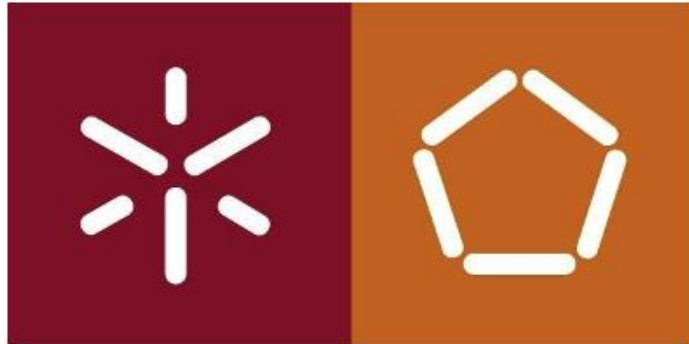
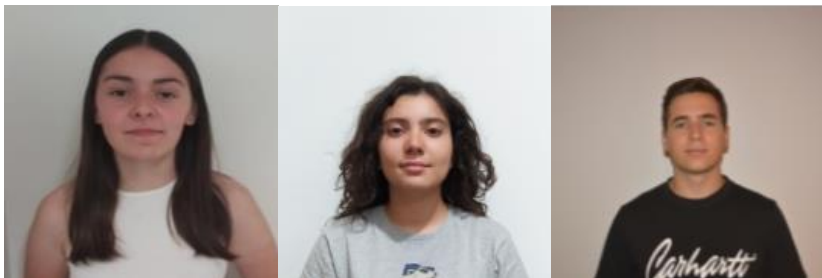


Universidade do Minho

Licenciatura em Engenharia Informática



TP3 -Nível de Ligação Lógica: Redes Ethernet, Protocolo ARP e Redes Locais sem Fios (Wi-Fi)



Trabalho realizado por:
Margarida Cunha da Silva, A104357
Maria Leonor Carvalho da Cunha, A103997
Tiago Rodrigues Barros, A104530.

Redes de Computadores

PL9 - Grupo 91
April 16, 2024

Índice

1. Parte 1.....	3
1.1. Exercício 1	3
1.2. Exercício 2	4
2. Parte 2.....	11
2.1. Exercício 1	11
2.2. Exercício 2	13
2.3. Exercício 3	16
2.4. Exercício 4	18
Conclusão	20

1. Parte 1

1.1. Exercício 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 os primeiros dados HTTP referentes à página alojada no servidor.

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

31 27.404244915	10.0.0.20	10.0.1.10	TCP	74 44796 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=325568095 TSecr=0 WS=128
32 27.404273755	10.0.1.10	10.0.0.20	TCP	74 80 → 44796 [SYN, ACK] Seq=0 Ack=1 Win=65152 Len=0 MSS=1460 SACK_PERM=1 TSval=959433019 TSecr=325568095 WS=128
33 27.404288880	10.0.0.20	10.0.1.10	TCP	66 44796 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=325568095 TSecr=959433019
34 27.404322318	10.0.0.20	10.0.1.10	HTTP	139 661 → 80 [HTTP/1.1] Seq=1 Ack=74 Win=65152 Len=0 TSval=959433019 TSecr=325568095
35 27.404344519	10.0.1.10	10.0.0.20	TCP	66 80 → 44796 [ACK] Seq=1 Ack=74 Win=65152 Len=0 TSval=959433019 TSecr=325568095
36 27.404586412	10.0.1.10	10.0.0.20	HTTP	552 HTTP/1.1 200 OK
37 27.404634475	10.0.0.20	10.0.1.10	TCP	66 44796 → 80 [ACK] Seq=74 Ack=487 Win=63872 Len=0 TSval=325568096 TSecr=959433020
38 27.406080600	10.0.0.20	10.0.1.10	TCP	66 44796 → 80 [FIN, ACK] Seq=74 Ack=487 Win=64128 Len=0 TSval=325568097 TSecr=959433020
39 27.406093751	10.0.1.10	10.0.0.20	TCP	66 80 → 44796 [FIN, ACK] Seq=487 Ack=75 Win=65152 Len=0 TSval=959433021 TSecr=325568097
40 27.406043858	10.0.0.20	10.0.1.10	TCP	66 44796 → 80 [ACK] Seq=75 Ack=488 Win=64128 Len=0 TSval=325568097 TSecr=959433021

Figure 1: Pacote TCC

▶ Frame 34: 139 bytes on wire (1112 bits), 139 bytes captured (1112 bits) on interface veth2.0.42, id 0
▼ Ethernet II, Src: 00:00:00:aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00:aa:00:02 (00:00:00:aa:00:02)
▶ Destination: 00:00:00:aa:00:02 (00:00:00:aa:00:02)
▶ Source: 00:00:00:aa:00:00 (00:00:00:aa:00:00)
Type: IPv4 (0x0800)
▶ Internet Protocol Version 4, Src: 10.0.0.20, Dst: 10.0.1.10
▶ Transmission Control Protocol, Src Port: 44796, Dst Port: 80, Seq: 1, Ack: 1, Len: 63
▶ Hypertext Transfer Protocol

Figure 2: Trama capturada

Resposta: O endereço MAC do destino é 00:00:00:aa:00:02 e refere-se ao endereço físico do router. O endereço MAC na origem é 00:00:00:aa:00:00, este refere-se ao endereço físico da máquina que estamos a utilizar para realizar a captura.

2. Qual o valor hexadecimal do campo Type da trama Ethernet? O que significa?

Resposta: O endereço é 0x0800 (Figure 2) e significa que a camada superior está a utilizar o protocolo IPv4.

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: Conforme a captura de rede fornecida, a trama em questão possui um tamanho total de 139 bytes. No entanto, apenas 85 bytes são destinados aos dados do nível aplicacional, ou seja, o conteúdo da requisição HTTP.

Cálculo da sobrecarga: 85 bytes / 139 bytes \approx 0,6115
 Sobrecarga em porcentagem: 0,6115*100% = 61,15%

A análise revela que a pilha protocolar introduz uma sobrecarga significativa de 61,15% no tamanho total da trama.

0000	00 00 00 aa 00 02 00 00	00 aa 00 00 08 00 45 00E.
0010	00 7d 47 40 40 00 40 06	de 1d 0a 00 00 14 0a 00	}G@.@.....
0020	01 0a ae fc 00 50 02 f1	4c 0c ee 24 4c 37 80 18P..L..\$L7..
0030	01 f6 29 d2 00 00 01 01	08 0a 13 67 c6 5f 39 2f	..).....g_9/
0040	c9 3b 47 45 54 20 2f 20	48 54 54 50 2f 31 2e 31	.;GET / HTTP/1.1
0050	0d 0a 48 6f 73 74 3a 20	31 30 2e 30 2e 31 2e 31	..Host: 10.0.1.1
0060	30 0d 0a 55 73 65 72 2d	41 67 65 6e 74 3a 20 63	0..User- Agent: c
0070	75 72 6c 2f 37 2e 36 38	2e 30 0d 0a 41 63 63 65	url/7.68 .0..Acce
0080	70 74 3a 20 2a 2f 2a 0d	0a 0d 0a	pt: */* ...

Figure 3: Valores dos bytes da trama em estudo

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

```

> Frame 36: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface veth2.0.42, id 0
> 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)
  > Source: 00:00:00_aa:00:02 (00:00:00:aa:00:02)
  Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 10.0.1.10, Dst: 10.0.0.20
> Transmission Control Protocol, Src Port: 80, Dst Port: 44796, Seq: 1, Ack: 74, Len: 486
> Hypertext Transfer Protocol
  
```

Figure 4: Resposta HTTP

Resposta: Como podemos ver na figura 4, o endereço é 00:00:00:aa:00:02 e corresponde ao endereço físico do router com que estamos a comunicar.

5. Qual é o endereço MAC do destino? A que interface corresponde?

Resposta: O endereço MAC do destino é 00:00:00:aa:00:00 e corresponde ao endereço físico da nossa máquina.

