

Práctica 1

Apellidos: López Pérez

Nombre: Marta

Titulación: Grado de Ingeniería del Informática

Grupo: A

PC de la práctica: PC709

- 1.- Lea el enunciado de la práctica para obtener la traza de Wireshark necesaria para responder las siguientes preguntas
- 2.- Lea atentamente las notas al final del enunciado de la práctica (recuerde en guardar la traza – fichero p1.pcapng – y tomar capturas de pantallas justificando de dónde obtuvo las respuestas)
- 3.- No olvide rellenar arriba el equipo en el que realizó las prácticas (en el que capturó el tráfico)
- 4.- En la memoria entregada, puede borrar este cuadro

Ejercicio 1. Elija un mensaje dns, y localice en la cabecera Ethernet II la siguiente información (haga capturas de pantalla donde aparezcan estos datos):

- Número de trama elegida:
- Información de la dirección MAC de su computadora.
Dirección MAC (en hexadecimal): 40:a8:f0:55:12:10
Fabricante de NIC (en hexadecimal): 40:a8:f0 nombre: Hewlett Packard
Número de serie de NIC (en hexadecimal): 55:12:10
- Información de la dirección MAC de *gateway/router*.
Dirección MAC (en hexadecimal): c4:b3:6a:0a:2e:75
Fabricante de NIC (en hexadecimal): c4:b3:6a nombre: Cisco Systems, Inc
Número de serie de NIC (en hexadecimal): 0a:2e:75

The screenshot shows a Wireshark capture of a DNS query. The packet list on the left shows a DNS query from 192.168.166.9 to 150.214.57.7. The packet details on the right show the Ethernet II header with Source MAC 40:a8:f0:55:12:10 and Destination MAC c4:b3:6a:0a:2e:75. The packet bytes at the bottom show the hexadecimal representation of the Ethernet II header and the start of the IP packet.

No.	Time	Source	Destination	Protocol	Length	Info
782	25.988860	192.168.166.9	150.214.57.7	DNS	84	Standard query
783	25.989442	150.214.57.7	192.168.166.9	DNS	541	Standard query
926	30.776282	192.168.166.9	150.214.57.7	DNS	74	Standard query
927	30.776838	150.214.57.7	192.168.166.9	DNS	547	Standard query
1262	42.561676	192.168.166.9	150.214.57.7	DNS	76	Standard query
1263	42.562029	150.214.57.7	192.168.166.9	DNS	302	Standard query
1389	47.060820	192.168.166.9	150.214.57.7	DNS	84	Standard query
1391	47.061292	150.214.57.7	192.168.166.9	DNS	541	Standard query
1778	64.659361	192.168.166.9	150.214.57.7	DNS	83	Standard query
1779	64.659838	150.214.57.7	192.168.166.9	DNS	217	Standard query
2675	110.127874	192.168.166.9	150.214.57.7	DNS	84	Standard query
2676	110.128439	150.214.57.7	192.168.166.9	DNS	541	Standard query
3425	140.923652	192.168.166.9	150.214.57.7	DNS	81	Standard query
3426	140.924071	150.214.57.7	192.168.166.9	DNS	291	Standard query
4095	166.699807	192.168.166.9	150.214.57.7	DNS	81	Standard query
4096	166.700169	150.214.57.7	192.168.166.9	DNS	291	Standard query
4345	172.542706	192.168.166.9	150.214.57.7	DNS	76	Standard query
4346	172.543074	150.214.57.7	192.168.166.9	DNS	302	Standard query
4352	172.572447	192.168.166.9	150.214.57.7	DNS	76	Standard query
4353	172.572733	150.214.57.7	192.168.166.9	DNS	128	Standard query
4615	182.157895	192.168.166.9	150.214.57.7	DNS	80	Standard query
4616	182.158251	150.214.57.7	192.168.166.9	DNS	265	Standard query
4625	182.179384	192.168.166.9	150.214.57.7	DNS	80	Standard query
4626	182.179682	150.214.57.7	192.168.166.9	DNS	135	Standard query
4633	182.210349	192.168.166.9	150.214.57.7	DNS	76	Standard query

Frame 4095: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface 0

Ethernet II, Src: HewlettP_55:12:10 (40:a8:f0:55:12:10), Dst: Cisco_0a:2e:75 (c4:b3:6a:0a:2e:75)

Destination: Cisco_0a:2e:75 (c4:b3:6a:0a:2e:75)

Address: Cisco_0a:2e:75 (c4:b3:6a:0a:2e:75)

.....0. = LG bit: Globally unique address (factory default)

.....0. = IG bit: Individual address (unicast)

Source: HewlettP_55:12:10 (40:a8:f0:55:12:10)

Address: HewlettP_55:12:10 (40:a8:f0:55:12:10)

.....0. = LG bit: Globally unique address (factory default)

.....0. = IG bit: Individual address (unicast)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 192.168.166.9, Dst: 150.214.57.7

User Datagram Protocol, Src Port: 54394, Dst Port: 53

Domain Name System (query)

0000 c4 b3 6a 0a 2e 75 40 a8 f0 55 12 10 08 00 45 00 ..j..u@. .U....E-

0010 00 43 10 59 00 00 80 11 00 00 c0 a8 a6 09 96 d6 .C.Y.....

0020 39 07 d4 7a 00 35 00 2f 36 d0 9b 1d 01 00 00 01 9..z.5./ 6.....

0030 00 00 00 00 00 00 0b 69 6e 66 6f 72 6d 61 74 69i nformati

0040 63 61 02 63 76 03 75 6d 61 02 65 73 00 00 01 00 ca.cv.um a.es....

0050 01 .

Ejercicio 2. Indique qué filtro debe añadir para que se muestren las tramas donde no se utilice su dirección MAC.

