ICMP: traceroute en Wireshark

Consigna

Realizar un captura con el Wireshark de traceroute (si puede en IPv6) con las opciones TCP y luego con UDP, y realizar un informe en PDF.

Introducción

El comando `traceroute` es una herramienta que se utiliza para seguir la traza que hace un paquete a través de la red. Para ello, envía paquetes IP con el campo TTL (Time To Live) incrementado en 1 en cada iteración. En cada iteración, el paquete se envía multiple veces y se espera a que el host de destino responda con un mensaje ICMP de tipo "Time Exceeded". Cuando el host (router) responde, este informa la dirección IP del mismo y nos permite reconstruir la ruta que siguió el paquete. Por otro lado para asegurarse de que el paquete llegue al host de destino, se usa un puerto que probablemente esté cerrado en el host de destino, de esta forma el host de destino responderá con un mensaje ICMP de tipo "Port Unreachable" y el comando `traceroute` sabrá que llegó al host de destino.

Desarrollo

Comando utilizado

Para realizar el traceroute al host, se utilizó el siguiente comando:

```
sudo traceroute -T -4 -q N developer.mozilla.org >
traceroute_output_tcp.txt

traceroute -U -4 -q N developer.mozilla.org > traceroute_output_udp.txt
```

Donde:

- `sudo`: se utiliza para ejecutar el comando con permisos de superusuario (necesario para el caso de TCP).
- `traceroute`: comando utilizado para seguir la traza de un paquete a través de la red.
- `-T`: utiliza TCP como protocolo de transporte.
- `-U`: utiliza UDP como protocolo de transporte.
- `-4`: utiliza IPv4 (hice la prueba con IPv6 y no lo admite el destino).
- `-q N`: envía N paquetes de datos al host por cada TTL.
- `developer.mozilla.org`: host al que se envían los paquetes.
- `> output.txt`: redirige la salida del comando a un archivo.

Para hacer una prubea inicial, usamos `N=2` para hacer una primera prueba y asegurarnos de que el comando funciona correctamente.

Análisis de los resultados - TCP

```
traceroute to developer.mozilla.org (34.111.97.67), 30 hops max, 60 byte
packets
 1  N-MGISMONDI.mshome.net (172.30.144.1)  1.243 ms  1.087 ms
 2  192.168.0.1 (192.168.0.1)  11.893 ms  12.765 ms
 3  * *
 4  10.242.4.189 (10.242.4.189)  28.654 ms  29.084 ms
 5  * *
 6  * *
 7  192.178.84.75 (192.178.84.75)  28.915 ms  30.973 ms
 8  142.251.239.191 (142.251.239.191)  28.689 ms 172.253.71.9
(172.253.71.9)  33.769 ms
 9  67.97.111.34.bc.googleusercontent.com (34.111.97.67)  25.321 ms
34.700 ms
```

Podemos ver que en 9 saltos llegamos al host de destino. En el salto 3, 5 y 6 no obtuvimos respuesta, lo cual puede deberse a que los routers no responden a los paquetes con TTL expirado, sino que simplemente los descartan. Por otro lado, en el salto 8 vemos que el paquete llegó por dos caminos diferentes, esto se puede dar por la forma en la que se distribuyen los paquetes en la red es dificil saberlo a ciencia cierta. Por otro lado, en cada salto podemos no solo ver la dirección IP del router, sino también el tiempo que tardó en responder (el RTT).

