



Universidade do Minho
Escola de Engenharia

Redes de Computadores TP4 PL5 Grupo 1

Dezembro de 2019



Ana Margarida Campos
A85166



Ana Catarina Gil A85266



Tânia Rocha A85176

1 Acesso Rádio

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 a que o espectro está a operar a rede sem fios é 2437 MHz. Como observado na fig.1, o canal que corresponde a esta mesma frequência é o canal 6.

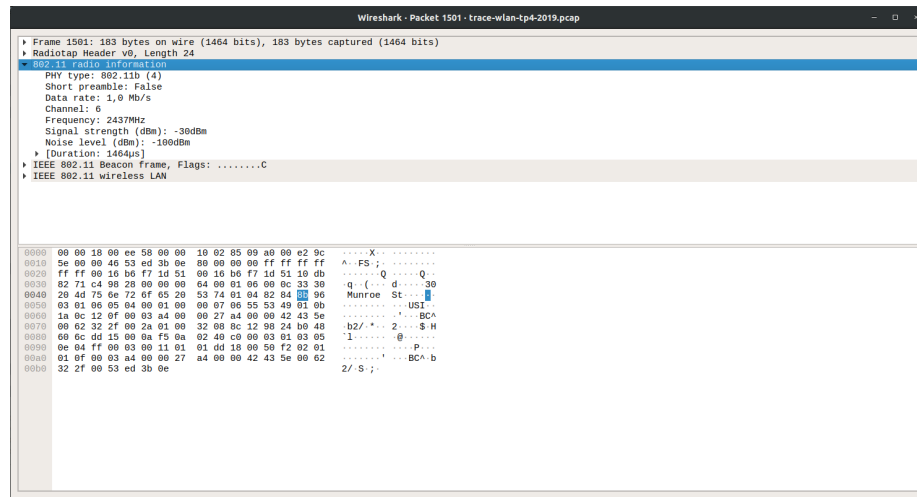


Figure 1: Trama correspondente ao número 1501.

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

A versão da norma IEEE 802.11 que está a ser utilizada é 802.11b.(Fig.1)

1.3 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.

Também observável na Fig.1, o débito enviado pela trama escolhida é 1.0 Mb/s, que corresponde a 8Mbps. Este valor não corresponde ao débito máximo, visto que o máximo é 11Mbps, uma vez que a versão utilizada é 802.11b.

2 Scanning

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

Os SSID dos dois APs são os seguintes:

SSID = 30 Munroe St

SSID = linksys_SES_24086

No.	Time	Source	Destination	Protocol	Length	Info
2320	71.445542	Cisco-L1.f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3810, FN=0, Flags=.....C, B1=100, SSID=30 Munroe St
2322	71.147898	Cisco-L1.f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3813, FN=0, Flags=.....C, B1=100, SSID=30 Munroe St
2323	71.258339	Cisco-L1.f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3812, FN=0, Flags=.....C, B1=100, SSID=30 Munroe St
2327	71.352780	Cisco-L1.f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3813, FN=0, Flags=.....C, B1=100, SSID=30 Munroe St
2328	71.455965	Cisco-L1.f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3814, FN=0, Flags=.....C, B1=100, SSID=30 Munroe St
2331	71.557330	Cisco-L1.f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3815, FN=0, Flags=.....C, B1=100, SSID=30 Munroe St
2334	71.658897	Cisco-L1.f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3816, FN=0, Flags=.....C, B1=100, SSID=30 Munroe St
2336	71.762287	Cisco-L1.f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3817, FN=0, Flags=.....C, B1=100, SSID=30 Munroe St
2337	71.864626	Cisco-L1.f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3818, FN=0, Flags=.....C, B1=100, SSID=30 Munroe St
2338	71.967182	Cisco-L1.f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3819, FN=0, Flags=.....C, B1=100, SSID=30 Munroe St
2339	72.069393	Cisco-L1.f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3820, FN=0, Flags=.....C, B1=100, SSID=30 Munroe St
2340	72.172249	Cisco-L1.f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3821, FN=0, Flags=.....C, B1=100, SSID=30 Munroe St
2343	72.274367	Cisco-L1.f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3822, FN=0, Flags=.....C, B1=100, SSID=30 Munroe St
2345	72.376568	Cisco-L1.f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3823, FN=0, Flags=.....C, B1=100, SSID=30 Munroe St
2347	72.478921	Cisco-L1.f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3824, FN=0, Flags=.....C, B1=100, SSID=30 Munroe St
2348	72.581464	Cisco-L1.f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3825, FN=0, Flags=.....C, B1=100, SSID=30 Munroe St
2349	72.683846	Cisco-L1.f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3826, FN=0, Flags=.....C, B1=100, SSID=30 Munroe St
2352	72.786234	Cisco-L1.f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3826, FN=0, Flags=.....C, B1=100, SSID=30 Munroe St
2353	72.888678	Cisco-L1.f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3829, FN=0, Flags=.....C, B1=100, SSID=30 Munroe St
2354	72.991058	Cisco-L1.f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3830, FN=0, Flags=.....C, B1=100, SSID=30 Munroe St
2357	73.093344	Cisco-L1.f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3831, FN=0, Flags=.....C, B1=100, SSID=30 Munroe St
2359	73.195849	Cisco-L1.f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3832, FN=0, Flags=.....C, B1=100, SSID=30 Munroe St
2364	73.298063	Cisco-L1.f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3833, FN=0, Flags=.....C, B1=100, SSID=linksys_SES_24086
2368	73.398107	Cisco-L1.f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3833, FN=0, Flags=.....C, B1=100, SSID=30 Munroe St
2361	73.498462	Cisco-L1.f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3834, FN=0, Flags=.....C, B1=100, SSID=30 Munroe St
2362	73.593948	Cisco-L1.f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3835, FN=0, Flags=.....C, B1=100, SSID=30 Munroe St
2363	73.695445	Cisco-L1.f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3836, FN=0, Flags=.....C, B1=100, SSID=30 Munroe St
2369	69.463202	Cisco-L1.f5:ba:bb	Broadcast	802.11	132	Beacon frame, SN=3838, FN=0, Flags=.....C, B1=100, SSID=linksys_SES_24086
2371	11.101576	Cisco-L1.f5:ba:bb	Broadcast	802.11	132	Beacon frame, SN=3840, FN=0, Flags=.....C, B1=100, SSID=linksys_SES_24086

Figure 2: Trama de beacon

2.2 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.

Em ambas as tramas beacon o intervalo de tempo é 0.102400 segundos. A periodicidade é apenas verificada para o AP 30 Munroe St.

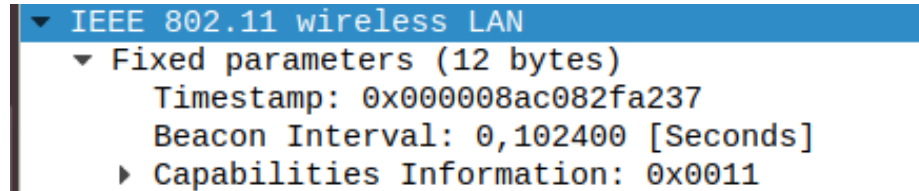


Figure 3: Intervalo da trama Beacon

2.3 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

O MAC address de origem é 00:16:b6:f7:1d:51.(Fig.4)

```
▶ Frame 2331: 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
    ....00 = Version: 0
    ....00.. = Type: Management frame (0)
    1000 .... = Subtype: 8
  ▼ Flags: 0x00
    ....000 = 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 1110 0111 .... = Sequence number: 3815
  Frame check sequence: 0xb6c510b [correct]
  [FCS Status: Good]
▶ IEEE 802.11 wireless LAN
```

Figure 4: Endereço Mac de Origem

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

O MAC address de destino é ff:ff:ff:ff:ff:ff.

```
▶ 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
    ....00 = Version: 0
    ....00.. = Type: Management frame (0)
    1000 .... = Subtype: 8
  ▼ Flags: 0x00
    ....000 = 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 1110 0101 .... = Sequence number: 3813
```

