

REDES Y SISTEMAS DISTRIBUIDOS

PRÁCTICAS BLQ 1

- PRÁCTICA 1**
- PRÁCTICA 2**
- PRÁCTICA 3**

MARTA LÓPEZ PÉREZ

INGENIERÍA INFORMÁTICA 2ºA

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 pane shows a list of packets, with packet 4095 selected. The packet details pane shows the structure of the selected packet, and the packet bytes pane shows the raw data in hexadecimal and ASCII.

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 69  ....i 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, and its details are expanded. 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 Internet Protocol Version 4 section shows the source as `192.168.164.85` and the destination as `239.255.255.250`. The packet bytes section 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 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, IP header, UDP header, and DNS 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

The image shows a Wireshark packet capture of an HTTP GET request. The top section displays a list of packets, with packet 374 selected. The packet details pane shows the following layers:

- 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

The packet bytes pane shows the raw data of the frame, which is a reassembled TCP segment. The bottom status bar indicates that the frame is 60 bytes and the reassembled TCP is 4479 bytes. The bottom right corner shows the packet count: 6844 packets, with 374 displayed (5.5%).

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

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

[illegible]

- ¿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 screenshot shows the Wireshark interface with packet 3252 selected. The packet list shows an ARP request from 192.168.1.104 to the broadcast address. The packet details pane shows the Ethernet II header and the ARP request. The hex data pane shows the raw bytes of the packet, with the ARP request structure highlighted.

No.	Time	Source	Destination	Protocol	Length	Info
3199	131.572617	HewlettP_4e:b5:e5	Broadcast	ARP	60	Who has 192.168.1.104
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 192.168.1.104
3252	134.150189	HewlettP_55:12:45	Broadcast	ARP	60	Who has 192.168.1.104
3269	134.601294	VMware_9a:ec:cb	Broadcast	ARP	60	Who has 192.168.1.104
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 192.168.1.104
3319	136.909489	HewlettP_4e:ac:3d	Broadcast	ARP	60	Who has 192.168.1.104

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
>	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.

Práctica 2

Apellidos: **López Pérez**

Nombre: **Marta**

Titulación: Grado de Ingeniería Informática

Grupo: **2ºA**

PC de la práctica: **PC CASA**

Lea el enunciado de la práctica para saber cómo generar el tráfico de cada ejercicio.

Ejercicio 1. Observe la cabecera IP de los diferentes datagramas:

- ¿Qué protocolo se indica en el campo “protocolo” en la cabecera de los datagramas que transportan mensajes ICMP, FTP y HTTP?

Protocolo	Valor Campo protocolo	Valor (HEX)	Número de trama
ICMP	ICMP (1)	01	34987
HTTP	TCP (6)	06	1557
FTP	TCP (6)	06	9761

No.	Time	Source	Destination
1463	2.978790	192.168.1.138	192.168.1.1
1469	2.982821	192.168.1.1	192.168.1.138
1478	2.988845	192.168.1.138	192.168.1.1
1482	2.993281	192.168.1.1	192.168.1.138
1486	2.995703	192.168.1.138	216.58.209.80
1493	3.021718	216.58.209.80	192.168.1.1
1557	3.284756	192.168.1.138	172.217.168.138
1599	3.361435	192.168.1.138	192.168.1.1
1655	3.462213	192.168.1.138	192.168.1.1
1711	3.562409	172.217.168.138	192.168.1.1

Ethernet II, Src: IntelCor_41:77:f6 (84:ef:18:41:77:f6), Dst: 02:00:0c:00:00:00, Protocol: 0x0800, Length: 60			
Internet Protocol Version 4, Src: 192.168.1.138, Destination: 172.217.168.138, TTL: 64, Protocol: 6, Length: 60			
TCP, Src Port: 443, Destination Port: 80, Seq: 3055446, Win: 65535, Len: 0			

No.	Time	Source	Destination
9620	19.652134	150.214.40.67	192.168.1.138
9624	19.652404	192.168.1.138	150.214.40.67
9664	19.707025	150.214.40.67	192.168.1.138
9666	19.707129	192.168.1.138	150.214.40.67
9697	19.762008	150.214.40.67	192.168.1.138
9736	19.817801	192.168.1.138	150.214.40.67
9761	19.874312	150.214.40.67	192.168.1.138
9790	19.931020	150.214.40.67	192.168.1.138
9792	19.931224	192.168.1.138	150.214.40.67
9831	19.987095	150.214.40.67	192.168.1.138

Frame 9761: 109 bytes on wire (872 bits), 109 bytes captured (872 bits) on interface 0, Ethernet II, Src: zte_ef:c3:79 (8c:e1:17:ef:c3:79), Dst: 02:00:0c:00:00:00, Protocol: 0x0800, Length: 109			
Internet Protocol Version 4, Src: 150.214.40.67, Destination: 192.168.1.138, TTL: 64, Protocol: 6, Length: 95			
TCP, Src Port: 80, Destination Port: 80, Seq: 9761, Win: 65535, Len: 0			

No.	Time	Source	Destination
34947	62.737703	192.168.1.138	150.214.54.249
34987	62.791901	150.214.54.249	192.168.1.138

Frame 34987: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0, Ethernet II, Src: zte_ef:c3:79 (8c:e1:17:ef:c3:79), Dst: 02:00:0c:00:00:00, Protocol: 0x0800, Length: 74			
Internet Protocol Version 4, Src: 150.214.54.249, Destination: 192.168.1.138, TTL: 64, Protocol: 1, Length: 60			
ICMP Echo (ping) Request, Seq: 32768, Len: 0			

- ¿Qué indica este campo?

