



Universidade do Minho
Escola de Engenharia
Licenciatura em Engenharia Informática

Unidade Curricular de Redes de Computadores

Ano Letivo de 2023/2024

Trabalho Prático Nº 3

Grupo 74

Nível de Ligação Lógica:

Redes Ethernet,

Protocolo ARP,

Redes Locais sem Fios (Wi-Fi)

Tomás Henrique Alves Melo (A104529)
José Pedro Torres Vasconcelos (A100763)
Sandro José Rodrigues Coelho (A105672)

7 de maio de 2024

RC

Índice

1	Parte 1	1
1.1	Captura e análise de Tramas Ethernet	1
1.1.1	Exercício 1	1
1.1.2	Exercício 2	2
1.1.3	Exercício 3	2
1.1.4	Exercício 4	4
1.1.5	Exercício 5	4
1.2	Protocolo ARP e Domínios de Colisão	4
1.2.1	Exercício 1	4
1.2.2	Exercício 2	5
1.2.3	Exercício 3	6
1.2.4	Exercício 4	9
1.2.5	Exercício 5	9
1.2.6	Exercício 6	9
1.2.7	Exercício 7	11
2	Parte 2 - Redes Locais sem Fios (Wi-Fi)	12
2.1	Acesso Rádio	12
2.1.1	Exercício 1	12
2.1.2	Exercício 2	13
2.1.3	Exercício 3	14
2.2	Scanning Passivo e Scanning Ativo	14
2.2.1	Exercício 4	14
2.2.2	Exercício 5	15
2.2.3	Exercício 6	16
2.2.4	Exercício 7	16
2.2.5	Exercício 8	16
2.2.6	Exercício 9	18
2.2.7	Exercício 10	18
2.2.8	Exercício 11	18
2.3	Processo de Associação	19
2.3.1	Exercício 12	19
2.3.2	Exercício 13	19
2.4	Transferência de Dados	20
2.4.1	Exercício 14	20
2.4.2	Exercício 15	21

2.4.3	Exercício 16	22
3	Conclusões retiradas	23

Lista de Figuras

1.1	Trama capturada	1
1.2	Informação ethernet da trama	2
1.3	Campo Type	2
1.4	Length do pacote IPv4	2
1.5	Transmission Control Protocol	3
1.6	Demonstração gráfica para cálculo do número de bytes da sobrecarga (overhead)	3
1.7	Informação Ethernet da trama	4
1.8	Resultado obtido pelo comando <code>arp -a</code>	5
1.9	Trama Broadcast	5
1.10	Trama Ethernet	5
1.11	Address Resolution Protocol	6
1.12	Arp reply	7
1.13	Tabela de encaminhamento gerada por <code>netstat -rn</code>	7
1.14	Output gerado por <code>ifconfig</code>	8
1.15	Comando <code>arp</code>	8
1.16	Captura da interface sobre o Burro	9
1.17	Captura da interface do PC da Fiona	9
1.18	Primeiro SET de troca de pacotes	10
1.19	Segundo SET de troca de pacotes	10
1.20	Diagrama de todas as mensagens trocadas	10
1.21	Tabela de comutação	11
2.1	Informação da trama 74 - RadioTap Header	13
2.2	802.11 radio information	13
2.3	Taxa de transmissão	14
2.4	Informação da trama 674	15
2.5	Antes da ativação da verificação	15
2.6	Após a ativação da verificação	15
2.7	Informação da trama com indicação da periodicidade e taxas de transmissão suportadas pelo AP da trama	16
2.8	Lista de SSIDs	17
2.9	Filtro Wireshark utilizado	18
2.10	Sequência de tramas	19
2.11	Diagrama de sequências das tramas trocadas	20
2.12	Informação da trama 574	21
2.13	Tramas resultantes do filtro	22

2.14	Transferência de dados com CTS/RTS	22
2.15	Transferência de dados sem CTS/RTS	22

1 Parte 1

1.1 Captura e análise de Tramas Ethernet

"Com o aumento do preço da habitação em Braga, o *Shrek* e o *Burro* tomam a decisão economicamente sensata e decidem voltar à sua casa no *Pântano*. A sua rede local é constituída por um *switch* (*n2*), um *router* para acesso à rede (*n1*), assim como os portáteis do *Shrek* e do *Burro*, ligados por *Ethernet* a *n2*. O *router n1* está ainda ligado a um *hub* (*n3*), que se conecta ao portátil da *Fiona* e ao servidor do conhecido site de notícias *pantanews.com*. A caminho, o *Shrek* fica a saber que houve um ataque aos servidores do seu site de notícias favorito, o *Pantanews*, e que todos os seus dados terão sido apagados. Assim que chegam a casa, o *Shrek* aproveita para verificar se realmente há algum problema com o *site* (*servidor - 10.0.1.10*). Utilize o comando *curl* para o efeito (poderá consultar o manual do comando com *man curl*), apontando diretamente para o endereço do servidor. Pare a captura do *Wireshark*, e analise a trama que contém a primeira mensagem de dados *HTTP* enviada pelo *Shrek*."

