DJILLALI LIABES UNIVERSITY OF SIDI BEL ABBES
FACULTY OF EXACT SCIENCES
DEPARTMENT OF COMPUTER SCIENCE

Module : Technologies des réseaux sans fil
2ND YEAR OF MASTER'S DEGREE IN
NETWORKS,INFORMATION SYSTEMS & SECURITY(RSSI)
2022/2023

Wireshark
TP

Student:
HADJAZI M.Hisham
Group: 01 / RSSI

Module Instructor:
Pr.BOUKLI-HACENE Sofiane
TP Instructor:
Pr.BOUKLI-HACENE Sofiane

A paper submitted in fulfilment of the requirements for the
Technologies des réseaux sans fil TP-Wireshark

January 2, 2023

Contents

1 Workspace of TP-Wireshark **1**

2 Description of the network configuration: **2**

3 Traffic description: **3**

4 AP and station configuration details. Access point: **4**

5 Questions: **5**
5.1 Display beacon frames ? 5
5.1.1 Which version of the wifi protocol ? 5
5.1.2 What is the type of multiplexing (spread spectrum) ? 6
5.1.3 What is the highest data rate supported by the access point ? . . 7
5.2 Display RTS / CTS and ACK control frames 7
5.2.1 What is the estimated value of the SIFS from the first 3 RTS ? . . 9
5.3 Show all ICMP packets 11
5.4 Display data frames 12
5.5 Combine the previous filters 12
5.5.1 What do you see? 13

Chapter 1

Workspace of TP-Wireshark

Notes regarding this solution :
This solution and the executions of the code in it was done in the following machine :

- *PC* : Lenovo IdeaPad S210 8GB
- *OS* : Linux Mint 21.1 Vanessa Kernel v5.15.0-56
- *Wireshark on linux* : v3.6.2

Chapter 2

Description of the network configuration:

Consider the network configuration shown in the diagram below. The AP (192.168.2.183) is connected to the backbone machine (192.168.2.201) via an Ethernet network. The station (192.168.2.228) is associated with the access point via a wireless link. A sniffer (Wireshark in Monitor mode) observes the frames exchanged between the station and the AP.

Ping packets from the station with IP address: 192.168.2.228 to the one with IP address: 192.168.2.201 with different Fragment and RTS / CTS Threshold values were captured. Trace file name: case1.pcap

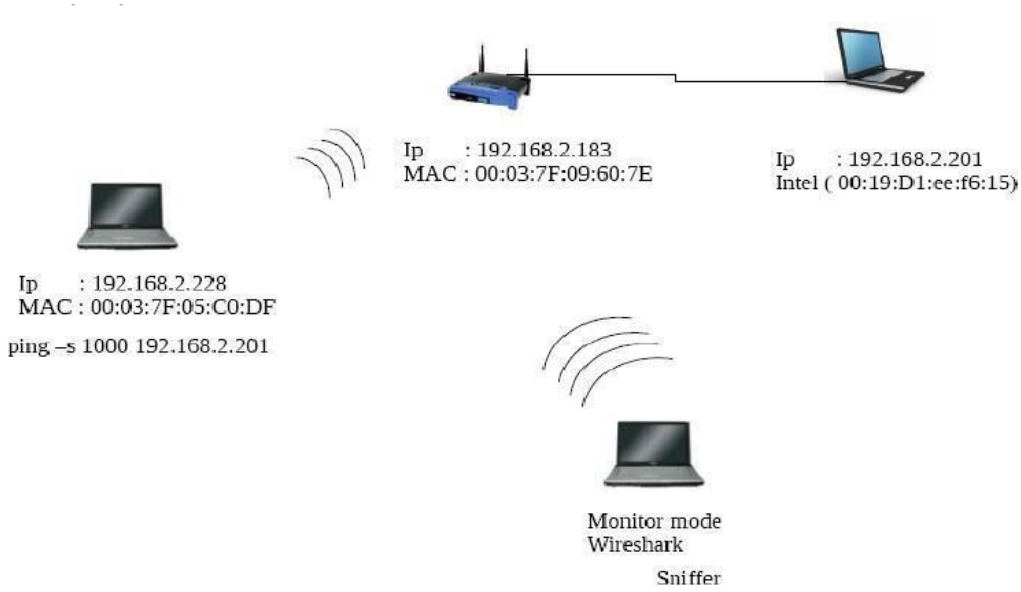

FIGURE 2.1: TP Topology

Chapter 3

Traffic description:

The station generates ICMP traffic using the ping command. The RTS/CTS threshold is set to a 512 bytes and the fragmentation threshold is set to 512 bytes. The payload of the icmp is 1000 bytes. Since the payload of 1000 bytes is greater than the RTS/CTS fragmentation threshold of 512 bytes, the frames sent are fragmented.

Chapter 4

AP and station configuration details. Access point:

- MAC address: 00:03:07 F: 09:60:7E
- IP address: 192.168.2.183
- ESSID: "AUKBCDEMO"
- Mode: Master
- Channel: 1
- Frequency: 2.412 GHz (channel 1)
- IP Source: 192.168.2.228
- IP Source: 192.168.2.228
- IP Destination: 192.168.2.201

Chapter 5

Questions:

5.1 Display beacon frames ?

To display beacon frames in Wireshark, follow these steps:

1. Start Wireshark and open the capture file that contains the beacon frames.
2. In the "Filter" field at the top of the Wireshark window, enter **"wlan.fc.type_subtype == 0x08"**. This filter will show only beacon frames.
3. Click the "Apply" button to apply the filter. Wireshark will now display only beacon frames in the packet list.
4. To view the details of a beacon frame, select it in the packet list and then click the "Details" tab in the middle pane. This will show the contents of the beacon frame, including the beacon interval, the SSID, and other information.

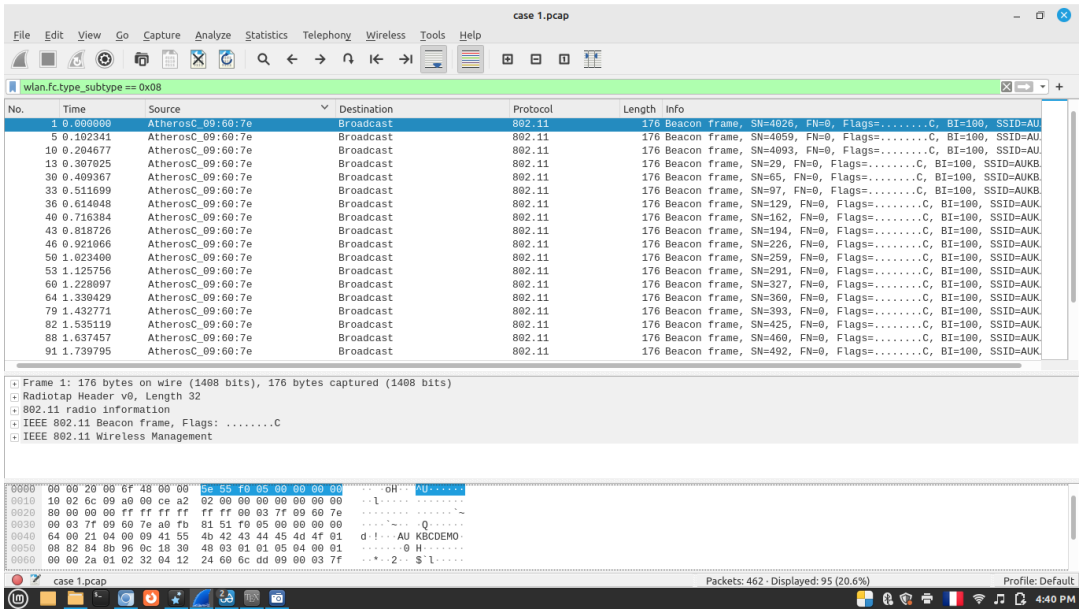

FIGURE 5.1: beacon frames

5.1.1 Which version of the wifi protocol ?

To view the details of a beacon frame, select it in the packet list and then click the "Details" tab in the middle pane. In the middle pane, expand the **"IEEE 802.11 wireless LAN radio information"** section. The "PHY type" field will show the version of the WiFi protocol being used.

There are 2 wireless devices the first is **00:03:7f:09:60:7e** and the second is **00:24:2b:44:44:3b**. both are using **802.11b** wifi version as seen in the screen shots below.

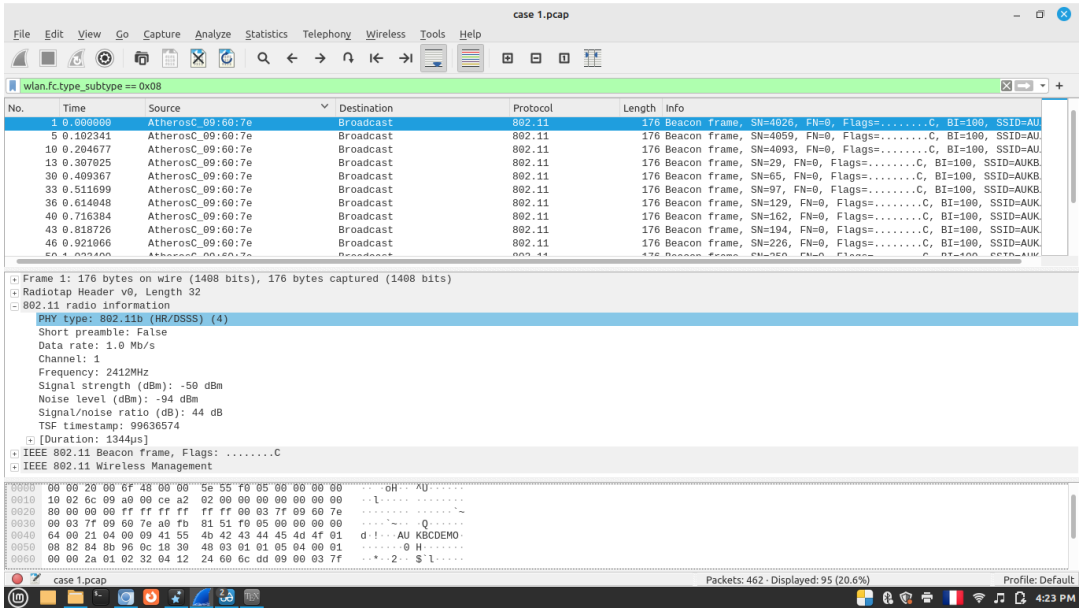

FIGURE 5.2: wifi protocol used in 1st device

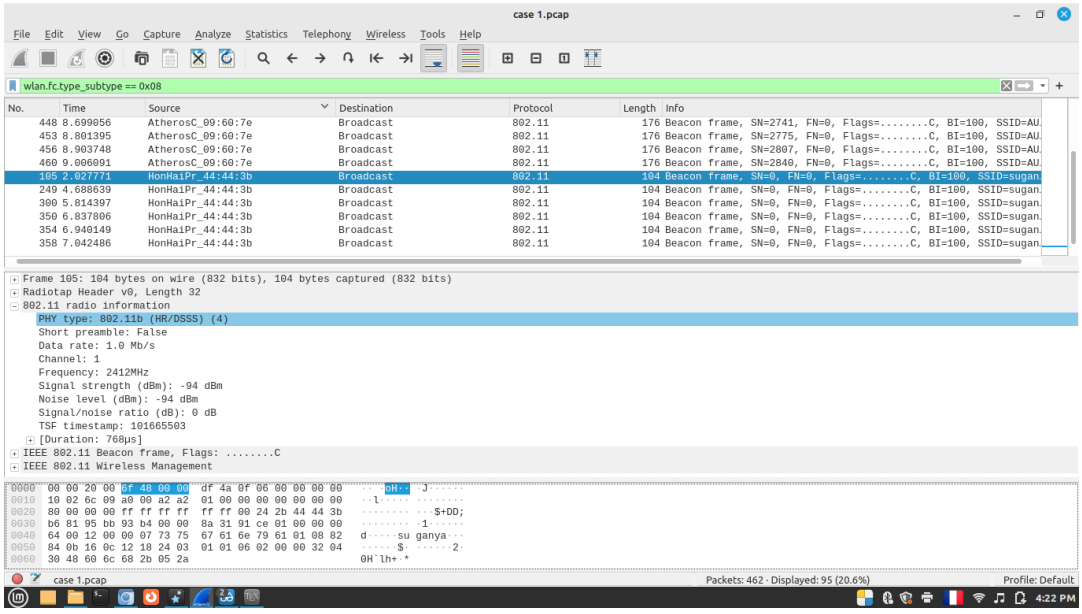

FIGURE 5.3: wifi protocol used in 2nd device

5.1.2 What is the type of multiplexing (spread spectrum) ?

To determine the spread spectrum multiplexing type in a WiFi capture file, you can use the "PHY type" field, which is located in the "IEEE 802.11 wireless LAN radio information" section of the packet details pane.

The "PHY type" field indicates the version of the WiFi protocol being used, and the different versions of the WiFi protocol use different types of spread spectrum

multiplexing. Here is a list of the PHY types and the corresponding spread spectrum multiplexing type:

1. 802.11a: OFDM (Orthogonal Frequency-Division Multiplexing)
2. **802.11b: HR/DSSS (High Rate DSSS)**
3. 802.11g: ERP-OFDM (Extended Rate PHY OFDM)
4. 802.11n: HT (High Throughput)
5. 802.11ac: VHT (Very High Throughput)

As seen in the previous screen shots it is written next to the wifi protocol **802.11b: HR/DSSS** which means **High-rate/direct sequence spread spectrum** multiplexing.

5.1.3 What is the highest data rate supported by the access point ?

It is hard to know sense it could be operating in multiple modes and we only captured the beacons according to the devices connected to the access point not to mention that it can be configured to work in 802.11b but the access point is able to support up to 802.11n for example. but according to only the information we have in the capture file we can assume the following:

1. We found that it is using the **802.11b** wifi protocol.
2. It is also using the **HR/DSSS** spread spectrum.

Assuming the data rate has not been modified by the administrator, the highest **theoretical** data rate should be **11Mbps**[1].

5.2 Display RTS / CTS and ACK control frames

To display Request to Send (RTS) and Clear to Send (CTS) control frames, as well as Acknowledgment (ACK) frames, in Wireshark, In the "Filter" field at the top of the Wireshark window, for RTS we enter **"wlan.fc.type_subtype == 27"**, and for CTS we use **"wlan.fc.type_subtype == 28"**, finally for ACK we can use **"wlan.fc.type_subtype == 29"**. These filters will show us RTS, CTS, and ACK frames.

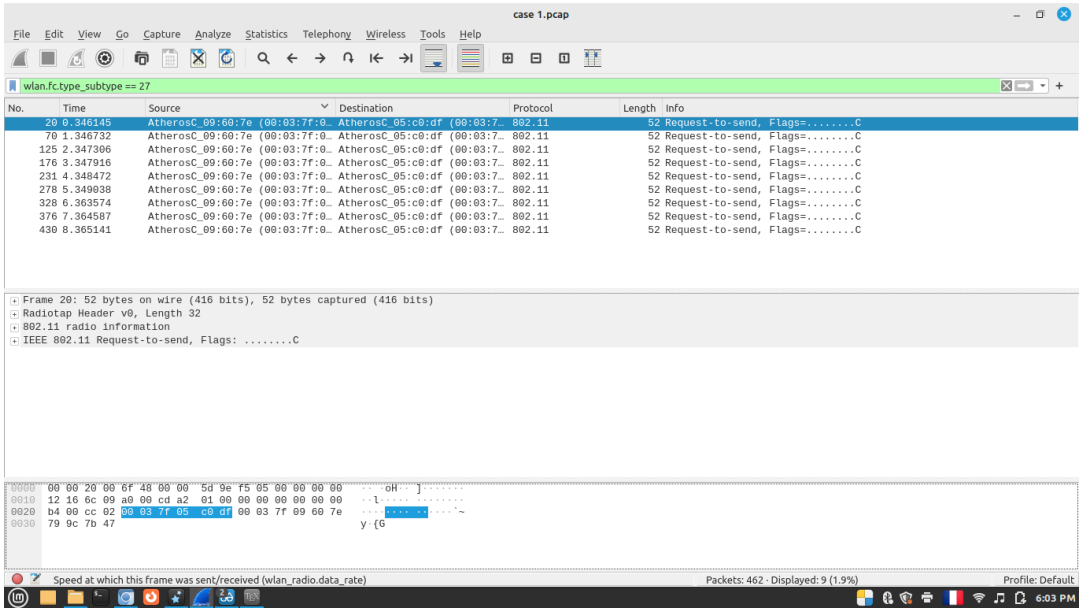

FIGURE 5.4: Request to Send

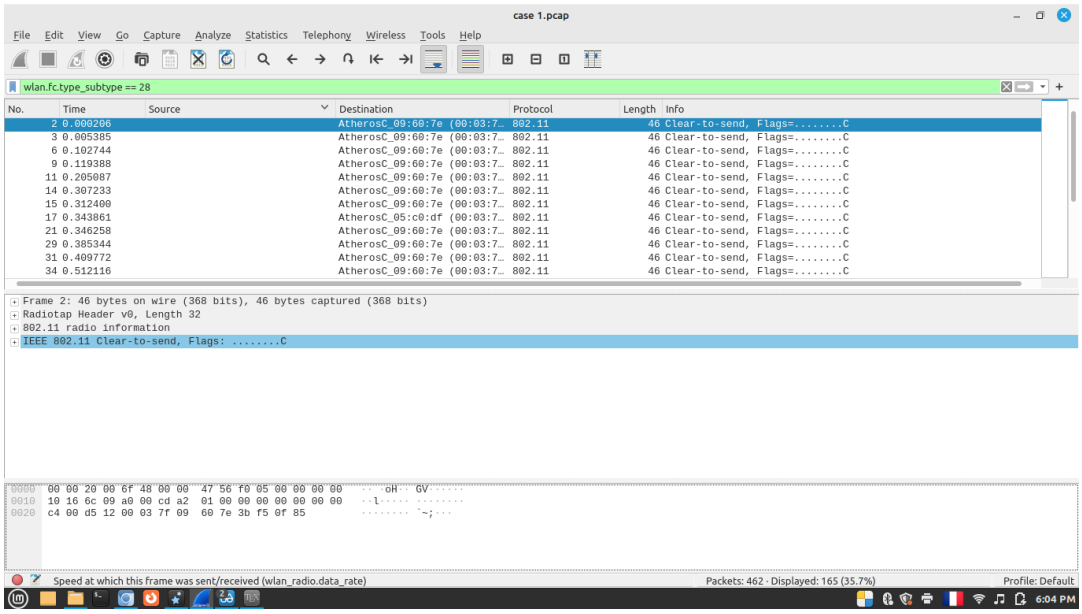

FIGURE 5.5: Clear to Send

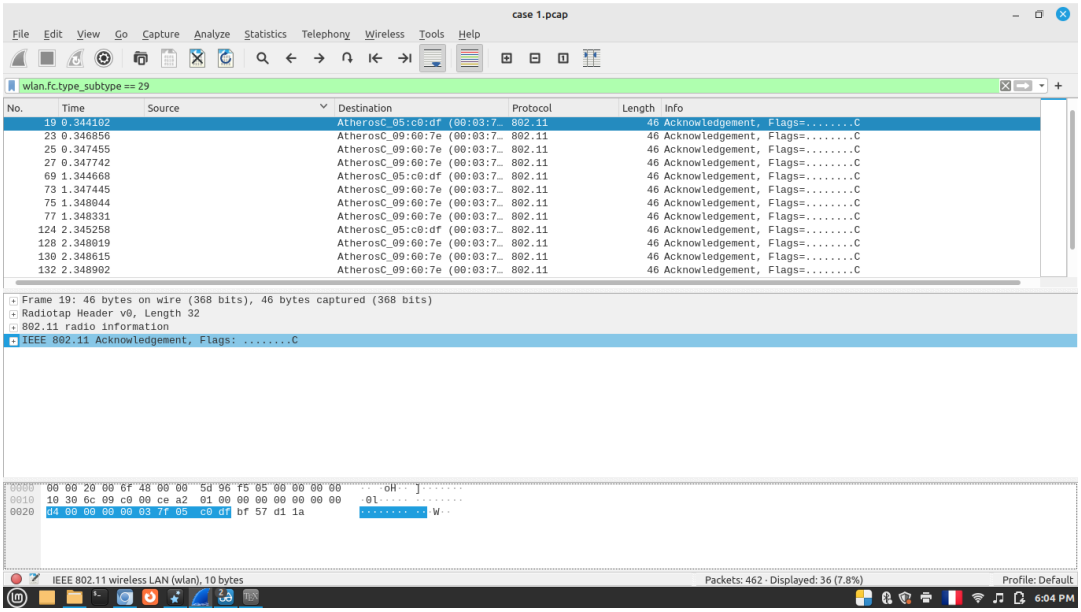

FIGURE 5.6: Acknowledgment

5.2.1 What is the estimated value of the SIFS from the first 3 RTS ?

The Short Inter-Frame Space (SIFS) is the minimum amount of time that a station must wait before transmitting a frame after receiving a frame from another station.

To estimate the value of SIFS from the first 3 RTS frames in a capture file, you can use Wireshark's "Time Delta" column, which shows the time difference between consecutive frames.

To estimate the SIFS value we need to :

1. Display RTS, CTS and ACK traffic only using this filter **"wlan.fc.type_subtype == 27 || wlan.fc.type_subtype == 28 || wlan.fc.type_subtype == 29"**
2. Either **subtract** the times of transmission from the first RTS until last ACK one at a time.
3. Or better activate **Time Delta** which will do it by it self.
4. Repeat for the next RTS.
5. Take the average found.

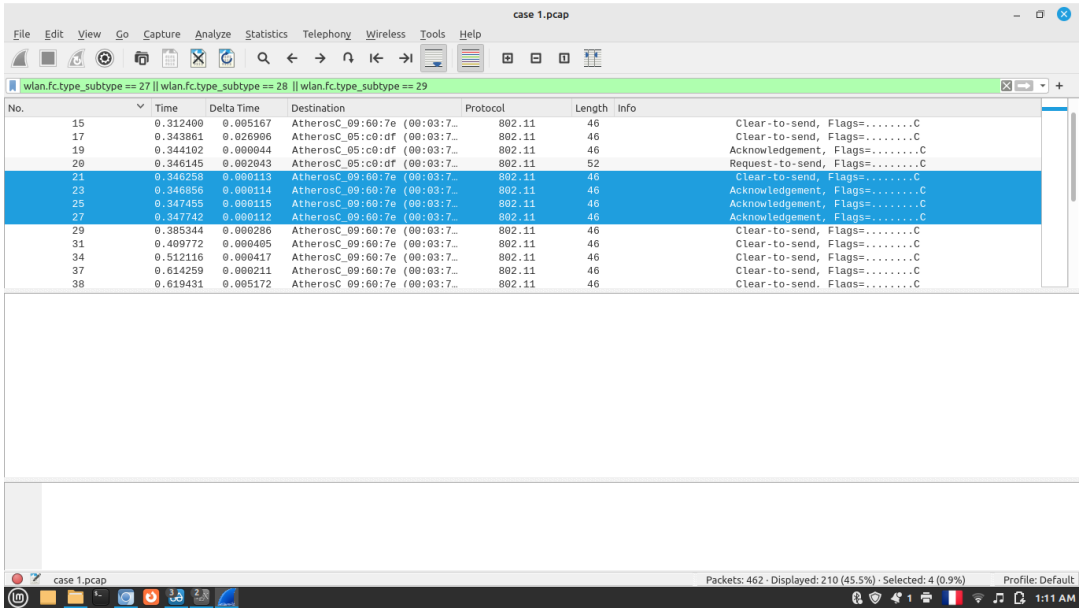

FIGURE 5.7: 1st RTS

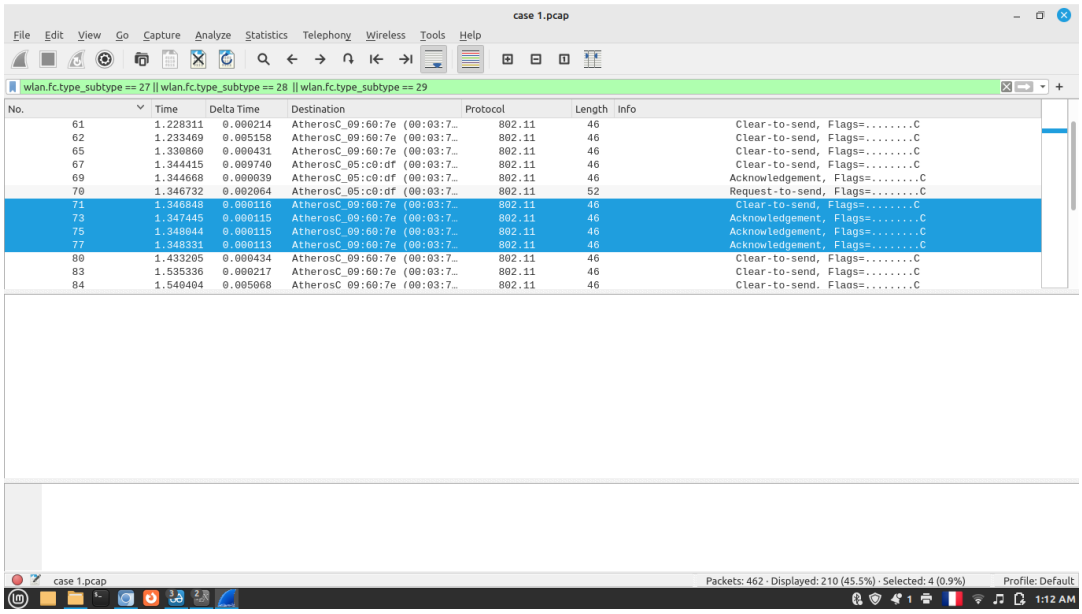

FIGURE 5.8: 2nd RTS

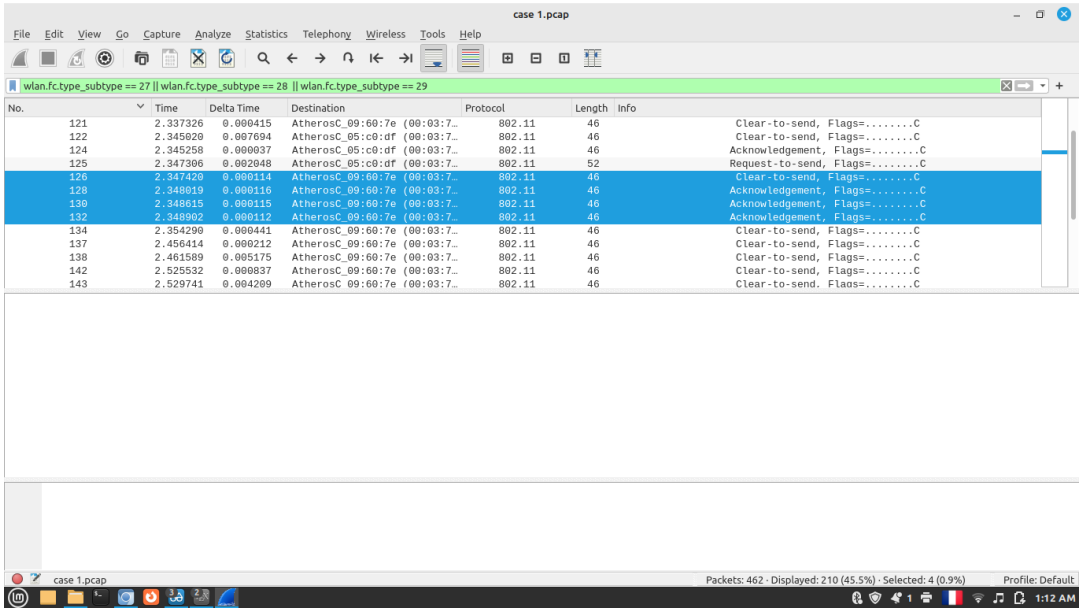

FIGURE 5.9: 3rd RTS

Now lets get the first RTS frame which is frame number **20**, the next frame is a CTS frame and it must be frame number **21**. We know there is a **SIFS** between these two frames so If we subtract the times **0.346258 - 0.346145 = 0.000113** or **11.3 µs**. Checking the second RTS frame which is frame number **70** along with the CTS frame number **71**, and repeat the subtraction of the times **1.346848 - 1.346732 = 0.000116** or **11.6 µs**. now lets do it again for the third RTS frame numbered **125** and CTS frame numbered **1262.346848 - 2.346732 = 0.000114** or **11.4 µs**. If we take the average of the three results we found it is around **11.43 µs**. In the 802.11b standard, the Short Inter-Frame Space (SIFS) is defined as the time a station must wait before transmitting a frame after receiving a frame from another station. The SIFS value for 802.11b is **10 µs** or 10 microseconds.[3]. Now if we look at the screen shots of the three RTS's and check the **Delta Time** column we see that it subtracts by it self from the previous frame and gives us the same results that we just found, not just that it does it with all frames and if carefully look at all the times that are similar to what we found they are all SIFS times too.

5.3 Show all ICMP packets

To display Internet Control Message Protocol (ICMP) packets in Wireshark, In the "Filter" field at the top of the Wireshark window, enter **"icmp"**. This filter will show all ICMP packets.

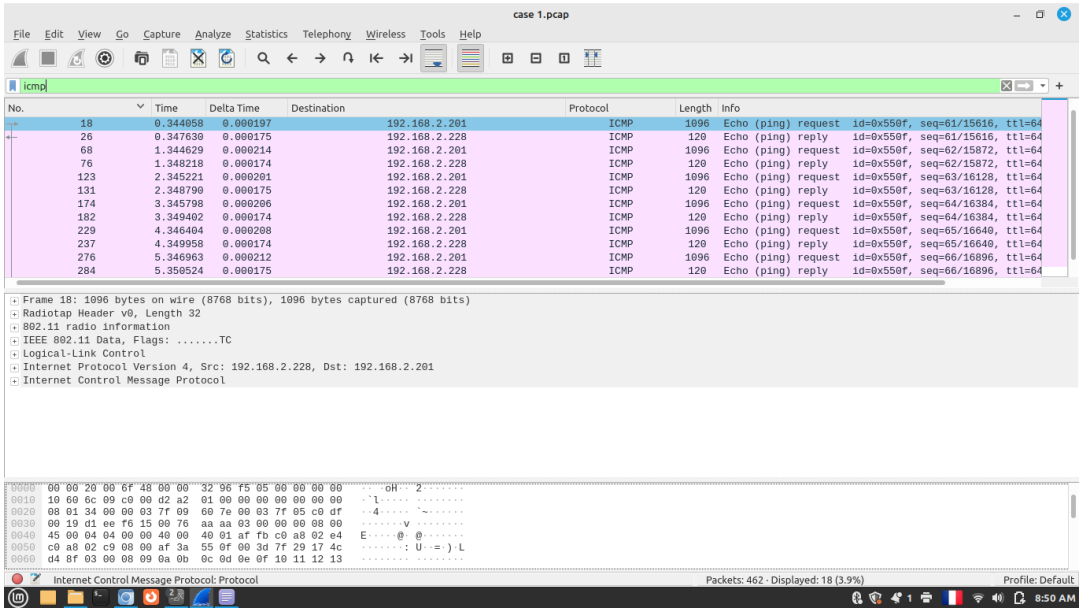

FIGURE 5.10: ALL ICMP Traffic

5.4 Display data frames

To display data frames (also known as data packets or data units) in Wireshark, you can use the filter **"wlan.fc.type == 2"**. This filter will show all frames that contain data, regardless of the protocol being used.

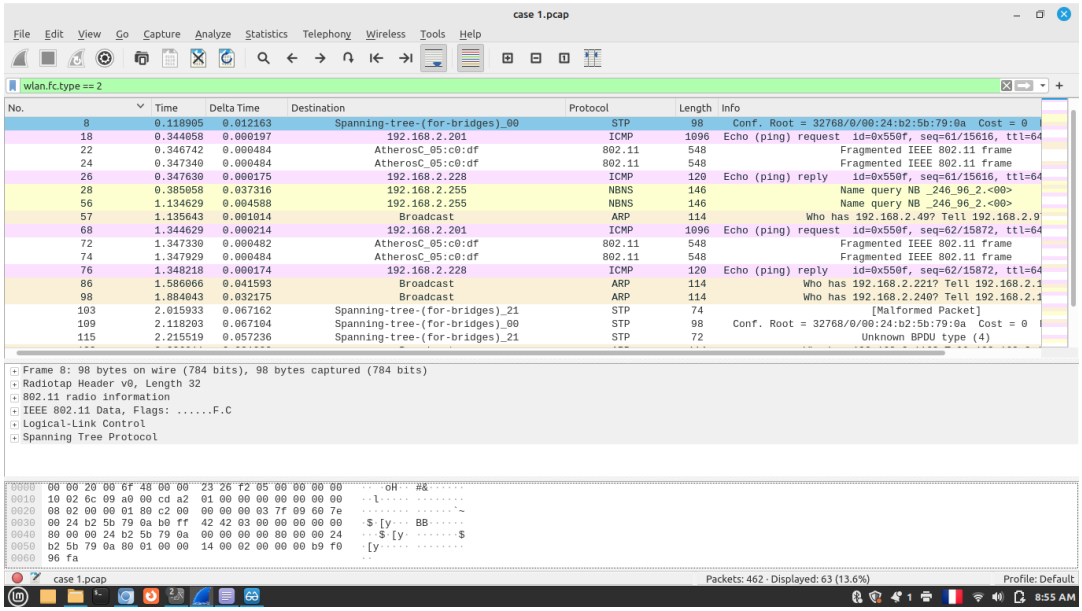

FIGURE 5.11: ALL Data Traffic

5.5 Combine the previous filters

If we combine all the previous filters we get the following **"wlan.fc.type_subtype==8 || wlan.fc.type_subtype == 27 || wlan.fc.type_subtype == 28 || wlan.fc.type_subtype == 29 || icmp || wlan.fc.type == 2"**.

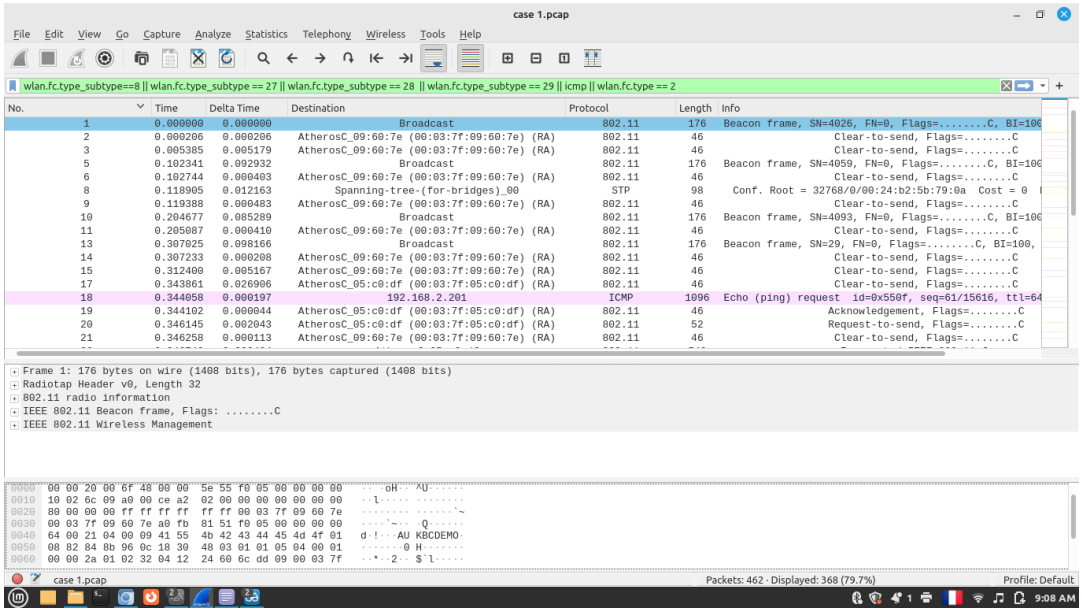

FIGURE 5.12: Combining all filters

5.5.1 What do you see?

This is the entire traffic between a station and an access point from the moment it wants to send **RTS** and receiving the **CTS** from the access point, then the **data** frame is sent and finally a **ACK**. this is the essence of CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance).

