## *Asociación*

**Cuestión 1.** Localiza las tramas Beacon:

Usando el filtro ***wlan.fc.type_subtype == 0x0008*** obtenemos todas las tramas Beacon.

a) ¿Cuántas APs están en la cobertura de la estación desde la que se realizó la captura?

Sabiendo que las tramas Beacon son enviadas por los APs, vemos que en la *Wireshark_802_11* hay 7 access points, y en la *Wireshark_802_11LOCAL* hay 34:

Wireshark: WLAN Traffic Statistics: Wireshark_802_11_LOCAL.pcap

Network Overview - Filter: wlan.fc.type_subtype == 0x0008

| BSSID | Ch. | SSID | % Packets | Beacons | Data Packets | Probe Req | Probe Resp | Auth | Deauth | Other | Protection |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Cisco_43:ba:c0 | 1 | pas | 1.24 % | 57 | 0 | 0 | 0 | 0 | 0 | 0 | |
| Cisco_1b:d5:00 | 1 | pas | 1.92 % | 88 | 0 | 0 | 0 | 0 | 0 | 0 | |
| Cisco_a9:50:a0 | 1 | pas | 4.16 % | 191 | 0 | 0 | 0 | 0 | 0 | 0 | |
| Cisco_9a:9d:50 | 1 | pas | 4.12 % | 189 | 0 | 0 | 0 | 0 | 0 | 0 | |
| Cisco_1b:d2:60 | 1 | pas | 3.77 % | 173 | 0 | 0 | 0 | 0 | 0 | 0 | |
| Cisco_9b:54:d0 | 1 | pas | 3.44 % | 158 | 0 | 0 | 0 | 0 | 0 | 0 | |
| Cisco_1b:d5:05 | 1 | pdi | 2.20 % | 101 | 0 | 0 | 0 | 0 | 0 | 0 | |
| Cisco_43:ba:c5 | 1 | pdi | 1.44 % | 66 | 0 | 0 | 0 | 0 | 0 | 0 | |
| Cisco_a9:50:a5 | 1 | pdi | 3.46 % | 159 | 0 | 0 | 0 | 0 | 0 | 0 | |
| Cisco_1b:d2:65 | 1 | pdi | 3.18 % | 146 | 0 | 0 | 0 | 0 | 0 | 0 | |
| Cisco_9b:54:d5 | 1 | pdi | 3.57 % | 164 | 0 | 0 | 0 | 0 | 0 | 0 | |
| Cisco_9a:9d:55 | 1 | pdi | 3.88 % | 178 | 0 | 0 | 0 | 0 | 0 | 0 | |

Selected Network

| Address | % Packets | Data Sent | Data Received | Probe Req | Probe Resp | Auth | Deauth | Other | Comment |
|---|---|---|---|---|---|---|---|---|---|
| Broadcast | 0.00 % | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| Cisco_9a:9d:55 | 0.00 % | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Base station |

*Imagen 1: Aps in* Wireshark_802_11LOCAL

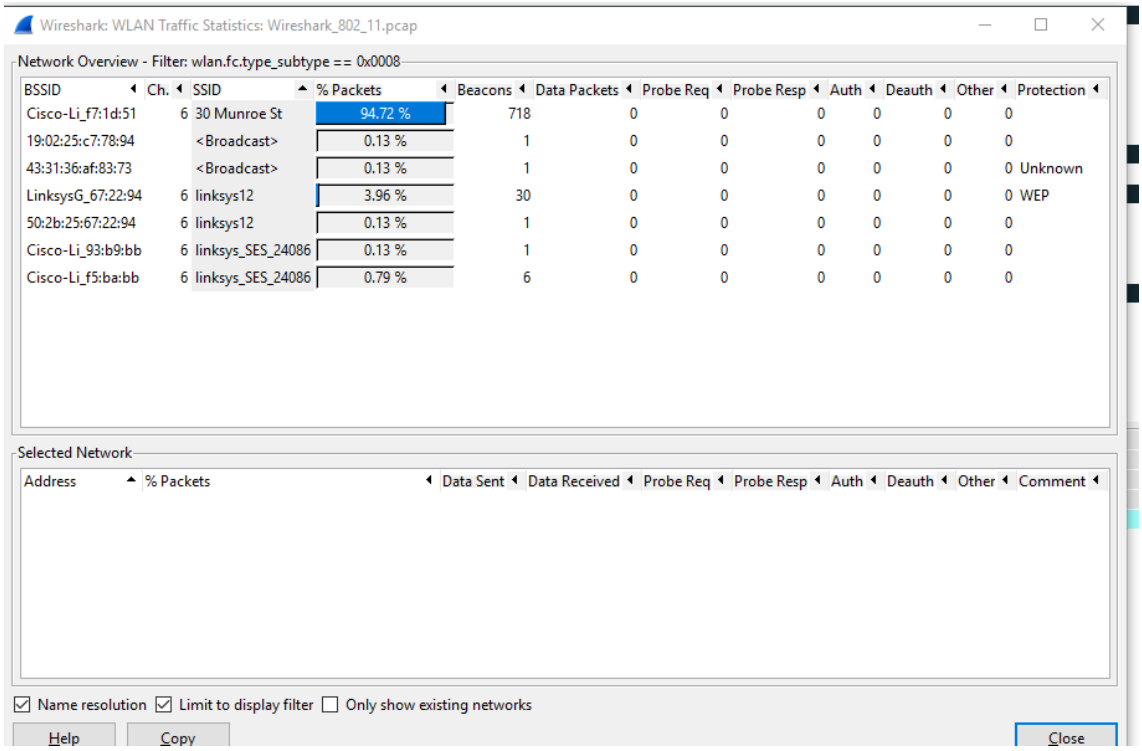
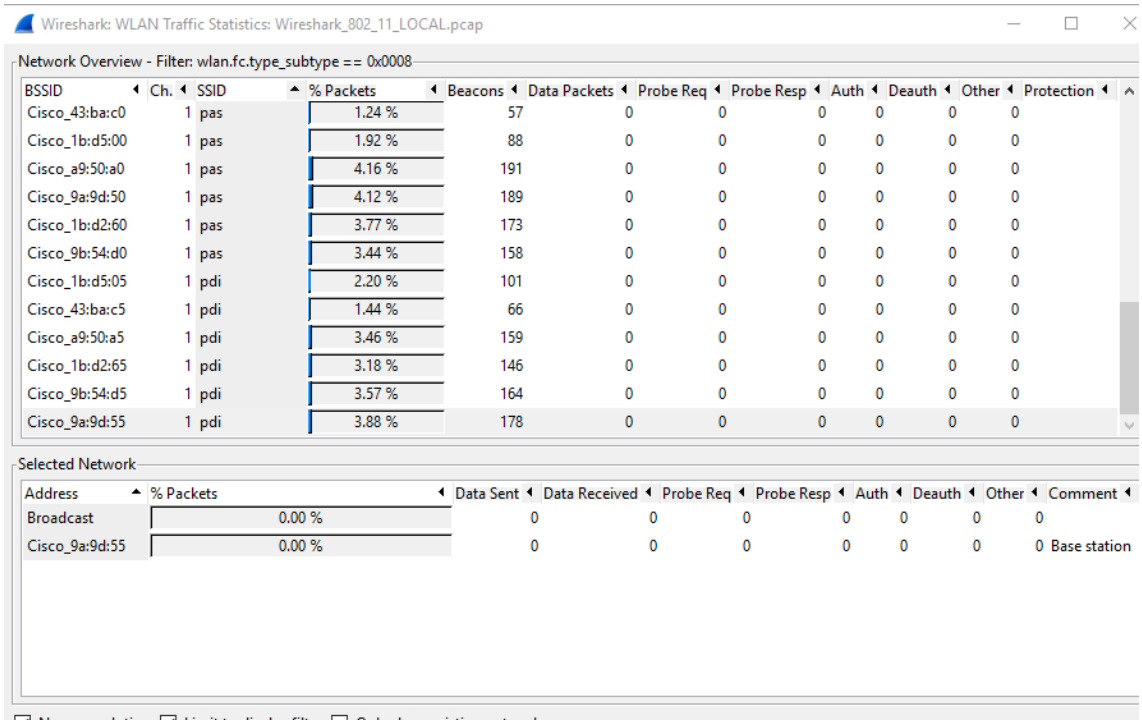


