

UNIVERSIDADE DO MINHO  
DEPARTAMENTO DE INFORMÁTICA  
REDES DE COMPUTADORES

Trabalho 3

Simão Brito (A89482)  
António Silva (A89558)  
José Martins (A90122)

1 de fevereiro de 2021



Simão Brito A89482



António Silva A89558



José Martins A90122

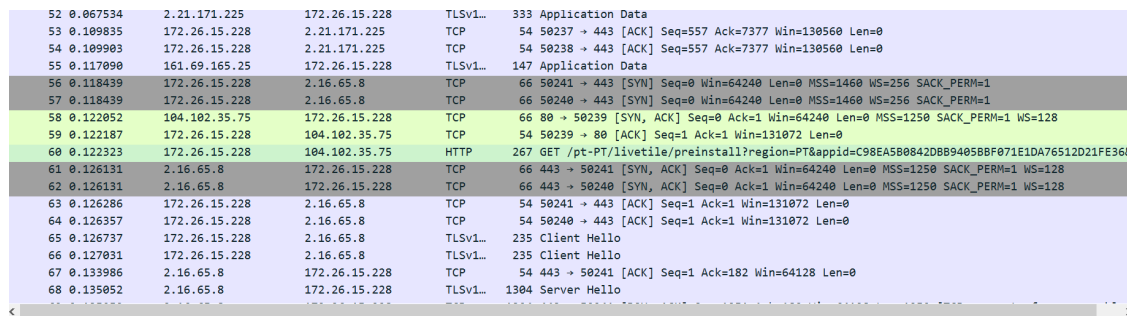
# Conteúdo

<b>1</b>	<b>Captura e Análise de Tramas Ethernet</b>	<b>4</b>
1.1	Obtenha o número de ordem da sequência de bytes capturada (coluna da esquerda na janela do Wireshark) correspondente à mensagem HTTP GET enviada pelo seu computador para o servidor Web, bem como o começo da respectiva mensagem HTTP Response proveniente do servidor. . . . .	4
1.2	1. Anote os endereços MAC de origem e de destino da trama capturada. . . . .	5
1.3	2. Identifique a que sistemas se referem. Justifique. . . . .	5
1.4	3. Qual o valor hexadecimal do campo Type da trama Ethernet? O que significa? . . . . .	5
1.5	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. . . . .	6
1.6	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)). . . . .	7
1.7	6. Qual é o endereço Ethernet da fonte? A que sistema de rede corresponde? Justifique. . . . .	7
1.8	7. Qual é o endereço MAC do destino? A que sistema corresponde? . . . . .	7
1.9	8. Atendendo ao conceito de desencapsulamento protocolar, identifique os vários protocolos contidos na trama recebida. . . . .	7
<b>2</b>	<b>Protocolo ARP</b>	<b>8</b>
2.1	9. Observe o conteúdo da tabela ARP. Diga o que significa cada uma das colunas . . . . .	8
2.1.1	No sentido de observar o envio e recepção de mensagens ARP, é conveniente apagar o conteúdo da cache ARP. Caso contrario, é provável que a associação entre endereços IP e MAC já exista em cache. . . . .	9
2.2	10. 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? . . . . .	9
2.3	11. Qual o valor hexadecimal do campo tipo da trama Ethernet? O que indica? . . . . .	10
2.4	12. Como pode confirmar que se trata efetivamente de um pedido ARP? Identifique que tipo de endereços estão contidos na mensagem ARP? Que conclui? . . . . .	10
2.5	13. Explícite que tipo de pedido ou pergunta é feita pelo host de origem? . . . . .	10
2.6	14. Localize a mensagem ARP que é a resposta ao pedido ARP efetuado. . . . .	11
2.6.1	a. Qual o valor do campo ARP opcode? O que especifica? . . . . .	11
2.6.2	b. Em que posição da mensagem ARP está a resposta ao pedido ARP ? . . . . .	11
<b>3</b>	<b>ARP Gratuito</b>	<b>12</b>
3.1	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 gratuito enviado? . . . . .	12

3.2	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. . . . .	13
<b>4</b>	<b>Conclusão</b>	<b>15</b>

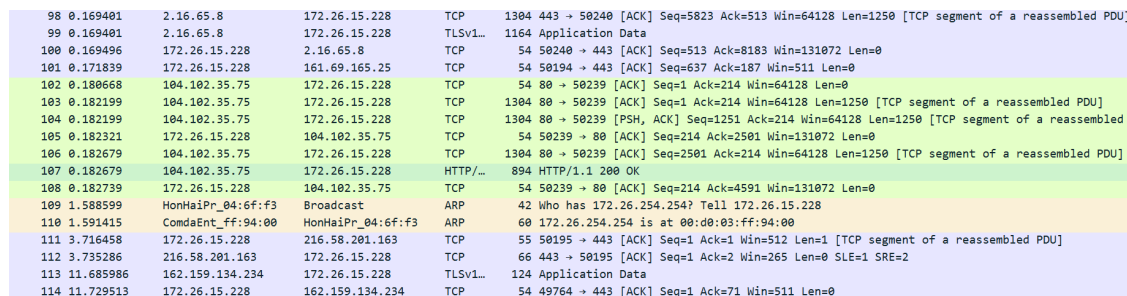
## Captura e Análise de Tramas Ethernet

**1.1 Obtenha o número de ordem da sequência de bytes capturada (coluna da esquerda na janela do Wireshark) correspondente à mensagem HTTP GET enviada pelo seu computador para o servidor Web, bem como o começo da respectiva mensagem HTTP Response proveniente do servidor.**



