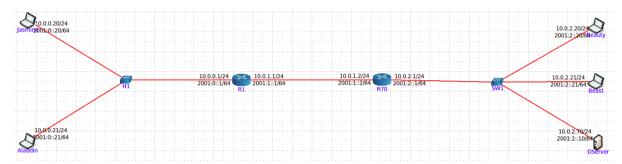
Relatório TP3

Grupo PL70:

André Santos a106854 Daniel Parente a107363 Pedro Ferreira a107292



PARTE I - Captura e análise de Tramas **Ethernet**

1.1) Questão: Anote os endereços MAC de origem e MAC destino da trama capturada. Identifique a que hosts se referem. Justifique.

Resposta: Podemos concluir que o MAC 00:00:00_aa:00:00 corresponde ao host Jasmine que corresponde à source neste caso no sentido cliente-servidor.

Podemos também ver o MAC 00:00:00 aa:00:02 que corresponde ao host R1, destination no sentido cliente-servidor.

No.	Time So	ource	Destination	Protocol	Length Info			
г	6 7.9905584 10	0.0.0.20	10.0.2.70	SSH	82 Client:	Encrypted	packet	(len=16)
	9 8.0312485 10	0.0.0.20	10.0.2.70	SSH	110 Client:	Encrypted	packet	(len=44)
	11 8.0313583 10	0.0.2.70	10.0.0.20	SSH	110 Server:	Encrypted	packet	(len=44)
	13 8.0314363 10	0.0.0.20	10.0.2.70	SSH	126 Client:	Encrypted	packet	(len=60)
	14 8.0407508 10	0.0.2.70	10.0.0.20	SSH	118 Server:	Encrypted	packet	(len=52)
	16 9.8167708 10	0.0.0.20	10.0.2.70	SSH	150 Client:	Encrypted	packet	(len=84)
	17 9.8357012 10	0.0.2.70	10.0.0.20	SSH	94 Server:	Encrypted	packet	(len=28)
	19 9.8358667 10	0.0.0.20	10.0.2.70	SSH	178 Client:	Encrypted	packet	(len=112)
	21 9.9675687 10	0.0.2.70	10.0.0.20	SSH	534 Server:	Encrypted	packet	(len=468)
	23 9.9995357 10	0.0.2.70	10.0.0.20	SSH	110 Server:	Encrypted	packet	(len=44)
	25 9.9997467 10	0.0.0.20	10.0.2.70	SSH	1146 Client:	Encrypted	packet	(len=1080)
	27 10.001375 10	0.0.2.70	10.0.0.20	SSH	174 Server:	Encrypted	packet	(len=108)
	28 10.005965 10	0.0.2.70	10.0.0.20	SSH	966 Server:	Encrypted	packet	(len=900)
	31 10.043474 10	0.0.2.70	10.0.0.20	SSH	118 Server:	Encrypted	packet	(len=52)

- > Frame 19: 178 bytes on wire (1424 bits), 178 bytes captured (1424 bits) on interface veth1.0.90, id 0
 Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:02 (00:00:00:aa:00:02)
 Destination: 00:00:00_aa:00:02 (00:00:00:aa:00:02)
 Source: 00:00:00_aa:00:00 (00:00:00:aa:00:00)

- Type: IPv4 (0x0800)

1.2) Questão: Qual o valor hexadecimal do campo Type contido no header da trama Ethernet? O que significa? Qual o campo do header IP que tem semântica idêntica?

Resposta: O valor é 0x0800 e indica que indica que o protocolo encapsulado é IPv4

```
Figher til, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:02 (00:00:00:aa:00:02)

Destination: 00:00:00_aa:00:02 (00:00:00:aa:00:02)

Source: 00:00:00_aa:00:00 (00:00:00:aa:00:00)

Type: IPv4 (0x0800)
```

Dentro do próprio cabeçalho *IP* existe um campo chamado Protocol que tem exatamente a mesma semântica e objetivo: identificar qual o protocolo que está a ser encapsulado.

```
Fragment offset: 0
Time to live: 64
Protocol: TCP (6)
Header checksum: 0x67e1 [validation disabled]
```

1.3) Questão: Quantos bytes são usados no encapsulamento protocolar, i.e., desde o início da trama até ao início dos dados do nível aplicacional? Calcule e indique, em percentagem, a sobrecarga (overhead) introduzida pela pilha protocolar.

Resposta: Tamanho da pilha protocolar: 178 bytes. $Overhead \ total = 20(IPv4) + 32(TCP) + 14 \ (Ethernet) = 66$ Percentegem Overhead = 66/178 = 37%

1.4) Questão: Qual é o endereço MAC da fonte? A que host e interface corresponde? Justifique.

Resposta: Trama Ethernet escolhida:

```
110 Server: Encrypted packet (len=44)
                                                                                                 1146 Client: Encrypted packet (len=1080)
174 Server: Encrypted packet (len=108)
       25 9.9997467... 10.0.0.20
27 10.001375... 10.0.2.70
                                                           10.0.2.70
                                                                                       SSH
                                                           10.0.0.20
                                                                                       SSH
       28 10.005965... 10.0.2.70
31 10.043474... 10.0.2.70
                                                           10.0.0.20
                                                                                       SSH
                                                                                                   966 Server: Encrypted packet (len=900)
                                                                                                   118 Server: Encrypted packet (len=52)
Frame 21: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits) on interface veth1.0.90, id 0  
   Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:00 (00:00:00:aa:00:00)
   Destination: 00:00:00_aa:00:00 (00:00:00:aa:00:00)
   > Source: 00:00:00_aa:00:02 (00:00:00:aa:00:02)
Type: IPv4 (0x0800)

    Internet Protocol Version 4, Src: 10.0.2.70, Dst: 10.0.0.20
    Transmission Control Protocol, Src Port: 22, Dst Port: 42332, Seq: 125, Ack: 317, Len: 468

SSH Protocol
```

Endereço MAC da fonte: 00:00:00:aa:00:02

Host/Interface: O endereço corresponde ao R1 pois MAC são endereços camada 2 que só é usada pelo router dentro da mesma rede. Não faria assim sentido vermos os MAC do servidor que está numa outra rede.

1.5) Questão: Qual é o endereço MAC do destino? A que host e interface corresponde?

Resposta: Endereço MAC do destino: 00:00:00:aa:00:00

Host/Interface:O endereço corresponde à Jasmine.

2.1) Questão: Observe o conteúdo da tabela ARP de Aladdin com o comando arp -a. Com a ajuda do manual ARP (man arp), interprete o significado de cada uma das colunas da tabela.