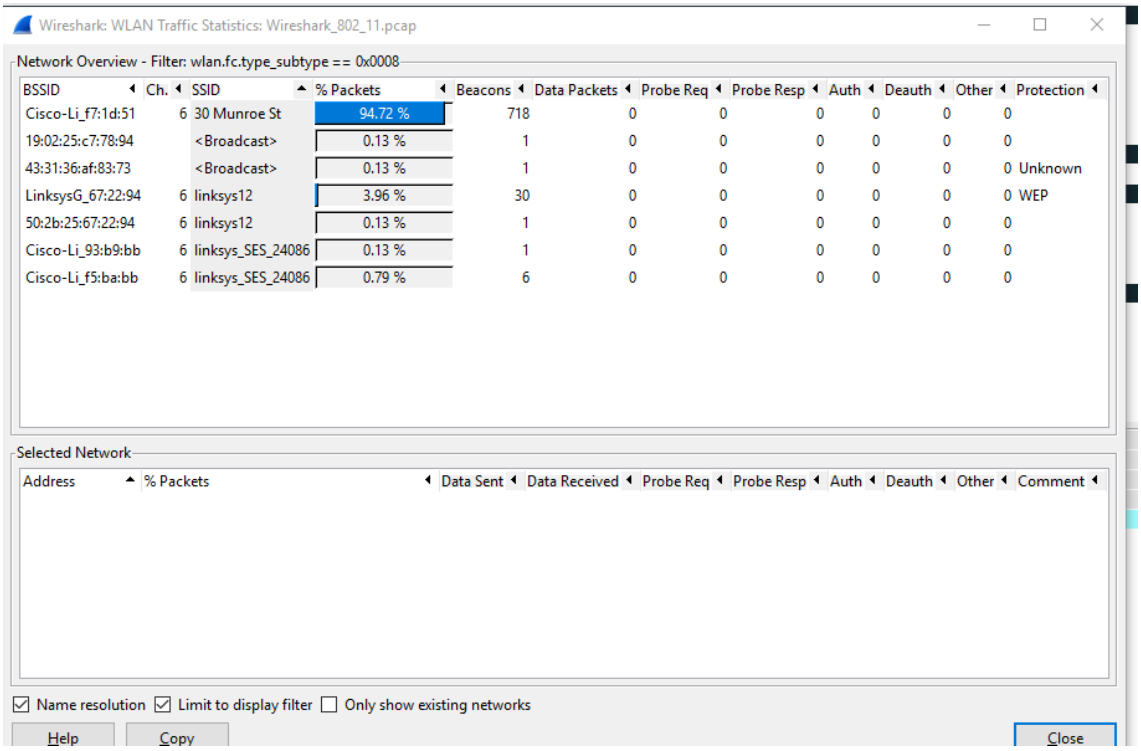

*Imagen 2: Aps in* Wireshark_802_11

b) ¿Cuáles son sus identificadores?

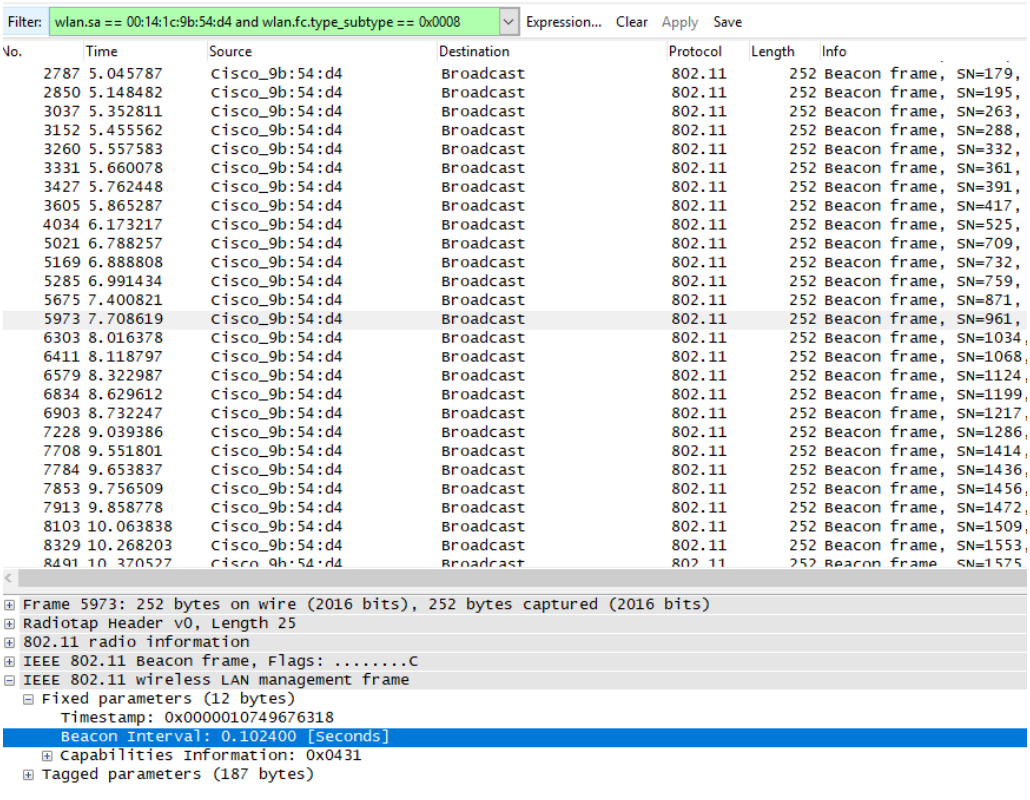
- En la captura LOCAL tenemos los SSIDs: Broadcast, ICB-Wifi, NEO, WifiUma, alumnos, eduroam, pas, pdi.



