Redes de Computadores

Uma imagem com ClipArt

Descrição gerada automaticamente

Trabalho prático 4

19 de dezembro de 2019

**Grupo nº 6**

Filipa Alves dos Santos (A83631)

Hugo André Coelho Cardoso (A85006)

João da Cunha e Costa (A84775)

Uma imagem com pessoa, parede, homem, interior

Descrição gerada automaticamenteUma imagem com pessoa, céu, homem, parede

Descrição gerada automaticamenteUma imagem com pessoa, parede, vestuário, sorriso

Descrição gerada automaticamente

Mestrado Integrado em Engenharia Informática

Universidade do Minho

**Índice de conteúdos**

**1. Questões e Repostas 3**

1.1. Acesso Rádio 3

1.2. Scanning 3

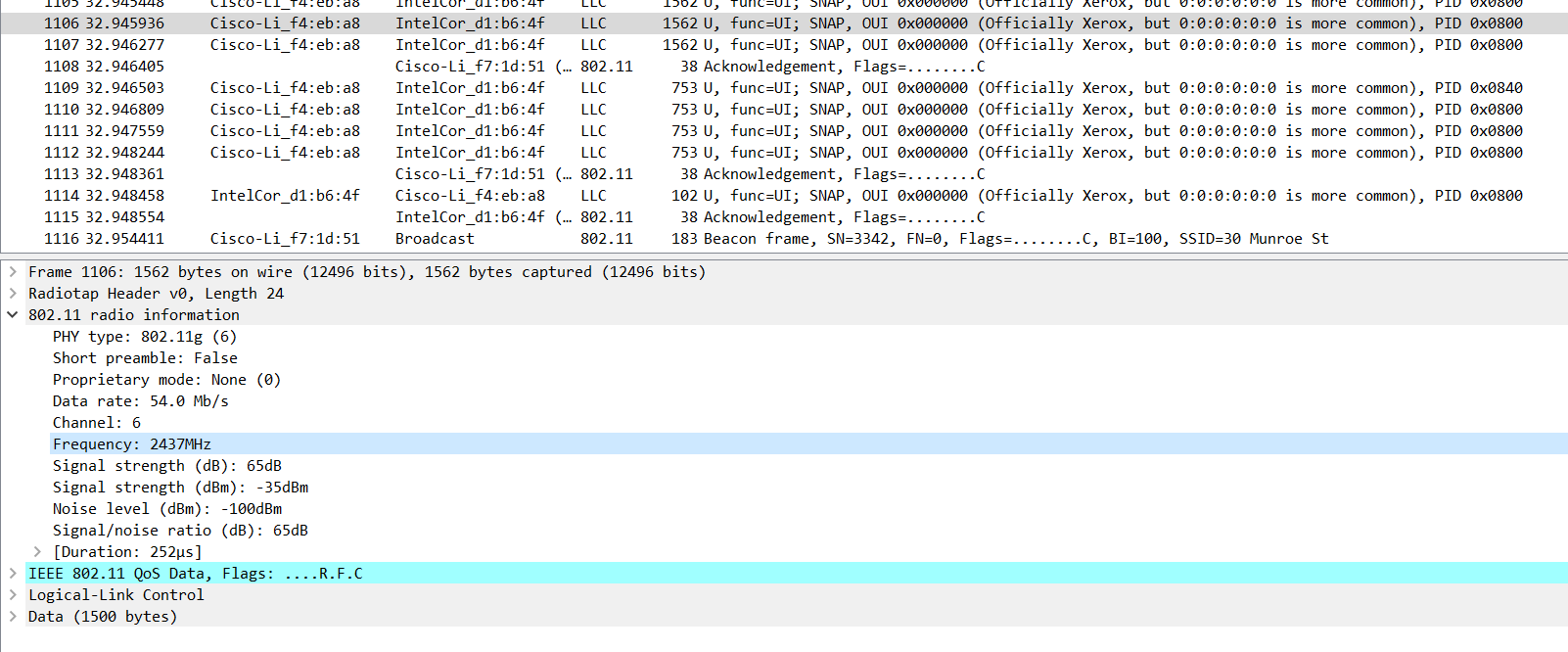
1.3. Processo de Associação 8

1.4. Transferência de Dados 12

**2. Conclusões 15**

1. **Questões e Respostas**

**1.1.** **Acesso Rádio**

**3)** Para a trama correspondente com o número 1YXX (com Y=turno e XX=grupo, e.g., 1101)

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

Frequency: 2437MHz, no Channel: 6.

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

PHY type: 802.11g (6)

**3.3)** 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.

Data Rate: 54.0 Mb/s. Este débito corresponde ao máximo porque a capacidade teórica da versão IEEE 802.11g é 54Mb/s.

**1.2.** **Scanning**

**4)** As tramas beacon permitem efetuar scanning passivo em redes Wi-Fi. Para a captura de tramas disponibilizada, responda às seguintes questões:

**4.4)** Quais são os SSIDs dos dois APs que estão a emitir a maioria das tramas de beacon?

Por observação do ficheiro do Wireshark, SSID = 30 Munroe St e SSID = linksys12 são os SSIDs dos dois APs que estão a emitir a maioria das tramas.

