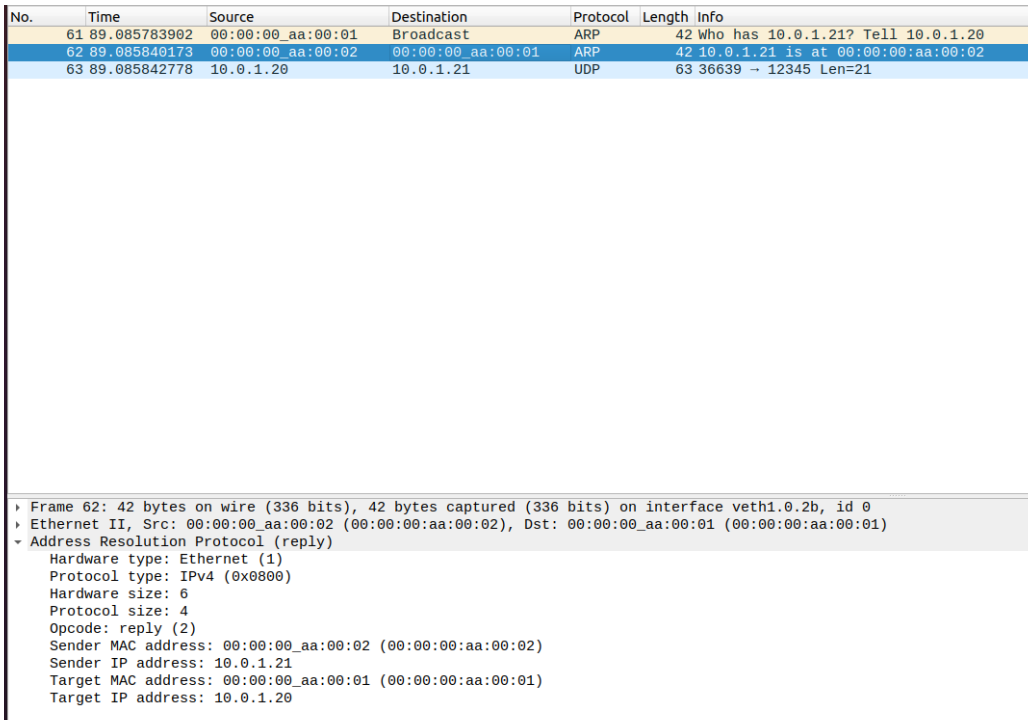
Q1:
Alice eth0: 10.0.1.20/24, 00:00:00:aa:00:01
Bob eth0: 10.0.1.21/24, 00:00:00:aa:00:02
Carol eth0: 10.0.0.20/24, 00:00:00:bb:00:01
Router eth0: 10.0.0.1/24, 00:00:00:bb:00:00
Router eth1: 10.0.1.1/24, 00:00:00:aa:00:00
(IP in the first field, MAC address in the second one)

