

PING, ICMP & Traceroute

Introducción a los Sistemas Distribuidos (75.43)

Universidad de Buenos Aires, Facultad de Ingeniería

Julio, 2020



PING

PING

- Packet Internet Groper

- Herramienta

- Origin

¿Para qué se usa hoy en día?

diagnosticar

problemas de red en los 70

PING

Se utiliza para comprobar el tiempo que tarda un paquete de información en llegar a una dirección IP que hayamos indicado y luego volver



PING

Paquetes que envía PING:

- ICMP Echo Request
- ICMP Echo Replay/Response

Diagnosticar el estado, velocidad y calidad de una red.

PING

Funcionamiento:

`ping` <URL | dirección IP>

Para terminar utilizar Ctrl + c

PING

```
agustin@agustin-VivoBook ~> ping -a 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
From 100.72.9.42 icmp_seq=1 Packet filtered
64 bytes from 8.8.8.8: icmp_seq=2 ttl=114 time=58.2 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=114 time=69.0 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=114 time=36.9 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=114 time=40.7 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=114 time=23.3 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=114 time=16.4 ms
^C
--- 8.8.8.8 ping statistics ---
7 packets transmitted, 6 received, +1 errors, 14,2857% packet loss, time 6007ms
rtt min/avg/max/mdev = 16.419/40.747/69.017/18.316 ms
```

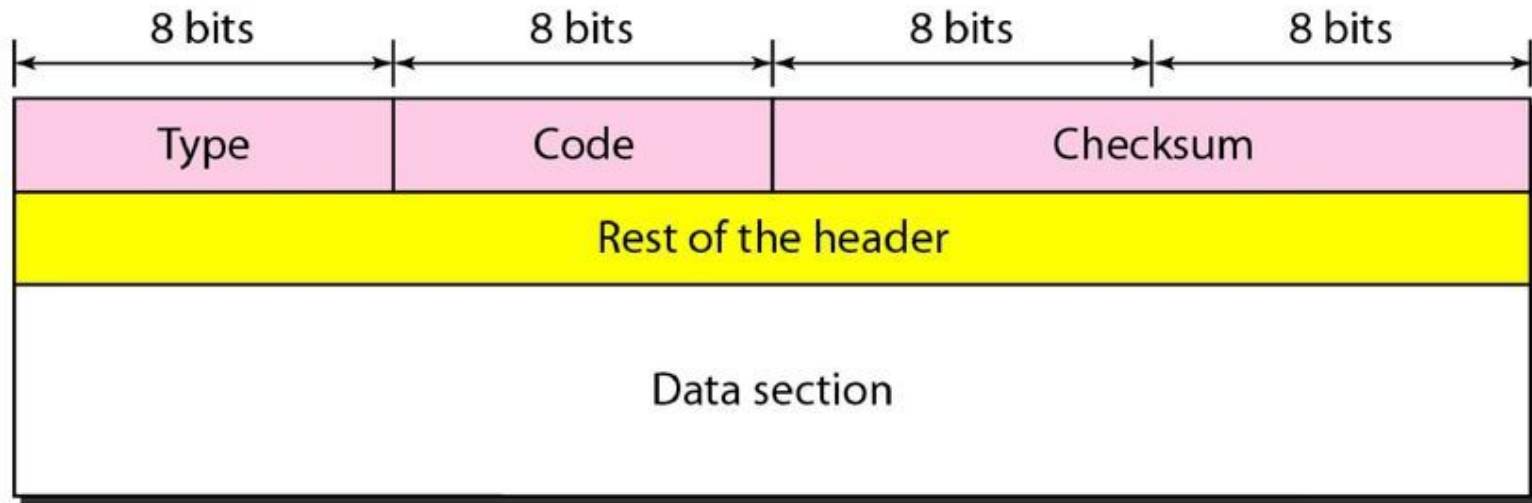
```
agustin@agustin-VivoBook ~> ping 8.8.8.8
ping: connect: Network is unreachable
```

ICMP

ICMP

- Internet Control Message Protocol - RFC 792
- Protocolo de señales para IP
- Mensajes de control, diagnóstico y reporte de errores
- Forma parte del conjunto de protocolos IP

ICMP - Formato



- **Type:** tipo de mensaje
- **Código:** subtipo al tipo dado
- **Checksum:** Datos comprobación de errores.
Calculado a partir del header ICMP + datos.
- **Resto del header:** Varía en función del tipo y código ICMP

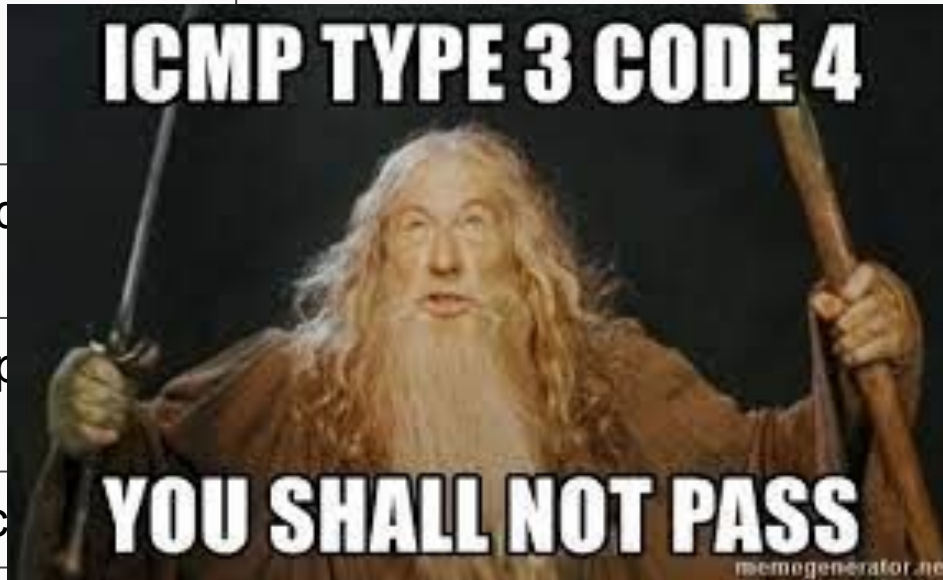
ICMP

- Hay dos categorías importantes de mensajes ICMP:
 - **Query**
 - **Error reporting**



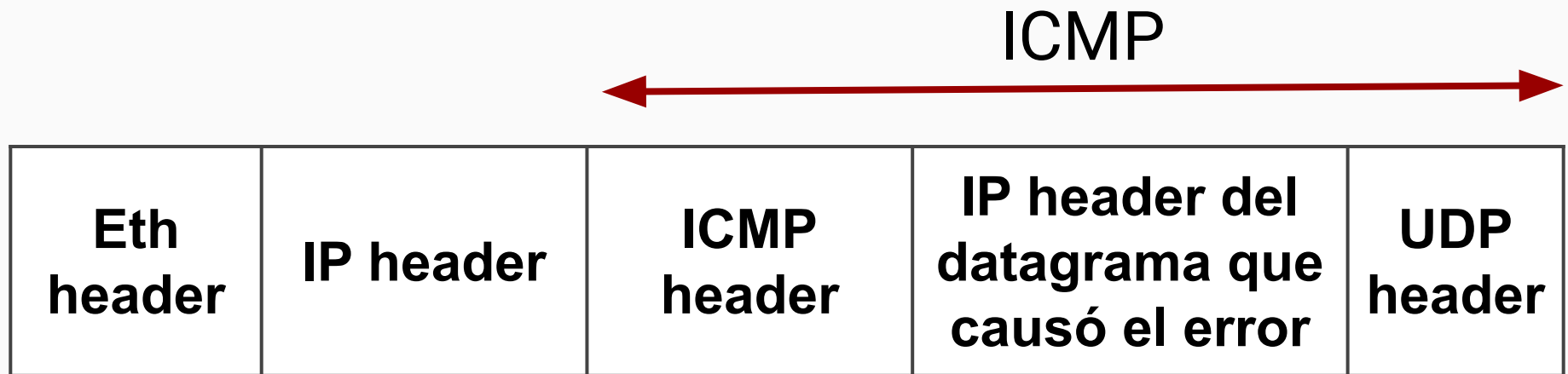
ICMP - Mensajes Principales

Type	Name	Message
3	Destination Unreachable	Red, host, puerto, protocolo inaccesible o desconocido
		Prohibida es
8	Echo Request	Posibilidad de una
0	Echo Reply	
11	Time Exceeded	→ TTL = 0
5	Redirect	El router informa de una ruta más directa que la que se está utilizando
4	Source Quench <deprecado>	Ejerce control de flujo sobre el emisor cuando se detecta congestión



