2020

Universidade do Minho
Escola de Engenharia

REDES DE COMPUTADORES

TRABALHO PRÁTICO 3 - ETHERNET E PROTOCOLO ARP

GRUPO 63

A89533 - Ana Carneiro

A89517 - Diogo Araújo

A89518 – Ema Dias

ÍNDICE

CAPTURA E ANÁLISE DE TRAMAS ETHERNET 2

1. Anote os endereços MAC de origem e de destino da trama capturada. 2
2. Identifique a que sistemas se referem. Justifique 2
3. Qual o valor hexadecimal do campo Type da trama Ethernet? O que significa? 2
4. Quantos bytes são usados desde o início da trama até ao caractere ASCII "G" do método HTTP GET? Calcule e indique, em percentagem, a sobrecarga (overhead) introduzida pela pilha protocolar no envio do HTTP GET. 3
5. Através de visualização direta ou construindo um filtro específico, verifique se foram detetadas tramas com erros (por verificação do campo FCS (Frame Check Sequence)). 3
6. Qual é o endereço Ethernet da fonte? A que sistema de rede corresponde? Justifique. 4
7. Qual é o endereço MAC do destino? A que sistema corresponde? 4
8. Atendendo ao conceito de desencapsulamento protocolar, identifique os vários protocolos contidos na trama recebida. 4

PROTOCOLO ARP 5

9. Observe o conteúdo da tabela ARP. Diga o que significa cada uma das colunas. 5
10. 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? 6
11. Qual o valor hexadecimal do campo tipo da trama Ethernet? O que indica? 6
12. Como pode confirmar que se trata efetivamente de um pedido ARP? Identifique que tipo de endereços estão contidos na mensagem ARP? Que conclui? 6
13. Explicite que tipo de pedido ou pergunta é feita pelo host de origem? 7
14. Localize a mensagem ARP que é a resposta ao pedido ARP efetuado. 7
    a. Qual o valor do campo ARP opcode? O que especifica? 7
    b. Em que posição da mensagem ARP está a resposta ao pedido ARP? 7

ARP GRATUITO 8

15. Identifique um pacote de pedido ARP gratuito originado pelo seu sistema. Analise o conteúdo de um pedido ARP gratuito e identifique em que se distingue dos restantes pedidos ARP. Registe a trama Ethernet correspondente. Qual o resultado esperado face ao pedido ARP gratuito enviado? 8

DOMÍNIOS DE COLISÃO 9

16. Através da opção tcpdump verifique e compare como flui o tráfego nas diversas interfaces dos vários dispositivos no departamento A (LAN comutada) e no departamento B (LAN partilhada) quando gera tráfego intra-departamento (por exemplo, através do comando ping). Que conclui? 9
    a. Comente os resultados obtidos quanto à utilização de hubs e switches no contexto de controlar ou dividir domínios de colisão. Documente as suas observações e conclusões com base no tráfego observado/capturado 10

CONCLUSÃO 11

CAPTURA E ANÁLISE DE TRAMAS ETHERNET

MENSAGEM HTTP GET

No.	Time	Source	Destination	Protocol	Length	Info
8799	458.338608	172.26.84.152	13.107.4.52	TCP	54	60905 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
8800	458.338825	172.26.84.152	13.107.4.52	HTTP	208	GET /connecttest.txt HTTP/1.1
8801	458.380568	13.107.4.52	172.26.84.152	TCP	60	80 → 60905 [ACK] Seq=1 Ack=155 Win=524800 Len=0
8802	458.380568	13.107.4.52	172.26.84.152	HTTP	568	HTTP/1.1 200 OK (text/plain)
8803	458.380568	13.107.4.52	172.26.84.152	TCP	60	80 → 60905 [FIN, ACK] Seq=515 Ack=155 Win=524800 Len=0
8804	458.380692	172.26.84.152	13.107.4.52	TCP	54	60905 → 80 [ACK] Seq=155 Ack=516 Win=65024 Len=0
8805	458.380810	172.26.84.152	13.107.4.52	TCP	54	60905 → 80 [FIN, ACK] Seq=155 Ack=516 Win=65024 Len=0

