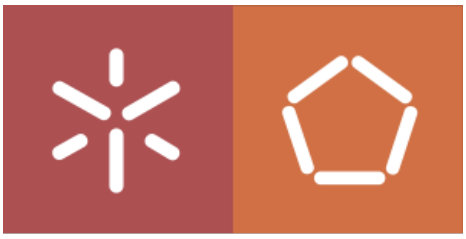


Universidade do Minho
Escola de Engenharia

Redes de Computadores TP3

Novembro de 2019


Ana Margarida Campos


Ana Catarina Gil


Tânia Rocha

1 Acesso Rádio

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

A frequência a que o espetro está a operar a rede sem fios é 2437 MHz. Como observado na fig.1, o canal que corresponde a esta mesma frequência é o canal 6.

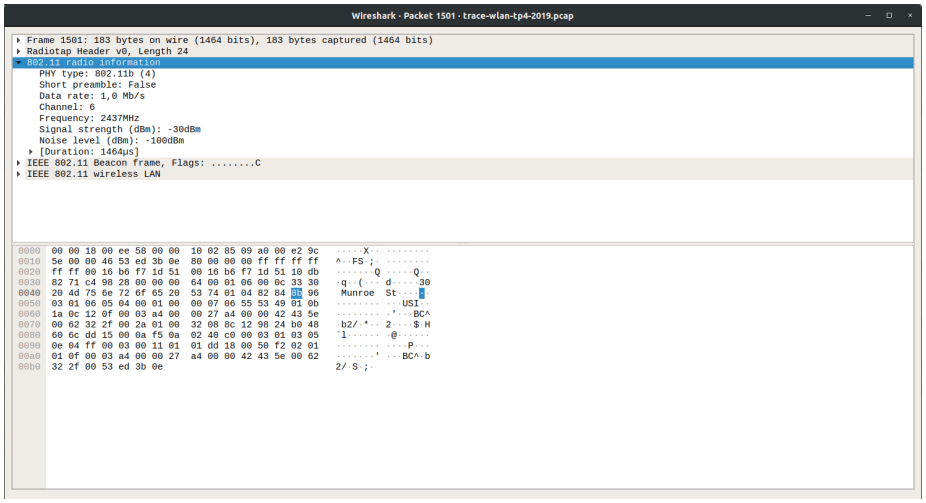


Figure 1: Trama correspondente ao número 1501.

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

A versão da norma IEEE 802.11 que está a ser utilizada é 802.11b.(Fig.1)

1.2.1 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.

Também observável na Fig.1, o débito enviado pela trama escolhida é 1.0 Mb/s, que corresponde a 8Mbps. Este valor não corresponde ao débito máximo, visto que o máximo é 11Mbps, uma vez que a versão utilizada é 802.11b.

2 Scanning

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

Os SSID dos dois APs são os seguintes:
SSID = 30 Munroe St
SSID = linksys_SES_24086

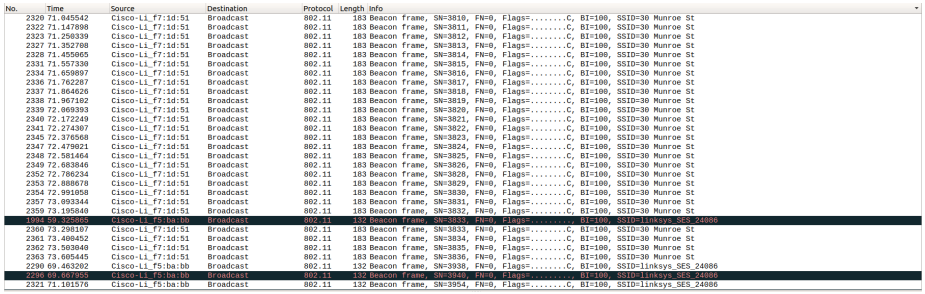


Figure 2: Trama de beacon

2.2 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.

Em ambas as tramas beacon o intervalo de tempo é 0.102400 segundos. A periocidade é apenas verificada para o AP 30 Munroe St.

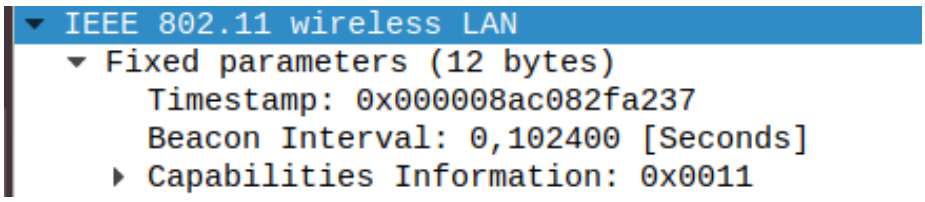


Figure 3: Intervalo da trama Beacon

2.3 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

O MAC address de origem é 00:16:b6:f7:1d:51.(Fig.4)

