



Universidade do Minho

Licenciatura em Engenharia Informática

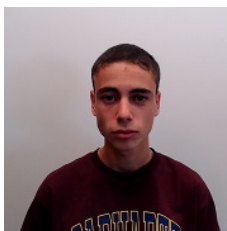
Redes de Computadores

Trabalho Prático 4

Grupo 34



Diogo Rebelo
(A93278)



Hugo Brandão
(A93287)



Gonçalo Freitas
(A93297)

20 de junho de 2023

Conteúdo

1	Questões e Respostas	3
1	Ponto nº 4: Captura e análise de Tramas Ethernet	3
1.1	Alínea 1	3
1.2	Alínea 2	3
1.3	Alínea 3	4
2	Ponto nº 5: Scanning Passivo e Scanning Ativo	5
2.1	Alínea 4	5
2.2	Alínea 5	6
3	Alínea 6	6
4	Alínea 7	7
5	Alínea 8	8
6	Alínea 9	8
7	Alínea 10	11
8	Alínea 11	12
9	Ponto nº 6: Processo de Associação	14
9.1	Alínea 12	14
9.2	Alínea 13	16
10	Ponto 7: Transferência de Dados	17
10.1	Alínea 14	17
10.2	Alínea 15	17
10.3	Alínea 16	18
10.4	Alínea 17	19
10.5	Alínea 18	19
2	Conclusão	22

Lista de Figuras

1	Trama selecionada (34)	3
2	Informações de rádio	3
3	Débitos suportados	4
4	Tipo e subtipo da trama	5
5	Endereços MAC em uso na trama	6
6	Debitos da trama	6
7	Beacon Interval	7
8	SSIDs a operar na vizinhança da STA	8

9	FCS	8
10	Definições <i>default</i>	9
11	Definição alterada	9
12	Filtro sugerido	9
13	Filtro para todos os erros	10
14	FCS atualizado	10
15	Tráfego das tramas <i>probing request/response</i>	11
16	Informação sobre as tramas <i>probing request/response</i>	12
17	Comandos e respectivas associações.	14
18	Processo de associação completo - redes IEEE 802.11.	15
19	Processo de associação completo - diagrama - redes 802.11.	16
20	Trama de dados nº431	17
21	Endereços MAC relativos à trama nº431	18
22	<i>Frame Control Field</i> da trama nº433	18
23	Tramas de <i>Acknowledgment</i>	19
24	Informação das tramas 427 a 440	20
25	Filtro aplicado	20
26	Transferência de dados com RTC/CTS	20
27	Transferência de dados sem RTC/CTS	21

1. Questões e Respostas

Ponto nº 4: Captura e análise de Tramas Ethernet

Selecione a trama de ordem XX correspondente ao seu identificador de grupo (TurnoGrupo, e.g., 11).

Seguindo as instruções do enunciado chegamos à seguinte trama:

No.	Time	Source	Destination	Protocol	Length	Info
34	0.921756	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2101, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
> Frame 34: 296 bytes on wire (2368 bits), 296 bytes captured (2368 bits)						
> Radiotap Header v0, Length 25						
> 802.11 radio information						
> IEEE 802.11 Beacon frame, Flags:C						
> IEEE 802.11 Wireless Management						

Figura 1: Trama selecionada (34)

Alínea 1

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

Analisando a seguinte imagem chegamos à conclusão que a rede está a operar a uma frequência de 2467MHz no canal 12.

802.11 radio information
PHY type: 802.11b (HR/DSSS) (4)
Short preamble: False
Data rate: 1,0 Mb/s
Channel: 12
Frequency: 2467MHz

Figura 2: Informações de rádio

Alínea 2

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

Tal como conseguimos verificar na primeira linha da Figura 2, a versão que está a ser usada é a 802.11b.

Alínea 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 a que a trama escolhida foi enviada foi 1,0 Mb/s (linha *Data rate* da Figura 2). Após um pouco de investigação teórica, chegamos à conclusão que o débito máximo da versão 802.11b é 11Mb/s.

Contudo analisando a informação da trama no *Wireshark* verificamos uma incongruência:

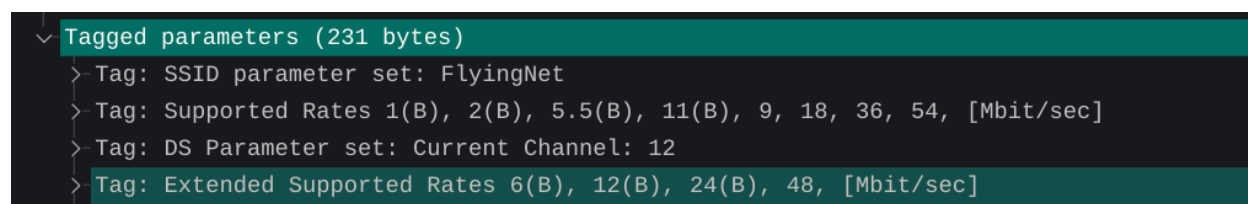


Figura 3: Débitos suportados

Na figura acima um débito máximo suportado é 54 Mb/s, o qual é característico da versão 802.11g da norma. Tendo isto em conta supomos que existe algum erro na análise do *Wireshark*. De qualquer das formas, o débito apresentado não é o débito máximo.

Ponto nº 5: Scanning Passivo e Scanning Ativo

Como referido, as tramas beacon permitem efetuar *scanning* passivo em redes IEEE 802.11 (Wi-Fi). Para a captura de tramas disponibilizada, e considerando XX o seu nº de grupo, responda às seguintes questões:

Alínea 4

Selecione a trama *beacon* de ordem $(260 + XX)$. 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)?

A trama selecionada é a 294 $(260 + 34)$, e como podemos ver na seguinte imagem, esta pertence ao tipo *Management* (0) e o seu subtipo é *Beacon* (8). Sendo possível através do anexo fornecido no enunciado, verificar que estes pertencem ao *Frame Control*.

