

# PRÁCTICA WIRESHARK

Ethan Alexander y Verónica Villaseca  
1ºASIR IES Alonso de Avellaneda

## Tabla de contenido

Tramas de broadcast: .....	2
ARP .....	2
DHCP .....	3
Lista de protocolos de broadcast: .....	4
¿Qué protocolos viajan sobre el nivel de enlace? .....	5
Conversación Ping:.....	6
Parte en casa.....	7
Que he encontrado.....	7
Broadcast: .....	7
Datos capa de enlace: .....	7
Conversación ping:.....	8

## Tramas de broadcast:

para poder filtrar en WireShark los datos que vayan por broadcast se aplica el filtro:

*eth.addr == ff:ff:ff:ff:ff:ff*

Aplicando este filtro hemos encontrado lo siguiente:

## ARP

Wireshark interface showing a list of ARP broadcast packets. The filter applied is `eth.addr == ff:ff:ff:ff:ff:ff`. The packet list shows various ARP requests and responses. The packet details pane shows the structure of an ARP request frame.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Ubiquiti_fa:00:b5	Broadcast	ARP	60	Who has 10.1.0.1? Tell 10.1.1.10
24	0.750362	PcsCompu_7f:4d:83	Broadcast	ARP	60	Who has 192.168.37.200? Tell 192.168.37.229
39	1.500825	PcsCompu_7f:4d:83	Broadcast	ARP	60	Who has 192.168.37.200? Tell 192.168.37.229
42	1.750533	PcsCompu_7f:4d:83	Broadcast	ARP	60	Who has 192.168.37.200? Tell 192.168.37.229
86	2.750583	PcsCompu_7f:4d:83	Broadcast	ARP	60	Who has 192.168.37.200? Tell 192.168.37.229
137	3.844383	PcsCompu_7f:4d:83	Broadcast	ARP	60	Who has 192.168.37.200? Tell 192.168.37.229
141	4.138864	PcsCompu_26:18:82	Broadcast	ARP	42	Who has 10.1.1.20? Tell 10.1.1.24
146	4.139666	PcsCompu_26:18:82	Broadcast	ARP	60	Who has 10.1.1.20? Tell 10.1.1.55
147	4.140172	PcsCompu_26:18:82	Broadcast	ARP	60	Who has 10.1.1.20? Tell 10.1.1.55
162	4.766188	PcsCompu_7f:4d:83	Broadcast	ARP	60	Who has 192.168.37.200? Tell 192.168.37.229
164	4.854192	Ubiquiti_36:64:5b	Broadcast	ARP	60	Who has 10.1.0.1? Tell 10.1.1.57
171	5.750372	PcsCompu_7f:4d:83	Broadcast	ARP	60	Who has 192.168.37.200? Tell 192.168.37.229
267	11.645718	Routerbo_e8:b9:80	Broadcast	ARP	60	Who has 10.1.1.28? Tell 10.1.0.2
268	11.645874	Routerbo_e8:b9:80	Broadcast	ARP	60	Who has 10.1.1.28? Tell 10.1.0.2
278	12.252516	PcsCompu_05:06:04	Broadcast	ARP	60	Who has 10.1.0.103? Tell 10.1.1.28
281	12.252516	PcsCompu_05:06:04	Broadcast	ARP	60	Who has 10.1.0.2? Tell 10.1.1.28
298	12.476449	PcsCompu_05:06:04	Broadcast	ARP	60	Who has 10.1.0.1? Tell 10.1.1.28
335	13.299027	Comtrend_69:02:c3	Broadcast	ARP	60	Who has 10.1.1.55? Tell 10.1.0.1
349	13.516000	PcsCompu_7f:4d:83	Broadcast	ARP	60	Who has 192.168.37.200? Tell 192.168.37.229
372	14.250620	PcsCompu_7f:4d:83	Broadcast	ARP	60	Who has 192.168.37.200? Tell 192.168.37.229
390	15.252780	PcsCompu_7f:4d:83	Broadcast	ARP	60	Who has 192.168.37.200? Tell 192.168.37.229
412	16.250130	PcsCompu_7f:4d:83	Broadcast	ARP	60	Who has 192.168.37.200? Tell 192.168.37.229
417	17.237809	PcsCompu_7f:4d:83	Broadcast	ARP	60	Who has 192.168.37.200? Tell 192.168.37.229
425	18.250501	PcsCompu_7f:4d:83	Broadcast	ARP	60	Who has 192.168.37.200? Tell 192.168.37.229
433	19.269717	HewlettP_06:e0:f4	Broadcast	ARP	60	Who has 10.1.0.2? Tell 10.1.1.100
456	21.829590	PcsCompu_7f:4d:83	Broadcast	ARP	60	Who has 192.168.37.200? Tell 192.168.37.229
464	22.751159	PcsCompu_7f:4d:83	Broadcast	ARP	60	Who has 192.168.37.200? Tell 192.168.37.229
482	23.750835	PcsCompu_7f:4d:83	Broadcast	ARP	60	Who has 192.168.37.200? Tell 192.168.37.229
498	24.953991	PcsCompu_7f:4d:83	Broadcast	ARP	60	Who has 192.168.37.200? Tell 192.168.37.229
505	25.740384	PcsCompu_7f:4d:83	Broadcast	ARP	60	Who has 192.168.37.200? Tell 192.168.37.229

