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

Tiago Alves a80872, Francisco Costa a95227, Cláudio Bessa a97063

28 de abril de 2022

1 Secção Questão-Resposta

1.1 Captura e análise de Tramas Ethernet

Na realização da captura de Tramas, ao contrário ao solicitado no enunciado, indo de acordo ao que a docente sugeriu, utilizamos um *website* com *http* puro, logo não encriptado. O *site* utilizado foi o seguinte: http://info.cern.ch/.

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

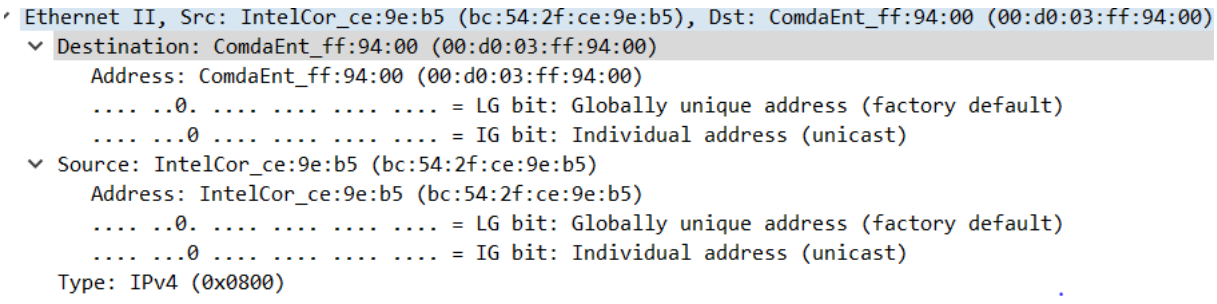

Figura 1: Endereços MAC de origem e de destino

1.1.2 Identifique a que sistemas se referem. Justifique.

R: Os campos de origem e destino representam a nossa máquina e o respetivo *website* de *http* puro. Conseguimos verificar isso através da verificação no *Wireshark* pelas colunas *Source* e *Destination* que contêm os IP's dos respetivos sistemas.

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

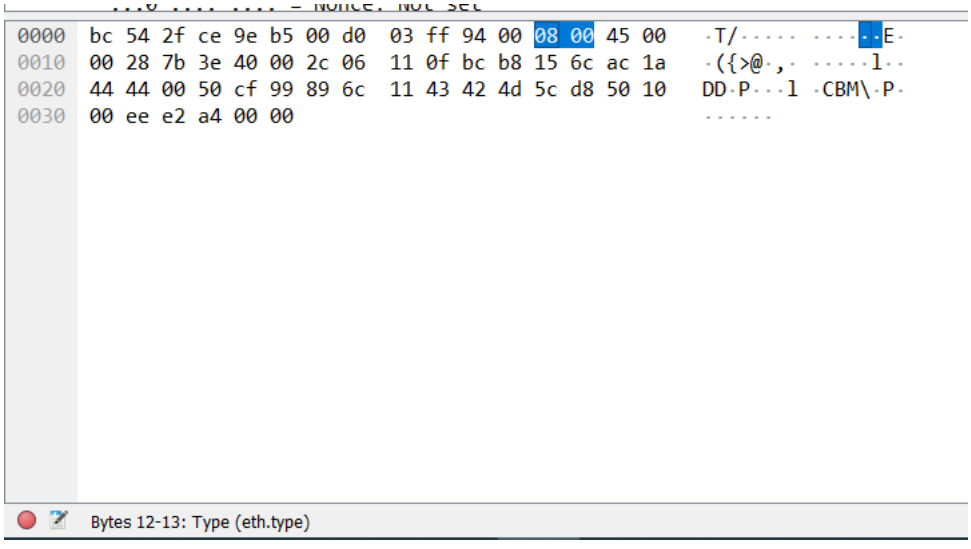

Figura 2: Campo *type* da trama *ethernet*

R: O valor obtido no campo *type* serve para indicar o tipo de encapsulamento protocular do campo de dados. Admitindo assim diferentes tipos de encapsulamento. Desses tipos podemos ver componentes comuns como o protocolo IPv4 e ARP.

1.1.4 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.

