

Redes Sem fio (802.11)

João Monteiro, Mário Leite, and Miguel Pinto

University of Minho, Department of Informatics, 4710-057 Braga, Portugal
e-mail: {a53690,a61021,a61049}@alunos.uminho.pt

1 Questões e Respostas

1.1 Acesso Rádio

Questão 1: Selecione uma trama da ligação e identifique em que frequência do espectro está a operar a rede sem fios e a que débito foi enviada a trama escolhida?

Escolhemos a trama dos t=24.82s, a rede sem fios opera a uma frequência do espectro de 2437GHz e a trama escolhida foi enviada a um débito de 48Mb/s.

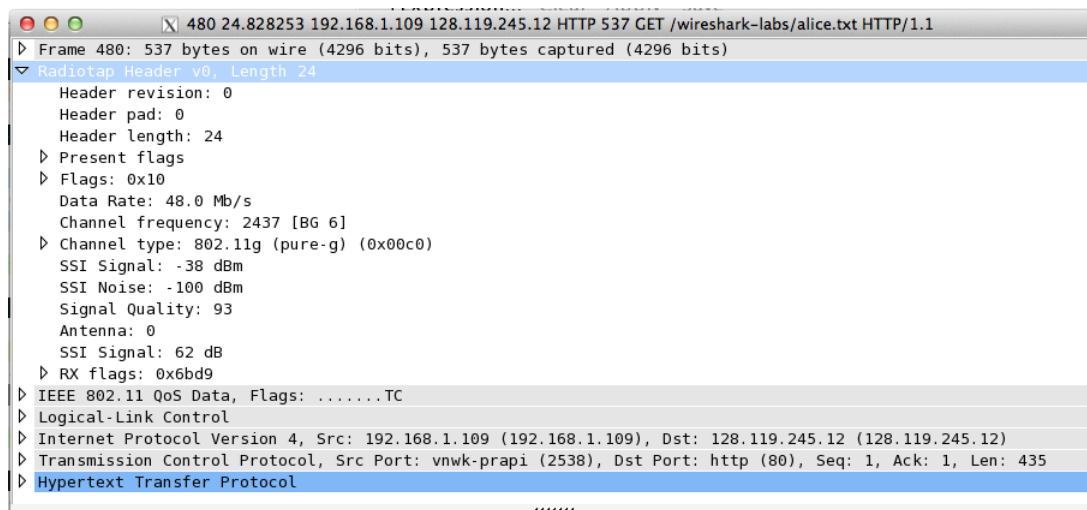


Fig. 1. Trama Ligação

Questão 2: Qual o número e o tipo do canal que está a ser usado para a comunicação rádio?

Para a comunicação rádio está a ser usado canal 6 e o tipo 802.11g.

Questão 3: Indique qual o índice de qualidade do sinal.

O índice de qualidade do sinal é de 93%.

1.2 Tramas Beacon

Questão 4: Qual o tipo de uma trama beacon? Indique quais os seus identificadores de tipo e subtipo. Em que parte da trama estão especificados?

Uma trama beacon é do tipo Management (type value: 00 e subtype value: 1000 [0x08]).

```
IEEE 802.11 Beacon frame, Flags: .....C  
Type/Subtype: Beacon frame (0x08)
```

Fig. 2. Trama Beacon

Questão 5: Identifique os SSIDs dos APs (Access Points) que estão a operar na rede e diga qual tende a proporcionar a melhor qualidade de sinal?

Os SSIDs dos APs que estão a operar na rede são o linksys12 e o 30 Munroe St.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Cisco-Li_f7:1d:51	Broadcast	802.11		183 Beacon frame, SN=2854, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
3	0.085474	Cisco-Li_f7:1d:51	Broadcast	802.11		183 Beacon frame, SN=2855, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
4	0.187919	Cisco-Li_f7:1d:51	Broadcast	802.11		183 Beacon frame, SN=2856, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
9	0.290284	Cisco-Li_f7:1d:51	Broadcast	802.11		183 Beacon frame, SN=2857, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
10	0.294432	Linksysd_67:22:94	Broadcast	802.11		90 Beacon frame, SN=3072, FN=0, Flags=.....C, BI=62, SSID=11 [truncated]
11	0.393174	Cisco-Li_f7:1d:51	Broadcast	802.11		183 Beacon frame, SN=2858, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
13	0.495032	Cisco-Li_f7:1d:51	Broadcast	802.11		183 Beacon frame, SN=2859, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
14	0.499197	Linksysd_67:22:94	Broadcast	802.11		90 Beacon frame, SN=3074, FN=0, Flags=.....C, BI=100, SSID=11Linksys12
15	0.597382	Cisco-Li_f7:1d:51	Broadcast	802.11		183 Beacon frame, SN=2860, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
16	0.601687	Linksysd_67:22:94	Broadcast	802.11		90 Beacon frame, SN=3075, FN=0, Flags=.....C, BI=100, SSID=linksys12
17	0.699847	Cisco-Li_f7:1d:51	Broadcast	802.11		183 Beacon frame, SN=2861, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
18	0.807736	Cisco-Li_f7:1d:51	Broadcast	802.11		183 Beacon frame, SN=2862, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St

