

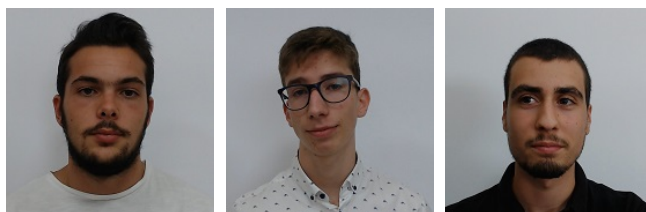


Universidade do Minho  
Mestrado Integrado em Engenharia Informática  
3ºano - 1º Semestre

**Redes de Computadores**

## **TP4: Redes Sem Fios (802.11)**

Grupo 1 - PL1



a83732 – Gonçalo Rodrigues Pinto  
a84197 – João Pedro Araújo Parente  
a84829 – José Nuno Martins da Costa

19 de Dezembro de 2019

# Conteúdo

<b>1</b>	<b>Introdução</b>	<b>3</b>
<b>2</b>	<b>Questões e Respostas</b>	<b>3</b>
2.1	Acesso Rádio . . . . .	3
2.2	Scanning . . . . .	4
2.3	Processo de Associação . . . . .	9
2.4	Transferência de Dados . . . . .	14
<b>3</b>	<b>Conclusão</b>	<b>17</b>

## Lista de Figuras

1	Trama com o número 1101. . . . .	3
2	Uma trama beacon para o AP 30 Munroe St. . . . .	4
3	Uma trama beacon para o AP linksys_SES_24086. . . . .	5
4	A trama com número 2101. . . . .	6
5	Uma trama beacon recebida incorrectamente. . . . .	7
6	Filtro Wireshark que permite visualizar todas as tramas probing request e probing response, simultaneamente. . . . .	8
7	Um probing request para o qual houve um probing response. . . . .	9
8	Ações realizados pelo host imediatamente após t=49 ara terminar a associação. . . . .	10
9	Ações realizados pelo host imediatamente após t=49 para a autenticação. . . . .	10
10	Authentication algorithim. . . . .	11
11	Authentication algorithim. . . . .	12
12	Instantes onde aparece o associate request e response. . . . .	12
13	Taxas de transmissão que o host está disposto a usar. . . . .	12
14	Taxas de transmissão que o AP está disposto a usar. . . . .	13
15	Sequência de tramas. . . . .	13
16	Processo de associação. . . . .	14
17	Exemplo de como funciona as tramas 802.11 SYN/ACK/SYNACK. . . . .	14
18	Trama 802.11 que contém o segmento SYN TCP para a primeira sessão TCP. . . . .	15
19	Trama 802.11 que contém o segmento SYNACK para esta sessão TCP. . . . .	16

# 1 Introdução

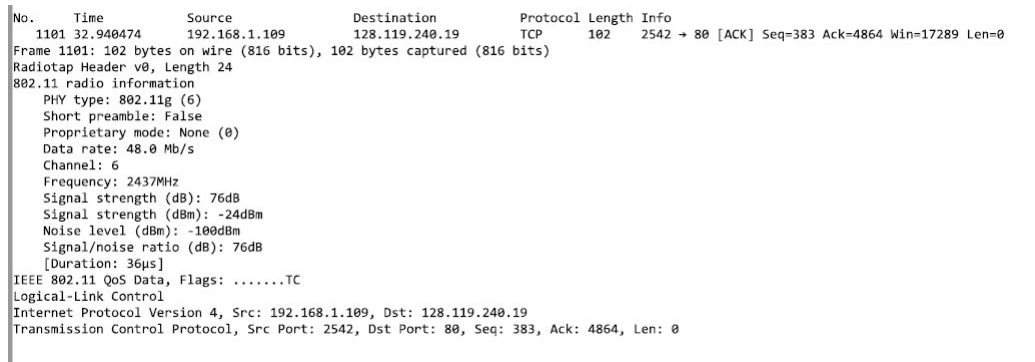
O objectivo deste trabalho foi estudar os vários aspectos do protocolo IEEE 802.11, tais como o formato das tramas, o endereçamento dos componentes envolvidos na comunicação sem fios, os tipos de tramas mais comuns, bem como a operação do protocolo.

