

Trabalho Prático 4

José Pedro Silva, José Ricardo Cunha, and Válder Carvalho

University of Minho, Department of Informatics, 4710-057 Braga, Portugal
e-mail: {a84577,a84302,a84464}@alunos.uminho.pt

Resumo É explicada a resolução dos exercícios de todas as partes do trabalho prático número 4. São abordados os conceitos do protocolo 802.11, explorado o conceito de Wi-Fi, pontos de acesso, *beacons*, *association requests*, entre outros deste tipo. É feita a análise de um conjunto de tramas utilizando, novamente, o *Wireshark* para este efeito.

1 Introdução

Com este trabalho pretendemos mostrar a nossa interpretação dos problemas apresentados, assim como tentar explicitar o nosso raciocínio lógico, de modo a conseguir uma melhor visão da tecnologia em Redes, mergulhando nas ideias intrínsecas por base neste ramo científico.

Tentamos de forma concisa agrupar as ideias e definições num pequeno relatório que apenas contém comentários gerais às várias questões apresentadas, tentando detalhar ao máximo os conceitos mais relevantes para cada problema. Desta vez, estaremos a analisar no Wireshark um conjunto de tramas de nível de ligação Wi-Fi (protocolo IEEE 802.11) usando uma captura de tráfego já guardada.

Nos **Exercícios da parte 3** (secção 2.1), abordamos a forma como se ligam a nível físico as interfaces Wi-Fi e a rede que estão conectadas.

Nos **Exercícios da parte 4** (secção 2.2), analisamos como se realiza o *scanning* passivo em redes Wi-Fi.

Nos **Exercícios da parte 6** (secção 2.3), verificamos como um host se associa a um ponto de acesso para enviar dados.

Nos **Exercícios da parte 7** (secção 2.4), visualizamos como se realiza a transferência de dados de um host para outro.

Todos os exercícios são extremamente importantes porque fazem ponte com as aulas teóricas assim como o trabalho prático anterior, isto é, servem para cimentar conhecimentos já adquiridos e que, certamente, são importantes na formação de futuros engenheiros, não só para este ramo em concreto mas sim como conhecimentos transversais.

2 Questões e Respostas

2.1 Exercícios parte 3

Para a trama correspondente com o número 1YXX (com Y=turno e XX=grupo, e.g., 1101).

As respostas seguintes utilizam o número de trama dada por **1201** (PL2, grupo 1).

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

```
✓- 802.11 radio information
  |
  |- PHY type: 802.11g (6)
  |- Short preamble: False
  |- Proprietary mode: None (0)
  |- Data rate: 48,0 Mb/s
  |- Channel: 6
  |- Frequency: 2437MHz
  |- Signal strength (dB): 66dB
  |- Signal strength (dBm): -34dBm
  |- Noise level (dBm): -100dBm
  |- Signal/noise ratio (dB): 66dB
  >- [Duration: 280µs]
```

Print parcial da trama 1201

Como vemos pela imagem, a frequência é 2437MHz e o canal é o 6.

- **2)** Identifique a versão da norma IEEE 802.11 que está a ser usada.
Como vemos pela imagem anterior, está a ser usada a norma 802.11g (**PHY type**).

- **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.
Está a ser usado, novamente pela imagem anterior, um *datarate*=48 Mb/s. O protocolo 802.11g permite, no entanto, velocidades máximas de 54 Mb/s.
O facto de não se obter este total deve-se a atenuações do meio, que tornam o sinal mais fraco à medida que nos afastamos do AP.

2.2 Exercícios parte 4

As tramas beacon permitem efetuar scanning passivo em redes Wi-Fi. Para a captura de tramas disponibilizada, responda às seguintes questões

- 4) Quais são os SSIDs dos dois APs que estão a emitir a maioria das tramas de beacon?
Os dois AP's são *IntelCor_d1:b6:4f* e *Cisco-Li_f7:1d:51* com os SSID's *linksys_SES_24086* e *30 Monroe St*, respetivamente.
- 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.

```
IEEE 802.11 wireless LAN
├─ Fixed parameters (12 bytes)
│   ├── Timestamp: 9534922036096
│   ├── Beacon Interval: 0,102400 [Seconds]
│   └─> Capabilities Information: 0x0011
```

Intervalo de transmissão

Como vemos pela imagem anterior, vemos que o intervalo é de 0.1024 segundos, tanto para um AP como para outro.

Não é sempre periódico por causa do protocolo CSMA, ou seja, se o canal está ocupado, o beacon não é enviado imediatamente.

