

UNIVERSIDADE DO MINHO

ENGENHARIA INFORMÁTICA

21/22

---

## **Redes - TP3**

---

Afonso Amorim A97569

Luís Ferreira A95111

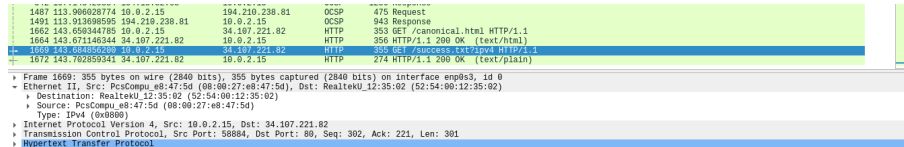
Pedro Dantas A97396

## **Índice**

<b>1</b>	<b>Captura e análise de Tramas Ethernet</b>	<b>3</b>
<b>2</b>	<b>Protocolo ARP</b>	<b>5</b>
<b>3</b>	<b>Domínios de colisão</b>	<b>8</b>
<b>4</b>	<b>Conclusão</b>	<b>9</b>

# 1 Captura e análise de Tramas Ethernet

## Exercício 1



No.	Time	Source	Destination	Protocol	Length	Info
1487	113.086028774	10.0.2.15	194.210.238.81	OCSP	475	Request
1491	113.91398555	194.210.238.81	10.0.2.15	OCSP	943	Response
1662	143.658344785	10.0.2.15	34.107.221.82	HTTP	353	GET /canonical.html HTTP/1.1
1664	143.671140344	34.107.221.82	10.0.2.15	HTTP	356	HTTP/1.1 200 OK (text/html)
1609	143.683506200	10.0.2.15	34.107.221.82	HTTP	356	GET /success.txt/ipv4 HTTP/1.1
1672	143.702859341	34.107.221.82	10.0.2.15	HTTP	274	HTTP/1.1 200 OK (text/plain)

Frame 1609: 355 bytes on wire (2840 bits), 355 bytes captured (2840 bits) on interface enp0s3, id 0  
Ethernet II, Src: PcsCompu\_e8:47:5d (08:00:27:e8:47:5d), Dst: RealtekU\_12:35:02 (52:54:00:12:35:02)  
Destination: RealtekU\_12:35:02 (52:54:00:12:35:02)  
Source: PcsCompu\_e8:47:5d (08:00:27:e8:47:5d)  
Type: IPv4 (0x0800)  
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 34.107.221.82  
Transmission Control Protocol, Src Port: 58884, Dst Port: 80, Seq: 302, Ack: 221, Len: 301  
Hypertext Transfer Protocol

Fig. 1

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

Endereço MAC de origem: **08:00:27:e8:47:5d**

Endereço MAC de destino: **52:54:00:12:35:02**

## Exercício 2

Identifique a que sistemas se referem. Justifique.

Relativamente à origem, o endereço físico é referente ao nosso computador (máquina utilizada). Por outro lado, o endereço de destino refere-se ao *router* com o qual a nossa máquina está a comunicar.

## Exercício 3

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

Como se pode verificar pela figura 1, o *Type* é (0x800), pelo que concluímos que a camada superior está a usar um protocolo IPv4.

## Exercício 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.

### Exercício 5

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

Tendo em conta a figura 1, podemos verificar que o endereço *Ethernet* da fonte é (52:54:00:12:35:02), correspondente ao endereço físico do *router* que está a ser acedido pela nossa máquina.

### Exercício 6

1491	131.91399895	194.210.238.81	10.0.2.15	UCSP	543 Response
1602	143.65944785	10.0.2.15	34.107.221.82	HTTP	353 GET /canonical.html HTTP/1.1
1603	143.65944785	34.107.221.82	10.0.2.15	HTTP	356 HTTP/1.1 200 OK (text/html)
1609	143.68485208	10.0.2.15	34.107.221.82	HTTP	355 GET /success.txt?ip= HTTP/1.1
1672	143.70285934	34.107.221.82	10.0.2.15	HTTP	274 HTTP/1.1 200 OK (text/plain)

```

# Frame 1672: 274 bytes on wire (2192 bits), 274 bytes captured (2192 bits) on interface em083, id 0
# Ethernet II, Src: RealtekU 12:35:02 (52:54:00:12:35:02), Dst: PcsCompu:e8:47:5d (08:00:27:e8:47:5d)
#   # Source: RealtekU 12:35:02 (52:54:00:12:35:02)
#   # Type: IPv4 (0x8000)
#   # Internet Protocol Version 4, Src: 34.107.221.82, Dst: 10.0.2.15
#   # Transmission Control Protocol, Src Port: 80, Dst Port: 58884, Seq: 221, Ack: 603, Len: 228
#   # Hypertext Transfer Protocol
#   # Line-based text data: text/plain (1 lines)

```

Fig. 2

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

Tendo em conta a figura 2, verificamos que o endereço MAC do destino é (08:00:27:e8:47:5d), correspondente ao endereço físico da nossa máquina.

