REDES DE COMPUTADORAS

Tema 2: IPv6 and VLAN

Integrantes:

- Izquierdo, Agustina
- Navarro, Matias Alejandro

Carrera: Ing. en computación

Profesor: Matías R. Cuenca del Rey

Ayudantes alumnos: Elisabeth Leonhardt - Andrés Serjoy - Mariano Aguero - Matthew Aguerreberry - Matias Kleiner - Agustin Montero - Ramiro Morales - Sergio Sulca - Natasha Tomattis

Fecha: 4/04/2019

Izquierdo, Agustina
Navarro, Matías

Práctico 1: Tráfico en capa de enlace relacionado con IPv4 e IPv6

Ejercicio 1: Tráfico IPv4 e IPv6 con CORE

Consignas: Configuración de red IPv4/IPv6

1.- Crear el esquema de red sobre el software de emulación CORE.

2.- Probar conectividad entre el Cliente1 y Cliente2 enviando 3 paquetes ICMPv4 usando el comando “ping” para IPv4.

3.- Probar conectividad entre el Cliente1 y Cliente2 enviando 3 paquetes ICMPv6 usando el comando “ping6” para IPv6.

4.- Iniciar tráfico ICMPv4 en el Cliente1 con destino Cliente2. Analizar tráfico con “tcpdump” sobre las dos redes, capturar screenshots y responder las siguientes preguntas:

4.1.- ¿Cuáles son las comunicaciones ARP que suceden?

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

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

4.4.- ¿Por qué no hay necesidad de contar con un “switch” en esta topología?

4.5.- ¿Qué datos contiene la tabla ARP del host origen (Cliente1)?

4.6.- ¿Qué datos contiene la tabla ARP del host destino (Cliente2)?

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

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

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

5.- Iniciar tráfico ICMPv6 en el Cliente1 con destino Cliente2. Analizar el tráfico con “tcpdump” sobre las dos redes, capturar screenshots y responder a las siguientes preguntas:

5.1.- ¿Cuáles son las comunicaciones NDP que suceden?

5.2.- NDP reemplaza a ARP?

5.3.- ¿Cuáles son las diferencias entre NDP y ARP?

5.4.- Describa todas las funciones de NDP

5.5.- ¿Existen direcciones de broadcast en IPv6? Cual es su diferencia con las direcciones de broadcast de IPv4?

5.6.- ¿Cuál es la diferencia entre las direcciones link-local, site-local, global? Ejemplificar.

Ejercicio 2: Ruteo estático IPv4/IPv6 con Linux

Consignas

Configuración de red IPv4/IPv6

1.- Sobre los Routers: Configurar de manera permanente las interfaces de red con direcciones IP a elección.

2.- Sobre los Routers: Configurar para que realice ip_forwarding de manera permanente.

3.- Sobre los Clientes: Utilizando la aplicación de configuración de red gráfica NetworkManager, asignar de manera permanente y las direcciones IPs correspondiente. Configurar como Default Gateway el Router que pertenezca a la misma red.

4.- Sobre los Clientes: Con la configuración hecha hasta ahora. Ejecutar los siguientes tests y responder las siguientes preguntas

> 4.1.- Ping al Default gateway. Explicar el proceso de comunicación. Para IPv4: Protocolos ARP, IPv4 e ICMP. Para IPv6: Protocolos NDP, IPv6 e ICMPv6.
>
> 4.2.- Ping a el otro Cliente. Explicar el proceso de comunicación. Para IPv4: Protocolos ARP, IPv4 e ICMP. Para IPv6: Protocolos NDP, IPv6 e ICMPv6.

5.- Restaurar Clientes y Routers a su configuración original.

6.- Examinar tráfico en la red con wireshark y filtrar mensajes NDP. ¿Cuáles son los mensajes NDP que circulan y con qué frecuencia? Identificar y explicar cada uno de los 4 tipos de mensajes explicando direcciones de origen y destino en capa 2 y 3.

Ejercicio 3: Configuración de VLANs sobre GNU/Linux

Consignas

Configuración de VLANs

1.- Sobre el Router: Configurar de manera permanente las interfaces de VLAN
2.- Sobre el Cliente: Configurar de manera permanente las interfaces de VLAN

Configuración de IPv6

3.- Sobre el Router: Configurar de manera permanente el direccionamiento en las tres interfaces VLAN

4.- Sobre el Cliente: Configurar de manera permanente el direccionamiento en las dos interfaces VLAN

Pruebas

5.- Ejecutar ICMP echo request entre todas las interfaces VLAN y lograr que todas se comuniquen entre ellas

6.- Con tcpdump recabe datos, para luego abrir con wireshark e identifique los distintos tags de VLAN que se encuentran en las tramas ethernet.

7.- Detallar todas las conexiones que suceden en capa 2 y capa 3 desde que se configura el direccionamiento en las interfaces hasta que finaliza la ejecución de un ICMP echo reply entre dos interfaces de distinta VLAN.

Ejercicio 4: Configuración de VLANs sobre CISCO IOS

Consignas

Configuración de VLANs

1.- Sobre el Router: Configurar 4 vlans distintas sobre una única interfaz. Todas las interfaces deben estar etiquetadas.

2.- Sobre el Router: Configurar una nueva vlan como nativa. Esta vlan no se usará.

3.- Sobre el Switch: Configurar una interfaz de idéntica forma que la interfaz del Router.

4.- Sobre el Switch: Configurar 4 interfaces en distintas vlans, en todas ellas evitando el etiquetado.

5.- Sobre los Clientes: Conectar a los puertos de switch sin necesidad de configurar ninguna interfaz con VLAN.

Configuración de IPv6

6.- Plantear y proponer un direccionamiento IPv6 para todas las interfaces de todos los equipos.

Pruebas

7.- Lograr conectividad entre todos los componentes. Probar que el etiquetado de VLANs y el ruteo funcionan.

Ejercicio 1: Tráfico IPv4 e IPv6 con CORE

1.- Crear el esquema de red sobre el software de emulación CORE.

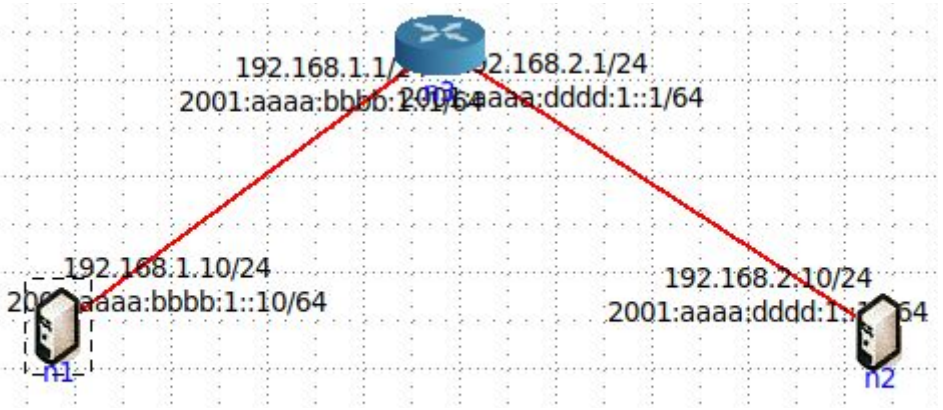


Imagen 1.1 - Esquema de red (CORE)

2.- Probar conectividad entre el Cliente1 y Cliente2 enviando 3 paquetes ICMPv4 usando el comando “ping” para IPv4.

```
root@n1:/tmp/pycore.44825/n1.conf# ping -c 3 192.168.2.10
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=0.218 ms
64 bytes from 192.168.2.10: icmp_seq=2 ttl=63 time=0.177 ms
64 bytes from 192.168.2.10: icmp_seq=3 ttl=63 time=0.208 ms

--- 192.168.2.10 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2050ms
rtt min/avg/max/mdev = 0.177/0.201/0.218/0.017 ms
root@n1:/tmp/pycore.44825/n1.conf#
```

Imagen 1.2 - Ping IPv4 desde Cliente 1 a Cliente 2

3.- Probar conectividad entre el Cliente1 y Cliente2 enviando 3 paquetes ICMPv6 usando el comando “ping6” para IPv6.

```
root@n1:/tmp/pycore.44825/n1.conf# ping6 -c 3 2001:aaaa:dddd:1::1
PING 2001:aaaa:dddd:1::1(2001:aaaa:dddd:1::1) 56 data bytes
64 bytes from 2001:aaaa:dddd:1::1: icmp_seq=1 ttl=64 time=0.177 ms
64 bytes from 2001:aaaa:dddd:1::1: icmp_seq=2 ttl=64 time=0.156 ms
64 bytes from 2001:aaaa:dddd:1::1: icmp_seq=3 ttl=64 time=0.134 ms

--- 2001:aaaa:dddd:1::1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2038ms
rtt min/avg/max/mdev = 0.134/0.155/0.177/0.022 ms
root@n1:/tmp/pycore.44825/n1.conf#
```

