



Redes de Computadores 2019/2020

TP4: Redes sem Fios (802.11) Grupo 05



Ana Afonso
A85762



João Diogo Mota
A80791



Márcia Teixeira
A80943



1. Questões e Respostas

1.1 Acesso Rádio

Questão 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 em que a rede sem fios está a operar é: 2437MHz, o que corresponde ao canal 6.

```
▶ Frame 1405: 183 bytes on wire (1464 bits), 183 bytes captured (1464 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): 69dB
  Signal strength (dBm): -31dBm
  Noise level (dBm): -100dBm
  Signal/noise ratio (dB): 69dB
  ▶ [Duration: 1464µs]
▶ IEEE 802.11 Beacon frame, Flags: .....C
▶ IEEE 802.11 wireless LAN
```

Figura 1: Análise da Trama - Frequência e Canal

Questão 2

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

Está a ser usada a versão 802.11b (4).

```
▶ Frame 1405: 183 bytes on wire (1464 bits), 183 bytes captured (1464 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): 69dB
  Signal strength (dBm): -31dBm
  Noise level (dBm): -100dBm
  Signal/noise ratio (dB): 69dB
  ▶ [Duration: 1464µs]
▶ IEEE 802.11 Beacon frame, Flags: .....C
▶ IEEE 802.11 wireless LAN
```

Figura 2: Análise de Trama - PHY type



Questão 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 escolhida (1405) foi enviada é de 1.0 Mb/s. Tal como podemos ver através da Figura 4, esse débito não corresponde ao débito máximo a que a interface Wi-Fi pode operar visto que este é de 54Mb/s.

```
▶ Frame 1405: 183 bytes on wire (1464 bits), 183 bytes captured (1464 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): 69dB
  Signal strength (dBm): -31dBm
  Noise level (dBm): -100dBm
  Signal/noise ratio (dB): 69dB
▶ [Duration: 1464µs]
▶ IEEE 802.11 Beacon frame, Flags: .....C
▶ IEEE 802.11 wireless LAN
```

Figura 3: Análise da Trama - Data rate

```
▶ Frame 1405: 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
▼ IEEE 802.11 wireless LAN
  ▶ Fixed parameters (12 bytes)
  ▼ 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: 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: Vendor Specific: Airgo Networks, Inc.
    ▶ Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
```

Figura 4: Análise da Trama - Tag: Extended Supported Rates



1.2 Scanning

Questão 4

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

Os SSIDs dos dois APs que estão a emitir a maioria das tramas beacon são: *30 Munroe St* e *linksys12*.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|-------------------|-------------------|----------|--------|--|
| 246 | 11.491223 | Cisco-Li-f7:1d:51 | broadcast | 802.11 | 183 | Beacon frame, Src=2984, Prio=0, Flags=.....C, BI=100, SSID=30 Munroe St |
| 247 | 11.491463 | IntelCor_d1:b6:4f | Cisco-Li-f7:1d:51 | 802.11 | 54 | QoS Null function (No data), SN=1584, Prio=0, Flags=.....TC |
| 248 | 11.491568 | IntelCor_d1:b6:4f | IntelCor_d1:b6:4f | 802.11 | 38 | Acknowledgement, Flags=.....C |
| 249 | 11.492442 | Cisco-Li-f7:1d:51 | Cisco-Li-f7:1d:51 | 802.11 | 54 | QoS Null function (No data), SN=1585, Prio=0, Flags=...P...TC |
| 250 | 11.492542 | IntelCor_d1:b6:4f | IntelCor_d1:b6:4f | 802.11 | 38 | Acknowledgement, Flags=.....C |
| 251 | 11.503787 | Cisco-Li-f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=2983, Prio=0, Flags=.....C, BI=100, SSID=30 Munroe St |
| 252 | 11.506148 | Cisco-Li-f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=2984, Prio=0, Flags=.....C, BI=100, SSID=30 Munroe St |
| 253 | 11.506857 | 08:86:bcd2:22:94 | ff:ff:ff:ff:ff:ff | 802.11 | 96 | Beacon frame, SN=3183, Prio=0, Flags=.....C, BI=114, SSID=linksys12 |
| 254 | 11.736489 | Cisco-Li-f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=2985, Prio=0, Flags=.....C, BI=100, SSID=30 Munroe St |
| 255 | 11.866890 | Cisco-Li-f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=2986, Prio=0, Flags=.....C, BI=100, SSID=30 Munroe St |
| 256 | 11.963428 | Cisco-Li-f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=2987, Prio=0, Flags=.....C, BI=100, SSID=30 Munroe St |
| 257 | 12.065096 | Cisco-Li-f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=2988, Prio=0, Flags=.....C, BI=100, SSID=30 Munroe St |
| 258 | 12.168142 | Cisco-Li-f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=2989, Prio=0, Flags=.....C, BI=100, SSID=30 Munroe St |
| 259 | 12.278538 | Cisco-Li-f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=2990, Prio=0, Flags=.....C, BI=100, SSID=30 Munroe St |
| 260 | 12.380694 | IntelCor_1f:57:13 | Broadcast | 802.11 | 75 | Probe Request, SN=460, Prio=0, Flags=.....C, SSID=80802 |
| 261 | 12.382948 | Cisco-Li-39:8a:28 | Cisco-Li-39:8a:28 | 802.11 | 38 | Acknowledgement, Flags=.....C |
| 262 | 12.372835 | Cisco-Li-f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=2991, Prio=0, Flags=.....C, BI=100, SSID=30 Munroe St |
| 263 | 12.388515 | Cisco-Li-f7:1d:51 | IntelCor_1f:57:13 | 802.11 | 177 | Probe Response, SN=2992, Prio=0, Flags=.....C, BI=100, SSID=30 Munroe St |
| 264 | 12.381114 | Cisco-Li-f7:1d:51 | IntelCor_1f:57:13 | 802.11 | 177 | Probe Response, SN=2992, Prio=0, Flags=.....C, BI=100, SSID=30 Munroe St |
| 265 | 12.383564 | Cisco-Li-f7:1d:51 | IntelCor_1f:57:13 | 802.11 | 177 | Probe Response, SN=2992, Prio=0, Flags=.....C, BI=100, SSID=30 Munroe St |
| 266 | 12.385862 | Cisco-Li-f7:1d:51 | IntelCor_1f:57:13 | 802.11 | 177 | Probe Response, SN=2992, Prio=0, Flags=.....C, BI=100, SSID=30 Munroe St |
| 267 | 12.386565 | Cisco-Li-f7:1d:51 | IntelCor_1f:57:13 | 802.11 | 177 | Probe Response, SN=2992, Prio=0, Flags=.....C, BI=100, SSID=30 Munroe St |
| 268 | 12.388067 | Cisco-Li-f7:1d:51 | IntelCor_1f:57:13 | 802.11 | 177 | Probe Response, SN=2992, Prio=0, Flags=.....C, BI=100, SSID=30 Munroe St |
| 269 | 12.389438 | Cisco-Li-f7:1d:51 | IntelCor_1f:57:13 | 802.11 | 177 | Probe Response, SN=2992, Prio=0, Flags=.....C, BI=100, SSID=30 Munroe St |
| 270 | 12.475300 | Broadcast | Cisco-Li-f7:1d:51 | 802.11 | 183 | Beacon frame, SN=2993, Prio=0, Flags=.....C, BI=100, SSID=30 Munroe St |
| 271 | 12.475442 | IntelCor_d1:b6:4f | Cisco-Li-f7:1d:51 | 802.11 | 54 | QoS Null function (No data), SN=1586, Prio=0, Flags=.....TC |
| 272 | 12.475548 | IntelCor_d1:b6:4f | IntelCor_d1:b6:4f | 802.11 | 38 | Acknowledgement, Flags=.....C |

Figura 5: Captura do tráfego WireShark

Questão 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.