- En la otra captura tenemos las siguientes identificaciones: Broadcast, 30 Munroe St, lynksis12, lynksis_SES_24086.



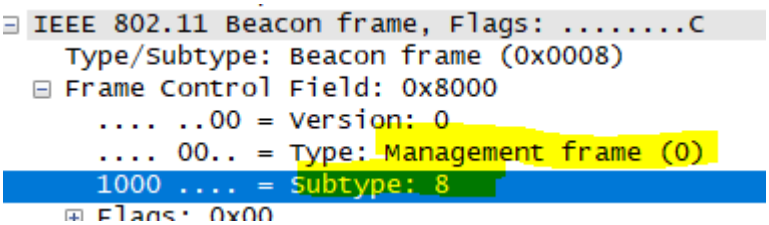

c) ¿Cada cuánto tiempo envían una trama de Beacon?



Si aplicamos un filtro para una source address específica, obtenemos que, de media, las tramas Beacon se envían con entre 0,102400s entre ellas (desde una misma fuente).

d) ¿Qué tipo de trama es?

Son tramas Beacon, es decir, tramas del tipo Management (type = 0, subtype = 8).




**Ejercicio 1.** Muestra la estructura y contenido de los campos de una trama Beacon (de ambos ficheros)

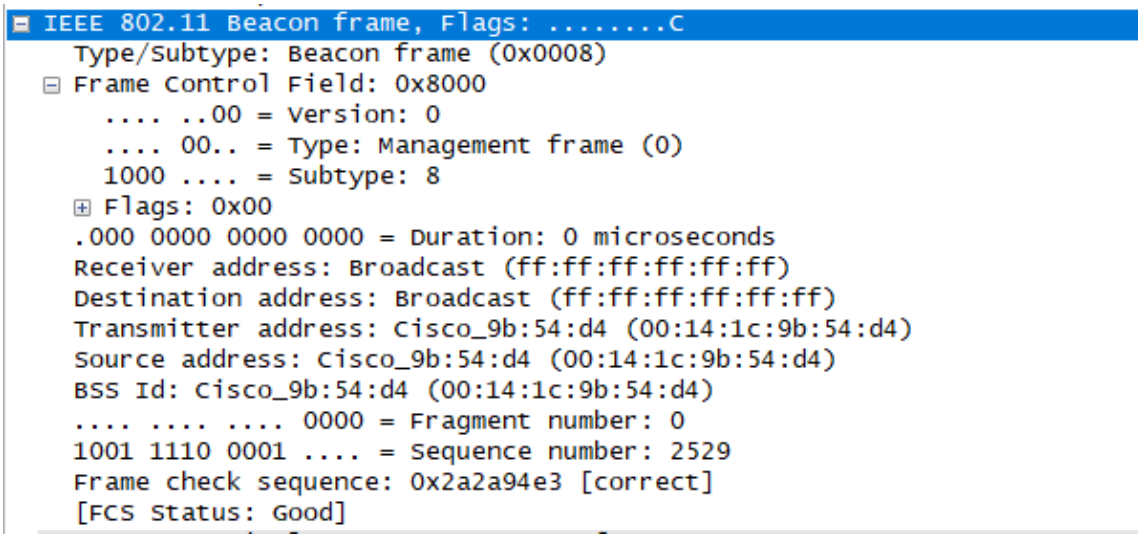



*Imagen 3: Ejemplo estructura trama Beacon (Wireshark_802_11_LOCAL)*

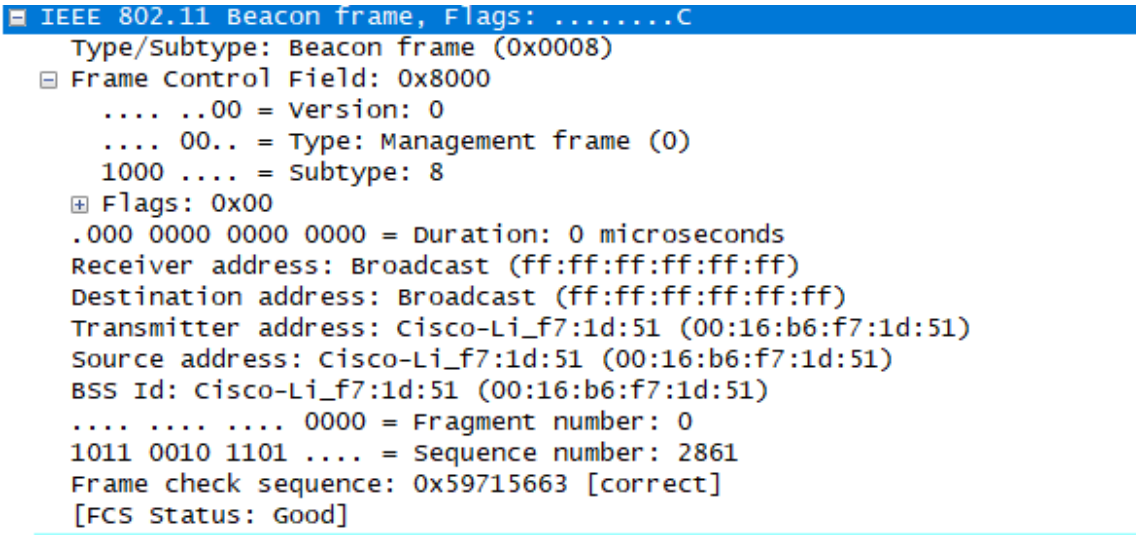



*Imagen 4: Ejemplo estructura trama Beacon (Wireshark_802_11)*

**Cuestión 2.** ¿En la captura, hay alguna estación que realice un escaneo activo? ¿Hay APs que respondan? ¿Qué tipos de tramas son? (Consulta e indica el valor de campo tipo)

a) Sí: en la captura *Wireshark_802_11* las estaciones Intelcor_1f:57:13 e Intelcor_d1:b6:4f; y en la versión *LOCAL*, Apple_3a:5d:96 y la HonHairPr_7e:b7:25 entre otras.

