TP1: Nível de Ligação Lógica - Ethernet e Protocolo ARP; Redes Sem Fios (IEEE 802.11)

Grupo 15:

- ***Diogo Aires, a91685***
- ***Eduardo Pereira, a70619***
- ***João Silva, a91638***

Parte 1- Nível de Ligação Lógica- Protocolo ARP

3. - Ethernet

Pergunta 1) ***Anote os endereços MAC de origem e de destino da trama capturada.*** -

```
Ethernet II, Src: IntelCor_eb:8f:34 (40:ec:99:eb:8f:34), Dst: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
 > Destination: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
 > Source: IntelCor_eb:8f:34 (40:ec:99:eb:8f:34)
```

Origem: 40:ec:99:eb:8f:34

Destino: 00:d0:03:ff:94:00

Pergunta 2) ***Identifique a que sistemas se referem. Justifique.***

O endereço de origem refere-se à máquina utilizada para fazer a pesquisa. O endereço de destino refere-se à interface do router que pertence à mesma rede IP que a origem.

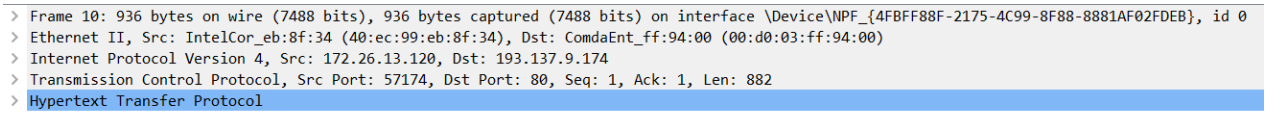
Pergunta 3) ***Qual o valor hexadecimal do campo Type da trama Ethernet? O que significa?***

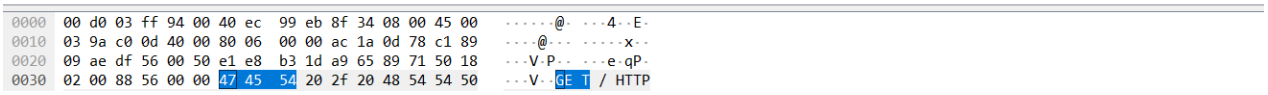
```
Ethernet II, Src: AzureWav_81:c8:ab (48:e7:da:81:c8:ab), Dst: ComdaEnt_ff:94:00 (00:d0:03:
 > Destination: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
 > Source: AzureWav_81:c8:ab (48:e7:da:81:c8:ab)
   Type: IPv4 (0x0800)
```

Type: IPv4 (0x0800)

Significa que a informação a ser transmitida é do tipo de protocolo IP.

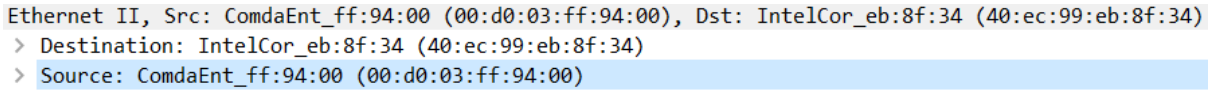
Pergunta 4) ***Quantos bytes são usados desde o início da trama até ao caractere ASCII "G" do método HTTP GET? Calcule e indique, em percentagem, a sobrecarga (overhead) introduzida pela pilha protocolar no envio do HTTP GET (considere o FCS).***





São utilizados 54 bytes desde o início da trama até ao caractere "G". A sobrecarga pode ser determinada, dividindo o número de Bytes usados pelo número total de Bytes. Ou seja: 54/936 que dá aproximadamente 0.06 ou seja o overhead foi de 6%.

Pergunta 5) ***Qual é o endereço Ethernet da fonte? A que sistema de rede corresponde? Justifique.***

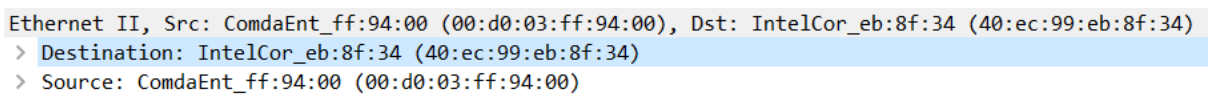


00:d0:03:ff:94:00

O endereço Ethernet da fonte refere-se à interface do router que pertence à mesma rede IP que o destino.

Pergunta 6) ***Qual é o endereço MAC do destino? A que sistema corresponde?***

40:ec:99:eb:8f:34
Corresponde à máquina utilizada para fazer a pesquisa. Neste caso, o nosso computador pessoal.



Pergunta 7) ***Atendendo ao conceito de desencapsulamento protocolar, identifique os vários protocolos contidos na trama recebida.***

```
Ethernet II, Src: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00), Dst: IntelCor_eb:8f:34 (40:ec:99:eb:8f:34)
 > Destination: IntelCor_eb:8f:34 (40:ec:99:eb:8f:34)
 > Source: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
   Type: IPv4 (0x0800)
```

De acordo com o campo Type da trama Ethernet, podemos ver que, dentro, está encapsulado o protocolo IP.

```
Internet Protocol Version 4, Src: 193.137.9.174, Dst: 172.26.13.120
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
   Total Length: 1287
   Identification: 0x25d5 (9685)
 > Flags: 0x40, Don't fragment
   Fragment Offset: 0
   Time to Live: 126
   Protocol: TCP (6)
```

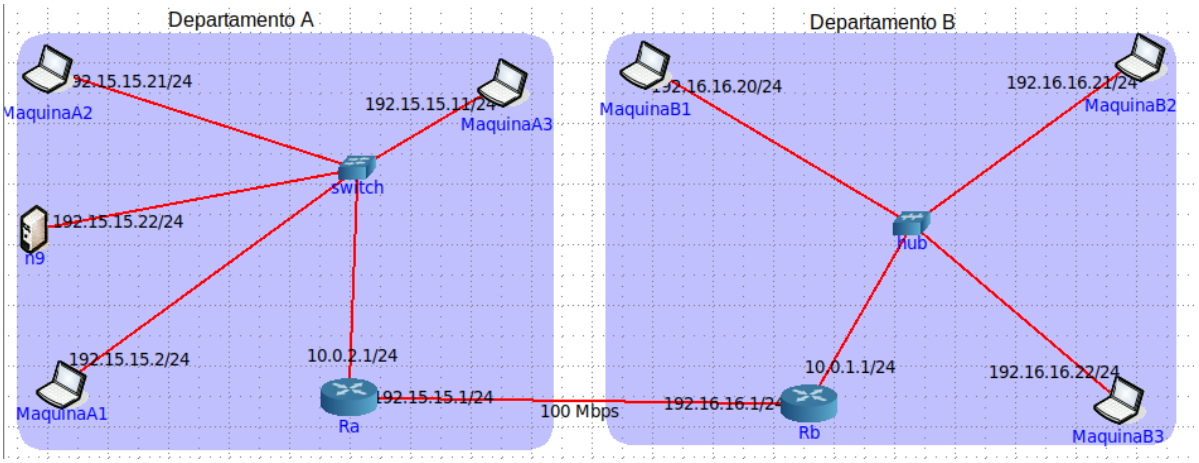
Expandindo a trama IP, tirando o cabeçalho, podemos ver, no campo Protocol, que está encapsulado o protocolo TCP(6).