## 2 Questões e Respostas

Após descarregar da plataforma de ensino a captura *trace-wlan-tp4-2019.pcap* e posteriormente abertura do ficheiro no software Wireshark. Respondemos às seguintes questões.

### 2.1 Acesso Rádio

Como foi observado, a sequência de bytes capturada inclui informação do nível físico (radio information), para além dos bytes correspondentes a tramas 802.11. Como foi solicitado no enunciado do presente trabalho responde-se as questões abaixo apresentadas tendo em consideração a trama com o número 1101 (turno PL1, grupo 01).



```
No.    Time                Source                Destination            Protocol Length Info
1101  32.940474           192.168.1.109         128.119.240.19         TCP                    102    2542 → 80 [ACK] Seq=383 Ack=4864 Win=17289 Len=0
Frame 1101: 102 bytes on wire (816 bits), 102 bytes captured (816 bits)
Radiotap Header v0, Length 24
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): 76dB
  Signal strength (dBm): -24dBm
  Noise level (dBm): -100dBm
  Signal/noise ratio (dB): 76dB
  [Duration: 36µs]
IEEE 802.11 QoS Data, Flags: .....TC
Logical-Link Control
Internet Protocol Version 4, Src: 192.168.1.109, Dst: 128.119.240.19
Transmission Control Protocol, Src Port: 2542, Dst Port: 80, Seq: 383, Ack: 4864, Len: 0
```

Figura 1: Trama com o número 1101.

- 1. Identificar em que frequência do espectro está a operar a rede sem fios, e o canal que corresponde a essa frequência.**  
A rede sem fios está a operar na frequência 2437MHz do espectro. Esta frequência corresponde ao canal 6.
- 2. Identificar a versão da norma IEEE 802.11 que está a ser usada**  
A versão da norma IEEE 802.11 que está a ser usada é a norma 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.

A trama escolhida tem um débito de 48.0 Mb/s. Este débito não corresponde ao débito máximo a que interface Wi-Fi pode operar pois como foi dito anteriormente a norma utilizada é 802.11g e esta norma só permite atingir débitos até 54Mb/s, ou seja, o débito registado encontra-se abaixo do débito máximo.

## 2.2 Scanning

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

```
No.      Time          Source           Destination      Protocol Length Info
1500 42.579556 Cisco-Li_f7:1d:51 Broadcast         802.11 183 Beacon frame, SN=3504, FN=0, Flags=.....C,
BI=100, SSID=30 Munroe St
Frame 1500: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits)
Radiotap Header v0, Length 24
802.11 radio information
IEEE 802.11 Beacon frame, Flags: .....C
Type/Subtype: Beacon frame (0x0008)
Frame Control Field: 0x8000
.000 0000 0000 0000 = Duration: 0 microseconds
Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
Source address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
.... .... 0000 = Fragment number: 0
1101 1011 0000 .... = Sequence number: 3504
Frame check sequence: 0xa028b529 [unverified]
[FCS Status: Unverified]
IEEE 802.11 wireless LAN
Fixed parameters (12 bytes)
Timestamp: 174361600386
Beacon Interval: 0.102400 [Seconds]
Capabilities Information: 0x0601
Tagged parameters (119 bytes)
Tag: SSID parameter set: 30 Munroe St
Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
Tag: DS Parameter set: Current Channel: 6
Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
Tag: Country Information: Country Code US, Environment Indoor
Tag: EDCA Parameter Set
Tag: ERP Information
Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
Tag: Vendor Specific: Airgo Networks, Inc.
Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
```

