

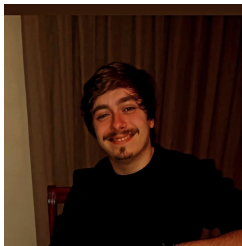
Redes de Computadores

Relatório Trabalho Prático 3

Nível de Ligação Lógica: Redes Ethernet, Protocolo ARP e Redes Locais sem Fios (Wi-Fi)

Grupo 89 LEI - 2º Ano - 2º Semestre

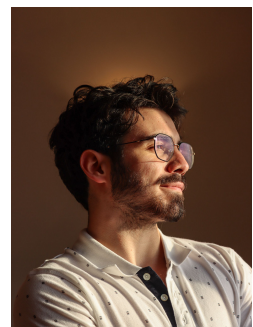
Ano Letivo 2024/2025



Tiago Guedes
A97369



Diogo Goncalves
A101919



Tiago Carneiro
A93207

Braga,
4 de junho de 2025

Conteúdo

1	Parte 1	3
1.1	Captura e análise de Tramas Ethernet	3
1.2	Protocolo ARP e Domínios de Colisão	6
1.3	Serviço de NAT/PAT	11
2	Parte 2	12
2.1	Acesso Rádio	12
2.2	Scanning Passivo e Scanning Ativo	13
2.3	Processo de Associação	17
2.4	Transferência de Dados	18
3	Conclusões	20

Lista de Figuras

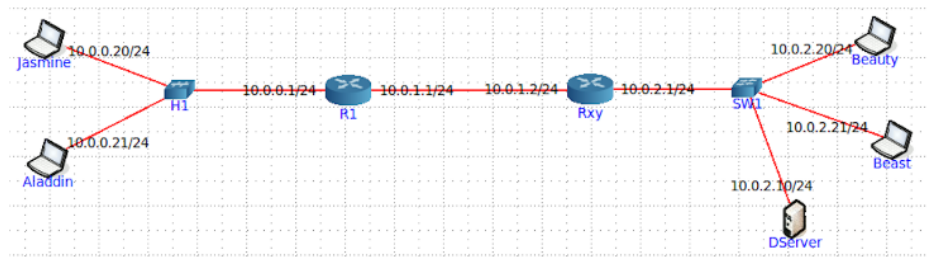
1	Mac de origem e Mac destino da trama capturada	3
2	Execução do comando <code>core@10.0.2.89</code>	3
3	Header IP	4
4	Encapsulamento Protocolar	4
5	Bytes utilizados no encapsulamento	4
6	Endereços MAC da fonte e do destino	5
7	Resultado do comando <code>arp -a</code>	6
8	Valores hexadecimais do MAC origem e do MAC destino	6
9	Mensagem ARP	6
10	OpCode da mensagem ARP	7
11	Output <code>ifconfig</code>	7
12	Output <code>netstat -rn</code>	8
13	Output <code>arp</code>	8
14	Tabela ARP do Aladdin	9
15	Tabela ARP do Beast	9
16	Diagrama entre Aladdin e Hosts ate a receção do primeiro pacote	9
17	<code>ifconfig</code> a mostrar MAC de Beast	10
18	<code>ifconfig</code> a mostrar MAC de Beauty	10
19	<code>ifconfig</code> a mostrar MAC de DServer	10
20	<code>ifconfig</code> a mostrar MAC de R89	11
21	Tabela da comutação completa da casa da Beauty e do Beast	11
22	Radio Header	12
23	Print Wireshark da Norma	13
24	Print Wireshark da Taxa de Transmissão da Trama	13
25	Trama Beacon 89	14
26	Deteção de erros Correct	14
27	Wireless Management Beacon	15
28	Aplicação do Filtro referido em cima	16
29	Sendo HitronTech o Source Address	17
30	Sendo HitronTech o Destination Address	18
31	Diagrama das tramas trocadas	18
32	Campo <i>Frame Control</i> da trama especificada	19
33	Tráfego de WLAN	20

1 Parte 1

1.1 Captura e análise de Tramas Ethernet

A topologia de rede representada na figura abaixo é constituída por: (i) uma LAN comutada que interliga os *hosts Beauty, Beast* e o servidor *DServer* (Disney Server) através de um *switch* (SW1) ao *router* de acesso Rxy; (ii) uma LAN partilhada que interliga os *hosts Jasmine, Aladdin* através de um *hub* ao *router* de acesso (R1); e (iii) uma rede IP ponto-a-ponto que interliga as duas LANs.

Construa a topologia indicada e particularize o router Rxy com o seu número de grupo (e.g., R27 para o grupo 7 do turno PL2). De igual forma, o endereço IP do servidor *DServer* deve ser alterado para incluir o seu número de grupo no identificador da host interface (4º octeto), e.g. 10.0.2.27, bem como o seu endereço MAC, e.g., 00:00:00:AA:BB:27.



Ative a topologia de rede e ative o Wireshark na interface de saída do *host Jasmine*. Antes de ver a sua série favorita, a Jasmine começa por abrir um terminal e estabelecer um acesso seguro ao servidor *DServer* usando o comando `ssh core@10.0.2.xy`.

1. Anote os endereços MAC de origem e MAC destino da trama capturada. Identifique a que *hosts* se referem. Justifique.

```
▶ Frame 18: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface veth8.0.72, id 1
▶ 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)
    Address: 00:00:00_aa:00:02 (00:00:00:aa:00:02)
    ..0. .... = LG bit: Globally unique address (factory default)
    ...0 .... = IG bit: Individual address (unicast)
  ▶ Source: 00:00:00_aa:00:00 (00:00:00:aa:00:00)
    Address: 00:00:00_aa:00:00 (00:00:00:aa:00:00)
    ..0. .... = LG bit: Globally unique address (factory default)
    ...0 .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
▶ Internet Protocol Version 4, Src: 10.0.0.20, Dst: 10.0.2.89
▶ Transmission Control Protocol, Src Port: 60744, Dst Port: 22, Seq: 1, Ack: 1, Len: 42
  Source Port: 60744
```

Figura 1: Mac de origem e Mac destino da trama capturada

```
# Host 10.0.2.89 found: line 1
/root/.ssh/known_hosts updated.
Original contents retained as /root/.ssh/known_hosts.old
root@Jasmine:/tmp/pycore.42455/Jasmine.conf# ssh core@10.0.2.89
The authenticity of host '10.0.2.89 (10.0.2.89)' can't be established.
RSA key fingerprint is SHA256:ICSzo06akGGuXukoqYKKWY4fHv+IifBV3SmA73drNA.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.89' (RSA) to the list of known hosts.
core@10.0.2.89's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.11.0-37-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

129 updates can be applied immediately.
1 of these updates is a standard security update.
To see these additional updates run: apt list --upgradable

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your
Internet connection or proxy settings

Your Hardware Enablement Stack (HWE) is supported until April 2025.
core@DServer:~$
```

Figura 2: Execução do comando `core@10.0.2.89`

Tendo em conta a trama capturada, temos que o endereço MAC de origem é 00:00:00:aa:00:00 e o endereço MAC de destino é 00:00:00:aa:00:02, visto que o próximo salto de um pacote que pretende aceder ao exterior será o router ao qual a máquina se encontra associada.

