Universidade do Minho
Escola de Engenharia

Redes de Computadores

Licenciatura em Engenharia Informática

Ano Letivo de 2023/2024

TP3

Diogo Gabriel Lopes Miranda (a100839)

João Ricardo Ribeiro Rodrigues (a100598)

Délio Miguel Lopes Alves (a94557)

RC

Índice

Parte 1

1.1 Captura e análise de Tramas Ethernet

Questão 1 - **Anote os endereços MAC de origem e de destino da trama capturada. Identifique a que sistemas se referem. Justifique.**

R: Do ponto de vista do IP, tanto o *host Shrek* como o *servidor Patanews* conhecem o IP um do outro. No entanto, relativamente aos endereços MAC, o mesmo já não acontece. Estes apenas têm conhecimento do MAC do próximo salto no caminho para o destino, ou seja, deste caso, o MAC do *router n1*.

Como podemos observar na figura abaixo, o endereço MAC de origem é 00:00:00:aa:00:00 (indicado no campo *source*) e o endereço MAC de destino é 00:00:00:aa:00:02 (indicado no campo *destination)*.

O endereço de origem corresponde ao *host Shrek* e o endereço de destino corresponde ao *router n1*.

```
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:02 (00:00:00:aa:00:02)
 ▸ Destination: 00:00:00_aa:00:02 (00:00:00:aa:00:02)
 ▸ Source: 00:00:00_aa:00:00 (00:00:00:aa:00:00)
```

Figura 1 - Destination e Source do campo Ethernet do pacote HTTP GET

Questão 2 - **Qual o valor hexadecimal do campo Type da trama Ethernet? O que significa?**

R: O valor do campo *Type* é 0x800 (ou 2048 em decimal), tal como se pode ver pela figura abaixo. Este indica o tipo de dados que a trama transporta, neste caso um pacote IPv4. No caso de o valor ser inferior ou igual a 1500, este representaria o comprimento dos dados na trama Ethernet (*length*).

```
Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:02 (00:00:00:aa:00:02)
 ▸ Destination: 00:00:00_aa:00:02 (00:00:00:aa:00:02)
 ▸ Source: 00:00:00_aa:00:00 (00:00:00:aa:00:00)
   Type: IPv4 (0x0800)
```

Figura 2 - Detalhes de campo Ethernet do pacote HTTP GET

Questão 3 - **Quantos bytes são usados no encapsulamento protocolar, i.e. desde o início da trama até ao início dos dados do nível aplicacional? Calcule e indique, em percentagem, a sobrecarga (overhead) introduzida pela pilha protocolar.**

R: Até ao início dos dados do nível aplicacional existem uma grande quantidade bytes que corresponde aos *headers* dos restantes protocolos encapsulados.

Os tamanhos dos *headers* são os seguintes:

- Ethernet II – 14 bytes
- IPv4 – 20 bytes
- TCP – 32 bytes

O que nos dá um total de 66 bytes ocupados por *headers*, dos 139 bytes totais do datagrama, como se pode ver na figura abaixo.

Figura 3 - Tamanho total do datagrama

Assim sendo, podemos realizar o cálculo abaixo que nos indica que a percentagem de *overhead* introduzida pela pilha protocolar é 47.48%.

$$\frac{66}{139} \times 100 = 47.48\%$$

Questão 4 - **Qual é o endereço Ethernet da fonte? A que sistema de rede corresponde? Justifique.**

R: Tal como podemos observar na figura abaixo, o endereço Ethernet da fonte é 00:00:00:aa:00:02.

Tendo em conta a justificação da *Questão 1*, podemos verificar que o endereço MAC de destino é o endereço do router a que *Shrek* está ligado, o *router n1*.

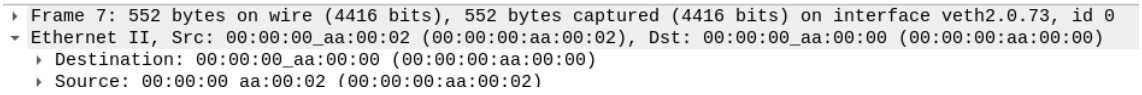


Figura 4 - Destination e Source do campo Ethernet do pacote HTTP OK

Questão 5 - **Qual é o endereço MAC do destino? A que interface corresponde?**

O endereço MAC do destino é 00:00:00:aa:00:00, como se pode ver pela imagem abaixo.

Tendo em conta a justificação da *Questão 1,* verificamos que o endereço corresponde ao endereço de *Shrek*.

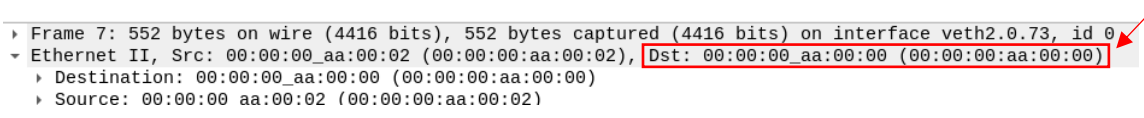


Figura 5 - Destination e Source do campo Ethernet do pacote HTTP OK

1.2 Protocolo ARP e Domínios de Colisão

Questão 1 - **Observe o conteúdo da tabela ARP do Shrek com o comando arp -a. Com a ajuda do manual ARP (man arp), interprete o significado de cada uma das colunas da tabela.**

R: Através do manual ARP, conseguimos interpretar o significado de cada uma das colunas da tabela ARP. Tendo isso em consideração, conseguimos concluir que, a coluna *Adress* corresponde aos endereços(*host*), neste caso temos o *gateway* da rede local. A coluna *HWtype*, fornece-nos o protocolo de camadas físicas utilizado. A coluna *HWaddress*, neste caso, dás-nos o endereço MAC. A coluna *Flags* mostra-nos o tipo de registo que está a ser introduzido em memória. No nosso caso, esse valor foi "C", o que indica este registo foi obtido dinamicamente pelo protocolo ARP e não introduzido manualmente. A coluna *Mask* diz-nos a máscara da sub-rede utilizada. Por fim, a coluna *Iface* diz-nos a interface de rede, neste caso eth0.

```
root@Shrek:/tmp/pycore.43737/Shrek.conf# arp -a
? (10.0.0.1) at 00:00:00:aa:00:02 [ether] on eth0
```

Figura 6 - Execução comando arp -a

```
root@Shrek:/tmp/pycore.43737/Shrek.conf# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.0.1                 ether   00:00:00:aa:00:02   C                     eth0
```

Figura 7 - Execução comando "arp"

Questão 2 - **Observe a trama Ethernet que contém a mensagem com o pedido ARP (ARP Request).**

```
▸ Frame 4: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface veth2.0.b5, id 0
▾ Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▸ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ▸ Source: 00:00:00_aa:00:00 (00:00:00:aa:00:00)
    Type: ARP (0x0806)
▸ Address Resolution Protocol (request)
```

Figura 8 - wireshark comando "arp"

Alínea a **- Qual é o valor hexadecimal dos endereços MAC origem e destino? Como interpreta e justifica o endereço destino usado?**

R: Tal como se pode ver na *Fig.8*, o valor em hexadecimal do endereço de origem é 00:00:00:aa:00:00 e o endereço de destino da trama Ethernet é ff:ff:ff:ff:ff:ff *(Broadcast)*.

