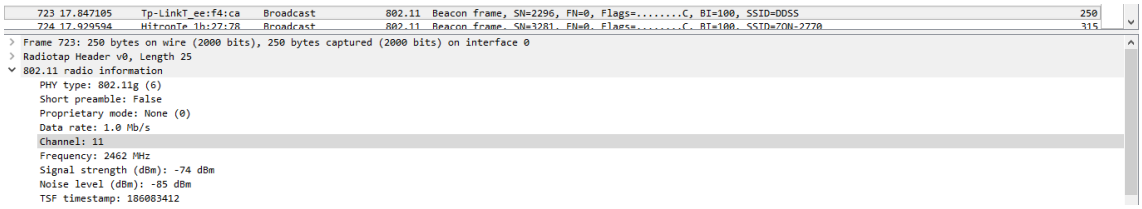
PARTE 1

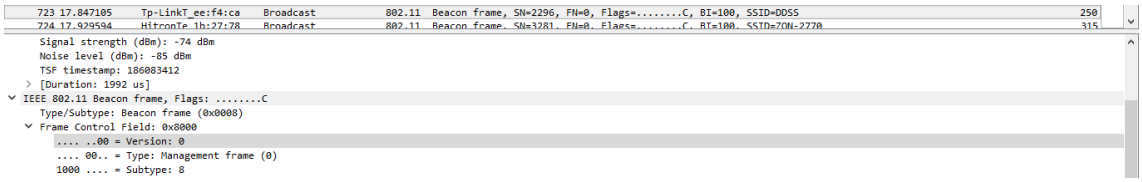
Acesso Rádio

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



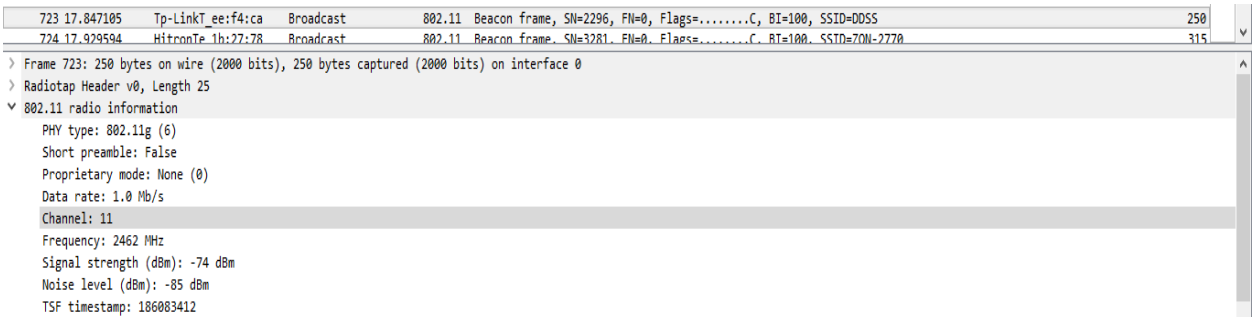
R: Como podemos ver pelas imagens acima, a frequência é 2462 e está no canal 11.

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



R: A versão utilizada é a g tal como podemos ver pela imagem.