1.2. Exercício 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	0.000000000	10.0.0.1	224.0.0.5	OSPF	78 Hello Packet
2	0.020725945	fe80::20::ff02::5		OSPF	90 Hello Packet
3	2.001279893	10.0.0.1	224.0.0.5	OSPF	78 Hello Packet
4	2.209044482	fe80::20::ff02::2		ICMPv6	70 Router Solicitation from 00:00:00:aa:00:00
5	2.720923544	fe80::7c::ff02::2		ICMPv6	70 Router Solicitation from 0a:da:9f:54:62:da
6	2.720930336	fe80::20::ff02::2		ICMPv6	70 Router Solicitation from 00:00:00:aa:00:01
7	3.408709343	fe80::a0::ff02::2		ICMPv6	70 Router Solicitation from a2:a9:45:22:fc:f5
8	4.002431971	10.0.0.1	224.0.0.5	OSPF	78 Hello Packet
9	5.288948647	fe80::7c::ff02::fb		MONS	107 Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR _ipp._tcp.local, "QM" question
10	5.389161274	fe80::a0::ff02::fb		MONS	107 Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR _ipp._tcp.local, "QM" question
11	6.003632634	10.0.0.1	224.0.0.5	OSPF	78 Hello Packet
12	8.004997352	10.0.0.1	224.0.0.5	OSPF	78 Hello Packet
13	10.005209939	10.0.0.1	224.0.0.5	OSPF	78 Hello Packet
14	10.020906715	fe80::20::ff02::5		OSPF	90 Hello Packet
15	12.006315056	10.0.0.1	224.0.0.5	OSPF	78 Hello Packet
16	14.006813344	10.0.0.1	224.0.0.5	OSPF	78 Hello Packet
17	15.048603531	00:00:00::	Broadcast	ARP	42 Who has 10.0.0.1? Tell 10.0.0.20
18	15.048628017	00:00:00::	00:00:00:aa::	ARP	42 10.0.0.1 is at 00:00:00:aa:00:02
19	15.048630812	10.0.0.20	10.0.1.10	TCP	74 38510 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=397065572 TSecr=0 WS=128
20	15.048631660	10.0.1.10	10.0.0.20	TCP	74 80 - 38510 [SYN, ACK] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1238760052 TSecr=397065572 WS=128
21	15.048660693	10.0.0.20	10.0.1.10	TCP	60 38510 - 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=397065572 TSecr=1238760052
22	15.048689171	10.0.0.20	10.0.1.10	HTTP	130 GET / HTTP/1.1
23	15.048705051	10.0.1.10	10.0.0.20	TCP	60 80 - 38510 [ACK] Seq=1 Ack=74 Win=61512 Len=0 TSval=1238760052 TSecr=397065572
24	15.048919782	10.0.1.10	10.0.0.20	HTTP	552 HTTP/1.1 200 OK
25	15.048926343	10.0.0.20	10.0.1.10	TCP	60 38510 - 80 [ACK] Seq=74 Ack=487 Win=63872 Len=0 TSval=397065572 TSecr=1238760052
26	15.048953048	10.0.0.20	10.0.1.10	TCP	60 38510 - 80 [FIN, ACK] Seq=74 Ack=487 Win=64128 Len=0 TSval=1238760052 TSecr=1238760052
27	15.048980440	10.0.1.10	10.0.0.20	TCP	60 80 - 38510 [FIN, ACK] Seq=487 Ack=75 Win=61512 Len=0 TSval=238760053 TSecr=397065573
28	15.048983746	10.0.0.20	10.0.1.10	TCP	60 38510 - 80 [ACK] Seq=75 Ack=488 Win=64128 Len=0 TSval=397065573 TSecr=1238760053
29	16.007668651	10.0.0.1	224.0.0.5	OSPF	78 Hello Packet
30	17.312605078	fe80::20::ff02::2		ICMPv6	70 Router Solicitation from 00:00:00:aa:00:00
31	18.009108232	10.0.0.1	224.0.0.5	OSPF	78 Hello Packet
32	18.593068935	fe80::7c::ff02::2		ICMPv6	70 Router Solicitation from 0a:da:9f:54:62:da
33	18.593102297	fe80::20::ff02::2		ICMPv6	70 Router Solicitation from 00:00:00:aa:00:01
34	19.972791191	fe80::20::ff02::5		OSPF	90 Hello Packet
35	20.009449663	10.0.0.1	224.0.0.5	OSPF	78 Hello Packet
36	20.129847095	00:00:00::	00:00:00:aa::	ARP	42 Who has 10.0.0.20? Tell 10.0.0.1
37	20.129959096	00:00:00::	00:00:00:aa:00:00	ARP	42 10.0.0.20 is at 00:00:00:aa:00:00
38	21.206463910	fe80::7c::ff02::fb		MONS	107 Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR _ipp._tcp.local, "QM" question
39	21.389937895	fe80::a0::ff02::fb		MONS	107 Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR _ipp._tcp.local, "QM" question
40	22.013877092	10.0.0.1	224.0.0.5	OSPF	78 Hello Packet
41	22.176934218	fe80::a0::ff02::2		ICMPv6	70 Router Solicitation from a2:a9:45:22:fc:f5

Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface veth2.0.7f, id 0

Ethernet II, Src: 00:00:00:aa:00:02 (00:00:00:aa:00:02), Dst: IPv4mcast_05 (01:00:5e:00:00:05)

Destination: IPv4mcast_05 (01:00:5e:00:00:05)

Source: 00:00:00:aa:00:02 (00:00:00:aa:00:02)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 10.0.0.1, Dst: 224.0.0.5

Open Shortest Path First

0000 01 00 5e 00 00 05 00 00 00 aa 00 02 08 00 45 c0 ..A.....E

0010 00 40 5f e2 00 00 01 59 6e bd 0a 00 00 01 e0 00 @....Yn.....

0020 00 05 02 01 00 2c 0a 00 00 01 00 00 00 e8 c6[.....

0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02[.....

0040 02 01 00 00 00 0a 0a 00 00 01 00 00 00 00 00

Figure 5: Captura do tráfego na interface do Shrek

```

vcmd
root@Shrek:/tmp/pycore.33533/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.33533/Shrek.conf#
  
```

Figure 6: Aceder ao pantanews.com no Shrek através do comando curl

No.	Time	Source	Destination	Protocol	Length	Info
1	0.60099900	fe80::30	ff02::fb	MDNS	107	Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR _ipp._tcp.local, "QM" question
2	0.696517099	10.0.0.1	224.0.0.5	OSPF	78	Hello Packet
3	2.697215824	10.0.0.1	224.0.0.5	OSPF	78	Hello Packet
4	2.707265291	fe80::20	ff02::5	OSPF	90	Hello Packet
5	3.420429368	fe80::cf	ff02::2	ICMPv6	70	Router Solicitation from 32:a1:f0:f5:cf:d4
6	4.099436320	10.0.0.1	224.0.0.5	OSPF	78	Hello Packet
7	4.709478642	fe80::20	ff02::5	ICMPv6	70	Router Solicitation from 00:00:00:aa:00:01
8	5.468371834	fe80::30	ff02::2	ICMPv6	70	Router Solicitation from 32:a1:f0:f5:cf:d4
9	5.980381609	fe80::20	ff02::2	ICMPv6	70	Router Solicitation from 00:00:00:aa:00:00
10	5.709946940	10.0.0.1	224.0.0.5	OSPF	78	Hello Packet
11	6.912442985	fe80::cf	ff02::fb	MDNS	107	Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR _ipp._tcp.local, "QM" question
12	8.001032229	fe80::30	ff02::fb	MDNS	107	Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR _ipp._tcp.local, "QM" question
13	8.709722945	10.0.0.1	224.0.0.5	OSPF	78	Hello Packet
14	10.701801654	10.0.0.1	224.0.0.5	OSPF	78	Hello Packet
15	12.701848440	10.0.0.1	224.0.0.5	OSPF	78	Hello Packet
16	12.714641251	fe80::20	ff02::5	OSPF	90	Hello Packet
17	14.703087759	10.0.0.1	224.0.0.5	OSPF	78	Hello Packet
18	16.704185204	10.0.0.1	224.0.0.5	OSPF	78	Hello Packet
19	18.704731271	10.0.0.1	224.0.0.5	OSPF	78	Hello Packet
20	18.780355791	fe80::cf	ff02::2	ICMPv6	70	Router Solicitation from 32:a1:f0:f5:cf:d4
21	20.572657327	fe80::20	ff02::2	ICMPv6	70	Router Solicitation from 00:00:00:aa:00:01
22	20.705773534	10.0.0.1	224.0.0.5	OSPF	78	Hello Packet
23	21.084109907	fe80::30	ff02::2	ICMPv6	70	Router Solicitation from 32:a1:f0:f5:cf:d4
24	22.668840154	fe80::20	ff02::5	OSPF	90	Hello Packet
25	22.705935036	10.0.0.1	224.0.0.5	OSPF	78	Hello Packet
26	22.912247188	fe80::cf	ff02::fb	MDNS	107	Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR _ipp._tcp.local, "QM" question
27	24.002692566	fe80::30	ff02::fb	MDNS	107	Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR _ipp._tcp.local, "QM" question
28	24.707142841	10.0.0.1	224.0.0.5	OSPF	78	Hello Packet
29	25.436428415	fe80::20	ff02::2	ICMPv6	70	Router Solicitation from 00:00:00:aa:00:00
30	26.708527698	10.0.0.1	224.0.0.5	OSPF	78	Hello Packet
31	28.708618729	10.0.0.1	224.0.0.5	OSPF	78	Hello Packet
32	30.708802354	10.0.0.1	224.0.0.5	OSPF	78	Hello Packet
33	32.630921528	fe80::20	ff02::5	OSPF	90	Hello Packet
34	32.704351941	fe80::20	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
35	32.708884448	10.0.0.1	224.0.0.5	OSPF	78	Hello Packet
36	33.596436962	fe80::20	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
37	34.710368486	10.0.0.1	224.0.0.5	OSPF	78	Hello Packet
38	36.710898131	10.0.0.1	224.0.0.5	OSPF	78	Hello Packet

Frame 1: 107 bytes on wire (856 bits), 107 bytes captured (856 bits) on interface veth3.0.b9, id 0
 Ethernet II, Src: 32:a1:f0:f5:cf:d4 (32:a1:f0:f5:cf:d4), Dst: IPv6multicast_fb (33:33:00:00:00:fb)
 Destination: IPv6multicast_fb (33:33:00:00:00:fb)
 Source: 32:a1:f0:f5:cf:d4 (32:a1:f0:f5:cf:d4)
 Type: IPv6 (0x86dd)
 Internet Protocol Version 6, Src: fe80::30a1:feff:fe5:cf:d4, Dst: ff02::fb
 User Datagram Protocol, Src Port: 5353, Dst Port: 5353
 Multicast Domain Name System (query)

Figure 7: Captura do tráfego na interface do Burro

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.

```

</body></html>root@Shrek:/tmp/pycore.33533/Shrek.conf# arp -a
? (10.0.0.1) at 00:00:00:aa:00:02 [ether] on eth0
root@Shrek:/tmp/pycore.33533/Shrek.conf#
  
```

Figure 8: Comando `arp -a` no shrek

No.	Time	Source	Destination	Protocol	Length	Info
17	15.048603531	00:00:00:aa:00:00	Broadcast	ARP	42	Who has 10.0.0.1? Tell 10.0.0.20
18	15.048628017	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
36	20.129047895	00:00:00:aa:00:02	00:00:00:aa:00:00	ARP	42	Who has 10.0.0.20? Tell 10.0.0.1
37	20.129059006	00:00:00:aa:00:00	00:00:00:aa:00:02	ARP	42	10.0.0.20 is at 00:00:00:aa:00:00

Figure 9: tabela ARP

Resposta: A primeira coluna mostra os endereços IPs e a segunda coluna mostra os endereços MAC.

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: O valor hexadecimal do endereço MAC origem é 00:00:00:aa:00:00 e o endereço de destino MAC é ff:ff:ff:ff:ff:ff (Broadcast). Como o nosso dispositivo não está diretamente conectado ao dispositivo de destino, para onde enviamos a mensagem, é necessário enviar a mensagem para todos os dispositivos da rede até que o dispositivo pretendido responda ao seu endereço MAC, é por isso que o nosso endereço de destino é ff:ff:ff:ff:ff:ff.

```

▶ Frame 17: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface veth2.0.7f, id 0
▼ Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▶ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ▶ Source: 00:00:00_aa:00:00 (00:00:00:aa:00:00)
  Type: ARP (0x0806)
▼ Address Resolution Protocol (request)
  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

```

Figure 10: Trama com o pedido ARP

b. Qual o valor hexadecimal do campo Tipo da trama Ethernet? O que indica?

