Redes Inalámbricas

Redes de Ordenadores para Robots y Máquinas Inteligentes

GSyC
Departamento de Teoría de la Señal y Comunicaciones y
Sistemas Telemáticos y Computación

Marzo de 2024

Contenidos

1 Introducción

2 Nivel Físico

3 Arquitectura Funcional y Topologías

4 Descubrimiento, autenticación y asociación

5 Nivel MAC

6 Trama 802.11

Introducción

- IEEE 802.11 es el estándar de facto para redes WLAN (Wireless Local Area Networks). En este estándar se especifica:
  - **El control de acceso al medio** (MAC): Organiza el modo de acceso de las estaciones para el uso de un medio compartido:
    - Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). Acceso múltiple por detección de portadora y **evitación de colisiones**.
    - Diferente a Ethernet 802.3 CSMA/CD que utiliza una técnica de detección de colisiones.
  - **El nivel físico**: Establece diferentes tipos de codificación/modulación para el envío de datos. Da lugar a diferentes estándares y velocidades.
    - 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, 802.11ax, 802.11be

Evolución de los estándares 802.11

- Evolución de los estándares 802.11 (en 2018 Wi-Fi Alliance creó la terminología "Wi-Fi X"):
  - **802.11** (Wi-Fi 0, no oficialmente): banda 2.4GHz, 2 Mbps
  - **802.11b** (Wi-Fi 1, no oficialmente): banda 2.4GHz, 11 Mbps
  - **802.11a** (Wi-Fi 2, no oficialmente): banda 5 GHz, 54 Mbps
  - **802.11g** (Wi-Fi 3, no oficialmente); banda 2.4 GHz, 54 Mbps
  - **802.11n (Wi-Fi 4)**: bandas 2.4 GHz y 5 GHz, 600 Mbps
  - **802.11ac (Wi-Fi 5)**: banda 5 GHz, 1300 Mbps
  - **802.11ax (Wi-Fi 6, Wi-Fi 6E)**: bandas 2.4 Ghz, 5 GHz, 6 GHz (6E), 10 Gbps
  - **802.11be (Wi-Fi 7, 2024)**: bandas 2.4 GHz, 5 GHz, 6 GHz, 46 Gbps

Datos expresados en condiciones óptimas, a 1 m de distancia del emisor y sin interferencias.

Enlaces inalámbricos

- **Pérdidas de propagación**: la radiación electromagnética se atenúa según atraviesa la materia (paredes), la intensidad de la señal decrece según se incrementa la distancia entre emisor y receptor.
- **Interferencias con otras señales**: Una banda de frecuencias puede ser usada con diferentes fines y por diferentes dispositivos. Por ejemplo la banda de 2.4 GHz usada para redes inalámbricas 802.11b también la usan microondas y bluetooth. El ruido electroagnético presente en el entorno también puede provocar interferencias.
- **Prograpación multicanal**: parte de las ondas electromagnéticas se reflejan en los objetos y paredes, provocando que la señal llegue al receptor a través de caminos con diferentes longitudes y por tanto la señal no llega de forma nítida.

- **CONSECUENCIA:** los errores de transmisión serán más comunes en los enlaces inalámbricos que en los cableados. En los protocolos de transmisión en medios inalámbricos se utilizan, además de técnicas de detección de errores, retransmisiones para tener fiabilidad en el nivel de enlace (a diferencia de los protocolos de transmisión en medios guiados).

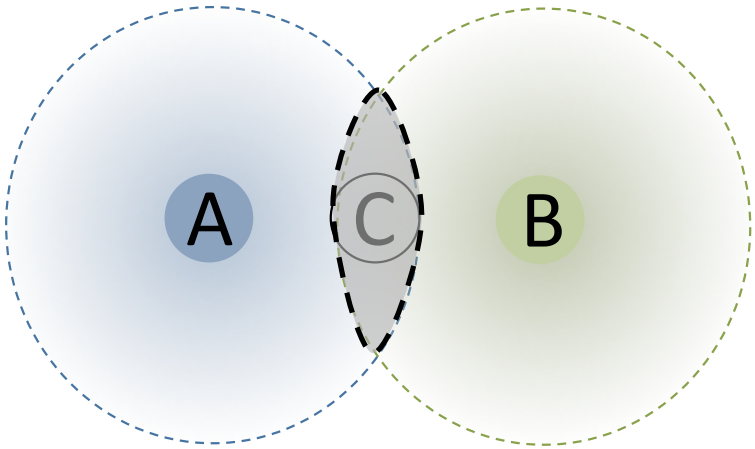
Acceso al medio en redes inalámbricas

- En redes inalámbricas escuchar el medio no da suficiente información para saber si habrá o no colisiones, por lo que los protocolos CSMA/CD que se usan en redes de cable no son aplicables:
  - El alcance de las estaciones inalámbricas es limitado: no todas oyen a todas
  - Lo que importa es lo que oye el receptor: habrá colisión si el receptor oye dos señales a la vez

Acceso al medio en redes inalámbricas

El problema del "nodo oculto"

- En redes cableadas, el emisor antes de transmitir escucha para, si hay otra transmisión en curso, esperar para no colisionar.
- Pero en redes inalámbricas, en algunos casos no escuchar nada no significa que no vaya a haber colisión:

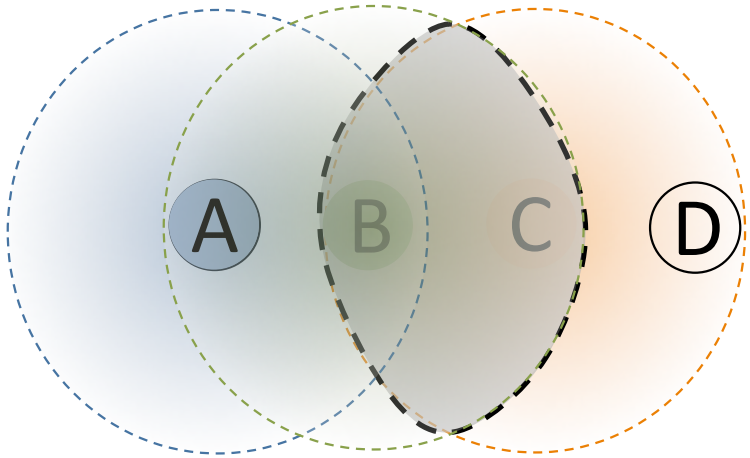


- A se plantea si transmitir a C mientras B está ya transmitiendo a C.
- A no oye a B, pero C sí. Por lo tanto si A transmite habrá colisión en el receptor (C) sin que A lo sepa. B es un nodo oculto para A.

Acceso al medio en redes inalámbricas

El problema del "nodo expuesto"

- En redes inalámbricas, en algunos casos escuchar otra señal no significa que sí vaya a haber colisión:



- B se plantea trasmitir a A mientras C ya está transmitiendo a D.
- B oye a C antes de transmitir, y se espera. Pero si transmitiera a A (que no oye a C), A recibiría la transmisión de B sin problema. C es un nodo expuesto para B.

Evitar colisiones en redes inalámbricas

- Como lo importante es lo que escucha el receptor, algunas técnicas le hacen hablar a priori. Por ejemplo:
  - El emisor solicita permiso para enviar utilizando una trama RTS (Request to Send).
  - El receptor envía el permiso a través de una trama CTS (Clear to Send). Dado que esta trama CTS alcanza a todas las máquinas en el alcance del receptor, todas ellas conocen que hay una estación que ha recibido el permiso para enviar, y por tanto no enviarán nada (durante un tiempo).
  - El receptor debe confirmar que ha recibido los datos enviando un ACK.
- Además, en redes inalámbricas se intenta evitar las colisiones haciéndolas estadísticamente poco probables aunque varias estaciones transmitan a la vez: técnicas de espectro expandido.

Relación señal ruido (SNR)

- La señal transmitida en origen llega al receptor degradada por las caracterísiticas de los enlaces inalámbricos y el ruido del entorno.
- La **relación señal ruido** (SNR, Signal-to Noise Ratio) es una medida de la intensidad de señal recibida (la información que se está transmitiendo) y el ruido. Se mide en decibelios (dB).

$$SNR = 20 \log(\frac{señal}{ruido})[dB]$$

$\uparrow$ SNR $\rightarrow$ más fácil será extraer la señal del ruido

- Las técnicas de modulación se utilizan para codificar la información para su transmisión a través de un medio inalámbrico. Para un determinado **esquema de modulación**:
  - $\uparrow$ SNR $\rightarrow \downarrow$ tasa de errores.
  - Dado un valor de SNR, $\uparrow$ velocidad de transmisión $\rightarrow \uparrow$ tasa de errores.
- En determindadas condiciones de SNR se puede adaptar la técnica de modulación en la transmisión y obtener un mejor compromiso de velocidad de transmisión y tasa de errores.