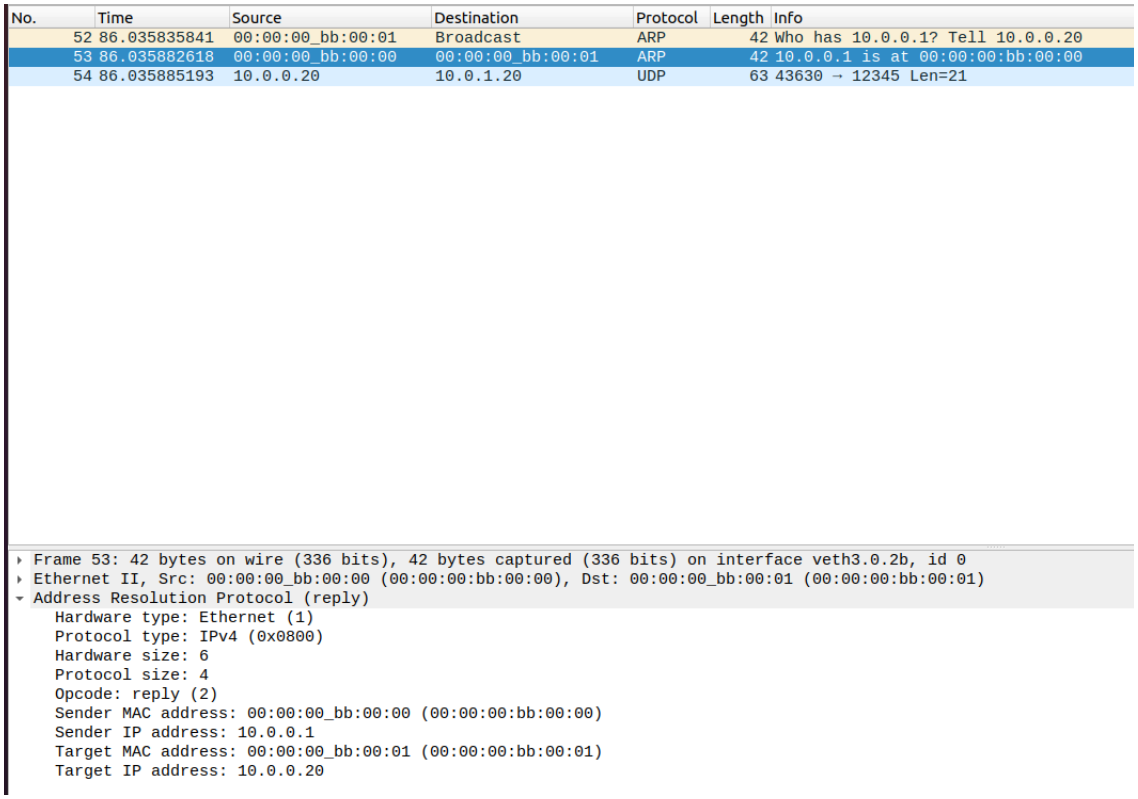
Q2:
The first packet has the job to find the MAC address of the destination host identified by it's IP in the packet. So the first packet has source == MAC addr of Alice and destination == Broadcast to send the packet to all hosts in the subnet. Bob receives that ARP packet and, because it has the destination IP of the packet, replies (to Alice) with another ARP packet identifying it's IP and MAC addresses. The UDP packet is only sent after the ARP packets, because the sender needs to know both the IP and MAC addresses of the destination before sending it.



Q3:
We can conclude that when Bob received the first ARP packet from Alice it registered in it's ARP table the translation between IP and MAC address of Alice to be able to reach it.

Q4:
The first packet is sent from Carol to all hosts in the subnet to find the MAC address of the host matching the destination IP. It finds no answer in the same subnet, so the router will forward the packet from that subnet to another one (this is the difference to Q2: the hosts communicating are not in the same network). This probably happens until the ARP packet finds it's correct

destination. Then, the destination host replies with a packet to Carol identifying it's MAC address. This packet also passes through the router. Only after knowing Alice's IP and MAC addresses, Carol can send the UDP packet.

