

TP1: Nível de Ligação Lógica - *Ethernet* e Protocolo ARP; Redes Sem Fios (IEEE 802.11)

Ana Silva (a91678), Paulo Freitas (a100053) e Rúben Machado (a91656)

Questões e Respostas

1 Nível de Ligação Lógica - *Ethernet* e Protocolo ARP

1.1 Captura e Análise de Tramas *Ethernet*

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

O endereço MAC de origem (Fig. 1) corresponde a (00:d0:03:ff:94:00).

Fig. 1. Endereço MAC de origem (*Source*)

> Source: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)

O endereço MAC de destino (Fig. 2) corresponde a (b0:a4:60:b4:a2:35).

Fig. 2. Endereço MAC de destino (*Destination*)

> Destination: IntelCor_b4:a2:35 (b0:a4:60:b4:a2:35)

2) Identifique a que sistemas se referem. Justifique.

O endereço MAC de origem pertence à máquina do autor, enquanto o endereço MAC do destino pertence ao router da sala de aula (rede LAN) onde se realizou a experiência.

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

O valor hexadecimal do campo *Type* da trama *Ethernet* corresponde a 0x0806 (Fig.3 – vermelho) referindo-se ao tipo de protocolo da *Ethernet* que foi capturado, neste caso o endereço IPv4 (Fig.3 – verde).

Fig. 3. O campo *Type* da trama *Ethernet*

Type: IPv4 (0x0806)

- 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 (considere o FCS).

Os bytes usados no início da trama até ao caractere ASCII “G” do método HTTP GET foram 54, além disso a sobrecarga (*overhead*) introduzida pela pilha protocolar no envio do HTTP GET corresponde a 5.84% (6% arredondado às unidades) num total de 924 *bytes* (Fig.4).

Fig. 4. *Overhead* no envio do HTTP GET

00 d0 03 ff 94 00 b0 a4 60 b4 a2 35 08 00 45 00S..E..
03 8e 2e 0f 40 00 80 06 d5 ba ac 1a 7c 4e c1 89	...@... N..
09 ae cd 4d 00 50 b9 b4 c8 88 2e 2d aa af 50 18	...M.P...P..
01 fb 1c 6c 00 00 47 45 54 20 2f 20 48 54 54 50	...l...GET / HTTP
2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e	/1.1..Host: www.
73 63 6f 6d 2e 75 6d 69 6e 68 6f 2e 70 74 0d 0a	scom.umi nho.pt..
43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70	Connecti on: keep
2d 61 6c 69 76 65 0d 0a 43 61 63 68 65 2d 43 6f	-alive.. Cache-Co
6e 74 72 6f 6c 3a 20 6d 61 78 2d 61 67 65 3d 30	ntrol: m ax-age=0
0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 63 75	..Upgrad e-Insecu
72 65 2d 52 65 71 75 65 73 74 73 3a 20 31 0d 0a	re-Reque sts: 1..
55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69	User-Age nt: Mozi
6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73	lla/5.0 (Windows
20 4e 54 20 31 30 2e 30 3b 20 57 69 6e 36 34 3b	NT 10.0 ; Win64;
20 78 36 34 29 20 41 70 70 6c 65 57 65 62 4b 69	x64) Ap pleWebKi
74 2f 35 33 37 2e 33 36 20 28 4b 48 54 4d 4c 2c	t/537.36 (KHTML,
20 6c 69 6b 65 20 47 65 63 6b 6f 29 20 43 68 72	like Ge cko) Chr
6f 6d 65 2f 39 30 2e 30 2e 34 34 33 30 2e 32 31	ome/90.0 .4430.21
34 20 53 61 66 61 72 69 2f 35 33 37 2e 33 36 0d	4 Safari /537.36.
0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f 68 74	.Accept: text/ht
6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78	ml,appli cation/x
68 74 6d 6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 61	html+xml ,applica
74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 69	tion/xml ;q=0.9,i
6d 61 67 65 2f 61 76 69 66 2c 69 6d 61 67 65 2f	mage/avi f,image/
77 65 62 70 2c 69 6d 61 67 65 2f 61 70 6e 67 2c	webp,ima ge/apng,
2a 2f 2a 3b 71 3d 30 2e 38 2c 61 70 70 6c 69 63	*/*;q=0. 8,applic
61 74 69 6f 6e 2f 73 69 67 6e 65 64 2d 65 78 63	ation/si gned-exc
68 61 6e 67 65 3b 76 3d 62 33 3b 71 3d 30 2e 39	hange;v= b3;q=0.9
0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f 64 69 6e	..Accept -Encodin

Fig. 5. Tamanho (*bytes*) da trama

Frame 5: 924 bytes on wire (7392 bits), 924 bytes captured (7392 bits) on interface \Device\NPF_{96E56597-15CA-4B16-AB07-1801FC635A18},

- 5) 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), sendo este correspondente ao endereço *Ethernet* do *router* da sala de aula (Fig.6).

Fig. 6. Endereço *Ethernet* da fonte (*Source*)

> Source: ComdaEnt_ff:94:00 (00:d0:03:ff:94:00)

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

O endereço MAC do destino é (b0:a4:60:b4:a2:35), correspondendo à máquina do autor (Fig.7).

Fig. 7. Endereço MAC do destino (*Destination*)

> Destination: IntelCor_b4:a2:35 (b0:a4:60:b4:a2:35)

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

Os protocolos contidos na trama recebida (Fig.8) são os seguintes: TCP (*Transmission Control Protocol*), SSDP (*Simple Service Discovery Protocol*), IP (*Internet Protocol*), HTTP (*Hypertext Transfer Protocol*).

