



UNIVERSIDADE DO MINHO

DEPARTAMENTO DE INFORMÁTICA

TP3: Nível de Ligação Lógica  
Redes Ethernet e Protocolo ARP  
PL12 – Grupo 120

Francisco Peixoto (a84668)      José Fernandes (a93163)  
Henrique Parola (a93325)

Maio 2022

## **Conteúdo**

<b>1</b>	<b>Introdução</b>	<b>1</b>
<b>2</b>	<b>Captura e análise de Tramas Ethernet</b>	<b>2</b>
<b>3</b>	<b>Protocolo ARP</b>	<b>6</b>
<b>4</b>	<b>Domínios de colisão</b>	<b>11</b>
<b>5</b>	<b>Conclusão</b>	<b>13</b>

# 1 Introdução

Este trabalho foi realizado no âmbito da disciplina de Redes de Computadores da Licenciatura em Engenharia Informática da universidade do Minho. Neste trabalho foram respondidas diversas questões relacionadas com o protocolo Ethernet e ARP.

Inicialmente serão apresentadas algumas experiências realizadas na rede Eduroam da Universidades do Minho, de modo a ser feita uma análise das tramas Ethernet capturadas após ser acedido a plataforma do Elearning. De seguida é explorado o protocolo ARP no detalhe, com modificações nas tabelas ARP para um melhor entendimento de tal protocolo. Por fim será investigado o conceito de "domínios de colisão", fazendo uso da topologia do Core criada no trabalho anterior.

## 2 Captura e análise de Tramas Ethernet

```
No.      Time          Source           Destination      Protocol Length Info
  44 3.427910      172.26.109.29    193.137.9.150    TLSv1.2    773    Application Data
Frame 44: 773 bytes on wire (6184 bits), 773 bytes captured (6184 bits) on interface \Device\NPF_{6AD8C3E6-F113-495F-9065-B10E986452AA}, id 0
Ethernet II, Src: LiteonTe_5a:fd:a9 (94:e9:79:5a:fd:a9), Dst: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
    Destination: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
    Source: LiteonTe_5a:fd:a9 (94:e9:79:5a:fd:a9)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 172.26.109.29, Dst: 193.137.9.150
Transmission Control Protocol, Src Port: 60252, Dst Port: 443, Seq: 644, Ack: 6171, Len: 719
Transport Layer Security
```

Figura 1: Captura da Frame 44, relativa à mensagem de acesso ao servidor (HTTP GET encriptada)

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

Como pode ser visto na imagem acima, o endereço MAC de origem é **94:e9:79:5a:fd:a9**, enquanto o de destino é **00:d0:03:ff:94:00**.

### 2) Identifique a que sistemas se referem. Justifique.

O endereço MAC de origem trata-se de um *host* que foi o portátil usado para a experiência. Para justificar isto foi realizado o comando **ipconfig** como se mostra abaixo:

```
Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . : lan
Description . . . . . : Qualcomm Atheros QCA9377 Wireless Network Adapter
Physical Address. . . . . : 94-E9-79-5A-FD-A9
```

Figura 2: Endereço MAC da origem

O sistema referente ao endereço MAC de destino é um *router*. Isto porque, apesar do IP destino ser o do servidor do Elearning e apesar de estar no contexto da rede Eduroam, dado os testes terem sido realizados numa zona distinta da localização dos servidores da Universidade, então podemos concluir que o pacote capturado devia necessariamente passar por um *router* até chegar ao destino pretendido.

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

Como pode ser visto na Figura 1, o valor do campo Type é **0x0800**. Este valor indica o protocolo da camada acima (*network layer*) que está encapsulado na trama Ethernet que, nesse caso, é o protocolo 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.

São usados 53 *bytes* até ao início dos dados do nível aplicacional, como comprova a imagem seguinte com o *byte 53* ainda relativo ao TCP e o *byte 54* relativo ao TLS. Desta maneira, como o pacote capturado possui no total 773 *bytes*, então o *overhead* introduzido na pilha protocolar foi de aproximadamente 7%.

