

Universidade do Minho

Escola de Engenharia

Licenciatura em Engenharia Informática

Unidade Curricular de Redes de Computadores

Ano Letivo de 2022/2023

Trabalho Prático Nº4 **Redes sem Fios (Wi-Fi)**

Grupo 57

A94942 Miguel Velho Raposo

A78823 João Carlos Cotinho Sotomaior Neto

A91775 José Pedro Batista Fonte

14 de maio de 2023

Índice

Lista de Figuras	3
1 Introdução	4
2 Trabalho Desenvolvido	5
2.1 Acesso Rádio	5
2.2 Scanning Passivo e Scanning Ativo	6
2.3 Processo de Associação	10
2.4 Transferência de Dados	11
3 Conclusão	14

Lista de Figuras

2.1	Trama 57	5
2.2	Trama 157	6
2.3	Débitos suportados pelo AP	7
2.4	Intervalor da Trama Beacon	8
2.5	Probe Request and Response identificados	9
2.6	Probe Requests and Responses	9
2.7	Endereçamentos	9
2.8	Tramas de Autenticação e Associação	10
2.9	Diagrama	10
2.10	Trama 8503	11
2.11	Frame Control Trama 8503	11
2.12	Trama 8521	12
2.13	QoS Data	12
2.14	Data Transfer	13
2.15	Data Transfer	13

1 Introdução

Este relatório foi escrito pelo grupo 57 e surge no âmbito do Trabalho Prático 4 da Unidade Curricular de Redes de Computadores lecionada no 2º semestre do Ano Letivo 2022/23.

O tema do trabalho é Redes sem Fios (Wi-Fi) e tem como objetivo fornecer uma visão abrangente do protocolo IEEE 802.11, que é amplamente utilizado em redes sem fio em todo o mundo. Neste trabalho, vamos explorar vários aspetos desse protocolo, incluindo o formato das tramas, o endereçamento dos dispositivos envolvidos na comunicação sem fios, os tipos de tramas mais comuns e a operação geral do protocolo. Com uma compreensão mais profunda desses aspectos, podemos melhorar nossa capacidade de projetar, configurar e solucionar problemas em redes sem fio baseadas no protocolo IEEE 802.11.

2 Trabalho Desenvolvido

2.1 Acesso Rádio

Selecione a trama de ordem 57 correspondente ao seu identificador de grupo.

```
> Frame 57: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface en0, id 0
  Radiotap Header v0, Length 56
    Header revision: 0
    Header pad: 0
    Header length: 56
    Present flags
    MAC timestamp: 514771
    Flags: 0x12
    Data Rate: 24,0 Mb/s
    Channel frequency: 2412 [BG 1]
    Channel flags: 0x0480, 2 GHz spectrum, Dynamic CCK-OFDM
    Antenna signal: -89 dBm
    Antenna noise: -93 dBm
    Antenna: 0
    Vendor namespace: Broadcom-0
    Vendor namespace: Broadcom-3
  802.11 radio information
    PHY type: 802.11g (ERP) (6)
    Proprietary mode: None (0)
    Data rate: 24,0 Mb/s
    Channel: 1
    Frequency: 2412MHz
    Signal strength (dBm): -89 dBm
    Noise level (dBm): -93 dBm
    Signal/noise ratio (dB): 4 dB
    TSF timestamp: 514771
    [Duration: 28µs]
  IEEE 802.11 Request-to-send, Flags: .....C
    Type/Subtype: Request-to-send (0x001b)
    Frame Control Field: 0xb400
    .000 0000 1101 0010 = Duration: 210 microseconds
    Receiver address: ce:90:6f:21:42:3a (ce:90:6f:21:42:3a)
    Transmitter address: PTInovac_d6:88:50 (00:06:91:d6:88:50)
    Frame check sequence: 0xf9bf3a88 [unverified]
    [FCS Status: Unverified]
```

Figura 2.1: Trama 57

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

Pelos campos *Frequency* e *Channel* do cabeçalho *802.11 Radio Information* entende-se que está a operar nos 2412 MHz, que é o mesmo que dizer 2.4 Ghz e no canal 1.

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

Como é possível verificar pelo campo *PHY Type* está a ser utilizada a norma 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 Wi-Fi pode operar? Justifique.