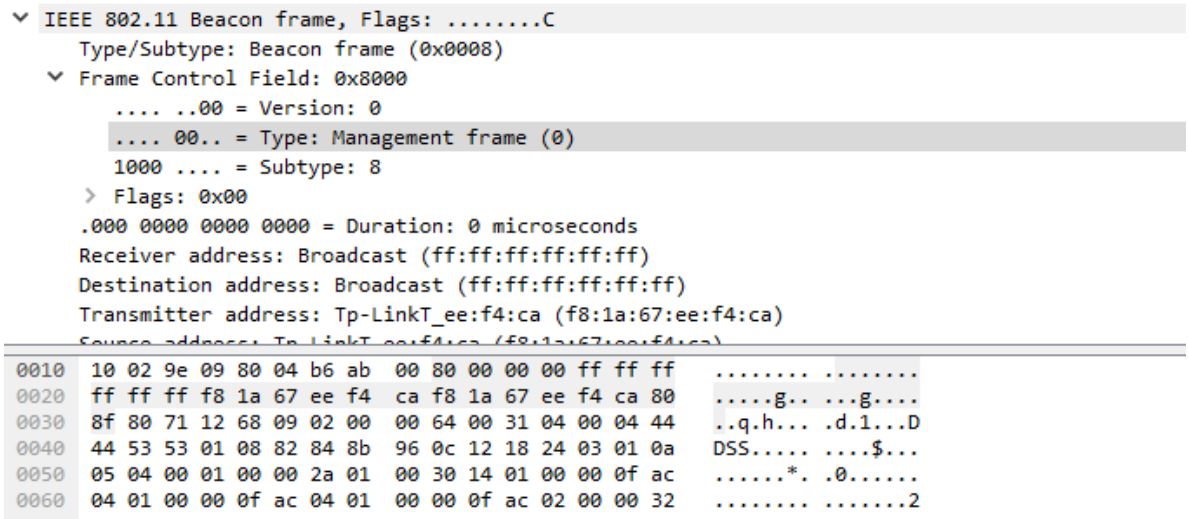
3. Qual o débito a que foi enviada a trama escolhida? Será que esse débito corresponde ao débito máximo a que a interface WiFi pode operar? Justifique.



R: O débito a que foi enviada a trama 45 é 1.0 Mb/s. Sendo o standard 802.11g estes podem operar até 54MBits/s portanto não corresponde ao máximo sendo este de 54Mb/s.

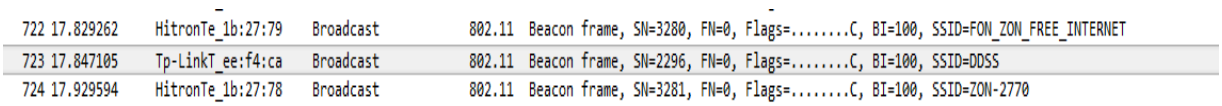
Scanning Passivo e Scanning Ativo

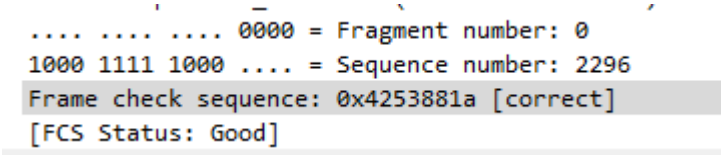
4. Selecione uma trama beacon (cujo número de ordem inclua o seu número de grupo). Esta trama pertence a que tipo de tramas 802.11? Indique o valor dos seus identificadores de tipo e de subtipo. Em que parte concreta do cabeçalho da trama estão especificados (ver anexo)?



R: O tipo da trama é Management frame e o seu tipo é 0 e subtipo é 8. A parte da trama em que estão especificados é visível na segunda imagem apresentada.

