TP4 : Redes Sem Fios (802.11)

Henrique Neto, Sara Marques e Tiago Gomes

Universidade do Minho, Departamento de Informática, 4710-057 Braga, Portugal
e-mail: {a89618,a89477,a78141}@alunos.uminho.pt

Resumo O objetivo deste trabalho é explorar os vários aspetos do protocolo IEEE 802.11, tais como as tramas mais comuns, o modo de endereçamento dos vários componentes envolvidos nas comunicações sem fios, o formato e estrutura das tramas, e a operação de controlo.

1 Acesso Rádio

```
No. Time       Source             Destination Protocol Length
367 15.259284 HitronTe_af:b1:99 Broadcast   802.11   205
Info
Beacon frame, SN=2382, FN=0, Flags=........C, BI=100, SSID=NOS_WIFI_Fon

Frame 367: 205 bytes on wire (1640 bits), 205 bytes captured (1640 bits)
Radiotap Header v0, Length 25
802.11 radio information
    PHY type: 802.11g (ERP) (6)
    Short preamble: False
    Proprietary mode: None (0)
    Data rate: 1,0 Mb/s
    Channel: 12
    Frequency: 2467MHz
    Signal strength (dBm): -61 dBm
    Noise level (dBm): -87 dBm
    Signal/noise ratio (dB): 26 dB
    TSF timestamp: 35059937
        [Duration: 1632µs]
        [Preamble: 192µs]
        [IFS: 745µs]
        [Start: 35058305µs]
        [End: 35059937µs]
IEEE 802.11 Beacon frame, Flags: ........C
IEEE 802.11 Wireless Management
    Tag: SSID parameter set: NOS_WIFI_Fon
    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
    (...)
    Tag: Extended Supported Rates 6(B), 12(B), 24(B), 48, [Mbit/sec]
    (...)
```

1. **Identifique em que frequência do espectro está a operar a rede sem fios, e o canal que corresponde essa frequência.**
   - A frequência do espectro a analisar é 2467Hz, sendo que este corresponde ao canal 12.
2. **Identifique a versão da norma IEEE 802.11 que está a ser usada.**
   - A versão da norma IEEE 802.11 utilizada é a 802.11g.
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.**
   - Pela *radio information* presente na trama observamos que o débito enviado à trama selecionada foi de $1Mbit/s$, que segundo a *Tag: Supported Rates* presente na sequência de bytes de *IEEE 802.11 Wireless Management* não corresponde ao débito máximo suportado, sendo este de $54Mbit/s$.

2 Scanning Passivo e Scanning Ativo

4. **Selecione uma trama beacon (e.g., trama 1067). 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)?**
   - A trama 1067 é uma trama do tipo *management* (gestão) e de subtipo *beacon* (sendo denominada assim de trama beacon), ou seja, o valor do identificador do tipo é 00 e o do subtipo é 1000.
5. **Para a trama acima, identifique todos os endereços MAC em uso. Que conclui quanto à sua origem e destino?**
   - Os endereços MAC identificados para a trama 1067 foram os seguintes:

     ```
     Recetor Broadcast - ff:ff:ff:ff:ff:ff
     Destino Broadcast - ff:ff:ff:ff:ff:ff
     Transmitter (ou seja, AP) - bc:14:01:af:b1:99
     Origem - bc:14:01:af:b1:99
     Basic Service Set (BSS) - bc:14:01:af:b1:99
     ```

     Sendo que o endereço destino e recetor (`ff:ff:ff:ff:ff:ff`) referem-se a qualquer interface que consiga detetar a trama (*Broadcast*), e o endereço de origem (`bc:14:01:af:b1:99`) refere-se ao router de distribuição do ponto de acesso indicado.
6. **Uma trama beacon anuncia que o AP pode suportar vários débitos de base, assim como vários débitos adicionais (extended supported rates). Indique quais são esses débitos?**

   ```
   IEEE 802.11 Wireless Management
       Tag: Extended Supported Rates 6(B), 12(B), 24(B), 48, [Mbit/sec]
   ```

