

UNIVERSIDADE DO MINHO

LICENCIATURA EM ENGENHARIA INFORMÁTICA

Redes de Computadores

Grupo 52

TP4 : Redes sem Fios (Wi-Fi)

António Luís Braga Mendes (A84675)

Maria Eugénia Bessa Cunha (A93264)

Vicente Gonçalves Moreira (A93296)

Maio 2022

Questões e Respostas

4 Acesso Rádio

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

A rede está a operar a uma frequência de **2467Mhz** (MegaHertz). Esta frequência corresponde ao **canal 12**.

Figura 1: Frequência Trama 802.11

```
▶ Frame 56: 296 bytes on wire (2368 bits), 296 bytes captured
▶ Radiotap Header v0, Length 25
▼ 802.11 radio information
  PHY type: 802.11g (ERP) (6)
  Short preamble: False
  Proprietary mode: None (0)
  Data rate: 1,0 Mb/s
  Channel: 12
  Frequency: 2467MHz
  Signal strength (dBm): -60dBm
  Noise level (dBm): -88dBm
  Signal/noise ratio (dB): 28dB
  TSF timestamp: 21848118
  ▶ [Duration: 2360µs]
▶ IEEE 802.11 Beacon frame, Flags: .....C
▶ IEEE 802.11 Wireless Management
```

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

A versão utilizada na norma IEEE 802.11 é a versão **802.11g (ERP)**

Figura 2: Versão Trama 802.11

```
▶ Frame 56: 296 bytes on wire (2368 bits), 296 bytes captured
▶ Radiotap Header v0, Length 25
▼ 802.11 radio information
  PHY type: 802.11g (ERP) (6)
  Short preamble: False
  Proprietary mode: None (0)
  Data rate: 1,0 Mb/s
  Channel: 12
  Frequency: 2467MHz
  Signal strength (dBm): -60dBm
  Noise level (dBm): -88dBm
  Signal/noise ratio (dB): 28dB
  TSF timestamp: 21848118
  ▶ [Duration: 2360µs]
▶ IEEE 802.11 Beacon frame, Flags: .....C
▶ IEEE 802.11 Wireless Management
```

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.

Para a trama escolhida, o débito desta corresponde a 1Mb/s (1 Megabyte por Segundo). Segundo a norma IEEE, a versão 802.11g é capaz de operar a um débito máximo de 54Mbps (6.75 Mb/s), no entanto este débito não é alcançado devido não só à "falta de necessidade" deste débito para tramas curtas, como também uma forma de gerir a capacidade da rede entre outros *hosts*, permitindo que o débito máximo desta seja partilhado entre vários dispositivos.

Figura 3: Débito Trama 802.11

```
▶ Frame 56: 296 bytes on wire (2368 bits), 296 bytes captured
▶ Radiotap Header v0, Length 25
▼ 802.11 radio information
  PHY type: 802.11g (ERP) (6)
  Short preamble: False
  Proprietary mode: None (0)
  Data rate: 1,0 Mb/s
  Channel: 12
  Frequency: 2467MHz
  Signal strength (dBm): -60dBm
  Noise level (dBm): -88dBm
  Signal/noise ratio (dB): 28dB
  TSF timestamp: 21848118
  ▶ [Duration: 2360µs]
▶ IEEE 802.11 Beacon frame, Flags: .....C
▶ IEEE 802.11 Wireless Management
```

5 Scanning Passivo e Scanning Ativo

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

A trama selecionada pertence ao tipo de tramas 802.11g (ERP). Os seus valores identificadores do tipo e subtipo da trama escolhida são respetivamente **0** e **8**. Estes valores podem ser encontrados na secção "Frame Control" das tramas 802.11, estando esta secção localizada nos primeiros 2 *bytes* da trama enviada. Mais especificamente, o seu tipo pode ser encontrado no 3º e 4º bit da trama, e o seu subtipo entre os *bits* 5 e 8. (Ordem de leitura da trama)

Figura 4: Tipo/Sub-Tipo Trama 802.11

```
▶ Frame 312: 296 bytes on wire (2368 bits), 296 bytes captured (2368 bits)
▶ Radiotap Header v0, Length 25
▼ 802.11 radio information
  PHY type: 802.11g (ERP) (6)
  Short preamble: False
  Proprietary mode: None (0)
  Data rate: 1,0 Mb/s
  Channel: 12
  Frequency: 2467MHz
  Signal strength (dBm): -64dBm
  Noise level (dBm): -87dBm
  Signal/noise ratio (dB): 23dB
  TSF timestamp: 32190374
  ▶ [Duration: 2360µs]
▼ 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: 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 0101 .... = Sequence number: 2325
  Frame check sequence: 0x42c4951c [correct]
  [FCS Status: Good]
▶ IEEE 802.11 Wireless Management
```

