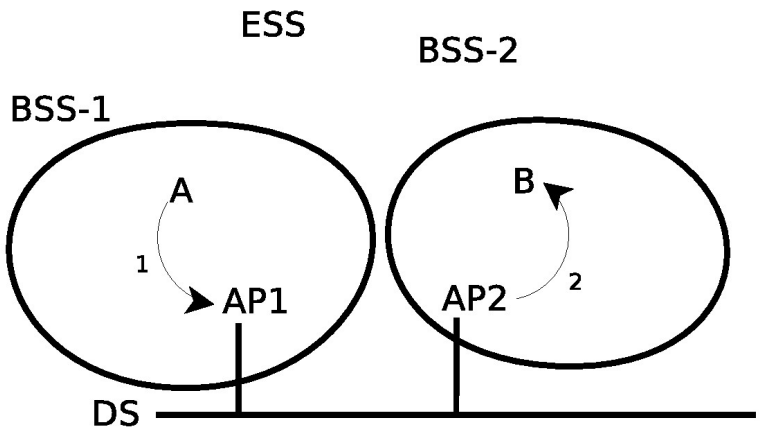


Trama 1

- Origen: A
- Destino: B
- Transmisor: A
- Receptor: AP

Trama 2

- Origen: A
- Destino: B
- Trasmisor: AP
- Receptor: B



Trama 1

- Origen: A
- Destino: B
- Transmisor: A
- Receptor: AP1

Trama 2

- Origen: A
- Destino: B
- Trasmisor: AP2
- Receptor: B

- ¿Dónde veríamos una trama como esta?
  - Origen: A
  - Destino: B
  - Trasmisor: AP1
  - Receptor: AP2
- En lo relativo a las direcciones que aparecen en la trama ¿En qué se diferencia un AP en 802.11 frente a un bridge en 802.3?

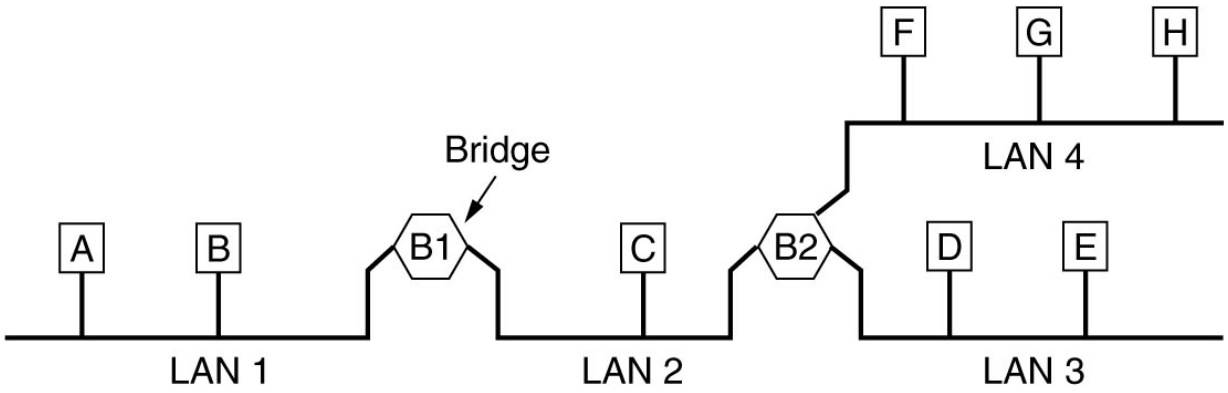
El sistema de distribución

- 802.11 no especifica cómo funciona el DS
- 802.11f intentó normalizarlo. Propuesto en 2003, retirado en 2006
- En el hardware de primera generación, se exigía verdadero nivel de enlace entre los AP
- El hardware moderno puede soportar conexiones punto a punto

Según los equipos empleados, el DS puede ser de distinta complejidad

- Puede limitarse a llevar todas las tramas a todos los AP
- Puede emplear un algoritmo como el de aprendizaje, y llevar cada trama solo al AP al que se haya asociado la WSTA

Algoritmo de aprendizaje



- B2 aprende que F está en la LAN 4. No envía a la LAN 3 las tramas para F
- B2 no es un router. Todas las máquinas tienen la percepción de compartir el medio

- En una red de cable, cada máquina está en una sola red ¿cierto?
- ¿Y en una red inalámbrica?
- ¿El sistema de distribución puede tener enlaces redundantes?

