Universidade do Minho
Mestrado Integrado em Engenharia Informática

Redes de Computadores

TP4, Redes Sem Fios (802.11)

Henrique Paz (A84372), Joana Afonso Gomes (A84912), João Neves (A81366)

Dezembro 2019

1 Acesso Rádio

Nota: a nossa trama é **1107**.

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

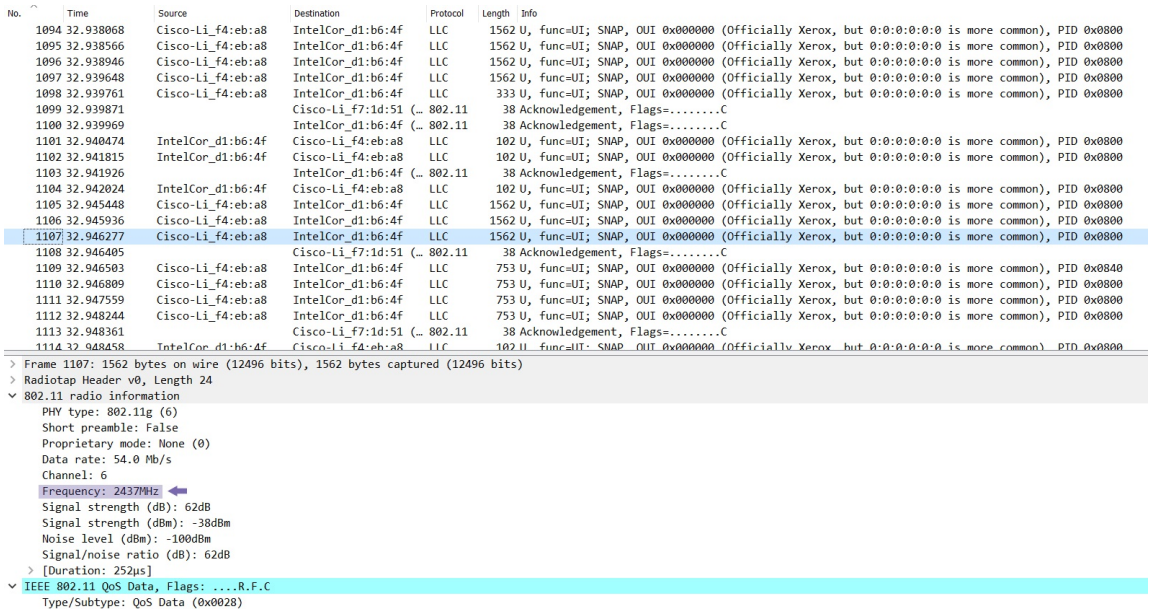


Figura 1

A frequência do espetro é **2437Hz** e o canal que corresponde a essa frequência é **6**.

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

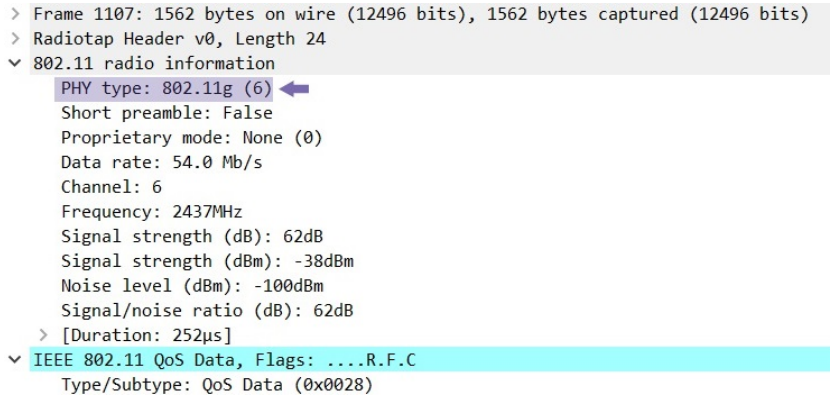


Figura 2

A versão que está a ser usada é 802.11g.

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.**

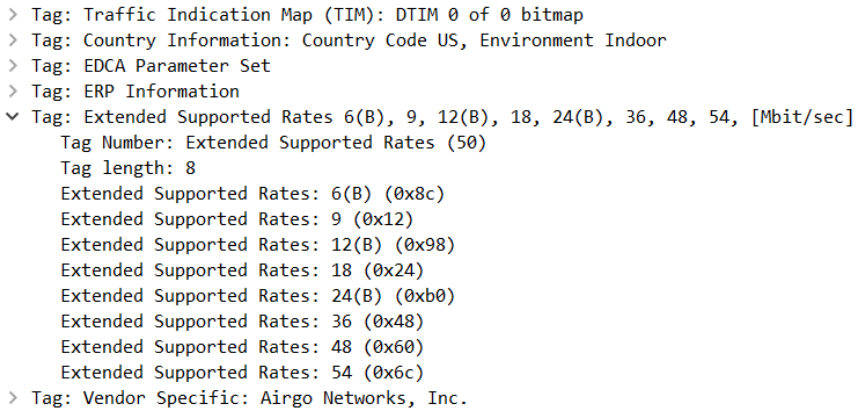


Figura 3

Na Figura 3 podemos observar que a trama foi enviada com um débito de 54Mb/s.
A partir da Figura 3 podemos concluir que o débito máximo a que a interface pode operar é 54Mb/s. Assim, concluímos que o débito enviado a trama corresponde ao débito máximo a que a interface pode operar.

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 de *beacon* são **30 Munroe St** é **linksys_ses_24086**.

