# IEEE 802.11 con Wireshark

**1A. (Para Wireshark_802_11 y Wireshark_802_11LOCAL) ¿Cuántas APs están en la cobertura de la estación desde la que se realizó la captura? (Localiza las tramas Beacon) ¿Cuáles son los identificadores de las tres estaciones desde las que se están recibiendo más tramas de este tipo? ¿Cada cuánto tiempo envían una trama Beacon? ¿Qué tipo de trama es? (valor del campo tipo).**

*Comando usado: wlan.fc.type_subtype==8*

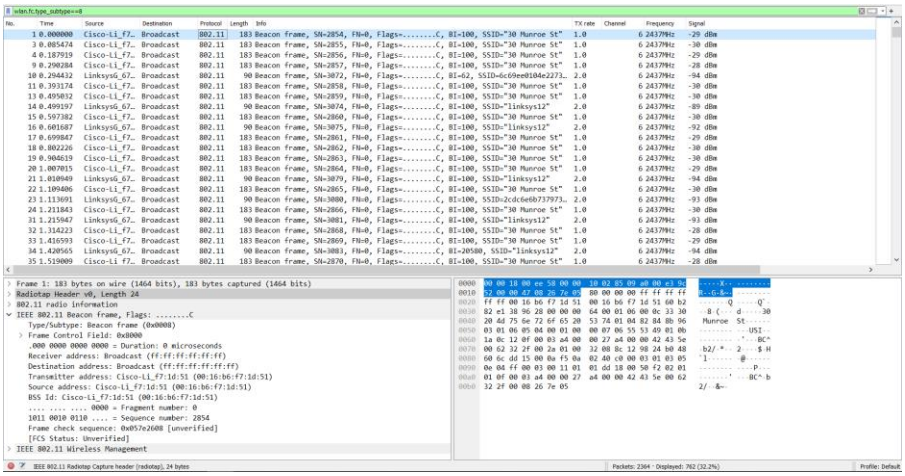
El valor del campo tipo para todas las tramas es 0, ya que son tramas de gestión.

Tiempo de intervalo de envío de tramas igual para todas las estaciones.

```
▾ IEEE 802.11 Wireless Management
  ▾ Fixed parameters (12 bytes)
      Timestamp: 9534964429292
      Beacon Interval: 0.102400 [Seconds]
    ▸ Capabilities Information: 0x0011
```

d3:95:ca:bb:f0:f5 / LinksysG_67:22:94 / Cisco-Li_f7:1d:51 / Cisco-Li_f5:ba:bb / 00:ac:20:67:22:94 / 00:86:bc:d2:22:94

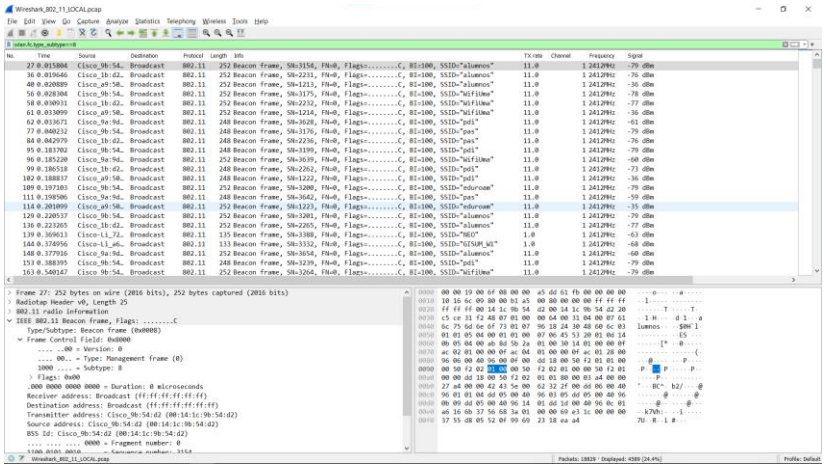
| ***N*** | ***AP*** | ***Tiempo Envío (segundos)*** |
|---|---|---|
| 1 | Cisco-Li_f7:1d:51 | 0.102400 |
| 2 | Cisco-Li_f5:ba:bb | 0.102400 |
| 3 | LinksysG_67:22:94 | 0.102400 |



