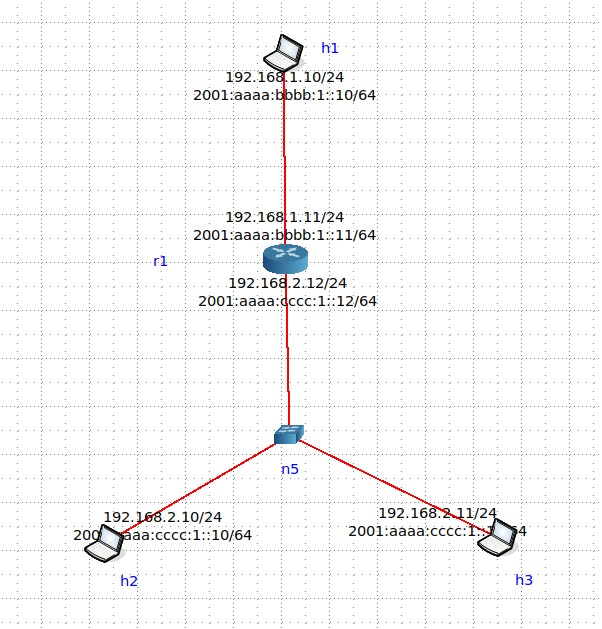
**TP1: Análisis de tráfico IPv6 en capa 3**

DESARROLLO

## A ) Tráfico IPv4 e IPv6 con CORE

1. Creación de esquema de red en CORE.



* ¿Cual es la diferencia entre un simulador y un emulador?

|  |  |
| --- | --- |
| Simulador | Emulador |
| Define un espacio definido por software (environment) | Define un espacio definido por software (environment) |
| Diseñado para crear un escenario que contiene todas las variables y configuraciones de software que pueden existir en el escenario real de la aplicación | Diseñado para imitar tanto las variables hardware como software. |
| No imitan el hardware. Solamente define escenarios software |  |
|  | Están entre medio de simuladores y dispositivos reales |
| Asegura que la aplicación cumple con performance esperada al interactuar con aplicaciones externas o escenarios | Prueba como el software interactúa con el hardware subyacente o con una combinación entre hardware/software |
| Permiten construir y evaluar modelos experimentales | Permiten evaluar el comportamiento real |

* ¿Por que CORE es considerado un emulador ?

Es considerado un emulador ya que me permite realizar operaciones y obtener funcionalidades que son posibles de realizar en una red verdadera (definición de emulador) y no sólo demostrar el comportamiento de la red.

Permite replicar una conexión cliente/servidor sin la necesidad de dispositivos reales como routers así como también replicar tráfico de red.

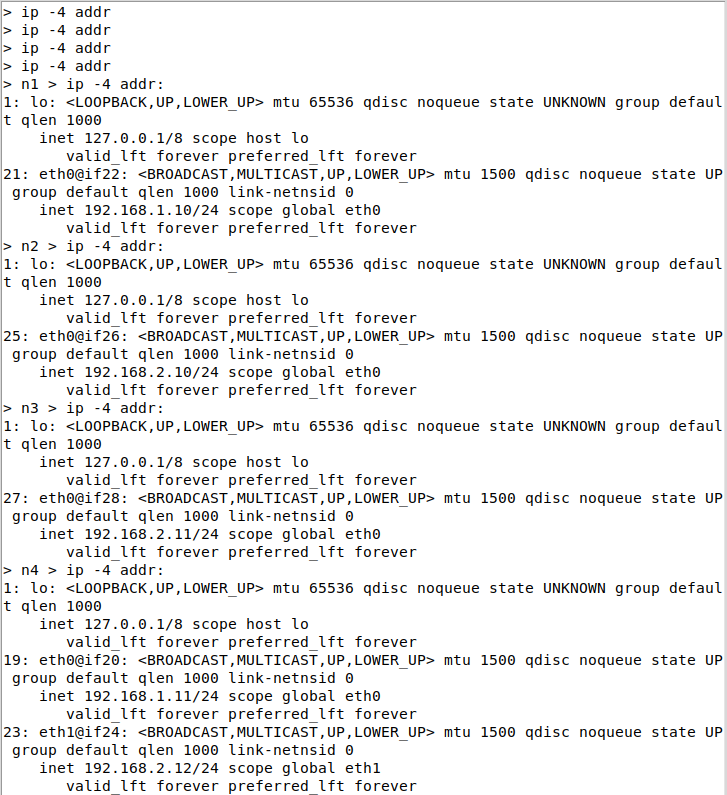
* ¿Conoce algún simulador en el área de redes ?

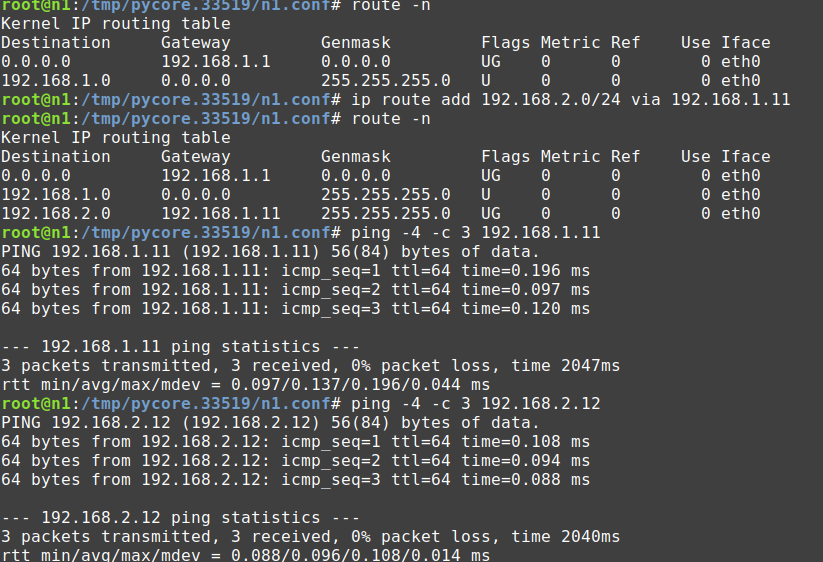
SI, GNS3 o Cisco Packet Tracer.

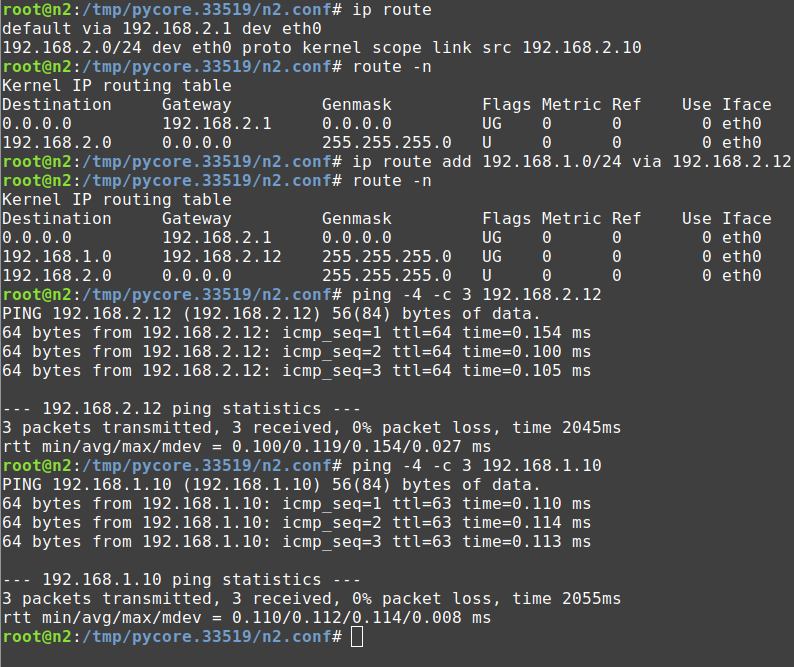
2) Conectividad entre hosts usando ICMPv4

