

UNIVERSIDADE DO MINHO

LICENCIATURA EM ENGENHARIA INFORMÁTICA

Redes de Computadores - RC  
Trabalho Prático 3

Bernardo Saraiva (A93189)  
José Gonçalves (A93204)  
Gonçalo Santos (A93279)

25/03/2022

# Conteúdo

<b>1</b>	<b>Captura e análise de Tramas Ethernet</b>	<b>4</b>
1.1	Anote os endereços MAC de origem e de destino da trama capturada. . . . .	5
1.2	Identifique a que sistemas se referem. Justifique. . . . .	5
1.3	Qual o valor hexadecimal do campo Type da trama Ethernet? O que significa? . .	5
1.4	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. . . . .	6
1.5	Qual é o endereço Ethernet da fonte? A que sistema de rede corresponde? Justifique.	8
1.6	Qual é o endereço MAC do destino? A que sistema corresponde? . . . . .	9
1.7	Atendendo ao conceito de desencapsulamento protocolar, identifique os vários protocolos contidos na trama recebida. . . . .	9
<b>2</b>	<b>Protocolo ARP</b>	<b>10</b>
2.1	8. Observe o conteúdo da tabela ARP. Diga o que significa cada uma das colunas.	10
2.2	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? . . . . .	11
2.3	10. Qual o valor hexadecimal do campo tipo da trama Ethernet? O que indica? . .	12
2.4	11. Como pode confirmar que se trata efetivamente de um pedido ARP? Identifique que tipo de endereços estão contidos na mensagem ARP? Que conclui? . . . . .	12
2.5	12. Explícite que tipo de pedido ou pergunta é feita pelo host de origem. . . . .	13
2.6	13. Localize a mensagem ARP que é a resposta ao pedido ARP efetuado. . . . .	14
2.6.1	a. Qual o valor do campo ARP opcode? O que especifica? . . . . .	14
2.6.2	b. Em que campo da mensagem ARP está a resposta ao pedido ARP? . . .	14

2.7	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
<b>3</b>	<b>5. Domínio de colisão</b>	<b>16</b>
3.1	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? . . . . .	16
3.2	16. Construa manualmente a tabela de comutação do switch do Departamento B, atribuindo números de porta à sua escolha. . . . .	16
<b>4</b>	<b>Conclusões</b>	<b>18</b>

