

Practical Exercises 1

Surname: Hejhal

Name: Jakub

Degree (Ing. del Software/Ing. Informática/Ing. Computadores): Erasmussus student

PC Label in the lab (e.g. 012): personal laptop

Exercise 1. Find an HTTP packet in the packet trace (the first that your computer sent with a GET message) and complete the following schema with the information contained in this packet (make screenshots where these data appear).

MAC address information of your computer.

MAC Address: 40 a3 cc 2a a6 d9

NIC Manufacturer: Intel Corporate

NIC serial number: 2a a6 d9

MAC address information of gateway/router.

MAC Address: 02 10 18 37 91 9c

NIC Manufacturer: not found (<https://aruljohn.com/mac/021018>) , my router probably uses random mac address after each reboot for security reasons

NIC serial number: 37 91 9c

Exercise 2. Which filter do you use to show all frames where your MAC address is not used? Why do you receive these frames? (To answer this question, observe the features of the destination MAC addresses used by these frames)

Answer:

My MAC is 40:a3:cc:2a:a6:d9. Therefore the wireshark filter looks like this:

`eth.src != 40:a3:cc:2a:a6:d9 and eth.dst != 40:a3:cc:2a:a6:d9`

eth.src != 40:a3:cc:2a:a6:d9 and eth.dst != 40:a3:cc:2a:a6:d9						
No.	Time	Source	Destination	Protocol	Length	Info
478	41.665485548	192.168.0.232	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
495	45.352043999	192.168.0.1	224.0.0.1	IGMPv3	60	Membership Query, general
821	61.633848189	192.168.0.32	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
827	62.657649151	192.168.0.32	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
831	63.681738109	192.168.0.32	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
844	64.706241400	192.168.0.32	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
4452	151.952388662	192.168.0.232	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
5053	170.793873283	192.168.0.1	224.0.0.1	IGMPv3	60	Membership Query, general
6358	181.646758366	192.168.0.32	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
6390	182.672514431	192.168.0.32	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
6481	183.695087990	192.168.0.32	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
6493	184.718789023	192.168.0.32	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
7394	210.421176468	HuaweiTe_f6:cd:ec	Broadcast	ARP	60	Who has 192.168.0.1? Tell 192.168.0.55
7484	211.957326470	192.168.0.232	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
8794	271.963780540	192.168.0.232	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
9367	295.310930298	192.168.0.1	224.0.0.1	IGMPv3	60	Membership Query, general
9495	301.659974534	192.168.0.32	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
9539	302.683965067	192.168.0.32	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
9557	303.708057032	192.168.0.32	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
9583	304.690500433	192.168.0.32	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
▶ Frame 7394: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface wlp2s0, id 0 ▼ Ethernet II, Src: HuaweiTe_f6:cd:ec (30:74:96:f6:cd:ec), Dst: Broadcast (ff:ff:ff:ff:ff:ff) ▼ Destination: Broadcast (ff:ff:ff:ff:ff:ff) Address: Broadcast (ff:ff:ff:ff:ff:ff)1.... = LG bit: Locally administered address (this is NOT the factory default)1.... = IG bit: Group address (multicast/broadcast) ▼ Source: HuaweiTe_f6:cd:ec (30:74:96:f6:cd:ec) Address: HuaweiTe_f6:cd:ec (30:74:96:f6:cd:ec)0.... = LG bit: Globally unique address (factory default)0.... = IG bit: Individual address (unicast) Type: ARP (0x0806) Padding: e48e794f990c742cac91d383700acd86f2cc ▼ Address Resolution Protocol (request) Hardware type: Ethernet (1) Protocol type: IPv4 (0x0800) Hardware size: 6						

I receive a lot of different frames, whose destination and source MAC is different from mine. The previous screenshot shows ARP request from my phone on the same WIFI. It's destination MAC is Broadcast, so it makes sense I receive this frame.

