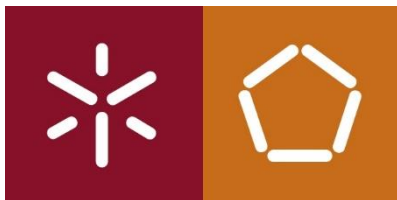


Redes de Computadores



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)



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)

| | | | | |
|----------------|-------------------|-----------------------------|--------|--|
| 1103 32.943448 | Cisco-Li_f4:eb:a8 | IntelCor_d1:b6:4f | LLC | 1562 U, func=UI; SNAP, OUI 0x000000 (Officially Xerox, but 0:0:0:0:0:0 is more common), PID 0x0800 |
| 1106 32.945936 | Cisco-Li_f4:eb:a8 | IntelCor_d1:b6:4f | LLC | 1562 U, func=UI; SNAP, OUI 0x000000 (Officially Xerox, but 0:0:0:0:0:0 is more common), PID 0x0800 |
| 1107 32.946277 | Cisco-Li_f4:eb:a8 | IntelCor_d1:b6:4f | LLC | 1562 U, func=UI; SNAP, OUI 0x000000 (Officially Xerox, but 0:0:0:0:0:0 is more common), PID 0x0800 |
| 1108 32.946405 | | Cisco-Li_f7:1d:51 (~ 802.11 | | 38 Acknowledgement, Flags=.....C |
| 1109 32.946503 | Cisco-Li_f4:eb:a8 | IntelCor_d1:b6:4f | LLC | 753 U, func=UI; SNAP, OUI 0x000000 (Officially Xerox, but 0:0:0:0:0:0 is more common), PID 0x0840 |
| 1110 32.946809 | Cisco-Li_f4:eb:a8 | IntelCor_d1:b6:4f | LLC | 753 U, func=UI; SNAP, OUI 0x000000 (Officially Xerox, but 0:0:0:0:0:0 is more common), PID 0x0800 |
| 1111 32.947559 | Cisco-Li_f4:eb:a8 | IntelCor_d1:b6:4f | LLC | 753 U, func=UI; SNAP, OUI 0x000000 (Officially Xerox, but 0:0:0:0:0:0 is more common), PID 0x0800 |
| 1112 32.948244 | Cisco-Li_f4:eb:a8 | IntelCor_d1:b6:4f | LLC | 753 U, func=UI; SNAP, OUI 0x000000 (Officially Xerox, but 0:0:0:0:0:0 is more common), PID 0x0800 |
| 1113 32.948361 | | Cisco-Li_f7:1d:51 (~ 802.11 | | 38 Acknowledgement, Flags=.....C |
| 1114 32.948458 | IntelCor_d1:b6:4f | Cisco-Li_f4:eb:a8 | LLC | 102 U, func=UI; SNAP, OUI 0x000000 (Officially Xerox, but 0:0:0:0:0:0 is more common), PID 0x0800 |
| 1115 32.948554 | | IntelCor_d1:b6:4f (~ 802.11 | | 38 Acknowledgement, Flags=.....C |
| 1116 32.954411 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 Beacon frame, SN=3342, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St |

> Frame 1106: 1562 bytes on wire (12496 bits), 1562 bytes captured (12496 bits)

> Radiotap Header v0, Length 24

> 802.11 radio information

PHY type: 802.11g (6)
Short preamble: False
Proprietary mode: None (0)
Data rate: 54.0 Mb/s
Channel: 6
Frequency: 2437MHz
Signal strength (dB): 65dB
Signal strength (dBm): -35dBm
Noise level (dBm): -100dBm
Signal/noise ratio (dB): 65dB

> [Duration: 252µs]

> IEEE 802.11 QoS Data, Flags:R.F.C

> Logical-Link Control

> Data (1500 bytes)

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.

| No. | Time | Source | Destination | Protocol | Length | Info | Tag |
|-----|----------|-------------------|-------------|----------|--------|--|-----|
| 1 | 0.000000 | Cisco-Li-f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SII=2854, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St | ✓ |
| 3 | 0.005474 | Cisco-Li-f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SII=2855, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St | ✓ |
| 4 | 0.187919 | Cisco-Li-f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SII=2856, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St | ✓ |
| 9 | 0.290284 | Cisco-Li-f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SII=2857, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St | ✓ |
| 10 | 0.294432 | Linksys6_67:22:94 | Broadcast | 802.11 | 90 | Beacon frame, SII=3072, FN=0, Flags=.....C, BI=62, SSID=li\357\277\275\001\004\357\277\275[Malformed Packet] | ✓ |
| 11 | 0.393174 | Cisco-Li-f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SII=2858, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St | ✓ |
| 13 | 0.495932 | Cisco-Li-f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SII=2859, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St | ✓ |
| 14 | 0.499197 | Linksys6_67:22:94 | Broadcast | 802.11 | 90 | Beacon frame, SII=3074, FN=0, Flags=.....C, BI=100, SSID=linksys12 | ✓ |
| 15 | 0.597382 | Cisco-Li-f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SII=2860, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St | ✓ |
| 16 | 0.601687 | Linksys6_67:22:94 | Broadcast | 802.11 | 90 | Beacon frame, SII=3075, FN=0, Flags=.....C, BI=100, SSID=linksys12 | ✓ |

