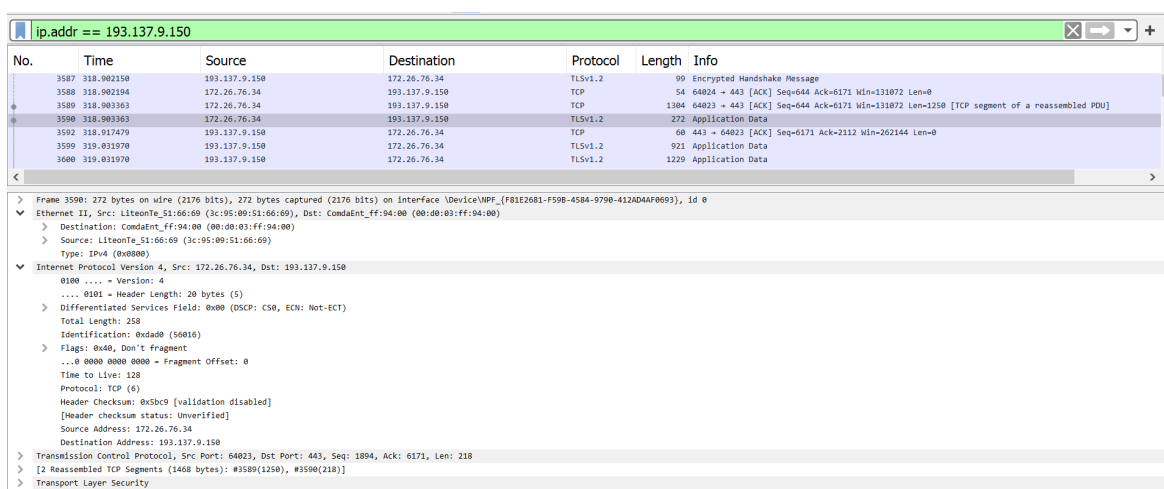


Trabalho Prático 3: Nível de Ligação Lógica: Redes Ethernet e Protocolo ARP

Alexandra Santos, Inês Ferreira e Joana Branco
Universidade do Minho, Departamento de Informática
email: {a94523, a97372, a96584}@alunos.uminho.pt

Captura e análise de Tramas Ethernet

Localize o estabelecimento da conexão entre o cliente e o servidor HTTP (sequência de tramas com as TCP flags TCP SYN, SYN-ACK, ACK ativas).



The image shows a Wireshark packet capture window with a filter set to 'ip.addr == 193.137.9.150'. The packet list shows several packets, with packet 3590 selected. The packet details pane shows the structure of the selected packet, which is an Ethernet II frame containing an Internet Protocol Version 4 packet, which in turn contains a Transmission Control Protocol (TCP) segment. The TCP segment is an encrypted handshake message.

No.	Time	Source	Destination	Protocol	Length	Info
3587	318.902150	193.137.9.150	172.26.76.34	TLSv1.2	99	Encrypted Handshake Message
3588	318.902194	172.26.76.34	193.137.9.150	TCP	54	64024 → 443 [ACK] Seq=644 Ack=6171 Win=131072 Len=0
3589	318.903363	172.26.76.34	193.137.9.150	TCP	1304	64023 → 443 [ACK] Seq=644 Ack=6171 Win=131072 Len=1250 [TCP segment of a reassembled PDU]
3590	318.903363	172.26.76.34	193.137.9.150	TLSv1.2	272	Application Data
3592	318.917479	193.137.9.150	172.26.76.34	TCP	60	443 → 64023 [ACK] Seq=6171 Ack=2112 Win=262144 Len=0
3599	319.031970	193.137.9.150	172.26.76.34	TLSv1.2	921	Application Data
3600	319.031970	193.137.9.150	172.26.76.34	TLSv1.2	1229	Application Data

Frame 3590: 272 bytes on wire (2176 bits), 272 bytes captured (2176 bits) on interface \Device\NPF_{F81E2681-F598-4584-9790-412AD4AF0093}, id 0
Ethernet II, Src: Liteont_51:66:69 (3c:95:09:51:66:69), Dst: ComdaEnt_ff:94:00 (00:00:03:ff:94:00)
> Destination: ComdaEnt_ff:94:00 (00:00:03:ff:94:00)
> Source: Liteont_51:66:69 (3c:95:09:51:66:69)
Type: IPv4 (0x0000)
Internet Protocol Version 4, Src: 172.26.76.34, Dst: 193.137.9.150
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 258
Identification: 0x0a00 (3968)
> Identification: 0x0a00 (3968)
> Flags: 0x00, Don't Fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: TCP (6)
Header Checksum: 0x5bc9 [validation disabled]
[Header checksum status: Unverified]
Source Address: 172.26.76.34
Destination Address: 193.137.9.150
> Transmission Control Protocol, Src Port: 64023, Dst Port: 443, Seq: 1894, Ack: 6171, Len: 218
> [2 Reassembled TCP Segments (1468 bytes): #3589(1250), #3590(218)]
> Transport Layer Security

