



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

Redes de Computadores

Grupo 7 - TP8

Gabriela Santos Ferreira da Cunha - a97393

Nuno Guilherme Cruz Varela - a96455

Simão Jorge da Silva Costa - a95176

1 Captura e análise de Tramas Ethernet

Assegure-se que a cache do seu browser está vazia.

Ative o Wireshark na sua máquina nativa.

No seu browser, acesse ao URL <https://elearning.uminho.pt>.

Pare a captura do Wireshark., e proceda da seguinte forma:

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

Após a fase de estabelecimento seguro da conexão, obtenha o número de ordem da sequência de bytes capturada (coluna da esquerda na janela do Wireshark) correspondente à trama que transporta os primeiros dados aplicativos enviados do cliente para o servidor (Application Data). Identifique também o número de ordem da trama com a resposta proveniente do servidor que contém os dados correspondentes ao acesso web realizado pelo cliente (browser).

28 0.104025644	172.26.80.79	193.137.9.150	TLv1.2	748 Application Data
29 0.121679768	193.137.9.150	172.26.80.79	TCP	66 443 - 45468 [ACK] Seq=6171 Ack=1326 Win=262144 Len=0 TSval=16...
30 0.153859942	193.137.9.150	172.26.80.79	TLv1.2	922 Application Data

Figura 1: Dados aplicativos transportados entre o cliente e o servidor.

Pela figura 1, o número de ordem da sequência de bytes capturada correspondente à trama que transporta os primeiros dados aplicativos enviados do cliente para o servidor é 28 e o número de ordem da trama com a resposta proveniente do servidor é 30.

Responda às perguntas seguintes com base no conteúdo da trama Ethernet que contém a mensagem de acesso ao servidor (HTTP GET encriptada).

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

▶ Frame 28: 748 bytes on wire (5984 bits), 748 bytes captured (5984 bits) on interface wlp3s0, id 0
▼ Ethernet II, Src: LiteonTe 8a:34:ca (ac:b5:7d:8a:34:ca), Dst: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
▶ Destination: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
▶ Source: LiteonTe 8a:34:ca (ac:b5:7d:8a:34:ca)
Type: IPv4 (0x0800)
▶ Internet Protocol Version 4, Src: 172.26.80.79, Dst: 193.137.9.150
▶ Transmission Control Protocol, Src Port: 45468, Dst Port: 443, Seq: 644, Ack: 6171, Len: 682
▶ Transport Layer Security

Figura 2: Dados relativos à trama que transporta os primeiros dados enviados do cliente para o servidor.

Através da figura 2, verificamos que o endereço MAC origem (cliente) é “ac:b5:7d:8a:34:ca” e o do destino (servidor) é “00:d0:03:ff:94:00”.

Exercício 2 Identifique a que sistemas se referem. Justifique.

```
inet 172.26.80.79 netmask 255.255.0.0 broadcast 172.26.255.255
inet6 fe80::1bb8:e272:1f11:78cf prefixlen 64 scopeid 0x20<link>
ether ac:b5:7d:8a:34:ca txqueuelen 1000 (Ethernet)
```

Figura 3: Comando “ifconfig” - endereços IP e MAC do nosso computador.

O endereço MAC de origem é referente ao nosso computador e o de destino ao servidor do *elarning.uminho.pt*.

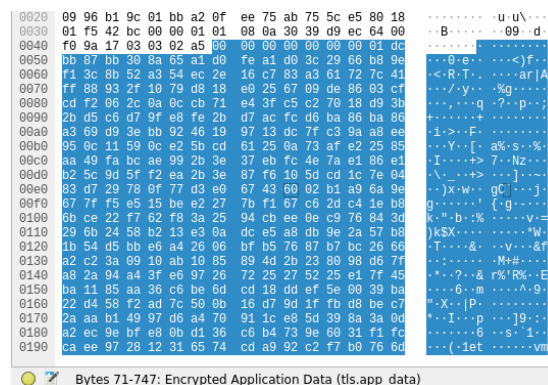
Exercício 3 Qual o valor hexadecimal do campo “Type” da trama Ethernet? O que significa?

```
▼ Ethernet II, Src: LiteonTe_8a:34:ca (ac:b5:7d:8a:34:ca), Dst: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
  ▶ Destination: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
  ▶ Source: LiteonTe_8a:34:ca (ac:b5:7d:8a:34:ca)
  ▶ Type: IPv4 (0x0800)
```

Figura 4: Valor hexadecimal do campo “Type”.

