

UNIVERSIDADE DO MINHO
DEPARTAMENTO DE INFORMÁTICA

Redes de Computadores
TP4: Redes Sem Fios (802.11)
Grupo N° 8 PL6

Gonçalo Almeida (A84610)

Emanuel Rodrigues (A84776)

Lázaro Pinheiro (A86788)

18 de Dezembro de 2019

Conteúdo

1	Questões e Respostas	3
1.1	Acesso Rádio	3
1.2	Scanning	4
1.3	Processo de Associação	15
1.4	Transferência de Dados	21
2	Conclusão	24

Capítulo 1

Questões e Respostas

1.1 Acesso Rádio

The screenshot shows a Wireshark capture of a single IEEE 802.11 Probe Response frame. The frame details are as follows:

- ▶ Frame 1608: 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 (dB): 71dB
 - Signal strength (dBm): -29dBm
 - Noise level (dBm): -100dBm
 - Signal/noise ratio (dB): 71dB
 - [Duration: 1416µs]
- IEEE 802.11 Probe Response, Flags:R...C
- IEEE 802.11 wireless LAN

Figura 1.1: Datagrama 1

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

A frequência do espectro é 2437 MHz e corresponde ao canal 6.

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

A versão da norma IEEE 802.11 em uso é a 802.11b.

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.

O débito a que a trama foi enviada é de 1 Mb/s e não corresponde ao débito máximo a que a interface Wi-Fi pode operar, pois para a versão da norma utilizada este é de 11 Mb/s.

