Universidade do Minho

Braga, Portugal

TRABALHO PRÁTICO 3 - RELATÓRIO

Redes Ethernet, Protocolo ARP e WiFi

Redes de Computadores

Departamento de Informática

Engenharia Informática 2024/25

Grupo 69:

Duarte Escairo Brandão Reis Silva

Pedro Emanuel Organista Silva

Tiago Silva Figueiredo

Maio 2025

Índice

1. Parte 1 1
   1.1. Captura e análise de Tramas Ethernet 1
      1.1.1. 1
      1.1.2. 1
      1.1.3. 1
      1.1.4. 2
      1.1.5. 2
   1.2. Protocolo ARP e Domínios de Colisão 2
      1.2.1. 2
      1.2.2. 2
      1.2.3. 3
      1.2.4. 5
      1.2.5. 5
      1.2.6. 5
      1.2.7. 6
      1.2.8. 7
   1.3. 7
2. Parte 2 8
   2.1. 8
   2.2. 8
   2.3. 9
   2.4. 9
   2.5. 10
   2.6. 10
   2.7. 10
   2.8. 11
   2.9. 12
   2.10. 13
   2.11. 14
   2.12. 14
   2.13. 14
   2.14. 15
   2.15. 16
   2.16. 17
3. Conclusão 18

1. Parte 1

1.1. Captura e análise de Tramas Ethernet

1.1.1.

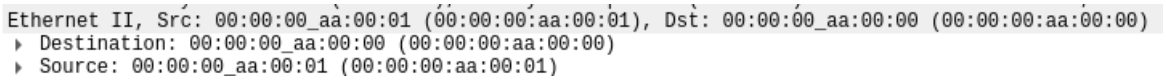
Anote os endereços MAC de origem e MAC destino da trama capturada. Identifique a que hosts se referem. Justifique.

RESPOSTA:

Os endereços MAC origem e destino são os seguintes:

MAC origem: 00:00:00:aa:00:01 -> identifica a Jasmine

MAC destino: 00:00:00:aa:00:00 -> identifica o router R1



O IP é um endereço lógico, enquanto que o MAC é um endereço físico. Ao enviar um pacote, o IP destino mantém-se, contudo o MAC identifica apenas o próximo nó. Neste caso em concreto, o próximo nó é o router R1, daí o MAC destino ser o dele.

1.1.2.

Qual o valor hexadecimal do campo Type contido no header da trama Ethernet? O que significa? Qual o campo do header IP que tem semântica idêntica?

RESPOSTA:

O campo Type numa trama Ethernet indica a camada protocolar acima, então neste caso, como o valor hexadecimal é 0x0800, indica que a camada protocolar acima é IPv4. O campo do header IP que tem semântica idêntica é o protocol.

1.1.3.

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.

RESPOSTA:

Bytes usados no encapsulamento protocolar:

Ethernet -> 14 bytes (default)

IP -> 20 bytes (default)

TCP -> 32 bytes (20 + 12 options)

Total: $14 + 20 + 32 = 66$ bytes

Percentagem de overhead: $\frac{66}{110} * 100 = 60\%$

(O valor 110 corresponde ao tamanho total do frame)

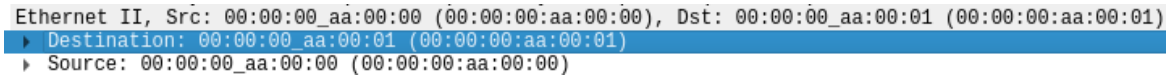
1.1.4.

Qual é o endereço MAC da fonte? A que host e interface corresponde? Justifique

RESPOSTA:

Endereço MAC da fonte: 00:00:00:aa:00:00

Identifica o router R1



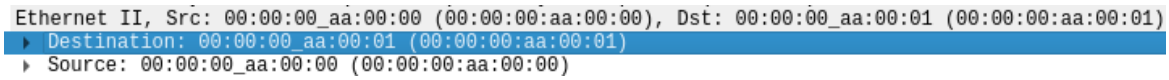
1.1.5.

Qual é o endereço MAC do destino? A que host e interface corresponde?

RESPOSTA:

Endereço MAC do destino: 00:00:00:aa:00:01

Identifica a Jasmine



1.2. Protocolo ARP e Domínios de Colisão

1.2.1.

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

RESPOSTA:

A primeira coluna representa o nome do dispositivo, a segunda o endereço IP, a terceira o MAC address e a última a porta onde este dispositivo se conecta a ele.

```
root@Aladdin:/tmp/pycore.40961/Aladdin.conf# arp -a
? (10.0.0.1) at 00:00:00:aa:00:00 [ether] on eth0
```

1.2.2.

Observe a trama Ethernet que contém a mensagem com o pedido ARP (ARP Request).

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

RESPOSTA:

MAC origem: 00:00:00:aa:00:02 -> Aladdin

MAC destino: ff:ff:ff:ff:ff:ff -> Broadcast

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

Como o Aladdin não sabe num primeiro momento para quem deve enviar os pacotes, de forma a que estes cheguem ao seu destino que é o servidor, é enviado um ARP request (em broadcast), para que no reply o Alladin passe a conhecer a quem deve enviar os pacotes

b) Qual o valor hexadecimal do campo Type da trama Ethernet? O que indica?

RESPOSTA:

O campo Type numa trama Ethernet indica a camada protocolar acima, então neste caso, como o valor hexadecimal é 0x0806, indica que a camada protocolar acima é ARP.

```
Type: ARP (0x0806)
```

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

RESPOSTA:

O opcode da trama Ethernet indica que se trata de um request (pedido), o destino ser broadcast também é um indicador que se trata de um pedido, e ainda como o TARGET MAC address está a 0, isso significa que também estamos perante um pedido.

```
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 ▸ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
 ▸ Source: 00:00:00_aa:00:02 (00:00:00:aa:00:02)
   Type: ARP (0x0806)
Address Resolution Protocol (request)
   Hardware type: Ethernet (1)
   Protocol type: IPv4 (0x0800)
   Hardware size: 6
   Protocol size: 4
   Opcode: request (1)
   Sender MAC address: 00:00:00_aa:00:02 (00:00:00:aa:00:02)
   Sender IP address: 10.0.0.21
   Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
   Target IP address: 10.0.0.1
```

1.2.3.

Localize a mensagem ARP que é a resposta ao pedido ARP efetuado.

