

TP4: Redes sem fios (802.11)

Diogo Afonso Costa, Daniel Maia, and Vitor Castro

University of Minho, Department of Informatics, 4710-057 Braga, Portugal
e-mail: {a78034,a77531,a77870}@alunos.uminho.pt

Abstract. Este trabalho tem como objectivo explorar as particularidades do protocolo IEEE 802.11, especificamente, o formato das tramas, o endereçamento dos componentes envolvidos na comunicação sem fios e os tipos de tramas mais comuns, bem como a operação do protocolo.

1 Introdução

2 Acesso Rádio (Para a trama correspondente 733)

2.1 Exercício 1

Questão

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

Resposta

A rede sem fios encontra-se a operar numa frequência de 2462MHz, que consequentemente pertence ao espectro dos 2GHz.

Além disso, o canal usado é o número 11.

Realização

```
Radiotap Header v0, Length 25
Header revision: 0
Header pad: 0
Header length: 25
Present flags
MAC timestamp: 186492754
Flags: 0x10
Data Rate: 1,0 Mb/s
Channel frequency: 2462 [BG 11]
Channel flags: 0x0480, 2 GHz spectrum, Dynamic CCK-OFDM
...0... = Turbo: False
...0... = Complementary Code Keying (CCK): False
...0... = Orthogonal Frequency-Division Multiplexing (OFDM): False
...1... = 2 GHz spectrum: True
...0... = 5 GHz spectrum: False
...0... = Passive: False
...1... = Dynamic CCK-OFDM: True
...0... = Gaussian Frequency Shift Keying (GFSK): False
...0... = GSM (900MHz): False
...0... = Static Turbo: False
...0... = Half Rate Channel (10MHz Channel Width): False
...0... = Quarter Rate Channel (5MHz Channel Width): False
SSI Signal: -74dBm
SSI Noise: -85dBm
Antenna: 0
802.11 radio information
PHY type: 802.11g (6)
Short preamble: False
Proprietary mode: None (0)
Data rate: 1,0 Mb/s
Channel: 11
Frequency: 2462MHz
Signal strength (dbm): -74dBm
Noise level (dbm): -85dBm
TSF timestamp: 186492754
[Duration: 1992µs]
```

Fig. 1: Frequência do espectro em que a rede sem fios se encontra a operar assim como o respetivo canal.

2.2 Exercício 2

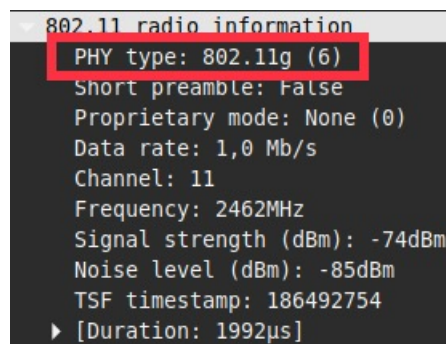
Questão

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

Resposta

A versão utilizada é a IEEE 802.11g.

Realização



```
802.11 radio information
  PHY type: 802.11g (6)
  Short preamble: False
  Proprietary mode: None (0)
  Data rate: 1,0 Mb/s
  Channel: 11
  Frequency: 2462MHz
  Signal strength (dBm): -74dBm
  Noise level (dBm): -85dBm
  TSF timestamp: 186492754
  ▶ [Duration: 1992µs]
```

Fig. 2: Versão da norma IEEE utilizada.