ICMP - Ejemplo

- ICMP Destination Unreachable
(generado por un paquete UDP)



ICMP - Error reporting

- IP es no confiable → Mejor esfuerzo → errores
- ICMP no corrige errores, sólo los reporta
- Los mensajes se envían siempre al host inicial (src_ip)

ICMP - Error reporting

- No se reportan errores si el paquete causante:
 - Es ICMP
 - Es de broadcast (IP o L2)
 - Es un fragmento distinto al primero
- Para evitar
 - Loops
 - Packet explosions

Traceroute



Traceroute

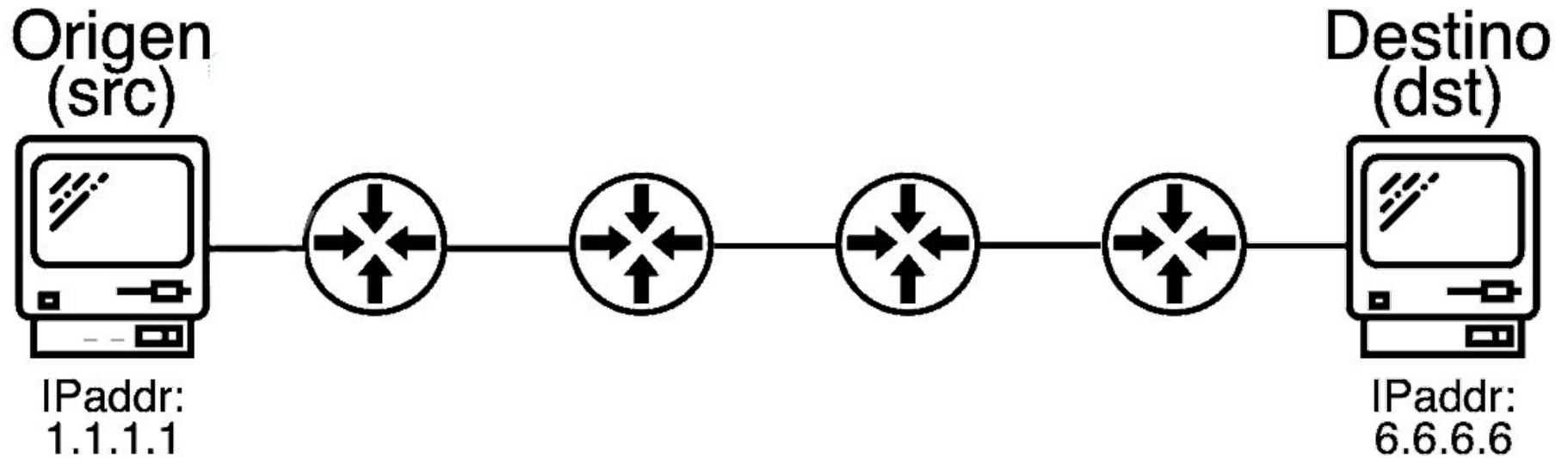
- Es una herramienta que sirve para descubrir las redes entre un origen (src) y un destino (dst).
- IP fue concebido como un protocolo end-to-end, por lo cual los host desconocen la estructura de la red.

Traceroute

- ¿Qué propósito cumple?
 - Releva la red
 - Diagnóstico
- Utiliza el protocolo ICMP para su funcionamiento.
- Los routers intermedios deben estar habilitados a responder mensajes ICMP.

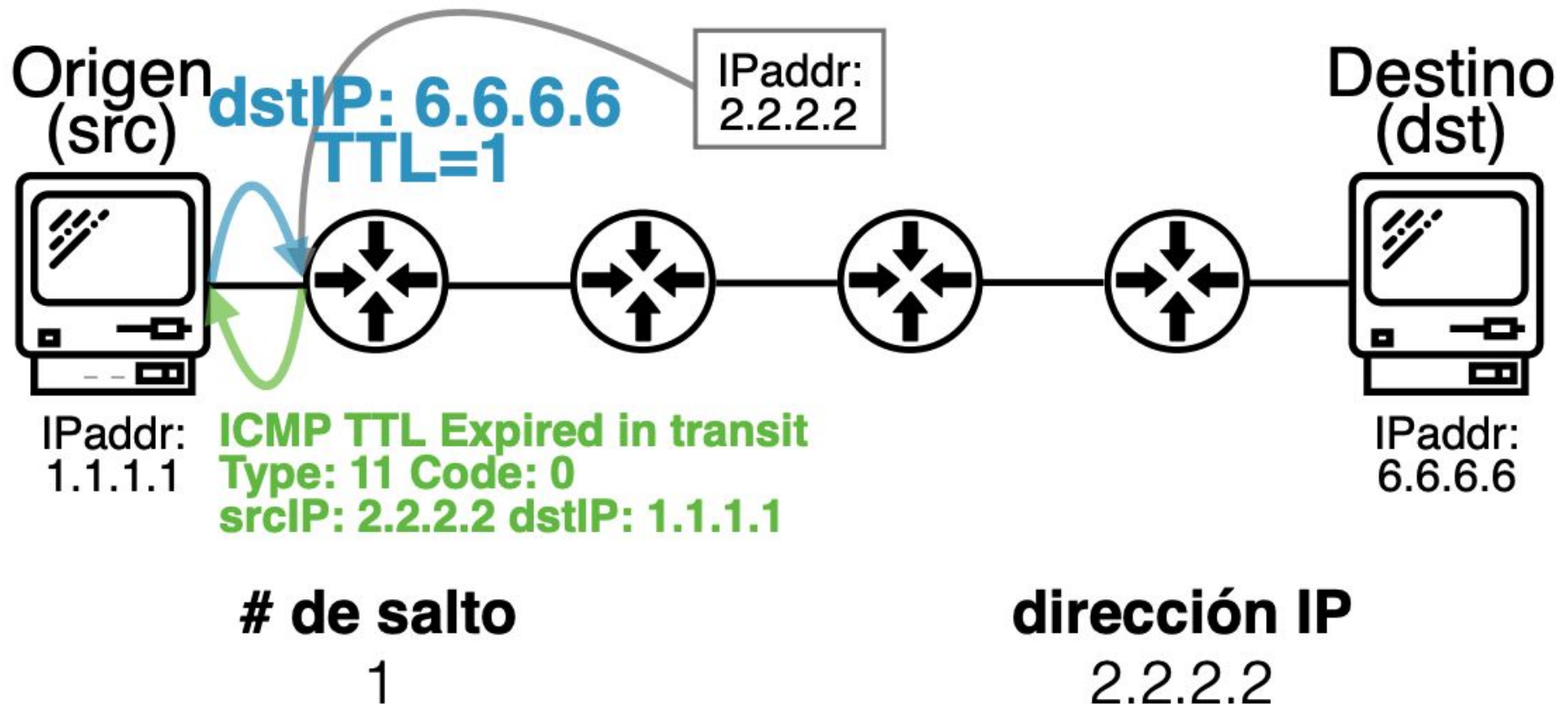
¿Cómo funciona?

