

Práctica con WhireShark II

Antonio J. Galán Herrera



Índice

Cuestión 1	2
Ejercicio 1	4
Cuestión 2*	6
Ejercicio 2	8
Cuestión 3	9
Ejercicio 3	11
Cuestión 4	11
Cuestión 5	12
Ejercicio 4	15
Ejercicio 5	16
Cuestión 6	19
Cuestión 7	21
Cuestión 8	23

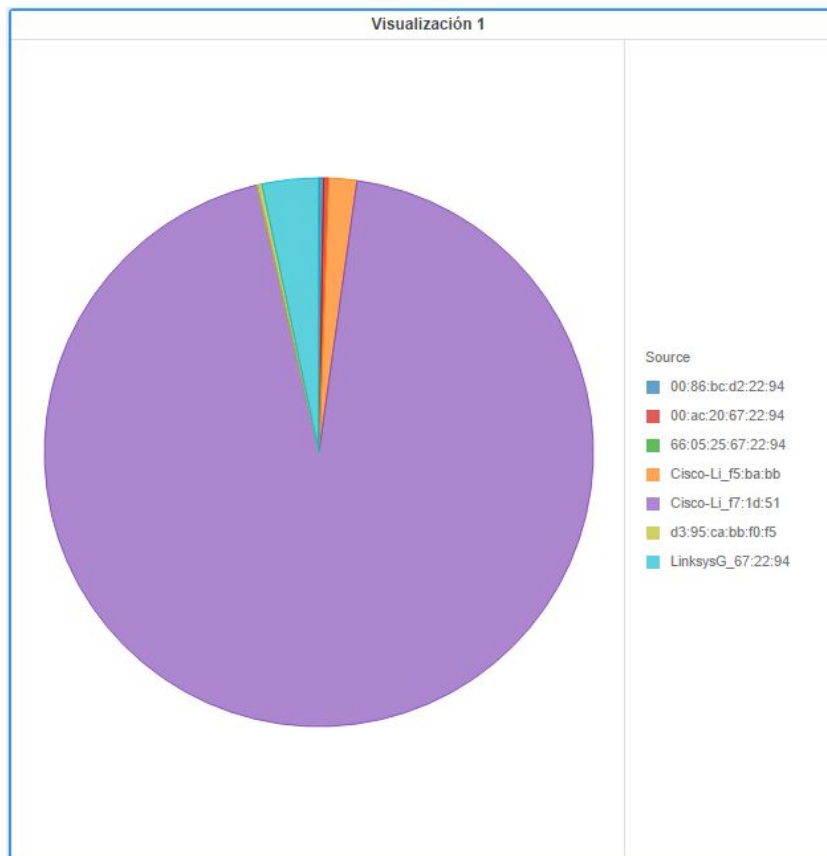
Cuestión 1

Localiza las tramas Beacon en las trazas [Whireshark_802_11.pcapng](#) y [Whireshark_802_11_LOCAL.pcapng](#).

1. ¿Cuántos APs están en la cobertura de la estación desde la que se realizó la captura? ¿Cuáles son sus identificadores
2. ¿Cada cuanto tiempo se envía una trama de Beacon? ¿Qué tipo de trama es? Indica el valor de campo tipo.

Traza [Whireshark_802_11.pcapng](#).

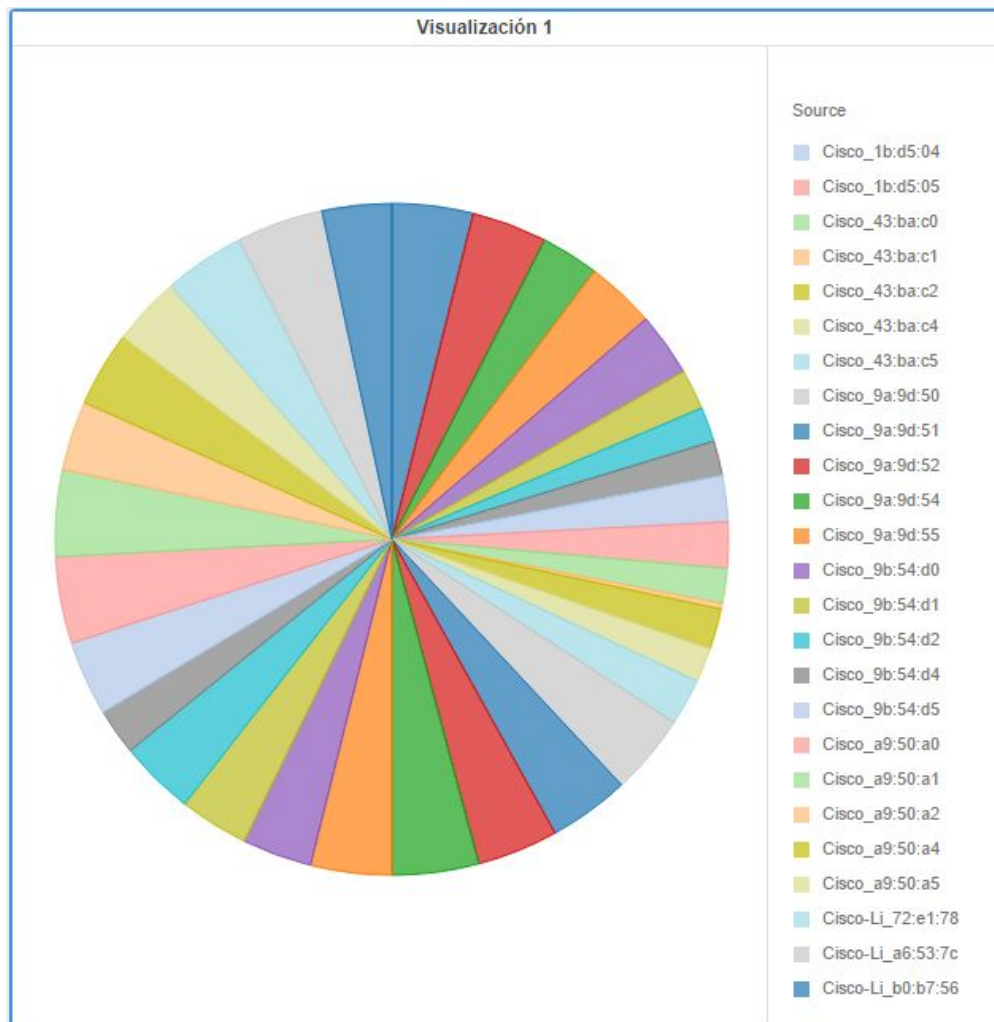
1. En la traza hay 7 APs (Access Points), correspondientes a las diferentes fuentes de la traza. Esta es la proporción de envío de tramas de dichas fuentes, junto a sus identificadores:



-
2. Las tramas se envían cada 0,1 segundos aproximadamente.

Traza [Whreshark_802_11_LOCAL.pcapng](#).

1. En la traza hay 33 APs (Access Points), correspondientes a las distintas fuentes de la traza. Esta es la proporción de envío de tramas de dichas fuentes, junto a sus identificadores:



2. Las tramas se envían cada 0,1 segundos aproximadamente.

Ejercicio 1

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

Traza [Wireshark_802_11.pcapng](#).