*802.11*

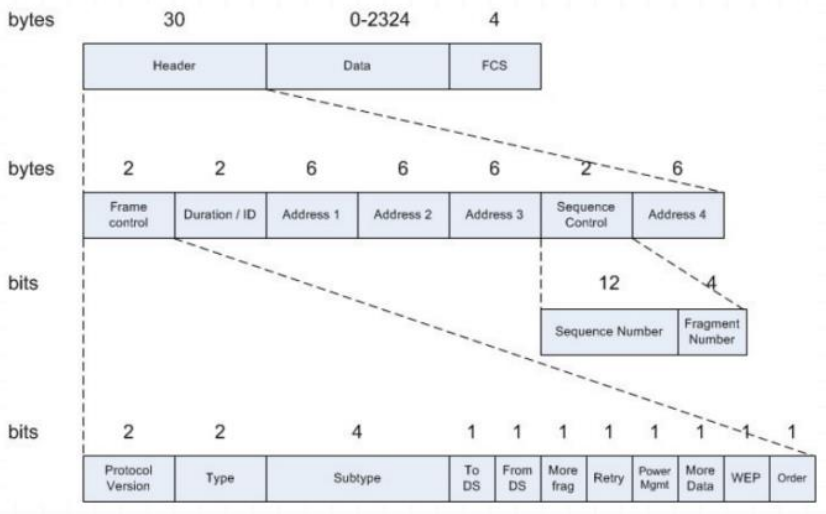
Hay 33 APs

Mas repetidas: 00:1e: 7a:a9:50:a5 / 00:1e:7a:a9:50:a4 / 00:1e:7a:a9:50:a2



*802.11 Local*

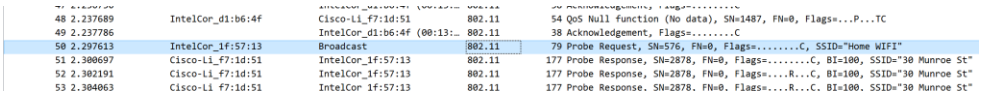
**1B. (Para Wireshark_802_11) Muestra con una captura de pantalla la estructura y contenido de los campos de una trama Beacon.**




**2A. (Para Wireshark_802_11 y Wireshark_802_11LOCAL) ¿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 del campo tipo).**

*Wireshark_802_11*

Tramas 50 y 51, donde InterCor manda un mensaje BroadCast de tipo Probe Request y le responde AP Cisco-Li… con una trama de tipo Probe Request.



Las tramas que realizan un escaneo activo son IntelCor_1f: 57:13 y IntelCor_d1: b6:4f, y los puntos de acceso que responde es Cisco-Li_f7:1d:51.

*Wireshark_802_11_LOCAL*

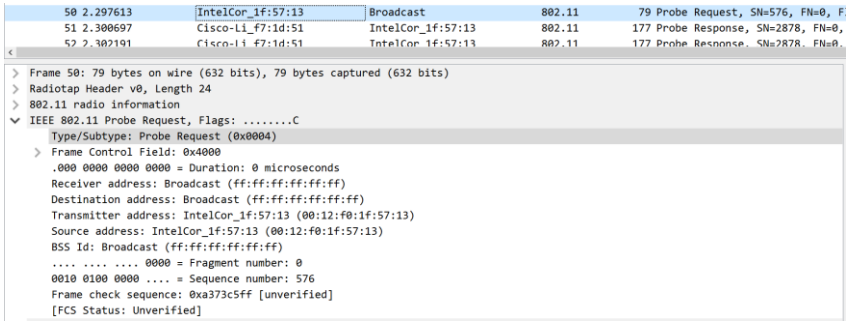
Tenemos hasta 8 estaciones que realizan escaneos activos.