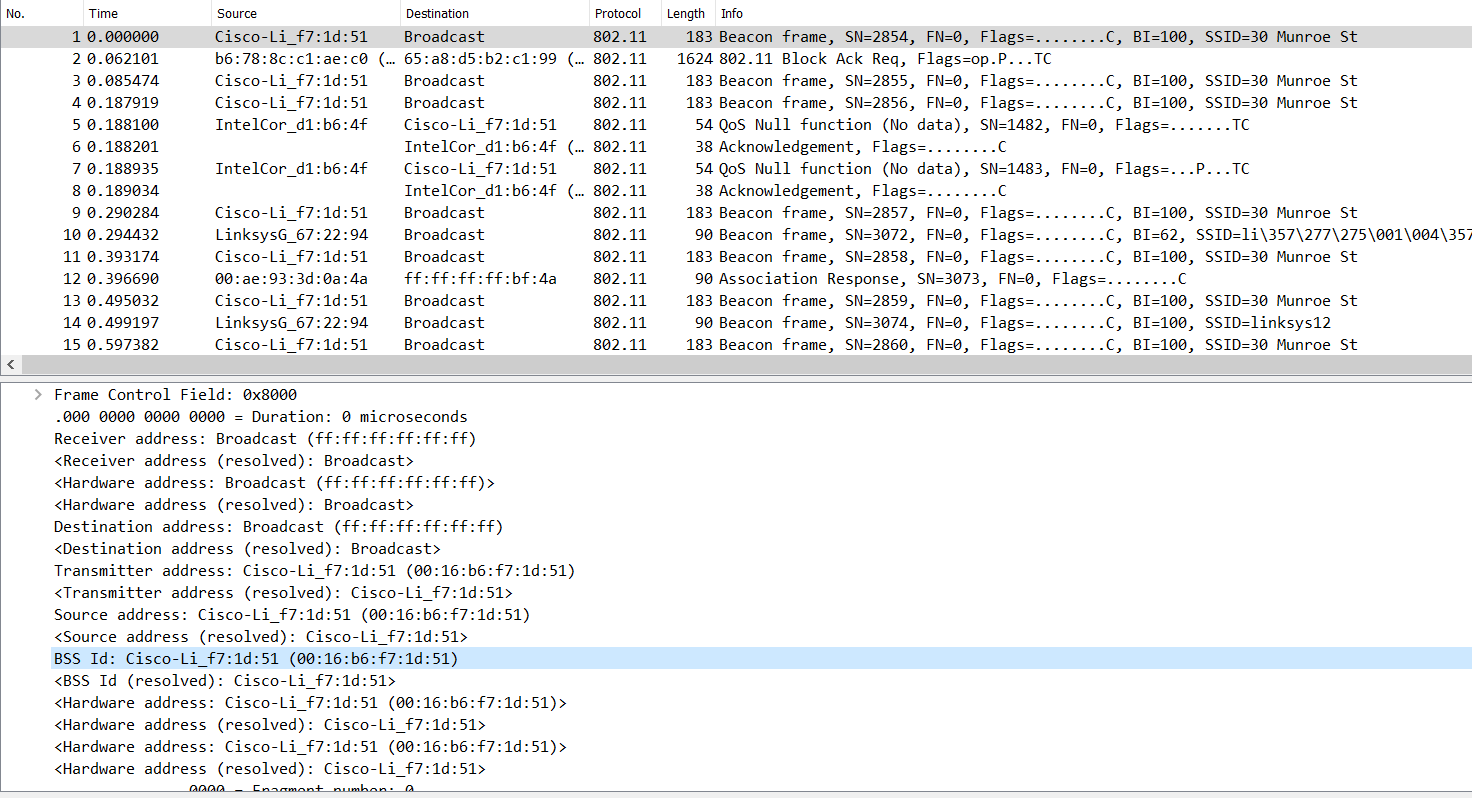
**4.5)** Qual o intervalo de tempo entre a transmissão de tramas beacon para o AP linksys\_ses\_24086? E do AP 30 Munroe St? (Pista: o intervalo está contido na própria trama). Na prática, a periodicidade de tramas beacon é verificada? Tente explicar porquê.

Uma imagem com captura de ecrã

Descrição gerada automaticamente

Na teoria, o “Beacon Interval” para o AP linksys\_ses\_24086 e para o AP 30 Munroe St é, para ambos, 0.120400 [Seconds]. Isto não se verifica na prática porque, se compararmos 2 tramas consecutivas (p.e., a No.1 e 3) concluímos que a diferença do “Time” de chegada de cada é diferente de 0.120400s (0.085474 – 0.000000).

**4.6)** Qual é (em notação hexadecimal) o endereço MAC de origem da trama beacon de 30 Munroe St? Para detalhes sobre a estrutura das tramas 802.11, veja a secção 7 da norma IEEE 802.11 citada no início.



Como se observa pela figura acima, o MAC address de origem é 00:16:b6:f7:1d:51.