Contenidos

1 Introducción

2 Nivel Físico

3 Arquitectura Funcional y Topologías

4 Descubrimiento, autenticación y asociación

5 Nivel MAC

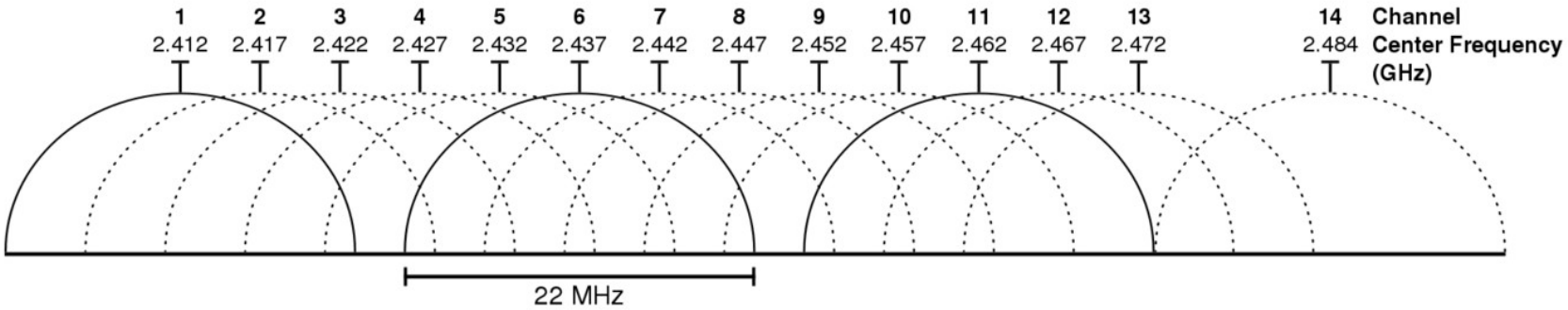
6 Trama 802.11

Nivel físico

- La familia IEEE 802.11 utiliza el espectro radioeléctrico cuyo uso está regulado por el organismo internacional (ITU-R, International Telecommunication Union - Radio). Normalmente es necesario licencia para usar una franja del espectro.
- Algunas de las variantes de la especificación 802.11 utilizan la banda de 2.4GHz (ISM, Industrial, Scientific and Medical) que es no–regulada y está disponible para ser usada sin licencia de emisión. Puede sufrir interferencias con electrodomésticos (como el microondas), o con bluetooth.
- En la banda de 5GHz (y en Wi-Fi 6E y Wi-Fi 7 también en la banda de 6 GHz) no hay otras tecnologías que estén usando esta frecuencia, por tanto hay menos interferencia pero la señal no puede penetrar tan lejos como en 2.4GHz. Alcanza mayores velocidades que en la banda de 2.4GHz pero a menor distancia.

Nivel físico

- Una banda de frecuencias está dividida en **canales**, cada uno de ellos ocupa una parte de la banda o espectro.
- En Europa la banda de 2.4GHz va desde 2.412 MHz a los 2.472 MHz dividida en **13 canales de 20 MHz cada uno separados 5MHz** (en Norteamérica son 11 canales y en Japón 14 separados 12MHz).



- Los canales solapan entre sí y se producen interferencias cocanal. En lugares cercanos se suelen usar canales lo más alejados posible (en Norteamérica: 1, 6, 11; en Europa: 1, 7, 13).
- En la banda de 5GHz hay 21 canales de 20 MHz no superpuestos, también se pueden usar canales de 40MHz, 80MHz, o 160 MHz.

Tecnologías de transmisión

- Modulación por saltos de frecuencia (FHSS, Frequency-Hopping Spread Spectrum)
- Espectro expandido de secuencia directa (DSSS, Direct-Sequence Spread Spectrum)
- Multiplexión por división en frecuencias ortogonales (OFDM, Orthogonal Frequency-Division Multiplexing)

Contenidos

1 Introducción

2 Nivel Físico

3 Arquitectura Funcional y Topologías

4 Descubrimiento, autenticación y asociación

5 Nivel MAC

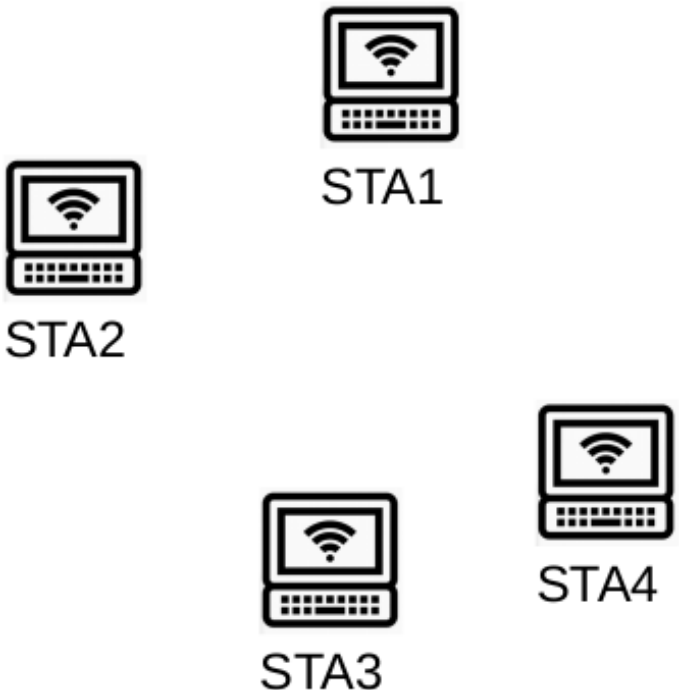
6 Trama 802.11

Arquitectura funcional

- La arquitectura 802.11 está basada en una **arquitectura celular**. El sistema está dividido en celdas cuyo tamaño depende del alcance de la antena emisora/receptora.
- Un **punto de acceso** (AP, Access Point) es una estación base que proporciona conectividad a las **estaciones** (STA) que pueden ser nodos fijos o móviles. Normalmente el punto de acceso está conectado a una red cableada llamada sistema de distribución (DS, Distribution System) que es la que proporciona el encaminamiento a otras subredes.

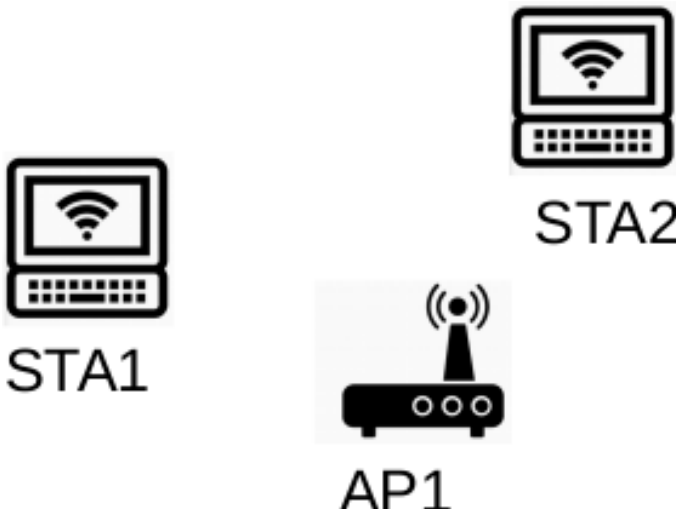
Topologías de red: Redes Ad-hoc o IBSS

- Ad-hoc o IBSS (Independient Basic Service Set): no hay punto de acceso. Los nodos se conectan entre ellos, de igual a igual. Cada trama es recibida por todos los nodos que se encuentran en el rango de alcance del emisor. Para enviar a nodos que no están en el alcance habrá que usar otros nodos en el alcance como *routers*.