Figure 5: Endereço Mac de Destino

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

O MAC address BSS ID é 00:16:p6:f7:1d:51.

```

802.11 radio information
IEEE 802.11 Beacon frame, Flags: .....C
  Type/Subtype: Beacon frame (0x0008)
  Frame Control Field: 0x0000
    ....0000 = Version: 0
    ....00.. = Type: Management frame (0)
    1000 .... = Subtype: 8
  Flags: 0x00
    ....0000 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x0)
    ....0... = More Fragments: This is the last fragment
    ....0... = Retry: Frame is not being retransmitted
    ...0 .... = PWR MGT: STA will stay up
    ..0. .... = More Data: No data buffered
    .0.. .... = Protected flag: Data is not protected
    0... .... = Order flag: Not strictly ordered
    .000 0000 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 1110 0101 .... = Sequence number: 3813
    Frame check sequence: 0x7796f4db [correct]
  
```

Figure 6: Endereço Mac BSS ID da trama beacon 30 Munroe St

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

<pre> Tagged parameters (119 bytes) Tag: SSID parameter set: 30 Munroe St Tag: Supported Rates (1) 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) </pre> <p>Data Rates</p>	<pre> Tag: Extended Supported Rates (50) 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) (0x80) Extended Supported Rates: 36 (0x48) Extended Supported Rates: 48 (0x60) Extended Supported Rates: 54 (0x6c) </pre> <p>Extended Supported Rates</p>
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

2.7 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)?

O valor do tipo é 0. O valor do subtipo é 8. A parte do cabeçalho onde estão especificados é na Frame Control File.

```

▼ IEEE 802.11 Beacon frame, Flags: .....C
  Type/Subtype: Beacon frame (0x0008)
  ▼ Frame Control Field: 0x8000
    .... ..00 = Version: 0
    .... 00.. = Type: Management frame (0)
    1000 .... = Subtype: 8
    -- -- --

```

Figure 7: Tipos e subtipos da trama

2.8 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.

Sim, está a ser utilizado em todas, mas como podemos observar nem todas estão a ser corretas.

```

▼ 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
    1101 1011 0001 .... = Sequence number: 3505
    Frame check sequence: 0x0e3bed53 [correct]
    [FCS Status: Good]
  ▶ IEEE 802.11 wireless LAN

```

Figure 8: Frame Check Sequence [correct]

```

▶ Radiotap Header v0, Length 24
▶ 802.11 radio information
▼ IEEE 802.11 Beacon frame, Flags: .....
  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: LinksysG_67:22:94 (00:06:25:67:22:94)
    Source address: LinksysG_67:22:94 (00:06:25:67:22:94)
    BSS Id: LinksysG_67:22:94 (00:06:25:67:22:94)
    .... .... 0000 = Fragment number: 0
    1100 0000 0111 .... = Sequence number: 3079
  ▶ Frame check sequence: 0x324da246 incorrect, should be 0x44490d26
    [FCS Status: Bad]
▶ IEEE 802.11 wireless LAN

```

Figure 9: Frame Check Sequence [incorrect]

2.9 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.

Receiver Address : ff:ff:ff:ff:ff:ff
 Destination Address : ff:ff:ff:ff:ff:ff
 Transmitter Address : 00:16:b6:f7:1d:51
 Source Address : 00:16:b6:f7:1d:51

```

▶ 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
    1101 1011 0001 .... = Sequence number: 3505
    Frame check sequence: 0x0e3bed53 [correct]
    [FCS Status: Good]
▶ IEEE 802.11 wireless LAN

```

Figure 10: Registos MAC

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

Como é observável na seguinte figura. Para conseguirmos obter simultaneamente o Probe Response e o Probe Request tivemos que filtrar através dos seus endereços correspondentes. 0x0004 para o Probe Request e 0x0005 para o Probe Response. O Filtro utilizado foi 'wlan.fc.type_subtype == 0x0004 or wlan.fc.type_subtype == 0x0005', onde o 'or' foi o que permitiu observá-los simultaneamente.

