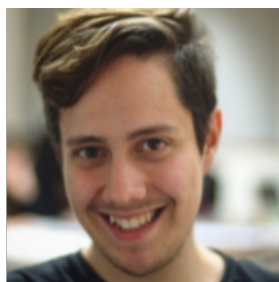




Beatriz Rocha
A84003



Filipe Guimarães
A85308



Gonçalo Ferreira
A84073

Relatório do Trabalho Prático 4 de Redes de Computadores Grupo 1

17 de Dezembro de 2019



Conteúdo

1	Acesso Rádio	4
1.1	Pergunta 1	4
1.2	Pergunta 2	4
1.3	Pergunta 3	4
2	Scanning	6
2.1	Pergunta 4	6
2.2	Pergunta 5	6
2.3	Pergunta 6	7
2.4	Pergunta 7	7
2.5	Pergunta 8	8
2.6	Pergunta 9	8
2.7	Pergunta 10	9
2.8	Pergunta 11	9
2.9	Pergunta 12	10
2.10	Pergunta 13	10
2.11	Pergunta 14	11
2.12	Pergunta 15	11
3	Processo de Associação	13
3.1	Pergunta 16	13
3.2	Pergunta 17	14
3.3	Pergunta 18	14
3.4	Pergunta 19	14
3.5	Pergunta 20	15
3.6	Pergunta 21	15
3.7	Pergunta 22	16
3.8	Pergunta 23	17
3.9	Pergunta 24	17
4	Transferência de Dados	19
4.1	Pergunta 25	19
4.2	Pergunta 26	19
4.3	Pergunta 27	20
4.4	Pergunta 28	20
4.5	Pergunta 29	21
4.6	Pergunta 30	21

Lista de Figuras

1.1	Trama correspondente ao número 1401	4
2.1	SSIDs dos dois APs que estão a emitir a maioria das tramas beacon	6
2.2	Intervalos de tempo entre transmissões	7
2.3	Endereços MAC	7
2.4	Data rates e extended supported rates	8
2.5	Campo <i>Type/Subtype</i> da trama 1402	9
2.6	Filtro aplicado	9
2.7	Endereços MAC usados	10
2.8	Probe request	11
2.9	Probe response	11
2.10	Probing request para o qual houve um probing response	11
3.1	Trace imediatamente após t=49	13
3.2	Mensagens de authentication	14
3.3	Tramas authentication enviadas pelo host para e do AP e vice-versa	15
3.4	Associate request e associate response	15
3.5	Taxas de transmissão que o host está disposto a usar	16
3.6	Taxas de transmissão que o AP está disposto a usar	16
3.7	Filtro aplicado	17
3.8	Captura sem filtros	17
3.9	Diagrama que ilustra a sequência de todas as tramas trocadas . .	18
4.1	Segmentos para a primeira sessão tcp	19
4.2	Endereços IP para o primeiro segmento da primeira sessão TCP .	20
4.3	Trama 802.11 que contém o segmento SYNACK	20

Capítulo 1

Acesso Rádio

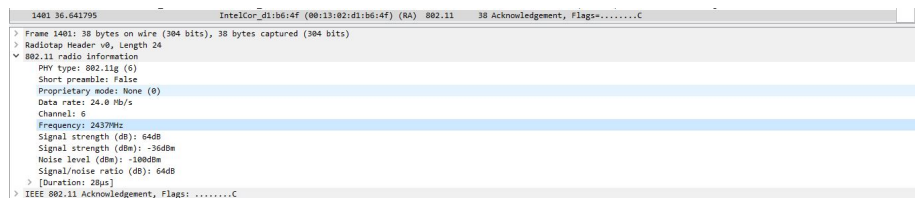


Figura 1.1: Trama correspondente ao número 1401

1.1 Pergunta 1

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

Como podemos observar na figura acima, a rede sem fios está a operar na frequência do espectro 2437 MHz, que corresponde ao canal 6.

1.2 Pergunta 2

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

A versão da norma IEEE 802.11 que está a ser usada é 802.11g, como pode ser visto no campo PHY type da figura acima.

1.3 Pergunta 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.

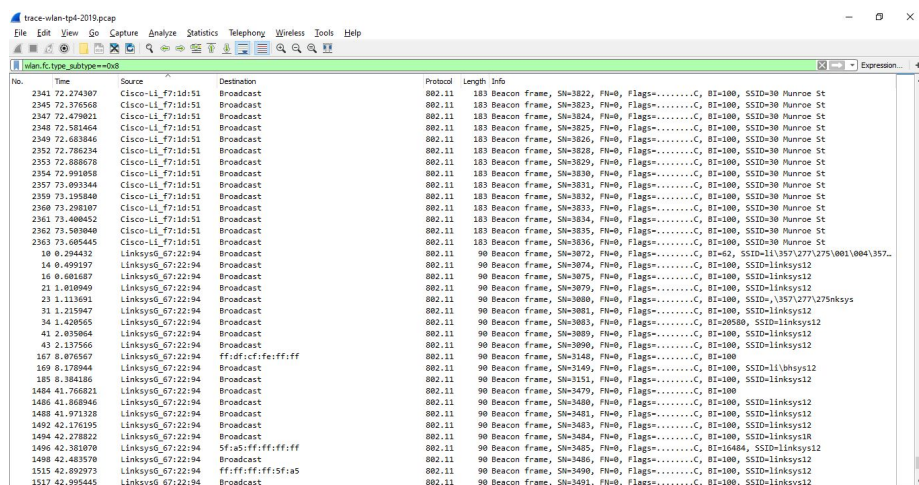
A trama escolhida foi enviada a um débito de 24 Mb/s, como podemos ver no campo Data rate da figura acima. Este débito não corresponde ao débito máximo a que a interface Wi-Fi pode operar, uma vez que esse é 54 Mb/s, pois a versão da norma IEEE 802.11 que está a ser usada é 802.11g.