eth.src != 40:a3:cc:2a:a6:d9 and eth.dst != 40:a3:cc:2a:a6:d9						
No.	Time	Source	Destination	Protocol	Length	Info
478	41.665485548	192.168.0.232	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
495	45.352043999	192.168.0.1	224.0.0.1	IGMPv3	60	Membership Query, general
821	61.633848189	192.168.0.32	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
827	62.657649151	192.168.0.32	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
831	63.681738109	192.168.0.32	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
844	64.706241400	192.168.0.32	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
4452	151.952388662	192.168.0.232	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
5053	170.793873283	192.168.0.1	224.0.0.1	IGMPv3	60	Membership Query, general
6358	181.646758366	192.168.0.32	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
6390	182.672514431	192.168.0.32	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
6481	183.695087990	192.168.0.32	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
6493	184.718789023	192.168.0.32	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
7394	210.421176468	HuaweiTe_f6:cd:ec	Broadcast	ARP	60	Who has 192.168.0.1? Tell 192.168.0.55
7484	211.957326470	192.168.0.232	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
8794	271.963780540	192.168.0.232	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
9367	295.310930298	192.168.0.1	224.0.0.1	IGMPv3	60	Membership Query, general
9495	301.659974534	192.168.0.32	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
9539	302.683965067	192.168.0.32	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
9557	303.708057032	192.168.0.32	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
9563	304.620500433	192.168.0.32	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
▶ Frame 827: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits) on interface wlp2s0, id 0 ▼ Ethernet II, Src: AzureWav_38:13:a7 (f0:03:8c:38:13:a7), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa) ▼ Destination: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa) Address: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)0. = LG bit: Globally unique address (factory default)1. = IG bit: Group address (multicast/broadcast) ▼ Source: AzureWav_38:13:a7 (f0:03:8c:38:13:a7) Address: AzureWav_38:13:a7 (f0:03:8c:38:13:a7)0. = LG bit: Globally unique address (factory default)0. = IG bit: Individual address (unicast) Type: IPv4 (0x0800) ▶ Internet Protocol Version 4, Src: 192.168.0.32, Dst: 239.255.255.250 ▶ User Datagram Protocol, Src Port: 53963, Dst Port: 1900 ▶ Simple Service Discovery Protocol						

On the other hand, I receive a lot of frames, whose Source and Destination address is not mine MAC and neither Broadcast MAC, as can be seen on the previous screenshot. This is because their Destination MAC is ethernet multicast address.

Exercise 3. Draw the protocol stack and the packet encapsulation that corresponds to each of the following packets: ARP, ICMP, DNS and HTTP packets. Include a screenshot with the information you have used to draw each protocol stack (i.e., the center part of the screen that shows the content of the selected packet).

ARP

Time	Source	Destination	Protocol	Length	Info
336.33.112083780	MS-NLB-PhysServer-1...	IntelCor_2a:a6:d9	ARP	60	Who has 192.168.0.56? Tell 192.168.0.1
337.33.112092214	IntelCor_2a:a6:d9	MS-NLB-PhysServer-1...	ARP	42	192.168.0.56 is at 40:a3:cc:2a:a6:d9
824.62.301665633	MS-NLB-PhysServer-1...	IntelCor_2a:a6:d9	ARP	60	Who has 192.168.0.56? Tell 192.168.0.1
825.62.301680786	IntelCor_2a:a6:d9	MS-NLB-PhysServer-1...	ARP	42	192.168.0.56 is at 40:a3:cc:2a:a6:d9
2275.91.090920545	MS-NLB-PhysServer-1...	IntelCor_2a:a6:d9	ARP	60	Who has 192.168.0.56? Tell 192.168.0.1
2276.91.090930770	IntelCor_2a:a6:d9	MS-NLB-PhysServer-1...	ARP	42	192.168.0.56 is at 40:a3:cc:2a:a6:d9

```

▶ Frame 336: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface wlp2s0, id 0
▼ Ethernet II, Src: MS-NLB-PhysServer-16_18:37:91:9c (02:10:18:37:91:9c), Dst: IntelCor_2a:a6:d9 (40:a3:cc:2a:a6:d9)
  ▼ Destination: IntelCor_2a:a6:d9 (40:a3:cc:2a:a6:d9)
    Address: IntelCor_2a:a6:d9 (40:a3:cc:2a:a6:d9)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  ▼ Source: MS-NLB-PhysServer-16_18:37:91:9c (02:10:18:37:91:9c)
    Address: MS-NLB-PhysServer-16_18:37:91:9c (02:10:18:37:91:9c)
    ....1. .... = LG bit: Locally administered address (this is NOT the factory default)
    ....0. .... = IG bit: Individual address (unicast)
  Type: ARP (0x0806)
  Padding: 00000000000000000000000000000000
▼ Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: MS-NLB-PhysServer-16_18:37:91:9c (02:10:18:37:91:9c)
  Sender IP address: 192.168.0.1
  Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
  Target IP address: 192.168.0.56