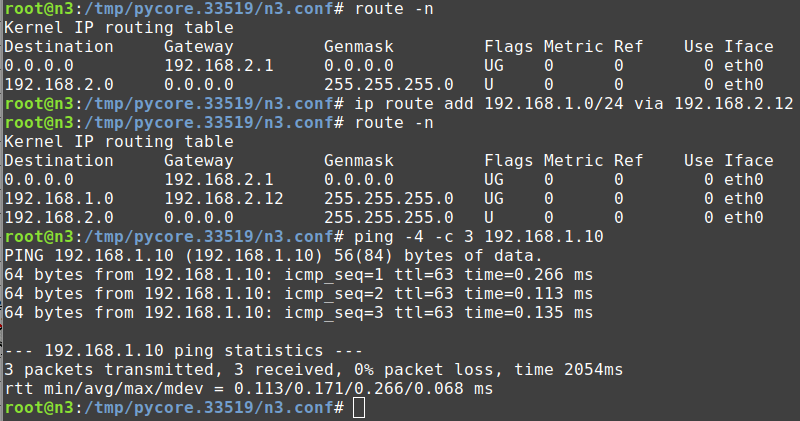
1. Utilizo la interfaz gráfica para setear elementos y enlaces.
2. Asigno dirección IPv4 e IPv6 mediante interfaz gráfica
3. Confgurar tablas de routeo en cada host

Comando: *ip route add* <DIRECCION DE SUBRED/MASCARA> *via* <DIRECCION DE SALIDA>



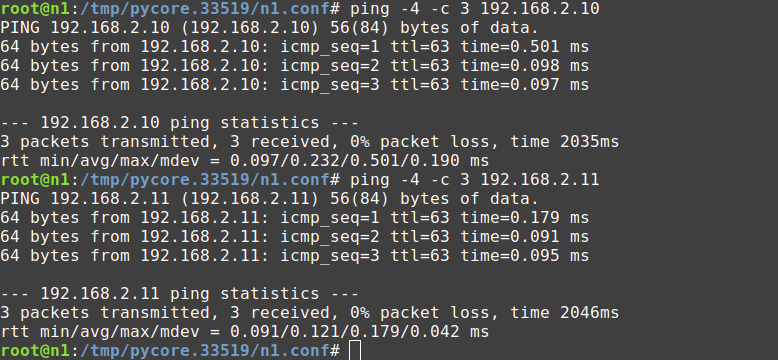


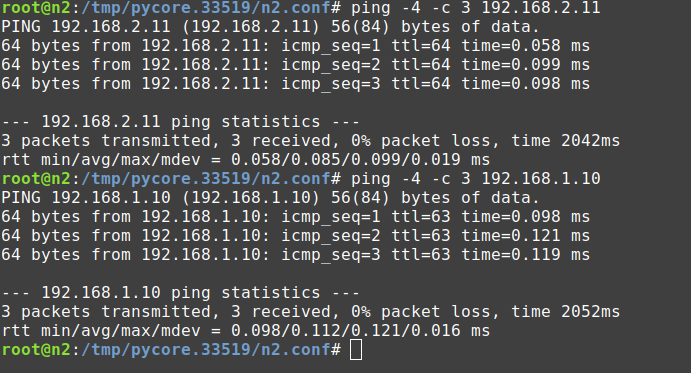




Envío ping de prueba utilizando el comando:

|  |
| --- |
| *ping -4 -c 3 <DESTINO>* |

**

**

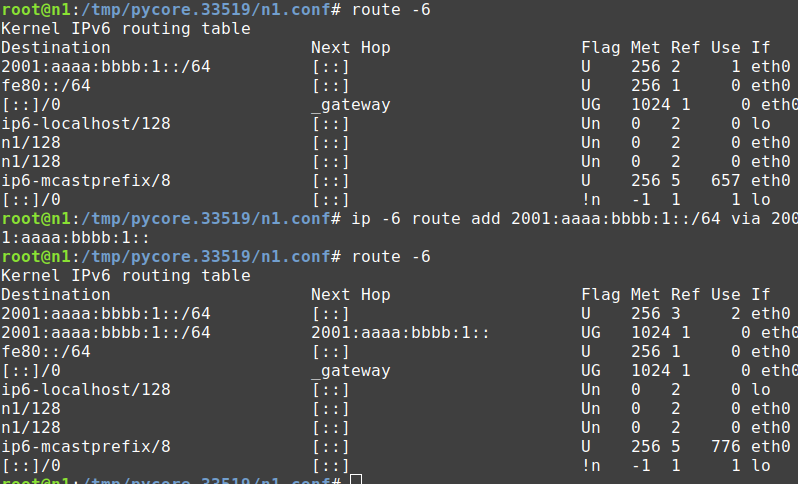
**

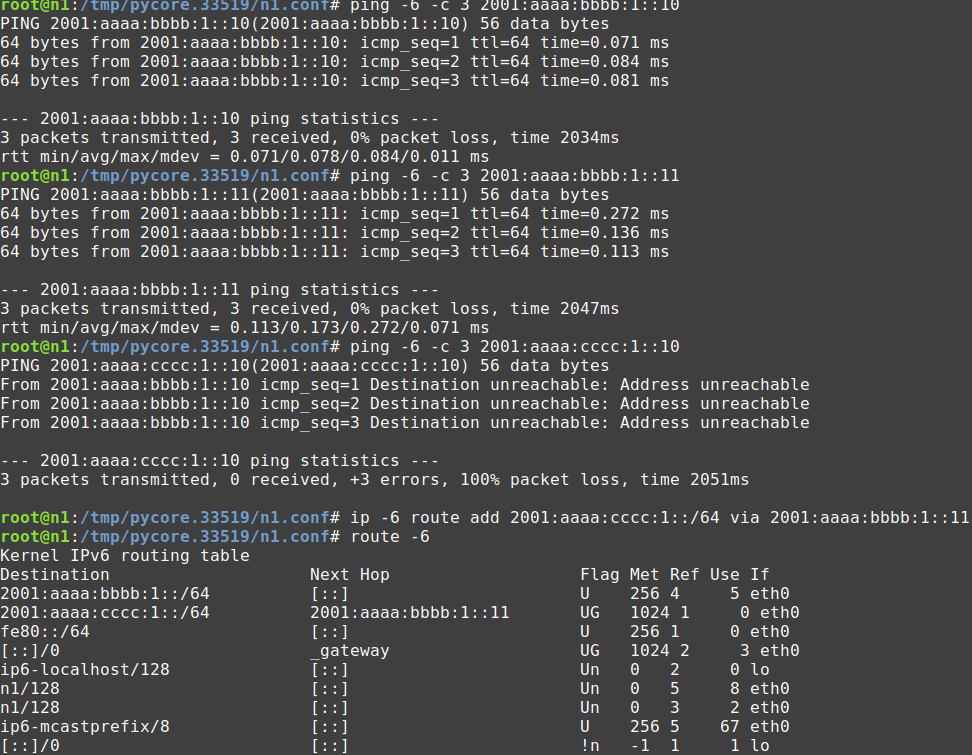
3) Conectividad entre hosts usando ICMPv6

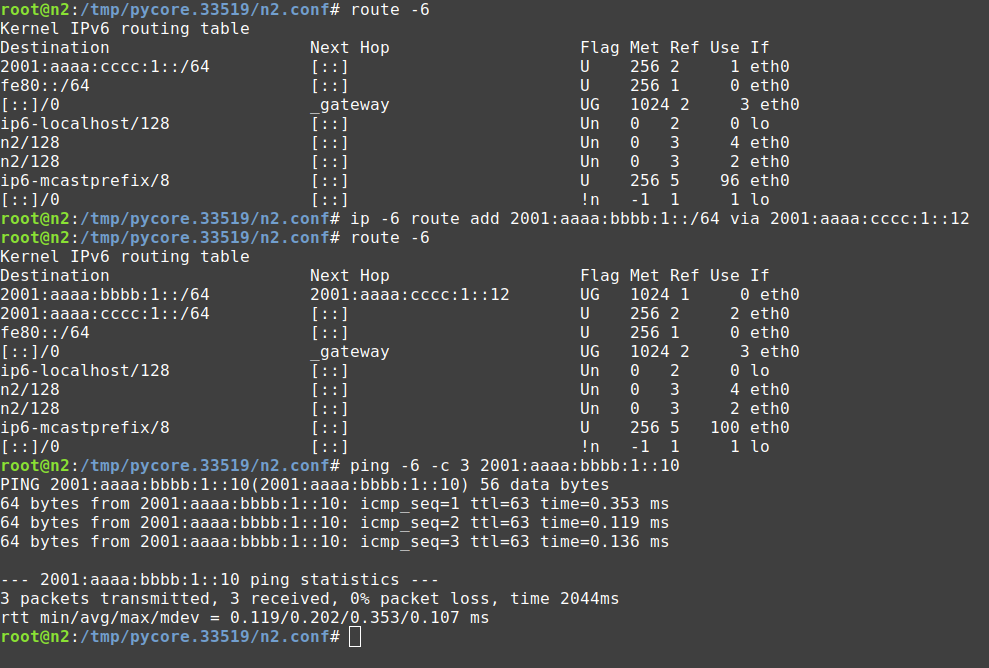
1. Configuro manualmente las tablas de routeo en cada host para IPv6