Spanning Tree Protocol

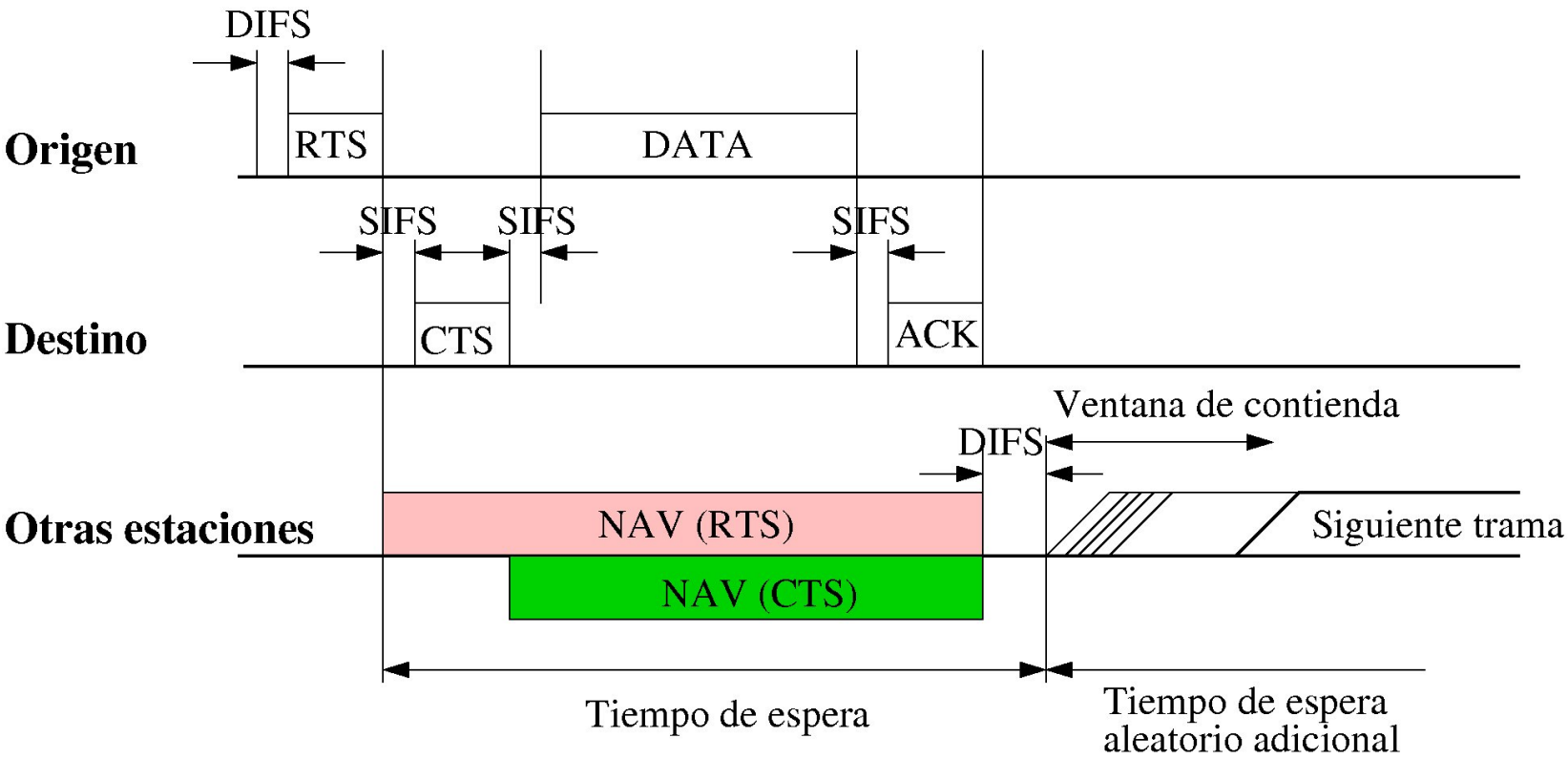
Acceso al medio en 802.11b,g

- Una de las técnicas empleadas es MACA, con un ACK adicional al final:
  - RTS: permiso para transmitir
  - CTS: listo para recibir una transmisión
  - DATA: trama de datos
  - ACK: trama de datos recibida correctamente
- NAV (Network Allocation Vector). Portadora virtual. El RTS, CTS y dato indican durante cuánto tiempo permanecerá ocupado el medio.

