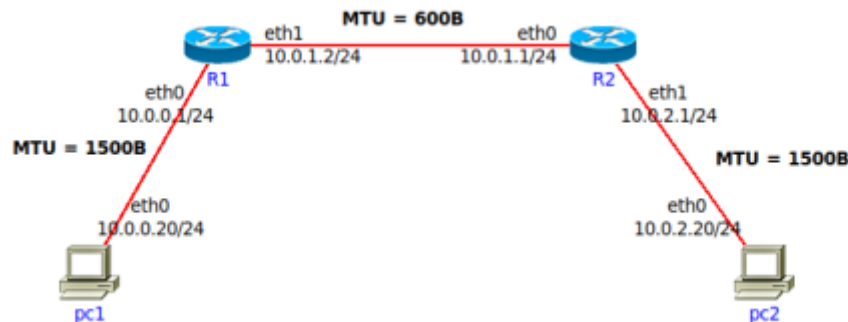


Práctica 8

Fragmentación

2. Se tiene la siguiente red con los MTUs indicados en la misma. Si desde pc1 se envía un paquete IP a pc2 con un tamaño total de 1500 bytes (cabecera IP más payload) con el campo Identification = 20543, responder:



- Indicar IPs origen y destino y campos correspondientes a la fragmentación cuando el paquete sale de pc1

IP Origen 10.0.0.20/24

IP Destino 10.0.2.20/24

Header: 20

Tamaño total: 1500

Identificación: 20543

DF Flag: 0

MF Flag: 0

Fragment Offset: 0

- ¿Qué sucede cuando el paquete debe ser reenviado por el router R1?

Como el enlace entre el router R1 y el R2 tiene un MTU de 600B, el paquete se debe fragmentar.

- Indicar cómo quedarían los paquetes fragmentados para ser enviados por el enlace entre R1 y R2.

Para fragmentar hay que tomar el valor máximo del MTU y restarle el valor del header (20), luego hay que encontrar el múltiplo de 8 más cercano a ese número.

1

Header: 20

Tamaño total: 596

Identificación 20543

DF Flag: 0

MF Flag: 1
Fragment Offset: 0

2
Header: 20
Tamaño total: 596
Identificación 20543
DF Flag: 0
MF Flag: 1
Fragment Offset: 72

3
Header: 20
Tamaño total: 348
Identificación 20543
DF Flag: 0
MF Flag: 0
Fragment Offset: 144

Anotaciones:

- Al tamaño total le sumo el header. La suma de los totales de los fragmentos me debería dar el total del original + 20 * (cantidad de fragmentos – 1)
- El offset se calcula como la suma del tamaño de datos (SIN HEADERS) de los fragmentos anteriores dividido por 8.
- El ultimo fragmento tiene el MF Flag en 0.
- El primer fragmento tiene el offset en 0.

▪ **¿Dónde se unen nuevamente los fragmentos? ¿Qué sucede si un fragmento no llega?**

Se reúnen de nuevo en los sistemas terminales. Si se pierde un fragmento, se deben retransmitir todos los fragmentos del paquete original. Sin embargo, IP no tiene mecanismos para comprobar la llegada de los fragmentos, así que depende de las decisiones de los protocolos de las capas superiores.

▪ **Si un fragmento tiene que ser reenviado por un enlace con un MTU menor al tamaño del fragmento, ¿qué hará el router con ese fragmento?**

Lo vuelve a fragmentar.

3. ¿Qué es el ruteo? ¿Por qué es necesario?

El ruteo consiste en seleccionar la interfaz de salida y el próximo salto. Involucra a los routers y hosts. Es necesario para que un paquete vaya de un extremo a otro.

4. En las redes IP el ruteo puede configurarse en forma estática o en forma dinámica. Indique ventajas y desventajas de cada método.

- Ventajas

Estática	Dinámica
Simplicidad: El enrutamiento estático es fácil de configurar y entender, especialmente en redes pequeñas y simples.	Adaptabilidad: El enrutamiento dinámico se ajusta automáticamente a cambios en la red, como enlaces caídos o nuevas rutas disponibles, lo que mejora la resiliencia de la red.
Control total: El administrador de red tiene un control total sobre las rutas y puede diseñar la red según sus necesidades específicas.	Escalabilidad: Es más adecuado para redes grandes y complejas, ya que la configuración se propaga automáticamente a través de la red.
Menos carga en la red: El enrutamiento estático generalmente genera menos tráfico de enrutamiento en la red, ya que las rutas se configuran manualmente y no cambian automáticamente.	Eficiencia de recursos: Enrutamiento dinámico puede encontrar rutas óptimas en función de métricas como la velocidad o la carga de los enlaces, lo que mejora la eficiencia del tráfico.

- Desventajas

Estática	Dinámica
No se adapta a cambios: El enrutamiento estático no se ajusta automáticamente a cambios en la topología de la red, lo que significa que si una ruta falla o cambia, debe actualizarse manualmente.	Mayor complejidad: La configuración y el mantenimiento del enrutamiento dinámico pueden ser más complejos que el enrutamiento estático, lo que requiere un conocimiento más profundo.
No es escalable: En redes grandes y complejas, la gestión manual de rutas puede volverse abrumadora y propensa a errores.	Mayor tráfico de enrutamiento: El enrutamiento dinámico genera más tráfico de enrutamiento en la red, ya que los routers intercambian información sobre las rutas, lo que puede consumir ancho de banda.
Menos eficiente en términos de tiempo: En una red grande, configurar y mantener el enrutamiento estático puede ser más demorado que utilizar enrutamiento dinámico.	Posible inestabilidad: Si no se configura adecuadamente, el enrutamiento dinámico puede causar problemas de estabilidad en la red.

- Enrutamiento Estático:

- La tabla se configura y modifica manualmente por un administrador de red.
- No se adapta automáticamente a cambios en la red, lo que puede llevar a problemas en caso de fallos.
- Adecuado para redes con tráfico predecible y es simple de diseñar e implementar.
- No requiere protocolos de enrutamiento complejos.
- Rutas están definidas por el usuario y no cambian a menos que se modifiquen manualmente.
- No emplea algoritmos complejos para calcular rutas.
- Adecuado para redes pequeñas.