O endereço de destino é então o Broadcast, uma vez que o computador que envia o pedido ARP precisa de conhecer o endereço MAC de destino. Assim, envia uma mensagem para o endereço Broadcast (o que equivale a enviar para todas as interfaces adjacentes) e aguarda uma resposta do computador de destino com o seu endereço MAC. Quando recebe essa resposta, adiciona o valor à tabela ARP.

Alínea b **- Qual o valor hexadecimal do campo Tipo da trama Ethernet? O que indica?**

R: O valor hexadecimal do campo Tipo da trama Ethernet é (0x0806), como se pode ver pelo campo Type da *Fig.8*, e indica que se trata do protocolo ARP.

Figura 9-Campo type da Fig.8

***Alínea c* - Observando a mensagem ARP, como pode saber que se trata efetivamente de um pedido ARP? Refira duas formas distintas de obter essa informação.**

R: Como se pode ver na imagem abaixo, o campo *Opcode* possui o valor 1, o que nos indica que, de facto, se trata de um pedido ARP. Por outro lado, também conseguimos verificar que o endereço destino é um Broadcast que, tal como referido anteriormente, é o envio de uma mensagem a todas as interfaces adjacentes com o intuito de pedir (request) ao endereço destino, o que nos permite então ver que a mensagem é um pedido ARP.

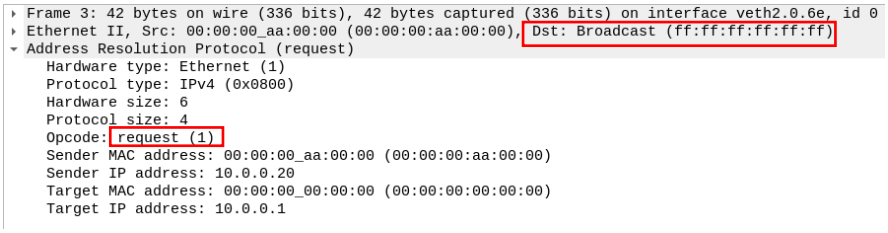


Figura 10-Mensagem ARP

***Questão 3* - Localize a mensagem ARP que é a resposta ao pedido ARP efetuado.**

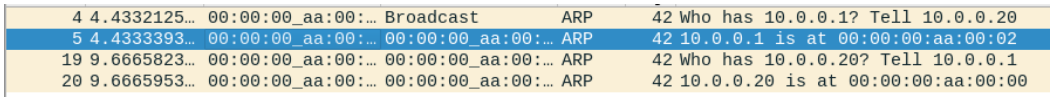


Figura 11 - Mensagem ARP reply

***Alínea a* - Qual o valor do campo ARP opcode? O que especifica?**

R: O campo ARP **Opcode** tem um valor de 2, como se pode ver pela figura abaixo, indicando que esta mensagem ARP se trata efetivamente de uma ARP Reply, respondendo ao pedido anterior.

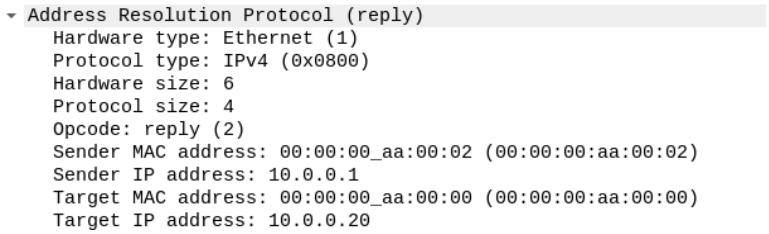


Figura 12- Mensagem ARP

***Alínea b* - Em que posição da mensagem ARP está a resposta ao pedido ARP efetuado?**

R: A resposta ao pedido ARP efetuado está no campo “Sender MAC address” como podemos ver pelas Fig.10 e Fig.11.

```
42 10.0.0.1 is at 00:00:00:aa:00:02
```

Figura 13-Mensagem reply ARP

```
▾ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: 00:00:00_aa:00:02 (00:00:00:aa:00:02)
    Sender IP address: 10.0.0.1
    Target MAC address: 00:00:00_aa:00:00 (00:00:00:aa:00:00)
    Target IP address: 10.0.0.20
```

Figura 14-ARP Replay

***Alínea c* - Identifique a que sistemas correspondem os endereços MAC de origem e de destino da trama em causa, recorrendo aos comandos ifconfig, netstat -rn e arp executados no PC selecionado.**

R: Podemos identificar, como sistema correspondente ao endereço MAC de origem, o router "n1", pois através do comando arp identificamos, facilmente, a correspondência entre o seu endereço IP e o seu endereço MAC e conseguimos identificar na topologia a que sistema pertence.

