TP4 - Redes Sem Fios

Engenharia Informática
Universidade do Minho
2019/2020

Grupo - PL6.G06

Paulo Lima | a89983

Mafalda Costa | a83919

Maria Silva | a83840

Objetivo

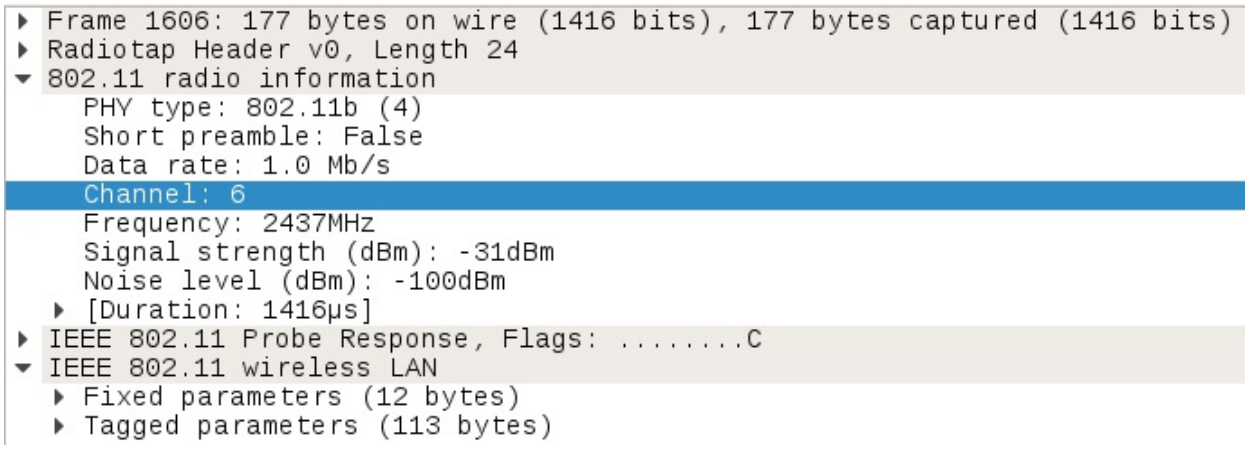
- Aprofundar o conhecimento sobre o protocolo IEEE 802.1.
- Conhecer as tramas mais comuns e o seu formato.
- Endereçamento dos componentes envolvidos na comunicação sem fios.

Questões e Respostas

3 - Acesso Rádio

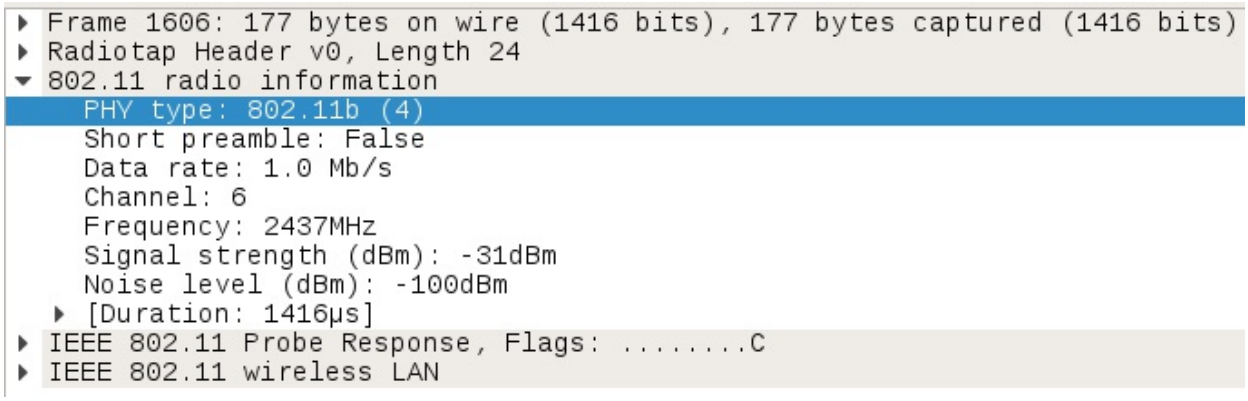
1) Identifique em que frequência do espectro está a operar a rede sem fios, e o canal que corresponde a essa frequência.

A frequência em que opera são os 2437 MHz e o canal é o 6.



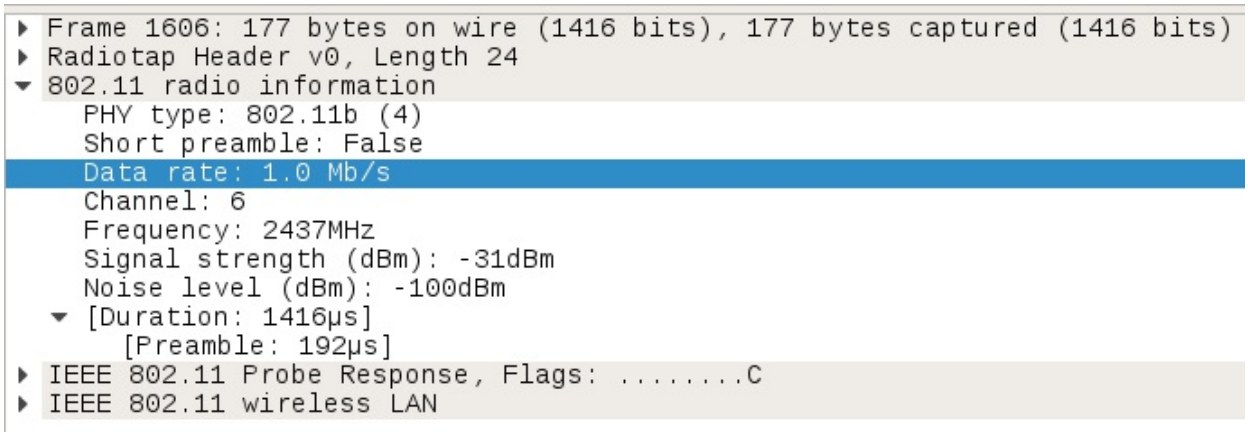
2) Identifique a versão da norma IEEE 802.11 que está a ser usada.