Fig. 8. Protocolos da trama

41	1.748312	193.137.9.174	172.26.124.78	TCP	1304 80 -> 52557 [ACK] Seq=15001 Ack=871 Win=65535 Len=1250 [TCP segment of a reassembled PDU]
42	1.748312	193.137.9.174	172.26.124.78	TCP	1304 80 -> 52557 [ACK] Seq=16251 Ack=871 Win=65535 Len=1250 [TCP segment of a reassembled PDU]
43	1.748312	193.137.9.174	172.26.124.78	TCP	1304 80 -> 52557 [ACK] Seq=17501 Ack=871 Win=65535 Len=1250 [TCP segment of a reassembled PDU]
44	1.748312	193.137.9.174	172.26.124.78	TCP	1304 80 -> 52557 [ACK] Seq=18751 Ack=871 Win=65535 Len=1250 [TCP segment of a reassembled PDU]
45	1.748312	193.137.9.174	172.26.124.78	TCP	1304 80 -> 52557 [ACK] Seq=19001 Ack=871 Win=65535 Len=1250 [TCP segment of a reassembled PDU]
46	1.748312	193.137.9.174	172.26.124.78	TCP	1304 80 -> 52557 [ACK] Seq=41251 Ack=871 Win=65535 Len=1250 [TCP segment of a reassembled PDU]
47	1.748312	193.137.9.174	172.26.124.78	TCP	1301 HTTP/1.1 200 OK (text/html)
48	1.748312	172.26.124.78	193.137.9.174	TCP	54 52557 -> 80 [ACK] Seq=871 Ack=51248 Win=512 Len=0
49	1.540109	193.137.9.174	172.26.124.78	TCP	80 [TCP Seq ACK 1047] 80 -> 52557 [ACK] Seq=41248 Ack=871 Win=65535 Len=0
50	2.002162	172.26.124.78	239.255.255.250	SSDP	230 M-SEARCH * HTTP/1.1
51	3.002177	172.26.124.78	239.255.255.250	SSDP	230 M-SEARCH * HTTP/1.1
52	4.050521	172.26.124.78	54.225.175.245	TCP	55 51860 -> 443 [ACK] Seq=1 Ack=1 Win=500 Len=1 [TCP segment of a reassembled PDU]
53	4.787930	54.225.175.245	172.26.124.78	TCP	66 443 -> 51860 [ACK] Seq=1 Ack=2 Win=128 Len=0 SYN=2

* Frame 1: 230 bytes on wire (1840 bits), 230 bytes captured (1840 bits) on Interface 'DeviceVRF1_96156597-15CA-4B07-1B01FC35A3B', 1
 * Ethernet II, Src: IntelCor_b4:a2:35 (b0:a4:60:b4:a2:35), Dst: DpReceiv_7f:ff:fa (01:00:00:7f:ff:fa)
 * Internet Protocol Version 4, Src: 172.26.124.78, Dst: 239.255.255.250
 * User Datagram Protocol, Src Port: 65520, Dst Port: 1900
 * Simple Service Discovery Protocol

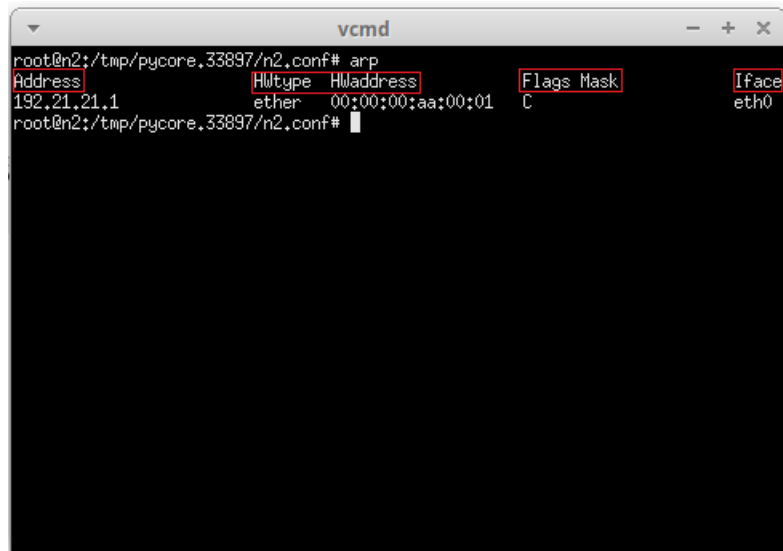
1.2 Protocolo ARP

8) Abra uma consola na *host* onde efetuou o *ping*. Observe o conteúdo da tabela ARP com o comando *arp*.

a. Com a ajuda do manual *arp* (*man arp*), interprete o significado de cada uma das colunas da tabela.

A tabela ARP fornece 3 parâmetros: o IP (*Internet Protocol*), neste caso, *Address*; o endereço físico, ou seja, o tipo e endereço MAC; a máscara (*Flags Mask*); e, por fim, a interface (Fig.9).