1.1.1 Exercício 1

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

82	128	219279763	00:00:00:aa:00:02	00:00:00:aa:00:00	ARP	42	10	0	0	1	1	at	00:00:00:aa:00:02				
83	128	219231255	10:0:0:20	10:0:1:10	TCP	74	39738	-	80	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	SACK_PERM=1	TSval=125738...	
84	128	219268977	10:0:1:10	10:0:0:20	TCP	74	80	-	39738	[SYN, ACK]	Seq=9	Ack=1	Win=65169	Len=0	MSS=1460	SACK_PERM=1	T...
85	128	219279376	10:0:0:20	10:0:1:10	TCP	68	39738	-	80	[ACK]	Seq=1	Ack=1	Win=64256	Len=0	TSval=1257388191	TSecr=8416...	
86	128	219336552	10:0:0:20	10:0:1:10	HTTP	139	GET / HTTP/1.1										
87	128	219454993	10:0:1:10	10:0:0:20	TCP	66	80	-	39738	[ACK]	Seq=1	Ack=74	Win=65152	Len=0	TSval=841656501	TSecr=1257...	
88	128	220377640	10:0:1:10	10:0:0:20	HTTP	552	HTTP/1.1 200 OK										
89	128	220491859	10:0:0:20	10:0:1:10	TCP	66	39738	-	80	[ACK]	Seq=74	Ack=487	Win=63872	Len=0	TSval=1257388192	TSecr=8...	
90	128	22214824	10:0:0:20	10:0:1:10	TCP	66	39738	-	80	[FIN, ACK]	Seq=74	Ack=487	Win=64128	Len=0	TSval=1257388194	T...	
91	128	222266671	10:0:1:10	10:0:0:20	TCP	68	80	-	39738	[FIN, ACK]	Seq=487	Ack=75	Win=65152	Len=0	TSval=841656504	Tse...	
92	128	222266689	10:0:0:20	10:0:1:10	TCP	66	39738	-	80	[ACK]	Seq=75	Ack=488	Win=64128	Len=0	TSval=1257388194	TSecr=8...	
93	130	878666187	10:0:0:1	224:0:0:5	OSPF	78	Hello Packet										

Figura 1.1: Trama capturada

R: Pela imagem acima concluímos que a trama a analisar deverá ser a 86, que se encontra encriptada. A imagem abaixo fornece informações dos endereços MAC origem e destino. O endereço MAC origem é 00:00:00:aa:00:00, que corresponde ao sistema de origem de onde é enviado o pedido, neste caso, a máquina local. O endereço MAC destino 00:00:00:aa:00:02 irá corresponder ao AP, neste caso, o router.

```

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)
    Address: 00:00:00_aa:00:02 (00:00:00:aa:00:02)
    ....0 .... = LG bit: Globally unique address (factory default)
    ....0 .... = IG bit: Individual address (unicast)
  Source: 00:00:00_aa:00:00 (00:00:00:aa:00:00)
    Address: 00:00:00_aa:00:00 (00:00:00:aa:00:00)
    ....0 .... = LG bit: Globally unique address (factory default)
    ....0 .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)

```

Figura 1.2: Informação ethernet da trama

1.1.2 Exercício 2

"Qual o valor hexadecimal do campo *Type* da trama *Ethernet*? O que significa?"

Type: IPv4 (0x0800)

Figura 1.3: Campo Type

R: O campo *Type* é importante, pois especifica qual é o protocolo de nível superior encapsulado no corpo (*payload*) da trama *Ethernet*. O valor 0x0800 indica que o *payload* da trama contém um pacote *IPv4*, informando o sistema que este deve usar as regras específicas do *IPv4*.

1.1.3 Exercício 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."

```

▶ Frame 86: 139 bytes on wire (1112 bits), 13
▶ Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00)
▶ Internet Protocol Version 4, Src: 10.0.0.20
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
▶ Differentiated Services Field: 0x00 (DSCP)
  Total Length: 125

```

Figura 1.4: Length do pacote IPv4

```

Transmission Control Protocol, Src Port: 39738, Dst Port: 80
Source Port: 39738
Destination Port: 80
[Stream index: 0]
[TCP Segment Len: 73]
Sequence number: 1 (relative sequence number)
Sequence number (raw): 3750566886
[Next sequence number: 74 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
Acknowledgment number (raw): 3857079648
1000 .... = Header Length: 32 bytes (8)

```

Figura 1.5: Transmission Control Protocol

R: Compreendendo as camadas de rede e os princípios de encapsulamento, que envolvem a incorporação de dados de camadas superiores em pacotes de diferentes tamanhos com cabeçalhos específicos, é importante notar o seguinte: o cabeçalho do *IPv4*, que é imediatamente encapsulado após a trama *Ethernet* e por sua vez encapsula os dados das camadas superiores, inclui um campo que especifica o tamanho total do pacote, neste caso, 125 *bytes*. O tamanho da trama *ethernet* é fixo e equivalente a 14 *bytes*. Podemos deste modo então determinar o tamanho total da trama, $(14 + 125) = 139$ *bytes*. O cabeçalho *IP* é definido como 20 *bytes*. Pela análise da imagem, observa-se que o cabeçalho *TCP* possui um total de 32 *bytes* (20 *bytes* + 12 *bytes* de *options*). A sobrecarga (*overhead*) vai corresponder exatamente a $(12 + 20 + 32)$ *bytes*, isto é, 66 *bytes*. O valor, em percentagem, pode ser calculado pela divisão de 66 (sobrecarga) por 139 (total *length*) que resulta em aproximadamente 0.4749 que, multiplicado por 100, resulta num valor final de 47.5%. Abaixo é dada uma representação deste cálculo para mais simples entendimento.

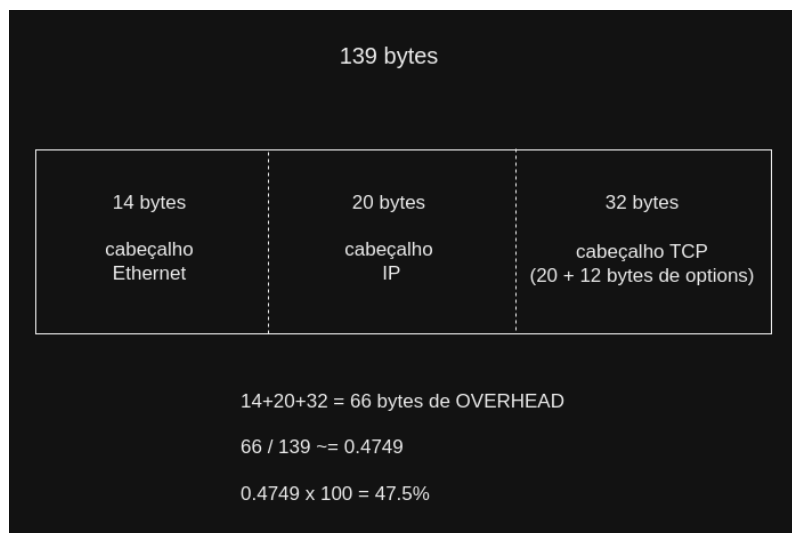


Figura 1.6: Demonstração gráfica para cálculo do número de bytes da sobrecarga (overhead)