Wireshark_802_11.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

wlan[0] == 0x80

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2854, FN=0, Flags=..
3	0.085474	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2855, FN=0, Flags=..
4	0.187919	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2856, FN=0, Flags=..
9	0.290284	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2857, FN=0, Flags=..
10	0.294432	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3072, FN=0, Flags=..
11	0.303174	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2858, FN=0, Flags=..

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

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

Duración

Direcciones

Control de secuencia

FCS (Frame Check Secuencia)

Traza Whireshark_802_11_LOCAL.pcapng.

Wireshark_802_11_LOCAL.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Filter: wlan[0] == 0x80

No.	Time	Source	Destination	Protocol	Length	Info
27	0.015804	Cisco_9b:54:d2	Broadcast	802.11	252	Beacon frame, SN=3154, FN=0, Flags=..
36	0.019646	Cisco_1b:d2:62	Broadcast	802.11	252	Beacon frame, SN=2231, FN=0, Flags=..
40	0.020889	Cisco_a9:50:a2	Broadcast	802.11	252	Beacon frame, SN=1213, FN=0, Flags=..
56	0.028304	Cisco_9b:54:d4	Broadcast	802.11	252	Beacon frame, SN=3175, FN=0, Flags=..
58	0.030931	Cisco_1b:d2:64	Broadcast	802.11	252	Beacon frame, SN=2232, FN=0, Flags=..

< 802.11 radio information

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

0000 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:d2 (00:14:1c:9b:54:d2)

Source address: Cisco_9b:54:d2 (00:14:1c:9b:54:d2)

BSS Id: Cisco_9b:54:d2 (00:14:1c:9b:54:d2)

- 0000 = Fragment number: 0
- 1100 0101 0010 = Sequence number: 3154
- Frame check sequence: 0xa4ea1823 [correct]
- [FCS Status: Good]

> IEEE 802.11 wireless LAN

Duración

Direcciones

Control de secuencia

FCS (Frame Check Sequence)

Cuestión 2*

1. ¿Hay alguna estación que realice un escaneo activo en la captura*?

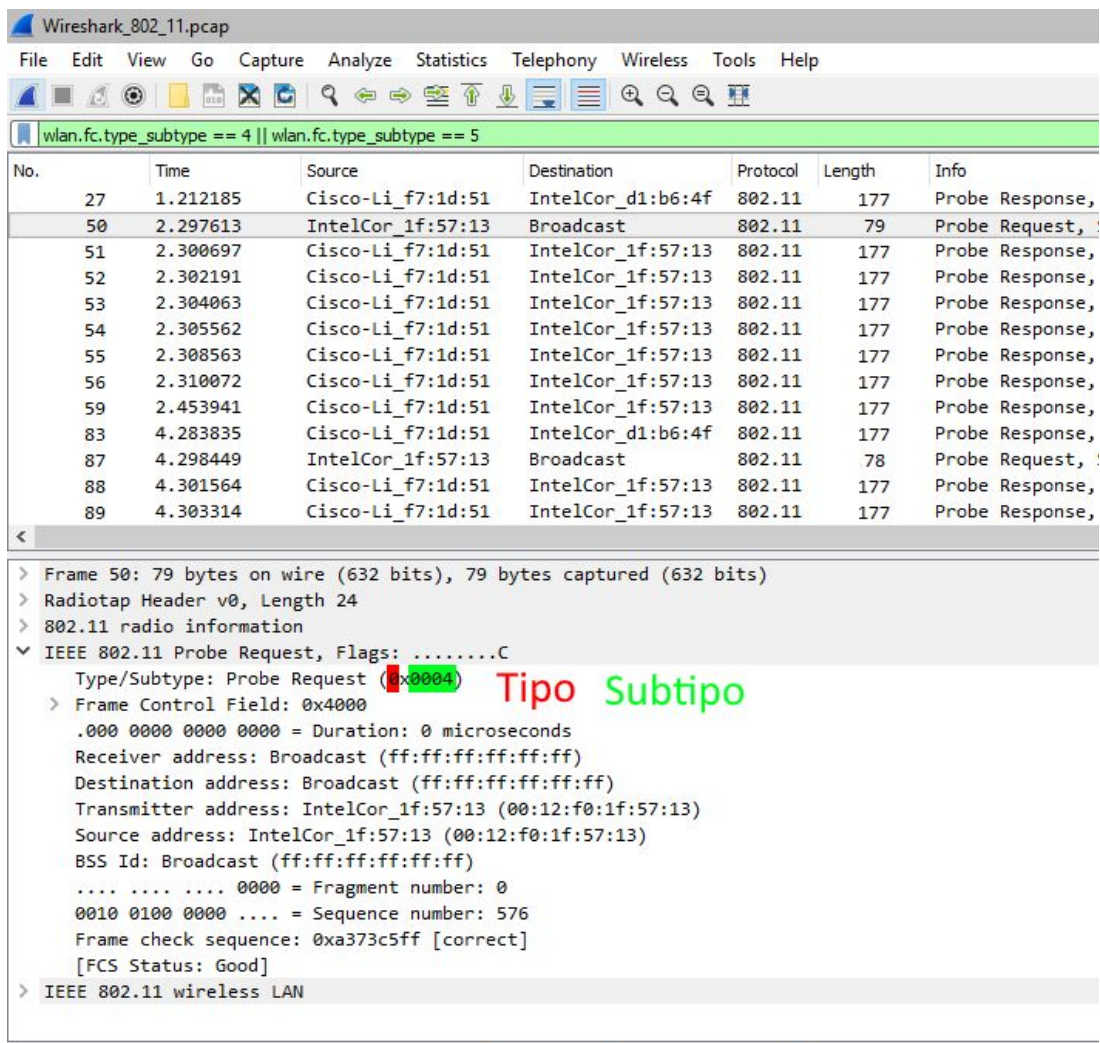
Sí, hay 2 estaciones: IntelCor_1f:57:13 y la otra es IntelCor_d1:b6:4f.

2. ¿Hay APs que respondan?

Sí, hay una estación: Cisco-Li_f7:1d:51.

3. ¿Qué tipos de tramas son?

Se tratan de tramas de gestión, de subtipos 4 (request) y 5 (response).



The image shows a Wireshark capture of a network packet. The top pane displays a list of captured packets. The bottom pane shows the details of the selected packet (Frame 50), which is an IEEE 802.11 Probe Request.