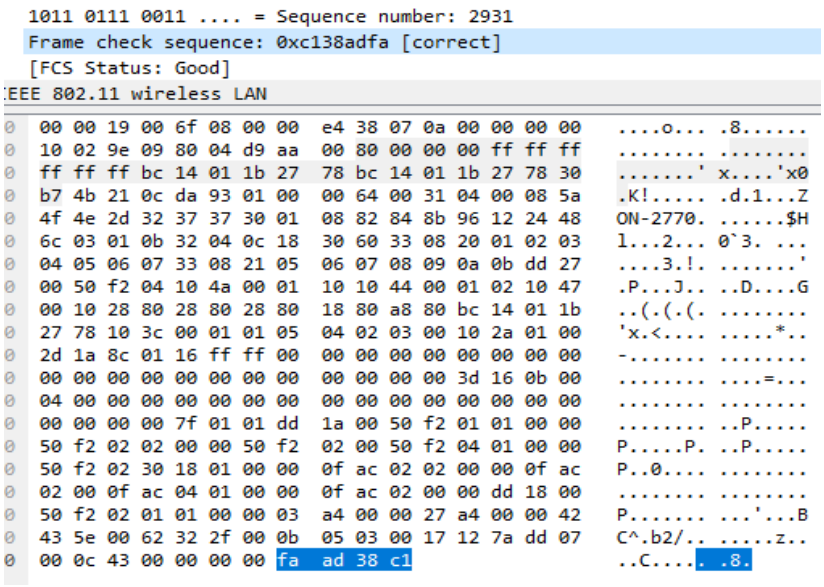
5. Liste todos os SSIDs dos APs (Access Points) que estão a operar na vizinhança da STA de captura? Explicite o modo como obteve essa informação. Como sugestão pode construir um filtro de visualização apropriado (tomando como base a resposta da alínea anterior) que lhe permita obter a listagem pretendida.



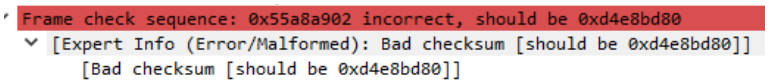


R: As SSIDs dos APs que estão a operar na rede são a SSID= DDSS, a SSID=FON_ZON_FREE_INTERNET e a SSID=ZON-2770. A que tende a proporcionar a melhor qualidade de sinal é SSID=DDSS (ver primeira imagem).

6. Verifique se está a ser usado o método de detecção de erros (CRC), e se todas as tramas Beacon são recebidas corretamente. Justifique a conveniência em usar detecção de erros neste tipo de redes locais.



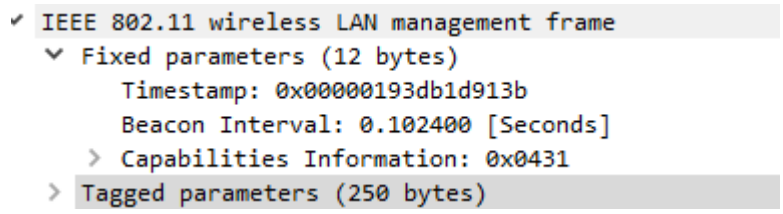
O valor de FCS varia de trama para trama sendo na maior parte delas correto e uma outra parte incorreto. Logo o CRC está a ser usado.



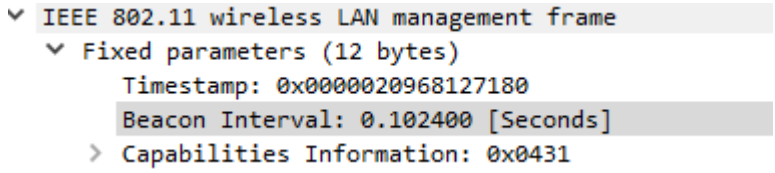
Concluímos que estamos a falar de Collision Avoidance. Este processo é usado neste tipo de redes locais ao contrário do método de Collision Detection usado nos outros tipos de rede.

Este ultimo método citado não é apropriado visto que nas redes sem fios não assumem que as diferentes estações envolvidas possam transmitir e receber dados entre si.
Em suma em Collision Avoidance a estação que recebe dados verifica se CRC é valido. Se assim for, envia uma mensagem de ACK à estação que enviou os dados.

7. Para dois dos APs identificados, indique qual é o intervalo de tempo previsto entre tramas beacon consecutivas? (Nota: este valor é anunciado na própria trama beacon). Na prática, a periodicidade de tramas beacon é verificada? Tente explicar porquê.