1.1.4 Exercício 4

"Qual é o endereço *Ethernet* da fonte? A que sistema de rede corresponde? Justifique"

```
Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:00 (00:00:00:aa:00:00)
  Destination: 00:00:00_aa:00:00 (00:00:00:aa:00:00)
    Address: 00:00:00_aa:00:00 (00:00:00:aa:00:00)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  Source: 00:00:00_aa:00:02 (00:00:00:aa:00:02)
    Address: 00:00:00_aa:00:02 (00:00:00:aa:00:02)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
```

Figura 1.7: Informação *Ethernet* da trama

R: O endereço *Ethernet* da fonte, 00:00:00:aa:00:02, identifica o *Access Point* (AP), que neste caso é o *router* de acesso (destino, como visto na imagem acima).

1.1.5 Exercício 5

"Qual é o endereço *MAC* do destino? A que interface corresponde?"

R: O endereço *Ethernet* do destino, 00:00:00:aa:00:00, está associado à interface da máquina local (origem, como visto na imagem acima).

1.2 Protocolo ARP e Domínios de Colisão

"Deverá ter a cache *ARP* completamente vazia antes de iniciar esta secção: reinicie a topologia, ou utilize o comando **arp -d**. Um pouco mais preocupado com a segurança dos seus dados, o *Shrek* repara que a *Fiona* sabe sempre por onde andou a navegar. Para averiguar esta situação, o *Shrek* experimenta de novo aceder ao site do *pantanews.com* (10.0.1.10) através do comando **curl**. Certifique-se que está a capturar tráfego com o *Wireshark* na interface do *Shrek* e na do *Burro*."

1.2.1 Exercício 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."

```

root@Shrek:/tmp/pycore.39159/Shrek.conf# curl 10.0.1.10
<html><body><!-- generated by utility.py:HttpService -->
<h1>Pantanews web server</h1>
<p>This is the default web page for this server.</p>
<p>The web server software is running but no content has been added, yet.</p>
<li>eth0 - ['10.0.1.10/24', '2001::1::10/64']</li>
</body></html>root@Shrek:/tmp/pycore.39159/Shrek.conf# arp -a
? (10.0.0.1) at 00:00:00:aa:00:02 [ether] on eth0
root@Shrek:/tmp/pycore.39159/Shrek.conf#

```

Figura 1.8: Resultado obtido pelo comando arp -a

R: O endereço IP corresponde a 10.0.0.1 e o endereço MAC é 00:00:00:aa:00:02. A entrada correspondente na tabela ARP está associada à interface de rede eth0, uma vez que foi através desta interface que se deu a troca de pedidos ou respostas ARP.

1.2.2 Exercício 2

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

26	22.017589855	10.0.0.1	224.0.0.5	OSPF	78	Hello Packet
27	22.882318928	00:00:00:aa:00:00	Broadcast	ARP	42	Who has 10.0.0.1? Tell 10.0.0.28
28	22.882343742	00:00:00:aa:00:02	00:00:00:aa:00:00	ARP	42	10.0.0.1 is at 00:00:00:aa:00:02

Figura 1.9: Trama Broadcast

Alínea a)

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

```

Destination: Broadcast (ff:ff:ff:ff:ff:ff)
Address: Broadcast (ff:ff:ff:ff:ff:ff)
.....1..... = LG bit: Locally administered address (this is NOT the factory default)
.....1..... = IG bit: Group address (multicast/broadcast)
Source: 00:00:00:aa:00:00 (00:00:00:aa:00:00)
Address: 00:00:00:aa:00:00 (00:00:00:aa:00:00)
.....0..... = LG bit: Globally unique address (factory default)
.....0..... = IG bit: Individual address (unicast)
Type: ARP (0x0806)

```

Figura 1.10: Trama Ethernet

R: Na trama de *Ethernet*, o valor hexadecimal do endereço MAC origem é 00:00:00:aa:00:00. Por outro lado, o valor hexadecimal do endereço MAC destino é desconhecido, sendo enviado para todos os dispositivos da rede local um pacote com o IP destino (10.0.1.10), de modo a descobrir o endereço MAC desejado.

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* (Type: ARP (0x0806)), indicando que a trama de *ethernet* encapsula um protocolo *ARP*.

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."

```
▼ 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:00:00 (00:00:00:aa:00:00)
  Sender IP address: 10.0.0.20
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 10.0.0.1
```

Figura 1.11: Address Resolution Protocol

R: É possível observar que esta mensagem se trata de um pedido *ARP* através destes métodos:

- O campo *opcode* na mensagem *ARP* especifica o tipo de operação. Pela imagem acima, verificamos que este corresponde a 1 (Opcode: request(1)) indicando que se trata de um *ARP request*. Caso o mesmo fosse 2, tratar-se-ia de um *ARP reply*.
- A outra forma existente de verificar se este se trata de um *ARP request* é indica pelo *Target MAC address*, no caso em que este seja composto por apenas zeros (00:00:00:00:00:00), o que se verifica.

1.2.3 Exercício 3

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

Alínea a)

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

```

▼ 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 1.12: Arp reply

R: O valor do campo *Opcode* é 2 (*Opcode*: reply(2)), indicando que o tipo de operação é um *ARP reply* ou seja, é uma resposta para um pedido *ARP*.

Alínea b)

"Em que posição da mensagem ARP está a resposta ao pedido ARP efetuado?"

R: A resposta ao pedido efetuado anteriormente é respondido através do campo *MAC* origem, pelo facto de a resposta ser entregue apenas pelo dispositivo correspondente ao endereço *IP* entregue.

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."