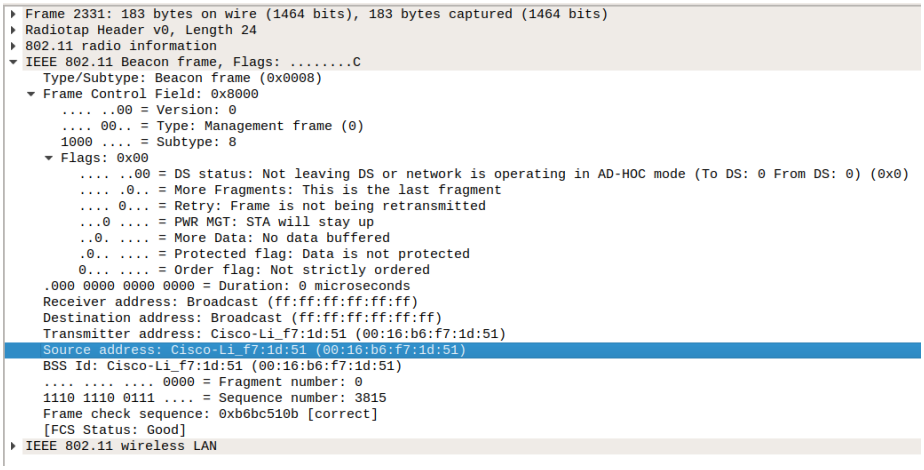


Figure 4: Endereço Mac de Origem

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

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

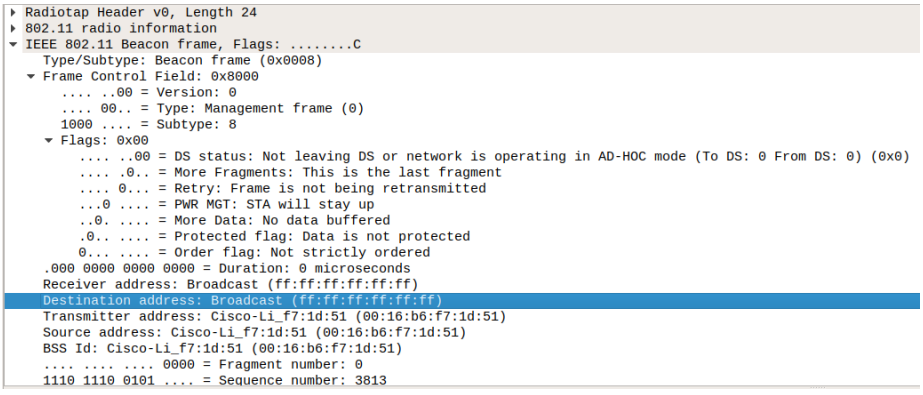


Figure 5: Endereço Mac de Destino

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

O MAC address BSS ID é 00:16:p6:f7:1d:51.

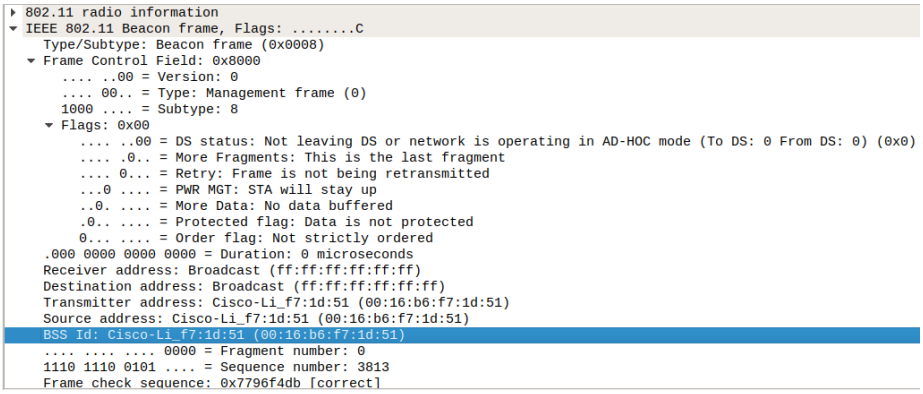
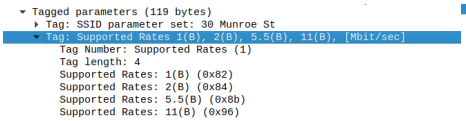
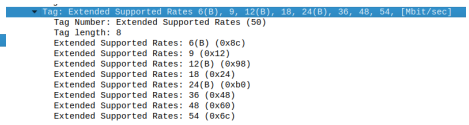


Figure 6: Endereço Mac BSS ID da trama beacon 30 Munroe St

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



Data Rates



Extended Supported Rates

2.7 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)?

O valor do tipo é 0. O valor do subtipo é 8. A parte do cabeçalho onde estão especificados é na Frame Control File.

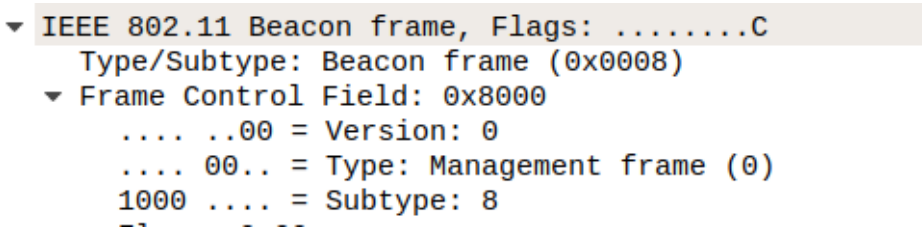


Figure 7: Tipos e subtipos da trama

2.8 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.