- ¿Qué filtro has utilizado? `eth.src ne 40:a8:f0:55:12:10 and eth.dst ne 40:a8:f0:55:12:10`
- ¿Cuántas tramas recibe? 5041 de 6844
- ¿Por qué recibe esas tramas? (Para responder esta pregunta, observe las características de las direcciones MAC destino de esas tramas)
 - Porque hay tramas de tipo broadcast (`ff:ff:ff:ff:ff:ff`) y `IPv4mcast_7f:ff:fa`.

The image shows a Wireshark packet capture interface. At the top, a filter is applied: `eth.src ne 40:a8:f0:55:12:10 and eth.dst ne 40:a8:f0:55:12:10`. The packet list shows several SSDP and ARP packets. Packet 915 is selected, showing details for Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol. The Ethernet II section shows the destination as `IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)` and the source as `Micro-St_c7:c4:97 (40:61:86:c7:c4:97)`. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
904	30.193444	192.168.166.58	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
905	30.194232	192.168.209.157	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
906	30.241007	192.168.164.206	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
907	30.245896	Vmware_9a:ec:cb	Broadcast	ARP	60	Who has 192.168.164.85? Tell 192.168.167.201
908	30.322021	172.17.30.116	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
909	30.339514	fe80::6195:948c:a89...	ff02::1:3	LLMNR	86	Standard query 0x67cd ANY pc0305
910	30.339797	192.168.164.85	224.0.0.252	LLMNR	66	Standard query 0x67cd ANY pc0305
911	30.369967	150.214.239.210	239.255.255.250	SSDP	259	NOTIFY * HTTP/1.1
912	30.370291	150.214.239.210	239.255.255.250	SSDP	345	NOTIFY * HTTP/1.1
913	30.370292	150.214.239.210	239.255.255.250	SSDP	349	NOTIFY * HTTP/1.1
914	30.370293	150.214.239.210	239.255.255.250	SSDP	279	NOTIFY * HTTP/1.1
915	30.373049	192.168.164.85	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
918	30.490687	192.168.208.143	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1

Frame 915: 179 bytes on wire (1432 bits), 179 bytes captured (1432 bits) on interface \Device\NPF_{9BEE4EA5-203E-4E5A-9014-9C2EB5EA0CF3}, id 0

Ethernet II, Src: Micro-St_c7:c4:97 (40:61:86:c7:c4:97), 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: Micro-St_c7:c4:97 (40:61:86:c7:c4:97)

Address: Micro-St_c7:c4:97 (40:61:86:c7:c4:97)

....0. = LG bit: Globally unique address (factory default)

....0. = IG bit: Individual address (unicast)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 192.168.164.85, Dst: 239.255.255.250

0000 01 00 5e 7f ff fa 40 61 86 c7 c4 97 08 00 45 00 ..^...@aE.

0010 00 a5 65 42 00 00 04 11 fc 0d c0 a8 a4 55 ef ff ..eB....U..

0020 ff fa fd 02 07 6c 00 91 b3 46 4d 2d 53 45 41 52l..FM-SEAR

0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48 CH * HTTP/1.1..H

0040 6f 73 74 3a 20 32 33 39 2e 32 35 35 2e 32 35 35 ost: 239.255.255

0050 2e 32 35 30 3a 31 39 30 30 0d 0a 53 54 3a 20 75 .250:190 0..ST: u

0060 72 6e 3a 73 63 68 65 6d 61 73 2d 75 70 6e 70 2d rn:schem as-upnp-

0070 6f 72 67 3a 64 65 76 69 63 65 3a 49 6e 74 65 72 org:device:Inter

0080 6e 65 74 47 61 74 65 77 61 79 44 65 76 69 63 65 netGatewayDevice

0090 3a 31 0d 0a 4d 61 6e 3a 20 22 73 73 64 70 3a 64 :1..Man: "ssdp:d

p1.pcapng

Packets: 6844 · Displayed: 5041 (73.7%)

Ejercicio 3. Dibuje la torre de protocolos (tal como se ha visto en clase, es decir, en la parte inferior los protocolos de más bajo nivel) de un paquete ARP, uno ICMP, uno DNS y uno HTTP.

- Torre de protocolos de un paquete ARP (número de trama seleccionada: 195)
 - Frame 1562: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{9BEE4EA5-203E-4E5A-9014-9C2EB5EA0CF3}, id 0
 - Ethernet II, Src: Apple_cb:61:52 (0c:4d:e9:cb:61:52), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 - Address Resolution Protocol (request)