```

root@Shrek:/tmp/pycore.39159/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.39159/Shrek.conf# █

```

Figura 1.13: Tabela de encaminhamento gerada por *netstat -rn*

```

root@Shrek:/tmp/pycore.39159/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 fe80::200:ff:feaa:0 prefixlen 64 scopeid 0x20<link>
    inet6 2001::20 prefixlen 64 scopeid 0x0<global>
    ether 00:00:00:aa:00:00 txqueuelen 1000 (Ethernet)
    RX packets 2356 bytes 191366 (191,3 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 24 bytes 1873 (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 4 bytes 324 (324,0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 324 (324,0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@Shrek:/tmp/pycore.39159/Shrek.conf#

```

Figura 1.14: Output gerado por *ifconfig*

```

root@Shrek:/tmp/pycore.39159/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.39159/Shrek.conf#

```

Figura 1.15: Comando *arp*

R: O endereço MAC origem corresponde ao do Shrek e o endereço MAC destino corresponde ao n1 (router).

Alínea d)

"Justifique o modo de comunicação (unicast vs. broadcast) usado no envio da resposta ARP (ARP Reply)."

R: A resposta ARP (ARP reply) é transmitida utilizando o modo de comunicação unicast porque é destinada apenas ao dispositivo que fez a solicitação inicial. Em contraste, um pedido ARP (ARP request) é enviado como broadcast para alcançar todos os dispositivos na rede local, já que o solicitante não possui informações sobre qual dispositivo detém o endereço IP necessário. A eficácia das comunicações é aumentada pelo uso de unicast nas respostas ARP, pois garante que apenas o dispositivo requerente receba a mensagem, evitando tráfego desnecessário na rede. Além disso, a privacidade é mantida, pois o endereço MAC do dispositivo alvo é compartilhado somente com o solicitante, e não com toda a rede.

1.2.4 Exercício 4

"O Burro recebeu toda a informação trocada na interação anterior? Qual será a razão para tal?"

17	16.389666849	10.0.0.1	224.0.0.5	OSPF	78	Hello Packet
18	17.165409734	00:00:00_aa:00:00	Broadcast	ARP	42	Who has 10.0.0.1? Tell 10.0.0.20
19	17.929627308	fe80::c0e8:7fff:fe6...	ff02::2	ICMPv6	70	Router Solicitation from ca:e8:7f:62:4f:70

Figura 1.16: Captura da interface sobre o Burro

R: Sim, recebe toda a informação pois é inicialmente enviado como endereço destino, a nível de Ethernet, o Broadcast. Isto é, o Shrek envia para todos os dispositivos da sua rede local. Após o Burro receber o pacote e verificar que o endereço deste não corresponde ao endereço do destino, este acaba por descartar o pacote.

1.2.5 Exercício 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"

7	5.747072539	fe80::3c34:0a1f:fe5...	ff02::1b	MUNS	107	Standard query 0x0000 PTR 1005.1
8	5.900220590	00:00:00_aa:00:03	Broadcast	ARP	42	Who has 10.0.1.10? Tell 10.0.1.1
9	5.900230126	00:00:00_aa:00:05	00:00:00_aa:00:03	ARP	42	10.0.1.10 is at 00:00:00:aa:00:05
10	5.900233471	10.0.0.20	10.0.1.10	TCP	74	30882 -> 80 [SYN] Seq=84740

Figura 1.17: Captura da interface do PC da Fiona

R: Como é possível observar o PC da Fiona recebe os mesmos pacotes de request e reply de ARP do Pantanews devido à maneira como o hub age. Este acaba por descartar os pacotes recebidos, após o reconhecimento de que estes pacotes não são para este (Pc da Fiona).

1.2.6 Exercício 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."

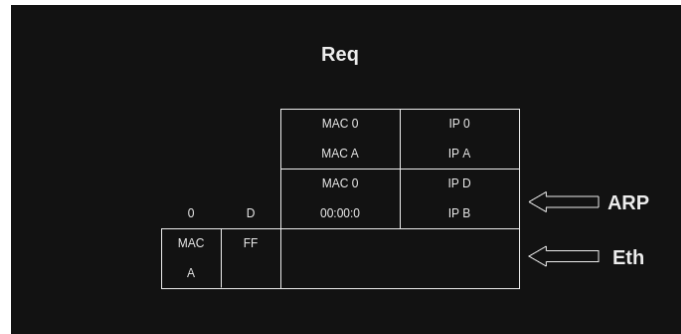


Figura 1.18: Primeiro SET de troca de pacotes

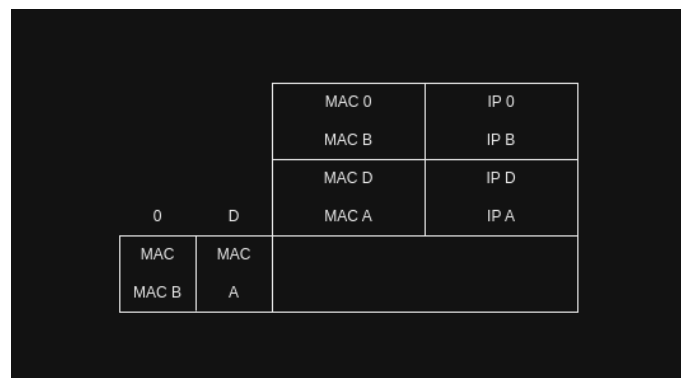


Figura 1.19: Segundo SET de troca de pacotes

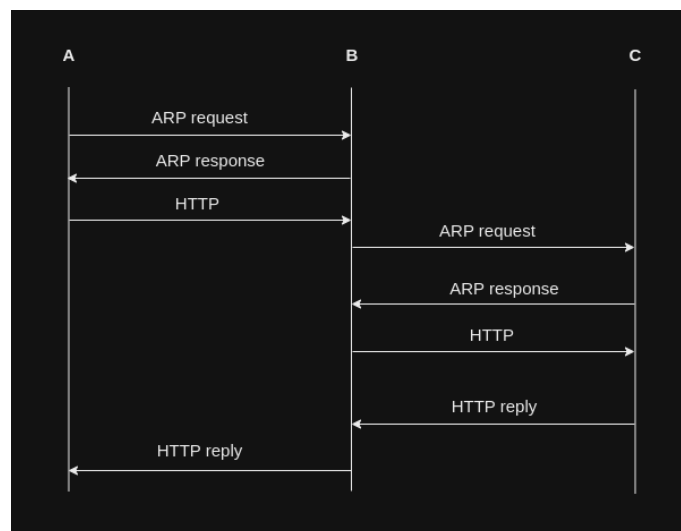


Figura 1.20: Diagrama de todas as mensagens trocadas

R: Como é possível observar pela tabela, primeiro é realizado um ARP request do sistema A (Shrek), para o sistema B (n1), seguido de um ARP reply do sistema B para o sistema A,

completando com um HTTP do sistema A para o sistema B. De seguida, o sistema B envia um ARP request para o sistema C (Pantanews), e recebe de volta do sistema C um ARP reply, em que de seguida envia o HTTP entregue pelo sistema A para o sistema C. Por fim, o sistema C envia o HTTP reply para o sistema B, que o redireciona para o sistema A.

1.2.7 Exercício 7

"Construa manualmente a tabela de comutação do switch da casa do Shrek, atribuindo números de porta à sua escolha."

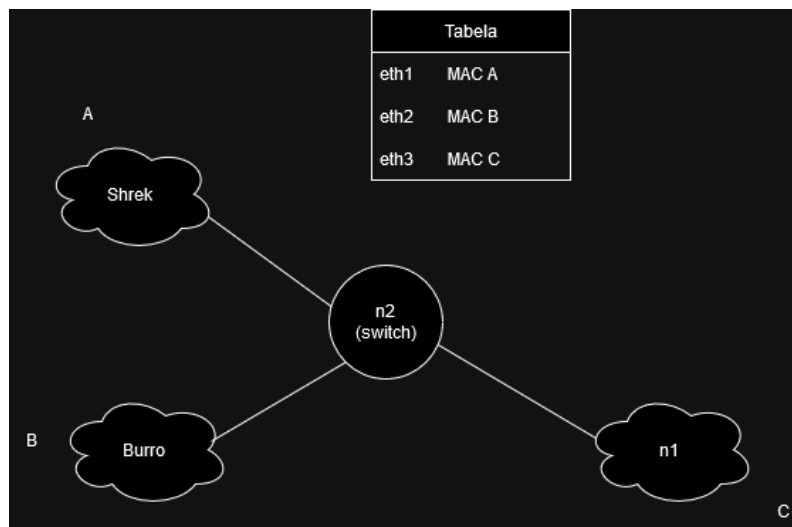


Figura 1.21: Tabela de comutação

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

"A Fiona decide ir morar com o Shrek e o Burro, mas com a condição de deixarem de ter os cabos Ethernet espalhados pela casa. O Shrek decide então comprar equipamento Wireless e faz uma captura de tráfego para perceber melhor o seu funcionamento. Descarregue da plataforma de ensino a captura WLAN-traffic-20240415.pcapng.zip e abra o ficheiro .pcapng no Wireshark."

2.1 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 XX correspondente ao seu identificador de grupo (TurnoGrupo, e.g., 11)."

2.1.1 Exercício 1

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