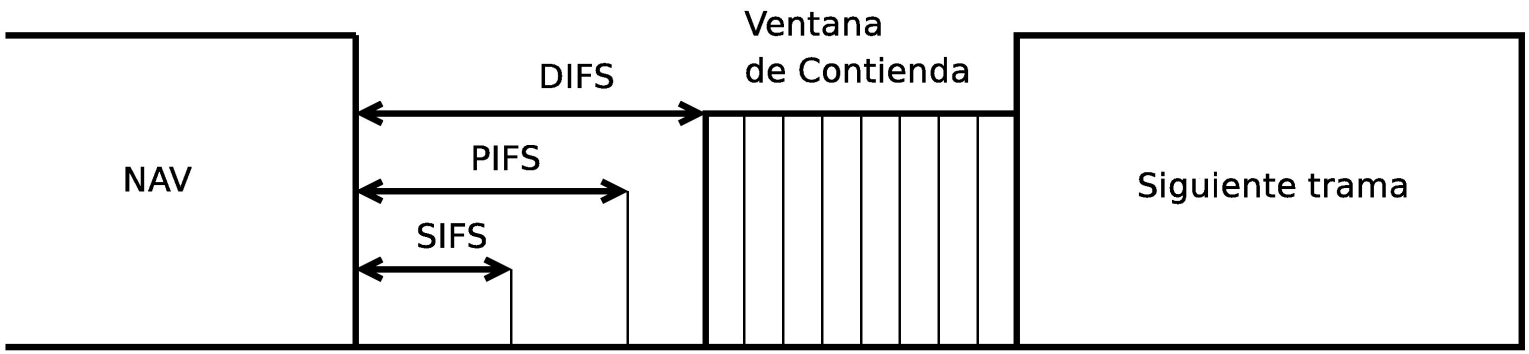
- Si no se recibe el ACK, se reintenta el envío (como si no se recibe el CTS).
- El ACK implica que cada trama de datos es asentida (innecesario en una red de cable)
- ¿Qué pasa en broadcast o multicast?

MACA genera una sobrecarga, RTS y CTS son opcionales y en la práctica no se usan mucho
No son necesarios si:

- Hay pocas estaciones. Es sencillo retransmitir
- La red es muy densa. Todos las estaciones estan dentro del radio de alcance de todos
- Las tramas son muy pequeñas. Alguna tarjetas permite configurar el umbral (*RTS threshold*) a partir del cual se considera que una trama es *pequeña*


DIFS
Origen
RTS
DATA
SIFS
SIFS
SIFS
Destino
CTS
ACK
Ventana de contienda
DIFS
Otras estaciones
NAV (RTS)
Siguiente trama
NAV (CTS)
Tiempo de espera
Tiempo de espera
aleatorio adicional

La variación de los espacios entre tramas crea niveles de prioridad



- SIFS (Short InterFrame space, espacio corto entre tramas). Tramas de prioridad más alta: CTS, ACK
- PIFS (PCF InterFrame space, espacio entre tramas de la función de coordinación Puntual). Tramas sin contienda.
- DIFS (DCF InterFrame space, espacio entre tramas de la función de coordinación distribuida). Tramas con contienda (RTS).

Ventana de contienda: metáfora

Podemos explicar el funcionamiento de la ventana de contienda con la siguiente metáfora:

- Juego de n jugadores, solo puede ganar 1. El valor de n es desconocido
- Cada jugador tira uno o varios dados, no de 6 caras sino unos *dados de rol* con diferente número de caras
- Gana el jugador con número más bajo, quienes pierden lo vuelve a intentar, con un dado de más caras
- En caso de empate, todos pierden, aunque no lo perciban inicialmente
- Cuando se llega al dado con el número máximo de caras, se siguen repitiendo tiradas m veces