El protocolo que se utiliza en cada trama.

```
Microsoft Windows [Versión 10.0.18362.778]
(c) 2019 Microsoft Corporation. Todos los derechos reservados.

C:\WINDOWS\system32>arp -d
C:\WINDOWS\system32>ipconfig /flushdns

Configuración IP de Windows

Se vació correctamente la caché de resolución de DNS.

C:\WINDOWS\system32>ping -n 1 informatica.cv.uma.es

Haciendo ping a frontalcv7.cv.uma.es [150.214.54.249] con 32 bytes de datos:
Respuesta desde 150.214.54.249: bytes=32 tiempo=54ms TTL=49

Estadísticas de ping para 150.214.54.249:
    Paquetes: enviados = 1, recibidos = 1, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 54ms, Máximo = 54ms, Media = 54ms

C:\WINDOWS\system32>
```

Ejercicio 2. Seleccione una petición de ICMP de su equipo (el mensaje *echo request*) y complete la siguiente tabla indicando la dirección IP destino (en la cabecera IP) y la dirección MAC destino (en la cabecera Ethernet). Repita el proceso con una petición FTP (en *Info* poner *request*).

	ICMP	FTP
Dirección IP destino (cab IP)	150.214.54.249	192.168.1.138
Dirección MAC destino (cab Ethernet)	8c:e1:17:ef:c3:79	84:ef:18:41:77:f6
Número de trama	34947	9790

No.	Time	Source	Destination	Protocol	Length	Info
34947	62.737703	192.168.1.138	150.214.54.249	ICMP	74	Echo (ping) request
34987	62.791901	150.214.54.249	192.168.1.138	ICMP	74	Echo (ping) response

Frame 34947: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF...
 Ethernet II, Src: IntelCor_41:77:f6 (84:ef:18:41:77:f6), Dst: zte_ef:c3:79 (8c:e1:17:ef:c3:79)
 Internet Protocol Version 4, Src: 192.168.1.138, Dst: 150.214.54.249
 Internet Control Message Protocol

No.	Time	Source	Destination	Protocol	Length	Info
9761	19.874312	150.214.40.67	192.168.1.138	FTP	109	Response: 200 OK
9790	19.931020	150.214.40.67	192.168.1.138	FTP	77	Response: 200 OK
9792	19.931224	192.168.1.138	150.214.40.67	FTP	60	Request: QUIT
9831	19.987095	150.214.40.67	192.168.1.138	FTP	68	Response: 200 OK

Frame 9790: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface \Device\NPF...
 Ethernet II, Src: zte_ef:c3:79 (8c:e1:17:ef:c3:79), Dst: IntelCor_41:77:f6 (84:ef:18:41:77:f6)
 Internet Protocol Version 4, Src: 150.214.40.67, Dst: 192.168.1.138
 Transmission Control Protocol, Src Port: 21, Dst Port: 58192, Seq: 1285, Ack: 91, Len: 23
 File Transfer Protocol (FTP)
 [Current working directory: /]

- ¿Por qué las direcciones MAC destino son iguales pero las direcciones IP destino no?

La dirección MAC es la dirección física del dispositivo y por eso no cambia, mientras que la dirección IP cambia dependiendo del protocolo, por eso es distinta.

```
C:\WINDOWS\system32>arp -d
C:\WINDOWS\system32>ipconfig /flushdns
Configuración IP de Windows
Se vació correctamente la caché de resolución de DNS.
C:\WINDOWS\system32>ping -n 1 informatica.cv.uma.es -l 1200
Haciendo ping a frontalcv7.cv.uma.es [150.214.54.249] con 1200 bytes de datos:
Respuesta desde 150.214.54.249: bytes=1200 tiempo=56ms TTL=49
Estadísticas de ping para 150.214.54.249:
    Paquetes: enviados = 1, recibidos = 1, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 56ms, Máximo = 56ms, Media = 56ms
C:\WINDOWS\system32>ping -n 1 informatica.cv.uma.es -l 3100
Haciendo ping a frontalcv7.cv.uma.es [150.214.54.249] con 3100 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Estadísticas de ping para 150.214.54.249:
    Paquetes: enviados = 1, recibidos = 0, perdidos = 1
    (100% perdidos),
```


Ejercicio 3. Responda las siguientes preguntas:

- ¿Cuál es el tipo de mensaje ICMP y su código (tanto para las peticiones como las respuestas)?

No.	Time	Source	Destination	Protocol	Length	Info
25192	49.395974	192.168.1.139	150.214.54.249	ICMP	1242	Echo (ping) request
25216	49.452333	150.214.54.249	192.168.1.139	ICMP	1242	Echo (ping) reply
28223	56.518672	192.168.1.139	150.214.54.249	ICMP	182	Echo (ping) request

> Frame 25192: 1242 bytes on wire (9936 bits), 1242 bytes captured (9936 bits) on interface \Device\NPF...
> Ethernet II, Src: IntelCor_41:77:f6 (84:ef:18:41:77:f6), Dst: zte_ef:c3:79 (8c:e1:17:ef:c3:79)
> Internet Protocol Version 4, Src: 192.168.1.139, Dst: 150.214.54.249
> Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0

No.	Time	Source	Destination	Protocol	Length	Info
25192	49.395974	192.168.1.139	150.214.54.249	ICMP	1242	Echo (ping) request
25216	49.452333	150.214.54.249	192.168.1.139	ICMP	1242	Echo (ping) reply
28223	56.518672	192.168.1.139	150.214.54.249	ICMP	182	Echo (ping) request

> Frame 25216: 1242 bytes on wire (9936 bits), 1242 bytes captured (9936 bits) on interface \Device\NPF...
> Ethernet II, Src: zte_ef:c3:79 (8c:e1:17:ef:c3:79), Dst: IntelCor_41:77:f6 (84:ef:18:41:77:f6)
> Internet Protocol Version 4, Src: 150.214.54.249, Dst: 192.168.1.139
> Internet Control Message Protocol
Type: 0 (Echo (ping) reply)
Code: 0

Para el resto de preguntas y rellenar la tabla considere solo las peticiones.

