

Atividade sobre Wi-fi

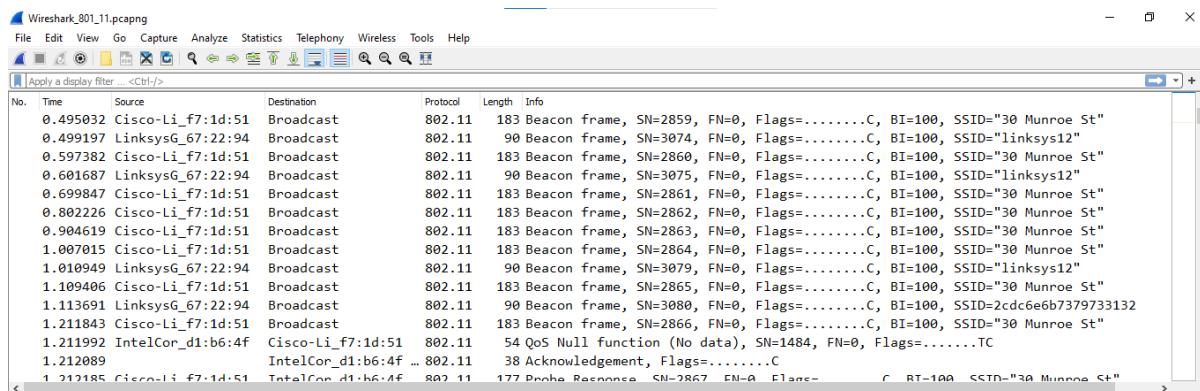
Redes de Computadores

Sabrina Araújo Cardoso - 118210114

Wireshark Lab: 802.11 Wifi

A atividade foi feita utilizando o pacote capturado pelo autor.

- **Questão 1:** Quais são os SSIDs dos dois pontos de acesso que estão emitindo a maioria dos quadros de beacon neste rastreamento?



No.	Time	Source	Destination	Protocol	Length	Info
0.495032		Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2859, FN=0, Flags=.....C, BI=100, SSID="30 Munroe St"
0.499197		LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3074, FN=0, Flags=.....C, BI=100, SSID="linksys12"
0.597382		Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2860, FN=0, Flags=.....C, BI=100, SSID="30 Munroe St"
0.601687		LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3075, FN=0, Flags=.....C, BI=100, SSID="linksys12"
0.699847		Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2861, FN=0, Flags=.....C, BI=100, SSID="30 Munroe St"
0.802226		Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2862, FN=0, Flags=.....C, BI=100, SSID="30 Munroe St"
0.904619		Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2863, FN=0, Flags=.....C, BI=100, SSID="30 Munroe St"
1.007015		Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2864, FN=0, Flags=.....C, BI=100, SSID="30 Munroe St"
1.010949		LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3079, FN=0, Flags=.....C, BI=100, SSID="linksys12"
1.109406		Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2865, FN=0, Flags=.....C, BI=100, SSID="30 Munroe St"
1.113691		LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3080, FN=0, Flags=.....C, BI=100, SSID="linksys12"
1.211843		Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2866, FN=0, Flags=.....C, BI=100, SSID="30 Munroe St"
1.211992		IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1484, FN=0, Flags=.....TC
1.212089		IntelCor_d1:b6:4f	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C
1.212185		Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	177	Probe Response, SN=2867, FN=0, Flags=.....C, BI=100, SSID="30 Munroe St"

Os dois pontos de acesso que estão emitindo a maioria dos quadros de beacon são:

SSID="30 Munroe St"

SSID="linksys12"

- **Questão 2:** Quais são os intervalos de tempo entre as transmissões dos quadros de beacon do ponto de acesso linksys_ses_24086? E do ponto de acesso 30 Munroe St? (Dica: esse intervalo de tempo está contido no próprio quadro de beacon).

```

    IEEE 802.11 Wireless Management
    Fixed parameters (12 bytes)
      Timestamp: 174319001986
      Beacon Interval: 0,102400 [Seconds]
    Capabilities Information: 0x0601
    Tagged parameters (119 bytes)

```

Beacon Interval: **0.1024 segundos**

- **Questão 3:** Qual é o endereço MAC de origem (em notação hexadecimal) no quadro de beacon do 30 Munroe St? Lembre-se da Figura 7.13 no texto, onde o endereço de origem, destino e BSS são três endereços usados em um quadro 802.11. Para uma discussão detalhada da estrutura do quadro 802.11, consulte a seção 7 no documento de padrões IEEE 802.11 (citado acima).

```

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: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Source address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    .... 0000 = Fragment number: 0
    1011 0010 0110 .... = Sequence number: 2854
    Frame check sequence: 0x057e2608 [unverified]
    [FCS Status: Unverified]

```

Source Address de 30 Munroe St é **00:16:b6:f7:1d:51**

- **Questão 4:** Qual é o endereço MAC de destino (em notação hexadecimal) no quadro de beacon do 30 Munroe St?

