

UNIVERSIDADE DO MINHO  
DEPARTAMENTO DE INFORMÁTICA

TP3:Ethernet e ARP  
Grupo N<sup>o</sup> 51

Bruno Carvalho (A89476)

João Correia (A84414)

Rúben Cerqueira (A89593)

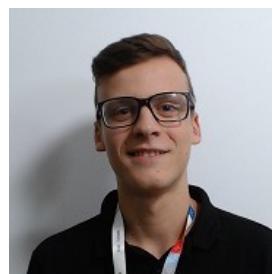
9 de dezembro de 2020



Bruno



João



Rúben

# Conteúdo

<b>1</b>	<b>Captura e análise de tramas Ethernet</b>	<b>3</b>
1.1	Exercício 1 . . . . .	3
1.2	Exercício 2 . . . . .	3
1.3	Exercício 3 . . . . .	3
1.4	Exercício 4 . . . . .	4
1.5	Exercício 5 . . . . .	4
1.6	Exercício 6 . . . . .	4
1.7	Exercício 7 . . . . .	5
1.8	Exercício 8 . . . . .	5
<b>2</b>	<b>Protocolo ARP</b>	<b>6</b>
2.1	Exercício 9 . . . . .	6
2.2	Exercício 10 . . . . .	6
2.3	Exercício 11 . . . . .	7
2.4	Exercício 12 . . . . .	7
2.5	Exercício 13 . . . . .	8
2.6	Exercício 14 . . . . .	8
<b>3</b>	<b>ARP Gratuito</b>	<b>10</b>
3.1	Exercício 15 . . . . .	10
<b>4</b>	<b>Domínios de Colisão</b>	<b>12</b>
4.1	Exercício 16 . . . . .	12
<b>5</b>	<b>Conclusão</b>	<b>14</b>

# Capítulo 1

## Captura e análise de tramas Ethernet

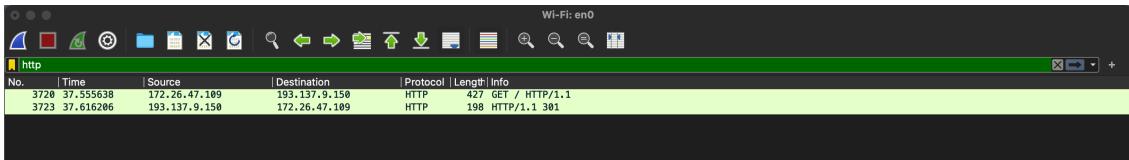


Figura 1.1: Endereços MAC

### 1.1 Exercício 1

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

```
> Frame 3720: 427 bytes on wire (3416 bits), 427 bytes captured (3416 bits) on interface en0, id 0
  ✓ Ethernet II, Src: Apple_d1:29:eb (38:f9:d3:d1:29:eb), Dst: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
    > Destination: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
    > Source: Apple_d1:29:eb (38:f9:d3:d1:29:eb)
      Type: IPv4 (0x0800)
  > Internet Protocol Version 4, Src: 172.26.47.109, Dst: 193.137.9.150
  > Transmission Control Protocol, Src Port: 50385, Dst Port: 80, Seq: 1, Ack: 1, Len: 361
  > Hypertext Transfer Protocol
```

Figura 1.2: Packets HTTP capturados

Como indicado na figura 1.2, o endereço MAC de origem é 38:f9:d3:d1:29:eb e o destino é 00:d0:03:ff:94:00.

### 1.2 Exercício 2

**Identifique a que sistemas se referem. Justifique.**

O endereço no campo *Source* refere-se à interface da máquina nativa, o endereço no campo *Destination* é referente à interface do router da rede local a que a máquina nativa está ligada.

### 1.3 Exercício 3

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

Como indicado na figura 1.2, o campo Type tem o valor **0x0800**, indicando que se trata do protocolo IPv4.