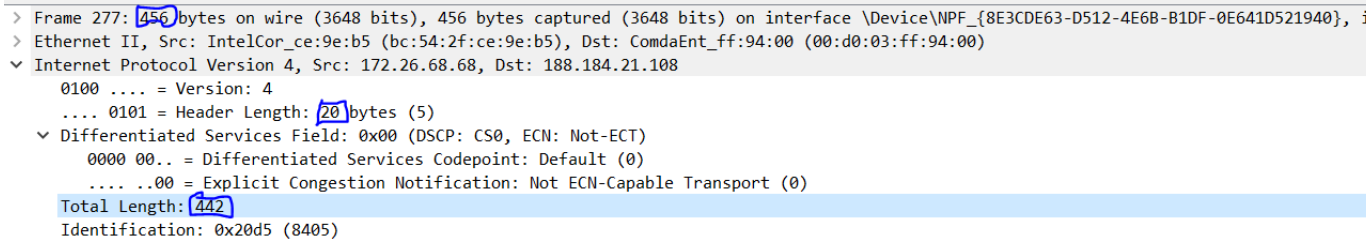

Figura 3: Encapsulamento protocular

R: São utilizados 456 bytes desde o início da trama até ao início dos dados, tendo o *overhead* 11.84%.

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

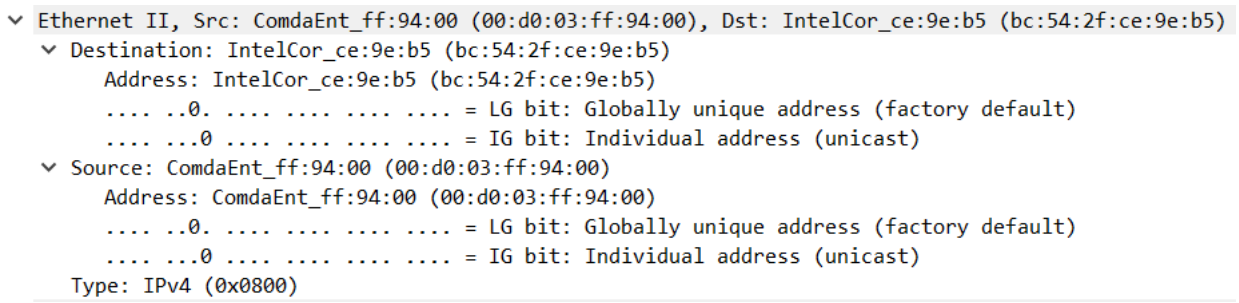

Figura 4: Endereço *ethernet* da fonte

R: Agora, inversamente ao que se tinha passado anteriormente, o *source* será o *http* e o *destination* a nossa máquina, conseguindo identifical de igual forma no *Wireshark* pelos respetivos IP's.

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

R: O endereço MAC do destino, tal como verificado na figura 4 é 00:d0:03:ff:94:00. Sendo ele correspondente ao MAC associado à nossa máquina.

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

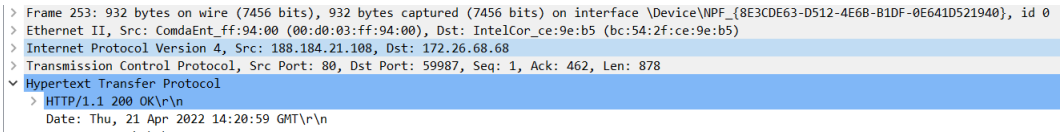

Figura 5: Desancapsulamento protocular

R: $HTTP \subset TCP \subset IP \subset Ethernet$

1.2 Protocolo ARP

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

```
C:\Users\MSI>arp -a

Interface: 172.26.9.57 --- 0x3
  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
  239.192.152.143       01-00-5e-40-98-8f     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.56.1 --- 0xc
  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
  239.192.152.143       01-00-5e-40-98-8f     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Figura 6: Tabela ARP

R: A primeira coluna demonstra o IP, a segunda coluna demonstra o MAC *address* e a terceira coluna demonstra as ligações entre MAC e IP, se for dinamica, essa ligação é guardada enquanto for usada e alterada caso seja necessario, se for estática a ligação é automaticamente criada pelo computador.

1.2.2 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?

