



UNIVERSIDADE DO MINHO  
LICENCIATURA EM ENGENHARIA INFORMÁTICA

## **REDES DE COMPUTADORES**

### **Trabalho Prático 4 REDES SEM FIOS (WI-FI)**

Mariana Gonçalves (a100662) Maya Gomes (a100822) Vicente Martins  
(a100713)

May 17, 2023

## **Conteúdos**

<b>1</b>	<b>Introdução</b>	<b>3</b>
<b>2</b>	<b>Questões e respostas I - Acesso Rádio</b>	<b>3</b>
2.1	Questão 1: . . . . .	3
2.2	Questão 2: . . . . .	3
2.3	Questão 3: . . . . .	3
2.4	Questão 4: . . . . .	4
<b>3</b>	<b>Questões e respostas II - Scanning Passivo e Scanning Ativo</b>	<b>4</b>
3.1	Questão 5: . . . . .	4
3.2	Questão 6: . . . . .	5
3.3	Questão 7: . . . . .	5
3.4	Questão 8: . . . . .	6
3.5	Questão 9: . . . . .	8
3.6	Questão 10: . . . . .	9
3.7	Questão 11: . . . . .	10
3.8	Questão 12: . . . . .	11
<b>4</b>	<b>Questões e respostas III - Processo de Associação</b>	<b>12</b>
4.1	Questão 13: . . . . .	12
4.2	Questão 14: . . . . .	14
<b>5</b>	<b>Questões e respostas IV - Transferência de Dados</b>	<b>15</b>
5.1	Questão 15: . . . . .	15
5.2	Questão 16: . . . . .	15
5.3	Questão 17: . . . . .	16
5.4	Questão 18: . . . . .	17
5.5	Questão 19: . . . . .	17
<b>6</b>	<b>Conclusão</b>	<b>19</b>

# 1 Introdução

## 2 Questões e respostas I - Acesso Rádio

### 2.1 Questão 1:

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

Analizando a figura abaixo chegamos à conclusão que a rede opera numa frequência de 2412 MHz no canal 1.

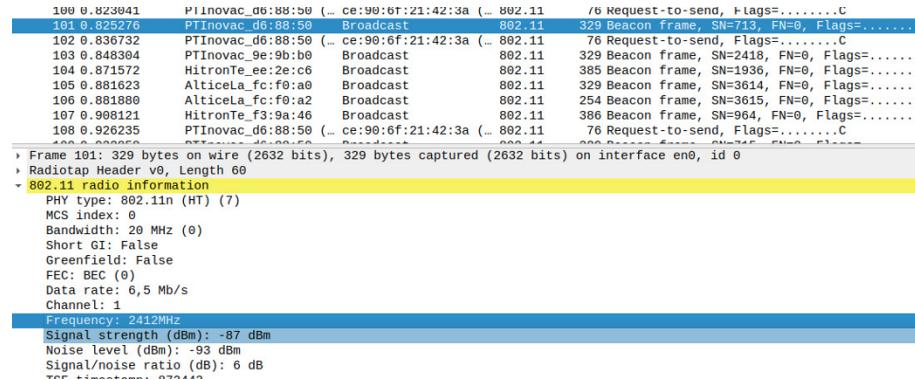


Figura 1: Trama 101 selecionada.

### 2.2 Questão 2:

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

Tal como vemos na figura acima, a versão a ser usada é 802.11n .

### 2.3 Questão 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.*

O débito, tal como referido na figura acima(Data Rate), é de 6,5 Mb/s.

Na figura acima o débito máximo suportado é 54 Mb/s. Desta forma, o débito apresentado não é o débito máximo.

O protocolo 802.11 é capaz de suportar velocidades de até 600 Mb/s, dependendo das condições da rede e das configurações utilizadas.

```

    - Tagged parameters (229 bytes)
      > Tag: SSID parameter set: MEO-D68850
      > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 18, 24, 36, 54, [Mbit/sec]
      > Tag: DS Parameter set: Current Channel: 1
      > Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
      > Tag: ERP Information

```

Figura 2: Débitos suportados.

## 2.4 Questão 4:

*Verifique qual a força do sinal (Signal strength) e a qualidade expectável de receção da trama, sabendo que:*

Signal strength	Expected Quality
-90dBm	Chances of connecting are very low at this level
-80dBm	Unreliable signal strength
-67dBm	Reliable signal strength— the edge of what Cisco considers to be adequate to support Voice over WLAN
-55dBm	Anything down to this level can be considered excellent signal strength.
-30dBm	Maximum signal strength, you are probably standing right next to the access point.

Figura 3: Figura fornecida no enunciado.

Sendo que o *Signal strength* é de -87 dBm e que esse valor é mais próximo de -90 dBm, a qualidade expectável é muito baixa.

## 3 Questões e respostas II - Scanning Passivo e Scanning Ativo

### 3.1 Questão 5:

*Selecione uma trama beacon cuja ordem (ou terminação) corresponda a XX. Esta trama pertence a que tipo de tramas 802.11? Identifique o valor dos identificadores de tipo e de subtipo da trama. Em que parte concreta do cabeçalho da trama estão especificados (ver anexo)?*

A trama selecionada é a 101, e como podemos ver na seguinte imagem, esta pertence ao tipo *Management* (0) e o seu subtipo é *Beacon* (8). Através do anexo fornecido no enunciado podemos verificar que estes pertencem ao *Frame Control*.

```

- IEEE 802.11 Beacon frame, Flags: .....
  Type/Subtype: Beacon frame (0x0008)
    - Frame Control Field: 0x8000
      .... .00 = Version: 0
      .... 00.. = Type: Management frame (0)
      1000 .... = Subtype: 8
    - Flags: 0x00
      .000 0000 0000 0000 = Duration: 0 microseconds

```

Figura 4: Tipo e subtipo da trama.

### 3.2 Questão 6:

*Para a trama acima, identifique todos os endereços MAC em uso. Que conclui quanto à sua origem e destino?*

Analizando a trama identificamos os seguintes endereços MAC (em parêntesis):

```

Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
Transmitter address: PTInovac_d6:88:50 (00:06:91:d6:88:50)
Source address: PTInovac_d6:88:50 (00:06:91:d6:88:50)

```

Figura 5: Endereços MAC em uso na trama.

