

REDES DE LOS COMPUTADORES

PRÁCTICA 1

INTRODUCCIÓN

En esta primera práctica se pretende introducir en las redes de computadores de forma práctica. Para ello se analizará el estudio de una Red de Área Local (LAN) que emplea la arquitectura de red TCP/IP. Esta arquitectura de red se ha convertido en un estándar para los sistemas de transmisión de datos actuales y proporciona la tecnología base para multitud de aplicaciones: correo electrónico, servidores WWW, servidores FTP, videostreaming, etc

CUESTIONES (ANÁLISIS DE UNA CAPTURA DE DATOS)

En las siguientes capturas de pantalla se responderán a las preguntas realizadas en el documento iniciales, a continuación se indicará los filtros que se han ido usando para la realización del ejercicio:

Tráfico de Difusión o 'broadcast'

En el cuadro de filtros indicar `eth.dst == FF:FF:FF:FF:FF:FF`

Filtro por dirección IP en general

José Ángel Berná Galiano. DFISTS. Universidad de Alicante

En el cuadro de filtros indicar: `ip.addr == 193.145.233.8`

Filtro por dirección IP destino

En el cuadro de filtros indicar: `ip.dst == 193.145.233.8`

Filtro por dirección IP origen

En el cuadro de filtros indicar: `ip.src == 193.145.233.8`

Filtro por dirección IP destino y origen

En el cuadro de filtros indicar: `ip.dst == 193.145.233.8 and ip.src == 172.20.43.203`

Filtrado de todos los paquetes IP con el campo TTL mayor o igual a 64

En el cuadro de filtros indicar: `ip.ttl >= 0x40` o `ip.ttl >= 64`.

Filtrado de todos los paquetes IP que contengan el texto aula24

En el cuadro de filtros indicar: `ip contains "aula24"`.

Cuestión 1: Calcula el porcentaje de paquetes ethernet de difusión existentes en la captura. (paquetes de difusión/paquetes totales * 100).

eth.dst == FF:FF:FF:FF:FF:FF						
No.	Time	Source	Destination	Protocol	Length	Info
456	31.599606	172.20.43.204	172.20.43.255	UDP	82	51093 → 1947 Len=40
466	32.491801	172.20.43.216	172.20.43.255	UDP	82	63454 → 1947 Len=40
479	33.393316	172.20.43.199	172.20.43.255	UDP	82	53156 → 1947 Len=40
495	36.408388	172.20.43.206	172.20.43.255	UDP	82	54378 → 1947 Len=40
504	36.430955	172.20.43.210	172.20.43.255	UDP	82	62687 → 1947 Len=40
518	36.477715	172.20.43.223	172.20.43.255	UDP	82	55060 → 1947 Len=40
553	37.948807	172.20.43.219	172.20.43.255	UDP	82	60176 → 1947 Len=40
567	38.123620	172.20.43.228	172.20.43.255	UDP	82	54406 → 1947 Len=40
585	39.740874	172.20.43.212	172.20.43.255	UDP	82	61468 → 1947 Len=40
627	41.568947	172.20.43.225	172.20.43.255	UDP	82	54008 → 1947 Len=40
639	42.474214	172.20.43.226	172.20.43.255	UDP	82	53101 → 1947 Len=40
660	43.247397	172.20.43.215	172.20.43.255	UDP	82	61644 → 1947 Len=40
> Frame 660: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) > Ethernet II, Src: Giga-Byt_04:cc:6a (18:c0:4d:04:cc:6a), Dst: Broadcast (ff:ff:ff:ff:ff:ff) > Internet Protocol Version 4, Src: 172.20.43.215, Dst: 172.20.43.255 > User Datagram Protocol, Src Port: 61644, Dst Port: 1947 > Data (40 bytes)						

Paquetes: 732 · Mostrado: 47 (6.4%)

Perfil: Default

Cuestión 2: Calcula el porcentaje de paquetes IP existentes en la captura.

ip.addr == 172.20.43.212						
No.	Time	Source	Destination	Protocol	Length	Info
640	42.798657	172.20.43.212	172.25.40.31	ICMP	106	Echo (ping) request id=0x0001, seq=118/30208, ttl=2 (reply in 641)
641	42.821349	172.25.40.31	172.20.43.212	ICMP	106	Echo (ping) reply id=0x0001, seq=118/30208, ttl=254 (request in 640)
642	42.821905	172.20.43.212	172.25.40.31	ICMP	106	Echo (ping) request id=0x0001, seq=119/30464, ttl=2 (reply in 643)
643	42.851596	172.25.40.31	172.20.43.212	ICMP	106	Echo (ping) reply id=0x0001, seq=119/30464, ttl=254 (request in 642)
644	42.852173	172.20.43.212	172.25.40.31	ICMP	106	Echo (ping) request id=0x0001, seq=120/30720, ttl=2 (reply in 647)
645	42.861879	152.199.19.74	172.20.43.212	TCP	60	80 → 55111 [ACK] Seq=1 Ack=1 Win=133 Len=0
646	42.861898	172.20.43.212	152.199.19.74	TCP	54	[TCP ACKed unseen segment] 55111 → 80 [ACK] Seq=1 Ack=2 Win=1023 Len=0
647	42.882081	172.25.40.31	172.20.43.212	ICMP	106	Echo (ping) reply id=0x0001, seq=120/30720, ttl=254 (request in 644)
648	42.882992	172.20.43.212	193.145.233.5	DNS	85	Standard query 0x4e1b PTR 31.40.25.172.in-addr.arpa
649	42.914074	172.20.43.212	193.145.233.6	DNS	85	Standard query 0x4e1b PTR 31.40.25.172.in-addr.arpa
650	42.922586	193.145.233.5	172.20.43.212	DNS	142	Standard query response 0x4e1b No such name PTR 31.40.25.172.in-addr.arpa SOA aitana.cpd.ua.es
651	42.952963	193.145.233.6	172.20.43.212	DNS	142	Standard query response 0x4e1b No such name PTR 31.40.25.172.in-addr.arpa SOA aitana.cpd.ua.es
> Frame 651: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) > Ethernet II, Src: ca:02:2f:3a:00:00 (ca:02:2f:3a:00:00), Dst: Giga-Byt_07:ad:c1 (18:c0:4d:07:ad:c1) > Internet Protocol Version 4, Src: 193.145.233.6, Dst: 172.20.43.212 > User Datagram Protocol, Src Port: 53, Dst Port: 54162 > Domain Name System (response)						

Paquetes: 732 · Mostrado: 202 (27.6%)

