Practical Exercises 1

Surname: Hejhal **Name**: Jakub

Degree (Ing. del Software/Ing. Informática/Ing. Computadores): Erasmsus 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.
                     Source
                                         Destination
                                                             Protocol Length Info
     478 41.665485548 192.168.0.232
                                         239.255.255.250
                                                             SSDP
                                                                       167 M-SEARCH * HTTP/1.1
                                                             IGMPv3
     495 45.352043999 192.168.0.1
                                         224.0.0.1
                                                                       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
                                                                      216 M-SEARCH * HTTP/1.1
                                        239.255.255.250
                                                             SSDP
     831 63.681738109 192.168.0.32
                                        239.255.255.250
                                                             SSDP
                                                                      216 M-SEARCH * HTTP/1.1
                                                                       216 M-SEARCH * HTTP/1.1
     844 64.706241400 192.168.0.32
                                         239.255.255.250
                                                             SSDP
    4452 151.952388662 192.168.0.232
                                                                      167 M-SEARCH * HTTP/1.1
                                         239.255.255.250
                                                             SSDP
                                                             IGMPv3 60 Membership 400.,...
SSDP 216 M-SEARCH * HTTP/1.1
    5053 170.793873283 192.168.0.1
                                         224.0.0.1
                                                                        60 Membership Query, general
    6358 181.646758366 192.168.0.32
                                         239.255.255.250
                                                                   216 M-SEARCH * HTTP/1.1
    6390 182.672514431 192.168.0.32
                                         239.255.255.250
                                                                  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
    60 Who has 192.168.0.17
    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
                                                                       167 M-SEARCH * HTTP/1.1
                                                             SSDP
                                         239.255.255.250
    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
                                                                       216 M-SEARCH * HTTP/1.1
    9539 302.683965067 192.168.0.32
                                         239.255.255.250
                                                             SSDP
    9557 303.708057032 192.168.0.32
                                                                      216 M-SEARCH * HTTP/1.1
                                        239.255.255.250
                                                             SSDP
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)
   Destination: Broadcast (ff:ff:ff:ff:ff:ff)
       Address: Broadcast (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
```

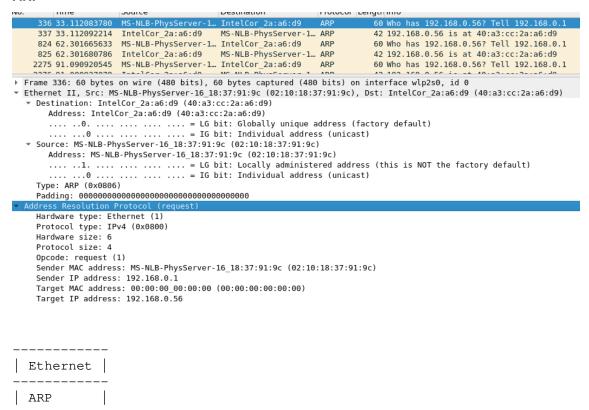
I receive a lot of different frames, whose destination and source MAC is different from mine. The previous screenshot shows ARP request from my phone on the same WIFI. It's destination MAC is Broadcast, so it makes sense I receive this frame.

lo.	Time	Source	Destination	Protocol L	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		
L	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		239.255.255.250	SSDP	216 M-SEARCH * HTTP/1.1		
	0000 204 620000422		220 255 255 250	CCDD	DIC M CEADOU * UTTD/1 1		
	•	-) on interface wlp2s0, id 0		
		_	-	IPV4mcast	_7f:ff:fa (01:00:5e:7f:ff:fa)		
1		mcast_7f:ff:fa (01:00					
		cast_7f:ff:fa (01:00:5					
		= LG b	, ,		,		
		= IG b	•	ilticast/b	roadcast)		
1		38:13:a7 (f0:03:8c:38					
		Nav_38:13:a7 (f0:03:8d					
		= LG b			•		
		= IG b	oit: Individual addres	ss (unicas	t)		
Type: IPv4 (0x0800)							
_	Internet Protocol Version 4, Src: 192.168.0.32, Dst: 239.255.255.250						
		ol, Src Port: 53963,	•	233.230			

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 adddress.

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



ICMP

Ä	icmp										
ο.		Source	Destination		Length Info						
	1 0.000000000	93.173.138.108	192.168.0.56	ICMP				ble (Host u			
-	40 3.700941723	192.168.0.56	172.217.17.14	ICMP							(reply in 41)