## 1.4 Exercício 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.

0000	00	d0	03	ff	94	00	38	f9	d3	d1	29	eb	08	00	45	00	.....8.....E
0010	01	9d	00	00	40	00	40	06	92	b4	ac	1a	2f	6d	c1	89	....@@..../m...
0020	09	96	c4	d1	00	50	f1	df	aa	2e	75	6c	de	9e	80	18	....P... .ul....
0030	08	02	ab	8b	00	00	01	01	08	0a	13	dd	50	7c	b3	0c	.....P ..
0040	f2	cd	47	45	54	20	2f	20	48	54	54	50	2f	31	2e	31	..[GET] / HTTP/1.1
0050	0d	0a	48	6f	73	74	3a	20	65	6c	65	61	72	6e	69	6e	..Host: elearnin
0060	67	2e	75	6d	69	6e	68	6f	2e	70	74	0d	0a	55	70	67	g.uminho.pt..Upg
0070	72	61	64	65	2d	49	6e	73	65	63	75	72	65	2d	52	65	rade-Ins ecure-Re
0080	71	75	65	73	74	73	3a	20	31	0d	0a	41	63	63	65	70	quests: 1..Accep
0090	74	3a	20	74	65	78	74	2f	68	74	6d	6c	2c	61	70	70	t: text/ html,app
00a0	6c	69	63	61	74	69	6f	6e	2f	78	68	74	6d	6c	2b	78	lication /xhtml+x
00b0	6d	6c	2c	61	70	70	6c	69	63	61	74	69	6f	6e	2f	78	ml,appli cation/x
00c0	6d	6c	3b	71	3d	30	2e	39	2c	2a	2f	2a	3b	71	3d	30	ml;q=0.9 ,/*/*;q=0
00d0	2e	38	0d	0a	55	73	65	72	2d	41	67	65	6e	74	3a	20	.8..User-Agent:
00e0	4d	6f	7a	69	6c	6c	61	2f	35	2e	30	20	28	4d	61	63	Mozilla/ 5.0 (Mac
00f0	69	6e	74	6f	73	68	3b	20	49	6e	74	65	6c	20	4d	61	intosh; Intel Ma
0100	63	20	4f	53	20	58	20	31	30	5f	31	35	5f	36	29	20	c OS X 1 0_15_6)
0110	41	70	70	6c	65	57	65	62	4b	69	74	2f	36	30	35	2e	AppleWeb Kit/605.
0120	31	2e	31	35	20	28	4b	48	54	4d	4c	2c	20	6c	69	6b	1.15 (KH TML, lik
0130	65	20	47	65	63	6b	6f	29	20	56	65	72	73	69	6f	6e	e Gecko) Version
0140	2f	31	34	2e	30	2e	31	20	53	61	66	61	72	69	2f	36	/14.0.1 Safari/6
0150	30	35	2e	31	2e	31	35	0d	0a	41	63	63	65	70	74	2d	05.1.15..Accept-
0160	4c	61	6e	67	75	61	67	65	3a	20	65	6e	2d	67	62	0d	Language : en-gb.

Figura 1.3: Trama do pedido GET

Observando a figura 1.3, os valores hexadecimais de dos pares de bytes encontram-se agrupados em blocos de 8, perfazendo 66 bytes até ao carácter ASCII “G”.

A trama tem um comprimento total de 427 bytes, o que se concretiza numa sobrecarga de  $(66/427)*100 = 15.46\%$ .

## 1.5 Exercício 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)).

Na observação da trama, o grupo reparou na ausência do campo FCS. Este comportamento deve-se ao facto de atualmente as redes ethernet serem bastante mais robustas e a chance de serem propagados packets com *checksums* incorretos, assim como a de a **Network Interface Card (NIC)** as capturar.