Figura 1: Início da trama

1. Anote os endereços MAC de origem e de destino da trama capturada.

R: Endereço MAC de origem: 3c:95:09:51:66:69

Endereço MAC de destino: 00:d0:03:ff:94:00

2. Identifique a que sistemas se referem. Justifique.

R: Tendo em conta a tabela de encaminhamento e a tabela resultante do protocolo ARP podemos consultar a rota *Default*, mais concretamente, o endereço de *Gateway* e o *Physical Address*, consecutivamente. Considerando este último, verifica-se que é igual ao endereço MAC de destino da conexão entre o cliente e o servidor, ou seja, ao *elearning.uminho.pt*.

```
C:\Users\ojard>netstat -rn
=====
Interface List
=====
13...0a 00 27 00 00 0d .....VirtualBox Host-Only Ethernet Adapter
8...3e 95 09 51 66 69 .....Microsoft Wi-Fi Direct Virtual Adapter
12...4e 95 09 51 66 69 .....Microsoft Wi-Fi Direct Virtual Adapter #2
17...3c 95 09 51 66 69 .....Qualcomm Atheros QCA9377 Wireless Network Adapter
6...3c 95 09 51 66 6a .....Bluetooth Device (Personal Area Network)
1.....Software Loopback Interface 1
=====

IPv4 Route Table
=====
Active Routes:
=====
Network Destination    Netmask          Gateway          Interface        Metric
-----
0.0.0.0                0.0.0.0          172.26.254.254   172.26.76.34     55
127.0.0.0              255.0.0.0        On-link          127.0.0.1        331
127.0.0.1              255.255.255.255  On-link          127.0.0.1        331
127.255.255.255        255.255.255.255 On-link          127.0.0.1        331
172.26.0.0             255.255.0.0      On-link          172.26.76.34     311
172.26.76.34          255.255.255.255 On-link          172.26.76.34     311
172.26.255.255        255.255.255.255 On-link          172.26.76.34     311
192.168.56.0           255.255.255.0    On-link          192.168.56.1     281
192.168.56.1          255.255.255.255 On-link          192.168.56.1     281
192.168.56.255        255.255.255.255 On-link          192.168.56.1     281
224.0.0.0             240.0.0.0        On-link          127.0.0.1        331
224.0.0.0             240.0.0.0        On-link          192.168.56.1     281
224.0.0.0             240.0.0.0        On-link          172.26.76.34     311
255.255.255.255        255.255.255.255 On-link          127.0.0.1        331
255.255.255.255        255.255.255.255 On-link          192.168.56.1     281
255.255.255.255        255.255.255.255 On-link          172.26.76.34     311
=====
```

Figura 2: Tabela de encaminhamento do cliente

```
C:\Users\ojard>arp -a
Interface: 192.168.56.1 --- 0xd
Internet Address      Physical Address      Type
192.168.56.255        ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static

Interface: 172.26.76.34 --- 0x11
Internet Address      Physical Address      Type
172.26.254.254        00-d0-03-ff-94-00    dynamic
172.26.255.255        ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static
```

Figura 3: Protocolo ARP do cliente

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

R: Como podemos observar na figura 1, o campo do *Type* da trama Ethernet é 0x0800. Este campo representa o protocolo da camada superior, assim sendo, o IPv4.

4. Quantos bytes são usados no encapsulamento protocolar, i.e. desde o início da trama até ao início dos dados do nível aplicacional (Application Data Protocol: http-over-tls)? Calcule e indique, em percentagem, a sobrecarga (overhead) introduzida pela pilha protocolar.

R: No total, foram usados 272 *bytes* no encapsulamento protocolar, tal como se pode verificar no campo *Length* da figura 1. Estes valores foram extraídos do campo *header length* do nível IPv4 e nível TCP. Já ao nível da *Ethernet*, ao total dos dados foi retirado o *payload* do TCP e o seu valor de *header length*. Assim sendo, a sobrecarga pode ser calculada da seguinte forma:

$$\text{overhead} = (34+20+20)/272 * 100 = 27,2\%$$

A seguir responda às seguintes perguntas, baseado no conteúdo da trama Ethernet que contém o primeiro byte da resposta HTTP proveniente do servidor.