O débito foi 24.0 Mb/s, como é possível ver pelo campo *Data Rate*. O valor não corresponde ao valor de débito máximo visto que esse valor é de 54 Mbps segundo o estabelecido pelo protocolo 802.11g.

4) Verifique qual a força do sinal (Signal strength) e a qualidade expectável de receção da trama, sabendo que:

O campo *Signal Strength* indica o valor de -89 dBm o que significa que a qualidade de receção da trama é muito má e a probabilidade de uma conexão bem sucedida é muito baixa.

2.2 Scanning Passivo e Scanning Ativo

5) Selecione uma trama beacon cuja ordem (ou terminação) corresponda a 57. Esta trama pertence a que tipo de tramas 802.11? Identifique o valor dos identificadores de tipo e de subtipo da trama. Em que parte concreta do cabeçalho da trama estão especificados (ver anexo)?

```
> Frame 157: 386 bytes on wire (3088 bits), 386 bytes captured (3088 bits) on interface en0, id 0
> Radiotap Header v0, Length 60
v 802.11 radio information
  PHY type: 802.11n (HT) (7)
  MCS index: 0
  Bandwidth: 20 MHz (0)
  Short GI: False
  Greenfield: False
  FEC: BEC (0)
  Data rate: 6,5 Mb/s
  Channel: 1
  Frequency: 2412MHz
  Signal strength (dBm): -46 dBm
  Noise level (dBm): -94 dBm
  Signal/noise ratio (dB): 48 dB
  TSF timestamp: 1465342
  ... ..1 = Last part of an A-MPDU: True
  ... ..0 = A-MPDU delimiter CRC error: False
  A-MPDU aggregate ID: 0
> [Duration: 444µs]
v 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_f3:9a:46 (74:9b:e8:f3:9a:46)
  Source address: HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)
  BSS Id: HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)
  .... ..0000 = Fragment number: 0
  0011 1100 1010 .... = Sequence number: 970
  Frame check sequence: 0x92156cf0 [unverified]
  [FCS Status: Unverified]
> IEEE 802.11 Wireless Management
```

Figura 2.2: Trama 157

Esta trama pertence ao tipo de tramas 802.11n e ao tipo/subtipo 0x0008 (Beacon Frame), segundo o campo *PHY type* e *Type/Subtype*, respetivamente.

6) Para a trama acima, identifique todos os endereços MAC em uso. Que conclui quanto à sua origem e destino?

- Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
- Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
- Transmitter address: HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)
- Source address: HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)

É possível concluir que o pacote é enviado pelo AP **HitronTe_f3:9a:46** para todos dispositivos dentro do seu alcance, daí o destino endereçado ser Broadcast.

7) Verifique se está a ser usado o método de detecção de erros (CRC). Justifique. Justifique o porquê de ser necessário usar detecção de erros em redes sem fios.

Está a ser utilizado CRC que no Wireshark é identificado pelo campo FCS, que neste caso tem o valor 0x92156cf0. A detecção de erros é uma técnica essencial em redes sem fios para garantir a confiabilidade, eficiência e compatibilidade da comunicação, ao mitigar as interferências e os erros que podem afetar a transmissão e receção de dados.

As tramas beacon permitem especificar parâmetros de funcionamento úteis para apoiar a operação e a gestão das ligações em fios.

8) Uma trama beacon anuncia que o AP pode suportar vários débitos de base (B), assim como vários débitos adicionais (extended supported rates). Indique quais são esses débitos.

Como é possível ver pela figura 2.3, o AP consegue suportar débitos até 54 Mbps.

<pre>IEEE 802.11 Wireless Management Fixed parameters (12 bytes) Tagged parameters (286 bytes) Tag: SSID parameter set: "FlyingNet" Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18, [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: 6(B) (0x8c) Supported Rates: 9 (0x12) Supported Rates: 12(B) (0x98) Supported Rates: 18 (0x24)</pre>	<pre>Tag: Extended Supported Rates 24(B), 36, 48, 54, [Mbit/sec] Tag Number: Extended Supported Rates (50) Tag length: 4 Extended Supported Rates: 24(B) (0xb0) Extended Supported Rates: 36 (0x48) Extended Supported Rates: 48 (0x60) Extended Supported Rates: 54 (0x6c)</pre>
---	---

(a) Supported Rates

(b) Extended Supported Rates

Figura 2.3: Débitos suportados pelo AP

9) Qual o intervalo de tempo previsto entre tramas beacon consecutivas (este valor é anunciado na própria trama beacon)? Na prática, a periodicidade de tramas beacon provenientes do mesmo AP é verificada com precisão? Justifique.

