

Universidade do Minho



Redes de Computadores

RC-TP2

MESTRADO INTEGRADO EM ENGENHARIA INFORMÁTICA

3º ANO

GRUPO 61

RENATO ANDRÉ ARAÚJO AZEVEDO
GONÇALO COSTA DE ALMEIDA
MARIA SOFIA MARTINHO GONÇALVES JORDÃO MARQUES

A89547
A88292
A87963

Índice

1	Captura e análise de Tramas Ethernet	3
1.1	Ex1	3
1.2	Ex2	3
1.3	Ex3	3
1.4	Ex4	3
1.5	Ex5	4
1.6	Ex6	4
1.7	Ex7	5
1.8	Ex8	5
2	Protocolo ARP	5
2.1	Ex9	5
2.2	Ex10	5
2.3	Ex11	6
2.4	Ex12	6
2.5	Ex13	7
2.6	Ex14	7
	2.6.1 Alinea a	7
	2.6.2 Alinea b	7
3	ARP Gratuito	8
3.1	Ex15	8
4	Domínios de colisão	8
4.1	Ex16	8
5	Conclusão	9

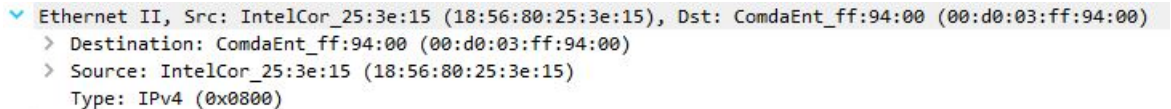
1 Captura e análise de Tramas Ethernet

1.1 Ex1

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

Endereço origem: 18:56:80:25:3e:15

Endereço destino: 00:d0:03:ff:94:00



```
▼ Ethernet II, Src: IntelCor_25:3e:15 (18:56:80:25:3e:15), Dst: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
  > Destination: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
  > Source: IntelCor_25:3e:15 (18:56:80:25:3e:15)
  Type: IPv4 (0x0800)
```

Figure 1: Endereços MAC

1.2 Ex2

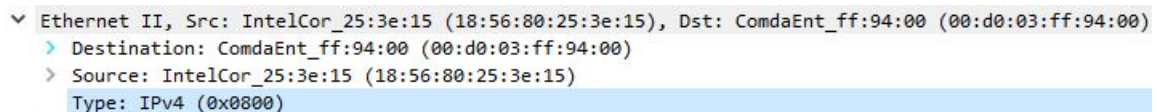
Identifique a que sistemas se referem. Justifique.

Uma vez que os endereços MAC correspondem a nós imediatamente adjacentes na rede, então o endereço destino corresponde ao router à qual estamos ligados, enquanto que o endereço origem corresponde à nossa máquina nativa.

1.3 Ex3

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

O valor hexadecimal do campo Type é 0x800, e indica o tipo do protocolo encapsulado, neste caso, IPv4.



```
▼ Ethernet II, Src: IntelCor_25:3e:15 (18:56:80:25:3e:15), Dst: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
  > Destination: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
  > Source: IntelCor_25:3e:15 (18:56:80:25:3e:15)
  Type: IPv4 (0x0800)
```

Figure 2: Valor do campo Type

1.4 Ex4

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.

Desde o início da trama até ao caractere ASCII “G” são usados 54 bytes. Como o tamanho total da trama é de 513 bytes, então o overhead introduzido pela pilha protocolar é igual a $54/513 = 0.105263$, o que corresponde a cerca de 10% do tamanho total.

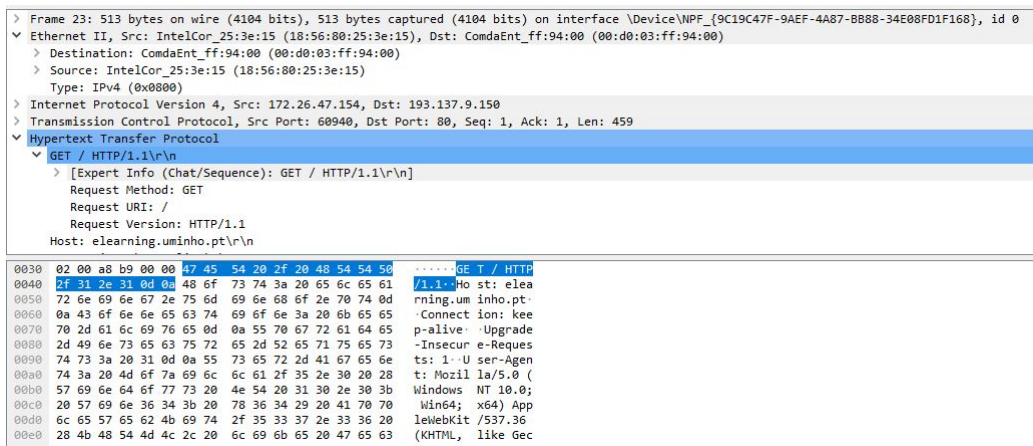


Figure 3: Trama capturada

1.5 Ex5

Através de visualização direta ou construindo um filtro específico, verifique se foram detetadas tramas com erros (por verificação do campo FCS (Frame Check Sequence)).