2.3 Exercício 3

Questão

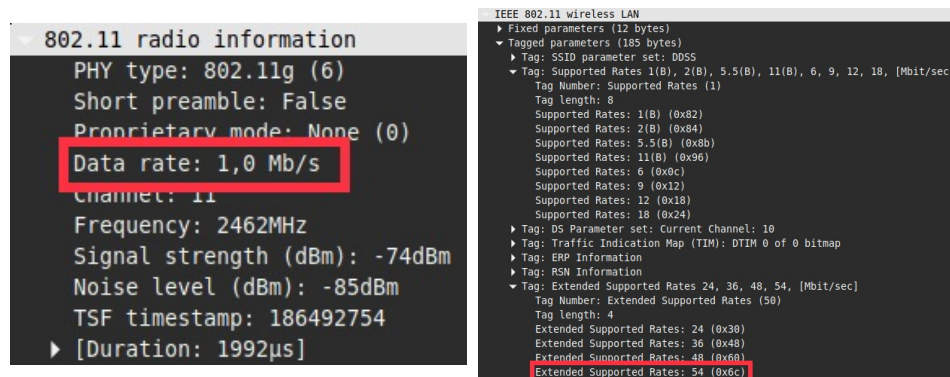
Qual o débito a que foi enviada a trama escolhida? Será que esse débito corresponde ao débito máximo a que a interface WiFi pode operar? Justifique.

Resposta

A trama escolhida foi enviada a 1.0 Mb/s. Visto tratar-se de uma trama que usa a norma IEEE 802.11g tem-se por defeito acesso a débitos até 54 Mb/s [1].

Efetivamente, a razão pela qual o débito se encontra consideravelmente baixo em relação ao máximo permitido pode resultar de diferentes fatores. Nomeadamente, quando a distância entre o *host* e o ponto de acesso (AP) aumenta, o *signal-to-noise ratio* (SNR) aumenta e o bit error ratio (BER) também. Por forma a combater o declínio na qualidade da ligação, caso a distância assim o justifique, o débito a que a trama é transmitida pode ser diminuído por forma a aumentar o SNR e o BER. Deste modo, também por esta razão a frequência que se encontra a operar a ligação seja relativamente baixa (2462 MHz) quando comparada com a frequência máxima que uma ligação 802.11g pode oferecer, ou seja, 5 GHz [1] [2] [3].

Realização



The figure consists of two side-by-side screenshots from a network analysis tool. The left screenshot, titled '802.11 radio information', shows various parameters: PHY type: 802.11g (6), Short preamble: False, Proprietary mode: None (0), Data rate: 1,0 Mb/s (highlighted with a red box), Channel: 11, Frequency: 2462MHz, Signal strength (dBm): -74dBm, Noise level (dBm): -85dBm, TSF timestamp: 186492754, and Duration: 1992µs. The right screenshot, titled 'IEEE 802.11 wireless LAN', shows a tree view of parameters. Under 'Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6, 9, 12, 18, [Mbit/sec]', it lists supported rates: 1(B) (0x82), 2(B) (0x84), 5.5(B) (0x8b), 11(B) (0x96), 6 (0x0c), 9 (0x12), 12 (0x18), and 18 (0x24). Under 'Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]', it lists extended supported rates: 24 (0x30), 36 (0x48), 48 (0x60), and 54 (0x6c) (highlighted with a red box).

Fig. 3: Comparação do débito da trama com o máximo permitido na norma 802.11g.

3 Scanning Passivo e Scanning Ativo

3.1 Exercício 4

Questão

Selecione uma trama beacon (cujo número de ordem inclua o seu número de grupo [33]). 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 (ver anexo)?

Resposta

[Trama nº 233] Esta trama é uma *Management Frame* (identificador 00) de subtipo *Beacon* (identificador 1000 em binário, 8 em decimal). Os identificadores estão presentes em IEEE 802.11 Beacon Frame, no campo Frame Control, nos bits 4-5 e 0-3, respetivamente.