Cuestión 3: Calcula el porcentaje de paquetes no IP existentes en la captura

ip.addr != 172.20.43.212						
No.	Time	Source	Destination	Protocol	Length	Info
640	42.798657	172.20.43.212	172.25.40.31	ICMP	106	Echo (ping) request id=0x0001, seq=118/30208, ttl=2 (reply in 641)
641	42.821349	172.25.40.31	172.20.43.212	ICMP	106	Echo (ping) reply id=0x0001, seq=118/30208, ttl=254 (request in 640)
642	42.821905	172.20.43.212	172.25.40.31	ICMP	106	Echo (ping) request id=0x0001, seq=119/30464, ttl=2 (reply in 643)
643	42.851596	172.25.40.31	172.20.43.212	ICMP	106	Echo (ping) reply id=0x0001, seq=119/30464, ttl=254 (request in 642)
644	42.852173	172.20.43.212	172.25.40.31	ICMP	106	Echo (ping) request id=0x0001, seq=120/30720, ttl=2 (reply in 647)
645	42.861879	152.199.19.74	172.20.43.212	TCP	60	80 → 55111 [ACK] Seq=1 Ack=1 Win=133 Len=0
646	42.861898	172.20.43.212	152.199.19.74	TCP	54	[TCP ACKed unseen segment] 55111 → 80 [ACK] Seq=1 Ack=2 Win=1023 Len=0
647	42.882081	172.25.40.31	172.20.43.212	ICMP	106	Echo (ping) reply id=0x0001, seq=120/30720, ttl=254 (request in 644)
648	42.882992	172.20.43.212	193.145.233.5	DNS	85	Standard query 0x4e1b PTR 31.40.25.172.in-addr.arpa
649	42.914074	172.20.43.212	193.145.233.6	DNS	85	Standard query 0x4e1b PTR 31.40.25.172.in-addr.arpa
650	42.922586	193.145.233.5	172.20.43.212	DNS	142	Standard query response 0x4e1b No such name PTR 31.40.25.172.in-addr.arpa SOA aitana.cpd.ua.es
651	42.952963	193.145.233.6	172.20.43.212	DNS	142	Standard query response 0x4e1b No such name PTR 31.40.25.172.in-addr.arpa SOA aitana.cpd.ua.es
> Frame 651: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) > Ethernet II, Src: ca:02:2f:3a:00:00 (ca:02:2f:3a:00:00), Dst: Giga-Byt_07:ad:c1 (18:c0:4d:07:ad:c1) > Internet Protocol Version 4, Src: 193.145.233.6, Dst: 172.20.43.212 > User Datagram Protocol, Src Port: 53, Dst Port: 54162 > Domain Name System (response)						

Paquetes: 732 · Mostrado: 296 (40.4%)

Cuestión 4: Calcula el porcentaje de paquetes IP enviados por el equipo del alumno.

ip.dst == 172.20.43.212						
No.	Time	Source	Destination	Protocol	Length	Info
604	40.299721	172.20.43.230	172.20.43.212	ICMP	70	Destination unreachable (Port unreachable)
605	40.299727	172.25.2.99	172.20.43.212	HTTP	1514	Continuation
607	40.338046	172.25.2.99	172.20.43.212	TCP	1514	[TCP Out-Of-Order] 1947 → 55131 [ACK] Seq=1461 Ack=1304 Win=65536 Len=1460
609	40.340131	172.25.2.99	172.20.43.212	HTTP	1514	[TCP Spurious Retransmission] Continuation
612	40.662945	172.25.2.99	172.20.43.212	HTTP	1514	Continuation
628	41.641292	172.25.2.99	172.20.43.212	HTTP	1514	Continuation
641	42.821349	172.25.40.31	172.20.43.212	ICMP	106	Echo (ping) reply id=0x0001, seq=118/30208, ttl=254 (request in 640)
643	42.851596	172.25.40.31	172.20.43.212	ICMP	106	Echo (ping) reply id=0x0001, seq=119/30464, ttl=254 (request in 642)
645	42.861879	152.199.19.74	172.20.43.212	TCP	60	80 → 55111 [ACK] Seq=1 Ack=1 Win=133 Len=0
647	42.882081	172.25.40.31	172.20.43.212	ICMP	106	Echo (ping) reply id=0x0001, seq=120/30720, ttl=254 (request in 644)
650	42.922586	193.145.233.5	172.20.43.212	DNS	142	Standard query response 0x4e1b No such name PTR 31.40.25.172.in-addr.arpa SOA aitana.cpd.ua.es
651	42.952963	193.145.233.6	172.20.43.212	DNS	142	Standard query response 0x4e1b No such name PTR 31.40.25.172.in-addr.arpa SOA aitana.cpd.ua.es
Frame 651: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface eth0						
Ethernet II, Src: ca:02:2f:3a:00:00 (ca:02:2f:3a:00:00), Dst: Giga-Byt_07:ad:c1 (18:c0:4d:07:ad:c1)						
Internet Protocol Version 4, Src: 193.145.233.6, Dst: 172.20.43.212						
User Datagram Protocol, Src Port: 53, Dst Port: 54162						
Domain Name System (response)						

Paquetes: 732 · Mostrado: 94 (12.8%)

Cuestión 5: Calcula el porcentaje de paquetes IP recibidos por el equipo del alumno

ip.src == 172.20.43.212						
No.	Time	Source	Destination	Protocol	Length	Info
604	40.299721	172.20.43.230	172.20.43.212	ICMP	70	Destination unreachable (Port unreachable)
605	40.299727	172.25.2.99	172.20.43.212	HTTP	1514	Continuation
607	40.338046	172.25.2.99	172.20.43.212	TCP	1514	[TCP Out-Of-Order] 1947 → 55131 [ACK] Seq=1461 Ack=1304 Win=65536 Len=1460
609	40.340131	172.25.2.99	172.20.43.212	HTTP	1514	[TCP Spurious Retransmission] Continuation
612	40.662945	172.25.2.99	172.20.43.212	HTTP	1514	Continuation
628	41.641292	172.25.2.99	172.20.43.212	HTTP	1514	Continuation
641	42.821349	172.25.40.31	172.20.43.212	ICMP	106	Echo (ping) reply id=0x0001, seq=118/30208, ttl=254 (request in 640)
643	42.851596	172.25.40.31	172.20.43.212	ICMP	106	Echo (ping) reply id=0x0001, seq=119/30464, ttl=254 (request in 642)
645	42.861879	152.199.19.74	172.20.43.212	TCP	60	80 → 55111 [ACK] Seq=1 Ack=1 Win=133 Len=0
647	42.882081	172.25.40.31	172.20.43.212	ICMP	106	Echo (ping) reply id=0x0001, seq=120/30720, ttl=254 (request in 644)
650	42.922586	193.145.233.5	172.20.43.212	DNS	142	Standard query response 0x4e1b No such name PTR 31.40.25.172.in-addr.arpa SOA aitana.cpd.ua.es
651	42.952963	193.145.233.6	172.20.43.212	DNS	142	Standard query response 0x4e1b No such name PTR 31.40.25.172.in-addr.arpa SOA aitana.cpd.ua.es
Frame 651: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface eth0						
Ethernet II, Src: ca:02:2f:3a:00:00 (ca:02:2f:3a:00:00), Dst: Giga-Byt_07:ad:c1 (18:c0:4d:07:ad:c1)						
Internet Protocol Version 4, Src: 193.145.233.6, Dst: 172.20.43.212						
User Datagram Protocol, Src Port: 53, Dst Port: 54162						
Domain Name System (response)						

Paquetes: 732 · Mostrado: 114 (15.6%)

Cuestión 6: Visualiza los paquetes IP que contengan la cadena 'Sistemas'. ¿ Con qué aplicación están relacionados ?

