



UNIVERSIDADE DO MINHO

DEPARTAMENTO DE INFORMÁTICA

Redes de Computadores
Trabalho Prático 3

—
Grupo N^o 10

Ariana Lousada (A87998)
Rui Armada (A90468)
Sofia Santos (A89615)

4 de junho de 2022

Conteúdo

1	Questões e Respostas	3
1.1	Captura e análise de Tramas Ethernet	3
1.2	Protocolo ARP	5
1.3	ARP Gratuito	8
1.4	Domínios de colisão	8
2	Conclusão e Análise de Resultados	12

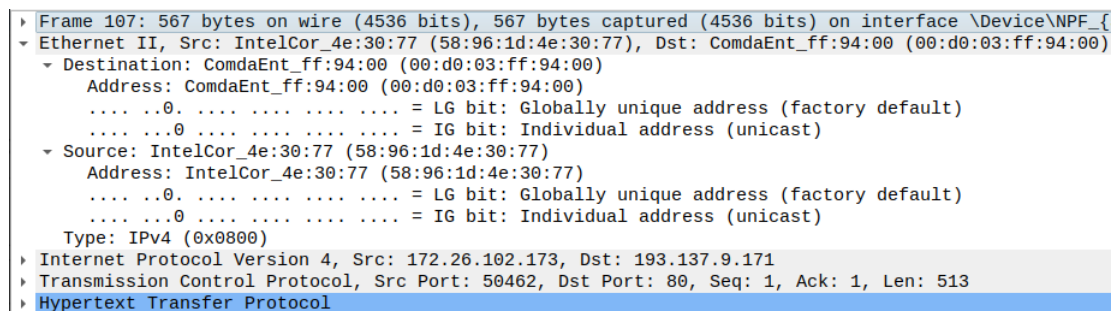
Capítulo 1

Questões e Respostas

Para a resolução deste trabalho, foram-nos propostas várias questões, as quais vamos passar a responder neste capítulo:

1.1 Captura e análise de Tramas Ethernet

- 1) **Anote os endereços MAC de origem e de destino da trama capturada.**



```

Frame 107: 567 bytes on wire (4536 bits), 567 bytes captured (4536 bits) on interface \Device\NPF_{...}
Ethernet II, Src: IntelCor_4e:30:77 (58:96:1d:4e:30:77), Dst: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
  Destination: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
    Address: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  Source: IntelCor_4e:30:77 (58:96:1d:4e:30:77)
    Address: IntelCor_4e:30:77 (58:96:1d:4e:30:77)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 172.26.102.173, Dst: 193.137.9.171
Transmission Control Protocol, Src Port: 50462, Dst Port: 80, Seq: 1, Ack: 1, Len: 513
Hypertext Transfer Protocol

```

Figura 1.1: Trama capturada (HTTP Get)

O endereço MAC de origem é 58:96:1d:4e:30:77 e o endereço MAC de destino é 00:d0:03:ff:94:00.

- 2) **Identifique a que sistemas se referem. Justifique.**

O campo Source refere-se à interface da nossa máquina nativa e o campo Destination corresponde ao router da rede local à qual estamos ligados.

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

Como podemos observar na figura 1.1, o campo Type da trama Ethernet tem o valor 0x0800, que indica que o protocolo utilizado ao nível da rede é o IPv4.

- 4) Quantos bytes são usados desde o início da trama até ao caracteres ASCII “G” do método HTTP GET? Calcule e indique, em percentagem, a sobrecarga (overhead) introduzida pela pilha protocolar no envio do HTTP GET.

0000	00 d0 03 ff 94 00 58 96 1d 4e 30 77 08 00 45 b8X. .N0w..E.
0010	02 29 36 ba 40 00 80 06 00 00 ac 1a 66 ad c1 89	.)6.@... ..f...
0020	09 ab c5 1e 00 50 e3 a0 dc 4e a2 5e 52 50 50 18P... .N^RPP.
0030	01 02 f8 55 00 00 47 45 54 20 2f 20 48 54 54 50	...U...GE T / HTTP
0040	2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 61 6c 75 6e	/1.1..Ho st: alun
0050	6f 73 2e 75 6d 69 6e 68 6f 2e 70 74 0d 0a 43 6f	os.uminh o.pt..Co
0060	6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61	nnnection : keep-a
0070	6c 69 76 65 0d 0a 55 70 67 72 61 64 65 2d 49 6e	live..Up grade-In
0080	73 65 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a	secure-R equests:
0090	20 31 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20	1..User -Agent:
00a0	4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e	Mozilla/ 5.0 (Win
00b0	64 6f 77 73 20 4e 54 20 31 30 2e 30 3b 20 57 69	dows NT 10.0; Wi
00c0	6e 36 34 3b 20 78 36 34 29 20 41 70 70 6c 65 57	n64; x64) Applew
00d0	65 62 4b 69 74 2f 35 33 37 2e 33 36 20 28 4b 48	ebKit/53 7.36 (KH
00e0	54 4d 4c 2c 20 6c 69 6b 65 20 47 65 63 6b 6f 29	TML, lik e Gecko)