O Destination Address de 30 Munroe St é **ff:ff:ff:ff:ff:ff**

- **Questão 5:** Qual é o MAC BSS id (em notação hexadecimal) no quadro de beacon do 30 Munroe St?

O endereço MAC BSS ID no quadro de beacon do 30 Munroe St é 00:16:b6:f7:1d:51. Ele é o mesmo que o endereço de origem.

- **Questão 6:** Os quadros de beacon do ponto de acesso 30 Munroe St anunciam que o ponto de acesso pode suportar quatro taxas de dados e oito "taxas suportadas estendidas" adicionais. Quais são essas taxas?

```

▼ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
  Tag Number: Supported Rates (1)
  Tag length: 4
  Supported Rates: 1(B) (0x82)
  Supported Rates: 2(B) (0x84)
  Supported Rates: 5.5(B) (0x8b)
  Supported Rates: 11(B) (0x96)
> Tag: DS Parameter set: Current Channel: 6
> Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
> Tag: Country Information: Country Code US, Environment Indoor
> Tag: EDCA Parameter Set
> Tag: ERP Information
▼ Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
  Tag Number: Extended Supported Rates (50)
  Tag length: 8
  Extended Supported Rates: 6(B) (0x8c)
  Extended Supported Rates: 9 (0x12)
  Extended Supported Rates: 12(B) (0x98)
  Extended Supported Rates: 18 (0x24)
  Extended Supported Rates: 24(B) (0xb0)
  Extended Supported Rates: 36 (0x48)
  Extended Supported Rates: 48 (0x60)
  Extended Supported Rates: 54 (0x6c)

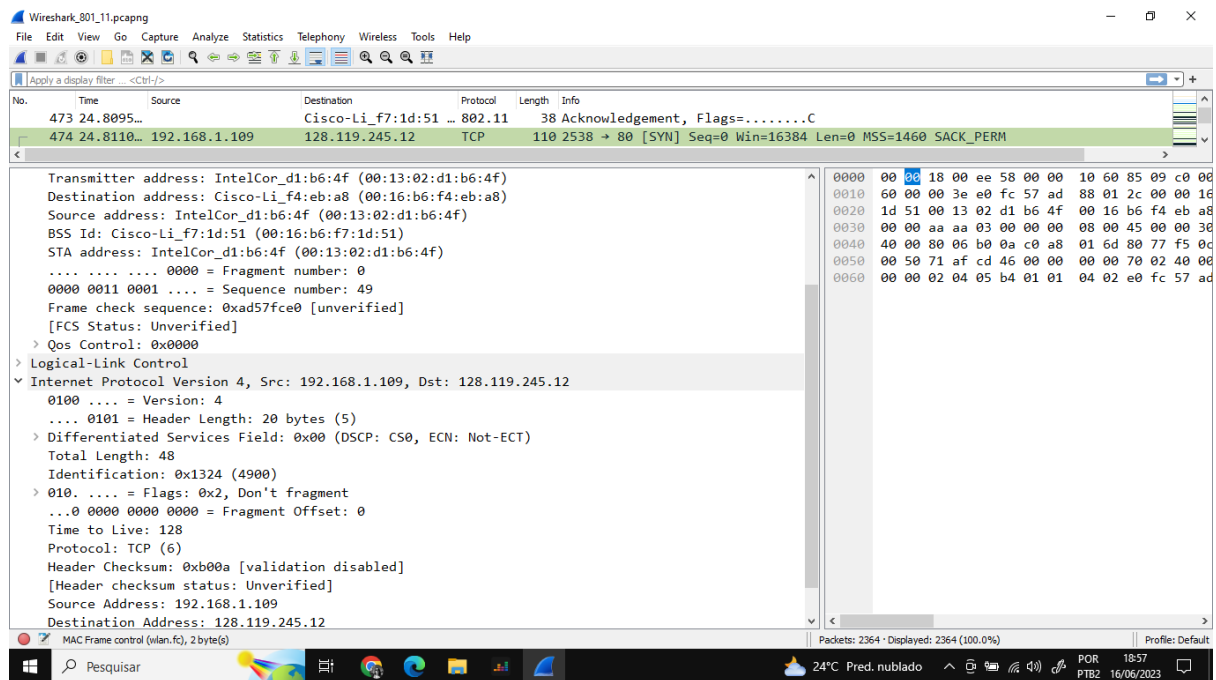
```

Supported Rates: 1.0, 2.0, 5.5, 11.0 Mbps.