Realização

No.	Time	Source	Destination	Protocol	Length	Info
221	5.328037	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3035, FH=0, Flags=.....C, BI=100, SSID=ZON-2770
222	5.329996	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3036, FH=0, Flags=.....C, BI=100, SSID=FOU_ZON_FREE_INTERNET
223	5.363373	Tp-LinkT_ee:f4:ca	Broadcast	802.11	250	Beacon frame, SN=2171, FH=0, Flags=.....C, BI=100, SSID=DOSS5
224	5.430388	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3037, FH=0, Flags=.....C, BI=100, SSID=ZON-2770
225	5.432251	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3038, FH=0, Flags=.....C, BI=100, SSID=FOU_ZON_FREE_INTERNET
226	5.532811	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3039, FH=0, Flags=.....C, BI=100, SSID=ZON-2770
227	5.534673	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3040, FH=0, Flags=.....C, BI=100, SSID=FOU_ZON_FREE_INTERNET
228	5.635164	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3041, FH=0, Flags=.....C, BI=100, SSID=ZON-2770
229	5.637059	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3042, FH=0, Flags=.....C, BI=100, SSID=FOU_ZON_FREE_INTERNET
230	5.670182	Tp-LinkT_ee:f4:ca	Broadcast	802.11	250	Beacon frame, SN=2175, FH=0, Flags=.....C, BI=100, SSID=DOSS5
231	5.737657	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3043, FH=0, Flags=.....C, BI=100, SSID=ZON-2770
232	5.739472	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3044, FH=0, Flags=.....C, BI=100, SSID=FOU_ZON_FREE_INTERNET
233	5.839995	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3045, FH=0, Flags=.....C, BI=100, SSID=ZON-2770
234	5.841959	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3046, FH=0, Flags=.....C, BI=100, SSID=FOU_ZON_FREE_INTERNET
235	5.942522	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3047, FH=0, Flags=.....C, BI=100, SSID=ZON-2770
236	5.944342	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3048, FH=0, Flags=.....C, BI=100, SSID=FOU_ZON_FREE_INTERNET
237	5.977022	Tp-LinkT_ee:f4:ca	Broadcast	802.11	250	Beacon frame, SN=2178, FH=0, Flags=.....C, BI=100, SSID=DOSS5
238	6.044920	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3049, FH=0, Flags=.....C, BI=100, SSID=ZON-2770
239	6.046755	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3050, FH=0, Flags=.....C, BI=100, SSID=FOU_ZON_FREE_INTERNET

> Frame 233: 315 bytes on wire (2520 bits), 315 bytes captured (2520 bits) on Interface 0

> Radiotap Header v0, Length 25

> 802.11 radio information

IEEE 802.11 Beacon frame, Flags=.....C

▼ Type/Subtype: Beacon frame (0x0000)

▼ Frame Control Field: 0x0000

.... 00 = Version: 0

.... 00.. = Type: Management frame (0)

1000 = Subtype: 8

> Flags: 0x00

.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: HitronTe_1b:27:78 (bc:14:01:1b:27:78)

Source address: HitronTe_1b:27:78 (bc:14:01:1b:27:78)

855 Id: HitronTe_1b:27:78 (bc:14:01:1b:27:78)

..... 0000 = Fragment number: 0

1011 1110 0101 = Sequence number: 3045

Fig. 4: Os identificadores do tipo e subtipo da trama *Beacon*.

3.2 Exercício 5

Questão

Liste todos os SSIDs dos APs (Access Points) que estão a operar na vizinhança da STA de captura? Explícite o modo como obteve essa informação. Como sugestão pode construir um filtro de visualização apropriado (tomando como base a resposta da alínea anterior) que lhe permita obter a listagem pretendida.

Resposta

Ao aplicar o filtro `wlan.fc == 0x8000`, obtém-se todas as tramas *beacon*, enviadas pelos AP's circundantes. Observando o campo IEEE 802.11 wireless LAN -> Tagged parameters -> Tag: SSID parameter set -> SSID ao longo das tramas capturadas, determina-se que existem 3 AP's, com os SSID's ZON-2770, FON_ZON_FREE_INTERNET e DDSS.