Resposta: O valor do campo tipo trama é 0x0806 e indica que a camada superior está a usar o protocolo ARP.

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: Trata-se efetivamente de um pedido ARP pois temos a indicação que é uma “request” na figura 10.

Para além disso, na mensagem ARP estão contidos os endereços IP e MAC e o protocolo ARP permite converter um endereço IP num endereço MAC.

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

```

▶ Frame 18: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface veth2.0.7f, id 0
▼ 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)
  ▶ Source: 00:00:00_aa:00:02 (00:00:00:aa:00:02)
  Type: ARP (0x0806)
▼ 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

```

Figure 11: 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 é 2. Assim podemos concluir que, o IP 10.0.0.20 recebe a mensagem de “request” e está a enviar o seu endereço MAC com resposta.

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

Resposta: A resposta ao pedido encontra-se entre os bytes 15 e 42, como podemos ver na imagem abaixo.

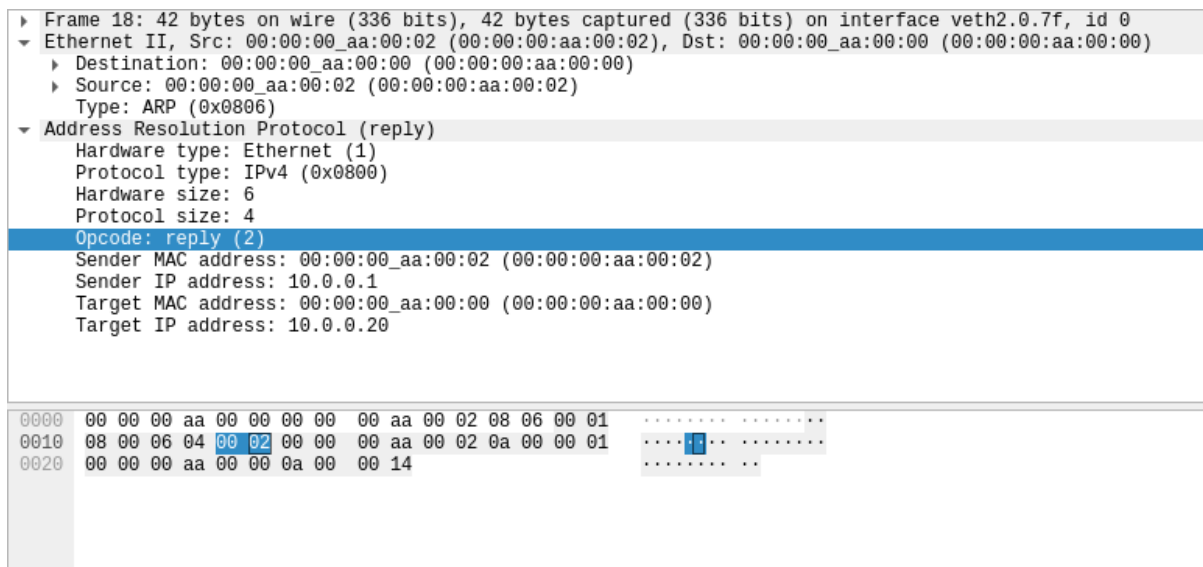


Figure 12: Trama com a resposta ARP

- 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.38945/Shrek.conf# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.0.20 netmask 255.255.255.0 broadcast 0.0.0.0
    inet6 2001::20 prefixlen 64 scopeid 0x0<global>
    inet6 fe80::200:ff:feaa:0 prefixlen 64 scopeid 0x20<link>
    ether 00:00:00:aa:00:00 txqueuelen 1000 (Ethernet)
    RX packets 4506 bytes 371136 (371.1 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 17 bytes 1382 (1.3 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@Shrek:/tmp/pycore.38945/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.38945/Shrek.conf# arp
root@Shrek:/tmp/pycore.38945/Shrek.conf#
```

Figure 13: comandos `ifconfig`, `netstat -rn`, `arp` no Shrek

Resposta: Com base na figura podemos concluir que o endereço ether é 00:00:00:aa:00:00, e é o endereço MAC de origem.

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

Resposta: A resposta ARP é encaminhada como unicast, ao contrário do pedido que é transmitido em broadcast. Isto garante que a resposta seja entregue diretamente ao dispositivo que solicitou, aumentando a eficiência e economizando recursos de rede. Optar por enviar a resposta como broadcast seria redundante e iria gerar tráfego desnecessário na rede, já que todos os dispositivos teriam que processar a mensagem ARP.

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

Resposta: Na captura de tráfego, podemos observar que o Burro envia um pacote ARP para o RACI solicitando o endereço MAC do PC2. Isso indica que o Burro não possui o endereço MAC do PC2 em sua tabela ARP. Sem o endereço MAC do PC2, o Burro não pode enviar pacotes para ele diretamente.

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.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.1.1	224.0.0.5	OSPF	78	Hello Packet
2	0.000102020	10.0.1.1	224.0.0.5	OSPF	78	Hello Packet
3	2.018897072	fe80::20:f02::5		OSPF	98	Hello Packet
4	4.001295525	10.0.1.1	224.0.0.5	OSPF	78	Hello Packet
5	6.002844057	10.0.1.1	224.0.0.5	OSPF	78	Hello Packet
6	8.004802836	10.0.1.1	224.0.0.5	OSPF	78	Hello Packet
7	8.592727199	00:00:00:00:00:00	Broadcast	ARP	42	Who has 10.0.1.10? Tell 10.0.1.1
8	8.592738734	00:00:00:00:00:00	aa:aa:aa:aa:aa:aa	ARP	42	10.0.1.10 is at 00:00:00:aa:aa:aa
9	8.592741751	10.0.0.20	10.0.1.10	TCP	74	60260 -> 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3104024483 TSecr=0 WS=128
10	8.592752374	10.0.1.10	10.0.0.20	TCP	74	80 -> 60260 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=318806422 TSecr=3104024483 WS=128
11	8.592765312	10.0.0.20	10.0.1.10	TCP	66	60260 -> 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3104024484 TSecr=318806422
12	8.592769815	10.0.0.20	10.0.1.10	HTTP	130	GET / HTTP/1.1
13	8.592808678	10.0.1.10	10.0.0.20	TCP	66	80 -> 60260 [ACK] Seq=1 Ack=74 Win=65152 Len=0 TSval=318806422 TSecr=3104024484
14	8.593048545	10.0.1.10	10.0.0.20	HTTP	552	HTTP/1.1 200 OK
15	8.593107865	10.0.0.20	10.0.1.10	TCP	66	60260 -> 80 [ACK] Seq=74 Ack=487 Win=63872 Len=0 TSval=3104024484 TSecr=318806422
16	8.594471143	10.0.0.20	10.0.1.10	TCP	66	60260 -> 80 [FIN, ACK] Seq=74 Ack=487 Win=64128 Len=0 TSval=3104024485 TSecr=318806422
17	8.594491668	10.0.1.10	10.0.0.20	TCP	66	80 -> 60260 [FIN, ACK] Seq=487 Ack=75 Win=65152 Len=0 TSval=318806423 TSecr=3104024485
18	8.594504767	10.0.0.20	10.0.1.10	TCP	66	60260 -> 80 [ACK] Seq=75 Ack=488 Win=64128 Len=0 TSval=318806423 TSecr=318806423
19	8.619763691	fe80::58:f02::2		ICMPv6	70	Router Solicitation from 5a:63:09:a6:ef:c1
20	10.005087565	10.0.1.1	224.0.0.5	OSPF	78	Hello Packet
21	10.023833508	fe80::f0:f02::2		ICMPv6	70	Router Solicitation from 5a:63:09:a6:ef:c1
22	11.692072575	fe80::20:f02::2		ICMPv6	70	Router Solicitation from 00:00:00:aa:00:05
23	12.005351202	10.0.1.1	224.0.0.5	OSPF	78	Hello Packet
24	12.005412168	fe80::20:f02::5		OSPF	98	Hello Packet
25	12.972058580	fe80::20:f02::2		ICMPv6	70	Router Solicitation from 00:00:00:aa:00:04
26	13.172077261	fe80::f0:f02::f0		MDNS	107	Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR _ipps._tcp.local, "QM" question
27	13.742387070	00:00:00:00:00:00	aa:aa:aa:aa:aa:aa	ARP	42	Who has 10.0.1.1? Tell 10.0.1.10
28	13.742413789	00:00:00:00:00:00	aa:aa:aa:aa:aa:aa	ARP	42	10.0.1.1 is at 00:00:00:aa:aa:aa
29	14.006630418	10.0.1.1	224.0.0.5	OSPF	78	Hello Packet
30	14.252889421	fe80::58:f02::f0		MDNS	107	Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR _ipps._tcp.local, "QM" question
31	16.007235305	10.0.1.1	224.0.0.5	OSPF	78	Hello Packet
32	18.008538072	10.0.1.1	224.0.0.5	OSPF	78	Hello Packet
33	20.009036433	10.0.1.1	224.0.0.5	OSPF	78	Hello Packet
34	22.003959118	fe80::20:f02::16		ICMPv6	98	Multicast Listener Report Message v2
35	22.008245667	fe80::20:f02::5		OSPF	98	Hello Packet
36	22.009049518	10.0.1.1	224.0.0.5	OSPF	78	Hello Packet

Frame 1: 78 bytes on wire (624 bits): 78 bytes captured (624 bits) on interface veth0.0.00, 10 s

Ethernet II, Src: 00:00:00:aa:00:03 (00:00:00:aa:00:03), Dst: IPv4mcast_05 (01:00:5e:00:00:05)

Destination: IPv4mcast_05 (01:00:5e:00:00:05)

Source: 00:00:00:aa:00:03 (00:00:00:aa:00:03)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 10.0.1.1, Dst: 224.0.0.5

Open Shortest Path First

0000 01 00 5e 00 00 05 00 00 00 aa 00 03 00 00 45 c0E

0010 00 00 fc 23 00 00 01 59 d1 7b 0a 00 01 01 e0 00 @ # . . Y {

0020 00 05 02 01 00 2c 0a 00 00 01 00 00 00 e7 c6

0030 00 00 00 00 00 00 00 00 00 ff ff 00 00 00 02

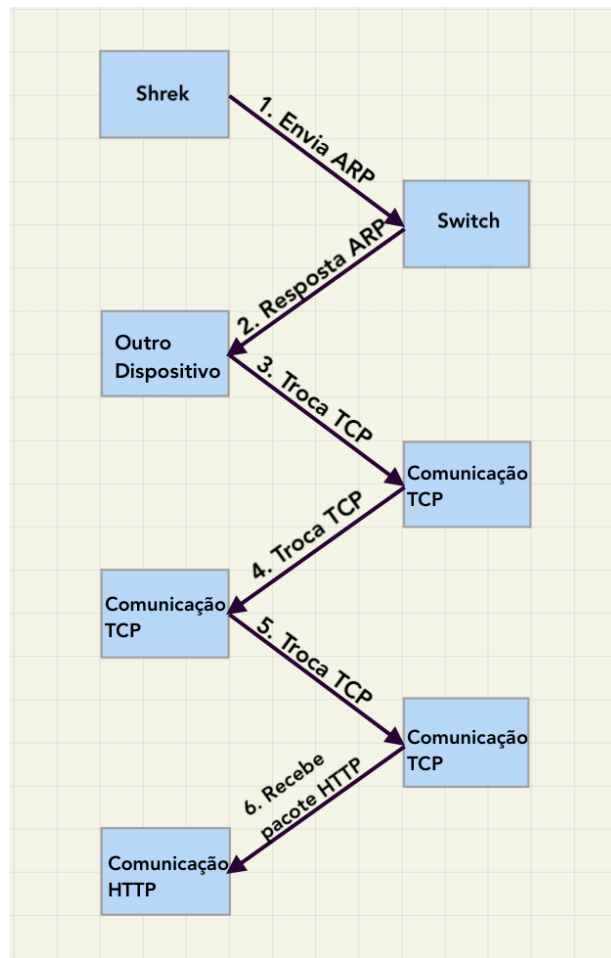
0040 02 01 00 00 00 00 0a 00 01 01 00 00 00 00

Figure 14: Captura do tráfego da interface Fiona

Resposta: A captura de tráfego da interface Fiona mostra que ela desempenha um papel ativo na rede. Ela troca pacotes OSPF com outros routers para construir e manter a topologia da rede, trocando pacotes TCP com outros hosts para transferir dados, acessando web servers e trocando mensagens ICMP com outros dispositivos para testar a conectividade e anunciar sua presença na rede.

