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 aplicacionais 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 aplicacionais 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

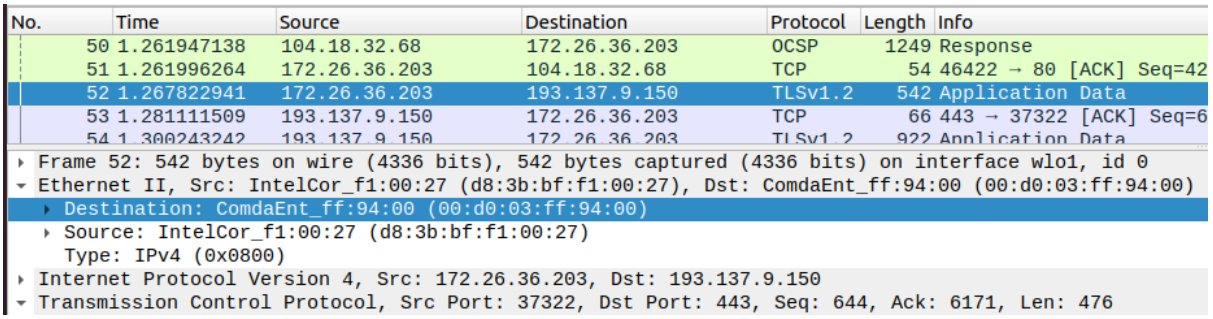

Fig. 1 - Endereços MAC de origem e destino.

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”.

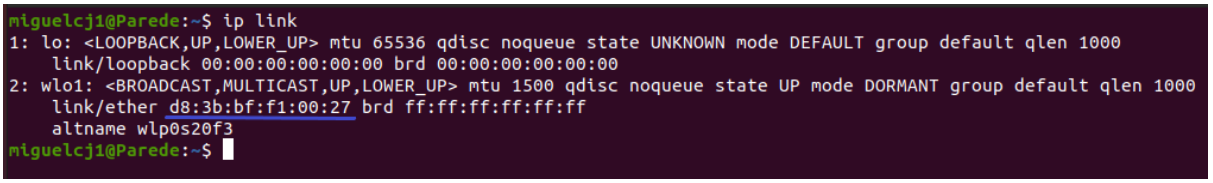

Fig. 2 - Endereço MAC do nosso computador.

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

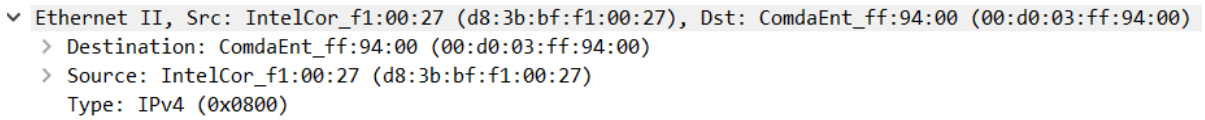

Fig. 3 - Campo Type da trama Ethernet.

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.

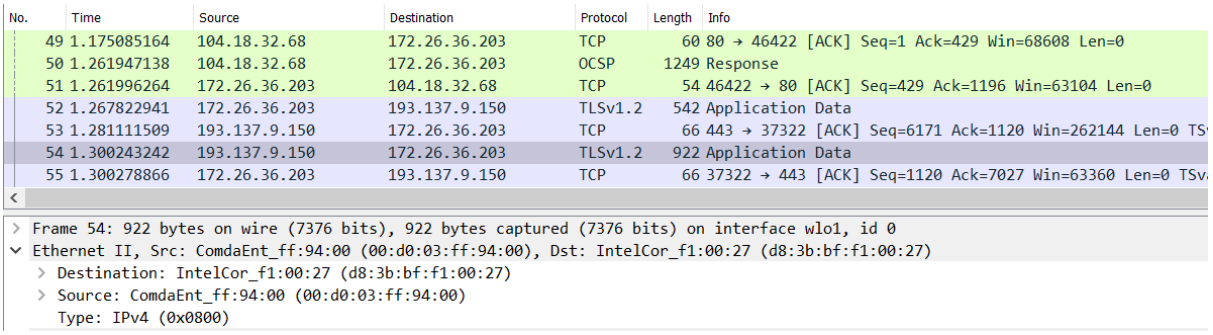

Fig. 4 - Trama que contém o primeiro byte da resposta HTTP.