## 1.6 Exercício 6

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

```

> Frame 3723: 198 bytes on wire (1584 bits), 198 bytes captured (1584 bits) on interface en0, id 0
└ Ethernet II, Src: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00), Dst: Apple_d1:29:eb (38:f9:d3:d1:29:eb)
  > Destination: Apple_d1:29:eb (38:f9:d3:d1:29:eb)
  > Source: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
    Type: IPv4 (0x0800)
  > Internet Protocol Version 4, Src: 193.137.9.150, Dst: 172.26.47.109
  > Transmission Control Protocol, Src Port: 80, Dst Port: 50385, Seq: 1, Ack: 362, Len: 132
  > Hypertext Transfer Protocol

0000  38 f9 d3 d1 29 eb 00 00  03 ff 94 00 08 00 45 00  8·... ).... ····E·
0010  00 b8 68 8f 40 00 7e 06  ed 09 c1 89 09 96 ac 1a  ··h @~ ····
0020  2f 6d 00 50 c4 d1 75 6c  de 9e f1 df ab 97 80 18  /m·P·ul ····
0030  04 01 d1 f9 00 00 01 01  08 0a b3 0c f3 06 13 dd  ···· ····
0040  50 7c 48 54 54 50 2f 31  2e 31 20 33 30 31 20 0d  P|HTTP/1 .1 301 ·
0050  0a 4c 6f 63 61 74 69 6f  6e 3a 20 68 74 74 70 73  ·Location: https
0060  3a 2f 2f 65 6c 65 61 72  6e 69 6e 67 2e 75 6d 69  ://clearning.umi
0070  6e 68 6f 2e 70 74 2f 0d  0a 43 6f 6e 74 65 6e 74  nho.pt/. ·Content
0080  2d 4c 65 6e 67 74 68 3a  20 30 0d 0a 44 61 74 65  -Length: 0 ·Date
0090  3a 20 57 65 64 2c 20 32  35 20 4e 6f 76 20 32 30  : Wed, 2 5 Nov 20
00a0  32 30 20 30 39 3a 31 32  3a 31 32 20 47 4d 54 0d  20 09:12 :12 GMT
00b0  0a 43 6f 6e 6e 65 63 74  69 6f 6e 3a 20 63 6c 6f  ·Connect ion: clo
00c0  73 65 0d 0a 0d 0a  ····

```

Figura 1.4: Trama Ethernet captada

Observando a figura 1.4, o campo *Source*, indicativo do endereço Ethernet da fonte é 00:d0:03:ff:94:00, correspondente ao router da rede local.

## 1.7 Exercício 7

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

Observando novamente a imagem relativa ao exercício anteriores, o campo *Destination* tem o valor 38:f9:d3:d1:29:eb, correspondente à interface ativa da máquina nativa.

## 1.8 Exercício 8

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

Na figura 1.4 observam-se os 4 protocolos contidos na trama: Ethernet II, Internet Protocol Verson 4 (*IPv4*), Transmission Control Protocol (*TCP*) e Hypertext Transfer Protocol (*HTML*).

## Capítulo 2

# Protocolo ARP

### 2.1 Exercício 9

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

```
Rubens-MacBook-Pro:~ ruben$ arp -a
? (172.26.47.109) at 38:f9:d3:d1:29:eb on en0 ifscope permanent [ethernet]
? (172.26.254.254) at 0:d0:3:ff:94:0 on en0 ifscope [ethernet]
? (172.26.255.255) at ff:ff:ff:ff:ff:ff on en0 ifscope [ethernet]
? (224.0.0.251) at 1:0:5e:0:0:fb on en0 ifscope permanent [ethernet]
? (239.255.255.250) at 1:0:5e:7f:ff:fa on en0 ifscope permanent [ethernet]
```

Figura 2.1: Tabela ARP

A tabela ARP será uma tabela de reencaminhamento que será preenchida de acordo com o histórico de comunicações da máquina nativa.

A primeira coluna apresenta o endereço IP do host, a segunda coluna (entre o *at* e o *on*) apresenta o endereço MAC para o qual enviar um pacote endereçado ao endereço da primeira coluna, sendo a última coluna referente à interface relativa ao envio do pacote.

### 2.2 Exercício 10

```
[Rubens-MacBook-Pro:~ ruben$ ping 172.26.46.5
PING 172.26.46.5 (172.26.46.5): 56 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
Request timeout for icmp_seq 2
Request timeout for icmp_seq 3
^C
--- 172.26.46.5 ping statistics ---
5 packets transmitted, 0 packets received, 100.0% packet loss
Rubens-MacBook-Pro:~ ruben$ ]
```

Figura 2.2: Tentativa de Ping

Como é possível observar na Figura 2.2 não foi possível fazer um ping para um host da sala de aula de outro grupo uma vez que a rede **eduroam** não permite tal comunicação.

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?