```

v Radiotap Header v0, Length 56
  Header revision: 0
  Header pad: 0
  Header length: 56
  > Present flags
    MAC timestamp: 1100794564
  > Flags: 0x12
    Data Rate: 24.0 Mb/s
    Channel frequency: 2412 [BG 1]
  v Channel flags: 0x0480, 2 GHz spectrum, Dynamic CCK-OFDM
    .... = 700 MHz spectrum: False
    ...0. = 800 MHz spectrum: False
    ...0.. = 900 MHz spectrum: False
    ....0 = Turbo: False
    ...0. = Complementary Code Keying (CCK): False
    ...0.. = Orthogonal Frequency-Division Multiplexing (OFDM): False
    ....1 = 2 GHz spectrum: True
    ...0. = 5 GHz spectrum: False
    ...0. = Passive: False
    ....1 = Dynamic CCK-OFDM: True
    ...0. = Gaussian Frequency Shift Keying (GFSK): False
    ...0. = GSM (900MHz): False
    ...0. = Static Turbo: False
    ...0. = Half Rate Channel (10MHz Channel Width): False
    ...0. = Quarter Rate Channel (5MHz Channel Width): False
  Antenna signal: -75 dBm
  Antenna noise: -94 dBm

```

Figura 2.1: Informação da trama 74 - RadioTap Header

R: No campo de 'HeaderTap', o frame analisado (Frame 74), apresenta uma frequência de 2.412 GHz, que corresponde ao canal 1. Informações relevantes -> Channel flags: 0x0480, 2 GHz spectrum, Dynamic CCK-OFDM.

2.1.2 Exercício 2

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

```

v 802.11 radio information
  PHY type: 802.11g (ERP) (6)
  Proprietary mode: None (0)
  Data rate: 24.0 Mb/s
  Channel: 1
  Frequency: 2412MHz
  Signal strength (dBm): -75 dBm
  Noise level (dBm): -94 dBm
  Signal/noise ratio (dB): 19 dB
  TSF timestamp: 1100794564
  > [Duration: 28µs]

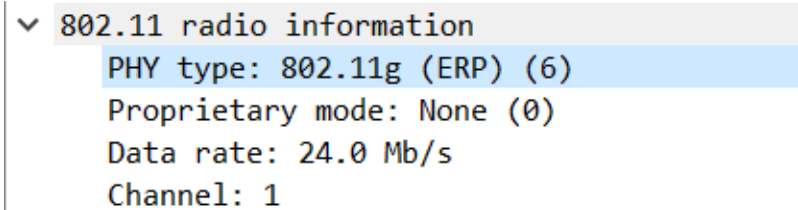
```

Figura 2.2: 802.11 radio information

R: Acima, através do campo PHY type, conclui-se que a versão da norma IEEE 802.11 a ser usada é a 802.11g.

2.1.3 Exercício 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."