- Enrutamiento Dinámico:
- La tabla se construye automáticamente mediante protocolos de enrutamiento.
- Se adapta a cambios en la red, lo que permite recuperarse de fallos de enlaces o nodos.
- Ideal para redes grandes con una alta cantidad de hosts.
- Utiliza algoritmos complejos para calcular rutas de manera dinámica.
- Las configuraciones y la creación de la tabla son automáticas y controladas por el enrutador.
- Las rutas se actualizan según cambia la topología de la red.

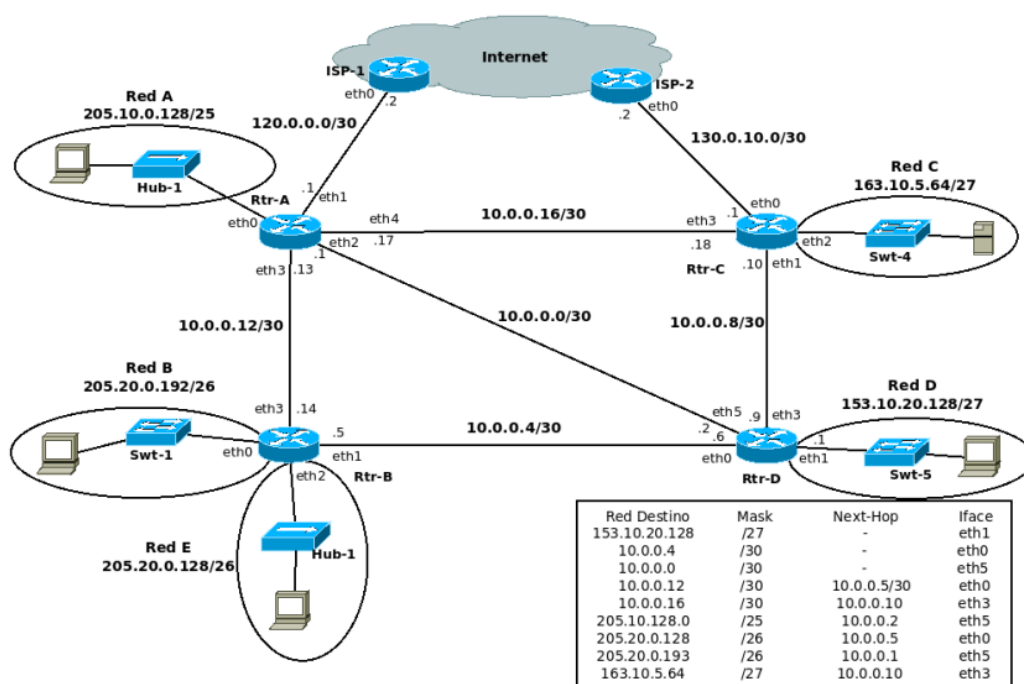
<https://es.quora.com/Cu%C3%A1ndo-se-recomendar%C3%AD-a-usar-enrutamiento-est%C3%A1tico-y-cu%C3%A1ndo-enrutamiento-din%C3%A1mico#:~:text=En%20el%20enrutamiento%20est%C3%A1tico%2C%20la,de%20los%20protocolos%20de%20enrutamiento.>

5. Una máquina conectada a una red pero no a Internet, ¿tiene tabla de ruteo?

Una máquina conectada a una red local, incluso si no está conectada a Internet, tiene una tabla de enrutamiento para gestionar la comunicación dentro de la red local.

La tabla de enrutamiento contiene información sobre las rutas disponibles en la red y cómo alcanzar otras máquinas dentro de esa red. En una red local, las rutas pueden ser bastante simples, ya que generalmente solo hay unos pocos dispositivos interconectados, como computadoras y dispositivos de red. Sin embargo, aún se necesita una tabla de enrutamiento para determinar cómo enviar datos entre estos dispositivos.

6. Observando el siguiente gráfico y la tabla de ruteo del router D, responder:



a. ¿Está correcta esa tabla de ruteo? En caso de no estarlo, indicar el o los errores encontrados. Escribir la tabla correctamente (no es necesario agregar las redes que conectan contra los ISPs)

- Next-Hop 10.0.0.5/30 → No se puede esto, no debe tener la máscara.
- Falta 10.0.0.8
- 205.10.128.0 no es una dirección de red que esta presente en el gráfico. Además a 205.10.0.128 el Next-Hop es el router 10.0.0.1
- 205.20.0.193 es una dirección de host y no de red.

Red Destino	Mask	Next-Hop	Iface
153.10.20.128	/27	-	eth1
10.0.0.4	/30	-	eth0
10.0.0.0	/30	-	eth5
10.0.0.8	/30	-	eth3
10.0.0.12	/30	10.0.0.5	eth0
10.0.0.16	/30	10.0.0.10	eth3
205.10.0.128	/25	10.0.0.1	eth5
205.20.0.192	/26	10.0.0.5	eth0
205.20.0.128	/26	10.0.0.5	eth0
163.10.5.64	/27	10.0.0.10	eth3

b. Con la tabla de ruteo del punto anterior, Red D, ¿tiene salida a Internet? ¿Por qué? ¿Cómo lo solucionaría? Suponga que los demás routers están correctamente configurados, con salida a Internet y que Rtr-D debe salir a Internet por Rtr-C.

No, no tiene salida a Internet, porque la tabla de ruteo no tiene ninguna entrada que lleve a algún ISP. Para solucionarlo habría que agregar una red default que tenga como Next-Hop a Rtr-C

Red Destino	Mask	Next-Hop	Iface
0.0.0.0	/0	10.0.0.10	eth3

- c. Teniendo en cuenta lo aplicado en el punto anterior, si en Rtr-C estuviese la siguiente entrada en su tabla de ruteo qué sucedería si desde una PC en Red D se quiere acceder un servidor con IP 163.10.5.15.

Red Destino	Mask	Next-Hop	Iface
163.10.5.0	/24	10.0.0.9	eth1

Se entraría en un loop hasta que finalice el TTL del paquete IP y se descarte.

- d. ¿Es posible aplicar sumarización en esa tabla, la del router Rtr-D? ¿Por qué? ¿Qué debería suceder para poder aplicarla?

- En 10.0.0.4 y 10.0.0.8 se podría aplicar si no tuvieran distinta interfaz.
- En 205.20.0.192 y 205.20.0.128 si se puede aplicar ya que tiene el mismo salto e interfaz.

- e. La sumarización aplicada en el punto anterior, ¿se podría aplicar en Rtr-B? ¿Por qué?

No se podría aplicar ya que son redes que están directamente conectadas con interfaces distintas.