Bytes 54-56: Request Method (http.request.method)

Figura 1.2: Pacote em hexadecimal e texto

Como é possível ver na figura 1.2, o carácter 'G' corresponde ao byte 54 (contado a partir do 0), logo são usados 54 bytes desde o início da trama. Tendo o pacote 567 bytes, isto traduz-se num overhead de aproximadamente 9,5%.

- 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)).

Após visualização direta e utilizando um filtro, não nos foi possível encontrar o campo FCS. Isto indica-nos que não foram detetados erros.

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

▶	Frame 108: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits) on interface \Device\NPF_{
▼	Ethernet II, Src: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00), Dst: IntelCor_4e:30:77 (58:96:1d:4e:30:77)
▼	Destination: IntelCor_4e:30:77 (58:96:1d:4e:30:77)
	Address: IntelCor_4e:30:77 (58:96:1d:4e:30:77)
0. = LG bit: Globally unique address (factory default)
0. = IG bit: Individual address (unicast)
▼	Source: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
	Address: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)
0. = LG bit: Globally unique address (factory default)
0. = IG bit: Individual address (unicast)
	Type: IPv4 (0x0800)
▶	Internet Protocol Version 4, Src: 193.137.9.171, Dst: 172.26.102.173
▶	Transmission Control Protocol, Src Port: 80, Dst Port: 50462, Seq: 1, Ack: 514, Len: 129
▶	Hypertext Transfer Protocol

Figura 1.3: Trama capturada (Resposta)

O endereço da fonte é 00:d0:03:ff:94:00, correspondendo ao router da rede local à qual estamos ligados.

- 7) **Qual é o endereço MAC do destino? A que sistema corresponde?**
 O endereço do destino é 58:96:1d:4e:30:77, correspondendo à interface da nossa máquina nativa.
- 8) **Atendendo ao conceito de desencapsulamento protocolar, identifique os vários protocolos contidos na trama recebida.**
 Os protocolos contidos na trama recebida são: Ethernet II, Internet Protocol Version 4 (IPv4), Transmission Control Protocol (TCP) e Hypertext Transfer Protocol (HTTP).

1.2 Protocolo ARP

- 9) **Observe o conteúdo da tabela ARP. Diga o que significa cada uma das colunas.**

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

Interface: 172.26.102.173 --- 0x8		
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
Interface: 192.168.56.1 --- 0xc		
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

Figura 1.4: Tabela ARP

Ao observarmos a tabela, é possível concluir que a primeira coluna representa os endereços IP, a segunda os correspondentes endereços MAC e a terceira o tipo de entrada da tabela (dinâmica ou estática). O tipo de entrada indica se a entrada é temporária (dinâmica) ou permanente (estática).

- 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?.

428	3.765450	IntelCor_4e:30:77	Broadcast	ARP	42 Who has 172.26.254.254? Tell 172.26.102.173
433	3.807688	ComdaEnt_ff:94:00	IntelCor_4e:30:77	ARP	60 172.26.254.254 is at 00:d0:03:ff:94:00


```

Frame 428: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{5515C8A4-1FDA-4B3E-B85D-F3...}
Ethernet II, Src: IntelCor_4e:30:77 (58:96:1d:4e:30:77), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  Source: IntelCor_4e:30:77 (58:96:1d:4e:30:77)
  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_4e:30:77 (58:96:1d:4e:30:77)
  Sender IP address: 172.26.102.173
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 172.26.254.254

```

Figura 1.5: Pedido ARP

Na trama ethernet, podemos verificar que o endereço de origem e destino são respetivamente 58:96:1d:4e:30:77 e ff:ff:ff:ff:ff:ff. O endereço de destino corresponde ao endereço de broadcast e é utilizado para que todos os endereços conectados à rede recebam o pedido.

