Lab Practice 8: Wi-Fi Traffic analysis

1. Preliminary Work

Required reading: Kurose, 7th edition, subsections 7.3.1 to 7.3.3 (pages 440–451)

Tasks to complete before the lab session: Read the *Introduction* section, study the *802.11 Frame Format* section, and solve the exercise provided in *Annex I.*
Video: [To be viewed before the lab session]: https://media.upv.es/#/portal/video/c702b81a-35f9-469f-89e1-d1852b93ac83

2. Introduction

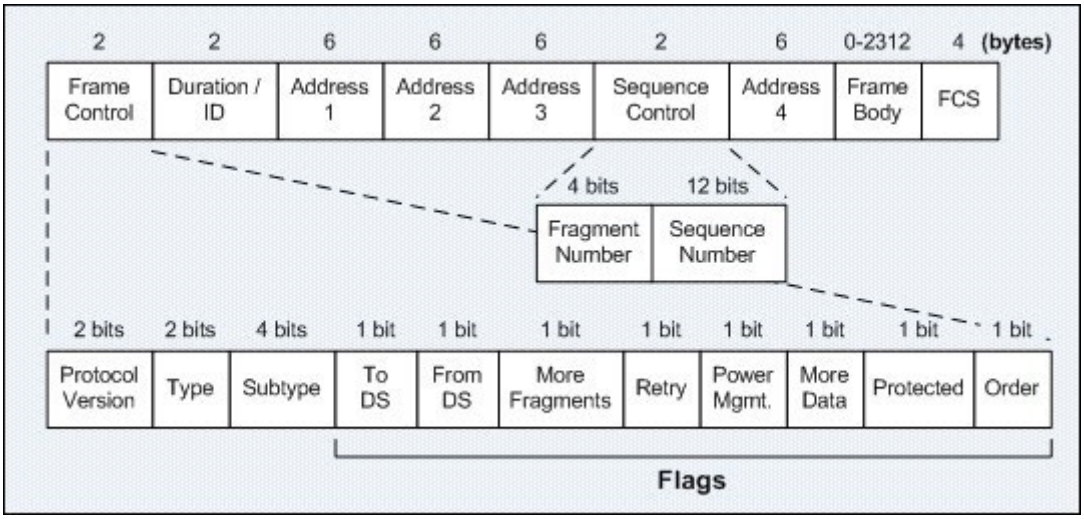
Wireless data networks have practically become essential in our daily lives. After their widespread adoption in laptops, we now use them on all types of mobile devices (phones, tablets, etc.). The reason for their popularity is clear: they offer a flexibility that wired networks do not. Additionally, the lack of physical connectors allows for the manufacturing of more compact and portable devices.

However, because the signal carrying the data in the transmission medium is not physically protected—as it is in wired networks—the performance of wireless networks is generally inferior to that of wired ones. Nevertheless, the greater flexibility they provide usually outweighs this performance loss in most cases.

In this lab session, we will carry out an initial study of wireless data networks that follow the IEEE 802.11 standard. Note that these networks are much more complex than wired networks such as Ethernet. For this reason, in this practice we will perform a basic analysis without diving deeply into the detailed functioning of IEEE 802.11 networks. We will also include in this study some aspects related to the wired network that connects to the access point of a given wireless network.

3. IEEE 802.11 Frame Format

The general format of IEEE 802.11 frames is shown in the following figure, which also illustrates the structure of two header fields: the *Control* field and the *Sequence* field.



As a brief introduction, the meaning of each field in the 802.11 frame is as follows:

- **Frame Control:** This field includes several subfields and flags necessary for the correct operation of the protocol. The meaning of these subfields and flags will be described further below.
- **Duration/ID:** This field has various meanings depending on the values of bits 15 and 14 (the MSB bits). In summary, this field can either indicate the number of microseconds the transmission medium will be occupied by the current frame transmission, or convey information related to power-saving mechanisms in wireless devices (specifically, to trigger the transmission of stored frames from the access point while the device was in power-saving mode).
- **Addresses 1, 2, 3, and 4:** These 48-bit fields contain the MAC addresses involved in the current frame. As a general rule, and specifically for data frames:
    - The **Address 1** field contains the MAC address of the device that is to receive the transmitted frame.
    - The **Address 2** field contains the MAC address of the device that transmitted the wireless signal.