- ¿Qué filtro podría poner para que sólo aparezcan los fragmentos relacionados con un datagrama concreto?
ip.id == identificador
- Completa la siguiente tabla, indicando los flags que tiene activo cada fragmento, su identificador y su desplazamiento (para cada tamaño escribe un valor por cada fragmento, separados por comas (,) cuando hay varios fragmentos).

Tamaño	Número de tramas	Identificadores	Flags	Desplazamientos
1200	1	0xb057	0x0000	0
3100	3	0xb058	0x0172	2960

Time	Source	Destination
15532 31.971813	188.122.88.193	192.168.1.139
25192 49.395974	192.168.1.139	150.214.54.249

Frame 25192: 1242 bytes on wire (9936 bits), 1242 bytes captured (9936 bits) on interface \Device\NPF...
Ethernet II, Src: IntelCor_41:77:f6 (84:ef:18:41:77:f6), Dst: zte_ef:c3:79 (8c:e1:17:ef:c3:79)
Internet Protocol Version 4, Src: 192.168.1.139, Dst: 150.214.54.249
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not Set)
Total Length: 1228
Identification: 0xb057 (45143)
Flags: 0x0000
Fragment offset: 0
Time to live: 128
Protocol: ICMP (1)

Tamaño = 1200

Time	Source	Destination
15533 31.974794	188.122.88.193	192.168.1.139
28221 56.518671	192.168.1.139	150.214.54.249
28222 56.518671	192.168.1.139	150.214.54.249
28223 56.518672	192.168.1.139	150.214.54.249

Frame 28223: 182 bytes on wire (1456 bits), 182 bytes captured (1456 bits) on interface \Device\NPF...
Ethernet II, Src: IntelCor_41:77:f6 (84:ef:18:41:77:f6), Dst: zte_ef:c3:79 (8c:e1:17:ef:c3:79)
Internet Protocol Version 4, Src: 192.168.1.139, Dst: 150.214.54.249
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not Set)
Total Length: 168
Identification: 0xb058 (45144)
Flags: 0x0172
Fragment offset: 2960
Time to live: 128
Protocol: ICMP (1)

Tamaño = 3100

Ejercicio 4. Realice dos pings a **informatica.cv.uma.es** con tamaños MAX y MAX+1 y el bit DF activo (MAX es el tamaño máximo calculado). Añada una captura de pantalla.

```
C:\WINDOWS\system32>arp -d
C:\WINDOWS\system32>ipconfig /flushdns

Configuración IP de Windows

Se vació correctamente la caché de resolución de DNS.

C:\WINDOWS\system32>ping -n 1 informatica.cv.uma.es -l 1472 -f

Haciendo ping a frontalcv7.cv.uma.es [150.214.54.249] con 1472 bytes de datos:
Respuesta desde 150.214.54.249: bytes=1472 tiempo=55ms TTL=49

Estadísticas de ping para 150.214.54.249:
    Paquetes: enviados = 1, recibidos = 1, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 55ms, Máximo = 55ms, Media = 55ms

C:\WINDOWS\system32>ping -n 1 informatica.cv.uma.es -l 1473 -f

Haciendo ping a frontalcv7.cv.uma.es [150.214.54.249] con 1473 bytes de datos:
Es necesario fragmentar el paquete pero se especificó DF.

Estadísticas de ping para 150.214.54.249:
    Paquetes: enviados = 1, recibidos = 0, perdidos = 1
    (100% perdidos),
```

- ¿Cuál es el valor máximo?

1472

- ¿Por qué es ese tamaño?

Para calcular ese número tenemos que coger y al valor máximo de la MTU que es 1500 bytes le tenemos que restar 20 bytes de la cabecera del protocolo IP y 8 bytes de la cabecera de ICMP.

$1500 - 20 - 8 = 1472$.

- ¿En la traza de wireshark aparece el segundo ping? ¿Por qué?

No aparece, porque si observamos la terminal, aparece que se pierde el paquete, ya que no se puede fragmentar y no puede mandar todos sus bytes.

Ejercicio 5. Haga un ping a **informatica.cv.uma.es** usando un TTL creciente, empezando por 1 y deteniéndose cuando se empiece a recibir una respuesta del servidor. Observe en Wireshark el intercambio de paquetes que se produce.

```
C:\WINDOWS\system32>arp -d
C:\WINDOWS\system32>ipconfig /flushdns

Configuración IP de Windows

Se vació correctamente la caché de resolución de DNS.

C:\WINDOWS\system32>ping -n 1 informatica.cv.uma.es -i 1

Haciendo ping a frontalcv7.cv.uma.es [150.214.54.249] con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 150.214.54.249:
    Paquetes: enviados = 1, recibidos = 0, perdidos = 1
    (100% perdidos),

C:\WINDOWS\system32>ping -n 1 informatica.cv.uma.es -i 2

Haciendo ping a frontalcv7.cv.uma.es [150.214.54.249] con 32 bytes de datos:
Respuesta desde 100.85.0.1: TTL expirado en tránsito.

Estadísticas de ping para 150.214.54.249:
    Paquetes: enviados = 1, recibidos = 1, perdidos = 0
    (0% perdidos),
```

- Número de trama analizado
5101

icmp

Time	Source	Destination	Protocol
2812 6.424138	192.168.1.139	150.214.54.249	ICMP
5090 13.770884	192.168.1.139	150.214.54.249	ICMP
5101 13.798822	100.85.0.1	192.168.1.139	ICMP

Frame 5101: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on in Ethernet II, Src: zte_ef:c3:79 (8c:e1:17:ef:c3:79), Dst: IntelCor_41:77:f6 Internet Protocol Version 4, Src: 100.85.0.1, Dst: 192.168.1.139 Internet Control Message Protocol

Type: 11 (Time-to-live exceeded)
Code: 0 (Time to live exceeded in transit)
Checksum: 0x9fa3 [correct]
[Checksum Status: Good]
Unused: 00000000

Internet Protocol Version 4, Src: 192.168.1.139, Dst: 150.214.54.249

0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 60
Identification: 0xb3df (46047)
> Flags: 0x0000
Fragment offset: 0
Time to live: 1

Expert Info (Note/Sequence): "Time To Live" only 1
["Time To Live" only 1]
[Severity level: Note]

• ¿Qué mensaje ICMP se recibe cuando los paquetes no llegan (tipo, código y significado tiene dicho mensaje)?

