Universidade do Minho
Mestrado Integrado em Engenharia Informática

Redes de Computadores
2019/2020

TP4: Redes sem Fios (802.11)
Grupo 05

Ana Afonso
A85762

João Diogo Mota
A80791

Márcia Teixeira
A80943

1. Questões e Respostas

1.1 Acesso Rádio

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

A frequência do espetro em que a rede sem fios está a operar é: 2437MHz, o que corresponde ao canal 6.

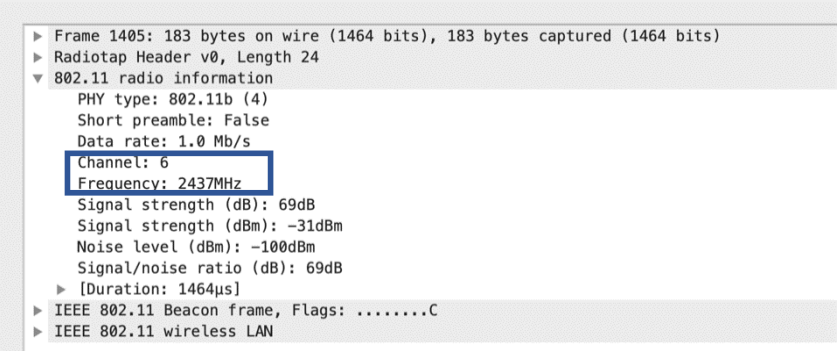


Figura 1: Análise da Trama - Frequência e Canal

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

Está a ser usada a versão 802.11b (4).

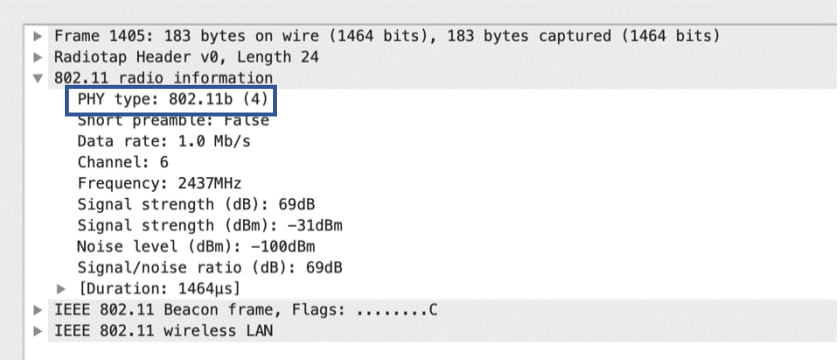


Figura 2: Análise de Trama - PHY type

Questão 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 a que a trama escolhida (1405) foi enviada é de 1.0 Mb/s. Tal como podemos ver através da Figura 4, esse débito não corresponde ao débito máximo a que a interface Wi-Fi pode operar visto que este é de 54Mb/s.

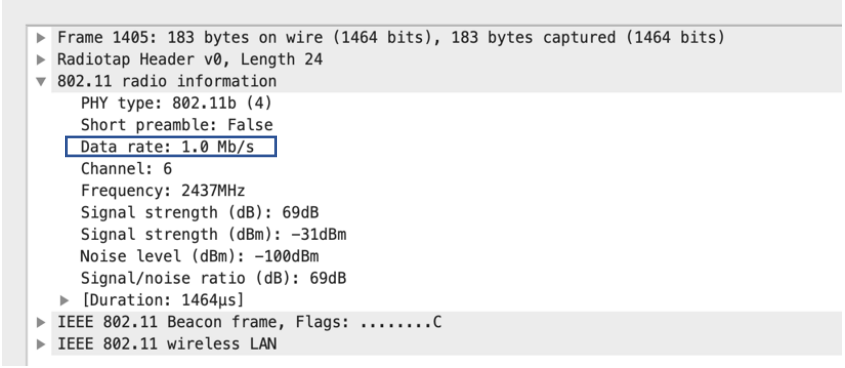


Figura 3: Análise da Trama - Data rate

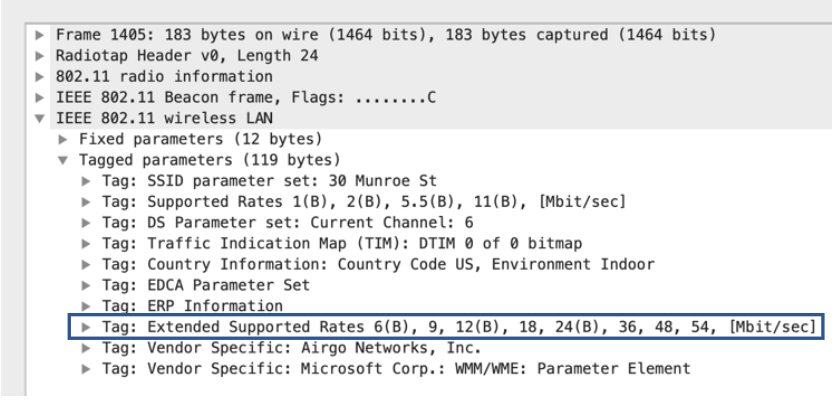
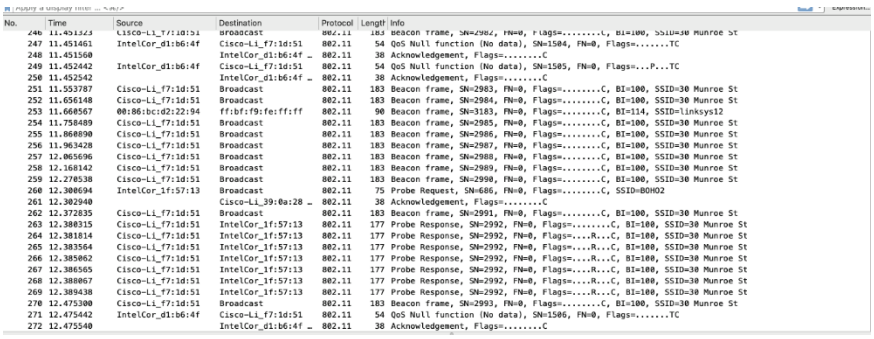


Figura 4: Análise da Trama - Tag: Extended Supported Rates

1.2 Scanning

Questão 4
Quais são os SSIDs dos dois APs que estão a emitir a maioria das tramas beacon?

Os SSIDs dos dois APs que estão a emitir a maioria das tramas beacon são: *30 Munroe St* e *linksys12*.