Tirando o cabeçalho tcp, vemos que está encapsulado o protocolo HTTP.

```
Transmission Control Protocol, Src Port: 80, Dst Port: 56932, Seq: 42501, Ack: 883, Len: 1247
   Source Port: 80
   Destination Port: 56932
```

De acordo com a imagem acima, a porta da origem, no protocolo TCP, é a porta 80.

4. PROTOCOLO ARP



Todo o desenvolvimento da parte “Protocolo ARP” foi feito a partir destes dois departamentos criados.

O Departamento A:

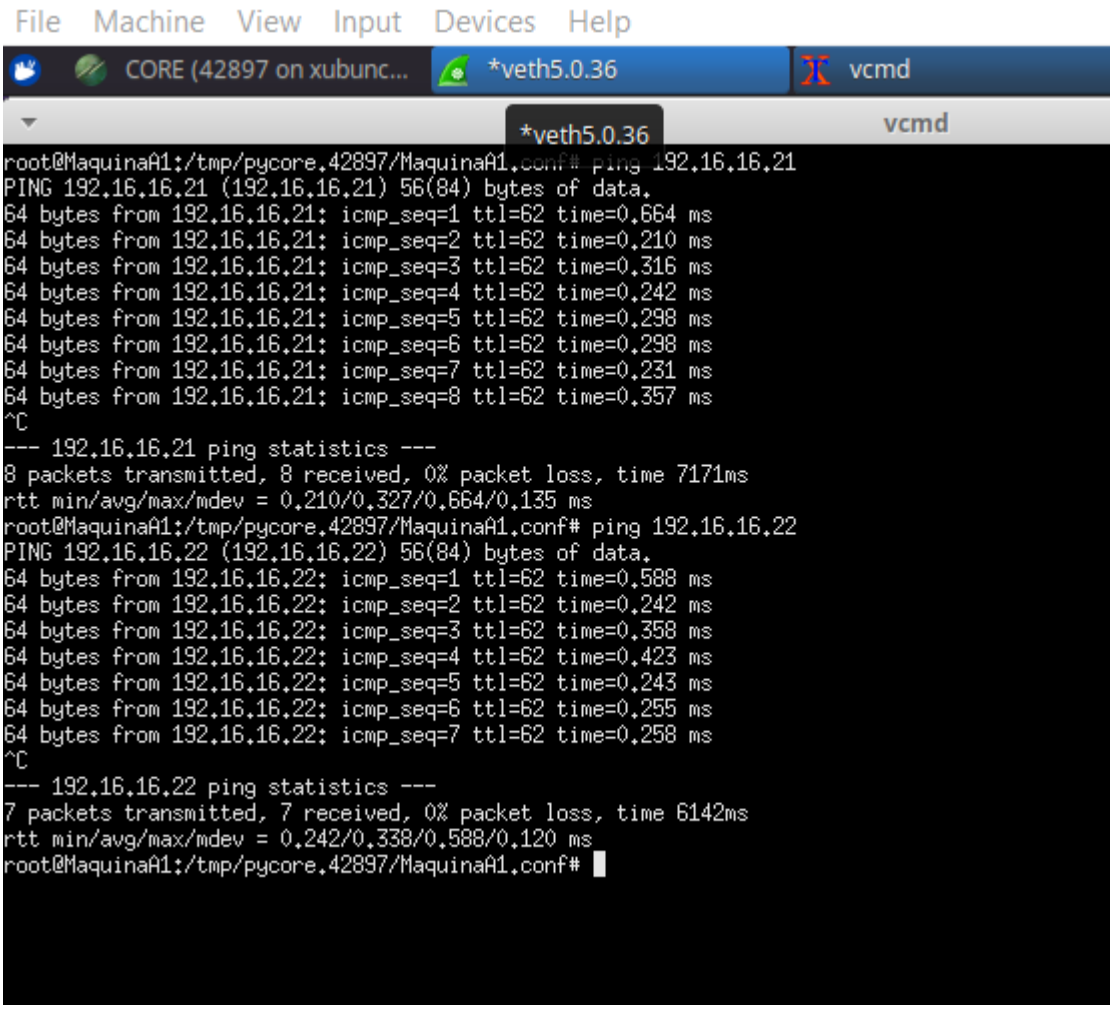
- 3 hosts
- 1 servidor
- 1 switch
- 1 router

O Departamento B:

- 3 hosts
- 1 hub
- 1 router

Pergunta 8) ***Abra uma consola no host onde efetuou o ping. Observe o conteúdo da tabela ARP com o comando arp.***

O ping foi feito a partir da MaquinaA1 (inserido no Departamento A, com IP - 192.15.15.22) para a MaquinaB2 e MaquinaB3 (inseridas no Departamento B com IP's, respetivamente - 192.16.16.21 e 192.16.16.22)



Queremos ver agora a tabela arp.
No mesmo vcmd, utilizando o comando "arp" obtivemos:

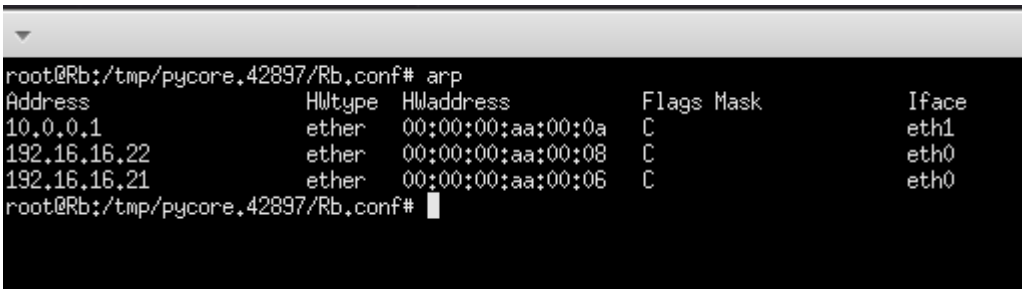
a)Com a ajuda do manual arp (man arp), interprete o significado de cada uma das colunas da tabela.