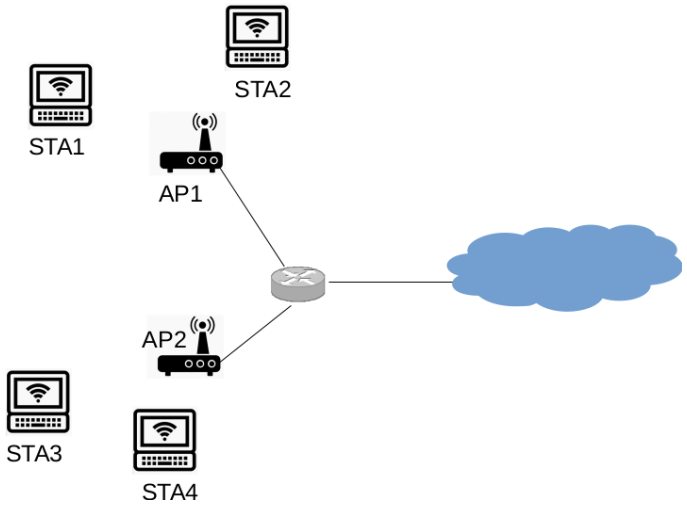
Topologías de red: Redes en modo infraestructura o BSS

- Infraestructura o BSS (Basic Service Set): hay un punto de acceso (AP) al que nodos tienen que asociarse. El AP "actúa como hub" para los nodos asociados a él. La comunicación entre los nodos siempre se realiza a través del AP, incluso aunque las estaciones se encuentren dentro del radio de alcance directo entre ellas.



Topologías de red: Redes en modo BSS extendido o ESS

- **BSS Extendido o ESS (Extended Service Set)**: varios AP conectados normalmente a través de una red cableada. Cada AP da servicio a su celda, correspondiendo con su alcance. Los AP usan un identificador común de forma que los nodos pueden moverse entre celdas y cambiar de AP según reciban mayor potencia de señal. Se denomina *roaming* o itinerancia entre celdas.



- La conexión entre los AP también puede realizarse de forma inalámbrica a través del sistema WDS (Wireless Distribution System).

Contenidos

1 Introducción

2 Nivel Físico

3 Arquitectura Funcional y Topologías

4 Descubrimiento, autenticación y asociación

5 Nivel MAC

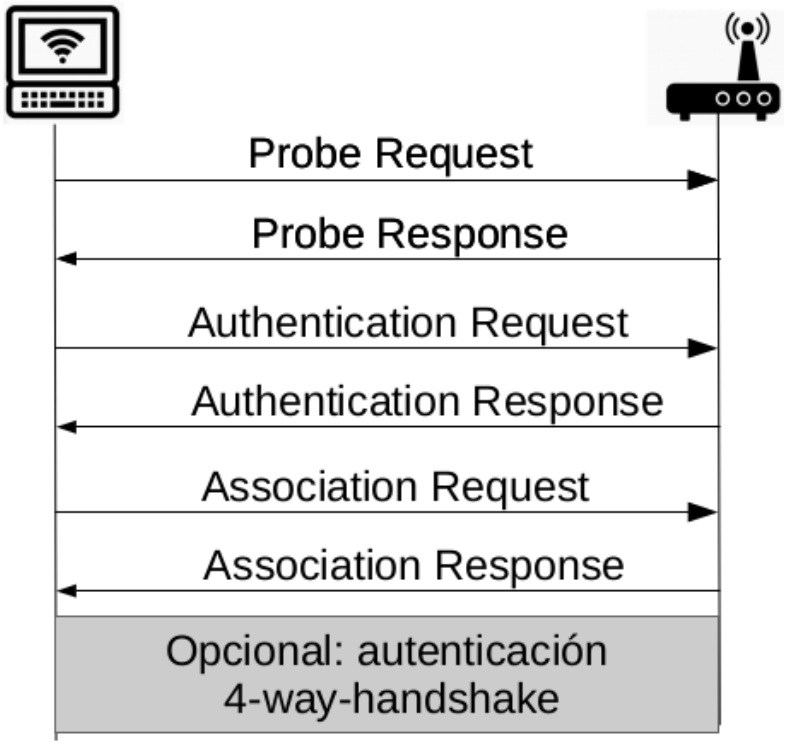
6 Trama 802.11

Canales y elección de SSID

- En el modo infraestructura una estación necesita asociarse con un punto de acceso antes de poder transmitir.
- Un punto de acceso tendrá configurado un **SSID** (Service Set Identifier) y un **canal para transmitir**.
- Una estación puede conocer el SSID de un AP de 2 formas:
  1. El AP envía **tramas baliza** (beacon frames) que incluyen el SSID del AP. Las estaciones recorren todos los canales disponibles en la banda para recibir todas las tramas baliza que están transmitiendo los AP a los que tiene alcance. De esta forma se permite la posibilidad de seleccionar el SSID de un AP, y se denomina **escaneado pasivo**. La estación elige un AP y envía un mensaje `Probe Request` y espera como respuesta un `Probe Response`.
  2. El AP no envía tramas baliza. La estación envía un mensaje `Probe Request` sin especificar SSID a Broadcast para cada canal y espera respuesta (`Probe Response`). Va explorando todos los canales disponibles, y se denomina **escaneado activo**.

Autenticación y asociación

- Fase de descubrimiento: el nodo solicita el descubrimiento de la red y los APs en su alcance responden a dicho mensaje.
- Fase de autenticación: normalmente Open (anteriormente WEP). La autenticación real se realiza después.
- Fase de asociación: el nodo solicita la asociación y el AP confirma. A partir de aquí comienza el intercambio de datos. Normalmente se suele realizar configuración IP a través de DHCP.
- Autenticación opcional: 4-way-handshake. Autenticación mutua.



Fase de descubrimiento: Probe request/response

- La estación envía `Probe Request`, el AP responde con `Probe Response`.
- El mensaje `Probe Request` lleva información sobre:
  - El **SSID** en el que la estación está interesada. Solo si el AP tiene configurado ese SSID responderá. Si SSID=0 (`Wildcard SSID` o *Null Probe Request*), el SSID no está especificado y responderán todos los APs.
  - Las **velocidades soportadas** por el dispositivo, el **canal** usado y **parámetros de mejora** introducidos por el 802.11n HT (Higher Throughput) Capabilities y por 802.11ax HE (High Eficiency) Capabilities.
- El mensaje `Probe Response` lleva información sobre el SSID, las velocidades del AP, algoritmos de seguridad soportados, etc.
- Si la estación está usando un escaneado activo, en la búsqueda de una red para conectarse envía un `Probe Request` por cada canal con SSID=0.

Fase de autenticación: Authentication request/response

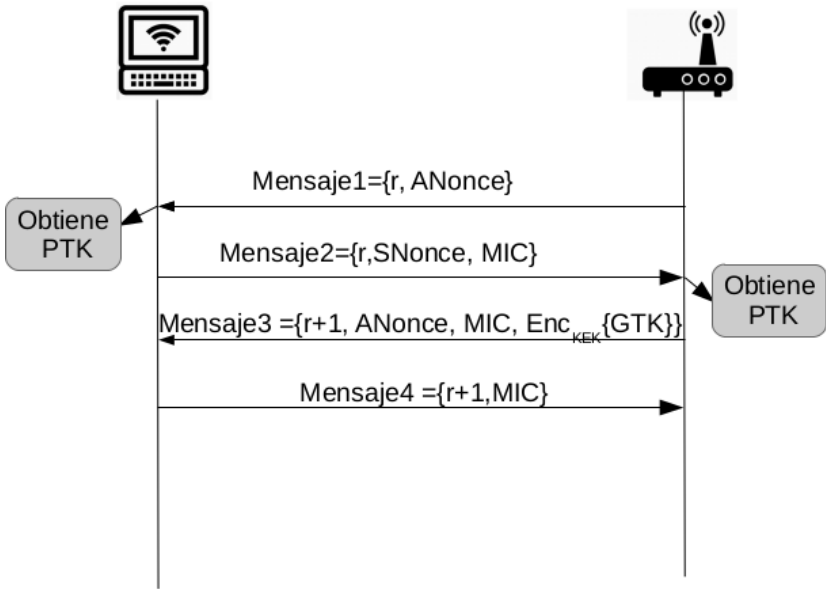
- No es una autenticación real ya que en este punto no se utilizan mecanismos de seguridad, que vendrán posteriormente.
- Se definen dos mecanismos:
  - Share Key Authentication: usa WEP (Wired Equivalent Privacy). Actualmente no debería usarse (está obsoleto por utilizar un cifrado muy débil).
  - Open Authentication: también llamado Null Authentication. La autenticación se realizará después.
    - WPA2-Personal: basado en una clave compartida (PSK, Pre-shared-Key). Se utiliza en redes domésticas.
    - WPA2-Enterprise: basado en un servidor que proporciona la autenticación del usuario. Se utiliza en redes de empresas.

Fase de asociación: Association request/response

- La estación envía `Association Request`, el AP responde con `Association Response`. El objetivo es obtener un identificador AID (Association IDentifier), un número único que el AP asigna a cada cliente.
- El mensaje `Association Request` lleva información sobre:
  - `listen interval`: Para cuando la estación entra en modo de ahorro de energía, este campo indica cada cuánto tiempo el dispositivo se activará para recibir tramas de baliza del AP, medido en períodos de envío de balizas
  - SSID
  - las velocidades básicas y extendidas (opcionales) soportadas por el dispositivo
  - algoritmos de seguridad soportados
  - ...
- El mensaje `Association Response` incluye el AID e información sobre las velocidades del AP. Para que una estación pueda asociarse a un AP, la estación debe soportar todas las velocidades básicas anunciadas por el AP.