A versão utilizada é a 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.

A trama foi enviada com um débito de 1 Mbps. Sendo que o máximo a que a interface Wi-Fi pode operar são 11 Mbps, conluimos que o débito de envio não corresponde ao máximo.

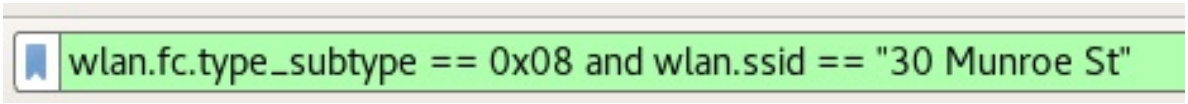


4 - Scanning

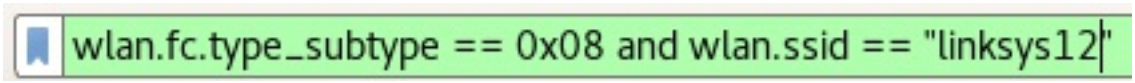
4) Quais são os SSIDs dos dois APs que estão a emitir a maioria das tramas de beacon?

Incialmente, aplicámos no Wireshark, o filtro `wlan.fc.type_subtype == 0x08` para obtermos apenas as tramas `Beacon`. De seguida, ordenámos por `Source` e comparámos os diferentes MAC Address para perceber quais são os dois que emitem mais tramas. Para obtermos o número de pacotes de cada SSID aplicámos o filtro `wlan.fc.type_subtype == 0x08 and wlan.ssid == 'nome_SSID'`.
Concluímos que os dois SSIDs que correspondem aos Access Points que emitem a maioria das tramas são 30 Munroe St e linksys12.