O campo “Type” tem valor hexadecimal 0x0800 e representa o protocolo que a camada superior está a usar (IPv4).

Exercício 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.



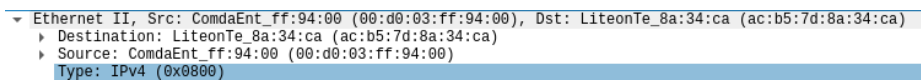
```
0020 09 96 b1 9c 01 bb a2 0f ee 75 ab 75 5c e5 80 18 .....u-u...
0030 01 f5 42 bc 00 00 01 01 00 0a 30 39 d9 ec 64 00 ..B.....09.d.
0040 f0 9a 17 03 03 02 a5 00 00 00 00 00 00 01 dc .....<f...
0050 bb 87 bb 30 8a 65 a1 d0 fe a1 d0 3c 29 66 b8 9e ...0.e...<f...
0060 f1 3c 8b 52 a3 54 ec 2e 16 c7 83 a3 61 72 7c 41 <.R.T...ar|A
0070 ff 88 93 2f 10 79 d8 18 e0 25 67 09 de 86 03 cf .../y...%g...
0080 cd f2 06 2c 0a 0c cb 71 e4 3f c5 c2 70 18 d9 3b ...q?...p...
0090 2b d5 c6 d7 9f e8 fe 2b d7 ac fc d6 ba 86 ba 86 .....+.....
00a0 a3 69 d9 3e bb 92 46 19 97 13 dc 7f c3 9a a8 ee ..1>..F.....
00b0 95 0e 11 59 0e e2 5b cd 61 25 0a 73 af e2 25 85 ...Y...[a%:s-%
00c0 aa 49 fa bc ae 90 2b 3e 37 eb fc 4e 7a e1 06 e1 ..I...>7..Nz...
00d0 b2 5c 9d 5f f2 ea 2b 3e 87 f6 10 5d cd 1c 7e 04 ..\...+>...]-...
00e0 83 d7 29 78 0f 77 d3 e0 67 43 00 02 b1 a9 6a 9e ...x.w...gC...j.
00f0 67 7f f5 e5 15 be e2 27 7b f1 67 c6 2d c4 1e b8 g.....{g...
0100 6b ce 22 f7 62 f8 3a 25 94 cb ee 0e c9 76 84 3d k..".b.:%.....v.=
0110 29 6b 24 58 b2 13 e3 0a dc e5 a8 db 9e 2a 57 b8 )kSX.....*W.
0120 1b 54 d5 bb e6 a4 26 06 bf b5 76 87 b7 bc 26 66 ..T...&...v...&f
0130 a2 c2 3a 09 19 ab 10 85 89 4d 2b 23 80 98 d6 7f .....M#....
0140 a8 2a 94 a4 3f e0 97 26 72 25 27 52 25 e1 7f 45 ...?..& r%R%..E
0150 ba 11 85 aa 30 c6 be 6d cd 18 dd ef 5e 00 39 ba ...6..m....A.9.
0160 22 d4 58 f2 ad 7c 50 0b 16 d7 9d 1f fb d8 be c7 ..X..|P.....
0170 2a aa b1 49 97 d6 a4 70 91 1c e8 5d 30 8a 3a 0d ..I...p...j9...
0180 a2 ec 9e bf e8 0b d1 36 c6 b4 73 9e 60 31 f1 fc .....6...s..1..
0190 ca ee 97 28 12 31 65 74 cd a9 92 c2 f7 b0 76 6d ...(-1et .....vm
```

Bytes 71-747: Encrypted Application Data (tls.app_data)

Figura 5: Bytes da trama onde são armazenados os dados.

No encapsulamento protocolar são utilizados 71 bytes. Os restantes bytes são usados para armazenar os dados do nível aplicacional (71 até 747). A sobrecarga introduzida pela pilha protocolar é de $\frac{71}{747} \times 100 = 9.505\%$.

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



```
▼ Ethernet II, Src: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00), Dst: LiteonTe_8a:34:ca (ac:b5:7d:8a:34:ca)
  ▶ Destination: LiteonTe_8a:34:ca (ac:b5:7d:8a:34:ca)
  ▶ Source: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
  Type: IPv4 (0x0800)
```

Figura 6: Dados relativos à trama que transporta os primeiros dados enviados do servidor para o cliente.

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

Através da figura 6, o endereço Ethernet da fonte é “00:d0:03:ff:94:00” e o sistema de rede ao qual corresponde é o servidor.