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

Ao observarmos a figura 1.5, é possível verificar que o campo Type tem o valor 0x0806, o que por sua vez indica que o campos de dados pertence ao ARP.

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

A mensagem ARP contém os endereços IP quer do destino quer da origem, sendo que se trata de um ARP request então acaba também por mostrar o endereço MAC do endereço IP da origem e do destino.

- 13) Explícite que tipo de pedido ou pergunta é feita pelo host de origem?

A pergunta realizada pela nossa máquina é "Who has 172.26.254.254? Tell 172.26.102.173", ou seja, "Quem tem 172.26.254.254? Digam a 172.26.102.173". Assim sendo, como resposta iremos obter o endereço MAC do equipamento que tiver o endereço indicado na pergunta (172.26.254.254).

- 14) Localize a mensagem ARP que é a resposta ao pedido ARP efetuado.

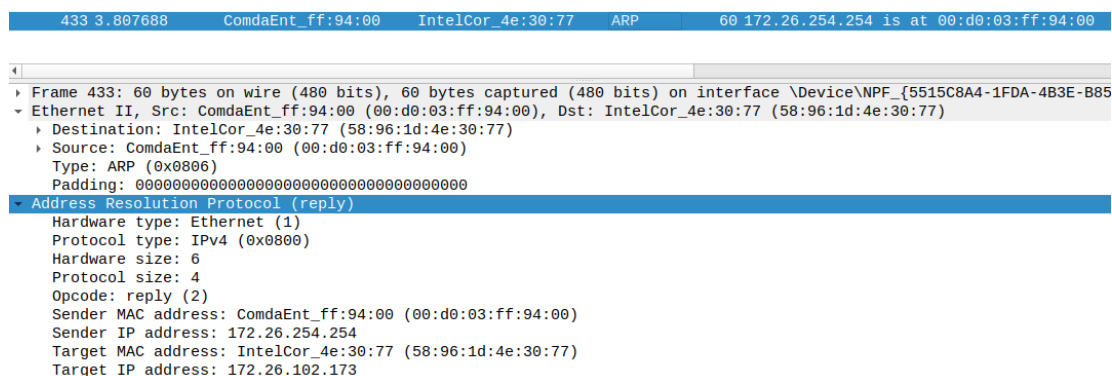


Figura 1.6: Resposta ao pedido ARP

- 14.a) Qual o valor do campo ARP opcode? O que especifica?.

O valor do campo ARP Opcode é 2, que indica que se trata de uma resposta ARP.

- 14.b) Em que posição da mensagem ARP está a resposta ao pedido ARP?

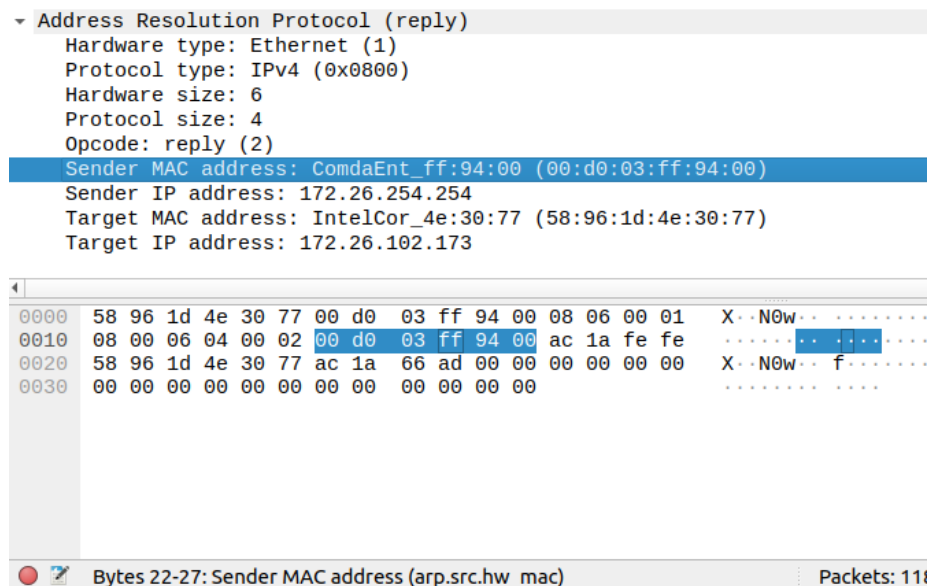
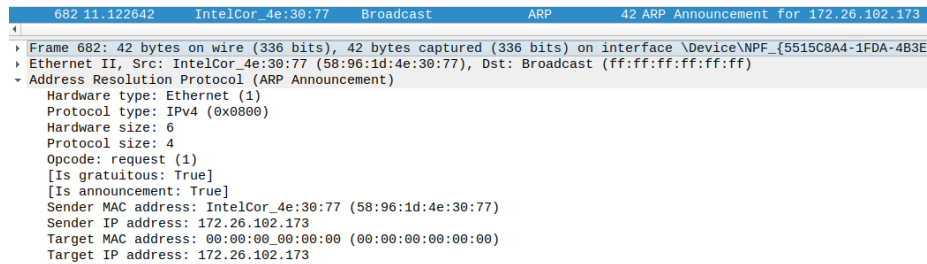