Frame 42: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF\_{412010BB-CAFC-4CA1-A892-2CCFFD71C5A8}, id 0  
> Ethernet II, Src: PcsCompu\_7f:4d:83 (08:00:27:7f:4d:83), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
> Address Resolution Protocol (request)

0000 ff ff ff ff ff 08 00 27 7f 4d 83 08 06 00 01 .....M.....  
0010 08 00 06 04 00 01 08 00 27 7f 4d 83 c0 a8 25 e5 .....M.....

Source or Destination Hardware Address (eth.addr), 6 byte(s)

Paquetes: 512 · Mostrado: 113 (22.1%) · Perdido: 0 (0.0%) · Perfil: Default

**ARP:** Es el protocolo de resolución, es decir, es la que se encarga de vincular una dirección MAC con una dirección IP o lógica.

## DHCP

\*Ethernet 2

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

eth.addr == ff:ff:ff:ff:ff:ff

No.	Time	Source	Destination	Protocol	Length	Info
412	16.250130	PcsCompu_7f:4d:83	Broadcast	ARP	60	Who has 192.168.37.200? Tell 192.168.37.229
417	17.237809	PcsCompu_7f:4d:83	Broadcast	ARP	60	Who has 192.168.37.200? Tell 192.168.37.229
425	18.250501	PcsCompu_7f:4d:83	Broadcast	ARP	60	Who has 192.168.37.200? Tell 192.168.37.229
433	19.269717	HewlettP_06:e0:f4	Broadcast	ARP	60	Who has 10.1.0.2? Tell 10.1.1.100
456	21.829590	PcsCompu_7f:4d:83	Broadcast	ARP	60	Who has 192.168.37.200? Tell 192.168.37.229
464	22.751159	PcsCompu_7f:4d:83	Broadcast	ARP	60	Who has 192.168.37.200? Tell 192.168.37.229
482	23.750835	PcsCompu_7f:4d:83	Broadcast	ARP	60	Who has 192.168.37.200? Tell 192.168.37.229
498	24.953991	PcsCompu_7f:4d:83	Broadcast	ARP	60	Who has 192.168.37.200? Tell 192.168.37.229
505	25.749384	PcsCompu_7f:4d:83	Broadcast	ARP	60	Who has 192.168.37.200? Tell 192.168.37.229
8	0.692160	10.1.1.1	10.1.255.255	BROWSER	273	Host Announcement A33PC02, Workstation, Server, Print Queue Server, Xenix ...
387	15.059631	10.1.1.152	10.1.255.255	BROWSER	273	Host Announcement A31PC07, Workstation, Server, Print Queue Server, Xenix ...
388	15.060171	10.1.1.98	10.1.255.255	BROWSER	273	Host Announcement A31PC04, Workstation, Server, Print Queue Server, Xenix ...
402	15.562054	10.1.1.125	10.1.255.255	BROWSER	273	Host Announcement A37PC14, Workstation, Server, Print Queue Server, Xenix ...
452	21.555317	10.1.1.55	10.1.255.255	BROWSER	243	Host Announcement PC-ALUMNO, Workstation, Server, NT Workstation, Potentia...
501	25.642730	10.1.1.202	10.1.255.255	BROWSER	273	Host Announcement A32PC03, Workstation, Server, Print Queue Server, Xenix ...
502	25.642730	10.1.1.25	10.1.255.255	BROWSER	273	Host Announcement A32PC05, Workstation, Server, Print Queue Server, Xenix ...
503	25.642730	10.1.1.4	10.1.255.255	BROWSER	273	Host Announcement A32PC09, Workstation, Server, Print Queue Server, Xenix ...
504	25.642730	10.1.1.130	10.1.255.255	BROWSER	273	Host Announcement A32PC13, Workstation, Server, Print Queue Server, Xenix ...
265	11.628496	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xe3d2d00d
276	12.149086	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xe3d2d00d
155	4.245656	10.1.1.6	255.255.255.255	MNDP	166	5678 → 5678 Len=124
160	4.666473	10.1.1.37	255.255.255.255	MNDP	166	5678 → 5678 Len=124
457	21.945507	0.0.0.0	255.255.255.255	MNDP	180	5678 → 5678 Len=138
460	21.951323	10.1.0.2	255.255.255.255	MNDP	181	5678 → 5678 Len=139
4	0.402963	10.1.1.24	10.1.255.255	NBNS	92	Name query NB WORKGROUP<1c>
5	0.692160	10.1.1.99	255.255.255.255	NBNS	110	Registration NB WORKGROUP<00>
6	0.692160	10.1.1.99	255.255.255.255	NBNS	110	Registration NB WIN-9JIV33B87U4<00>
7	0.692160	10.1.1.99	255.255.255.255	NBNS	110	Registration NB WIN-9JIV33B87U4<20>
34	1.189024	10.1.1.24	10.1.255.255	NBNS	92	Name query NB WORKGROUP<1c>
35	1.157040	10.1.1.00	255.255.255.255	NBNS	110	Registration NB WIN-9JIV33B87U4<20>