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
v Ethernet II, Src: Chongqin_b0:8b:51 (d4:1b:81:b0:8b:51), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  v 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)
  v 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)
v 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?

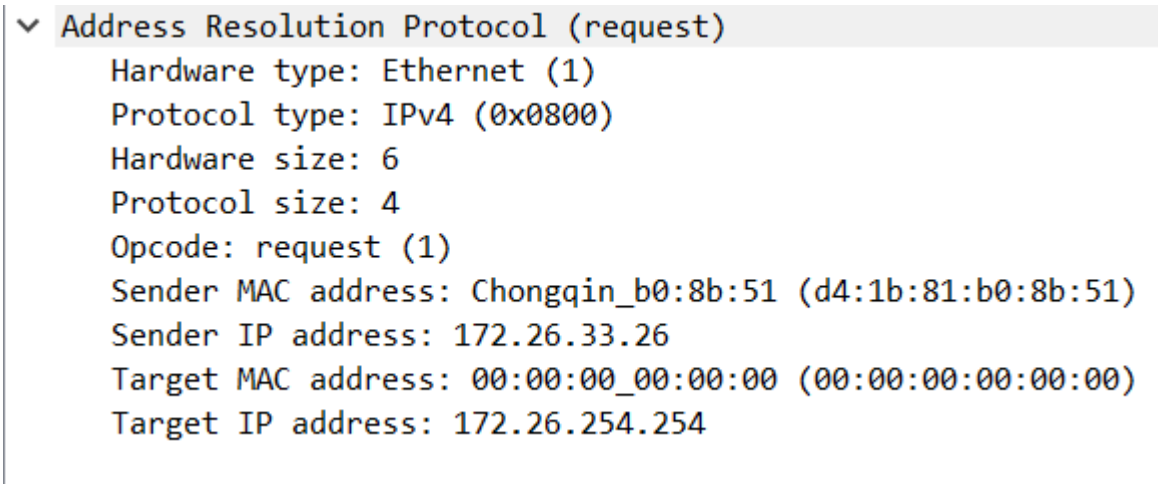

Fig. 7 - Address Resolution Protocol.

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 Adress 00:00:00:00:00:00 (endereço de broadcast).

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

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)
v 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.

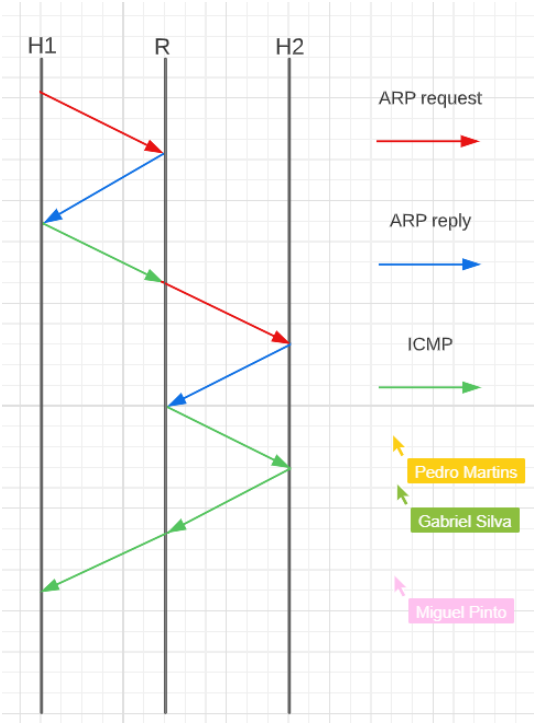

Fig. 10 - Diagrama cronológico de mensagens.