traceroute 6.6.6.6



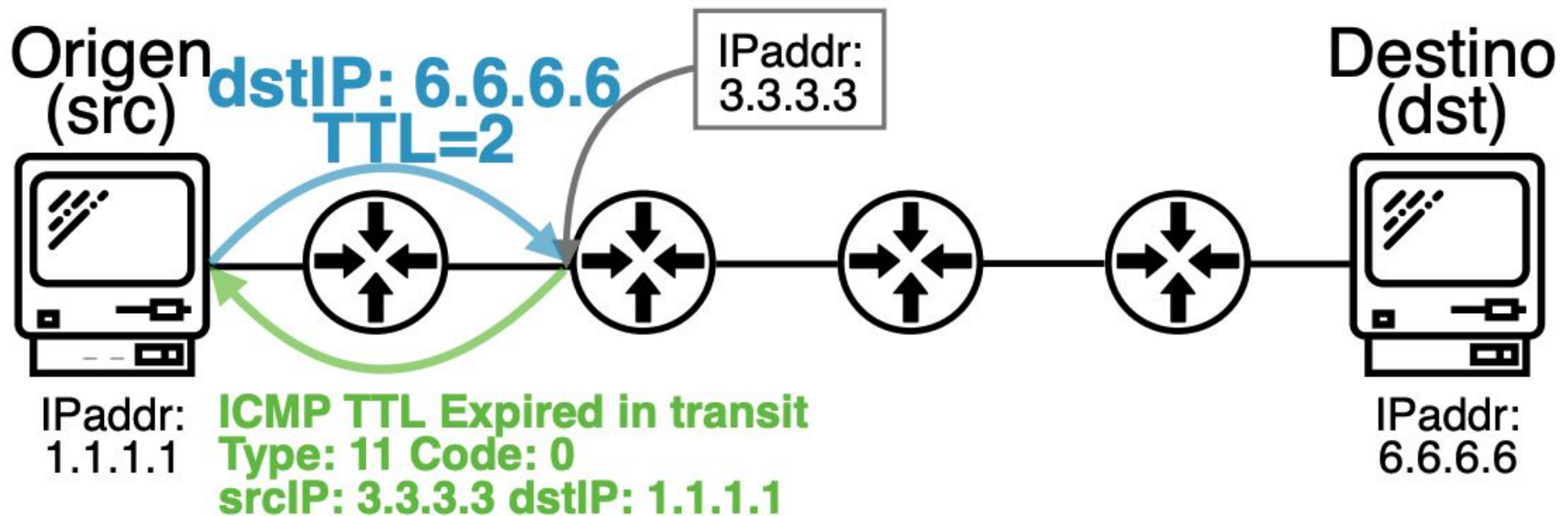
¿Cómo funciona?

traceroute 6.6.6.6



¿Cómo funciona?

traceroute 6.6.6.6



de salto

1

2

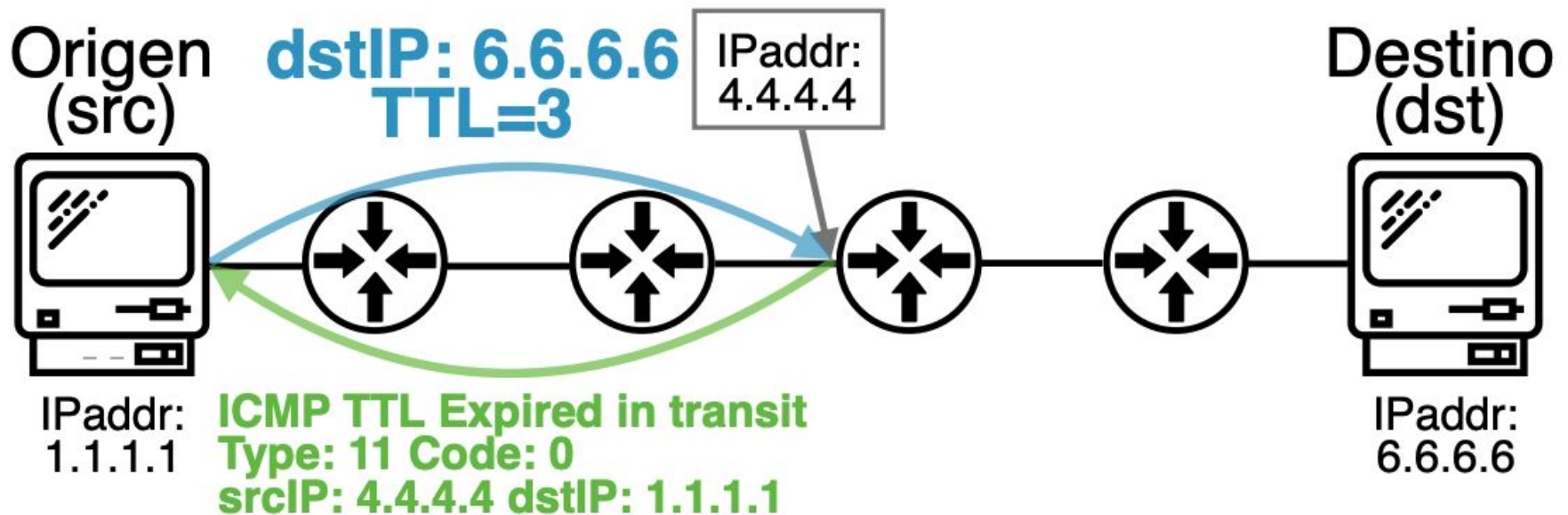
dirección IP

2.2.2.2

3.3.3.3

¿Cómo funciona?

traceroute 6.6.6.6



de salto

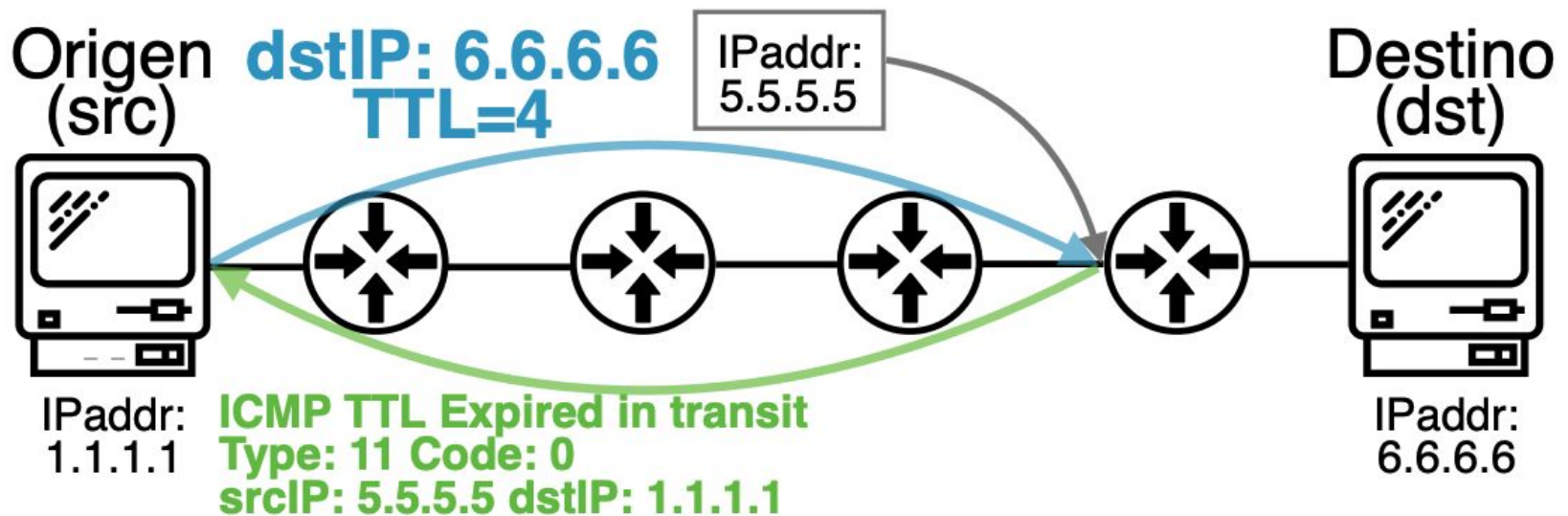
1
2
3

dirección IP

2.2.2.2
3.3.3.3
4.4.4.4

¿Cómo funciona?