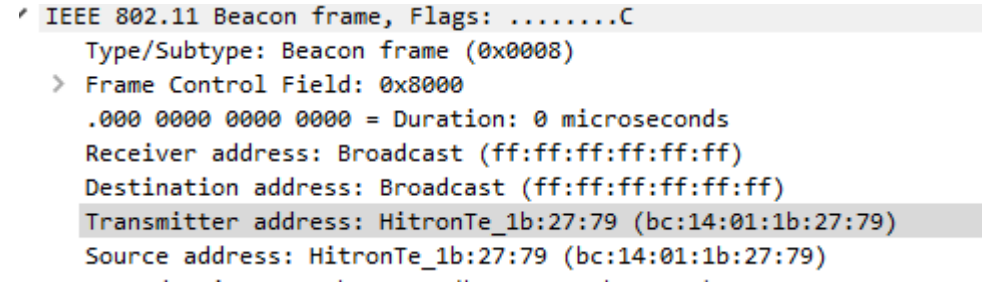


ZON-2770

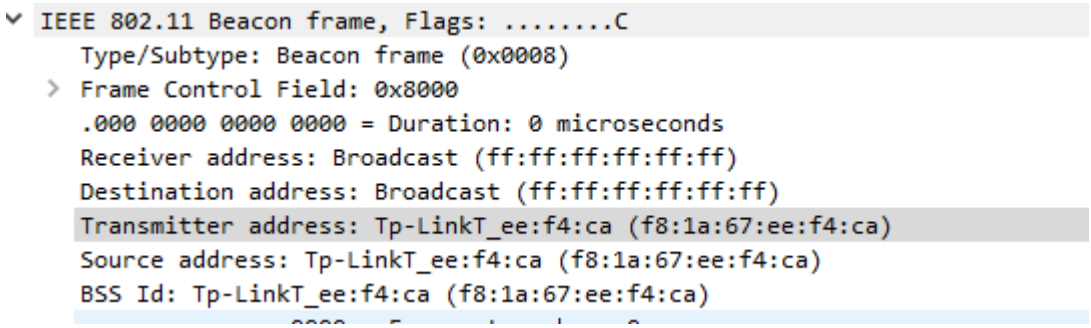


DDSS

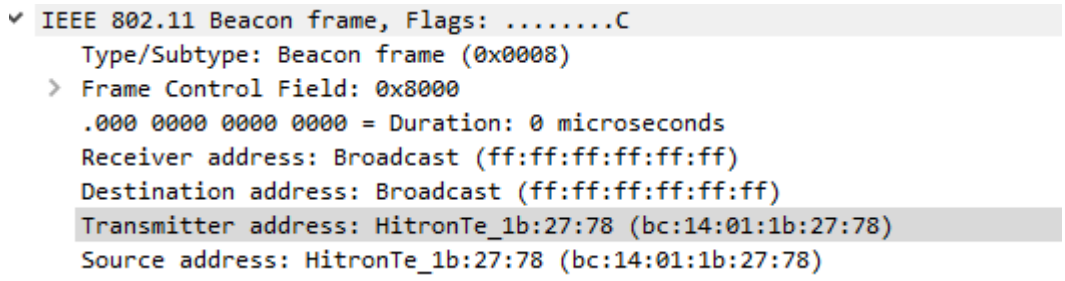
8. Identifique e registe todos os endereços MAC usados nas tramas beacon enviadas pelos APs. Recorde que o endereçamento está definido no cabeçalho das tramas 802.11, podendo ser utilizados até quatro endereços com diferente semântica. Para uma descrição detalhada da estrutura da trama 802.11, consulte o anexo ao enunciado.