> Frame 3: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits)
 > Radiotap Header v0, Length 24
 > 802.11 radio information
 > IEEE 802.11 Beacon frame, Flags:C
 > IEEE 802.11 wireless LAN
 > Fixed parameters (12 bytes)
 Timestamp: 174319104386
 Beacon Interval: 0.102400 [Seconds]
 > Capabilities Information: 0x0001
 > Tagged parameters (119 bytes)
 > Tag: SSID parameter set: 30 Munroe St
 > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
 > Tag: DS Parameter set: Current Channel: 6
 > Tag: Traffic Indication Map (TIM): DTIM 0 of 0 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: Vendor Specific: Airo Networks, Inc.
 > Tag: Vendor Specific: Microsoft Corp.: WMM/QoS: Parameter Element

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.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|--------------------|------------------------------|----------|--------|---|
| 1 | 0.000000 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=2854, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St |
| 2 | 0.062181 | b6:78:8c:c1:aec:0 | (... 65:a8:d5:b2:c1:99 (...) | 802.11 | 1624 | 802.11 Block Ack Req, Flags=op.P...TC |
| 3 | 0.085474 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=2855, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St |
| 4 | 0.187919 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=2856, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St |
| 5 | 0.188100 | IntelCor_d1:b6:4f | Cisco-Li_f7:1d:51 | 802.11 | 54 | QoS Null function (No data), SN=1482, FN=0, Flags=.....TC |
| 6 | 0.188201 | | IntelCor_d1:b6:4f (...) | 802.11 | 38 | Acknowledgement, Flags=.....C |
| 7 | 0.188935 | IntelCor_d1:b6:4f | Cisco-Li_f7:1d:51 | 802.11 | 54 | QoS Null function (No data), SN=1483, FN=0, Flags=...P...TC |
| 8 | 0.189034 | | IntelCor_d1:b6:4f (...) | 802.11 | 38 | Acknowledgement, Flags=.....C |
| 9 | 0.290284 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=2857, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St |
| 10 | 0.294432 | LinksysG_67:22:94 | Broadcast | 802.11 | 90 | Beacon frame, SN=3072, FN=0, Flags=.....C, BI=62, SSID=li\357\277\275\001\004\357 |
| 11 | 0.393174 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=2858, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St |
| 12 | 0.396690 | 00:aec:93:3d:0a:4a | ff:ff:ff:ff:bf:4a | 802.11 | 90 | Association Response, SN=3073, FN=0, Flags=.....C |
| 13 | 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 |
| 14 | 0.499197 | LinksysG_67:22:94 | Broadcast | 802.11 | 90 | Beacon frame, SN=3074, FN=0, Flags=.....C, BI=100, SSID=linksys12 |
| 15 | 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 |

<

> Frame Control Field: 0x8000

.000 0000 0000 0000 = Duration: 0 microseconds

Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)

<Receiver address (resolved): Broadcast>

<Hardware address: Broadcast (ff:ff:ff:ff:ff:ff)>

<Hardware address (resolved): Broadcast>

Destination address: Broadcast (ff:ff:ff:ff:ff:ff)

<Destination address (resolved): Broadcast>

Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)

<Transmitter address (resolved): Cisco-Li_f7:1d:51>

Source address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)

<Source address (resolved): Cisco-Li_f7:1d:51>

BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)

<BSS Id (resolved): Cisco-Li_f7:1d:51>

<Hardware address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)>

<Hardware address (resolved): Cisco-Li_f7:1d:51>

<Hardware address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)>

<Hardware address (resolved): Cisco-Li_f7:1d:51>

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?

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|-------------------------|-------------------------|----------|--------|--|
| 1 | 0.000000 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=2854, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St |
| 2 | 0.062101 | b6:78:8c:c1:ae:c0 (...) | 65:a8:d5:b2:c1:99 (...) | 802.11 | 1624 | 802.11 Block Ack Req, Flags=op.P...TC |
| 3 | 0.085474 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=2855, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St |
| 4 | 0.187919 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=2856, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St |
| 5 | 0.188100 | IntelCor_d1:b6:4f | Cisco-Li_f7:1d:51 | 802.11 | 54 | QoS Null function (No data), SN=1482, FN=0, Flags=.....TC |
| 6 | 0.188201 | | IntelCor_d1:b6:4f (...) | 802.11 | 38 | Acknowledgement, Flags=.....C |
| 7 | 0.188935 | IntelCor_d1:b6:4f | Cisco-Li_f7:1d:51 | 802.11 | 54 | QoS Null function (No data), SN=1483, FN=0, Flags=...P...TC |
| 8 | 0.189034 | | IntelCor_d1:b6:4f (...) | 802.11 | 38 | Acknowledgement, Flags=.....C |

| |
|---|
| > Tag: SSID parameter set: 30 Munroe St |
| ✓ 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 0 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) |
| > Tag: Vendor Specific: Airgo Networks, Inc. |