| | | | | | |
|---|---|---|---|---|---|
| 18430 | 22.377093 | ASUSTekC_56:d3:99 | Cisco_1b:d2:62 | 802.11 | 53 Null function (No data), SN=98, FN=0, Flags=...P...TC |
| 12340 | 15.128219 | HewlettP_d1:04:03 | Broadcast | 802.11 | 82 Probe Request, SN=1183, FN=0, Flags=........C, SSID="Red wifi MatAp" |
| 8102 | 10.063376 | HewlettP_54:cb:7c | Broadcast | 802.11 | 90 Probe Request, SN=1315, FN=0, Flags=........C, SSID="FTE-8105" |
| 8114 | 10.079555 | HewlettP_54:cb:7c | Broadcast | 802.11 | 90 Probe Request, SN=1316, FN=0, Flags=........C, SSID="FTE-8105" |
| 8136 | 10.115964 | HewlettP_54:cb:7c | Broadcast | 802.11 | 90 Probe Request, SN=1318, FN=0, Flags=........C, SSID="FTE-8105" |
| 16754 | 20.261517 | HewlettP_54:cb:7c | Broadcast | 802.11 | 90 Probe Request, SN=1341, FN=0, Flags=........C, SSID="FTE-8105" |
| 16791 | 20.298477 | HewlettP_54:cb:7c | Broadcast | 802.11 | 90 Probe Request, SN=1343, FN=0, Flags=........C, SSID="FTE-8105" |
| 6180 | 7.895536 | MurataMa_56:bf:1e | Broadcast | 802.11 | 294 Probe Request, SN=2, FN=0, Flags=........C, SSID=Wildcard (Broadcast) |
| 13217 | 16.046146 | HTC_83:a1:a7 | Broadcast | 802.11 | 99 Probe Request, SN=2038, FN=0, Flags=........C, SSID=Wildcard (Broadcast) |
| 5187 | 6.905003 | HonHaiPr_7e:b7:25 | Broadcast | 802.11 | 71 Probe Request, SN=2886, FN=0, Flags=........C, SSID=Wildcard (Broadcast) |
| 16337 | 19.714248 | SamsungE_c3:c4:19 | Broadcast | 802.11 | 293 Probe Request, SN=3, FN=0, Flags=........C, SSID="WLAN_2CE5" |
| 5027 | 6.794017 | Apple_3a:5d:96 | Broadcast | 802.11 | 92 Probe Request, SN=3677, FN=0, Flags=........C, SSID="CIC-IPN" |
| 16351 | 19.735677 | SamsungE_c3:c4:19 | Broadcast | 802.11 | 293 Probe Request, SN=6, FN=0, Flags=........C, SSID="WLAN_2CE5" |
| 18079 | 21.952146 | ASUSTekC_56:d3:99 | Broadcast | 802.11 | 145 Probe Request, SN=81, FN=0, Flags=........C, SSID=Wildcard (Broadcast) |
| 18119 | 21.972567 | ASUSTekC_56:d3:99 | Broadcast | 802.11 | 145 Probe Request, SN=82, FN=0, Flags=........C, SSID=Wildcard (Broadcast) |
| 15649 | 18.847555 | Cisco_1b:d5:01 | HonHaiPr_c2:e3:2b | 802.11 | 246 Probe Response, SN=1440, FN=0, Flags=........C, BI=100, SSID="eduroam" |
| 15650 | 18.849048 | Cisco_1b:d5:02 | HonHaiPr_c2:e3:2b | 802.11 | 246 Probe Response, SN=1441, FN=0, Flags=........C, BI=100, SSID="alumnos" |
| 15652 | 18.854979 | Cisco_1b:d5:05 | HonHaiPr_c2:e3:2b | 802.11 | 242 Probe Response, SN=1443, FN=0, Flags=........C, BI=100, SSID="pdi" |
| 5190 | 6.919555 | Cisco_a9:50:a1 | HonHaiPr_7e:b7:25 | 802.11 | 246 Probe Response, SN=1600, FN=0, Flags=........C, BI=100, SSID="eduroam" |
| 5194 | 6.921403 | Cisco_a9:50:a1 | HonHaiPr_7e:b7:25 | 802.11 | 246 Probe Response, SN=1600, FN=0, Flags=....R...C, BI=100, SSID="eduroam" |
| 5196 | 6.922638 | Cisco_a9:50:a2 | HonHaiPr_7e:b7:25 | 802.11 | 246 Probe Response, SN=1601, FN=0, Flags=........C, BI=100, SSID="alumnos" |
| 5197 | 6.923288 | Cisco_a9:50:a2 | HonHaiPr_7e:b7:25 | 802.11 | 246 Probe Response, SN=1601, FN=0, Flags=....R...C, BI=100, SSID="alumnos" |
| 5199 | 6.924505 | Cisco_a9:50:a4 | HonHaiPr_7e:b7:25 | 802.11 | 246 Probe Response, SN=1602, FN=0, Flags=........C, BI=100, SSID="WifiUma" |
| 5202 | 6.925694 | Cisco_a9:50:a4 | HonHaiPr_7e:b7:25 | 802.11 | 246 Probe Response, SN=1602, FN=0, Flags=....R...C, BI=100, SSID="WifiUma" |
| 5204 | 6.927518 | Cisco_a9:50:a5 | HonHaiPr_7e:b7:25 | 802.11 | 242 Probe Response, SN=1603, FN=0, Flags=........C, BI=100, SSID="pdi" |

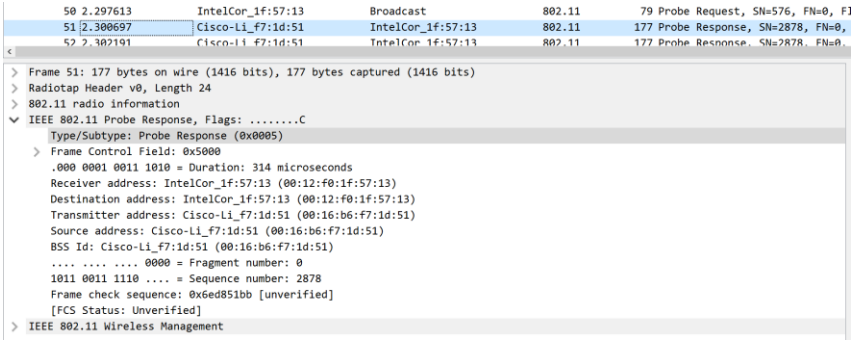
*Se adjuntan algunas de ellas*

**2B. (Para Wireshark_802_11 y Wireshark_802_11LOCAL) Localiza en la captura alguna trama de petición activo y la respuesta correspondiente. Muestra con una captura de pantalla la estructura y contenido de ambas tramas.**