FON_ZON FREE INTERNET MAC: bc:14:01:1b:27:79

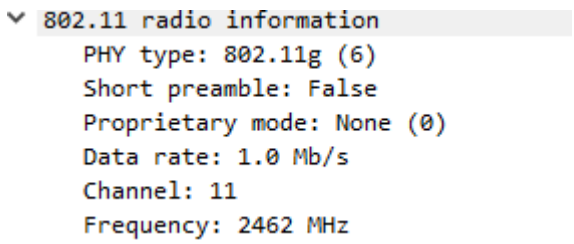


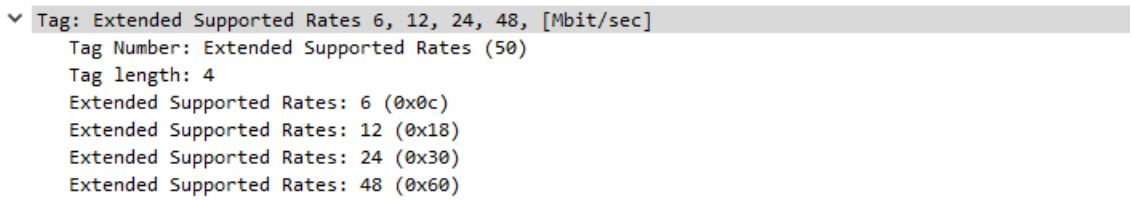
DDSS: f8:1a:67:ee:f4:ca



ZON-2770: bc:14:01:1b:27:78

9. As tramas beacon anunciam que o AP pode suportar vários débitos de base assim como vários “extended supported rates”. Indique quais são esses débitos?





R: Esses débitos suportados são 1.0Mb/s.

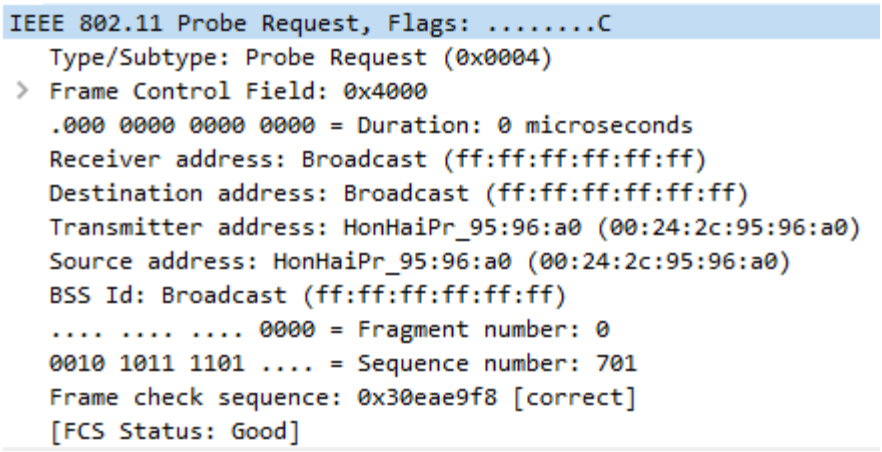
Transferência de Dados

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

R: Usamos o filtro seguinte, uma vez que as tramas de prohibing request e prohibing response apresentam são 0x04 e 0x05 respetivamente:

wlan.fc.type subtype eq 0x04 or wlan.fc.type subtype eq 0x05

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?



R: Estamos perante Active Scanning, visto que são os hosts que procuram informações dos AP's nas suas vizinhanças.

Processo de Associação

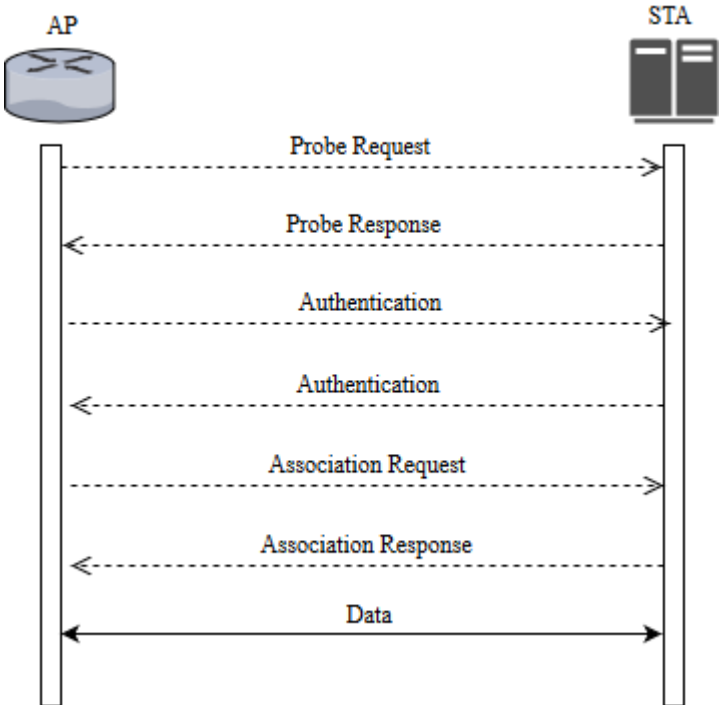
12. Identifique uma sequência de tramas que corresponda a um processo de associação completo entre a STA e o AP, incluindo a fase de autenticação.