Capítulo 2

Scanning

2.1 Pergunta 4

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



No.	Time	Source	Destination	Protocol	Length	Info
2341	72.274307	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3822, Fm=0, Flags=.....C, B=100, SSID=30 Munroe St
2345	72.376568	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3823, Fm=0, Flags=.....C, B=100, SSID=30 Munroe St
2347	72.479821	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3824, Fm=0, Flags=.....C, B=100, SSID=30 Munroe St
2348	72.501464	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3825, Fm=0, Flags=.....C, B=100, SSID=30 Munroe St
2349	72.683846	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3826, Fm=0, Flags=.....C, B=100, SSID=30 Munroe St
2352	72.786234	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3828, Fm=0, Flags=.....C, B=100, SSID=30 Munroe St
2353	72.888678	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3829, Fm=0, Flags=.....C, B=100, SSID=30 Munroe St
2354	72.991858	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3830, Fm=0, Flags=.....C, B=100, SSID=30 Munroe St
2357	73.093344	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3831, Fm=0, Flags=.....C, B=100, SSID=30 Munroe St
2359	73.195880	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3832, Fm=0, Flags=.....C, B=100, SSID=30 Munroe St
2360	73.298197	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3833, Fm=0, Flags=.....C, B=100, SSID=30 Munroe St
2361	73.400452	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3834, Fm=0, Flags=.....C, B=100, SSID=30 Munroe St
2362	73.503040	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3835, Fm=0, Flags=.....C, B=100, SSID=30 Munroe St
2363	73.605445	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3836, Fm=0, Flags=.....C, B=100, SSID=30 Munroe St
18	0.294432	Linksys6_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3872, Fm=0, Flags=.....C, B=42, SSID=11\357\277\275\003\004\357..
14	0.499197	Linksys6_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3874, Fm=0, Flags=.....C, B=100, SSID=linksys12
16	0.601887	Linksys6_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3875, Fm=0, Flags=.....C, B=100, SSID=linksys12
21	1.010949	Linksys6_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3879, Fm=0, Flags=.....C, B=100, SSID=linksys12
23	1.113691	Linksys6_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3880, Fm=0, Flags=.....C, B=100, SSID=11\357\277\275\003\004\357..
31	1.215947	Linksys6_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3881, Fm=0, Flags=.....C, B=100, SSID=linksys12
34	1.420905	Linksys6_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3883, Fm=0, Flags=.....C, B=100, SSID=linksys12
41	2.035084	Linksys6_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3889, Fm=0, Flags=.....C, B=100, SSID=linksys12
43	2.137566	Linksys6_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3890, Fm=0, Flags=.....C, B=100, SSID=linksys12
167	8.076567	Linksys6_67:22:94	ff:ff:ff:ff:ff:ff	802.11	90	Beacon frame, SN=3148, Fm=0, Flags=.....C, B=100, SSID=linksys12
169	8.178944	Linksys6_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3149, Fm=0, Flags=.....C, B=100, SSID=11\357\277\275\003\004\357..
185	8.384186	Linksys6_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3151, Fm=0, Flags=.....C, B=100, SSID=linksys12
1484	41.766821	Linksys6_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3479, Fm=0, Flags=.....C, B=100, SSID=linksys12
1486	41.860946	Linksys6_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3480, Fm=0, Flags=.....C, B=100, SSID=linksys12
1488	41.971328	Linksys6_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3481, Fm=0, Flags=.....C, B=100, SSID=linksys12
1492	42.176195	Linksys6_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3483, Fm=0, Flags=.....C, B=100, SSID=linksys12
1494	42.278222	Linksys6_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3484, Fm=0, Flags=.....C, B=100, SSID=linksys12
1496	42.361070	Linksys6_67:22:94	Sf:a5:ff:ff:ff:ff	802.11	90	Beacon frame, SN=3485, Fm=0, Flags=.....C, B=16404, SSID=linksys12
1498	42.483570	Linksys6_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3486, Fm=0, Flags=.....C, B=100, SSID=linksys12
1515	42.892973	Linksys6_67:22:94	ff:ff:ff:ff:ff:ff	802.11	90	Beacon frame, SN=3490, Fm=0, Flags=.....C, B=100, SSID=linksys12
1517	42.995445	Linksys6_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3491, Fm=0, Flags=.....C, B=100, SSID=linksys12

Figura 2.1: SSIDs dos dois APs que estão a emitir a maioria das tramas beacon

Tendo em consideração que as beacon frames apresentam Type/Subtype 0x0008, começamos por aplicar o filtro wlan.fc.type_subtype==0x8 para visualizarmos apenas as beacon frames. Posto isto, os SSIDs dos dois APs que estão a emitir a maioria das tramas beacon são 30 Munroe St e linksys12, como podemos ver na figura acima.

