Trabalho Prático Nº3 – Nível de Ligação Lógica : Redes Ethernet e Protocolo ARP

Grupo 17 - Ana Rita Poças (a97284) , Bernard Georges (a96326) e João Pedro Braga (a97368)

3. Captura e análise de Tramas Ethernet

```
No.     Time           Source                Destination           Protocol Length Info
    557 13.932257169   172.26.6.194          193.137.9.150         TLSv1.2  1311   Application Data
Frame 557: 1311 bytes on wire (10488 bits), 1311 bytes captured (10488 bits) on interface wlp11s0, id 0
Ethernet II, Src: dc:41:a9:6c:a5:de (dc:41:a9:6c:a5:de), Dst: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
    Destination: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
    Source: dc:41:a9:6c:a5:de (dc:41:a9:6c:a5:de)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 172.26.6.194, Dst: 193.137.9.150
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1297
    Identification: 0x2adf (10975)
    Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0x8d0c [validation disabled]
    [Header checksum status: Unverified]
    Source: 172.26.6.194
    Destination: 193.137.9.150
Transmission Control Protocol, Src Port: 49858, Dst Port: 443, Seq: 644, Ack: 6171, Len: 1245
Transport Layer Security
```

1. Anote os endereços MAC de origem e de destino da trama capturada.
Src: IntelCor_6c:a5:de (dc:41:a9:6c:a5:de), Dst: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)

2. Identifique a que sistemas se referem. Justifique.
O nosso sistema é representado pelo endereço MAC (dc:41:a9:6c:a5:de) e o sistema do router é representado pelo endereço MAC (00:d0:03:ff:94:00).

3. Qual o valor hexadecimal do campo Type da trama Ethernet? O que significa?
Type: IPv4 (0x0800) este tem como objetivo identificar o IPv4

4. Quantos bytes são usados no encapsulamento protocolar, i.e. desde o início da trama até ao início dos dados do nível aplicacional? Calcule e indique, em percentagem, a sobrecarga (overhead) introduzida pela pilha protocolar

São utilizados para o cabeçalho de Ethernet 14 bytes, para o cabeçalho de IP 20 bytes e para o cabeçalho de TCP 32 bytes.
14+20+32 = 66 bytes de overhead, cerca de 5% do tamanho total do pacote

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

```
No.     Time           Source                Destination           Protocol Length Info
    569 13.977352043   193.137.9.150         172.26.6.194          TLSv1.2  917    Application Data
Frame 569: 917 bytes on wire (7336 bits), 917 bytes captured (7336 bits) on interface wlp11s0, id 0
Ethernet II, Src: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00), Dst: dc:41:a9:6c:a5:de (dc:41:a9:6c:a5:de)
    Destination: dc:41:a9:6c:a5:de (dc:41:a9:6c:a5:de)
    Source: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 193.137.9.150, Dst: 172.26.6.194
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 903
    Identification: 0x0d78 (3448)
    Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 253
    Protocol: TCP (6)
    Header checksum: 0xeefc [validation disabled]
    [Header checksum status: Unverified]
    Source: 193.137.9.150
    Destination: 172.26.6.194
Transmission Control Protocol, Src Port: 443, Dst Port: 49858, Seq: 6171, Ack: 1889, Len: 851
Transport Layer Security
```

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

Src: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
O endereço corresponde ao sistema do site a que foi solicitado um pedido de envio de dados.

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

Dst: IntelCor_6c:a5:de (dc:41:a9:6c:a5:de)
O endereço corresponde ao usuário do site, neste caso o grupo.

