

eTP4: Redes Sem Fios (802.11)

Filipa Correia Parente, José André Martins Pereira, Ricardo André Gomes
Petronilho

University of Minho, Department of Informatics, 4710-057 Braga, Portugal e-mail:
{a82145,a82880,a81744}@alunos.uminho.pt

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

```
▶ Frame 321: 296 bytes on wire (2368 bits), 296 bytes captured (2368 bits)
▶ Radiotap Header v0, Length 25
▼ 802.11 radio information
    PHY type: 802.11g (6)
    Short preamble: False
    Proprietary mode: None (0)
    Data rate: 1.0 Mb/s
    Channel: 12
    Frequency: 2467MHz
    Signal strength (dBm): -64dBm
    Noise level (dBm): -87dBm
    TSF timestamp: 32702365
    ▶ [Duration: 2360µs]
▶ IEEE 802.11 Beacon frame, Flags: .....C
▶ IEEE 802.11 wireless LAN
```

Figura 1 –Campo radio information da trama 321.

Resposta:

A frequência do espectro é 2465MHz e o respetivo canal é o 12, tal como se pode ver no retângulo a vermelho.

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

Resposta:

A versão da norma **IEEE 802.11** é g (6), tal como se pode ver no retângulo azul.

3) 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.

```
▶ Frame 321: 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
▼ IEEE 802.11 wireless LAN
  ▶ Fixed parameters (12 bytes)
  ▼ Tagged parameters (231 bytes)
    ▶ Tag: SSID parameter set: FlyingNet
    ▶ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 9, 18, 36, 54, [Mbit/sec]
    ▶ Tag: DS Parameter set: Current Channel: 12
```

Figura 2 – Data rates suportados pelo AP.

Resposta:

O débito a que foi enviada a trama foi de 1 Mbit/s, como se pode verificar na **Figura 1**, no retângulo verde, no entanto esse débito não corresponde ao máximo, pois este é 54 Mbit/s, tal como se pode ver na Figura 2 no campo **Supported Rates**.

4) Selecione uma *trama beacon* (e.g., a trama 3XX). 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:

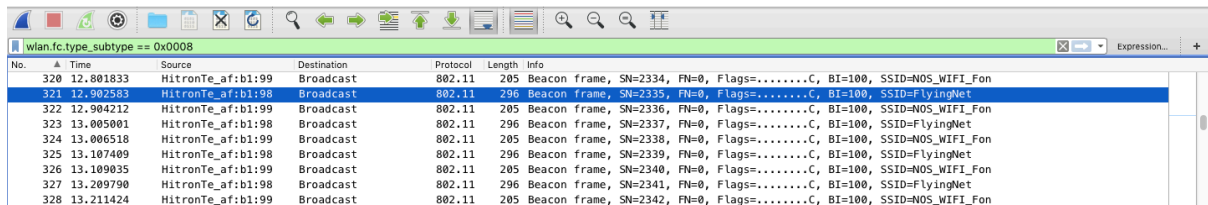
```
▶ Frame 321: 296 bytes on wire (2368 bits), 296 bytes captured (2368 bits)
▶ Radiotap Header v0, Length 25
▶ 802.11 radio information
▼ IEEE 802.11 Beacon frame, Flags: .....C
  Type/Subtype: Beacon frame (0x0008)
  ▼ Frame Control Field: 0x8000
    .... ..00 = Version: 0
    .... 00.. = Type: Management frame (0)
    1000 .... = Subtype: 8
  ▶ Flags: 0x00
```

Figura 3 – Tipo e subtipo da trama 802.11.

O tipo do Beacon frame é **Management frame (0)** e o subtipo é 8.

5) Liste todos os SSIDs dos APs (*Access Points*) que estão a operar na vizinhança da STA de captura? Explique 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:



| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|-------------------|-------------|----------|--------|--|
| 320 | 12.801833 | HitronTe_af:b1:98 | Broadcast | 802.11 | 205 | Beacon frame, SN=2334, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon |
| 321 | 12.902583 | HitronTe_af:b1:98 | Broadcast | 802.11 | 296 | Beacon frame, SN=2335, FN=0, Flags=.....C, BI=100, SSID=FlyingNet |
| 322 | 12.904212 | HitronTe_af:b1:98 | Broadcast | 802.11 | 205 | Beacon frame, SN=2336, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon |
| 323 | 13.005001 | HitronTe_af:b1:98 | Broadcast | 802.11 | 296 | Beacon frame, SN=2337, FN=0, Flags=.....C, BI=100, SSID=FlyingNet |
| 324 | 13.006518 | HitronTe_af:b1:98 | Broadcast | 802.11 | 205 | Beacon frame, SN=2338, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon |
| 325 | 13.107409 | HitronTe_af:b1:98 | Broadcast | 802.11 | 296 | Beacon frame, SN=2339, FN=0, Flags=.....C, BI=100, SSID=FlyingNet |
| 326 | 13.109035 | HitronTe_af:b1:98 | Broadcast | 802.11 | 205 | Beacon frame, SN=2340, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon |
| 327 | 13.209790 | HitronTe_af:b1:98 | Broadcast | 802.11 | 296 | Beacon frame, SN=2341, FN=0, Flags=.....C, BI=100, SSID=FlyingNet |
| 328 | 13.211424 | HitronTe_af:b1:98 | Broadcast | 802.11 | 205 | Beacon frame, SN=2342, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon |

Figura 4 – Filtro dos Beacons com o tipo/subtipo = 0x0008.

Os **SSIDs** dos **APs** são: **NOS_WIFI_Fon**, **FlyingNet**, sendo que esta informação foi obtida usando um filtro (**wlan.fc.type_subtype == 0x0008**), uma vez que as tramas de **Gestão Beacon** tem o tipo e **subtipo == 0x0008**, que é o valor obtido na alínea anterior.

6) Verifique se está a ser usado o método de detecção de erros (CRC), e se todas as tramas Beacon são recebidas corretamente. Justifique o porquê de usar detecção de erros neste tipo de redes locais.

Resposta:

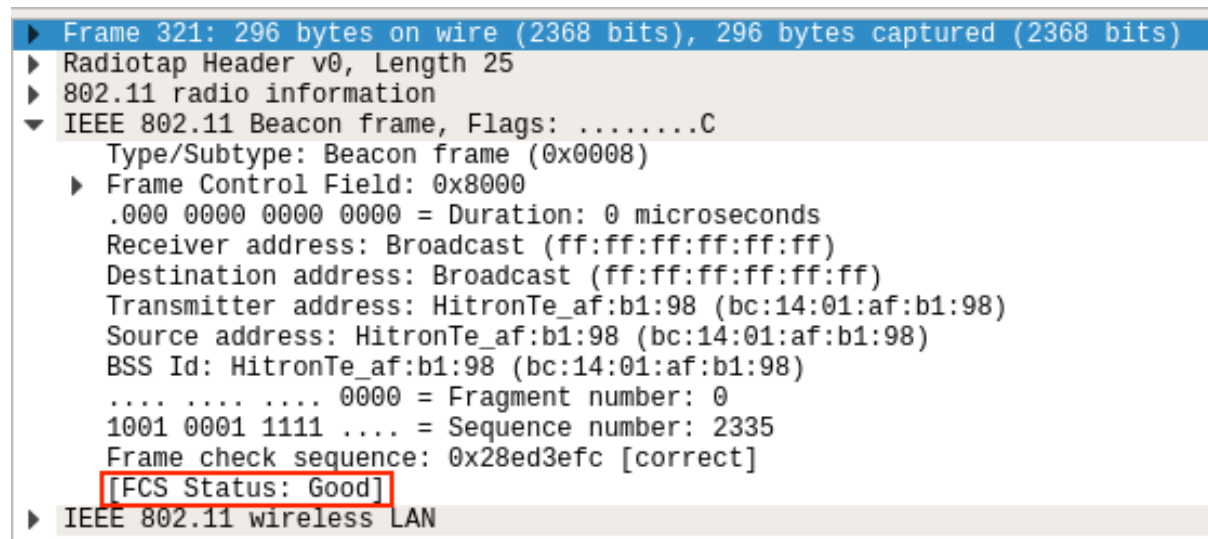


Figura 5 – Campo FCS presente em trama Beacon.

Tendo em conta a existência nas tramas do Frame Check Sequence (ou FCS), é possível concluir que o método de detecção de erros (CRC) está a ser usado.

Analisando as tramas Beacon, neste caso proveniente dos AP's (estações), é possível observar no campo FCS status, que o estado do FCS é bom. Isto quer dizer que a trama enviada chegou ao destino sem erros.

7) 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:

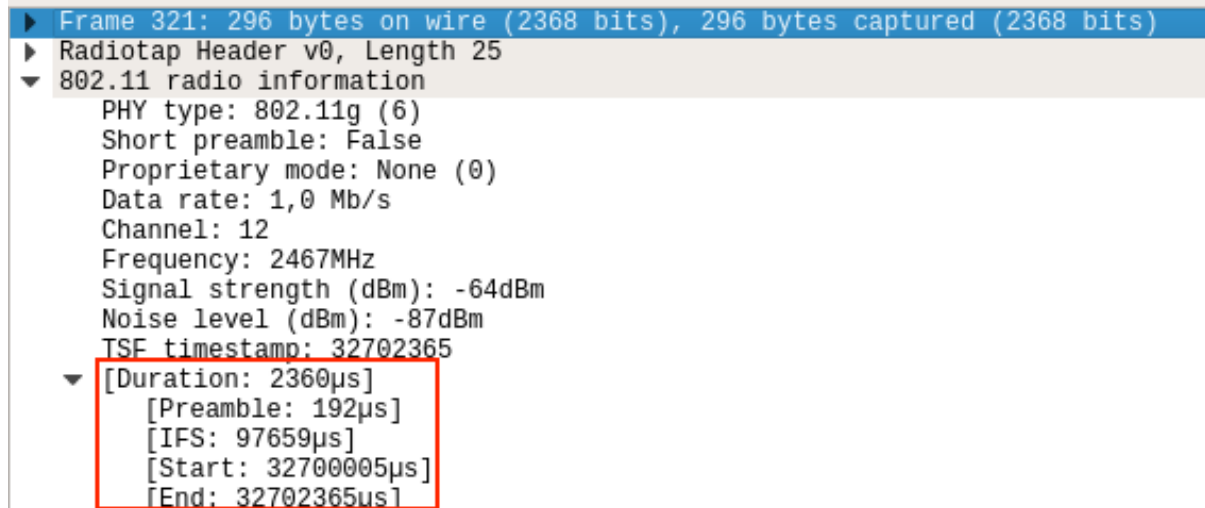


Figura 6 – Campo Duration.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|-------------------|-------------|----------|--------|--|
| 315 | 12.595378 | HitronTe_af:b1:98 | Broadcast | 802.11 | 296 | Beacon frame, SN=2329, FN=0, Flags=.....C, BI=100, SSID=FlyingNet |
| 316 | 12.597010 | HitronTe_af:b1:99 | Broadcast | 802.11 | 295 | Beacon frame, SN=2330, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon |
| 317 | 12.597788 | HitronTe_af:b1:98 | Broadcast | 802.11 | 296 | Beacon frame, SN=2331, FN=0, Flags=.....C, BI=100, SSID=FlyingNet |
| 318 | 12.599435 | HitronTe_af:b1:99 | Broadcast | 802.11 | 295 | Beacon frame, SN=2332, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon |
| 319 | 12.800183 | HitronTe_af:b1:98 | Broadcast | 802.11 | 296 | Beacon frame, SN=2333, FN=0, Flags=.....C, BI=100, SSID=FlyingNet |
| 320 | 12.801833 | HitronTe_af:b1:99 | Broadcast | 802.11 | 295 | Beacon frame, SN=2334, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon |
| 321 | 12.902583 | HitronTe_af:b1:98 | Broadcast | 802.11 | 296 | Beacon frame, SN=2335, FN=0, Flags=.....C, BI=100, SSID=FlyingNet |
| 322 | 12.904212 | HitronTe_af:b1:99 | Broadcast | 802.11 | 295 | Beacon frame, SN=2336, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon |

Figura 7 – Tramas analisadas.

Com base na análise das tramas Beacon provenientes de dois AP's diferentes, é possível verificar, no campo Duration, que o intervalo de tempo previsto entre 2 consecutivas é de 2360 microsegundos.

Contudo ao analisar a diferença entre os tempos de chegada das duas tramas, cada uma proveniente de um AP diferente, verificamos que o intervalo de tempo ultrapassava o tempo previsto (tendo em conta as tramas presentes na imagem seguinte o intervalo de tempo é de 1629 microsegundos).

Esta discrepância é verificada, visto que podem existir outros sistemas a ocupar o meio utilizado para comunicar, daí o AP ter de esperar que o meio esteja disponível para poder enviar a trama pretendida, não respeitando desta forma o intervalo de tempo.

8) 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:

```
▶ Frame 321: 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: 0x8000
    .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_af:b1:98 (bc:14:01:af:b1:98)
    Source address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
    BSS Id: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
    .... 0000 = Fragment number: 0
    1001 0001 1111 .... = Sequence number: 2335
    Frame check sequence: 0x28ed3efc [correct]
    [FCS Status: Good]
  ▶ IEEE 802.11 wireless LAN
```

Figura 8 – Frame 321 com o AP com SSID = FlyingNet.

```
▶ Frame 322: 205 bytes on wire (1640 bits), 205 bytes captured (1640 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: 0x8000
    .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_af:b1:99 (bc:14:01:af:b1:99)
    Source address: HitronTe_af:b1:99 (bc:14:01:af:b1:99)
    BSS Id: HitronTe_af:b1:99 (bc:14:01:af:b1:99)
    .... 0000 = Fragment number: 0
    1001 0010 0000 .... = Sequence number: 2336
    Frame check sequence: 0x4105c94a [correct]
    [FCS Status: Good]
  ▶ IEEE 802.11 wireless LAN
```

Figura 9 – Frame 322, com o AP com SSID = NOS_WIFI_Fon.

