Práctica WLAN: Parte 2

Cristina Díaz García

Diciembre 2018

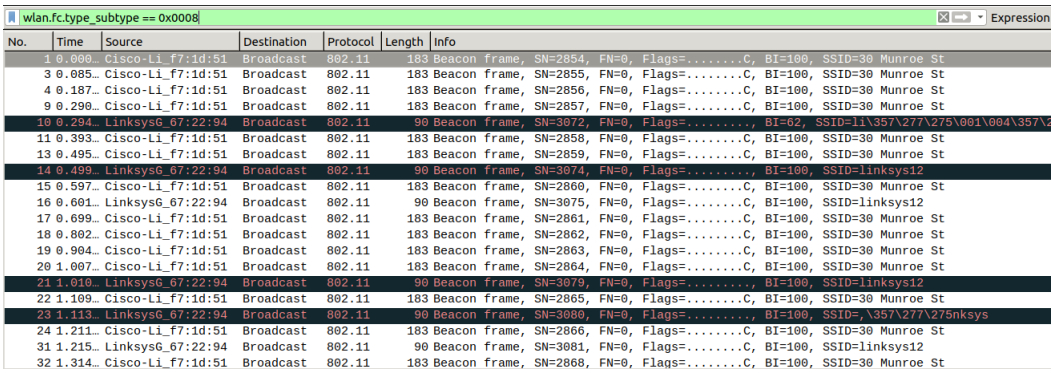
Índice

1. Cuestión 1

1.1. WLAN_802_11

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

Usando el filtro *wlan.fc.type_subtype == 0x0008* obtenemos las tramas Beacon. Guardamos los paquetes obtenidos como CSV, y haciendo uso del comando cut, obtenemos de la información el campo de los SSIDs. En total hay 4 APs.



¿Cuales son sus identificadores?

- 30 Munroe St
- linksys12
- linksys1R
- linksys_SES_24086

Como se puede comprobar en la imagen siguiente, los nombres de los SSIDs están corruptos en algunos paquetes.

```
SSID=30 Munroe St"
SSID=li\\357\\277\\275\\001\\004\\357\\277[Malformed Packet]"
SSID=linksys12"
SSID=li\\bhsys12"
SSID=linksys1R"
SSID=linksys_SES_24086"
SSID=lin\\357\\277\\275~ys"
SSID=lin+\\357\\277\\275ys"
SSID=winksys_SES_24086\\001\\004\\357\\277\\275\\357\\277\\275\\357\\277\\275\\357\\277\\275\\003[Malformed Packet]"
SSID=lin+m\\357\\277\\275s[Packet size limited during capture]"
```

¿Cada cuanto tiempo envían una trama de Beacon?

Cada décima de segundo aproximadamente.

```
Beacon Interval: 0,102400 [Seconds]
```

¿Qué tipo de trama es? (valor de campo tipo)
Es de tipo 0.

```
▾ IEEE 802.11 Beacon frame, Flags: ........C
    Type/Subtype: Beacon frame (0x0008)
```

1.2. WLAN_802_11_LOCAL

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

Usando el filtro *wlan.fc.type_subtype == 0x0008* obtenemos las tramas Beacon. Guardamos los paquetes obtenidos como CSV, y haciendo uso del comando cut, obtenemos de la información el campo de los SSIDs. En total hay 4 APs.

wlan.fc.type_subtype == 0x0008 — Expression…

No.	Time	Source	Destination	Protocol	Length	Info
27	0.015…	Cisco_9b:54:d2	Broadcast	802.11	252	Beacon frame, SN=3154, FN=0, Flags=........C, BI=100, SSID=alumnos
36	0.019…	Cisco_1b:d2:62	Broadcast	802.11	252	Beacon frame, SN=2231, FN=0, Flags=........C, BI=100, SSID=alumnos
40	0.020…	Cisco_a9:50:a2	Broadcast	802.11	252	Beacon frame, SN=1213, FN=0, Flags=........C, BI=100, SSID=alumnos
56	0.028…	Cisco_9b:54:d4	Broadcast	802.11	252	Beacon frame, SN=3175, FN=0, Flags=........C, BI=100, SSID=WifiUma
58	0.030…	Cisco_1b:d2:64	Broadcast	802.11	252	Beacon frame, SN=2232, FN=0, Flags=........C, BI=100, SSID=WifiUma
61	0.033…	Cisco_a9:50:a4	Broadcast	802.11	252	Beacon frame, SN=1214, FN=0, Flags=........C, BI=100, SSID=WifiUma
62	0.033…	Cisco_9a:9d:55	Broadcast	802.11	248	Beacon frame, SN=3628, FN=0, Flags=........C, BI=100, SSID=pdi
77	0.040…	Cisco_9b:54:d0	Broadcast	802.11	248	Beacon frame, SN=3176, FN=0, Flags=........C, BI=100, SSID=pas
84	0.042…	Cisco_1b:d2:60	Broadcast	802.11	248	Beacon frame, SN=2236, FN=0, Flags=........C, BI=100, SSID=pas
95	0.183…	Cisco_9b:54:d5	Broadcast	802.11	248	Beacon frame, SN=3199, FN=0, Flags=........C, BI=100, SSID=pdi
96	0.185…	Cisco_9a:9d:54	Broadcast	802.11	252	Beacon frame, SN=3639, FN=0, Flags=........C, BI=100, SSID=WifiUma
99	0.186…	Cisco_1b:d2:65	Broadcast	802.11	248	Beacon frame, SN=2262, FN=0, Flags=........C, BI=100, SSID=pdi
102	0.188…	Cisco_a9:50:a5	Broadcast	802.11	248	Beacon frame, SN=1222, FN=0, Flags=........C, BI=100, SSID=pdi
109	0.197…	Cisco_9b:54:d1	Broadcast	802.11	252	Beacon frame, SN=3200, FN=0, Flags=........C, BI=100, SSID=eduroam
111	0.198…	Cisco_9a:9d:50	Broadcast	802.11	248	Beacon frame, SN=3642, FN=0, Flags=........C, BI=100, SSID=pas
114	0.201…	Cisco_a9:50:a1	Broadcast	802.11	252	Beacon frame, SN=1223, FN=0, Flags=........C, BI=100, SSID=eduroam
129	0.220…	Cisco_9b:54:d2	Broadcast	802.11	252	Beacon frame, SN=3201, FN=0, Flags=........C, BI=100, SSID=alumnos

¿Cuales son sus identificadores?

- alumnos
- WifiUma
- pdi
- pas
- eduroam
- NEO
- GISUM_W1
- ICBWifi

```
SSID=alumnos"
SSID=WifiUma"
SSID=pdi"
SSID=pas"
SSID=eduroam"
SSID=NEO"
SSID=GISUM_W1"
SSID=ICB-Wifi"
```

¿Cada cuanto tiempo envían una trama de Beacon?
Cada décima de segundo aproximadamente.

```
Beacon Interval: 0,102400 [Seconds]
```

¿Qué tipo de trama es? (valor de campo tipo)
Es de tipo 0.

```
▾ IEEE 802.11 Beacon frame, Flags: ........C
    Type/Subtype: Beacon frame (0x0008)
```

2. Ejercicio 1

Muestra la estructura y contenido de los campos de una trama Beacon (de ambos ficheros)

Al ser la estructura y el contenido de los campos el mismo, muestro una trama Beacon correcta y una corrupta del archivo *WLAN_802_11*

Trama Beacon correcta

```
▾ Frame 1: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits)
    Encapsulation type: IEEE 802.11 plus radiotap radio header (23)
    Arrival Time: Jun 29, 2007 04:05:07.072457000 CEST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1183082707.072457000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 183 bytes (1464 bits)
    Capture Length: 183 bytes (1464 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: radiotap:wlan_radio:wlan]
▾ Radiotap Header v0, Length 24
    Header revision: 0
    Header pad: 0
    Header length: 24
  ▾ Present flags
    ▾ Present flags word: 0x000058ee
        .... .... .... .... .... .... .... ...0 = TSFT: Absent
        .... .... .... .... .... .... .... ..1. = Flags: Present
        .... .... .... .... .... .... .... .1.. = Rate: Present
        .... .... .... .... .... .... .... 1... = Channel: Present
        .... .... .... .... .... .... ...0 .... = FHSS: Absent
        .... .... .... .... .... .... ..1. .... = dBm Antenna Signal: Present
```

```
        .... .... .... .... .... .... .1.. .... = dBm Antenna Noise: Present
        .... .... .... .... .... .... 1... .... = Lock Quality: Present
        .... .... .... .... .... ...0 .... .... = TX Attenuation: Absent
        .... .... .... .... .... ..0. .... .... = dB TX Attenuation: Absent
        .... .... .... .... .... .0.. .... .... = dBm TX Power: Absent
        .... .... .... .... .... 1... .... .... = Antenna: Present
        .... .... .... .... ...1 .... .... .... = dB Antenna Signal: Present
        .... .... .... .... ..0. .... .... .... = dB Antenna Noise: Absent
        .... .... .... .... .1.. .... .... .... = RX flags: Present
        .... .... .... .0.. .... .... .... .... = Channel+: Absent
        .... .... .... 0... .... .... .... .... = MCS information: Absent
        .... .... ...0 .... .... .... .... .... = A-MPDU Status: Absent
        .... .... ..0. .... .... .... .... .... = VHT information: Absent
        .... .... .0.. .... .... .... .... .... = frame timestamp: Absent
        .... .... 0... .... .... .... .... .... = HE information: Absent
        .... ...0 .... .... .... .... .... .... = HE-MU information: Absent
        ...0 000. .... .... .... .... .... .... = Reserved: 0x0
        ..0. .... .... .... .... .... .... .... = Radiotap NS next: False
        .0.. .... .... .... .... .... .... .... = Vendor NS next: False
        0... .... .... .... .... .... .... .... = Ext: Absent
  ▾ Flags: 0x10
      .... ...0 = CFP: False
      .... ..0. = Preamble: Long
      .... .0.. = WEP: False
      .... 0... = Fragmentation: False
      ...1 .... = FCS at end: True
```

```
    ..0. .... = Data Pad: False
    .0.. .... = Bad FCS: False
    0... .... = Short GI: False
  Data Rate: 1,0 Mb/s
  Channel frequency: 2437 [BG 6]
▾ Channel flags: 0x00a0, Complementary Code Keying (CCK), 2 GHz spectrum
    .... .... ...0 .... = Turbo: False
    .... .... ..1. .... = Complementary Code Keying (CCK): True
    .... .... .0.. .... = Orthogonal Frequency-Division Multiplexing (OFDM): False
    .... .... 1... .... = 2 GHz spectrum: True
    .... ...0 .... .... = 5 GHz spectrum: False
    .... ..0. .... .... = Passive: False
    .... .0.. .... .... = Dynamic CCK-OFDM: False
    .... 0... .... .... = Gaussian Frequency Shift Keying (GFSK): False
    ...0 .... .... .... = GSM (900MHz): False
    ..0. .... .... .... = Static Turbo: False
    .0.. .... .... .... = Half Rate Channel (10MHz Channel Width): False
    0... .... .... .... = Quarter Rate Channel (5MHz Channel Width): False
  Antenna signal: -29dBm
  Antenna noise: -100dBm
  Signal Quality: 82
  Antenna: 0
  dB antenna signal: 71dB
▸ RX flags: 0x2608
▾ 802.11 radio information
  PHY type: 802.11b (4)
```

```
  Short preamble: False
  Data rate: 1,0 Mb/s
  Channel: 6
  Frequency: 2437MHz
  Signal strength (dBm): -29dBm
  Noise level (dBm): -100dBm
▾ [Duration: 1464µs]
    [Preamble: 192µs]
▾ 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: 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
  1011 0010 0110 .... = Sequence number: 2854
  Frame check sequence: 0x057e2608 [correct]
  [FCS Status: Good]
▾ IEEE 802.11 wireless LAN
▾ Fixed parameters (12 bytes)
    Timestamp: 0x000000289638e182
    Beacon Interval: 0,102400 [Seconds]
  ▾ Capabilities Information: 0x0601
      .... .... .... ...1 = ESS capabilities: Transmitter is an AP
      .... .... .... ..0. = IBSS status: Transmitter belongs to a BSS
      .... ..1. .... 00.. = CFP participation capabilities: QAP (HC) does not use CFP for delivery of unicast data type frames (0x80)
      .... .... ...0 .... = Privacy: AP/STA cannot support WEP
      .... .... ..0. .... = Short Preamble: Not Allowed
      .... .... .0.. .... = PBCC: Not Allowed
      .... .... 0... .... = Channel Agility: Not in use
      .... ...0 .... .... = Spectrum Management: Not Implemented
      .... .1.. .... .... = Short Slot Time: In use
      .... 0... .... .... = Automatic Power Save Delivery: Not Implemented
      ...0 .... .... .... = Radio Measurement: Not Implemented
      ..0. .... .... .... = DSSS-OFDM: Not Allowed
      .0.. .... .... .... = Delayed Block Ack: Not Implemented
      0... .... .... .... = Immediate Block Ack: Not Implemented
▾ Tagged parameters (119 bytes)
```

```
▾ Tag: SSID parameter set: 30 Munroe St
    Tag Number: SSID parameter set (0)
    Tag length: 12
    SSID: 30 Munroe St
▾ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
    Tag Number: Supported Rates (1)
    Tag length: 4
    Supported Rates: 1(B) (0x82)
    Supported Rates: 2(B) (0x84)
    Supported Rates: 5.5(B) (0x8b)
    Supported Rates: 11(B) (0x96)
▾ Tag: DS Parameter set: Current Channel: 6
    Tag Number: DS Parameter set (3)
    Tag length: 1
    Current Channel: 6
▾ Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    Tag Number: Traffic Indication Map (TIM) (5)
    Tag length: 4
    DTIM count: 0
    DTIM period: 1
  ▾ Bitmap control: 0x00
      .... ...0 = Multicast: False
      0000 000. = Bitmap Offset: 0x00
    Partial Virtual Bitmap: 00
▾ Tag: Country Information: Country Code US, Environment Indoor
    Tag Number: Country Information (7)
```

```
    Tag length: 6
    Code: US
    Environment: Indoor (0x49)
  ▾ Country Info: First Channel Number: 1, Number of Channels: 11, Maximum Transmit Power Level: 26 dBm
      First Channel Number: 1
      Number of Channels: 11
      Maximum Transmit Power Level: 26dBm
▾ Tag: EDCA Parameter Set
    Tag Number: EDCA Parameter Set (12)
    Tag length: 18
  ▾ WME QoS Info: 0x0f
      0... .... = U-APSD: Disabled
      .... 1111 = Parameter Set Count: 0xf
      .000 .... = Reserved: 0x0
    Reserved: 00
  ▾ Ac Parameters ACI 0 (Best Effort), ACM no, AIFSN 3, ECWmin/max 4/10 (CWmin/max 15/1023), TXOP 0
    ▾ ACI / AIFSN Field: 0x03
        .00. .... = ACI: Best Effort (0)
        ...0 .... = Admission Control Mandatory: No
        .... 0011 = AIFSN: 3
        0... .... = Reserved: 0
    ▾ ECW: 0xa4
        1010 .... = ECW Max: 10
        .... 0100 = ECW Min: 4
        CW Max: 1023
        CW Min: 15
```

```
      TXOP Limit: 0
  ▾ Ac Parameters ACI 1 (Background), ACM no, AIFSN 7, ECWmin/max 4/10 (CWmin/max 15/1023), TXOP 0
    ▾ ACI / AIFSN Field: 0x27
        .01. .... = ACI: Background (1)
        ...0 .... = Admission Control Mandatory: No
        .... 0111 = AIFSN: 7
        0... .... = Reserved: 0
    ▾ ECW: 0xa4
        1010 .... = ECW Max: 10
        .... 0100 = ECW Min: 4
        CW Max: 1023
        CW Min: 15
      TXOP Limit: 0
  ▾ Ac Parameters ACI 2 (Video), ACM no, AIFSN 2, ECWmin/max 3/4 (CWmin/max 7/15), TXOP 94
    ▾ ACI / AIFSN Field: 0x42
        .10. .... = ACI: Video (2)
        ...0 .... = Admission Control Mandatory: No
        .... 0010 = AIFSN: 2
        0... .... = Reserved: 0
    ▾ ECW: 0x43
        0100 .... = ECW Max: 4
        .... 0011 = ECW Min: 3
        CW Max: 15
        CW Min: 7
      TXOP Limit: 94
  ▾ Ac Parameters ACI 3 (Voice), ACM no, AIFSN 2, ECWmin/max 2/3 (CWmin/max 3/7), TXOP 47
```

```
    ACI / AIFSN Field: 0x62
        .11. .... = ACI: Voice (3)
        ...0 .... = Admission Control Mandatory: No
        .... 0010 = AIFSN: 2
        0... .... = Reserved: 0
    ECW: 0x32
        0011 .... = ECW Max: 3
        .... 0010 = ECW Min: 2
        CW Max: 7
        CW Min: 3
      TXOP Limit: 47
Tag: ERP Information
    Tag Number: ERP Information (42)
    Tag length: 1
  ERP Information: 0x00
      .... ...0 = Non ERP Present: Not set
      .... ..0. = Use Protection: Not set
      .... .0.. = Barker Preamble Mode: Not set
      0000 0... = Reserved: 0x00
Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    Tag Number: Extended Supported Rates (50)
    Tag length: 8
    Extended Supported Rates: 6(B) (0x8c)
    Extended Supported Rates: 9 (0x12)
    Extended Supported Rates: 12(B) (0x98)
    Extended Supported Rates: 18 (0x24)
```

```
    Extended Supported Rates: 24(B) (0xb0)
    Extended Supported Rates: 36 (0x48)
    Extended Supported Rates: 48 (0x60)
    Extended Supported Rates: 54 (0x6c)
Tag: Vendor Specific: Airgo Networks, Inc.
    Tag Number: Vendor Specific (221)
    Tag length: 21
    OUI: 00:0a:f5 (Airgo Networks, Inc.)
    Vendor Specific OUI Type: 10
    Vendor Specific Data: 0a0240c000030103050e04ff000300110101
Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
    Tag Number: Vendor Specific (221)
    Tag length: 24
    OUI: 00:50:f2 (Microsoft Corp.)
    Vendor Specific OUI Type: 2
    Type: WMM/WME (0x02)
    WME Subtype: Parameter Element (1)
    WME Version: 1
  WME QoS Info: 0x0f
      0... .... = U-APSD: Disabled
      .... 1111 = Parameter Set Count: 0xf
      .000 .... = Reserved: 0x0
    Reserved: 00
  Ac Parameters ACI 0 (Best Effort), ACM no, AIFSN 3, ECWmin/max 4/10 (CWmin/max 15/1023), TXOP 0
    ACI / AIFSN Field: 0x03
        .00. .... = ACI: Best Effort (0)
```

```
        ...0 .... = Admission Control Mandatory: No
        .... 0011 = AIFSN: 3
        0... .... = Reserved: 0
    ECW: 0xa4
        1010 .... = ECW Max: 10
        .... 0100 = ECW Min: 4
        CW Max: 1023
        CW Min: 15
      TXOP Limit: 0
  Ac Parameters ACI 1 (Background), ACM no, AIFSN 7, ECWmin/max 4/10 (CWmin/max 15/1023), TXOP 0
    ACI / AIFSN Field: 0x27
        .01. .... = ACI: Background (1)
        ...0 .... = Admission Control Mandatory: No
        .... 0111 = AIFSN: 7
        0... .... = Reserved: 0
    ECW: 0xa4
        1010 .... = ECW Max: 10
        .... 0100 = ECW Min: 4
        CW Max: 1023
        CW Min: 15
      TXOP Limit: 0
  Ac Parameters ACI 2 (Video), ACM no, AIFSN 2, ECWmin/max 3/4 (CWmin/max 7/15), TXOP 94
    ACI / AIFSN Field: 0x42
        .10. .... = ACI: Video (2)
        ...0 .... = Admission Control Mandatory: No
        .... 0010 = AIFSN: 2
```

```
        0... .... = Reserved: 0
      ECW: 0x43
        0100 .... = ECW Max: 4
        .... 0011 = ECW Min: 3
        CW Max: 15
        CW Min: 7
      TXOP Limit: 94
    Ac Parameters ACI 3 (Voice), ACM no, AIFSN 2, ECWmin/max 2/3 (CWmin/max 3/7), TXOP 47
      ACI / AIFSN Field: 0x62
        .11. .... = ACI: Voice (3)
        ...0 .... = Admission Control Mandatory: No
        .... 0010 = AIFSN: 2
        0... .... = Reserved: 0
      ECW: 0x32
        0011 .... = ECW Max: 3
        .... 0010 = ECW Min: 2
        CW Max: 7
        CW Min: 3
      TXOP Limit: 47
```