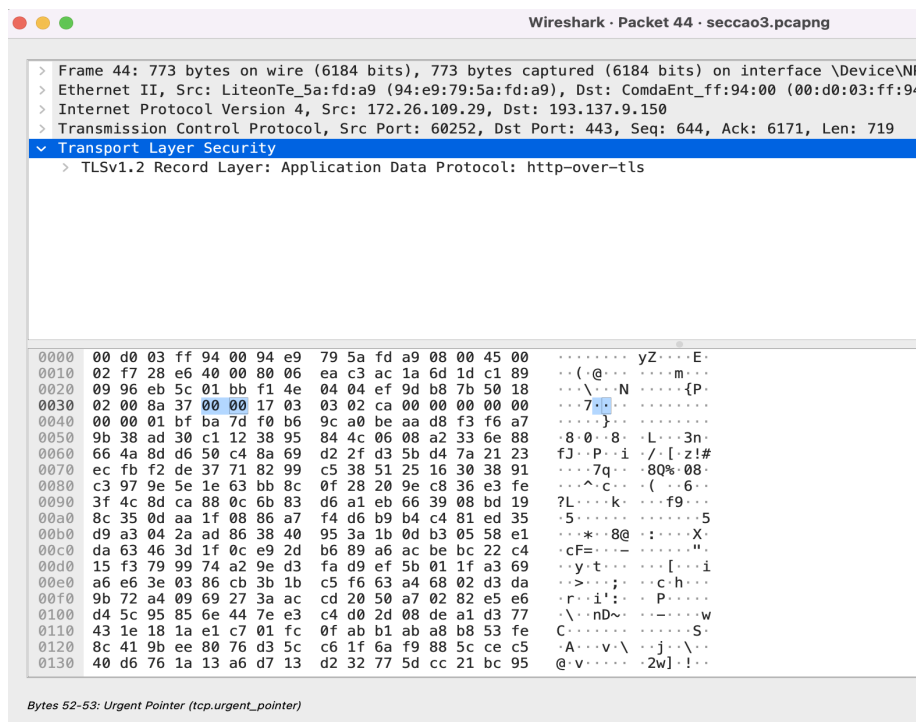


Figura 3: Último byte referente ao TCP - byte 53

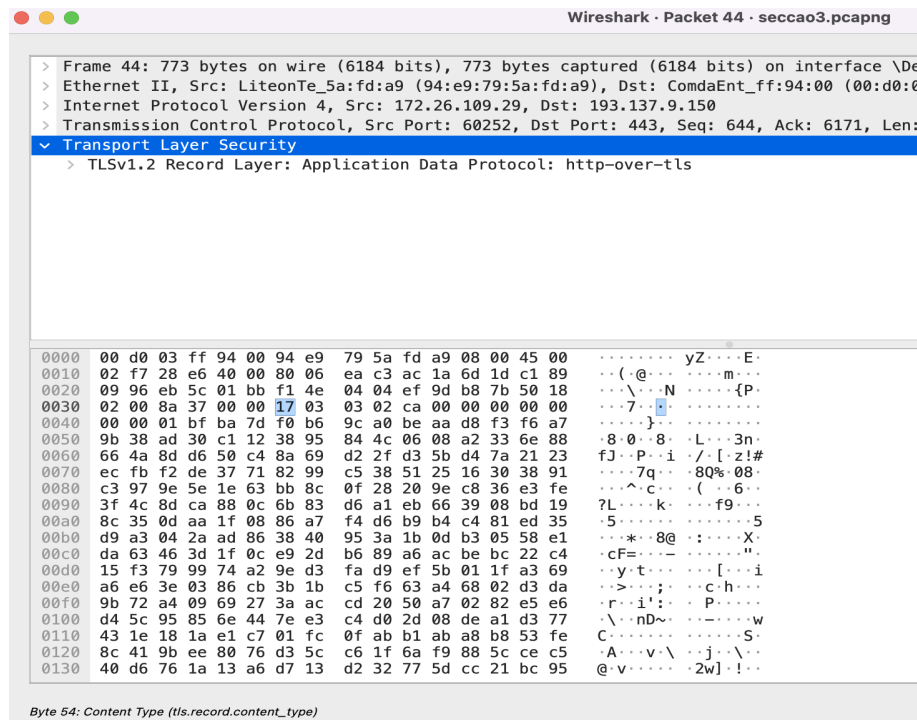


Figura 4: Primeiro byte referente ao TLS - byte 54

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
48	3.485269	193.137.9.150	172.26.109.29	TLSv1.2	910	Application Data
Frame 48: 910 bytes on wire (7280 bits), 910 bytes captured (7280 bits) on interface \Device\NPF_{6AD8C3E6-F113-495F-9065-B10E986452AA}, id 0						
Ethernet II, Src: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00), Dst: LiteonTe_5a:fd:a9 (94:e9:79:5a:fd:a9)						
Destination: LiteonTe_5a:fd:a9 (94:e9:79:5a:fd:a9)						
Source: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)						
Type: IPv4 (0x0800)						
Internet Protocol Version 4, Src: 193.137.9.150, Dst: 172.26.109.29						
Transmission Control Protocol, Src Port: 443, Dst Port: 60252, Seq: 6171, Ack: 1363, Len: 856						
Transport Layer Security						

Figura 5: Captura da Frame 48, relativa à mensagem que contém o primeiro byte da resposta HTTP proveniente do servidor

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

Como pode ser visto na imagem acima, o endereço Ethernet da fonte é **00:d0:03:ff:94:00**, que corresponde ao mesmo *router* citado na **questão 2**.

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

Como pode ser visto na imagem acima, o endereço MAC de destino é **94:e9:79:5a:fd:a9**, que corresponde ao mesmo portátil mostrado na figura 2.

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