Na figura 4 podemos observar os **MAC address** contidos na trama enviada pelo **AP** com **SSID = FlyingNet**, onde **addr1 = (ff:ff:ff:ff:ff:ff)**, **addr2 = (ff:ff:ff:ff:ff:ff)**, **addr3 = (bc:14:01:af:b1:98)**, **addr4 = (bc:14:01:af:b1:98)**.

Na figura 5, podemos observar os **MAC address** contidos na trama enviada pelo **AP** com **SSID = NOS_WIFI_Fon**, onde **addr1 = (ff:ff:ff:ff:ff:ff)**, **addr2 = (ff:ff:ff:ff:ff:ff)**, **addr3 = (bc:14:01:af:b1:99)**, **addr4 = (bc:14:01:af:b1:99)**.

9) 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:

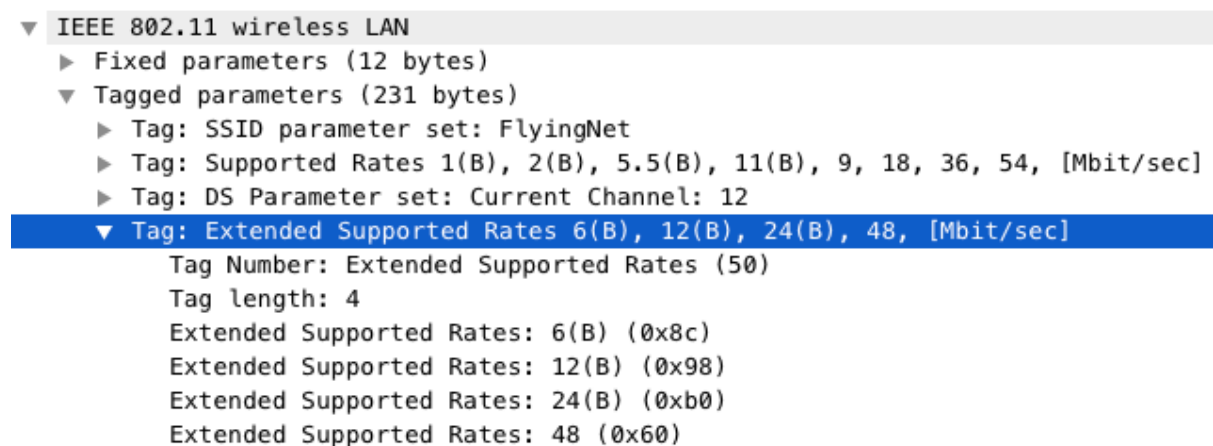


Figura 10 – Débitos suportados.

Os Rates suportados pelo AP são: 6 Mbit/s, 12 Mbit/s, 24 Mbit/s, 48 Mbit/s.

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

Resposta:

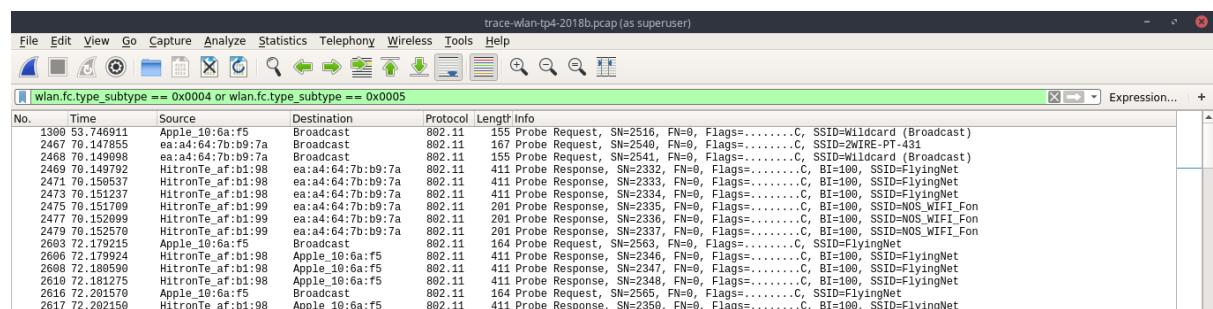


Figura 11 – Tramas filtradas

Para filtrar os probing requests e os probing responses usámos, à semelhança da alínea 5, o filtro "wlan.fc.type_subtype == 0x0004 or wlan.fc.type_subtype == 0x0005", em que 0x0004 e 0x0005 correspondem, respetivamente, a uma trama do subtipo probe request e do subtipo probe response. Conclui-se isso com base na tabela apresentada nos anexos disponibilizados no enunciado.

12) 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:

Antes de qualquer associação todos os dispositivos necessitam de se autenticar, tal é visível na figura 12.

