

3. Primeiro Passo

Descarregue da plataforma de ensino a captura WLAN-traffic-20230502a.pcapng.zip e abra o ficheiro .pcapng no Wireshark.

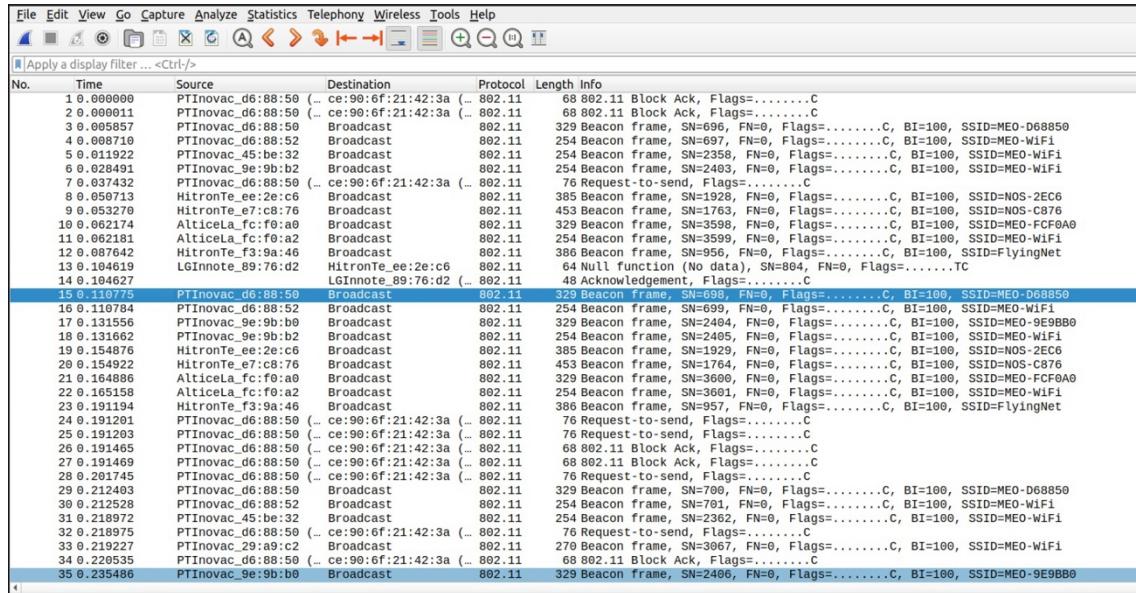


Figura 1 – Printscreen da wlam no wireshark

4. Acesso Rádio

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

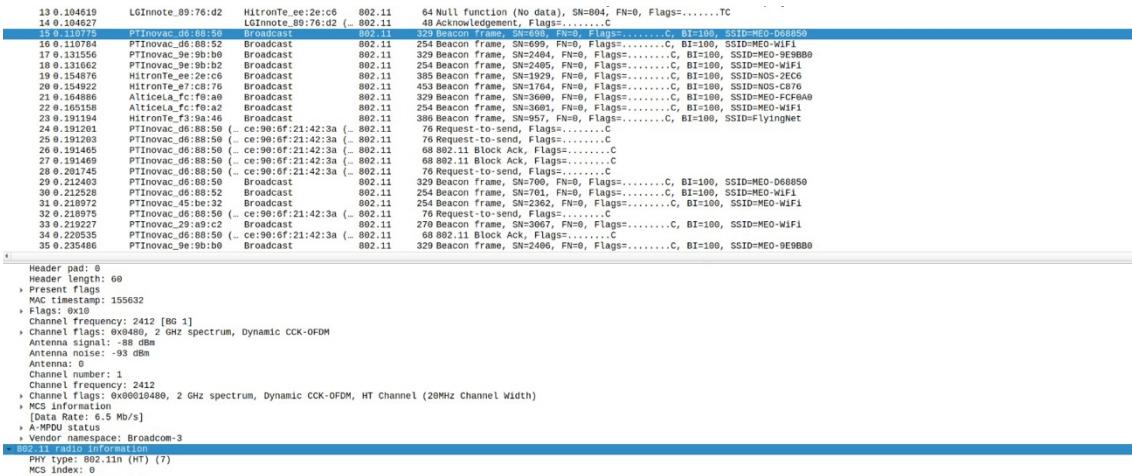


Figura 2 -Trama atribuída ao grupo (15)

A frequência do espetro é 2412 MHz, e o canal corresponde a esta frequência é o 1.

