

IEEE 802.11 con Wireshark

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

Comando usado: wlan.fc.type_subtype==8

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

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

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

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

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

The screenshot shows the Wireshark interface with a list of captured packets. The top pane displays a list of IEEE 802.11 Beacon frames from various sources (Cisco-Li_f7, LinksysG_67, Cisco-Li_f5). The middle pane shows the details of the selected frame (Frame 1: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits)). The bottom pane shows the raw packet data in hexadecimal and ASCII.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info	Tx rate	Channel	Frequency	Signal
1	0.000000	Cisco-Li_f7	Broadcast	802.11	183	Beacon frame, Src=2054, Prio=0, Flags=.....C, B1=100, SSID="30 Marroes St"	1.0	6.243798	-29 dBm	
3	0.005474	Cisco-Li_f7	Broadcast	802.11	183	Beacon frame, Src=2054, Prio=0, Flags=.....C, B1=100, SSID="30 Marroes St"	1.0	6.243798	-30 dBm	
4	0.187919	Cisco-Li_f7	Broadcast	802.11	183	Beacon frame, Src=2054, Prio=0, Flags=.....C, B1=100, SSID="30 Marroes St"	1.0	6.243798	-29 dBm	
9	0.290284	Cisco-Li_f7	Broadcast	802.11	183	Beacon frame, Src=2054, Prio=0, Flags=.....C, B1=100, SSID="30 Marroes St"	1.0	6.243798	-28 dBm	
10	0.294412	LinksysG_67	Broadcast	802.11	90	Beacon frame, Src=3074, Prio=0, Flags=.....C, B1=0, SSID="66e0b0a2273"	2.0	6.243798	-34 dBm	
11	0.391774	Cisco-Li_f7	Broadcast	802.11	183	Beacon frame, Src=2054, Prio=0, Flags=.....C, B1=100, SSID="30 Marroes St"	1.0	6.243798	-30 dBm	
13	0.409012	Cisco-Li_f7	Broadcast	802.11	183	Beacon frame, Src=2054, Prio=0, Flags=.....C, B1=100, SSID="30 Marroes St"	1.0	6.243798	-30 dBm	
14	0.499197	LinksysG_67	Broadcast	802.11	90	Beacon frame, Src=3074, Prio=0, Flags=.....C, B1=100, SSID="linksys12"	2.0	6.243798	-30 dBm	
15	0.507382	Cisco-Li_f7	Broadcast	802.11	183	Beacon frame, Src=2054, Prio=0, Flags=.....C, B1=100, SSID="30 Marroes St"	1.0	6.243798	-30 dBm	
16	0.601887	LinksysG_67	Broadcast	802.11	90	Beacon frame, Src=3074, Prio=0, Flags=.....C, B1=100, SSID="linksys12"	2.0	6.243798	-32 dBm	
17	0.699847	Cisco-Li_f7	Broadcast	802.11	183	Beacon frame, Src=2054, Prio=0, Flags=.....C, B1=100, SSID="30 Marroes St"	1.0	6.243798	-29 dBm	
18	0.802226	Cisco-Li_f7	Broadcast	802.11	183	Beacon frame, Src=2054, Prio=0, Flags=.....C, B1=100, SSID="30 Marroes St"	1.0	6.243798	-30 dBm	
19	0.906519	Cisco-Li_f7	Broadcast	802.11	183	Beacon frame, Src=2054, Prio=0, Flags=.....C, B1=100, SSID="30 Marroes St"	1.0	6.243798	-30 dBm	
20	1.007015	Cisco-Li_f7	Broadcast	802.11	183	Beacon frame, Src=2054, Prio=0, Flags=.....C, B1=100, SSID="30 Marroes St"	1.0	6.243798	-29 dBm	
21	1.010486	LinksysG_67	Broadcast	802.11	90	Beacon frame, Src=3074, Prio=0, Flags=.....C, B1=100, SSID="linksys12"	2.0	6.243798	-34 dBm	
22	1.109406	Cisco-Li_f7	Broadcast	802.11	183	Beacon frame, Src=2054, Prio=0, Flags=.....C, B1=100, SSID="30 Marroes St"	1.0	6.243798	-30 dBm	
23	1.113091	LinksysG_67	Broadcast	802.11	90	Beacon frame, Src=3080, Prio=0, Flags=.....C, B1=100, SSID="30 Marroes St"	1.0	6.243798	-93 dBm	
24	1.211841	Cisco-Li_f7	Broadcast	802.11	183	Beacon frame, Src=2054, Prio=0, Flags=.....C, B1=100, SSID="30 Marroes St"	1.0	6.243798	-30 dBm	
31	1.215667	LinksysG_67	Broadcast	802.11	90	Beacon frame, Src=3081, Prio=0, Flags=.....C, B1=100, SSID="linksys12"	2.0	6.243798	-93 dBm	
32	1.314223	Cisco-Li_f7	Broadcast	802.11	183	Beacon frame, Src=2054, Prio=0, Flags=.....C, B1=100, SSID="30 Marroes St"	1.0	6.243798	-28 dBm	
33	1.415993	Cisco-Li_f7	Broadcast	802.11	183	Beacon frame, Src=2054, Prio=0, Flags=.....C, B1=100, SSID="30 Marroes St"	1.0	6.243798	-29 dBm	
34	1.420545	LinksysG_67	Broadcast	802.11	90	Beacon frame, Src=3081, Prio=0, Flags=.....C, B1=20580, SSID="linksys12"	2.0	6.243798	-34 dBm	
35	1.510009	Cisco-Li_f7	Broadcast	802.11	183	Beacon frame, Src=2054, Prio=0, Flags=.....C, B1=100, SSID="30 Marroes St"	1.0	6.243798	-28 dBm	