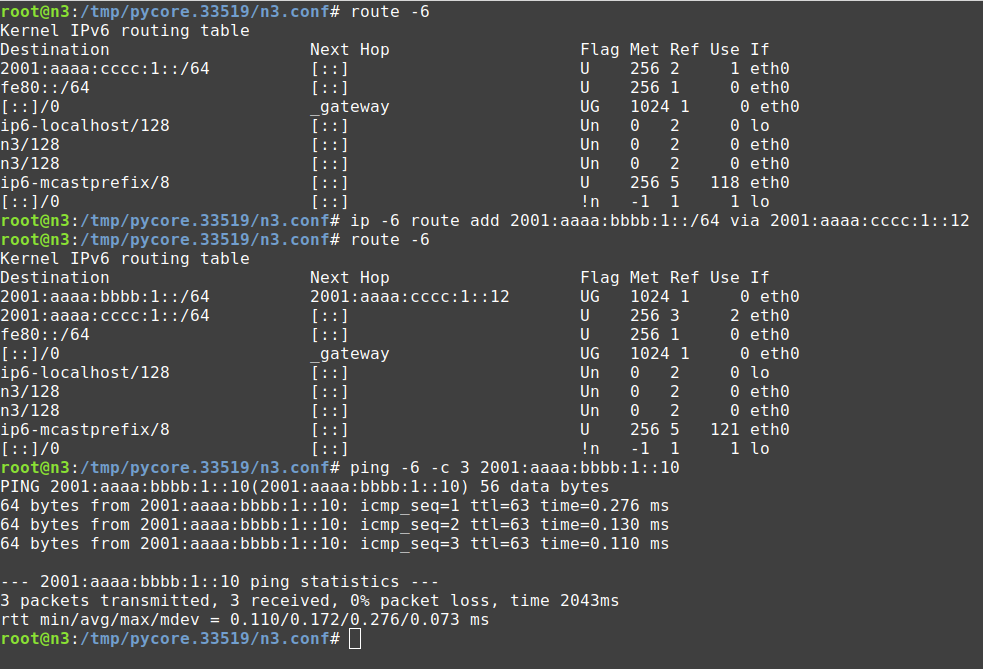
Comando:

*Ip -6 route add <DIRECCION DE SUBRED/MASCARA> via <DIRECCION DE SALIDA>*



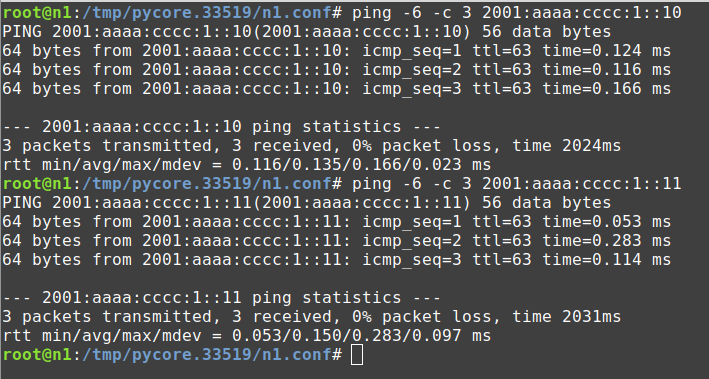




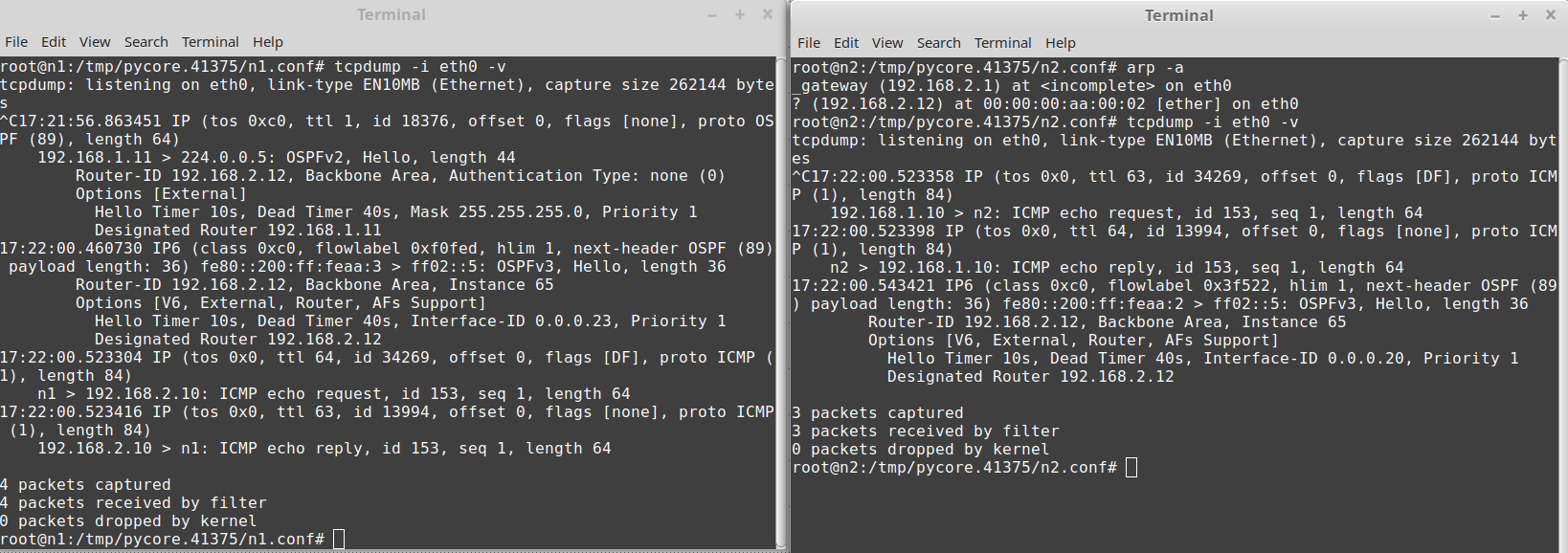


Envío ping para IPv6, utilizando el siguiente comando:

*ping -6 -c <CANT PAQUETES> <DIRECCIÓN DE DESTINO IPv6>*



4) Análisis de tráfico en IPv4





Borrado de tabla ARP en router



ICMPv3

1. ¿Cuáles son las comunicaciones ARP que suceden? Ejemplifica brevemente y con capturas cómo funciona la traducción de direcciones lógicas a direcciones físicas.

Recordar:

* Dirección lógica: dirección IP.
* Dirección física: dirección de MAC. Es única en todo el mundo y está asociada a la NIC (Network Interface Card)

Por lo tanto, para comunicarnos entre redes separadas debemos pasar de nuestra dirección lógica usada en la red local y utilizar la dirección física. Se usa ARP. Teniendo la dirección de capa 3 (IP) podemos obtener la dirección de capa 1 (MAC) para iniciar una comunicación entre dispositivos de redes no locales.