Figura 2: Uma trama beacon para o AP 30 Munroe St.

```

No.      Time           Source           Destination      Protocol Length Info
 1513  42.839707      Cisco-Li_f5:ba:bb Broadcast         802.11    132 Beacon frame, SN=3643, FN=0, Flags=.....C,
BI=100, SSID=linksys_SES_24086
Frame 1513: 132 bytes on wire (1056 bits), 132 bytes captured (1056 bits)
Radiotap Header v0, Length 24
802.11 radio information
IEEE 802.11 Beacon frame, Flags: .....C
IEEE 802.11 wireless LAN
Fixed parameters (12 bytes)
  Timestamp: 6351964365199
  Beacon Interval: 0.102400 [Seconds]
  Capabilities Information: 0x0011
Tagged parameters (68 bytes)

```

Figura 3: Uma trama beacon para o AP linksys\_SES\_24086.

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 e 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? Na prática, a periodicidade de tramas beacon é verificada? Tente explicar porquê.**

O intervalo de tempo entre a transmissão de tramas beacon para o AP linksys\_ses\_2406 é 0.102400s. E o intervalo de tempo entre a transmissão de tramas beacon para o AP 30 Munroe St é também 0.102400s. Este intervalo de tempo entre as tramas beacon é um parâmetro configurável nos APs, por defeito está configurado a 0.102400s ou 100TU (sendo que  $TU = 1024E-6$ ), neste caso em particular é evidente que os APs estão configurados a 100TU, a periodicidade entre as tramas vai ser verificada dado que a comunicação tem de ser feita em intervalos múltiplos de TU dado que estes são mais fáceis de implementar em hardware com 1MHz de período de relógio.

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 30Munroe St em notação hexadecimal 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 de destino na trama de 30 Munroe St é ff:ff:ff:ff:ff:ff, o que equivale a broadcast.

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

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?

As quatro data rates que as tramas beacon do AP 30 Munroe St anunciam que o AP suporta são 1(B), 2(B), 5.5(B), 11(B) [Mbit/sec]. E as oito extended supported rates adicionais são 6(B), 9, 12(B), 18, 24(B), 36, 48, 54 [Mbit/sec].

```
No.      Time          Source           Destination      Protocol Length Info
 2101  61.624991    Cisco-Li_f7:1d:51 Broadcast         802.11   183   Beacon frame, SN=3709, FN=0, Flags=.....C,
BI=100, SSID=30 Munroe St
Frame 2101: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits)
Radiotap Header v0, Length 24
802.11 radio information
IEEE 802.11 Beacon frame, Flags: .....C
  Type/Subtype: Beacon frame (0x0008)
  Frame Control Field: 0x8000
    .... 0000 = 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
  1110 0111 1101 .... = Sequence number: 3709
  Frame check sequence: 0xfd557420 [unverified]
  [FCS Status: Unverified]
IEEE 802.11 wireless LAN
```

Figura 4: A trama com número 2101.

10. Selecionando a trama beacon 2101. 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 seleccionada pertence ao tipo 802.11b do conjunto de tramas 802.11. O valor do seu identificador é 00 (management frame - 0) e valor do subtipo é 1000 (8).

```

▶ Frame 169: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
▶ Radiotap Header v0, Length 24
▶ 802.11 radio information
* IEEE 802.11 Beacon frame, Flags: .....
  Type/Subtype: Beacon frame (0x0008)
  ▶ Frame Control Field: 0x0000
    .... ..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: LinksysG_67:22:94 (00:06:25:67:22:94)
  Source address: LinksysG_67:22:94 (00:06:25:67:22:94)
  BSS Id: LinksysG_67:22:94 (00:06:25:67:22:94)
  .... .... 0000 = Fragment number: 0
  1100 0100 1101 .... = Sequence number: 3149
▶ Frame check sequence: 0xd9bdce0a incorrect, should be 0x9283a76d
  [FCS Status: Bad]
▶ IEEE 802.11 wireless LAN

```

Figura 5: Uma trama beacon recebida incorrectamente.