R: Usamos o seguinte filtro: wlan.fc.type subtype eq 0x00 or wlan.fc.type subtype eq 0x01 or wlan.fc.type subtype eq 0x0b

Os valores de 0x00,0x01,0x0b correspondem às tramas association request, association response e authentication, respetivamente.

2027 57.879041	Apple_d1:fe:a8	HitronTe_1b:27:78	802.11	70 Authentication, SN=1147, FN=0, Flags=........C
2029 57.879965	HitronTe_1b:27:78	Apple_d1:fe:a8	802.11	59 Authentication, SN=3308, FN=0, Flags=........C
2031 57.881708	Apple_d1:fe:a8	HitronTe_1b:27:78	802.11	185 Association Request, SN=1148, FN=0, Flags=.....
2035 57.890902	HitronTe_1b:27:78	Apple_d1:fe:a8	802.11	225 Association Response, SN=3309, FN=0, Flags=.....

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



Transferência de Dados

14. Considere a trama de dados nº1054. 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?

    A direccionalidade de 1054 é a seguinte:

```
..01 = DS status: Frame from STA to DS via an AP (To DS: 1 From DS: 0) (0x1)
```

Como podemos ver, o DS Status é igual a 01, ou seja, indica que a trama parte da máquina(STA) para o sistema de distribuição(DS) através do acess point(AP). Logo não é igual a WLAN porque este requeria que o valor do DS fosse igual a 0, algo que podemos ver que não acontece em cima.

15. Para a trama de dados nº1054, 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?

```
Receiver address: HitronTe_1b:27:78 (bc:14:01:1b:27:78)
Destination address: HitronTe_1b:27:76 (bc:14:01:1b:27:76)
Transmitter address: Apple_d1:fe:a8 (a4:d1:d2:d1:fe:a8)
Source address: Apple_d1:fe:a8 (a4:d1:d2:d1:fe:a8)
BSS Id: HitronTe_1b:27:78 (bc:14:01:1b:27:78)
STA address: Apple_d1:fe:a8 (a4:d1:d2:d1:fe:a8)
```

Podemos ver em cima que o endereço bc:14:01:1b:27:78 está nos campos BSS id e Receiver address.O endereço bc:14:01:1b:27:76 refere-se exclusivamente a destination address. Por fim é o endereço a4:d1:d2:d1:fe:a8 que se refere a Transmitter adress,Source address e STA address.

16. Como interpreta a trama nº1060 face à sua direccionalidade e endereçamento MAC?

```
10 = DS status: Frame from DS to a STA via AP(To DS: 0 From DS: 1) (0x2)
```

Em cima encontra-se a direccionalidade da trama 1060.

Podemos ver que é ao contrario. Logo parte do DS para o host sem fios(STA) através do acess point(AP).

```
Receiver address: Apple_d1:fe:a8 (a4:d1:d2:d1:fe:a8)
Destination address: Apple_d1:fe:a8 (a4:d1:d2:d1:fe:a8)
Transmitter address: HitronTe_1b:27:78 (bc:14:01:1b:27:78)
Source address: HitronTe_1b:27:76 (bc:14:01:1b:27:76)
BSS Id: HitronTe_1b:27:78 (bc:14:01:1b:27:78)
STA address: Apple_d1:fe:a8 (a4:d1:d2:d1:fe:a8)
```

Verificamos ainda que o STA address corresponde ao endereço MAC de destino, que por sua vez este último corresponde ao router de acesso ao sistema de distribuição

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.)