tracert 6.6.6.6



de salto

1

2

3

4

dirección IP

2.2.2.2

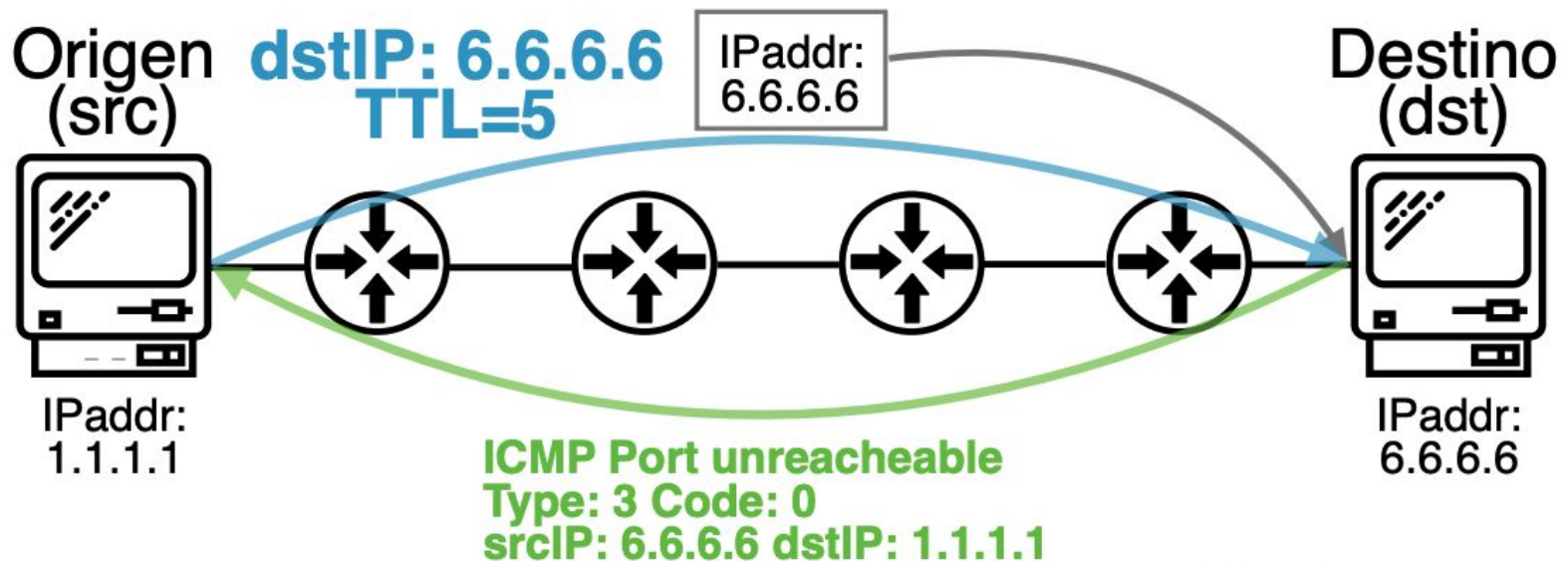
3.3.3.3

4.4.4.4

5.5.5.5

¿Cómo funciona?

traceroute 6.6.6.6



de salto

1
2
3
4
5

dirección IP

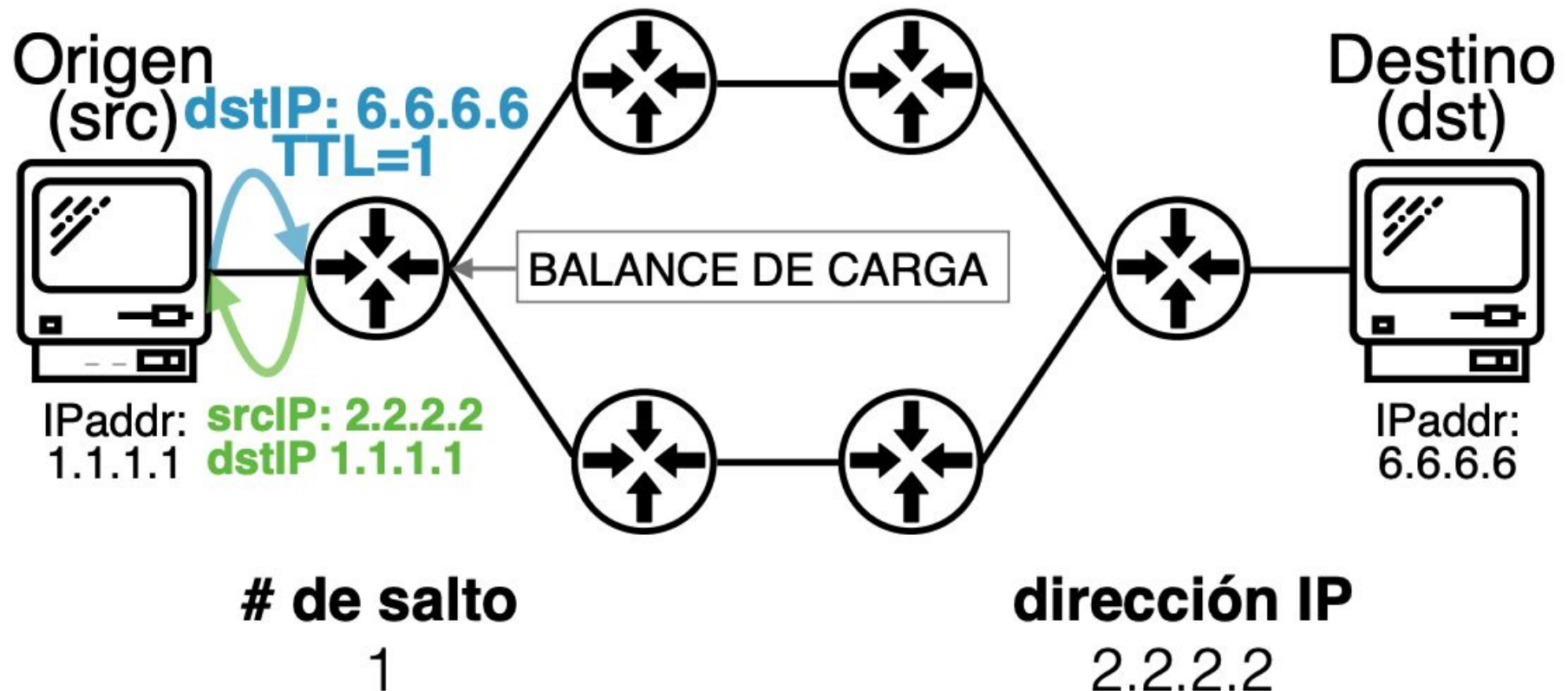
2.2.2.2
3.3.3.3
4.4.4.4
5.5.5.5
6.6.6.6

¿Cómo funciona?