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

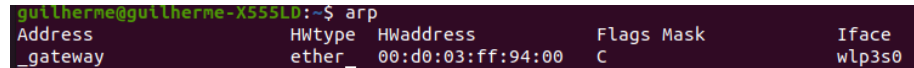
A partir da figura 6, mais uma vez, o endereço MAC do destino é “ac:b5:7d:8a:34:ca” e o sistema ao qual corresponde é o cliente (o nosso computador).

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

Os vários protocolos contidos na trama recebida são Ethernet II, TCP e IPV4.

2 Protocolo ARP

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

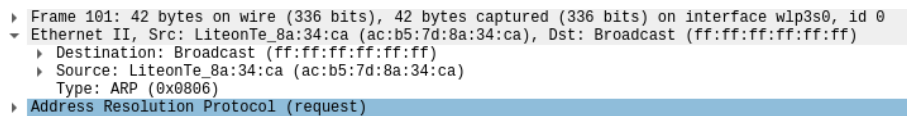


Address	HWtype	HWaddress	Flags	Mask	Iface
_gateway	ether	00:d0:03:ff:94:00	C		wlp3s0

Figura 7: Conteúdo da tabela ARP.

- A primeira coluna da tabela, "Address", corresponde ao endereço IP do router - gateway da rede local.
- Na segunda coluna podemos analisar o tipo de conexão existente, isto é, o protocolo de camada física utilizado - Ethernet.
- Na terceira coluna, está presente o endereço MAC do router.
- A quarta coluna diz-nos se o endereço foi definido pelo utilizador, extraído manualmente ou é incompleto. Como o valor é "C", concluímos que este registo foi obtido dinamicamente pelo protocolo ARP.
- A quinta coluna indica a máscara de subrede.
- A última coluna indica-nos o nome da interface de rede.

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



```
▶ Frame 101: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface wlp3s0, id 0
▼ Ethernet II, Src: LiteonTe_8a:34:ca (ac:b5:7d:8a:34:ca), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▶ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ▶ Source: LiteonTe_8a:34:ca (ac:b5:7d:8a:34:ca)
  ▶ Type: ARP (0x0806)
▶ Address Resolution Protocol (request)
```

Figura 8: Dados relativos à trama que contém a mensagem com o pedido ARP.

O endereço MAC da origem é "ac:b5:7d:8a:34:ca" e o endereço MAC do destino é "ff:ff:ff:ff:ff:ff". O endereço destino é o de broadcast, visto que o host que faz o ping necessita de saber qual é o endereço destino. Desta forma, envia uma mensagem para todas as interfaces com o objetivo de obter uma resposta da máquina destino com o seu endereço MAC.

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

Pela figura 8, verificamos que o valor hexadecimal do campo tipo é 0x0806 e este representa o protocolo ARP.

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

```
▶ Frame 101: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface wlp3s0, id 0
▶ Ethernet II, Src: LiteonTe_8a:34:ca (ac:b5:7d:8a:34:ca), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▼ Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: LiteonTe_8a:34:ca (ac:b5:7d:8a:34:ca)
  Sender IP address: 192.168.83.102
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 192.168.83.10
```

Figura 9: Dados do campo ARP (request) relativos à trama que contém a mensagem com o pedido ARP.

Como se verifica na figura acima, trata-se de um pedido ARP, visto que o campo *opcode* tem o valor “*request (1)*”. Na mensagem ARP estão incluídos 4 endereços :

- *Sender MAC address* - endereço MAC da nossa máquina
- *Sender IP address* - endereço IP da nossa máquina
- *Target MAC address* - endereço MAC do destino
- *Target IP address* - endereço IP do destino

O endereço MAC do destino encontra-se a zeros, visto que a tabela ARP foi limpa e, portanto, o endereço é desconhecido.

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

101 6.952152764	LiteonTe_8a:34:ca	Broadcast	ARP	42 Who has 192.168.83.10? Tell 192.168.83.102
102 7.815687357	b0:60:88:e7:28:63	LiteonTe_8a:34:ca	ARP	42 192.168.83.10 is at b0:60:88:e7:28:63
120 12.180270682	b0:60:88:e7:28:63	LiteonTe_8a:34:ca	ARP	42 Who has 192.168.83.102? Tell 192.168.83.10
121 12.180295719	LiteonTe_8a:34:ca	b0:60:88:e7:28:63	ARP	42 192.168.83.102 is at ac:b5:7d:8a:34:ca

Figura 10: Trama com a pergunta feita pelo host de origem.