Frame 1: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits)

Ethernet II Header, Src: Cisco-Li_f7:1d:51, Length: 1464

IEEE 802.11 Beacon frame, Flags:C

Type/Subtype: Beacon frame (0x0000)

Frame Control Field: 0x0000

Duration: 0x0000

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)

Seq. No: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)

Fragment number: 0

Sequence number: 2054

Frame check sequence: 0x00000000 (unverified)

[FCS Status: Unverified]

IEEE 802.11 Wireless Management

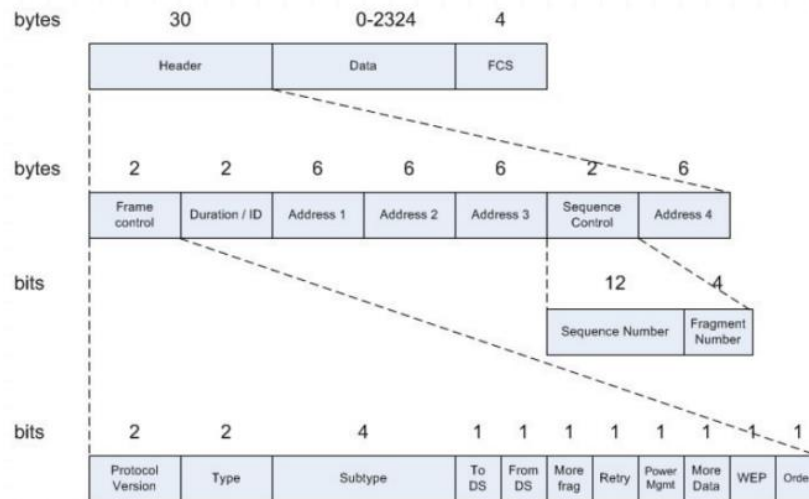
Hay 33 APs

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

No.	Time	Source	Destination	Protocol	Length	Info	Traps	Channel	Frequency	Signal
27.0.015084		Cisco-9b:54:...	Broadcast	802.11	252	Beacon frame, SN=1154, FN=0, Flags=.....C, SSID="alumnos"	11.0	1.241290	-79 dBm	
30.0.015086		Cisco-9b:54:...	Broadcast	802.11	252	Beacon frame, SN=1213, FN=0, Flags=.....C, SSID="alumnos"	11.0	1.241290	-79 dBm	
40.0.020889		Cisco-9b:54:...	Broadcast	802.11	252	Beacon frame, SN=1213, FN=0, Flags=.....C, SSID="alumnos"	11.0	1.241290	-36 dBm	
50.0.020894		Cisco-9b:54:...	Broadcast	802.11	252	Beacon frame, SN=1175, FN=0, Flags=.....C, SSID="alumnos"	11.0	1.241290	-79 dBm	
58.0.030051		Cisco-9b:54:...	Broadcast	802.11	252	Beacon frame, SN=1232, FN=0, Flags=.....C, SSID="alumnos"	11.0	1.241290	-77 dBm	
61.0.031099		Cisco-9b:54:...	Broadcast	802.11	252	Beacon frame, SN=1214, FN=0, Flags=.....C, SSID="alumnos"	11.0	1.241290	-36 dBm	
62.0.031071		Cisco-9b:54:...	Broadcast	802.11	248	Beacon frame, SN=1030, FN=0, Flags=.....C, SSID="alumnos"	11.0	1.241290	-61 dBm	
77.0.040232		Cisco-9b:54:...	Broadcast	802.11	248	Beacon frame, SN=1176, FN=0, Flags=.....C, SSID="pas"	11.0	1.241290	-79 dBm	
68.0.042709		Cisco-9b:54:...	Broadcast	802.11	248	Beacon frame, SN=1236, FN=0, Flags=.....C, SSID="pas"	11.0	1.241290	-79 dBm	
95.0.181702		Cisco-9b:54:...	Broadcast	802.11	248	Beacon frame, SN=1199, FN=0, Flags=.....C, SSID="pas"	11.0	1.241290	-79 dBm	
96.0.185208		Cisco-9b:54:...	Broadcast	802.11	252	Beacon frame, SN=1039, FN=0, Flags=.....C, SSID="alumnos"	11.0	1.241290	-66 dBm	
99.0.185218		Cisco-9b:54:...	Broadcast	802.11	248	Beacon frame, SN=1052, FN=0, Flags=.....C, SSID="pas"	11.0	1.241290	-71 dBm	
102.0.188817		Cisco-9b:54:...	Broadcast	802.11	248	Beacon frame, SN=1222, FN=0, Flags=.....C, SSID="pas"	11.0	1.241290	-36 dBm	
109.0.197783		Cisco-9b:54:...	Broadcast	802.11	252	Beacon frame, SN=1086, FN=0, Flags=.....C, SSID="alumnos"	11.0	1.241290	-79 dBm	