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.

Resposta:



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

Resposta: Está associado a porta 1 do switch, o endereço MAC 00:00:00:aa:00:02. O endereço MAC 00:00:00:aa:00:00 está associado à porta 2 do switch.

A tabela abaixo, indica ao switch, tendo por base o endereço MAC de destino, por qual porta ele deve encaminhar os pacotes. Quando é recebido pelo switch um pacote com um endereço MAC 00:00:00:aa:00:02, ele encaminha-o para a porta 1, quando recebe um pacote com o endereço MAC 00:00:00:aa:00:00, ele encaminha-o para a porta 2.

MAC address	Porta
00:00:00:aa:00:02	1
00:00:00:aa:00:00	2

Tabela 1: Tabela de comutação de Switch

2. Parte 2

2.1. Exercício 1

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.

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).

No.	Time	Source	Destination	Protocol	Length	Info
859	1.715832	PTInovac_67:77:60	Broadcast	802.11	305	Beacon frame, SN=1617, FN=0, Flags=.....C, BI=100, SSID=ME...
860	1.715835	PTInovac_67:77:62	Broadcast	802.11	230	Beacon frame, SN=1618, FN=0, Flags=.....C, BI=100, SSID=ME...
861	1.717019	PTInovac_67:77:60	SamsungE_7f:71:a7	802.11	76	Request-to-send, Flags=.....C
862	1.717023	PTInovac_67:77:60	PTInovac_67:77:60	802.11	68	Clear-to-send, Flags=.....C
863	1.717026	SamsungE_7f:71:a7	PTInovac_67:77:60	802.11	68	802.11 Block Ack, Flags=.....C
864	1.719197	PTInovac_67:77:60	SamsungE_7f:71:a7	802.11	76	Request-to-send, Flags=.....C
865	1.719200	PTInovac_67:77:60	PTInovac_67:77:60	802.11	68	Clear-to-send, Flags=.....C
866	1.721029	SamsungE_7f:71:a7	PTInovac_67:77:60	802.11	68	802.11 Block Ack, Flags=.....C
867	1.721023	PTInovac_67:77:60	SamsungE_7f:71:a7	802.11	76	Request-to-send, Flags=.....C
868	1.721025	PTInovac_67:77:60	PTInovac_67:77:60	802.11	68	Clear-to-send, Flags=.....C
869	1.721028	SamsungE_7f:71:a7	PTInovac_67:77:60	802.11	68	802.11 Block Ack, Flags=.....C
870	1.741780	PTInovac_9e:9b:b0	Broadcast	802.11	305	Beacon frame, SN=69, FN=0, Flags=.....C, BI=100, SSID=ME0...
871	1.741837	PTInovac_9e:9b:b2	Broadcast	802.11	230	Beacon frame, SN=70, FN=0, Flags=.....C, BI=100, SSID=ME0...
872	1.751491	PTInovac_67:77:60	SamsungE_7f:71:a7	802.11	76	Request-to-send, Flags=.....C
873	1.751499	PTInovac_67:77:60	PTInovac_67:77:60	802.11	68	Clear-to-send, Flags=.....C
874	1.751502	SamsungE_7f:71:a7	PTInovac_67:77:60	802.11	68	802.11 Block Ack, Flags=.....C
875	1.762029	PTInovac_67:77:60	SamsungE_7f:71:a7	802.11	76	Request-to-send, Flags=.....C
876	1.762034	PTInovac_67:77:60	SamsungE_7f:71:a7	802.11	76	Request-to-send, Flags=.....C
877	1.762038	PTInovac_67:77:60	SamsungE_7f:71:a7	802.11	76	Request-to-send, Flags=.....C
878	1.769937	SamsungE_7f:71:a7	PTInovac_67:77:60	802.11	64	Null function (No data), SN=1106, FN=0, Flags=...P...TC
879	1.769940	SamsungE_7f:71:a7	PTInovac_67:77:60	802.11	64	Null function (No data), SN=1106, FN=0, Flags=...PR...TC
880	1.769951	SamsungE_7f:71:a7	PTInovac_67:77:60	802.11	64	Null function (No data), SN=1106, FN=0, Flags=...PR...TC
881	1.769956	SamsungE_7f:71:a7	PTInovac_67:77:60	802.11	48	Acknowledgement, Flags=.....C
882	1.812663	SamsungE_7f:71:a7	SamsungE_7f:71:a7	802.11	48	Acknowledgement, Flags=.....C
883	1.812669	SamsungE_7f:71:a7	PTInovac_67:77:60	802.11	76	Request-to-send, Flags=.....C
884	1.812672	SamsungE_7f:71:a7	SamsungE_7f:71:a7	802.11	68	Clear-to-send, Flags=.....C
885	1.812676	PTInovac_67:77:60	SamsungE_7f:71:a7	802.11	68	802.11 Block Ack, Flags=.....C
886	1.818806	PTInovac_67:77:60	Broadcast	802.11	305	Beacon frame, SN=1619, FN=0, Flags=.....C, BI=100, SSID=ME...
887	1.818811	PTInovac_67:77:62	Broadcast	802.11	230	Beacon frame, SN=1620, FN=0, Flags=.....C, BI=100, SSID=ME...
888	1.826046	a6:ef:15:08:32:99	Broadcast	802.11	222	Beacon frame, SN=1338, FN=0, Flags=.....C, BI=100, SSID=ph...
889	1.854067	56:5f:07:ef:4f:be	PTInovac_67:77:60	802.11	64	Null function (No data), SN=820, FN=0, Flags=...P...TC
890	1.854066	56:5f:07:ef:4f:be	PTInovac_67:77:60	802.11	48	Acknowledgement, Flags=.....C
891	1.865868	tp-LinkT_a3:af:08	Broadcast	802.11	282	Beacon frame, SN=1015, FN=0, Flags=.....C, BI=100, SSID=TP...
892	1.891819	SamsungE_7f:71:a7	PTInovac_67:77:60	802.11	76	Request-to-send, Flags=.....C
893	1.891828	PTInovac_67:77:60	SamsungE_7f:71:a7	802.11	68	802.11 Block Ack, Flags=.....C
894	1.904051	PTInovac_67:77:60	SamsungE_7f:71:a7	802.11	76	Request-to-send, Flags=.....C
895	1.904061	PTInovac_67:77:60	SamsungE_7f:71:a7	802.11	76	Request-to-send, Flags=.....C
896	1.904063	PTInovac_67:77:60	SamsungE_7f:71:a7	802.11	76	Request-to-send, Flags=.....C
897	1.904067	PTInovac_67:77:60	SamsungE_7f:71:a7	802.11	76	Request-to-send, Flags=.....C
898	1.904071	PTInovac_67:77:60	PTInovac_67:77:60	802.11	68	Clear-to-send, Flags=.....C
899	1.904074	SamsungE_7f:71:a7	PTInovac_67:77:60	802.11	68	802.11 Block Ack, Flags=.....C
900	1.916130	SamsungE_7f:71:a7	PTInovac_67:77:60	802.11	76	Request-to-send, Flags=.....C
901	1.916136	PTInovac_67:77:60	SamsungE_7f:71:a7	802.11	68	Clear-to-send, Flags=.....C
902	1.916139	PTInovac_67:77:60	SamsungE_7f:71:a7	802.11	68	802.11 Block Ack, Flags=.....C
903	1.919996	PTInovac_67:77:60	Broadcast	802.11	305	Beacon frame, SN=1621, FN=0, Flags=.....C, BI=100, SSID=ME...
904	1.920000	PTInovac_67:77:60	Broadcast	802.11	230	Beacon frame, SN=1622, FN=0, Flags=.....C, BI=100, SSID=ME...
Frame 891: 282 bytes on wire (2256 bits), 282 bytes captured (2256 bits) on interface en0, id 0						
0000	00 00 24 00 6f 08 00 40	bb ed b0 41 00 00 00 00	..\$.o..@...A...			
0010	10 02 6c 09 80 04 b0 a3	00 01 00 10 18 03 04 09	...1.....			
0020	b0 07 c0 0d 80 00 00 00	ff ff ff ff ff ff b0 4eN			
0030	26 a3 af 08 b0 4e 26 a3	af 08 70 80 41 8d 5a	&...Na...p?A.Z			
0040	45 01 00 00 64 00 31 04	00 0f 54 50 2d 4c 49 4e	E...d1...TP-LIN			
0050	4b 5f 41 50 5f 41 46 30	38 01 08 82 84 8b 96 0c	KAP_AF0 8.....			
0060	12 18 24 03 01 02 05 04	00 01 00 03 2a 01 00 30	..\$......*..0			

Figure 15: Trama 891 selecionada.

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

888 1.826046	a6:ef:15:08:32:99	Broadcast	802.11	222 Beacon frame, SN=1338, FN=0, Flags=.....C, BI=100, SSID=ph..
889 1.854067	56:5f:07:ef:4f:be	PTInovac_67:77:60	802.11	64 Null function (No data), SN=820, FN=0, Flags=...P...TC
890 1.854086	56:5f:07:ef:4f:be	(.. 802.11	48 Acknowledgement, Flags=.....C	
891 1.865868	Tp-LinkI a3:af:08	Broadcast	802.11	282 Beacon frame, SN=1015, FN=0, Flags=.....C, BI=100, SSID=TP..
892 1.891819	SamsungE_7f:71:a7	(.. PTInovac_67:77:60	802.11	76 Request-to-send, Flags=.....C
893 1.891828	PTInovac_67:77:60	(.. SamsungE_7f:71:a7	802.11	68 802.11 Block Ack, Flags=.....C
894 1.904051	PTInovac_67:77:60	(.. SamsungE_7f:71:a7	802.11	76 Request-to-send, Flags=.....C