Fig. 9. Tabela ARP



```
root@n2:/tmp/pycore.33897/n2.conf# arp
```

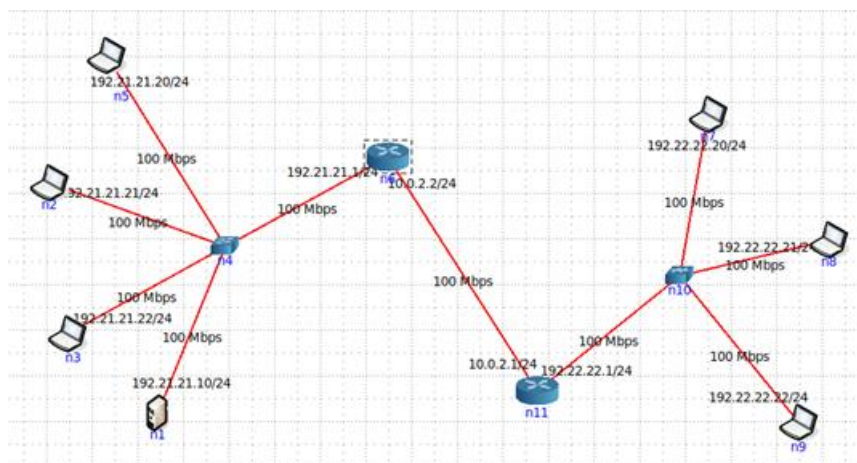
Address	Hwtype	Hwaddress	Flags	Mask	Iface
192.21.21.1	ether	00:00:00:aa:00:01	C		eth0

```
root@n2:/tmp/pycore.33897/n2.conf#
```

- b. Indique, justificando, qual o equipamento da *intranet* em causa que poderá apresentar a maior tabela ARP em termos de número de entradas.

O equipamento da *intranet* que poderá apresentar a maior tabela ARP é o *router* n6 (Fig.10), porque o departamento A possui 4 interfaces (3 *hosts* + 1 servidor) enquanto o departamento B apenas possui 3 interfaces (3 *hosts*). Por outro lado, o *hub* e o *switch* não poderiam ser considerados, visto que estes equipamentos não trabalham com tabelas ARP, mas com endereços MAC.

Fig. 10. Diagrama dos departamentos: A (esquerda) e B (direita)



- 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?

Os valores hexadecimais dos endereços de origem (Fig.11 - vermelho) correspondem a (00:00:00:aa:00:05), e destino (Fig.11 - verde) na trama *Ethernet* que contém a mensagem com o pedido ARP correspondem a (ff:ff:ff:ff:ff:ff).

Fig. 11. Endereços MAC de origem e destino da trama *Ethernet*

arp						
No.	Time	Source	Destination	Protocol	Length	Info
28	20.684978861	00:00:00_aa:00:05	Broadcast	ARP	42	Who has 192.21.21.1? Tell 192.21.21.21
29	20.685441046	00:00:00_aa:00:01	00:00:00_aa:00:05	ARP	42	192.21.21.1 is at 00:00:00:aa:00:01
44	25.856366476	00:00:00_aa:00:01	00:00:00_aa:00:05	ARP	42	Who has 192.21.21.1? Tell 192.21.21.1
45	25.856377640	00:00:00_aa:00:05	00:00:00_aa:00:01	ARP	42	192.21.21.21 is at 00:00:00:aa:00:05

▶ Frame 28: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface veth2.0.ed, id 0
 ▶ Ethernet II, Src: 00:00:00_aa:00:05 (00:00:00:aa:00:05), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 ▶ Address Resolution Protocol (request)

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

O valor hexadecimal do campo tipo da trama *Ethernet* é (ff:ff:ff:ff:ff:ff), ou seja, endereço MAC de destino é desconhecido. Por isso, a máquina utiliza o método de *broadcast* para encontrar um receptor.

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

Como podemos observar na imagem abaixo (Fig.12), sabemos que se trata de um pedido ARP, onde é possível identificar os endereços MAC, tanto da origem como do destino, do pedido efetuado. O protocolo ARP tem como objetivo identificar o MAC de uma máquina, com recurso ao IP.

Fig. 12. Pedido ARP

No.	Time	Source	Destination	Protocol	Length	Info
28	0.000000	00:00:00:aa:00:05	Broadcast	ARP	42	Who has 192.21.21.1? Tell 192.21.21.1
29	0.000000	00:00:00:aa:00:05	00:00:00:aa:00:05	ARP	42	192.21.21.1 is at 00:00:00:aa:00:05
44	25.85636476	00:00:00:aa:00:05	00:00:00:aa:00:05	ARP	42	Who has 192.21.21.2? Tell 192.21.21.1
45	25.856377849	00:00:00:aa:00:05	00:00:00:aa:00:05	ARP	42	192.21.21.2 is at 00:00:00:aa:00:05

* Frame 28: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface veth2.8.05, id 0
 * Ethernet II, Src: 00:00:00:aa:00:05 (00:00:00:aa:00:05), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 * Destination: Broadcast (ff:ff:ff:ff:ff:ff)
 * Source: 00:00:00:aa:00:05 (00:00:00:aa:00:05)
 * Type: ARP (Request)

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

O pedido feito pelo *host* de origem faz-se através de um *broadcast*, ou seja, envia um pedido para todos na rede com a finalidade de identificar o *host* de destino.

- 13) Localize a mensagem ARP que é a resposta ao pedido ARP efetuado.
 a. Qual o valor do campo ARP *opcode*? O que especifica?

O valor do campo ARP *opcode* tem valor 2, que corresponde a um ARP *Reply* (Fig.13).

Fig. 13. Campo ARP *Opcode*

Opcode: reply (2)

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

A resposta ao pedido ARP encontra-se na posição 00 02 (Fig.14).

Fig. 14. Posição da mensagem ARP

Opcode: reply (2)	
Sender MAC address: 00:00:00_aa:00:01 (00:00:00:aa:00:01)	
Sender IP address: 192.21.21.1	
Target MAC address: 00:00:00_aa:00:05 (00:00:00:aa:00:05)	
Target IP address: 192.21.21.21	

0000	00 00 00 aa 00 05 00 00 00 aa 00 01 08 06 00 01
0010	08 00 06 04 00 02 00 00 00 aa 00 01 c0 15 15 01
0020	00 00 00 aa 00 05 c0 15 15 15

- c. A resposta ARP é enviada em *broadcast*? Justifique o modo de envio usado na resposta ARP.

