

TP4 - Redes Sem Fios



Engenharia Informática
Universidade do Minho
2019/2020

Grupo - PL6.G06



Paulo Lima | a89983



Mafalda Costa | a83919



Maria Silva | a83840

Objetivo

- Aprofundar o conhecimento sobre o protocolo IEEE 802.1.
- Conhecer as tramas mais comuns e o seu formato.
- Endereçamento dos componentes envolvidos na comunicação sem fios.

Questões e Respostas

3 - Acesso Rádio

1) Identifique em que frequência do espectro está a operar a rede sem fios, e o canal que corresponde a essa frequência.

A frequência em que opera são os 2437 MHz e o canal é o 6.

```
▶ Frame 1606: 177 bytes on wire (1416 bits), 177 bytes captured (1416 bits)
▶ Radiotap Header v0, Length 24
└─ 802.11 radio information
    PHY type: 802.11b (4)
    Short preamble: False
    Data rate: 1.0 Mb/s
    Channel: 6
        Frequency: 2437MHz
        Signal strength (dBm): -31dBm
        Noise level (dBm): -100dBm
        ▶ [Duration: 1416µs]
    └─ IEEE 802.11 Probe Response, Flags: . . . . . C
    └─ IEEE 802.11 wireless LAN
        ▶ Fixed parameters (12 bytes)
        ▶ Tagged parameters (113 bytes)
```

2) Identifique a versão da norma IEEE 802.11 que está a ser usada.

A versão utilizada é a 802.11b.

```
▶ Frame 1606: 177 bytes on wire (1416 bits), 177 bytes captured (1416 bits)
▶ Radiotap Header v0, Length 24
└─ 802.11 radio information
    PHY type: 802.11b (4)
        Short preamble: False
        Data rate: 1.0 Mb/s
        Channel: 6
        Frequency: 2437MHz
        Signal strength (dBm): -31dBm
        Noise level (dBm): -100dBm
        ▶ [Duration: 1416µs]
    └─ IEEE 802.11 Probe Response, Flags: . . . . . C
    └─ IEEE 802.11 wireless LAN
```

3) Qual o débito a que foi enviada a trama escolhida? Será que esse débito corresponde ao débito máximo a que a interface Wi-Fi pode operar? Justifique.

A trama foi enviada com um débito de 1 Mbps. Sendo que o máximo a que a interface Wi-Fi pode operar são 11 Mbps, conluimos que o débito de envio não corresponde ao máximo.

```
▶ Frame 1606: 177 bytes on wire (1416 bits), 177 bytes captured (1416 bits)
▶ Radiotap Header v0, Length 24
└ ▶ 802.11 radio information
    PHY type: 802.11b (4)
    Short preamble: False
    Data rate: 1.0 Mb/s
    Channel: 6
    Frequency: 2437MHz
    Signal strength (dBm): -31dBm
    Noise level (dBm): -100dBm
    ▶ [Duration: 1416µs]
        [Preamble: 192µs]
▶ IEEE 802.11 Probe Response, Flags: . . . . . C
▶ IEEE 802.11 wireless LAN
```

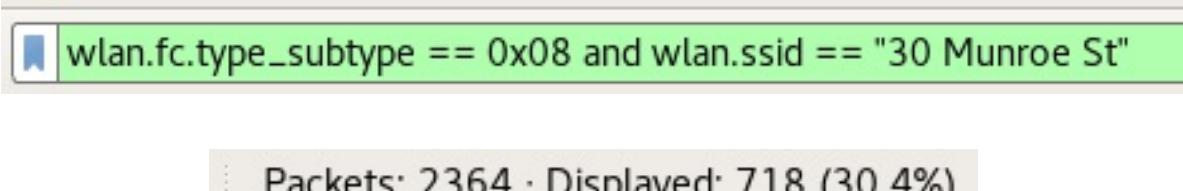
4 - Scanning

4) Quais são os SSIDs dos dois APs que estão a emitir a maioria das tramas de beacon?

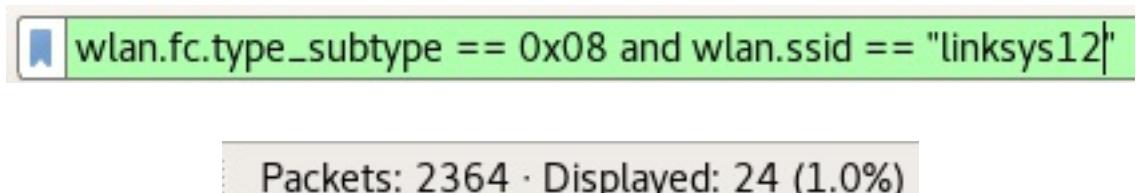
Incialmente, aplicámos no Wireshark, o filtro `wlan.fc.type_subtype == 0x08` para obtermos apenas as tramas `Beacon`. De seguida, ordenámos por `Source` e comparámos os diferentes MAC Address para perceber quais são os dois que emitem mais tramas. Para obtermos o número de pacotes de cada SSID aplicámos o filtro `wlan.fc.type_subtype == 0x08 and wlan.ssid == 'nome_SSID'`.

Concluímos que os dois SSIDs que correspondem aos Access Points que emitem a maioria das tramas são 30 Munroe St e linksys12.