Qualidade do sinal do AP linksys12:

```
SSI Signal: -94 dBm  
SSI Noise: -100 dBm  
Signal Quality: 17  
Antenna: 0  
SSI Signal: 8 dB  
SSI Signal: -94 dBm  
SSI Noise: -100 dBm  
Signal Quality: 11  
Antenna: 0  
SSI Signal: -94 dBm  
SSI Noise: -100 dBm  
Signal Quality: 11  
Antenna: 0  
SSI Signal: 8 dB
```

Qualidade do sinal do AP 30 Munroe St:

```

SST Noise: -100 dBm
Signal Quality: 88
Antenna: 0
SST Signal: 72 dB
SST Noise: -100 dBm
Signal Quality: 94
Antenna: 0
SST Signal: 71 dB
SST Noise: -100 dBm
Signal Quality: 100
Antenna: 0
SST Signal: 70 dB

```

Através da observação dos valores da qualidade do sinal, podemos facilmente inferir que o SSID 30 Munroe St é aquele que tende a proporcionar melhor qualidade de sinal.

Questão 6: Para dois dos APs identificados, indique quais são os intervalos de tempo previstos entre as transmissões de tramas *beacon*? (nota: este valor é anunciado na própria trama *beacon*).

```

IEEE 802.11 wireless LAN management frame
Fixed parameters (12 bytes)
Timestamp: 0x000000289664a182
Beacon Interval: 0.102400 [seconds]
Capabilities information: 0x0001
Tagged parameters (119 bytes)
Tag: SSID parameter set: 30 Munroe St
Tag: Supported Rates 1(b), 2(b), 5.5(b), 11(b), [Mb
Tag: RF Parameters set: Supported Channels: 6

```

Fig. 3. Beacon Interval

Como se pode ver pela figura, os intervalos de tempo são de 0.1024 segundos.

Questão 7: Na prática, a periodicidade de tramas *beacon* é verificada? Tente explicar porquê?

Para se verificar uma qualquer transmissão é necessário 0.1024 segundos, pelo menos, para que esta se verifique (tempo mínimo). Ou seja, é independente de haver ou não colisões. No entanto, este tempo pode aumentar caso haja colisões. Verifica-se portanto, contenção nas transmissões. Haverá transmissões que “vão esperar” mais tempo do que os 0.1024 (nunca menos que isso). Aquela transmissão que ganhar o acesso ao meio, será a transmitida.

Questão 8: Identifique e registre todos os endereços MAC usados nas tramas *beacon* enviadas pelos APs? Recorde que fonte, destino e BSS ID são endereços contidos no cabeçalho das tramas 802.11. Para uma descrição detalhada da estrutura da trama 802.11, veja a secção 7 da norma IEEE 802.11 (citada acima).

```

IEEE 802.11 Beacon frame, Flags: .....C
Type/Subtype: Beacon frame (0x08)
Frame Control Field: 0x8000
Duration: 0 microseconds
Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
Source address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
Fragment number: 0
Sequence number: 2880
Frame check sequence: 0x99116b74 [correct]
IEEE 802.11 wireless LAN management frame

```

Fig. 4. Trama 802.11

Analisando a trama 802.11, apresentada na figura, pode-se verificar que o endereço MAC é 00:16:b6:f7:1d:51. O endereço MAC de destino é ff:ff:ff:ff:ff:ff. O endereço MAC de BSS na trama Beacon é 00:16:b6:f7:1d:51.