Pela figura 2.6, é possível verificar o valor de 0.1024 segundos entre cada trama beacon consecutiva. No geral, embora a periodicidade das tramas Beacon possa variar em certas circunstâncias, ela é geralmente confiável o suficiente para fornecer uma base sólida para a sincronização e o gestão de dispositivos numa rede sem fios.

```
▼ IEEE 802.11 Wireless Management
  ▼ Fixed parameters (12 bytes)
    Timestamp: 905889485187
    Beacon Interval: 0,102400 [Seconds]
  > Capabilities Information: 0x0431
  > Tagged parameters (286 bytes)
```

Figura 2.4: Intervalo da Trama Beacon

10) Identifique e liste os SSIDs dos APs que estão a operar na vizinhança da STA de captura. Explícite o modo como obteve essa informação (por exemplo, se usou algum filtro para o efeito).

A lista obtida utilizando um filtro para tramas beacon (**wlan.fc.type_subtype==0x0008**) leva a concluir que existem estes APs na vizinhança:

- MEO-D68850 (trama 3)
- MEO-WiFi (trama 4)
- NOS- 2EC6 (trama 8)
- NOS-C876 (trama 9)
- MEO-FCF0A0 (trama 10)
- FlyingNet (trama 12)
- MEO-9E9BB0 (trama 17)

Os Beacon Frames são pacotes de controle transmitidos periodicamente pelos pontos de acesso em redes sem fios, estes são usados para anunciar a existência de uma rede sem fios e fornecer informações para que os dispositivos se possam conectar a ela.

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

Com o filtro `wlan.fc.type_subtype==0x0005` para obter os Probe Response e `wlan.fc.type_subtype==0x0004` para obter os Probe Request, resultando nos seguintes pacotes:

No.	Time	Source	Destination	Protocol	Length	Info
150	1.381604	HitronTe_f3:9a:46	SamsungE_1a:10:f6	802.11	486	Probe Response, SN=1936, FN=0, Flags=.....C, BI=100, SSID="FlyingNet"
151	1.382387	HitronTe_f3:9a:46	SamsungE_1a:10:f6	802.11	486	Probe Response, SN=1936, FN=0, Flags=.....C, BI=100, SSID="FlyingNet"
152	1.391750	HitronTe_f3:9a:46	SamsungE_1a:10:f6	802.11	486	Probe Response, SN=1936, FN=0, Flags=.....C, BI=100, SSID="FlyingNet"
153	1.391879	HitronTe_ee:2e:c6	SamsungE_1a:10:f6	802.11	485	Probe Response, SN=2192, FN=0, Flags=.....C, BI=100, SSID="NOS-2EC6"
155	1.399123	SamsungE_1a:10:f6	Broadcast	802.11	122	Probe Request, SN=1124, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
277	2.710713	HitronTe_ee:2e:c6	AltoBeam_08:32:99	802.11	485	Probe Response, SN=2193, FN=0, Flags=.....C, BI=100, SSID="NOS-2EC6"
279	2.720237	HitronTe_ee:2e:c6	AltoBeam_08:32:99	802.11	485	Probe Response, SN=2193, FN=0, Flags=.....C, BI=100, SSID="NOS-2EC6"
334	3.297107	PTInovac_45:be:32	ea:52:54:89:2b:72	802.11	224	Probe Response, SN=2424, FN=0, Flags=.....C, BI=100, SSID="MEO-WiFi"
335	3.297177	PTInovac_45:be:32	ea:52:54:89:2b:72	802.11	224	Probe Response, SN=2424, FN=0, Flags=.....C, BI=100, SSID="MEO-WiFi"
336	3.290315	PTInovac_45:be:32	ea:52:54:89:2b:72	802.11	224	Probe Response, SN=2424, FN=0, Flags=.....C, BI=100, SSID="MEO-WiFi"
788	7.826332	AltoBeam_08:32:99	Broadcast	802.11	110	Probe Request, SN=1111, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
789	7.832355	HitronTe_ee:2e:c6	AltoBeam_08:32:99	802.11	485	Probe Response, SN=2195, FN=0, Flags=.....C, BI=100, SSID="NOS-2EC6"
791	7.835604	HitronTe_ee:2e:c6	AltoBeam_08:32:99	802.11	485	Probe Response, SN=2195, FN=0, Flags=.....C, BI=100, SSID="NOS-2EC6"
793	7.838631	AltoBeam_08:32:99	Broadcast	802.11	110	Probe Request, SN=1112, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
796	7.859430	HitronTe_ee:2e:c6	AltoBeam_08:32:99	802.11	485	Probe Response, SN=2196, FN=0, Flags=.....C, BI=100, SSID="NOS-2EC6"
797	7.862565	HitronTe_ee:2e:c6	AltoBeam_08:32:99	802.11	485	Probe Response, SN=2196, FN=0, Flags=.....C, BI=100, SSID="NOS-2EC6"
798	7.868818	HitronTe_ee:2e:c6	AltoBeam_08:32:99	802.11	485	Probe Response, SN=2196, FN=0, Flags=.....C, BI=100, SSID="NOS-2EC6"

