

Universidade do Minho

REDES DE COMPUTADORES

MESTRADO INTEGRADO EM ENGENHARIA INFORMÁTICA

REDES SEM FIOS (802.11) [TP4]

GRUPO 9

A85227 João Pedro Rodrigues Azevedo

A85729 Paulo Jorge da Silva Araújo

A83719 Pedro Filipe Costa Machado

Braga
Dezembro 2019

Conteúdo

1	Introdução	2
2	Análise das questões propostas	3
2.1	Acesso Rádio	3
2.2	Scanning	4
2.3	Processo de Associação	8
2.4	Transferência de Dados	12
3	Conclusões	14

Capítulo 1

Introdução

Este trabalho foi realizado no âmbito da Unidade Curricular de Redes de computadores, trata-se do último trabalho prático e teve como objetivo principal o estudo do protocolo IEEE 802.11 tais como o formato das tramas, o endereçamento dos componentes envolvidos na comunicação sem fios, os tipos de tramas mais comuns, bem como a operação do protocolo.

Deste modo, ao longo deste relatório vão ser apresentadas as várias questões enunciadas e respostas estruturadas às mesmas com diversas demonstrações práticas da sua validade levando a uma secção final de conclusões onde fazemos um balanço de todo o trabalho realizado e a sua importância nesta Unidade Curricular.

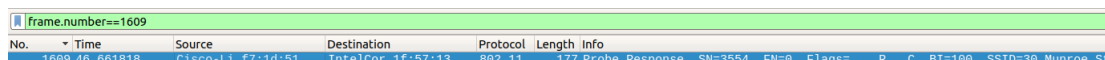
Capítulo 2

Análise das questões propostas

2.1 Acesso Rádio

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

R: Estamos no turno PL6 e somos o grupo 09, logo utilizamos a trama com número de registo **1609**. Utilizamos, para o efeito, o seguinte filtro: `"frame.number == 1609"`. Obtivemos o seguinte registo e o respetivo **frame** correspondente a uma *Trama de Resposta (Probe Response)*:



No.	Time	Source	Destination	Protocol	Length	Info
1609	46.661818	Cisco-L1_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=3554, FN=8, Flags=...R...C, BI=100, SSID=30 Munroe St

Figura 2.1: Registo 1609 da captura Wireshark.

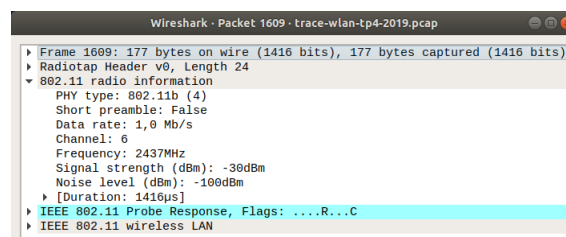


Figura 2.2: Trama correspondente ao registo filtrado.

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

R: A rede sem fios está a operar numa frequência de **2437MHz** (2.4GHz) correspondente ao **canal 6**.

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

R: Para frequências daquela magnitude e tendo em atenção a figura acima, conseguimos afirmar que está a ser usada a versão **802.11b** (campo *”PHY type”*¹ do pacote).

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.”*

¹ Abreviação para *Physical layer*.

R: A trama escolhida foi enviada a um débito de 1.0Mbps (campo *Data rate* do pacote). Não corresponde ao débito máximo a que a interface Wi-Fi pode operar visto que, segundo os *standards* referentes a esta versão da norma IEEE 802.11 indicam um débito máximo teórico de 11Mbps.