Questão 9: As tramas *beacon* anunciam que o AP pode suportar vários débitos de dados base assim como vários ”*extendedsupportedrates*” adicionais. Quais são esses débitos?

```
IEEE 802.11 wireless LAN management frame
  Fixed parameters (12 bytes)
    Timestamp: 0x00000028965b4182
    Beacon Interval: 0,102400 [Seconds]
    Capabilities Information: 0x0601
  Tagged parameters (119 bytes)
    Tag: SSID parameter set: 30 Munroe St
    Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
    Tag: DS Parameter set: Current channel: 6
    Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    Tag: Country Information: Country Code US, Environment Indoor
    Tag: EDCA Parameter Set: Undecoded
    Tag: ERP Information
    Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    Tag: Vendor Specific: AirgoNet
    Tag: Vendor Specific: Microsoft: WMM/WME: Parameter Element
```

Fig. 5. Débitos de dados

Pode-se verificar, pela análise da figura 3, que o AP pode suportar 4 débitos de dados, sendo eles: 1, 2, 5.5 e 11 (Mbit/seg). Pode suportar ainda como adicionais: 6, 9, 12, 18, 24, 36, 48, 54 (Mbit/seg).

1.3 Transferência de Dados

Questão 10: Localize a trama 802.11 que contenha o segmento TCP SYN para a primeira conexão TCP (que descarrega alice.txt). Quais são os três campos de endereço contidos na trama 802.11? Qual o endereço MAC correspondente ao host ligado sem fios? E ao AP? E ao router de acesso (primeiro salto)? Qual é o endereço IP do host sem fios que envia este segmento TCP? Qual é endereço IP de destino? A que sistema corresponde esse endereço IP destino?

A trama 802.11 que contém o segmento TCP SYN foi enviado aos t=24.811093. Os endereços MAC de destino, de envio e BSS ID são, respectivamente 00:16:b6:f4:eb:a8, 00:13:02:d1:b6:4f e 00:16:b6:f7:1d:51. O endereço BSS ID corresponde ao router do primeiro salto, enquanto que o endereço MAC de destino corresponde ao AP e o endereço MAC de envio corresponde ao host.

O endereço do host, que manda este segmento TCP, é 192.168.1.109, sendo este o endereço de envio. Por outro lado, o endereço de destino é 128.119.245.12 correspondente ao servidor gaia.cs.umass.edu.

No.	Time	Source	Destination	Protocol	Length	Info
469	24.795573		Cisco-Li_f7:1d:51 (RA)	802.11	30	Acknowledgement, Flags=.....C
470	24.795673	192.168.1.109	68.87.71.226	DNS	125	Standard query 0x7892 A gaia.cs.umass.edu
471	24.795769		IntelCor_d1:b6:4f (RA)	802.11	38	Acknowledgement, Flags=.....C
472	24.809325	68.87.71.226	192.168.1.109	DNS	141	Standard query response 0x7892 A 128.119.245.12
473	24.809513		Cisco-Li_f7:1d:51 (RA)	802.11	38	Acknowledgement, Flags=.....C
474	24.811093	192.168.1.109	128.119.245.12	TCP	110	vnwk-prapi > http [SYN] Seq=0 Win=16384 Len=0 MSS=1460
475	24.811231		IntelCor_d1:b6:4f (RA)	802.11	38	Acknowledgement, Flags=.....C
476	24.827751	128.119.245.12	192.168.1.109	TCP	110	http > vnwk-prapi [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
477	24.827922		Cisco-Li_f7:1d:51 (RA)	802.11	38	Acknowledgement, Flags=.....C
478	24.828024	192.168.1.109	128.119.245.12	TCP	102	vnwk-prapi > http [ACK] Seq=1 Ack=1 Win=17520 Len=0
479	24.828140		IntelCor_d1:b6:4f (RA)	802.11	38	Acknowledgement, Flags=.....C
480	24.828253	192.168.1.109	128.119.245.12	HTTP	537	GET /wireshark-labs/alice.txt HTTP/1.1
481	24.828352		IntelCor_d1:b6:4f (RA)	802.11	38	Acknowledgement, Flags=.....C
482	24.846898	128.119.245.12	192.168.1.109	TCP	108	http > vnwk-prapi [ACK] Seq=1 Ack=436 Win=6432 Len=0
483	24.847058		Cisco-Li_f7:1d:51 (RA)	802.11	38	Acknowledgement, Flags=.....C

```
> IEEE 802.11 QoS Data, Flags: .....TC
  Type/Subtype: QoS Data (0x28)
  ▶ Frame Control Field: 0x8801
  .000 0000 0010 1100 = Duration: 44 microseconds
  Receiver address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
  BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
  Transmitter address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
  Source address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
  Destination address: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)
  Fragment number: 0
  Sequence number: 49
  ▶ Frame check sequence: 0xad57fce0 [correct]
  ▶ Qos Control: 0x0000
  ▶ Logical-Link Control
  ▶ Internet Protocol Version 4, Src: 192.168.1.109 (192.168.1.109), Dst: 128.119.245.12 (128.119.245.12)
  ▶ Transmission Control Protocol, Src Port: vnwk-prapi (2538), Dst Port: http (80), Seq: 0, Len: 0
```