Figura 2.5: Probe Request and Response identificados

12) 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?

788	7.826332	AltoBeam_08:32:99	Broadcast	802.11	110	Probe Request, SN=1111, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
789	7.832355	HitronTe_ee:2e:c6	AltoBeam_08:32:99	802.11	485	Probe Response, SN=2195, FN=0, Flags=.....C, BI=100, SSID="NOS-2EC6"
791	7.835604	HitronTe_ee:2e:c6	AltoBeam_08:32:99	802.11	485	Probe Response, SN=2195, FN=0, Flags=.....C, BI=100, SSID="NOS-2EC6"
793	7.838631	AltoBeam_08:32:99	Broadcast	802.11	110	Probe Request, SN=1112, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
796	7.859430	HitronTe_ee:2e:c6	AltoBeam_08:32:99	802.11	485	Probe Response, SN=2196, FN=0, Flags=.....C, BI=100, SSID="NOS-2EC6"
797	7.862565	HitronTe_ee:2e:c6	AltoBeam_08:32:99	802.11	485	Probe Response, SN=2196, FN=0, Flags=.....C, BI=100, SSID="NOS-2EC6"
798	7.868818	HitronTe_ee:2e:c6	AltoBeam_08:32:99	802.11	485	Probe Response, SN=2196, FN=0, Flags=.....C, BI=100, SSID="NOS-2EC6"

Figura 2.6: Probe Requests and Responses

Pela figura 2.7, é possível ver os endereços utilizados no probe request e no response. O probe request é endereçado em broadcast pelo STA para conhecer ativamente quais são os APs no alcance. Já o probe response corresponde à resposta dada por estes APs, logo é endereçado ao STA que fez o probe request.

O Probe Request e o Probe Response são tipos de tramas de gestão de WLAN utilizados para descobrir e anunciar ativamente a presença de um Access Point (AP) ou um dispositivo cliente na rede sem fio.

IEEE 802.11 Probe Request, Flags:C Type/Subtype: Probe Request (0x0004) > 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: AltoBeam_08:32:99 (a4:ef:15:08:32:99) Source address: AltoBeam_08:32:99 (a4:ef:15:08:32:99)	IEEE 802.11 Probe Response, Flags:C Type/Subtype: Probe Response (0x0005) > Frame Control Field: 0x5000 .000 0001 0011 1010 = Duration: 314 microseconds Receiver address: AltoBeam_08:32:99 (a4:ef:15:08:32:99) Destination address: AltoBeam_08:32:99 (a4:ef:15:08:32:99) Transmitter address: HitronTe_ee:2e:c6 (90:aa:c3:ee:2e:c6) Source address: HitronTe_ee:2e:c6 (90:aa:c3:ee:2e:c6)
--	--

(a) Probe Request

(b) Probe Response

Figura 2.7: Endereçamentos

2.3 Processo de Associação

13) Identifique uma sequência de tramas que corresponda a um processo de associação realizado com sucesso entre a STA e o AP, incluindo a fase de autenticação.

