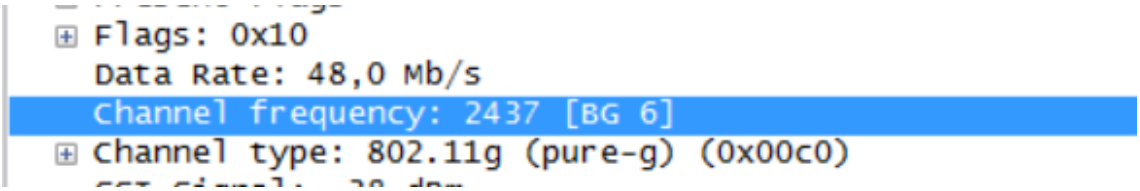
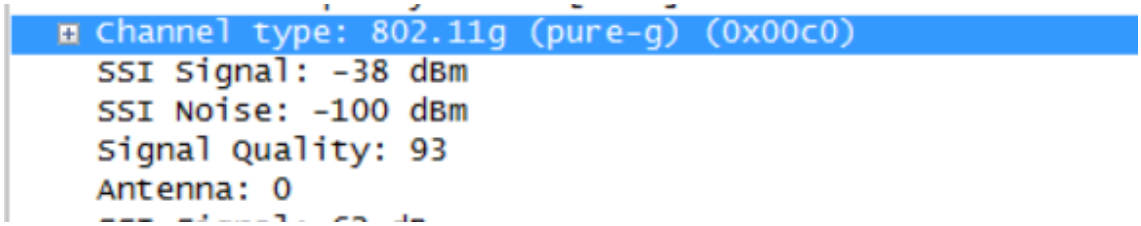
Questões e Respostas

1. Seleccione uma das tramas e identifique em que frequência do espectro está a operar a rede sem fios. Tente identificar a que canal corresponde essa frequência (sugestão: ver norma IEEE 802.11).



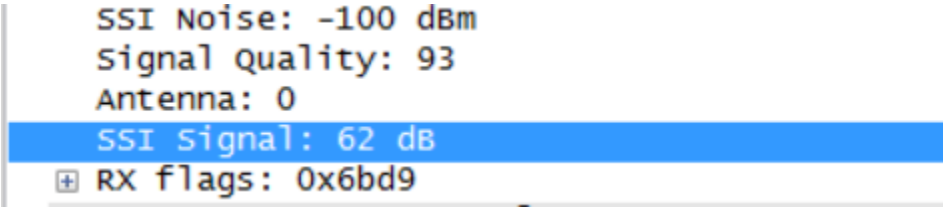
A trama selecionada foi t=24.828s onde host faz um pedido http, como podemos ver a frequência é 2437 e esta no canal 6.

2. Qual o tipo do canal que está a ser usado para a comunicação rádio? Qual o débito a que foi enviada a trama escolhida.



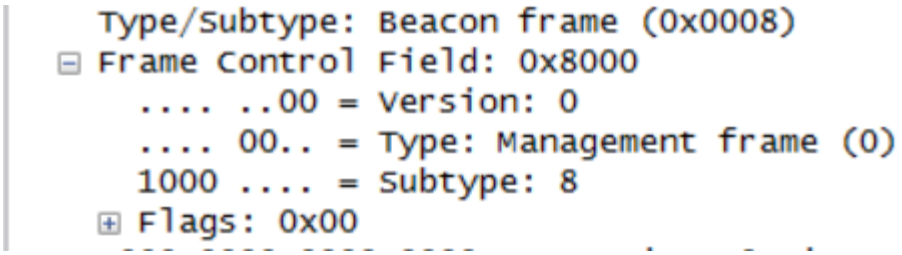
O tipo de canal para a comunicação rádio é 802.11g,