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)?

| | | | | | | |
|------|-----------|-------------------|-----------|--------|-----|---------------|
| 1205 | 33.056759 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, |
|------|-----------|-------------------|-----------|--------|-----|---------------|

| |
|---|
| > Frame 1205: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits) |
| > Radiotap Header v0, Length 24 |
| > 802.11 radio information |
| ✓ IEEE 802.11 Beacon frame, Flags:C |
| Type/Subtype: Beacon frame (0x0008) |
| ✓ Frame Control Field: 0x8000 |
|00 = Version: 0 |
| 00.. = Type: Management frame (0) |
| 1000 = Subtype: 8 |

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.

```
▼ IEEE 802.11 Beacon frame, Flags: .....
  Type/Subtype: Beacon frame (0x0008)
  > Frame Control Field: 0x8000
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: 5f:a5:ff:ff:ff:ff (5f:a5:ff:ff:ff:ff)
    <Receiver address (resolved): 5f:a5:ff:ff:ff:ff>
    <Hardware address: 5f:a5:ff:ff:ff:ff (5f:a5:ff:ff:ff:ff)>
    <Hardware address (resolved): 5f:a5:ff:ff:ff:ff>
    Destination address: 5f:a5:ff:ff:ff:ff (5f:a5:ff:ff:ff:ff)
    <Destination address (resolved): 5f:a5:ff:ff:ff:ff>
    Transmitter address: LinksysG_67:22:94 (00:06:25:67:22:94)
    <Transmitter address (resolved): LinksysG_67:22:94>
    Source address: LinksysG_67:22:94 (00:06:25:67:22:94)
    <Source address (resolved): LinksysG_67:22:94>
    BSS Id: LinksysG_67:22:94 (00:06:25:67:22:94)
    <BSS Id (resolved): LinksysG_67:22:94>
    <Hardware address: LinksysG_67:22:94 (00:06:25:67:22:94)>
    <Hardware address (resolved): LinksysG_67:22:94>
    <Hardware address: LinksysG_67:22:94 (00:06:25:67:22:94)>
    <Hardware address (resolved): LinksysG_67:22:94>
    .... 0000 = Fragment number: 0
    1101 1001 1101 .... = Sequence number: 3485
  > Frame check sequence: 0x79f611cc incorrect, should be 0xa1bf68cc
    [FCS Status: Bad]
```

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 registre 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.

```
▼ 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)
    <Receiver address (resolved): Broadcast>
    <Hardware address: Broadcast (ff:ff:ff:ff:ff:ff)>
    <Hardware address (resolved): Broadcast>
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    <Destination address (resolved): Broadcast>
    Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    <Transmitter address (resolved): Cisco-Li_f7:1d:51>
    Source address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    <Source address (resolved): Cisco-Li_f7:1d:51>
    BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    <BSS Id (resolved): Cisco-Li_f7:1d:51>
    <Hardware address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)>
    <Hardware address (resolved): Cisco-Li_f7:1d:51>
    <Hardware address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)>
    <Hardware address (resolved): Cisco-Li_f7:1d:51>
    .... 0000 = Fragment number: 0
    1011 0010 0110 .... = Sequence number: 2854
    Frame check sequence: 0x057e2608 [unverified]
    [FCS Status: Unverified]
```

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.