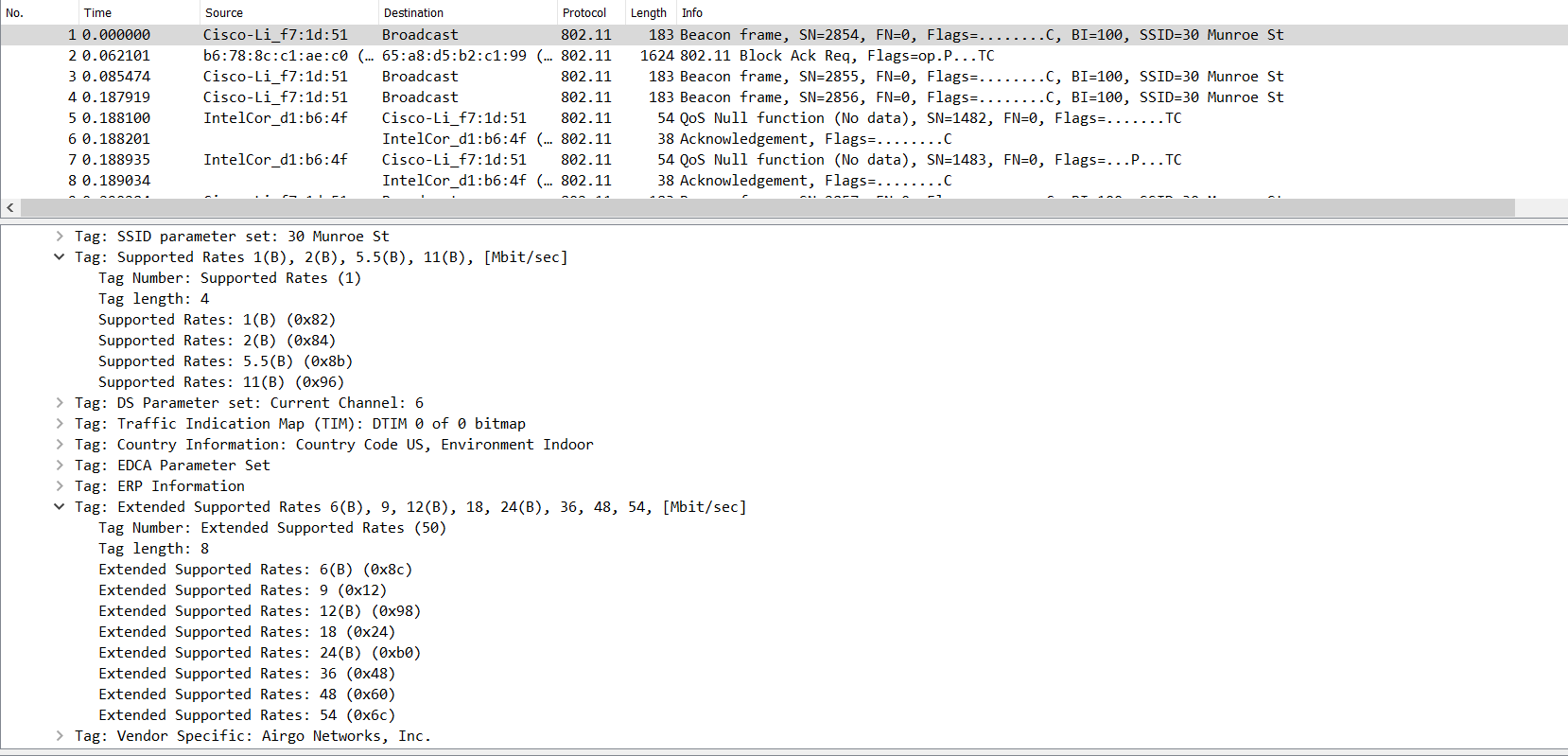
**4.7)** Qual é (em notação hexadecimal) o endereço MAC de destino na trama de 30 Munroe St?

O endereço MAC de destino é ff:ff:ff:ff:ff:ff.

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

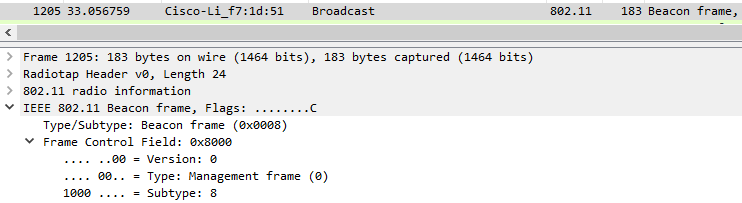
O MAC BSS ID é 00:16:b6:f7:1d:51.

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



O AP suporta 4 data rates: “1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]” e oito extended supported rates: “6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]”.

**4.10)** Selecione uma trama beacon (e.g., a trama 1YXX com Y=turno e XX=grupo, e.g., 1101). 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)?

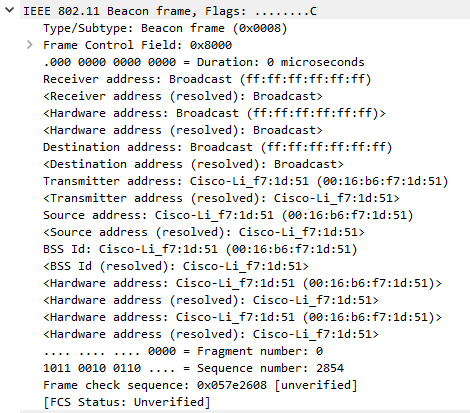


Selecionamos a trama 1205 e podemos verificar que o tipo, de valor 0, é “Management frame” e o subtipo, de valor 1000, é 8. Assim, o valor de tipo/subtipo é “Beacon frame”. A parte do cabeçalho da trama onde estão especificados é a “Frame Control Field”.

