



Universidade do Minho
Escola de Engenharia

Redes de Computadores TP3

Novembro de 2019



Ana Margarida Campos



Ana Catarina Gil



Tânia Rocha

1 Captura e análise de tramas Ethernet

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

Origem: 3c:52:82:e5:bc:4c

Destino: 00:0c:29:d2:19:f0

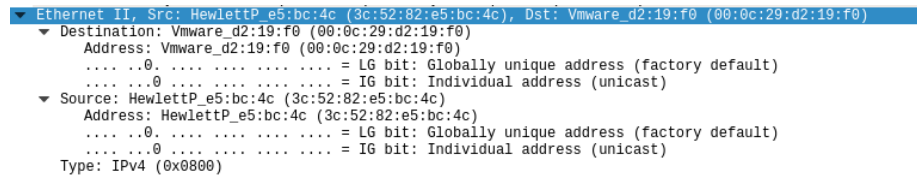


Figure 1: Endereços MAC de origem e destino

1.2 Identifique a que sistemas se referem. Justifique.

O endereço MAC de origem corresponde ao nosso computador e o de destino corresponde ao router.

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

O valor hexadecimal do campo Type é 0x0800 e indica o tipo de encapsulamento (IPv4 neste caso).

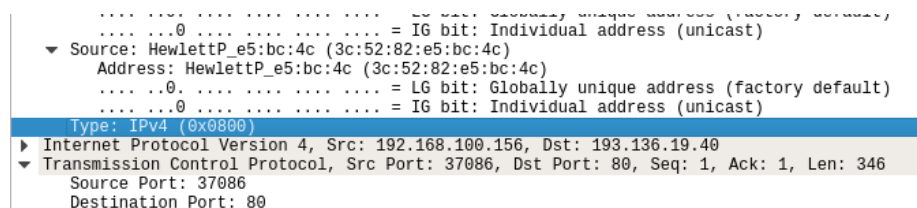


Figure 2: Valor hexadecimal do campo Type

1.4 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.

Até ao carater “G” (ascii:0x47) são usados 66 bytes. No total são usados 412 bytes, logo a percentagem de sobrecarga é de $(66/412)*100 = 16,02$

```

Hypertext Transfer Protocol
  GET / HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /
      Request Version: HTTP/1.1
      Host: miei.di.uminho.pt\r\n
      User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:67.0) Gecko/20100101 Firefox/67.0\r\n
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
      Accept-Language: pt-PT,pt;q=0.8,en;q=0.5,en-US;q=0.3\r\n
      Accept-Encoding: gzip, deflate\r\n
      Connection: keep-alive\r\n
      Upgrade-Insecure-Requests: 1\r\n
      \r\n
      [Full request URI: http://miei.di.uminho.pt/]
      [HTTP request 1/1]
      [Response in frame: 22]

```

```

0000 00 0c 29 d2 19 f0 3c 52 82 e5 bc 4c 08 00 45 00 ...<R...L..E
0010 01 8e f9 e3 40 00 40 06 45 91 c0 a8 64 9c c1 88 ...@.E..d..
0020 13 28 90 de 00 50 d3 5a 22 61 b5 ff de 4d 80 18 ...P.Z"a...M..
0030 00 e5 4f c1 00 00 01 01 08 0a c9 99 df a1 de 82 ...0.....
0040 4e df 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31 N GET / HTTP/1.1
0050 0d 0a 48 6f 73 74 3a 20 6d 69 65 69 2e 64 69 2e ..Host: miei.di.
0060 75 6d 69 6e 68 6f 2e 70 74 0d 0a 55 73 65 72 2d uminho.p t..User-
0070 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 Agent: Mozilla/5
0080 2e 30 20 28 58 31 31 3b 20 55 62 75 6e 74 75 3b .0 (X11; Ubuntu;
0090 20 4c 69 6e 75 78 20 78 38 36 5f 36 34 3b 20 72 Linux x 86_64; r
00a0 76 3a 36 37 2a 30 20 20 47 65 63 6b 6f 2f 32 30 v:67.0) Gecko/20

```

Figure 3: Pilha protocolar no envio HTTP GET

1.5 Através de visualização direta de uma trama capturada, verifique que, possivelmente, o campo FCS (Frame Check Sequence) usado para deteção de erros não está a ser usado. Em sua opinião, porque será?

Não aparece porque estamos numa ligação Ethernet um quadro danificado deve ser descartado.