```

Ethernet
ARP

ICMP

icmp						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	93.173.138.108	192.168.0.56	ICMP	90	Destination unreachable (Host unreachable)
40	3.700941723	192.168.0.56	172.217.17.14	ICMP	98	Echo (ping) request id=0x0003, seq=1/256, ttl=64 (reply in 41)
41	3.730489631	172.217.17.14	192.168.0.56	ICMP	98	Echo (ping) reply id=0x0003, seq=1/256, ttl=55 (request in 40)
48	4.701458634	192.168.0.56	172.217.17.14	ICMP	98	Echo (ping) request id=0x0003, seq=2/512, ttl=64 (reply in 49)
49	4.726947366	172.217.17.14	192.168.0.56	ICMP	98	Echo (ping) reply id=0x0003, seq=2/512, ttl=55 (request in 48)

▶ Frame 48: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlp2s0, id 0 ▼ Ethernet II, Src: IntelCor_2a:a6:d9 (40:a3:cc:2a:a6:d9), Dst: MS-NLB-PhysServer-16_18:37:91:9c (02:10:18:37:91:9c) Destination: MS-NLB-PhysServer-16_18:37:91:9c (02:10:18:37:91:9c) Address: MS-NLB-PhysServer-16_18:37:91:9c (02:10:18:37:91:9c)1. = LG bit: Locally administered address (this is NOT the factory default)0. = IG bit: Individual address (unicast) Source: IntelCor_2a:a6:d9 (40:a3:cc:2a:a6:d9) Address: IntelCor_2a:a6:d9 (40:a3:cc:2a:a6:d9)0. = LG bit: Globally unique address (factory default)0. = IG bit: Individual address (unicast) Type: IPv4 (0x0800) ▼ Internet Protocol Version 4, Src: 192.168.0.56, Dst: 172.217.17.14 0100 = Version: 4 0101 = Header Length: 20 bytes (5) ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 84 Identification: 0xbf24 (48932) Flags: 0x4000, Don't fragment Fragment offset: 0 Time to live: 64 Protocol: ICMP (1) Header checksum: 0xfcbc [validation disabled] [Header checksum status: Unverified] Source: 192.168.0.56 Destination: 172.217.17.14 ▼ Internet Control Message Protocol Type: 8 (Echo (ping) request) Code: 0 Checksum: 0xebe2 [correct] [Checksum Status: Good] Identifier (BE): 3 (0x0003) Identifier (LE): 768 (0x0300) Sequence number (BE): 2 (0x0002) Sequence number (LE): 512 (0x0200) [Response frame: 49] Timestamp from icmp data: Mar 30, 2020 22:39:20.000000000 CEST [Timestamp from icmp data (relative): 0.953821252 seconds] ▶ Data (48 bytes)