Resposta:

```
vcmd
root@Aladdin:/tmp/pycore.37889/Aladdin.conf# arp -a
? (10.0.0.1) at 00:00:00:00:02 [ether] on eth0
```

Após analisar a tabela ARP podemos concluir que "aprendeu" o endereço MAC correspondente ao endereço IP 10.0.0.1(R1). A tabela apresenta os seguintes campos : Endereço IP do host cujo MAC foi resolvido -> 10.0.0.1

Endereço MAC correspondente ao IP (associado via protocolo ARP) -> 00:00:00:aa:00:02 Tipo de rede -> [ether]

Interface de rede local -> eth()

2.2. a) Questão: Qual é o valor hexadecimal dos endereços MAC origem e destino? Como interpreta e justifica o endereço destino usado?

Resposta:

```
▼ Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: Broadcast (ff:ff:ff:ff:ff:ff) 
▶ Destination: Broadcast (ff:ff:ff:ff:ff) 
▶ Source: 00:00:00_aa:00:01 (00:00:00:aa:00:01) 
Type: ARP (0x0806)
```

Endereço MAC origem -> 00:00:00_aa:00:01

Endereco MAC destino -> ff:ff:ff:ff:ff

É usado o endereço MAC destino ff:ff:ff:ff:ff pois trata-se de uma mensagem Broadcast, para todos os dispositivos na rede do endereço de origem (00:00:00_aa:00:01), pois este pretende saber o endereço MAC proprietário do endereço *IP 10.0.0.1*

2.2. b) Questão: Qual o valor hexadecimal do campo Type da trama Ethernet? O que indica?

Resposta: Valor Hexadecimal do *Type*: 0x806

Indica que os dados do campo protocolar superior são um pacote ARP.

2.2. c) Questão: Observando a mensagem ARP, como pode saber que se trata efetivamente de um pedido ARP? Refira duas formas distintas de obter essa informação.

Resposta: Podemos concluir que se trata de um pedido *ARP* analisando os campos *Opcode e Target MAC address.*

Podemos ver que o valor no campo é 1, mostrando assim que se trata de um pedido. No campo *Target MAC address* está o endereço *00:00:00:00:00:00* pois não é ainda conhecido o MAC destino. Desta forma, conseguimos ter a certeza que se trata de um pedido *ARP*.

2.3. a) Questão: Qual o valor do campo ARP opcode? O que especifica?

Resposta: O valor do campo **Opcode** é 2, especificando assim que se trata de uma resposta *Arp*.

```
> Frame 79: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface veth1.0.95, id 0
> Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:01 (00:00:00:aa:00:01)

✓ Address Resolution Protocol (reply)

Hardware type: Ethernet (1)

Protocol type: IPv4 (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: reply (2)

Sender MAC address: 00:00:00_aa:00:02 (00:00:00:aa:00:02)

Sender IP address: 10.0.0.1

Target MAC address: 00:00:00_aa:00:01 (00:00:00:aa:00:01)

Target IP address: 10.0.0.21
```

2.3. b) Questão: Em que campo da mensagem ARP está a resposta ao pedido ARP efetuado?

Resposta: A resposta vem no campo Sender MAC address.

```
    Frame 79: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface veth1.0.95, id 0
    Ethernet II, Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02), Dst: 00:00:00_aa:00:01 (00:00:00:aa:00:01)
    *Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: 00:00:00_aa:00:02 (00:00:00:aa:00:02)
    Sender IP address: 10.0.0.1
    Target MAC address: 00:00:00_aa:00:01 (00:00:00:aa:00:01)
    Target IP address: 10.0.0.21
```

2.3. c) Questão: Identifique a que sistemas correspondem os endereços MAC de origem e de destino da trama em causa, recorrendo aos comandos ifconfig, netstat - rn e arp executados no host selecionado (Aladdin).

Resposta:

```
Sender MAC address: 00:00:00_aa:00:02 (00:00:00:aa:00:02)

Sender IP address: 10.0.0.1

Target MAC address: 00:00:00_aa:00:01 (00:00:00:aa:00:01)

Target IP address: 10.0.0.21
```

Executando o comando *ifconfig* no host Aladdin percebemos que endereço MAC : 00:00:00:aa:00:01 pertence a ele mesmo.

```
ineco zvvi;;zi premixien o4 scopeiu vxvvgiobaiz
ether 00:00:00:aa:00:01 txqueuelen 1000 (Ethernet)
DV ababata 172 butaa 01040 (01 o VD)
```

De seguida executando o comando *arp*, vemos que o endereço MAC : 00:00:00:aa:00:02, tem como endereço lógico *IP* o endereço 10.0.0.1.

Finalmente, aplicando o comando **netstat -rn** vemos que a rota *default* corresponde a esse mesmo endereço **IP** 10.0.0.1 .Podemos assim concluir que o endereço MAC : 00:00:00:aa:00:02 corresponde ao router R1.

```
Kernel IP routing table
                                                   Flags
                                                           MSS Window
                                                                        irtt Iface
                 Gateway
                                  Genmask
Destination
                                  0.0.0.0
255.255.255.0
0.0.0.0
                 10.0.0.1
                                                   UG
                                                             0.0
                                                                           0 eth0
10.0.0.0
                 0.0.0.0
                                                             0.0
                                                                           0 eth0
                                                   Ш
root@Aladdin:/tmp/pycore.37985/Aladdin.conf#
```

Resumindo:

Endereço MAC 00:00:00:aa:00:01 -> Aladdin Endereço MAC 00:00:00:aa:00:02 -> R1

2.3. d) Questão: Discuta, justificando, o modo de comunicação (unicast vs. broadcast) usado no envio da resposta ARP (ARP Reply).

Resposta: No envio da resposta *ARP (ARP Reply)*, o modo de comunicação usado é *unicast*, pois apenas o solicitador original recebe a resposta. Desta forma, é possível aumentar a segurança, reduzir o tráfego e sobrecarregamento das tabelas *ARP*, pois caso contrário todos os dispositivos iriam receber o pedido.

2.4) Questão: Verifique se a Jasmine teve conhecimento ou não de todo o tráfego gerado pelo acesso secreto do Aladdin? Qual será a razão para tal?

Resposta: A Jasmine teve acesso ao tráfego gerado pelo acesso secreto do Aladdin, pois estão ligados a um *Hub* que repete todo o tráfego para todas as portas.