Trama Beacon incorrecta

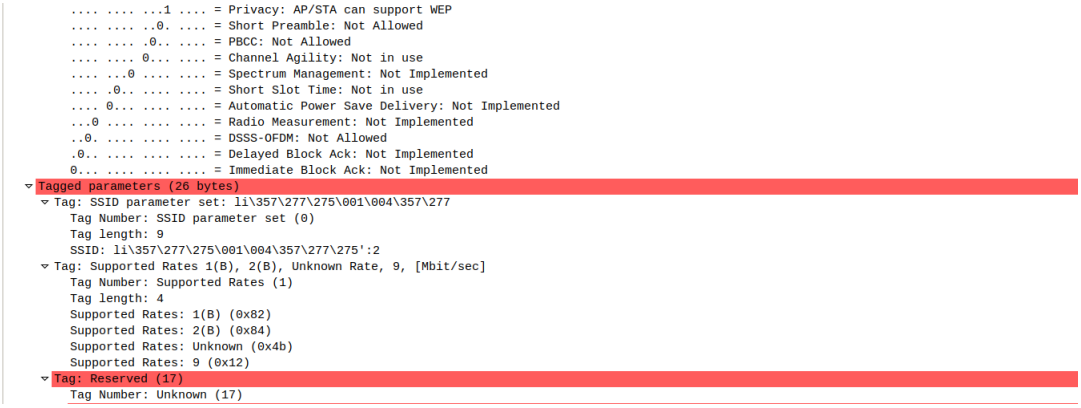
```
Frame 10: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
  Encapsulation type: IEEE 802.11 plus radiotap radio header (23)
  Arrival Time: Jun 29, 2007 04:05:07.366889000 CEST
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1183082707.366889000 seconds
  [Time delta from previous captured frame: 0.004148000 seconds]
  [Time delta from previous displayed frame: 0.004148000 seconds]
  [Time since reference or first frame: 0.294432000 seconds]
  Frame Number: 10
  Frame Length: 90 bytes (720 bits)
  Capture Length: 90 bytes (720 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: radiotap:wlan_radio:wlan]
  [Coloring Rule Name: Checksum Errors]
  [Coloring Rule String [truncated]: eth.fcs.status=="Bad" || ip.checksum.status=="Bad" || tcp.checksum.status=="Bad" || udp.checksum.status=="Bad"
Radiotap Header v0, Length 24
  Header revision: 0
  Header pad: 0
  Header length: 24
  Present flags
    Present flags word: 0x000058ee
      .... .... .... .... .... .... .... ...0 = TSFT: Absent
      .... .... .... .... .... .... .... ..1. = Flags: Present
      .... .... .... .... .... .... .... .1.. = Rate: Present
                                          1... = Channel: Present
```

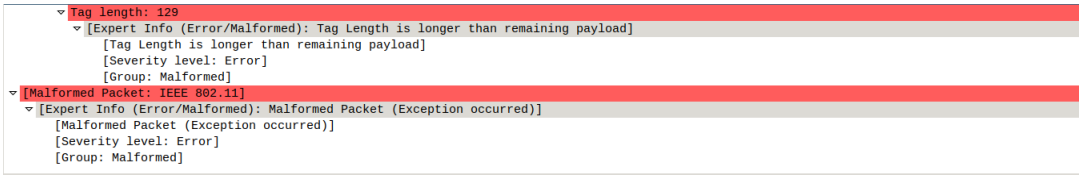
```
      .... .... .... .... .... .... .... 1... = Channel: Present
      .... .... .... .... .... .... ...0 .... = FHSS: Absent
      .... .... .... .... .... .... ..1. .... = dBm Antenna Signal: Present
      .... .... .... .... .... .... .1.. .... = dBm Antenna Noise: Present
      .... .... .... .... .... .... 1... .... = Lock Quality: Present
      .... .... .... .... .... ...0 .... .... = TX Attenuation: Absent
      .... .... .... .... .... ..0. .... .... = dB TX Attenuation: Absent
      .... .... .... .... .... .0.. .... .... = dBm TX Power: Absent
      .... .... .... .... .... 1... .... .... = Antenna: Present
      .... .... .... .... ...1 .... .... .... = dB Antenna Signal: Present
      .... .... .... .... ..0. .... .... .... = dB Antenna Noise: Absent
      .... .... .... .... .1.. .... .... .... = RX flags: Present
      .... .... .... .0.. .... .... .... .... = Channel+: Absent
      .... .... .... 0... .... .... .... .... = MCS information: Absent
      .... .... ...0 .... .... .... .... .... = A-MPDU Status: Absent
      .... .... ..0. .... .... .... .... .... = VHT information: Absent
      .... .... .0.. .... .... .... .... .... = frame timestamp: Absent
      .... .... 0... .... .... .... .... .... = HE information: Absent
      .... ...0 .... .... .... .... .... .... = HE-MU information: Absent
      ...0 000. .... .... .... .... .... .... = Reserved: 0x0
      ..0. .... .... .... .... .... .... .... = Radiotap NS next: False
      .0.. .... .... .... .... .... .... .... = Vendor NS next: False
      0... .... .... .... .... .... .... .... = Ext: Absent
  Flags: 0x10
      .... ...0 = CFP: False
```

```
    .... ..0. = Preamble: Long
    .... .0.. = WEP: False
    .... 0... = Fragmentation: False
    ...1 .... = FCS at end: True
    ..0. .... = Data Pad: False
    .0.. .... = Bad FCS: False
    0... .... = Short GI: False
  Data Rate: 2,0 Mb/s
  Channel frequency: 2437 [BG 6]
▾ Channel flags: 0x00a0, Complementary Code Keying (CCK), 2 GHz spectrum
    .... .... ...0 .... = Turbo: False
    .... .... ..1. .... = Complementary Code Keying (CCK): True
    .... .... .0.. .... = Orthogonal Frequency-Division Multiplexing (OFDM): False
    .... .... 1... .... = 2 GHz spectrum: True
    .... ...0 .... .... = 5 GHz spectrum: False
    .... ..0. .... .... = Passive: False
    .... .0.. .... .... = Dynamic CCK-OFDM: False
    .... 0... .... .... = Gaussian Frequency Shift Keying (GFSK): False
    ...0 .... .... .... = GSM (900MHz): False
    ..0. .... .... .... = Static Turbo: False
    .0.. .... .... .... = Half Rate Channel (10MHz Channel Width): False
    0... .... .... .... = Quarter Rate Channel (5MHz Channel Width): False
  Antenna signal: -94dBm
  Antenna noise: -100dBm
  Signal Quality: 17
```

```
  Antenna: 0
  dB antenna signal: 6dB
▾ RX flags: 0xca4f, Bad PLCP
    .... .... .... .... .... ..1. = Bad PLCP: True
▾ 802.11 radio information
  PHY type: 802.11b (4)
  Short preamble: False
  Data rate: 2,0 Mb/s
  Channel: 6
  Frequency: 2437MHz
  Signal strength (dBm): -94dBm
  Noise level (dBm): -100dBm
▾ [Duration: 456µs]
    [Preamble: 192µs]
▾ IEEE 802.11 Beacon frame, Flags: .........
  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: LinksysG_67:22:94 (00:06:25:67:22:94)
  Source address: LinksysG_67:22:94 (00:06:25:67:22:94)
  BSS Id: LinksysG_67:22:94 (00:06:25:67:22:94)
  .... .... .... 0000 = Fragment number: 0
  1100 0000 0000 .... = Sequence number: 3072
▾ Frame check sequence: 0x01d2ca4f incorrect, should be 0xe146497f
  ▾ [Expert Info (Error/Malformed): Bad checksum [should be 0xe146497f]]
      [Bad checksum [should be 0xe146497f]]
      [Severity level: Error]
      [Group: Malformed]
  [FCS Status: Bad]
▾ IEEE 802.11 wireless LAN
▾ Fixed parameters (12 bytes)
    Timestamp: 0xa000493c059f6318
    Beacon Interval: 0,063488 [Seconds]
  ▾ Capabilities Information: 0x0011
      .... .... .... ...1 = ESS capabilities: Transmitter is an AP
      .... .... .... ..0. = IBSS status: Transmitter belongs to a BSS
      .... ..0. .... 00.. = CFP participation capabilities: No point coordinator at AP (0x00)
```

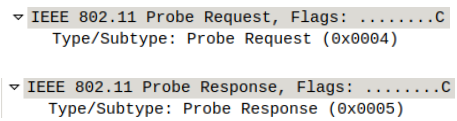




3. Cuestión 2

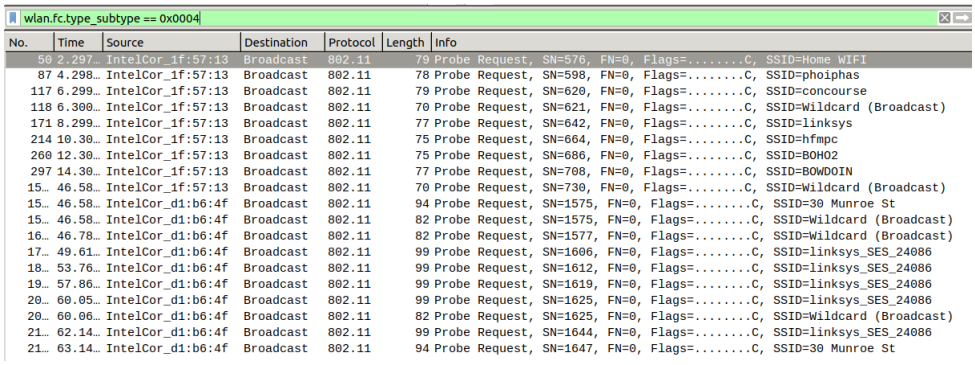
En la captura, ¿hay alguna estación que realice un escaneo activo? ¿Hay APs que respondan? ¿Qué tipos de tramas son? (Consulta e indica el valor de campo tipo)

Sí, se comprueban en las tramas Probe Request para las que escanean activamente y con las tramas Probe Response para las que responden a estos escaneos. Los tipos de tramas son 0 en ambos casos.



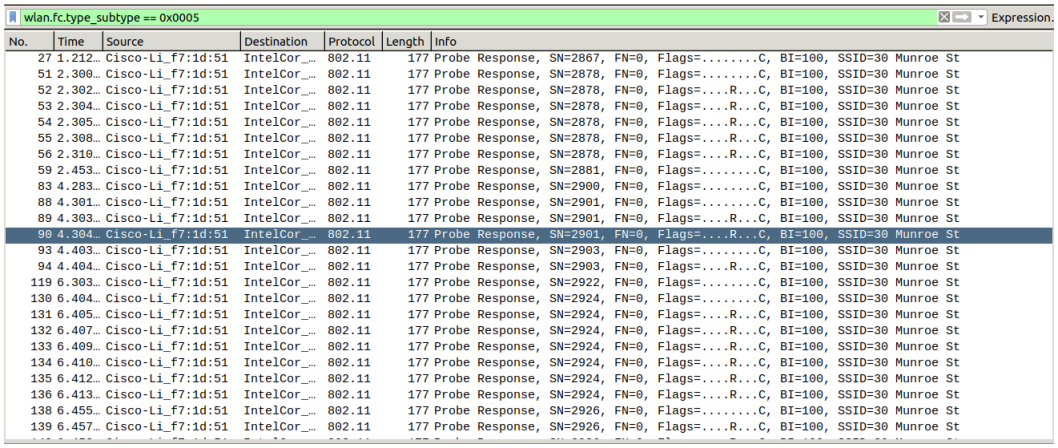
3.1. WLAN_802_11

Las estaciones que escanean son las que se ven en las capturas, y solo una responde, 30 Munroe St.



wlan.fc.type_subtype == 0x0004

No.	Time	Source	Destination	Protocol	Length	Info
50	2.297…	IntelCor_1f:57:13	Broadcast	802.11	79	Probe Request, SN=576, FN=0, Flags=........C, SSID=Home WIFI
87	4.298…	IntelCor_1f:57:13	Broadcast	802.11	78	Probe Request, SN=598, FN=0, Flags=........C, SSID=phoiphas
117	6.299…	IntelCor_1f:57:13	Broadcast	802.11	79	Probe Request, SN=620, FN=0, Flags=........C, SSID=concourse
118	6.300…	IntelCor_1f:57:13	Broadcast	802.11	70	Probe Request, SN=621, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
171	8.299…	IntelCor_1f:57:13	Broadcast	802.11	77	Probe Request, SN=642, FN=0, Flags=........C, SSID=linksys
214	10.30…	IntelCor_1f:57:13	Broadcast	802.11	75	Probe Request, SN=664, FN=0, Flags=........C, SSID=hfmpc
260	12.30…	IntelCor_1f:57:13	Broadcast	802.11	75	Probe Request, SN=686, FN=0, Flags=........C, SSID=BOHO2
297	14.30…	IntelCor_1f:57:13	Broadcast	802.11	77	Probe Request, SN=708, FN=0, Flags=........C, SSID=BOWDOIN
15…	46.58…	IntelCor_1f:57:13	Broadcast	802.11	70	Probe Request, SN=730, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
15…	46.58…	IntelCor_d1:b6:4f	Broadcast	802.11	94	Probe Request, SN=1575, FN=0, Flags=........C, SSID=30 Munroe St
15…	46.58…	IntelCor_d1:b6:4f	Broadcast	802.11	82	Probe Request, SN=1575, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
16…	46.78…	IntelCor_d1:b6:4f	Broadcast	802.11	82	Probe Request, SN=1577, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
17…	49.61…	IntelCor_d1:b6:4f	Broadcast	802.11	99	Probe Request, SN=1606, FN=0, Flags=........C, SSID=linksys_SES_24086
18…	53.76…	IntelCor_d1:b6:4f	Broadcast	802.11	99	Probe Request, SN=1612, FN=0, Flags=........C, SSID=linksys_SES_24086
19…	57.86…	IntelCor_d1:b6:4f	Broadcast	802.11	99	Probe Request, SN=1619, FN=0, Flags=........C, SSID=linksys_SES_24086
20…	60.05…	IntelCor_d1:b6:4f	Broadcast	802.11	99	Probe Request, SN=1625, FN=0, Flags=........C, SSID=linksys_SES_24086
20…	60.06…	IntelCor_d1:b6:4f	Broadcast	802.11	82	Probe Request, SN=1625, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
21…	62.14…	IntelCor_d1:b6:4f	Broadcast	802.11	99	Probe Request, SN=1644, FN=0, Flags=........C, SSID=linksys_SES_24086
21…	63.14…	IntelCor_d1:b6:4f	Broadcast	802.11	94	Probe Request, SN=1647, FN=0, Flags=........C, SSID=30 Munroe St