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

```
-----  
802.11 radio information  
PHY type: 802.11n (HT) (7)  
MCS Index: 0  
Bandwidth: 20 MHz (0)  
Short GI: False  
Greenfield: False  
FEC: BEC (0)  
Data rate: 6.5 Mb/s  
Channel: 1  
Frequency: 2412MHz  
Signal strength (dBm): -88 dBm  
Noise level (dBm): -93 dBm  
Signal/noise ratio (dB): 5 dB  
TSF timestamp: 155632  
.....1 = Last part of an A-MPDU: True  
.....0. = A-MPDU delimiter CRC error: False  
A-MPDU aggregate TD: 0
```

Figura 3 – Printscreen da norma IEEE 802.11 que está a ser usada

A versão da norma IEEE 802.11n utilizada é a que está sublinhada na imagem e é standard da geração Wi-Fi 4.

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.

```
FEC: BEC (0)  
Data rate: 6.5 Mb/s  
Channel: 1  
Frequency: 2412MHz  
Signal strength (dBm): -88 dBm  
Noise level (dBm): -93 dBm  
Signal/noise ratio (dB): 5 dB  
TSF timestamp: 155632  
.....1 = Last part of an A-MPDU: True
```

Figura 4 - Printscreen do débito a que foi enviado a trama escolhida.

O débito a que foi enviada a trama está na imagem (6.5 Mb/s). Como vimos na figura 3, a interface Wi-Fi está na geração 4 o que garante uma capacidade máxima de débito de 600 Mb/s logo, não foi atingida a capacidade máxima.

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.

Uma vez que a banda encontra-se suficientemente próxima de (-90 dBm) mais precisamente -88 dBm, podemos concluir que, a qualidade esperada é que as chances de conectividade são muito pequenas.

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 TurnoGrupo (PLXX), responda às seguintes questões:

- 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 subtipo da trama. Em que parte concreta do cabeçalho da trama estão especificados (ver anexo)?

```
IEEE 802.11 Beacon frame, Flags: ....C
  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
        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)
        BSS Id: PTInovac_d6:88:50 (00:06:91:d6:88:50)
        .... .... .000 = Fragment number: 0
        0010 1011 1010 .... = Sequence number: 698
        Frame check sequence: 0x1660adac [unverified]
        [FCS Status: Unverified]
  > IEEE 802.11 Wireless Management
```

Figura 5 – Printscreen do type e do subtype da trama 15

Como está presente na figura, o “type” e o “subtype” da trama 15 é 0 (“Management frame”) e 8 (“Beacon”), respectivamente.

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

```
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)
```