No.	Time	Source	Destination	Protocol	Length Info
	82 93.572625	10.0.0.21	10.0.2.70	TCP	66 47344 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=158610935
	83 93.574118	10.0.0.21	10.0.2.70	SSHv2	108 Client: Protocol (SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.12)
	84 93.574141	10.0.2.70	10.0.0.21	TCP	66 22 → 47344 [ACK] Seq=1 Ack=43 Win=65152 Len=0 TSval=66900381
	85 93.589838	10.0.2.70	10.0.0.21	SSHv2	108 Server: Protocol (SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.12)
	86 93.589849	10.0.0.21	10.0.2.70	TCP	66 47344 → 22 [ACK] Seq=43 Ack=43 Win=64256 Len=0 TSval=1586109
	87 93.590025	10.0.0.21	10.0.2.70	TCP	1514 47344 → 22 [ACK] Seq=43 Ack=43 Win=64256 Len=1448 TSval=1586
	88 93.590026	10.0.0.21	10.0.2.70	SSHv2	154 Client: Key Exchange Init
	89 93.590055	10.0.2.70	10.0.0.21	TCP	66 22 → 47344 [ACK] Seq=43 Ack=1579 Win=63616 Len=0 TSval=66900
	90 93.591546	10.0.2.70	10.0.0.21	SSHv2	1114 Server: Key Exchange Init
	91 93.592950	10.0.0.21	10.0.2.70	SSHv2	114 Client: Diffie-Hellman Key Exchange Init
	92 93.597275	10.0.2.70	10.0.0.21	SSHv2	1182 Server: Diffie-Hellman Key Exchange Reply, New Keys, Encrypt
	93 93.636031	10.0.0.21	10.0.2.70	TCP	66 47344 → 22 [ACK] Seq=1627 Ack=2207 Win=64128 Len=0 TSval=158
	94 94.077681	10.0.0.1	224.0.0.5	OSPF	78 Hello Packet
	95 96.068626	10.0.0.21	10.0.2.70	SSHv2	82 Client: New Keys
	96 96.078601	10.0.0.1	224.0.0.5	OSPF	78 Hello Packet
	97 96.108175	10.0.2.70	10.0.0.21	TCP	66 22 → 47344 [ACK] Seq=2207 Ack=1643 Win=64128 Len=0 TSval=669
	98 96.108202	10.0.0.21	10.0.2.70	SSHv2	110 Client: Encrypted packet (len=44)
	99 96.108231	10.0.2.70	10.0.0.21	TCP	66 22 → 47344 [ACK] Seq=2207 Ack=1687 Win=64128 Len=0 TSval=669
	100 96.108306	10.0.2.70	10.0.0.21	SSHv2	110 Server: Encrypted packet (len=44)
	101 96.108316	10.0.0.21	10.0.2.70	TCP	66 47344 → 22 [ACK] Seq=1687 Ack=2251 Win=64128 Len=0 TSval=158
	102 96.108385	10.0.0.21	10.0.2.70	SSHv2	126 Client: Encrypted packet (len=60)

2.5) Questão: De igual modo, verifique se a Beauty teve conhecimento ou não de todo o tráfego gerado pelo acesso secreto do Beast? Qual será a razão para tal?

Resposta: A *Beauty* não teve acesso, pois estão ligados a um *Switch* que encaminha para a porta correta.

```
Protocol Length Info
                    fe80::200:ff:fe... ff02::5
                                                                                90 Hello Packet
78 Hello Packet
  1 0.0000000...
 2 0.0174106... 10.0.2.1
                                            224.0.0.5
                                                                    0SPF
 3 2.0175524... 10.0.2.1
                                            224.0.0.5
                                                                    0SPF
                                                                                 78 Hello Packet
                                                                                 70 Router Solicitation from 26:23:76:23:77:96
  4 3.9326154... fe80::2423:76ff... ff02::2
                                            224.0.0.5
                                                                                 78 Hello Packet
 5 4.0177931... 10.0.2.1
                                                                    0SPF
 7 8.0182599... 10.0.2.1 224.0.0. 8 8.0285960... fe80::200:ff:fe... ff02::2 9 10.010156... fe80::200:ff:fe... ff02::5
                                            224.0.0.5
                                                                    OSPF
                                                                                 78 Hello Packet
78 Hello Packet
                                             224.0.0.5
                                                                     ICMP...
                                                                                 70 Router Solicitation from 00:00:00:aa:00:07
10 10.018352... 10.0.2.1 224.0.0.5
11 10.076596... fe80::e4e6:83ff... ff02::2
12 12.018749... 10.0.2.1 224.0.0.5
13 13.378269... fe80::e4e6:83ff... ff02::fb
                                                                                 78 Hello Packet
                                            224.0.0.5
                                                                    OSPF
                                                                    ICMP...
OSPF
                                                                                 70 Router Solicitation from 0e:46:4c:32:ac:36
78 Hello Packet
                                            224.0.0.5
                                                                    MDNS
                                                                              203 Standard query 0x0000 PTR _nfs._tcp.local, "QM" question PTR...
14 14 .019066... 10.0.2.1 224.0.0.5
15 14.307531... fe80::2423:76ff... ff02::fb
                                                                               203 Standard guery 0x0000 PTR nfs. tcp.local, "OM" guestion PTR...
                                                                    MDNS
16 16.019425... 10.0.2.1
17 18.019729... 10.0.2.1
                                                                                 78 Hello Packet
78 Hello Packet
                                             224.0.0.5
                                                                    OSPF
18 20.019882... 10.0.2.1 224.0.0.5
19 20.029340... fe80::200:ff:fe... ff02::5
20 20.316780... fe80::200:ff:fe... ff02::2
                                                                    0SPF
                                                                                 78 Hello Packet
                                                                                 90 Hello Packet
                                                                                 70 Router Solicitation from 00:00:00:aa:00:06
21 20.316848... fe80::200:ff:fe... ff02::2
                                                                                 70 Router Solicitation from 00:00:00:aa:bb:70
```

2.6) Questão: Consulte a tabela ARP do Aladdin e do Beast. Que principal diferença entre as tabelas obtidas e que impacto tem no funcionamento da rede?

Resposta:

Tabela do Aladdin:

```
root@Aladdin:/tmp/pycore.39819/Aladdin.conf# arp -a
? (10.0.0.1) at 00:00:00:aa:00:02 [ether] on eth0
```

Tabela do Beast:

```
root@Beast:/tmp/pycore.39819/Beast.conf# arp -a
? (10.0.2.70) at 00:00:00:aa:bb:70 [ether] on eth0
root@Beast:/tmp/pycore.39819/Beast.conf#
```

Como podemos ver, *Aladdin* tem conhecimento do endereço MAC do router a que está ligado, enquanto *Beast* tem conhecimento do endereço MAC do servidor destino.