O intervalo de tempo é constante como podemos verificar pelo campo *“Beacon Interval”*, sendo este $t = 0.102400s$. Esta periodicidade é verificada visto que se tratam de tramas de tipo *“Management”* (como é possível verificar através da tabela anexada ao enunciado).



```
▶ Frame 1514: 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
▼ IEEE 802.11 wireless LAN
  ▼ Fixed parameters (12 bytes)
    Timestamp: 174361907586
    Beacon Interval: 0.102400 [Seconds]
  ▶ Capabilities Information: 0x0601
  ▶ Tagged parameters (119 bytes)
```

Figura 6: Análise dos campos da trama – Beacon Interval

```
▶ Frame 1518: 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
▼ IEEE 802.11 wireless LAN
  ▼ Fixed parameters (12 bytes)
    Timestamp: 174362112386
    Beacon Interval: 0.102400 [Seconds]
  ▶ Capabilities Information: 0x0601
  ▶ Tagged parameters (119 bytes)
```

Figura 7: Análise dos campos da trama - Beacon Interval

```
▶ Frame 1499: 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: 6351964057993
    Beacon Interval: 0.102400 [Seconds]
  ▶ Capabilities Information: 0x0011
  ▶ Tagged parameters (68 bytes)
```

Figura 8: Análise dos campos da trama - Beacon Interval

```
▶ Frame 1513: 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: 6351964365199
    Beacon Interval: 0.102400 [Seconds]
  ▶ Capabilities Information: 0x0011
  ▶ Tagged parameters (68 bytes)
```

Figura 9: Análise dos campos da trama - Beacon Interval

Questão 6

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

O endereço MAC de origem da trama *beacon* de 30 Munroe St é 00:16:b6:f7:1d:51.

```
▶ Frame 1514: 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
  1101 1011 0100 .... = Sequence number: 3508
  Frame check sequence: 0x517a3acf [unverified]
  [FCS Status: Unverified]
▼ IEEE 802.11 wireless LAN
  ▶ Fixed parameters (12 bytes)
  ▶ Tagged parameters (119 bytes)
```

Figura 10: Análise da trama - Campo Source address



Questão 7

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

O endereço MAC de destino da trama *beacon* de *Munroe St* é ff:ff:ff:ff:ff:ff.

```
▶ Frame 1514: 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
  1101 1011 0100 .... = Sequence number: 3508
  Frame check sequence: 0x517a3acf [unverified]
  [FCS Status: Unverified]
▼ IEEE 802.11 wireless LAN
  ▶ Fixed parameters (12 bytes)
  ▶ Tagged parameters (119 bytes)
```

Figura 11: Análise da trama - Campo Destination address

Questão 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 de: 00:16:b6:f7:1d:51.

```
▶ Frame 1514: 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
  1101 1011 0100 .... = Sequence number: 3508
  Frame check sequence: 0x517a3acf [unverified]
  [FCS Status: Unverified]
▼ IEEE 802.11 wireless LAN
  ▶ Fixed parameters (12 bytes)
  ▶ Tagged parameters (119 bytes)
```

Figura 12: Análise da trama - Campo BSS Id



Questão 9

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

Supported Rates: 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]

Extended Supported Rates: 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]

```
► Frame 1514: 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
▼ IEEE 802.11 wireless LAN
  ► Fixed parameters (12 bytes)
  ▼ 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: 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: Vendor Specific: Airgo Networks, Inc.
    ► Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
```

Figura 13: Análise da trama - Campos Supported Rates & Extended Supported Rates

Questão 10

Selecione uma trama beacon.

Esta trama pertence a que tipo de tramas 802.11? Indique o valor dos seus identificadores de tipo e de subtipo. Em que parte concreta do cabeçalho da trama estão especificados?

A trama usada foi 1405.

Como o *Type* = 00 e o *Subtype* = 1000 entende-se que esta trama pertence ao tipo das tramas de gestão (*Management Frame*) e ao subtipo *Beacon*.

Os identificadores estão especificados no byte 24.

```
► Frame 1405: 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 (0x0000)
  Frame Control Field: 0x0000
    .... 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 .... = PMR 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)
```

Figura 14: Análise da trama – Campos type e subtype



Questão 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 nesse tipo de redes locais.

De modo a verificar se está a ser usado o método de deteção de erros CRC e se todas as tramas beacon são recebidas corretamente, foram utilizados os seguintes filtros:

- “ wlan.fc.type_subtype==0x0008”, para selecionar as tramas *Beacon*;
- “wlan.fcs.status==bad”, para restringir as tramas que contêm erros.

Como é possível verificar na figura 15, existiram erros, consequentemente, pode concluir-se que certas tramas não são recebidas corretamente.

O uso de mecanismos de deteção de erros neste tipo de redes locais é muito importante, uma vez que se trata de uma rede sem fios, que ao contrário de uma ligação *ethernet*, é bastante mais propícia a colisões.

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|-----------|-------------------|-------------------|----------|--------|--|
| 10 | 0.284432 | LinksysG_67:22:19 | Broadcast | 802.11 | 90 | Beacon frame, SN=3072, FH=0, Flags=....., BI=02, SSID=Linksys12 |
| 14 | 0.499197 | LinksysG_67:22:19 | Broadcast | 802.11 | 90 | Beacon frame, SN=3074, FH=0, Flags=....., BI=100, SSID=Linksys12 |
| 21 | 1.018949 | LinksysG_67:22:19 | Broadcast | 802.11 | 90 | Beacon frame, SN=3079, FH=0, Flags=....., BI=100, SSID=Linksys12 |
| 23 | 1.113691 | LinksysG_67:22:19 | Broadcast | 802.11 | 90 | Beacon frame, SN=3080, FH=0, Flags=....., BI=100, SSID=Linksys12 |
| 34 | 1.424955 | LinksysG_67:22:19 | Broadcast | 802.11 | 90 | Beacon frame, SN=3083, FH=0, Flags=....., BI=20588, SSID=Linksys12 |
| 41 | 2.835064 | LinksysG_67:22:19 | Broadcast | 802.11 | 90 | Beacon frame, SN=3089, FH=0, Flags=....., BI=100, SSID=Linksys12 |
| 167 | 8.075567 | LinksysG_67:22:19 | ff:df:cf:fe:ff:ff | 802.11 | 90 | Beacon frame, SN=3148, FH=0, Flags=....., BI=100 |
| 169 | 8.178944 | LinksysG_67:22:19 | Broadcast | 802.11 | 90 | Beacon frame, SN=3149, FH=0, Flags=....., BI=100, SSID=Linksys12 |
| 253 | 11.660567 | 00:16:b6:f7:1d:51 | ff:bf:f9:fe:ff:ff | 802.11 | 90 | Beacon frame, SN=3183, FH=0, Flags=....., BI=114, SSID=Linksys12 |
| 1484 | 41.746021 | LinksysG_67:22:19 | Broadcast | 802.11 | 90 | Beacon frame, SN=3479, FH=0, Flags=....., BI=100 |
| 1484 | 42.278822 | LinksysG_67:22:19 | Broadcast | 802.11 | 90 | Beacon frame, SN=3484, FH=0, Flags=....., BI=100, SSID=Linksys12 |
| 1496 | 42.391070 | LinksysG_67:22:19 | ff:a5:ff:ff:ff:ff | 802.11 | 90 | Beacon frame, SN=3485, FH=0, Flags=....., BI=16484, SSID=Linksys12 |
| 1515 | 42.892973 | LinksysG_67:22:19 | ff:ff:ff:ff:ff:a5 | 802.11 | 90 | Beacon frame, SN=3490, FH=0, Flags=....., BI=100, SSID=Linksys12 |
| 1519 | 43.097945 | LinksysG_67:22:19 | Broadcast | 802.11 | 90 | Beacon frame, SN=3492, FH=0, Flags=pm..M... |
| 1521 | 43.208573 | LinksysG_67:22:19 | Broadcast | 802.11 | 90 | Beacon frame, SN=3493, FH=0, Flags=....., BI=770, SSID=Linksys12 |
| 1540 | 43.917194 | LinksysG_67:22:19 | ff:ff:ff:ff:ff:ff | 802.11 | 90 | Beacon frame, SN=3500, FH=0, Flags=....., BI=100, SSID=Linksys12 |
| 1545 | 44.310450 | d3:95:ca:bb:f0:15 | 3e:d3:27:e6:65:7f | 802.11 | 1624 | Beacon frame, SN=54, FH=11, Flags=papPMPPT. |
| 1550 | 44.633946 | 00:16:b6:f7:22:19 | Broadcast | 802.11 | 90 | Beacon frame, SN=3507, FH=0, Flags=....., BI=100, SSID=Linksys12 |
| 1557 | 44.887707 | Cisco-L1_f5:ba:1b | Broadcast | 802.11 | 132 | Beacon frame, SN=3663, FH=13, Flags=....., BI=8, SSID=Linksys_SES_24886 |
| 1895 | 56.182695 | 00:16:b6:f7:22:19 | Sa:15:ff:ff:ff:ff | 802.11 | 90 | Beacon frame, SN=3620, FH=4, Flags=....., BI=100, SSID=Linksys_SES_24886 |
| 1981 | 59.325865 | Cisco-L1_f5:ba:1b | Broadcast | 802.11 | 132 | Beacon frame, SN=3833, FH=0, Flags=....., BI=100, SSID=Linksys_SES_24886 |
| 2296 | 69.667955 | Cisco-L1_f5:ba:1b | Broadcast | 802.11 | 132 | Beacon frame, SN=3940, FH=0, Flags=....., BI=100, SSID=Linksys_SES_24886 |
| 2310 | 70.336947 | LinksysG_67:22:19 | Broadcast | 802.11 | 90 | Beacon frame, SN=3760, FH=0, Flags=....., BI=2304 |
| 2342 | 72.282076 | LinksysG_67:22:19 | ff:26:ff:ff:ff:ff | 802.11 | 90 | Beacon frame, SN=3779, FH=0, Flags=....., BI=100, SSID=Linksys12 |