No.	Time	Source	Destination	Protocol	Length	Info
247	11.451461	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1504, FN=0, Flags=.......TC
248	11.451560		IntelCor_d1:b6:4f …	802.11	38	Acknowledgement, Flags=........C
249	11.452442	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1505, FN=0, Flags=...P...TC
250	11.452542		IntelCor_d1:b6:4f …	802.11	38	Acknowledgement, Flags=........C
251	11.553787	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2983, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
252	11.656148	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2984, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
253	11.660567	00:06:cb:d2:22:94	ff:bf:f9:fe:ff:ff	802.11	90	Beacon frame, SN=3183, FN=0, Flags=........C, BI=114, SSID=linksys12
254	11.758489	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2985, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
255	11.860890	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2986, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
256	11.963428	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2987, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
257	12.065696	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2988, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
258	12.168142	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2989, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
259	12.270538	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2990, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
260	12.300694	IntelCor_1f:57:13	Broadcast	802.11	75	Probe Request, SN=686, FN=0, Flags=........C, SSID=BOHO2
261	12.302940		Cisco-Li_39:0a:28 …	802.11	38	Acknowledgement, Flags=........C
262	12.372835	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2991, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
263	12.380315	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2992, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
264	12.381814	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2992, FN=0, Flags=....R...C, BI=100, SSID=30 Munroe St
265	12.383564	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2992, FN=0, Flags=....R...C, BI=100, SSID=30 Munroe St
266	12.385062	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2992, FN=0, Flags=....R...C, BI=100, SSID=30 Munroe St
267	12.386565	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2992, FN=0, Flags=....R...C, BI=100, SSID=30 Munroe St
268	12.388067	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2992, FN=0, Flags=....R...C, BI=100, SSID=30 Munroe St
269	12.389438	Cisco-Li_f7:1d:51	IntelCor_1f:57:13	802.11	177	Probe Response, SN=2992, FN=0, Flags=....R...C, BI=100, SSID=30 Munroe St
270	12.475300	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2993, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
271	12.475442	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1506, FN=0, Flags=.......TC
272	12.475540		IntelCor_d1:b6:4f …	802.11	38	Acknowledgement, Flags=........C

Figura 5: Captura do tráfego WireShark

Questão 5
Qual o intervalo de tempo entre a transmissão de tramas beacon para o AP *linksys_ses_24086*? E do AP 30 Munroe St? (Pista: o intervalo está contido na própria trama). Na prática, a periodicidade de tramas beacon é verificada? Tente explicar porquê.

O intervalo de tempo é constante como podemos verificar pelo campo "*Beacon Interval",* sendo este t = 0.102400s. Esta periodicidade é verificada visto que se tratam de tramas de tipo "*Management"* (como é possível verificar através da tabela anexada ao enunciado).

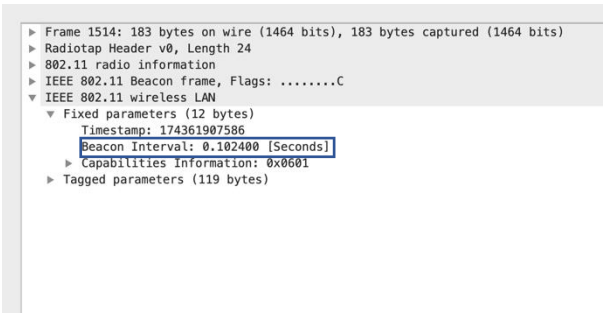


Figura 6: Análise dos campos da trama – Beacon Interval

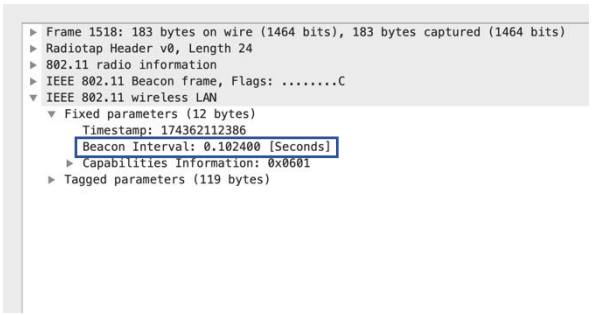


Figura 7: Análise dos campos da trama - Beacon Interval

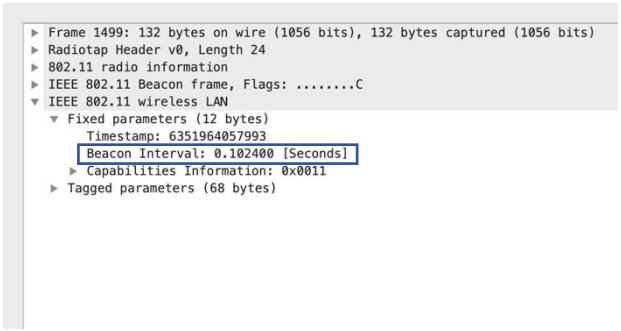


Figura 8: Análise dos campos da trama - Beacon Interval

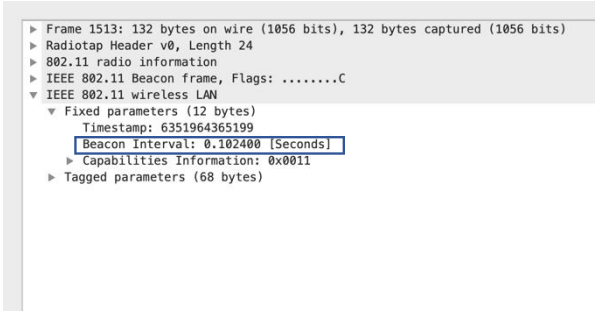


Figura 9: Análise dos campos da trama - Beacon Interval

Questão 6

Qual é (em notação hexadecimal) o endereço MAC de origem da trama beacon de 30 Munroe St?

O endereço MAC de origem da trama *beacon* de *30 Munroe St* é 00:16:b6:f7:1d:51.

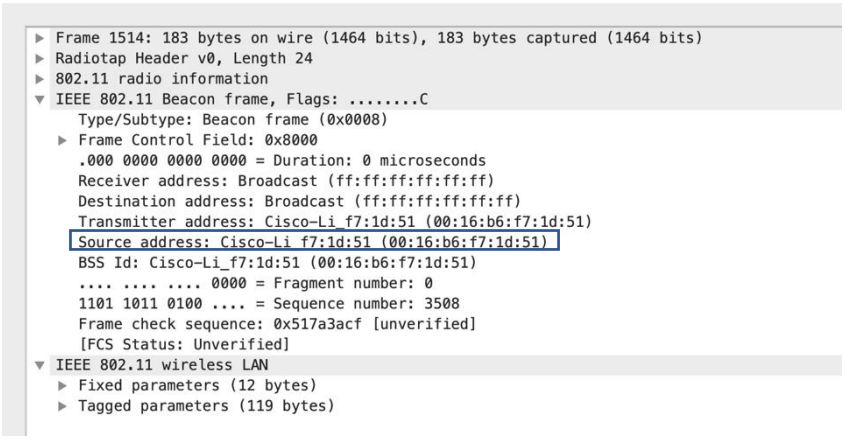


Figura 10: Análise da trama - Campo Source address

Questão 7
Qual é (em notação hexadecimal) o endereço MAC de destino na trama de 30 Munroe St?

O endereço MAC de destino da trama *beacon* de *Munroe St* é ff:ff:ff:ff:ff:ff.