Isto acontece pois **Beast** encontra-se na mesma rede que o servidor podendo assim fazer ligação direta com o mesmo, situação que não acontece com o **Aladdin.**

2.7) Questão: Esboce um diagrama em que ilustre claramente, e de forma cronológica, todo o tráfego layer 2 (tramas) entre o Aladdin e os hosts com os quais comunica, até à receção do primeiro pacote que contém dados do acesso remoto.

```
Resposta:
```

```
[Aladdin]
|--[1] ARP Request: "Quem tem 10.0.0.1?" (para Gateway R1)
| H1 Switch]
| [Router R1]
| --[2] ARP Reply: "10.0.0.1 é 00:00:00:aa:00:02" (MAC de R1)
| [Aladdin]
| --[3] TCP SYN → 10.0.2.10:22 (primeira tentativa SSH)
| [H1] → R1 → R0 → SW1 → DServer
| [DServer]
| --[4] TCP SYN-ACK ← resposta do DServer
| [Aladdin]
| --[5] TCP ACK → estabelece conexão
| --[6] Primeiro pacote com dados SSH (criptografado)
```

2.8) Questão: Construa manualmente a tabela de comutação completa do switch da casa da Beauty e do Beast, (SW1) atribuindo números de porta à sua escolha.

Resposta:

Podemos ver, analisando o pedido Arp de Beast que o seu MAC é 00:00:00_aa:00:07

```
▶ Frame 41: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface veth8.0.95, id 0
▼ Ethernet II, Src: 00:00:00_aa:00:07 (00:00:00:aa:00:07), Dst: Broadcast (ff:ff:ff:ff:ff)
▼ Destination: Broadcast (ff:ff:ff:ff:ff)
▼ Source: 00:00:00_aa:00:07 (00:00:00:aa:00:07)
    Type: ARP (0x0806)
▼ Address Resolution Protocol (request)
```

MAC addres Porta 00:00:00:aa:bb:70 Fa0/1

00:00:00_aa:00:07 Fa0/2

3.1) Questão: Como proteção, a Jasmine e o Aladdin, juntamente com a Beauty e o Beast, decidiram conectar R1 e Rxy a uma rede de um ISP com endereços IP públicos, mantendo todo o endereçamento privado das suas LANs. Sabe-se que o ISP não encaminha tráfego para redes privadas, portanto, R1 e Rxy não conseguem encaminhar tráfego para endereços privados remotos, i.e., não fisicamente adjacentes.

Discuta que solução implementaria em R1 e em Rxy de modo a manter todas as funcionalidades anteriormente existentes (conectividade IP, acesso ssh ao servidor, etc.).

Resposta:

Para garantir que tudo continue a funcionar como anteriormente — incluindo o acesso SSH ao servidor e a comunicação entre dispositivos nas redes internas — é necessário configurar tradução de endereços de rede (NAT), mais concretamente NAT com sobrecarga (PAT), nos routers R1 e R70.

Como o fornecedor de serviços de Internet (ISP) apenas encaminha tráfego com endereços IP públicos, os IPs privados das LANs não são diretamente acessíveis a partir do exterior. Ao implementar PAT, os routers passam a substituir os IPs privados de origem por um IP público atribuído pelo ISP, associando cada ligação a uma porta específica. Desta forma, vários dispositivos podem partilhar o mesmo IP público sem conflitos, porque são diferenciados pelas portas.

Quando os pacotes de resposta chegam ao router, este utiliza a tabela de traduções para devolver os dados ao equipamento correto dentro da rede privada. Desta forma, é mantido o esquema de endereçamento privado nas redes locais, é permitido que o tráfego saia da rede interna usando um IP público, compatível com as regras do ISP e garante-se que todas as funcionalidades anteriores, como o acesso remoto por SSH, continuem operacionais sem alterações no funcionamento do sistema.

PARTE II

1. Acesso Rádio

```
Wireshark - Packet 70 · WLAN-traffic-20250407.pcapng

Frame 70: 305 bytes on wire (2440 bits), 305 bytes captured (2440 bits) on interface en0, id 0
Radiotap Header v0, Length 36
802.11 radio information
PHY type: 802.11g (ERP) (6)
Short preamble: False
Proprietary mode: None (0)
Data rate: 1,0 Mb/s
Channel: 1
Frequency: 2412MHz
Signal strength (dBm): -86dBm
Noise level (dBm): -93dBm
Signal/noise ratio (dB): 7dB
TSF timestamp: 2852627266
| [Duration: 2344µs]
| IEEE 802.11 Beacon frame, Flags: ..... C
| IEEE 802.11 Wireless Management
| Fixed parameters (12 bytes)
Timestamp: 6076142901170
Beacon Interval: 0,102400 [Seconds]
| Capabilities Information: 0x1411
```

Trama 802.11 referente ao grupo

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

Resposta: Como se pode analisar na figura, a frequência é 2412MHz, a operar no canal 1.

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

Resposta: 802.11g

1.3 Questão: Qual a taxa de transmissão a que foi enviada a trama escolhida? Será que essa taxa de transmissão corresponde à máxima que a interface Wi-Fi pode operar? Justifique.

Resposta:

Como podemos analisar, a trama tem capacidades da norma IEEE 802.11n (que tem uma velocidade de transmissão de 600Mbps), mas foi transmitida a 1Mbp (taxa de transmissão normal das Beacon Frames - usam as taxas de transmissão mais baixas possíveis). Esta informação pode ser consultada na imagem abaixo:

```
MAC timestamp: 285262720
Flags: 0x10
Data Rate: 1,0 Mb/s
Channel frequency: 2412
Channel flags: 0x0480 3
```

2. Scanning Passivo e Scanning Ativo

2.4 Questão: Selecione uma trama beacon cuja ordem (ou terminação) corresponda ao seu ID de grupo. Esta trama pertence a que tipo de tramas 802.11? Identifique o valor dos identificadores de tipo e de subtipo da trama. Em que parte concreta do cabeçalho da trama estão especificados (ver Anexo I)?

```
Frame Control Field: 0x8000

Frame Control Field: 0x8000

.000 0000 0000 0000 = Duration: 0 microsec

Frame Control Field: 0x8000

......00 = Version: 0

.....00... = Type: Management frame (0)

1000 .... = Subtype: 8
```

Resposta: Foi escolhida a mesma trama das alíneas anteriores, por ser a primeira trama que cumpre o requisito pedido. Pertence, como já vimos, às tramas do tipo 802.11g. Identificador de tipo: 00

Identificador de subtipo: 0008

Esta parte encontra-se identificada no cabeçalho da trama, nos bits referentes ao Frame Control. O Type ocupa 2 bits (neste caso, 00 - indica que a trama é do tipo "Management"), e o Subtype ocupa 4 bits(neste caso, 1000 - indica que a trama é do subtipo "Beacon").