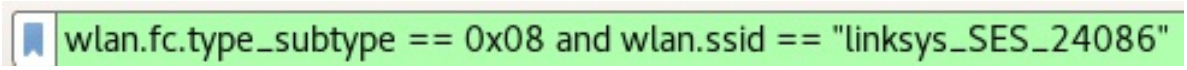
- 1º

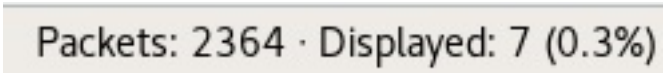


- 2º



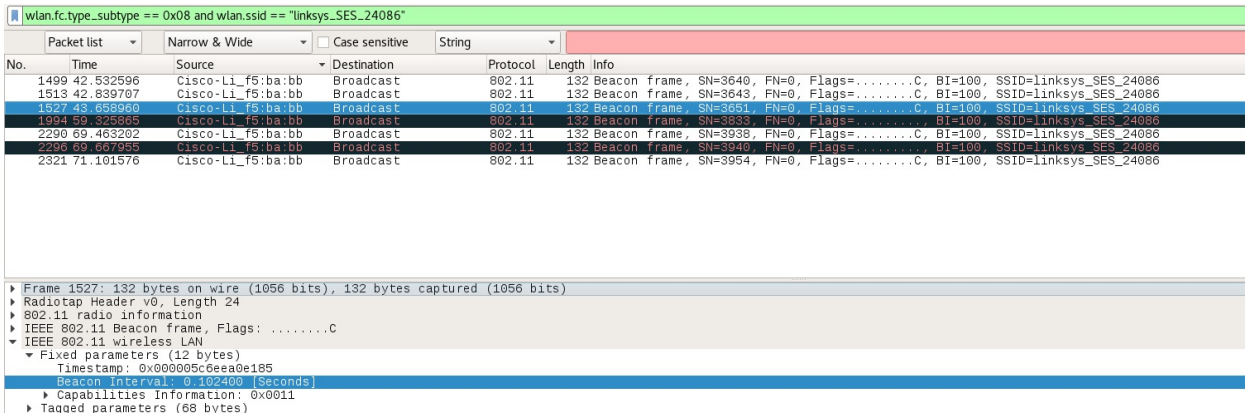
- 3º

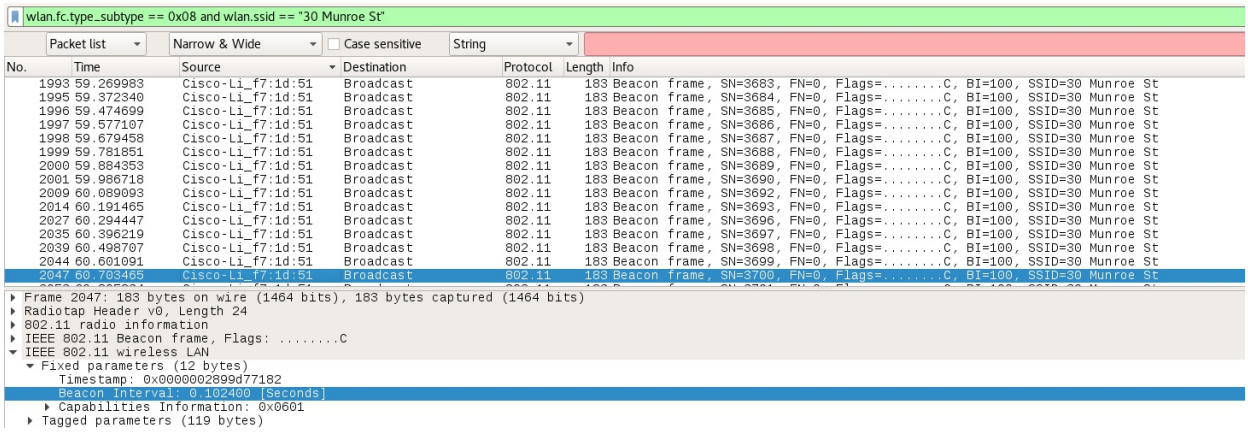


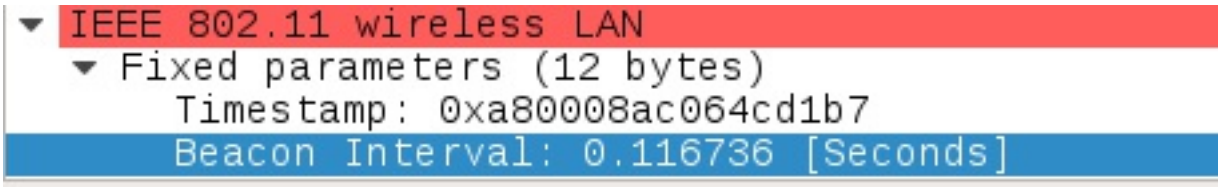


5) Qual o intervalo de tempo entre a transmissão de tramas beacon para o AP linksys_ses_24086? E do AP 30 Munroe St? Na prática, a periodicidade de tramas beacon é verificada? Tente explicar porquê.

Para ambos os casos o intervalo de tempo mais comum é de 0.102400 segundos.
Não, pois existem algumas tramas em que a periodicidade não é mantida.







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 39 Munroe St é 00:16:b6:f7:1d:51.

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

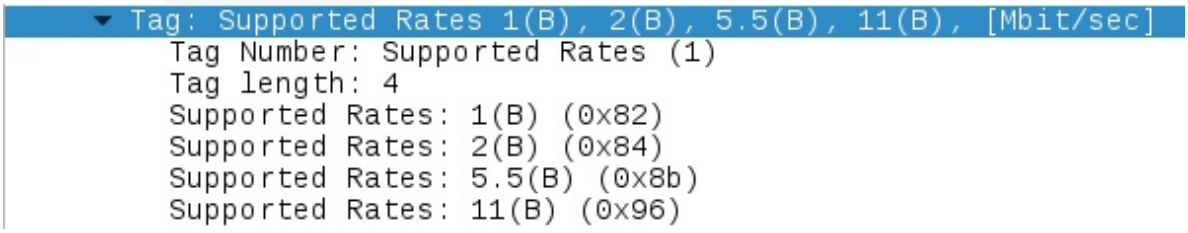
O endereço MAC é mesmo que o da origem, logo o 00:16:b6:f7:1d:51, pois estes estão em Broadcast.

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

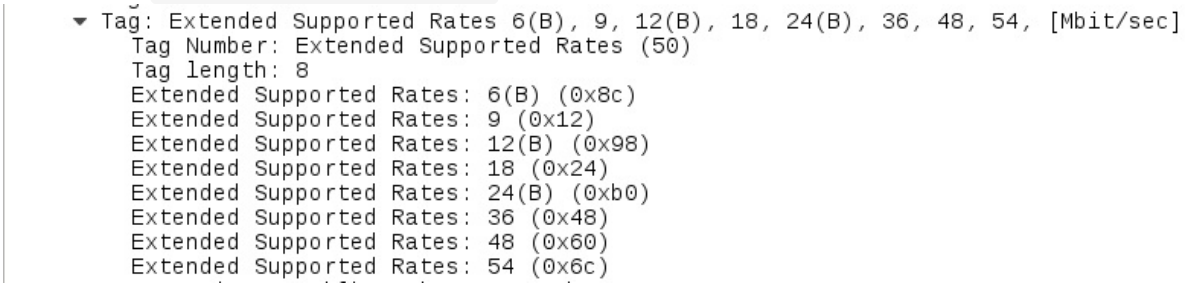
O endereço MAC é o 00:16:b6:f7:1d:51.

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?

- Supported - `supported rates`.