Figura 15: Análise do tráfego Wireshark com filtros

Questão 12

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

- Receiver address: 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



```
► Frame 1405: 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
  1101 0111 1000 .... = Sequence number: 3448
  Frame check sequence: 0xd1b97e79 [unverified]
  [FCS Status: Unverified]
► IEEE 802.11 wireless LAN
```

Figura 17: Análise da trama - Endereços MAC

Questão 13

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

Para visualizar todas as tramas *probing request* e *probing response* foram utilizados os filtros “wlan.fc.type_subtype==4” e “wlan.fc.type_subtype==5”, respetivamente.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|-------------------|-------------------|----------|--------|--|
| 27 | 1.221285 | Cisco-Li_f7:1d:51 | IntelCor_f1:57:13 | 802.11 | 177 | Probe Request, Src=2867, Prio=0, Flags=.....C, BSS=100, SSID=30 Munroe St |
| 50 | 2.287613 | IntelCor_f1:57:13 | Broadcast | 802.11 | 79 | Probe Response, Src=576, Prio=0, Flags=.....C, SSID=Home WiFi |
| 51 | 2.288097 | Cisco-Li_f7:1d:51 | IntelCor_f1:57:13 | 802.11 | 177 | Probe Response, Src=2878, Prio=0, Flags=.....C, BSS=100, SSID=30 Munroe St |
| 52 | 2.282191 | Cisco-Li_f7:1d:51 | IntelCor_f1:57:13 | 802.11 | 177 | Probe Response, Src=2878, Prio=0, Flags=.....C, BSS=100, SSID=30 Munroe St |
| 53 | 2.384063 | Cisco-Li_f7:1d:51 | IntelCor_f1:57:13 | 802.11 | 177 | Probe Response, Src=2878, Prio=0, Flags=.....C, BSS=100, SSID=30 Munroe St |
| 54 | 2.385562 | Cisco-Li_f7:1d:51 | IntelCor_f1:57:13 | 802.11 | 177 | Probe Response, Src=2878, Prio=0, Flags=.....C, BSS=100, SSID=30 Munroe St |
| 55 | 2.385563 | Cisco-Li_f7:1d:51 | IntelCor_f1:57:13 | 802.11 | 177 | Probe Response, Src=2878, Prio=0, Flags=.....C, BSS=100, SSID=30 Munroe St |
| 56 | 2.318072 | Cisco-Li_f7:1d:51 | IntelCor_f1:57:13 | 802.11 | 177 | Probe Response, Src=2878, Prio=0, Flags=.....C, BSS=100, SSID=30 Munroe St |
| 59 | 2.453961 | Cisco-Li_f7:1d:51 | IntelCor_f1:57:13 | 802.11 | 177 | Probe Response, Src=2881, Prio=0, Flags=.....C, BSS=100, SSID=30 Munroe St |
| 63 | 4.293335 | Cisco-Li_f7:1d:51 | IntelCor_f1:57:13 | 802.11 | 177 | Probe Response, Src=2900, Prio=0, Flags=.....C, BSS=100, SSID=30 Munroe St |
| 67 | 4.298449 | IntelCor_f1:57:13 | Broadcast | 802.11 | 78 | Probe Request, Src=580, Prio=0, Flags=.....C, SSID=phiphap |
| 80 | 4.301564 | Cisco-Li_f7:1d:51 | IntelCor_f1:57:13 | 802.11 | 177 | Probe Response, Src=2901, Prio=0, Flags=.....C, BSS=100, SSID=30 Munroe St |
| 89 | 4.383314 | Cisco-Li_f7:1d:51 | IntelCor_f1:57:13 | 802.11 | 177 | Probe Response, Src=2901, Prio=0, Flags=.....C, BSS=100, SSID=30 Munroe St |
| 90 | 4.384014 | Cisco-Li_f7:1d:51 | IntelCor_f1:57:13 | 802.11 | 177 | Probe Response, Src=2901, Prio=0, Flags=.....C, BSS=100, SSID=30 Munroe St |
| 93 | 4.403454 | Cisco-Li_f7:1d:51 | IntelCor_f1:57:13 | 802.11 | 177 | Probe Response, Src=2903, Prio=0, Flags=.....C, BSS=100, SSID=30 Munroe St |
| 94 | 4.484939 | Cisco-Li_f7:1d:51 | IntelCor_f1:57:13 | 802.11 | 177 | Probe Response, Src=2903, Prio=0, Flags=.....C, BSS=100, SSID=30 Munroe St |
| 117 | 6.299785 | IntelCor_f1:57:13 | Broadcast | 802.11 | 79 | Probe Request, Src=621, Prio=0, Flags=.....C, SSID=McLard (Broadcast) |
| 118 | 6.380439 | IntelCor_f1:57:13 | Broadcast | 802.11 | 78 | Probe Request, Src=621, Prio=0, Flags=.....C, SSID=McLard (Broadcast) |
| 119 | 6.383313 | Cisco-Li_f7:1d:51 | IntelCor_f1:57:13 | 802.11 | 177 | Probe Response, Src=2922, Prio=0, Flags=.....C, BSS=100, SSID=30 Munroe St |
| 130 | 6.484446 | Cisco-Li_f7:1d:51 | IntelCor_f1:57:13 | 802.11 | 177 | Probe Response, Src=2924, Prio=0, Flags=.....C, BSS=100, SSID=30 Munroe St |
| 131 | 6.485038 | Cisco-Li_f7:1d:51 | IntelCor_f1:57:13 | 802.11 | 177 | Probe Response, Src=2924, Prio=0, Flags=.....C, BSS=100, SSID=30 Munroe St |
| 132 | 6.487562 | Cisco-Li_f7:1d:51 | IntelCor_f1:57:13 | 802.11 | 177 | Probe Response, Src=2924, Prio=0, Flags=.....C, BSS=100, SSID=30 Munroe St |
| 133 | 6.489063 | Cisco-Li_f7:1d:51 | IntelCor_f1:57:13 | 802.11 | 177 | Probe Response, Src=2924, Prio=0, Flags=.....C, BSS=100, SSID=30 Munroe St |
| 134 | 6.419562 | Cisco-Li_f7:1d:51 | IntelCor_f1:57:13 | 802.11 | 177 | Probe Response, Src=2924, Prio=0, Flags=.....C, BSS=100, SSID=30 Munroe St |
| 135 | 6.412063 | Cisco-Li_f7:1d:51 | IntelCor_f1:57:13 | 802.11 | 177 | Probe Response, Src=2924, Prio=0, Flags=.....C, BSS=100, SSID=30 Munroe St |
| 136 | 6.413562 | Cisco-Li_f7:1d:51 | IntelCor_f1:57:13 | 802.11 | 177 | Probe Response, Src=2924, Prio=0, Flags=.....C, BSS=100, SSID=30 Munroe St |
| 138 | 6.455573 | Cisco-Li_f7:1d:51 | IntelCor_f1:57:13 | 802.11 | 177 | Probe Response, Src=2926, Prio=0, Flags=.....C, BSS=100, SSID=30 Munroe St |
| 139 | 6.457064 | Cisco-Li_f7:1d:51 | IntelCor_f1:57:13 | 802.11 | 177 | Probe Response, Src=2926, Prio=0, Flags=.....C, BSS=100, SSID=30 Munroe St |
| 140 | 6.458887 | Cisco-Li_f7:1d:51 | IntelCor_f1:57:13 | 802.11 | 177 | Probe Response, Src=2926, Prio=0, Flags=.....C, BSS=100, SSID=30 Munroe St |
| 141 | 6.460863 | Cisco-Li_f7:1d:51 | IntelCor_f1:57:13 | 802.11 | 177 | Probe Response, Src=2926, Prio=0, Flags=.....C, BSS=100, SSID=30 Munroe St |
| 142 | 6.461563 | Cisco-Li_f7:1d:51 | IntelCor_f1:57:13 | 802.11 | 177 | Probe Response, Src=2926, Prio=0, Flags=.....C, BSS=100, SSID=30 Munroe St |
| 143 | 6.463062 | Cisco-Li_f7:1d:51 | IntelCor_f1:57:13 | 802.11 | 177 | Probe Response, Src=2926, Prio=0, Flags=.....C, BSS=100, SSID=30 Munroe St |