Ventana de contienda: funcionamiento real

- La ventana de contienda se divide inicialmente en 31 ranuras
- La estación intenta transmitir en una ranura aleatoria
- Si el medio está ocupado, lo reintenta con una ventana de 63 ranuras
- Si sigue ocupado, reintenta con 127, 255, 511 y 1023
- Cada ranura siempre tiene la misma longitud (mientras no cambie la versión de 802.11), por tanto en cada reintento la ventana (casi) dobla su tamaño
- Con 1023 se puede reintentar varias veces antes de desistir
- Cada vez que el envío tiene éxito o se da por perdido, la ventana vuelve al mínimo
- Cuanto más moderna es la versión de 802.11, mas cortos son los espacios y las ranuras. Pero el número de espacios y ranuras, se mantiene

IEEE 802.11e

En el año 2005, aparece IEEE 802.11e que añade calidad de servicio (QoS)
Aparecen 4 nuevas categorías de tramas, de diferente prioridad

- Background
- Best Effort
- Video
- Voice

Para diferenciar este tráfico se definen los tiempos de acceso al medio y las ventanas de contención correspondientes

Mejora de la fiabilidad

- Una estación adapta dinámicamente la velocidad de transmisión a las pérdidas
- Si hay muchas pérdidas, la trama se puede dividir en fragmentos más pequeños, cada uno con su propio CRC, que se envían por parada y espera
  - Con parada y espera, el número de retransmisiones no es conocido a priori, con lo que NAV no puede saber cuánto tiempo estará ocupado el medio. ¿Cómo evitar las colisiones?

Compatibilidad 802.11b 802.11g

La modulación en 802.11g es distinta a 802.11b. Pero se añaden mecanismos para hacerlo compatible

- Los interfaces 802.11g pueden usar la modulación de 802.11b
- Obviamente, a la inversa no es cierto

Sean
A,B,C: 802.11b
X,Y,Z: 802.11g

- Un AP debe enviar balizas como en 802.11b, porque no sabe si el receptor será A,B,C o X,Y,Z

- Máquinas que cambian tramas | Otras máquinas en la celda

  A <--> X | (No importa)

  No hay problema. Se usa 802.11b
- Máquinas que cambian tramas | Otras máquinas en la celda

  X <--> Y | Z

  No hay problema. Se usa 802.11g

- Máquinas que cambian tramas | Otras máquinas en la celda

  X <--> Y | A

Problema. A no va detectar las tramas X <--> Y
Es necesario que X e Y *protejan* sus tramas

- O bien
  CTS* , Dato, ACK
- O bien
  RTS*, CTS*, Dato, ACK

(*) Trama de control al estilo 802.11b

Asociación al AP

Mediante las tramas de gestión correspondientes:

1. Scanning
   - Activo
     - La WSTA envía tramas `ProbeRequest` (en todos los canales) Puede especificar SSID. Incluye las velocidades que soporta
     - los AP vecinos contestan con un `ProbeResponse`
   - Pasivo
     - La WSTA espera el beacon de un AP (buscando en todos los canales)
2. Autentificación
3. Asociación
   - La WSTA selecciona AP y le envía `AssociationRequest`
   - El AP elegido envía un `AssociationResponse`
   - Opcionalmente, la WSTA se despide del AP anterior (si lo hay)

Roaming

La palabra *roaming* es ambigua, según el contexto puede referirse a

- Cambiar de AP
- Cambiar de AP manteniendo las conexiones abiertas
  - Saliendo incluso de subred IP
- Mantener la sesión entre dos redes distintas. P.e. 802.11 y UMTS

Ahorro de energía

- La movilidad suele implicar uso de baterías, es muy importante ahorrar energía
- Una WTSA puede *dormir* (*Powersaving Mode, PS*)
  - En Modo *Infraestructure BSS* el funcionamiento es sencillo, todo el tráfico pasa por el AP, que conoce el estado de cada WSTA, almacena las tramas para los dormidos y las envía cuando despiertan
  - En modo IBSS el funcionamiento es más complejo, el rendimiento es menor, los periodos de *sueño* son menores

- El cliente puede ahorrar energía mediante el flag *power management*
  - 0: *Estoy despierto*
  - 1: *Voy a dormir, guárdame lo que venga*

  Esto se envía en tramas sin ningún otro contenido (*Null function (no data)*
- En las versiones iniciales, el cliente dormía entre baliza y baliza (enviada p.e. cada 100 ms)
- Si el cliente tiene que enviar audio, este sueño puede ser demasiado largo. En el año 2005 aparece APSD: *Automatic Power Save Delivery*: el WSTA duerme hasta que tiene algo que enviar (p.e. cada 20 ms), entonces también recibe lo pendiente