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

Endereço Ethernet da fonte = 00:0c:29:d2:19:f0

Corresponde ao router da rede local.

```

Frame 22: 547 bytes on wire (4376 bits), 547 bytes captured (4376 bits) on interface 0
Ethernet II, Src: Vmware_d2:19:f0 (00:0c:29:d2:19:f0), Dst: HewlettP_e5:bc:4c (3c:52:82:e5:bc:4c)
  Destination: HewlettP_e5:bc:4c (3c:52:82:e5:bc:4c)
    Address: HewlettP_e5:bc:4c (3c:52:82:e5:bc:4c)
      ...0. .... = LG bit: Globally unique address (factory default)
      ...0. .... = IG bit: Individual address (unicast)
  Source: Vmware_d2:19:f0 (00:0c:29:d2:19:f0)
    Address: Vmware_d2:19:f0 (00:0c:29:d2:19:f0)
      ...0. .... = LG bit: Globally unique address (factory default)
      ...0. .... = IG bit: Individual address (unicast)

```

Figure 4: Endereço Ethernet

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

O endereço MAC do destino = 3c:52:82:e5:bc:4c

Este mesmo corresponde ao IP do nosso computador.

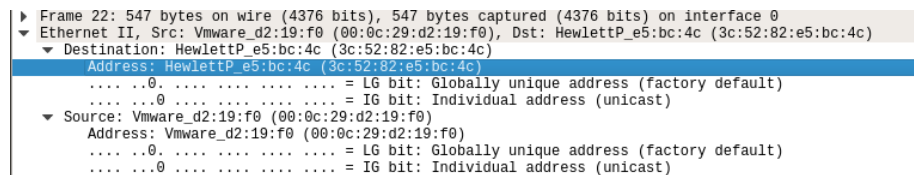


Figure 5: Endereço Mac do destino.

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

Os vários protocolos contidos na trama recebida são IPv4 ,TCP e HTTP.

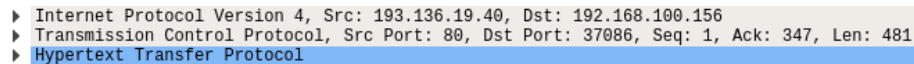


Figure 6: Protocolos contidos na trama.

2 Protocolo ARP

2.1 Observe o conteúdo da tabela ARP. Explique o significado de cada uma das colunas.

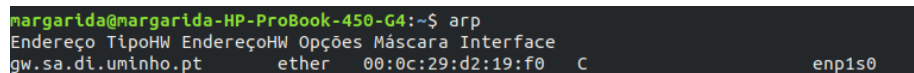


Figure 7: Comando arp.

Nota : Conforme confirmado na aula prática, o nosso computador não estava a executar o comando arp corretamente. Tal se verifica na fig.7. Mesmo assim, através de pesquisa conseguimos responder à questão.

Coluna Endereço : Representa o endereço IP do destino.

Coluna tipoWH : Representa o meio de ligação até ao destino.

Coluna EndereçoHW : Representa o MAC adress do destino.

Coluna Máscara : Representa o tipo de entrada.

Coluna Interface : Representa o tipo de interface.

2.2 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?

Como observado na figura o valor hexadecimal do destino é 0c:9d:92:35:f2:fb e o da origem é 3c:52:82:e5:bc:4c. Estes valores representam os endereços MAC. O endereço do destino Mac é para onde estamos a testar o ping.

```
▼ Ethernet II, Src: HewlettP_e5:bc:4c (3c:52:82:e5:bc:4c), Dst: AsustekC_35:f2:fb (0c:9d:92:35:f2:fb)
  ▶ Destination: AsustekC_35:f2:fb (0c:9d:92:35:f2:fb)
  ▶ Source: HewlettP_e5:bc:4c (3c:52:82:e5:bc:4c)
  Type: ARP (0x0806)
  - Address Resolution Protocol (request)
```

Figure 8: Valores Hexadécimais dos endereços de origem e de destino.

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

Como observado na figura anterior, o valor do campo tipo da trama Ethernet é ARP(0x0806). Isto indica qual o protocolo utilizado.

2.4 Qual o valor do campo ARP opcode? O que especifica? Se necessário, consulte a RFC do protocolo ARP (<http://tools.ietf.org/html/rfc826.html>)

O valor do campo ARP opcode é Request(1). Isto significa que, neste caso, a trama tem como objetivo o pedido do endereço MAC destino da trama em questão. RFC é um método de conversão de endereços IP em endereços Ethernet.

```
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: HewlettP_e5:bc:4c (3c:52:82:e5:bc:4c)
  Sender IP address: 192.168.100.156
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 192.168.100.211
```

Figure 9: Valor do campo ARP code.

2.5 Identifique que tipo de endereços está contido na mensagem ARP? Que conclui?

Os endereços contidos na mensagem ARP são o IP e o MAC da origem e do destino. Ou seja os endereços que permitem a troca de tramas entre estes.

2.6 Explícite que tipo de pedido ou pergunta é feito pelo host de origem?

O host de origem pede o endereço MAC para o qual pretende enviar a trama.

