

Universidade do Minho

MESTRADO INTEGRADO EM ENGENHARIA INFORMÁTICA

17/12/2019

Redes de Computadores

TP4:Redes Sem Fios (802.11)

PL4 Grupo 9:

António Gonçalves (A85516)

João Araújo (A84306)

João Silva (A81761)

Contents

1	Acesso rádio	2
2	Scanning	3
3	Processo de associação	9
4	Transferência de dados	12
5	Conclusão	14

1 Acesso rádio

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

```
1409 37.459808 Cisco-Li_f7:1d:51
> Frame 1409: 183 bytes on wire (1464 bi
> Radiotap Header v0, Length 24
v 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): 70dB
  Signal strength (dBm): -30dBm
  Noise level (dBm): -100dBm
  Signal/noise ratio (dB): 70dB
> [Duration: 1464µs]
```

Figure 1: Informações sobre a rede sem fios.

Como podemos observar na figura anterior, a rede está a operar numa frequência de 2437 MHz, que corresponde ao canal 6.

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

Está a ser utilizada a norma 802.11b.

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

Esta trama tem um débito de 1 Mb/s. Uma vez que se trata da norma 802.11b, o seu débito máximo é de 11 Mb/s.

2 Scanning

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

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

5- Qual o intervalo de tempo entre a transmissão de tramas beacon para o AP linksys_ses_24086? E do AP 30 Munroe St? (Pista: o intervalo está contido na própria trama). Na prática, a periodicidade de tramas beacon é verificada? Tente explicar porquê.

```
14 0.499197 LinksysG_67:22:94 Broadcast 802.11 90 Beacon frame,
> Frame 14: 90 bytes on wire (720 bits), 90 bytes captured (720 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: 9534921933578
    Beacon Interval: 0.102400 [Seconds]
    > Capabilities Information: 0x0011
  > Tagged parameters (26 bytes)
```

Figure 2: Intervalo de tempo para o AP linksys12.

O intervalo de tempo entre transmissões para o AP linksys12 é de 0.1024 segundos.

```
14 0.499197 LinksysG_67:22:94 Broadcast 802.11 90 Beacon frame,
15 0.597382 Cisco-Li_f7:1d:51 Broadcast 802.11 183 Beacon frame,
16 0.601687 LinksysG_67:22:94 Broadcast 802.11 90 Beacon frame,
17 0.699847 Cisco-Li_f7:1d:51 Broadcast 802.11 183 Beacon frame,
> Frame 17: 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: 174319718786
    Beacon Interval: 0.102400 [Seconds]
    > Capabilities Information: 0x0011
  > Tagged parameters (119 bytes)
```

Figure 3: Intervalo de tempo para o AP 30 Munroe St.

Para o AP 30 Munroe St, o intervalo de tempo é igual. Podemos também observar que a periodicidade das tramas beacon não se verifica, uma vez que $0.601687 - 0.499197 = 0.10249$, que é um valor bastante próximo do esperado de 0.1024. Isto acontece porque o AP espera algum tempo para ter a certeza que não existem outros sistemas a tentar aceder ao meio, aumentando o intervalo entre as tramas.

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

```

17 0.699847 Cisco-Li_f7:1d:51 Broadcast 802.11 183 Beacon
> Frame 17: 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
  1011 0010 1101 .... = Sequence number: 2861
  Frame check sequence: 0x59715663 [unverified]
  [FCS Status: Unverified]
> IEEE 802.11 wireless LAN

```

Figure 4: Informações da trama beacon de 30 Munroe St.

O endereço de origem tem o valor de 00:16:b6:f7:1d:51.

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

O endereço de destino da trama é ff:ff:ff:ff:ff:ff.

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

O MAC BSS ID da trama é 00:16:b6:f7:1d:51.

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

```

▼ 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

```

Figure 5: Informações da trama beacon de 30 Munroe St.

-Data Rates: 1, 2, 5.5 e 11 Mb/s;

-Extended supported rates: 6, 9, 12, 18, 24, 36, 48 e 54 Mb/s.