2.5 Questão: Verifique se está a ser usado o método de deteção de erros (CRC). Justifique. (Poderá ter de ativar a verificação no Wireshark, em Edit -> Preferences -> Protocols -> IPv4 -> "Validate Checksum if Possible")

```
.... 0000 = Fragment number: 0
  0101 1011 0001 .... = Sequence number: 1457
  Frame check sequence: 0x19191dec [unverified]
   [FCS Status: Unverified]
IEEE 802.11 Wireless Management
    no cimescamp, 2002021200

▼ Flags: 0x10
     .... ...0 = CFP: False
      .... ..0. = Preamble: Long
      .... .0.. = WEP: False
     .... 0... = Fragmentation: False
     ...1 .... = FCS at end: True
      ..0. .... = Data Pad: False
      .0.. .... = Bad FCS: False
     0... = Short GI: False
   Data Rate: 1.0 Mb/s
```

Resposta: As tramas Beacon têm um campo, FCS (Frame Check Sequence), nos últimos 4 bytes, para deteção de erros. Esta, como está marcada a "unverified", significa que está a ser usada, mas não verificada. O bit na flag simplesmente refere-se à existência do FCS no fim da trama.

2.6 Questão: Justifique o porquê de ser necessário usar deteção de erros em redes sem fios.

Resposta: A deteção de erros em redes sem fios (WI-FI, Bluetooth, entre outras) é essencial devido às características do meio de transmissão (o ar). Como este é mais propenso a alterações e/ou perturbações, a interferência dos dados torna-se mais provável do que em redes com fios. Um dos aspetos que leva a este processo é o Path Loss, ou a atenuação do sinal, produzido por obstáculos naturais, ou simplesmente pelo aumento da distância até aos APs.

Além disso, sinais de outros dispositivos ativos na zona podem colidir com o sinal que se quer transmitir, podendo causar corrupção dos dados.

2.7 Questão: Uma trama beacon anuncia o intervalo entre beacons às várias taxas de transmissão (B) que o AP suporta, assim como várias taxas de transmissão adicionais (extended supported rates). Indique qual a periodicidade e as taxas de transmissão suportadas pelo AP da trama beacon selecionada.

```
Timestamp: 6076142901170
Beacon Interval: 0,102400 [Seconds]

Capabilities Information: 0x1411

Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 18, 24, 36, 54, [Mbit/sec]
Tag Number: Supported Rates (1)
Tag length: 8
Supported Rates: 1(B) (0x82)
Supported Rates: 2(B) (0x84)
Supported Rates: 5.5(B) (0x8b)
Supported Rates: 11(B) (0x96)
Supported Rates: 18 (0x24)
Supported Rates: 24 (0x30)
Supported Rates: 36 (0x48)
Supported Rates: 54 (0x6c)
```

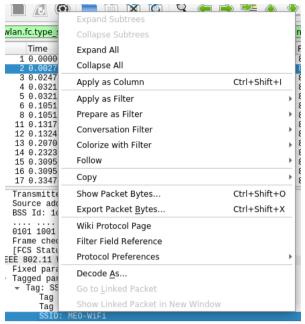
Resposta: O intervalo entre beacons transmitidos é de 0.1024 *100 = 102.4 microsegundos (valor obtido através da primeira print). Na segunda imagem, podemos observar quatro valores de taxas básicas (as marcadas com B), que são as taxas básicas que todos os dispositivos que se conectam à AP têm de suportar. As outras taxas (18, 24, 36 e 54 Mbps) não são obrigatórias, mas podem ser usadas, caso seja possível.

2.8 Questão: Identifique e liste os SSIDs dos APs que estão a operar na vizinhança da STA de captura. Explicite o modo como obteve essa informação (por exemplo, se usou algum filtro para o efeito).

```
(wlan.fc.type_subtype == 0x08 || wlan.fc.type_subtype == 0x05) && wlan.ssid

Resposta:
```

Foi aplicado o seguinte filtro: "wlan.fc.type_subtype == 0x08" e "wlan.fc.type_subtype == 0x05" filtram as tramas, para apenas mostrar as do tipo Beacon ou Probe Response, respetivamente, as únicas que contêm (ou podem conter) a tag SSID preenchida. O segundo filtro, "wlan.ssid", certifica-se que são excluídas todas as tramas destes tipos que não tenham o campo SSID preenchido.



De seguida, clicou-se com o botão direito num item "SSID" de uma trama aleatória, e escolheu-se a opção "Apply as Column." Podemos assim, listar todos os SSID que estão a operar.