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

O método de detecção de erros CRC está a ser utilizado pois as trama beacon tem a flag FCS (Frame Check Sequence) a verdadeira contudo algumas das tramas beacon não foram recebidas correctamente porque o campo FCS no campo IEEE 802.11 Beacon frame indica que a trama está incorrecta (por exemplo, a trama 169 - presente na figura 5 do presente relatório). É usado este tipo de mecanismos de detecção de erros neste tipo de redes locais porque a comunicação sem fios está muito mais susceptível a erros e interferências logo é necessário haver métodos que permitem detectá-los.

12. **Identifique e registe todos os endereços MAC usados nas tramas beacon enviadas pelos APs.**

Os endereços MAC de origem usados nas tramas beacon enviadas pelos APs foram 00:16:b6:f7:1d:51, 00:18:39:f5:ba:bb e 00:06:25:67:22:94.



No trace disponibilizado também foi registrado scanning ativo, i.e., envolvendo tramas probe request e probe response, comum nas redes Wi-Fi como alternativa ao scanning passivo.

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	2.300697	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=phoiphos
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	78	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
131	6.405938	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2924, FN=0, Flags=.....R...C, BI=100, SSID=30 Munroe St
132	6.407562	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2924, FN=0, Flags=.....R...C, BI=100, SSID=30 Munroe St
133	6.409063	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2924, FN=0, Flags=.....R...C, BI=100, SSID=30 Munroe St
134	6.410562	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2924, FN=0, Flags=.....R...C, BI=100, SSID=30 Munroe St
135	6.412063	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2924, FN=0, Flags=.....R...C, BI=100, SSID=30 Munroe St

Figura 6: Filtro Wireshark que permite visualizar todas as tramas probing request e probing response, simultaneamente.

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

Probe Request destination MAC BSS ID: ff:ff:ff:ff:ff:ff

Probe Response source MAC BSS ID: 00:16:b6:f7:1d:51

A estação envia uma trama Probe Request quando precisa de obter informações de uma outra estação, esta trama é útil para uma estação determinar quais os pontos de acesso que estão dentro do seu alcance rádio.

À trama Probe Request uma outra estação ou ponto de acesso irão responder com uma trama de Probe Response, contendo informações úteis tais como taxas de dados suportadas, etc.

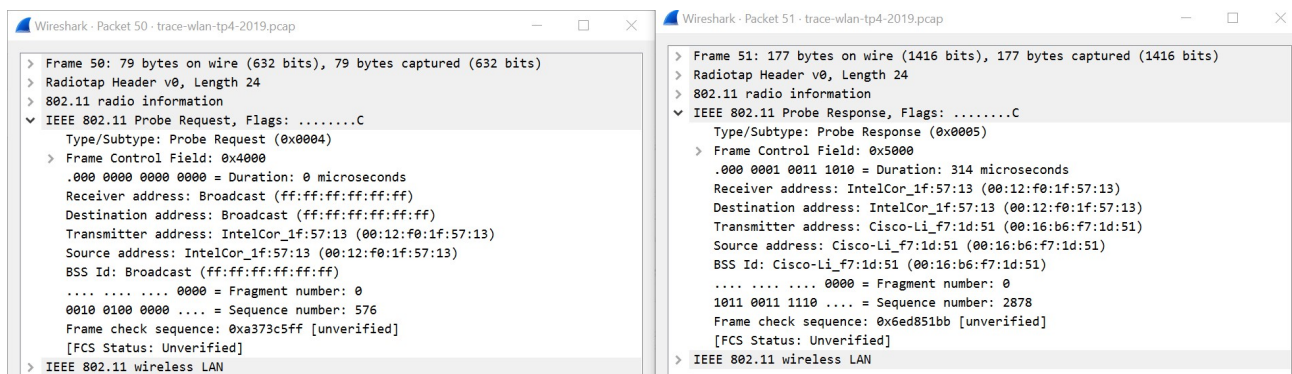


Figura 7: Um probing request para o qual houve um probing response.

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?**

Uma estação com o endereço MAC 00:12:f0:1f:57:13 faz um pedido à rede para ver se há algum ponto de acesso ou estação disponível no seu alcance rádio e o ponto de acesso ou estação, com o endereço MAC 00:16:b6:f7:1d:51, respondem de volta com as suas taxas de dados suportadas, entre outras informações.