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.**

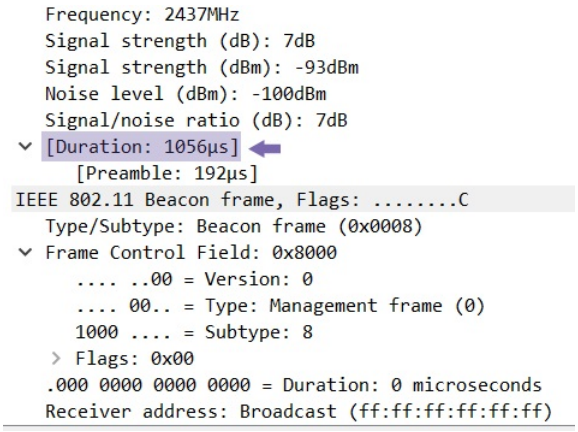


Figura 4

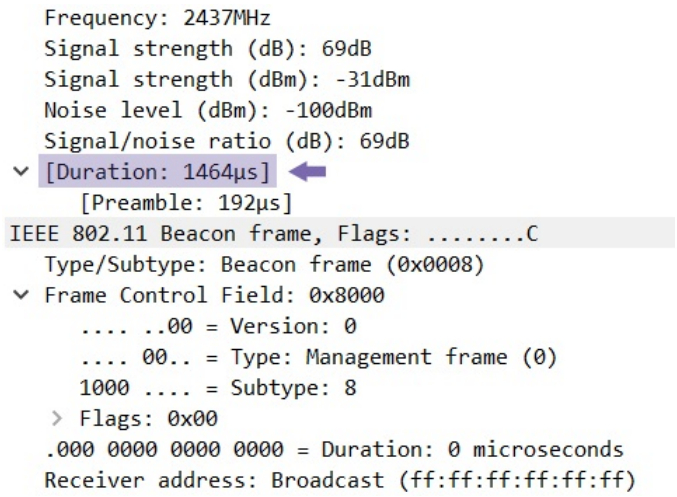


Figura 5

Como podemos observar nas Figuras 5 e 6, o intervalo de tempo entre a

transmissão de tramas beacon para o AP linksys_ses_24086 é 10564] e para o AP 30 Munroe St 1464.

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.**

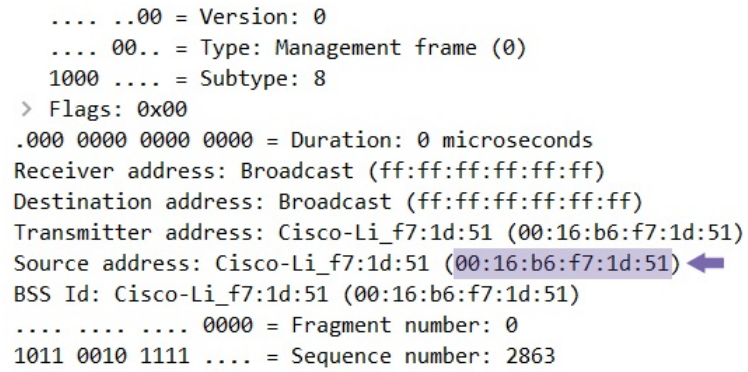


Figura 6

O endereço MAC de origem da trama beacon de 30 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??**

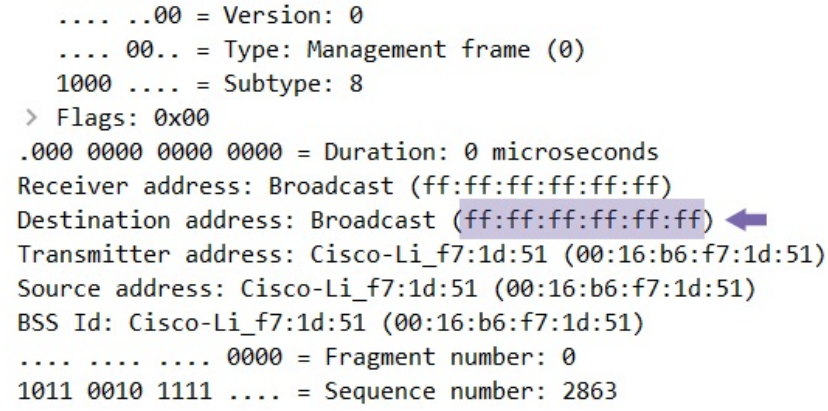


Figura 7

O endereço MAC de destino na trama de 30 Munroe St é **ff:ff:ff:ff:ff:ff**.

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

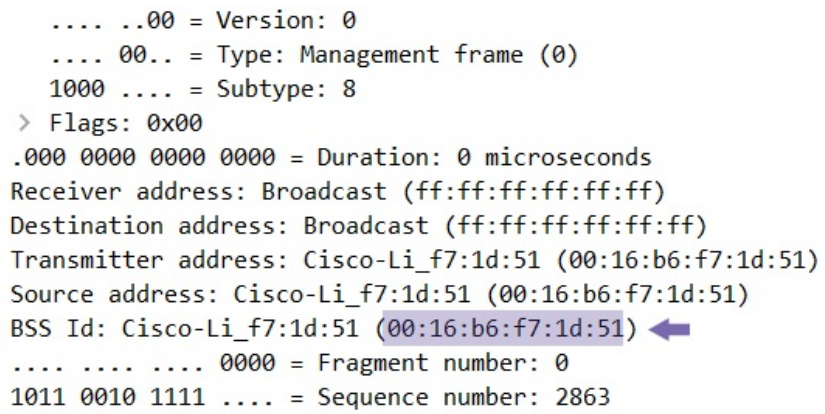


Figura 8

O MAC BSS ID da trama beacon de 30 Munroe St 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?**