| wlan.fc.type == 0&&(wlan.fc.subtype == 4 wlan.fc.subtype == 5) | | | | | |
|---|----------|-------------------|-------------------|----------|--|
| No. | Time | Source | Destination | Protocol | Length Info |
| 27 | 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 |
| 50 | 2.297613 | IntelCor_1f:57:13 | Broadcast | 802.11 | 79 Probe Request, SN=576, FN=0, Flags=.....C, SSID=Home WIFI |
| 51 | 2.300697 | Cisco-Li_f7:1d:51 | IntelCor_1f:57:13 | 802.11 | 177 Probe Response, SN=2878, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St |
| 52 | 2.302191 | Cisco-Li_f7:1d:51 | IntelCor_1f:57:13 | 802.11 | 177 Probe Response, SN=2878, FN=0, Flags=...R...C, BI=100, SSID=30 Munroe St |
| 53 | 2.304063 | Cisco-Li_f7:1d:51 | IntelCor_1f:57:13 | 802.11 | 177 Probe Response, SN=2878, FN=0, Flags=...R...C, BI=100, SSID=30 Munroe St |
| 54 | 2.305562 | Cisco-Li_f7:1d:51 | IntelCor_1f:57:13 | 802.11 | 177 Probe Response, SN=2878, FN=0, Flags=...R...C, BI=100, SSID=30 Munroe St |
| 55 | 2.308563 | Cisco-Li_f7:1d:51 | IntelCor_1f:57:13 | 802.11 | 177 Probe Response, SN=2878, FN=0, Flags=...R...C, BI=100, SSID=30 Munroe St |
| 56 | 2.310072 | Cisco-Li_f7:1d:51 | IntelCor_1f:57:13 | 802.11 | 177 Probe Response, SN=2878, FN=0, Flags=...R...C, BI=100, SSID=30 Munroe St |
| 59 | 2.453941 | Cisco-Li_f7:1d:51 | IntelCor_1f:57:13 | 802.11 | 177 Probe Response, SN=2881, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St |
| 83 | 4.283835 | Cisco-Li_f7:1d:51 | IntelCor_d1:b6:4f | 802.11 | 177 Probe Response, SN=2900, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St |
| 87 | 4.298449 | IntelCor_1f:57:13 | Broadcast | 802.11 | 78 Probe Request, SN=598, FN=0, Flags=.....C, SSID=phoiphass |
| 88 | 4.301564 | Cisco-Li_f7:1d:51 | IntelCor_1f:57:13 | 802.11 | 177 Probe Response, SN=2901, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St |
| 89 | 4.303314 | Cisco-Li_f7:1d:51 | IntelCor_1f:57:13 | 802.11 | 177 Probe Response, SN=2901, FN=0, Flags=...R...C, BI=100, SSID=30 Munroe St |
| 90 | 4.304814 | Cisco-Li_f7:1d:51 | IntelCor_1f:57:13 | 802.11 | 177 Probe Response, SN=2901, FN=0, Flags=...R...C, BI=100, SSID=30 Munroe St |
| 93 | 4.403454 | Cisco-Li_f7:1d:51 | IntelCor_1f:57:13 | 802.11 | 177 Probe Response, SN=2903, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St |
| 94 | 4.404939 | Cisco-Li_f7:1d:51 | IntelCor_1f:57:13 | 802.11 | 177 Probe Response, SN=2903, FN=0, Flags=...R...C, BI=100, SSID=30 Munroe St |
| 117 | 6.299705 | IntelCor_1f:57:13 | Broadcast | 802.11 | 79 Probe Request, SN=620, FN=0, Flags=.....C, SSID=concourse |
| 118 | 6.300439 | IntelCor_1f:57:13 | Broadcast | 802.11 | 70 Probe Request, SN=621, FN=0, Flags=.....C, SSID=Wildcard (Broadcast) |

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?

| | | | | | |
|----|----------|-------------------|-------------------|--------|---------------------|
| 50 | 2.297613 | IntelCor_1f:57:13 | Broadcast | 802.11 | 79 Probe Request, |
| 51 | 2.300697 | Cisco-Li_f7:1d:51 | IntelCor_1f:57:13 | 802.11 | 177 Probe Response, |

```

> Frame 50: 79 bytes on wire (632 bits), 79 bytes captured (632 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
✓ IEEE 802.11 Probe Request, Flags: .....C
  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)
    <Receiver address (resolved): Broadcast>
    <Hardware address: Broadcast (ff:ff:ff:ff:ff:ff)>
    <Hardware address (resolved): Broadcast>
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    <Destination address (resolved): Broadcast>
    Transmitter address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
    <Transmitter address (resolved): IntelCor_1f:57:13>
    Source address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
    <Source address (resolved): IntelCor_1f:57:13>
    BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)

```


(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)

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

```
50 2.297613 IntelCor_1f:57:13 Broadcast 802.11 79 Probe Request,
51 2.300697 Cisco-Li_f7:1d:51 IntelCor_1f:57:13 802.11 177 Probe Response,
> Frame 51: 177 bytes on wire (1416 bits), 177 bytes captured (1416 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
▼ IEEE 802.11 Probe Response, Flags: .....C
  Type/Subtype: Probe Response (0x0005)
  > Frame Control Field: 0x5000
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
    <Receiver address (resolved): IntelCor_1f:57:13>
    <Hardware address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)>
    <Hardware address (resolved): IntelCor_1f:57:13>
    Destination address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
    <Destination address (resolved): IntelCor_1f:57:13>
    Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    <Transmitter address (resolved): Cisco-Li_f7:1d:51>
    Source address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    <Source address (resolved): Cisco-Li_f7:1d:51>
    BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    <BSS Id (resolved): Cisco-Li_f7:1d:51>
```

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?

```
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 IntelCor_d1:b6:4f (00:13:02:d1:b... 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
```


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?

| wlan.fc.type_subtype==11 | | | | | | |
|--------------------------|-----------|-------------------|-------------------|----------|--------|--|
| 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 |

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?