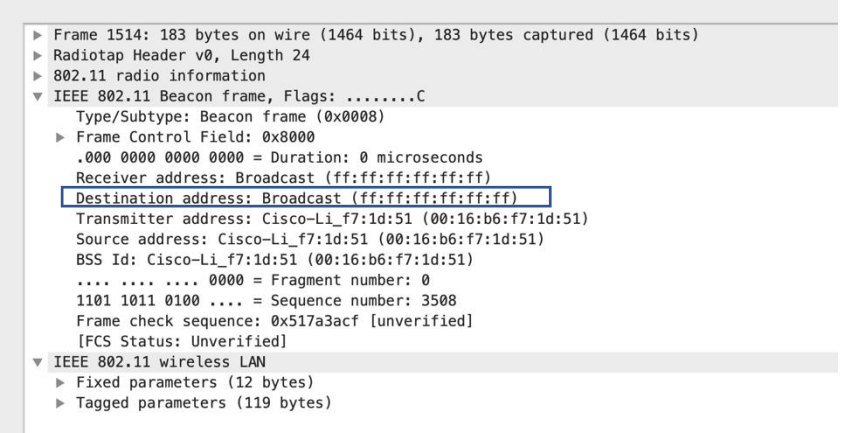


Figura 11: Análise da trama - Campo Destination address

Questão 8
Qual é (em notação hexadecimal) o MAC BSS ID da trama beacon de 30 Munroe St?

O MAC BSS ID da trama *beacon* de 30 *Munroe St* é de: 00:16:b6:f7:1d:51.

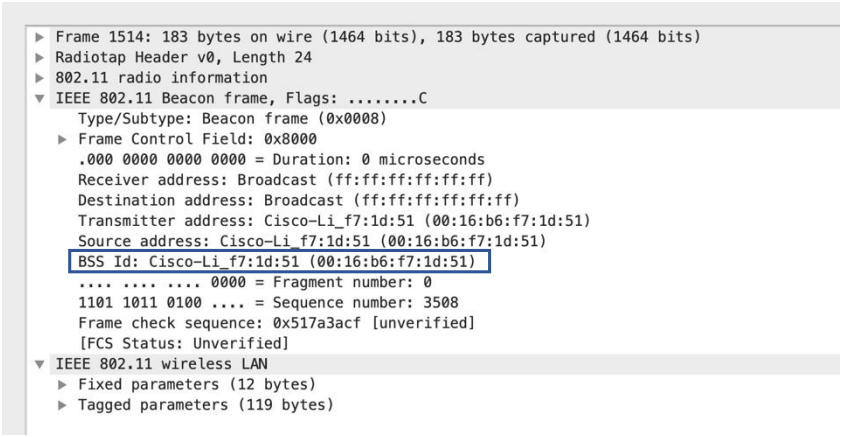


Figura 12: Análise da trama - Campo BSS Id

Questão 9

As tramas beacon do AP 30 Munroe St anunciam que o AP suporta quatro data rates e oito extended suported rates adicionais. Quais são?

Supported Rates: 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
Extended Supported Rates: 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]

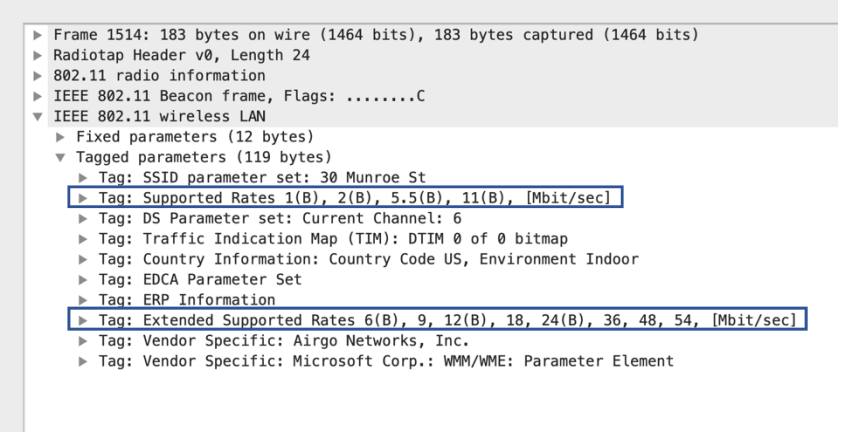


Figura 13: Análise da trama - Campos Supported Rates & Extended Supported Rates

Questão 10

Selecione uma trama beacon.
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?

A trama usada foi 1405.
Como o *Type* = 00 e o *Subtype* = 1000 entende-se que esta trama pertence ao tipo das tramas de gestão (*Management Frame*) e ao subtipo *Beacon*.
Os identificadores estão especificados no byte 24.

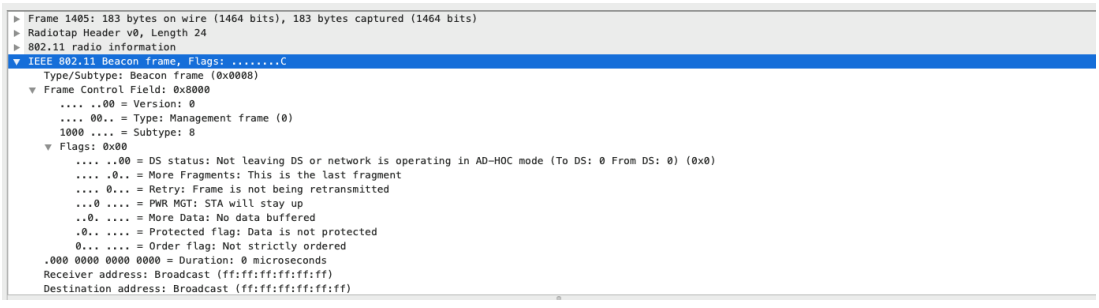


Figura 14: Análise da trama – Campos type e subtype

Questão 11

Verifique se está a ser usado o método de deteção de erros CRC e se todas as tramas beacon são recebidas corretamente. Justifique o uso de mecanismos de deteção de erros nesse tipo de redes locais.

De modo a verificar se está a ser usado o método de deteção de erros CRC e se todas as tramas beacon são recebidas corretamente, foram utilizados os seguintes filtros:

-“ wlan.fc.type_subtype==0x0008”, para selecionar as tramas *Beacon;*
-“wlan.fcs.status==bad“, para restringir as tramas que contêm erros.

Como é possível verificar na figura 15, existiram erros, consequentemente, pode concluir-se que certas tramas não são recebidas corretamente.
O uso de mecanismos de deteção de erros neste tipo de redes locais é muito importante, uma vez que se trata de uma rede sem fios, que ao contrário de uma ligação *ethernet*, é bastante mais propícia a colisões.