Extended Supported Rates: 6.0, 9.0, 12.0, 18.0, 24.0, 36.0, 48.0, 54.0 Mbps.

- **Questão 7:** Encontre o quadro 802.11 que contém o segmento TCP SYN para esta primeira sessão TCP (que baixa o arquivo alice.txt). Quais são os três campos de endereço MAC no quadro 802.11? Qual endereço MAC neste quadro corresponde ao host sem fio (forneça a representação hexadecimal do

endereço MAC do host)? Ao ponto de acesso? Ao roteador de primeira etapa? Qual é o endereço IP do host sem fio que envia este segmento TCP? Qual é o endereço IP de destino? Esse endereço IP de destino corresponde ao host, ponto de acesso, roteador de primeira etapa ou a algum outro dispositivo conectado à rede? Explique.



O TCP SYN é enviado em **t = 24,811093** segundos.

O endereço MAC do host que envia o TCP SYN é **00:13:02:d1:b6:4f**.

O endereço MAC de destino, é **00:16:b6:f4:eb:a8**.

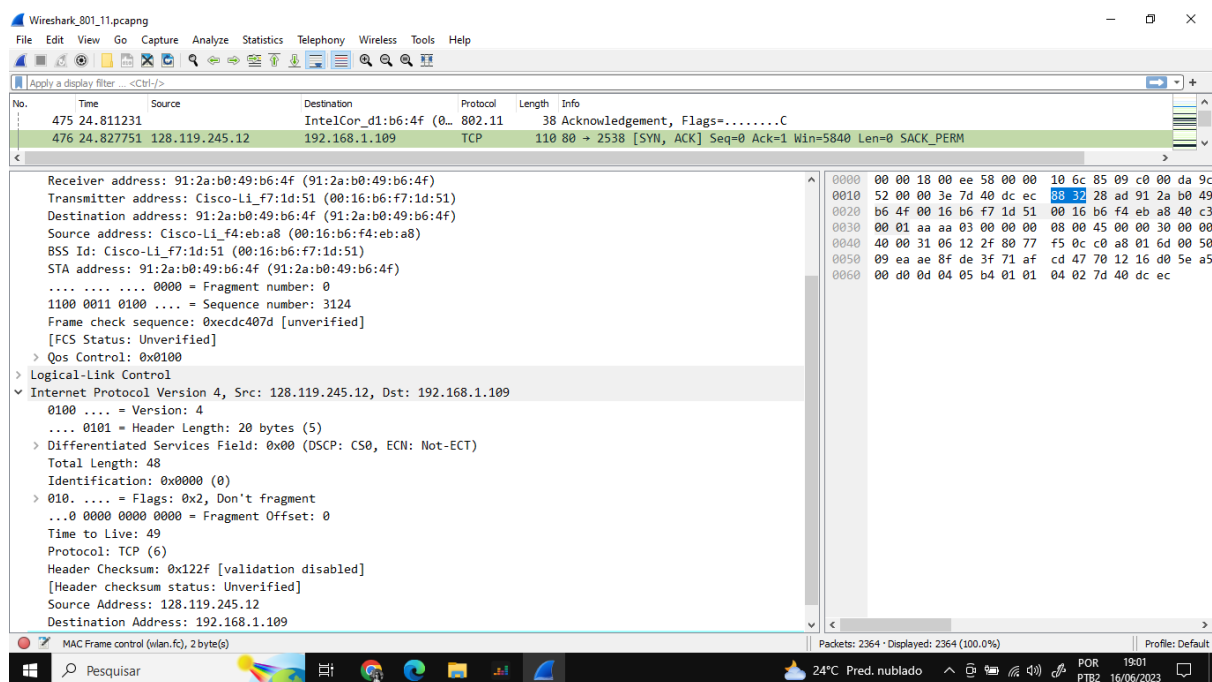
O endereço MAC do BSS é **00:16:b6:f7:1d:51**.

O endereço IP do host que envia o TCP SYN é **192.168.1.109** (Observe que este é um endereço com NAT)

O endereço de destino é **128.119.245.12**.