A Tabela ARP é uma estrutura que mantém os mais recentes mapeamentos de endereço de IP´s em endereços físicos.

Após efetuados os pings e verificada a tabela arp, vemos que nesta tabela encontramos as seguintes colunas:

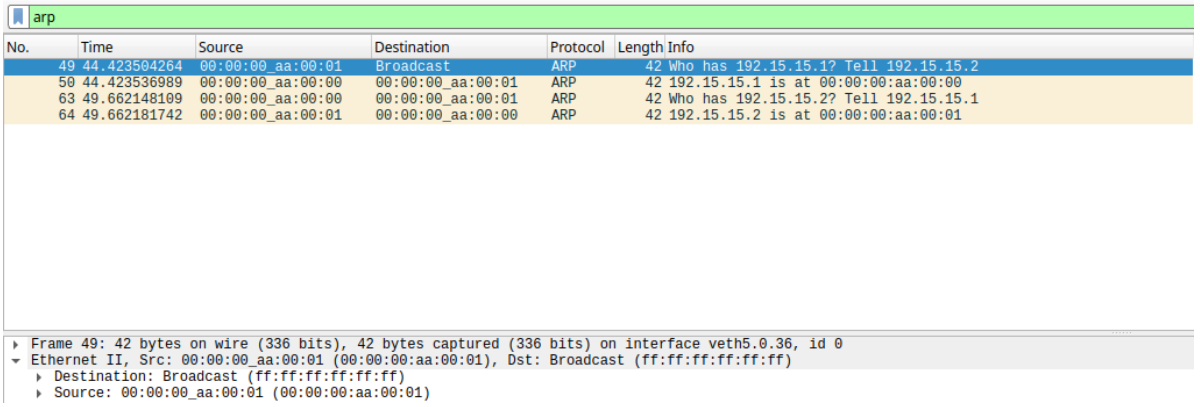
- *Address* : endereço de IP do router Ra, para onde foi enviado o ping
- *HWtype* : indica quais classes de entrada deve procurar(neste caso ether - ethernet)
- *HWaddress* : MAC address do router (Ra) do departamento onde foi efetuado o ping
- *Flags Mask* : C = este tipo de entrada é visto quando as entradas são automaticamente introduzidas na tabela, através do protocolo ARP.
- *IFace* : especifica a qual interface o par de endereços IP e MAC deve ser associado (neste caso, ether(0)).

b)Indique, justificando, qual o equipamento da intranet em causa que poderá apresentar a maior tabela ARP em termos de número de entradas.



Como podemos ver, o router Rb, é o equipamento da intranet que apresenta a maior tabela de arp. Isto, pois está conectado ao router Ra (router do Departamento A, de onde veio o ping, efetuado por uma máquina ligado a este mesmo router) e daí parte para as máquinas para onde o ping foi mandado (Máquina B2 e Máquina B3), máquinas estas que estão ligadas a este router Rb (do Departamento B).

Pergunta 9) ***Qual é o valor hexadecimal dos endereços origem e destino na trama Ethernet que contém a mensagem com o pedido ARP (ARP Request)? Como interpreta e justifica o endereço destino usado?***



Source: 00:00:00:aa:00:01
Destination: Broadcast (ff:ff:ff:ff:ff:ff)

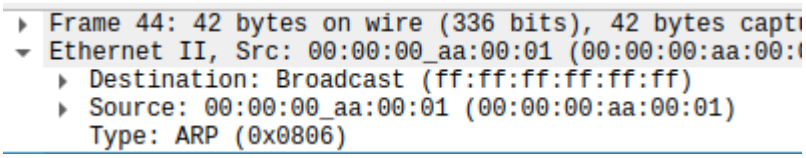
O endereço do destino usado (Broadcast (ff:ff:ff:ff:ff:ff)) porque neste ponto, a origem não conhece o MAC address destinatário e, deste modo, não consegue enviar um pedido unicast.
Assim, todas as máquinas na mesma rede recebem o pedido ARP.

(ff:ff:ff:ff:ff:ff) representa o Ethernet Broadcast address.

Pergunta 10) ***. Qual o valor hexadecimal do campo tipo da trama Ethernet? O que indica?***

wireshark - ETHERNET - TYPE - ARP (0X0806)

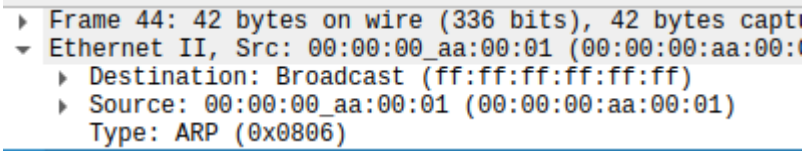
Indica que protocolo está a ser encapsulado, neste caso ARP.



Pergunta 11) ***Como pode confirmar que se trata efetivamente de um pedido ARP? Identifique que tipo de endereços estão contidos na mensagem ARP? O que conclui?***

O EtherType, que neste caso contém o valor hexadecimal 0X0806, indica que está a ser efetuado um pacote ARP.

Os endereços contidos na mensagem são referentes aos MAC address da Máquina A1 (origem/source) e como não sabe o MAC address do destino do "ping" o campo é preenchido com ff:ff:ff:ff:ff:ff (destination) - neste caso, o MAC address pretendido é o da Máquina B2 (primeiro ping).



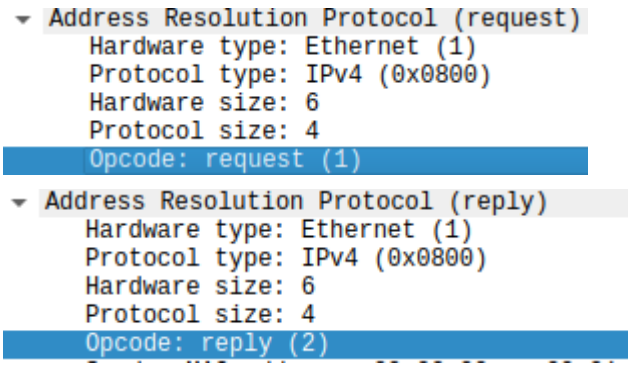
Pergunta 12) ***Explicite que tipo de pedido ou pergunta é feita pelo host de origem?***

O host de origem pretende saber o MAC address correspondente ao IP para onde foi enviado o ping.