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).

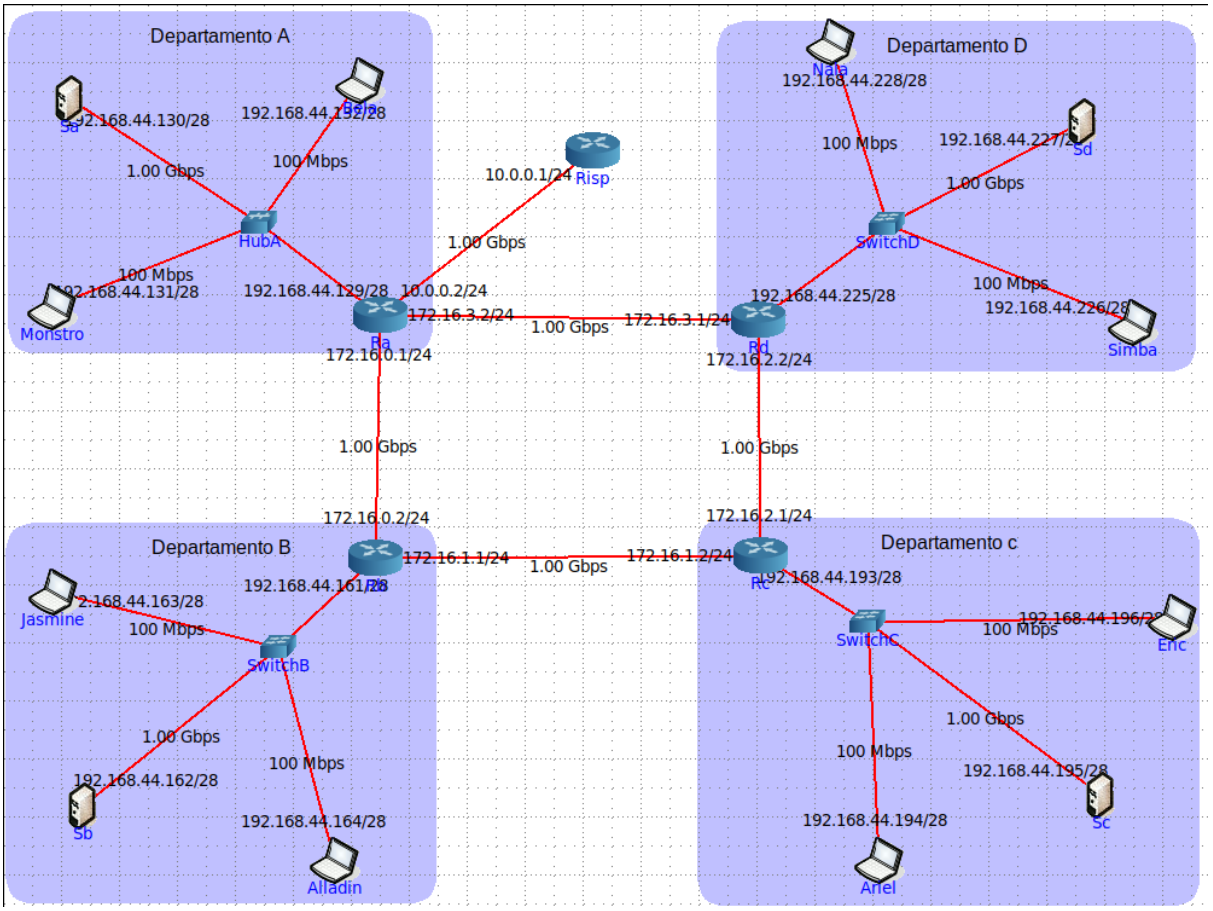

Fig. 11 - Topologia modificada.

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?