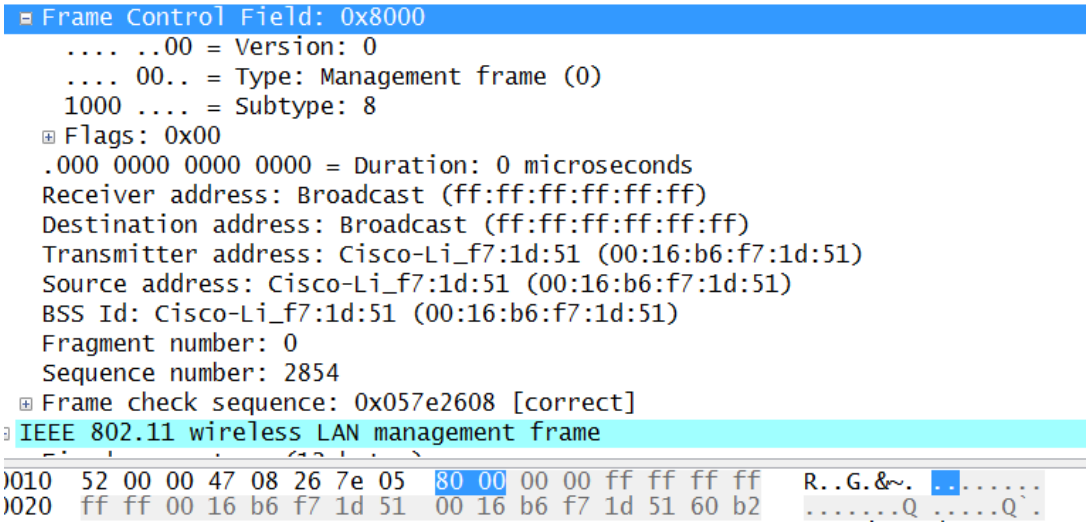
3. Indique qual o índice de qualidade do sinal.



O índice de qualidade do sinal é 93.

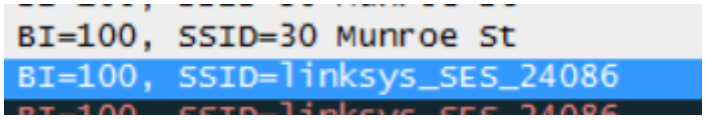
4. Qual o tipo de uma trama beacon? Indique quais os seus identificadores de tipo e subtipo. Em que parte da trama estão especificados?

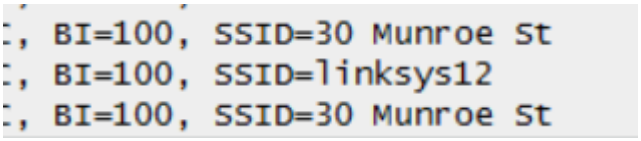


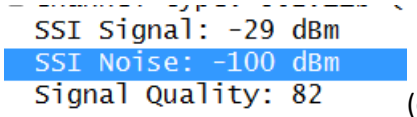


Uma trama beacon é uma “Management Frame”, identificador de tipo 0 e de subtipo 8.

5. Identifique os SSIDs dos APs (Access Points) que estão a operar na rede e diga qual tende a proporcionar a melhor qualidade de sinal?





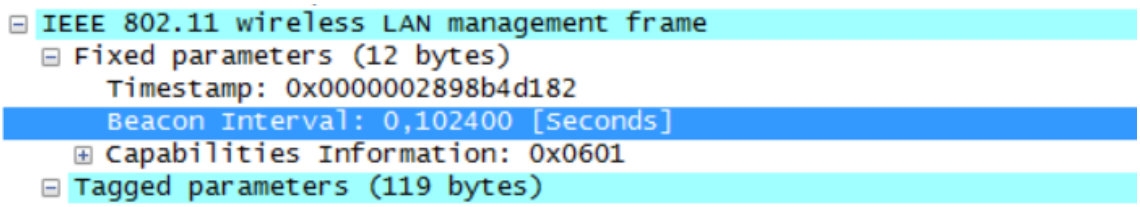


(qualidade do sinal de 30MunroeST)

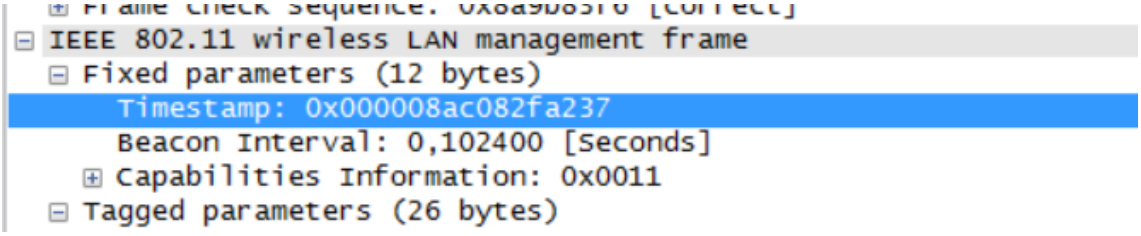
Vamos ter 3 SSIDs, “30 Munroe St”, “linksys_ses_24086” e “linksys12”. O que tende a proporcionar melhor qualidade de sinal é o “30 Munroe ST”.

