

Trabalho Prático 3
Redes de Computadores
PL53

Gonçalo Soares^[a93286], Mariana Rodrigues^[a93229], and Rita Teixeira^[a89494]

Universidade do Minho

Captura e Análise de Tramas Ethernet

Começamos o projeto por, como o enunciado pede, limpar a cache do *browser* a utilizar, ativar o Wireshark e aceder ao URL <https://elearning.uminho.pt>. Seguidamente, paramos a captura do Wireshark e selecionamos as mensagens de HTTP GET.

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

Analisando a trama obtida:

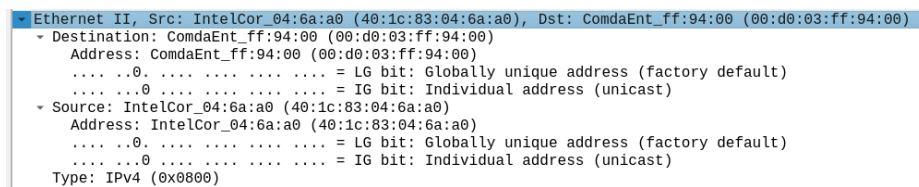


Figura 1. Informação da trama da mensagem HTTP GET

É possível concluir que o endereço MAC de origem é **IntelCor_04:6a:a0 (40:1c:83:04:6a:a0)** e o de destino é **ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)**.

2 Pergunta 2 - Identifique a que sistemas se referem. Justifique.

O endereço MAC de origem corresponde ao da interface da nossa máquina nativa, isto é, o nosso computador. Já o MAC de destino, corresponde ao router da rede local à qual estávamos ligados.

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

Partindo da informação mostrada na Figura 1, é possível identificar que o valor do campo *Type*, valor que identifica o protocolo IPv4, é **0x0800**. Este campo serve para identificar o protocolo encapsulado no campo de dados da trama selecionada, ou seja, IPv4.

- 4 Pergunta 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.

```
▼ Frame 590: 1088 bytes on wire (8704 bits), 1088 bytes captured (8704 bits) on interface wlp0s20f3, id 0
```

Figura 2. Tamanho da trama

TCP payload (1022 bytes)

Figura 3. Tamanho do payload da trama

É possível calcular quantos bytes são usados no encapsulamento protocolar, através da subtração do *payload* ao tamanho total da trama. Assim sendo, foi realizado $1088 - 1022 = 66$ de maneira a determinar o valor de bytes usados no encapsulamento protocolar. Este valor corresponde a $66/1088 = 6.07\%$ de overhead.

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

```

[Capturing data using tcpdump on interface wlp0s20f3]
▼ Ethernet II, Src: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00), Dst: IntelCor_04:6a:a0 (40:1c:83:04:6a:a0)
  ▼ Destination: IntelCor_04:6a:a0 (40:1c:83:04:6a:a0)
    Address: IntelCor_04:6a:a0 (40:1c:83:04:6a:a0)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  ▼ Source: 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)
  Type: IPv4 (0x0800)

```

Figura 4. Tabela ARP

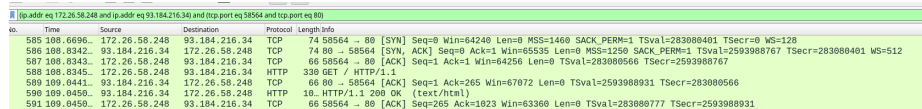
O endereço Ethernet da fonte é **ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)**, que corresponde ao router da rede local à qual nos encontravamos ligados.

6 Pergunta 6 - Qual   o endereo MAC do destino? A que sistema corresponde?

Ainda mencionando a figura anterior, o endereo MAC do destino   **Intel-Cor_04:6a:a0 (40:1c:83:04:6a:a0)**. O endereo MAC   usado para identificar os dispositivos f sicos de origem e destino no segmento de rede local. Assim sendo, neste caso o endereo refere-se ao sistema que consiste no computador no qual foi realizado o trabalho.

7 Pergunta 7 - Atendendo ao conceito de desencapsulamento protocolar, identifique os v rios protocolos contidos na trama recebida.