```
▼ 802.11 radio information
  PHY type: 802.11g (ERP) (6)
  Proprietary mode: None (0)
  Data rate: 24.0 Mb/s
  Channel: 1
```

Figura 2.3: Taxa de transmissão

R: A taxa de transmissão em que foi enviada a trama, foi de 24.0 Mb/s, porém para o tipo de protocolo de rede usada, neste caso 802.11g, a taxa de transmissão máxima possível é 54 Mb/s. Conclui-se que não corresponde ao valor máximo.

2.2 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 XX o seu nº de TurnoGrupo (PLXX), responda às seguintes questões:"

2.2.1 Exercício 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)?"

674 1.410490	PTInovac_67:77:62	Broadcast	802.11	230 Beacon frame, SN=161
<pre> > Frame 674: 230 bytes on wire (1840 bits), 230 bytes captured (1840 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: 0x0000 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_67:77:62 (00:06:91:67:77:62) Source address: PTInovac_67:77:62 (00:06:91:67:77:62) BSS Id: PTInovac_67:77:62 (00:06:91:67:77:62) 0000 = Fragment number: 0 0110 0100 1100 = Sequence number: 1612 Frame check sequence: 0xca21fae7 [unverified] [FCS Status: Unverified] > IEEE 802.11 Wireless Management </pre>				

Figura 2.4: Informação da trama 674

R: Foi selecionada a trama 674. Esta pertence ao tipo 'Management frame'. O valor do identificador do tipo é 0. O valor do identificador de subtipo é 8, indicando que a trama pertence às tramas de gestão que são anúncios (beacons).

2.2.2 Exercício 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")"

```

.... .... 0000 = Fragment number: 0
0110 0100 1100 .... = Sequence number: 1612
Frame check sequence: 0xca21fae7 [unverified]
[FCS Status: Unverified]

```

Figura 2.5: Antes da ativação da verificação

```

0110 0100 1100 .... = Sequence number: 1612
Frame check sequence: 0xca21fae7 [correct]
[FCS Status: Good]

```

Figura 2.6: Após a ativação da verificação

R: O campo estava a ser utilizado, porém, não estava a ser verificado, como podemos ver, assim que foi ativado o campo, este mesmo demonstrou que como o seu estado encontra-se como 'Good', verifica-se que este estava pronto a ser usado.

2.2.3 Exercício 6

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

R: Em redes sem fio, assim como *Ethernet*, é possível receber pacotes corrompidos ou não receber os mesmos, porém isto acaba por ser uma questão de probabilidade, como com *Ethernet*, o meio de entrega é mais seguro e confiável, é mais difícil de acontecer perdas de pacotes e corrupção do mesmo. Já nas redes sem fio, é mais fácil de perder e corromper os pacotes devido a haver mais interferência com outros dispositivos.

2.2.4 Exercício 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."