Aplicando o filtro fcs, que mostra as tramas com erros, nenhum resultado é mostrado, o que significa que não foi detetada nenhuma trama com erros.

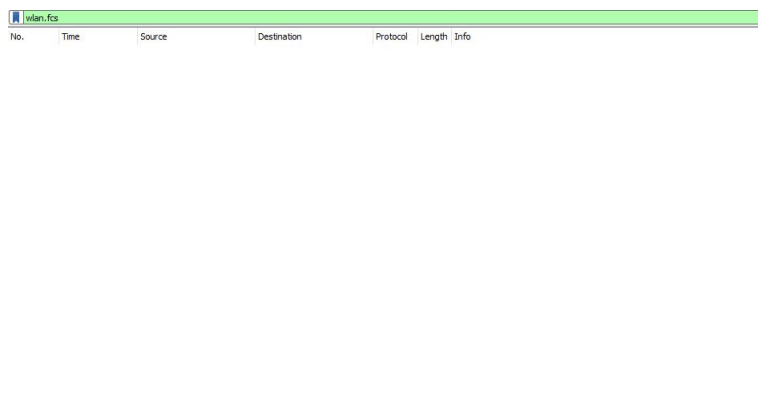


Figure 4: Tramas com erros

1.6 Ex6

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

O endereço Ethernet da fonte é 00:d0:03:ff:94:00. Este endereço corresponde à rede a que estamos ligados, uma vez que estes endereços nós adjacentes numa mesma rede.

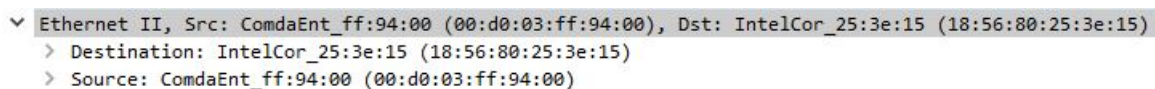


Figure 5: Endereços fonte e destino

1.7 Ex7

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

O endereço MAC do destino é 18:56:80:25:3e:15, e corresponde à nossa máquina nativa.

1.8 Ex8

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

```
> Frame 28: 186 bytes on wire (1488 bits), 186 bytes captured (1488 bits) on interface \Device\NPF_{9C19C47F-9AEF-4A87-BB88-34E08FD1F168}, id 0
> Ethernet II, Src: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00), Dst: IntelCor_25:3e:15 (18:56:80:25:3e:15)
> Internet Protocol Version 4, Src: 193.137.9.150, Dst: 172.26.47.154
> Transmission Control Protocol, Src Port: 80, Dst Port: 60940, Seq: 1, Ack: 460, Len: 132
> Hypertext Transfer Protocol
```

Figure 6: Endereços fonte e destino

Os protocolos contidos na trama são Ethernet, IPv4 (Internet Protocol Version 4), TCP (Transmission Control Protocol), e HTTP (Hypertext Transfer Protocol).

2 Protocolo ARP

2.1 Ex9

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

A primeira coluna identifica os endereços ip, a segunda coluna representa os endereços MAC correspondentes, e a terceira coluna diz-nos o tipo de endereçamento. É ainda possível verificar qual a interface onde os endereços estão definidos.

```
C:\Users\Utilizador>c:\windows\system32\arp -a

Interface: 192.168.56.1 --- 0x8
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: 172.26.107.7 --- 0x11
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
239.255.255.250       01-00-5e-7f-ff-fa    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static
```

Figure 7: Endereços MAC

2.2 Ex10

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?

O endereço de origem é 68:94:23:a1:b2:a8.

O endereço de destino é ff:ff:ff:ff:ff:ff.