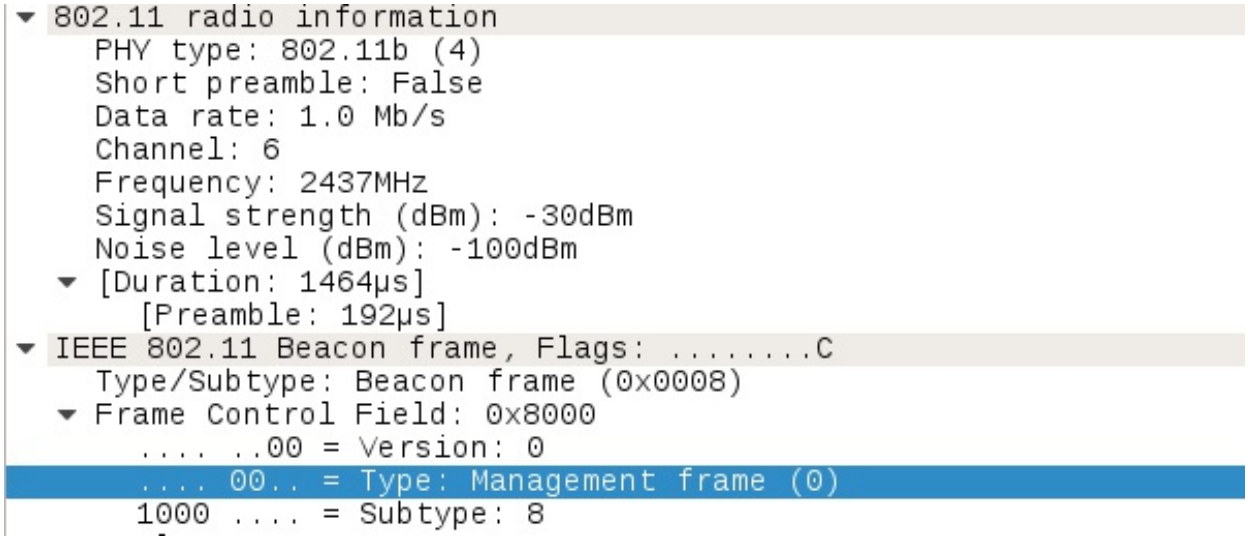


- Extended - `extendend supported rates`.



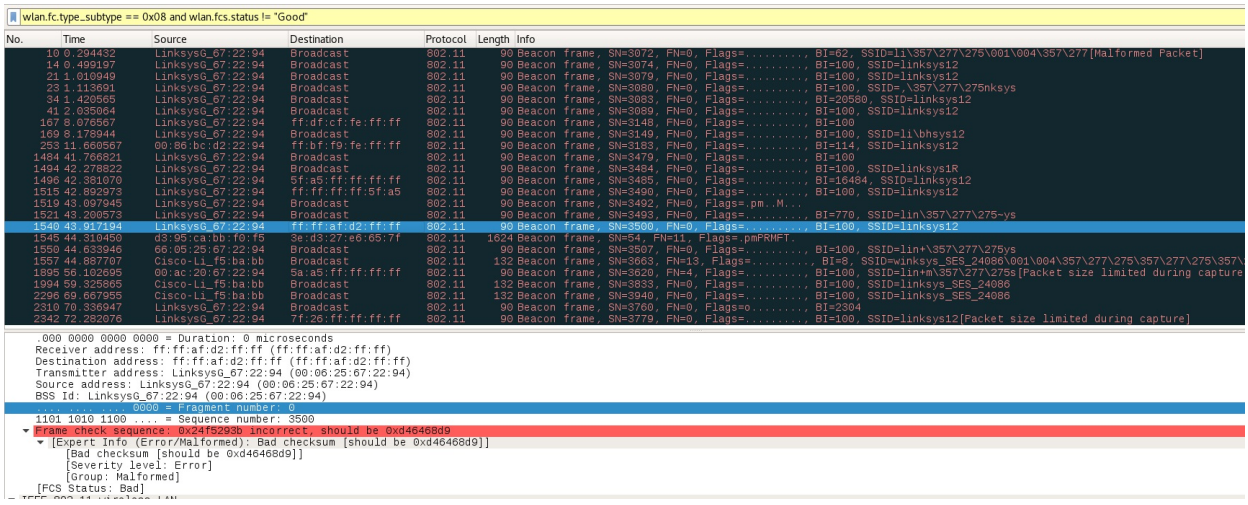
10) Selecione uma trama beacon. Esta trama pertence a que tipo de tramas 802.11? Indique o valor dos seus identificadores de tipo e de subtipo. Em que parte concreta do cabeçalho da trama estão especificados?

A trama pertence ao tipo 802.11b. O seu tipo é Management Frame e o subtipo é 0x0008 o que significa atráves da tabela podemos inferir que se trata de um Beacon.

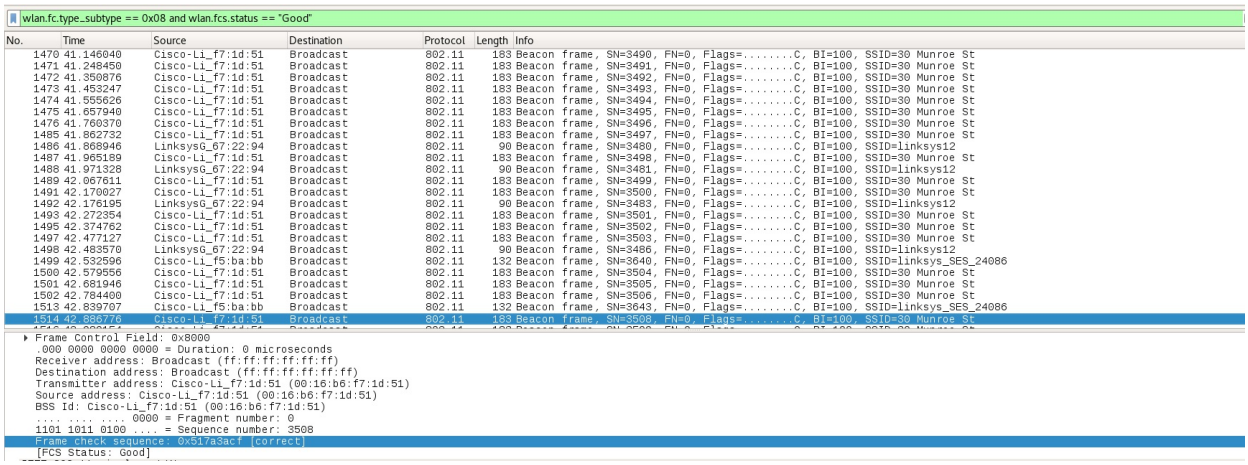


11) Verifique se está a ser usado o método de deteção de erros CRC e se todas as tramas beacon são recebidas corretamente. Justifique o uso de mecanismos de deteção de erros neste tipo de redes locais.