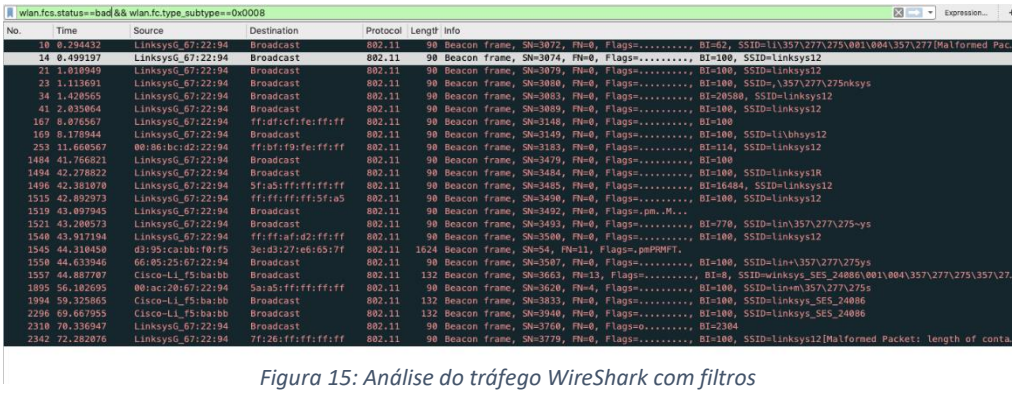


Figura 15: Análise do tráfego WireShark com filtros

Questão 12

Identifique e registe 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.

-Receiver address: ff:ff:ff:ff:ff:ff
-Destination address: ff:ff:ff:ff:ff:ff
-Transmiter address: 00:16:b6:f7:1d:51
-Source address: 00:16:b6:f7:1d:51

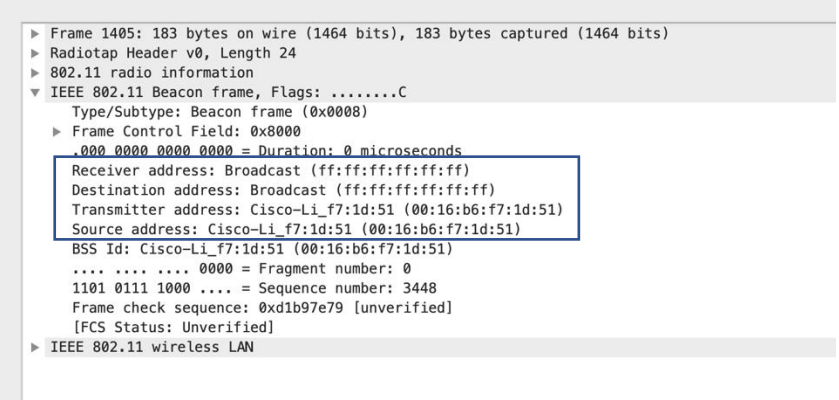


Figura 17: Análise da trama - Endereços MAC

Questão 13

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

Para visualizar todas as tramas *probing request* e *probing response* foram utilizados os filtros “wlan.fc.type_subtype==4” e “wlan.fc.type_subtype==5”, respetivamente.

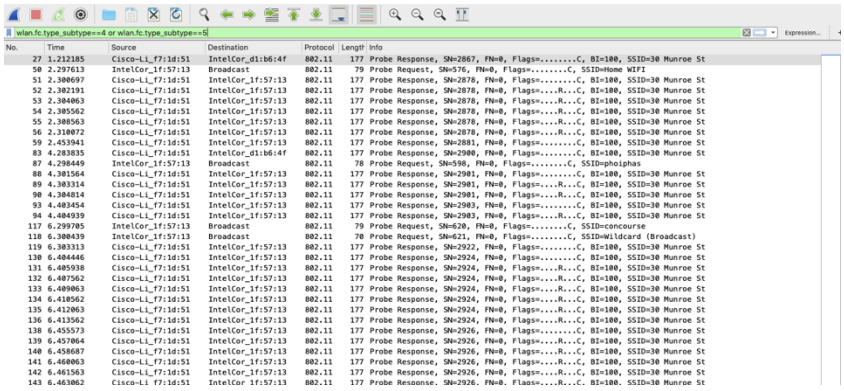


Figura 18: Análise do tráfego Wireshark com filtros

Questão 14

Quais são os endereços MAC BSS ID de destino e origem nestas tramas? Qual o objetivo deste tipo de tramas?

BSS Id Destino: ff:ff:ff:ff:ff:ff
BSS Id Origem: 00:16:b6:f7:1d:51
Um *host* envia um *probe request* quando pretende encontrar um AP (*Access Point)*, por sua vez, o AP envia uma resposta denominada de *probe response*.

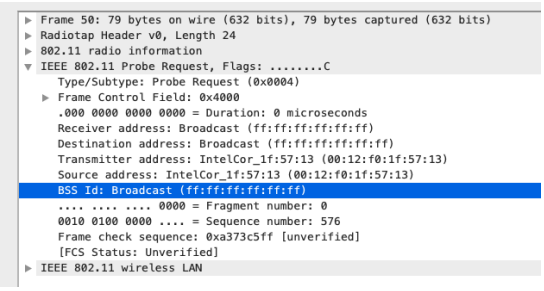


Figura 19: Análise da trama - BSS Id Destino

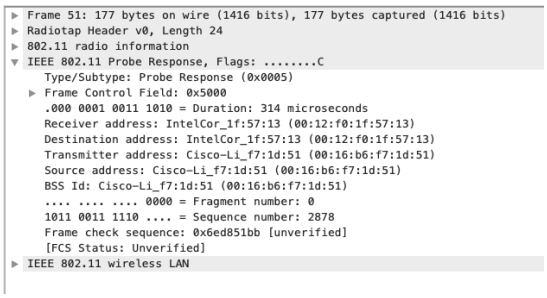


Figura 20: Análise da trama - BSS Id Origem

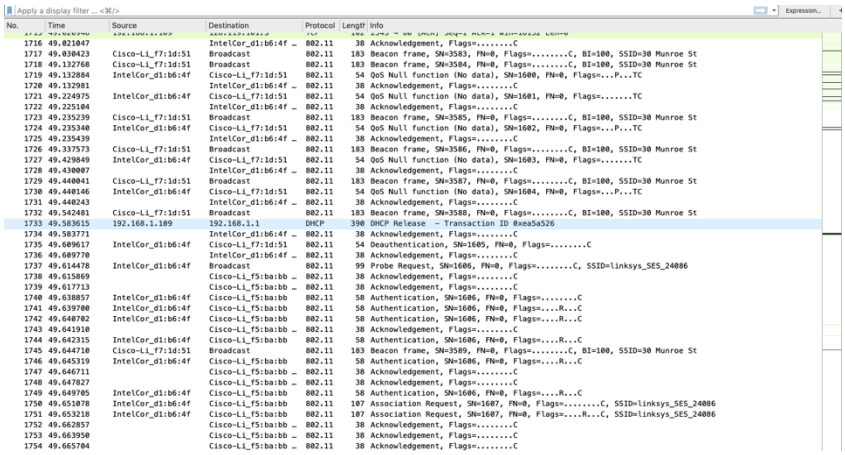
<u>Questão 15</u>
Identifique um probing request para o qual tenha havido um probing response. Face ao endereçamento usado, indique a que sistemas são endereçadas estas tramas e explique qual o propósito das mesmas?