Figura 1.7: Posição da resposta da mensagem ARP

A resposta ao pedido ARP está nos bytes 22-27, sendo que a mensagem ARP começa no byte 14, logo a resposta encontra-se nos bytes 9 a 14 da mensagem ARP.

1.3 ARP Gratuito

- 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?



```
682 11.122642 IntelCor_4e:30:77 Broadcast ARP 42 ARP Announcement for 172.26.102.173
1
Frame 682: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{5515C8A4-1FDA-4B3E...}
Ethernet II, Src: IntelCor_4e:30:77 (58:96:1d:4e:30:77), 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_4e:30:77 (58:96:1d:4e:30:77)
  Sender IP address: 172.26.102.173
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 172.26.102.173
```

Figura 1.8: Captura do ARP gratuito

O que distingue um pedido ARP gratuito dos restantes pedidos ARP é: a flag *Is Gratuitous* a True e o sender e target IP serem o mesmo. O resultado esperado será não obter resposta. Caso se obtenha resposta, isso significa que existe outro host na rede com o mesmo endereço.

1.4 Domínios de colisão

- 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.

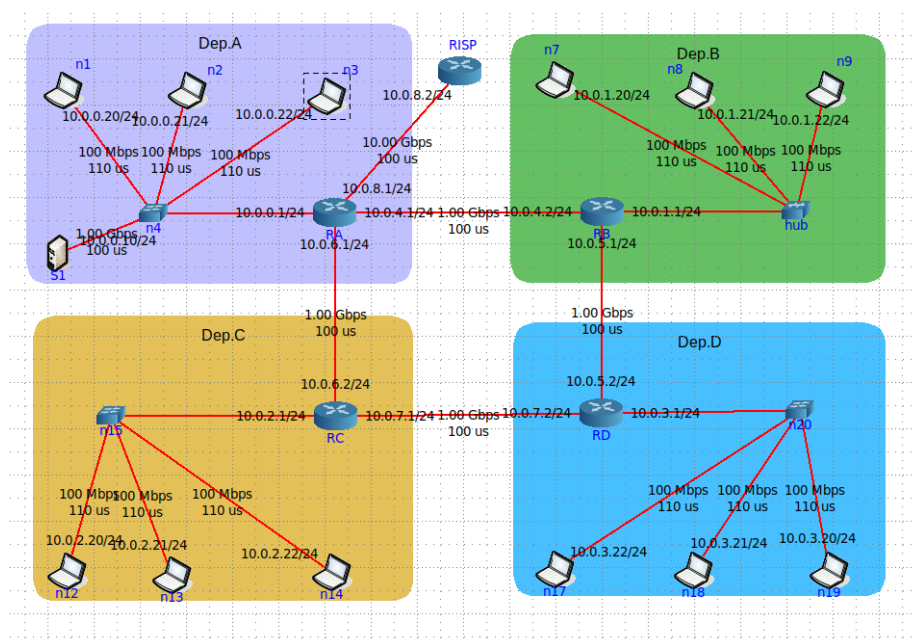


Figura 1.9: Topologia do TP2 alterada

```

root@n2: /tmp/pycore.36177/n2.conf
root@n2: /tmp/pycore.36177/n2.conf# tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C15:51:17.341367 IP 10.0.0.1 > 224.0.0.5: OSPFv2, Hello, length 44
15:51:17.611398 IP6 fe80::200:ff:feaa:4 > ff02::5: OSPFv3, Hello, length 36
15:51:22.603639 IP6 fe80::200:ff:feaa:1 > ip6-allrouters: ICMP6, router solicitation, length 16
15:51:26.597143 ARP, Request who-has 10.0.0.21 tell 10.0.0.20, length 28
15:51:26.597167 ARP, Reply 10.0.0.21 is-at 00:00:00:aa:00:01 (oui Ethernet), length 28
15:51:26.597998 IP 10.0.0.20 > 10.0.0.21: ICMP echo request, id 25, seq 1, length 64
15:51:26.598028 IP 10.0.0.21 > 10.0.0.20: ICMP echo reply, id 25, seq 1, length 64
15:51:27.343001 IP 10.0.0.1 > 224.0.0.5: OSPFv2, Hello, length 44
15:51:27.609548 IP 10.0.0.20 > 10.0.0.21: ICMP echo request, id 25, seq 2, length 64
15:51:27.609587 IP 10.0.0.21 > 10.0.0.20: ICMP echo reply, id 25, seq 2, length 64
15:51:27.617622 IP6 fe80::200:ff:feaa:4 > ff02::5: OSPFv3, Hello, length 36
15:51:28.605564 IP 10.0.0.20 > 10.0.0.21: ICMP echo request, id 25, seq 3, length 64
15:51:28.605612 IP 10.0.0.21 > 10.0.0.20: ICMP echo reply, id 25, seq 3, length 64

13 packets captured
13 packets received by filter
0 packets dropped by kernel
root@n2: /tmp/pycore.36177/n2.conf#