A resposta ARP não é enviada em *broadcast*, visto que o envio é realizado para o *host* de origem que fez o pedido ARP.

- 14) Verifique se o ping feito ao segundo *host* originou pacotes ARP e justifique a situação observada.

O segundo *host* não originou pacotes ARP, visto que o pedido ARP realiza-se com um *broadcast* para que possa identificar o endereço MAC do *host* de destino. No segundo *ping*, não será necessário realizar outro *broadcast*, já que se sabe o endereço MAC do *host* de destino, sendo assim desnecessário originar outro pacote ARP (Fig.15).

Fig. 15. Pacotes ARP

No.	Time	Source	Destination	Protocol	Length	Info
28	29.684978861	00:00:00_aa:00:05	Broadcast	ARP	42	Who has 192.21.21.1? Tell 192.21.21.21
29	29.685441046	00:00:00_aa:00:01	00:00:00_aa:00:05	ARP	42	192.21.21.1 is at 00:00:00:aa:00:01
44	25.856366476	00:00:00_aa:00:01	00:00:00_aa:00:05	ARP	42	Who has 192.21.21.21? Tell 192.21.21.1
45	25.856377649	00:00:00_aa:00:05	00:00:00_aa:00:01	ARP	42	192.21.21.21 is at 00:00:00:aa:00:05

Frame 29: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface veth2.0.ed, id 0	
Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:05 (00:00:00:aa:00:05)	
Address Resolution Protocol (reply)	
Hardware type: Ethernet (1)	
Protocol type: IPv4 (0x0800)	
Hardware size: 6	
Protocol size: 4	
Opcode: reply (2)	
Sender MAC address: 00:00:00_aa:00:01 (00:00:00:aa:00:01)	
Sender IP address: 192.21.21.1	
Target MAC address: 00:00:00_aa:00:05 (00:00:00:aa:00:05)	
Target IP address: 192.21.21.21	

- 15) Apresente um esquema apenas com as máquinas envolvidas no envio do pedido *ping* desde a origem até ao destino, bem como os endereços IP e MAC das respectivas interfaces de rede, podendo para tal recorrer ao comando *ifconfig*. Represente nesse esquema as tramas com os pedidos e respostas ARP geradas ao longo da rota pelo envio do pedido *ping*. Indique para cada trama os endereços MAC origem e destino presentes no cabeçalho *Ethernet*, bem como os endereços *Sender MAC*, *Sender IP*, *Target MAC* e *Target IP* presentes no pacote ARP. Assinale com uma seta o sentido de cada pacote e com um número a ordem de sequência dos pacotes. Considere todas as tabelas ARP vazias no momento em que se fez o *ping*. Ignore a situação da resposta ao pedido *ping*.

Fig. 16. Esquema da ordem de envio de pacotes

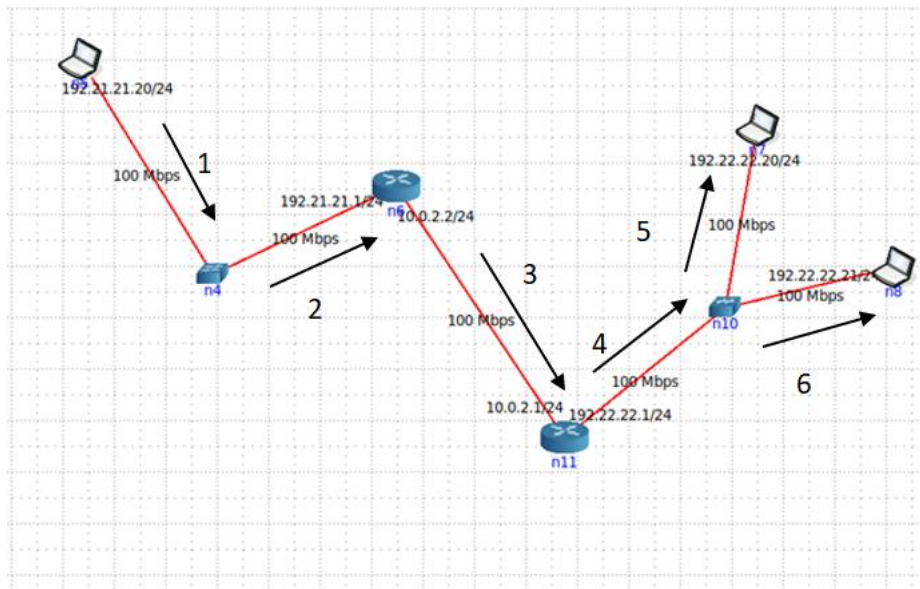


Fig. 17. Tabela do router n6

```

root@n6:/tmp/pycore.32783/n6.conf# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.21.21.1 netmask 255.255.255.0 broadcast 0.0.0.0
    inet6 2001::1 prefixlen 64 scopeid 0x0<global>
    inet6 fe80::200:ff:feaa:1 prefixlen 64 scopeid 0x20<link>
    ether 00:00:00:aa:00:01 txqueuelen 1000 (Ethernet)
    RX packets 58 bytes 8038 (8.0 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 78 bytes 6476 (6.4 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.2 netmask 255.255.255.0 broadcast 0.0.0.0
    inet6 fe80::200:ff:feaa:4 prefixlen 64 scopeid 0x20<link>
    inet6 2001:2::2 prefixlen 64 scopeid 0x0<global>
    ether 00:00:00:aa:00:04 txqueuelen 1000 (Ethernet)
    RX packets 139 bytes 15496 (15.4 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 93 bytes 8454 (8.4 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@n6:/tmp/pycore.32783/n6.conf#