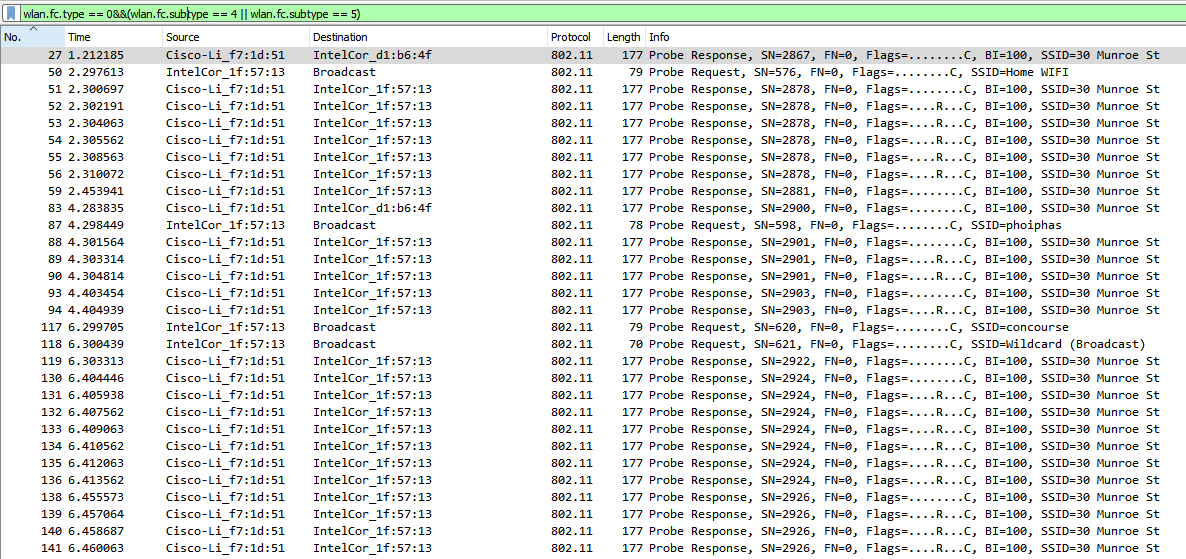
**4.11)** Verifique se está a ser usado o método de deteção de erros CRC e se todas as tramas beacon são recebidas corretamente. Justifique o uso de mecanismos de deteção de erros neste tipo de redes locais.

Após ativar o método de deteção de erros CRC nas definições do Wireshark, verificamos que nem todas as tramas Beacon são bem recebidas, embora a maioria o seja. É necessário utilizar deteção de erros porque o tipo de rede local representa uma Rede Wi-Fi. As redes Wi-Fi são mais suscetíveis a erros o que implica que seja utilizado um campo que verifique se as tramas Beacon são recebidas corretamente.

**4.12)** 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. Para uma descrição detalhada da estrutura da trama 802.11, consulte o anexo ao enunciado.



São usados os endereços “Receiver adress”, “Destination adress”, “Transmitter adress” e “Source address”.

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

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

Probe request:

MAC BSS ID destino – AP / MAC BSS ID origem – host

Probe response:

MAC BSS ID destino – host / MAC BSS ID origem – AP

É pela receção de tramas Beacon (passive scanning) ou pelo varrimento dos vários canais rádio (active scanning) que uma estação (host) pode optar por um AP mais favorável. Neste caso, o host está a usar probe requests/responses para procurar um AP ao qual se ligar.

**4.15)** 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?

Uma imagem com captura de ecrã

Descrição gerada automaticamente

(Vamos usar as tramas 50 e 51 como exemplos de probe request e response)

Probe request:

BSSID: ff:ff:ff:ff:ff:ff (broadcast)

Destino: ff:ff:ff:ff:ff:ff (broadcast)

Origem: 00:12:f0:1f:57:13 (host)

Uma imagem com captura de ecrã

Descrição gerada automaticamente Os probe requests enviam um pedido ao AP para averiguar se podem estabelecer uma conexão ou não.

Probe response:

BSSID: 00:16:b6:f7:1d:51

Destino: 00:12:f0:1f:57:13 (host)

Origem: 00:16:b6:f7:1d:51

O SSID especificado recebe a mensagem e envia uma probe response de resposta ao host, indicando se pode ser estabelecida conexão ou não.