• ¿Qué incluye dicho mensaje ICMP como información adicional?

Ejercicio 6. Responda a las siguientes preguntas:

```

C:\WINDOWS\system32>arp -d
C:\WINDOWS\system32>ipconfig /flushdns

Configuración IP de Windows

Se vació correctamente la caché de resolución de DNS.

C:\WINDOWS\system32>tracert informatica.cv.uma.es

Trazo a la dirección frontalcv7.cv.uma.es [150.214.54.249]
sobre un máximo de 30 saltos:

 1      *         *         *         Tiempo de espera agotado para esta solicitud.
 2     26 ms     24 ms     24 ms     100.85.0.1
 3     17 ms     16 ms     18 ms     10.15.4.81
 4     16 ms     17 ms     16 ms     10.0.24.54
 5     17 ms     17 ms     17 ms     be4430.rcr22.svq01.atlas.cogentco.com [149.11.19.193]
 6     30 ms     30 ms     30 ms     be3240.ccr31.vlc02.atlas.cogentco.com [154.54.59.13]
 7     34 ms     34 ms     35 ms     be3356.ccr32.mad05.atlas.cogentco.com [154.54.57.241]
 8     35 ms     34 ms     35 ms     be3379.agr22.mad05.atlas.cogentco.com [154.54.39.146]
 9     35 ms     35 ms     35 ms     be3481.nr51.b015537-1.mad05.atlas.cogentco.com [154.25.1.110]
10     42 ms     35 ms     35 ms     149.14.242.226
11     44 ms     43 ms     44 ms     130.206.245.122
12     60 ms     62 ms     76 ms     cica-router-backup.red.rediris.es [130.206.211.42]
13     61 ms     61 ms     60 ms     uma-router.red.cica.es [150.214.231.170]
14     54 ms     53 ms     63 ms     tuneles.uma.es [150.214.47.249]
15     55 ms     55 ms     54 ms     te6009dixie.ruma.uma.es [150.214.41.238]
16      *         *         *         Tiempo de espera agotado para esta solicitud.
17     54 ms     54 ms     55 ms     frontalcv7.cv.uma.es [150.214.54.249]

Trazo completa.

```

- Indique el número de los paquetes utilizados para responder estas preguntas

Números indicados en cada pregunta.

- ¿Qué tipo de paquetes (protocolo de más alto nivel) usa **tracert** para hacer su función?

Los de tipo ICMP. Paquetes 3,4,5,53,54,55,56... hay 93 en total que se usan al hacer el tracert.

ip.dst == 150.214.54.249 && ip.src == 192.168.1.139						
	Time	Source	Destination	Protocol	Length	Info
3	0.039988	192.168.1.139	150.214.54.249	ICMP	106	Echo (ping) request id=0x0001, seq=1000/59395, ttl=1 (r
4	3.698818	192.168.1.139	150.214.54.249	ICMP	106	Echo (ping) request id=0x0001, seq=1001/59651, ttl=1 (r
5	7.685441	192.168.1.139	150.214.54.249	ICMP	106	Echo (ping) request id=0x0001, seq=1002/59907, ttl=1 (r
53	11.699653	192.168.1.139	150.214.54.249	ICMP	106	Echo (ping) request id=0x0001, seq=1003/60163, ttl=2 (r
54	11.725579	100.85.0.1	192.168.1.139	ICMP	70	Time-to-live exceeded (Time to live exceeded in transi
55	11.727705	192.168.1.139	150.214.54.249	ICMP	106	Echo (ping) request id=0x0001, seq=1004/60419, ttl=2 (r
56	11.751832	100.85.0.1	192.168.1.139	ICMP	70	Time-to-live exceeded (Time to live exceeded in transi
57	11.753955	192.168.1.139	150.214.54.249	ICMP	106	Echo (ping) request id=0x0001, seq=1005/60675, ttl=2 (r
58	11.778176	100.85.0.1	192.168.1.139	ICMP	70	Time-to-live exceeded (Time to live exceeded in transi
67	17.336530	192.168.1.139	150.214.54.249	ICMP	106	Echo (ping) request id=0x0001, seq=1006/60931, ttl=3 (r
68	17.354103	10.15.4.81	192.168.1.139	ICMP	182	Time-to-live exceeded (Time to live exceeded in transi
69	17.356188	192.168.1.139	150.214.54.249	ICMP	106	Echo (ping) request id=0x0001, seq=1007/61187, ttl=3 (r
70	17.372971	10.15.4.81	192.168.1.139	ICMP	182	Time-to-live exceeded (Time to live exceeded in transi
71	17.375057	192.168.1.139	150.214.54.249	ICMP	106	Echo (ping) request id=0x0001, seq=1008/61443, ttl=3 (r
72	17.393073	10.15.4.81	192.168.1.139	ICMP	182	Time-to-live exceeded (Time to live exceeded in transi

- Además de los mensajes propios para obtener el camino, **tracert** puede provocar que se realicen otros envíos auxiliares para conseguir información o mostrar de forma más amistosa la información, ¿qué otros mensajes pueden ser necesarios?