2.2 Scanning

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

R: Para filtrar apenas as tramas do tipo *Beacon* utilizamos o seguinte filtro:

```
wlan.fc.type_subtype==0x08.
```

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

R: Com o filtro acima referido, conseguimos reparar que existem 3 SSIDs diferentes, sendo eles: "30 Munroe St", "linksys_SES_24086" e "linksys12". Para verificar os dois APs que estão a emitir a maioria das tramas *beacon*, aplicámos os filtros:

- `wlan.fc.type_subtype==0x08 && wlan.ssid == "30 Munroe St"`

Resultado: 718 pacotes;

- `wlan.fc.type_subtype==0x08 && wlan.ssid == "linksys_SES_24086"`

Resultado: 7 pacotes;

- `wlan.fc.type_subtype==0x08 && wlan.ssid == "linksys12"`

Resultado: 24 pacotes;

Deste modo, os SSID 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."*

R: Para melhor visualização da trama, segue-se um *printscreen* de uma trama *beacon* correspondente ao SSID "linksys_SES_2406":

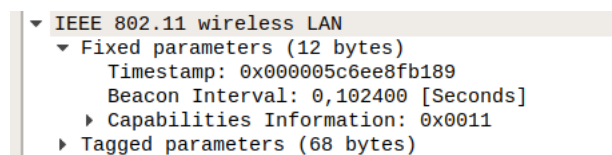


Figura 2.3: Trama beacon correspondente ao pacote com No 1499.

O intervalo de tempo entre a transmissão de tramas beacon (*beacon interval*) é de 0.1024 segundos. O mesmo se verifica para o AP "30 Munroe St".

wlan.fc.type_subtype==0x08 && wlan.ssid == "linksys_SES_24086"				wlan.fc.type_subtype==0x08 && wlan.ssid == "30 Munroe St"			
No.	Time	Source	Destination	Io.	Time	Source	Destination
1499	42.532596	Cisco-Li_f5:ba:bb	Broadcast	1	0.000000	Cisco-Li_f7:1d:51	Broadcast
1513	42.839767	Cisco-Li_f5:ba:bb	Broadcast	3	0.085474	Cisco-Li_f7:1d:51	Broadcast
1527	43.658960	Cisco-Li_f5:ba:bb	Broadcast	4	0.187919	Cisco-Li_f7:1d:51	Broadcast
1624	52.228865	Cisco-Li_f5:ba:bb	Broadcast	9	0.298284	Cisco-Li_f7:1d:51	Broadcast
2290	69.463282	Cisco-Li_f5:ba:bb	Broadcast	11	0.393174	Cisco-Li_f7:1d:51	Broadcast
2296	69.667955	Cisco-Li_f5:ba:bb	Broadcast	13	0.495032	Cisco-Li_f7:1d:51	Broadcast
2321	71.101576	Cisco-Li_f5:ba:bb	Broadcast	15	0.597382	Cisco-Li_f7:1d:51	Broadcast
				17	0.699847	Cisco-Li_f7:1d:51	Broadcast
				18	0.802226	Cisco-Li_f7:1d:51	Broadcast

(a) "linksys_SES_24086".

(b) "30 Munroe St".

Figura 2.4: Tramas *beacon* para os SSIDs considerados.

Na prática, os pacotes *beacon* vindos do AP "30 Munroe St" cumprem a regularidade definida pelo *beacon interval*, de 0.1024s, tendo mantido um débito de cerca de 10 pacotes por segundo. Tal não acontece com as tramas vindas do SSID "linksys_SES_24086", tendo emitido apenas cerca de 1 a 2 tramas por segundo. Uma possível razão para a não regularidade de tramas enviadas rege-se, por exemplo, pela distância do dispositivo onde foi feita a captura ao AP com esse SSID ou até o congestionamento da rede Wi-Fi no momento.

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."

R: Tome-se, por exemplo, a trama *beacon* seguinte (registo de captura No. 1):

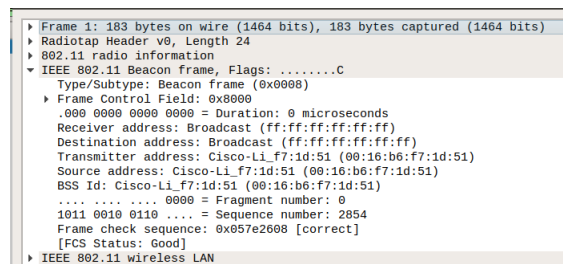


Figura 2.5: Trama *beacon* com SSID "30 Munroe St".