  Note that the MAC address in **Address 1** may not be the final destination of the frame (for example, the final destination might be a wired device beyond the access point). Likewise, the MAC address in **Address 2** may not be the original source of the data carried in the 802.11 frame (e.g., the source could be a wired device). For this reason, a third field, **Address 3**, is required to indicate this information. The **Address 3** field contains either the actual source or the final destination of the data (whether on the wired or wireless side). To correctly interpret the information in the **Address 3** field, we must consult the "To DS" and "From DS" flags found in the **Frame Control** field.

  Finally, the **Address 4** field is used for communication between access points and therefore falls outside the scope of this initial study on IEEE 802.11 networks.

- **Sequence Control:** This field is used to reassemble higher-layer messages that were transmitted in fragments, and to detect duplicate frame reception. It has two subfields:
    - **Fragment Number:** When a higher-layer message is fragmented, this subfield indicates the fragment number (the first fragment is numbered 0, and subsequent fragments use consecutive numbers).
    - **Sequence Number:** This subfield acts as an identifier so that two different frames have different sequence numbers. If a frame must be retransmitted (for instance, because an ACK was not received), the retransmitted frame retains the same sequence number. This allows the receiver to determine whether the data is new or was already received. Note that all fragments of a given frame share the same sequence number.
- **Frame Body:** This field contains the data sent in the frame. Its maximum length is 2304 bytes (2312 including WEP data).
- **FCS (Frame Check Sequence):** This is a CRC code used to verify whether the frame was received without transmission errors.

Regarding the **"Frame Control"** field, the different subfields and flags it contains are as follows:

- **Protocol Version:** Indicates the exact version of the 802.11 protocol used in the rest of the frame. Currently, there is only one version of 802.11, assigned the value 0. Future versions may use different values.
- **Type and Subtype:** Indicate the type of the current frame, as well as its subtype. The main frame types are:
    - **Management (type = 00)**
    - **Control (type = 01)**
    - **Data (type = 10)**

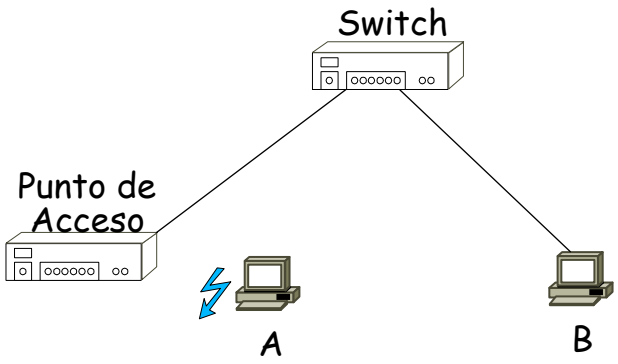
  Each frame type includes various subtypes. For example, within the **"Management"** type, we find (among others):
    - **Association Request (0000)**
    - **Association Response (0001)**
    - **Probe Request (0100)**
    - **Probe Response (0101)**
    - **Beacon (1000)**

  Within the **"Control"** type, common subtypes include:
    - **RTS (1011)**
    - **CTS (1100)**
    - **Acknowledgment (1101)**
- **ToDS and FromDS:** These flags are primarily used to indicate whether the current frame comes from the access point (**DS** stands for **Distribution System**, referring to the wired network), or whether it is going to the access point:
    - **ToDS = 1 and FromDS = 0:** The frame originates in the wireless segment and is intended for the access point.
    - **ToDS = 0 and FromDS = 1:** The frame is transmitted from the access point and is intended for a wireless station.
    - The other two combinations of these flags are also used and have their own meanings, but they will not be discussed in this lab.
- **More Fragments:** This flag works similarly to the "More Fragments" bit in the IP datagram header. When a message from an upper layer has been fragmented into multiple frames, all fragments (except the last one) carry this flag set to one.
- **Retry:** This bit is set to one when a previously transmitted frame is being retransmitted. It helps the receiver identify and discard duplicate frames.
- **Power Management:** When a station transmits a frame and sets this bit to one, it indicates that it will enter power-saving mode after the current transmission (and thus will not be able to receive frames, which must be temporarily stored by the access point).

