



Camada de Ligação Lógica: Ethernet e Protocolo ARP

J.G¹, M.F², P.G.³, T.C.⁴

Licenciatura em Ciências da Computação (LCC)

Universidade do Minho, R. da Universidade, 4710-057 Braga
Licenciatura em Ciências da Computação
gci@reitoria.uminho.pt

¹ João Guedes - A94013

² Miguel Freitas - A91635

³ Pedro Gomes - A91647

⁴ Tomás Campinho - A91668

TP3: Redes Sem Fios (802.11)

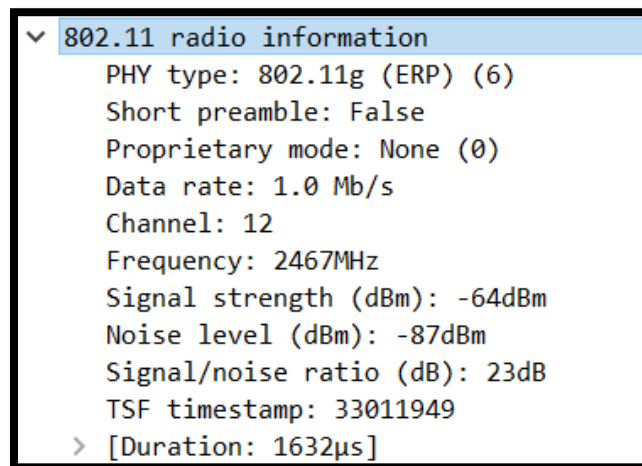
TP3: Redes Sem Fios (802.11) (Respostas)

Acesso Rádio

Abrimos o wireshark e abrimos a captura que a docente anexou. Uma vez tudo pronto selecionamos a trama correspondente ao nosso número de TurnoGrupo (e.g., 28 – PL2, G8),

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 em que está a operar a rede sem fios no canal é 2467MHz e o canal que corresponde essa frequência é 12



Channel: 12

Frequency: 2467MHz

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

A versão da norma IEEE 802.11 que está a ser usada é a versão 802.11g (3) (usar referência)

3	802.11g	2003	2.4 GHz	802.11, 802.11b	54 Mbps	ERP-OFDM	20 MHz	1
---	---------	------	---------	-----------------	---------	----------	--------	---

PHY type: 802.11g (ERP) (6)

<https://support.metageek.com/hc/en-us/articles/202162320-WiFi-PHY-Types>

TP3: Redes Sem Fios (802.11)

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 (consultar campo Supported Rates).

O débito a que foi enviada a trama foi 1.0 Mb/s. Não, esse débito não corresponde ao débito máximo, uma vez que o débito máximo a que a interface Wifi pode operar é **54Mbps/s** (verificar o print a baixo indicado).

```
Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 9, 18, 36, 54, [Mbit/sec]
Tag Number: Supported Rates (1)
Tag length: 8
Supported Rates: 1(B) (0x82)
Supported Rates: 2(B) (0x84)
Supported Rates: 5.5(B) (0x8b)
Supported Rates: 11(B) (0x96)
Supported Rates: 9 (0x12)
Supported Rates: 18 (0x24)
Supported Rates: 36 (0x48)
Supported Rates: 54 (0x6c)
```

Data rate: 1.0 Mb/s

TP3: Redes Sem Fios (802.11)

Scanning Passivo e Scanning Ativo

As tramas beacon permitem efetuar scanning passivo em redes IEEE 802.11 (WiFi). O AP envia periodicamente tramas Beacon para anunciar a sua presença e transmitir informações tais como a data e hora, o SSID, e outros parâmetros relativos ao AP, a todas as interfaces rádio que estão dentro do seu alcance rádio. É pela recepção de tramas Beacon (passive scanning) ou pelo varrimento dos vários canais rádio (active scanning) que uma estação pode optar por um AP mais favorável.

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)?

Esta trama pertence ao tipo “Beacon Frame” do tipo de tramas 802.11.

```
Type/Subtype: Beacon frame (0x0008)
▼ Frame Control Field: 0x8000
    .... ..00 = Version: 0
    .... 00.. = Type: Management frame (0)
    1000 .... = Subtype: 8
```

Valores

- **Type:** 0 Management Frame
- **Subtype:** 8

A parte concreta do cabeçalho em que a trama está especificado estão nesta parte da trama.

```
IEEE 802.11 Beacon frame, Flags: .....C
```

TP3: Redes Sem Fios (802.11)

5. 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.

Obtemos esta informação através da visualização da coluna que contém a informação dos SSID, que só constam estes dois pontos de acesso. Sendo assim, estes são os dois SSIDs que estão na vizinhança da STA de captura:

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:b1:99	Broadcast	802.11	205 Beacon frame, SN=2342, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon

wlan.ssid == 2WIRE-PT-431						
No.	Time	Source	Destination	Protocol	Length	Info
2467	70.147855	ea:a4:64:7b:b9:7a	Broadcast	802.11	167	Probe Request, SN=2540, FN=0, Flags=.....C, SSID=2WIRE-PT-431

6. Para um 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.

Beacon Interval: 0.102400 [Seconds]

O intervalo de tempo previsto entre tramas beacon consecutivas é o valor que apresenta na figura acima assinalada.