2.2 Pergunta 5

Qual o intervalo de tempo entre a transmissão de tramas beacon para o AP linksys.ses.24086? E do AP 30 Munroe St? (Pista: o intervalo

está contido na própria trama). Na prática, a periodicidade de tramas beacon é verificada? Tente explicar porquê.

```
> Frame 2290: 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: .....C
▼ IEEE 802.11 wireless LAN
  ▼ Fixed parameters (12 bytes)
    Timestamp: 6351990989206
    Beacon Interval: 0.102400 [Seconds]
    > Capabilities Information: 0x0011
  > Tagged parameters (68 bytes)
```

Figura 2.2: Intervalos de tempo entre transmissões

O intervalo de tempo entre a transmissão de tramas beacon para o AP linksys_ses_24086 é 0.1024 segundos, bem como do AP 30 Munroe St, como podemos ver na figura acima. Na prática, a periodicidade de tramas beacon é verificada, o que se deve ao facto de as principais funções do Beacon Interval ser alertar que a rede está ativa e sincronizar a transmissão dos dados, sendo costume variar entre os 10 e os 1000 milissegundos.

2.3 Pergunta 6

Qual é (em notação hexadecimal) o endereço MAC de origem da trama beacon de 30 Munroe St? Para detalhes sobre a estrutura das tramas 802.11, veja a secção 7 da norma IEEE 802.11 citada no início.

```
245 11.348982 Cisco-Li_f7:1d:51 Broadcast 802.11 183 Beacon frame, SN=2981, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
> Frame Control Field: 0x0000
  .000 0000 0000 0000 = Duration: 0 microseconds
  Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
  Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
  Source address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
  BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
  .... .... 0000 = Fragment number: 0
  1011 1010 0101 .... = Sequence number: 2981
  Frame check sequence: 0x1a3772d3 [unverified]
  [FCS Status: Unverified]
> IEEE 802.11 wireless LAN
```

Figura 2.3: Endereços MAC

O endereço MAC de origem da trama beacon de 30 Munroe St é 00:16:b6:f7:1d:51, como podemos ver no campo Source address da figura acima.

2.4 Pergunta 7

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

O endereço MAC de destino na trama de 30 Munroe St é ff:ff:ff:ff:ff:ff, como podemos ver no campo Destination address da figura 2.3.

2.5 Pergunta 8

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

O MAC BSS ID da trama beacon de 30 Munroe St é 00:16:b6:f7:1d:51, como podemos ver no campo BSS Id da figura 2.3.

2.6 Pergunta 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?

```
▼ IEEE 802.11 wireless LAN
  ▼ Fixed parameters (12 bytes)
    Timestamp: 174392627586
    Beacon Interval: 0.102400 [Seconds]
    > Capabilities Information: 0x0601
  ▼ Tagged parameters (119 bytes)
    > Tag: SSID parameter set: 30 Munroe St
    ▼ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
      Tag Number: Supported Rates (1)
      Tag length: 4
      Supported Rates: 1(B) (0x82)
      Supported Rates: 2(B) (0x84)
      Supported Rates: 5.5(B) (0x8b)
      Supported Rates: 11(B) (0x96)
    > Tag: DS Parameter set: Current Channel: 6
    > Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    > Tag: Country Information: Country Code US, Environment Indoor
    > Tag: EDCA Parameter Set
    > Tag: ERP Information
    ▼ Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
      Tag Number: Extended Supported Rates (50)
      Tag length: 8
      Extended Supported Rates: 6(B) (0x8c)
      Extended Supported Rates: 9 (0x12)
      Extended Supported Rates: 12(B) (0x98)
      Extended Supported Rates: 18 (0x24)
      Extended Supported Rates: 24(B) (0xb0)
      Extended Supported Rates: 36 (0x48)
      Extended Supported Rates: 48 (0x60)
      Extended Supported Rates: 54 (0x6c)
    > Tag: Vendor Specific: Airgo Networks, Inc.
    > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
```

Figura 2.4: Data rates e extended supported rates

Os quatro data rates que o AP 30 Munroe St suporta são 1, 2, 5.5 e 11 em Mbit/s e os oito extended supported rates que o mesmo AP suporta são 6, 9, 12, 18, 24, 36, 48 e 54 em Mbit/s, como podemos ver na figura acima.

2.7 Pergunta 10

Selecione uma trama beacon (e.g., a trama 1YXX com Y=turno e XX=grupo, e.g., 1101). 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 (ver anexo)?

1402 36.743046	Cisco-Li_f7:1d:51	Broadcast	802.11	183 Beacon frame, SN=3445, FH=0, Flags=.....C, BI=100, SSID=30 Munroe St
1403 36.845467	Cisco-Li_f7:1d:51	Broadcast	802.11	183 Beacon frame, SN=3446, FH=0, Flags=.....C, BI=100, SSID=30 Munroe St

<

> Frame 1402: 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:C

Type/Subtype: Beacon frame (0x0008)

> Frame Control Field: 0x0000

.000 0000 0000 0000 = Duration: 0 microseconds

Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)

Destination address: Broadcast (ff:ff:ff:ff:ff:ff)

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

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

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

.... 0000 = Fragment number: 0

1101 0111 0101 = Sequence number: 3445

Frame check sequence: 0xe7773235 [unverified]

[FCS Status: Unverified]

Figura 2.5: Campo *Type/Subtype* da trama 1402

Uma vez que a trama correspondente ao nosso grupo é do tipo *Acknowledgement*, vamos considerar a trama seguinte (1402). O tipo de tramas 802.11 a que esta trama pertence é Beacon frame e o valor dos identificadores de tipo e subtipo é 0x0008, tal como podemos ver no campo Type/Subtype da figura acima. Esta informação encontra-se no campo frame control do cabeçalho da trama.