No. Time	Source	Destination	Protocol L	ength SSID ▲ Ir	nfo
62329 293.891108	a6:ef:15:08:32:99	Broadcast	802.11	222 phi_F41927C3C600 B	leacon frame, SN=1454, FN=0, Flags=C, BI=100, SSID=ph
62270 293.679820	a6:ef:15:08:32:99	Broadcast	802.11		eacon frame, SN=1452, FN=0, Flags=C, BI=100, SSID=ph
62125 293.168034	a6:ef:15:08:32:99	Broadcast	802.11		leacon frame, SN=1447, FN=0, Flags=C, BI=100, SSID=ph
62047 292.963297	a6:ef:15:08:32:99	Broadcast	802.11		leacon frame, SN=1445, FN=0, Flags=C, BI=100, SSID=ph
61975 292.862321	a6:ef:15:08:32:99	Broadcast	802.11	222 phi_F41927C3C600 B	eacon frame, SN=1444, FN=0, Flags=C, BI=100, SSID=ph
80 1.432/29	a0:e1:15:08:32:99	Broaucast	802.11	ZZZ DUT_F419Z/C3C000	Beacon Trame, SN=23/3, FN=0, F1ags=, B1=100, SSID=pn
62405 294.129474	Tp-LinkT_f1:af:69	Broadcast	802.11	306 Vodafone-D0ED8A	Beacon frame, SN=2095, FN=0, Flags=C, BI=100, SSID=Vo
62283 293.720544	Tp-LinkT_f1:af:69	Broadcast	802.11	306 Vodafone-D0ED8A	Beacon frame, SN=2091, FN=0, Flags=C, BI=100, SSID=Vo
62230 293.518867	Tp-LinkT_f1:af:69	Broadcast	802.11	306 Vodafone-D0ED8A	Beacon frame, SN=2089, FN=0, Flags=C, BI=100, SSID=Vo
752 9.557105	Tp-LinkT_f1:af:69	Broadcast	802.11	1 306 Vodafone-D0FD8	BA Beacon frame, SN=2987, FN=0, Flags=C, BI=100, SSID=Vo
51027 273.434238	d0:cf:0e:95:fd:24	Broadcast	802.11		Beacon frame, SN=1466, FN=0, Flags=C, BI=100, SSID=NO
46020 244.660480	d0:cf:0e:95:fd:24	Broadcast	802.11		Beacon frame, SN=1153, FN=0, Flags=C, BI=100, SSID=NO
61816 292.542114	fc:77:7b:ee:c8:b6	Broadcast	802.11		Beacon frame, SN=1020, FN=0, Flags=C, BI=100, SSID=NO
4/1 0.229808	IC://:/D:ee:C8:D0	Broaucast	802.11	424 NUS-U8B0	Beacon Irame, SN=2139, FN=0, F1ags=, B1=100, SS1D=NU
62472 294.855987	40:ed:00:8e:b3:f8	Broadcast	802.11	276 NOS-9946 EXT	Beacon frame, SN=2328, FN=0, Flags=C, BI=100, SSID=NO
62394 294.035175	40:ed:00:8e:b3:f8	Broadcast	802.11	276 NOS-9946 EXT	Beacon frame, SN=2314, FN=0, Flags=C, BI=100, SSID=NO
62335 293.931093	40:ed:00:8e:b3:f8	Broadcast	802.11	276 NOS-9946 EXT	Beacon frame, SN=2313, FN=0, Flags=C, BI=100, SSID=NO
201 4.034330	40.cu.00.0c.po.10	DI VAUCAS L	002.11	210 NO3-3340_EAI	DEACUTE FEATURE, SW-2129, FW-0, F1493 D1-100, SSID-NU
62327 293.884750	HitronTe_4d:52:c6	Broadcast	802.11	329 NOS-52C6	Beacon frame, SN=2662, FN=0, Flags=C, BI=100, SSID=NO
62090 293.081300	HitronTe_4d:52:c6	18:87:40:ea:8c:e6	802.11	453 NOS-52C6	Probe Response, SN=615, FN=0, Flags=C, BI=100, SSID=N
389 5.321190	HitronTe_4d:52:c6	Broadcast	802.11	329 NOS-52C6	Beacon frame, SN=3541, FN=0, Flags=
62446 294.597440	90:aa:c3:e5:26:f6	Broadcast	802.11	329 NOS-26F6	Beacon frame, SN=2885, FN=0, Flags=C, BI=100, SSID=NO
62436 294.494766	90:aa:c3:e5:26:f6	Broadcast	802.11	329 NOS-26F6	Beacon frame, SN=2884, FN=0, Flags=C, BI=100, SSID=NO
213 3.003300	30.aa.b3.c3.20.10	DIVAULASE	002.11	323 NU3-20FU	DEALUH HAME, SN-STOI, FN-U, FIAYS, DI-100, SSID-NU
63029 300.872923	PTInovac_29:a9:c0	BeijingX_0a:80:66	802.11		xo Probe Response, SN=2470, FN=0, Flags=RC, BI=100, SSID=
63028 300.872874	PTInovac 29:a9:c0	BeijingX_0a:80:66	802.11		xo Probe Response, SN=2470, FN=0, Flags=RC, BI=100, SSID=
62996 300.233694	PTInovac_29:a9:c0	Broadcast	802.11		xo Beacon frame, SN=2456, FN=0, Flags=C, BI=100, SSID=Ma
62986 300.129266	PTInovac_29:a9:c0	Broadcast	802.11		xo Beacon frame, SN=2454, FN=0, Flags=C, BI=100, SSID=Ma
09 1.Z000/Z	PIINOVAC_Z9:a9:C0	COLLTHELL 32:D0:5T	8⊌Z.II		XO Probe Response, SN=3847, FN=0, Flags=, B1=100, SSID=
63032 300.888276	PTInovac_9b:f2:a2	Broadcast	802.11	230 MEO-WiFi	Beacon frame, SN=193, FN=0, Flags=C, BI=100, SSID=MEO
63031 300.882115	PTInovac_29:a9:c2	BeijingX_0a:80:66	802.11	240 MEO-WiFi	Probe Response SN=2471 EN=0 Flags= R C RT=100 SSTD=
62025 200 057250 2 0.002/92	10:57:20:fc:f0:02 10:5/:30:T0:T⊎:82	Broadcast	002.11 802.11	230 MEO WiFi 230 MEU-W1F1	Beacon Frame CN-2967 FM-0 Flags DT-400 SCTD-ME Beacon Trame, SN=1430, FN=0, Flags
62988 300.136892	1c:57:3e:fc:f0:a2	Broadcast	802.11	305 MEO-FCF0A0	Beacon frame, SN=3342, FN=0, Flags=C, BI=100, SSID=ME
62945 299.629271	1c:57:3e:fc:f0:a0	Broadcast	802.11	305 MEO-FCF0A0	Beacon frame, SN=3332, FN=0, Flags=C, BI=100, SSID=ME
62936 299.522711	1c:57:3e:fc:f0:a0	Broadcast	802.11	305 MEO-FCF0A0	Beacon frame, SN=3330, FN=0, Flags=C, BI=100, SSID=ME
3/34 3⊎.000411	PIINOVAC T1:/5:/8	Broadcast	802.11	305 MEU-F1/5/0	Beacon Trame, SN=18/, FN=U, F1ags= B1=10U, SS1D=MEU
63022 300.785721	PTInovac_9b:f2:a0	Broadcast	802.11	337 MEO-9BF2A0	Beacon frame, SN=190, FN=0, Flags=C, BI=100, SSID=MEO
63019 300.683170	PTInovac 9b:f2:a0	Broadcast	802.11	337 MEO-9BF2A0	Beacon frame, SN=188, FN=0, Flags=C, BI=100, SSID=MEO
63010 300.580931	PTInovac 9b:f2:a0	Broadcast	802.11	337 MEO-9BF2A0	Beacon frame, SN=185, FN=0, Flags=C, BI=100, SSID=MEO
4 U.U3Z1/8	PIINOVAC_9D:IZ:a⊎	Broaucast	802.II	331 MEU-9BFZAU	Beacon Trame, SN=1319, FN=0, F1ags= B1=100, SSID=ME
61786 292.331103	PTInovac_85:4c:80	Broadcast	802.11	305 MEO-854C80	Beacon frame, SN=3224, FN=0, Flags=C, BI=100, SSID=ME
59644 286.699170	PTInovac_85:4c:80	Broadcast	802.11	305 MEO-854C80	Beacon frame, SN=3102, FN=0, Flags=C, BI=100, SSID=ME
53237 282.501767	PTTnovac 85:4c:80	Broadcast	802.11	305 MFO-854C80	Beacon frame, SN=3012, FN=0, Flags=C. BT=100, SSID=ME
62586 295.379097	PTInovac_82:88:30	Broadcast	802.11	337 MEO-828830	Beacon frame, SN=1752, FN=0, Flags=C, BI=100, SSID=ME
62569 295.174312	PTInovac_82:88:30	Broadcast	802.11	337 MEO-828830	Beacon frame, SN=1732, FN=0, Flags=C, BI=100, SSID=ME
62462 204 764770	DTTnovac 82:88:30	Broadcast	QQ2 11	337 MED-020000	Reacon frame SN-17/A EN-A Elade- C RT-18A SSTD-ME
312 4.3590/5	PI1novac_82:88:30	Broadcast	802.11	33/ MEO-828830	Beacon frame, SN=29, FN=0, Flags=C, B1=100, SSID=MEO
62464 294.793813	PTInovaç_66:db:70	Broadcast	802.11	337 MEO-66DB70	Beacon frame, SN=364, FN=0, Flags=C, BI=100, SSID=MEO
62395 294.077088	PTInovaç_66:db:70	Broadcast	802.11	337 MEO-66DB70	Beacon frame, SN=347, FN=0, Flags=C, BI=100, SSID=MEO
62323 293.872276	PTTnovac_66:db:70	Broadcast	802.11	337 MEO-66DB70	Beacon frame, SN=343, FN=0, Flags=C. BT=100, SSTD=MF0
62599 295.464934	f0:09:0d:ba:0e:0e	Broadcast	802.11	274 GVBRAGA_quarto	Beacon frame, SN=1933, FN=0, Flags=C, BI=100, SSID=GV
62585 295.361738	f0:09:0d:ba:0e:0e	Broadcast	802.11	274 GVBRAGA quarto	Beacon frame, SN=1932, FN=0, Flags=C, BI=100, SSID=GV
62434 294.443097	f0:09:0d:ba:0e:0e	Broadcast	802.11	274 GVBRAGA_quarto	Beacon frame, SN=1923, FN=0, Flags=C, BI=100, SSID=GV
3304 200 00000	10.00.0d.ba.0e.0e	THICKTOOL TO TA 'AC	002.11	206 GVDRAGA quarto	Proue Response, 3N-2006, FN-0, Frays
63027 300.866701	dc:62:79:31:e2:39	BeijingX_0a:80:66	802.11	237 GVBRAGA EXT	Probe Response, SN=4087, FN=0, Flags=C, BI=100, SSID=
63026 300.860456	dc:62:79:31:e2:39	BeijingX_0a:80:66	802.11	237 GVBRAGA EXT	Probe Response, SN=4086, FN=0, Flags=C, BI=100, SSID=
62024 200 047002	460.70.040.00	Proadcast Annadosst	002.11	257 GVBRAGA_EXT	Docon framo CM-4005 FM-0 Flage C DT-400 CCTD-CV
Z41 3.443334	UC.UZ.13.J1.E2.J3				Poscon framo CN-4005 FN-0 Flags
62473 294.901413	d0:cf:0e:7f:87:74	Broadcast	802.11	363 GVBRAGA	Beacon frame, SN=2306, FN=0, Flags=C, BI=100, SSID=GV
62466 294.797037	d0:cf:0e:7f:87:74	Broadcast	802.11	363 GVBRAGA	Beacon frame, SN=2305, FN=0, Flags=C, BI=100, SSID=GV
1,5011,510,510510	00.00.00.75.07.75	D. outoude	202.11	202 2727.12.	Boulon f. ame, SN 2020, FN 0, Flago BI 100, COID SN.
63030 300.882107	HitronTe_f3:9a:46	Broadcast	802.11	362 FlyingNet	Beacon frame, SN=1782, FN=0, Flags=C, BI=100, SSID=F1
63021 300.779575	HitronTe_f3:9a:46	Broadcast	802.11	362 FlyingNet	Beacon frame, SN=1781, FN=0, Flags=C, BI=100, SSID=F1
			44		200 2 MM 18 N 11222 N NT 200 COTS E1