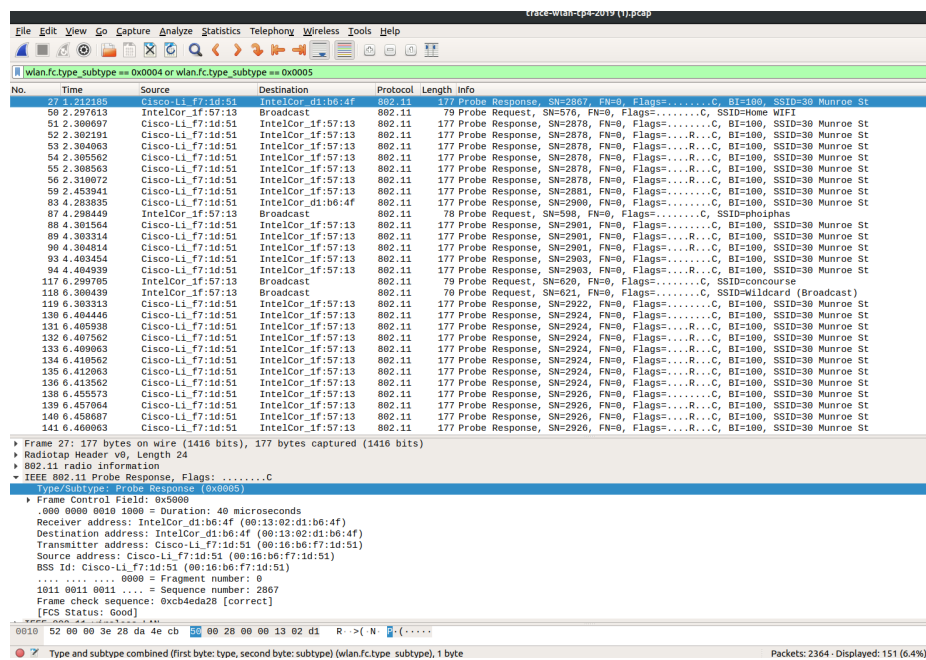


Figure 11: Probe Request e Probe Response

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

O objetivo da Trama Probe Request é obter informações de uma outra estação. Esta trama é útil para um STA determinar quais os APs que estão dentro do seu alcance rádio. Por outro lado, o objetivo da trama Probe Response é de fornecer a resposta contendo informações sobre as taxas de dados suportadas. Para cada uma das tramas os endereços Destinations e Source são os seguintes:

Probe Request:

Source MAC Address : 00:16:b6:f7:1d:51

Destination MAC Address : 00:12:f0:1f:57:13

Probe Response:

Source MAC Address : 00:12:f0:1f:57:13

Destination MAC Address : ff:ff:ff:ff:ff:ff

```
138 6.455573 Cisco-Li_f7:1d:51 IntelCor_1f:57:13 802.11 177 Probe Response, SN=2926, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
139 6.457864 Cisco-Li_f7:1d:51 IntelCor_1f:57:13 802.11 177 Probe Response, SN=2926, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
140 6.459593 Cisco-Li_f7:1d:51 IntelCor_1f:57:13 802.11 177 Probe Response, SN=2926, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
141 6.460963 Cisco-Li_f7:1d:51 IntelCor_1f:57:13 802.11 177 Probe Response, SN=2926, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
> Frame 140: 177 bytes on wire (1416 bits), 177 bytes captured (1416 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
  IEEE 802.11 Probe Response, Flags: .....C
    Type/Subtype: Probe Response (0x0005)
    > Frame Control Field: 0x0000
      000 0001 0011 1010 = Duration: 314 microseconds
      Receiver address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
      Destination address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
      Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
      Source address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
      BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
      .... .. 0000 = Fragment number: 0
      1011 0110 1110 .... = Sequence number: 2926
      Frame check sequence: 0x5c8e1061 [correct]
      [FCS Status: Good]
```