52	0.067534	2.21.171.225	172.26.15.228	TLsv1_	333 Application Data
53	0.109835	172.26.15.228	2.21.171.225	TCP	54 50237 → 443 [ACK] Seq=557 Ack=7377 Win=130560 Len=0
54	0.109903	172.26.15.228	2.21.171.225	TCP	54 50238 → 443 [ACK] Seq=557 Ack=7377 Win=130560 Len=0
55	0.117090	161.69.165.25	172.26.15.228	TLsv1_	147 Application Data
56	0.118439	172.26.15.228	2.16.65.8	TCP	66 50241 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
57	0.118439	172.26.15.228	2.16.65.8	TCP	66 50240 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
58	0.122052	104.102.35.75	172.26.15.228	TCP	66 80 → 50239 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1250 SACK_PERM=1 WS=128
59	0.122187	172.26.15.228	104.102.35.75	TCP	54 50239 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
60	0.122323	172.26.15.228	104.102.35.75	HTTP	267 GET /pt-PT/livetile/preinstall?region=PT&appid=C98EA5B0842DB894058BF071E1DA76512D21FE368F
61	0.126131	2.16.65.8	172.26.15.228	TCP	66 443 → 50241 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1250 SACK_PERM=1 WS=128
62	0.126131	2.16.65.8	172.26.15.228	TCP	66 443 → 50240 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1250 SACK_PERM=1 WS=128
63	0.126286	172.26.15.228	2.16.65.8	TCP	54 50241 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
64	0.126357	172.26.15.228	2.16.65.8	TCP	54 50240 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
65	0.126737	172.26.15.228	2.16.65.8	TLsv1_	235 Client Hello
66	0.127031	172.26.15.228	2.16.65.8	TLsv1_	235 Client Hello
67	0.133906	2.16.65.8	172.26.15.228	TCP	54 443 → 50241 [ACK] Seq=1 Ack=182 Win=64128 Len=0
68	0.135052	2.16.65.8	172.26.15.228	TLsv1_	1304 Server Hello

Figura 1.1: Análise de Tramas Ethernet onde é possível identificar o número de ordem da mensagem HTTP GET



98	0.169401	2.16.65.8	172.26.15.228	TCP	1304 443 → 50240 [ACK] Seq=5823 Ack=513 Win=64128 Len=1250 [TCP segment of a reassembled PDU]
99	0.169401	2.16.65.8	172.26.15.228	TLsv1_	1164 Application Data
100	0.169496	172.26.15.228	2.16.65.8	TCP	54 50240 → 443 [ACK] Seq=513 Ack=8183 Win=131072 Len=0
101	0.171839	172.26.15.228	161.69.165.25	TCP	54 50194 → 443 [ACK] Seq=637 Ack=187 Win=511 Len=0
102	0.180668	104.102.35.75	172.26.15.228	TCP	54 80 → 50239 [ACK] Seq=1 Ack=214 Win=64128 Len=0
103	0.182199	104.102.35.75	172.26.15.228	TCP	1304 80 → 50239 [ACK] Seq=1 Ack=214 Win=64128 Len=1250 [TCP segment of a reassembled PDU]
104	0.182199	104.102.35.75	172.26.15.228	TCP	1304 80 → 50239 [PSH, ACK] Seq=1251 Ack=214 Win=64128 Len=1250 [TCP segment of a reassembled PDU]
105	0.182321	172.26.15.228	104.102.35.75	TCP	54 50239 → 80 [ACK] Seq=214 Ack=2501 Win=131072 Len=0
106	0.182679	104.102.35.75	172.26.15.228	TCP	1304 80 → 50239 [ACK] Seq=2501 Ack=214 Win=64128 Len=1250 [TCP segment of a reassembled PDU]
107	0.182679	104.102.35.75	172.26.15.228	HTTP/_	894 HTTP/1.1 200 OK
108	0.182739	172.26.15.228	104.102.35.75	TCP	54 50239 → 80 [ACK] Seq=214 Ack=4591 Win=131072 Len=0
109	1.588599	HonHaiPr_04:6f:f3	Broadcast	ARP	42 Who has 172.26.254.254? Tell 172.26.15.228
110	1.591415	ComdaEnt_ff:94:00	HonHaiPr_04:6f:f3	ARP	60 172.26.254.254 is at 00:d0:03:ff:94:00
111	3.716458	172.26.15.228	216.58.201.163	TCP	55 50195 → 443 [ACK] Seq=1 Ack=1 Win=512 Len=1 [TCP segment of a reassembled PDU]
112	3.735286	216.58.201.163	172.26.15.228	TCP	66 443 → 50195 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE=2
113	11.685986	162.159.134.234	172.26.15.228	TLsv1_	124 Application Data
114	11.729513	172.26.15.228	162.159.134.234	TCP	54 49764 → 443 [ACK] Seq=1 Ack=71 Win=511 Len=0

Figura 1.2: Análise de Tramas Ethernet onde é possível identificar o número de ordem da mensagem HTTP Response

Na Fig 1.1 é possível identificar que o número de ordem da sequência de bytes capturada correspondente à mensagem HTTP GET é 60. Do mesmo modo, na Fig 1.2 é identificável que o número de ordem correspondente à mensagem HTTP Response é 107.