```

Frame 891: 282 bytes on wire (2256 bits), 282 bytes captured (2256 bits) on interface en0, id 0
  Radiotap Header v0, Length 36
  802.11 radio information
    PHY type: 802.11g (ERP) (6)
    Short preamble: False
    Proprietary mode: None (0)
    Data rate: 1,0 Mb/s
    Channel: 1
    Frequency: 2412MHz
    Signal strength (dBm): -80dBm
    Noise level (dBm): -93dBm
    Signal/noise ratio (dB): 13dB
    TSF timestamp: 1102114235
    [Duration: 2160µs]
  IEEE 802.11 Beacon frame, Flags: .....C
  IEEE 802.11 Wireless Management

```

Figure 16: frequência de espectro da trama 891

Resposta: A frequência é de 2412MHz no canal 1.

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

Resposta: A versão usada é 802.11n.

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.

```

IEEE 802.11 Wireless Management
  Fixed parameters (12 bytes)
  Tagged parameters (206 bytes)
    Tag: SSID parameter set: TP-LINK_AP_AF08
    Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6, 9, 12, 18, [Mbit/sec]
    Tag: DS Parameter set: Current Channel: 2
    Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    Tag: ERP Information
    Tag: RSN Information
    Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
    Tag: HT Capabilities (802.11n D1.10)
    Tag: HT Information (802.11n D1.10)
    Tag: Extended Capabilities (8 octets)
    Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
    Tag: Vendor Specific: Atheros Communications, Inc.: Advanced Capability
    Tag: Vendor Specific: Microsoft Corp.: WPS

```

Figure 17: Débito suportado

Resposta: Como comprovamos na figura 16, o data rate é de 1,0 Mb/s. Sendo assim, o débito máximo suportado é de 11 Mb/s. O protocolo 802.11 é capaz de suportar velocidades de até 600 Mb/s, dependendo das condições da rede e das configurações utilizadas.

Como podemos observar na figura 16, o data rate da trama é de 1,0 Mb/s. No entanto, isso não significa que o utilizador final esteja a receber dados a essa velocidade. O débito máximo real depende de diversos fatores, como o protocolo de camada superior utilizado, o tipo de modulação, a taxa de erro da rede e as configurações da interface Wi-Fi.

O protocolo 802.11 possui diferentes versões, cada uma com sua taxa máxima teórica. Por exemplo, o 802.11b suporta até 11 Mb/s, enquanto o 802.11ac pode chegar a 1.750 Mb/s (em condições ideais).

É importante ressaltar que a velocidade real de uma rede Wi-Fi raramente atinge a taxa máxima teórica. Interferência de outras redes, obstáculos físicos, congestionamento da rede e configurações incorretas podem reduzir significativamente o desempenho.

2.2. Exercício 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:

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)?

```
▼ IEEE 802.11 Beacon frame, Flags: .....C
  Type/Subtype: Beacon frame (0x0008)
  ▼ Frame Control Field: 0x8000
    .... ..00 = Version: 0
    .... 00.. = Type: Management frame (0)
    1000 .... = Subtype: 8
    ▶ Flags: 0x00
    .000 0000 0000 0000 = Duration: 0 microseconds
```

Figure 18: tipo e subtipo da trama

Resposta: A trama que selecionamos foi a 891, e como podemos ver na figura 18, esta pertence ao tipo *Management* (0) e o seu subtipo é *Beacon* (8). Através do anexo fornecido no enunciado podemos verificar que estes pertencem ao *Frame Control*.

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")