Figura 18: Análise do tráfego Wireshark com filtros

Questão 14

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

BSS Id Destino: ff:ff:ff:ff:ff:ff

BSS Id Origem: 00:16:b6:f7:1d:51

Um *host* envia um *probe request* quando pretende encontrar um AP (*Access Point*), por sua vez, o AP envia uma resposta denominada de *probe response*.



```
▶ Frame 50: 79 bytes on wire (632 bits), 79 bytes captured (632 bits)
▶ Radiotap Header v0, Length 24
▶ 802.11 radio information
▼ IEEE 802.11 Probe Request, Flags: .....C
  Type/Subtype: Probe Request (0x0004)
  ▶ Frame Control Field: 0x4000
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Transmitter address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
    Source address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
    BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
    .... 0000 = Fragment number: 0
    0010 0100 0000 .... = Sequence number: 576
    Frame check sequence: 0xa373c5ff [unverified]
    [FCS Status: Unverified]
▶ IEEE 802.11 wireless LAN
```

Figura 19: Análise da trama - BSS Id Destino

```
▶ Frame 51: 177 bytes on wire (1416 bits), 177 bytes captured (1416 bits)
▶ Radiotap Header v0, Length 24
▶ 802.11 radio information
▼ IEEE 802.11 Probe Response, Flags: .....C
  Type/Subtype: Probe Response (0x0005)
  ▶ Frame Control Field: 0x5000
    .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 0011 1110 .... = Sequence number: 2878
    Frame check sequence: 0x6ed851bb [unverified]
    [FCS Status: Unverified]
▶ IEEE 802.11 wireless LAN
```

Figura 20: Análise da trama - BSS Id Origem

Questão 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?

Um exemplo de um *probing request* encontra-se na trama 50 (figura 19), esta trama é enviada do *host* para *broadcast* com o intuito de localizar um AP (*Access Point*). O *probing response* correspondente ao *probing request* enviado, encontra-se na trama 51 (figura 20). Esta mensagem é enviada pelo AP para o *host*, indicando que se encontra disponível para conexão.

1.3 Processo de Associação

Questão 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?

As duas tramas enviadas pelo host no trace imediatamente após $t = 49$ s para terminar a associação com o AP 30 Munroe St são as tramas nº 1733 e 1735. Seria de esperar que tivesse sido enviada uma trama de *Disassociation request*.



| No. | Time | Source | Destination | Protocol | Length | Info |
|------|-----------|-------------------|-------------------|----------|--------|--|
| 1716 | 49.821047 | IntelCor_d1:b6:4f | IntelCor_d1:b6:4f | 802.11 | 38 | Acknowledgement, Flags=.....C |
| 1717 | 49.830423 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 163 | Beacon Frame, SN=3583, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St |
| 1718 | 49.132768 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 163 | Beacon Frame, SN=3584, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St |
| 1719 | 49.132884 | IntelCor_d1:b6:4f | Cisco-Li_f7:1d:51 | 802.11 | 54 | QoS Null function (No data), SN=1600, FN=0, Flags=...P...TC |
| 1720 | 49.132981 | IntelCor_d1:b6:4f | IntelCor_d1:b6:4f | 802.11 | 38 | Acknowledgement, Flags=.....C |
| 1721 | 49.224975 | IntelCor_d1:b6:4f | Cisco-Li_f7:1d:51 | 802.11 | 54 | QoS Null function (No data), SN=1601, FN=0, Flags=...P...TC |
| 1722 | 49.225104 | IntelCor_d1:b6:4f | IntelCor_d1:b6:4f | 802.11 | 38 | Acknowledgement, Flags=.....C |
| 1723 | 49.235239 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 163 | Beacon Frame, SN=3585, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St |
| 1724 | 49.235340 | IntelCor_d1:b6:4f | Cisco-Li_f7:1d:51 | 802.11 | 54 | QoS Null function (No data), SN=1602, FN=0, Flags=...P...TC |
| 1725 | 49.235439 | IntelCor_d1:b6:4f | IntelCor_d1:b6:4f | 802.11 | 38 | Acknowledgement, Flags=.....C |
| 1726 | 49.337573 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 163 | Beacon Frame, SN=3586, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St |
| 1727 | 49.420949 | IntelCor_d1:b6:4f | Cisco-Li_f7:1d:51 | 802.11 | 54 | QoS Null function (No data), SN=1603, FN=0, Flags=...P...TC |
| 1728 | 49.430807 | IntelCor_d1:b6:4f | IntelCor_d1:b6:4f | 802.11 | 38 | Acknowledgement, Flags=.....C |
| 1729 | 49.440041 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 163 | 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=1604, FN=0, Flags=...P...TC |
| 1731 | 49.440243 | IntelCor_d1:b6:4f | IntelCor_d1:b6:4f | 802.11 | 38 | Acknowledgement, Flags=.....C |
| 1732 | 49.542481 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 163 | Beacon Frame, SN=3588, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St |
| 1733 | 49.583015 | 192.168.1.109 | 192.168.1.1 | 602P | 390 | SNMP Release - Transaction ID 0xead536 |
| 1734 | 49.583771 | IntelCor_d1:b6:4f | IntelCor_d1:b6:4f | 802.11 | 38 | Acknowledgement, Flags=.....C |
| 1735 | 49.608917 | IntelCor_d1:b6:4f | Cisco-Li_f7:1d:51 | 802.11 | 54 | Beautification, SN=1605, FN=0, Flags=.....C |
| 1736 | 49.609770 | IntelCor_d1:b6:4f | 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 | 49.615809 | IntelCor_d1:b6:4f | Cisco-Li_f5:ba:bb | 802.11 | 38 | Acknowledgement, Flags=.....C |
| 1739 | 49.617713 | IntelCor_d1:b6:4f | Cisco-Li_f5:ba:bb | 802.11 | 38 | Acknowledgement, Flags=.....C |
| 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 |
| 1743 | 49.642315 | 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 |
| 1745 | 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 |
| 1747 | 49.647711 | IntelCor_d1:b6:4f | Cisco-Li_f5:ba:bb | 802.11 | 38 | Acknowledgement, Flags=.....C |
| 1748 | 49.647827 | IntelCor_d1:b6:4f | Cisco-Li_f5:ba:bb | 802.11 | 38 | Acknowledgement, Flags=.....C |
| 1749 | 49.649705 | IntelCor_d1:b6:4f | Cisco-Li_f5:ba:bb | 802.11 | 58 | Authentication, SN=1606, FN=0, Flags=.....R...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 | 49.652318 | 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 |
| 1752 | 49.662857 | IntelCor_d1:b6:4f | Cisco-Li_f5:ba:bb | 802.11 | 38 | Acknowledgement, Flags=.....C |
| 1753 | 49.663950 | IntelCor_d1:b6:4f | Cisco-Li_f5:ba:bb | 802.11 | 38 | Acknowledgement, Flags=.....C |
| 1754 | 49.665704 | IntelCor_d1:b6:4f | Cisco-Li_f5:ba:bb | 802.11 | 38 | Acknowledgement, Flags=.....C |