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

RESPOSTA:

O valor do campo ARP opcode tem valor 2, e especifica que se trata de uma resposta (reply).

```
Opcode: reply (2)
```

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

RESPOSTA:

A resposta está no campo Sender MAC address, e vem com o valor 00:00:00:aa:00:00.

```
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:00:00 (00:00:00:aa:00:00)
   Sender IP address: 10.0.0.1
   Target MAC address: 00:00:00_aa:00:02 (00:00:00:aa:00:02)
   Target IP address: 10.0.0.21
```

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 host selecionado (Aladdin)

RESPOSTA:

```
root@Aladdin:/tmp/pycore.45265/Aladdin.conf# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.0.21  netmask 255.255.255.0  broadcast 0.0.0.0
        inet6 fe80::200:ff:feaa:2  prefixlen 64  scopeid 0x20<link>
        inet6 2001::21  prefixlen 64  scopeid 0x0<global>
        ether 00:00:00:aa:00:02  txqueuelen 1000  (Ethernet)
        RX packets 705  bytes 74322 (74.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 199  bytes 22834 (22.8 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 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@Aladdin:/tmp/pycore.45265/Aladdin.conf#
```

```
root@Aladdin:/tmp/pycore.45265/Aladdin.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@Aladdin:/tmp/pycore.45265/Aladdin.conf# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.0.1                 ether   00:00:00:aa:00:00   C                     eth0
```

MAC de origem: 00:00:00:aa:00:00 -> router R1

MAC de destino: 00:00:00:aa:00:02 -> Aladdin

d) Discuta, justificando, o modo de comunicação (unicast vs. broadcast) usado no envio da resposta ARP (ARP Reply).

RESPOSTA:

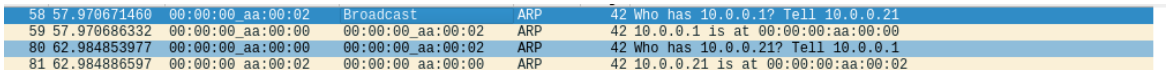
A resposta ao pedido é feita em unicast, pois o destino já sabe o caminho para a origem

1.2.4.

Verifique se a Jasmine teve conhecimento ou não de todo o tráfego gerado pelo acesso secreto do Aladdin? Qual será a razão para tal?

RESPOSTA:

A Jasmine teve acesso ao tráfego secreto gerado pelo Aladdin porque na rede onde os dois se encontram existe um Hub, e os Hubs enviam tudo o que recebem em broadcast, logo tanto os pedidos como as respostas que o Hub recebeu, (nomeadamente as respostas do servidor) foram parar tanto ao Aladdin como na Jasmine.

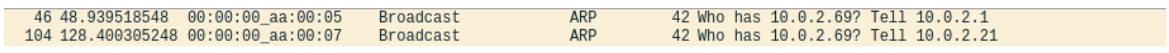


1.2.5.

De igual modo, verifique se a Beauty teve conhecimento ou não de todo o tráfego gerado pelo acesso secreto do Beast? Qual será a razão para tal?

RESPOSTA:

A Beauty não teve conhecimento do tráfego gerado pelo Beast , porque a resposta do servidor foi direcionada diretamente para o Beast. O switch que existe na rede onde os dois se encontram enviou a resposta diretamente para o Beast. Contudo a Beauty recebeu dois ARP request, um deles quando o Aladdin queria comunicar com o servidor, e outro quando o Beast queria comunicar com o servidor.



1.2.6.

Consulte a tabela ARP do Aladdin e do Beast. Que principal diferença entre as tabelas obtidas e que impacto tem no funcionamento da rede?

RESPOSTA:

A diferença entre as tabelas é que, o Aladdin só conhece o endereço MAC do router R1, enquanto que o Beast só conhece o endereço MAC do router R69. Por estes motivos, o Aladdin só consegue comunicar com dispositivos

que estejam acessíveis via o router R1, e o Beast só consegue comunicar com dispositivos acessíveis via o router R69.

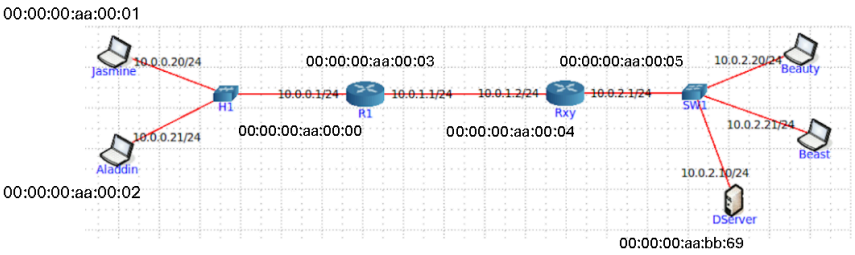
```
root@Aladdin:/tmp/pycore.45265/Aladdin.conf# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.0.1                 ether   00:00:00:aa:00:00   C                     eth0
```

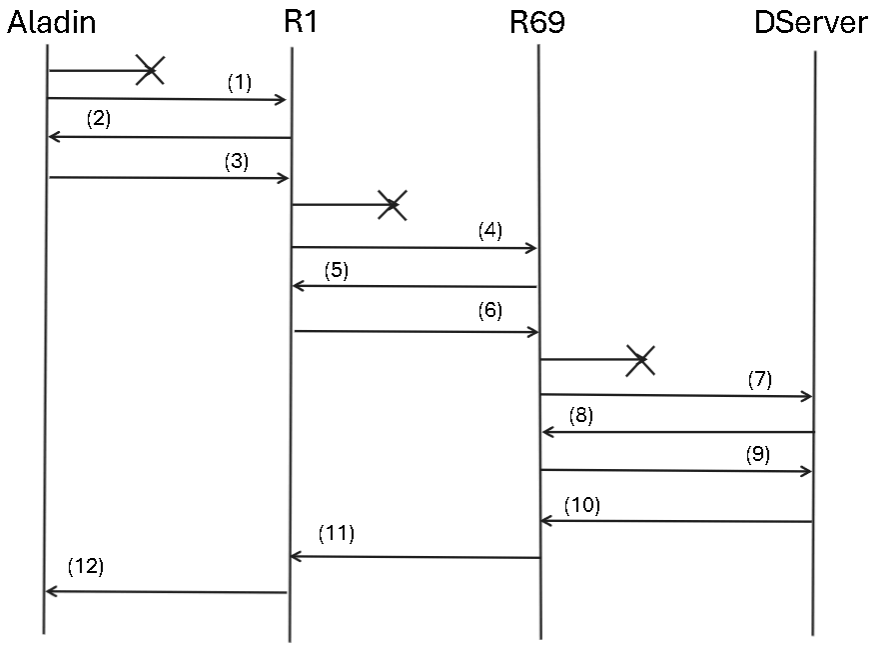
```
root@Beast:/tmp/pycore.40961/Beast.conf# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.69                ether   00:00:00:aa:bb:69   C                     eth0
```