# Capítulo 1

## Captura e análise de Tramas Ethernet

No	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	172.26.42.139	239.255.255.250	SSDP	214	M-SEARCH * HTTP/1.1
2	1.000685646	172.26.42.139	239.255.255.250	SSDP	214	M-SEARCH * HTTP/1.1
3	1.463794639	172.26.42.139	193.137.16.75	DNS	90	Standard query 0xadab AAAA elearning.uminho.pt OPT
4	1.467291295	193.137.16.75	172.26.42.139	DNS	144	Standard query response 0xadab AAAA elearning.uminho.pt SOA dns.uminho.pt OPT
5	1.468135383	172.26.42.139	193.137.9.150	TCP	74	48078 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=18180075 TSecr=0 WS=128
6	1.471579817	193.137.9.150	172.26.42.139	TCP	74	80 → 48078 [SYN, ACK] Seq=0 Ack=1 Win=12500 Len=0 MSS=1250 WS=4 SACK_PERM=1 TSval=1656896965 TSecr=1656896965
7	1.471863609	172.26.42.139	193.137.9.150	TCP	66	48078 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=18180078 TSecr=1656896965
8	1.482938435	172.26.42.139	193.137.16.75	DNS	95	Standard query 0xc862 A detectportal.firefox.com OPT
9	1.482917833	172.26.42.139	193.137.16.75	DNS	95	Standard query 0xc862 AAAA detectportal.firefox.com OPT
10	1.616199549	172.26.42.139	193.137.9.150	HTTP	407	GET / HTTP/1.1
11	1.612790484	193.137.16.75	172.26.42.139	DNS	206	Standard query response 0xc862 A detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAME
12	1.614609164	193.137.9.150	172.26.42.139	HTTP	198	HTTP/1.0 302 Moved Temporarily
13	1.614672969	172.26.42.139	193.137.9.150	TCP	66	48078 → 80 [ACK] Seq=342 Ack=133 Win=64128 Len=0 TSval=18180221 TSecr=1656897188
14	1.614747766	193.137.16.75	172.26.42.139	DNS	218	Standard query response 0xc862 AAAA detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAME
15	1.615537123	172.26.42.139	34.107.221.82	TCP	74	37512 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1933591629 TSecr=0 WS=128
16	1.628476265	34.107.221.82	172.26.42.139	TCP	74	80 → 37512 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1250 SACK_PERM=1 TSval=2354910912 TSecr=1933591629
17	1.628565615	172.26.42.139	34.107.221.82	TCP	66	37512 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1933591642 TSecr=2354910912
18	1.628832765	172.26.42.139	34.107.221.82	HTTP	357	GET /canonical.html HTTP/1.1
19	1.642082266	34.107.221.82	172.26.42.139	TCP	66	80 → 37512 [ACK] Seq=1 Ack=292 Win=66816 Len=0 TSval=2354910926 TSecr=1933591642
20	1.643241859	34.107.221.82	172.26.42.139	HTTP	366	HTTP/1.1 200 OK (text/html)
21	1.643290371	172.26.42.139	34.107.221.82	TCP	66	37512 → 80 [ACK] Seq=292 Ack=303 Win=64000 Len=0 TSval=1933591657 TSecr=2354910926
22	1.649462484	172.26.42.139	193.137.16.75	DNS	99	Standard query 0xec0f AAAA contile.services.mozilla.com OPT
23	1.650805879	193.137.16.75	172.26.42.139	DNS	180	Standard query response 0xec0f AAAA contile.services.mozilla.com SOA ns-679.awdns-20.net OPT
24	1.651508083	172.26.42.139	34.117.237.239	TCP	74	54686 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1758106112 TSecr=0 WS=128
25	1.665752264	34.117.237.239	172.26.42.139	TCP	74	443 → 54686 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1250 SACK_PERM=1 TSval=4488087781 TSecr=1758106112
26	1.665795648	172.26.42.139	34.117.237.239	TCP	66	54686 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1758196126 TSecr=4488087781
27	1.666603209	172.26.42.139	193.137.16.75	DNS	84	Standard query 0x5a1b AAAA ipv4only.arpa OPT
28	1.667912753	193.137.16.75	172.26.42.139	DNS	141	Standard query response 0x5a1b AAAA ipv4only.arpa SOA sns.dns.icann.org OPT
29	1.668404686	172.26.42.139	34.117.237.239	TLSv1.3	583	Client Hello
30	1.668585071	172.26.42.139	34.107.221.82	TCP	74	37514 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1933591682 TSecr=0 WS=128
31	1.671211386	172.26.42.139	193.137.16.75	DNS	108	Standard query 0xa41e A firefox.settings.services.mozilla.com OPT
32	1.671405744	172.26.42.139	193.137.16.75	DNS	108	Standard query 0xa400 AAAA firefox.settings.services.mozilla.com OPT
33	1.672789297	193.137.16.75	172.26.42.139	DNS	192	Standard query response 0xa400 AAAA firefox.settings.services.mozilla.com SOA ns-1627.awdns-11.co
34	1.682900478	34.117.237.239	172.26.42.139	TCP	66	443 → 54686 [ACK] Seq=1 Ack=518 Win=66816 Len=0 TSval=4488087798 TSecr=1758106129
35	1.683546974	34.107.221.82	172.26.42.139	TCP	74	80 → 37514 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1250 SACK_PERM=1 TSval=4230492942 TSecr=1933591682
36	1.683579497	172.26.42.139	34.107.221.82	TCP	66	37514 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1933591697 TSecr=4230492942
37	1.683724452	172.26.42.139	34.107.221.82	HTTP	359	GET /success.txt?tip4 HTTP/1.1
38	1.686647248	34.117.237.239	172.26.42.139	TLSv1.3	2542	Server Hello, Change Cipher Spec

Figura 1.1: Captura de tráfego após aceder elearning.uminho.pt

- Trama que transporta os primeiros dados aplicacionais enviados do cliente - 29
- Trama com a resposta proveniente do servidor que contém os dados correspondentes ao acesso web realizado pelo cliente - 38

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

```
▶ Frame 29: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface wlo1, id 0
▶ Ethernet II, Src: IntelCor_d6:0a:b0 (18:1d:ea:d6:0a:b0), Dst: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
  ▶ Destination: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
  ▶ Source: IntelCor_d6:0a:b0 (18:1d:ea:d6:0a:b0)
    Type: IPv4 (0x0800)
▶ Internet Protocol Version 4, Src: 172.26.42.139, Dst: 34.117.237.239
▶ Transmission Control Protocol, Src Port: 54686, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
▶ Transport Layer Security
```

Figura 1.2: Endereços MAC

Como é possível observar na figura 1.2 o endereço mac destino é 00:d0:03:ff:94:00 e o endereço origem é 18:1d:ea:d6:0a:b0.

## 1.2 Identifique a que sistemas se referem. Justifique.

Os endereços MAC anteriormente referidos presentes na Figura 1, são, respectivamente, o do host em que estamos a realizar o request e o do router local.