Um exemplo de um *probing request* encontra-se na trama 50 (figura 19), esta trama é enviada do *host* para *broadcast* com o intuito de localizar um AP (*Access Point).* O *probing response* correspondente ao *probing request* enviado, encontra-se na trama 51 (figura 20). Esta mensagem é enviada pelo AP para o *host*, indicando que se encontra disponível para conexão.

1.3 Processo de Associação

<u>Questão 16</u>
Quais as duas ações realizadas (i.e., tramas enviadas) pelo host no trace imediatamente após t=49 para terminar a associação com o AP 30 Munroe St que estava ativa quando o trace teve início? (Pista: uma é na camada IP e outra na camada de ligação 802.11). Observando a especificação 802.11, seria de esperar outra trama, mas que não aparece?

As duas tramas enviadas pelo host no trace imediatamente após t = 49s para terminar a associação com o AP 30 Munroe St são as tramas nº 1733 e 1735.
Seria de esperar que tivesse sido enviada uma trama de *Disassociation request.*



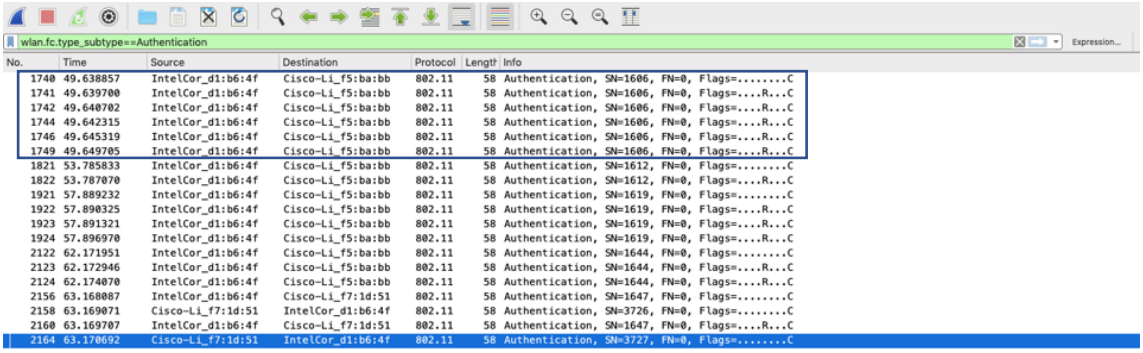
No.	Time	Source	Destination	Protocol	Length	Info
1716	49.021047		IntelCor_d1:b6:4f …	802.11	38	Acknowledgement, Flags=.....C
1717	49.030423	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3583, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1718	49.132768	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3584, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1719	49.132884	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1600, FN=0, Flags=...P...TC
1720	49.132981		IntelCor_d1:b6:4f …	802.11	38	Acknowledgement, Flags=.....C
1721	49.224975	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1601, FN=0, Flags=.....TC
1722	49.225104		IntelCor_d1:b6:4f …	802.11	38	Acknowledgement, Flags=.....C
1723	49.235239	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3585, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1724	49.235340	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1602, FN=0, Flags=...P...TC
1725	49.235439		IntelCor_d1:b6:4f …	802.11	38	Acknowledgement, Flags=.....C
1726	49.337573	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3586, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1727	49.429849	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1603, FN=0, Flags=.....TC
1728	49.430007		IntelCor_d1:b6:4f …	802.11	38	Acknowledgement, Flags=.....C
1729	49.440041	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3587, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1730	49.440146	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1604, FN=0, Flags=...P...TC
1731	49.440243		IntelCor_d1:b6:4f …	802.11	38	Acknowledgement, Flags=.....C
1732	49.542481	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3588, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1733	49.583615	192.168.1.109	192.168.1.1	DHCP	390	DHCP Release - Transaction ID 0xea5a526
1734	49.583771		IntelCor_d1:b6:4f …	802.11	38	Acknowledgement, Flags=.....C
1735	49.689617	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	Deauthentication, SN=1605, FN=0, Flags=.....C
1736	49.689770		IntelCor_d1:b6:4f …	802.11	38	Acknowledgement, Flags=.....C
1737	49.614478	IntelCor_d1:b6:4f	Broadcast	802.11	99	Probe Request, SN=1606, FN=0, Flags=.....C, SSID=linksys_SES_24086
1738	49.615869		Cisco-Li_f5:ba:bb …	802.11	38	Acknowledgement, Flags=.....C
1739	49.617713		Cisco-Li_f5:ba:bb …	802.11	38	Acknowledgement, Flags=.....C
1740	49.638857	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=.....C
1741	49.639700	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1742	49.640702	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1743	49.641910		Cisco-Li_f5:ba:bb …	802.11	38	Acknowledgement, Flags=.....C
1744	49.642315	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1745	49.644710	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3589, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
1746	49.645319	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1747	49.646711		Cisco-Li_f5:ba:bb …	802.11	38	Acknowledgement, Flags=.....C
1748	49.647827		Cisco-Li_f5:ba:bb …	802.11	38	Acknowledgement, Flags=.....C
1749	49.649705	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1750	49.651078	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1607, FN=0, Flags=.....C, SSID=linksys_SES_24086
1751	49.653218	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	107	Association Request, SN=1607, FN=0, Flags=....R...C, SSID=linksys_SES_24086
1752	49.662857		Cisco-Li_f5:ba:bb …	802.11	38	Acknowledgement, Flags=.....C
1753	49.663950		Cisco-Li_f5:ba:bb …	802.11	38	Acknowledgement, Flags=.....C
1754	49.665704		Cisco-Li_f5:ba:bb …	802.11	38	Acknowledgement, Flags=.....C

Figura 21: Análise do tráfego wireshark

Questão 17

Examine o trace e procure tramas de authentication enviadas do host para um AP e vice-versa. Quantas mensagens de authentication foram enviadas do host para o AP linksys_ses_24086 (que tem o endereço MAC Cisco_Li_f5:ba:bb) aproximadamente ao t=49?

Através do filtro: "wlan.fc.type_subtype==Authentication" obtiveram-se as tramas de *authentication*.
Num intervalo de 1s após t = 49s, foram enviadas 6 mensagens de *authentication* do host para o AP linksys_ses_24086.



wlan.fc.type_subtype==Authentication

No.	Time	Source	Destination	Protocol	Length	Info
1740	49.638857	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=.....C
1741	49.639700	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1742	49.640702	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1744	49.642315	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1746	49.645319	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1749	49.649705	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1821	53.785833	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1612, FN=0, Flags=.....C
1822	53.787070	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1612, FN=0, Flags=....R...C
1921	57.889232	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=.....C
1922	57.890325	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
1923	57.891321	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
1924	57.896970	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
2122	62.171951	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0, Flags=.....C
2123	62.172946	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0, Flags=....R...C
2124	62.174070	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58	Authentication, SN=1644, FN=0, Flags=....R...C
2156	63.168087	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58	Authentication, SN=1647, FN=0, Flags=.....C
2158	63.169071	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58	Authentication, SN=3726, FN=0, Flags=.....C
2160	63.169707	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58	Authentication, SN=1647, FN=0, Flags=....R...C
2164	63.170692	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58	Authentication, SN=3727, FN=0, Flags=.....C

Figura 22: Análise do tráfego wireshark com filtro

Questão 18
Qual o tipo de autenticação pretendida pelo host? Aberta ou usando uma chave?