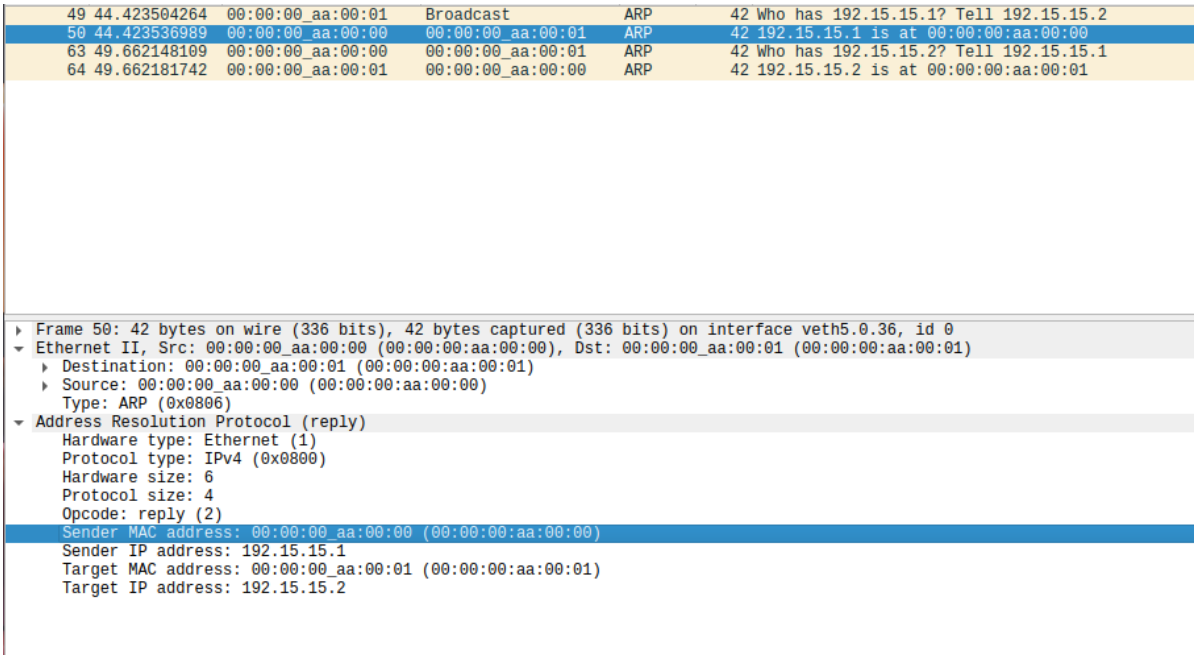
Pergunta 13) ***Localize a mensagem ARP que é a resposta ao pedido ARP efetuado.***

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

Se o valor do campo opcode do ARP for (1) é referente ao pedido (request).
Se o valor do campo opcode do ARP for (2) é referente à resposta (reply).



b) Em que posição da mensagem ARP está a resposta ao pedido ARP?



A posição da resposta da mensagem ARP : 00:00:00:aa:00:00

c) A resposta ARP é enviada em broadcast? Justifique o modo de envio usado na resposta ARP.

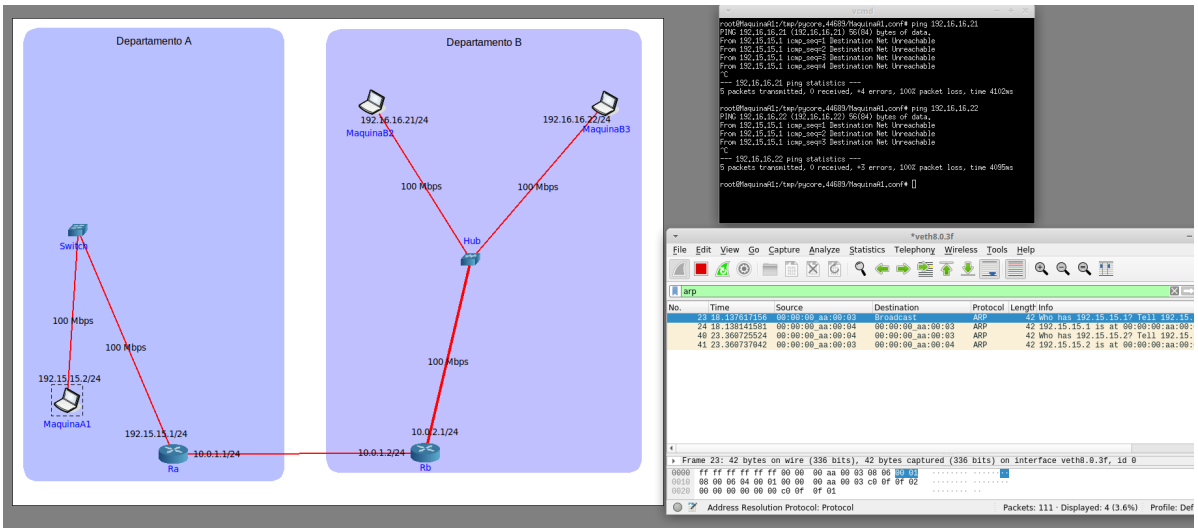
Não. A mensagem (ARP request) é enviada em unicast, de uma máquina A para uma máquina B, guardando assim o MAC address da origem na tabela ARP.
Quando é enviada a ARP reply (da máquina B para a máquina A), já é conhecido o MAC address da máquina A (dispositivo origem do protocolo).

Pergunta 14) Verifique se o ping feito ao segundo host originou pacotes ARP e justifique a situação observada.

Não.
Com o primeiro ARP request, enviado em broadcast, a tabela ARP da máquina origem é preenchida com o IP e MAC address do router (Ra) onde a mensagem será então transmitida (para o router Rb e daí parte para a máquina destino).
No segundo ping, onde o processo é o mesmo, mas na tabela ARP (da máquina origem) já se encontra o IP e MAC address pretendido (do router Ra), logo, não são efetuados/originados pacotes ARP, pois a máquina procura primeiro se o endereço na tabela já existe (como neste caso) e trabalha a partir daí. Caso contrário, são originados novos pacotes ARP.

