GUIÃO 5

Ex 2

By analyzing the captured packets, there is a big amount of them, so we'll have to use filters for the packets.

Assossiation

The filters used to see the association packets are:

- `wlan.fc.type_subtype==0 || wlan.fc.type_subtype==1` → used to watch assosciation request and responses, respectively.
- `wlan.addr == mac_pc` → used to filter the MAC address of PC2, coupled with an AND (&&).

After each connection, there is an exchange of Authentication packets between PC2 and the Router.

Authentication

The filters used to see the association packets are:

- `wlan.fc.type_subtype==11 || wlan.fc.type_subtype==12` → used to watch authentication and deauthentication, respectively.
- `wlan.addr == mac_pc` → used to filter the MAC address of PC2, coupled with an AND (&&).

Since we're connecting to a network with no password, the Authentication process uses an Open System algorithm.

On the other hand, on the Deauthentication process, it disconnects with a reason behind it.

Probe

These packets are constantly transmitted so that the router may know how many clients are currently connected, and where they are connected.

Ex 3

As mentioned before, association packets are exchanged on a new connection, and responsible for informing the router about the information of the connecting device.

After pinging the Router and applying the filter `icmp`, on PC1 while keeping the MAC address filter, we can see that they exchange ARP packets. During pinging process, after each request, we get Request to Send (RTS) and Clear to Send (CTS) packets.

Ex 4

Since now we are sending larger packets, the connection elapsed time will be higher and it's also more unstable.

Since the limit of the RTS and CTS packets is 1000 bytes and we are trying to send packets larger than that, it ends up resulting on that unstability.

Those packets are used to limit the bandwidth used by each user, otherwise it could overwhelm the router and cause connection issues for other users.

Ex 5

During the authentication process, since now we are using a private network, instead of having just the association packets, we will also have authentication packets with keys to validate the connection.

We also won't be able to capture ICMP packets from this connection.