WPA Personal: 4-way-handshake

- Basado en un secreto compartido: Pairwise Master Key (PMK).
- Verifica que ambos extremos conocen el secreto.
- Se calcula una clave compartida de sesión: Pairwise Transient Key (PTK) que es el resultado de hacer un conjunto de operaciones con:
  - PMK
  - ANonce y SNonce: números aleatorios generados por AP y por STA. Si las mismas entidades AP y STA se vuelven a comunicar generarán nuevos nonces y por tanto una nueva clave de sesión.
  - Direcciones MAC de AP y STA.
- La clave PTK es la concatenación de varias subclaves:
  - KCK (Key Confirmation Key): para integridad en los mensakes de 4-way handshake. Utilizada para calcular MIC (Message Integrity Check).
  - KEK (Key Encryption Key): para cifrar claves.
  - TK (Temporal Key): para cifrar datos.
- La clave GTK (Group Temporal Key): clave para mensajes de broadcast y multicast compartida por el AP y todos sus clientes.
- **Si se conoce el secreto compartido (PMK) y se capturan los mensajes de 4-way-handshake se puede derivar la clave de sesión y descifrar los datos.**



Contenidos

1 Introducción

2 Nivel Físico

3 Arquitectura Funcional y Topologías

4 Descubrimiento, autenticación y asociación

5 Nivel MAC

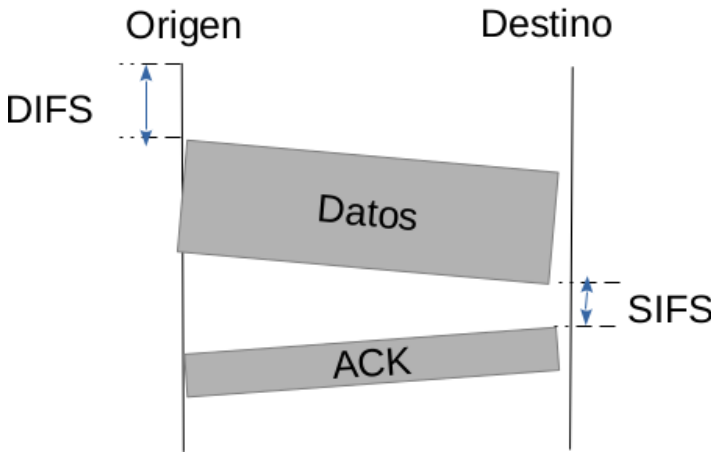
6 Trama 802.11

IEEE 802.11 Nivel MAC

- Los mecanismos de acceso al medio compartido permiten organizar el uso del canal. Se implementan dos funcionalidades:
  - Función de Coordinación Puntual (PCF, Puntual Coordination Function). Se usa para acceso determinista al canal a través de Round Robin. El AP controla qué estación puede transmitir en cada momento. Es una coordinación centralizada.
  - Función de Coordinación Distribuida (DCF, Distributed Coordination Function). Se usa para acceso por contienda implementado con CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance). Comunicación asíncrona entre estaciones.

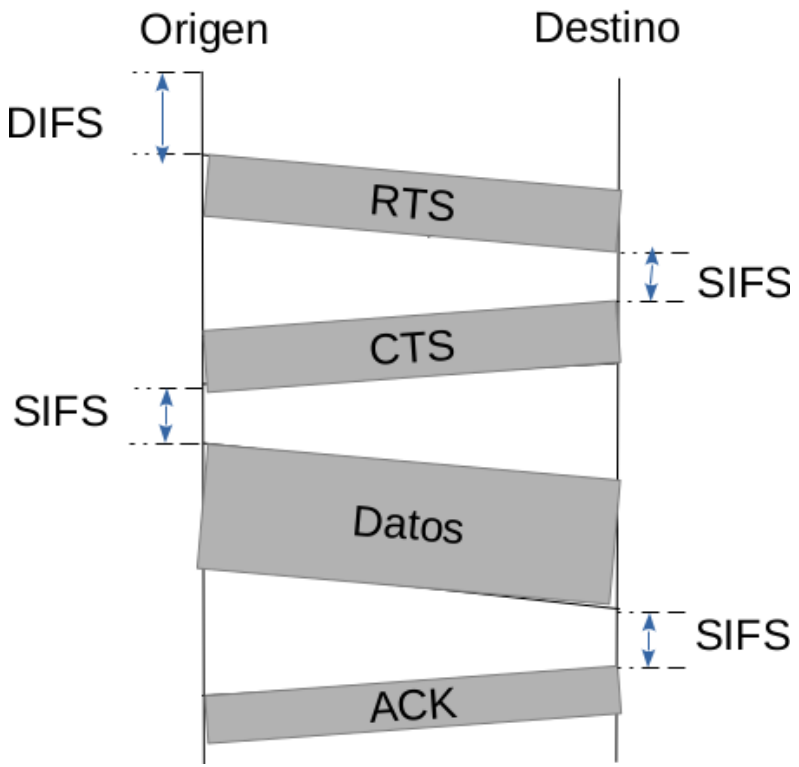
DCF, Distributed Coordination Function

- Si el origen quiere trasmitir y el medio está libre:
  - El origen espera DIFS (DCF Inter Frame Space, $\sim 50\mu s$).
  - El origen transmite los datos.
  - El receptor debe esperar SIFS (Short Inter Frame Space), $\sim 10\mu s$, antes de enviar el ACK, que es un mensaje de alta prioridad.
- Si el origen quiere trasmitir y el medio está ocupado:
  - El origen espera a que el canal esté libre.
  - El origen espera DIFS ($\sim 50\mu s$).
  - El origen espera un tiempo aleatorio adicional (ventana de contienda).
  - El origen comprueba si el canal está libre para empezar transmisión. Si no lo está vuelve al principio.
- Si una estación no recibe ACK, supone que ha habido colisión y reintenta el envío.



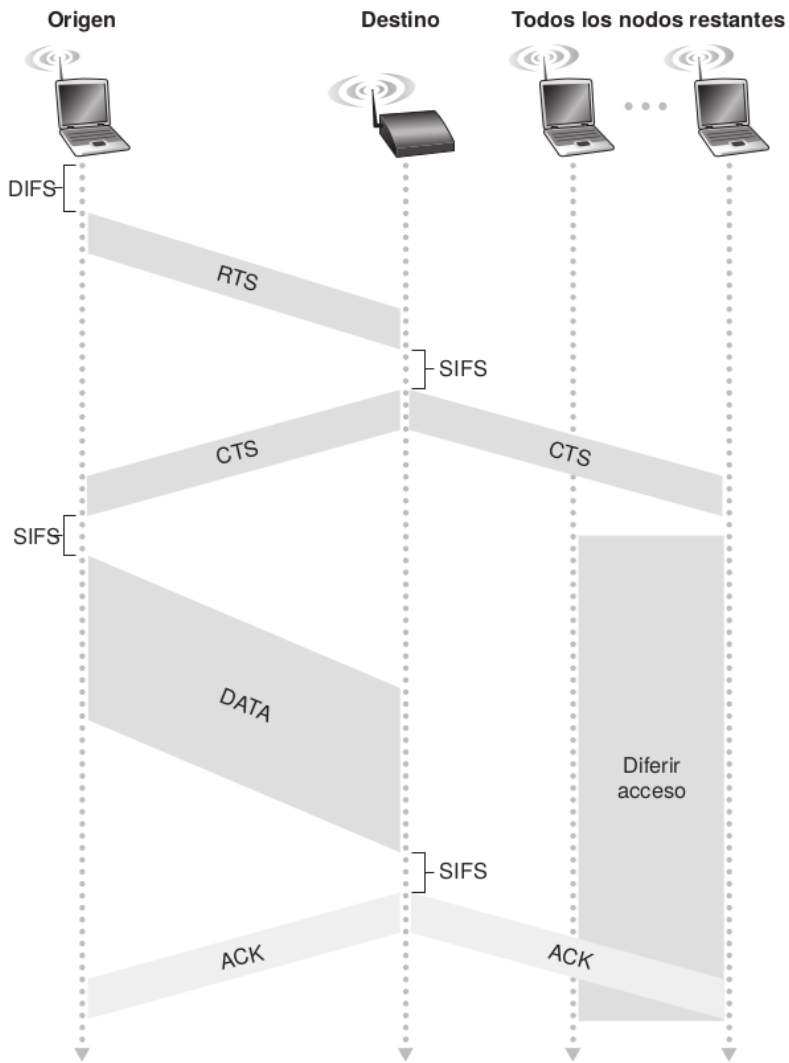
MACA: MultiAccess Collision Avoidance

- RTS/CTS complementa CSMA/CA.
- El emisor antes de enviar datos, manda una trama RTS (Request To Send) indicando la longitud de datos que quiere enviar.
  - Los RTS podrían colisionar, pero son tramas cortas. Se reintenta.
- El receptor responde con trama CTS (Clear To Send) y con el mismo valor de longitud de datos si el receptor está libre o con RxBUSY si el receptor está ocupado .
- El emisor puede enviar los datos.
- RTS/CTS es opcional, normalmente se activa sólo para tramas por encima de una determinada longitud.