Realização

No.	Time	Source	Destination	Protocol	Length	Info
227	5.534673	HitronTe_lb:27:79	Broadcast	802.11	233	Beacon frame, SNI=3848, FNI=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
228	5.635164	HitronTe_lb:27:78	Broadcast	802.11	315	Beacon frame, SNI=3841, FNI=0, Flags=.....C, BI=100, SSID=ZON-2770
229	5.637859	HitronTe_lb:27:79	Broadcast	802.11	233	Beacon frame, SNI=3842, FNI=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
230	5.678182	Tp-LinkT_eef4:ca	Broadcast	802.11	250	Beacon frame, SNI=2175, FNI=0, Flags=.....C, BI=100, SSID=DDSS
231	5.737657	HitronTe_lb:27:78	Broadcast	802.11	315	Beacon frame, SNI=3843, FNI=0, Flags=.....C, BI=100, SSID=ZON-2770
232	5.739472	HitronTe_lb:27:79	Broadcast	802.11	233	Beacon frame, SNI=3844, FNI=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
233	5.839995	HitronTe_lb:27:78	Broadcast	802.11	315	Beacon frame, SNI=3845, FNI=0, Flags=.....C, BI=100, SSID=ZON-2770
234	5.841959	HitronTe_lb:27:79	Broadcast	802.11	233	Beacon frame, SNI=3846, FNI=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
235	5.942522	HitronTe_lb:27:78	Broadcast	802.11	315	Beacon frame, SNI=3847, FNI=0, Flags=.....C, BI=100, SSID=ZON-2770
236	5.944342	HitronTe_lb:27:79	Broadcast	802.11	233	Beacon frame, SNI=3848, FNI=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
237	5.977822	Tp-LinkT_eef4:ca	Broadcast	802.11	250	Beacon frame, SNI=2176, FNI=0, Flags=.....C, BI=100, SSID=DDSS
238	6.044920	HitronTe_lb:27:78	Broadcast	802.11	315	Beacon frame, SNI=3849, FNI=0, Flags=.....C, BI=100, SSID=ZON-2770
239	6.046755	HitronTe_lb:27:79	Broadcast	802.11	233	Beacon frame, SNI=3850, FNI=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
240	6.079395	Tp-LinkT_eef4:ca	Broadcast	802.11	250	Beacon frame, SNI=2179, FNI=0, Flags=.....C, BI=100, SSID=DDSS
241	6.147388	HitronTe_lb:27:78	Broadcast	802.11	315	Beacon frame, SNI=3851, FNI=0, Flags=.....C, BI=100, SSID=ZON-2770
242	6.149175	HitronTe_lb:27:79	Broadcast	802.11	233	Beacon frame, SNI=3852, FNI=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
243	6.250848	HitronTe_lb:27:78	Broadcast	802.11	315	Beacon frame, SNI=3853, FNI=0, Flags=.....C, BI=100, SSID=ZON-2770
244	6.251932	HitronTe_lb:27:79	Broadcast	802.11	233	Beacon frame, SNI=3854, FNI=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
245	6.352652	HitronTe_lb:27:78	Broadcast	802.11	315	Beacon frame, SNI=3855, FNI=0, Flags=.....C, BI=100, SSID=ZON-2770

> Frame 233: 315 bytes on wire (2520 bits), 315 bytes captured (2520 bits) on Interface 0

> Radiotap Header v0, Length 25

> 802.11 radio information

> IEEE 802.11 Beacon frame, Flags:C

> Fixed parameters (12 bytes)

> Tagged parameters (250 bytes)

> Tag: SSID parameter set: ZON-2770

> Tag Number: SSID parameter set (0)

> Tag Length: 8

> SSID: ZON-2770

> Tag: Supported Rates 1(0), 2(0), 5.5(0), 11(0), 9, 18, 36, 54, [Mbit/sec]

> Tag: DS Parameter set: Current Channel: 11

> Tag: Extended Supported Rates 6, 12, 24, 48, [Mbit/sec]

> Tag: AP Channel Report: Operating Class 32, Channel List : 1, 2, 3, 4, 5, 6, 7,

> Tag: AP Channel Report: Operating Class 33, Channel List : 5, 6, 7, 8, 9, 10, 11,

> Tag: Vendor Specific: Microsoft: WPS

> Tag: Traffic Indication Map (TIM): DTIM 2 of 0 bitmap

> Tag: ERP Information

> Tag: HT Capabilities (802.11n D1.10)

Fig. 5: O SSID da trama 233; O Wireshark destaca esta informação por defeito.

Questão

Resposta

Realização

Fig. 6: O campo FCS de uma trama corrompida; nota-se que o *Wireshark* destaca os campos corrompidos.