ip contains "Sistemas"						
No.	Time	Source	Destination	Protocol	Length	Info
344	21.084811	172.25.32.166	172.20.43.212	HTTP	502	HTTP/1.1 200 OK (text/html)
351	21.165960	172.25.32.166	172.20.43.212	HTTP	502	HTTP/1.1 200 OK (text/html)
Frame 344: 502 bytes on wire (4016 bits), 502 bytes captured (4016 bits) on interface \Device\NPF_{87194A3C-C304-4745-9373-216E7B1D7C13}, id 0						
Ethernet II, Src: ca:02:2f:3a:00:00 (ca:02:2f:3a:00:00), Dst: Giga-Byt_07:ad:c1 (18:c0:4d:07:ad:c1)						
Internet Protocol Version 4, Src: 172.25.32.166, Dst: 172.20.43.212						
Transmission Control Protocol, Src Port: 80, Dst Port: 55853, Seq: 1, Ack: 317, Len: 448						
Hypertext Transfer Protocol						
Line-based text data: text/html (6 lines)						

Cuestión 7: Determina la dirección IP del servidor web www.dfists.ua.es.

Con la captura anterior podemos observar que el ip es el siguiente: 172.25.32.166

Cuestión 8: Visualiza todos los paquetes IP que contengan la cadena 'abcd' y sean intercambiados con la dirección IP de tu máquina.

ip.addr == 172.20.43.212 && data contains "abcd"						
No.	Time	Source	Destination	Protocol	Length	Info
140	9.304442000	172.20.43.212	172.20.43.230	ICMP	74	Echo (ping) request
141	9.313451000	172.20.43.230	172.20.43.212	ICMP	74	Echo (ping) reply
144	10.314568000	172.20.43.212	172.20.43.230	ICMP	74	Echo (ping) request
146	10.322340000	172.20.43.230	172.20.43.212	ICMP	74	Echo (ping) reply
149	11.332272000	172.20.43.212	172.20.43.230	ICMP	74	Echo (ping) request
151	11.340839000	172.20.43.230	172.20.43.212	ICMP	74	Echo (ping) reply
168	12.335039000	172.20.43.212	172.20.43.230	ICMP	74	Echo (ping) request
170	12.339333000	172.20.43.230	172.20.43.212	ICMP	74	Echo (ping) reply
308	21.295959000	172.20.43.212	172.20.43.230	IPv4	1514	Fragmented IP protoc
309	21.295959000	172.20.43.212	172.20.43.230	ICMP	162	Echo (ping) request
310	21.301517000	172.20.43.230	172.20.43.212	IPv4	1514	Fragmented IP protoc
311	21.301517000	172.20.43.230	172.20.43.212	ICMP	162	Echo (ping) reply
329	22.307621000	172.20.43.212	172.20.43.230	IPv4	1514	Fragmented IP protoc
330	22.307621000	172.20.43.212	172.20.43.230	ICMP	162	Echo (ping) request
331	22.311274000	172.20.43.230	172.20.43.212	IPv4	1514	Fragmented IP protoc
332	22.311274000	172.20.43.230	172.20.43.212	ICMP	162	Echo (ping) reply
340	23.310284000	172.20.43.212	172.20.43.230	IPv4	1514	Fragmented IP protoc
341	23.310284000	172.20.43.212	172.20.43.230	ICMP	162	Echo (ping) request

Paquetes: 732 · Mostrado: 24 (3.3%)

Cuestión 9: Respecto a los paquetes obtenidos en el apartado anterior, ¿pertenecen a algún protocolo en concreto? Explica qué aplicación o programa ha podido generar esos paquetes.

<ul style="list-style-type: none"> Internet Protocol Version 4, Src: 172.20.43.212, Dst: 172.20.43.230 <ul style="list-style-type: none"> 0100 = Version: 4 0101 = Header Length: 20 bytes (5) > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) <ul style="list-style-type: none"> Total Length: 60 Identification: 0x3cd0 (15568) > 000. = Flags: 0x0 <ul style="list-style-type: none"> ...0 0000 0000 0000 = Fragment Offset: 0 Time to Live: 128 Protocol: ICMP (1) Header Checksum: 0x0000 [validation disabled] [Header checksum status: Unverified] Source Address: 172.20.43.212 Destination Address: 172.20.43.230 > Internet Control Message Protocol
--

Cuestión 10: Visualiza aquellos paquetes que contengan el campo protocolo de la cabecera IP igual a 17.

Utilizamos el siguiente filtro el cual el 17 nos indica del valor de UDP.

ip.proto == 17				
No.	Time	Source	Destination	Protocol
123	8.583023000	172.20.43.207	224.0.0.251	MDNS
126	8.583393000	172.20.43.207	224.0.0.252	LLMNR
128	8.583550000	172.20.43.207	224.0.0.252	LLMNR
129	8.584007000	172.20.43.207	172.20.43.255	UDP
130	8.675287000	172.20.43.215	224.0.0.251	MDNS
132	8.675701000	172.20.43.215	224.0.0.251	MDNS
135	8.676142000	172.20.43.215	224.0.0.252	LLMNR
137	8.676334000	172.20.43.215	224.0.0.252	LLMNR

Cuestión 11: Visualiza todos los paquetes que contengan el campo TTL (Time to Live) de la cabecera IP igual a 1.

ip.ttl == 1						
No.	Time	Source	Destination	Protocol	Length	Info
120	8.477068000	172.20.43.213	239.255.255.250	SSDP	217	M-SEARCH * HT
121	8.582721000	172.20.43.207	224.0.0.251	MDNS	79	Standard quer
123	8.583023000	172.20.43.207	224.0.0.251	MDNS	79	Standard quer
126	8.583393000	172.20.43.207	224.0.0.252	LLMNR	73	Standard quer
128	8.583550000	172.20.43.207	224.0.0.252	LLMNR	73	Standard quer
130	8.675287000	172.20.43.215	224.0.0.251	MDNS	79	Standard quer
132	8.675701000	172.20.43.215	224.0.0.251	MDNS	79	Standard quer
135	8.676142000	172.20.43.215	224.0.0.252	LLMNR	73	Standard quer

```

> Frame 100: 79 bytes on wire (632 bits), 79 bytes captured (632 bits)
> Ethernet II, Src: Giga-Byt_05:d2:c1 (18:c0:4d:05:d2:c1), Dst: IPv4mcast_fb (01:00:5e:00:00:fb)
> Internet Protocol Version 4, Src: 172.20.43.225, Dst: 224.0.0.251
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 65
    Identification: 0xc28d (49805)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 1
    Protocol: UDP (17)
    Header Checksum: 0x3e2e [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.20.43.225
    Destination Address: 224.0.0.251
  > User Datagram Protocol, Src Port: 5353, Dst Port: 5353
  > Multicast Domain Name System (query)

