

Asociación

Cuestión 1. Localiza las tramas Beacon:

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

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

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

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

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

Imagen 1: Aps in Wireshark_802_11LOCAL

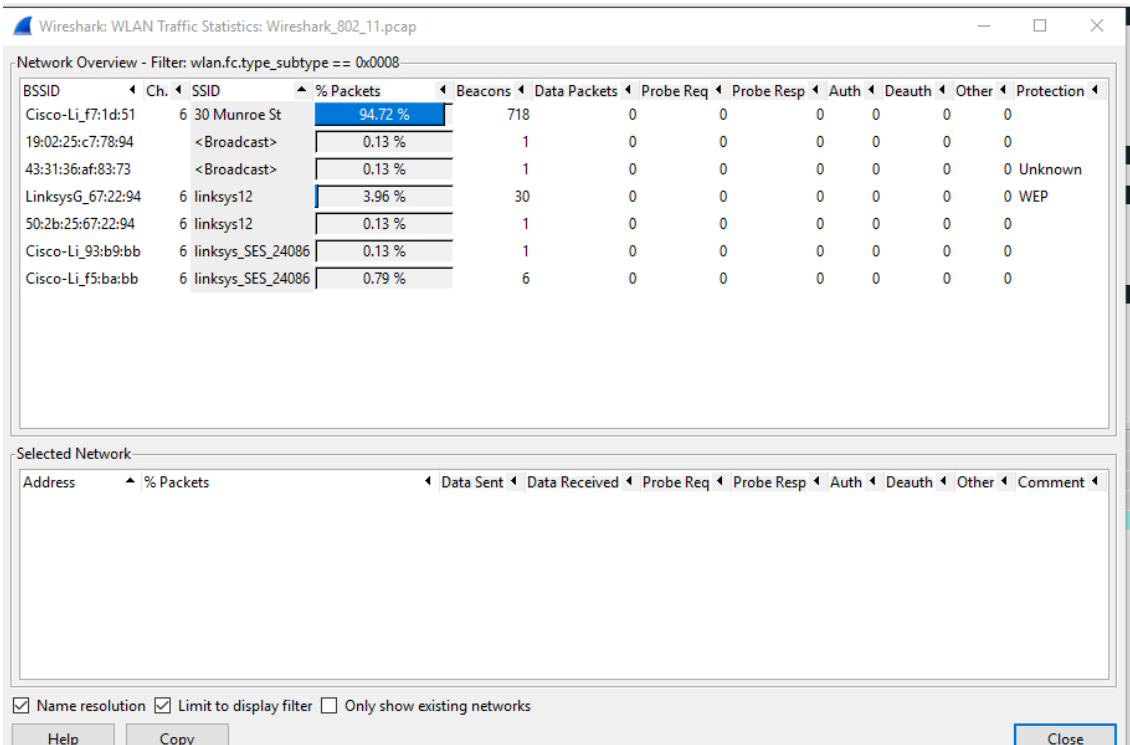
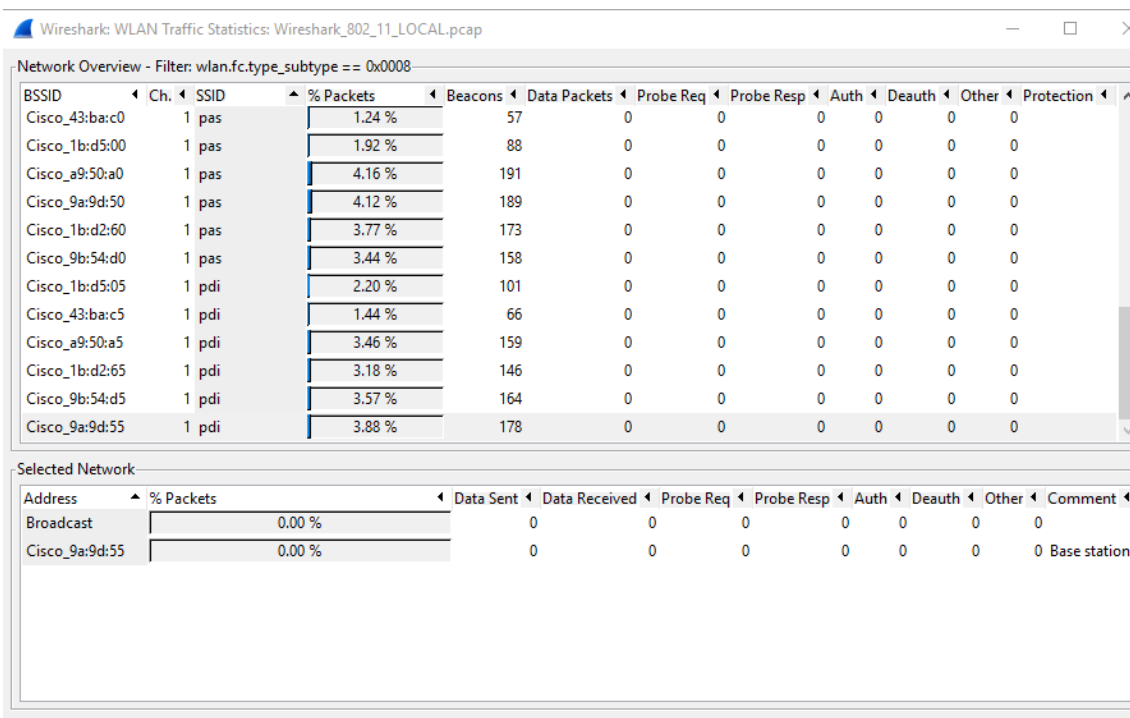