## 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 respondemos as seguintes questões.

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? Observando a especificação 802.11, seria de esperar outra trama, mas que não aparece?**

As duas ações realizadas 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 foi Deauthentication e DHCP Release.

Observando a especificação 802.11, seria de esperar uma trama de dissociação.

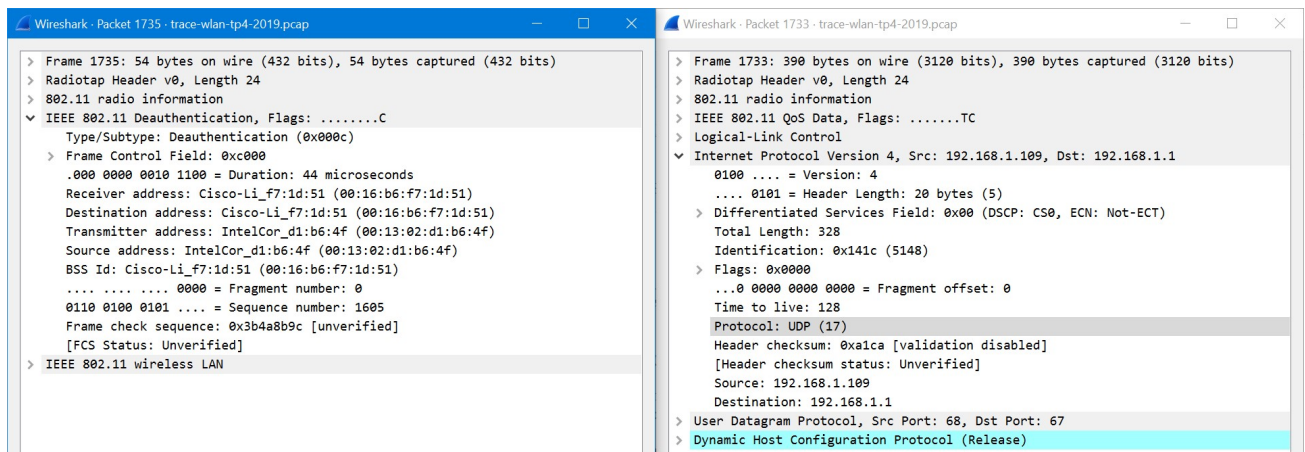


Figura 8: Ações realizadas pelo host imediatamente após  $t=49$  ara terminar a associação.

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  $t=49$ ?

Foram enviadas 6 mensagens de authentication para o AP linksys\_ses\_24086 (que tem o endereço MAC Cisco\_Li\_f5:ba:bb) aproximadamente para o  $t=49$ .

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=....R...C
1822	53.787079	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1612, FN=0, Flags=....R...C
1921	57.880232	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...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=....R...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	62.174079	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=....R...C
2158	63.169071	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58	Authentication, SN=3726, FN=0, Flags=....R...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=....R...C

Figura 9: Ações realizadas pelo host imediatamente após  $t=49$  para a autenticação.

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

O tipo de autenticação pretendida pelo host é aberta.