```

```

0000  01 00 5e 00 00 fb 18 c0 4d 05 d2 c1 08 00 45 00  --^...M.....E-
0010  00 41 c2 8d 00 00 01 11 3e 2e ac 14 2b e1 e0 00  -A.....>...+...
0020  00 fb 14 e9 14 e9 00 2d a7 8a 00 00 00 00 00 01  -.....s rvroscsi
0030  00 00 00 00 00 00 0d 73 72 76 72 6f 63 73 63 69  -.....ence-loc al....
0040  65 6e 63 65 05 6c 6f 63 61 6c 00 00 1c 00 01

```

Cuestión 12: Visualiza todos los paquetes que contengan el campo TTL (Time to Live) de la cabecera IP igual a 2.

ip.ttl == 2							
No.		Source	Destination	Protocol	Length	Info	
640	42.798657000	172.20.43.212	172.25.40.31	ICMP	106	Echo (ping	
642	42.821905000	172.20.43.212	172.25.40.31	ICMP	106	Echo (ping	
644	42.852173000	172.20.43.212	172.25.40.31	ICMP	106	Echo (ping	

> Frame 640: 106 bytes on wire (8480 bits) captured (106 bytes) over interface 0

> Ethernet II, Src: Giga-Byt_08:00:27:00:00:00, Dst: Realtek_08:00:27:00:00:00

> Internet Protocol Version 4, Src: 172.20.43.212, Dst: 172.25.40.31

> ICMP Echo (ping request), Id: 0, Seq: 1

> Time to Live: 2

> Payload: ICMP Echo (ping request) data

0000

ca 02 2f 3a 00 00 18 c0 4d 07 ad c1 08 00 45 00

0010

00 5c 32 7e 00 00 02 01 00 00 ac 14 2b d4 ac 19

0020

28 1f 08 00 f7 88 00 01 00 76 00 00 00 00 00 00

0030

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0040

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0050

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0060

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Cuestión 13: Respecto de los apartados 11 y 12, ¿Qué protocolo aparece? ¿Qué aplicación puede haberlos generado y por qué?

Los campos TTL (Time to Live) de la cabecera IP indican el número de saltos o enrutadores que un paquete puede atravesar antes de ser descartado. Cuando el TTL alcanza un valor de 1 o 2, significa que el paquete puede realizar un número muy limitado de saltos antes de ser eliminado.

Cuestión 14: Determina qué porcentaje de los paquetes IP capturados están fragmentados (paquetes con el bit MORE FRAGMENTS activo)

ip.flags.mf == 1							
No.	Time	Source	Destination	Protocol	Length	Info	
308	21.295959000	172.20.43.230	172.20.43.230	IPv4	1514	Fragmented IP protocol (p	
310	21.301517000	172.20.43.230	172.20.43.212	IPv4	1514	Fragmented IP protocol (p	
329	22.307621000	172.20.43.212	172.20.43.230	IPv4	1514	Fragmented IP protocol (p	
331	22.311274000	172.20.43.230	172.20.43.212	IPv4	1514	Fragmented IP protocol (p	
340	23.310284000	172.20.43.212	172.20.43.230	IPv4	1514	Fragmented IP protocol (p	
342	23.320801000	172.20.43.230	172.20.43.212	IPv4	1514	Fragmented IP protocol (p	
355	24.328289000	172.20.43.212	172.20.43.230	IPv4	1514	Fragmented IP protocol (p	
357	24.330242000	172.20.43.230	172.20.43.212	IPv4	1514	Fragmented IP protocol (p	

Paquetes: 732 · Mostrado: 8 (1.1%)

PÁGINA 6

CUESTIONES (PROTOCOLO ARP)

Antes de la realización de las cuestiones se deberán de emplearon una serie de comandos lo cuales también se indicará que hará cada uno:

ipconfig /all: Este comando muestra información detallada de la configuración de red de tu computadora. Proporciona detalles sobre la dirección IP, la máscara de subred, la puerta de enlace predeterminada, las conexiones de red activas y más.

netstat -rn: Este comando muestra la tabla de enrutamiento de tu computadora. Proporciona información sobre cómo se dirigen los paquetes de datos en la red, incluyendo las rutas hacia las diferentes redes y la puerta de enlace predeterminada.

route delete 0.0.0.0: Este comando se utiliza para eliminar una ruta de red predeterminada o una puerta de enlace predeterminada de la tabla de enrutamiento. El 0.0.0.0 es una representación común de la puerta de enlace predeterminada.

ipconfig /release: Este comando libera todas las direcciones IP asignadas a tu computadora por servidores DHCP (Protocolo de Configuración Dinámica de Host). Básicamente, desconecta tu computadora de la red.

ipconfig /renew: Después de usar ipconfig /release, puedes utilizar este comando para renovar las direcciones IP asignadas por un servidor DHCP. Tu computadora solicitará una nueva dirección IP al servidor DHCP de la red.

En las siguientes imágenes se muestra las capturas una vez se hayan ejecutando los comandos:

```
C:\>ipconfig/all

Configuración IP de Windows

Nombre de host. . . . . : clt24-15
Sufijo DNS principal . . . . . :
Tipo de nodo. . . . . : híbrido
Enrutamiento IP habilitado. . . : no
Proxy WINS habilitado . . . . . : no

Adaptador de Ethernet Ethernet:

Sufijo DNS específico para la conexión. . :
Descripción . . . . . : Realtek PCIe GbE Family Controller
Dirección física. . . . . : 18-C0-4D-07-AD-C1
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . : sí
Vínculo: dirección IPv6 local. . . : fe80::76ff:9bd8:d97e:49f%11(Preferido)
Dirección IPv4. . . . . : 172.20.43.212(Preferido)
Máscara de subred. . . . . : 255.255.255.192
Concesión obtenida. . . . . : miércoles, 20 de septiembre de 2023 15:06:48
La concesión expira . . . . . : jueves, 28 de septiembre de 2023 15:06:48
Puerta de enlace predeterminada . . . : 172.20.43.230
Servidor DHCP . . . . . : 172.25.2.42
IAID DHCPv6 . . . . . : 85508173
DUID de cliente DHCPv6. . . . . : 00-01-00-01-2C-4B-13-60-18-C0-4D-07-AD-C1
Servidores DNS. . . . . : 193.145.233.5
                          193.145.233.6
NetBIOS sobre TCP/IP. . . . . : habilitado

Adaptador de Ethernet VirtualBox Host-Only Network:

Sufijo DNS específico para la conexión. . :
Descripción . . . . . : VirtualBox Host-Only Ethernet Adapter
Dirección física. . . . . : 0A-00-27-00-00-11
DHCP habilitado . . . . . : no
Configuración automática habilitada . . : sí
Vínculo: dirección IPv6 local. . . : fe80::91c7:9b8a:2d70:bc77%17(Preferido)
Dirección IPv4. . . . . : 192.168.56.1(Preferido)
Máscara de subred. . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . :
Servidor DHCPv6 . . . . . : 470417447
DUID de cliente DHCPv6. . . . . : 00-01-00-01-2C-4B-13-60-18-C0-4D-07-AD-C1
Servidores DNS. . . . . : fec0:0:0:ffff::1%1
                          fec0:0:0:ffff::2%1
                          fec0:0:0:ffff::3%1
NetBIOS sobre TCP/IP. . . . . : habilitado

C:\>
```

```
C:\>netstat -rn

=====
Lista de interfaces
11...18 c0 4d 07 ad c1 .....Realtek PCIe GbE Family Controller
17...0a 00 27 00 00 11 .....VirtualBox Host-Only Ethernet Adapter
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             172.20.43.230         172.20.43.212  26
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
172.20.43.192       255.255.255.192     En vínculo            172.20.43.212  281
172.20.43.212       255.255.255.255     En vínculo            172.20.43.212  281
172.20.43.255       255.255.255.255     En vínculo            172.20.43.212  281
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            172.20.43.212  281
255.255.255.255     255.255.255.255     En vínculo            127.0.0.1      331

C:\>route delete 0.0.0.0
Correcto

C:\>ipconfig /release

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

Sufijo DNS específico para la conexión. . :
Vínculo: dirección IPv6 local. . . : fe80::76ff:9bd8:d97e:49f%11
Puerta de enlace predeterminada . . . :

Adaptador de Ethernet VirtualBox Host-Only Network:

Sufijo DNS específico para la conexión. . :
Vínculo: dirección IPv6 local. . . : fe80::91c7:9b8a:2d70:bc77%17
Dirección IPv4. . . . . : 192.168.56.1
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . :

C:\>
```