Imagen 2: Aps in Wireshark_802_11

- b) ¿Cuáles son sus identificadores?
- En la captura LOCAL tenemos los SSIDs: Broadcast, ICB-Wifi, NEO, WifiUma, alumnos, eduroam, pas, pdi.



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

Wireshark: WLAN Traffic Statistics: Wireshark_802_11.pcap

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

BSSID	Ch.	SSID	% Packets	Beacons	Data Packets	Probe Req	Probe Resp	Auth	Deauth	Other	Protection
Cisco-Li_f7:1d:51	6	30 Munroe St	94.72 %	718	0	0	0	0	0	0	0
19:02:25:c7:78:94		<Broadcast>	0.13 %	1	0	0	0	0	0	0	0
43:31:36:af:83:73		<Broadcast>	0.13 %	1	0	0	0	0	0	0	Unknown
LinksysG_67:22:94	6	lynksys12	3.96 %	30	0	0	0	0	0	0	WEP
50:2b:25:67:22:94	6	lynksys12	0.13 %	1	0	0	0	0	0	0	0
Cisco-Li_93:b9:bb	6	lynksys_SES_24086	0.13 %	1	0	0	0	0	0	0	0
Cisco-Li_f5:ba:bb	6	lynksys_SES_24086	0.79 %	6	0	0	0	0	0	0	0

Selected Network:

Address	% Packets	Data Sent	Data Received	Probe Req	Probe Resp	Auth	Deauth	Other	Comment
---------	-----------	-----------	---------------	-----------	------------	------	--------	-------	---------

