

Redes de Computadoras 2020

TP1: Análisis de tráfico IPv6 en capa 3

Alumnos:

Losano Quintana, Juan Cruz (locxhalosano45@gmail.com)

Piñero, Tomás Santiago (tom-300@hotmail.com)

Docente:

Natasha Tomattis (natasha.tomattis@mi.unc.edu.ar)

Ayudantes: Aguerreberry Matthew, Sulca Sergio, Moral Ramiro

Objetivos

Configuración de dual stack(IPv4 e IPv6) en hosts usando el emulador CORE. Análisis de tráfico, comportamiento de *ARP*, *NDP* e *ICMP*. Asignación de direcciones de forma dinámica usando DHCP.

Requisitos

- Computadora por cada 2 personas

Consignas

Tráfico IPv4 e IPv6 con CORE

Recomendaciones

- Lea con cuidado las consignas
- Tenga certeza de los comandos que ejecuta

Diagrama de red

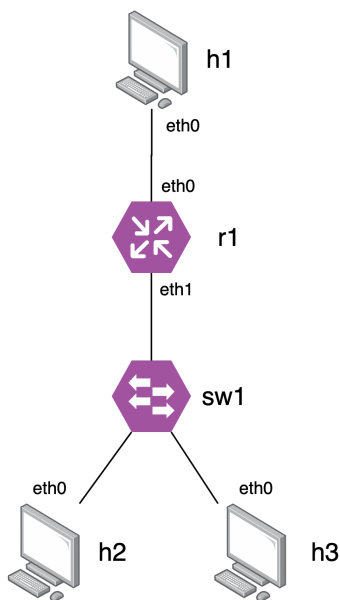


Tabla de asignación de direcciones IPv4 e IPv6

Computadora	Interfaz de red	Dirección IP
h1	eth0	IPv4: 192.168.1.10/24
		IPv6: 2001:aaaa:bbbb:1::10/64
h2	eth0	IPv4: 192.168.2.10/24
		IPv6: 2001:aaaa:cccc:1::10/64
h3	eth0	IPv4: 192.168.2.11/24
		IPv6: 2001:aaaa:cccc:1::11/64
r1	eth0	IPv4: 192.168.1.11/24
		IPv6: 2001:aaaa:bbbb:1::11/64
	eth1	IPv4: 192.168.2.12/24
		IPv6: 2001:aaaa:cccc:1::12/64

Consignas

1. Crear el esquema de red sobre el software de emulación CORE. ¿Cuál es la diferencia entre un simulador y un emulador?

La diferencia entre un emulador y un simulador es que el primero imita tanto el hardware como el software del objeto deseado, mientras que el segundo únicamente imita el software del objeto.

¿Por qué CORE es considerado un emulador?

CORE es considerado un emulador porque permite crear redes y conectarlas a redes y dispositivos reales.

¿Conoce algún simulador en el área de redes?

Sí, GNS3.

2. Probar conectividad entre todos los hosts enviando 3 paquetes ICMPv4 usando el comando “ping” para IPv4.

```
root@h1: /tmp/pycore.37005/h1.conf
File Edit View Search Terminal Help
root@h1:/tmp/pycore.37005/h1.conf# ping 192.168.2.10
PING 192.168.2.10 (192.168.2.10) 56(84) bytes of data.
64 bytes from 192.168.2.10: icmp_seq=1 ttl=63 time=0.129 ms
64 bytes from 192.168.2.10: icmp_seq=2 ttl=63 time=0.119 ms
64 bytes from 192.168.2.10: icmp_seq=3 ttl=63 time=0.121 ms
^C
--- 192.168.2.10 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2036ms
rtt min/avg/max/mdev = 0.119/0.123/0.129/0.004 ms
root@h1:/tmp/pycore.37005/h1.conf# ping 192.168.2.11
PING 192.168.2.11 (192.168.2.11) 56(84) bytes of data.
64 bytes from 192.168.2.11: icmp_seq=1 ttl=63 time=0.107 ms
64 bytes from 192.168.2.11: icmp_seq=2 ttl=63 time=0.136 ms
64 bytes from 192.168.2.11: icmp_seq=3 ttl=63 time=0.135 ms
^C
--- 192.168.2.11 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2030ms
rtt min/avg/max/mdev = 0.107/0.126/0.136/0.013 ms
root@h1:/tmp/pycore.37005/h1.conf#
```