Sendo assim conclui-se que a origem tem um endereço MAC **00:06:91:d6:88:50** e o destino **ff:ff:ff:ff:ff:ff**. Desta forma, isso implica que esta trama foi transmitida para todos os nós da rede.

### 3.3 Questão 7:

*Verifique se está a ser usado o método de deteção de erros (CRC). Justifique. Justifique o porquê de ser necessário usar deteção de erros em redes sem fios.*

Ao verificar inicialmente se o método de deteção de erros está ativo, deparamo-nos com a informação presente na figura abaixo. A partir dessa, concluímos que o CRC não está ativo.

```

Frame check sequence: 0xca61f668 [unverified]
[FCS Status: Unverified]

```

Figura 6: FCS.

Ao investigar as configurações do Wireshark verificamos a possibilidade de ativar a opção de deteção de erros.

Search: wlan

Name	Status	Type	Value
Protocols			
IEEE 802.11			
wlan.check_checksum	IEEE 802.11	Boolean	FALSE
wlan.check_fcs	wireless LAN	Boolean	FALSE

Figura 7: Definições default.

Search: wlan

Name	Status	Type	Value
Protocols			
IEEE 802.11			
wlan.check_checksum	Changed	Boolean	TRUE
wlan.check_fcs	Changed	Boolean	TRUE

Figura 8: Definições alterada.

```
0010 1100 1001 .... = Sequence number: 713
Frame check sequence: 0xca61f668 [correct]
[FCS Status: Good]
```

Figura 9: FCS alterado.

A deteção de erros em redes sem fio é essencial devido a algumas características como: a interferência do canal, a propagação do sinal, a mobilidade dos dispositivos, as limitações de largura de banda ou ainda os protocolos de correção de erros. Para além disso, ela desempenha um papel importante na garantia da eficiência e qualidade da comunicação em redes sem fio.

### 3.4 Questão 8:

*Uma trama beacon anuncia que o AP pode suportar vários débitos de base (B), assim como vários débitos adicionais (extended supported rates). Indique quais são esses débitos.*

- ▶ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 18, 24, 36, 54, [Mbit/sec]
- ▶ Tag: DS Parameter set: Current Channel: 1
- ▶ Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
- ▶ Tag: ERP Information
- ▶ Tag: Extended Supported Rates 6, 9, 12, 48, [Mbit/sec]

Figura 10: Debitos da trama.

Tal como conseguimos analisar na secção acima, os débitos suportados são:

- 1 Mb/s
- 2 Mb/s
- 5.5 Mb/s
- 11 Mb/s
- 18 Mb/s
- 24 Mb/s
- 36 Mb/s
- 54 Mb/s

E os débitos adicionais suportados são:

- 6 Mb/s
- 9 Mb/s
- 12 Mb/s
- 48 Mb/s

### 3.5 Questão 9:

*Qual o intervalo de tempo previsto entre tramas beacon consecutivas (este valor é anunciado na própria trama beacon)? Na prática, a periodicidade de tramas beacon provenientes do mesmo AP é verificada com precisão? Justifique.*

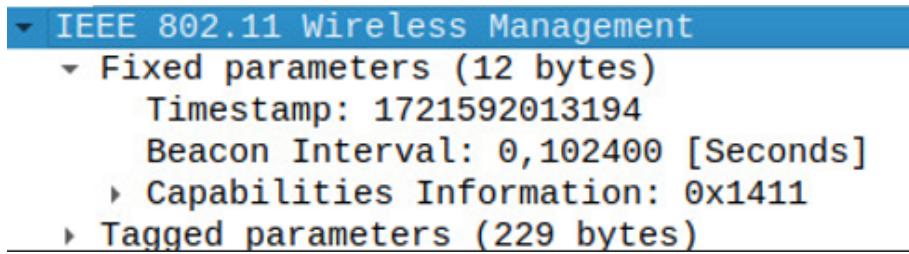


Figura 11: Beacon Interval.

O valor de intervalo de tempo previsto entre tramas *beacon* consecutivas é **0.102400** segundos. Devido ao acontecimento de atrasos no envio dos tramas *beacon*, este valor é um valor aproximado ao valor real, não podendo ser verificado com precisão.

### 3.6 Questão 10:

*Identifique e liste os SSIDs dos APs que estão a operar na vizinhança da STA de captura. Explicite o modo como obteve essa informação (por exemplo, se usou algum filtro para o efeito).*

De modo a obter os SSIDs dos APs, utilizamos o filtro `wlan.ssid` no wireshark que nos dá as tramas `beacon` capturados provenientes dos APs que conseguem comunicar com a STA. Com o uso deste filtro chegamos à conclusão que os três SSIDs são FlyingNet, NOS e MEO.