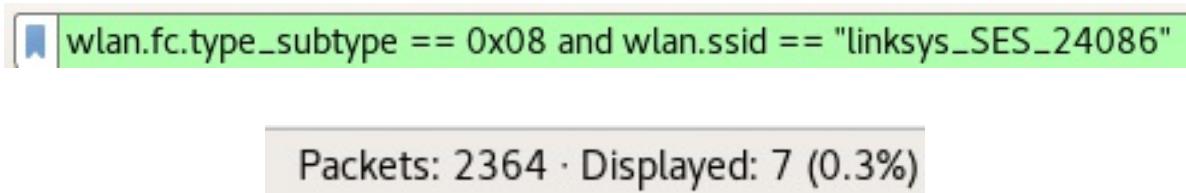
- 1º



- 2º



- 3º



5) Qual o intervalo de tempo entre a transmissão de tramas beacon para o AP linksys_ses_24086? E do AP 30 Munroe St? Na prática, a periodicidade de tramas beacon é verificada? Tente explicar porquê.

Para ambos os casos o intervalo de tempo mais comum é de 0.102400 segundos.

Não, pois existem algumas tramas em que a periodicidade não é mantida.

wlan.fc.type_subtype == 0x08 and wlan.ssid == "linksys_SES_24086"					
No.	Time	Source	Destination	Protocol	Length Info
1499	42.532596	Cisco-Li_f5:ba:bb	Broadcast	802.11	132 Beacon frame, SN=3640, FN=0, Flags=.....C, BI=100, SSID=linksys_SES_24086
1513	42.839707	Cisco-Li_f5:ba:bb	Broadcast	802.11	132 Beacon frame, SN=3643, FN=0, Flags=.....C, BI=100, SSID=linksys_SES_24086
1527	43.658960	Cisco-Li_f5:ba:bb	Broadcast	802.11	132 Beacon frame, SN=3651, FN=0, Flags=.....C, BI=100, SSID=linksys_SES_24086
1994	59.325865	Cisco-Li_f5:ba:bb	Broadcast	802.11	132 Beacon frame, SN=3833, FN=0, Flags=.....C, BI=100, SSID=linksys_SES_24086
2290	69.463202	Cisco-Li_f5:ba:bb	Broadcast	802.11	132 Beacon frame, SN=3938, FN=0, Flags=.....C, BI=100, SSID=linksys_SES_24086
2296	69.867955	Cisco-Li_f5:ba:bb	Broadcast	802.11	132 Beacon frame, SN=3940, FN=0, Flags=.....C, BI=100, SSID=linksys_SES_24086
2321	71.101576	Cisco-Li_f5:ba:bb	Broadcast	802.11	132 Beacon frame, SN=3954, FN=0, Flags=.....C, BI=100, SSID=linksys_SES_24086

▶ Frame 1527: 132 bytes on wire (1056 bits), 132 bytes captured (1056 bits)
▶ Radiotap Header v0, Length 24
▶ 802.11 radio information
▶ IEEE 802.11 Beacon frame, Flags:
▶ IEEE 802.11 wireless LAN
▼ Fixed parameters (12 bytes)
Timestamp: 0x000005c6ea0e185
Beacon Interval: 0.102400 [Seconds]
▶ Capabilities Information: 0x0011
▶ Tagged parameters (68 bytes)

wlan.fc.type_subtype == 0x08 and wlan.ssid == "30 Munroe St"					
No.	Time	Source	Destination	Protocol	Length Info
1993	59.269983	Cisco-Li_f7:id:51	Broadcast	802.11	183 Beacon frame, SN=3683, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1995	59.372340	Cisco-Li_f7:id:51	Broadcast	802.11	183 Beacon frame, SN=3684, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1996	59.474699	Cisco-Li_f7:id:51	Broadcast	802.11	183 Beacon frame, SN=3685, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1997	59.577107	Cisco-Li_f7:id:51	Broadcast	802.11	183 Beacon frame, SN=3686, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1998	59.679458	Cisco-Li_f7:id:51	Broadcast	802.11	183 Beacon frame, SN=3687, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1999	59.781851	Cisco-Li_f7:id:51	Broadcast	802.11	183 Beacon frame, SN=3688, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
2000	59.884353	Cisco-Li_f7:id:51	Broadcast	802.11	183 Beacon frame, SN=3689, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
2001	59.986718	Cisco-Li_f7:id:51	Broadcast	802.11	183 Beacon frame, SN=3690, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
2009	60.089093	Cisco-Li_f7:id:51	Broadcast	802.11	183 Beacon frame, SN=3692, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
2014	60.191465	Cisco-Li_f7:id:51	Broadcast	802.11	183 Beacon frame, SN=3693, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
2207	60.294447	Cisco-Li_f7:id:51	Broadcast	802.11	183 Beacon frame, SN=3696, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
2305	60.396219	Cisco-Li_f7:id:51	Broadcast	802.11	183 Beacon frame, SN=3697, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
2309	60.498707	Cisco-Li_f7:id:51	Broadcast	802.11	183 Beacon frame, SN=3698, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
2404	60.601091	Cisco-Li_f7:id:51	Broadcast	802.11	183 Beacon frame, SN=3699, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
2047	60.703465	Cisco-Li_f7:id:51	Broadcast	802.11	183 Beacon frame, SN=3700, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St

```
▶ Frame 2047: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits)
▶ Radiotap Header v0, Length 24
▶ 802.11 radio information
▶ IEEE 802.11 Beacon frame, Flags: .....