**¿VEN ALGÚN
PROBLEMA?**

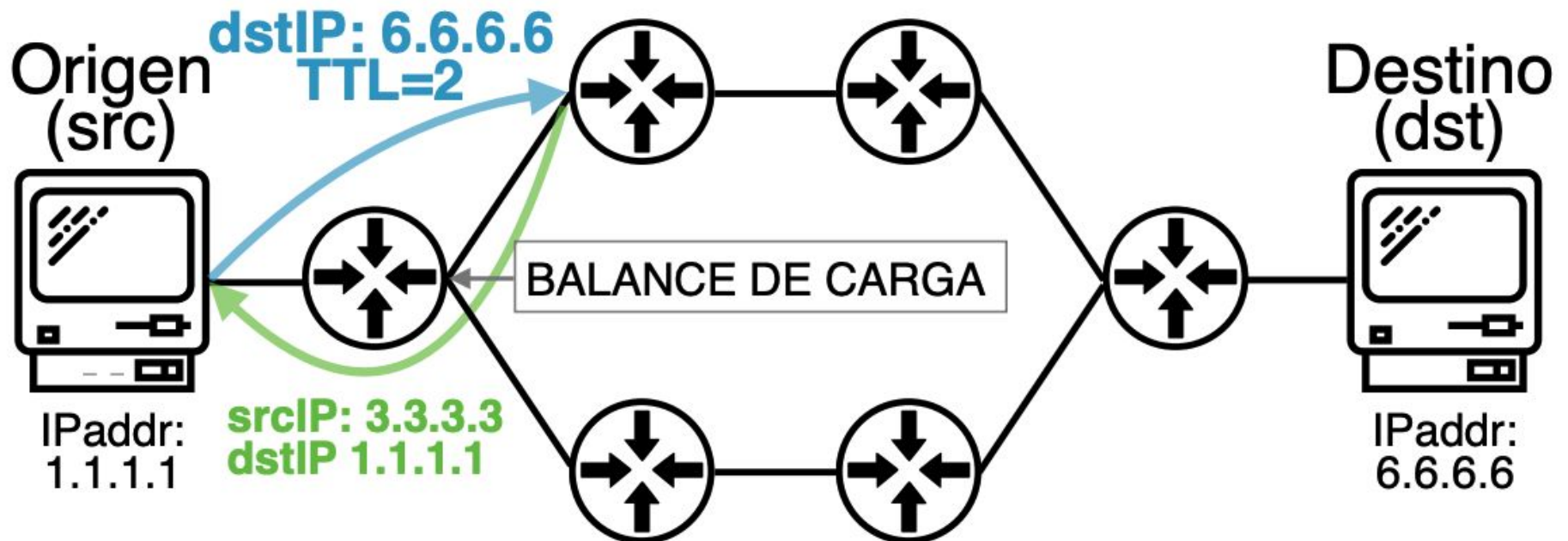
Traceroute y Balance de Carga

traceroute 6.6.6.6



Traceroute y Balance de Carga

traceroute 6.6.6.6



de salto

1

2

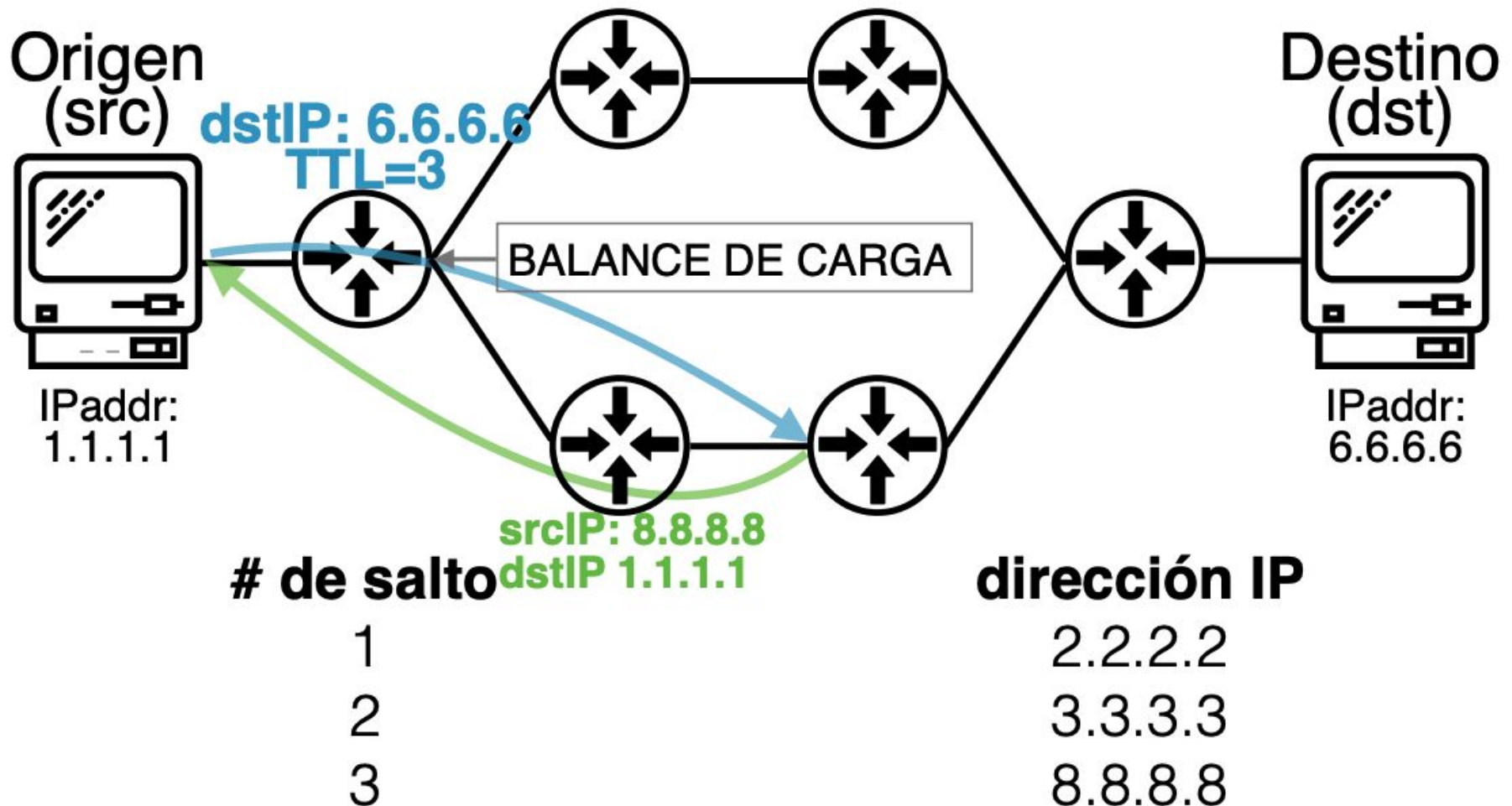
dirección IP

2.2.2.2

3.3.3.3

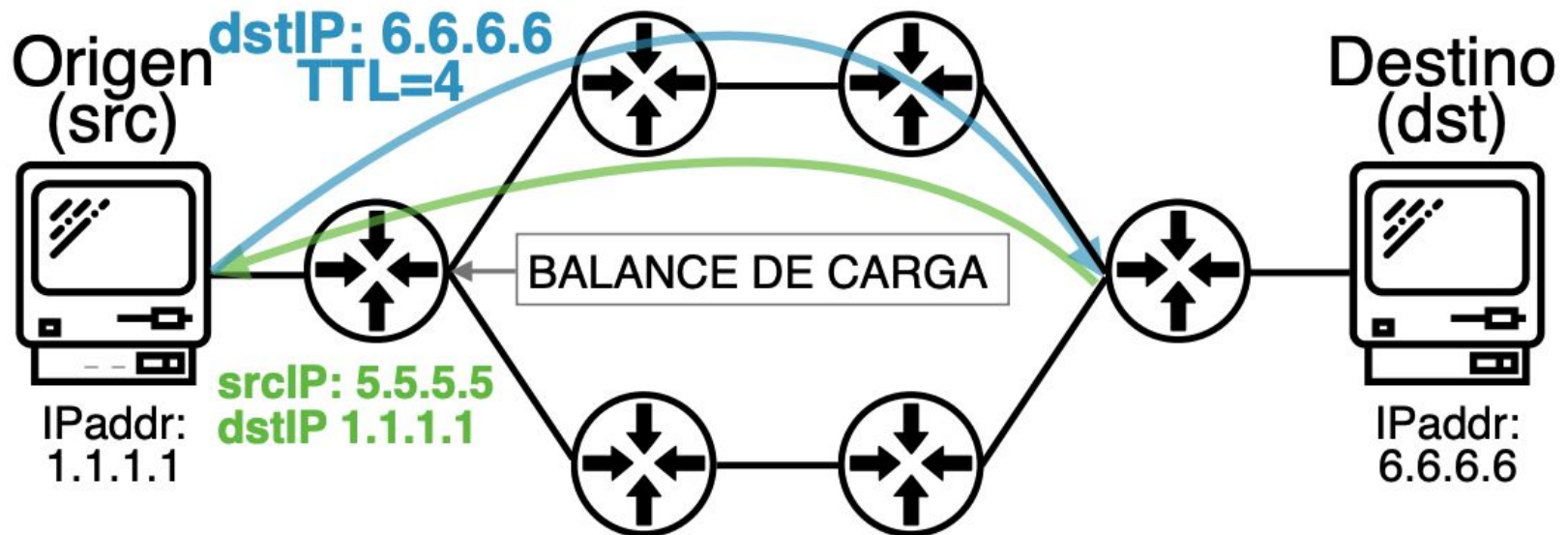
Traceroute y Balance de Carga

traceroute 6.6.6.6



Traceroute y Balance de Carga

traceroute 6.6.6.6



de salto