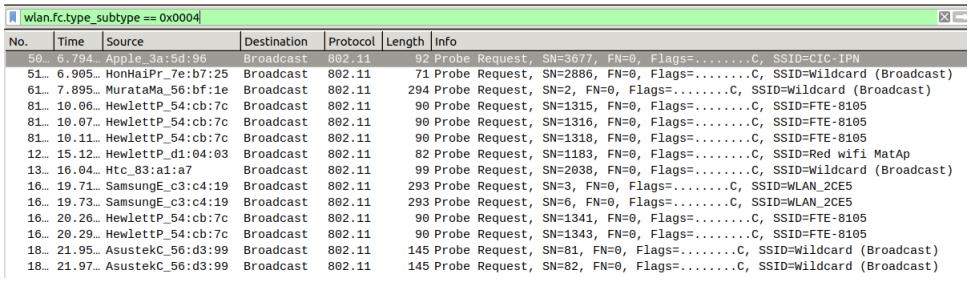
wlan.fc.type_subtype == 0x0005 — Expression…

No.	Time	Source	Destination	Protocol	Length	Info
27	1.212…	Cisco-Li_f7:1d:51	IntelCor_…	802.11	177	Probe Response, SN=2867, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
51	2.300…	Cisco-Li_f7:1d:51	IntelCor_…	802.11	177	Probe Response, SN=2878, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
52	2.302…	Cisco-Li_f7:1d:51	IntelCor_…	802.11	177	Probe Response, SN=2878, FN=0, Flags=....R...C, BI=100, SSID=30 Munroe St
53	2.304…	Cisco-Li_f7:1d:51	IntelCor_…	802.11	177	Probe Response, SN=2878, FN=0, Flags=....R...C, BI=100, SSID=30 Munroe St
54	2.305…	Cisco-Li_f7:1d:51	IntelCor_…	802.11	177	Probe Response, SN=2878, FN=0, Flags=....R...C, BI=100, SSID=30 Munroe St
55	2.308…	Cisco-Li_f7:1d:51	IntelCor_…	802.11	177	Probe Response, SN=2878, FN=0, Flags=....R...C, BI=100, SSID=30 Munroe St
56	2.310…	Cisco-Li_f7:1d:51	IntelCor_…	802.11	177	Probe Response, SN=2878, FN=0, Flags=....R...C, BI=100, SSID=30 Munroe St
59	2.453…	Cisco-Li_f7:1d:51	IntelCor_…	802.11	177	Probe Response, SN=2881, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
83	4.283…	Cisco-Li_f7:1d:51	IntelCor_…	802.11	177	Probe Response, SN=2900, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
88	4.301…	Cisco-Li_f7:1d:51	IntelCor_…	802.11	177	Probe Response, SN=2901, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
89	4.303…	Cisco-Li_f7:1d:51	IntelCor_…	802.11	177	Probe Response, SN=2901, FN=0, Flags=....R...C, BI=100, SSID=30 Munroe St
90	4.304…	Cisco-Li_f7:1d:51	IntelCor_…	802.11	177	Probe Response, SN=2901, FN=0, Flags=....R...C, BI=100, SSID=30 Munroe St
93	4.403…	Cisco-Li_f7:1d:51	IntelCor_…	802.11	177	Probe Response, SN=2903, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
94	4.404…	Cisco-Li_f7:1d:51	IntelCor_…	802.11	177	Probe Response, SN=2903, FN=0, Flags=....R...C, BI=100, SSID=30 Munroe St
119	6.303…	Cisco-Li_f7:1d:51	IntelCor_…	802.11	177	Probe Response, SN=2922, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
130	6.404…	Cisco-Li_f7:1d:51	IntelCor_…	802.11	177	Probe Response, SN=2924, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
131	6.405…	Cisco-Li_f7:1d:51	IntelCor_…	802.11	177	Probe Response, SN=2924, FN=0, Flags=....R...C, BI=100, SSID=30 Munroe St
132	6.407…	Cisco-Li_f7:1d:51	IntelCor_…	802.11	177	Probe Response, SN=2924, FN=0, Flags=....R...C, BI=100, SSID=30 Munroe St
133	6.409…	Cisco-Li_f7:1d:51	IntelCor_…	802.11	177	Probe Response, SN=2924, FN=0, Flags=....R...C, BI=100, SSID=30 Munroe St
134	6.410…	Cisco-Li_f7:1d:51	IntelCor_…	802.11	177	Probe Response, SN=2924, FN=0, Flags=....R...C, BI=100, SSID=30 Munroe St
135	6.412…	Cisco-Li_f7:1d:51	IntelCor_…	802.11	177	Probe Response, SN=2924, FN=0, Flags=....R...C, BI=100, SSID=30 Munroe St
136	6.413…	Cisco-Li_f7:1d:51	IntelCor_…	802.11	177	Probe Response, SN=2924, FN=0, Flags=....R...C, BI=100, SSID=30 Munroe St
138	6.455…	Cisco-Li_f7:1d:51	IntelCor_…	802.11	177	Probe Response, SN=2926, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
139	6.457…	Cisco-Li_f7:1d:51	IntelCor_…	802.11	177	Probe Response, SN=2926, FN=0, Flags=....R...C, BI=100, SSID=30 Munroe St

3.2. WLAN_802_11LOCAL

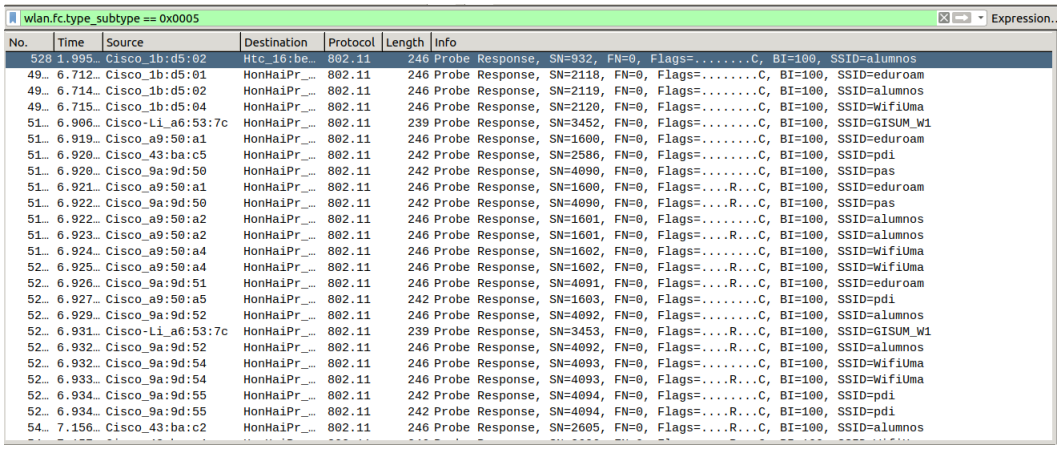
Las estaciones que escanean son las que se ven en las capturas. Para obtener las que responden, realizamos el mismo procedimiento de la primera cuestión, y son:

- alumnos
- eduroam
- WifiUma
- GISUM_W1
- pdi
- pas
- NEO
- ICBWifi



wlan.fc.type_subtype == 0x0004

No.	Time	Source	Destination	Protocol	Length	Info
50…	6.794…	Apple_3a:5d:96	Broadcast	802.11	92	Probe Request, SN=3677, FN=0, Flags=........C, SSID=CIC-IPN
51…	6.905…	HonHaiPr_7e:b7:25	Broadcast	802.11	71	Probe Request, SN=2886, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
61…	7.895…	MurataMa_56:bf:1e	Broadcast	802.11	294	Probe Request, SN=2, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
81…	10.06…	HewlettP_54:cb:7c	Broadcast	802.11	90	Probe Request, SN=1315, FN=0, Flags=........C, SSID=FTE-8105
81…	10.07…	HewlettP_54:cb:7c	Broadcast	802.11	90	Probe Request, SN=1316, FN=0, Flags=........C, SSID=FTE-8105
81…	10.11…	HewlettP_54:cb:7c	Broadcast	802.11	90	Probe Request, SN=1318, FN=0, Flags=........C, SSID=FTE-8105
12…	15.12…	HewlettP_d1:04:03	Broadcast	802.11	82	Probe Request, SN=1183, FN=0, Flags=........C, SSID=Red wifi MatAp
13…	16.04…	Htc_83:a1:a7	Broadcast	802.11	99	Probe Request, SN=2038, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
16…	19.71…	SamsungE_c3:c4:19	Broadcast	802.11	293	Probe Request, SN=3, FN=0, Flags=........C, SSID=WLAN_2CE5
16…	19.73…	SamsungE_c3:c4:19	Broadcast	802.11	293	Probe Request, SN=6, FN=0, Flags=........C, SSID=WLAN_2CE5
16…	20.26…	HewlettP_54:cb:7c	Broadcast	802.11	90	Probe Request, SN=1341, FN=0, Flags=........C, SSID=FTE-8105
16…	20.29…	HewlettP_54:cb:7c	Broadcast	802.11	90	Probe Request, SN=1343, FN=0, Flags=........C, SSID=FTE-8105
18…	21.95…	AsustekC_56:d3:99	Broadcast	802.11	145	Probe Request, SN=81, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
18…	21.97…	AsustekC_56:d3:99	Broadcast	802.11	145	Probe Request, SN=82, FN=0, Flags=........C, SSID=Wildcard (Broadcast)



wlan.fc.type_subtype == 0x0005 Expression…

No.	Time	Source	Destination	Protocol	Length	Info
528	1.995…	Cisco_1b:d5:02	Htc_16:be…	802.11	246	Probe Response, SN=932, FN=0, Flags=........C, BI=100, SSID=alumnos
49…	6.712…	Cisco_1b:d5:01	HonHaiPr_…	802.11	246	Probe Response, SN=2118, FN=0, Flags=........C, BI=100, SSID=eduroam
49…	6.714…	Cisco_1b:d5:02	HonHaiPr_…	802.11	246	Probe Response, SN=2119, FN=0, Flags=........C, BI=100, SSID=alumnos
49…	6.715…	Cisco_1b:d5:04	HonHaiPr_…	802.11	246	Probe Response, SN=2120, FN=0, Flags=........C, BI=100, SSID=WifiUma
51…	6.906…	Cisco-Li_a6:53:7c	HonHaiPr_…	802.11	239	Probe Response, SN=3452, FN=0, Flags=........C, BI=100, SSID=GISUM_W1
51…	6.919…	Cisco_a9:50:a1	HonHaiPr_…	802.11	246	Probe Response, SN=1600, FN=0, Flags=........C, BI=100, SSID=eduroam
51…	6.920…	Cisco_43:ba:c5	HonHaiPr_…	802.11	242	Probe Response, SN=2586, FN=0, Flags=........C, BI=100, SSID=pdi
51…	6.920…	Cisco_9a:9d:50	HonHaiPr_…	802.11	242	Probe Response, SN=4090, FN=0, Flags=........C, BI=100, SSID=pas
51…	6.921…	Cisco_a9:50:a1	HonHaiPr_…	802.11	246	Probe Response, SN=1600, FN=0, Flags=....R...C, BI=100, SSID=eduroam
51…	6.922…	Cisco_9a:9d:50	HonHaiPr_…	802.11	242	Probe Response, SN=4090, FN=0, Flags=....R...C, BI=100, SSID=pas
51…	6.922…	Cisco_a9:50:a2	HonHaiPr_…	802.11	246	Probe Response, SN=1601, FN=0, Flags=........C, BI=100, SSID=alumnos
51…	6.923…	Cisco_a9:50:a2	HonHaiPr_…	802.11	246	Probe Response, SN=1601, FN=0, Flags=....R...C, BI=100, SSID=alumnos
51…	6.924…	Cisco_a9:50:a4	HonHaiPr_…	802.11	246	Probe Response, SN=1602, FN=0, Flags=........C, BI=100, SSID=WifiUma
52…	6.925…	Cisco_a9:50:a4	HonHaiPr_…	802.11	246	Probe Response, SN=1602, FN=0, Flags=....R...C, BI=100, SSID=WifiUma
52…	6.926…	Cisco_9a:9d:51	HonHaiPr_…	802.11	246	Probe Response, SN=4091, FN=0, Flags=....R...C, BI=100, SSID=eduroam
52…	6.927…	Cisco_a9:50:a5	HonHaiPr_…	802.11	242	Probe Response, SN=1603, FN=0, Flags=........C, BI=100, SSID=pdi
52…	6.929…	Cisco_9a:9d:52	HonHaiPr_…	802.11	246	Probe Response, SN=4092, FN=0, Flags=........C, BI=100, SSID=alumnos
52…	6.931…	Cisco-Li_a6:53:7c	HonHaiPr_…	802.11	239	Probe Response, SN=3453, FN=0, Flags=....R...C, BI=100, SSID=GISUM_W1
52…	6.932…	Cisco_9a:9d:52	HonHaiPr_…	802.11	246	Probe Response, SN=4092, FN=0, Flags=....R...C, BI=100, SSID=alumnos
52…	6.932…	Cisco_9a:9d:54	HonHaiPr_…	802.11	246	Probe Response, SN=4093, FN=0, Flags=........C, BI=100, SSID=WifiUma
52…	6.933…	Cisco_9a:9d:54	HonHaiPr_…	802.11	246	Probe Response, SN=4093, FN=0, Flags=....R...C, BI=100, SSID=WifiUma
52…	6.934…	Cisco_9a:9d:55	HonHaiPr_…	802.11	242	Probe Response, SN=4094, FN=0, Flags=........C, BI=100, SSID=pdi
52…	6.934…	Cisco_9a:9d:55	HonHaiPr_…	802.11	242	Probe Response, SN=4094, FN=0, Flags=....R...C, BI=100, SSID=pdi
54…	7.156…	Cisco_43:ba:c2	HonHaiPr_…	802.11	246	Probe Response, SN=2605, FN=0, Flags=....R...C, BI=100, SSID=alumnos

4. Ejercicio 2

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

51…	6.905…	HonHaiPr_7e:b7:25	Broadcast	802.11	71	Probe Request, SN=2886, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
51…	6.906…	Cisco-Li_a6:53:7c	HonHaiPr_…	802.11	239	Probe Response, SN=3452, FN=0, Flags=........C, BI=100, SSID=GISUM_W1