- f. Escriba la tabla de ruteo de Rtr-B teniendo en cuenta lo siguiente:

- Debe llegarse a todas las redes del gráfico
- Debe salir a Internet por Rtr-A
- Debe pasar por Rtr-D para llegar a Red D
- Sumarizar si es posible

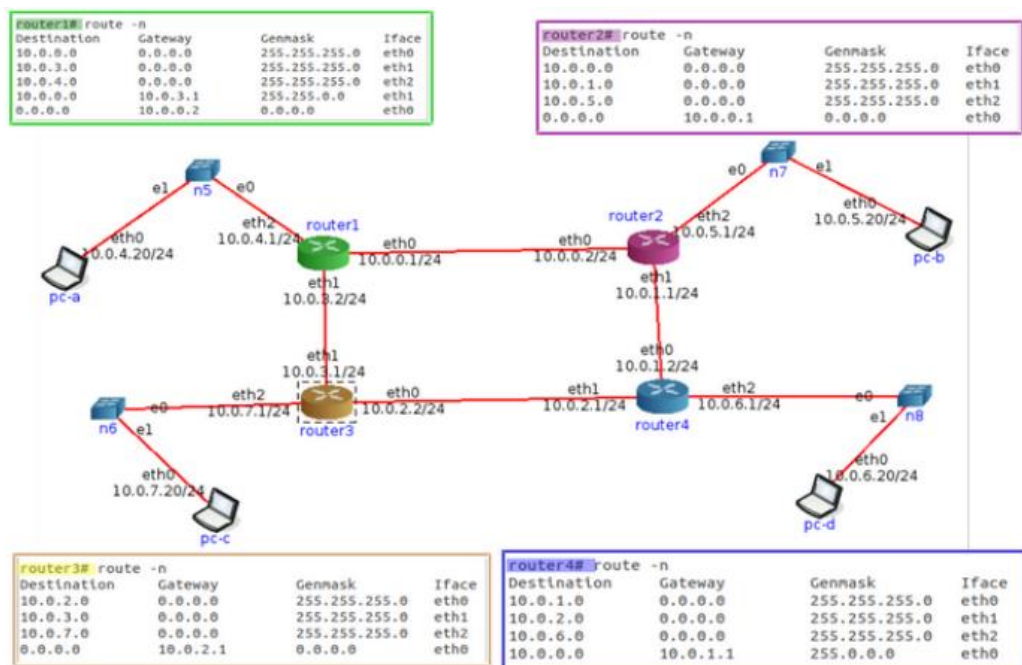
Red Destino	Mask	Next-Hop	Iface
205.20.0.192	/26	-	eth0
205.20.0.128	/26	-	eth2
10.0.0.12	/30	-	eth3
10.0.0.4	/30	-	eth1
10.0.0.8	/30	10.0.0.6	eth1
10.0.0.0	/30	10.0.0.13	eth3

10.0.0.16	/30	10.0.0.13	eth3
153.10.20.128	/27	10.0.0.6	eth1
163.10.5.64	/27	10.0.0.6	eth1
205.10.0.128	/25	10.0.0.13	eth3
120.0.0.0	/30	10.0.0.13	eth3
130.0.10.0	/30	10.0.0.13	eth3
0.0.0.0	/0	10.0.0.13	eth3

- g. Si Rtr-C pierde conectividad contra ISP-2, ¿es posible restablecer el acceso a Internet sin esperar a que vuelva la conectividad entre esos dispositivos?

Se podría reestablecer el acceso a Internet si los routers tienen en su tabla de ruteo la red ISP-1, es decir, a la red destino 120.0.0.0/30 para la cual se debe pasar por el router A.

7. Evalúe para cada caso si el mensaje llegará a destino, saltos que tomará y tipo de respuesta recibida el emisor



- Un mensaje ICMP enviado por PC-B a PC-C.
Debe enviar a 10.0.7.20/24
 - Se envía a 10.0.5.1/24 – Router2

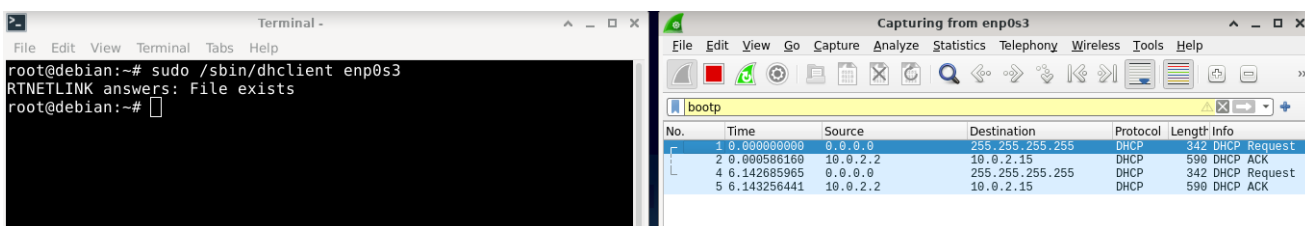
- Como no hay ninguna entrada con destino que coincida (ningún rango) lo envía al default que es el router2
- En el router2 coincide con 10.0.0.0 con la máscara 255.255.0.0 por lo que es enviado al router3.
- El mensaje llega a PC-C desde el router3 por la interfaz eth2.
- Se realizan 4 saltos y se responde ICMP tipo 0 y código 0 (eco)
- **Un mensaje ICMP enviado por PC-C a PC-B.**
Debe enviar a 10.0.5.20/24:
 - Se envía a 10.0.7.1/24 – Router3.
 - Como es default el router3 envía al router4.
 - En el router4 se fija en la entrada de 10.0.0.0 (se puede por la máscara que se tiene) y el paquete se envía al router2 por eth0.
 - El mensaje llega a PC-B desde el router2 por la interfaz eth2.
 - Se realizan 4 saltos y se responde ICMP tipo 0 y código 0 (eco)
- **Un mensaje ICMP enviado por PC-C a 8.8.8.8.**
Debe enviar a 8.8.8.8:
 - Se envía a 10.0.7.1/24 – Router3.
 - No coincide con ninguno, por default el router3 envía al router4.
 - En el router4 no se tiene por default y no coincide con ninguno por lo que se descarta el mensaje.
 - Se realizan 2 saltos y se responde ICMP tipo 3 y código 0 (red inalcanzable)
- **Un mensaje ICMP enviado por PC-B a 8.8.8.8.**
 - Se envía a 10.0.5.1/24 – Router2
 - Lo envía por el default, por lo que lo envía al router1.
 - En el router1 también entra por default por lo que es enviado al router2. Se entra en un loop hasta que termina el TTL.
 - Se realizan tantos saltos como sea el TTL y se responde ICMP tipo 11 y código 0 (TTL caducado)

DHCP y NAT

8. Con la máquina virtual con acceso a Internet realice las siguientes observaciones respecto de la autoconfiguración IP vía DHCP:

- a. **Inicie una captura de tráfico Wireshark utilizando el filtro bootp para visualizar únicamente tráfico de DHCP.**

- b. En una terminal de root, ejecute el comando `sudo /sbin/dhclient eth0` y analice el intercambio de paquetes capturado.