Sim, está a ser utilizado em todas, mas como podemos observar nem todas estão a ser corretas.

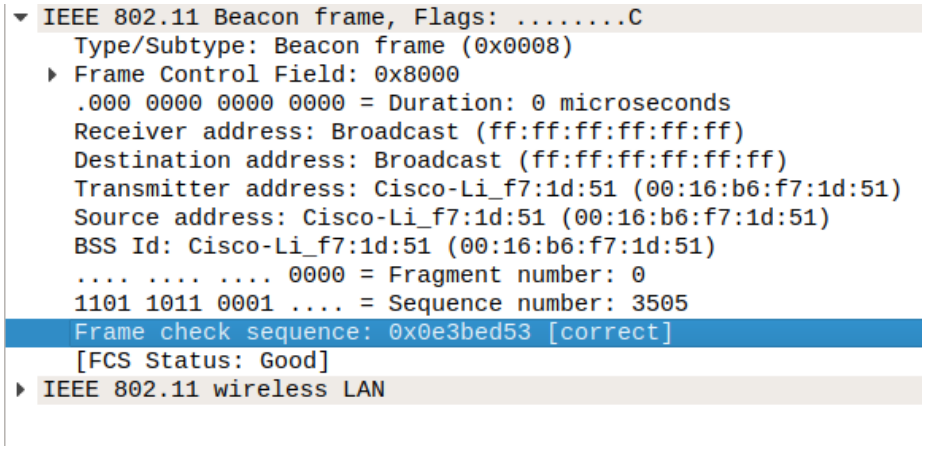


Figure 8: Frame Check Sequence [correct]

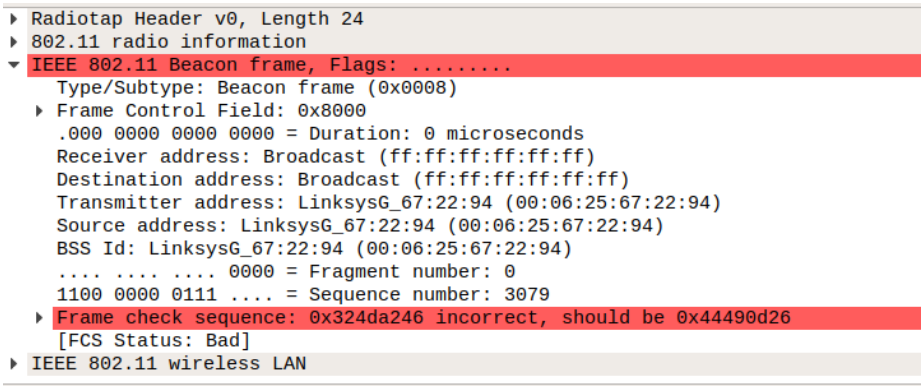


Figure 9: Frame Check Sequence [incorrect]

2.9 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.

Receiver Address : ff:ff:ff:ff:ff:ff
Destination Address : ff:ff:ff:ff:ff:ff
Transmitter Address : 00:16:b6:f7:1d:51
Source Address : 00:16:b6:f7:1d:51

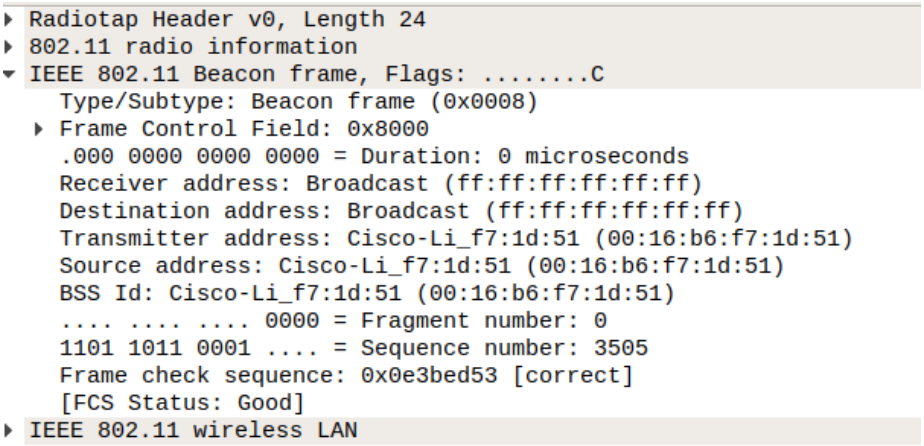


Figure 10: Registos MAC

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

Como é observácel na sefuinte figura. Para conseguirmos obter simultaneamente o Probe Response e o Probe Request tivemos que filtrar através dos seu endereços correspondentes. 0x0004 para o Probe Request e 0x0005 para o Probe Response. O Filtro utilizado foi 'wlan.fc.type_subtype == 0x0004 or wlan.fc.type_subtype == 0x0005' , onde o 'or' foi o que permitiu observa-los simultaneamente.