arp

No.	Time	Source	Destination	Protocol	Length	Info
1344	45.190492	Apple_f6:bb:71	Broadcast	ARP	60	Who has 192.168.166.201? Tell 192.168.164.166
1357	45.385746	HewlettP_55:1c:75	Broadcast	ARP	60	Who has 192.168.167.201? Tell 192.168.166.30
1363	45.853414	HewlettP_55:1c:82	Broadcast	ARP	60	Who has 192.168.167.202? Tell 192.168.166.19
1372	46.192532	Apple_f6:bb:71	Broadcast	ARP	60	Who has 192.168.166.201? Tell 192.168.164.166
1394	47.195360	Apple_f6:bb:71	Broadcast	ARP	60	Who has 192.168.166.201? Tell 192.168.164.166
1434	48.904588	HewlettP_49:b8:16	Broadcast	ARP	60	Who has 192.168.167.201? Tell 192.168.166.25
1485	51.163560	HewlettP_52:98:be	Broadcast	ARP	60	Who has 192.168.167.201? Tell 192.168.166.28
1492	51.380677	HewlettP_55:12:10	Cisco_0a:2e:75	ARP	42	Who has 192.168.167.254? Tell 192.168.166.9
1493	51.381045	Cisco_0a:2e:75	HewlettP_55:12:10	ARP	60	192.168.167.254 is at c4:b3:6a:0a:2e:75
1544	53.930769	HewlettP_52:98:b6	Broadcast	ARP	60	Who has 192.168.167.201? Tell 192.168.166.16
1562	54.862234	Apple_cb:61:52	Broadcast	ARP	60	Who has 192.168.166.201? Tell 192.168.164.185
1600	55.865043	Apple_cb:61:52	Broadcast	ARP	60	Who has 192.168.166.201? Tell 192.168.164.185
1601	55.869083	HewlettP_49:b8:16	Broadcast	ARP	60	Who has 192.168.167.254? Tell 192.168.166.25
1617	56.867412	Apple_cb:61:52	Broadcast	ARP	60	Who has 192.168.166.201? Tell 192.168.164.185
1654	59.121296	Vmware_9a:ec:cb	Broadcast	ARP	60	Who has 192.168.166.190? Tell 192.168.167.201
1670	59.691213	HewlettP_52:98:bc	Broadcast	ARP	60	Who has 192.168.167.201? Tell 192.168.166.1
1699	60.880220	HewlettP_55:12:10	Cisco_0a:2e:75	ARP	42	Who has 192.168.167.254? Tell 192.168.166.9
1700	60.880512	Cisco_0a:2e:75	HewlettP_55:12:10	ARP	60	192.168.167.254 is at c4:b3:6a:0a:2e:75
1789	65.370943	Vmware_9a:ec:cb	Broadcast	ARP	60	Who has 192.168.166.165? Tell 192.168.167.201

> Frame 1562: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{9BEE4EA5-203E-4E5A-9014-9C2EB5EA0CF3}, id 0
> Ethernet II, Src: Apple_cb:61:52 (0c:4d:e9:cb:61:52), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)

Offset	Hex	ASCII
0000	ff ff ff ff ff ff 0c 4d e9 cb 61 52 08 06 00 01M..aR....
0010	08 00 06 04 00 01 0c 4d e9 cb 61 52 c0 a8 a4 b9M..aR....
0020	00 00 00 00 00 00 c0 a8 a6 c9 00 00 00 00 00
0030	00 00 00 00 00 00 00 00 00 00 00 00 00 00

Address Resolution Protocol: Protocol

Packets: 6844 · Displayed: 195 (2.8%)

- Torre de protocolos de un paquete ICMP (número de trama seleccionada: 10)
 - Frame 565: 370 bytes on wire (2960 bits), 370 bytes captured (2960 bits) on interface \Device\NPF_{9BEE4EA5-203E-4E5A-9014-9C2EB5EA0CF3}, id 0
 - Ethernet II, Src: VMware_9a:ec:cb (00:50:56:9a:ec:cb), Dst: HewlettP_55:12:10 (40:a8:f0:55:12:10)
 - Internet Protocol Version 4, Src: 192.168.167.201, Dst: 192.168.166.9
 - Internet Control Message Protocol

icmp

Time	Source	Destination	Protocol	Length	Info
565	18.732450	192.168.167.201	192.168.166.9	ICMP	370 Destination unreachable (Host administratively prohibited)
3427	140.929578	192.168.166.9	150.214.54.249	ICMP	74 Echo (ping) request id=0x0001, seq=1/256, ttl=128 (reply in 3428)
3428	140.930187	150.214.54.249	192.168.166.9	ICMP	74 Echo (ping) reply id=0x0001, seq=1/256, ttl=61 (request in 3427)
3458	141.934707	192.168.166.9	150.214.54.249	ICMP	74 Echo (ping) request id=0x0001, seq=2/512, ttl=128 (reply in 3459)
3459	141.935647	150.214.54.249	192.168.166.9	ICMP	74 Echo (ping) reply id=0x0001, seq=2/512, ttl=61 (request in 3458)
3483	142.946522	192.168.166.9	150.214.54.249	ICMP	74 Echo (ping) request id=0x0001, seq=3/768, ttl=128 (reply in 3484)
3484	142.947178	150.214.54.249	192.168.166.9	ICMP	74 Echo (ping) reply id=0x0001, seq=3/768, ttl=61 (request in 3483)
3509	143.958864	192.168.166.9	150.214.54.249	ICMP	74 Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (reply in 3510)
3510	143.959528	150.214.54.249	192.168.166.9	ICMP	74 Echo (ping) reply id=0x0001, seq=4/1024, ttl=61 (request in 3509)
5220	189.168900	192.168.164.43	192.168.164.165	ICMP	74 Echo (ping) request id=0x0001, seq=60/15360, ttl=32 (no response found!)

> Frame 565: 370 bytes on wire (2960 bits), 370 bytes captured (2960 bits) on interface \Device\NPF_{9BEE4EA5-203E-4E5A-9014-9C2EB5EA0CF3}, id 0
 > Ethernet II, Src: VMware_9a:ec:cb (00:50:56:9a:ec:cb), Dst: HewlettP_55:12:10 (40:a8:f0:55:12:10)
 > Internet Protocol Version 4, Src: 192.168.167.201, Dst: 192.168.166.9
 > Internet Control Message Protocol

```

0000  40 a8 f0 55 12 10 00 50 56 9a ec cb 08 00 45 00  @..U...P V.....E.
0010  01 64 17 7e 00 00 40 01 92 f7 c0 a8 a7 c9 c0 a8  .d~...@.....
0020  a6 09 03 0a cd 5f 00 00 00 00 45 00 01 48 2e 59  ....E..H.Y
0030  00 00 80 11 3c 28 c0 a8 a6 09 c0 a8 a7 c9 00 44  ....<...D
0040  00 43 01 34 ce d9 01 01 06 00 48 11 02 02 00 00  .C.4....H....
0050  00 00 c0 a8 a6 09 00 00 00 00 00 00 00 00 00 00  ....
0060  00 00 40 a8 f0 55 12 10 00 00 00 00 00 00 00 00  ..@..U.....
0070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ....
0080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ....
0090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ....
  