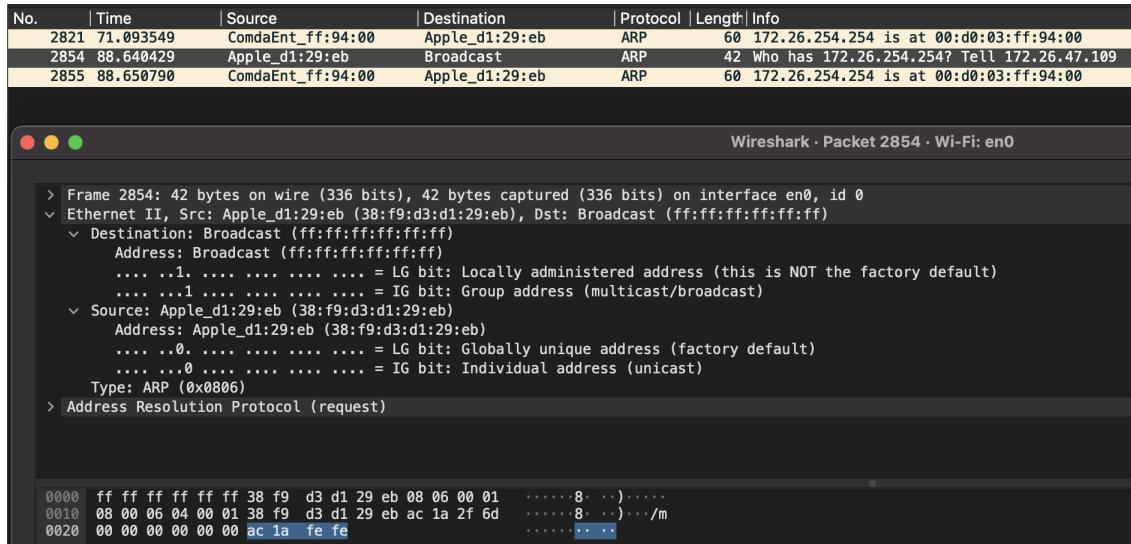


Figura 2.3: Pedido ARP

Observando a figura 2.3 conclui-se que o endereço de origem da trama é 38:f9:d3:d1:29:eb e de destino é ff:ff:ff:ff:ff:ff.

Visto que a tabela de endereçamento da qual proveio este pacote ainda não tinha uma entrada para o endereço MAC correspondente ao endereço IP ao qual o pacote era destinado, o pacote foi enviado a todos os host ligados à origem de trama.

O host com o IP correto deverá responder com o seu endereço MAC.

## 2.3 Exercício 11

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

Através do análise da Figura 2.3 conclui-se que o campo tipo da trama em hexadecimal será 0x0806 que corresponde ao tipo ARP.

## 2.4 Exercício 12

Como pode confirmar que se trata efetivamente de um pedido ARP? Identifique que tipo de endereços estão contidos na mensagem ARP? Que conclui? (Se necessário, consulte a RFC do protocolo ARP <http://tools.ietf.org/html/rfc826.html>.).