```
▼ IEEE 802.11 Wireless Management
  ▼ Fixed parameters (12 bytes)
    Timestamp: 3249753194391
    Beacon Interval: 0.102400 [Seconds]
    > Capabilities Information: 0x1401
  ▼ Tagged parameters (154 bytes)
    > Tag: SSID parameter set: "MEO-WiFi"
    > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 18, 24, 36, 54, [Mbit/sec]
    > Tag: DS Parameter set: Current Channel: 1
```

Figura 2.7: Informação da trama com indicação da periodicidade e taxas de transmissão suportadas pelo AP da trama

R: Como verificado na captura, o intervalo *beacon* é de 0.102400 segundos e as taxas de transmissão suportadas são 1(B), 2(B), 5.5(B), 11(B), 18, 24, 36, 54, *Mbit/segundo*.

2.2.5 Exercício 8

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

BSSID	Channel	SSID
> 00:06:91:67:77:60	1	MEO-677760
> 00:06:91:67:77:62	1	MEO-WiFi
> 00:06:91:82:88:30	1	MEO-828830
> 00:06:91:82:88:32	1	MEO-WiFi
> 00:06:91:9b:f2:a0	1	MEO-9BF2A0
> 00:06:91:9b:f2:a2	1	MEO-WiFi
> 00:06:91:9e:9b:b0	1	MEO-9E9BB0
> 00:06:91:9e:9b:b2	1	MEO-WiFi
> 00:06:91:f1:75:70	1	MEO-F17570
> 00:06:91:f1:75:72	1	MEO-WiFi
> 7c:16:89:f8:7f:24		<Broadcast>
> 7c:db:98:40:93:f3	1	NOS-93F3
> 94:a4:f9:16:a9:b4	1	GV Casa
> a6:ef:15:08:32:99	1	phi_F41927C3C6...
> b0:4e:26:a3:af:08	2	TP-LINK_AP_AF08
> b0:76:1b:52:87:80	1	Vodafone-528777
> c8:70:23:1f:a2:70	1	MEO-1FA270
> c8:70:23:1f:a2:72	1	MEO-WiFi
> ca:c9:a3:7a:03:2a	1	shellyswitch25-C...
> cc:19:a8:ac:4b:50	1	Sky
> cc:19:a8:ac:4b:52	1	MEO-WiFi
> d8:78:7f:00:5d:a0	1	MEO-9BF2A0
> da:78:7f:00:5d:a2	1	MEO-WiFi
> fc:77:7b:ed:1c:a6	1	NOS-1CA6
> ff:ff:ff:ff:ff:ff	1	<Broadcast>
> ff:ff:ff:ff:ff:ff		Vodafone-B56E07
> ff:ff:ff:ff:ff:ff	1	FlyingNet

Figura 2.8: Lista de SSIDs

R: É possível observar várias redes com a mesma *SSID*, pois dá-se que apesar de ser a mesma rede, esta é anunciada por *APs* diferentes, resultando em leituras separadas da mesma.

2.2.6 Exercício 9

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

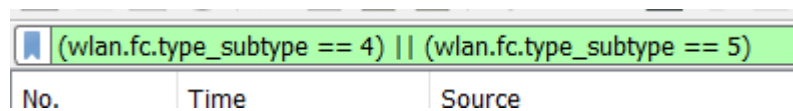


Figura 2.9: Filtro Wireshark utilizado

R: O filtro usado é o seguinte "(wlan.fc.type_subtype == 4) || (wlan.fc.type_subtype == 5)".

2.2.7 Exercício 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."

R: De acordo com as seguintes informações obtidas:

- MEO-677760 -> -88 dBm
- MEO-Wifi -> -69 dBm
- MEO-9E9BB0 -> -88 dBm
- GV Casa -> -88 dBm
- TP-LINK_AP_AF08 -> -80 dBm

Assim sendo, a melhor rede para se conectar será a MEO-Wifi, pois a 'Signal Strength' é a mais alta de entre as disponíveis.

2.2.8 Exercício 11

"Os valores de taxa de transmissão do Wi-Fi estão diretamente associados à qualidade da recepção 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."

R:

- Força de sinal: -69 dBm -> 16-QAM
- Data rate teórico = 26 mb/s
- Data rate real = 1.0 mb/s

2.3 Processo de Associação

"Numa rede Wi-Fi estruturada, um nodo ou STA deve associar-se a um ponto de acesso antes de enviar dados. O processo de associação nas redes IEEE 802.11 é executada enviando a trama association request da STA para o AP e a trama association response enviada pelo AP para a STA, em resposta ao pedido de associação recebido. Este processo é antecedido por uma fase de autenticação. Para a sequência de tramas capturada:"

2.3.1 Exercício 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."

12851 98.356049	92:97:e1:69:c3:d5	Broadcast	802.11	166 Probe Request, SN=3107, FN=0, Flags=.....C, SSID="MEO-WiFi"
12852 98.356172	PTInovac_67:77:62	92:97:e1:69:c3:d5	802.11	224 Probe Response, SN=3666, FN=0, Flags=.....C, BI=100, SSID="MEO-WiFi"
12853 98.356176		PTInovac_67:77:62 (-	802.11	48 Acknowledgement, Flags=.....C
12854 98.362240		Broadcast_04:c3:d5 (-	802.11	68 Clear-to-send, Flags=.....C
12855 98.374622	92:97:e1:69:c3:d5	PTInovac_67:77:62	802.11	105 Authentication, SN=674, FN=0, Flags=.....C
12856 98.374625		92:97:e1:69:c3:d5 (-	802.11	48 Acknowledgement, Flags=.....C
12857 98.374728	PTInovac_67:77:62	92:97:e1:69:c3:d5	802.11	81 Authentication, SN=3667, FN=0, Flags=.....C
12858 98.374732		PTInovac_67:77:62 (-	802.11	48 Acknowledgement, Flags=.....C

Figura 2.10: Sequência de tramas

R: É possível observar na imagem acima a sequência de tramas pedida, incluindo assim todos os passos responsáveis pelo funcionamento do mesmo.

2.3.2 Exercício 13

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

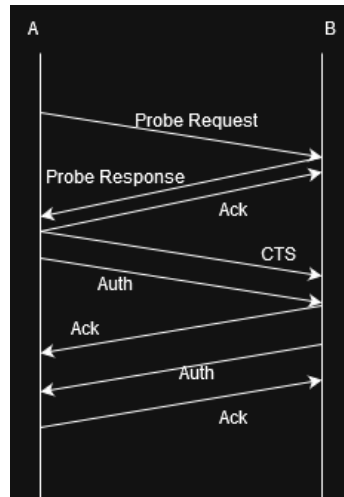


Figura 2.11: Diagrama de sequências das tramas trocadas