	41 3.730489631	172.217.17.14	192.168.0.56	ICMP	98 Echo ((request in 40)
2	48 4.701458634	192.168.0.56	172.217.17.14	ICMP							(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)
			, 98 bytes captured (7								
			40:a3:cc:2a:a6:d9), Ds		hysServer-16	_18:37	:91:9c (6	92:10:18:37:	91:9c)		
			8:37:91:9c (02:10:18:								
			:37:91:9c (02:10:18:3 LG bit: Locally admin:		(*bi- i-	NOT +	h- f+-				
			IG bit: Individual ad			NOT C	ne racto	y deraditi)			
		2a:a6:d9 (40:a3:co		iless (unitca	31)						
		_2a.ao.do (40.ao.ee lCor 2a:a6:d9 (40:a									
			LG bit: Globally uniq	io addross (factory defai	u1+)					
			IG bit: Individual ad			ucc,					
	Type: IPv4 (0x08		10 DIC. Individual da	aress (united	50,						
			.168.0.56, Dst: 172.21	17.17.14							
	0100 = Vers		,								
	0101 = Head	er Length: 20 bytes	(5)								
	Differentiated S	ervices Field: 0x00	(DSCP: CS0, ECN: Not	-ECT)							
	Total Length: 84										
	Identification:	0xbf24 (48932)									
	▶ Flags: 0x4000, D	on't fragment									
	Fragment offset:	Θ									
	Time to live: 64										
	Protocol: ICMP (1)									
		0xfcbc [validation									
	[Header checksum	status: Unverified	1]								
	Source: 192.168.										
	Destination: 172										
	Internet Control Me										
	Type: 8 (Echo (p	ing) request)									
	Code: 0										
	Checksum: 0xebe2										
	[Checksum Status										
	Identifier (BE):										
	Identifier (LE):										
	Sequence number	(LE): 512 (0x0200)									
	[Response frame:										
			020 22:39:20.00000000	A CEST							
			e): 0.953821252 second								
	Data (48 bytes)	Temp data (recalive	.,. 0.955621252 Second	21							

DNS

	ins				
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
г	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		192.168.0.56	DNS	91 Standard query response OxffcO A play.google.com A 216.58.211
4	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		192.168.0.56	DNS	91 Standard query response 0xc323 A play.google.com A 216.58.211
	2146 85.695875392		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.techn
	2413 97.372960065		192.168.0.1	DNS	66 Standard query 0xd380 A target
	2414 97.372978759		192.168.0.1	DNS	66 Standard query 0x7581 AAAA target
	2415 97.381872397		192.168.0.56	DNS	66 Standard query response 0xd380 A target
	2410 07 201072007		75 1 100 0 50	DAIC .	CC Chandrad
					on interface wlp2s0, id 0
					hysServer-16_18:37:91:9c (02:10:18:37:91:9c)
'			37:91:9c (02:10:18:37:		
			:91:9c (02:10:18:37:9		(this is NOT the factors defeath)
					ess (this is NOT the factory default)
			bit: Individual addre	ss (unica	St)
,		2a:a6:d9 (40:a3:cc:2a			
		Cor_2a:a6:d9 (40:a3:c			5
			bit: Globally unique		
			bit: Individual addre	ss (unica	ST)
	Type: IPv4 (0x080		0.0.56 0-+- 100		
			8.0.56, Dst: 192.168.0	9.1	
		ol, Src Port: 36784,	DST PORT: 53		
► D	omain Name System (query)			

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

HTTP

_						
, I	nttp					
No.		Time	Source	Destination	Protocol L	ength Info
	317	6 28.393651968	212.145.41.179	192.168.0.56	0CSP	979 Response
+	383	1 29.773844627	192.168.0.56	77.75.75.173	HTTP	485 GET / HTTP/1.1
4	385	7 29.842603517	77.75.75.173	192.168.0.56	HTTP	415 HTTP/1.1 301 Moved Permanently (text/html)
		7 30.028076081		212.145.41.179	0CSP	449 Request
			212 1/15 //1 170	102 168 A 56	ncsp	070 Reconned
						s) on interface wlp2s0, id 0
						ysServer-16_18:37:91:9c (02:10:18:37:91:9c)
,	r De		ILB-PhysServer-16_18:3			
			B-PhysServer-16_18:37			
						ss (this is NOT the factory default)
			= IG		ss (unicas	t)
	50		_2a:a6:d9 (40:a3:cc:2a Cor 2a:a6:d9 (40:a3:c			
			LG l		addross (f	actory default)
			= IG i			
	Tv	pe: IPv4 (0x080		DIC. INGIVIGUAL AUGIE	33 (united)	· ·
v 1			ersion 4, Src: 192.168	3.0.56. Dst: 77.75.75	. 173	
		00 = Versi		,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,		
		0101 = Heade	er Length: 20 bytes (5)		
			rvices Field: 0x00 (D		T)	
	To	tal Length: 471	L			
	Id	entification: 0)x3f64 (16228)			
	Fl:	ags: 0x4000, Do	on't fragment			
		agment offset:	0			
		me to live: 64				
		otocol: TCP (6)				
			0x9fe4 [validation di	sabled]		
			status: Unverified]			
		urce: 192.168.0				
. 19		stination: 77.7				1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
			l Protocol, Src Port:	54894, DST Port: 80,	Seq: 1, A	CK: 1, Len: 419
		text Transfer F T / HTTP/1.1\r\				
		st: novinky.cz\				
			la/5.0 (X11; Linux x8	6 64: rv:74 0) Gecko	/20100101 6	irefox/74 A\r\n
			.application/xhtml+xm			
			en-US,en;q=0.5\r\n	re, appered error, xiire, q=0	7. 5, 1mage, w	(CDP) / /q=0.0(1 (II
			gzip, deflate\r\n			
		nnection: keep-				
				; qfp 64b=hoEnYvMLb	xFAi28cSs1	.12pgZd25FsS k3ca7brscPAn.K7\r\n
			Requests: 1\r\n			
	\r					
	[F	ull request URI	<pre>[: http://novinky.cz/]</pre>			
	[H	TTP request 1/1	1]			
	[R	esponse in fram	ie: 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

HTTP