Podría ser necesario algunos de tipo DNS, ya que traduce las direcciones IP a las URL que les corresponde

Tramas 163,165,166,167,168 las del siguiente ejemplo.

Time	Source	Destination	Protocol	Length	Info
161 33.146821	192.168.1.139	150.214.54.249	ICMP	106	Echo (ping) request id=0x0001, seq=1025/260, ttl=9 (n
162 33.182375	154.25.1.110	192.168.1.139	ICMP	110	Time-to-live exceeded (Time to live exceeded in transi
163 33.182914	192.168.1.139	150.214.54.249	ICMP	106	Echo (ping) request id=0x0001, seq=1026/516, ttl=9 (n
164 33.218342	154.25.1.110	192.168.1.139	ICMP	110	Time-to-live exceeded (Time to live exceeded in transi
165 33.220669	192.168.1.139	46.6.113.34	DNS	85	Standard query 0x70e5 PTR 110.1.25.154.in-addr.arpa
166 33.476347	46.6.113.34	192.168.1.139	DNS	145	Standard query response 0x70e5 PTR 110.1.25.154.in-add
167 33.550150	192.168.1.139	46.6.113.34	DNS	91	Standard query 0xa3e6 A settings-win.data.microsoft.co
168 33.589053	46.6.113.34	192.168.1.139	DNS	154	Standard query response 0xa3e6 A settings-win.data.mic
169 33.589464	192.168.1.139	51.124.78.146	TCP	66	62132 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=25

```

Name: 110.1.25.154.in-addr.arpa
[Name Length: 25]
[Label Count: 6]
Type: PTR (domain name PointeR) (12)
Class: IN (0x0001)

Answers
  110.1.25.154.in-addr.arpa: type PTR, class IN, be3481.nr51.b015537-1.mad05.atlas.cogentco.com
    Name: 110.1.25.154.in-addr.arpa
    Type: PTR (domain name PointeR) (12)
    Class: IN (0x0001)
    Time to live: 43200 (12 hours)
    Data length: 48
    Domain Name: be3481.nr51.b015537-1.mad05.atlas.cogentco.com

```

Si nos fijamos en la captura de la consola de este ejercicio en el ttl 9, observamos que esta trama DNS le devuelve la IP del nodo intermedio para que se vaya moviendo, pero esta IP está invertida.

```

[Request In: 165]
[Time: 0.055638000 seconds]
84 ef 18 41 77 f6 8c e1 17 ef c3 79 08 00 45 00 ...Aw...y..E.
00 83 b5 b8 40 00 fc 11 67 55 2e 06 71 22 c0 a8 ...@...gU..q"
01 8b 00 35 c6 a9 00 6f be ad 70 e5 81 80 00 01 ...5...o..p....
00 01 00 00 00 00 03 31 30 01 31 02 32 35 03 .....1 10.1.25.
31 35 34 07 69 6e 2d 61 64 64 72 04 61 72 70 61 154.in-a ddr.arpa
00 00 0c 00 01 c0 0c 00 0c 00 01 00 00 a8 c0 00 .....
30 06 62 65 33 34 38 31 04 6e 72 35 31 09 62 30 0-be3481-nr51-b0
31 35 35 33 37 2d 31 05 6d 61 64 30 35 05 61 74 15537-1-mad05-at
6c 61 73 08 63 6f 67 65 6e 74 63 6f 03 63 6f 6d las.coge ntco.com
00

```

- ¿Qué estrategia usa **tracert** para averiguar qué máquina hay en cada salto del paquete?

Según las diferentes tablas de encaminamiento de router a router se envían ICMP hasta que llega al destino determinado. Las tramas en negro devuelven la IP de los nodos intermedios y las tramas DNS las IPs de destino de los nodos intermedios, así es como se ve todos los pasos que hace.

Práctica 3

Apellidos: López Pérez

Nombre: Marta

Titulación: Grado de Ingeniería Informática

Grupo: 2ºA

PC de la práctica: casa

Lea el enunciado de la práctica para saber el contexto de cada ejercicio.

Recuerde en añadir capturas de pantalla de la ejecución de todos los comandos que se piden en la práctica.

Ejercicio 1 (versión Windows). El comando `ipconfig /all` de Windows muestra información sobre las interfaces de red de la máquina. Ejecute dicho comando en un terminal y, busque la información de su interfaz física e identifique su IP, máscara y puerta de enlace asociada (haga una captura y márkelas). También apunte el campo denominado **Descripción** (lo usaremos más adelante).

- ¿Cuál es el identificador de su red?
192.168.1.0

Ejercicio 1 (versión MAC/Linux). El comando `ifconfig` de MAC/Linux (o en `ip` algunos Linux) muestra información sobre las interfaces de red de la máquina. Ejecute en un terminal:

MAC: `ifconfig; netstat -rn | grep "UGS" | awk '{print "Pasarela: " $2}'`

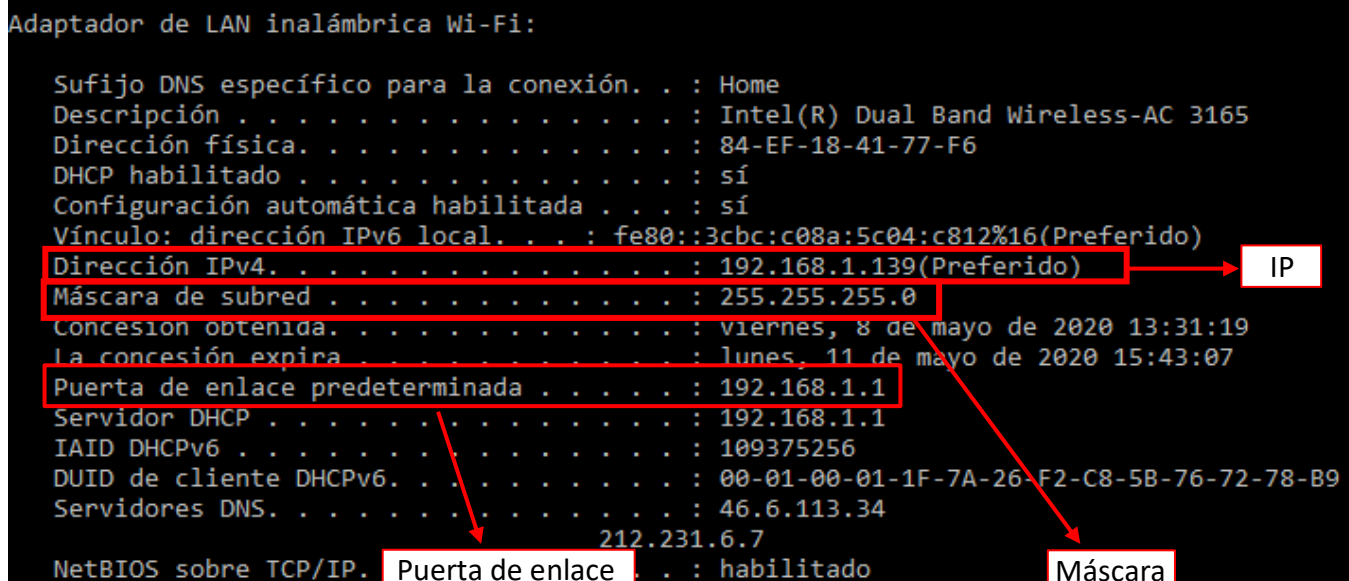
Linux: `ip ad sh; ip ro sh | grep "default" | awk '{print "Pasarela: " $3}'`

busque la información de su interfaz física asociado a su IP, máscara y puerta de enlace asociada (haga una captura y márkelas). También apunte el nombre de dicho interfaz (la primera palabra delante de la configuración que suele tener alguna de las siguientes formas: `ethX`, `wlpXsY`, `enpXsY`, `ensX...`) que lo usaremos más adelante (lo denominaremos **Descripción**).

- ¿Cuál es el identificador de su red?

Adaptador de LAN inalámbrica Wi-Fi:

```
Sufijo DNS específico para la conexión. . . : Home
Descripción . . . . . : Intel(R) Dual Band Wireless-AC 3165
Dirección física. . . . . : 84-EF-18-41-77-F6
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí
Vínculo: dirección IPv6 local. . . : fe80::3cbc:c08a:5c04:c812%16(Preferido)
Dirección IPv4. . . . . : 192.168.1.139(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Concesión obtenida. . . . . : viernes, 8 de mayo de 2020 13:31:19
La concesión expira . . . . . : lunes, 11 de mayo de 2020 15:43:07
Puerta de enlace predeterminada . . . . . : 192.168.1.1
Servidor DHCP . . . . . : 192.168.1.1
IAID DHCPv6 . . . . . : 109375256
DUID de cliente DHCPv6. . . . . : 00-01-00-01-1F-7A-26-F2-C8-5B-76-72-78-B9
Servidores DNS. . . . . : 46.6.113.34
NetBIOS sobre TCP/IP. . . . . : 212.231.6.7
NetBIOS sobre TCP/IP. . . . . : habilitado
```



Ejercicio 2. Observe los datos de la red en Linux usando el comando `ifconfig` en un terminal. Aparecerá la configuración de dos interfaces: uno llamado **lo** y otro cuyo nombre puede variar (lo utilizaremos en otros ejercicios y nos referiremos a él como **interfazReal**).

- Observe en primer lugar el interfaz **lo**, ¿para qué se usa este interfaz?

El loopback(lo) es una interfaz de red virtual especial que el ordenador usa para comunicarse consigo mismo. Se usa principalmente para diagnósticos y para conectarse con los servidores que están activos en la máquina local.

- Ahora analice el otro interfaz (**interfazReal**), de acuerdo a esos datos (dirección IP y máscara), ¿está el Linux de la máquina virtual en la misma red IPv4 que el Windows de la máquina huésped?

Si.

- ¿Por qué?

Porque tienen la misma máscara (255.255.255.0) y los bits que representan la red (o lo que es lo mismo, los bit que la máscara tiene a 1) son iguales en ambas IPs:

```
alumno@RySD:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.1.141  netmask 255.255.255.0  broadcast 192.168.1.255
    inet6 fe80::a00:27ff:fe09:4381  prefixlen 64  scopeid 0x20<link>
    ether 08:00:27:09:43:81  txqueuelen 1000  (Ethernet)
    RX packets 249992  bytes 351931585 (351.9 MB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 35912  bytes 6934022 (6.9 MB)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
    inet6 ::1  prefixlen 128  scopeid 0x10<host>
    loop txqueuelen 1000  (Bucle local)
    RX packets 5613  bytes 564748 (564.7 KB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 5613  bytes 564748 (564.7 KB)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Ejercicio 3. Vuelva a ejecutar el comando `ifconfig`.

- ¿Qué IP/máscara tiene activada ahora el **interfazReal**?

Ninguna.

- ¿Por qué tiene ese tipo de configuración?

Porque antes de ejecutar el comando `ifconfig`, hemos puesto otros comandos que han hecho que se modifique la configuración.

```
alumno@RySD:~$ sudo /etc/init.d/network-manager stop
[sudo] contraseña para alumno:
[ ok ] Stopping network-manager (via systemctl): network-manager.service.
alumno@RySD:~$ sudo kill -9 `cat /run/dhclient-enp0s3.pid`
alumno@RySD:~$ sudo ip address flush enp0s3
alumno@RySD:~$ sudo rm /etc/resolv.conf
```

El primero desactiva el servicio de red, el segundo desactiva el cliente de DHCP, el tercero libera la IP asignada actualmente, y el último elimina la configuración del DNS.