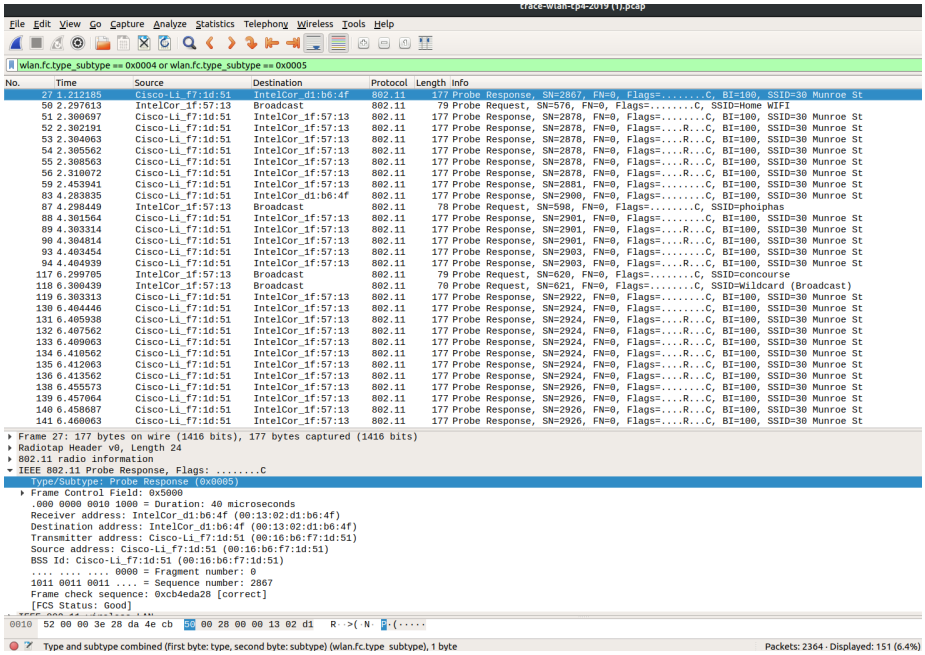


Figure 11: Probe Request e Probe Response

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

O obsetivo da Trama Probe Request é obter informações de uma outra estação. Esta trama é útil para um STA determinar quais os APs que estão dentro do seu alcance rádio. Por outro lado, o objetivo da trama Probe Response é de fornecer a resposta contendo informações sobre as taxas de dados suportadas. Para cada uma das tramas os endereços Destinations e Sorce são os seguintes:
Probe Request:
Source MAC Address : 00.16:6b:f7:id:51

Destination MAC Adress : 00:12:f0:1f:57:13
Probe Response:
Source MAC Address : 00:12:f0:1f:57:13
Destination MAC Adress : ff:ff:ff:ff:ff:ff

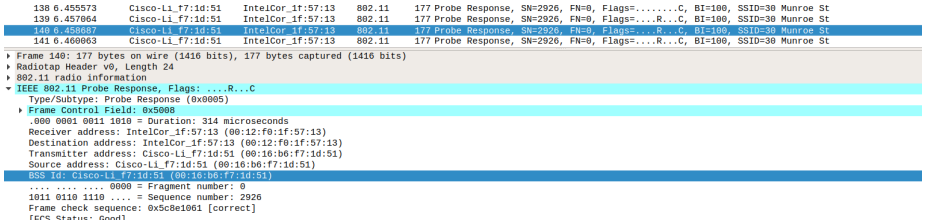


Figure 12: MAC BSS ID de Destino da trama Probe Response

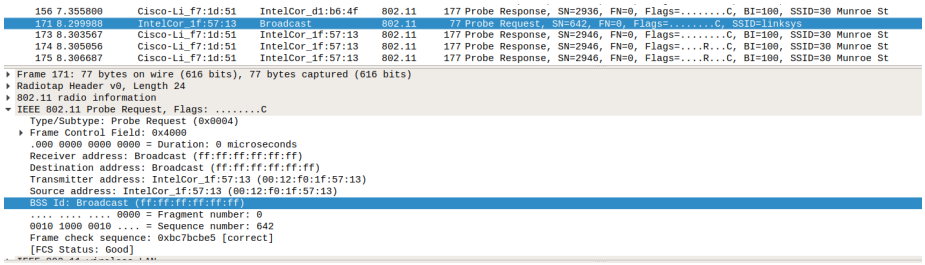


Figure 13: MAC BSS ID de Destino da trama Probe Response

2.12 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?

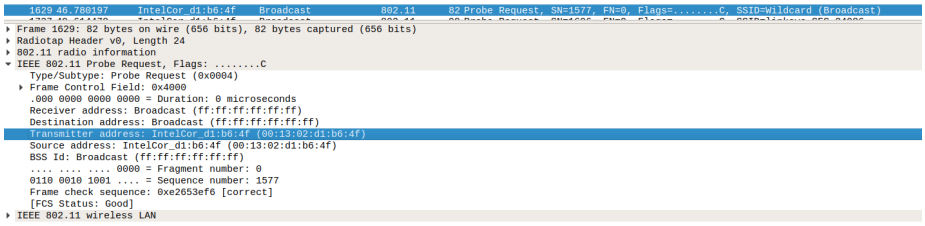


Figure 14: Endereço de Probe Request

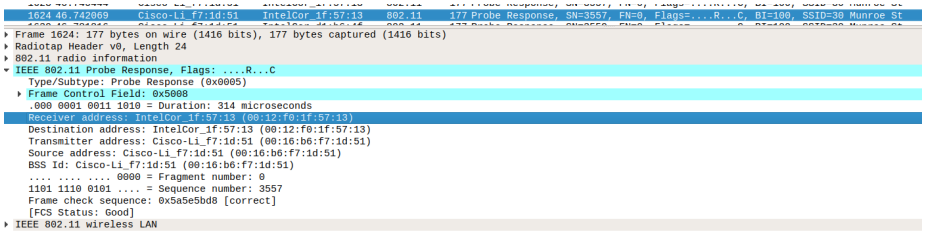


Figure 15: Endereço de Probe Response

3 Processo de Associação

3.1 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 ações realizadas ocorrem quando t=49.583615,em que o DHCP release é enviado pelo Host para o DHCP server, cujo IP é 192.168.1.109, e quando t=49.609617, o Host envia uma frame de DEAUTHENTIFICATION. Era também esperado que estivesse presente a trama de DISASSOCIATION.