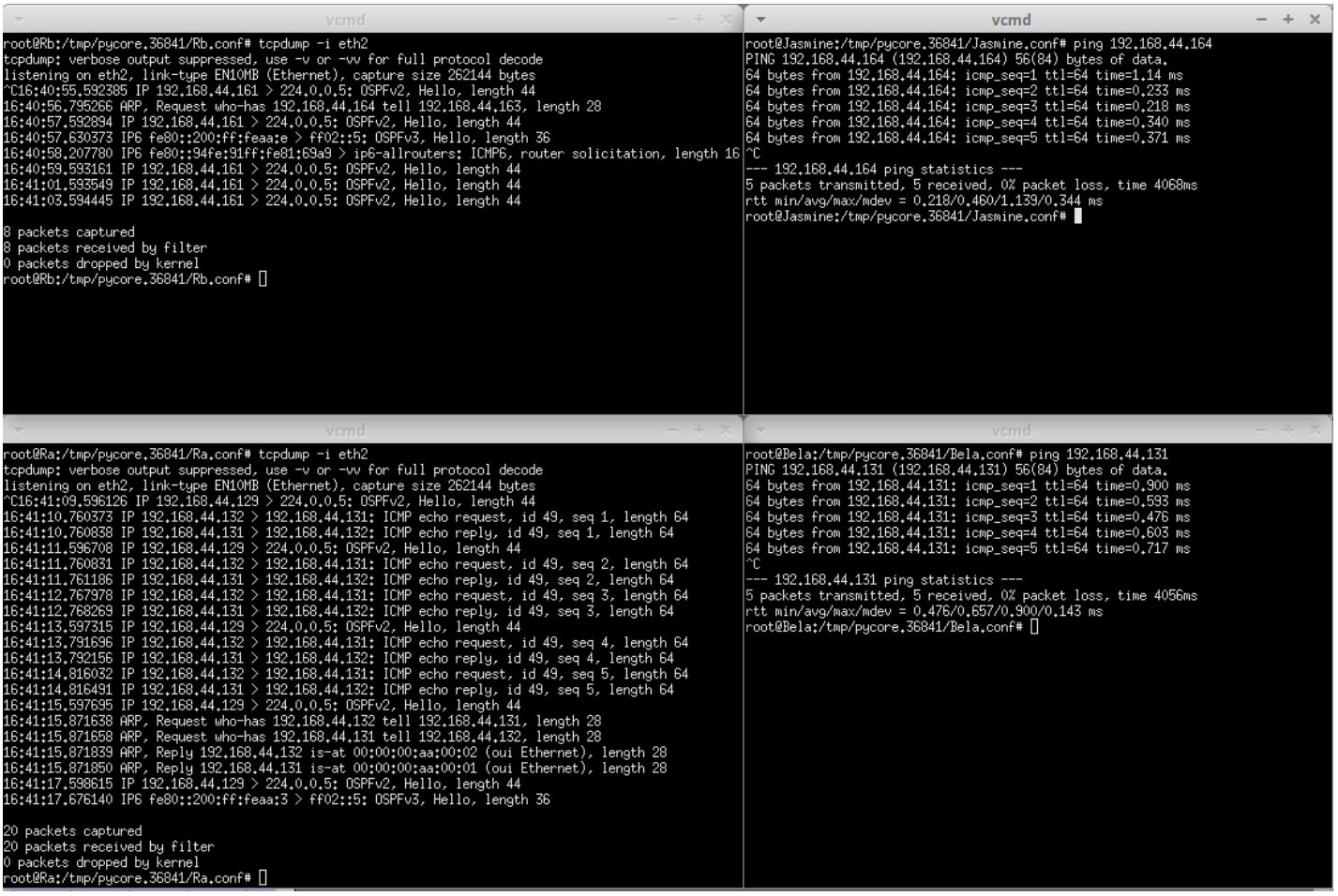

Fig. 12 - Testes de fluxo de tráfego.

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.