6. Para dois dos APs identificados, indique quais são os intervalos de tempo previstos entre as transmissões de tramas beacon? (nota: este valor é anunciado na própria trama beacon).

"30 Muneroe St"



"Linkys12"



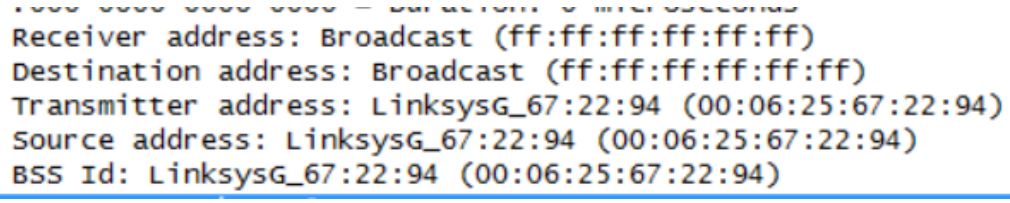
Os intervalos de tempos previstos entre as transmissões de tramas beacon é 0,1024 segundos.

7. Na prática, a periodicidade de tramas beacon é verificada? Tente explicar porquê?

No modo infraestrutura, os relógios de todas as estações devem estar sincronizados com o relógio do AP. Para tal o AP transmite tramas periódicas (tipo Beacon), que contêm o valor do relógio do AP, no momento exato da transmissão. As estações recetoras verificam o valor do relógio no momento de receção e corrigem o seu, de maneira a manter a sincronização com o relógio do AP. No valor do relógio do AP, já está incluído o tempo de propagação da trama para se manter uma sincronização exata entre o AP e a estação.

8. Identifique e registe todos os endereços MAC usados nas tramas beacon enviadas pelos APs. Recorde que fonte, destino e BSS ID são endereços contidos no cabeçalho das tramas 802.11. Para uma descrição detalhada da estrutura da trama 802.11, veja a secção 7 da norma IEEE 802.11 (citada acima).

Linksys12



Mac: 00:06:25:67:22:94

30 Muneroe St

```
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)
```

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

Linksys_SES_24086

```
Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
Transmitter address: Cisco-Li_f5:ba:bb (00:18:39:f5:ba:bb)
Source address: Cisco-Li_f5:ba:bb (00:18:39:f5:ba:bb)
BSS Id: Cisco-Li_f5:ba:bb (00:18:39:f5:ba:bb)
```

Mac:00:18:39:f5:ba:bb

9. As tramas beacon anunciam que o AP pode suportar vários débitos de dados base assim como vários “extended supported rates” adicionais. Quais são esses débitos?

```
⊞ Flags: 0x10
  Data Rate: 1,0 Mb/s
  Channel frequency: 2437 [BG 6]
```

```
⊟ 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)
```

Os débitos da trama beacon é 1 mb/s.

10. Localize a trama 802.11 que contenha o segmento TCP SYN para a primeira conexão TCP (que descarrega alice.txt). Quais são os três campos de endereço contidos na trama 802.11? Qual o endereço MAC correspondente ao host ligado sem fios? E ao AP? E ao router de acesso (primeiro salto)? Qual é o endereço IP do host sem fios que envia este segmento TCP? E o endereço IP destino do mesmo? A que sistema corresponde esse endereço IP destino?

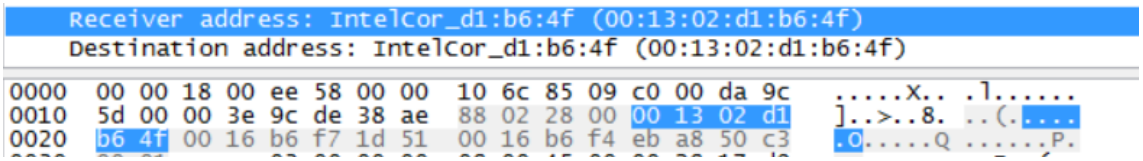
```
.000 0000 0010 1100 = Duration: 44 microseconds
Receiver address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
Transmitter address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
Source address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
Destination address: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)
Fragment number: 0
```