Podemos ainda ver também, como sistema correspondente ao endereço MAC de destino, o host "Shrek", através do comando ifconfig que mostra tanto o seu endereço IP como o seu endereço MAC.

```
root@Shrek:/tmp/pycore.38435/Shrek.conf# netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         10.0.0.1        0.0.0.0         UG        0 0          0 eth0
10.0.0.0        0.0.0.0         255.255.255.0   U         0 0          0 eth0
root@Shrek:/tmp/pycore.38435/Shrek.conf# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.0.1                 ether   00:00:00:aa:00:02   C                     eth0
root@Shrek:/tmp/pycore.38435/Shrek.conf# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.0.20  netmask 255.255.255.0  broadcast 0.0.0.0
        inet6 2001::20  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::200:ff:feaa:0  prefixlen 64  scopeid 0x20<link>
        ether 00:00:00:aa:00:00  txqueuelen 1000  (Ethernet)
        RX packets 878  bytes 73116 (73.1 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 23  bytes 1803 (1.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 648 (648.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 648 (648.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figura 15

***Alínea d* - Justifique o modo de comunicação (unicast vs. broadcast) usado no envio da resposta ARP (ARP Reply).**

R:O protocolo Address Resolution Protocol (ARP) é utilizado para mapeamento de endereços IP para endereços físicos de rede (MAC). Quando um dispositivo necessita de enviar um pacote para outro dispositivo da sua rede, ele pode usar o ARP para descobrir qual é o endereço MAC do dispositivo de destino.

Quando um dispositivo emite uma solicitação ARP (ARP Request), ele envia uma mensagem de broadcast para todos os dispositivos da sua rede local, perguntando "quem possui o endereço IP X?". Todos os dispositivos na rede receberão então esta mensagem e o dispositivo a que corresponder o endereço IP especificado enviará então uma resposta ARP (ARP Reply) contendo seu endereço MAC para o dispositivo solicitante.

A resposta ARP é enviada em unicast, ou seja, é direcionada especificamente ao dispositivo que fez a solicitação ARP original. Isto acontece porque o dispositivo solicitante precisa do endereço MAC específico do dispositivo de destino para enviar o pacote de dados. Enviar a resposta em broadcast para todos os dispositivos na rede seria ineficiente e poderia causar tráfego desnecessário na rede. Portanto, a resposta ARP é sempre enviada em unicast para minimizar o tráfego na rede e garantir a entrega eficiente de pacotes entre os diferentes dispositivos.

***Questão 4* - O Burro recebeu toda a informação trocada na interação anterior? Qual será a razão para tal?**

R: Não, o Burro não recebeu toda a informação do pedido do Sherk. O burro recebeu o pedido inicial, mas não recebeu a resposta relativa a esse pedido. Isto acontece devido ao facto de o pedido inicial do Sherk ter sido em Broadcast. O switch n2, vai distribuir este pedido, por todos dispositivos conectados a ele, garantindo com que o Burro receba o pedido.

Em relação à resposta transmitida pelo Pantanews, esta será enviada no formato unicast diretamente para o endereço do Sherk. Quando tal resposta alcança o switch n2, este consulta a sua tabela de endereços MAC e redireciona a resposta diretamente para o Sherk. Assim, o Burro não recebe a mensagem de resposta do Pantanews, uma vez que o switch a direciona para o destino com o endereço MAC especificado na mensagem.

1	0.0000000…	10.0.0.1	224.0.0.5	OSPF	78 Hello Packet
2	2.0007178…	10.0.0.1	224.0.0.5	OSPF	78 Hello Packet
3	2.4313075…	00:00:00_aa:00:…	Broadcast	ARP	42 Who has 10.0.0.1? Tell 10.0
4	4.0022570…	10.0.0.1	224.0.0.5	OSPF	78 Hello Packet
5	6.0023215…	10.0.0.1	224.0.0.5	OSPF	78 Hello Packet

Figura 16

***Questão 5* - Repita a experiência com uma captura na interface do PC da Fiona. Documente as suas observações e conclusões com base no tráfego observado/capturado.**

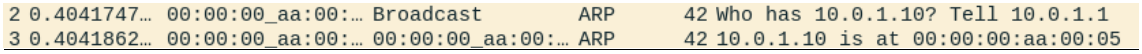


Figura 17

R: Como se pode observar na figura acima, a Fiona recebe tanto o pedido em Broadcast, feito pelo Sherk, como a resposta proveniente do Pantanews. Isto deve-se ao facto dos pedidos em Broadcast serem enviados para todos os dispositivos na rede. Contudo, ao contrário do Burro, a Fiona recebe a resposta, pois o hub ao qual está ligada retransmite todas as mensagens que recebe para todos os dispositivos a ele ligados, independentemente do endereço MAC de destino. Esta situação evidencia uma limitação dos hubs, que não filtram o tráfego com base no endereço MAC.

Questão 6 - **Esboce um diagrama em que indique claramente, e de forma cronológica, todas as mensagens trocadas entre o Shrek e os sistemas com os quais comunica, até à recepção do primeiro pacote que contém dados HTTP. Assuma que todas as tabelas ARP se encontram inicialmente vazias.**

1º ARP Request

		IP O: Shrek	MAC O: Shrek
		IP D: n1	MAC D: 00:00:00:00:00:00
MAC O: Shrek	MAC D: ff:ff:ff:ff:ff:ff		

1º ARP Reply

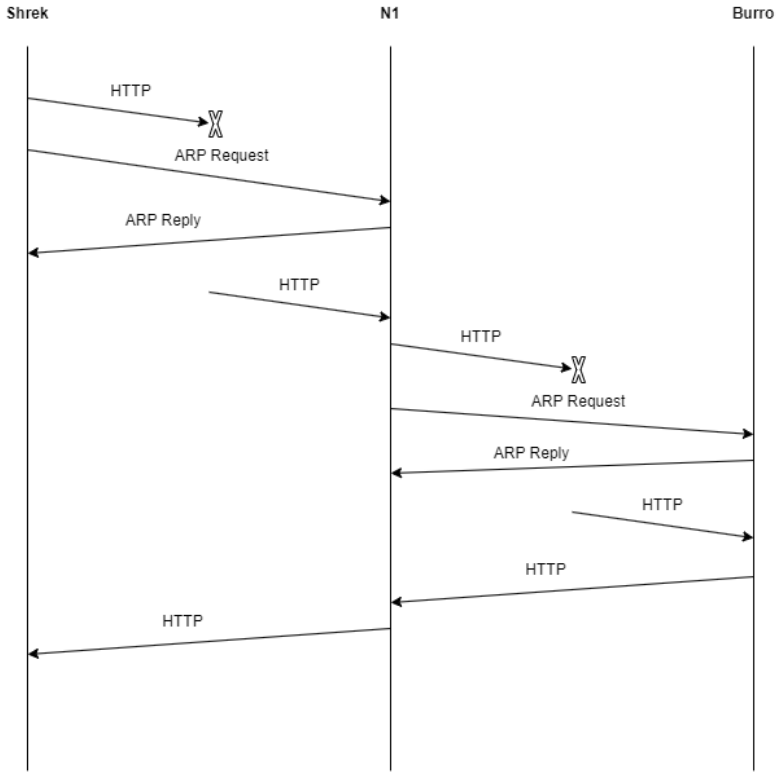
		IP O: n1	MAC O: n1
		IP D: Sherk	MAC D: Shrek
MAC O: n1	MAC D: Sherk		

2º ARP Request

		IP O: n1	MAC O: n1
		IP D: Pantanews	MAC D: 00:00:00:00:00:00
MAC O: n1	MAC D: ff:ff:ff:ff:ff:ff		

2º ARP Reply

		IP O: Pantanews	MAC O: Pantanews
		IP D:n1	MAC D: n1
MAC O: Pantanews	MAC D: n1		



Questão 7 - **Construa manualmente a tabela de comutação do switch da casa do Shrek, atribuindo números de porta à sua escolha.**

1	MAC Shrek: 00:00:00:aa:00:00
2	MAC Burro: 00:00:00:aa:00:01
3	MAC N1: 00:00:00:aa:00:02

Parte 2 - Redes Locais sem Fios (Wi-Fi)

2.1 Acesso Rádio

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

A nossa trama é a trama de ordem 60. A sua informação está apresentada na figura abaixo.

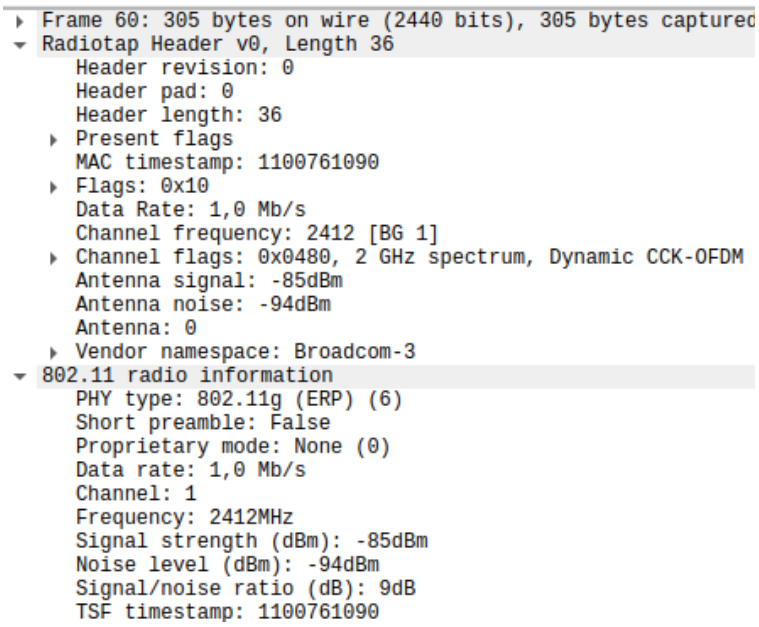


Figura 18-Informações da trama 60

A frequência do espetro em que a rede sem fios está a operar é 2412 MHz, como podemos verificar pela imagem acima no campo *Channel Frequency*.

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

A versão da norma IEEE 802.11 que está a ser usado é a IEEE 802.11g, como podemos verificar pelo campo *PHY Type* da *Figura 18*.

Questão 3 - **Qual a taxa de transmissão a que foi enviada a trama escolhida? Será que essa taxa de transmissão corresponde à máxima que a interface Wi-Fi pode operar? Justifique.**

A taxa de transmissão a que foi enviada foi 1 Mb/s, como indicado no campo *Data rate* da *Figura 18*.

Esta não é a taxa de transmissão máxima a que a interface Wi-Fi pode operar, visto que a norma IEEE 802.11g tem uma taxa de transmissão máxima teórica de 54 Mb/s.

2.2 *Scanning* Passivo e Scanning Ativo

Questão 4 - **Selecione uma trama beacon cuja ordem (ou terminação) corresponda a XX. Esta trama pertence a que tipo de tramas 802.11? Identifique o valor dos identificadores de tipo e de subtipo da trama. Em que parte concreta do cabeçalho da trama estão especificados (ver Anexo I)?**

R: A nossa trama beacon a utilizar é a trama de ordem 60, que, por coincidência, é a mesma trama que utilizamos nas questões anteriores.

O tipo desta trama é 802.11g.