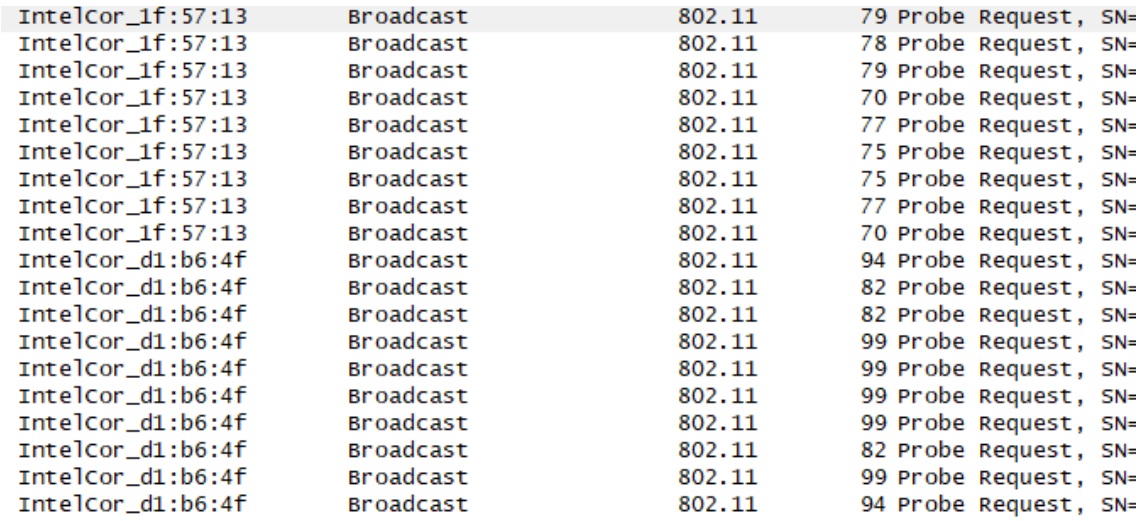



*Imagen 5: Probe Requests en Wireshark_802_11.*

| | | | |
|---|---|---|---|
| Apple_3a:5d:96 | Broadcast | 802.11 | 92 Probe Request, SN |
| HonHaiPr_7e:b7:25 | Broadcast | 802.11 | 71 Probe Request, SN |
| MurataMa_56:bf:1e | Broadcast | 802.11 | 294 Probe Request, SN |
| HewlettP_54:cb:7c | Broadcast | 802.11 | 90 Probe Request, SN |
| HewlettP_54:cb:7c | Broadcast | 802.11 | 90 Probe Request, SN |
| HewlettP_54:cb:7c | Broadcast | 802.11 | 90 Probe Request, SN |
| HewlettP_d1:04:03 | Broadcast | 802.11 | 82 Probe Request, SN |
| Htc_83:a1:a7 | Broadcast | 802.11 | 99 Probe Request, SN |
| SamsungE_c3:c4:19 | Broadcast | 802.11 | 293 Probe Request, SN |
| SamsungE_c3:c4:19 | Broadcast | 802.11 | 293 Probe Request, SN |
| HewlettP_54:cb:7c | Broadcast | 802.11 | 90 Probe Request, SN |
| HewlettP_54:cb:7c | Broadcast | 802.11 | 90 Probe Request, SN |
| AsustekC_56:d3:99 | Broadcast | 802.11 | 145 Probe Request, SN |
| AsustekC_56:d3:99 | Broadcast | 802.11 | 145 Probe Request, SN |

*Imagen 6: Probe Requests en Wireshark_802_11_LOCAL.*

b) Sí.

Filter: wlan.fc.type_subtype == 0x05 Expression... Clear Apply Save

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 528 | 1.995322 | Cisco_1b:d5:02 | Htc_16:be:22 | 802.11 | 246 | Probe Response, S |
| 4900 | 6.712736 | Cisco_1b:d5:01 | HonHaiPr_c2:e3:2b | 802.11 | 246 | Probe Response, S |
| 4903 | 6.714411 | Cisco_1b:d5:02 | HonHaiPr_c2:e3:2b | 802.11 | 246 | Probe Response, S |
| 4906 | 6.715754 | Cisco_1b:d5:04 | HonHaiPr_c2:e3:2b | 802.11 | 246 | Probe Response, S |
| 5188 | 6.906983 | Cisco-Li_a6:53:7c | HonHaiPr_7e:b7:25 | 802.11 | 239 | Probe Response, S |
| 5190 | 6.919555 | Cisco_a9:50:a1 | HonHaiPr_7e:b7:25 | 802.11 | 246 | Probe Response, S |
| 5191 | 6.920222 | Cisco_43:ba:c5 | HonHaiPr_7e:b7:25 | 802.11 | 242 | Probe Response, S |
| 5193 | 6.920808 | Cisco_9a:9d:50 | HonHaiPr_7e:b7:25 | 802.11 | 242 | Probe Response, S |
| 5194 | 6.921403 | Cisco_a9:50:a1 | HonHaiPr_7e:b7:25 | 802.11 | 246 | Probe Response, S |
| 5195 | 6.922036 | Cisco_9a:9d:50 | HonHaiPr_7e:b7:25 | 802.11 | 242 | Probe Response, S |
| 5196 | 6.922638 | Cisco_a9:50:a2 | HonHaiPr_7e:b7:25 | 802.11 | 246 | Probe Response, S |
| 5197 | 6.923288 | Cisco_a9:50:a2 | HonHaiPr_7e:b7:25 | 802.11 | 246 | Probe Response, S |
| 5199 | 6.924505 | Cisco_a9:50:a4 | HonHaiPr_7e:b7:25 | 802.11 | 246 | Probe Response, S |
| 5202 | 6.925694 | Cisco_a9:50:a4 | HonHaiPr_7e:b7:25 | 802.11 | 246 | Probe Response, S |
| 5203 | 6.926903 | Cisco_9a:9d:51 | HonHaiPr_7e:b7:25 | 802.11 | 246 | Probe Response, S |