Ethernet

Link layer

IPv4

Network layer

ICMP

Transport layer

DNS

dns						
No.	Time	Source	Destination	Protocol	Length	Info
2034	85.043329309	192.168.0.1	192.168.0.56	DNS	123	Standard query response 0xa096 AAAA ogs.google.com CNAME www3
2119	85.582238098	192.168.0.56	192.168.0.1	DNS	75	Standard query 0xffc0 A play.google.com
2120	85.582262504	192.168.0.56	192.168.0.1	DNS	75	Standard query 0x0bcb AAAA play.google.com
2121	85.586533302	192.168.0.56	192.168.0.1	DNS	75	Standard query 0xc323 A play.google.com
2123	85.614919790	192.168.0.1	192.168.0.56	DNS	91	Standard query response 0xffc0 A play.google.com A 216.58.211
2124	85.614920011	192.168.0.1	192.168.0.56	DNS	103	Standard query response 0x0bcb AAAA play.google.com AAAA 2a00
2125	85.614920055	192.168.0.1	192.168.0.56	DNS	91	Standard query response 0xc323 A play.google.com A 216.58.211
2146	85.695875392	192.168.0.56	192.168.0.1	DNS	75	Standard query 0x9113 A play.google.com
2147	85.695902781	192.168.0.56	192.168.0.1	DNS	75	Standard query 0x201f AAAA play.google.com
2149	85.705386550	192.168.0.1	192.168.0.56	DNS	91	Standard query response 0x9113 A play.google.com A 216.58.211
2150	85.705386761	192.168.0.1	192.168.0.56	DNS	103	Standard query response 0x201f AAAA play.google.com AAAA 2a00
2409	97.319769863	192.168.0.56	192.168.0.1	DNS	82	Standard query 0xdc2a A target.technicolor.net
2410	97.319788449	192.168.0.56	192.168.0.1	DNS	82	Standard query 0x132d AAAA target.technicolor.net
2411	97.372789632	192.168.0.1	192.168.0.56	DNS	141	Standard query response 0xdc2a No such name A target.technico
2412	97.372789932	192.168.0.1	192.168.0.56	DNS	141	Standard query response 0x132d No such name AAAA target.technico
2413	97.372960065	192.168.0.56	192.168.0.1	DNS	66	Standard query 0xd380 A target
2414	97.372978759	192.168.0.56	192.168.0.1	DNS	66	Standard query 0x7581 AAAA target
2415	97.381872397	192.168.0.1	192.168.0.56	DNS	66	Standard query response 0xd380 A target
2416	97.381872397	192.168.0.1	192.168.0.56	DNS	66	Standard query response 0x7581 AAAA target
▶ Frame 2120: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface wlp2s0, id 0 ▼ Ethernet II, Src: IntelCor_2a:a6:d9 (40:a3:cc:2a:a6:d9), Dst: MS-NLB-PhysServer-16_18:37:91:9c (02:10:18:37:91:9c) ▼ Destination: MS-NLB-PhysServer-16_18:37:91:9c (02:10:18:37:91:9c) Address: MS-NLB-PhysServer-16_18:37:91:9c (02:10:18:37:91:9c)1..... = LG bit: Locally administered address (this is NOT the factory default)0..... = IG bit: Individual address (unicast) ▼ Source: IntelCor_2a:a6:d9 (40:a3:cc:2a:a6:d9) Address: IntelCor_2a:a6:d9 (40:a3:cc:2a:a6:d9)0..... = LG bit: Globally unique address (factory default)0..... = IG bit: Individual address (unicast) Type: IPv4 (0x0800) ▶ Internet Protocol Version 4, Src: 192.168.0.56, Dst: 192.168.0.1 ▶ User Datagram Protocol, Src Port: 36784, Dst Port: 53 ▶ Domain Name System (query)						

Ethernet	Link layer
IPv4	Network layer
UDP	Transport layer
DNS	Application layer

HTTP

http						
No.	Time	Source	Destination	Protocol	Length Info	
3176	28.393651968	212.145.41.179	192.168.0.56	OCSP	979	Response
3831	28.772844827	192.168.0.56	77.75.75.173	HTTP	485	GET / HTTP/1.1
3857	29.842603517	77.75.75.173	192.168.0.56	HTTP	415	HTTP/1.1 301 Moved Permanently (text/html)
3957	30.028076081	192.168.0.56	212.145.41.179	OCSP	449	Request
3966	30.065074970	212.145.41.179	192.168.0.56	OCSP	070	Response
▶ Frame 3831: 485 bytes on wire (3880 bits), 485 bytes captured (3880 bits) on interface wlp2s0, id 0 ▼ Ethernet II, Src: IntelCor_2a:a6:d9 (40:a3:cc:2a:a6:d9), Dst: MS-NLB-PhysServer-16_18:37:91:9c (02:10:18:37:91:9c) Destination: MS-NLB-PhysServer-16_18:37:91:9c (02:10:18:37:91:9c) Address: MS-NLB-PhysServer-16_18:37:91:9c (02:10:18:37:91:9c)1..... = LG bit: Locally administered address (this is NOT the factory default)0..... = IG bit: Individual address (unicast) Source: IntelCor_2a:a6:d9 (40:a3:cc:2a:a6:d9) Address: IntelCor_2a:a6:d9 (40:a3:cc:2a:a6:d9)0..... = LG bit: Globally unique address (factory default)0..... = IG bit: Individual address (unicast) Type: IPv4 (0x0800) ▼ Internet Protocol Version 4, Src: 192.168.0.56, Dst: 77.75.75.173 0100 = Version: 4 0101 = Header Length: 20 bytes (5) Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 471 Identification: 0x3f64 (16228) Flags: 0x4000, Don't fragment Fragment offset: 0 Time to live: 64 Protocol: TCP (6) Header checksum: 0x9fe4 [validation disabled] [Header checksum status: Unverified] Source: 192.168.0.56 Destination: 77.75.75.173 ▶ Transmission Control Protocol, Src Port: 54894, Dst Port: 80, Seq: 1, Ack: 1, Len: 419 ▼ Hypertext Transfer Protocol GET / HTTP/1.1\r\n Host: novinky.cz\r\n User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:74.0) Gecko/20100101 Firefox/74.0\r\n Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n Accept-Language: en-US,en;q=0.5\r\n Accept-Encoding: gzip, deflate\r\n Connection: keep-alive\r\n Cookie: __gfp_64b=hoEnYvMLbxFAi28c5s112pqZd25Fs5_k3ca7brscPAN.K7\r\n Upgrade-Insecure-Requests: 1\r\n \r\n [Full request URI: http://novinky.cz/] [HTTP request 1/1] [Response in frame: 3857]						