Figura 1: Mensagem HTTP GET

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

```
> Frame 8800: 208 bytes on wire (1664 bits), 208 bytes captured (1664 bits) on interface \Device\NPF_{6DFD5661-FCCC-46FD-B3DE-5617A86C3699}, id 0
v Ethernet II, Src: AzureWav_67:36:93 (80:91:33:67:36:93), Dst: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
  v Destination: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
      Address: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: AzureWav_67:36:93 (80:91:33:67:36:93)
      Address: AzureWav_67:36:93 (80:91:33:67:36:93)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 172.26.84.152, Dst: 13.107.4.52
> Transmission Control Protocol, Src Port: 60905, Dst Port: 80, Seq: 1, Ack: 1, Len: 154
> Hypertext Transfer Protocol
```

Figura 2: Informação sobre a mensagem HTTP GET da figura 1

O endereço MAC da fonte, tal como está na figura 2, é dado por 80:91:33:67:36:93. O endereço MAC do destino é 00:d0:03:ff:94:00.

2. Identifique a que sistemas se referem. Justifique

O endereço da *source* corresponde á nossa máquina e o do *destination* refere-se á interface do router da rede local.

Como foi a nossa máquina a enviar a mensagem para o servidor WEB, então significa que a interface da nossa máquina será a origem da trama. Como a nossa máquina não reconhece endereços fora da rede local então este pedido (HTTP GET) é enviado para um router de acesso (endereço de destino) que, posteriormente, enviará a trama para o servidor WEB e obter a página WEB esperada.

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

O valor hexadecimal é dado por 0x0800 que representa o protocolo IPv4.

4. Quantos bytes são usados desde o início da trama até ao caractere ASCII "G" do método HTTP GET? Calcule e indique, em percentagem, a sobrecarga (overhead) introduzida pela pilha protocolar no envio do HTTP GET.

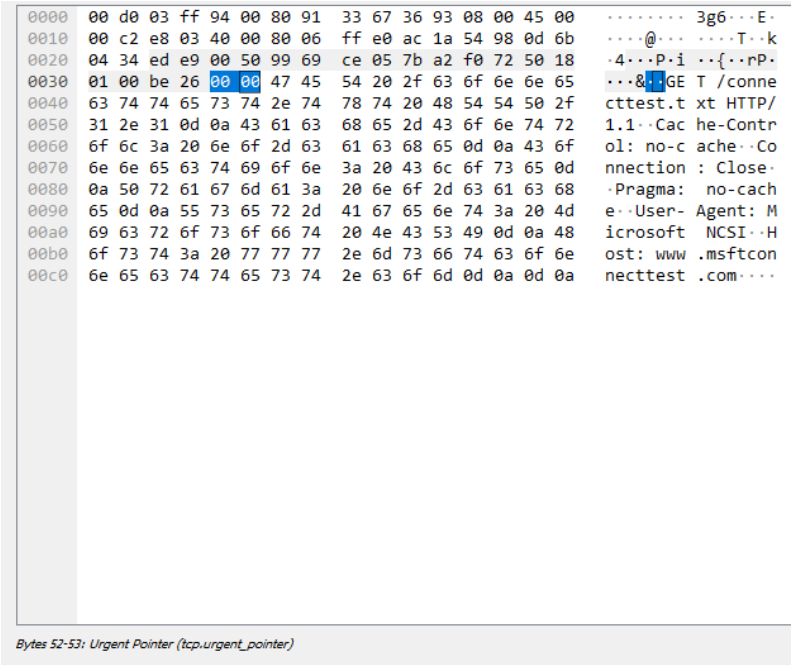

Figura 3: Informação sobre o conteúdo da trama do método HTTP GET

Até ao caracter 'G' são usados 54 bytes. Sabendo que a trama tem 208 bytes (pois o primeiro byte conta como 0) então a percentagem de overhead introduzida pela pilha protocolar é dada por: $\frac{54}{208} * 100 \approx 26\%$

5. Através de visualização direta ou construindo um filtro específico, verifique se foram detetadas tramas com erros (por verificação do campo FCS (Frame Check Sequence)).

Não foram verificadas tramas com erros na captura de tráfego feita.