Figura 21: Análise do tráfego wireshark

Questão 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?

Através do filtro: “wlan.fc.type_subtype==Authentication” obtiveram-se as tramas de authentication.

Num intervalo de 1s após t = 49s, foram enviadas 6 mensagens de authentication do host para o AP linksys_ses_24086.

| 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 |
| 1743 | 49.642315 | 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 |
| 1745 | 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 |
| 1747 | 49.647711 | IntelCor_d1:b6:4f | Cisco-Li_f5:ba:bb | 802.11 | 38 | Acknowledgement, Flags=.....C |
| 1748 | 49.647827 | IntelCor_d1:b6:4f | Cisco-Li_f5:ba:bb | 802.11 | 38 | Acknowledgement, Flags=.....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 | 57.898325 | 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 22: Análise do tráfego wireshark com filtro



Questão 18

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

O tipo de autenticação pretendida pelo host é aberta.

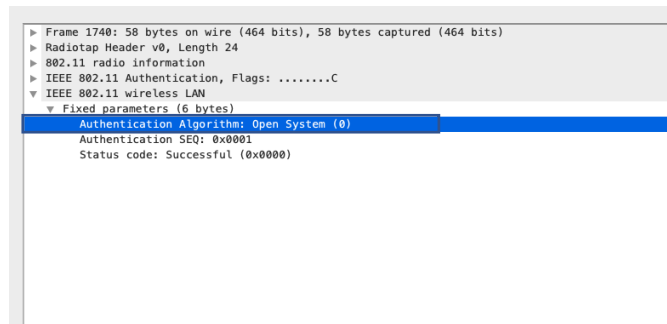


Figura 23: Análise de trama - Campo Authentication Algorithm

Questão 19

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

Não são observadas respostas de *authentication* do AP no trace, como é possível verificar na figura 24.

| 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... |
| 1742 | 49.640702 | IntelCor_d1:b6:4f | Cisco-Li_f5:ba:bb | 802.11 | 58 | Authentication, SN=1606, FN=0, Flags=.....R... |
| 1744 | 49.642315 | IntelCor_d1:b6:4f | Cisco-Li_f5:ba:bb | 802.11 | 58 | Authentication, SN=1606, FN=0, Flags=.....R... |
| 1746 | 49.645319 | IntelCor_d1:b6:4f | Cisco-Li_f5:ba:bb | 802.11 | 58 | Authentication, SN=1606, FN=0, Flags=.....R... |
| 1749 | 49.649705 | IntelCor_d1:b6:4f | Cisco-Li_f5:ba:bb | 802.11 | 58 | Authentication, SN=1606, FN=0, Flags=.....R... |
| 1821 | 53.785833 | IntelCor_d1:b6:4f | Cisco-Li_f5:ba:bb | 802.11 | 58 | Authentication, SN=1612, FN=0, Flags=.....R... |
| 1822 | 53.787070 | IntelCor_d1:b6:4f | Cisco-Li_f5:ba:bb | 802.11 | 58 | Authentication, SN=1612, FN=0, Flags=.....R... |
| 1921 | 57.889232 | IntelCor_d1:b6:4f | Cisco-Li_f5:ba:bb | 802.11 | 58 | Authentication, SN=1619, FN=0, Flags=.....R... |
| 1922 | 57.890325 | IntelCor_d1:b6:4f | Cisco-Li_f5:ba:bb | 802.11 | 58 | Authentication, SN=1619, FN=0, Flags=.....R... |
| 1923 | 57.891321 | IntelCor_d1:b6:4f | Cisco-Li_f5:ba:bb | 802.11 | 58 | Authentication, SN=1619, FN=0, Flags=.....R... |
| 1924 | 57.896970 | IntelCor_d1:b6:4f | Cisco-Li_f5:ba:bb | 802.11 | 58 | Authentication, SN=1619, FN=0, Flags=.....R... |
| 2122 | 62.171951 | IntelCor_d1:b6:4f | Cisco-Li_f5:ba:bb | 802.11 | 58 | Authentication, SN=1644, FN=0, Flags=.....R... |
| 2123 | 62.172946 | IntelCor_d1:b6:4f | Cisco-Li_f5:ba:bb | 802.11 | 58 | Authentication, SN=1644, FN=0, Flags=.....R... |
| 2124 | 62.174070 | IntelCor_d1:b6:4f | Cisco-Li_f5:ba:bb | 802.11 | 58 | Authentication, SN=1644, FN=0, Flags=.....R... |
| 2156 | 63.160807 | IntelCor_d1:b6:4f | Cisco-Li_f7:1d:51 | 802.11 | 58 | Authentication, SN=1647, FN=0, Flags=.....R... |
| 2158 | 63.169071 | Cisco-Li_f7:1d:51 | IntelCor_d1:b6:4f | 802.11 | 58 | Authentication, SN=3726, FN=0, Flags=.....R... |
| 2160 | 63.169707 | IntelCor_d1:b6:4f | Cisco-Li_f7:1d:51 | 802.11 | 58 | Authentication, SN=1647, FN=0, Flags=.....R... |
| 2164 | 63.170692 | Cisco-Li_f7:1d:51 | IntelCor_d1:b6:4f | 802.11 | 58 | Authentication, SN=3727, FN=0, Flags=.....R... |

Figura 24: Análise do tráfego wireshark com filtros

Questão 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 uma trama authentication do host para o AP 30 Munroe St. E quando aparece a resposta authentication do AP para o host?