Cada trama inclui um checksum CRC-32.
Se os códigos CRC não são semelhantes, a mensagem contém erros de dados, e o dispositivo poderá realizar ações para corrigir como reler a mensagem ou pedir que a enviem novamente. Sem isto, os dados poderiam ser tratados como corretos e sem erro.
Portanto, sim, nos resultados abaixo podemos ver que isto está a ser verificado.

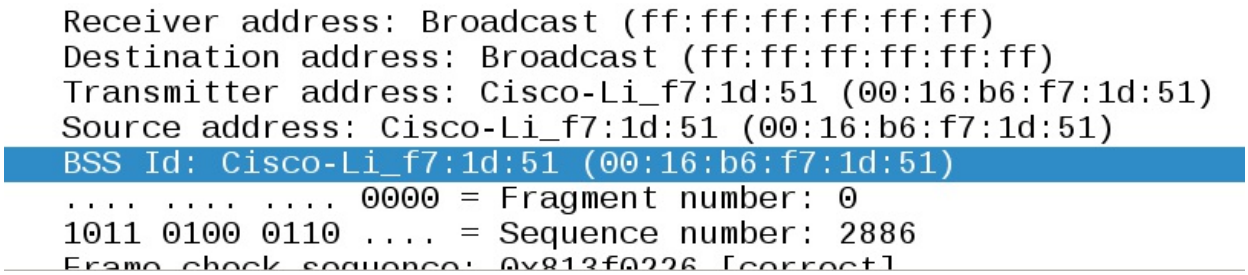


Filtro que apresenta tramas com checksum incorreto



Filtro que apresenta tramas com checksum correto

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.



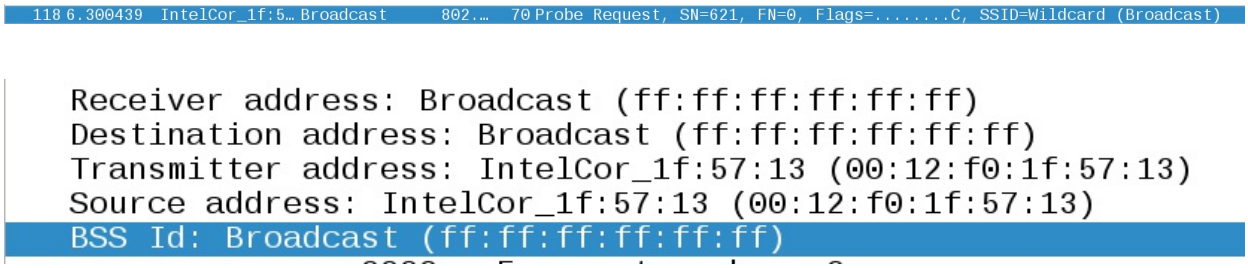
13) Estabeleça um filtro Wireshark apropriado que lhe permita visualizar todas as tramas probing request e probing response, simultaneamente.

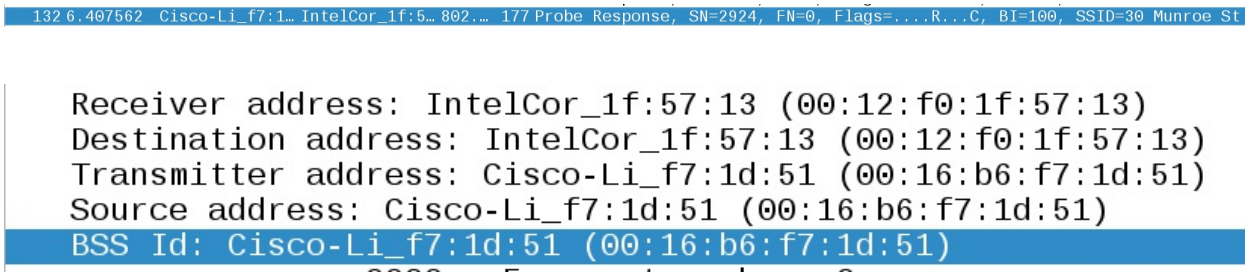
O comando usado foi:

```
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?

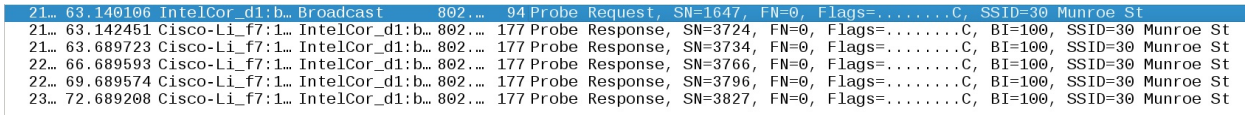
O Probe Request é enviado de uma estação quando requer informações de outra estação.
A Probe Response é enviada de um AP que contém informações de capacidade, taxas de dados suportadas, entre outras, após receber um Probe Request.

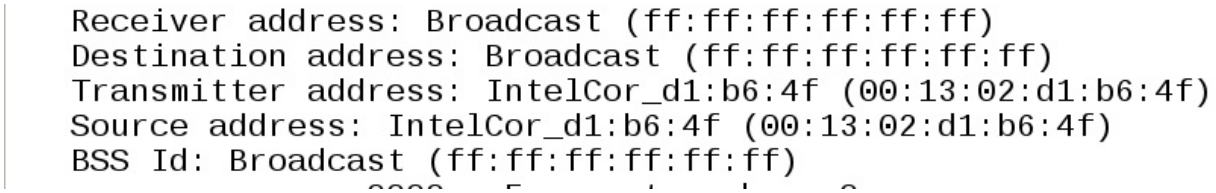




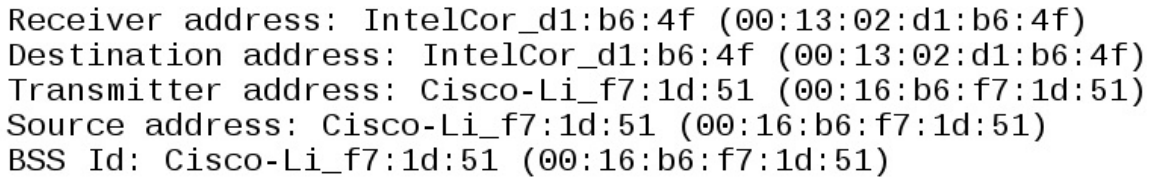
15) Identifique um probing request para o qual tenha havido um probing response. Face ao endereçamento usado, indique a que sistemas são endereçadas estas tramas e explique qual o propósito das mesmas?

Através do Probe Request, a estação solicita informações de um AP específico (especificado pelo SSID), ou de todos os AP's na área (especificados com o SSID Broadcast). Neste caso, verificamos a segunda opção:





A Probe Response é enviada para a estação que requisitou a informação (mostrado nas imagens).



6 - 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?

- 1.

