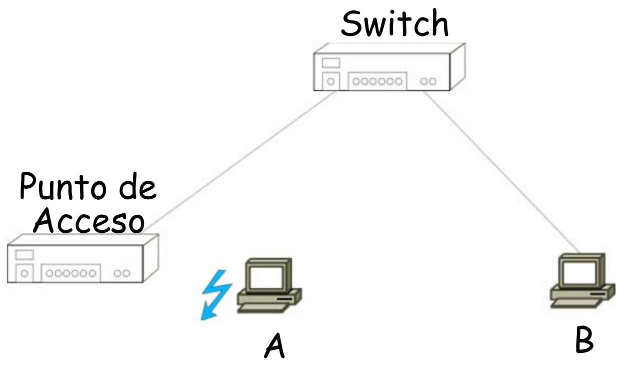
Lab 8: WIFI Traffic Analysis

1. Traffic Analysis. Scenario 1

Given the following topology:



We have captured the traffic generated when computer A runs “**ping -c 1 dir_IP_B**”. You can see the captured traffic in computer A and computer B in the files **wifi2cable_1** and **wifi2cable_2**.

Exercise 1. Open the file **wifi2cable_1** with wireshark and answer the following questions.

1. Where have the frames been captured? The wired or wireless segment of the network?
2. What is the IP address of computer A? What is the IP address of computer B?
3. Why are the first two frames of the capture generated?
4. Which are the physical addresses that appear in the captured frames? Whose physical addresses are these?
5. What is the length of the datagrams sent? Were the datagrams fragmented? What is the length of data in the ICMP message?

Exercise 2.

In exercise 1, you analysed some frames of the traffic generated by the command "**ping –c 1 dir_IP_B,**"; in this exercise, we will analyse the rest of the frames. Open the file **wifi2cable_2** (in this capture you can only see the frames related to the command ping. In **wifi2cable_2_completa** you can see the full capture).

1. Where have the frames been captured? The wired or wireless segment of the network?
2. Write the different types of frames you can see in the capture.
3. Can you see ARP or ICMP messages as you did in **wifi2cable_1?** Why do you think you cannot see them?
4. Try to locate the frames generated by the command ping.

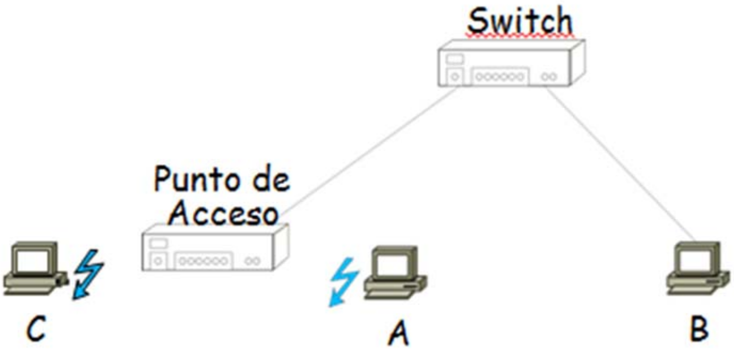
You cannot see the data of the captured frames because they are encrypted according to WPA-PSK protocol. To see the ARP and ICMP messages encapsulated in the frames you have to go to "**Edit**"-->"**Preferences**" and there, select the protocol "**IEEE802.11**,". In the options that you can modify, go to "**Ignore the protection bit**" and select "**Yes – with IV**". Afterwards, you will be able to see the data in the captured frames.

Exercise 3.

1. How many ARP frames are there? Is it the same number as in **wifi2cable_1**? Why?
2. What is the physical address of the Access Point? Is it the wired or wireless physical address? Was this physical address in **wifi2cable_1**? Why?
3. Focus on the first two ARP frames of the capture (frames 1 and 2 of the capture). They look quite similar; do you see any difference between them?
4. Analyse bits "From DS" and "To DS" in both frames. Write the meaning of the value of these bits.
5. Look for ARP reply in the capture. Are the physical addresses the same as in the previous capture? Why?
6. Now, focus on the echo request and echo reply of the command ping. What are the physical addresses in these frames?
7. What are the IP addresses in the capture? Are the IP addresses the same as in **wifi2cable_1**? What is the IP address of the Access Point?
8. Focus on the sequence number of the frames generated by the command ping (compare the ARP reply and the ping reply). Are the sequence numbers consecutive?
9. Are ICMP messages fragmented? and ARP messages?

2. Traffic Analysis. Scenario 2

Given the following topology:



Now, we have another wireless station, computer C. C is associated with the same Access Point as A, but A and C cannot sense each other.

We have captured the traffic generated when computer A runs "**ping -c 1 dir_IP_C**". You can see the captured traffic in computer A and computer B in the files **wifi2wifi_1** and **wifi2wifi_2** (this time the capture files are as they were captured, without deleting irrelevant frames from the output traffic analysis point of view).

Exercise 4. Open the file **wifi2wifi_1** with the wireshark, and answer the following questions:

1. What is(are) the type of frame(s) that you can see in this file?
2. Look for physical and IP addresses. Whose addresses are these? Are they the same addresses as in Scenario 1?
3. With the information in wifi2wifi_1, can you find out the physical and/or IP addresses of Scenario 2 computers?

Exercise 5. Open the file **wifi2wifi_2** with the wireshark and answer the following questions:

1. Is the physical address of the computer A in many frames? What is the meaning of these frames?

2. Focus on the first frame with A as the source MAC address. What is the meaning of these frames? What MAC addresses are involved? Whose MAC addresses are these? What IP addresses are involved? Whose IP addresses are these? This frame seems repeated in the capture, why?

4. Locate the frame generated as a response to the previous frame. Who transmits the frame? Who is the original creator of the frame? Is there a frame transmitted by the original creator? Why?

5. Based on the previous frame, what is A looking for in its first frame sent?

6. Check the bits "ToDS" and "FromDS" in the previous frames, are they the

expected values?

7. Look for “echo request” and “echo reply” frames generated when A runs “**ping -c 1 dir_IP_C**”. What is the transmitter MAC address of each frame? What is the MAC address of the original creator of the frame? What is the destination address of each frame? Who should keep a copy of the frames? Will they be retransmitted?

8. Taking into account that both A and C are associated with the same Access Point and they cannot sense each other, are you missing any frames related to the command ping?