```

Internet Control Message Protocol: Protocol

Packets: 6844 • Displayed: 10 (0.1%)

- Torre de protocolos de un paquete DNS (número de trama seleccionada: 28)
 - Frame 782: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{9BEE4EA5-203E-4E5A-9014-9C2EB5EA0CF3}, id 0
 - Ethernet II, Src: HewlettP_55:12:10 (40:a8:f0:55:12:10), Dst: Cisco_0a:2e:75 (c4:b3:6a:0a:2e:75)
 - Internet Protocol Version 4, Src: 192.168.166.9, Dst: 150.214.57.
 - User Datagram Protocol, Src Port: 53906, Dst Port: 53
 - Domain Name System (query)

The image shows a Wireshark packet capture analysis of a DNS query. The top section displays a list of packets, with packet 782 selected. The bottom section shows the packet details for the selected packet, highlighting the Domain Name System (query) protocol. The packet bytes section at the bottom shows the raw data of the packet, including the Ethernet II header, Internet Protocol Version 4 header, User Datagram Protocol header, and the Domain Name System query data.

No.	Time	Source	Destination	Protocol	Length	Info
782	25.988860	192.168.166.9	150.214.57.7	DNS	84	Standard query 0xe78d A sls.update.microsoft.com
783	25.989442	150.214.57.7	192.168.166.9	DNS	541	Standard query response 0xe78d A sls.update.microsoft.com CNAME sls.update.micr
926	30.776282	192.168.166.9	150.214.57.7	DNS	74	Standard query 0xa762 A login.live.com
927	30.776838	150.214.57.7	192.168.166.9	DNS	547	Standard query response 0xa762 A login.live.com CNAME login.msa.msidentity.com
1262	42.561676	192.168.166.9	150.214.57.7	DNS	76	Standard query 0xc348 A proxy.lcc.uma.es
1263	42.562029	150.214.57.7	192.168.166.9	DNS	302	Standard query response 0xc348 A proxy.lcc.uma.es A 192.168.167.202 NS simba.sa
1389	47.060820	192.168.166.9	150.214.57.7	DNS	84	Standard query 0x90d2 A sls.update.microsoft.com
1391	47.061292	150.214.57.7	192.168.166.9	DNS	541	Standard query response 0x90d2 A sls.update.microsoft.com CNAME sls.update.micr
1778	64.659361	192.168.166.9	150.214.57.7	DNS	83	Standard query 0xcdbc A www.msftconnecttest.com
1779	64.659838	150.214.57.7	192.168.166.9	DNS	217	Standard query response 0xcdbc A www.msftconnecttest.com CNAME v4ncsi.msedge.ne
2675	110.127874	192.168.166.9	150.214.57.7	DNS	84	Standard query 0x1f24 A sls.update.microsoft.com
2676	110.128439	150.214.57.7	192.168.166.9	DNS	541	Standard query response 0x1f24 A sls.update.microsoft.com CNAME sls.update.micr
3425	140.923652	192.168.166.9	150.214.57.7	DNS	81	Standard query 0x074a A informatica.cv.uma.es
3426	140.924071	150.214.57.7	192.168.166.9	DNS	291	Standard query response 0x074a A informatica.cv.uma.es CNAME frontalcv7.cv.uma.
4095	166.699807	192.168.166.9	150.214.57.7	DNS	81	Standard query 0x9b1d A informatica.cv.uma.es
4096	166.700169	150.214.57.7	192.168.166.9	DNS	291	Standard query response 0x9b1d A informatica.cv.uma.es CNAME frontalcv7.cv.uma.
4345	172.542706	192.168.166.9	150.214.57.7	DNS	76	Standard query 0x4d78 A proxy.lcc.uma.es