O dispositivo envia um pedido de autenticação ao AP e caso este último aceite a nova identidade o mesmo envia uma confirmação de autenticação, desta forma verifica-se que a autenticação foi bem-sucedida. Outra forma de provar tal efeito é o facto de o pedido de associação ser efetuado uma vez que para que tal aconteça garantidamente o dispositivo tem de estar autenticado, mesmo que a rede seja aberta.

De seguida é enviado um pedido de associação pelo dispositivo indicando o SSID do AP a que se pretende conectar, o seu NIC entre outros campos necessários para estabelecer a associação.

Por último é enviado uma resposta de associação indicando na mesma o ID de associação entre outros dados referentes á associação como se verifica na figura 13.

| wlan.fc.type_subtype == 0x0000 wlan.fc.type_subtype == 0x0001 wlan.fc.type_subtype == 0x000B | | | | | |
|--|-----------|-------------------|-------------------|----------|--|
| No. | Time | Source | Destination | Protocol | Length Info |
| 2486 | 70.361782 | Apple_10:6a:f5 | HitronTe_af:b1:98 | 802.11 | 70 Authentication, SN=2542, FN=0, Flags=.....C |
| 2488 | 70.381869 | HitronTe_af:b1:98 | Apple_10:6a:f5 | 802.11 | 59 Authentication, SN=2338, FN=0, Flags=.....C |
| 2490 | 70.383512 | Apple_10:6a:f5 | HitronTe_af:b1:98 | 802.11 | 175 Association Request, SN=2543, FN=0, Flags=.....C, SSID=FlyingNet |
| 2492 | 70.389339 | HitronTe_af:b1:98 | Apple_10:6a:f5 | 802.11 | 225 Association Response, SN=2339, FN=0, Flags=.....C |

Figura 12 – Tramas de autenticação e associação.

| | |
|---|---|
| ▶ | Frame 2492: 225 bytes on wire (1800 bits), 225 bytes captured (1800 bits) |
| ▶ | Radiotap Header v0, Length 25 |
| ▶ | 802.11 radio information |
| ▶ | IEEE 802.11 Association Response, Flags:C |
| ▼ | IEEE 802.11 wireless LAN |
| ▼ | Fixed parameters (6 bytes) |
| ▶ | Capabilities Information: 0x0c31 |
| | Status code: Successful (0x0000) |
| | ..00 0000 0000 0001 = Association ID: 0x0001 |
| ▶ | Tagged parameters (166 bytes) |

Figura 13 – Trama de resposta de associação.

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

Resposta:

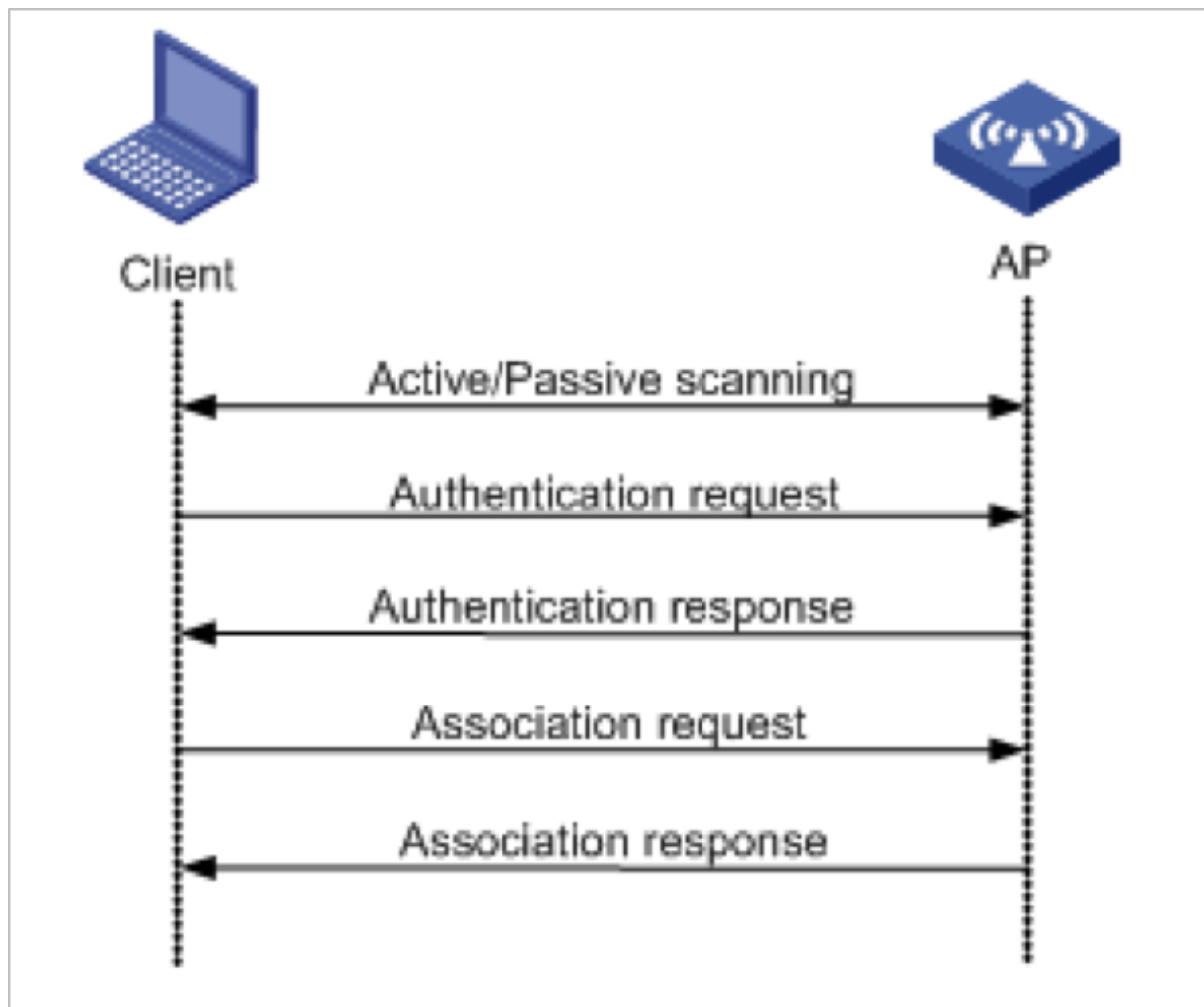


Figura 14 -Tramas envolvidas no processo de associação.

O esquema acima é bastante intuitivo acerca do processo de associação, no entanto é implícito que o Active/Passive scanning foi efetuado através de uma trama Beacon.

14) Considere a trama de dados no455. 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?

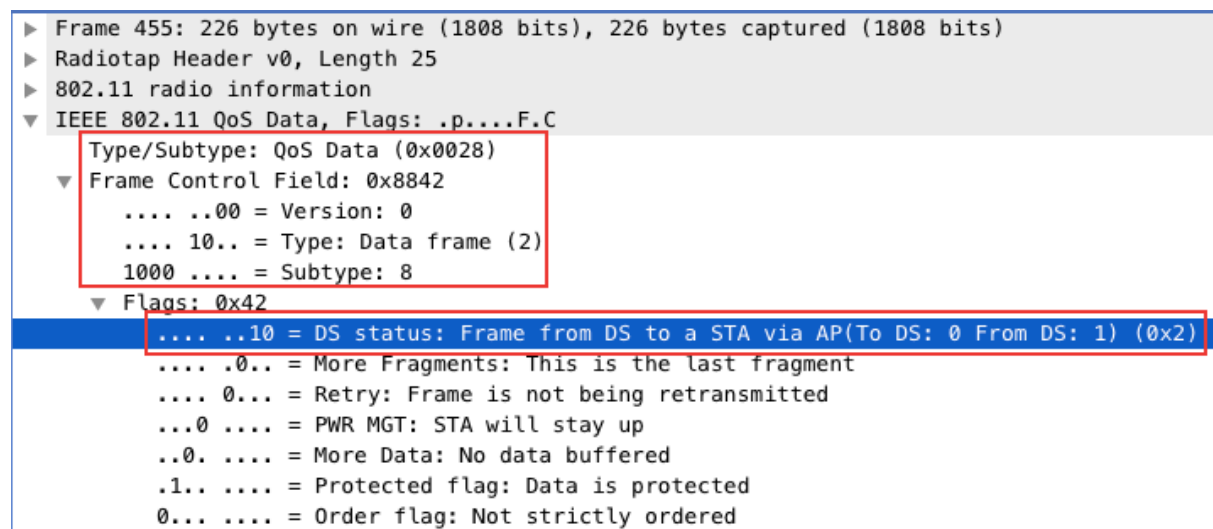


Figura 15 – Campo Frame Control na trama nº455.

Resposta:

Como se pode verificar na figura acima, a direccionalidade da trama **455** é do sistema de distribuição (**DS**) para o **STA** via **AP**, sendo que o tipo é 2 e o subtipo é 8, logo **fromDS** vale 1 e o **toDS** vale 0, logo a direccionalidade é local à **WLAN**.