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

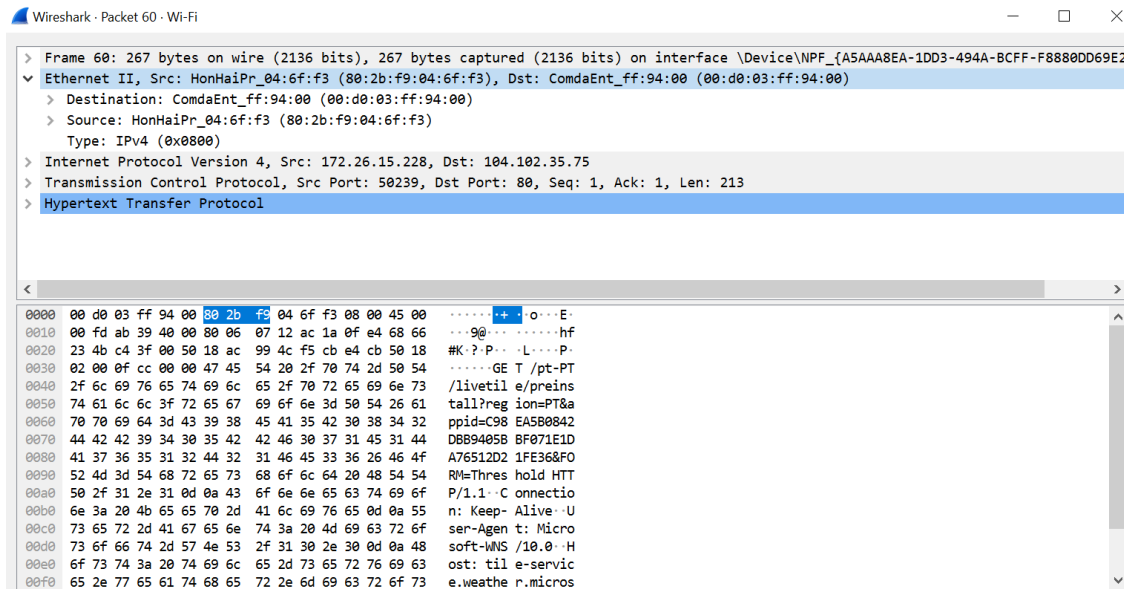


Figura 1.3: Cabeçalho da trama Ethernet que contém a mensagem HTTP GET

O endereço MAC de origem é: 80:2b:f9:04:6f:f3.

O endereço MAC de destino é: 00:d0:03:ff:94:00.

## 1.3 2. Identifique a que sistemas se referem. Justifique.

O primeiro refere-se ao endereço da interface de ethernet do nosso computador. O segundo refere-se ao endereço da interface do router da rede local. O endereço de origem representa o local, a partir do qual é enviada a trama e por isso corresponde à interface da nossa máquina. Uma vez que a nossa máquina não tem conhecimento sobre endereços externos à rede local, então o endereço de destino corresponde à interface do router da rede local.

## 1.4 3. Qual o valor hexadecimal do campo Type da trama Ethernet? O que significa?

Como se pode ver na Figura 1.3 o valor hexadecimal do campo Type é 0x0800. Significa que encapsula um pacote IPV4.

1.5 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.