Imagen 1.3 - Ping IPv6 desde Cliente 1 a Cliente 2

4.- Iniciar tráfico ICMPv4 en el Cliente1 con destino Cliente2. Analizar tráfico con “tcpdump” sobre las dos redes, capturar screenshots y responder las siguientes preguntas:

Tcpdump Host1:

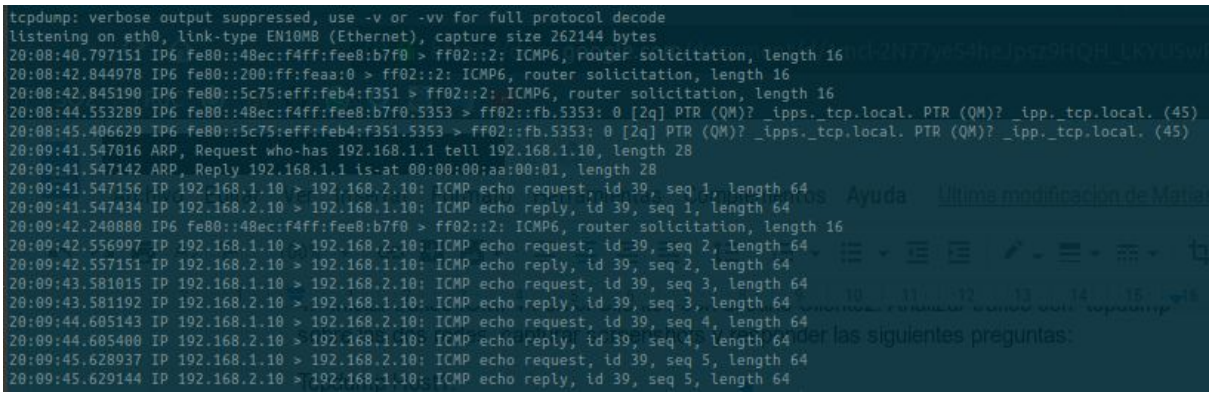


Imagen 1.4 - Host1 Tráfico ICMPv4 captura con “tcpdump”

Tcpdump Host2:

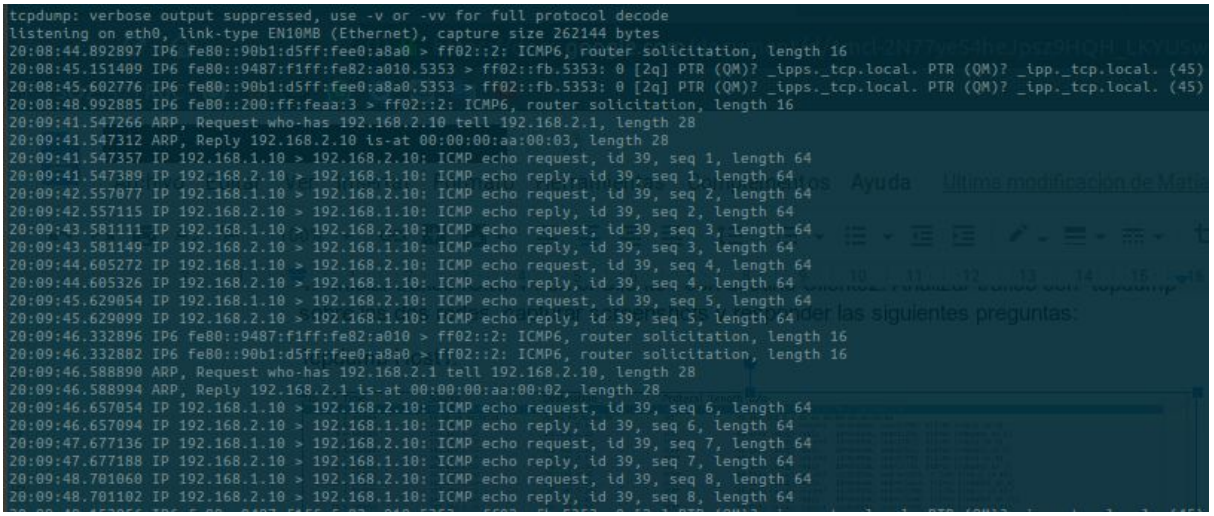


Imagen 1.5 - Host 2 Tráfico ICMPv4 captura con “tcpdump”

4.1.- ¿Cuáles son las comunicaciones ARP que suceden?

Las comunicaciones ARP que suceden son:

- ARP Request desde el Host1 a Broadcast
- ARP Reply desde el Router por la interfaz eth0 al Host1
- ARP Request desde el Router a Broadcast por su interfaz eth1
- ARP Reply desde el Host2 al Router

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

Las direcciones IPs en los datagramas son:

- 192.168.1.10 (Host 1)
- 192.168.2.10 (Host 2)

Estas direcciones IP cambian entre Source y Destination dependiendo de quien esté enviado el paquete.

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

Por que está directamente conectado a ambas redes.

Pero si esto no fuera así, lo sabría a través de su tabla de ruteo (Routing Table). Allí se enlistan todas las redes de destino que este router puede alcanzar y la mejor ruta para hacerlo; esta es calculada según un criterio de confiabilidad por el Administrador de distancia, utilizando algún protocolo.

4.4.- ¿Por qué no hay necesidad de contar con un “switch” en esta topología?

No hay necesidad de contar con un switch en esta topología dado que los mismos son utilizados para unir/conectar dispositivos dentro de una **misma** red, no proporcionan conectividad con otras redes y menos con Internet, para esto se requiere un Router.

Al tener sólo un Host por red en la topología presente, los switchs no son necesarios.

4.5.- ¿Qué datos contiene la tabla ARP del host origen (Cliente1)?

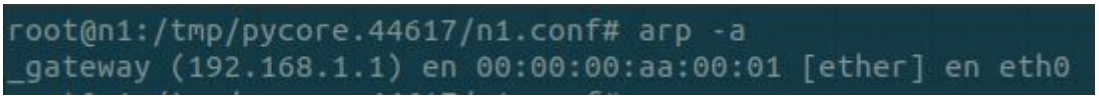


Imagen 1.6 - Tabla ARP del Host 1 (Cliente 1)

Podemos observar la dirección IP en este caso 192.168.1.1 que le corresponde a la interfaz eth0 que comunica Host1 con el Router, seguida de su respectiva dirección física (MAC) 00:00:00:aa:00:01.

4.6.- ¿Qué datos contiene la tabla ARP del host destino (Cliente2)?

Imagen 1.7 - Tabla ARP del Host 2 (Cliente 2)

Podemos observar la dirección IP en este caso 192.168.2.1 que le corresponde a la interfaz eth0 que comunica Host2 con el Router, seguida de su respectiva dirección física (MAC) 00:00:00:aa:00:02.

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

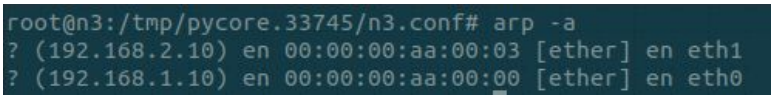


Imagen 1.8 - Tabla ARP del Router (R1)

Aquí podemos observar dos entradas en la tabla ARP. En la primera vemos la dirección IP correspondiente al Host2 seguida de su dirección física a la cual llega a través de la interfaz eth1 del Router.

Mientras que en la segunda entrada vemos la dirección IP correspondiente al Host1 seguida de su dirección física correspondiente, a la cual llega a través de la interfaz eth0 del Router.

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

Las direcciones de Broadcast en IPv4 son las llamadas direcciones de difusión, cuya utilidad es poder desde un nodo emisor enviar a una multitud de nodos receptores de manera simultánea; pero sólo se hace a las subredes concretas dentro de una misma red ya que sólo funcionan en un mismo dominio de broadcast.

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

Las direcciones Multicast en IPv4 utilizan un rango especial de direcciones denominado “rango de **clase D**”. Estas direcciones no identifican nodos sino redes o subredes.

Al momento de enviar un paquete a una dirección de multidifusión, todos los enrutadores intermedios se limitan a reenviar el paquete hasta el enrutador de dicha subred. Y este último se encarga de hacerlo llegar a todos los nodos que se encuentran en la subred.