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

Protocol: TCP (6)
TLSv1.2 Record Layer: Application Data Protocol: http-over-tls

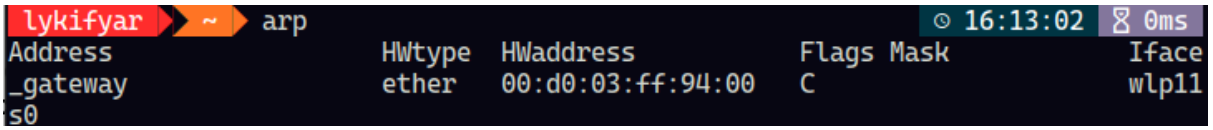
4. Protocolo ARP

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

Interface: 192.168.56.1 --- 0x2
  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

Interface: 172.26.98.251 --- 0x9
  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
```

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

A primeira coluna representa o IP de cada host da rede e este é um endereço que depende da rede. A segunda coluna representa o seu endereço MAC que é um dado pelo NIC sendo único para cada usuário independente da sua rede. Já a última coluna representa o tipo de dados que o usuário está a transportar.

É possível identificar os endereços de broadcast isto porque o seu MAC address é ff-ff-ff-ff-ff-ff



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 32644: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{3F9EB3
Ethernet II, Src: LiteonTe_2a:ef:bb (14:5a:fc:2a:ef:bb), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
```

O destination no pedido ARP é como mostrado em cima ff:ff:ff:ff:ff:ff que se designa como o broadcast isso porque o objetivo inicial do programa é encontrar o valor MAC do host com o ip 172.26.57.47 que é seu destino.

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

`Type: ARP (0x0806)`, o valor apresentado indica que o payload é um pacote do tipo 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?

```
Opcode: request (1)
Sender MAC address: dc:41:a9:6c:a5:de (dc:41:a9:6c:a5:de)
Sender IP address: 172.26.6.194
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
Target IP address: 172.26.76.34
```

O Opcode confirma que efetivamente estamos perante um pedido ARP.
A mensagem ARP contém IP da origem e do seu destino final e MAC da origem e do router.

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

O host de origem inicialmente não possui o MAC address do seu destino necessitando primeiramente gerar sua tabela ARP ele pede primeiramente o endereço MAC de seu objetivo guardando em sua tabela e podendo agora mandar o sua trama para este endereço.

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

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

```
Opcode: reply (2)
```

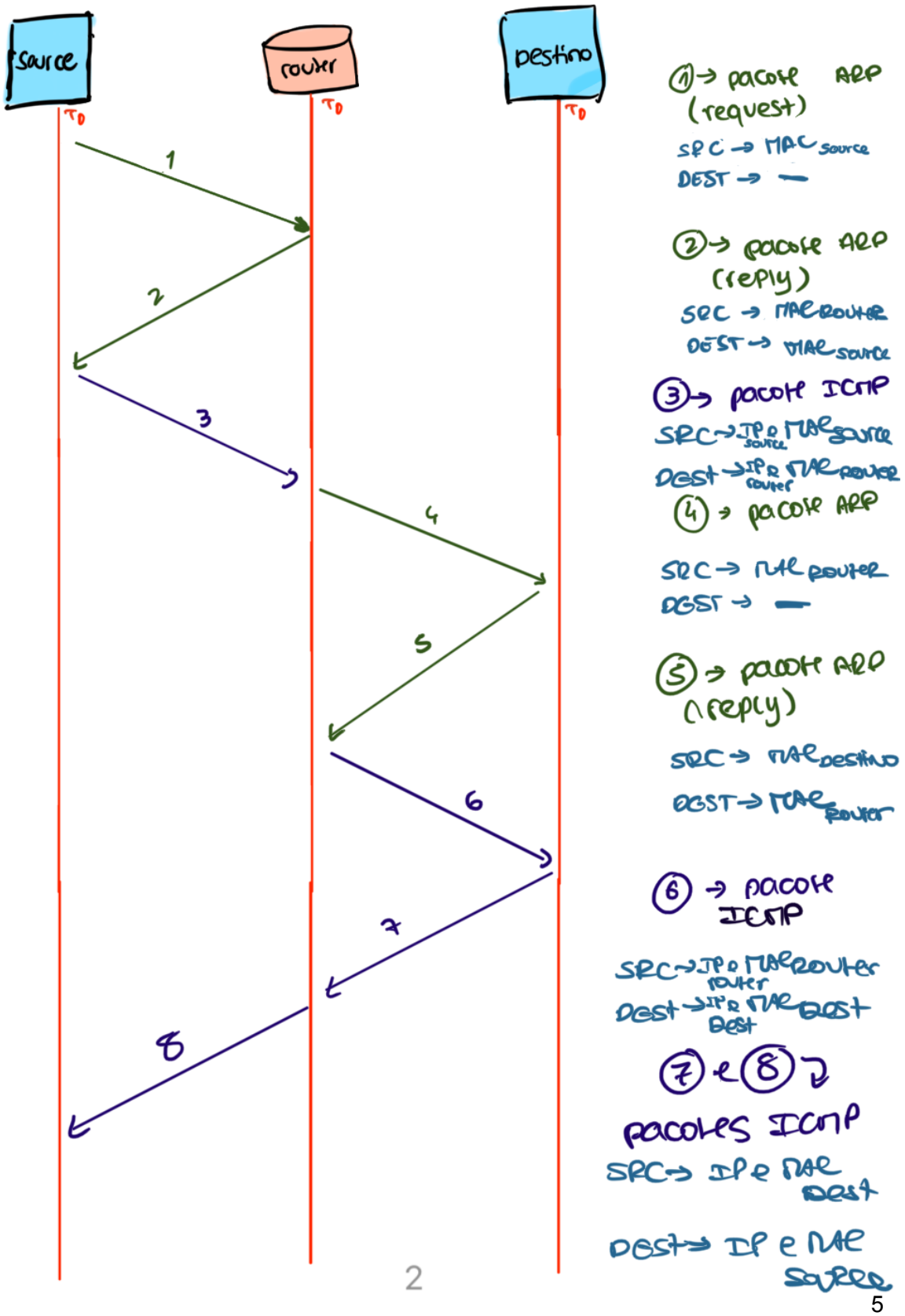
O valor do campo Opcode é 2, que especifica uma resposta (reply).