Las comunicaciones ARP que suceden son mensajes de tipo:

* Petición (Request)
* Respuesta (Reply)

1) El host que envía el ping (host **n1**) quiere enviar el mensaje hacia el host 2. Sabe que está fuera de su red y para comunicarse con la red 192.168.2.0/24 debe enviar el mensaje a 192.168.1.12 (router) pero no conoce la dirección MAC para enviar ya que su tabla ARP está vacía. Por lo tanto, envía un mensaje peticionando a éste por su MAC así como también envía su propia dirección MAC, 00:00:00:aa:00:04

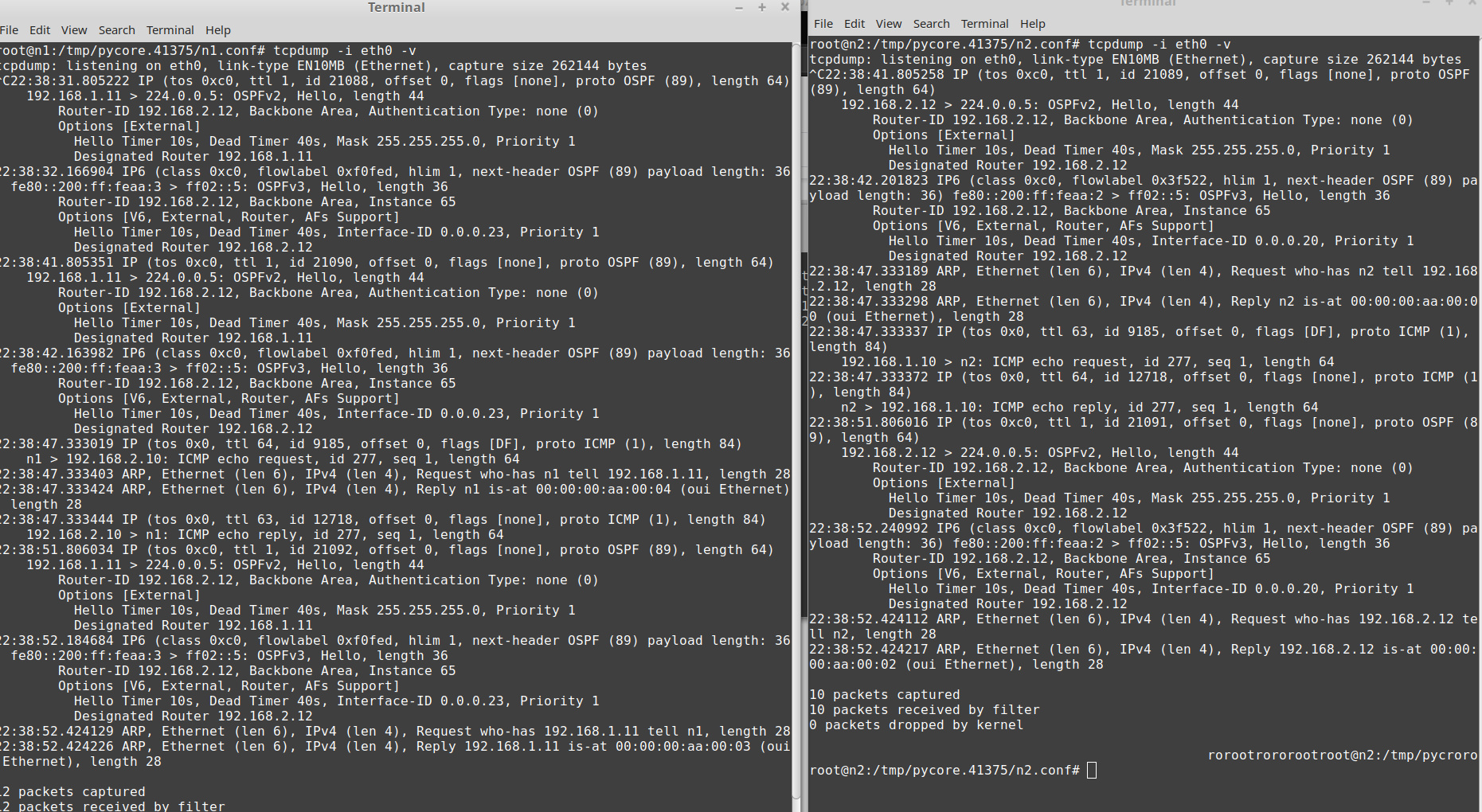
2) El router devuelve un mensaje ARP indicando al host n1 que el dispositivo con la dirección IP de próximo salto del router conectado a su red tiene como dirección MAC 00:00:00:aa:00:03.

En la otra red sucede lo siguiente:

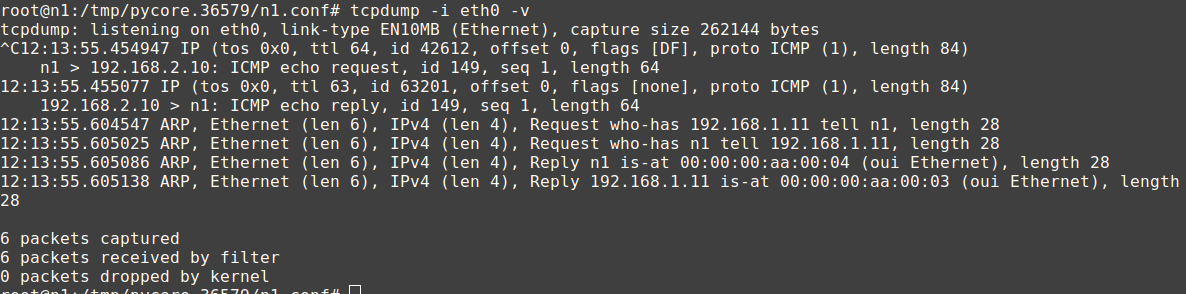
3) El router recibe el mensaje IP cuyo destino es el host 2 de la red contigua. Para ello, debe enviar el mensaje al enlace del router con la red 192.168.2.0/24

Como su tabla ARP sólo contiene la MAC del host 1, peticiona la MAC del host 2 teniendo en cuenta la dirección del destino del paquete IP, 192.168.2.10 (n2). Recibe un mensaje de respuesta con la MAC de host 2 y guarda en su tabla ARP.

4) El mensaje IP llega a host 2. Debe retornar el mensaje ping de respuesta a host 1, y como su tabla ARP está vacía, peticiona al router por la dirección MAC del enlace de salida (192.168.2.12). Recibe luego, por parte del router, un mensaje ARP de respuesta con la dirección MAC del enlace. Actualiza la tabla y puede finalmente enviar el ping de respuesta.



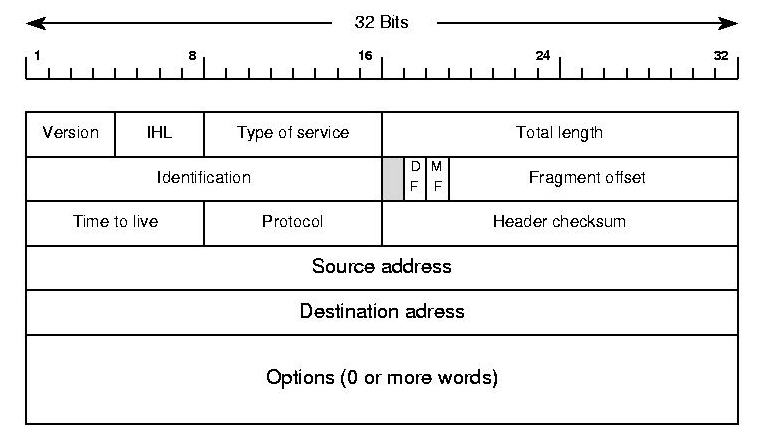
1. ¿Cuáles son las direcciones IPs en los datagramas IPs?



Direcciones:

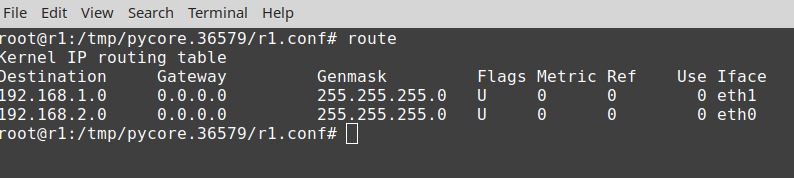
Source address: dirección IPv4 del host que envía el datagrama.

Destination address: dirección IPv4 del host al que está destinado el datagrama.