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

Observando os campos *Source address* e *Transmitter address* concluímos que o endereço MAC do dispositivo de origem é **bc:14:01:af:b1:98**. Já nos campos *Receiver address* e *Destination address* podemos observar o endereço MAC do dispositivo de destino. Neste exemplo o endereço de destino é **ff:ff:ff:ff:ff:ff**, indicando que esta trama se trata de uma trama de *Broadcast*.

Figura 5: Endereços MAC

```
▶ Frame 312: 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
  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: 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 0101 .... = Sequence number: 2325
    Frame check sequence: 0x42c4951c [unverified]
    [FCS Status: Unverified]
▶ IEEE 802.11 Wireless Management
```

5.6 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?

Analisando a informação contida na trama beacon, em específico, dentro dos *Tagged parameters*, podemos encontrar uma lista de débitos suportados, assim como uma lista de débitos extras. Estes são os seguintes:

- ***Supported Rates:*** (Mbps)

- 1
- 2
- 5.5
- 11
- 9
- 18
- 36
- 54

- ***Extended Rates:*** (Mbps)

- 6
- 12
- 24
- 48

Figura 6: Débitos Suportados

```
▶ Frame 312: 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
  ▶ Fixed parameters (12 bytes)
  ▼ Tagged parameters (231 bytes)
    ▶ Tag: SSID parameter set: FlyingNet
    ▼ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 9, 18, 36, 54, [Mbit/sec]
      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: 9 (0x12)
      Supported Rates: 18 (0x24)
      Supported Rates: 36 (0x48)
      Supported Rates: 54 (0x6c)
    ▶ Tag: DS Parameter set: Current Channel: 12
    ▼ Tag: Extended Supported Rates 6(B), 12(B), 24(B), 48, [Mbit/sec]
      Tag Number: Extended Supported Rates (50)
      Tag length: 4
      Extended Supported Rates: 6(B) (0x8c)
      Extended Supported Rates: 12(B) (0x98)
      Extended Supported Rates: 24(B) (0xb0)
      Extended Supported Rates: 48 (0x60)
    ▶ Tag: Vendor Specific: Microsoft Corp.: WPS
```

5.7 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.

Analisando o campo *Beacon Interval* presente na informação da trama *Beacon*, podemos concluir que o intervalo desta foi definido com um intervalo de 0.102 segundos. Este periodo, apesar de definido, apenas se verifica com algum nível de precisão, havendo pequenos atrasos ou adiantamentos. Isto ocorre devido aos tempos de transmissão que podem variar, assim como o nível de "ocupação" do AP, ou seja, este pode estar a transmitir outras tramas a vários *hosts*, falhando assim o intervalo definido.

Figura 7: Intervalo tramas Beacon

```

▶ Frame 312: 296 bytes on wire (2368 bits), 296 bytes captured
▶ Radiotap Header v0, Length 25
▶ 802.11 radio information
▶ IEEE 802.11 Beacon frame, Flags: .....C
▼ IEEE 802.11 Wireless Management
  ▼ Fixed parameters (12 bytes)
    Timestamp: 1149682995688
    Beacon Interval: 0,102400 [Seconds]
    ▶ Capabilities Information: 0x0c31
  ▶ Tagged parameters (231 bytes)

```

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

Para este exercício, utilizamos um filtro de forma a listar todas as tramas *Beacon* capturadas, visto que são estas as tramas utilizadas para "anunciar" as várias redes WiFi presentes. Como visto pelos exercícios anteriores, sabemos que o subtipo destas tem o valor de 8 logo, utilizamos o seguinte filtro:

wlan.fc.type_subtype == 0x08

Depois de obtida a lista de capturas filtradas, analisamos esta e concluímos que apenas existem dois SSID's presentes na vizinhança da STA de captura. **FlyingNet** e **NOS_WIFI_Fon**