RESPOSTA HTTP

No.	Time	Source	Destination	Protocol	Length	Info
8799	458.338608	172.26.84.152	13.107.4.52	TCP	54	60905 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
8800	458.338825	172.26.84.152	13.107.4.52	HTTP	208	GET /connecttest.txt HTTP/1.1
8801	458.380568	13.107.4.52	172.26.84.152	TCP	60	80 → 60905 [ACK] Seq=1 Ack=155 Win=524800 Len=0
8802	458.380568	13.107.4.52	172.26.84.152	HTTP	568	HTTP/1.1 200 OK (text/plain)
8803	458.380568	13.107.4.52	172.26.84.152	TCP	60	80 → 60905 [FIN, ACK] Seq=515 Ack=155 Win=524800 Len=0
8804	458.380692	172.26.84.152	13.107.4.52	TCP	54	60905 → 80 [ACK] Seq=155 Ack=516 Win=65024 Len=0

Figura 4: Mensagem HTTP OK

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

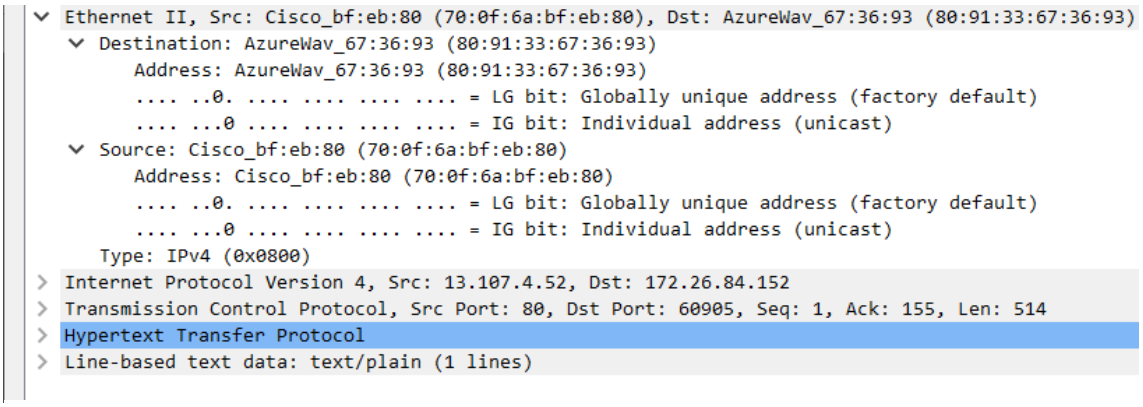

Figura 5: Informação sobre a mensagem de resposta HTTP

O endereço da fonte 70:0f:6a:bf:eb:80, corresponde ao endereço MAC do router da rede local, pois, só conseguimos ter acesso aos endereços dos dispositivos ligados à rede local.

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

O endereço de destino 80:91:33:67:36:93 corresponde ao endereço MAC da interface da nossa máquina.

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

Através da figura 5 conseguimos identificar os diferentes protocolos, isto é, IPv4, TCP e Ethernet

PROTOCOLO ARP

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

```
C:\WINDOWS\system32> arp -a

Interface: 172.26.104.62 --- 0x7
  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

Interface: 192.168.56.1 --- 0x11
  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
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Figura 6: Conteúdo da cache ARP

A primeira coluna representa o endereço IP do *host*, a segunda representa o endereço MAC e a última coluna representa o tipo de endereçamento, que poderá ser estático ou dinâmico. Antes de iniciar a captura no Wireshark será necessário apagar o conteúdo da cache ARP (caso contrário seria provável que a associação entre endereços IP e MAC já existisse na cache):

```
C:\WINDOWS\system32>arp -d *

C:\WINDOWS\system32> arp -a

Interface: 172.26.104.62 --- 0x7
  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

Interface: 192.168.56.1 --- 0x11
  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
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Figura 7: Apagar conteúdo cache ARP

10. 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?