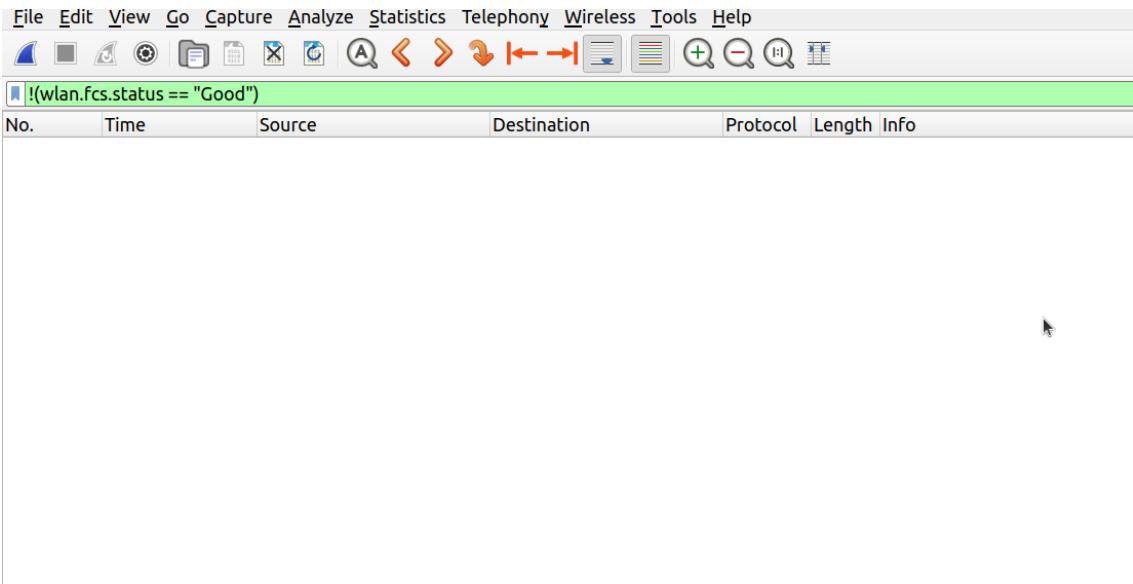
Figura 7 – Endereços Mac

Os endereços MAC em uso estão apresentados na imagem supramencionada. Uma vez que o endereço MAC de destino é de “Broadcast”, podemos concluir que a trama foi enviada para todos os diapositivos que são capazes de a receber.

- 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.

Primeiramente, alteramos as definições do “Wireshark” de modo a conseguir visualizar o campo “FCS Status”. De seguida, com o filtro “!(wlan.fcs.status == “Good”)” do “Wireshark” eliminamos todas as tramas sem erros.

Dado que, o “Wireshark” não está a sinalizar nada que indique que haja erros de CRC, podemos concluir que este não está a usar o método de deteção de erros. Desta forma, obtemos a seguinte imagem.



A deteção de erros em redes sem fios é utilizada de forma a detetar interferências ou obstrução nas tramas.

- 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.**

```

> Frame 15: 329 bytes on wire (2632 bits), 32
> Radiotap Header v0, Length 60
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: ....C
> IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
    Timestamp: 1721591296388
    Beacon Interval: 0.102400 [Seconds]
    > Capabilities Information: 0x1411
  > Tagged parameters (229 bytes)
    > Tag: SSID parameter set: MEO-D68850
    > Tag: Supported Rates 1(B), 2(B), 5.5(B),
      Tag Number: Supported Rates (1)
      Tag length: 8
      Supported Rates: 1(B) (0x82)
      Supported Rates: 2(B) (0x84)
      Supported Rates: 5.5(B) (0x8b)
      Supported Rates: 11(B) (0x96)
      Supported Rates: 18 (0x24)
      Supported Rates: 24 (0x30)
      Supported Rates: 36 (0x48)
      Supported Rates: 54 (0x6c)
    > 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]
      Tag Number: Extended Supported Rates (50)
      Tag length: 4
      Extended Supported Rates: 6 (0x0c)
      Extended Supported Rates: 9 (0x12)
      Extended Supported Rates: 12 (0x18)
      Extended Supported Rates: 48 (0x60)
    > Tag: RSN Information
  
```

Os débitos suportados pela trama são os que estão descritos na figura em cima.

```

> Frame 15: 329 bytes on wire (2632 bits), 329 bytes captured (2632 bits)
> Radiotap Header v0, Length 60
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: ....C
> IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
    Timestamp: 1721591296388
    Beacon Interval: 0.102400 [Seconds]
    > Capabilities Information: 0x1411
  > 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
    > 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]
      Tag Number: Extended Supported Rates (50)
      Tag length: 4
      Extended Supported Rates: 6 (0x0c)
      Extended Supported Rates: 9 (0x12)
      Extended Supported Rates: 12 (0x18)
      Extended Supported Rates: 48 (0x60)
    > Tag: RSN Information
  
```

Os débitos adicionais estão descritos na figura em cima.

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.

```
> Frame 15: 329 bytes on wire (2632 bits), 329 bytes c
> Radiotap Header v0, Length 60
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: .......C
-> IEEE 802.11 Wireless Management
  -> Fixed parameters (12 bytes)
    Timestamp: 1721591296388
    Beacon Interval: 0.102400 [Seconds]
    -> Capabilities Information: 0x1411
  -> Transmitter parameters (229 bytes)
```

O valor previsto para o intervalo de tempo entre tramas beacon consecutivas está presente na imagem (0.102400 segundos) e, uma vez que é uma aproximação, a sua precisão é reduzida dado a imprevistos como, por exemplo, o AP não estar disponível no momento em que deve ser enviada a trama.