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

R: O endereço *Ethernet* da fonte é 00:d0:03:ff:94:00 e corresponde ao endereço *Gateway* da rota *Default*. Tendo em conta que o servidor não se encontra na mesma sub rede do cliente, esta conexão não é feita diretamente. Há que estabelecer ligação primeiro com um *router* é por isso que se observa esta rota.

38831	2470.671979	193.137.9.150	172.26.76.34	TLSv1.2	202	Application Data
38830	2470.671979	193.137.9.150	172.26.76.34	TLSv1.2	759	Application Data
38824	2470.666530	193.137.9.150	172.26.76.34	TCP	60	443 → 64120 [ACK] Seq=138 Ack=2838 Win=262144 Len=0
38822	2470.663528	193.137.9.150	172.26.76.34	TCP	60	443 → 64120 [ACK] Seq=138 Ack=1819 Win=260888 Len=0
38816	2470.660967	193.137.9.150	172.26.76.34	TLSv1.2	99	Encrypted Handshake Message


```

> Frame 38831: 202 bytes on wire (1616 bits), 202 bytes captured (1616 bits) on interface \Device\NPF_{F81E2681-F59B-4584-9790-412AD4AF0693}, id 0
▼ Ethernet II, Src: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00), Dst: LiteonTe_51:66:69 (3c:95:09:51:66:69)
  > Destination: LiteonTe_51:66:69 (3c:95:09:51:66:69)
  > Source: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
    Type: IPv4 (0x0800)
  > Internet Protocol Version 4, Src: 193.137.9.150, Dst: 172.26.76.34
  > Transmission Control Protocol, Src Port: 443, Dst Port: 64120, Seq: 843, Ack: 2838, Len: 148
  > Transport Layer Security

```

Figura 4: Trama com o primeiro byte da resposta HTTP do servidor

6. Qual é o endereço MAC do destino? A que sistema corresponde?

R: O endereço MAC do destino é 3c:95:09:51:66:69 e corresponde ao cliente, ou seja, ao nosso computador.

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

R: Tendo em conta a figura anterior, os protocolos contidos na trama são o IPv4, TCP e o Ethernet.

Protocolo ARP

8. Observe o conteúdo da tabela ARP. Diga o que significa cada uma das colunas.

R: Na primeira coluna temos os *Address*, que é o endereço. Na coluna *HWtype* vemos qual o protocolo de camada física que é a *Ethernet*. Já na *HWaddress* observa-se qual o endereço MAC, o protocolo ARP permite saber o endereço MAC através do seu IP. Na coluna da *flag* é apresentado um “C”. Este tipo de entrada é visto quando as entradas são inseridas dinamicamente pelo protocolo ARP (as flags dizem-nos como o MAC *Address* foi posto na memória). Na coluna *Iface* temos a interface da rede neste caso wlp0s20f3.

```

ines@ines-IdeaPad-5-14IIL05:~$ arp
Address          HWtype  HWaddress      Flags Mask    Iface
_gateway         ether    00:d0:03:ff:94:00 C              wlp0s20f3
ines@ines-IdeaPad-5-14IIL05:~$

```

Figura 5: Tabela ARP

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

R: Endereço origem 38:68:93:6b:39:3d

Endereço destino: ff:ff:ff:ff:ff:ff

Interpretando o resultado, o endereço de origem corresponde ao nosso computador e o endereço destino é o de *Broadcast*. Este último é apresentado desta maneira porque como não se sabe o endereço MAC destino, ele envia para todas as interfaces.