```

Fig. 18. Tabela do *router* n11

```

root@n11:/tmp/pycore.32783/n11.conf# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.22.22.1 netmask 255.255.255.0 broadcast 0.0.0.0
    inet6 fe80::200:ff:feaa:2 prefixlen 64 scopeid 0x20<link>
    inet6 2001::1 prefixlen 64 scopeid 0x0<global>
    ether 00:00:00:aa:00:02 txqueuelen 1000 (Ethernet)
    RX packets 76 bytes 9816 (9.8 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 141 bytes 11582 (11.5 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.1 netmask 255.255.255.0 broadcast 0.0.0.0
    inet6 fe80::200:ff:feaa:3 prefixlen 64 scopeid 0x20<link>
    inet6 2001::2 prefixlen 64 scopeid 0x0<global>
    ether 00:00:00:aa:00:03 txqueuelen 1000 (Ethernet)
    RX packets 208 bytes 21476 (21.4 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 154 bytes 13624 (13.6 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@n11:/tmp/pycore.32783/n11.conf#

```

1.3 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?

O tráfego gerado no departamento A (LAN comutada), vai ser fluído e sem perdas. Enquanto, no departamento B (LAN Partilhada) vai-se tornar numa rede contenciosa, onde existirá competição e, em algumas vezes, haverá alguma perda (Fig. 19).

Fig. 19. Tabela *tcpdump*

```

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
18:13:28.822993 IP6 fe80::200:ff:feaa:1 > ff02::5: OSPFv3, Hello, length 36
18:13:29.046687 IP 192.21.21.1 > 224.0.0.5: OSPFv2, Hello, length 44
18:13:31.046828 IP 192.21.21.1 > 224.0.0.5: OSPFv2, Hello, length 44
18:13:33.047229 IP 192.21.21.1 > 224.0.0.5: OSPFv2, Hello, length 44
18:13:35.048611 IP 192.21.21.1 > 224.0.0.5: OSPFv2, Hello, length 44
18:13:37.049703 IP 192.21.21.1 > 224.0.0.5: OSPFv2, Hello, length 44
18:13:38.851921 IP6 fe80::200:ff:feaa:1 > ff02::5: OSPFv3, Hello, length 36
18:13:39.049845 IP 192.21.21.1 > 224.0.0.5: OSPFv2, Hello, length 44

```

2 Redes Sem Fios (IEEE 802.11)

2.1 Acesso Rádio

- 1) Identifique em que frequência do espectro está a operar a rede sem fios, e o canal que corresponde essa frequência.

O espectro está a operar com uma frequência de 2467 MHz (Fig.20 – verde) na rede sem fios que corresponde ao canal 12 (Fig.20 – vermelho).

Fig. 20. Canal (*Channel*) e Frequência (*Frequency*) da rede sem fios

Channel: 12
Frequency: 2467MHz

- 2) Identifique a versão da norma IEEE 802.11 que está a ser usada.

A versão que está a ser usada da norma IEEE 802.11 é a 802.11b (Fig.21).

Fig. 21. Versão da norma IEEE 802.11

PHY type: 802.11b (HR/DSSS) (4)

- 3) Qual o débito a que foi enviada a trama escolhida? Será que esse débito corresponde ao débito máximo a que a interface *Wi-Fi* pode operar? Justifique.

O débito que foi enviada na trama escolhida foi 1,0 Mb/s (Fig.22). Por outro lado, o débito máximo que a interface *Wi-Fi* pode operar corresponde a 50 Mb/s (Fig.23). Porém, este débito não é utilizado para garantir que a trama *beacon* chegue a todos os *hosts*, preferencialmente usa-se o menor débito possível.

Fig. 22. Débito (*Data rate*) que foi enviada na trama 421

Data rate: 1,0 Mb/s

Fig. 23. Débito máximo

Tag Number: Extended Supported Rates (50)

2.2 Scanning Passivo e Scanning Ativo

- 4) **Selecione a trama *beacon* 21. Esta trama pertence a que tipo de tramas 802.11? Indique o valor dos seus identificadores de tipo e de subtipo. Em que parte concreta do cabeçalho da trama estão especificados?**

A trama pertence às tramas 802.11 do tipo *Management* (Fig.25). A trama *beacon* (Fig.28 – vermelho) é do tipo 00 (0) e subtipo 1000 (8), estando especificados na *Frame Control Field* (Fig.28 – verde).

Fig. 24. Tipo da trama 802.11

00	Management	1000	Beacon
----	------------	------	--------

Fig. 25. Tipo e subtipo da trama *beacon* 421

```
IEEE 802.11 Beacon frame, Flags: .....C
Type/Subtype: Beacon frame (0x0008)
  Frame Control Field: 0x8000
    ....00 = Version: 0
    ....00. = Type: Management frame (0)
    1000.... = Subtype: 8
```

- 5) **Para a trama acima, identifique todos os endereços MAC em uso. Que conclui quanto à sua origem e destino?**

O endereço MAC de origem e destino são (bc:14:01:af:b1:98) e (ff:ff:ff:ff:ff:ff), respetivamente. A trama *beacon* procura encontrar através do *broadcast* o endereço MAC do *host* de destino (Fig.26).