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

```
Sender MAC address: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
Sender IP address: 172.26.254.254
```

Encontra-se no campo MAC address.

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.



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?

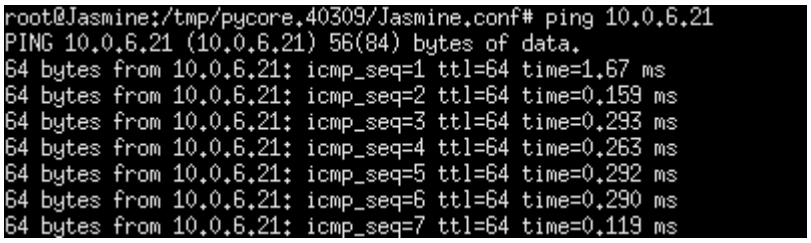
Bela

```
root@Bela:/tmp/pycore.40309/Bela.conf# ping 10.0.7.21
PING 10.0.7.21 (10.0.7.21) 56(84) bytes of data.
64 bytes from 10.0.7.21: icmp_seq=1 ttl=64 time=0.559 ms
64 bytes from 10.0.7.21: icmp_seq=2 ttl=64 time=1.19 ms
64 bytes from 10.0.7.21: icmp_seq=3 ttl=64 time=2.02 ms
64 bytes from 10.0.7.21: icmp_seq=4 ttl=64 time=1.77 ms
64 bytes from 10.0.7.21: icmp_seq=5 ttl=64 time=12.7 ms
64 bytes from 10.0.7.21: icmp_seq=6 ttl=64 time=1.75 ms
64 bytes from 10.0.7.21: icmp_seq=7 ttl=64 time=2.14 ms
64 bytes from 10.0.7.21: icmp_seq=8 ttl=64 time=1.30 ms
64 bytes from 10.0.7.21: icmp_seq=9 ttl=64 time=4.01 ms
64 bytes from 10.0.7.21: icmp_seq=10 ttl=64 time=1.82 ms
64 bytes from 10.0.7.21: icmp_seq=11 ttl=64 time=0.806 ms
64 bytes from 10.0.7.21: icmp_seq=12 ttl=64 time=2.21 ms
```