Probe Request

```
Frame 5187: 71 bytes on wire (568 bits), 71 bytes captured (568 bits)
    Encapsulation type: IEEE 802.11 plus radiotap radio header (23)
    Arrival Time: Oct 29, 2012 09:57:01.043582000 CET
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1351501021.043582000 seconds
    [Time delta from previous captured frame: 0.001135000 seconds]
    [Time delta from previous displayed frame: 0.110986000 seconds]
    [Time since reference or first frame: 6.905003000 seconds]
    Frame Number: 5187
    Frame Length: 71 bytes (568 bits)
    Capture Length: 71 bytes (568 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: radiotap:wlan_radio:wlan]
Radiotap Header v0, Length 25
    Header revision: 0
    Header pad: 0
    Header length: 25
  Present flags
    Present flags word: 0x0000086f
        .... .... .... .... .... .... .... ...1 = TSFT: Present
        .... .... .... .... .... .... .... ..1. = Flags: Present
        .... .... .... .... .... .... .... .1.. = Rate: Present
        .... .... .... .... .... .... .... 1... = Channel: Present
        .... .... .... .... .... .... ...0 .... = FHSS: Absent
        .... .... .... .... .... .... ..1. .... = dBm Antenna Signal: Present
                                          1      = dBm Antenna Noise: Present
```

```
        .... .... .... .... .... .... .1.. .... = dBm Antenna Noise: Present
        .... .... .... .... .... .... 0... .... = Lock Quality: Absent
        .... .... .... .... .... ...0 .... .... = TX Attenuation: Absent
        .... .... .... .... .... ..0. .... .... = dB TX Attenuation: Absent
        .... .... .... .... .... .0.. .... .... = dBm TX Power: Absent
        .... .... .... .... .... 1... .... .... = Antenna: Present
        .... .... .... .... ...0 .... .... .... = dB Antenna Signal: Absent
        .... .... .... .... ..0. .... .... .... = dB Antenna Noise: Absent
        .... .... .... .... .0.. .... .... .... = RX flags: Absent
        .... .... .... .0.. .... .... .... .... = Channel+: Absent
        .... .... .... 0... .... .... .... .... = MCS information: Absent
        .... .... ...0 .... .... .... .... .... = A-MPDU Status: Absent
        .... .... ..0. .... .... .... .... .... = VHT information: Absent
        .... .... .0.. .... .... .... .... .... = frame timestamp: Absent
        .... .... 0... .... .... .... .... .... = HE information: Absent
        .... ...0 .... .... .... .... .... .... = HE-MU information: Absent
        ...0 000. .... .... .... .... .... .... = Reserved: 0x0
        ..0. .... .... .... .... .... .... .... = Radiotap NS next: False
        .0.. .... .... .... .... .... .... .... = Vendor NS next: False
        0... .... .... .... .... .... .... .... = Ext: Absent
    MAC timestamp: 4224383902
  Flags: 0x10
      .... ...0 = CFP: False
      .... ..0. = Preamble: Long
      .... .0.. = WEP: False
      .... 0... = Fragmentation: False
```

```
      ...1 .... = FCS at end: True
      ..0. .... = Data Pad: False
      .0.. .... = Bad FCS: False
      0... .... = Short GI: False
    Data Rate: 1,0 Mb/s
    Channel frequency: 2412 [BG 1]
  Channel flags: 0x0080, 2 GHz spectrum
      .... .... ...0 .... = Turbo: False
      .... .... ..0. .... = Complementary Code Keying (CCK): False
      .... .... .0.. .... = Orthogonal Frequency-Division Multiplexing (OFDM): False
      .... .... 1... .... = 2 GHz spectrum: True
      .... ...0 .... .... = 5 GHz spectrum: False
      .... ..0. .... .... = Passive: False
      .... .0.. .... .... = Dynamic CCK-OFDM: False
      .... 0... .... .... = Gaussian Frequency Shift Keying (GFSK): False
      ...0 .... .... .... = GSM (900MHz): False
      ..0. .... .... .... = Static Turbo: False
      .0.. .... .... .... = Half Rate Channel (10MHz Channel Width): False
      0... .... .... .... = Quarter Rate Channel (5MHz Channel Width): False
    Antenna signal: -84dBm
    Antenna noise: -89dBm
    Antenna: 0
802.11 radio information
    PHY type: 802.11 DSSS (3)
    Data rate: 1,0 Mb/s
    Channel: 1
```

```
    Frequency: 2412MHz
    Signal strength (dBm): -84dBm
    Noise level (dBm): -89dBm
    TSF timestamp: 4224383902
▾ IEEE 802.11 Probe Request, Flags: ........C
    Type/Subtype: Probe Request (0x0004)
  ▾ Frame Control Field: 0x4000
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      0100 .... = Subtype: 4
    ▾ 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: HonHaiPr_7e:b7:25 (c0:18:85:7e:b7:25)
    Source address: HonHaiPr_7e:b7:25 (c0:18:85:7e:b7:25)
    BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
    .... .... .... 0000 = Fragment number: 0
    1011 0100 0110 .... = Sequence number: 2886
```

```
    Frame check sequence: 0xddb5c5f9 [correct]
    [FCS Status: Good]
▾ IEEE 802.11 wireless LAN
  ▾ Tagged parameters (18 bytes)
    ▾ Tag: SSID parameter set: Wildcard SSID
        Tag Number: SSID parameter set (0)
        Tag length: 0
        SSID:
    ▾ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6, 9, 12, 18, [Mbit/sec]
        Tag Number: Supported Rates (1)
        Tag length: 8
        Supported Rates: 1(B) (0x82)
        Supported Rates: 2(B) (0x84)
        Supported Rates: 5.5(B) (0x8b)
        Supported Rates: 11(B) (0x96)
        Supported Rates: 6 (0x0c)
        Supported Rates: 9 (0x12)
        Supported Rates: 12 (0x18)
        Supported Rates: 18 (0x24)
    ▾ Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
        Tag Number: Extended Supported Rates (50)
        Tag length: 4
        Extended Supported Rates: 24 (0x30)
        Extended Supported Rates: 36 (0x48)
        Extended Supported Rates: 48 (0x60)
        Extended Supported Rates: 54 (0x6c)
```

```
    ▾ Tag: DS Parameter set: Current Channel: 2
        Tag Number: DS Parameter set (3)
        Tag length: 1
        Current Channel: 2
    ▾ Tag: Vendor Specific: Broadcom
        Tag Number: Vendor Specific (221)
        Tag length: 9
        OUI: 00:10:18 (Broadcom)
        Vendor Specific OUI Type: 2
        Vendor Specific Data: 020000000000
```

Probe Response

```
Frame 5188: 239 bytes on wire (1912 bits), 239 bytes captured (1912 bits)
    Encapsulation type: IEEE 802.11 plus radiotap radio header (23)
    Arrival Time: Oct 29, 2012 09:57:01.045562000 CET
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1351501021.045562000 seconds
    [Time delta from previous captured frame: 0.001980000 seconds]
    [Time delta from previous displayed frame: 0.001980000 seconds]
    [Time since reference or first frame: 6.906983000 seconds]
    Frame Number: 5188
    Frame Length: 239 bytes (1912 bits)
    Capture Length: 239 bytes (1912 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: radiotap:wlan_radio:wlan]
Radiotap Header v0, Length 25
    Header revision: 0
    Header pad: 0
    Header length: 25
  Present flags
    Present flags word: 0x0000086f
        .... .... .... .... .... .... .... ...1 = TSFT: Present
        .... .... .... .... .... .... .... ..1. = Flags: Present
        .... .... .... .... .... .... .... .1.. = Rate: Present
        .... .... .... .... .... .... .... 1... = Channel: Present
        .... .... .... .... .... .... ...0 .... = FHSS: Absent
        .... .... .... .... .... .... ..1. .... = dBm Antenna Signal: Present
```

```
        .... .... .... .... .... .... .1.. .... = dBm Antenna Noise: Present
        .... .... .... .... .... .... 0... .... = Lock Quality: Absent
        .... .... .... .... .... ...0 .... .... = TX Attenuation: Absent
        .... .... .... .... .... ..0. .... .... = dB TX Attenuation: Absent
        .... .... .... .... .... .0.. .... .... = dBm TX Power: Absent
        .... .... .... .... .... 1... .... .... = Antenna: Present
        .... .... .... .... ...0 .... .... .... = dB Antenna Signal: Absent
        .... .... .... .... ..0. .... .... .... = dB Antenna Noise: Absent
        .... .... .... .... .0.. .... .... .... = RX flags: Absent
        .... .... .... .0.. .... .... .... .... = Channel+: Absent
        .... .... .... 0... .... .... .... .... = MCS information: Absent
        .... .... ...0 .... .... .... .... .... = A-MPDU Status: Absent
        .... .... ..0. .... .... .... .... .... = VHT information: Absent
        .... .... .0.. .... .... .... .... .... = frame timestamp: Absent
        .... .... 0... .... .... .... .... .... = HE information: Absent
        .... ...0 .... .... .... .... .... .... = HE-MU information: Absent
        ...0 000. .... .... .... .... .... .... = Reserved: 0x0
        ..0. .... .... .... .... .... .... .... = Radiotap NS next: False
        .0.. .... .... .... .... .... .... .... = Vendor NS next: False
        0... .... .... .... .... .... .... .... = Ext: Absent
    MAC timestamp: 4224384492
  Flags: 0x10
      .... ...0 = CFP: False
      .... ..0. = Preamble: Long
      .... .0.. = WEP: False
      .... 0... = Fragmentation: False
```

```
      ...1 .... = FCS at end: True
      ..0. .... = Data Pad: False
      .0.. .... = Bad FCS: False
      0... .... = Short GI: False
    Data Rate: 1,0 Mb/s
    Channel frequency: 2412 [BG 1]
  Channel flags: 0x0080, 2 GHz spectrum
      .... .... ...0 .... = Turbo: False
      .... .... ..0. .... = Complementary Code Keying (CCK): False
      .... .... .0.. .... = Orthogonal Frequency-Division Multiplexing (OFDM): False
      .... .... 1... .... = 2 GHz spectrum: True
      .... ...0 .... .... = 5 GHz spectrum: False
      .... ..0. .... .... = Passive: False
      .... .0.. .... .... = Dynamic CCK-OFDM: False
      .... 0... .... .... = Gaussian Frequency Shift Keying (GFSK): False
      ...0 .... .... .... = GSM (900MHz): False
      ..0. .... .... .... = Static Turbo: False
      .0.. .... .... .... = Half Rate Channel (10MHz Channel Width): False
      0... .... .... .... = Quarter Rate Channel (5MHz Channel Width): False
    Antenna signal: -67dBm
    Antenna noise: -89dBm
    Antenna: 0
802.11 radio information
    PHY type: 802.11 DSSS (3)
    Data rate: 1,0 Mb/s
    Channel: 1
```

```
    Frequency: 2412MHz
    Signal strength (dBm): -67dBm
    Noise level (dBm): -89dBm
    TSF timestamp: 4224384492
▾ IEEE 802.11 Probe Response, Flags: ........C
    Type/Subtype: Probe Response (0x0005)
  ▾ Frame Control Field: 0x5000
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      0101 .... = Subtype: 5
    ▾ 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 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: HonHaiPr_7e:b7:25 (c0:18:85:7e:b7:25)
    Destination address: HonHaiPr_7e:b7:25 (c0:18:85:7e:b7:25)
    Transmitter address: Cisco-Li_a6:53:7c (00:23:69:a6:53:7c)
    Source address: Cisco-Li_a6:53:7c (00:23:69:a6:53:7c)
    BSS Id: Cisco-Li_a6:53:7c (00:23:69:a6:53:7c)
    .... .... .... 0000 = Fragment number: 0
    1101 0111 1100 .... = Sequence number: 3452
```

```
    Frame check sequence: 0x4aa5a95b [correct]
    [FCS Status: Good]
▾ IEEE 802.11 wireless LAN
  ▾ Fixed parameters (12 bytes)
      Timestamp: 0x000007d2d647c9fc
      Beacon Interval: 0,102400 [Seconds]
    ▾ Capabilities Information: 0x0411
        .... .... .... ...1 = ESS capabilities: Transmitter is an AP
        .... .... .... ..0. = IBSS status: Transmitter belongs to a BSS
        .... ..0. .... 00.. = CFP participation capabilities: No point coordinator at AP (0x00)
        .... .... ...1 .... = Privacy: AP/STA can support WEP
        .... .... ..0. .... = Short Preamble: Not Allowed
        .... .... .0.. .... = PBCC: Not Allowed
        .... .... 0... .... = Channel Agility: Not in use
        .... ...0 .... .... = Spectrum Management: Not Implemented
        .... .1.. .... .... = Short Slot Time: In use
        .... 0... .... .... = Automatic Power Save Delivery: Not Implemented
        ...0 .... .... .... = Radio Measurement: Not Implemented
        ..0. .... .... .... = DSSS-OFDM: Not Allowed
        .0.. .... .... .... = Delayed Block Ack: Not Implemented
        0... .... .... .... = Immediate Block Ack: Not Implemented
  ▾ Tagged parameters (174 bytes)
    ▾ Tag: SSID parameter set: GISUM_W1
        Tag Number: SSID parameter set (0)
        Tag length: 8
        SSID: GISUM_W1
    ▾ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 18, 24, 36, 54, [Mbit/sec]
        Tag Number: Supported Rates (1)
        Tag length: 8
        Supported Rates: 1(B) (0x82)
        Supported Rates: 2(B) (0x84)
        Supported Rates: 5.5(B) (0x8b)
        Supported Rates: 11(B) (0x96)
        Supported Rates: 18 (0x24)
        Supported Rates: 24 (0x30)
        Supported Rates: 36 (0x48)
        Supported Rates: 54 (0x6c)
    ▾ Tag: DS Parameter set: Current Channel: 1
        Tag Number: DS Parameter set (3)
        Tag length: 1
        Current Channel: 1
    ▾ Tag: ERP Information
        Tag Number: ERP Information (42)
        Tag length: 1
      ▾ ERP Information: 0x04
          .... ...0 = Non ERP Present: Not set
          .... ..0. = Use Protection: Not set
          .... .1.. = Barker Preamble Mode: Set
          0000 0... = Reserved: 0x00
    ▾ Tag: ERP Information
        Tag Number: ERP Information (47)
        Tag length: 1
```

```
    ERP Information: 0x04
        .... ...0 = Non ERP Present: Not set
        .... ..0. = Use Protection: Not set
        .... .1.. = Barker Preamble Mode: Set
        0000 0... = Reserved: 0x00
  Tag: Extended Supported Rates 6, 9, 12, 48, [Mbit/sec]
    Tag Number: Extended Supported Rates (50)
    Tag length: 4
    Extended Supported Rates: 6 (0x0c)
    Extended Supported Rates: 9 (0x12)
    Extended Supported Rates: 12 (0x18)
    Extended Supported Rates: 48 (0x60)
  Tag: Vendor Specific: Microsoft Corp.: WPS
    Tag Number: Vendor Specific (221)
    Tag length: 126
    OUI: 00:50:f2 (Microsoft Corp.)
    Vendor Specific OUI Type: 4
    Type: WPS (0x04)
    Version: 0x10
        Data Element Type: Version (0x104a)
        Data Element Length: 1
        Version: 0x10
    Wifi Protected Setup State: Configured (0x02)
        Data Element Type: Wifi Protected Setup State (0x1044)
        Data Element Length: 1
        Wifi Protected Setup State: Configured (0x02)
```

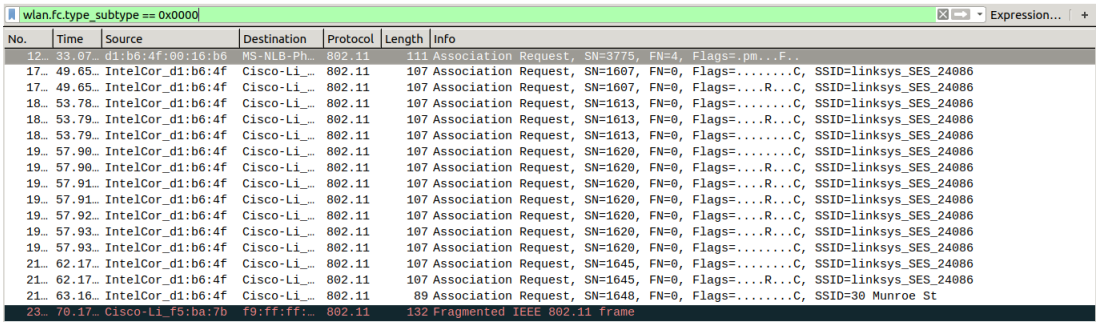
```
    Response Type: AP (0x03)
        Data Element Type: Response Type (0x103b)
        Data Element Length: 1
        Response Type: AP (0x03)
    UUID E
        Data Element Type: UUID E (0x1047)
        Data Element Length: 16
        UUID Enrollee: 138140001dd211b29fffc67e816b4bfb
    Manufacturer: Linksys
        Data Element Type: Manufacturer (0x1021)
        Data Element Length: 7
        Manufacturer: Linksys
    Model Name: Router
        Data Element Type: Model Name (0x1023)
        Data Element Length: 6
        Model Name: Router
    Model Number: WRT54G2
        Data Element Type: Model Number (0x1024)
        Data Element Length: 7
        Model Number: WRT54G2
    Serial Number: CSV01J4F1673
        Data Element Type: Serial Number (0x1042)
        Data Element Length: 12
        Serial Number: CSV01J4F1673
    Primary Device Type
        Data Element Type: Primary Device Type (0x1054)
```

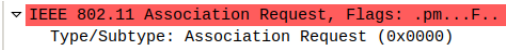
```
        Data Element Length: 8
        Primary Device Type: 00060050f2040001
        Category: Network Infrastructure (0x0006)
        Subcategory: AP (0x0001)
    Device Name: Wireless-G Router
        Data Element Type: Device Name (0x1011)
        Data Element Length: 17
        Device Name: Wireless-G Router
    Config Methods: 0x0084
        Data Element Type: Config Methods (0x1008)
        Data Element Length: 2
        Configuration Methods: 0x0084
        .... .... .... ...0 = USB: 0x0
        .... .... .... ..0. = Ethernet: 0x0
        .... .... .... .1.. = Label: 0x1
        .... .... .... 0... = Display: 0x0
        ..0. .... .... .... = Virtual Display: 0x0
        .0.. .... .... .... = Physical Display: 0x0
        .... .... ...0 .... = External NFC: 0x0
        .... .... ..0. .... = Internal NFC: 0x0
        .... .... .0.. .... = NFC Interface: 0x0
        .... .... 1... .... = Push Button: 0x1
        .... ..0. .... .... = Virtual Push Button: 0x0
        .... .0.. .... .... = Physical Push Button: 0x0
        .... ...0 .... .... = Keypad: 0x0
  Tag: Vendor Specific: Broadcom
```

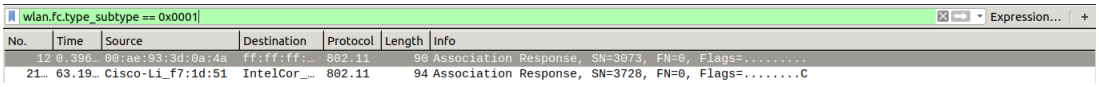
```
        Tag Number: Vendor Specific (221)
        Tag length: 9
        OUI: 00:10:18 (Broadcom)
        Vendor Specific OUI Type: 2
        Vendor Specific Data: 0200f4000000
```