La utilidad del mismo es, como ya mencionamos, la posibilidad de hacer llegar datagramas a un grupo específico de receptores de manera simultánea.

5.- Iniciar tráfico ICMPv6 en el Cliente1 con destino Cliente2. Analizar el tráfico con “tcpdump” sobre las dos redes, capturar screenshots y responder a las siguientes preguntas:

5.1.- ¿Cuáles son las comunicaciones NDP que suceden?

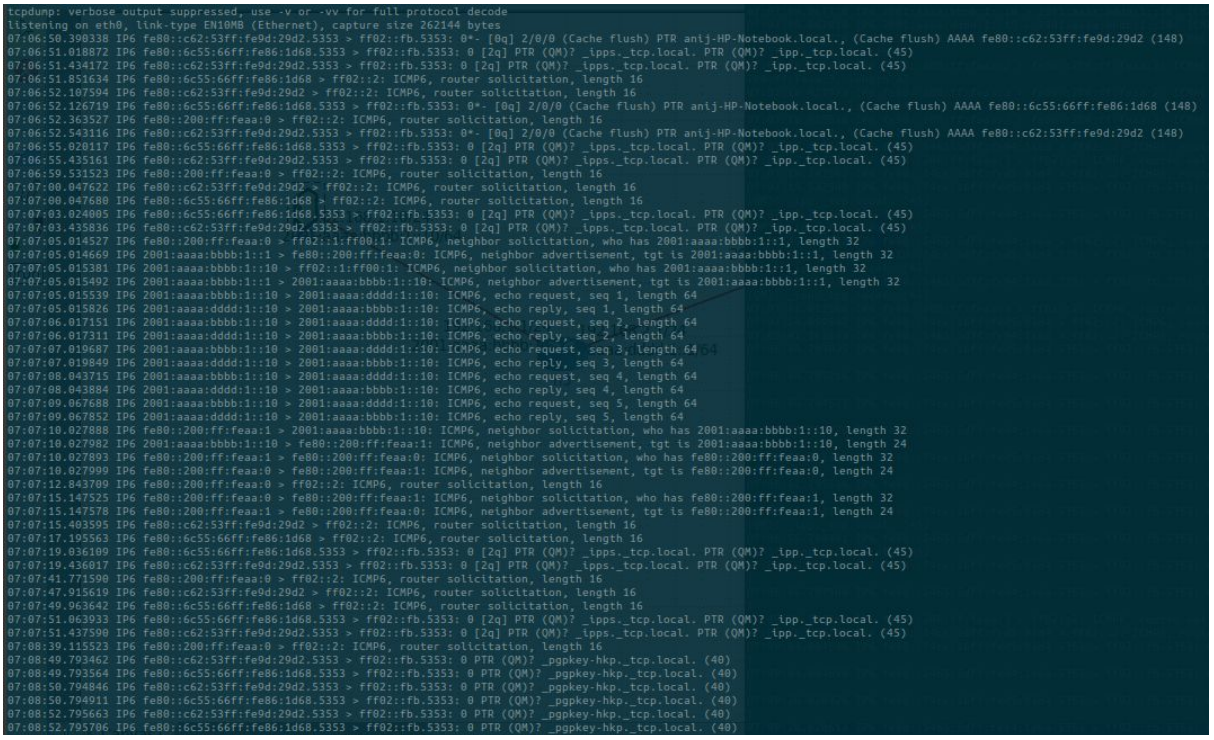


Imagen 1.9 - Análisis tráfico tcpdump desde Cliente

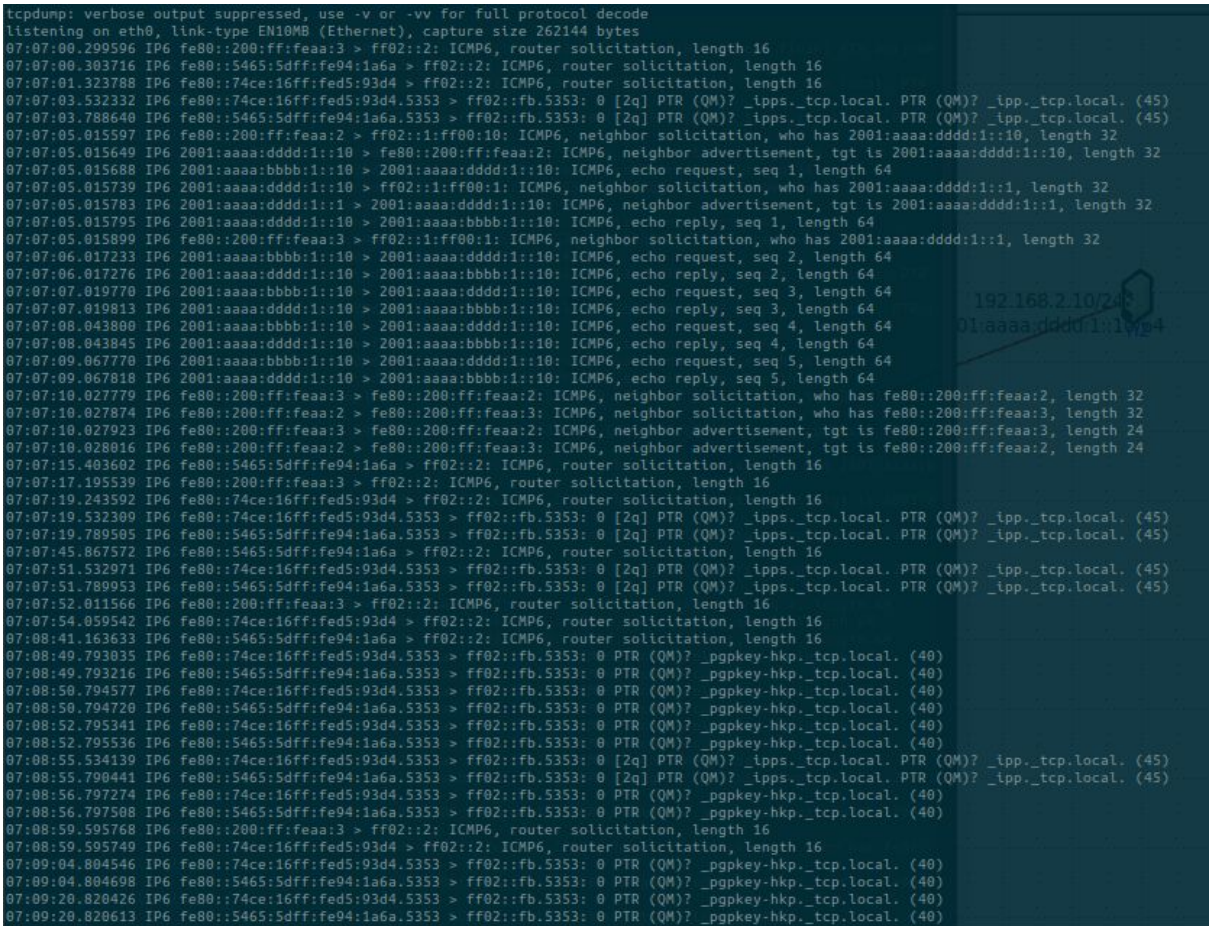


Imagen 1.10 - Análisis tráfico tcpdump desde Cliente 2

Las comunicaciones NDP que se pueden observar son:

- Neighbor Solicitation
- Neighbor Advertisement
- Router Solicitation
- Router Advertisement

5.2.- ¿NDP reemplaza a ARP?

Se puede decir que NDP reemplaza a ARP en IPv6 dado que cumple con la misma función que está a la hora de descubrir vecinos en nuestro segmento de red; pero no sólo se encarga de dicha tarea, también incorpora funcionalidades de ICMP (protocolo de control de mensajes de internet) como por ejemplo, identificar problemas de direccionamiento en nuestra red.

5.3.- ¿Cuáles son las diferencias entre NDP y ARP?

- NDP incorpora funcionalidades de ICMP que ARP no posee, como el descubrimiento de enrutador y redireccionamiento .
- NDP habilita Automatic Neighbor y Router Discovery de manera que nodo que se conecta a la red descubre automáticamente otros nodos presentes y ve sus direcciones IP (Automatic Detection of DNS servers).
- NDP no utiliza broadcast.
- NDP puede ejecutarse mandando mensajes multicast, mientras que ARP por unicast.

5.4.- Describa todas las funciones de NDP

- Incorpora funcionalidades de ICMPv6, construyendo una manera simple para que las terminales conozcan las direcciones IPv6 de los vecinos.
- Incorpora detección automática de DNS de servers, de esta forma nodo que se conecta descubre otros nodos presentes en la red y ve sus direcciones.
- Mapea direcciones IP con MAC.