Cuestión 1: Verifica la presencia de paquetes ARP en la red ejecutando el comando ping -n 1 172.20.43.231 y que la secuencia de las mismas se corresponde con la descrita en el enunciado de la práctica.

```
C:\>ping -n 1 172.20.43.231

Haciendo ping a 172.20.43.231 con 32 bytes de datos:
Respuesta desde 172.20.43.231: bytes=32 tiempo=8ms TTL=255

Estadísticas de ping para 172.20.43.231:
    Paquetes: enviados = 1, recibidos = 1, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 8ms, Máximo = 8ms, Media = 8ms
```

```
C:\>ping -n 1 172.20.43.231

Haciendo ping a 172.20.43.231 con 32 bytes de datos:
Respuesta desde 172.20.43.231: bytes=32 tiempo=13ms TTL=255

Estadísticas de ping para 172.20.43.231:
    Paquetes: enviados = 1, recibidos = 1, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 13ms, Máximo = 13ms, Media = 13ms
```

```
C:\>arp -a

Interfaz: 172.20.43.212 --- 0xb
Dirección de Internet      Dirección física      Tipo
172.20.43.213              18-c0-4d-07-ad-f9    dinámico
172.20.43.219              18-c0-4d-02-19-f8    dinámico
172.20.43.227              18-c0-4d-05-dd-37    dinámico
172.20.43.230              ca-02-2f-3a-00-00    dinámico
172.20.43.231              ca-05-71-85-00-00    dinámico
172.20.43.255              ff-ff-ff-ff-ff-ff    estático
224.0.0.5                  01-00-5e-00-00-05    estático
224.0.0.13                 01-00-5e-00-00-0d    estático
224.0.0.22                 01-00-5e-00-00-16    estático
224.0.0.251                01-00-5e-00-00-fb    estático
224.0.0.252                01-00-5e-00-00-fc    estático
239.255.255.250            01-00-5e-7f-ff-fa    estático

Interfaz: 192.168.56.1 --- 0x11
Dirección de Internet      Dirección física      Tipo
192.168.56.255             ff-ff-ff-ff-ff-ff    estático
224.0.0.1                  01-00-5e-00-00-01    estático
224.0.0.5                  01-00-5e-00-00-05    estático
224.0.0.13                 01-00-5e-00-00-0d    estático
224.0.0.22                 01-00-5e-00-00-16    estático
224.0.0.251                01-00-5e-00-00-fb    estático
224.0.0.252                01-00-5e-00-00-fc    estático
255.255.255.255            ff-ff-ff-ff-ff-ff    estático
```

Cuestión 2: Verifica el funcionamiento de ARP enviando un paquete IP a la máquina de tu compañero. Ejecuta el comando ping -n 1 IP_compañero y determina los paquetes ARP y mensajes ICMP Echo Request e ICMP Echo Reply que aparecen.

```
C:\>arp -a

Interfaz: 172.20.43.213 --- 0xb
Dirección de Internet      Dirección física      Tipo
172.20.43.195             d8-84-66-77-44-9a    dinámico
172.20.43.198             18-c0-4d-07-bd-94    dinámico
172.20.43.199             18-c0-4d-01-df-06    dinámico
172.20.43.200             18-c0-4d-05-8f-28    dinámico
172.20.43.201             18-c0-4d-01-e2-67    dinámico
172.20.43.202             18-c0-4d-07-be-f2    dinámico
172.20.43.204             18-c0-4d-04-cc-39    dinámico
172.20.43.205             18-c0-4d-05-8f-5a    dinámico
172.20.43.206             18-c0-4d-07-ad-d4    dinámico
172.20.43.207             18-c0-4d-07-ad-ff    dinámico
172.20.43.209             18-c0-4d-05-dd-29    dinámico
172.20.43.210             18-c0-4d-02-19-c1    dinámico
172.20.43.211             18-c0-4d-01-e6-77    dinámico
172.20.43.212             18-c0-4d-07-ad-c1    dinámico
172.20.43.214             18-c0-4d-05-9e-7b    dinámico
172.20.43.215             18-c0-4d-04-cc-6a    dinámico
172.20.43.217             18-c0-4d-01-e6-79    dinámico
172.20.43.218             18-c0-4d-06-9d-c2    dinámico
172.20.43.220             18-c0-4d-05-d6-b1    dinámico
172.20.43.221             18-c0-4d-07-ad-c0    dinámico
172.20.43.222             18-c0-4d-05-8f-09    dinámico
172.20.43.223             18-c0-4d-05-d2-9f    dinámico
172.20.43.224             18-c0-4d-07-ad-bb    dinámico
172.20.43.225             18-c0-4d-05-d2-c1    dinámico
172.20.43.226             18-c0-4d-07-bd-ac    dinámico
172.20.43.227             18-c0-4d-05-dd-37    dinámico
172.20.43.230             ca-02-2f-3a-00-00    dinámico
172.20.43.255             ff-ff-ff-ff-ff-ff    estático
224.0.0.2                 01-00-5e-00-00-02    estático
224.0.0.5                 01-00-5e-00-00-05    estático
224.0.0.13                01-00-5e-00-00-0d    estático
224.0.0.22                01-00-5e-00-00-16    estático
224.0.0.251               01-00-5e-00-00-fb    estático
224.0.0.252               01-00-5e-00-00-fc    estático
239.255.255.250           01-00-5e-7f-ff-fa    estático
255.255.255.255           ff-ff-ff-ff-ff-ff    estático

Interfaz: 192.168.56.1 --- 0x11
Dirección de Internet      Dirección física      Tipo
192.168.56.255            ff-ff-ff-ff-ff-ff    estático
224.0.0.1                 01-00-5e-00-00-01    estático
224.0.0.2                 01-00-5e-00-00-02    estático
224.0.0.5                 01-00-5e-00-00-05    estático
224.0.0.13                01-00-5e-00-00-0d    estático
224.0.0.22                01-00-5e-00-00-16    estático
224.0.0.251               01-00-5e-00-00-fb    estático
224.0.0.252               01-00-5e-00-00-fc    estático
239.255.255.250           01-00-5e-7f-ff-fa    estático
255.255.255.255           ff-ff-ff-ff-ff-ff    estático

C:\>arp -a

Interfaz: 172.20.43.212 --- 0xb
Dirección de Internet      Dirección física      Tipo
172.20.43.213             18-c0-4d-07-ad-f9    dinámico
172.20.43.219             18-c0-4d-02-19-f8    dinámico
172.20.43.227             18-c0-4d-05-dd-37    dinámico
172.20.43.230             ca-02-2f-3a-00-00    dinámico
172.20.43.255             ff-ff-ff-ff-ff-ff    estático
224.0.0.5                 01-00-5e-00-00-05    estático
224.0.0.13                01-00-5e-00-00-0d    estático
224.0.0.22                01-00-5e-00-00-16    estático
224.0.0.251               01-00-5e-00-00-fb    estático
224.0.0.252               01-00-5e-00-00-fc    estático
224.0.0.252               01-00-5e-00-00-fc    estático
239.255.255.250           01-00-5e-7f-ff-fa    estático
239.255.255.250           01-00-5e-7f-ff-fa    estático

Interfaz: 192.168.56.1 --- 0x11
Dirección de Internet      Dirección física      Tipo
192.168.56.255            ff-ff-ff-ff-ff-ff    estático
224.0.0.1                 01-00-5e-00-00-01    estático
224.0.0.5                 01-00-5e-00-00-05    estático
224.0.0.13                01-00-5e-00-00-0d    estático
224.0.0.22                01-00-5e-00-00-16    estático
224.0.0.251               01-00-5e-00-00-fb    estático
224.0.0.252               01-00-5e-00-00-fc    estático
224.0.0.252               01-00-5e-00-00-fc    estático
255.255.255.255           ff-ff-ff-ff-ff-ff    estático
```

```

C:\>arp -d 172.20.43.231
No se encontró la entrada especificada.

C:\>arp -a 172.20.43.231
No se encontraron entradas ARP.

C:\>arp -a

Interfaz: 172.20.43.213 --- 0xb