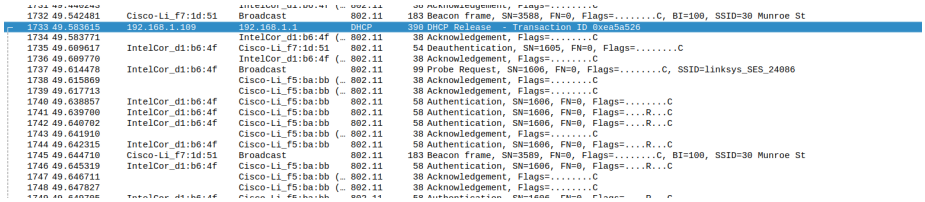


Figure 16: Tramas em que t=49

3.2 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?

Existem 15 mensagens de autenticação enviadas.

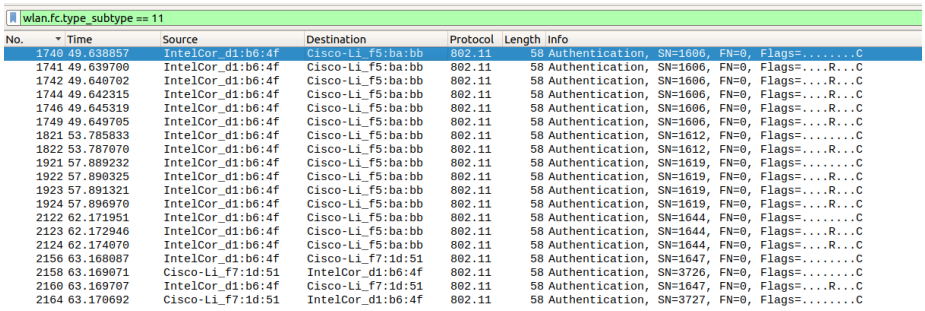


Figure 17: Número de mensagens enviadas para o AP linksys_ses_24086

3.3 Qual o tipo de autenticação pretendida pelo host, aberta ou usando uma chave?

O tipo de autenticação pretendida é aberta.

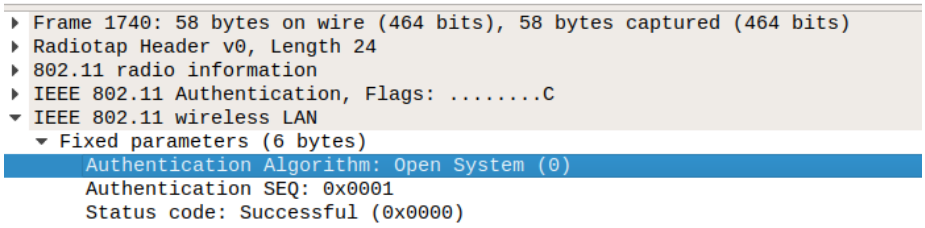


Figure 18: Autenticação aberta

3.4 Observa-se a resposta de authentication do AP linksys_ses_24086 AP no trace?

Não se observa resposta de autenticação.

3.5 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?

Em t= 63.168087 aparece a trama de autenticação. Para a resposta, t=63.161272.