Source	Destination
192.168.1.109	128.119.245.12

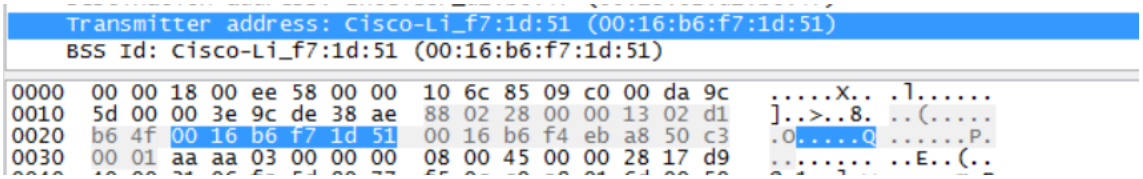
Neste caso vamos ter que o “Receiver” igual ao “Destination address” logo terão o mesmo endereço e temos o “Source” que terá outro endereço. O mac do host ligado sem fios é 00:13:02:d1:b6:4f, o ap é 00:16:b6:f4:eb:a8 sendo o router de acesso igual. O Ip do host sem fios que envia o segmento TCP é 192.168.1.109 sendo o endereço IP destino 128.119.245.12. O endereço IP destino corresponde ao servidor destino.

11. Localize a trama 802.11 que contém o segmento TCP SYN ACK para esta conexão TCP. Quais são os campos de endereçamento MAC contidos na trama 802.11? Que endereço MAC corresponde ao host? Qual o endereço MAC do originador da trama 802.11 que contém o segmento TCP proveniente do servidor? (nota: este aspecto deve ter ficado claro com a realização do TP2)

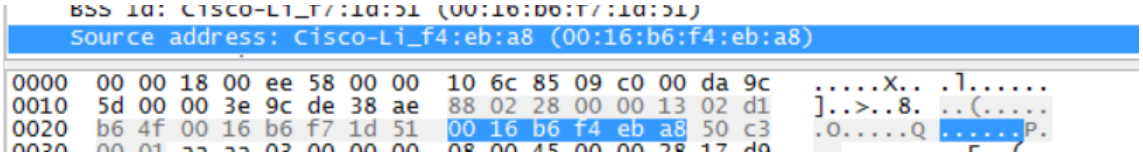
Os três campos de endereço contidos na trama 802.11 são:



que contem o receiver address e o destination address,



que contem o transmitter address e o BSS ID, e por ultimo



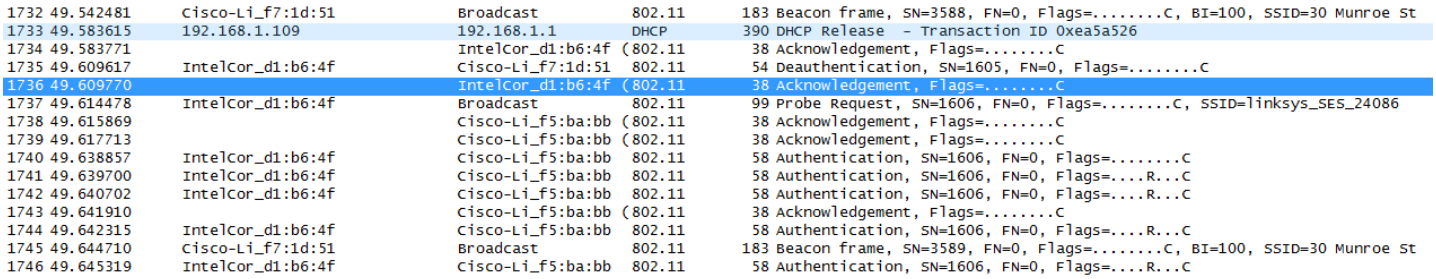
que contem o Source address.

O endereço Mac do host é 00:13:02:d1:b6:4f e o mac do originador da trama é 00:16:b6:f7:1d:51.

12. Verifique como é especificada a direccionalidade das tramas no cabeçalho 802.11, tomando como exemplo as tramas identificadas em 10) e 11)

Como podemos ver pelas perguntas 10 e 11 e com o auxílio do wireshark, reparamos que o cliente vai lançar uma flag para obter dados do servidor, obtendo uma resposta do servidor e este mesmo pedindo também dados ao cliente. De seguida o cliente responde, começando assim então a transferência de dados necessária para o descarregamento do ficheiro.