1.2 Scanning

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

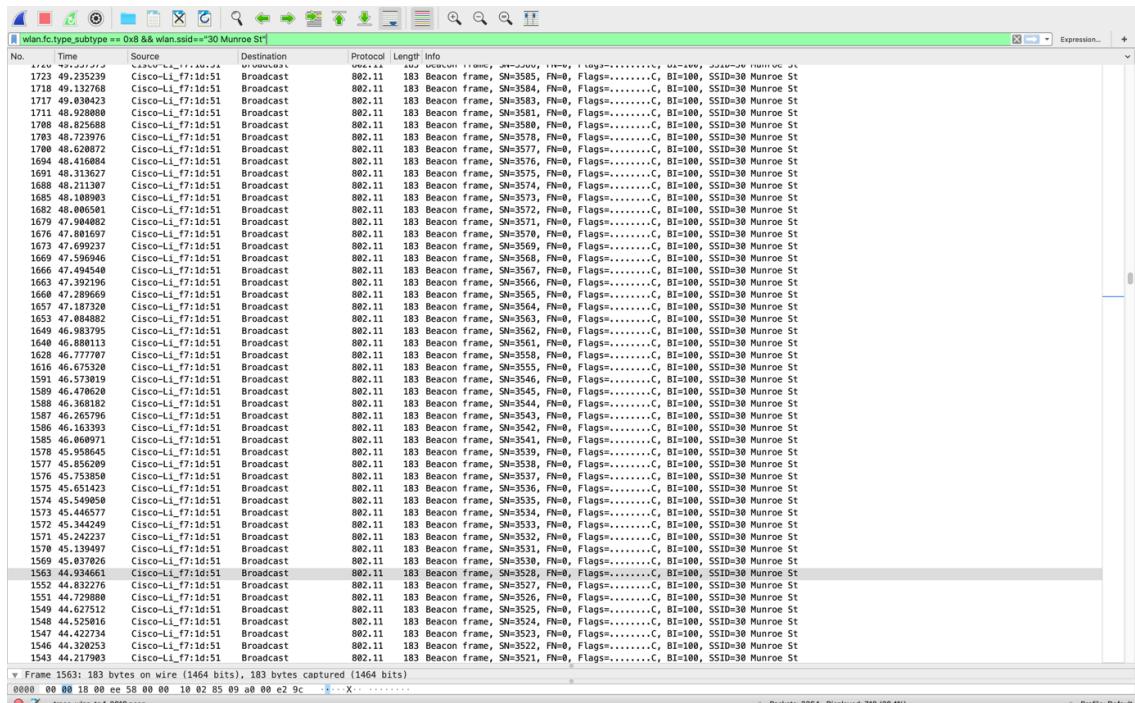


Figura 1.2: Filtragem de tramas de beacon emitidas por 30 Munroe St

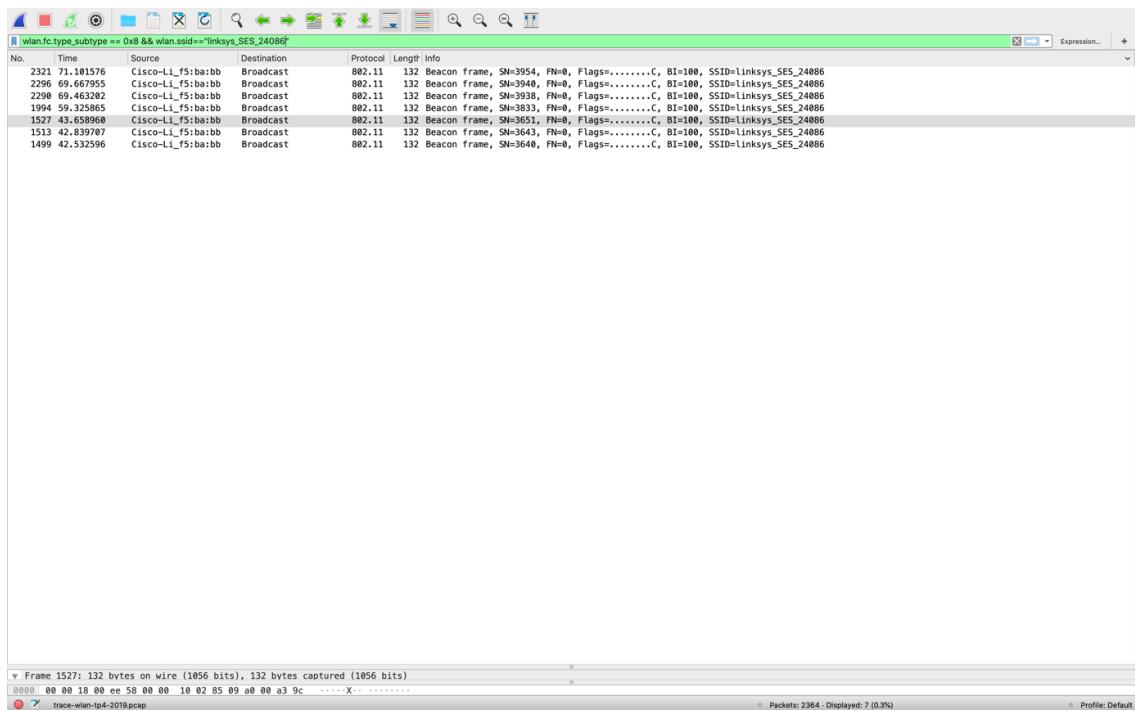


Figura 1.3: Filtragem de tramas de beacon emitidas por linksys'SES'24086

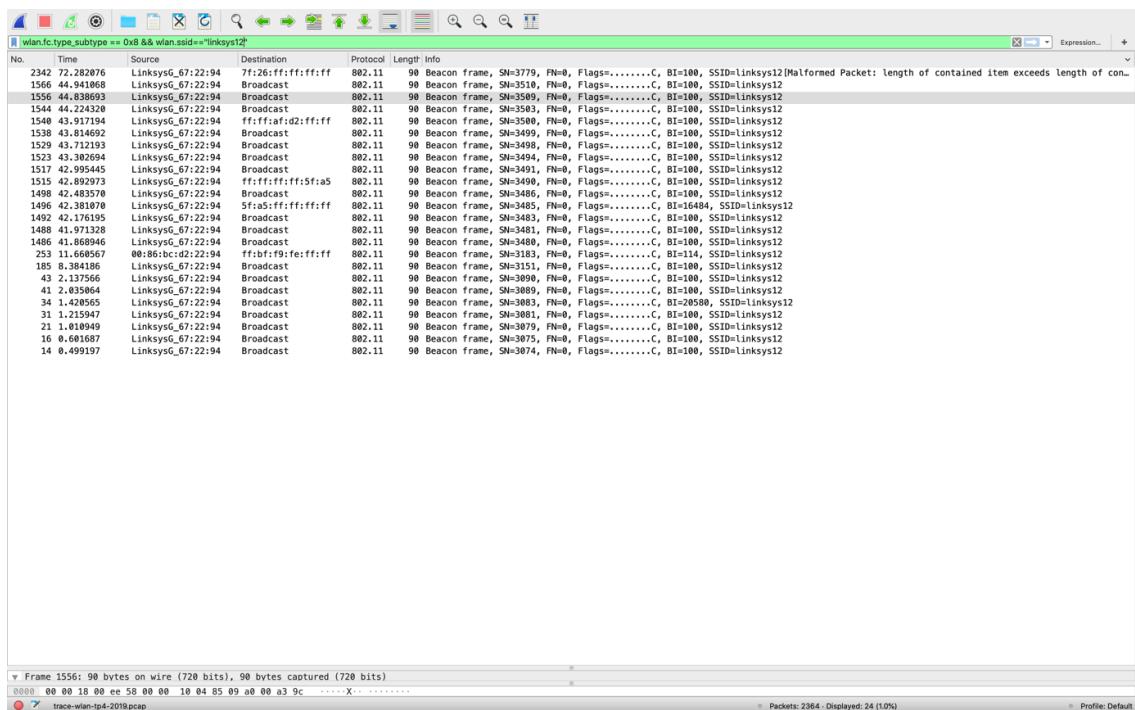


Figura 1.4: Filtragem de tramas de beacon emitidas por linksys12

Os SSIDs dos APs que estão a emitir a maioria das tramas de beacon são 30 Munroe St e

linksys12.

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.

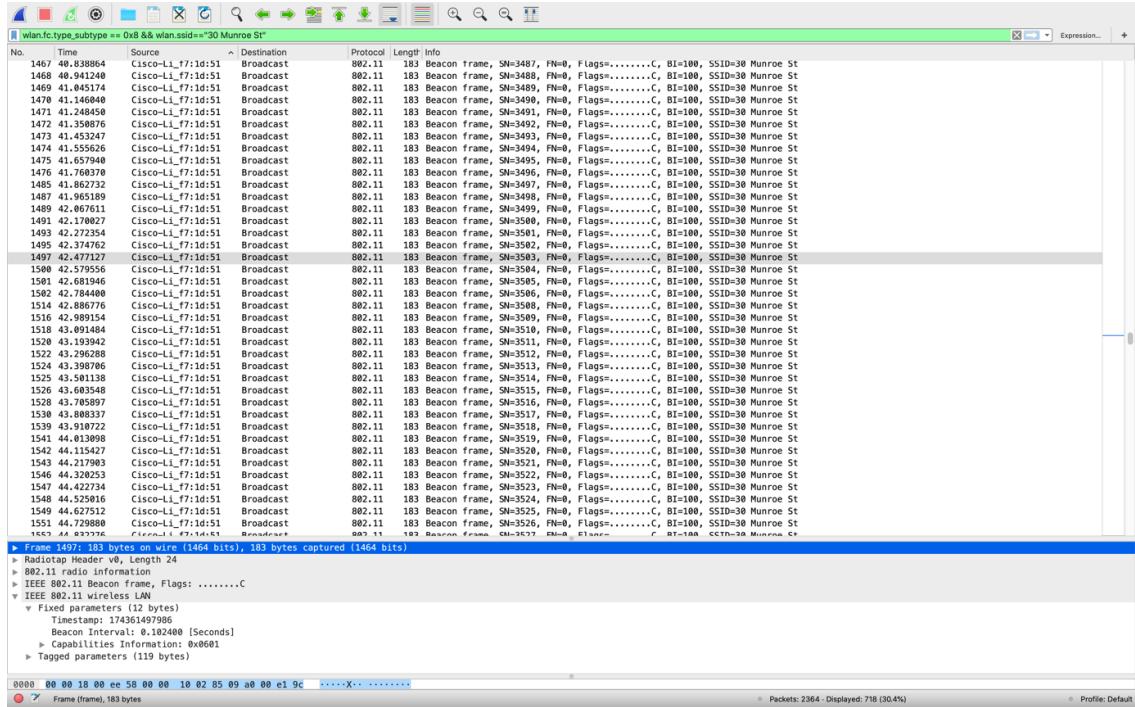


Figura 1.5: Filtragem de tramas de beacon emitidas por 30 Munroe St com datagrama