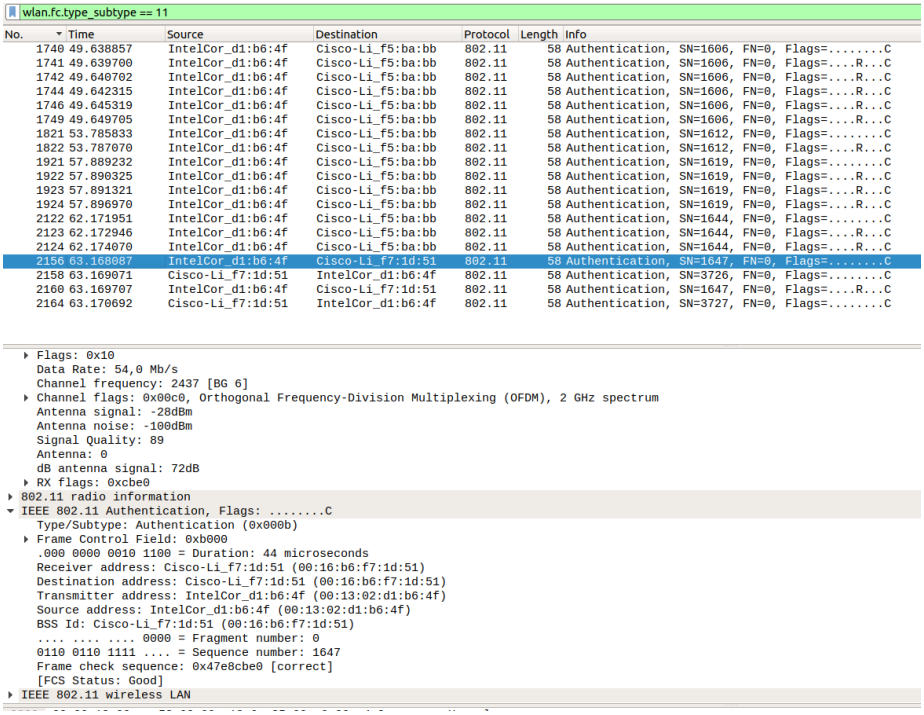


Figure 19: Intervalo em que uma trama authetification aparece

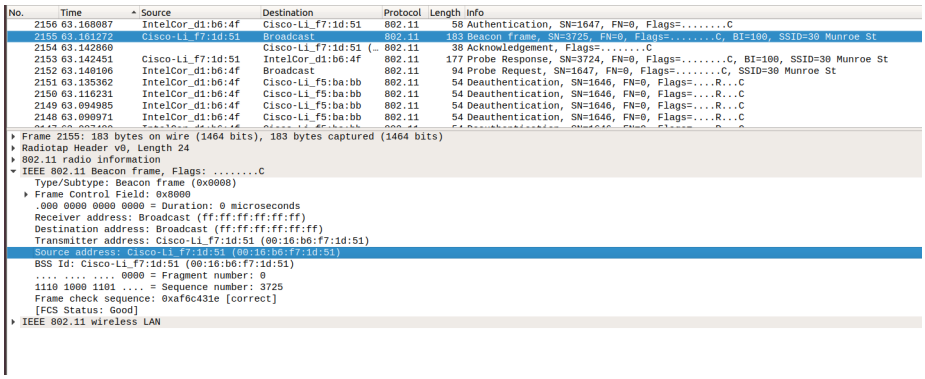


Figure 20: Intervalo em que uma trama de resposta aparece

3.6 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 Que taxas de transmissão o host está disposto a usar? E o AP? Munroe St? Quando é enviado o correspondente associate reply ?

O host enviou um ASSOCIATION REQUEST para Munroe St a t = 63.19910 e este repondeu a t=63.192101.

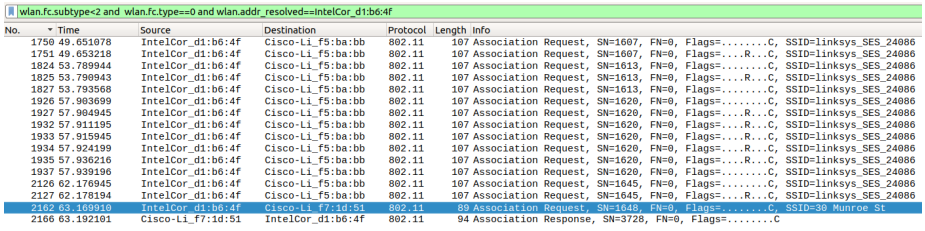


Figure 21: Taxas de transmissão

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

1, 2, 5.5, 11, 6, 9, 12, 18 [Mbit/sec].

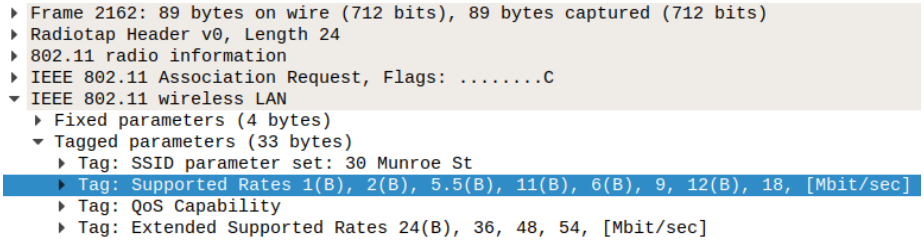


Figure 22: Taxas de transmissão

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

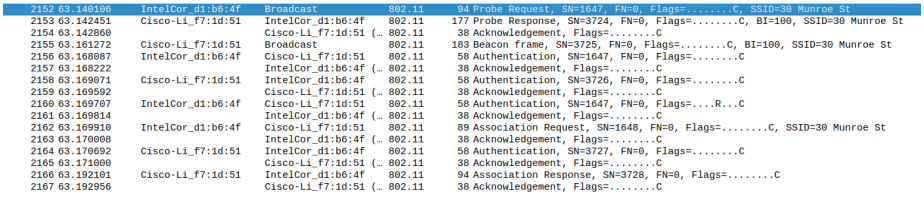


Figure 23: sequência de tramas

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

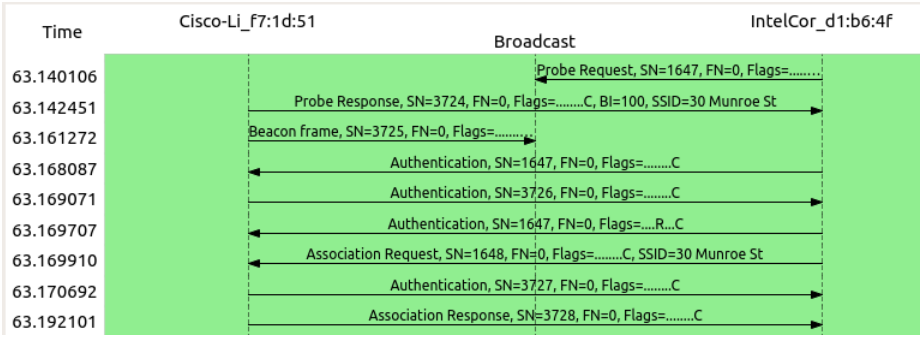


Figure 24: Diagrama de Sequência

4 Transferência de Dados

4.1 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?