- c. Analice la información registrada en el archivo `/var/lib/dhcp/dhclient.leases`, ¿cuál parece su función?

```
root@debian:~# cat /var/lib/dhcp/dhclient.leases
lease {
  interface "enp0s3";
  fixed-address 10.0.2.15;
  filename "Redes y Comunicaciones v22.2.pxe";
  option subnet-mask 255.255.255.0;
  option routers 10.0.2.2;
  option dhcp-lease-time 86400;
  option dhcp-message-type 5;
  option domain-name-servers 181.30.140.195,181.30.140.134,181.30.140.134;
  option dhcp-server-identifier 10.0.2.2;
  option domain-name "fibertel.com.ar";
  renew 4 2023/11/02 02:42:35;
  rebind 4 2023/11/02 11:52:44;
  expire 4 2023/11/02 14:52:44;
}
lease {
  interface "enp0s3";
  fixed-address 10.0.2.15;
  filename "Redes y Comunicaciones v22.2.pxe";
  option subnet-mask 255.255.255.0;
  option dhcp-lease-time 86400;
  option routers 10.0.2.2;
  option dhcp-message-type 5;
  option dhcp-server-identifier 10.0.2.2;
  option domain-name-servers 181.30.140.195,181.30.140.134,181.30.140.134;
  option domain-name "fibertel.com.ar";
  renew 4 2023/11/02 00:38:27;
  rebind 4 2023/11/02 11:53:18;
  expire 4 2023/11/02 14:53:18;
}
```

Se mantiene un registro de las asignaciones de direcciones IP y otra información de configuración que se obtuvo del servidor DHCP.

- d. Ejecute el siguiente comando para eliminar información temporal asignada por el servidor DHCP.

`rm /var/lib/dhcp/dhclient.leases`

```
root@debian:~# rm /var/lib/dhcp/dhclient.leases
root@debian:~# cat /var/lib/dhcp/dhclient.leases
cat: /var/lib/dhcp/dhclient.leases: No such file or directory
```

- e. En una terminal de root, vuelva a ejecutar el comando `sudo /sbin/dhclient eth0` y analice el intercambio de paquetes capturado nuevamente ¿a qué se debió la diferencia con lo observado en el punto “b”?

901	248.659216211	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover	- Transaction ID 0x78082656
902	248.659811092	10.0.2.2	10.0.2.15	DHCP	590	DHCP Offer	- Transaction ID 0x78082656
903	252.130349905	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover	- Transaction ID 0x78082656
904	252.130957276	10.0.2.2	10.0.2.15	DHCP	590	DHCP Offer	- Transaction ID 0x78082656
905	252.131051362	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request	- Transaction ID 0x78082656
906	252.131735397	10.0.2.2	10.0.2.15	DHCP	590	DHCP ACK	- Transaction ID 0x78082656

En el punto “b” el cliente DHCP solicita una dirección IP al servidor DHCP en la red. El servidor DHCP asigna una dirección IP y otros parámetros de configuración que se registra en el archivo `/var/lib/dhclient/leases`. Cuando se elimina el archivo `dhclient.leases` y luego se ejecuta `sudo /sbin/dhclient enp0s3`, el cliente DHCP no puede encontrar un archivo `dhclient.leases` previamente existente para consultar información de arrendamientos anteriores. Esto lleva a un comportamiento ligeramente diferente:

Al eliminar `dhclient.leases`, el cliente DHCP no tiene registro de direcciones IP anteriores ni de otros parámetros de configuración. Por lo tanto, inicia una solicitud DHCP desde cero, como si fuera la primera vez que se conecta a la red. Dado que el cliente DHCP inicia una nueva solicitud, el servidor DHCP en la red asigna una dirección IP y otros parámetros de configuración nuevamente al cliente. Esto significa que habrá un nuevo intercambio de paquetes DHCP entre el cliente y el servidor.

La diferencia principal se debe a la falta de un archivo `dhclient.leases` que contenga registros previos de asignaciones de direcciones IP. Cuando el archivo se elimina, el cliente DHCP actúa como si estuviera configurándose por primera vez en la red, lo que resulta en un nuevo proceso de asignación de dirección IP por parte del servidor DHCP.

(god i love chatgpt)

- f. Tanto en “b” como en “e”, ¿qué información es brindada al host que realiza la petición DHCP, además de la dirección IP que tiene que utilizar?

- Dirección IP asignada.
- Máscara de subred.
- Puerta de enlace predeterminada.
- Servidores DNS.

- Configuración proxy por WPAD (Web Proxy Auto-Discovery Protocol)
- Dirección IP del servidor DHCP que atendió la solicitud.
- Duración del arrendamiento (lease time).

<https://www.adslzone.net/como-se-hace/wifi/activar-dhcp/>
<https://www.redeszone.net/tutoriales/internet/que-es-protocolo-dhcp/>
<https://learn.microsoft.com/es-es/windows-server/networking/technologies/dhcp/dhcp-top>
<https://sites.uclouvain.be/SystInfo/manpages/man8/dhclient.8.html#:~:text=DESCRIPTION,by%20statically%20assigning%20an%20address.>
 (acordarme de leer esto para entender el tema).

9. ¿Qué es NAT y para qué sirve? De un ejemplo de su uso y analice cómo funcionaría en ese entorno. Ayuda: analizar el servicio de Internet hogareño en el cual varios dispositivos usan Internet simultáneamente.

Network Address Translation es un proceso de traducción de direcciones. Se utiliza para traducir direcciones privadas dentro de un espacio no privado (no “enrutable” en Internet) a direcciones públicas para un espacio público.