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 encontrar SSIDs dos APs que estão a operar na vizinhança, no “Wireshark”, fomos retirando através de um filtro composto todos os “SSIDs” que íamos eliminando. Desta forma, geramos o seguinte filtro:

```
(((((((((((!(wlan.ssid == "MEO-FCF0A0")) && !(wlan.ssid == "NOS-2EC6")) &&
!(wlan.ssid == "MEO-9E9BB0")) && !(wlan.ssid == "NOS-C876")) && !(wlan.ssid ==
"MEO-D68850")) && !(wlan.ssid == "FlyingNet")) ) && !(wlan.ssid == "MEO-WiFi") &&
wlan.ssid ) && !(wlan.ssid == "Masmorra do Sexo")) && !(wlan.ssid == "MEO-9BF2A0"))
&& !(wlan.ssid == "MEO-45BE30")) && !(wlan.ssid == "GV BRAGA")) && !(wlan.ssid ==
"TP-LINK_AP_AF08")) && !(wlan.ssid == "Vodafone-48683C")) && !(wlan.ssid == "K6000
```

```
Plus")) && !(wlan.ssid == "Vodafone-DC61F7")) && !(wlan.ssid == "MEO-D9EDE0")) &&
!(wlan.ssid == "GRUPO GV")) && !(wlan.ssid == "IA 2 5")
```

Conseguimos averiguar que os Aps que operam na vizinhança são os que aparecem no filtro, pois no “Wireshark” apenas surgem tramas com o “SSID” igual a “Wildcard (Broadcast)”.

No.	Time	Source	Destination	Protocol	Length	Info
8964	75.292290	Tp-LinkT_ce:58:d2	Broadcast	802.11	82	Probe Request, SN=110, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
8965	75.292304	Tp-LinkT_ce:58:d2	Broadcast	802.11	82	Probe Request, SN=111, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
788	7.826332	AltoBeam_08:32:99	Broadcast	802.11	110	Probe Request, SN=1111, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
793	7.838631	AltoBeam_08:32:99	Broadcast	802.11	110	Probe Request, SN=1112, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
155	1.399123	Samsung_E_1a:10:f6	Broadcast	802.11	122	Probe Request, SN=1124, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
9046	75.749213	b6:2f:79:e2:28:36	Broadcast	802.11	156	Probe Request, SN=1208, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
2247	20.876163	Google_c6:fe:31	Broadcast	802.11	85	Probe Request, SN=139, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
7519	65.968023	ec:a1:38:96:76:7b	Broadcast	802.11	94	Probe Request, SN=146, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
7520	65.968030	ec:a1:38:96:76:7b	Broadcast	802.11	94	Probe Request, SN=147, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
1339	12.958765	ARRISGro_a6:bc:a9	Broadcast	802.11	134	Probe Request, SN=1576, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
5436	45.886096	ARRISGro_a6:bc:a9	Broadcast	802.11	134	Probe Request, SN=1612, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
5437	45.927921	ARRISGro_a6:bc:a9	Broadcast	802.11	134	Probe Request, SN=1613, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
5456	46.006604	ARRISGro_a6:bc:a9	Broadcast	802.11	134	Probe Request, SN=1615, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
9470	78.863673	ARRISGro_a6:bc:a9	Broadcast	802.11	134	Probe Request, SN=1649, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
9488	78.961428	ARRISGro_a6:bc:a9	Broadcast	802.11	134	Probe Request, SN=1659, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
9344	78.016116	0e:5f:4a:19:fa:c6	Broadcast	802.11	123	Probe Request, SN=169, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
9356	78.025463	0e:5f:4a:19:fa:c6	Broadcast	802.11	123	Probe Request, SN=170, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
7174	62.915126	Google_aa:21:98	Broadcast	802.11	85	Probe Request, SN=2042, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
10298	85.969694	a6:f0:9e:5b:1e:71	Broadcast	802.11	156	Probe Request, SN=2366, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
10636	88.936022	HuaweiTE_53:bc:16	Broadcast	802.11	144	Probe Request, SN=255, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
2481	22.187383	42:e6:25:0a:97:7e	Broadcast	802.11	94	Probe Request, SN=2718, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
2402	22.187389	42:e6:25:0a:97:7e	Broadcast	802.11	94	Probe Request, SN=2719, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
2735	25.178835	Tp-LinkT_ce:58:d2	Broadcast	802.11	82	Probe Request, SN=36, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
2736	25.178843	Tp-LinkT_ce:58:d2	Broadcast	802.11	82	Probe Request, SN=37, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)