111.0.198596		Cisco-9b:54:...	Broadcast	802.11	248	Beacon frame, SN=1042, FN=0, Flags=.....C, SSID="pas"	11.0	1.241290	-59 dBm	
114.0.201099		Cisco-9b:54:...	Broadcast	802.11	252	Beacon frame, SN=1223, FN=0, Flags=.....C, SSID="alumnos"	11.0	1.241290	-35 dBm	
129.0.220137		Cisco-9b:54:...	Broadcast	802.11	252	Beacon frame, SN=1081, FN=0, Flags=.....C, SSID="alumnos"	11.0	1.241290	-79 dBm	
130.0.223205		Cisco-9b:54:...	Broadcast	802.11	252	Beacon frame, SN=1205, FN=0, Flags=.....C, SSID="alumnos"	11.0	1.241290	-77 dBm	
139.0.309613		Cisco-9b:54:...	Broadcast	802.11	133	Beacon frame, SN=1180, FN=0, Flags=.....C, SSID="alumnos"	1.0	1.241290	-61 dBm	
144.0.374956		Cisco-9b:54:...	Broadcast	802.11	133	Beacon frame, SN=1332, FN=0, Flags=.....C, SSID="USAP_M"	1.0	1.241290	-68 dBm	
148.0.377756		Cisco-9b:54:...	Broadcast	802.11	252	Beacon frame, SN=1054, FN=0, Flags=.....C, SSID="alumnos"	11.0	1.241290	-66 dBm	
151.0.388395		Cisco-9b:54:...	Broadcast	802.11	248	Beacon frame, SN=1239, FN=0, Flags=.....C, SSID="pas"	11.0	1.241290	-79 dBm	
163.0.540147		Cisco-9b:54:...	Broadcast	802.11	252	Beacon frame, SN=1264, FN=0, Flags=.....C, SSID="alumnos"	11.0	1.241290	-79 dBm	

802.11 Local

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



2A. (Para Wireshark_802_11 y Wireshark_802_11LOCAL) ¿En la captura, hay alguna estación que realice un escaneo activo? ¿Hay APs que respondan? ¿Qué tipos de tramas son? (Consulta e indica el valor del campo tipo).

Wireshark_802_11

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

48 2.237689	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54 QoS Null function (No data), SN=1487, FN=0, Flags=...P...TC
49 2.237786	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f (00:13:00:00:00:00)	802.11	38 Acknowledgement, Flags=.....C
50 2.207613	IntelCor_Li_f7:1d:51	Broadcast	802.11	79 Probe Request, SN=276, FN=0, Flags=.....C, SSID="Home WiFi"
51 2.308697	Cisco-Li_f7:1d:51	IntelCor_Li_f7:1d:51	802.11	177 Probe Response, SN=2878, FN=0, Flags=.....R...C, BI=100, SSID="30 Munroe St"
52 2.382191	Cisco-Li_f7:1d:51	IntelCor_Li_f7:1d:51	802.11	177 Probe Response, SN=2878, FN=0, Flags=.....R...C, BI=100, SSID="30 Munroe St"
53 2.384063	Cisco-Li_f7:1d:51	IntelCor_Li_f7:1d:51	802.11	177 Probe Response, SN=2878, FN=0, Flags=.....R...C, BI=100, SSID="30 Munroe St"

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

Wireshark_802_11_LOCAL

Tenemos hasta 8 estaciones que realizan escaneos activos.