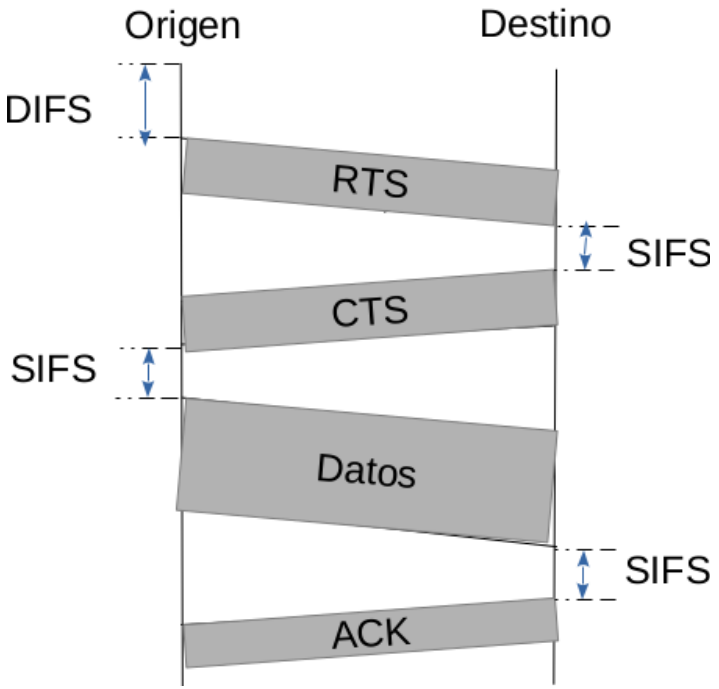
MACA y el problema del nodo oculto

- El origen envía trama RTS con la longitud de los datos que desea enviar.
- El destino responde con CTS para que el origen envíe su trama de esa longitud.
- Otros nodos restantes no tienen por qué recibir la trama RTS del origen pero sí reciben la trama CTS del destino con la longitud de los datos que desea enviar. Con esta información los otros nodos puede deducir cuanto tiempo estará ocupado el canal, ya que sabe la velocidad de transmisión y la cantidad de datos a enviar.
- El origen envía la trama con los datos.
- El destino envía ACK.



Network Allocation Vector (NAV)

- Las estaciones hacen una predicción de cuanto tiempo es necesario para completar la transmisión (hasta el envío del ACK incluido) y que el medio quede libre.
- Tanto RTS como CTS envían un campo `Duration/ID` con el tiempo que se necesita para que la transmisión termine (hasta que se complete con el ACK). Los datos también llevan su campo `Duration`. Por último el ACK lleva `Duration=0`.
- NAV siempre utilizará como duración un valor por encima de los que pueda estimar. Ejemplo (calcular de abajo hacia arriba):
  - RTS: `Duration`= 200 μs >= SIFS +`Duration (CTS)`
  - CTS: `Duration` = 150 μs >= SIFS + `Duration (Data)`
  - Data: `Duration` = 100 μs >= SIFS
  - ACK: `Duration` = 0 μs



Contenidos

1 Introducción

2 Nivel Físico

3 Arquitectura Funcional y Topologías

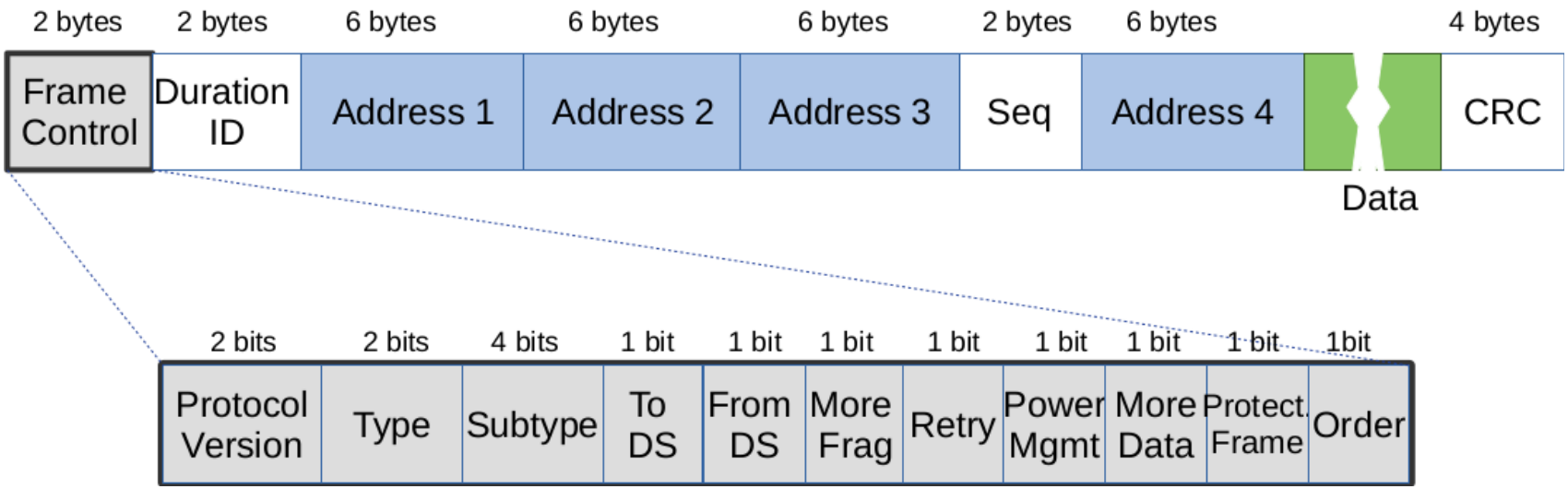
4 Descubrimiento, autenticación y asociación

5 Nivel MAC

6 Trama 802.11

Trama 802.11

- La trama 802.11 tiene los siguientes campos:

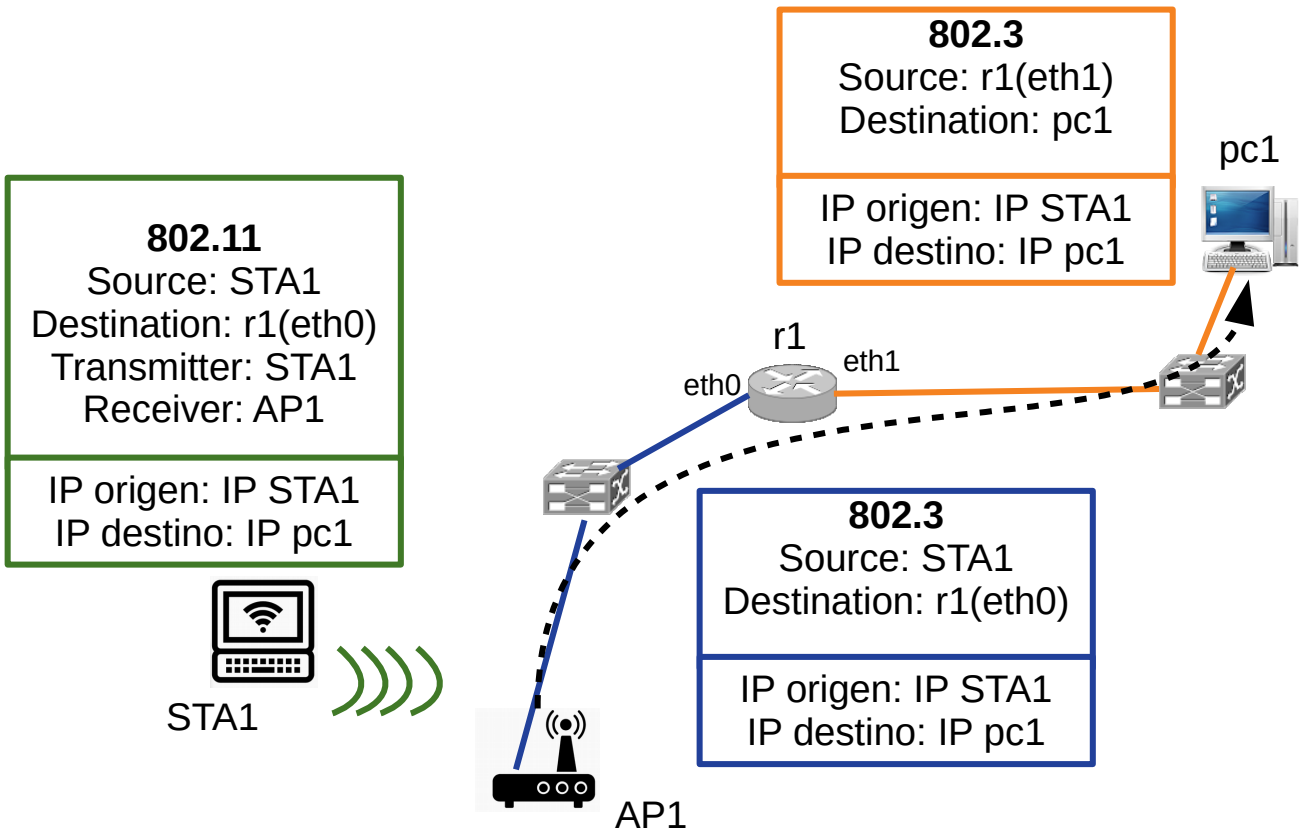


- **4 direcciones** MAC (6 bytes) que tienen diferente significado según sea el tipo de trama:
  - Dirección 1: receptor de la trama (`Receiver Address`, RA)
  - Dirección 2: transmisor de la trama (`Transmitter Address`, TA).
  - Dirección 3: diferente valor según el tipo de trama
  - Dirección 4: sólo se utiliza en algunos casos

Direcciones en Wireshark

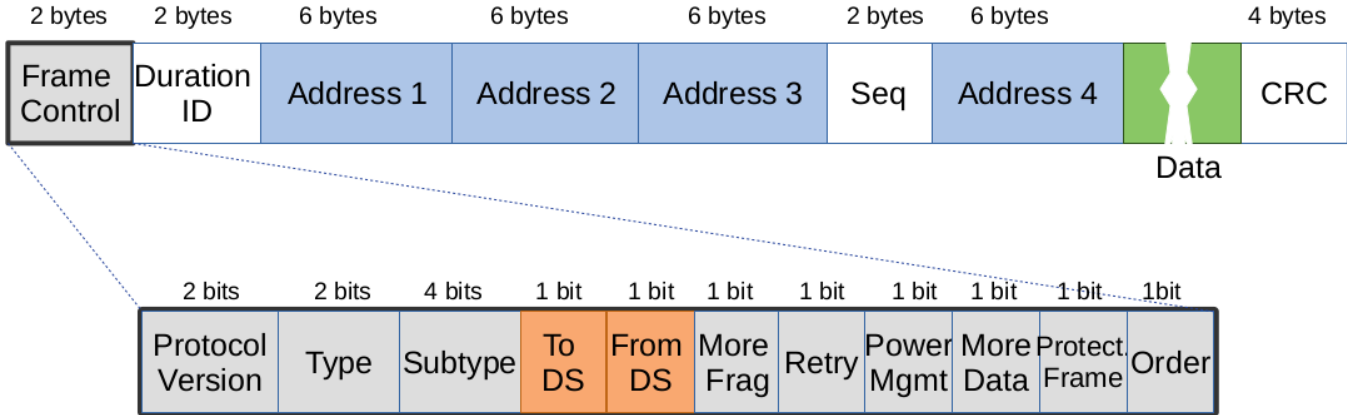
- Wireshark siempre señala en las tramas 802.11 los valores de 5 direcciones Ethernet por su significado, sin reflejar si posición en los 4 campos de la trama.
- Direcciones por su significado:
  - Source Address (SA): Origen de la trama: el que la crea originalmente
  - Destination Address (DA): Destino de la trama: al que va dirigida por el creador de la trama
  - Transmitter Address (TA): Transmisor de la trama: el que ha transmitido esta trama
  - Receiver Address (RA): Receptor de la trama: al que se la envía el transmisor
  - BSS Id: Dirección del AP (si lo hubiera), independientemente de si envía o recibe la trama
- En muchos casos algunas de las direcciones tienen el mismo valor, esta es la razón de que no siempre se usen las 4 direcciones del formato de la trama: sólo se usan las necesarias.

Comunicación STA1 → pc1



El campo To DS / From DS

- El campo `To DS` / `From DS` da significado a los campos de direcciones:



  - **To DS=0; From DS=0**
    Trama enviadas en modo ad-hoc. También en modo infraestructura para tramas de gestión y control donde los nodos que se comunican son directamente una estación y un AP.
  - **To DS=0; From DS=1**
    Trama que proviene de un DS, enviada por AP y destinada a una estación inalámbrica.
  - **To DS=1; From DS=0**
    Trama enviada por una estación inalámbrica a través de un AP y destinada a un DS.
  - **To DS=1; From DS=1**
    Trama que usa las 4 direcciones, por estar involucrados 2 APs. Se usa en redes mesh o con WDS o repetidores.

Las direcciones y el campo To DS / From DS

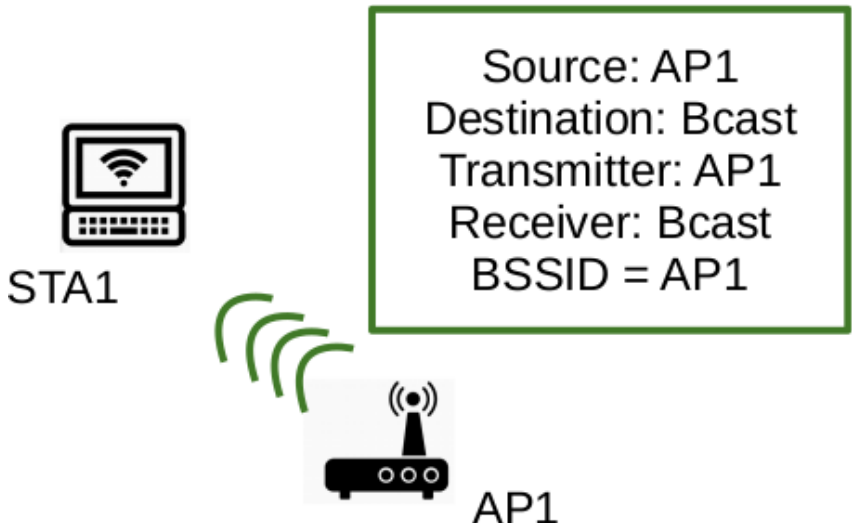
To DS	From DS	Dirección1	Dirección2	Dirección3	Dirección4
0	0	RA=DA	TA=SA	BSSID	
0	1	RA=DA	TA=BSSID	SA	
1	0	RA=BSSID	TA=SA	DA	
1	1	RA	TA	DA	SA

- RA: Receiver Address
- TA: Transmitter Address
- DA: Destination Address
- SA: Source Address
- BSSID: Basic Service Set ID = AP Address (dirección del AP), en redes ad-hoc se genera un BSSID aleatorio.

El número de direcciones utilizadas depende de la trama, la mayoría usa SA, DA y BSSID. Por eso están juntas las 3 primeras direcciones.

