

Universidade do Minho
Redes de Computadores
Trabalho Prático III

Ano letivo 2021/2022

a97363, Gabriel Alexandre Monteiro da Silva

a96106, Miguel Silva Pinto

a97613, Pedro Miguel Castilho Martins

Captura e análise de Tramas Ethernet

A captura de tráfego deverá ser efetuada usando a aplicação Wireshark instalada na máquina nativa. Uma vez que as salas de aula atuais não disponibilizam uma ligação com fios a uma rede Ethernet, a captura será realizada na rede Eduroam. Este facto não impacta na realização do trabalho porque, por defeito, o Wireshark disponibiliza o tráfego capturado ao utilizador como sendo (pseudo) Ethernet.

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

Ative o Wireshark na sua máquina nativa.

No seu browser, aceda 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, SYN ACK, 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).

Note que os dados aplicativos são enviados de forma segura usando o protocolo TLS (Transport Layer Security), mapeados para um segmento TCP, transportado num datagrama IP que, por sua vez, é encapsulado no campo de dados da trama Ethernet. Expanda a informação do nível da ligação de dados e observe o conteúdo da trama Ethernet (cabeçalho e dados (payload)).

Responda às perguntas seguintes com base no conteúdo da trama Ethernet que contém a mensagem de acesso ao servidor (HTTP GET encriptada). Sempre que aplicável, deve incluir a impressão dos dados relativa ao pacote capturado (ou parte dele) necessária para fundamentar a resposta à questão colocada. Para imprimir um pacote, use File->Print, escolha Selected packet only e Packet summary line, ou use qualquer outro método que lhe pareça adequado para a captura desses dados. Selecione o mínimo detalhe necessário para responder à pergunta.

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

R: Endereço MAC da origem -> d8:3b:bf:f1:00:27

Endereço MAC do destino-> 00:d0:03:ff:94:00

No.	Time	Source	Destination	Protocol	Length	Info
50	1.261947138	104.18.32.68	172.26.36.203	OCSP	1249	Response
51	1.261996264	172.26.36.203	104.18.32.68	TCP	54	46422 → 80 [ACK] Seq=42
52	1.267822941	172.26.36.203	193.137.9.150	TLSv1.2	542	Application Data
53	1.281111509	193.137.9.150	172.26.36.203	TCP	66	443 → 37322 [ACK] Seq=6
54	1.300243242	193.137.9.150	172.26.36.203	TLSv1.2	922	Application Data
▶ Frame 52: 542 bytes on wire (4336 bits), 542 bytes captured (4336 bits) on interface wlo1, id 0						
▼ Ethernet II, Src: IntelCor_f1:00:27 (d8:3b:bf:f1:00:27), Dst: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)						
▶ Destination: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)						
▶ Source: IntelCor_f1:00:27 (d8:3b:bf:f1:00:27)						
Type: IPv4 (0x0800)						
▶ Internet Protocol Version 4, Src: 172.26.36.203, Dst: 193.137.9.150						
▼ Transmission Control Protocol, Src Port: 37322, Dst Port: 443, Seq: 644, Ack: 6171, Len: 476						

Fig. 1 - Endereços MAC de origem e destino.

2. Identifique a que sistemas se referem. Justifique.

R: O sistema de origem refere-se ao nosso computador, e o sistema destino refere-se à interface do router da rede local, pois o nosso computador não conhece endereços MAC fora da rede local. Quanto ao sistema origem, podemos verificar que o nosso endereço MAC é o mesmo, através do comando “ip link”.

```
miguelcj1@Paredes:~$ ip link
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: wlo1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP mode DORMANT group default qlen 1000
    link/ether d8:3b:bf:f1:00:27 brd ff:ff:ff:ff:ff:ff
    altname wlp0s20f3
miguelcj1@Paredes:~$
```

Fig. 2 - Endereço MAC do nosso computador.

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

```
▼ Ethernet II, Src: IntelCor_f1:00:27 (d8:3b:bf:f1:00:27), Dst: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
  > Destination: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
  > Source: IntelCor_f1:00:27 (d8:3b:bf:f1:00:27)
    Type: IPv4 (0x0800)
```

Fig. 3 - Campo Type da trama Ethernet.