```
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: IntelCor_40:fe:3e (28:11:a8:40:fe:3e)
    Sender IP address: 172.26.9.57
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 172.26.254.254
```

Figura 7: ARP Request

R:

MAC origem 28:11:a8:40:fe:3e

MAC destino ff:ff:ff:ff:ff

Quando a origem não tem nenhuma informação na tabela ARP do seu próximo salto, o protocolo ARP envia uma mensagem para este endereço (ff:ff:ff:ff:ff) procurando o MAC pretendido.

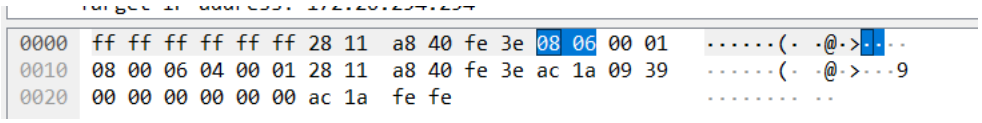

Figura 8: Campo *type* da trama

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

R: O valor do campo *type* da trama *Ethernet* é 0806 e indica-nos o protocolo utilizado, neste caso protocolo ARP.

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

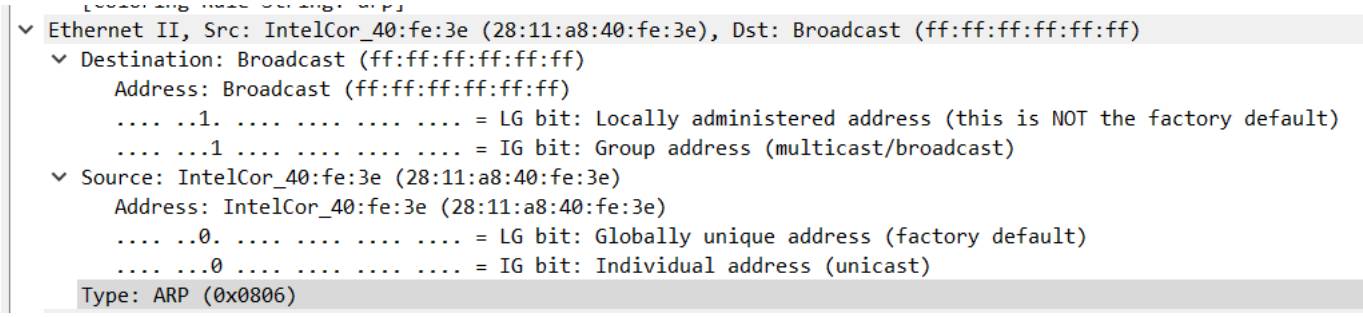

Figura 9: Endereços contido no ARP