```

Dirección de Internet	Dirección física	Tipo
172.20.43.195	d8-84-66-77-44-9a	dinámico
172.20.43.198	18-c0-4d-07-bd-94	dinámico
172.20.43.199	18-c0-4d-01-df-06	dinámico
172.20.43.200	18-c0-4d-05-8f-28	dinámico
172.20.43.201	18-c0-4d-01-e2-67	dinámico
172.20.43.202	18-c0-4d-07-be-f2	dinámico
172.20.43.204	18-c0-4d-04-cc-39	dinámico
172.20.43.205	18-c0-4d-05-8f-5a	dinámico
172.20.43.206	18-c0-4d-07-ad-d4	dinámico
172.20.43.207	18-c0-4d-07-ad-ff	dinámico
172.20.43.209	18-c0-4d-05-dd-29	dinámico
172.20.43.210	18-c0-4d-02-19-c1	dinámico
172.20.43.211	18-c0-4d-01-e6-77	dinámico
172.20.43.212	18-c0-4d-07-ad-c1	dinámico
172.20.43.214	18-c0-4d-05-9e-2b	dinámico
172.20.43.215	18-c0-4d-04-cc-6a	dinámico
172.20.43.217	18-c0-4d-01-e6-79	dinámico
172.20.43.218	18-c0-4d-06-9d-c2	dinámico
172.20.43.220	18-c0-4d-05-d6-b1	dinámico
172.20.43.221	18-c0-4d-07-ad-c0	dinámico
172.20.43.222	18-c0-4d-05-8f-09	dinámico
172.20.43.223	18-c0-4d-05-d2-9f	dinámico
172.20.43.224	18-c0-4d-07-ad-bb	dinámico
172.20.43.225	18-c0-4d-05-d2-c1	dinámico
172.20.43.226	18-c0-4d-07-bd-ac	dinámico
172.20.43.227	18-c0-4d-05-dd-37	dinámico
172.20.43.230	ca-02-2f-3a-00-00	dinámico
172.20.43.255	ff-ff-ff-ff-ff-ff	estático
224.0.0.2	01-00-5e-00-00-02	estático
224.0.0.5	01-00-5e-00-00-05	estático
224.0.0.13	01-00-5e-00-00-0d	estático
224.0.0.22	01-00-5e-00-00-16	estático
224.0.0.251	01-00-5e-00-00-fb	estático
224.0.0.252	01-00-5e-00-00-fc	estático
239.255.255.250	01-00-5e-7f-ff-fa	estático
255.255.255.255	ff-ff-ff-ff-ff-ff	estático

```

Interfaz: 192.168.56.1 --- 0x11

```

Dirección de Internet	Dirección física	Tipo
192.168.56.255	ff-ff-ff-ff-ff-ff	estático
224.0.0.1	01-00-5e-00-00-01	estático
224.0.0.2	01-00-5e-00-00-02	estático
224.0.0.5	01-00-5e-00-00-05	estático
224.0.0.13	01-00-5e-00-00-0d	estático
224.0.0.22	01-00-5e-00-00-16	estático
224.0.0.251	01-00-5e-00-00-fb	estático
224.0.0.252	01-00-5e-00-00-fc	estático
239.255.255.250	01-00-5e-7f-ff-fa	estático
255.255.255.255	ff-ff-ff-ff-ff-ff	estático

```

C:\>

```

Cuestión 3: Verifica el modo de funcionamiento de ARP cuando se envía un datagrama (paquete IP) a otra red. Determina la dirección IP por la que se pregunta en los paquetes ARP Request que genera tu equipo al ejecutar el comando. Ten en cuenta que sólo podrá visualizarse la secuencia ARP correspondiente a tu segmento físico.

```
-C:\>arp -d 172.20.43.230
-
-C:\>ping -n 1 10.4.2.5
-
-Haciendo ping a 10.4.2.5 con 32 bytes de datos:
-Respuesta desde 10.4.2.5: bytes=32 tiempo=28ms TTL=254

Estadísticas de ping para 10.4.2.5:
    Paquetes: enviados = 1, recibidos = 1, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 28ms, Máximo = 28ms, Media = 28ms
```

Cuestión 4: Determina a través de qué estación de la red 172.20.43.192/26 procede el paquete ICMP Echo de respuesta al ejecutar el comando ping a los siguientes destinos. Para ello hay que determinar la dirección MAC de origen del paquete ICMP Echo de respuesta y ver en la tabla caché de ARP a que máquina se corresponde en la red.

```
C:\>ping -n 1 10.4.2.6

Haciendo ping a 10.4.2.6 con 32 bytes de datos:
Respuesta desde 10.4.2.6: bytes=32 tiempo=9ms TTL=255

Estadísticas de ping para 10.4.2.6:
    Paquetes: enviados = 1, recibidos = 1, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 9ms, Máximo = 9ms, Media = 9ms

C:\>ping -n 1 10.4.2.5

Haciendo ping a 10.4.2.5 con 32 bytes de datos:
Respuesta desde 10.4.2.5: bytes=32 tiempo=22ms TTL=254

Estadísticas de ping para 10.4.2.5:
    Paquetes: enviados = 1, recibidos = 1, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 22ms, Máximo = 22ms, Media = 22ms
```