No.	Time	Source	Destination	Protocol	Length	Info
11	3.662565931	38:68:93:6b:39:3d	Broadcast	ARP	42	Who has 172.26.6.194? Tell 172.26.21.213
12	4.676097499	38:68:93:6b:39:3d	Broadcast	ARP	42	Who has 172.26.6.194? Tell 172.26.21.213
13	5.700016989	38:68:93:6b:39:3d	Broadcast	ARP	42	Who has 172.26.6.194? Tell 172.26.21.213
14	6.724040208	38:68:93:6b:39:3d	Broadcast	ARP	42	Who has 172.26.6.194? Tell 172.26.21.213
15	7.748069604	38:68:93:6b:39:3d	Broadcast	ARP	42	Who has 172.26.6.194? Tell 172.26.21.213
16	8.772095226	38:68:93:6b:39:3d	Broadcast	ARP	42	Who has 172.26.6.194? Tell 172.26.21.213
21	9.796130657	38:68:93:6b:39:3d	Broadcast	ARP	42	Who has 172.26.6.194? Tell 172.26.21.213
26	10.820054150	38:68:93:6b:39:3d	Broadcast	ARP	42	Who has 172.26.6.194? Tell 172.26.21.213
27	11.844011231	38:68:93:6b:39:3d	Broadcast	ARP	42	Who has 172.26.6.194? Tell 172.26.21.213
51	12.866125311	38:68:93:6b:39:3d	Broadcast	ARP	42	Who has 172.26.6.194? Tell 172.26.21.213
128	13.892089756	38:68:93:6b:39:3d	Broadcast	ARP	42	Who has 172.26.6.194? Tell 172.26.21.213
139	14.916076343	38:68:93:6b:39:3d	Broadcast	ARP	42	Who has 172.26.6.194? Tell 172.26.21.213
142	15.944108650	38:68:93:6b:39:3d	Broadcast	ARP	42	Who has 172.26.6.194? Tell 172.26.21.213

Frame 11: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface wlp0s20f3, id 0
 Ethernet II, Src: 38:68:93:6b:39:3d (38:68:93:6b:39:3d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 Destination: Broadcast (ff:ff:ff:ff:ff:ff)
 Source: 38:68:93:6b:39:3d (38:68:93:6b:39:3d)
 Address: 38:68:93:6b:39:3d (38:68:93:6b:39:3d)
 ...0. = LG bit: Globally unique address (factory default)
 ...0. = IG bit: Individual address (unicast)
 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: 38:68:93:6b:39:3d (38:68:93:6b:39:3d)
 Sender IP address: 172.26.21.213
 Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
 Target IP address: 172.26.6.194

Figura 6: Filtro ARP no Wireshark

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

R: O valor hexadecimal do campo *Type* da trama *Ethernet* é 0x0806 e corresponde ao protocolo ARP, isto é, o *payload* é um pacote ARP.

11. Como pode confirmar que se trata efetivamente de um pedido ARP? Identifique que tipo de endereços estão contidos na mensagem ARP? Que conclui?

R: Como podemos ver na figura 6, o campo “*Opcode: request (1)*” indica que é um pedido ARP. Os endereços contidos na mensagem são os IP do host origem e host destino, ou seja, *Sender Ip Address* e *Target Ip Address*, respetivamente.

12. Explícite que tipo de pedido ou pergunta é feita pelo host de origem.

R: A pergunta feita pelo host de origem é “*Who has x?*”, onde *x* corresponde ao endereço final (172.26.6.194 o endereço que demos *ping*), ou seja, onde ele deverá chegar, objetivo final. Interpretando a segunda parte da mensagem “*Tell y*”, corresponde ao endereço do *router* (172.26.21.213) que serve como mediador, ou seja, o intermediário.

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

No.	Time	Source	Destination	Protocol	Length	Info
1670	142.088070834	38:68:93:6b:39:3d	ComdaEnt_ff:94:00	ARP	42	Who has 172.26.254.254? Tell 172.26.21.213
1673	142.340497704	ComdaEnt_ff:94:00	38:68:93:6b:39:3d	ARP	60	172.26.254.254 is at 00:d0:03:ff:94:00
4391	235.780028116	38:68:93:6b:39:3d	ComdaEnt_ff:94:00	ARP	42	Who has 172.26.254.254? Tell 172.26.21.213
4399	235.825522392	ComdaEnt_ff:94:00	38:68:93:6b:39:3d	ARP	60	172.26.254.254 is at 00:d0:03:ff:94:00
4796	264.456059940	38:68:93:6b:39:3d	ComdaEnt_ff:94:00	ARP	42	Who has 172.26.254.254? Tell 172.26.21.213
4797	264.478707827	ComdaEnt_ff:94:00	38:68:93:6b:39:3d	ARP	60	172.26.254.254 is at 00:d0:03:ff:94:00
5610	323.332061684	38:68:93:6b:39:3d	ComdaEnt_ff:94:00	ARP	42	Who has 172.26.254.254? Tell 172.26.21.213
5617	323.359138140	ComdaEnt_ff:94:00	38:68:93:6b:39:3d	ARP	60	172.26.254.254 is at 00:d0:03:ff:94:00
5919	347.140056082	38:68:93:6b:39:3d	ComdaEnt_ff:94:00	ARP	42	Who has 172.26.254.254? Tell 172.26.21.213
5920	347.148293776	ComdaEnt_ff:94:00	38:68:93:6b:39:3d	ARP	60	172.26.254.254 is at 00:d0:03:ff:94:00
6009	388.359970363	38:68:93:6b:39:3d	ComdaEnt_ff:94:00	ARP	42	Who has 172.26.254.254? Tell 172.26.21.213
6010	388.508668706	ComdaEnt_ff:94:00	38:68:93:6b:39:3d	ARP	60	172.26.254.254 is at 00:d0:03:ff:94:00
9144	717.575963560	38:68:93:6b:39:3d	ComdaEnt_ff:94:00	ARP	42	Who has 172.26.254.254? Tell 172.26.21.213