Figura 8: Lista SSID's

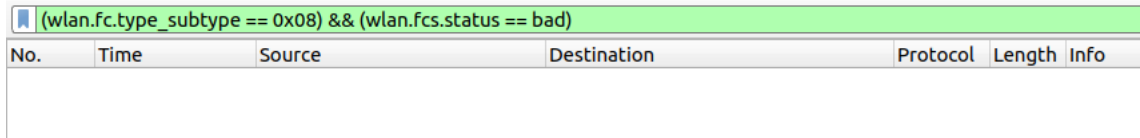
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2083, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2	0.001662	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2084, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
3	0.102552	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2085, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
4	0.104164	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2086, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
5	0.204951	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2087, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
6	0.206582	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2088, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
7	0.307368	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2089, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
8	0.308999	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2090, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
9	0.409749	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2091, FN=0, Flags=.....C, BI=100, SSID=FlyingNet

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

Para verificar se os métodos de deteção de erros estavam a ser utilizados, utilizamos o seguinte filtro fornecido pelos docentes, obtendo o seguinte resultado:

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

Figura 9: Filtro sem Resultados



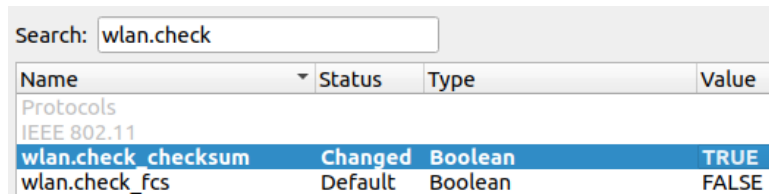
The image shows the Wireshark interface with a filter bar at the top containing the filter `(wlan.fc.type_subtype == 0x08) && (wlan.fcs.status == bad)`. Below the filter bar, the packet list table is empty, indicating no results were found.

No.	Time	Source	Destination	Protocol	Length	Info
-----	------	--------	-------------	----------	--------	------

No entanto, quando aplicado, não obtemos quaisquer resultados, o que intrigou o grupo. Depois de algumas análises das tramas de exercícios anteriores, encontramos o campo *FCS* responsável pela deteção de erros. No entanto, em todas as tramas testadas, apesar de esta conter valores únicos para cada trama, como esperado, encontramos também uma *flag* local do *wireshark* a indicar que esta *checksum* não tinha sido verificada (*[unverified]*).

Depois de uma pesquisa na internet, encontramos que, por defeito, a verificação local da *checksum* das tramas 802.11 está desativada, sendo necessário ativar esta nas definições do *wireshark*. Após a ativação desta funcionalidade, repetimos o filtro, obtendo assim os seguintes resultados:

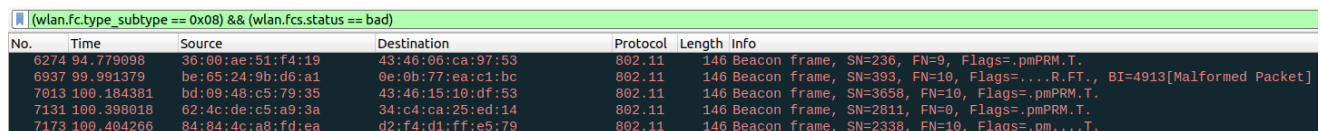
Figura 10: Definição WireShark



The image shows the 'Preferences' dialog for 'wlan.check' in Wireshark. The search bar contains 'wlan.check'. The table below shows the configuration for 'wlan.check_checksum' and 'wlan.check_fcs'.

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

Figura 11: Tramas corrompidas



The image shows the Wireshark interface with the same filter as Figure 9. The packet list table now displays five corrupted frames (802.11 Beacon frames) where the FCS status is 'bad'.

No.	Time	Source	Destination	Protocol	Length	Info
6274	94.779098	36:00:ae:51:f4:19	43:46:06:ca:97:53	802.11	146	Beacon frame, SN=236, FN=9, Flags=.pmPRM.T.
6937	99.991379	be:65:24:9b:d6:a1	0e:0b:77:ea:c1:bc	802.11	146	Beacon frame, SN=393, FN=10, Flags=...R.FT., BI=4913[Malformed Packet]
7013	100.184381	bd:09:48:c5:79:35	43:46:15:10:df:53	802.11	146	Beacon frame, SN=3658, FN=10, Flags=.pmPRM.T.
7131	100.398018	62:4c:de:c5:a9:3a	34:c4:ca:25:ed:14	802.11	146	Beacon frame, SN=2811, FN=0, Flags=.pmPRM.T.
7173	100.404266	84:84:4c:a8:fd:ea	d2:f4:d1:ff:e5:79	802.11	146	Beacon frame, SN=2338, FN=10, Flags=.pm...T.