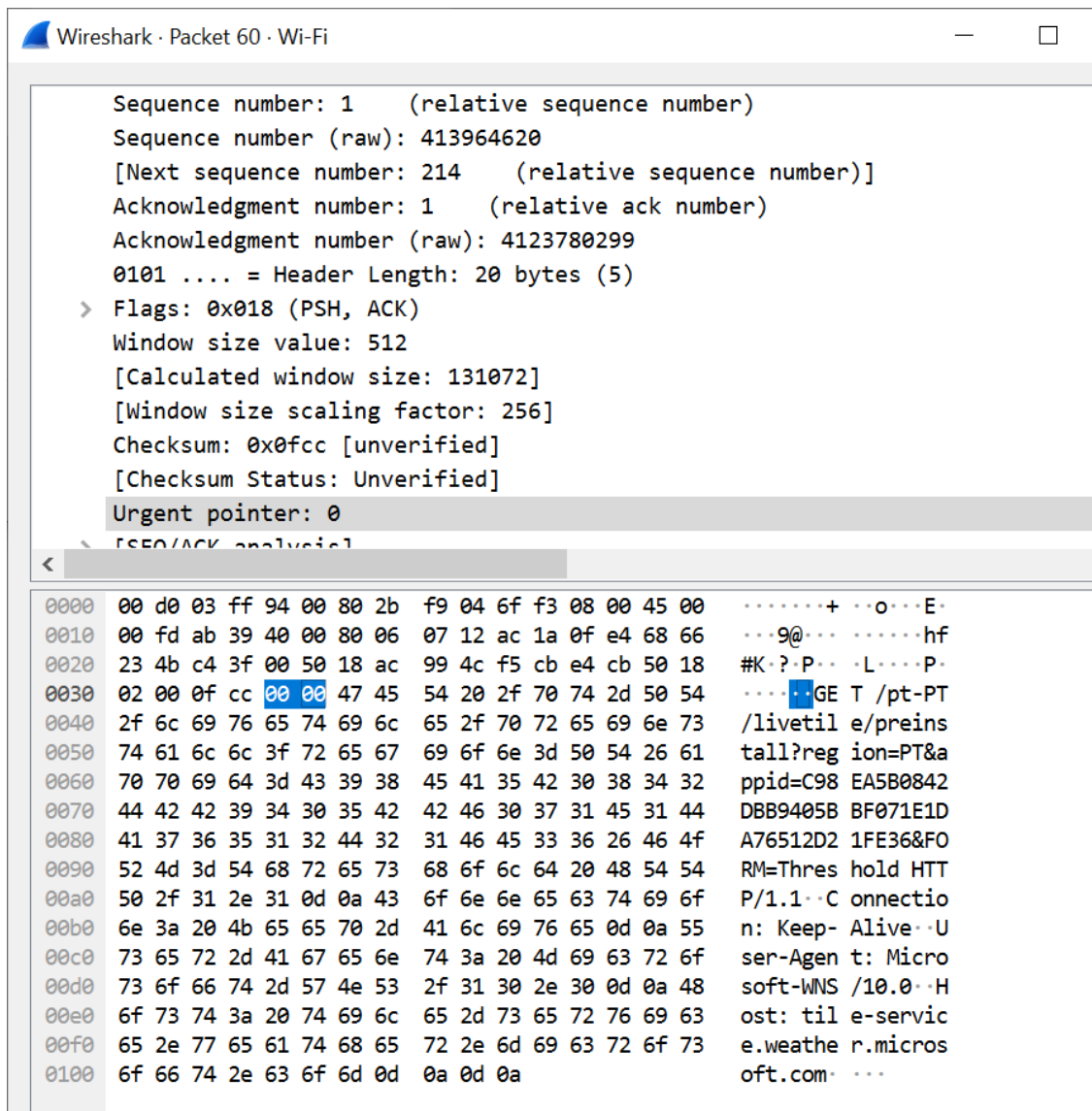


Figura 1.4

Como vemos na Figura 1.4, se contarmos os bytes até a zona selecionada concluímos que o cabeçalho da trama Ethernet tem 54 bytes.

$54/267 = 20,2$ (em percentagem)

Através do calculo efetuado acima podemos afirmar que temos uma percentagem de 20,2 de sobrecarga introduzida pela pilha protocolar no envio do HTTP GET.

## 1.6 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)).

O campo FCS(Frame Check Sequence) não aparece na trama capturada. Posto isto, concluímos que não foi utilizada, uma vez que a rede ethernet é pouco suscetível a erros.

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

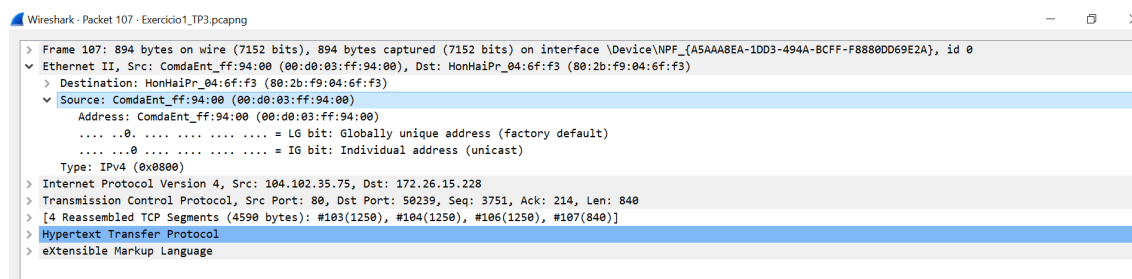


Figura 1.5: Cabeçalho da trama Ethernet que contém a o primeiro byte da mensagem HTTP Response

O endereço Ethernet da fonte é 00:d0:03:ff:94:00. Corresponde ao endereço do router da rede local, com o qual estamos a comunicar

## 1.8 7. Qual é o endereço MAC do destino? A que sistema corresponde?

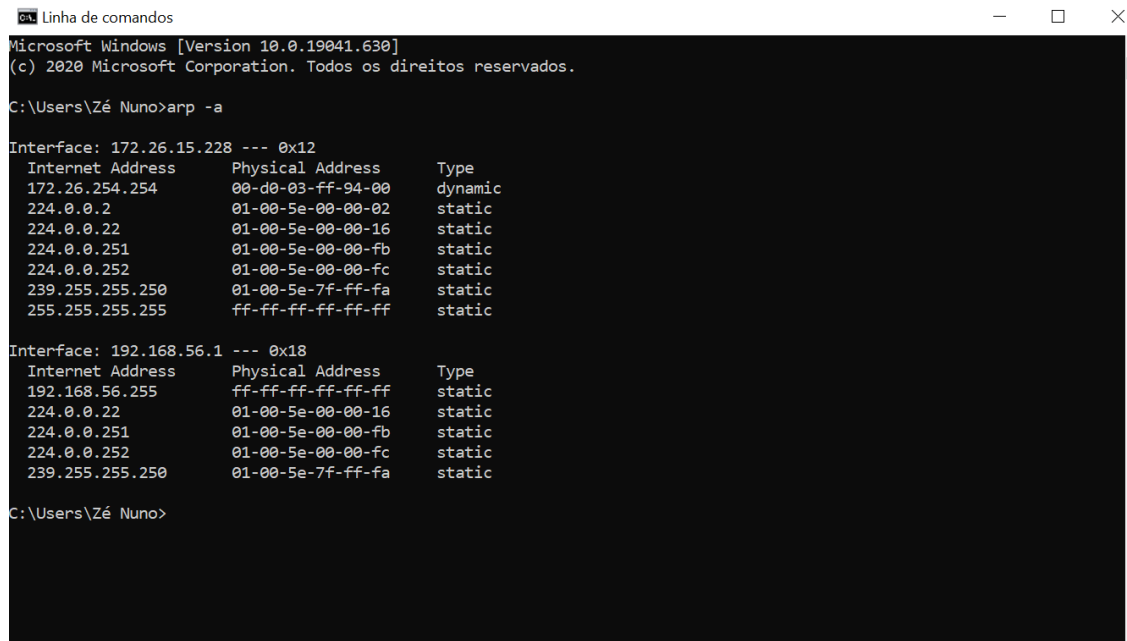
O endereço MAC de destino é: 80:2b:f9:04:6f:f3. Este sistema corresponde à interface de ethernet do nosso computador.