3. Probar conectividad entre todos los hosts enviando 3 paquetes ICMPv6 usando el comando “ping6” para IPv6.

```
root@h1: /tmp/pycore.37005/h1.conf
File Edit View Search Terminal Help
root@h1:/tmp/pycore.37005/h1.conf# ping6 2001:aaaa:cccc:1::10
PING 2001:aaaa:cccc:1::10(2001:aaaa:cccc:1::10) 56 data bytes
64 bytes from 2001:aaaa:cccc:1::10: icmp_seq=1 ttl=63 time=0.153 ms
64 bytes from 2001:aaaa:cccc:1::10: icmp_seq=2 ttl=63 time=0.127 ms
64 bytes from 2001:aaaa:cccc:1::10: icmp_seq=3 ttl=63 time=0.135 ms
^C
--- 2001:aaaa:cccc:1::10 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2035ms
rtt min/avg/max/mdev = 0.127/0.138/0.153/0.014 ms
root@h1:/tmp/pycore.37005/h1.conf# ping6 2001:aaaa:cccc:1::11
PING 2001:aaaa:cccc:1::11(2001:aaaa:cccc:1::11) 56 data bytes
64 bytes from 2001:aaaa:cccc:1::11: icmp_seq=1 ttl=63 time=0.304 ms
64 bytes from 2001:aaaa:cccc:1::11: icmp_seq=2 ttl=63 time=0.134 ms
64 bytes from 2001:aaaa:cccc:1::11: icmp_seq=3 ttl=63 time=0.132 ms
^C
--- 2001:aaaa:cccc:1::11 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2026ms
rtt min/avg/max/mdev = 0.132/0.190/0.304/0.080 ms
root@h1:/tmp/pycore.37005/h1.conf#
```

4. Iniciar tráfico ICMP en el Cliente1 con destino Cliente2. Analizar tráfico con “tcpdump” sobre las dos redes, capturar screenshots y responder las siguientes preguntas:
 - a. ¿Cuáles son las comunicaciones ARP que suceden? Ejemplifica brevemente y con capturas cómo funciona la traducción de direcciones lógicas a direcciones físicas.

The image displays two Wireshark network traffic captures side-by-side. The left capture, labeled 'Host 1', shows an ARP request from 192.168.1.11 to 192.168.1.10 and a corresponding ARP reply. The right capture, labeled 'Router1 eth0', shows an ARP request from 192.168.1.11 to 192.168.1.10 and a corresponding ARP reply. Both screenshots show the packet details pane with the ARP protocol selected.

El host 1 manda un ARP request solicitando la MAC de 192.168.1.11, que es la interfaz eth0 del router 1, éste devuelve su MAC para que el host 1 la incorpore a su tabla ARP y a su vez el router 1 guarda en su tabla ARP la MAC del host 1.

El host 1 manda mensaje ICMP para el host 2 (192.168.2.10), cuando el paquete llega al router, la interfaz eth1 hace un ARP request para encontrar la dirección MAC del host 2 (192.168.2.10), que recibe el request ARP de r1-eth1 y le manda un reply con la MAC de su interfaz, y a su vez guarda la MAC de r1-eth1 en su tabla ARP.

Finalmente el router 1 guarda la MAC del host 2 en su tabla y manda el paquete ICMP.