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

Com uma breve pesquisa no “Google”, procuramos encontrar filtros que nos permitiam visualizar as tramas probing request e probing response. Assim, reparamos que é possível procurar tramas pelo seu subtipo. Com isto, vimos que os subtipos de probing request e probing response são respetivamente 4 e 5. Desta forma, chegamos à seguinte figura:

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
wlan.fc.type_subtype == 4 wlan.fc.type_subtype == 5						
No.	Time	Source	Destination	Protocol	Length	Info
150	1.381604	HitronTe_f3:9a:46	Samsung_E_1a:10:f6	802.11	486	Probe Response, SN=1936, FN=0, Flags=.....R..C, BI=100, SSID=FlyingNet
151	1.382387	HitronTe_f3:9a:46	Samsung_E_1a:10:f6	802.11	486	Probe Response, SN=1936, FN=0, Flags=.....R..C, BI=100, SSID=FlyingNet
152	1.391750	HitronTe_f3:9a:46	Samsung_E_1a:10:f6	802.11	486	Probe Response, SN=1936, FN=0, Flags=.....R..C, BI=100, SSID=NOS-2EC6
153	1.391879	HitronTe_ee:2e:c6	Samsung_E_1a:10:f6	802.11	485	Probe Response, SN=2192, FN=0, Flags=.....R..C, BI=100, SSID=NOS-2EC6
155	1.399123	Samsung_E_1a:10:f6	Broadcast	802.11	122	Probe Request, SN=1124, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
277	2.710713	HitronTe_ee:2e:c6	AltoBeam_08:32:99	802.11	485	Probe Response, SN=2193, FN=0, Flags=.....R..C, BI=100, SSID=NOS-2EC6
279	2.729237	HitronTe_ee:2e:c6	AltoBeam_08:32:99	802.11	485	Probe Response, SN=2193, FN=0, Flags=.....R..C, BI=100, SSID=NOS-2EC6
334	2.297107	ed:92:4d:99:20:b2	ed:92:4d:99:20:b2	802.11	224	Probe Response, SN=224, FN=0, Flags=.....R..C, BI=100, SSID=MEO-WiFi
335	3.712777	PTInovac_45:bc:32	ed:92:4d:99:20:b2	802.11	224	Probe Response, SN=224, FN=0, Flags=.....R..C, BI=100, SSID=MEO-WiFi
336	3.390915	PTInovac_45:bc:32	ed:92:4d:99:20:b2	802.11	224	Probe Response, SN=224, FN=0, Flags=.....R..C, BI=100, SSID=MEO-WiFi
788	7.826332	AltoBeam_08:32:99	Broadcast	802.11	118	Probe Request, SN=1111, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
789	7.832355	HitronTe_ee:2e:c6	AltoBeam_08:32:99	802.11	485	Probe Response, SN=2195, FN=0, Flags=.....R..C, BI=100, SSID=NOS-2EC6
791	7.835604	HitronTe_ee:2e:c6	AltoBeam_08:32:99	802.11	485	Probe Response, SN=2195, FN=0, Flags=.....R..C, BI=100, SSID=NOS-2EC6
793	7.838631	AltoBeam_08:32:99	Broadcast	802.11	118	Probe Request, SN=1112, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
796	7.859430	HitronTe_ee:2e:c6	AltoBeam_08:32:99	802.11	485	Probe Response, SN=2196, FN=0, Flags=.....R..C, BI=100, SSID=NOS-2EC6
797	7.862565	HitronTe_ee:2e:c6	AltoBeam_08:32:99	802.11	485	Probe Response, SN=2196, FN=0, Flags=.....R..C, BI=100, SSID=NOS-2EC6
798	7.868818	HitronTe_ee:2e:c6	AltoBeam_08:32:99	802.11	485	Probe Response, SN=2196, FN=0, Flags=.....R..C, BI=100, SSID=NOS-2EC6

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?