- 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?

O valor hexadecimal do campo type é 0x0800. Em baixo conseguimos ver o header IP idêntico ao valor de type.

```

▶ Frame 15: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface veth8.0.72, 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)
    Address: 00:00:00_aa:00:02 (00:00:00:aa:00:02)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  ▼ Source: 00:00:00_aa:00:00 (00:00:00:aa:00:00)
    Address: 00:00:00_aa:00:00 (00:00:00:aa:00:00)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
▶ Internet Protocol Version 4, Src: 10.0.0.20, Dst: 10.0.2.89
▶ Transmission Control Protocol, Src Port: 60744, Dst Port: 22, Seq: 0, Len: 0

```

Figura 3: Header IP

- 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.

Em baixo conseguimos visualizar o encapsulamento protocolar e quantos bytes foram utilizados a partir do início da trama até ao nível aplicacional:

```

▼ Transmission Control Protocol, Src Port: 60744, Dst Port: 22, Seq: 0, Len: 0
  Source Port: 60744
  Destination Port: 22
  [Stream index: 0]
  [TCP Segment Len: 0]
  Sequence number: 0 (relative sequence number)
  Sequence number (raw): 1694147766
  [Next sequence number: 1 (relative sequence number)]
  Acknowledgment number: 0
  Acknowledgment number (raw): 0
  1010 .... = Header Length: 40 bytes (10)
  ▶ Flags: 0x002 (SYN)
  Window size value: 64240
  [Calculated window size: 64240]
  Checksum: 0x0263 [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0

```

Figura 4: Encapsulamento Protocolar

```

▶ Frame 18: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface veth8.0.72, id 1
▼ 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)
    Address: 00:00:00_aa:00:02 (00:00:00:aa:00:02)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  ▼ Source: 00:00:00_aa:00:00 (00:00:00:aa:00:00)
    Address: 00:00:00_aa:00:00 (00:00:00:aa:00:00)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
▶ Internet Protocol Version 4, Src: 10.0.0.20, Dst: 10.0.2.89
▼ Transmission Control Protocol, Src Port: 60744, Dst Port: 22, Seq: 1, Ack: 1, Len: 42
  Source Port: 60744

```

Figura 5: Bytes utilizados no encapsulamento

São usados 66 bytes no encapsulamento protocolar, sendo 14 correspondentes ao header Ethernet, 20 ao IP e 32 ao TCP.

$$\frac{66}{108} \times 100 = 61,1\%$$

A seguir responda às seguintes perguntas, baseado no conteúdo de uma das tramas Ethernet que contém a resposta proveniente do servidor.

4. Qual é o endereço MAC da fonte? A que *host* e interface corresponde? Justifique.

```
▼ Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: 00:00:00_aa:00:06 (00:00:00:aa:00:06)
  ▼ Destination: 00:00:00_aa:00:06 (00:00:00:aa:00:06)
    Address: 00:00:00_aa:00:06 (00:00:00:aa:00:06)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  ▼ Source: 00:00:00_aa:00:00 (00:00:00:aa:00:00)
    Address: 00:00:00_aa:00:00 (00:00:00:aa:00:00)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
```

Figura 6: Endereços MAC da fonte e do destino

Através da Figura 6, conseguimos identificar o endereço MAC da fonte, neste caso, do Router1.

5. Qual é o endereço MAC do destino? A que *host* e interface corresponde?

Novamente, pela Figura 6, é possível identificar o endereço MAC do destino, que neste caso corresponde ao dispositivo Jasmine.

1.2 Protocolo ARP e Domínios de Colisão

Deverá ter a *cache* ARP completamente vazia antes de iniciar esta secção: reinicie a topologia, ou utilize o comando `arp -d`.

Comece a capturar tráfego com o Wireshark na interface dos *hosts Jasmine, Aladdin, Beauty e Beast*. Não sabendo que a *Jasmine* e a *Beauty* estavam a capturar tráfego, o *Aladdin* e o *Beast* fazem um acesso secreto por `ssh` para o servidor *DServer*. Efetue esse acesso e depois pare as várias capturas de tráfego.

1. 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.

Efetuando o comando `arp -a`, obtemos o seguinte output:

```
root@Aladdin:/tmp/pycore.33043/Aladdin.conf# arp -a
? (10.0.0.1) at 00:00:00:aa:00:00 [ether] on eth0
root@Aladdin:/tmp/pycore.33043/Aladdin.conf#
```

Figura 7: Resultado do comando `arp -a`

A primeira coluna apresenta endereços IP ou nomes dos hosts; a segunda indica o tipo da conexão (neste caso, Ethernet); a terceira mostra o endereço MAC do dispositivo de destino; a quarta representa as flags (neste caso, a flag `-c` indica que a conexão foi estabelecida com sucesso); e, por fim, a última coluna indica a interface do dispositivo de destino.

2. Observe a trama Ethernet que contém a mensagem com o pedido ARP (ARP Request).
 - a. Qual é o valor hexadecimal dos endereços MAC origem e destino? Como interpreta e justifica o endereço destino usado?

```
▶ Frame 35: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface veth5.0.92, id 0
▼ Ethernet II, Src: 00:00:00_aa:00:07 (00:00:00:aa:00:07), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▶ Destination: Broadcast (ff: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)
```

Figura 8: Valores hexadecimais do MAC origem e do MAC destino

O endereço de destino da trama Ethernet é `ff:ff:ff:ff:ff:ff` e o de origem é `00:00:00:aa:00:07`. Podemos compreender que esse endereço de destino é utilizado para realizar um broadcast, pois, como é objetivo do protocolo ARP, pretende-se descobrir um determinado endereço IP. Para isso, pergunta-se a toda a rede local se algum dispositivo possui o endereço pretendido.

Se existir algum dispositivo com esse endereço, ele deverá comunicá-lo e, dessa forma, o sistema que realizou o ARP Request passará a conhecer a informação desejada.

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

```
▶ Frame 35: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface veth5.0.92, id 0
▼ Ethernet II, Src: 00:00:00_aa:00:07 (00:00:00:aa:00:07), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▶ Destination: Broadcast (ff: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)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: 00:00:00_aa:00:07 (00:00:00:aa:00:07)
  Sender IP address: 10.0.0.21
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 10.0.0.1
```

Figura 9: Mensagem ARP

Observando a mensagem ARP, podemos identificar que se trata de um pedido ARP por meio do campo "Opcode: request (1)", que indica explicitamente que é um pedido. Além disso, o endereço MAC de destino "00:00:00:00:00:00" (composto apenas por zeros) demonstra que o emissor desconhece o MAC associado ao IP de destino que está tentando resolver.