No.	Time	Source	Destination	Protocol	Length	Info
63	0.519642	PTInovac_d6:88:59	Broadcast	802.11	329	Beacon frame, SN=766, FN=0, Flags=.....C, BI=100, SSID=MEO-D68859
64	0.519882	PTInovac_d6:88:52	Broadcast	802.11	254	Beacon frame, SN=767, FN=0, Flags=.....C, BI=100, SSID=MEO-Wifi
65	0.520599	PTInovac_45:be:30	Broadcast	802.11	329	Beacon frame, SN=2367, FN=0, Flags=.....C, BI=100, SSID=MEO-45BE30
66	0.526284	PTInovac_45:be:32	Broadcast	802.11	254	Beacon frame, SN=2368, FN=0, Flags=.....C, BI=100, SSID=MEO-Wifi
67	0.530098	PTInovac_9e:9b:c6	Broadcast	802.11	254	Beacon frame, SN=2413, FN=0, Flags=.....C, BI=100, SSID=MEO-Wifi
68	0.534474	HironTe_e7:c8:c6	Broadcast	802.11	385	Beacon frame, SN=1934, FN=0, Flags=.....C, BI=100, SSID=NOS-2EC6
69	0.564553	HironTe_e7:c8:76	Broadcast	802.11	453	Beacon frame, SN=1769, FN=0, Flags=.....C, BI=100, SSID=NOS-C876
70	0.5746851	AlticeLfa_fc:f0:a0	Broadcast	802.11	329	Beacon frame, SN=3608, FN=0, Flags=.....C, BI=100, SSID=MEO-FCF0A0
71	0.575043	AlticeLfa_fc:f0:a2	Broadcast	802.11	254	Beacon frame, SN=3609, FN=0, Flags=.....C, BI=100, SSID=MEO-Wifi
72	0.601428	HironTe_f3:9a:46	Broadcast	802.11	388	Beacon frame, SN=961, FN=0, Flags=.....C, BI=100, SSID=flyingNet
73	0.621977	PTInovac_d9:88:50	Broadcast	802.11	329	Beacon frame, SN=788, FN=0, Flags=.....C, BI=100, SSID=MEO-D68850
74	0.622106	PTInovac_45:be:32	Broadcast	802.11	254	Beacon frame, SN=2370, FN=0, Flags=.....C, BI=100, SSID=MEO-45BE32
75	0.645326	PTInovac_9e:9b:c6	Broadcast	802.11	329	Beacon frame, SN=2409, FN=0, Flags=.....C, BI=100, SSID=MEO-0E9B00
76	0.645479	PTInovac_9e:9b:b2	Broadcast	802.11	254	Beacon frame, SN=2415, FN=0, Flags=.....C, BI=100, SSID=MEO-Wifi
80	0.665755	HironTe_ee:2e:c6	Broadcast	802.11	385	Beacon frame, SN=1934, FN=0, Flags=.....C, BI=100, SSID=NOS-2EC6
81	0.666556	HironTe_e7:c8:76	Broadcast	802.11	453	Beacon frame, SN=1769, FN=0, Flags=.....C, BI=100, SSID=NOS-C876
82	0.676869	AlticeLfa_fc:f0:a0	Broadcast	802.11	329	Beacon frame, SN=3610, FN=0, Flags=.....C, BI=100, SSID=MEO-FCF0A0
83	0.676973	AlticeLfa_fc:f0:a2	Broadcast	802.11	254	Beacon frame, SN=3611, FN=0, Flags=.....C, BI=100, SSID=MEO-Wifi
88	0.703381	HironTe_f3:9a:46	Broadcast	802.11	388	Beacon frame, SN=962, FN=0, Flags=.....C, BI=100, SSID=flyingNet
89	0.704114	PTInovac_d9:88:50	Broadcast	802.11	329	Beacon frame, SN=789, FN=0, Flags=.....C, BI=100, SSID=MEO-D68850
91	0.769299	HironTe_ee:2e:c6	Broadcast	802.11	385	Beacon frame, SN=1935, FN=0, Flags=.....C, BI=100, SSID=NOS-2EC6
92	0.769312	HironTe_e7:c8:76	Broadcast	802.11	453	Beacon frame, SN=1770, FN=0, Flags=.....C, BI=100, SSID=NOS-C876
93	0.779412	AlticeLfa_fc:f0:a0	Broadcast	802.11	329	Beacon frame, SN=3612, FN=0, Flags=.....C, BI=100, SSID=MEO-FCF0A0
94	0.779824	AlticeLfa_fc:f0:a2	Broadcast	802.11	254	Beacon frame, SN=3613, FN=0, Flags=.....C, BI=100, SSID=MEO-Wifi
97	0.805726	HironTe_f3:9a:46	Broadcast	802.11	388	Beacon frame, SN=963, FN=0, Flags=.....C, BI=100, SSID=flyingNet
101	0.825276	PTInovac_d6:88:59	Broadcast	802.11	329	Beacon frame, SN=713, FN=0, Flags=.....C, BI=100, SSID=flyingNet
102	0.825277	PTInovac_d6:88:50	Broadcast	802.11	329	Beacon frame, SN=714, FN=0, Flags=.....C, BI=100, SSID=MEO-D68850
104	0.871572	HironTe_ee:2e:c6	Broadcast	802.11	385	Beacon frame, SN=1936, FN=0, Flags=.....C, BI=100, SSID=NOS-2EC6
105	0.881623	AlticeLfa_fc:f0:a0	Broadcast	802.11	329	Beacon frame, SN=3614, FN=0, Flags=.....C, BI=100, SSID=MEO-FCF0A0
106	0.881889	AlticeLfa_fc:f0:a2	Broadcast	802.11	254	Beacon frame, SN=3615, FN=0, Flags=.....C, BI=100, SSID=MEO-Wifi
107	0.908121	HironTe_f3:9a:46	Broadcast	802.11	388	Beacon frame, SN=964, FN=0, Flags=.....C, BI=100, SSID=flyingNet
109	0.932658	PTInovac_d6:88:50	Broadcast	802.11	329	Beacon frame, SN=715, FN=0, Flags=.....C, BI=100, SSID=MEO-D68850
110	0.932664	PTInovac_d6:88:52	Broadcast	802.11	254	Beacon frame, SN=716, FN=0, Flags=.....C, BI=100, SSID=MEO-Wifi
111	0.936478	PTInovac_45:be:30	Broadcast	802.11	254	Beacon frame, SN=2376, FN=0, Flags=.....C, BI=100, SSID=MEO-Wifi
112	0.936474	PTInovac_45:be:c2	Broadcast	802.11	279	Beacon frame, SN=2421, FN=0, Flags=.....C, BI=100, SSID=MEO-Wifi
113	0.950753	PTInovac_9e:9b:b0	Broadcast	802.11	329	Beacon frame, SN=2420, FN=0, Flags=.....C, BI=100, SSID=MEO-0E9B00
114	0.950868	PTInovac_9e:9b:b2	Broadcast	802.11	254	Beacon frame, SN=2421, FN=0, Flags=.....C, BI=100, SSID=MEO-Wifi
115	0.974151	HironTe_ee:2e:c6	Broadcast	802.11	385	Beacon frame, SN=1937, FN=0, Flags=.....C, BI=100, SSID=NOS-2EC6
117	0.974863	HironTe_e7:c8:76	Broadcast	802.11	453	Beacon frame, SN=1772, FN=0, Flags=.....C, BI=100, SSID=NOS-C876

Figura 12: SSIDs a operar na vizinhança da STA.