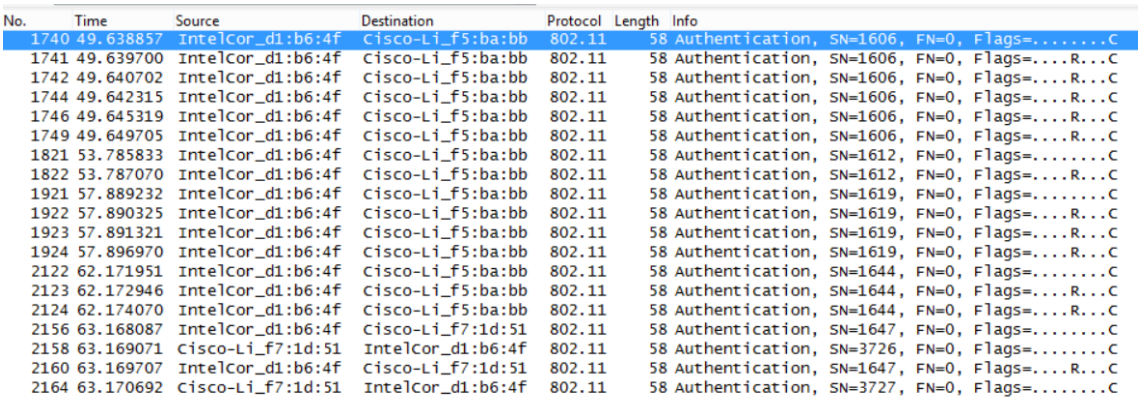
13. Que ação é tomada pelo host após t=49.5s que determina a quebra de associação com o AP 30 Munroe St que existia desde que a captura de tramas começou? Como interpreta as tramas 802.11 subsequentes relacionadas com a anterior ação? Segundo a especificação IEEE 802.11, há alguma trama que seria esperada, mas não aparece?



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	49.609617	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54 Deauthentication, SN=1605, FN=0, Flags=........C
1736	49.609770		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

É enviada uma trama de Deauthentication ao AP, o que quebrou a associação com o AP 30 Munroe St. As tramas 802.11 subsequentes indicam que o host tentou authenticar-se noutro AP, o linksys_SES_24086, depois de se desconectar de 30 Munroe St. Segundo a especificação IEE 802.11 o AP deveria responder ao Association Request enviado pelo host, mas não aparece nenhuma resposta

14. Examine o ficheiro de trace e procure tramas de autenticação enviadas pelo host para o AP e vice-versa (se filtrar os resultados por wlan.fc.type_subtype ajuda a localização). Quantas tramas de AUTHENTICATION são enviadas do host sem fios para o AP linksys_SES_24086 AP? Durante que período de tempo?



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

São 15 tramas de AUTHENTICATION que são enviados para o AP linksys_SES_24086, durante o instante 49.638857 e o 63.168087 o que da 13.52923 segundos.

15. O host tenta usar algum algoritmo de autenticação/chave ou tenta aceder de forma aberta? Existe alguma resposta do AP linksys_SES_24086 ao pedido de autenticação? Porquê?

O host tenta aceder através do algoritmo de autenticação/chave. Não existe resposta do AP linksys_SES_24086 do pedido de autenticação porque este não tem uma chave de encriptação logo não pode ser autentificada.

16. Estabeleça um filtro adequado para localizar simultaneamente estes subtipos de trama de uma forma rápida e eficiente. Quais são os endereços MAC do originador, receptor e BSS ID nestas tramas? Qual é a função deste tipo de tramas?

Filtro: wlan.fc.type_subtype == 4 || wlan.fc.type_subtype == 5

Nas tramas Probe Request existem dois endereços MAC de originadores diferentes, 00:12:f0:1f:57:13 e 00:13:02:d1:b6:4f. Estas tramas são enviadas em Broadcast pelo que os recetores e BSS ID são ff:ff:ff:ff:ff:ff.

Nas tramas Probe Response temos resposta de dois APs, no primeiro, o MAC address do originador é 00:16:b6:f7:1d:51, o do recetor é 00:13:02:d1:b6:4f e o BSS ID é 00:16:b6:f7:1d:51.

No segundo, o MAC address do originador é a8:97:42:03:b0:b0, o do recetor é d9:51:90:31:16:30 e o BSS ID é 57:ac:42:16:91:eb. Estas tramas são usadas para os hosts descobrirem os APs que estão ao seu alcance e para, ao responderem, informarem sobre o data rate suportado e outras características.

```
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: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
Source address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)

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: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
Source address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
```

```
Type/Subtype: Probe Response (0x0005)
⊞ Frame Control Field: 0x5008
.000 0001 0011 1010 = Duration: 314 microseconds
Receiver address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
Destination address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
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)

Type/Subtype: Probe Response (0x0005)
⊞ Frame Control Field: 0x52f9
Duration/ID: 2693 (reserved)
Receiver address: d9:51:90:31:16:30 (d9:51:90:31:16:30)
Destination address: d9:51:90:31:16:30 (d9:51:90:31:16:30)
Transmitter address: a8:97:42:03:b0:b0 (a8:97:42:03:b0:b0)
Source address: a8:97:42:03:b0:b0 (a8:97:42:03:b0:b0)
BSS Id: 57:ac:42:16:91:eb (57:ac:42:16:91:eb)
```

17. Certifique-se do tipo de canal que está a ser usado e identifique os APs que, maioritariamente, estão a ser anunciados.

