TÉCNICO LISBOA

Computer Networks — 2021/22		Assignment:	Lab 10
Understanding Wi-Fi		Issued:	2022-02-02
Wi-Fi (IEEE 802.11)		Submission Due:	2022-02-04
Authors:	João M. Tiago Prof. Luis D. Pedrosa	Comments Due:	-
		Version:	1.0

Submission note. Create a single PDF file containing your answers, and attach the file to the submission form in Moodle. Remember to include all relevant screenshots, diagrams, or pictures that you may consider relevant in the PDF file itself.

1 Goals of the laboratory

- Explore the structure of Wi-Fi frames.
- Learn the basics about Wi-Fi (dis)association and data transfer.

2 The large family of IEEE 802 standards

IEEE 802 is a family (or collection) of networking standards mainly applied to local area networks (or LANs, as you may remember from the previous laboratory). These standards cover technologies in the physical and data-link layers, such as Ethernet and wireless network protocols. This large family of standards is divided into smaller working groups (or areas of focus), each of which responsible for developing, implementing, and maintaining different standards.

In particular, the IEEE 802.11 working group is responsible for Wi-Fi, which is a collection of standards that implement wireless LAN (or WLAN) communication, so that different, heterogeneous devices (such as laptops, printers, smartphones, or tablets) can communicate with each other, as well as access the Internet wirelessly.

3 Wi-Fi (or IEEE 802.11)

There are several IEEE 802.11 standards (such as 802.11a or 802.11b), which differ at the physical layer, regarding the frequency range they use to transfer data, or the rate at which that data is exchanged, for instance. Despite that, they share some common characteristics, like the link-layer frame structure, as you will see later.

3.1 Wireless LAN architecture

A typical wireless LAN architecture, as depicted in Figure 1, is built of one (or more) **basic service sets** (or BSS), where a BSS contains one (or more) **wireless stations** (devices that support wireless connection to a network), and a central base station (the so-called **access point**, or AP).

Computer Networks — 2021/22		Assignment:	Lab 10
Understanding Wi-Fi		Issued:	2022-02-02
Wi-Fi (IEEE 802.11)		Submission Due:	2022-02-04
Authors:	João M. Tiago Prof. Luis D. Pedrosa	Comments Due:	-
		Version:	1.0