Isso corresponde ao servidor gaia.cs.umass.edu. É importante entender que o endereço MAC de destino do quadro que contém o SYN é diferente do endereço IP de destino do pacote IP contido neste quadro.

- **Questão 8:** Encontre o quadro 802.11 que contém o segmento SYNACK para esta sessão TCP. Quais são os três campos de endereço MAC no quadro 802.11? Qual endereço MAC neste quadro corresponde ao host? Ao ponto de acesso? Ao roteador de primeira etapa? O endereço MAC do remetente no quadro corresponde ao endereço IP do dispositivo que enviou o segmento TCP encapsulado neste datagrama? (Dica: revise a Figura 6.19 no texto se você não tem certeza de como responder a esta pergunta, ou a parte correspondente da pergunta anterior. É especialmente importante que você entenda isso).



O TCP SYNACK é recebido em **t = 24,827751** segundos no rastreamento.

O endereço MAC do remetente do quadro 802.11 que contém o segmento TCP SYNACK é **00:16:b6:f4:eb:a8**, que é o roteador do primeiro salto ao qual o host está conectado.

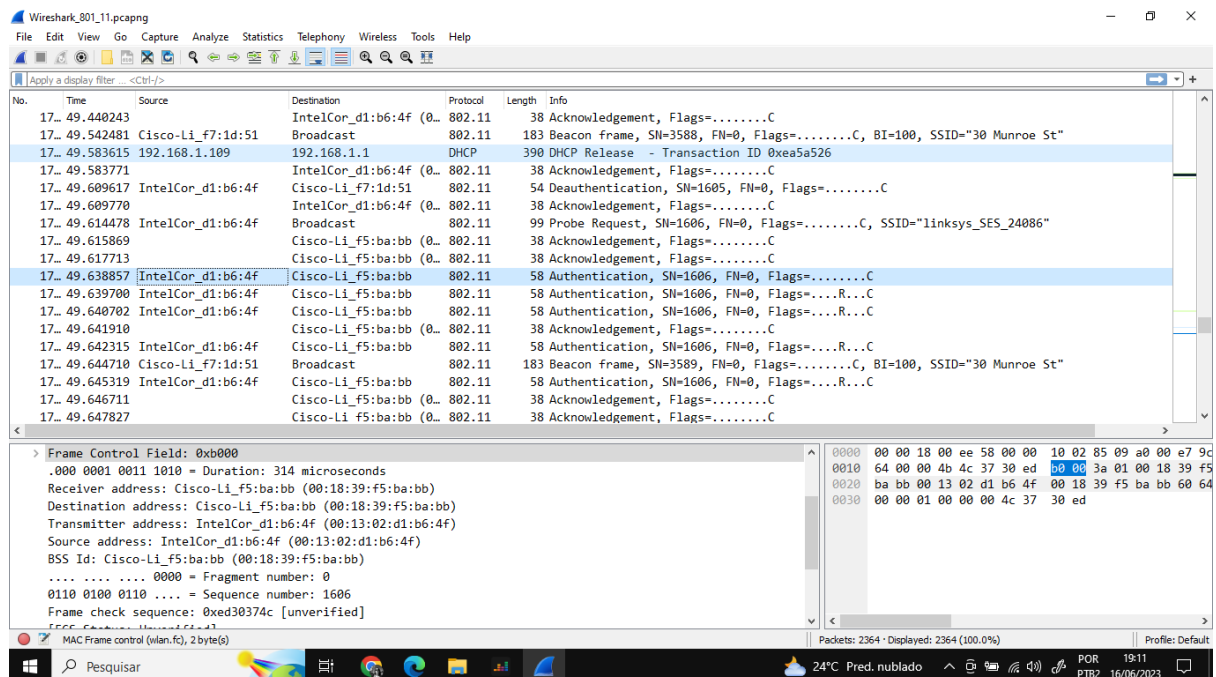
O endereço MAC de destino, que é o próprio host, é **91:2a:b0:49:b6:4f**.

O endereço MAC do BSS é **00:16:b6:f7:1d:51**.

O endereço IP do servidor que envia o TCP SYNACK é **128.119.245.12** (gaia.cs.umass.edu).

O endereço de destino é **192.168.1.109** (nosso PC wireless).