- **More Data:** Since the access point must store frames destined for devices that are in power-saving mode, this bit is used by the access point to indicate whether it has pending frames to send.
- **Protected (WEP):** This bit is set to one when a frame is encrypted.
- **Order:** If frames need to be transmitted in the order they were generated (or received at the access point), this bit is set to one. Note that enforcing in-order delivery requires additional resources from both the sender and receiver.

4. Traffic Analysis. Scenario 1

To begin our study of traffic generated by wireless stations, we will use the scenario shown in the figure:



In this scenario, we have two computers. Computer A is associated with the access point, while computer B has a wired network connection.

Instead of performing packet captures ourselves using Wireshark, we will use pre-recorded captures available in the files **wifi2cable_1**, **wifi2cable_2**, and **wifi2cable_2_completa**. These files can be found on PoliformaT.

The reason for using pre-recorded captures is that capturing wireless traffic is not straightforward. To capture such traffic (and view the IEEE 802.11 fields), the wireless network card must support **monitor mode**. Additionally, the network lab has a high volume of wireless traffic, which would greatly complicate the analysis. Therefore, the captures we will study were taken in a low-traffic environment.

The traffic to be analysed was generated by running the command **ping -c 1 IP_addr_B** from computer A. Packet captures were made simultaneously on both computer A and computer B using Wireshark (hence the two capture files).

Exercise 1. Open the file **wifi2cable_2_completa** in Wireshark and answer the following questions:

1. Look at the beacon frames, specifically the information shown in "**802.11 radio information**":
    a. At what speed are the beacons being transmitted? 1.0Mb/s
    b. On which channel/frequency? 2437MHz
2. Now analyse the section **"IEEE 802.11 Wireless Management"** and indicate:
    a. How often are the beacon frames sent? 0.307200 seconds

   b. What is the SSID of the network? JAZZTEL_C9F6 54Mbit/s
   c. What is the maximum transmission rate supported by the access point? (in tagged parameters,supported rates)
   d. Which Wi-Fi standard (annex) is implemented by the AP? 802.11n
   e. What kind of security is supported? What encryption type? What authentication method? (look for ***Unicast Cipher Suite*** and ***Auth Key Management*** elements)
3. Looking at the full trace, indicate: Security: WPA | Encryption: AES (CCM) | Auth: PSK (I think)
   a. What types of **management frames** appear? Beacon, probe response
   b. What types of **control frames** appear? RTS (request to send), Acknowledgement
   c. What types of **data frames** appear? QoS Data, Data
   d. Look at the **802.11 radio information** field in the data frames. Are all frames transmitted at the same speed? Why? No

Note: You can use the filters wlan.fc.type == 0, wlan.fc.type == 1, and wlan.fc.type == 2 to speed up the search for different frame types.

Exercise 2. Open the file **wifi2cable_1** in Wireshark. Remember that the traffic to be analysed was generated by running the command **ping -c 1 IP_addr_B** on computer A. Answer the following questions:

1. According to the frame format shown by Wireshark, were the frames captured on the wired network segment or the wireless segment? Wired, as they all have Ethernet information
2. What is the IP address of computer A? What is the IP address of computer B? 192.168.1.130 192.168.1.128
3. Why are the first two frames in the capture generated? Because A needs to know the MAC address of B to set it as the destination.
4. What physical addresses appear in the frames? To whom do those physical addresses belong? ff:ff:ff:ff:ff:ff to broadcast the ARP request, 00:16:ea:28:5a:88 (corresponds to A), 00:24:1d:c2:42:25 (corresponds to B)

Exercise 3. After analysing part of the traffic generated by the command **ping -c 1 IP_addr_B** in the previous exercise, in this exercise we will analyse the remaining traffic generated. To do so, open the capture **wifi2cable_2** (this capture has been filtered to include only the frames that are a direct result of the ping command to make traffic analysis easier. The full capture is available in the file **wifi2cable_2_completa**).