- 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.

```
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 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 1100 .... = Sequence number: 2860
├─ Frame check sequence: 0x4c2dfbc0 [correct]
└─ [FCS Status: Good]
```

Endereço MAC de origem do beacon

O endereço pedido é 00:16:b6:f7:1d:51.

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

O endereço de destino é broadcast (ff:ff:ff:ff:ff:ff).

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

O endereço é, também, 00:16:b6:f7:1d:51.

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

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

Rates e Extended Rates do AP 30 Munroe St

As suportadas são: 1, 2, 5.5 e 11 Mbit/s.

As extended supported rates são: 6, 9, 12, 18, 24, 36, 48 e 54 Mbit/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)?

```
> 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 0010 0110 .... = Sequence number: 3366
  Frame check sequence: 0xfaf9f6bf [correct]
  [FCS Status: Good]
```

Tipo da trama 802.11

Selecione a trama 1205, vemos que o valor de tipo/subtipo é de 0x0008, ou seja, identifica uma beacon frame. Está contida no **Frame Control Field**.

- 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.

```
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 1010 1000 .... = Sequence number: 2984
- Frame check sequence: 0x7704e1c7 [correct]
- [FCS Status: Good]

IEEE 802.11 Beacon frame, Flags: .....
- Type/Subtype: Beacon frame (0x0008)
> Frame Control Field: 0x8000
- .000 0010 1101 0101 = Duration: 725 microseconds
- Receiver address: ff:bf:f9:fe:ff:ff (ff:bf:f9:fe:ff:ff)
- Destination address: ff:bf:f9:fe:ff:ff (ff:bf:f9:fe:ff:ff)
- Transmitter address: 00:86:bc:d2:22:94 (00:86:bc:d2:22:94)
- Source address: 00:86:bc:d2:22:94 (00:86:bc:d2:22:94)
- BSS Id: LinksysG_67:22:94 (00:06:25:67:22:94)
- .... 0000 = Fragment number: 0
- 1100 0110 1111 .... = Sequence number: 3183
> Frame check sequence: 0x35bb97ba incorrect, should be 0x8722e2aa
- [FCS Status: Bad]
```

Tramas com e sem erros (frame check sequence)

Após ativar, no Wireshark, o campo CRC, vemos que algumas das tramas vêm com erros (FCS: incorrect), mas a maior parte são corretas (FCS: correct).

É importante a existência de correção de erros porque o ruído do meio leva a que pacotes possam ser recebidos com informação incorreta e, num sistema como Wi-Fi muito suscetível a atenuações pelo meio ambiente, tem de haver esta salvaguarda de modo a evitar perda de informação.

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

```

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 1010 0111 .... = Sequence number: 2983
  Frame check sequence: 0x107a57bf [correct]
  [FCS Status: Good]

```

Endereços MAC usados

Pela imagem vemos que os endereços são: Receiver address, Destination address, Transmitter address e Source address.

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

No.	Time	Source	Destination	Protocol	Length	Info
27	1.212185	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	177	Probe Response, SN=2867, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
50	2.297613	IntelCor_1f:57:13	Broadcast	802.11	79	Probe Request, SN=576, FN=0, Flags=.....C, SSID=Home WIFI
51	2.309697	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2878, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
52	2.302191	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2878, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
53	2.304063	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2878, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
54	2.305562	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2878, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
55	2.308563	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2878, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
56	2.310072	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2878, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
59	2.453941	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2881, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
83	4.283835	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	177	Probe Response, SN=2900, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
87	4.298449	IntelCor_1f:57:13	Broadcast	802.11	78	Probe Request, SN=598, FN=0, Flags=.....C, SSID=pholphas
88	4.301564	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2901, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
89	4.303314	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2901, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
90	4.304814	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2901, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
93	4.403454	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2903, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
94	4.404939	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2903, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
117	6.290705	IntelCor_1f:57:13	Broadcast	802.11	79	Probe Request, SN=620, FN=0, Flags=.....C, SSID=concourse
118	6.300439	IntelCor_1f:57:13	Broadcast	802.11	79	Probe Request, SN=621, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)

Filtro WireShark + probing request/response

O comando 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?

(Utiliza-se as tramas 51 e 52 como exemplo.)

Há dois tipos de tramas:

- Probe request

```

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)

```

Probe request (trama 51)

O BSSID é o de broadcast (ff:ff:ff:ff:ff:ff), que também é o endereço de destino, que parte do MAC de origem 00:12:f0:1f:57:13. O que este tipo de trama faz é um pedido ao AP para ver se pode realizar uma conexão ou não, portanto envia um pacote para as suas redondezas e o SSID especificado recebe e processa essa mensagem, enviando a resposta de volta ao host através de um probe response.