*Tramas 50 y 51 en por ejemplo Wireshark_802_11*

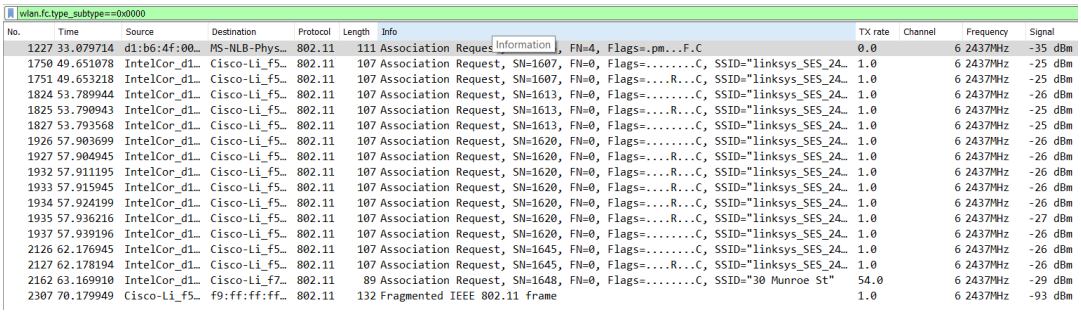



*Probe Request*




*Probe Response*

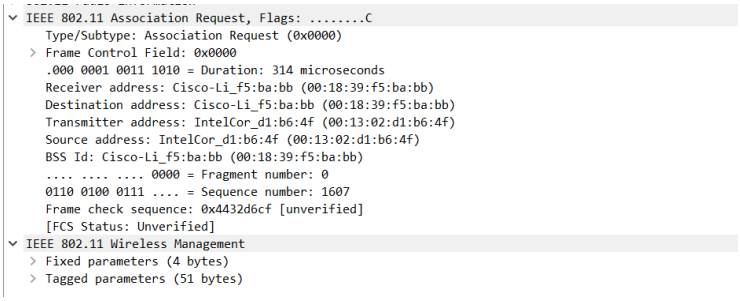
## 3A. Localiza en la captura Wireshark_802_11 alguna petición de asociación. ¿Qué información incluye? Localiza en la captura alguna respuesta de asociación. ¿Qué información incluye? ¿Qué tipos de tramas son? (valor del campo tipo).



wlan.fc.type_subtype==0x0000

| No. | Time | Source | Destination | Protocol | Length | Info | TX rate | Channel | Frequency | Signal |
|---|---|---|---|---|---|---|---|---|---|---|
| 1227 | 33.079714 | d1:b6:4f:00… | MS-NLB-Phys… | 802.11 | 111 | Association Reques[Information], FN=4, Flags=.pm...F.C | 0.0 | 6 | 2437MHz | -35 dBm |
| 1750 | 49.651078 | IntelCor_d1… | Cisco-Li_f5… | 802.11 | 107 | Association Request, SN=1607, FN=0, Flags=........C, SSID="linksys_SES_24… | 1.0 | 6 | 2437MHz | -25 dBm |
| 1751 | 49.653218 | IntelCor_d1… | Cisco-Li_f5… | 802.11 | 107 | Association Request, SN=1607, FN=0, Flags=....R...C, SSID="linksys_SES_24… | 1.0 | 6 | 2437MHz | -25 dBm |
| 1824 | 53.789944 | IntelCor_d1… | Cisco-Li_f5… | 802.11 | 107 | Association Request, SN=1613, FN=0, Flags=........C, SSID="linksys_SES_24… | 1.0 | 6 | 2437MHz | -26 dBm |
| 1825 | 53.790943 | IntelCor_d1… | Cisco-Li_f5… | 802.11 | 107 | Association Request, SN=1613, FN=0, Flags=....R...C, SSID="linksys_SES_24… | 1.0 | 6 | 2437MHz | -25 dBm |
| 1827 | 53.793568 | IntelCor_d1… | Cisco-Li_f5… | 802.11 | 107 | Association Request, SN=1613, FN=0, Flags=........C, SSID="linksys_SES_24… | 1.0 | 6 | 2437MHz | -25 dBm |
| 1926 | 57.903699 | IntelCor_d1… | Cisco-Li_f5… | 802.11 | 107 | Association Request, SN=1620, FN=0, Flags=........C, SSID="linksys_SES_24… | 1.0 | 6 | 2437MHz | -26 dBm |
| 1927 | 57.904945 | IntelCor_d1… | Cisco-Li_f5… | 802.11 | 107 | Association Request, SN=1620, FN=0, Flags=....R...C, SSID="linksys_SES_24… | 1.0 | 6 | 2437MHz | -26 dBm |
| 1932 | 57.911195 | IntelCor_d1… | Cisco-Li_f5… | 802.11 | 107 | Association Request, SN=1620, FN=0, Flags=....R...C, SSID="linksys_SES_24… | 1.0 | 6 | 2437MHz | -26 dBm |
| 1933 | 57.915945 | IntelCor_d1… | Cisco-Li_f5… | 802.11 | 107 | Association Request, SN=1620, FN=0, Flags=....R...C, SSID="linksys_SES_24… | 1.0 | 6 | 2437MHz | -26 dBm |
| 1934 | 57.924199 | IntelCor_d1… | Cisco-Li_f5… | 802.11 | 107 | Association Request, SN=1620, FN=0, Flags=....R...C, SSID="linksys_SES_24… | 1.0 | 6 | 2437MHz | -26 dBm |
| 1935 | 57.936216 | IntelCor_d1… | Cisco-Li_f5… | 802.11 | 107 | Association Request, SN=1620, FN=0, Flags=....R...C, SSID="linksys_SES_24… | 1.0 | 6 | 2437MHz | -27 dBm |
| 1937 | 57.939196 | IntelCor_d1… | Cisco-Li_f5… | 802.11 | 107 | Association Request, SN=1620, FN=0, Flags=........C, SSID="linksys_SES_24… | 1.0 | 6 | 2437MHz | -26 dBm |
| 2126 | 62.176945 | IntelCor_d1… | Cisco-Li_f5… | 802.11 | 107 | Association Request, SN=1645, FN=0, Flags=........C, SSID="linksys_SES_24… | 1.0 | 6 | 2437MHz | -26 dBm |
| 2127 | 62.178194 | IntelCor_d1… | Cisco-Li_f5… | 802.11 | 107 | Association Request, SN=1645, FN=0, Flags=....R...C, SSID="linksys_SES_24… | 1.0 | 6 | 2437MHz | -26 dBm |
| 2162 | 63.169910 | IntelCor_d1… | Cisco-Li_f7… | 802.11 | 89 | Association Request, SN=1648, FN=0, Flags=........C, SSID="30 Munroe St" | 54.0 | 6 | 2437MHz | -29 dBm |
| 2307 | 70.179949 | Cisco-Li_f5… | f9:ff:ff:ff… | 802.11 | 132 | Fragmented IEEE 802.11 frame | 1.0 | 6 | 2437MHz | -93 dBm |