   - Os débitos adicionais suportados são 6, 12, 24 e 48 Mb/sec.
7. **Qual 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 provenientes do mesmo AP é verificada? Tente explicar porquê.**
   - ```
     IEEE 802.11 Wireless Management
     Fixed parameters (12 bytes)
     Timestamp: 1149712386890
     Beacon Interval: 0,102400 [Seconds]
     Capabilities Information: 0x0c21
     ```

     O intervalo previsto entre tramas beacon consecutivas é de 0,1024 segundos, embora que na prática este valor possa não ser mantido devido a questões de latência ou caso existam outras tramas a serem transmitidas simultaneamente, obrigando a que exista um tempo de espera adicional.
8. **Identifique e liste os SSIDs dos APs que estão a operar na vizinhança da STA de captura? Explicite o modo como obteve essa informação (por exemplo, se usou algum filtro para o efeito).**
   - Foi utilizado o filtro $wlan.ssid$, obtendo-se os seguintes SSIDs:

     ```
     Tag Number: SSID parameter set (0)
     Tag Number: 12
     SSID: NOS_WIFI_Fon

     Tag Number: SSID parameter set (0)
     Tag Number: 9
     SSID: FlyingNet
     ```

9. **Verifique se está a ser usado o método de deteção de erros (CRC). Justifique.**
   Use o filtro: $(wlan.fc.type\_subtype == 0\mathbf{x}08)\ \&\&\ (wlan.fcs.status == bad)$
   Que conclui?
   Justifique o porquê de usar deteção de erros em redes sem fios.
     ```

– De facto está a ser usado o método de deteção de erros, visto que cada trama tem presente um campo FCS *(Frame Control Sequence)*. Ao usarmos o filtro mencionado estamos a selecionar todas as tramas do subtipo *Beacon* do tipo *Management* que apresentam erros, ou seja, para os quais o valor do fcs é inválido (*bad*). Com isto podemos observar que existem 5 mensagens nesta situação tendo elas os números 6274, 6937, 7013, 7131 e 7173. O uso de deteção de erros é fulcral numa rede sem fios pois é espectado que várias interfaces possam usar o mesmo canal de comunicação, o que torna os erros por colisões um acontecimento inevitável mesmo com os vários métodos e técnicas usados para os mitigar. Adicionalmente, o meio em que se transmite as tramas está sujeito a ruído significativo proveniente do ambiente físico em si que podem corromper as tramas.

No trace disponibilizado foi também registado scanning ativo (envolvendo tramas probe request e probe response), comum nas redes Wi-Fi como alternativa ao scanning passivo.

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

```
(wlan.fc.type_subtype == 0x04) || (wlan.fc.type_subtype == 0x05)
```

11. **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?**

– Foram identificadas as tramas 2468 e 2469 que retratam, respetivamente, um *Probe Request* seguido pelo respetivo *Probe Response*. Ambas as tramas têm as flags relativas ao sistema de distribuição a 0, que é o esperado visto que as mensagens são só para interfaces locais. Assim concluímos que o endereçamento contém 3 endereços correspondentes ao destino (*Destination address*), origem (*Source address*) e o identificador do serviço da rede (*BSS Id*), que comunicam de maneira *ad hoc*.

```
No.  Time       Source            Destination Protocol Length Info
2468 70.149098 ea:a4:64:7b:b9:7a Broadcast   802.11   155    Probe Request

Frame 2468: 155 bytes on wire (1240 bits), 155 bytes captured (1240 bits)
Radiotap Header v0, Length 25
802.11 radio information
IEEE 802.11 Probe Request, Flags: ........C
    Source address: ea:a4:64:7b:b9:7a (ea:a4:64:7b:b9:7a)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Transmitter address: ea:a4:64:7b:b9:7a (ea:a4:64:7b:b9:7a)
    BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
IEEE 802.11 Wireless Management
```

– A trama de *Probe Request* é enviada pela máquina `ea:a4:64:7b:b9:7a` para *Broadcast* (`ff:ff:ff:ff:ff:ff`), ou seja, é enviada uma mensagem a todas as máquinas que estejam em alcance, com o objetivo de pedir informações sobre a forma de ficar a conhecer o ambiente e as melhores opções de comunicação. Note-se também que como se pretende contactar todas as interfaces em todos os serviços disponíveis, o endereço *BSSID* também corresponde a *Broadcast*.