- b. ¿Cuáles son las direcciones IPs en los datagramas IPs?

```
root@r1:/tmp/pycore.34791/r1.conf# tcpdump -v -X
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C16:47:22.388820 IP (tos 0x0, ttl 64, id 13572, offset 0, flags [DF], proto ICMP (1), length 84)
  192.168.1.10 > 192.168.2.10: ICMP echo request, id 42, seq 1, length 64
    0x0000: 4500 0054 3504 4000 4001 8140 c0a8 010a E..T5.@..@....
    0x0010: c0a8 020a 0800 cc8b 002a 0001 4a29 715e .....*..J)q^
    0x0020: 0000 0000 abee 0500 0000 0000 1011 1213 .....
    0x0030: 1415 1617 1819 1a1b 1c1d 1e1f 2021 2223 .....!"#
    0x0040: 2425 2627 2829 2a2b 2c2d 2e2f 3031 3233 $%&'()*+,-./0123
    0x0050: 3435 3637 4567
16:47:22.388872 IP (tos 0x0, ttl 63, id 52425, offset 0, flags [none], proto ICMP (1), length 84)
  192.168.2.10 > 192.168.1.10: ICMP echo reply, id 42, seq 1, length 64
    0x0000: 4500 0054 ccc9 0000 3f01 2a7b c0a8 020a E..T....?.*{....
    0x0010: c0a8 010a 0000 d48b 002a 0001 4a29 715e .....*..J)q^
    0x0020: 0000 0000 abee 0500 0000 0000 1011 1213 .....
    0x0030: 1415 1617 1819 1a1b 1c1d 1e1f 2021 2223 .....!"#
    0x0040: 2425 2627 2829 2a2b 2c2d 2e2f 3031 3233 $%&'()*+,-./0123
    0x0050: 3435 3637 4567
```

Las direcciones IP de origen están marcadas en verde, mientras que las de destino están marcadas en rojo.

- c. ¿Cómo sabe el router como comunicar un host con otro host?

A través de la dirección IP y usando la tabla ARP buscando la MAC.

- d. ¿Para qué usamos el switch? ¿Por que el switch no tiene asignadas direcciones IP en sus interfaces?

El switch se utiliza para conectar el host 2 con el host 3 porque el switch se encarga de la trama ethernet capa 2 y solo ve a dónde mandar paquetes a través de la dirección física.

- e. ¿Qué datos contiene la tabla ARP de h1?

La tabla ARP del host 1 muestra únicamente la dirección IP del default gateway al que se encuentra conectado.

```
root@h1:/tmp/pycore.37005/h1.conf
File Edit View Search Terminal Help
root@h1:/tmp/pycore.37005/h1.conf# arp -a
gateway (192.168.1.11) at 00:00:00:aa:00:01 [ether] on eth0
root@h1:/tmp/pycore.37005/h1.conf#
```

- f. ¿Qué datos contiene la tabla ARP de h3?

La tabla ARP del host 3 muestra únicamente la dirección IP del default gateway al que se encuentra conectado.

```
root@h3: /tmp/pycore.37005/h3.conf
File Edit View Search Terminal Help
root@h3:/tmp/pycore.37005/h3.conf# arp -a
gateway (192.168.2.12) at 00:00:00:aa:00:02 [ether] on eth0
root@h3:/tmp/pycore.37005/h3.conf#
```

- g. ¿Qué datos contiene la tabla ARP del router?

La tabla ARP del router muestra las direcciones IP de los dispositivos que tiene conectados a sus interfaces, que son el host1, host2 y host3.

```
root@r1: /tmp/pycore.37005/r1.conf
File Edit View Search Terminal Help
root@r1:/tmp/pycore.37005/r1.conf# arp -a
? (192.168.2.11) at 00:00:00:aa:00:04 [ether] on eth1
? (192.168.2.10) at 00:00:00:aa:00:03 [ether] on eth1
? (192.168.1.10) at 00:00:00:aa:00:00 [ether] on eth0
root@r1:/tmp/pycore.37005/r1.conf#
```

- h. ¿Qué son las direcciones de broadcast en IPv4? Cual es su utilidad?

La dirección de broadcast IPv4 es una dirección especial que utiliza la dirección más alta en el rango de la red, y sirve comunicar a todos los hosts pertenecientes a dicha red.

- i. ¿Qué son las direcciones de multicast en IPv6? Cual es su utilidad?

La dirección de multicast IPv6 es una dirección que pertenece a un grupo determinado de hosts dentro de la red, por lo que es utilizada para enviar los paquetes únicamente a los hosts interesados en él.