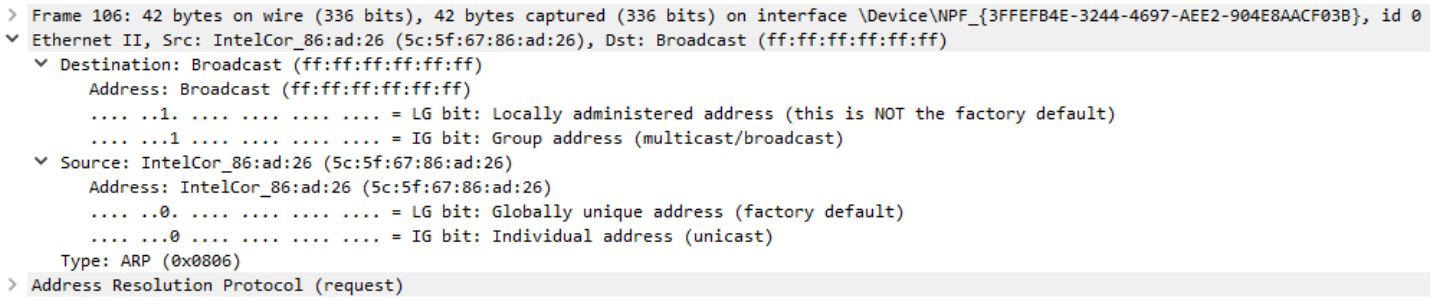

Figura 8: Captura Wireshark (ARP Request)

O endereço MAC de origem é dado por 5c:5f:67:86:ad:26 e o endereço MAC de destino é dado por ff:ff:ff:ff:ff:ff.

O endereço MAC destino é o endereço de Broadcast, com os bits todos iguais a 1. É usado este endereço para que todos os *hosts* da rede local possam receber a trama Ethernet. Para cada *host* que recebe a trama, há verificação se os endereços IP da trama e do *host* coincidem. Caso não coincidam, o *host* descarta a trama Ethernet e caso contrário, processa-a. Tal acontece, pois, o *host* com endereço MAC 5c:5f:67:86:ad:26 não conhece o endereço MAC do destino, pelo que terá de enviar o pedido ARP a todos os *hosts* da rede local.

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

O valor hexadecimal é Ox0806. Encapsula uma *frame* ARP.

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

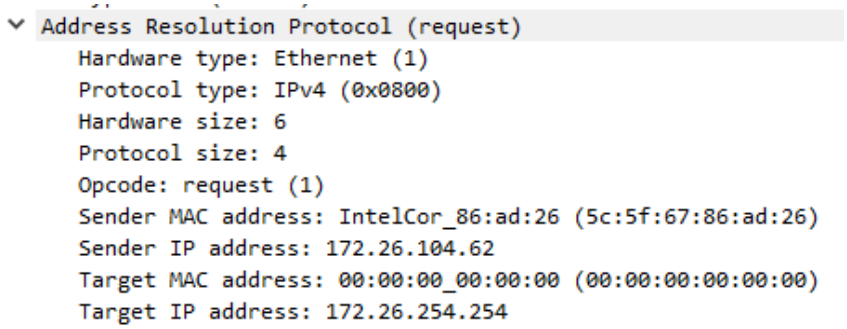

Figura 9: Address Resolution Protocol (request)

Trata-se de um pedido ARP, pois o campo *opcode* tem valor '*request* (1)'. O tipo de endereços que a mensagem ARP contém são endereços MAC e endereços IP. Os endereços MAC presentes na mensagem são:

- *Sender MAC Address*: 5c:5f:67:86:ad:26;
- *Target MAC Address*: 00:00:00:00:00:00;

Os endereços IP presentes na mensagem ARP são:

- *Sender IP Address*: 172.26.104.62;
- *Target IP Address*: 172.26.254.254;

Como o host Sender quer conhecer o endereço MAC do host com o IP 172.26.254.254, então este envia um pedido ARP para todos os hosts através do endereço de broadcast (neste caso o endereço Target MAC é 00:00:00:00:00:00).

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

```
106 3.353625    IntelCor_86:ad:26   Broadcast           ARP         42 Who has 172.26.254.254? Tell 172.26.104.62
```

Figura 10: Pergunta feita pelo host de origem

O *Host* de origem com o IP 172.26.104.62 pergunta qual é o endereço MAC do *Host* com IP 172.26.254.254 (figura 10). Este pedido pode ser traduzido da seguinte forma: O *Host* que tiver o endereço IP 172.26.254.254, deverá devolver o seu endereço MAC para o *Host* com IP 172.26.104.62. Esta mensagem é enviada a todos os *Hosts* da rede local.

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

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

```
> Frame 110: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{3FFEFB4E-3244-4697-AEE2-904E8AACF03B}, id 0
> Ethernet II, Src: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00), Dst: IntelCor_86:ad:26 (5c:5f:67:86:ad:26)
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: IntelCor_86:ad:26 (5c:5f:67:86:ad:26)
    Target IP address: 172.26.104.62
```

Figura 11: Mensagem ARP Reply

O valor do campo *opcode* é '*reply* (2)'. Especifica que é a resposta a um pedido ARP anterior.