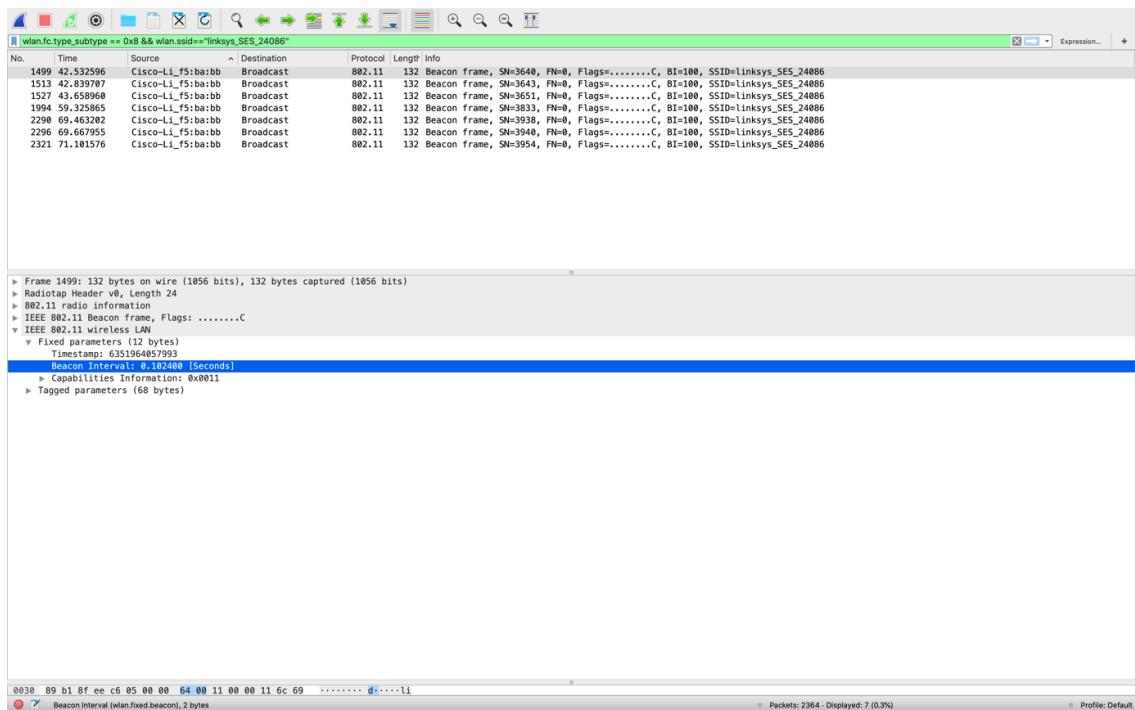


Figura 1.6: Filtragem de tramas de beacon emitidas por linksys`SES`24086 com datagrama

O intervalo de tempo entre a transmissão de tramas beacon para o AP linksys'ses'24086 é 0.102400 segundos e para o AP 30 Munroe St é, também, 0.102400 segundos. Na prática, a periodicidade de tramas beacon é verificada, visto que os tempos de transmissão são sempre os mesmos.

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.

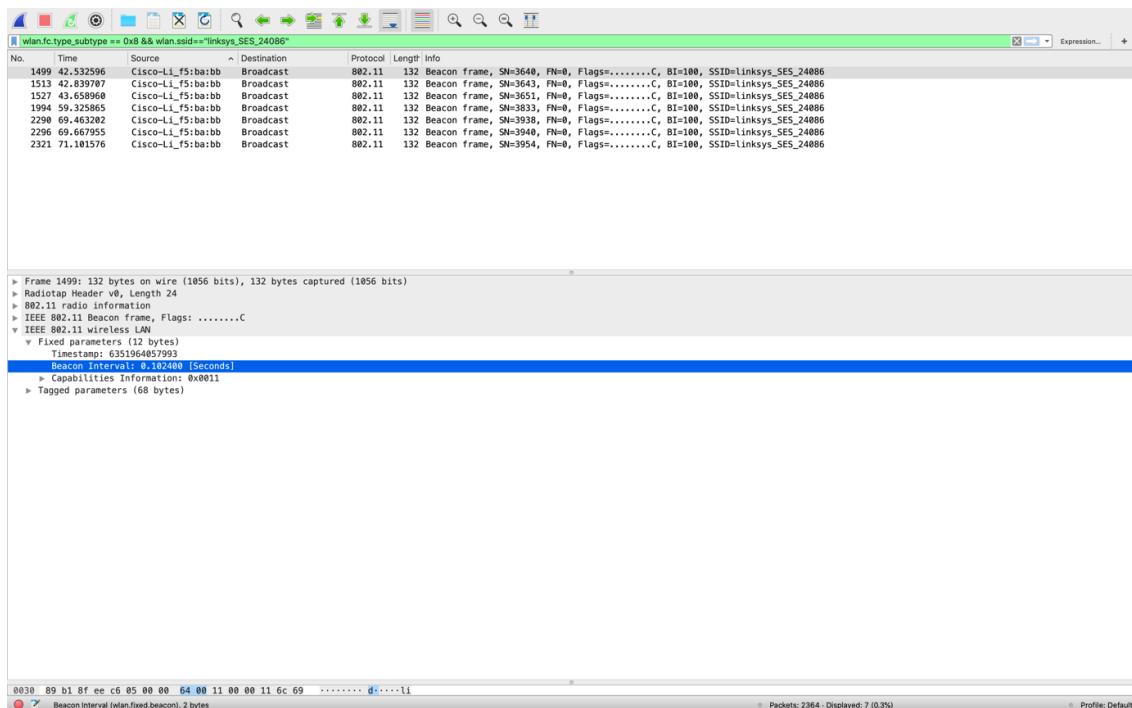


Figura 1.7: Datagrama 2

O endereço MAC de origem da trama beacon de 30 Munroe St é 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 de destino na trama 30 Munroe St é ff:ff:ff:ff:ff:ff (broadcast).