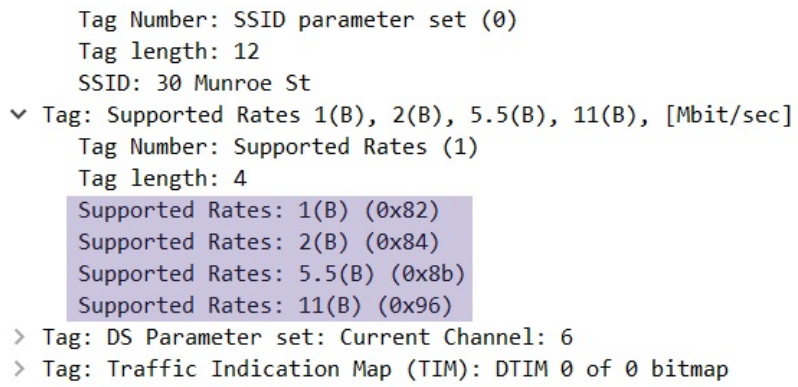


Figura 9

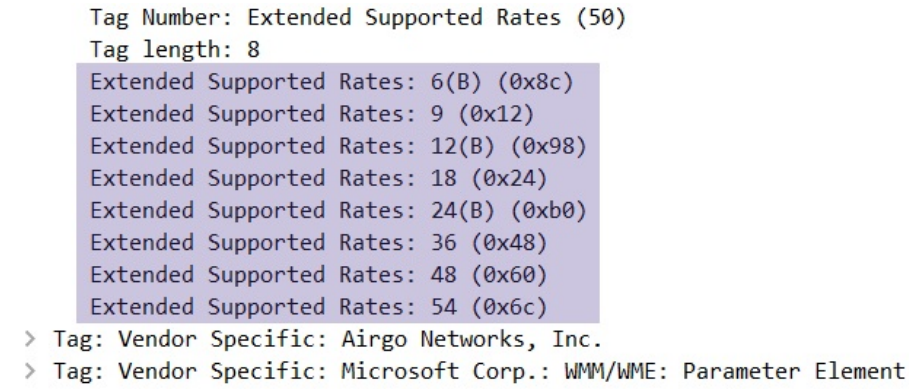


Figura 10

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)?**

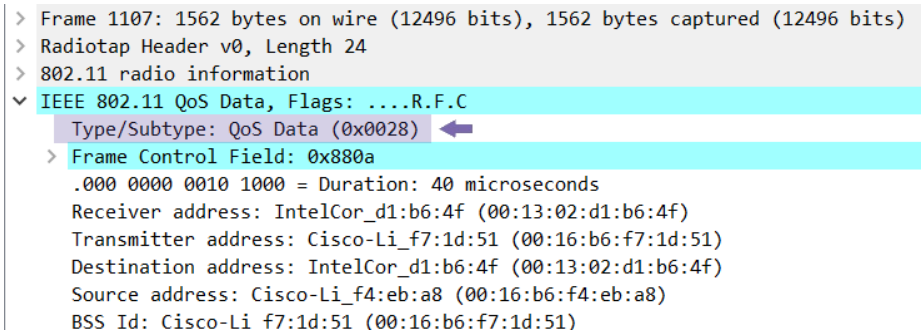


Figura 11

A trama que selecionamos é 1107. Esta trama pertence ao tipo Data. O valor dos seus identificadores de tipo e subtipo é QoS Data (0x0028). Estão especificadas na parte do cabeçalho correspondente ao IEEE 802.11 QoS Data, Flags. (...).

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.**

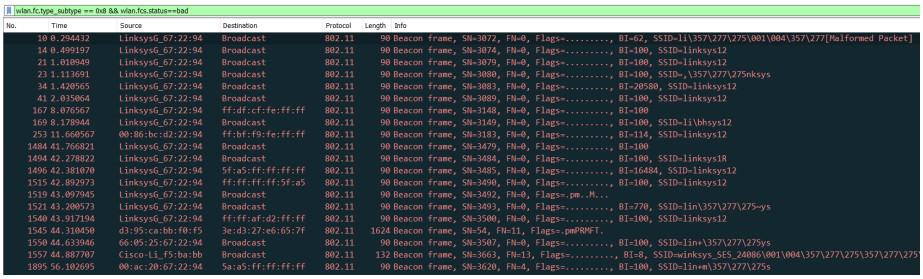


Figura 12: Resultado da aplicação do filtro.

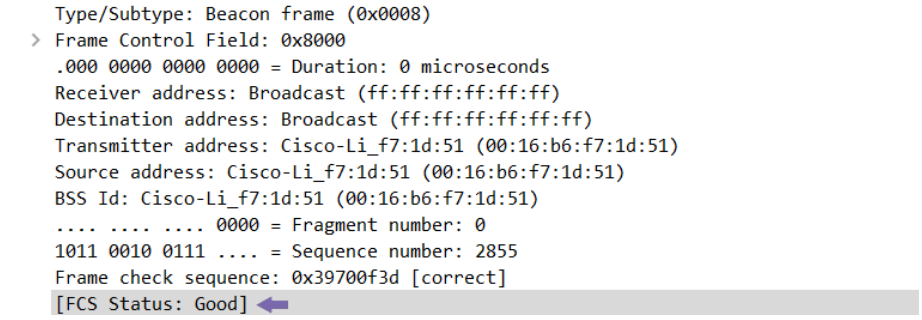


Figura 13: Trama Beacon sem erros.

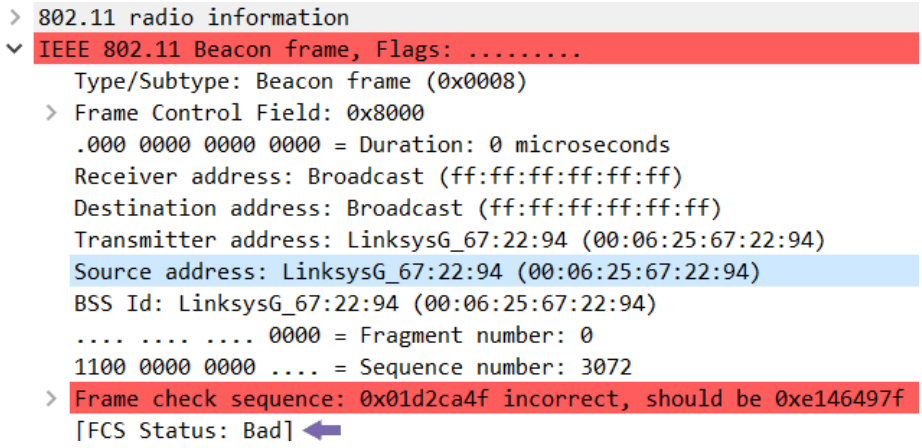


Figura 14: Trama Beacon com erros.