Pergunta 15) ***Apresente um esquema apenas com as máquinas envolvidas no envio do pedido ping desde a origem até ao destino, bem como os endereços IP e MAC das respectivas interfaces de rede, podendo para tal recorrer ao comando ifconfig. Represente nesse esquema as tramas com os pedidos e respostas ARP geradas ao longo da rota pelo envio do pedido ping. Indique para cada trama os endereços MAC origem e destino presentes no cabeçalho Ethernet, bem como os endereços Sender MAC, Sender IP, Target MAC e Target IP presentes no pacote ARP. Assinale com uma seta o sentido de cada pacote e com um número a ordem de sequência dos pacotes. Considere todas as tabelas ARP vazias no momento em que se fez o ping. Ignore a situação da resposta ao pedido ping.***

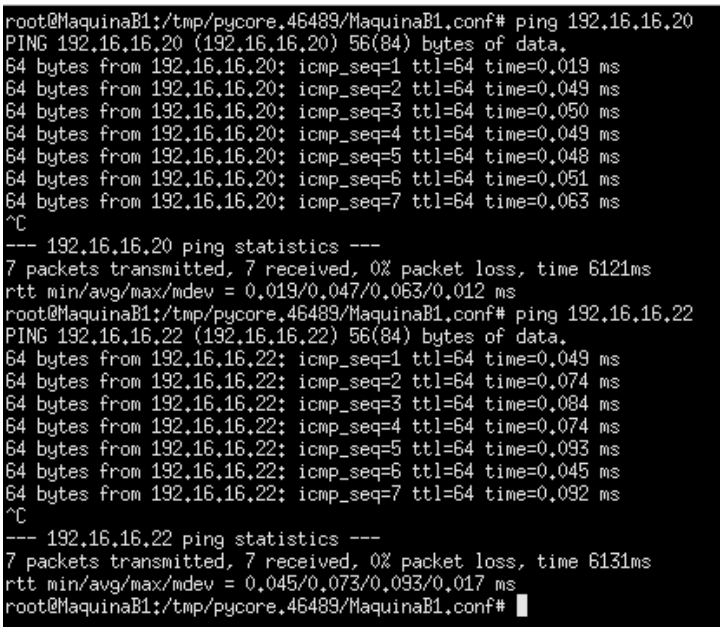
O esquema das máquinas envolvidas no envio do ping, pode ser representado: (ao lado do esquema apresento a tabela ARP e também o envio do ping a partir da MáquinaA1)

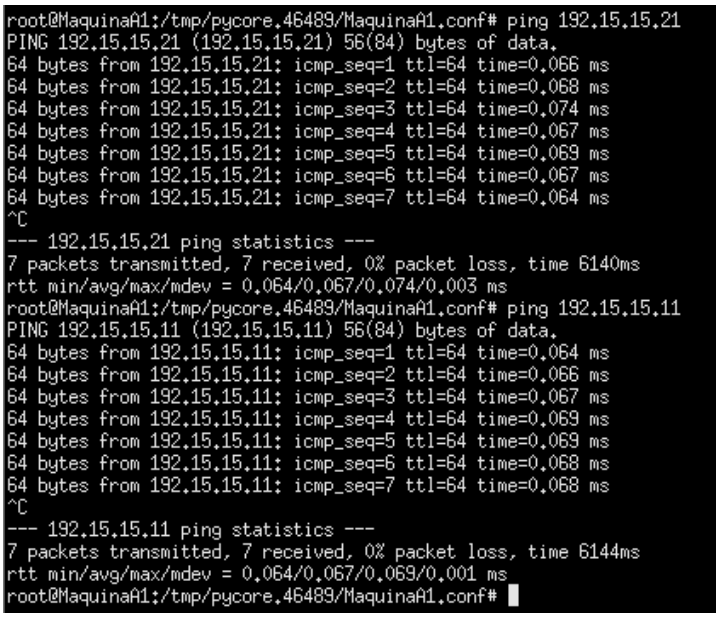


5. Domínios de Colisão

Pergunta 16) ***Através da opção tcpdump, verifique e compare como flui o tráfego nas diversas interfaces dos vários dispositivos no departamento A (LAN comutada) e no departamento B (LAN partilhada) quando gera tráfego intra-departamento (por exemplo, através do comando ping). Que conclui?***

O tráfego gerado no Departamento A foi feito através do envio de uma mensagem “ping” da Máquina A1 para as máquinas, respetivamente, A2 e A3.
O tráfego gerado no Departamento B foi feito através do envio de uma mensagem “ping” da Máquina B1 para as máquinas, respetivamente, B2 e B3.