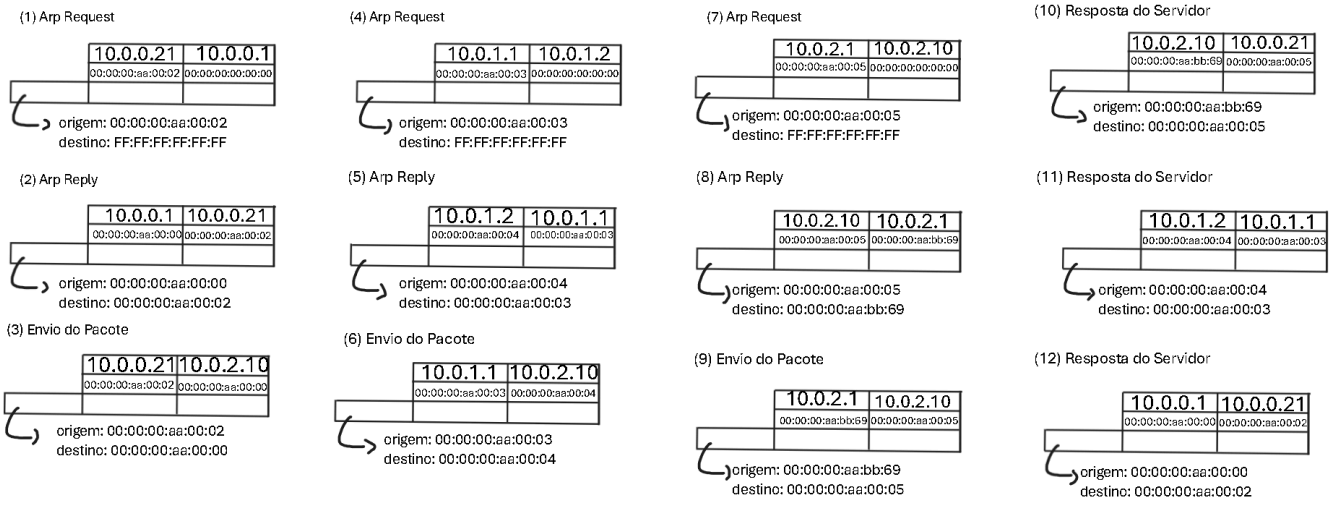
1.2.7.

Esboce um diagrama em que ilustre claramente, e de forma cronológica, todo o tráfego layer 2 (tramas) entre o Aladdin e os hosts com os quais comunica, até à receção do primeiro pacote que contém dados do acesso remoto.

RESPOSTA:



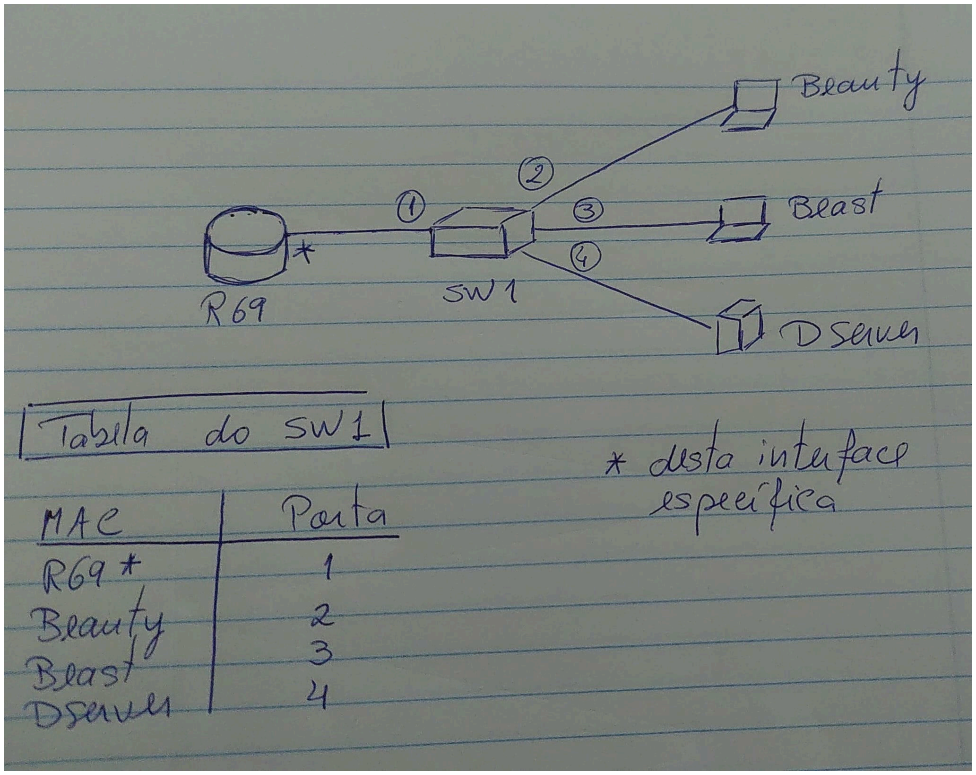




1.2.8.

Construa manualmente a tabela de comutação completa do switch da casa da Beauty e do Beast, (SW1) atribuindo números de porta à sua escolha.

RESPOSTA:



1.3.

Como proteção, a Jasmine e o Aladdin, juntamente com a Beauty e o Beast, decidiram conectar R1 e Rxy a uma rede de um ISP com endereços IP públicos, mantendo todo o endereçamento privado das suas LANs. Sabe-se que o ISP não encaminha tráfego para

redes privadas, portanto, R1 e Rxy não conseguem encaminhar tráfico para endereços privados remotos, i.e., não fisicamente adjacentes.

Discuta que solução implementaria em R1 e em Rxy de modo a manter todas as funcionalidades anteriormente existentes (conectividade IP, acesso ssh ao servidor, etc.).