Figure 12: MAC BSS ID de Destino da trama Probe Response

```
156 7.355800 Cisco-Li_f7:1d:51 IntelCor_d1:b6:4f 802.11 177 Probe Response, SN=2936, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
171 8.299988 IntelCor_1f:57:13 Broadcast 802.11 77 Probe Request, SN=642, FN=0, Flags=.....C, SSID=linksys
173 8.303567 Cisco-Li_f7:1d:51 IntelCor_1f:57:13 802.11 177 Probe Response, SN=2946, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
174 8.305056 Cisco-Li_f7:1d:51 IntelCor_1f:57:13 802.11 177 Probe Response, SN=2946, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
175 8.306687 Cisco-Li_f7:1d:51 IntelCor_1f:57:13 802.11 177 Probe Response, SN=2946, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
> Frame 171: 77 bytes on wire (616 bits), 77 bytes captured (616 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 1000 0010 .... = Sequence number: 642
      Frame check sequence: 0xabc7bcb5 [correct]
      [FCS Status: Good]
```

Figure 13: MAC BSS ID de Destino da trama Probe Response

2.12 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?

```
1629 46.780197 IntelCor_d1:b6:4f Broadcast 802.11 82 Probe Request, SN=1577, FN=0, Flags=.....C, SSID=wildcard (Broadcast)
> Frame 1629: 82 bytes on wire (656 bits), 82 bytes captured (656 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_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)
      .... .. 0000 = Fragment number: 0
      0110 0010 1001 .... = Sequence number: 1577
      Frame check sequence: 0xe2653ef6 [correct]
      [FCS Status: Good]
  IEEE 802.11 wireless LAN
```

Figure 14: Endereço de Probe Request

1624	48	742869	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=3557, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
▶ Frame 1624: 177 bytes on wire (1416 bits), 177 bytes captured (1416 bits) ▶ Radiotap Header v0, Length 24 ▶ 802.11 radio information ▶ IEEE 802.11 Probe Response, Flags:C Type/Subtype: Probe Response (0x0005) ▶ Frame Control Field: 0x5008 0000 0001 0011 1010 = Duration: 314 microseconds 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: 6x5a5e5bd8 [correct] [FCS Status: Good] ▶ IEEE 802.11 wireless LAN							

Figure 15: Endereço de Probe Response

3 Processo de Associação

3.1 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?

As duas ações realizadas ocorrem quando $t=49.583615$, em que o DHCP release é enviado pelo Host para o DHCP server, cujo IP é 192.168.1.109, e quando $t=49.609617$, o Host envia uma frame de DEAUTHENTICATION. Era também esperado que estivesse presente a trama de DISASSOCIATION.

1732	48	542481	Cisco-Li_f7:1d:51	Broadcast	802.11	163	Beacon frame, SN=3588, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1733	48	583615	192.168.1.109	192.168.1.1	DHCP	390	DHCP Release - Transaction ID 0x5a5a520
1734	48	583771	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C
1735	48	589617	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	Deauthentication, SN=1006, FN=0, Flags=.....C
1736	48	589779	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C
1737	48	614478	IntelCor_d1:b6:4f	Broadcast	802.11	99	Probe Request, SN=1006, FN=0, Flags=.....C, SSID=linksys_SES_24086
1738	48	615860	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	38	Acknowledgement, Flags=.....C
1739	48	617713	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	38	Acknowledgement, Flags=.....C
1740	48	638957	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1006, FN=0, Flags=.....C
1741	48	639700	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1006, FN=0, Flags=.....C
1742	48	640702	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1006, FN=0, Flags=.....C
1743	48	641910	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	38	Acknowledgement, Flags=.....C
1744	48	642315	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1006, FN=0, Flags=.....C
1745	48	644710	Cisco-Li_f7:1d:51	Broadcast	802.11	163	Beacon frame, SN=3589, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1746	48	645319	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1006, FN=0, Flags=.....C
1747	48	646711	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	38	Acknowledgement, Flags=.....C
1748	48	647827	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	38	Acknowledgement, Flags=.....C

Figure 16: Tramas em que $t=49$

3.2 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 $t=49$?

Existem 15 mensagens de autenticação enviadas.

wlan.fc.type_subtype == 11						
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	49.639709	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

Figure 17: Número de mensagens enviadas para o AP linksys_ses_24086

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

O tipo de autenticação pretendida é 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)

Figure 18: Autenticação aberta

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

Não se observa resposta de autenticação.