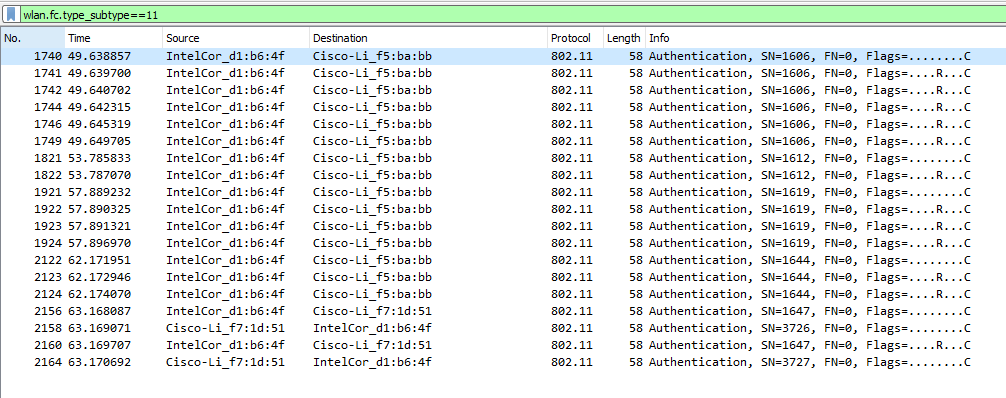
**1.3.** **Processo de Associação**

**6)** Para a sequência de tramas capturada no ficheiro disponibilizado indique:

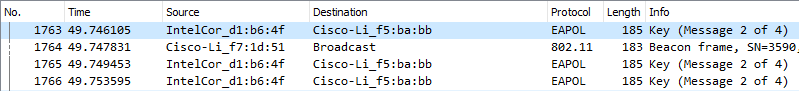
**6.16)** Quais as duas ações realizadas (i.e., tramas enviadas) pelo host no trace imediatamente após t=49 para terminar a associação com o AP 30 Munroe St que estava ativa quando o trace teve início? (Pista: uma é na camada IP e outra na camada de ligação 802.11). Observando a especificação 802.11,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



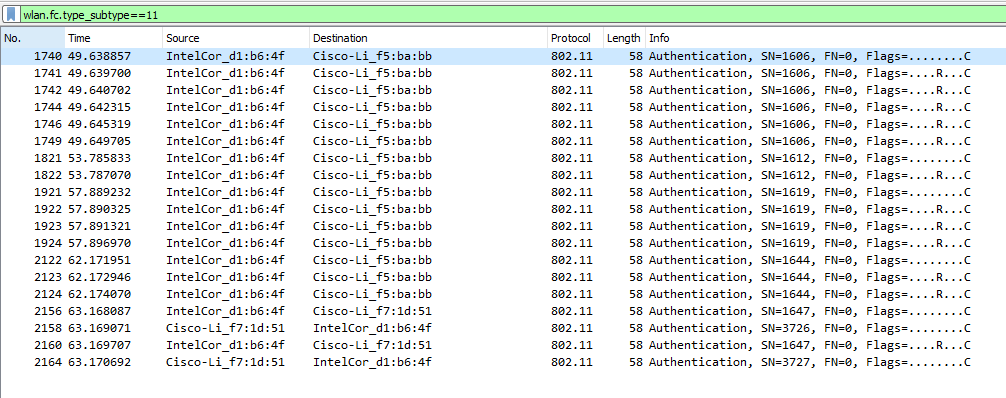
O host envia um pacote DHCP na camada IP para se desassociar do AP 30 Monroe Street e, de seguida, envia uma trama de desautenticação na camada de ligação 802.11 para terminar a ligação ao AP completamente. Segundo a especificação 802.11, seria de esperar também uma probe request enviada pelo host, que não aparece aqui.

**6.17)** 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?

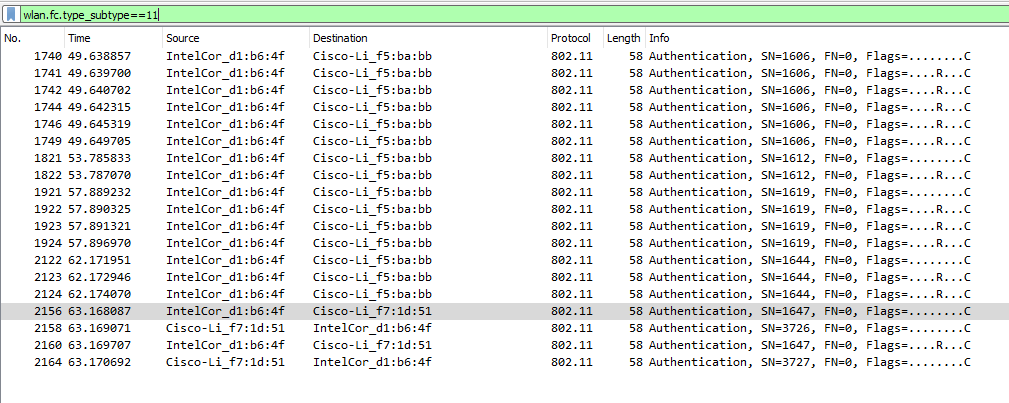
Aplicamos o filtro “wlan.fc.type\_subtype == 11” para filtrar mensagens de autenticação. O host enviou 6 mensagens de autenticação para o AP linksys\_ses\_24086 aproximadamente ao t = 49.

**6.18)** Qual o tipo de autenticação pretendida pelo *host*, aberta ou usando uma chave?

Autenticação com chave, como podemos ver mais abaixo das tramas de autenticação, o host envia a chave ao AP.

**6.19)** Observa-se a resposta de authentication do AP linksys\_ses\_24086 AP no trace?

Não. Como podemos ver no print, o host envia imensos pedidos de autenticação ao AP linksys\_ses\_24086 (endereço MAC Cisco-Li\_f5:ba:bb) mas este nunca envia uma resposta.