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

A reposta ao pedido ARP será o endereço MAC do *Host* com IP 172.26.254.254. A resposta está no campo *Sender MAC Address* que, neste caso, é 00:d0:03:ff:94:00. Neste

momento, o *Host* com endereço MAC 5c:5f:67:86:ad:26 conhece o endereço MAC do *Host* com IP 172.26.254.254.

ARP GRATUITO

395	15.974980	IntelCor_b3:36:02	Broadcast	ARP	42 Who has 172.26.55.252? (ARP Probe)
468	16.972818	IntelCor_b3:36:02	Broadcast	ARP	42 Who has 172.26.55.252? (ARP Probe)
636	17.974909	IntelCor_b3:36:02	Broadcast	ARP	42 Who has 172.26.55.252? (ARP Probe)
960	18.971562	IntelCor_b3:36:02	Broadcast	ARP	42 ARP Announcement for 172.26.55.252

Figura 12: ARP Gratuito

15. Identifique um pacote de pedido ARP gratuito originado pelo seu sistema. Analise o conteúdo de um pedido ARP gratuito e identifique em que se distingue dos restantes pedidos ARP. Registe a trama Ethernet correspondente. Qual o resultado esperado face ao pedido ARP gratuito enviado?

Na figura 6 podemos ver um pacote de ARP Gratuito (ARP *Announcement* segundo a terminologia do wireshark). O que distingue este pacote dos pacotes ARP restantes é a presença de uma *flag* que identifica o pacote ARP como gratuito, tal como esta descrito a azul na figura 7.

```
Address Resolution Protocol (ARP Announcement)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    [Is gratuitous: True]
    [Is announcement: True]
    Sender MAC address: IntelCor_b3:36:02 (7c:2a:31:b3:36:02)
    Sender IP address: 172.26.55.252
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 172.26.55.252
```

Figura 13: Informação sobre o ARP Gratuito

```
Ethernet II, Src: IntelCor_b3:36:02 (7c:2a:31:b3:36:02), 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: IntelCor_b3:36:02 (7c:2a:31:b3:36:02)
      Address: IntelCor_b3:36:02 (7c:2a:31:b3:36:02)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
> Address Resolution Protocol (ARP Announcement)
```

Figura 14: Trama Ethernet no pacote ARP Gratuito

O ARP gratuito é uma forma de anunciar um novo endereço MAC na rede e por isso esses pacotes são enviados por *broadcast* de forma voluntária para que todos os sistemas na rede possam atualizar as suas tabelas ARP. Assim, de forma a cumprir com

este propósito é enviado para a rede o endereço ff:ff:ff:ff:ff:ff que corresponde ao endereço *broadcast* no caso de uma rede Ethernet, tal como se pode ver na figura 8.