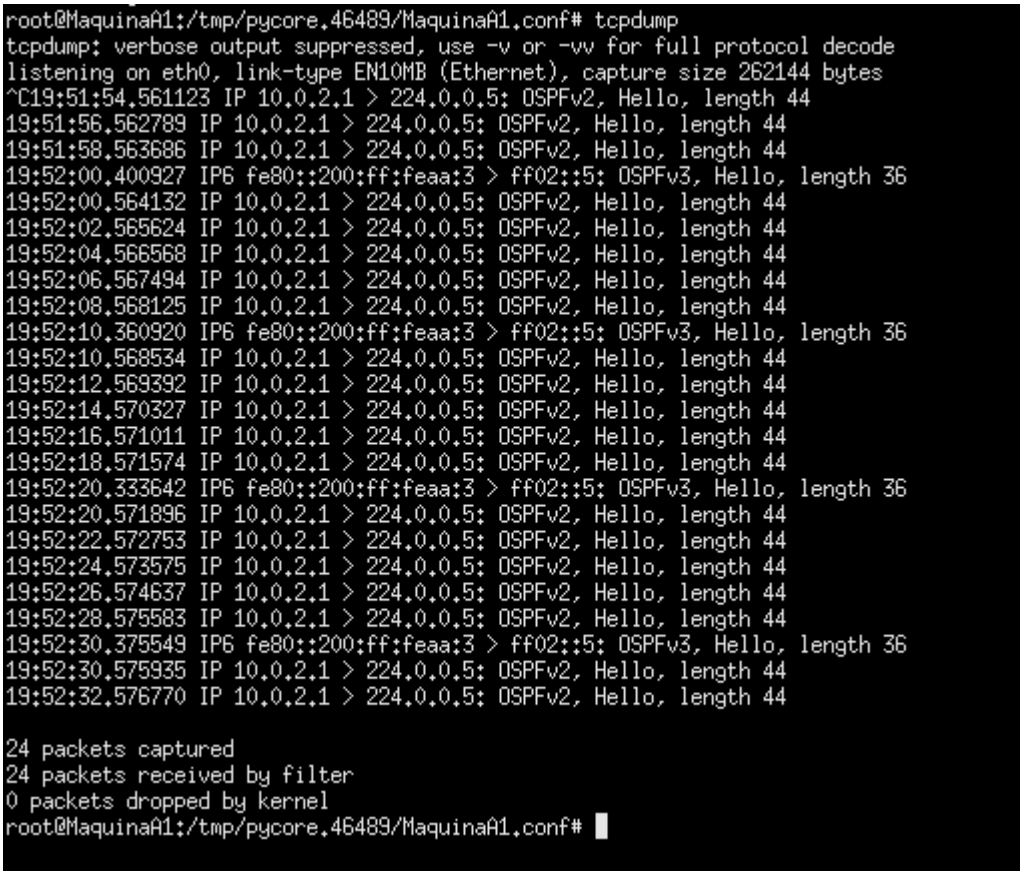


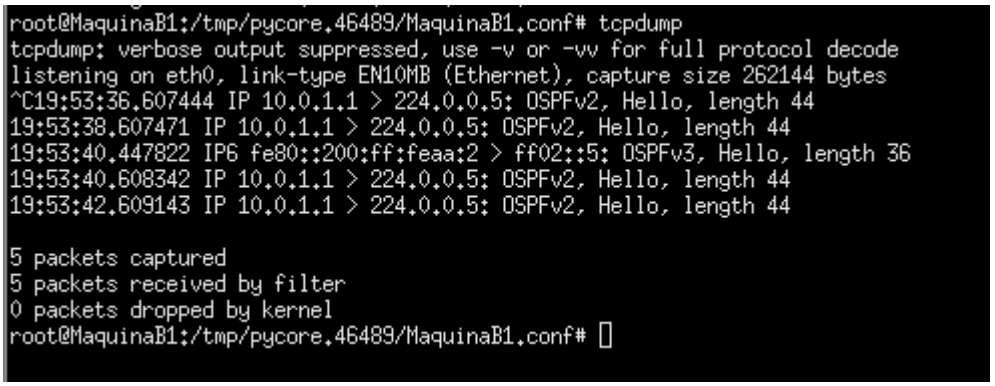


Gerado o tráfico, queremos agora ver como este flui, através do comando *tcpdump*.

Conseguimos facilmente perceber que o tráfego flui muito mais facilmente, isto é, de forma mais rápida no Departamento A que no Departamento B.

Conseguimos concluir então que a Ethernet comutada tem muitas vantagens sobre a Ethernet partilhada.
Feitas algumas pesquisas, uma das maiores vantagens são maior largura de banda e cabeamento simplificado. Mas a maior vantagem é restringir os domínios de colisão, o que causa menos colisão no meio compartilhado causando uma melhor performance na rede.





Parte 2 - Redes Sem Fios (IEEE 802.11)

3. Acesso Rádio

Wireshark · Packet 414 · trace-wlan-tp4.pcap

```
Frame 414: 205 bytes on wire (1640 bits), 205 bytes captured (1640 bits)
Radiotap Header v0, Length 25
802.11 radio information
IEEE 802.11 Beacon frame, Flags: ........C
IEEE 802.11 Wireless Management
```

Estamos a analisar a trama 414 (correspondente ao grupo número 15, a trama 415 era muito genérica e não tinha as informações requeridas).

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

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

A rede está a operar no espectro dos 2 GHz sendo que a frequência do canal é de 2467 MHz. Esta frequência corresponde ao canal 12.

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

```
802.11 radio information
   PHY type: 802.11b (HR/DSSS) (4)
```

```
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
```

A versão que está a ser usada é a versão IEEE 802.11b. O tipo é 00 correspondente a *Management*, o subtipo é 8 (1000) que corresponde a *Beacon*.

Pergunta 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.***

```
802.11 radio information
    PHY type: 802.11b (HR/DSSS) (4)
    Short preamble: False
    Data rate: 1,0 Mb/s
```

Norma	Ano	Velocidade Máxima	Frequência
IEEE 802.11b	1999	11 Mbps	2,4 GHz

A trama 414 foi enviada com um débito de 1Mb/s. A versão 802.11b da norma IEEE 802.11 fornece um débito de até 11Mb/s, por isso o débito da trama escolhida não corresponde ao máximo a que a interface pode operar.

4. Scanning Passivo e Scanning Ativo

Wireshark · Packet 14 · trace-wlan-tp4.pcap

```
Frame 14: 205 bytes on wire (1640 bits), 205 bytes captured (1640 bits)
Radiotap Header v0, Length 25
802.11 radio information
IEEE 802.11 Beacon frame, Flags: ........C
IEEE 802.11 Wireless Management
```

Estamos a analisar a trama 14 (correspondente ao grupo número 15, a trama 15 era muito genérica e não tinha as informações requeridas).

Pergunta 4) ***Selecione a trama beacon 14. 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?***

```
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
```

Esta trama pertence ao tipo *Beacon Frame*. O valor do seu identificador de tipo é 00 correspondente a uma trama de *Management* e o valor do seu subtipo é 1000 (8) correspondente a *Beacon*.

O tipo e o subtipo da trama 14 estão descritos no Campo de Controlo da Trama.

Pergunta 5) ***Para a trama acima, identifique todos os endereços MAC em uso. Que conclui quanto à sua origem e destino?***

```
IEEE 802.11 Beacon frame, Flags: ........C
   Type/Subtype: Beacon frame (0x0008)
 > Frame Control Field: 0x8000
   .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:b1:99 (bc:14:01:af:b1:99)
   Source address: HitronTe_af:b1:99 (bc:14:01:af:b1:99)
   BSS Id: HitronTe_af:b1:99 (bc:14:01:af:b1:99)
```

Os endereços MAC em uso para a trama 14 são o Endereço Origem (bc:14:01:af:b1:99) e Destino (ff:ff:ff:ff:ff:ff).

O endereço Origem é o endereço MAC de quem faz o pedido.
Um endereço IP de broadcast para uma rede necessita de um endereço MAC de broadcast correspondente no quadro Ethernet. Em redes Ethernet, este endereço MAC tem todos os bits a 1 em cada octeto, o que se representa em hexadecimal como ff. O endereço MAC de broadcast são 48 bits a 1, daí vem o endereço ff:ff:ff:ff:ff:ff.

Pergunta 6) ***Qual é o intervalo de tempo previsto entre tramas beacon consecutivas? Na prática, a periodicidade de tramas beacon provenientes do mesmo AP é verificada com precisão? Justifique.***

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"
10	0.411376	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2092, FN=0, Flags=........C, BI=100, SSID="NOS_WIFI_Fon"
11	0.512117	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2093, FN=0, Flags=........C, BI=100, SSID="FlyingNet"
12	0.513707	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2094, FN=0, Flags=........C, BI=100, SSID="NOS_WIFI_Fon"
13	0.614562	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2095, FN=0, Flags=........C, BI=100, SSID="FlyingNet"
14	0.616191	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2096, FN=0, Flags=........C, BI=100, SSID="NOS_WIFI_Fon"

O intervalo de tempo previsto entre tramas *beacon* consecutivas é 100 ms. A periodicidade das tramas beacon não é precisa, pois a diferença entre cada tempo de envio não é igual à medida que o processo avança. Por exemplo, de 0 para 1, a diferença de tempo é de 1,662 ms, porém, entre 1 e 2, é de 10,089 ms.