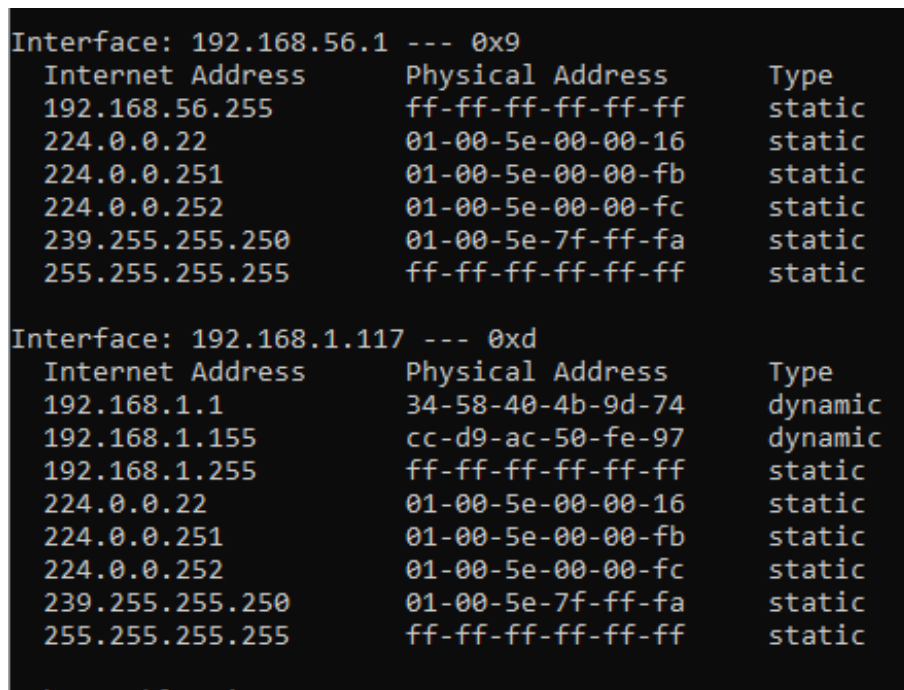
### Exercício 7

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

Os protocolos TCP (*Transmission Control Protocol*), IPv4 (*Internet Protocol Version 4*), HTTP (*Hypertext Transfer Protocol*) e *Ethernet*.

## 2 Protocolo ARP

### Exercício 8



```
Interface: 192.168.56.1 --- 0x9
  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: 192.168.1.117 --- 0xd
  Internet Address      Physical Address      Type
  192.168.1.1           34-58-40-4b-9d-74    dynamic
  192.168.1.155         cc-d9-ac-50-fe-97    dynamic
  192.168.1.255         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
```

Fig. 3

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

Como podemos observar na figura 3, a primeira coluna corresponde aos endereços IP, enquanto a segunda corresponde aos endereços MAC.

### Exercício 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?

1890	415.868917238	PcsCompu_e8:47:5d	RealtekU_12:35:02	0x0000	90	IPv4
1891	416.063115374	RealtekU_12:35:02	PcsCompu_e8:47:5d	0x0000	90	IPv4
1892	416.063115667	RealtekU_12:35:02	PcsCompu_e8:47:5d	0x0000	90	IPv4
1893	416.868678144	PcsCompu_e8:47:5d	RealtekU_12:35:02	0x0000	90	IPv4
1894	417.011042105	RealtekU_12:35:02	PcsCompu_e8:47:5d	0x0000	90	IPv4
1895	420.960814859	PcsCompu_e8:47:5d	RealtekU_12:35:02	ARP	42	Who has 10.0.2.2? Tell 10.0.2.15
1896	420.961294948	RealtekU_12:35:02	PcsCompu_e8:47:5d	ARP	60	10.0.2.2 is at 52:54:00:12:35:02
▶ Frame 1895: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface enp0s3, id 0						
▼ Ethernet II, Src: PcsCompu_e8:47:5d (08:00:27:e8:47:5d), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)						
▶ Destination: RealtekU_12:35:02 (52:54:00:12:35:02)						
▶ Source: PcsCompu_e8:47:5d (08:00:27:e8:47:5d)						
Type: ARP (0x0806)						
▶ Address Resolution Protocol (request)						