3.5 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?

Em t= 63.168087 aparece a trama de autenticação. Para a resposta, t=63.161272.

wlan.fc.type_subtype == 11						
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	62.174970	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0, Flags=.....R...C
2158	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

<ul style="list-style-type: none"> Flags: 0x10 Data Rate: 54,0 Mb/s Channel Frequency: 2437 [BG 6] Channel flags: 0x00c0, Orthogonal Frequency-Division Multiplexing (OFDM), 2 GHz spectrum Antenna signal: -28dBm Antenna noise: -100dBm Signal Quality: 89 Antenna: 0 dB antenna signal: 72dB RX flags: 0xcbe0 802.11 radio information IEEE 802.11 Authentication, Flags:C <ul style="list-style-type: none"> Type/Subtype: Authentication (0x000b) Frame Control Field: 0xb000 <ul style="list-style-type: none"> 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 0110 1111 = Sequence number: 1647 Frame check sequence: 0x47e8cbe0 [correct] [FCS Status: Good] IEEE 802.11 wireless LAN

Figure 19: Intervalo em que uma trama authentication aparece

No.	Time	Source	Destination	Protocol	Length	Info
2156	63.169087	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58	Authentication, SN=1647, FN=0, Flags=.....C
2155	63.161272	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3725, FN=9, Flags=.....C, BI=109, SSID=30 Munroe St
2154	63.142860	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C
2153	63.142451	IntelCor_d1:b6:4f	Broadcast	802.11	177	Probe Response, SN=3724, FN=0, Flags=.....C, BI=109, SSID=30 Munroe St
2152	63.140100	IntelCor_d1:b6:4f	Broadcast	802.11	94	Probe Request, SN=1647, FN=9, Flags=.....C, SSID=30 Munroe St
2151	63.135362	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	54	Deauthentication, SN=1646, FN=0, Flags=....R...C
2150	63.116231	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	54	Deauthentication, SN=1646, FN=0, Flags=....R...C
2149	63.094985	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	54	Deauthentication, SN=1646, FN=0, Flags=....R...C
2148	63.090971	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	54	Deauthentication, SN=1646, FN=0, Flags=....R...C
▶ Frame 2155: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits) on interface 0 ▶ Radiotap Header v0, Length 24 ▶ IEEE 802.11 radio information ▶ Type/Subtype: Beacon frame (8x8000) ▶ 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 1110 1000 1101 = Sequence number: 3725 Frame check sequence: 0xaf6c431e [correct] [FCS Status: good] ▶ IEEE 802.11 wireless LAN						

Figure 20: Intervalo em que uma trama de resposta aparece

3.6 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 Que taxas de transmissão o host está disposto a usar? E o AP? Munroe St? Quando é enviado o correspondente associate reply ?

O host enviou um ASSOCIATION REQUEST para Munroe St a $t = 63.19910$ e este respondeu a $t=63.192101$.

wlan.fc.subtype=2 and wlan.fc.type=0 and wlan.addr_resolved=IntelCor_d1:b6:4f						
No.	Time	Source	Destination	Protocol	Length	Info
1750	49.051978	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
1751	49.053218	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=....R...C, SSID=linksys_SES_24086
1825	53.789943	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=....R...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=....R...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=....R...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=....R...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

Figure 21: Taxas de transmissão

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

1, 2, 5.5, 11, 6, 9, 12, 18 [Mbit/sec].

- ▶ 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]

Figure 22: Taxas de transmissão

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

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 (- 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 (- 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	Cisco-Li_f7:1d:51	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 63.170006		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	