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|-----------|-------------------|-------------------|----------|--------|-----------------------|
| 1763 | 49.746105 | IntelCor_d1:b6:4f | Cisco-Li_f5:ba:bb | EAPOL | 185 | Key (Message 2 of 4) |
| 1764 | 49.747831 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=3590 |
| 1765 | 49.749453 | IntelCor_d1:b6:4f | Cisco-Li_f5:ba:bb | EAPOL | 185 | Key (Message 2 of 4) |
| 1766 | 49.753595 | IntelCor_d1:b6:4f | Cisco-Li_f5:ba:bb | EAPOL | 185 | Key (Message 2 of 4) |

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 autenticação do AP linksys ses 24086 AP no trace?

| wlan.fc.type_subtype==11 | | | | | | |
|--------------------------|-----------|-------------------|-------------------|----------|--------|--|
| 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 |

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?

| wlan.fc.type_subtype==11 | | | | | | |
|--------------------------|-----------|-------------------|-------------------|----------|--------|---|
| 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 |

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 ?

| wlan.fc.type_subtype==0 | | | | | | |
|-------------------------|-----------|-------------------|-------------------------------------|----------|--------|--|
| No. | Time | Source | Destination | Protocol | Length | Info |
| 1227 | 33.079714 | d1:b6:4f:00:16:b6 | MS-NLB-PhysServer-32_08:00:00:13... | 802.11 | 111 | Association Request, SN=3775, FN=4, Flags=.pm...F.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 |
| 1824 | 53.789944 | IntelCor_d1:b6:4f | Cisco-Li_f5:ba:bb | 802.11 | 107 | Association Request, SN=1613, FN=0, Flags=.....C, SSID=linksys_SES_24086 |
| 1825 | 53.790943 | IntelCor_d1:b6:4f | Cisco-Li_f5:ba:bb | 802.11 | 107 | Association Request, SN=1613, FN=0, Flags=...R...C, SSID=linksys_SES_24086 |
| 1827 | 53.793568 | IntelCor_d1:b6:4f | Cisco-Li_f5:ba:bb | 802.11 | 107 | Association Request, SN=1613, FN=0, Flags=.....C, SSID=linksys_SES_24086 |
| 1926 | 57.903699 | IntelCor_d1:b6:4f | Cisco-Li_f5:ba:bb | 802.11 | 107 | Association Request, SN=1620, FN=0, Flags=.....C, SSID=linksys_SES_24086 |
| 1927 | 57.904945 | IntelCor_d1:b6:4f | Cisco-Li_f5:ba:bb | 802.11 | 107 | Association Request, SN=1620, FN=0, Flags=...R...C, SSID=linksys_SES_24086 |
| 1932 | 57.911195 | IntelCor_d1:b6:4f | Cisco-Li_f5:ba:bb | 802.11 | 107 | Association Request, SN=1620, FN=0, Flags=...R...C, SSID=linksys_SES_24086 |
| 1933 | 57.915945 | IntelCor_d1:b6:4f | Cisco-Li_f5:ba:bb | 802.11 | 107 | Association Request, SN=1620, FN=0, Flags=...R...C, SSID=linksys_SES_24086 |
| 1934 | 57.924199 | IntelCor_d1:b6:4f | Cisco-Li_f5:ba:bb | 802.11 | 107 | Association Request, SN=1620, FN=0, Flags=...R...C, SSID=linksys_SES_24086 |
| 1935 | 57.936216 | IntelCor_d1:b6:4f | Cisco-Li_f5:ba:bb | 802.11 | 107 | Association Request, SN=1620, FN=0, Flags=...R...C, SSID=linksys_SES_24086 |
| 1937 | 57.939196 | IntelCor_d1:b6:4f | Cisco-Li_f5:ba:bb | 802.11 | 107 | Association Request, SN=1620, FN=0, Flags=.....C, SSID=linksys_SES_24086 |
| 2126 | 62.176945 | IntelCor_d1:b6:4f | Cisco-Li_f5:ba:bb | 802.11 | 107 | Association Request, SN=1645, FN=0, Flags=.....C, SSID=linksys_SES_24086 |
| 2127 | 62.178194 | IntelCor_d1:b6:4f | Cisco-Li_f5:ba:bb | 802.11 | 107 | Association Request, SN=1645, FN=0, Flags=...R...C, SSID=linksys_SES_24086 |
| 2162 | 63.169910 | IntelCor_d1:b6:4f | Cisco-Li_f7:1d:51 | 802.11 | 89 | Association Request, SN=1648, FN=0, Flags=.....C, SSID=30 Munroe St |
| 2307 | 70.179949 | Cisco-Li_f5:ba:7b | f9:ff:ff:ff:ff:ff | 802.11 | 132 | Fragmented IEEE 802.11 frame |

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.