Fig. 26. Endereços MAC

421 17.817787 HitronTe_afb1:98 Broadcast 802.11 296 Beacon frame, SN=2431, FN=0, Flags=.....C, BI=100, SSID="FlyingNet"

422 17.819437 HitronTe_afb1:98 Broadcast 802.11 205 Beacon frame, SN=2432, FN=0, Flags=.....C, BI=100, SSID="NOS_WIFI_Fon"

> Frame 421: 296 bytes on wire (2368 bits), 296 bytes captured (2368 bits)

> Radiotap Header v0, Length 25

> 802.11 radio information

▼ IEEE 802.11 Beacon frame, Flags:C

Type/Subtype: Beacon frame (0x0008)

> Frame Control Field: 0x0000

.....000000000000 = Duration: 0 microseconds

Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)

Destination address: Broadcast (ff:ff:ff:ff:ff:ff)

Transmitter address: HitronTe_afb1:98 (bc:14:01:afb1:98)

Source address: HitronTe_afb1:98 (bc:14:01:afb1:98)

BSS Id: HitronTe_afb1:98 (bc:14:01:afb1:98)

.....0000 = Fragment number: 0

1001 0111 1111 = Sequence number: 2431

Frame check sequence: 0x4614c1e7 [unverified]

[FCS Status: Unverified]

> IEEE 802.11 Wireless Management

- 6) Qual o intervalo de tempo previsto entre tramas *beacon* consecutivas? Na prática, a periodicidade de tramas *beacon* provenientes do mesmo AP é verificada com precisão? Justifique.

O intervalo de tempo previsto entre tramas *beacon* consecutivas correspondem a 0,102400 segundos (Fig.27). A periodicidade das tramas *beacon* provenientes do mesmo AP não é verificada com precisão, sobretudo no controlo ao acesso será necessário haver competição (rede contenciosa). Caso haja atrasos no controlo, este será mais lento porque estará ocupado, logo a trama *beacon* seguinte terá de esperar.

Fig. 27. Intervalo da trama *beacon*

Beacon Interval: 0,102400 [Seconds]

- 7) Identifique e liste os SSIDs dos APs que estão a operar na vizinhança da STA de captura? Explícite o modo como obteve essa informação.

A listagem foi obtida através do filtro (Fig.28) localizado no Wireshark em *Wireless LAN Statistics*.

Fig. 28. Listagem dos SSIDs

BSSID	Channel	SSID	Percent Pack	Percent Retry	Retry	Beacons	Data Pkts	Be Reqs	Be Resp	Auths	Deauths	Other	Protection
> bc:14:01:afb1:98	12	FlyingNet	49.0	0.0	0	1256	18	0	0	0	0	0	CCMP
> bc:14:01:afb1:99	12	NOS_WIFI_Fon	47.9	0.0	0	1245	0	0	0	0	0	0	
> ff:ff:ff:ff:ff:ff	11	<Broadcast>	0.2	0.0	0	0	0	5	0	0	0	0	
> ff:ff:ff:ff:ff:ff	12	2WIRE-PT-431	0.0	0.0	0	0	0	1	0	0	0	0	
> ff:ff:ff:ff:ff:ff	12	FlyingNet	2.8	0.0	0	0	0	74	0	0	0	0	

Display filter: wlan.addr == ff:ff:ff:ff:ff:ff Apply

- 8) Face ao endereçamento usado, indique a que sistemas são endereçadas ambas as tramas e explique qual o propósito das mesmas?

O endereço MAC de origem de uma trama e de outra trama no qual o endereço MAC do destino vai ser o mesmo, trata-se de um *probe request* e de um *probe response*. O *probe request* têm como finalidade para as STAs determinar os APs que se encontram dentro do alcance rádio, ou seja, obter informações de outras estações. Enquanto, os *probe response* vão transmitir as informações pedidas pelas STAs (Fig.29).