Inicialmente, usamos um filtro para verificar se todas as tramas Beacon são recebidas corretamente, e verificamos que nem todas são (Figura 13). Acima destacamos as diferenças entre uma trama Beacon sem erros (Figura 14) e uma trama com erros (Figura 15). O método de deteção de erros CRC é usado no campo *Frame Check Sequence*, mostrando o status (se for recebida corretamente ***Good***, caso contrário, ***Bad***). O uso de mecanismos de deteção de erros tem uma grande importância no que toca à manutenção da integridade dos dados em canais com ruído e em sistemas de armazenamento não imunes a falhas.

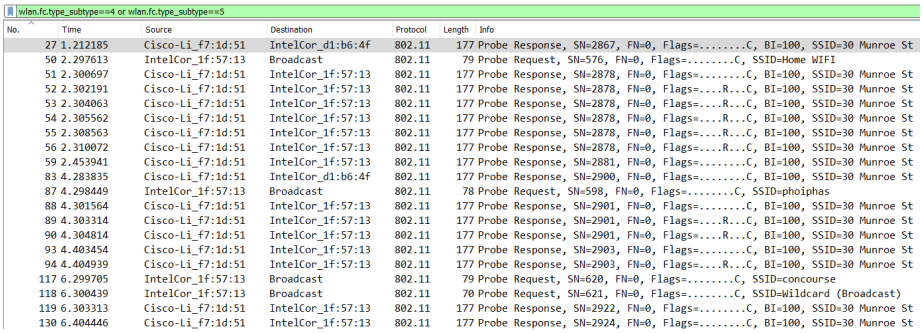
12) **Identifique e registe todos os endereços MAC usados nas tramas beacon enviadas pelos APs. Recorde que o endereçamento está definido no cabeçalho das tramas 802.11 podendo ser utilizados até quatro endereços com diferente semântica. Para uma descrição detalhada da estrutura da trama 802.11, consulte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

```
> RX flags: 0x6054
> 802.11 radio information
v 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 1000 .... = Sequence number: 2856
    Frame check sequence: 0xe5bf6054 [correct]
```

Figura 15

Como podemos ver na Figura 16, nas tramas Beacon enviadas pelos APs estão os registos **Receiver Address**, **Destination Address**, **Transmitter Address** e **Sourse Address**. O Receiver Address e o Destination Address têm valor ff:ff:ff:ff:ff:ff (*broadcast address*), e o Transmitter address e o Source Address têm o mesmo valor (00:16:b6:f7:1d:51). .

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



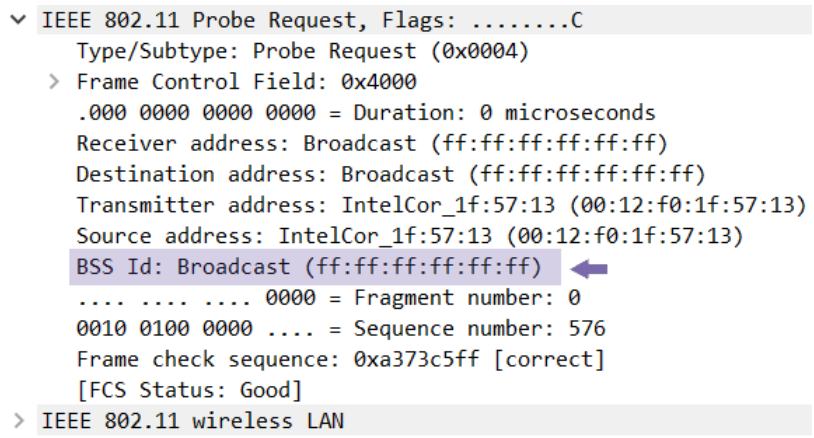
wlan.fc.type_subtype==4 or wlan.fc.type_subtype==5

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	2.300697	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=....R...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=....R...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=....R...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=....R...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=....R...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=phoiphas
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=....R...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=....R...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=....R...C, BI=100, SSID=30 Munroe St
117	6.299705	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	70	Probe Request, SN=621, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
119	6.303313	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2922, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
130	6.404446	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2924, FN=0, Flags=........C, BI=100, SSID=30 Munroe St

Figura 16

Aplicamos o filtro wlan.fc.type_subtype==0x4 or wlan.fc.type_subtype==0x5 dado que as tramas probing request e probring response têm subtipo 4 e 5, respetivamente.

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



```
IEEE 802.11 Probe Request, Flags: ........C
    Type/Subtype: Probe Request (0x0004)
  > Frame Control Field: 0x4000
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Transmitter address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
    Source address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
    BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
    .... .... .... 0000 = Fragment number: 0
    0010 0100 0000 .... = Sequence number: 576
    Frame check sequence: 0xa373c5ff [correct]
    [FCS Status: Good]
> IEEE 802.11 wireless LAN
```

Figura 17: Endereço MAC BSS ID de origem.