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

0000	00 d0 03 ff 94 00 18 1d ea d6 0a b0 08 00 45 00	.....E
0010	02 39 d8 a1 40 00 40 06 79 13 ac 1a 2a 8b 22 75	9..@. y...*"u
0020	ed ef d5 9e 01 bb f4 ad 1f 9b f9 88 18 15 80 18	.....
0030	01 f6 e9 35 00 00 01 01 08 0a 68 cb f1 a1 1a b5	...5...h...
0040	46 e5 16 03 01 02 00 01 00 01 fc 03 03 46 08 a4	F.....F..
0050	1a 06 b6 7f c3 82 47 66 82 c8 65 7f e9 e9 ad 71	.....Gf...e...q
0060	59 85 18 33 c2 8a 1f d7 ed 60 b9 e1 e8 20 a0 a8	Y..3.....
0070	4c 66 6c 22 a1 64 e6 2d 93 15 dd 42 c1 aa 93 40	Lfl"d-...B..@
0080	b1 0a 8f a7 da 9c 26 45 1c 09 69 22 03 eb 00 22	.....&E...i"...
0090	13 01 13 03 13 02 c0 2b c0 2f cc a9 cc a8 c0 2c	.....+ /.....,
00a0	c0 30 c0 0a c0 09 c0 13 c0 14 00 9c 00 9d 00 2f	0...../
00b0	00 35 01 00 01 91 00 00 00 21 00 1f 00 00 1c 63	5.....!.....c
00c0	6f 6e 74 69 6c 65 2e 73 65 72 76 69 63 65 73 2e	ontile.s ervices.
00d0	6d 6f 7a 69 6c 6c 61 2e 63 6f 6d 00 17 00 00 ff	mozilla. com.....
00e0	01 00 01 00 00 0a 00 0e 00 0c 00 1d 00 17 00 18	.....
00f0	00 19 01 00 01 01 00 0b 00 02 01 00 00 23 00 00	.....#..
0100	00 10 00 0e 00 0c 02 68 32 08 68 74 74 70 2f 31	.....h 2http/1
0110	2e 31 00 05 00 05 01 00 00 00 00 22 00 0a 00	.1....."
0120	08 04 03 05 03 06 03 02 03 00 33 00 6b 00 69 00	.....3.k.i.
0130	1d 00 20 37 90 9e 58 9d c6 2a e4 60 b4 a6 79 7a	.. 7..X..*...yz
0140	8a e8 87 56 fc e6 c8 c6 f5 f4 e4 d4 8c 87 26 1a	..V.....&
0150	77 b8 3c 00 17 00 41 04 cc f0 54 81 48 77 ac 27	w<...A...T.Hw.'
0160	72 a0 64 b4 fd b6 8e e9 0f 0f b5 1d 1f d7 7e d9	r.d.....~
0170	bc ee aa ad 23 b2 3b e8 da 4e ac fa 01 32 6b 14	...#;h N...2k.
0180	cc f3 8c 56 f1 ab a1 bb 01 c4 bd c8 ac fb 9a 35	..V.....5
0190	27 5a 3b db 0d 3e 98 a4 00 2b 00 05 04 03 04 03	'Z;...>...+
01a0	03 00 0d 00 18 00 16 04 03 05 03 06 03 08 04 08	.....

Figura 1.3: Valor Hexadecimal

O valor do type em hexadecimal é 0x0800, o que significa que o protocolo usado para transmitir a trama analisada é um protocolo IPv4.

## 1.4 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 29: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface wlo1, id 0																
▶ Ethernet II, Src: IntelCor_d6:0a:b0 (18:1d:ea:d6:0a:b0), Dst: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)																
▶ Internet Protocol Version 4, Src: 172.26.42.139, Dst: 34.117.237.239																
▶ Transmission Control Protocol, Src Port: 54686, Dst Port: 443, Seq: 1, Ack: 1, Len: 517																
▶ Transport Layer Security																

Figura 1.4: Tamanho overhead Ethernet

<ul style="list-style-type: none"> <li>Frame 29: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface wlo1, id 0</li> <li>Ethernet II, Src: IntelCor_d6:0a:b0 (18:1d:ea:d6:0a:b0), Dst: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)</li> <li>Internet Protocol Version 4, Src: 172.26.42.139, Dst: 34.117.237.239</li> <li>Transmission Control Protocol, Src Port: 54686, Dst Port: 443, Seq: 1, Ack: 1, Len: 517</li> <li>Transport Layer Security</li> </ul>			
0000	00 d0 03 ff 94 00 18 1d	ea d6 0a b0 08 00 45 00	.....E.
0010	02 39 d8 a1 40 00 40 06	79 13 ac 1a 2a 8b 22 75	..9..@..y...*"u
0020	ed ef d5 9e 01 bb f4 ad	1f 9b f9 88 18 15 80 18	.....
0030	01 f6 e9 35 00 00 01 01	08 0a 68 cb f1 a1 1a b5	..5.....h.....
0040	46 e5 16 03 01 02 00 01	00 01 fc 03 03 46 08 a4	F.....F..
0050	1a 06 b6 7f c3 82 47 66	82 c8 65 7f e9 e9 ad 71	.....Gf...e...q
0060	59 85 18 33 c2 8a 1f d7	ed 60 b9 e1 e8 20 a0 a8	Y..3.....
0070	4c 66 6c 22 a1 64 e6 2d	93 15 dd 42 c1 aa 93 40	Lfl"d..B...@
0080	b1 0a 8f a7 da 9c 26 45	1c 09 69 22 03 eb 00 22	.....&E...i"..."
0090	13 01 13 03 13 02 c0 2b	c0 2f cc a9 cc a8 c0 2c	.....+.../.....,
00a0	c0 30 c0 0a c0 09 c0 13	c0 14 00 9c 00 9d 00 2f	.0......./
00b0	00 35 01 00 01 91 00 00	00 21 00 1f 00 00 1c 63	.5.....!.....c
00c0	6f 6e 74 69 6c 65 2e 73	65 72 76 69 63 65 73 2e	ontile.s ervices.
00d0	6d 6f 7a 69 6c 6c 61 2e	63 6f 6d 00 17 00 00 ff	mozilla. com.....
00e0	01 00 01 00 00 0a 00 0e	00 0c 00 1d 00 17 00 18	.....
00f0	00 19 01 00 01 01 00 0b	00 02 01 00 00 23 00 00	.....#..
0100	00 10 00 0e 00 0c 02 68	32 08 68 74 74 70 2f 31	.....h 2 http/1
0110	2e 31 00 05 00 05 01 00	00 00 00 00 22 00 0a 00	.1.....".....
0120	08 04 03 05 03 06 03 02	03 00 33 00 6b 00 69 00	.....3.k.i.
0130	1d 00 20 37 90 9e 58 9d	c6 2a e4 60 b4 a6 79 7a	.. 7..X..*...yz
0140	8a e8 87 56 fc e6 c8 c6	f5 f4 e4 d4 8c 87 26 1a	...V.....&
0150	77 b8 3c 00 17 00 41 04	cc f0 54 81 48 77 ac 27	w<...A...T.Hw.'
0160	72 a0 64 b4 fd b6 8e e9	0f 0f b5 1d 1f d7 7e d9	r.d.....
0170	bc ee aa ad 23 b2 3b 68	da 4e ac fa 01 32 6b 14	...#.;h.N...2k.
0180	cc f3 8c 56 f1 ab a1 bb	01 c4 bd c8 ac fb 9a 35	...V.....5
0190	27 5a 3b db 0d 3e 98 a4	00 2b 00 05 04 03 04 03	'Z;->...+.....
01a0	03 00 0d 00 18 00 16 04	03 05 03 06 03 08 04 08	.....