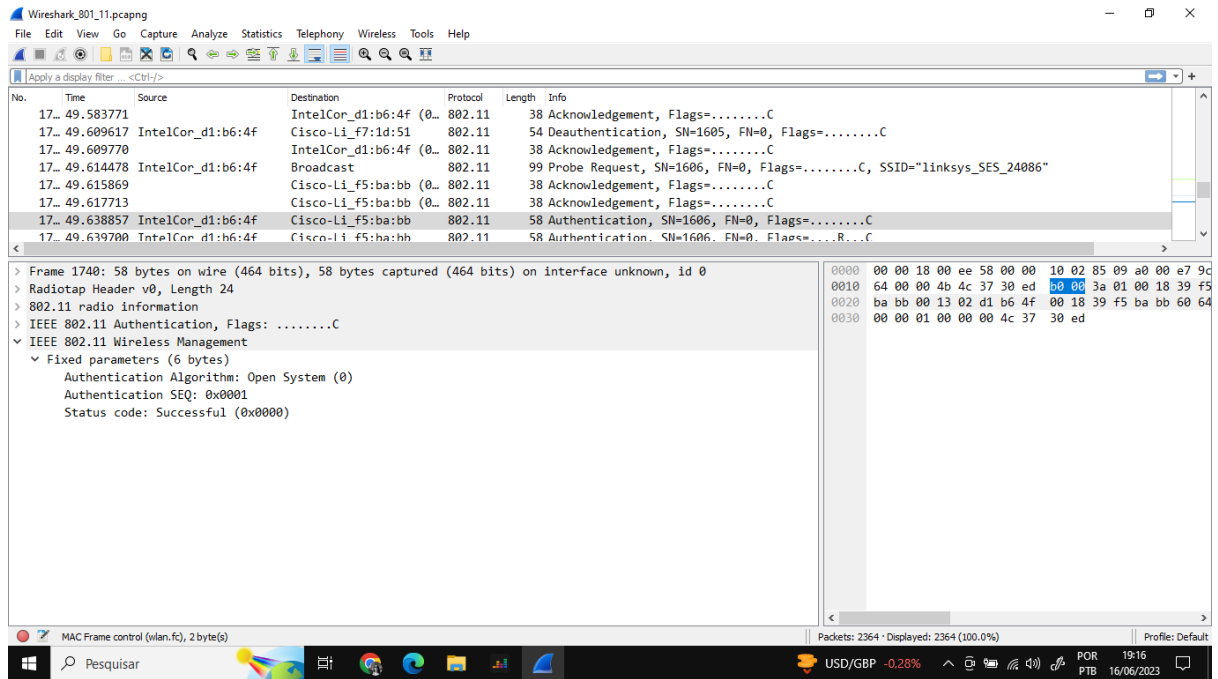
linksys_ses_24086 (que possui um endereço MAC de Cisco_Li_f5:ba:bb) a partir de cerca de t=49?



São enviadas 18 autenticações.

A primeira autenticação do host para o AP ocorre em t = 49.638857.

- **Questão 11:** O host deseja que a autenticação exija uma chave ou seja aberta?



Authentication Algorithm: **Open System (0)**

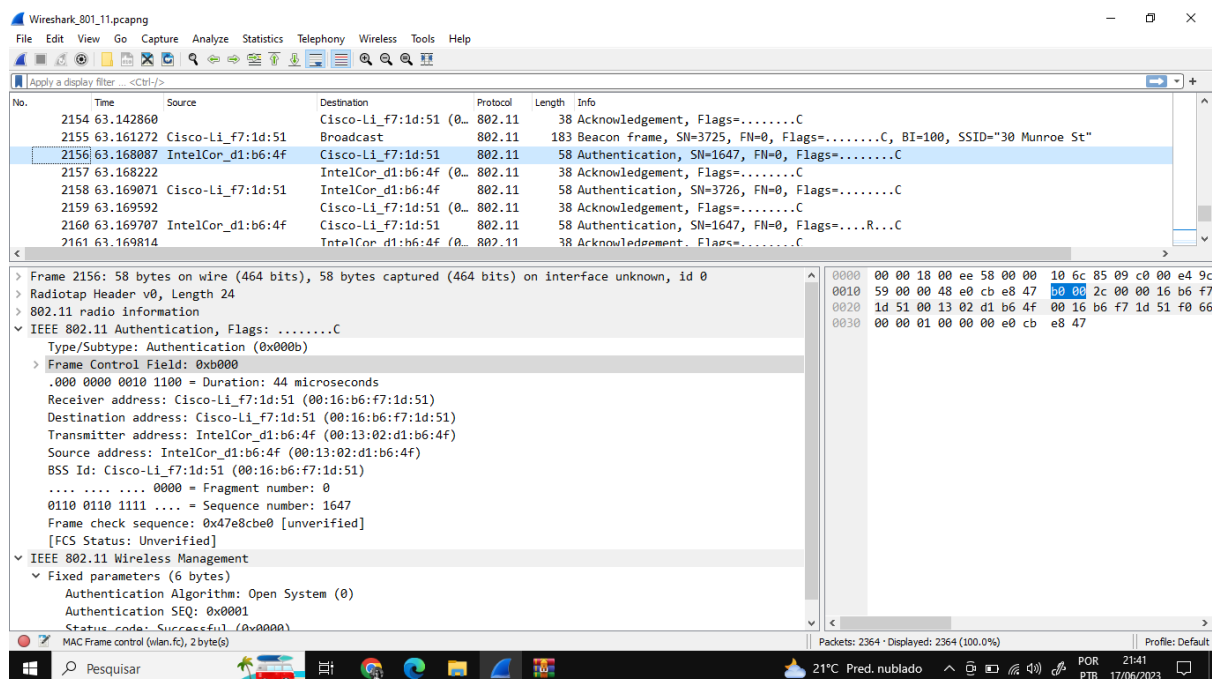
O host está solicitando que a associação seja aberta.