802.11h

802.11a y 802.11n emplean banda 5GHz, que en EEUU esta libre para ICM pero en Europa puede interferir con radar y satélites. Para evitarlo, se desarrolla 802.11h

- Selección dinámica de frecuencias (DFS Dynamic Frequency Selection)
  - AP y WSTA acuerdan qué canales emplear
    En el association request, el WSTA dice qué canales soporta, el AP le admite, usa esos, o le rechaza.
  - Intervalos de silencio: en el beacon hay instrucciones para que todos fijen su NAV y queden un tiempo en silencio, para detectar radar o satélites
- Control de la potencia de transmisión (TPC Transmitter Power Control)
  - ¿Cuánto más potencia, mejor?
  - Para cada trama, se responde cuántos dB hay que subir o bajar para alcanzar potencia *óptima*

Point Coordination Function (PCF)

Técnica de sondeo (*polling*)

- Hay un periodo sin contienda, AP determina quien transmite
- El AP pregunta a cada WSTA si tiene algo que transmitir. Puede incluir datos en *piggybacking*
- Cada WSTA responde con una trama de datos, o con una trama *null*
- Se fija un NAV al principio del periodo de contienda

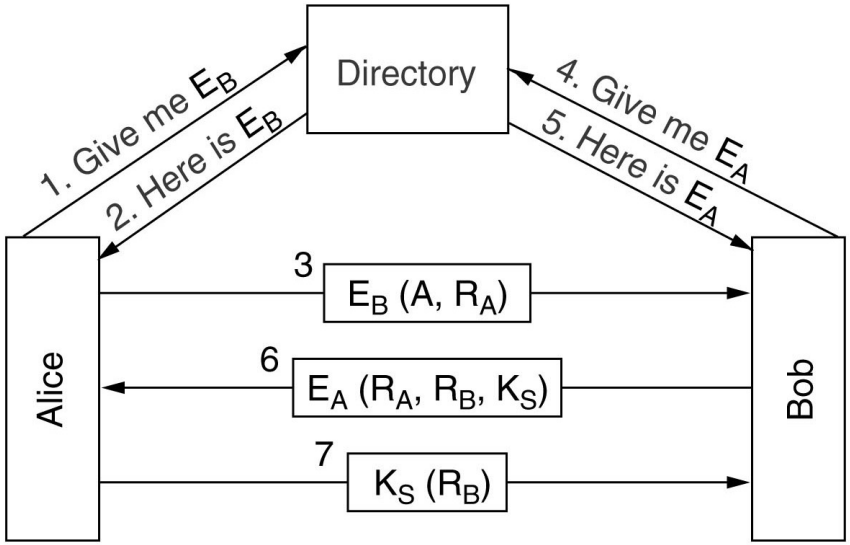
Muy complicado, no se usa

Criptografía de clave pública

Año 1976, Diffie y Hellman.

- E: Clave de cifrado o pública. D: Clave de descifrado o privada D. Son distintas (asimétricas)
- $D(E(P)) = P$
- Muy dificil romper el sistema (p.e. obtener D) teniendo E.
- La clave privada sirve para descifrar. Debe mantenerse en secreto
- La clave pública sirve para cifrar. Puede conocerla todo el mundo (lo importante es que se conozca la clave correcta)
- Conociendo la clave pública de alguien, podemos cifrar un mensaje que solo él, con su clave privada, podrá descifrar

Autenticación con clave pública



1,2: A obtiene la clave pública de B
3: A envía su remite y un reto cifrados con la clave de B
4,5: B obtiene la clave pública de A
6: B cifra, con la clave de A: el reto de A, un reto nuevo y una clave simétrica
7: A envía el reto de B con la clave simétrica, que se empleará en la sesión