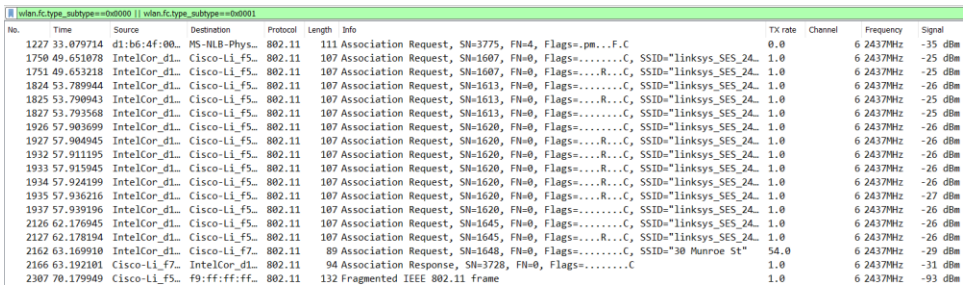
*Filtramos con wlan.fc.type_subtype==0x0000*



```
▾ IEEE 802.11 Association Request, Flags: ........C
    Type/Subtype: Association Request (0x0000)
  › Frame Control Field: 0x0000
    .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 [unverified]
    [FCS Status: Unverified]
▾ IEEE 802.11 Wireless Management
  › Fixed parameters (4 bytes)
  › Tagged parameters (51 bytes)
```

*Ejemplo de contenido de la trama*

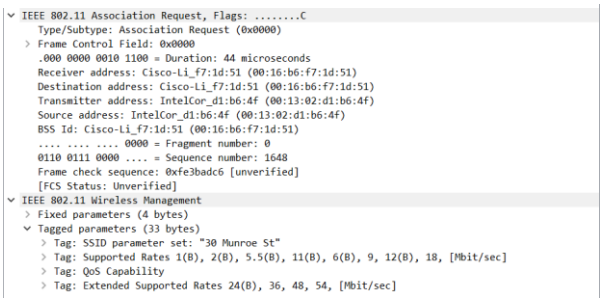
## 3B. Localiza en la captura Wireshark_802_11 alguna trama de petición de asociación y la respuesta correspondiente. Muestra con una captura de pantalla la estructura y contenido de ambas tramas.