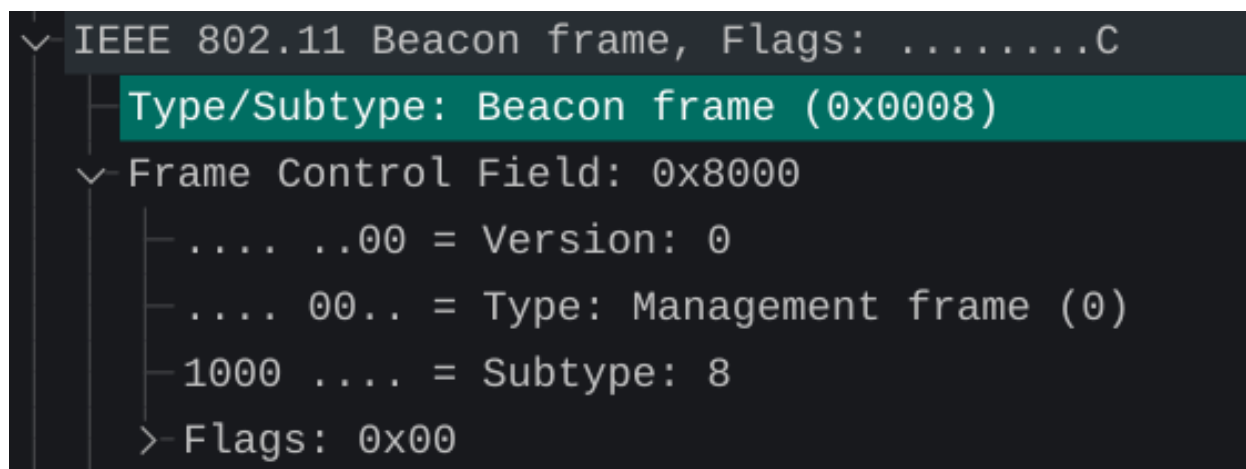


Figura 4: Tipo e subtipo da trama

Alínea 5

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

Analisando 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: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
Source address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
```

Figura 5: Endereços MAC em uso na trama

Sendo assim conclui-se que a origem tem um endereço MAC bc:14:01:af:b1:98 e o destino sendo ff:ff:ff:ff:ff:ff implica que esta trama foi transmitida para todos os nós da rede.

Alínea 6

Uma trama beacon anuncia que o AP pode suportar vários débitos de base, 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), 9, 18, 36, 54, [Mbit/sec]
> Tag: DS Parameter set: Current Channel: 12
> Tag: Extended Supported Rates 6(B), 12(B), 24(B), 48, [Mbit/sec]
```

Figura 6: 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

- 9 Mb/s
- 18 Mb/s
- 36 Mb/s
- 54 Mb/s

E os débitos adicionais suportados são:

- 6 Mb/s
- 12 Mb/s
- 24 Mb/s
- 48 Mb/s

Alínea 7

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.

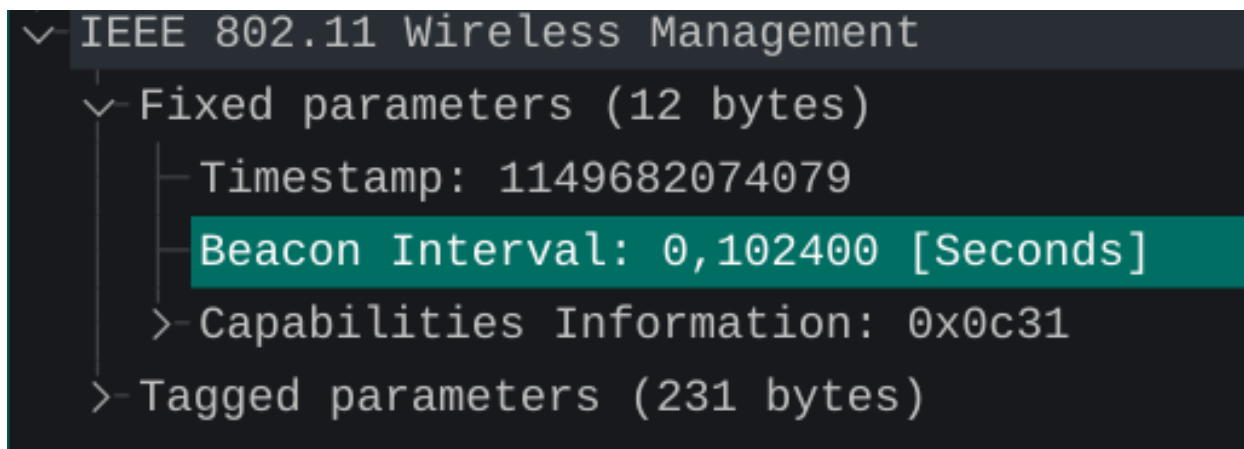


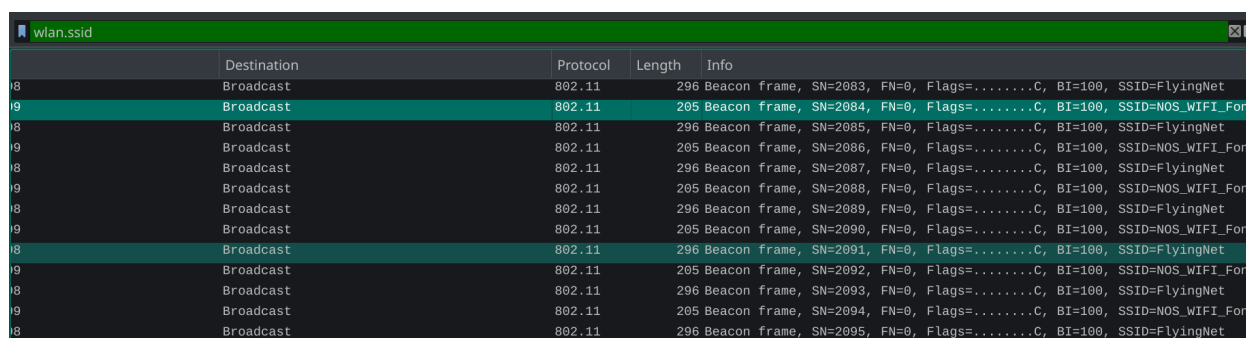
Figura 7: Beacon Interval

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

Alínea 8

Identifique e liste os SSIDs dos APs que estão a operar na vizinhança da STA de captura? Explícite 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 a utilização deste filtro chegamos à conclusão que os dois únicos SSIDs são *FlyingNet* e *NOS_WIFI_Fon*.