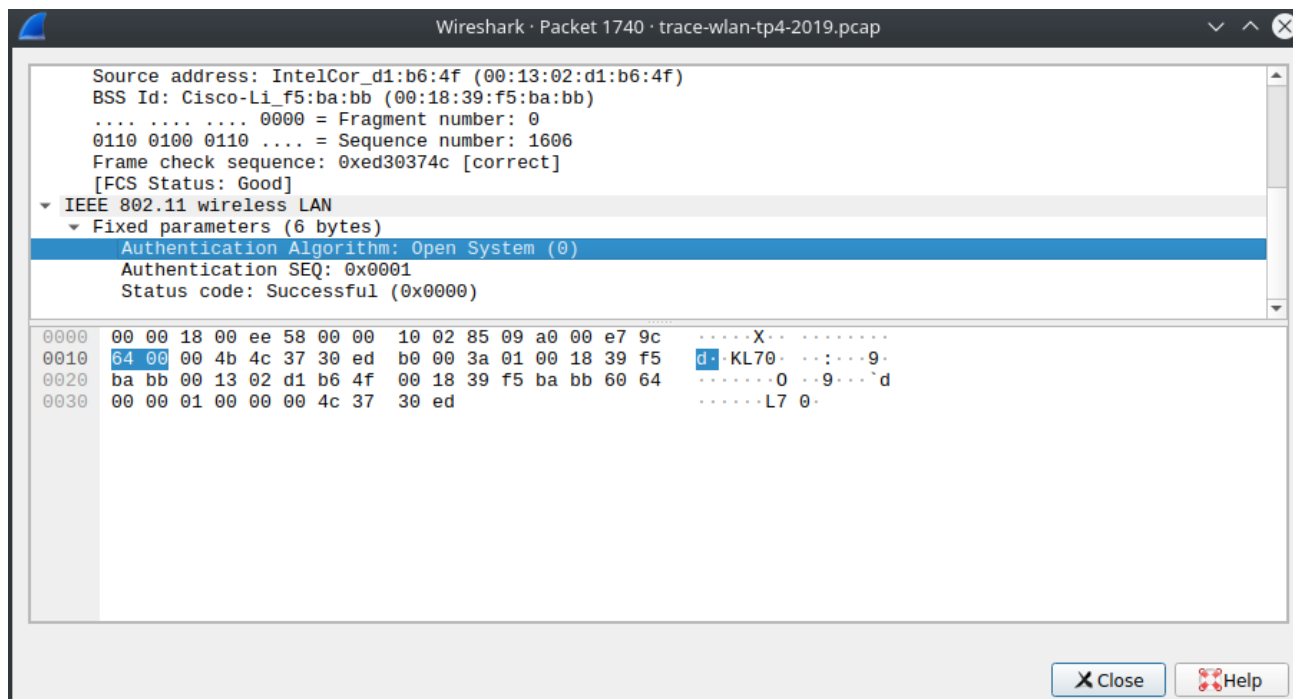


Figura 10: Authentication algorithm.

19. Observa-se a resposta de authentication do AP linksys\_ses\_24086 AP no trace?

Não se verifica resposta de authentication do AP linksys\_ses\_24086 AP no trace.

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? Há uma trama de autenticação do host para o AP 30 Monroe St no instante 63.168087. Outra autenticação é enviada no instante 63.169071.

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
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

Figura 11: Authentication algorithm.

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 host para o AP 30 Munroe St aparece ao instante 63.169910 e o correspondente associate reply é enviado ao instante 63.192101.

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 12: Instantes onde aparece o associate request e response.

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

O host está disposto a usar as seguintes taxas de transmissão 1, 2, 5.5, 11, 6, 9, 12 e 18 [Mbit/sec]. Por outro lado, o AP está disposto a suportar as seguintes taxas de transmissão 1, 2, 5.5 e 11 [Mbit/sec].

2162 63.169910 IntelCor_d1:b6:4f Cisco-Li_f7:1d:51 802.11 89 Association Request, SN=1648					
▶ Frame 2162: 89 bytes on wire (712 bits), 89 bytes captured (712 bits)					
▶ 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)					
▼ 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: Extended Supported Rates 24(B), 36, 48, 54, [Mbit/sec]					

Figura 13: Taxas de transmissão que o host está disposto a usar.