```

6) Qual é (em notação hexadecimal) o endereço MAC de origem da trama beacon de 30 Munroe St?

O endereço MAC de origem da trama beacon de 39 Munroe St é 00:16:b6:f7:1d:51.

Source address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)

7) Qual é (em notação hexadecimal) o endereço MAC de destino na trama de 30 Munroe St?

O endereço MAC é mesmo que o da origem, logo o 00:16:b6:f7:1d:51, pois estes estão em Broadcast.

Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)

8) Qual é (em notação hexadecimal) o MAC BSS ID da trama beacon de 30 Munroe St?

O endereço MAC é o 00:16:b6:f7:1d:51.

BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)

9) As tramas beacon do AP 30 Munroe St anunciam que o AP suporta quatro data rates e oito extended supported rates adicionais. Quais são?

- Supported - supported rates .

▼ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
Tag Number: Supported Rates (1)
Tag length: 4
Supported Rates: 1(B) (0x82)
Supported Rates: 2(B) (0x84)
Supported Rates: 5.5(B) (0x8b)
Supported Rates: 11(B) (0x96)

- Extended - extendend supported rates .

▼ Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
Tag Number: Extended Supported Rates (50)
Tag length: 8
Extended Supported Rates: 6(B) (0x8c)
Extended Supported Rates: 9 (0x12)
Extended Supported Rates: 12(B) (0x98)
Extended Supported Rates: 18 (0x24)
Extended Supported Rates: 24(B) (0xb0)
Extended Supported Rates: 36 (0x48)
Extended Supported Rates: 48 (0x60)
Extended Supported Rates: 54 (0x6c)

- 10) Selecione uma trama beacon. Esta trama pertence a que tipo de tramas 802.11? Indique o valor dos seus identificadores de tipo e de subtipo. Em que parte concreta do cabeçalho da trama estão especificados?**

A trama pertence ao tipo 802.11b. O seu tipo é Management Frame e o subtipo é 0x0008 o que significa através da tabela podemos inferir que se trata de um Beacon.

```

▼ 802.11 radio information
  PHY type: 802.11b (4)
  Short preamble: False
  Data rate: 1.0 Mb/s
  Channel: 6
  Frequency: 2437MHz
  Signal strength (dBm): -30dBm
  Noise level (dBm): -100dBm
  ▼ [Duration: 1464µs]
    [Preamble: 192µs]
▼ IEEE 802.11 Beacon frame, Flags: .....
  Type/Subtype: Beacon frame (0x0008)
  ▼ Frame Control Field: 0x8000
    .... .00 = Version: 0
    .... 00.. = Type: Management frame (0)
    1000 .... = Subtype: 8

```

- 11) Verifique se está a ser usado o método de deteção de erros CRC e se todas as tramas beacon são recebidas corretamente. Justifique o uso de mecanismos de deteção de erros neste tipo de redes locais.**

Cada trama inclui um checksum CRC-32.

Se os códigos CRC não são semelhantes, a mensagem contém erros de dados, e o dispositivo poderá realizar ações para corrigir como reler a mensagem ou pedir que a enviem novamente. Sem isto, os dados poderiam ser tratados como corretos e sem erro.

Portanto, sim, nos resultados abaixo podemos ver que isto está a ser verificado.