5.5.- ¿Existen direcciones de broadcast en IPv6? ¿Cual es su diferencia con las direcciones de broadcast de IPv4?

No se implementan direcciones de broadcast en IPv6, en su lugar se utilizan direcciones de Multicast las cuáles son usadas por múltiples interfaces que participan de la multidifusión entre los routers de la red. De esta manera el paquete enviado por una de estas direcciones se entrega a **todas** las interfaces pertenecientes a ese grupo de dirección multicast.

Las direcciones Multicast se componen del prefijo: **ff02::1:ff00:0/104** y los últimos 24 bits corresponden a dirección IP.

5.6.- ¿Cuál es la diferencia entre las direcciones link-local, site-local, global? Ejemplificar.

Dichas direcciones son tipos de direcciones IPv6 existentes dentro de la categoría Unicast (unidifusión, emisor-receptor), las dos primeras son un equivalente a direcciones privadas en IPv4 pero con ciertas diferencias.

- Link-Local: Estas se asignan a una interfaz de manera automática a partir del momento que activamos IPv6 en un nodo. El prefijo de las mismas es **FE80::/10** y no pueden ser encaminadas a través de routers fuera del segmento de red local.
  La porción de nodo que son los últimos 64 bits se forman con formato EUI-64, donde se toma los 48 bits de dirección MAC de la tarjeta Ethernet y se le coloca 16 bits adicionales predefinidos por protocolo IPv6 (**FFFE**). Por ejemplo:

  FE80::211:21**FF:FE**6C:C86B

- Site-Local: A diferencia de las LLA es que estas pueden ser encaminadas fuera del segmento de red local, es decir enviar paquetes entre diferentes segmentos de red pero no hacia Internet.
  Aquí los primeros 10 bits se establecen con valor hexadecimal **FEC0::/10**, los últimos 64 bits se componen de la misma forma que las Link-Local. Por ejemplo:

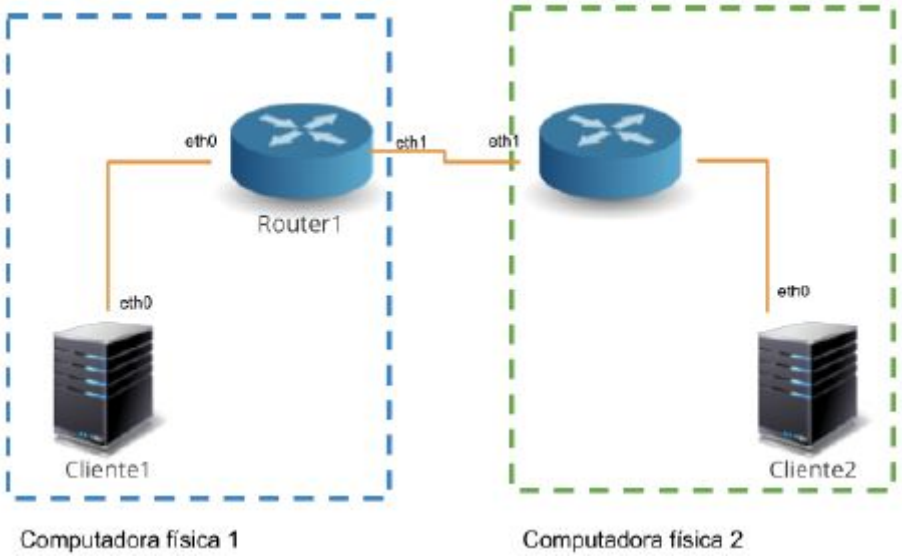
  FEC0::CE00:3B**FF:FE**85:0

  Ya son obsoletas.

- Global: Estas son un equivalente de direcciones IP públicas en IPv4. Estás sí pueden ser encaminadas a través de internet. Sus primero 3 bits se componen por 001 por lo que el prefijo de estas direcciones IP en hexadecimal será **2000::/3**. Actualmente el bloque de direcciones 2000::/3 está reservado por la IANA para una futura asignación.
  https://sites.google.com/site/tknikaipv6/2-direccionamiento/2-2-direccionamiento/2-2-3-direcciones-unicast-globales

Ejercicio 2: Ruteo estático IPv4/IPv6 con Linux

Configuración de red IPv4/IPv6



Computadora	Interfaz de red	Dirección IP
Cliente1	eth0	IPv4: 192.168.1.10
		IPv6: 2001:aaaa:aaaa:1::10
Cliente2	eth0	IPv4: 192.168.2.10
		IPv6: 2001:bbbb:bbbb:1::10
Router1	eth0	IPv4: 192.168.1.1
		IPv6: 2001:aaaa:aaaa:1::1
	eth1	IPv4: 192.168.3.1
		IPv6: 2001:aaaa:bbbb:1::1
Router2	eth0	IPv4: 192.168.3.2
		IPv6: 2001:aaaa:bbbb:1::2
	eth1	IPv4: 192.168.2.1
		IPv6: 2001:bbbb:bbbb:1::1

1.- Sobre los Routers: Configurar de manera permanente las interfaces de red con direcciones IP a elección.

Para esto se tuvo que editar el archivo “/etc/netplan/50-cloud-init.yam1” de cada Ubuntu-Server.

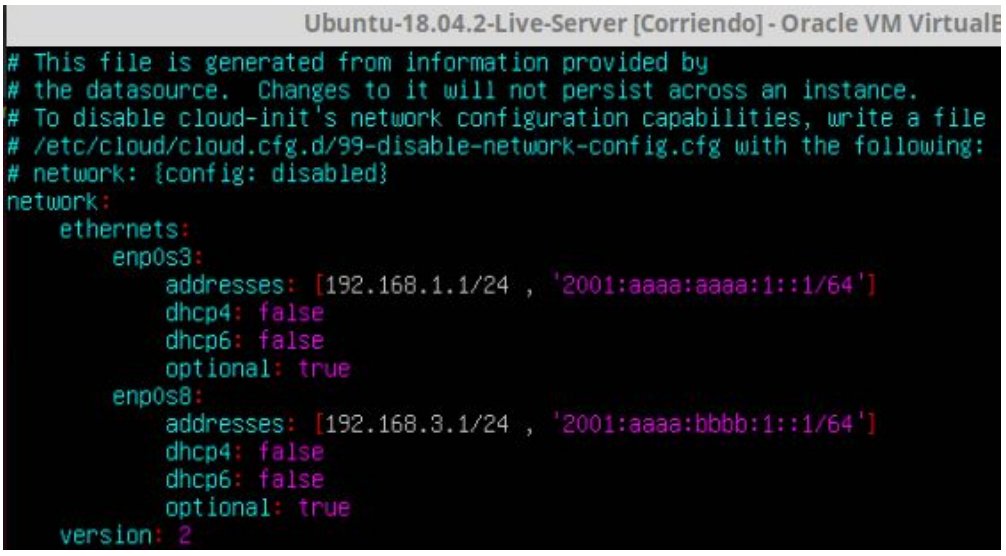


Imagen 2.1 - Configuración de las Interfaces del Router (R1)

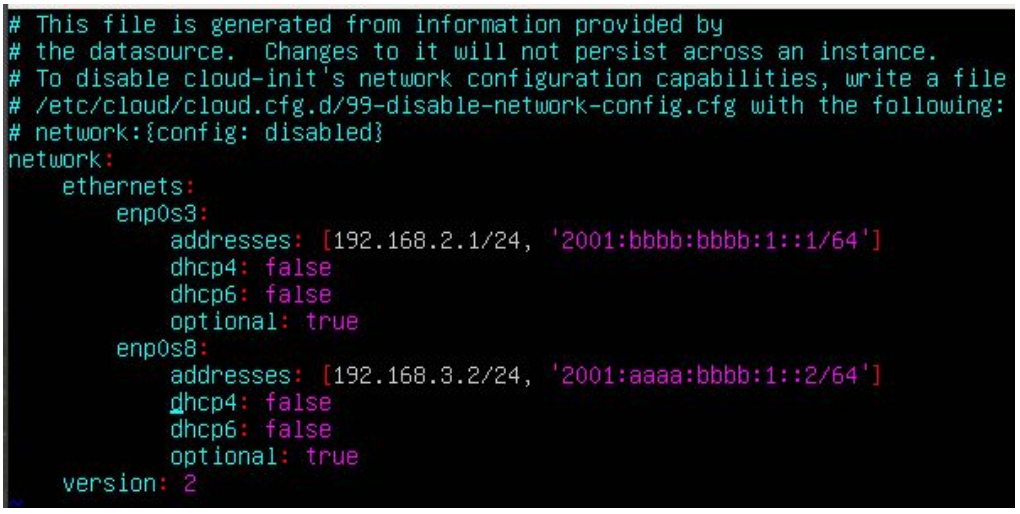


Imagen 2.2 - Configuración de las Interfaces del Router (R2)

2.- Sobre los Routers: Configurar para que realice ip_forwarding de manera permanente.