Observando a imagem:



No.	Time	Source	Destination	Protocol	Length	Info
585	108.6696..	172.26.58.248	93.184.216.34	TCP	74	58564 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=283888401 TSecr=0 WS=128
586	108.8342..	93.184.216.34	172.26.58.248	TCP	74	80 → 58564 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1250 SACK_PERM=1 TSval=2593988767 TSecr=283888401 WS=512
587	108.8343..	172.26.58.248	93.184.216.34	TCP	66	58564 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=283888566 TSecr=2593988767
588	108.8345..	172.26.58.248	93.184.216.34	HTTP	338	GET / HTTP/1.1
589	109.0441..	93.184.216.34	172.26.58.248	TCP	66	80 → 58564 [ACK] Seq=1 Ack=265 Win=67072 Len=0 TSval=2593988931 TSecr=283888566
590	109.0450..	93.184.216.34	172.26.58.248	HTTP	10..	HTTP/1.1 200 OK (text/html)
591	109.0450..	172.26.58.248	93.184.216.34	TCP	66	58564 → 80 [ACK] Seq=265 Ack=1023 Win=63360 Len=0 TSval=283888777 TSecr=2593988931

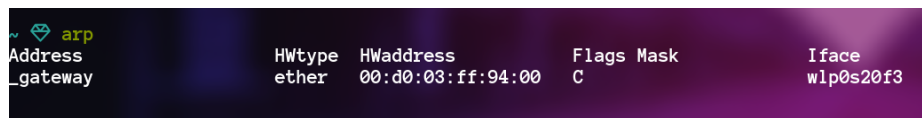
Figura 5. Captura de Tramas Ethernet

  poss vel identificar v rios protocolos na trama capturada. Estes s o:

- Ethernet II
- Internet Protocol version 4 (IPv4)
- Transmission Control Protocol (TCP)
- HyperText Transfer Protocol (HTTP)

Protocolo ARP

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



Address	HWtype	HWaddress	Flags	Mask	Iface
gateway	ether	00:d0:03:ff:94:00	C		wlp0s20f3

Figura 6. Tabela ARP

A tabela ARP é usada para manter uma correlação entre cada endereço MAC e seu endereço IP correspondente. Assim sendo, a coluna *Address* registra os endereços IP, podendo estes ser apresentados através do nome do dispositivo ao qual o IP refere. Na segunda coluna podemos observar o tipo de protocolo de rede associado (que no nosso caso a conexão é do tipo Ethernet) e a terceira coluna mostra o endereço físico do dispositivo (MAC address). A coluna *Flags Mask* dá informação relevante sobre a entrada dos valores na tabela (neste caso, como a *flag* apresentada é 'C', significa que as entradas na tabela são aprendidas dinamicamente pelo protocolo *arp*). Por fim, a coluna *Iface* identifica o interface usado pelo dispositivo.

- 9 Pergunta 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 159: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface wlp0s20f3, id 0
  ▶ Interface id: 0 (wlp0s20f3)
    Encapsulation type: Ethernet (1)
    Arrival Time: Apr 21, 2022 15:18:10.697800220 WEST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1650550690.697800220 seconds
    [Time delta from previous captured frame: 3.391728108 seconds]
    [Time delta from previous displayed frame: 3.391728108 seconds]
    [Time since reference or first frame: 55.188475637 seconds]
    Frame Number: 159
    Frame Length: 42 bytes (336 bits)
    Capture Length: 42 bytes (336 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:arp]
    [Coloring Rule Name: ARP]
    [Coloring Rule String: arp]
  ▼ Ethernet II, Src: IntelCor_04:6a:a0 (40:1c:83:04:6a:a0), 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_04:6a:a0 (40:1c:83:04:6a:a0)
    Address: IntelCor_04:6a:a0 (40:1c:83:04:6a:a0)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
  ▼ 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_04:6a:a0 (40:1c:83:04:6a:a0)
    Sender IP address: 172.26.119.148
    Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
    Target IP address: 172.26.254.254

```

Figura 7. Pedido ARP

Os endereos de origem e destino na trama Ethernet so, respetivamente, **40:1c:83:04:6a:a0** e **ff:ff:ff:ff:ff:ff**.

A necessidade de uma mensagem do tipo ARP *request* surge quando um dispositivo deseja saber o endereo MAC do dispositivo com o qual a fonte deseja comunicar. Assim sendo,  necessrio que ambos os dispositivos conheam o endereo IP e MAC um do outro. Cada dispositivo de uma rede conhece o endereo IP dos outros dispositivos, mas no o endereo MAC. Deste modo, o ARP *request*  gerado pelo dispositivo de origem para obter o endereo MAC do dispositivo de destino.

10 Pergunta 10 - Qual o valor hexadecimal do campo Tipo da trama Ethernet? O que indica?

O campo Tipo (*Type*) da trama Ethernet apresenta o valor 0x0800. Este campo indica qual o protocolo que se encontra encapsulado no *payload* da *frame*, que neste caso  o ARP.

11 Pergunta 11 - Como pode confirmar que se trata efetivamente de um pedido ARP? Identifique que tipo de endereços estão contidos na mensagem ARP? Que conclui?

Através da parte da Figura 5 que retrata o pedido ARP:

```

Type: ARP (0x00000000)
▼ 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_04:6a:a0 (40:1c:83:04:6a:a0)
  Sender IP address: 172.26.119.148
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 172.26.254.254
  
```

Figura 8. Mensagem do tipo ARP request

Aqui podemos constatar que o campo *opcode* contém "request" e código 1, logo podemos concluir que se trata de uma mensagem *ARP request*.

Os tipos de endereços contidos nessa mensagem são os endereços de **IP** origem e destino, e endereço *MAC* origem, visto que a origem ainda não conhece o endereço *MAC* de origem.

12 Pergunta 12 - Explícite que tipo de pedido ou pergunta é feita pelo host de origem.

Observando a imagem:

159 55.18847...	IntelCor_04:6a:a0	Broadcast	ARP	42 Who has 172.26.254.254? Tell 172.26.119.148
160 55.19960...	ComdaEnt_ff:94:00	IntelCor_04:6a:a0	ARP	60 172.26.254.254 is at 00:00:03:ff:94:00

Figura 9. Pergunta feita pelo host de origem

"Who has 172.26.254.254? Tell 172.26.119.148"

A máquina origem pretende saber quem tem o endereço de **IP** 172.26.254.254, pelo que pergunta a todos os *hosts* qual deles é que tem esse endereço, e pede para enviar essa resposta para o endereço de **IP** 172.26.119.148.