10- Selecione uma trama beacon (e.g., a trama 1YXX com Y=turno e XX= grupo, e.g., 1101). Esta trama pertence a que tipo de tramas 802.11? Indique o valor dos seus identificadores de tipo e de subtipo. Em que parte concreta do cabeçalho da trama estão especificados (ver anexo)?

```

1409 37.459808 Cisco-Li_f7:1d:51 Broadcast
> Frame 1409: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits) on interface 0
> 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

```

Figure 6: Informações da trama beacon 1409.

Esta trama é uma trama de Management, tendo os valores de 00 (Beacon) para a flag Type e 1000 (Management) para a flag Subtype.

```

.... 00.. = Type: Management frame (0)
1000 .... = Subtype: 8
0010 64 00 00 46 52 15 67 04 80 00 00 00 ff ff ff ff d..FR.g:.....
0020 ff ff 00 16 b6 f7 1d 51 00 16 b6 f7 1d 51 c0 d7 .....Q.....Q..
0030 82 c1 74 98 28 00 00 00 64 00 01 06 00 0c 33 30 ..t-(...d.....30
0040 20 4d 75 6e 72 6f 65 20 53 74 01 04 82 84 8b 96 Munroe St.....
0050 03 01 06 05 04 00 01 00 00 07 06 55 53 49 01 0b .....USI...
Byte 24: Subtype (wlan.fc.subtype)

```

Figure 7: Bytes da trama.

Estes valores estão especificados no byte 25 da trama.

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

```

Frame check sequence: 0x38e38aab [unverified]
[FCS Status: Unverified]

```

Figure 8: Campo de erros.

Como podemos observar, não está verificado o campo Frame check sequence. No entanto, como desta vez estamos a utilizar uma rede sem fios, a probabilidade de ocorrência de colisões e erros nas tramas é muito superior, portanto seria importante utilizar um método que nos ajudaria a detetar este tipo de erros.

12- Identifique e registre todos os endereços MAC usados nas tramas beacon enviadas pelos APs. Recorde que o endereçamento está definido no cabeçalho das tramas 802.11 podendo ser utilizados até quatro endereços com diferente semântica. Para uma descrição detalhada da estrutura da trama 802.11, consulte o anexo ao enunciado.

Como podemos observar nas imagens abaixo, os endereços MAC usados nas tramas são o Receiver address, que é o endereço MAC de quem recebe a trama, o Destination address, o endereço a quem a trama se destina e o Transmitter address, que é o endereço de quem vai transmitir a trama.

13 0.495032	Cisco-Li_f7:1d:51	Broadcast	802.11
> Frame 13: 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 1011 0010 1011 = Sequence number: 2859 Frame check sequence: 0xbc03354d [unverified] [FCS Status: Unverified] > IEEE 802.11 wireless LAN			

Figure 9: MAC address do AP 30 Munroe ST.

14 0.499197	LinksysG_67:22:94	Broadcast	802.11
> Frame 14: 90 bytes on wire (720 bits), 90 bytes captured (720 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: LinksysG_67:22:94 (00:06:25:67:22:94) Source address: LinksysG_67:22:94 (00:06:25:67:22:94) BSS Id: 50:2b:25:67:22:94 (50:2b:25:67:22:94) 0000 = Fragment number: 0 1100 0000 0010 = Sequence number: 3074 Frame check sequence: 0x5d5654a6 [unverified] [FCS Status: Unverified] > IEEE 802.11 wireless LAN			

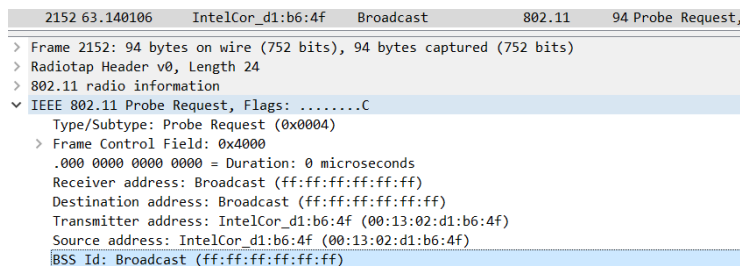
Figure 10: Mac address do AP linksys12.