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.

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?

▼ 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: Airon Networks Inc.

Figura 1.8: Datagrama com data rates e extended supported rates

Data rates:
 1(B) (0x82)
 2(B) (0x84)

Extended supported rates:
 5.5(B) (0x8b)
 11(B) (0x96)
 6(B) (0x8c)
 9 (0x12)
 12(B) (0x98)
 18 (0x24)
 24(B) (0xb0)
 36 (0x48)
 48 (0x60)
 54 (0x6c)

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 subtípico. Em que parte concreta do cabeçalho da trama estão especificados (ver anexo)?

```

▼ 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
  ▼ 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 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
  1110 0001 1111 .... = Sequence number: 3615
  Frame check sequence: 0x33ffb367 [unverified]
  FCS Status: Unverified

```

Figura 1.9

Esta trama pertence ao tipo de Management Frame, onde o identificador de tipo tem valor 0 e o de subtipo 8. Com base no anexo, percebeu-se que estão especificados na parte de sequence control do cabeçalho da trama.

Fenômenos como o ruído e as interferências também ocorrem, podendo deturpar a mensagem original. Devido a este problema são aplicados códigos de detecção e correção de erros às transmissões.

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

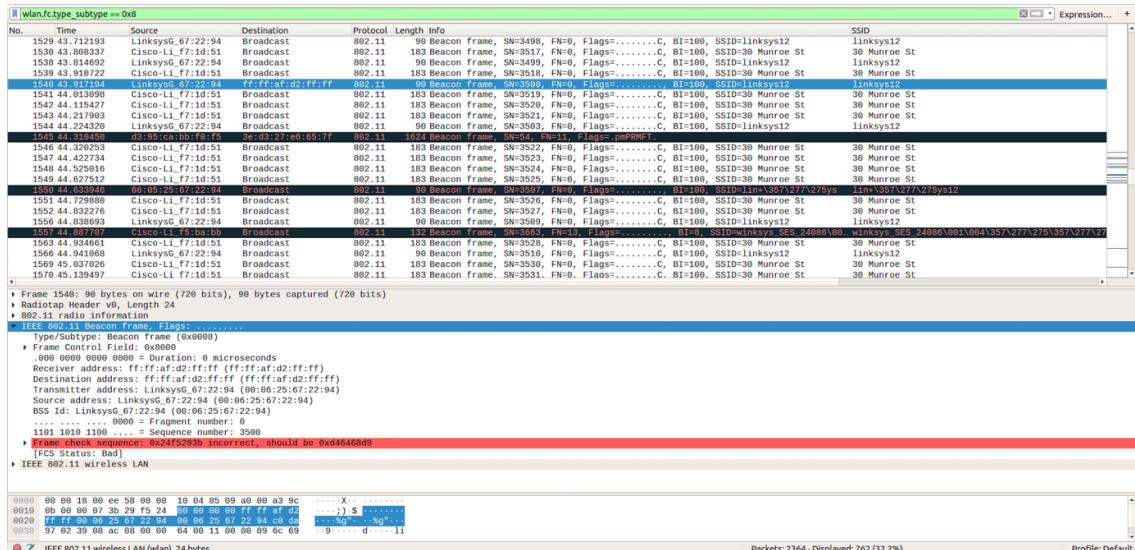


Figura 1.10

O método de correção de erros CRC está a ser usado, pois o Frame check sequence em algumas

tramas possuí o valor incorrect, logo nem todas as tramas são recebidas corretamente.

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

```
▶ Frame 940: 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: 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 = Fragment number: 0
        1100 1100 1001 .... = Sequence number: 3273
        Frame check sequence: 0xcf49211c [unverified]
        [FCS Status: Unverified]
    ▶ IEEE 802.11 wireless LAN
```

Figura 1.11

Na trama analisada, são utilizados 3 endereços MAC diferentes, cujos valores são:

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

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)