5. Iniciar tráfico ICMP v3 (IPv6) entre h1 y h3. Analizar el tráfico con “tcpdump” sobre las dos redes, capturar screenshots y responder a las siguientes preguntas:
 - a. ¿Cuáles son las comunicaciones NDP que suceden? Identifique los distintos tipos de mensajes NDP haciendo foco en las direcciones IP de origen y destino de cada uno.

```

root@r1: /tmp/pycore.35981/r1.conf
File Edit View Search Terminal Help
root@r1:/tmp/pycore.35981/r1.conf# tcpdump -i any 'ip6 && icmp6 && (ip6[40] == 1
33 || ip6[40] == 134 || ip6[40] == 135 || ip6[40] == 136)' -v -X
tcpdump: listening on any, link-type LINUX_SLL (Linux cooked), capture size 2621
44 bytes
20:40:43.604917 IP6 (hlim 255, next-header ICMPv6 (58) payload length: 16) fe80:
:fc19:c6ff:fe69:7248 > ip6-allrouters: [icmp6 sum ok] ICMP6, router solicitation
, length 16
    source link-address option (1), length 8 (1): fe:19:c6:69:72:48
    0x0000: 6000 0000 0010 3aff fe80 0000 0000 0000 .....
    0x0010: fc19 c6ff fe69 7248 ff02 0000 0000 0000 ....irH.....
    0x0020: 0000 0000 0000 0002 8500 1196 0000 0000 .....
    0x0030: 0101 fe19 c669 7248 .....irH
20:40:43.604960 IP6 (hlim 255, next-header ICMPv6 (58) payload length: 16) fe80:
:482d:f1ff:fe3b:728c > ip6-allrouters: [icmp6 sum ok] ICMP6, router solicitation
, length 16
    source link-address option (1), length 8 (1): 3e:be:09:bc:79:44
    0x0000: 6000 0000 0010 3aff fe80 0000 0000 0000 .....
    0x0010: 482d f1ff fe3b 728c ff02 0000 0000 0000 H-...;r.....
    0x0020: 0000 0000 0000 0002 8500 0f7a 0000 0000 .....Z....
    0x0030: 0101 3ebe 09bc 7944 ..>...yD
20:40:44.117183 IP6 (hlim 255, next-header ICMPv6 (58) payload length: 16) fe80:
:3cbe:9ff:febc:7944 > ip6-allrouters: [icmp6 sum ok] ICMP6, router solicitation,
length 16
    source link-address option (1), length 8 (1): 3e:be:09:bc:79:44
    0x0000: 6000 0000 0010 3aff fe80 0000 0000 0000 .....
    0x0010: 3cbe 09ff febc 7944 ff02 0000 0000 0000 <...yD.....
    0x0020: 0000 0000 0000 0002 8500 fbb0 0000 0000 .....
    0x0030: 0101 3ebe 09bc 7944 ..>...yD
20:40:44.161325 IP6 (hlim 255, next-header ICMPv6 (58) payload length: 32) 2001:
aaaa:bbbb:1::10 > ff02::1:ff00:11: [icmp6 sum ok] ICMP6, neighbor solicitation,
length 32, who has r1
    source link-address option (1), length 8 (1): 00:00:00:aa:00:00
    0x0000: 6000 0000 0020 3aff 2001 aaaa bbbb 0001 .....
    0x0010: 0000 0000 0000 0010 ff02 0000 0000 0000 .....
    0x0020: 0000 0001 ff00 0011 8700 6bf2 0000 0000 .....k.....
    0x0030: 2001 aaaa bbbb 0001 0000 0000 0000 0011 .....
    0x0040: 0101 0000 00aa 0000 .....
20:40:44.161346 IP6 (hlim 255, next-header ICMPv6 (58) payload length: 32) r1 >
2001:aaaa:bbbb:1::10: [icmp6 sum ok] ICMP6, neighbor advertisement, length 32, t
gt is r1, Flags [router, solicited, override]
    destination link-address option (2), length 8 (1): 00:00:00:aa:00:01
    0x0000: 6000 0000 0020 3aff 2001 aaaa bbbb 0001 .....
    0x0010: 0000 0000 0000 0011 2001 aaaa bbbb 0001 .....
    0x0020: 0000 0000 0000 0010 8800 018d e000 0000 .....
    0x0030: 2001 aaaa bbbb 0001 0000 0000 0000 0011 .....
    0x0040: 0201 0000 00aa 0001 .....

```

Los hosts envían un paquete router solicitation para encontrar los routers (marcado en celeste y en azul), a lo que el router responde con un router advertisement (no figura en la captura). Luego verifican los hosts vecinos por medio de neighbor solicitation, por lo que su vecino responde con un neighbor advertisement. La direcciones IP de Se puede ver la dirección IP de origen está marcada en rojo y la dirección destino en verde.

b. NDP reemplaza a ARP?