| wlan.fc.type_subtype==1 | | | | | |
|-------------------------|-----------|-------------------|-------------------|----------|--|
| No. | Time | Source | Destination | Protocol | Length Info |
| 12 | 0.396690 | 00:ae:93:3d:0a:4a | ff:ff:ff:ff:bf:4a | 802.11 | 90 Association Response, SN=3073, FN=0, Flags=.....C |
| 2166 | 63.192101 | Cisco-Li_f7:1d:51 | IntelCor_d1:b6:4f | 802.11 | 94 Association Response, SN=3728, FN=0, Flags=.....C |

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?

| wlan.fc.type_subtype==0 | | | | | |
|--|-----------|-------------------|-------------------|----------|--|
| No. | Time | Source | Destination | Protocol | Length Info |
| 2162 | 63.169910 | IntelCor_d1:b6:4f | Cisco-Li_f7:1d:51 | 802.11 | 89 Association Request, SN=1648, FN=0, Flags=.....C, SSID=30 Munroe St |
| > Frame 2162: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) | | | | | |
| > Radiotap Header v0, Length 24 | | | | | |
| > 802.11 radio information | | | | | |
| > IEEE 802.11 Association Request, Flags:C | | | | | |
| IEEE 802.11 wireless LAN | | | | | |
| Fixed parameters (4 bytes) | | | | | |
| Tagged parameters (33 bytes) | | | | | |
| Tag: SSID parameter set: 30 Munroe St | | | | | |
| Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18, [Mbit/sec] | | | | | |
| Tag: QoS Capability | | | | | |
| Tag: Extended Supported Rates 24(B), 36, 48, 54, [Mbit/sec] | | | | | |

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].

| wlan.fc.type_subtype==1 | | | | | |
|---|-----------|-------------------|-------------------|----------|--|
| No. | Time | Source | Destination | Protocol | Length Info |
| 2166 | 63.192101 | Cisco-Li_f7:1d:51 | IntelCor_d1:b6:4f | 802.11 | 94 Association Response, SN=3728, FN=0, Flags=.....C |
| > Frame 2166: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) | | | | | |
| > Radiotap Header v0, Length 24 | | | | | |
| > 802.11 radio information | | | | | |
| > IEEE 802.11 Association Response, Flags:C | | | | | |
| IEEE 802.11 wireless LAN | | | | | |
| Fixed parameters (6 bytes) | | | | | |
| Tagged parameters (36 bytes) | | | | | |
| Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec] | | | | | |
| Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec] | | | | | |
| Tag: EDCA Parameter Set | | | | | |

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

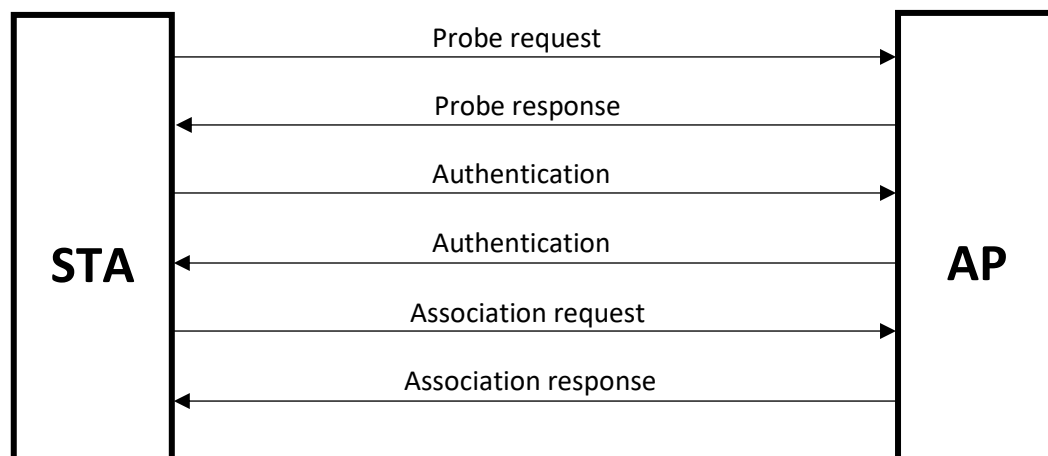
6.23) Identifique uma sequência de tramas que corresponda a um processo de associação completo entre a STA e o AP, incluindo a fase de autenticação.