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

Os protocolos que conseguimos identificar na trama recebida foram os seguintes: HTTP (Hypertext Transfer Protocol), Ethernet II, IPV4 (Internet Protocol Version 4) e TCP(Transmission Control Protocol).

## Protocolo ARP

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



```
Microsoft Windows [Version 10.0.19041.630]
(c) 2020 Microsoft Corporation. Todos os direitos reservados.

C:\Users\Zé Nuno>arp -a

Interface: 172.26.15.228 --- 0x12
Internet Address      Physical Address      Type
172.26.254.254        00-d0-03-ff-94-00    dynamic
224.0.0.2             01-00-5e-00-00-02    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: 192.168.56.1 --- 0x18
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

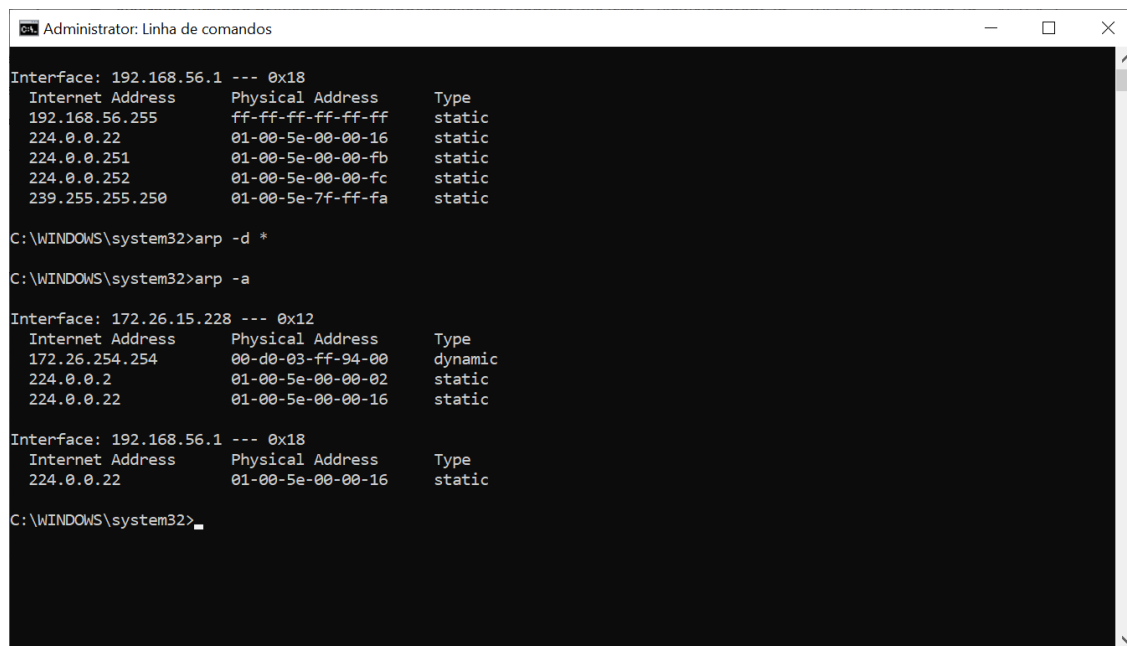
C:\Users\Zé Nuno>
```

Figura 2.1: Execução do comando arp -a

A primeira coluna refere-se ao endereço IP do host. A segunda representa o MAC address que lhe corresponde. Por sua vez a terceira coluna evidencia o tipo de encaminhamento efetuado(dinâmico ou estático).



2.1.1 No sentido de observar o envio e recepção de mensagens ARP, é conveniente apagar o conteúdo da cache ARP. Caso contrario, é provável que a associação entre endereços IP e MAC já exista em cache.



```
Administrator: Linha de comandos

Interface: 192.168.56.1 --- 0x18
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

C:\WINDOWS\system32>arp -d *

C:\WINDOWS\system32>arp -a

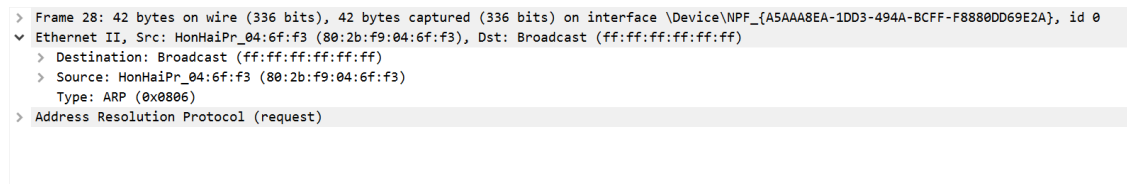
Interface: 172.26.15.228 --- 0x12
Internet Address      Physical Address      Type
172.26.254.254        00-d0-03-ff-94-00     dynamic
224.0.0.2             01-00-5e-00-00-02     static
224.0.0.22            01-00-5e-00-00-16     static

Interface: 192.168.56.1 --- 0x18
Internet Address      Physical Address      Type
224.0.0.22            01-00-5e-00-00-16     static

C:\WINDOWS\system32>
```

Figura 2.2: Execução do comando arp -d \* seguido do comando arp -a

2.2 10. 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?



```
> Frame 28: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{A5AAA8EA-1DD3-494A-BCFF-F8880DD69E2A}, id 0
▼ Ethernet II, Src: HonHaiPr_04:6f:f3 (80:2b:f9:04:6f:f3), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: HonHaiPr_04:6f:f3 (80:2b:f9:04:6f:f3)
    Type: ARP (0x0806)
  > Address Resolution Protocol (request)
```

Figura 2.3

O valor hexadecimal dos endereços origem e destino são 80:2b:f9:04:6f:f3 e ff:ff:ff:ff:ff:ff respectivamente. Quando o valor hexadecimal do endereço destino é ff:ff:ff:ff:ff:ff(Broadcast), então todos

os nós da rede recebem e processam a trama. Assim sendo este endereço é usado que possa ser recebido por todos os hosts da rede.