Como podemos observar, foram capturadas **5 tramas corrompidas**, ou seja, tramas as quais a sua informação contida não corresponde ao valor encontrado na sua *checksum*. Isto ocorre devido a erros de transmissão entre o AP e o STA, visto que estes sinais são transmitidos "sem fios", estão sujeitos a interferências do meio de propagação, como objetos que bloqueiam o sinal, a reflexão deste em objetos ou devido à fraqueza do sinal devido à larga distância entre os dispositivos. Por estes motivos, uma conexão sem fios necessita de um controlo de deteção de erros, de forma a garantir que não existem falhas na transmissão de tramas.

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

Para este exercício, com a utilização da tabela fornecida pelos docentes, calculamos os valores de tipo e subtipo das tramas *Probing Request* e *Probing Response*, chegando ao resultado que estas tem o valor 4 e 5, respetivamente.

(Versão Tipo Subtipo) → (00 00 0100) (00 00 0101) → (0x04) (0x05)

Depois, geramos o seguinte filtro:

(wlan.fc.type_subtype == 0x04) or (wlan.fc.type_subtype == 0x05)

5.11 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?

Utilizando o filtro obtido no exercício anterior, obtemos uma listagem de tramas *Probing Request* e *Probing Response*, escolhendo de seguida um par destas tramas, os quais os endereços de origem e destino correspondessem, ou seja, para um determinado *Request* de um dispositivo, fosse obtido um *Response* para esse mesmo dispositivo. Obtemos assim o seguinte par de tramas:

Figura 12: Par Probing Request/Response

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)
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

Analisando em mais detalhe os endereços das tramas, podemos observar que a primeira trama correspondente ao *Probing Request* tem como endereço MAC de origem um dispositivo que se pretende conectar a alguma rede, e o seu endereço de destino é **ff:ff:ff:ff:ff:ff**, indicando que esta trama é uma trama de *Broadcast*, ou seja, é uma transmissão para todos os dispositivos próximos.

Neste exemplo, depois desta trama de *Broadcast* com o pedido de *Probing* ser transmitida, podemos observar que um dispositivo, neste caso, um AP, com o endereço MAC **bc:14:01:af:b1:98** respondeu a este *Request*, enviando assim ao dispositivo interessado em conectar-se não só o seu endereço MAC como também o SSID da rede que este AP é responsável por gerir. Desta forma o dispositivo Host poderá conhecer os vários AP's e redes que estão disponíveis na sua localização.

6 Processo de Associação

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

Para este exercício, e repetindo o processo de filtragem por tipo de subtipo da trama, começamos por desenvolver um filtro que capturasse todas as tramas dos tipos *Association Request*, *Association Response* e, como antes do processo de associação existe um processo de autenticação, incluímos também as tramas *Authentication*. Por último, visto que cada fase do processo é intercalado com um trama de confirmação, incluímos também a captura de tramas *Acknowledgement*, obtendo o seguinte filtro final, assim como a lista de resultados das tramas capturadas, de forma a demonstrar um processo de associação completo:

(wlan.fc.type_subtype == 0x00) or (wlan.fc.type_subtype == 0x01) or (wlan.fc.type_subtype == 0x0b) or (wlan.fc.type_subtype == 0x1d)