| | | | | | |
|------|-----------|-------------------|-------------------------------------|--------|--|
| 2152 | 63.140106 | IntelCor_d1:b6:4f | Broadcast | 802.11 | 94 Probe Request, SN=1647, FN=0, Flags=.....C, SSID=30 Munroe St |
| 2153 | 63.142451 | Cisco-Li_f7:1d:51 | IntelCor_d1:b6:4f | 802.11 | 177 Probe Response, SN=3724, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St |
| 2154 | 63.142860 | Cisco-Li_f7:1d:51 | Cisco-Li_f7:1d:51 (00:16:b6:f7:1... | 802.11 | 38 Acknowledgement, Flags=.....C |
| 2155 | 63.161272 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 Beacon frame, SN=3725, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St |
| 2156 | 63.168087 | IntelCor_d1:b6:4f | Cisco-Li_f7:1d:51 | 802.11 | 58 Authentication, SN=1647, FN=0, Flags=.....C |
| 2157 | 63.168222 | IntelCor_d1:b6:4f | IntelCor_d1:b6:4f (00:13:02:d1:b... | 802.11 | 38 Acknowledgement, Flags=.....C |
| 2158 | 63.169071 | Cisco-Li_f7:1d:51 | IntelCor_d1:b6:4f | 802.11 | 58 Authentication, SN=3726, FN=0, Flags=.....C |
| 2159 | 63.169592 | Cisco-Li_f7:1d:51 | Cisco-Li_f7:1d:51 (00:16:b6:f7:1... | 802.11 | 38 Acknowledgement, 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 |
| 2161 | 63.169814 | IntelCor_d1:b6:4f | IntelCor_d1:b6:4f (00:13:02:d1:b... | 802.11 | 38 Acknowledgement, Flags=.....C |
| 2162 | 63.169910 | IntelCor_d1:b6:4f | Cisco-Li_f7:1d:51 | 802.11 | 89 Association Request, SN=1648, FN=0, Flags=.....C, SSID=30 Munroe St |
| 2163 | 63.170008 | IntelCor_d1:b6:4f | IntelCor_d1:b6:4f (00:13:02:d1:b... | 802.11 | 38 Acknowledgement, Flags=.....C |
| 2164 | 63.170692 | Cisco-Li_f7:1d:51 | IntelCor_d1:b6:4f | 802.11 | 58 Authentication, SN=3727, FN=0, Flags=.....C |
| 2165 | 63.171000 | Cisco-Li_f7:1d:51 | IntelCor_d1:b6:4f (00:16:b6:f7:1... | 802.11 | 38 Acknowledgement, Flags=.....C |
| 2166 | 63.192101 | Cisco-Li_f7:1d:51 | IntelCor_d1:b6:4f | 802.11 | 94 Association Response, SN=3728, FN=0, Flags=.....C |

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.



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?

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|-----------|---------------|----------------|----------|--------|---|
| 474 | 24.811093 | 192.168.1.109 | 128.119.245.12 | TCP | 110 | 2538 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1 |
| 1011 | 32.808574 | 192.168.1.109 | 128.119.240.19 | TCP | 110 | 2541 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1 |
| 1034 | 32.869262 | 192.168.1.109 | 128.119.240.19 | TCP | 110 | 2542 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1 |
| 1119 | 32.957207 | 192.168.1.109 | 128.119.240.19 | TCP | 110 | 2544 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1 |
| 1121 | 32.958198 | 192.168.1.109 | 128.119.240.19 | TCP | 110 | 2545 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1 |
| 1142 | 32.981949 | 192.168.1.109 | 64.233.187.104 | TCP | 110 | 2546 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1 |
| 1143 | 32.982315 | 192.168.1.109 | 64.233.187.104 | TCP | 110 | [TCP Out-Of-Order] 2546 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1 |
| 1153 | 33.001575 | 192.168.1.109 | 128.119.240.19 | TCP | 110 | 2547 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1 |
| 1262 | 33.099063 | 192.168.1.109 | 128.119.240.19 | TCP | 110 | 2548 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1 |
| 1280 | 33.115208 | 192.168.1.109 | 128.119.240.19 | TCP | 110 | 2549 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1 |
| 1714 | 49.020356 | 128.119.101.5 | 192.168.1.109 | TCP | 108 | 80 → 2543 [SYN, PSH, ECN, NS] Seq=2758133200 Win=7504[Malformed Packet] |

| |
|--|
| Type/Subtype: QoS Data (0x0028) |
| > Frame Control Field: 0x8801 |
| .0000 0000 0010 1100 = Duration: 44 microseconds |
| Receiver address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51) |
| <Receiver address (resolved): Cisco-Li_f7:1d:51> |
| <Hardware address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)> |
| <Hardware address (resolved): Cisco-Li_f7:1d:51> |
| Transmitter address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f) |
| <Transmitter address (resolved): IntelCor_d1:b6:4f> |
| <Hardware address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)> |
| <Hardware address (resolved): IntelCor_d1:b6:4f> |
| Destination address: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8) |
| <Destination address (resolved): Cisco-Li_f4:eb:a8> |
| Source address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f) |
| <Source address (resolved): IntelCor_d1:b6:4f> |
| BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51) |
| <BSS Id (resolved): Cisco-Li_f7:1d:51> |
| STA address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f) |
| <STA address (resolved): IntelCor_d1:b6:4f> |
| = Fragment number: 0 |
| 0000 0011 0001 = Sequence number: 49 |