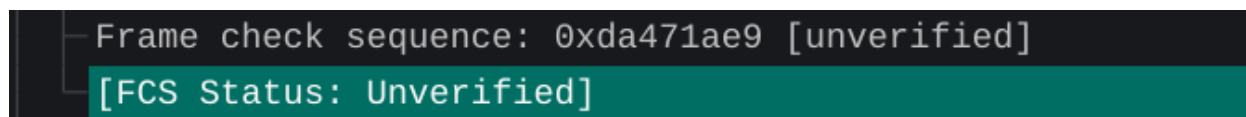
	Destination	Protocol	Length	Info
18	Broadcast	802.11	296	Beacon frame, SN=2083, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
19	Broadcast	802.11	205	Beacon frame, SN=2084, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
18	Broadcast	802.11	296	Beacon frame, SN=2085, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
19	Broadcast	802.11	205	Beacon frame, SN=2086, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
18	Broadcast	802.11	296	Beacon frame, SN=2087, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
19	Broadcast	802.11	205	Beacon frame, SN=2088, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
18	Broadcast	802.11	296	Beacon frame, SN=2089, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
19	Broadcast	802.11	205	Beacon frame, SN=2090, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
18	Broadcast	802.11	296	Beacon frame, SN=2091, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
19	Broadcast	802.11	205	Beacon frame, SN=2092, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
18	Broadcast	802.11	296	Beacon frame, SN=2093, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
19	Broadcast	802.11	205	Beacon frame, SN=2094, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
18	Broadcast	802.11	296	Beacon frame, SN=2095, FN=0, Flags=.....C, BI=100, SSID=FlyingNet

Figura 8: SSIDs a operar na vizinhança da STA

Alínea 9

Verifique se está a ser usado o método de deteção de erros (CRC)

Inicialmente ao verificar se o método de deteção de erros está ativo deparamo-nos com a seguinte informação.



```

Frame check sequence: 0xda471ae9 [unverified]
[FCS Status: Unverified]
  
```

Figura 9: FCS

Daqui retiramos que o CRC não está ativo, contudo, ao investigar as configurações do *Wireshark* verificamos que a opção relacionada com a deteção de erros estava desativada, procedendo assim a ativá-la.

Search: wlan.check

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

Figura 10: Definições *default*

Search: wlan.check

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

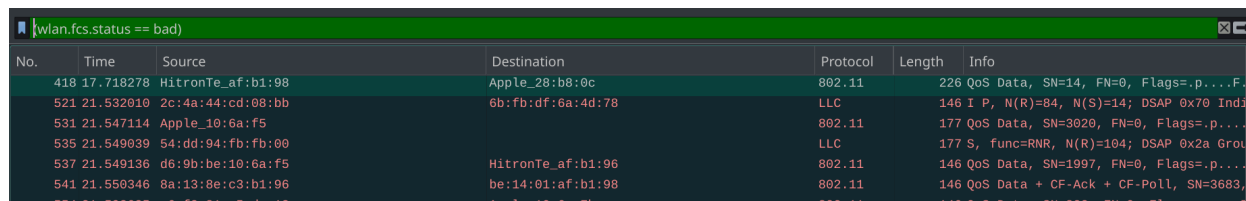
Figura 11: Definição alterada

Tendo estas novas condições mesmo assim, utilizando o filtro proposto não encontramos nenhum resultado. Contudo ao continuar a analisar as tramas e utilizar outros filtros conseguimos verificar que, de facto, o controlo de erros está ativo.

(wlan.fc.type_subtype == 0x08) && (wlan.fcs.status == bad)

No.	Time	Source	Destination	Protocol	Length	Info

Figura 12: Filtro sugerido



Wireshark packet list with filter `wlan.fcs.status == bad`. The table shows several packets, but none are displayed, indicating that the filter successfully filtered out all packets where the FCS status was 'Good'.

No.	Time	Source	Destination	Protocol	Length	Info
418	17.718278	HitronTe_af:b1:98	Apple_28:b8:0c	802.11	226	QoS Data, SN=14, FN=0, Flags=p...F.
521	21.532010	2c:4a:44:cd:08:bb	6b:fb:df:6a:4d:78	LLC	146	I P, N(R)=84, N(S)=14; DSAP 0x70 Indi
531	21.547114	Apple_10:6a:f5		802.11	177	QoS Data, SN=3020, FN=0, Flags=p...
535	21.549039	54:dd:94:fb:fb:00		LLC	177	S, func=RNR, N(R)=104; DSAP 0x2a Grou
537	21.549136	d6:0b:be:10:6a:f5	HitronTe_af:b1:96	802.11	146	QoS Data, SN=1907, FN=0, Flags=p...
541	21.550346	8a:13:8e:c3:b1:96	be:14:01:af:b1:98	802.11	146	QoS Data + CF-Ack + CF-Poll, SN=3683,
554	21.582635	a6:f2:81:a5:dc:12	Apple_18:6a:7b	802.11	146	QoS Data, SN=832, FN=0, Flags=p...

Figura 13: Filtro para todos os erros

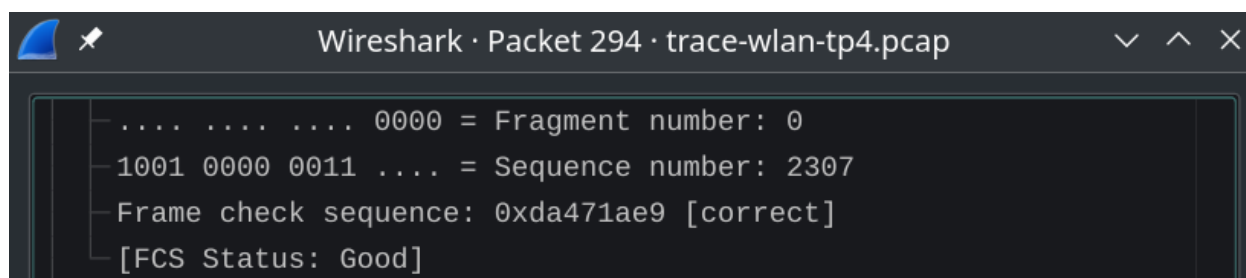


Figura 14: FCS atualizado

Concluindo, é necessário detecção de erros pois numa rede sem fios é mais provável a existência de perdas de pacotes.