- **Questão 12:** Você vê uma resposta de AUTENTICAÇÃO do AP linksys_ses_24086 no rastreamento?

Não consigo encontrar nenhuma resposta do AP. Isso provavelmente ocorre porque o AP está configurado para exigir uma chave ao se associar a ele, portanto, o AP provavelmente está ignorando (ou seja, não respondendo) às solicitações de acesso aberto.

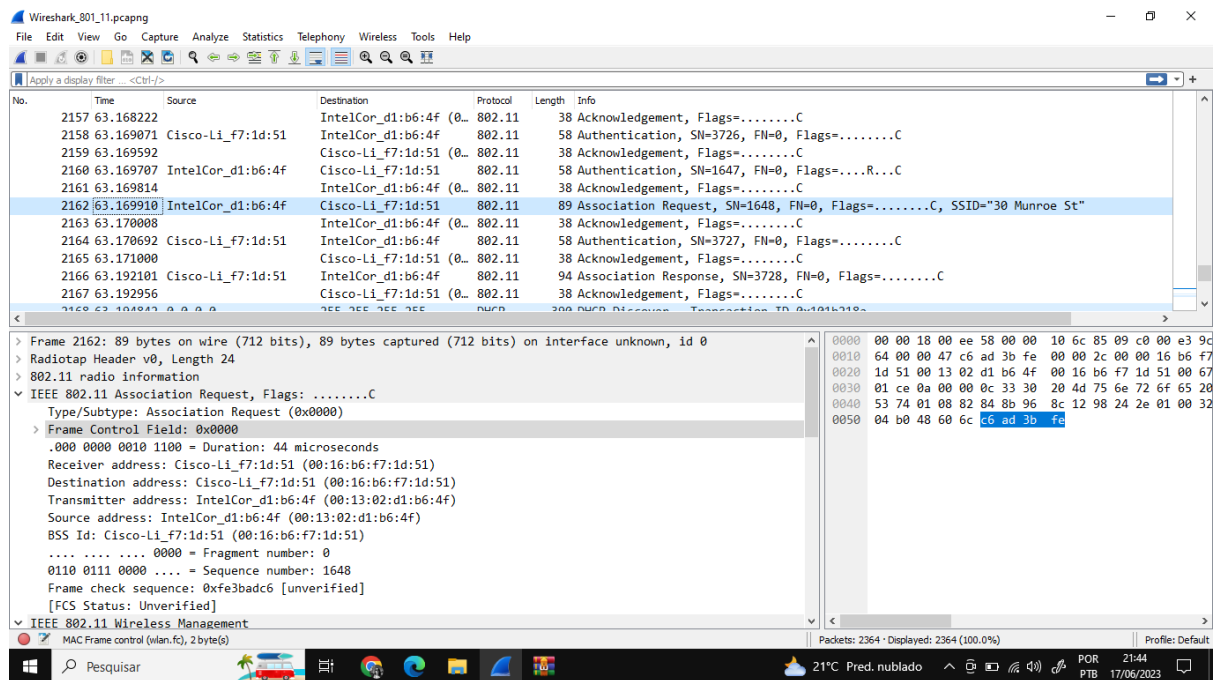
- **Questão 13:** Agora vamos considerar o que acontece quando o host desiste de tentar se associar ao AP linksys_ses_24086 e agora tenta se associar ao AP 30 Munroe St. Procure por quadros de AUTENTICAÇÃO enviados pelo host para o AP e vice-versa. Em que momentos há um quadro de AUTENTICAÇÃO do host para o AP 30 Munroe St e quando há uma resposta de AUTENTICAÇÃO enviada por esse AP em resposta ao host? (Observação: você pode usar a expressão de filtro "wlan.fc.subtype == 11 e wlan.fc.type == 0 e wlan.addr ==