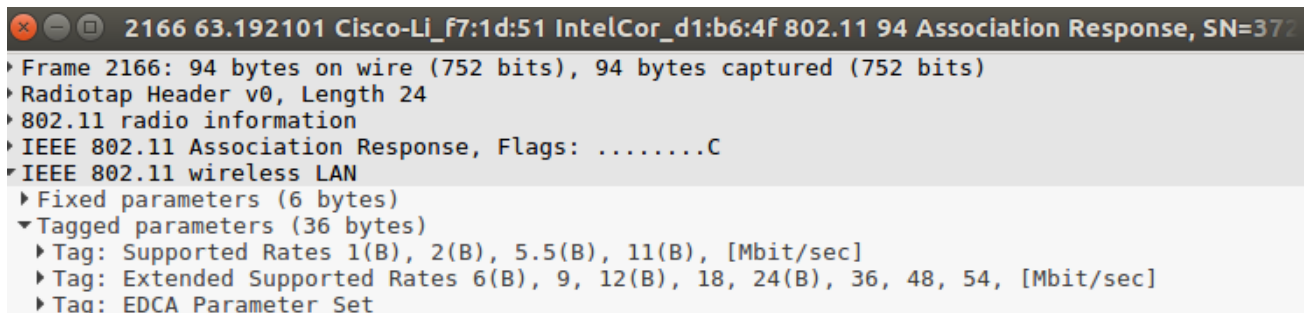


Figura 14: Taxas de transmissão que o AP está disposto a usar.

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.

A sequência de tramas que corresponde a um processo de associação completo entre a STA e o AP é um probe request, probe response, authentication request, authentication response, association request e por fim association response.

2004 60.058940	IntelCor_d1:b6:4f	Broadcast	802.11	99 Probe Request, SN=1625, FN=0, Flags=.....C, SSID=linksys_SES_24086
2005 60.060065	IntelCor_d1:b6:4f	Broadcast	802.11	82 Probe Request, SN=1625, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
2006 60.062438	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	177 Probe Response, SN=3691, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
2018 60.256570	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	177 Probe Response, SN=3694, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
2019 60.258070	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	177 Probe Response, SN=3694, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
2020 60.259945	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	177 Probe Response, SN=3694, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
2021 60.280076	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	177 Probe Response, SN=3695, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
2121 62.144576	IntelCor_d1:b6:4f	Broadcast	802.11	99 Probe Request, SN=1644, FN=0, Flags=.....C, SSID=linksys_SES_24086
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
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=.....C, SSID=linksys_SES_24086
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-Li_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 63.168087	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
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 15: Sequência de tramas.

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

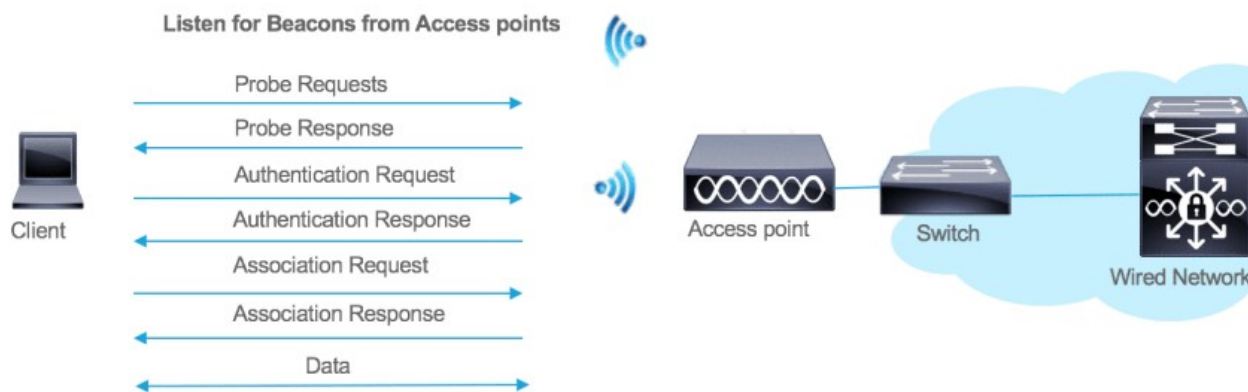


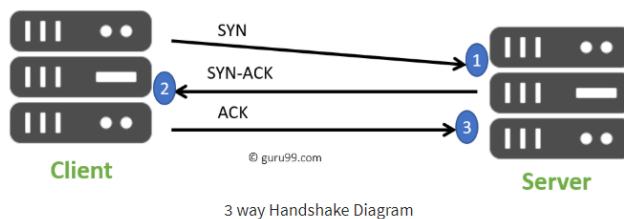
Figura 16: Processo de associação.