No, NDP no reemplaza a ARP, simplemente agrega mejoras y nuevas funcionalidades para IPv6.

c. Describa todas las funciones de NDP

- Autoconfiguración de direcciones IP: Al iniciar el sistema, los nodos crean de manera automática, por medio de la configuración automática sin estado (SLAAC, stateless address autoconfiguration), una dirección de enlace-local en cada interface con IPv6 habilitado
- Descubrimiento de routers y vecinos: permite a un host conocer a sus vecinos, es decir, le permite saber qué routers y qué hosts están conectados con él.
- Detección de direcciones duplicadas: los nodos son capaces de detectar si una dirección está siendo utilizada.
- Resolución de direcciones: es el proceso por el cual un nodo obtiene la dirección MAC de otro nodo de la red local a partir de su dirección de IPv6.
- Descubrimiento de servidores DNS: Como parte del proceso de arranque, el protocolo NDP de IPv6 provee una dirección de un servidor DNS.

d. ¿Existen direcciones de broadcast en IPv6? Como se reemplaza esta funcionalidad en IPv6?

No existen direcciones de broadcast en IPv6. Esta funcionalidad se reemplaza por el multicast, que consiste en enviar un paquete al "grupo de multicast" que tiene asociada una dirección.

e. ¿Cuál es la diferencia entre las direcciones link-local, unique-local, global? Ejemplificar. En qué caso usaría a cada una?

La diferencia entre ellas es el alcance que tienen. Link-local (fe80::/10) llega únicamente al sector de la red en la que el host se encuentra conectado; unique-local (fd00::/7) no puede salir de su red y la global (2000::/3) es la dirección pública.

Link-local es utilizada para el descubrimiento de vecinos y auto-address configuration. Unique-local es una dirección privada, por lo que pueden realizarse redes para organizaciones.

Links de ayuda

- [core/install.md at master · coreemu/core](#)
- Capítulos 6 y 22 Comer

Autoconfiguración de direcciones IPv4 en linux namespaces

Recomendaciones

- Lea con cuidado las consignas
- Tenga certeza de los comandos que ejecuta

Diagrama de red

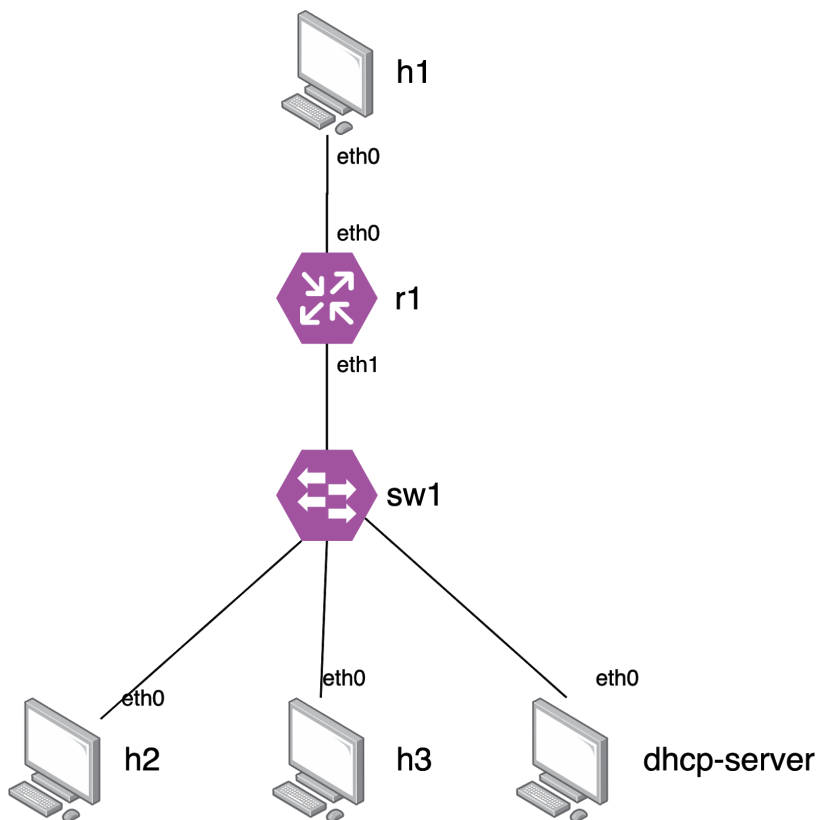


Tabla de asignación de direcciones IPv4

Computadora	Interfaz de red	Direccion IP
h1	eth0	IPv4: 192.168.1.10/24
dhcp-server	eth0	Pool: 192.168.2.0/24
r1	eth0	IPv4: 192.168.1.11/24
	eth1	IPv4: 192.168.2.12/24