```
Figure 602. 401 bytes of Fithernet II, Src: Intel

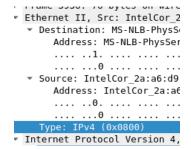
Destination: MS-NLB-
Address: MS-NLB-Pl
.....0

Source: IntelCor_2a:
Address: IntelCor
....0
....0

Type: IPv4 (0x0800)
```

ICMP

DNS

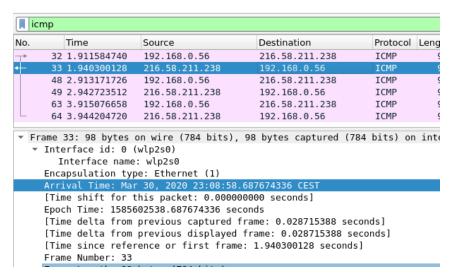


EtherType is a two-octet field in an Ethernet frame. It is used to indicate which protocol is encapsulated in the payload of the frame. ICMP, HTTP and DNS have the same EtherType field, because all of those protocols use IPv4 protocol at network OSI layer.

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?

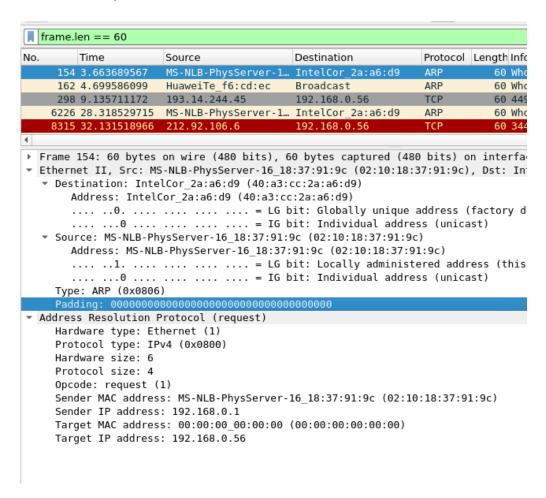


Time difference between ICMP request and ICMP response frames (Time delta from previous displayed frame field) is 0.028715388 seconds, which is 28.71 ms. This time is called round trip time.

```
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
```

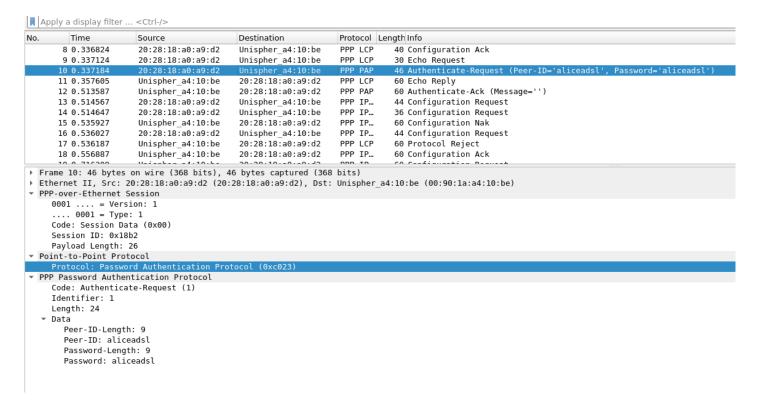
This round trip time value is consistent with the output of ping command.

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?



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?



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 stablishing, 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:

		Dounce	Describer		zenga mo
- 7	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.