```
No.  Time       Source            Destination       Protocol Length Info
2469 70.149792 HitronTe_af:b1:98 ea:a4:64:7b:b9:7a 802.11   411    Probe Response, SSID=FlyingNet
Frame 2469: 411 bytes on wire (3288 bits), 411 bytes captured (3288 bits)
Radiotap Header v0, Length 25
802.11 radio information
IEEE 802.11 Probe Response, Flags: ........C
    Source address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
    Destination address: ea:a4:64:7b:b9:7a (ea:a4:64:7b:b9:7a)
    Transmitter address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
    BSS Id: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
IEEE 802.11 Wireless Management
```

– Esta trama corresponde a um *Probe Response* enviado como resposta ao pedido da máquina `ea:a4:64:7b:b9:7a` referido anteriormente. Os endereços presentes indicam a interface destino da mensagem, ou seja, a máquina que efetuou o pedido, a interface origem correspondente à máquina que está a responder (`bc:14:01:af:b1:98`) seguido do respetivo identificador do *service set* do ponto de acesso em que está ser realizada a comunicação. Neste caso coincide com o endereço da máquina que faz a transmissão. No final da transmissão uma mensagem de gestão do subtipo *Acknowledgment* foi enviada a confirmar a receção. Adicionalmente, foram enviadas outras mensagens semelhantes a esta (variando por exemplo o *SSID*) que contribuíram na angariação pedida pela máquina inicial.
– Por fim, a interface `ea:a4:64:7b:b9:7a` passa a conter informação sobre o ambiente à sua volta, o que permite escolher a melhor opção para efetuar comunicações que possa a vir precisar.

3 Processo de Associação

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.**
    – As tramas 2486 a 2493 correspondem a um processo de associação completo entre a STA e o AP.

No.	Time	Source	Destination	Protocol	Length	Info
2486	70.361782	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	70	Authentication
2487	70.362050		Apple_10:6a:f5(RA)	802.11	39	Acknowledgement
2488	70.381869	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	59	Authentication
2489	70.381878		HitronTe_af:b1:98(RA)	802.11	39	Acknowledgement
2490	70.383512	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	175	Association Request
2491	70.383873		Apple_10:6a:f5(RA)	802.11	39	Acknowledgement
2492	70.389339	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	225	Association Response
2493	70.389352		HitronTe_af:b1:98(RA)	802.11	39	Acknowledgement

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

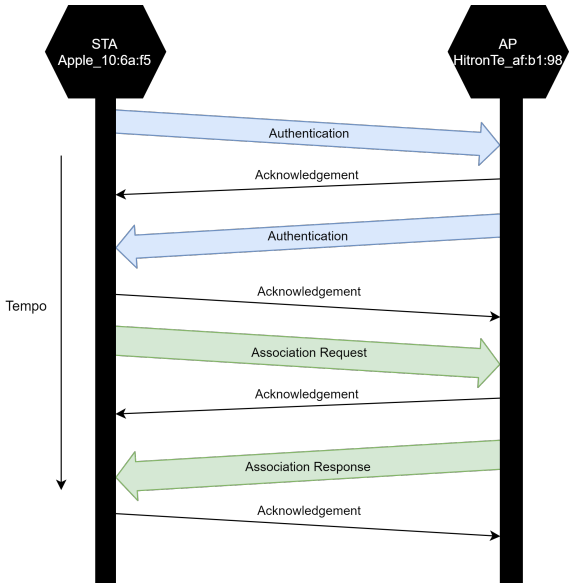

Figura 1. Diagrama de sequência das tramas

4 Transferência de Dados

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?**