O tipo de autenticação pretendida pelo host é aberta.

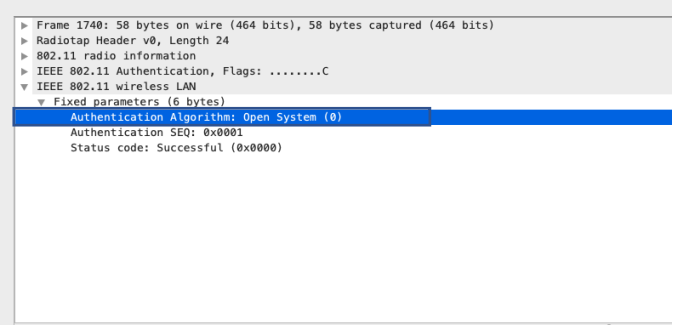


Figura 23: Análise de trama - Campo Authentication Algorithm

Questão 19
Observa-se a resposta de authentication do AP *linksys_ses_24086* AP no trace?

Não são observadas respostas de *authentication* do AP no trace, como é possível verificar na figura 24.

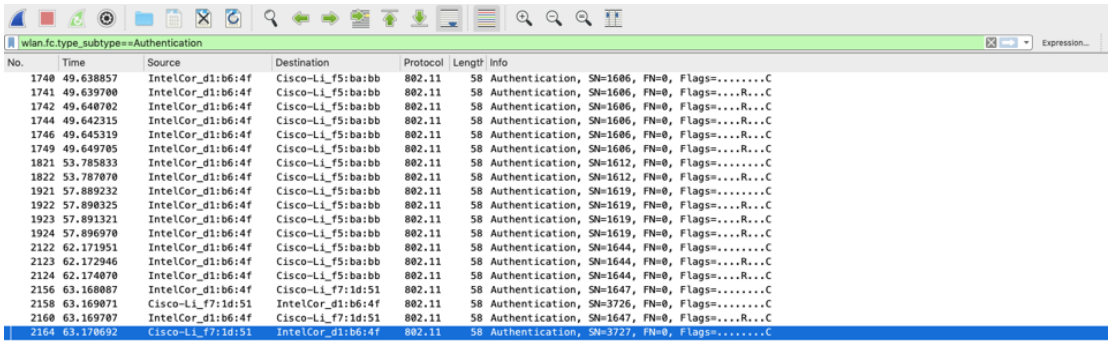


Figura 24: Análise do tráfego wireshark com filtros

Questão 20

Vamos agora considerar o que acontece quando o host desiste de se associar ao AP *linksys_ses_24086* AP e se tenta associar ao AP 30 Munroe ST. Procure tramas authentication enviadas pelo host para e do AP e vice-versa. Em que tempo aparece uma trama authentication do host para o AP 30 Munroe St. E quando aparece a resposta authentication do AP para o host?

Em t = 63.168087s é enviada uma trama de authentication pelo host para o AP 30 Munroe St. Em t = 63.169071s é enviada uma trama de autenticação como resposta do AP para o host.

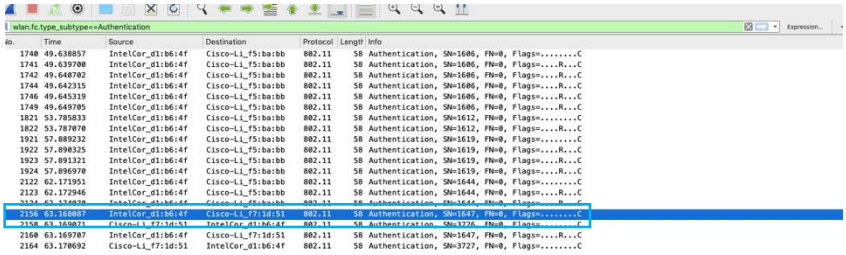


Figura 25: Análise do tráfego wireshark com filtros

Questão 21

Um associate request do host para o AP e uma trama de associate response correspondente do AP para o host são usados para que o host seja associado a um AP. Quando aparece o associate request do host para o AP 30 Munroe St? Quando é enviado o correspondente associate reply?

Em t = 63.169910s é enviado um *associate request* do host para o AP 30 *Munroe ST*. O correspondente *association reply* é enviado em t = 63.192101s.

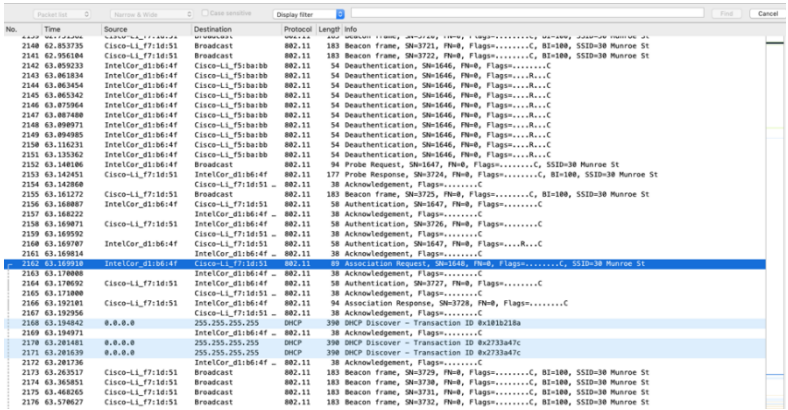


Figura 26: Análise do tráfego wireshark

Questão 22
Que taxas de transmissão o host está disposto a usar? E o AP?

As taxas de transmissão que o host está disposto a usar são: 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, 54, [Mbit/sec].
As taxas de transmissão que o AP está disposto a usar, tal como verificado através da figura 28, são as mesmas que as do host.