Ethernet	Link layer
IPv4	Network layer
TCP	Transport layer
HTTP	Application layer

Exercise 4. Observe carefully the Ethernet II **type** field in the obtained trace and make a screenshot for each protocol in the table below. What is the utility of this field? Why different frames contain the same type value? After answering these questions fill the following table with the number that appears for the type field.

Tipo en la cabecera Ethernet II	
ARP	0x0806
HTTP	0x0800
ICMP	0x0800
DNS	0x0800

ARP

```

▼ Ethernet II, Src: MS-NLB-Phys
  ▼ Destination: IntelCor_2a:a6:
    Address: IntelCor_2a:a6:
      ....0. ....
      ....0 ....
  ▼ Source: MS-NLB-PhysServer-1
    Address: MS-NLB-PhysServ
      ....1. ....
      ....0 ....
  Type: ARP (0x0806)
  Padding: 0000000000000000
  ▼ Address Resolution Protocol (i
    ...
  
```

HTTP

```

Frame 602: 401 bytes on wire
▼ Ethernet II, Src: Intel
  ▼ Destination: MS-NLB-
    Address: MS-NLB-Pl
      ....1. ....
      ....0 ....
  ▼ Source: IntelCor_2a:
    Address: IntelCor_
      ....0. ....
      ....0 ....
  Type: IPv4 (0x0800)

```

ICMP

```

Frame 4011: 98 bytes on wire
▼ Ethernet II, Src: MS-NLB-Ph
  ▼ Destination: IntelCor_2a:
    Address: IntelCor_2a:a
      ....0. ....
      ....0 ....
  ▼ Source: MS-NLB-PhysServer
    Address: MS-NLB-PhysSe
      ....1. ....
      ....0 ....
  Type: IPv4 (0x0800)
  ▼ Internet Protocol Version 4

```


DNS

```

    Ethernet II, Src: IntelCor_2
      Destination: MS-NLB-PhysS
        Address: MS-NLB-PhysSer
          ....1. ....
          ....0
      Source: IntelCor_2a:a6:d9
        Address: IntelCor_2a:a6
          ....0. ....
          ....0
          Type: IPv4 (0x0800)
    Internet Protocol Version 4,

```

EtherType is a two-octet field in an Ethernet frame. It is used to indicate which protocol is encapsulated in the payload of the frame. ICMP, HTTP and DNS have the same EtherType field, because all of those protocols use IPv4 protocol at network OSI layer.

Exercise 5. Pay attention to the difference between the times of the ICMP request and its answer. How much time is it? What is the concept of the theory that corresponds to this time? The ping command returns some lines with the following format:

Respuesta desde 150.214.57.60: bytes=32 tiempo=45ms TTL=50

Observe times obtained by the ping command and compare them with the times that appear in the Wireshark trace. Are times obtained by the ping command consistent with times that appear in the Wireshark trace?

icmp					
No.	Time	Source	Destination	Protocol	Leng
32	1.911584740	192.168.0.56	216.58.211.238	ICMP	98
33	1.940300128	216.58.211.238	192.168.0.56	ICMP	98
48	2.913171726	192.168.0.56	216.58.211.238	ICMP	98
49	2.942723512	216.58.211.238	192.168.0.56	ICMP	98
63	3.915076658	192.168.0.56	216.58.211.238	ICMP	98
64	3.944204720	216.58.211.238	192.168.0.56	ICMP	98

▼ Frame 33: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▼ Interface id: 0 (wlp2s0)
Interface name: wlp2s0
Encapsulation type: Ethernet (1)
Arrival Time: Mar 30, 2020 23:08:58.687674336 CEST
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1585602538.687674336 seconds
[Time delta from previous captured frame: 0.028715388 seconds]
[Time delta from previous displayed frame: 0.028715388 seconds]
[Time since reference or first frame: 1.940300128 seconds]
Frame Number: 33

Time difference between ICMP request and ICMP response frames (Time delta from previous displayed frame field) is 0.028715388 seconds, which is 28.71 ms. This time is called round trip time.

```
kubik@terminator ~/l/networking (master)> ping google.com
PING google.com (216.58.211.238) 56(84) bytes of data:
64 bytes from mad01s24-in-f14.1e100.net (216.58.211.238): icmp_seq=1 ttl=55 time=28.7 ms
```

This round trip time value is consistent with the output of ping command.