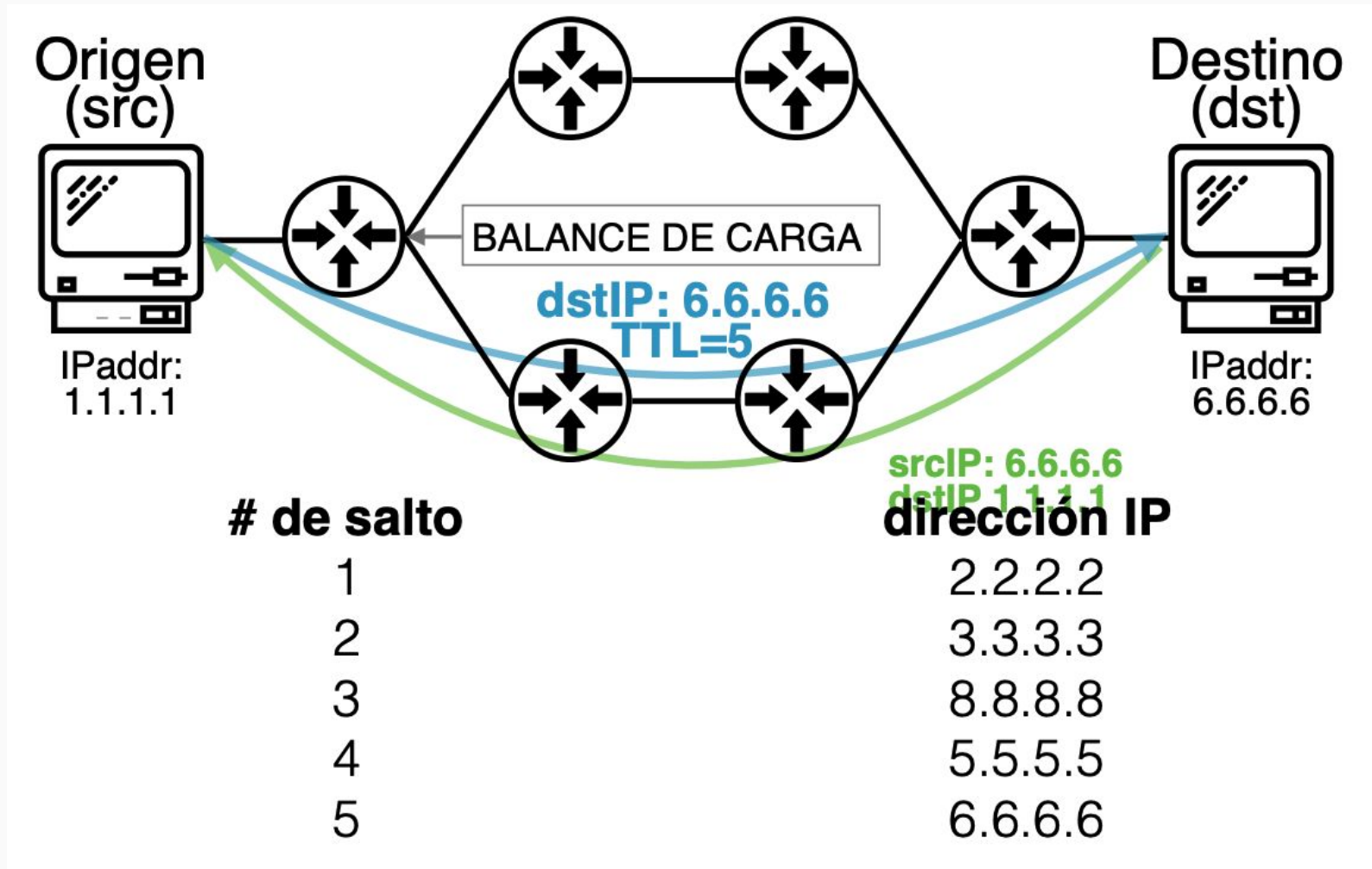
1
2
3
4

dirección IP

2.2.2.2
3.3.3.3
8.8.8.8
5.5.5.5

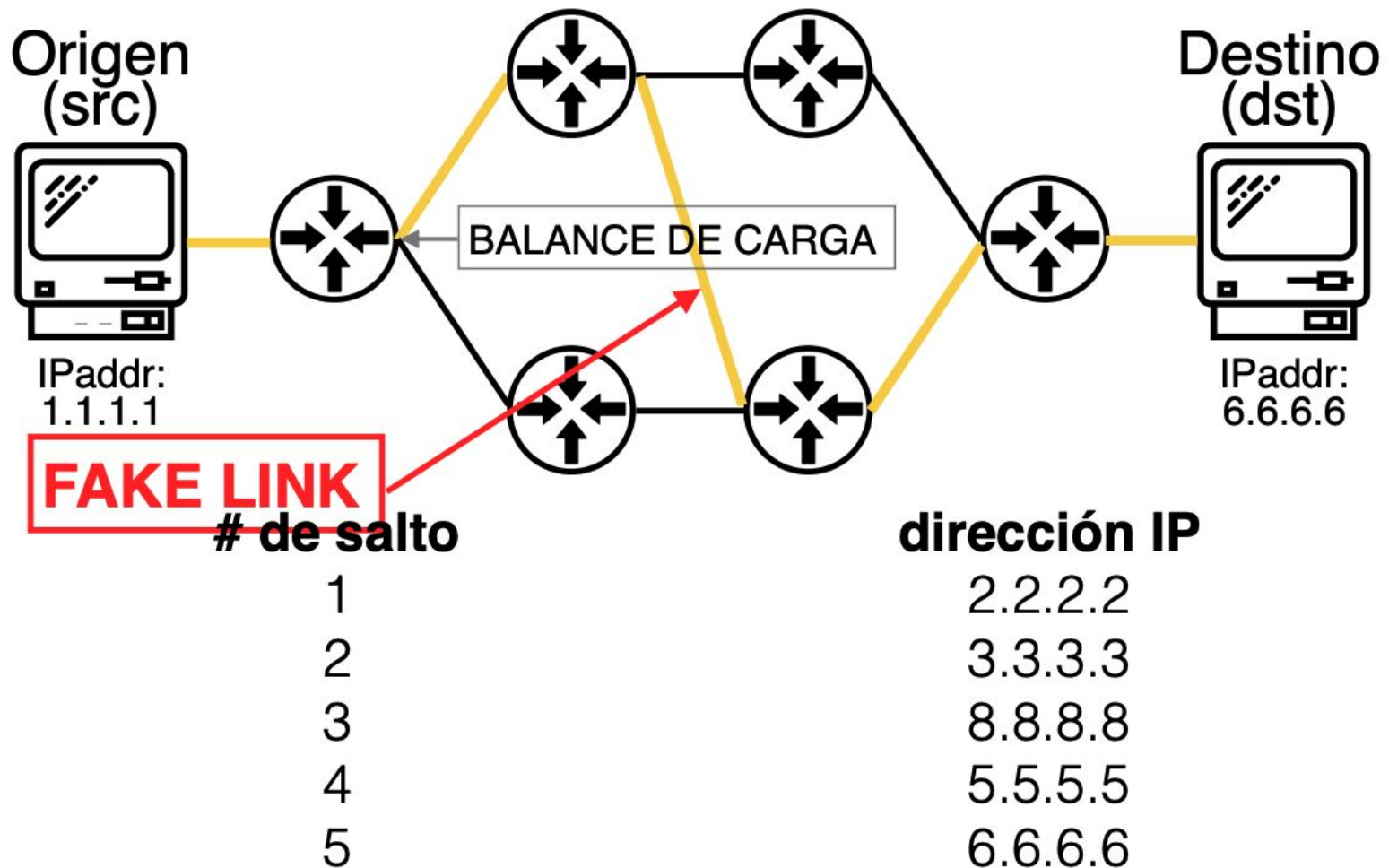
Traceroute y Balance de Carga

traceroute 6.6.6.6



Traceroute y Balance de Carga

traceroute 6.6.6.6



Traceroute y Balance de Carga

- **Solución:**

PARIS-TRACEROUTE

- Manipulando los headers que envía para mantener flujos.
- Se basa en que los routers respetan la RFC2991 ante ECMP