RESPOSTA:

Para manter as funcionalidades da rede após ligar os routers R1 e R69 a uma rede do ISP, é necessário configurar NAT/PAT nos routers. Isso permite que dispositivos internos com endereços IP privados comuniquem com o exterior e entre si, mesmo quando o ISP rejeita tráfego com endereços privados. Se for necessário aceder a dispositivos internos a partir do exterior (como um servidor SSH), também é necessário configurar redirecionamento de portas.

2. Parte 2
Acesso Rádio

Como pode ser observado, a sequência de bytes capturada inclui meta-informação do nível físico (radiotap header, radio information) obtida do firmware da interface Wi-Fi, para além dos bytes correspondentes a tramas 802.11. Selecione a trama de ordem xy correspondente ao seu identificador de grupo (TurnoGrupo, e.g., 27).

2.1.

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

RESPOSTA:

A rede sem fios está a operar numa frequência de 2412 MHz, e o canal correspondente a essa frequência é o canal 1.

```
64 1.131866     1c:57:3e:fc:f0:a2   Broadcast           802.11    230 Beacon frame, SN=1454, FN=0, Flags=........C, BI=100, SSID=MEO-WiFi
65 1.153978     HitronTe_f3:9a:46   Broadcast           802.11    362 Beacon frame, SN=2539, FN=0, Flags=........C, BI=100, SSID=FlyingNet
66 1.160059     PTInovac_9b:f2:a0   Broadcast           802.11    337 Beacon frame, SN=1346, FN=0, Flags=........C, BI=100, SSID=MEO-9BF2A0
67 1.160063     PTInovac_9b:f2:a2   Broadcast           802.11    230 Beacon frame, SN=1347, FN=0, Flags=........C, BI=100, SSID=MEO-WiFi
68 1.256435     HitronTe_f3:9a:46   Broadcast           802.11    362 Beacon frame, SN=2540, FN=0, Flags=........C, BI=100, SSID=FlyingNet
69 1.258072     PTInovac_29:a9:c0   Continen_95:b6:21   802.11    434 Probe Response, SN=3847, FN=0, Flags=........C, BI=100, SSID=Masmorra do Sexo
70 1.333529     1c:57:3e:fc:f0:a0   Broadcast           802.11    305 Beacon frame, SN=1457, FN=0, Flags=........C, BI=100, SSID=MEO-FCF0A0
71 1.358705     HitronTe_f3:9a:46   Broadcast           802.11    362 Beacon frame, SN=2541, FN=0, Flags=........C, BI=100, SSID=FlyingNet
72 1.364900     PTInovac_9b:f2:a0   Broadcast           802.11    337 Beacon frame, SN=1350, FN=0, Flags=........C, BI=100, SSID=MEO-9BF2A0
73 1.390748     1c:57:3e:fc:f0:a0   Continen_95:b6:21   802.11    380 Probe Response, SN=1459, FN=0, Flags=........C, BI=100, SSID=MEO-FCF0A0
74 1.390877     1c:57:3e:fc:f0:a0   Continen_95:b6:21   802.11    380 Probe Response, SN=1459, FN=0, Flags=....R...C, BI=100, SSID=MEO-FCF0A0
75 1.397421     1c:57:3e:fc:f0:a0   Continen_95:b6:21   802.11    380 Probe Response, SN=1459, FN=0, Flags=....R...C, BI=100, SSID=MEO-FCF0A0
```

```
Channel: 1
Frequency: 2412MHz
```

2.2.

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

RESPOSTA:

A versão da norma que está a ser usada é a 802.11g

```
802.11 radio information
    PHY type: 802.11g (ERP) (6)
```

2.3.

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.

RESPOSTA:

A taxa de transmissão foi de 1,0 Mb/s. Não, não corresponde à taxa máxima de transmissão, pois essa tem valor de 54 Mb/s.

```
Data rate: 1,0 Mb/s
```

IEEE Standard	Year Adopted	Frequency	Max. Data Rate	Max. Range
802.11a	1999	5 GHz	54 Mbps	400 ft.
802.11b	1999	2.4 GHz	11 Mbps	450 ft.
802.11g	2003	2.4 GHz	54 Mbps	450 ft.

Scanning Passivo e Scanning Ativo

Como referido, as tramas beacon permitem efetuar scanning passivo em redes IEEE 802.11 (Wi-Fi). Para a captura de tramas disponibilizada, e considerando xy o seu nº de TurnoGrupo (PLxy), responda às seguintes questões:

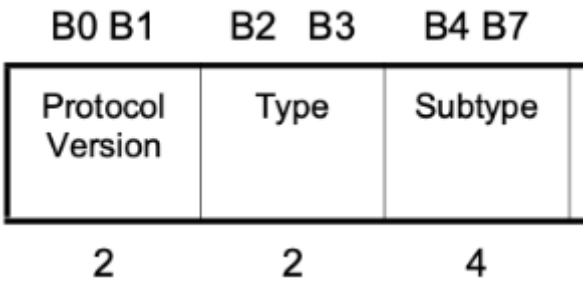
2.4.

Selecione uma trama beacon cuja ordem (ou terminação) corresponda ao seu ID de grupo. 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)?

RESPOSTA:

Esta trama pertence ao tipo *Managment frame*. O identificador do tipo é 00, e o do subtipo é 1000. Estes valores estão especificados no Frame Control, nos primeiros 2 octetos, mais especificamente o tipo está nos bits 2 e 3, e o subtipo está nos bits 4 a 7.

```
Frame 269: 362 bytes on wire (2896 bits), 362 bytes captured (2896 bits) on interface en0, id 0
Radiotap Header v0, Length 36
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
```



2.5.

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")

RESPOSTA:

Sim, o método de deteção de erros (CRC) está a ser usado, como indicado pela presença do campo Frame Check Sequence, mesmo que o Wireshark indique "[unverified]". Isso apenas significa que não foi possível verificar a validade.

```
Frame check sequence: 0x630caf7d [unverified]
[FCS Status: Unverified]
```

2.6.

Justifique o porquê de ser necessário usar deteção de erros em redes sem fios.

RESPOSTA:

Em redes sem fios é preciso usar deteção de erros pois o pacote pode ser corrompido devido a este ser transmitido pelo ar, onde existem várias transmissões a acontecer e por isso poderão existir várias colisões dos sinais e assim, os pacotes ficarem corrompidos. Em redes com fios esse problema não existe porque o meio não é propício a misturas.