### 3.7 Questão 11:

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

O filtro que permite essa visualização é:

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

Estamos a testar o subtipo das tramas, filtrando as de *probing request* (4) e as de *probing response* (5). Assim, a visualização após a aplicação do filtro, comprova a apresentação de tramas deste tipo:

No.	Time	Source	Destination	Protocol	Length	Info
159 1.381694		HironTe_f3:9a:46	SamsungE_1a:10:f6	802.11	486	Probe Response, SN=1936, FN=0, Flags=.....C, BI=100, SSID:FlyingNet
151 1.382387		HironTe_f3:9a:46	SamsungE_1a:10:f6	802.11	485	Probe Response, SN=1936, FN=0, Flags=.....R..C, BI=100, SSID:FlyingNet
152 1.391756		HironTe_f3:9a:46	SamsungE_1a:10:f6	802.11	485	Probe Response, SN=1936, FN=0, Flags=.....R..C, BI=100, SSID:FlyingNet
153 1.391879		HironTe_e2:c6	SamsungE_1a:10:f6	802.11	485	Probe Response, SN=2192, FN=0, Flags=.....R..C, BI=100, SSID=NOS-2EC6
154 1.391923		SamsungE_1a:10:f6	Broadcast	802.11	146	Probe Request, SN=1936, FN=0, Flags=.....C, BI=100, SSID:NOS-2EC6
277 7.477443		HironTe_e2:c6	AltBeam_08:32:99	802.11	485	Probe Response, SN=2193, FN=0, Flags=.....C, BI=100, SSID=NOS-2EC6
279 2.728237		HironTe_e2:c6	AltBeam_08:32:99	802.11	485	Probe Response, SN=2193, FN=0, Flags=.....R..C, BI=100, SSID=NOS-2EC6
334 3.297197		PTInovac_45:be:32	ea:52:54:89:2b:72	802.11	224	Probe Response, SN=2244, FN=0, Flags=.....C, BI=100, SSID:MEO-WiFi
335 3.297177		PTInovac_45:be:32	ea:52:54:89:2b:72	802.11	224	Probe Response, SN=2244, FN=0, Flags=.....R..C, BI=100, SSID:MEO-WiFi
336 3.300315		PTInovac_45:be:32	ea:52:54:89:2b:72	802.11	224	Probe Response, SN=2244, FN=0, Flags=.....R..C, BI=100, SSID:MEO-WiFi
789 7.826332		AltBeam_08:32:99	Broadcast	802.11	119	Probe Request, SN=1111, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
789 7.826332		AltBeam_08:32:99	AltBeam_08:32:99	802.11	485	Probe Response, SN=2190, FN=0, Flags=.....C, BI=100, SSID=NOS-2EC6
791 7.826364		HironTe_e2:c6	AltBeam_08:32:99	802.11	485	Probe Response, SN=2190, FN=0, Flags=.....R..C, BI=100, SSID=NOS-2EC6
793 7.826361		AltBeam_08:32:99	Broadcast	802.11	119	Probe Request, SN=1112, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
796 7.859430		HironTe_e2:c6	AltBeam_08:32:99	802.11	485	Probe Response, SN=2196, FN=0, Flags=.....C, BI=100, SSID=NOS-2EC6
797 7.862565		HironTe_e2:c6	AltBeam_08:32:99	802.11	485	Probe Response, SN=2196, FN=0, Flags=.....R..C, BI=100, SSID=NOS-2EC6
798 7.866818		HironTe_e2:c6	AltBeam_08:32:99	802.11	485	Probe Response, SN=2196, FN=0, Flags=.....R..C, BI=100, SSID=NOS-2EC6
962 9.389248		PTInovac_29:a9:c0	ARRISGro_a9:9e:98	802.11	434	Probe Response, SN=3266, FN=0, Flags=.....C, BI=100, SSID=Masmorra
963 9.396784		PTInovac_29:a9:c0	ARRISGro_a9:9e:98	802.11	434	Probe Response, SN=3266, FN=0, Flags=.....R..C, BI=100, SSID=Masmorra
964 9.403215		PTInovac_29:a9:c0	ARRISGro_a9:9e:98	802.11	434	Probe Response, SN=3266, FN=0, Flags=.....C, BI=100, SSID=Masmorra
965 9.403215		PTInovac_29:a9:c0	ARRISGro_a9:9e:98	802.11	434	Probe Response, SN=3266, FN=0, Flags=.....R..C, BI=100, SSID=Masmorra
967 9.409475		PTInovac_29:a9:c0	ARRISGro_a9:9e:98	802.11	434	Probe Response, SN=3266, FN=0, Flags=.....C, BI=100, SSID=Masmorra
968 9.412592		PTInovac_29:a9:c0	ARRISGro_a9:9e:98	802.11	240	Probe Response, SN=3267, FN=0, Flags=.....C, BI=100, SSID=MEO-WiFi
969 9.413792		PTInovac_29:a9:c2	ARRISGro_a9:9e:98	802.11	240	Probe Response, SN=3267, FN=0, Flags=.....R..C, BI=100, SSID=MEO-WiFi
970 9.418856		PTInovac_29:a9:c2	ARRISGro_a9:9e:98	802.11	240	Probe Response, SN=3267, FN=0, Flags=.....R..C, BI=100, SSID=MEO-WiFi
971 9.418951		PTInovac_29:a9:c2	ARRISGro_a9:9e:98	802.11	240	Probe Response, SN=3267, FN=0, Flags=.....R..C, BI=100, SSID=MEO-WiFi
973 9.418951		HironTe_e2:c6	ARRISGro_a9:9e:98	802.11	517	Probe Response, SN=2201, FN=0, Flags=.....R..C, BI=100, SSID=Wildcard (Broadcast)
1339 12.959765		ARRISGro_a6:bc:a0	Broadcast	802.11	134	Probe Request, SN=1576, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
1340 12.964426		HironTe_e2:c6	AltBeam_08:32:99	802.11	485	Probe Response, SN=2197, FN=0, Flags=.....C, BI=100, SSID=NOS-2EC6
1342 12.977069		HironTe_e2:c6	ARRISGro_a6:bc:a0	802.11	485	Probe Response, SN=2198, FN=0, Flags=.....C, BI=100, SSID=NOS-2EC6
1349 13.038314		HironTe_e2:c6	ARRISGro_a6:bc:a0	802.11	485	Probe Response, SN=2199, FN=0, Flags=.....C, BI=100, SSID=NOS-2EC6
1406 13.569918		HironTe_e2:c6	ARRISGro_a6:bc:a0	802.11	485	Probe Response, SN=2200, FN=0, Flags=.....C, BI=100, SSID=NOS-2EC6
1407 13.579566		HironTe_e2:c6	ARRISGro_a6:bc:a0	802.11	485	Probe Response, SN=2200, FN=0, Flags=.....R..C, BI=100, SSID=NOS-2EC6
1413 13.812268		HironTe_e2:c6	ARRISGro_a6:bc:a0	802.11	485	Probe Response, SN=2201, FN=0, Flags=.....R..C, BI=100, SSID=NOS-2EC6
1413 13.812267		HironTe_e2:c6	ARRISGro_a6:bc:a0	802.11	485	Probe Response, SN=2201, FN=0, Flags=.....R..C, BI=100, SSID=NOS-2EC6
1424 13.746366	22:58:38:50:79:94	Broadcast		802.11	139	Probe Request, SN=723, FN=0, Flags=.....C, SSID=IA 2
1428 13.762607	22:58:38:50:79:94	Broadcast		802.11	139	Probe Request, SN=734, FN=0, Flags=.....C, SSID=IA 2
1523 14.889662	HironTe_e2:c8:76	ea:52:54:89:2b:72		802.11	517	Probe Response, SN=1914, FN=0, Flags=.....C, BI=100, SSID=NOS-C876
1526 14.9895248	PTInovac_45:be:30	ea:52:54:89:2b:72		802.11	380	Probe Response, SN=2651, FN=0, Flags=.....C, BI=100, SSID=MEO-45BE3