A pergunta feita pelo host de origem é “Who has 192.168.83.10? Tell 192.168.83.102“. O host de origem pretende saber quem tem o endereço IP 192.168.83.10, perguntando, assim, a todos os hosts. A resposta deve conter o respetivo endereço MAC deste host e deve ser enviada para o endereço IP 192.168.83.102.

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

```

▶ Frame 102: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface wlp3s0, id 0
▶ Ethernet II, Src: b0:60:88:e7:28:63 (b0:60:88:e7:28:63), Dst: LiteonTe_8a:34:ca (ac:b5:7d:8a:34:ca)
▼ Address Resolution Protocol (reply)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0000)
  Hardware size: 6
  Protocol size: 4
  Opcode: reply (2)
  Sender MAC address: b0:60:88:e7:28:63 (b0:60:88:e7:28:63)
  Sender IP address: 192.168.83.10
  Target MAC address: LiteonTe_8a:34:ca (ac:b5:7d:8a:34:ca)
  Target IP address: 192.168.83.102

```

Figura 11: Trama com a resposta ao pedido ARP.

A resposta ao pedido ARP efetuado encontra-se no frame imediatamente a seguir ao do pedido, isto é, frame 102.

Alínea A Qual o valor do campo ARP opcode? O que especifica?

O valor do campo opcode é “reply (2)“, o que significa que se trata de uma mensagem resposta do tipo ARP.

Alínea B Em que campo da mensagem ARP está a resposta ao pedido ARP?

A resposta ao pedido ARP está no campo Sender MAC Address.

Exercício 14 Na situação em que efetua um ping a outro host, assuma 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.

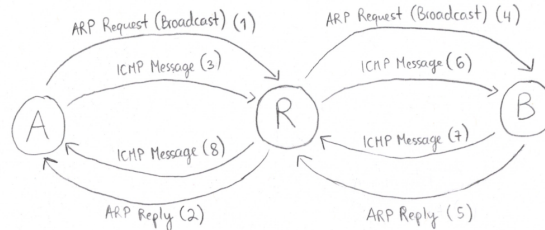


Figura 12: Diagrama com as mensagens ARP e ICMP trocadas.

3 Domínios de Colisão

Ative o emulador CORE e carregue a topologia de rede com a solução de sub-netting que construiu no âmbito do TP2. Substitua o switch do departamento A por um hub (repetidor).

Exercício 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?

Dois terminais de linha de comando mostrando a execução do tcpdump. O terminal da esquerda (root@SA) mostra a captura de pacotes na interface eth0, incluindo mensagens de Hello OSPFv2 e mensagens de echo request/reply de ICMP. O terminal da direita (root@Bela) mostra o resultado de um ping de 192.168.87.131 para 192.168.87.131, com estatísticas de tempo de resposta (rtt) e perda de pacotes.

Figura 13: Fluxo do tráfego no departamento A.


```

root@88B:/tmp/pycore,33917/SB.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
16:31:04.826326 IP 192.168.87.145 > 224.0.0.5: OSPFv2, Hello, length 44
16:31:06.772930 IP 192.168.87.148 > 192.168.87.147: ICMP echo request, id 43, seq 1, length 64
16:31:06.824114 IP 192.168.87.145 > 224.0.0.5: OSPFv2, Hello, length 44
16:31:08.865337 IP 192.168.87.145 > 224.0.0.5: OSPFv2, Hello, length 44
16:31:09.883944 IP 6 fe80::200:ff:feaa:15 > ff02::5: OSPFv3, Hello, length 36
5 packets captured
5 packets received by filter
0 packets dropped by kernel
root@88B:/tmp/pycore,33917/SB.conf#

root@Jasmine1:/tmp/pycore,33917/Jasmine.conf# ping 192.168.87.147
PING 192.168.87.147 (192.168.87.147) 56(84) bytes of data:
64 bytes from 192.168.87.147: icmp_seq=1 ttl=64 time=1.00 ms
64 bytes from 192.168.87.147: icmp_seq=2 ttl=64 time=0.184 ms
64 bytes from 192.168.87.147: icmp_seq=3 ttl=64 time=0.132 ms
--- 192.168.87.147 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2020ms
rtt min/avg/max/mdev = 0.132/0.439/1.002/0.398 ms
root@Jasmine1:/tmp/pycore,33917/Jasmine.conf#

```

Figura 14: Fluxo do tráfego no departamento B.

No departamento A, rede partilhada, o dispositivo de interligação (*hub*) envia para todos os dispositivos informação acerca do ping feito do *host* Bela para o Monstro. Ao observar a figura 13, verificamos o comportamento referido, em que o Servidor A recebe informação sobre este ping.