Fig. 29. Filtro aplicado a *Probes Request* e *Response*

wlan.fc.type_subtype == 4 wlan.fc.type_subtype == 5							
No.	Time	Source	Destination	Protoc	Length	BSS Id	Info
1300	53.746911	Apple_10:6a:f5	Broadcast	802.11	155	ff:ff:ff:ff:ff:ff	Probe Request, SN=2516, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
2467	70.147855	ea:a4:64:7b:b9:7a	Broadcast	802.11	167	ff:ff:ff:ff:ff:ff	Probe Request, SN=2540, FN=0, Flags=.....C, SSID=2WIRE-PT-431
2468	70.149098	ea:a4:64:7b:b9:7a	Broadcast	802.11	155	ff:ff:ff:ff:ff:ff	Probe Request, SN=2541, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
2469	70.149792	HitronTe_afb1:98	ea:a4:64:7b:b9:7a	802.11	411	bc:14:01:afb1:98	Probe Response, SN=2332, FN=0, Flags=.....C, BI=100, SSID="FlyingNet"
2471	70.150537	HitronTe_afb1:98	ea:a4:64:7b:b9:7a	802.11	411	bc:14:01:afb1:98	Probe Response, SN=2333, FN=0, Flags=.....C, BI=100, SSID="FlyingNet"
2473	70.151237	HitronTe_afb1:98	ea:a4:64:7b:b9:7a	802.11	411	bc:14:01:afb1:98	Probe Response, SN=2334, FN=0, Flags=.....C, BI=100, SSID="FlyingNet"
2475	70.151709	HitronTe_afb1:98	ea:a4:64:7b:b9:7a	802.11	201	bc:14:01:afb1:98	Probe Response, SN=2335, FN=0, Flags=.....C, BI=100, SSID="NOS_WIFI_Fon"
2477	70.152099	HitronTe_afb1:98	ea:a4:64:7b:b9:7a	802.11	201	bc:14:01:afb1:98	Probe Response, SN=2336, FN=0, Flags=.....C, BI=100, SSID="NOS_WIFI_Fon"
2479	70.152570	HitronTe_afb1:98	ea:a4:64:7b:b9:7a	802.11	201	bc:14:01:afb1:98	Probe Response, SN=2337, FN=0, Flags=.....C, BI=100, SSID="NOS_WIFI_Fon"
2603	72.179215	Apple_10:6a:f5	Broadcast	802.11	164	ff:ff:ff:ff:ff:ff	Probe Request, SN=2563, FN=0, Flags=.....C, SSID="FlyingNet"
2606	72.179924	HitronTe_afb1:98	Apple_10:6a:f5	802.11	411	bc:14:01:afb1:98	Probe Response, SN=2346, FN=0, Flags=.....C, BI=100, SSID="FlyingNet"
2608	72.180590	HitronTe_afb1:98	Apple_10:6a:f5	802.11	411	bc:14:01:afb1:98	Probe Response, SN=2347, FN=0, Flags=.....C, BI=100, SSID="FlyingNet"
2610	72.181275	HitronTe_afb1:98	Apple_10:6a:f5	802.11	411	bc:14:01:afb1:98	Probe Response, SN=2348, FN=0, Flags=.....C, BI=100, SSID="FlyingNet"
2616	72.201570	Apple_10:6a:f5	Broadcast	802.11	164	ff:ff:ff:ff:ff:ff	Probe Request, SN=2565, FN=0, Flags=.....C, SSID="FlyingNet"
2617	72.202150	HitronTe_afb1:98	Apple_10:6a:f5	802.11	411	bc:14:01:afb1:98	Probe Response, SN=2350, FN=0, Flags=.....C, BI=100, SSID="FlyingNet"
2619	72.202807	HitronTe_afb1:98	Apple_10:6a:f5	802.11	411	bc:14:01:afb1:98	Probe Response, SN=2351, FN=0, Flags=.....C, BI=100, SSID="FlyingNet"
2621	72.203485	HitronTe_afb1:98	Apple_10:6a:f5	802.11	411	bc:14:01:afb1:98	Probe Response, SN=2352, FN=0, Flags=.....C, BI=100, SSID="FlyingNet"
2650	72.488998	Apple_10:6a:f5	Broadcast	802.11	164	ff:ff:ff:ff:ff:ff	Probe Request, SN=2585, FN=0, Flags=.....C, SSID="FlyingNet"
2653	72.502553	Apple_10:6a:f5	Broadcast	802.11	164	ff:ff:ff:ff:ff:ff	Probe Request, SN=2586, FN=0, Flags=.....C, SSID="FlyingNet"
2677	72.568343	Apple_10:6a:f5	Broadcast	802.11	164	ff:ff:ff:ff:ff:ff	Probe Request, SN=2589, FN=0, Flags=.....C, SSID="FlyingNet"

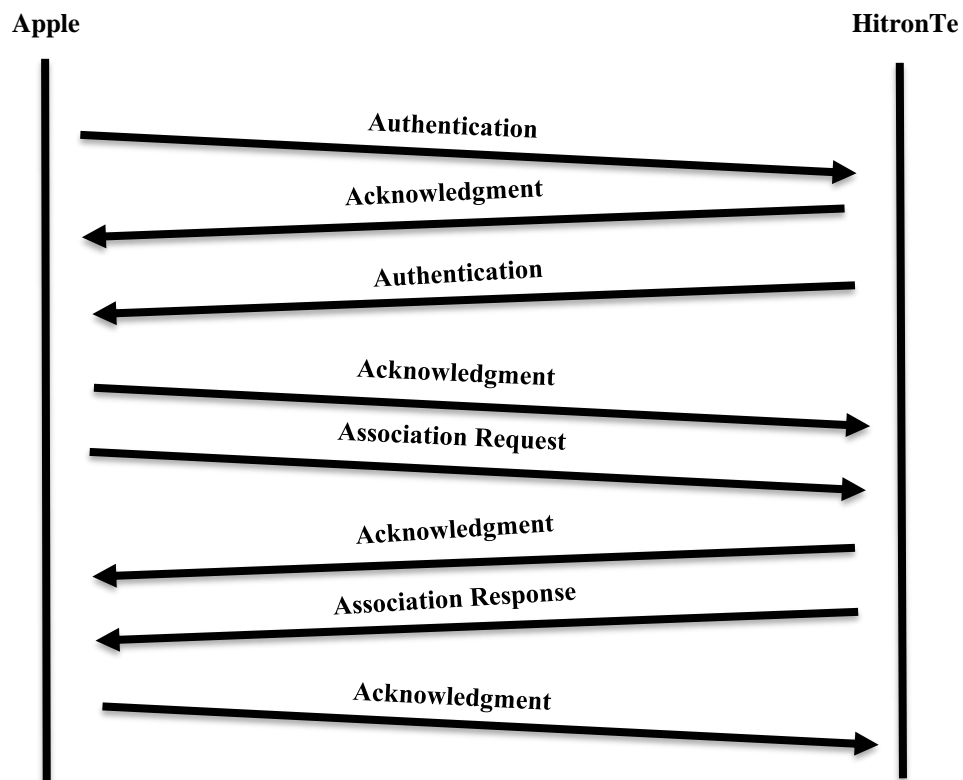
2.3 Processo de Associação

- 9) Identifique uma sequência de tramas que corresponda a um processo de associação completo entre a STA e o AP, incluindo a fase de autenticação.