1010	28.139748147	HewlettP_e5:bc:4c	AsustekC_35:f2:fb	ARP	42	Who has 192.168.100.211? Tell 192.168.100.156
1011	28.139899925	AsustekC_35:f2:fb	HewlettP_e5:bc:4c	ARP	60	192.168.100.211 is at 0c:9d:92:35:f2:fb

Figure 10: Host de origem.

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

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

Neste caso, o valor do campo ARP opcode é Reply(2).

```
Padding: 00000000000000000000000000000000
```

▼ Address Resolution Protocol (reply)

- Hardware type: Ethernet (1)
- Protocol type: IPv4 (0x0800)
- Hardware size: 6
- Protocol size: 4
- Opcodes: reply (2)

Sender MAC address: AsustekC_35:f2:fb (0c:9d:92:35:f2:fb)
Sender IP address: 192.168.100.211
Target MAC address: HewlettP_e5:bc:4c (3c:52:82:e5:bc:4c)
Target IP address: 192.168.100.156

Figure 11: Mensagem ARP.

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

A posição da mensagem ARP encontra-se desde os 23 aos 28 bytes.

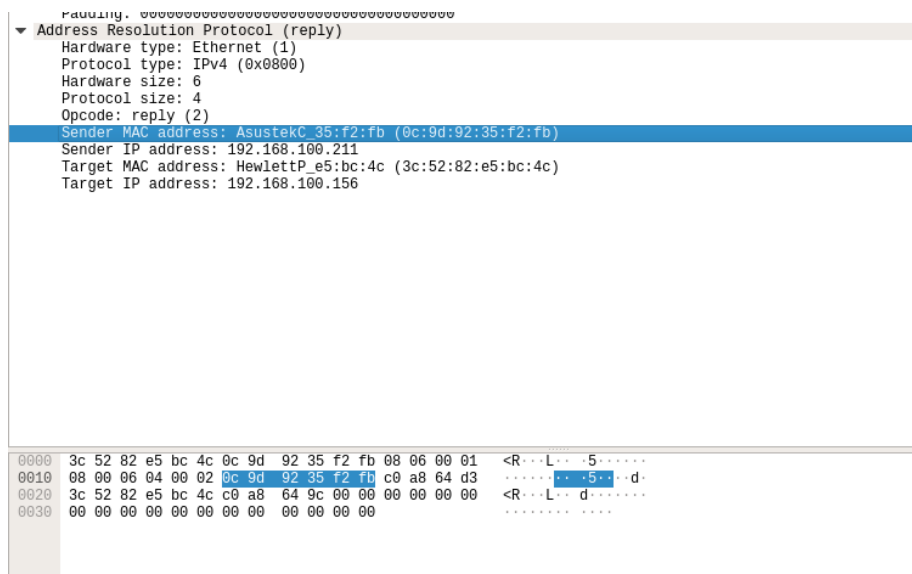


Figure 12: Mensagem ARP.

2.8 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?

Com a utilização do comando `arping -U 192.168.100.156` (o IP da nossa máquina), obtivemos ARP's gratuitos. O que diferencia o pedido ARP gratuito dos restantes pedidos é que no pedido ARP gratuito existe uma flag `Is gratuitous`: `True` e apresenta endereço de destino igual ao de origem. Prevê-se que não exista resposta por parte deste ARP gratuito, pois isso significaria que existe algo na rede com um IP igual ao da nossa máquina.

No.	Time	Source	Destination	Protocol	Length	Info
42	9.965819533	Vmware_d2:19:f0	HewlettP_e5:bc:4c	ARP	60	Who has 192.168.100.156? Tell 192.168.100.254
43	9.965835900	HewlettP_e5:bc:4c	Vmware_d2:19:f0	ARP	42	192.168.100.156 is at 3c:52:82:e5:bc:4c
760	41.473699527	HewlettP_e5:bc:4c	Broadcast	ARP	42	Who has 192.168.100.254? Tell 192.168.100.156
761	41.473982766	Vmware_d2:19:f0	HewlettP_e5:bc:4c	ARP	60	192.168.100.254 is at 00:0c:29:d2:19:f0
949	50.434249642	Vmware_d2:19:f0	HewlettP_e5:bc:4c	ARP	60	Who has 192.168.100.156? Tell 192.168.100.254
950	50.434287861	HewlettP_e5:bc:4c	Vmware_d2:19:f0	ARP	42	192.168.100.156 is at 3c:52:82:e5:bc:4c
1127	93.974371514	Vmware_d2:19:f0	HewlettP_e5:bc:4c	ARP	60	Who has 192.168.100.156? Tell 192.168.100.254
1128	93.974394210	HewlettP_e5:bc:4c	Vmware_d2:19:f0	ARP	42	192.168.100.156 is at 3c:52:82:e5:bc:4c
1168	107.001965764	HewlettP_e5:bc:4c	Broadcast	ARP	42	Gratuitous ARP for 192.168.100.156 (Request)
1170	108.092227558	HewlettP_e5:bc:4c	Broadcast	ARP	42	Gratuitous ARP for 192.168.100.156 (Request)
1172	109.092436023	HewlettP_e5:bc:4c	Broadcast	ARP	42	Gratuitous ARP for 192.168.100.156 (Request)
▶ Frame 1168: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0						
▶ Ethernet II, Src: HewlettP_e5:bc:4c (3c:52:82:e5:bc:4c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)						
▼ Address Resolution Protocol (request/gratuitous ARP)						
Hardware type: Ethernet (1)						
Protocol type: IPv4 (0x0800)						
Hardware size: 6						
Protocol size: 4						
Opcode: request (1)						
[is gratuitous: true]						
Sender MAC address: HewlettP_e5:bc:4c (3c:52:82:e5:bc:4c)						
Sender IP address: 192.168.100.156						
Target MAC address: Broadcast (ff:ff:ff:ff:ff:ff)						
Target IP address: 192.168.100.156						