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

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

R: O destino para esta trama é *Broadcast* cujo endereço MAC corresponde a ff:ff:ff:ff:ff:ff.

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

R: O BSS ID da trama pedida é Cisco-LI-f7:1d:51, cuja notação hexadecimal corresponde a 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?"

R: Através da imagem seguinte (retirada da captura do pacote):

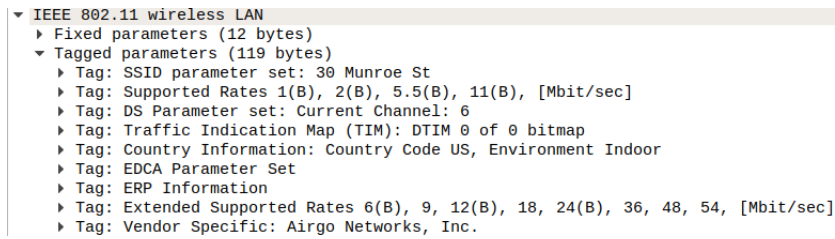


Figura 2.6: *Supported rates*.

Verificamos que tem quatro *supported rates*: 1, 2, 5.5, 11 [Mbp/s]. Tem, também, 8 *extended supported rates*: 6, 9, 12, 18, 24, 36, 48, 54 [Mbp/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)?"

R: Para o nosso turno e grupo a trama beacon a selecionar seria 1609 mas a mesma não existe na captura. Portanto decidimos usar a trama beacon 1616. Esta trama beacon é do tipo de tramas de gestão (*Management frames*) e cujo subtipo é 8. São beacon frames(0x0008) cujo tipo é management frame(0) e o subtipo é 8. Estes campos estão indicados na secção *Frame Control* do cabeçalho da trama da camada *IEEE 802.11 beacon frame*.

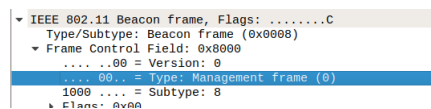


Figura 2.7: Tipo e subtipo da trama beacon.

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."

R: Apesar de não ser visível o campo CRC nas tramas beacon capturadas pelo Wireshark, conseguimos perceber que existem alguns pacotes que estão corrompidos, como por exemplo:

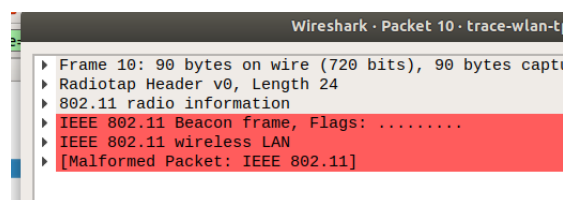


Figura 2.8: Pacote corrompido.

Tal facto indica-nos que o mecanismo de deteção de erros CRC pode eventualmente estar a ser usado e, assim sendo, nem todas as tramas beacon são recebidas corretamente. Neste tipo de redes locais torna-se crucial a utilização de mecanismos como estes visto que a vulnerabilidade a fatores externos é muito grande e pode causar o corrompimento do pacote e, por outro lado, estes algoritmos são rápidos de implementar e verificar com operações binárias detetando o ruído que se possa vir a acumular nos canais de transmissão.

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."

R:

1. AP cujo SSID é "30 Munroe St":

Destination/Receiver: **Broadcast**, MAC = ff:ff:ff:ff:ff:ff;

Source/Transmitter: **Cisco_Li_F7:1d:51**, MAC = 00:16:b6:f7:1d:51;

BSSID: **Cisco_Li_F7:1d:51**, MAC = 00:16:b6:f7:1d:51;

2. AP cujo SSID é "linksys12":

Destination/Receiver: **Broadcast**, MAC = ff:ff:ff:ff:ff:ff;

Source/Transmitter: **LinksysG_67:22:94**, MAC = 00:06:25:67:22:94;

BSSID: **LinksysG_67:22:94**, MAC = 00:06:25:67:22:94;

3. AP cujo SSID é "linksys_SES_24086":

Destination/Receiver: **Broadcast**, MAC = ff:ff:ff:ff:ff:ff;