Frame 1673: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface wlp0s20f3, id 0
 Ethernet II, Src: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00), Dst: 38:68:93:6b:39:3d (38:68:93:6b:39:3d)
 Address Resolution Protocol (reply)
 Hardware type: Ethernet (1)
 Protocol type: IPv4 (0x0800)
 Hardware size: 6
 Protocol size: 4
 Opcode: reply (2)
 Sender MAC address: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
 Sender IP address: 172.26.254.254
 Target MAC address: 38:68:93:6b:39:3d (38:68:93:6b:39:3d)

Figura 7: ARP reply

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

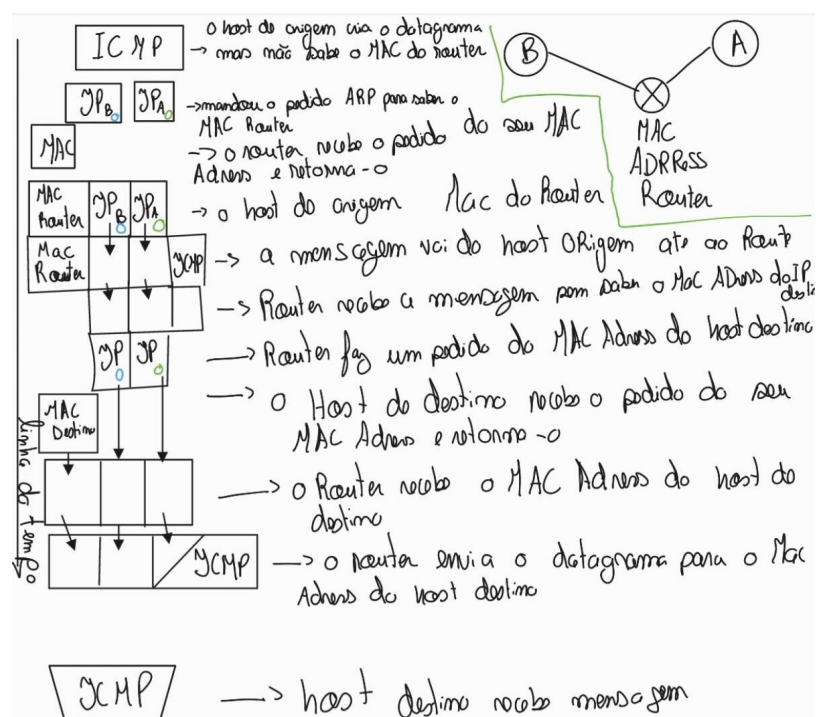
R: O valor do campo ARP *opcode* é “reply (2)”, ou seja, corresponde a uma resposta.

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

R: A resposta ao pedido ARP está representada no campo *Sender MAC address*.

14. Na situação em que efetua um ping a outro host, assumo que este está diretamente ligado ao mesmo router, mas noutra subrede, e que todas as tabelas ARP se encontram inicialmente vazias. Esboce um diagrama em que indique claramente, e de forma cronológica, todas as mensagens ARP e ICMP trocadas, até à recepção da resposta ICMP do host destino.

R:



Domínios de colisão

15. Através da opção tcpdump verifique e compare como flui o tráfego nas diversas interfaces do dispositivo de interligação no departamento A (LAN partilhada) e no departamento B (LAN comutada) quando se gera tráfego intra-departamento (por exemplo, fazendo ping IPaddr da Bela para Monstro, da Jasmine para o Alladin, etc.) Que conclui?