**6.20)** 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 um trama authentication do host para o AP 30 Munroe St. e quando aparece a resposta authentication do AP para o host?

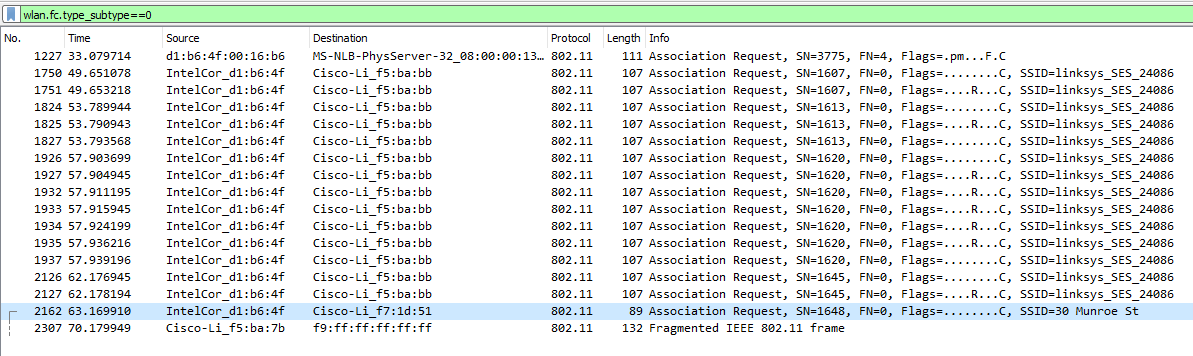
Usamos o filtro “wlan.fc.type\_subtype == 11” para filtrar mensagens de autenticação.

O AP 30 Munroe St. tem o endereço MAC Cisco-Li\_f7:1d:51.

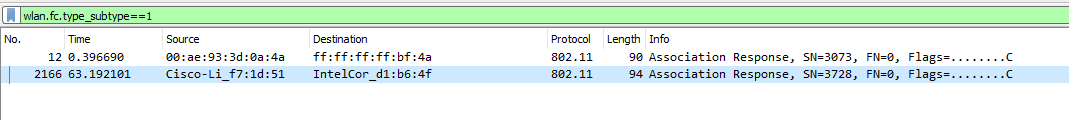
Trama authentication do host para o AP: t = 63.168087

Trama authentication do AP para o host: t = 63.169071

**6.21)** 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 ?

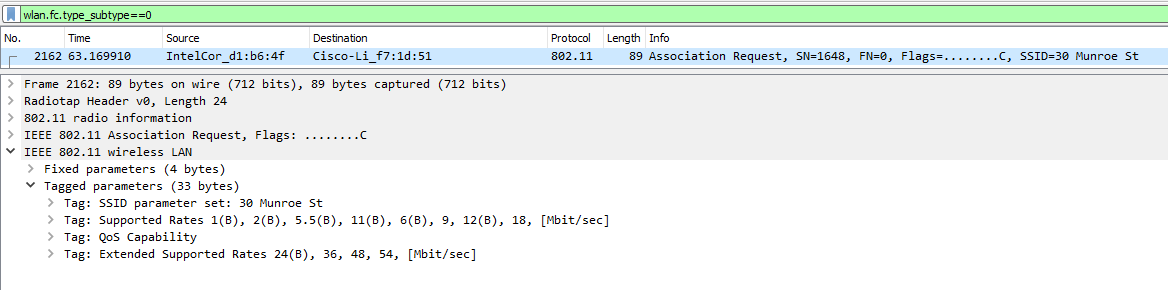


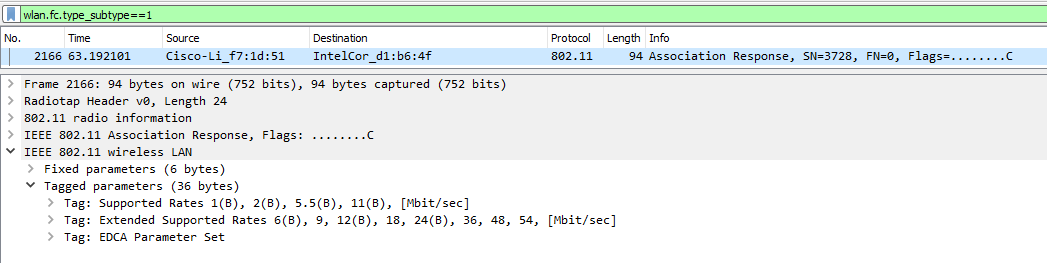
Usamos o filtro “wlan.fc.type\_subtype == 0” para filtrar association requests.

 O association request do host para o AP 30 Munroe St. aparece em t = 63.169910.

Usamos o filtro “wlan.fc.type\_subtype == 1” para filtrar association replies.