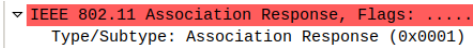
5. Cuestión 3

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)









6. Ejercicio 3

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

Petición de asociación

```
▾ Frame 2162: 89 bytes on wire (712 bits), 89 bytes captured (712 bits)
    Encapsulation type: IEEE 802.11 plus radiotap radio header (23)
    Arrival Time: Jun 29, 2007 04:06:10.242367000 CEST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1183082770.242367000 seconds
    [Time delta from previous captured frame: 0.000096000 seconds]
    [Time delta from previous displayed frame: 0.991716000 seconds]
    [Time since reference or first frame: 63.169910000 seconds]
    Frame Number: 2162
    Frame Length: 89 bytes (712 bits)
    Capture Length: 89 bytes (712 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: radiotap:wlan_radio:wlan]
▾ Radiotap Header v0, Length 24
    Header revision: 0
    Header pad: 0
    Header length: 24
  ▾ Present flags
    ▾ Present flags word: 0x000058ee
        .... .... .... .... .... .... .... ...0 = TSFT: Absent
        .... .... .... .... .... .... .... ..1. = Flags: Present
        .... .... .... .... .... .... .... .1.. = Rate: Present
        .... .... .... .... .... .... .... 1... = Channel: Present
        .... .... .... .... .... .... ...0 .... = FHSS: Absent
        .... .... .... .... .... .... ..1. .... = dBm Antenna Signal: Present
```

```
        .... .... .... .... .... .... .1.. .... = dBm Antenna Noise: Present
        .... .... .... .... .... .... 1... .... = Lock Quality: Present
        .... .... .... .... .... ...0 .... .... = TX Attenuation: Absent
        .... .... .... .... .... ..0. .... .... = dB TX Attenuation: Absent
        .... .... .... .... .... .0.. .... .... = dBm TX Power: Absent
        .... .... .... .... .... 1... .... .... = Antenna: Present
        .... .... .... .... ...1 .... .... .... = dB Antenna Signal: Present
        .... .... .... .... ..0. .... .... .... = dB Antenna Noise: Absent
        .... .... .... .... .1.. .... .... .... = RX flags: Present
        .... .... .... .0.. .... .... .... .... = Channel+: Absent
        .... .... .... 0... .... .... .... .... = MCS information: Absent
        .... .... ...0 .... .... .... .... .... = A-MPDU Status: Absent
        .... .... ..0. .... .... .... .... .... = VHT information: Absent
        .... .... .0.. .... .... .... .... .... = frame timestamp: Absent
        .... .... 0... .... .... .... .... .... = HE information: Absent
        .... ...0 .... .... .... .... .... .... = HE-MU information: Absent
        ...0 000. .... .... .... .... .... .... = Reserved: 0x0
        ..0. .... .... .... .... .... .... .... = Radiotap NS next: False
        .0.. .... .... .... .... .... .... .... = Vendor NS next: False
        0... .... .... .... .... .... .... .... = Ext: Absent
  ▾ Flags: 0x10
      .... ...0 = CFP: False
      .... ..0. = Preamble: Long
      .... .0.. = WEP: False
      .... 0... = Fragmentation: False
      ...1 .... = FCS at end: True
```

```
      ..0. .... = Data Pad: False
      .0.. .... = Bad FCS: False
      0... .... = Short GI: False
    Data Rate: 54,0 Mb/s
    Channel frequency: 2437 [BG 6]
  ▾ Channel flags: 0x00c0, Orthogonal Frequency-Division Multiplexing (OFDM), 2 GHz spectrum
      .... .... ...0 .... = Turbo: False
      .... .... ..0. .... = Complementary Code Keying (CCK): False
      .... .... .1.. .... = Orthogonal Frequency-Division Multiplexing (OFDM): True
      .... .... 1... .... = 2 GHz spectrum: True
      .... ...0 .... .... = 5 GHz spectrum: False
      .... ..0. .... .... = Passive: False
      .... .0.. .... .... = Dynamic CCK-OFDM: False
      .... 0... .... .... = Gaussian Frequency Shift Keying (GFSK): False
      ...0 .... .... .... = GSM (900MHz): False
      ..0. .... .... .... = Static Turbo: False
      .0.. .... .... .... = Half Rate Channel (10MHz Channel Width): False
      0... .... .... .... = Quarter Rate Channel (5MHz Channel Width): False
    Antenna signal: -29dBm
    Antenna noise: -100dBm
    Signal Quality: 100
    Antenna: 0
    dB antenna signal: 71dB
  ▾ RX flags: 0xadc6, Bad PLCP
      .... .... .... .... .... ..1. = Bad PLCP: True
▾ 802.11 radio information
```

```
    PHY type: 802.11g (6)
    Short preamble: False
    Proprietary mode: None (0)
    Data rate: 54,0 Mb/s
    Channel: 6
    Frequency: 2437MHz
    Signal strength (dBm): -29dBm
    Noise level (dBm): -100dBm
  ▽ [Duration: 32µs]
      [Preamble: 20µs]
▽ 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
        .... ..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 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 [correct]
    [FCS Status: Good]
▽ IEEE 802.11 wireless LAN
  ▽ Fixed parameters (4 bytes)
    ▽ Capabilities Information: 0xce01
        .... .... .... ...1 = ESS capabilities: Transmitter is an AP
        .... .... .... ..0. = IBSS status: Transmitter belongs to a BSS
        .... ..1. .... 00.. = CFP participation capabilities: QAP (HC) does not use CFP for delivery of unicast data type frames (0x80)
        .... .... ...0 .... = Privacy: AP/STA cannot support WEP
        .... .... ..0. .... = Short Preamble: Not Allowed
        .... .... .0.. .... = PBCC: Not Allowed
        .... .... 0... .... = Channel Agility: Not in use
        .... ...0 .... .... = Spectrum Management: Not Implemented
        .... .1.. .... .... = Short Slot Time: In use
        .... 1... .... .... = Automatic Power Save Delivery: Implemented
        ...0 .... .... .... = Radio Measurement: Not Implemented
        ..0. .... .... .... = DSSS-OFDM: Not Allowed
        .1.. .... .... .... = Delayed Block Ack: Implemented
        1... .... .... .... = Immediate Block Ack: Implemented
      Listen Interval: 0x000a
```

```
  ▽ Tag: SSID parameter set: 30 Munroe St
      Tag Number: SSID parameter set (0)
      Tag length: 12
      SSID: 30 Munroe St
  ▽ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18, [Mbit/sec]
      Tag Number: Supported Rates (1)
      Tag length: 8
      Supported Rates: 1(B) (0x82)
      Supported Rates: 2(B) (0x84)
      Supported Rates: 5.5(B) (0x8b)
      Supported Rates: 11(B) (0x96)
      Supported Rates: 6(B) (0x8c)
      Supported Rates: 9 (0x12)
      Supported Rates: 12(B) (0x98)
      Supported Rates: 18 (0x24)
  ▽ Tag: QoS Capability
      Tag Number: QoS Capability (46)
      Tag length: 1
    ▽ QoS Information (STA): 0x00
        .... ...0 = AC_VO U-APSD Flag: Neither Trigger-enabled nor Delivery-enabled
        .... ..0. = AC_VI U-APSD Flag: Neither Trigger-enabled nor Delivery-enabled
        .... .0.. = AC_BK U-APSD Flag: Neither Trigger-enabled nor Delivery-enabled
        .... 0... = AC_BE U-APSD Flag: Neither Trigger-enabled nor Delivery-enabled
        ...0 .... = Q-Ack: STAs MIB attribute dot11QAckOptionImplemented is false
        .00. .... = Max SP Length: AP may deliver all buffered MSDUs, A-MSDUs and MMPDUs (0x0)
        0... .... = More Data Ack: STA cannot process ACK frames with the More Data bit in the Frame Control field set to 1
```

```
    Tag Number: Extended Supported Rates (50)
    Tag length: 4
    Extended Supported Rates: 24(B) (0xb0)
    Extended Supported Rates: 36 (0x48)
    Extended Supported Rates: 48 (0x60)
    Extended Supported Rates: 54 (0x6c)
```

Respuesta

```
Frame 2166: 94 bytes on wire (752 bits), 94 bytes captured (752 bits)
  Encapsulation type: IEEE 802.11 plus radiotap radio header (23)
  Arrival Time: Jun 29, 2007 04:06:10.264558000 CEST
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1183082770.264558000 seconds
  [Time delta from previous captured frame: 0.021101000 seconds]
  [Time delta from previous displayed frame: 0.022191000 seconds]
  [Time since reference or first frame: 63.192101000 seconds]
  Frame Number: 2166
  Frame Length: 94 bytes (752 bits)
  Capture Length: 94 bytes (752 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: radiotap:wlan_radio:wlan]
Radiotap Header v0, Length 24
  Header revision: 0
  Header pad: 0
  Header length: 24
  Present flags
    Present flags word: 0x000058ee
      .... .... .... .... .... .... .... ...0 = TSFT: Absent
      .... .... .... .... .... .... .... ..1. = Flags: Present
      .... .... .... .... .... .... .... .1.. = Rate: Present
      .... .... .... .... .... .... .... 1... = Channel: Present
      .... .... .... .... .... .... ...0 .... = FHSS: Absent
      .... .... .... .... .... .... ..1. .... = dBm Antenna Signal: Present
```

```
      .... .... .... .... .... .... .1.. .... = dBm Antenna Noise: Present
      .... .... .... .... .... .... 1... .... = Lock Quality: Present
      .... .... .... .... .... ...0 .... .... = TX Attenuation: Absent
      .... .... .... .... .... ..0. .... .... = dB TX Attenuation: Absent
      .... .... .... .... .... .0.. .... .... = dBm TX Power: Absent
      .... .... .... .... .... 1... .... .... = Antenna: Present
      .... .... .... .... ...1 .... .... .... = dB Antenna Signal: Present
      .... .... .... .... ..0. .... .... .... = dB Antenna Noise: Absent
      .... .... .... .... .1.. .... .... .... = RX flags: Present
      .... .... .... .0.. .... .... .... .... = Channel+: Absent
      .... .... .... 0... .... .... .... .... = MCS information: Absent
      .... .... ...0 .... .... .... .... .... = A-MPDU Status: Absent
      .... .... ..0. .... .... .... .... .... = VHT information: Absent
      .... .... .0.. .... .... .... .... .... = frame timestamp: Absent
      .... .... 0... .... .... .... .... .... = HE information: Absent
      .... ...0 .... .... .... .... .... .... = HE-MU information: Absent
      ...0 000. .... .... .... .... .... .... = Reserved: 0x0
      ..0. .... .... .... .... .... .... .... = Radiotap NS next: False
      .0.. .... .... .... .... .... .... .... = Vendor NS next: False
      0... .... .... .... .... .... .... .... = Ext: Absent
  Flags: 0x10
    .... ...0 = CFP: False
    .... ..0. = Preamble: Long
    .... .0.. = WEP: False
    .... 0... = Fragmentation: False
    ...1 .... = FCS at end: True
```

```
    ..0. .... = Data Pad: False
    .0.. .... = Bad FCS: False
    0... .... = Short GI: False
  Data Rate: 1,0 Mb/s
  Channel frequency: 2437 [BG 6]
▾ Channel flags: 0x00a0, Complementary Code Keying (CCK), 2 GHz spectrum
    .... .... ...0 .... = Turbo: False
    .... .... ..1. .... = Complementary Code Keying (CCK): True
    .... .... .0.. .... = Orthogonal Frequency-Division Multiplexing (OFDM): False
    .... .... 1... .... = 2 GHz spectrum: True
    .... ...0 .... .... = 5 GHz spectrum: False
    .... ..0. .... .... = Passive: False
    .... .0.. .... .... = Dynamic CCK-OFDM: False
    .... 0... .... .... = Gaussian Frequency Shift Keying (GFSK): False
    ...0 .... .... .... = GSM (900MHz): False
    ..0. .... .... .... = Static Turbo: False
    .0.. .... .... .... = Half Rate Channel (10MHz Channel Width): False
    0... .... .... .... = Quarter Rate Channel (5MHz Channel Width): False
  Antenna signal: -31dBm
  Antenna noise: -100dBm
  Signal Quality: 100
  Antenna: 0
  dB antenna signal: 69dB
▾ RX flags: 0xab2b, Bad PLCP
    .... .... .... .... .... ..1. = Bad PLCP: True
▾ 802.11 radio information
```

```
  PHY type: 802.11b (4)
  Short preamble: False
  Data rate: 1,0 Mb/s
  Channel: 6
  Frequency: 2437MHz
  Signal strength (dBm): -31dBm
  Noise level (dBm): -100dBm
▾ [Duration: 752µs]
    [Preamble: 192µs]
▾ 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
      .... ..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 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]
▾ IEEE 802.11 wireless LAN
▾ Fixed parameters (6 bytes)
  ▾ Capabilities Information: 0x0601
      .... .... .... ...1 = ESS capabilities: Transmitter is an AP
      .... .... .... ..0. = IBSS status: Transmitter belongs to a BSS
      .... ..1. .... 00.. = CFP participation capabilities: QAP (HC) does not use CFP for delivery of unicast data type frames (0x80)
      .... .... ...0 .... = Privacy: AP/STA cannot support WEP
      .... .... ..0. .... = Short Preamble: Not Allowed
      .... .... .0.. .... = PBCC: Not Allowed
      .... .... 0... .... = Channel Agility: Not in use
      .... ...0 .... .... = Spectrum Management: Not Implemented
      .... .1.. .... .... = Short Slot Time: In use
      .... 0... .... .... = Automatic Power Save Delivery: Not Implemented
      ...0 .... .... .... = Radio Measurement: Not Implemented
      ..0. .... .... .... = DSSS-OFDM: Not Allowed
      .0.. .... .... .... = Delayed Block Ack: Not Implemented
      0... .... .... .... = Immediate Block Ack: Not Implemented
    Status code: Successful (0x0000)
    ..00 0000 0000 0101 = Association ID: 0x0005
```

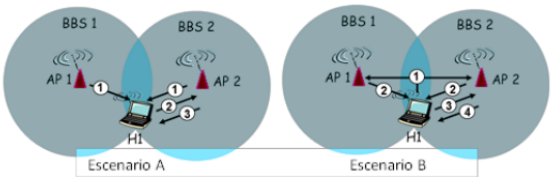
```
Tagged parameters (36 bytes)
  Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
      Tag Number: Supported Rates (1)
      Tag length: 4
      Supported Rates: 1(B) (0x82)
      Supported Rates: 2(B) (0x84)
      Supported Rates: 5.5(B) (0x8b)
      Supported Rates: 11(B) (0x96)
  Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
      Tag Number: Extended Supported Rates (50)
      Tag length: 8
      Extended Supported Rates: 6(B) (0x8c)
      Extended Supported Rates: 9 (0x12)
      Extended Supported Rates: 12(B) (0x98)
      Extended Supported Rates: 18 (0x24)
      Extended Supported Rates: 24(B) (0xb0)
      Extended Supported Rates: 36 (0x48)
      Extended Supported Rates: 48 (0x60)
      Extended Supported Rates: 54 (0x6c)
  Tag: EDCA Parameter Set
      Tag Number: EDCA Parameter Set (12)
      Tag length: 18
    WME QoS Info: 0x0f
        0... .... = U-APSD: Disabled
        .... 1111 = Parameter Set Count: 0xf
        .000 .... = Reserved: 0x0
```

```
      Reserved: 00
    Ac Parameters ACI 0 (Best Effort), ACM no, AIFSN 3, ECWmin/max 4/10 (CWmin/max 15/1023), TXOP 0
      ACI / AIFSN Field: 0x03
          .00. .... = ACI: Best Effort (0)
          ...0 .... = Admission Control Mandatory: No
          .... 0011 = AIFSN: 3
          0... .... = Reserved: 0
      ECW: 0xa4
          1010 .... = ECW Max: 10
          .... 0100 = ECW Min: 4
          CW Max: 1023
          CW Min: 15
        TXOP Limit: 0
    Ac Parameters ACI 1 (Background), ACM no, AIFSN 7, ECWmin/max 4/10 (CWmin/max 15/1023), TXOP 0
      ACI / AIFSN Field: 0x27
          .01. .... = ACI: Background (1)
          ...0 .... = Admission Control Mandatory: No
          .... 0111 = AIFSN: 7
          0... .... = Reserved: 0
      ECW: 0xa4
          1010 .... = ECW Max: 10
          .... 0100 = ECW Min: 4
          CW Max: 1023
          CW Min: 15
        TXOP Limit: 0
    Ac Parameters ACI 2 (Video), ACM no, AIFSN 2, ECWmin/max 3/4 (CWmin/max 7/15), TXOP 94
```

```
      ACI / AIFSN Field: 0x42
          .10. .... = ACI: Video (2)
          ...0 .... = Admission Control Mandatory: No
          .... 0010 = AIFSN: 2
          0... .... = Reserved: 0
      ECW: 0x43
          0100 .... = ECW Max: 4
          .... 0011 = ECW Min: 3
          CW Max: 15
          CW Min: 7
        TXOP Limit: 94
    Ac Parameters ACI 3 (Voice), ACM no, AIFSN 2, ECWmin/max 2/3 (CWmin/max 3/7), TXOP 47
      ACI / AIFSN Field: 0x62
          .11. .... = ACI: Voice (3)
          ...0 .... = Admission Control Mandatory: No
          .... 0010 = AIFSN: 2
          0... .... = Reserved: 0
      ECW: 0x32
          0011 .... = ECW Max: 3
          .... 0010 = ECW Min: 2
          CW Max: 7
          CW Min: 3
        TXOP Limit: 47
```

7. Cuestión 4

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



El escenario B, ya que hay comunicación directa entre los Puntos de Acceso sin necesidad de un intermediario.