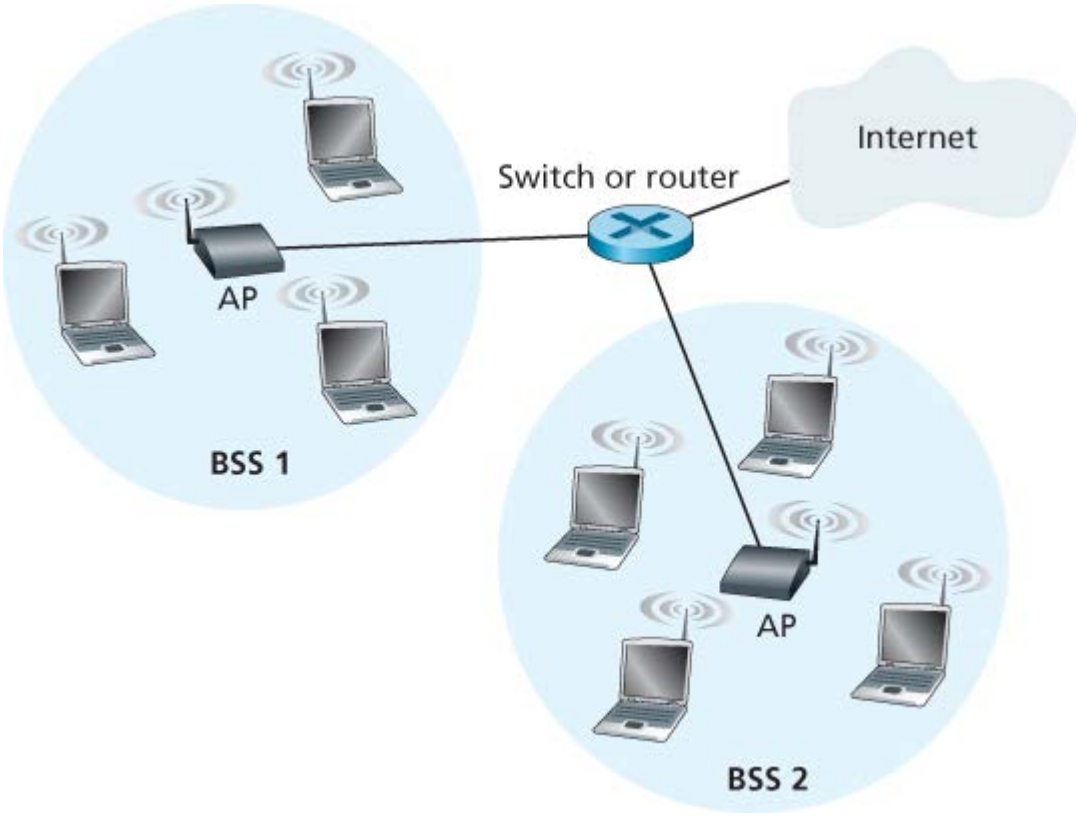

Figure 1: Wireless LAN architecture

3.2 The IEEE 802.11 frame

A IEEE 802.11 frame shares some similarities with an Ethernet frame, but also contains a number of fields that are specific for wireless links. Figure 2 provides a hollistic view of the structure of IEEE 802.11 frames.

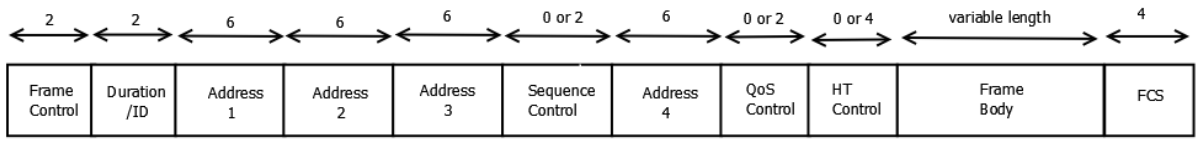

Figure 2: 802.11 frame

The frame is constructed of (1) common fields (which are present in all types of frames), and (2) specific fields (which may be present or absent in the frame, depending on some specific common fields).

3.2.1 The frame control field

The first two bytes of the frame constitute the frame control field, which gives a hint on the purpose and content of the frame. Figure 3 shows the structure of this field.

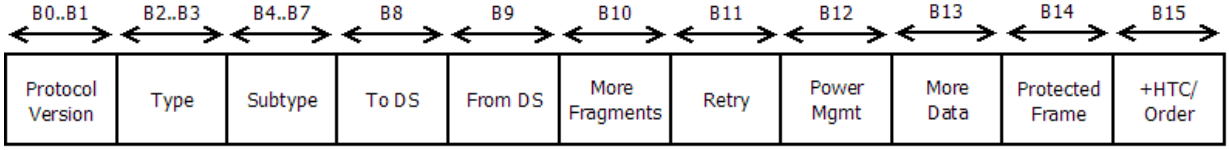

Figure 3: 802.11 Frame Control field

Out of all fields in the frame control field, one can single out two important fields that play a particularly pivotal role: `type` and `subtype`. Field `type` sets the type of 802.11 frame (either management, control, data, or extension), and field `subtype` sets the subtype for a given type of frame (for instance, a management frame can be a beacon). You can learn more about the different types of IEEE 802.11 frames here (in particular, there is a table at the middle of the webpage that can be very useful to answer some questions below).

3.2.2 Multiple address fields

A IEEE 802.11 frame has four 48-bit MAC address fields (a striking difference when compared to an Ethernet frame, which considers two address fields only, a source and destination).

> **Note.** We will focus our attention on the first three MAC addresses in the frame. The fourth MAC address is required by wireless networks in ad hoc mode, which is out of the scope of this laboratory.

To understand why two MAC addresses are not enough, recall Figure 1 and think of the following hypothetical scenario. Suppose you are on your smartphone, which is connected to a wireless network via some access point, and try to access `tecnico.ulisboa.pt` from your browser. HTTP(S) packets will be exchanged between your smartphone and Técnico's web server, but what path will they traverse? First, HTTP packets will need to be moved from your smartphone to the access point it is connected to. Then, they need to be moved along the way to the proper router's interface, which will, at last, forward packets to the web server based on forwarding rules.