Filtro para authentication

- wlan.fc.type_subtype == 0x000b

Filtro para association request e association response

- wlan.fc.type_subtype == 0x0000 || wlan.fc.type_subtype == 0x0001

0472 73.450730	AzureIav_0f:0e:9b	HitronTe_f3:9a:46	802.11	70 Authentication, SN=262, FN=0, Flags=.....C
0473 73.450745	HitronTe_f3:9a:46	AzureIav_0f:0e:9b (80:c5:f2:0f:0e:9b) (RA)	802.11	48 Acknowledgement, Flags=.....C
0474 73.450775	AzureIav_0f:0e:9b	HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46) (RA)	802.11	70 Authentication, SN=1965, FN=0, Flags=.....C
0475 73.450780	HitronTe_f3:9a:46	AzureIav_0f:0e:9b	802.11	48 Acknowledgement, Flags=.....C
0476 73.459546	AzureIav_0f:0e:9b	HitronTe_f3:9a:46	802.11	164 Association Request, SN=263, FN=0, Flags=.....C, SSID="FlyingIet"
0477 73.459553	HitronTe_f3:9a:46	AzureIav_0f:0e:9b (80:c5:f2:0f:0e:9b) (RA)	802.11	48 Acknowledgement, Flags=.....C
0478 73.459638	AzureIav_0f:0e:9b	HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46) (RA)	802.11	210 Association Response, SN=1966, FN=0, Flags=.....C
0479 73.459643	HitronTe_f3:9a:46	AzureIav_0f:0e:9b	802.11	48 Acknowledgement, Flags=.....C

Figura 2.8: Tramas de Autenticação e Associação

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

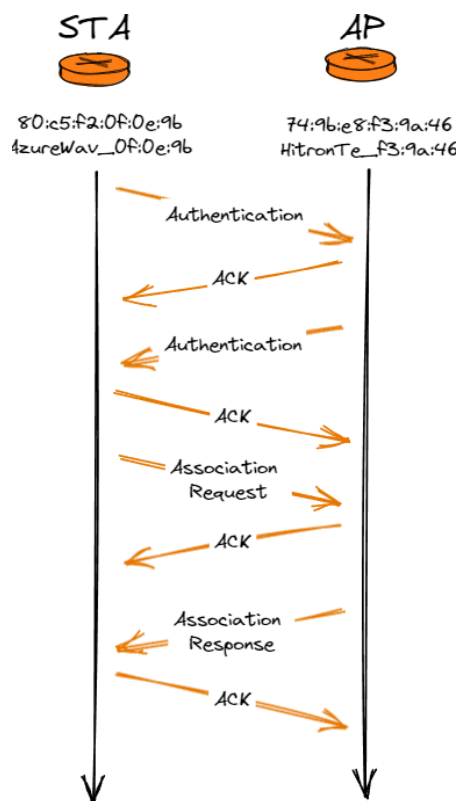


Figura 2.9: Diagrama

2.4 Transferência de Dados

```
> Frame 8503: 188 bytes on wire (1504 bits), 188 bytes captured (1504 bits) on interface en0, id 0
> Radiotap Header v0, Length 58
  802.11 radio information
    PHY type: 802.11n (HT) (7)
    MCS index: 4
    Bandwidth: 20 MHz (0)
    Short GI: False
    Greenfield: True
    FEC: LDPC (1)
    Data rate: 39.0 Mb/s
    Channel: 1
    Frequency: 2412MHz
    Signal strength (dBm): -32 dBm
    Noise level (dBm): -93 dBm
    Signal/noise ratio (dB): 61 dB
    TSF timestamp: 73562794
    .... = Last part of an A-MPDU: False
    .... = A-MPDU delimiter CRC error: False
    A-MPDU aggregate ID: 0
  [Duration: 56µs]
  IEEE 802.11 QoS Data, Flags: .p....TC
    Type/Subtype: QoS Data (0x0028)
    > Frame Control Field: 0x8841
      .000 0000 0011 0000 = Duration: 48 microseconds
      Receiver address: HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)
      Transmitter address: AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)
      Destination address: IPv6mcast_16 (33:33:00:00:00:16)
      Source address: AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)
      BSS Id: HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)
      STA address: AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)
      .... = Fragment number: 0
      0000 0000 0000 .... = Sequence number: 0
      Frame check sequence: 0x57cf2fa2 [unverified]
      [FCS Status: Unverified]
    > Qos Control: 0x0000
    > CCMP parameters
  > Data (92 bytes)
```