328 13.211424	13.312189 - 13.211424 = 0.100765
329 13.312189	

Quanto à pergunta se esta periodicidade de tramas beacon é verificada a resposta é sim é verificada uma vez que o valor calculado se encontra dentro do valor esperado que é verificado.

TP3: Redes Sem Fios (802.11)

7. 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

Ambos transmitem com destino a todos os aparelhos, em Broadcast.

NOS_WIFI_FON

```
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)
```

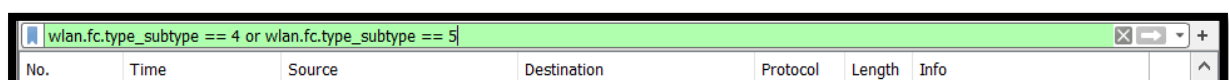
FlyingNet

```
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)
```

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



Combinado os dois.



TP3: Redes Sem Fios (802.11)

9. 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?

2603 72.179215	Apple_10:6a:f5	Broadcast	802.11	164	Probe Request, SN=2563, FN=0, Flags=.....C, SSID=FlyingNet
2606 72.179924	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	411	Probe Response, SN=2346, FN=0, Flags=.....C, BI=100, SSID=FlyingNet

Probe request é enviado pelo Apple_10:6a:f5 em **brodcast** para a FlyingNet. Depois o HitronTe_af:b1:98 quando recebe o pacote envia **probe response** para o Apple_10:6a:f5 para poder iniciar o processo de autenticação.

TP3: Redes Sem Fios (802.11)

Processo de Associação

Numa rede WiFi estruturada, um host deve associar-se a um ponto de acesso antes de enviar dados. O processo de associação nas redes IEEE 802.11 é executada enviando a trama association request do host para o AP e a trama association response enviada pelo AP para o host, em resposta ao pedido de associação recebido. Este processo é antecedido por uma fase de autenticação.

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

Station:

Apple_10:6a:f5

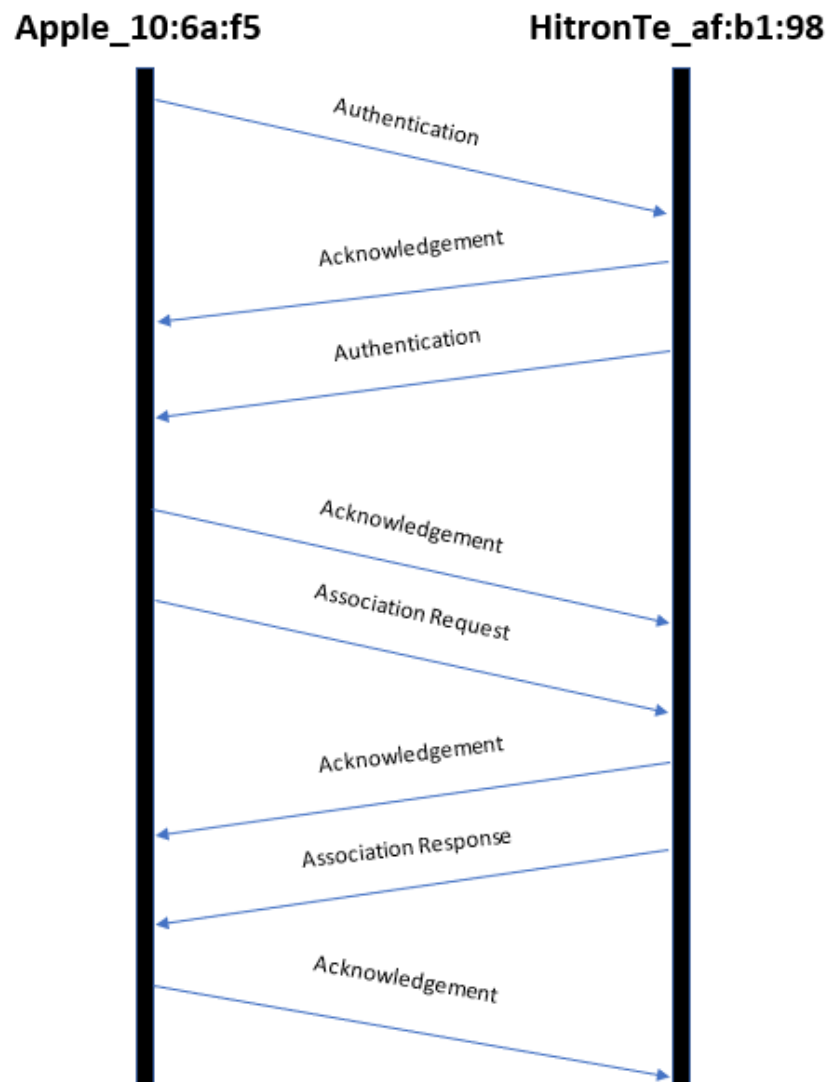
Access Point:

HitronTe_af:b1:98

TP3: Redes Sem Fios (802.11)

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

2485 70.352671		Broadcom_04:6a:f5 (... 802.11	39 Clear-to-send, Flags=.....C
2486 70.361782	Apple_10:6a:f5	HitronTe_af:b1:98 802.11	70 Authentication, SN=2542, FN=0, Flags=.....C
2487 70.362050		Apple_10:6a:f5 (64:...	39 Acknowledgement, Flags=.....C
2488 70.381869	HitronTe_af:b1:98	Apple_10:6a:f5 802.11	59 Authentication, SN=2338, FN=0, Flags=.....C
2489 70.381878		HitronTe_af:b1:98 (... 802.11	39 Acknowledgement, 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
2491 70.383873		Apple_10:6a:f5 (64:...	39 Acknowledgement, Flags=.....C
2492 70.389339	HitronTe_af:b1:98	Apple_10:6a:f5 802.11	225 Association Response, SN=2339, FN=0, Flags=.....C
2493 70.389352		HitronTe_af:b1:98 (... 802.11	39 Acknowledgement, Flags=.....C



TP3: Redes Sem Fios (802.11)

Transferência de Dados

O trace disponibilizado, para além de tramas de gestão da ligação de dados, inclui tramas de dados e de controlo da transferência desses mesmos dados.

- 12. 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?**

Type/Subtype: QoS Data (0x0028)

É direccionado ao aparelho Apple:

455 18.536644 HitronTe_af:b1:98 Apple_71:41:a1

https://en.wikipedia.org/wiki/802.11_Frame_Types

- 13. 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 (DS)? Como interpreta só estarem dois endereços MAC distintos em uso?**

Host:

Destination address: Apple_71:41:a1 (d8:a2:5e:71:41:a1)

Router (DS):

Transmitter address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)

Estão os dois descritos pois a comunicação é efetuada entre os dois aparelhos e não para a rede inteira. O endereço host é d8:a2:5e:71:41:a1. O endereço AP é bc:14:01:af:b1:98. O endereço router é bc:14:01:af:b1:98.

TP3: Redes Sem Fios (802.11)

14. Como interpreta a trama nº457 face à sua direccionalidade? Identifique os endereços usados se o MAC do router do DS fosse 00:11:22:33:44:55:66:77?

Quanto a direccionalidade, seria ao contrário da questão anterior, alternando o emissor e o recetor. A source seria esta:

Source address: Apple_71:41:a1 (d8:a2:5e:71:41:a1)

A destination será o mac hipotético:

00:11:22:33:44:55:66:77

15. 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.)

O subtipo de tramas de controlo que são transmitidas são Ack (Acknowledgment) para assegurar que as tramas foram recebidas. (Referência) A razão pela qual têm de existir é porque é transmitida por um meio Wifi, ou seja, não é ethernet, logo suscetível a erros.

Type/Subtype: Acknowledgement (0x001d)

TP3: Redes Sem Fios (802.11)

16. 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.

Não está a ser utilizado, contudo, já foi visto no capítulo anterior a existência de RTS-CTS. Os sistemas envolvidos são o aparelho apple e o router. Existe comunicação em ambas as direções entre estes aparelhos.

455	18.536644	HitronTe_af:b1:98	Apple_71:41:a1	802.11
456	18.536653		HitronTe_af:b1:98 (...)	802.11
457	18.539762	Apple_71:41:a1	HitronTe_af:b1:98	802.11

TP3: Redes Sem Fios (802.11)

Conclusões

Os resultados obtidos no desenvolver do trabalho, permitiram ao grupo compreender inúmeros aspetos técnicos e linguagem relacionadas com o conteúdo em questão. (protocolo IEEE 802.11, formato das tramas, o endereçamento das comunicações sem fios, tramas mais comuns, etc...).

Uma vez que já dominamos o WireShark, neste trabalho utilizamos várias ferramentas desta aplicação, como por exemplo os filtros, e não só mas foi preciso também identificar as tramas e aplicar tudo que na teoria fomos praticando.

Na nossa opinião, este trabalho decorreu como previsto, contudo, achamos algumas questões de maior dificuldade e de uma necessidade crescente de pesquisa relativa à especificidade técnica relacionada e à inexperiência a este nível da matéria envolvida. O grupo apresentou mais dificuldades nas últimas questões deste relatório, pois não conseguimos chegar a um consenso entre o grupo, uma vez que o tema era um pouco ambíguo de interpretação.

No entanto, achamos que conseguimos cumprir todos os objetivos pedidos no trabalho, sendo este bem-sucedido.

TP3: Redes Sem Fios (802.11)

Referências

<https://support.metageek.com/hc/en-us/articles/202162320-WiFi-PHY-Types>

https://en.wikipedia.org/wiki/802.11_Frame_Types

https://en.wikipedia.org/wiki/Quality_of_service