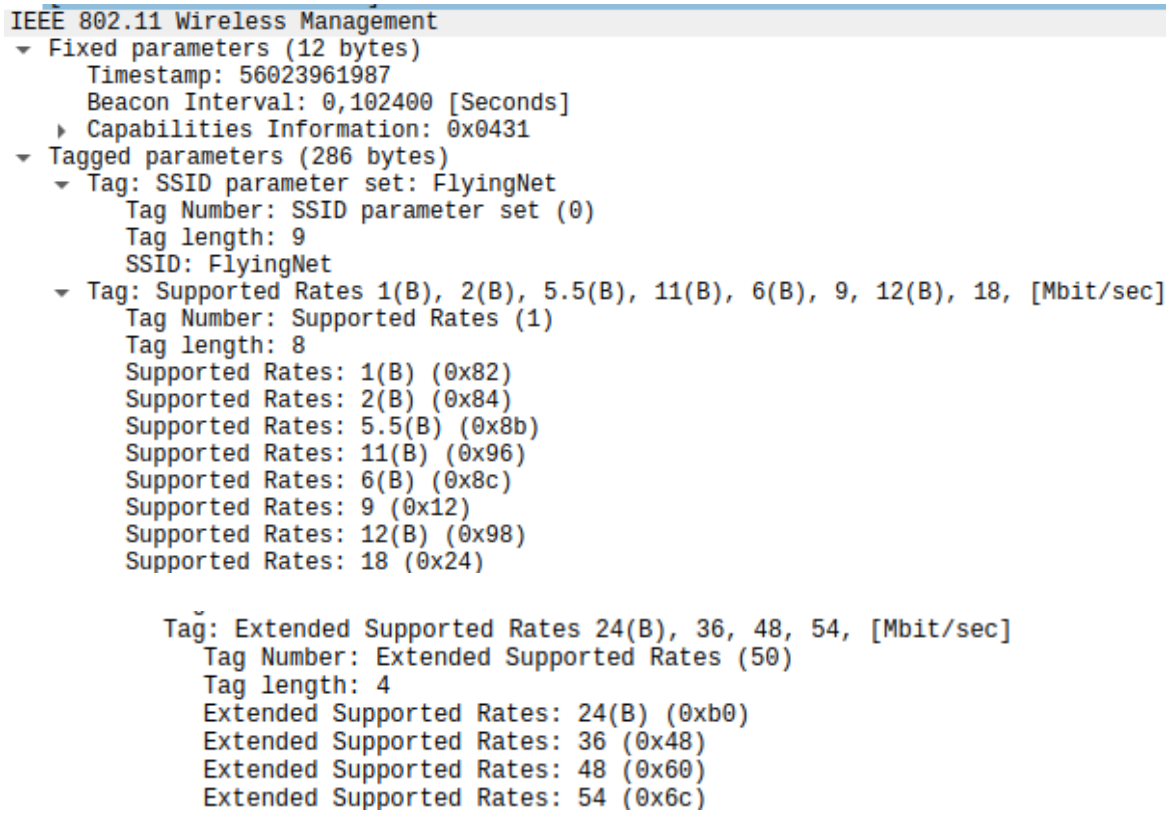
2.7.

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.

RESPOSTA:

A periodicidade é de 0.102400 segundos.

As taxas de transmissão suportadas pelo AP da trama são: 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, 54 Mbit/s



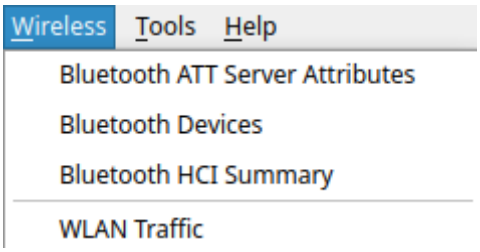
2.8.

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).

RESPOSTA:

Foi utilizado o filtro WLAN Traffic.

BSSID	Channel	SSID
00:06:91:29:a9:c0	1	Masmorra do Sexo
00:06:91:29:a9:c2	1	MEO-WiFi
00:06:91:45:70:40		<Broadcast>
00:06:91:77:f9:60		<Broadcast>
00:06:91:82:88:30	1	MEO-828830
00:06:91:82:88:32	1	MEO-WiFi
00:06:91:85:4c:80	1	MEO-854C80
00:06:91:85:4c:82	1	NOS-55F6
00:06:91:9b:f2:a0	1	MEO-9BF2A0
00:06:91:9b:f2:a2	1	MEO-WiFi
00:06:91:f1:75:70	1	MEO-F17570
00:06:91:f1:75:72	1	ZON-2770
14:8c:4a:8c:89:c0		<Broadcast>
18:a6:f7:f1:af:69	1	Vodafone-D0ED8A
1c:57:3e:fc:f0:a0	1	MEO-FCF0A0
1c:57:3e:fc:f0:a2	1	MEO-WiFi
2c:9d:1e:d0:ed:90		<Broadcast>
40:ed:00:8e:b3:f8	1	NOS-9946_EXT
74:9b:e8:4d:52:c6	1	NOS-52C6
74:9b:e8:f3:9a:46	1	FlyingNet
90:aa:c3:e5:26:f6	1	NOS-26F6
a6:ef:15:08:32:99	1	phi_F41927C3C600
cc:19:a8:66:db:70	1	MEO-66DB70
cc:19:a8:66:db:72	1	MEO-WiFi
d0:cf:0e:7f:87:74	1	GVBRAGA
d0:cf:0e:95:fd:24	1	ZON-82F0
d8:78:7f:a2:67:d0		<Broadcast>
da:78:7f:a2:67:d2		<Broadcast>
dc:62:79:31:e2:39	1	GVBRAGA_EXT
f0:09:0d:ba:0e:0e	1	GVBRAGA_quarto
f8:53:29:30:69:84		<Broadcast>
fc:77:7b:ee:c8:b6	1	NOS-C8B6
ff:ff:ff:ff:ff:ff	2	<Broadcast>
ff:ff:ff:ff:ff:ff	1	GVBRAGA NOS
ff:ff:ff:ff:ff:ff		FlyingNet_2.4GEXT
ff:ff:ff:ff:ff:ff	1	eduroam
ff:ff:ff:ff:ff:ff	1	rededaquinta
ff:ff:ff:ff:ff:ff	1	abriluchi
ff:ff:ff:ff:ff:ff	1	Vodafone-B724A9
ff:ff:ff:ff:ff:ff	1	*WIFI-AIRPORT
ff:ff:ff:ff:ff:ff	1	Villa-Montsouris
ff:ff:ff:ff:ff:ff		Le bistro de longchamp
ff:ff:ff:ff:ff:ff	1	EXT_5
ff:ff:ff:ff:ff:ff	1	CDC_1ANDAR_CLIENTES
ff:ff:ff:ff:ff:ff	1	NOS-26F6



2.9.