No.	Time	Source	Destination	Protocol	Length	Info
791	7.835604	HitronTe_ee:2e:c6	AltoBeam_08:32:99	802.11	485	Probe Response, SN=2195, FN=0, Flags=.....R..C, BI=100, SSID=NOS-2EC6
793	7.838631	AltoBeam_08:32:99	Broadcast	802.11	118	Probe Request, SN=1112, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
796	7.859430	HitronTe_ee:2e:c6	AltoBeam_08:32:99	802.11	485	Probe Response, SN=2196, FN=0, Flags=.....R..C, BI=100, SSID=NOS-2EC6

Na figura mencionada em cima, podemos observar um “probing request” e um “probing response”. O “probing request” foi criado pela estação AltoBeam e foi enviado em “broadcast”, com o intuito de identificar as redes próximas. De seguida, observamos o “probing response” de uma estação que recebeu o “probing request” inicial e que envia as informações relativas à sua rede. Sumariamente, o “probing request” serve para identificar redes próximas, dai ser enviado em “Broadcast”, enquanto que, o “probing

“response”, é uma resposta ao pedido anterior, de forma a confirmar que existe pelo menos uma rede nas proximidades.

6. 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:

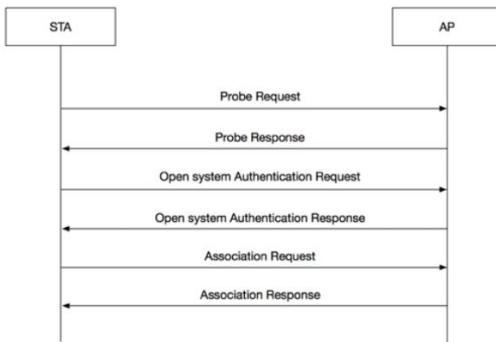
- 13) Identifique uma sequência de tramas que corresponda a um processo de associação realizado com sucesso entre a STA e o AP, incluindo a fase de autenticação.**

Com recurso ao filtro “wlan.fc.type_subtype == 0x0000 || wlan.fc.type_subtype == 0x0001”, encontramos as tramas de “association request” e de “association response”. De seguida, retiramos o filtro e observamos a sequência completa como descrito na seguinte figura.

8472 73.456738	AzureWay_0f:0e:9b	HitronTe_f3:9a:46	862.11	70 Authentication, SN=262, FN=0, Flags=.....C
8473 73.456745		AzureWay_0f:0e:9b (..	862.11	48 Acknowledgement, Flags=.....C
8474 73.456775	HitronTe_f3:9a:46	AzureWay_0f:0e:9b	862.11	70 Authentication, SN=1965, FN=0, Flags=.....C
8475 73.456780		HitronTe_f3:9a:46 (..	862.11	48 Acknowledgement, Flags=.....C
8476 73.459546	AzureWay_0f:0e:9b	HitronTe_f3:9a:46	862.11	164 Association Request, SN=263, FN=0, Flags=.....C, SSID=FlyingNet
8477 73.459553		AzureWay_0f:0e:9b (..	862.11	48 Acknowledgement, Flags=.....C
8478 73.459638	HitronTe_f3:9a:46	AzureWay_0f:0e:9b	862.11	210 Association Response, SN=1966, FN=0, Flags=.....C
8479 73.459643		HitronTe_f3:9a:46 (..	862.11	48 Acknowledgement, Flags=.....C

Nesta imagem, visualizamos a “Authentication Request ” e “Authentication Response”, como também a “Probe Request” e a “Probe Response”

- 14) Efetue um diagrama que ilustre a sequência de todas as tramas trocadas no processo.**



7. Transferência de Dados

O trace disponibilizado, para além de tramas de gestão da ligação de dados, inclui tramas de dados e tramas de controlo da transferência desses mesmos dados.