Source/Transmitter: **Cisco-Li_f5:ba:bb**, MAC = 00:18:39:fa:ba:bb;

BSSID: **Cisco-Li_f5:ba:bb**, MAC = 00:18:39:fa:ba:bb;

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

R: O filtro estabelecido foi o seguinte:

```
wlan.fc.type_subtype == 4 or wlan.fc.type_subtype == 5
```

Sendo que, a expressão com *subtype == 4* filtra os *Probe Request* e a segunda os *Probe Response*.

wlan.fc.type_subtype==4 wlan.fc.type_subtype==5						
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	2.306697	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	2.382191	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2878, FN=0, Flags=....R...C, BI=100, SSID=30 Munroe St
53	2.384063	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2878, FN=0, Flags=....R...C, BI=100, SSID=30 Munroe St
54	2.395562	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2878, FN=0, Flags=....R...C, BI=100, SSID=30 Munroe St

Figura 2.9: Filtro: probe request e probe response.

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

R:

- Probe Request (pacote 50, por exemplo):

Destination/Receiver: **Broadcast**, MAC = ff:ff:ff:ff:ff:ff;

Source/Transmitter: **IntelCor_1f:57:13**, MAC = 00:12:f0:1f:57:13;

BSSID: **Broadcast**, MAC = ff:ff:ff:ff:ff:ff;

- **Probe Response** (pacote 134, por exemplo):

Destination/Receiver: **IntelCor_1f:57:13**, MAC = 00:12:f0:1f:57:13;

Source/Transmitter: **Cisco_Li_f7:1d:51**, MAC = 00:16:b6:f7:1d:51;

BSSID: **Cisco_Li_f7:1d:51**, MAC = 00:16:b6:f7:1d:51;

As tramas **Probe Request** servem inicialmente para a estação obter informações de uma outra estação. Esta trama é útil para uma STA determinar quais os APs que estão dentro do seu alcance rádio (active scanning).

As tramas **Probe Response** servem para a STA ou o AP responder com informações sobre as taxas de dados suportadas, etc.

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?"

R: Os pacotes apresentados acima servem como um exemplo para um pedido e uma resposta. O Probe Request foi realizado pelo sistema identificado pelo SSID **Home WiFi** e o Probe Response pelo sistema **30 Munroe St**.

O Probe Request serviu para o AP IntelCor_1f:57:13 pedir informações sobre APs que possam estar no seu alcance, especificados pelo seu SSID. Informação como os débitos de transmissão suportados, etc. são requeridas por este AP. Assim, o Probe Response informa o AP *source* das características do seu sistema.

2.3 Processo de Associação

"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?"

R: Ao visualizarmos o tracerout após t=49 encontramos duas ações que são enviadas pelo host para terminar a associação com o AP 30 Munroe St, como ilustramos em seguida:

Time	Source	Destination	Protocol	Length	Info
1731.49.440243	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C	
1732.49.542481	Cisco-Li-f7:1d:51	Broadcast	183	Beacon frame, SN=3588, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St	
1733.49.583615	192.168.1.109	192.168.1.1	390	DHCP Release - Transaction ID 0xea5a526	
1734.49.583771	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C	
1735.49.609617	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	
1737.49.614478	IntelCor_d1:b6:4f	Broadcast	99	Probe Request, SN=1606, FN=0, Flags=.....C, SSID=linksys_SES_24086	
1738.49.616260	Cisco-Li-f7:1d:51	802.11	38	Acknowledgement, Flags=.....C	

Figura 2.10: As duas tramas enviadas pelo host.

No instante $t = 49.583615$ vemos o envio de uma trama **DHCP Release** desde o host para o servidor DHCP que serviu para indicar ao servidor DHCP que o IP atribuído anteriormente (192.168.1.109) já não será mais necessário.