IntelCor_d1:b6:4f" para exibir apenas os quadros de AUTENTICAÇÃO neste rastreamento para este host sem fio.)



Em **t = 63.168087**, há um quadro de AUTENTICAÇÃO enviado de **00:13:02:d1:b6:4f** (o host sem fio) para **00:16:b7:f7:1d:51**. Em **t = 63.169071**, há uma AUTENTICAÇÃO enviada no sentido inverso.

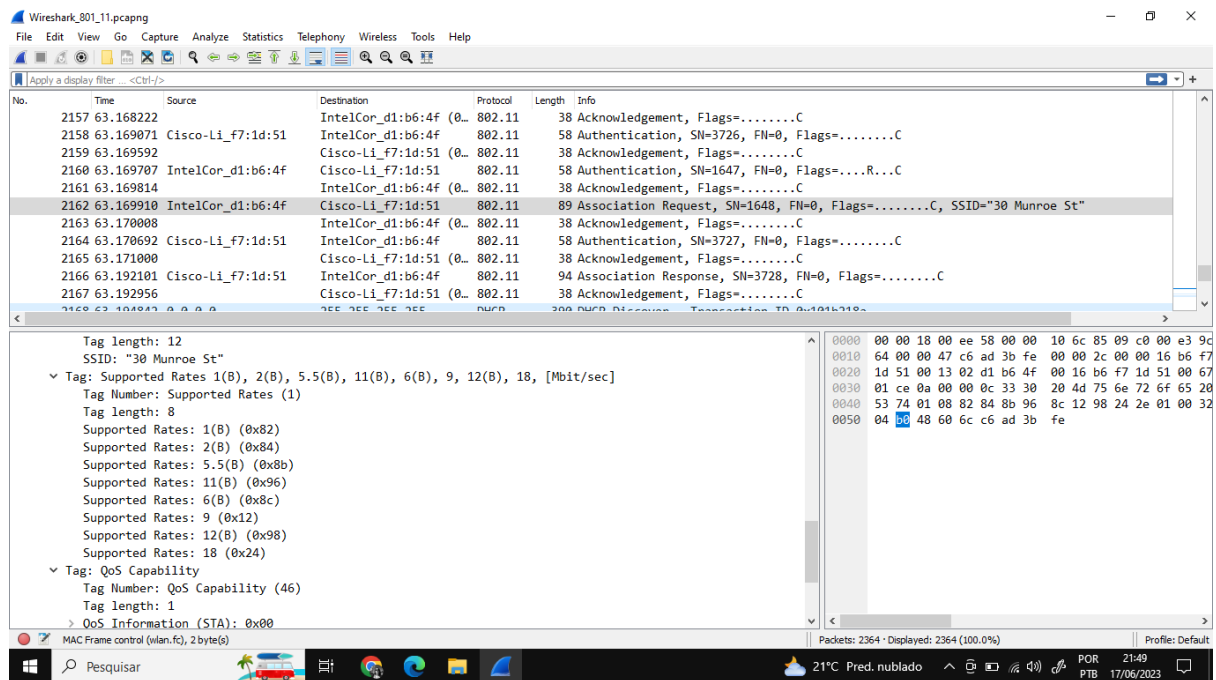
- **Questão 14:** Uma solicitação de ASSOCIAÇÃO do host para o AP e um quadro de RESPOSTA DE ASSOCIAÇÃO correspondente do AP para o host são usados para o host se associar a um AP. Em que momento há uma solicitação de ASSOCIAÇÃO do host para o AP 30 Munroe St? Quando é enviada a resposta de ASSOCIAÇÃO correspondente? (Observação: você pode usar a expressão de filtro "wlan.fc.subtype < 2 e wlan.fc.type == 0 e wlan.addr == IntelCor_d1:b6:4f" para exibir apenas os quadros de solicitação de ASSOCIAÇÃO e RESPOSTA DE ASSOCIAÇÃO neste rastreamento.)