Exercise 6. According to what we have seen in theory classes, Ethernet frames must have a minimum length of 64 bytes (46 bytes of data). On the other hand, Wireshark does not show the CRC field (it is processed by the NIC), so the length of the showed frame will be equal or greater than 60 bytes. Look for a 60 bytes size frame (define the filter: `frame.len == 60`). What is the mechanism used to fulfil the length limit constraint if the size of the data to be transmitted is lower than 46 bytes?

[illegible]

We can see, that the rest of the Ethernet frame is padded by zeros.

Exercise 7. What is the mechanism used for the authentication in the traffic captured? What are the frames that negotiate the use of this field?

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
8	0.336824	20:28:18:a0:a9:d2	Unispher_a4:10:be	PPP LCP	40	Configuration Ack
9	0.337124	20:28:18:a0:a9:d2	Unispher_a4:10:be	PPP LCP	30	Echo Request
10	0.337184	20:28:18:a0:a9:d2	Unispher_a4:10:be	PPP PAP	46	Authenticate-Request (Peer-ID='aliceadsl', Password='aliceadsl')
11	0.357605	Unispher_a4:10:be	20:28:18:a0:a9:d2	PPP LCP	60	Echo Reply
12	0.513587	Unispher_a4:10:be	20:28:18:a0:a9:d2	PPP PAP	60	Authenticate-Ack (Message='')
13	0.514567	20:28:18:a0:a9:d2	Unispher_a4:10:be	PPP IP...	44	Configuration Request
14	0.514647	20:28:18:a0:a9:d2	Unispher_a4:10:be	PPP IP...	36	Configuration Request
15	0.535927	Unispher_a4:10:be	20:28:18:a0:a9:d2	PPP IP...	60	Configuration Nak
16	0.536027	20:28:18:a0:a9:d2	Unispher_a4:10:be	PPP IP...	44	Configuration Request
17	0.536187	Unispher_a4:10:be	20:28:18:a0:a9:d2	PPP LCP	60	Protocol Reject
18	0.556887	Unispher_a4:10:be	20:28:18:a0:a9:d2	PPP IP...	60	Configuration Ack
19	0.712300	Unispher_a4:10:be	20:28:18:a0:a9:d2	PPP IP...	60	Configuration Request

▶ Frame 10: 46 bytes on wire (368 bits), 46 bytes captured (368 bits)

▶ Ethernet II, Src: 20:28:18:a0:a9:d2 (20:28:18:a0:a9:d2), Dst: Unispher_a4:10:be (00:90:1a:a4:10:be)

▼ PPP-over-Ethernet Session

0001 = Version: 1

.... 0001 = Type: 1

Code: Session Data (0x00)

Session ID: 0x18b2

Payload Length: 26

▼ Point-to-Point Protocol

Protocol: Password Authentication Protocol (0xc023)

▼ PPP Password Authentication Protocol

Code: Authenticate-Request (1)

Identifier: 1

Length: 24

▼ Data

Peer-ID-Length: 9

Peer-ID: aliceadsl

Password-Length: 9

Password: aliceadsl

PPP uses Password Authentication Protocol (PAP) for client authentication. We can see 2 PAP frames.

- 1) PAP Authenticate-Request with Peer-ID: aliceadsl and Password: aliceadsl
- 2) Server response PAP frame - Authenticate Acknowledgement

Exercise 8. In the trace, it is possible to see the process that corresponds to the phases of establishing, authenticating and networking. Take screenshots of frames that corresponds to these phases indicating the phase that correspond in each case. What is the protocol at the network level that will be used to transmit the data?