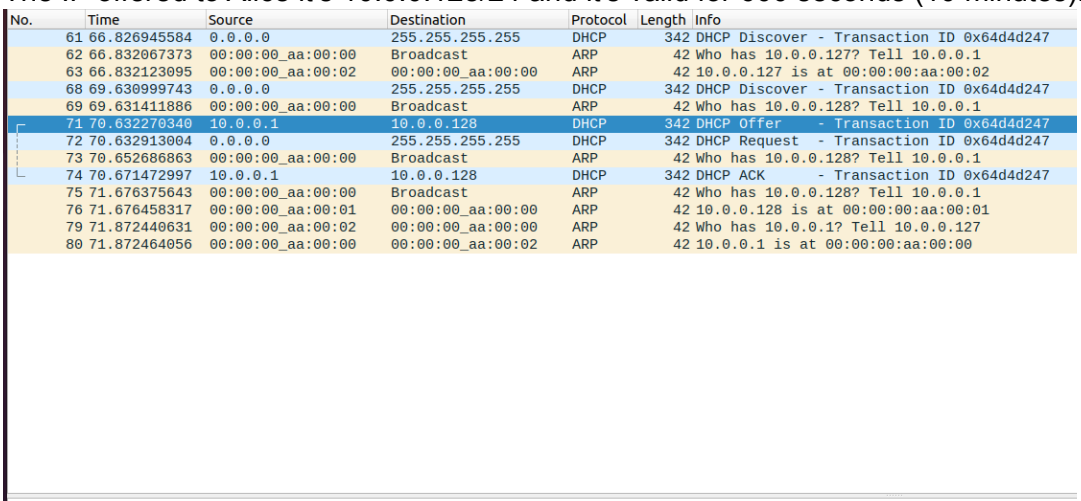


No.	Time	Source	Destination	Protocol	Length	Info
52	86.035835841	00:00:00_bb:00:01	Broadcast	ARP	42	Who has 10.0.0.1? Tell 10.0.0.20
53	86.035882618	00:00:00_bb:00:00	00:00:00_bb:00:01	ARP	42	10.0.0.1 is at 00:00:00:bb:00:00
54	86.035885193	10.0.0.20	10.0.1.20	UDP	63	43630 → 12345 Len=21

```
▸ Frame 53: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface veth3.0.2b, id 0
▸ Ethernet II, Src: 00:00:00_bb:00:00 (00:00:00:bb:00:00), Dst: 00:00:00_bb:00:01 (00:00:00:bb:00:01)
▾ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: 00:00:00_bb:00:00 (00:00:00:bb:00:00)
    Sender IP address: 10.0.0.1
    Target MAC address: 00:00:00_bb:00:01 (00:00:00:bb:00:01)
    Target IP address: 10.0.0.20
```

Q5:

The IP offered to Alice it's 10.0.0.128/24 and it's valid for 600 seconds (10 minutes).