Já no departamento B, rede comutada, em que se utiliza o dispositivo de interligação *switch*, este encaminha a mensagem diretamente para o dispositivo pretendido e, ao contrário do *hub*, os restantes dispositivos não têm informação acerca desta mensagem.

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

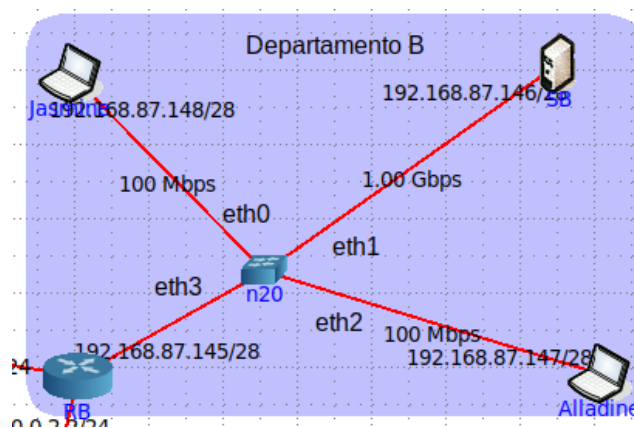


Figura 15: Topologia do departamento B.

```

vcmd
root@Jasmine:/tmp/pycore.41123/Jasmine.conf# ping 192.168.87.146
PING 192.168.87.146 (192.168.87.146) 56(84) bytes of data.
64 bytes from 192.168.87.146: icmp_seq=1 ttl=64 time=0.926 ms
^C
--- 192.168.87.146 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.926/0.926/0.926/0.000 ms
root@Jasmine:/tmp/pycore.41123/Jasmine.conf# ping 192.168.87.147
PING 192.168.87.147 (192.168.87.147) 56(84) bytes of data.
64 bytes from 192.168.87.147: icmp_seq=1 ttl=64 time=0.281 ms
^C
--- 192.168.87.147 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.281/0.281/0.281/0.000 ms
root@Jasmine:/tmp/pycore.41123/Jasmine.conf# ping 192.168.87.145
PING 192.168.87.145 (192.168.87.145) 56(84) bytes of data.
64 bytes from 192.168.87.145: icmp_seq=1 ttl=64 time=0.881 ms
^C
--- 192.168.87.145 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.881/0.881/0.881/0.000 ms
root@Jasmine:/tmp/pycore.41123/Jasmine.conf# arp -n
Address                  Hwtype  Hwaddress  Flags Mask              Iface
192.168.87.146            ether    00:00:00:aa:00:0c    C                eth0
192.168.87.145            ether    00:00:00:aa:00:19    C                eth0
192.168.87.147            ether    00:00:00:aa:00:0d    C                eth0
root@Jasmine:/tmp/pycore.41123/Jasmine.conf# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.87.148 netmask 255.255.255.240 broadcast 0.0.0.0
    inet6 2001:5::20 prefixlen 64 scopeid 0x0<global>
    inet6 fe80::200:ff:feaa:b prefixlen 64 scopeid 0x20<link>
    ether 00:00:00:aa:00:0b txqueuelen 1000 (Ethernet)
    RX packets 249 bytes 21419 (21.4 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 22 bytes 1648 (1.6 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Figura 16: Endereços MAC das interfaces do departamento B.

Através das figuras acima, construímos a seguinte tabela:

Interface	Endereço MAC
0	00:00:00:aa:00:0b
1	00:00:00:aa:00:0c
2	00:00:00:aa:00:0d
3	00:00:00:aa:00:19

Tabela 1: Tabela de comutação do switch do departamento B.

4 Conclusão

Na primeira parte deste trabalho, capturamos e analisamos tramas Ethernet, com recurso ao Wireshark.

Na segunda parte, estudamos o funcionamento do protocolo ARP, que permite fazer um mapeamento entre endereços do nível de rede e endereços do nível de ligação lógica de forma a possibilitar a entrega de dados.

Por último, utilizando o CORE, pudemos analisar a diferença entre *switches* e *hubs* e os impactos que estes têm no tráfego de rede, no sentido de controlar ou dividir domínios de colisão.

Assim, este trabalho permitiu-nos, essencialmente, aprofundar os nossos conhecimentos acerca do funcionamento do nível lógico de rede, com foco na tecnologia Ethernet e no protocolo ARP (*Address Resolution Protocol*).