Permite que múltiples dispositivos en una red compartan una única dirección IP pública. Por ejemplo, en una red doméstica donde hay varios dispositivos que desean acceder a Internet a través de un router. NAT traduce las direcciones IP privadas de estos dispositivos en una única dirección IP pública, lo que permite que se comuniquen con Internet. El router lleva un registro de estas traducciones para dirigir correctamente los datos a los dispositivos locales.

Esto permite que haya un ahorro de direcciones públicas IPv4 debido a que las privadas se pueden repetir en los diferentes espacios privados (pero no dentro de uno mismo) y esto permite que varios dispositivos que están en una misma red privada puedan usar la misma dirección pública o que necesariamente no haya una dirección pública para cada dirección privada.

NAPT tiene en cuenta el puerto y toca también capa de transporte.

10. ¿Qué especifica la RFC 1918 y cómo se relaciona con NAT?

La RFC 1918 especifica un conjunto de direcciones IP reservadas para uso en redes privadas.

La RFC 1918 establece tres bloques de direcciones IP privadas en el rango de direcciones IPv4:

10.0.0.0 a 10.255.255.255
172.16.0.0 a 172.31.255.255
192.168.0.0 a 192.168.255.255

La relación entre esta RFC y NAT es que NAT se utiliza para permitir que dispositivos con direcciones IP privadas en una red local se comuniquen a través de una única dirección IP pública, que es visible en Internet.

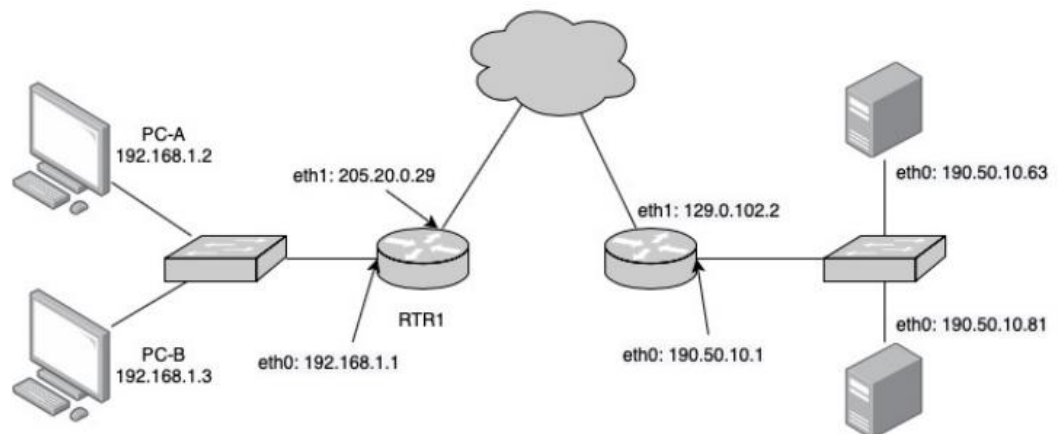
11. En la red de su casa o trabajo verifique la dirección IP de su computadora y luego acceda a www.cualesmiip.com. ¿Qué observa? ¿Puede explicar qué sucede?

ipconfig.

Salen distintas ip. Con ipconfig salen las privadas de IPv4 y en www.cualesmiip.com sale la pública IPv4.

12. Resuelva las consignas que se dan a continuación.

a. En base a la siguiente topología y a las tablas que se muestran, complete los datos que faltan.



PC-A (ss)

Local Address:Port	Peer Address:Port
192.168.1.2:49273	190.50.10.63:80
192.168.1.2:37484	190.50.10.63:25
192.168.1.2: 51238	190.50.10.81:8080

PC-B (ss)

Local Address:Port	Peer Address:Port
192.168.1.3:52734	190.50.10.81:8081
192.168.1.3:39275	190.50.10.81:8080

RTR-1 (Tabla de NAT)

Lado LAN	Lado WAN
192.168.1.2:49273	205.20.0.29:25192
192.168.1.2:51238	205.20.0.29:16345
192.168.1.3:52734	205.20.0.29:51091
192.168.1.2:37484	205.20.0.29:41823
192.168.1.3:39275	205.20.0.29:9123

SRV-A (ss)

Local Address:Port	Peer Address:Port
190.50.10.63:80	205.20.0.29:25192
190.50.10.63:25	205.20.0.29:41823

SRV-B (ss)

Local Address:Port	Peer Address:Port
190.50.10.81:8080	205.20.0.29:16345
190.50.10.81:8081	205.20.0.29:51091
190.50.10.81:8080	205.20.0.29:9123

b. En base a lo anterior, responda:**i. ¿Cuántas conexiones establecidas hay y entre qué dispositivos?**

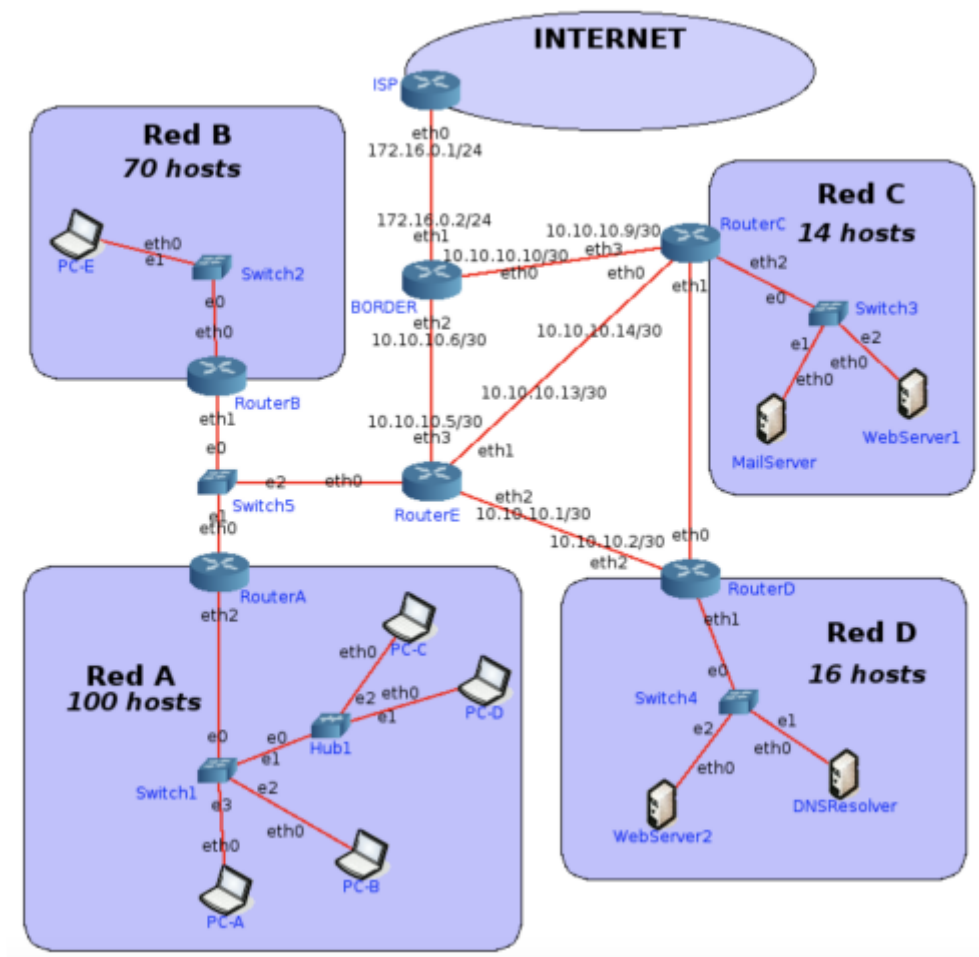
Hay 5 conexiones:

- PC-A 192.168.1.2:49273 y 190.50.10.63:80 SRV-A
- PC-A 192.168.1.2:37484 y 190.50.10.63:25 SRV-A
- PC-A 192.168.1.2: 51238 y 190.50.10.81:8080 SRV-B
- PC-B 192.168.1.3:52734 y 190.50.10.81:8081 SRV-B
- PC-B 192.168.1.3:39275 y 190.50.10.81:8080 SRV-B

ii. ¿Quién inició cada una de las conexiones? ¿Podrían haberse iniciado en sentido inverso? ¿Por qué? Investigue qué es port forwarding y si serviría como solución en este caso.

Las conexiones fueron iniciadas por los clientes ya que estos tienen direcciones privadas. Si se tiene Port Forwarding en el router para dirigir el tráfico hacia dispositivos específicos en la red local se podría realizar la conexión en el sentido inverso.

Ejercicio de repaso



13. Asigne las redes que faltan utilizando los siguientes bloques y las consideraciones debajo:

226.10.20.128/27 200.30.55.64/26 127.0.0.0/24 192.168.10.0/29
 224.10.0.128/27 224.10.0.64/26 192.168.10.0/24 10.10.10.0/27

- Red C y la Red D deben ser públicas.

- Los enlaces entre routers deben utilizar redes privadas.
- Se debe desperdiciar la menor cantidad de IP posibles.
- Si va a utilizar un bloque para dividir en subredes, asignar primero la red con más cantidad de hosts y luego las que tienen menos.
- Las redes elegidas deben ser válidas.

226.10.20.100 00000 /27 – No puedo utilizar, reservada para multicast - Publica

224.10.0.100 00000 /27 – No puedo utilizar, reservada para multicast - Publica

200.30.55.01 000000 /26 – Libre para usar - Publica

224.10.0.01 000000 /26 – No puedo utilizar, reservada para multicast - Publica

127.0.0. 00000000 /24 – No puedo utilizar, reservada para loopback - Publica

192.168.10. 00000000 /24 – Si utilizo esta para subnetting no puedo utilizar

192.168.10.0/29 porque se solapan - Privada

192.168.10. 00000 000 /29 – Considerar la de arriba - Privada

10.10.10. 000 00000 /27 – Puedo utilizarla pero debo considerar las subredes /30 que ya se asignaron en el grafico - Privada

Red A necesita 100 hosts por lo que necesita 7 bits que generarían 128 hosts

127.0.0.0/24 no es una red valida, puesto que está reservada para loopback

Voy a utilizar la 192.168.10.0/24, esto genera que no pueda utilizar la

192.168.10.0/29, por que se solaparían.

192.168.10. 00000000

255.255.255. 00000000 Mascara de red

255.255.255. 1 0000000 Mascara de Subred

Queda 1 bit para ser usados para subredes.

192.168.10.00000000/25 - 192.168.10.0/25 - Asignado para la Red A

192.168.10.10000000/25 - 192.168.10.128/25 - Libre para seguir haciendo subnetting.

Red B necesita 70 hosts por lo que necesita 7 bits que generarían 128 hosts

Por lo que voy a utilizar a la subred 192.168.10.128/25 que me quedo libre.

Red D necesita 16 hosts, necesita 5 bits que generarían 32 hosts y que la red sea pública, la única publica que puedo utilizar es 200.30.55.64/26

200.30.55.01000000

255.255.255.11000000 Mascara de red

255.255.255.11100000 Mascara de subred

Queda 1 bit para ser usados para subredes.

200.30.55.01000000/27 – 200.30.55.64/27 – Asignado para la Red D

200.30.55.01100000/27 – 200.30.55.96/27 – Libre para seguir haciendo subnetting.

Red C necesita 14 hosts, necesita 4 bits que generarían 16 hosts y que la red sea pública. En este caso vamos a seguir subneteando a 200.30.55.96/27

200.30.55.01100000

255.255.255.11100000 Mascara de red

255.255.255.11110000 Mascara de subred

Queda 1 bit para ser usado para subredes

200.30.55.01100000/28 - 200.30.55.96/28 – Asignado para la Red C

200.30.55.01110000/28 - 200.30.55.112/28 – Libre para seguir haciendo subnetting.

Router D - Router C necesitan 4 hosts por lo que necesitan 2 bits que generarían 4 hosts. A su vez se necesita que sea una red privada, tengo que

subnetear 10.10.10.0/27 evitando que se solapen con las que están en el gráfico. No puedo utilizar el bloque 192.168.10.0/29 porque se solaparía con 192.168.10.0/25 que ya fue asignada a la Red A.

10.10.10.00000000

255.255.255.11100000 Mascara de red

255.255.255.11111100 Mascara de subred

Quedan 3 bits para ser usados para subredes:

10.10.10.00000000 – 10.10.10.0/30 – Asignada para Router E y Router D

10.10.10.00000100 – 10.10.10.4/30 – Asignada para Router E y Border

10.10.10.00001000 – 10.10.10.8/30 – Asignada para Router C y Border

10.10.10.00001100 – 10.10.10.12/30 – Asignada para Router C y Router E

10.10.10.00010000 - 10.10.10.16/30 – Asigno a Router D - Router C

10.10.10.00010100 - 10.10.10.20/30 – Libre para ser asignada.