Pergunta 7) ***Identifique e liste os SSIDs dos APs que estão a operar na vizinhança da STA de captura? Explicite o modo como obteve essa informação.***

```
IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  v Tagged parameters (231 bytes)
    v Tag: SSID parameter set: "FlyingNet"
        Tag Number: SSID parameter set (0)
        Tag length: 9
        SSID: "FlyingNet"
```

```
IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  v Tagged parameters (140 bytes)
    v Tag: SSID parameter set: "NOS_WIFI_Fon"
        Tag Number: SSID parameter set (0)
        Tag length: 12
        SSID: "NOS_WIFI_Fon"
```

Se expandirmos os campos dos parâmetros SSIDs, os SSIDs a operar na vizinhança da STA são “FlyingNet” e “NOS_WIFI_FON”.

Pergunta 8) ***Identifique um probing request para o qual tenha havido um probing response.***
Face ao endereçamento usado, indique a que sistemas são endereçadas ambas as tramas e explique qual o propósito das mesmas.

```
  6264 94.724102    Apple_28:b8:0c    Broadcast         802.11    146 Probe Request, SN=0, FN=0, Flags=........, SSID="FlyingNet"
  6265 94.735334    Apple_28:b8:0c    Broadcast         802.11    146 Probe Request, SN=0, FN=0, Flags=........, SSID="FlyingNet"
 17047 123.056614   Apple_28:b8:0c    Broadcast         802.11    152 Probe Request, SN=0, FN=0, Flags=........, SSID="FlyingNet"
 17048 123.058579   HitronTe_af:b1:98 Apple_28:b8:0c    802.11    411 Probe Response, SN=2602, FN=0, Flags=........C, BI=100, SSID="FlyingNet"
 17049 123.059374   HitronTe_af:b1:98 Apple_28:b8:0c    802.11    411 Probe Response, SN=2603, FN=0, Flags=........C, BI=100, SSID="FlyingNet"
 17050 123.060076   HitronTe_af:b1:98 Apple_28:b8:0c    802.11    411 Probe Response, SN=2604, FN=0, Flags=........C, BI=100, SSID="FlyingNet"
 17051 123.067827   Apple_28:b8:0c    Broadcast         802.11    152 Probe Request, SN=0, FN=0, Flags=........, SSID="FlyingNet"
 17052 123.069745   HitronTe_af:b1:98 Apple_28:b8:0c    802.11    411 Probe Response, SN=2605, FN=0, Flags=........C, BI=100, SSID="FlyingNet"
 17053 123.070516   HitronTe_af:b1:98 Apple_28:b8:0c    802.11    411 Probe Response, SN=2606, FN=0, Flags=........C, BI=100, SSID="FlyingNet"
 17054 123.071161   HitronTe_af:b1:98 Apple_28:b8:0c    802.11    411 Probe Response, SN=2607, FN=0, Flags=........C, BI=100, SSID="FlyingNet"
 17055 123.081118   Apple_28:b8:0c    Broadcast         802.11    152 Probe Request, SN=0, FN=0, Flags=........, SSID="FlyingNet"
 17057 123.091464   Apple_28:b8:0c    Broadcast         802.11    152 Probe Request, SN=0, FN=0, Flags=........, SSID="FlyingNet"
```

```
rame 17047: 152 bytes on wire (1216 bits), 152 bytes captured (1216 bits)
adiotap Header v0, Length 25
02.11 radio information
EEE 802.11 Probe Request, Flags: ........
  Type/Subtype: Probe Request (0x0004)
> Frame Control Field: 0x4000
  .000 0000 0000 0000 = Duration: 0 microseconds
  Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
  Transmitter address: Apple_28:b8:0c (68:a8:6d:28:b8:0c)
  Source address: Apple_28:b8:0c (68:a8:6d:28:b8:0c)
  BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
```

```
0000  00 00 19 00 0f 00 00 00  86 d3 83 08 00 00 00 00   ........ ........
0010  00 02 a3 09 80 00 00 00  90 40 00 00 00 ff ff ff   ........ .@......
0020  ff ff ff 68 a8 6d 28 b8  0c ff ff ff ff ff ff 00   ...h.m(. ........
0030  00 00 09 46 6c 79 69 6e  67 4e 65 74 01 04 02 04   ...Flyin gNet....
0040  0b 16 32 08 0c 12 18 24  30 48 60 6c 03 01 0c 2d   ..2....$ 0H`l...-
0050  1a ad 19 1b ff ff ff 00  00 00 00 00 00 00 00 00   ........ ........
0060  00 00 00 00 00 00 00 00  00 00 00 dd 0b 00 17 f2   ........ ........
0070  0a 00 01 04 00 00 00 00  dd 1e 00 90 4c 33 ad 19   ........ ....L3..
0080  1b ff ff ff 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0090  00 00 00 00 00 00 00 00                           ........
```

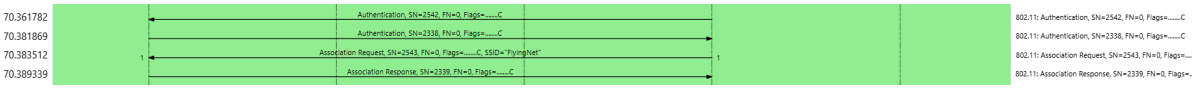
Uma estação envia um pedido (probing request) em broadcast para descobrir que redes existem nas suas proximidades.
O AP, responde, com informações relativas ao mesmo, através do probing response.