```
▾ 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_9e:9b:b0 (00:06:91:9e:9b:b0)
    Source address: PTInovac_9e:9b:b0 (00:06:91:9e:9b:b0)
    BSS Id: PTInovac_9e:9b:b0 (00:06:91:9e:9b:b0)
    .... .... .... 0000 = Fragment number: 0
    0000 0010 1100 .... = Sequence number: 44
    Frame check sequence: 0x8df2bd52 [correct]
    [FCS Status: Good]
```

Figura 19 - Informações da trama beacon 60

Como podemos ver no campo *Frame Control Field* o identificador de tipo é 0 e o identificador de subtipo é 8. Estes estão indicados no campo Frame Control do cabeçalho da trama.

Questão 5 - **Verifique se está a ser usado o método de deteção de erros (CRC). Justifique. (Poderá ter de ativar a verificação no Wireshark, em Edit -> Preferences -> Protocols -> IPv4 -> "Validate Checksum if Possible")**

R:Inicialmente, nenhum protocolo de controlo de erros está ativo, como podemos verificar na *Figura 20*. No entanto, após ativar as opções. *Assume packets have FCS* e *Validate the FCS checksum if possible,* o protocolo de controlo de erros é ativado, e é fornecido um *FCS Status* indicando se o pacote se encontra bem ou não, como podemos verificar pela *Figura 21*.

```
▾ 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_9e:9b:b0 (00:06:91:9e:9b:b0)
    Source address: PTInovac_9e:9b:b0 (00:06:91:9e:9b:b0)
    BSS Id: PTInovac_9e:9b:b0 (00:06:91:9e:9b:b0)
    .... .... .... 0000 = Fragment number: 0
    0000 0010 1100 .... = Sequence number: 44
    Frame check sequence: 0x8df2bd52 [unverified]
```

Figura 20-Sem protocolo de controlo de erros