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

Como se pode ver na figura da alínea anterior, o valor hexadecimal do campo tipo é 0x0806. Indica que encapsula uma frame ARP.

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

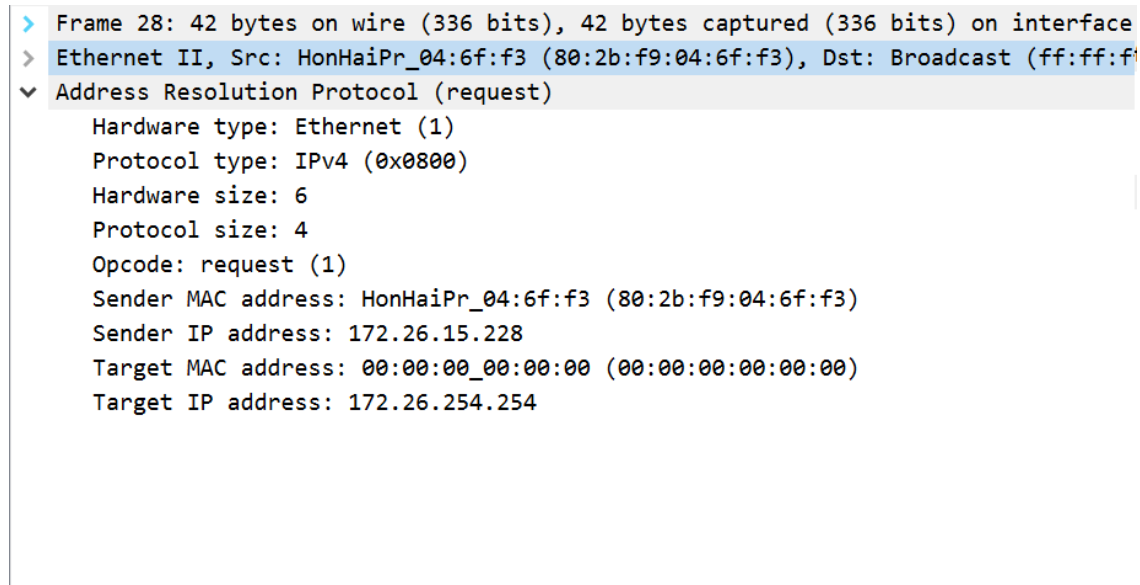


Figura 2.4

Observando a Fig 2.4, podemos confirmar que se trata de um pedido ARP uma vez que o campo Opcode sinaliza uma “request” ou seja um pedido. Estão contidos na mensagem ARP endereços IP(Sender IP e Target IP) e endereços MAC(Sender MAC e Target MAC). Tal como se pode ver na figura o host com endereço IP 172.26.15.228 e MAC 80:2b:f9:04:6f:f3 quer saber qual o endereço MAC do host com IP 172.26.254.254 então o target MAC é o endereço de BroadCast.

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

O host de origem pergunta aos hosts da rede qual o mac do host cujo endereço IP é 172.26.254.254.

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

```
> Frame 29: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface
> Ethernet II, Src: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00), Dst: HonHaiPr_04:6f:f3
✓ 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_04:6f:f3 (80:2b:f9:04:6f:f3)
  Target IP address: 172.26.15.228
```

Figura 2.5: Mensagem ARP resposta

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

O valor do campo ARP opcode é reply(2). Especifica que é uma resposta(reply) a um pedido anterior(request).

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

A resposta ao pedido ARP está na Sender IP (00:d0:03:ff:94:00) e Sender MAC (172.26.254.254).

## ARP Gratuito

- 3.1 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 gratuito enviado?

```
> Frame 68: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{FECDD1F0-A092-4C6A-BD18-2B19591ADEC9}, id 0
> Ethernet II, Src: IntelCor_6b:14:df (30:24:32:6b:14:df), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▼ 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_6b:14:df (30:24:32:6b:14:df)
  Sender IP address: 172.26.97.113
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 172.26.97.113
```

Figura 3.1: ARP gratuito

O que distingue o ARP gratuito dos restantes pedidos ARP é a presença da flag [Is Gratuitous: True] e o Sender IP e Target IP serem iguais.

3.2 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.