R: Valor do campo Type: 0x0800. Indica o tipo de dados que a trama transporta, neste caso um pacote 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: O número de bytes usados no encapsulamento protocolar são:

Ethernet II - 14 bytes | $14/542 = 2.583\%$

IPv4 - 20 bytes | $20/542 = 3.690\%$

TCP - 32 bytes | $32/542 = 5.904\%$

Total : 66 bytes | $66/542 = 12.177\%$

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, correspondente ao endereço MAC do router da rede local, pois só é possível saber os endereços MAC dos dispositivos conectados à rede local.

No.	Time	Source	Destination	Protocol	Length	Info
49	1.175085164	104.18.32.68	172.26.36.203	TCP	60	80 → 46422 [ACK] Seq=1 Ack=429 Win=68608 Len=0
50	1.261947138	104.18.32.68	172.26.36.203	OCSP	1249	Response
51	1.261996264	172.26.36.203	104.18.32.68	TCP	54	46422 → 80 [ACK] Seq=429 Ack=1196 Win=63104 Len=0
52	1.267822941	172.26.36.203	193.137.9.150	TLSv1.2	542	Application Data
53	1.281111509	193.137.9.150	172.26.36.203	TCP	66	443 → 37322 [ACK] Seq=6171 Ack=1120 Win=262144 Len=0 TSv
54	1.300243242	193.137.9.150	172.26.36.203	TLSv1.2	922	Application Data
55	1.300278866	172.26.36.203	193.137.9.150	TCP	66	37322 → 443 [ACK] Seq=1120 Ack=7027 Win=63360 Len=0 TSv


```

> Frame 54: 922 bytes on wire (7376 bits), 922 bytes captured (7376 bits) on interface wlo1, id 0
▼ Ethernet II, Src: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00), Dst: IntelCor_f1:00:27 (d8:3b:bf:f1:00:27)
  > Destination: IntelCor_f1:00:27 (d8:3b:bf:f1:00:27)
  > Source: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
  Type: IPv4 (0x0800)

```

Fig. 4 - Trama que contém o primeiro byte da resposta HTTP.

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

R: O endereço MAC do destino é d8:3b:bf:f1:00:27, correspondente ao nosso computador.

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

R: Ethernet, IPV4, TCP.

Protocolo ARP

Nesta secção, pretende-se analisar a operação do protocolo ARP. Verifique o conteúdo da cache ARP do seu computador.

- Windows: Digite arp ou c:\windows\system32\arp na linha de comando.
- Linux/Unix: O comando arp pode estar em vários locais, nomeadamente /sbin/arp (Linux), /usr/sbin/arp (FreeBSD) ou /usr/etc/arp (para outras variantes de Unix). O comando arp sem argumentos ou com a opção -a mostra o conteúdo da cache do seu computador (consultar man arp).

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

R: A primeira coluna indica o endereço IP do host, a segunda coluna indica o endereço MAC e a última coluna indica o tipo de endereçamento.

```
Microsoft Windows [Version 10.0.19043.1645]
(c) Microsoft Corporation. Todos os direitos reservados.

C:\Users\pemic>arp -a

Interface: 172.26.33.26 --- 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
```

Fig. 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 destino usado?

```
> Frame 15: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{F70627F3-903D-430D-A677-211F0CBC56DE}, id 0
▼ Ethernet II, Src: Chongqin_b0:8b:51 (d4:1b:81:b0:8b:51), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▼ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    Address: Broadcast (ff:ff:ff:ff:ff:ff)
    ....1. .... = LG bit: Locally administered address (this is NOT the factory default)
    ....1. .... = IG bit: Group address (multicast/broadcast)
  ▼ Source: Chongqin_b0:8b:51 (d4:1b:81:b0:8b:51)
    Address: Chongqin_b0:8b:51 (d4:1b:81:b0:8b:51)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
  ▼ Address Resolution Protocol (request)
```

Fig. 6 - Pedido ARP capturado no WireShark.

R: O endereço MAC de origem é d4:1b:81:b0:8b:51 e o endereço MAC de destino é ff:ff:ff:ff:ff:ff.

O endereço MAC do destino é o endereço de broadcast, com os bits todos a 1. Este endereço é usado para que todos os hosts da rede local recebam a trama Ethernet, e estes hosts verificam se há correspondência entre os seus endereços IP e os endereços IP da trama. Se não houver correspondência, o host descarta a trama Ethernet, caso contrário, este envia o seu endereço MAC ao host de origem, guardando esse endereço MAC recebido, na sua tabela ARP.