R: A diferença entre o switch e o hub é que o primeiro recebe um pacote com informação e verifica qual é o destino na sua tabela de encaminhamento. Por outro lado, o hub recebe um pacote e envia a informação dela para todo o lado, criando assim colisões e tráfego. Logo, podemos concluir que os *switches* são muito mais rápidos.

```
root@Bela:/tmp/pycore.32929/Bela.conf# tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C17:39:00.211453 IP 10.0.4.1 > 224.0.0.5: OSPFv2, Hello, length 44
17:39:02.212328 IP 10.0.4.1 > 224.0.0.5: OSPFv2, Hello, length 44

2 packets captured
2 packets received by filter
0 packets dropped by kernel
root@Bela:/tmp/pycore.32929/Bela.conf# ping 10.0.4.21
PING 10.0.4.21 (10.0.4.21) 56(84) bytes of data:
64 bytes from 10.0.4.21: icmp_seq=1 ttl=64 time=0.039 ms
64 bytes from 10.0.4.21: icmp_seq=2 ttl=64 time=0.160 ms
^C
--- 10.0.4.21 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1012ms
rtt min/avg/max/mdev = 0.039/0.099/0.160/0.060 ms
root@Bela:/tmp/pycore.32929/Bela.conf#
```

Figura 9: Tráfego no departamento A

```
root@Jasmine:/tmp/pycore.32929/Jasmine.conf# tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C17:39:48.675317 IP6 fe80::200:ff:feaa:58 > ff02::5: OSPFv3, Hello, length 36
17:39:48.818729 IP 192.168.16.153 > 224.0.0.5: OSPFv2, Hello, length 44

2 packets captured
2 packets received by filter
0 packets dropped by kernel
root@Jasmine:/tmp/pycore.32929/Jasmine.conf# ping 192.168.16.156
PING 192.168.16.156 (192.168.16.156) 56(84) bytes of data:
64 bytes from 192.168.16.156: icmp_seq=1 ttl=64 time=0.234 ms
64 bytes from 192.168.16.156: icmp_seq=2 ttl=64 time=0.560 ms
64 bytes from 192.168.16.156: icmp_seq=3 ttl=64 time=0.644 ms
^C
--- 192.168.16.156 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2026ms
rtt min/avg/max/mdev = 0.234/0.479/0.644/0.176 ms
root@Jasmine:/tmp/pycore.32929/Jasmine.conf#
```

Figura 10: Tráfego no departamento B

16. Construa manualmente a tabela de comutação do switch do Departamento B, atribuindo números de porta à sua escolha.

R: A topologia do departamento B usada no relatório anterior é apresentada na figura 11.

Porta	MAC Address	Interface	TTL
1	00:00:00:aa:00:58	e0	64
2	00:00:00:aa:00:59	e1	64
3	00:00:00:aa:00:5a	e2	64
4	00:00:00:aa:00:5b	e3	64

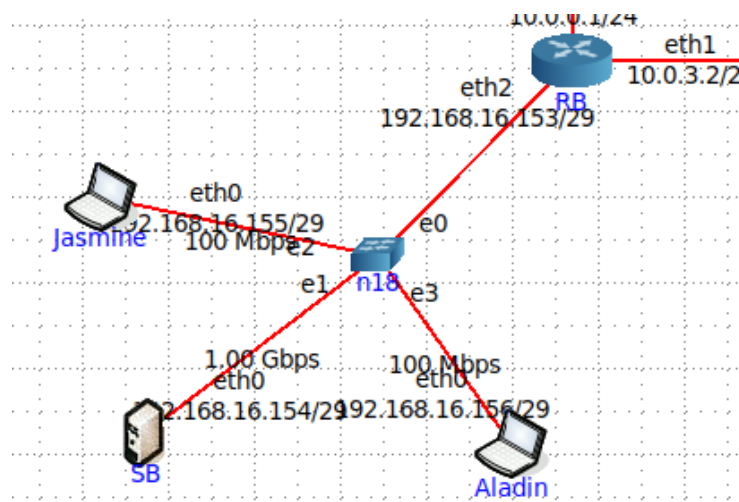


Figura 11: Topologia do departamento B

Conclusão

Neste trabalho foi possível explorar o conhecimento a nível da ligação lógica, mais concretamente, as rede *Ethernet* e o protocolo ARP.

Desenvolveram-se conceitos mencionados nos trabalhos práticos anteriores e que são bastante relevantes para o objetivo final de aprendizagem.

Neste exercício foram sentidas menos dificuldades em comparação aos exercícios anteriores e sentimos que os conceitos foram bem interiorizados.