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

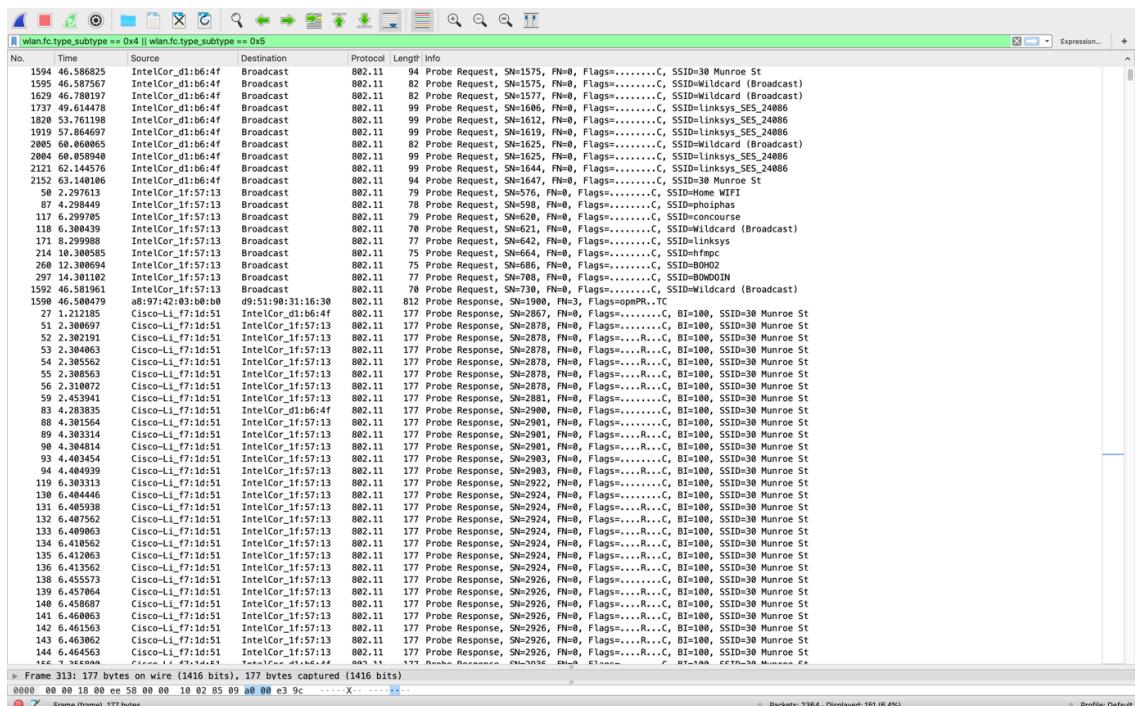


Figura 1.12: filtro no Wireshark

O filtro utilizado no Wireshark que permite visualizar todas as tramas probing request e probing response foi:
`wlan.fc.type_subtype == 0x4 —— wlan.fc.type_subtype == 0x5`

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

```

▶ Frame 214: 75 bytes on wire (600 bits), 75 bytes captured (600 bits)
▶ Radiotap Header v0, Length 24
▶ 802.11 radio information
▼ IEEE 802.11 Probe Request, Flags: ....C
    Type/Subtype: Probe Request (0x0004)
    ▶ Frame Control Field: 0x4000
        .000 0000 0000 0000 = Duration: 0 microseconds
        Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
        Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
        Transmitter address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
        Source address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
        BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
        .... .... 0000 = Fragment number: 0
        0010 1001 1000 .... = Sequence number: 664
        Frame check sequence: 0x52d7bee8 [unverified]
        [FCS Status: Unverified]
    ▶ IEEE 802.11 wireless LAN

```

Figura 1.13

```

▶ Frame 1622: 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: ....R...C
    Type/Subtype: Probe Response (0x0005)
    ▶ Frame Control Field: 0x5008
        .000 0001 0011 1010 = Duration: 314 microseconds
        Receiver address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
        Destination address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
        Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
        Source address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
        BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
        .... .... 0000 = Fragment number: 0
        1101 1110 0101 .... = Sequence number: 3557
        Frame check sequence: 0xe75bf12b [unverified]
        [FCS Status: Unverified]
    ▶ IEEE 802.11 wireless LAN

```

Figura 1.14

OOS endereços MAC BSS ID de destino e origem nestas trama variam para os Probe Request e os Probe Response. Num Probe Request o endereço MAC BSS ID tem valor (ff:ff:ff:ff:ff:ff), sendo o mesmo para todas as tramas. Num Probe Response o endereço MAC BSS ID tem valor (00:16:b6:f7:1d:51).

Este tipo de tramas são usadas para descrever secções de uma rede local sem fio.

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?

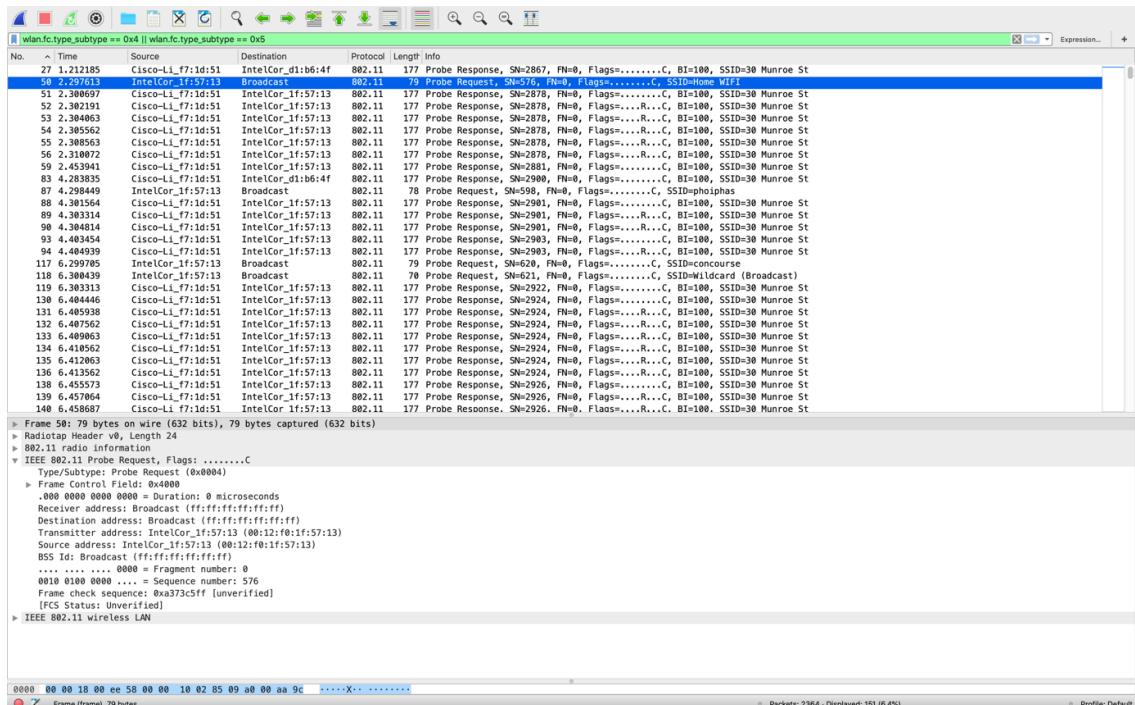


Figura 1.15

1.3 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? (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?