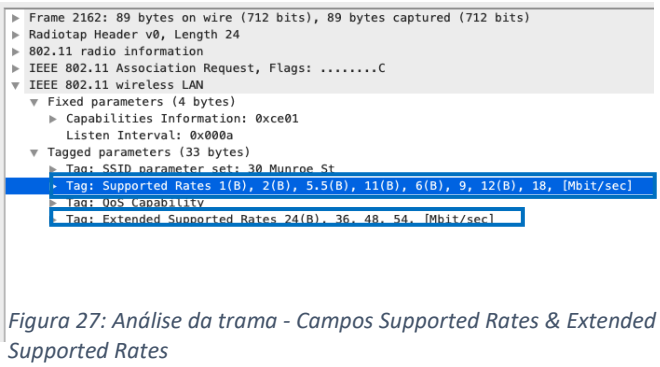


Figura 27: Análise da trama - Campos Supported Rates & Extended Supported Rates

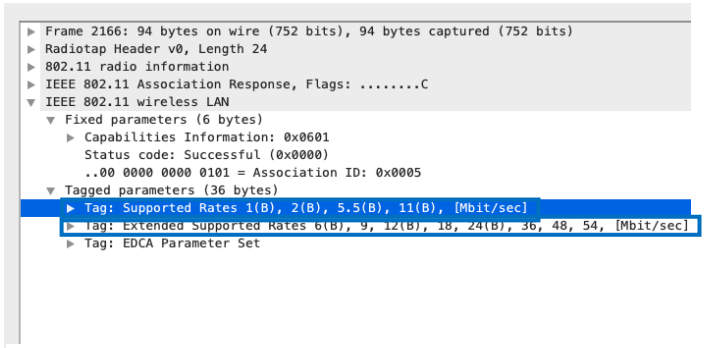


Figura 28: Análise da trama - Campos Supported Rates & Extended Supported Rates

Questão 23
Identifique uma sequência de tramas que corresponda a um processo de associação completo entre a STA e o AP, incluindo a fase de autenticação.

A sequência de tramas correspondentes a um processo de associação completo entre STA e o AP encontra-se identificada na figura 29.

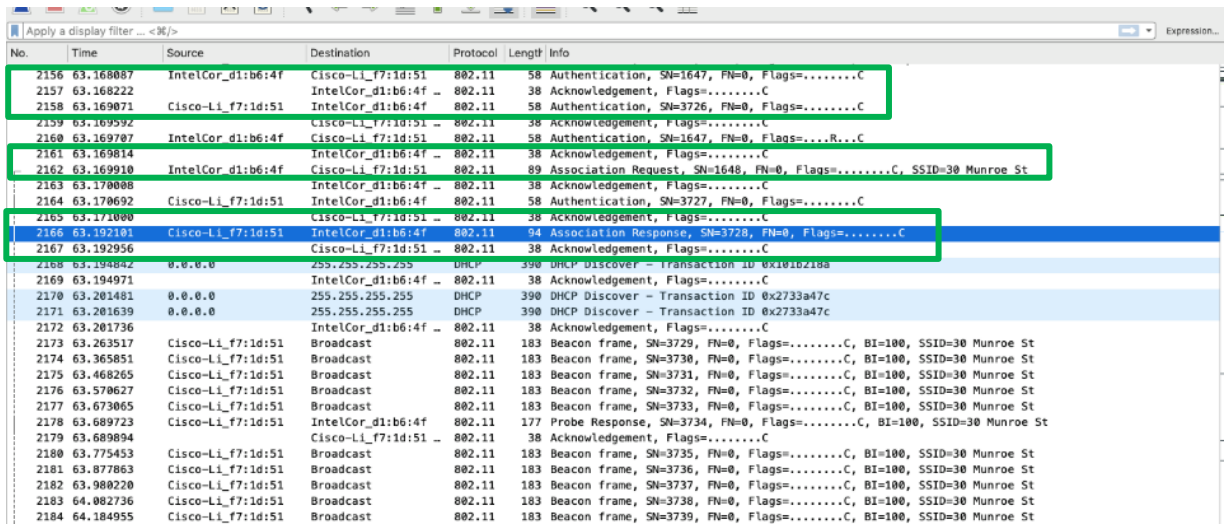
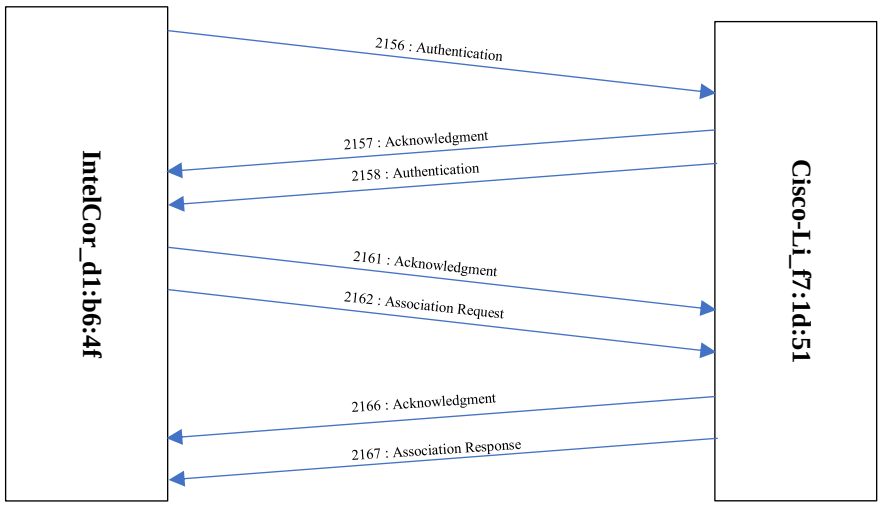


Figura 29: Análise do tráfego wireshark

Questão 24
Efetue um diagrama que ilustre a sequência de todas as tramas trocadas no processo de associação, incluindo a fase de autenticação.



1.4 Transferência de Dados

Questão 25
Encontre a trama 802.11 que contém o segmento SYN TCP para a primeira sessão TCP (download alice.txt). Quais são os três campos dos endereços MAC na trama 802.11?

Os três campos dos endereços MAC na trama 802.11 são:
- STA address: 00:13:02:d1:b6:4f
- Destination address: 00:16:b6:f4:eb:a8
- BSS Id: 00:16:b6:f7:1d:51

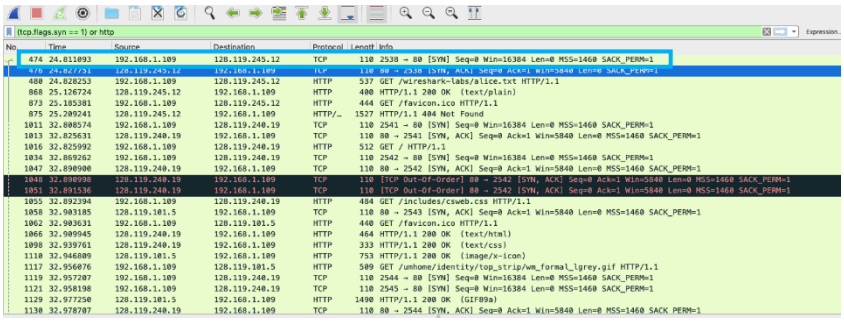


Figura 30: Tráfego wireshark com filtro syn == 1

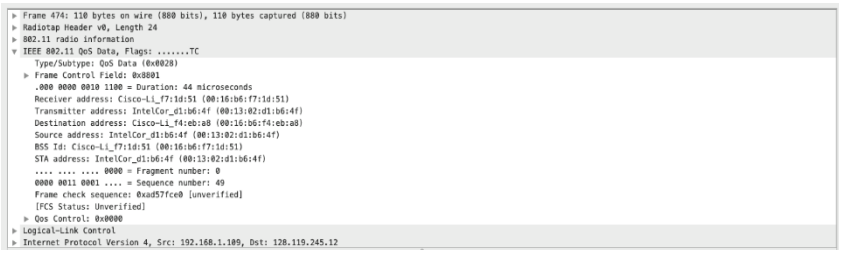


Figura 31: Análise da trama - endereços MAC

<u>Questão 26</u>

Qual o endereço MAC nesta trama que corresponde ao host (em notação hexadecimal)? Qual o do AP? Qual o do router do primeiro salto? Qual o endereço IP do host que está a enviar este segmento TCP? Qual o endereço IP de destino?