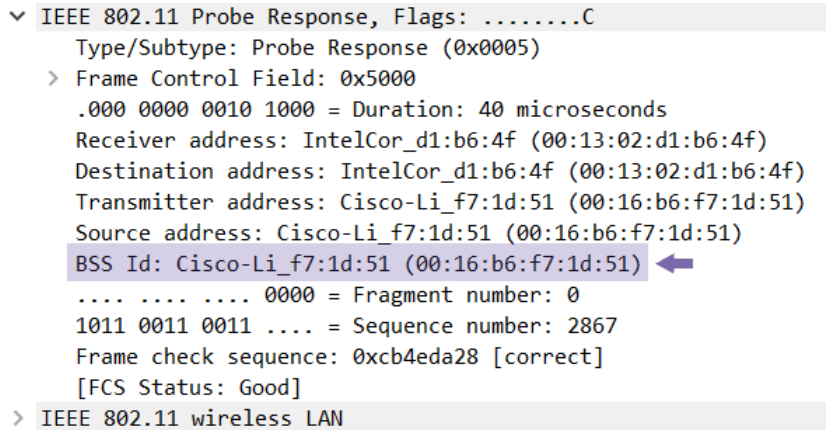


Figura 18: Endereço MAC BSS ID de destino.

Na Figura 19 está endereço MAC BSS ID de origem e na Figura 19 o endereço MAC BSS ID de destino.

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?**

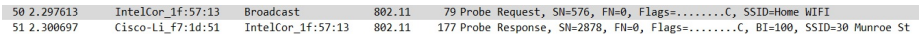
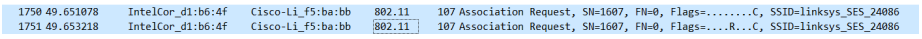


Figura 19

É possível verificar que a trama 50 representa um *probing request* e a 51 é a *probing response* correspondente.
A *frame* 50 é uma STA (IntelCor_1f:57:13), que é emitida para todos os equipamentos da rede, de modo a encontrar um AP.
A trama 51, por sua vez, é a resposta do AP (Cisco-Li_f7:1d:51) para a STA.

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?**



1750	49.651078	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1607, FN=0, Flags=.......C, SSID=linksys_SES_24086
1751	49.653218	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1607, FN=0, Flags=....R...C, SSID=linksys_SES_24086

Figura 20

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
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
2160	63.169707	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58	Authentication, SN=1647, FN=0, Flags=....R...C
2164	63.170692	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58	Authentication, SN=3727, FN=0, Flags=.......C

Figura 21: Tramas enviadas do host para o AP linksys_ses_24086

Foram enviadas 17 mensagens de *authentication* do host para o AP .

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

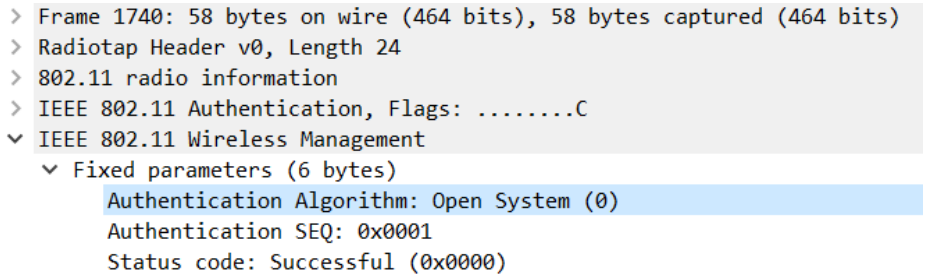


Figura 22

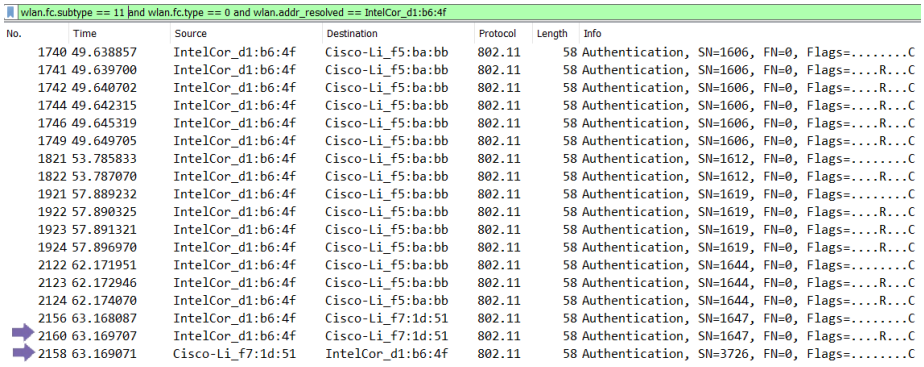
O tipo de autenticação pretendida pelo host é aberta.

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

Figura 23

Como podemos constatar na figura 23, observamos resposta de authentication 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?**



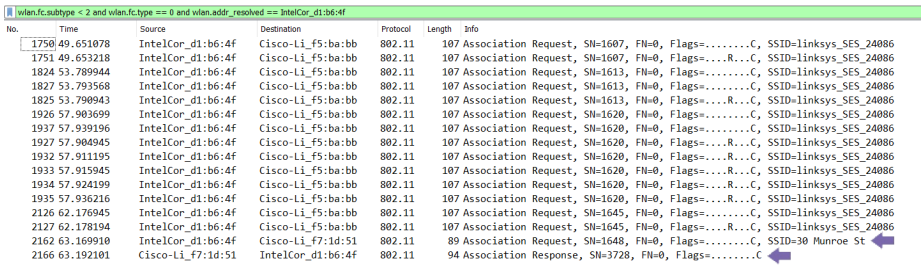
wlan.fc.subtype == 11 and wlan.fc.type == 0 and wlan.addr_resolved == IntelCor_d1:b6:4f

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
2156	63.168087	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58	Authentication, SN=1647, 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
2158	63.169071	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58	Authentication, SN=3726, FN=0, Flags=........C

Figura 24

Há uma *authentication* do host para o AP 30 Munroe St. quando t = 63.169071. A resposta do AP para o host aparece a t = 63.170692.