2.8 Pergunta 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.

[wlan.fc.type_subtype==0x0008 && wlan.fcs.status==bad]						Expression...	
No.	Time	Source	Destination	Protocol	Length	Info	

Figura 2.6: Filtro aplicado

No final da trama, vimos que o método de deteção de erros CRC (campo Frame check sequence) existe, mas não está a ser verificado ([unverified]) (figura 2.5). De seguida, observamos se todas as tramas beacon são recebidas corretamente, aplicando o filtro `wlan.fc.type_subtype==0x0008 && wlan.fcs.status==bad`. Nenhuma mensagem é recebida incorretamente, tal como podemos ver na figura acima. A deteção de erros é crucial neste tipo de redes locais, uma vez que existe uma elevada probabilidade de colisão. Para além disso, é importante mencionar que este método de deteção de erros é relativamente fácil de implementar. Acreditamos que, no nosso caso, o CRC poderá não estar a ser verificado, uma vez que o hardware poderá estar a filtrar as mensagens incorretas e, conseqüentemente, estas não chegam aos níveis superiores.

2.9 Pergunta 12

Identifique e registre 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. Para uma descrição detalhada da estrutura da trama 802.11, consulte o anexo ao enunciado.

```
> Frame Control Field: 0x8000
.000 0000 0000 0000 = Duration: 0 microseconds
Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
Source address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
```

0000	00 00 18 00 ee 58 00 00	10 02 85 09 a0 00 e2 9cX.....
0010	64 00 00 46 35 32 77 e7	80 00 00 00 ff ff ff ff	d..F52w.....
0020	ff ff 00 16 b6 f7 1d 51	00 16 b6 f7 1d 51 50 d7Q.....QP.
0030	82 d1 69 98 28 00 00 00	64 00 01 06 00 0c 33 30	..i.(...d....30
0040	20 4d 75 6e 72 6f 65 20	53 74 01 04 82 84 8b 96	Munroe St.....
0050	03 01 06 05 04 00 01 00	00 07 06 55 53 49 01 0bUSI..
0060	1a 0c 12 0f 00 03 a4 00	00 27 a4 00 00 42 43 5e'...BC^
0070	00 62 32 2f 00 2a 01 00	32 08 8c 12 98 24 b0 48	..b2/.*. 2....\$.H
0080	60 6c dd 15 00 0a f5 0a	02 40 c0 00 03 01 03 05	`l.....@.....
0090	0e 04 ff 00 03 00 11 01	01 dd 18 00 50 f2 02 01P...
00a0	01 0f 00 03 a4 00 00 27	a4 00 00 42 43 5e 00 62'...BC^..b
00b0	32 2f 00 35 32 77 e7		2/.52w..

Figura 2.7: Endereços MAC usados

Na figura acima, podemos ver que nas tramas beacon enviadas pelos APs estão presentes três endereços:

- Destination address
- Source address
- BSS Id

Para todos os SSID, o Destination address toma o valor ff:ff:ff:ff:ff:ff (Broadcast). Podemos ver ainda que os endereços MAC associados ao Source address e ao BSS Id são iguais (00:16:b6:f7:1d:51).

2.10 Pergunta 13

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

As tramas probing request e probing response apresentam subtipo 4 e 5, respectivamente. Então, para observarmos todas estas tramas simultaneamente, usamos o filtro *wlan.fc.type_subtype==0x4 or wlan.fc.type_subtype==0x5*.

2.11 Pergunta 14

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

50	2.297613	IntelCor_if:57:13	Broadcast	802.11	79	Probe Request, SN=576, FN=0, Flags=.....C, SSID=Home WIFI
27	1.212185	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	177	Probe Response, SN=2867, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St

<

>

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_if:57:13 (00:12:f0:1f:57:13)

Source address: IntelCor_if: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

0000 00 00 18 00 ee 58 00 00 10 02 85 09 a0 00 aa 9cX.....

0010 5e 00 00 0e ff c5 73 a3 40 00 00 00 ff ff ff ff A.....s.....

0020 ff ff 00 12 f0 1f 57 13 00 16 b6 f7 1d 51M.....\$

0030 00 09 4b 6f 6d 65 20 57 49 4e 49 01 08 02 04 00Home WIF.....

0040 16 0c 12 18 24 32 04 30 40 60 6c ff c5 73 a3\$2 0 H'L.....s

Figura 2.8: Probe request

51	2.308697	Cisco-Li_f7:1d:51	IntelCor_if:57:13	802.11	177	Probe Response, SN=2878, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
50	2.297613	IntelCor_if:57:13	Broadcast	802.11	79	Probe Request, SN=576, FN=0, Flags=.....C, SSID=Home WIFI
27	1.212185	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	177	Probe Response, SN=2867, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St

<

> Frame Control Field: 0x5000

.000 0001 0011 1010 = Duration: 314 microseconds

Receiver address: IntelCor_if:57:13 (00:12:f0:1f:57:13)

Destination address: IntelCor_if: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

0000 00 00 18 00 ee 58 00 00 10 02 85 09 a0 00 e2 9cX.....

0010 64 00 00 4b 6f 6d 65 20 57 49 4e 49 01 08 02 04 d..P.Q n P.....

0020 57 13 00 16 b6 f7 1d 51 00 16 b6 f7 1d 51Q.....

0030 d9 3f 5c 96 28 00 00 00 64 00 01 06 00 0c 33 30 ?\.....d.....30

0040 20 4d 75 6e 72 6f 65 20 53 74 01 04 02 04 0b 96 Munroe St.....

0050 03 01 06 07 06 55 53 49 01 0b 1a 0c 12 0f 00 03US.....