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

El router sabe como comunicar hosts de dos redes distintas debido a que contiene en su tabla de routeo las indicaciones sobre cual interfaz usar para comunicar mensajes que se trasmiten de una red a otra.



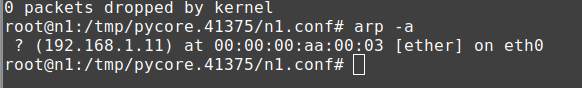
1. ¿Para qué usamos el switch? ¿Por que el switch no tiene asignadas direcciones IP en sus interfaces?

Utilizamos un switch para dar comunicación los distintos dispositivos que forman una red local. Permite transportar paquetes a uno o más de uno de los dispositivos a los que está conectado.

El switch no tiene asignada direcciones IP debido a que opera en capa 2 (capa de enlace) y utiliza direcciones MAC para poder realizar el direccionamiento de los datos. Para ello, el switch busca coincidencias en su tabla de direcciones MAC con la dirección de destino que el paquete recibido contiene.

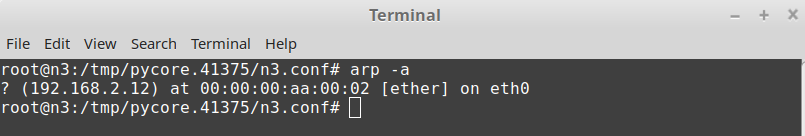
1. ¿Qué datos contiene la tabla ARP de h1?

Tabla ARP en host 1



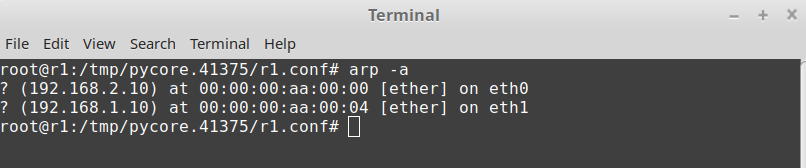
1. ¿Qué datos contiene la tabla ARP de h3?

Tabla ARP en host 3



1. ¿Qué datos contiene la tabla ARP del router?

Tabla ARP en router r1



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

Las direcciones broadcast en IPv4 se usan para enviar un mismo mensaje a todos los dispositivos conectados a dicha red.

1. ¿Qué son las direcciones de multicast en IPv4? Cual es su utilidad?

Permite enviar mensajes a un conjunto de varios (no necesariamente todos) dispositivos conectados a dicha red

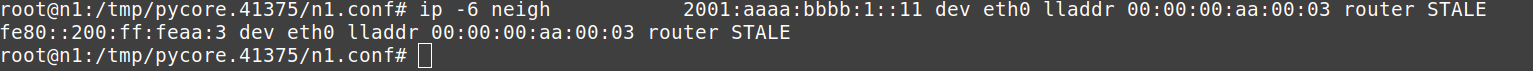
5) Análisis de tráfico para IPv6

Tabla de vecinos de IPv6 en router R1

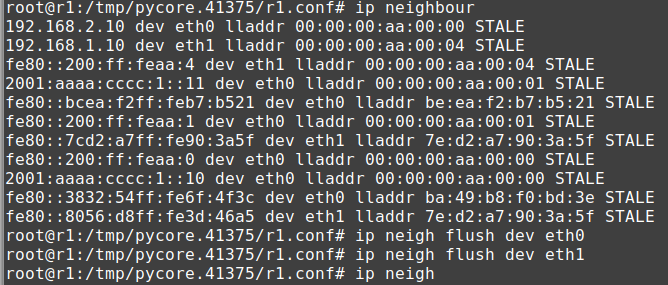
Cabe aclarar que las tablas de vecinos (neighbours table) se completa automáticamente en IPv6 al ejecutarse de forma instantánea el protocolo NDP al encender cada interfaz. Para observar los mensajes que se intercambian, se procede a borrar dicha tabla.