No.	Time	Source	Destination	Protocol	Length	Info
27	1.212185	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	177	Probe Response,
50	2.297613	IntelCor_1f:57:13	Broadcast	802.11	79	Probe Request,
51	2.300697	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response,
52	2.302191	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response,
53	2.304063	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response,
54	2.305562	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response,
55	2.308563	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response,
56	2.310072	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response,
59	2.453941	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response,
83	4.283835	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	177	Probe Response,
87	4.298449	IntelCor_1f:57:13	Broadcast	802.11	78	Probe Request,
88	4.301564	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response,
89	4.303314	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response,

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) **Tipo Subtipo**
> 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 [correct]
[FCS Status: Good]
> IEEE 802.11 wireless LAN

Wireshark_802_11.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

wlan.fc.type_subtype == 4 || wlan.fc.type_subtype == 5

No.	Time	Source	Destination	Protocol	Length	Info
27	1.212185	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	177	Probe Response,
50	2.297613	IntelCor_1f:57:13	Broadcast	802.11	79	Probe Request, :
51	2.300697	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response,
52	2.302191	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response,
53	2.304063	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response,
54	2.305562	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response,
55	2.308563	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response,
56	2.310072	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response,
59	2.453941	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response,
83	4.283835	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	177	Probe Response,
87	4.298449	IntelCor_1f:57:13	Broadcast	802.11	78	Probe Request, :
88	4.301564	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response,
89	4.303314	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response,

> 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) **Tipo Subtipo**

▼ 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 Fr

.... 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

* Se ha usado la traza [Whireshark_802_11.pcapng](#).

Ejercicio 2

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

Puede observarse lo que se pide en las capturas del apartado 3 del ejercicio anterior, donde la petición activa corresponde con la primera captura y la respuesta con la segunda.

Cuestión 3

1. Localiza en las capturas alguna respuesta de asociación.

Traza [Wireshark_802_11.pcapng](#).

The image shows a Wireshark window titled "Wireshark_802_11.pcap". The filter bar at the top displays the expression "wlan.fc.type_subtype == 1". The packet list pane shows two packets. Packet 12 is an "Association Response" frame from source "00:ae:93:3d:0a:4a" to destination "ff:ff:ff:ff:bf:4a". Packet 2166 is another "Association Response" frame from source "Cisco-Li_f7:1d:51" to destination "IntelCor_d1:b6:4f". The packet details pane for packet 2166 is expanded, showing the following structure:

- Frame 2166: 94 bytes on wire (752 bits), 94 bytes captured (752 bits)
- Radiotap Header v0, Length 24
- 802.11 radio information
- 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]
- IEEE 802.11 wireless LAN

The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII:

```
0000 00 00 18 00 ee 58 00 00 10 02 85 09 a0 00 e1 9c .....X.....
0010 64 00 00 45 2b ab f2 37 10 00 3a 01 00 13 02 d1 d..E+..7..:....
0020 b6 4f 00 16 b6 f7 1d 51 00 16 b6 f7 1d 51 00 e9 .O.....Q.....Q..
0030 01 06 00 00 05 c0 01 04 82 84 8b 96 32 08 8c 12 .....2....
0040 98 24 b0 48 60 6c 0c 12 0f 00 03 a4 00 00 27 a4 $.H`l.....'..
0050 00 00 42 43 5e 00 62 32 2f 00 2b ab f2 37 ..BC^..b2 /..+..7
```

The status bar at the bottom indicates "Packets: 2364 • Displayed: 2 (0.1%) | Profile: Default".

Traza [Wireshark_802_11_LOCAL.pcapng](#).

The image shows a Wireshark window titled "Wireshark_802_11_LOCAL.pcap". The filter bar at the top displays the expression "wlan.fc.type_subtype == 1". The packet list pane shows a single packet, number 14086, at time 17.013521, from source "Cisco_1b:d5:02" to destination "LiteonTe_1d:02:6c", with protocol "802.11" and length "139". The packet details pane shows the structure of the IEEE 802.11 Association Response frame, including the Radiotap Header, 802.11 radio information, and the IEEE 802.11 Association Response frame itself. The frame control field is expanded, showing the version (0), type (Management frame), and subtype (1). The flags are 0x00. The duration is 213 microseconds. The receiver address is LiteonTe_1d:02:6c (74:de:2b:1d:02:6c). The destination address is LiteonTe_1d:02:6c (74:de:2b:1d:02:6c). The transmitter address is Cisco_1b:d5:02 (00:0a:b8:1b:d5:02). The source address is Cisco_1b:d5:02 (00:0a:b8:1b:d5:02). The BSS Id is Cisco_1b:d5:02 (00:0a:b8:1b:d5:02). The fragment number is 0. The sequence number is 945. The frame check sequence is 0xa022f3fa [correct]. The FCS status is Good. The packet bytes pane shows the raw data of the frame, with the first few bytes highlighted in blue.

No.	Time	Source	Destination	Protocol	Length	Info
14086	17.013521	Cisco_1b:d5:02	LiteonTe_1d:02:6c	802.11	139	Association Res

> Frame 14086: 139 bytes on wire (1112 bits), 139 bytes captured (1112 bits)
> Radiotap Header v0, Length 25
> 802.11 radio information
▼ 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 0000 1101 0101 = Duration: 213 microseconds
 Receiver address: LiteonTe_1d:02:6c (74:de:2b:1d:02:6c)
 Destination address: LiteonTe_1d:02:6c (74:de:2b:1d:02:6c)
 Transmitter address: Cisco_1b:d5:02 (00:0a:b8:1b:d5:02)
 Source address: Cisco_1b:d5:02 (00:0a:b8:1b:d5:02)
 BSS Id: Cisco_1b:d5:02 (00:0a:b8:1b:d5:02)
 0000 = Fragment number: 0
 0011 1011 0001 = Sequence number: 945
 Frame check sequence: 0xa022f3fa [correct]
 [FCS Status: Good]
 > IEEE 802.11 wireless LAN

0000 00 00 19 00 6f 08 00 00 95 3a 65 fc 00 00 00 00o... :e.....
0010 10 16 6c 09 80 00 aa a9 00 10 00 d5 00 74 de 2b ...l..... t.+
0020 1d 02 6c 00 0a b8 1b d5 02 00 0a b8 1b d5 02 10 ...l.....
0030 3b 31 04 00 00 02 c0 01 07 96 18 24 30 48 60 6c ;l..... \$0H`l
0040 dd 05 00 40 96 03 05 dd 05 00 40 96 14 00 dd 18 ...@..... @.....
0050 00 50 f2 02 01 01 80 00 03 a4 00 00 27 a4 00 00 ..P..... '.....
0060 42 43 5e 00 62 32 2f 00 dd 1d 00 40 96 0c 01 a6 BC^b2/.. @.....
0070 16 fe 1b bd ab 3a 01 00 00 b7 65 0b 00 00 00 42:.. e...B
0080 b0 ee 0b 61 40 f9 e1 fa f3 22 a0a@... "

Wireshark_802_11_LOCAL.pcap | Packets: 18829 • Displayed: 1 (0.0%) | Profile: Default

2. ¿Qué información incluye?

Tipo y subtipo de la trama, campo de control de la trama, dirección del receptor, dirección de destino, dirección del emisor, dirección de origen, BSS ID, número de fragmento, número de secuencia y checksum de la trama.

3. ¿Qué tipos de tramas con?

Tramas de gestión, ya que se corresponden con el tipo 0; y como se indica en el enunciado, son tramas de respuesta de asociación, cuyo subtipo es 1.

Ejercicio 3

Localiza en las capturas alguna trama de petición de asociación y la respuesta correspondiente.