5. Processo de Associação

Pergunta 9) ***Identifique uma sequência de tramas que corresponda a um processo de associação completo entre a STA e o AP, incluindo a fase de autenticação.***

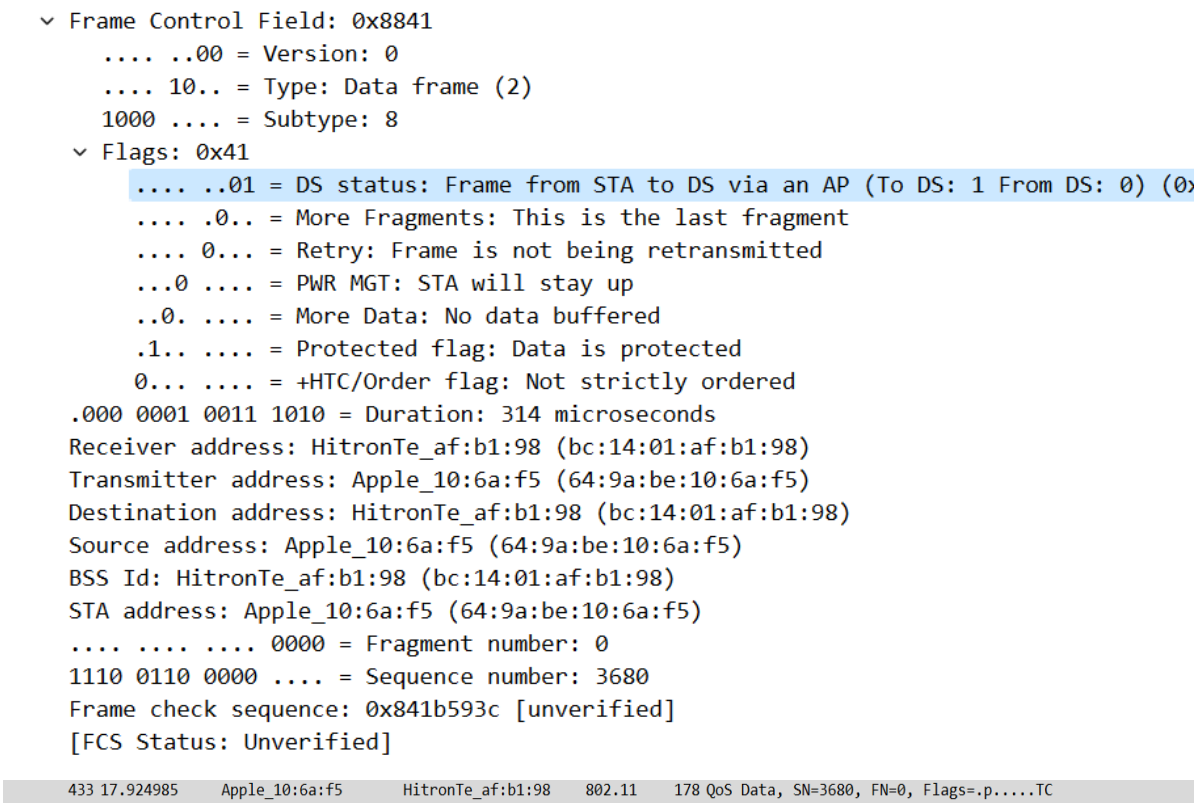
2486	70.361782	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	70	Authentication, SN=2542, FN=0, Flags=........C
2487	70.362050		Apple_10:6a:f5 (64:…	802.11	39	Acknowledgement, Flags=........C
2488	70.381869	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	59	Authentication, SN=2338, FN=0, Flags=........C
2489	70.381878		HitronTe_af:b1:98 (…	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 (64:…	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 (…	802.11	39	Acknowledgement, Flags=........C

Pergunta 10) ***Efetue um diagrama que ilustre, com as tramas identificadas na alínea anterior, a sequência de todas as tramas trocadas no processo de autenticação e associação entre o STA e o AP.***



6. Transferência de Dados

Pergunta 11) ***Considere a trama de dados nº 433. Sabendo que o campo Frame Control contido no cabeçalho das tramas 802.11 permite especificar a direcionalidade das tramas, o que pode concluir face à direcionalidade dessa trama? Será local à WLAN?***



Como podemos ver no campo DS Status, verificando (To DS: 1 From DS: 0), conseguimos concluir que a Wireless Data Frame está a ser enviada de um cliente móvel para uma rede “com fios”, ou seja, vem do STA para o DS.

Pergunta 12) ***Para a trama de dados da alínea anterior, 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.***

host sem fios (STA): bc:14:01:af:b1:98
AP: 64:9a:be:10:6a:f5
router de acesso: bc:14:01:af:b1:98

```
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)
```

Pergunta 13) ***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.***

```
433 17.924985    Apple_10:6a:f5       HitronTe_af:b1:98    802.11    178 QoS Data, SN=3680, FN=0, Flags=.p.....TC
434 17.925298                         Apple_10:6a:f5 (64:… 802.11     39 Acknowledgement, Flags=........C
435 17.927587    Apple_28:b8:0c       HitronTe_af:b1:98    802.11     49 Null function (No data), SN=0, FN=0, Flags=.......T
436 17.927618                         Apple_28:b8:0c (68:… 802.11     39 Acknowledgement, Flags=........C
```

São transmitidas tramas do tipo “acknowledgement”.
Estas mesmas, indicam que a transmissão foi efetuada com sucesso.

Pergunta 14) ***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. Dê um exemplo de uma transferência de dados em que é usada a opção RTC/CTS e um outro em que não é usada, identificando a direcionalidade das tramas e os sistemas envolvidos.***

```
10819 106.296237    HitronTe_af:b1:98 (… Apple_10:6a:f5 (64:… 802.11     45 Request-to-send, Flags=........C
10820 106.296241                         HitronTe_af:b1:98 (… 802.11     39 Clear-to-send, Flags=........C
10821 106.296295    Apple_10:6a:f5 (64:… HitronTe_af:b1:98 (… 802.11     57 802.11 Block Ack, Flags=........C
10822 106.297263    Apple_10:6a:f5       HitronTe_af:b1:96    802.11    160 QoS Data, SN=25, FN=0, Flags=.p.....TC
10823 106.297278                         Apple_10:6a:f5 (64:… 802.11     39 Acknowledgement, Flags=........C
```

Na transferência de dados acima, é usada a opção de RTS/CTS.

```
433 17.924985    Apple_10:6a:f5       HitronTe_af:b1:98    802.11    178 QoS Data, SN=3680, FN=0, Flags=.p.....TC
434 17.925298                         Apple_10:6a:f5 (64:… 802.11     39 Acknowledgement, Flags=........C
435 17.927587    Apple_28:b8:0c       HitronTe_af:b1:98    802.11     49 Null function (No data), SN=0, FN=0, Flags=.......T
436 17.927618                         Apple_28:b8:0c (68:… 802.11     39 Acknowledgement, Flags=........C
```

Na transferência de dados acima, não é usada a opção de RTS/CTS.

Conclusão

Após a realização deste trabalho, juntamente com a “teoria” dada nas aulas teóricas, todos os temas abordados acima, desde o Protocolo ARP até à Transferência de Dados, tornaram-se, de certa forma, mais fáceis de entender.
A abordagem ao Wireshark foi notoriamente útil para o desenvolvimento deste projeto. Ajudou-nos a perceber como as wireless networks (por exemplo) funcionam, juntamente com as tramas de ethernet, entre outros.