```
▾ 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_9e:9b:b0 (00:06:91:9e:9b:b0)
    Source address: PTInovac_9e:9b:b0 (00:06:91:9e:9b:b0)
    BSS Id: PTInovac_9e:9b:b0 (00:06:91:9e:9b:b0)
    .... .... .... 0000 = Fragment number: 0
    0000 0010 1100 .... = Sequence number: 44
    Frame check sequence: 0x8df2bd52 [correct]
```

Figura 21 - Com protocolo de erros

Questão 6 - **Justifique o porquê de ser necessário usar deteção de erros em redes sem fios.**

R: Contrariamente às redes Ethernet, as redes sem fios são extremamente suscetíveis a interferência, o que torna a probabilidade de um pacote ser corrompido extremamente alta. Como tal, os protocolos de deteção de erros são muito importantes para detetar estas situações e poderem ser corrigidas.

Questão 7 - **Uma trama beacon anuncia o intervalo entre beacons às várias taxas de transmissão (B) que o AP suporta, assim como várias taxas de transmissão adicionais (extended supported rates). Indique qual a periodicidade e as taxas de transmissão suportadas pelo AP da trama beacon selecionada.**

R:As taxas de transmissão e a periodicidade suportadas podem ser encontradas na secção *IEE 802.11 Wireless Management* da trama, como podemos visualizar na figura abaixo.

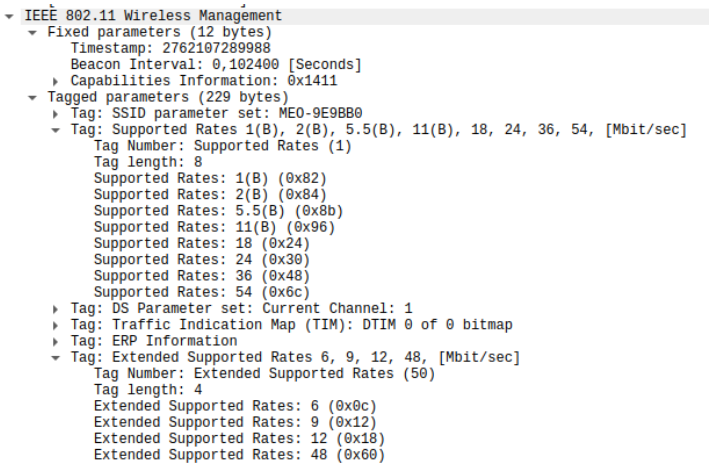


Figura 22 - Taxas de transmissão e periodicidade suportadas

As taxas de transmissão suportadas são:

- 1(B) Mbit/s
- 2(B) Mbit/s
- 5.5(B) Mbit/s
- 11(B) Mbit/s
- 18 Mbit/s
- 24 Mbit/s
- 36 Mbit/s
- 54 Mbit/s

As taxas de transmissão adicionais são:

- 6 Mbit/s
- 9 Mbit/s
- 12 Mbit/s
- 48 Mbit/s

Os items que possuem um (B) são as taxas básicas, taxas obrigatórias para todos os dispositivos Wi-Fi na rede.

Questão 8 - **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).**

R: Alguns dos SSIDs dos APs que estão a operar na vizinhança da STA de captura são:

- "Meo-677760"
- "Meo-9E9BB0"
- "TP-LINK_AP_AF08"
- "Vodafone-528777"

Para obter estas informações recorremos ao uso do filtro "wlan.ssid" e analisamos o campo ssid .

wlan.ssid

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	PTInovac_9e:9b:…	Broadcast	802.…	230	Beacon frame, SN=34, FN=0, Flags=........C, BI=100, SSID=MEO-WiFi
2	0.073779	PTInovac_67:77:…	Broadcast	802.…	305	Beacon frame, SN=1581, FN=0, Flags=........C, BI=100, SSID=MEO-677760
3	0.076298	PTInovac_67:77:…	Broadcast	802.…	230	Beacon frame, SN=1582, FN=0, Flags=........C, BI=100, SSID=MEO-WiFi
4	0.100873	PTInovac_9e:9b:…	Broadcast	802.…	305	Beacon frame, SN=35, FN=0, Flags=........C, BI=100, SSID=MEO-9E9BB0
5	0.103341	PTInovac_9e:9b:…	Broadcast	802.…	230	Beacon frame, SN=36, FN=0, Flags=........C, BI=100, SSID=MEO-WiFi
6	0.161139	PTInovac_9b:f2:…	Broadcast	802.…	230	Beacon frame, SN=199, FN=0, Flags=........C, BI=100, SSID=MEO-WiFi
7	0.179258	PTInovac_67:77:…	Broadcast	802.…	305	Beacon frame, SN=1583, FN=0, Flags=........C, BI=100, SSID=MEO-677760
21	0.205777	PTInovac_9e:9b:…	Broadcast	802.…	305	Beacon frame, SN=37, FN=0, Flags=........C, BI=100, SSID=MEO-9E9BB0
22	0.205853	PTInovac_9e:9b:…	Broadcast	802.…	230	Beacon frame, SN=38, FN=0, Flags=........C, BI=100, SSID=MEO-WiFi
37	0.261720	PTInovac_9b:f2:…	Broadcast	802.…	337	Beacon frame, SN=200, FN=0, Flags=........C, BI=100, SSID=MEO-9BF2A0
38	0.281683	PTInovac_67:77:…	Broadcast	802.…	305	Beacon frame, SN=1585, FN=0, Flags=........C, BI=100, SSID=MEO-677760
39	0.281707	PTInovac_67:77:…	Broadcast	802.…	230	Beacon frame, SN=1586, FN=0, Flags=........C, BI=100, SSID=MEO-WiFi
40	0.308231	PTInovac_9e:9b:…	Broadcast	802.…	305	Beacon frame, SN=39, FN=0, Flags=........C, BI=100, SSID=MEO-9E9BB0
41	0.308305	PTInovac_9e:9b:…	Broadcast	802.…	230	Beacon frame, SN=40, FN=0, Flags=........C, BI=100, SSID=MEO-WiFi
42	0.330925	Tp-LinkT_a3:af:…	Broadcast	802.…	282	Beacon frame, SN=996, FN=0, Flags=........C, BI=100, SSID=TP-LINK_AP_AF08
43	0.364087	PTInovac_9b:f2:…	Broadcast	802.…	337	Beacon frame, SN=202, FN=0, Flags=........C, BI=100, SSID=MEO-9BF2A0
44	0.364191	PTInovac_9b:f2:…	Broadcast	802.…	230	Beacon frame, SN=203, FN=0, Flags=........C, BI=100, SSID=MEO-WiFi
45	0.383974	PTInovac_67:77:…	Broadcast	802.…	305	Beacon frame, SN=1587, FN=0, Flags=........C, BI=100, SSID=MEO-677760
46	0.384686	PTInovac_67:77:…	Broadcast	802.…	230	Beacon frame, SN=1588, FN=0, Flags=........C, BI=100, SSID=MEO-WiFi
49	0.410555	PTInovac_9e:9b:…	Broadcast	802.…	305	Beacon frame, SN=41, FN=0, Flags=........C, BI=100, SSID=MEO-9E9BB0
50	0.410675	PTInovac_9e:9b:…	Broadcast	802.…	230	Beacon frame, SN=42, FN=0, Flags=........C, BI=100, SSID=MEO-WiFi
52	0.433234	Tp-LinkT_a3:af:…	Broadcast	802.…	282	Beacon frame, SN=997, FN=0, Flags=........C, BI=100, SSID=TP-LINK_AP_AF08

Figura 23 - Resultado Filtro "wlan.ssid "

Questão 9 - **Estabeleça um filtro Wireshark apropriado que lhe permita visualizar todas as tramas probing request e probing response, simultaneamente.**

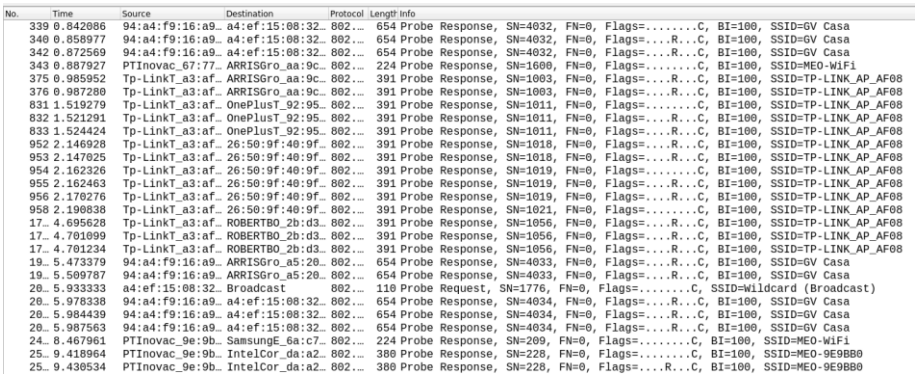
De forma a visualizar as tramas *probing request* e *probing response* simultaneamente aplicamos o seguinte filtro à captura Wireshark:

wlan.fc.type_subtype == 0x04 || wlan.fc.type_subtype == 0x05

wlan.fc.type_subtype == 0x04 : Esta parte do filtro filtra as tramas cujo subtipo seja 0x04 (probing request)

wlan.fc.type_subtype == 0x05 : Esta parte do filtro filtra as tramas cujo subtipo seja 0x05 (probing response)

O resultado do filtro é apresentado na figura seguinte:



No.	Time	Source	Destination	Protocol	Length	Info
339	0.842086	94:a4:f9:16:a9…	a4:ef:15:08:32…	802.…	654	Probe Response, SN=4032, FN=0, Flags=........C, BI=100, SSID=GV Casa