wlan.fc.type_subtype == 0x08 and wlan.fc.status != "Good"									
No.	Time	Source	Destination	Protocol	Length	Info			
10 0 204432	Linksys_67:22:94	Broadcast		802.11	90	Beacon frame, SN=3072, FN=0, Flags=....., BI=62, SSID=lin\357\277\275\001\004\357\277[Malformed Packet]			
14 0 499197	Linksys_67:22:94	Broadcast		802.11	90	Beacon frame, SN=3074, FN=0, Flags=....., BI=100, SSID=linksys12			
21 1.010949	Linksys_67:22:94	Broadcast		802.11	90	Beacon frame, SN=3079, FN=0, Flags=....., BI=100, SSID=linksys12			
23 1.113691	Linksys_67:22:94	Broadcast		802.11	90	Beacon frame, SN=3080, FN=0, Flags=....., BI=100, SSID=\357\277\275nksys			
34 1.406565	Linksys_67:22:94	Broadcast		802.11	90	Beacon frame, SN=3083, FN=0, Flags=....., BI=100, SSID=linksys12			
45 0.935064	Linksys_67:22:94	Broadcast		802.11	90	Beacon frame, SN=3084, FN=0, Flags=....., BI=100, SSID=linksys12			
16 7.076567	Linksys_67:22:94	ff:ff:c1:fe:ff:ff		802.11	90	Beacon frame, SN=3148, FN=0, Flags=....., BI=100, SSID=linksys12			
16 8.178944	Linksys_67:22:94	Broadcast		802.11	90	Beacon frame, SN=3149, FN=0, Flags=....., BI=100, SSID=lin\bhsys12			
25 11.660567	00:86:bc:d2:22:94	ff:ff:f9:fe:ff:ff		802.11	90	Beacon frame, SN=3183, FN=0, Flags=....., BI=114, SSID=linksys12			
1484 41.766821	Linksys_67:22:94	Broadcast		802.11	90	Beacon frame, SN=3401, FN=0, Flags=....., BI=100, SSID=linksys1R			
1494 42.382222	Linksys_67:22:94	Broadcast		802.11	90	Beacon frame, SN=3404, FN=0, Flags=....., BI=100, SSID=linksys1R			
1496 42.381070	Linksys_67:22:94	ff:ff:ff:ff:ff:ff		802.11	90	Beacon frame, SN=3485, FN=0, Flags=....., BI=16484, SSID=linksys12			
1515 42.892973	Linksys_67:22:94	ff:ff:ff:ff:ff:ff		802.11	90	Beacon frame, SN=3499, FN=0, Flags=....., BI=100, SSID=linksys12			
1519 43.097945	Linksys_67:22:94	Broadcast		802.11	90	Beacon frame, SN=3492, FN=0, Flags=....., BI=770, SSID=lin\357\277\275-y			
1521 43.200573	Linksys_67:22:94	Broadcast		802.11	90	Beacon frame, SN=3493, FN=0, Flags=....., BI=100, SSID=linksys12			
1520 43.917194	Linksys_67:22:94	ff:ff:ff:d2:ff:ff		802.11	90	Beacon frame, SN=3500, FN=0, Flags=....., BI=100, SSID=linksys12			
1544 44.000000	d3:00:00:00:00:00	ff:ff:ff:ff:ff:ff		802.11	1624	Beacon frame, SN=3501, FN=0, Flags=....., BI=100, SSID=linksys12[Packet size limited during capture]			
1550 44.633946	66:05:28:67:22:94	Broadcast		802.11	90	Beacon frame, SN=3507, FN=0, Flags=....., BI=100, SSID=lin\357\277\275y			
1557 44.887707	Cisco-L1_f5:ba:bb	Broadcast		802.11	132	Beacon frame, SN=3663, FN=13, Flags=....., BI=8, SSID=linksys_SES_2408\001\004\357\277\275\357\277\275[Packet size limited during capture]			
1894 56.102695	00:ac:20:67:22:94	5a:as:ff:ff:ff:ff		802.11	90	Beacon frame, SN=3620, FN=4, Flags=....., BI=100, SSID=lin\m\357\277\275[Packet size limited during capture]			
1994 59.325868	Cisco-L1_f5:ba:bb	Broadcast		802.11	132	Beacon frame, SN=3633, FN=0, Flags=....., BI=100, SSID=linksys_SES_24086			
2291 60.833795	Cisco-L1_f5:ba:bb	Broadcast		802.11	132	Beacon frame, SN=3640, FN=0, Flags=....., BI=100, SSID=linksys_SES_24086			
2319 70.833447	Linksys_67:22:94	Broadcast		802.11	90	Beacon frame, SN=3760, FN=0, Flags=....., BI=2304			
2342 72.282076	Linksys_67:22:94	7f:26:ff:ff:ff:ff		802.11	90	Beacon frame, SN=3779, FN=0, Flags=....., BI=100, SSID=linksys12[Packet size limited during capture]			
000 0000 0000 0000 = Duration: 0 microseconds Receiver address: ff:ff:af:d2:ff:ff (ff:ff:af:d2:ff:ff) Destination address: ff:ff:af:d2:ff:ff (ff:ff:af:d2:ff:ff) Transmitter address: Linksys_67:22:94 (00:00:00:25:67:22:94) Source address: Linksys_67:22:94 (00:00:00:25:67:22:94) BSS Id: Linksys_67:22:94 (00:00:00:25:67:22:94)									
1101 1010 1100 = Sequence number: 3500 Frame check sequence: 0x24f5293b incorrect, should be 0xd46468d9 ▼ [Expert Info (Error/ Malformed): Bad checksum [should be 0xd46468d9]] [Bad checksum [should be 0xd46468d9]] [Severity: level: Error] [Offset: 0x0000000000000000] [Offset: 0x0000000000000000] [FCS Status: Bad] 									