Ejemplo: trama beacon desde AP a todas las estaciones (I)

- To DS=0; From DS=0
- Dirección 1 = RA = DA = Broadcast
- Dirección 2 = TA = SA = Dirección del AP
- Dirección 3 = BSSID = Dirección del AP



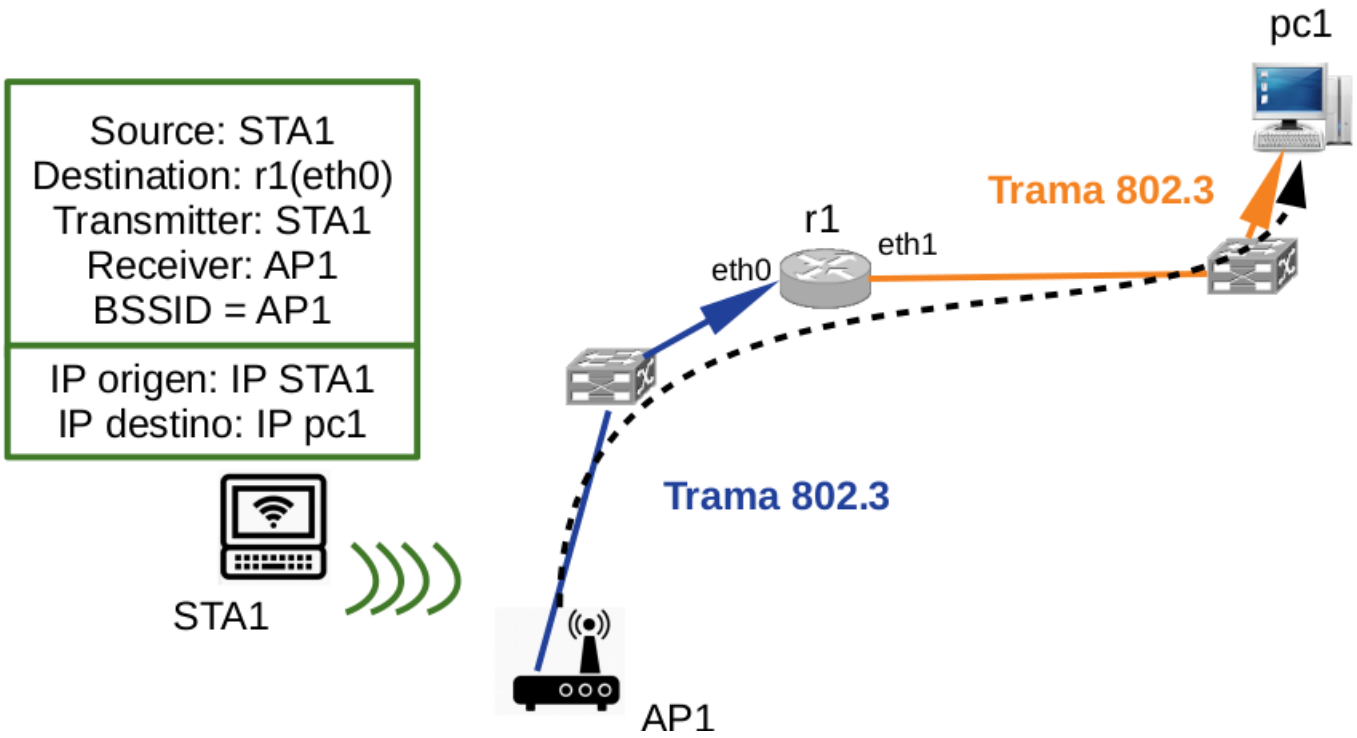
Ejemplo: trama beacon desde AP a todas las estaciones (II)

- To DS=0; From DS=0
- Dirección 1 = RA = DA = Broadcast
- Dirección 2 = TA = SA = Dirección del AP
- Dirección 3 = BSSID = Dirección del AP

```
IEEE 802.11 Beacon frame, Flags: ........C
  Type/Subtype: Beacon frame (0x0008)
▾ Frame Control Field: 0x8000
    .... ..00 = Version: 0
    .... 00.. = Type: Management frame (0)
    1000 .... = Subtype: 8
  ▾ Flags: 0x00
      .... ..00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x0)
      .... .0.. = More Fragments: This is the last fragment
      .... 0... = Retry: Frame is not being retransmitted
      ...0 .... = PWR MGT: STA will stay up
      ..0. .... = More Data: No data buffered
      .0.. .... = Protected flag: Data is not protected
      0... .... = Order flag: Not strictly ordered
  000 0000 0000 0000 = Duration: 0 microseconds
  Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
  Transmitter address: Objetivo_57:cc:97 (68:f9:56:57:cc:97)
  Source address: Objetivo_57:cc:97 (68:f9:56:57:cc:97)
  BSS Id: Objetivo_57:cc:97 (68:f9:56:57:cc:97)
  .... .... .... 0000 = Fragment number: 0
  0010 1010 0011 .... = Sequence number: 675
  Frame check sequence: 0xe51e563f [correct]
```

Ejemplo: trama de datos desde estación a DS (I)

- To DS=1; From DS=0
- Dirección 1 = RA = BSSID = Dirección del AP
- Dirección 2 = TA = SA = Dirección origen
- Dirección 3 = DA = Dirección del router



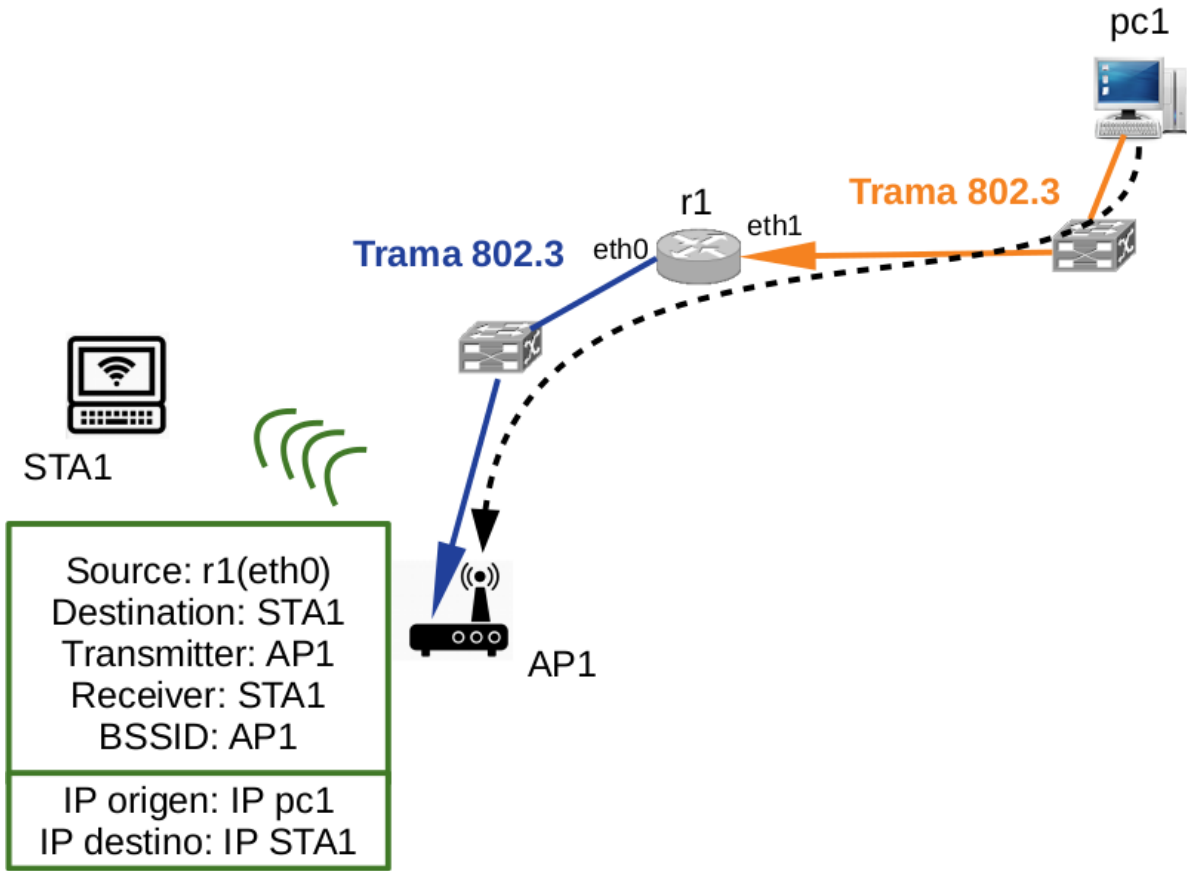
Ejemplo: trama de datos desde estación a DS (II)

- To DS=1; From DS=0
- Dirección 1 = RA = BSSID = Dirección del AP
- Dirección 2 = TA = SA = Dirección origen
- Dirección 3 = DA = Dirección del router

```
▾ IEEE 802.11 QoS Data, Flags: .p.....TC
    Type/Subtype: QoS Data (0x0028)
  ▾ Frame Control Field: 0x8841
      .... ..00 = Version: 0
      .... 10.. = Type: Data frame (2)
      1000 .... = Subtype: 8
    ▾ Flags: 0x41
        .... ..01 = DS status: Frame from STA to DS via an AP (To DS: 1 From DS: 0) (0x1)
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
        ...0 .... = PWR MGT: STA will stay up
        ..0. .... = More Data: No data buffered
        .1.. .... = Protected flag: Data is protected
        0... .... = Order flag: Not strictly ordered
    .000 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: Objetivo_57:cc:97 (68:f9:56:57:cc:97)
    Transmitter address: Azurewav_36:b8:00 (dc:f5:05:36:b8:00)
    Destination address: Objetivo_57:cc:96 (68:f9:56:57:cc:96)
    Source address: Azurewav_36:b8:00 (dc:f5:05:36:b8:00)
    BSS Id: Objetivo_57:cc:97 (68:f9:56:57:cc:97)
    STA address: Azurewav_36:b8:00 (dc:f5:05:36:b8:00)
    .... .... .... 0000 = Fragment number: 0
    1001 1011 0001 .... = Sequence number: 2481
```