Se editó archivo “/etc/sysctl.conf” de ambos routers en sus respectivos Ubuntu-Server, descomentar las siguientes líneas:

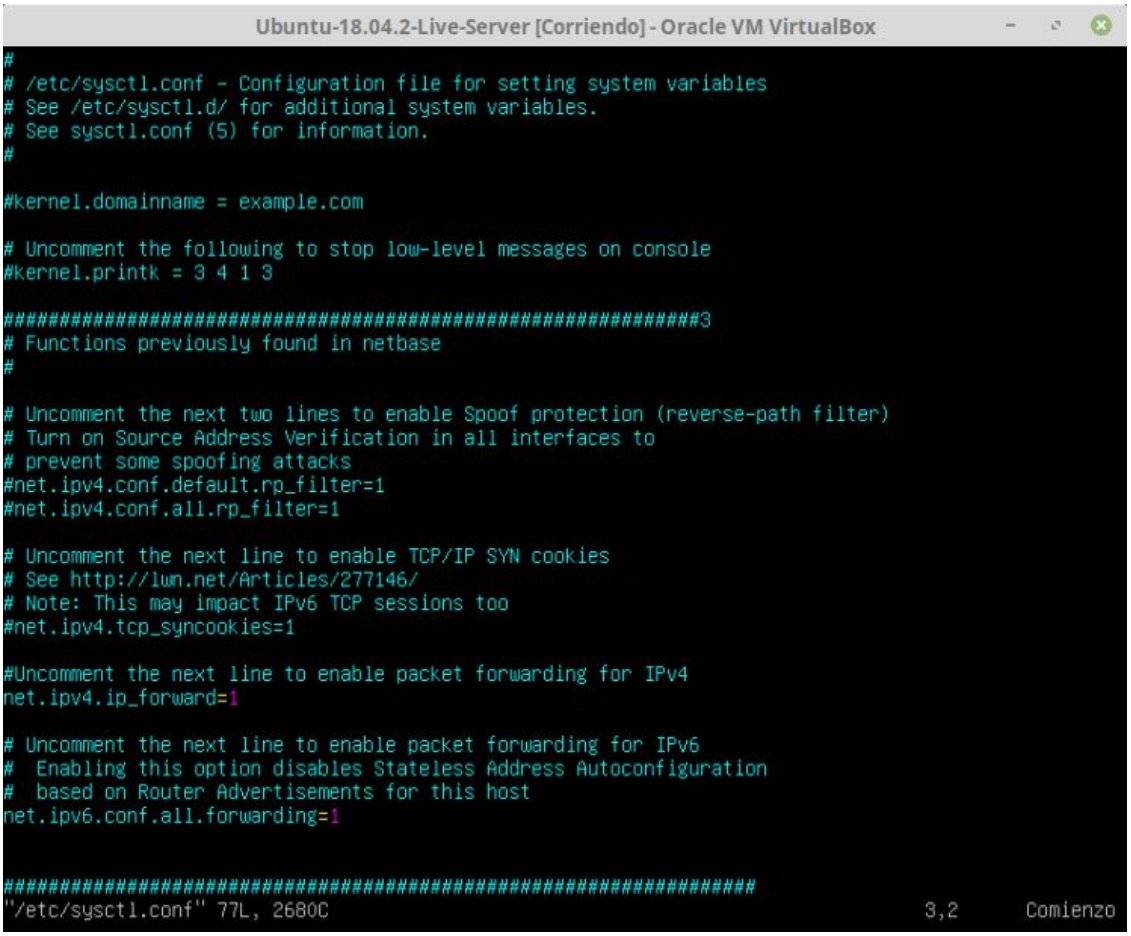


Imagen 2.3 - Forwarding Router (R1)

3.- Sobre los Clientes: Utilizando la aplicación de configuración de red gráfica NetworkManager, asignar de manera permanente y las direcciones IPs correspondiente. Configurar como Default Gateway el Router que pertenezca a la misma red.

Imagen 2.4 - IPv4 Host 1

Imagen 2.5 - IPv6 Host 1

Imagen 2.6 - IPv4 Host 2

Imagen 2.7 - IPv6 Host 2

4.- Sobre los Clientes: Con la configuración hecha hasta ahora. Ejecutar los siguientes tests y responder las siguientes preguntas.

4.1.- Ping al Default gateway. Explicar el proceso de comunicación. Para IPv4: Protocolos ARP, IPv4 e ICMP. Para IPv6: Protocolos NDP, IPv6 e ICMPv6.

```
matiasnavarro@matiasnavarro-VirtualBox:~$ ping -c 4 192.168.2.10
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=2.05 ms
64 bytes from 192.168.2.10: icmp_seq=2 ttl=63 time=2.12 ms
64 bytes from 192.168.2.10: icmp_seq=3 ttl=63 time=2.33 ms
64 bytes from 192.168.2.10: icmp_seq=4 ttl=63 time=2.15 ms

--- 192.168.2.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 2.059/2.168/2.338/0.113 ms
matiasnavarro@matiasnavarro-VirtualBox:~$ ping -6 -c 4 2001:bbbb:bbbb:1::10
PING 2001:bbbb:bbbb:1::10(2001:bbbb:bbbb:1::10) 56 data bytes
64 bytes from 2001:bbbb:bbbb:1::10: icmp_seq=1 ttl=62 time=3.12 ms
64 bytes from 2001:bbbb:bbbb:1::10: icmp_seq=2 ttl=62 time=3.77 ms
64 bytes from 2001:bbbb:bbbb:1::10: icmp_seq=3 ttl=62 time=2.65 ms
64 bytes from 2001:bbbb:bbbb:1::10: icmp_seq=4 ttl=62 time=2.76 ms

--- 2001:bbbb:bbbb:1::10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
```

Imagen 2.8 - Ping IPv4 e IPv6 desde Cliente 1 a Default Gateway

4.2.- Ping a el otro Cliente. Explicar el proceso de comunicación. Para IPv4: Protocolos ARP, IPv4 e ICMP. Para IPv6: Protocolos NDP, IPv6 e ICMPv6.

```
matiasnavarro@matiasnavarro-VirtualBox:~$ ping -c 4 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=0.362 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=0.816 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=0.628 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=0.378 ms

--- 192.168.1.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3011ms
rtt min/avg/max/mdev = 0.362/0.546/0.816/0.188 ms
matiasnavarro@matiasnavarro-VirtualBox:~$ ping -6 -c 4 2001:aaaa:aaaa:1::1
PING 2001:aaaa:aaaa:1::1(2001:aaaa:aaaa:1::1) 56 data bytes
64 bytes from 2001:aaaa:aaaa:1::1: icmp_seq=1 ttl=64 time=0.381 ms
64 bytes from 2001:aaaa:aaaa:1::1: icmp_seq=2 ttl=64 time=0.643 ms
64 bytes from 2001:aaaa:aaaa:1::1: icmp_seq=3 ttl=64 time=0.630 ms
64 bytes from 2001:aaaa:aaaa:1::1: icmp_seq=4 ttl=64 time=0.939 ms

--- 2001:aaaa:aaaa:1::1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
```

Imagen 2.9 - Ping IPv4 e IPv6 desde Cliente 1 a Cliente 2

IPv4: El Host1 (H1) al tratar de hacer ping observa que la IP solicitada 192.168.2.10 no pertenece a la red, por lo que deberá mandar el ping a su default gateway Router1 (R1) pero como esté no conoce la MAC de la interfaz a la que está conectado primero realiza la consulta ARP. Una vez que el H1 tiene la MAC del R1, le manda el ping request, esté sabe que la IP de destino pertenece a una de las redes a la cual está conectado, pero desconoce la MAC por lo que hace un broadcast preguntando por ella. El R1 obtiene la respuesta y ahora que conoce la MAC del receptor, la request del ping le llega finalmente al Host2 y este responde con un Ping Reply.

IPv6: Primero el H1 debe hacer un Router Solicitation para descubrir routers en la red local utilizando como destino la dirección de multidifusión para routers (Multicast ff02::2). Ahora el R1 debe responder a esta solicitud con un mensaje de Router Advertisement, enviándolo directamente a la dirección del solicitante.