Questão 11: Localize a trama 802.11 que contém o segmento TCP SYN ACK para esta conexão TCP. Quais são os três campos de endereços MAC contidos na trama 802.11? Que endereço MAC corresponde ao host? O endereço MAC do originador da trama corresponde ao endereço IP do dispositivo que envia o segmento TCP encapsulado no datagrama? (nota: este aspecto deve ter ficado claro com a realização do TP2).

A trama 802.11 que contém o segmento TCP SYN ACK foi enviado aos t=24.827751. Os endereços MAC de destino, de envio e BSS ID são, respectivamente 91:2a:b0:49:b6:4f, 00:16:b6:f4:eb:a8 e 00:16:b6:f7:1d:51. O endereço MAC de destino corresponde ao host. O endereço MAC de envio corresponde ao primeiro router em que ocorre um hop (salto). O endereço IP do dispositivo que envia o TCP é 128.119.245.12, enquanto que o endereço de destino é 192.168.1.109, correspondendo este ao pc usado para o trabalho experimental.

No.	Time	Source	Destination	Protocol	Length	Info
471	24.795769		IntelCor_d1:b6:4f (RA)	802.11	38	Acknowledgement, Flags=.....C
472	24.809325	68.87.71.226	192.168.1.109	DNS	141	Standard query response 0x7892 A 128.119.245.12
473	24.809513		Cisco-Li_f7:1d:51 (RA)	802.11	38	Acknowledgement, Flags=.....C
474	24.811093	192.168.1.109	128.119.245.12	TCP	110	vnwk-prapi > http [SYN] Seq=0 Win=16384 Len=0 MSS=1
475	24.811231		IntelCor_d1:b6:4f (RA)	802.11	38	Acknowledgement, Flags=.....C
476	24.827751	128.119.245.12	192.168.1.109	TCP	110	http > vnwk-prapi [SYN, ACK] Seq=0 Ack=1 Win=5840 L
477	24.827922		Cisco-Li_f7:1d:51 (RA)	802.11	38	Acknowledgement, Flags=.....C
478	24.828024	192.168.1.109	128.119.245.12	TCP	102	vnwk-prapi > http [ACK] Seq=1 Ack=1 Win=17520 Len=0
479	24.828140		IntelCor_d1:b6:4f (RA)	802.11	38	Acknowledgement, Flags=.....C
480	24.828253	192.168.1.109	128.119.245.12	HTTP	537	GET /wireshark-labs/alice.txt HTTP/1.1
481	24.828352		IntelCor_d1:b6:4f (RA)	802.11	38	Acknowledgement, Flags=.....C

```
> Frame 476: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
> Radiotap Header v0, Length 24
> IEEE 802.11 QoS Data, Flags: ..mP..F..
  Type/Subtype: QoS Data (0x28)
  ▶ Frame Control Field: 0x8832
  Duration/ID: 11560 (reserved)
  Receiver address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
  Destination address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
  Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
  BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
  Source address: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)
  Fragment number: 0
  Sequence number: 3124
  ▶ Frame check sequence: 0xecdc407d [incorrect, should be 0x296ed094]
  ▶ QoS Control: 0x0100
```

Questão 12: Que tipo de tramas de controlo 802.11 ocorrem na transferência de dados realizada? Quando ocorrem?

É utilizada apenas 1 trama de controlo: o ACK(Acknowledgment). O cliente requisita uma conexão enviando um SYN(synchronize) ao servidor. O servidor confirma esta requisição mandando um SYN-ACK de volta ao cliente. O cliente por sua vez responde com uma trama ACK, e a conexão está estabelecida.