Notice how **three distinct network interfaces** (and, thus, three distinct MAC addresses) are involved in the process: the smartphone's, the access point's, and the router's. This explains why three MAC addresses are present the IEEE 802.11 frame:

- Address 2 is the MAC address of the source wireless station (the smartphone);
- Address 1 is MAC address of the access point that will receive the frame;
- Address 3 is the MAC address of the router interface.

3.2.3 Frame body (or payload)

Typically, the payload of a IEEE 802.11 frame is an IP datagram (carrying, for instance, the HTTP request in the scenario above). The payload is typically smaller than 1500 bytes, and is followed by a 32-bit cyclic redundancy check (CRC) code, so that the receiver can detect bit errors in the received frame.

4 Exercises

4.1 Access point association

Before sending or receiving network-layer data over the wireless network (for example, an HTTP request to Técnico's web server), each wireless station needs to connect to a single access point in its range through **access point association**.

Wireless stations may become aware of new access points in the vicinity through **passive scanning** or **active scanning** (explained below). Regardless of the approach, the wireless station will always choose an access point to connect to (perhaps the one with the highest signal strength) by sending it an **association request frame**, to which the access point responds with an **association response frame**, concluding the process of association.

4.1.1 Passive scanning

In passive scanning, access points advertise themselves by periodically broadcasting **beacon frames**, which contain their identification (the SSID – Service Set Identifier, also

known as the network name, and the MAC address). Figure 4 illustrates the approach.

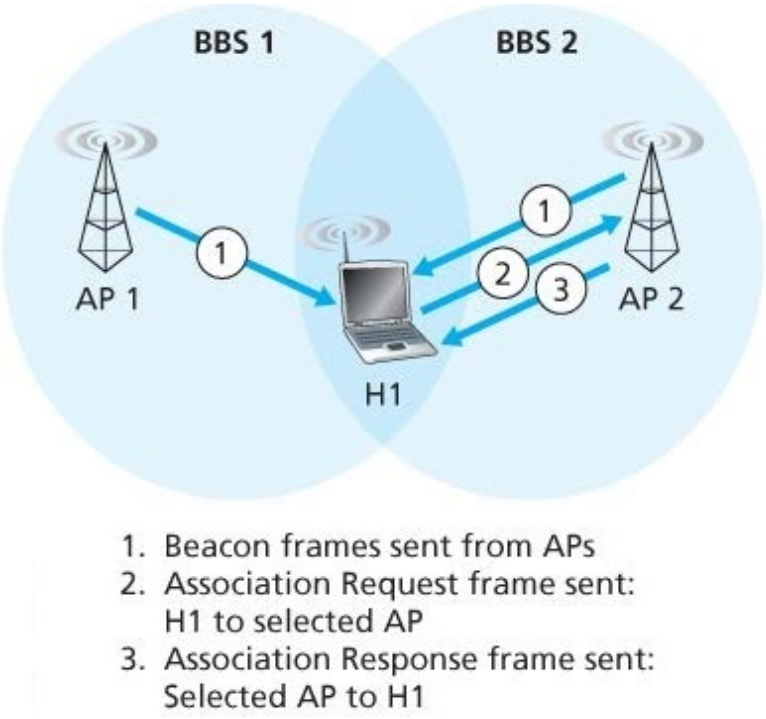

Figure 4: Passive scanning

4.1.2 Active scanning

In active scanning, wireless stations broadcast a **probe request frame** that is received by all access points within their range. Available access points will respond with a **probe response frame**. Figure 5 illustrates the approach.

4.1.3 Questions

To answer questions below, load trace file `wifi_0.pcap` into Wireshark. You will be mainly looking for evidence of passive and active scanning performed by a wireless station (an Apple device) that is already connected to an access point.

Note. The payload of the IEEE 802.11 frames in the trace file is encrypted.

Question 1. Provide a valid Wireshark filter that can be used to display beacon frames only. Explain its meaning.

Hint. Consider using the frame control `type` and `subtype`.