Aqui estão alguns exemplos de todos os SSIDs diferentes a operar.

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

```
Resposta: wlan.fc.type_subtype == 0x05 || wlan.fc.type_subtype == 0x04  
"wlan.fc.type_subtype == 0x04" -> filtra tramas probing request;  
"wlan.fc.type_subtype == 0x05" -> filtra tramas probing response
```

2.10 Questão: Assuma que a STA de captura consegue-se associar a qualquer AP na vizinhança. Dadas as tramas recebidas através do scanning ativo e passivo, observe os valores da força do sinal (Signal Strength) nas meta-informações de nível físico e indique a qual AP a STA de captura se deve associar para obter a melhor qualidade de ligação possível. Indique como chegou a esta resposta.

Resposta: Foi aplicado um filtro diferente, "wlan.fc.type_subtype == 0x05 || wlan.fc.type_subtype == 0x08", para mostrar apenas as tramas que contêm o RSSI do AP. Foi adicionada uma coluna, para mostrar os valores da força do sinal (em dBm) da trama. Assim, conseguimos ver que a trama com maior RSSI é a seguinte:

No.	Time	Source	Destination	Protocol	Length SSID	Info	Signal strength (dBm)
39127	191.415288	HitronTe f3:9a:46	Broadcast	802.11	362 FlvingNet	Beacon frame, SN=672, FN=0, Flags=C, BI=100, SSID=Fly	-39dBm

2.11 Questão: Os valores de taxa de transmissão do Wi-Fi estão diretamente associados à qualidade da receção do sinal. Considerando os valores de sensibilidade mínima (Minimum Sensivity) e taxa de transmissão (Data Rate) que constam nas tabelas de referência (ver Anexo II), e a força do sinal recebido nas tramas do AP identificado na resposta anterior, estime o débito que a STA obterá nessa ligação.

Resposta: O valor obtido (-39 dBm) é muito superior aos requisitos de sensibilidade mínima para todas as modulações. Isso significa que a STA pode operar no maior nível de modulação suportado pelo AP (que aqui é 64–QAM 5/6).

Como aqui se assume que todos os dispositivos IEEE 802.11n utilizam um GI de 800ns, podemos inferir pela tabela do Anexo II que o débito será de 65Mbps.

3. Processo de Associação

3.12 Questão: Identifique uma sequência de tramas que corresponda a um processo de associação realizado com sucesso entre a STA e o AP, incluindo a fase de autenticação.