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

R: O valor hexadecimal é 0x0806, como podemos ver na figura 6. Indica que encapsula uma frame 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?

```
▼ Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: Chongqin_b0:8b:51 (d4:1b:81:b0:8b:51)
  Sender IP address: 172.26.33.26
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 172.26.254.254
```

Fig. 7 - Address Resolution Protocol.

R: Podemos confirmar que se trata de um pedido ARP, pois o campo *opcode* tem o valor “request(1)”. Os endereços que a mensagem ARP contém são os endereços MAC e endereços IP. Como o Sender quer descobrir o endereço MAC do host com o endereço IP 172.26.254.254, o host Sender envia a todos os hosts uma mensagem com um Target MAC Address 00:00:00:00:00:00 (endereço de broadcast).

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

15 10.645463	Chongqin_b0:8b:51	Broadcast	ARP	42 Who has 172.26.254.254? Tell 172.26.33.26
--------------	-------------------	-----------	-----	--

Fig. 8 - Pergunta feita pelo host.

R: O host de origem pergunta a todos os hosts da rede local, qual é o endereço MAC que tem o endereço IP 172.26.254.254, e pede para lhe enviarem a resposta para o endereço IP 172.26.33.26.

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

```
> Frame 16: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{F70627F3-903D-430D-A677-211F0CBC56DE}, id 0
> Ethernet II, Src: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00), Dst: Chongqin_b0:8b:51 (d4:1b:81:b0:8b:51)
  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: Chongqin_b0:8b:51 (d4:1b:81:b0:8b:51)
    Target IP address: 172.26.33.26
```

Fig. 9 - ARP Reply.

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

R: O valor do campo opcode é “reply (2)”, especificando que é a resposta a um pedido ARP.

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

R: A resposta ao pedido ARP está no campo “Sender MAC adress”.

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.

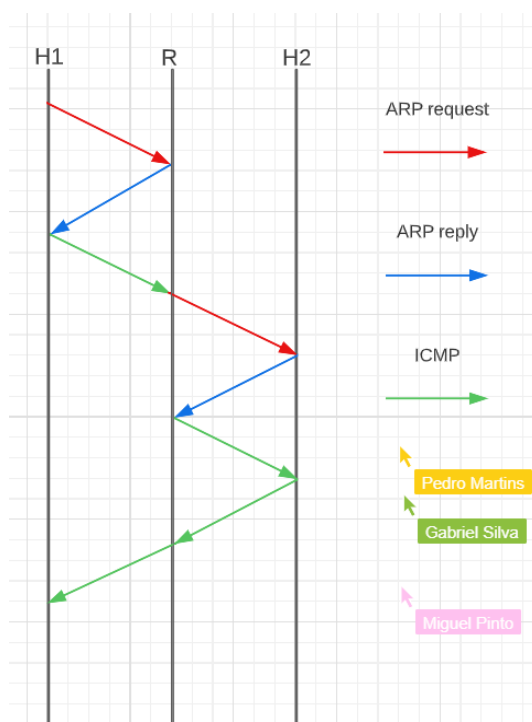


Fig. 10 - Diagrama cronológico de mensagens.

Domínios de colisão

Uma rede local onde existam vários equipamentos ligados através de um meio partilhado comum constitui o que é denominado um domínio de colisão. Esta designação decorre da possibilidade de vários hosts poderem coincidir temporalmente no envio de uma trama, causando uma interferência mútua (colisão) que deteriora as tramas originalmente enviadas. Num domínio de colisão, apenas um dispositivo pode transmitir num determinado instante e os restantes ficam à escuta para prevenir colisões. Por esse facto, a largura de banda é partilhada entre os diversos dispositivos. Na presença de uma colisão, os dispositivos envolvidos têm que retransmitir a mesma trama Ethernet algum tempo depois. As normas Ethernet implementam um método de controlo de acesso ao meio denominado CSMA/CD (estudado nas aulas teóricas), que prevê a resolução de colisões. Os domínios de colisão existem em segmentos de rede com equipamentos interligados via hubs partilhados (repetidores) e também em redes sem fios (Wi-Fi). As redes atuais usam maioritariamente comutadores de rede (switches) para eliminar as colisões. Conectando cada dispositivo a uma porta do comutador, cada porta constitui um domínio de colisão (se a comunicação for half-duplex) ou são eliminados se a comunicação for full-duplex. Ative o emulador CORE e carregue a topologia de rede com a solução de subnetting que construiu no âmbito do TP2. Substitua o switch do departamento A por um hub (repetidor).