- Probe response

```
✓ 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)
```

Probe response (trama 52)

O BSSID é 00:16:b6:f7:1d:51, identificando o BSSID do AP que recebeu a mensagem (destino pretendido pela trama anterior). Por outro lado, o endereço de destino é o do host que enviou a probe request anterior, indicando se pode, ou não, conectar-se.

- 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?*
Esta pergunta foi respondida em 14).

2.3 Exercícios parte 6

Numa rede Wi-Fi estruturada um host deve associar-se a um ponto de acesso antes de enviar dados. O processo de associação nas redes IEEE 802.11 é executada enviando a trama association request do host para o AP e a trama association response enviada pelo AP para o host, em resposta ao pedido de associação recebido. Este processo é antecedido por uma fase de autenticação. Para a sequência de tramas capturada no ficheiro disponibilizado indique:

- 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 (- 802.11	38	Acknowledgement, Flags=.....C
1735	49.609617	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54 Deauthentication, SN=1605, FN=0, Flags=.....C
1736	49.609770		IntelCor_d1:b6:4f (- 802.11	38	Acknowledgement, Flags=.....C

Trama DHCP seguida por uma de deauthentication

Vemos pela imagem que o host envia uma mensagem DHCP (camada IP) para terminar a associação com o AP, de modo a libertar o seu IP na rede. Seguidamente, envia uma mensagem de *deauthentication* (camada de ligação 802.11), isto é, uma mensagem que contém o porquê de ter sido desfeita esta associação.

- 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 $t=49$?

wlan.fc.subtype==11						
No.	Time	Source	Destination	Protocol	Length	Info
1044	32.889945			802.11	571	Unrecognized (Reserved frame), Flags=...P....
1740	49.638857	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=.....C
1741	49.639700	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=...R...C
1742	49.640702	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=...R...C
1744	49.642315	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=...R...C
1746	49.645319	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=...R...C
1749	49.649705	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=...R...C
1821	53.785833	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1612, FN=0, Flags=.....C
1822	53.787070	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1612, FN=0, Flags=...R...C
1921	57.889232	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=.....C
1922	57.890325	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=...R...C
1923	57.891321	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=...R...C
1924	57.896970	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=...R...C
2122	62.171951	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0, Flags=.....C
2123	62.172946	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0, Flags=...R...C
2124	62.174070	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0, Flags=...R...C
2156	63.168087	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58	Authentication, SN=1647, FN=0, Flags=.....C
2158	63.169071	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58	Authentication, SN=3726, FN=0, Flags=.....C

Mensagens de authentication

Seguindo $t=49$, vemos pela imagem que foram enviadas 15 tramas de autenticação (usando o filtro wlan.fc.subtype==11) por parte deste host para o AP Cisco-Li_f5:ba:bb.

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


```

IEEE 802.11 wireless LAN
  Fixed parameters (6 bytes)
    Authentication Algorithm: Open System (0)
    Authentication SEQ: 0x0001
    Status code: Successful (0x0000)

```

Tipo de autenticação

O tipo de autenticação pretendida é aberta, como vemos pela imagem.

- 19) *Observa-se a resposta de authentication do AP linksys_ses_24086 AP no trace?*
 Não, vemos que nunca obtém resposta por parte deste AP, na 16ª trama usando este filtro vemos que ele seleciona um outro AP para se conectar.
- 20) *Vamos agora considerar o que acontece quando o host desiste de se associar ao AP linksys_ses_24086 AP e se tenta associar ao AP 30 Munroe St. Procure tramas authentication enviadas pelo host para e do AP e vice-versa. Em que tempo aparece um trama authentication do host para o AP 30 Munroe St. e quando aparece a resposta authentication do AP para o host?*

No.	Time	Source	Destination	Protocol	Length	Info
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=.....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=.....C
1923	57.891321	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=.....C
1924	57.896970	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=.....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=.....C
2124	62.174070	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0, Flags=.....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=.....C
2164	63.170692	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58	Authentication, SN=3727, FN=0, Flags=.....C
2274	68.662233	83:17:c6:ae:cd:9c	72:8e:bb:91:31:97	LLC	1586	I, N(R)=12, N(S)=108; DSAP 0xc2 Group, SSAP 0xf6 Command

Tempo da autenticação do host->AP e AP->host

Quando t=63.168087 (16ª trama), o host tenta-se associar a um novo AP, isto é, Cisco-Li_f7:1d:51. A resposta a este pedido de autenticação está imediatamente a seguir, em 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?*