Como pode ser visto na Figura 4 e, analogamente ao que já foi explicado na questão 3, o protocolo da *network layer* encapsulado na trama Ethernet é o protocolo IPv4. Porém, indo mais a fundo, ao analisarmos o cabeçalho do datagrama IP vemos que o campo Protocol contém o valor **0x6** que indica que o protocolo encapsulado dentro do pacote IP é por sua vez o protocolo TCP.

```
No.      Time      Source      Destination      Protocol Length Info
  48 3.485269    193.137.9.150 172.26.109.29    TLSv1.2  910    Application Data
Frame 48: 910 bytes on wire (7280 bits), 910 bytes captured (7280 bits) on interface \Device\NPF_{6AD8C3E6-F113-495F-9065-B10E986452AA}, id 0
Ethernet II, Src: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00), Dst: LiteonTe_5a:fd:a9 (94:e9:79:5a:fd:a9)
Internet Protocol Version 4, Src: 193.137.9.150, Dst: 172.26.109.29
 0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 896
 Identification: 0x0137 (311)
 Flags: 0x40, Don't fragment
 ...0 0000 0000 0000 = Fragment Offset: 0
 Time to Live: 253
 Protocol: TCP (6)
 Header Checksum: 0x94e9 [validation disabled]
 [Header checksum status: Unverified]
 Source Address: 193.137.9.150
 Destination Address: 172.26.109.29
Transmission Control Protocol, Src Port: 443, Dst Port: 60252, Seq: 6171, Ack: 1363, Len: 856
Transport Layer Security
```

Figura 6: Protocolo encapsulado no IPv4

Há ainda o protocolo TLS que corre sobre o TCP (entre a *transport layer* e a *application layer*), como pode ser observado na figura 5.