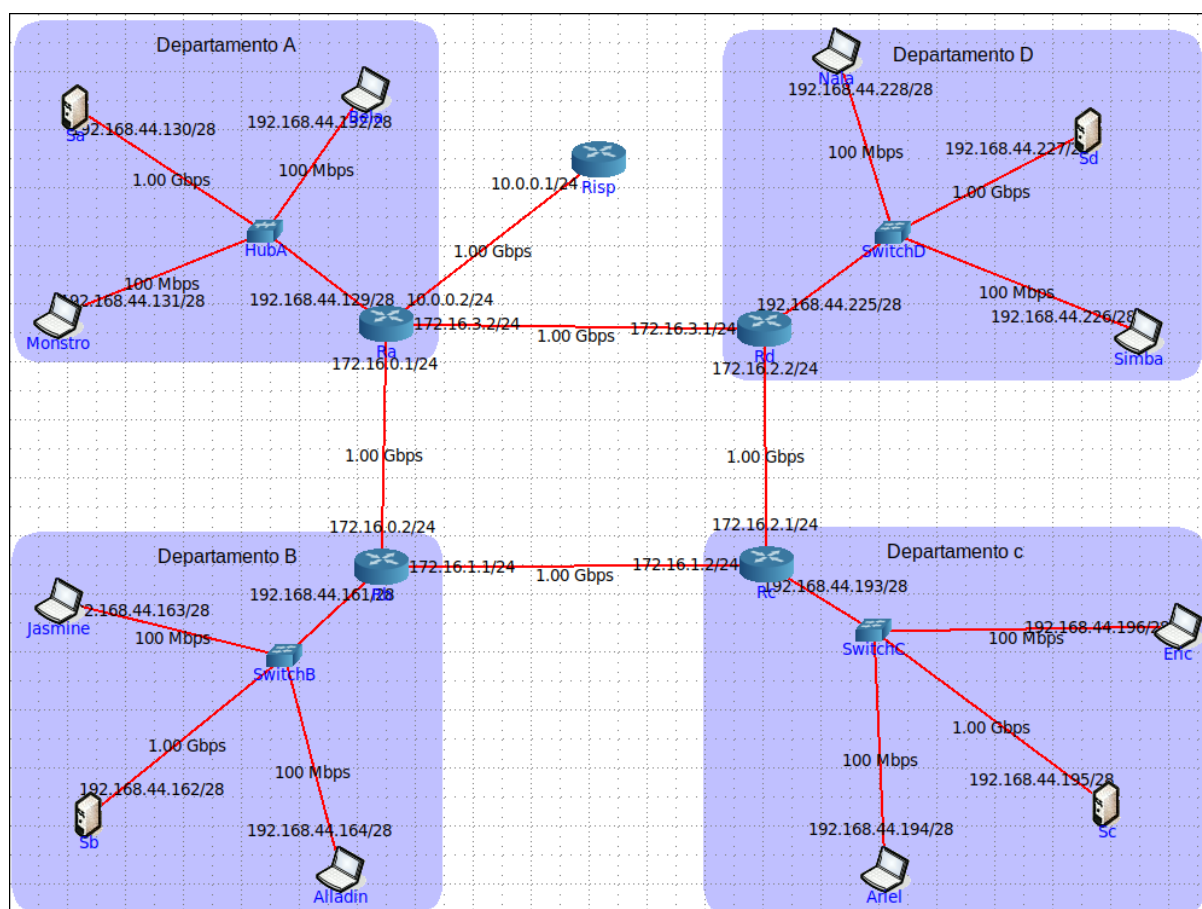


Fig. 11 - Topologia modificada.

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?