Figura 13: Tráfego das tramas *probing request/response*.

Este filtro irá exibir todas as tramas de *Probe Request* (`wlan.fc.type_subtype == 0x04`) e *Probe Response* (`wlan.fc.type_subtype == 0x05`) capturadas na sua captura do Wireshark.

### 3.8 Questão 12:

*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?*

```
▶ Frame 788: 110 bytes on wire (880 bits), 110 bytes captured ( 
  ▶ Radiotap Header v0, Length 36
  ▶ 802.11 radio information
  ▶ 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: AltoBeam_08:32:99 (a4:ef:15:08:32:99)
      Source address: AltoBeam_08:32:99 (a4:ef:15:08:32:99)
      BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
      .... .... 0000 = Fragment number: 0
      0100 0101 0111 .... = Sequence number: 1111
      Frame check sequence: 0x098f83be [unverified]
      [FCS Status: Unverified]
  ▶ IEEE 802.11 Wireless Management
    ▶ Tagged parameters (46 bytes)

  ▶ Frame 789: 485 bytes on wire (3880 bits), 485 bytes captured
  ▶ Radiotap Header v0, Length 36
  ▶ 802.11 radio information
  ▶ IEEE 802.11 Probe Response, Flags: .......c
    Type/Subtype: Probe Response (0x0005)
    ▶ Frame Control Field: 0x5000
      .000 0001 0011 1010 = Duration: 314 microseconds
      Receiver address: AltoBeam_08:32:99 (a4:ef:15:08:32:99)
      Destination address: AltoBeam_08:32:99 (a4:ef:15:08:32:99)
      Transmitter address: HitronTe_ee:2e:c6 (90:aa:c3:ee:2e:c6)
      Source address: HitronTe_ee:2e:c6 (90:aa:c3:ee:2e:c6)
      BSS Id: HitronTe_ee:2e:c6 (90:aa:c3:ee:2e:c6)
      .... .... 0000 = Fragment number: 0
      1000 1001 0011 .... = Sequence number: 2195
      Frame check sequence: 0xd9b31174 [unverified]
      [FCS Status: Unverified]
  ▶ IEEE 802.11 Wireless Management
    ▶ Fixed parameters (12 bytes)
    ▶ Tagged parameters (409 bytes)
```

Figura 14: Informação sobre as tramas probing request/response.

Através da figura fornecida, podemos observar que há um pedido de sondagem (*probing request*) identificado pelo campo de controle de quadro (*Frame Control Field*) com o valor 0x4000. Além disso, encontramos a resposta à sondagem (*probing*

*response*), identificada pelo campo de controle de quadro com o valor 0x5000. Ao analisar estas duas tramas, podemos verificar que o endereço do transmissor (*Transmitter Address*) da primeira trama é igual ao endereço de destino (*Destination Address*) da segunda trama. Assim temos que:

- Através da imagem fornecida, podemos observar que a trama *probing request* está a ser enviada para o sistema *Broadcast*, enquanto a trama *probing response* está sendo endereçada ao sistema HitronTe\_ee:2e:c6,
- A *Probe Request*, enviada por uma estação (STA), tem a finalidade de obter informações sobre as redes 802.11 próximas, ou seja, determinar quais pontos de acesso (APs) estão dentro do alcance do seu rádio. Já a *Probe Response*, enviada por um AP, fornece informações relevantes à STA, como o nome da rede sem fio (SSID), as taxas de dados suportadas, o tipo de criptografia (se aplicável) e outras capacidades do AP.

## 4 Questões e respostas III - Processo de Associação

### 4.1 Questão 13:

*Identifique uma sequência de tramas que corresponda a um processo de associação realizado com sucesso entre a STA e o AP, incluindo a fase de autenticação*

Para obter o conjunto completo de conexões entre a estação (STA) e o ponto de acesso (AP) em um processo de associação, foi necessário desenvolver um filtro que nos fornecesse, de maneira conveniente, um conjunto organizado dessas conexões.

Sendo assim, o filtro aplicado foi:

```
wlan.fc.type == 0  
and (wlan.fc.type subtype == 0  
or wlan.fc.type subtype == 1  
or wlan.fc.type subtype == 11)
```

A tabela apresentada contém informações sobre os filtros e as tramas associadas a eles. Estamos, essencialmente, filtrando os quadros de gerenciamento (*Management Frames*) e, dentro deles, aqueles que são do tipo "Association Request"(Solicitação de Associação), "Association Response"(Resposta de Associação) e "Authentication"(Autenticação). Essas são fases relevantes do processo de associação.