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

RESPOSTA:

O filtro estabelecido foi:

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

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

No.	Time	Source	Destination	Protocol	Length	Signal strengt	Info
1623	19.859889	MS-NLB-PhysS…	Broadcast	802.11	208	-25dBm	Probe Reques…
1620	19.853562	MS-NLB-PhysS…	Broadcast	802.11	208	-25dBm	Probe Reques…
1518	18.829692	ca:8c:cf:d6:…	Broadcast	802.11	208	-25dBm	Probe Reques…
1524	18.853607	ca:8c:cf:d6:…	Broadcast	802.11	208	-26dBm	Probe Reques…
1615	19.806401	6e:92:f3:f3:…	Broadcast	802.11	208	-27dBm	Probe Reques…
1611	19.790975	6e:92:f3:f3:…	Broadcast	802.11	208	-27dBm	Probe Reques…
9274	52.221780	AzureWav_0f:…	Broadcast	802.11	110	-28dBm	Probe Reques…
2034	23.661926	fe:bd:a5:05:…	Broadcast	802.11	217	-28dBm	Probe Reques…
2006	23.354102	62:07:ab:20:…	Broadcast	802.11	208	-29dBm	Probe Reques…
2005	23.351137	de:03:dc:e6:…	Broadcast	802.11	220	-29dBm	Probe Reques…
2000	23.316563	62:07:ab:20:…	Broadcast	802.11	208	-29dBm	Probe Reques…
1999	23.316469	de:03:dc:e6:…	Broadcast	802.11	220	-29dBm	Probe Reques…
44083	229.055630	AzureWav_0f:…	Broadcast	802.11	110	-30dBm	Probe Reques…
9313	52.312062	Tp-LinkT_ce:…	Broadcast	802.11	82	-30dBm	Probe Reques…
9312	52.312057	Tp-LinkT_ce:…	Broadcast	802.11	82	-30dBm	Probe Reques…
44099	229.103021	AzureWav_0f:…	Broadcast	802.11	110	-31dBm	Probe Reques…
10854	58.588908	f6:1a:7e:48:…	Broadcast	802.11	208	-31dBm	Probe Reques…
9258	52.202711	Tp-LinkT_ce:…	Broadcast	802.11	82	-31dBm	Probe Reques…
9257	52.202706	Tp-LinkT_ce:…	Broadcast	802.11	82	-31dBm	Probe Reques…
6948	47.172102	5e:1b:97:a6:…	Broadcast	802.11	208	-31dBm	Probe Reques…
6944	47.162882	5e:1b:97:a6:…	Broadcast	802.11	208	-31dBm	Probe Reques…
32326	152.670851	6a:9d:77:d6:…	Broadcast	802.11	125	-32dBm	Probe Reques…
10876	58.690744	86:4f:4e:1c:…	Broadcast	802.11	208	-32dBm	Probe Reques…
10855	58.599204	f6:1a:7e:48:…	Broadcast	802.11	208	-32dBm	Probe Reques…

2.10.

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 indique a qual AP a STA de captura se deve associar para obter a melhor qualidade de ligação possível. Indique como chegou a esta resposta.

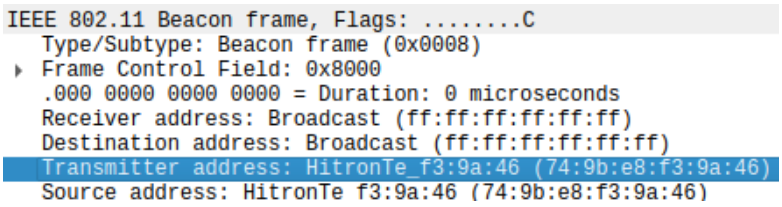
RESPOSTA:

Filtrando pelas tramas probing request e probing response e depois ordenando pelo menor ruído, ficamos com:

wlan.fc.type_subtype == 0x08 || wlan.fc.type_subtype == 0x05

No.	Time	Source	Destination	Protocol	Length	Signal strength (dBm)	Info
39127	191.415288	HitronTe_f3:9a:46	Broadcast	802.11	362	-39dBm	Beacon frame, SN=672, FN=0, Flags=........C, BI=100, SSID=FlyingNet
39142	191.519316	HitronTe_f3:9a:46	Broadcast	802.11	362	-41dBm	Beacon frame, SN=673, FN=0, Flags=........C, BI=100, SSID=FlyingNet
62491	294.942721	HitronTe_f3:9a:46	Broadcast	802.11	362	-42dBm	Beacon frame, SN=1721, FN=0, Flags=........C, BI=100, SSID=FlyingNet
39175	191.619924	HitronTe_f3:9a:46	Broadcast	802.11	362	-42dBm	Beacon frame, SN=674, FN=0, Flags=........C, BI=100, SSID=FlyingNet
39097	191.312888	HitronTe_f3:9a:46	Broadcast	802.11	362	-42dBm	Beacon frame, SN=671, FN=0, Flags=........C, BI=100, SSID=FlyingNet
39041	191.005679	HitronTe_f3:9a:46	Broadcast	802.11	362	-42dBm	Beacon frame, SN=668, FN=0, Flags=........C, BI=100, SSID=FlyingNet
38819	190.086750	HitronTe_f3:9a:46	Broadcast	802.11	362	-42dBm	Beacon frame, SN=659, FN=0, Flags=........C, BI=100, SSID=FlyingNet
299	4.225971	HitronTe_f3:9a:46	Broadcast	802.11	362	-42dBm	Beacon frame, SN=2569, FN=0, Flags=........C, BI=100, SSID=FlyingNet
287	4.123548	HitronTe_f3:9a:46	Broadcast	802.11	362	-42dBm	Beacon frame, SN=2568, FN=0, Flags=........C, BI=100, SSID=FlyingNet
276	3.918868	HitronTe_f3:9a:46	Broadcast	802.11	362	-42dBm	Beacon frame, SN=2566, FN=0, Flags=........C, BI=100, SSID=FlyingNet
63030	300.882107	HitronTe_f3:9a:46	Broadcast	802.11	362	-43dBm	Beacon frame, SN=1782, FN=0, Flags=........C, BI=100, SSID=FlyingNet
62567	295.147545	HitronTe_f3:9a:46	Broadcast	802.11	362	-43dBm	Beacon frame, SN=1723, FN=0, Flags=........C, BI=100, SSID=FlyingNet
62460	294.737941	HitronTe_f3:9a:46	Broadcast	802.11	362	-43dBm	Beacon frame, SN=1719, FN=0, Flags=........C, BI=100, SSID=FlyingNet
45829	243.230119	HitronTe_f3:9a:46	Broadcast	802.11	362	-43dBm	Beacon frame, SN=1204, FN=0, Flags=........C, BI=100, SSID=FlyingNet
39209	191.824768	HitronTe_f3:9a:46	Broadcast	802.11	362	-43dBm	Beacon frame, SN=676, FN=0, Flags=........C, BI=100, SSID=FlyingNet
39021	190.903237	HitronTe_f3:9a:46	Broadcast	802.11	362	-43dBm	Beacon frame, SN=667, FN=0, Flags=........C, BI=100, SSID=FlyingNet
38875	190.288744	HitronTe_f3:9a:46	Broadcast	802.11	362	-43dBm	Beacon frame, SN=661, FN=0, Flags=........C, BI=100, SSID=FlyingNet