Quedo libre este bloque 10.10.10.24/29 (me di cuenta por CIDR).

10.10.10.00011000/29 - 10.10.10.24/29 - Asigno a Router A - Router B – Router E

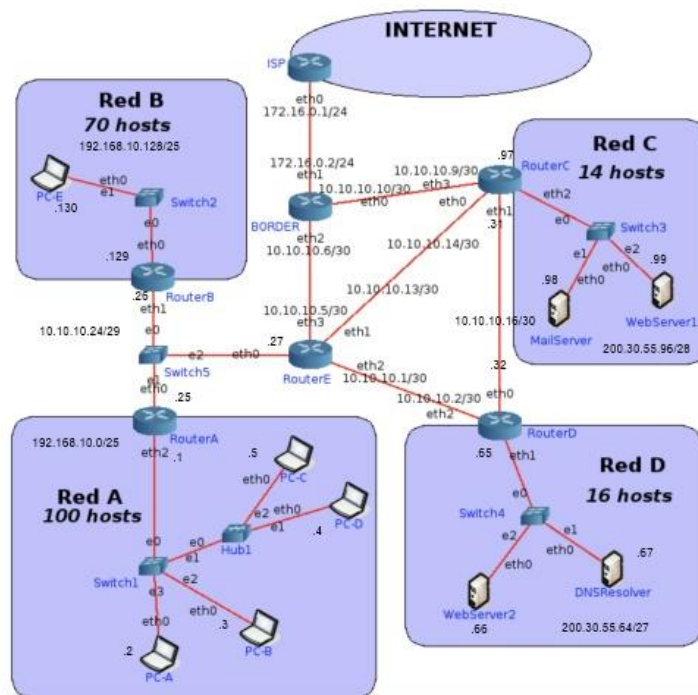
(no se si hice bien este ejercicio)

14. Asigne IP a todas las interfaces de las redes listadas a continuación.

Nota: Los routers deben tener asignadas las primeras IP de la red. Para enlaces entre routers, asignar en el siguiente orden: RouterA, RouterB, RouterC, RouterD y RouterE

- **Red A, Red B, Red C y Red D.**
- **Red entre RouterA-RouterB-RouterE.**
- **Red entre RouterC-RouterD.**

Dios sabe que lo intente



15. Realice las tablas de rutas de RouterE y BORDER considerando:

- Siempre se deberá tomar la ruta más corta.
- Sumarizar siempre que sea posible.
- El tráfico de Internet a la Red D y viceversa debe atravesar el RouterC.
- Todos los hosts deben poder conectarse entre sí y a Internet.

Border

Destination	Mask	Next-Hop	Iface
10.10.10.8	/30	-	eth0
172.16.0.0	/24	-	eth1
10.10.10.4	/30	-	eth2
10.10.10.12	/30	10.10.10.5	eth2
10.10.10.0	/30	10.10.10.5	eth2
10.10.10.24	/29	10.10.10.5	eth2
192.168.10.128	/25	10.10.10.5	eth2
192.168.10.0	/25	10.10.10.5	eth2
10.10.10.16	/30	10.10.10.9	eth0
200.30.55.64	/27	10.10.10.9	eth0
200.30.55.96	/28	10.10.10.9	eth0
0.0.0.0	/0	172.16.0.1	eth1

10.10.10.0 – 10.10.10.00000000
 10.10.10.12 – 10.10.10.00001100
 10.10.10.24 – 10.10.10.00011000

No se puede sumarizar porque no son consecutivos.

192.168.10.0 – 192.168.10.00000000
 192.168.10.128 – 192.168.10.10000000

Acá si se puede

200.30.55.64 – 200.30.55.01000000
 200.30.55.96 – 200.30.55.01100000

Acá también se puede

Border Sumarizado

Destination	Mask	Next-Hop	Iface
10.10.10.8	/30	-	eth0
172.16.0.0	/24	-	eth1
10.10.10.4	/30	-	eth2
10.10.10.12	/30	10.10.10.5	eth2
10.10.10.0	/30	10.10.10.5	eth2
10.10.10.24	/29	10.10.10.5	eth2
192.168.10.0	/24	10.10.10.5	eth2
10.10.10.16	/30	10.10.10.9	eth0
200.30.55.64	/26	10.10.10.9	eth0
0.0.0.0	/0	172.16.0.1	eth1

Router E

Destination	Mask	Next-Hop	Iface
10.10.10.24	/29	-	eth0
10.10.10.12	/30	-	eth1
10.10.10.0	/30	-	eth2
10.10.10.4	/30	-	eth3
10.10.10.8	/30	10.10.10.6	eth3

10.10.10.16	/30	10.10.10.14	eth1
200.30.55.96	/28	10.10.10.14	eth1
200.30.55.64	/27	10.10.10.14	eth1
192.168.10.0	/25	10.10.10.25	eth0
192.168.10.128	/25	10.10.10.26	eth0
172.16.0.0	/24	10.10.10.6	eth3
0.0.0.0	/0	10.10.10.6	eth3

200.30.55.64 – 200.30.55.01000000

200.30.55.96 – 200.30.55.01100000

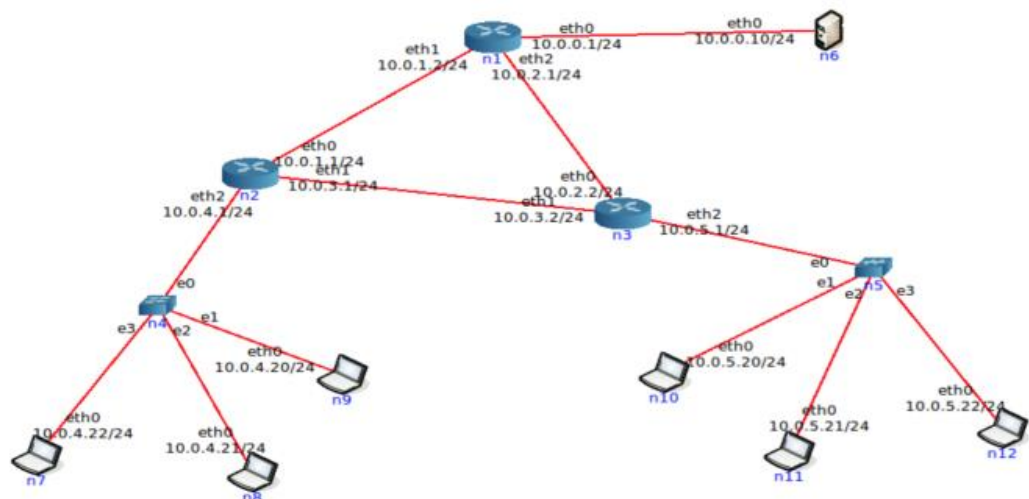
Se puede sumarizar

Despues nada mas porque no hay concidencia en salto/interface ni tampoco son consecutivos.