Os Aps a ser anunciados são os seguintes:

```
CiscoInc_e4:b3:20          AsustekC_21:4a:61

ZteCorpo_be:72:a4          LgElectr_0e:1e:5e
```

Estando todos eles a trabalhar em 802.11g

```
Channel type: 802.11g (0x0480)
```

18. Tomando como exemplo a estação cujo endereço MAC é AsustekC_21:4a:61 (00:22:15:21:4a:61), identifique a ocorrência de troca de dados envolvendo tramas de controlo RTS/CTS. Verifique a seu sentido de envio (toDS, fromDS). Registe o endereçamento MAC dos sistemas envolvidos, explicando o seu papel no processo de troca de dados.

```
LiteonTe_81:55:74 (TA)        AsustekC_21:4a:61 (802.11      45 Request-to-send, Flags=........C
LiteonTe_81:55:74 (TA)        AsustekC_21:4a:61 (802.11      45 Request-to-send, Flags=........C
LiteonTe_81:55:74 (TA)        AsustekC_21:4a:61 (802.11      45 Request-to-send, Flags=........C )
LiteonTe_81:55:74 (TA)        AsustekC_21:4a:61 (802.11      45 Request-to-send, Flags=........C
LiteonTe_81:55:74 (TA)        AsustekC_21:4a:61 (802.11      45 Request-to-send, Flags=........C
LiteonTe_81:55:74 (TA)        AsustekC_21:4a:61 (802.11      45 Request-to-send, Flags=........C
                              AsustekC_21:4a:61 (802.11      39 Acknowledgement, Flags=........C
                              AsustekC_21:4a:61 (802.11      39 Acknowledgement, Flags=........C
LiteonTe_81:55:74 (TA)        AsustekC_21:4a:61 (802.11      45 Request-to-send, Flags=........C
```

Como podemos ver na imagem acima vamos ter várias tramas RTS.

Neste caso irá operar em modo AD-HOC, apenas havendo transmissão entre AP e estação sem conexão com a rede de distribuição, estando o toDS e o fromDS a 0.

No RTS, iremos ter apenas um AP, o LiteonTe_81:55:74 com mac: 48:d2:24:81:55:74, a transmitir para a estação do asustekc_21:4a:61 com mac: 00:22:15:21:4a:61.

```
  Type/Subtype: Request-to-send (0x001b)
⊞ Frame Control Field: 0xb400
  .000 0001 0110 0000 = Duration: 352 microseconds
  Receiver address: AsustekC_21:4a:61 (00:22:15:21:4a:61)
  Transmitter address: LiteonTe_81:55:74 (48:d2:24:81:55:74)
```

Depois, o AP irá receber um CTS. Neste tipo de trama apenas existe destino, não existe origem, como podemos ver na imagem abaixo.

```
  Type/Subtype: Clear-to-send (0x001c)
⊞ Frame Control Field: 0xc400
  .000 0001 0000 1100 = Duration: 268 microseconds
  Receiver address: LiteonTe_81:55:74 (48:d2:24:81:55:74)
```

O endereço mac irá ser crucial para identificar as máquinas que irão realizar a troca de dados.

Conclusão

Este TP foi acerca de redes sem fios (802.11). Dentro deste tema abordamos vários tópicos, alguns tipos de tramas, limitações na captura de trafego, transferência de dados, associação e desassociação, probing e RTS/CTS.

Apesar de algumas dificuldades, conseguimos finalizar o relatório, aumento o nosso nível de conhecimento acerca destes assuntos. Aprendemos a fazer filtros na ferramenta de WireShark, o que nos ajudou muito, pois esta contém muita informação e a capacidade de filtrar é ótimo.

Aprendemos também a saber a diferença entre uma estação e um acess point, como estas comunicam entre si e com o cliente, como é o caso dos TCP SYN que faz a ligação com o servidor de maneira a que consigamos fazer a transferência de dados.

Apesar de termos conhecimento que nem todas as respostas estão corretas pensamos ter mencionada informação importante em todas elas.