DOMÍNIOS DE COLISÃO

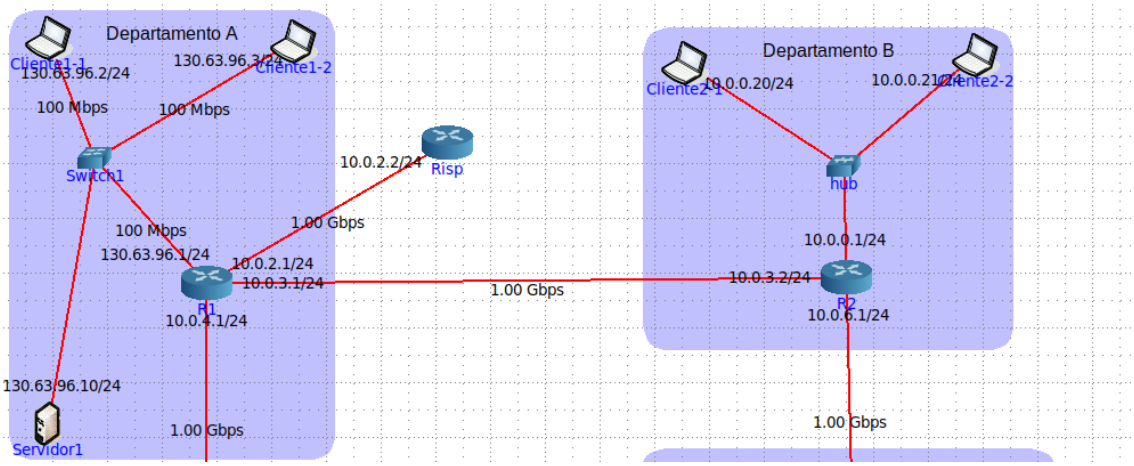

Figura 15: Topologia de rede

16. Através da opção tcpdump verifique e compare como flui o tráfego nas diversas interfaces dos vários dispositivos no departamento A (LAN comutada) e no departamento B (LAN partilhada) quando gera tráfego intra-departamento (por exemplo, através do comando ping). Que conclui?

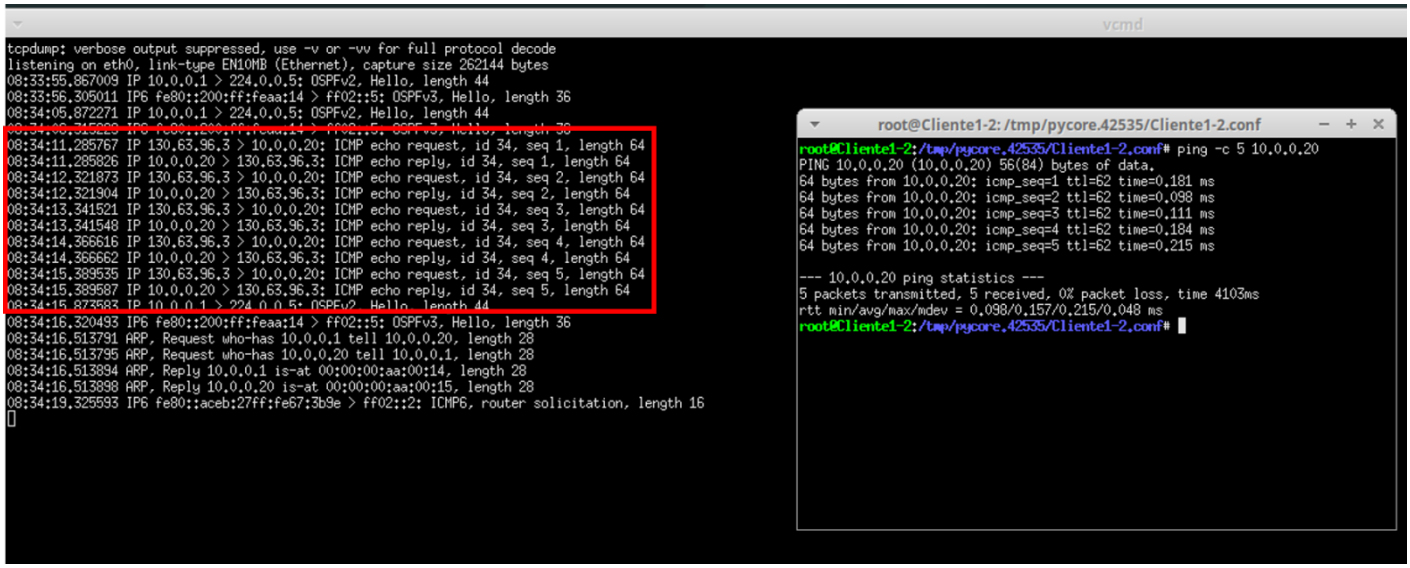

Figura 16: Conectividade entre departamento A e B

Após estabelece conectividade entre A e B através do envio de mensagens do cliente 1-2 para cliente 2-1 (com o uso do comando ping), obteve-se (com uso do comando tcpdump) o bloco vermelho na figura 16 que indica que o cliente 2-2 também recebeu essas mensagens enviadas.

a. Comente os resultados obtidos quanto à utilização de hubs e switches no contexto de controlar ou dividir domínios de colisão. Documente as suas observações e conclusões com base no tráfego observado/capturado