No.	Time	Source	Destination	Protocol	Length	Info
1980	59.098589	IntelCor_d1:b6:4f	Cisco-L1_f5:ba:bb	EAPOL	185	Key (Message 2 of 4)
1982	59.102829	IntelCor_d1:b6:4f	Cisco-L1_f5:ba:bb	EAPOL	185	Key (Message 2 of 4)
1984	59.107443	IntelCor_d1:b6:4f	Cisco-L1_f5:ba:bb	EAPOL	185	Key (Message 2 of 4)
1985	59.110319	IntelCor_d1:b6:4f	Cisco-L1_f5:ba:bb	EAPOL	185	Key (Message 2 of 4)
1987	59.110569	IntelCor_d1:b6:4f	Cisco-L1_f5:ba:bb	EAPOL	185	Key (Message 2 of 4)
1988	59.124450	IntelCor_d1:b6:4f	Cisco-L1_f5:ba:bb	EAPOL	185	Key (Message 2 of 4)
1990	59.130949	IntelCor_d1:b6:4f	Cisco-L1_f5:ba:bb	EAPOL	185	Key (Message 2 of 4)
1991	59.142195	IntelCor_d1:b6:4f	Cisco-L1_f5:ba:bb	EAPOL	185	Key (Message 2 of 4)
2126	62.176945	IntelCor_d1:b6:4f	Cisco-L1_f5:ba:bb	802.11	107	Association Request, SN=1645, FN=0, Flags=.....C, SSID=Linksys_SES_24086
2127	62.178194	IntelCor_d1:b6:4f	Cisco-L1_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-L1_f7:1d:51	802.11	89	Association Request, SN=1648, FN=0, Flags=.....C, SSID=30 Munroe St
2166	63.192101	Cisco-L1_f7:1d:51	IntelCor_d1:b6:4f	802.11	94	Association Response, SN=3728, FN=0, Flags=.....C

Tempo a que são enviados os associate request/reply

Usando o filtro indicado na figura, vemos que o tempo que aparece esse associate request do host é em t=63.169910. A association response do AP está em t=63.192101.

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

Como vemos pela figura, estão a ser utilizadas as seguintes taxas de transmissão:

- 1, 2, 5.5, 11, 6, 9, 12 e 18 Mbit/s [host]

```
> 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: 0xce01
    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 Number: QoS Capability (46)
      Tag length: 1
    > QoS Information (STA): 0x00
    > Tag: Extended Supported Rates 24(B), 36, 48, 54, [Mbit/sec]
```

Taxas de transmissão do host

- 1, 2, 5.5, 11 Mbit/s [AP]

```
> 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
```

Taxas de transmissão do AP

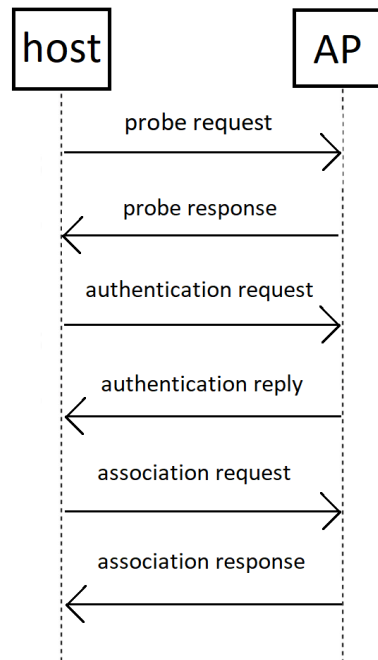
- 23) Identifique uma sequência de tramas que corresponda a um processo de associação completo entre a STA e o AP, incluindo a fase de autenticação.

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-L1_f7:1d:51	IntelCor_d1:b6:4f	802.11	177	Probe Response, SN=3724, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
2156	63.160807	IntelCor_d1:b6:4f	Cisco-L1_f7:1d:51	802.11	58	Authentication, SN=1647, FN=0, Flags=.....C
2158	63.160971	Cisco-L1_f7:1d:51	IntelCor_d1:b6:4f	802.11	58	Authentication, SN=3726, FN=0, Flags=.....C
2160	63.160707	IntelCor_d1:b6:4f	Cisco-L1_f7:1d:51	802.11	58	Authentication, SN=1647, FN=0, Flags=....R...C
2162	63.160910	IntelCor_d1:b6:4f	Cisco-L1_f7:1d:51	802.11	89	Association Request, SN=1648, FN=0, Flags=.....C, SSID=30 Munroe St
2164	63.170692	Cisco-L1_f7:1d:51	IntelCor_d1:b6:4f	802.11	58	Authentication, SN=3727, FN=0, Flags=.....C
2166	63.192101	Cisco-L1_f7:1d:51	IntelCor_d1:b6:4f	802.11	94	Association Response, SN=3728, FN=0, Flags=.....C
2178	63.689723	Cisco-L1_f7:1d:51	IntelCor_d1:b6:4f	802.11	177	Probe Response, SN=3734, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St

Sequência de tramas com as várias fases

As tramas pedidas estão no intervalo [2152,2166] na imagem anterior, utilizando o filtro `wlan.fc.subtype==4 || wlan.fc.subtype==5 || wlan.fc.subtype==11 || wlan.fc.subtype==1 || wlan.fc.subtype==0`.

