Práctica/Laboratorio de Capa de Enlace

Amoroso, Lihuel Pablo 13497/2; Gasquez, Federico Ramón 13598/6

Grupo A

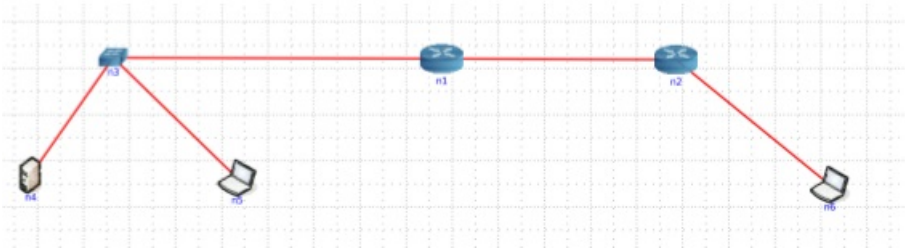

Figura 1: Topología

1. Genere la topología de la figura 1, asigne direcciones IP y arme el ruteo para que todos sean "visibles" por IP.

1.1. Realice el comando ping(echo request) de n6 a n5 y capture el tráfico. Muestre encabezados Ethernet, y, de los contenidos, indique tipo de paquete, IP origen, IP destino cuando corresponda. Analice la diferencia entre las tramas IP y los mensajes ARP.

N6(eth0)
ARP request
Encabezados Ethernet

- Src: 00:00:00_aa:00:06 (00:00:00:aa:00:06)
- Dst: Broadcast (ff:ff:ff:ff:ff:ff)

- Type: ARP (0x0806)

Paquete ARP

- Sender IP address: 10.0.2.2 (10.0.2.2)
- Target IP address: 10.0.2.1 (10.0.2.1)

ARP reply

Encabezados Ethernet

- Src: 00:00:00_aa:00:05 (00:00:00:aa:00:05)
- Dst: 00:00:00_aa:00:06 (00:00:00:aa:00:06)
- Type: ARP (0x0806)

Paquete ARP

- Sender IP address: 10.0.2.1 (10.0.2.1)
- Target IP address: 10.0.2.2 (10.0.2.2)

ICMP request

Encabezados Ethernet

- Src: 00:00:00_aa:00:06 (00:00:00:aa:00:06)
- Dst: 00:00:00_aa:00:05 (00:00:00:aa:00:05)
- Type: IP (0x0800)

Paquete IP

- Source: 10.0.2.2 (10.0.2.2)
- Destination: 10.0.0.3 (10.0.0.3)

ICMP reply

Encabezados Ethernet

- Src: 00:00:00_aa:00:05 (00:00:00:aa:00:05)
- Dst: 00:00:00_aa:00:06 (00:00:00:aa:00:06)
- Type: IP (0x0800)

Paquete IP

- Source: 10.0.0.3 (10.0.0.3)
- Destination: 10.0.2.2 (10.0.2.2)

N2(eth0)

ARP request

Encabezados Ethernet

- Src: 00:00:00_aa:00:04 (00:00:00:aa:00:04)
- Dst: 00:00:00_aa:00:03 (00:00:00:aa:00:03)
- Type: ARP (0x0806)

Paquete ARP

- Sender IP address: 10.0.1.2 (10.0.1.2)
- Target IP address: 10.0.1.1 (10.0.1.1)

ARP reply

Encabezados Ethernet

- Src: 00:00:00_aa:00:03 (00:00:00:aa:00:03)
- Dst: 00:00:00_aa:00:04 (00:00:00:aa:00:04)
- Type: ARP (0x0806)

Paquete ARP

- Sender IP address: 10.0.1.1 (10.0.1.1)

- Target IP address: 10.0.1.2 (10.0.1.2)

ICMP request

Encabezados Ethernet

- Src: 00:00:00_aa:00:04 (00:00:00:aa:00:04)
- Dst: 00:00:00_aa:00:03 (00:00:00:aa:00:03)
- Type: IP (0x0800)

Paquete IP

- Source: 10.0.2.2 (10.0.2.2)
- Destination: 10.0.0.3 (10.0.0.3)

ICMP reply

Encabezados Ethernet

- Dst: 00:00:00_aa:00:03 (00:00:00:aa:00:03)
- Src: 00:00:00_aa:00:04 (00:00:00:aa:00:04)
- Type: IP (0x0800)