Alínea 10

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

O filtro, adaptado à sua utilização no Wireshark, que permite essa visualização é:

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

Adaptando o filtro a uma expressão lógica, fica:

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

Estamos a testar o subtipo das tramas, filtrando as de *probing request* (4) e as de *probing response* (5).

A visualização após aplicação do filtro, comprova-se a apresentação de tramas desse tipo:

wlan.fc.type_subtype==4 or wlan.fc.type_subtype==5						
No.	Time	Source	Destination	Protocol	Length	Info
1300	53.746911	Apple_10:6a:f5	Broadcast	802.11	155	Probe Request, SN=2516, FN=0, Flags=.....C, SSID=Wildcard ...
2467	70.147855	ea:a4:64:7b:b9:7a	Broadcast	802.11	167	Probe Request, SN=2540, FN=0, Flags=.....C, SSID=2WIRE-PT...
2468	70.149098	ea:a4:64:7b:b9:7a	Broadcast	802.11	155	Probe Request, SN=2541, FN=0, Flags=.....C, SSID=Wildcard ...
2469	70.149792	HitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	411	Probe Response, SN=2332, FN=0, Flags=.....C, BI=100, SSID=...
2471	70.150537	HitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	411	Probe Response, SN=2333, FN=0, Flags=.....C, BI=100, SSID=...
2473	70.151237	HitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	411	Probe Response, SN=2334, FN=0, Flags=.....C, BI=100, SSID=...
2475	70.151709	HitronTe_af:b1:99	ea:a4:64:7b:b9:7a	802.11	201	Probe Response, SN=2335, FN=0, Flags=.....C, BI=100, SSID=...
2477	70.152099	HitronTe_af:b1:99	ea:a4:64:7b:b9:7a	802.11	201	Probe Response, SN=2336, FN=0, Flags=.....C, BI=100, SSID=...
2479	70.152570	HitronTe_af:b1:99	ea:a4:64:7b:b9:7a	802.11	201	Probe Response, SN=2337, FN=0, Flags=.....C, BI=100, SSID=...
2603	72.179215	Apple_10:6a:f5	Broadcast	802.11	164	Probe Request, SN=2563, FN=0, Flags=.....C, SSID=FlyingNet
2606	72.179924	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	411	Probe Response, SN=2346, FN=0, Flags=.....C, BI=100, SSID=...
2608	72.180590	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	411	Probe Response, SN=2347, FN=0, Flags=.....C, BI=100, SSID=...
2610	72.181275	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	411	Probe Response, SN=2348, FN=0, Flags=.....C, BI=100, SSID=...
2616	72.201570	Apple_10:6a:f5	Broadcast	802.11	164	Probe Request, SN=2565, FN=0, Flags=.....C, SSID=FlyingNet
2617	72.202150	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	411	Probe Response, SN=2350, FN=0, Flags=.....C, BI=100, SSID=...
2619	72.202807	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	411	Probe Response, SN=2351, FN=0, Flags=.....C, BI=100, SSID=...
2621	72.203485	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	411	Probe Response, SN=2352, FN=0, Flags=.....C, BI=100, SSID=...
2650	72.488998	Apple_10:6a:f5	Broadcast	802.11	164	Probe Request, SN=2585, FN=0, Flags=.....C, SSID=FlyingNet
2653	72.502553	Apple_10:6a:f5	Broadcast	802.11	164	Probe Request, SN=2586, FN=0, Flags=.....C, SSID=FlyingNet
2677	72.568343	Apple_10:6a:f5	Broadcast	802.11	164	Probe Request, SN=2589, FN=0, Flags=.....C, SSID=FlyingNet
2678	72.578258	Apple_10:6a:f5	Broadcast	802.11	164	Probe Request, SN=2590, FN=0, Flags=.....C, SSID=FlyingNet
4455	82.621343	7c:ea:6d:ff:a2:cc	Broadcast	802.11	71	Probe Request, SN=62, FN=0, Flags=.....C, SSID=Wildcard (B...

Figura 15: Tráfego das tramas *probing request/response*.

Alínea 11

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?

```
No.      Time      Source      Destination      Protocol Length Info
 2468 70.149098    ea:a4:64:7b:b9:7a Broadcast      802.11   155   Probe Request, SN=2541, FN=0,
Flags=.....C, SSID=Wildcard (Broadcast)
Frame 2468: 155 bytes on wire (1240 bits), 155 bytes captured (1240 bits)
Radiotap Header v0, Length 25
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: ea:a4:64:7b:b9:7a (ea:a4:64:7b:b9:7a)
Source address: ea:a4:64:7b:b9:7a (ea:a4:64:7b:b9:7a)
BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
.... .... 0000 = Fragment number: 0
1001 1110 1101 .... = Sequence number: 2541
Frame check sequence: 0xb4f532e2 [unverified]
[FCS Status: Unverified]
IEEE 802.11 Wireless Management
No.      Time      Source      Destination      Protocol Length Info
 2469 70.149792    HitronTe_af:b1:98 ea:a4:64:7b:b9:7a 802.11   411   Probe Response, SN=2332, FN=0,
Flags=.....C, BI=100, SSID=FlyingNet
Frame 2469: 411 bytes on wire (3288 bits), 411 bytes captured (3288 bits)
Radiotap Header v0, Length 25
802.11 radio information
IEEE 802.11 Probe Response, Flags: .....C
Type/Subtype: Probe Response (0x0005)
Frame Control Field: 0x5000
.000 0000 0011 0010 = Duration: 50 microseconds
Receiver address: ea:a4:64:7b:b9:7a (ea:a4:64:7b:b9:7a)
Destination address: ea:a4:64:7b:b9:7a (ea:a4:64:7b:b9:7a)
Transmitter address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
Source address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
BSS Id: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
.... .... 0000 = Fragment number: 0
1001 0001 1100 .... = Sequence number: 2332
Frame check sequence: 0xbce842e3 [unverified]
[FCS Status: Unverified]
IEEE 802.11 Wireless Management
```

Figura 16: Informação sobre as tramas *probing request/response*.

Através da imagem acima, conseguimos identificar um *probing request* (Frame Control Field: 0x4000), e a sua resposta, *probing response* (Frame Control Field: 0x5000), verificando que o Transmitter Address da primeira trama é igual ao Destination Address da segunda trama.