Figura 2.9: Probe response

O endereço MAC BSS Id de destino é ff:ff:ff:ff:ff:ff (Broadcast), tal como podemos ver na figura 2.8. O endereço MAC BSS Id de origem é 00:16:b6:f7:1d:51, tal como podemos ver na figura 2.9. A trama probe request é uma trama especial enviada por um cliente, requisitando informação de um AP específico identificado por um SSID ou de todos os APs na área identificados por um broadcast SSID. Semelhante a uma beacon frame, concluímos que a trama probe response contém a mesma informação requerida para dois clientes começarem a comunicar.

2.12 Pergunta 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?

118	6.308439	IntelCor_if:57:13	Broadcast	802.11	70	Probe Request, SN=621, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
119	6.308313	Cisco-Li_f7:1d:51	IntelCor_if:57:13	802.11	177	Probe Response, SN=2922, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St

Figura 2.10: Probing request para o qual houve um probing response

Na figura acima, é possível verificar que a trama 118 é um probing request e a 119 é o probing response correspondente. A frame 118 é uma Broadcast enviada pelo

IntelCor_1f:57:13 que é emitida para todos os equipamentos da rede, de modo a encontrar um AP. Já a trama 119 é a resposta do AP (Cisco.Li_f7:1d:51) para a respectiva STA (IntelCor_1f:57:13).

Capítulo 3

Processo de Associação

3.1 Pergunta 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? (Pista: uma é na camada IP e outra na camada de ligação 802.11). Observando a especificação 802.11, seria de esperar outra trama, mas que não aparece?

No.	Time	Source	Destination	Protocol	Length	Info
1729	49.440041	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3587, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1730	49.440146	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1684, FN=0, Flags=...P...TC
1731	49.440243		IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C
1732	49.542481	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3588, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1733	49.583615	192.168.1.109	192.168.1.1	DHCP	390	DHCP Release - Transaction ID 0xae5a526
1734	49.583771		IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C
1735	49.609617	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	Deauthentication, SN=1605, FN=0, Flags=.....C
1736	49.609770		IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C
1737	49.614478	IntelCor_d1:b6:4f	Broadcast	802.11	99	Probe Request, SN=1606, FN=0, Flags=.....C, SSID=linksys_SES_24086
1738	49.615869		Cisco-Li_f5:ba:bb	802.11	38	Acknowledgement, Flags=.....C
1739	49.617713		Cisco-Li_f5:ba:bb	802.11	38	Acknowledgement, Flags=.....C

.... 00.. = Type: Management frame (0)
1100 = Subtype: 12
> Flags: 0x00
> 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)
.... 0000 = Fragment number: 0
0110 0100 0101 = Sequence number: 1605
Frame check sequence: 0x3b4a8b9c [unverified]
[FCS Status: Unverified]
▼ IEEE 802.11 wireless LAN
▼ Fixed parameters (2 bytes)
Reason code: Unspecified reason (0x0001)

Figura 3.1: Trace imediatamente após $t=49$

Como podemos ver na figura acima, no instante de tempo $t = 49.583615$ é enviado um "DHCP release" pelo host para o servidor DHCP cujo endereço IP é 192.168.1.1 na rede que o host está a abandonar. No instante de tempo $t = 49.609617$, o host envia uma "Deauthentication" frame (Frame Type = 00 (Management), Frame Subtype = 12 (Deauthentication)). Observando a especificação 802.11, vemos que "Reason Code : unspecified reason" e, portanto, concluímos que uma trama poderá ter esperado que um Disassociation request fosse enviado, daí não aparecer.

3.2 Pergunta 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?

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	49.649705	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=.....R...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=.....R...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=.....R...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
2156	63.168087	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58	Authentication, SN=1647, FN=0, Flags=.....R...C
2160	63.169707	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58	Authentication, SN=1647, FN=0, Flags=.....R...C
2158	63.169071	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58	Authentication, SN=3726, FN=0, Flags=.....R...C
2164	63.170692	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58	Authentication, SN=3727, FN=0, Flags=.....R...C

Signal/noise ratio (dB): 75dB

> [Duration: 464µs]

> 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)

Figura 3.2: Mensagens de authentication

Observando a figura acima, vemos que foram enviadas 17 mensagens de authentication do host para o AP linksys_ses_24086.

3.3 Pergunta 18

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

Como podemos ver no campo "Authentication Algorithm" da figura 3.2, o tipo de autenticação pretendida pelo host é aberta.

3.4 Pergunta 19

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

Não se observa nenhuma resposta de authentication do AP linksys_ses_24086 no trace. É provável que isto se deva ao facto de o AP estar configurado para pedir uma chave quando se associa a esse AP, portanto o AP provavelmente está a ignorar pedidos cuja autenticação é aberta.

3.5 Pergunta 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?

No.	Time	Source	Destination	Protocol	Length	Info
2123	62.172946	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0, Flags=....R...C
2124	62.174079	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0, Flags=....R...C
2156	63.168087	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58	Authentication, SN=1647, FN=0, Flags=.....C
2160	63.169707	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58	Authentication, SN=1647, FN=0, Flags=.....R...C
2158	63.169071	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58	Authentication, SN=3726, FN=0, Flags=.....C
2164	63.170692	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58	Authentication, SN=3727, FN=0, Flags=.....C
1	0.000000	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2854, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St

```

Signal/noise ratio (dB): 72dB
> [Duration: 28µs]
▼ 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 [unverified]
    [FCS Status: Unverified]

```

Figura 3.3: Tramas authentication enviadas pelo host para e do AP e vice-versa

Como podemos observar na figura acima, no instante de tempo $t = 63.168087$ existe uma authentication frame enviada a partir de 00:13:02:d1:b6:4f (Transmitter address) para 00:16:b6:f7:1d:51 (BSS Id). No instante de tempo $t = 63.169071$ existe uma authentication frame enviada na direção inversa (do BSS Id para o Transmitter address).