Question 2. A beacon frame has been captured at around `t = 20.070568 s`. What is the SSID and the MAC address of the access point being advertised? When is the next

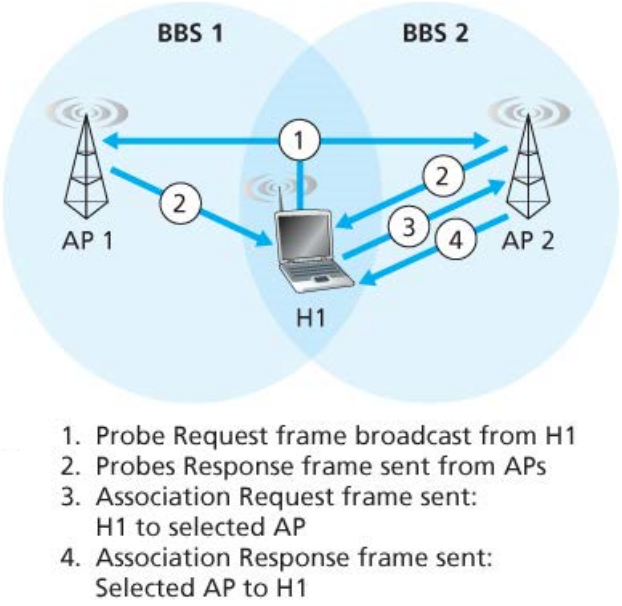

Figure 5: Active scanning

beacon frame, transmitted by the same access point, expected to be captured? Explain how you found that out.

Question 3. Provide a valid Wireshark filter that can be used to display probe response frames only. Explain its meaning.

Question 4. A probe request frame has been captured at around `t = 27.243760 s`. What is the MAC address of the Apple device broadcasting the probe request frame? What is the SSID and the MAC address of the access point the frame is going to be delivered to? Did the Apple device get a probe response frame back from that access point? Explain how you found that out.

4.2 Data transfer

Upon successful association, the wireless station can start sending and receiving network-layer data over the wireless network (bear in mind that the access point will always be an intermediate between the station and the appropriate router interface).

4.2.1 Questions

To answer questions below, load trace file `wifi_1.pcap` into Wireshark. You will be mainly looking for data exchanged between a wireless station (an Apple device) and the access point it is already connected to.

> **Note.** The payload of the IEEE 802.11 frames in the trace file is also encrypted, but Wireshark can successfully decrypt it once you specify the password being used by the access point. To do that, open the Wireshark configuration window for the IEEE 802.11 protocol (go to `Edit > Preferences > Protocols > IEEE 802.11`). Start by ensuring that `Enable encryption` is ticked, and proceed to edit the encryption keys used by Wireshark. Add a new key of type `wpa-pwd` with value `Induction` (you are telling Wireshark to try to use that password to decrypt traffic).

Question 5. Can you find any evidence of active scanning being performed by the Apple device? And does it get any response back from any access point at all? If so, indicate its/their SSID and MAC address. Explain how you found that out, and attach a screenshot of Wireshark to support your explanation.

Question 6. Provide a valid Wireshark filter that can be used to display data frames that carry HTTP requests only. Explain its meaning.

Question 7. At around `t = 14.390505 s`, the Apple device performs an HTTP GET request to a web server running at `66.230.200.228`. Which domain did the Apple device access, and which resource (URI) did it request? What is the MAC address of the access point the frame was forwarded to? Explain how you found that out.

Question 8. The HTTP response to the request from Question 7. was received at around `t = 14.496485 s`. The source address of the encapsulating IEEE 802.11 frame is `00:0c:41:82:b2:53`. Does this MAC address correspond to the IPv4 address of the device that sent the HTTP response (i.e. the appropriate interface of the web server)? Explain how you found that out.

4.3 Access point disassociation

To disassociate from a given access point, the wireless station must send a **disassociation frame** to the access point it is currently attached to. There is no response frame to the disassociation frame, meaning that the association is immediately broken.

4.3.1 Questions

To answer questions below, keep trace file `wifi_1.pcap` loaded into Wireshark.

Question 9. Provide a valid Wireshark filter that can be used to display disassociation frames only. Explain its meaning.

Question 10. By the end of the trace file, a disassociation event takes place. Around what time does it happen, and which party initiated the process? Explain how you found that out.

Computer Networks — 2021/22		Assignment:	Lab 10
Understanding Wi-Fi		Issued:	2022-02-02
Wi-Fi (IEEE 802.11)		Submission Due:	2022-02-04
Authors:	João M. Tiago Prof. Luis D. Pedrosa	Comments Due:	-
		Version:	1.0

Question 11. Is the MAC address of the first-hop router ever involved in the disassociation process? Explain how you found that out.

Question 12. Upon disassociation, is the access point still active? If so, can the Apple device perform one more HTTP request through the access point? Explain how you found that out.