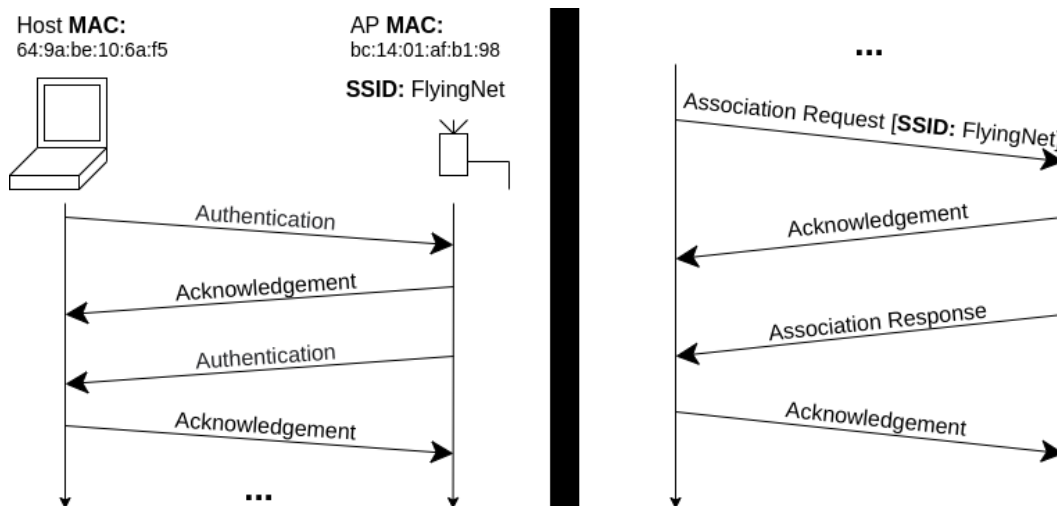
Figura 13: Processo de Associação

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
2487	70.362050	Apple_10:6a:f5	Apple_10:6a:f5 (64:9a:be:10...	802.11	39	Acknowledgement, Flags=.....C
2488	70.381869	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	59	Authentication, SN=2338, FN=0, Flags=.....C
2489	70.381878	HitronTe_af:b1:98	HitronTe_af:b1:98 (bc:14:01...	802.11	39	Acknowledgement, 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=FlyingNet
2491	70.383873	Apple_10:6a:f5	Apple_10:6a:f5 (64:9a:be:10...	802.11	39	Acknowledgement, Flags=.....C
2492	70.389339	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	225	Association Response, SN=2339, FN=0, Flags=.....C
2493	70.389352	HitronTe_af:b1:98	HitronTe_af:b1:98 (bc:14:01...	802.11	39	Acknowledgement, Flags=.....C

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

Utilizando a listagem de tramas obtidas no exercício anterior, construímos o seguinte diagrama que demonstra todas as tramas trocadas no processo de associação:

Figura 14: Diagrama Temporal do Processo de Associação



7 Transferência de Dados

7.14 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?

Observando a trama, em específico, as flags presentes no *Control Frame* desta, podemos observar que as *flags* (baseado no anexo) *To AP* e *From AP* têm, respetivamente os valores 0 e 1, indicando que esta trama está a ser enviada a partir de um AP, em direção a um STA. Concluimos assim que este envio da trama é local à WLAN.

(Nota: Apesar da nomenclatura destas flags serem diferentes entre o anexo e o wireshark (To AP/To DS), estes não impactam a direccionalidade da trama)

Figura 15: Direccionalidade da Trama

```

▶ Frame 431: 226 bytes on wire (1808 bits), 226 bytes captured (1808 bits)
▶ Radiotap Header v0, Length 25
▶ 802.11 radio information
▼ IEEE 802.11 QoS Data, Flags: .p....F.C
  Type/Subtype: QoS Data (0x0028)
  ▼ 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... .... = Order flag: Not strictly ordered
      .000 0000 0010 0100 = Duration: 36 microseconds
      Receiver address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)
      Transmitter address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
      Destination address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)
      Source address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
      BSS Id: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
      STA address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)
      .... .... 0000 = Fragment number: 0
      0011 0011 1110 .... = Sequence number: 830
      Frame check sequence: 0x793feef8 [correct]
      [FCS Status: Good]
    ▶ Qos Control: 0x0000
    ▶ CCMP parameters
  ▶ Data (163 bytes)
```

7.15 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?

Ao analisar a lista de endereços, assim como a sua localização na trama (com auxílio do *hexdump* do wireshark) chegamos à conclusão dos seguintes endereços:

- Address 1 (Receiver): 64:91:be:10:6a:f5
- Address 2 (Transmitter): bc:14:01:af:b1:98
- Address 3 (Router Interface): bc:14:01:af:b1:98