```
17… 49.583615 192.168.1.109  192.168.1.1    DHCP      390 DHCP Release  - Transaction ID 0xea5a526
```

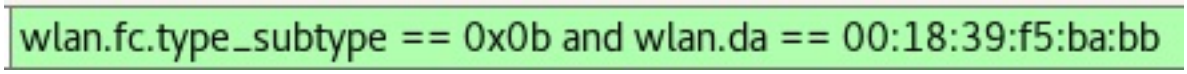
```
▸ Frame 1735: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
▸ Radiotap Header v0, Length 24
▸ 802.11 radio information
▾ IEEE 802.11 Deauthentication, Flags: ........C
    Type/Subtype: Deauthentication (0x000c)
  ▾ Frame Control Field: 0xc000
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      1100 .... = Subtype: 12
    ▾ 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 .... = 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)
    Destination address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Transmitter address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    Source address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
```

- 2.

```
17… 49.609617 IntelCor_d1:b… Cisco-Li_f7:1… 802.11      54 Deauthentication, SN=1605, FN=0, Flags=........C
```

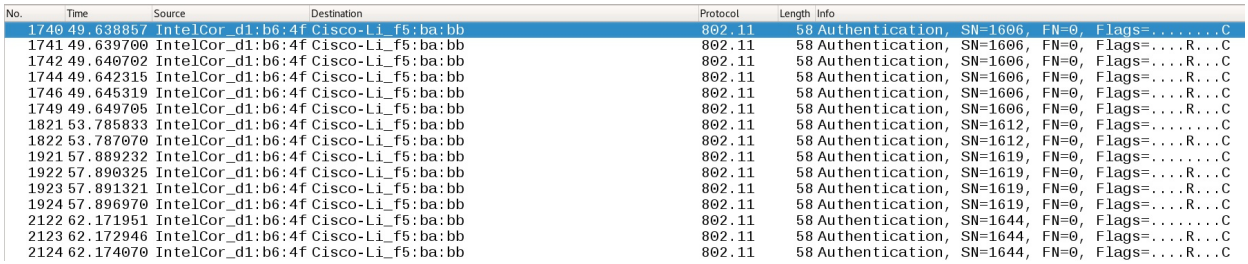
```
▸ Radiotap Header v0, Length 24
▸ 802.11 radio information
▾ IEEE 802.11 Deauthentication, Flags: ........C
    Type/Subtype: Deauthentication (0x000c)
  ▾ Frame Control Field: 0xc000
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      1100 .... = Subtype: 12
    ▾ Flags: 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 .... = 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)
    Destination address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Transmitter address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    Source address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
```

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?



Filtro aplicado no Wireshark

Cerca de 6 tramas aproximadamente ao t=49.

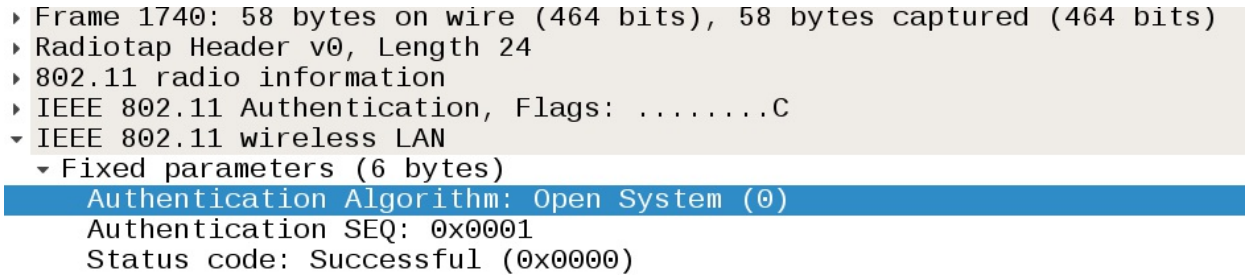


No.	Time	Source	Destination	Protocol	Length	Info
1740	49.638857	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=........C
1741	49.639700	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1742	49.640702	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1744	49.642315	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1746	49.645319	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1749	49.649705	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1821	53.785833	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1612, FN=0, Flags=........C
1822	53.787070	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1612, FN=0, Flags=....R...C
1921	57.889232	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=........C
1922	57.890325	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
1923	57.891321	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
1924	57.896970	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
2122	62.171951	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0, Flags=........C
2123	62.172946	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0, Flags=....R...C
2124	62.174070	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0, Flags=....R...C

Número de tramas mostradas após ser aplicado o filtro

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

Autenticação aberta.



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

Não se verifica resposta.

No.	Time	Source	Destination	Protocol	Length	Info
17…	49.638857	IntelCor_d1:b…	Cisco-Li_f5:b…	802.11	58	Authentication, SN=1606, FN=0, Flags=.......C