No.	Time	Source	Destination	Protocol	Length	Info
474	24.811093	192.168.1.109	128.119.245.12	TCP	110	vnwk-prapi > http [SYN] Seq=0 Win=16384 Len=0 MSS=1
475	24.811231		IntelCor_d1:b6:4f (RA)	802.11	38	Acknowledgement, Flags=.....C
476	24.827751	128.119.245.12	192.168.1.109	TCP	110	http > vnwk-prapi [SYN, ACK] Seq=0 Ack=1 Win=5840 L
477	24.827922		Cisco-Li_f7:1d:51 (RA)	802.11	38	Acknowledgement, Flags=.....C
478	24.828024	192.168.1.109	128.119.245.12	TCP	102	vnwk-prapi > http [ACK] Seq=1 Ack=1 Win=17520 Len=0
479	24.828140		IntelCor_d1:b6:4f (RA)	802.11	38	Acknowledgement, Flags=.....C

1.4 Associação e Desassociação

Questão 13: Que ação é tomada pelo host após $t=49.5s$ que determina a quebra de associação com o AP 30 Munroe St que existia desde que a captura de tramas começou? Como interpreta as tramas 802.11 subsequentes relacionadas com a anterior ação? Segundo a especificação IEEE 802.11, há alguma trama que seria esperada, mas não aparece?

A ação tomada pelo host em $t=49.583615$ que determina a quebra de associação é o envio de uma trama DHCP Release, como se comprova na imagem abaixo. A trama subsequentes relacionada com a anterior é o envio aos $t=49.609617$ de uma trama de desautenticação. Seria esperado que fosse enviada uma trama de desassociação.

No.	Time	Source	Destination	Protocol	Length	Info
1719	49.132884	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1600, FN=0, Flags=...P...TC
1720	49.132981	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f (RA)	802.11	38	Acknowledgement, Flags=.....C
1721	49.224975	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1601, FN=0, Flags=.....TC
1722	49.225104	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f (RA)	802.11	38	Acknowledgement, Flags=.....C
1723	49.235239	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3585, FN=0, Flags=.....C, BI=100, SSID=30
1724	49.235340	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1602, FN=0, Flags=...P...TC
1725	49.235439	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f (RA)	802.11	38	Acknowledgement, Flags=.....C
1726	49.337573	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3586, FN=0, Flags=.....C, BI=100, SSID=30
1727	49.429849	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1603, FN=0, Flags=.....TC
1728	49.430007	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f (RA)	802.11	38	Acknowledgement, Flags=.....C
1729	49.440041	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3587, FN=0, Flags=.....C, BI=100, SSID=30
1730	49.440146	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1604, FN=0, Flags=...P...TC
1731	49.440243	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f (RA)	802.11	38	Acknowledgement, Flags=.....C
1732	49.542481	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3588, FN=0, Flags=.....C, BI=100, SSID=30
1733	49.583615	192.168.1.109	192.168.1.1	DHCP	390	DHCP Release - Transaction ID 0xea5a526
1734	49.583771	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f (RA)	802.11	38	Acknowledgement, Flags=.....C
1735	49.609617	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	Deauthentication, SN=1605, FN=0, Flags=.....C
1736	49.609770	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f (RA)	802.11	38	Acknowledgement, Flags=.....C
1737	49.614478	IntelCor_d1:b6:4f	Broadcast	802.11	99	Probe Request, SN=1606, FN=0, Flags=.....C, SSID=linksys_SE

Fig. 6. Ações levadas a cabo pelo host

Questão 14: Examine o ficheiro de trace e procure tramas de autenticação enviadas pelo host para o AP e vice versa (se filtrar os resultados por wlan.fc.type_subtype ajuda a localização). Quantas tramas de AUTHENTICATION são enviadas do host sem fios para o AP linksys_SES_24086 AP? Durante que período de tempo?

Através do uso do filtro wlan.fc.type == 0x0b, verifica-se que existem 15 tramas de AUTHENTICATION enviadas pelo host, durante cerca de 12.535213 segundos.

No.	Time	Source	Destination	Protocol	Length	Info
1740	49.638857	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=.....C
1741	49.639700	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1742	49.640702	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1744	49.642315	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1746	49.645319	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1749	49.649705	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1821	53.785833	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1612, FN=0, Flags=....R...C
1822	53.787070	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1612, FN=0, Flags=....R...C
1921	57.889232	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
1922	57.890325	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
1923	57.891321	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
1924	57.896970	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
2122	62.171951	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0, Flags=....R...C
2123	62.172946	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0, Flags=....R...C
2124	62.174070	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0, Flags=....R...C

Fig. 7. Mensagens de autenticação enviadas pelo host

Questão 15: O host tenta usar algum algoritmo de autenticação/chave ou tenta aceder de forma aberta? Existe alguma resposta do AP linksys_SES_24086 ao pedido de autenticação? Porquê?

O host tenta aceder de forma aberta, não necessitando de chave. Não existe nenhuma resposta do AP, isto acontece porque o AP está configurado para exigir uma chave mas como a autenticação é aberta o AP não responde a pedidos de forma aberta.