Análisis de los resultados - UDP

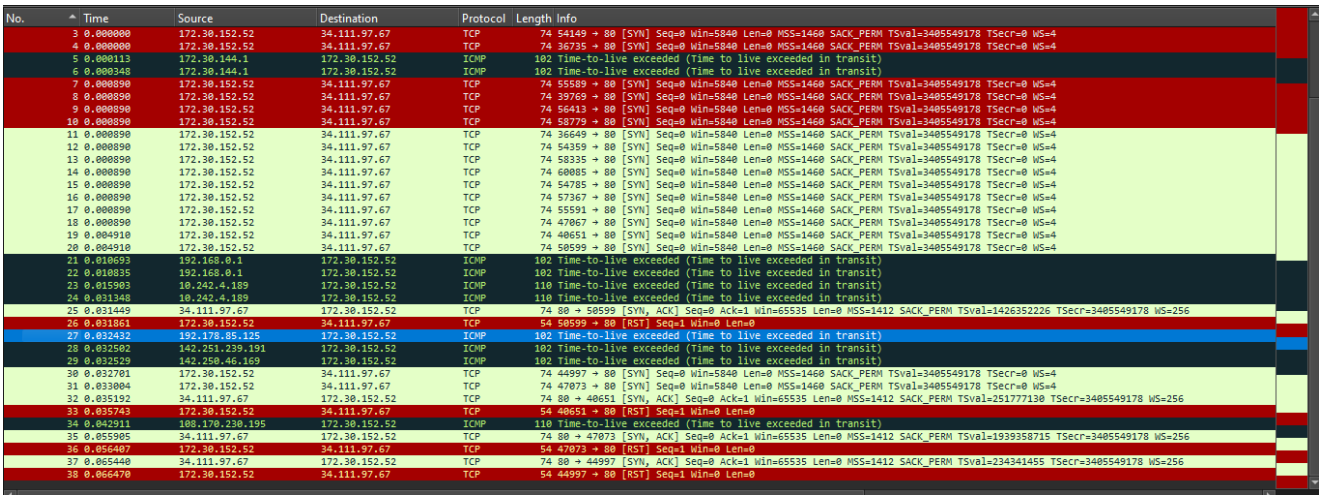
```
traceroute to developer.mozilla.org (34.111.97.67), 30 hops max, 60 byte
packets
 1  N-MGISMONDI.mshome.net (172.30.144.1)  0.519 ms  0.983 ms
 2  192.168.0.1 (192.168.0.1)  10.652 ms  9.629 ms
 3  10.29.192.1 (10.29.192.1)  22.009 ms  21.825 ms
 4  10.242.4.189 (10.242.4.189)  21.793 ms  21.675 ms
 5  * *
 6  cpe-200-115-194-182.telecentro-reversos.com.ar (200.115.194.182)
23.395 ms  23.375 ms
 7  108.170.230.195 (108.170.230.195)  24.907 ms 192.178.85.125
(192.178.85.125)  23.337 ms
 8  142.251.239.191 (142.251.239.191)  22.342 ms 108.170.237.241
(108.170.237.241)  23.259 ms
 9  67.97.111.34.bc.googleusercontent.com (34.111.97.67)  32.182 ms
27.581 ms
```

En este caso, similar al anterior, en 9 saltos llegamos al host de destino. En el salto 5 no obtuvimos respuesta, mismo caso que en TCP.

Capturas de Wireshark

A continuación se muestran las capturas realizadas con Wireshark:

Captura TCP



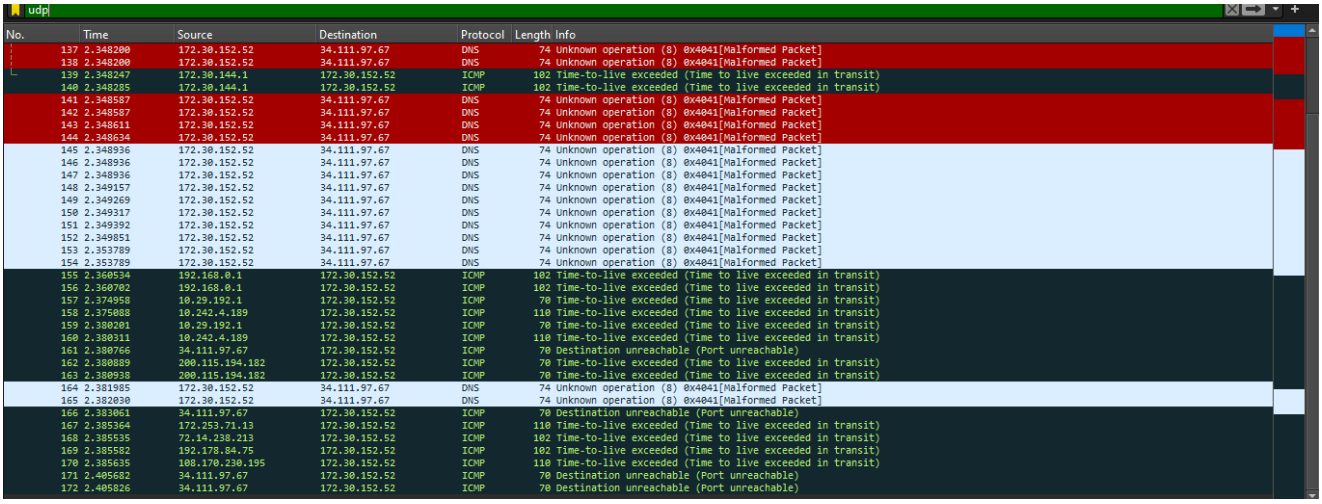
No.	Time	Source	Destination	Protocol	Length	Info
3	0.000000	172.30.152.52	34.111.97.67	TCP	74	54149 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=3405549178 TSecr=0 WS=4
4	0.000000	172.30.152.52	34.111.97.67	TCP	74	36735 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=3405549178 TSecr=0 WS=4
5	0.000113	172.30.144.1	172.30.152.52	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
6	0.000348	172.30.144.1	172.30.152.52	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
7	0.000890	172.30.152.52	34.111.97.67	TCP	74	55589 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=3405549178 TSecr=0 WS=4
8	0.000890	172.30.152.52	34.111.97.67	TCP	74	39769 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=3405549178 TSecr=0 WS=4
9	0.000890	172.30.152.52	34.111.97.67	TCP	74	56413 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=3405549178 TSecr=0 WS=4
10	0.000890	172.30.152.52	34.111.97.67	TCP	74	58779 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=3405549178 TSecr=0 WS=4
11	0.000890	172.30.152.52	34.111.97.67	TCP	74	36649 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=3405549178 TSecr=0 WS=4
12	0.000890	172.30.152.52	34.111.97.67	TCP	74	54359 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=3405549178 TSecr=0 WS=4
13	0.000890	172.30.152.52	34.111.97.67	TCP	74	58335 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=3405549178 TSecr=0 WS=4
14	0.000890	172.30.152.52	34.111.97.67	TCP	74	60085 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=3405549178 TSecr=0 WS=4
15	0.000890	172.30.152.52	34.111.97.67	TCP	74	54785 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=3405549178 TSecr=0 WS=4
16	0.000890	172.30.152.52	34.111.97.67	TCP	74	57367 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=3405549178 TSecr=0 WS=4
17	0.000890	172.30.152.52	34.111.97.67	TCP	74	55591 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=3405549178 TSecr=0 WS=4
18	0.000890	172.30.152.52	34.111.97.67	TCP	74	47067 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=3405549178 TSecr=0 WS=4
19	0.004910	172.30.152.52	34.111.97.67	TCP	74	40651 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=3405549178 TSecr=0 WS=4
20	0.004910	172.30.152.52	34.111.97.67	TCP	74	50599 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=3405549178 TSecr=0 WS=4
21	0.010693	192.168.0.1	172.30.152.52	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
22	0.010835	192.168.0.1	172.30.152.52	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
23	0.015903	10.242.4.189	172.30.152.52	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
24	0.031348	10.242.4.189	172.30.152.52	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
25	0.031449	34.111.97.67	172.30.152.52	TCP	74	80 → 50599 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM TSval=1426352226 TSecr=3405549178 WS=256
26	0.031861	172.30.152.52	34.111.97.67	TCP	54	50599 → 80 [RST] Seq=1 Win=0 Len=0
27	0.032432	192.178.85.125	172.30.152.52	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
28	0.032502	142.251.239.191	172.30.152.52	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
29	0.032529	142.250.46.169	172.30.152.52	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
30	0.032701	172.30.152.52	34.111.97.67	TCP	74	44997 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=3405549178 TSecr=0 WS=4
31	0.033004	172.30.152.52	34.111.97.67	TCP	74	47073 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=3405549178 TSecr=0 WS=4
32	0.035192	34.111.97.67	172.30.152.52	TCP	74	80 → 40651 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM TSval=251777130 TSecr=3405549178 WS=256
33	0.035743	172.30.152.52	34.111.97.67	TCP	54	40651 → 80 [RST] Seq=1 Win=0 Len=0
34	0.042911	108.170.230.195	172.30.152.52	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
35	0.055905	34.111.97.67	172.30.152.52	TCP	74	80 → 47073 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM TSval=1939358715 TSecr=3405549178 WS=256
36	0.056407	172.30.152.52	34.111.97.67	TCP	54	47073 → 80 [RST] Seq=1 Win=0 Len=0
37	0.065440	34.111.97.67	172.30.152.52	TCP	74	80 → 44997 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM TSval=234341455 TSecr=3405549178 WS=256
38	0.066470	172.30.152.52	34.111.97.67	TCP	54	44997 → 80 [RST] Seq=1 Win=0 Len=0

Podemos ver como por cada salto, se envían 2 paquetes (2 conexiones TCP) y se espera a que el host de destino responda con un mensaje ICMP.

Al final llegan los paquetes con el RST activado, lo cual indica que el puerto está cerrado y por ende llegamos al host de destino.

Además en cada ICMP de los perdidos podemos ver la source IP del router que rechazó el paquete.

