Trabalho Prático Nº2

Universidade do Minho

Ana Inês Leite

a96159@uminho.pt

Diana Filipa Ferreira Malheiro Teixeira

a97516@uminho.pt

Pedro Marcelo Bogas Oliveira

a95076@uminho.pt

Índice

Objetivo

Este trabalho prático tem por principal objetivo a exploração da camada de ligação lógica, focando o uso da tecnologia Ethernet e o protocolo ARP.

Questões e Respostas

1. **Anote os endereços MAC de origem e de destino da trama capturada.**
    - MAC origem: 00:bb:60:86:80:35
    - MAC destino: 00:d0:03:ff:94:00

Figura 1-Endereços MAC e o Type da trama

2. **Identifique a que sistemas se referem. Justifique.**
    - Origem – nosso computador
    - Destino – servidor do e-learning

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

    O valor hexadecimal do campo Type da trama Ethernet, tal como é visível na figura anterior, é 0x0800 e representa o protocolo de camada superior utilizado, 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.**

    O número de bytes usados será de 66 bytes, pois:
    - Ethernet length = 14 bytes;
    - IP = 20 bytes;
    - TCP = 32 bytes;

    Sendo, por sua vez, a overhead:

    - Ethernet vai de 14 a 33 bytes, logo tem 20 de cabeçalho.
    - IP vai de 35 a 53 bytes, logo tem 19.
    - TCP vai de 54 a 152, logo tem 99.

Face a isto, temos que o overhead vai ser de 461, o que resulta numa percentagem de sobrecarga de 14.317%.

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

O endereço Ethernet da fonte é 00:d0:03:ff:94:00 e corresponde ao default gateway da rede local. A noção de que as tramas são trocadas entre o nosso computador e o default gateway é fundamentada pelo facto de o servidor não se encontrar na rede local, não sendo alcançável.

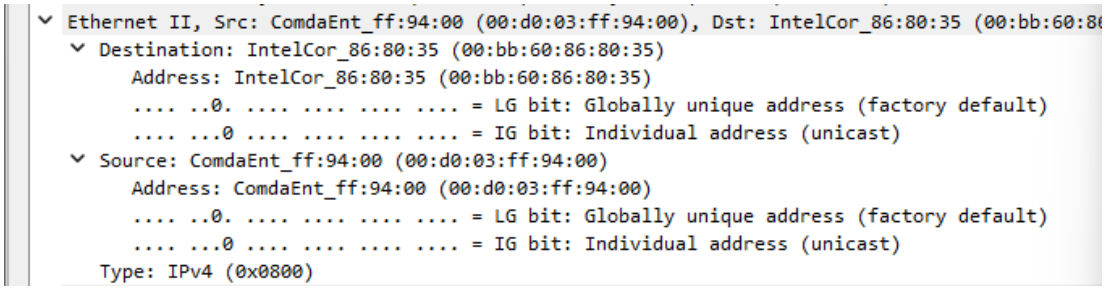

Figura 2-Endereços da trama capturada

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

O endereço MAC do destino, tal como podemos observar na figura em cima colocada, é 00:bb:60:86:80:35 e corresponde à interface Ethernet da nossa máquina.

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

Os protocolos contidos na trama recebida são Ethernet,IPv4 e TCP.

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

- Interface – interface de rede
- Internet Address – endereços
- Physical Address – endereço MAC ou Ethernet (protocolo da camada física também é do tipo Ethernet)
- Type – tipo de protocolo da camada física usado

```
Interface: 192.168.56.1 --- 0x6
  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: 172.26.97.244 --- 0xd
  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
```

Figura 3-comando arp -a

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?**

O valor hexadecimal do endereço origem é 00:bb:60:86:80:35 e destino é ff:ff:ff:ff:ff:ff.

O endereço destino utilizado é o Broadcast e é utilizado porque a máquina necessita de informação sobre o mesmo. Desta forma, a máquina envia a ARP request para o endereço Broadcast e espera que o destino lhe indique o seu endereço MAC, posteriormente colocado na tabela ARP.

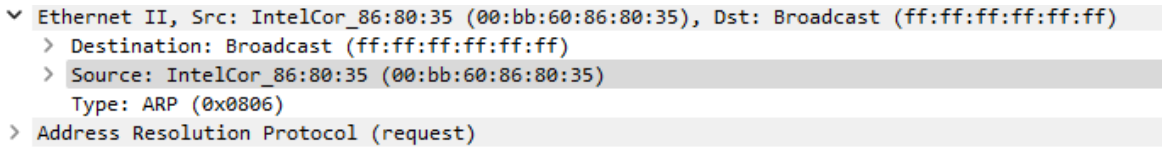

Figura 4-Endereços e Type

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

O valor hexadecimal do campo tipo da trama Ethernet, como podemos ver na figura 4, é 0x0806 e indica que está a ser utilizado o protocolo 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?**

No campo Opcode, lê-se "request(1)", o que nos leva a concluir que estamos na presença de uma mensagem com ARP request. Observando os endereços da mensagem ARP, concluímos que são do tipo IP(origem e destino) e MAC(origem).