Paquete IP

- Source: 10.0.0.3 (10.0.0.3)
- Destination: 10.0.2.2 (10.0.2.2)

N1(eth0)

ARP request

Encabezados Ethernet

- Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02)
- Dst: Broadcast (ff:ff:ff:ff:ff:ff)

- Type: ARP (0x0806)

Paquete ARP

- Sender IP address: 10.0.0.1 (10.0.0.1)
- Target IP address: 10.0.0.3 (10.0.0.3)

ARP reply

Encabezados Ethernet

- Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01)
- Dst: 00:00:00_aa:00:02 (00:00:00:aa:00:02))
- Type: ARP (0x0806)

Paquete ARP

- Sender IP address: 10.0.0.3 (10.0.0.3)
- Target IP address: 10.0.0.1 (10.0.0.1)

ICMP request

Encabezados Ethernet

- Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02)
- Dst: 00:00:00_aa:00:01 (00:00:00:aa:00:01)
- Type: IP (0x0800)

Paquete IP

- Source: 10.0.2.2 (10.0.2.2)
- Destination: 10.0.0.3 (10.0.0.3)

ICMP reply

Encabezados Ethernet

- Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01)
- Dst: 00:00:00_aa:00:02 (00:00:00:aa:00:02)
- Type: IP (0x0800)

Paquete IP

- Source: 10.0.0.3 (10.0.0.3)
- Destination: 10.0.2.2 (10.0.2.2)

N5(eth0)

ARP request

Encabezados Ethernet

- Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02)
- Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Type: ARP (0x0806)

Paquete ARP

- Sender IP address: 10.0.0.1 (10.0.0.1)
- Target IP address: 10.0.0.3 (10.0.0.3)

ARP reply

Encabezados Ethernet

- Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01)
- Dst: 00:00:00_aa:00:02 (00:00:00:aa:00:02))
- Type: ARP (0x0806)

Paquete ARP

- Sender IP address: 10.0.0.3 (10.0.0.3)

- Target IP address: 10.0.0.1 (10.0.0.1)

ICMP request

Encabezados Ethernet

- Src: 00:00:00_aa:00:02 (00:00:00:aa:00:02)
- Dst: 00:00:00_aa:00:01 (00:00:00:aa:00:01)
- Type: IP (0x0800)

Paquete IP

- Source: 10.0.2.2 (10.0.2.2)
- Destination: 10.0.0.3 (10.0.0.3)

ICMP reply

Encabezados Ethernet

- Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01)
- Dst: 00:00:00_aa:00:02 (00:00:00:aa:00:02)
- Type: IP (0x0800)

Paquete IP

- Source: 10.0.0.3 (10.0.0.3)
- Destination: 10.0.2.2 (10.0.2.2)

Diferencia entre paquete IP y ARP: la diferencia está en la capa y, por lo tanto, en qué dato se modifica. El paquete IP pertenece a una capa más alta que ARP y la IP destino y fuente no se modifican en todo el trayecto(incluso sería un problema si se modificaran, puesto que no se podría continuar); sin embargo, la IP emisora y receptora en los paquetes ARP en cada interfaz se va modificando conforme necesita encontrar la siguiente para poder continuar y que se lleve a cabo el PING.

1.2. Con la captura anterior, analice los mensajes ARP involucrados en el ruteo.

Analizando los mensajes anteriores ARP entre las diferentes interfaces, se puede observar que ARP funciona de la siguiente manera:

1. Cuando una interfaz A quiere comunicarse con B envía un ARP request por broadcast, indicando que se busca la MAC de quien tenga la IP de B y que quien la tenga responda a A.
2. El ARP request se distribuye por todo el dominio de broadcast y, si alguien tiene la IP buscada, es ese quién contesta con una ARP reply.
3. Quien conteste el ARP request con un ARP reply sabe exactamente a quién contestarle: la información viene ya en el paquete.
4. Cuando B recibe el ARP request y contesta, éste indica que la IP buscada se encuentra en tal dirección de MAC.
5. Cuando A recibe el ARP reply de B, guarda la IP de B asociada a la MAC recibida. De esta manera es que A podrá comunicarse con B. Cada entrada tiene un TTL asociado, por lo que será necesario repetir este proceso periódicamente. Eventualmente, B podría guardarse también la MAC de A en su tabla ARP para futuras comunicaciones.