Figure 13: ARP Gratuito.

3 Domínios de colisão

3.1 Faça ping de n1 para n2. Verifique com a opção tcpdump como flui o tráfego nas diversas interfaces dos vários dispositivos. Que conclui?

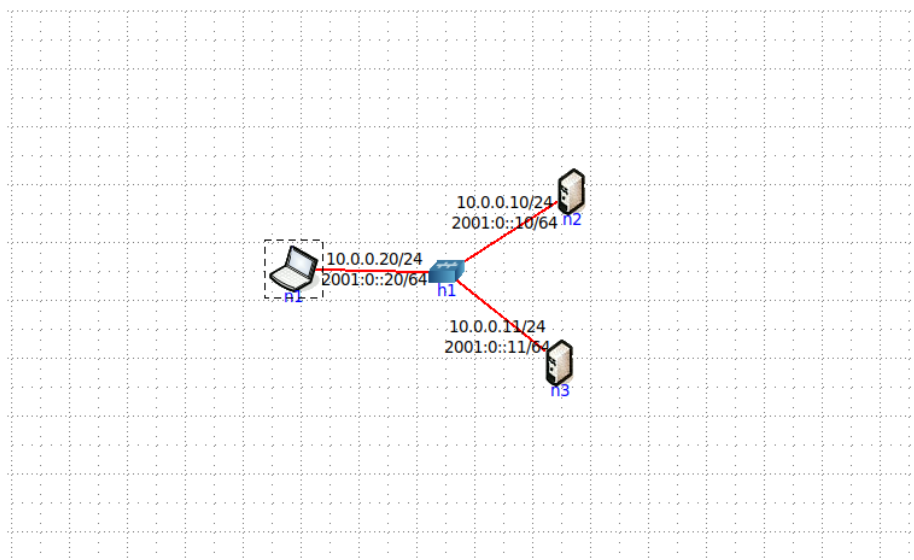


Figure 14: Mensagem ARP.


```
root@n1:/tmp/pycore.45533/n1.conf# ping 10.0.0.10
PING 10.0.0.10 (10.0.0.10) 56(84) bytes of data.
64 bytes from 10.0.0.10: icmp_seq=1 ttl=64 time=0.196 ms
64 bytes from 10.0.0.10: icmp_seq=2 ttl=64 time=0.129 ms
^C
--- 10.0.0.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1005ms
rtt min/avg/max/mdev = 0.129/0.162/0.196/0.035 ms
root@n1:/tmp/pycore.45533/n1.conf#
```

Figure 17: ping de n1 para n2

[illegible]

Figure 18: tcpdump no servidor n3.

[illegible]

Figure 19: tcpdump no servidor n2.

Nas figuras apresentadas anteriormente, é possível observar que ao fazer ping do laptop n1 para o servidor n2, os pacotes são todos entregues ao destino pretendido, que neste caso é o n2. Reparámos que, o n3, apenas recebe os protocolos que ele necessita. Tal é possível, pois a mensagem é enviada para o switch que a envia diretamente para o host. Os switches ao limitar o envio da mensagem apenas para o destino pretendido, reduzem a possibilidade de colisão. Assim, podemos concluir que os switches são mais viáveis do que os hubs.

4 Conclusão

Com a realização deste trabalho conseguimos aprofundar conhecimentos acerca dos endereços MAC, ARP, Ethernet e interligações de redes locais. Isto deve-se, ao facto de para a resposta às questões do enunciado termos de efetuar capturas e as fazer as respetivas análises de tramas Ethernet com auxílio do software wireshark.

Utilizamos também a ferramenta CORE para podermos comparara eficácia da utilização dos switchs e hubs na diminuição de colisões de tramas Ethernet.