## 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.

### TCP Three-Way Handshake Process

TCP traffic begins with a three-way handshake. In this TCP handshake process, a client needs to initiate the conversation by requesting a communication session with the Server:



- **Step 1:** In the first step, the client establishes a connection with a server. It sends a segment with SYN and informs the server about the client should start communication, and with what should be its sequence number.
- **Step 2:** In this step server responds to the client request with SYN-ACK signal set. ACK helps you to signify the response of segment that is received and SYN signifies what sequence number it should able to start with the segments.
- **Step 3:** In this final step, the client acknowledges the response of the Server, and they both create a stable connection will begin the actual data transfer process.

Figura 17: Exemplo de como funciona as tramas 802.11 SYN/ACK/SYN-ACK.

```

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
Frame 474: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
Radiotap Header v0, Length 24
802.11 radio information
IEEE 802.11 QoS Data, Flags: .....TC
Type/Subtype: QoS Data (0x0028)
Frame Control Field: 0x8801
.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)
.... .... 0000 = Fragment number: 0
0000 0011 0001 .... = Sequence number: 49
Frame check sequence: 0xad57fce0 [unverified]
[FCS Status: Unverified]
Qos Control: 0x0000
Logical-Link Control
Internet Protocol Version 4, Src: 192.168.1.109, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 2538, Dst Port: 80, Seq: 0, Len: 0

```

Figura 18: Trama 802.11 que contém o segmento SYN TCP para a primeira sessão TCP.

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 endereços MAC na trama 802.11 são do host, do AP e do router do primeiro salto.

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 endereço MAC nesta trama que corresponde ao host é 00:13:02:d1:b6:4f, em notação hexadecimal. Do AP é 00:16:b6:f7:1d:51. O endereço do router do primeiro salto é 00:16:b6:f4:eb:a8. O endereço IP do host que está enviar este segmento TCP 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.** Este endereço IP de destino corresponde ao router do primeiro salto, pois o destination address é do router e este pacote é enviado para esse endereço.



```

> Frame 1013: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
▼ IEEE 802.11 QoS Data, Flags: .....F.C
    Type/Subtype: QoS Data (0x0028)
    > Frame Control Field: 0x8802
        .000 0000 0010 1000 = Duration: 40 microseconds
        Receiver address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
        Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
        Destination address: IntelCor_d1:b6:4f (00:13:02:d1: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: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
        .... .... 0000 = Fragment number: 0
        1100 1111 0010 .... = Sequence number: 3314
        Frame check sequence: 0x20e725d9 [unverified]
        [FCS Status: Unverified]
    > Qos Control: 0x0300
> Logical-Link Control
> Internet Protocol Version 4, Src: 128.119.240.19, Dst: 192.168.1.109
> Transmission Control Protocol, Src Port: 80, Dst Port: 2541, Seq: 0, Ack: 1, Len: 0

```

Figura 19: Trama 802.11 que contém o segmento SYNACK para esta sessão TCP.

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 dos endereços MAC na trama 802.11 são do host, do AP e da router do primeiro salto.

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

O endereço MAC nesta trama que corresponde ao host é 00:13:02:d1:b6:4f, em notação hexadecimal. O endereço AP é 00:16:b6:f7:1d:51. E o do router é 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.**

O endereço MAC da origem nesta trama é 00:16:b6:f4:eb:a8 que corresponde ao endereço ip 128.119.240.19, como podemos ver na figura 18.

### **3 Conclusão**

O presente relatório descreveu, de forma sucinta, a resolução das questões propostas utilizando os softwares disponibilizados pelos docentes.

Após a realização deste trabalho, ficamos conscientes dos vários aspectos 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.

Consideramos que os principais objectivos foram cumpridos.

Sentimos que a realização deste trabalho prático consolidou os nossos conhecimentos do protocolo IEEE 802.11.