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 ?**



wlan.fc.subtype < 2 and wlan.fc.type == 0 and wlan.addr_resolved == IntelCor_d1:b6:4f

No.	Time	Source	Destination	Protocol	Length	Info
1750	49.651078	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1607, FN=0, Flags=........C, SSID=linksys_SES_24086
1751	49.653218	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1607, FN=0, Flags=....R...C, SSID=linksys_SES_24086
1824	53.789944	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1613, FN=0, Flags=........C, SSID=linksys_SES_24086
1827	53.793568	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1613, FN=0, Flags=........C, SSID=linksys_SES_24086
1825	53.790943	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1613, FN=0, Flags=....R...C, SSID=linksys_SES_24086
1926	57.903699	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=........C, SSID=linksys_SES_24086
1937	57.939196	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=........C, SSID=linksys_SES_24086
1927	57.904945	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=....R...C, SSID=linksys_SES_24086
1932	57.911195	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=....R...C, SSID=linksys_SES_24086
1933	57.915945	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=....R...C, SSID=linksys_SES_24086
1934	57.924199	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=....R...C, SSID=linksys_SES_24086
1935	57.936216	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=....R...C, SSID=linksys_SES_24086
2126	62.176945	IntelCor_d1:b6:4f	Cisco-Li_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-Li_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-Li_f7:1d:51	802.11	89	Association Request, SN=1648, FN=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, FN=0, Flags=........C

Figura 25

Há um *associate request* do host para o AP 30 Munroe St. quando t = 63.169910, cuja resposta aparece a t = 63.192101.

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

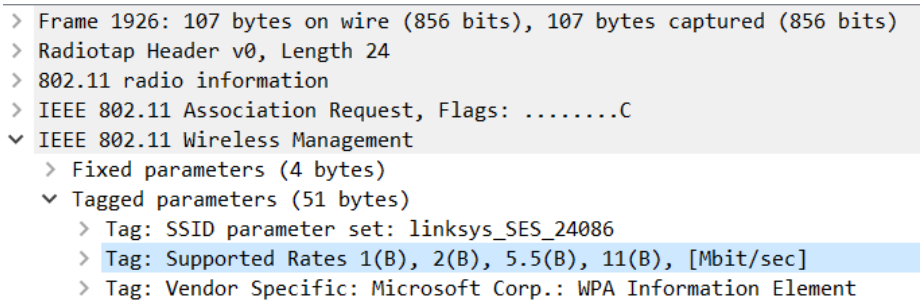


Figura 26

Como podemos ver na Figura 26, as taxas que o host está disposto a usar são 1, 2, 5.5 e 11 Mbps.

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.**

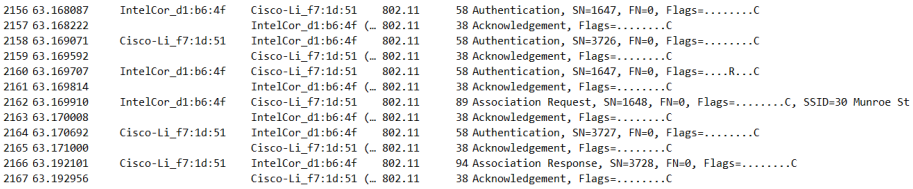


Figura 27

- Primeiramente, na trama **2156**, há uma autenticação da STA;
- Nas trama **2157** e **2158**, há um reconhecimento da receção da autenticação da STA e uma *authentication* do AP;

- Nas tramas **2159** e **2162** dá-se *acknowledgement* pelo STA, que faz um *request* de *association* ao AP. (Nota:nesta parte aparentou-nos haver uma duplicação de autenticações e, por recomendação, decidimos ignorar essa replicação.);
- Nas tramas **2163** e **2164**, há envio de uma trama *acknowledgement* pelo AP e o AP faz um *association request* ao STA;
- Na **2165** e na **2166** a STA envia uma trama *Acknowledgement* e o AP responde ao *association request* com um *association response*;
- Por fim, na trama **2167**, o STA "informa" o *aknowledgment* da resposta do AP.