18430	22.377093	ASUSTek_56:d3:99	Cisco_1b:d2:62	802.11	53 Null function (No data), SN=98, FN=0, Flags=...P...TC
12340	15.128219	HewlettP_d1:04:83	Broadcast	802.11	82 Probe Request, SN=1183, FN=0, Flags=.....C, SSID="Red wifi MatAp"
8102	10.063376	HewlettP_54:cb:7c	Broadcast	802.11	90 Probe Request, SN=1315, FN=0, Flags=.....C, SSID="FTE-B105"
8114	10.079555	HewlettP_54:cb:7c	Broadcast	802.11	90 Probe Request, SN=1316, FN=0, Flags=.....C, SSID="FTE-B105"
8136	10.115964	HewlettP_54:cb:7c	Broadcast	802.11	90 Probe Request, SN=1318, FN=0, Flags=.....C, SSID="FTE-B105"
16754	20.261517	HewlettP_54:cb:7c	Broadcast	802.11	90 Probe Request, SN=1341, FN=0, Flags=.....C, SSID="FTE-B105"
16791	20.298477	HewlettP_54:cb:7c	Broadcast	802.11	90 Probe Request, SN=1343, FN=0, Flags=.....C, SSID="FTE-B105"
6180	7.895536	MurataWa_56:bf:1e	Broadcast	802.11	294 Probe Request, SN=2, FN=0, Flags=.....C, SSID=wildcard (Broadcast)
13217	16.046146	HTC_83:a1:a7	Broadcast	802.11	99 Probe Request, SN=2038, FN=0, Flags=.....C, SSID=wildcard (Broadcast)
5187	6.905003	HonHaiPr_7e:b7:25	Broadcast	802.11	71 Probe Request, SN=2886, FN=0, Flags=.....C, SSID=wildcard (Broadcast)
16337	19.714248	SamsungE_c3:c4:19	Broadcast	802.11	293 Probe Request, SN=3, FN=0, Flags=.....C, SSID="WLAN_2CES"
5807	6.794017	Apple_3a:5d:96	Broadcast	802.11	92 Probe Request, SN=3677, FN=0, Flags=.....C, SSID="CIC-IPW"
16351	19.735677	SamsungE_c3:c4:19	Broadcast	802.11	293 Probe Request, SN=4, FN=0, Flags=.....C, SSID="WLAN_2CES"
18079	21.952146	ASUSTek_56:d3:99	Broadcast	802.11	145 Probe Request, SN=81, FN=0, Flags=.....C, SSID=wildcard (Broadcast)
18119	21.972567	ASUSTek_56:d3:99	Broadcast	802.11	145 Probe Request, SN=82, FN=0, Flags=.....C, SSID=wildcard (Broadcast)
15649	18.847555	Cisco_1b:d5:01	HonHaiPr_c2:e3:2b	802.11	246 Probe Response, SN=1440, FN=0, Flags=.....C, BI=100, SSID="eduroam"
15650	18.849048	Cisco_1b:d5:02	HonHaiPr_c2:e3:2b	802.11	246 Probe Response, SN=1441, FN=0, Flags=.....C, BI=100, SSID="alumnos"
15652	18.854979	Cisco_1b:d5:05	HonHaiPr_c2:e3:2b	802.11	242 Probe Response, SN=1443, FN=0, Flags=.....C, BI=100, SSID="pdi"
5190	6.919555	Cisco_a9:50:a1	HonHaiPr_7e:b7:25	802.11	246 Probe Response, SN=1600, FN=0, Flags=.....C, BI=100, SSID="eduroam"
5194	6.921403	Cisco_a9:50:a1	HonHaiPr_7e:b7:25	802.11	246 Probe Response, SN=1600, FN=0, Flags=.....R...C, BI=100, SSID="eduroam"
5196	6.922638	Cisco_a9:50:a2	HonHaiPr_7e:b7:25	802.11	246 Probe Response, SN=1601, FN=0, Flags=.....C, BI=100, SSID="alumnos"
5197	6.923208	Cisco_a9:50:a2	HonHaiPr_7e:b7:25	802.11	246 Probe Response, SN=1601, FN=0, Flags=.....R...C, BI=100, SSID="alumnos"
5199	6.924505	Cisco_a9:50:a4	HonHaiPr_7e:b7:25	802.11	246 Probe Response, SN=1602, FN=0, Flags=.....C, BI=100, SSID="Wifiluma"
5202	6.925694	Cisco_a9:50:a4	HonHaiPr_7e:b7:25	802.11	246 Probe Response, SN=1602, FN=0, Flags=.....R...C, BI=100, SSID="Wifiluma"
5204	6.927518	Cisco_a9:50:a5	HonHaiPr_7e:b7:25	802.11	242 Probe Response, SN=1603, FN=0, Flags=.....C, BI=100, SSID="ndi"

Se adjuntan algunas de ellas

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

Tramas 50 y 51 en por ejemplo Wireshark_802_11

50	2.297613	IntelCor_1f:57:13	Broadcast	802.11	79 Probe Request, SN=576, FN=0, F
51	2.300697	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177 Probe Response, SN=2878, FN=0,
52	2.302191	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177 Probe Response, SN=2878, FN=0,