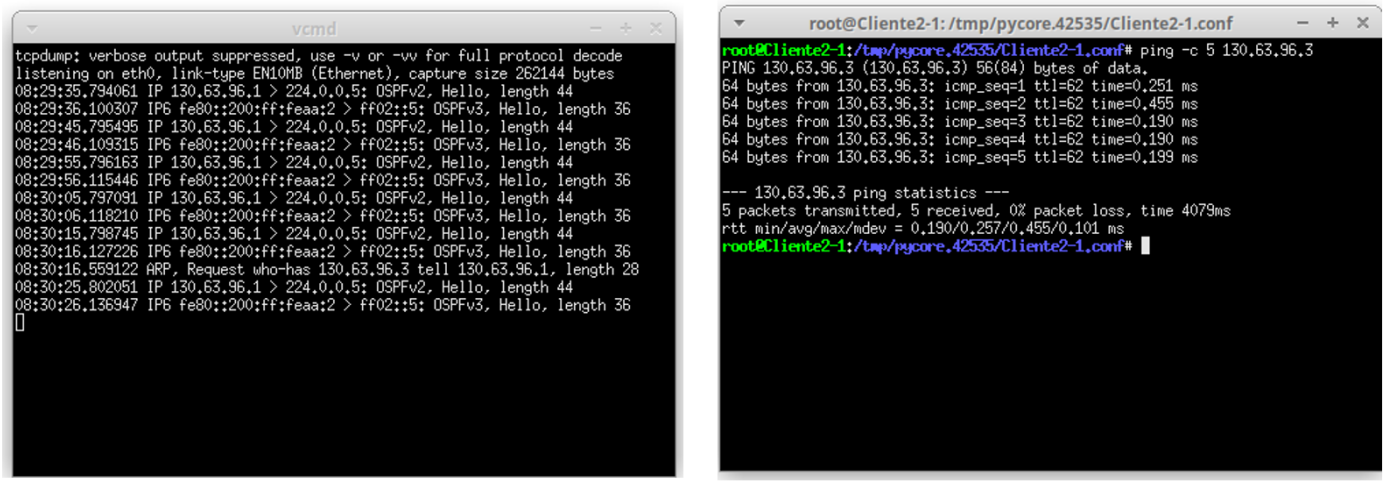

Figura 17: Conectividade entre o departamento B e A

Através da análise da conectividade entre os departamentos A e B e entre B e A, conseguimos reparar que quando se verifica o tráfego de mensagens para o cliente 1-1, durante a troca de informação entre o cliente 2-1 e o cliente 1-2, este não obtém nenhuma mensagem dirigida ao cliente 1-2 (figura 17). Por outro lado, quando se verifica o tráfego para o cliente 2-2, durante a troca de mensagens entre o cliente 1-2 e o 2-1, este obtém mensagens direcionadas para o cliente 2-1 (bloco vermelho da figura 16).

Isto leva-nos a concluir que o uso de um hub impede que haja direcionamento de mensagens entre os vários host conectados a ele, isto é, qualquer informação que seja dirigida a um host específico, os outros que também estejam conectados ao hub recebem essa informação. No caso do switch, este dirige cada mensagem recebida para o host de destino, exclusivamente.

CONCLUSÃO

Neste trabalho prático, mais uma vez podemos referir que tivemos oportunidade de consolidar os conceitos lecionados nas aulas teóricas. Desta vez, conceitos relacionados com as temáticas da camada de ligação lógica.

Desta forma, temos confiança que ampliamos os nossos conhecimentos face ao conteúdo da tecnologia Ethernet e do Protocolo ARP (*Address Resolution Protocol*), compreendendo o seu funcionamento.

Além do mencionado, é importante realçar que este trabalho permitiu-nos visualizar de forma prática a transferência de dados, capturando a mesma e analisando as tramas Ethernet, através do programa wireshark. Com esta análise pudemos avaliar a presença de erros e identificar campos, tais como o *Type*, *Source Address* e *Destination Address*.

Ainda, podemos afirmar que a realização do mesmo nos proporcionou, também, a possibilidade de trabalhar com endereços MAC, percebendo que estes são endereços físicos dos sistemas das redes locais e promoveu o confronto com o conceito de desencapsulamento protocolar.

Tal como referido anteriormente, este projeto teve como objetivo explorar o protocolo ARP e face ao exposto, foi analisado o conteúdo da tabela ARP, podendo observar-se o envio e receção de mensagens ARP.

Por fim, pudemos avaliar a utilização de hubs e switches no controlo de domínios de colisão.

Em suma, este trabalho foi necessário para a expansão de conhecimentos relativos à Link Layer e visualização prática do funcionamento da mesma.