340	0.858977	94:a4:f9:16:a9…	a4:ef:15:08:32…	802.…	654	Probe Response, SN=4032, FN=0, Flags=....R...C, BI=100, SSID=GV Casa
342	0.872569	94:a4:f9:16:a9…	a4:ef:15:08:32…	802.…	654	Probe Response, SN=4032, FN=0, Flags=....R...C, BI=100, SSID=GV Casa
343	0.887927	PTInovac_67:77…	ARRISGro_aa:9c…	802.…	224	Probe Response, SN=1600, FN=0, Flags=........C, BI=100, SSID=MEO-WiFi
375	0.985952	Tp-LinkT_a3:af…	ARRISGro_aa:9c…	802.…	391	Probe Response, SN=1003, FN=0, Flags=....R...C, BI=100, SSID=TP-LINK_AP_AF08
376	0.987280	Tp-LinkT_a3:af…	ARRISGro_aa:9c…	802.…	391	Probe Response, SN=1003, FN=0, Flags=....R...C, BI=100, SSID=TP-LINK_AP_AF08
831	1.519279	Tp-LinkT_a3:af…	OnePlusT_92:95…	802.…	391	Probe Response, SN=1011, FN=0, Flags=........C, BI=100, SSID=TP-LINK_AP_AF08
832	1.521291	Tp-LinkT_a3:af…	OnePlusT_92:95…	802.…	391	Probe Response, SN=1011, FN=0, Flags=....R...C, BI=100, SSID=TP-LINK_AP_AF08
833	1.524424	Tp-LinkT_a3:af…	OnePlusT_92:95…	802.…	391	Probe Response, SN=1011, FN=0, Flags=....R...C, BI=100, SSID=TP-LINK_AP_AF08
952	2.146928	Tp-LinkT_a3:af…	26:50:9f:40:9f…	802.…	391	Probe Response, SN=1018, FN=0, Flags=....R...C, BI=100, SSID=TP-LINK_AP_AF08
953	2.147025	Tp-LinkT_a3:af…	26:50:9f:40:9f…	802.…	391	Probe Response, SN=1018, FN=0, Flags=....R...C, BI=100, SSID=TP-LINK_AP_AF08
954	2.162326	Tp-LinkT_a3:af…	26:50:9f:40:9f…	802.…	391	Probe Response, SN=1019, FN=0, Flags=........C, BI=100, SSID=TP-LINK_AP_AF08
955	2.162463	Tp-LinkT_a3:af…	26:50:9f:40:9f…	802.…	391	Probe Response, SN=1019, FN=0, Flags=....R...C, BI=100, SSID=TP-LINK_AP_AF08
956	2.170276	Tp-LinkT_a3:af…	26:50:9f:40:9f…	802.…	391	Probe Response, SN=1019, FN=0, Flags=....R...C, BI=100, SSID=TP-LINK_AP_AF08
958	2.190838	Tp-LinkT_a3:af…	26:50:9f:40:9f…	802.…	391	Probe Response, SN=1021, FN=0, Flags=........C, BI=100, SSID=TP-LINK_AP_AF08
17…	4.695628	Tp-LinkT_a3:af…	ROBERTBO_2b:d3…	802.…	391	Probe Response, SN=1056, FN=0, Flags=....R...C, BI=100, SSID=TP-LINK_AP_AF08
17…	4.701099	Tp-LinkT_a3:af…	ROBERTBO_2b:d3…	802.…	391	Probe Response, SN=1056, FN=0, Flags=....R...C, BI=100, SSID=TP-LINK_AP_AF08
17…	4.701234	Tp-LinkT_a3:af…	ROBERTBO_2b:d3…	802.…	391	Probe Response, SN=1056, FN=0, Flags=....R...C, BI=100, SSID=TP-LINK_AP_AF08
19…	5.473379	94:a4:f9:16:a9…	ARRISGro_a5:20…	802.…	654	Probe Response, SN=4033, FN=0, Flags=....R...C, BI=100, SSID=GV Casa
19…	5.509787	94:a4:f9:16:a9…	ARRISGro_a5:20…	802.…	654	Probe Response, SN=4033, FN=0, Flags=....R...C, BI=100, SSID=GV Casa
20…	5.933333	a4:ef:15:08:32…	Broadcast	802.…	110	Probe Request, SN=1776, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
20…	5.978338	94:a4:f9:16:a9…	a4:ef:15:08:32…	802.…	654	Probe Response, SN=4034, FN=0, Flags=....R...C, BI=100, SSID=GV Casa
20…	5.984439	94:a4:f9:16:a9…	a4:ef:15:08:32…	802.…	654	Probe Response, SN=4034, FN=0, Flags=....R...C, BI=100, SSID=GV Casa
20…	5.987563	94:a4:f9:16:a9…	a4:ef:15:08:32…	802.…	654	Probe Response, SN=4034, FN=0, Flags=....R...C, BI=100, SSID=GV Casa
24…	8.467961	PTInovac_9e:9b…	SamsungE_6a:c7…	802.…	224	Probe Response, SN=209, FN=0, Flags=........C, BI=100, SSID=MEO-WiFi
25…	9.418964	PTInovac_9e:9b…	IntelCor_da:a2…	802.…	380	Probe Response, SN=228, FN=0, Flags=........C, BI=100, SSID=MEO-9E9BB0
25…	9.430534	PTInovac_9e:9b…	IntelCor_da:a2…	802.…	380	Probe Response, SN=228, FN=0, Flags=....R...C, BI=100, SSID=MEO-9E9BB0

Figura 24 - Resultado dos filtros

Questão 10 - **Assuma que a STA de captura consegue se associar a qualquer AP na vizinhança. Dadas as tramas recebidas através do scanning ativo e passivo, observe os valores da força do sinal (Signal Strength) nas meta-informações de nível físico e aponte qual AP a STA de captura deve se associar para obter a melhor qualidade de ligação possível. Indique como chegou a esta resposta.**

De forma a fazer esta análise e obter a melhor qualidade de ligação possível, escolhemos os 4 SSIDs mais frequentes, e vamos fazer esta análise entre apenas esses. Para cada SSID iremos analisar apenas uma trama pois tramas com o mesmo SSID irão ter valores muito semelhantes de *signal strength* entre eles.

BSSID	Channel	SSID	Percent Packe	Percent Retry	Retry	Beacons	Data Pkts	obe Reqs	obe Resp	Auths	Deauths	Other	Protection
00:06:91:67:77:60	1	MEO-677760	30.6	10.4	272	1152	1330	4	131	0	0	0	Unknown
00:06:91:67:77:62	1	MEO-WiFi	16.6	11.2	160	1111	138	0	148	2	0	24	
00:06:91:82:88:30	1	MEO-828830	1.2	0.0	0	87	15	0	0	0	0	0	Unknown
00:06:91:82:88:32	1	MEO-WiFi	0.9	0.0	0	77	0	0	0	0	0	0	
00:06:91:9b:f2:a0	1	MEO-9BF2A0	3.8	2.8	9	226	82	1	13	0	0	0	Unknown
00:06:91:9b:f2:a2	1	MEO-WiFi	3.0	0.4	1	257	0	0	1	0	0	0	
00:06:91:9e:9b:b0	1	MEO-9E9BB0	12.1	2.6	27	927	70	0	37	0	0	0	Unknown
00:06:91:9e:9b:b2	1	MEO-WiFi	10.6	4.2	38	855	0	0	53	0	0	0	
00:06:91:f1:75:70	1	MEO-F17570	0.0	0.0	0	2	1	0	0	0	0	0	Unknown
00:06:91:f1:75:72	1	MEO-WiFi	0.0	0.0	0	2	0	0	0	0	0	0	
7c:16:89:f8:7f:24		<Broadcast>	0.2	38.9	7	0	18	0	0	0	0	0	Unknown
7c:db:98:40:93:f3	1	NOS-93F3	0.2	0.0	0	20	0	0	0	0	0	0	
94:a4:f9:16:a9:b4	1	GV Casa	4.3	68.3	250	10	83	0	273	0	0	0	Unknown
a6:ef:15:08:32:99	1	phi_F41927C3C6…	0.8	2.9	2	65	0	0	3	0	0	0	
b0:4e:26:a3:af:08	2	TP-LINK_AP_AF08	11.1	8.7	83	669	156	0	122	0	0	7	Unknown
b0:76:1b:52:87:80	1	Vodafone-528777	0.8	7.6	5	58	2	0	6	0	0	0	Unknown
c8:70:23:1f:a2:70	1	MEO-1FA270	0.6	0.0	0	47	7	0	0	0	0	0	Unknown
c8:70:23:1f:a2:72	1	MEO-WiFi	1.1	11.1	10	80	0	0	1	9	0	0	

Figura 25 - WLAN Traffic

Analisando a figura acima, nomeadamente a coluna *Percent Packets*, escolhemos os seguintes SSIDs: MEO-677760, MEO-WiFi, MEO-9E9BB0 e TP-LINK_AP_AF08.

MEO-9BF2A0

Escolhendo uma trama de cada, obtivemos os seguintes resultados:

```
▸ Frame 10778: 143 bytes on wire (1144 bits), 143 bytes captured (1144 bits) on interface en0, id 0
▸ Radiotap Header v0, Length 36
▾ 802.11 radio information
    PHY type: 802.11g (ERP) (6)
    Short preamble: False
    Proprietary mode: None (0)
    Data rate: 1,0 Mb/s
    Channel: 1
    Frequency: 2412MHz
    Signal strength (dBm): -74dBm
    Noise level (dBm): -93dBm
    Signal/noise ratio (dB): 19dB
    TSF timestamp: 1181997554
  ▸ [Duration: 1048µs]
```

Figura 26 - Trama com SSID = MEO-677760

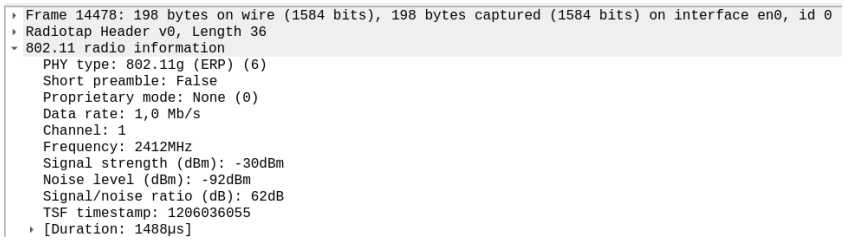


Figura 27 - Trama com SSID = MEO-WiFi

Questão 11 - **Os valores de taxa de transmissão do Wi-Fi estão diretamente associados à qualidade da receção do sinal, utilizando-se dos valores de sensibilidade mínima (Minimum Sensivity) e taxa de transmissão (Data Rate) das tabelas referência do Anexo II, da força do sinal recebido nas tramas do AP indicado da resposta anterior, estime o débito que a STA obterá nessa ligação.**

2.3 Processo de Associação

Questão 12 - **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.**

R: Inicialmente, observamos múltiplas tramas de autenticação trocadas entre as STA e AP.

Especificamente, a trama de **Association Request** mostra a STA enviou um pedido para se associar ao AP, em seguda uma **Association Response** positiva, indica um sucesso na associação.

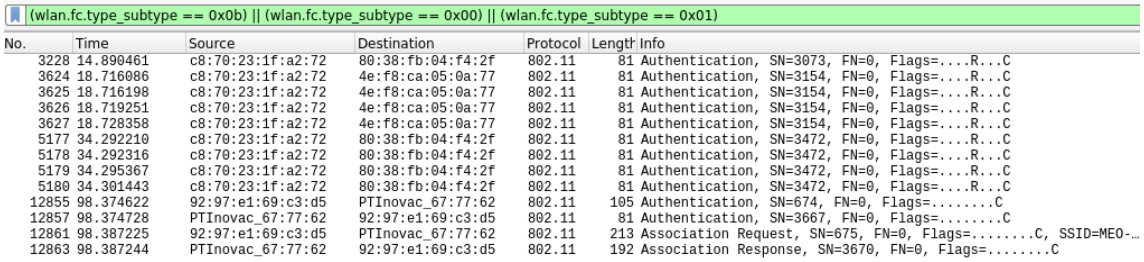


Figura 28

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

R: O diagrama que ilustra a sequência de todas as tramas trocadas que são trocadas no processo é o seguinte:

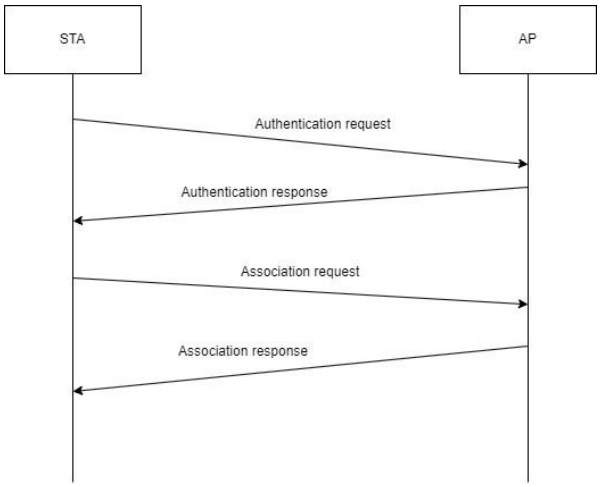


Figura 29

2.4 Transferência de Dados

Questão 14 - **Estabeleça um filtro apropriado e selecione uma trama de dados (Data ou QoS Data), cujo número de ordem inclua o seu identificador de grupo (terminação XX, ou X caso não exista XX). 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?**

R: Aplicamos um filtro para obter Data ou QoS Data **(Wlan.fc.type == 2) && (wlan.fc.subtype == 0 || wlan.fc.subtype == 8)**, o nosso grupo é 60 escolhemos a trama 260**.**