8. Cuestión 5

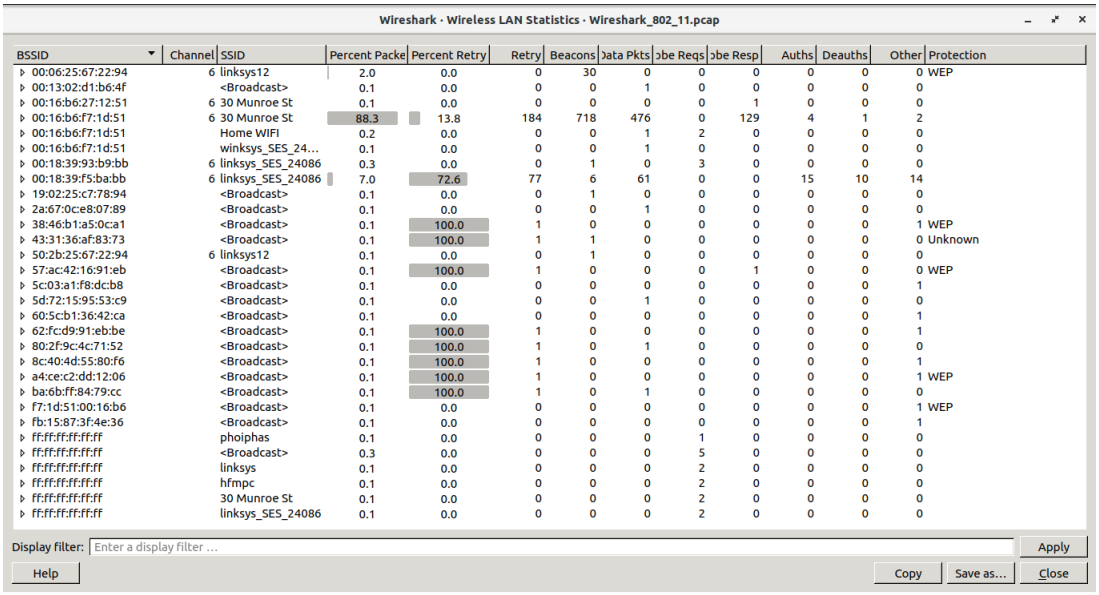
¿Cuántas tramas de datos diferentes observas en la captura? ¿Qué estaciones participan de esta comunicación? ¿Hay comunicación directa entre estaciones o siempre interviene un punto de acceso?

wlan.fc.type == 2 — Expression

No.	Time	Source	Destination	Protocol	Length	Info
420	21.69…	IntelCor_d1:b6:4f	Cisco-Li_…	802.11	54	QoS Null function (No data), SN=1525, FN=0, Flags=...P...TC
432	22.71…	IntelCor_d1:b6:4f	Cisco-Li_…	802.11	54	QoS Null function (No data), SN=1526, FN=0, Flags=.......TC
434	22.71…	IntelCor_d1:b6:4f	Cisco-Li_…	802.11	54	QoS Null function (No data), SN=1527, FN=0, Flags=...P...TC
446	23.73…	IntelCor_d1:b6:4f	Cisco-Li_…	802.11	54	QoS Null function (No data), SN=1528, FN=0, Flags=.......TC
448	23.73…	IntelCor_d1:b6:4f	Cisco-Li_…	802.11	54	QoS Null function (No data), SN=1529, FN=0, Flags=...P...TC
463	24.76…	IntelCor_d1:b6:4f	Cisco-Li_…	802.11	54	QoS Null function (No data), SN=1531, FN=0, Flags=...P...TC
465	24.79…	IntelCor_d1:b6:4f	88:01:2c:…	LLC	90	S P, func=RNR, N(R)=87; DSAP Banyan Vines Group, SSAP 0x6a Command
466	24.79…	IntelCor_d1:b6:4f	Broadcast	ARP	90	Who has 192.168.1.1? Tell 192.168.1.109
468	24.79…	Cisco-Li_f7:1d:51	Cisco-Li_…	802.11	90	Fragmented IEEE 802.11 frame
470	24.79…	192.168.1.109	68.87.71.…	DNS	125	Standard query 0x7892 A gaia.cs.umass.edu
472	24.80…	68.87.71.226	192.168.1…	DNS	141	Standard query response 0x7892 A gaia.cs.umass.edu A 128.119.245.12
474	24.81…	192.168.1.109	128.119.2…	TCP	110	2538 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
476	24.82…	128.119.245.12	192.168.1…	TCP	110	80 → 2538 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 SACK_PERM=1
478	24.82…	192.168.1.109	128.119.2…	TCP	102	2538 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
480	24.82…	192.168.1.109	128.119.2…	HTTP	537	GET /wireshark-labs/alice.txt HTTP/1.1
482	24.84…	128.119.245.12	192.168.1…	TCP	108	80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0
484	24.84…	128.119.245.12	192.168.1…	TCP	108	[TCP Dup ACK 482#1] 80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0
486	24.84…	128.119.245.12	192.168.1…	TCP	415	80 → 2538 [PSH, ACK] Seq=1 Ack=436 Win=6432 Len=313 [TCP segment of a reassembled PD…
488	24.85…	128.119.245.12	192.168.1…	TCP	1562	80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460 [TCP segment of a reassembled PDU]
489	24.85…	128.119.245.12	192.168.1…	TCP	1562	[TCP Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460
490	24.85…	128.119.245.12	192.168.1…	TCP	1562	[TCP Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460

Hay bastantes subtipos de tramas de datos. Los que más se repiten son:

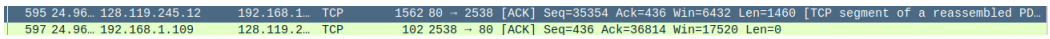
- Standard query
- QoS Null Function (No data)
- Null Function (No data)
- ACK
- SYN-ACK
- PSH-ACK



Las estaciones que participan son las de la imagen anterior. Siempre interviene un Punto de Acceso en la comunicación, como es normal en este tipo de comunicaciones.

9. Ejercicio 4

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



Trama de datos

```
Frame 595: 1562 bytes on wire (12496 bits), 1562 bytes captured (12496 bits)
    Encapsulation type: IEEE 802.11 plus radiotap radio header (23)
    Arrival Time: Jun 29, 2007 04:05:32.032842000 CEST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1183082732.032842000 seconds
    [Time delta from previous captured frame: 0.001179000 seconds]
    [Time delta from previous displayed frame: 0.001184000 seconds]
    [Time since reference or first frame: 24.960385000 seconds]
    Frame Number: 595
    Frame Length: 1562 bytes (12496 bits)
    Capture Length: 1562 bytes (12496 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: radiotap:wlan_radio:wlan:llc:ip:tcp]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
Radiotap Header v0, Length 24
    Header revision: 0
    Header pad: 0
    Header length: 24
  Present flags
    Present flags word: 0x000058ee
        .... .... .... .... .... .... .... ...0 = TSFT: Absent
        .... .... .... .... .... .... .... ..1. = Flags: Present
        .... .... .... .... .... .... .... .1.. = Rate: Present
        .... .... .... .... .... .... .... 1... = Channel: Present
```

```
        .... .... .... .... .... .... ...0 .... = FHSS: Absent
        .... .... .... .... .... .... ..1. .... = dBm Antenna Signal: Present
        .... .... .... .... .... .... .1.. .... = dBm Antenna Noise: Present
        .... .... .... .... .... .... 1... .... = Lock Quality: Present
        .... .... .... .... .... ...0 .... .... = TX Attenuation: Absent
        .... .... .... .... .... ..0. .... .... = dB TX Attenuation: Absent
        .... .... .... .... .... .0.. .... .... = dBm TX Power: Absent
        .... .... .... .... .... 1... .... .... = Antenna: Present
        .... .... .... .... ...1 .... .... .... = dB Antenna Signal: Present
        .... .... .... .... ..0. .... .... .... = dB Antenna Noise: Absent
        .... .... .... .... .1.. .... .... .... = RX flags: Present
        .... .... .... .0.. .... .... .... .... = Channel+: Absent
        .... .... .... 0... .... .... .... .... = MCS information: Absent
        .... .... ...0 .... .... .... .... .... = A-MPDU Status: Absent
        .... .... ..0. .... .... .... .... .... = VHT information: Absent
        .... .... .0.. .... .... .... .... .... = frame timestamp: Absent
        .... .... 0... .... .... .... .... .... = HE information: Absent
        .... ...0 .... .... .... .... .... .... = HE-MU information: Absent
        ...0 000. .... .... .... .... .... .... = Reserved: 0x0
        ..0. .... .... .... .... .... .... .... = Radiotap NS next: False
        .0.. .... .... .... .... .... .... .... = Vendor NS next: False
        0... .... .... .... .... .... .... .... = Ext: Absent
  Flags: 0x10
      .... ...0 = CFP: False
      .... ..0. = Preamble: Long
      .... .0.. = WEP: False
```

```
      .... 0... = Fragmentation: False
      ...1 .... = FCS at end: True
      ..0. .... = Data Pad: False
      .0.. .... = Bad FCS: False
      0... .... = Short GI: False
    Data Rate: 48,0 Mb/s
    Channel frequency: 2437 [BG 6]
  Channel flags: 0x00c0, Orthogonal Frequency-Division Multiplexing (OFDM), 2 GHz spectrum
      .... .... ...0 .... = Turbo: False
      .... .... ..0. .... = Complementary Code Keying (CCK): False
      .... .... .1.. .... = Orthogonal Frequency-Division Multiplexing (OFDM): True
      .... .... 1... .... = 2 GHz spectrum: True
      .... ...0 .... .... = 5 GHz spectrum: False
      .... ..0. .... .... = Passive: False
      .... .0.. .... .... = Dynamic CCK-OFDM: False
      .... 0... .... .... = Gaussian Frequency Shift Keying (GFSK): False
      ...0 .... .... .... = GSM (900MHz): False
      ..0. .... .... .... = Static Turbo: False
      .0.. .... .... .... = Half Rate Channel (10MHz Channel Width): False
      0... .... .... .... = Quarter Rate Channel (5MHz Channel Width): False
    Antenna signal: -36dBm
    Antenna noise: -100dBm
    Signal Quality: 89
    Antenna: 0
    dB antenna signal: 64dB
  RX flags: 0x6216, Bad PLCP
```

```
    .... .... .... .... .... ..1. = Bad PLCP: True
▾ 802.11 radio information
    PHY type: 802.11g (6)
    Short preamble: False
    Proprietary mode: None (0)
    Data rate: 48,0 Mb/s
    Channel: 6
    Frequency: 2437MHz
    Signal strength (dBm): -36dBm
    Noise level (dBm): -100dBm
  ▾ [Duration: 280µs]
      [Preamble: 20µs]
▾ IEEE 802.11 QoS Data, Flags: ......F.C
    Type/Subtype: QoS Data (0x0028)
  ▾ Frame Control Field: 0x8802
      .... ..00 = Version: 0
      .... 10.. = Type: Data frame (2)
      1000 .... = Subtype: 8
    ▾ Flags: 0x02
        .... ..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
        .... 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 0010 1000 = Duration: 40 microseconds
    Receiver address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Destination address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    Source address: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)
    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
    1100 0101 0000 .... = Sequence number: 3152
    Frame check sequence: 0x125d6216 [correct]
    [FCS Status: Good]
  ▾ Qos Control: 0x0500
      .... .... .... 0000 = TID: 0
      [.... .... .... .000 = Priority: Best Effort (Best Effort) (0)]
      .... .... ...0 .... = EOSP: Service period
      .... .... .00. .... = Ack Policy: Normal Ack (0x0)
      .... .... 0... .... = Payload Type: MSDU
    ▾ 0000 0101 .... .... = QAP PS Buffer State: 0x05
        .... ..0. .... .... = Buffer State Indicated: No
▾ Logical-Link Control
  ▾ DSAP: SNAP (0xaa)
      1010 101. = SAP: SNAP
      .... ...0 = IG Bit: Individual
  ▾ SSAP: SNAP (0xaa)
      1010 101. = SAP: SNAP
      .... ...0 = CR Bit: Command
```

```
  ▾ Control field: U, func=UI (0x03)
      000. 00.. = Command: Unnumbered Information (0x00)
      .... ..11 = Frame type: Unnumbered frame (0x3)
    Organization Code: 00:00:00 (Officially Xerox, but
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.109
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▾ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 1500
    Identification: 0x180d (6157)
  ▾ Flags: 0x4000, Don't fragment
      0... .... .... .... = Reserved bit: Not set
      .1.. .... .... .... = Don't fragment: Set
      ..0. .... .... .... = More fragments: Not set
      ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 49
    Protocol: TCP (6)
    Header checksum: 0xf475 [validation disabled]
    [Header checksum status: Unverified]
    Source: 128.119.245.12
    Destination: 192.168.1.109
▾ Transmission Control Protocol, Src Port: 80, Dst Port: 2538, Seq: 35354, Ack: 436, Len: 1460
    Source Port: 80
```

```
Destination Port: 2538
[Stream index: 0]
[TCP Segment Len: 1460]
Sequence number: 35354    (relative sequence number)
[Next sequence number: 36814    (relative sequence number)]
Acknowledgment number: 436    (relative ack number)
0101 .... = Header Length: 20 bytes (5)
Flags: 0x010 (ACK)
   000. .... .... = Reserved: Not set
   ...0 .... .... = Nonce: Not set
   .... 0... .... = Congestion Window Reduced (CWR): Not set
   .... .0.. .... = ECN-Echo: Not set
   .... ..0. .... = Urgent: Not set
   .... ...1 .... = Acknowledgment: Set
   .... .... 0... = Push: Not set
   .... .... .0.. = Reset: Not set
   .... .... ..0. = Syn: Not set
   .... .... ...0 = Fin: Not set
   [TCP Flags: ·····A····]
Window size value: 6432
[Calculated window size: 6432]
[Window size scaling factor: -2 (no window scaling used)]
Checksum: 0x575e [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
[SEQ/ACK analysis]
```

```
   [iRTT: 0.016931000 seconds]
   [Bytes in flight: 2920]
   [Bytes sent since last PSH flag: 8760]
[Timestamps]
   [Time since first frame in this TCP stream: 0.149292000 seconds]
   [Time since previous frame in this TCP stream: 0.001184000 seconds]
TCP payload (1460 bytes)
[Reassembled PDU in frame: 868]
TCP segment data (1460 bytes)
```