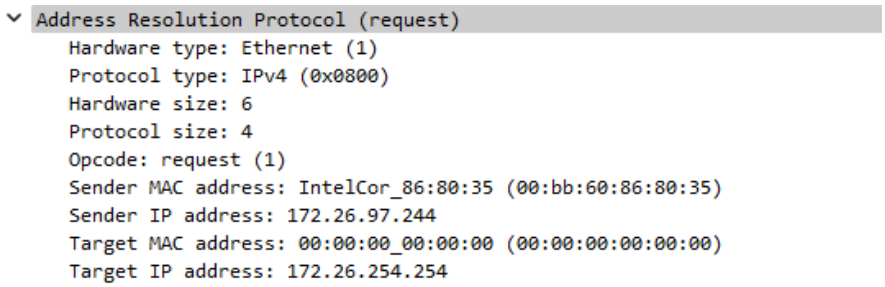

Figura 5-campo Opcode da trama

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

O host de origem pergunta aos restantes hosts qual tem o endereço 172.26.254.254 e pede que a resposta seja enviada para o endereço 172.26.97.244.

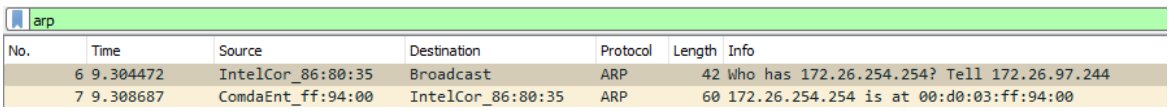

Figura 6-Pergunta/Pedido feito pelo host

13. **Localize a mensagem ARP que é a resposta ao pedido ARP efetuado.**
    a. **Qual o valor do campo ARP opcode? O que especifica?**

        O valor do campo ARP opcode é "reply (2)" e especifica uma mensagem ARP reply.

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

        No campo Sender MAC address.

```
Ethernet II, Src: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00), Dst: IntelCor_86:80:35 (00:bb:60:86:80:35)
  Destination: IntelCor_86:80:35 (00:bb:60:86:80:35)
  Source: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
  Type: ARP (0x0806)
  Padding: 00000000000000000000000000000000000000
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_86:80:35 (00:bb:60:86:80:35)
  Target IP address: 172.26.97.244
```