Muestra la estructura y contenido de ambas tramas.

Cuestión 4

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

Escenario A: Pasivo.

Porque la estación H1 solo envía una señal de respuesta a la estación AP2.

Escenario B: Activo.

Porque la estación H1 envía una señal que reciben tanto AP1 como AP2, pero en este caso ambas estaciones envían una señal de respuesta a H1 (y entonces se conecta con AP2).

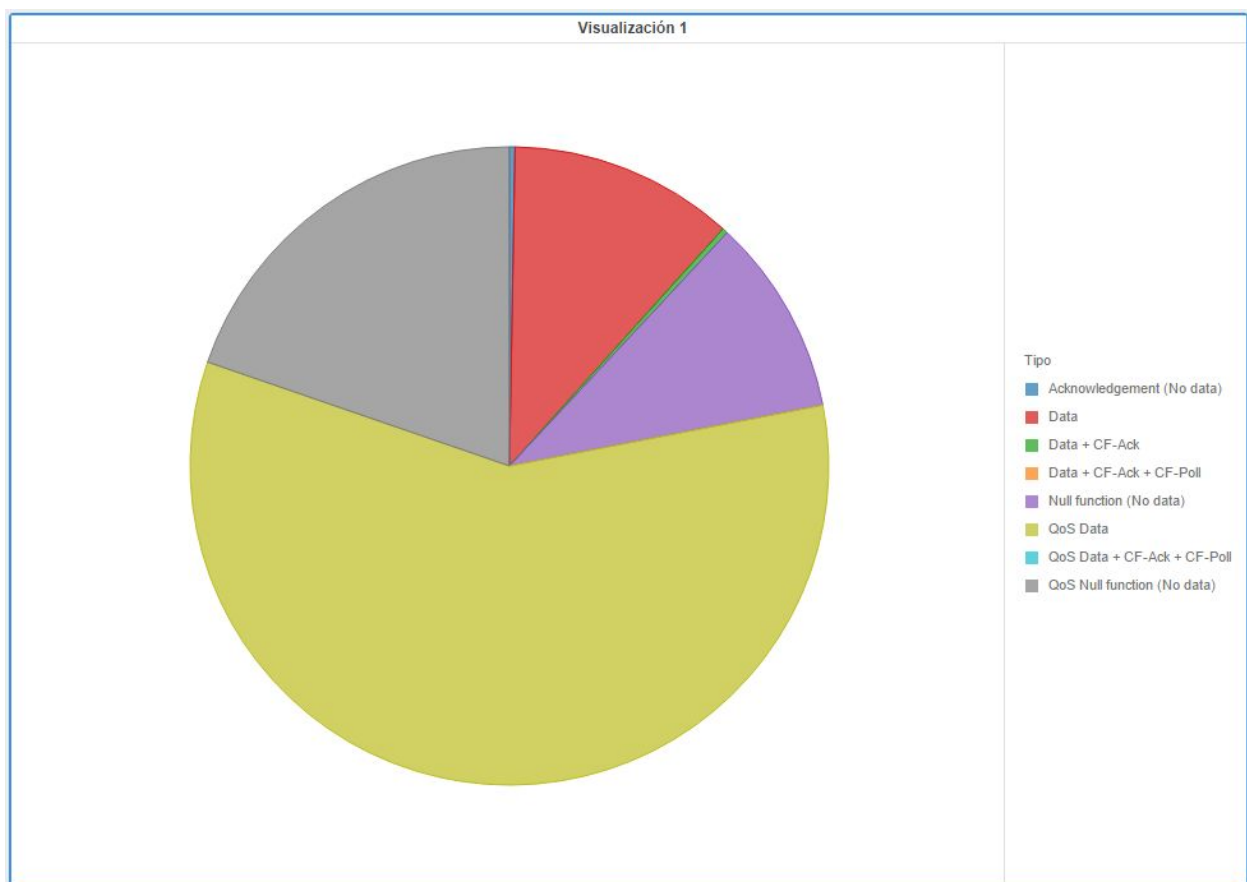
Cuestión 5

1. ¿Cuántas tramas de datos diferentes observas en la captura?

En ambos casos se ha usado el filtro `wlan.fc.type == 2` para filtrar por tramas de tipo 2, las tramas de datos. Al no especificar un subtipo, aparecen todos.

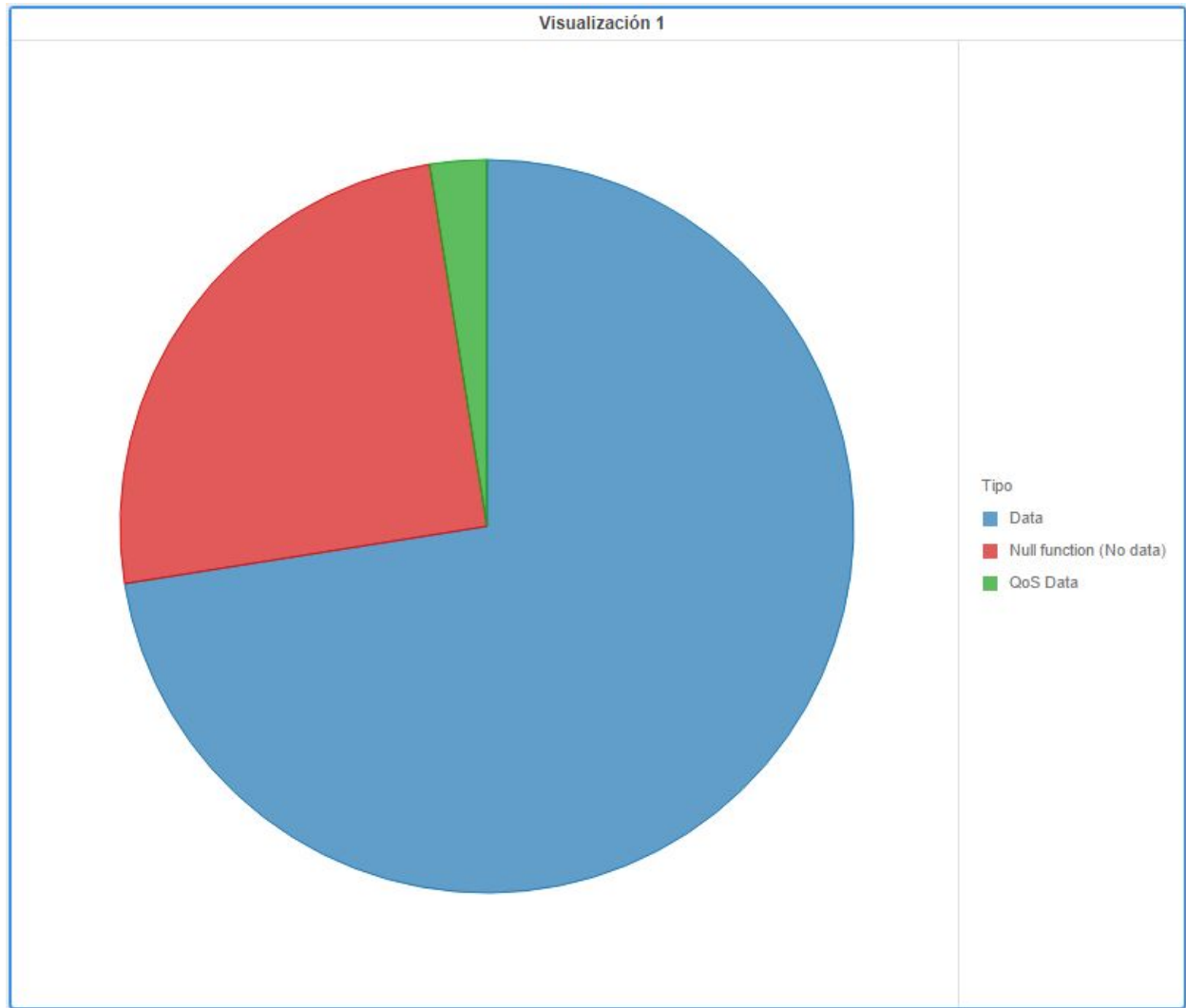
Traza [Whireshark_802_11.pcapng](#).