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

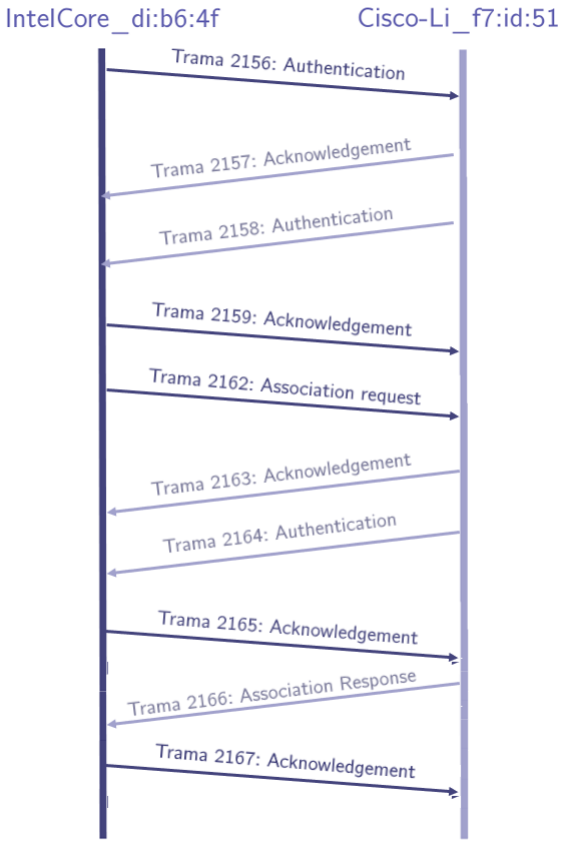


Figura 28

4 Transferência de 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?**

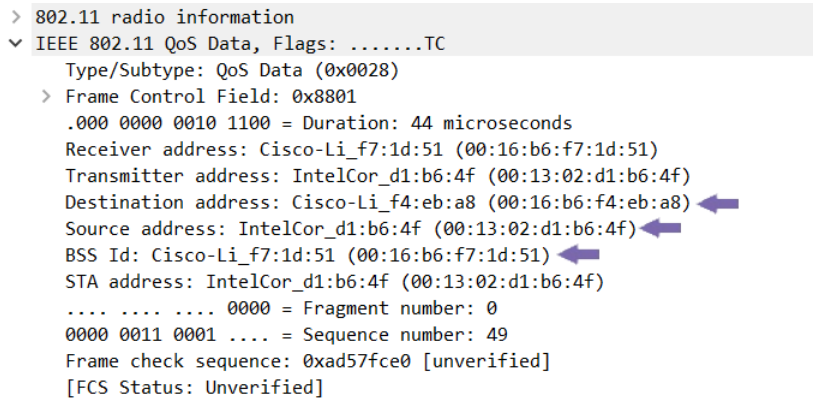


Figura 29 bss id Cisco-li: _f7:1d:51(00:16:b6:f7:1d:51)
source adress IntelCor:_d1:b6:4f(00:13:02:d1:b6:4f)
destination Cisco-Li:_f4:eb:a8(00:16:b6:f4:eb:a8)

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?**

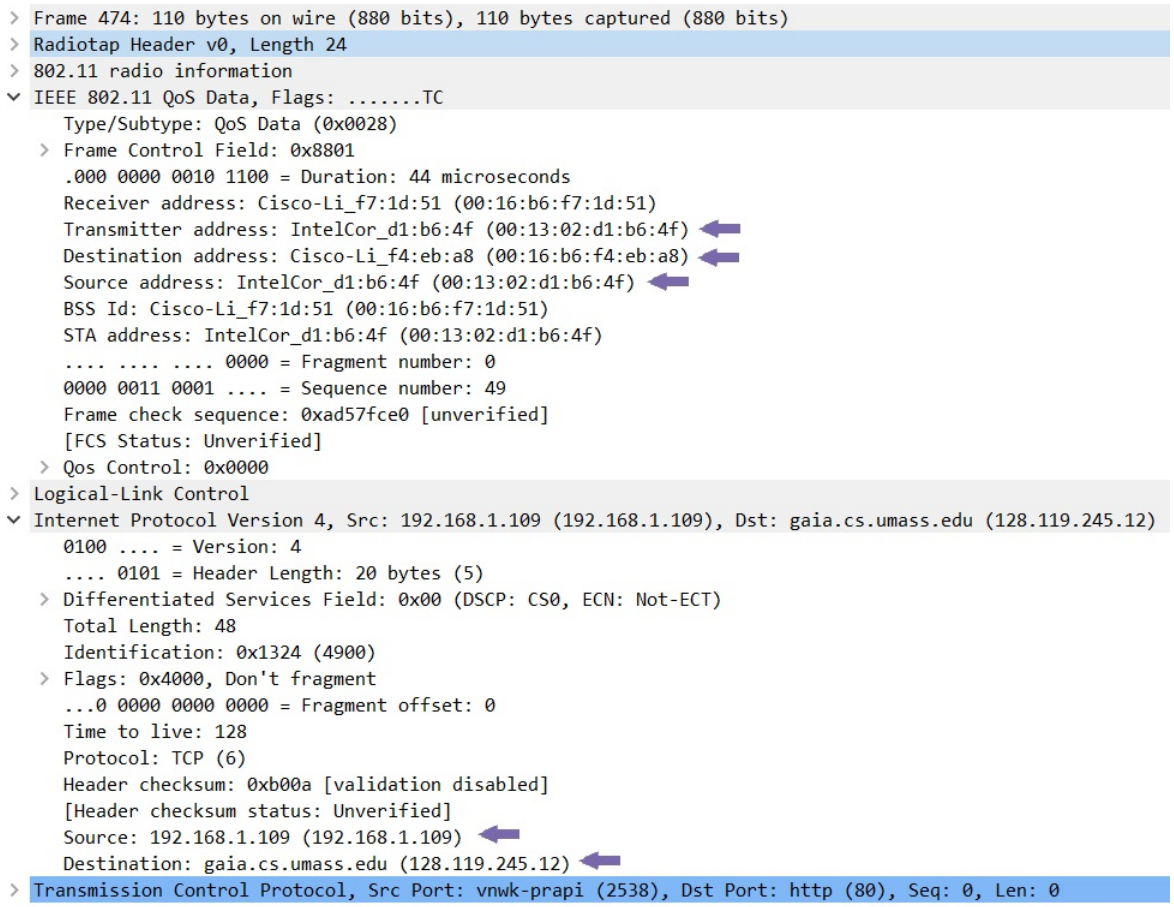


Figura 30 Host: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
AP: - Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)
Primeiro salto: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
IP host que envia segmento: 192.168.1.109
IP de destino: _ 128.119.245.12 (gaia.cs.umass.edu)

-

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

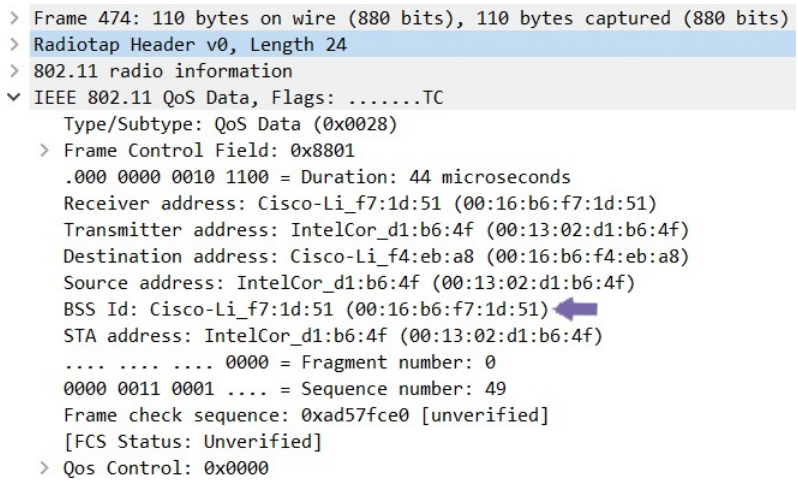


Figura 31 Corresponde a um AP, pois tem um BSS Id.