3. Localize a mensagem ARP que é a resposta ao pedido ARP efetuado.

a. Qual o valor do campo ARP opcode? O que especifica?

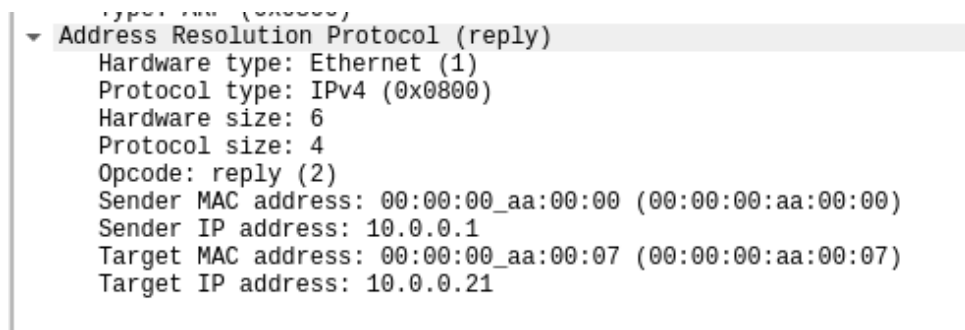


Figura 10: OpCode da mensagem ARP

O valor do campo é 2, especificando, assim, que se trata de uma mensagem ARP Reply.

b. Em que campo da mensagem ARP está a resposta ao pedido ARP efetuado?

O campo da mensagem é o Sender MAC Address.

- c. 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*).

```
root@Aladdin:/tmp/pycore.33043/Aladdin.conf# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.0.21 netmask 255.255.255.0 broadcast 0.0.0.0
    inet6 fe80::200:ff:feaa:7 prefixlen 64 scopeid 0x20<link>
    inet6 2001::21 prefixlen 64 scopeid 0x0<global>
    ether 00:00:00:aa:00:07 txqueuelen 1000 (Ethernet)
    RX packets 1063 bytes 91130 (91.1 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 50 bytes 6810 (6.8 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 324 (324.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 324 (324.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Figura 11: Output ifconfig


```

root@Aladdin:/tmp/pycore.33043/Aladdin.conf# netstat -rn
Kernel IP routing table
Destination      Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0          10.0.0.1        0.0.0.0         UG      0 0        0 eth0
10.0.0.0         0.0.0.0         255.255.255.0   U       0 0        0 eth0
root@Aladdin:/tmp/pycore.33043/Aladdin.conf#

```

Figura 12: Output netstat -rn

```

root@Aladdin:/tmp/pycore.33043/Aladdin.conf# arp
Address          HWtype  HWaddress      Flags Mask    Iface
10.0.0.1         ether   00:00:00:aa:00:00  C           eth0
root@Aladdin:/tmp/pycore.33043/Aladdin.conf#

```

Figura 13: Output arp

O endereço MAC 00:00:00:aa:00:00 pertence ao dispositivo R1.

O endereço MAC 00:00:00:aa:00:07 pertence ao dispositivo Aladdin.

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

Numa resposta ARP (ARP Reply), o modo de comunicação utilizado é *unicast*, porque o dispositivo que responde já conhece o endereço MAC do solicitante, tornando desnecessário o envio para todos os dispositivos na rede. Esse método é mais eficiente, pois reduz o tráfego na rede ao enviar a informação apenas para o dispositivo que a solicitou.

O endereço MAC do solicitante foi obtido a partir do pedido ARP original, o que permite essa comunicação direcionada. Em contraste, o pedido ARP inicial utiliza *broadcast*, justamente porque o dispositivo não conhece o endereço MAC de destino, sendo necessário enviar a mensagem para toda a rede.

4. Verifique se a *Jasmine* teve conhecimento ou não de todo o tráfego gerado pelo acesso secreto do *Aladdin*? Qual será a razão para tal?

A *Jasmine* consegue ver o tráfego do *Aladdin* porque estão ligados ao mesmo hub. Ela conseguiu capturar todo o tráfego SSH gerado pelo *Aladdin* porque ambos estão conectados ao mesmo hub. Os hubs operam na camada física (camada 1) do modelo OSI e simplesmente retransmitem qualquer sinal recebido para todas as suas portas, sem qualquer filtragem baseada em endereços. Isso significa que, quando o *Aladdin* enviou pacotes SSH para o servidor *DServer*, esses pacotes foram transmitidos para todas as portas do hub, incluindo a porta onde a *Jasmine* está conectada. Assim, a *Jasmine* pôde capturar todo o tráfego, mesmo que não fosse destinado a ela.

5. 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?

A *Beauty* não conseguiu capturar o tráfego SSH gerado pelo *Beast* porque ambos estão conectados a um switch. Os switches operam na camada 2 do modelo OSI e utilizam tabelas de endereços MAC para encaminhar pacotes apenas para as portas específicas onde estão os dispositivos de destino. Diferentemente dos hubs, os switches não enviam todo o tráfego para todas as portas. Portanto, o tráfego *unicast* entre o *Beast* e o servidor *DServer* foi direcionado especificamente para essas portas, sem passar pela porta onde a *Beauty* está conectada, o que impossibilitou a captura desse tráfego.

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

```

vcmd
root@Aladdin:/tmp/pycore.33043/Aladdin.conf# arp -a
? (10.0.0.1) at 00:00:00:aa:00:00 [ether] on eth0
root@Aladdin:/tmp/pycore.33043/Aladdin.conf#

```

Figura 14: Tabela ARP do Aladdin

```

vcmd
root@Beast:/tmp/pycore.33043/Beast.conf# arp -a
? (10.0.2.89) at 00:00:00:aa:00:89 [ether] on eth0
root@Beast:/tmp/pycore.33043/Beast.conf#

```

Figura 15: Tabela ARP do Beast

Analisando as tabelas ARP, a principal diferença é que o Aladdin conhece apenas o endereço MAC do gateway 10.0.0.1, enquanto o Beast conhece apenas o endereço MAC do dispositivo 10.0.2.89 (DServer). Esse padrão indica que cada dispositivo mantém informações ARP apenas da sua própria sub-rede local.

O impacto disso é que toda comunicação entre dispositivos de sub-redes diferentes (como Aladdin e Beast) deve, necessariamente, passar pelos routers, criando isolamento de camada 2 entre os segmentos da rede. Isso aumenta a segurança e permite o controle do tráfego entre sub-redes.

7. 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 recepção do primeiro pacote que contém dados do acesso remoto.

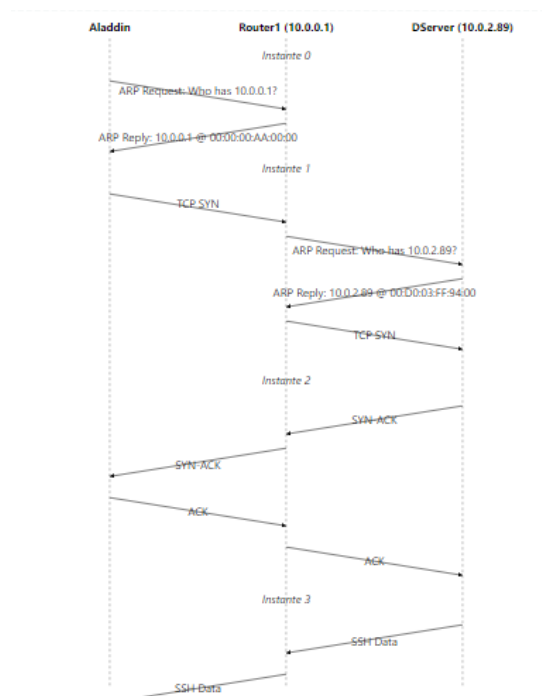


Figura 16: Diagrama entre Aladdin e Hosts até a recepção do primeiro pacote

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