En esta traza intervienen 8 tipos de tramas de datos diferentes, mostradas en función de su uso en la siguiente imagen:



Traza [Wireshark_802_11_LOCAL.pcapng](#).

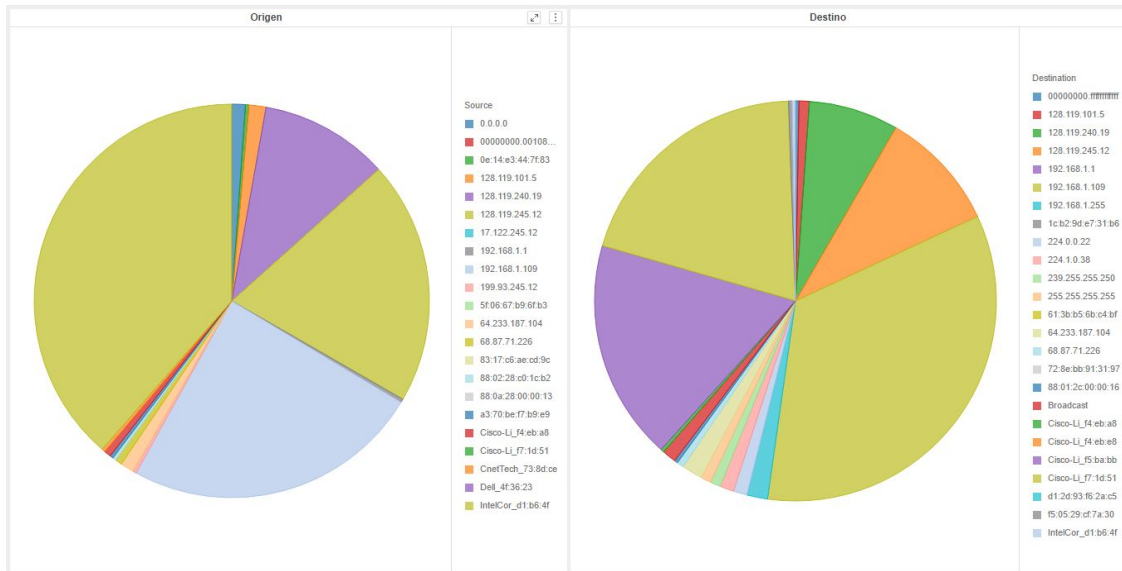
En esta traza intervienen 3 tipos de tramas de datos diferentes, mostradas en función de su uso en la siguiente imagen:



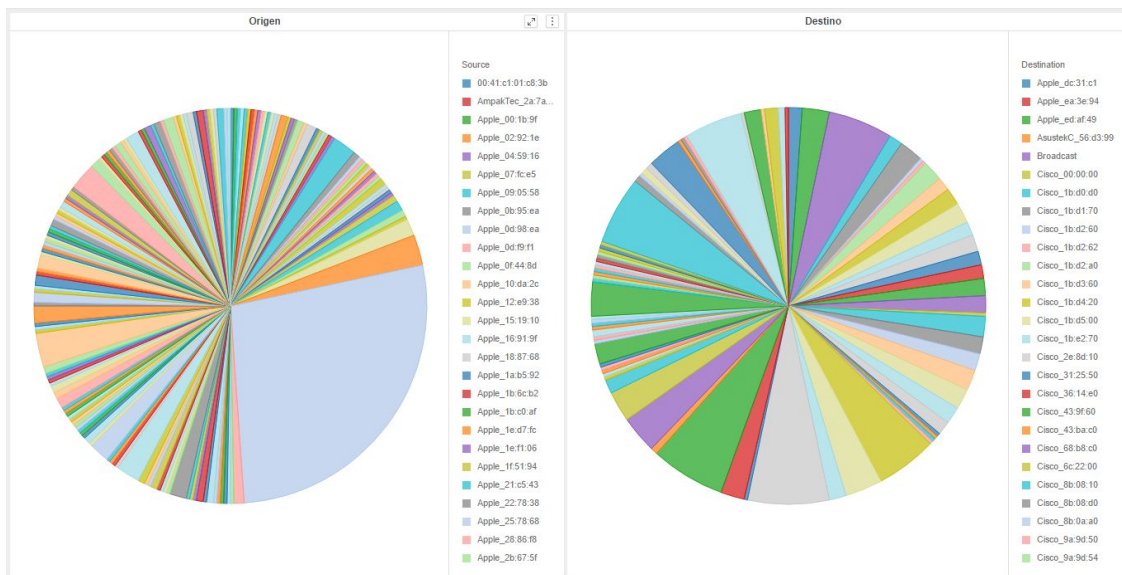
2. ¿Qué estaciones participan en esta comunicación?

Traza [Whire shark_802_11.pcapng](#).

En esta traza participan 22 estaciones emisoras y 25 receptoras, cuya proporción de uso es la siguiente:



Traza [Whire shark_802_11_LOCAL.pcapng](#).



-
3. ¿Hay comunicación directa entre estaciones o siempre interviene un punto de acceso?

Ejercicio 4

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

Ejercicio 5

Localiza en la captura alguna trama de datos NULL.

Muestra la estructura y contenido de esta trama.

Traza [Wireshark_802_11.pcapng](#).

The image shows a Wireshark capture of a network traffic file named `Wireshark_802_11.pcap`. The filter bar at the top is set to `wlan.fc.type_subtype == 0x0024`, which filters for Null function frames. The packet list shows a series of frames from 2002 to 2033, all of which are IEEE 802.11 Null function frames with a length of 52 bytes. The packet details pane for frame 2002 is expanded, showing the following structure:

- Frame 2002: 52 bytes on wire (416 bits), 52 bytes captured (416 bits)
- Radiotap Header v0, Length 24
- 802.11 radio information
 - 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
 - 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)
 - Fragment number: 0
 - Sequence number: 1624
 - Frame check sequence: 0xb94abff7 [correct]
 - [FCS Status: Good]

The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII:

```
0000 00 00 18 00 ee 58 00 00 10 02 85 09 a0 00 e6 9c .....X.....
0010 64 00 00 4a f7 bf 4a b9 48 11 3a 01 00 18 39 f5 d..J...J. H.:...9.
0020 ba bb 00 13 02 d1 b6 4f 00 18 39 f5 ba bb 80 65 .....O ..9.....e
0030 f7 bf 4a b9 ...J.
```

The status bar at the bottom indicates that there are 2364 packets in the capture, with 77 (3.3%) displayed. The profile is set to Default.