```
Frame check sequence: 0x4dff8a5f [unverified]
[FCS Status: Unverified]
```

Figure 19: FCS

Resposta: Quando tentamos verificar se o método de deteção de erros está ativo, apareceu a informação que indicamos acima na figura 19. Podemos, portanto, concluir que o CRC não está ativo.

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

As tramas *beacon* são enviadas periodicamente e permitem especificar parâmetros de funcionamento para apoiar a operação e a gestão das ligações sem fios.

Resposta: É necessário usar deteção de erros em redes sem fios, pois devido a existir interferência com o meio ambiente, como, por exemplo, dispositivos eletrónicos e ruídos elétricos; existir atenuação do sinal devido a obstáculos físicos e a própria distância entre o transmissor e o recetor; erros de transmissão, como colisões, ruídos do canal e colisões; e,

por fim, mobilidade, pois é uma rede bastante usada em dispositivos móveis, como telemóveis. Todos estes motivos fazem com que exista erros em redes sem fios, daí a sua importância no seu uso.

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.

891 1.865868	Tp-LinkT_a3:af:98	Broadcast	802.11	282 Beacon frame, SN=1615, FN=0, Flags=.....C, BI=100, SSID=TP-LINK_AP_AF08
892 1.891819	SamsungE_7f:71:a7	(- PTInovac_67:77:60 (-	802.11	76 Request-to-send, Flags=.....C
893 1.891828	PTInovac_67:77:60	(- SamsungE_7f:71:a7 (-	802.11	68 802.11 Block Ack, Flags=.....C
894 1.904051	PTInovac_67:77:60	(- SamsungE_7f:71:a7 (-	802.11	76 Request-to-send, Flags=.....C
895 1.904061	PTInovac_67:77:60	(- SamsungE_7f:71:a7 (-	802.11	76 Request-to-send, Flags=.....C
896 1.904063	PTInovac_67:77:60	(- SamsungE_7f:71:a7 (-	802.11	76 Request-to-send, Flags=.....C
897 1.904067	PTInovac_67:77:60	(- SamsungE_7f:71:a7 (-	802.11	76 Request-to-send, Flags=.....C
898 1.904071	PTInovac_67:77:60	(- PTInovac_67:77:60 (-	802.11	68 Clear-to-send, Flags=.....C
899 1.904074	SamsungE_7f:71:a7	(- PTInovac_67:77:60 (-	802.11	68 802.11 Block Ack, Flags=.....C
900 1.910130	SamsungE_7f:71:a7	(- PTInovac_67:77:60 (-	802.11	76 Request-to-send, Flags=.....C
901 1.910136	SamsungE_7f:71:a7	(- SamsungE_7f:71:a7 (-	802.11	68 Clear-to-send, Flags=.....C
902 1.910139	PTInovac_67:77:60	(- SamsungE_7f:71:a7 (-	802.11	68 802.11 Block Ack, Flags=.....C
903 1.919996	PTInovac_67:77:60	Broadcast	802.11	305 Beacon frame, SN=1621, FN=0, Flags=.....C, BI=100, SSID=ME0-677760
904 1.921826	PTInovac_67:77:62	Broadcast	802.11	230 Beacon frame, SN=1622, FN=0, Flags=.....C, BI=100, SSID=ME0-WiFi1

IEEE 802.11 Wireless Management

Fixed parameters (12 bytes)

Timestamp: 1397383577984
Beacon Interval: 0,102400 [Seconds]
Capabilities Information: 0x0431

Tagged parameters (206 bytes)

Tag: SSID parameter set: TP-LINK_AP_AF08
Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6, 9, 12, 18, [Mbit/sec]
Tag: DS Parameter set: Current Channel: 2
Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
Tag: ERP Information
Tag: RSN Information
Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
Tag: HT Capabilities (802.11n D1.10)
Tag: HT Information (802.11n D1.10)
Tag: Extended Capabilities (8 octets)
Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
Tag: Vendor Specific: Atheros Communications, Inc.: Advanced Capability
Tag: Vendor Specific: Microsoft Corp.: WPS

Figure 20: Débitos das tramas

Resposta: O intervalo de tempo previsto entre tramas beacon consecutivas é anunciado na trama, em Fixed parameters -> Beacon Interval que, neste caso, é 0.102400 segundos (visível na figura acima). A periodicidade como podemos ver na figura acima é 0,027979 , $((1,919996-1,865868)+(1,921826-1,919996))/2$.

As taxas de transmissão suportadas são:

- 1 Mb/s
- 2 Mb/s
- 5.5 Mb/s
- 11 Mb/s
- 6 Mb/s
- 9 Mb/s
- 12 Mb/s
- 18 Mb/s;

8. Identifique e liste os SSIDs dos APs que estão a operar na vizinhança da STA de captura. Explique o modo como obteve essa informação (por exemplo, se usou algum filtro para o efeito). No trace disponibilizado foi também registado scanning

ativo (envolvendo tramas probe request e probe response), comum nas redes Wi-Fi como alternativa ao scanning passivo.

wlan.ssid					
No.	Time	Source	Destination	Protocol	Length Info
808	1.510343	PTInovac_67:77:60	Broadcast	802.11	305 Beacon frame, SN=1613, FN=0, Flags=.....C, BI=100, SSID=MEO-677760
809	1.512539	PTInovac_67:77:62	Broadcast	802.11	230 Beacon frame, SN=1614, FN=0, Flags=.....C, BI=100, SSID=MEO-WiFi
831	1.519279	Tp-LinkT_a3:af:08	OnePlusT_92:95:d9	802.11	391 Probe Response, SN=1011, FN=0, Flags=.....C, BI=100, SSID=TP-LINK AP_AF08
832	1.521291	Tp-LinkT_a3:af:08	OnePlusT_92:95:d9	802.11	391 Probe Response, SN=1011, FN=0, Flags=.....C, BI=100, SSID=TP-LINK AP_AF08
833	1.524424	Tp-LinkT_a3:af:08	OnePlusT_92:95:d9	802.11	391 Probe Response, SN=1011, FN=0, Flags=.....C, BI=100, SSID=TP-LINK AP_AF08
840	1.534013	PTInovac_9e:9b:b0	Broadcast	802.11	305 Beacon frame, SN=65, FN=0, Flags=.....C, BI=100, SSID=MEO-9E98B0
841	1.536496	PTInovac_9e:9b:b2	Broadcast	802.11	230 Beacon frame, SN=66, FN=0, Flags=.....C, BI=100, SSID=MEO-WiFi
845	1.558871	Tp-LinkT_a3:af:08	Broadcast	802.11	282 Beacon frame, SN=1612, FN=0, Flags=.....C, BI=100, SSID=TP-LINK AP_AF08
846	1.612845	PTInovac_67:77:60	Broadcast	802.11	305 Beacon frame, SN=1615, FN=0, Flags=.....C, BI=100, SSID=MEO-677760
847	1.612940	PTInovac_67:77:62	Broadcast	802.11	230 Beacon frame, SN=1616, FN=0, Flags=.....C, BI=100, SSID=MEO-WiFi
848	1.641108	PTInovac_9e:9b:b2	Broadcast	802.11	230 Beacon frame, SN=68, FN=0, Flags=.....C, BI=100, SSID=MEO-WiFi
849	1.671593	b0:76:1b:52:87:80	Broadcast	802.11	388 Beacon frame, SN=3839, FN=0, Flags=.....C, BI=100, SSID=Vodafone-528777
854	1.697119	PTInovac_9b:f2:a2	Broadcast	802.11	230 Beacon frame, SN=231, FN=0, Flags=.....C, BI=100, SSID=MEO-WiFi
859	1.715832	PTInovac_67:77:60	Broadcast	802.11	305 Beacon frame, SN=1617, FN=0, Flags=.....C, BI=100, SSID=MEO-677760
860	1.715835	PTInovac_67:77:62	Broadcast	802.11	230 Beacon frame, SN=1618, FN=0, Flags=.....C, BI=100, SSID=MEO-WiFi
879	1.741700	PTInovac_9e:9b:b0	Broadcast	802.11	305 Beacon frame, SN=69, FN=0, Flags=.....C, BI=100, SSID=MEO-9E98B0
871	1.741837	PTInovac_9e:9b:b2	Broadcast	802.11	230 Beacon frame, SN=70, FN=0, Flags=.....C, BI=100, SSID=MEO-WiFi
886	1.818806	PTInovac_67:77:60	Broadcast	802.11	305 Beacon frame, SN=1619, FN=0, Flags=.....C, BI=100, SSID=MEO-677760
887	1.818811	PTInovac_67:77:62	Broadcast	802.11	230 Beacon frame, SN=1620, FN=0, Flags=.....C, BI=100, SSID=MEO-WiFi
888	1.826046	a6:ef:15:08:32:99	Broadcast	802.11	222 Beacon frame, SN=1338, FN=0, Flags=.....C, BI=100, SSID=phi_F41927C3C600
891	1.865868	Tp-LinkT_a3:af:08	Broadcast	802.11	282 Beacon frame, SN=1615, FN=0, Flags=.....C, BI=100, SSID=TP-LINK AP_AF08
983	1.919996	PTInovac_67:77:60	Broadcast	802.11	305 Beacon frame, SN=1621, FN=0, Flags=.....C, BI=100, SSID=MEO-677760
994	1.921826	PTInovac_67:77:62	Broadcast	802.11	230 Beacon frame, SN=1622, FN=0, Flags=.....C, BI=100, SSID=MEO-WiFi
998	1.946544	PTInovac_9e:9b:b0	Broadcast	802.11	305 Beacon frame, SN=73, FN=0, Flags=.....C, BI=100, SSID=MEO-9E98B0
999	1.949194	PTInovac_9e:9b:b2	Broadcast	802.11	230 Beacon frame, SN=74, FN=0, Flags=.....C, BI=100, SSID=MEO-WiFi
923	2.819669	PTInovac_67:77:60	Broadcast	802.11	305 Beacon frame, SN=1623, FN=0, Flags=.....C, BI=100, SSID=MEO-677760
924	2.827067	PTInovac_67:77:62	Broadcast	802.11	230 Beacon frame, SN=1624, FN=0, Flags=.....C, BI=100, SSID=MEO-WiFi

Figure 21: SSIDs a operar na vizinhança da STA

Resposta: De modo a obter os SSIDs dos APs, utilizamos o filtro wlan.ssid no wireshark que nos dá as tramas beacon capturados provenientes dos APs que conseguem comunicar com a STA. Com o uso deste filtro chegamos à conclusão que os três SSIDs são MEO, TP-LINK, Vodafone e phi.

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

wlan.fc.type_subtype == 0x04 or wlan.fc.type_subtype == 0x05					
No.	Time	Source	Destination	Protocol	Length Info
339	0.842086	94:a4:f9:16:a9:b4	a4:ef:15:08:32:99	802.11	654 Probe Response, SN=4032, FN=0, Flags=.....C, BI=100, SSID=...
340	0.858977	94:a4:f9:16:a9:b4	a4:ef:15:08:32:99	802.11	654 Probe Response, SN=4032, FN=0, Flags=.....C, BI=100, SSID=...
342	0.872569	94:a4:f9:16:a9:b4	a4:ef:15:08:32:99	802.11	654 Probe Response, SN=4032, FN=0, Flags=.....C, BI=100, SSID=...
343	0.887927	PTInovac_67:77:62	ARRISGro_aa:9c:66	802.11	224 Probe Response, SN=1600, FN=0, Flags=.....C, BI=100, SSID=...
375	0.985952	Tp-LinkT_a3:af:08	ARRISGro_aa:9c:66	802.11	391 Probe Response, SN=1003, FN=0, Flags=.....C, BI=100, SSID=...
376	0.987280	Tp-LinkT_a3:af:08	ARRISGro_aa:9c:66	802.11	391 Probe Response, SN=1003, FN=0, Flags=.....C, BI=100, SSID=...
831	1.519279	Tp-LinkT_a3:af:08	OnePlusT_92:95:d9	802.11	391 Probe Response, SN=1011, FN=0, Flags=.....C, BI=100, SSID=...
832	1.521291	Tp-LinkT_a3:af:08	OnePlusT_92:95:d9	802.11	391 Probe Response, SN=1011, FN=0, Flags=.....C, BI=100, SSID=...
833	1.524424	Tp-LinkT_a3:af:08	OnePlusT_92:95:d9	802.11	391 Probe Response, SN=1011, FN=0, Flags=.....C, BI=100, SSID=...
952	2.146928	Tp-LinkT_a3:af:08	26:50:9f:40:9f:ad	802.11	391 Probe Response, SN=1018, FN=0, Flags=.....C, BI=100, SSID=...
953	2.147025	Tp-LinkT_a3:af:08	26:50:9f:40:9f:ad	802.11	391 Probe Response, SN=1018, FN=0, Flags=.....C, BI=100, SSID=...
954	2.162326	Tp-LinkT_a3:af:08	26:50:9f:40:9f:ad	802.11	391 Probe Response, SN=1019, FN=0, Flags=.....C, BI=100, SSID=...
955	2.162463	Tp-LinkT_a3:af:08	26:50:9f:40:9f:ad	802.11	391 Probe Response, SN=1019, FN=0, Flags=.....C, BI=100, SSID=...
956	2.170276	Tp-LinkT_a3:af:08	26:50:9f:40:9f:ad	802.11	391 Probe Response, SN=1019, FN=0, Flags=.....C, BI=100, SSID=...
950	2.190938	Tp-LinkT_a3:af:08	26:50:9f:40:9f:ad	802.11	391 Probe Response, SN=1021, FN=0, Flags=.....C, BI=100, SSID=...
1713	4.695628	Tp-LinkT_a3:af:08	ROBERTB0_2b:d3:65	802.11	391 Probe Response, SN=1056, FN=0, Flags=.....C, BI=100, SSID=...