- 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?**

```

8503 73.511585 Azurewav_0f:0e:9b IPv4Broadcast_16 802.11 186 QoS Data, SN=0, 
8504 73.511588 HitronTe_f3:9a:46 (... Azurewav_0f:0e:9b (... 802.11 68 802.11 Block ACK
8505 73.530748 PTInovac_d6:88:58 Broadcast 802.11 329 Beacon frame, SN
8506 73.530757 Azurewav_0f:0e:9b Broadcast 802.11 448 QoS Data, SN=1,
8507 73.530760 HitronTe_f3:9a:46 (... Azurewav_0f:0e:9b (... 802.11 68 802.11 Block ACK
8508 73.531678 PTInovac_d6:88:52 Broadcast 802.11 254 Beacon frame, SN
8509 73.534969 PTInovac_45:be:32 Broadcast 802.11 254 Beacon frame, SN

Frame 8503: 188 bytes on wire (1564 bits), 188 bytes captured (1564 bits) on interface en0, i
> Radiotap Header v0, Length 58
> 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 more buffered
    .1.... = Protected flag: Data is protected
    0.... .... = +HTC/Order flag: Not strictly ordered
    .000 0000 0011 0000 = Duration: 48 microseconds
  
```

Como podemos observar pela figura em cima, a trama tem a seguinte direção: (To DS: 1 From DS: 0), o que significa que o pacote está a ser enviado de um STA para o DS. Logo, podemos inferir que é local à “wlan”.

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)?

```

Frame 8503: 188 bytes on wire (1504 bits), 188 bytes captured (1504 bits)
RadioType Header v0, Length 58
802.11 radio information
IEEE 802.11 QoS Data, Flags: .p.....TC
  Type/Subtype: QoS Data (0x0028)
  Frame Control Field: 0x8841
  .000 0000 0011 0000 = Duration: 48 microseconds
  Receiver address: HironTe_f3:9a:46 (74:9b:e8:f3:9a:46)
  Transmitter address: AzureWav_0f:0e:9b (80:c5:f2:f0:0e:9b)
  Destination address: IPv6mcast_16 (33:33:00:00:00:16)
  Source address: Azurewav_0f:0e:9b (80:c5:f2:f0:0e:9b)
  BSS Id: HironTe_f3:9a:46 (74:9b:e8:f3:9a:46)

```

Como observamos na imagem, o “destination” é o DS, o “receiver” é o AP e o “transmitter” é o STA. Deste modo, os endereços Mac são os seguintes:

STA: 80:c5:f2:0f:0e:9b

DS: 33:33:00:00:00:16

AP: 74:9b:e8:f3:9a:46

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

Tendo em conta a alínea 15) relativamente ao direcionamento tomado, através desta imagem em cima, inferimos que a direção é contrária, ou seja, vem de um DS para um STA.

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.)

8512 73.542839	AzureWave_0f:0e:9b	HitronTe_f3:9a:46	802.11	73 Action, SN=612, FN=0, Flags=.....C, Dialog Token:
8513 73.542845	AzureWave_0f:0e:9b	(... HitronTe_f3:9a:46	802.11	48 Acknowledgment, Flags=.....C
8514 73.544132	HitronTe_f3:9a:46	AzureWave_0f:0e:9b	802.11	73 Action, SN=2, FN=0, Flags=.....C, Dialog Token=:
8515 73.544136	AzureWave_0f:0e:9b	HitronTe_f3:9a:46	802.11	48 Acknowledgment, Flags=.....C
8516 73.544143	HitronTe_f3:9a:46	AzureWave_0f:0e:9b	802.11	73 Action, SN=613, FN=0, Flags=.....C, Dialog Token:
8517 73.544147	AzureWave_0f:0e:9b	HitronTe_f3:9a:46	802.11	73 Action, SN=613, FN=0, Flags=.....R..C, Dialog Token:
8518 73.544151	HitronTe_f3:9a:46	AzureWave_0f:0e:9b	802.11	48 Acknowledgment, Flags=.....C
8519 73.544155	AzureWave_0f:0e:9b	(... HitronTe_f3:9a:46	802.11	76 Request-to-send, Flags=.....C
8520 73.544159	HitronTe_f3:9a:46	AzureWave_0f:0e:9b	802.11	72 Clear-to-send, Flags=.....C
8521 73.544163	76:9b:e8:f3:9a:43	AzureWave_0f:0e:9b	802.11	444 QoS Data, SN=2, FN=0, Flags=....P....F.C
8522 73.544167	AzureWave_0f:0e:9b	(... HitronTe_f3:9a:46	802.11	68 802.11 Block Ack, Flags=.....C
8523 73.544170	HitronTe_f3:9a:46	(... AzureWave_0f:0e:9b	802.11	76 Request-to-send, Flags=.....C

O subtipo das tramas de controlo que é transmitido ao longo da transferência de dados é o acknowledge (ACK). Esse tipo de trama é importante uma vez que, tem como propósito afirmar as transmissões que foram realizadas com sucesso. Este, é enviado às estações que por sua vez que interpretam como um sinal confirmação da receção da trama.