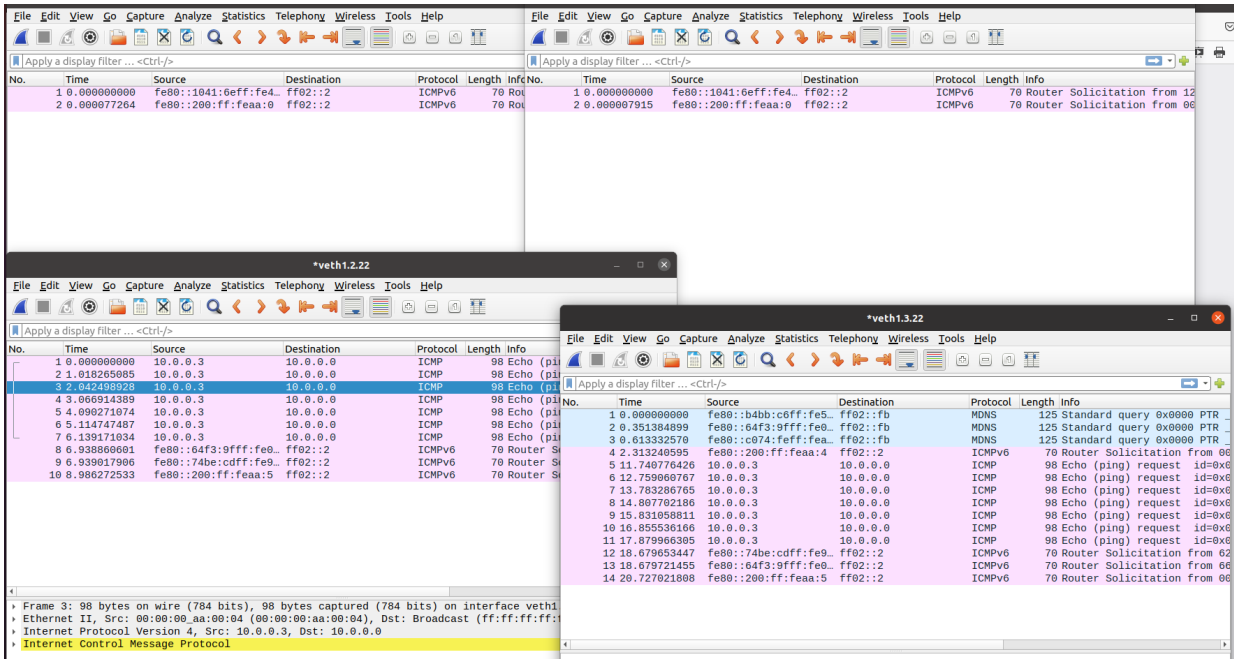


No.	Time	Source	Destination	Protocol	Length	Info
61	66.826945584	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x64d4d247
62	66.832067373	00:00:00_aa:00:00	Broadcast	ARP	42	Who has 10.0.0.127? Tell 10.0.0.1
63	66.832123095	00:00:00_aa:00:02	00:00:00_aa:00:00	ARP	42	10.0.0.127 is at 00:00:00:aa:00:02
68	69.630999743	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x64d4d247
69	69.631411886	00:00:00_aa:00:00	Broadcast	ARP	42	Who has 10.0.0.128? Tell 10.0.0.1
71	70.632270340	10.0.0.1	10.0.0.128	DHCP	342	DHCP Offer - Transaction ID 0x64d4d247
72	70.632913004	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x64d4d247
73	70.652686863	00:00:00_aa:00:00	Broadcast	ARP	42	Who has 10.0.0.128? Tell 10.0.0.1
74	70.671472997	10.0.0.1	10.0.0.128	DHCP	342	DHCP ACK - Transaction ID 0x64d4d247
75	71.676375643	00:00:00_aa:00:00	Broadcast	ARP	42	Who has 10.0.0.128? Tell 10.0.0.1
76	71.676458317	00:00:00_aa:00:01	00:00:00_aa:00:00	ARP	42	10.0.0.128 is at 00:00:00:aa:00:01
79	71.872440631	00:00:00_aa:00:02	00:00:00_aa:00:00	ARP	42	Who has 10.0.0.1? Tell 10.0.0.127
80	71.872464056	00:00:00_aa:00:00	00:00:00_aa:00:02	ARP	42	10.0.0.1 is at 00:00:00:aa:00:00

```
  Hops: 0
  Transaction ID: 0x64d4d247
  Seconds elapsed: 3
▸ Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 10.0.0.128
  Next server IP address: 10.0.0.1
  Relay agent IP address: 0.0.0.0
  Client MAC address: 00:00:00_aa:00:01 (00:00:00:aa:00:01)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
▸ Option: (53) DHCP Message Type (Offer)
▸ Option: (54) DHCP Server Identifier (10.0.0.1)
▾ Option: (51) IP Address Lease Time
    Length: 4
    IP Address Lease Time: (600s) 10 minutes
▸ Option: (1) Subnet Mask (255.255.255.0)
▸ Option: (3) Router
```

Q6:
The router broadcasts ARP requests before sending the DHCP offer to Alice to identify which IPs are available (for lease) in it's network.