Figura 1.5: Tamnho overhead IP

```

> Frame 29: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface wlo1, id 0
> Ethernet II, Src: IntelCor_d6:0a:b0 (18:1d:ea:d6:0a:b0), Dst: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
> Internet Protocol Version 4, Src: 172.26.42.139, Dst: 34.117.237.239
> Transmission Control Protocol, Src Port: 54686, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
> Transport Layer Security

0000  00 d0 03 ff 94 00 18 1d ea d6 0a b0 08 00 45 00 .....E
0010  02 39 d8 a1 40 00 40 06 79 13 ac 1a 2a 8b 22 75 -9-@- y...*"u
0020  ed ef d5 9e 01 bb f4 ad 1f 9b f9 88 18 15 80 18 .....
0030  01 f6 e9 35 00 00 01 01 08 0a 68 cb f1 a1 1a b5 ...5...h....
0040  46 e5 16 03 01 02 00 01 00 01 fc 03 03 46 08 a4 F.....F..
0050  1a 06 b6 7f c3 82 47 66 82 c8 65 7f e9 e9 ad 71 .....Gf...e...q
0060  59 85 18 33 c2 8a 1f d7 ed 60 b9 e1 e8 20 a0 a8 Y-3.....
0070  4c 66 6c 22 a1 64 e6 2d 93 15 dd 42 c1 aa 93 40 Lf!"-d-...B...@
0080  b1 0a 8f a7 da 9c 26 45 1c 09 69 22 03 eb 00 22 .....&E...i"...
0090  13 01 13 03 13 02 c0 2b c0 2f cc a9 cc a8 c0 2c .....+.../....,
00a0  c0 30 c0 0a c0 09 c0 13 c0 14 00 9c 00 9d 00 2f -0...../
00b0  00 35 01 00 01 91 00 00 00 21 00 1f 00 00 1c 63 -5.....!.....c
00c0  6f 6e 74 69 6c 65 2e 73 65 72 76 69 63 65 73 2e ontile.s ervices.
00d0  6d 6f 7a 69 6c 6c 61 2e 63 6f 6d 00 17 00 00 ff mozilla. com....
00e0  01 00 01 00 00 0a 00 0e 00 0c 00 1d 00 17 00 18 .....
00f0  00 19 01 00 01 01 00 0b 00 02 01 00 00 23 00 00 .....#..
0100  00 10 00 0e 00 0c 02 68 32 08 68 74 74 70 2f 31 .....h 2 http/1
0110  2e 31 00 05 00 05 01 00 00 00 00 00 22 00 0a 00 .1....."....
0120  08 04 03 05 03 06 03 02 03 00 33 00 6b 00 69 00 ...3:k.i
0130  1d 00 20 37 90 9e 58 9d c6 2a e4 60 b4 a6 79 7a ..7-X-...*...yz
0140  8a e8 87 56 fc e6 c8 c6 f5 f4 e4 d4 8c 87 26 1a ..V.....&
0150  77 b8 3c 00 17 00 41 04 cc f0 54 81 48 77 ac 27 w<-A-...T.Hw-'
0160  72 a0 64 b4 fd b6 8e e9 0f 0f b5 1d 1f d7 7e d9 r-d-...~...
0170  bc ee aa ad 23 b2 3b 68 da 4e ac fa 01 32 6b 14 ...#;h-N...2k
0180  cc f3 8c 56 f1 ab a1 bb 01 c4 bd c8 ac fb 9a 35 ..V.....5
0190  27 5a 3b db 0d 3e 98 a4 00 2b 00 05 04 03 04 03 'Z;...>...+.....
01a0  03 00 0d 00 18 00 16 04 03 05 03 06 03 08 04 08 .....