Após a aplicação do filtro, obtiveram-se as tramas seguintes:

wlan.fc.type==0 & (wlan.fc.type_subtype==0    wlan.fc.type_subtype==1    wlan.fc.type_subtype==11)						
>	Time	Source	Destination	Protocol	Length	Info
7739 67.948851	fe:01:24:24:88:7e	LGInnote_73:d8:2f	802.11	82	Authentication, SN=1646, FN=0, Flags=.....C	
8472 73.458730	AzureWav_0f:0e:9b	HitronTe_f3:9a:46	802.11	70	Authentication, SN=262, FN=0, Flags=.....C	
8474 73.458775	HitronTe_f3:9a:46	AzureWav_0f:0e:9b	802.11	70	Authentication, SN=1965, FN=0, Flags=.....C	
8476 73.459546	AzureWav_0f:0e:9b	HitronTe_f3:9a:46	802.11	164	Association Request, SN=263, FN=0, Flags=.....C, SSID=FlyingNet	
8478 73.459638	HitronTe_f3:9a:46	AzureWav_0f:0e:9b	802.11	210	Association Response, SN=1966, FN=0, Flags=.....C	

Figura 15: Processo de associação completo - redes IEEE 802.11.

Observa-se que o processo de associação consiste em duas etapas, autenticação e associação, ambas com uma solicitação e uma resposta:

- Solicitação de Autenticação - *Frame 8472*
- Resposta de Autenticação - *Frame 8474*
- Solicitação de Associação - *Frame 8476*
- Resposta de Associação - *Frame 8478*

#### 4.2 Questão 14:

Efetue um diagrama que ilustre a sequência de todas as tramas trocadas no processo.

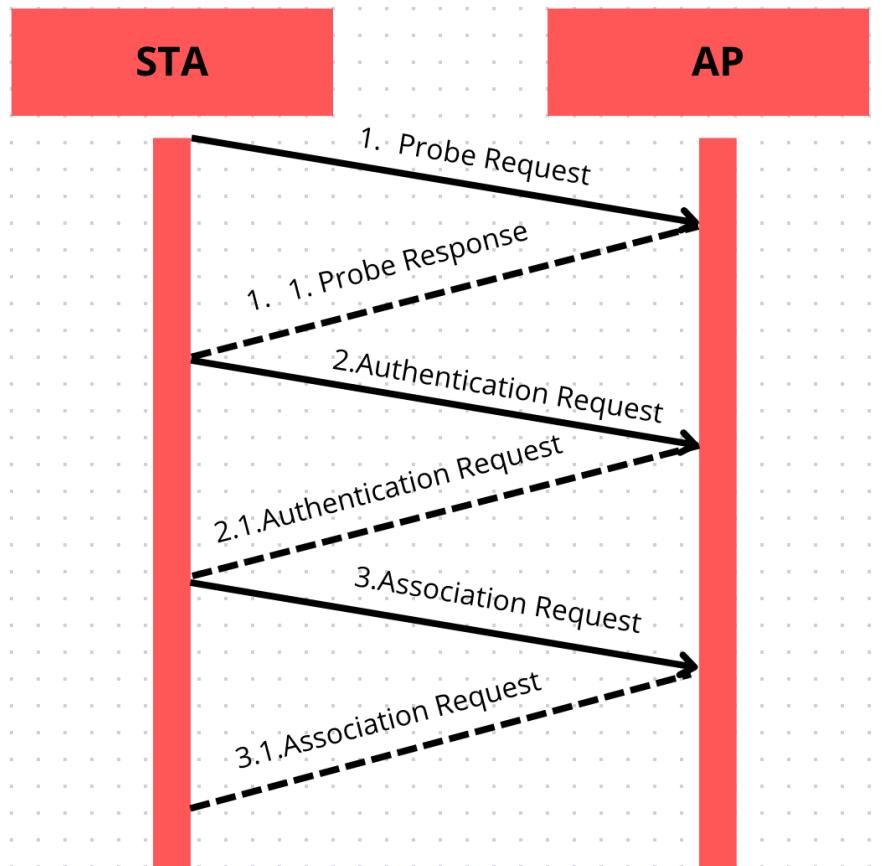


Figura 16: Processo de associação completo - diagrama - redes 802.11.

Além disso, este processo também inclui as tramas de sondagem (*probing*) que estão representadas no diagrama acima.

## 5 Questões e respostas IV - Transferência de Dados

### 5.1 Questão 15:

Considere a trama de dados nº8503. Sabendo que o campo Frame Control contido no cabeçalho das tramas 802.11 permite especificar a direccionalidade das tramas, o que pode concluir face à direccionalidade dessa trama, será local à WLAN?

Analizando a flag referente ao DS status, da figura abaixo, podemos concluir que a direccionalidade desta trama pode ser observada através dos campos "To DS: 1" e "From DS: 0". O primeiro indica que a trama é direcionada ao DS e o segundo que não é verdade que a trama é proveniente do DS, ou seja, podemos concluir que a trama é destinada à WLAN (Wireless Local Area Network) e não é proveniente desta mesma.

```
802.11 radio information
IEEE 802.11 QoS Data, Flags: .p.....TC
Type/Subtype: QoS Data (0x0028)
Frame Control Field: 0x8841
    .... ..00 = Version: 0
    .... 10.. = Type: Data frame (2)
    1000 .... = Subtype: 8
Flags: 0x41
    .... ..01 = DS status: Frame from STA to DS via an AP (To DS: 1 From DS: 0) (0x1)
    .... ..0.. = More Fragments: This is the last fragment
    .... 0... = Retry: Frame is not being retransmitted
    ...0 .... = PWR MGT: STA will stay up
    ..0. .... = More Data: No data buffered
    .1... .... = Protected flag: Data is protected
    0... .... = +HTC/Order flag: Not strictly ordered
.000 0000 0011 0000 = Duration: 48 microseconds
Receiver address: HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)
Transmitter address: Another device (00:1f:00:0f:00:01)
```

Figura 17: Trama de dados nº8503.

### 5.2 Questão 16:

Para a trama de dados nº8503, transcreva os endereços MAC em uso, identificando quais os endereços correspondentes à estação sem fios (STA), ao AP e ao router de acesso ao sistema de distribuição (DS)?

```

    0.... .... = +HTC/Order flag: Not strictly ordered
.000 0000 0011 0000 = Duration: 48 microseconds
Receiver address: HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)
Transmitter address: AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)
Destination address: IPv6mcast_16 (33:33:00:00:00:16)
Source address: AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)
BSS Id: HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)
STA address: AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)
.... .... 0000 = Fragment number: 0
0000 0000 0000 .... = Sequence number: 0
Frame check sequence: 0x57cf2fa2 [unverified]
[FCS Status: Unverified]
↳ Qos Control: 0x0000
↳ CCMP parameters

```

Figura 18: Endereços MAC relativos à trama nº8503.