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?**

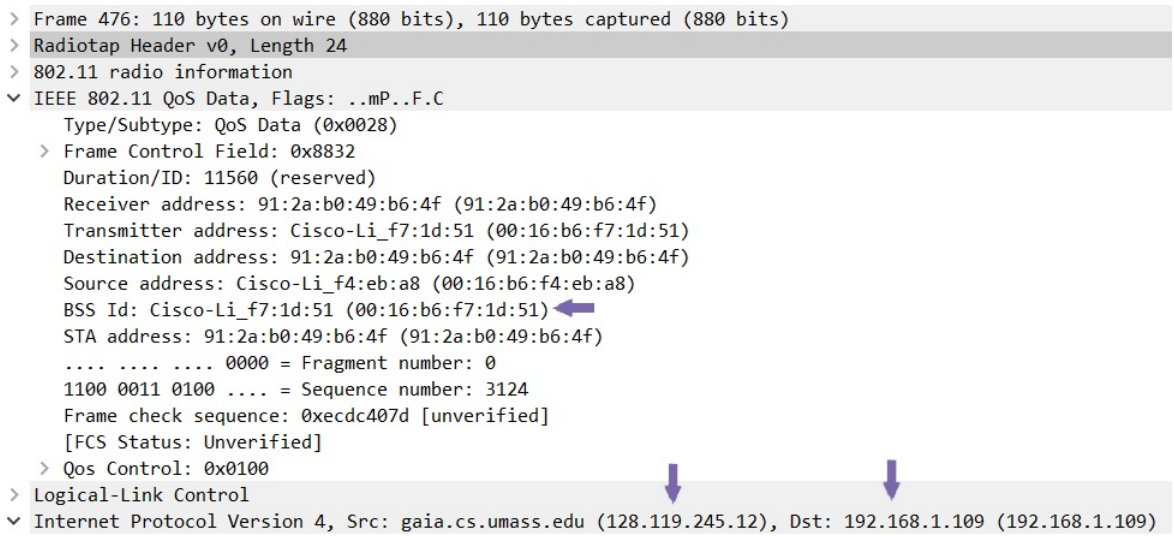


Figura 32

BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)

Destination: 91:2a:b0:4:b6:4f
Source: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)

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

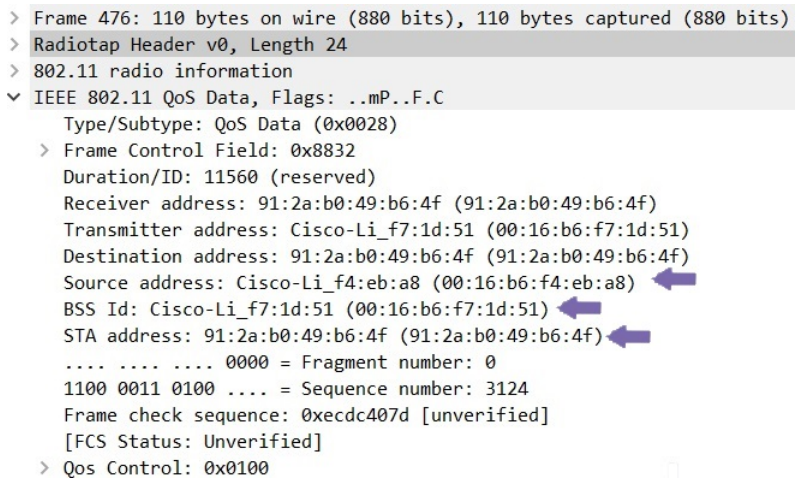


Figura 33 Host: STA (91:2a:b0:19:b6:4f) AP: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8) Router do primeiro salto: Cisco-Li1_f7:1d:51 (00:16:b6:f7:1d:51).

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

O MAC *address* na trama não corresponde ao endereco IP do dispositivo que enviou o segmento tcp encapsulado no datagrama, pois o endereço IP TCP SYNACK é 128.119.245.12. No entanto, o endereço IP de destino é 192.168.1.109.

5 Conclusão

Neste trabalho tivemos a oportunidade de desenvolver várias capacidades de análise relativamente a vários protocolos, nomeadamente o protocolo IEEE 802.11. Para a análise do protocolo enunciado, recorremos ao *Wireshark.*
Desta forma foram propostos vários tipos de análise em relação ao protocolo proposto, como por exemplo, o acesso Rádio, que consiste na informação a nível físico, que pertence á sequência de *bytes* capturada, o *Scanning.* O *Scanning* filtra a nossa análise num tipo específico de tramas, isto é, as tramas *beacon* que permitem efetuar o *scanning* passivo em redes Wi-Fi e também as tramas *probe request* e *probe response* que correspondem ao *scanning* ativo.
Para além destes, foi nos proposto também uma análise de processos de associação onde um *host* deve associar-se a um ponto de acesso antes de enviar dados(análise de tramas *association request* do *host* e *association response* enviado pelo AP).
Por fim, procedemos ao estudo de tramas de transferência disponibilizadas, juntamente com as tramas de dados de associação, que têm como objetivo o controlo da transferência de dados.
Em suma, ao longo destes projetos, foram esclarecidos muitos conceitos que eram para nós ainda abstratos, ficando a certeza que serão aproveitados no futuro.