Fig. 4

O valor do endereço origem é 08:00:27:e8:47:5d, enquanto o do destino é ff:ff:ff:ff:ff:ff. Este último pode ser justificado pelo facto de, na nossa tabela arp, o valor do endereço MAC não estar associado ao endereço IP para o qual o *ping* é enviado. Desta forma, é necessário enviar uma mensagem para todos os dispositivos na rede de modo a que o dispositivo pretendido possa responder e, assim, guardar o valor do endereço MAC. Para isto é utilizado o endereço de Broadcast ff:ff:ff:ff:ff:ff.

### Exercício 10

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

Tendo em conta a figura x, podemos verificar que o valor hexadecimal do campo tipo da trama *Ethernet* é 0x0806, o que nos indica que a camada acima está a utilizar o protocolo ARP.

### Exercício 11

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

É possível verificar se se trata ou não de um pedido ARP através da análise do protocolo utilizado que, neste caso, é de facto um protocolo ARP, dado por 0x0806. Uma mensagem ARP contém tanto endereços IP como endereços MAC, pelo que podemos concluir que o protocolo ARP realiza a conversão de um endereço IP para um endereço MAC da respetiva interface ativa.

## Exercício 12

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

Tendo em conta que a nossa tabela arp não possui uma associação entre o endereço IP para o qual é enviado um ping e o seu respetivo endereço MAC, envia-se uma mensagem ARP para todos os dispositivos na rede de modo a que, caso o endereço IP pretendido receba esta mesma mensagem, seja possível responder com o seu endereço MAC.

## Exercício 13

```
▼ Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_e8:47:5d (08:00:27:e8:47:5d)
  ▼ Destination: PcsCompu_e8:47:5d (08:00:27:e8:47:5d)
    Address: PcsCompu_e8:47:5d (08:00:27:e8:47:5d)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  ▼ Source: RealtekU_12:35:02 (52:54:00:12:35:02)
    Address: RealtekU_12:35:02 (52:54:00:12:35:02)
    ....1. .... = LG bit: Locally administered address (this is NOT the factory default)
    ....0. .... = IG bit: Individual address (unicast)
  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: RealtekU_12:35:02 (52:54:00:12:35:02)
    Sender IP address: 10.0.2.2
    Target MAC address: PcsCompu_e8:47:5d (08:00:27:e8:47:5d)
    Target IP address: 10.0.2.15
```

Fig. 5

```
▼ Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: PcsCompu_e8:47:5d (08:00:27:e8:47:5d)
  Sender IP address: 10.0.2.15
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 10.0.2.2
```

0000	52	54	00	12	35	02	08	00	27	e8	47	5d	08	06	00	01	RT	5	...	'G	...
0010	08	00	06	04	00	01	08	00	27	e8	47	5d	0a	00	02	0f	.....	..	'G	.....	
0020	00	00	00	00	00	00	0a	00	02	02							.....				

Fig. 6

### Alínea (A)

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

O valor do campo ARP opcode é 2, pelo que podemos concluir que é a *reply* (como indicado na figura 5) a uma mensagem de *request* efetuada anteriormente. Nesta *reply* será enviado o endereço MAC.

Alínea (B)

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

A resposta ao pedido ARP encontra-se entre 23 - 28 *bytes*, como podemos verificar através da figura 6. Esta informação pode ser obtida através do *Sender MAC Address*.

#### Exercício 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 receção da resposta ICMP do *host* destino.

### 3 Domínios de colisão

#### Exercício 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?

#### Exercício 16

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



## 4 Conclusão

Após a realização do trabalho podemos concluir que obtivemos uma melhor compreensão em relação a tramas *Ethernet* e ao protocolo ARP, que foram estudados nas duas primeiras fases. Para isto utilizamos o *software* de captura e análise de tramas *Wireshark*. Esta ferramenta foi essencial para diversos aspectos como: a verificação dos protocolos utilizados, o encapsulamento aquando da transferência de processos, o tipo de mensagem ARP, etc. Foi também utilizado, indiretamente, o *CORE*, sendo que não foram necessárias alterações em relação ao que foi feito num trabalho prático realizado anteriormente.