Figura 7-mensagem ARP reply

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.**

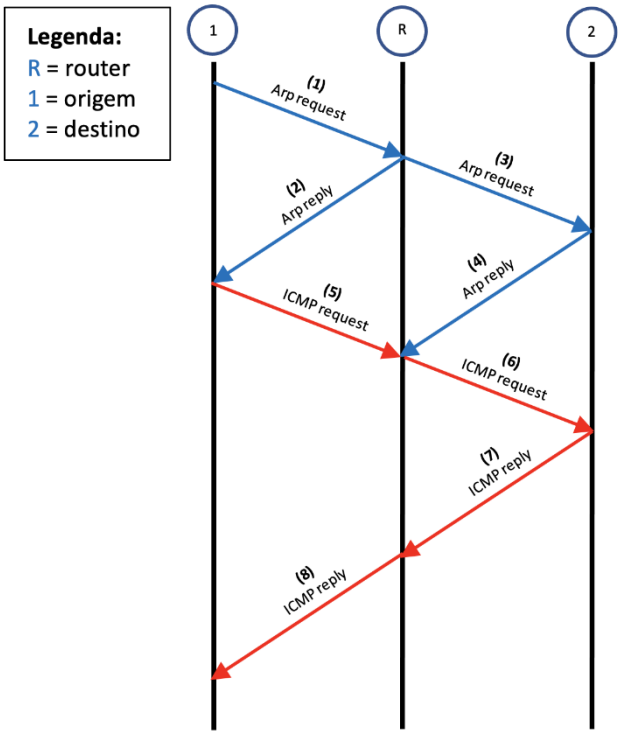

Figura 8-Diagrama de mensagens ARP e ICMP

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?**

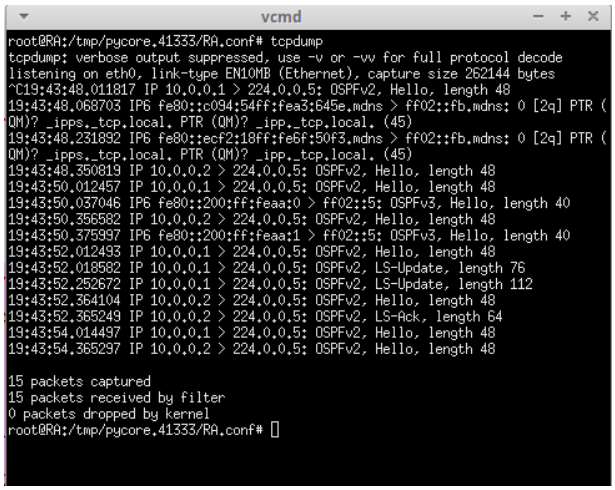

Figura 11-Comando tcpdump em A

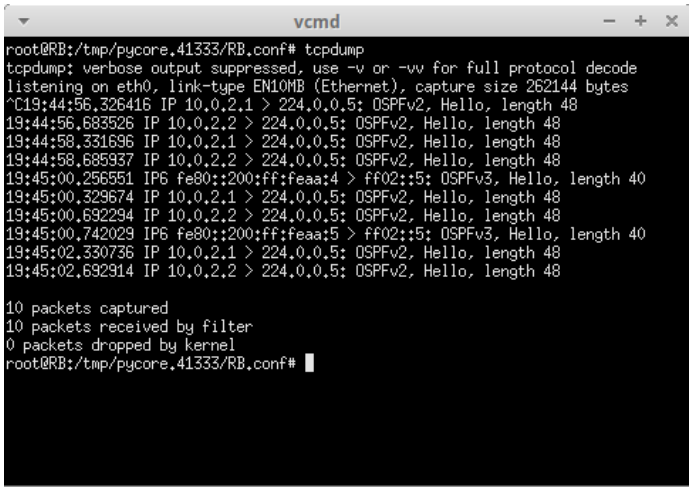

Figura 9-Comando tcpdump em B

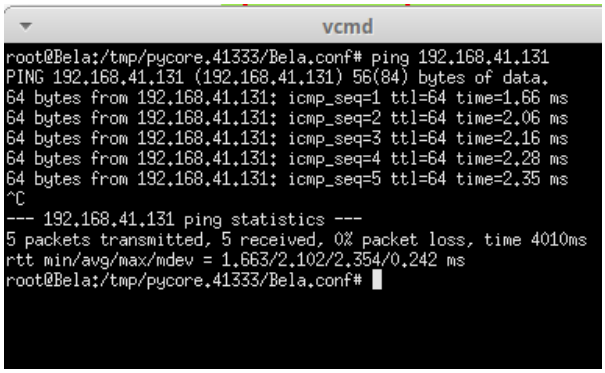

Figura 12-Ping da Bela para o Monstro

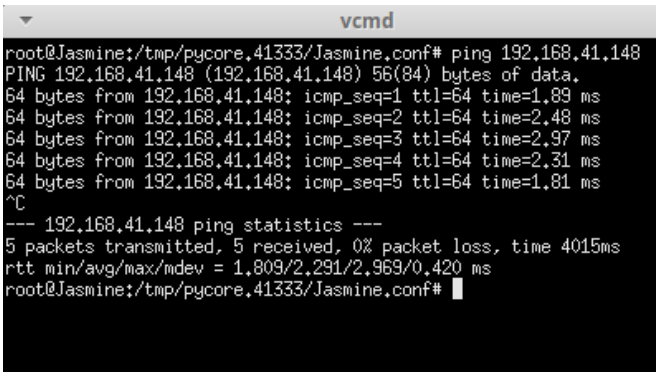

Figura 10-Ping da Jasmine para o Alladin

Como podemos ver nas figuras acima,

- no departamento A(rede partilhada), é utilizado um repetidor (hub), sendo possível, depois de executar o comando ping, observar as tramas enviadas – echo request e echo reply
- no departamento B(rede comutada), é utilizado um switch, e essas tramas não são capturadas como consequência de execução docomando ping, ao contrário do que acontece no departamento A.

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

MAC address	Interface	TTL
Jasmine	1	60
Alladin	2	60
SB	3	60

Conclusão

Concluída a execução deste trabalho prático foi-nos permitido consolidar melhor a matéria e perceber a sua utilidade no que toca a temas como endereços MAC, mensagem com protocolos ARP, interligação de redes locais, captura e análise de tramas Ethernet.