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

O filtro utilizado para visualizar apenas as tramas probing request (subtype 4) e as probing response (subtype 5) é :

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

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

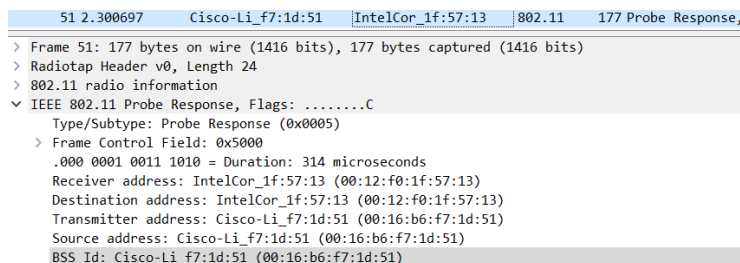


```

2152 63.140106 IntelCor_d1:b6:4f Broadcast 802.11 94 Probe Request,
> Frame 2152: 94 bytes on wire (752 bits), 94 bytes captured (752 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
v 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)

```

Figure 11: Endereço BSS Id da trama Probe Request.



```

51 2.300697 Cisco-Li_f7:1d:51 IntelCor_1f:57:13 802.11 177 Probe Response,
> Frame 51: 177 bytes on wire (1416 bits), 177 bytes captured (1416 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
v 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)

```

Figure 12: Endereço BSS Id da trama Probe Response.

Na trama de Probe Request, o BSS Id está em Broadcast (ff:ff:ff:ff:ff:ff) e na trama de Probe Response o BSS Id é o endereço do AP 30 Munroe St. As tramas Probe Request servem para perceber quais os AP que estão a operar, assim é enviada a trama em Broadcast. Por outro lado, as tramas Probe Response representam a resposta ao Request e já possui o MAC address que pretendemos alcançar.

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?

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

Figure 13: Probing Request e Probing Response correspondente.

```

171 8.299988 IntelCor_1f:57:13 Broadcast 802.11 77 Probe Request,
> 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)

```

Figure 14: Endereços do Probing Request.

```

173 8.303567 Cisco-Li_f7:1d:51 IntelCor_1f:57:13 802.11 177 Probe Response,
> Frame 173: 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)

```

Figure 15: Endereços do Probing Response.

O Probing Request é enviado em Broadcast, uma vez que irá ver quais as máquinas que estão acessíveis. O Probing Response terá como destino o AP que enviou o Request.

3 Processo de associação

16- Quais as duas ações realizadas (i.e., tramas enviadas) pelo host no trace imediatamente após t=49 para terminar a associação com o AP 30 Munroe St que estava ativa quando o trace teve início? (Pista: uma é na camada IP e outra na camada de ligação 802.11). Observando a especificação 802.11, seria de esperar outra trama, mas que não aparece?

1733	49.583615	192.168.1.109	192.168.1.1	DHCP	390 DHCP Release - Transaction ID 0xea5a526
1734	49.583771	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f ...	802.11	38 Acknowledgement, Flags=.....C
1735	49.609617	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54 Deauthentication, SN=1605, FN=0, Flags=.....C

Figure 16: Duas tramas após t=49.

Para ocorrer a desassociação seria de esperar que estivesse presente uma trama Desassociation.

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?

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

Figure 17: Mensagens de Authentication.

Foram enviadas 3 mensagens de authentication do host para linksys_ses_24086.

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

```
▼ Flags: 0x00
....0000 = DS status: Not leaving DS or network is o
....00.. = 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
```

Figure 18: Flags da mensagem de authentication.

Uma vez que a Protected flag se encontra a 0, a autenticação será aberta.

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

1741	49.639700	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1606, FN=0, Flags=....R...C
------	-----------	-------------------	-------------------	--------	---

Figure 19: Resposta do linksys_ses_24086.

Existe uma resposta do AP uma vez que existe uma mensagem de Acknowledgement.

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

2155 63.161272	Cisco-Li_f7:1d:51	Broadcast	802.11	183 Beacon frame, SN=3725, FH=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, FH=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, FH=0, Flags=.....C

Figure 20: Mensagens de Authentication.

Existe uma mensagem de authentication para 30 Munroe St ao t= 63.168087 e a resposta ao t=63.169071.