```

Figura 1.6: Tamnho overhead TCP

Como podemos verificar nas figuras 1.4, 1.5, 1.6 o cabeçalho possui 66 bytes ( $14(Ethernet) + 20(IP) + 32(TCP)$ ). Como toda a trama possui 583 bytes existe um overhead de  $66/583 * 100 = 11.32\%$

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

```

> Frame 38: 2542 bytes on wire (20336 bits), 2542 bytes captured (20336 bits) on interface wlo1, id 0
> Ethernet II, Src: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00), Dst: IntelCor_d6:0a:b0 (18:1d:ea:d6:0a:b0)
  > Destination: IntelCor_d6:0a:b0 (18:1d:ea:d6:0a:b0)
  > Source: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
    Type: IPv4 (0x0800)
  > Internet Protocol Version 4, Src: 34.117.237.239, Dst: 172.26.42.139
  > Transmission Control Protocol, Src Port: 443, Dst Port: 54686, Seq: 1, Ack: 518, Len: 2476
  > Transport Layer Security

```

Figura 1.7: Endereço ethernet da fonte

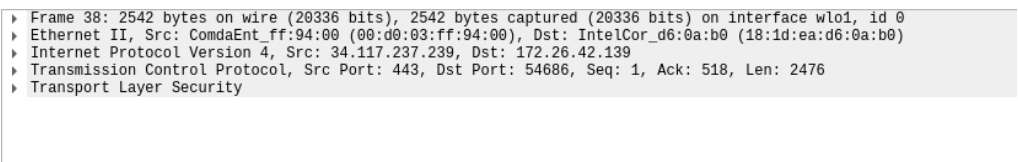


Como é possível verificar na figura 1.7 o endereço da ethernet da fonte é o 00:d0:03:ff:94:00 e corresponde ao router da rede local.

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

Assim como no exercício anterior, ao analisar a 1.7 apercebemo-nos que o endereço de destino é o 18:1d:ea:d6:0a:b0, correspondente à interface ativa da máquina que realizou o request.

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



```
▶ Frame 38: 2542 bytes on wire (20336 bits), 2542 bytes captured (20336 bits) on interface wlo1, id 0
▶ Ethernet II, Src: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00), Dst: IntelCor_d6:0a:b0 (18:1d:ea:d6:0a:b0)
▶ Internet Protocol Version 4, Src: 34.117.237.239, Dst: 172.26.42.139
▶ Transmission Control Protocol, Src Port: 443, Dst Port: 54686, Seq: 1, Ack: 518, Len: 2476
▶ Transport Layer Security
```

Figura 1.8: Vários Protocolos usados na transmissão da trama

De acordo com a figura 1.8, é possível perceber que os protocolos usados no encapsulamento da trama recebida foram: Ethernet II, IP (Internet Protocol), TCP (Transmission Control Protocol) e HTTPS (Hyper Text Transfer Protocol Secure).

## Capítulo 2

# Protocolo ARP

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

```
core@xubuncore:~$ arp
Address                  Hwtype  Hwaddress      Flags Mask       Iface
gateway                  ether    52:54:00:12:35:02 C               enp0s3
```

Figura 2.1: Comando 'arp' em terminal Linux

O comando arp, tal como é possível verificar na imagem disposta acima, permite listar os conteúdo atuais da cache ARP.

- **Address** indica o endereço, pelo que apenas se tem o gateway da rede local.
- **Hwtype** indica o tipo de protocolo de camada física usado.
- **Hwaddress** indica o endereço MAC da máquina.
- **Flags** indica o tipo de registo que está a ser colocado em memória. Neste caso, a flag C é demonstrada quando as entradas são aprendidas dinamicamente pelo protocolo ARP, e não manualmente.
- **Mask** indica a máscara de subrede, caso exista.
- **Iface** indica o nome da interface que se está a utilizar.

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

Interface: 192.168.56.1 --- 0x12
    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
    255.255.255.255      ff-ff-ff-ff-ff-ff    static

Interface: 172.26.35.136 --- 0x16
    Internet Address      Physical Address      Type
    172.26.254.254        00-d0-03-ff-94-00    dynamic
    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 2.2: Comando 'arp -a' em terminal Windows

O comando arp -a, é usado para demonstrar a tabela ARP para um determinado endereço IP, assim como permite verificar as entradas da cache.

- **Internet Address** - indica o conjunto dos endereço IPV4.
- **Physical Address** - corresponde a endereços MAC que foram descobertos ao longo das várias transmissões de tramas.
- **Type** - corresponde ao tipo de linha adicionada, isto é, se o registo adicionado é do tipo estático ou dinâmico.