*Imagen 7: Probe Responses en LOCAL.*

Filter: wlan.fc.type_subtype == 0x05 Expression... Clear Apply Save

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 27 | 1.212185 | Cisco-Li_f7:1d:51 | IntelCor_d1:b6:4f | 802.11 | 177 | Probe Response, SN=2867, Fl |
| 51 | 2.300697 | Cisco-Li_f7:1d:51 | IntelCor_1f:57:13 | 802.11 | 177 | Probe Response, SN=2878, Fl |
| 52 | 2.302191 | Cisco-Li_f7:1d:51 | IntelCor_1f:57:13 | 802.11 | 177 | Probe Response, SN=2878, Fl |
| 53 | 2.304063 | Cisco-Li_f7:1d:51 | IntelCor_1f:57:13 | 802.11 | 177 | Probe Response, SN=2878, Fl |
| 54 | 2.305562 | Cisco-Li_f7:1d:51 | IntelCor_1f:57:13 | 802.11 | 177 | Probe Response, SN=2878, Fl |
| 55 | 2.308563 | Cisco-Li_f7:1d:51 | IntelCor_1f:57:13 | 802.11 | 177 | Probe Response, SN=2878, Fl |
| 56 | 2.310072 | Cisco-Li_f7:1d:51 | IntelCor_1f:57:13 | 802.11 | 177 | Probe Response, SN=2878, Fl |
| 59 | 2.453941 | Cisco-Li_f7:1d:51 | IntelCor_1f:57:13 | 802.11 | 177 | Probe Response, SN=2881, Fl |
| 83 | 4.283835 | Cisco-Li_f7:1d:51 | IntelCor_d1:b6:4f | 802.11 | 177 | Probe Response, SN=2900, Fl |
| 88 | 4.301564 | Cisco-Li_f7:1d:51 | IntelCor_1f:57:13 | 802.11 | 177 | Probe Response, SN=2901, Fl |
| 89 | 4.303314 | Cisco-Li_f7:1d:51 | IntelCor_1f:57:13 | 802.11 | 177 | Probe Response, SN=2901, Fl |
| 90 | 4.304814 | Cisco-Li_f7:1d:51 | IntelCor_1f:57:13 | 802.11 | 177 | Probe Response, SN=2901, Fl |
| 93 | 4.403454 | Cisco-Li_f7:1d:51 | IntelCor_1f:57:13 | 802.11 | 177 | Probe Response, SN=2903, Fl |
| 94 | 4.404939 | Cisco-Li_f7:1d:51 | IntelCor_1f:57:13 | 802.11 | 177 | Probe Response, SN=2903, Fl |
| 119 | 6.303313 | Cisco-Li_f7:1d:51 | IntelCor_1f:57:13 | 802.11 | 177 | Probe Response, SN=2922, Fl |
| 130 | 6.404446 | Cisco-Li_f7:1d:51 | IntelCor_1f:57:13 | 802.11 | 177 | Probe Response, SN=2924, Fl |
| 131 | 6.405938 | Cisco-Li_f7:1d:51 | IntelCor_1f:57:13 | 802.11 | 177 | Probe Response, SN=2924, Fl |
| 132 | 6.407562 | Cisco-Li_f7:1d:51 | IntelCor_1f:57:13 | 802.11 | 177 | Probe Response, SN=2924, Fl |
| 133 | 6.409063 | Cisco-Li_f7:1d:51 | IntelCor_1f:57:13 | 802.11 | 177 | Probe Response, SN=2924, Fl |
| 134 | 6.410562 | Cisco-Li_f7:1d:51 | IntelCor_1f:57:13 | 802.11 | 177 | Probe Response, SN=2924, Fl |

*Imagen 8: Probe Responses en Wireshark_802_11.*

c) Son tramas del tipo Probe Request (subtipo 4, enviadas por las estaciones en un escaneo activo) y del tipo Probe Response (subtipo 5, enviadas por los APs en respuesta a las Requests). Ambas son del tipo 0 (management).

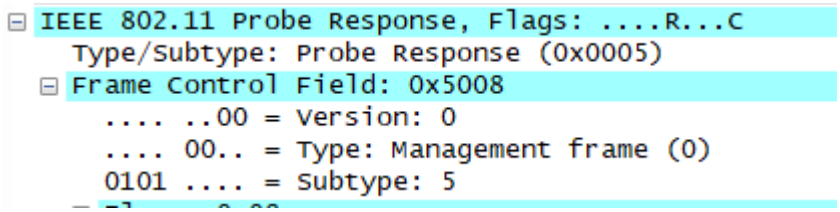



*Imagen 9: Probe Response*

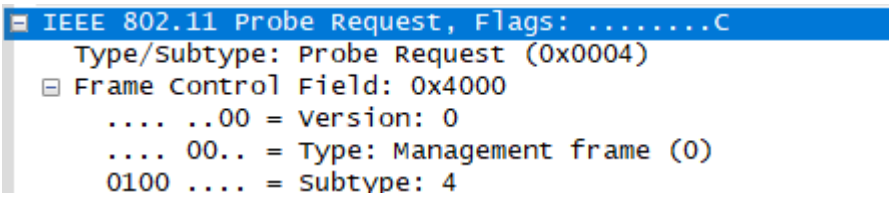



*Imagen 10: Probe Request*

**Ejercicio 2.** Localiza en la captura alguna trama de petición activo y la respuesta correspondiente. Muestra la estructura y contenido de ambas tramas.