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.

Relativamente ao primeiro exemplo, com base na seguinte figura, afirmamos que a opção RTC/CTS não foi utilizada por causa da direção das tramas (DS status: Not leaving..).

```
+ Frame 8611: 48 bytes on wire (384 bits), 48 bytes captured (384 bits) on interface 8
- Radiotap Header V0, Length 34
  Header revision: 0
  Header pad: 0
  Header timestamp: 34
  > Present Flags
    MAC timestamp: 73591757
  IEEE 802.11 Radio Information
    Data Rate: 1.0 Mb/s
    Channel frequency: 2412 [B6 1]
    Channel flags: 0x0480, 2 GHz Spectrum, Dynamic CCK-OFDM
    Antenna noise: -93 dBm
    Antenna gain: 0
    > Available Address Space: Broadcom-3
    IEEE 802.11 radio information
  IEEE 802.11 Acknowledgment, Flags: ....C
  Type/Subtype: Acknowledgment (0x001d)
  + Frame 8610: 48 bytes on wire (384 bits), 48 bytes captured (384 bits) on interface 8
    ... .00 = Version: 0
    ... .01.. = Type: Control frame (1)
    ... .01.. = Subtype: 13
    - Flags: 0x00
      ... ..00 = DS status: Not leaving DS or network is operating in AD-HOC mode
      ... .0.. = More Fragments: This is the last fragment
      ... .0.. = More Fragment: Frame is being retransmitted
      ... .0.. = PWR MGT: STA will stay up
      ... .0.. = More Data: No data buffered
      ... .0.. = More Data: No data buffered
      ... .0.. = HT/C/Order flag: Not strictly ordered
      ... .0.. = Duration: 0 microseconds
    Received address: HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)
    Frame check sequence: 00343d3cf8 [unverified]
    [FCS Status: Unverified]
```

Um exemplo onde a transferência de dados usando a opção RTC/CTS foi realizada, segue-se na figura em baixo.

8512	73.542839	AzureWav_0f:0e:9b	HitronTe_f3:9a:46	802.11	73 Action, SN=612, FN=0, Flags=.L....C, Dialog Token
8513	73.542845	AzureWav_0f:0e:9b	(..	802.11	48 Acknowledgement, Flags=.....C
8514	73.544132	HitronTe_f3:9a:46	AzureWav_0f:0e:9b	(..	73 Action, SN=2, FN=0, Flags=.....C, Dialog Token=;
8515	73.544136	HitronTe_f3:9a:46	AzureWav_0f:0e:9b	(..	48 Acknowledgement, Flags=.....C
8516	73.544143	AzureWav_0f:0e:9b	HitronTe_f3:9a:46	(..	73 Action, SN=613, FN=0, Flags=.....C, Dialog Token
8517	73.544147	AzureWav_0f:0e:9b	HitronTe_f3:9a:46	(..	73 Action, SN=613, FN=0, Flags=...R...C, Dialog Token
8518	73.544151	AzureWav_0f:0e:9b	AzureWav_0f:0e:9b	(..	48 Acknowledgement, Flags=.....C
8519	73.544155	HitronTe_f3:9a:46	AzureWav_0f:0e:9b	(..	76 Request-to-send, Flags=.....C
8520	73.544159	HitronTe_f3:9a:46	AzureWav_0f:0e:9b	(..	72 Clear-to-send, Flags=.....C
8521	73.544162	76:9b:89:f3:0b:43	AzureWav_0f:0e:9b	802.11	44 QoS Data, SN=3, FN=0, Flags=p...F.C
8522	73.544167	AzureWav_0f:0e:9b	(.. HitronTe_f3:9a:46	(.. 802.11	68 802.11 Block Ack, Flags=.....C
8523	73.544170	HitronTe_f3:9a:46	(.. AzureWav_0f:0e:9b	(.. 802.11	76 Request-to-send, Flags=.....C