```

root@Beast:/tmp/pycore.40183/Beast.conf# ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.21 netmask 255.255.255.0 broadcast 0.0.0.0
    inet6 2001:2::21 prefixlen 64 scopeid 0x0<global>
    inet6 fe80::200:ff:feaa:5 prefixlen 64 scopeid 0x20<link>
    ether 00:00:00:aa:00:05 txqueuelen 1000 (Ethernet)
    RX packets 99 bytes 10294 (10.2 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 10 bytes 892 (892.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@Beast:/tmp/pycore.40183/Beast.conf#

```

Figura 17: ifconfig a mostrar MAC de Beast

Conseguimos reter que o MAC de Beast é 00:00:00:aa:00:04.

```

root@Beauty:/tmp/pycore.40183/Beauty.conf# ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.20 netmask 255.255.255.0 broadcast 0.0.0.0
    inet6 fe80::200:ff:feaa:4 prefixlen 64 scopeid 0x20<link>
    inet6 2001:2::20 prefixlen 64 scopeid 0x0<global>
    ether 00:00:00:aa:00:04 txqueuelen 1000 (Ethernet)
    RX packets 172 bytes 16232 (16.2 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 12 bytes 1032 (1.0 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@Beauty:/tmp/pycore.40183/Beauty.conf#

```

Figura 18: ifconfig a mostrar MAC de Beauty

Conseguimos reter que o MAC de Beauty é 00:00:00:aa:00:05.

```

root@DServer:/tmp/pycore.40183/DServer.conf# ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.89 netmask 255.255.255.0 broadcast 0.0.0.0
    inet6 2001:2::10 prefixlen 64 scopeid 0x0<global>
    inet6 fe80::200:ff:feaa:89 prefixlen 64 scopeid 0x20<link>
    ether 00:00:00:aa:00:89 txqueuelen 1000 (Ethernet)
    RX packets 229 bytes 20634 (20.6 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 12 bytes 1032 (1.0 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@DServer:/tmp/pycore.40183/DServer.conf#

```

Figura 19: ifconfig a mostrar MAC de DServer

Conseguimos reter que o MAC de DServer é 00:00:00:aa:00:89.

```

root@R89:/tmp/pycore.40183/R89.conf# ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.1.2 netmask 255.255.255.0 broadcast 0.0.0.0
    inet6 fe80::200:ff:feaa:2 prefixlen 64 scopeid 0x20<link>
    inet6 2001::1:2 prefixlen 64 scopeid 0x0<global>
    ether 00:00:00:aa:00:02 txqueuelen 1000 (Ethernet)
    RX packets 112 bytes 11772 (11.7 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 64 bytes 6068 (6.0 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.1 netmask 255.255.255.0 broadcast 0.0.0.0
    inet6 2001::2:1 prefixlen 64 scopeid 0x0<global>
    inet6 fe80::200:ff:feaa:3 prefixlen 64 scopeid 0x20<link>
    ether 00:00:00:aa:00:03 txqueuelen 1000 (Ethernet)
    RX packets 76 bytes 8320 (8.3 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 50 bytes 4312 (4.3 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@R89:/tmp/pycore.40183/R89.conf#

```

Figura 20: ifconfig a mostrar MAC de R89

Conseguimos reter que o MAC de DServer é 00:00:00:aa:00:02.

MAC Address	Interface	TTL	Device Name
00:00:00:aa:00:04	eth1	60	beuty
00:00:00:aa:00:05	eth2	60	beast
00:00:00:aa:00:89	eth3	60	DServer
00:00:00:aa:00:02	eth4	60	r89

Figura 21: Tabela da comutação completa da casa da Beauty e do Beast

1.3 Serviço de NAT/PAT

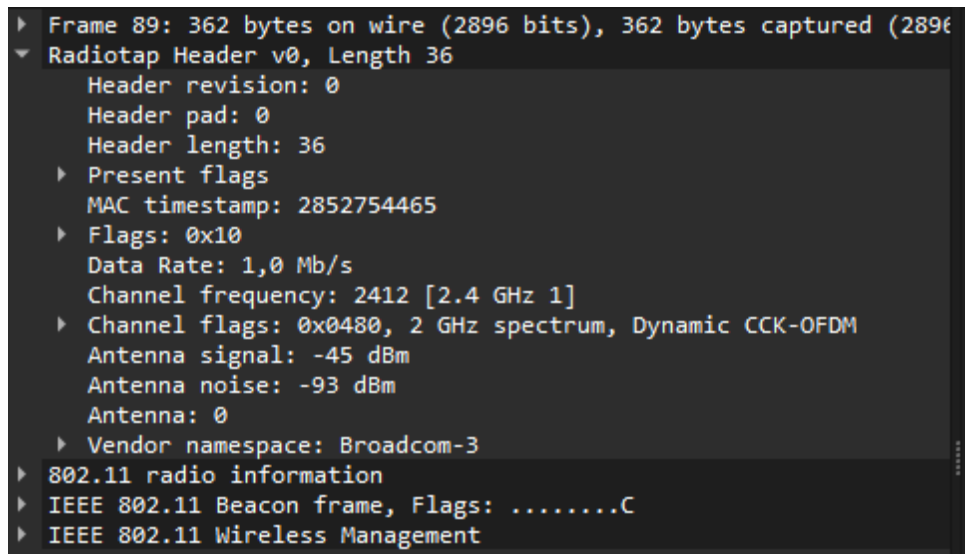
1. Como proteção, a *Jasmine* e o *Aladdin*, juntamente com a *Beauty* e o *Beast*, decidiram conectar R1 e Rxy a uma rede de um ISP com endereços IP públicos, mantendo todo o endereçamento privado das suas LANs. Sabe-se que o ISP não encaminha tráfego para redes privadas, portanto, R1 e Rxy não conseguem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

Para manter todas as funcionalidades, como a conectividade IP e o acesso SSH ao servidor, deve-se configurar NAT/PAT com overload (também conhecido como NAT dinâmico com tradução por porta) em ambos os routers, R1 e R89. Cada router deve usar o endereço IP público atribuído pelo ISP na interface externa para traduzir os endereços privados da sua LAN. Dessa forma, todos os dispositivos da rede interna podem comunicar com o exterior, mesmo que compartilhem o mesmo IP público. Essa configuração assegura que o tráfego seja encaminhado corretamente, evitando o bloqueio por parte do ISP, que não aceita pacotes destinados a endereços privados.

2 Parte 2

2.1 Acesso Rádio