Com base na trama da figura acima concluímos assim que os endereços MAC correspondentes são:

- STA : 80:c5:f2:0f:0e:9b
- AP : 74:9b:e8:f3:9a:46
- Router : 74:9b:e8:f3:9a:46

### 5.3 Questão 17:

*Como interpreta a trama nº8521 face à sua direccionalidade e endereçamento MAC?*

```

↳ Frame Control Field: 0x8842
.... .00 = Version: 0
.... 10.. = Type: Data frame (2)
1000 .... = Subtype: 8
↳ Flags: 0x42
.... .10 = DS status: Frame from DS to a STA via AP(To DS: 0 From DS: 1) (0x2)
.... .0.. = More Fragments: This is the last fragment
.... 0... = Retry: Frame is not being retransmitted
...0 .... = PWR MGT: STA will stay up
..0. .... = More Data: No data buffered
.1... .... = Protected flag: Data is protected
0.... .... = +HTC/Order flag: Not strictly ordered
.000 0000 0011 1100 = Duration: 60 microseconds
Receiver address: AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)
Transmitter address: HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)
Destination address: AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)
Source address: 76:9b:e8:f3:9a:43 (76:9b:e8:f3:9a:43)
BSS Id: HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)
STA address: AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)
.... .... 0000 = Fragment number: 0
0000 0000 0010 .... = Sequence number: 2
Frame check sequence: 0x72f260b4 [unverified]
[FCS Status: Unverified]

```

Figura 19: Endereços MAC relativos à trama nº8521.

Analizando a figura acima conseguimos concluir que esta trama parte do DS com destino ao STA, pois "To DS: 0" e "From DS: 1". Isto é comprovado também pelo

endereçamento MAC, pois o BSS Id é igual *ap Source* e o STA *address* é igual ao *Destination address*.

#### 5.4 Questão 18:

*Que subtipo de tramas de controlo são transmitidas ao longo da transferência de dados acima mencionada? Tente explicar a razão de terem de existir (contrariamente ao que acontece numa rede Ethernet.)*

De forma a apenas visualizar as tramas de controlo utilizamos o filtro: **wlan.fc.type == 1**.

wlan.fc.type==1						
o.	Time	Source	Destination	Protocol	Length	Info
8492	73.487828	AzureWav_0f:0e:9b (... 802.11			48	Acknowledgement, Flags=.....C
8493	73.489842	Time (format as specified) ce:90:6f:21:42:3a (... 802.11			68	802.11 Block Ack, Flags=.....C
8494	73.489848	PTInovac_d6:88:50 (... ce:90:6f:21:42:3a (... 802.11			76	Request-to-send, Flags=.....C
8495	73.492500	PTInovac_d6:88:50 (... ce:90:6f:21:42:3a (... 802.11			76	Request-to-send, Flags=.....C
8496	73.496901	PTInovac_d6:88:50 (... ce:90:6f:21:42:3a (... 802.11			76	Request-to-send, Flags=.....C
8500	73.511572	AzureWav_0f:0e:9b (... 802.11			48	Acknowledgement, Flags=.....C
8502	73.511582	HironTe_f3:9a:46 (... AzureWav_0f:0e:9b (... 802.11			68	802.11 Block Ack, Flags=.....C
8507	73.530760	HironTe_f3:9a:46 (... AzureWav_0f:0e:9b (... 802.11			68	802.11 Block Ack, Flags=.....C
8511	73.542835	HironTe_f3:9a:46 (... 802.11			48	Acknowledgement, Flags=.....C
8513	73.542845	AzureWav_0f:0e:9b (... 802.11			48	Acknowledgement, Flags=.....C
8515	73.544136	HironTe_f3:9a:46 (... 802.11			48	Acknowledgement, Flags=.....C
8518	73.544151	AzureWav_0f:0e:9b (... 802.11			48	Acknowledgement, Flags=.....C
8519	73.544155	HironTe_f3:9a:46 (... AzureWav_0f:0e:9b (... 802.11			76	Request-to-send, Flags=.....C
8520	73.544159	HironTe_f3:9a:46 (... 802.11			72	Clear-to-send, Flags=.....C
8522	73.544167	AzureWav_0f:0e:9b (... HironTe_f3:9a:46 (... 802.11			68	802.11 Block Ack, Flags=.....C
8523	73.544170	HironTe_f3:9a:46 (... AzureWav_0f:0e:9b (... 802.11			76	Request-to-send, Flags=.....C
8524	73.544174	HironTe_f3:9a:46 (... 802.11			72	Clear-to-send, Flags=.....C
8526	73.544219	AzureWav_0f:0e:9b (... HironTe_f3:9a:46 (... 802.11			68	802.11 Block Ack, Flags=.....C
8527	73.544224	PTInovac_d6:88:50 (... ce:90:6f:21:42:3a (... 802.11			76	Request-to-send, Flags=.....C
8528	73.552942	PTInovac_d6:88:50 (... ce:90:6f:21:42:3a (... 802.11			76	Request-to-send, Flags=.....C
8529	73.559878	PTInovac_d6:88:50 (... ce:90:6f:21:42:3a (... 802.11			76	Request-to-send, Flags=.....C
8531	73.560179	AzureWav_0f:0e:9b (... 802.11			48	Acknowledgement, Flags=.....C
8533	73.561412	HironTe_f3:9a:46 (... 802.11			48	Acknowledgement, Flags=.....C

Figura 20: Tramas de Acknowledgment.

O tipo específico de tramas de controlo que são transmitidas são os *Acknowledgments* (ACK). Essas tramas são essenciais, pois as redes sem fio têm uma maior probabilidade de perda de dados em comparação com as redes *Ethernet*. O nó transmissor não pode ter certeza de que o nó receptor recebeu corretamente as informações sem a confirmação por meio das tramas ACK. Estas tramas servem portanto para avisar a fonte que a mensagem chegou corretamente ao destino. Caso contrário, a origem não teria possibilidade de saber se o conteúdo enviado chegou corretamente ao destino.