1. Based on the information in this capture, were the frames captured on the wired network segment or the wireless segment? Wireless segment (protocol is 802.11)
2. Can you see the contents of the ARP and ICMP messages that were visible in the previous capture? What do you think is the reason why you cannot see the contents of these messages? No, we can't. Wifi packets are encrypted.
3. Try to locate in this capture the frames generated by executing the ping command that complement the traffic analysed in the previous exercise. They are frames number 4 and 5

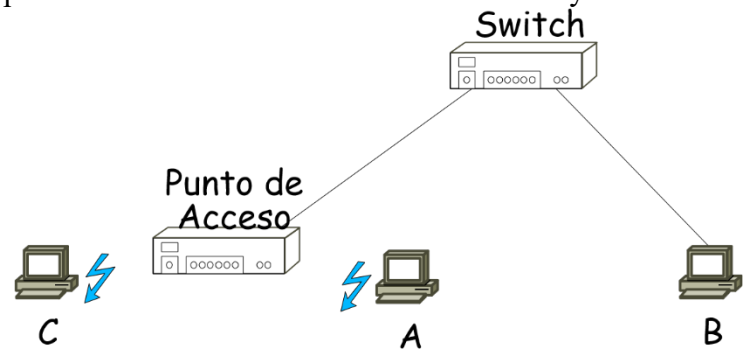
The reason why the data contained in the captured frames is not visible in Exercise 3 is that this data is encrypted using the WPA-PSK protocol. To view the ARP and ICMP messages within the captured frames, you would need the key associated with the access point. This key is similar to those commonly entered when connecting to a Wi-Fi network from Windows or Linux. In our case, since the computer used to capture the traffic already had the key, you just need to go to the menu: **Edit → Preferences**, and in the window that appears, search for the protocol **"IEEE 802.11"**. In the modifiable options, locate the one that says **"Ignore the protection bit"** and select **"Yes – with IV"**. From that point on, you will be able to view the content of the captured frames.

Exercise 4. After modifying the encryption options as described above, answer the following questions

1. Locate the ARP protocol frames. How many are there? Is the number of ARP frames the same as in the previous capture? Why or why not? Now there are 3 ARP frames, as both A and the AP have to broadcast the packet asking for B's physical address (and B has to respond).
2. What is the physical address of the access point? Is it the physical address on the wired side or the wireless side? 38:72:c0:a2:c9:f6, it is the one in the wireless side
3. Focus on the first two ARP frames (frames 1 and 2 in the capture). Analyse the **From DS** and **To DS** bits of both frames. What conclusions can you draw? Are these conclusions consistent with the differences you observed in the previous question?
   First (A to router): To DS: 1, From DS: 0 | Second (router to A): To DS: 0, From DS: 1
4. Now focus on the ping request and reply. What MAC addresses are involved in both frames? [Request]: Receiver: 38:72:c0:a2:c9:f6 (router) Transmitter: 00:16:ea:28:5a:88 (A) Destination: 00:24:1d:c2:42:25 (B)
   [Reply]: Receiver: 00:16:ea:28:5a:88 (A) Transmitter: 38:72:c0:a2:c9:f6 (router) Destination: 00:16:ea:28:5a:88 (A)
5. Look at the sequence numbers of the different frames generated as a result of the ping command (compare the ARP reply and the ping reply). Are they sequential?
   Yes. The sequence number for the ARP reply is 65, and the one for the ping reply is 66.

5. Traffic Analysis. Scenario 2

We will continue our study of wireless networks by introducing an additional computer into the capture scenario. Now we have the setup shown in the following figure, where wireless station C has been added and is associated with the same access point as computer A from the previous scenario. Computers A and C cannot see each other directly.



As in the previous analysis, we will analyse the traffic generated by the command **ping -c 1 IP_addr_C**, which is once again executed on computer A. To capture this traffic, Wireshark was run on both computer B and computer A (again, we have two capture files: **wifi2wifi_1** and **wifi2wifi_2** (this time the captures have not been cleaned)).

Exercise 5. Open the capture file wifi2wifi_1 in Wireshark and answer the following questions:

1. What does this capture file contain? Is it correct that the frame(s) shown on screen are present? Is any frame missing? Only 1 ARP request is received, so this must have been captured in computer B. Only 1 is sent through Ethernet and arrives to B.
2. Check the MAC addresses and IP addresses that appear in the file. To whom do these addresses belong? Are they the same as in the previous scenario?
   The MAC address of A is the source, and A is asking for the MAC address of C, which must be 192.168.1.131.
   The IP address of A (192.168.1.131) also appears in the broadcast.