R: Realmente trata-se de um pedido ARP, devido ao nível *Ethernet* possuir o protocolo $0x0806$, onde, pelas verificações efetuadas anteriormente, são informações previas sobre o destino que estamos a tentar aceder.

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

Figura 10: Host origem

R: O *host* de origem, manda um *broadcast* a todas as máquinas no seu departamento, efetua um *search* do IP, neste caso 193.136.9.254, após envio dos "pacotes", receberá a informaçao da pretendida *interface*, assim criando uma *cache* ARP.

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

a)

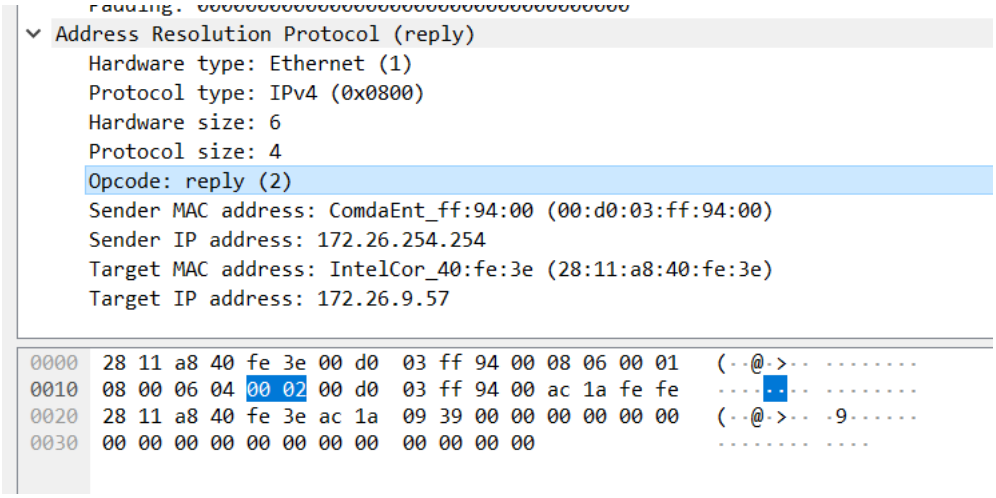

Figura 11: Resposta ao pedido ARP

R: O valor do *opcode* é 2, pois trata-se da resposta, o pedido ARP tem *opcode* 1.

b)

1.2.7 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.

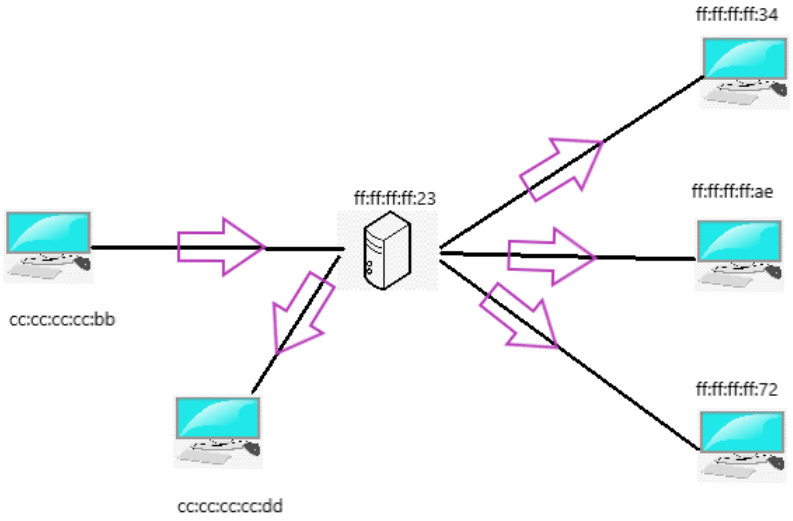

Figura 12: Diagrama de mensagens enviadas

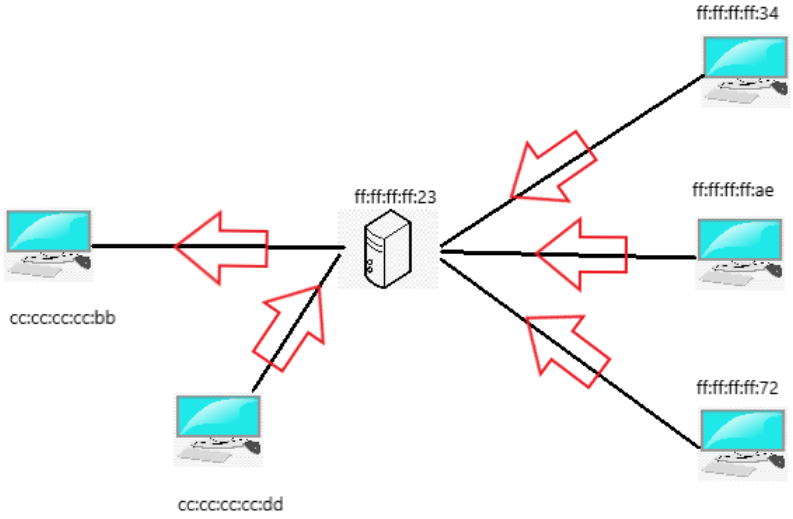

Figura 13: Diagrama de mensagens recebidas