Establishing PPP connection:

5	0.133822	20:28:18:a0:a9:d2	Unispher_a4:10:be	PPP LCP	36 Configuration Request
6	0.336644	Unispher_a4:10:be	20:28:18:a0:a9:d2	PPP LCP	60 Configuration Request
7	0.336664	Unispher_a4:10:be	20:28:18:a0:a9:d2	PPP LCP	60 Configuration Ack
8	0.336824	20:28:18:a0:a9:d2	Unispher_a4:10:be	PPP LCP	40 Configuration Ack

PPP Authentication:

Time	Source	Destination	Protocol	Length	Message
10	0.337184	20:28:18:a0:a9:d2	Unispher_a4:10:be	PPP PAP	46 Authenticate-Request (Peer-ID='aliceadsl', Password='aliceadsl')
12	0.513587	Unispher_a4:10:be	20:28:18:a0:a9:d2	PPP PAP	60 Authenticate-Ack (Message='')

Networking:

In the traffic captured, we can see only configuration of IPv4 protocol over PPP, there is no useful IPv4 traffic encapsulated.

Here are the frames that correspond to configuration of IPv4 addresses and client primary and secondary DNS servers.

13	0.514567	20:28:18:a0:a9:d2	Unispher_a4:10:be	PPP IPCP	44 Configuration Request
14	0.514647	20:28:18:a0:a9:d2	Unispher_a4:10:be	PPP IPV6CP	36 Configuration Request
15	0.535927	Unispher_a4:10:be	20:28:18:a0:a9:d2	PPP IPCP	60 Configuration Nak
16	0.536027	20:28:18:a0:a9:d2	Unispher_a4:10:be	PPP IPCP	44 Configuration Request
17	0.536187	Unispher_a4:10:be	20:28:18:a0:a9:d2	PPP LCP	60 Protocol Reject
18	0.556887	Unispher_a4:10:be	20:28:18:a0:a9:d2	PPP IPCP	60 Configuration Ack
19	0.716309	Unispher_a4:10:be	20:28:18:a0:a9:d2	PPP IPCP	60 Configuration Request
20	0.716449	20:28:18:a0:a9:d2	Unispher_a4:10:be	PPP IPCP	32 Configuration Ack

Code: Session Data (0x00)					
Session ID: 0x18b2					
Payload Length: 24					
▼ Point-to-Point Protocol					
Protocol: Internet Protocol Control Protocol (0x8021)					
▼ PPP IP Control Protocol					
Code: Configuration Ack (2)					
Identifier: 2 (0x02)					
Length: 22					
▼ Options: (18 bytes), IP Address, Primary DNS Server IP Address, Secondary DNS Server IP Address					
▼ IP Address					
Type: IP Address (3)					
Length: 6					
IP Address: 79.51.70.114					
▼ Primary DNS Server IP Address					
Type: Primary DNS Server IP Address (129)					
Length: 6					
Primary DNS Address: 85.37.17.41					
▼ Secondary DNS Server IP Address					
Type: Secondary DNS Server IP Address (131)					
Length: 6					
Secondary DNS Address: 85.38.28.83					

Exercise 9. Develop a program in Java that list all the network interfaces of our computer that have a MAC address assigned using the **NetworkInterface** class. In addition, the program should provide the following information about the interface: short name of the interface, MAC, if the MAC is globally or locally managed and if the interface is up and running. The output should be as follows:

```
wlan1: 68:07:15:1F:99:A2 - global - (down) .  
wlan2: 6A:07:15:1F:99:A1 - local - (up) .  
eth2: D8:CB:8A:F5:8B:4E - global - (up) .  
wlan3: 68:07:15:1F:99:A1 - global - (down) .
```

The code is self-explanatory, with the help of some comments.

Guidelines of the report

- It is recommended the use of the provided Word template.
- Include in the same report all the exercises corresponding to Part 1 (exercises 1, 2 and 3).
- The front page must inform about: (i) list of the exercises included; (ii) data that identifies the student (i.e. name, group, etc). Please **use the template** provided in the Campus Virtual
- Start each exercise on a separate page.
- For each exercise include both the statement of the exercise as well as the solution. Define custom styles for the different parts of the document (e.g. title, statement, solution, etc.)
- In the screenshots (using <alt>+<impr pant>) the student must mark those parts corresponding to what is requested by the exercise (using a drawing utility). Also add a brief text explaining what is shown.
- The student must upload the report in PDF.
- Upload a .zip file with the report and the file .pcap with the trace of the captured packets.
- The report should include an explicative schema detailing the most significant parts of the code. You must deliver the source code (in independent files) jointly with the report.