## 2.2 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?

```
C:\Users\josej>ping 192.168.43.78

Pinging 192.168.43.78 with 32 bytes of data:
Reply from 192.168.43.78: bytes=32 time=358ms TTL=64
Reply from 192.168.43.78: bytes=32 time=56ms TTL=64
Reply from 192.168.43.78: bytes=32 time=58ms TTL=64
Reply from 192.168.43.78: bytes=32 time=65ms TTL=64

Ping statistics for 192.168.43.78:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 56ms, Maximum = 358ms, Average = 134ms
```

Figura 2.3: Ping para um host da sala de aula

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.104	192.168.1.1	ARP	84	Application Data
2	0.001312	192.168.1.1	192.168.1.104	ARP	84	Application Data
3	0.001999	192.168.1.104	192.168.1.1	TCP	54	443 → 80 [ACK] Seq=2043131101 Len=0
4	0.002009	192.168.1.104	192.168.1.1	TCP	54	443 → 80 [ACK] Seq=2043131101 Len=0
5	0.002044	192.168.1.104	192.168.1.1	TCP	54	443 → 80 [ACK] Seq=2043131101 Len=0
6	0.002112	192.168.1.104	192.168.1.1	TCP	54	443 → 80 [ACK] Seq=2043131101 Len=0
7	0.002181	192.168.1.104	192.168.1.1	TCP	54	443 → 80 [ACK] Seq=2043131101 Len=0
8	0.002250	192.168.1.104	192.168.1.1	TCP	54	443 → 80 [ACK] Seq=2043131101 Len=0
9	0.002319	192.168.1.104	192.168.1.1	TCP	54	443 → 80 [ACK] Seq=2043131101 Len=0
10	0.002388	192.168.1.104	192.168.1.1	TCP	54	443 → 80 [ACK] Seq=2043131101 Len=0
11	0.002457	192.168.1.104	192.168.1.1	TCP	54	443 → 80 [ACK] Seq=2043131101 Len=0
12	0.002526	192.168.1.104	192.168.1.1	TCP	54	443 → 80 [ACK] Seq=2043131101 Len=0
13	0.002595	192.168.1.104	192.168.1.1	TCP	54	443 → 80 [ACK] Seq=2043131101 Len=0
14	0.002664	192.168.1.104	192.168.1.1	TCP	54	443 → 80 [ACK] Seq=2043131101 Len=0
15	0.002733	192.168.1.104	192.168.1.1	TCP	54	443 → 80 [ACK] Seq=2043131101 Len=0
16	0.002802	192.168.1.104	192.168.1.1	TCP	54	443 → 80 [ACK] Seq=2043131101 Len=0
17	0.002871	192.168.1.104	192.168.1.1	TCP	54	443 → 80 [ACK] Seq=2043131101 Len=0
18	0.002940	192.168.1.104	192.168.1.1	TCP	54	443 → 80 [ACK] Seq=2043131101 Len=0
19	0.003009	192.168.1.104	192.168.1.1	TCP	54	443 → 80 [ACK] Seq=2043131101 Len=0
20	0.003078	192.168.1.104	192.168.1.1	TCP	54	443 → 80 [ACK] Seq=2043131101 Len=0
21	0.003147	192.168.1.104	192.168.1.1	TCP	54	443 → 80 [ACK] Seq=2043131101 Len=0
22	0.003216	192.168.1.104	192.168.1.1	TCP	54	443 → 80 [ACK] Seq=2043131101 Len=0
23	0.003285	192.168.1.104	192.168.1.1	TCP	54	443 → 80 [ACK] Seq=2043131101 Len=0
24	0.003354	192.168.1.104	192.168.1.1	TCP	54	443 → 80 [ACK] Seq=2043131101 Len=0
25	0.003423	192.168.1.104	192.168.1.1	TCP	54	443 → 80 [ACK] Seq=2043131101 Len=0
26	0.003492	192.168.1.104	192.168.1.1	TCP	54	443 → 80 [ACK] Seq=2043131101 Len=0
27	0.003561	192.168.1.104	192.168.1.1	TCP	54	443 → 80 [ACK] Seq=2043131101 Len=0
28	0.003630	192.168.1.104	192.168.1.1	TCP	54	443 → 80 [ACK] Seq=2043131101 Len=0
29	0.003699	192.168.1.104	192.168.1.1	TCP	54	443 → 80 [ACK] Seq=2043131101 Len=0
30	0.003768	192.168.1.104	192.168.1.1	TCP	54	443 → 80 [ACK] Seq=2043131101 Len=0

Figura 2.4: Endereços Source e Destination do acesso a <https://alunos.uminho.pt>

O endereço de destino é o broadcast porque a máquina de onde foi feito o acesso a <https://alunos.uminho.pt> não tem conhecimento do endereço MAC do servidor, uma vez que tem a tabela se encontra vazia e não conhece nenhum equipamento com aquele endereço IP, então envia um ARP request em broadcast para todos os dispositivos da subrede, de forma a obter o endereço MAC correspondente ao endereço IP pretendido. Relativamente ao endereço de origem, é o da interface ativa da máquina do aluno, de onde partiu o acesso, e corresponde a 84:fd:d1:7f:3e:f1.