☒ Name resolution ☒ Limit to display filter ☐ Only show existing networks

Help Copy Close

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

Filter: wlan.sa == 00:14:1c:9b:54:d4 and wlan.fc.type_subtype == 0x0008

Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
2787	5.045787	Cisco_9b:54:d4	Broadcast	802.11	252	Beacon frame, SN=179,
2850	5.148482	Cisco_9b:54:d4	Broadcast	802.11	252	Beacon frame, SN=195,
3037	5.352811	Cisco_9b:54:d4	Broadcast	802.11	252	Beacon frame, SN=263,
3152	5.455562	Cisco_9b:54:d4	Broadcast	802.11	252	Beacon frame, SN=288,
3260	5.557583	Cisco_9b:54:d4	Broadcast	802.11	252	Beacon frame, SN=332,
3331	5.660078	Cisco_9b:54:d4	Broadcast	802.11	252	Beacon frame, SN=361,
3427	5.762448	Cisco_9b:54:d4	Broadcast	802.11	252	Beacon frame, SN=391,
3605	5.865287	Cisco_9b:54:d4	Broadcast	802.11	252	Beacon frame, SN=417,
4034	6.173217	Cisco_9b:54:d4	Broadcast	802.11	252	Beacon frame, SN=525,
5021	6.788257	Cisco_9b:54:d4	Broadcast	802.11	252	Beacon frame, SN=709,
5169	6.888808	Cisco_9b:54:d4	Broadcast	802.11	252	Beacon frame, SN=732,
5285	6.991434	Cisco_9b:54:d4	Broadcast	802.11	252	Beacon frame, SN=759,
5675	7.400821	Cisco_9b:54:d4	Broadcast	802.11	252	Beacon frame, SN=871,
5973	7.708619	Cisco_9b:54:d4	Broadcast	802.11	252	Beacon frame, SN=961,
6303	8.016378	Cisco_9b:54:d4	Broadcast	802.11	252	Beacon frame, SN=1034,
6411	8.118797	Cisco_9b:54:d4	Broadcast	802.11	252	Beacon frame, SN=1068,
6579	8.322987	Cisco_9b:54:d4	Broadcast	802.11	252	Beacon frame, SN=1124,
6834	8.629612	Cisco_9b:54:d4	Broadcast	802.11	252	Beacon frame, SN=1199,
6903	8.732247	Cisco_9b:54:d4	Broadcast	802.11	252	Beacon frame, SN=1217,
7228	9.039386	Cisco_9b:54:d4	Broadcast	802.11	252	Beacon frame, SN=1286,
7708	9.551801	Cisco_9b:54:d4	Broadcast	802.11	252	Beacon frame, SN=1414,
7784	9.653837	Cisco_9b:54:d4	Broadcast	802.11	252	Beacon frame, SN=1436,
7853	9.756509	Cisco_9b:54:d4	Broadcast	802.11	252	Beacon frame, SN=1456,
7913	9.858778	Cisco_9b:54:d4	Broadcast	802.11	252	Beacon frame, SN=1472,
8103	10.063838	Cisco_9b:54:d4	Broadcast	802.11	252	Beacon frame, SN=1509,
8329	10.268203	Cisco_9b:54:d4	Broadcast	802.11	252	Beacon frame, SN=1553,
8491	10.370527	Cisco_9b:54:d4	Broadcast	802.11	252	Beacon frame, SN=1575,

Frame 5973: 252 bytes on wire (2016 bits), 252 bytes captured (2016 bits)

Radiotap Header v0, Length 25

802.11 radio information

IEEE 802.11 Beacon frame, Flags:C

IEEE 802.11 wireless LAN management frame

Fixed parameters (12 bytes)

Timestamp: 0x0000010749676318

Beacon Interval: 0.102400 [Seconds]

Capabilities Information: 0x0431

Tagged parameters (187 bytes)

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

d) ¿Qué tipo de trama es?

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

```
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
```

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

```
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
    .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_9b:54:d4 (00:14:1c:9b:54:d4)
    Source address: Cisco_9b:54:d4 (00:14:1c:9b:54:d4)
    BSS Id: Cisco_9b:54:d4 (00:14:1c:9b:54:d4)
    .... .... 0000 = Fragment number: 0
    1001 1110 0001 .... = Sequence number: 2529
    Frame check sequence: 0x2a2a94e3 [correct]
    [FCS Status: Good]
```

Imagen 3: Ejemplo estructura trama Beacon (Wireshark_802_11_LOCAL)