Por otro lado, el H1 usa el Neighbor Solicitation para obtener la dirección MAC de los vecinos (En este caso R1). El router ahora responde con un Neighbor Advertisement. Ahora H1 envía el Ping Request ya que sabe hacía donde enviarlo.

El Router2 (R2) ahora debe enviar este paquete al Host2 (H2), usando mensajes del tipo Neighbor Solicitation y Advertisement el R2 descubre la dirección MAC del destino y envía el Ping Request. Finalmente el H2 responde al R2 con un Ping Reply y este simplemente llega al H1 ya que ya se conocieron las direcciones MAC necesarias.

5.- Restaurar Clientes y Routers a su configuración original.

6.- Examinar tráfico en la red con wireshark y filtrar mensajes NDP. ¿Cuáles son los mensajes NDP que circulan y con qué frecuencia? Identificar y explicar cada uno de los 4 tipos de mensajes explicando direcciones de origen y destino en capa 2 y 3.

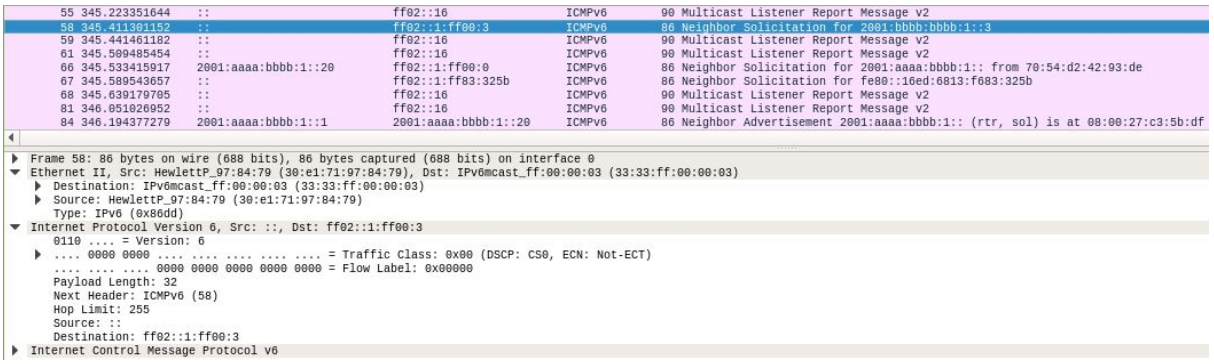


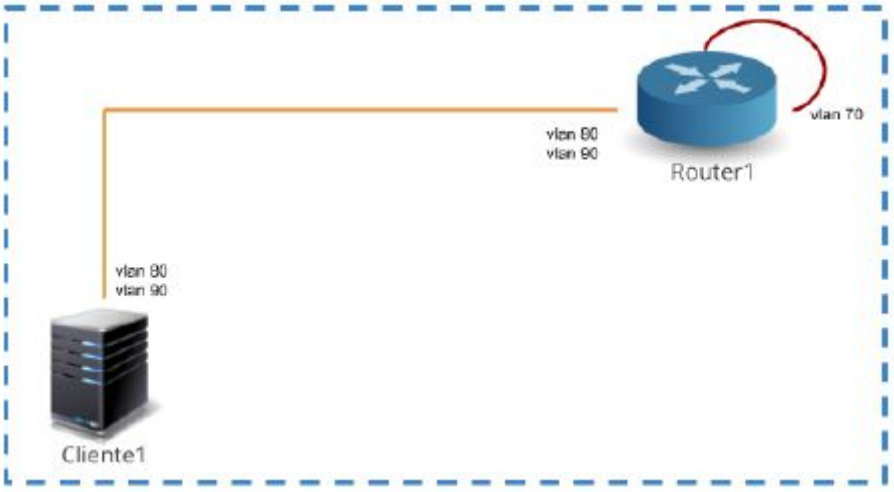
Imagen 2.10 - Captura Wireshark ICMPv6

Los 4 tipos de mensajes NDP que circulan son:

- Neighbor Solicitation :Envía solicitando información de los vecinos o verificando su "actividad"
- Neighbor Advertisement : Responde a la solicitud de vecino.
- Router Solicitation : Se envía para obtener información acerca de los routers de la red, verificando periódicamente su actividad.
- Router Advertisement : Envía una respuesta a la solicitud de routers.

Estos mensajes se detectan con una alta frecuencia, dado que en el momento que se conecta un nodo empiezan a intercambiarse estos, para conocer información sobre sus vecinos o verificar periódicamente su actividad.

Ejercicio 3: Configuración de VLANs sobre GNU/Linux



Computadora	Interfaz de red	Dirección IP
Cliente1	vlan 80	IPv6: 2001:aaaa:bbbb:1::10/64
	vlan 90	IPv6: 2001:aaaa:cccc:1::10/64
Router1	vlan 80	IPv6: 2001:aaaa:bbbb:1::aaaa/64
	vlan 90	IPv6: 2001:aaaa:cccc:1::aaaa/64
	vlan 70	IPv6: 2001:aaaa:dddd:1::aaaa/64

Imagen 3.1 - Topología de VLAN y tabla de direcciones

Consignas

Configuración de VLANs

1.- Sobre el Router: Configurar de manera permanente las interfaces de VLAN.

En Ubuntu-Server para Router, se tuvo que ejecutar comando **ifupdown** para que trabaje con el archivo de configuración “etc/network/interfaces”.

2.- Sobre el Cliente: Configurar de manera permanente las interfaces de VLAN

Configuración de IPv6

3.- Sobre el Router: Configurar de manera permanente el direccionamiento en las tres interfaces VLAN

4.- Sobre el Cliente: Configurar de manera permanente el direccionamiento en las dos interfaces VLAN

Pruebas

5.- Ejecutar ICMP echo request entre todas las interfaces VLAN y lograr que todas se comuniquen entre ellas

```
anij@anij:~$ ping -c3 2001:aaaa:bbbb:1::aaaa -I enp0s10.80
PING 2001:aaaa:bbbb:1::aaaa(2001:aaaa:bbbb:1::aaaa) from 2001:aaaa:bbbb:1::aaaa enp0s10.80: 56 data
bytes
64 bytes from 2001:aaaa:bbbb:1::aaaa: icmp_seq=1 ttl=64 time=0.095 ms
64 bytes from 2001:aaaa:bbbb:1::aaaa: icmp_seq=2 ttl=64 time=0.065 ms
64 bytes from 2001:aaaa:bbbb:1::aaaa: icmp_seq=3 ttl=64 time=0.140 ms

--- 2001:aaaa:bbbb:1::aaaa ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2039ms
rtt min/avg/max/mdev = 0.065/0.100/0.140/0.030 ms
anij@anij:~$ ping -c3 2001:aaaa:cccc:1::aaaa -I enp0s10.90
PING 2001:aaaa:cccc:1::aaaa(2001:aaaa:cccc:1::aaaa) from 2001:aaaa:cccc:1::aaaa enp0s10.90: 56 data
bytes
64 bytes from 2001:aaaa:cccc:1::aaaa: icmp_seq=1 ttl=64 time=0.030 ms
64 bytes from 2001:aaaa:cccc:1::aaaa: icmp_seq=2 ttl=64 time=0.144 ms
64 bytes from 2001:aaaa:cccc:1::aaaa: icmp_seq=3 ttl=64 time=0.141 ms

--- 2001:aaaa:cccc:1::aaaa ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2040ms
rtt min/avg/max/mdev = 0.030/0.105/0.144/0.053 ms
anij@anij:~$ ping -c3 2001:aaaa:dddd:1::aaaa -I enp0s10.70
PING 2001:aaaa:dddd:1::aaaa(2001:aaaa:dddd:1::aaaa) from 2001:aaaa:dddd:1::aaaa enp0s10.70: 56 data
bytes
64 bytes from 2001:aaaa:dddd:1::aaaa: icmp_seq=1 ttl=64 time=0.110 ms
64 bytes from 2001:aaaa:dddd:1::aaaa: icmp_seq=2 ttl=64 time=0.137 ms
64 bytes from 2001:aaaa:dddd:1::aaaa: icmp_seq=3 ttl=64 time=0.138 ms

--- 2001:aaaa:dddd:1::aaaa ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2029ms
rtt min/avg/max/mdev = 0.110/0.128/0.138/0.015 ms
anij@anij:~$ ping -c3 2001:aaaa:dddd:1::aaaa -I enp0s10.80
connect: Network is unreachable
anij@anij:~$ ping -c3 2001:aaaa:dddd:1::aaaa -I enp0s10.90
connect: Network is unreachable
anij@anij:~$ ping -c3 2001:aaaa:cccc:1::aaaa -I enp0s10.70
connect: Network is unreachable
anij@anij:~$ _
```