Confirmación

```
Frame 597: 102 bytes on wire (816 bits), 102 bytes captured (816 bits)
   Encapsulation type: IEEE 802.11 plus radiotap radio header (23)
   Arrival Time: Jun 29, 2007 04:05:32.033054000 CEST
   [Time shift for this packet: 0.000000000 seconds]
   Epoch Time: 1183082732.033054000 seconds
   [Time delta from previous captured frame: 0.000098000 seconds]
   [Time delta from previous displayed frame: 0.000212000 seconds]
   [Time since reference or first frame: 24.960597000 seconds]
   Frame Number: 597
   Frame Length: 102 bytes (816 bits)
   Capture Length: 102 bytes (816 bits)
   [Frame is marked: False]
   [Frame is ignored: False]
   [Protocols in frame: radiotap:wlan_radio:wlan:llc:ip:tcp]
   [Coloring Rule Name: HTTP]
   [Coloring Rule String: http || tcp.port == 80 || http2]
Radiotap Header v0, Length 24
   Header revision: 0
   Header pad: 0
   Header length: 24
   Present flags
      Present flags word: 0x000058ee
         .... .... .... .... .... .... .... ...0 = TSFT: Absent
         .... .... .... .... .... .... .... ..1. = Flags: Present
         .... .... .... .... .... .... .... .1.. = Rate: Present
         .... .... .... .... .... .... .... 1... = Channel: Present
```

```
        .... .... .... .... .... .... ...0 .... = FHSS: Absent
        .... .... .... .... .... .... ..1. .... = dBm Antenna Signal: Present
        .... .... .... .... .... .... .1.. .... = dBm Antenna Noise: Present
        .... .... .... .... .... .... 1... .... = Lock Quality: Present
        .... .... .... .... .... ...0 .... .... = TX Attenuation: Absent
        .... .... .... .... .... ..0. .... .... = dB TX Attenuation: Absent
        .... .... .... .... .... .0.. .... .... = dBm TX Power: Absent
        .... .... .... .... .... 1... .... .... = Antenna: Present
        .... .... .... .... ...1 .... .... .... = dB Antenna Signal: Present
        .... .... .... .... ..0. .... .... .... = dB Antenna Noise: Absent
        .... .... .... .... .1.. .... .... .... = RX flags: Present
        .... .... .... .0.. .... .... .... .... = Channel+: Absent
        .... .... .... 0... .... .... .... .... = MCS information: Absent
        .... .... ...0 .... .... .... .... .... = A-MPDU Status: Absent
        .... .... ..0. .... .... .... .... .... = VHT information: Absent
        .... .... .0.. .... .... .... .... .... = frame timestamp: Absent
        .... .... 0... .... .... .... .... .... = HE information: Absent
        .... ...0 .... .... .... .... .... .... = HE-MU information: Absent
        ...0 000. .... .... .... .... .... .... = Reserved: 0x0
        ..0. .... .... .... .... .... .... .... = Radiotap NS next: False
        .0.. .... .... .... .... .... .... .... = Vendor NS next: False
        0... .... .... .... .... .... .... .... = Ext: Absent
    Flags: 0x10
        .... ...0 = CFP: False
        .... ..0. = Preamble: Long
        .... .0.. = WEP: False
```

```
        .... 0... = Fragmentation: False
        ...1 .... = FCS at end: True
        ..0. .... = Data Pad: False
        .0.. .... = Bad FCS: False
        0... .... = Short GI: False
    Data Rate: 54,0 Mb/s
    Channel frequency: 2437 [BG 6]
    Channel flags: 0x00c0, Orthogonal Frequency-Division Multiplexing (OFDM), 2 GHz spectrum
        .... .... ...0 .... = Turbo: False
        .... .... ..0. .... = Complementary Code Keying (CCK): False
        .... .... .1.. .... = Orthogonal Frequency-Division Multiplexing (OFDM): True
        .... .... 1... .... = 2 GHz spectrum: True
        .... ...0 .... .... = 5 GHz spectrum: False
        .... ..0. .... .... = Passive: False
        .... .0.. .... .... = Dynamic CCK-OFDM: False
        .... 0... .... .... = Gaussian Frequency Shift Keying (GFSK): False
        ...0 .... .... .... = GSM (900MHz): False
        ..0. .... .... .... = Static Turbo: False
        .0.. .... .... .... = Half Rate Channel (10MHz Channel Width): False
        0... .... .... .... = Quarter Rate Channel (5MHz Channel Width): False
    Antenna signal: -38dBm
    Antenna noise: -100dBm
    Signal Quality: 100
    Antenna: 0
    dB antenna signal: 62dB
    RX flags: 0x362d
                                    0... = Bad PLCP: False
```

```
        .... .... .... .... .... ..0. = Bad PLCP: False
802.11 radio information
    PHY type: 802.11g (6)
    Short preamble: False
    Proprietary mode: None (0)
    Data rate: 54,0 Mb/s
    Channel: 6
    Frequency: 2437MHz
    Signal strength (dBm): -38dBm
    Noise level (dBm): -100dBm
    [Duration: 32µs]
        [Preamble: 20µs]
IEEE 802.11 QoS Data, Flags: .......TC
    Type/Subtype: QoS Data (0x0028)
    Frame Control Field: 0x8801
        .... ..00 = Version: 0
        .... 10.. = Type: Data frame (2)
        1000 .... = Subtype: 8
    Flags: 0x01
        .... ..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
        .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)
    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 0100 0000 .... = Sequence number: 64
    Frame check sequence: 0x80c1362d [correct]
    [FCS Status: Good]
  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)
Logical-Link Control
  DSAP: SNAP (0xaa)
      1010 101. = SAP: SNAP
      .... ...0 = IG Bit: Individual
  SSAP: SNAP (0xaa)
      1010 101. = SAP: SNAP
      .... ...0 = CR Bit: Command
  Control field: U, func=UI (0x03)
```

```
      000. 00.. = Command: Unnumbered Information (0x00)
      .... ..11 = Frame type: Unnumbered frame (0x3)
    Organization Code: 00:00:00 (Officially Xerox, but
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.1.109, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 40
    Identification: 0x1333 (4915)
  Flags: 0x4000, Don't fragment
      0... .... .... .... = Reserved bit: Not set
      .1.. .... .... .... = Don't fragment: Set
      ..0. .... .... .... = More fragments: Not set
      ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0xb003 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.109
    Destination: 128.119.245.12
Transmission Control Protocol, Src Port: 2538, Dst Port: 80, Seq: 436, Ack: 36814, Len: 0
    Source Port: 2538
    Destination Port: 80
```

```
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 436    (relative sequence number)
    [Next sequence number: 436    (relative sequence number)]
    Acknowledgment number: 36814    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
  Flags: 0x010 (ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
      .... .... ..0. = Syn: Not set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ·····A····]
    Window size value: 17520
    [Calculated window size: 17520]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0xcc48 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  [SEQ/ACK analysis]
      [This is an ACK to the segment in frame: 595]
```

```
    [The RTT to ACK the segment was: 0.000212000 seconds]
    [iRTT: 0.016931000 seconds]
  [Timestamps]
    [Time since first frame in this TCP stream: 0.149504000 seconds]
    [Time since previous frame in this TCP stream: 0.000212000 seconds]
```

10. 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?

wlan.fc.type_subtype == 0x0024 — Expression

No.	Time	Source	Destination	Protocol	Length	Info
20…	60.05…	IntelCor_d1:b6:4f	Cisco-Li_…	802.11	52	Null function (No data), SN=1624, FN=0, Flags=...P...TC
20…	60.05…	IntelCor_d1:b6:4f	Cisco-Li_…	802.11	52	Null function (No data), SN=1624, FN=0, Flags=...PR..TC
20…	60.12…	IntelCor_d1:b6:4f	Cisco-Li_…	802.11	52	Null function (No data), SN=1625, FN=0, Flags=.......TC
20…	60.24…	IntelCor_d1:b6:4f	Cisco-Li_…	802.11	52	Null function (No data), SN=1626, FN=0, Flags=...P...TC
20…	60.24…	IntelCor_d1:b6:4f	Cisco-Li_…	802.11	52	Null function (No data), SN=1626, FN=0, Flags=...PR..TC
20…	60.25…	IntelCor_d1:b6:4f	Cisco-Li_…	802.11	52	Null function (No data), SN=1626, FN=0, Flags=...PR..TC
20…	60.28…	IntelCor_d1:b6:4f	Cisco-Li_…	802.11	52	Null function (No data), SN=1627, FN=0, Flags=.......TC
20…	60.28…	IntelCor_d1:b6:4f	Cisco-Li_…	802.11	52	Null function (No data), SN=1627, FN=0, Flags=....R..TC
20…	60.28…	IntelCor_d1:b6:4f	Cisco-Li_…	802.11	52	Null function (No data), SN=1627, FN=0, Flags=....R..TC
20…	60.28…	IntelCor_d1:b6:4f	Cisco-Li_…	802.11	52	Null function (No data), SN=1627, FN=0, Flags=....R..TC
20…	60.29…	IntelCor_d1:b6:4f	Cisco-Li_…	802.11	52	Null function (No data), SN=1627, FN=0, Flags=....R..TC
20…	60.30…	IntelCor_d1:b6:4f	Cisco-Li_…	802.11	52	Null function (No data), SN=1627, FN=0, Flags=....R..TC
20…	60.30…	IntelCor_d1:b6:4f	Cisco-Li_…	802.11	52	Null function (No data), SN=1627, FN=0, Flags=....R..TC
20…	60.35…	IntelCor_d1:b6:4f	Cisco-Li_…	802.11	52	Null function (No data), SN=1628, FN=0, Flags=...P...TC
20…	60.35…	IntelCor_d1:b6:4f	Cisco-Li_…	802.11	52	Null function (No data), SN=1628, FN=0, Flags=...PR..TC
20…	60.35…	IntelCor_d1:b6:4f	Cisco-Li_…	802.11	52	Null function (No data), SN=1628, FN=0, Flags=...PR..TC
20…	60.36…	IntelCor_d1:b6:4f	Cisco-Li_…	802.11	52	Null function (No data), SN=1628, FN=0, Flags=...PR..TC
20…	60.36…	IntelCor_d1:b6:4f	Cisco-Li_…	802.11	52	Null function (No data), SN=1628, FN=0, Flags=...PR..TC
20…	60.44…	IntelCor_d1:b6:4f	Cisco-Li_…	802.11	52	Null function (No data), SN=1629, FN=0, Flags=.......TC
20…	60.44…	IntelCor_d1:b6:4f	Cisco-Li_…	802.11	52	Null function (No data), SN=1629, FN=0, Flags=....R..TC
20…	60.44…	IntelCor_d1:b6:4f	Cisco-Li_…	802.11	52	Null function (No data), SN=1629, FN=0, Flags=....R..TC
20…	60.55…	IntelCor_d1:b6:4f	Cisco-Li_…	802.11	52	Null function (No data), SN=1630, FN=0, Flags=...P...TC
20…	60.55…	IntelCor_d1:b6:4f	Cisco-Li_…	802.11	52	Null function (No data), SN=1630, FN=0, Flags=...PR..TC
20…	60.55…	IntelCor_d1:b6:4f	Cisco-Li_…	802.11	52	Null function (No data), SN=1630, FN=0, Flags=...PR..TC

La principal diferencia es la ausencia del payload en la trama de datos y del campo de cuerpo. Se usa para mantener activo el canal de asociación, aprovechándose de su ligereza de su cabecera para un mayor ahorro energético.

```
Frame 2002: 52 bytes on wire (416 bits), 52 bytes captured (416 bits)
    Encapsulation type: IEEE 802.11 plus radiotap radio header (23)
    Arrival Time: Jun 29, 2007 04:06:07.128443000 CEST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1183082767.128443000 seconds
    [Time delta from previous captured frame: 0.069268000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 60.055986000 seconds]
    Frame Number: 2002
    Frame Length: 52 bytes (416 bits)
    Capture Length: 52 bytes (416 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: radiotap:wlan_radio:wlan]
Radiotap Header v0, Length 24
    Header revision: 0
    Header pad: 0
    Header length: 24
  Present flags
    Present flags word: 0x000058ee
        .... .... .... .... .... .... .... ...0 = TSFT: Absent
        .... .... .... .... .... .... .... ..1. = Flags: Present
        .... .... .... .... .... .... .... .1.. = Rate: Present
        .... .... .... .... .... .... .... 1... = Channel: Present
        .... .... .... .... .... .... ...0 .... = FHSS: Absent
        .... .... .... .... .... .... ..1. .... = dBm Antenna Signal: Present
```

```
        .... .... .... .... .... .... .1.. .... = dBm Antenna Noise: Present
        .... .... .... .... .... .... 1... .... = Lock Quality: Present
        .... .... .... .... .... ...0 .... .... = TX Attenuation: Absent
        .... .... .... .... .... ..0. .... .... = dB TX Attenuation: Absent
        .... .... .... .... .... .0.. .... .... = dBm TX Power: Absent
        .... .... .... .... .... 1... .... .... = Antenna: Present
        .... .... .... .... ...1 .... .... .... = dB Antenna Signal: Present
        .... .... .... .... ..0. .... .... .... = dB Antenna Noise: Absent
        .... .... .... .... .1.. .... .... .... = RX flags: Present
        .... .... .... .0.. .... .... .... .... = Channel+: Absent
        .... .... .... 0... .... .... .... .... = MCS information: Absent
        .... .... ...0 .... .... .... .... .... = A-MPDU Status: Absent
        .... .... ..0. .... .... .... .... .... = VHT information: Absent
        .... .... .0.. .... .... .... .... .... = frame timestamp: Absent
        .... .... 0... .... .... .... .... .... = HE information: Absent
        .... ...0 .... .... .... .... .... .... = HE-MU information: Absent
        ...0 000. .... .... .... .... .... .... = Reserved: 0x0
        ..0. .... .... .... .... .... .... .... = Radiotap NS next: False
        .0.. .... .... .... .... .... .... .... = Vendor NS next: False
        0... .... .... .... .... .... .... .... = Ext: Absent
  Flags: 0x10
      .... ...0 = CFP: False
      .... ..0. = Preamble: Long
      .... .0.. = WEP: False
      .... 0... = Fragmentation: False
      ...1 .... = FCS at end: True
```

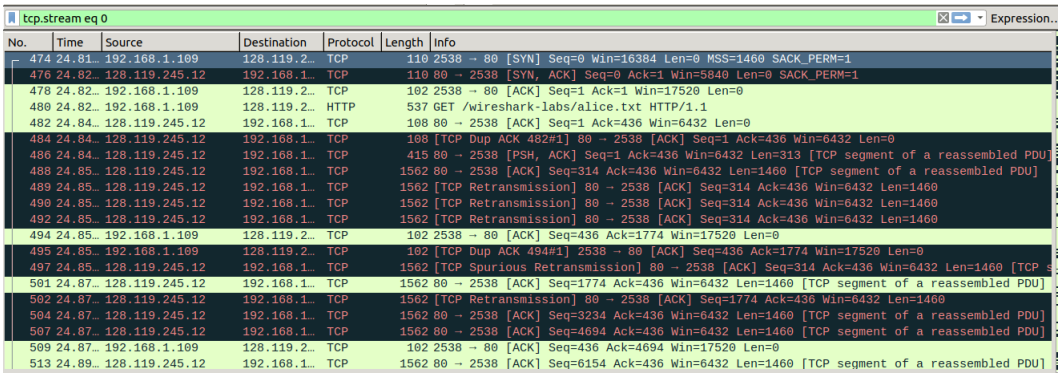
```
      ..0. .... = Data Pad: False
      .0.. .... = Bad FCS: False
      0... .... = Short GI: False
    Data Rate: 1,0 Mb/s
    Channel frequency: 2437 [BG 6]
  Channel flags: 0x00a0, Complementary Code Keying (CCK), 2 GHz spectrum
      .... .... ...0 .... = Turbo: False
      .... .... ..1. .... = Complementary Code Keying (CCK): True
      .... .... .0.. .... = Orthogonal Frequency-Division Multiplexing (OFDM): False
      .... .... 1... .... = 2 GHz spectrum: True
      .... ...0 .... .... = 5 GHz spectrum: False
      .... ..0. .... .... = Passive: False
      .... .0.. .... .... = Dynamic CCK-OFDM: False
      .... 0... .... .... = Gaussian Frequency Shift Keying (GFSK): False
      ...0 .... .... .... = GSM (900MHz): False
      ..0. .... .... .... = Static Turbo: False
      .0.. .... .... .... = Half Rate Channel (10MHz Channel Width): False
      0... .... .... .... = Quarter Rate Channel (5MHz Channel Width): False
    Antenna signal: -26dBm
    Antenna noise: -100dBm
    Signal Quality: 100
    Antenna: 0
    dB antenna signal: 74dB
  RX flags: 0xbff7, Bad PLCP
      .... .... .... .... .... ..1. = Bad PLCP: True
802.11 radio information
```

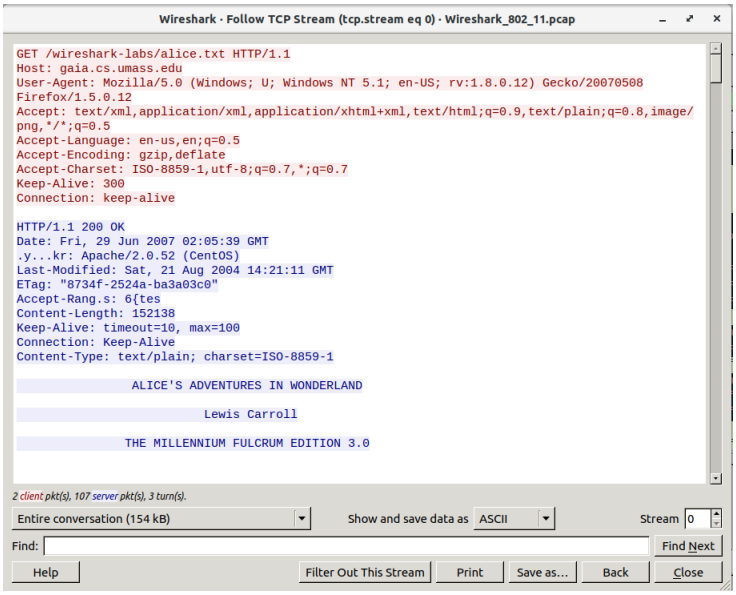
```
    PHY type: 802.11b (4)
    Short preamble: False
    Data rate: 1,0 Mb/s
    Channel: 6
    Frequency: 2437MHz
    Signal strength (dBm): -26dBm
    Noise level (dBm): -100dBm
  [Duration: 416µs]
      [Preamble: 192µs]
IEEE 802.11 Null function (No data), Flags: ...P...TC
    Type/Subtype: Null function (No data) (0x0024)
  Frame Control Field: 0x4811
      .... ..00 = Version: 0
      .... 10.. = Type: Data frame (2)
      0100 .... = Subtype: 4
    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 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: Cisco-Li_f5:ba:bb (00:18:39:f5:ba:bb)
    Transmitter address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
```

```
Destination address: Cisco-Li_f5:ba:bb (00:18:39:f5:ba:bb)
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)
STA address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
.... .... .... 0000 = Fragment number: 0
0110 0101 1000 .... = Sequence number: 1624
Frame check sequence: 0xb94abff7 [correct]
[FCS Status: Good]
```

11. Cuestión 6

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





11.1. 6.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?