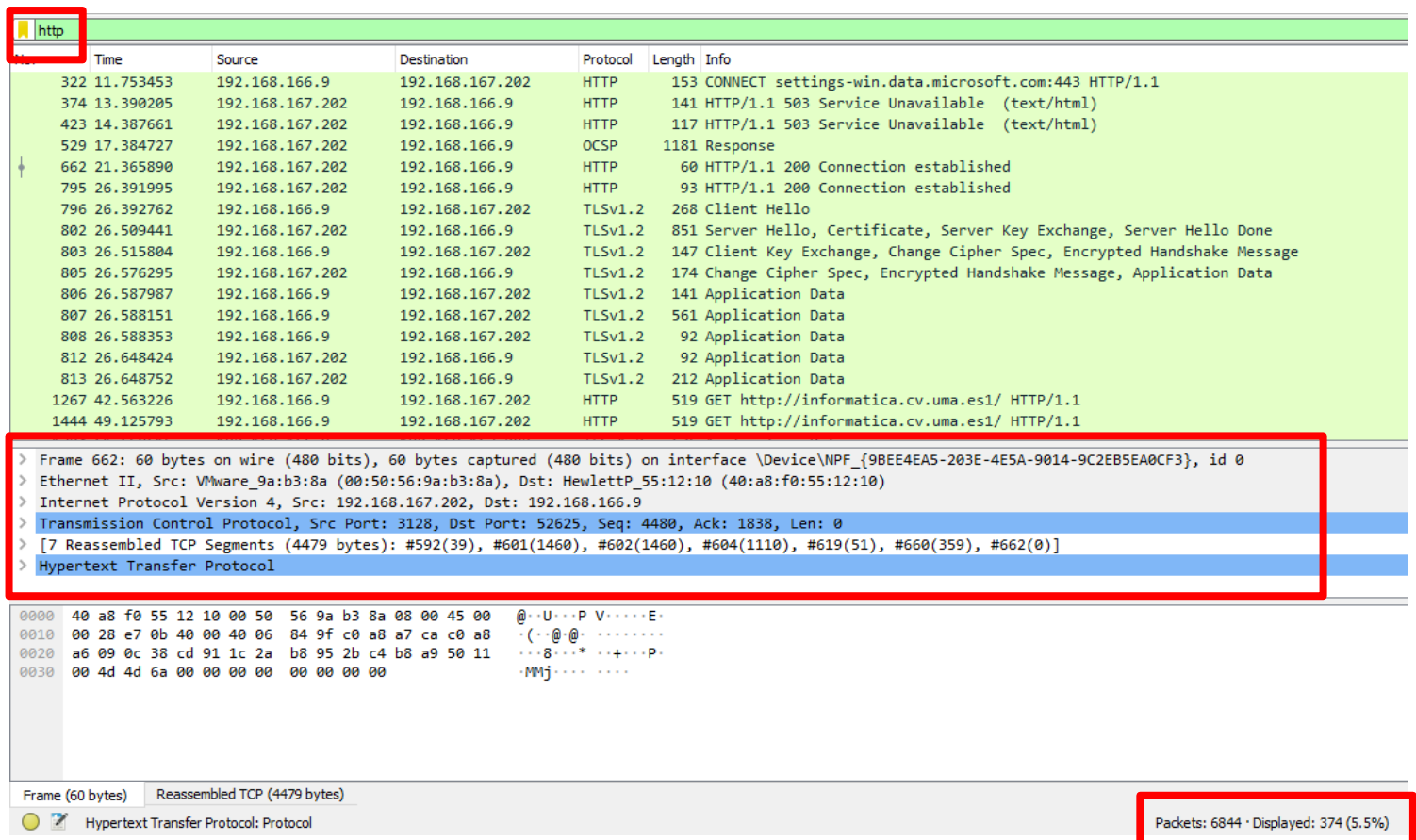
Frame 782: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{9BEE4EA5-203E-4E5A-9014-9C2EB5EA0CF3}, id 0
Ethernet II, Src: HewlettP_55:12:10 (40:a8:f0:55:12:10), Dst: Cisco_0a:2e:75 (c4:b3:6a:0a:2e:75)
Internet Protocol Version 4, Src: 192.168.166.9, Dst: 150.214.57.7
User Datagram Protocol, Src Port: 53906, Dst Port: 53
Domain Name System (query)

```
0000  c4 b3 6a 0a 2e 75 40 a8 f0 55 12 10 08 00 45 00  ..j..u@.  .U....E.
0010  00 46 10 52 00 00 80 11 00 00 c0 a8 a6 09 96 d6  .F.R....
0020  39 07 d2 92 00 35 00 32 36 d3 e7 8d 01 00 00 01  9....5.2 6.....
0030  00 00 00 00 00 00 03 73 6c 73 06 75 70 64 61 74  ....s ls updat
0040  65 09 6d 69 63 72 6f 73 6f 66 74 03 63 6f 6d 00  e.micros oft.com
0050  00 01 00 01  ....
```

Domain Name System: Protocol

Packets: 6844 · Displayed: 28 (0.4%)

- Torre de protocolos de un paquete HTTP (número de trama seleccionada: 374)
 - Frame 529: 1181 bytes on wire (9448 bits), 1181 bytes captured (9448 bits) on interface \Device\NPF_{9BEE4EA5-203E-4E5A-9014-9C2EB5EA0CF3}, id 0
 - Ethernet II, Src: VMware_9a:b3:8a (00:50:56:9a:b3:8a), Dst: HewlettP_55:12:10 (40:a8:f0:55:12:10)
 - Internet Protocol Version 4, Src: 192.168.167.202, Dst: 192.168.166.9
 - Transmission Control Protocol, Src Port: 3128, Dst Port: 52621, Seq: 1461, Ack: 1, Len: 1127
 - [2 Reassembled TCP Segments (2587 bytes): #528(1460), #529(1127)]
 - Hypertext Transfer Protocol
 - Online Certificate Status Protocol



http

No.	Time	Source	Destination	Protocol	Length	Info
322	11.753453	192.168.166.9	192.168.167.202	HTTP	153	CONNECT settings-win.data.microsoft.com:443 HTTP/1.1
374	13.390205	192.168.167.202	192.168.166.9	HTTP	141	HTTP/1.1 503 Service Unavailable (text/html)
423	14.387661	192.168.167.202	192.168.166.9	HTTP	117	HTTP/1.1 503 Service Unavailable (text/html)
529	17.384727	192.168.167.202	192.168.166.9	OCSP	1181	Response
662	21.365890	192.168.167.202	192.168.166.9	HTTP	60	HTTP/1.1 200 Connection established
795	26.391995	192.168.167.202	192.168.166.9	HTTP	93	HTTP/1.1 200 Connection established
796	26.392762	192.168.166.9	192.168.167.202	TLSv1.2	268	Client Hello
802	26.509441	192.168.167.202	192.168.166.9	TLSv1.2	851	Server Hello, Certificate, Server Key Exchange, Server Hello Done
803	26.515804	192.168.166.9	192.168.167.202	TLSv1.2	147	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
805	26.576295	192.168.167.202	192.168.166.9	TLSv1.2	174	Change Cipher Spec, Encrypted Handshake Message, Application Data
806	26.587987	192.168.166.9	192.168.167.202	TLSv1.2	141	Application Data
807	26.588151	192.168.166.9	192.168.167.202	TLSv1.2	561	Application Data
808	26.588353	192.168.166.9	192.168.167.202	TLSv1.2	92	Application Data
812	26.648424	192.168.167.202	192.168.166.9	TLSv1.2	92	Application Data
813	26.648752	192.168.167.202	192.168.166.9	TLSv1.2	212	Application Data
1267	42.563226	192.168.166.9	192.168.167.202	HTTP	519	GET http://informatica.cv.uma.es1/ HTTP/1.1
1444	49.125793	192.168.166.9	192.168.167.202	HTTP	519	GET http://informatica.cv.uma.es1/ HTTP/1.1