### 3 Protocolo ARP

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

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

Interface: 192.168.56.1 --- 0x3
  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: 172.26.109.29 --- 0xb
  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
  239.255.102.18        01-00-5e-7f-66-12    static
  239.255.255.250       01-00-5e-7f-ff-fa    static
  255.255.255.255       ff-ff-ff-ff-ff-ff    static
```

Figura 7: Tabela ARP

A tabela ARP mantém uma correlação entre endereços MAC e endereços IP de interfaces de máquinas na rede. Na Figura 6 podemos ver na primeira coluna a listagem dos endereços IP e na segunda os endereços MAC correspondentes. Há ainda uma terceira coluna que indica se o tipo da entrada da tabela é dinâmica ou estática. No caso de ser **dinâmica** quer dizer que tal entrada na tabela foi obtida a partir de resoluções ARP concluídas com êxito (automáticas sem o interveniente de um administrador) e são entradas que ficam mantidas apenas por um período de tempo. Por outro lado o tipo **estático** corresponde a entradas adicionadas manualmente à tabela e são mantidas de forma permanente.

Procedimento efetuado para as questões 9 à 14:

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

Interface: 192.168.56.1 --- 0x3
  Internet Address      Physical Address      Type
  224.0.0.22            01-00-5e-00-00-16    static

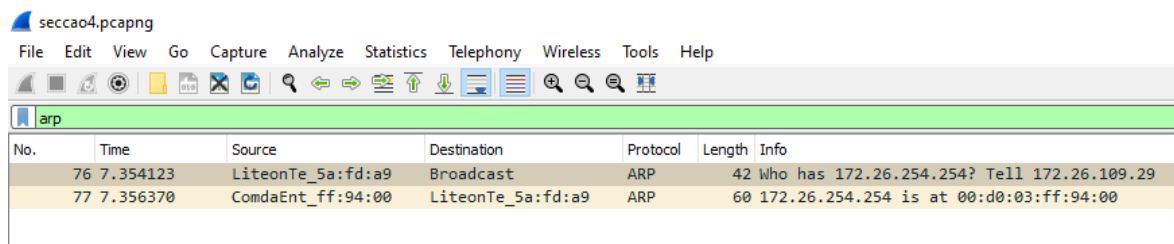
Interface: 172.26.109.29 --- 0xb
  Internet Address      Physical Address      Type
  224.0.0.22            01-00-5e-00-00-16    static

C:\WINDOWS\system32>
```

Figura 8: Nova tabela ARP depois de limpar a cache

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?





No.	Time	Source	Destination	Protocol	Length	Info
76	7.354123	LiteonTe_5a:fd:a9	Broadcast	ARP	42	Who has 172.26.254.254? Tell 172.26.109.29
77	7.356370	ComdaEnt_ff:94:00	LiteonTe_5a:fd:a9	ARP	60	172.26.254.254 is at 00:d0:03:ff:94:00

Figura 9: Frames relativas a aplicar o filtro - protocolo ARP

```

No.      Time      Source           Destination      Protocol Length Info
Frame 76: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{6AD8C3E6-F113-495F-9065-B10E986452AA}, id 0
Ethernet II, Src: LiteonTe_5a:fd:a9 (94:e9:79:5a:fd:a9), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  Source: LiteonTe_5a:fd:a9 (94:e9:79:5a:fd:a9)
  Type: ARP (0x0806)
Address Resolution Protocol (request)

```

Figura 10: Primeira Frame obtida através do filtro

A figura 9 mostra o filtro realizado para a seleção dos pacotes ARP capturados. O primeiro pacote (nº76) contém a mensagem com o *ARP Request*. O valor do endereço de origem é (LiteonTe\_5a:fd:a9) **94:e9:79:5a:fd:a9**, enquanto o endereço de destino na trama Ethernet é (Broadcast) **ff:ff:ff:ff:ff:ff**.