> Frame 50: 79 bytes on wire (632 bits), 79 bytes captured (632 bits)

> Radiotap Header v0, Length 24

> 802.11 radio information

▼ IEEE 802.11 Probe Request, Flags:C

Type/Subtype: Probe Request (0x0004)

> Frame Control Field: 0x4000

.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 0100 0000 = Sequence number: 576

Frame check sequence: 0xa373c5ff [unverified]

[FCS Status: Unverified]

Probe Request

50	2.297613	IntelCor_1f:57:13	Broadcast	802.11	79 Probe Request, SN=576, FN=0, F
51	2.300697	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177 Probe Response, SN=2878, FN=0,
52	2.302191	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177 Probe Response, SN=2878, FN=0,

> Frame 51: 177 bytes on wire (1416 bits), 177 bytes captured (1416 bits)

> Radiotap Header v0, Length 24

> 802.11 radio information

▼ IEEE 802.11 Probe Response, Flags:C

Type/Subtype: Probe Response (0x0005)

> Frame Control Field: 0x5000

.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 0011 1110 = Sequence number: 2878

Frame check sequence: 0x6e0851bb [unverified]

[FCS Status: Unverified]

> IEEE 802.11 Wireless Management

Probe Response

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

wlan.fc.type_subtype==0x0000														
No.	Time	Source	Destination	Protocol	Length	Info					Tx rate	Channel	Frequency	Signal
1227	33.079714	d1:b6:4f:00...	MS-NLB-Phys...	802.11	111	Association Request, SN=1607, FN=0, Flags=.....C, SSID="linksys_SES_24...	0.0			6	2437MHz	-35 dBm		
1750	49.651078	IntelCor_d1...	Cisco-Li_f5...	802.11	107	Association Request, SN=1607, FN=0, Flags=.....C, SSID="linksys_SES_24...	1.0			6	2437MHz	-25 dBm		
1751	49.653218	IntelCor_d1...	Cisco-Li_f5...	802.11	107	Association Request, SN=1607, FN=0, Flags=.....R...C, SSID="linksys_SES_24...	1.0			6	2437MHz	-25 dBm		
1824	53.789944	IntelCor_d1...	Cisco-Li_f5...	802.11	107	Association Request, SN=1613, FN=0, Flags=.....C, SSID="linksys_SES_24...	1.0			6	2437MHz	-26 dBm		
1825	53.790943	IntelCor_d1...	Cisco-Li_f5...	802.11	107	Association Request, SN=1613, FN=0, Flags=.....R...C, SSID="linksys_SES_24...	1.0			6	2437MHz	-25 dBm		
1827	53.793568	IntelCor_d1...	Cisco-Li_f5...	802.11	107	Association Request, SN=1613, FN=0, Flags=.....C, SSID="linksys_SES_24...	1.0			6	2437MHz	-25 dBm		
1926	57.903699	IntelCor_d1...	Cisco-Li_f5...	802.11	107	Association Request, SN=1620, FN=0, Flags=.....C, SSID="linksys_SES_24...	1.0			6	2437MHz	-26 dBm		
1927	57.904945	IntelCor_d1...	Cisco-Li_f5...	802.11	107	Association Request, SN=1620, FN=0, Flags=.....R...C, SSID="linksys_SES_24...	1.0			6	2437MHz	-26 dBm		
1932	57.911195	IntelCor_d1...	Cisco-Li_f5...	802.11	107	Association Request, SN=1620, FN=0, Flags=.....R...C, SSID="linksys_SES_24...	1.0			6	2437MHz	-26 dBm		
1933	57.915945	IntelCor_d1...	Cisco-Li_f5...	802.11	107	Association Request, SN=1620, FN=0, Flags=.....R...C, SSID="linksys_SES_24...	1.0			6	2437MHz	-26 dBm		
1934	57.924199	IntelCor_d1...	Cisco-Li_f5...	802.11	107	Association Request, SN=1620, FN=0, Flags=.....R...C, SSID="linksys_SES_24...	1.0			6	2437MHz	-26 dBm		
1935	57.936216	IntelCor_d1...	Cisco-Li_f5...	802.11	107	Association Request, SN=1620, FN=0, Flags=.....R...C, SSID="linksys_SES_24...	1.0			6	2437MHz	-27 dBm		
1937	57.939196	IntelCor_d1...	Cisco-Li_f5...	802.11	107	Association Request, SN=1620, FN=0, Flags=.....C, SSID="linksys_SES_24...	1.0			6	2437MHz	-26 dBm		
2126	62.176945	IntelCor_d1...	Cisco-Li_f5...	802.11	107	Association Request, SN=1645, FN=0, Flags=.....C, SSID="linksys_SES_24...	1.0			6	2437MHz	-26 dBm		
2127	62.178194	IntelCor_d1...	Cisco-Li_f5...	802.11	107	Association Request, SN=1645, FN=0, Flags=.....R...C, SSID="linksys_SES_24...	1.0			6	2437MHz	-26 dBm		
2162	63.169910	IntelCor_d1...	Cisco-Li_f7...	802.11	89	Association Request, SN=1648, FN=0, Flags=.....C, SSID="30 Munroe St"	54.0			6	2437MHz	-29 dBm		
2307	70.179949	Cisco-Li_f5...	f9:ff:ff:ff...	802.11	132	Fragmented IEEE 802.11 frame	1.0			6	2437MHz	-93 dBm		