wlan.fc.type_subtype==0x0000 || wlan.fc.type_subtype==0x0001

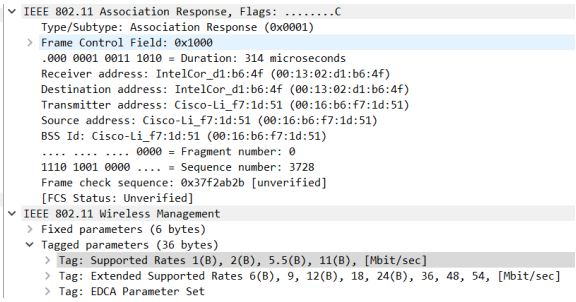
| No. | Time | Source | Destination | Protocol | Length | Info | TX rate | Channel | Frequency | Signal |
|---|---|---|---|---|---|---|---|---|---|---|
| 1227 | 33.079714 | d1:b6:4f:00… | MS-NLB-Phys… | 802.11 | 111 | Association Request, SN=3775, FN=4, Flags=.pm...F.C | 0.0 | 6 | 2437MHz | -35 dBm |
| 1750 | 49.651078 | IntelCor_d1… | Cisco-Li_f5… | 802.11 | 107 | Association Request, SN=1607, FN=0, Flags=........C, SSID="linksys_SES_24… | 1.0 | 6 | 2437MHz | -25 dBm |
| 1751 | 49.653218 | IntelCor_d1… | Cisco-Li_f5… | 802.11 | 107 | Association Request, SN=1607, FN=0, Flags=....R...C, SSID="linksys_SES_24… | 1.0 | 6 | 2437MHz | -25 dBm |
| 1824 | 53.789944 | IntelCor_d1… | Cisco-Li_f5… | 802.11 | 107 | Association Request, SN=1613, FN=0, Flags=........C, SSID="linksys_SES_24… | 1.0 | 6 | 2437MHz | -26 dBm |
| 1825 | 53.790943 | IntelCor_d1… | Cisco-Li_f5… | 802.11 | 107 | Association Request, SN=1613, FN=0, Flags=....R...C, SSID="linksys_SES_24… | 1.0 | 6 | 2437MHz | -25 dBm |
| 1827 | 53.793568 | IntelCor_d1… | Cisco-Li_f5… | 802.11 | 107 | Association Request, SN=1613, FN=0, Flags=........C, SSID="linksys_SES_24… | 1.0 | 6 | 2437MHz | -25 dBm |
| 1926 | 57.903699 | IntelCor_d1… | Cisco-Li_f5… | 802.11 | 107 | Association Request, SN=1620, FN=0, Flags=........C, SSID="linksys_SES_24… | 1.0 | 6 | 2437MHz | -26 dBm |
| 1927 | 57.904945 | IntelCor_d1… | Cisco-Li_f5… | 802.11 | 107 | Association Request, SN=1620, FN=0, Flags=....R...C, SSID="linksys_SES_24… | 1.0 | 6 | 2437MHz | -26 dBm |
| 1932 | 57.911195 | IntelCor_d1… | Cisco-Li_f5… | 802.11 | 107 | Association Request, SN=1620, FN=0, Flags=....R...C, SSID="linksys_SES_24… | 1.0 | 6 | 2437MHz | -26 dBm |
| 1933 | 57.915945 | IntelCor_d1… | Cisco-Li_f5… | 802.11 | 107 | Association Request, SN=1620, FN=0, Flags=....R...C, SSID="linksys_SES_24… | 1.0 | 6 | 2437MHz | -26 dBm |
| 1934 | 57.924199 | IntelCor_d1… | Cisco-Li_f5… | 802.11 | 107 | Association Request, SN=1620, FN=0, Flags=....R...C, SSID="linksys_SES_24… | 1.0 | 6 | 2437MHz | -26 dBm |
| 1935 | 57.936216 | IntelCor_d1… | Cisco-Li_f5… | 802.11 | 107 | Association Request, SN=1620, FN=0, Flags=....R...C, SSID="linksys_SES_24… | 1.0 | 6 | 2437MHz | -27 dBm |
| 1937 | 57.939196 | IntelCor_d1… | Cisco-Li_f5… | 802.11 | 107 | Association Request, SN=1620, FN=0, Flags=........C, SSID="linksys_SES_24… | 1.0 | 6 | 2437MHz | -26 dBm |
| 2126 | 62.176945 | IntelCor_d1… | Cisco-Li_f5… | 802.11 | 107 | Association Request, SN=1645, FN=0, Flags=........C, SSID="linksys_SES_24… | 1.0 | 6 | 2437MHz | -26 dBm |
| 2127 | 62.178194 | IntelCor_d1… | Cisco-Li_f5… | 802.11 | 107 | Association Request, SN=1645, FN=0, Flags=....R...C, SSID="linksys_SES_24… | 1.0 | 6 | 2437MHz | -26 dBm |
| 2162 | 63.169910 | IntelCor_d1… | Cisco-Li_f7… | 802.11 | 89 | Association Request, SN=1648, FN=0, Flags=........C, SSID="30 Munroe St" | 54.0 | 6 | 2437MHz | -29 dBm |
| 2166 | 63.192101 | Cisco-Li_f7… | IntelCor_d1… | 802.11 | 94 | Association Response, SN=3728, FN=0, Flags=........C | 1.0 | 6 | 2437MHz | -31 dBm |
| 2307 | 70.179949 | Cisco-Li_f5… | f9:ff:ff:ff… | 802.11 | 132 | Fragmented IEEE 802.11 frame | 1.0 | 6 | 2437MHz | -93 dBm |

*Filtramos por wlan.fc.type_subtype==0x0000 || wlan.fc.type_subtype==0x0001*



```
▾ IEEE 802.11 Association Request, Flags: ........C
    Type/Subtype: Association Request (0x0000)
  › Frame Control Field: 0x0000
    .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)
    .... .... .... 0000 = Fragment number: 0
    0110 0111 0000 .... = Sequence number: 1648
    Frame check sequence: 0xfe3badc6 [unverified]
    [FCS Status: Unverified]
▾ IEEE 802.11 Wireless Management
  › Fixed parameters (4 bytes)
  ▾ Tagged parameters (33 bytes)
    › Tag: SSID parameter set: "30 Munroe St"
    › Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18, [Mbit/sec]
    › Tag: QoS Capability
    › Tag: Extended Supported Rates 24(B), 36, 48, 54, [Mbit/sec]
```

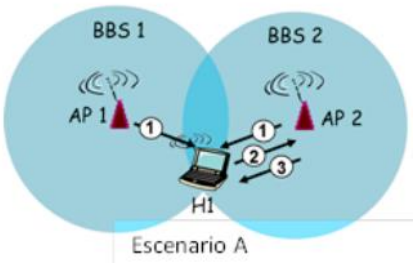
*Trama Association Request*



```
▾ IEEE 802.11 Association Response, Flags: ........C
    Type/Subtype: Association Response (0x0001)
  › Frame Control Field: 0x1000
    .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 [unverified]
    [FCS Status: Unverified]
▾ IEEE 802.11 Wireless Management
  › Fixed parameters (6 bytes)
  ▾ Tagged parameters (36 bytes)
    › Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
    › Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    › Tag: EDCA Parameter Set
```

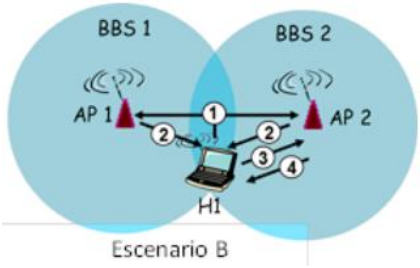
*Trama Association Response*

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



Escenario A

El escenario A representa un **escaneo pasivo**. Los puntos de acceso se ponen en contacto con la estación enviándole tramas Beacon. La estación elige un punto de acceso para mandar peticiones de conexión con Association Request y la AP responde con un Association Response.