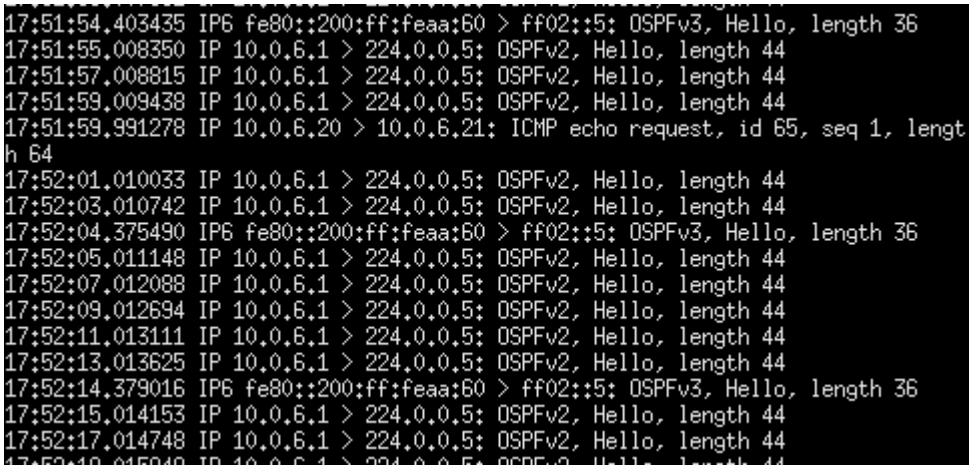
Output de tcpdump no server A

```
17:37:57.067072 IP 10.0.7.20 > 10.0.7.21: ICMP echo request, id 76, seq 11, leng
th 64
17:37:57.070564 IP 10.0.7.21 > 10.0.7.20: ICMP echo reply, id 76, seq 11, length
 64
17:37:58.069100 IP 10.0.7.20 > 10.0.7.21: ICMP echo request, id 76, seq 12, leng
th 64
17:37:58.071338 IP 10.0.7.21 > 10.0.7.20: ICMP echo reply, id 76, seq 12, length
 64
17:37:58.573136 IP 10.0.7.1 > 224.0.0.5: OSPFv2, Hello, length 44
17:37:59.070731 IP 10.0.7.20 > 10.0.7.21: ICMP echo request, id 76, seq 13, leng
th 64
17:37:59.072898 IP 10.0.7.21 > 10.0.7.20: ICMP echo reply, id 76, seq 13, length
 64
17:38:00.072372 IP 10.0.7.20 > 10.0.7.21: ICMP echo request, id 76, seq 14, leng
th 64
17:38:00.074099 IP 10.0.7.21 > 10.0.7.20: ICMP echo reply, id 76, seq 14, length
 64
17:38:00.573952 IP 10.0.7.1 > 224.0.0.5: OSPFv2, Hello, length 44
17:38:01.074203 IP 10.0.7.20 > 10.0.7.21: ICMP echo request, id 76, seq 15, leng
th 64
```

Jasmine para Alladin



Output do tcpdump do server B



Verificamos que, ao utilizar ping da Bela para o Monstro, o Servidor A recebe todos os pacotes que entram em trânsito na rede devido ao ping (através do tcpdump), mesmo não sendo destinado a este dispositivo.

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.

Comparado com os hubs, que propagam os pacotes que recebe para todos os dispositivos adjacentes, os switches são capazes de minimizar estes domínios de colisão, isto porque o switch compromete-se a registar os destinos em primeira instância para posteriormente apenas enviar os pacotes aos destinos corretos e não para todos os destinos possíveis, evitando colisões após este ponto.

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

	MAC ADDRESS	INTERFACE	TTL
Jasmine	00:00:00:aa:00:62	E2	60
SB	00:00:00:aa:00:61	E1	60
Aladin	00:00:00:aa:00:63	E3	60
RB	00:00:00:aa:00:60	E0	60

Conclusão

A realização deste trabalho prático, possibilitou a consolidação dos conceitos que tínhamos adquirido anteriormente nas aulas teóricas, sobretudo os conceitos de Redes Ethernet e Protocolo ARP, que serão fundamentais para o bom aproveitamento à Unidade Curricular e necessários no decorrer das nossas aprendizagens como futuros Engenheiros Informáticos.