3.4 Exercício 7

Questão

Para dois dos APs identificados, indique qual é o intervalo de tempo previsto entre tramas beacon consecutivas? (Nota: este valor é anunciado na própria trama beacon). Na prática, a periodicidade de tramas beacon é verificada? Tente explicar porquê.

Resposta

SSID ZON-2770: intervalo de acordo com a trama: 0.102400 s

SSID FON_ZON_FREE_INTERNET: intervalo de acordo com a trama: 0.102400 s

Na prática, o valor do intervalo de tempo varia cerca de ± 0.0001 s relativamente ao intervalo previsto. Isto pode se dever ao facto de que é necessário fazer deteção de erros ao receber cada trama. Isto é tido em conta pelo beacon interval e, como o tempo necessário para fazer a verificação é imutável, ocorrem pequenas variâncias no intervalo entre tramas.

Realização

No.	Time	Source	Destination	Protocol	Length	Info
225	5.432251	HitronTe_ib:27:79	Broadcast	802.11	233	Beacon frame, SN=3038, FH=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
226	5.532811	HitronTe_ib:27:79	Broadcast	802.11	315	Beacon frame, SN=3039, FH=0, Flags=.....C, BI=100, SSID=ZON-2770
227	5.534673	HitronTe_ib:27:79	Broadcast	802.11	233	Beacon frame, SN=3040, FH=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
228	5.635164	HitronTe_ib:27:79	Broadcast	802.11	315	Beacon frame, SN=3041, FH=0, Flags=.....C, BI=100, SSID=ZON-2770
229	5.637059	HitronTe_ib:27:79	Broadcast	802.11	233	Beacon frame, SN=3042, FH=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
230	5.670182	Tp-Link_eef4:ca	Broadcast	802.11	250	Beacon frame, SN=2175, FH=0, Flags=.....C, BI=100, SSID=0055
231	5.737657	HitronTe_ib:27:79	Broadcast	802.11	315	Beacon frame, SN=3043, FH=0, Flags=.....C, BI=100, SSID=ZON-2770
232	5.739472	HitronTe_ib:27:79	Broadcast	802.11	233	Beacon frame, SN=3044, FH=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
233	5.839995	HitronTe_ib:27:79	Broadcast	802.11	315	Beacon frame, SN=3045, FH=0, Flags=.....C, BI=100, SSID=ZON-2770
234	5.841955	HitronTe_ib:27:79	Broadcast	802.11	233	Beacon frame, SN=3046, FH=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
235	5.942522	HitronTe_ib:27:79	Broadcast	802.11	233	Beacon frame, SN=3047, FH=0, Flags=.....C, BI=100, SSID=ZON-2770
236	5.944342	HitronTe_ib:27:79	Broadcast	802.11	233	Beacon frame, SN=3048, FH=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
237	5.977022	Tp-Link_eef4:ca	Broadcast	802.11	250	Beacon frame, SN=2178, FH=0, Flags=.....C, BI=100, SSID=0055
238	6.044920	HitronTe_ib:27:79	Broadcast	802.11	315	Beacon frame, SN=3049, FH=0, Flags=.....C, BI=100, SSID=ZON-2770
239	6.046755	HitronTe_ib:27:79	Broadcast	802.11	233	Beacon frame, SN=3050, FH=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
240	6.079395	Tp-Link_eef4:ca	Broadcast	802.11	250	Beacon frame, SN=2179, FH=0, Flags=.....C, BI=100, SSID=0055
241	6.147308	HitronTe_ib:27:79	Broadcast	802.11	315	Beacon frame, SN=3051, FH=0, Flags=.....C, BI=100, SSID=ZON-2770
242	6.149175	HitronTe_ib:27:79	Broadcast	802.11	233	Beacon frame, SN=3052, FH=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
243	6.250408	HitronTe_ib:27:79	Broadcast	802.11	315	Beacon frame, SN=3053, FH=0, Flags=.....C, BI=100, SSID=ZON-2770
244	6.251932	HitronTe_ib:27:79	Broadcast	802.11	233	Beacon frame, SN=3054, FH=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET

Frame 233: 315 bytes on wire (2520 bits), 315 bytes captured (2520 bits) on interface 0

Radiotap Header v0, Length 25

802.11 radio information

IEEE 802.11 Beacon frame, Flags:C

IEEE 802.11 Wireless LAN

Fixed parameters (12 bytes)

Timestamp: 0x00000193da553143

Beacon Interval: 0.102400 (seconds)

Capabilities Information: 0x0431

Tagged parameters (250 bytes)

Tag: SSID parameter set: ZON-2770

Fig. 7: Um exemplo de um intervalo real entre duas tramas beacon do mesmo AP, igual a 0.102527 s.

No.	Time	Source	Destination	Protocol	Length	Info
225	5.432251	HitronTe_ib:27:79	Broadcast	002.11	233	Beacon frame, SN=3038, FH=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
226	5.532811	HitronTe_ib:27:79	Broadcast	002.11	315	Beacon frame, SN=3039, FH=0, Flags=.....C, BI=100, SSID=ZON-2770
227	5.534673	HitronTe_ib:27:79	Broadcast	002.11	233	Beacon frame, SN=3040, FH=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
228	5.635164	HitronTe_ib:27:79	Broadcast	002.11	315	Beacon frame, SN=3041, FH=0, Flags=.....C, BI=100, SSID=ZON-2770
229	5.637959	HitronTe_ib:27:79	Broadcast	002.11	233	Beacon frame, SN=3042, FH=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
230	5.670182	Tp-LinkT_e:fa:ca	Broadcast	002.11	250	Beacon frame, SN=2175, FH=0, Flags=.....C, BI=100, SSID=0055
231	5.737657	HitronTe_ib:27:79	Broadcast	002.11	315	Beacon frame, SN=3043, FH=0, Flags=.....C, BI=100, SSID=ZON-2770
232	5.739472	HitronTe_ib:27:79	Broadcast	002.11	233	Beacon frame, SN=3044, FH=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
233	5.832995	HitronTe_ib:27:79	Broadcast	002.11	315	Beacon frame, SN=3045, FH=0, Flags=.....C, BI=100, SSID=ZON-2770
234	5.841959	HitronTe_ib:27:79	Broadcast	002.11	233	Beacon frame, SN=3046, FH=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
235	5.842522	HitronTe_ib:27:79	Broadcast	002.11	315	Beacon frame, SN=3047, FH=0, Flags=.....C, BI=100, SSID=ZON-2770
236	5.944342	HitronTe_ib:27:79	Broadcast	002.11	233	Beacon frame, SN=3048, FH=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
237	5.977822	Tp-LinkT_e:fa:ca	Broadcast	002.11	250	Beacon frame, SN=2176, FH=0, Flags=.....C, BI=100, SSID=0055
238	6.044920	HitronTe_ib:27:79	Broadcast	002.11	315	Beacon frame, SN=3049, FH=0, Flags=.....C, BI=100, SSID=ZON-2770
239	6.046755	HitronTe_ib:27:79	Broadcast	002.11	233	Beacon frame, SN=3050, FH=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
240	6.079395	Tp-LinkT_e:fa:ca	Broadcast	002.11	250	Beacon frame, SN=2179, FH=0, Flags=.....C, BI=100, SSID=0055
241	6.147380	HitronTe_ib:27:79	Broadcast	002.11	315	Beacon frame, SN=3051, FH=0, Flags=.....C, BI=100, SSID=ZON-2770
242	6.149175	HitronTe_ib:27:79	Broadcast	002.11	233	Beacon frame, SN=3052, FH=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET
243	6.250840	HitronTe_ib:27:79	Broadcast	002.11	315	Beacon frame, SN=3053, FH=0, Flags=.....C, BI=100, SSID=ZON-2770
244	6.251932	HitronTe_ib:27:79	Broadcast	002.11	233	Beacon frame, SN=3054, FH=0, Flags=.....C, BI=100, SSID=FON_ZON_FREE_INTERNET


```

> Frame 234: 233 bytes on wire (1864 bits), 233 bytes captured (1864 bits) on interface 0
> Radiotap Header v0, Length 25
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: .....C
  IEEE 802.11 wireless LAN
    Fixed parameters (12 bytes)
      Timestamp: 0x00000193da653b25
      Beacon Interval: 0.102400 (Seconds)
      Capabilities Information: 0x0421
    Tagged parameters (168 bytes)
      Tag: SSID parameter set: FON_ZON_FREE_INTERNET

```

Fig. 8: Um exemplo de um intervalo real entre duas tramas beacon do mesmo AP, igual a 0.102383 s.