2.4 Transferência de Dados

"O trace disponibilizado, para além de tramas de gestão da ligação de dados, inclui tramas de dados e tramas de controlo da transferência desses mesmos dados."

2.4.1 Exercício 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?"

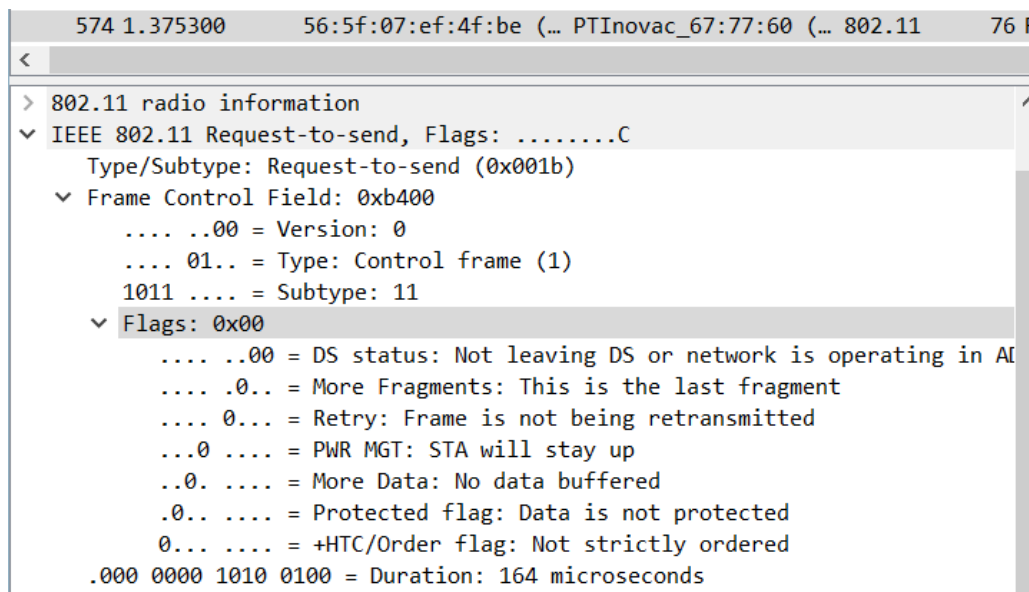


Figura 2.12: Informação da trama 574

R: Sobre a trama 574, encontrada através do uso do seguinte filtro:

- Filtro usado: (wlan.fc.type_subtype == 32) || (wlan.fc.type_subtype == 40)

Como nenhum endereço de destino é fornecido, isto sugere que a trama não é direcionada a uma certa *WLAN*, mas sim para todos os dispositivos disponíveis dentro do seu alcance.

2.4.2 Exercício 15

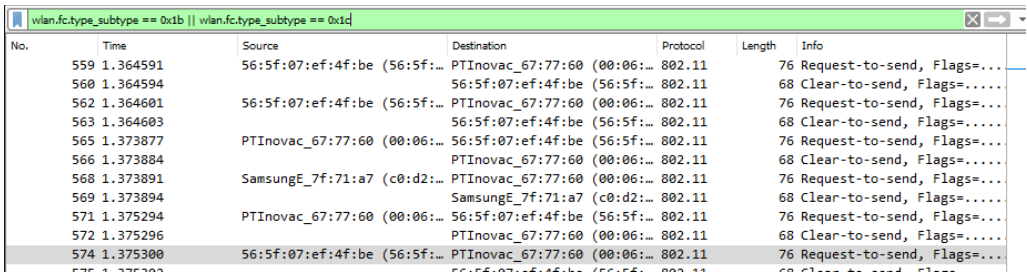
"Para a trama de dados selecionada, transcreva os endereços MAC em uso, identificando quais os endereços correspondentes à estação sem fios (STA), ao AP e ao router de acesso ao sistema de distribuição (DS)?"

R: Para a trama 574, encontra-se a seguinte informação:

- Endereço MAC da STA: *Transmitter address*: 56:5f:07:ef:4f:be (56:5f:07:ef:4f:be)
- Endereço MAC do AP: *Receiver address*: PTInovac_67:77:60 (00:06:91:67:77:60)
- Endereço MAC do router de acesso ao sistema de distribuição(DS): Este não se encontra definido

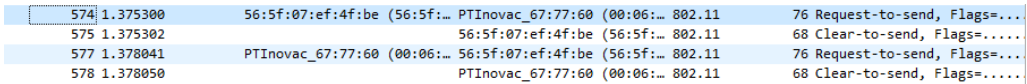
2.4.3 Exercício 16

"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."



No.	Time	Source	Destination	Protocol	Length	Info
559	1.364591	56:5f:07:ef:4f:be (56:5f:...	PTInovac_67:77:60 (00:06:...	802.11	76	Request-to-send, Flags=...
560	1.364594	56:5f:07:ef:4f:be (56:5f:...	56:5f:07:ef:4f:be (56:5f:...	802.11	68	Clear-to-send, Flags=.....
562	1.364601	56:5f:07:ef:4f:be (56:5f:...	PTInovac_67:77:60 (00:06:...	802.11	76	Request-to-send, Flags=...
563	1.364603	56:5f:07:ef:4f:be (56:5f:...	56:5f:07:ef:4f:be (56:5f:...	802.11	68	Clear-to-send, Flags=.....
565	1.373877	PTInovac_67:77:60 (00:06:...	56:5f:07:ef:4f:be (56:5f:...	802.11	76	Request-to-send, Flags=...
566	1.373884	PTInovac_67:77:60 (00:06:...	PTInovac_67:77:60 (00:06:...	802.11	68	Clear-to-send, Flags=.....
568	1.373891	SamsungE_7f:71:a7 (c0:d2:...	PTInovac_67:77:60 (00:06:...	802.11	76	Request-to-send, Flags=...
569	1.373894	SamsungE_7f:71:a7 (c0:d2:...	SamsungE_7f:71:a7 (c0:d2:...	802.11	68	Clear-to-send, Flags=.....
571	1.375294	PTInovac_67:77:60 (00:06:...	56:5f:07:ef:4f:be (56:5f:...	802.11	76	Request-to-send, Flags=...
572	1.375296	PTInovac_67:77:60 (00:06:...	PTInovac_67:77:60 (00:06:...	802.11	68	Clear-to-send, Flags=.....
574	1.375300	56:5f:07:ef:4f:be (56:5f:...	PTInovac_67:77:60 (00:06:...	802.11	76	Request-to-send, Flags=...

Figura 2.13: Tramas resultantes do filtro



574	1.375300	56:5f:07:ef:4f:be (56:5f:...	PTInovac_67:77:60 (00:06:...	802.11	76	Request-to-send, Flags=...
575	1.375302	56:5f:07:ef:4f:be (56:5f:...	56:5f:07:ef:4f:be (56:5f:...	802.11	68	Clear-to-send, Flags=.....
577	1.378041	PTInovac_67:77:60 (00:06:...	56:5f:07:ef:4f:be (56:5f:...	802.11	76	Request-to-send, Flags=...
578	1.378050	PTInovac_67:77:60 (00:06:...	PTInovac_67:77:60 (00:06:...	802.11	68	Clear-to-send, Flags=.....

Figura 2.14: Transferência de dados com CTS/RTS

12852	98.356172	PTInovac_67:77:62	92:97:e1:69:c3:d5	802.11	224	Probe Response, SN=3666, FN=0, Flags=...
12853	98.356176	PTInovac_67:77:62 (...)	802.11	48	Acknowledgement, Flags=.....C	
12854	98.362240	Broadcom_04:c3:d5 (...)	802.11	68	Clear-to-send, Flags=.....C	
12855	98.374622	92:97:e1:69:c3:d5	PTInovac_67:77:62	802.11	105	Authentication, SN=674, FN=0, Flags=....
12856	98.374625	92:97:e1:69:c3:d5 (...)	802.11	48	Acknowledgement, Flags=.....C	

Figura 2.15: Transferência de dados sem CTS/RTS

3 Conclusões retiradas

Este trabalho prático proporcionou-nos uma exploração detalhada e aplicada dos conceitos fundamentais de redes Ethernet e Wi-Fi, com um foco em especial no Protocolo ARP e na camada de ligação de dados. As atividades realizadas permitiram-nos solidificar o entendimento teórico através da prática direta, utilizando ferramentas como Wireshark para captura e análise de tráfego de rede. Esta componente prática permitiu explorar uma variedade de tramas e os procedimentos de controlo, sendo possível perceber como esses elementos influenciam diretamente na comunicação entre os dispositivos em redes wireless e Ethernet. Assim, ao enfrentarmos os desafios na implementação e manutenção de redes de computadores, reconhecemos a importância de dominar esses conhecimentos fundamentais.