> Frame 662: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{9BEE4EA5-203E-4E5A-9014-9C2EB5EA0CF3}, id 0

> Ethernet II, Src: VMware_9a:b3:8a (00:50:56:9a:b3:8a), Dst: HewlettP_55:12:10 (40:a8:f0:55:12:10)

> Internet Protocol Version 4, Src: 192.168.167.202, Dst: 192.168.166.9

> Transmission Control Protocol, Src Port: 3128, Dst Port: 52625, Seq: 4480, Ack: 1838, Len: 0

> [7 Reassembled TCP Segments (4479 bytes): #592(39), #601(1460), #602(1460), #604(1110), #619(51), #660(359), #662(0)]

> Hypertext Transfer Protocol

0000 40 a8 f0 55 12 10 00 50 56 9a b3 8a 08 00 45 00 @..U...P V.....E.

0010 00 28 e7 0b 40 00 40 06 84 9f c0 a8 a7 ca c0 a8 .(..@. @.

0020 a6 09 0c 38 cd 91 1c 2a b8 95 2b c4 b8 a9 50 11 ...8...* ..+...P.

0030 00 4d 4d 6a 00 00 00 00 00 00 00 00 00 00 00 .MMj....

Frame (60 bytes) Reassembled TCP (4479 bytes)

Hypertext Transfer Protocol: Protocol

Packets: 6844 · Displayed: 374 (5.5%)

Ejercicio 4. Observe el campo **tipo** de la cabecera Ethernet II para cada uno de los mensajes anteriores.

Tipo en la cabecera Ethernet II		
	Hexadecimal	Texto
ARP	(0x0806)	ARP
HTTP	(0x0800)	IPv4
ICMP	(0x0800)	IPv4
DNS	(0x0800)	IPv4

arp			http			icmp			dns		
No.	Time	Source	No.	Time	Source	No.	Time	Source	No.	Time	Source
356	12.880584	Hewlett-Packard	322	11.753453	192.168.1.100	565	18.732450	192.168.1.100	782	25.988860	192.168.1.100
357	12.881075	Cisco	374	13.390205	192.168.1.100	3427	140.929578	192.168.1.100	783	25.989442	15.15.15.15
441	14.870906	Elis	423	14.387661	192.168.1.100	3428	140.930187	150.150.150.150	926	30.776282	192.168.1.100
459	15.246620	Hewlett-Packard	529	17.384727	192.168.1.100	3458	141.934707	192.168.1.100	927	30.776838	15.15.15.15
470	15.397349	Hewlett-Packard	662	21.365890	192.168.1.100	3459	141.935647	150.150.150.150	1262	42.561676	192.168.1.100
503	16.243514	Apple	795	26.391995	192.168.1.100	3483	142.946522	192.168.1.100	1263	42.562029	15.15.15.15
514	16.688866	Hewlett-Packard	796	26.392762	192.168.1.100	3484	142.947178	150.150.150.150	1389	47.060820	192.168.1.100
524	17.247566	Apple	802	26.509441	192.168.1.100	3509	143.958864	192.168.1.100	1391	47.061292	15.15.15.15
540	17.784286	Hewlett-Packard	803	26.515804	192.168.1.100	3510	143.959528	150.150.150.150	1778	64.659361	192.168.1.100
Frame 524: 60 bytes on wire (480 bits) captured on interface eth0			Frame 662: 60 bytes on wire (480 bits) captured on interface eth0			Frame 565: 370 bytes on wire (2960 bits) captured on interface eth0			Frame 782: 84 bytes on wire (672 bits) captured on interface eth0		
Ethernet II, Src: Apple_f6:ac:7b:64:2e:52, Dst: Broadcast			Ethernet II, Src: VMware_9a:b3:2d:1a:5a:00, Dst: Hewlett-Packard			Ethernet II, Src: VMware_9a:ec:8d:9d:1a:5a:00, Dst: Hewlett-Packard			Ethernet II, Src: Hewlett-Packard_08:00:27:00:00:00, Dst: Cisco_08:00:27:00:00:00		
Destination: Broadcast			Destination: Hewlett-Packard			Destination: Hewlett-Packard			Destination: Cisco_08:00:27:00:00:00		
.....1.....		0.....		0.....		0.....		
.....1.....		0.....		0.....		0.....		
Source: Apple_f6:ac:7b:64:2e:52			Source: VMware_9a:b3:2d:1a:5a:00			Source: VMware_9a:ec:8d:9d:1a:5a:00			Source: Hewlett-Packard_08:00:27:00:00:00		
Address: Apple_f6:ac:7b:64:2e:52			Address: VMware_9a:b3:2d:1a:5a:00			Address: VMware_9a:ec:8d:9d:1a:5a:00			Address: Hewlett-Packard_08:00:27:00:00:00		
.....0.....		0.....		0.....		0.....		
.....0.....		0.....		0.....		0.....		
Type: ARP (0x0806)			Type: IPv4 (0x0800)			Type: IPv4 (0x0800)			Type: IPv4 (0x0800)		

- ¿Qué significa este campo?
 - Define varios protocolos en la capa de red.
- ¿Por qué en tramas diferentes es igual?
 - ARP / IPv4 representa la forma en que se transmite, por lo que puede haber distintos tramas que lo transmitan de la misma de la misma forma.