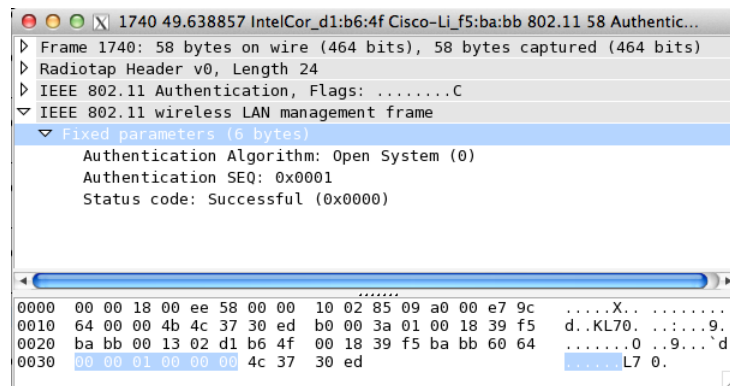


Fig. 8. Pacote Authentication enviado pelo host sem fios ao AP

Questão 16: Identifique as ações 802.11 (após t=63.16s) que decorrem do comportamento analisado na questão anterior e quais os sistemas envolvidos? Usando um filtro apropriado, registre a janela do wireshark que ilustre as tramas de gestão trocadas que ajuda a fundamentar a sua resposta.

As ações que decorrem após t=63.16 são: Association Request (t=63.169910), envia do host para o AP 30 Munroe St, e Association Response (t=63.192101), é a corresponde resposta do AP para o host.

O filtro usado para determinar estas ações foi `wlan.fc.type_subtype == 0||wlan.fc.type_subtype == 1`.

No.	Time	Source	Destination	Protocol	Length	Info
12	0.396690	00:ae:93:3d:0a:4a	ff:ff:ff:ff:bf:4a	802.11	90	Association Response, SN=3073, FN=0, Flags=.....C, SSID=linksy [Malformed P
1227	33.079714	d1:b6:4f:00:16:b6	02:28:00:00:13:02	802.11	111	Association Request, SN=3775, FN=4, Flags=pm...F..
1750	49.651078	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1607, FN=0, Flags=.....C, SSID=linksy
1751	49.653218	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1607, FN=0, Flags=...R...C, SSID=linksy
1824	53.789944	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1613, FN=0, Flags=.....C, SSID=linksy
1825	53.790943	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1613, FN=0, Flags=...R...C, SSID=linksy
1827	53.793568	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1613, FN=0, Flags=.....C, SSID=linksy
1926	57.903699	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=.....C, SSID=linksy
1927	57.904945	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=...R...C, SSID=linksy
1932	57.911195	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=...R...C, SSID=linksy
1933	57.915945	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=...R...C, SSID=linksy
1934	57.924199	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=...R...C, SSID=linksy
1935	57.936216	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=...R...C, SSID=linksy
1937	57.939196	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1620, FN=0, Flags=.....C, SSID=linksy
2126	62.176945	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1645, FN=0, Flags=.....C, SSID=linksy
2127	62.178194	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1645, FN=0, Flags=...R...C, SSID=linksy
2162	63.169910	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	89	Association Request, SN=1648, FN=0, Flags=.....C, SSID=30 Mun
2166	63.192101	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	94	Association Response, SN=3728, FN=0, Flags=.....C
2307	70.179949	Cisco-Li_f5:ba:7b	f9:ff:ff:ff:ff:ff	802.11	132	Fragmented IEEE 802.11 frame

Fig. 9. Tramas de gestão trocadas

Questão 17: Caracterize a nova associação do host com o AP (30 Munroe St).

Através da imagem seguinte é possível verificar o tipo de canal que está a ser usado, 802.11g com um data rate de 54Mb/s, a capacidade do AP e as velocidades/débitos de ligação suportadas, 1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18. Pode suportar ainda adicionalmente: 24(B), 36, 48 e 54 [MBit/sec].