En la captura *Wireshark_802_11* encontramos una request y una response entre un AP y una estación:

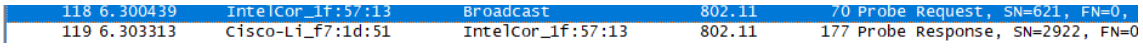



*Imagen 11: Interacción entre AP y estación base.*

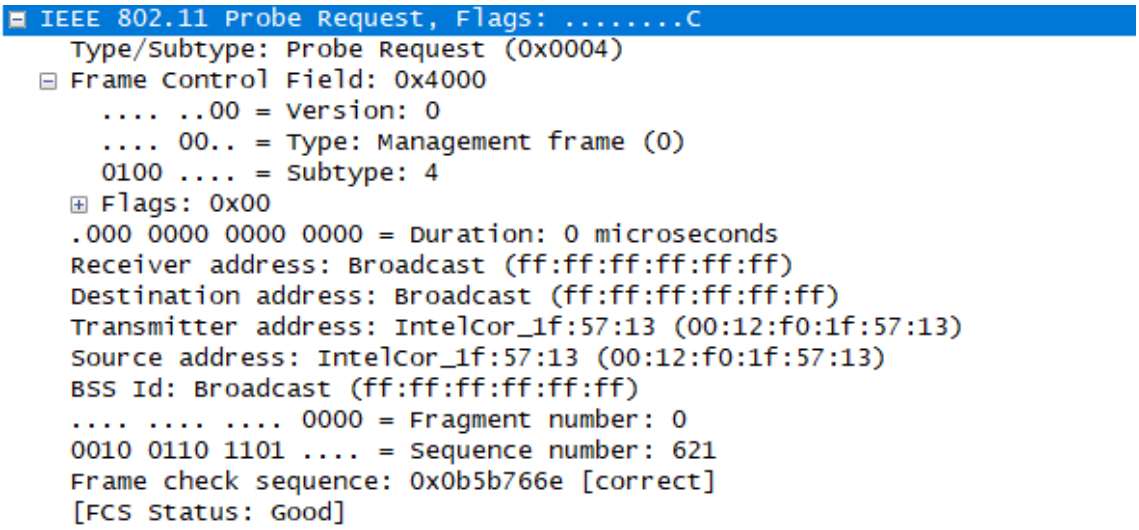



*Imagen 12: Probe request de la trama nº 118.*

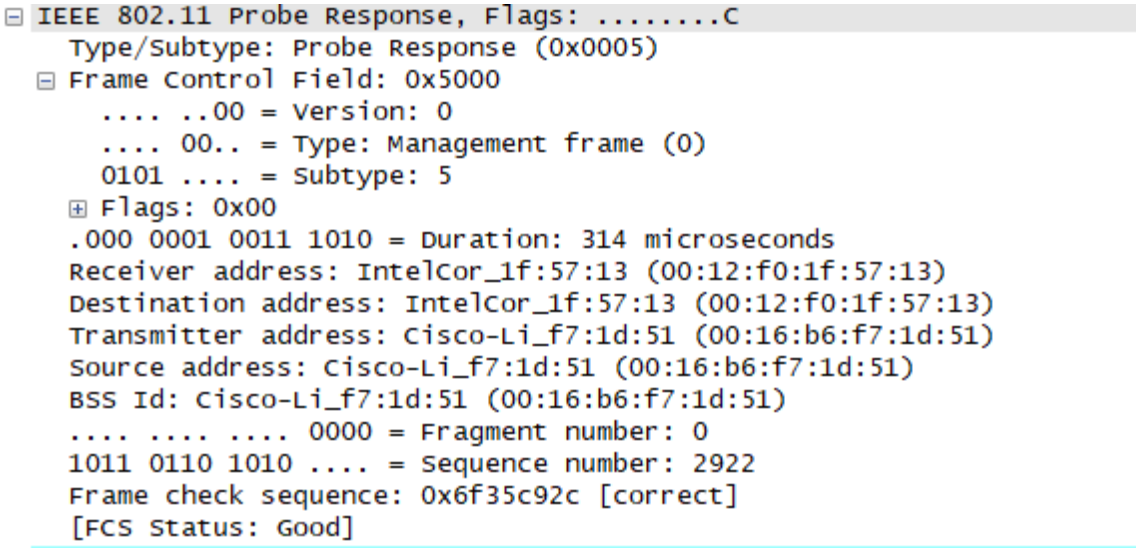



*Imagen 13: Probe response de la trama nº 119*

**Cuestión 3.** Localiza en la captura alguna petición de asociación. ¿Qué información incluye? Localiza en la captura alguna respuesta de asociación ¿Qué información incluye? ¿Qué tipos de tramas con? (valor de campo tipo)

Vamos a analizar la captura *Wireshark_802_11*:

a) Usando el filtro "*wlan.fc.type_subtype == 0x00*" obtenemos todas las tramas *Association Request:*

```
IEEE 802.11 Association Request, Flags: ........C
  Type/Subtype: Association Request (0x0000)
  Frame Control Field: 0x0000
    .... ..00 = Version: 0
    .... 00.. = Type: Management frame (0)
    0000 .... = Subtype: 0
    Flags: 0x00
  .000 0001 0011 1010 = Duration: 314 microseconds
  Receiver address: Cisco-Li_f5:ba:bb (00:18:39:f5:ba:bb)
  Destination address: Cisco-Li_f5:ba:bb (00:18:39:f5:ba:bb)
  Transmitter address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
  Source address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
  BSS Id: Cisco-Li_f5:ba:bb (00:18:39:f5:ba:bb)
  .... .... .... 0000 = Fragment number: 0
  0110 0100 0111 .... = Sequence number: 1607
  Frame check sequence: 0x4432d6cf [correct]
  [FCS Status: Good]
```

*Imagen 14: Ejemplo estructura de un Association Request*

Podemos observar que contiene los datos del destinatario deseado y del emisor, aparte de su tipo (0, management) y subtipo (0, Association Request).

b) Utilizando el filtro "*wlan.fc.type_subtype == 0x01*" obtenemos todas las tramas Association Response:

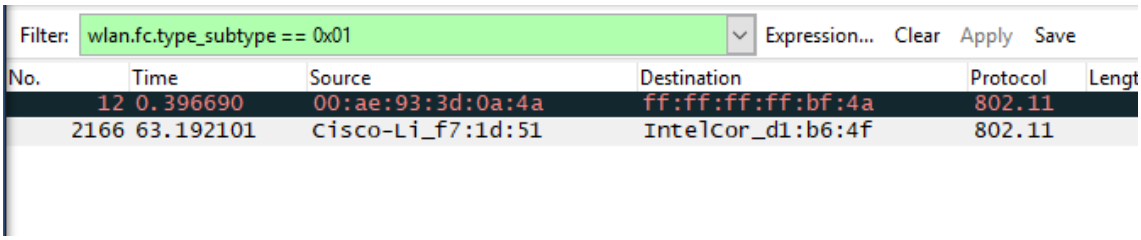



*Imagen 15: Association Responses en la captura analizada.*

Tenemos que uno de ellos muestra errores, mientras que el otro contiene la siguiente estructura:

```
IEEE 802.11 Association Response, Flags: ........C
  Type/Subtype: Association Response (0x0001)
  Frame Control Field: 0x1000
    .... ..00 = Version: 0
    .... 00.. = Type: Management frame (0)
    0001 .... = Subtype: 1
    Flags: 0x00
  .000 0001 0011 1010 = Duration: 314 microseconds
  Receiver address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
  Destination address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
  Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
  Source address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
  BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
  .... .... .... 0000 = Fragment number: 0
  1110 1001 0000 .... = Sequence number: 3728
  Frame check sequence: 0x37f2ab2b [correct]
  [FCS Status: Good]
```