1.3. En n1 agregue una entrada estática en la tabla de ARP con la IP de n4 y la MAC de n5. Limpie las tablas de ARP y vuelva a hacer el ping de n6 a n5. Capture en simultáneo el tráfico en n4 y n5.

Lo que hicimos fue agregar una tabla estatica en n1 con la IP de n4 y MAC de n5. Usamos el comando que está abajo. Luego realizamos el ping de n6 a n5. Mientras el ping se llevaba a cabo, se adjunta lo que recolectó el TCPdump.

```
root@n1:/tmp/pycore.56332/n1.conf# arp -s 10.0.0.2 00:00:00:aa:00:01
root@n1:/tmp/pycore.56332/n1.conf# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.0.2                 ether   00:00:00:aa:00:01   CM                    eth0
root@n1:/tmp/pycore.56332/n1.conf#
```

Figura 2: Comando ARP utilizado y tabla

```
root@n6:/tmp/pycore.56332/n6.conf# ping -c4 10.0.0.3
PING 10.0.0.3 (10.0.0.3) 56(84) bytes of data.
64 bytes from 10.0.0.3: icmp_seq=1 ttl=62 time=0.304 ms
64 bytes from 10.0.0.3: icmp_seq=2 ttl=62 time=0.310 ms
64 bytes from 10.0.0.3: icmp_seq=3 ttl=62 time=0.176 ms
64 bytes from 10.0.0.3: icmp_seq=4 ttl=62 time=0.232 ms

--- 10.0.0.3 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt min/avg/max/mdev = 0.176/0.255/0.310/0.057 ms
root@n6:/tmp/pycore.56332/n6.conf#
```

Figura 3: Ping de n6 a n5

```
root@n5:/tmp/pycore.56332/n5.conf# tcpdump -vv
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
16:23:08.678998 IP (tos 0xc0, ttl 1, id 3919, offset 0, flags [none], proto OSPF (89), length 64)
    10.0.0.1 > 224.0.0.5: OSPFv2, Hello, length 44
        Router-ID 10.0.0.1, Backbone Area, Authentication Type: none (0)
        Options [External]
          Hello Timer 10s, Dead Timer 40s, Mask 255.255.255.0, Priority 1
          Designated Router 10.0.0.1
16:23:08.795870 IP6 (class 0xc0, hlim 1, next-header OSPF (89) payload length: 36) fe80::200:ff:feaa:2 > ff02::5: OSPFv3, Hello, length 36
        Router-ID 10.0.0.1, Backbone Area
        Options [V6, External, Router]
          Hello Timer 10s, Dead Timer 40s, Interface-ID 0.0.6.199, Priority 1
          Designated Router 10.0.0.1
          Neighbor List:
16:23:09.045538 IP (tos 0xc0, ttl 64, id 45050, offset 0, flags [none], proto ICMP (1), length 95)
    10.0.0.1 > 10.0.0.2: ICMP net 172.28.0.29 unreachable, length 75
        IP (tos 0x0, ttl 64, id 38536, offset 0, flags [DF], proto UDP (17), length 67)
    10.0.0.2.58165 > 172.28.0.29.domain: [bad udp cksum 0xb67b -> 0x62e7!] 32812+ PTR? 1.0.0.10.in-addr.arpa. (39)
16:23:09.045560 IP (tos 0xc0, ttl 63, id 45050, offset 0, flags [none], proto ICMP (1), length 95)
    10.0.0.1 > 10.0.0.2: ICMP net 172.28.0.29 unreachable, length 75
        IP (tos 0x0, ttl 64, id 38536, offset 0, flags [DF], proto UDP (17), length 67)
    10.0.0.2.58165 > 172.28.0.29.domain: [bad udp cksum 0xb67b -> 0x62e7!] 32812+ PTR? 1.0.0.10.in-addr.arpa. (39)
^C16:23:09.576552 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 10.0.0.1 tell 10.0.0.3, length 28
16:23:09.576632 ARP, Ethernet (len 6), IPv4 (len 4), Reply 10.0.0.1 is-at 00:00:00:aa:00:02 (oui Ethernet), length 28
16:23:09.576638 IP (tos 0x0, ttl 64, id 42855, offset 0, flags [DF], proto UDP (17), length 68)
    10.0.0.3.42808 > 172.28.0.29.domain: [bad udp cksum 0xb67d -> 0x0c62!] 18490+ PTR? 5.0.0.224.in-addr.arpa. (40)
16:23:09.576722 IP (tos 0xc0, ttl 64, id 54669, offset 0, flags [none], proto ICMP (1), length 96)
    10.0.0.1 > 10.0.0.3: ICMP net 172.28.0.29 unreachable, length 76
        IP (tos 0x0, ttl 64, id 42855, offset 0, flags [DF], proto UDP (17), length 68)
    10.0.0.3.42808 > 172.28.0.29.domain: [bad udp cksum 0xb67d -> 0x0c62!] 18490+ PTR? 5.0.0.224.in-addr.arpa. (40)
```