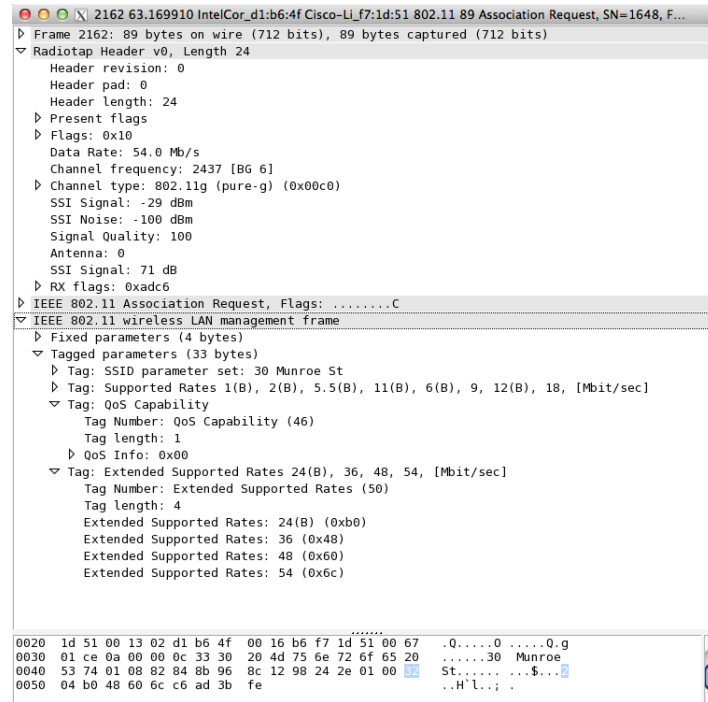
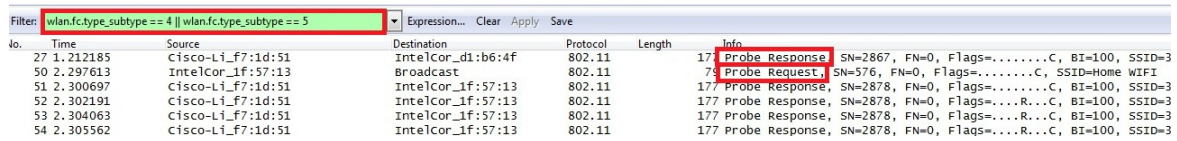


Fig. 10. Tramas de Association Response

1.5 Probing

Questão 18: Quais são os endereços MAC do originador, receptor e BSS ID nestas tramas? Qual é a função deste tipo de tramas?

Através do uso deste filtro: `wlan.fc.type_subtype == 4 || wlan.fc.type_subtype == 5` conseguimos obter simultaneamente os subtipos Probe Request e Probe Response de forma fácil.



No.	Time	Source	Destination	Protocol	Length	Info
27	1.212185	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	177	Probe Response, SN=2867, FN=0, Flags=.....C, BI=100, SSID=3
50	2.297613	IntelCor_1f:57:13	Broadcast	802.11	79	Probe Request, SN=576, FN=0, Flags=.....C, SSID=Home WIFI
51	2.300697	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2878, FN=0, Flags=.....C, BI=100, SSID=3
52	2.302191	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2878, FN=0, Flags=.....C, BI=100, SSID=3
53	2.304063	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2878, FN=0, Flags=.....C, BI=100, SSID=3
54	2.305562	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2878, FN=0, Flags=.....C, BI=100, SSID=3

Fig. 11. Probe Request e Probe Response

Informações da trama Probe Response:

```
IEEE 802.11 Probe Response, Flags: .....C
Type/Subtype: Probe Response (0x05)
[+] Frame Control Field: 0x5000
    .000 0000 0010 1000 = Duration: 40 microseconds
    Receiver address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    Destination address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Source address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Fragment number: 0
    Sequence number: 2867
[+] Frame check sequence: 0xcb4eda28 [correct]
```

Fig. 12. Probe Response

Uma trama Probe Request é usada quando a estação precisa de obter informações de uma outra estação. Uma trama Probe Response contém informações sobre as taxas de dados suportadas.

```
IEEE 802.11 Probe Request, Flags: .....C
Type/Subtype: Probe Request (0x04)
[+] Frame Control Field: 0x4000
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Transmitter address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
    Source address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
    BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
    Fragment number: 0
    Sequence number: 576
[+] Frame check sequence: 0xa373c5ff [correct]
```

Fig. 13. Probe Request

1.6 Opções RTS/CTS

Questão 19: Certifique-se do tipo de canal que está a ser usado e identifique todos os APs que estão a ser anunciados.

O tipo de canal utilizado é o 802.11g e os AP's anunciados foram 2: eduroam e eventos.

Questão 20: Tomando como exemplo a estação cujo endereço MAC é `HonHaiPr_27:46:a2` (`0c : 60 : 76 : 27 : 46 : a2`), identifique a ocorrência de troca de dados envolvendo tramas de controlo RTS/CTS. Verifique a seu sentido de envio (toDS, fromDS). Registe o endereçamento MAC dos sistemas envolvidos, explicando o seu papel no processo de troca de dados.