```
alumno@RySD:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    ether 08:00:27:09:43:81 txqueuelen 1000 (Ethernet)
    RX packets 251280 bytes 352688501 (352.6 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 36640 bytes 7084170 (7.0 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Bucle local)
    RX packets 8112 bytes 764350 (764.3 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8112 bytes 764350 (764.3 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```


Ejercicio 4. Configure la IP y la máscara de subred en Linux con el siguiente comando:

```
sudo ifconfig interfazReal dirIP netmask máscara1
```

donde los valores de **interfazReal**, **dirIP** y **máscara** son los mismos valores que observó en ejercicio 2.

Ponemos en la consola el siguiente comando:

```
sudo ifconfig enp0s3 192.168.1.141 netmask 255.255.255.0
```

```
alumno@RySD:~$ sudo ifconfig enp0s3 192.168.1.141 netmask 255.255.255.0
alumno@RySD:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.1.141  netmask 255.255.255.0  broadcast 192.168.1.255
    ether 08:00:27:09:43:81  txqueuelen 1000  (Ethernet)
    RX packets 251299  bytes 352689641 (352.6 MB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 36653  bytes 7085846 (7.0 MB)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
    inet6 ::1  prefixlen 128  scopeid 0x10<host>
    loop txqueuelen 1000  (Bucle local)
    RX packets 10188  bytes 928946 (928.9 KB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 10188  bytes 928946 (928.9 KB)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Ejercicio 5. Intente ahora hacer desde Linux un ping² a la IP de loopback (127.0.0.1), la IP del Windows de su propia máquina, a la IP de su router/puerta de enlace y a una máquina externa a la red (intente tanto por nombre **informatica.cv.uma.es** como por IP: **150.214.54.249**)

- ¿Cuáles funcionan y cuáles no?

IP de de loopback (127.0.0.1) → SI

```
alumno@RySD:~$ ping -c 1 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.030 ms

--- 127.0.0.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.030/0.030/0.030/0.000 ms
```

IP del Windows de su propia máquina → Se pierden los paquetes pero SI se realiza el ping

```
alumno@RySD:~$ ping -c 1 192.168.1.139
PING 192.168.1.139 (192.168.1.139) 56(84) bytes of data.

--- 192.168.1.139 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms
```

IP de su router/puerta de enlace → SI

```
alumno@RySD:~$ ping -c 1 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=6.25 ms

--- 192.168.1.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 6.254/6.254/6.254/0.000 ms
```

IP a una máquina externa a la red, con nombre **informatica.cv.uma.es** → NO

```
alumno@RySD:~$ ping -c 1 informatica.cv.uma.es
ping: informatica.cv.uma.es: Fallo temporal en la resolución del nombre
```

IP 150.214.54.249 → NO

```
alumno@RySD:~$ ping -c 1 150.214.54.249
connect: La red es inaccesible
```

2 Haga los pings con la opción `-c 1` para que solo envíe un mensaje ICMP.

Ejercicio 6. Observe la tabla de encaminamiento de su máquina virtual Linux con el comando `route`.

- ¿Cómo explica esta tabla por qué algunos pings de los anteriores funcionan y otros no?

Se nos muestra una tabla con las redes con las que nos podemos comunicar porque comparten una red local, por eso nos permite comunicarnos con las 2/5 IPs del ejercicio anterior. Sin embargo al intentar conectar con una red como la de la misma máquina o la de la página del campus de la UMA nos pone que es imposible acceder.

```
alumno@RySD:~$ route
Tabla de rutas IP del núcleo
Destino          Pasarela          Genmask          Indic Métric Ref       Uso Interfaz
192.168.1.0      0.0.0.0           255.255.255.0   U      0      0        0 enp0s3
```

Ejercicio 7. Además de consultar la tabla de encaminamiento, con el comando `route` podemos modificarla (necesita ser root, use `sudo` delante del comando. Usando esos comandos realice las siguientes acciones:

- Añada una entrada de encaminamiento por defecto usando el comando `c` (como valor de gateway use la misma puerta de enlace que en Windows). Vuelva a probar los pings que fallaron en el ejercicio 5 y comente el motivo por el que ahora funcionan algunos que antes no.

```
alumno@RySD:~$ sudo route add default gw 192.168.1.1
[sudo] contraseña para alumno:
```

IP máquina externa con nombre `informatica.cv.uma.es` → antes NO / ahora NO

```
alumno@RySD:~$ ping -c 1 informatica.cv.uma.es
ping: informatica.cv.uma.es: Fallo temporal en la resolución del nombre
```

IP `150.214.54.249` → antes NO / ahora SI

```
alumno@RySD:~$ ping -c 1 150.214.54.249
PING 150.214.54.249 (150.214.54.249) 56(84) bytes of data.
64 bytes from 150.214.54.249: icmp_seq=1 ttl=49 time=136 ms

--- 150.214.54.249 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 136.644/136.644/136.644/0.000 ms
```

Gracias al comando que pusimos antes de comprobar si funcionaban, hemos conseguido que funcione el ping a la IP `150.214.54.249` porque hemos añadido la dirección de IP de nuestra Gateway por defecto lo que hace que se puedan realizar el ping a dicha IP.

- Finalmente, cree el fichero **/etc/resolv.conf**³ con la línea **nameserver 8.8.8.8** (DNS gratuito ofrecido por Google). ¿Funcionan ahora todos los pings?