Em **t = 63.169910**, há um quadro de ASSOCIATION RESPONSE enviado de **00:13:02:d1:b6:4f** (o host sem fio) para **00:16:b7:f7:1d:51** (o BSS).

Em **t = 63.192101**, há uma ASSOCIATION RESPONSE enviada no sentido inverso do BSS para o host sem fio.

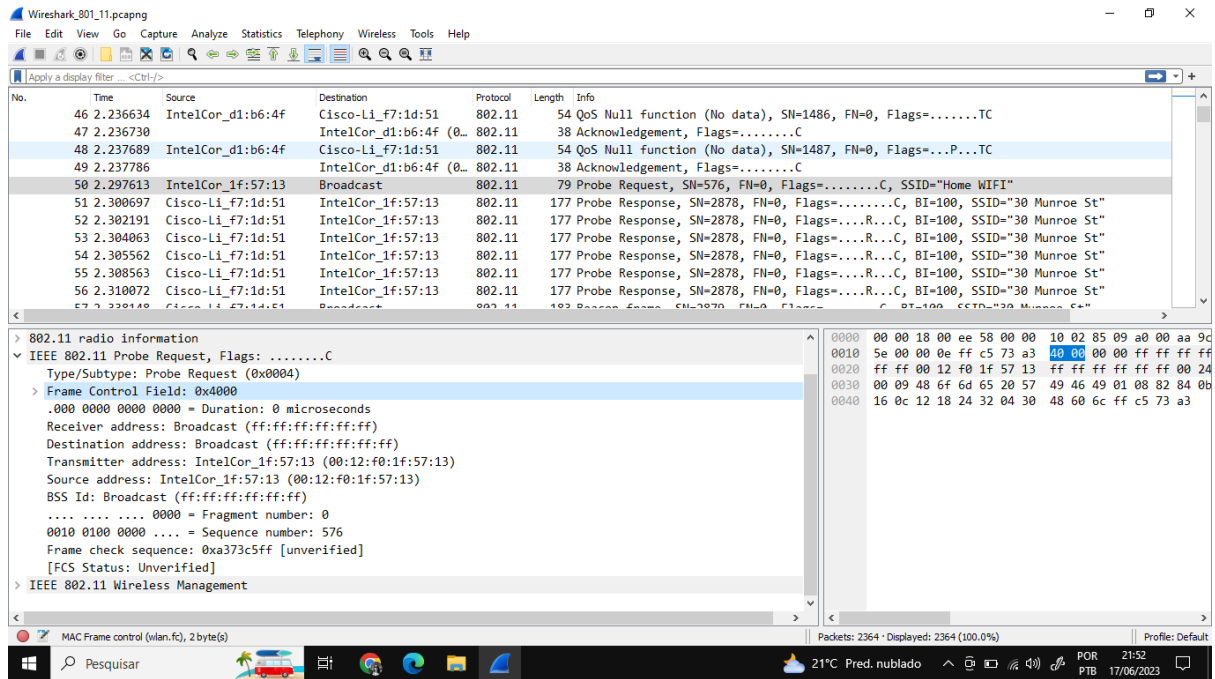
- **Questão 15:** Quais taxas de transmissão o host está disposto a usar? E o AP? Para responder a essa pergunta, você precisará analisar os campos de parâmetros do quadro de gerenciamento de LAN sem fio 802.11.



No quadro de ASSOCIATION REQUEST, as taxas suportadas são anunciadas como **1, 2, 5.5, 11, 6, 9, 12, 18, 24, 32, 48 e 54 Mbps**.

As mesmas taxas são anunciadas na ASSOCIATION RESPONSE.

- **Questão 16:** Quais são os endereços MAC do remetente, destinatário e BSS ID nesses quadros? Qual é o objetivo desses dois tipos de quadros? (Para responder a esta última pergunta, você precisará consultar as referências online citadas anteriormente neste laboratório).



Em **t = 2.297613**, há um PROBE REQUEST enviado com origem **00:12:f0:1f:57:13**, destino **ff:ff:ff:ff:ff:ff** e BSS ID **ff:ff:ff:ff:ff:ff**.

Em **t = 2.300697**, há um PROBE RESPONSE enviado com origem **00:16:b6:f7:1d:51**, destino e BSS ID **00:16:b6:f7:1d:51**.

Um PROBE REQUEST é usado por um host na varredura ativa para encontrar um Ponto de Acesso. Um PROBE RESPONSE é enviado pelo ponto de acesso para o host que enviou a solicitação.