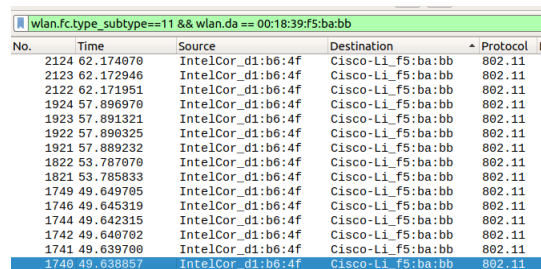
Posteriormente, no instante $t = 49.609617$ o host envia uma trama Deauthentication, de modo a terminar a ligação de forma segura e, portanto, é enviada uma mensagem a dizer que um dispositivo que está na rede já não se vai encontrar lá e portanto tem de ser retirado da lista de dispositivos connectados.

Ainda seria de esperar ser encontrada uma outra trama, neste caso uma de *Disassociation*. Isto porque esta permite que uma STA envie uma trama de dissociação para outra STA ou para o AP quando quer terminar a associação e para libertação de memória na tabela de associações.

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 $t=49$?"*

R: As tramas de **authentication** cujo destino é o AP descrito na pergunta podem ser visualizadas com o seguinte filtro:

`wlan.fc.type_subtype==11 && wlan.da == 00:18:39:f5:ba:bb`



No.	Time	Source	Destination	Protocol	Length
2124	62.174870	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	
2123	62.172946	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	
2122	62.171951	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	
1924	57.896970	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	
1923	57.891321	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	
1922	57.896325	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	
1921	57.889232	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	
1822	53.787070	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	
1821	53.785833	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	
1749	49.649705	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	
1746	49.645319	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	
1744	49.642315	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	
1742	49.648762	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	
1741	49.639700	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	
1740	49.638857	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	

Figura 2.11: Tramas **authentication** capturadas para o AP pedido.

Temos então que, a partir do instante inicial $t = 49$, existem 15 tramas de authentication do host para o AP linksys_ses_24086. A primeira destas mensagens ocorre para $t = 49.638857$ e a última ocorre para $t = 62.174070$.

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

R: O tipo de autenticação pretendida pelo host é aberta, pois como podemos observar na imagem seguinte o Authentication Algorithm é *Open System*:

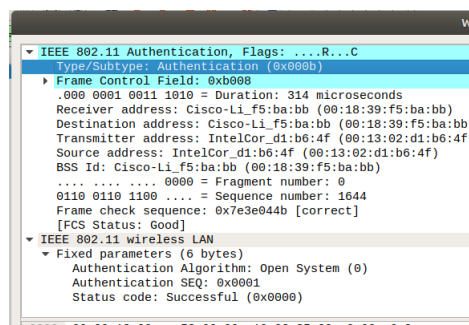


Figura 2.12: Trama de **authentication**.

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

R: Aplicámos, portanto, o filtro na direção oposta:

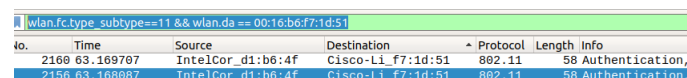
```
wlan.fc.type_subtype==11 && wlan.da == 00:13:02:d1:b6:4f
```

E não verificámos nenhuma resposta de autenticação vinda do AP linksys_SES_24086.

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?"

R: Para conseguirmos visualizar apenas as tramas usamos o seguinte filtro:

```
wlan.fc.type_subtype==11 && wlan.da == 00:16:b6:f7:1d:51
```



No.	Time	Source	Destination	Protocol	Length	Info
2160	63.169707	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58	Authentication,
2196	63.168087	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58	Authentication,

Figura 2.13: Tramas **authentication** capturadas para o AP pedido.

Para o instante $t = 63.168087$ existe uma trama **authentication** envidada com origem o host **00:13:02:d1:b6:4f** e destino o AP **30 Munroe St**.