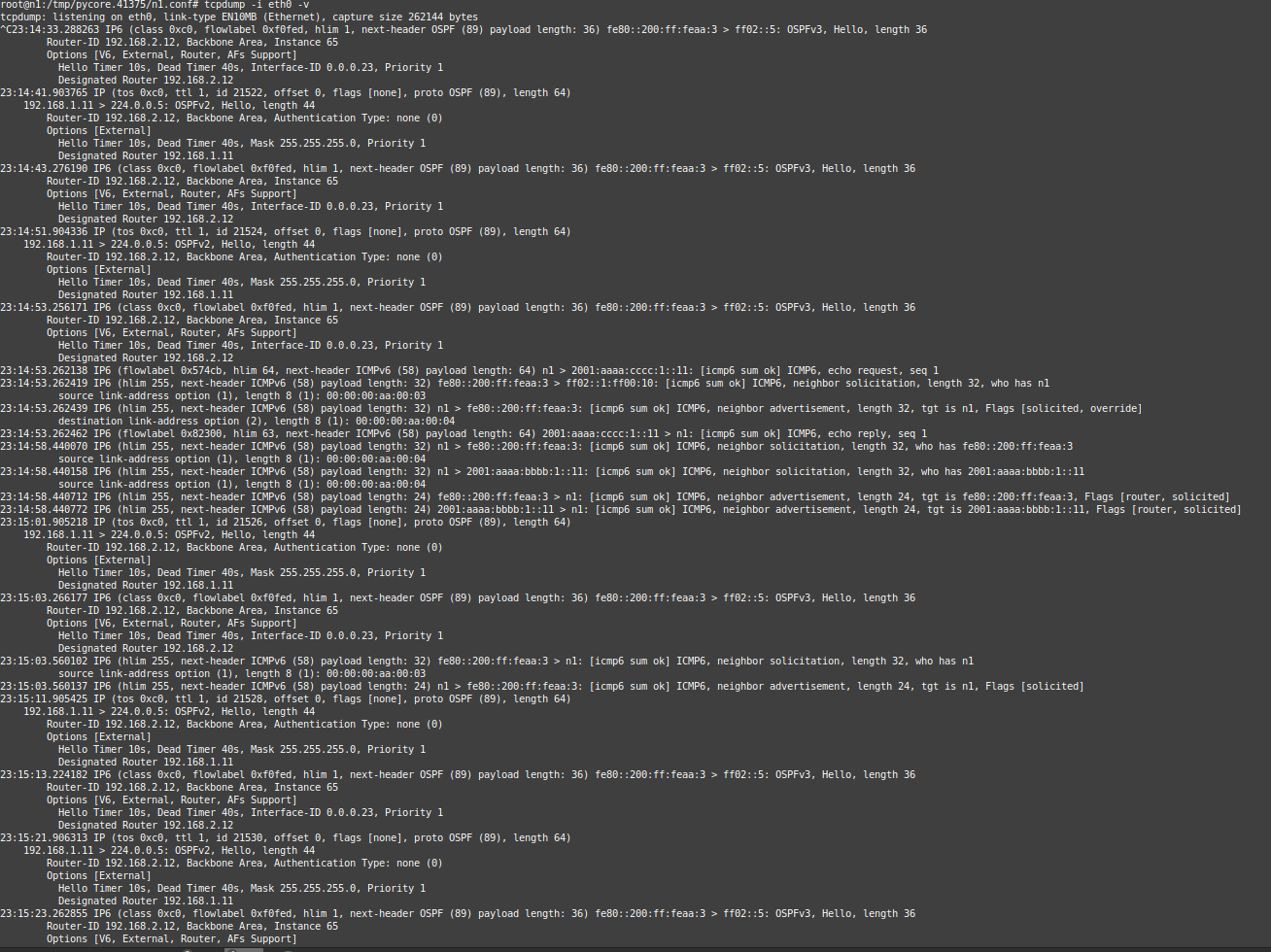
Tabla de vecinos en h1

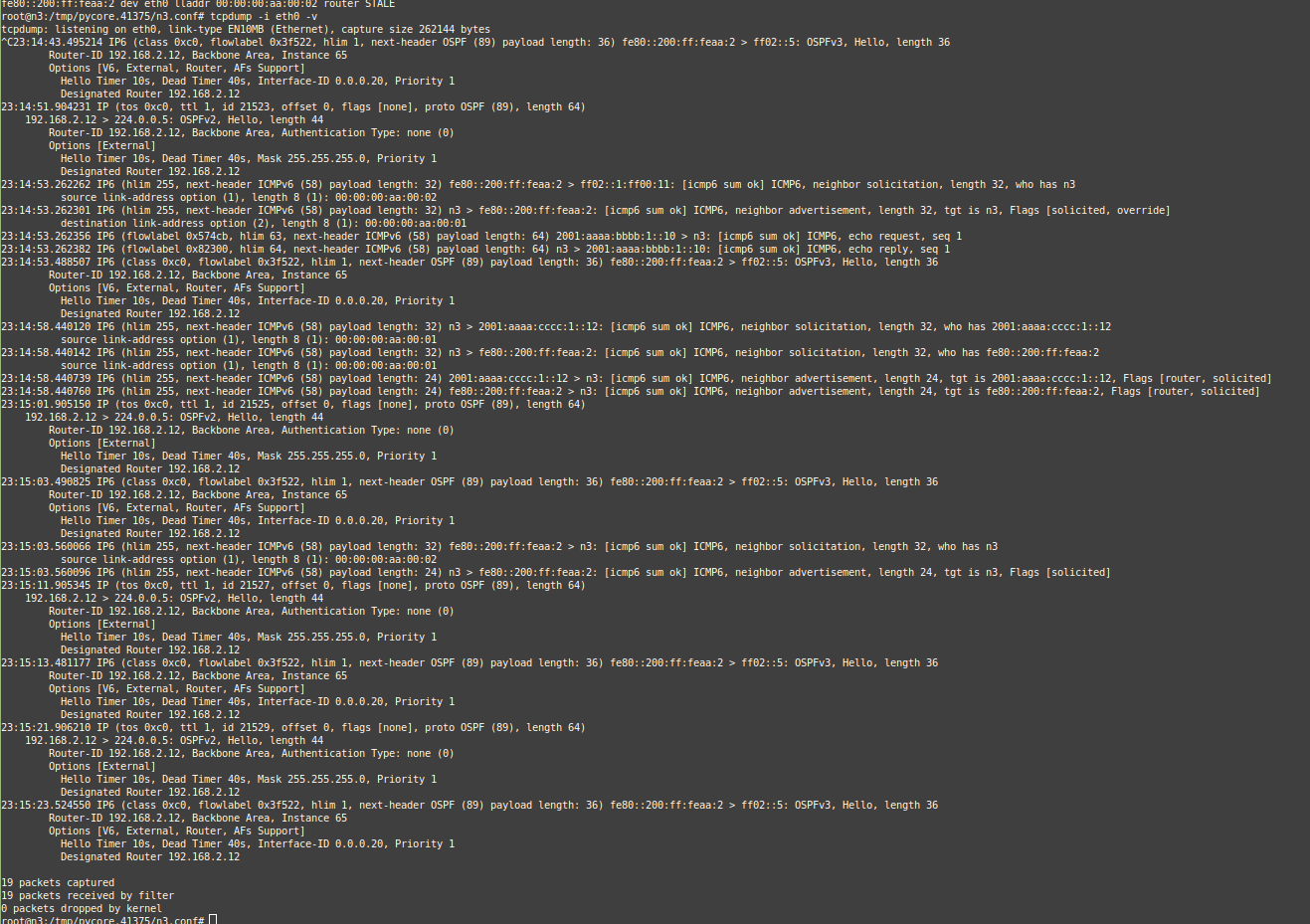


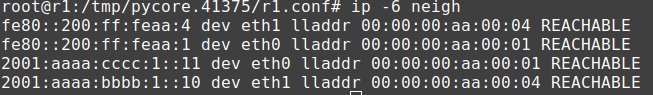
Borrar tabla de vecinos en r1



Con tabla limpia, inicio nuevo ping IPv6 y capturo tráfico

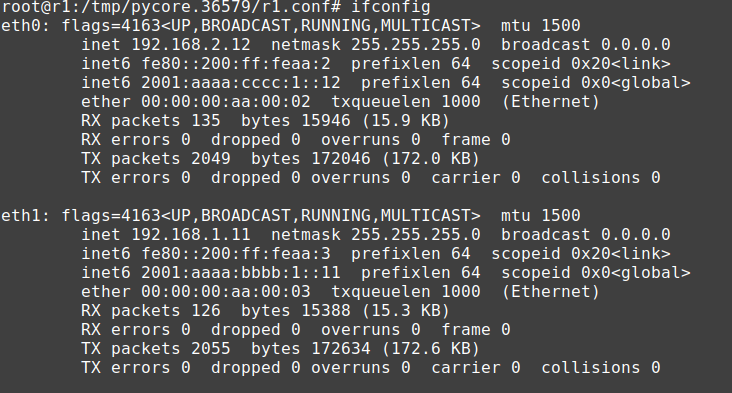






1. ¿Cuáles son las comunicaciones NDP que suceden? Identifique los distintos tipos de mensajes NDP haciendo foco en las direcciones IP de origen y destino de cada uno.

Cabe aclarar que el router posee dos direcciones IPv6 distintas en las dos interfaces del router, una dirección local y otra global. Siendo la global la configurada por nosotros. Pero, recolectando información, los usuarios de redes aconsejan no borrar las direcciones locales de interfaces ya que NDP utiliza la misma para su funcionamiento.



Se observan dos tipos de mensajes NDP (Neighbour Discovery Protocol)

* **Neighbour solicitation (NS):** enviado por host o router oara determinar la dirección MAC de un dispositivo vecino (conectado a él) o para verificar si todavía puede comunicarse con él mediante la MAC aprendida.
* **Neighbour advertisement (NA):** mensaje de respuesta a un mensaje de NS. También se usa para inidicar cambios en la dirección de capa de enlace del dispositivo.

En host 1, al intentar enviar el ping hacia el host 3, se produce el intercambio de mensajes NDP siguiente:

|  |  |  |  |
| --- | --- | --- | --- |
| i | Origen | Destino | Tipo mensaje NDP |
| 1 | fe80::200::ff:feaa:3: (interfaz r1 red 1) | Ff02::1:ff00:10:  (dirección multicast de red 1) | NS |
| 2 | 2001:aaaa:bbbb:1::11 (n1) | Fe80::200::ff:feaa:3 (r1) | NS |
| 3 | 2001:aaaa:bbbb:1::11 (n1) | 2001:aaaa:cccc:1::11 (n3) | NS |
| 4 | Fe80::200::ff:feaa:3  (interfaz r1 red 1) | 2001:aaaa:bbbb:1::11 (n1) | NA |
| 5 | 2001:aaaa:cccc:1::11 (n3) | 2001:aaaa:bbbb:1::11 (n1) | NA |
| 6 | Fe80::200::ff:feaa:3:  (interfaz r1 red 1) | 2001:aaaa:bbbb:1::11 (n1) | NS |
| 7 | 2001:aaaa:bbbb:1::11 (n1) | fe80::200::ff:feaa:3 (interfaz r1 red 1) | NA |
|  |  |  |  |

1. ¿NDP reemplaza a ARP?

Sí, el reemplazo de ARP en IPv6 es NDP. Es una nueva forma de encontrar las direcciones de capa de enlace de dispositivos en la red local. NDP utiliza mensajes ICMPv6 junto a direcciones multicast para poder lograr su cometido.

1. Describa todas las funciones de NDP

* Router solicitation:

Al activarse una interfaz de red, los hosts envían mensajes de solicitud de routers con el objetivo de que los routers respondan con mensajes de forma inmediata para poder conocer información y dirección de capa de enlace.

* Router advertisement

Un router envía periódicamente este mensaje enviando información de capa de red y de enlace a la red o para dar respuesta a mensajes de solicitud de routers.

Contiene información sobre direcciones de dispositivos de la misma red, configuración de direcciones, valores de salto, etc.

* Neighbour solicitation

Enviado por hosts o routers para conocer la dirección de capa de enlace de sus vecinos. También, puede ser usado para verificar si la dirección almacenada anteriormente todavía es válida para la comunicación con él.