Escenario B

El escenario B representa un **escaneo activo**. En este caso es la estación quién manda tramas Probe Request buscando APs cercanos, quienes reciben la trama y le envían de vuelta a la estación una trama Probe Response para confirma que existe. Tras ello, es la estación la que nuevamente el elige una AP y empieza a enviarle peticiones.

**5A. ¿Cuántas tramas de datos diferentes observas en la captura Wireshark_802_11LOCAL? ¿Qué estaciones participan de esta comunicación? ¿Hay comunicación directa entre estaciones o siempre interviene un punto de acceso?**

Encontramos tramas Data, QoS Data y Null Function. Entre las estaciones que participan se encuentran Cisco, Apple, ASUS e Intel, donde se producen entre ellas comunicaciones directas.

**5B Localiza en la captura Wireshark_802_11 alguna trama de datos y la confirmación correspondiente. Muestra la estructura y contenido de ambas tramas.**

```
1719 49.132884  IntelCor_d1…  Cisco-Li_f7…  802.11     54 QoS Null function (No data), SN=1600, FN=0, Flags=...P...TC
1720 49.132981                IntelCor_d1…  802.11     38 Acknowledgement, Flags=........C
```

```
IEEE 802.11 QoS Null function (No data), Flags: ...P...TC
    Type/Subtype: QoS Null function (No data) (0x002c)
  > Frame Control Field: 0xc811
    .000 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Transmitter address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    Destination address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    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
    0110 0100 0000 .... = Sequence number: 1600
    Frame check sequence: 0x41e92fa3 [unverified]
    [FCS Status: Unverified]
  > Qos Control: 0x0000
```

*Trama QoS*

```
IEEE 802.11 Acknowledgement, Flags: ........C
    Type/Subtype: Acknowledgement (0x001d)
  > Frame Control Field: 0xd400
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    Frame check sequence: 0xe08e68a4 [unverified]
    [FCS Status: Unverified]
```

*Trama ACK de confirmación*

**5C. Localiza en la captura Wireshark_802_11LOCAL 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?**

```
> 802.11 radio information
v IEEE 802.11 Null function (No data), Flags: ....R.FTC
    Type/Subtype: Null function (No data) (0x0024)
  v Frame Control Field: 0x480b
      .... ..00 = Version: 0
      .... 10.. = Type: Data frame (2)
      0100 .... = Subtype: 4
    > Flags: 0x0b
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: Cisco_43:9f:60 (00:13:80:43:9f:60)
    Transmitter address: Cisco-Li_72:e1:78 (00:14:bf:72:e1:78)
    Destination address: Cisco_43:9f:60 (00:13:80:43:9f:60)
    Source address: Cisco-Li_72:e1:78 (00:14:bf:72:e1:78)
    .... .... .... 0000 = Fragment number: 0
    1111 0110 1001 .... = Sequence number: 3945
    Frame check sequence: 0xf3aacee2 [unverified]
    [FCS Status: Unverified]
```

No contiene el campo Data, ya que no contiene datos. La utilidad principal que tiene este tipo de tramas son varias, como para el mantenimiento de la conexión, permitiendo mantener activa la conexión entre un dispositivo cliente y un AP. Enviar información sobre el estado del dispositivo, como el consumo, o para sincronizar dispositivos como cuando queremos hacer un *login* a un servidor.

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

**6A. ¿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?**

http

| No. | Time | Source | Destination | Protocol | Length | Info | TX rate | Channel | Frequency | Signal |
|---|---|---|---|---|---|---|---|---|---|---|
| 480 | 24.828253 | 192.168.1.109 | 128.119.245… | HTTP | 537 | GET /wireshark-labs/alice.txt HTTP/1.1 | 48.0 | 6 | 2437MHz | -38 dBm |
| 868 | 25.126724 | 128.119.245… | 192.168.1.109 | HTTP | 400 | HTTP/1.1 200 OK (text/plain) | 48.0 | 6 | 2437MHz | -36 dBm |
| 873 | 25.185381 | 192.168.1.109 | 128.119.245… | HTTP | 444 | GET /favicon.ico HTTP/1.1 | 54.0 | 6 | 2437MHz | -38 dBm |
| 875 | 25.209241 | 128.119.245… | 192.168.1.109 | HTTP/… | 1527 | HTTP/1.1 404 Not Found | 48.0 | 6 | 2437MHz | -38 dBm |
| 1016 | 32.825992 | 192.168.1.109 | 128.119.240… | HTTP | 512 | GET / HTTP/1.1 | 54.0 | 6 | 2437MHz | -24 dBm |
| 1055 | 32.892394 | 192.168.1.109 | 128.119.240… | HTTP | 484 | GET /includes/csweb.css HTTP/1.1 | 48.0 | 6 | 2437MHz | -23 dBm |
| 1062 | 32.903631 | 192.168.1.109 | 128.119.101.5 | HTTP | 440 | GET /favicon.ico HTTP/1.1 | 48.0 | 6 | 2437MHz | -22 dBm |
| 1066 | 32.909945 | 128.119.240… | 192.168.1.109 | HTTP | 464 | HTTP/1.1 200 OK (text/html) | 48.0 | 6 | 2437MHz | -34 dBm |
| 1098 | 32.939761 | 128.119.240… | 192.168.1.109 | HTTP | 333 | HTTP/1.1 200 OK (text/css) | 54.0 | 6 | 2437MHz | -38 dBm |
| 1110 | 32.946809 | 128.119.101.5 | 192.168.1.109 | HTTP | 753 | HTTP/1.1 200 OK (image/x-icon) | 54.0 | 6 | 2437MHz | -36 dBm |
| 1117 | 32.956076 | 192.168.1.109 | 128.119.101.5 | HTTP | 509 | GET /umhome/identity/top_strip/wm_formal_lgrey.gif HTTP/1.1 | 54.0 | 6 | 2437MHz | -24 dBm |
| 1129 | 32.977250 | 128.119.101.5 | 192.168.1.109 | HTTP | 1490 | HTTP/1.1 200 OK (GIF89a) | 48.0 | 6 | 2437MHz | -34 dBm |
| 1140 | 32.980813 | 192.168.1.109 | 128.119.240… | HTTP | 484 | GET /images/spacer.gif HTTP/1.1 | 54.0 | 6 | 2437MHz | -25 dBm |
| 1169 | 33.022167 | 192.168.1.109 | 128.119.240… | HTTP | 494 | GET /images/csbldng_entrance.jpg HTTP/1.1 | 54.0 | 6 | 2437MHz | -24 dBm |
| 1183 | 33.032012 | 192.168.1.109 | 64.233.187.… | HTTP | 468 | GET /urchin.js HTTP/1.1 | 54.0 | 6 | 2437MHz | -24 dBm |