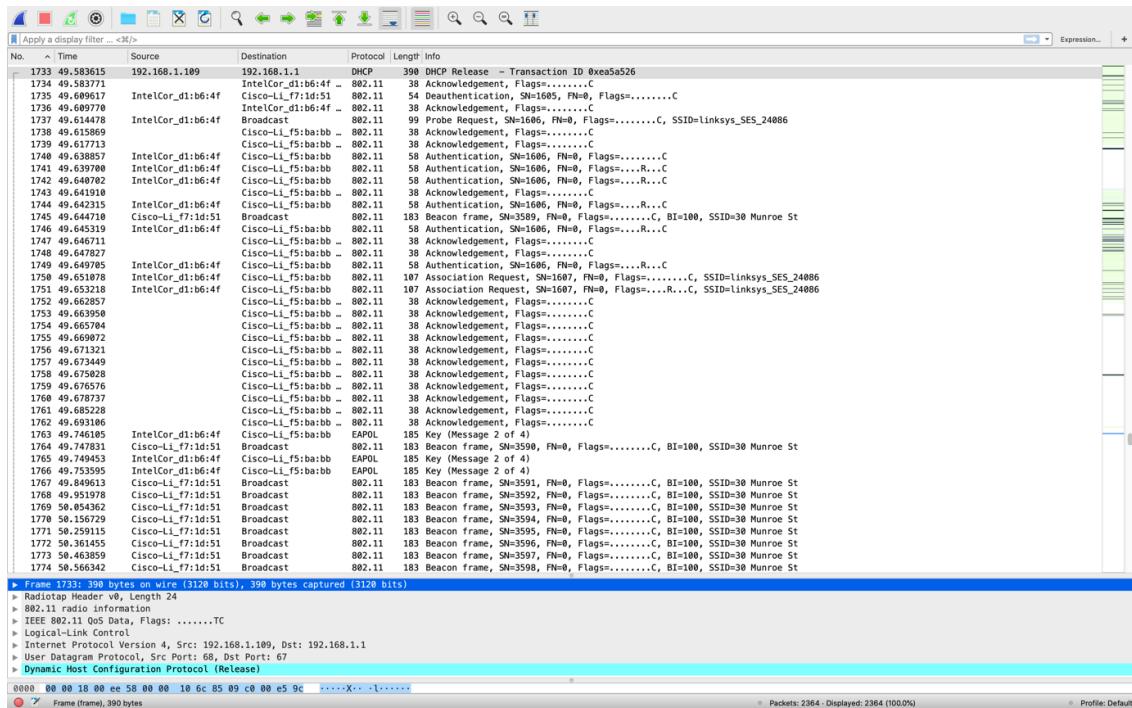


Figura 1.16

As ações realizadas pelo host foram as tramas com o número 1733 e 1734. Seria de esperar uma trama disassociation.

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'L1'f5:ba:bb) aproximadamente ao t=49?

wlan.fc.type_subtype == 0x0B && wlan.da == 00:18:39:f5:ba:bb						
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=.....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

▶ Frame 1749: 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:R...C
▼ IEEE 802.11 wireless LAN
▼ Fixed parameters (6 bytes)
Authentication Algorithm: Open System (0)
Authentication SEQ: 0x0001
Status code: Successful (0x0000)

Figura 1.17

Aplicou-se um filtro para facilitar a tarefa pedida. Posteriormente, percebeu-se que foram enviadas 6 mensagens do host para o AP linksys'sses'24086 aproximadamente ao t = 49.

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

▶ Frame 1749: 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:R...C
▼ IEEE 802.11 wireless LAN
▼ Fixed parameters (6 bytes)
Authentication Algorithm: Open System (0)
Authentication SEQ: 0x0001
Status code: Successful (0x0000)

Figura 1.18

O host não tenta usar nenhum algoritmo de autenticação, como podemos ver no campo “Authentication Algorithm” da trama, que marca o sistema como sendo “Open System”.

19. Observa-se a resposta de authentication do AP linksys'sses'24086 AP no trace?

wlan.fc.type_subtype == 0x0B						
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=.....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
2156	63.168087	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58	Authentication, SN=1647, FN=0, Flags=.....C
2158	63.169071	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58	Authentication, SN=3726, 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
2164	63.170692	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58	Authentication, SN=3727, FN=0, Flags=.....C

▶ Frame 2158: 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:
▼ IEEE 802.11 wireless LAN
▼ Fixed parameters (6 bytes)
Authentication Algorithm: Open System (0)
Authentication SEQ: 0x0002
Status code: Successful (0x0000)

Figura 1.19

Sim, porque a trama 2158 tem como origem o Cisco-Li:f7:1d:51 e como destino o IntelCor:d1:b6:4f.

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

Figura 1.20

Filtrando todas as tramas obtemos todas as tramas authentication presentes na figura acima e percebeu-se que aparece uma trama do host para o AP 30 Munroe St no temp

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?

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 33.679714	d1:b6:4f:00:16:b6	MS-NLB-PhysServer->	802.11	111 Association Request, SN=3775, FN=4, Flags=.pm...F.C
1750 49.651078	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=....R...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 53.798943	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107 Association Request, SN=1613, FN=0, Flags=....R...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=....R...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=....R...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=....R...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=....R...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=....R...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 62.176945	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 62.178194	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107 Association Request, SN=1645, FN=0, Flags=....R...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
2307 70.179949	Cisco-Li_f5:ba:7b	f9:ff:ff:ff:ff:ff	802.11	132 Fragmented IEEE 802.11 frame

Figura 1.21

O association request do host para o AP 30 Munroe St ocorre no tempo 63.169910 e a association response correspondente ocorre no tempo 63.192101.