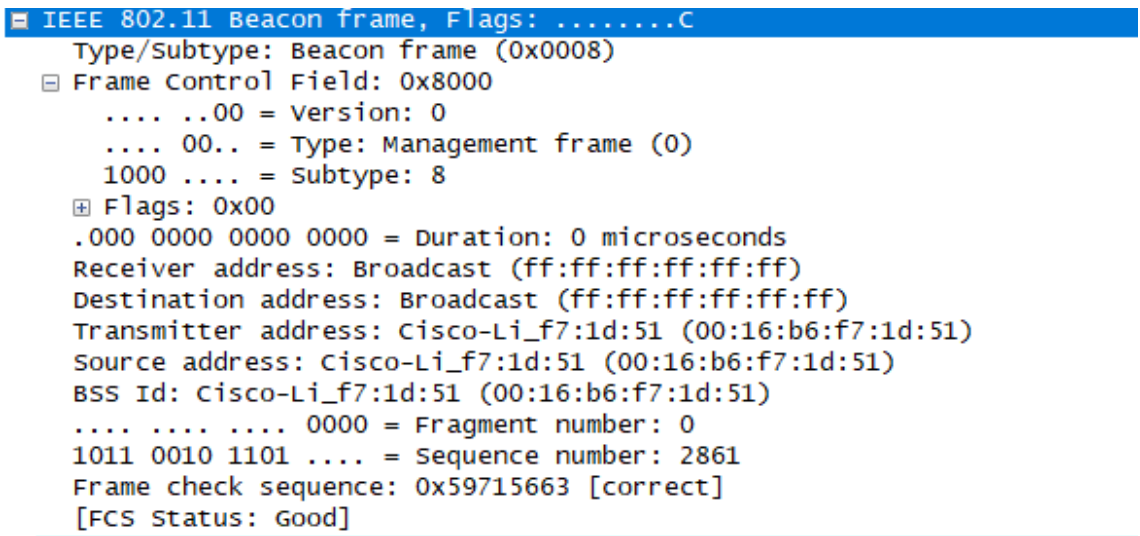


Imagen 4: Ejemplo estructura trama Beacon (Wireshark_802_11)

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

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

IntelCor_1f:57:13	Broadcast	802.11	79 Probe Request, SN=
IntelCor_1f:57:13	Broadcast	802.11	78 Probe Request, SN=
IntelCor_1f:57:13	Broadcast	802.11	79 Probe Request, SN=
IntelCor_1f:57:13	Broadcast	802.11	70 Probe Request, SN=
IntelCor_1f:57:13	Broadcast	802.11	77 Probe Request, SN=
IntelCor_1f:57:13	Broadcast	802.11	75 Probe Request, SN=
IntelCor_1f:57:13	Broadcast	802.11	75 Probe Request, SN=
IntelCor_1f:57:13	Broadcast	802.11	77 Probe Request, SN=
IntelCor_1f:57:13	Broadcast	802.11	70 Probe Request, SN=
IntelCor_d1:b6:4f	Broadcast	802.11	94 Probe Request, SN=
IntelCor_d1:b6:4f	Broadcast	802.11	82 Probe Request, SN=
IntelCor_d1:b6:4f	Broadcast	802.11	82 Probe Request, SN=
IntelCor_d1:b6:4f	Broadcast	802.11	99 Probe Request, SN=
IntelCor_d1:b6:4f	Broadcast	802.11	99 Probe Request, SN=
IntelCor_d1:b6:4f	Broadcast	802.11	99 Probe Request, SN=
IntelCor_d1:b6:4f	Broadcast	802.11	99 Probe Request, SN=
IntelCor_d1:b6:4f	Broadcast	802.11	82 Probe Request, SN=
IntelCor_d1:b6:4f	Broadcast	802.11	99 Probe Request, SN=
IntelCor_d1:b6:4f	Broadcast	802.11	94 Probe Request, SN=

Imagen 5: Probe Requests en Wireshark_802_11.

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

Imagen 6: Probe Requests en Wireshark_802_11_LOCAL.

b) Sí.