Em relação à análise, verificamos que:

- A trama *probing request* apresentada na figura é endereçada ao sistema **Broadcast** e a trama *probing response* surge endereçada ao sistema **HitronTe_af:b1:98**;
- A *Probe Request* enviada por uma STA ajuda a obter informações acerca das redes 802.11 na proximidade (determinar quais os APs que estão dentro do seu alcance rádio). Já a *Probe Response* enviada por um AP, ajuda a STA com algumas informações relevantes acerca de si (SSID (*wireless network name*), taxas de dados suportadas, tipo de encriptação (se aplicável) e outras capacidades do AP)[1].

Ponto nº 6: Processo de Associação

Alínea 12

Identifique uma sequência de tramas que corresponda a um processo de associação completo entre a STA e o AP, incluindo a fase de autenticação.

Como forma de obter este conjunto de tramas correspondentes a um processo de associação completo entre a STA e o AP, foi necessária a construção de um filtro que nos apresentasse o conjunto organizado das mesmas, de forma prática.

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)

Convertido na **expressão lógica** seguinte:

wlan.fc.type == 0

&& (wlan.fc.type_subtype == 0

|| wlan.fc.type_subtype == 1

|| wlan.fc.type_subtype == 11)

Frame Type/Subtype	Filter
Management Frames	wlan.fc.type==0
Association Request	wlan.fc.type_subtype==0
Association Response	wlan.fc.type_subtype==1
Reassociation Request	wlan.fc.type_subtype==2
Reassociation Response	wlan.fc.type_subtype==3
Probe Request	wlan.fc.type_subtype==4
Probe Response	wlan.fc.type_subtype==5
Beacon	wlan.fc.type_subtype==8
ATIM	wlan.fc.type_subtype==9
Disassociate	wlan.fc.type_subtype==10
Authentication	wlan.fc.type_subtype==11
Deauthentication	wlan.fc.type_subtype==12
Association Request	wlan.fc.type_subtype==0
Association Request	wlan.fc.type_subtype==0
Control Frames	wlan.fc.type==1
Power-Save Poll	wlan.fc.type_subtype==26
Request To Send - RTS	wlan.fc.type_subtype==27
Clear To Send - CTS	wlan.fc.type_subtype==28
Acknowledgement - ACK	wlan.fc.type_subtype==29
Data Frames	wlan.fc.type==2
NULL Data	wlan.fc.type_subtype==36

Figura 17: Comandos e respetivas associações.

Esta tabela contém a informação sobre os filtros e respetivas tramas associadas. Então, estamos basicamente a filtrar as *Management Frames* e, dentro destas, as que são do tipo *Association Request*, *Association Responde*, *Authentication*, fases relevantes do processo de associação.

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

wlan.fc.type==0 and (wlan.fc.type_subtype == 0 or wlan.fc.type_subtype == 1 or wlan.fc.type_subtype == 11)					
No.	Time	Source	Destination	Protocol	Length Info
2486	70.361782	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	70 Authentication, SN=2542, FN=0, Flags=.....C
2488	70.381869	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	59 Authentication, SN=2338, FN=0, Flags=.....C
2490	70.383512	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	175 Association Request, SN=2543, FN=0, Flags=.....C, SSID=Fly...
2492	70.389339	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	225 Association Response, SN=2339, FN=0, Flags=.....C
4692	83.663250	7c:ea:6d:ff:a2:cc	HitronTe_af:b1:98	802.11	59 Authentication, SN=67, FN=0, Flags=.....C
4694	83.663681	HitronTe_af:b1:98	7c:ea:6d:ff:a2:cc	802.11	59 Authentication, SN=2439, FN=0, Flags=.....C
4696	83.665976	7c:ea:6d:ff:a2:cc	HitronTe_af:b1:98	802.11	153 Association Request, SN=68, FN=0, Flags=.....C, SSID=Flyin...
4698	83.678873	HitronTe_af:b1:98	7c:ea:6d:ff:a2:cc	802.11	225 Association Response, SN=2440, FN=0, Flags=.....C
4699	83.680045	HitronTe_af:b1:98	7c:ea:6d:ff:a2:cc	802.11	225 Association Response, SN=2440, FN=0, Flags=....R...C
6915	99.967142	a8:05:ea:f5:cf:a8	e1:37:40:44:46:23	802.11	146 Authentication, SN=434, FN=1, Flags=op.P.M..C
7043	100.196334	dd:88:93:0f:ec:e9	af:40:cd:40:5f:82	802.11	146 Authentication, SN=2467, FN=4, Flags=p.P.M..C
7065	100.208375	d7:19:51:08:62:f9	6d:1b:44:1a:cc:11	802.11	146 Association Request, SN=2586, FN=7, Flags=pmPRM.TC
7163	100.403689	0a:57:13:28:40:84	79:5c:58:10:7a:cc	802.11	146 Association Response, SN=3497, FN=5, Flags=o.mP..F.C[Malforme...
13218	107.753005	20:b4:c4:ad:d7:19	d5:a5:29:9b:fe:00	802.11	1183 Authentication, SN=79, FN=13, Flags=o..PR.F.C[Malformed Packe...
16451	115.725544	fd:31:55:63:20:86	6a:8f:cd:88:f4:55	802.11	146 Authentication, SN=1054, FN=10, Flags=...P....C[Malformed Pac...

Figura 18: Processo de associação completo - redes IEEE 802.11.

Verifica-se que o processo possui as fases de autenticação e associação, ambas com um pedido e uma resposta:

1. Pedido de Autenticação - Frame 2486;
2. Resposta de Autenticação - Frame 2488;
3. Pedido de Associação - Frame 2490;
4. Resposta de Associação - Frame 2492.

Este processo contém também as tramas de *probing* anteriormente especificadas, que surgem inclusive representadas no diagrama abaixo[1].