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

2162 63.169910	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	89 Association Request, SN=1648, FH=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, FH=0, Flags=.....C

Figure 21: Association Request para o AP 30 Munroe ST. e Response associado.

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

- > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18, [Mbit/sec]
- > Tag: QoS Capability
- > Tag: Extended Supported Rates 24(B), 36, 48, 54, [Mbit/sec]

Figure 22: Possíveis taxas de transmissão(Association Request).

- > 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]

Figure 23: Possíveis taxas de transmissão(Association Response).

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.

2158 63.169871	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 63.169787	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 63.170008		IntelCor_d1:b6:4f	802.11	38 Acknowledgement, Flags=.....C
2164 63.170692	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58 Authentication, SN=3727, FN=0, Flags=.....C
2165 63.171000		Cisco-Li_f7:1d:51	802.11	38 Acknowledgement, Flags=.....C
2166 63.192101	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	94 Association Response, SN=3728, FN=0, Flags=.....C

Figure 24: Sequência de tramas do processo de associação.

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

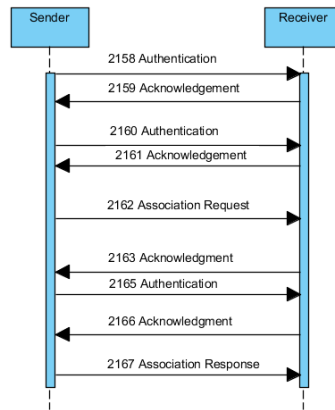


Figure 25: Diagrama do processo de associação.

4 Transferência de dados

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

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
.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)						

Figure 26: Endereços do início do download do ficheiro 'alice.txt'.

Os três campos são o endereço do Receiver, que é igual ao BSS Id, o do Transmitter, que é igual ao do Source e o do STA, e o do Destination.

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?

- Host: 00:13:02:d1:b6:4f
- AP: 00:16:b6:f4:eb:a8
- Router: 00:16:b6:f4:eb:a8

Source: 192.168.1.109
Destination: 128.119.245.12

Figure 27: IPs do destino e do host.

- IP do host: 192.168.1.109
- IP do destino: 128.119.245.12

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

O IP corresponde ao servidor que é utilizado para transmitir o ficheiro alicet.txt, uma vez que é enviado um pedido ao servidor para fazer a sincronização.

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

```

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
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)

```

Figure 28: Endereços da trama SYN ACK correspondente.

Os três campos são o endereço do Receiver, que é igual Destination e ao STA, o do Transmitter, que é igual ao BSS Id, e o Source.

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

Host: 00:16:b6:f4:eb:a8
 AP: 91:2a:b0:49:b6:4f
 Router: 00:16:b6:f4:eb:a8

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

```

Source: 128.119.245.12
Destination: 192.168.1.109

```

Figure 29: IPs do destino e do host.

Não. Como podemos observar na pergunta 26, o endereço MAC de origem é diferente do utilizado nesta segunda frame. Contudo, o endereço IP continua a ser o mesmo. Isto significa que, apesar de ter um único IP, o host funciona como se tivesse vários perfis para a transmissão de informação.

5 Conclusão

Neste quarto e último trabalho de Redes de Computadores, centrámo-nos na abordagem das redes IEEE 802.11, onde analisámos tipos de tramas, endereçamento dos componentes envolvidos, desta vez numa comunicação sem fios, e a operação do protocolo.

Começamos por abordar o "Acesso Rádio", onde aprendemos sobre a existência de uma camada com informação sobre o nível físico, como a frequência, canal, etc... De seguida, comparámos as diferenças entre um scanning ativo e passivo e verificamos que o primeiro resulta das tramas beacon e que nos permite descobrir as AP's que existem, enquanto que no segundo é utilizado o probe request e o probe response. Em terceiro lugar, relativamente ao Processo de Associação, vimos que a associação de um host a um ponto de acesso, para que seja possível o envio de dados, é efetuada através de um pedido de associação, ao qual se obtém a resposta de um Access Point. Por fim, analisámos o processo da transferência de dados com base em dois fatores: informação obtida na trama e no controlo de transferência.

Desta forma, ficamos mais familiarizados com o protocolo IEEE 802.11 e com as características de redes wireless.