> Frame 276: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF\_{412010BB-CAFC-4CA1-A892-2CCFFD71C5A8}, id 0

> Ethernet II, Src: PcsCompu\_05:06:04 (08:00:27:05:06:04), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255

> User Datagram Protocol, Src Port: 68, Dst Port: 67

> Dynamic Host Configuration Protocol (Request)

```

0000  ff ff ff ff ff ff 08 00 27 05 06 04 08 00 45 10  .....E.
0010  01 48 00 00 00 00 80 11 39 96 00 00 00 00 ff ff  .H.....9.....

```

**DHCP:** Es un protocolo de asignación de direcciones IP a las maquinas en la misma red que el servidor que proporciona el servicio.

## UDP

Wireshark interface showing a packet capture on Ethernet II. The filter is `eth.addr == ff:ff:ff:ff:ff:ff`. The packet list shows several NBNS and UDP packets. Packet 31 is selected, showing details for Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Data (15 bytes). The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
317	13.020878	10.1.1.152	255.255.255.255	NBNS	110	Registration NB WIN-9486F2AH73K<00>
340	13.392988	10.1.1.152	255.255.255.255	NBNS	110	Registration NB WIN-9486F2AH73K<20>
363	13.783965	10.1.1.152	255.255.255.255	NBNS	110	Registration NB WIN-9486F2AH73K<00>
364	13.783965	10.1.1.152	255.255.255.255	NBNS	110	Registration NB WORKGROUP<00>
368	14.145550	10.1.1.152	255.255.255.255	NBNS	110	Registration NB WIN-9486F2AH73K<20>
376	14.909349	10.1.1.152	255.255.255.255	NBNS	110	Registration NB WIN-9486F2AH73K<20>
386	15.059631	10.1.1.176	10.1.255.255	NBNS	92	Name query NB IEKCDQHQY<20>
389	15.093947	10.1.1.20	255.255.255.255	NBNS	92	Name query NB WPAD<00>
397	15.310799	10.1.1.176	10.1.255.255	NBNS	92	Name query NB PBHICUAFS<20>
401	15.561680	10.1.1.176	10.1.255.255	NBNS	92	Name query NB YIFCJIAJ<20>
403	15.843157	10.1.1.20	255.255.255.255	NBNS	92	Name query NB WPAD<00>
414	16.594154	10.1.1.20	255.255.255.255	NBNS	92	Name query NB WPAD<00>
438	19.797065	192.168.37.229	192.168.37.255	NBNS	92	Name query NB WORKGROUP<1c>
449	20.550806	192.168.37.229	192.168.37.255	NBNS	92	Name query NB WORKGROUP<1c>
450	21.313774	192.168.37.229	192.168.37.255	NBNS	92	Name query NB WORKGROUP<1c>
453	21.555317	10.1.1.100	10.1.255.255	NBNS	92	Name query NB WORKGROUP<1d>
462	22.096063	192.168.37.229	192.168.37.255	NBNS	92	Name query NB WORKGROUP<1c>
465	22.860561	192.168.37.229	192.168.37.255	NBNS	92	Name query NB WORKGROUP<1c>
473	23.625955	192.168.37.229	192.168.37.255	NBNS	92	Name query NB WORKGROUP<1c>
497	24.888188	10.1.1.20	255.255.255.255	NBNS	92	Name query NB WPAD<00>
500	25.641188	10.1.1.20	255.255.255.255	NBNS	92	Name query NB WPAD<00>
512	26.395099	10.1.1.20	255.255.255.255	NBNS	92	Name query NB WPAD<00>
31	0.802449	10.1.4.44	255.255.255.255	UDP	60	46135 → 3289 Len=15
40	1.597901	10.1.1.57	255.255.255.255	UDP	203	44967 → 10001 Len=161
43	1.809369	10.1.4.44	255.255.255.255	UDP	79	35293 → 1124 Len=37
229	9.186803	10.1.1.10	255.255.255.255	UDP	234	45043 → 10001 Len=192
263	11.600570	10.1.1.57	255.255.255.255	UDP	203	48939 → 10001 Len=161
432	19.260271	10.1.1.10	255.255.255.255	UDP	234	50548 → 10001 Len=192
454	21.606139	10.1.1.57	255.255.255.255	UDP	203	37167 → 10001 Len=161