The figure displays four terminal windows, each showing the output of a tcpdump command. The windows are arranged in a 2x2 grid. The top-left window shows a tcpdump command on interface eth2, capturing traffic from 192.168.44.161 to 192.168.44.164. The top-right window shows a ping command from Jasmine to 192.168.44.164, with the output showing 5 packets transmitted, 5 received, and 0% packet loss. The bottom-left window shows a tcpdump command on interface eth2, capturing traffic from 192.168.44.129 to 192.168.44.131. The bottom-right window shows a ping command from Bela to 192.168.44.131, with the output showing 5 packets transmitted, 5 received, and 0% packet loss.

```

root@Rb:/tmp/pycore.36841/Rb.conf# tcpdump -i eth2
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth2, link-type EN10MB (Ethernet), capture size 262144 bytes
^C16:40:55.592385 IP 192.168.44.161 > 224.0.0.5: OSPFv2, Hello, length 44
16:40:56.795266 ARP, Request who-has 192.168.44.164 tell 192.168.44.163, length 28
16:40:57.592894 IP 192.168.44.161 > 224.0.0.5: OSPFv2, Hello, length 44
16:40:57.630373 IP6 fe80::200:ff:feaa:e > ff02::5: OSPFv3, Hello, length 36
16:40:58.207780 IP6 fe80::94fe:91ff:fe81:69a9 > ip6-allrouters: ICMP6, router solicitation, length 16
16:40:59.593161 IP 192.168.44.161 > 224.0.0.5: OSPFv2, Hello, length 44
16:41:01.593549 IP 192.168.44.161 > 224.0.0.5: OSPFv2, Hello, length 44
16:41:03.594445 IP 192.168.44.161 > 224.0.0.5: OSPFv2, Hello, length 44

8 packets captured
8 packets received by filter
0 packets dropped by kernel
root@Rb:/tmp/pycore.36841/Rb.conf#

root@Jasmine:/tmp/pycore.36841/Jasmine.conf# ping 192.168.44.164
PING 192.168.44.164 (192.168.44.164) 56(84) bytes of data,
64 bytes from 192.168.44.164: icmp_seq=1 ttl=64 time=1.14 ms
64 bytes from 192.168.44.164: icmp_seq=2 ttl=64 time=0.233 ms
64 bytes from 192.168.44.164: icmp_seq=3 ttl=64 time=0.218 ms
64 bytes from 192.168.44.164: icmp_seq=4 ttl=64 time=0.340 ms
64 bytes from 192.168.44.164: icmp_seq=5 ttl=64 time=0.371 ms
^C
--- 192.168.44.164 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4068ms
rtt min/avg/max/mdev = 0.218/0.460/1.139/0.344 ms
root@Jasmine:/tmp/pycore.36841/Jasmine.conf#

root@Ra:/tmp/pycore.36841/Ra.conf# tcpdump -i eth2
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth2, link-type EN10MB (Ethernet), capture size 262144 bytes
^C16:41:09.596126 IP 192.168.44.129 > 224.0.0.5: OSPFv2, Hello, length 44
16:41:10.760373 IP 192.168.44.132 > 192.168.44.131: ICMP echo request, id 49, seq 1, length 64
16:41:10.760838 IP 192.168.44.131 > 192.168.44.132: ICMP echo reply, id 49, seq 1, length 64
16:41:11.596708 IP 192.168.44.129 > 224.0.0.5: OSPFv2, Hello, length 44
16:41:11.760831 IP 192.168.44.132 > 192.168.44.131: ICMP echo request, id 49, seq 2, length 64
16:41:11.761186 IP 192.168.44.131 > 192.168.44.132: ICMP echo reply, id 49, seq 2, length 64
16:41:12.767978 IP 192.168.44.132 > 192.168.44.131: ICMP echo request, id 49, seq 3, length 64
16:41:12.768269 IP 192.168.44.131 > 192.168.44.132: ICMP echo reply, id 49, seq 3, length 64
16:41:13.597315 IP 192.168.44.129 > 224.0.0.5: OSPFv2, Hello, length 44
16:41:13.791696 IP 192.168.44.132 > 192.168.44.131: ICMP echo request, id 49, seq 4, length 64
16:41:13.792156 IP 192.168.44.131 > 192.168.44.132: ICMP echo reply, id 49, seq 4, length 64
16:41:14.816032 IP 192.168.44.132 > 192.168.44.131: ICMP echo request, id 49, seq 5, length 64
16:41:14.816491 IP 192.168.44.131 > 192.168.44.132: ICMP echo reply, id 49, seq 5, length 64
16:41:15.597695 IP 192.168.44.129 > 224.0.0.5: OSPFv2, Hello, length 44
16:41:15.871638 ARP, Request who-has 192.168.44.132 tell 192.168.44.131, length 28
16:41:15.871658 ARP, Request who-has 192.168.44.131 tell 192.168.44.132, length 28
16:41:15.871839 ARP, Reply 192.168.44.132 is-at 00:00:00:aa:00:02 (oui Ethernet), length 28
16:41:15.871850 ARP, Reply 192.168.44.131 is-at 00:00:00:aa:00:01 (oui Ethernet), length 28
16:41:17.598615 IP 192.168.44.129 > 224.0.0.5: OSPFv2, Hello, length 44
16:41:17.676140 IP6 fe80::200:ff:feaa:3 > ff02::5: OSPFv3, Hello, length 36

20 packets captured
20 packets received by filter
0 packets dropped by kernel
root@Ra:/tmp/pycore.36841/Ra.conf#

root@Bela:/tmp/pycore.36841/Bela.conf# ping 192.168.44.131
PING 192.168.44.131 (192.168.44.131) 56(84) bytes of data,
64 bytes from 192.168.44.131: icmp_seq=1 ttl=64 time=0.900 ms
64 bytes from 192.168.44.131: icmp_seq=2 ttl=64 time=0.593 ms
64 bytes from 192.168.44.131: icmp_seq=3 ttl=64 time=0.476 ms
64 bytes from 192.168.44.131: icmp_seq=4 ttl=64 time=0.603 ms
64 bytes from 192.168.44.131: icmp_seq=5 ttl=64 time=0.717 ms
^C
--- 192.168.44.131 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4056ms
rtt min/avg/max/mdev = 0.476/0.657/0.900/0.143 ms
root@Bela:/tmp/pycore.36841/Bela.conf#