O endereço destino usado é justificado por conta da remoção da *cache* ARP realizada antes da captura. Assim, ao aceder <https://alunos.uminho.pt/PT>, a partir do serviço de resolução de nomes conseguimos obter o endereço IP destino porém não é conhecido o endereço MAC correspondente (justamente pela *cache* ter sido esvaziada). Desta maneira, para descobrir o endereço MAC pretendido, a nossa máquina envia uma solicitação ARP, utilizando o endereço IP conhecido como o endereço IP de destino e o endereço MAC de FF:FF:FF:FF:FF:FF - que corresponde a difusão (*broadcast*) Ethernet. Cada dispositivo no segmento receberá o pacote, mas somente a máquina com o IP destino responderá com o pacote de resposta ARP, listando seu endereço MAC [1].

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

O valor hexadecimal do campo tipo da trama Ethernet é **0x0806** que indica que o protocolo encapsulado no *payload* da trama Ethernet é 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.      Time          Source          Destination      Protocol Length Info
 76 7.354123      LiteonTe_5a:fd:a9  Broadcast        ARP           42    Who has 172.26.254.254? Tell 172.26.109.29
Frame 76: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{6AD8C3E6-F113-495F-9065-B10E986452AA},
id 0
Ethernet II, Src: LiteonTe_5a:fd:a9 (94:e9:79:5a:fd:a9), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: LiteonTe_5a:fd:a9 (94:e9:79:5a:fd:a9)
  Sender IP address: 172.26.109.29
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 172.26.254.254
```

Figura 11: Frame 76 - Pedido ARP

Podemos concluir que se trata efetivamente de um *ARP Request* porque o campo Opcode da mensagem ARP possui o valor 1, que indica ser uma mensagem do tipo *request*.

Os tipos de endereços que estão contidos na mensagem ARP são endereços IP e endereços MAC (da máquina de origem e máquina destino):

- Sender MAC address : (LiteonTe\_5a:fd:a9) 94:e9:79:5a:fd:a9
- Sender IP address: 172.26.109.29
- Target MAC address: 00:00:00:00:00:00
- Target IP address: 172.26.254.254

Os dados mostrados podem ser verificados na figura 11. Podemos concluir que o *sender*, nossa máquina, está tentando encontrar o endereço MAC de um determinado *host* cujo endereço IP é o *Target IP address*, justamente pelo facto do *Target MAC address* estar à zero. Este resultado vai de encontro com o facto da *cache* ARP estar vazia.

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

Como pode ser visto na Figura 8, o tipo de pergunta feita *host* de origem é "*Who has 172.26.254.254?*". Como já foi explicado na questão 9, como a máquina origem possui a *cache* ARP vazia, é preciso realizar uma resolução ARP para a obtenção do endereço MAC pretendido. Neste caso, a pergunta mostrada é difundida na rede para todos os *hosts*, mas apenas o *host* com o *Target IP address* solicitado responderá com o seu endereço MAC para a máquina origem de volta.

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

A mensagem ARP que é a resposta ao pedido ARP é o pacote nº77 mostrado na figura 9. Ao expandi-lo encontramos as seguintes informações:

```
No.      Time          Source           Destination      Protocol Length Info
  77 7.356370 ComdaEnt_ff:94:00 LiteonTe_5a:fd:a9 ARP          60      172.26.254.254 is at 00:d0:03:ff:94:00
Frame 77: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{6AD8C3E6-F113-495F-9065-B10E986452AA}, id 0
Ethernet II, Src: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00), Dst: LiteonTe_5a:fd:a9 (94:e9:79:5a:fd:a9)
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: LiteonTe_5a:fd:a9 (94:e9:79:5a:fd:a9)
  Target IP address: 172.26.109.29
```

Figura 12: Mensagem ARP expandida

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

O valor do campo ARP *opcode* 2, o que especifica que a mensagem ARP é uma ARP *reply*.

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

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

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.

Para a resolução precisa desta resposta, optou-se por concretizar a experiência proposta num cenário simulado no CORE. O cenário criado engloba dois *hosts* em subredes distintas, conectados diretamente a um mesmo *router*:



Figura 13: Topologia criada

Como as tabelas ARP se encontram inicialmente vazias e, como o *ping* a ser efetuado pelo *host* A tem como destino um *host* noutra subrede, então inicialmente é feito um *ARP request* para o *host* A identificar o *router* para reencaminhar o *ping request* para o devido destino. Uma vez recebido o *ARP request* vindo do *host* A, o *router* pode salvar na *cache* ARP o endereço MAC do *host* A para futuramente, quando tiver que mandar de volta o *ping reply* já saber o endereço MAC do *host* A, evitando a repetição da resolução ARP.