```
Frame Control Field: 0x8842
.... ..00 = Version: 0
.... 10.. = Type: Data frame (2)
1000 .... = Subtype: 8
Flags: 0x42
    .... ..10 = DS status: Frame from DS to a STA via AP(To DS: 0 From DS: 1) (0x2)
    .... .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
```

   – Ao analisar a especificação do campo de *Frame Control* desta trama, é possível observar que se trata de um pacote proveniente do sistema de distribuição (visto que a flag *From Ds* é 1) para uma estação de wireless (visto que a flag *To Ds* é 0) através de um ponto de acesso (AP), o que nos permite concluir que não se trata de uma trama local à *WLAN*. Também, através da análise do tipo e subtipo deste pacote, é possível verificar que se trata de um pacote de dados (*Type value: 10 -> Data*) que contém informação quanto à qualidade do serviço (*Subtype value: 1000 -> QoS*).

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?**

```
Destination address: Apple_71:41:a1 (d8:a2:5e:71:41:a1)
Transmitter address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
Source address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
```

   – O primeiro endereço presente na trama corresponderá ao destinatário , ou seja, *MAC adress* do STA que é `d8:a2:5e:71:41:a1`. O segundo endereço corresponderá ao *Access Point* (ou *BSS*), ou seja `bc:14:01:af:b1:98` que coincide com o terceiro endereço, sendo este o endereço da interface de acesso ao sistema de distribuição.

16. **Como interpreta a trama nº457 face à sua direcionalidade e endereçamento MAC?**

```
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

BSS Id: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
Source address: Apple_71:41:a1 (d8:a2:5e:71:41:a1)
Destination address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
```

   – Analisando as especificações desta trama, verifica-se que se trata de um pacote de dados proveniente de uma estação wireless (*From Ds* $= 0$) para o sistema de distribuição (*To Ds* $= 1$). Desta forma, podemos concluir que o primeiro endereço MAC presente será o *BSS Id* (`bc:14:01:af:b1:98`), ou seja a identificador do ponto de acesso (que designa o *service set*), seguido do endereço de origem (`d8:a2:5e:71:41:a1`) e pelo endereço da interface destino que neste caso coincide com o ponto de acesso.

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.)**

```
Trama 456 e Trama 458:
Frame Control Field: 0xd400
.... ..00 = Version: 0
.... 01.. = Type: Control frame (1)
1101 .... = Subtype: 13
Flags: 0x00
    .... ..00 = DS status: Not leaving DS or network is operating in AD-HOC mode
                (To DS: 0 From DS: 0) (0x0)
```

- As tramas 455 e 457, sendo tramas de dados relativos à qualidade de serviço, possuem um tamanho grande e por isso estão muito sujeitas a ruído e sobreposição de outros dispositivos que pode provocar danos nas mensagens, tornando-as corruptas e inválidas, ou até mesmo impedir a receção das mensagens por completo. Desta forma existe a necessidade de ser comunicado se uma determinada transmissão teve ou não sucesso, resultando assim na necessidade da transmissão de tramas de confirmação, como as tramas 456 e 458. Estas tratam-se de tramas de controlo (*Type value: 01 -> Control*) de reconhecimento (*Subtype value: 1101 -> Acknowledgement*) que informam o sucesso na receção do pacote enviado e que por sua vez são pequenas para minimizar o riscos de falhas na sua transmissão. Adicionalmente estas mensagens são locais e não interferem com o sistema de distribuição. Desta forma, podemos assumir que estas mensagens podem ser transmitidas na forma *ad hoc* visto que apenas é preciso comunicar entre duas interfaces que estão ao alcance uma da outra.
  Opcionalmente, embora não seja este o caso, poderiam também ser transmitidas tramas de controlo *Request To Send* e *Clear To Send* que serviriam para "reservar"o espaço de transmissão. Desta forma, uma estação poderia anunciar que pretende fazer uma transmissão, que caso fosse aceite reservaria o meio de transmissão, prevenindo interferências das outras estações.

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.**

- Nas tramas estudadas anteriormente não estavam a presentes tramas *Request To Send* e *Clear To Send*. Desta forma, para possibilitar o estudo concreto destas tramas, foi utilizado o seguinte filtro:

  ```
  wlan.fc.type_subtype==27 || wlan.fc.type_subtype==28
  ```

  O que nos demonstra que, de facto, está a ser utilizado a opção de RTS/CTS em algumas das trocas de dados entre a STA e o AP/Router da WLAN. Um destes casos, tratam-se das tramas 15 e 16 que iremos usar como exemplo.

```
No.  Time      Source            Destination       Protocol Length Info
15   0.631114  Apple_10:6a:f5    HitronTe_af:b1:98 802.11   45     Request-to-send

Frame 15: 45 bytes on wire (360 bits), 45 bytes captured (360 bits)
Radiotap Header v0, Length 25
802.11 radio information
IEEE 802.11 Request-to-send, Flags: ........C
    Type/Subtype: Request-to-send (0x001b)
    Frame Control Field: 0xb400
    .... ..00 = Version: 0
    .... 01.. = Type: Control frame (1)
    1011 .... = Subtype: 11
    Receiver address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
    Transmitter address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)
```

Na trama *Request To Send* (RTS), para além das informações de rádio e de controlo estão presentes dois endereços MAC. Um corresponde ao recetor destino da mensagem (neste caso é `bc:14:01:af:b1:98`) e o outro corresponde ao ponto de acesso que transmite a mensagem (neste caso é `64:9a:be:10:6a:f5`). O objetivo desta trama é anunciar ao nó destinatário que se pretende transmitir uma trama proveniente do endereço de origem. Estas mensagens são, por sua vez, locais e não têm qualquer significado no sistema de distribuição. Adicionalmente são de tamanho reduzido para minimizar colisões com outras mensagens.

```
No. Time       Source Destination       Protocol Length Info
16  0.631128          Apple_10:6a:f5   802.11   39     Clear-to-send

Frame 16: 39 bytes on wire (312 bits), 39 bytes captured (312 bits)
Radiotap Header v0, Length 25
802.11 radio information
IEEE 802.11 Clear-to-send, Flags: ........C
    Type/Subtype: Clear-to-send
    Frame Control Field: 0xc400
    .... ..00 = Version: 0
    .... 01.. = Type: Control frame (1)
    1100 .... = Subtype: 12
    Receiver address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)
```

Após a receção da trama para pedido de transmissão, o *AP* para qual se pretende fazer uma transmissão envia uma mensagem *Clear To Send*(CTS) contendo apenas o MAC da estação que fez o pedido como recetor destinado (ou seja `64:9a:be:10:6a:f5`). Desta forma ao receber esta mensagem a estação procede a enviar a mensagem pretendida. Alternativamente, as estações concorrentes ao receberem o *Clear To Send* aos quais não são os destinatários, iniciam um temporizador que as impede de transmitir para aquela estação, de maneira a impossibilitar colisões. Semelhante às mensagens *RTS* as mensagens *CTS* também possuem um tamanho reduzido com o mesmo objetivo minimizar colisões entre mensagens.

5 Conclusão

Em suma, este relatório apresenta as nossas respostas e estratégias utilizadas na análise de tramas do protocolo IEEE 802.11, e do modo de funcionamento das comunicações sem fios.

Ao longo deste trabalho foi possível estudar o formato, componentes e relevância dos diferentes tipos de tramas existentes na norma IEEE 802.11, para além de todo o processo envolvido na comunicação e transferência de dados numa rede sem fios, permitindo-nos aplicar o nosso conhecimento deste tema de um modo mais prático.

Consideramos que, de modo geral, o desenvolvimento deste trabalho contribuiu para o aprofundamento da nossa compreensão dos vários conceitos envolvidos no funcionamento das comunicações sem fios, para além da sua relevância na comunicação segura e eficiente de dados entre redes.