1714	4.701099	Tp-LinkT_a3:af:08	ROBERTB0_2b:d3:65	802.11	391 Probe Response, SN=1056, FN=0, Flags=.....C, BI=100, SSID=...
1715	4.701234	Tp-LinkT_a3:af:08	ROBERTB0_2b:d3:65	802.11	391 Probe Response, SN=1056, FN=0, Flags=.....C, BI=100, SSID=...
1901	5.473739	94:a4:f9:16:a9:b4	ARRISGro_a5:20:8a	802.11	654 Probe Response, SN=4033, FN=0, Flags=.....C, BI=100, SSID=...
1937	5.509787	94:a4:f9:16:a9:b4	ARRISGro_a5:20:8a	802.11	654 Probe Response, SN=4033, FN=0, Flags=.....C, BI=100, SSID=...
2054	5.933333	a4:ef:15:08:32:99	Broadcast	802.11	110 Probe Request, SN=1776, FN=0, Flags=.....C, SSID=Wildcard
2062	5.978338	94:a4:f9:16:a9:b4	a4:ef:15:08:32:99	802.11	654 Probe Response, SN=4034, FN=0, Flags=.....C, BI=100, SSID=...
2063	5.984439	94:a4:f9:16:a9:b4	a4:ef:15:08:32:99	802.11	654 Probe Response, SN=4034, FN=0, Flags=.....C, BI=100, SSID=...
2064	5.987562	94:a4:f9:16:a9:b4	a4:ef:15:08:32:99	802.11	654 Probe Response, SN=4034, FN=0, Flags=.....C, BI=100, SSID=...

Figure 22: tráfego das tramas probing request/response

Resposta: O filtro que permite essa visualização é: wlan.fc.type_subtype == 0x04 or wlan.fc.type_subtype == 0x05. Assim testamos o subtipo das tramas, filtrando as de probing request (4) e as de probing response (5). A visualização após a aplicação do filtro, comprova a apresentação de tramas representados na figura 22. Este filtro irá exibir todas as tramas de probe request (wlan.fc.type_subtype == 0x04) e probe response (wlan.fc.type_subtype == 0x05) capturadas na sua captura do Wireshark.

- 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.

Resposta: Como podemos ver na figura 16, a força do sinal é -80dBm. A força do sinal não é de confiança, pelo que não é dos piores sinais mas a probabilidade da conexão ser estabelecida é reduzida, o que significa que, a probabilidade de receber tramas, nestas condições, menor.

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.

Resposta:

De acordo com a tabela de referência do Anexo II, para um MCS 3 e uma sensibilidade mínima de -81 dBm, a taxa de transmissão máxima é de 24 Mbps.

Considerando um fator de redução de 50% devido a interferências, ruído e perdas de caminho, a taxa de transmissão efetiva seria de 12 Mbps (24 Mbps * 0.5).

O débito da ligação Wi-Fi é calculado da seguinte forma:

Débito = Taxa de transmissão efetiva * Tempo de transmissão útil

Débito = 12 Mbps * (1000 bytes / 8 bits/byte) * (1 ms / 1000 ms/s) = 1500 bps

2.3. Exercício 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:

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: Para obter o conjunto completo de conexões entre a estação (STA) e o ponto de acesso (AP) em um processo de associação, foi necessário desenvolver um filtro que nos fornecesse, de maneira conveniente, um conjunto organizado dessas conexões.

Sendo assim, o filtro aplicado foi:

wlan.fc.type == 0 && (wlan.fc.type subtype == 0 or wlan.fc.type subtype == 1 or wlan.fc.type subtype == 11)

A tabela apresentada contém informações sobre os filtros e as tramas associadas a eles.

Estamos, essencialmente, filtrando os quadros de gerenciamento (Management Frames) e,

dentro deles, aqueles que são do tipo "Association Request"(Solicitação de Associação), "Association Response"(Resposta de Associação) e "Authentication"(Autenticação). Essas são fases relevantes do processo de associação.

Após a aplicação do filtro, obtiveram-se as tramas seguintes:

wlan.fc.type==0 && (wlan.fc.type_subtype==0 wlan.fc.type_subtype==1 wlan.fc.type_subtype==11)					
No.	Time	Source	Destination	Protocol	Length Info
3228	14.890461	c8:70:23:1f:a2:72	80:38:fb:04:f4:2f	802.11	81 Authentication, SN=3073, FN=0, Flags=...R...C
3624	18.716086	c8:70:23:1f:a2:72	4e:f8:ca:05:0a:77	802.11	81 Authentication, SN=3154, FN=0, Flags=...R...C
3625	18.716198	c8:70:23:1f:a2:72	4e:f8:ca:05:0a:77	802.11	81 Authentication, SN=3154, FN=0, Flags=...R...C
3626	18.719251	c8:70:23:1f:a2:72	4e:f8:ca:05:0a:77	802.11	81 Authentication, SN=3154, FN=0, Flags=...R...C
3627	18.728358	c8:70:23:1f:a2:72	4e:f8:ca:05:0a:77	802.11	81 Authentication, SN=3154, FN=0, Flags=...R...C
5177	34.292210	c8:70:23:1f:a2:72	80:38:fb:04:f4:2f	802.11	81 Authentication, SN=3472, FN=0, Flags=...R...C
5178	34.292316	c8:70:23:1f:a2:72	80:38:fb:04:f4:2f	802.11	81 Authentication, SN=3472, FN=0, Flags=...R...C
5179	34.295367	c8:70:23:1f:a2:72	80:38:fb:04:f4:2f	802.11	81 Authentication, SN=3472, FN=0, Flags=...R...C
5180	34.301443	c8:70:23:1f:a2:72	80:38:fb:04:f4:2f	802.11	81 Authentication, SN=3472, FN=0, Flags=...R...C
12855	98.374622	92:97:e1:69:c3:d5	PTInovac_67:77:62	802.11	105 Authentication, SN=674, FN=0, 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
12861	98.387225	92:97:e1:69:c3:d5	PTInovac_67:77:62	802.11	213 Association Request, SN=675, FN=0, Flags=.....C, SSID=ME0-WiFi1
12863	98.387244	PTInovac_67:77:62	92:97:e1:69:c3:d5	802.11	192 Association Response, SN=3670, FN=0, Flags=.....C

Figure 23: Processo de associação completo - redes IEEE 802.11

Observa-se que o processo de associação consiste em duas etapas, autenticação e associação, ambas com uma solicitação e uma resposta:

- Solicitação de Autenticação - Frame 12855
- Resposta de Autenticação - Frame 12857
- Solicitação de Associação - Frame 12861
- Resposta de Associação - Frame 12863

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

Resposta:

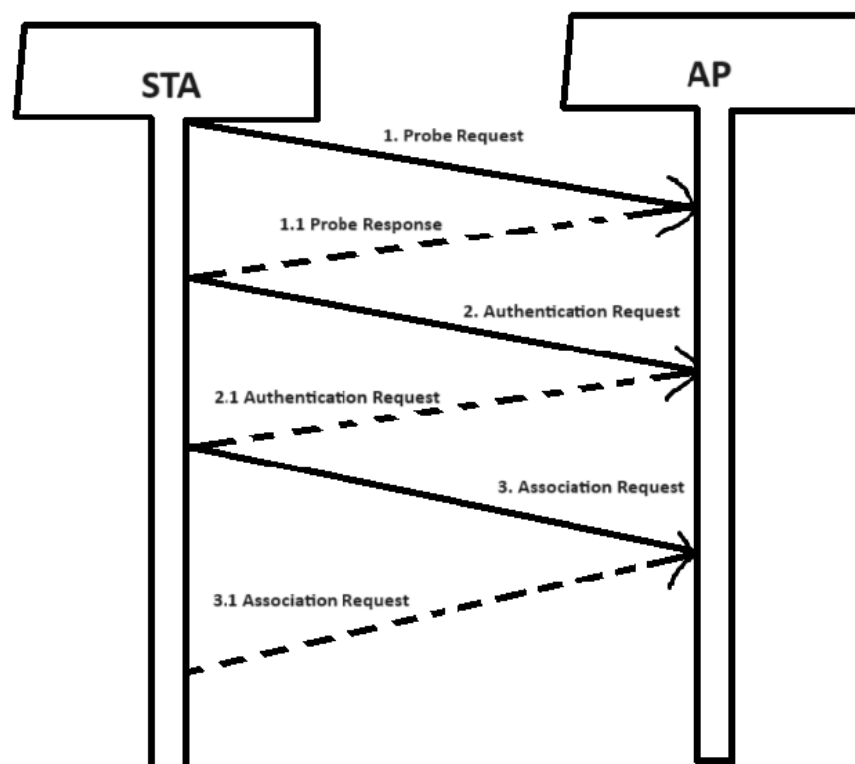


Figure 24: Processo de associação completo - diagrama - redes 802.11

2.4. Exercício 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.

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 direcionalidade das tramas, o que pode concluir face à direcionalidade dessa trama, será local à WLAN?

Resposta: Analisando a flag referente ao DS status, da figura abaixo, podemos concluir que a direcionalidade desta trama pode ser observada através dos campos "To DS: 0" e "From DS: 1". O primeiro indica que a trama não é direccionada ao DS e o segundo que a trama é proveniente do DS, ou seja, podemos concluir que a trama não é destinada à WLAN (Wireless Local Area Network) e é proveniente da mesma.

wlan && data					
No.	Time	Source	Destination	Protocol	Length Info
264	0.679178	PTInovac_67:77:5f	56:5f:07:ef:4f:be	802.11	1390 QoS Data, SN=1926, FN=0, Flags=.p..R.F.C
265	0.679180	PTInovac_67:77:5f	56:5f:07:ef:4f:be	802.11	1390 QoS Data, SN=1927, FN=0, Flags=.p..R.F.C
266	0.679184	PTInovac_67:77:5f	56:5f:07:ef:4f:be	802.11	1390 QoS Data, SN=1928, FN=0, Flags=.p..R.F.C
267	0.679189	PTInovac_67:77:5f	56:5f:07:ef:4f:be	802.11	691 QoS Data, SN=1929, FN=0, Flags=.p..R.F.C
268	0.679191	PTInovac_67:77:5f	56:5f:07:ef:4f:be	802.11	276 QoS Data, SN=1930, FN=0, Flags=.p..R.F.C
269	0.679195	PTInovac_67:77:5f	56:5f:07:ef:4f:be	802.11	1390 QoS Data, SN=1931, FN=0, Flags=.p..R.F.C
270	0.679197	PTInovac_67:77:5f	56:5f:07:ef:4f:be	802.11	739 QoS Data, SN=1932, FN=0, Flags=.p..R.F.C
291	0.697925	PTInovac_67:77:5f	56:5f:07:ef:4f:be	802.11	181 QoS Data, SN=1939, FN=0, Flags=.p....F.C
298	0.699074	PTInovac_67:77:5f	56:5f:07:ef:4f:be	802.11	187 QoS Data, SN=1942, FN=0, Flags=.p....F.C
334	0.801835	ARRISGro_fb:16:3d	IPv4mcast_7f:ff:fa	802.11	805 Data, SN=1598, FN=0, Flags=.p....F.C
351	0.910086	SamsungE_7f:71:a7	PTInovac_67:77:5f	802.11	185 QoS Data, SN=1416, FN=0, Flags=.p....TC
358	0.933251	CiscoSPV_ec:e6:66	IPv4mcast_7f:ff:fa	802.11	807 Data, SN=54, FN=0, Flags=.p....F.C
371	0.963807	SamsungE_7f:71:a7	PTInovac_67:77:5f	802.11	184 QoS Data, SN=1419, FN=0, Flags=.p....TC
390	1.002219	SamsungE_7f:71:a7	PTInovac_67:77:5f	802.11	184 QoS Data, SN=1421, FN=0, Flags=.p....TC
394	1.002233	SamsungE_7f:71:a7	PTInovac_67:77:5f	802.11	184 QoS Data, SN=1422, FN=0, Flags=.p....TC
398	1.002254	SamsungE_7f:71:a7	PTInovac_67:77:5f	802.11	184 QoS Data, SN=1423, FN=0, Flags=.p....TC
Frame 291: 181 bytes on wire (1448 bits), 181 bytes captured (1448 bits) on interface en0, id 0					
Radiotap Header v0, Length 58					
802.11 radio information					
IEEE 802.11 QoS Data, Flags: .p....F.C					
Type/Subtype: QoS Data (8x0028)					
Frame Control Field: 0x0842					
....00 = Version: 0					
....10.. = Type: Data frame (2)					
1000.... = Subtype: 8					
Flags: 0x42					
....10 = DS status: Frame from DS to a STA via AP (To DS: 0 From DS: 1) (0x2)					
....0... = More Fragments: This is the last fragment					
....0... = Retry: Frame is not being retransmitted					
....0... = PWR MGT: STA will stay up					
....10... = 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: 56:5f:07:ef:4f:be (56:5f:07:ef:4f:be)					
Transmitter address: PTInovac_67:77:60 (00:06:91:67:77:60)					
Destination address: 56:5f:07:ef:4f:be (56:5f:07:ef:4f:be)					
Source address: PTInovac_67:77:5f (00:06:91:67:77:5f)					
BSS Id: PTInovac_67:77:60 (00:06:91:67:77:60)					
STA address: 56:5f:07:ef:4f:be (56:5f:07:ef:4f:be)					
....0000.... = Fragment number: 0					
0111 1001 0011.... = Sequence number: 1939					
Frame check sequence: 0x90463894 [unverified]					
[FCS Status: Unverified]					
QoS Control: 0x0000					
CCMP parameters					
Data (85 bytes)					
0030	00 10 18 03 04 00 43 bd	00 00 88 42 30 00 56 5fC.....B0_V		
0040	07 ef 4f be 00 06 91 67	77 60 00 06 91 67 77 5f	..0...g w...gw		
0050	30 79 00 00 1d b6 00 20	85 00 00 00 27 8c 7c 8c	0y.....		
0060	1c ba dd 0d 1a 5f 3b ce	62 b8 ff 91 a4 00 fe d3;..b.....		
0070	71 61 0f 59 91 02 43 bd	70 79 05 24 99 e6 71 d7	qa.Y..C..py.S..g		
0080	c6 fe a2 c3 b8 c2 00 e0	4b 61 c3 3d b1 d5 76 caKa=..v		
0090	e5 cd 8e cc f5 1c 73 ce	0f 4a 63 83 c7 5c dd 8es..Jc..v		

Figure 23: Trama de dados nº 291

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: Com base na trama da figura abaixo concluímos assim que os endereços MAC correspondentes são:

- **STA:** 56:5f:07:ef:4f:be
- **AP:** 00:06:91:67:77:60
- **Router:** 56:5f:07:ef:4f:be