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

- ▶ 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
- ▼ IEEE 802.11 wireless LAN
 - ▶ Fixed parameters (6 bytes)
 - ▼ Tagged parameters (36 bytes)
 - ▶ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
 - ▶ Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
 - ▶ Tag: EDCA Parameter Set

Figura 1.22: Taxas de transmissão do host

```

▶ Frame 2162: 89 bytes on wire (712 bits), 89 bytes captured (712 bits)
▶ Radiotap Header v0, Length 24
▶ 802.11 radio information
▶ IEEE 802.11 Association Request, Flags: .......C
▼ IEEE 802.11 wireless LAN
  ▶ Fixed parameters (4 bytes)
  ▼ Tagged parameters (33 bytes)
    ▶ Tag: SSID parameter set: 30 Munroe St
    ▶ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18, [Mbit/sec]
    ▶ Tag: QoS Capability
    ▶ Tag: Extended Supported Rates 24(B), 36, 48, 54, [Mbit/sec]

```

Figura 1.23: Taxas de transmissão do AP

O host está disposto a usar as seguintes taxas de transmissão:
 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
 Quanto ao AP, as taxas de transmissão são as seguintes:
 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.

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	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	802.11	38 Acknowledgement, Flags=.....C
2160	63.169707	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f	802.11	58 Authentication, SN=1647, FN=0, Flags=....R...C
2161	63.169814		IntelCor_d1:b6:4f	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	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

Figura 1.24

Aplicamos um filtro para determinar todas as tramas Association Request e Association Response. De seguida selecionou-se as tramas com números 2162 e 2166. Remove-se o filtro e procurou-se as tramas identificadas. A sequência de tramas correspondente a um processo de associação completo entre STA e o AP está identificada na figura seguinte.

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

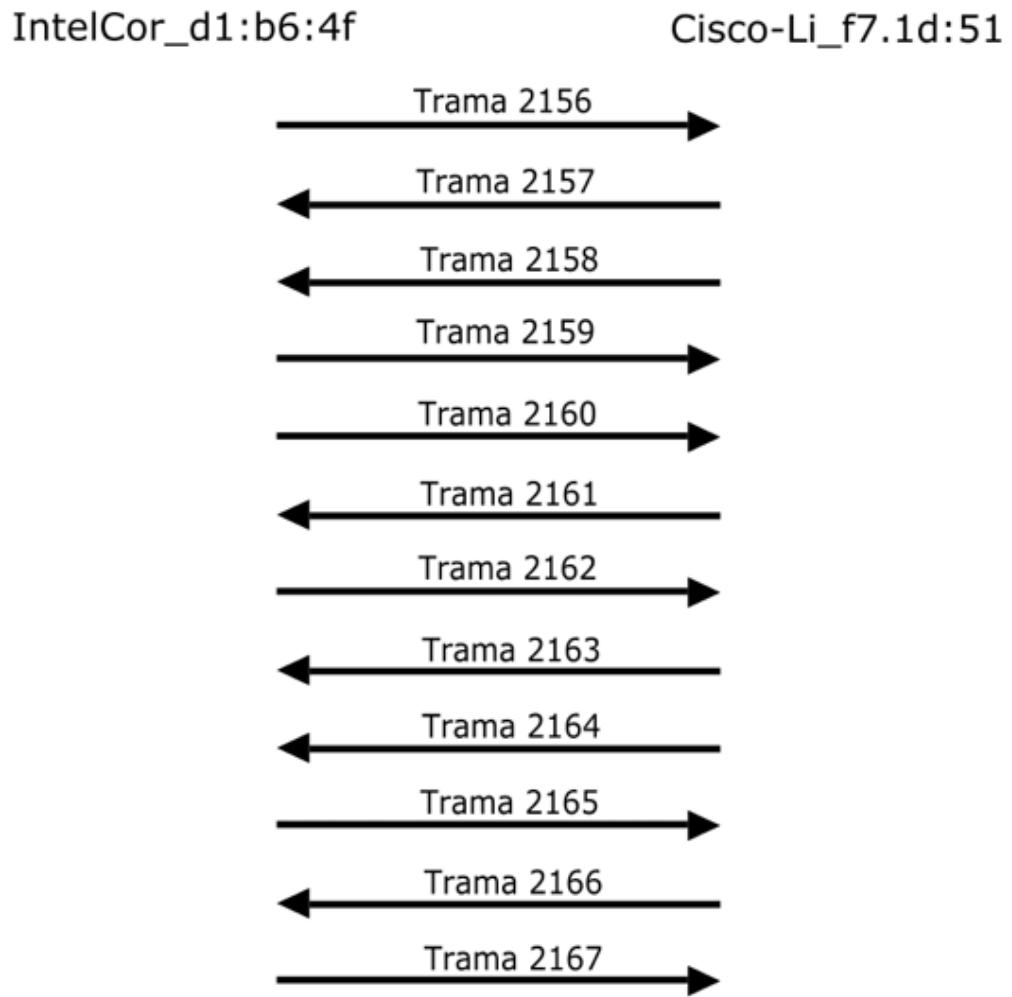


Figura 1.25: Diagrama do processo de associação

1.4 Transferência de Dados

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?

```
▶ 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
        .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 [unverified]
        [FCS Status: Unverified]
    ▶ Qos Control: 0x0000
    ▶ 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
```

Figura 1.26

Os três campos dos endereços MAC na trama 802.11 são:

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)

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?