Após receber o *ping request*, o *router* deve reencaminhá-lo para o *host* B, e para isso, executa uma resolução ARP (*broadcast*) para a subrede do *host* B. O *host* B recebe este *ARP request*, salva em *cache* o endereço MAC do *router* (analogamente ao que já foi explicado anteriormente) e responde o *router* com o *ARP reply*. O *router* de seguida encaminha o *ping* para o destino final e o *host* B responde com *ping reply* ao *router*, que de seguida reencaminhará o *ping reply* para o *host* A. Repare-se que não foram executadas resoluções ARP nesta fase justamente pelos dados em *cache* permitirem o conhecimento dos endereços MAC.

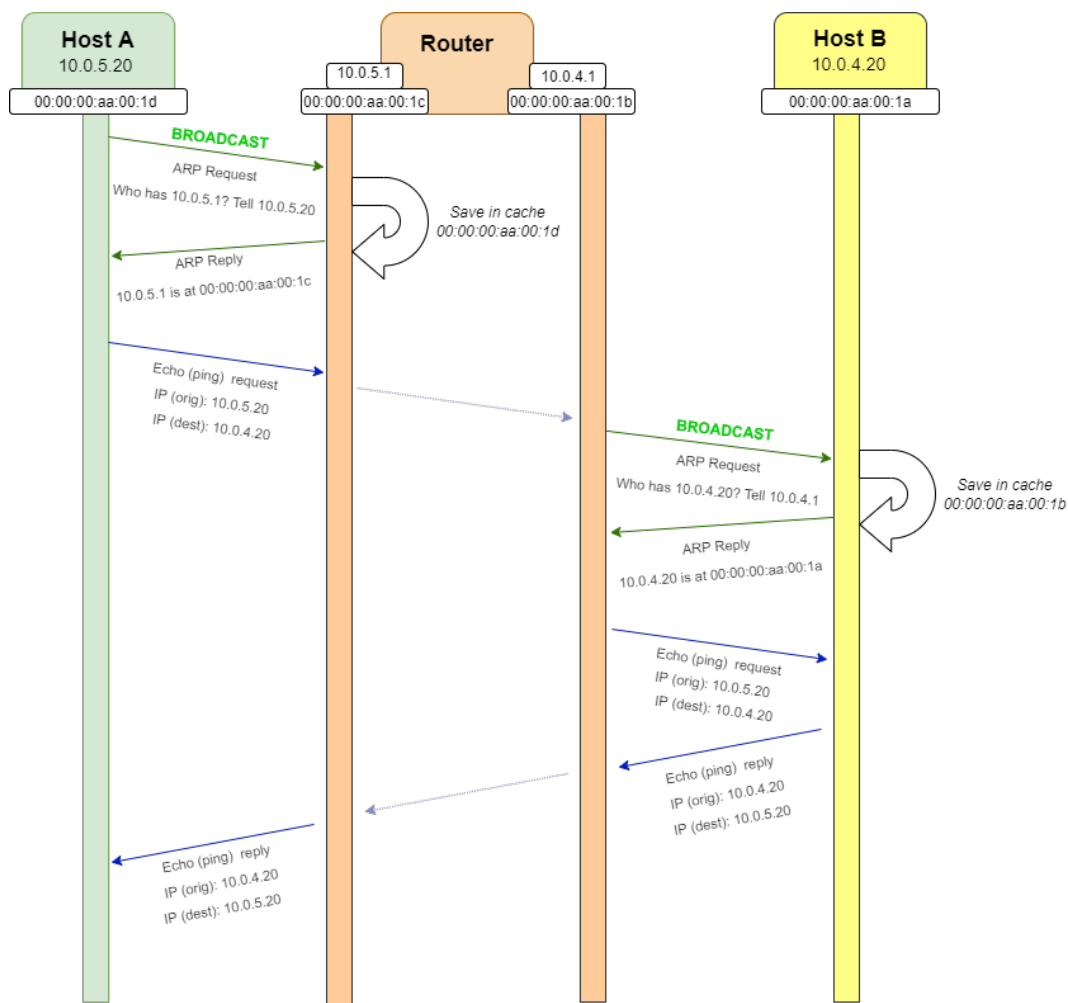


Figura 14: Diagrama temporal *ping*



Tal como observado anteriormente, com a utilização de hubs há um aumento do tráfego que flui na rede, o que diretamente aumenta a possibilidade de colisão dos pacotes enviados na rede, congestionando a mesma.

No contexto de switches, tal não aconteceria, ou seja, previne-se bastantes possíveis momentos de colisão de pacotes.

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

De forma a construir a tabela de comutação referente ao *switch* do Departamento B, atribuímos 1 à porta referente ao portátil Jasmine, 2 à porta referente ao Servidor B, 3 à porta referente ao portátil Alladin e por fim 4 à porta referente ao Router B.

Porta	Endereço MAC
1	00:00:00:aa:00:09
2	00:00:00:aa:00:08
3	00:00:00:aa:00:0a
4	00:00:00:aa:00:0b

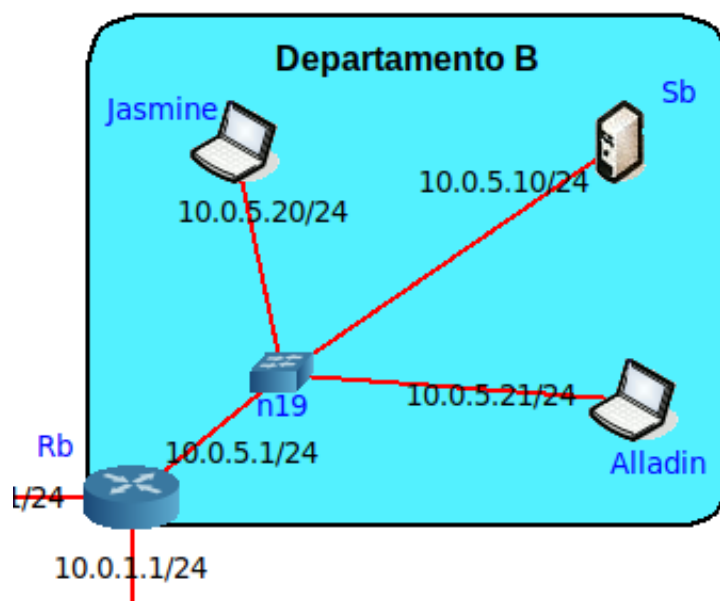


Figura 17: Topologia do Departamento B

## 5 Conclusão

Com este trabalho acreditamos ter aprofundado o conhecimento sobre os protocolos ARP e Ethernet. As experiências realizadas contribuíram na aplicação do conteúdo teórico lecionado nas aulas.

A decisão tomada na questão 14 de criar o próprio cenário mediante as condições do enunciado ajudou-nos a ter um melhor controlo de todos os processos efetuados na troca de pacotes capturados. Com isso, conseguimos confirmar a teoria com dados obtidos no Wireshark.

## Referências

- [1] study-ccna, *ARP (Address Resolution Protocol) explained*, <https://study-ccna.com/arp/#:~:text=ARP>