Daniel Alejandro Osornio López 0244685@up.edu.mx

Preguntas

Dirección MAC

```
ae@march ~> ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT
group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: enp3s0f0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP mode
DEFAULT group default qlen 1000
    link/ether 98:5a:eb:d3:c0:3c brd ff:ff:ff:ff:ff:ff
```

Dirección IPv4 & IPv6

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp3s0f0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group
default qlen 1000
    link/ether 98:5a:eb:d3:c0:3c brd ff:ff:ff:ff:ff:ff
    inet 172.25.133.34/24 brd 172.25.133.255 scope global enp3s0f0
       valid_lft forever preferred_lft forever
    inet6 2801:f0:20:c00:172:25:133:34/59 scope global
       valid_lft forever preferred_lft forever
    inet6 fe80::9a5a:ebff:fed3:c03c/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
```

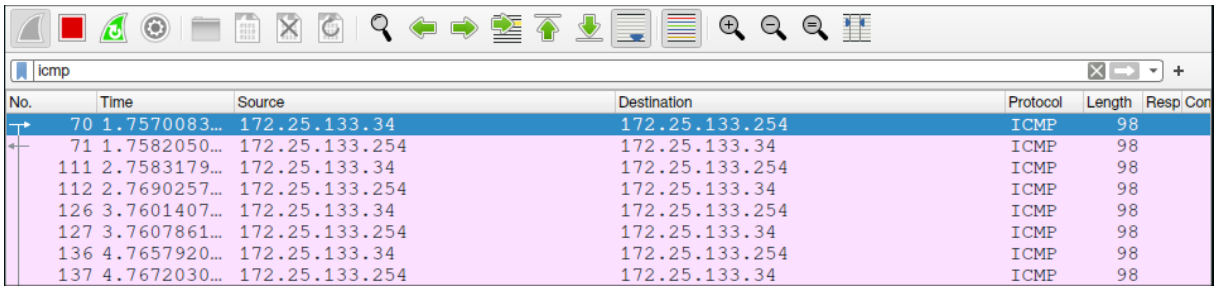
Es decir que mi dirección MAC es 98:5a:eb:d3:c0:3c, y la dirección IPv4 privada es 172.25.133.34, mientras que la dirección IPv6 es 2801:f0:20:c00:172:25:133:34.

Captura y Ping local

En mi red local hice ping al gateaway a la vez que le di a capturar en Wireshark

```
ae@march ~> ping 172.25.133.254
PING 172.25.133.254 (172.25.133.254) 56(84) bytes of data.
64 bytes from 172.25.133.254: icmp_seq=1 ttl=255 time=1.25 ms
64 bytes from 172.25.133.254: icmp_seq=2 ttl=255 time=10.7 ms
64 bytes from 172.25.133.254: icmp_seq=3 ttl=255 time=0.670 ms
64 bytes from 172.25.133.254: icmp_seq=4 ttl=255 time=1.44 ms
64 bytes from 172.25.133.254: icmp_seq=5 ttl=255 time=0.670 ms
64 bytes from 172.25.133.254: icmp_seq=6 ttl=255 time=53.6 ms
64 bytes from 172.25.133.254: icmp_seq=7 ttl=255 time=23.9 ms
64 bytes from 172.25.133.254: icmp_seq=8 ttl=255 time=8.93 ms
^C
--- 172.25.133.254 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7035ms
rtt min/avg/max/mdev = 0.670/12.646/53.579/17.181 ms
```

En wireshark podemos ver los paquetes intercambiados:



La MAC de ambos concuerda, se obtiene por medio de una solicitud ARP que el gateaway (en este caso) manda a todos los dispositivos de la red.

Captura datos remotos

Hice `ping` con un limite de 1 paquete para cada uno de los nombres dados:

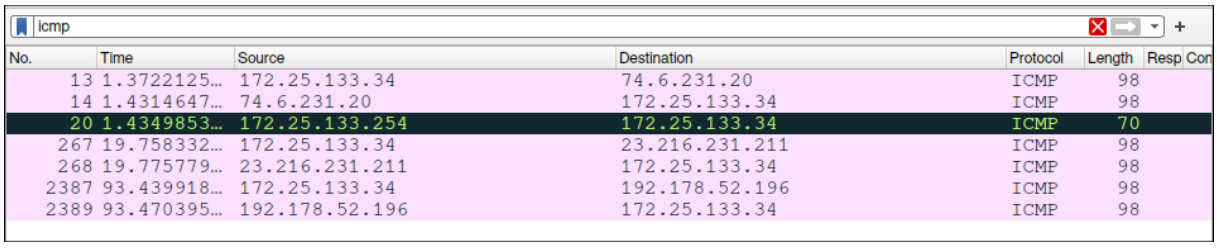
```
ae@march ~> ping -4 -c 1 www.yahoo.com
PING  (74.6.231.20) 56(84) bytes of data.
64 bytes from media-router-fp73.prod.media.vip.ne1.yahoo.com (74.6.231.20):
icmp_seq=1 ttl=50 time=59.3 ms

---  ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 59.265/59.265/59.265/0.000 ms
ae@march ~> ping -4 -c 1 www.cisco.com
PING  (23.216.231.211) 56(84) bytes of data.
64 bytes from a23-216-231-211.deploy.static.akamaitechnologies.com (23.216.231.211):
icmp_seq=1 ttl=56 time=17.5 ms

---  ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 17.463/17.463/17.463/0.000 ms
ae@march ~> ping -4 -c 1 www.google.com
PING  (192.178.52.196) 56(84) bytes of data.
64 bytes from tzqroa-ac-in-f4.1e100.net (192.178.52.196): icmp_seq=1 ttl=113
time=30.5 ms

---  ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 30.491/30.491/30.491/0.000 ms
ae@march ~>
```

Todos los paquetes intercambiados del tipo `icmp` se muestran en:



Las direcciones IP y MAC de los tres nombres, luego de inspeccionar los paquetes son:

Nombre	IP	MAC
www.yahoo.com	74.6.231.20	cc:ef:48:f8:52:7f

www.cisco.com	23.216.231.211	cc:ef:48:f8:52:7f
www.google.com	192.178.52.196	cc:ef:48:f8:52:7f

¿Qué es importante sobre esta información?

Las direcciones y *layers* involucrados

¿En qué se diferencia esta información de la información de ping local que recibió en la parte 1?

Todas las direcciones MAC son la misma

Pregunta reflexión

¿Por qué Wireshark muestra la dirección MAC vigente de los hosts locales, pero no la dirección MAC vigente de los hosts remotos?

Porque todos los paquetes son enviados al *gateaway*, quien en turno se encarga de mandar el mensaje hacia fuera de nuestra red local hasta que llegue nuestro mensaje a la máquina de destino.