Aplicando o mesmo filtro, mudando apenas o endereço de destino para o AP que fez o pedido de autenticação:

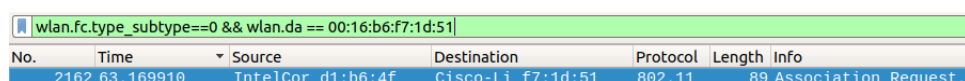
```
wlan.fc.type_subtype==11 && wlan.da == 00:13:02:d1:b6:4f
```

Vizualizamos que no instante $t = 63.169071$, muito pouco tempo depois do anterior, é enviado uma trama **authentication** no sentido oposto, ou seja desde o BSS para o host.

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?"

R: Para visualizar o **association request** do host para o AP **30 Munroe St**, aplicamos o seguinte filtro:

```
wlan.fc.type_subtype==0 && wlan.da == 00:16:b6:f7:1d:51
```



No.	Time	Source	Destination	Protocol	Length	Info
2162	63.169910	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	89	Association Request,

Figura 2.14: Pacote **association request** para o AP pedido.

Assim, o **association request** acontece para o instante $t = 63.169910$. Aplicando o filtro para obter o reply:

```
wlan.fc.type_subtype==1 && wlan.sa == 00:16:b6:f7:1d:51
```

Verificamos que o *reply* ocorre no instante $t = 63.192101$.

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

R: Os dois dispositivos, tanto no *request* como no *response* suportam as mesmas taxas de transmissão, que neste caso são 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 32, 48, and 54 [Mbp/s].

```

..00 0000 0000 0101 = ASSOCIATION ID: 0X0000
▼ 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 2.15: Taxas de transmissão suportadas.

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."

R: Aplicando o filtro a seguir apresentado conseguimos ver todos os pedidos de autenticação de associação e as suas respectivas respostas:

```
wlan.fc.type_subtype==0 or wlan.fc.type_subtype==1 or wlan.fc.type_subtype==11
or wlan.fc.type_subtype==12
```

Uma sequência de tramas possível seria a seguinte (pacote 2156 até ao 2166):

2151 63.135362	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	54 Deauthentication, SN=1646, FN=0, Flags=...R...C
2156 63.168887	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
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
2164 63.170692	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58 Authentication, SN=3727, FN=0, 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

Figura 2.16: Sequência de tramas trocadas no processo de associação e autenticação.

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

R:

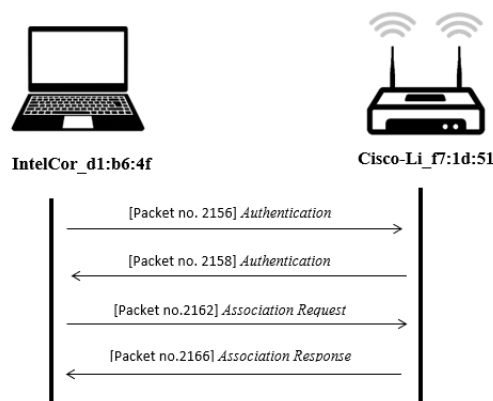


Figura 2.17: Sequência de tramas trocadas.

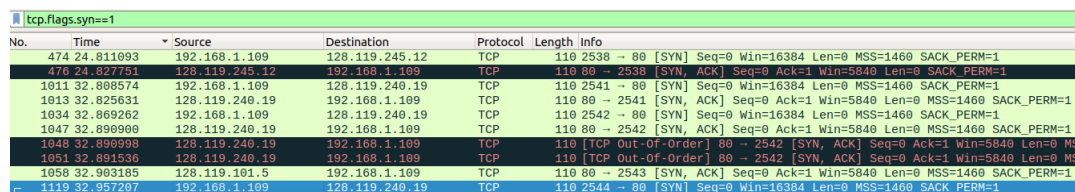
2.4 Transferência de Dados

"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 alice.txt). Quais são os três campos dos endereços MAC na trama 802.11? "

R: Para visualizar apenas as tramas SYN TCP utilizamos o seguinte filtro:

```
tcp.flags.syn == 1
```



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
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
1011	32.808574	192.168.1.109	128.119.240.19	TCP	110	2541 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
1013	32.825631	128.119.240.19	192.168.1.109	TCP	110	80 → 2541 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
1034	32.869262	192.168.1.109	128.119.240.19	TCP	110	2542 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
1047	32.890900	128.119.240.19	192.168.1.109	TCP	110	80 → 2542 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
1048	32.890998	128.119.240.19	192.168.1.109	TCP	110	[TCP Out-of-Order] 80 → 2542 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
1051	32.891536	128.119.240.19	192.168.1.109	TCP	110	[TCP Out-of-Order] 80 → 2542 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
1058	32.903185	128.119.101.5	192.168.1.109	TCP	110	80 → 2542 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
1119	32.957207	192.168.1.109	128.119.240.19	TCP	110	2544 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1

Figura 2.18: Trama com o segmento SYN TCP da primeira sessão.

A trama 802.11 que contém o segmento SYN TCP pretendido encontra-se no instante $t = 24.811093$.

Os três campos dos endereços MAC na trama correspondem ao *source address*: **00:13:02:d1:b6:4f**, *destination address*: **00:16:b6:f4:eb:a8** e *BSSID*: **00:16:b6:f7:1d:51**.

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

R: Os endereços pedidos podem ser encontrados na tabela seguinte:

Tipo de dispositivo	Endereço (MAC ou IP)
Wireless Host(Transmit. Addr.)	00:13:02:d1:b6:4f
AP	00:16:b6:f7:1d:51
First-Hop Router(Dest. Addr.)	00:16:b6:f4:eb:a8
Host origem	192.168.1.109
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."

R: O host sem fios é aquele que envia o pacote TCP e, portanto, o endereço IP de destino corresponde ao Router de primeiro salto.

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

R: A trama SYNACK corresponde ao pacote número 476, por exemplo, que pode ser visualizado na figura anterior (2.17).

```

    Frame Control Field: 0x8832
    Duration/ID: 11560 (reserved)
    Receiver address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
    Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Destination address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
    Source address: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)
    BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    STA address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
    .... 0000 = Fragment number: 0
    1100 0011 0100 .... = Sequence number: 3124

```

Figura 2.19: Campos da trama SYNACK

Os três campos dos endereços MAC na trama correspondem ao *source address*: **00:16:b6:f4:eb:a8**, *destination address*: **91:2a:b0:49:b6:4f** e *BSSID*: **00:16:b6:f7:1d:51**.

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

R: Os endereços podem ser visualizados na tabela seguinte:

Tipo	MAC adress
Host (Destination)	91:2a:b0:49:b6:4f
AP	00:16:b6:f7:1d:51
First-Hop Router (Source)	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."

R: O endereço MAC do *source* não corresponde ao endereço IP do dispositivo que enviou o segmento TCP encapsulado nesse datagrama, porque o endereço IP origem do pacote é 128.199.245.12 e, no entanto, o endereço IP de destino é 192.168.1.109, ou seja, pertencem a diferentes redes e, por sua vez, é impossível ter o mesmo endereço IP.

Capítulo 3

Conclusões

A elaboração deste trabalho permitiu aprimorar a vertente prática associada a esta Unidade Curricular, no qual se inclui o estudo do encapsulamento protocolar estruturado onde cada camada fornece serviços às camadas superiores e usa serviços disponibilizados pelas camadas inferiores. Começamos por analisar as diferentes tramas de gestão 802.11 que permitem que as estações (STAs) estabeleçam e mantenham a comunicação, entre elas, tramas de anúncio (*beacon*), de autenticação, de associação, etc...e a importância das mesmas para iniciar a conexão com um AP, terminar uma existente de forma segura e mesmo obter informações de outros APs que estejam no alcance rádio do host.

Durante a realização deste trabalho sentimos dificuldades na compreensão dos pacotes através do 'Wireshark' e da análise dos vários campos deste. Mesmo assim, achamos que acabamos o trabalho com um conhecimento bastante superior em relação a este tema, bem como na utilização do 'Wireshark' como forma de analisarmos os pacotes transmitidos.

Em suma, achamos que tanto este projeto como os anteriores foram bastante fulcrais para a realização desta cadeira, pois facilitou a interiorização da matéria lecionada pelas teóricas.