Figura 2.10: Trama 8503

15) Considere a trama de dados nº8503. 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: 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... .... = +HTC/Order flag: Not strictly ordered
```

Figura 2.11: Frame Control Trama 8503

O campo *DS status* dentro do *Frame Control* especifica que a trama é enviada do dispositivo (STA) para o sistema de distribuição (DS) pelo ponto de acesso (AP), e sim uma trama de dados QoS (Qualidade de Serviço) enviado de uma STA (Estação) para um DS (Sistema de Distribuição) ainda é considerado dentro da WLAN (Rede Local Sem Fio).

16) Para a trama de dados nº8503, transcreva os endereços MAC em uso, identificando quais os endereços correspondentes à estação sem fios (STA), ao AP e ao router de acesso ao sistema de distribuição (DS)?

- Receiver address: HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46) [AP]
- Transmitter address: AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b) [STA]
- Destination address: IPv6mcast_16 (33:33:00:00:00:16) [DS]
- Source address: AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b) [STA]

17) Como interpreta a trama nº8521 face à sua direccionalidade e endereçamento MAC?

```
> Frame 8521: 444 bytes on wire (3552 bits), 444 bytes captured (3552 bits) on interface enb, id 0
> Radiotap Header v0, Length 58
  802.11 radio information
    PHY type: 802.11a (HT) (7)
    MCS Index: 4
    Bandwidth: 20 MHz (0)
    Short GI: True
    Greenfield: False
    FEC: BEC (0)
    Data rate: 41.3 Mb/s
    Channel: 1
    Frequency: 2412MHz
    Signal strength (dBm): -42 dBm
    Noise level (dBm): -93 dBm
    Signal/noise ratio (dB): 51 dB
    TSF timestamp: 73595276
    .....0 = Last part of an A-MPDU: false
    .....0 = A-MPDU delimiter OK error: false
    A-MPDU aggregate ID: 0
  Duration: 80µs
  IEEE 802.11 QoS Data, Flags: p....F.C
  Type/Subtype: QoS Data (0x0028)
  Frame Control Field: 0x0028
    0000 0000 0011 1100 = Duration: 80 microseconds
    Receiver address: AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)
    Transmitter address: HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)
    Destination address: AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)
    Source address: 76:9b:e8:f3:9a:43 (76:9b:e8:f3:9a:43)
    BSS ID: HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)
    STA address: AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)
    .....0000 = Fragment number: 0
    0000 0000 0010 ..... = Sequence number: 2
    Frame check sequence: 8c72f00ba (unverified)
    [FCS Status: Unverified]
  QoS Control: 0x0006
  CTP parameters
  Data (348 bytes)
```

(a) Trama 8521