Figure 23: sequência de tramas

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

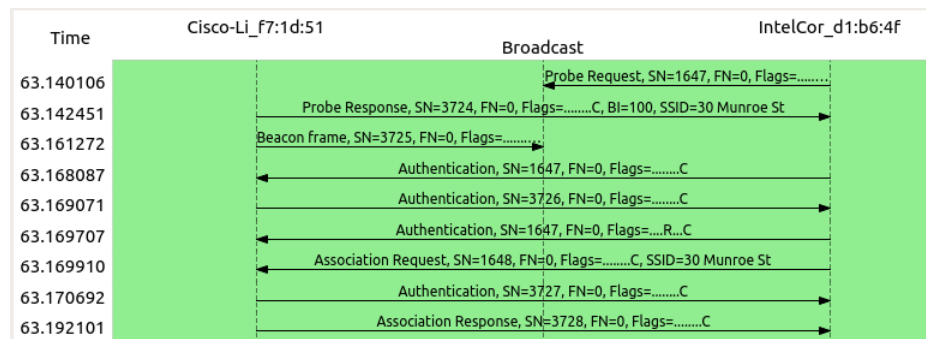


Figure 24: Diagrama de Sequência

4 Transferência de Dados

4.1 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?

Cisco-li: f7:1d:51(00:16:b6:f7:1d:51)
Source Address IntelCor: d1:b6:4f(00:13:02:d1:b6:4f)
Destination Cisco-Li: f4:eb:a8(00:16:b6:f4:eb:a8)

```
▶ 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 [correct]
    [FCS Status: Good]
```

Figure 25: Endereços MAC

4.2 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?

Host: IntelCor d1:b6:4f (00:13:02:d1:b6:4f)
AP: - Cisco-Li f4:eb:a8 (00:16:b6:f4:eb:a8)
1º salto: IntelCor d1:b6:4f (00:13:02:d1:b6:4f)
IP de Source: 192.168.1.109
IP de destino: 128.119.245.12

```

▶ 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 [correct]
        [FCS Status: Good]
    ▶ Qos Control: 0x0000
    ▶ Logical-Link Control
    ▼ 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
    ▶ Transmission Control Protocol, Src Port: 2538, Dst Port: 80, Seq: 0, Len: 0

```

Figure 26: Endereços e IP

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

Este endereço IP corresponde a um AP, visto que tem um BSS Id.

```
▶ 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 [correct]
    [FCS Status: Good]
```

Figure 27: Endereço IP de destino corresponde ao host

4.4 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?

Como é observável na figura seguinte, os endereços são:

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

Destination: 91:2a:b0:4:b6:4f

Source: Cisco-Li f4:eb:a8 (00:16:b6:f4:eb:a8)

```

▶ Frame 476: 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: ..mP..F..
  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 = Fragment number: 0
    1100 0011 0100 .... = Sequence number: 3124
  ▶ Frame check sequence: 0xecdc407d incorrect, should be 0x94d06e29
    [FCS Status: Bad]
  ▶ Qos Control: 0x0100
▶ Logical-Link Control
▼ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.109

```

Figure 28: Trama 802.11 que contém o segmento SYNACK para esta sessão TCP

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

Host: STA (91:2a:b0:19:b6:4f)

Source Address: Cisco-Li f4:eb:a8 (00:16:b6:f4:eb:a8)

1º salto: Cisco-Li1 f7:1d:51 (00:16:b6:f7:1d:51).

```

▶ Frame 476: 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: ..mP..F..
  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 = Fragment number: 0
    1100 0011 0100 .... = Sequence number: 3124

```

Figure 29: Endereço MAC

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

O MAC address na trama não corresponde ao endereço IP do dispositivo que enviou o segmento tcp encapsulado no datagrama, pois o endereço IP TCP SYNACK é 128.119.245.12. No entanto, o endereço IP de destino é 192.168.1.109.

5 Conclusão

Com a realização deste trabalho foi nos dada a oportunidade de desenvolver capacidades de interpretação sobre o protocolo IEEE 802.11. Isto deu-se através da análise no wireshark de um ficheiro fornecido pelos docentes com uma listagem de exercicios e de apontamentos sobre este mesmo assunto.

Foram-nos fornecidos exercicios sobre vários tópicos que nos permitiram aprofundar o conhecimento sobre os mesmos. Estes tópicos foram acesso rápido, scanning, processo de associação e transferência de dados.

Assim, podemos afirmar que este trabalho nos permitiu ter uma conhecimento mais abrangente sobre esta matéria, que nos pode vir a ser útil futuramente.