> Frame 31: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF\_{412010BB-CAFC-4CA1-A892-2CCFFD71C5A8}, id 0  
> Ethernet II, Src: Giga-Byt\_e5:c0:5e (18:c0:4d:e5:c0:5e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
> Internet Protocol Version 4, Src: 10.1.4.44, Dst: 255.255.255.255  
> User Datagram Protocol, Src Port: 46135, Dst Port: 3289  
> Data (15 bytes)

0000 ff ff ff ff ff ff 18 c0 4d e5 c0 5e 08 00 45 00 .....E:  
0010 00 2b 4a 16 40 00 40 11 e2 7f 0a 01 04 2c ff ff .+J:@@.....

Specifies if this is a locally administered or globally unique (IEEE assigned) address (eth.dst.lg), 3 byte(s) | Paquetes: 512 · Mostrado: 113 (22.1%) · Perdido: 0 (0.0%) | Perfil: Default

**UDP:** Este protocolo permite la transmisión sin conexión a datagramas.

## Lista de protocolos de broadcast:

**BROWSER:** Es el protocolo de HTTP/HTTPS

**MNDP:** Es un protocolo de descubrimiento, es parecido al ARP de IPv4, pero funciona en IPv6

**NBNS:** Es el protocolo de servicio de nombres NetBIOS.

¿Qué protocolos viajan sobre el nivel de enlace?

Protocolo	Código
ARP	0x0800
CDP	0x2000
STP	0x8000

## Conversación Ping:

Wireshark capture of a ping conversation to 8.8.8.8. The packet list shows four ICMP Echo (ping) requests and four replies. The packet details for packet 908 are expanded, showing Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol. The packet bytes are also displayed with a hex-to-ASCII conversion.

No.	Time	Source	Destination	Protocol	Length	Info
908	18.433589	10.1.1.123	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=16/4096, ttl=128 (reply in 909)
909	18.437194	8.8.8.8	10.1.1.123	ICMP	74	Echo (ping) reply id=0x0001, seq=16/4096, ttl=113 (request in 908)
928	19.449913	10.1.1.123	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=17/4352, ttl=128 (reply in 929)
929	19.453359	8.8.8.8	10.1.1.123	ICMP	74	Echo (ping) reply id=0x0001, seq=17/4352, ttl=113 (request in 928)
936	20.477737	10.1.1.123	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=18/4608, ttl=128 (reply in 937)
937	20.481297	8.8.8.8	10.1.1.123	ICMP	74	Echo (ping) reply id=0x0001, seq=18/4608, ttl=113 (request in 936)
950	21.509013	10.1.1.123	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=19/4864, ttl=128 (reply in 951)
951	21.512540	8.8.8.8	10.1.1.123	ICMP	74	Echo (ping) reply id=0x0001, seq=19/4864, ttl=113 (request in 950)