Figura 16: Endereços MAC

```

▶ Frame 431: 226 bytes on wire (1808 bits), 226 bytes captured (1808 bits)
▶ Radiotap Header v0, Length 25
▶ 802.11 radio information
▼ IEEE 802.11 QoS Data, Flags: .p....F.C
  Type/Subtype: QoS Data (0x0028)
  ▶ Frame Control Field: 0x8842
    .000 0000 0010 0100 = Duration: 36 microseconds
    Receiver address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)
    Transmitter address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
    Destination address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)
    Source address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
    BSS Id: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
    STA address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)
    .... 0000 = Fragment number: 0
    0011 0011 1110 .... = Sequence number: 830
    Frame check sequence: 0x793feef8 [correct]
    [FCS Status: Good]
  ▶ Qos Control: 0x0000

0000 00 00 19 00 6f 08 00 00 1a a1 3f 02 00 00 00 00 ...o... ..?....
0010 16 30 a3 09 80 04 bf a9 00 88 42 24 00 64 9a be -0..... ..B$.d..
0020 10 6a f5 bc 14 01 af b1 98 bc 14 01 af b1 98 e0 j.....
0030 33 00 00 79 e3 00 20 01 00 00 00 57 5f c3 ff 53 3..y... ..W_..S
0040 bb 95 b9 a5 5d 96 25 e6 fe d8 a3 9c 0f fd a3 59 ...]%. ....Y
0050 df 9c eb 48 19 77 ca 01 99 e7 19 20 9f bd 99 84 ...H.w... ..
0060 54 09 10 af 0a cb e1 6e 2d 29 d7 0b df 74 5e ea T.....n -)...t^
0070 e2 b9 e1 49 56 ee d7 63 52 c0 f3 ef 43 71 66 5d ...IV..c R...Cqf]
0080 30 f0 1b e7 90 e8 2d 0b 89 b2 88 92 8b da 75 6d 0.....um
0090 46 10 58 a6 ed 2c 36 1c 74 db 6f 4d 16 39 bb 65 F.X... ,6 t.oM.9.e
00a0 06 b2 7b ce d2 8f ae e8 37 5e 29 20 6e 57 15 0c ..{..... 7^). nW..
00b0 96 24 aa 66 1e 91 11 0a 89 08 a7 fb 7f 64 be 90 $.f.....d..
00c0 c5 97 1d 7d 38 7f b0 70 50 a2 25 1e c6 70 0a 82 ...}8..p P.%.p..
00d0 e9 83 89 03 52 7c e0 46 8b 1c 0f ab d3 f9 f8 ee ...R|F .....
00e0 3f 79 ?y

```

Como podemos observar, o endereço do host sem fios (STA) corresponde ao endereço localizado no **Address 1** (64:91:be:10:6a:f5), ou seja, esta trama de dados está direcionada a este host. Já os endereços MAC do AP e o seu router de acesso são idênticos **Address 2** = **Address 3** (bc:14:01:af:b1:98), o que nos leva a concluir que este dispositivo realiza ambas as funcionalidade de routing e transmissão de tramas entres os end hosts. (AP e DS)

7.16 Como interpreta a trama nº433 face à sua direccionalidade e endereçamento MAC?

Nesta trama, ao analisar as flags de direccionalidade presentes no *Control Frame*, concluímos que esta trama está direccionada do STA para o DS/AP. Podemos observar que os seguintes endereços MAC correspondem ao mapeamento feito no exercício anterior, mas com a direccionalidade invertida.

- **Receiver address:** bc:14:01:af:b1:98
- **Transmitter/Source/STA address:** 64:91:be:10:6a:f5
- **Destination address:** bc:14:01:af:b1:98

Figura 17: Direccionalidade e Endereços MAC

```
▶ Frame 433: 178 bytes on wire (1424 bits), 178 bytes captured (1424 bits)
▶ Radiotap Header v0, Length 25
▶ 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... .... = Order flag: Not strictly ordered
      .000 0001 0011 1010 = Duration: 314 microseconds
      Receiver address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
      Transmitter address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)
      Destination address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
      Source address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)
      BSS Id: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
      STA address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)
      .... .... 0000 = Fragment number: 0
      1110 0110 0000 .... = Sequence number: 3680
      Frame check sequence: 0x841b593c [correct]
      [FCS Status: Good]
    ▶ Qos Control: 0x0000
    ▶ CCMP parameters
  ▶ Data (115 bytes)
```

7.17 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.)

Ao longo de uma transferência de dados via sem fios, são utilizadas tramas de controlo do subtipo *Request to Send* e *Clear to Send*. Estas tramas existem devido à necessidade de controlar a transmissão de dados pelo meio de forma a evitar colisões, visto que, a qualquer momento, vários dispositivos (STA) podem estar ligados a um AP e, caso todos façam transmissões em simultâneo, haverá colisões de sinais, ficando todos os dados corrompidos e inutilizados.