```
(wlan.fc.type == 2) && (wlan.fc.subtype == 0 || wlan.fc.subtype == 8)
No.     Time        Source                Destination           Protocol Length Info
    259 0.677768    PTInovac_67:77:5f     56:5f:07:ef:4f:be     802.11    1390 QoS Data, SN=1931, FN=0, Flags=.p..R.F.C
    260 0.677770    PTInovac_67:77:5f     56:5f:07:ef:4f:be     802.11     739 QoS Data, SN=1932, FN=0, Flags=.p....F.C
    263 0.679174    PTInovac_67:77:5f     56:5f:07:ef:4f:be     802.11     184 QoS Data, SN=1925, FN=0, Flags=.p..R.F.C

▸ Frame 260: 739 bytes on wire (5912 bits), 739 bytes captured (5912 bits) on interface en0, id 0
▸ Radiotap Header v0, Length 58
▸ 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 0011 1100 = Duration: 60 microseconds
    Receiver address: 56:5f:07:ef:4f:be (56:5f:07:ef:4f:be)
    Transmitter address: PTInovac_67:77:60 (00:06:91:67:77:60)
    Destination address: 56:5f:07:ef:4f:be (56:5f:07:ef:4f:be)
    Source address: PTInovac_67:77:5f (00:06:91:67:77:5f)
    BSS Id: PTInovac_67:77:60 (00:06:91:67:77:60)
    STA address: 56:5f:07:ef:4f:be (56:5f:07:ef:4f:be)
    .... .... .... 0000 = Fragment number: 0
    0111 1000 1100 .... = Sequence number: 1932
    Frame check sequence: 0xf0893367 [correct]
    [FCS Status: Good]
  ▸ Qos Control: 0x0000
  ▸ CCMP parameters
▸ Data (643 bytes)
```

Figura 30

Address 1 (Receiver): 56:5f:07:ef:4f:be

Address 2 (Transmitter): 00:06:91:67:77:60

Address 3 (Source): 00:06:91:67:77:5f

Questão 15 - **Para a trama de dados selecionada, 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)?**

Address 1 (Receiver): 56:5f:07:ef:4f:be - STA

Address 2 (Transmitter): 00:06:91:67:77:60 - AP

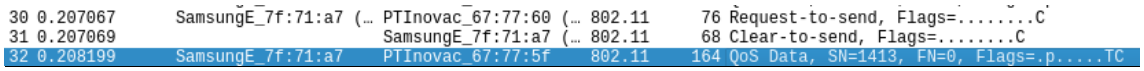
Address 3 (Source): 00:06:91:67:77:5f – router

Questão 16 - **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 envio de dados selecionado 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.**

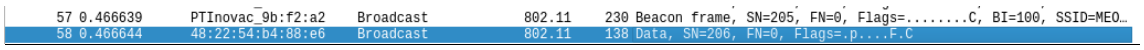
Durante uma transferência de dados em redes sem fios, são utilizadas tramas de controlo do subtipo “Request to Send” e “Clear to Send”. Estas tramas existem para controlar a transmissão de dados pelo meio a fim de evitar colisões. Isso ocorre porque vários dispositivos (STA) podem estar conectados a um ponto de acesso (AP) simultaneamente, e se todos transmitirem dados ao mesmo tempo, haverá colisões de sinais, resultando na corrupção e inutilização dos dados. Para evitar esta perda de eficiência e taxa de transferência, as tramas “Request to Send” e “Clear to Send” foram criadas com o objetivo de organizar e ordenar o envio e transmissão de dados por cada STA. Quando um dispositivo deseja transmitir dados, ele envia uma trama “Request to Send” para o AP, solicitando um “tempo de transmissão”. Se o tempo for permitido e alocado, o AP responde ao dispositivo com a trama “Clear to Send”, indicando que ele pode começar a enviar os dados. Este problema de colisões não é comum em redes Ethernet, especialmente em LANs comutadas, onde cada dispositivo possui um canal de transmissão direto e exclusivo, o que evita colisões. Além disso, vale a pena ressaltar que, numa LAN compartilhada, podem ocorrer colisões de dados, porém o controlo destas colisões é tratado nesses casos.

Exemplos:

Com RTC/CTS


30 0.207067 SamsungE_7f:71:a7 (… PTInovac_67:77:60 (… 802.11 76 Request-to-send, Flags=.....C
31 0.207069 SamsungE_7f:71:a7 (… 802.11 68 Clear-to-send, Flags=.....C
32 0.208199 SamsungE_7f:71:a7 PTInovac_67:77:5f 802.11 164 QoS Data, SN=1413, FN=0, Flags=.p.....TC

Sem RTC/CTS


57 0.466639 PTInovac_9b:f2:a2 Broadcast 802.11 230 Beacon frame, SN=205, FN=0, Flags=.....C, BI=100, SSID=MEO…
58 0.466644 48:22:54:b4:88:e6 Broadcast 802.11 138 Data, SN=206, FN=0, Flags=.p....F.C