Traza Whireshark_802_11_LOCAL.pcapng.

Wireshark_802_11_LOCAL.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Filter: wlan.fc.type_subtype == 0x0024

No.	Time	Source	Destination	Protocol	Length	Info
94	0.181857	Cisco-Li_72:e1:78	Cisco_2e:8d:10	802.11	59	Null function (No data)
105	0.191744	Cisco-Li_72:e1:78	Cisco_2e:8d:10	802.11	59	Null function (No data)
106	0.194987	Cisco-Li_72:e1:78	Cisco_2e:8d:10	802.11	59	Null function (No data)
107	0.195709	Cisco-Li_72:e1:78	Cisco_2e:8d:10	802.11	59	Null function (No data)
108	0.196500	Cisco-Li_72:e1:78	Cisco_1b:d1:70	802.11	59	Null function (No data)
110	0.197832	Cisco-Li_72:e1:78	Cisco_1b:d1:70	802.11	59	Null function (No data)
113	0.200267	Cisco-Li_72:e1:78	Cisco_1b:d1:70	802.11	59	Null function (No data)
115	0.202771	Cisco-Li_72:e1:78	Cisco_1b:d1:70	802.11	59	Null function (No data)
116	0.206436	Cisco-Li_72:e1:78	Cisco_1b:d1:70	802.11	59	Null function (No data)
128	0.216484	Cisco-Li_72:e1:78	Cisco_1b:d1:70	802.11	59	Null function (No data)
140	0.370063	Cisco-Li_72:e1:78	Cisco_9a:9d:70	802.11	59	Null function (No data)
141	0.370990	Cisco-Li_72:e1:78	Cisco_9a:9d:70	802.11	59	Null function (No data)
142	0.372158	Cisco-Li_72:e1:78	Cisco_9a:9d:70	802.11	59	Null function (No data)
145	0.376192	Cisco-Li_72:e1:78	Cisco_9a:9d:70	802.11	59	Null function (No data)
150	0.379507	Cisco-Li_72:e1:78	Cisco_9a:9d:70	802.11	59	Null function (No data)
151	0.380523	Cisco-Li_72:e1:78	Cisco_9a:9d:70	802.11	59	Null function (No data)
167	0.548324	Cisco-Li_72:e1:78	Cisco_1b:d3:60	802.11	59	Null function (No data)

> Frame 108: 59 bytes on wire (472 bits), 59 bytes captured (472 bits)

> Radiotap Header v0, Length 25

> 802.11 radio information

> IEEE 802.11 Null function (No data), Flags:FTC

Type/Subtype: Null function (No data) (0x0024)

> Frame Control Field: 0x4803

.... ..00 = Version: 0

.... 10.. = Type: Data frame (2)

0100 = Subtype: 4

> Flags: 0x003

.... ..11 = DS status: WDS (AP to AP) or Mesh (MP to MP) Frame (To DS: 1 From DS: 1) (0x3)

.... .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: Cisco_1b:d1:70 (00:0a:b8:1b:d1:70)

Transmitter address: Cisco-Li_72:e1:78 (00:14:bf:72:e1:78)

Destination address: Cisco_1b:d1:70 (00:0a:b8:1b:d1:70)

Source address: Cisco-Li_72:e1:78 (00:14:bf:72:e1:78)

.... 0000 = Fragment number: 0

1101 0011 1000 = Sequence number: 3384

Frame check sequence: 0xbfbf8144 [correct]

[FCS Status: Good]

```

0000 00 00 19 00 6f 08 00 00 ae 9e 64 fb 00 00 00 00 .....d.....
0010 10 02 6c 09 80 00 b6 a5 00 48 03 3a 01 00 0a b8 ..l.....H:....
0020 1b d1 70 00 14 bf 72 e1 78 00 0a b8 1b d1 70 80 ..p...x.....p
0030 d3 00 14 bf 72 e1 78 44 81 0f bf .....xD...

```

Wireshark_802_11_LOCAL.pcap

Packets: 18829 · Displayed: 2726 (14.5%)

Profile: Default

¿Qué la diferencia de las tramas de datos normales?

La diferencia de las tramas de tipo NULL es que no poseen un payload con información o, en otras palabras, no transportan datos. Tampoco *polls* ni ACKs.

¿Para qué sirve?

Su única función es la de transmitir el bit de gestión de potencia, con el que indica que la estación está cambiando a un estado de operación en baja potencia.

Cuestión 6

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

Muestra su contenido.

Como en la traza [Whireshark_802_11_LOCAL.pcapng](#) no aparecen tramas, se examinará únicamente la traza [Whireshark_802_11.pcapng](#).

The image shows a Wireshark capture of a network packet. The top pane displays a list of packets. Packet 474 is selected, showing it is a TCP SYN packet from 192.168.1.109 to 128.119.245.12. The bottom pane shows the detailed view of this packet, including the IEEE 802.11 QoS Data header and the Internet Protocol Version 4 header. The packet is a SYN packet with sequence number 0 and window size 0.

No.	Time	Source	Destination	Protocol	Length	Tipo	Info
474	24.811093	192.168.1.109	128.119.245.12	TCP	110	QoS Data	2538 → 80 [SYN] Seq=0 Win=16384 Len=0

Frame 474: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)

Radiotap Header v0, Length 24

802.11 radio information

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 0011 0001 = Sequence number: 49

Frame check sequence: 0xad57fce0 [correct]

[FCS Status: Good]

QoS Control: 0x0000

.....0000 = TID: 0

[.....0000 = 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

Internet Protocol Version 4, Src: 192.168.1.109, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 2538, Dst Port: 80, Seq: 0, Len: 0

0000 00 00 18 00 ee 58 00 00 10 60 85 09 c0 00 da 9cX.....

0010 00 00 00 3e e0 fc 57 ad 88 01 2c 00 00 16 b6 f7>..W.....

0020 1d 51 00 13 02 d1 b6 4f 00 16 b6 f4 eb a8 10 03Q.....0.....

0030 00 00 aa aa 03 00 00 00 08 00 45 00 00 30 13 24E..0.\$.....

0040 40 00 80 06 b0 0a c0 a8 01 6d 80 77 f5 0c 09 ea@.....m.w.....

A. ¿Cuáles son las tres direcciones MAC de esta trama?

Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:57).

IntelCor_d1:b6:4f (00:13:02:d1:b6:f4).

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

¿Cuál es la dirección MAC correspondiente al host inalámbrico desde el que se hace la petición? (representación hexadecimal)

00:13:02:d1:b6:f4 (IntelCor_d1:b6:4f).