*Imagen 16: Estructura trama Association Response en captura analizada.*

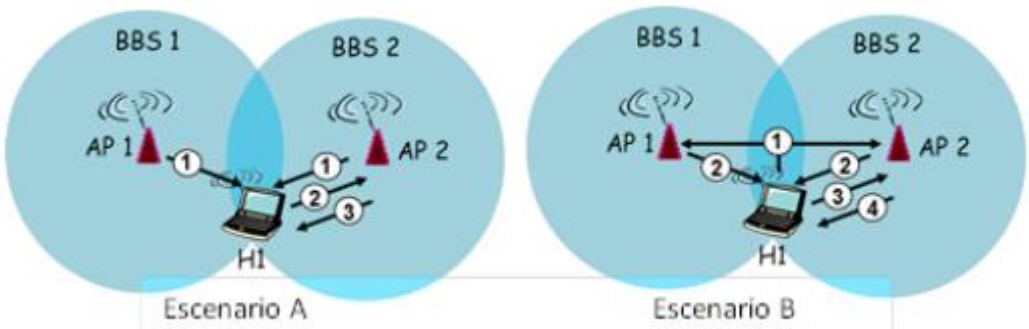
Vemos como el AP le responde a la petición de asociación anterior. La trama contiene la misma estructura que la Association Request.

c) Ambas son tramas del tipo management (tipo 0) y subtipo 0 (request) 1 (response).

**Ejercicio 3.** Localiza en la captura alguna trama de petición de asociación y la respuesta correspondiente. Muestra la estructura y contenido de ambas tramas.

**Realizado en la cuestión 3**

**Cuestión 4.** ¿Cuál de estos dos escenarios correspondería con un escaneado pasivo y con uno activo? ¿Por qué?



El escenario B sería el que representa la búsqueda activa, porque es la estación H1 la que inicia el escaneado, enviando un Probe Request a AP1 y AP2. En cambio, en el escenario A, tanto el Ap1 como el Ap2 envían tramas Beacon a H1, por lo que H1 estaría esperando a recibirla. A partir de ahí, observamos que H1 se comunica con P2 en ambos casos.

## *Transmisión de Datos*

**Cuestión 5.** ¿Cuántas tramas de datos diferentes observas en la captura? ¿Qué estaciones participan de esta comunicación? ¿Hay comunicación directa entre estaciones o siempre interviene un punto de acceso?

Usando el filtro "*wlan.fc.type==2*", enseñamos por pantalla todos los frames de tipo Data, que en este caso son: TCP, GET, SYN, ACK, PSH, OK, QoS Null function, Out of Order y FIN.

**Ejercicio 5.** Localiza en la captura alguna trama de datos NULL Muestra la estructura y contenido de esta trama. ¿Qué la diferencia de las tramas de datos normales? ¿Para qué sirve?

En la captura "*Wireshark_802_11*" encontramos varias tramas de datos NULL, por ejemplo, la siguiente:

```
> Frame 158: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
v IEEE 802.11 QoS Null function (No data), Flags: ...P...TC
    Type/Subtype: QoS Null function (No data) (0x002c)
  v Frame Control Field: 0xc811
      .... ..00 = Version: 0
      .... 10.. = Type: Data frame (2)
      1100 .... = Subtype: 12
    v Flags: 0x11
        .... ..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
        ...1 .... = PWR MGT: STA will go to sleep
        ..0. .... = More Data: No data buffered
        .0.. .... = Protected flag: Data is not protected
        0... .... = Order flag: Not strictly ordered
    .000 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Destination address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Transmitter address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    Source address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    STA address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    .... .... .... 0000 = Fragment number: 0
    0101 1101 1001 .... = Sequence number: 1497
    Frame check sequence: 0xd7131018 [correct]
    [FCS Status: Good]
  > Qos Control: 0x0000
```

*Imagen 17: En este caso, la STA que mandó el frame 158 va a pasar a estar offline.*

Este tipo de frames solo lo envían las STAs y no los APs, y su importancia yace en transportar el bit de *power management*, que será, o bien 0 ó 1. Esto quiere decir: si la estación manda un Null Data frame con el bit de PWR MGT a 0, está indicando al AP al que se lo envía que esta online, y listo para recibir información; en cambio, si estuviera a 1, estaría indicando que va a pasar a estar offline, y así los APs sabrían que no deberían enviarle información.

## *Direccionamiento*

**Cuestión 6.** Encuentra la trama que contenga el segmento TCP SYN de la primera sesión TCP (que descarga alice.txt). Muestra su contenido.

a) ¿Cuáles son las tres direcciones MAC de esta trama? ¿Cuál es la dirección MAC correspondiente al host inalámbrico desde el que se hace la petición? (representación hexadecimal) ¿Cuál la del punto de acceso? ¿y la del (primer) router?

Esta trama es la número 474, enviada en el tiempo t=24.811093s

i. Las direcciones MAC se muestran señaladas en la siguiente imagen:

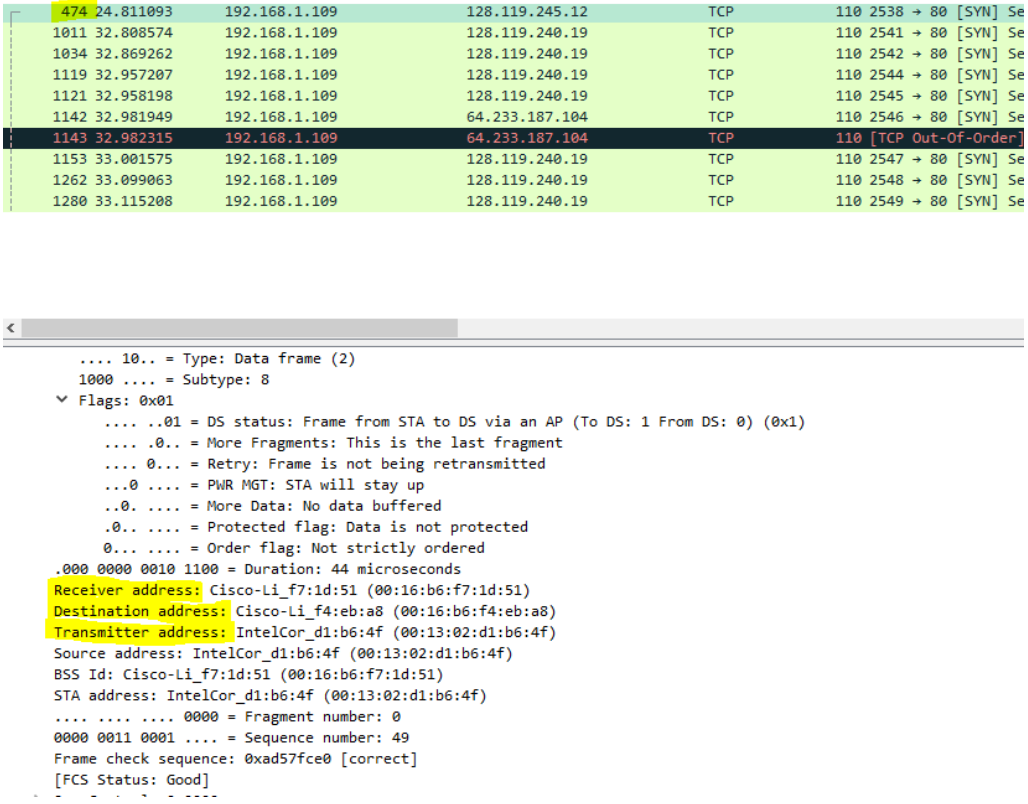



*Imagen 18: Trama 474, receiver address, destination address y trasnmitter address.*

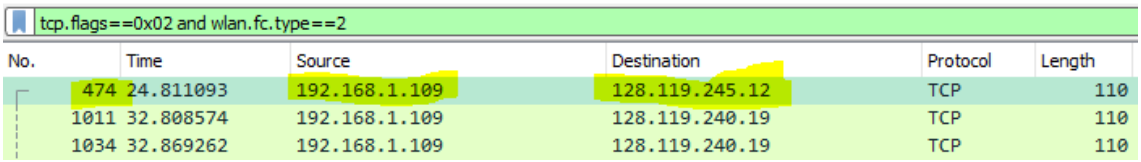
ii. Correspondería a la Souce address, que en este caso coincide con la Transmitter address: IntelCor_d1: b6:4f (00:13:02:d1:b6:4f)

iii. Destination address: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)

iv. La Receiver address: Cisco-Li_f7:1d:51

b) ¿Cuáles es la dirección IP del host inalámbrico que envía este segmento? ¿y la dirección IP destino? ¿con que se corresponde esta dirección IP destino? (host, punto de acceso, router, o cualquier otro dispositivo de la red). Razona tu respuesta.

i. Recordamos que nos encontramos en el frame #474. La IP desde la que se envía esta trama TCP es 192.168.1.109, y la IP de destino es 128.119.245.12.

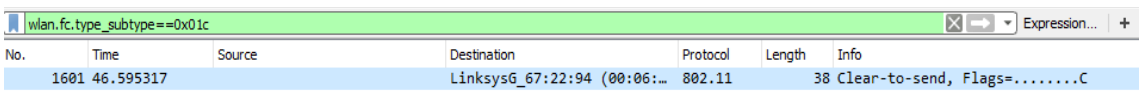



La IP de destino es la IP del AP (punto de acceso) al que se envía, ya que en la zona de control encontramos 3 direcciones, y esta se correspondería con la Receiver address, desde donde será redireccionado dicho paquete hasta llegar a la Destination address, que es a donde realmente queremos enviar los datos.

## *Colisiones*

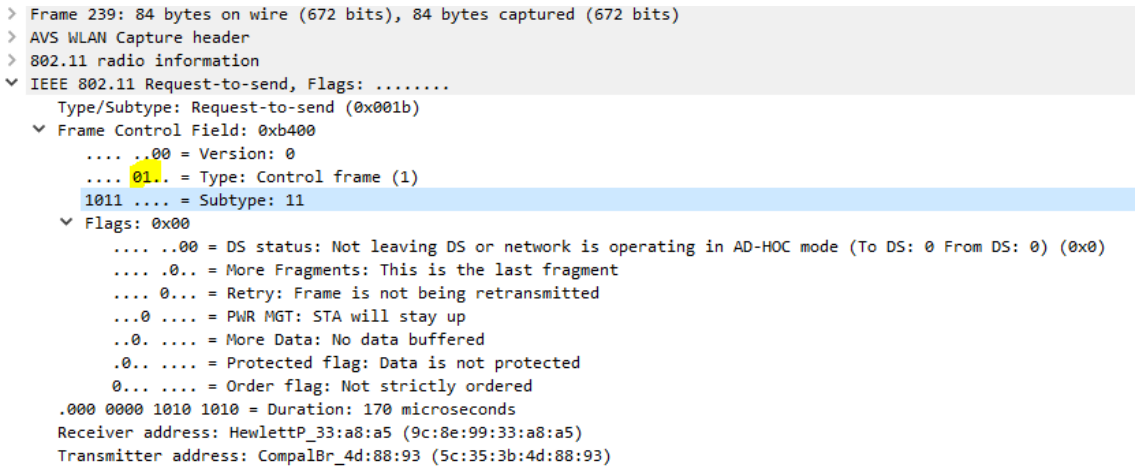
**Cuestión 7.** Localiza las tramas RTS y CTS capturadas en el fichero Wireshar_802_11.pcap. ¿Es posible que sólo haya tramas RTS o CTS? ¿Por qué?

En efecto, encontramos una única trama CTS y ningún RTS. Esto ocurre cuando un dispositivo se acaba de configurar y esta listo para recibir datos.



**Cuestión 8.** Localiza las tramas RTS y CTS en el fichero Wireshark_802_11_RTS_CTS.pcap. ¿Qué información contienen estas tramas? ¿Para qué sirve el valor NAV?

Por una parte, encontramos las tramas Request-to-send, cuya estructura es la siguiente:




Podemos observar que se trata de un frame de control, concretamente un RTS (subtipo 1011). Se utiliza para pedir acceso al canal (se le pide permiso al AP). Si el acceso es concedido, un frame del tipo CTS (Clear-to-send) será enviado de vuelta a la estación que envió el RTS.

Si buscamos tramas CTS encontramos la siguiente estructura en ellas: