

# Practice 1

**Surname:** Alfano

**Name:** Sara

**Degree:** Grado in Informatic Engineering

**Group:** A

**Label of PC used:** Personal computer

**Exercise 1. Choose any http message, and find in the Ethernet II header the following information (make screenshots of the following data):**

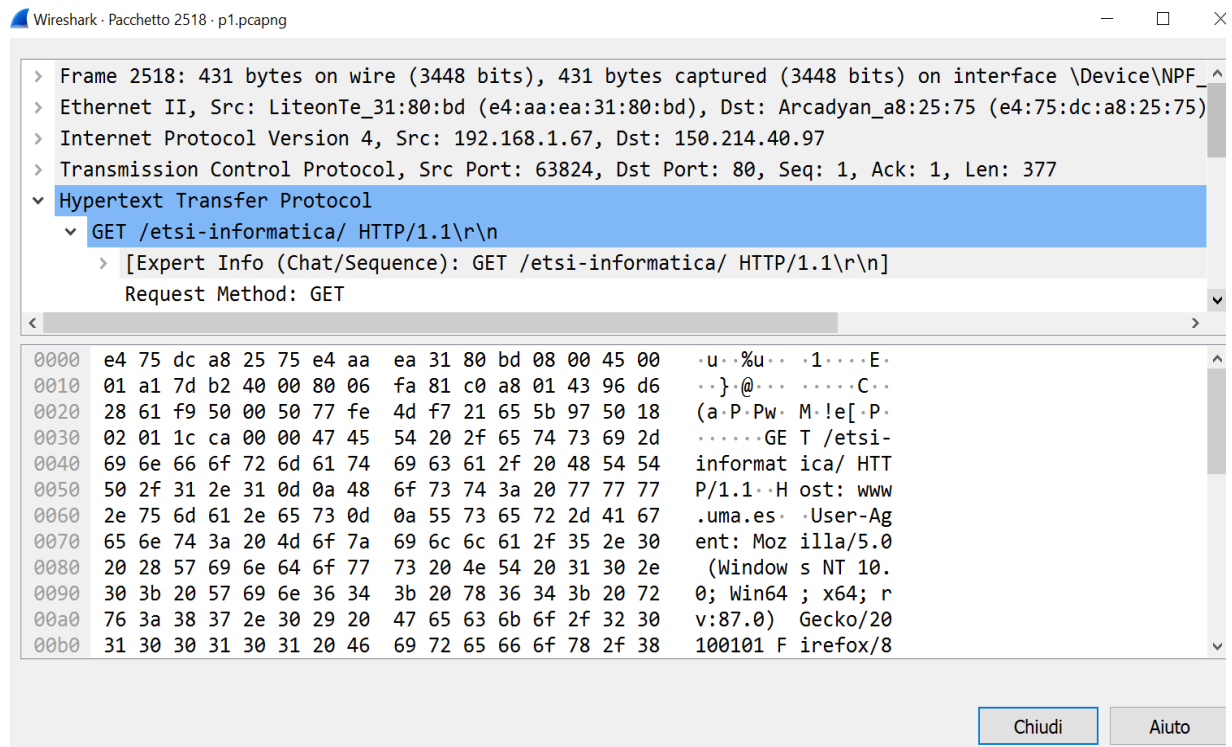
Frame number analysed: 2518

MAC address information of your computer.

MAC Address (in hexadecimal):	e4 aa ea 31 80 bd
NIC Manufacturer (in hexadecimal):	e4 aa ea      name: LiteonTe
NIC serial number (in hexadecimal):	31 80 bd

MAC address information of gateway/router.

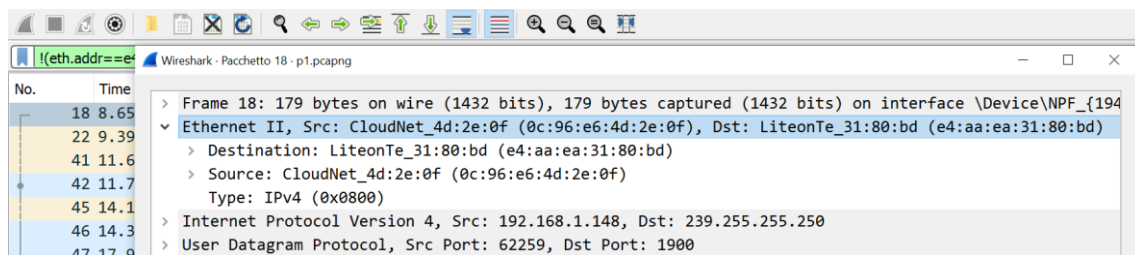
MAC Address (in hexadecimal):	e4 75 dc a8 25 75
NIC Manufacturer (in hexadecimal):	e4 75 dc      name: Arcadyan
NIC serial number (in hexadecimal):	a8 25 75



**Exercise 2. Which filter** do you apply to show all the frames where your MAC address is not used?

- Filter: `!(eth.addr == e4:75:dc:a8:25:75)`
- How many frames do you receive? 16
- Why do you receive these frames? (To answer this question, observe the features of the destination MAC addresses used by those frames) Because I excluded the frames with my MAC address, so in the features of the destinations MAC addresses I have another MAC address: e4:aa:ea:31:80:bd.

Example Frame 18:



Filter applied in Wireshark:

The image shows a Wireshark packet capture window with the filter `!(eth.addr == e4:75:dc:a8:25:75)` applied. The packet list shows 16 frames, all of which are M-SEARCH or Membership Report group messages. The filter bar at the top is highlighted in green.

No.	Time	Source	Destination	Protocol	Length	Info
18	8.65663	192.168.1.148	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
22	9.391971	Normere1_a8:25:77	Broadcast	ARP	42	Who has 192.168.1.59? Tell 1.1.1.2
41	11.644661	Normere1_a8:25:77	Broadcast	ARP	42	Who has 192.168.1.59? Tell 1.1.1.2
42	11.748686	192.168.1.148	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
45	14.102303	Normere1_a8:25:77	Broadcast	ARP	42	Who has 192.168.1.59? Tell 1.1.1.2
46	14.307782	192.168.1.148	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
47	17.918686	192.168.1.148	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
52	20.486274	192.168.1.148	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
63	23.346973	192.168.1.148	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
64	32.288636	192.168.1.67	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
65	33.300446	192.168.1.67	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
66	34.313436	192.168.1.67	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
67	35.313587	192.168.1.67	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
2380	45.506137	192.168.1.67	224.0.0.251	IGMPv2	46	Membership Report group 224.0.0.251
2381	45.508834	192.168.1.67	224.0.0.252	IGMPv2	46	Membership Report group 224.0.0.252
2475	50.495706	192.168.1.67	239.255.255.250	IGMPv2	46	Membership Report group 239.255.255.250

The status bar at the bottom shows: p1.pcapng | Pacchetti: 16261 · visualizzati: 16 (0.1%) | Profilo

**Exercise 3. Draw the protocol stack** (as see in class – the lower level protocols in the bottom) that corresponds to one ARP packet, one ICMP packet, one DNS packet and one HTTP packet:

- Protocol stack of an ARP package (number of selected frame: 41)
- Protocol stack of an ICMP package (number of selected frame 2518 )
- Protocol stack of a DNS package (number of selected frame: 20 )
- Protocol stack of an HTTP package (number of selected frame: 17 )

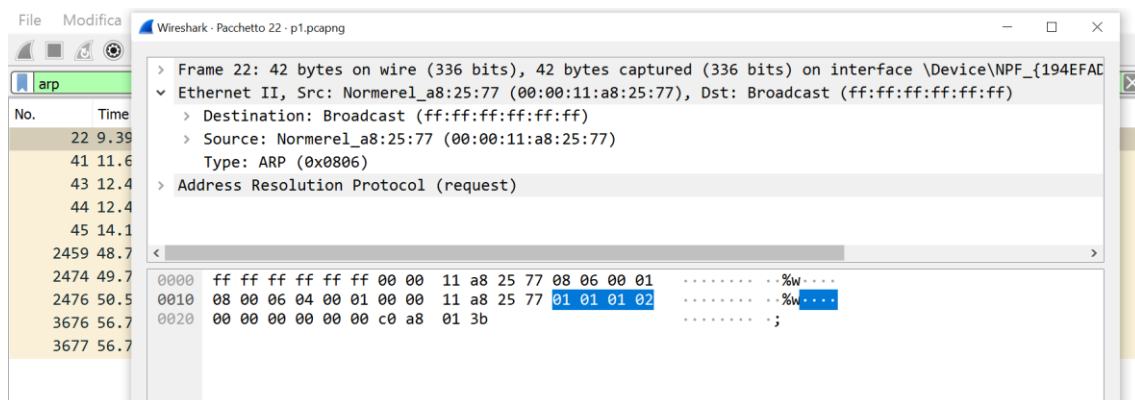
	<i>ARP</i>	<i>ICMP</i>	<i>DNS</i>	<i>HTTP</i>
<i>Application</i>			DNS	HTTP
<i>Transport</i>			UDP	TCP
<i>Internet</i>		IP/ICMP	IP	IP
<i>Data Link</i>	ETHERNET II/ARP	ETHERNET II	ETHERNET II	ETHERNET II

**Exercise 4.** Observe carefully the Ethernet II **type** field in the obtained trace for each one of the previous messages. Fill the following table and answer the questions:

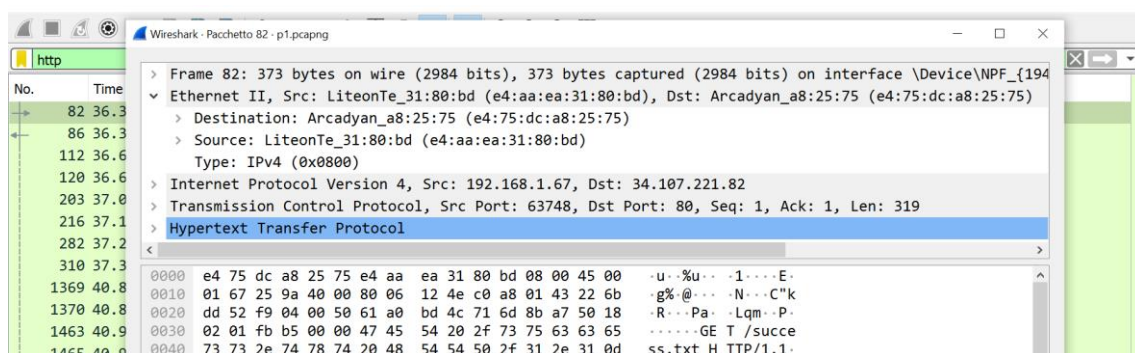
Ethernet II header type		
	Hexadecimal	Text
ARP	0X0806	ARP
HTTP	0X0800	IPv4
ICMP	0X0800	IPv4
DNS	0X0800	IPv4

- What is this field? This field contains a hexadecimal value that is used to indicate the type of upper-layer protocol in the data field.
- Why is it the same for different frames? Because they are using the same protocol

Example ARP:



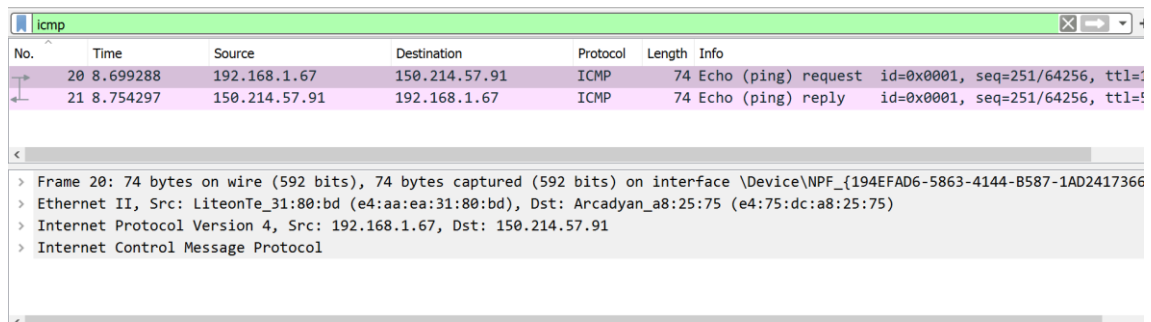
Example HTTP:



**Exercise 5.** In Wireshark observe **the difference between the time** of the first request ICMP (Echo (ping) request) and its answer (Echo (ping) reply):

- Write down the specific frame numbers chosen: 20 and 21
- How much time has passed (in milliseconds)?  $(8,754297 - 8,699288) = 0,055009\text{ms}$
- To which concept, taught in the lectures, matches that time? To the RTT (Round Trip Time)

Frames 20 and 21:

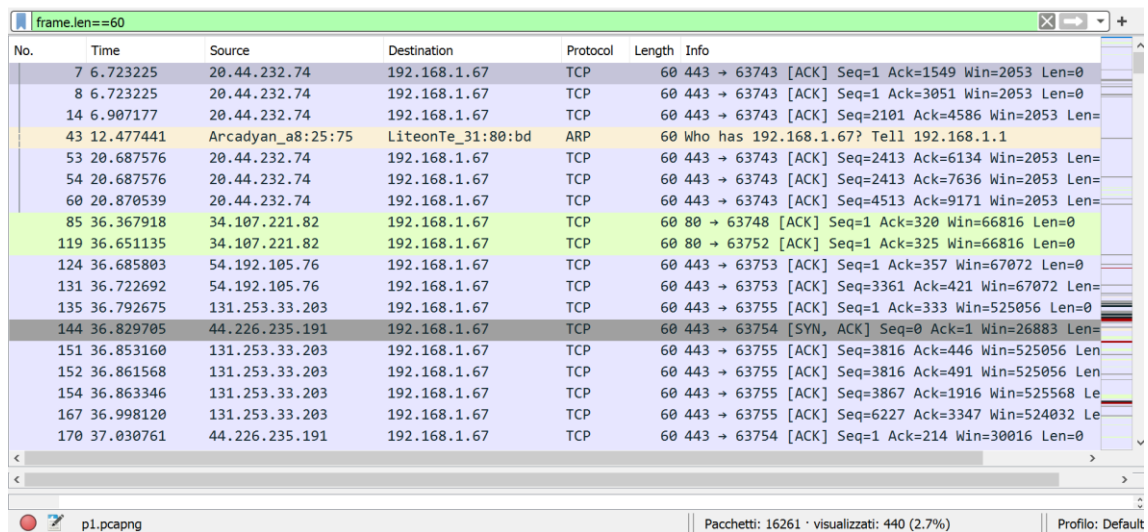


No.	Time	Source	Destination	Protocol	Length	Info
20	8.699288	192.168.1.67	150.214.57.91	ICMP	74	Echo (ping) request id=0x0001, seq=251/64256, ttl=!
21	8.754297	150.214.57.91	192.168.1.67	ICMP	74	Echo (ping) reply id=0x0001, seq=251/64256, ttl=!

< Frame 20: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF\_{194EFAD6-5863-4144-B587-1AD2417366} ...  
> Ethernet II, Src: LiteonTe\_31:80:bd (e4:aa:ea:31:80:bd), Dst: Arcadyan\_a8:25:75 (e4:75:dc:a8:25:75)  
> Internet Protocol Version 4, Src: 192.168.1.67, Dst: 150.214.57.91  
> Internet Control Message Protocol

**Exercise 6.** Based on the lectures, the Ethernet frames must have a **minimum size of 64 bytes**. Wireshark does not show the CRC field, as it is automatically handled by the network card. Hence, the frame that Wireshark shows may have a size of 60 bytes or more:

- Check a frame of size 60 (filter: `frame.len == 60`).
- How many frames have this feature? 440
- Which mechanisms are used to fill the size if the transmitted data is less than 46 bytes)?  
It is used the Padding mechanism.



No.	Time	Source	Destination	Protocol	Length	Info
7	6.723225	20.44.232.74	192.168.1.67	TCP	60	443 → 63743 [ACK] Seq=1 Ack=1549 Win=2053 Len=0
8	6.723225	20.44.232.74	192.168.1.67	TCP	60	443 → 63743 [ACK] Seq=1 Ack=3051 Win=2053 Len=0
14	6.907177	20.44.232.74	192.168.1.67	TCP	60	443 → 63743 [ACK] Seq=2101 Ack=4586 Win=2053 Len=0
43	12.477441	Arcadyan_a8:25:75	LiteonTe_31:80:bd	ARP	60	Who has 192.168.1.67? Tell 192.168.1.1
53	20.687576	20.44.232.74	192.168.1.67	TCP	60	443 → 63743 [ACK] Seq=2413 Ack=6134 Win=2053 Len=0
54	20.687576	20.44.232.74	192.168.1.67	TCP	60	443 → 63743 [ACK] Seq=2413 Ack=7636 Win=2053 Len=0
60	20.870539	20.44.232.74	192.168.1.67	TCP	60	443 → 63743 [ACK] Seq=4513 Ack=9171 Win=2053 Len=0
85	36.367918	34.107.221.82	192.168.1.67	TCP	60	80 → 63748 [ACK] Seq=1 Ack=320 Win=66816 Len=0
119	36.651135	34.107.221.82	192.168.1.67	TCP	60	80 → 63752 [ACK] Seq=1 Ack=325 Win=66816 Len=0
124	36.685803	54.192.105.76	192.168.1.67	TCP	60	443 → 63753 [ACK] Seq=1 Ack=357 Win=67072 Len=0
131	36.722692	54.192.105.76	192.168.1.67	TCP	60	443 → 63753 [ACK] Seq=3361 Ack=421 Win=67072 Len=0
135	36.792675	131.253.33.203	192.168.1.67	TCP	60	443 → 63755 [ACK] Seq=1 Ack=333 Win=525056 Len=0
144	36.829705	44.226.235.191	192.168.1.67	TCP	60	443 → 63754 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0
151	36.853160	131.253.33.203	192.168.1.67	TCP	60	443 → 63755 [ACK] Seq=3816 Ack=446 Win=525056 Len=0
152	36.861568	131.253.33.203	192.168.1.67	TCP	60	443 → 63755 [ACK] Seq=3816 Ack=491 Win=525056 Len=0
154	36.863346	131.253.33.203	192.168.1.67	TCP	60	443 → 63755 [ACK] Seq=3867 Ack=1916 Win=525568 Len=0
167	36.998120	131.253.33.203	192.168.1.67	TCP	60	443 → 63755 [ACK] Seq=6227 Ack=3347 Win=524032 Len=0
170	37.030761	44.226.235.191	192.168.1.67	TCP	60	443 → 63754 [ACK] Seq=1 Ack=214 Win=30016 Len=0

p1.pcapng | Pacchetti: 16261 · visualizzati: 440 (2.7%) | Profilo: Default

**Exercise 7.** Simulate that station A sends one frame to the AP having the stations in the two configurations: with/without hidden terminal. After choosing setting, press the start button, and observe stations B and C:

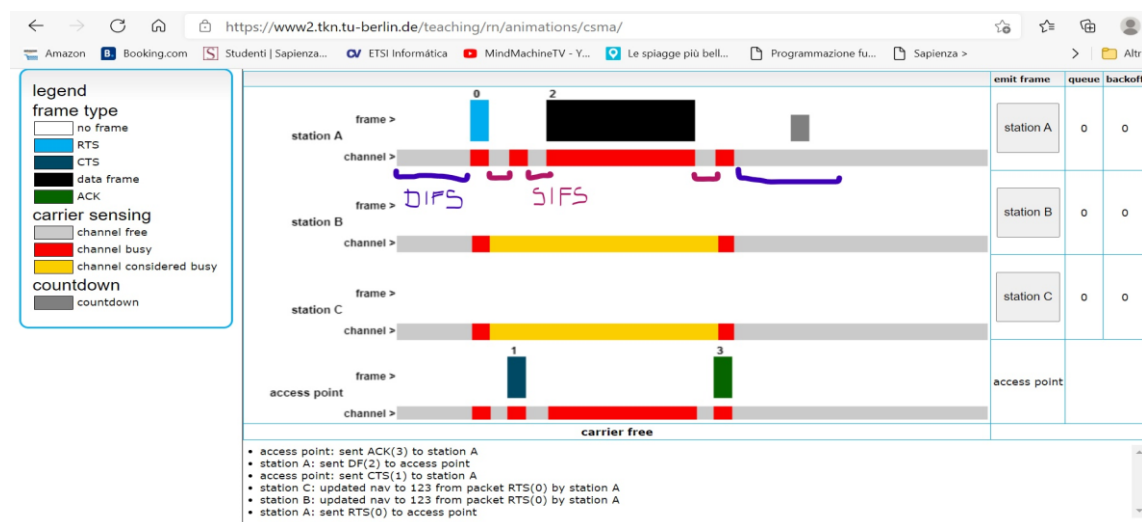
- When does the NAV timer start in each setting? The network allocation vector can be considered as a counter that counts down to zero. The maximum NAV duration is the transmission time required by frame, which is the time for which the channel will be busy. At the start of transmission of a frame, the NAV value is set to its maximum.

Without the hidden terminal it starts when the station A sends the RTS to the access point.

With hidden terminal starts after the access point send the CTS to station A.

- Why does it happen? Because a non-zero value indicates that the channel is busy, and so no station contends for it. When the NAV value decrements to 0, it indicates that the channel is free and the other stations can contend for it.
- Take a screenshot of each setting where one can see when the timer starts, and add them to the report indicating in one of them the DIFS and SIFS times observed.

### Without hidden terminal:

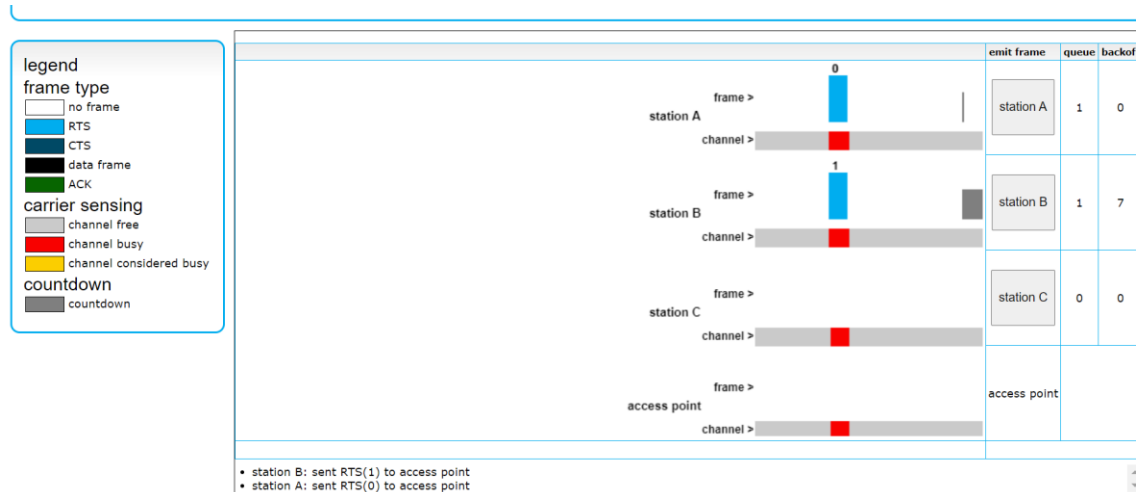


### With hidden terminal:



**Exercise 8.** Without hidden terminal, simulate that stations A and B try to send a frame (press in A and B before clicking Start):

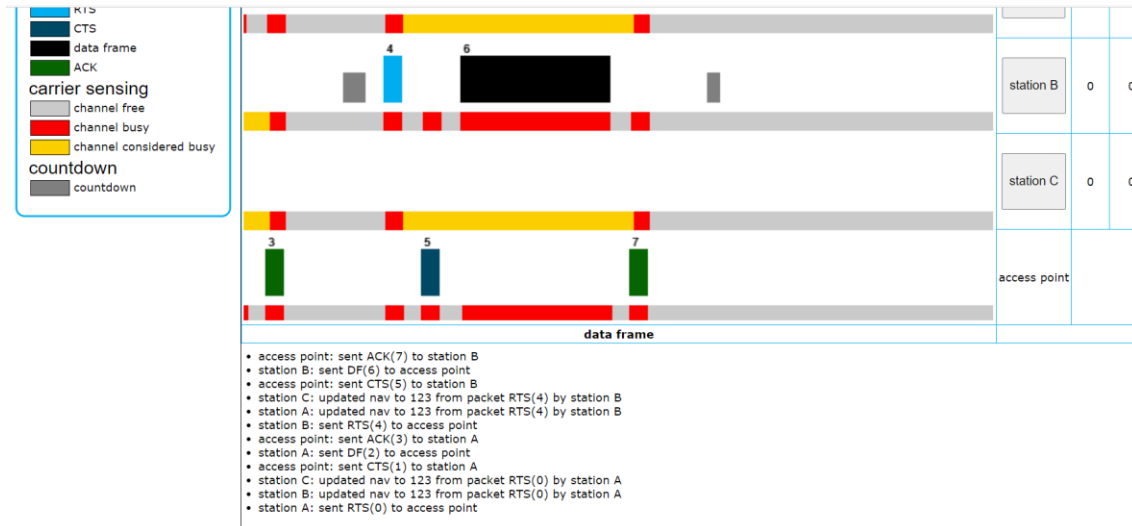
- How does the protocol detect that a collision occurs? It senses the medium after transmitting and detects if the signal being transmitted is different from the signal originally transmitted, in this case it means a collision occurred.
- How is it able to finally send one to the nodes without causing a collision? By retransmitting using the exponential backoff algorithm, until the AP sends out a CTS and puts all other nodes in NAV
- Take screenshots of the whole process and add them to the report.





**Exercise 9.** Now use both settings (with/without hidden terminal), and continue as follows: press the start button in order to send, but immediately press also B (before the graphical confirmation of A's send):

- Without hidden terminal:
  - Why is not station B starting to send (RTS transmission) before A finishes?  
Because station B is updated to NAV when station A sends the RTS, then it waits until station A finishes.



- With hidden terminal:
  - Why is A not detecting B RTS and AP CTS collision?  
Because the terminal is hidden.
  - Why does B send the RTS when A is sending the frame?  
Because it doesn't sense that station A is sending the frame and it is trying to send its RTS.
  - How is that A's frame is able to correctly arrive?  
It retransmits the frame after every collision until the duration of the countdown of B reaches a time where there is no collision. Then, the AP will send the ACK back to station A verifying that the frame arrived correctly.