```

Figura 1.10: Execução do tcpdump do dispositivo n2 do Departamento A

```
root@n3: /tmp/pycore.36177/n3.conf# tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C15:51:17.341367 IP 10.0.0.1 > 224.0.0.5: OSPFv2, Hello, length 44
15:51:17.611397 IP6 fe80::200:ff:feaa:4 > ff02::5: OSPFv3, Hello, length 36
15:51:22.603974 IP6 fe80::200:ff:feaa:1 > ip6-allrouters: ICMP6, router solicitation, length 16
15:51:26.597143 ARP, Request who-has 10.0.0.21 tell 10.0.0.20, length 28
15:51:27.343000 IP 10.0.0.1 > 224.0.0.5: OSPFv2, Hello, length 44
15:51:27.617621 IP6 fe80::200:ff:feaa:4 > ff02::5: OSPFv3, Hello, length 36

6 packets captured
6 packets received by filter
0 packets dropped by kernel
root@n3: /tmp/pycore.36177/n3.conf#
```

Figura 1.11: Execução do tcpdump do diapositivo n3 do Departamento A

```
root@n1: /tmp/pycore.36177/n1.conf# ping 10.0.0.21
PING 10.0.0.21 (10.0.0.21) 56(84) bytes of data.
64 bytes from 10.0.0.21: icmp_seq=1 ttl=64 time=2.92 ms
64 bytes from 10.0.0.21: icmp_seq=2 ttl=64 time=6.72 ms
64 bytes from 10.0.0.21: icmp_seq=3 ttl=64 time=1.06 ms
^C
--- 10.0.0.21 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2007ms
rtt min/avg/max/mdev = 1.066/3.571/6.723/2.355 ms
root@n1: /tmp/pycore.36177/n1.conf#
```

Figura 1.12: Execução do comando ping do diapositivo n1 para o n2 do Departamento A

```
root@n8: /tmp/pycore.36177/n8.conf# tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C15:45:57.419297 IP 10.0.1.1 > 224.0.0.5: OSPFv2, Hello, length 44
15:45:57.420235 IP6 fe80::200:ff:feaa:1a > ff02::5: OSPFv3, Hello, length 36
15:46:00.984234 IP6 fe80::e438:b2ff:fef6:8e1e.mdns > ff02::fb.mdns: 0 [2q] PTR
QM)? _ipps._tcp.local. PTR (QM)? _ipp._tcp.local. (45)
15:46:02.956163 IP6 fe80::20eb:abff:fe6f:c017.mdns > ff02::fb.mdns: 0 [2q] PTR
QM)? _ipps._tcp.local. PTR (QM)? _ipp._tcp.local. (45)
15:46:03.457084 IP 10.0.1.20 > 10.0.1.21: ICMP echo request, id 39, seq 1, len
h 64
15:46:03.457108 IP 10.0.1.21 > 10.0.1.20: ICMP echo reply, id 39, seq 1, lengt
h 64
15:46:04.472164 IP 10.0.1.20 > 10.0.1.21: ICMP echo request, id 39, seq 2, len
h 64
15:46:04.472246 IP 10.0.1.21 > 10.0.1.20: ICMP echo reply, id 39, seq 2, lengt
h 64
15:46:05.471080 IP 10.0.1.20 > 10.0.1.21: ICMP echo request, id 39, seq 3, len
h 64
15:46:05.471109 IP 10.0.1.21 > 10.0.1.20: ICMP echo reply, id 39, seq 3, lengt
h 64

10 packets captured
10 packets received by filter
0 packets dropped by kernel
root@n8: /tmp/pycore.36177/n8.conf# tcpdump
```