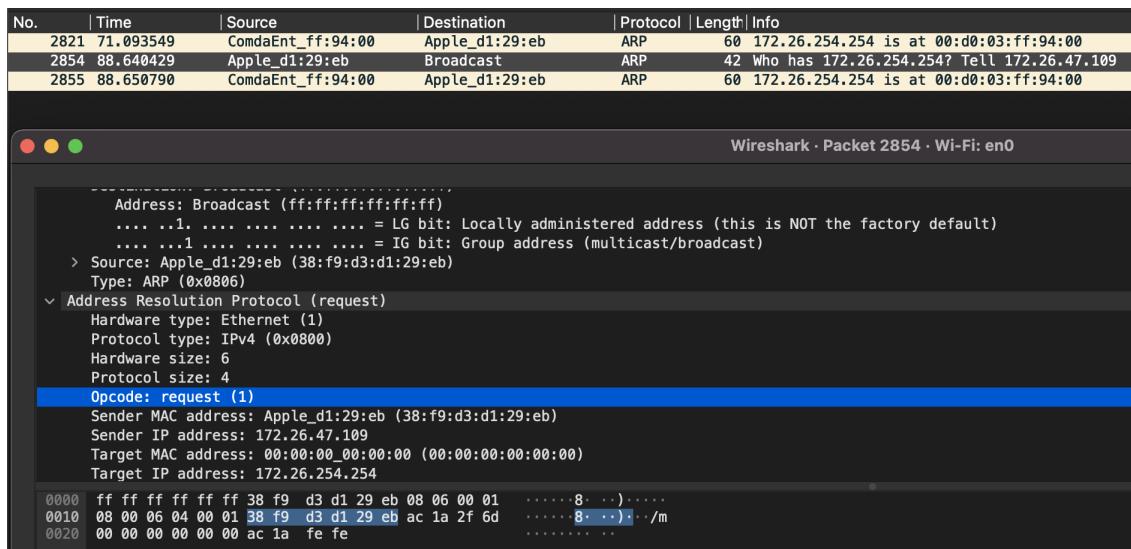


Figura 2.4: Campo opcode ARP Request

Para se saber se um dado pacote se trata de um ARP Request necessitamos de recorrer ao opcode que retrata esse tipo. Através da Figura 2.4 observamos que o opcode tem como valor 1, qualificando o pacote como ARP Request. Se o valor fosse 2, aí seria um ARP Reply. Na mensagem ARP terá endereços do tipo IP e MAC, tanto de origem como de destino.

## 2.5 Exercício 13

**Explicita que tipo de pedido ou pergunta é feito pelo host de origem?**

A máquina nativa faz a seguinte pergunta "Quem tem 172.26.254.254? Diga a 172.26.47.109". Ou seja, o que está a acontecer é que a nossa máquina pergunta a todos os hosts da rede pelo determinado IP. Se um desses hosts tiver esse IP, pede para que este envie uma resposta para o IP da nossa máquina. Com isto, obteremos o endereço MAC do host que enviará a resposta pretendida.

## 2.6 Exercício 14

**Localize a mensagem ARP que é a resposta ao pedido ARP efectuado.**

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

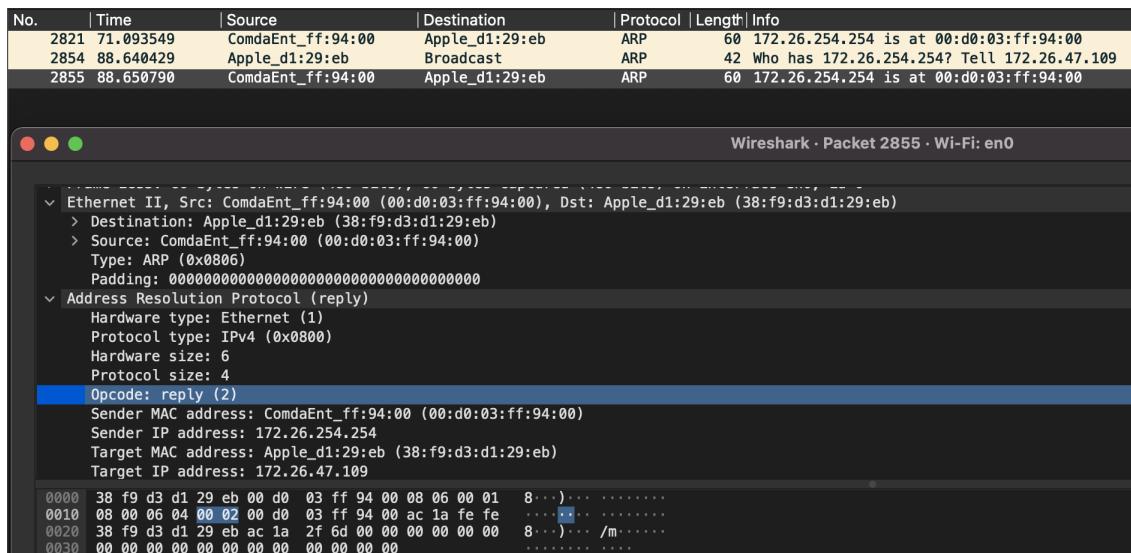


Figura 2.5: campo ARP opcode

Pode-se observar na Figura 2.5 que o valor do campo ARP opcode é 2, o que quer dizer que se trata de um ARP Reply. Este seguiu-se do ARP Request realizado anteriormente.