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

Observando a imagem:

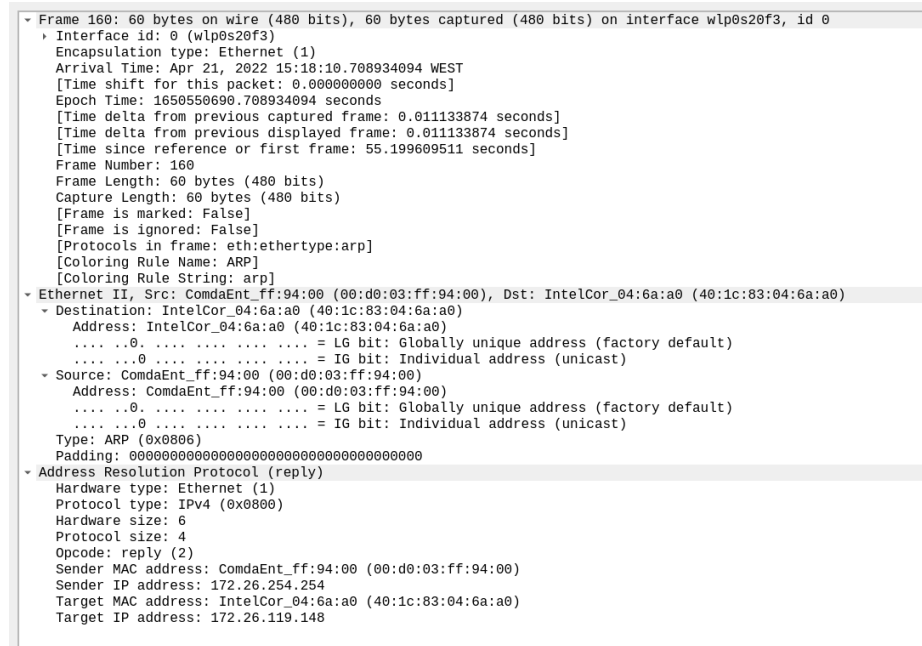


Figura 10. ARP Reply

13.1 Alínea a - Qual o valor do campo ARP opcode? O que especifica?

O valor do campo opcode é "reply" com código 2, que especifica que se trata de uma mensagem **ARP** reply.

13.2 Alínea b - Em que campo da mensagem ARP está a resposta ao pedido ARP?

A resposta ao pedido encontra-se presente no campo *Sender MAC address*.

- 14 Pergunta 14 - Na situação em que efetua um ping a outro host, assumo 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.

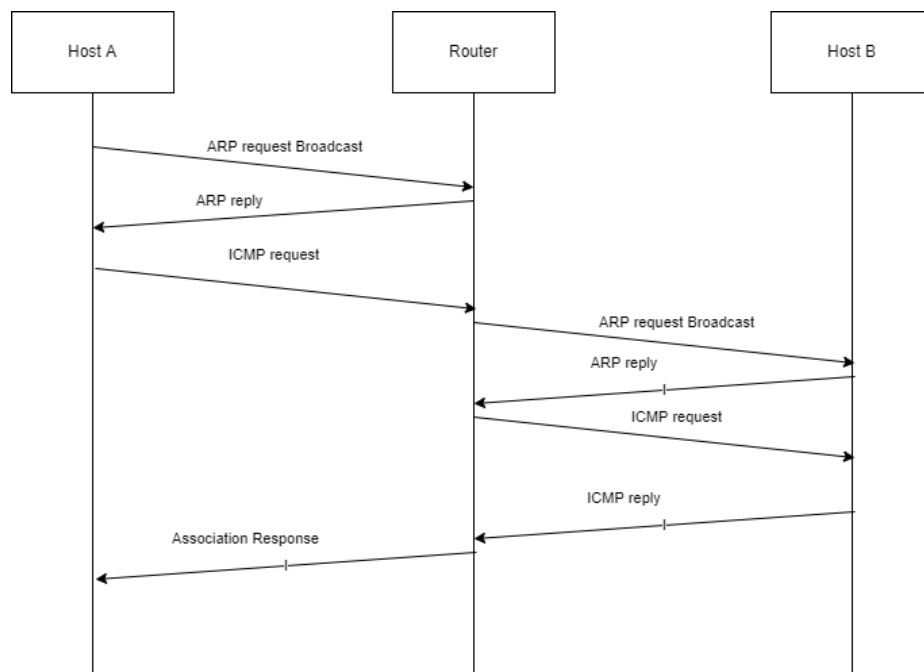


Figura 11. Diagrama das mensagens ARP e ICMP trocadas na situação descrita em cima

[illegible][illegible]

Com isto, é possível concluir que no Departamento B, como a rede é comutada devido ao uso de um *switch*, o computador *Aladin* não captura as tramas

enviadas pelo computador *Jasmin*. É de salientar que são capturas outras tramas, no entanto estas nada tem a ver com o comando ping efetuado.

Por outro lado, no Departamento A, onde a rede é partilhado devido ao uso de um *hub*, o computador *Monstro* consegue ver as tramas enviadas pelo computador *Bela*. Nomeadamente o *echo request* e o *echo reply*, entre a Bela (10.0.5.20) e o computador com endereço (10.0.8.20), resultado do comando *ping* 10.0.8.20 executado na *Bela*.