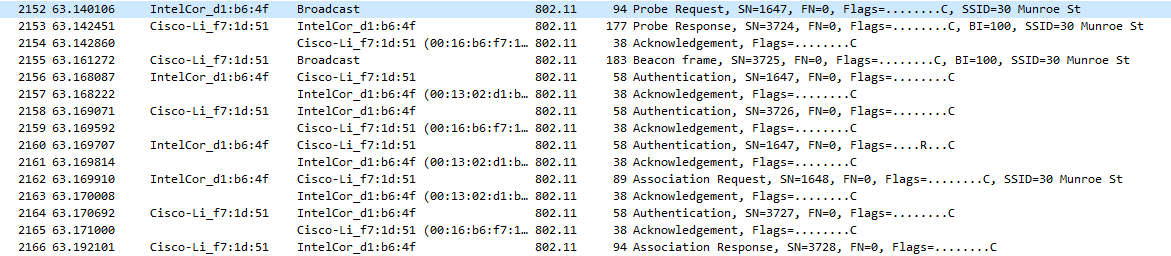
O association reply respetivo é enviado em t = 63.192101.

**6.22)** Que taxas de transmissão o host está disposto a usar? E o AP?

O host está disposto a usar as seguintes taxas de transmissão: 1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18 [Mbit/sec].

O AP está disposto a usar as seguintes taxas de transmissão: 1(B), 2(B), 5.5(B), 11(B) [Mbit/sec].

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



No início do tráfego mostrado no print, o host acabou de desautenticar o AP linksys\_ses\_24086.

Depois, envia uma probe request para obter informações de outro AP, neste caso o 30 Munroe St.. Obtém as informações no probe response enviado pelo mesmo e depois o AP e a STA (host) autenticam-se e associam-se.

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

**STA**

**AP**

Probe request

Probe response

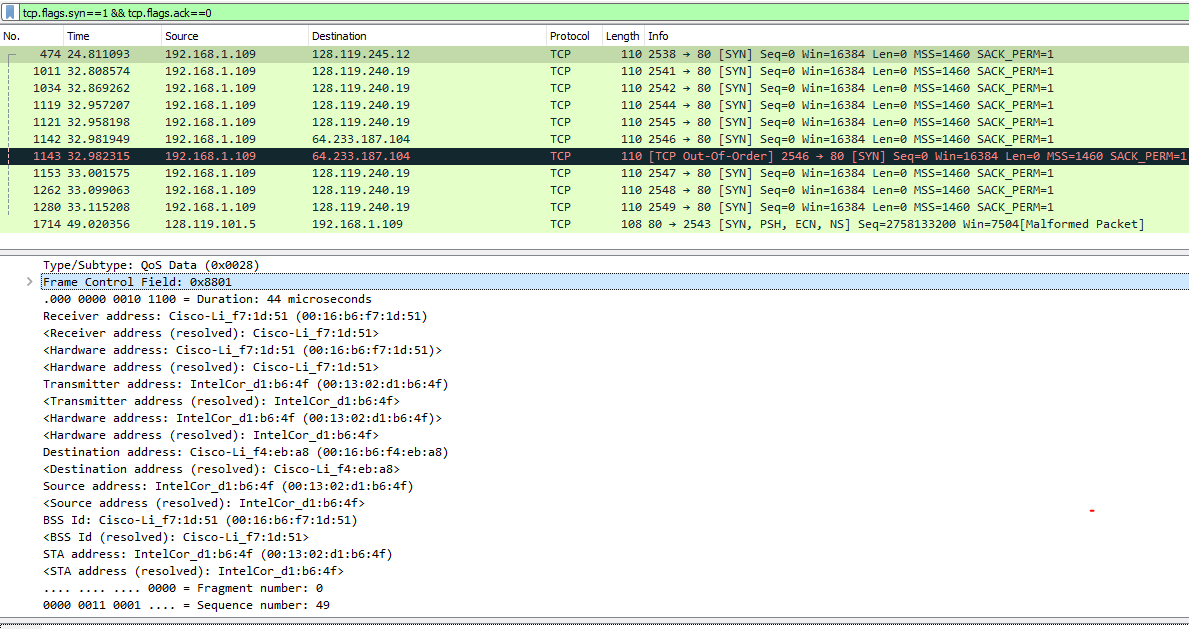
Authentication

Authentication

Association request

Association response

**1.4.** **Transferência de Dados**

**7.25)** 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?

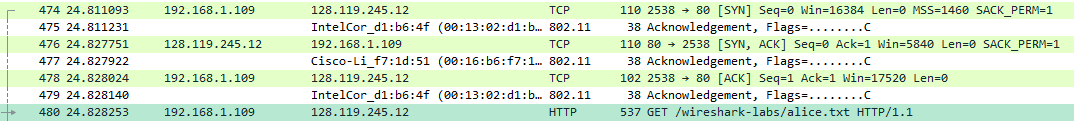
Usamos o filtro “tcp.flags.syn==1 && tcp.flags.ack==0” para filtrar todas as sessões TCP com pacotes SYN.

Os 3 campos MAC são:

Receiver address – 00:16:b6:f7:1d:51

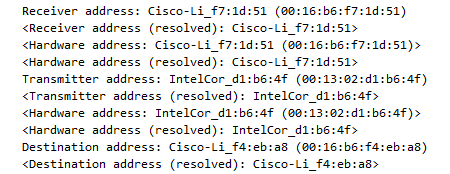
Transmitter address – 00:13:02:d1:b6:4f

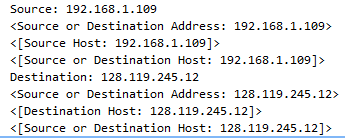
Destination address – 00:16:b6:f4:eb:a8



Como podemos observar neste print, a trama TCP 474 é onde se estabelece a conexão TCP para efetuar o download do alice.txt, pois este aparece mencionado na informação da trama HTTP mais abaixo.