```
▶ Frame 89: 362 bytes on wire (2896 bits), 362 bytes captured (2896
▼ Radiotap Header v0, Length 36
  Header revision: 0
  Header pad: 0
  Header length: 36
  ▶ Present flags
    MAC timestamp: 2852754465
  ▶ Flags: 0x10
    Data Rate: 1,0 Mb/s
    Channel frequency: 2412 [2.4 GHz 1]
  ▶ Channel flags: 0x0480, 2 GHz spectrum, Dynamic CCK-OFDM
    Antenna signal: -45 dBm
    Antenna noise: -93 dBm
    Antenna: 0
  ▶ Vendor namespace: Broadcom-3
  ▶ 802.11 radio information
  ▶ IEEE 802.11 Beacon frame, Flags: .....C
  ▶ IEEE 802.11 Wireless Management
```

Figura 22: Radio Header

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

A frequência do espectro em que está a operar é 2412 MHz. O canal correspondente é o 1.

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

A rede está utilizando o padrão IEEE 802.11n (Wi-Fi 4) na banda de 2.4 GHz, conforme indicado pelos campos HT Capabilities e HT Information. Ela também é compatível com os padrões mais antigos 802.11b/g, como mostram as taxas de transmissão suportadas (1 a 54 Mbps) e o parâmetro ERP Information. O canal em uso é o 1 (2.412 GHz), e não há indicação de suporte a padrões mais recentes como 802.11ac (Wi-Fi 5) ou 802.11ax (Wi-Fi 6). Portanto, a versão principal em uso é o 802.11n.

```
▶ Frame 89: 362 bytes on wire (2896 bits), 362 bytes captured (2896 bits) on interface en0,
▶ Radiotap Header v0, Length 36
▶ 802.11 radio information
▶ IEEE 802.11 Beacon frame, Flags: .....C
▼ IEEE 802.11 Wireless Management
  ▶ Fixed parameters (12 bytes)
  ▼ Tagged parameters (286 bytes)
    ▶ Tag: SSID parameter set: "FlyingNet"
    ▶ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18, [Mbit/sec]
    ▶ Tag: DS Parameter set: Current Channel: 1
    ▶ Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
    ▶ Tag: Country Information: Country Code PT, Environment All
    ▶ Tag: ERP Information
    ▶ Tag: Extended Supported Rates 24(B), 36, 48, 54, [Mbit/sec]
    ▶ Tag: HT Capabilities (802.11n D1.10)
    ▶ Tag: HT Information (802.11n D1.10)
    ▶ Tag: Extended Capabilities (8 octets)
    ▶ Tag: VHT Capabilities
    ▶ Tag: VHT Operation
    ▶ Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
    ▶ Tag: Vendor Specific: Atheros Communications, Inc.: Advanced Capability
    ▶ Tag: Vendor Specific: Qualcomm Inc.
    ▶ Tag: Vendor Specific: Qualcomm Inc.
    ▶ Tag: Vendor Specific: Microsoft Corp.: WPA Information Element
    ▶ Tag: RSN Information
    ▶ Tag: Vendor Specific: Microsoft Corp.: WPS
```

Figura 23: Print Wireshark da Norma

3. 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.

```
▶ Frame 89: 362 bytes on wire (2896 bits), 362 bytes captured (2896 bits) on interface en0,
▶ Radiotap Header v0, Length 36
  Header revision: 0
  Header pad: 0
  Header length: 36
  ▶ Present flags
  MAC timestamp: 2852754465
  ▶ Flags: 0x10
  Data Rate: 1,0 Mb/s
  Channel frequency: 2412 [2.4 GHz 1]
  ▶ Channel flags: 0x0480, 2 GHz spectrum, Dynamic CCK-OFDM
  Antenna signal: -45 dBm
  Antenna noise: -93 dBm
  Antenna: 0
  ▶ Vendor namespace: Broadcom-3
▶ 802.11 radio information
▶ IEEE 802.11 Beacon frame, Flags: .....C
▶ IEEE 802.11 Wireless Management
```

Figura 24: Print Wireshark da Taxa de Transmissão da Trama

2.2 Scanning Passivo e Scanning Ativo

4. 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 89: 362 bytes on wire (2896 bits), 362 bytes captured (2896 bits) on interface en0,
▶ Radiotap Header v0, Length 36
▶ 802.11 radio information
▶ IEEE 802.11 Beacon frame, Flags: .....C
▼ IEEE 802.11 Wireless Management
  ▶ Fixed parameters (12 bytes)
  ▼ Tagged parameters (286 bytes)
    ▶ Tag: SSID parameter set: "FlyingNet"
    ▶ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18, [Mbit/sec]
    ▶ Tag: DS Parameter set: Current Channel: 1
    ▶ Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
    ▶ Tag: Country Information: Country Code PT, Environment All
    ▶ Tag: ERP Information
    ▶ Tag: Extended Supported Rates 24(B), 36, 48, 54, [Mbit/sec]
    ▶ Tag: HT Capabilities (802.11n D1.10)
    ▶ Tag: HT Information (802.11n D1.10)
    ▶ Tag: Extended Capabilities (8 octets)
    ▶ Tag: VHT Capabilities
    ▶ Tag: VHT Operation
    ▶ Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
    ▶ Tag: Vendor Specific: Atheros Communications, Inc.: Advanced Capability
    ▶ Tag: Vendor Specific: Qualcomm Inc.
    ▶ Tag: Vendor Specific: Qualcomm Inc.
    ▶ Tag: Vendor Specific: Microsoft Corp.: WPA Information Element
    ▶ Tag: RSN Information
    ▶ Tag: Vendor Specific: Microsoft Corp.: WPS

```

Figura 25: Trama Beacon 89

A trama Beacon 89 é uma trama de Management (tipo 0), do subtipo Beacon (subtipo 8).

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

```

▼ 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)
  ▶ Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
  ▶ Transmitter address: HitronTechno_f3:9a:46 (74:9b:e8:f3:9a:46)
  ▶ Source address: HitronTechno_f3:9a:46 (74:9b:e8:f3:9a:46)
  ▶ BSS Id: HitronTechno_f3:9a:46 (74:9b:e8:f3:9a:46)
    .... 0000 = Fragment number: 0
    1001 1110 1110 .... = Sequence number: 2542
  Frame check sequence: 0xf4ff78ca [correct]
  [FCS Status: Good]
  [WLAN Flags: .....C]

```

Figura 26: Detecção de erros Correct

6. Justifique o porquê de ser necessário usar detecção de erros em redes sem fios.

É necessário devido a três fatores principais:

- O meio rádio é muito suscetível a ruído, interferências e fading.
- Pequenas variações no sinal podem causar inversões de bits.
- O CRC, ao nível da camada MAC, permite descartar frames corrompidos antes de os dados subirem à camada lógica, evitando comportamentos inesperados e retransmitindo apenas o necessário.

As tramas *beacon* são enviadas periodicamente e permitem especificar parâmetros de funcionamento para apoiar a operação e a gestão das ligações sem fios.

7. 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.

```
IEEE 802.11 Wireless Management
  Fixed parameters (12 bytes)
    Timestamp: 56021709187
    Beacon Interval: 0,102400 [Seconds]
    Capabilities Information: 0x0431
  Tagged parameters (286 bytes)
    Tag: SSID parameter set: "FlyingNet"
    Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18, [Mbit/sec]
    Tag: DS Parameter set: Current Channel: 1
    Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
    Tag: Country Information: Country Code PT, Environment All
    Tag: ERP Information
    Tag: Extended Supported Rates 24(B), 36, 48, 54, [Mbit/sec]
    Tag: HT Capabilities (802.11n D1.10)
    Tag: HT Information (802.11n D1.10)
    Tag: Extended Capabilities (8 octets)
    Tag: VHT Capabilities
    Tag: VHT Operation
    Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
    Tag: Vendor Specific: Atheros Communications, Inc.: Advanced Capability
    Tag: Vendor Specific: Qualcomm Inc.
    Tag: Vendor Specific: Qualcomm Inc.
    Tag: Vendor Specific: Microsoft Corp.: WPA Information Element
    Tag: RSN Information
    Tag: Vendor Specific: Microsoft Corp.: WPS
```

Figura 27: Wireless Management Beacon

Pela informação fornecida pelo Wireshark, a periodicidade e as taxas suportadas são:

- Periodicidade: 102,4 ms (10 beacons por segundo).
- Taxas de transmissão:
 - Taxas básicas (obrigatórias): 1, 2, 5,5, 6, 11, 12, 24 Mbps.
 - Taxas opcionais: 9, 18, 36, 48, 54 Mbps.
- Padrões envolvidos: 802.11b, 802.11g, 802.11n (e possivelmente 802.11ac, devido ao campo VHT).

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

Utilizando wlan.ssid como filtro — mais especificamente ((wlan.fc.type_subtype == 0x08 — wlan.fc.type_subtype == 0x05 — wlan.fc.type_subtype == 0x00)) — foram encontrados os seguintes SSIDs:

- FlyingNet
- GVBRAGA
- GVBRAGA_EXT
- GVBRAGA_quarto

- MEO-66DB70
- MEO-828830
- MEO-854C80
- MEO-9BF2A0
- MEO-F17570
- MEO-FCF0A0
- MEO-WiFi
- Masmorra do Sexo
- NOS-26F6
- NOS-52C6
- NOS-9946_EXT
- NOS-C8B6
- NOS-FD24
- Vodafone-D0ED8A
- phi_F41927C3C600

No *trace* disponibilizado foi também registado *scanning* ativo (envolvendo tramas *probe request* e *probe response*), comum nas redes Wi-Fi como alternativa ao *scanning* passivo.

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

O filtro que permite visualizar tanto as tramas Probe Request quanto as Probe Response é `wlan.fc.type_subtype == 4 or wlan.fc.type_subtype == 5`, pois Probe Request possui o subtipo 0x04 e Probe Response, o subtipo 0x05.

10. 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.

Aplicando o filtro `"(wlan.fc.type_subtype == 8 or wlan.fc.type_subtype == 5) and radiotap.dbm_antsignal"` e, em seguida, criando uma nova coluna a partir do Signal Strength.

Source	Destination	Protocol	Length	Info	Signal strength (dBm)
HitronTechno_f3:9a:...	Broadcast	802.11	362	Beacon frame, SN=672, FN=0, Flags=.....C, BI=100, SSID="FlyingNet"	-39 dBm
HitronTechno_f3:9a:...	Broadcast	802.11	362	Beacon frame, SN=673, FN=0, Flags=.....C, BI=100, SSID="FlyingNet"	-41 dBm
HitronTechno_f3:9a:...	Broadcast	802.11	362	Beacon frame, SN=1721, FN=0, Flags=.....C, BI=100, SSID="FlyingNet"	-42 dBm
HitronTechno_f3:9a:...	Broadcast	802.11	362	Beacon frame, SN=674, FN=0, Flags=.....C, BI=100, SSID="FlyingNet"	-42 dBm
HitronTechno_f3:9a:...	Broadcast	802.11	362	Beacon frame, SN=671, FN=0, Flags=.....C, BI=100, SSID="FlyingNet"	-42 dBm
HitronTechno_f3:9a:...	Broadcast	802.11	362	Beacon frame, SN=668, FN=0, Flags=.....C, BI=100, SSID="FlyingNet"	-42 dBm
HitronTechno_f3:9a:...	Broadcast	802.11	362	Beacon frame, SN=659, FN=0, Flags=.....C, BI=100, SSID="FlyingNet"	-42 dBm
HitronTechno_f3:9a:...	Broadcast	802.11	362	Beacon frame, SN=2569, FN=0, Flags=.....C, BI=100, SSID="FlyingNet"	-42 dBm

Figura 28: Aplicação do Filtro referido em cima

Pelo wireshark aplicando o filtro, o maior valor é -39, correspondente a "FlyingNet".

11. Os valores de taxa de transmissão do Wi-Fi estão diretamente associados à qualidade da recepção 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.

Com base na tabela de sensibilidade mínima (Anexo II) e no valor de sinal medido de -39 dBm para o AP selecionado, conclui-se que a ligação pode operar no mais elevado MCS suportado (MCS7, 64-QAM 5/6), cuja sensibilidade típica é de cerca de -65 dBm. Isso corresponde a uma taxa física de 65 Mbps.

Considerando a sobrecarga das camadas MAC e PHY, tem-se o seguinte:

- **Data Rate PHY (MCS7):** 65 Mbps
- **Overhead MAC/PHY:** em média, retira-se cerca de 15–20% da taxa bruta, devido a cabeçalhos, preâmbulos e ACKs.

Taxa útil estimada:

$$65 \text{ Mbps} \times (1 - 0,18) \approx 53,3 \text{ Mbps}$$

Portanto, estima-se que a STA obterá entre **50 a 55 Mbps de débito real** na camada de aplicação.

2.3 Processo de Associação

12. 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.

Utilizando o seguinte filtro:

```
wlan.sa == fe:bd:a5:05:6c:84 and wlan.da == 74:9b:e8:f3:9a:46 and  
(wlan.fc.type_subtype == 11 or wlan.fc.type_subtype == 0 or wlan.fc.type_subtype == 1)
```

Sendo:

- **Source Address (SA):** fe:bd:a5:05:6c:84
- **Destination Address (DA):** 74:9b:e8:f3:9a:46 (identificado como *HitronTechno_f3:9a:46*)

É possível visualizar as seguintes tramas:

wlan.da == fe:bd:a5:05:6c:84 and wlan.sa == 74:9b:e8:f3:9a:46 and (wlan.fc.type_subtype == 11 or wlan.fc.type_subtype == 0 or wlan.fc.type_subtype == 1)						
No.	Time	Source	Destination	Protocol	Length	Info
2044	23.707398	HitronTechno_f3:9a:...	fe:bd:a5:05:6c:84	802.11	70	Authentication, SN=3852, FN=0, Flags=.....C
2048	23.716772	HitronTechno_f3:9a:...	fe:bd:a5:05:6c:84	802.11	210	Association Response, SN=3853, FN=0, Flags=.....C
32462	153.870102	HitronTechno_f3:9a:...	fe:bd:a5:05:6c:84	802.11	70	Authentication, SN=3939, FN=0, Flags=.....C
32466	153.878503	HitronTechno_f3:9a:...	fe:bd:a5:05:6c:84	802.11	210	Association Response, SN=3940, FN=0, Flags=.....C
36371	182.165154	HitronTechno_f3:9a:...	fe:bd:a5:05:6c:84	802.11	70	Authentication, SN=3956, FN=0, Flags=.....C
36375	182.170791	HitronTechno_f3:9a:...	fe:bd:a5:05:6c:84	802.11	210	Association Response, SN=3957, FN=0, Flags=.....C

Figura 29: Sendo HitronTech o Source Address

Depois invertendo o Source Address com o Destination Address.

wlan.sa == fe:bd:a5:05:6c:84 and wlan.da == 74:9b:e8:f3:9a:46 and (wlan.fc.type_subtype == 11 or wlan.fc.type_subtype == 0 or wlan.fc.type_subtype == 1)						
No.	Time	Source	Destination	Protocol	Length	Info
2042	23.707373	fe:bd:a5:05:6c:84	HitronTechno_f3:9a:...	802.11	106	Authentication, SN=3343, FN=0, Flags=.....C
2046	23.710405	fe:bd:a5:05:6c:84	HitronTechno_f3:9a:...	802.11	202	Association Request, SN=3344, FN=0, Flags=.....C, SSID="FlyingNet"
32460	153.869966	fe:bd:a5:05:6c:84	HitronTechno_f3:9a:...	802.11	106	Authentication, SN=1556, FN=0, Flags=.....C
32464	153.874096	fe:bd:a5:05:6c:84	HitronTechno_f3:9a:...	802.11	202	Association Request, SN=1557, FN=0, Flags=.....C, SSID="FlyingNet"
36369	182.163376	fe:bd:a5:05:6c:84	HitronTechno_f3:9a:...	802.11	106	Authentication, SN=3823, FN=0, Flags=.....C
36373	182.167893	fe:bd:a5:05:6c:84	HitronTechno_f3:9a:...	802.11	202	Association Request, SN=3824, FN=0, Flags=.....C, SSID="FlyingNet"

Figura 30: Sendo HitronTech o Destination Address

- Efetue um diagrama que ilustre a sequência de todas as tramas trocadas no processo.

Diagrama de Troca de Tramas Wi-Fi 802.11

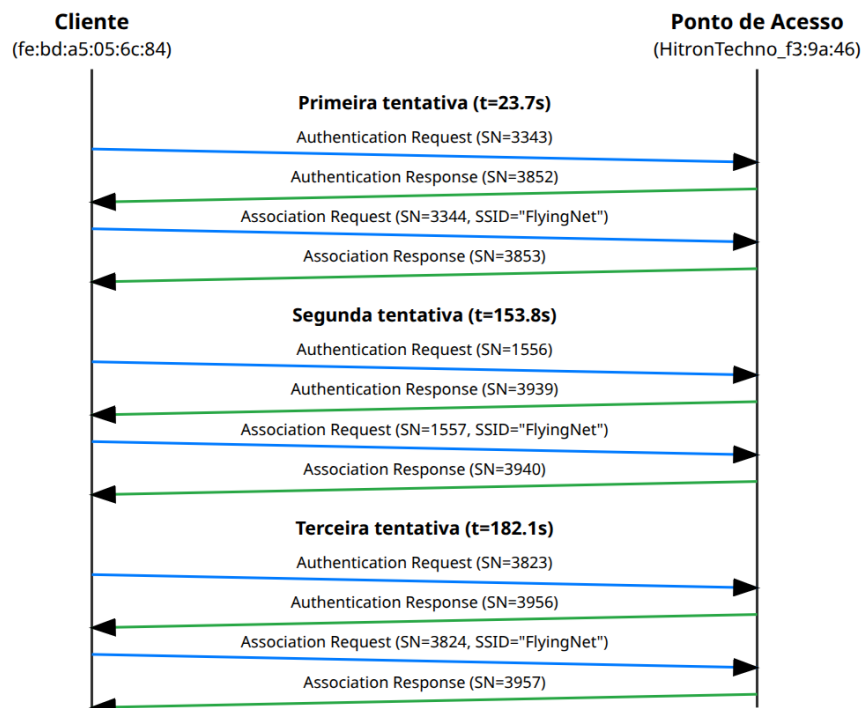


Figura 31: Diagrama das tramas trocadas

2.4 Transferência de Dados

O trace disponibilizado, para além de tramas de gestão da ligação de dados, inclui tramas de dados e tramas de controlo da transferência desses mesmos dados.

14. 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 direccionalidade das tramas, o que pode concluir face à direccionalidade dessa trama, será local à WLAN?

Utilizando o filtro `wlan.fc.type == 2` e seleccionando uma trama cujo identificador termina em 89:

```
> Frame 2489: 120 bytes on wire (960 bits), 120 bytes captured (960 bits) on interface en0
> Radiotap Header v0, Length 36
> 802.11 radio information
> IEEE 802.11 Data, Flags: .p...F.C
  Type/Subtype: Data (0x0020)
  Frame Control Field: 0x0842
    .... ..00 = Version: 0
    .... 10.. = Type: Data frame (2)
    0000 .... = Subtype: 0
    Flags: 0x42
      .... ..10 = DS status: Frame from DS to a STA via AP(To DS: 0 From DS: 1) (0x2)
      .... .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... .... = +HTC/Order flag: Not strictly ordered
    .000 0000 0000 0000 = Duration: 0 microseconds
  > Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
  > Transmitter address: HitronTechno_f3:9a:46 (74:9b:e8:f3:9a:46)
  > Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source address: 76:9b:e8:f3:9a:43 (76:9b:e8:f3:9a:43)
  > BSS Id: HitronTechno_f3:9a:46 (74:9b:e8:f3:9a:46)
  > STA address: Broadcast (ff:ff:ff:ff:ff:ff)
```

Figura 32: Campo *Frame Control* da trama especificada

Analisando o campo **Frame Control** (0x0842) da trama capturada, podemos concluir que esta não é local à WLAN. Os bits de estado DS (Distribution System) indicam:

To DS: 0 From DS: 1

Isso significa que a trama está a ser enviada do sistema de distribuição (DS) para uma estação (STA) através de um ponto de acesso (AP). Assim, conclui-se que a origem da trama é externa à rede sem fios, estando esta a ser encaminhada para um cliente wireless.

15. 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)?

Na trama de dados selecionada, podemos identificar os seguintes endereços MAC:

- **Endereço do recetor:** *Broadcast* (ff:ff:ff:ff:ff:ff)
- **Endereço do transmissor:** *HitronTechno_f3:9a:46* (74:9b:e8:f3:9a:46)
- **Endereço de destino:** *Broadcast* (ff:ff:ff:ff:ff:ff)
- **Endereço de origem:** 76:9b:e8:f3:9a:43
- **BSS ID:** *HitronTechno_f3:9a:46* (74:9b:e8:f3:9a:46)
- **Endereço da STA:** *Broadcast* (ff:ff:ff:ff:ff:ff)

Neste caso, identificamos que o ponto de acesso (AP) corresponde ao endereço *HitronTechno_f3:9a:46* (74:9b:e8:f3:9a:46), servindo como transmissor e também como identificador BSS. O router no sistema de distribuição (DS) é representado pelo endereço de origem 76:9b:e8:f3:9a:43.

A trama é de *broadcast*, ou seja, está destinada a todas as estações presentes na WLAN.

16. 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 direccionalidade das tramas e os sistemas envolvidos. Dê um exemplo de uma transferência de dados em que é usada a opção RTS/CTS e um outro em que não é usada.

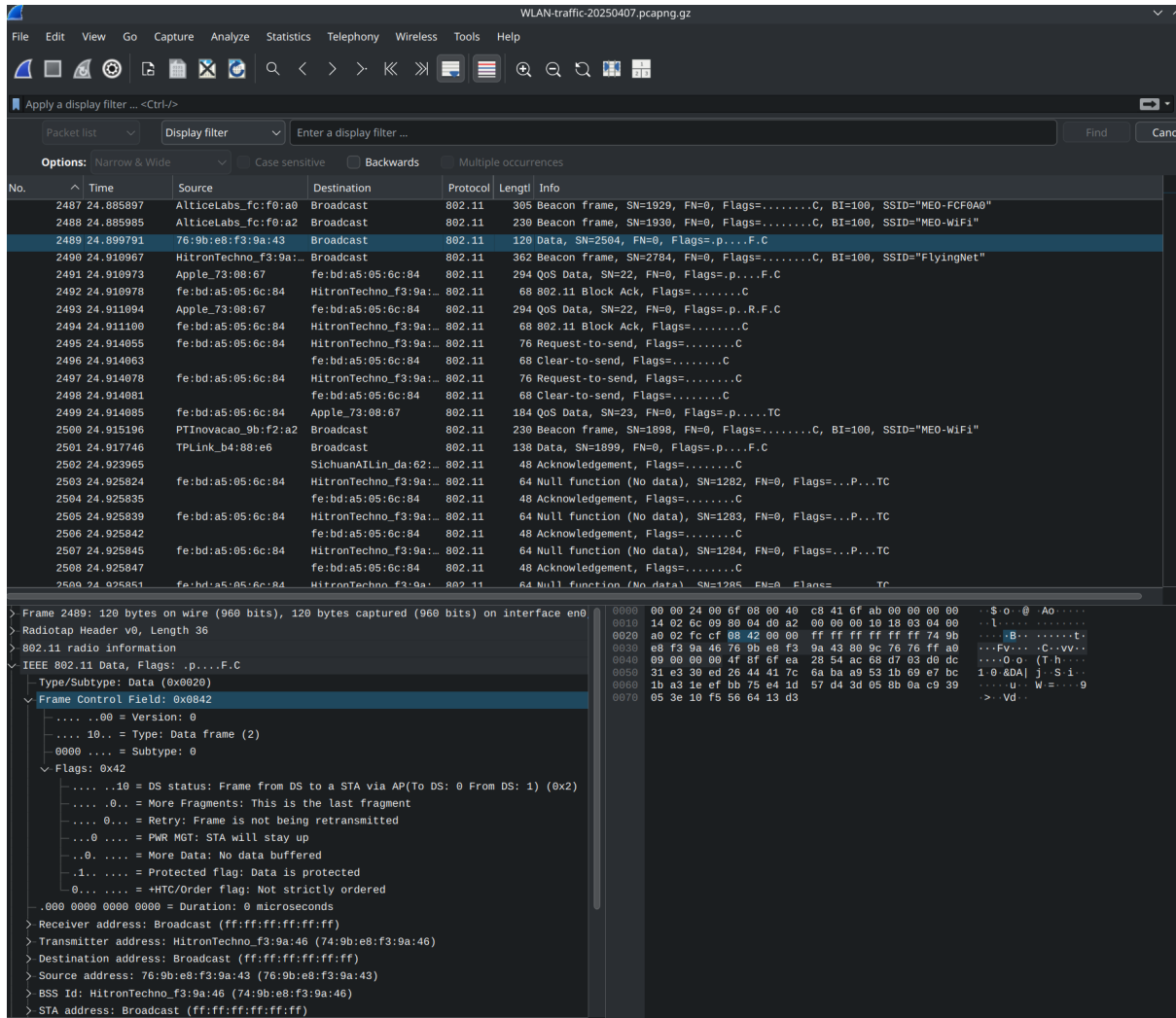


Figura 33: Tráfego de WLAN

A trama **2489** não utiliza o mecanismo *RTS/CTS*. Isso ocorre porque se trata de uma trama *broadcast*, e o uso de *RTS/CTS* é opcional, sendo normalmente aplicado apenas em transmissões *unicast* (entre dois dispositivos específicos).

Nas tramas *broadcast*, como é o caso da 2489, o uso de *RTS/CTS* não é necessário nem comum, pois não há um destinatário único com quem negociar o acesso ao meio. Assim, a trama **2489** é transmitida diretamente, sem pré-reserva do meio por meio do protocolo *RTS/CTS*.

3 Conclusões

Com a Parte 1 deste trabalho prático, foi possível consolidar os conceitos lecionados na unidade curricular, em particular aprofundando os conhecimentos relativos à camada de ligação, tais como os endereços MAC, o protocolo Ethernet e o protocolo ARP.

A Parte 2 teve como principal objetivo a aplicação dos conhecimentos adquiridos sobre redes wireless, incluindo o endereçamento, os tipos e subtipos de tramas Wi-Fi, bem como os mecanismos de controlo de acesso ao meio.

Para a recolha e análise das tramas, foi utilizada a ferramenta *Wireshark*, que permitiu a captura dos pacotes transmitidos num ambiente wireless. Posteriormente, foram aplicados filtros específicos com o intuito de selecionar apenas as tramas pertinentes à resolução do problema em estudo.

Em suma, este trabalho permitiu a consolidação dos conhecimentos teóricos através da sua aplicação prática, contribuindo de forma significativa para o desenvolvimento de competências técnicas na área das redes de computadores, tanto em ambientes com fios como sem fios.