Em ambos os casos, a nível de *request*, encontramos-nos na mesma situação, uma vez que as tabelas ARP se encontram vazias (foram limpas antes desta operação). Deste modo, a única diferença será o dispositivo que reconhecerá o request, e responderá ao pedido, de forma a preencher a tabela ARP do cliente.

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

O valor associado ao campo tipo da trama Ethernet, sinalizado por ether, tem como valor hexadecimal 0x0806, sendo associado ao Address Resolution Protocol.

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

Para verificar e confirmar que se trata de um pedido ARP, é necessário verificar se o campo OP CODE tem o valor 1, tratando-se assim de um ARP request (tal como indicado no campo OP CODE).

Relativamente ao tipo de endereços contidos na mensagem ARP, estará presente o endereço MAC da origem e o de broadcast. Note-se que dentro do corpo da mensagem poderá estar presente o IP que se procura.

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

O tipo de pedido efetuado é "Who has 172.26.254.254? Tell 172.26.254.254". Deste modo, podemos inferir que a máquina pretende saber de quem é este endereço, perguntando a todos os hosts e pedindo para enviar a resposta, de forma a conhecer a quem pertence o endereço MAC.

arp						
No.	Time	Source	Destination	Protocol	Length	Info
4	8.426039	IntelCor_7f:3e:f1	Broadcast	ARP	42	Who has 172.26.254.254? Tell 172.26.35.136
5	8.430446	ComdaEnt_ff:94:00	IntelCor_7f:3e:f1	ARP	60	172.26.254.254 is at 00:d0:03:ff:94:00

> Frame 4: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{E8F32AA2-0029-4FA1-9EFA-8F806397D1D3}, id 0
✓ Ethernet II, Src: IntelCor_7f:3e:f1 (84:fd:d1:7f:3e:f1), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Destination: Broadcast (ff:ff:ff:ff:ff:ff)
> Source: IntelCor_7f:3e:f1 (84:fd:d1:7f:3e:f1)
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_7f:3e:f1 (84:fd:d1:7f:3e:f1)
Sender IP address: 172.26.35.136
Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
Target IP address: 172.26.254.254

0000	ff ff ff ff ff ff 84 fd d1 7f 3e f1 08 06 00 01	.....->.....
0010	08 00 06 04 00 01 84 fd d1 7f 3e f1 ac 1a 23 88	.....->...#.
0020	00 00 00 00 00 00 ac 1a fe fe	.....

Figura 2.5: Protocolo ARP relativo à pesquisa alunos.uminho.pt

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

arp						
No.	Time	Source	Destination	Protocol	Length	Info
4	8.426039	IntelCor_7f:3e:f1	Broadcast	ARP	42	Who has 172.26.254.254? Tell 172.26.35.136
5	8.430446	ComdaEnt_ff:94:00	IntelCor_7f:3e:f1	ARP	60	172.26.254.254 is at 00:d0:03:ff:94:00

>	Frame 5: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{E8F32AA2-0D29-4FA1-9EFA-8F806397D1D3}, id 0
✓	Ethernet II, Src: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00), Dst: IntelCor_7f:3e:f1 (84:fd:d1:7f:3e:f1)
>	Destination: IntelCor_7f:3e:f1 (84:fd:d1:7f:3e:f1)
>	Source: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
	Type: ARP (0x0806)
	Padding: 00000000000000000000000000000000
✓	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_7f:3e:f1 (84:fd:d1:7f:3e:f1)
	Target IP address: 172.26.35.136

0000	84 fd d1 7f 3e f1 00 d0 03 ff 94 00 08 06 00 01	....>.....
0010	08 00 06 04 00 02 84 fd d1 7f 3e f1 ac 1a fe fe	.....ac 1a fe fe
0020	84 fd d1 7f 3e f1 ac 1a 23 88 00 00 00 00 00 00	.....#.....
0030	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....

Figura 2.6: Resposta capturada no wireshark

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

O valor deste campo será do tipo ARP Reply, sendo atribuído o valor 2. Esta resposta surge em seguida ao ARP request referido anteriormente.

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

A resposta ao pedido ARP será um MAC address, sendo indicada no campo **Sender MAC Address**.