Ejemplo: trama de datos desde DS a estación (I)

- To DS=0; From DS=1
- Dirección 1 = RA = DA = Dirección dispositivo Apple
- Dirección 2 = TA = BSSID = Dirección del AP
- Dirección 3 = SA = Dirección del router



Ejemplo de trama de datos desde DS a estación (II)

- To DS=0; From DS=1
- Dirección 1 = RA = DA = Dirección dispositivo Apple
- Dirección 2 = TA = BSSID = Dirección del AP
- Dirección 3 = SA = Dirección del router

```
IEEE 802.11 QoS Data, Flags: .p..R.F.C
  Type/Subtype: QoS Data (0x0028)
▾ Frame Control Field: 0x884a
    .... ..00 = Version: 0
    .... 10.. = Type: Data frame (2)
    1000 .... = Subtype: 8
  ▾ Flags: 0x4a
      .... ..10 = DS status: Frame from DS to a STA via AP(To DS: 0 From DS: 1) (0x2)
      .... .0.. = More Fragments: This is the last fragment
    ▾ .... 1... = Retry: Frame is being retransmitted
      ▸ [Expert Info (Note/Sequence): Retransmission (retry)]
      ...0 .... = PWR MGT: STA will stay up
      ..0. .... = More Data: No data buffered
      .1.. .... = Protected flag: Data is protected
      0... .... = Order flag: Not strictly ordered
  .000 0001 0000 0010 = Duration: 258 microseconds
  Receiver address: Apple_dd:b2:1f (fc:25:3f:dd:b2:1f)
  Transmitter address: Objetivo_57:cc:97 (68:f9:56:57:cc:97)
  Destination address: Apple_dd:b2:1f (fc:25:3f:dd:b2:1f)
  Source address: IntelCor_08:79:b0 (e4:70:b8:08:79:b0)
  BSS Id: Objetivo_57:cc:97 (68:f9:56:57:cc:97)
  STA address: Apple_dd:b2:1f (fc:25:3f:dd:b2:1f)
  .... .... .... 0000 = Fragment number: 0
  0001 1000 0111 .... = Sequence number: 391
```

Número de secuencia, duración y control de trama

- Cada vez que se recibe una trama con datos, se devuelve un ACK. Los ACK pueden perderse y la trama de datos se retransmite. El campo **Sequence number** sirve para distinguir si una trama de datos está duplicada.
- El valor del campo **Duration** almacena el tiempo que una estación tiene reservado el canal: envío de datos y su ACK. Se incluye en las tramas de datos, RTS y CTS.
- El campo de **Frame control** está dividido en subcampos, solo veremos algunos:
  - **Type y subtype** para distinguir tramas de asociación, RTS, CTS, ACK y datos.
  - **Flags To DS /From DS**: definen el sentido de la comunicación.
  - **Flag Retry** indica si es una retransmisión.
  - **Flag Protected** indica si se está utilizando cifrado.

Número de secuencia, duración y control de trama

```
▾ IEEE 802.11 Beacon frame, Flags: ........C
    Type/Subtype: Beacon frame (0x0008)
  ▾ Frame Control Field: 0x8000
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      1000 .... = Subtype: 8
    ▾ Flags: 0x00
        .... ..00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x0)
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
        ...0 .... = PWR MGT: STA will stay up
        ..0. .... = More Data: No data buffered
        .0.. .... = Protected flag: Data is not protected
        0... .... = Order flag: Not strictly ordered
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Transmitter address: Objetivo_57:cc:97 (68:f9:56:57:cc:97)
    Source address: Objetivo_57:cc:97 (68:f9:56:57:cc:97)
    BSS Id: Objetivo_57:cc:97 (68:f9:56:57:cc:97)
    .... .... .... 0000 = Fragment number: 0
    1110 0110 1010 .... = Sequence number: 3690
    Frame check sequence: 0x2cee6b59 [correct]
```

Tipos de tramas

- **Gestión**: `beacon` (baliza), `probe`, `authentication` y `association`.
- **Control**: Para facilitar el intercambio de datos: `RTS` (solicitud de envío), `CTS` (listo para envío), `ACK` (asentimiento de datos), `Block-ACK` (asentimiento de un conjunto de datos).
- **Datos**: `Data`, `QoS Data` (datos con calidad de servicio —vídeo o VoIP), `Null Data`.
  - La trama `Null Data` indica si una STA está activa (lleva power management bit=0). Si STA no está disponible (power management bit=1) y no puede recibir tramas, éstas deberán ser almacenadas en AP . Esta situación ocurre cuando la STA entra en modo de bajo consumo o cuando va a realizar roaming.

Trama Qos Data

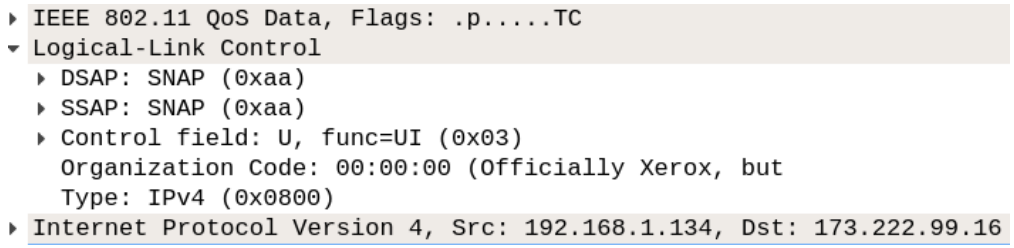
- Trama con un campo de control para calidad de servicio.
- Se han establecido 4 prioridades:
  - Background
  - Best Effort
  - Video
  - Audio

```
▾ IEEE 802.11 QoS Data, Flags: .p..R..TC
    Type/Subtype: QoS Data (0x0028)
  ▸ Frame Control Field: 0x8849
    .000 0000 0011 0000 = Duration: 48 microseconds
    Receiver address: Objetivo_57:cc:97 (68:f9:56:57:cc:97)
    Transmitter address: Apple_ac:8b:b1 (90:8d:6c:ac:8b:b1)
    Destination address: Objetivo_57:cc:96 (68:f9:56:57:cc:96)
    Source address: Apple_ac:8b:b1 (90:8d:6c:ac:8b:b1)
    BSS Id: Objetivo_57:cc:97 (68:f9:56:57:cc:97)
    STA address: Apple_ac:8b:b1 (90:8d:6c:ac:8b:b1)
    .... .... .... 0000 = Fragment number: 0
    0000 0000 1010 .... = Sequence number: 10
    Frame check sequence: 0xb0d4ccac [correct]
    [FCS Status: Good]
  ▾ Qos Control: 0x0001
      .... .... .... 0001 = TID: 1
      [.... .... .... .001 = Priority: Background (Background) (1)]
      .... .... ...0 .... = QoS bit 4: Bits 8-15 of QoS Control field are TXOP Duration Requested
      .... .... .00. .... = Ack Policy: Normal Ack (0x0)
      .... .... 0... .... = Payload Type: MSDU
      0000 0000 .... .... = TXOP Duration Requested: 0 (no TXOP requested)
```

LLC, Logical Link Control: IEEE 802.2

- Subnivel superior del nivel de enlace en redes de área local. Se encuentra por encima del subnivel MAC que depende de la tecnología de red usada: Ethernet, Token Ring, 802.11, etc.
- Es obligatorio usar LLC para todas las redes 802 salvo para Ethernet (802.3). Además hay una extensión a LLC que se llama Sub-Network Access Protocol (SNAP) que incluye los campos de la cabecera LLC y más.

- **Campos LLC:**
  - DSAP: Destination Service Access Point (1byte)
  - SSAP: Source Service Access Point (1 byte)
  - Control (1 ó 2 bytes)
- **Campos LLC+SNAP:**
  - DSAP: Destination Service Access Point (1byte)=0xaa
  - SSAP: Source Service Access Point (1 byte)=0xaa
  - Control (1 ó 2 bytes)
  - Organization Code (3 bytes)
  - EtherType (2 bytes)



Referencias

- Redes de computadoras, un enfoque descentente. Kurose, Ross. Pearson. Capítulo 7: Redes inalámbricas y móviles.
- 802.11 Wireless Networks: The Definitive Guide. Matthew S. Gast. O'Reilly. Capítulos 2,3 y 4.