Em $t = 63.168087s$ é enviada uma trama de authentication pelo host para o AP 30 Munroe St. Em $t = 63.169071s$ é enviada uma trama de autenticação como resposta do AP para o host.

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|-----------|-------------------|-------------------|----------|--------|--|
| 1748 | 49.638857 | IntelCor_d1b6:4f | Cisco-L1_f5:ba:bb | 802.11 | 58 | Authentication, SN=1686, FmB, Flags=.....C |
| 1741 | 49.639708 | IntelCor_d1b6:4f | Cisco-L1_f5:ba:bb | 802.11 | 58 | Authentication, SN=1686, FmB, Flags=.....C |
| 1742 | 49.640792 | IntelCor_d1b6:4f | Cisco-L1_f5:ba:bb | 802.11 | 58 | Authentication, SN=1686, FmB, Flags=.....C |
| 1744 | 49.642315 | IntelCor_d1b6:4f | Cisco-L1_f5:ba:bb | 802.11 | 58 | Authentication, SN=1686, FmB, Flags=.....C |
| 1746 | 49.645319 | IntelCor_d1b6:4f | Cisco-L1_f5:ba:bb | 802.11 | 58 | Authentication, SN=1686, FmB, Flags=.....C |
| 1749 | 49.649795 | IntelCor_d1b6:4f | Cisco-L1_f5:ba:bb | 802.11 | 58 | Authentication, SN=1686, FmB, Flags=.....C |
| 1821 | 53.785033 | IntelCor_d1b6:4f | Cisco-L1_f5:ba:bb | 802.11 | 58 | Authentication, SN=1612, FmB, Flags=.....C |
| 1822 | 53.787978 | IntelCor_d1b6:4f | Cisco-L1_f5:ba:bb | 802.11 | 58 | Authentication, SN=1612, FmB, Flags=.....C |
| 1921 | 57.899232 | IntelCor_d1b6:4f | Cisco-L1_f5:ba:bb | 802.11 | 58 | Authentication, SN=1619, FmB, Flags=.....C |
| 1922 | 57.899325 | IntelCor_d1b6:4f | Cisco-L1_f5:ba:bb | 802.11 | 58 | Authentication, SN=1619, FmB, Flags=.....C |
| 1923 | 57.891321 | IntelCor_d1b6:4f | Cisco-L1_f5:ba:bb | 802.11 | 58 | Authentication, SN=1619, FmB, Flags=.....C |
| 1924 | 57.899378 | IntelCor_d1b6:4f | Cisco-L1_f5:ba:bb | 802.11 | 58 | Authentication, SN=1619, FmB, Flags=.....C |
| 2122 | 62.171951 | IntelCor_d1b6:4f | Cisco-L1_f5:ba:bb | 802.11 | 58 | Authentication, SN=1644, FmB, Flags=.....C |
| 2123 | 62.172946 | IntelCor_d1b6:4f | Cisco-L1_f5:ba:bb | 802.11 | 58 | Authentication, SN=1644, FmB, Flags=.....C |
| 2156 | 63.168087 | IntelCor_d1b6:4f | Cisco-L1_f7:1d:51 | 802.11 | 58 | Authentication, SN=1647, FmB, Flags=.....C |
| 2158 | 63.169071 | Cisco-L1_f7:1d:51 | IntelCor_d1b6:4f | 802.11 | 58 | Authentication, SN=3726, FmB, Flags=.....C |
| 2159 | 63.169797 | IntelCor_d1b6:4f | Cisco-L1_f7:1d:51 | 802.11 | 58 | Authentication, SN=3726, FmB, Flags=.....C |
| 2164 | 63.170692 | Cisco-L1_f7:1d:51 | IntelCor_d1b6:4f | 802.11 | 58 | Authentication, SN=3727, FmB, Flags=.....C |

Figura 25: Análise do tráfego wireshark com filtros

Questão 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?

Em $t = 63.169910s$ é enviado um *associate request* do host para o AP 30 Munroe ST. O correspondente *association reply* é enviado em $t = 63.192101s$.

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|-----------|-------------------|-------------------|----------|--|---|
| 2148 | 62.853735 | Cisco-L1_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon Frame, SN=3731, FmB, Flags=.....C, B1=108, SSID=30 Munroe St |
| 2141 | 62.856184 | Cisco-L1_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon Frame, SN=3722, FmB, Flags=.....C, B1=108, SSID=30 Munroe St |
| 2142 | 62.859233 | IntelCor_d1b6:4f | Cisco-L1_f5:ba:bb | 802.11 | 54 | Deauthentication, SN=1646, FmB, Flags=.....C |
| 2143 | 62.861834 | IntelCor_d1b6:4f | Cisco-L1_f5:ba:bb | 802.11 | 54 | Deauthentication, SN=1646, FmB, Flags=.....C |
| 2144 | 62.863454 | IntelCor_d1b6:4f | Cisco-L1_f5:ba:bb | 802.11 | 54 | Deauthentication, SN=1646, FmB, Flags=.....C |
| 2145 | 62.865342 | IntelCor_d1b6:4f | Cisco-L1_f5:ba:bb | 802.11 | 54 | Deauthentication, SN=1646, FmB, Flags=.....C |
| 2146 | 62.875964 | IntelCor_d1b6:4f | Cisco-L1_f5:ba:bb | 802.11 | 54 | Deauthentication, SN=1646, FmB, Flags=.....C |
| 2147 | 62.887488 | IntelCor_d1b6:4f | Cisco-L1_f5:ba:bb | 802.11 | 54 | Deauthentication, SN=1646, FmB, Flags=.....C |
| 2148 | 62.890971 | IntelCor_d1b6:4f | Cisco-L1_f5:ba:bb | 802.11 | 54 | Deauthentication, SN=1646, FmB, Flags=.....C |
| 2149 | 62.894985 | IntelCor_d1b6:4f | Cisco-L1_f5:ba:bb | 802.11 | 54 | Deauthentication, SN=1646, FmB, Flags=.....C |
| 2150 | 63.118231 | IntelCor_d1b6:4f | Cisco-L1_f5:ba:bb | 802.11 | 54 | Deauthentication, SN=1646, FmB, Flags=.....C |
| 2151 | 63.123362 | IntelCor_d1b6:4f | Broadcast | 802.11 | 94 | Probe Request, SN=1647, FmB, Flags=.....C, SSID=30 Munroe St |
| 2152 | 63.143451 | IntelCor_d1b6:4f | IntelCor_d1b6:4f | 802.11 | 177 | Probe Response, SN=3724, FmB, Flags=.....C, B1=108, SSID=30 Munroe St |
| 2153 | 63.142680 | Cisco-L1_f7:1d:51 | Broadcast | 802.11 | 38 | Acknowledgment, Flags=.....C |
| 2155 | 63.161272 | Cisco-L1_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon Frame, SN=3725, FmB, Flags=.....C, B1=108, SSID=30 Munroe St |
| 2156 | 63.168087 | IntelCor_d1b6:4f | Cisco-L1_f7:1d:51 | 802.11 | 58 | Authentication, SN=1647, FmB, Flags=.....C |
| 2157 | 63.168222 | IntelCor_d1b6:4f | IntelCor_d1b6:4f | 802.11 | 38 | Acknowledgment, Flags=.....C |
| 2158 | 63.169797 | Cisco-L1_f7:1d:51 | IntelCor_d1b6:4f | 802.11 | 58 | Authentication, SN=3726, FmB, Flags=.....C |
| 2159 | 63.169592 | Cisco-L1_f7:1d:51 | IntelCor_d1b6:4f | 802.11 | 38 | Acknowledgment, Flags=.....C |
| 2160 | 63.169797 | IntelCor_d1b6:4f | Cisco-L1_f7:1d:51 | 58 | Authentication, SN=1647, FmB, Flags=.....C | |
| 2161 | 63.169814 | IntelCor_d1b6:4f | IntelCor_d1b6:4f | 38 | Acknowledgment, Flags=.....C | |
| 2162 | 63.169910 | IntelCor_d1b6:4f | Cisco-L1_f7:1d:51 | 802.11 | 89 | Association Request, SN=1648, FmB, Flags=.....C, SSID=30 Munroe St |
| 2163 | 63.170880 | IntelCor_d1b6:4f | IntelCor_d1b6:4f | 38 | Acknowledgment, Flags=.....C | |
| 2164 | 63.170892 | Cisco-L1_f7:1d:51 | IntelCor_d1b6:4f | 802.11 | 58 | Authentication, SN=3727, FmB, Flags=.....C |
| 2165 | 63.171800 | Cisco-L1_f7:1d:51 | IntelCor_d1b6:4f | 38 | Acknowledgment, Flags=.....C | |
| 2166 | 63.192181 | IntelCor_d1b6:4f | IntelCor_d1b6:4f | 94 | Association Response, SN=3728, FmB, Flags=.....C | |
| 2167 | 63.192956 | Cisco-L1_f7:1d:51 | IntelCor_d1b6:4f | 38 | Acknowledgment, Flags=.....C | |
| 2168 | 63.194842 | 8.8.8.8 | 255.255.255.255 | DHCP | 398 | DHCP Discover - Transaction ID 8x181218a |
| 2169 | 63.194971 | IntelCor_d1b6:4f | IntelCor_d1b6:4f | 38 | Acknowledgment, Flags=.....C | |
| 2170 | 63.201481 | 8.8.8.8 | 255.255.255.255 | DHCP | 398 | DHCP Discover - Transaction ID 8x273347c |
| 2171 | 63.201639 | 8.8.8.8 | 255.255.255.255 | DHCP | 398 | DHCP Discover - Transaction ID 8x273347c |
| 2172 | 63.201736 | IntelCor_d1b6:4f | IntelCor_d1b6:4f | 38 | Acknowledgment, Flags=.....C | |
| 2173 | 63.203517 | Cisco-L1_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon Frame, SN=3729, FmB, Flags=.....C, B1=108, SSID=30 Munroe St |
| 2174 | 63.203651 | Cisco-L1_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon Frame, SN=3730, FmB, Flags=.....C, B1=108, SSID=30 Munroe St |
| 2175 | 63.468265 | Cisco-L1_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon Frame, SN=3731, FmB, Flags=.....C, B1=108, SSID=30 Munroe St |
| 2176 | 63.578627 | Cisco-L1_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon Frame, SN=3732, FmB, Flags=.....C, B1=108, SSID=30 Munroe St |