Imagen 3.2 - ICMP entre todas las interfaces VLAN desde Router

```
anij@anij-VirtualBox:~$ ping -c3 2001:aaaa:bbbb:1::10 -I enp0s3.80
PING 2001:aaaa:bbbb:1::10(2001:aaaa:bbbb:1::10) from 2001:aaaa:bbbb:1::10 enp0s3.80: 56 data bytes
64 bytes from 2001:aaaa:bbbb:1::10: icmp_seq=1 ttl=64 time=0.079 ms
64 bytes from 2001:aaaa:bbbb:1::10: icmp_seq=2 ttl=64 time=0.139 ms
64 bytes from 2001:aaaa:bbbb:1::10: icmp_seq=3 ttl=64 time=0.144 ms

--- 2001:aaaa:bbbb:1::10 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2019ms
rtt min/avg/max/mdev = 0.079/0.120/0.144/0.032 ms
anij@anij-VirtualBox:~$ ping -c3 2001:aaaa:cccc:1::10 -I enp0s3.90
PING 2001:aaaa:cccc:1::10(2001:aaaa:cccc:1::10) from 2001:aaaa:cccc:1::10 enp0s3.90: 56 data bytes
64 bytes from 2001:aaaa:cccc:1::10: icmp_seq=1 ttl=64 time=0.109 ms
64 bytes from 2001:aaaa:cccc:1::10: icmp_seq=2 ttl=64 time=0.150 ms
64 bytes from 2001:aaaa:cccc:1::10: icmp_seq=3 ttl=64 time=0.147 ms

--- 2001:aaaa:cccc:1::10 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2028ms
rtt min/avg/max/mdev = 0.109/0.135/0.150/0.020 ms
anij@anij-VirtualBox:~$ ping -c3 2001:aaaa:cccc:1::10 -I enp0s3.80
connect: La red es inaccesible
anij@anij-VirtualBox:~$ ping -c3 2001:aaaa:bbbb:1::10 -I enp0s3.90
connect: La red es inaccesible
```

Imagen 3. 3 - ICMP entre todas las interfaces VLAN desde Host

6.- Con tcpdump recabe datos, para luego abrir con wireshark e identifique los distintos tags de VLAN que se encuentran en las tramas ethernet.

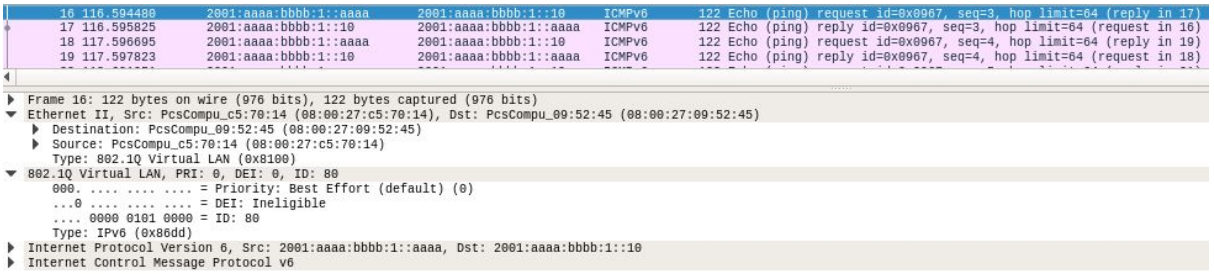


Imagen 3. 4 - ICMP entre todas las interfaces VLAN desde Host

7.- Detallar todas las conexiones que suceden en capa 2 y capa 3 desde que se configura el direccionamiento en las interfaces hasta que finaliza la ejecución de un ICMP echo reply entre dos interfaces de distinta VLAN.

Una vez que están configuradas las interfaces/subinterfaces los nodos empiezan a enviar mensajes NDP (NS,RS,NA,RA) de manera que puedan conocer todas las direcciones físicas (MAC) y las direcciones IPv6 de cada vecino o router correspondiente.

Luego, cuando se quiere realizar un ping desde uno de los host (Alpine 1) a otro (Alpine 2) el mensaje ICMPv6 Request viaja por el puerto access hacia el switch donde él mismo le coloca la etiqueta (tag) de la VLAN correspondiente y envía el paquete router.
Cuando el router recibe este paquete y ve que su etiqueta no coincide con el destino, cambia la etiqueta por la etiqueta correcta (VLAN destino) y se lo devuelvo al switch quién es el encargado de leer la etiqueta y distribuir el paquete al host correspondiente a la VLAN de la etiqueta. Y luego, se produce el reply de la misma forma, pero utiliza de manera inversa el ping request.

Hay que tener en cuenta que para que un paquete llegue de un host de una VLAN a otro de distinta VLAN, el paquete si o si necesita pasar por el router.

Ejercicio 4: Configuración de VLANs sobre CISCO IOS

Consignas

Configuración de VLANs

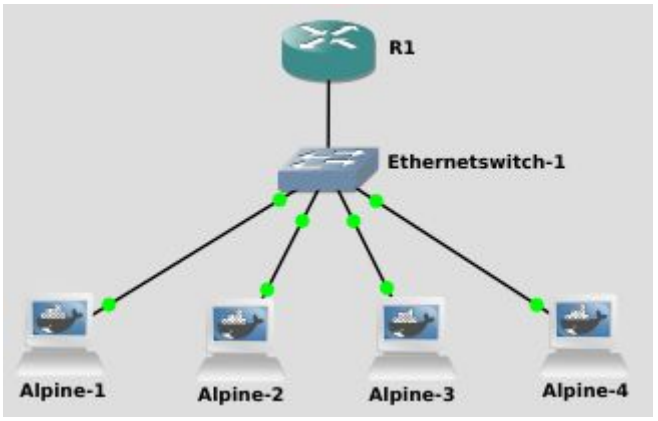


Imagen 4. 1 - Topología implementada en gns3

1.- Sobre el Router: Configurar 4 vlans distintas sobre una única interfaz. Todas las interfaces deben estar etiquetadas.

2.- Sobre el Router: Configurar una nueva vlan como nativa. Esta vlan no se usará.

```
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.1
 encapsulation dot1Q 1 native
 ipv6 address 2001:FFFF:FFFF:1::FFFF/64
!
interface FastEthernet0/0.10
 encapsulation dot1Q 10
 ipv6 address 2001:AAAA:AAAA:1::AAAA/64
!
interface FastEthernet0/0.20
 encapsulation dot1Q 20
 ipv6 address 2001:AAAA:BBBB:1::AAAA/64
!
interface FastEthernet0/0.30
 encapsulation dot1Q 30
 ipv6 address 2001:AAAA:CCCC:1::AAAA/64
!
interface FastEthernet0/0.40
 encapsulation dot1Q 40
 ipv6 address 2001:AAAA:DDDD:1::AAAA/64
!
```

Imagen 4. 2 - Configuración del Router

3.- Sobre el Switch: Configurar una interfaz de idéntica forma que la interfaz del Router

4.- Sobre el Switch: Configurar 4 interfaces en distintas vlans, en todas ellas evitando el etiquetado.

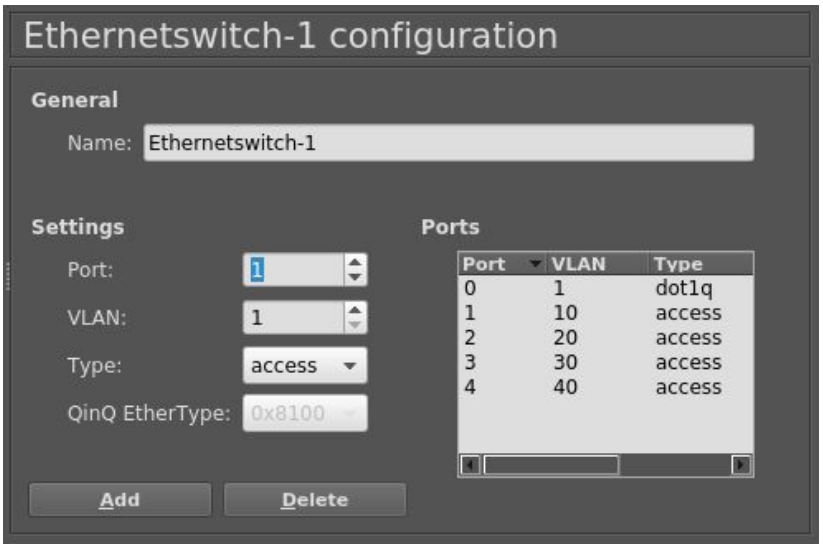


Imagen 4. 3 - Configuración del Switch en gns3

5.- Sobre los Clientes: Conectar a los puertos de switch sin necesidad de configurar ninguna interfaz con VLAN.