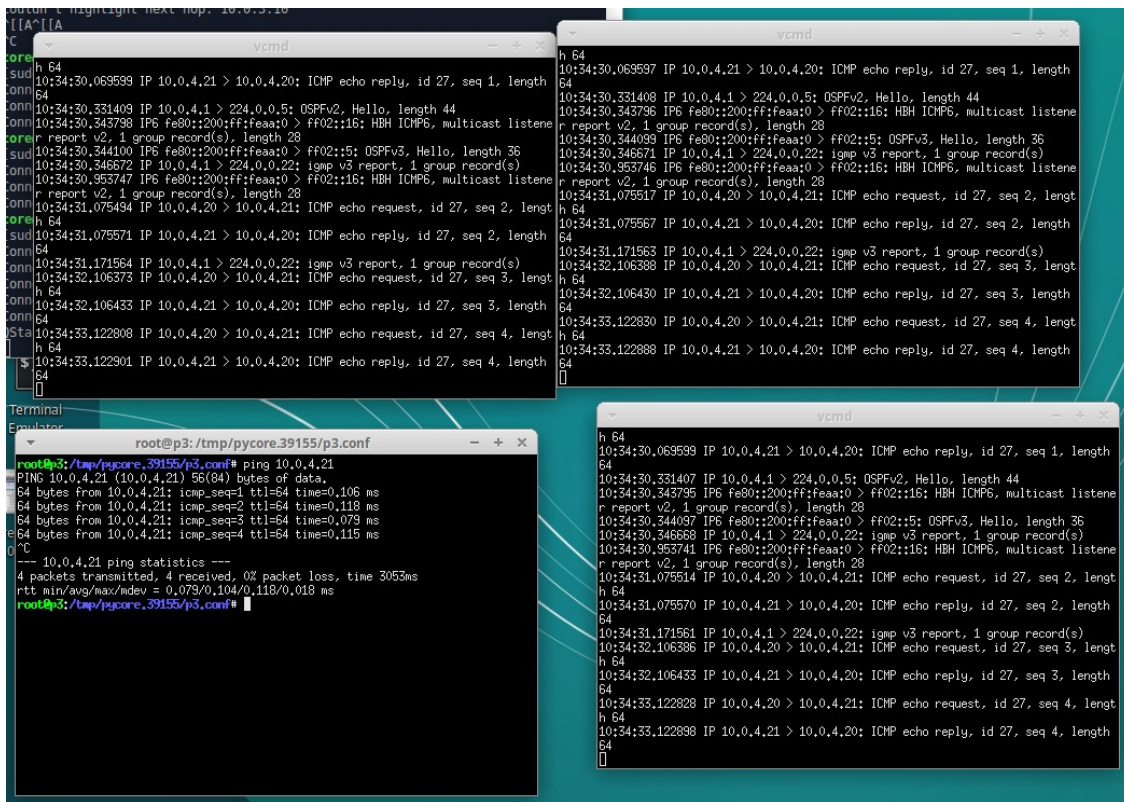
The screenshot displays a network simulation environment with several terminal windows. The top-left window shows the connection status of a 'core-daemon' and the execution of 'sudo core-nui'. The top-right window, titled 'vncmd', shows a list of network events including ICMP echo requests and replies between IP addresses 10.0.3.1 and 10.0.3.21. The bottom-left window shows the output of a 'ping 10.0.3.21' command, indicating successful connectivity with 0% packet loss. The bottom-right window, also titled 'vncmd', shows a 'tcpdump' command being executed on the 'eth0' interface, capturing network traffic.

```

Connecting to "core-daemon" (127.0.0.1:4038)...connected.
Connection to "core-daemon" (127.0.0.1:4038) closed.
Connecting to "core-daemon" (127.0.0.1:4038)...connected.
core@xubuntu:~$ sudo core-nui
[sudo] password for core:
core@xubuntu:~$ sudo core-nui
vncmd
10:26:24.619156 IP 10.0.3.1 > 224.0.0.22: igmp v3 report, 1 group record(s)
10:26:24.619240 IP6 fe80::200:ff:feaa:12 > ff02::5: OSPFv3, Hello, length 36
10:26:24.623898 IP6 fe80::200:ff:feaa:12 > ff02::16: HBH ICMP6, multicast listen
er report v2, 1 group record(s), length 28
10:26:24.687285 IP6 fe80::200:ff:feaa:12 > ff02::16: HBH ICMP6, multicast listen
er report v2, 1 group record(s), length 28
10:26:25.539300 IP 10.0.3.1 > 224.0.0.22: igmp v3 report, 1 group record(s)
10:26:25.539339 IP 10.0.3.1 > 224.0.0.5: OSPFv2, Hello, length 44
10:26:34.612339 IP 10.0.3.1 > 224.0.0.5: OSPFv2, Hello, length 44
10:26:34.619719 IP6 fe80::200:ff:feaa:12 > ff02::5: OSPFv3, Hello, length 36
10:26:36.479659 ARP, Request who-has 10.0.3.21 tell 10.0.3.20, length 28
10:26:36.480056 ARP, Reply 10.0.3.21 is-at 00:00:00:aa:00:08, length 28
10:26:36.480056 IP 10.0.3.20 > 10.0.3.21: ICMP echo request, id 26, seq 1, lengt
h 64
10:26:36.480616 IP 10.0.3.21 > 10.0.3.20: ICMP echo reply, id 26, seq 1, length
64
10:26:37.506740 IP 10.0.3.20 > 10.0.3.21: ICMP echo request, id 26, seq 2, lengt
h 64
10:26:37.507092 IP 10.0.3.21 > 10.0.3.20: ICMP echo reply, id 26, seq 2, length
64
10:26:38.530684 IP 10.0.3.20 > 10.0.3.21: ICMP echo request, id 26, seq 3, lengt
h 64
10:26:38.531044 IP 10.0.3.21 > 10.0.3.20: ICMP echo reply, id 26, seq 3, length
64
Termin
Emulat
64
Screenshot 202
0-10-
root@p1:/tmp/pycore.39155/p1.conf# ping 10.0.3.21
PING 10.0.3.21 (10.0.3.21) 56(84) bytes of data:
64 bytes from 10.0.3.21: icmp_seq=1 ttl=64 time=0.361 ms
64 bytes from 10.0.3.21: icmp_seq=2 ttl=64 time=0.373 ms
64 bytes from 10.0.3.21: icmp_seq=3 ttl=64 time=0.580 ms
^C
--- 10.0.3.21 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2051ms
rtt min/avg/max/mdev = 0.373/0.571/0.961/0.276 ms
root@p1:/tmp/pycore.39155/p1.conf#
vncmd
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
10:26:24.612033 IP 10.0.3.1 > 224.0.0.5: OSPFv2, Hello, length 44
10:26:24.619154 IP 10.0.3.1 > 224.0.0.22: igmp v3 report, 1 group record(s)
10:26:24.619239 IP6 fe80::200:ff:feaa:12 > ff02::5: OSPFv3, Hello, length 36
10:26:24.623888 IP6 fe80::200:ff:feaa:12 > ff02::16: HBH ICMP6, multicast listen
er report v2, 1 group record(s), length 28
10:26:24.687284 IP6 fe80::200:ff:feaa:12 > ff02::16: HBH ICMP6, multicast listen
er report v2, 1 group record(s), length 28
10:26:25.539297 IP 10.0.3.1 > 224.0.0.22: igmp v3 report, 1 group record(s)
10:26:34.612337 IP 10.0.3.1 > 224.0.0.5: OSPFv2, Hello, length 44
10:26:34.619717 IP6 fe80::200:ff:feaa:12 > ff02::5: OSPFv3, Hello, length 36
10:26:36.479903 ARP, Request who-has 10.0.3.21 tell 10.0.3.20, length 28