```

0... .... = Order flag: Not strictly ordered
.000 0000 0011 0000 = Duration: 48 microseconds
Receiver address: 56:5f:07:ef:4f:be (56:5f:07:ef:4f:be)
Transmitter address: PTInovac_67:77:60 (00:06:91:67:77:60)
Destination address: 56:5f:07:ef:4f:be (56:5f:07:ef:4f:be)
Source address: PTInovac_67:77:5f (00:06:91:67:77:5f)
BSS Id: PTInovac_67:77:60 (00:06:91:67:77:60)
STA address: 56:5f:07:ef:4f:be (56:5f:07:ef:4f:be)
.... .... 0000 = Fragment number: 0
0111 1001 0011 .... = Sequence number: 1939
Frame check sequence: 0x90463894 [unverified]
[FCS Status: Unverified]
Qos Control: 0x0000
CCMP parameters

```

Figure 24: Totalidade da trama

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.

Reposta: De forma a encontrar transferências de dados em que é usada a opção RTC/CTS em primeiro lugar aplicamos o seguinte filtro: wlan.fc.type_subtype == 0x1b || wlan.fc.type_subtype == 0x1c.

wlan.fc.type_subtype == 0x1b wlan.fc.type_subtype == 0x1c						
No.	Time	Source	Destination	Protocol	Length	Info
252	0.676572		PTInovac_67:77:60	(- 802.11	68	Clear-to-send, Flags=.....C
261	0.677776	PTInovac_67:77:60	(- 56:5f:07:ef:4f:be	(- 802.11	76	Request-to-send, Flags=.....C
262	0.677778		PTInovac_67:77:60	(- 802.11	68	Clear-to-send, Flags=.....C
274	0.694804	56:5f:07:ef:4f:be	(- 56:5f:07:ef:4f:be	(- 802.11	76	Request-to-send, Flags=.....C
275	0.694807		56:5f:07:ef:4f:be	(- 802.11	68	Clear-to-send, Flags=.....C
277	0.694813	56:5f:07:ef:4f:be	(- PTInovac_67:77:60	(- 802.11	76	Request-to-send, Flags=.....C
278	0.694815		56:5f:07:ef:4f:be	(- 802.11	68	Clear-to-send, Flags=.....C
280	0.694823	56:5f:07:ef:4f:be	(- PTInovac_67:77:60	(- 802.11	76	Request-to-send, Flags=.....C
281	0.694827		56:5f:07:ef:4f:be	(- 802.11	68	Clear-to-send, Flags=.....C
283	0.697896	PTInovac_67:77:60	(- 56:5f:07:ef:4f:be	(- 802.11	76	Request-to-send, Flags=.....C
284	0.697900		PTInovac_67:77:60	(- 802.11	68	Clear-to-send, Flags=.....C
286	0.697910	PTInovac_67:77:60	(- 56:5f:07:ef:4f:be	(- 802.11	76	Request-to-send, Flags=.....C
287	0.697913		PTInovac_67:77:60	(- 802.11	68	Clear-to-send, Flags=.....C
289	0.697918	PTInovac_67:77:60	(- 56:5f:07:ef:4f:be	(- 802.11	76	Request-to-send, Flags=.....C
290	0.697922		PTInovac_67:77:60	(- 802.11	68	Clear-to-send, Flags=.....C
293	0.697933	PTInovac_67:77:60	(- 56:5f:07:ef:4f:be	(- 802.11	76	Request-to-send, Flags=.....C
294	0.697937		PTInovac_67:77:60	(- 802.11	68	Clear-to-send, Flags=.....C
296	0.699064	PTInovac_67:77:60	(- 56:5f:07:ef:4f:be	(- 802.11	76	Request-to-send, Flags=.....C
297	0.699070		PTInovac_67:77:60	(- 802.11	68	Clear-to-send, Flags=.....C
307	0.758408	PTInovac_67:77:60	(- 56:5f:07:ef:4f:be	(- 802.11	76	Request-to-send, Flags=.....C
308	0.758413		PTInovac_67:77:60	(- 802.11	68	Clear-to-send, Flags=.....C
310	0.758418	PTInovac_67:77:60	(- 56:5f:07:ef:4f:be	(- 802.11	76	Request-to-send, Flags=.....C
311	0.758422		PTInovac_67:77:60	(- 802.11	68	Clear-to-send, Flags=.....C
313	0.758430	56:5f:07:ef:4f:be	(- PTInovac_67:77:60	(- 802.11	76	Request-to-send, Flags=.....C
314	0.758433		56:5f:07:ef:4f:be	(- 802.11	68	Clear-to-send, Flags=.....C
316	0.759444	56:5f:07:ef:4f:be	(- PTInovac_67:77:60	(- 802.11	76	Request-to-send, Flags=.....C
317	0.759448		56:5f:07:ef:4f:be	(- 802.11	68	Clear-to-send, Flags=.....C
319	0.761026	56:5f:07:ef:4f:be	(- PTInovac_67:77:60	(- 802.11	76	Request-to-send, Flags=.....C
320	0.761032		56:5f:07:ef:4f:be	(- 802.11	68	Clear-to-send, Flags=.....C

▶ Frame 290: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface en0, id 0 ▶ Radiotap Header v0, Length 54 ▶ 802.11 radio information ▶ IEEE 802.11 Clear-to-send, Flags:C ▶ Type/Subtype: Clear-to-send (0x001c) ▶ Frame control, flags: 0xc400 ▶00 = Version: 0 ▶01.. = Type: Control frame (1) ▶ 1100 = Subtype: 12 ▶ Flags: 0x00 ▶00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x0) ▶0... = More Fragments: This is the last fragment ▶0... = Retry: Frame is not being retransmitted ▶ ...0 = PWR MGT: STA will stay up ▶ ..0. = More Data: No data buffered ▶ ..0. = Protected: No data buffered

Figure 25: Filtro wlan.fc.type_subtype == 0x1b || wlan.fc.type_subtype == 0x1c

Conclusão

O foco principal deste trabalho é a exploração de vários aspectos relacionados às redes sem fio (Wi-Fi).

Inicialmente, abordamos o Acesso Rádio, onde investigamos a camada física das redes sem fio, incluindo elementos como canais e frequências.

Em seguida, comparamos o scanning ativo e passivo, destacando que o primeiro é realizado por meio das tramas beacon, permitindo a descoberta dos pontos de acesso disponíveis, enquanto o segundo utiliza o probe response.

No terceiro ponto, discutimos o Processo de Associação, necessário para estabelecer a conexão entre um dispositivo e um ponto de acesso. Este processo envolve um pedido de associação feito pelo dispositivo, seguido da resposta do ponto de acesso.

Por fim, examinamos o processo de Transferência de Dados, levando em consideração dois fatores: informações obtidas nas tramas e o controle da transferência.

Além disso, aprofundamos nosso conhecimento sobre as funcionalidades da ferramenta Wireshark, o que nos permitiu utilizá-la de maneira mais eficiente.