17…	49.639700	IntelCor_d1:b…	Cisco-Li_f5:b…	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
17…	49.640702	IntelCor_d1:b…	Cisco-Li_f5:b…	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
17…	49.642315	IntelCor_d1:b…	Cisco-Li_f5:b…	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
17…	49.645319	IntelCor_d1:b…	Cisco-Li_f5:b…	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
17…	49.649705	IntelCor_d1:b…	Cisco-Li_f5:b…	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
18…	53.785833	IntelCor_d1:b…	Cisco-Li_f5:b…	802.11	58	Authentication, SN=1612, FN=0, Flags=.......C
18…	53.787070	IntelCor_d1:b…	Cisco-Li_f5:b…	802.11	58	Authentication, SN=1612, FN=0, Flags=....R...C
19…	57.889232	IntelCor_d1:b…	Cisco-Li_f5:b…	802.11	58	Authentication, SN=1619, FN=0, Flags=.......C
19…	57.890325	IntelCor_d1:b…	Cisco-Li_f5:b…	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
19…	57.891321	IntelCor_d1:b…	Cisco-Li_f5:b…	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
19…	57.896970	IntelCor_d1:b…	Cisco-Li_f5:b…	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
21…	62.171951	IntelCor_d1:b…	Cisco-Li_f5:b…	802.11	58	Authentication, SN=1644, FN=0, Flags=.......C
21…	62.172946	IntelCor_d1:b…	Cisco-Li_f5:b…	802.11	58	Authentication, SN=1644, FN=0, Flags=....R...C
21…	62.174070	IntelCor_d1:b…	Cisco-Li_f5:b…	802.11	58	Authentication, SN=1644, FN=0, Flags=....R...C
21…	63.168087	IntelCor_d1:b…	Cisco-Li_f7:1…	802.11	58	Authentication, SN=1647, FN=0, Flags=.......C
21…	63.169071	Cisco-Li_f7:1…	IntelCor_d1:b…	802.11	58	Authentication, SN=3726, FN=0, Flags=.......C
21…	63.169707	IntelCor_d1:b…	Cisco-Li_f7:1…	802.11	58	Authentication, SN=1647, FN=0, Flags=....R...C
21…	63.170692	Cisco-Li_f7:1…	IntelCor_d1:b…	802.11	58	Authentication, SN=3727, FN=0, Flags=.......C

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?

Aparece uma trama Authentication de 00:13:02:d1:b6:4f para 00:16:b7:f7:1d:51, no *t = 63.168087*.

21…	63.168087	IntelCor_d1:b…	Cisco-Li_f7:1…	802.11	58	Authentication, SN=1647, FN=0, Flags=.......C

```
▾ IEEE 802.11 Authentication, Flags: .......C
    Type/Subtype: Authentication (0x000b)
  ▸ Frame Control Field: 0xb000
    .000 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Destination address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Transmitter address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    Source address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    .... .... .... 0000 = Fragment number: 0
    0110 0110 1111 .... = Sequence number: 1647
    Frame check sequence: 0x47e8cbe0 [correct]
    [FCS Status: Good]
```

A resposta é enviada no *t = 63.169071*.

21…	63.169071	Cisco-Li_f7:1…	IntelCor_d1:b…	802.11	58	Authentication, SN=3726, FN=0, Flags=.......C

```
▾ IEEE 802.11 Authentication, Flags: ........C
    Type/Subtype: Authentication (0x000b)
  ▸ Frame Control Field: 0xb000
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    Destination address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Source address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    .... .... .... 0000 = Fragment number: 0
    1110 1000 1110 .... = Sequence number: 3726
    Frame check sequence: 0x93eaefc9 [correct]
    [FCS Status: Good]
```

Filtro usado:

wlan.fc.subtype == 11

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

O ASSOCIATE REQUEST do host para o AP 30 Munroe St aparece aos 63.169910s e foi respondido aos 63.192101s.