3.6 Pergunta 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?

2162	63.169910	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	89	Association Request, SN=1648, FN=0, Flags=.....C, SSID=30 Munroe St
2163	63.170008		IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C
2164	63.170692	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58	Authentication, SN=3727, FN=0, Flags=.....C
2165	63.171000		Cisco-Li_f7:1d:51	802.11	38	Acknowledgement, Flags=.....C
2166	63.192101	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	94	Association Response, SN=3728, FN=0, Flags=.....C

```

▼ 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)

```

Figura 3.4: Associate request e associate response

Como podemos ver na figura acima, no instante de tempo $t = 63.169910$ existe uma "Association Request" frame enviada a partir de 00:13:02:d1:b6:4f (Transmitter address) para 00:16:b6:f7:1d:51 (BSS Id). No instante de tempo $t =$

63.192101 existe uma "Association Response" frame enviada na direção inversa (do BSS Id para o Transmitter address).

3.7 Pergunta 22

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

2162	63.169910	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	89 Association Request, SN=1648, FN=0, Flags=.....C, SSID=30 Munroe St
2163	63.170008		IntelCor_d1:b6:4f	802.11	38 Acknowledgement, Flags=.....C
2164	63.170692	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58 Authentication, SN=3727, FN=0, Flags=.....C
2165	63.171000		Cisco-Li_f7:1d:51	802.11	38 Acknowledgement, Flags=.....C
2166	63.192101	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	94 Association Response, SN=3728, FN=0, Flags=.....C
2167	63.192956		Cisco-Li_f7:1d:51	802.11	38 Acknowledgement, Flags=.....C


```

> 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: 0xfe3badc6 [unverified]
[FCS Status: Unverified]
v IEEE 802.11 wireless LAN
  v Fixed parameters (4 bytes)
  > Capabilities Information: 0xce01
    Listen Interval: 0x000a
  v 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]

```

Figura 3.5: Taxas de transmissão que o host está disposto a usar

No.	Time	Source	Destination	Protocol	Length	Info
2163	63.170008		IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C
2164	63.170692	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58	Authentication, SN=3727, FN=0, Flags=.....C
2165	63.171000		Cisco-Li_f7:1d:51	802.11	38	Acknowledgement, Flags=.....C
2166	63.192101	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	94	Association Response, SN=3728, FN=0, Flags=.....C
2167	63.192956		Cisco-Li_f7:1d:51	802.11	38	Acknowledgement, Flags=.....C
2168	63.194842	0.0.0.0	255.255.255.255	DHCP	390	DHCP Discover - Transaction ID 0x101b218a
2169	63.194971		IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C


```

> 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]
v IEEE 802.11 wireless LAN
  v Fixed parameters (6 bytes)
  > Capabilities Information: 0x0601
    Status code: Successful (0x0000)
    ..00 0000 0000 0101 = Association ID: 0x0005
  v 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]

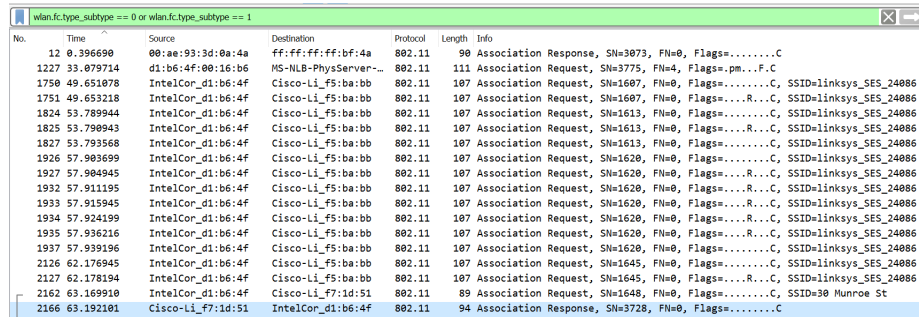
```

Figura 3.6: Taxas de transmissão que o AP está disposto a usar

Como podemos ver no campo "Supported Rates" e no campo "Extended Supported Rates" da figura 3.5, as taxas de transmissão que o host está disposto a usar são 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, 54 Mbps. As taxas de transmissão que o AP está disposto a usar são as mesmas, como podemos ver na figura 3.6.