Cisco-li: f7:1d:51(00:16:b6:f7:1d:51)
Source Address IntelCor: d1:b6:4f(00:13:02:d1:b6:4f)
Destination Cisco-Li: f4:eb:a8(00:16:b6:f4:eb:a8)

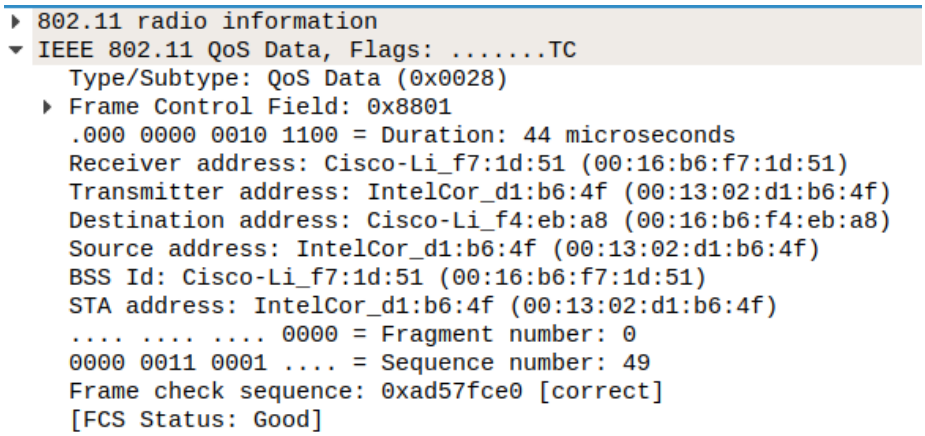


Figure 25: Endereços MAC

4.2 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?

Host: IntelCor d1:b6:4f (00:13:02:d1:b6:4f)
AP: - Cisco-Li f4:eb:a8 (00:16:b6:f4:eb:a8)
1º salto: IntelCor d1:b6:4f (00:13:02:d1:b6:4f)
IP de Source: 192.168.1.109
IP de destino: 128.119.245.12

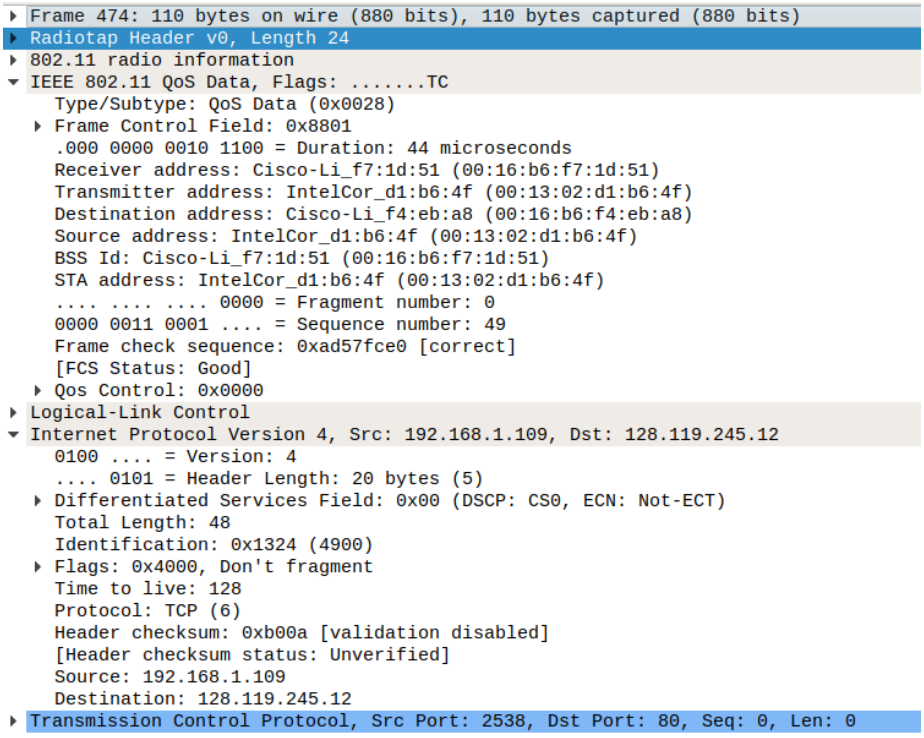


Figure 26: Endereços e IP

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

Este endereço IP corresponde a um AP, visto que tem um BSS Id.