Filtro que apresenta tramas com checksum incorreto

wlan.fc.type_subtype == 0x08 and wlan.fc.status == "Good"							
No.	Time	Source	Destination	Protocol	Length	Info	
1470 41.146040		Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3409, Fw=0, Flags=.....C, BI=100, SSID=30 Munroe St	
1471 41.246889		Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3411, Fw=0, Flags=.....C, BI=100, SSID=30 Munroe St	
1472 41.458976		Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3402, Fw=0, Flags=.....C, BI=100, SSID=30 Munroe St	
1473 41.453247		Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3493, Fw=0, Flags=.....C, BI=100, SSID=30 Munroe St	
1474 41.555626		Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3494, Fw=0, Flags=.....C, BI=100, SSID=30 Munroe St	
1475 41.657940		Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3495, Fw=0, Flags=.....C, BI=100, SSID=30 Munroe St	
1476 41.768770		Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3496, Fw=0, Flags=.....C, BI=100, SSID=30 Munroe St	
1477 41.872732		Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3497, Fw=0, Flags=.....C, BI=100, SSID=30 Munroe St	
1486 41.868946		LinksysG_67:22:94	Broadcast	802.11	190	Beacon frame, SN=3480, Fw=0, Flags=.....C, BI=100, SSID=linksys12	
1487 41.965189		Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3498, Fw=0, Flags=.....C, BI=100, SSID=linksys12	
1488 41.971328		LinksysG_67:22:94	Broadcast	802.11	190	Beacon frame, SN=3481, Fw=0, Flags=.....C, BI=100, SSID=linksys12	
1489 42.067611		Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3499, Fw=0, Flags=.....C, BI=100, SSID=30 Munroe St	
1490 42.176027		Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3500, Fw=0, Flags=.....C, BI=100, SSID=30 Munroe St	
1492 42.176095		LinksysG_67:22:94	Broadcast	802.11	183	Beacon frame, SN=3501, Fw=0, Flags=.....C, BI=100, SSID=linksys12	
1493 42.272354		Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3501, Fw=0, Flags=.....C, BI=100, SSID=30 Munroe St	
1495 42.374762		Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3502, Fw=0, Flags=.....C, BI=100, SSID=30 Munroe St	
1497 42.477127		Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3503, Fw=0, Flags=.....C, BI=100, SSID=30 Munroe St	
1498 42.483570		LinksysG_67:22:94	Broadcast	802.11	183	Beacon frame, SN=3486, Fw=0, Flags=.....C, BI=100, SSID=linksys12	
1499 42.483599		Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3487, Fw=0, Flags=.....C, BI=100, SSID=linksys_SES_24086	
1500 42.579556		Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3504, Fw=0, Flags=.....C, BI=100, SSID=30 Munroe St	
1501 42.681946		Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3505, Fw=0, Flags=.....C, BI=100, SSID=30 Munroe St	
1502 42.784400		Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3506, Fw=0, Flags=.....C, BI=100, SSID=30 Munroe St	
1513 42.839707		Cisco-Li_fs:b:a:bb	Broadcast	802.11	183	Beacon frame, SN=3643, Fw=0, Flags=.....C, BI=100, SSID=linksys_SES_24086	
1514 42.885776		Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3508, Fw=0, Flags=.....C, BI=100, SSID=30 Munroe St	

Frame Control Field: 0x8000
.0000 0000 0000 Duration: 0 microseconds
Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
Source address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
.... 0000 = Fragment number: 0
1011 0100 0110 = Sequence number: 2886
Frame check sequence: 0x813f0226 [correct]
[FCS Status: Good]

Filtro que apresenta tramas com checksum correto

12) Identifique e registe todos os endereços MAC usados nas tramas beacon enviadas pelos APs. Recorde que o endereçamento está definido no cabeçalho das tramas 802.11 podendo ser utilizados até quatro endereços com diferente semântica.

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 0100 0110 = Sequence number: 2886
Frame check sequence: 0x813f0226 [correct]

13) Estabeleça um filtro Wireshark apropriado que lhe permita visualizar todas as tramas probing request e probing response, simultaneamente.

O comando usado foi:

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

14) Quais são os endereços MAC BSS ID de destino e origem nestas tramas? Qual o objetivo deste tipo de tramas?

O Probe Request é enviado de uma estação quando requer informações de outra estação. A Probe Response é enviada de um AP que contém informações de capacidade, taxas de dados suportadas, entre outras, após receber um Probe Request.

```
118 6.300439 IntelCor_1f:5.. Broadcast      802... 70 Probe Request, SN=621, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
```

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)

```
132 6.407562 Cisco-Li_f7:1.. IntelCor_1f:5.. 802... 177 Probe Response, SN=2924, FN=0, Flags=...R...C, BI=100, SSID=30 Munroe St
```

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)

15) Identifique um probing request para o qual tenha havido um probing response. Face ao endereçamento usado, indique a que sistemas são endereçadas estas tramas e explique qual o propósito das mesmas?

Através do Probe Request, a estação solicita informações de um AP específico (especificado pelo SSID), ou de todos os AP's na área (especificados com o SSID Broadcast). Neste caso, verificamos a segunda opção:

```
21.. 63.140106 IntelCor_d1:b.. Broadcast 802... 94 Probe Request, SN=1647, FN=0, Flags=.....C, SSID=30 Munroe St
21.. 63.142451 Cisco-Li_f7:1.. IntelCor_d1:b.. 802... 177 Probe Response, SN=3724, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
21.. 63.689723 Cisco-Li_f7:1.. IntelCor_d1:b.. 802... 177 Probe Response, SN=3734, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
22.. 66.689593 Cisco-Li_f7:1.. IntelCor_d1:b.. 802... 177 Probe Response, SN=3766, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
22.. 69.689574 Cisco-Li_f7:1.. IntelCor_d1:b.. 802... 177 Probe Response, SN=3796, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
23.. 72.689208 Cisco-Li_f7:1.. IntelCor_d1:b.. 802... 177 Probe Response, SN=3827, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
```

```
Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
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: Broadcast (ff:ff:ff:ff:ff:ff)
```

A Probe Response é enviada para a estação que requisitou a informação (mostrado nas imagens).

```
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)
```

6 - Processo de Associação

16) Quais as duas ações realizadas (i.e., tramas enviadas) pelo host no trace imediatamente após t=49 para terminar a associação com o AP 30 Munroe St que estava ativa quando o trace teve início?