3.8 Pergunta 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.



No.	Time	Source	Destination	Protocol	Length	Info
12	0.396690	00:ae:93:3d:0a:4a	ff:ff:ff:ff:bf:4a	802.11	90	Association Response, SN=3073, FN=0, Flags=.....C
1227	33.079714	d1:b6:4f:00:16:b6	MS-NLB-PhysServer-	802.11	111	Association Request, SN=3775, FN=4, Flags=.pm...F.C
1750	49.651878	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1607, FN=0, Flags=.....C, SSID=linksys_SES_24086
1751	49.653218	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1607, FN=0, Flags=.....C, SSID=linksys_SES_24086
1824	53.789944	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1613, FN=0, Flags=.....C, SSID=linksys_SES_24086
1825	53.790943	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1613, FN=0, Flags=.....C, SSID=linksys_SES_24086
1827	53.793568	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1613, FN=0, Flags=.....C, SSID=linksys_SES_24086
1926	57.903699	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=.....C, SSID=linksys_SES_24086
1927	57.904945	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=.....C, SSID=linksys_SES_24086
1932	57.911195	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=.....C, SSID=linksys_SES_24086
1933	57.915945	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=.....C, SSID=linksys_SES_24086
1934	57.924199	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=.....C, SSID=linksys_SES_24086
1935	57.936216	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=.....C, SSID=linksys_SES_24086
1937	57.939196	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=.....C, SSID=linksys_SES_24086
2126	63.176945	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1645, FN=0, Flags=.....C, SSID=linksys_SES_24086
2127	63.178194	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1645, FN=0, Flags=.....C, SSID=linksys_SES_24086
2162	63.169910	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	89	Association Request, SN=1648, FN=0, Flags=.....C, SSID=30 Munroe St
2166	63.192101	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	94	Association Response, SN=3728, FN=0, Flags=.....C

Figura 3.7: Filtro aplicado

Começamos por aplicar o filtro `wlan.fc.type_subtype == 0 or wlan.fc.type_subtype == 1` de modo a identificar apenas as tramas association request e association response. De seguida, selecionamos as tramas 2162 e 2166 da figura acima.



No.	Time	Source	Destination	Protocol	Length	Info
2150	63.116231	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	54	Deauthentication, SN=1646, FN=0, Flags=....R...C
2151	63.135362	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	54	Deauthentication, SN=1646, FN=0, Flags=....R...C
2152	63.140106	IntelCor_d1:b6:4f	Broadcast	802.11	94	Probe Request, SN=1647, FN=0, Flags=.....C, SSID=30 Munroe St
2153	63.142451	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	177	Probe Response, SN=3724, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
2154	63.142860	Cisco-Li_f7:1d:51	Broadcast	802.11	38	Acknowledgement, Flags=.....C
2155	63.161272	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3725, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
2156	63.168087	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58	Authentication, SN=1647, FN=0, Flags=.....C
2157	63.168222	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C
2158	63.169071	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58	Authentication, SN=3726, FN=0, Flags=.....C
2159	63.169592	Cisco-Li_f7:1d:51	Cisco-Li_f7:1d:51	802.11	38	Acknowledgement, Flags=.....C
2160	63.169707	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58	Authentication, SN=1647, FN=0, Flags=....R...C
2161	63.169814	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	38	Acknowledgement, Flags=.....C
2162	63.169910	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	89	Association Request, SN=1648, FN=0, Flags=.....C, SSID=30 Munroe St
2163	63.170008	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	38	Acknowledgement, Flags=.....C
2164	63.170692	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58	Authentication, SN=3727, FN=0, Flags=.....C
2165	63.171000	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C
2166	63.192101	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	94	Association Response, SN=3728, FN=0, Flags=.....C
2167	63.192956	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	38	Acknowledgement, Flags=.....C

Figura 3.8: Captura sem filtros

De seguida, analisamos a captura sem filtro ordenada por tempo. Na figura acima, identificamos duas tramas de autenticação (tramas 2158 e 2160) e duas de confirmação (tramas 2159 e 2161). É importante mencionar que a fase de autenticação começa com a trama de autenticação 2158 e termina com a trama de confirmação 2161. Depois, inicia-se a fase de associação com uma authentication request frame (trama 2162) que termina com a trama de confirmação (trama 2167), o que nos permite concluir que a trama enviada não continha erros.

3.9 Pergunta 24

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

Na figura abaixo, podemos observar o diagrama que ilustra a sequência de todas as tramas trocadas no processo de associação, incluindo a fase de autenticação.

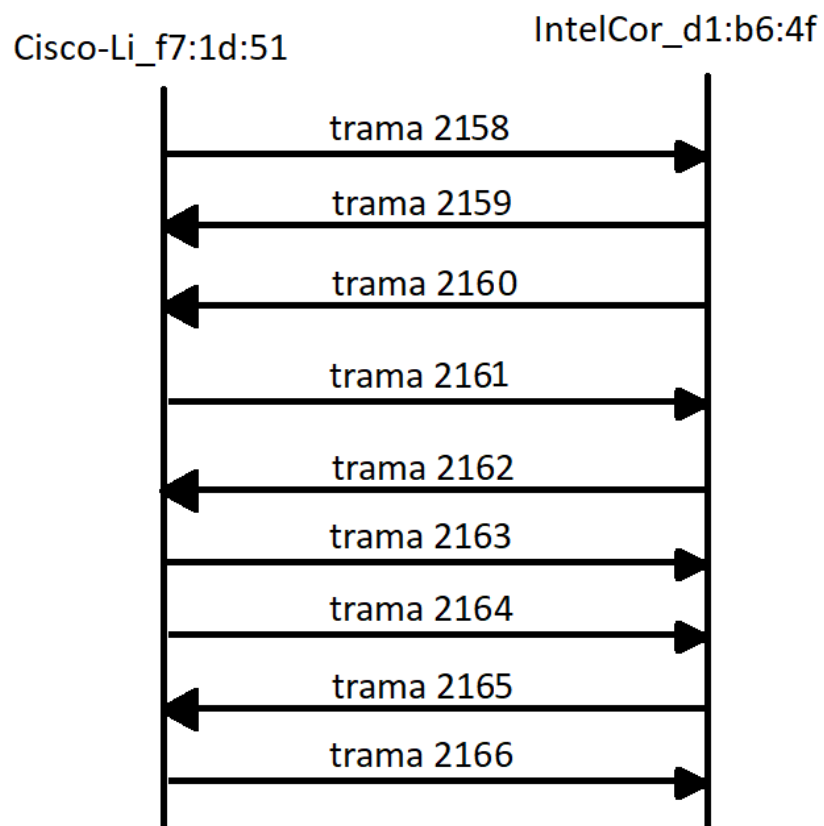


Figura 3.9: Diagrama que ilustra a sequência de todas as tramas trocadas

Capítulo 4

Transferência de Dados

4.1 Pergunta 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?

No.	Time	Source	Destination	Protocol	Length	Info
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:b6:4f (00:13:02:d1:b6:4f) (RA)	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_f7:1d:51 (00:16:b6:f7:1d:51) (RA)	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:b6:4f (00:13:02:d1:b6:4f) (RA)	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