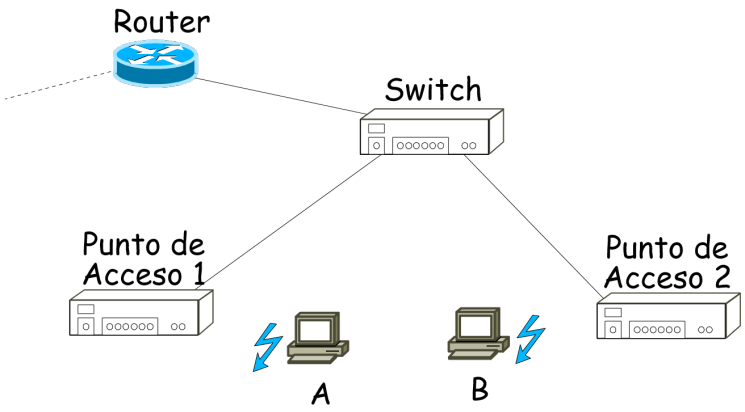
Exercise 6. Open the capture file **wifi2wifi_2** in Wireshark and answer the following questions:

1. In how many frames does the MAC address of computer A appear? What role do these frames play? It appears in an ARP broadcast and a reply (used to get C's MAC address), in a Request-to-send and in an Acknowledgement (used to request the channel), and in the ping request and reply.
2. Regarding the first frame in which computer A's MAC address appears as the source of the frame, what is the purpose of this frame? What information is being requested with it? What MAC addresses are involved in that first frame? To whom do those MAC addresses belong? It's an ARP request sent by A, to request the MAC address of C. The receiver address is the MAC address of the router, and the transmitter address is that of A.
3. The previous frame seems to be repeated in the capture. Analyse why this duplication occurs. The first frame is sent from A to the router, but the router then has to broadcast it. The second frame corresponds with this broadcast done by the router.
4. Locate the frame that was generated as a response to the previous one. Who transmitted this frame? Who originally created it? Does the original frame sent by the initial creator appear in the capture? Why or why not? The frame is transmitted from the router to A, and was originally created by C, with MAC address 00:18:de:a1:6d:ce.
5. Go back to the analysed frames and check their "ToDS" and "FromDS" bits. Are their values what you would expect for each frame?
6. Find the frames that contain the echo request and echo reply sent as a result of the command ping -c 1 IP_addr_C. What is the MAC address of the transmitter for each of those frames? And the MAC address of the original sender of the message contained in the frames? What destination addresses are used? The request is transmitted from A to the router, and is destined to C. The reply is originally sent by C, and is transmitted by the router and destined to A.
   Note that the MAC address of the access point, as well as the source and destination address of the frames, appear in different positions in the frame header depending on whether they are used as address 1, 2, or 3 (refer to Section 3 of the lab guide to review the 802.11 frame format).
7. Analyse the sequence number field of the following frames: beacon, ARP, and ping. Do you observe any relationship between the sequence numbers used by the access point?
8. Considering that stations A and C cannot see each other directly, but both can see the access point, is there any frame related to the ping command missing from the capture?
   No

Beacon frames have sequential sequence numbers. The ARP reply and echo reply (both transmitted by the router as well) also have sequential sequence numbers, but they seem unrelated to those of beacon frames.

Annex I

Exercise. Given the set of networks in the figure:



All networks comply with the IEEE 802.3 or IEEE 802.11 standards. The switch has learned the location of all machines after a period of operation. The router is correctly configured. Station A is associated with access point 1, while station B is associated with access point 2. The ARP caches of all systems are empty, except for that of the router, which contains all the necessary physical addresses

Indicate, by completing a table like the one below (use as many rows as needed), the sequence of frames that will be generated when sending an ICMP type 8 message from computer A to computer B (only the sending part; there's no need to describe the frames that would be generated for the reply). For physical addresses, use symbolic values such as A, B, AP1, AP2, etc. For IP addresses, use symbolic values such as IP A, IP B, IP R, etc.

Frame Type IEEE	Destination Address (if 802.3) / Address 1 (if 802.11)	Source Address (if 802.3) / Address 2 (if 802.11)	Address 3 (if 802.11)	Related IP Source Address (if any)	Related IP Destination Address (if any)	Role of the Frame	Machines (nodes) whose network interface receives a copy of the frame