Figura 1.13: Execução do tcpdump do diapositivo n8 do Departamento B

```
root@n9:/tmp/pycore.36177/n9.conf# tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
15:46:00.984232 IP6 fe80::e438:b2ff:fe6:8e1e.mdns > ff02::fb.mdns: 0 [2q] PTR (QM)? _ipps._tcp.local. PTR (QM)? _ipp._tcp.local. (45)
15:46:02.983481 IP6 fe80::8866:f8ff:fe7:9adc.mdns > ff02::fb.mdns: 0 [2q] PTR (QM)? _ipps._tcp.local. R (QM)? _ipp._tcp.local. (45)
15:46:03.457083 IP 10.0.1.20 > 10.0.1.21: ICMP echo request, id 39, seq 1, length 64
15:46:03.457260 IP 10.0.1.21 > 10.0.1.20: ICMP echo reply, id 39, seq 1, length 64
15:46:04.472161 IP 10.0.1.20 > 10.0.1.21: ICMP echo request, id 39, seq 2, length 64
15:46:04.472392 IP 10.0.1.21 > 10.0.1.20: ICMP echo reply, id 39, seq 2, length 64
15:46:05.471079 IP 10.0.1.20 > 10.0.1.21: ICMP echo request, id 39, seq 3, length 64
15:46:05.471256 IP 10.0.1.21 > 10.0.1.20: ICMP echo reply, id 39, seq 3, length 64
15:46:07.420022 IP 10.0.1.1 > 224.0.0.5: OSPFv2, Hello, length 44
15:46:07.420931 IP6 fe80::200:ff:feaa:1a > ff02::5: OSPFv3, Hello, length 36

10 packets captured
10 packets received by filter
0 packets dropped by kernel
root@n9:/tmp/pycore.36177/n9.conf#
```

Figura 1.14: Execução do tcpdump do diapositivo n9 do Departamento B

```
root@n7:/tmp/pycore.36177/n7.conf# ping 10.0.1.21
PING 10.0.1.21 (10.0.1.21) 56(84) bytes of data:
64 bytes from 10.0.1.21: icmp_seq=1 ttl=64 time=0.374 ms
64 bytes from 10.0.1.21: icmp_seq=2 ttl=64 time=4.99 ms
64 bytes from 10.0.1.21: icmp_seq=3 ttl=64 time=2.11 ms
^C
--- 10.0.1.21 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2012ms
rtt min/avg/max/mdev = 0.374/2.495/4.995/1.905 ms
root@n7:/tmp/pycore.36177/n7.conf#
```

Figura 1.15: Execução do comando ping do diapositivo n7 para o n8 do Departamento B

No departamento B, o ping feito pelo host n7 para o host n8 foi recebido tanto pelo host n8 como pelo n9. Já no departamento A, o ping feito pelo host n1 para o host n2, foi recebido pelo n2, mas não pelo n3. Com isto concluímos o funcionamento de um hub em comparação a um switch: o hub transmite um pacote por todos os hosts a si ligados, enquanto um switch encaminha os pacotes apenas para o host indicado.

Todos os hosts ligados a um hub pertencem ao mesmo domínio de colisão, enquanto que cada host ligado a um switch tem o seu domínio de colisão, não sendo partilhado com mais nenhum host. Isto resulta numa redução do um número de colisões quando se utilizam switches em comparação a quando se utilizam hubs, que são muito mais suscetíveis a colisões.

Capítulo 2

Conclusão e Análise de Resultados

Com a elaboração deste trabalho conseguimos ter uma experiência mais prática com os conceitos lecionados nas aulas teóricas, relativamente a pedidos e respostas HTTP, ao protocolo ARP e à Ethernet.

Com o estudo destes tópicos conseguimos perceber que estes são necessários para conseguir detetar os diferentes diapositivos ligados à mesma rede, permitindo a comunicação entre eles. Os pedidos e respostas HTTP permitem obter o endereço IP de um URL. O ARP permite a consulta dos endereços MAC dos diapositivos ligados à rede.

Em relação à Ethernet, com a pergunta final deste trabalho fomos capazes de perceber a diferença entre a utilização de um *Hub* e de um *Switch*.