Configuración de IPv6

6.- Plantear y proponer un direccionamiento IPv6 para todas las interfaces de todos los equipos.

Dispositivo	Interfaz de red	Dirección IPv6
(R1) VLAN Nativa	eth 0/0.1	2001:ffff:ffff:1::ffff
(R1) VLAN 10	eth 0/0.10	2001:aaaa:aaaa:1::aaaa
(R1) VLAN 20	eth 0/0.20	2001:aaaa:bbbb:1::aaaa
(R1) VLAN 30	eth 0/0.30	2001:aaaa:cccc:1::aaaa
(R1) VLAN 40	eth 0/0.40	2001:aaaa:dddd:1::aaaa
Alpine-1	eth 0/0	2001:aaaa:aaaa:1::10
Alpine-2	eth 0/0	2001:aaaa:bbbb:1::10
Alpine-3	eth 0/0	2001:aaaa:cccc:1::10
Alpine-4	eth 0/0	2001:aaaa:dddd:1::10

Pruebas

7.- Lograr conectividad entre todos los componentes. Probar que el etiquetado de VLANs y el ruteo funcionan.

```
/ # ping -c 3 2001:aaaa:aaaa:1::aaaa
PING 2001:aaaa:aaaa:1::aaaa (2001:aaaa:aaaa:1::aaaa): 56 data bytes
64 bytes from 2001:aaaa:aaaa:1::aaaa: seq=0 ttl=64 time=10.377 ms
64 bytes from 2001:aaaa:aaaa:1::aaaa: seq=1 ttl=64 time=8.546 ms
64 bytes from 2001:aaaa:aaaa:1::aaaa: seq=2 ttl=64 time=4.962 ms

--- 2001:aaaa:aaaa:1::aaaa ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 4.962/7.961/10.377 ms
/ # ping -c 3 2001:aaaa:bbbb:1::10
PING 2001:aaaa:bbbb:1::10 (2001:aaaa:bbbb:1::10): 56 data bytes
64 bytes from 2001:aaaa:bbbb:1::10: seq=0 ttl=63 time=15.451 ms
64 bytes from 2001:aaaa:bbbb:1::10: seq=1 ttl=63 time=12.425 ms
64 bytes from 2001:aaaa:bbbb:1::10: seq=2 ttl=63 time=20.309 ms

--- 2001:aaaa:bbbb:1::10 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 12.425/16.061/20.309 ms
/ # ping -c 3 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: seq=0 ttl=63 time=20.513 ms
64 bytes from 2001:aaaa:cccc:1::10: seq=1 ttl=63 time=16.029 ms
64 bytes from 2001:aaaa:cccc:1::10: seq=2 ttl=63 time=12.081 ms

--- 2001:aaaa:cccc:1::10 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 12.081/16.207/20.513 ms
/ # ping -c 3 2001:aaaa:dddd:1::10
PING 2001:aaaa:dddd:1::10 (2001:aaaa:dddd:1::10): 56 data bytes
64 bytes from 2001:aaaa:dddd:1::10: seq=0 ttl=63 time=13.104 ms
64 bytes from 2001:aaaa:dddd:1::10: seq=1 ttl=63 time=11.773 ms
64 bytes from 2001:aaaa:dddd:1::10: seq=2 ttl=63 time=19.041 ms

--- 2001:aaaa:dddd:1::10 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 11.773/14.639/19.041 ms
/ # ping -c 3 2001:ffff:ffff:1::ffff
PING 2001:ffff:ffff:1::ffff (2001:ffff:ffff:1::ffff): 56 data bytes
64 bytes from 2001:ffff:ffff:1::ffff: seq=0 ttl=64 time=4.555 ms
64 bytes from 2001:ffff:ffff:1::ffff: seq=1 ttl=64 time=2.694 ms
64 bytes from 2001:ffff:ffff:1::ffff: seq=2 ttl=64 time=1.311 ms

--- 2001:ffff:ffff:1::ffff ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 1.311/2.853/4.555 ms
```

Imagen 4.4 - Ping desde Host 1 hacia las demás VLANs

Router-Switch

```
    36 71.360732    2001:aaaa:aaaa:1::10    2001:aaaa:dddd:1::10    ICMPv6    122 Echo (ping) request id=0x3800, seq=3, hop limit=63 (reply in 37)
    37 71.360955    2001:aaaa:dddd:1::10    2001:aaaa:aaaa:1::10    ICMPv6    122 Echo (ping) reply id=0x3800, seq=3, hop limit=64 (request in 36)
    38 71.371102    2001:aaaa:dddd:1::10    2001:aaaa:aaaa:1::10    ICMPv6    122 Echo (ping) reply id=0x3800, seq=3, hop limit=63
    39 71.542505    fe80::c601:14ff:fee7:0  fe80::500d:20ff:feaa…   ICMPv6     90 Neighbor Solicitation for fe80::500d:20ff:feaa:b476 from c4:01:14:e7:00:00

▸ Frame 36: 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface 0
▸ Ethernet II, Src: c4:01:14:e7:00:00 (c4:01:14:e7:00:00), Dst: 9e:6c:6f:a0:4f:39 (9e:6c:6f:a0:4f:39)
▾ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 40
    000. .... .... .... = Priority: Best Effort (default) (0)
    ...0 .... .... .... = DEI: Ineligible
    .... 0000 0010 1000 = ID: 40
    Type: IPv6 (0x86dd)
▸ Internet Protocol Version 6, Src: 2001:aaaa:aaaa:1::10, Dst: 2001:aaaa:dddd:1::10
▸ Internet Control Message Protocol v6
```

Imagen 4.4 - Captura Wireshark Router1

Switch-Host

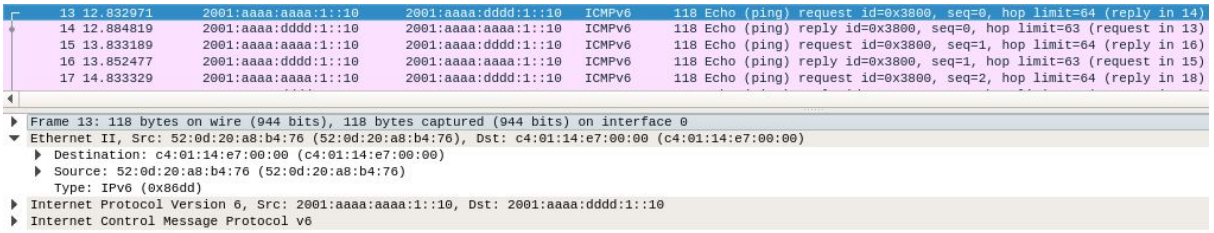


Imagen 4.4 - Captura Wireshark Host1 (VLAN 10)

Como se puede observar en las imágenes anteriores(*Imagen 4.3 y 4.4*) el etiquetado de la VLAN se da en los puertos troncales (en este caso, router-switch) y no es así en los de acceso (switch-host); dado que en los puertos troncales van a circular paquetes pertenecientes a diferentes VLANs y estas etiquetas permiten diferenciarlas.

Anexo: Comandos utilizados

- Ejercicio 2:
  - *ifconfig*
  - *sudo ifconfig “interfaz de red” up/down*
  - *ip a*
  - *ip route*
  - *ip -6 route*
  - *ping “IP Destino”* (con el atributo -c”N” antes de la IP le indico cuántos paquetes mandar)
  - *vim or nano “path archivo”*
  - *sudo netplan apply*
  - *sudo tcpdump -i “interfaz de red”*
  - *sudo ip (-6) route add “redDestino” via “ProximoSalto” dev “Interfaz de Red”*

- Ejercicio 3:
  - *sudo apt-get install vlan*
  - *sudo apt-get ifupdown*
  - *sudo modprobe 8021q*
  - *sudo vconfig add eth1 “Nº Interfaz”*
  - *sudo ip addr add IP/Mask dev eth1.”Nº Interfaz”*
  - *sudo ip link set up eth1.10*
  - *sudo su -c 'echo "8021q" >> /etc/modules'*

- Ejercicio 4:
  - Router:
    - *configure terminal*
    - *interface fastEthernet 0/0*
    - *no shutdown*
    - *encapsulation dot1q “Nº VLAN”*
    - *ip address “IP” “Mask”*
    - *copy running-config startup-config*
    - *show ipv6 route*
    - *show ipv6 interface*
    - *show running-config*