Figura 26: Análise do tráfego wireshark



Questão 22

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

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, [Mbit/sec].

As taxas de transmissão que o AP está disposto a usar, tal como verificado através da figura 28, são as mesmas que as do host.

```
▶ Frame 2162: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on 0
▶ 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)
    ▶ Capabilities Information: 0xc001
    Listen Interval: 0x000a
  ▼ 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 27: Análise da trama - Campos Supported Rates & Extended Supported Rates

```
▶ Frame 2166: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on 0
▶ 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)
    ▶ Capabilities Information: 0x0601
    Status code: Successful (0x0000)
    ..00 0000 0000 0101 = Association ID: 0x0005
  ▼ 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 28: Análise da trama - Campos Supported Rates & Extended Supported Rates

Questão 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.

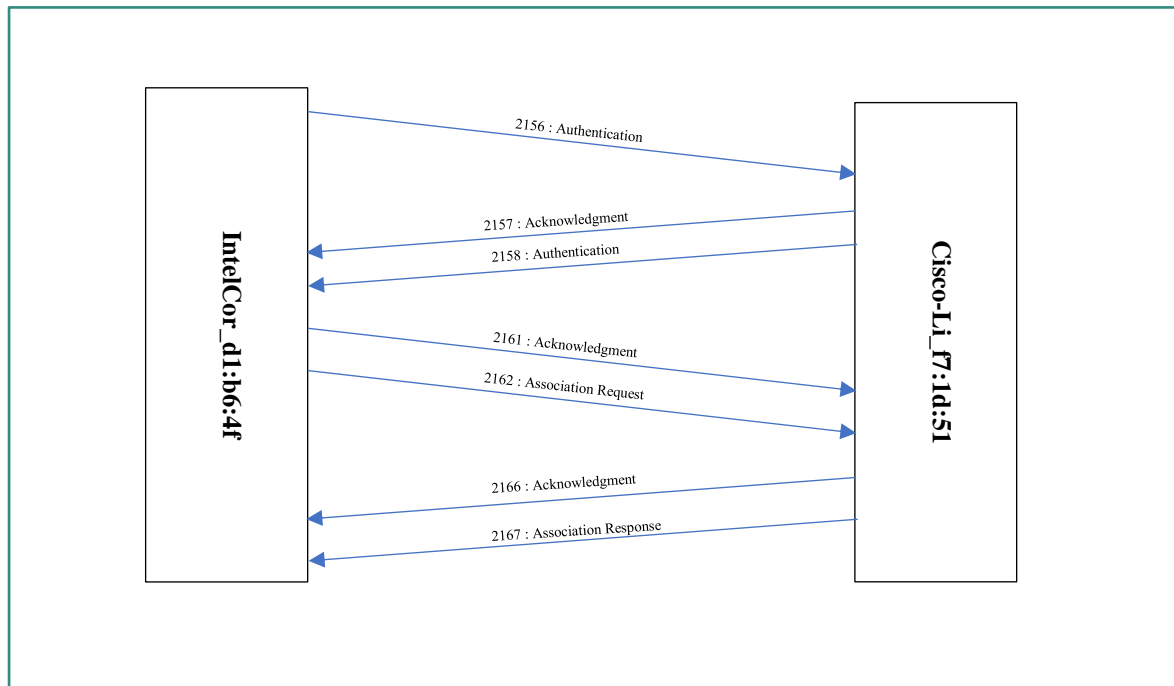
A sequência de tramas correspondentes a um processo de associação completo entre STA e o AP encontra-se identificada na figura 29.

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|-----------|-------------------|-------------------|----------|--------|--|
| 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 | IntelCor_d1:b6:4f | 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=.....C |
| 2161 | 63.169814 | IntelCor_d1:b6:4f | 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 | 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 | 63.171080 | 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 | Cisco-Li_f7:1d:51 | IntelCor_d1:b6:4f | 802.11 | 38 | Acknowledgement, Flags=.....C |
| 2168 | 63.194842 | 0.0.0.0 | 255.255.255.255 | DHCP | 390 | DHCP Discover - Transaction ID 0x1016219a |
| 2169 | 63.194971 | IntelCor_d1:b6:4f | IntelCor_d1:b6:4f | 802.11 | 38 | Acknowledgement, Flags=.....C |
| 2170 | 63.201481 | 0.0.0.0 | 255.255.255.255 | DHCP | 390 | DHCP Discover - Transaction ID 0x2733a47c |
| 2171 | 63.201639 | 0.0.0.0 | 255.255.255.255 | DHCP | 390 | DHCP Discover - Transaction ID 0x2733a47c |
| 2172 | 63.201736 | IntelCor_d1:b6:4f | IntelCor_d1:b6:4f | 802.11 | 38 | Acknowledgement, Flags=.....C |
| 2173 | 63.263517 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=3729, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St |
| 2174 | 63.365851 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=3730, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St |
| 2175 | 63.468265 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=3731, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St |
| 2176 | 63.570627 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=3732, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St |
| 2177 | 63.673065 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=3733, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St |
| 2178 | 63.689723 | Cisco-Li_f7:1d:51 | IntelCor_d1:b6:4f | 802.11 | 177 | Probe Response, SN=3734, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St |
| 2179 | 63.689894 | Cisco-Li_f7:1d:51 | IntelCor_d1:b6:4f | 802.11 | 38 | Acknowledgement, Flags=.....C |
| 2180 | 63.775453 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=3735, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St |
| 2181 | 63.877863 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=3736, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St |
| 2182 | 63.980220 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=3737, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St |
| 2183 | 64.082736 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=3738, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St |
| 2184 | 64.184955 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=3739, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St |