Como é possível observar na tabela, a trama com a melhor qualidade de ligação é a Nº39127, pois apresenta o menor nível de ruído. Assim, esta deverá ser a STA de procura que se pretende identificar como potencial ponto de acesso. Consultando o seu endereço MAC de transmissão — 'HitronTechno_f3:9a:46 (74:9b:e8:f3:9a:46)' — conclui-se que é a este AP que a STA de captura deverá tentar associar-se.



2.11.

Os valores de taxa de transmissão do Wi-Fi estão diretamente associados à qualidade da receção do sinal. Considerando os valores de sensibilidade mínima (Minimum Sensivity) e taxa de transmissão (Data Rate) que constam nas tabelas de referência (ver Anexo II), e a força do sinal recebido nas tramas do AP identificado na resposta anterior, estime o débito que a STA obterá nessa ligação.

RESPOSTA:

Como podemos ver na pergunta anterior, a trama com a melhor força de sinal, tem um valor de −39dBm, que é um valor de sensibilidade superior aos apresentados na tabela do Anexo II. Desta forma, se analisarmos o débito correspondente ao maior valor presente na tabela, podemos concluir que no nosso caso, o débito terá de ser maior ou igual a 65 Mb/s.

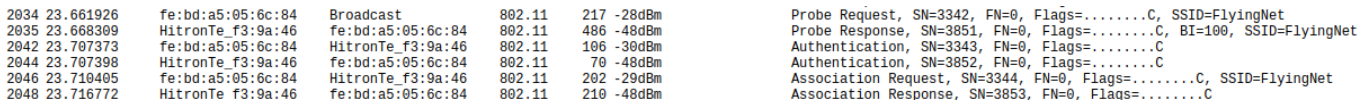
Processo de Associação

2.12.

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.

RESPOSTA:

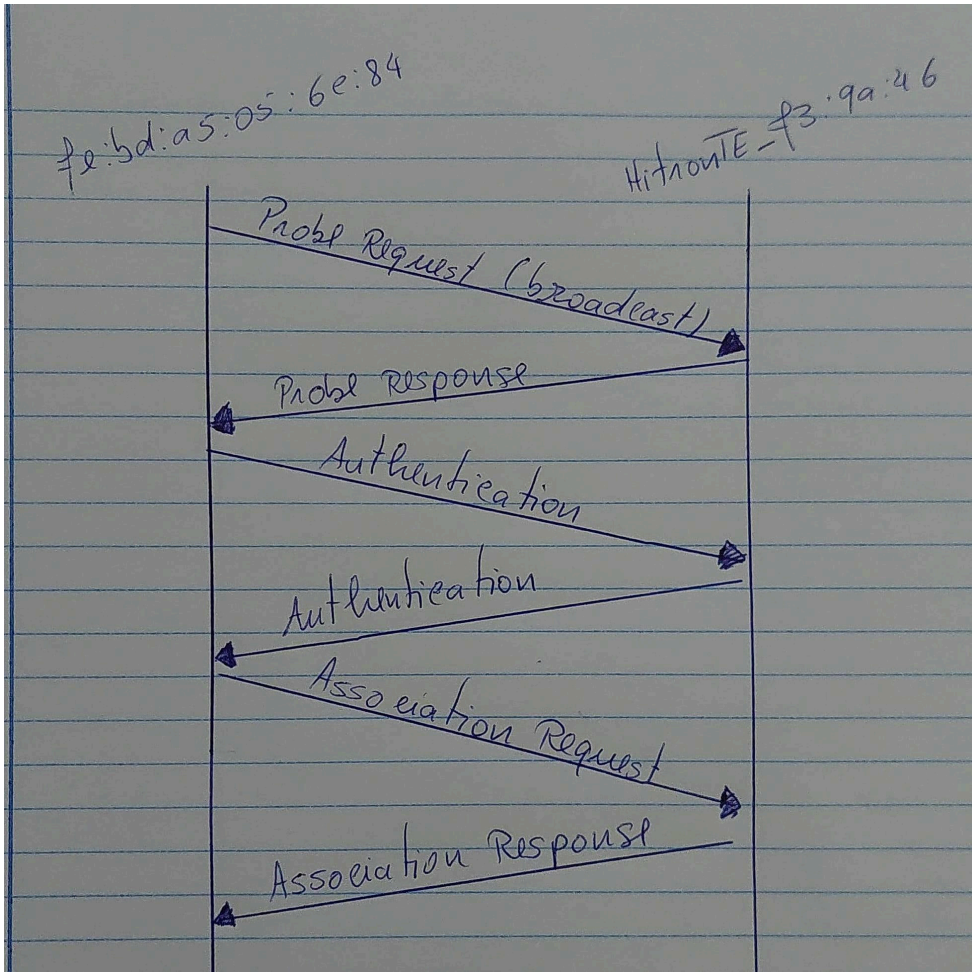
Usando o filtro: wlan.fc.type_subtype == 0 || wlan.fc.type_subtype == 1 || wlan.fc.type_subtype == 11 || wlan.fc.type_subtype == 4 || wlan.fc.type_subtype == 5, foi possível identificar as tramas:



2.13.

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

RESPOSTA:



Transferência de Dados

2.14.