15) Para a trama de dados no455, 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:

```
▶ Frame 455: 226 bytes on wire (1808 bits), 226 bytes captured (1808 bits)
▶ Radiotap Header v0, Length 25
▶ 802.11 radio information
▼ IEEE 802.11 QoS Data, Flags: .p....F.C
  Type/Subtype: QoS Data (0x0028)
  ▶ Frame Control Field: 0x8842
    .000 0000 0010 0100 = Duration: 36 microseconds
    Receiver address: Apple_71:41:a1 (d8:a2:5e:71:41:a1)
    Transmitter address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
    Destination address: Apple_71:41:a1 (d8:a2:5e:71:41:a1)
    Source address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
    BSS Id: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
    STA address: Apple_71:41:a1 (d8:a2:5e:71:41:a1)
    .... 0000 = Fragment number: 0
    0001 0001 0100 .... = Sequence number: 276
    Frame check sequence: 0xca46bf48 [correct]
    [FCS Status: Good]
  ▶ Qos Control: 0x0000
  ▶ CCMP parameters
```

Figura 16 – Endereços da trama 455.

O endereço MAC do host sem fios (STA) está no campo STA address (d8:a2:5e:71:41:a1), enquanto que o endereço do Access Point (AP) está no campo BSS Id (bc:14:01:af:b1:98).

16) Como interpreta a trama no457 face à sua direccionalidade e endereçamento MAC?

Resposta:

```
▶ Frame 457: 178 bytes on wire (1424 bits), 178 bytes captured (1424 bits)
▶ Radiotap Header v0, Length 25
▶ 802.11 radio information
▼ IEEE 802.11 QoS Data, Flags: .p.....TC
  Type/Subtype: QoS Data (0x0028)
  ▼ Frame Control Field: 0x8841
    .... ..00 = Version: 0
    .... 10.. = Type: Data frame (2)
    1000 .... = Subtype: 8
    ▼ Flags: 0x41
      .... ..01 = DS status: Frame from STA to DS via an AP (To DS: 1 From DS: 0) (0x1)
      .... .0.. = More Fragments: This is the last fragment
      .... 0... = Retry: Frame is not being retransmitted
      ...0 .... = PWR MGT: STA will stay up
      ..0. .... = More Data: No data buffered
      .1.. .... = Protected flag: Data is protected
      0... .... = Order flag: Not strictly ordered
    .000 0001 0011 1010 = Duration: 314 microseconds
  Receiver address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
  Transmitter address: Apple_71:41:a1 (d8:a2:5e:71:41:a1)
  Destination address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
  Source address: Apple_71:41:a1 (d8:a2:5e:71:41:a1)
  BSS Id: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
  STA address: Apple_71:41:a1 (d8:a2:5e:71:41:a1)
  .... .... 0000 = Fragment number: 0
  0100 1011 1001 .... = Sequence number: 1209
  Frame check sequence: 0x88cbfe48 [correct]
  [FCS Status: Good]
```

Figura 17 – Direccionalidade da trama 457.

Como podemos ver na figura a cima é possível observar que a direccionalidade da trama é do STA para o SD via AP e os seus correspondentes endereços MAC.

(Nota: a azul esta o endereço MAC destino e a magenta o de origem. A vermelho está o DS status que da a direccionalidade).

17) 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:

O subtipo de trama é QoS Data e é responsável por garantir uma qualidade de serviço na transmissão dos pacotes dos pacotes, através de priorização de tráfego e alocação adicional de recursos, visto que em redes wireless a probabilidade de ocorrerem colisões é muito maior do que em redes Ethernet.

18) 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:

| wlan.fc.type_subtype == 0x0008 | | | | | | |
|--------------------------------|-----------|-----------------------|-----------------------|----------|--------|-------------------------------|
| No. | Time | Source | Destination | Protocol | Length | Info |
| 15 | 0.631114 | Apple_10:6a:f5 (64... | HitronTe_af:b1:98 ... | 802.11 | 45 | Request-to-send, Flags=.....C |
| 16 | 0.631128 | | Apple_10:6a:f5 (64... | 802.11 | 39 | Clear-to-send, Flags=.....C |
| 23 | 0.631798 | Apple_10:6a:f5 (64... | HitronTe_af:b1:98 ... | 802.11 | 45 | Request-to-send, Flags=.....C |
| 24 | 0.631860 | | Apple_10:6a:f5 (64... | 802.11 | 39 | Clear-to-send, Flags=.....C |
| 78 | 3.130636 | | Apple_28:b8:0c (68... | 802.11 | 39 | Clear-to-send, Flags=.....C |
| 81 | 3.132873 | | Apple_28:b8:0c (68... | 802.11 | 39 | Clear-to-send, Flags=.....C |
| 85 | 3.133889 | | Apple_28:b8:0c (68... | 802.11 | 39 | Clear-to-send, Flags=.....C |
| 162 | 6.653376 | Apple_10:6a:f5 (64... | HitronTe_af:b1:98 ... | 802.11 | 45 | Request-to-send, Flags=.....C |
| 163 | 6.653389 | | Apple_10:6a:f5 (64... | 802.11 | 39 | Clear-to-send, Flags=.....C |
| 173 | 6.658172 | Apple_10:6a:f5 (64... | HitronTe_af:b1:98 ... | 802.11 | 45 | Request-to-send, Flags=.....C |
| 174 | 6.658178 | | Apple_10:6a:f5 (64... | 802.11 | 39 | Clear-to-send, Flags=.....C |
| 519 | 21.531991 | Apple_10:6a:f5 (64... | HitronTe_af:b1:98 ... | 802.11 | 45 | Request-to-send, Flags=.....C |
| 520 | 21.532004 | | Apple_10:6a:f5 (64... | 802.11 | 39 | Clear-to-send, Flags=.....C |
| 529 | 21.547047 | Apple_10:6a:f5 (64... | HitronTe_af:b1:98 ... | 802.11 | 45 | Request-to-send, Flags=.....C |
| 530 | 21.547057 | | Apple_10:6a:f5 (64... | 802.11 | 39 | Clear-to-send, Flags=.....C |
| 533 | 21.548964 | Apple_10:6a:f5 (64... | HitronTe_af:b1:98 ... | 802.11 | 45 | Request-to-send, Flags=.....C |
| 534 | 21.548970 | | Apple_10:6a:f5 (64... | 802.11 | 39 | Clear-to-send, Flags=.....C |
| 539 | 21.550282 | Apple_10:6a:f5 (64... | HitronTe_af:b1:98 ... | 802.11 | 45 | Request-to-send, Flags=.....C |
| 540 | 21.550288 | | Apple_10:6a:f5 (64... | 802.11 | 39 | Clear-to-send, Flags=.....C |
| 543 | 21.551568 | Apple_10:6a:f5 (64... | HitronTe_af:b1:98 ... | 802.11 | 45 | Request-to-send, Flags=.....C |
| 544 | 21.551576 | | Apple_10:6a:f5 (64... | 802.11 | 39 | Clear-to-send, Flags=.....C |
| 546 | 21.588982 | HitronTe_af:b1:98 ... | Apple_10:6a:f5 (64... | 802.11 | 45 | Request-to-send, Flags=.....C |
| 547 | 21.588987 | | HitronTe_af:b1:98 ... | 802.11 | 39 | Clear-to-send, Flags=.....C |
| 549 | 21.591336 | Apple_10:6a:f5 (64... | HitronTe_af:b1:98 ... | 802.11 | 45 | Request-to-send, Flags=.....C |
| 550 | 21.591340 | | Apple_10:6a:f5 (64... | 802.11 | 39 | Clear-to-send, Flags=.....C |
| 552 | 21.592549 | HitronTe_af:b1:98 ... | Apple_10:6a:f5 (64... | 802.11 | 45 | Request-to-send, Flags=.....C |
| 553 | 21.592557 | | HitronTe_af:b1:98 ... | 802.11 | 39 | Clear-to-send, Flags=.....C |
| 556 | 21.593710 | HitronTe_af:b1:98 ... | Apple_10:6a:f5 (64... | 802.11 | 45 | Request-to-send, Flags=.....C |
| 557 | 21.593720 | | HitronTe_af:b1:98 ... | 802.11 | 39 | Clear-to-send, Flags=.....C |

Figura 18 –Pacotes RTS e CTS.

Como podemos verificar na imagem acima, antes de ser enviada a trama 457, foram enviados pacotes de Request-to-send (RTS) e Clear-to-send (CTS), para evitar colisões. Em relação à direccionalidade o RTS é enviado pelo STA para o AP, enquanto que o CTS, é enviado pelo AP ao STA, como resposta ao seu pedido, que pode ser afirmativo ou negativo, isto é, se pode enviar naquele momento ou não.

Conclusões:

Com a conclusão deste trabalho ficamos com uma maior percepção dos processos envolvidos numa rede wireless.

Inicialmente verificou-se a gestão por parte do AP da largura de banda atribuída a cada STA. Por exemplo se existir um único STA numa rede wireless, este possuirá a largura de banda na sua totalidade. No entanto também existem situações, em que existem bastantes STA, mas com diferentes prioridades, sendo que este obtém larguras de banda maiores.

Ao contrário do que se verificou no trabalho prático três (Redes Ethernet), as redes wireless, contém controlo de erros (CRC, com FCS), visto que a probabilidade de ocorrência de colisões é muito maior. No entanto existem mecanismos para evitar as colisões, denominados RTS e CTS, que aquando da necessidade de envio de um pacote, inicialmente “questionam” o Access Point (AP) dessa possibilidade, e este responde com um pacote CTS.

Por fim, explorou-se o processo de associação de um STA a um AP, incluindo a fase antecessora responsável pela autenticação. Neste processo são usados pacotes de Authentication, Request Association e Reply Association, que informam o STA da possibilidade de se conectar ou não ao AP.