No.	icmp icmpv6	Source	Destination	Protocol	Length	Info
874 69.512414	172.25.2.46	172.20.43.212	ICMP	138	Destination unreachable (Port unreachable)	
995 70.266220	172.25.2.46	172.20.43.212	ICMP	138	Destination unreachable (Port unreachable)	
996 70.266429	172.25.2.46	172.20.43.212	ICMP	138	Destination unreachable (Port unreachable)	
1246 71.037033	172.25.2.46	172.20.43.212	ICMP	138	Destination unreachable (Port unreachable)	
1247 71.037238	172.25.2.46	172.20.43.212	ICMP	138	Destination unreachable (Port unreachable)	
1419 71.801442	172.25.2.46	172.20.43.212	ICMP	138	Destination unreachable (Port unreachable)	
1420 71.801973	172.25.2.46	172.20.43.212	ICMP	138	Destination unreachable (Port unreachable)	
4689 199.780221	172.20.43.212	10.4.2.6	ICMP	74	Echo (ping) request id=0x0001, seq=113/28928, ttl=128 (reply in 4690)	
4690 199.789308	10.4.2.6	172.20.43.212	ICMP	74	Echo (ping) reply id=0x0001, seq=113/28928, ttl=255 (request in 4689)	
4691 199.807809	172.20.43.212	10.4.2.5	ICMP	74	Echo (ping) request id=0x0001, seq=114/29184, ttl=128 (reply in 4692)	
4692 199.829732	10.4.2.5	172.20.43.212	ICMP	74	Echo (ping) reply id=0x0001, seq=114/29184, ttl=254 (request in 4691)	
4693 199.852325	172.20.43.212	10.4.2.2	ICMP	74	Echo (ping) request id=0x0001, seq=115/29440, ttl=128 (reply in 4694)	
4694 199.880188	10.4.2.2	172.20.43.212	ICMP	74	Echo (ping) reply id=0x0001, seq=115/29440, ttl=254 (request in 4693)	
4695 199.900960	172.20.43.212	10.4.2.1	ICMP	74	Echo (ping) request id=0x0001, seq=116/29696, ttl=128 (reply in 4696)	
4696 199.933626	10.4.2.1	172.20.43.212	ICMP	74	Echo (ping) reply id=0x0001, seq=116/29696, ttl=255 (request in 4695)	
4697 199.957925	172.20.43.212	10.3.7.0	ICMP	74	Echo (ping) request id=0x0001, seq=117/29952, ttl=128 (reply in 4703)	
4703 200.193067	10.3.7.0	172.20.43.212	ICMP	74	Echo (ping) reply id=0x0001, seq=117/29952, ttl=253 (request in 4697)	
4704 200.215017	172.20.43.212	10.3.2.0	ICMP	74	Echo (ping) request id=0x0001, seq=118/30208, ttl=128 (reply in 4705)	
4705 200.243605	10.3.2.0	172.20.43.212	ICMP	74	Echo (ping) reply id=0x0001, seq=118/30208, ttl=254 (request in 4704)	

Con las dos capturas donde se puede observar en la primera la ejecución del comando -arp y en el segundo la captura de WireShark podemos observar los broadcast mandados desde mi computador hasta las otras donde se ha hecho el ECHO,

Cuestión 5: Construye una tabla con los valores de las direcciones IP y MAC activas en la red del laboratorio de prácticas (red 172.20.43.192/26). Para ello emplea la aplicación ping con todas las direcciones IP del rango del laboratorio de prácticas.

Construye esta misma tabla para los equipos existentes en la LAN WiFi de tu residencia personal (la red IP a emplear será la del interfaz inalámbrico de tu ordenador portátil o del interfaz Ethernet, dependiendo de tu conectividad en tu residencia).

```
C:\>arp -d 172.20.43.231
No se encontró la entrada especificada.

C:\>arp -a 172.20.43.231
No se encontraron entradas ARP.

C:\>arp -a
```

Dirección de Internet	Dirección física	Tipo
172.20.43.195	d8-84-66-77-44-9a	dinámico
172.20.43.198	18-c0-4d-07-bd-94	dinámico
172.20.43.199	18-c0-4d-01-df-06	dinámico
172.20.43.200	18-c0-4d-05-8f-28	dinámico
172.20.43.201	18-c0-4d-01-e2-67	dinámico
172.20.43.202	18-c0-4d-07-be-f2	dinámico
172.20.43.204	18-c0-4d-04-cc-39	dinámico
172.20.43.205	18-c0-4d-05-8f-5a	dinámico
172.20.43.206	18-c0-4d-07-ad-d4	dinámico
172.20.43.207	18-c0-4d-07-ad-ff	dinámico
172.20.43.209	18-c0-4d-05-dd-29	dinámico
172.20.43.210	18-c0-4d-02-19-c1	dinámico
172.20.43.211	18-c0-4d-01-e6-77	dinámico
172.20.43.212	18-c0-4d-07-ad-c1	dinámico
172.20.43.214	18-c0-4d-05-9e-2b	dinámico
172.20.43.215	18-c0-4d-04-cc-6a	dinámico
172.20.43.217	18-c0-4d-01-e6-79	dinámico
172.20.43.218	18-c0-4d-06-9d-c2	dinámico
172.20.43.220	18-c0-4d-05-d6-b1	dinámico
172.20.43.221	18-c0-4d-07-ad-c0	dinámico
172.20.43.222	18-c0-4d-05-8f-09	dinámico
172.20.43.223	18-c0-4d-05-d2-9f	dinámico
172.20.43.224	18-c0-4d-07-ad-bb	dinámico
172.20.43.225	18-c0-4d-05-d2-c1	dinámico
172.20.43.226	18-c0-4d-07-bd-ac	dinámico
172.20.43.227	18-c0-4d-05-dd-37	dinámico
172.20.43.230	ca-02-2f-3a-00-00	dinámico
172.20.43.255	ff-ff-ff-ff-ff-ff	estático
224.0.0.2	01-00-5e-00-00-02	estático
224.0.0.5	01-00-5e-00-00-05	estático
224.0.0.13	01-00-5e-00-00-0d	estático
224.0.0.22	01-00-5e-00-00-16	estático
224.0.0.251	01-00-5e-00-00-fb	estático
224.0.0.252	01-00-5e-00-00-fc	estático
239.255.255.250	01-00-5e-7f-ff-fa	estático
255.255.255.255	ff-ff-ff-ff-ff-ff	estático

```
Interfaz: 192.168.56.1 --- 0x11
Dirección de Internet      Dirección física      Tipo
192.168.56.255             ff-ff-ff-ff-ff-ff    estático
224.0.0.1                   01-00-5e-00-00-01    estático
224.0.0.2                   01-00-5e-00-00-02    estático
224.0.0.5                   01-00-5e-00-00-05    estático
224.0.0.13                  01-00-5e-00-00-0d    estático
224.0.0.22                  01-00-5e-00-00-16    estático
224.0.0.251                 01-00-5e-00-00-fb    estático
224.0.0.252                 01-00-5e-00-00-fc    estático
239.255.255.250             01-00-5e-7f-ff-fa    estático
255.255.255.255             ff-ff-ff-ff-ff-ff    estático
```

Cuestión 6: Determina la secuencia ARP realizada y los mensajes ICMP intercambiados.
¿Qué podrías afirmar acerca de la estación 172.20.43.235?