3.5 Exercício 8

Questão

Identifique e registre todos os endereços MAC usados nas tramas beacon enviadas pelos APs. Recorde que o endereçamento está definido no cabeçalho das tramas 802.11, podendo ser utilizados até quatro endereços com diferente semântica. Para uma descrição detalhada da estrutura da trama 802.11, consulte o anexo ao enunciado.

Resposta

Realização

3.6 Exercício 9

Questão

As tramas beacon anunciam que o AP pode suportar vários débitos de base assim como vários “extended supported rates”. Indique quais são esses débitos?

Resposta

Realização

3.7 Exercício 10

Questão

Estabeleça um filtro Wireshark apropriado que lhe permita visualizar todas as tramas probing request ou probing response, simultaneamente.

Resposta

Realização

3.8 Exercício 11

Questão

Identifique um probing request para o qual tenha havido um probing response. Face ao endereçamento usado, indique a que sistemas são endereçadas estas tramas e explique qual o propósito das mesmas?

Resposta

Realização

4 Processo de Associação

4.1 Exercício 12

Questão

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

Resposta

Uma possível sequência de tramas que correspondem a um processo de associação completo são as identificadas pelos números 2027 (autenticação STA -> AP), 2029 (autenticação AP -> STA), 2031 (pedido de associação) e 2035 (resposta ao pedido de associação). Além destas é possível identificar tramas de confirmação de recepção (*Acknowledgment*) entre todas as tramas trocadas entre o STA e o AP.

Realização

2027	57.879041	Apple_d1:fe:a8	HitronTe_1b:27:78	802.11	70 Authentication, SN=1147, FN=0, Flags=.....C	16:20:55,012164
2028	57.879219		Apple_d1:fe:a8 (a4:d1:802.11)	39 Acknowledgement, Flags=.....C	16:20:55,012342	
2029	57.879965	HitronTe_1b:27:78	Apple_d1:fe:a8	802.11	59 Authentication, SN=3308, FN=0, Flags=.....C	16:20:55,013088
2030	57.880197		HitronTe_1b:27:78 (bc:802.11)	39 Acknowledgement, Flags=.....C	16:20:55,013320	
2031	57.881708	Apple_d1:fe:a8	HitronTe_1b:27:78	802.11	185 Association Request, SN=1148, FN=0, Flags=.....	16:20:55,014831
2032	57.882083		Apple_d1:fe:a8 (a4:d1:802.11)	39 Acknowledgement, Flags=.....C	16:20:55,015206	
2033	57.887191	HitronTe_1b:27:78	Broadcast	802.11	315 Beacon frame, SN=4061, FN=0, Flags=.....C, BI	16:20:55,020314
2034	57.888974	HitronTe_1b:27:79	Broadcast	802.11	233 Beacon frame, SN=4062, FN=0, Flags=.....C, BI	16:20:55,022097
2035	57.890902	HitronTe_1b:27:78	Apple_d1:fe:a8	802.11	225 Association Response, SN=3309, FN=0, Flags=.....	16:20:55,024025
2036	57.891033		HitronTe_1b:27:78 (bc:802.11)	39 Acknowledgement, Flags=.....C	16:20:55,024156	

Fig. 9: Sequência de tramas trocadas no processo de associação.

4.2 Exercício 13

Questão

Efetue um diagrama que ilustre a sequência de todas as tramas trocadas no processo.