Alínea 13

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

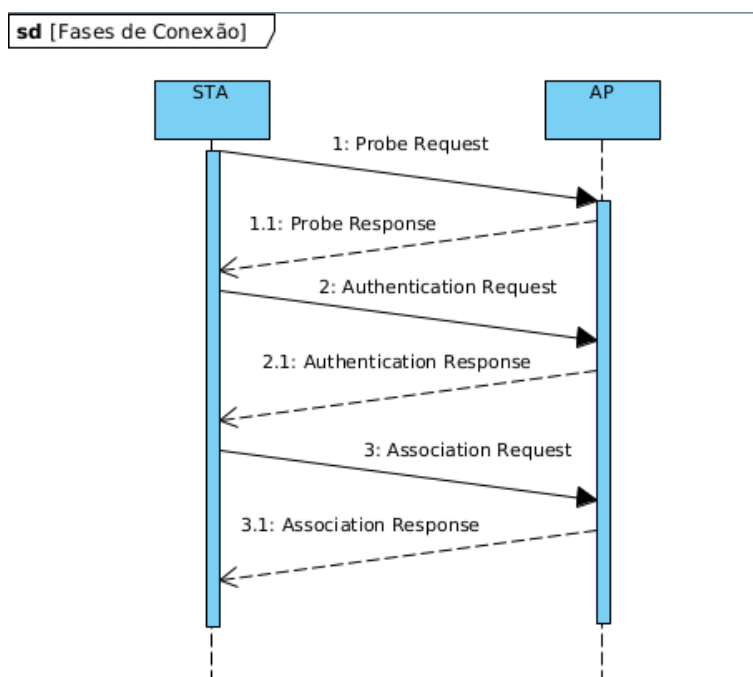


Figura 19: Processo de associação completo - diagrama - redes 802.11.

Ponto 7: Transferência de Dados

Alínea 14

Considere a trama de dados nº431. 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?

Analisando a *flag* referente ao *DS status* conseguimos concluir que como a trama é proveniente de *DS* então não é local à *WLAN*

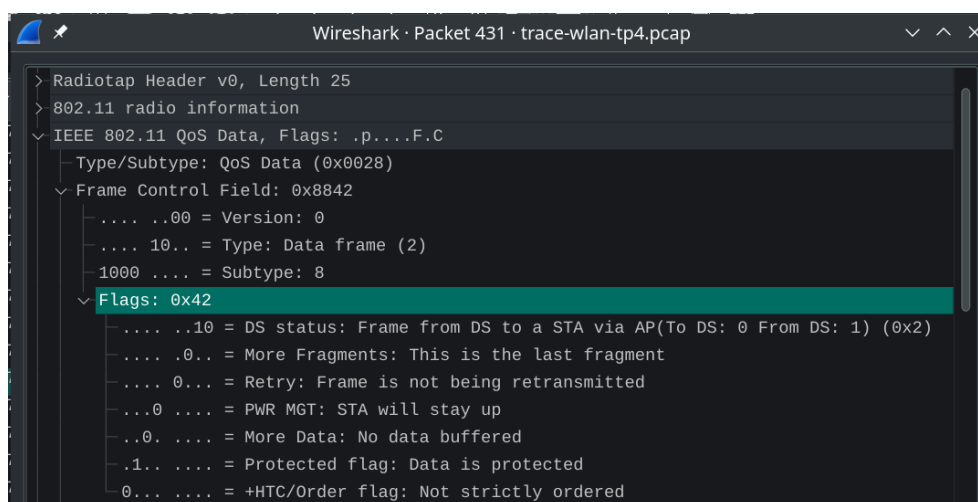


Figura 20: Trama de dados nº431

Alínea 15

Para a trama de dados nº431, transcreva os endereços MAC em uso, identificando qual o endereço MAC correspondente ao host sem fios (STA), ao AP e ao router de acesso ao sistema de distribuição?

De forma a descobrir a resposta à pergunta colocada, foi necessário analisar a seguinte secção da trama:

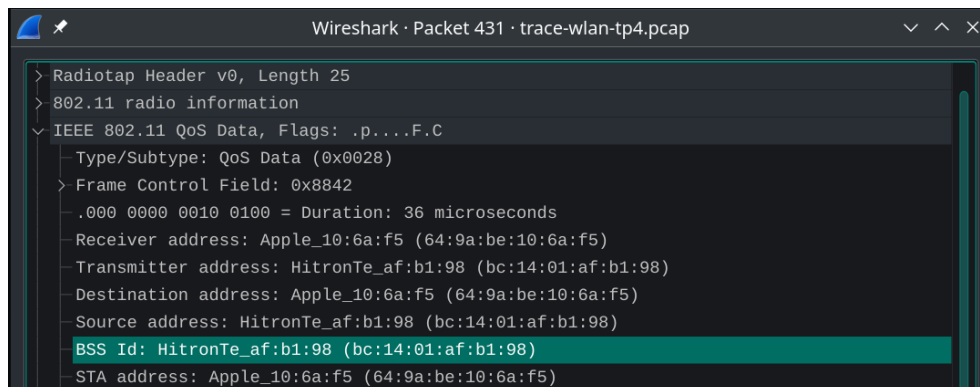


Figura 21: Endereços MAC relativos à trama n^o431

Concluimos assim que os endereços MAC correspondentes são:

1. STA : 64:9a:be:10:6a:f5
2. AP : bc:14:01:af:b1:98
3. Router : bc:14:01:af:b1:98

Alínea 16

| Como interpreta a trama n^o433 face à sua direccionalidade e endereçamento MAC?

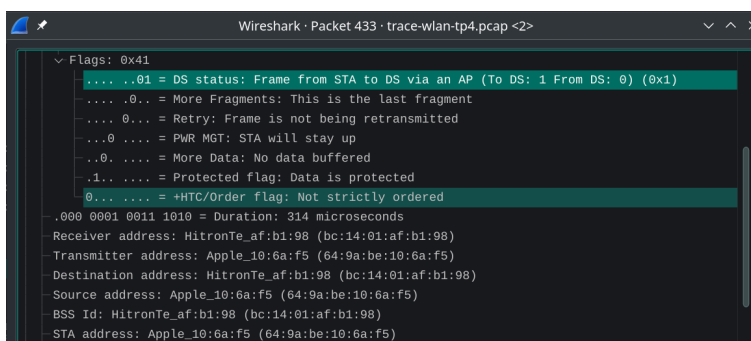


Figura 22: *Frame Control Field* da trama n^o433

Analisando a figura acima conseguimos concluir que esta trama parte do STA com destino ao DS, pois "To DS: 1" e "From DS: 0". Isto é comprovado também pelo endereçamento MAC, pois o *STA address* é igual ao *Source address* e o *BSS Id* é igual ao *Destination address*.