- El espectro es un medio compartido: cualquiera puede escuchar.
- No es muy distinto del cable: hay que alcanzar la misma seguridad (pero es más fácil acceder al espectro que a un cable)
- Opciones en 802.11:
  - Nada
  - Filtrado MAC. Fácil de saltar. No confidencialidad, integridad ni autenticación. Puede bastar para el acceso no autorizado de usuarios ordinarios
  - WEP (Wired Equivalent Privacy): Clave de 64 o de 128 bits. Débil, roto.
  - WEP dinámico. Pequeña mejora de WEP. No estándar.
  - WPA (Wireless Protected Access): Clave de 128 bits.
  - WPA2 (IEEE 802.11i): Más robusto, permite claves compartidas previamente, o claves individuales

No radiar el SSID apenas aporta incremento de seguridad. No evita los beacons

Características de WEP

Algoritmo de cifrado RC4

- Criptografía tradicional, de clave secreta
- Cifrado de flujo *Stream cipher*. Año 1987
- texto-claro XOR keystream = texto-cifrado
  texto-cifrado XOR keystream = texto-claro
  El keystream (flujo clave) es una secuencia pseudoaleatoria, generada a partir de clave secreta y vector de inicialización *initialization vector, IV*

- WEP no especifica cómo distribuir la clave, se supone que se hace a mano
- Toda la ESS comparte la misma clave para los broadcast
- El AP usa una clave distinta para cada WSTA en las tramas unicast
  - 4 slots para claves en los WSTA
  - Algunos cientos de slots en los AP
- El vector de inicialización se transmite en abierto
- La integridad se verifica mediante CRC-32

Debilidades de WEP

- `texto_claro xor keystream = texto_cifrado`

  ¿Qué pasa si `texto_claro=0` ?
- `texto_claro_1 xor keystream = texto_cifrado_1`
  `texto_claro_2 xor keystream = texto_cifrado_2`

  `a= texto_claro_1 xor texto_claro_2`
  `b= texto_cifrado_1 xor texto_cifrado_2`

  ¿Qué relación hay entre a y b?

- Misma clave de cifrado y autenticación
- Clave distribuida a mano
- Clave secreta pequeña (aunque hay versiones de 128 bits)
- Integridad pensada para detectar errores, no segura criptográficamente
- Todos los cifrados de flujo son vulnerables si se reutilizan los keystream. El único método de clave secreta 100 % seguro es el *one-time pad*: clave perfectamente aleatoria, sin reutilizar nunca

La potencia del Hardware y la legislación en EEUU era diferente en 1999.

WEP dinámico

WEP mejorado. No estándar.

- Las claves se distribuyen automáticamente
- Usa un slot para los unicast (una clave por cada par), otro para los broadcast
- Es mejor que WEP, pero sigue siendo inseguro

IEEE 802.11i

- Cuando se detectan los problemas de WEP, se empieza a trabajar en IEEE 802.11i
- WPA es una norma de la WiFi alliance, incluye buena parte del borrador de IEEE 802.11i de 2003. Usa RC4, las tarjetas viejas podían actualizarse mediante actualizaciones de firmware
- WPA2 implementa por completo IEEE 802.11i

Autentificación de usuarios en WPA2

- Modo *personal*. Para casa y pequeñas oficinas, PSK: Pre-shared key mode.
  - PBKDF2. Criptografía asimétrica. Razonablemente seguro con contraseñas de calidad
  - WPS: Wi-Fi Protected Setup. El administrador introduce en AP un PIN del WSTA. O pulsa botones simultáneamente. O lectura RFID
- Modo *enterprise*. Para empresas, autentificación de usuarios mediante IEEE 802.1X
  - Integrado con servidor RADIUS
    Remote Authentication Dial In User Service. Norma del IETF muy común en todo tipo de redes para AAA *Authentication, Authorization and Accounting*
    RFC 2138 (año 1997), RFC 2865 (año 2000)
  - EAP: Extensible Authentication Protocol

Encriptación en 802.1X

TKIP: Temporal Key Integrity Protocol
Diferencias con WEP:

- Una clave maestra genera las claves RC4 con las que se encriptan las tramas
- Cada trama usa una clave RC4 diferente
- Numeración de las tramas
- Integridad verificada mediante algoritmo MIC

Probablemente WPA2 seguirá siendo seguro durante muchos.
¿Cómo podemos afirmar esto, si continuamente se rompen los sistemas de protección de audio, vídeo, eBooks...?

Referencias

- "802.11 Wireless Networks (2nd ed), M. Gast, Ed. O'Reilly
- "Computer Networks" (5th ed), A. Tanenbaum