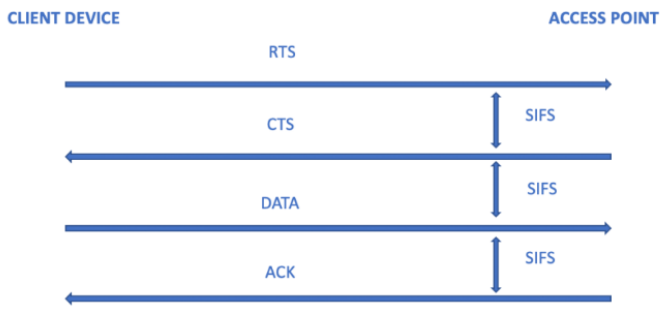

FIGURE 5.13: SIFS

RTS (Request to Send) and CTS (Clear to Send) frames are used to enhance the virtual carrier sense process. It is possible for a client station to be able to communicate with a AP, but not able to hear or be heard by any of the other client stations. This will lead to possible collisions when a station transmits[2].

RTS/CTS is a mechanism that performs NAV distribution and helps to prevent collisions from occurring. So when RTS/CTS is enabled on a STA, every time STA want to transmit a frame, it must perform RTS/CTS exchange prior to the normal data transmission.[2].

As we know medium access is very challenging when there are multiple stations. To provide guaranteed reservation of the common medium and hence uninterrupted data transmission, a station will use RTS/CTS message exchange. Following are the

frame fields of both the RTS frame and CTS frame. As mentioned, RTS does not have any data fields. NAV field in the RTS frame allows CTS frame to be completed. CTS frame will help reserve access for the data part (i.e. data frame)[4].

Below diagram (figure 9.4 IEEE-802.11-2012 std)summarize the RTS/CTS frame exchange and how each of them duration value is calculated[2].

1. **RTS duration = SIFS + CTS + SIFS + Data + SIFS + ACK**
2. **CTS duration = SIFS + Data + SIFS + ACK**

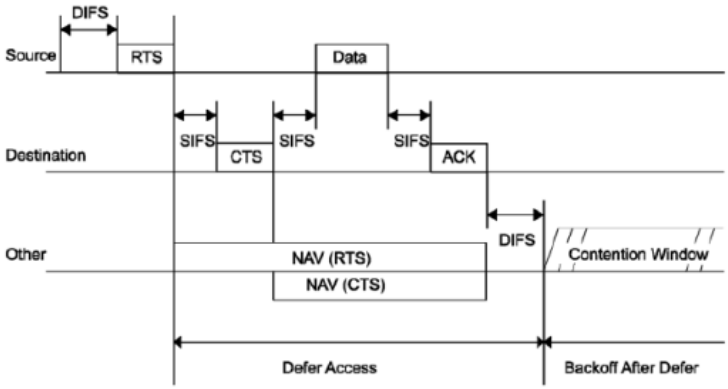

Figure 9-4—RTS/CTS/data/ACK and NAV setting

FIGURE 5.14: IEEE-802.11

If a data frame is a fragmented MSDU or MMPDU then the Duration/ID field of a data and ACK frames specifies the total duration of the next fragment and acknowledgment as shown below[2].

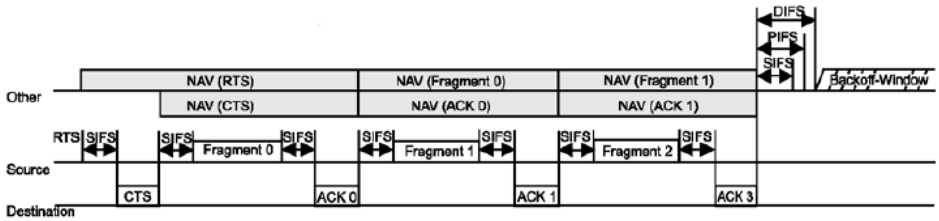

Figure 9-5—RTS/CTS with fragmented MSDU

FIGURE 5.15: fragmented MSDU

Bibliography

[1] *HR/DSSS (High-rate/direct sequence spread spectrum)*. en-GB. Jan. 2022. URL: https://telcomatraining.com/glossary/hr-dsss-high-rate-direct-sequence-spread-spectrum/ (visited on 01/01/2023).

[2] nayarasi. *CWAP – 802.11 Ctrl : RTS/CTS*. en. Oct. 2014. URL: https://mrncciew.com/2014/10/26/cwap-802-11-ctrl-rtscts/ (visited on 01/02/2023).

[3] nayarasi. *CWAP – 802.11 Medium Contention*. en. Oct. 2014. URL: https://mrncciew.com/2014/10/12/cwap-802-11-medium-contention/ (visited on 01/02/2023).

[4] *WLAN RTS CTS funtion-Application of RTS and CTS in 802.11 network*. URL: https://www.rfwireless-world.com/Terminology/WLAN-RTS-CTS-frame.html (visited on 01/02/2023).