* Neighbour advertisement

Mensaje enviado como respuesta a mensajes de solicitud. Además, el dispositivo de red puede enviar un NA para informar sobre cambios en su dirección de capa de enlace.

* Redirect

Utilizado por routers para informar a otros dispositivos de red sobre los mejores caminos disponibles hacia un destino.

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

No, IPv6 no implementa direcciones broadcast. En cambio, se utilizan direcciones multicast.

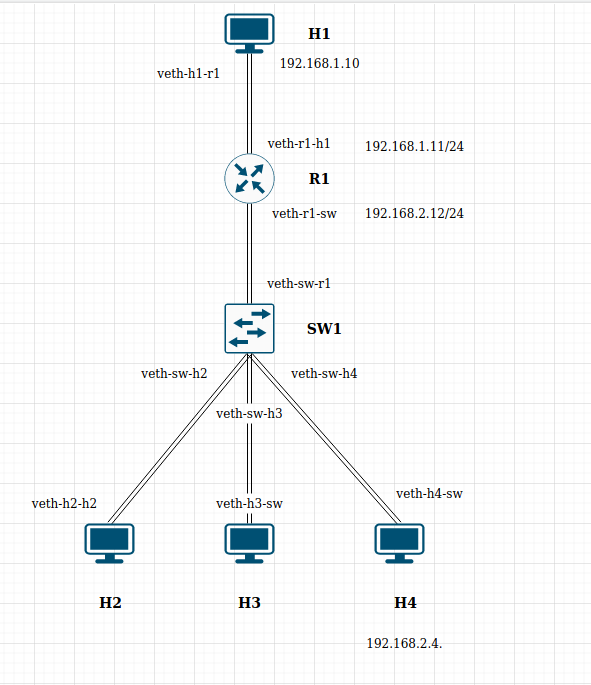
En IPv6, una dirección multicast permite llegar a TODOS los dispositivos de red que conforman un grupo. Así, se puede configurar una dirección multicast para varios grupos y enviar un mensaje IPv6 a ellos.

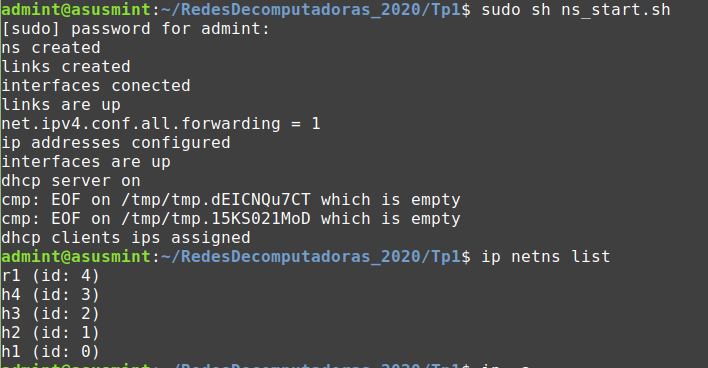
1. ¿Cuál es la diferencia entre las direcciones link-local, unique-local, global? Ejemplificar. En qué caso usaría a cada una ?

* Direcciones link-local:
* Empleadas para comunicarse entre dispositivos que comparten un mismo segmento de red.
* No son ruteables. No se pueden utilizar para comunicar dispositivos de diferente red. Los routers tampoco envían los mensajes a dispositivos en otros enlaces.
* Prefijo: fe80::/10
* Uso: descubrimiento (NDP) y comunicación entre nodos de una misma red
* Direcciones unique-local:
* Son análogas a direcciones privadas de IPv4.
* No son ruteables en Internet.
* Prefijo: *fc00::/8*
* Uso en redes privadas.
* Direcciones global:
* Análogas a direcciones públicas de IPv4
* Son ruteables
* Prefijo: 2000::/3
* Uso: para comunicación entre hosts de redes distintas a través de internet. Uso para redes públicas.

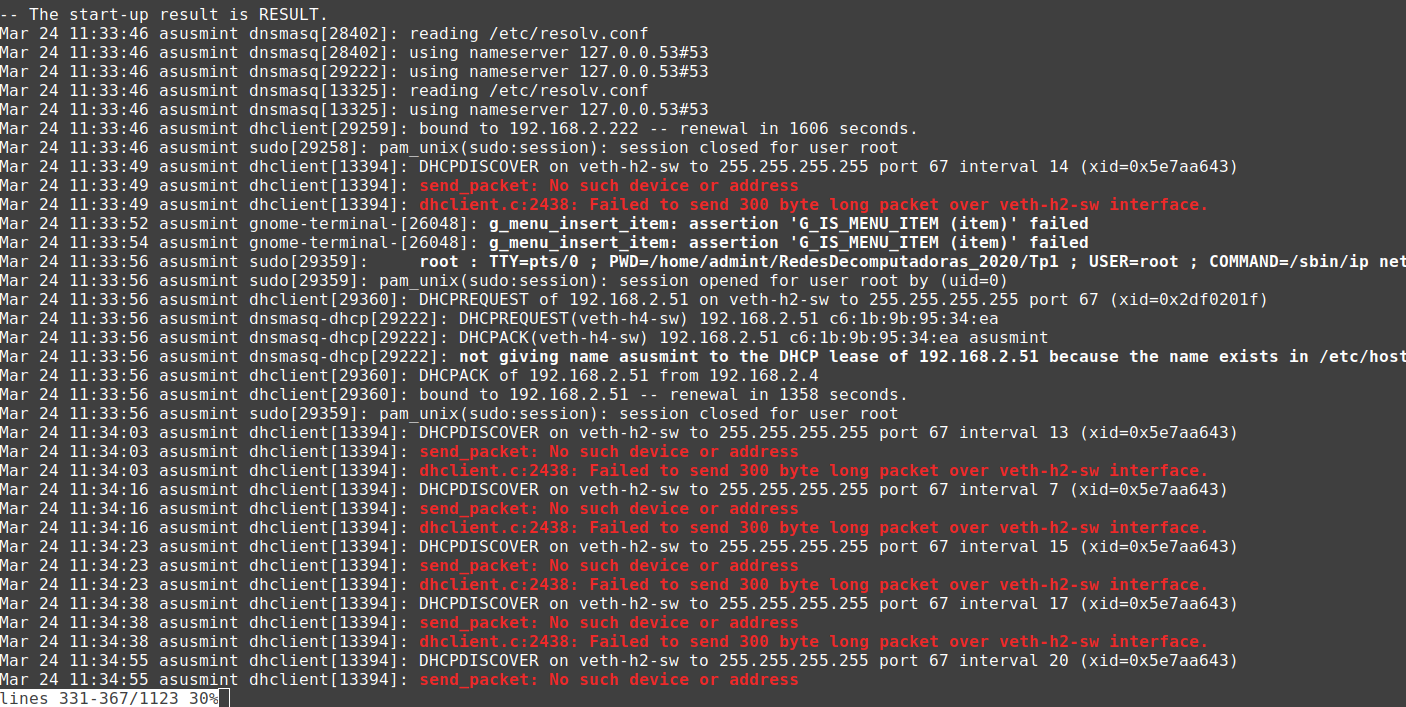
Autoconfiguración de direcciones IPv4 en linux namespaces