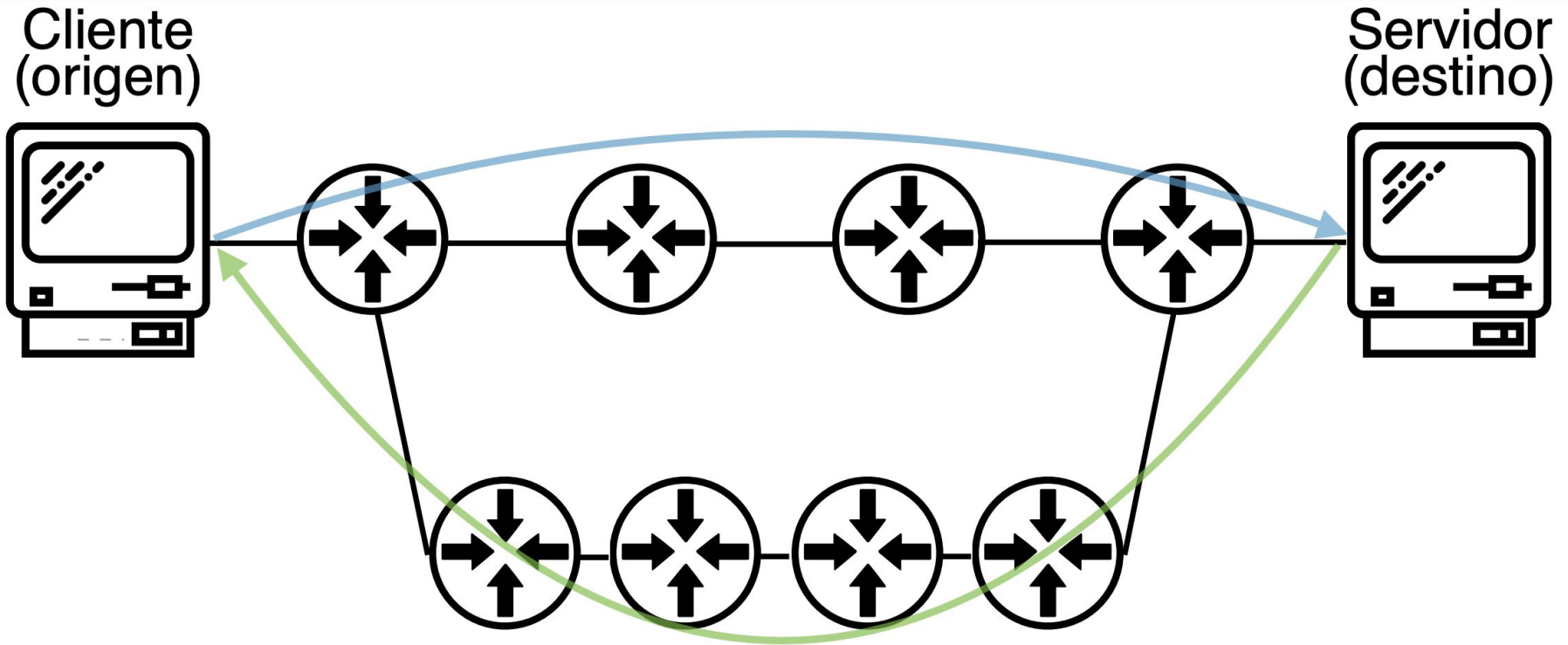
Traceroute y Balance de Carga

- Implementaciones:
 - *paris-traceroute*
 - *scamper*

Limitaciones

- Routers que no implementan ICMP
- IPs privadas dentro de un AS (autonomous system)
- Routers que no descartan paquetes con TTL=0
- Routers ocultando su dirección IP verdadera y devolviendo IP privada.