Captura UDP



udp

No.	Time	Source	Destination	Protocol	Length	Info
137	2.348200	172.30.152.52	34.111.97.67	DNS	74	Unknown operation (8) 0x4041[Malformed Packet]
138	2.348200	172.30.152.52	34.111.97.67	DNS	74	Unknown operation (8) 0x4041[Malformed Packet]
139	2.348247	172.30.144.1	172.30.152.52	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
140	2.348285	172.30.144.1	172.30.152.52	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
141	2.348587	172.30.152.52	34.111.97.67	DNS	74	Unknown operation (8) 0x4041[Malformed Packet]
142	2.348587	172.30.152.52	34.111.97.67	DNS	74	Unknown operation (8) 0x4041[Malformed Packet]
143	2.348611	172.30.152.52	34.111.97.67	DNS	74	Unknown operation (8) 0x4041[Malformed Packet]
144	2.348634	172.30.152.52	34.111.97.67	DNS	74	Unknown operation (8) 0x4041[Malformed Packet]
145	2.348936	172.30.152.52	34.111.97.67	DNS	74	Unknown operation (8) 0x4041[Malformed Packet]
146	2.348936	172.30.152.52	34.111.97.67	DNS	74	Unknown operation (8) 0x4041[Malformed Packet]
147	2.348936	172.30.152.52	34.111.97.67	DNS	74	Unknown operation (8) 0x4041[Malformed Packet]
148	2.349157	172.30.152.52	34.111.97.67	DNS	74	Unknown operation (8) 0x4041[Malformed Packet]
149	2.349269	172.30.152.52	34.111.97.67	DNS	74	Unknown operation (8) 0x4041[Malformed Packet]
150	2.349317	172.30.152.52	34.111.97.67	DNS	74	Unknown operation (8) 0x4041[Malformed Packet]
151	2.349392	172.30.152.52	34.111.97.67	DNS	74	Unknown operation (8) 0x4041[Malformed Packet]
152	2.349851	172.30.152.52	34.111.97.67	DNS	74	Unknown operation (8) 0x4041[Malformed Packet]
153	2.353789	172.30.152.52	34.111.97.67	DNS	74	Unknown operation (8) 0x4041[Malformed Packet]
154	2.353789	172.30.152.52	34.111.97.67	DNS	74	Unknown operation (8) 0x4041[Malformed Packet]
155	2.360534	192.168.0.1	172.30.152.52	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
156	2.360702	192.168.0.1	172.30.152.52	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
157	2.374958	10.29.192.1	172.30.152.52	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
158	2.375088	10.242.4.189	172.30.152.52	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
159	2.380201	10.29.192.1	172.30.152.52	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
160	2.380311	10.242.4.189	172.30.152.52	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
161	2.380766	34.111.97.67	172.30.152.52	ICMP	70	Destination unreachable (Port unreachable)
162	2.380889	200.115.194.182	172.30.152.52	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
163	2.380938	200.115.194.182	172.30.152.52	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
164	2.381985	172.30.152.52	34.111.97.67	DNS	74	Unknown operation (8) 0x4041[Malformed Packet]
165	2.382030	172.30.152.52	34.111.97.67	DNS	74	Unknown operation (8) 0x4041[Malformed Packet]
166	2.383061	34.111.97.67	172.30.152.52	ICMP	70	Destination unreachable (Port unreachable)
167	2.385364	172.253.71.13	172.30.152.52	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
168	2.385535	72.14.238.213	172.30.152.52	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
169	2.385582	192.178.84.75	172.30.152.52	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
170	2.385635	108.170.230.195	172.30.152.52	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
171	2.405682	34.111.97.67	172.30.152.52	ICMP	70	Destination unreachable (Port unreachable)
172	2.405826	34.111.97.67	172.30.152.52	ICMP	70	Destination unreachable (Port unreachable)

En este caso, no hace falta establecer la conexión TCP, simplemente se envían los paquetes por UDP y se espera que el host de destino responda con un mensaje ICMP.

En este caso, al igual que en TCP, se envían 2 paquetes por salto y se espera a que el host de destino responda.

Por último vemos que ahora si llegamos al host de destino, ya que el puerto está cerrado y el host de destino responde con un mensaje ICMP de tipo "Port Unreachable" y no con el "Time Exceeded" de los routers.

Conclusiones

Podemos ver que a pesar que algunos routers no respondan a TTLs expirados, podemos reconstruir la ruta que siguió el paquete a través de la red de una gran cantidad de routers. Por otro lado si bien no

pudimos hacer la prueba con IPv6, funciona de todas formas con IPv4.

Podemos agregar además que cerca de donde está el servidor de mozilla, tenemos algún tipo de balanceador de carga que cambia la ruta para llegar al mismo, esto empeora la traza ya que no nos permite determinar un camino fijo que siga el paquete.