O endereço MAC que corresponde ao *host* é 00:13:02:d1:b6:4f, o do AP é 00:16:b6:f4:eb:a8. Já o do router do primeiro salto é 00:16:b6:f7:1d:51. Tudo isto, encontra-se visível na figura 31.
O endereço IP do host que está a enviar este segmento TCP é 192.168.1.109, o endereço IP de destino é 128.119.245.12, como está apresentado na figura 32.

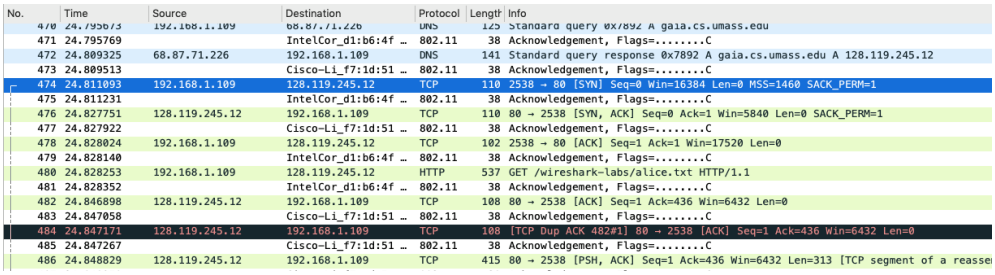


Figura 32: Captura do tráfego WireShark

Questão 27

Este endereço IP de destino corresponde ao host, AP, router do primeiro salto, ou outro equipamento de rede? Justifique.

Este endereço IP de destino corresponde a outro equipamento de rede, sendo este o servidor destino, uma vez que

Questão 28

Encontre agora a trama 802.11 que contém o segmento SYNACK para esta sessão TCP. Quais são os três campos dos endereços MAC na trama 802.11?

Os três campos dos endereços MAC na trama 802.11:
- STA address: 91:2a:b0:49:b6:4f
- BSS Id: 00:16:b6:f7:1d:51
- Source address: 00:16:b6:f4:eb:a8

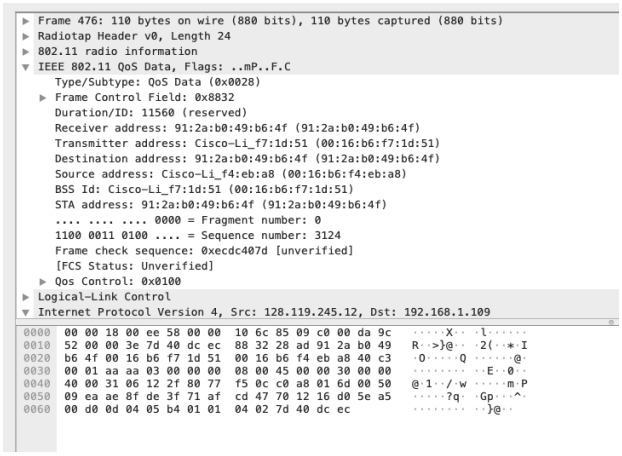


Figura 33: Análise da trama - Endereços MAC

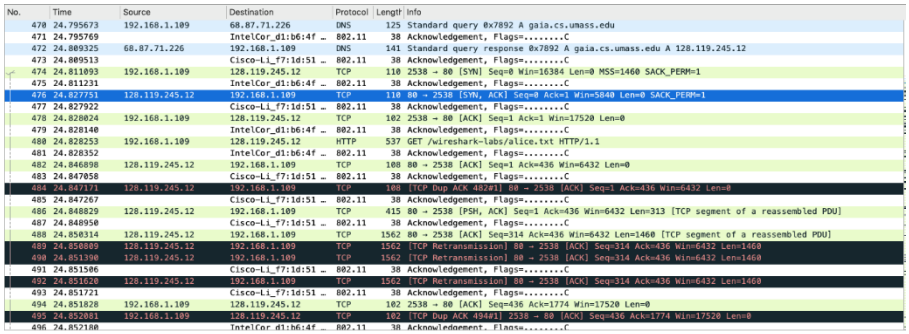


Figura 34: Análise do tráfego WireShark

Questão 29

Qual o endereço MAC nesta trama que corresponde ao host? Qual o AP? Qual o do router do primeiro salto?

O endereço MAC nesta trama que corresponde ao host é 91:2a:b0:49:b6:4f, o do AP é 00:16:b6:f7:1d:4f e o do router do primeiro salto é 00:16:b6:f7:1d:51. Tudo isto, encontra-se apresentado figura 33.

Questão 30

O endereço MAC de origem na trama corresponde ao endereço IP do dispositivo que enviou o segmento TCP encapsulado neste datagrama? Justifique.

Não, uma vez que o endereço IP é o endereço de origem que envia a trama com o segmento SYNACK (que se encontra fora da rede local e que corresponde à camada 3). Quando a mensagem chega ao AP da rede local é desencapsulada e é atribuído ao endereço de origem o endereço MAC do AP, visto que ocorre a transição para a camada 2, logo o endereço MAC de origem será o endereço MAC do AP.

2. Conclusões

Este trabalho tem como principal objetivo explorar vários aspetos do protocolo IEEE 802.11.
Com o intuito da exploração destes conceitos foi fornecida uma captura WireShark, na qual foram analisadas, numa primeira fase, as sequências de bytes capturadas (incluídas no nível físico – *radio information*), como também bytes relativos a tramas 802.11.
Seguidamente, analisou-se o *scanning* passivo em redes Wi-Fi, através das capturas de tramas *beacon,* onde foram ainda observados endereços MAC de origem e destino destas tramas, os intervalos de tempo entre a transmissão deste tipo de tramas *(Beacon Interval)* e a deteção de erros CRC. Já quanto ao *scanning* ativo foram examinadas tramas *probing request* e *probing response*.
Posteriormente, tendo consciência que numa rede Wi-Fi estruturada um *host* deve associar-se a um ponto de acesso (AP) antes de enviar dados, foi averiguado o processo de associação completo entre um *host* e um AP, este processo só é possível se forem enviadas tramas de associação após o envio de tramas de autenticação.
Relativamente à transferência de dados foram verificados os segmentos SYN TCP e SYNACK para as respetivas sessões TCP, analisou-se especificamente uma permuta realizada entre hosts e APs de diferentes redes.
Por fim, este trabalho tornou-se bastante revelador de conceitos apreendidos à priori, bem como a aprendizagem de novos conteúdos relativos ao protocolo IEEE 802.11.