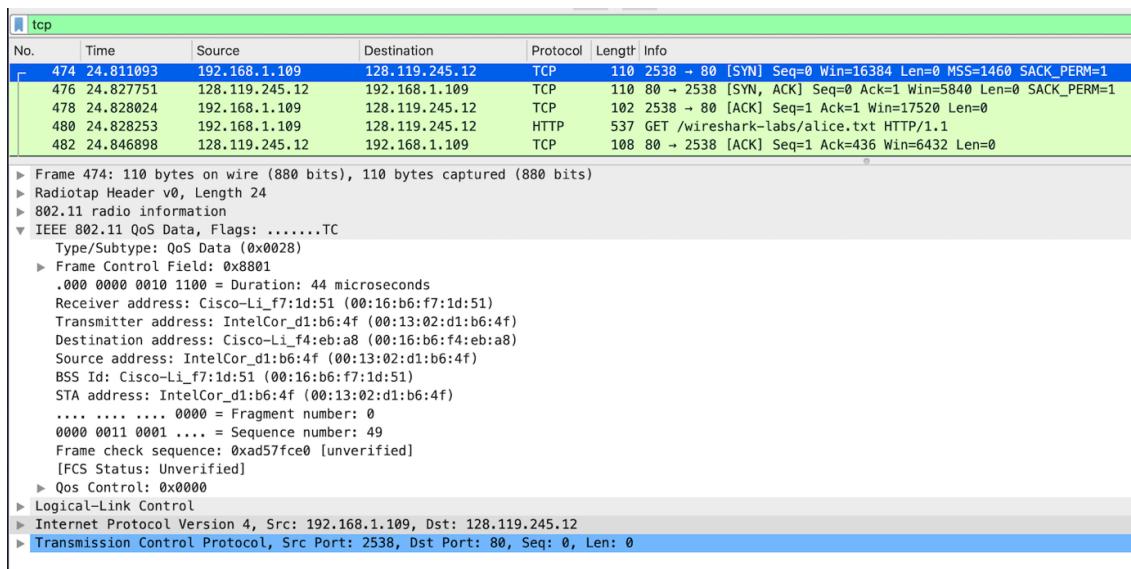


Figura 1.27

O endereço MAC do host é 00:16:b6:f7:1d:51, do AP é 00:13:02:d1:b6:4f e do router do primeiro salto é 00:16:b6:f4:eb:a8. O endereço IP do host que está a enviar este segmento TCP 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.

Como este endereço IP de destino tem como endereço MAC correspondente o 00:16:b6:f4:eb:a8, podemos afirmar que o endereço IP corresponde ao router do primeiro salto.

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?

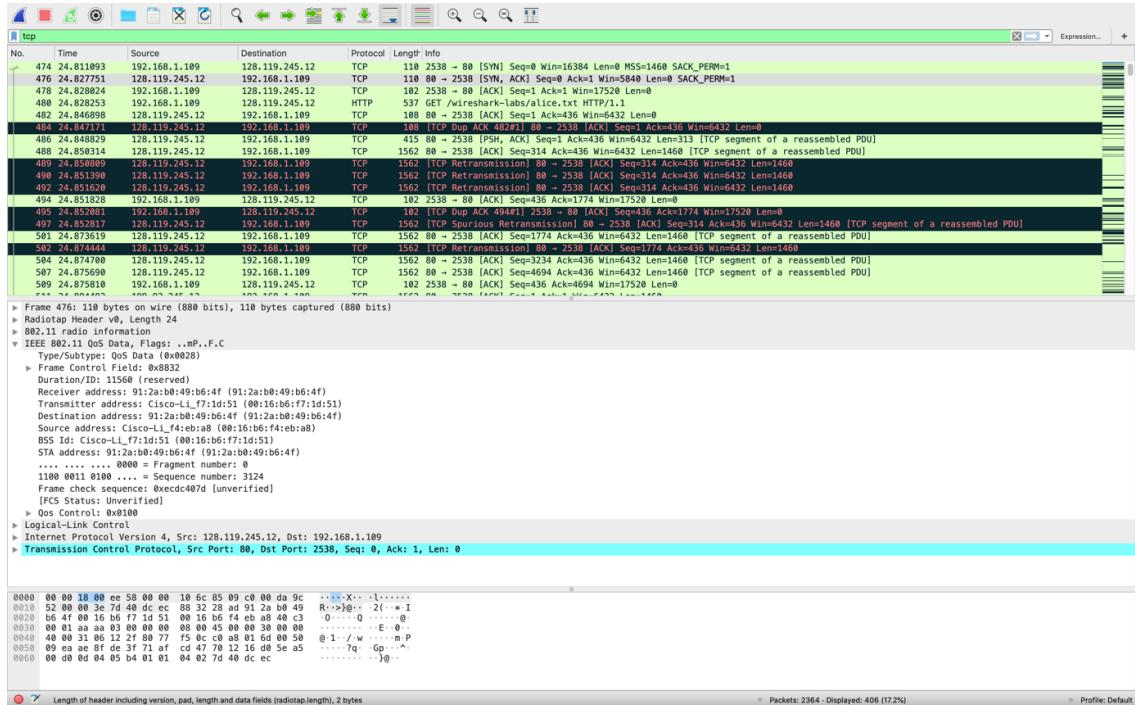


Figura 1.28

Os três campos dos endereços MAC na trama 802.11 são:
 Source address: Cisco-Li'f4:eb:a8 (00:16:b6:f4:eb:a8)
 Destination address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
 BSS Id: Cisco-Li'f7:1d:51 (00:16:b6:f7:1d:51)

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

O endereço MAC do host é 00:16:b6:f7:1d:51, do AP é 91:2a:b0:49:b6:4f e o router do primeiro salto é 00:16:b6:f4:eb:a8.

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 corresponde ao endereço IP 128.119.245.12, mas o IP do dispositivo que enviou o segmento TCP encapsulado neste datagrama é 192.168.1.109. Logo, o endereço MAC de origem na trama não corresponde ao endereço IP do dispositivo que enviou o segmento TCP encapsulado neste datagrama.

Capítulo 2

Conclusão

Com este trabalho prático conseguimos explorar vários aspectos do protocolo IEEE 802.11, nomeadamente, o formato das tramas, o endereçamento dos componentes envolvidos na comunicação sem fios, os tipos de tramas mais comuns e a operação do protocolo. Começamos por analisar informação rádio referente ao nível físico, seguimos para o estudo de scanning relativamente a tramas enviadas periodicamente. Por fim analisamos processos de associação e as suas trocas de tramas e estudamos a transferência de dados com os seus protocolos associados. Apesar da prática com a ferramenta Wireshark nos trabalhos práticos anteriores, ainda tivemos que aprofundar os nossos conhecimentos, nomeadamente, ao uso de filtros na ajuda da procura de tramas.