1. Con linux namespaces defina la topología que se muestra en el diagrama.

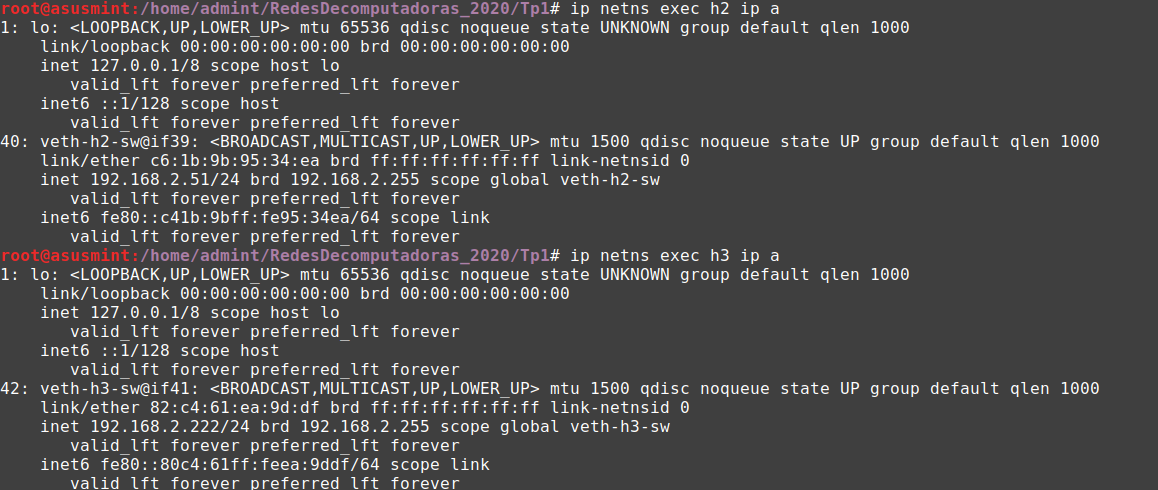




1. Configurar un dhcp server en el nuevo host, asegurarse que no entregue la IP del router que se asigno estaticamente.

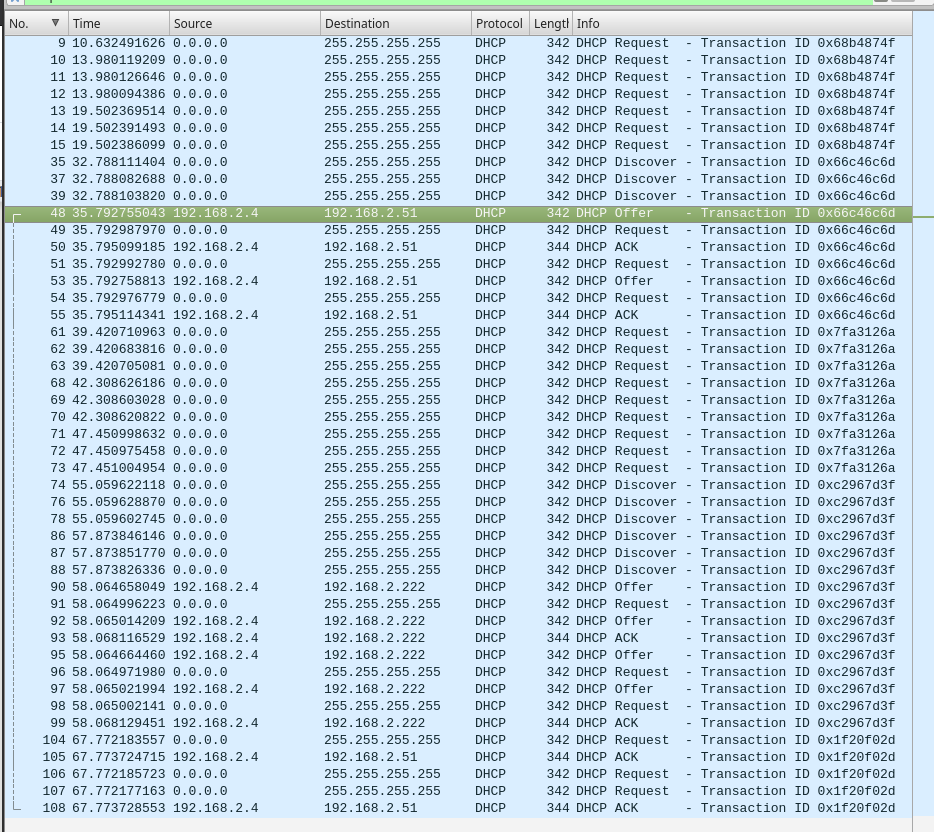


1. Usando el comando *dhclient* configurar dinámicamente la IP de h2 y h3. Qué direcciones se les asignaron?



|  |  |
| --- | --- |
| Direcciones asignadas mediante DHCP a hosts h2 y h3 | |
| Host | Dirección IPv4 |
| h2 | 192.168.2.51/24 |
| h3 | 192.168.2.222/24 |

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



**DHCP Discover:** Es el primer paso de la comunicación cliente/servidor DHCP. El cliente DHCP envía un mensaje mediante broadcast con el objetivo de encontrar un servidor DHCP en la red y conocer los parámetros de red que el servidor puede ofrecerle.

**DHCP Offer:** el servidor DHCP responde ante el mensaje Discover con éste mensaje que ofrece al cliente una dirección IPv4, un tiempo de préstamo (lease time) y otros parámetros de red.

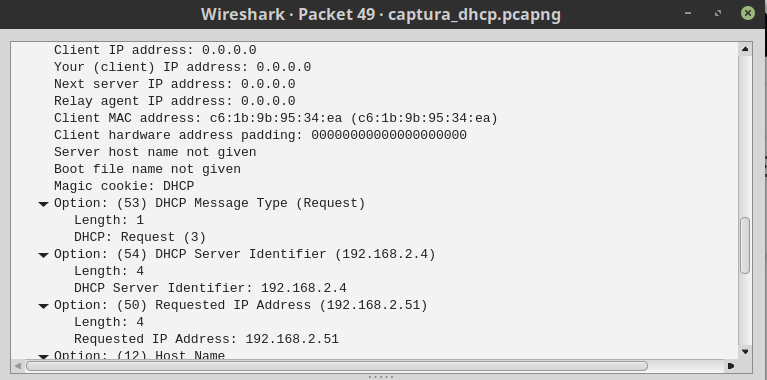
**DHCP Request:** El cliente envía este mensaje mediante broadcast como respuesta a un mensaje Offer. Indica cuál es el servidor que el cliente elige para interactuar. Todos los servidores que enviaron un DHCPOFFER reciben un DHCPREQUEST. Los servidores no elegidos toman el mensaje como aviso de rechazo.

**DHCP ACK:** El servidor elegido por el cliente recibe un DHCPREQUEST y envía este ACK como respuesta. DHCPACK contiene campos que indican la dirección IP prestada al cliente, tiempo de préstamo y parámetros de red que se configuran para el cliente.

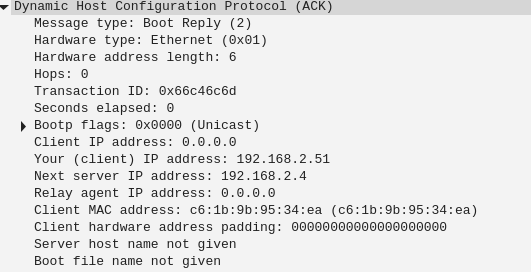
¿Cómo funciona DHCP? Explicado mediante captura en Wireshark.

Interacción host 2 con servidor DHCP en host 4: Trasacción ID 0x66x46c6d

El paquete 35 indica el inicio de la interacción. Host h2 envía un DHCPDiscover mediante broadcast (255.255.255.255) en la red buscando un servidor DHCP. Cómo el host h4 está configurado como servidor DHCP y está activo, responde a dicho mensaje con un DHCPOffer informando que tiene la dirección 192.168.2.51 para ofrecer. Host 2 acepta al servidor en h4 para servir la dirección IP.

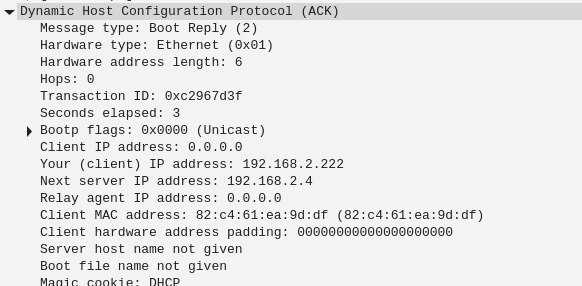


Finalmente, el servidor DHCP envía el mensaje DHCPACK.



Interacción host 3 con servidor DHCP en host 4: Trasacción ID 0xc2967d3f

Ídem a la interacción con host 2.



1. 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, no hay conectividad entre h1 y el resto de los hosts. Sucede que los hosts no tienen en su tabla de ruteo (tabla ARP) el camino para llegar a la otra red.

En IPv6 esto no sucede debido a que el uso del protocolo NDP se realiza de forma automática tanto en routers como en hosts y la tabla de vecinos (neighbour table) se completa de forma automática.