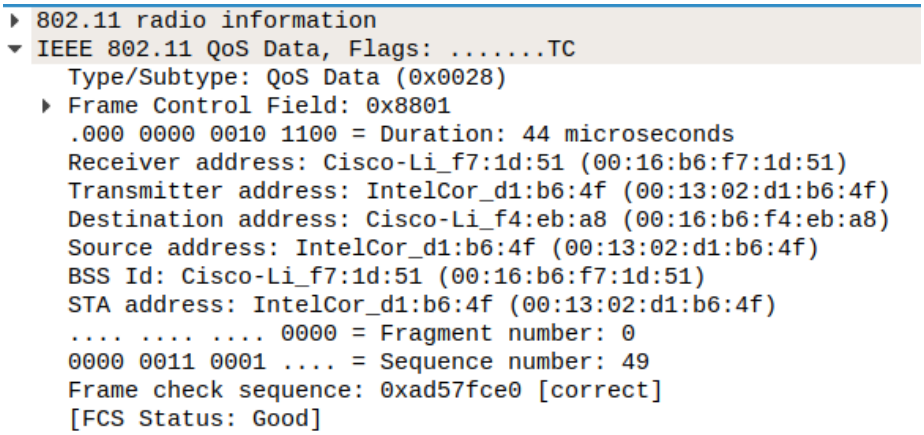


Figure 27: Endereço IP de destino corresponde ao host

4.4 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?

Como é observácel na figura seguinte, os endereços são:
BSS Id: Cisco-Li f7:1d:51 (00:16:b6:f7:1d:51)
Destination: 91:2a:b0:4:b6:4f
Source: Cisco-Li f4:eb:a8 (00:16:b6:f4:eb:a8)

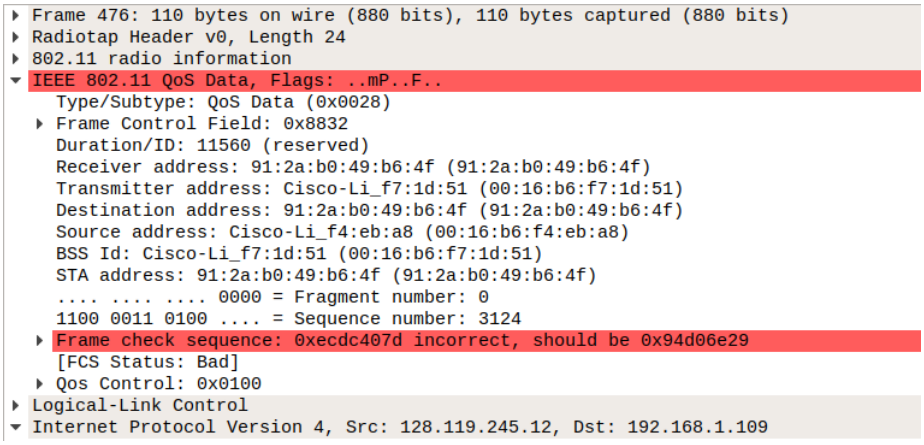


Figure 28: Trama 802.11 que contém o segmento SYNACK para esta sessão TCP

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

Host: STA (91:2a:b0:19:b6:4f)
Source Address: Cisco-Li f4:eb:a8 (00:16:b6:f4:eb:a8)
1º salto: Cisco-Li1 f7:1d:51 (00:16:b6:f7:1d:51).

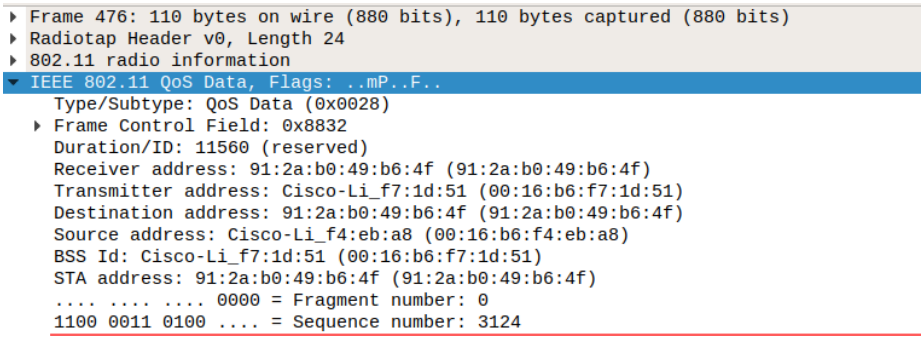


Figure 29: Endereço MAC

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

O MAC address na trama não corresponde ao endereco IP do dispositivo que enviou o segmento tcp encapsulado no datagrama, pois o endereço IP TCP SYNACK é 128.119.245.12. No entanto, o endereço IP de destino é 192.168.1.109.

5 Conclusão

Com a realização deste trabalho foi nos dada a oportunidade de desenvolver capacidades de interpretação sobre o protocolo IEEE 802.11. Isto deu-se através da análise no wireshark de um ficheiro fornecido pelos docentes com uma listagem de exercicios e de apontamentos sobre este mesmo assunto.
Foram-nos fornecidos exercicios sobre vários tópicos que nos permitiram aprofundar o conhecimento sobre os mesmos. Estes tópicos foram acesso rápido, scanning, processo de associação e transferência de dados.
Assim, podemos afirmar que este trabalho nos permitiu ter uma conhecimento mais abrangente sobre esta matéria, que nos pode vir a ser útil futuramente.