Figura 4: TCPdump de n4

```
root@n4:/tmp/pycore.56332/n4.conf# tcpdump -vv
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
16:22:58.678370 IP (tos 0xc0, ttl 1, id 3917, offset 0, flags [none], proto OSPF (89), length 64)
    10.0.0.1 > 224.0.0.5: OSPFv2, Hello, length 44
        Router-ID 10.0.0.1, Backbone Area, Authentication Type: none (0)
        Options [External]
          Hello Timer 10s, Dead Timer 40s, Mask 255.255.255.0, Priority 1
          Designated Router 10.0.0.1
16:22:58.785348 IP6 (class 0xc0, hlim 1, next-header OSPF (89) payload length: 36) fe80::200:ff:feaa:2 > ff02::5: OSPFv3, Hello, length 36
        Router-ID 10.0.0.1, Backbone Area
        Options [V6, External, Router]
          Hello Timer 10s, Dead Timer 40s, Interface-ID 0.0.6.199, Priority 1
          Designated Router 10.0.0.1
          Neighbor List:
16:22:59.033704 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 10.0.0.1 tell 10.0.0.2, length 28
16:22:59.033769 ARP, Ethernet (len 6), IPv4 (len 4), Reply 10.0.0.1 is-at 00:00:00:aa:00:02 (oui Ethernet), length 28
16:22:59.033775 IP (tos 0x0, ttl 64, id 36876, offset 0, flags [DF], proto UDP (17), length 68)
    10.0.0.2.39949 > 172.28.0.29.domain: [bad udp cksum 0xb67c -> 0x975a!] 51309+ PTR? 5.0.0.224.in-addr.arpa. (40)
16:22:59.033885 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 10.0.0.2 tell 10.0.0.3, length 28
16:22:59.033900 ARP, Ethernet (len 6), IPv4 (len 4), Reply 10.0.0.2 is-at 00:00:00:aa:00:00 (oui Ethernet), length 28
16:22:59.033917 IP (tos 0xc0, ttl 63, id 44888, offset 0, flags [none], proto ICMP (1), length 96)
    10.0.0.1 > 10.0.0.2: ICMP net 172.28.0.29 unreachable, length 76
        IP (tos 0x0, ttl 64, id 36876, offset 0, flags [DF], proto UDP (17), length 68)
    10.0.0.2.39949 > 172.28.0.29.domain: [bad udp cksum 0xb67c -> 0x975a!] 51309+ PTR? 5.0.0.224.in-addr.arpa. (40)
16:23:04.039498 IP (tos 0x0, ttl 64, id 38050, offset 0, flags [DF], proto UDP (17), length 68)
    10.0.0.2.39949 > 172.28.0.29.domain: [bad udp cksum 0xb67c -> 0x975a!] 51309+ PTR? 5.0.0.224.in-addr.arpa. (40)
16:23:04.039634 IP (tos 0xc0, ttl 63, id 44909, offset 0, flags [none], proto ICMP (1), length 96)
    10.0.0.1 > 10.0.0.2: ICMP net 172.28.0.29 unreachable, length 76
        IP (tos 0x0, ttl 64, id 38050, offset 0, flags [DF], proto UDP (17), length 68)
    10.0.0.2.39949 > 172.28.0.29.domain: [bad udp cksum 0xb67c -> 0x975a!] 51309+ PTR? 5.0.0.224.in-addr.arpa. (40)
16:23:59.097784 IP (tos 0x0, ttl 64, id 44402, offset 0, flags [DF], proto UDP (17), length 67)
    10.0.0.2.41926 > 172.28.0.29.domain: [bad udp cksum 0xb67b -> 0xb48a!] 28151+ PTR? 2.0.0.10.in-addr.arpa. (39)
16:23:59.097979 IP (tos 0xc0, ttl 63, id 52243, offset 0, flags [none], proto ICMP (1), length 95)
```

Figura 5: TCPdump de n5