De forma a que o pedido ARP seja enviado para todas as máquinas da rede, este é enviado por broadcast, possuindo assim o endereço destino ff:ff:ff:ff:ff:ff, que corresponde a encaminhar a mensagem para todas as interfaces da rede local. Assim, a máquina que possuir o endereço pedido, devolverá uma resposta com o seu endereço MAC, e todas as outras irão ignorar a mensagem.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	HonHaiPr_a1:b2:a8	Broadcast	ARP	42	Who has 172.26.254.254? Tel
2	0.633562	HonHaiPr_a1:b2:a8	Broadcast	ARP	42	Who has 172.26.254.254? Tel
3	0.635601	ComdaEnt_ff:94:00	HonHaiPr_a1:b2:a8	ARP	60	172.26.254.254 is at 00:00:00:00:00:00


```

<----->
> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{CDD368EC-41}
> Ethernet II, Src: HonHaiPr_a1:b2:a8 (68:94:23:a1:b2:a8), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    Address: Broadcast (ff:ff:ff:ff:ff:ff)
    ....01. .... = LG bit: Locally administered address (this is NOT the factory default)
    ....01. .... = IG bit: Group address (multicast/broadcast)
  > Source: HonHaiPr_a1:b2:a8 (68:94:23:a1:b2:a8)
    Address: HonHaiPr_a1:b2:a8 (68:94:23:a1:b2:a8)
    ....00. .... = LG bit: Globally unique address (factory default)
    ....00. .... = IG bit: Individual address (unicast)
  > Type: ARP (0x0806)
  > Address Resolution Protocol (request)
  
```

Figure 8: Endereços origem e destino

2.3 Ex11

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

O campo tipo tem o valor hexadecimal 0x0806 (Type: ARP (0x0806)) e indica que o tipo de trama que estamos a tratar é de facto ARP.

2.4 Ex12

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

O campo *Type*, como observamos na questão anterior, diz-nos que estamos a tratar do protocolo ARP.

Os endereços que estão contidos na mensagem são endereços MAC e IP como podemos verificar no campo do address resolution protocol (request). Podemos concluir de acordo com a figura que, o host cujo ip é 172.26.107.7 quer saber qual é o o endereço mac do host 172.26.254.254, então através da mensagem arp vai ser possível determinar qual esse endereço. Assim, será possível associar, tanto na fonte como no destino, o endereço ip ao endereço mac.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	HonHaiPr_a1:b2:a8	Broadcast	ARP	42	Who has 1
2	0.633562	HonHaiPr_a1:b2:a8	Broadcast	ARP	42	Who has 1
3	0.635601	ComdaEnt_ff:94:00	HonHaiPr_a1:b2:a8	ARP	60	172.26.25

```

<----->
> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Dev
> Ethernet II, Src: HonHaiPr_a1:b2:a8 (68:94:23:a1:b2:a8), 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: HonHaiPr_a1:b2:a8 (68:94:23:a1:b2:a8)
    Sender IP address: 172.26.107.7
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 172.26.254.254
  
```

Figure 9: Endereços na mensagem ARP

2.5 Ex13

Explicite que tipo de pedido ou pergunta é feita pelo host de origem?

A pergunta feita é "Who has 172.26.254.254? Tell 172.26.107.7". Como podemos observar, perguntamos ao host qual é o endereço mac do host cujo ip é 172.26.254.254, que é o endereço à qual fizemos ping, e pedimos para que devolva a resposta ao host 172.26.107.7, que corresponde ao ip da nossa maquina.

1	0.000000	HonHaiPr_a1:b2:a8	Broadcast	ARP	42	Who has 172.26.254.254? Tell 172.26.107.7
---	----------	-------------------	-----------	-----	----	---

Figure 10: Endereços na mensagem ARP

2.6 Ex14

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

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	HonHaiPr_a1:b2:a8	Broadcast	ARP	42	Who has 17
2	0.633562	HonHaiPr_a1:b2:a8	Broadcast	ARP	42	Who has 17
3	0.635601	ComdaEnt_ff:94:00	HonHaiPr_a1:b2:a8	ARP	60	172.26.254

<
> Destination: HonHaiPr_a1:b2:a8 (68:94:23:a1:b2:a8)
> 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: HonHaiPr_a1:b2:a8 (68:94:23:a1:b2:a8)
Target IP address: 172.26.107.7

Figure 11: Endereços na mensagem ARP

2.6.1 Alinea a

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

O valor do campo ARP opcode é: reply (2), e especifica que é uma resposta obtida ao ARP request feito anteriormente.

2.6.2 Alinea b

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

No campo Address Resolution Protocol (reply), podemos ver então que o endereço mac do host 172.26.254.254 é 00:d0:03:ff:94:00, ou seja a resposta é dada na campo *Sender MAC address*.

3 ARP Gratuito

3.1 Ex15

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 gratuito enviado?