¿Cuál es la dirección MAC del punto de acceso?

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

¿Y la dirección MAC del (primer) router?

00:16:b6:f7:1d:57 (Cisco-Li_f7:1d:51).

B. ¿Cuál es la dirección IP del host inalámbrico que envía este segmento?

192.168.1.109 .

¿Y la dirección IP destino?

128.119.245.12 .

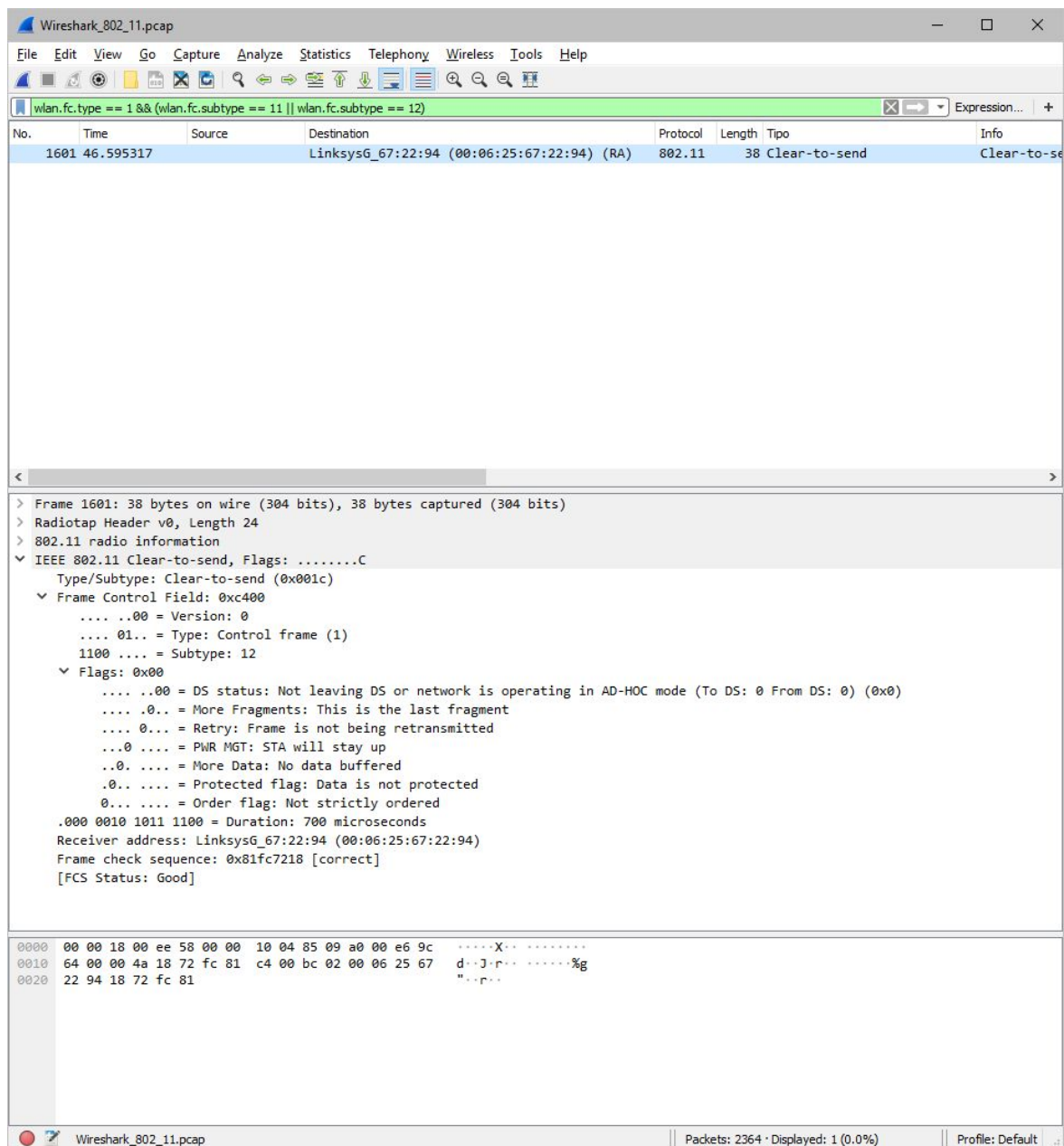
¿Con qué se corresponde esta dirección IP destino (host, punto de acceso, router, o cualquier otro dispositivo de la red)? Razona tu respuesta.

Se corresponde con un punto de acceso, ya que el campo DS Status en los Flags indica que es una trama distribuida desde una estación a través de un punto de acceso: DS status: Frame from STA to DS via AP (to DS: 1 from DS: 0).

Cuestión 7

Localiza las tramas RTS y CTS capturadas en el fichero [Wireshar_802_11.pcap](#).

Tal y como se ve en la imagen, al filtrarse por tramas RTS o CTS, solo hay una trama CTS en toda la captura:



¿Es posible que sólo haya tramas RTS o CTS? ¿Por qué?

Sí, sería posible: se recibiría únicamente RTS si un par de tramas de estaciones diferentes colisionasen entre sí -ya que no se produciría una respuesta CTS- y finalizase la captura durante el tiempo de espera aleatorio para la retransmisión de las tramas RTS; en cambio, podría recibirse fácilmente tramas CTS y no RTS si la estación que envía la trama CTS no es la misma que recibe la trama RTS, ya que la receptora de dicha trama puede retransmitir un CTS con NAV para indicar al resto de estaciones que no usen un canal determinado, de forma que realizando la captura sobre una de esas estaciones podrían registrarse únicamente tramas CTS.

Cuestión 8

Localiza las tramas RTS y CTS capturadas en el fichero [Wireshar_802_11_RTS_CTS.pcap](#).

¿Qué información contiene estas tramas?

Trama RTS:

The image shows a Wireshark capture of an IEEE 802.11 Request-to-Send (RTS) frame. The packet list on the left shows frame 68 at time 0.962997, source HonHaiPr_2e:38:ea, and destination CompalBr_4d:88:93. The packet details pane on the right shows the frame structure: AVS WLAN Capture header, 802.11 radio information, and IEEE 802.11 Request-to-send, Flags: The frame control field is 0xb400. The flags are: Type/Subtype: Request-to-send (0x001b), Version: 0, Type: Control frame (1), Subtype: 11, Flags: 0x00, DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x0), More Fragments: This is the last fragment, Retry: Frame is not being retransmitted, PWR MGT: STA will stay up, More Data: No data buffered, Protected flag: Data is not protected, Order flag: Not strictly ordered, 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). The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
64	0.898663		Tp-LinkT_bc:7a:12 (d8:5d:4c:bc:7a:12) (RA)	802.11	78 C	
68	0.962997	HonHaiPr_2e:38:ea (cc:af:78:2e:38:ea) (TA)	CompalBr_4d:88:93 (5c:35:3b:4d:88:93) (RA)	802.11	84 R	
69	0.963001		HonHaiPr_2e:38:ea (cc:af:78:2e:38:ea) (RA)	802.11	78 C	
70	0.963339	HonHaiPr_2e:38:ea (cc:af:78:2e:38:ea) (TA)	CompalBr_4d:88:93 (5c:35:3b:4d:88:93) (RA)	802.11	84 R	
71	0.963378		HonHaiPr_2e:38:ea (cc:af:78:2e:38:ea) (RA)	802.11	78 C	
72	0.963645	HonHaiPr_2e:38:ea (cc:af:78:2e:38:ea) (TA)	CompalBr_4d:88:93 (5c:35:3b:4d:88:93) (RA)	802.11	84 R	
73	0.963674		HonHaiPr_2e:38:ea (cc:af:78:2e:38:ea) (RA)	802.11	78 C	
75	0.964253	CompalBr_4d:88:93 (5c:35:3b:4d:88:93) (TA)	HewlettP_33:a8:a5 (9c:8e:99:33:a8:a5) (RA)	802.11	84 R	
76	0.964260		CompalBr_4d:88:93 (5c:35:3b:4d:88:93) (RA)	802.11	78 C	
80	0.971647	CompalBr_4d:88:93 (5c:35:3b:4d:88:93) (TA)	HonHaiPr_2e:38:ea (cc:af:78:2e:38:ea) (RA)	802.11	84 R	
81	0.971654		CompalBr_4d:88:93 (5c:35:3b:4d:88:93) (RA)	802.11	78 C	
83	0.972803	HonHaiPr_2e:38:ea (cc:af:78:2e:38:ea) (TA)	CompalBr_4d:88:93 (5c:35:3b:4d:88:93) (RA)	802.11	84 R	
84	0.972806		HonHaiPr_2e:38:ea (cc:af:78:2e:38:ea) (RA)	802.11	78 C	
85	0.973245		HonHaiPr_2e:38:ea (cc:af:78:2e:38:ea) (RA)	802.11	78 C	
86	0.973567		HonHaiPr_2e:38:ea (cc:af:78:2e:38:ea) (RA)	802.11	78 C	
87	0.973844	HonHaiPr_2e:38:ea (cc:af:78:2e:38:ea) (TA)	CompalBr_4d:88:93 (5c:35:3b:4d:88:93) (RA)	802.11	84 R	

> Frame 68: 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 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)

0000 80 21 10 01 00 00 00 40 1c 4c c4 f0 00 00 00 00@..L.....
0010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0d
0020 00 00 00 f0 00 00 00 00 00 00 00 00 00 00 02
0030 ff ff ff b6 ff ff ff a3 00 00 00 01 00 00 00 03
0040 b4 00 98 00 5c 35 3b 4d 88 93 cc af 78 2e 38 ea5;M....x.8.
0050 73 7f ce 9d s....

IEEE 802.11 wireless LAN (wlan), 16 bytes | Packets: 3926 · Displayed: 1064 (27.1%) | Profile: Default

Trama CTS:

Wireshark_802_11_RTS_CTS.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Filter: wlan.fc.type == 1 && (wlan.fc.subtype == 11 || wlan.fc.subtype == 12)

No.	Time	Source	Destination	Protocol	Length	Info
64	0.898663		Tp-LinkT_bc:7a:12 (d8:5d:4c:bc:7a:12) (RA)	802.11	78	C
68	0.962997	HonHaiPr_2e:38:ea (cc:af:78:2e:38:ea) (TA)	CompalBr_4d:88:93 (5c:35:3b:4d:88:93) (RA)	802.11	84	R
69	0.963001		HonHaiPr_2e:38:ea (cc:af:78:2e:38:ea) (RA)	802.11	78	C
70	0.963339	HonHaiPr_2e:38:ea (cc:af:78:2e:38:ea) (TA)	CompalBr_4d:88:93 (5c:35:3b:4d:88:93) (RA)	802.11	84	R
71	0.963378		HonHaiPr_2e:38:ea (cc:af:78:2e:38:ea) (RA)	802.11	78	C
72	0.963645	HonHaiPr_2e:38:ea (cc:af:78:2e:38:ea) (TA)	CompalBr_4d:88:93 (5c:35:3b:4d:88:93) (RA)	802.11	84	R
73	0.963674		HonHaiPr_2e:38:ea (cc:af:78:2e:38:ea) (RA)	802.11	78	C
75	0.964253	CompalBr_4d:88:93 (5c:35:3b:4d:88:93) (TA)	HewlettP_33:a8:a5 (9c:8e:99:33:a8:a5) (RA)	802.11	84	R
76	0.964260		CompalBr_4d:88:93 (5c:35:3b:4d:88:93) (RA)	802.11	78	C
80	0.971647	CompalBr_4d:88:93 (5c:35:3b:4d:88:93) (TA)	HonHaiPr_2e:38:ea (cc:af:78:2e:38:ea) (RA)	802.11	84	R
81	0.971654		CompalBr_4d:88:93 (5c:35:3b:4d:88:93) (RA)	802.11	78	C
83	0.972803	HonHaiPr_2e:38:ea (cc:af:78:2e:38:ea) (TA)	CompalBr_4d:88:93 (5c:35:3b:4d:88:93) (RA)	802.11	84	R
84	0.972806		HonHaiPr_2e:38:ea (cc:af:78:2e:38:ea) (RA)	802.11	78	C
85	0.973245		HonHaiPr_2e:38:ea (cc:af:78:2e:38:ea) (RA)	802.11	78	C
86	0.973567		HonHaiPr_2e:38:ea (cc:af:78:2e:38:ea) (RA)	802.11	78	C
87	0.973844	HonHaiPr_2e:38:ea (cc:af:78:2e:38:ea) (TA)	CompalBr_4d:88:93 (5c:35:3b:4d:88:93) (RA)	802.11	84	R

> Frame 69: 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

.... 0000 = Version: 0

.... 01.. = Type: Control frame (1)

1100 = Subtype: 12

Flags: 0x00

.... 0000 = 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 0110 1100 = Duration: 108 microseconds

Receiver address: HonHaiPr_2e:38:ea (cc:af:78:2e:38:ea)

0000 80 21 10 01 00 00 00 40 1c 4d 78 a0 00 00 00 00@·Mx.....

0010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0d

0020 00 00 00 f0 00 00 00 00 00 00 00 00 00 00 02

0030 ff ff ff e1 ff ff ff a3 00 00 00 01 00 00 03

0040 c4 00 6c 00 cc af 78 2e 38 ea d5 f1 df 4a1...x.8...J

IEEE 802.11 wireless LAN (wlan), 10 bytes

Packets: 3926 · Displayed: 1064 (27.1%)

Profile: Default

Como diferencia, puede apreciarse la Transmitter Address en la trama RTS, la cual no posee la trama CTS. Sin embargo, ambas tramas poseen los mismo campos: estado DS, más fragmentos, retransmisión, PWR MGT, Flag «protegida» y Flag de «orden».

¿Para qué sirve el valor NAV?

El valor NAV indica el tiempo que una estación necesita ocupar un canal. Dicho valor se adjunta al RTS enviado y tras recibirse, se difunde junto a los CTS al resto de estaciones, de este modo quedan notificadas y estas no ocupan el canal mencionado.