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

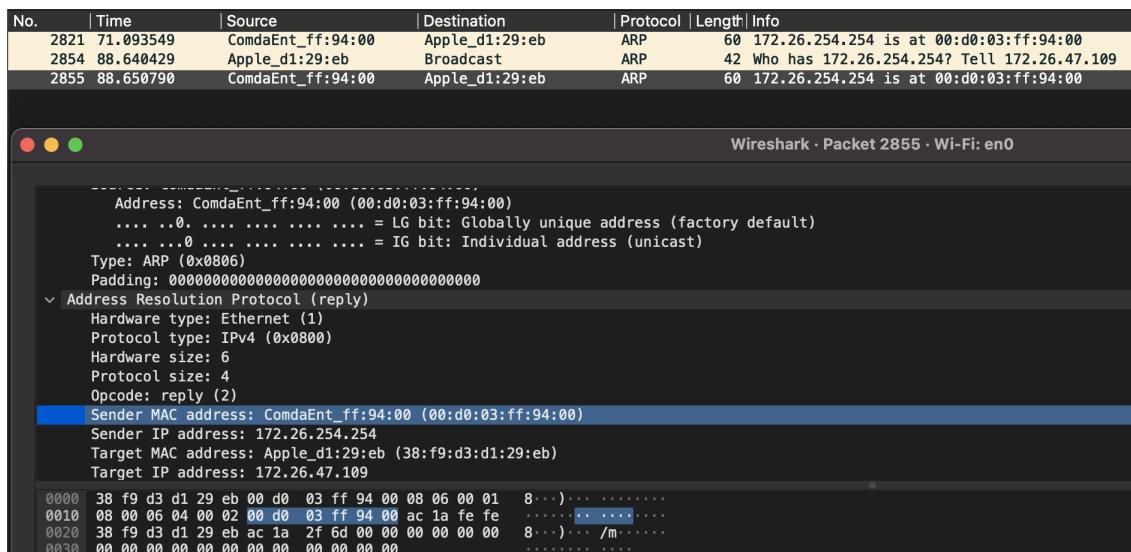


Figura 2.6: pedido ARP

É possível analisar na Figura 2.6 que a resposta ao pedido ARP se encontra entre o byte 22 e o byte 29 da trama.

# Capítulo 3

## ARP Gratuito

### 3.1 Exercício 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 enviado?

No.	Time	Source	Destination	Protocol	Length	Info
5	0.849013	Apple_d1:29:eb	ComdaEnt_ff:94:00	ARP	42	Who has 172.26.254.254? Tell 172.26.47.109
10	0.870243	Apple_d1:29:eb	ComdaEnt_ff:94:00	ARP	42	Who has 172.26.254.254? Tell 172.26.47.109
15	0.912482	Apple_d1:29:eb	ComdaEnt_ff:94:00	ARP	42	Who has 172.26.254.254? Tell 172.26.47.109
16	0.993500	Apple_d1:29:eb	ComdaEnt_ff:94:00	ARP	42	Who has 172.26.254.254? Tell 172.26.47.109
21	1.158281	Apple_d1:29:eb	ComdaEnt_ff:94:00	ARP	42	Who has 172.26.254.254? Tell 172.26.47.109
24	1.481515	Apple_d1:29:eb	ComdaEnt_ff:94:00	ARP	42	Who has 172.26.254.254? Tell 172.26.47.109
37	2.609955	Apple_d1:29:eb	ComdaEnt_ff:94:00	ARP	42	Who has 172.26.254.254? Tell 172.26.47.109
39	2.633648	Apple_d1:29:eb	ComdaEnt_ff:94:00	ARP	42	Who has 172.26.254.254? Tell 172.26.47.109
40	2.674540	Apple_d1:29:eb	ComdaEnt_ff:94:00	ARP	42	Who has 172.26.254.254? Tell 172.26.47.109
41	2.756060	Apple_d1:29:eb	ComdaEnt_ff:94:00	ARP	42	Who has 172.26.254.254? Tell 172.26.47.109
42	2.918752	Apple_d1:29:eb	ComdaEnt_ff:94:00	ARP	42	Who has 172.26.254.254? Tell 172.26.47.109
62	6.427192	Apple_d1:29:eb	ComdaEnt_ff:94:00	ARP	42	Who has 172.26.254.254? Tell 172.26.47.109
68	6.448800	Apple_d1:29:eb	ComdaEnt_ff:94:00	ARP	42	Who has 172.26.254.254? Tell 172.26.47.109
71	6.490871	Apple_d1:29:eb	ComdaEnt_ff:94:00	ARP	42	Who has 172.26.254.254? Tell 172.26.47.109
72	6.494976	Apple_d1:29:eb	ComdaEnt_ff:94:00	ARP	42	Who has 172.26.254.254? Tell 172.26.47.109
75	6.516055	Apple_d1:29:eb	ComdaEnt_ff:94:00	ARP	42	Who has 172.26.254.254? Tell 172.26.47.109
76	6.556363	Apple_d1:29:eb	ComdaEnt_ff:94:00	ARP	42	Who has 172.26.254.254? Tell 172.26.47.109
77	6.636575	Apple_d1:29:eb	ComdaEnt_ff:94:00	ARP	42	Who has 172.26.254.254? Tell 172.26.47.109
80	6.799051	Apple_d1:29:eb	ComdaEnt_ff:94:00	ARP	42	Who has 172.26.254.254? Tell 172.26.47.109
81	6.807971	ComdaEnt_ff:94:00	Apple_d1:29:eb	ARP	60	172.26.254.254 is at 00:d0:03:ff:94:00
82	6.808667	Apple_d1:29:eb	Broadcast	ARP	42	ARP Announcement for 172.26.47.109
87	6.900589	Apple_d1:29:eb	Broadcast	ARP	42	Who has 172.26.254.254? Tell 172.26.47.109