*Filtramos por http y la primera trama será la que buscamos*

```
v IEEE 802.11 QoS Data, Flags: .......TC
    Type/Subtype: QoS Data (0x0028)
  > Frame Control Field: 0x8801
    .000 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Transmitter address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    Destination address: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)
    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
    0000 0011 0011 .... = Sequence number: 51
    Frame check sequence: 0x147e6bd9 [unverified]
    [FCS Status: Unverified]
  v Qos Control: 0x0000
      .... .... .... 0000 = TID: 0
      [.... .... .... .000 = Priority: Best Effort (Best Effort) (0)]
      .... .... ...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)
```

Si observamos la trama podemos ver que en el campo DS status tenemos un valor de 01, donde el To DS es un 1 y el From DS es un 0. Por lo tanto, mirando las diapositivas podemos darnos cuenta de que estamos en el caso 3 de los mecanismos de direccionamiento.

```
..01 = DS status: Frame from STA to DS via an AP (To DS: 1 From DS: 0) (0x1)
```

**AP receptor**: 00:16:b6:f7:1d:51

**Origen**: 00:13:02:d1:b6:4f

**Destino**: 00:16:b6:f4:eb:a8

| To DS | From DS | Dirección 1 | Dirección 2 | Dirección 3 | Dirección 4 |
|---|---|---|---|---|---|
| 0 | 0 | Destino | Origen | ID de BSSS | N/A |
| 0 | 1 | Destino | AP emisor | Origen | N/A |
| 1 | 0 | AP receptor | Origen | Destino | N/A |
| 1 | 1 | AP receptor | AP emisor | Destino | Origen |

**6B. ¿Cuál 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.**

| | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 480 | 24.828253 | 192.168.1.109 | 128.119.245.12 | HTTP | 537 | GET /wireshark-labs/alice.txt HTTP/1.1 |

La IP del host que envía la petición es 192.168.1.109, y la IP destino es 128.119.245.12. La dirección IP corresponde con la página web de la universidad de Massachusetts.

**7. Localiza las tramas RTS y CTS en la captura Wireshark_802_11. ¿Es posible que sólo haya tramas RTS? ¿Y CTS? ¿Por qué?**

| | | | | | |
|---|---|---|---|---|---|
| 46.595317 | | LinksysG_67:22:94 (… | 802.11 | 38 | Clear-to-send, Flags=.....C |

Solo tenemos una trama que es CTS.

Puede haber solo tramas RTS o CTS. Por ejemplo, un punto de acceso puede enviar tramas RTS, pero no haber tramas CTS debido a que no hay nadie a quién haya podido conectarse. Y en el caso de CTS, se puede enviar una trama de este tipo para decir que la estación está disponible para recibir información, pero que durante el tiempo que dura la captura no se ha querido enviar nada.

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

**RTS**: Es una trama de control que indica la intención de transmitir y solicita permiso para hacerlo, ayudando a evitar colisiones en el canal al reservar tiempo para transmitir y notifica a otros dispositivos cercanos que deben esperar antes de intentar transmitir. Contiene la dirección del receptor y del transmisor y el NAV, que es el tiempo mencionado previamente que se solicita para reservar el canal y transmitir sin colisiones.

**CTS**: Trama que confirma que el canal está libre y que el dispositivo que envió la trama RTS puede proceder con la transmisión. Contiene la dirección del receptor y el NAV, menor que el del RTS.

**NAV**: El NAV es un vector de asignación de red, es el tiempo que se necesita utilizar el canal según el tamaño de la trama, en el RTS se manda al dispositivo al que se le quiere mandar información, y en el CTS se difunde por los demás dispositivos para que sepan que en ese tiempo el canal va a estar ocupado y hasta que no se acabe ese tiempo no intenten transmitir.