```
▼ Frame Control Field: 0x0028
  ....0000 = 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... .... = HT/Order flag: Not strictly ordered
```

(b) Frame Control da Trama 8521

Figura 2.12: Trama 8521

A trama sai do DS para o STA via o AP, isto significa que transita no sentido contrário da trama 8503.

18) Que subtipo de tramas de controlo são transmitidas ao longo da transferência de dados acima mencionada? Tente explicar a razão de terem de existir (contrariamente ao que acontece numa rede Ethernet.)

8519 73.544155	HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)	AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)	802.11	76 Request-to-send, Flags=.....C
8520 73.544159	HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)	AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)	802.11	72 Clear-to-send, Flags=.....C
8521 73.544163	76:9b:e8:f3:9a:43 (76:9b:e8:f3:9a:43)	AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)	802.11	444 QoS Data, SN=2, FN=0, Flags=p....F.C
8522 73.544167	AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)	HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)	802.11	68 802.11 Block Ack, Flags=.....C

Figura 2.13: QoS Data

Durante a transferência de dados numa rede wi-fi, são transmitidos vários subtipos de tramas de controlo para gerir o acesso ao meio de transmissão e garantir a confiabilidade da comunicação. Alguns exemplos de tramas de controlo são:

- **Request to Send (RTS) e Clear to Send (CTS):** utilizadas para controlar o acesso ao meio de transmissão e evitar colisões entre transmissões concorrentes.
- **Acknowledgement (ACK) :** utilizado para confirmar a recepção bem-sucedida de uma trama de dados.
- **Block Acknowledgement (Block ACK) :** utilizado para confirmar a recepção bem-sucedida de uma sequência de quadros de dados, reduzindo a sobrecarga de transmissão de confirmações.

Em redes sem fios, as tramas de controlo são necessárias para gerir o acesso ao meio de transmissão, evitando colisões e perda de dados devido ao compartilhamento do meio por vários dispositivos. Elas também ajudam a detetar e corrigir erros de transmissão, o que é especialmente importante em redes sem fio que apresentam maior taxa de erros devido a interferências do ambiente.

19) 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.

Sim, está a ser utilizada RTS/CTS sendo que a direccionalidade do RTS é do AP para o STA, depois o STA confirma a disponibilidade(CTS) ao AP, o STA recebe o QoS Data e confirma a receção ao AP.

Dê um exemplo de uma transferência de dados em que é usada a opção RTC/CTS e um outro em que não é usada.

Um exemplo com RTS/CTS

```

8519 73.544155 HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46) AzureWav_0f:0e:9b (80:c5:f2:0f:9b:46) 802.11 76 Request-to-send, Flags=.....C
8520 73.544159 HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46) HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46) 802.11 72 Clear-to-send, Flags=.....C
8521 73.544163 76:9b:e8:f3:9a:43 AzureWav_0f:0e:9b (80:c5:f2:0f:9b:46) 802.11 444 QoS Data, SN=2, FN=0, Flags=p....F.C
8522 73.544167 AzureWav_0f:0e:9b (80:c5:f2:0f:9b:46) HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46) 802.11 68 802.11 Block Ack, Flags=.....C

```

Figura 2.14: Data Transfer

Um exemplo sem RTS/CTS

```

387 3.818646 PTInovac_9e:9b:b2 Broadcast 802.11 254 Beacon frame, SN=2481, FN=0, Flags=.....C, BI=100, SSID="NEO-WIFI"
388 3.818653 PTInovac_9e:9b:b2 Spanning-tree-(for-bridges)_00 802.11 118 Data, SN=2482, FN=0, Flags=p....F.C
389 3.831156 AzureWav_0f:0e:9b (80:c5:f2:0f:9b:46) (TA) HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46) (RA) 802.11 68 802.11 Block Ack, Flags=.....C

```

Figura 2.15: Data Transfer

3 Conclusão

Em conclusão, a análise detalhada dos tópicos abordados neste relatório forneceu um conhecimento mais aprofundado sobre o funcionamento da tecnologia Wi-Fi. O estudo dos processos de acesso ao meio, scanning passivo e ativo, processo de associação e transferência de dados ajudou a compreender como as redes sem fios funcionam e como elas gerem o acesso ao meio, evitando colisões e perda de dados.

Com as perguntas sobre o Acesso Rádio compreendemos o protocolo 802.11 utilizado na ligação, assim como as implicações físicas na qualidade da ligação. No capítulo de Scanning Passivo e Scanning Ativo aprendemos como os dispositivos sem fios descobrem redes próximas. O Scanning Passivo é menos intrusivo, pois apenas escuta as transmissões, enquanto Scanning Ativo envia probes para procurar redes Wi-Fi. O estudo do Processo de Associação mostra como os dispositivos sem fios se conectam a uma rede Wi-Fi, um processo que inclui autenticação, associação e configuração dos parâmetros de conexão. Por último, no estudo da Transferência de Dados aprendemos como as tramas de controle ajudam a gerir o acesso ao meio de transmissão, evitando colisões e garantindo a confiabilidade da comunicação.

Em conclusão, compreender o funcionamento das redes Wi-Fi é crucial na era da comunicação sem fios. Desde a descoberta de redes até a transferência de dados, cada etapa do processo de conexão é importante e pode afetar a eficiência e a segurança da rede, portanto, um conhecimento aprofundado das redes Wi-Fi é fundamental para entender e desenvolver soluções assentes sobre esta tecnologia.