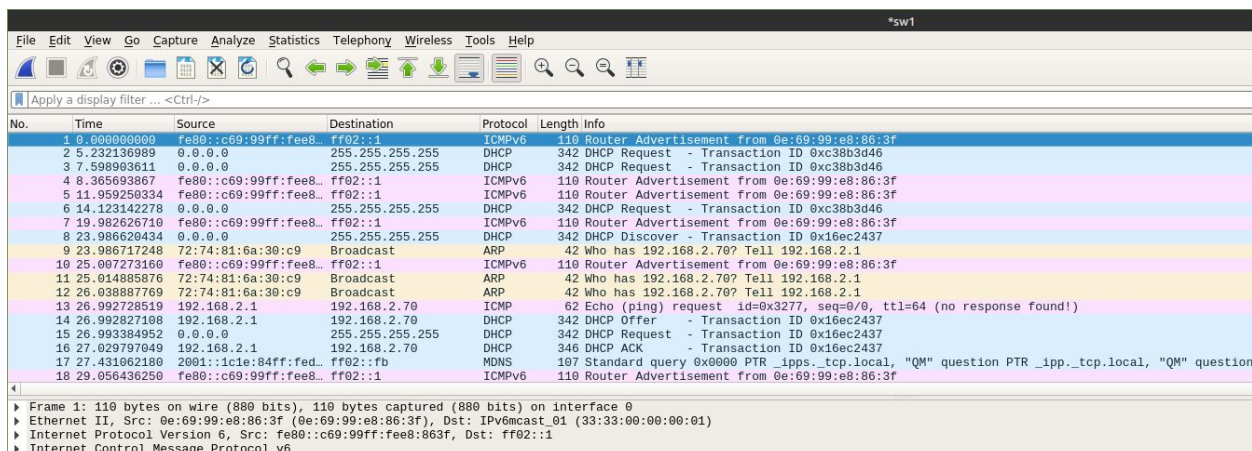
Consignas

1. Con linux namespaces defina la topología que se muestra en el diagrama. Ayuda: puede usar el script Gist que usamos en clase como base ya que la topología es la misma solo se agrega un host a la subnet de abajo
(<https://gist.github.com/natitomattis/be26889063203c0b33b33fa25c75a5b6>)
2. Configurar un dhcp server en el nuevo host, asegurarse que no entregue la IP del router que se asigno estaticamente.
3. Usando el comando `dhclient` configurar dinámicamente la IP de h2 y h3. Qué direcciones se les asignaron?