```
alumno@RySD:~$ sudo leafpad /etc/resolv.conf
(leafpad:2565): GLib-GIO-CRITICAL **: 02:58:13.619: g_dbus_proxy_new: assertion
'G_IS_DBUS_CONNECTION (connection)' failed
```

➔ PROBAMOS DE NUEVO LOS PINGS QUE FALLARON ANTES:

IP máquina externa con nombre `informatica.cv.uma.es` ➔ antes NO / ahora SI

```
alumno@RySD:~$ ping -c 1 informatica.cv.uma.es
PING frontalcv7.cv.uma.es (150.214.54.249) 56(84) bytes of data.
64 bytes from frontalcv7.cv.uma.es (150.214.54.249): icmp_seq=1 ttl=49 time=54.9 ms

--- frontalcv7.cv.uma.es ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 54.916/54.916/54.916/0.000 ms
```

- ¿Por qué funcionan los que antes fallaban?

Se consigue que funcionen todos finalmente.

Este último ping que se hace a `informatica.cv.uma.es` funciona ya que ahora cuando le pasas una URL, el archivo creado con `nameserver` le da una IP a esa URL y eso ocurre también en la tabla de encaminamiento, que en el por defecto va a esa red.

Ejercicio 8. Cuando se envía un mensaje al exterior de su red local se hacen dos consultas a su tabla de encaminamiento:

- Primero se busca la entrada que nos lleva al destino final. Al ser externa, se escogerá la entrada por defecto, que nos indica que debemos enviar a la puerta de enlace (su router).
- Luego buscamos la entrada para llegar a nuestro router (la entrada que nos permite comunicarnos con los equipos de nuestra red) que nos dirá que esta comunicación se puede hacer por entrega directa.

Observe la tabla de encaminamiento de su equipo (comando `route PRINT -4` en Windows, `netstat -rn` en MAC y `ip route show` en Linux). Haga una captura de pantalla donde se vean todas las entradas de la tabla marcando:

- Entrada que le permite comunicarse con un equipo su propia red física (diferente al suyo).
- Entrada por defecto

```
Microsoft Windows [Versión 10.0.18362.778]
(c) 2019 Microsoft Corporation. Todos los derechos reservados.

C:\WINDOWS\system32> route PRINT -4
=====
Lista de interfaces
 9...c8 5b 76 72 78 b9 .....Realtek PCIe GBE Family Controller
13...0a 00 27 00 00 0d .....VirtualBox Host-Only Ethernet Adapter
21...86 ef 18 41 77 f6 .....Microsoft Wi-Fi Direct Virtual Adapter
 5...84 ef 18 41 77 f7 .....Microsoft Wi-Fi Direct Virtual Adapter #3
16...84 ef 18 41 77 f6 .....Intel(R) Dual Band Wireless-AC 3165
 1.....Software Loopback Interface 1
=====

IPv4 Tabla de enrutamiento
=====
Rutas activas:
Destino de red      Máscara de red      Puerta de enlace      Interfaz      Métrica
-----
 0.0.0.0            0.0.0.0            192.168.1.1          192.168.1.139      40
127.0.0.0          255.0.0.0          En vínculo           127.0.0.1          331
127.0.0.1          255.255.255.255    En vínculo           127.0.0.1          331
127.255.255.255    255.255.255.255    En vínculo           127.0.0.1          331
192.168.1.0        255.255.255.0      En vínculo           192.168.1.139      296
192.168.1.139      255.255.255.255    En vínculo           192.168.1.139      296
192.168.1.255      255.255.255.255    En vínculo           192.168.1.139      296
192.168.56.0       255.255.255.0      En vínculo           192.168.56.1        281
192.168.56.1       255.255.255.255    En vínculo           192.168.56.1        281
192.168.56.255     255.255.255.255    En vínculo           192.168.56.1        281
224.0.0.0          240.0.0.0          En vínculo           127.0.0.1          331
224.0.0.0          240.0.0.0          En vínculo           192.168.56.1        281
224.0.0.0          240.0.0.0          En vínculo           192.168.1.139      296
255.255.255.255    255.255.255.255    En vínculo           127.0.0.1          331
255.255.255.255    255.255.255.255    En vínculo           192.168.56.1        281
255.255.255.255    255.255.255.255    En vínculo           192.168.1.139      296
=====
Rutas persistentes:
Ninguno
```

b)

a)

Ejercicio 9. Describa los principales elementos del código desarrollado (si el código ya tiene comentarios en el propio código, no es necesario incluir aquí nada) y una captura de pantalla de su ejecución.

En mi código, utilizo un método auxiliar distinto para cada cosa que vamos a mostrar, pero para poder realizar la implementación de estos métodos he necesitado crear más métodos privados que me han ayudado a llegar a la solución completa y de una manera general para cualquier ip que se ponga de entrada.

```
5 package pr3;
6
7 public class p3e8
8 {
9     public static void main(String[] args)
10    {
11        String cadena = "192.168.42.30 21";
12
13        String [] ip = cadena.split("[ .]");    //Dividimos la cadena en el array
14
15        int numMascara = Integer.parseInt(ip[4]);
16
17        String IP = mostrarIP(ip);
18        String MASCARA = mascaraIPdecimal(numMascara);
19
20        System.out.println("La IP introducida es: " + IP);
21        System.out.println("La mascara introducidaes : " + numMascara + " (" + MASCARA + ")");
22        System.out.println();
23        System.out.println("La IP es de clase " + claseIP(Integer.parseInt(ip[0])));
24        System.out.println("Red: " + indentificadorRed(IP, MASCARA) + "/" + numMascara);
25        System.out.println("Difusión: " + difusion(IP, MASCARA));
26        System.out.println("Número de IPs para host: " + numeroIPhost(numMascara));
27    }
28 }
```

Problems @ Javadoc Declaration Console

<terminated> p3e8 [Java Application] C:\Program Files\Java\jdk-12.0.2\bin\javaw.exe (10 may. 2020 15:24:00)

La IP introducida es: 192.168.42.30
La mascara introducidaes : 21 (255.255.248.0)

La IP es de clase C
Red: 192.168.40.0/21
Difusión: 192.168.47.255
Número de IPs para host: 2046