Ejercicio 5. En Wireshark observe **la diferencia entre el tiempo** de la primera petición icmp (Echo (ping) request) y su respuesta (Echo (ping) reply).

- Números de las tramas seleccionadas:
 - 3427,3428
- ¿Cuánto tiempo es (en milisegundos)?
 - [Response time: 0,609 ms]
- ¿A qué concepto visto en la parte de teoría equivale dicho tiempo?
 - Round-trip time

The screenshot shows the Wireshark interface with the 'icmp' filter applied. The packet list displays several ICMP Echo (ping) requests and replies. The packet details pane for frame 3428 (Echo (ping) reply) is expanded, showing the response time as 0,609 ms.

No.	Time	Source	Destination	Protocol	Length	Info
565	18.732450	192.168.167.201	192.168.166.9	ICMP	370	Destination unreachable
3427	140.929578	192.168.166.9	150.214.54.249	ICMP	74	Echo (ping) request
3428	140.930187	150.214.54.249	192.168.166.9	ICMP	74	Echo (ping) reply
3458	141.934707	192.168.166.9	150.214.54.249	ICMP	74	Echo (ping) request
3459	141.935647	150.214.54.249	192.168.166.9	ICMP	74	Echo (ping) reply
3483	142.946522	192.168.166.9	150.214.54.249	ICMP	74	Echo (ping) request
3484	142.947178	150.214.54.249	192.168.166.9	ICMP	74	Echo (ping) reply
3509	143.958864	192.168.166.9	150.214.54.249	ICMP	74	Echo (ping) request
3510	143.959528	150.214.54.249	192.168.166.9	ICMP	74	Echo (ping) reply
5220	189.168900	192.168.164.43	192.168.164.165	ICMP	74	Echo (ping) request

Frame 3428: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF...

Ethernet II, Src: Cisco_0a:2e:75 (c4:b3:6a:0a:2e:75), Dst: HewlettP_55:12:10 (40:a8:f0:55:12:10)

Destination: HewlettP_55:12:10 (40:a8:f0:55:12:10)

Source: Cisco_0a:2e:75 (c4:b3:6a:0a:2e:75)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 150.214.54.249, Dst: 192.168.166.9

Internet Control Message Protocol

Type: 0 (Echo (ping) reply)

Code: 0

Checksum: 0x555a [correct]

[Checksum Status: Good]

Identifier (BE): 1 (0x0001)

Identifier (LE): 256 (0x0100)

Sequence number (BE): 1 (0x0001)

Sequence number (LE): 256 (0x0100)

[Request frame: 3427]

[Response time: 0,609 ms]

Ejercicio 6. Según la teoría vista en clase, las tramas Ethernet deben tener un **tamaño mínimo** de 64 bytes. Wireshark no muestra el campo FCS (ya que es tratado automáticamente por la tarjeta de red), por lo que la trama mostrada en Wireshark tendrá un tamaño de 60 bytes o más.

- Busque una trama con tamaño 60 (filtro: `frame.len == 60`), proporciona el número de trama. ¿Cuántas tramas tienen esta característica?
 - Trama número 3252, se capturan 470 tramas con ese filtro.
- ¿Qué mecanismo se utiliza para completar el tamaño si los datos transmitidos son más pequeños de 46 bytes)?
 - Padding.

The image shows a Wireshark packet capture analysis of an ARP request. The packet list at the top shows packet 3252 as an ARP request from 192.168.167.254 to the broadcast address. The packet details pane shows the Ethernet II header, ARP request type, and a padding field. The packet bytes pane shows the hexadecimal representation of the frame, with the ARP request structure clearly visible.

No.	Time	Source	Destination	Protocol	Length	Info
3199	131.572617	HewlettP_4e:b5:e5	Broadcast	ARP	60	Who has 192.168.1.1
3214	132.211174	192.168.167.254	224.0.0.1	IGMPv2	60	Membership Query
3236	133.445609	Cisco_e7:37:19	Spanning-tree-(for-...	STP	60	Conf. Root = 3
3250	134.105661	VMware_9a:ec:cb	Broadcast	ARP	60	Who has 192.168.1.1
3252	134.150189	HewlettP_55:12:45	Broadcast	ARP	60	Who has 192.168.1.1
3269	134.601294	VMware_9a:ec:cb	Broadcast	ARP	60	Who has 192.168.1.1
3290	135.437776	Cisco_e7:37:19	Spanning-tree-(for-...	STP	60	Conf. Root = 3
3310	136.342829	HewlettP_4e:b5:e5	Broadcast	ARP	60	Who has 192.168.1.1
3319	136.909489	HewlettP_4e:ac:3d	Broadcast	ARP	60	Who has 192.168.1.1

Frame 3252: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF{...}

Ethernet II, Src: HewlettP_55:12:45 (40:a8:f0:55:12:45), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Destination: Broadcast (ff:ff:ff:ff:ff:ff)

Source: HewlettP_55:12:45 (40:a8:f0:55:12:45)

Type: ARP (0x0806)

Padding: 00000000000000000000000000000000

Address Resolution Protocol (request)

Offset	Hex	ASCII
0000	ff ff ff ff ff 40 a8 f0 55 12 45 08 06 00 01@.U.E..
0010	08 00 06 04 00 01 40 a8 f0 55 12 45 c0 a8 a6 1f@.U.E..
0020	00 00 00 00 00 00 c0 a8 a7 fe 00 00 00 00 00 00
0030	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

p1.pcapng | Packets: 6844 | Displayed: 470 (6.9%)

Ejercicio 7. Analizando esas trazas,

- ¿qué mecanismo de autenticación se usa?
 - PAP (password authentication protocol)
- ¿En qué tramas (indique el número) se negocia la utilización de dicho campo?
 - Tramas 9 y 10

pap				
	Time	Source	Destination	Protocol
9	0.337184	20:28:18:a0:a9:d2	Unispher_a4:10:be	PPP PAP
10	0.513587	Unispher_a4:10:be	20:28:18:a0:a9:d2	PPP PAP

Ejercicio 8. En la traza se ve el proceso correspondiente a las fases de establecer, autenticar y red vista en los apuntes.