> Frame 908: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF\_{412010BB-CAFC-4CA1-A892-2CCFFD71C5A8}, id 0  
> Ethernet II, Src: PcsCompu\_26:18:82 (08:00:27:26:18:82), Dst: Comtrend\_69:02:c3 (f8:8e:85:69:02:c3)  
> Internet Protocol Version 4, Src: 10.1.1.123, Dst: 8.8.8.8  
> Internet Control Message Protocol

0000 f8 8e 85 69 02 c3 08 00 27 26 18 82 08 00 45 00 ...i.... '&....E.  
0010 00 3c 0a 9c 00 00 80 01 00 00 0a 01 01 7b 08 08 ...<.....{..  
0020 08 08 08 00 4d 4b 00 01 00 10 61 62 63 64 65 66 ...MK... ..abcdef  
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ..ghijklmn opqrstuv  
0040 77 61 62 63 64 65 66 67 68 69 ..wabcdefg hi

Internet Control Message Protocol (icmp), 40 byte(s) | Paquetes: 1391 · Mostrado: 8 (0.6%) · Perdido: 0 (0.0%) | Perfil: Default

```
C:\Users\alumno>
C:\Users\alumno>ping 8.8.8.8

Haciendo ping a 8.8.8.8 con 32 bytes de datos:
Respuesta desde 8.8.8.8: bytes=32 tiempo=3ms TTL=113
Respuesta desde 8.8.8.8: bytes=32 tiempo=3ms TTL=113
Respuesta desde 8.8.8.8: bytes=32 tiempo=3ms TTL=113
Respuesta desde 8.8.8.8: bytes=32 tiempo=3ms TTL=113

Estadísticas de ping para 8.8.8.8:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 3ms, Máximo = 3ms, Media = 3ms

C:\Users\alumno>_
```

En esta parte del ejercicio hemos aplicado otro filtro del WireShark, el filtro usado es la **IP destino** del Ping, pero también se puede filtrar por el **protocolo ICMP**.

Broadcast:

Datos capa de enlace:

ARP	0x0800
-----	--------



## Conversación ping:

The image shows a Windows command prompt window titled "Símbolo del sistema" and a Wireshark network traffic capture window. The command prompt shows the execution of a ping command to 8.8.8.8, displaying the results of four successful pings and the statistics.

Microsoft Windows [Versión 10.0.22000.978]  
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\veron>ping 8.8.8.8

Haciendo ping a 8.8.8.8 con 32 bytes de datos:  
Respuesta desde 8.8.8.8: bytes=32 tiempo=5ms TTL=119  
Respuesta desde 8.8.8.8: bytes=32 tiempo=7ms TTL=119  
Respuesta desde 8.8.8.8: bytes=32 tiempo=6ms TTL=119  
Respuesta desde 8.8.8.8: bytes=32 tiempo=8ms TTL=119

Estadísticas de ping para 8.8.8.8:  
Paquetes: enviados = 4, recibidos = 4, perdidos = 0  
(0% perdidos),  
Tiempos aproximados de ida y vuelta en milisegundos:  
Mínimo = 5ms, Máximo = 8ms, Media = 6ms

C:\Users\veron>

The Wireshark window shows a capture of the network traffic. The filter is set to "ip.addr == 8.8.8.8". The packet list shows four ICMP Echo (ping) requests and four replies, all from 192.168.1.111 to 8.8.8.8.

No.	Time	Source	Destination	Protocol	Length	Info
40	7.698353	192.168.1.111	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128 (reply in 41)
41	7.703920	8.8.8.8	192.168.1.111	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=119 (request in 40)
42	8.715190	192.168.1.111	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128 (reply in 43)
43	8.722332	8.8.8.8	192.168.1.111	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=119 (request in 42)
53	9.718304	192.168.1.111	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128 (reply in 54)
54	9.724934	8.8.8.8	192.168.1.111	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=119 (request in 53)
58	10.722310	192.168.1.111	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (reply in 59)
59	10.730273	8.8.8.8	192.168.1.111	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=119 (request in 58)