Dirección IP host 2: 192.168.2.103/24

Dirección IP host 3: 192.168.2.70/24

4. Explique brevemente y con capturas (tcpdump o wireshark) como funciona DHCP y los mensajes que intervienen.



The image shows a Wireshark packet capture interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons. The main display area shows a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The packets are filtered by 'Apply a display filter ... <Ctrl-F>'. The selected packet is packet 18, which is a DHCP Router Advertisement from 0e:69:99:e8:86:3f to ff02::1. The packet details pane shows the Ethernet II header, Internet Protocol Version 6 header, and Internet Control Message Protocol v6 header.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	fe80::c69:99ff:fee8...	ff02::1	ICMPv6	110	Router Advertisement from 0e:69:99:e8:86:3f
2	5.232136989	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xc38b3d46
3	7.598989611	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xc38b3d46
4	8.385693867	fe80::c69:99ff:fee8...	ff02::1	ICMPv6	110	Router Advertisement from 0e:69:99:e8:86:3f
5	11.959250334	fe80::c69:99ff:fee8...	ff02::1	ICMPv6	110	Router Advertisement from 0e:69:99:e8:86:3f
6	14.123142278	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xc38b3d46
7	19.982626710	fe80::c69:99ff:fee8...	ff02::1	ICMPv6	110	Router Advertisement from 0e:69:99:e8:86:3f
8	23.986620434	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x16ec2437
9	23.986717248	72:74:81:6a:30:c9	Broadcast	ARP	42	Who has 192.168.2.70? Tell 192.168.2.1
10	25.007273160	fe80::c69:99ff:fee8...	ff02::1	ICMPv6	110	Router Advertisement from 0e:69:99:e8:86:3f
11	25.014895876	72:74:81:6a:30:c9	Broadcast	ARP	42	Who has 192.168.2.70? Tell 192.168.2.1
12	26.038887769	72:74:81:6a:30:c9	Broadcast	ARP	42	Who has 192.168.2.70? Tell 192.168.2.1
13	26.992728519	192.168.2.1	192.168.2.70	ICMP	62	Echo (ping) request id=0x3277, seq=0/0, ttl=64 (no response found!)
14	26.992827108	192.168.2.1	192.168.2.70	DHCP	342	DHCP Offer - Transaction ID 0x16ec2437
15	26.993384952	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x16ec2437
16	27.029797049	192.168.2.1	192.168.2.70	DHCP	346	DHCP ACK - Transaction ID 0x16ec2437
17	27.431062180	2001::1c1e:84ff:fed...	ff02::fb	MDNS	107	Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR _ipps._tcp.local, "QM" question
18	29.056436250	fe80::c69:99ff:fee8...	ff02::1	ICMPv6	110	Router Advertisement from 0e:69:99:e8:86:3f

Frame 1: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface 0
Ethernet II, Src: 0e:69:99:e8:86:3f (0e:69:99:e8:86:3f), Dst: IPv6mcast_01 (33:33:00:00:00:01)
Internet Protocol Version 6, Src: fe80::c69:99ff:fee8:863f, Dst: ff02::1
Internet Control Message Protocol v6

El cliente envía un mensaje Discover (broadcast) buscando un servidor DHCP. Al recibir este mensaje, el servidor responde al cliente con un mensaje Offer ofreciendo la dirección IP junto con la máscara. Una vez recibido este mensaje y aceptada la oferta, el cliente le envía un mensaje Request para confirmar los datos recibidos, que son confirmados por el servidor enviando un mensaje Acknowledgment.

```
root@Archimedes: ~  
File Edit View Search Terminal Tabs Help  
root@Archimedes: /home/mrgreen x root@Archimedes: ~ x  
root@Archimedes:~# dnsmasq --dhcp-range=192.168.2.13,192.168.2.254,255.255.255.0  
--interface=vpeer-dhcp --no-daemon  
dnsmasq: started, version 2.79 cachesize 150  
dnsmasq: compile time options: IPv6 GNU-getopt DBus i18n IDN DHCP DHCPv6 no-Lua  
FTP conntrack ipset auth DNSSEC loop-detect inotify  
dnsmasq-dhcp: DHCP, IP range 192.168.2.13 -- 192.168.2.254, lease time 1h  
dnsmasq: reading /etc/resolv.conf  
dnsmasq: using nameserver 127.0.0.53#53  
dnsmasq: read /etc/hosts - 6 addresses  
dnsmasq-dhcp: DHCPDISCOVER(vpeer-dhcp) 192.168.2.54 06:7a:b5:2b:7a:3b  
dnsmasq-dhcp: DHCPDISCOVER(vpeer-dhcp) 192.168.2.70 06:7a:b5:2b:7a:3b  
dnsmasq-dhcp: DHCPREQUEST(vpeer-dhcp) 192.168.2.70 06:7a:b5:2b:7a:3b  
dnsmasq-dhcp: DHCPACK(vpeer-dhcp) 192.168.2.70 06:7a:b5:2b:7a:3b Archimedes  
root@Archimedes:~# ip netns exec h2 bash  
root@Archimedes:~# dhclient -d  
Internet Systems Consortium DHCP Client 4.3.5  
Copyright 2004-2016 Internet Systems Consortium.  
All rights reserved.  
For info, please visit https://www.isc.org/software/dhcp/  
Listening on LPF/vpeer2/06:7a:b5:2b:7a:3b  
Sending on LPF/vpeer2/06:7a:b5:2b:7a:3b  
Sending on Socket/fallback  
DHCPREQUEST of 192.168.2.54 on vpeer2 to 255.255.255.255 port 67 (xid=0x463d8bc3)  
DHCPREQUEST of 192.168.2.54 on vpeer2 to 255.255.255.255 port 67 (xid=0x463d8bc3)  
DHCPREQUEST of 192.168.2.54 on vpeer2 to 255.255.255.255 port 67 (xid=0x463d8bc3)  
DHCPDISCOVER on vpeer2 to 255.255.255.255 port 67 interval 3 (xid=0x16ec2437)  
DHCPREQUEST of 192.168.2.70 on vpeer2 to 255.255.255.255 port 67 (xid=0x3724ec16)  
DHCPDISCOVER on vpeer2 to 255.255.255.255 port 67 interval 3 (xid=0x16ec2437)  
DHCPOFFER of 192.168.2.70 from 192.168.2.1  
DHCPACK of 192.168.2.70 from 192.168.2.1  
bound to 192.168.2.70 -- renewal in 1769 seconds.
```