R: O nosso host inicial cc:cc:cc:cc:bb não tem uma ligação para ff:ff:ff:ff:ae guardada em ARP, portanto o nosso *host* enviará um *ping* para todos os *hosts* presentes na rede. O *ping* pedirá ao *host* de IP ff:ff:ff:ff:ff, como já previamente citado, o ARP não tem ligações previamente criadas nesta rede.

Após o ICMP confirmar que os *pings* chegaram aos respetivos *hosts*, os mesmos enviarão para o sistema gerador de mensagens inicial os seus IPs, assim o ARP conseguirá criar uma ligação ao *host* ff:ff:ff:ff:ae, e também ligará à ff:ff:ff:ff:23.

1.3 Domínios de colisão

1.3.1 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?

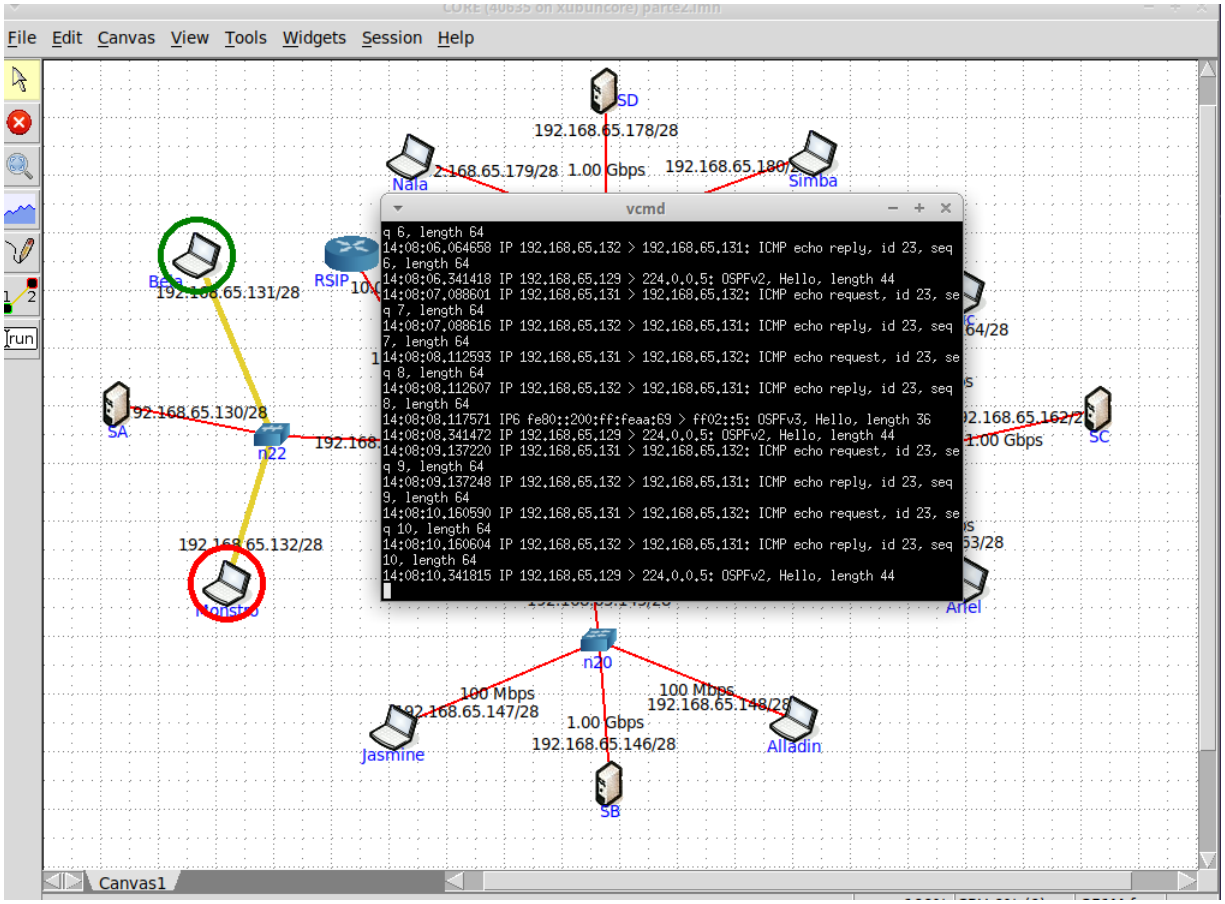

Figura 14: Departamento A com *hub*

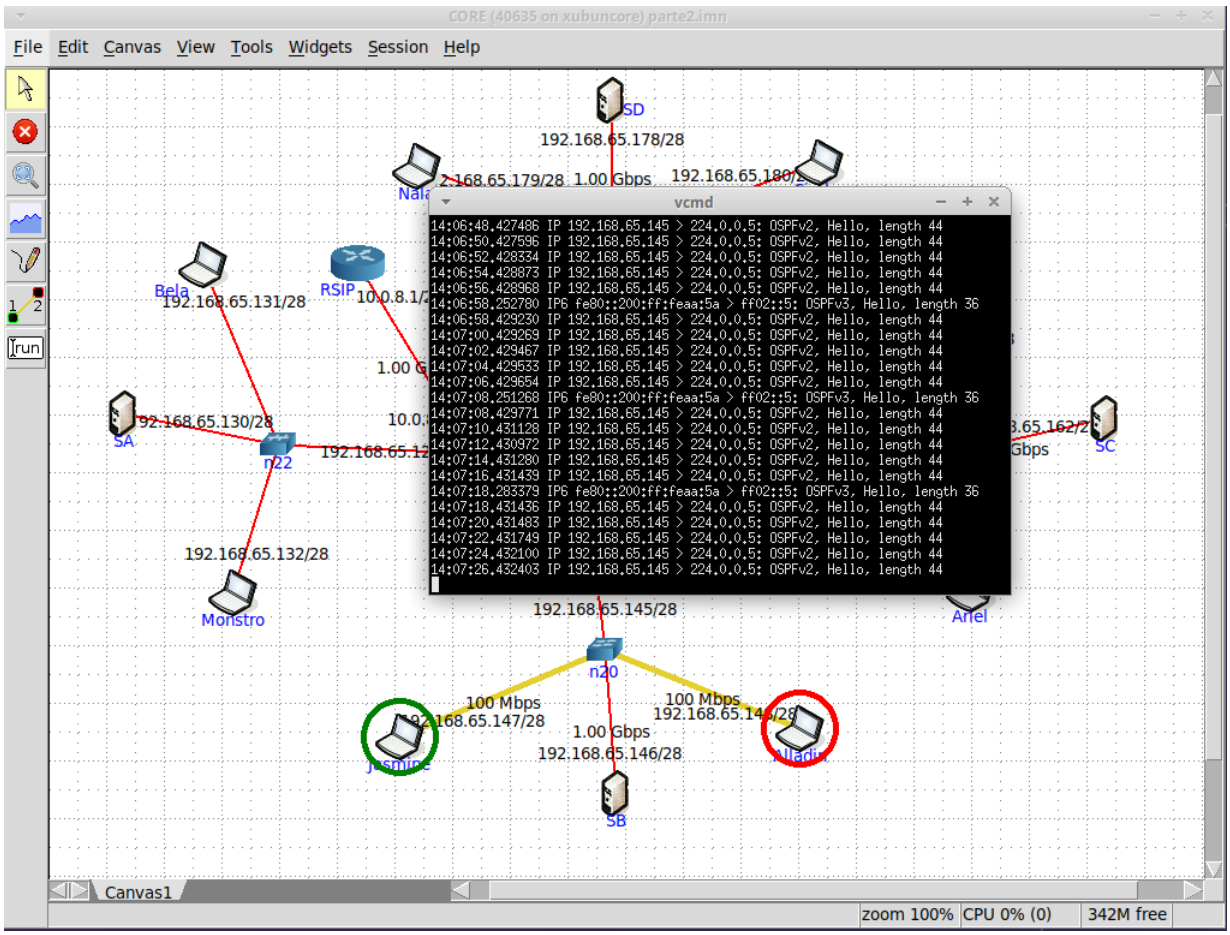

Figura 15: Departamento B com *switch*

R: Como podemos verificar pelas figuras acima representadas verificamos uma diferença de comportamentos entre os departamentos que utilizam *switch* ou *hub*. Na utilização de *switch* a rede é comutada, logo não é possível capturar qualquer tipo de tramas no tráfego entre Jasmine e Aladin. Já na rede partilha é possível verificar as tramas.

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

Name	Port	MAC address
RB	0	00:00:00:aa:00:87
Jasmine	1	00:00:00:aa:00:91
Alladin	2	00:00:00:aa:00:92
SB	3	00:00:00:aa:00:84

Figura 16: Tabela de comutação

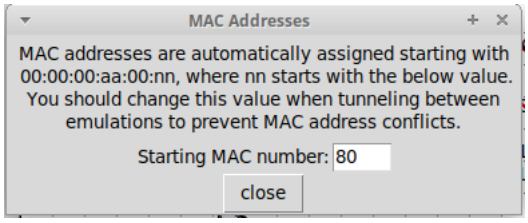

Figura 17: MAC *addresses*

2 Conclusão

R: Sumamente, consideramos que a utilização do *Wireshark* foi deveras mais fácil uma vez já não ser uma estreia no mesmo como no trabalho prático anterior. Uma vez que *switches* também de igual forma já tinham sido estudados de uma forma mais geral, não encontramos grandes surpresas. Continuamos a afirmar algumas dificuldades na relação e interpretação da parte mais teórica relativamente à prática.

Contudo, conseguimos obter um conhecimento e reconhecemos um entendimento relativo às redes *ethernet* e protocolo ARP.