```

Figura 3.2: Tráfego no departamento A



```
h 64
10:34:30.069599 IP 10.0.4.21 > 10.0.4.20: ICMP echo reply, id 27, seq 1, length 64
10:34:30.331409 IP 10.0.4.1 > 224.0.0.5: OSPFv2, Hello, length 44
10:34:30.343798 IP6 fe80::200:ff:feaa:0 > ff02::16: HBH ICMP6, multicast listen
r report v2, 1 group record(s), length 28
10:34:30.344099 IP6 fe80::200:ff:feaa:0 > ff02::5: OSPFv3, Hello, length 36
10:34:30.346671 IP 10.0.4.1 > 224.0.0.22: igmp v3 report, 1 group record(s)
10:34:30.346672 IP 10.0.4.1 > 224.0.0.22: igmp v3 report, 1 group record(s)
10:34:30.353747 IP6 fe80::200:ff:feaa:0 > ff02::16: HBH ICMP6, multicast listen
r report v2, 1 group record(s), length 28
10:34:31.075494 IP 10.0.4.20 > 10.0.4.21: ICMP echo request, id 27, seq 2, length 64
10:34:31.075671 IP 10.0.4.21 > 10.0.4.20: ICMP echo reply, id 27, seq 2, length 64
10:34:31.171564 IP 10.0.4.1 > 224.0.0.22: igmp v3 report, 1 group record(s)
10:34:32.106373 IP 10.0.4.20 > 10.0.4.21: ICMP echo request, id 27, seq 3, length 64
10:34:32.106433 IP 10.0.4.21 > 10.0.4.20: ICMP echo reply, id 27, seq 3, length 64
10:34:33.122808 IP 10.0.4.20 > 10.0.4.21: ICMP echo request, id 27, seq 4, length 64
10:34:33.122901 IP 10.0.4.21 > 10.0.4.20: ICMP echo reply, id 27, seq 4, length 64

root@p3:/tmp/pycore.39155/p3.conf# ping 10.0.4.21
PING 10.0.4.21 (10.0.4.21) 56(84) bytes of data,
64 bytes from 10.0.4.21: icmp_seq=1 ttl=64 time=0.106 ms
64 bytes from 10.0.4.21: icmp_seq=2 ttl=64 time=0.118 ms
64 bytes from 10.0.4.21: icmp_seq=3 ttl=64 time=0.079 ms
64 bytes from 10.0.4.21: icmp_seq=4 ttl=64 time=0.115 ms
--- 10.0.4.21 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3053ms
rtt min/avg/max/mdev = 0.079/0.104/0.118/0.018 ms
root@p3:/tmp/pycore.39155/p3.conf#
```

Figura 3.3: Trafego no departamento B

Como se pode verificar, no departamento B (departamento que tem o hub), analisando o tráfego de um host, apesar de não ser o destino da comunicação, recebe-a na mesma. De forma contrária, com a presença do switch em vez do hub no departamento A, reparamos que o host já não recebe o tráfego de p1 para p2.

## Conclusão

Mais uma vez, o trabalho prático ajudou a completar o conhecimento sobre a matéria lecionada nas aulas teóricas.

Com a sua realização, aprofundamos o nosso conhecimento relativo à camada de ligação lógica (Ethernet e Protocolo ARP).

Ficou de melhor forma perceptível a forma como são partilhados os endereços MAC nas redes locais, com a utilização de Protocolo ARP, utilizado para a transformação de endereços da camada Internet em endereços da camada de Link.

Por fim, foi-nos permitido analisar o funcionamento dos domínios de colisão e sua respetiva correção através da utilização de um switch de rede.

Em suma, todos o capítulo de Link Layer e conceitos a ele correspondentes foram abordados ao longo da realização deste trabalho prático. De salientar também, toda a informação contida no enunciado que ajudou na resposta às respetivas perguntas.