Sendo assim, os *hubs* transmitem a mensagem recebida para todos os nodos da rede através de um único canal de comunicação, tornando as colisões mais frequentes. No entanto, os *Switches* enviam a mensagem apenas para o destino pretendido, reduzindo assim a possibilidade de colisões. Posto isto, podemos afirmar que os *switches* são mais viáveis do que os *hubs*.

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

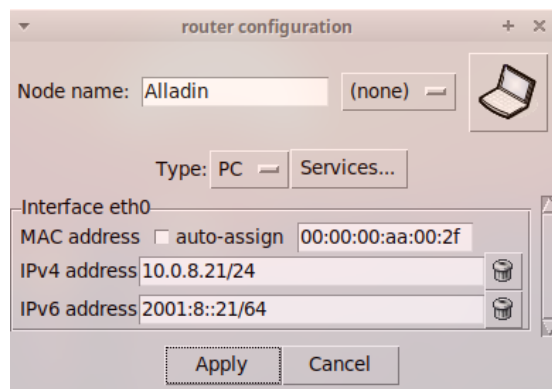


Figura 14. MAC Alladin

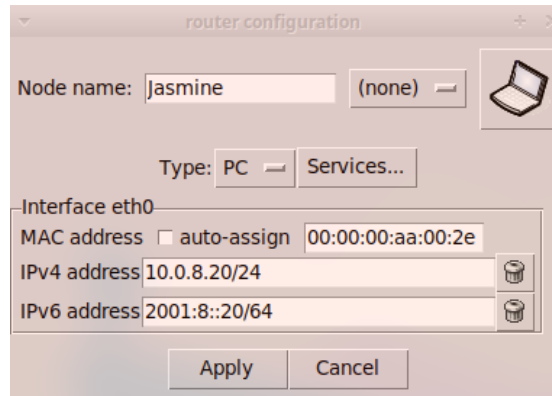


Figura 15. MAC Jasmine

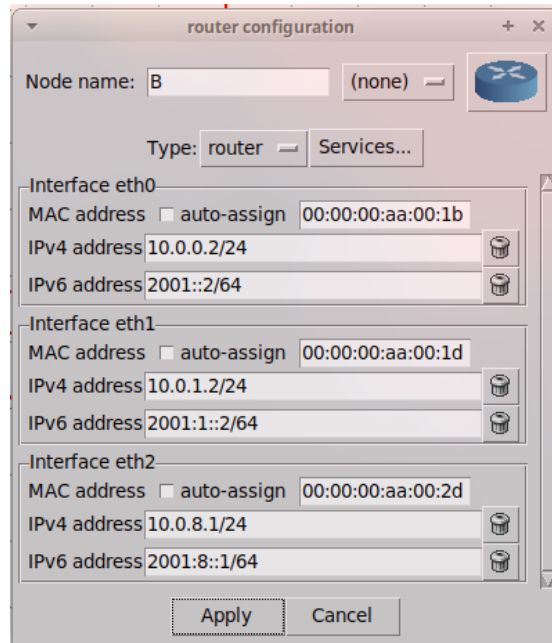


Figura 16. MAC Router B

Sendo assim, podemos concluir:

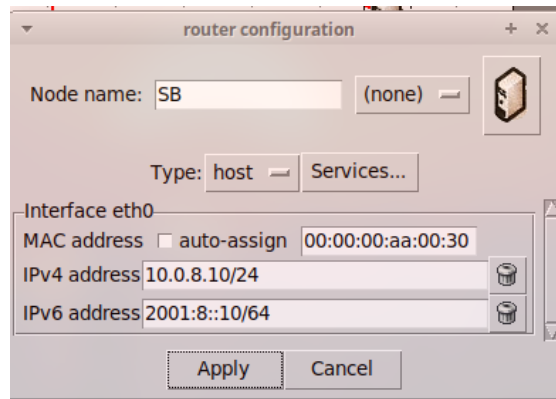


Figura 17. MAC Switch B

Nome	Mac Address	Port
Alladin	00:00:00:aa:00:2f	1
Jasmine	00:00:00:aa:00:2e	2
Router	00:00:00:aa:00:2d	3
SB	00:00:00:aa:00:30	4

Conclusão

Através da realização deste trabalho prático pudemos consolidar e aprofundar melhor a matéria lecionada nas aulas teóricas relativas à camada de ligação lógica, mais concretamente o uso da tecnologia Ethernet e o protocolo ARP.