Filter: wlan.fc.type_subtype == 0x05 Expression... Clear Apply Save						
No.	Time	Source	Destination	Protocol	Length	Info
528	1.995322	Cisco_lb:d5:02	Htc_16:be:22	802.11	246	Probe Response, S
4900	6.712736	Cisco_lb:d5:01	HonHaiPr_c2:e3:2b	802.11	246	Probe Response, S
4903	6.714411	Cisco_lb:d5:02	HonHaiPr_c2:e3:2b	802.11	246	Probe Response, S
4906	6.715754	Cisco_lb:d5:04	HonHaiPr_c2:e3:2b	802.11	246	Probe Response, S
5188	6.906983	Cisco-Li_a6:53:7c	HonHaiPr_7e:b7:25	802.11	239	Probe Response, S
5190	6.919555	Cisco_a9:50:a1	HonHaiPr_7e:b7:25	802.11	246	Probe Response, S
5191	6.920222	Cisco_43:ba:c5	HonHaiPr_7e:b7:25	802.11	242	Probe Response, S
5193	6.920808	Cisco_9a:9d:50	HonHaiPr_7e:b7:25	802.11	242	Probe Response, S
5194	6.921403	Cisco_a9:50:a1	HonHaiPr_7e:b7:25	802.11	246	Probe Response, S
5195	6.922036	Cisco_9a:9d:50	HonHaiPr_7e:b7:25	802.11	242	Probe Response, S
5196	6.922638	Cisco_a9:50:a2	HonHaiPr_7e:b7:25	802.11	246	Probe Response, S
5197	6.923288	Cisco_a9:50:a2	HonHaiPr_7e:b7:25	802.11	246	Probe Response, S
5199	6.924505	Cisco_a9:50:a4	HonHaiPr_7e:b7:25	802.11	246	Probe Response, S
5202	6.925694	Cisco_a9:50:a4	HonHaiPr_7e:b7:25	802.11	246	Probe Response, S
5203	6.926903	Cisco_9a:9d:51	HonHaiPr_7e:b7:25	802.11	246	Probe Response, S

Imagen 7: Probe Responses en LOCAL.

Filter: wlan.fc.type_subtype == 0x05 Expression... Clear Apply Save						
No.	Time	Source	Destination	Protocol	Length	Info
27	1.212185	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	177	Probe Response, SN=2867, FI
51	2.300697	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2878, FI
52	2.302191	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2878, FI
53	2.304063	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2878, FI
54	2.305562	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2878, FI
55	2.308563	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2878, FI
56	2.310072	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2878, FI
59	2.453941	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2881, FI
83	4.283835	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	177	Probe Response, SN=2900, FI
88	4.301564	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2901, FI
89	4.303314	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2901, FI
90	4.304814	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2901, FI
93	4.403454	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2903, FI
94	4.404939	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2903, FI
119	6.303313	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2922, FI
130	6.404446	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2924, FI
131	6.405938	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2924, FI
132	6.407562	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2924, FI
133	6.409063	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2924, FI
134	6.410562	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2924, FI

Imagen 8: Probe Responses en Wireshark_802_11.

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

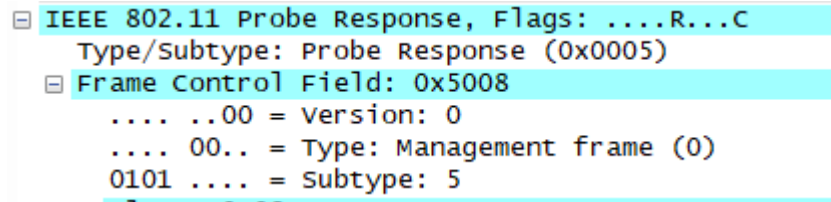


Imagen 9: Probe Response

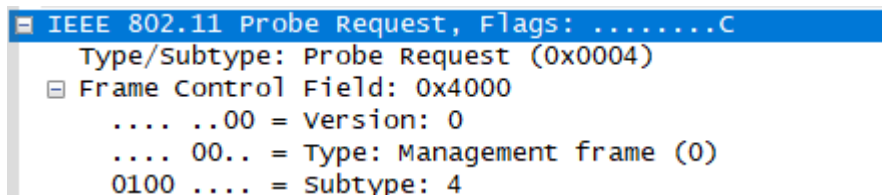


Imagen 10: Probe Request

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

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

118	6.300439	IntelCor_1f:57:13	Broadcast	802.11	70 Probe Request, SN=621, FN=0,
119	6.303313	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177 Probe Response, SN=2922, FN=0

Imagen 11: Interacción entre AP y estación base.


```
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
    .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: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
  Source address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
  BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
  .... .... 0000 = Fragment number: 0
  0010 0110 1101 .... = Sequence number: 621
  Frame check sequence: 0x0b5b766e [correct]
  [FCS Status: Good]
```

Imagen 12: Probe request de la trama n° 118.

```
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
    .000 0001 0011 1010 = Duration: 314 microseconds
  Receiver address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
  Destination address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
  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 0110 1010 .... = Sequence number: 2922
  Frame check sequence: 0x6f35c92c [correct]
  [FCS Status: Good]
```