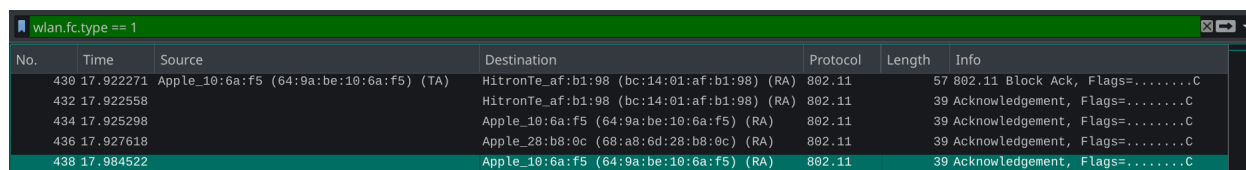
Alínea 17

Que subtipo de tramas de controlo são transmitidas ao longo da transferência de dados acima mencionada? Tente explicar porque razão têm 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
```

E obtivemos o seguinte resultado:



No.	Time	Source	Destination	Protocol	Length	Info
430	17.922271	Apple_10:6a:f5 (64:9a:be:10:6a:f5) (TA)	HitronTe_af:b1:98 (bc:14:01:af:b1:98) (RA)	802.11	57	802.11 Block Ack, Flags=.....C
432	17.922558		HitronTe_af:b1:98 (bc:14:01:af:b1:98) (RA)	802.11	39	Acknowledgement, Flags=.....C
434	17.925298	Apple_10:6a:f5 (64:9a:be:10:6a:f5) (RA)		802.11	39	Acknowledgement, Flags=.....C
436	17.927618	Apple_28:b8:0c (68:a8:6d:28:b8:0c) (RA)		802.11	39	Acknowledgement, Flags=.....C
438	17.984522	Apple_10:6a:f5 (64:9a:be:10:6a:f5) (RA)		802.11	39	Acknowledgement, Flags=.....C

Figura 23: Tramas de *Acknowledgment*

Sendo assim, o subtipo de tramas de controlo transmitidas é o *Acknowledgment*. Estas têm de existir pois a rede *wireless* é muito mais propensa a perdas do que a rede *Ethernet*, não tendo o nó de origem a certeza de que o nó de destino recebeu a informação corretamente.

Alínea 18

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.

Na imagem abaixo, na secção relativa à informação (coluna na extrema direita) verificamos que não foram usadas tramas *Request to Send* e *Clear To Send*.

427	17.922089	HitronTe_af:b1:98 (bc:14:01:af:b1:98) (TA)	Apple_10:6a:f5 (64:9a:be:10:6a:f5) (RA)	802.11	49 802.11 Block Ack Req, Flags=.....
428	17.922099	Apple_10:6a:f5 (64:9a:be:10:6a:f5) (TA)	HitronTe_af:b1:98 (bc:14:01:af:b1:98) (RA)	802.11	57 802.11 Block Ack, Flags=.....C
429	17.922190	HitronTe_af:b1:98 (bc:14:01:af:b1:98) (TA)	Apple_10:6a:f5 (64:9a:be:10:6a:f5) (RA)	802.11	49 802.11 Block Ack Req, Flags=.....
430	17.922271	Apple_10:6a:f5 (64:9a:be:10:6a:f5) (TA)	HitronTe_af:b1:98 (bc:14:01:af:b1:98) (RA)	802.11	57 802.11 Block Ack, Flags=.....C
431	17.922542	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	226 QoS Data, SN=830, FN=0, Flags=p...
432	17.922558	HitronTe_af:b1:98 (bc:14:01:af:b1:98) (RA)	802.11	39 Acknowledgement, Flags=.....C	
433	17.924985	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	178 QoS Data, SN=3680, FN=0, Flags=p...
434	17.925298	Apple_10:6a:f5 (64:9a:be:10:6a:f5) (RA)	802.11	39 Acknowledgement, Flags=.....C	
435	17.927587	Apple_28:b8:0c	HitronTe_af:b1:98	802.11	49 Null function (No data), SN=0, FN=0,
436	17.927618	Apple_28:b8:0c (68:a8:6d:28:b8:0c) (RA)	802.11	39 Acknowledgement, Flags=.....C	
437	17.984501	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	53 Null function (No data), SN=2499, FN=
438	17.984522	Apple_10:6a:f5 (64:9a:be:10:6a:f5) (RA)	802.11	39 Acknowledgement, Flags=.....C	
439	18.022592	HitronTe_af:b1:98	Broadcast	802.11	296 Beacon frame, SN=2435, FN=0, Flags=.
440	18.024220	HitronTe_af:b1:99	Broadcast	802.11	265 Beacon frame, SN=2436, FN=0, Flags=.

Figura 24: Informação das tramas 427 a 440

Voltando a analisar a figura 22 verificamos que os sistemas envolvidos são o *HitronTe* (destino) e *Apple* (origem). Na trama nº 431, a origem e o destino estão trocados, contudo os mesmos sistemas estão envolvidos.

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
```

Obtendo o seguinte output:

No.	Time	Source	Destination	Protocol	Length	Info
173	6.658172	Apple_10:6a:f5 (64:9a:be:10:6a:f5) (TA)	HitronTe_af:b1:98 (bc:14:01:af:b1:98) (RA)	802.11	45	Request-to-send, Flags=.....C
174	6.658178		Apple_10:6a:f5 (64:9a:be:10:6a:f5) (RA)	802.11	39	Clear-to-send, Flags=.....C
519	21.531991	Apple_10:6a:f5 (64:9a:be:10:6a:f5) (TA)	HitronTe_af:b1:98 (bc:14:01:af:b1:98) (RA)	802.11	45	Request-to-send, Flags=.....C
520	21.532004		Apple_10:6a:f5 (64:9a:be:10:6a:f5) (RA)	802.11	39	Clear-to-send, Flags=.....C
529	21.547047	Apple_10:6a:f5 (64:9a:be:10:6a:f5) (TA)	HitronTe_af:b1:98 (bc:14:01:af:b1:98) (RA)	802.11	45	Request-to-send, Flags=.....C

Figura 25: Filtro aplicado

Daqui selecionamos a transferência de dados iniciada na trama 519 e terminada na trama 528.