1054	31.139171	Apple_d1:fe:a8	HitronTe_1b:27:76	802.11	122 QoS Data, SN=4006, FN=0, Flags=
1055	31.139280	HitronTe_1b:27:78 (…	Apple_d1:fe:a8 (a4:…	802.11	57 802.11 Block Ack, Flags=.....
1056	31.139774	HitronTe_1b:27:78 (…	Apple_d1:fe:a8 (a4:…	802.11	49 802.11 Block Ack Req, Flags=...
1057	31.140244	Apple_d1:fe:a8 (a4:…	HitronTe_1b:27:78 (…	802.11	57 802.11 Block Ack, Flags=.....
1058	31.140255	Apple_d1:fe:a8	HitronTe_1b:27:78	802.11	68 Null function (No data), SN=110
1059	31.140315		Apple_d1:fe:a8 (a4:…	802.11	39 Acknowledgement, Flags=.....(
1060	31.141446	HitronTe_1b:27:76	Apple_d1:fe:a8	802.11	125 QoS Data, SN=1753, FN=0, Flags=

R: O subtipo de tramas é o ACK(acknowledgement). Serve de suporte para Collision Avoidance, algo que é necessário para redes sem fios.

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.

Request to Send:

```
IEEE 802.11 Request-to-send, Flags: ........C
   Type/Subtype: Request-to-send (0x001b)
 ▾ Frame Control Field: 0xb400
      .... ..00 = Version: 0
      .... 01.. = Type: Control frame (1)
      1011 .... = Subtype: 11
   ▾ Flags: 0x00
        .... ..00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x0)
        .... .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
        .0.. .... = Protected flag: Data is not protected
        0... .... = Order flag: Not strictly ordered
    .000 0000 0101 0110 = Duration: 86 microseconds
    Receiver address: HitronTe_1b:27:78 (bc:14:01:1b:27:78)
    Transmitter address: Apple_d1:fe:a8 (a4:d1:d2:d1:fe:a8)
```

Clear to Send:

```
IEEE 802.11 Clear-to-send, Flags: ........C
   Type/Subtype: Clear-to-send (0x001c)
 ▾ Frame Control Field: 0xc400
      .... ..00 = Version: 0
      .... 01.. = Type: Control frame (1)
      1100 .... = Subtype: 12
   ▾ Flags: 0x00
        .... ..00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x0)
        .... .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
        .0.. .... = Protected flag: Data is not protected
        0... .... = Order flag: Not strictly ordered
    .000 0000 0010 1010 = Duration: 42 microseconds
    Receiver address: Apple_d1:fe:a8 (a4:d1:d2:d1:fe:a8)
```

Conclusão

Este TP foi acerca de redes sem fios (802.11). Dentro deste tema abordamos vários tópicos, alguns tipos de tramas, limitações na captura de trafego, transferência de dados, associação e desassociação, probing e RTS/CTS.

Apesar de algumas dificuldades, conseguimos finalizar o relatório, aumento o nosso nível de conhecimento acerca destes assuntos. Aprendemos a fazer filtros na ferramenta de WireShark, o que nos ajudou muito, pois esta contém muita informação e a capacidade de filtrar é ótimo.

Aprendemos também a saber a diferença entre uma estação e um acess point, como estas comunicam entre si e com o cliente, como é o caso dos TCP SYN que faz a ligação com o servidor de maneira a que consigamos fazer a transferência de dados.

Apesar de termos conhecimento que nem todas as respostas estão corretas pensamos ter mencionada informação importante em todas elas.