.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)

Figura 4.1: Segmentos para a primeira sessão tcp

Como podemos ver na figura acima, na **trama 474** observamos o primeiro segmento **SYN TCP** para a primeira sessão **TCP** (download alice.txt). Os campos dos endereços presentes nesta trama 802.11 são:

- **Destination address** - 00:16:b6:f4:eb:a8
- **Source address** - 00:13:02:d1:b6:4f
- **BSS Id** - 00:16:b6:f7:1d:51

4.2 Pergunta 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?

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
Internet Protocol Version 4, Src: 192.168.1.109, Dst: 128.119.245.12 0100 = Version: 4 0101 = Header Length: 20 bytes (5) > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 48 Identification: 0x1324 (4900) > Flags: 0x4000, Don't fragment Time to live: 128 Protocol: TCP (6) Header checksum: 0xb00a [validation disabled] [Header checksum status: Unverified] Source: 192.168.1.109 Destination: 128.119.245.12						

Figura 4.2: Endereços IP para o primeiro segmento da primeira sessão TCP

Tal como podemos ver nas figuras 4.1 e 4.2, concluímos que:

- Endereço MAC que corresponde ao host - 00:13:02:d1:b6:4f
- Endereço do AP - 00:16:b6:f7:1d:51
- Endereço do router do primeiro salto - 00:16:b6:f4:eb:a8
- Endereço IP do host - 192.168.1.109
- Endereço IP de destino - 128.119.245.12

4.3 Pergunta 27

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

Este endereço de destino corresponde ao router do primeiro salto, uma vez que a origem da trama 476 é igual ao destino da trama 474, como podemos ver na figura 4.1.

4.4 Pergunta 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?

No.	Time	Source	Destination	Protocol	Length	Info
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:b6:4f ...	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
Type/Subtype: QoS Data (0x0028)						
> Frame Control Field: 0x8832						
Duration/ID: 11560 (reserved)						
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)						
0000	00 00 18 00 ee 58 00 00	10 6c 85 09 c0 00 da 9cX..1.....			
0010	52 00 00 3e 7d 40 dc ec	88 32 28 ad 91 2a b0 4f	R...>]@...-2<[11.1			
0020	b6 4f 00 16 b6 f7 1d 51	00 16 b6 f4 eb a8 40 c3	[.....Q.....@..			
0030	00 01 aa aa 03 00 00 00	08 00 45 00 00 30 00 00E...0...			
0040	40 00 31 06 12 2f 80 77	f5 0c c0 a8 01 6d 00 50	@1-/-w.....m:P			
0050	09 ea ae 8f de 3f 71 af	cd 47 70 12 16 d0 5e a5?q...Gp...^			
0060	00 00 ed 04 05 b4 01 01	04 02 7d 40 dc ec}@...			

Figura 4.3: Trama 802.11 que contém o segmento SYNACK

Como podemos observar na figura acima, a trama 802.11 que contém o segmento SYNACK para esta sessão TCP é a trama 476. Os três campos dos endereços MAC na trama 802.11 são:

- STA address (91:2a:b0:49:b6:4f)
- BSS Id (00:16:b6:f7:1d:51)
- Source address (00:16:b6:f4:eb:a8)

4.5 Pergunta 29

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

A partir da figura 4.3, podemos concluir que:

- Endereço MAC - 00:16:b6:f4:eb:a8
- Endereço do AP - 00:16:b6:f7:1d:51
- Endereço do router do primeiro salto - 91:2a:b0:49:b6:4f

4.6 Pergunta 30

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

O endereço MAC de origem na trama não corresponde ao endereço IP do dispositivo que enviou o segmento TCP encapsulado neste diagrama, uma vez que, enquanto o endereço MAC de origem da trama é referente ao AP que enviou essa trama, o IP é referente ao dispositivo que enviou o segmento TCP.

Capítulo 5

Conclusões

Neste trabalho prático começamos por identificar e analisar tramas referentes à norma IEEE 802.11.

Analizamos, posteriormente, tramas beacon e os seus respetivos SSID's, vários campos presentes nestas tramas, métodos de deteção de erros e endereços MAC presentes.

Observamos como é feita a associação entre um cliente e um AP e todas as ações realizadas entre o pedido (*Association Request*) e a resposta (*Association Response*).

Por fim, vimos tramas com segmentos SYN TCP e os endereços MAC e IP que nelas circulam.

Por fim, aprofundamos conhecimentos em Wireshark, nomeadamente na aplicação de filtros.

Posto isto, com este trabalho conseguimos pôr em prática aquilo que foi lecionado tanto nas aulas teóricas como nas aulas práticas. Para além disso, tivemos a oportunidade para consolidar melhor os nossos conhecimentos e acreditamos que os objetivos propostos foram alcançados.