#### 5.5 Questão 19:

*O uso de tramas Request To Send e Clear To Send, apesar de opcional, é comum para efetuar "pré-reserva" do acesso ao meio quando se pretende enviar tramas de dados, com o intuito de reduzir o número de colisões resultante maioritariamente de STAs escondidas. Para o exemplo acima, verifique se está a ser usada a opção RTS/CTS na troca de dados entre a STA e o AP/Router da WLAN, identificando a direccionalidade das tramas e os sistemas envolvidos. Dê um exemplo de uma transferência de dados em que é usada a opção RTC/CTS e um outro em que não é usada.*

De forma a encontrar transferências de dados em que é usada a opção RTC/CTS em primeiro lugar aplicamos o seguinte filtro: wlan.fc.type\_subtype == 0x1b || wlan.fc.type\_subtype == 0x1c

wlan.fc.type_subtype==0x1b    wlan.fc.type_subtype==0x1c						
O.	Time	Source	Destination	Protocol	Length	Info
8446	73.147630	PTInovac_d6:88:50	(... ce:90:6f:21:42:3a (... 802.11	76 Request-to-send, Flags=.....c		
8452	73.177063	PTInovac_d6:88:50	(... ce:90:6f:21:42:3a (... 802.11	76 Request-to-send, Flags=.....c		
8487	73.485446	PTInovac_d6:88:50	(... ce:90:6f:21:42:3a (... 802.11	76 Request-to-send, Flags=.....c		
8488	73.485452	PTInovac_d6:88:50	(... ce:90:6f:21:42:3a (... 802.11	76 Request-to-send, Flags=.....c		
8494	73.489048	PTInovac_d6:88:50	(... ce:90:6f:21:42:3a (... 802.11	76 Request-to-send, Flags=.....c		
8495	73.492500	PTInovac_d6:88:50	(... ce:90:6f:21:42:3a (... 802.11	76 Request-to-send, Flags=.....c		
8496	73.496901	PTInovac_d6:88:50	(... ce:90:6f:21:42:3a (... 802.11	76 Request-to-send, Flags=.....c		
8519	73.544155	HitronTe_f3:9a:46	(... AzureWav_0f:0e:9b (... 802.11	76 Request-to-send, Flags=.....c		
8520	73.544159	HitronTe_f3:9a:46	(... AzureWav_0f:0e:9b (... 802.11	72 Clear-to-send, Flags=.....c		
8523	73.544170	HitronTe_f3:9a:46	(... AzureWav_0f:0e:9b (... 802.11	76 Request-to-send, Flags=.....c		
8524	73.544174	HitronTe_f3:9a:46	(... AzureWav_0f:0e:9b (... 802.11	72 Clear-to-send, Flags=.....c		
8527	73.544224	PTInovac_d6:88:50	(... ce:90:6f:21:42:3a (... 802.11	76 Request-to-send, Flags=.....c		
8528	73.552942	PTInovac_d6:88:50	(... ce:90:6f:21:42:3a (... 802.11	76 Request-to-send, Flags=.....c		
8529	73.559878	PTInovac_d6:88:50	(... ce:90:6f:21:42:3a (... 802.11	76 Request-to-send, Flags=.....c		
8536	73.564447	PTInovac_d6:88:50	(... ce:90:6f:21:42:3a (... 802.11	76 Request-to-send, Flags=.....c		
8537	73.564463	PTInovac_d6:88:50	(... ce:90:6f:21:42:3a (... 802.11	76 Request-to-send, Flags=.....c		
8541	73.587828	PTInovac_d6:88:50	(... ce:90:6f:21:42:3a (... 802.11	76 Request-to-send, Flags=.....c		
8543	73.590971	PTInovac_d6:88:50	(... ce:90:6f:21:42:3a (... 802.11	76 Request-to-send, Flags=.....c		
8544	73.591043	PTInovac_d6:88:50	(... ce:90:6f:21:42:3a (... 802.11	76 Request-to-send, Flags=.....c		
8545	73.594214	PTInovac_d6:88:50	(... ce:90:6f:21:42:3a (... 802.11	76 Request-to-send, Flags=.....c		
8546	73.603494	PTInovac_d6:88:50	(... ce:90:6f:21:42:3a (... 802.11	76 Request-to-send, Flags=.....c		
8551	73.619045	PTInovac_d6:88:50	(... ce:90:6f:21:42:3a (... 802.11	76 Request-to-send, Flags=.....c		

Figura 21: Filtro aplicado.

Daqui selecionamos a transferência de dados iniciada na trama 519 e terminada na trama 522.

8518 / 73.544151	AzureWav_0f:0e:9b	HitronTe_f3:9a:46	082.11	/3 ACTION, SN=0x3, FN=0, Flags=....R..., Dialog Token=...
8519	73.544155	HitronTe_f3:9a:46	AzureWav_0f:0e:9b	082.11
				48 Acknowledgement, Flags=.....c
8520	73.544159	HitronTe_f3:9a:46	AzureWav_0f:0e:9b	082.11
8521	73.544163	76:9b:e8:f3:9a:43	AzureWav_0f:0e:9b	082.11
8522	73.544167	AzureWav_0f:0e:9b	HitronTe_f3:9a:46	082.11
8523	73.544170	HitronTe_f3:9a:46	AzureWav_0f:0e:9b	082.11
8524	73.544174	HitronTe_f3:9a:46	AzureWav_0f:0e:9b	082.11

Figura 22: Transferência de dados com RTC/CTS.

## 6 Conclusão

O principal objetivo deste trabalho é explorar diversos aspectos relacionados às redes sem fio (Wi-Fi).

No início, abordamos o Acesso Rádio, onde exploramos a camada física das redes sem fio, incluindo elementos como canal e frequência.

Em seguida, comparamos o *scanning* ativo e passivo, destacando que o primeiro é realizado através das tramas *beacon*, permitindo descobrir os pontos de acesso disponíveis, enquanto o segundo utiliza o *probe response*.

No terceiro ponto, discutimos o Processo de Associação, que é necessário para estabelecer a conexão entre um dispositivo e um ponto de acesso. Esse processo envolve um pedido de associação feito pelo dispositivo, seguido da resposta do ponto de acesso.

Por fim, analisamos o processo de Transferência de Dados, considerando dois fatores: informações obtidas nas tramas e o controle da transferência.

Além disso, aprofundamos o nosso conhecimento sobre as funcionalidades da ferramenta *Wireshark*, o que nos permitiu aproveitá-la de forma mais eficiente.

Em resumo, o grupo considera que o trabalho foi bem-sucedido, pois conseguimos responder a todas as perguntas, aprofundando e solidificando os conceitos teóricos ensinados.