Figura 3.1: Pacote de pedido ARP gratuito

Com a análise da 3.1 conclui-se que existem duas diferenças importantes que é importante ter em conta que são a flag *is gratuitous* e o campo do endereço de destino. Como podemos ver, esta pacote será um pedido ARP gratuito pois a flag *Is gratuitous* está a true. Além disso podemos

observar que o endereço MAC de destino é 00:00:00:00:00:00 e o endereço IP de destino é igual ao endereço IP da fonte. Com isto conclui-se que o pacote não espera por uma resposta, consistindo num ARP gratuito, cujo objetivo é dar a conhecer aos outros hosts os endereços MAC do host que enviou o pedido.

# Capítulo 4

## Domínios de Colisão

### 4.1 Exercício 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?

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.

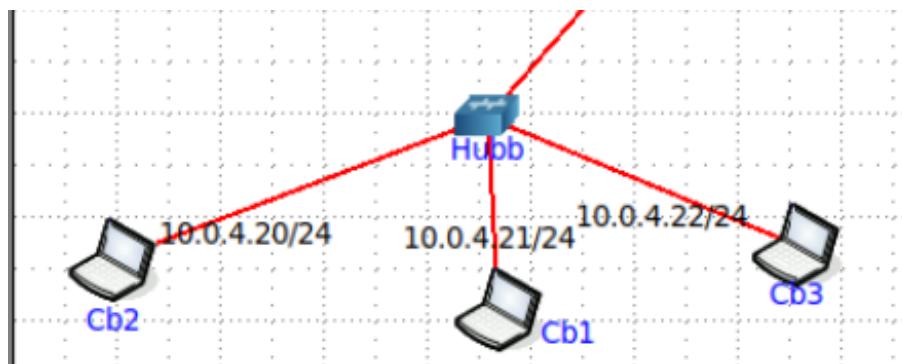


Figura 4.1: Topologia Proposta

De forma a poder comparar o funcionamento dos *switches* e dos *hubs*, foi necessário adicionar um terceiro computador no **departamento B**, ficando a topologia a utilizar com a configuração representada na figura 4.1.

No departamento B, onde foi utilizado um **hub** (LAN partilhada) executou-se o comando `ping` do computador CB2 para o computador CB3, estando o computador CB1 a correr o comando `tcpdump`. Como observado na figura 4.3, tanto o Cb3 como o Cb1 receberam os pacotes enviados por Cb2.

Isto deve-se ao funcionamento dos *hubs* Ethernet, em que qualquer pacote recebido numa porta é distribuído em todas as portas, o que, neste caso, resultou na redistribuição dos pacotes enviados por Cb2 através tanto da porta a que Cb1 estava ligado como Cb3.

