

# Redes de Computadores: TP4

4<sup>th</sup> December 2019

## Questões e Respostas:

### Trama 1204 (Grupo 4, Turno 2)

**1)**

Frequência do espectro: 2437 MHz

Canal: 6

**2)**

Version: 0

**3)**

Débito: 36.0 Mb/s

Não corresponde ao débito máximo da interface Wi-Fi, que, segundo o standard 802.11n, pode chegar aos 300 Mb/s (apenas uma antena).

**4)**

linksys\_SES\_24086

30 Munroe St

**5)**

Para o AP "linksys\_SES\_24086": 0.102400 Segundos

Para o AP "30 Munroe St": 0.102400 Segundos

---

**6)**

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

**7)**

ff:ff:ff:ff:ff:ff

**8)**

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

**9)**

Data Rates: 1.0, 2.0, 5.5 e 11.0 Mb/s

Extended Supported Rates: 6.0, 9.0, 12.0, 18.0, 24.0, 36.0, 48.0 e 54.0 Mb/s

**10)**

Trama 1204 (Acknowledgment)

Tipo: Control frame (1)

Subtipo: 13

No cabeçalho da trama, posição 2 a 4 (segundo o anexo do enunciado).

**11)**

```
BSS ID: CISCO-L1_T7:1d:51 (00:16:b6:f7:1d:51)
.... = Fragment number: 0
1101 0010 0110 .... = Sequence number: 3366
Frame check sequence: 0xfaf9f6bf [unverified]
[FCS Status: Unverified]
▼ IEEE 802.11 wireless LAN
  ▼ Fixed parameters (12 bytes)
    Timestamp: 174352077186
    Beacon Interval: 0,102400 [Seconds]
```

Dado a existência de Frame check sequence (FCS) podemos concluir que se está a utilizar um método CRC de detecção de erros.

## 12)

Utilizando a trama beacon 1205, podemos observar quatro endereços MAC:

```
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)
```

## 13)

wlan.fc.type\_subtype==4 or wlan.fc.type\_subtype==5

## 14)

Origem: IntelCor\_1f:57:13 (00:12:f0:1f:57:13) Destino: BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)

Pedir informações de uma outra estação sobre as APs ao seu alcance

## 15)

Origem: 00:16:b6:f7:1d:51 Destino: 00:12:f0:1f:57:13

Enviar a informação dos APs ao seu alcance para o destino que fez request.

## 16)

Em t = 49.583615 observamos um DHCP Release enviado pelo host para o servidor 192.168.1.1

Em t = 49.609617, o host envia uma trama Deauthentication.

Seria de esperar que fosse enviada uma trama Disassociation neste caso.

wlan.fc.subtype==11 and wlan.fc.type==0						
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

## 17)

A primeira trama Authentication do host para o AP acontece em t = 49.638857.

Tendo sido enviadas um total de 7 tramas de Authentication por volta de t = 49.

## 18)

Analisando a trama observamos que é especificado “Authentication Algorithm: Open System”, logo o host pretende uma autenticação aberta.

## 19)

Não é possível encontrar uma resposta do AP dado, isto acontece quando um AP está configurado para ignorar todos os pedidos com autenticação aberta, que é o que está a acontecer neste caso.

## 20)

Em t = 63.168087 existe uma trama Authentication do endereço 00:13:02:d1:b6:4f para 00:16:b7:f7:1d:51.

Em t = 63.169071 observa-se uma trama Authentication no sentido inverso (de 00:16:b7:f7:1d:51 para 00:13:02:d1:b6:4f)

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

## 21)

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 Mu...
2163	63.170008		IntelCor_d1:b6:4f (...)	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 (...)	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

Associate request: t = 63.169910 (de 00:13:02:d1:b6:4f para 00:16:b7:f7:1d:51)

Associate reply: t = 63.192101 (no sentido contrário)

## 22)

```
+ 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]
```

A trama Association Request mostra as seguintes taxas de transmissão: 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 32, 48, e 54 Mbps. Na Association Reply (AP) são usados as mesmas taxas.

23)

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 Mu...
2163	63.170008		IntelCor_d1:b6:4f (...)	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 (...)	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

Trama t = 63.169910 (Association request)

Trama t = 63.170692 (Authentication)

Trama t = 63.192101 (Association response)

24)

- PC
- AP
1. Probe request ----->

2. < ----- Probe Response

3. Authentication Open seq:1 ----->

4. <-----Authentication Open seq:2

5. Association Request ----->

6. <-----Association Response

7. <-----Data----->

25)

---

A primeira sessão TCP SYN é enviada em  $t = 24.811093$ .

## 26)

```
Receiver address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
Transmitter address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
Destination address: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)
Source address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
STA address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
```

```
Source: 192.168.1.109
Destination: 128.119.245.12
```

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

Endereço MAC destino: 00:16:b6:f4:eb:a8

Endereço MAC do BSS: 00:16:b6:f7:1d:51

Endereço IP do host: 192.168.1.109

Endereço IP destino: 128.199.245.12.

## 27)

Este endereço corresponde ao servidor onde se encontra Alice.txt

## 28)

```
Receiver address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
Destination address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
Source address: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)
BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
STA address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
```

A trama TCP SYNACK está em  $t = 24.827751$

Endereço MAC da source: 00:16:b6:f4:eb:a8

Endereço MAC destino: 91:2a:b0:49:b6:4f

Endereço MAC BSS: 00:16:b6:f7:1d:51

---

## 29)

Endereço MAC host: 91:2a:b0:49:b6:4f (endereço destino)

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

Endereço MAC AP: 00:16:b6:f7:1d:51

## 30)

O endereço MAC do host nesta trama é diferente do endereço IP do dispositivo que enviou o segmento TCP SYN. Isto porque a wireless interface do host funciona como se tivesse dois endereços de interface.

## Conclusão:

Este último trabalho provou-se ser difícil no sentido que foi necessário encontrar e usar vários filtros wireshark para encontrar as tramas pedidas nas questões.

Tivemos também de aprender a melhor analisar as tramas no wireshark, e utilizar os valores nos dados das tramas para filtrar o trace total.

Os anexos do enunciado foram também muito úteis para melhor perceber e identificar os vários tipos de tramas.