Resposta

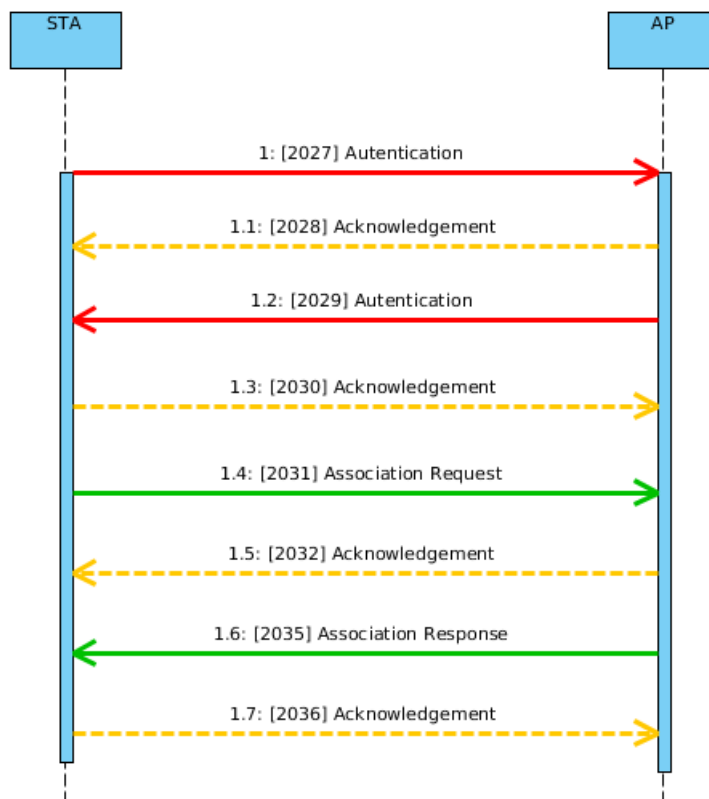


Fig. 10: Diagrama da sequência de tramas trocadas no processo de associação, realizado no *Visual Paradigm*.

Realização

5 Transferência de Dados

5.1 Exercício 14

Questão

Considere a trama de dados nº1054. 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?

Resposta

Realização

5.2 Exercício 15

Questão

Para a trama de dados nº1054, 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?

Resposta

Realização

5.3 Exercício 16

Questão

Como interpreta a trama nº 1060 face à sua direccionalidade e endereçamento MAC?

Resposta

Realização

5.4 Exercício 17

Questão

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.)

Resposta

Realização

5.5 Exercício 18

Questão

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. Para o exemplo acima, verifique se está a ser usada a opção RTS/CTS na troca de dados entre a STA e o AP/Router da WLAN, identificando a direccionalidade das tramas e os sistemas envolvidos.

Resposta

Realização

6 Conclusões

Neste trabalho foi abordada a camada de ligação lógica da pilha OSI e alguns dos seus componentes.

Primeiramente, procedeu-se à compreensão das tramas *ethernet* que permitiu consolidar bases para analisar as mensagens de ARP e as suas características. A compreensão do protocolo ARP, auxiliada pelos exercícios propostos, permitiu perceber a área em que este protocolo atua e quais as suas consequências.

Por fim, percebeu-se o impacto que têm os diferentes sistemas que constituem a rede. Nomeadamente, o domínio de colisão depende em grande parte da topologia utilizada e caso esta não previna antecipadamente as colisões de tramas na rede, são então utilizados protocolos que tem como objetivo evitar essas mesmas colisões através de diferentes abordagens, como é o caso do protocolo CSMA/CD que apenas transmite quando a rede se encontra desocupada.

References

1. James F. Kurose, K.W.R.: Computer Networking: A Top Down Approach. (Addison-Wesley)
2. Wikipedia: Bit error rate. https://en.wikipedia.org/wiki/Bit_error_rate (2017) [Online; acedido a 10-Dezembro-2017].
3. Wikipedia: Relação sinal-ruído. https://pt.wikipedia.org/wiki/Rela%C3%A7%C3%A3o_sinal-ru%C3%ADdo (2017) [Online; acedido a 10-Dezembro-2017].