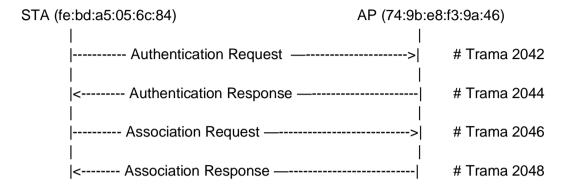
Resposta: Foi aplicado o filtro "wlan.fc.type_subtype == 0x00 || wlan.fc.type_subtype == 0x01 || wlanc.fc.type_subtype == 0x0b)", em que "0x00" corresponde às tramas Association Request, "0x01" corresponde às tramas Association Response, e "0x0b" corresponde às tramas de autenticação.

Assim, foi identificada a seguinte sequência de tramas, que representam um processo de associação entre a STA e o AP:

No	o. ▼ Time	Source	Destination	Protocol	Length Info	MAC
	2042 23.707373	fe:bd:a5:05:6c:84	HitronTe_f3:9a:46	802.11	106 Authentication, SN=3343, FN=0, Flags=	74:9b:e8:f3:9a:46,fe:bd:a5:05:6c:84,74:9b:e8:f3:9a:46
	2044 23.707398	HitronTe_f3:9a:46	fe:bd:a5:05:6c:84	802.11	70 Authentication, SN=3852, FN=0, Flags=	fe:bd:a5:05:6c:84,74:9b:e8:f3:9a:46,74:9b:e8:f3:9a:46
	2046 23.710405	fe:bd:a5:05:6c:84	HitronTe_f3:9a:46	802.11	202 Association Request, SN=3344, FN=0, Fla	74:9b:e8:f3:9a:46, fe:bd:a5:05:6c:84, 74:9b:e8:f3:9a:46
	2048 23.716772	HitronTe_f3:9a:46	fe:bd:a5:05:6c:84	802.11	210 Association Response, SN=3853, FN=0, F1	fe:bd:a5:05:6c:84,74:9b:e8:f3:9a:46,74:9b:e8:f3:9a:46

3.13 Questão: Efetue um diagrama que ilustre a sequência de todas as tramas trocadas no processo.

Resposta:



4. Transferência de Dados

4.14 Questão: Estabeleça um filtro apropriado e selecione uma trama de dados (Data ou QoS Data), cujo número de ordem inclua o seu identificador de grupo (terminação xy, ou y caso não exista xy). Sabendo que o campo Frame Control contido no cabeçalho das tramas 802.11 permite especificar a direcionalidade das tramas, o que pode concluir face à direcionalidade dessa trama, será local à WLAN?

Resposta: Foi aplicado o filtro "wlan.fc.type == 2 || wlan.fc.type == 1", para filtrar as tramas de dados, e as tramas de controlo, respetivamente. Seguindo as indicações, foi escolhida a trama 1170, do tipo QoS Data.

```
Type/Subtype: QOS Data (⊎X⊎⊎28)

Frame Control Field: 0x8841

......00 = Version: 0

.....10... = Type: Data frame (2)

1000 .... = Subtype: 8

Flags: 0x41

......01 = DS status: Frame from STA to DS via an AP (To DS: 1 From DS: 0) (0x1)

.....0... = More Fragments: This is the last fragment

....0... = Retry: Frame is not being retransmitted

...0.... = PWR MGT: STA will stay up

..0.... = More Data: No data buffered

.1.... = Protected flag: Data is protected

0..... = Order flag: Not strictly ordered
```

Como podemos analisar pelas Flags, a trama foi enviada por uma STA para um AP, sendo, assim, local à WLAN (ainda não saiu para uma rede externa).

4.15 Questão: Para a trama de dados selecionada, transcreva os endereços MAC em uso, identificando quais os endereços correspondentes à estação sem fios (STA), ao AP e ao router de acesso ao sistema de distribuição (DS)?

Resposta: Os endereços MAC são "d0:cf:0e:7f:87:74", "de:62:79:01:e2:39" e "ff:ff:ff:ff:ff:ff:ff:ff: O primeiro corresponde ao da STA (que é o que envia a trama), o segundo pertence ao AP, e o DS, neste caso, não está presente nos endereços, já que o destino é Broadcast

(endereço ff:ff:ff:ff:ff:ff), não estando a ser direcionada para um DS externo, como vimos na questão anterior.

4.16 Questão: O uso de tramas Request To Send e Clear To Send, apesar de opcional, é comum para efetuar "pré-reserva" do acesso ao meio quando se pretende enviar tramas de dados, com o intuito de reduzir o número de colisões resultante maioritariamente de STAs escondidas. Para o envio de dados selecionado acima, verifique se está a ser usada a opção RTS/CTS na troca de dados entre a STA e o AP/Router da WLAN, identificando a direcionalidade das tramas e os sistemas envolvidos. Dê um exemplo de uma transferência de dados em que é usada a opção RTC/CTS e um outro em que não é usada.

Resposta: Nesta trama em específico não está a ser usado o RTS/CTS, pois não é uma característica inerente das tramas Broadcast, estando presente apenas nas comunicações fim-a-fim.

Exemplo com RTS/CTS: Trama 181 (Tramas de Dados) Exemplo sem RTS/CTS: Trama 1170 (Tramas de Gestão)

Conclusão

Com este projeto, conseguimos entender como funcionam na prática as redes - desde a transmissão de dados em redes cabladas, até às redes sem fios. Percebemos, ao analisar as tramas Ethernet fornecidas, a importância e funcionalidade dos switches e dos hubs, e como gerem o tráfego de diferentes formas.

Os exercícios relativos ao protocolo ARP esclareceram e solidificaram o nosso conhecimento. Através da prática e da análise pelo *wireshark* foi possível compreender melhor os pedidos e respostas ARP, a importância da tabela ARP para o desempenho da rede e como o protocolo é fundamental para a comunicação entre dispositivos.

O NAT e o PAT também ficaram consolidados durante as atividades, permitindo uma compreensão mais clara de como esses mecanismos funcionam na tradução de endereços em redes privadas e no compartilhamento de um único endereço IP público entre múltiplos dispositivos.

Aprendemos, na segunda parte, os diferentes tipos de tramas que existem, as diferenças entre estas, e a analisar o efeito de vários fatores na qualidade da ligação, como a força do sinal ou a velocidade de transmissão.

Com tudo isso, podemos afirmar que foi uma oportunidade valiosa para aplicar os conceitos teóricos em cenários reais, e assim aprofundar o nosso conhecimento sobre a disciplina em geral.