Ejecuta los comandos: `Arp -d 172.20.43.235 && Ping -n 1 172.20.43.235`

```
C:\>ipconfig/renew

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::76ff:9bd8:d97e:49f%11
    Dirección IPv4. . . . . : 172.20.43.212
    Máscara de subred . . . . . : 255.255.255.192
    Puerta de enlace predeterminada . . . . . : 172.20.43.195

Adaptador de Ethernet VirtualBox Host-Only Network:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::91c7:9b8a:2d70:bc77%17
    Dirección IPv4. . . . . : 192.168.56.1
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . :

C:\>arp -d 172.20.43.235

C:\>ping -n 1 172.20.43.235

Haciendo ping a 172.20.43.235 con 32 bytes de datos:
Respuesta desde 172.20.43.212: Host de destino inaccesible.

Estadísticas de ping para 172.20.43.235:
    Paquetes: enviados = 1, recibidos = 1, perdidos = 0
    (0% perdidos),
```

No.	Time	Source	Destination	Protocol	Length	Info
695	68.469389	172.25.2.46	172.20.43.212	ICMP	138	Destination unreachable (Port unreachable)
696	68.469600	172.25.2.46	172.20.43.212	ICMP	138	Destination unreachable (Port unreachable)
717	69.223491	172.25.2.46	172.20.43.212	ICMP	138	Destination unreachable (Port unreachable)
718	69.223721	172.25.2.46	172.20.43.212	ICMP	138	Destination unreachable (Port unreachable)
849	69.988295	172.25.2.46	172.20.43.212	ICMP	138	Destination unreachable (Port unreachable)
850	69.988522	172.25.2.46	172.20.43.212	ICMP	138	Destination unreachable (Port unreachable)
1027	70.743188	172.25.2.46	172.20.43.212	ICMP	138	Destination unreachable (Port unreachable)
1028	70.743419	172.25.2.46	172.20.43.212	ICMP	138	Destination unreachable (Port unreachable)

icmpv6							
No.	icmpv6	Source	Destination	Protocol	Length	Info	
379	46.003800	fe80::76ff:9bd8:d97...	ff02::16	ICMPv6	110	Multicast Listener Report Message v2	
380	46.016314	fe80::76ff:9bd8:d97...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2	
381	46.016314	fe80::76ff:9bd8:d97...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2	
382	46.017558	fe80::76ff:9bd8:d97...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2	
383	46.017723	fe80::76ff:9bd8:d97...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2	
387	46.324818	fe80::76ff:9bd8:d97...	ff02::16	ICMPv6	110	Multicast Listener Report Message v2	
485	52.330445	fe80::76ff:9bd8:d97...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2	
486	52.330478	fe80::76ff:9bd8:d97...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2	
502	52.826466	fe80::76ff:9bd8:d97...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2	
518	55.825699	fe80::76ff:9bd8:d97...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2	
521	55.828887	fe80::76ff:9bd8:d97...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2	
538	56.324723	fe80::76ff:9bd8:d97...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2	
675	68.388967	fe80::76ff:9bd8:d97...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2	
679	68.407503	fe80::76ff:9bd8:d97...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2	
681	68.407766	fe80::76ff:9bd8:d97...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2	
684	68.407970	fe80::76ff:9bd8:d97...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2	
707	68.821772	fe80::76ff:9bd8:d97...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2	
728	69.408405	fe80::76ff:9bd8:d97...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2	
730	69.410320	fe80::76ff:9bd8:d97...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2	
827	69.824320	fe80::76ff:9bd8:d97...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2	

Cuestión 7: Ejecuta el comando `ping -n 1 172.20.41.244` y determina la secuencia ARP realizada. ¿ Aparecen paquetes ARP ? ¿ Por qué ? ¿ Recibes algún mensaje ICMP Echo Reply de la estación 172.20.41.244 ? ¿ A qué crees que puede ser debido ?

```
C:\>ping -n 1 172.20.41.244

Haciendo ping a 172.20.41.244 con 32 bytes de datos:
Respuesta desde 172.20.43.195: Red de destino inaccesible.

Estadísticas de ping para 172.20.41.244:
    Paquetes: enviados = 1, recibidos = 1, perdidos = 0
              (0% perdidos),
```

No.	Time	Source	Destination	Protocol	Length	Info
193	13.677972	172.20.43.212	172.20.41.244	ICMP	74	Echo (ping) request id=0x0001, seq=112/28672, ttl=128 (no response found!)
194	13.678614	172.20.43.195	172.20.43.212	ICMP	102	Destination unreachable (Communication administratively filtered)

DIRECCIONAMIENTO IP

Ejercicio 1: Se desean establecer 7 subredes dentro de la red 193.145.230.0/24 con el mismo número de equipos. Determina en cuántos bits hay que ampliar la máscara de red y cuáles son los rangos de direcciones IP para todas las subredes resultantes.

Al ser 7 subredes hay que ampliar en la máscara 3 bits

Las 7 subredes serían las siguientes con sus rangos (en rojo se indica la ampliación de red):

193.145.230.**000**000001 → 193.147.230.00011110 ; 193.147.230.00011111 (broadcast)

193.145.230.**001**000000 → 193.147.230.00111110 ; 193.147.230.00111111

193.145.230.**010**000000 → 193.147.230.01011110 ; 193.147.230.01011111

193.145.230.**011**000000 → 193.147.230.01111110 ; 193.147.230.01111111

193.145.230.**100**000000 → 193.147.230.10011110 ; 193.147.230.10011111

193.145.230.**101**000000 → 193.147.230.10111110 ; 193.147.230.10111111

193.145.230.**110**000000 → 193.147.230.11011110 ; 193.147.230.11011111

Ejercicio 2: Se desean establecer 5 subredes dentro de la red 130.20.0.0/22. Determina en cuántos bits hay que ampliar la máscara de red y cuáles son los rangos de direcciones IP para todas las subredes resultantes.

Similar al ejercicio anterior nos dan el siguiente direccionamiento IP:

130.20.0000000**00**.000000000 → 130.20.000000000.01111110 ; 130.20.000000000.01111111 (broadcast)

130.20.00000000.100000000 → 130.20.000000000.11111110 ; 130.20.000000000.11111111 (broadcast)

130.20.000000001.000000000 → 130.20.000000001.11111110 ; 130.20.000000001.11111111 (broadcast)

130.20.000000001.100000000 → 130.20.000000001.11111110 ; 130.20.000000001.11111111 (broadcast)

130.20.000000010.000000000 → 130.20.000000010.11111110 ; 130.20.000000010.11111111 (broadcast)