5. Hay conectividad entre h1 y el resto de los hosts ? Por qué ? Por que con IPv6 no tuvimos este inconveniente ? Realice las configuraciones necesarias para que funcione el ping entre h1 y el resto de los hosts.

No hay conectividad entre el host1 y el resto de los hosts porque IPv4 utiliza ARP y al no tener el próximo salto definido (gateway) no sabe a dónde ir para salir de su red, mientras que IPv6 utiliza NDP, lo que le permite conocer los dispositivos a los que el host está conectado fuera de su red, permitiéndole saber por dónde ir para llegar a hosts de otra red.

```
root@Archimedes: ~  
File Edit View Search Terminal Tabs Help  
root@Archimedes: ~ x root@Archimedes: ~ x root@Archimedes: ~ x  
root@Archimedes:~# ping 192.168.2.88  
PING 192.168.2.88 (192.168.2.88) 56(84) bytes of data.  
64 bytes from 192.168.2.88: icmp_seq=1 ttl=63 time=0.198 ms  
64 bytes from 192.168.2.88: icmp_seq=2 ttl=63 time=0.134 ms  
64 bytes from 192.168.2.88: icmp_seq=3 ttl=63 time=0.180 ms  
^C  
--- 192.168.2.88 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2033ms  
rtt min/avg/max/mdev = 0.134/0.170/0.198/0.030 ms  
root@Archimedes:~#
```

Ping del host 1 al host 2.


```
root@Archimedes: ~  
File Edit View Search Terminal Tabs Help  
root@Archimedes: ~ x root@Archimedes: ~ x root@Archimedes: ~ x [ + ] [ v ]  
root@Archimedes:~# ping 192.168.2.237  
PING 192.168.2.237 (192.168.2.237) 56(84) bytes of data.  
64 bytes from 192.168.2.237: icmp_seq=1 ttl=63 time=0.116 ms  
64 bytes from 192.168.2.237: icmp_seq=2 ttl=63 time=0.128 ms  
64 bytes from 192.168.2.237: icmp_seq=3 ttl=63 time=0.119 ms  
^C  
--- 192.168.2.237 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2048ms  
rtt min/avg/max/mdev = 0.116/0.121/0.128/0.005 ms  
root@Archimedes:~#
```

Ping del host 1 al host 3.

```
root@Archimedes: ~  
File Edit View Search Terminal Tabs Help  
root@Archimedes: ~ x root@Archimedes: ~ x root@Archimedes: ~ x [ + ] [ v ]  
root@Archimedes:~# ping 192.168.2.1  
PING 192.168.2.1 (192.168.2.1) 56(84) bytes of data.  
64 bytes from 192.168.2.1: icmp_seq=1 ttl=63 time=0.227 ms  
64 bytes from 192.168.2.1: icmp_seq=2 ttl=63 time=0.118 ms  
64 bytes from 192.168.2.1: icmp_seq=3 ttl=63 time=0.120 ms  
^C  
--- 192.168.2.1 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2052ms  
rtt min/avg/max/mdev = 0.118/0.155/0.227/0.050 ms  
root@Archimedes:~#
```

Ping del host 1 al dhcp-server.

Links de ayuda

- [DHCP configuration file /etc/dhcp/dhcpd.conf explained](#)
- Capítulo 22 Comer