953	9.348687	IntelCor_25:3e:15	Broadcast	ARP	42	[ARP Announcement for 172.26.47.154]
1108	10.124952	IntelCor_25:3e:15	Broadcast	ARP	42	Who has 172.26.254.254? Tell 172.26.47.154
1110	10.126735	ComdaEnt_ff:94:00	IntelCor_25:3e:15	ARP	60	172.26.254.254 is at 00:d0:03:ff:94:00
1699	18.996368	IntelCor_25:3e:15	Broadcast	ARP	42	Who has 172.26.254.254? Tell 172.26.47.154
1700	19.000702	ComdaEnt_ff:94:00	IntelCor_25:3e:15	ARP	60	172.26.254.254 is at 00:d0:03:ff:94:00


```
> Frame 953: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{9C19C47F-9AEF-4A87-BB88-34E08FD1F168}, id 0
> Ethernet II, Src: IntelCor_25:3e:15 (18:56:80:25:3e:15), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Destination: Broadcast (ff:ff:ff:ff:ff:ff)
> Source: IntelCor_25:3e:15 (18:56:80:25:3e:15)
  Type: ARP (0x0806)
> Address Resolution Protocol (ARP Announcement)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  [Is gratuitous: True]
  [Is announcement: True]
  Sender MAC address: IntelCor_25:3e:15 (18:56:80:25:3e:15)
  Sender IP address: 172.26.47.154
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 172.26.47.154
```

Figure 12: ARP gratuito

Ao contrario dos restantes pedidos ARP, o ARP gratuito possui tanto no ip de origem como no ip destino, o ip da nossa maquina. Além disso, este pacote possui uma flag propria que o identifica como uma ARP gratuito. Este pedido ARP gratuito serve para informar à rede do ip da nossa máquina, bem como o endereço MAC. Tal como seria de esperar, neste pedido não é esperado uma resposta.

4 Domínios de colisão

4.1 Ex16

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.

Ao fazer ping do laptop 1 para o laptop 2 no departamento A, podemos observar com o tcpdum (aberto no laptop 2 e no router) que apenas o laptop 2, e mais nenhuma outra interface da rede, irá receber a mensagem. Já no departamento B, isto não acontece, uma vez que ao dar ping do laptop 1 para o laptop 2, conseguimos verificar com o tcpdum que a mensagem chega até ao router. Estes resultados mostram que ao contrario do hub, o switch envia a mensagem apenas para o destino, enquanto que o hub faz broadcast da mensagem. Em termos de controlar ou dividir dominios de colisão, podemos concluir que os switch permitem um maior controlo, havendo uma separação dos domínios de colisão.

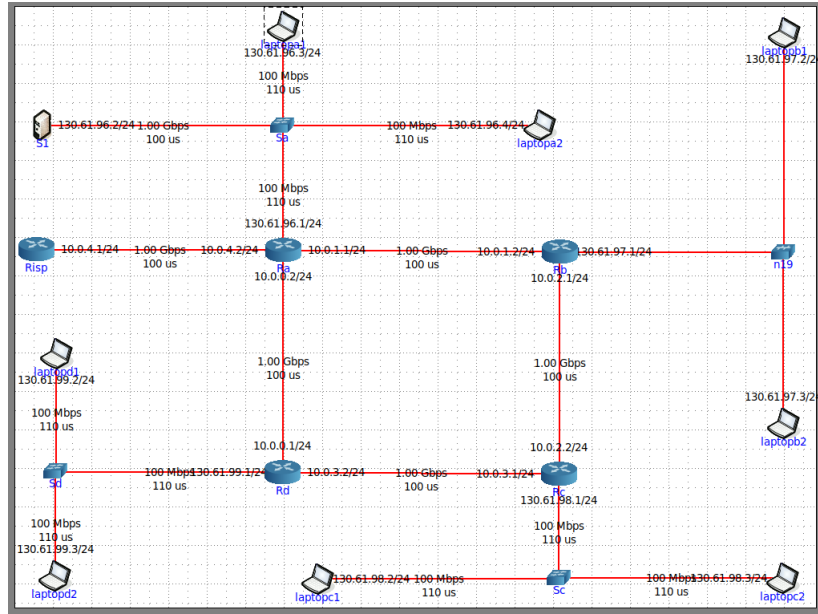


Figure 13: Topologia

5 Conclusão

A realização deste trabalho prático permite um melhor entendimento do endereçamento ethernet e do protocolo ARP, bem como os seus diferentes campos. Além disso, percebemos melhor como funcionam os pedidos ARP numa rede, como por exemplo a existencia de ARPs gratuitos, e o seu proposito, bem como a importancia deste protocolo para as redes locais. Por fim, conseguimos ainda diferenciar um hub de um switch, com um melhor entendimento dos domínios de colisão, e como estes dois os tratam.