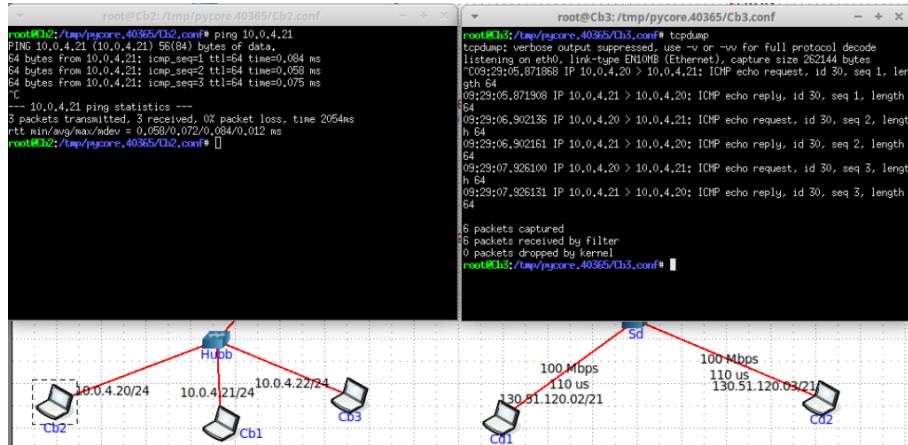


Figura 4.2: Ping de Cb2 para Cb3 com traceroute em Cb1

No departamento A, foi utilizado um **switch** (LAN comutada). Executou-se o comando *ping* do computador Ca1 para o servidor S1 , estando o computador Ca2 a correr o comando *tcpdump*. Como observado na figura 4.3, apenas o S1 recebe os pacotes enviados por Ca1, assim como apenas o Ca1 recebe a resposta enviada pelo servidor S1, estando o computador Ca2 ignorante do restante tráfego na subrede.

Este comportamento deve-se à utilização de um *switch* Ethernet, ao invés de um hub. Um switch envia o pacote apenas para o host indicado ao invés de o propagar a todos os dispositivos a ele ligados. Isto é possível pois são estabelecidos vários canais de comunicação.

Devido a este facto, que permite transmissões simultâneas, e em contraste com os *hubs*, onde não existem canais separados, os *switches* configuram-se como a melhor opção para reduzir o número de colisões, pois as colisões, quando elas existirem, serão restringidas a um domínio muito menor.

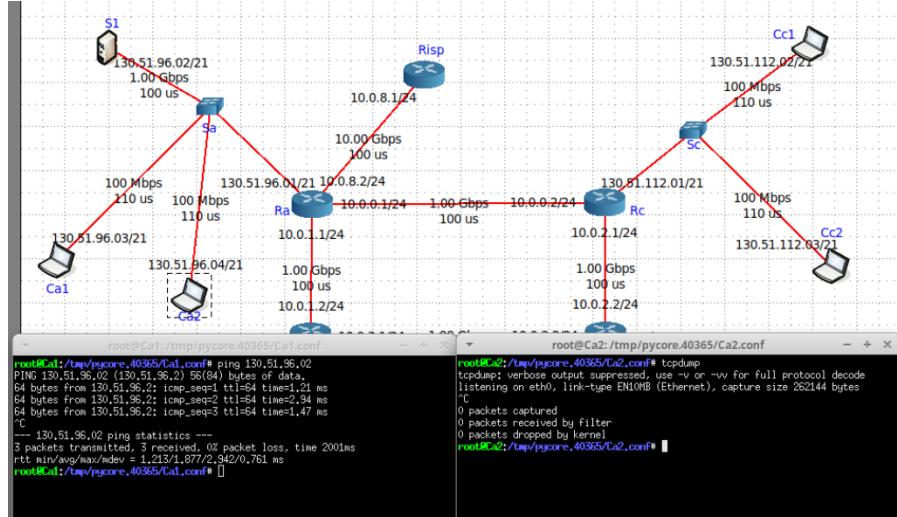


Figura 4.3: Ping de Ca2 para S1 com traceroute em Ca1

# Capítulo 5

## Conclusão

Este trabalho permitiu a exploração da temática «**Nível de Ligação Lógica: Ethernet e Protocolo ARP**

Dentro desta temática foram estudados conceitos associados a tramas Ethernet e ao seu endereçamento através de Endereços MAC e o protocolo de endereçamento ARP.

Para tal, e à semelhança do TP2, foi utilizado o Wireshark e a ferramenta de emulação CORE. A ferramenta CORE permitiu emular as topologias propostas e estudar a diferença entre switches e hubs Ethernet. O Wireshark permitiu captar pacotes e inspecionar a parte do seu conteúdo relevante ao protocolo Ethernet, observando endereços e outras informações necessárias.

Em conclusão, julgamos ter alcançado o aproveitamento desejável, o que permitiu aprofundar e consolidar o conhecimento nas várias componentes exploradas durante o projeto: Captura e análise de Tramas Ethernet, Protocolo ARP, ARP Gratuito e Domínios de colisão.