- Indique cada trama (sin considerar las que excluyeron en el primer párrafo de este paso) a qué fase corresponde.

No.	Time	Source	Destination	Protocol
11	0.514567	20:28:18:a0:a9:d2	Unispher_a4:10:be	PPP IPCP
13	0.535927	Unispher_a4:10:be	20:28:18:a0:a9:d2	PPP IPCP
14	0.536027	20:28:18:a0:a9:d2	Unispher_a4:10:be	PPP IPCP
16	0.556887	Unispher_a4:10:be	20:28:18:a0:a9:d2	PPP IPCP
17	0.716309	Unispher_a4:10:be	20:28:18:a0:a9:d2	PPP IPCP
18	0.716449	20:28:18:a0:a9:d2	Unispher_a4:10:be	PPP IPCP
12	0.514647	20:28:18:a0:a9:d2	Unispher_a4:10:be	PPP IPV6CP
5	0.133822	20:28:18:a0:a9:d2	Unispher_a4:10:be	PPP LCP
6	0.336644	Unispher_a4:10:be	20:28:18:a0:a9:d2	PPP LCP
7	0.336664	Unispher_a4:10:be	20:28:18:a0:a9:d2	PPP LCP
8	0.336824	20:28:18:a0:a9:d2	Unispher_a4:10:be	PPP LCP
15	0.536187	Unispher_a4:10:be	20:28:18:a0:a9:d2	PPP LCP
9	0.337184	20:28:18:a0:a9:d2	Unispher_a4:10:be	PPP PAP
10	0.513587	Unispher_a4:10:be	20:28:18:a0:a9:d2	PPP PAP
1	0.000000	20:28:18:a0:a9:d2	Broadcast	PPPoED
2	0.024960	Unispher_a4:10:be	20:28:18:a0:a9:d2	PPPoED
3	0.025060	20:28:18:a0:a9:d2	Unispher_a4:10:be	PPPoED
4	0.114162	Unispher_a4:10:be	20:28:18:a0:a9:d2	PPPoED

- ¿Qué protocolo del nivel de red se va a usar para transmitir los datos?
- Protocolo PPPoE.

No.	Time	Source	Des
3	0.025060	20:28:18:a0:a9:d2	Unispher_a4:10:be
4	0.114162	Unispher_a4:10:be	20:28:18:a0:a9:d2
5	0.133822	20:28:18:a0:a9:d2	Unispher_a4:10:be

<	
>	Frame 4: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▼	Ethernet II, Src: Unispher_a4:10:be (00:90:1a:a4:10:be), Dst: 20:28:18:a0:a9:d2 (20:28:18:a0:a9:d2)
>	Destination: 20:28:18:a0:a9:d2 (20:28:18:a0:a9:d2)
>	Source: Unispher_a4:10:be (00:90:1a:a4:10:be)
>	Type: PPPoE Discovery (0x8863)
>	PPP-over-Ethernet Discovery

Ejercicio 9. Desarrolle un código Java que usando la clase previa liste todos los interfaces de red activos mostrando su nombre y MAC.

- Incluya una captura de pantalla con la salida obtenida.

```
1 package pr1;
2
3 import java.net.NetworkInterface;
4 import java.net.SocketException;
5 import java.util.Enumeration;
6
7 public class InterfacesRed
8 {
9     public static void main(String[] args)
10    {
11        Enumeration<NetworkInterface> listaInterfaz;
12
13        try
14        {
15            listaInterfaz = NetworkInterface.getNetworkInterfaces();
16
17            while(listaInterfaz.hasMoreElements())
18            {
19                NetworkInterface interfaz = listaInterfaz.nextElement();
20                StringBuilder sb = new StringBuilder();
21
22                if(interfaz.isUp() && interfaz != null)
23                {
24                    byte[] dirMac=interfaz.getHardwareAddress();
25
26                    if(dirMac!=null)
27                    {
28                        int i = 0, longitud = dirMac.length;
29
30                        while(i < longitud)
31                        {
32                            if(i != (longitud - 1))
33                            {
34                                sb.append(String.format("%02X:", dirMac[i]));
35                            }
36                            else
37                            {
38                                sb.append(String.format("%02X", dirMac[i]));
39                            }
40
41                            i++;
42                        }
43                        System.out.println("Interfaz " + interfaz.getName()+ ": MAC = " + sb.toString());
44                    }
45                }
46            }
47        }
48        catch (SocketException se)
49        {
50            System.out.println(se.toString());
51        }
52    }
53 }
54
```

Console

terminated: InterfacesRed [Java Application] C:\Program Files\Java\jdk-12.0.2\bin\javaw.exe (9 may. 2020 16:54:14)

```
Interfaz eth4: MAC = 0A:00:27:00:00:0D
Interfaz wlan1: MAC = 84:EF:18:41:77:F6
```

- Explique el código.

Se crea una lista enumerada y la completamos con las distintas interfaces. Mientras la lista creada tenga elementos vamos a ir comprobando que el siguiente elemento no sea null y que esté activo. Si todo esto se cumple y existe una dirección mac para esa interfaz se va a ir agregando esta dirección byte a byte.

Por pantalla se va a mostrar el resultado en el formato

→ Interfaz *nombre*: MAC = *dirección mac*.

En caso que se encontrase algún error se mostraría también por pantalla gracias a que recogemos todo el código con el try y capturamos las excepciones que puedan aparecer.