Filtramos con wlan.fc.type_subtype==0x0000

```
IEEE 802.11 Association Request, Flags: .....C
Type/Subtype: Association Request (0x0000)
> Frame Control Field: 0x0000
  .000 0001 0011 1010 = Duration: 314 microseconds
Receiver address: Cisco-Li_f5:ba:bb (00:18:39:f5:ba:bb)
Destination address: Cisco-Li_f5:ba:bb (00:18:39:f5:ba:bb)
Transmitter address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
Source address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
BSS Id: Cisco-Li_f5:ba:bb (00:18:39:f5:ba:bb)
.... .. 0000 = Fragment number: 0
0110 0100 0111 .... = Sequence number: 1607
Frame check sequence: 0x4432d6cf [unverified]
[FCS Status: Unverified]
IEEE 802.11 Wireless Management
> Fixed parameters (4 bytes)
> Tagged parameters (51 bytes)
```

Ejemplo de contenido de la trama

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

wlan.fc.type_subtype==0x0000 wlan.fc.type_subtype==0x0001													
No.	Time	Source	Destination	Protocol	Length	Info				Tx rate	Channel	Frequency	Signal
1227	33.079714	d1:b6:4f:00...	MS-NLB-Phys...	802.11	111	Association Request, SN=3775, FN=4, Flags=..pm...F.C				0.0		6 2437MHz	-35 dBm
1750	49.651078	IntelCor_d1...	Cisco-Li_f5...	802.11	107	Association Request, SN=1607, FN=0, Flags=.....C, SSID="linksys_SES_24..."				1.0		6 2437MHz	-25 dBm
1751	49.653218	IntelCor_d1...	Cisco-Li_f5...	802.11	107	Association Request, SN=1607, FN=0, Flags=.....R...C, SSID="linksys_SES_24..."				1.0		6 2437MHz	-25 dBm
1824	53.789944	IntelCor_d1...	Cisco-Li_f5...	802.11	107	Association Request, SN=1613, FN=0, Flags=.....C, SSID="linksys_SES_24..."				1.0		6 2437MHz	-26 dBm
1825	53.790943	IntelCor_d1...	Cisco-Li_f5...	802.11	107	Association Request, SN=1613, FN=0, Flags=.....R...C, SSID="linksys_SES_24..."				1.0		6 2437MHz	-25 dBm
1827	53.793568	IntelCor_d1...	Cisco-Li_f5...	802.11	107	Association Request, SN=1613, FN=0, Flags=.....C, SSID="linksys_SES_24..."				1.0		6 2437MHz	-25 dBm
1926	57.903699	IntelCor_d1...	Cisco-Li_f5...	802.11	107	Association Request, SN=1620, FN=0, Flags=.....C, SSID="linksys_SES_24..."				1.0		6 2437MHz	-26 dBm
1927	57.904945	IntelCor_d1...	Cisco-Li_f5...	802.11	107	Association Request, SN=1620, FN=0, Flags=.....R...C, SSID="linksys_SES_24..."				1.0		6 2437MHz	-26 dBm
1932	57.911195	IntelCor_d1...	Cisco-Li_f5...	802.11	107	Association Request, SN=1620, FN=0, Flags=.....R...C, SSID="linksys_SES_24..."				1.0		6 2437MHz	-26 dBm
1933	57.915945	IntelCor_d1...	Cisco-Li_f5...	802.11	107	Association Request, SN=1620, FN=0, Flags=.....R...C, SSID="linksys_SES_24..."				1.0		6 2437MHz	-26 dBm
1934	57.924199	IntelCor_d1...	Cisco-Li_f5...	802.11	107	Association Request, SN=1620, FN=0, Flags=.....R...C, SSID="linksys_SES_24..."				1.0		6 2437MHz	-26 dBm
1935	57.936216	IntelCor_d1...	Cisco-Li_f5...	802.11	107	Association Request, SN=1620, FN=0, Flags=.....R...C, SSID="linksys_SES_24..."				1.0		6 2437MHz	-27 dBm
1937	57.939196	IntelCor_d1...	Cisco-Li_f5...	802.11	107	Association Request, SN=1620, FN=0, Flags=.....C, SSID="linksys_SES_24..."				1.0		6 2437MHz	-26 dBm
2126	62.176945	IntelCor_d1...	Cisco-Li_f5...	802.11	107	Association Request, SN=1645, FN=0, Flags=.....C, SSID="linksys_SES_24..."				1.0		6 2437MHz	-26 dBm
2127	62.178194	IntelCor_d1...	Cisco-Li_f5...	802.11	107	Association Request, SN=1645, FN=0, Flags=.....R...C, SSID="linksys_SES_24..."				1.0		6 2437MHz	-26 dBm
2162	63.169910	IntelCor_d1...	Cisco-Li_f7...	802.11	89	Association Request, SN=1648, FN=0, Flags=.....C, SSID="30 Munroe St"				54.0		6 2437MHz	-29 dBm
2166	63.192101	Cisco-Li_f7...	IntelCor_d1...	802.11	94	Association Response, SN=3728, FN=0, Flags=.....C				1.0		6 2437MHz	-31 dBm
2307	70.179949	Cisco-Li_f5...	f9:ff:ff:ff...	802.11	132	Fragmented IEEE 802.11 frame				1.0		6 2437MHz	-93 dBm