Imagen 13: Probe response de la trama n° 119

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

Vamos a analizar la captura *Wireshark_802_11*:

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

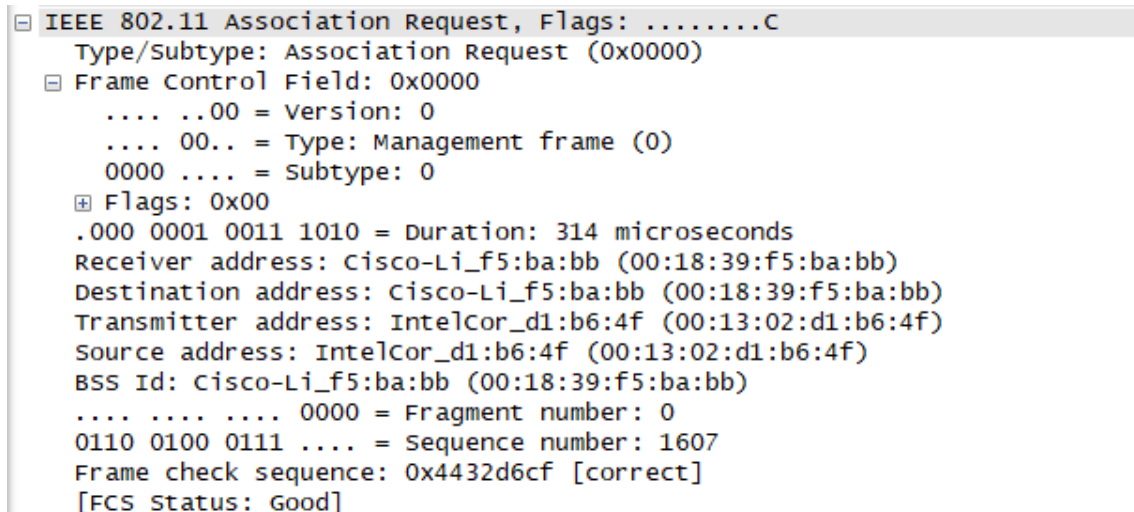


Imagen 14: Ejemplo estructura de un *Association Request*

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

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

Filter: <i>wlan.fc.type_subtype == 0x01</i>		Expression...	Clear	Apply	Save
No.	Time	Source	Destination	Protocol	Length
12	0.396690	00:ae:93:3d:0a:4a	ff:ff:ff:ff:bf:4a	802.11	
2166	63.192101	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	

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

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

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

Imagen 16: Estructura trama Association Response en captura analizada.

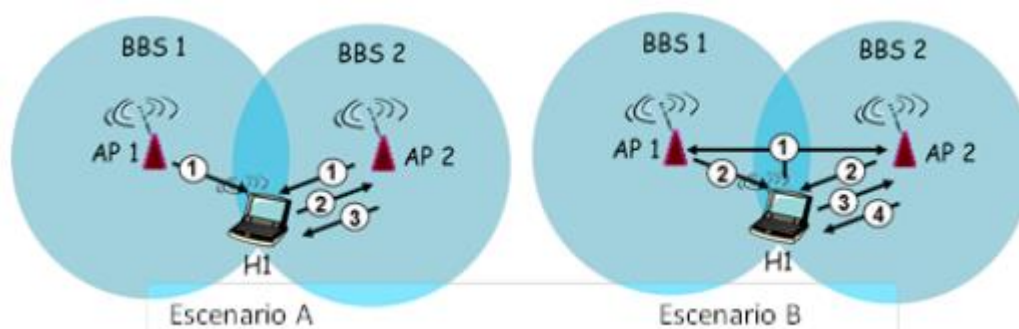
Vemos como el AP le responde a la petición de asociación anterior. La trama contiene la misma estructura que la Association Request.