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 xy, ou y caso não exista xy). 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?

RESPOSTA:

Usando o filtro 'wlan.fc.type_subtype == 0x20 || wlan.fc.type_subtype == 0x28' foi possível identificar a trama:

```
Frame 3869: 244 bytes on wire (1952 bits), 244 bytes captured (1952 bits) on interface en0, id 0
Radiotap Header v0, Length 58
802.11 radio information
IEEE 802.11 QoS Data, Flags: .p.....TC
   Type/Subtype: QoS Data (0x0028)
 ▾ Frame Control Field: 0x8841
      .... ..00 = Version: 0
      .... 10.. = Type: Data frame (2)
      1000 .... = Subtype: 8
   ▾ Flags: 0x41
         .... ..01 = DS status: Frame from STA to DS via an AP (To DS: 1 From DS: 0) (0x1)
         .... .0.. = More Fragments: This is the last fragment
         .... 0... = Retry: Frame is not being retransmitted
         ...0 .... = PWR MGT: STA will stay up
         ..0. .... = More Data: No data buffered
         .1.. .... = Protected flag: Data is protected
         0... .... = Order flag: Not strictly ordered
   .000 0000 0011 0000 = Duration: 48 microseconds
   Receiver address: HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)
   Transmitter address: fe:bd:a5:05:6c:84 (fe:bd:a5:05:6c:84)
   Destination address: 76:9b:e8:f3:9a:43 (76:9b:e8:f3:9a:43)
   Source address: fe:bd:a5:05:6c:84 (fe:bd:a5:05:6c:84)
   BSS Id: HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)
   STA address: fe:bd:a5:05:6c:84 (fe:bd:a5:05:6c:84)
   .... .... .... 0000 = Fragment number: 0
   0000 0100 0100 .... = Sequence number: 68
   Frame check sequence: 0xb76415ea [unverified]
   [FCS Status: Unverified]
```

Como é possível observar, To DS = 1, From DS = 0, isto significa que a trama vai da STA para o DS, ou seja, para o AP.

A trama pode ou não ser local à WLAN , isso depende do destino final dos dados. A direcionalidade indica apenas que ela está a entrar no AP, mas não garante que permanecerá dentro da WLAN.

2.15.

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)?

RESPOSTA:

Usando a trama apresentada na pergunta anterior, foi possível transcrever os seguintes endereços MAC:

- **Receiver address: HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46) → AP**
- **Transmitter address: fe:bd:a5:05:6c:84 (fe:bd:a5:05:6c:84) → STA**
- **Destination address: 76:9b:e8:f3:9a:43 (76:9b:e8:f3:9a:43) → DS**
- **Source address: fe:bd:a5:05:6c:84 (fe:bd:a5:05:6c:84)**
- **BSS Id: HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)**
- **STA address: fe:bd:a5:05:6c:84 (fe:bd:a5:05:6c:84)**

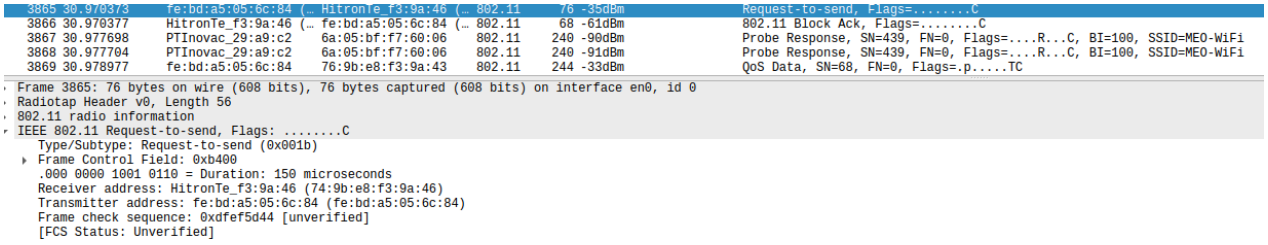
Tal como é possível observar, o endereço MAC do AP é 'HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)' e o endereço MAC do STA é 'fe:bd:a5:05:6c:84 (fe:bd:a5:05:6c:84'. Como o endereço MAC do AP é igual ao endereço

MAC do receiver e o endereço MAC do STA é igual ao endereço MAC da source, o endereço do router de acesso ao DS será o 76:9b:e8:f3:9a:43 (76:9b:e8:f3:9a:43).

2.16.

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.

RESPOSTA:



Tal como é possível verificar na figura anterior, a trama Nº3865 é uma trama Request to Send (RTS). Esta é enviada antes da trama 3869 pois funciona como um mecanismo de pré-reserva de acesso ao AP para o qual a trama 3869 está a ser enviada.

O mecanismo RTS/CTS é usado em redes Wi-Fi para evitar colisões, especialmente quando há estações escondidas. É ativado, por exemplo, quando duas STAs não se veem mas comunicam com o mesmo AP. Já em ambientes com boa qualidade de sinal e pouco tráfego, o RTS/CTS não é usado para evitar overhead desnecessário.

3. Conclusão

Ao longo deste trabalho, foi possível aprofundar os conhecimentos sobre o funcionamento das redes de computadores, em particular no que diz respeito à análise de tramas Ethernet e comunicação em redes sem fios. Através da utilização do Wireshark, foi possível observar diretamente o conteúdo das tramas trocadas entre dispositivos, compreendendo melhor como funciona o processo de comunicação no nível 2.

Na análise das tramas Ethernet, destacaram-se conceitos como o endereço MAC de origem e de destino, o campo Type que identifica o protocolo da camada superior, e a importância da tabela ARP para a resolução de endereços IP em endereços físicos.

No caso das redes sem fios, a análise focou-se na norma IEEE 802.11 e nas suas diferentes componentes, como tramas beacon, probe requests/responses e o processo de associação a um ponto de acesso. Através destes pacotes, foi possível perceber como os dispositivos descobrem e se ligam a redes disponíveis, bem como os fatores que influenciam a qualidade da ligação, como a potência do sinal e o ruído.

Em suma, este trabalho proporcionou uma experiência prática fundamental para consolidar os conhecimentos teóricos sobre redes, tornando visíveis os mecanismos de comunicação que muitas vezes passam despercebidos ao utilizador final. A utilização do Wireshark revelou-se uma ferramenta essencial para esta análise, permitindo observar o comportamento real das redes em diferentes contextos e compreender melhor as decisões tomadas pelos protocolos subjacentes.