Figura 29: Análise do tráfego wireshark

Questão 24

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



1.4 Transferência de Dados

Questão 25

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

Os três campos dos endereços MAC na trama 802.11 são:

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



Universidade do Minho
Mestrado Integrado em Engenharia Informática

| 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 | 192.168.1.109 | 128.119.245.12 | TCP | 110 | 80 → 2538 [ACK] Seq=0 Ack=1 Win=5840 Len=0 SACK_PERM=1 |
| 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 | 128.119.245.12 | 192.168.1.109 | TCP | 110 | 80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0 |
| 478 | 24.828024 | 192.168.1.109 | 128.119.245.12 | TCP | 110 | 2538 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0 |
| 479 | 24.828140 | 128.119.245.12 | 192.168.1.109 | TCP | 110 | 2538 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0 |
| 480 | 24.828253 | 192.168.1.109 | 128.119.245.12 | HTTP | 537 | GET /wireshark-labs/alice.txt HTTP/1.1 |
| 481 | 24.828352 | 128.119.245.12 | 192.168.1.109 | HTTP | 400 | HTTP/1.1 200 OK (text/plain) |
| 482 | 24.846898 | 128.119.245.12 | 192.168.1.109 | TCP | 110 | 80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0 |
| 483 | 24.847058 | 128.119.245.12 | 192.168.1.109 | TCP | 110 | 80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0 |
| 484 | 24.847171 | 128.119.245.12 | 192.168.1.109 | TCP | 110 | [TCP Dup ACK 482#1] 80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0 |
| 485 | 24.847267 | 128.119.245.12 | 192.168.1.109 | TCP | 110 | 80 → 2538 [PSH, ACK] Seq=1 Ack=436 Win=6432 Len=313 [TCP segment of a reassembled data stream] |
| 486 | 24.848829 | 128.119.245.12 | 192.168.1.109 | TCP | 415 | 80 → 2538 [PSH, ACK] Seq=1 Ack=436 Win=6432 Len=313 [TCP segment of a reassembled data stream] |

Figura 30: Tráfego wireshark com filtro syn == 1

| Frame 474: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface 0 |
|---|
| RadioTap Header v0, Length 24 |
| 802.11 radio information |
| IEEE 802.11 QoS Data, Flags:TC |
| Type/Subtype: QoS Data (0x0028) |
| Frame Control field: 0x0001 |
| Type: 0000 0000 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_f1:b6:a8 (00:16:b6:f1:b6: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: 0xad57fceb (unverified) |
| [FC Status: Unverified] |
| QoS Control: 0x0000 |
| Logical-Link Control |
| Internet Protocol Version 4, Src: 192.168.1.109, Dst: 128.119.245.12 |

Figura 31: Análise da trama - endereços MAC

Questão 26

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

O endereço MAC que corresponde ao *host* é 00:13:02:d1:b6:4f, o do AP é 00:16:b6:f4:eb:a8. Já o do router do primeiro salto é 00:16:b6:f7:1d:51. Tudo isto, encontra-se visível na figura 31.

O endereço IP do host que está a enviar este segmento TCP é 192.168.1.109, o endereço IP de destino é 128.119.245.12, como está apresentado na figura 32.

| 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 | 192.168.1.109 | 128.119.245.12 | TCP | 110 | 80 → 2538 [ACK] Seq=0 Ack=1 Win=5840 Len=0 SACK_PERM=1 |
| 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 | 128.119.245.12 | 192.168.1.109 | TCP | 110 | 80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0 |
| 478 | 24.828024 | 192.168.1.109 | 128.119.245.12 | TCP | 110 | 2538 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0 |
| 479 | 24.828140 | 128.119.245.12 | 192.168.1.109 | TCP | 110 | 2538 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0 |
| 480 | 24.828253 | 192.168.1.109 | 128.119.245.12 | HTTP | 537 | GET /wireshark-labs/alice.txt HTTP/1.1 |
| 481 | 24.828352 | 128.119.245.12 | 192.168.1.109 | HTTP | 400 | HTTP/1.1 200 OK (text/plain) |
| 482 | 24.846898 | 128.119.245.12 | 192.168.1.109 | TCP | 110 | 80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0 |
| 483 | 24.847058 | 128.119.245.12 | 192.168.1.109 | TCP | 110 | 80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0 |
| 484 | 24.847171 | 128.119.245.12 | 192.168.1.109 | TCP | 110 | [TCP Dup ACK 482#1] 80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0 |
| 485 | 24.847267 | 128.119.245.12 | 192.168.1.109 | TCP | 110 | 80 → 2538 [PSH, ACK] Seq=1 Ack=436 Win=6432 Len=313 [TCP segment of a reassembled data stream] |
| 486 | 24.848829 | 128.119.245.12 | 192.168.1.109 | TCP | 415 | 80 → 2538 [PSH, ACK] Seq=1 Ack=436 Win=6432 Len=313 [TCP segment of a reassembled data stream] |

Figura 32: Captura do tráfego WireShark

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

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?

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



Figura 34: Análise do tráfego WireShark



Questão 29

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

O endereço MAC nesta trama que corresponde ao host é 91:2a:b0:49:b6:4f, o do AP é 00:16:b6:f7:1d:4f e o do router do primeiro salto é 00:16:b6:f7:1d:51. Tudo isto, encontra-se apresentado figura 33.

Questão 30

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

Não, uma vez que o endereço IP é o endereço de origem que envia a trama com o segmento SYNACK (que se encontra fora da rede local e que corresponde à camada 3). Quando a mensagem chega ao AP da rede local é desencapsulada e é atribuído ao endereço de origem o endereço MAC do AP, visto que ocorre a transição para a camada 2, logo o endereço MAC de origem será o endereço MAC do AP.



2. Conclusões

Este trabalho tem como principal objetivo explorar vários aspetos do protocolo IEEE 802.11.

Com o intuito da exploração destes conceitos foi fornecida uma captura WireShark, na qual foram analisadas, numa primeira fase, as sequências de bytes capturadas (incluídas no nível físico – *radio information*), como também bytes relativos a tramas 802.11.

Seguidamente, analisou-se o *scanning* passivo em redes Wi-Fi, através das capturas de tramas *beacon*, onde foram ainda observados endereços MAC de origem e destino destas tramas, os intervalos de tempo entre a transmissão deste tipo de tramas (*Beacon Interval*) e a deteção de erros CRC. Já quanto ao *scanning* ativo foram examinadas tramas *probing request* e *probing response*.

Posteriormente, tendo consciência que numa rede Wi-Fi estruturada um *host* deve associar-se a um ponto de acesso (AP) antes de enviar dados, foi averiguado o processo de associação completo entre um *host* e um AP, este processo só é possível se forem enviadas tramas de associação após o envio de tramas de autenticação.

Relativamente à transferência de dados foram verificados os segmentos SYN TCP e SYNACK para as respetivas sessões TCP, analisou-se especificamente uma permuta realizada entre hosts e APs de diferentes redes.

Por fim, este trabalho tornou-se bastante revelador de conceitos apreendidos à priori, bem como a aprendizagem de novos conteúdos relativos ao protocolo IEEE 802.11.