Fig. 30. Tramas com processo de associação completo entre STA e AP (fase de autenticação)

wlan.fc.type == 0 && (wlan.fc.subtype == 0 wlan.fc.type_subtype == 1)						
No.	Time	Source	Destination	Protoc	Length	Info
2490	70.383512	Apple_10:6a:f5	HitronTe_afb1:98	802.11	175	Association Request, SN=2543, FN=0, Flags=.....C, SSID="FlyingNet"
2492	70.389339	HitronTe_afb1:98	Apple_10:6a:f5	802.11	225	Association Response, SN=2339, FN=0, Flags=.....C
4696	83.665976	7cea:6d:ffa2:cc	HitronTe_afb1:98	802.11	153	Association Request, SN=68, FN=0, Flags=.....C, SSID="FlyingNet"
4698	83.678873	HitronTe_afb1:98	7cea:6d:ffa2:cc	802.11	225	Association Response, SN=2440, FN=0, Flags=.....C
4699	83.680045	HitronTe_afb1:98	7cea:6d:ffa2:cc	802.11	225	Association Response, SN=2440, FN=0, Flags=.....R...C
7163	100.403689	0a:57:13:28:40:84	79:5c:58:10:7a:cc	802.11	146	Association Response, SN=3497, FN=5, Flags=o.mP..F.C

- 10) Efetue um diagrama que ilustre, com as tramas identificadas na alínea anterior, a sequência de todas as tramas trocadas no processo de autenticação e associação entre o STA e o AP.



2.4 Transferência de Dados

- 11) Considere a trama de dados nº 433. Sabendo que o campo *Frame Control* contido no cabeçalho das tramas 802.11 permite especificar a direccionalidade das tramas, o que pode concluir face à direccionalidade dessa trama? Será local à WLAN?

A trama é local à WLAN, visto que a direccionalidade da trama é DS:1 para DS: 0 (Fig.31).

Fig. 31. Direccionalidade da trama

.... ..01 = DS status: Frame from STA to DS via an AP (To DS: 1 From DS: 0) (0x1)

- 12) Para a trama de dados da alínea anterior, transcreva os endereços MAC em uso, identificando qual o endereço MAC correspondente ao *host* sem fios (STA), ao AP e ao *router* de acesso ao sistema de distribuição.

O endereço MAC correspondente ao *host* sem fios (STA) vai ser (bc:14:01:af:b1:98), ou seja, o endereço MAC de destino; enquanto o endereço MAC (bc:14:01:af:b1:98) do BSS Id vai corresponder ao AP, e por fim, o *router* de acesso ao sistema de distribuição terá a função de DS e AP, visto que *router* e o STA pertencem à mesma trama (Fig.32).

Fig. 32. Endereços MAC

```
Receiver address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
Transmitter address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)
Destination address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
Source address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)
BSS Id: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
STA address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)
```

- 13) Que subtipo de tramas de controlo são transmitidas ao longo da transferência de dados acima mencionada? Tente explicar porque razão têm de existir, contrariamente ao que acontece numa rede *Ethernet*.

As tramas de controlo transmitidas são as *Acknowledgement*. Estas desempenham um papel fundamental, visto que a transferência de dados só acontece se existir uma resposta de confirmação (Fig. 33). Caso não aconteça, não haverá a transferência de dados.

Fig. 33. Subtipo das tramas de controlo

433	17.924985	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	178	QoS Data, SN=3680, FN=0, Flags=...TC
434	17.925298		Apple_10:6a:f5 (64:9a:...	802.11	39	Acknowledgement, Flags=.....C
435	17.927587	Apple_28:b8:0c	HitronTe_af:b1:98	802.11	49	Null function (No data), SN=0, FN=0, Flags=.....T
436	17.927618		Apple_28:b8:0c (68:a8:...	802.11	39	Acknowledgement, Flags=.....C
437	17.984501	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	53	Null function (No data), SN=2499, FN=0, Flags=...P...TC
438	17.984522		Apple_10:6a:f5 (64:9a:...	802.11	39	Acknowledgement, Flags=.....C

- 14) O uso de tramas *Request To Send* e *Clear To Send*, apesar de opcional, é comum para efetuar "pré-reserva" do acesso ao meio quando se pretende enviar tramas de dados, com o intuito de reduzir o número de colisões resultante maioritariamente de STAs escondidas. Dê um exemplo de uma transferência de dados em que é usada a opção RTC/CTS e um outro em que não é usada, identificando a direccionalidade das tramas e os sistemas envolvidos.

Fig. 34. Transferência de dados com e sem RTC/CTS respectivamente

718 27.138490	HitronTe_af:b1:98 (bc...	Apple_10:6af5 (64:9a:...	802.11	45 Request-to-send, Flags=.....C
719 27.138558		HitronTe_af:b1:98 (bc...	802.11	39 Clear-to-send, Flags=.....C
720 27.138613	HitronTe_af:b1:96	Apple_10:6af5	802.11	146 QoS Data, SN=842, FN=0, Flags=p...F.C
721 27.138666	Apple_10:6af5 (64:9a:...	HitronTe_af:b1:98 (bc...	802.11	57 802.11 Block Ack, Flags=.....C
722 27.154862	Apple_10:6af5	HitronTe_af:b1:98	802.11	53 Null function (No data), SN=2507, FN=0, Flags=...P...TC
723 27.154880		Apple_10:6af5 (64:9a:...	802.11	39 Acknowledgement, Flags=.....C

3 Conclusão

A finalidade deste trabalho aspira mostrar ao docente os conhecimentos adquiridos dos autores nas aulas práticas. Os temas propostos foram, de uma forma geral, abordados e estudados. As temáticas sobre o nível da ligação lógica e redes sem fios apresentou alguns desafios aos autores. Porém, com determinação, perseverança e através dos conhecimentos teóricos adquiridos, superaram-se os obstáculos presentes no trabalho. O estudo das capturas e análises de dados da trama *Ethernet*, assim como o funcionamento e utilidades do protocolo ARP e no estudo das redes sem fios (IEEE 802.11) proporcionou uma abundância e variedade de conhecimentos adquiridos nas aulas práticas, recorrendo às aplicações CORE e *Wireshark*. No seu geral, foi um estudo realmente interessante e definitivamente instrutivo, elevando o grau de conhecimento dos autores.