- **Dirección MAC del host:** 00:13:02:d1:b6:4f
- **Punto de Acceso:** 00:16:b6:f7:1d:51
- **Primer router:** 00:13:02:d1:b6:4f

```
▾ IEEE 802.11 QoS Data, Flags: .......TC
    Type/Subtype: QoS Data (0x0028)
  ▾ Frame Control Field: 0x8801
      .... ..00 = Version: 0
      .... 10.. = Type: Data frame (2)
      1000 .... = Subtype: 8
    ▾ Flags: 0x01
        .... ..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
        .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)
    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)
```

11.2. 6.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

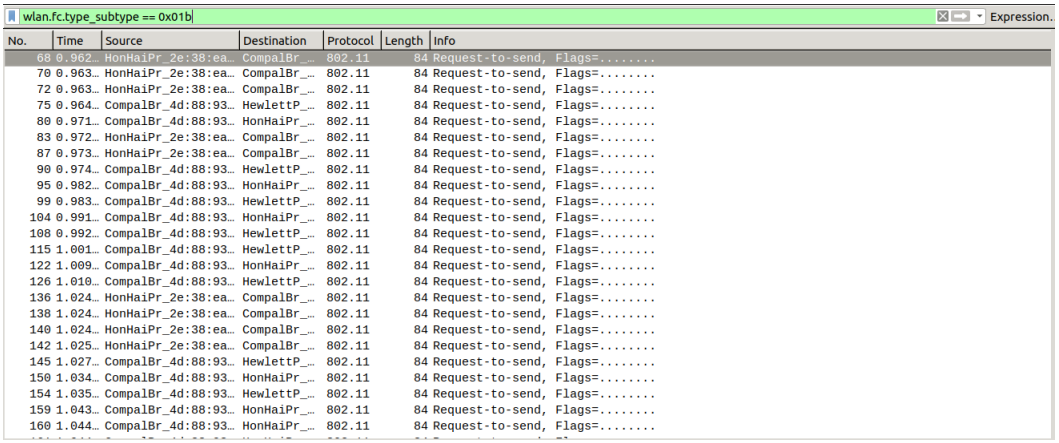
- **Host inalámbrico:** 192.168.1.109
- **IP destino:** 128.119.245.12 (AP, ya quelos bits del mecanimo de direccionamiento están a 01)

```
Source: 192.168.1.109
Destination: 128.119.245.12
```

12. Cuestión 7

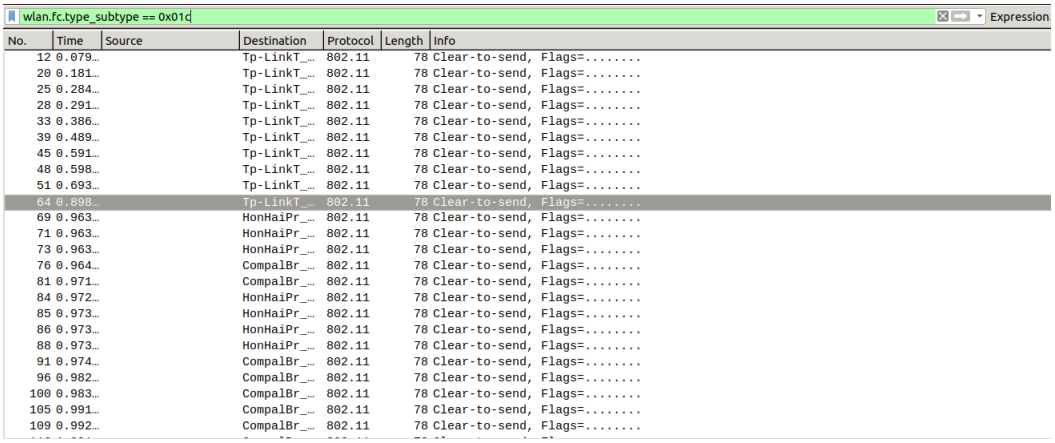
Localiza las tramas RTS y CTS capturadas en el fichero Wireshar_802_11.pcap. ¿Es posible que sólo haya tramas RTS o CTS? ¿Por qué?

Tiene sentido que haya tramas RTS sin CTS, ya que se pueden efectuar peticiones sin que haya respuesta. Sin embargo, no lo tiene que sea al revés, ya que carece de sentido enviar una respuesta sin una petición.



wlan.fc.type_subtype == 0x01b — Expression...

No.	Time	Source	Destination	Protocol	Length	Info
68	0.962…	HonHaiPr_2e:38:ea…	CompalBr_…	802.11	84	Request-to-send, Flags=........
70	0.963…	HonHaiPr_2e:38:ea…	CompalBr_…	802.11	84	Request-to-send, Flags=........
72	0.963…	HonHaiPr_2e:38:ea…	CompalBr_…	802.11	84	Request-to-send, Flags=........
75	0.964…	CompalBr_4d:88:93…	HewlettP_…	802.11	84	Request-to-send, Flags=........
80	0.971…	CompalBr_4d:88:93…	HonHaiPr_…	802.11	84	Request-to-send, Flags=........
83	0.972…	HonHaiPr_2e:38:ea…	CompalBr_…	802.11	84	Request-to-send, Flags=........
87	0.973…	HonHaiPr_2e:38:ea…	CompalBr_…	802.11	84	Request-to-send, Flags=........
90	0.974…	CompalBr_4d:88:93…	HewlettP_…	802.11	84	Request-to-send, Flags=........
95	0.982…	CompalBr_4d:88:93…	HonHaiPr_…	802.11	84	Request-to-send, Flags=........
99	0.983…	CompalBr_4d:88:93…	HewlettP_…	802.11	84	Request-to-send, Flags=........
104	0.991…	CompalBr_4d:88:93…	HonHaiPr_…	802.11	84	Request-to-send, Flags=........
108	0.992…	CompalBr_4d:88:93…	HewlettP_…	802.11	84	Request-to-send, Flags=........
115	1.001…	CompalBr_4d:88:93…	HewlettP_…	802.11	84	Request-to-send, Flags=........
122	1.009…	CompalBr_4d:88:93…	HonHaiPr_…	802.11	84	Request-to-send, Flags=........
126	1.010…	CompalBr_4d:88:93…	HewlettP_…	802.11	84	Request-to-send, Flags=........
136	1.024…	HonHaiPr_2e:38:ea…	CompalBr_…	802.11	84	Request-to-send, Flags=........
138	1.024…	HonHaiPr_2e:38:ea…	CompalBr_…	802.11	84	Request-to-send, Flags=........
140	1.024…	HonHaiPr_2e:38:ea…	CompalBr_…	802.11	84	Request-to-send, Flags=........
142	1.025…	HonHaiPr_2e:38:ea…	CompalBr_…	802.11	84	Request-to-send, Flags=........
145	1.027…	CompalBr_4d:88:93…	HewlettP_…	802.11	84	Request-to-send, Flags=........
150	1.034…	CompalBr_4d:88:93…	HonHaiPr_…	802.11	84	Request-to-send, Flags=........
154	1.035…	CompalBr_4d:88:93…	HewlettP_…	802.11	84	Request-to-send, Flags=........
159	1.043…	CompalBr_4d:88:93…	HonHaiPr_…	802.11	84	Request-to-send, Flags=........
160	1.044…	CompalBr_4d:88:93…	HonHaiPr_…	802.11	84	Request-to-send, Flags=........



wlan.fc.type_subtype == 0x01c — Expression...

No.	Time	Source	Destination	Protocol	Length	Info
12	0.079…		Tp-LinkT_…	802.11	78	Clear-to-send, Flags=........
20	0.181…		Tp-LinkT_…	802.11	78	Clear-to-send, Flags=........
25	0.284…		Tp-LinkT_…	802.11	78	Clear-to-send, Flags=........
28	0.291…		Tp-LinkT_…	802.11	78	Clear-to-send, Flags=........
33	0.386…		Tp-LinkT_…	802.11	78	Clear-to-send, Flags=........
39	0.489…		Tp-LinkT_…	802.11	78	Clear-to-send, Flags=........
45	0.591…		Tp-LinkT_…	802.11	78	Clear-to-send, Flags=........
48	0.598…		Tp-LinkT_…	802.11	78	Clear-to-send, Flags=........
51	0.693…		Tp-LinkT_…	802.11	78	Clear-to-send, Flags=........
64	0.898…		Tp-LinkT_…	802.11	78	Clear-to-send, Flags=........
69	0.963…		HonHaiPr_…	802.11	78	Clear-to-send, Flags=........
71	0.963…		HonHaiPr_…	802.11	78	Clear-to-send, Flags=........
73	0.963…		HonHaiPr_…	802.11	78	Clear-to-send, Flags=........
76	0.964…		CompalBr_…	802.11	78	Clear-to-send, Flags=........
81	0.971…		CompalBr_…	802.11	78	Clear-to-send, Flags=........
84	0.972…		HonHaiPr_…	802.11	78	Clear-to-send, Flags=........
85	0.973…		HonHaiPr_…	802.11	78	Clear-to-send, Flags=........
86	0.973…		HonHaiPr_…	802.11	78	Clear-to-send, Flags=........
88	0.973…		HonHaiPr_…	802.11	78	Clear-to-send, Flags=........
91	0.974…		CompalBr_…	802.11	78	Clear-to-send, Flags=........
96	0.982…		CompalBr_…	802.11	78	Clear-to-send, Flags=........
100	0.983…		CompalBr_…	802.11	78	Clear-to-send, Flags=........
105	0.991…		CompalBr_…	802.11	78	Clear-to-send, Flags=........
109	0.992…		CompalBr_…	802.11	78	Clear-to-send, Flags=........

13. Cuestión 8

Localiza las tramas RTS y CTS capturadas en el fichero Wireshar_802_11_RTS_CTS.pcap. ¿Qué información contiene estas tramas? ¿Para qué sirve el valor NAV?

El valor NAV (Network Allocation Vector) se usa para calcular el tiempo que el medio está siendo usado, y por lo tanto, saber cuándo enviar peticiones para usarlo y así reducir las colisiones de peticiones.

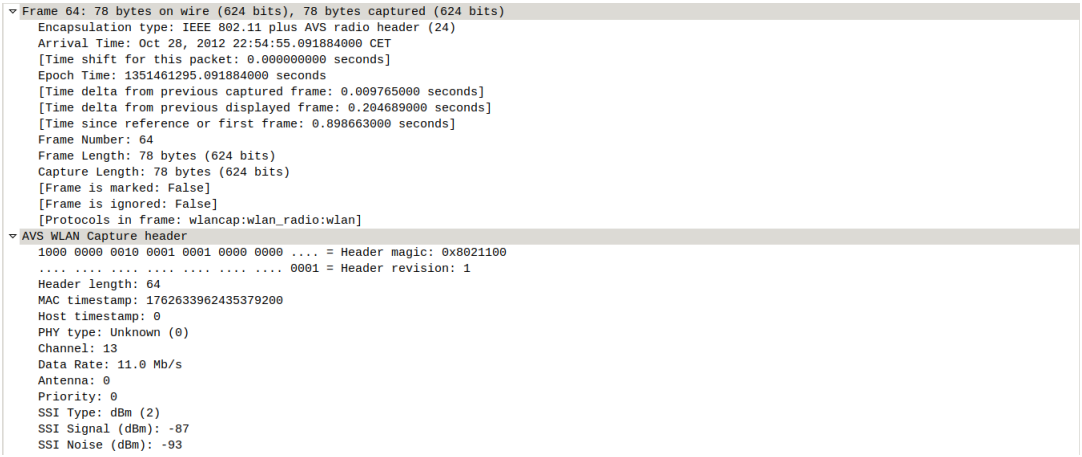
RTS

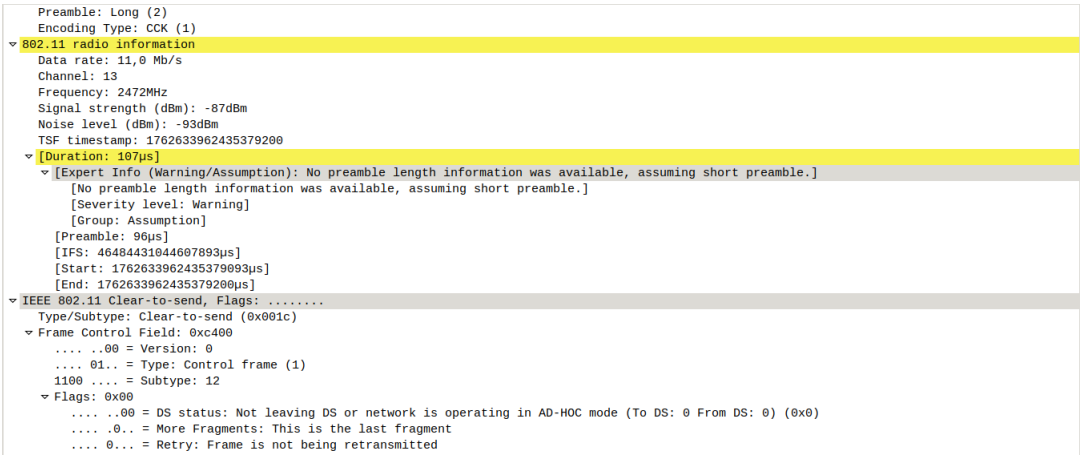
```
▽ Frame 68: 84 bytes on wire (672 bits), 84 bytes captured (672 bits)
    Encapsulation type: IEEE 802.11 plus AVS radio header (24)
    Arrival Time: Oct 28, 2012 22:54:55.156218000 CET
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1351461295.156218000 seconds
    [Time delta from previous captured frame: 0.004373000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.962997000 seconds]
    Frame Number: 68
    Frame Length: 84 bytes (672 bits)
    Capture Length: 84 bytes (672 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: wlancap:wlan_radio:wlan]
▽ AVS WLAN Capture header
    1000 0000 0010 0001 0001 0000 0000 .... = Header magic: 0x8021100
    .... .... .... .... .... .... .... 0001 = Header revision: 1
    Header length: 64
    MAC timestamp: 2039221266363187200
    Host timestamp: 0
    PHY type: Unknown (0)
    Channel: 13
    Data Rate: 24.0 Mb/s
    Antenna: 0
    Priority: 0
    SSI Type: dBm (2)
    SSI Signal (dBm): -74
    SSI Noise (dBm): -93
```

```
    Preamble: Short (1)
    Encoding Type: OFDM (3)
▽ 802.11 radio information
    Data rate: 24,0 Mb/s
    Channel: 13
    Frequency: 2472MHz
    Signal strength (dBm): -74dBm
    Noise level (dBm): -93dBm
    TSF timestamp: 2039221266363187200
  ▽ [Duration: 28µs]
      [Preamble: 20µs]
      [IFS: 29424820944895972µs]
      [Start: 2039221266363187172µs]
      [End: 2039221266363187200µs]
▽ IEEE 802.11 Request-to-send, Flags: ........
    Type/Subtype: Request-to-send (0x001b)
  ▽ Frame Control Field: 0xb400
      .... ..00 = Version: 0
      .... 01.. = Type: Control frame (1)
      1011 .... = Subtype: 11
    ▽ 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 1001 1000 = Duration: 152 microseconds
    Receiver address: CompalBr_4d:88:93 (5c:35:3b:4d:88:93)
    Transmitter address: HonHaiPr_2e:38:ea (cc:af:78:2e:38:ea)
```

CTS


Frame 64: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
Encapsulation type: IEEE 802.11 plus AVS radio header (24)
Arrival Time: Oct 28, 2012 22:54:55.091884000 CET
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1351461295.091884000 seconds
[Time delta from previous captured frame: 0.009765000 seconds]
[Time delta from previous displayed frame: 0.204689000 seconds]
[Time since reference or first frame: 0.898663000 seconds]
Frame Number: 64
Frame Length: 78 bytes (624 bits)
Capture Length: 78 bytes (624 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: wlancap:wlan_radio:wlan]
AVS WLAN Capture header
1000 0000 0010 0001 0001 0000 0000 .... = Header magic: 0x8021100
.... 0001 = Header revision: 1
Header length: 64
MAC timestamp: 1762633962435379200
Host timestamp: 0
PHY type: Unknown (0)
Channel: 13
Data Rate: 11.0 Mb/s
Antenna: 0
Priority: 0
SSI Type: dBm (2)
SSI Signal (dBm): -87
SSI Noise (dBm): -93


Preamble: Long (2)
Encoding Type: CCK (1)
802.11 radio information
Data rate: 11,0 Mb/s
Channel: 13
Frequency: 2472MHz
Signal strength (dBm): -87dBm
Noise level (dBm): -93dBm
TSF timestamp: 1762633962435379200
[Duration: 107µs]
[Expert Info (Warning/Assumption): No preamble length information was available, assuming short preamble.]
[No preamble length information was available, assuming short preamble.]
[Severity level: Warning]
[Group: Assumption]
[Preamble: 96µs]
[IFS: 46484431044607893µs]
[Start: 1762633962435379093µs]
[End: 1762633962435379200µs]
IEEE 802.11 Clear-to-send, Flags: ....
Type/Subtype: Clear-to-send (0x001c)
Frame Control Field: 0xc400
.... ..00 = Version: 0
.... 01.. = Type: Control frame (1)
1100 .... = Subtype: 12
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
.001 0010 0011 1011 = Duration: 4667 microseconds
Receiver address: Tp-LinkT_bc:7a:12 (d8:5d:4c:bc:7a:12)