2.7 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

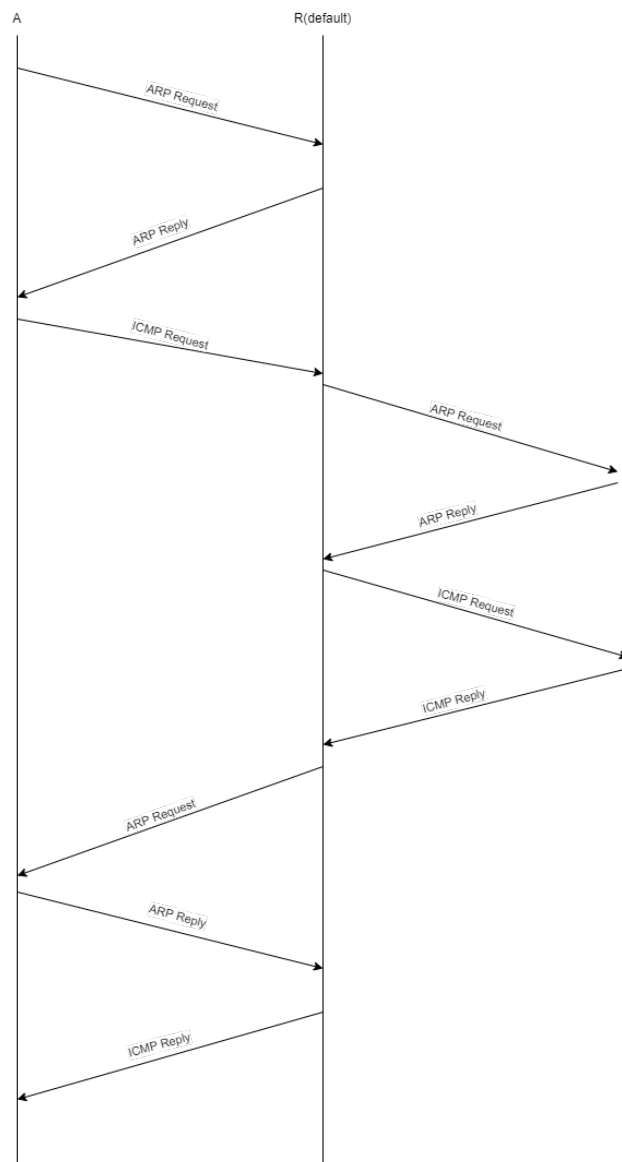


Figura 2.7: Diagrama relativo a um ping entre host's em subredes diferentes

## Capítulo 3

### 5. Domínio de colisão

- 3.1 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?**

Através desta experiência é possível concluir que o tráfego que flui na rede do departamento A, onde o switch foi trocado pelo hub, é superior ao tráfego que circula no departamento B, isto devido ao facto que no departamento A, o hub irá fazer flood do tráfego que recebe de um host específico para o resto da rede. Em contrapartida o switch da rede do departamento B uma vez que já tem a sua tabela completa apenas encaminha o tráfego para o seu destino, reduzindo assim o tráfego presente na rede.

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

Assumindo que a tabela de comutação do switch do departamento B se encontra vazia, foram realizados pings do Jasmine para o Router, Aladin e o servidor B. Sendo que é adicionada inicialmente a entrada referente ao Jasmine, seguida da entrada para o Router, Aladin e Servidor B.



maquina	Endereço mac	Porta
Jasmine	00:00:00:aa:00:0f	1
Router	00:00:00:aa:00:0c	2
Aladin	00:00:00:aa:00:10	3
Servidor	00:00:00:aa:00:15	4

Figura 3.1: tabela de comutação

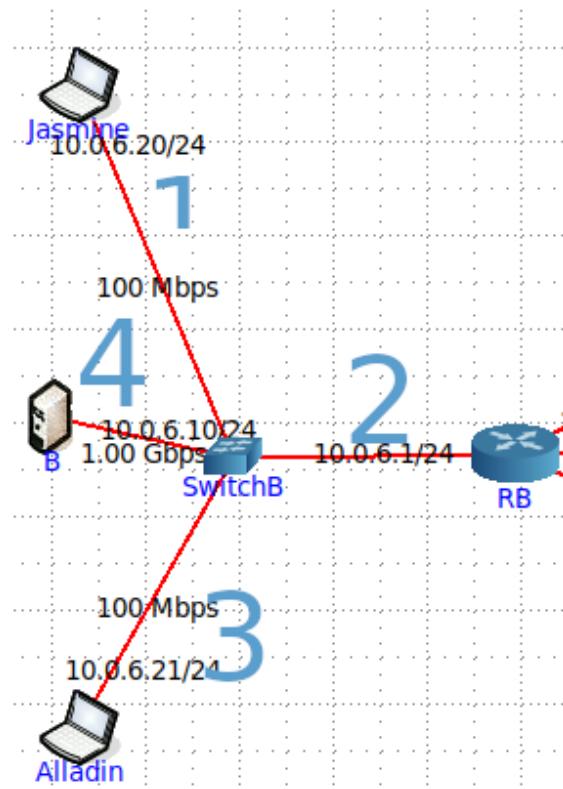


Figura 3.2: Rede do departamento B

## Capítulo 4

# Conclusões

Com o presente trabalho foi possível aprofundar o conhecimento sobre a Ethernet e respetivos pedidos de comunicação através do protocolo ARP. O desenvolvimento do trabalho associado ao presente relatório envolveu a utilização do simulador de redes CORE, e da ferramenta de captura e análise de pacotes Wireshark. A utilização conjunta destas ferramentas permitiu a clara observação das técnicas de encapsulamento usadas para transferência de processos, com maior foco no protocolo ARP. Foi possível averiguar as técnicas associadas a este protocolo no que toca à informação dos endereços envolvidos, bem como à análise de pedidos e respostas do mesmo.

Em suma, este trabalho permitiu salientar os benefícios da utilização de redes Ethernet, nomeadamente associados à facilidade da comunicação e transmissão de informação, bem como o papel fundamental dos protocolos ARP para o seu correto funcionamento.