No.	Time	Source	Destination	Protocol	Length	Info
518	21.505709	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2504, FN=0, Flags=.
519	21.531991	Apple_10:6a:f5 (64:9a:be:10:6a:f5) (TA)	HitronTe_af:b1:98 (bc:14:01:af:b1:98) (RA)	802.11	45	Request-to-send, Flags=.....C
520	21.532004		Apple_10:6a:f5 (64:9a:be:10:6a:f5) (RA)	802.11	39	Clear-to-send, Flags=.....C
521	21.532010	2c:4a:44:cd:08:bb	6b:fb:df:6a:4d:78	LLC	146	I P, N(R)=84, N(S)=14; DSAP 0x70 Ind
522	21.532013	HitronTe_af:b1:98 (bc:14:01:af:b1:98) (TA)	Apple_10:6a:f5 (64:9a:be:10:6a:f5) (RA)	802.11	57	802.11 Block Ack, Flags=.....C
523	21.532097	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	53	Null function (No data), SN=2500, FN=
524	21.532171		Apple_10:6a:f5 (64:9a:be:10:6a:f5) (RA)	802.11	39	Acknowledgement, Flags=.....C
525	21.532275	HitronTe_af:b1:98 (bc:14:01:af:b1:98) (TA)	Apple_10:6a:f5 (64:9a:be:10:6a:f5) (RA)	802.11	49	802.11 Block Ack Req, Flags=.....C
526	21.532345	Apple_10:6a:f5 (64:9a:be:10:6a:f5) (TA)	HitronTe_af:b1:98 (bc:14:01:af:b1:98) (RA)	802.11	57	802.11 Block Ack, Flags=.....C
527	21.532554	HitronTe_af:b1:98 (bc:14:01:af:b1:98) (TA)	Apple_10:6a:f5 (64:9a:be:10:6a:f5) (RA)	802.11	49	802.11 Block Ack Req, Flags=.....C
528	21.532564	Apple_10:6a:f5 (64:9a:be:10:6a:f5) (TA)	HitronTe_af:b1:98 (bc:14:01:af:b1:98) (RA)	802.11	57	802.11 Block Ack, Flags=.....C
529	21.547047	Apple_10:6a:f5 (64:9a:be:10:6a:f5) (TA)	HitronTe_af:b1:98 (bc:14:01:af:b1:98) (RA)	802.11	45	Request-to-send, Flags=.....C

Figura 26: Transferência de dados com RTC/CTS

Outro exemplo de uma transferência de dados sem a opção RTC/CTS seria a seguinte:

457	18.539762	Apple_71:41:a1	Hitronfe_af:b1:98	802.11	178 QoS Data, SN=1209, FN=0, Flags=.p...
458	18.540043		Apple_71:41:a1 (d8:a2:5e:71:41:a1) (RA)	802.11	39 Acknowledgement, Flags=.....C

Figura 27: Transferência de dados sem RTC/CTS

2. Conclusão

O presente trabalho visa primordialmente explorar vários aspetos alusivos às redes sem fios (wifi). Neste sentido, aprofunda-se o protocolo IEEE 802.11 [2], particularmente, o formato das tramas, o endereçamento dos componentes deste tipo de comunicação, os tipos de tramas (controlo, gestão e dados) mais comuns e a operação do protocolo. O estudo em questão seguiu uma abordagem estruturada de acordo com as fases dos processos presentes numa comunicação sem fios, tendo também em conta os tipos de *scanning*.

Assim, as fases do mesmo foram:

1. Estudo do Acesso a Rádio, nomeadamente, a informação do nível físico presente neste tipo de tramas, a frequência da rede e o canal a esta associado e o débito da informação transmitida;
2. Estudo dos Tipos de *Scanning*. Em relação ao *Scanning* Passivo, analisa-se as tramas *beacon* da respetiva ordem e deteção de erros. Em relação ao *Scanning* Ativo, analisa-se os tipos das tramas *probing*;
3. Estudo do Processo de Associação, nomeadamente, as suas fases em detalhe, no estabelecimento de uma comunicação sem fios, com representação em diagrama temporal;
4. Estudo do Processo de Transferência de Dados, particularmente, direcionamento de tramas, endereçamento MAC e ferramentas de controlo de erros.

Através de cada um destes tópicos anteriores, é possível apresentar as nossas conclusões em relação a cada um:

(1) Foi perceptível a existência de informação do nível físico nas tramas utilizadas neste acesso a rádio;

(2) Compreenderam-se as várias diferenças entre os tipos de *Scanning* a nível de:

- Segurança: com *scanning* ativo, é necessária a existência de *firewalls*, fornecendo-se credenciais de servidor. Com *scanning* passivo, não há necessidade de abrir *firewalls*, fornecer credenciais ou mesmo estabelecer uma conexão à Internet;
- Deteção de Erros: a existência ou não, consoante a tipo;
- O grupo compreendeu que utilizar uma combinação entre os dois tipos de *scanning* seria mais promissor e que esta decisão dependeria do propósito em questão;
- Em cada tipo, utilizam-se diferentes tramas (*beacon* & *probing*);

(3) Percebemos que a troca de dados entre uma STA e um AP está dependente de um processo dividido em duas fases, uma de autenticação e outra de associação, ambas com um pedido ao qual se efetua uma resposta;

(4) Compreendemos a necessidade da existência de tramas de controlo numa rede *wireless* e como identificar os diferentes sistemas e as suas funções nas tramas.

Em relação às dificuldades encontradas, é de exaltar a alínea 3, onde foram apresentadas informações contraditórias no relatório apresentado pelo *Wireshark* e a alínea 9, na qual foi necessário alterar as próprias definições do *Wireshark* para visualizar um resultado mais fidedigno.

Concluindo, o grupo considera este trabalho bem conseguido, já que respondemos a todas as perguntas, aprofundando e consolidando conceitos teóricos lecionados.

Referências

- [1] “802.11 association process explained - cisco meraki.” [Online]. Available: https://documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/802.11_Association_Process_Explained
- [2] J. F. Kurose and K. W. Ross, *Computer networking : a top-down approach*.