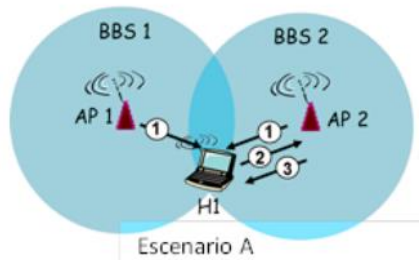
Filtramos por wlan.fc.type_subtype==0x0000 || wlan.fc.type_subtype==0x0001

```
IEEE 802.11 Association Request, Flags: .....C
Type/Subtype: Association Request (0x0000)
> Frame Control Field: 0x0000
  .000 0000 0010 1100 = Duration: 44 microseconds
Receiver address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
Destination address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
Transmitter address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
Source address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
.... .. 0000 = Fragment number: 0
0110 0111 0000 .... = Sequence number: 1648
Frame check sequence: 0xf3badc6 [unverified]
[FCS Status: Unverified]
IEEE 802.11 Wireless Management
> Fixed parameters (4 bytes)
> Tagged parameters (33 bytes)
  > Tag: SSID parameter set: "30 Munroe St"
  > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18, [Mbit/sec]
  > Tag: QoS Capability
  > Tag: Extended Supported Rates 24(B), 36, 48, 54, [Mbit/sec]
IEEE 802.11 Association Response, Flags: .....C
Type/Subtype: Association Response (0x0001)
> Frame Control Field: 0x1000
  .000 0001 0011 1010 = Duration: 314 microseconds
Receiver address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
Destination address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
Source address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
.... .. 0000 = Fragment number: 0
1110 1001 0000 .... = Sequence number: 3728
Frame check sequence: 0x37f2ab2b [unverified]
[FCS Status: Unverified]
IEEE 802.11 Wireless Management
> Fixed parameters (6 bytes)
> Tagged parameters (36 bytes)
  > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
  > Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
  > Tag: EDCA Parameter Set
```

Trama Association Request

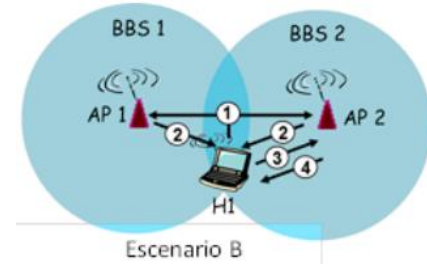
Trama Association Response

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



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

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



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

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

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

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

```

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

Trama QoS

```

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

Trama ACK de confirmación

5C. Localiza en la captura Wireshark_802_11LOCAL alguna trama de datos NULL Muestra la estructura y contenido de esta trama. ¿Qué la diferencia de las tramas de datos normales? ¿Para qué sirve?

```
> 802.11 radio information
▼ IEEE 802.11 Null function (No data), Flags: ....R.FTC
  Type/Subtype: Null function (No data) (0x0024)
  ▼ Frame Control Field: 0x480b
    ....00 = Version: 0
    ....10.. = Type: Data frame (2)
    0100 .... = Subtype: 4
    > Flags: 0x0b
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: Cisco_43:9f:60 (00:13:80:43:9f:60)
    Transmitter address: Cisco-Li_72:e1:78 (00:14:bf:72:e1:78)
    Destination address: Cisco_43:9f:60 (00:13:80:43:9f:60)
    Source address: Cisco-Li_72:e1:78 (00:14:bf:72:e1:78)
    .... .... 0000 = Fragment number: 0
    1111 0110 1001 .... = Sequence number: 3945
    Frame check sequence: 0xf3aace2 [unverified]
    [FCS Status: Unverified]
```

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

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

6A. ¿Cuáles son las tres direcciones MAC de esta trama? ¿Cuál es la dirección MAC correspondiente al host inalámbrico desde el que se hace la petición? (representación hexadecimal) ¿Cuál la del punto de acceso? ¿y la del (primer) router?

