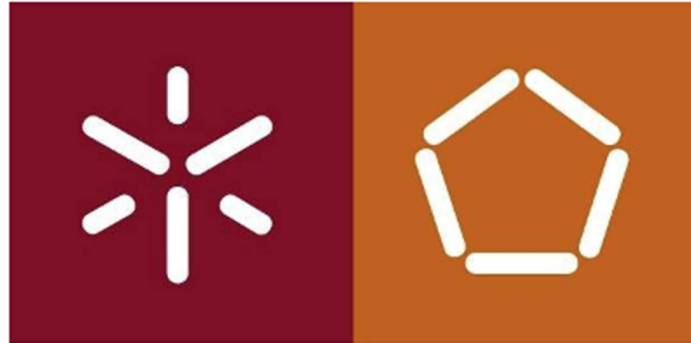


Universidade do Minho

Licenciatura em Engenharia Informática



TP3 - Nível de Ligação Lógica: Redes Ethernet, Protocolo ARP e Redes Locais sem Fios (Wi-Fi)



Trabalho realizado por:

Eduarda Mafalda Martins Vieira, A104098

João Pedro Ferreira e Ferreira, A104539

Maria Leonor Carvalho da Cunha, A103997

Redes de Computadores

PL5 - Grupo 3

abril de 2025

Índice

Parte 1 - Redes Ethernet e Protocolo ARP	3
Exercício 1- Captura e análise de Tramas Ethernet	3
Exercício 2- Protocolo ARP e Domínios de Colisão.....	5
Exercício 3 - Serviço de NAT/PAT.....	10
Parte 2 – Redes locais sem fios (Wi-fi)	10
Exercício 1 – Acesso Rádio.....	11
Exercício 2 – Scanning Passivo e Scanning Ativo.....	12
Exercício 3 – Processo de Associação.....	15
Exercício 4 - Transferências de Dados.....	17
Conclusão.....	19

Parte 1 - Redes Ethernet e Protocolo ARP

Exercício 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.

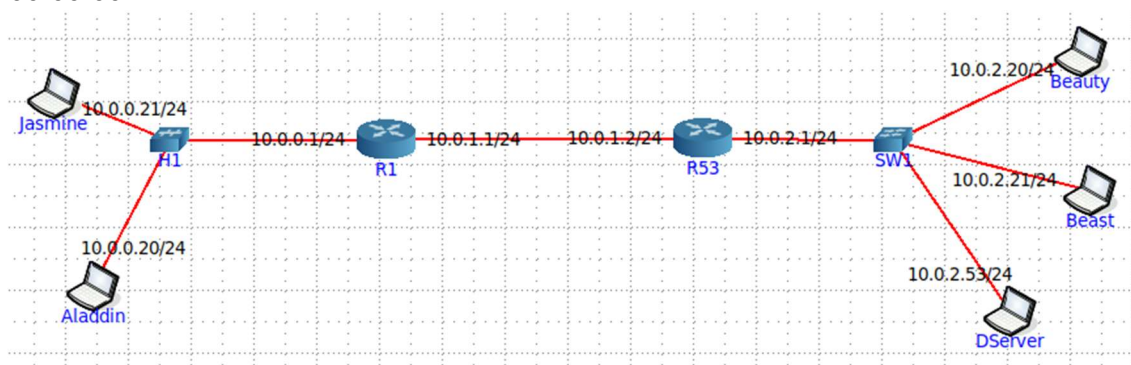


Figura 1 - topologia de rede construída com os dados do grupo

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`. Pare a captura do Wireshark e analise a trama que contém os primeiros dados referentes ao tráfego ssh dirigido ao servidor.

```
root@Jasmine:/tmp/pycore.35823/Jasmine.conf# ssh core@10.0.2.53
The authenticity of host '10.0.2.53 (10.0.2.53)' can't be established.
RSA key fingerprint is SHA256:H9F+oINK8c1HG9gRTALUceXFD1GnIa0XdLFFkbAykEQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.53' (RSA) to the list of known hosts.
core@10.0.2.53's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.15.0-130-generic x86_64)

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

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

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Your Hardware Enablement Stack (HWE) is supported until April 2025.
core@DServer:~$ arp
Address          Hwtype  Hwaddress      Flags Mask      Iface
10.0.2.1         ether   00:00:00:aa:00:05 C                eth0
core@DServer:~$ exit
logout
Connection to 10.0.2.53 closed.
root@Jasmine:/tmp/pycore.35823/Jasmine.conf# arp
Address          Hwtype  Hwaddress      Flags Mask      Iface
10.0.0.1         ether   00:00:00:aa:00:02 C                eth0
root@Jasmine:/tmp/pycore.35823/Jasmine.conf#
```

Figura 2 - Ligação da Jasmine ao servidor DServer e tabelas ARP de DServer e Jasmine

No.	Time	Source	Destination	Protocol	Length	Info
18	13.127475217	10.0.0.21	10.0.2.53	TCP	74	45764 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=217922476 TSecr=0 WS=
19	13.127475217	10.0.2.53	10.0.0.21	TCP	74	22 → 45764 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=3470148649
20	13.127487448	10.0.0.21	10.0.2.53	TCP	66	45764 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=217922476 TSecr=3470148649
21	13.132774330	10.0.0.21	10.0.2.53	SSHv2	108	Client: Protocol (SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.11)
22	13.132808898	10.0.2.53	10.0.0.21	TCP	66	22 → 45764 [ACK] Seq=1 Ack=43 Win=65152 Len=0 TSval=3470148654 TSecr=217922481
23	13.136742176	10.0.2.53	10.0.0.21	SSHv2	108	Server: Protocol (SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.11)

Figura 3 - Captura Wireshark da trama

<p>Frame 18: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface veth1.0.64, id 0</p> <p>Ethernet II, Src: 00:00:00:aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00:aa:00:02 (00:00:00:aa:00:02)</p> <ul style="list-style-type: none"> Destination: 00:00:00:aa:00:02 (00:00:00:aa:00:02) Source: 00:00:00:aa:00:01 (00:00:00:aa:00:01) Type: IPv4 (0x0800) Internet Protocol Version 4, Src: 10.0.0.21, Dst: 10.0.2.53 Transmission Control Protocol, Src Port: 45764, Dst Port: 22, Seq: 0, Len: 0

Figura 4 - Trama Capturada

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

Resposta: O endereço MAC de origem é 00:00:00:aa:00:02 e o endereço MAC de destino é 00:00:00:aa:00:01. O primeiro é o endereço físico da máquina onde foi executado o que foi pedido, o segundo refere-se ao endereço físico do router.

2. 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 endereço é 0x0800 (Figura 4) e significa que a camada superior está a utilizar o protocolo IPv4.

3. 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: Conforme a captura de rede, a trama em questão possui um tamanho total de 74 bytes. No entanto, apenas 54 bytes (soma dos headers: 14 ethernet, 20 IPv4, 20 TCP) são destinados aos dados no nível aplicacional, ou seja, o conteúdo da requisição HTTP.

Cálculo da sobrecarga: 54 bytes / 74 bytes ≈ 0,7297

Sobrecarga em percentagem: 0,7297*100% = 72,97% ≈ 73%

A análise revela que a pilha protocolar introduz uma sobrecarga significativa de 73% no tamanho total da trama.

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

Resposta: O endereço é 00:00:00:aa:00:01, como podemos ver na figura 4, e corresponde ao endereço físico do router com que estamos a comunicar (o endereço MAC da fonte corresponde ao host com IP 10.0.0.21 (Jasmine), na interface de rede associada a esse endereço MAC).

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

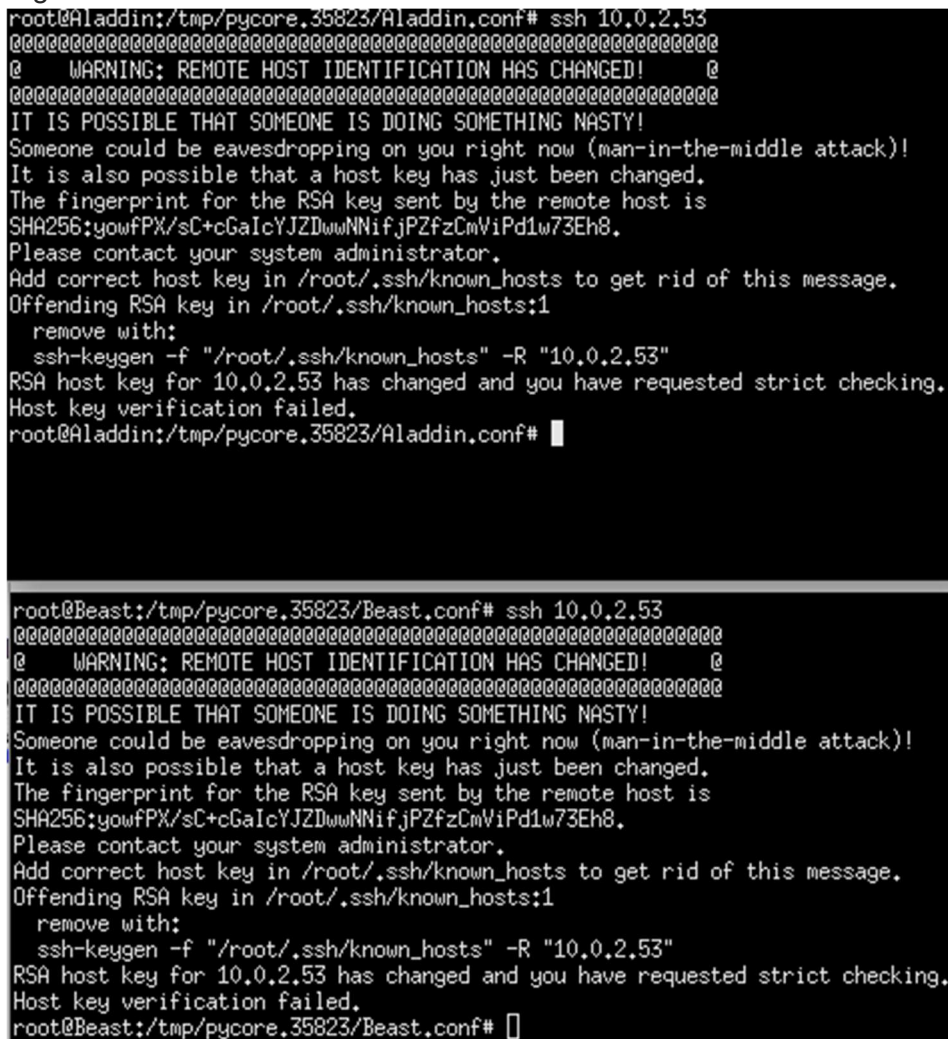
Resposta: O endereço MAC do destino é 00:00:00:aa:00:02 e corresponde ao endereço físico da nossa máquina.

Exercício 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.



```
root@Aladdin:/tmp/pycore.35823/Aladdin.conf# ssh 10.0.2.53
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
SHA256:yowfPX/sC+cGaIcYJZDwwNNifjPZfzCmViPd1w73Eh8.
Please contact your system administrator.
Add correct host key in /root/.ssh/known_hosts to get rid of this message.
Offending RSA key in /root/.ssh/known_hosts:1
  remove with:
    ssh-keygen -f "/root/.ssh/known_hosts" -R "10.0.2.53"
RSA host key for 10.0.2.53 has changed and you have requested strict checking.
Host key verification failed.
root@Aladdin:/tmp/pycore.35823/Aladdin.conf# █

root@Beast:/tmp/pycore.35823/Beast.conf# ssh 10.0.2.53
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
SHA256:yowfPX/sC+cGaIcYJZDwwNNifjPZfzCmViPd1w73Eh8.
Please contact your system administrator.
Add correct host key in /root/.ssh/known_hosts to get rid of this message.
Offending RSA key in /root/.ssh/known_hosts:1
  remove with:
    ssh-keygen -f "/root/.ssh/known_hosts" -R "10.0.2.53"
RSA host key for 10.0.2.53 has changed and you have requested strict checking.
Host key verification failed.
root@Beast:/tmp/pycore.35823/Beast.conf# █
```

Figura 5 – Comando ssh do Aladdin e do Beast

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.

Resposta: A primeira coluna mostra os endereços IPs e a segunda coluna mostra os endereços MAC.

```
root@Aladdin:/tmp/pycore.35823/Aladdin.conf# arp -a
? (10.0.0.1) at 00:00:00:aa:00:02 [ether] on eth0
root@Aladdin:/tmp/pycore.35823/Aladdin.conf#
```

Figura 6 - Comando arp -a no Aladdin

No.	Time	Source	Destination	Protocol	Length	Info
67	85.743364107	00:00:00_aa:00:00	Broadcast	ARP	42	Who has 10.0.0.1? Tell 10.0.0.20
68	85.743408672	00:00:00_aa:00:02	00:00:00_aa:00:00	ARP	42	10.0.0.1 is at 00:00:00:aa:00:02
88	90.951810139	00:00:00_aa:00:02	00:00:00_aa:00:00	ARP	42	Who has 10.0.0.20? Tell 10.0.0.1
89	90.952015607	00:00:00_aa:00:00	00:00:00_aa:00:02	ARP	42	10.0.0.20 is at 00:00:00:aa:00:00

Figura 7 - Tabela ARP

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?

Resposta: O valor hexadecimal do endereço MAC origem é 00:00:00:aa:00:00 e o endereço de destino MAC é ff:ff:ff:ff:ff:ff (Broadcast). Como o nosso dispositivo não está diretamente conectado ao dispositivo de destino, para onde enviamos a mensagem, é necessário enviar a mensagem para todos os dispositivos da rede até que o dispositivo pretendido responda ao seu endereço MAC, é por isso que o nosso endereço de destino é ff:ff:ff:ff:ff:ff.

```

> Frame 67: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface veth2.0.64, id 0
- Ethernet II, Src: 00:00:00_aa:00:00 (00:00:00:aa:00:00), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: 00:00:00_aa:00:00 (00:00:00:aa:00:00)
  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:00:00 (00:00:00:aa:00:00)
  Sender IP address: 10.0.0.20
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 10.0.0.1

```

Figura 8 - Trama com o pedido ARP

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

Resposta: O valor do campo tipo trama é 0x0806 e indica que a camada superior está a usar o protocolo ARP.

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

Resposta: Trata-se efetivamente de um pedido ARP pois temos a indicação que é uma “request” na figura (acima). Para além disso, na mensagem ARP estão contidos os endereços IP e MAC e o protocolo ARP permite converter um endereço IP num endereço MAC.

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

```
▶ Frame 68: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface veth2.0.64, 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: ARP (0x0806)
▼ 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:00:00 (00:00:00:aa:00:00)
  Target IP address: 10.0.0.20
```

Figura 9 - Mensagem ARP que é a resposta ao pedido ARP efetuado

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

Resposta: O valor do campo ARP opcode é 2. Assim podemos concluir que, o IP 10.0.0.20 recebe a mensagem de “request” e está a enviar o seu endereço MAC com resposta.

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

Resposta: No cabeçalho Ethernet, incluem-se 3 informações – o destinatário, o emissor da mensagem, e o tipo. A segunda, o emissor é o equipamento procurado pelo host que emitiu o pedido ARP, que por sua vez, este envia o seu endereço ao host que o procurava.

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).

Resposta:

```

root@Aladdin:/tmp/pycore.35823/Aladdin.conf# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.0.20 netmask 255.255.255.0 broadcast 0.0.0.0
    inet6 fe80::200:ff:feaa:0 prefixlen 64 scopeid 0x20<link>
    inet6 2001::20 prefixlen 64 scopeid 0x0<global>
    ether 00:00:00:aa:00:00 txqueuelen 1000 (Ethernet)
    RX packets 948 bytes 82448 (82,4 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 26 bytes 3554 (3,5 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

root@Aladdin:/tmp/pycore.35823/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.35823/Aladdin.conf# arp
Address HWtype HWaddress Flags Mask Iface
10.0.0.1 ether 00:00:00:aa:00:02 C eth0
root@Aladdin:/tmp/pycore.35823/Aladdin.conf#

```

Figura 10 - Comando ifconfig, netstat -rn e arp no Aladdin

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

Resposta: Com base na figura podemos concluir que o endereço ether é 00:00:00:aa:00:00, e é o endereço MAC de origem. A resposta ARP é encaminhada como unicast, ao contrário do pedido que é transmitido em broadcast. Isto garante que a resposta seja entregue diretamente ao dispositivo que solicitou, aumentando a eficiência e economizando recursos de rede. Optar por enviar a resposta como broadcast seria redundante e iria gerar tráfego desnecessário na rede, já que todos os dispositivos teriam de processar a mensagem ARP.

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?

Resposta:

No caso da Jasmine se analisarmos a captura de tráfego, podemos ver que recebeu o ARP request frame mas também recebeu o ARP reply from source 00:00:00:aa:00:02(R1). Quando a resposta ao ARP request é um ARP response frame, o router R1 transmitiu esta frame ao endereço 00:00:00:aa:00:01, que corresponde ao Aladdin.

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?

Resposta:

No caso da Beauty, não recebe todo o tráfego gerado pelo acesso secreto do Beast. Analisando o tráfego, o dispositivo *Beauty* recebeu a trama de solicitação ARP, como seria de esperar para uma trama com o endereço de destino ff:ff:ff:ff:ff:ff (broadcast); no entanto, esta foi a única trama identificada por este host. Após isso, não houve

mais nenhuma difusão necessária e o dispositivo *Beauty* nunca foi o destino de nenhuma trama relevante durante a interação, portanto, não foi o recetor de nenhuma mensagem.

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?

Resposta:

```
root@Beast:/tmp/pycore.35823/Beast.conf# arp
Address          HWtype  HWaddress      Flags Mask    Iface
10.0.2.53         ether   00:00:00:aa:bb:53  C             eth0
root@Beast:/tmp/pycore.35823/Beast.conf#
```

Figura 11 - comando arp no Beast

```
root@Aladdin:/tmp/pycore.35823/Aladdin.conf# arp
Address          HWtype  HWaddress      Flags Mask    Iface
10.0.0.1          ether   00:00:00:aa:00:02  C             eth0
root@Aladdin:/tmp/pycore.35823/Aladdin.conf#
```

Figura 12 - comando arp no Aladdin

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 receção do primeiro pacote que contém dados do acesso remoto.

Resposta:

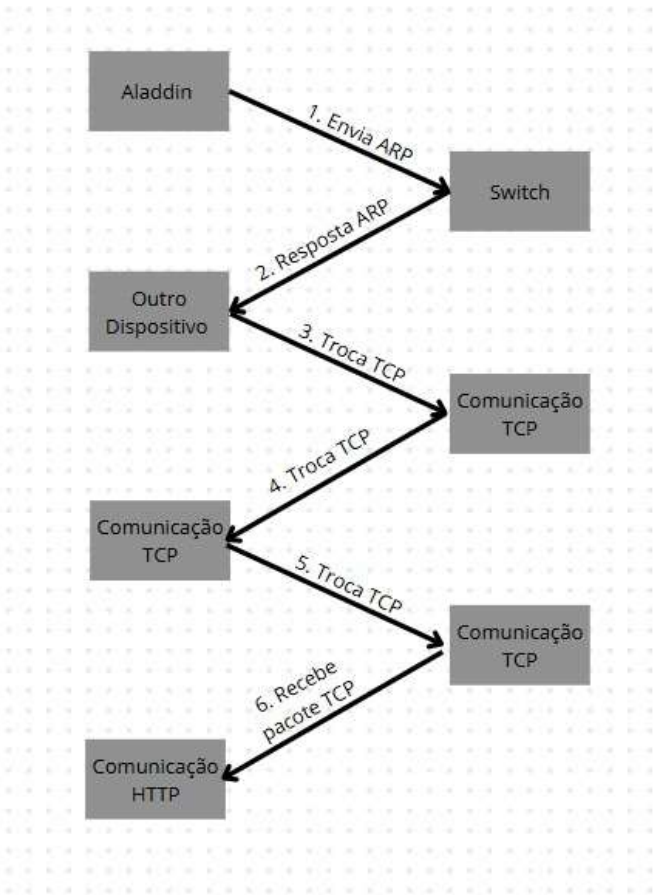


Figura 13 - Diagrama de Tráfego

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.

Resposta:

No.	Time	Source	Destination	Protocol	Length	Info
45	61.665748670	00:00:00_aa:00:05	Broadcast	ARP	42	Who has 10.0.2.53? Tell 10.0.2.1
69	88.582886896	00:00:00_aa:00:07	Broadcast	ARP	42	Who has 10.0.2.53? Tell 10.0.2.21
70	88.582928597	00:00:00_aa:bb:53	00:00:00_aa:00:07	ARP	42	10.0.2.53 is at 00:00:00:aa:bb:53
90	93.753931804	00:00:00_aa:bb:53	00:00:00_aa:00:07	ARP	42	Who has 10.0.2.21? Tell 10.0.2.53
91	93.753943203	00:00:00_aa:00:07	00:00:00_aa:bb:53	ARP	42	10.0.2.21 is at 00:00:00:aa:bb:53

Figura 14- Beast

No.	Time	Source	Destination	Protocol	Length	Info
56	74.213406856	00:00:00_aa:00:05	Broadcast	ARP	42	Who has 10.0.2.53? Tell 10.0.2.1
80	101.130553807	00:00:00_aa:00:07	Broadcast	ARP	42	Who has 10.0.2.53? Tell 10.0.2.21

Figura 15- Beauty

Mac Address	Porta	Nome
10.0.2.20/24	1	Beauty
10.0.2.21/24	2	Beast
10.0.2.53/24	3	DServer

Tabela 1: Tabela de Comutação do Switch

Exercício 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.).

Resposta: Para manter todas as funcionalidades existentes entre as redes privadas (comunicação IP entre Jasmine/Aladdin e Beauty/Beast, acesso SSH ao DServer, etc.), mesmo com o ISP a recusar encaminhamento de endereços privados, a solução recomendada é estabelecer um túnel GRE ou IPsec entre os routers R1 e R53, encapsulando os pacotes IP privados em pacotes com endereços IP públicos. Este túnel permite que as LANs privadas comuniquem de forma segura e transparente, como se estivessem na mesma rede, sem necessidade de alterar o endereçamento interno.

Parte 2 – Redes locais sem fios (Wi-fi)

A Jasmine, como não gosta de ver os cabos da rede Ethernet espalhados pelo palácio, convenceu o Aladdin a substituir a infraestrutura Ethernet por uma rede sem fios. O Aladdin decidiu então comprar equipamento Wi-Fi e fazer uma captura de tráfego para perceber melhor o funcionamento da rede. Descarregue da plataforma de

ensino a captura WLAN-traffic-20250407.pcapng.zip e abra o ficheiro .pcapng no Wireshark. Não se esqueça que deve ser incluída evidência prática que sustente a Resposta às questões.

Exercício 1 – Acesso Rádio

Como pode ser observado, a sequência de bytes capturada inclui meta-informação do nível físico (radiotap header, radio information) obtida do firmware da interface Wi-Fi, para além dos bytes correspondentes a tramas 802.11. Selecione a trama de ordem xy correspondente ao seu identificador de grupo (TurnoGrupo, e.g., 27).

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

No.	Time	Source	Destination	Protocol	Length	Info
40	0.846720	HitronTe_f3:9a:46	Broadcast	802.11	362	Beacon frame, SN=2536, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
41	0.854009	PTinovac_9b:f2:a2	Broadcast	802.11	230	Beacon frame, SN=1338, FN=0, Flags=.....C, BI=100, SSID=ME0-WiFi
42	0.894695	f680:54e7:92ff:fed	ff02::1	ICMPv6	148	Multicast Listener Query
43	0.911432	1c:57:3e:fc:f0:a2	52:90:27:97:1c:c3	802.11	380	Probe Response, SN=1447, FN=0, Flags=.....C, BI=100, SSID=ME0-FCF0A0
44	0.918283	1c:57:3e:fc:f0:a0	52:90:27:97:1c:c3	802.11	380	Probe Response, SN=1447, FN=0, Flags=.....C, BI=100, SSID=ME0-FCF0A0
45	0.923034	1c:57:3e:fc:f0:a0	Broadcast	802.11	305	Beacon frame, SN=1448, FN=0, Flags=.....C, BI=100, SSID=ME0-FCF0A0
46	0.940345	1c:57:3e:fc:f0:a0	52:90:27:97:1c:c3	802.11	380	Probe Response, SN=1447, FN=0, Flags=.....C, BI=100, SSID=ME0-FCF0A0
47	0.941955	1c:57:3e:fc:f0:a0	52:90:27:97:1c:c3	802.11	380	Probe Response, SN=1447, FN=0, Flags=.....C, BI=100, SSID=ME0-FCF0A0
48	0.949617	HitronTe_f3:9a:46	Broadcast	802.11	362	Beacon frame, SN=2537, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
49	0.950397	1c:57:3e:fc:f0:a0	52:90:27:97:1c:c3	802.11	380	Probe Response, SN=1447, FN=0, Flags=.....C, BI=100, SSID=ME0-FCF0A0
50	0.971665	1c:57:3e:fc:f0:a0	52:90:27:97:1c:c3	802.11	380	Probe Response, SN=1447, FN=0, Flags=.....C, BI=100, SSID=ME0-FCF0A0
51	0.971777	1c:57:3e:fc:f0:a0	52:90:27:97:1c:c3	802.11	380	Probe Response, SN=1447, FN=0, Flags=.....C, BI=100, SSID=ME0-FCF0A0
52	0.974066	1c:57:3e:fc:f0:a2	52:90:27:97:1c:c3	802.11	224	Probe Response, SN=1450, FN=0, Flags=.....C, BI=100, SSID=ME0-WiFi
53	0.974079	1c:57:3e:fc:f0:a2	52:90:27:97:1c:c3	802.11	224	Probe Response, SN=1450, FN=0, Flags=.....C, BI=100, SSID=ME0-WiFi
54	0.981156	1c:57:3e:fc:f0:a2	52:90:27:97:1c:c3	802.11	224	Probe Response, SN=1450, FN=0, Flags=.....C, BI=100, SSID=ME0-WiFi

Frame 53: 224 bytes on wire (1792 bits), 224 bytes captured (1792 bits) on interface en0, id 0

Radiotap Header v0, Length 36

Header revision: 0

Header pad: 0

Header length: 36

Present flags

MAC timestamp: 2852273386

Flags: 0x10

Data rate: 1.0 Mb/s

Channel frequency: 2412 [BG 1]

Channel flags: 0x0480, 2 GHz spectrum, Dynamic CCK-OFDM

Antenna signal: -87dBm

Antenna noise: -93dBm

Antenna: 0

Vendor namespace: Broadcom-3

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): -87dBm

Noise level (dBm): -93dBm

Signal/noise ratio (dB): 6dB

TSF timestamp: 2852273386

Duration: 1696µs

IEEE 802.11 Probe Response, Flags:R...C

Type/Subtype: Probe Response (0x0095)

Frame Control Field: 0x5098

000 0001 0011 1010 = Duration: 314 microseconds

Receiver address: 52:90:27:97:1c:c3 (52:90:27:97:1c:c3)

Destination address: 52:90:27:97:1c:c3 (52:90:27:97:1c:c3)

Transmitter address: 1c:57:3e:fc:f0:a2 (1c:57:3e:fc:f0:a2)

Source address: 1c:57:3e:fc:f0:a2 (1c:57:3e:fc:f0:a2)

Figura 16 - Trama 53 selecionada

Resposta: A frequência 2412MHz no canal 1.

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

Resposta: A versão é 802.11 Probe Response

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.

Resposta:

Como comprovamos na figura 12, o data rate é de 1,0 Mb/s. Sendo assim, o débito máximo suportado é de 11 Mb/s. O protocolo 802.11 é capaz de suportar velocidades de até 600 Mb/s, dependendo das condições da rede e das configurações utilizadas. Como podemos observar na figura 12, o data rate da trama é de 1,0 Mb/s. No entanto, isso não significa que o utilizador final esteja a receber dados a essa velocidade. O débito máximo real depende de diversos fatores, como o protocolo de camada superior utilizado, o tipo de modulação, a taxa de erro da rede e as configurações da

interface Wi-Fi. O protocolo 802.11 possui diferentes versões, cada uma com sua taxa máxima teórica. Por exemplo, o 802.11b suporta até 11 Mb/s, enquanto o 802.11ac pode chegar a 1.750 Mb/s (em condições ideais). É importante ressaltar que a velocidade real de uma rede Wi-Fi raramente atinge a taxa máxima teórica. Interferência de outras redes, obstáculos físicos, congestionamento da rede e configurações incorretas podem reduzir significativamente o desempenho.

Exercício 2 – Scanning Passivo e Scanning Ativo

Como referido, as tramas beacon permitem efetuar scanning passivo em redes IEEE 802.11 (Wi-Fi). Para a captura de tramas disponibilizada, e considerando xy o seu nº de TurnoGrupo (PLxy), responda às seguintes questões:

No.	Time	Source	Destination	Protocol	Length	Info
151	2.125694	1c:57:3e:fc:f0:a0	b8:2d:28:7a:9b:68	802.11	48	Acknowledgement, Flags=.....C
152	2.151581	1c:57:3e:fc:f0:a0	Broadcast	802.11	305	Beacon frame, SN=1478, FN=0, Flags=.....C, BI=100, SSID=ME0-FCF8A0
153	2.162795	PTInovac_29:a9:c2	Continen_95:b6:21	802.11	240	Probe Response, SN=3884, FN=0, Flags=.....C, BI=100, SSID=ME0-WiFi


```

Frame 153: 230 bytes on wire (1840 bits), 230 bytes captured (1840 bits) on interface en0, id 0
  Interface id: 0 (en0)
  Encapsulation type: IEEE 802.11 plus radiotap radio header (23)
  Arrival Time: Apr 7, 2025 13:22:06.452135000 WEST
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1744628526.452135000 seconds
  [Time delta from previous captured frame: 0.000066000 seconds]
  [Time delta from previous displayed frame: 0.000066000 seconds]
  [Time since reference or first frame: 2.151647000 seconds]
  Frame Number: 153
  Frame Length: 230 bytes (1840 bits)
  Capture Length: 230 bytes (1840 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: radiotap:wlan_radio:wlan]
  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
      [Duration: 1744us]
    IEEE 802.11 Beacon frame, Flags: .....C
      Type/Subtype: Beacon frame (0x0008)
      Frame Control Field: 0x0000
        .... 00 = Version: 0
        .... 00.. = Type: Management frame (0)
        1000 .... = Subtype: 8
        Flags: 0x00
        .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: 1c:57:3e:fc:f0:a2 (1c:57:3e:fc:f0:a2)
        Source address: 1c:57:3e:fc:f0:a2 (1c:57:3e:fc:f0:a2)
        BSS Id: 1c:57:3e:fc:f0:a2 (1c:57:3e:fc:f0:a2)
        .... 0000 = Fragment number: 0
        0101 1100 1000 .... = Sequence number: 1480
        Frame check sequence: 0xa5b78fd9 [unverified]
        [FCS Status: Unverified]
      IEEE 802.11 Wireless Management
  
```

Figura 15 17 - seleção de trama

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)?

```

IEEE 802.11 Beacon frame, Flags: .....C
  Type/Subtype: Beacon frame (0x0008)
  Frame Control Field: 0x0000
    .... 00 = Version: 0
    .... 00.. = Type: Management frame (0)
    1000 .... = Subtype: 8
    Flags: 0x00
    .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: 1c:57:3e:fc:f0:a2 (1c:57:3e:fc:f0:a2)
    Source address: 1c:57:3e:fc:f0:a2 (1c:57:3e:fc:f0:a2)
    BSS Id: 1c:57:3e:fc:f0:a2 (1c:57:3e:fc:f0:a2)
    .... 0000 = Fragment number: 0
    0101 1100 1000 .... = Sequence number: 1480
    Frame check sequence: 0xa5b78fd9 [unverified]
  
```

Figura 16 18 - tipo e subtipo da trama

Resposta: A trama que selecionamos foi a 153, e como podemos ver na figura 13, esta pertence ao tipo Management (0) e o seu subtipo é Beacon (8). Através do anexo fornecido no enunciado podemos verificar que estes pertencem ao Frame Control.

5. 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")

Frame check sequence: 0xa5b78fd9 [correct]
[FCS Status: Good]

Figura 17 19 - FCS

Resposta: O pacote capturado pelo Wireshark com a indicação "[FCS Status: Good]", o que significa que o FCS presente no pacote, ou seja, o CRC está ativo na rede.

6. Justifique o porquê de ser necessário usar detecção de erros em redes sem fios. As tramas beacon são enviadas periodicamente e permitem especificar parâmetros de funcionamento para apoiar a operação e a gestão das ligações sem fios.

Resposta: É necessário usar detecção de erros em redes sem fios porque estas estão particularmente sujeitas a diversos fatores que comprometem a integridade da transmissão de dados. Interferências causadas por dispositivos eletrônicos, ruídos eletromagnéticos, atenuação do sinal provocada por obstáculos físicos e pela distância entre transmissor e recetor, bem como colisões no canal de comunicação, são causas frequentes de erros. Além disso, a mobilidade dos dispositivos — característica típica deste tipo de rede — aumenta a variabilidade das condições do canal. A detecção de erros garante que os dados recebidos sejam válidos, contribuindo para uma comunicação fiável e eficiente, essencial para o correto funcionamento da rede.

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.

No.	Time	Source	Destination	Protocol	Length	Info
152	2.151581	1c:57:3e:fc:f0:a0	Broadcast	802.11	305	Beacon frame, SN=1470, FN=0, Flags=.....C, BI=100, SSID=MEQ-FCF0A0
153	2.151547	1c:57:3e:fc:f0:a0	Broadcast	802.11	240	Probe Response, SN=3884, FN=0, Flags=.....C, BI=100, SSID=MEQ-WiFi1
154	2.152705	PfInovac.29:a8:c2	Continen.95:b6:21	802.11	240	Probe Response, SN=3884, FN=0, Flags=.....C, BI=100, SSID=MEQ-WiFi1
155	2.171531	PfInovac.29:a8:c2	Continen.95:b6:21	802.11	240	Probe Response, SN=3884, FN=0, Flags=.....C, BI=100, SSID=MEQ-WiFi1
156	2.178106	HitronTe.f3:9a:46	Broadcast	802.11	362	Beacon frame, SN=2549, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
157	2.184381	PfInovac.3b:f2:a0	Broadcast	802.11	337	Beacon frame, SN=1368, FN=0, Flags=.....C, BI=100, SSID=MEQ-96F2A0
158	2.201981	1c:57:3e:fc:f0:a0	Continen.95:b6:21	802.11	380	Probe Response, SN=1481, FN=0, Flags=.....C, BI=100, SSID=MEQ-FCF0A0
159	2.202641	1c:57:3e:fc:f0:a0	Continen.95:b6:21	802.11	380	Probe Response, SN=1481, FN=0, Flags=.....C, BI=100, SSID=MEQ-FCF0A0
160	2.205780	1c:57:3e:fc:f0:a0	Continen.95:b6:21	802.11	380	Probe Response, SN=1481, FN=0, Flags=.....C, BI=100, SSID=MEQ-FCF0A0
161	2.209940	1c:57:3e:fc:f0:a0	Continen.95:b6:21	802.11	380	Probe Response, SN=1481, FN=0, Flags=.....C, BI=100, SSID=MEQ-FCF0A0
162	2.213451	1c:57:3e:fc:f0:a0	Continen.95:b6:21	802.11	380	Probe Response, SN=1481, FN=0, Flags=.....C, BI=100, SSID=MEQ-FCF0A0
163	2.216771	1c:57:3e:fc:f0:a0	Continen.95:b6:21	802.11	380	Probe Response, SN=1481, FN=0, Flags=.....C, BI=100, SSID=MEQ-FCF0A0

IEEE 802.11 Beacon frame, Flags:C
Time/Channel: Beacon frame (3050000)

Figura 1820 - Débitos dos Tramas

IEEE 802.11 Wireless Management
Fixed parameters (12 bytes)
Timestamp: 6976143721696
Beacon Interval: 0.102400 [Seconds]
Capabilities Information: 0x1481
.....1 = ESS capabilities: Transmitter is an AP
.....0 = IBSS status: Transmitter belongs to a BSS
.....00 = CFP participation capabilities: No point coordinator at AP (0x00)
.....0 = Privacy: AP/STA cannot support WEP
.....0 = Short Preamble: Not Allowed
.....0 = PBCC: Not Allowed
.....0 = Channel Agility: Not in use
.....0 = Spectrum Management: Not Implemented
.....1 = Short Slot Time: In use
.....0 = Automatic Power Save Delivery: Not Implemented
.....1 = Radio Measurement: Implemented
.....0 = DSSS-OFDM: Not Allowed
.....0 = Delayed Block Ack: Not Implemented
.....0 = Immediate Block Ack: Not Implemented
Tagged parameters (154 bytes)
Tag: SSID parameter set: MEQ-WiFi1
Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 18, 24, 36, 54, [Mbit/sec]
Tag: DS Parameter set: Current Channel: 1
Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
Tag: ERP Information
Tag: Extended Supported Rates 6, 9, 12, 48, [Mbit/sec]
Tag: QSS Load Element 802.11e CCA Version
Tag: Measurement Pilot Transmission
Tag: RM Enabled Capabilities (5 octets)
Tag: HT Capabilities (802.11n D1.10)
Tag: HT Information (802.11n D1.10)
Tag: Extended Capabilities (8 octets)
Tag: Vendor Specific: Broadcom
Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element

Figura 19 21 - Débitos dos Tramas

Resposta:

O intervalo de tempo previsto entre tramas beacon consecutivas é anunciado na trama, em Fixed parameters -> Beacon Interval que, neste caso, é 0.102400 segundos (visível na figura acima). A periodicidade como podemos ver na figura acima é

0,016367 , ((2.178106-2.151647)+(2.184381-2.178106))/2. As taxas de transmissão suportadas são:

- 1Mb/s
- 2 Mb/s
- 5.5 Mb/s
- 11 Mb/s
- 6 Mb/s
- 9 Mb/s
- 12 Mb/s
- 18 Mb/s;

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).

wlan.ssid					
No.	Time	Source	Destination	Protocol	Length Info
888	1.518343	PTInovac_67:77:62	Broadcast	802.11	365 Beacon frame, SN=1613, FN=0, Flags=.....C, BI=100, SSID=MEO-677760
889	1.512539	PTInovac_67:77:62	Broadcast	802.11	230 Beacon frame, SN=1614, FN=0, Flags=.....C, BI=100, SSID=MEO-WiFi1
831	1.519279	Tp-LinkT_a3:af:08	OnePlusT_92:95:d9	802.11	391 Probe Response, SN=1011, FN=0, Flags=.....C, BI=100, SSID=TP-LINK AP AF08
832	1.521291	Tp-LinkT_a3:af:08	OnePlusT_92:95:d9	802.11	391 Probe Response, SN=1011, FN=0, Flags=.....C, BI=100, SSID=TP-LINK AP AF08
833	1.524424	Tp-LinkT_a3:af:08	OnePlusT_92:95:d9	802.11	391 Probe Response, SN=1011, FN=0, Flags=.....C, BI=100, SSID=TP-LINK AP AF08
840	1.534013	PTInovac_9e:9b:b2	Broadcast	802.11	365 Beacon frame, SN=65, FN=0, Flags=.....C, BI=100, SSID=MEO-9E9880
841	1.536496	PTInovac_9e:9b:b2	Broadcast	802.11	230 Beacon frame, SN=66, FN=0, Flags=.....C, BI=100, SSID=MEO-WiFi1
845	1.558871	Tp-LinkT_a3:af:08	Broadcast	802.11	282 Beacon frame, SN=1012, FN=0, Flags=.....C, BI=100, SSID=TP-LINK AP AF08
846	1.612845	PTInovac_67:77:60	Broadcast	802.11	365 Beacon frame, SN=1615, FN=0, Flags=.....C, BI=100, SSID=MEO-677760
847	1.612940	PTInovac_67:77:62	Broadcast	802.11	230 Beacon frame, SN=1616, FN=0, Flags=.....C, BI=100, SSID=MEO-WiFi1
848	1.641108	PTInovac_9e:9b:b2	Broadcast	802.11	230 Beacon frame, SN=68, FN=0, Flags=.....C, BI=100, SSID=MEO-WiFi1
849	1.671593	00:76:1b:52:87:00	Broadcast	802.11	368 Beacon frame, SN=3839, FN=0, Flags=.....C, BI=100, SSID=Vodafone-528777
854	1.697119	PTInovac_9b:72:a2	Broadcast	802.11	230 Beacon frame, SN=231, FN=0, Flags=.....C, BI=100, SSID=MEO-WiFi1
859	1.715832	PTInovac_67:77:60	Broadcast	802.11	365 Beacon frame, SN=1617, FN=0, Flags=.....C, BI=100, SSID=MEO-677760
860	1.715835	PTInovac_67:77:62	Broadcast	802.11	230 Beacon frame, SN=1618, FN=0, Flags=.....C, BI=100, SSID=MEO-WiFi1
870	1.741780	PTInovac_9e:9b:b2	Broadcast	802.11	365 Beacon frame, SN=69, FN=0, Flags=.....C, BI=100, SSID=MEO-9E9880
871	1.741837	PTInovac_9e:9b:b2	Broadcast	802.11	230 Beacon frame, SN=70, FN=0, Flags=.....C, BI=100, SSID=MEO-WiFi1
886	1.818806	PTInovac_67:77:60	Broadcast	802.11	365 Beacon frame, SN=1619, FN=0, Flags=.....C, BI=100, SSID=MEO-677760
887	1.818811	PTInovac_67:77:62	Broadcast	802.11	230 Beacon frame, SN=1620, FN=0, Flags=.....C, BI=100, SSID=MEO-WiFi1
888	1.826046	a6:ef:15:08:32:99	Broadcast	802.11	222 Beacon frame, SN=1338, FN=0, Flags=.....C, BI=100, SSID=phi.F41927C3C600
891	1.865868	Tp-LinkT_a3:af:08	Broadcast	802.11	282 Beacon frame, SN=1015, FN=0, Flags=.....C, BI=100, SSID=TP-LINK AP AF08
903	1.919996	PTInovac_67:77:60	Broadcast	802.11	365 Beacon frame, SN=1621, FN=0, Flags=.....C, BI=100, SSID=MEO-677760
904	1.921826	PTInovac_67:77:62	Broadcast	802.11	230 Beacon frame, SN=1622, FN=0, Flags=.....C, BI=100, SSID=MEO-WiFi1
908	1.946544	PTInovac_9e:9b:b2	Broadcast	802.11	365 Beacon frame, SN=73, FN=0, Flags=.....C, BI=100, SSID=MEO-9E9880
909	1.949194	PTInovac_9e:9b:b2	Broadcast	802.11	230 Beacon frame, SN=74, FN=0, Flags=.....C, BI=100, SSID=MEO-WiFi1
923	2.019669	PTInovac_67:77:60	Broadcast	802.11	365 Beacon frame, SN=1623, FN=0, Flags=.....C, BI=100, SSID=MEO-677760
924	2.027067	PTInovac_67:77:62	Broadcast	802.11	230 Beacon frame, SN=1624, FN=0, Flags=.....C, BI=100, SSID=MEO-WiFi1

Figura 2022 - SSIDs a operar na vizinhança da STA

Resposta: De modo a obter os SSIDs dos APs, utilizamos o filtro wlan.ssid no wireshark que nos dá as tramas beacon capturados provenientes dos APs que conseguem comunicar com a STA. Com o uso deste filtro chegamos à conclusão que os três SSIDs são MEO, TPLINK, Vodafone e phi.

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

84	1.422604	1c:57:3e:fc:f0:a2	Continen_95:b6:21	802.11	224 Probe Response, SN=1460, FN=0, Flags=...R...C, BI=100, SSID=MEO-WiFi1
85	1.426046	1c:57:3e:fc:f0:a2	Continen_95:b6:21	802.11	224 Probe Response, SN=1460, FN=0, Flags=...R...C, BI=100, SSID=MEO-WiFi1
90	1.479261	PTInovac_29:a9:c2	Continen_95:b6:21	802.11	240 Probe Response, SN=3854, FN=0, Flags=...R...C, BI=100, SSID=MEO-WiFi1
91	1.494785	1c:57:3e:fc:f0:a0	Continen_95:b6:21	802.11	380 Probe Response, SN=1463, FN=0, Flags=...R...C, BI=100, SSID=MEO-FCF0A0
92	1.496590	1c:57:3e:fc:f0:a0	Continen_95:b6:21	802.11	380 Probe Response, SN=1463, FN=0, Flags=...R...C, BI=100, SSID=MEO-FCF0A0
93	1.503422	1c:57:3e:fc:f0:a0	Continen_95:b6:21	802.11	380 Probe Response, SN=1463, FN=0, Flags=...R...C, BI=100, SSID=MEO-FCF0A0
94	1.510858	PTInovac_29:a9:c0	Continen_95:b6:21	802.11	434 Probe Response, SN=3855, FN=0, Flags=...R...C, BI=100, SSID=Masmorra do
95	1.510980	1c:57:3e:fc:f0:a0	Continen_95:b6:21	802.11	380 Probe Response, SN=1463, FN=0, Flags=...R...C, BI=100, SSID=MEO-FCF0A0
96	1.520171	1c:57:3e:fc:f0:a0	Continen_95:b6:21	802.11	380 Probe Response, SN=1463, FN=0, Flags=...R...C, BI=100, SSID=MEO-FCF0A0
97	1.520275	1c:57:3e:fc:f0:a0	Continen_95:b6:21	802.11	380 Probe Response, SN=1463, FN=0, Flags=...R...C, BI=100, SSID=MEO-FCF0A0
98	1.523463	PTInovac_29:a9:c0	Continen_95:b6:21	802.11	434 Probe Response, SN=3855, FN=0, Flags=...R...C, BI=100, SSID=Masmorra do
99	1.526654	1c:57:3e:fc:f0:a0	Continen_95:b6:21	802.11	380 Probe Response, SN=1463, FN=0, Flags=...R...C, BI=100, SSID=MEO-FCF0A0
100	1.529756	1c:57:3e:fc:f0:a2	Continen_95:b6:21	802.11	224 Probe Response, SN=1464, FN=0, Flags=...R...C, BI=100, SSID=MEO-WiFi1
103	1.539398	1c:57:3e:fc:f0:a2	Continen_95:b6:21	802.11	224 Probe Response, SN=1464, FN=0, Flags=...R...C, BI=100, SSID=MEO-WiFi1
104	1.548625	1c:57:3e:fc:f0:a2	Continen_95:b6:21	802.11	224 Probe Response, SN=1464, FN=0, Flags=...R...C, BI=100, SSID=MEO-WiFi1
105	1.556872	1c:57:3e:fc:f0:a2	Continen_95:b6:21	802.11	224 Probe Response, SN=1464, FN=0, Flags=...R...C, BI=100, SSID=MEO-WiFi1
106	1.556898	1c:57:3e:fc:f0:a2	Continen_95:b6:21	802.11	224 Probe Response, SN=1464, FN=0, Flags=...R...C, BI=100, SSID=MEO-WiFi1
108	1.569260	1c:57:3e:fc:f0:a2	Continen_95:b6:21	802.11	224 Probe Response, SN=1464, FN=0, Flags=...R...C, BI=100, SSID=MEO-WiFi1
122	1.810785	1c:57:3e:fc:f0:a0	Continen_95:b6:21	802.11	380 Probe Response, SN=1471, FN=0, Flags=...R...C, BI=100, SSID=MEO-FCF0A0
123	1.821220	1c:57:3e:fc:f0:a0	Continen_95:b6:21	802.11	380 Probe Response, SN=1471, FN=0, Flags=...R...C, BI=100, SSID=MEO-FCF0A0
124	1.822843	1c:57:3e:fc:f0:a0	Continen_95:b6:21	802.11	380 Probe Response, SN=1471, FN=0, Flags=...R...C, BI=100, SSID=MEO-FCF0A0
125	1.830404	PTInovac_29:a9:c0	Continen_95:b6:21	802.11	434 Probe Response, SN=3867, FN=0, Flags=...R...C, BI=100, SSID=Masmorra do
126	1.837565	1c:57:3e:fc:f0:a0	Continen_95:b6:21	802.11	380 Probe Response, SN=1471, FN=0, Flags=...R...C, BI=100, SSID=MEO-FCF0A0
127	1.837589	1c:57:3e:fc:f0:a0	Continen_95:b6:21	802.11	380 Probe Response, SN=1471, FN=0, Flags=...R...C, BI=100, SSID=MEO-FCF0A0
128	1.846958	1c:57:3e:fc:f0:a0	Continen_95:b6:21	802.11	380 Probe Response, SN=1471, FN=0, Flags=...R...C, BI=100, SSID=MEO-FCF0A0
131	1.856365	1c:57:3e:fc:f0:a0	Continen_95:b6:21	802.11	380 Probe Response, SN=1471, FN=0, Flags=...R...C, BI=100, SSID=MEO-FCF0A0
132	1.862554	1c:57:3e:fc:f0:a2	Continen_95:b6:21	802.11	224 Probe Response, SN=1474, FN=0, Flags=...R...C, BI=100, SSID=MEO-WiFi1
133	1.862648	1c:57:3e:fc:f0:a2	Continen_95:b6:21	802.11	224 Probe Response, SN=1474, FN=0, Flags=...R...C, BI=100, SSID=MEO-WiFi1
134	1.865830	1c:57:3e:fc:f0:a2	Continen_95:b6:21	802.11	224 Probe Response, SN=1474, FN=0, Flags=...R...C, BI=100, SSID=MEO-WiFi1
136	1.875978	1c:57:3e:fc:f0:a2	Continen_95:b6:21	802.11	224 Probe Response, SN=1474, FN=0, Flags=...R...C, BI=100, SSID=MEO-WiFi1
137	1.875984	1c:57:3e:fc:f0:a2	Continen_95:b6:21	802.11	224 Probe Response, SN=1474, FN=0, Flags=...R...C, BI=100, SSID=MEO-WiFi1
138	1.881273	1c:57:3e:fc:f0:a2	Continen_95:b6:21	802.11	224 Probe Response, SN=1474, FN=0, Flags=...R...C, BI=100, SSID=MEO-WiFi1
139	1.881281	1c:57:3e:fc:f0:a2	Continen_95:b6:21	802.11	224 Probe Response, SN=1474, FN=0, Flags=...R...C, BI=100, SSID=MEO-WiFi1
145	2.062284	PTInovac_29:a9:c2	Continen_95:b6:21	802.11	240 Probe Response, SN=3880, FN=0, Flags=...R...C, BI=100, SSID=MEO-WiFi1
154	2.162705	PTInovac_29:a9:c2	Continen_95:b6:21	802.11	240 Probe Response, SN=3884, FN=0, Flags=...R...C, BI=100, SSID=MEO-WiFi1
155	2.171531	PTInovac_29:a9:c2	Continen_95:b6:21	802.11	240 Probe Response, SN=3884, FN=0, Flags=...R...C, BI=100, SSID=MEO-WiFi1
158	2.201981	1c:57:3e:fc:f0:a0	Continen_95:b6:21	802.11	380 Probe Response, SN=1481, FN=0, Flags=...R...C, BI=100, SSID=MEO-FCF0A0

Figura 23 21 - tráfego das tramas probing request/response

Resposta: Usamos o filtro `wlan.fc.type_subtype == 4 || wlan.fc.type_subtype == 5`

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.

Resposta: Como podemos ver na figura 14, a força do sinal é -93dBm. A força do sinal não é de confiança, pelo que não é dos piores sinais mas a probabilidade da conexão ser estabelecida é reduzida, o que significa que, a probabilidade de receber tramas, nestas condições, menor.

11. 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:

De acordo com a tabela de referência do Anexo II, precisamos considerar que:

1. Com um sinal de -93 dBm, estamos bem abaixo até mesmo da sensibilidade mínima para o MCS 0 (BPSK 1/2) que é de -82 dBm.
2. Em condições tão desfavoráveis, o sistema provavelmente tentaria usar a modulação mais robusta possível, que seria BPSK 1/2 (MCS 0), mas mesmo esta teria dificuldade em estabelecer conexão.
3. Para o MCS 0, a taxa de transmissão máxima é de 6,5 Mbps (com GI de 800 ns).
4. Considerando um fator de redução muito maior devido ao sinal extremamente fraco, interferências, ruído e perdas de caminho (em vez de 50%, um fator de redução de aproximadamente 90% seria mais realista para um sinal tão fraco), a taxa de transmissão efetiva seria:

Taxa efetiva = 6,5 Mbps * 0,1 = 0,65 Mbps

5. O débito da ligação Wi-Fi é calculado da seguinte forma:

Débito = Taxa de transmissão efetiva * Tempo de transmissão útil
 $\text{Débito} = 0,65 \text{ Mbps} * (1000 \text{ bytes} / 8 \text{ bits/byte}) * (1 \text{ ms} / 1000 \text{ ms/s})$
 $\text{Débito} = 81,25 \text{ bps}$

Portanto, com um sinal de -93 dBm, o débito esperado seria de aproximadamente 81,25 bps, o que é extremamente baixo e praticamente inviável para qualquer aplicação prática. Na realidade, a conexão provavelmente seria instável ou não se estabeleceria de todo.

Exercício 3 – Processo de Associação

Numa rede Wi-Fi estruturada, um nodo ou STA deve associar-se a um ponto de acesso antes de enviar dados. O processo de associação nas redes IEEE 802.11 é executada enviando a trama association request da STA para o AP e a trama association response enviada pelo AP para a STA, em resposta ao pedido de associação recebido. Este processo é antecedido por uma fase de autenticação. Para

a sequência de tramas capturada:

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.

Resposta: Para obter o conjunto completo de conexões entre a estação (STA) e o ponto de acesso (AP) em um processo de associação, foi necessário desenvolver um filtro que nos fornecesse, de maneira conveniente, um conjunto organizado dessas conexões. Sendo assim, o filtro aplicado foi:

wlan.fc.type == 0 && (wlan.fc.type subtype == 0 or wlan.fc.type subtype == 1 or wlan.fc.type subtype == 11)

A tabela apresentada contém informações sobre os filtros e as tramas associadas a eles. Estamos, essencialmente, filtrando os quadros de gerenciamento (Management Frames) e, dentro deles, aqueles que são do tipo "Association Request" (Solicitação de Associação), "Association Response" (Resposta de Associação) e "Authentication" (Autenticação). Essas são fases relevantes do processo de associação. Após a aplicação do filtro, obtiveram-se as tramas seguintes:

wlan.fc.type == 0 && (wlan.fc.type subtype == 0 or wlan.fc.type subtype == 1 or wlan.fc.type subtype == 11)					
No.	Time	Source	Destination	Protocol	Length Info
2042	23.707373	fe:bd:a5:05:6c:84	HitronTe_f3:9a:46	802.11	186 Authentication, SN=3343, FN=0, Flags=.....C
2044	23.707398	HitronTe_f3:9a:46	fe:bd:a5:05:6c:84	802.11	70 Authentication, SN=3852, FN=0, Flags=.....C
2046	23.710405	fe:bd:a5:05:6c:84	HitronTe_f3:9a:46	802.11	202 Association Request, SN=3344, FN=0, Flags=.....C, SSID=FlyingNet
2048	23.716772	HitronTe_f3:9a:46	fe:bd:a5:05:6c:84	802.11	210 Association Response, SN=3853, FN=0, Flags=.....C
10365	56.657756	Apple_71:41:a1	HitronTe_f3:9a:46	802.11	81 Authentication, SN=1387, FN=0, Flags=.....C
10368	56.659782	HitronTe_f3:9a:46	Apple_71:41:a1	802.11	70 Authentication, SN=3889, FN=0, Flags=.....C
10372	56.661907	Apple_71:41:a1	HitronTe_f3:9a:46	802.11	205 Association Request, SN=1388, FN=0, Flags=.....C, SSID=FlyingNet
10376	56.669795	HitronTe_f3:9a:46	Apple_71:41:a1	802.11	210 Association Response, SN=3890, FN=0, Flags=.....C
10530	57.303645	AzureWav_0f:0e:9b	HitronTe_f3:9a:46	802.11	70 Authentication, SN=257, FN=0, Flags=.....C
10532	57.303655	HitronTe_f3:9a:46	AzureWav_0f:0e:9b	802.11	70 Authentication, SN=3891, FN=0, Flags=.....C
10534	57.304688	HitronTe_f3:9a:46	AzureWav_0f:0e:9b	802.11	70 Authentication, SN=3891, FN=0, Flags=.....R....C
10536	57.306944	AzureWav_0f:0e:9b	HitronTe_f3:9a:46	802.11	164 Association Request, SN=258, FN=0, Flags=.....C, SSID=FlyingNet
10538	57.309946	HitronTe_f3:9a:46	AzureWav_0f:0e:9b	802.11	210 Association Response, SN=3892, FN=0, Flags=.....C

Figura 22 24- Processo de associação completo - redes IEEE 802.11

Observa-se que o processo de associação consiste em duas etapas, autenticação e associação, ambas com uma solicitação e uma resposta:

- Solicitação de Autenticação - Frame 10530
- Resposta de Autenticação - Frame 10532
- Solicitação de Associação - Frame 10536
- Resposta de Associação - Frame 10538

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

Resposta:

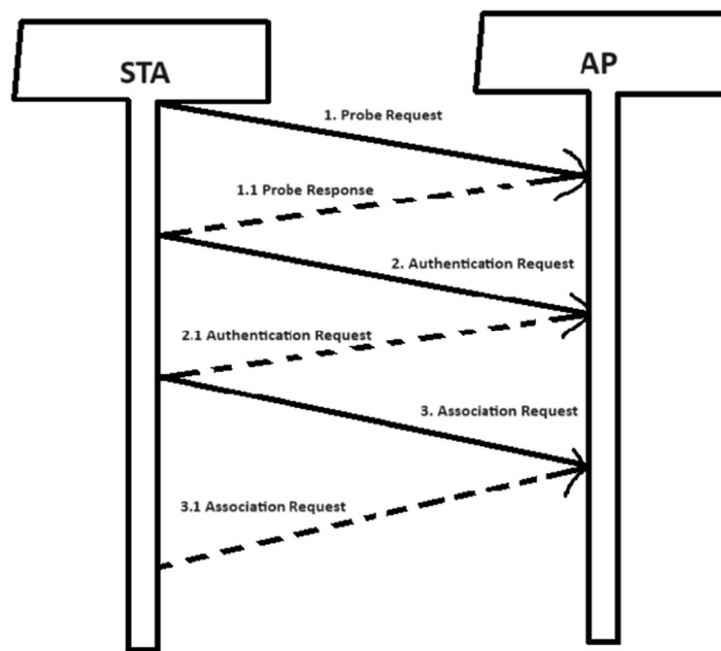


Figura 23 25- Processo de associação completo- diagrama- redes 802.11

Exercício 4 - Transferências 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 direcionalidade das tramas, o que pode concluir face à direcionalidade dessa trama, será local à WLAN?

Resposta:

Analisando a flag referente ao DS status, da figura abaixo, podemos concluir que a direcionalidade desta trama pode ser observada através dos campos "To DS: 0" e "From DS: 1". O primeiro indica que a trama não é direccionada ao DS e o segundo que a trama é proveniente do DS, ou seja, podemos concluir que a trama não é destinada à WLAN (Wireless Local Area Network) e é proveniente da mesma.

wlan && data					
No.	Time	Source	Destination	Protocol	Length Info
251	3.566484	PIInovac 66:db:70	Spanning-tree-(for...	802.11	122 Data, SN=1687, FN=0, Flags=p....F.C
290	4.129407	b8:2d:28:7a:9b:68	76:9b:e8:f3:9a:43	802.11	175 QoS Data, SN=1615, FN=0, Flags=p....TC
305	4.248888	b8:2d:28:7a:9b:68	76:9b:e8:f3:9a:43	802.11	164 QoS Data, SN=1616, FN=0, Flags=p....TC
321	4.539316	PIInovac 9b:f2:a0	Spanning-tree-(for...	802.11	122 Data, SN=1421, FN=0, Flags=p....F.C
347	4.840670	48:22:54:b4:88:e6	Broadcast	802.11	138 Data, SN=1428, FN=0, Flags=pm....F.C
348	4.840674	48:22:54:b4:88:e6	Broadcast	802.11	138 Data, SN=1429, FN=0, Flags=p....F.C
385	5.224785	PIInovac 20:a9:c9	Spanning-tree-(for...	802.11	122 Data, SN=3956, FN=0, Flags=p....F.C
▶ Frame 305: 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits) on interface en0, id 0 ▶ Radiotap Header v0, Length 58 ▶ 802.11 radio information ▶ IEEE 802.11 QoS Data, Flags: .p....TC Type/Subtype: QoS Data (0x0028) ▶ Frame Control Field: 0x0000000000 = Version: 010.. = Type: Data frame (2) 1000.... = Subtype: 8 ▶ Flags: 0x4101 = DS status: Frame from STA to DS via an AP (To DS: 1 From DS: 0) (0x1)0.. = More Fragments: This is the last fragment0... = 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 .000 0000 0011 0000 = Duration: 48 microseconds Receiver address: HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46) Transmitter address: b8:2d:28:7a:9b:68 (b8:2d:28:7a:9b:68) Destination address: 76:9b:e8:f3:9a:43 (76:9b:e8:f3:9a:43) Source address: b8:2d:28:7a:9b:68 (b8:2d:28:7a:9b:68) BSS Id: HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46) STA address: b8:2d:28:7a:9b:68 (b8:2d:28:7a:9b:68)0000 = Fragment number: 0 0110 0101 0000 = Sequence number: 1616 Frame check sequence: 0xa78ccf8b [correct] [FCS Status: Good] ▶ Qos Control: 0x0000 ▶ CCMP parameters ▶ Data (68 bytes)					
0029	6c 09 01 22 1f 18 07 24	00 00 00 00 00 04 00 00 55	1.....\$.....U		
0030	00 10 18 03 04 00 3f 09	00 00 00 00 00 00 00 00 74 9b?.....U		
0040	e8 f3 9a 46 b8 2d 28 7a	9b 08 76 9b e8 f3 9a 43	...F...{z..hv...C		
0050	00 05 00 00 0c e8 00 20	00 00 00 00 04 ae f6 2e	e.....d...		
0060	e6 f7 fb 5e cb e8 55 24	d0 d7 f1 7c 5c a9 fa 55	...A..US.....U		
0070	cf 1e 83 3c 8a 2c 3f 09	a6 69 46 55 bc 6f 83 a6	...<.,?..1FUo...		
0080	29 02 2c 1c 4a e2 17 1b	c1 20 fe 1b a7 e2 15 56),.....V		
0090	93 f8 48 fd 1a 19 fd d8	45 f9 d9 dc 80 a8 e9 4b	.H.....E.....K		
00a0	9b cf 8c a7			

Figura 2426 -Trama de dados nº 305

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)?

Resposta: Com base na trama da figura abaixo concluímos assim que os endereços MAC correspondentes são:

- STA: b8:2d:28:7a:9b:68
- AP: 74:9b:e8:f3:9a:46
- Router: 76:9b:e8:f3:9a:43

Receiver address: HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)
Transmitter address: b8:2d:28:7a:9b:68 (b8:2d:28:7a:9b:68)
Destination address: 76:9b:e8:f3:9a:43 (76:9b:e8:f3:9a:43)
Source address: b8:2d:28:7a:9b:68 (b8:2d:28:7a:9b:68)
BSS Id: HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)
STA address: b8:2d:28:7a:9b:68 (b8:2d:28:7a:9b:68)
.....0000 = Fragment number: 0
0110 0101 0000 = Sequence number: 1616
Frame check sequence: 0xa78ccf8b [correct]

Figura 27- Totalidade da trama

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 RTC/CTS e um outro em que não é usada.

Resposta: De forma a encontrar transferências de dados em que é usada a opção RTC/CTS em primeiro lugar aplicamos o seguinte filtro: wlan.fc.type_subtype == 0x1b || wlan.fc.type_subtype == 0x1c.

wlan.fc.type_subtype == 0x1b wlan.fc.type_subtype == 0x1c					
No.	Time	Source	Destination	Protocol	Length Info
252	0.676572		PTInovac_67:77:60 (- 802.11	68	Clear-to-send, Flags=.....C
261	0.677776	PTInovac_67:77:60 (- 56:5f:07:ef:4f:be (- 802.11	76	Request-to-send, Flags=.....C	
262	0.677778		PTInovac_67:77:60 (- 802.11	68	Clear-to-send, Flags=.....C
274	0.694884	56:5f:07:ef:4f:be (- 802.11	76	Request-to-send, Flags=.....C	
275	0.694897		56:5f:07:ef:4f:be (- 802.11	68	Clear-to-send, Flags=.....C
277	0.694913	56:5f:07:ef:4f:be (- 802.11	76	Request-to-send, Flags=.....C	
278	0.694815		56:5f:07:ef:4f:be (- 802.11	68	Clear-to-send, Flags=.....C
280	0.694823	56:5f:07:ef:4f:be (- 802.11	76	Request-to-send, Flags=.....C	
281	0.694827		56:5f:07:ef:4f:be (- 802.11	68	Clear-to-send, Flags=.....C
283	0.697896	PTInovac_67:77:60 (- 802.11	76	Request-to-send, Flags=.....C	
284	0.697900		PTInovac_67:77:60 (- 802.11	68	Clear-to-send, Flags=.....C
286	0.697910	PTInovac_67:77:60 (- 802.11	76	Request-to-send, Flags=.....C	
287	0.697913		PTInovac_67:77:60 (- 802.11	68	Clear-to-send, Flags=.....C
289	0.697918	PTInovac_67:77:60 (- 802.11	76	Request-to-send, Flags=.....C	
290	0.697922		PTInovac_67:77:60 (- 802.11	68	Clear-to-send, Flags=.....C
293	0.697933	PTInovac_67:77:60 (- 802.11	76	Request-to-send, Flags=.....C	
294	0.697937		PTInovac_67:77:60 (- 802.11	68	Clear-to-send, Flags=.....C
296	0.699064	PTInovac_67:77:60 (- 802.11	76	Request-to-send, Flags=.....C	
297	0.699070		PTInovac_67:77:60 (- 802.11	68	Clear-to-send, Flags=.....C
307	0.758408	PTInovac_67:77:60 (- 802.11	76	Request-to-send, Flags=.....C	
308	0.758413		PTInovac_67:77:60 (- 802.11	68	Clear-to-send, Flags=.....C
310	0.758418	PTInovac_67:77:60 (- 802.11	76	Request-to-send, Flags=.....C	
311	0.758422		PTInovac_67:77:60 (- 802.11	68	Clear-to-send, Flags=.....C
313	0.758430	56:5f:07:ef:4f:be (- 802.11	76	Request-to-send, Flags=.....C	
314	0.758433		56:5f:07:ef:4f:be (- 802.11	68	Clear-to-send, Flags=.....C
316	0.759444	56:5f:07:ef:4f:be (- 802.11	76	Request-to-send, Flags=.....C	
317	0.759448		56:5f:07:ef:4f:be (- 802.11	68	Clear-to-send, Flags=.....C
319	0.761026	56:5f:07:ef:4f:be (- 802.11	76	Request-to-send, Flags=.....C	
320	0.761032		56:5f:07:ef:4f:be (- 802.11	68	Clear-to-send, Flags=.....C

Frame 290: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface en0, id 0
RadioTap Header v0, Length 54
802.11 radio information
IEEE 802.11 Clear-to-send, Flags:C
Type/Subtype: Clear-to-send (0x001c)
Frame Control Field: 0xc400
.....00 = Version: 0
.....01.. = Type: Control frame (1)
1100 = Subtype: 12
Flags: 0x00
.....00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x0)
.....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

Figura 28 - Filtro wlan.fc.type_subtype == 0x1b || wlan.fc.type_subtype == 0x1c

Conclusão

Este trabalho permitiu-nos explorar os conceitos fundamentais do nível de ligação lógica, focando em redes Ethernet, protocolo ARP e redes Wi-Fi.

Na primeira parte, analisámos o funcionamento das redes Ethernet e a estrutura das tramas através do Wireshark, identificando campos como endereços MAC e o campo Type. Investigámos o protocolo ARP, observando a diferença entre ARP Request (broadcast) e ARP Reply (unicast), essenciais para a resolução de endereços na rede.

Na segunda parte, estudámos as redes Wi-Fi, analisando o acesso rádio (frequências, canais e normas IEEE 802.11), os mecanismos de scanning passivo (tramas beacon) e ativo (probe requests/responses) para descoberta de redes, e o processo de associação entre estações e pontos de acesso. Por fim, examinámos a transferência de dados em redes sem fios e mecanismos como RTS/CTS que mitigam problemas de estações escondidas.

A ferramenta Wireshark foi fundamental para visualizar na prática os conceitos estudados, contribuindo significativamente para a nossa compreensão do funcionamento das redes de comunicação e dos desafios inerentes ao nível de ligação lógica.