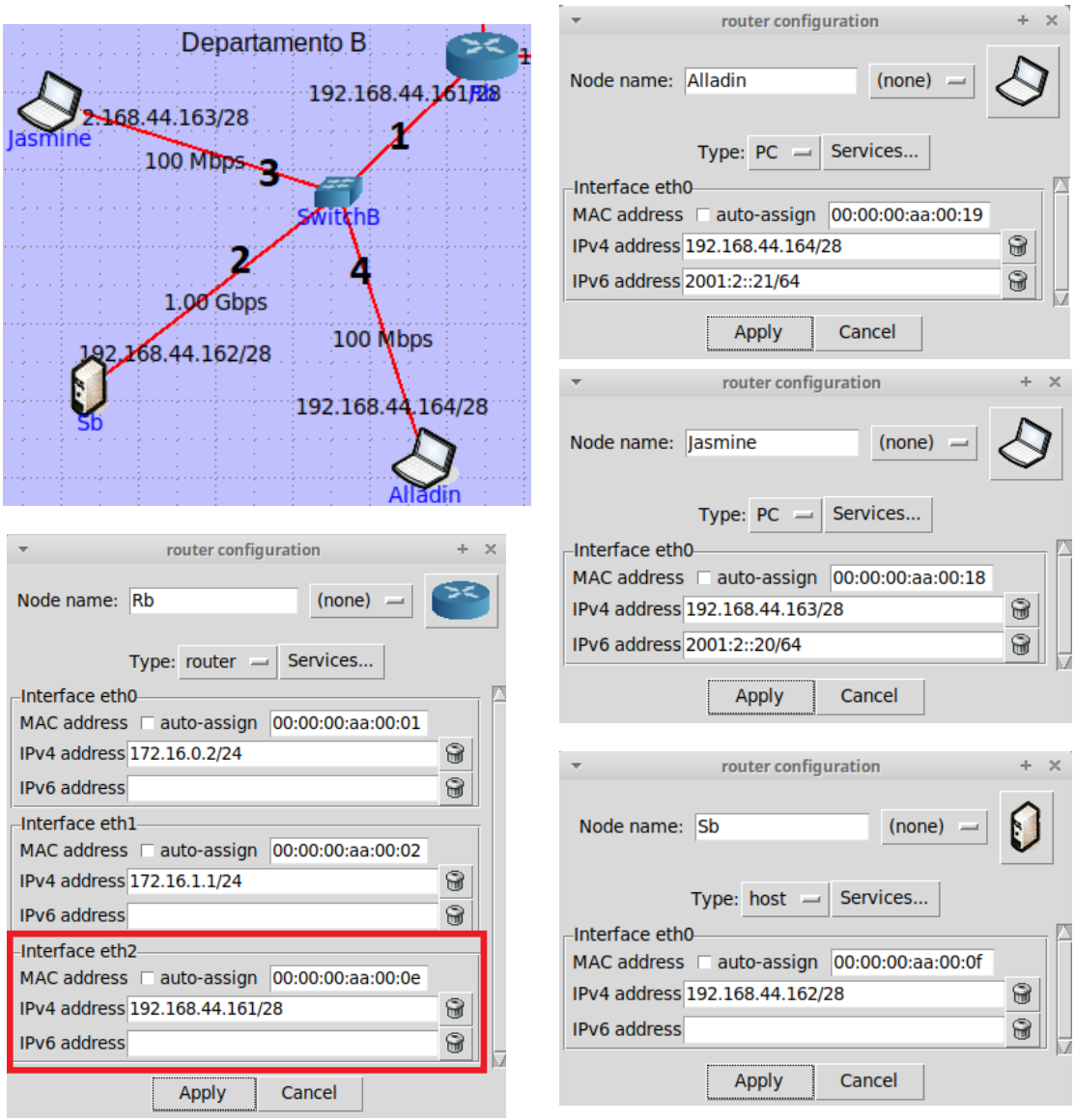

Fig. 14 - Mac addresses e interfaces do switch.

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.