No.	Time	Source	Destination	Protocol	Length	Info	Tx rate	Channel	Frequency	Signal
480	24.828253	192.168.1.109	128.119.245...	HTTP	537	GET /wireshark-labs/alice.txt HTTP/1.1	48.0	6	243.794Hz	-38 dBm
868	25.126724	128.119.245...	192.168.1.109	HTTP	400	HTTP/1.1 200 OK (text/plain)	48.0	6	243.794Hz	-36 dBm
873	25.185381	192.168.1.109	128.119.245...	HTTP	444	GET /favicon.ico HTTP/1.1	54.0	6	243.794Hz	-38 dBm
875	25.209241	128.119.245...	192.168.1.109	HTTP	1527	HTTP/1.1 404 Not Found	48.0	6	243.794Hz	-38 dBm
1016	32.825992	192.168.1.109	128.119.240...	HTTP	512	GET / HTTP/1.1	54.0	6	243.794Hz	-24 dBm
1055	32.892394	192.168.1.109	128.119.240...	HTTP	484	GET /includes/cweb.css HTTP/1.1	48.0	6	243.794Hz	-23 dBm
1062	32.903631	192.168.1.109	128.119.101.5	HTTP	440	GET /favicon.ico HTTP/1.1	48.0	6	243.794Hz	-22 dBm
1066	32.909945	128.119.240...	192.168.1.109	HTTP	464	HTTP/1.1 200 OK (text/html)	48.0	6	243.794Hz	-34 dBm
1098	32.939761	128.119.240...	192.168.1.109	HTTP	333	HTTP/1.1 200 OK (text/css)	54.0	6	243.794Hz	-38 dBm
1119	32.946889	128.119.101.5	192.168.1.109	HTTP	753	HTTP/1.1 200 OK (image/x-icon)	54.0	6	243.794Hz	-36 dBm
1117	32.956076	192.168.1.109	128.119.101.5	HTTP	509	GET /unhome/identity/top_strip/un_formal_lgrey.gif HTTP/1.1	54.0	6	243.794Hz	-24 dBm
1129	32.977250	128.119.101.5	192.168.1.109	HTTP	1490	HTTP/1.1 200 OK (GIF89a)	48.0	6	243.794Hz	-34 dBm
1140	32.980813	192.168.1.109	128.119.240...	HTTP	484	GET /images/spacer.gif HTTP/1.1	54.0	6	243.794Hz	-25 dBm
1169	33.022167	192.168.1.109	128.119.240...	HTTP	494	GET /images/cshling_entrance.jpg HTTP/1.1	54.0	6	243.794Hz	-24 dBm
1183	33.032012	192.168.1.109	64.233.187...	HTTP	468	GET /urchin.js HTTP/1.1	54.0	6	243.794Hz	-24 dBm

Filtramos por http y la primera trama será la que buscamos

```
▼ IEEE 802.11 QoS Data, Flags: .....TC
  Type/Subtype: QoS Data (0x0028)
  > Frame Control Field: 0x8801
    .000 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Transmitter address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    Destination address: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)
    Source address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    STA address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    .... .... 0000 = Fragment number: 0
    0000 0011 0011 .... = Sequence number: 51
    Frame check sequence: 0x147e6bd9 [unverified]
    [FCS Status: Unverified]
  ▼ QoS Control: 0x0000
    .... .... 0000 = TID: 0
    [.... .... 0000 = Priority: Best Effort (Best Effort) (0)]
    .... .... 00.. = QoS bit 4: Bits 8-15 of QoS Control field are TXOP Duration Requested
    .... .... 00.. = Ack Policy: Normal Ack (0x0)
    .... .... 0... = Payload Type: MSDU
    0000 0000 .... .... = TXOP Duration Requested: 0 (no TXOP requested)
```

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

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

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

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

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

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

6B. ¿Cuál es la dirección IP del host inalámbrico que envía este segmento? ¿y la dirección IP destino? ¿con que se corresponde esta dirección IP destino? (host, punto de acceso, router, o cualquier otro dispositivo de la red). Razona tu respuesta.

Time	Source	Destination	Protocol	Length	Info
480.24.828253	192.168.1.109	128.119.245.12	HTTP	537	GET /wireshark-labs/alice.txt HTTP/1.1

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

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

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

Solo tenemos una trama que es CTS.

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

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

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

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

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