Asimetria de Caminos



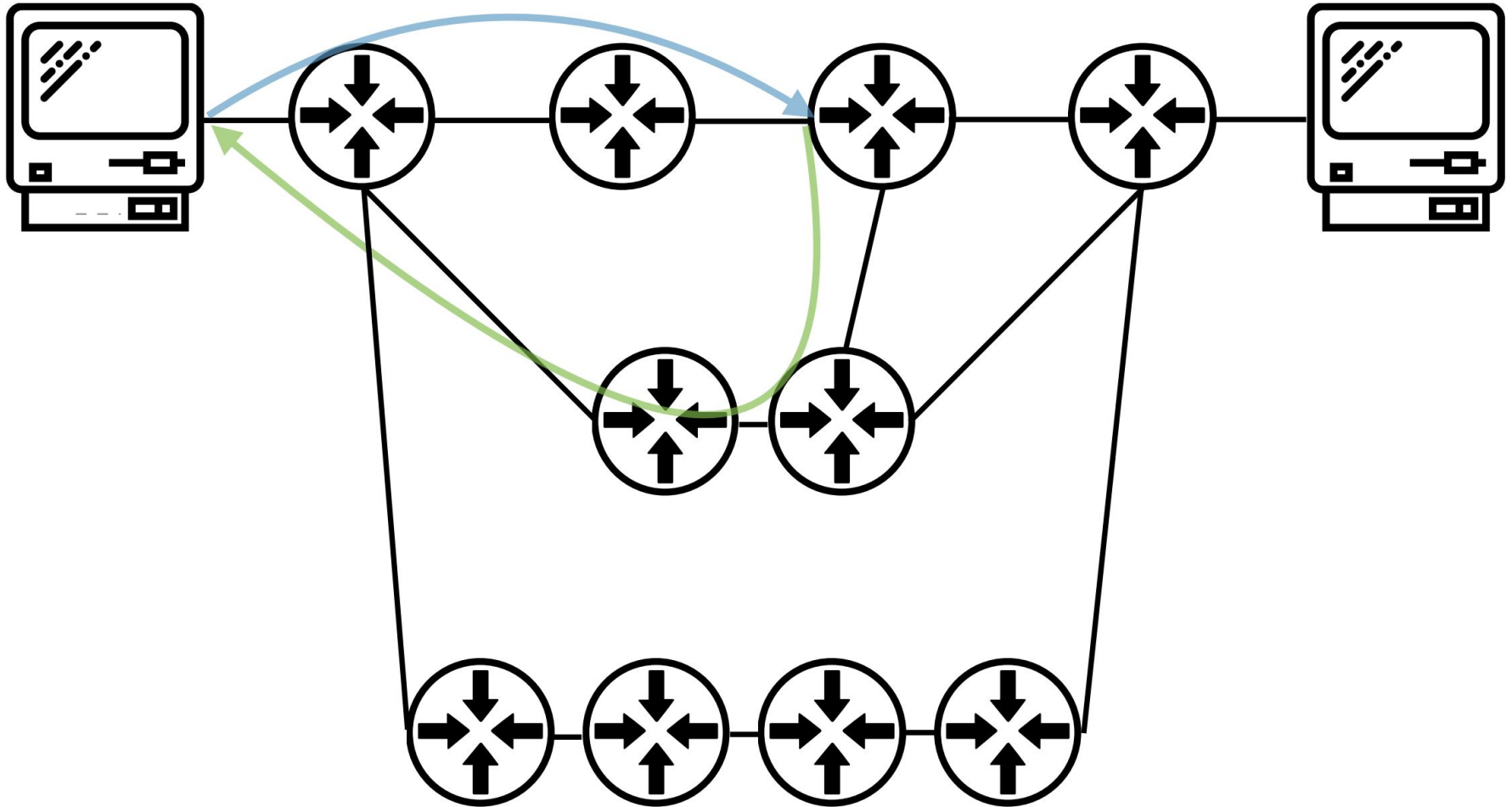
- camino de ida \neq camino de vuelta

Asimetria de Caminos

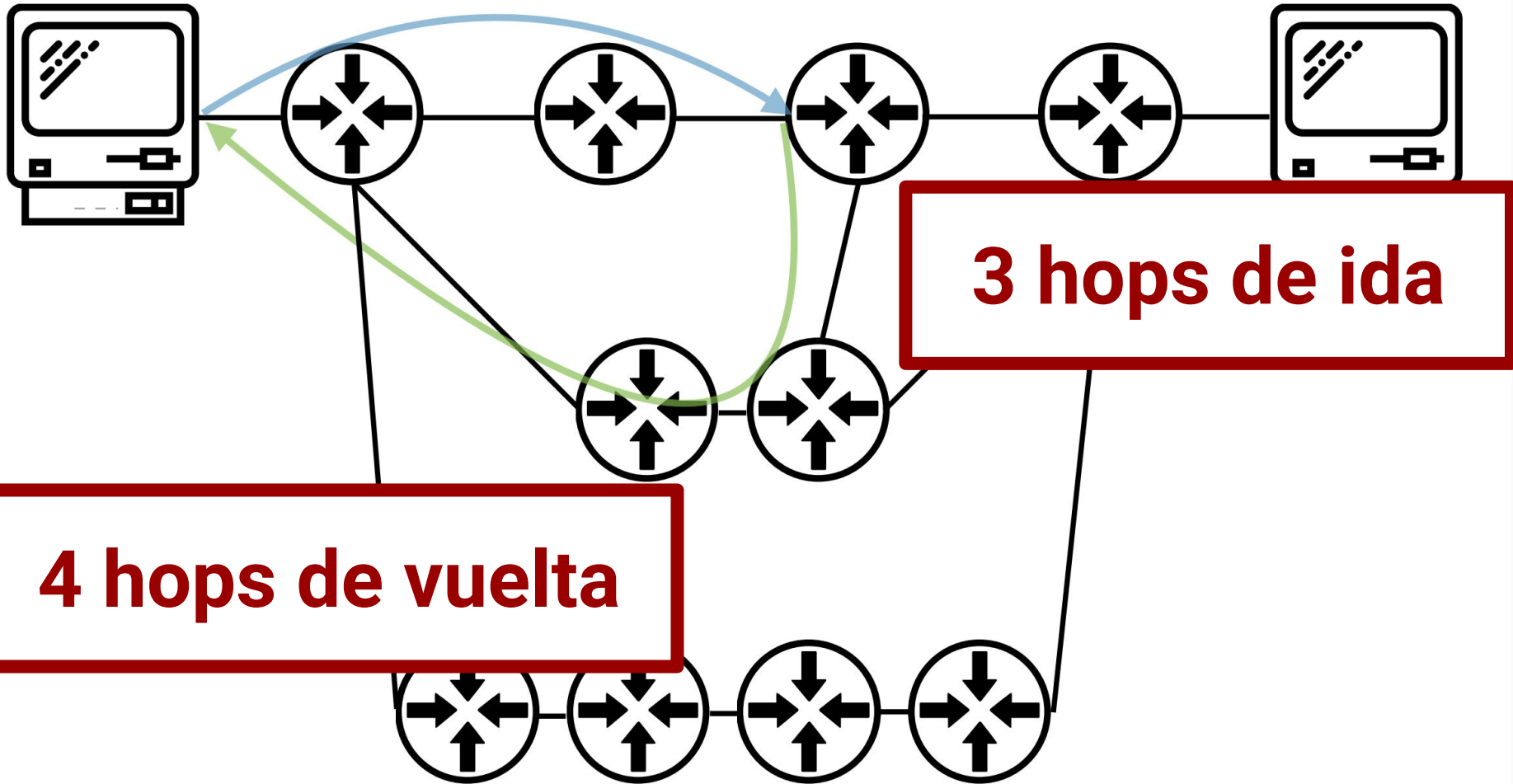
replyTTL

- Sabemos que TTL inicial de la respuesta es 255 o 64
- Si $\{255, 64\} - \text{replyTTL} \neq$ cantidad de saltos de ida, entonces sabemos que hay asimetría de caminos

Asimetría de Caminos



Asimetría de Caminos



Asimetria de Caminos

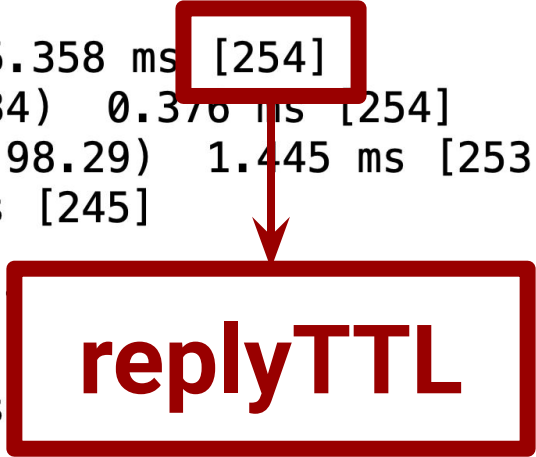
```
esteban@server:~$ sudo paris-traceroute -q 1 -w 1 -M 7 ipv4-c367-  
nyc001-ix.1.oca.nflxvideo.net --print_ttl
```

```
traceroute [(179.0.156.2:33456) -> (23.246.7.195:33457)], protocol  
udp, algo hopbyhop, duration 35 s  
 1 fw-vlan500.lacnic.net.uy (179.0.156.1) 5.358 ms [254]  
 2 edgemvd01-bbone.lacnic.net.uy (200.7.84.34) 0.376 ms [254]  
 3 ibb2cor3-be200-1703.antel.net.uy (200.40.98.29) 1.445 ms [253]  
 4 192.168.2.217 (192.168.2.217) 174.307 ms [245]  
    MPLS Label 34878 TTL=1 | 16032  
 5 192.168.1.90 (192.168.1.90) 166.382 ms !T2 [244]  
    MPLS Label 34243 TTL=2 | 16032  
 6 192.168.2.166 (192.168.2.166) 167.931 ms !T3 [248]  
    MPLS Label 24002 TTL=3 | 16032  
 7 ibr2nyx2-te0-7-0-2.antel.net.uy (200.40.0.38) 173.225 ms [249]  
 8 *  
 9 *  
10 *  
11 *  
12 *  
13 *  
14 *
```

Asimetria de Caminos

```
esteban@server:~$ sudo paris-traceroute -q 1 -w 1 -M 7 ipv4-c367-nyc001-ix.1.oca.nflxvideo.net --print_ttl
```

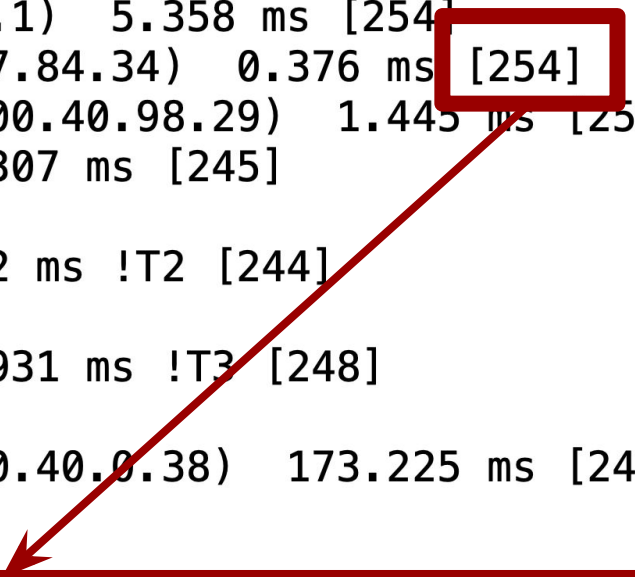
```
traceroute [(179.0.156.2:33456) -> (23.246.7.195:33457)], protocol
udp, algo hopbyhop, duration 35 s
 1  fw-vlan500.lacnic.net.uy (179.0.156.1)  5.358 ms [254]
 2  edgemvd01-bbone.lacnic.net.uy (200.7.84.34)  0.376 ms [254]
 3  ibb2cor3-be200-1703.antel.net.uy (200.40.98.29)  1.445 ms [253]
 4  192.168.2.217 (192.168.2.217)  174.307 ms [245]
    MPLS Label 34878 TTL=1 | 16032
 5  192.168.1.90 (192.168.1.90)  166.382 ms !
    MPLS Label 34243 TTL=2 | 16032
 6  192.168.2.166 (192.168.2.166)  167.931 ms
    MPLS Label 24002 TTL=3 | 16032
 7  ibr2nyx2-te0-7-0-2.antel.net.uy (200.40.0.38)  173.225 ms [249]
 8  *
 9  *
10  *
11  *
12  *
13  *
14  *
```



Asimetria de Caminos

```
esteban@server:~$ sudo paris-traceroute -q 1 -w 1 -M 7 ipv4-c367-nyc001-ix.1.oca.nflxvideo.net --print_ttl
```

```
traceroute [(179.0.156.2:33456) -> (23.246.7.195:33457)], protocol
udp, algo hopbyhop, duration 35 s
 1 fw-vlan500.lacnic.net.uy (179.0.156.1) 5.358 ms [254]
 2 edgemvd01-bbone.lacnic.net.uy (200.7.84.34) 0.376 ms [254]
 3 ibb2cor3-be200-1703.antel.net.uy (200.40.98.29) 1.445 ms [253]
 4 192.168.2.217 (192.168.2.217) 174.307 ms [245]
   MPLS Label 34878 TTL=1 | 16032
 5 192.168.1.90 (192.168.1.90) 166.382 ms !T2 [244]
   MPLS Label 34243 TTL=2 | 16032
 6 192.168.2.166 (192.168.2.166) 167.931 ms !T3 [248]
   MPLS Label 24002 TTL=3 | 16032
 7 ibr2nyx2-te0-7-0-2.antel.net.uy (200.40.0.38) 173.225 ms [249]
 8 *
 9 *
10 *
11 *
12 *
13 *
14 *
```



255 - 254 = 1 hop a la vuelta

Asimetria de Caminos

```
esteban@server:~$ sudo paris-traceroute -q 1 -w 1 -M 7 ipv4-c367-nyc001-ix.1.oca.nflxvideo.net --print_ttl
```

```
traceroute [(179.0.156.2:33456) -> (23.246.7.195:33457)], protocol  
udp, algo hopbyhop, duration 35 s
```

```
1  
2  
3  
4  
5 M  
6 192.168.2.166 (192.168.2.166) 167.931 ms !13 [248]  
MPLS Label 24002 TTL=3 | 16032  
7 ibr2nyx2-te0-7-0-2.antel.net.uy (200.40.0.38) 173.225 ms [249]  
8 *  
9 *  
10 *  
11 *  
12 *  
13 *  
14 *
```

HAY ASIMETRIA

255 - 254 = 1 hop a la vuelta

Información DNS

- Consulta DNS reversa
- Se conoce la IP, se quiere conocer el dominio para esa IP
- ¿Para que nos sirve?
 - TLD
 - Código IANA
 - Sistema Autónomo

Bibliografía

- RFC 792
- <https://paris-traceroute.net/>