```

Fig. 12 - Testes de fluxo de tráfego.

R: Como podemos ver na figura em cima, no Departamento A (as duas janelas de baixo), sendo uma LAN partilhada devido ao uso de um Hub, quando é feito um “ping” entre a Bela e o Monstro o router Ra captura as tramas enviadas entre os 2 computadores pela interface eth2. Nas outras interfaces isso já não acontece. O Departamento B (as duas janelas de cima), sendo uma LAN comutada devido ao uso de um Switch, quando é feito um “ping” entre a Jasmine e Alladin o router Rb não captura as tramas enviadas entre os 2 computadores por qualquer interface. Com estas observações podemos concluir que o uso de um Hub impede que haja direcionamento de mensagens entre host, visto que qualquer host conectado ao Hub recebe essa informação. Já um Switch permite dirigir uma mensagem a um host de forma encapsulada.

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

MAC adress	Interface	TTL
00:00:00:aa:00:0e	1	60
00:00:00:aa:00:0f	2	60
00:00:00:aa:00:18	3	60
00:00:00:aa:00:19	4	60

Fig. 13 - Tabela de comutação do switch.

The network diagram for Department B shows a central switch (SwitchB) connected to four nodes: Jasmine (PC), Sb (Server), Alladin (PC), and Rb (Router). Each connection is labeled with a number (1-4) and a speed. The configuration windows show the settings for each node's interface eth0.

Router configuration for Rb (Router):

- Node name: Rb
- Type: router
- Interface eth0: MAC address 00:00:00:aa:00:01, IPv4 address 172.16.0.2/24, IPv6 address
- Interface eth1: MAC address 00:00:00:aa:00:02, IPv4 address 172.16.1.1/24, IPv6 address
- Interface eth2: MAC address 00:00:00:aa:00:0e, IPv4 address 192.168.44.161/28, IPv6 address

Router configuration for Jasmine (PC):

- Node name: Jasmine
- Type: PC
- Interface eth0: MAC address 00:00:00:aa:00:18, IPv4 address 192.168.44.163/28, IPv6 address 2001:2::20/64

Router configuration for Alladin (PC):

- Node name: Alladin
- Type: PC
- Interface eth0: MAC address 00:00:00:aa:00:19, IPv4 address 192.168.44.164/28, IPv6 address 2001:2::21/64

Router configuration for Sb (Server):

- Node name: Sb
- Type: host
- Interface eth0: MAC address 00:00:00:aa:00:0f, IPv4 address 192.168.44.162/28, IPv6 address

Fig. 14 - Mac addresses e interfaces do switch.

Conclusão

Com este trabalho prático conseguimos aplicar os conhecimentos obtidos nas aulas teóricas em situações mais práticas e perceber melhor conceitos relativos à camada de ligação lógica. A utilização de programas como o WireShark também nos permitiu ter uma melhor aproximação à realidade de conceitos como a tecnologia Ethernet, protocolo ARP, endereços MAC e como tudo isto se relaciona e funciona na prática. Em suma, este trabalho permitiu-nos visualizar todos os conceitos teóricos de uma maneira interativa com a utilização das diversas ferramentas que nos permitiram ver o funcionamento da camada de ligação lógica.