- 1.

```
| 17... 49.583615 192.168.1.109 192.168.1.1      DHCP      390 DHCP Release - Transaction ID 0xea5a526.
```

```
> Frame 1735: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
-> IEEE 802.11 Deauthentication, Flags: .......c
    Type/Subtype: Deauthentication (0x000c)
-> Frame Control Field: 0xc000
    .... ..00 = Version: 0
    .... 00.. = Type: Management frame (0)
    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
    .0000 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)
```

- 2.

```
| 17... 49.609617 IntelCor_d1:b... Cisco-Li_f7:1... 802.11      54 Deauthentication, SN=1605, FN=0, Flags=.....c
```

```
> Radiotap Header v0, Length 24
> 802.11 radio information
-> IEEE 802.11 Deauthentication, Flags: .......c
    Type/Subtype: Deauthentication (0x000c)
-> Frame Control Field: 0xc000
    .... ..00 = Version: 0
    .... 00.. = Type: Management frame (0)
    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
    .0000 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)
```

17) Examine o trace e procure tramas de authentication enviadas do host para um AP e vice-versa. Quantas mensagens de authentication foram enviadas do host para o AP **linksys_ses_24086** (que tem o endereço MAC **Cisco_Li_f5:ba:bb**) aproximadamente ao t=49?

wlan.fc.type_subtype == 0x0b and wlan.da == 00:18:39:f5:ba:bb

Filtro aplicado no Wireshark

Cerca de 6 tramas aproximadamente ao t=49.

No.	Time	Source	Destination	Protocol	Length	Info
1740	49.638857	IntelCor_d1:b6:4f Cisco-Li_f5:ba:bb		802.11	58	Authentication, SN=1606, FN=0, Flags=.....C
1741	49.639700	IntelCor_d1:b6:4f Cisco-Li_f5:ba:bb		802.11	58	Authentication, SN=1606, FN=0, Flags=....R..C
1742	49.640702	IntelCor_d1:b6:4f Cisco-Li_f5:ba:bb		802.11	58	Authentication, SN=1606, FN=0, Flags=....R..C
1744	49.642315	IntelCor_d1:b6:4f Cisco-Li_f5:ba:bb		802.11	58	Authentication, SN=1606, FN=0, Flags=....R..C
1746	49.645319	IntelCor_d1:b6:4f Cisco-Li_f5:ba:bb		802.11	58	Authentication, SN=1606, FN=0, Flags=....R..C
1749	49.649765	IntelCor_d1:b6:4f Cisco-Li_f5:ba:bb		802.11	58	Authentication, SN=1606, FN=0, Flags=....R..C
1821	53.785833	IntelCor_d1:b6:4f Cisco-Li_f5:ba:bb		802.11	58	Authentication, SN=1612, FN=0, Flags=.....C
1822	53.787070	IntelCor_d1:b6:4f Cisco-Li_f5:ba:bb		802.11	58	Authentication, SN=1612, FN=0, Flags=....R..C
1921	57.889232	IntelCor_d1:b6:4f Cisco-Li_f5:ba:bb		802.11	58	Authentication, SN=1619, FN=0, Flags=.....C
1922	57.890325	IntelCor_d1:b6:4f Cisco-Li_f5:ba:bb		802.11	58	Authentication, SN=1619, FN=0, Flags=....R..C
1923	57.891321	IntelCor_d1:b6:4f Cisco-Li_f5:ba:bb		802.11	58	Authentication, SN=1619, FN=0, Flags=....R..C
1924	57.896970	IntelCor_d1:b6:4f Cisco-Li_f5:ba:bb		802.11	58	Authentication, SN=1619, FN=0, Flags=....R..C
2122	62.171951	IntelCor_d1:b6:4f Cisco-Li_f5:ba:bb		802.11	58	Authentication, SN=1644, FN=0, Flags=.....C
2123	62.172946	IntelCor_d1:b6:4f Cisco-Li_f5:ba:bb		802.11	58	Authentication, SN=1644, FN=0, Flags=....R..C
2124	62.174070	IntelCor_d1:b6:4f Cisco-Li_f5:ba:bb		802.11	58	Authentication, SN=1644, FN=0, Flags=....R..C

Packets: 2364 · Displayed: 15 (0.6%)

Número de tramas mostradas após ser aplicado o filtro

18) Qual o tipo de autenticação pretendida pelo host, aberta ou usando uma chave?

Autenticação aberta.

- ▶ Frame 1740: 58 bytes on wire (464 bits), 58 bytes captured (464 bits)
- ▶ Radiotap Header v0, Length 24
- ▶ 802.11 radio information
- ▶ IEEE 802.11 Authentication, Flags:C
- ▶ IEEE 802.11 wireless LAN
 - ▼ Fixed parameters (6 bytes)
 - Authentication Algorithm: Open System (0)
 - Authentication SEQ: 0x0001
 - Status code: Successful (0x0000)

19) Observa-se a resposta de authentication do AP linksys_ses_24086 AP no trace?

Não se verifica resposta.