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



2.4 Exercícios parte 7

O trace disponibilizado, para além de tramas de gestão da ligação de dados inclui tramas de dados e de controlo da transferência desses mesmos 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?

```
✓ Flags: 0x01
  .... 01 = DS status: Frame from STA to DS via an AP (To DS: 1 From DS: 0) (0x1)
  .... 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 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)
```

Endereços MAC do segmento SYN TCP

Os endereços MAC são: Receiver, Transmitter e Destination, que podem ser visualizados na figura.

- 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?

```
> Flags: 0x4000, Don't fragment
  ...0 0000 0000 0000 = Fragment offset: 0
  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
```

IP's do segmento

Como os campos são *To DS: 1* e *From DS: 0*:

- MAC do host: 00:13:02:d1:b6:4f
- MAC do AP: 00:16:b6:f7:1d:51
- MAC do Router do 1º salto: 00:16:b6:f4:eb:a8

- 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.
Este IP de destino corresponde ao AP, que é o que estabelece a ligação para uma rede "cabelada"e, portanto, o local de conexão para redes exteriores.
- 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?

```

Flags: 0x32
  ....10 = DS status: Frame from DS to a STA via AP(To DS: 0 From DS: 1) (0x2)
  ....0.. = More Fragments: This is the last fragment
  ....0... = Retry: Frame is not being retransmitted
  ...1.... = PWR MGT: STA will go to sleep
  ..1.... = More Data: Data is buffered for STA at AP
  .0...   = Protected flag: Data is not protected
  0...    = Order flag: Not strictly ordered
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)

```

Endereços MAC do segmento SYNACK

Os endereços MAC são: Receiver, Transmitter e Destination, que podem ser visualizados na figura.

- 29) Qual o endereço MAC nesta trama que corresponde ao host? Qual o do AP? Qual o do router do primeiro salto?
Como os campos são *To DS: 0* e *From DS: 1*, tem-se:
- MAC do host: 00:16:b6:f4:eb:a8
 - MAC do AP: 00:16:b6:f7:1d:51
 - MAC do router do 1º salto: 91:2a:b0:49:b6:4f
- 30) O endereço MAC de origem na trama corresponde ao endereço IP do dispositivo que enviou o segmento TCP encapsulado neste datagrama? Justifique.
O IP do host que enviou a trama é 192.168.1.109 e, no entanto, esta tem IP 128.119.245.12, portanto, não são iguais.

3 Conclusões

No final de realizar este trabalho, num contexto geral, sentimos que conseguimos atingir os objetivos pretendidos, pelo que conseguimos por fim estabelecer uma ponte entre o que foi lecionado nas aulas teóricas e as aplicações práticas dos conceitos e temas propostos.

Em particular, nos **Exercícios da parte 3**, conseguimos extrair do Wireshark informação acerca do meio físico que as tramas utilizam para serem propagadas, que tem valores por defeito e que está tudo controlado.

Nos **Exercícios da parte 4**, percebemos como é que os dispositivos fazem scanning passivo e ativo por novas redes Wireless, assim como a importância dos CRC e o porquê de ser muito difícil obter rendimento máximo neste tipo de redes.

Nos **Exercícios da parte 6** conseguimos analisar o processo de associação dos dispositivos (etapa antes de serem enviados dados), assim como autenticações, na sua ordem cronológica.

Por fim, nos **Exercícios da parte 7**, analisamos como é que efetivamente estes dados são transferidos, tendo em atenção os vários endereços MAC que existem em cada trama.

Sentimos que este projeto nos ajudou a perceber melhor o protocolo 802.11, que é importante para o nosso dia-a-dia como engenheiros, porque, atualmente, toda a comunicação é sem fios e ter formação base nestas tecnologias é sempre uma mais valia.

Referências

1. Notas de Apoio das Aulas Teóricas
2. *ANSI/IEEE Standard 802.11*, 1999 Edition (R2003), <http://gaia.cs.umass.edu/wireshark-labs/802.11-1999.pdf>