```
21… 63.169910 IntelCor_d1:b… Cisco-Li_f7:1… 802.11     89 Association Request, SN=1648, FN=0, Flags=........C, SSID=30 Munroe St
21… 63.192101 Cisco-Li_f7:1… IntelCor_d1:b… 802.11     94 Association Response, SN=3728, FN=0, Flags=........C
```

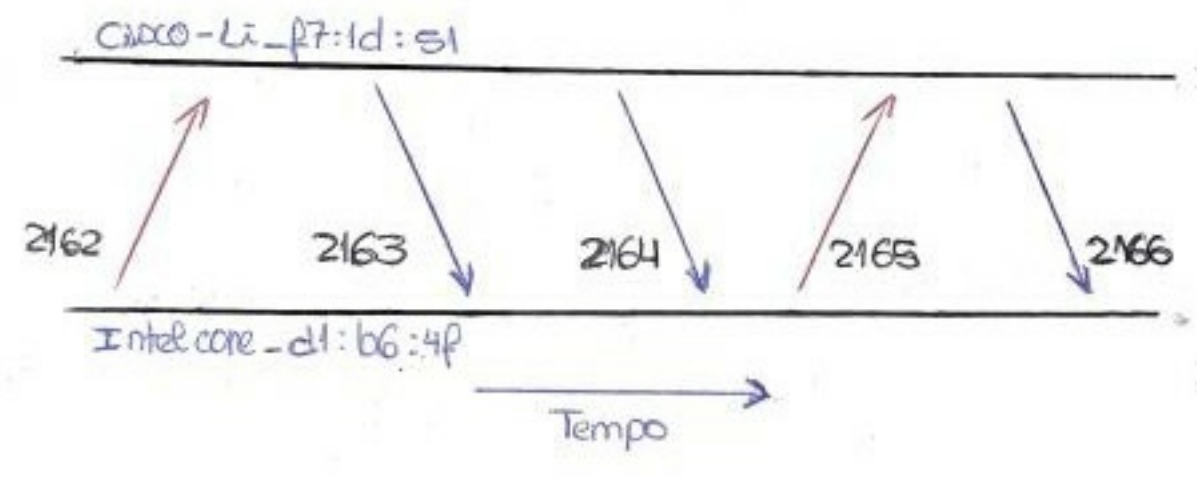
22) Que taxas de transmissão o host está disposto a usar? E o AP?

```
▾ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18, [Mbit/sec]
```

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.

```
21… 63.169910 IntelCor_d1:b… Cisco-Li_f7:1… 802.11     89 Association Request, SN=1648, FN=0, Flags=........C, SSID=30 Munroe St
21… 63.170008                IntelCor_d1:b… 802.11     38 Acknowledgement, Flags=........C
21… 63.170692 Cisco-Li_f7:1… IntelCor_d1:b… 802.11     58 Authentication, SN=3727, FN=0, Flags=........C
21… 63.171000                Cisco-Li_f7:1… 802.11     38 Acknowledgement, Flags=........C
21… 63.192101 Cisco-Li_f7:1… IntelCor_d1:b… 802.11     94 Association Response, SN=3728, FN=0, Flags=........C
```

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



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 MAC adresses são 00:13:02:d1:b6:4f, 00:16:b6:f4:eb:a8 e 00:16:b6:f7:1d:51.

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		IntelCor_d1:b…	802.11	38	Acknowledgement, Flags=........C
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		Cisco-Li_f7:1…	802.11	38	Acknowledgement, Flags=........C
478	24.828024	192.168.1.109	128.119.245.12	TCP	102	2538 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
479	24.828140		IntelCor_d1:b…	802.11	38	Acknowledgement, Flags=........C
480	24.828253	192.168.1.109	128.119.245.12	HTTP	537	GET /wireshark-labs/alice.txt HTTP/1.1

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?

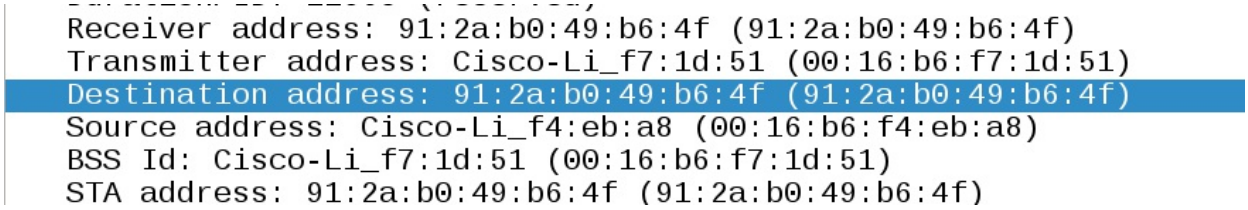
O MAC adress do host é 00:13:02:d1:b6:4f, o do AP é 00:16:b6:f7:1d:51 e o do router do primeiro salto é 00:16:b6:f4:eb:a8. O endereço IP do host é 192.168.1.109 e o endereço IP de destino é 128.119.245.12.

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

Sabemos que não corresponde ao host porque o host somos nós, sabemos também que não é o AP porque o ap não tem um IP e nao é o router porque este nao faz parte da nossa rede. Concluímos assim que corresponde a outro equipamento de rede.

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?

Os três campos de MAC adress são 00:16:b6:f4:eb:a8, 00:16:b6:f7:1d:51 e 91:2a:b0:49:b6:4f.



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

O MAC adress que corresponde ao host é 00:16:b6:f4:eb:a8.O MAC adress que corresponde ao AP é 00:16:b6:f7:1d:51. O MAC adress que corresponde ao router do primeiro 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.

Corresponde. Na pergunta 28 descobrimos qual o host(MAC adress de origem), na pergunta 29 descobrimos qual o endereço IP do dispositivo que enviou o segmento TCP e concluímos que é o mesmo.

Conclusões

Com este trabalho expandimos o nosso conhecimento acerca de redes sem fios. Aprofundamos o nosso conhecimento sobre tramas de gestão, que nos permitem analisar as comunicações entre STA's(estações) e AP's.

As tramas de gestão que exploramos foram, authentication, association request e response, beacon, e probe request e response.

As tramas de dados permitiram-nos analisar os vários pacotes e recolher informção importante sobre a gestão da rede.

Este trabalho ajudou-nos a perceber melhor sobre diferentes conceitos e a consolidar o conhecimento dos protocolos, aplicando filtros no wireshark.