No.	Time	Source	Destination	Protocol	Length	Info
17...	49.638857	IntelCor_d1:b...	Cisco-Li_f5:b...	802.11	58	Authentication, SN=1606, FN=0, Flags=.....C
17...	49.639700	IntelCor_d1:b...	Cisco-Li_f5:b...	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
17...	49.640702	IntelCor_d1:b...	Cisco-Li_f5:b...	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
17...	49.642315	IntelCor_d1:b...	Cisco-Li_f5:b...	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
17...	49.645319	IntelCor_d1:b...	Cisco-Li_f5:b...	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
17...	49.649705	IntelCor_d1:b...	Cisco-Li_f5:b...	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
18...	53.785833	IntelCor_d1:b...	Cisco-Li_f5:b...	802.11	58	Authentication, SN=1612, FN=0, Flags=.....C
18...	53.787070	IntelCor_d1:b...	Cisco-Li_f5:b...	802.11	58	Authentication, SN=1612, FN=0, Flags=....R...C
19...	57.889232	IntelCor_d1:b...	Cisco-Li_f5:b...	802.11	58	Authentication, SN=1619, FN=0, Flags=.....C
19...	57.890325	IntelCor_d1:b...	Cisco-Li_f5:b...	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
19...	57.891321	IntelCor_d1:b...	Cisco-Li_f5:b...	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
19...	57.896970	IntelCor_d1:b...	Cisco-Li_f5:b...	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
21...	62.171951	IntelCor_d1:b...	Cisco-Li_f5:b...	802.11	58	Authentication, SN=1644, FN=0, Flags=.....C
21...	62.172946	IntelCor_d1:b...	Cisco-Li_f5:b...	802.11	58	Authentication, SN=1644, FN=0, Flags=....R...C
21...	62.174070	IntelCor_d1:b...	Cisco-Li_f5:b...	802.11	58	Authentication, SN=1644, FN=0, Flags=....R...C
21...	63.168087	IntelCor_d1:b...	Cisco-Li_f7:1...	802.11	58	Authentication, SN=1647, FN=0, Flags=.....C
21...	63.169071	Cisco-Li_f7:1...	IntelCor_d1:b...	802.11	58	Authentication, SN=3726, FN=0, Flags=.....C
21...	63.169707	IntelCor_d1:b...	Cisco-Li_f7:1...	802.11	58	Authentication, SN=1647, FN=0, Flags=....R...C
21...	63.170692	Cisco-Li_f7:1...	IntelCor_d1:b...	802.11	58	Authentication, SN=3727, FN=0, Flags=.....C

20) Vamos agora considerar o que acontece quando o host desiste de se associar ao AP linksys_ses_24086 AP e se tenta associar ao AP 30 Munroe St. Procure tramas authentication enviadas pelo host para e do AP e vice-versa. Em que tempo aparece um trama authentication do host para o AP 30 Munroe St. e quando aparece a resposta authentication do AP para o host?

Aparece uma trama Authentication de 00:13:02:d1:b6:4f para 00:16:b7:f7:1d:51, no $t = 63.168087$.

21... 63.168087 IntelCor_d1:b... Cisco-Li_f7:1... 802.11 58 Authentication, SN=1647, FN=0, Flags=.....C

▼ IEEE 802.11 Authentication, Flags:C
Type/Subtype: Authentication (0x000b)
► Frame Control Field: 0xb000
.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 0110 1111 = Sequence number: 1647
Frame check sequence: 0x47e8cbe0 [correct]
[FCS Status: Good]

A resposta é enviada no $t = 63.169071$.

21... 63.169071 Cisco-Li_f7:1... IntelCor_d1:b... 802.11 58 Authentication, SN=3726, FN=0, Flags=.....C

```

▼ IEEE 802.11 Authentication, Flags: . . . . . C
  Type/Subtype: Authentication (0x000b)
  ▶ Frame Control Field: 0xb000
    . 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 1000 1110 . . . = Sequence number: 3726
    Frame check sequence: 0x93eaefc9 [correct]
    [FCS Status: Good]

```

Filtro usado:

wlan.fc.subtype == 11

21) Um associate request do host para o AP e uma trama de associate response correspondente do AP para o host são usados para que o host seja associado a um AP. Quando aparece o associate request do host para o AP 30 Munroe St? Quando é enviado o correspondente associate reply

O ASSOCIATE REQUEST do host para o AP 30 Munroe St aparece aos 63.169910s e foi respondido aos 63.192101s.

21.. 63.169910 IntelCor_d1:b.. Cisco-Li_f7:1.. 802.11	89 Association Request, SN=1648, FN=0, Flags=.....C, SSID=30 Munroe St
21.. 63.192101 Cisco-Li_f7:1.. IntelCor_d1:b.. 802.11	94 Association Response, SN=3728, FN=0, Flags=.....C

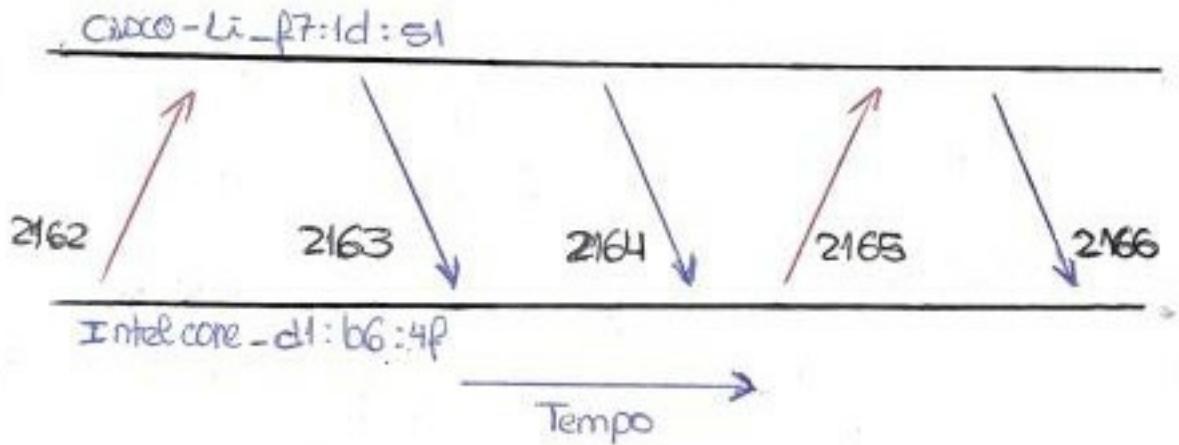
22) Que taxas de transmissão o host está disposto a usar? E o AP?