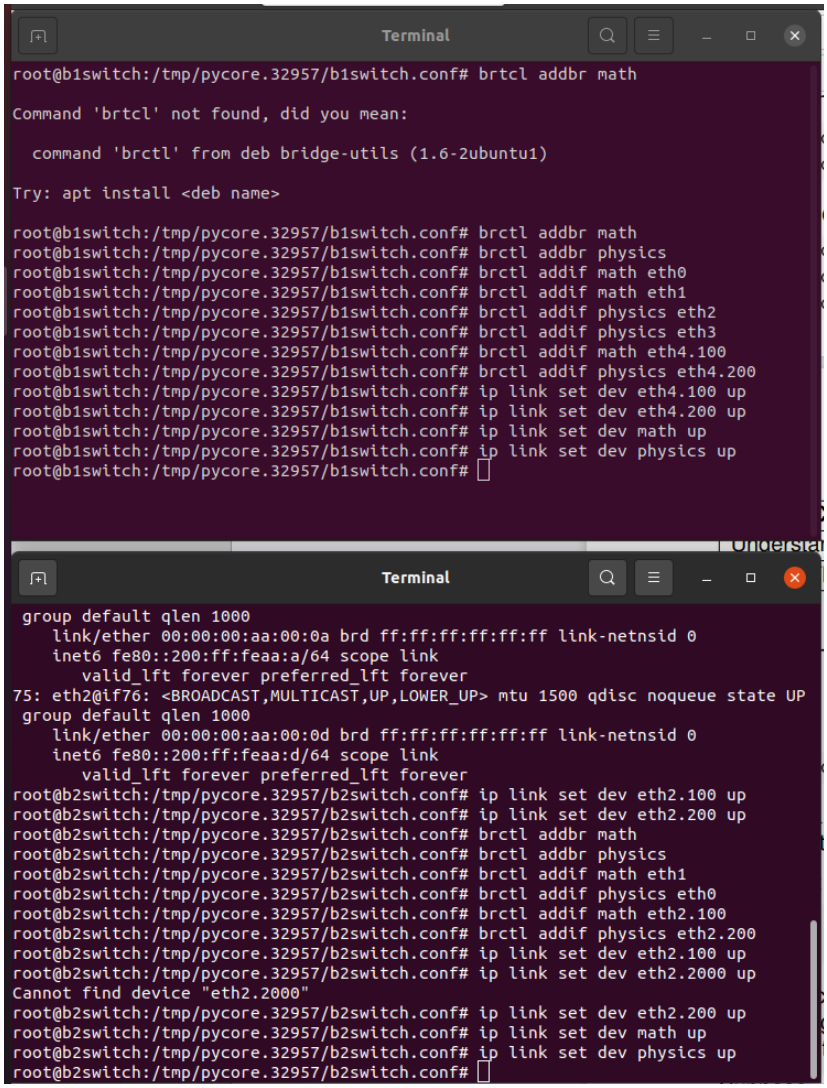
Q7:
Only the interfaces eth2 and eth3 of the switch, belonging to the same VLAN, see the broadcasts of that VLAN. Interfaces eth0 and eth1 don't see the broadcasts, because they are in a separate VLAN, hence not seeing the communications happening in another VLAN.



Interfaces eth0 and eth1 on top, from left to right. And eth2 and eth3 on bottom, from left to right.

Q8:
The interface eth4 of the switch in building 1 needs to tag the packets going through it with VLAN tags so the switch in building 2 knows where the packets came from (which VLAN in building 1) and can redirect them accordingly to hosts of the same VLAN in building 2.

Q9:
Run this in switch of building 2 with <TAGGED_IF> = eth2:
ip link add link <TAGGED_IF> name <TAGGED_IF>.100 type vlan id 100
ip link add link <TAGGED_IF> name <TAGGED_IF>.200 type vlan id 200
ip link set dev <TAGGED_IF>.100 up
ip link set dev <TAGGED_IF>.200 up
And then run the commands shown on the screenshot (top window shows commands to run on switch of building 1 and bottom window shows commands to run on switch of building 2).

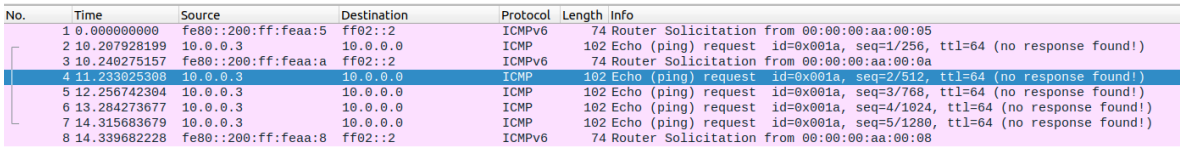


Q10:

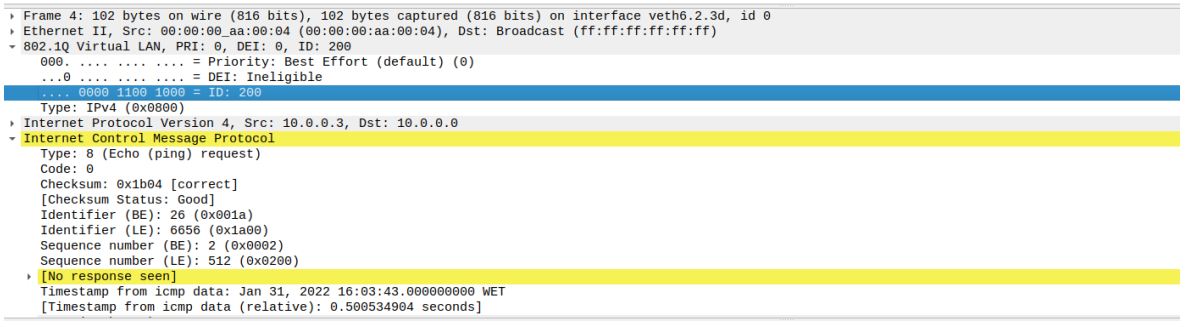
On the switch of building 2, only interfaces eth2 (more specifically eth2.200) and eth0 see the broadcasts, because they belong to the same VLAN (configured using trunk ports). Interface eth1 doesn't see the broadcasts, because it is in a different VLAN, hence not able to see communications in other VLANs.

Q11:

As we can see in the screenshot, the VLAN tag field (ID) has the value 200, meaning that it belongs to the VLAN of Physicists. This happens because the packet was generated in one host belonging to this VLAN and, since both VLANs cannot communicate with each other, the packet can only reach other hosts in the same VLAN.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	fe80::200:ff:feaa:5	ff02::2	ICMPv6	74	Router Solicitation from 00:00:00:aa:00:05
2	10.207928199	10.0.0.3	10.0.0.0	ICMP	102	Echo (ping) request id=0x001a, seq=1/256, ttl=64 (no response found!)
3	10.240275157	fe80::200:ff:feaa:a	ff02::2	ICMPv6	74	Router Solicitation from 00:00:00:aa:00:0a
4	11.233025308	10.0.0.3	10.0.0.0	ICMP	102	Echo (ping) request id=0x001a, seq=2/512, ttl=64 (no response found!)
5	12.256742304	10.0.0.3	10.0.0.0	ICMP	102	Echo (ping) request id=0x001a, seq=3/768, ttl=64 (no response found!)
6	13.284273677	10.0.0.3	10.0.0.0	ICMP	102	Echo (ping) request id=0x001a, seq=4/1024, ttl=64 (no response found!)
7	14.315683679	10.0.0.3	10.0.0.0	ICMP	102	Echo (ping) request id=0x001a, seq=5/1280, ttl=64 (no response found!)
8	14.339682228	fe80::200:ff:feaa:8	ff02::2	ICMPv6	74	Router Solicitation from 00:00:00:aa:00:08



```
▸ Frame 4: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface veth6.2.3d, id 0
▸ Ethernet II, Src: 00:00:00_aa:00:04 (00:00:00:aa:00:04), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▾ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 200
    000. .... .... .... = Priority: Best Effort (default) (0)
    ...0 .... .... .... = DEI: Ineligible
    .... 0000 1100 1000 = ID: 200
    Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 10.0.0.3, Dst: 10.0.0.0
▾ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x1b04 [correct]
    [Checksum Status: Good]
    Identifier (BE): 26 (0x001a)
    Identifier (LE): 6656 (0x1a00)
    Sequence number (BE): 2 (0x0002)
    Sequence number (LE): 512 (0x0200)
  ▸ [No response seen]
    Timestamp from icmp data: Jan 31, 2022 16:03:43.000000000 WET
    [Timestamp from icmp data (relative): 0.500534904 seconds]
```

Q12:

No, because the VLAN tag is only used between the switches (when communicating with each other using bridges) to identify which VLAN the packet belongs to and redirect it accordingly. After it gets redirected, it reaches the subnet without any VLAN tags, because it's already in the correct VLAN.