Aos $t=1.169531000$ s, dá-se a primeira tentativa de uma ocorrência RTS/CTS: um RTS enviado pela estação emissora (`HonHaiPr_27 : 46 : a2`) para a estação receptora `Cisco_95 : 25 : 60`. Não houve resposta. Com isso, a estação emissora reenvia outro RTS para o mesmo destino, aos $t=1.170665000$ s, com a resposta CTS por parte da estação receptora para a estação emissora a surgir aos $t=1.170754000$. Os endereços MAC da estação emissora e receptora são, respectivamente, `0c : 60 : 76 : 27 : 46 : a2` (`HonHaiPr_27 : 46 : a2`) e `00 : 17 : df : 95 : 25 : 60` (`Cisco_95 : 25 : 60`).

Ligação RTS/CTS:

No.	Time	Source	Destination	Protocol	Length	Info
859	1.169531000	HonHaiPr_27:46:a2	Cisco_95:25:60 (RA)	802.11	45	Request-to-send, Flags=.....C
860	1.169769000	HonHaiPr_8a:82:9d	Pentacom_72:03:fc	802.11	119	QoS Data, SN=1402, FN=0, Flags=p....TC
861	1.169840000		HonHaiPr_8a:82:9d (RA)	802.11	39	Acknowledgement, Flags=.....C
862	1.170294000	Pentacom_72:03:fc	HonHaiPr_8a:82:9d	802.11	1499	QoS Data, SN=342, FN=0, Flags=p..R.F.C
863	1.170301000		Cisco_95:25:60 (RA)	802.11	39	Acknowledgement, Flags=.....C
864	1.170665000	HonHaiPr_27:46:a2	Cisco_95:25:60 (RA)	802.11	45	Request-to-send, Flags=.....C
865	1.170754000		HonHaiPr_27:46:a2 (RA)	802.11	39	Clear-to-send, Flags=.....C
866	1.170757000	HonHaiPr_27:46:a2	Pentacom_72:03:fc	802.11	119	QoS Data, SN=2663, FN=0, Flags=p..R..TC
867	1.170804000		HonHaiPr_27:46:a2 (RA)	802.11	39	Acknowledgement, Flags=.....C

Endereços MAC da origem e destino:

```
▶ Frame 864: 45 bytes on wire (360 bits), 45 bytes captured (360 bits) on interface 0
▶ Radiotap Header v0, Length 25
▼ IEEE 802.11 Request-to-send, Flags: .....C
  Type/Subtype: Request-to-send (0x1b)
  ▶ Frame Control Field: 0xb400
    .000 0000 1010 0000 = Duration: 160 microseconds
    Receiver address: Cisco_95:25:60 (00:17:df:95:25:60)
    Transmitter address: HonHaiPr_27:46:a2 (0c:60:76:27:46:a2)
  ▶ Frame check sequence: 0x4bd02881 [correct]
```

2 Conclusões

Verificamos informação do nível físico (rádio), para além dos *bytes* correspondentes a tramas 802.11. Foi-nos possível identificar a frequência do espectro da rede sem fios, a que débito foi enviada a trama escolhida, o número e tipo de canal de uma comunicação rádio e qual o índice da qualidade do sinal.

Pudemos aprofundar os conhecimentos sobre as tramas beacon. Desde o seu tipo e subtipo aos endereços MAC por elas usadas. Conseguimos também, perceber melhor o uso que os Access Points 802.11 fazem destas tramas.

Ficamos a saber que não houve ocorrências RTS/CTS na captura Wireshark_802_11.pca, apenas ligações ACK.

Identificado a trama de controlo envolvido nessa captura, foi explicado o “three-way handshake” entre um cliente e o servidor. A restante resolução dessa secção ocorreu sem maior dificuldade, já que correspondia apenas na análise do tráfego no wireshark da captura em estudo.

Já na parte de associação e desassociação, vimos como funcionam alguns filtros do wireshark, tais como verificar as tramas de autenticação, pedidos e respostas de associação. Percebeu-se como um host tenta fazer a autenticação com o ap.

Percebemos as funções entre tramas PROBE REQUEST e PROBE RESPONSE. Vendo as suas evidentes diferenças.

Nas opções RTS/CTS, a maior dificuldade foi encontrar a primeira ligação RTS/CTS contendo a estação HonHaiPr_27:46:a2 e os AP's envolvidos, numa vasta lista da captura crc2013-eduroam.pcap. Depois foi fácil a resolução da restante secção.