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

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

Realizado en la cuestión 3

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



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

Transmisión de Datos

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

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

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

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

```
> Frame 158: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
▼ IEEE 802.11 QoS Null function (No data), Flags: ...P...TC
  Type/Subtype: QoS Null function (No data) (0x002c)
  ▼ Frame Control Field: 0xc811
    .... ..00 = Version: 0
    .... 10.. = Type: Data frame (2)
    1100 .... = Subtype: 12
  ▼ Flags: 0x11
    .... ..01 = DS status: Frame from STA to DS via an AP (To DS: 1 From DS: 0) (0x1)
    .... .0.. = More Fragments: This is the last fragment
    .... 0... = Retry: Frame is not being retransmitted
    ...1 .... = PWR MGT: STA will go to sleep
    ..0. .... = More Data: No data buffered
    .0.. .... = Protected flag: Data is not protected
    0... .... = Order flag: Not strictly ordered
    .000 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Destination address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Transmitter address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    Source address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    STA address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    .... .... 0000 = Fragment number: 0
    0101 1101 1001 .... = Sequence number: 1497
    Frame check sequence: 0xd7131018 [correct]
    [FCS Status: Good]
  > Qos Control: 0x0000
```

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

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

Direccionamiento

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

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

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

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

474	24.811093	192.168.1.109	128.119.245.12	TCP	110 2538 → 80 [SYN] Se
1011	32.808574	192.168.1.109	128.119.240.19	TCP	110 2541 → 80 [SYN] Se
1034	32.869262	192.168.1.109	128.119.240.19	TCP	110 2542 → 80 [SYN] Se
1119	32.957207	192.168.1.109	128.119.240.19	TCP	110 2544 → 80 [SYN] Se
1121	32.958198	192.168.1.109	128.119.240.19	TCP	110 2545 → 80 [SYN] Se
1142	32.981949	192.168.1.109	64.233.187.104	TCP	110 2546 → 80 [SYN] Se
1143	32.982315	192.168.1.109	64.233.187.104	TCP	110 [TCP Out-Of-Order]
1153	33.001575	192.168.1.109	128.119.240.19	TCP	110 2547 → 80 [SYN] Se
1262	33.099063	192.168.1.109	128.119.240.19	TCP	110 2548 → 80 [SYN] Se
1280	33.115208	192.168.1.109	128.119.240.19	TCP	110 2549 → 80 [SYN] Se

```
<
.... 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)
Destination address: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)
Transmitter address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
Source address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
STA address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
.... .... 0000 = Fragment number: 0
0000 0011 0001 .... = Sequence number: 49
Frame check sequence: 0xad57fce0 [correct]
[FCS Status: Good]
.. - - - - -
```

Imagen 18: Trama 474, receiver address, destination address y trasnmmitter address.

- ii. Correspondería a la Source address, que en este caso coincide con la Transmitter address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
 - iii. Destination address: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)
 - iv. La Receiver address: Cisco-Li_f7:1d:51
- b) ¿Cuáles es la dirección IP del host inalámbrico que envía este segmento? ¿y la dirección IP destino? ¿con que se corresponde esta dirección IP destino? (host, punto de acceso, router, o cualquier otro dispositivo de la red). Razona tu respuesta.
- i. Recordamos que nos encontramos en el frame #474. La IP desde la que se envía esta trama TCP es 192.168.1.109, y la IP de destino es 128.119.245.12.

tcp.flags==0x02 and wlan.fc.type==2					
No.	Time	Source	Destination	Protocol	Length
474	24.811093	192.168.1.109	128.119.245.12	TCP	110
1011	32.808574	192.168.1.109	128.119.240.19	TCP	110
1034	32.869262	192.168.1.109	128.119.240.19	TCP	110

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

Colisiones

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

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

wlan.fc.type_subtype==0x01c						
No.	Time	Source	Destination	Protocol	Length	Info
1601	46.595317		Linksys6_67:22:94 (00:06:...	802.11	38	Clear-to-send, Flags=.....C

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

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

```
> Frame 239: 84 bytes on wire (672 bits), 84 bytes captured (672 bits)
> AVS WLAN Capture header
> 802.11 radio information
▼ 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 1010 1010 = Duration: 170 microseconds
      Receiver address: HewlettP_33:a8:a5 (9c:8e:99:33:a8:a5)
      Transmitter address: CompalBr_4d:88:93 (5c:35:3b:4d:88:93)
```

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

Si buscamos tramas CTS encontramos la siguiente estructura en ellas:

```
> Frame 12: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
> AVS WLAN Capture header
> 802.11 radio information
▼ 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)
```