▼ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18, [Mbit/sec]
--

23) Identifique uma sequência de tramas que corresponda a um processo de associação completo entre a STA e o AP, incluindo a fase de autenticação.

21.. 63.169910 IntelCor_d1:b.. Cisco-Li_f7:1.. 802.11	89 Association Request, SN=1648, FN=0, Flags=.....C, SSID=30 Munroe St
21.. 63.170008 IntelCor_d1:b.. 802.11	38 Acknowledgement, Flags=.....C
21.. 63.170692 Cisco-Li_f7:1.. IntelCor_d1:b.. 802.11	58 Authentication, SN=3727, FN=0, Flags=.....C
21.. 63.171000 Cisco-Li_f7:1.. 802.11	38 Acknowledgement, Flags=.....C
21.. 63.192101 Cisco-Li_f7:1.. IntelCor_d1:b.. 802.11	94 Association Response, SN=3728, FN=0, Flags=.....C

24) Efetue um diagrama que ilustre a sequência de todas as tramas trocadas no processo de associação, incluindo a fase de autenticação.



25) Encontre a trama 802.11 que contém o segmento SYN TCP para a primeira sessão TCP (download alice.txt). Quais são os três campos dos endereços MAC na trama 802.11?

Os três campos dos MAC addresses são 00:13:02:d1:b6:4f, 00:16:b6:f4:eb:a8 e 00:16:b6:f7:1d:51.

474	24.811093	192.168.1.109	128.119.245.12	TCP	110 2538 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
475	24.811231		IntelCor_d1:b.. 802.11		38 Acknowledgement, Flags=.....C
476	24.827751	128.119.245.12	192.168.1.109	TCP	110 80 → 2538 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 SACK_PERM=1
477	24.827922		Cisco-Li_f7:1.. 802.11		38 Acknowledgement, Flags=.....C
478	24.828024	192.168.1.109	128.119.245.12	TCP	102 2538 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
479	24.828140		IntelCor_d1:b.. 802.11		38 Acknowledgement, Flags=.....C
+ 480	24.828253	192.168.1.109	128.119.245.12	HTTP	537 GET /wireshark-labs/alice.txt HTTP/1.1

26) Qual o endereço MAC nesta trama que corresponde ao host (em notação hexadecimal)? Qual o do AP? Qual o do router do primeiro salto? Qual o endereço IP do host que está a enviar este segmento TCP? Qual o endereço IP de destino?

O MAC address do host é 00:13:02:d1:b6:4f, o do AP é 00:16:b6:f7:1d:51 e o do router do primeiro salto é 00:16:b6:f4:eb:a8. O endereço IP do host é 192.168.1.109 e o endereço IP de destino é 128.119.245.12.

27) Este endereço IP de destino corresponde ao host, AP, router do primeiro salto, ou outro equipamento de rede? Justifique.

Sabemos que não corresponde ao host porque o host somos nós, sabemos também que não é o AP porque o AP não tem um IP e não é o router porque este não faz parte da nossa rede. Concluímos assim que corresponde a outro equipamento de rede.

28) Encontre agora a trama 802.11 que contém o segmento SYNACK para esta sessão TCP. Quais são os três campos dos endereços MAC na trama 802.11?

Os três campos de MAC address são 00:16:b6:f4:eb:a8, 00:16:b6:f7:1d:51 e 91:2a:b0:49:b6:4f.

```
-->-----  
Receiver address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)  
Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)  
Destination address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)  
Source address: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)  
BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)  
STA address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
```

29) Qual o endereço MAC nesta trama que corresponde ao host? Qual o do AP? Qual o do router do primeiro salto?

O MAC address que corresponde ao host é 00:16:b6:f4:eb:a8. O MAC address que corresponde ao AP é 00:16:b6:f7:1d:51. O MAC address que corresponde ao router do primeiro salto 91:2a:b0:49:b6:4f.

30) O endereço MAC de origem na trama corresponde ao endereço IP do dispositivo que enviou o segmento TCP encapsulado neste datagrama? Justifique.

Corresponde. Na pergunta 28 descobrimos qual o host(MAC address de origem), na pergunta 29 descobrimos qual o endereço IP do dispositivo que enviou o segmento TCP e concluímos que é o mesmo.

Conclusões

Com este trabalho expandimos o nosso conhecimento acerca de redes sem fios. Aprofundamos o nosso conhecimento sobre tramas de gestão, que nos permitem analisar as comunicações entre STA's(estações) e AP's.

As tramas de gestão que exploramos foram, authentication, association request e response, beacon, e probe request e response.

As tramas de dados permitiram-nos analisar os vários pacotes e recolher informação importante sobre a gestão da rede.

Este trabalho ajudou-nos a perceber melhor sobre diferentes conceitos e a consolidar o conhecimento dos protocolos, aplicando filtros no wireshark.