Para evitar esta perda de eficiência/débito, foram criadas as tramas *Request to Send* e *Clear to Send*, como o objetivo de organizar e ordenar o envio/transmissão de dados por cada STA. Quando um dispositivo pretende transmitir dados, este começa por enviar ao AP uma trama *Request to Send*, de forma a pedir um "tempo de transmissão". Caso este tempo seja permitido e alocado, o AP irá responder ao dispositivo com a trama *Clear to Send*, indicando que poderá começar a enviar dados.

Este problema não é comum em redes Ethernet visto que, nestas redes, em específico, em LAN's comutadas, cada dispositivo contém um canal de transmissão direto e único que permite evitar quaisquer colisões. É de notar que numa LAN partilhada poderá ocorrer colisões de dados, no entanto, este controlo de colisões já é tratado.

7.18 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

Para este exercício, visto que a trama N^o433 do exercício anterior se trata de uma trama de dados, começamos por observar as tramas capturadas em "redor" desta:

Figura 18: Transmissão de Dados sem Controlo

431 17.922542	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	226 QoS Data, SN=830, FN=0, Flags=...
432 17.922558		HitronTe_af:b1:98 (bc:14:01...	802.11	39 Acknowledgement, Flags=.....
433 17.924985	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	178 QoS Data, SN=3680, FN=0, Flags=...
434 17.925298		Apple_10:6a:f5 (64:9a:be:10...	802.11	39 Acknowledgement, Flags=.....
435 17.927587	Apple_28:b8:0c	HitronTe_af:b1:98	802.11	49 Null function (No data), SN=0, ...
436 17.927618		Apple_28:b8:0c (68:a8:6d:28...	802.11	39 Acknowledgement, Flags=.....

Como podemos observar, nesta transmissão de dados, não houve qualquer controlo de colisões através das tramas *RTS* ou *CTS*.

Para encontrar um exemplo de uma transferência de dados que utilize este controlo, começamos por filtrar as várias tramas com o seguinte filtro:

**wlan.fc.type_subtype == 0x1b or wlan.fc.type_subtype == 0x1c or
(wlan.fc.type_subtype >= 0x20 and wlan.fc.type_subtype <= 0x2f)**

O objetivo deste filtro será listar todas as tramas *RTS* e *CTS*, assim como listar todas as tramas de dados, de forma a facilitar a descoberta de uma transmissão em específico. Depois de obter as tramas resultantes e observado estas, encontramos uma transmissão de dados que utiliza este controlo, estando a sua trama de *RTS* na frame número 816. Depois de encontrado, desfizemos o filtro de forma a observar todas as tramas, eis o resultado obtido:

Figura 19: Transmissão de Dados com Controlo

816 30.824814	HitronTe_af:b1:98 (bc:...	Apple_10:6a:f5 (64:9a:be:10...	802.11	45 Request-to-send, Flags=.....C
817 30.824869		HitronTe_af:b1:98 (bc:14:01...	802.11	39 Clear-to-send, Flags=.....C
818 30.824928	HitronTe_af:b1:96	Apple_10:6a:f5	802.11	146 QoS Data, SN=843, FN=0, Flags=p....F.C
819 30.824938	Apple_10:6a:f5 (64:9a:...	HitronTe_af:b1:98 (bc:14:01...	802.11	57 802.11 Block Ack, Flags=.....C
820 30.841236	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	53 Null function (No data), SN=2509, FN=0, Flags=...P...TC
821 30.841257		Apple_10:6a:f5 (64:9a:be:10...	802.11	39 Acknowledgement, Flags=.....C

Como podemos ver, nesta transferência ocorreu um controlo de envio, com o AP a enviar uma trama *RTS* ao STA e, depois de aceite através da trama *CTS*, estes trocam dados, assim como tramas de confirmação.

Conclusão

Com a conclusão deste trabalho prático, encontramos-nos satisfeitos com as respostas desenvolvidas em cada secção, assim como o trabalho em geral. Acreditamos que alcançamos todas as metas propostas pelos docentes, assim como ter justificado adequadamente os resultados observados.

Este trabalho permitiu cimentar o nosso conhecimento acerca do protocolo Wifi, percebendo melhor os vários detalhes e acerca do protocolo 802.11. Pudemos analisar o conteúdo das tramas *Wifi* e entender a sua importância, analisamos a deteção de erros presente nas tramas, investigamos o funcionamento dos processos de associação entre AP's e STA's, assim como o mecanismo de controlo de acesso utilizado para evitar colisões de transmissão.