**7.26)** 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?





Endereço MAC do host: 00:13:02:d1:b6:4f

Endereço MAC do AP: 00:16:b6:f7:1d:51

Endereço MAC do router do 1º salto: 00:16:b6:f4:eb:a8

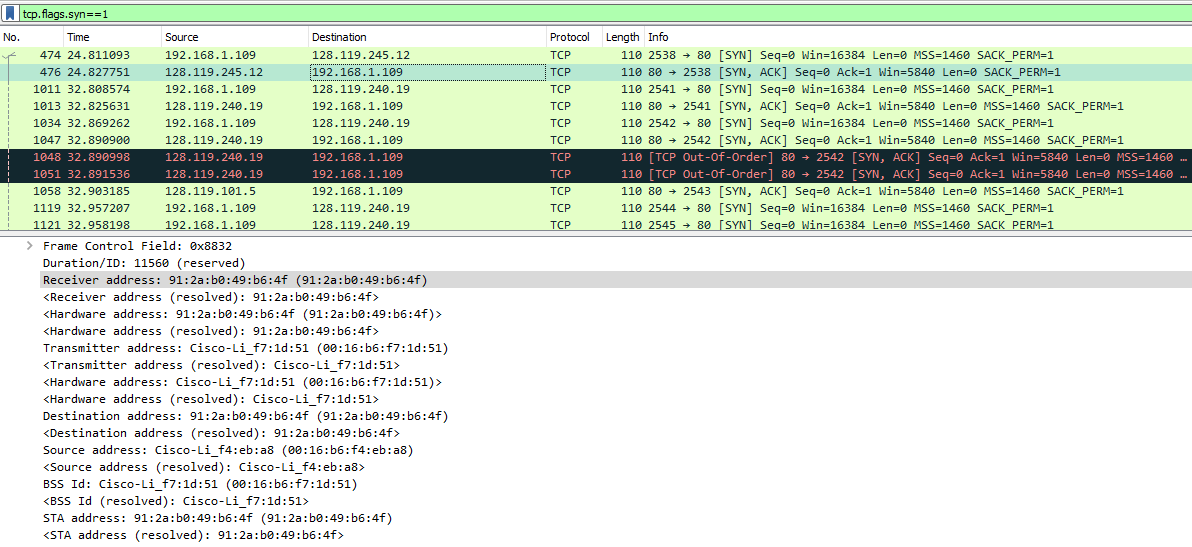
Endereço IP do host: 192.168.1.109

Endereço IP de destino: 128.119.245.12

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



Como podemos observar, o pacote é recebido no endereço IP de destino, que depois envia uma resposta de acknowledgement ao servidor. Logo, corresponde ao AP.

**7.28)** Encontre agora a trama 802.11 que contém o segmento SYNACK para esta sessão TCP. Quais são 6 os três campos dos endereços MAC na trama 802.11?

Usamos o filtro “tcp.flags.syn==1” para selecionar tanto pacotes SYN como SYN/ACK.

Os 3 campos MAC são:

Receiver address – 91:2a:b0:49:b6:4f

Transmitter address – 00:16:b6:f7:1d:51

Destination address – 91:2a:b0:49:b6:4f

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

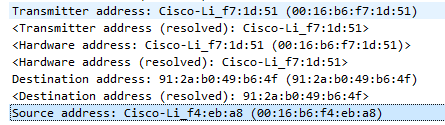
Como se pode observar no print da pergunta anterior:

Endereço MAC do host: 91:2a:b0:49:b6:4f

Endereço MAC do AP: 00:16:b6:f7:1d:51

Endereço MAC do router do primeiro salto: 91:2a:b0:49:b6:4f

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



O endereço MAC de origem na trama (00:16:b6:f4:eb:a8) não corresponde ao IP do dispositivo que enviou o segmento TCP encapsulado neste programa, pois esse tem um endereço MAC diferente (00:16:b6:f7:1d:51).

1. **Conclusões**

Em conclusão, após a realização deste trabalho prático, verificamos a consolidação dos conceitos aprendidos nas aulas teóricas e sentimos que atingimos os objetivos pretendidos para o mesmo.

De forma resumida, apresenta-se de seguida os resultados mais relevantes da aprendizagem decorrente deste trabalho:

- Informação das tramas ao nível físico (radio information)

- Scanning passivo em redes Wi-Fi envolvendo tramas beacon

- Scanning ativo em redes Wi-Fi envolvendo tramas probe request e probe response

- Processo de associação nas redes IEEE 802.11(fase antes do envia de dados), bem como o processo de autenticação usado.

- Mecanismos de detenção de erros em redes locais

- Transferência de dados entre a estação e o AP

O grupo considera que foi bem-sucedido no trabalho e que foi uma experiência positiva para o desenvolvimento e consolidação de conhecimentos da matéria de Redes de Computadores.