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

| | | | | | |
|-----|-----------|----------------|---------------------------------------|--------|---|
| 474 | 24.811093 | 192.168.1.109 | 128.119.245.12 | TCP | 110 2538 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1 |
| 475 | 24.811231 | | IntelCor_d1:b6:4f (00:13:02:d1:b6:4f) | 802.11 | 38 Acknowledgement, Flags=.....C |
| 476 | 24.827751 | 128.119.245.12 | 192.168.1.109 | TCP | 110 80 → 2538 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 SACK_PERM=1 |
| 477 | 24.827922 | | Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51) | 802.11 | 38 Acknowledgement, Flags=.....C |
| 478 | 24.828024 | 192.168.1.109 | 128.119.245.12 | TCP | 102 2538 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0 |
| 479 | 24.828140 | | IntelCor_d1:b6:4f (00:13:02:d1:b6:4f) | 802.11 | 38 Acknowledgement, Flags=.....C |
| 480 | 24.828253 | 192.168.1.109 | 128.119.245.12 | HTTP | 537 GET /wireshark-labs/alice.txt HTTP/1.1 |

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

```
Receiver address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
<Receiver address (resolved): Cisco-Li_f7:1d:51>
<Hardware address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)>
<Hardware address (resolved): Cisco-Li_f7:1d:51>
Transmitter address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
<Transmitter address (resolved): IntelCor_d1:b6:4f>
<Hardware address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)>
<Hardware address (resolved): IntelCor_d1:b6:4f>
Destination address: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)
<Destination address (resolved): Cisco-Li_f4:eb:a8>
```

```
Source: 192.168.1.109
<Source or Destination Address: 192.168.1.109>
<[Source Host: 192.168.1.109]>
<[Source or Destination Host: 192.168.1.109]>
Destination: 128.119.245.12
<Source or Destination Address: 128.119.245.12>
<[Destination Host: 128.119.245.12]>
<[Source or Destination Host: 128.119.245.12]>
```

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.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|----------------|----------------|----------|--------|---|
| 474 | 24.811093 | 192.168.1.109 | 128.119.245.12 | TCP | 110 | 2538 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1 |
| 476 | 24.827751 | 128.119.245.12 | 192.168.1.109 | TCP | 110 | 80 → 2538 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 SACK_PERM=1 |

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?

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|-----------|----------------|----------------|----------|--------|---|
| 474 | 24.811093 | 192.168.1.109 | 128.119.245.12 | TCP | 110 | 2538 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1 |
| 476 | 24.827751 | 128.119.245.12 | 192.168.1.109 | TCP | 110 | 80 → 2538 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 SACK_PERM=1 |
| 1011 | 32.808574 | 192.168.1.109 | 128.119.240.19 | TCP | 110 | 2541 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1 |
| 1013 | 32.825631 | 128.119.240.19 | 192.168.1.109 | TCP | 110 | 80 → 2541 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 |
| 1034 | 32.869262 | 192.168.1.109 | 128.119.240.19 | TCP | 110 | 2542 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1 |
| 1047 | 32.890900 | 128.119.240.19 | 192.168.1.109 | TCP | 110 | 80 → 2542 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 |
| 1048 | 32.890998 | 128.119.240.19 | 192.168.1.109 | TCP | 110 | [TCP Out-Of-Order] 80 → 2542 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 ... |
| 1051 | 32.891536 | 128.119.240.19 | 192.168.1.109 | TCP | 110 | [TCP Out-Of-Order] 80 → 2542 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 ... |
| 1058 | 32.903185 | 128.119.101.5 | 192.168.1.109 | TCP | 110 | 80 → 2543 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 |
| 1119 | 32.957207 | 192.168.1.109 | 128.119.240.19 | TCP | 110 | 2544 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1 |
| 1121 | 32.958198 | 192.168.1.109 | 128.119.240.19 | TCP | 110 | 2545 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1 |

```

> Frame Control Field: 0x8832
Duration/ID: 11560 (reserved)
Receiver address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
<Receiver address (resolved): 91:2a:b0:49:b6:4f>
<Hardware address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)>
<Hardware address (resolved): 91:2a:b0:49:b6:4f>
Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
<Transmitter address (resolved): Cisco-Li_f7:1d:51>
<Hardware address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)>
<Hardware address (resolved): Cisco-Li_f7:1d:51>
Destination address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
<Destination address (resolved): 91:2a:b0:49:b6:4f>
Source address: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)
<Source address (resolved): Cisco-Li_f4:eb:a8>
BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
<BSS Id (resolved): Cisco-Li_f7:1d:51>
STA address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
<STA address (resolved): 91:2a:b0:49:b6:4f>

```

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.

```
Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
<Transmitter address (resolved): Cisco-Li_f7:1d:51>
<Hardware address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)>
<Hardware address (resolved): Cisco-Li_f7:1d:51>
Destination address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
<Destination address (resolved): 91:2a:b0:49:b6:4f>
Source address: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)
```

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).

2. 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 envio 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.