Router E Sumarizado

Destination	Mask	Next-Hop	Iface
10.10.10.24	/29	-	eth0
10.10.10.12	/30	-	eth1
10.10.10.0	/30	-	eth2
10.10.10.4	/30	-	eth3
10.10.10.8	/30	10.10.10.6	eth3
10.10.10.16	/30	10.10.10.14	eth1
200.30.55.64	/26	10.10.10.14	eth1
192.168.10.0	/25	10.10.10.25	eth0
192.168.10.128	/25	10.10.10.26	eth0
172.16.0.0	/24	10.10.10.6	eth3
0.0.0.0	/0	10.10.10.6	eth3

16. Utilizando la máquina virtual, se configurará ruteo estático en la red que se muestra en el siguiente gráfico:



- Antes de empezar el ejercicio ejecute en una terminal el siguiente comando:
`sudo iptables -P FORWARD ACCEPT`
- Inicie la herramienta CORE y abra el archivo 1-ruteo-estatico.imn.
- Inicie la virtualización de la topología.
- Analice las tablas de ruteo de las diferentes PCs y de los routers.
¿Qué observa? ¿Puede explicar por qué?

n1

```

vcmd
root@n1:/tmp/pycore.37757/n1.conf# netstat -r
Kernel IP routing table
Destination      Gateway         Genmask         Flags   MSS Window  irtt Iface
10.0.0.0          0.0.0.0         255.255.255.0   U        0  0          0 eth0
10.0.1.0          0.0.0.0         255.255.255.0   U        0  0          0 eth1
10.0.2.0          0.0.0.0         255.255.255.0   U        0  0          0 eth2
10.0.3.0          10.0.1.1        255.255.255.0   UG       0  0          0 eth1
10.0.4.0          10.0.1.1        255.255.255.0   UG       0  0          0 eth1
10.0.5.0          10.0.2.2        255.255.255.0   UG       0  0          0 eth2
root@n1:/tmp/pycore.37757/n1.conf#

```

n2

```

Kernel IP routing table
Destination      Gateway         Genmask         Flags   MSS Window  irtt Iface
10.0.0.0          10.0.1.2        255.255.255.0   UG       0  0          0 eth0
10.0.1.0          0.0.0.0         255.255.255.0   U        0  0          0 eth0
10.0.2.0          10.0.1.2        255.255.255.0   UG       0  0          0 eth0
10.0.3.0          0.0.0.0         255.255.255.0   U        0  0          0 eth1
10.0.4.0          0.0.0.0         255.255.255.0   U        0  0          0 eth2
10.0.5.0          10.0.3.2        255.255.255.0   UG       0  0          0 eth1
root@n2:/tmp/pycore.37757/n2.conf#

```

n3

Kernel IP routing table							
Destination	Gateway	Genmask	Flags	MSS	Window	irtt	Iface
10.0.0.0	10.0.2.1	255.255.255.0	UG	0	0	0	eth0
10.0.1.0	10.0.2.1	255.255.255.0	UG	0	0	0	eth0
10.0.2.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
10.0.3.0	0.0.0.0	255.255.255.0	U	0	0	0	eth1
10.0.4.0	10.0.3.1	255.255.255.0	UG	0	0	0	eth1
10.0.5.0	0.0.0.0	255.255.255.0	U	0	0	0	eth2

n7

Kernel IP routing table							
Destination	Gateway	Genmask	Flags	MSS	Window	irtt	Iface
default	10.0.4.1	0.0.0.0	UG	0	0	0	eth0
10.0.4.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0

Noto que las tablas de ruteo de las PC son más pequeñas y tardan más en cargar que la de los routers. Además la de la PC tiene un default.

- e. Configure las direcciones IP de las interfaces según lo que muestra el gráfico (para entrar a configurar cada equipo (PC o router) debe hacer doble click sobre el mismo, lo cual abre una terminal de comandos). Por ejemplo:

- En la PC n6 debe configurar la interfaz eth0 con la IP 10.0.0.10.
- En el Router n1 debe configurar la eth0 con la IP 10.0.0.1, la eth1 con la IP 10.0.1.2 y la eth2 con la 10.0.2.1.

n1

Kernel IP routing table							
Destination	Gateway	Genmask	Flags	MSS	Window	irtt	Iface
default	10.0.4.1	0.0.0.0	UG	0	0	0	eth0
10.0.4.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0

y así con el resto

- f. Analice las tablas de ruteo de las diferentes PCs y de los routers. ¿Qué observa? ¿Puede explicar por qué?

Observo que todo sigue igual. Supongo que es porque las direcciones IP de las interfaces ya estaban configuradas.

- g. Compruebe conectividad. Para ello, tome por ejemplo la PC n7 y haga un ping a cada una de las diferentes IPs que configuró. ¿Qué ocurre y por qué?**

El ping es exitoso porque la configuración de las tablas de ruteo es la correcta.

- h. Configure una ruta por defecto en todas las computadoras y analice los cambios en las tablas de ruteo.**

Me dice que el archivo ya existe (JA)

- i. Compruebe conectividad repitiendo el mismo procedimiento que hizo anteriormente. ¿Qué ocurre y por qué?**

El ping es exitoso porque la configuración de las tablas de ruteo es la correcta.

- j. Función de ruteo: un dispositivo que actúe como router requiere tener habilitado el encaminamiento de paquetes entre sus interfaces.**

- **Verificar IP_FORWARD, en los routers y las PCs, obteniendo la configuración con: `cat /proc/sys/net/ipv4/ip_forward`
El valor 0 indica funcionalidad desactivada (esto es correcto para las PCs). 1 indica que está habilitado (esto es requerido para los routers).**

En los hosts también esta activado idk why.

- k. Configure en los routers rutas estáticas a cada una de las redes de la topología (no utilice rutas por defecto).**

Ya estaba esto YA ESTABA TODO (mejor)

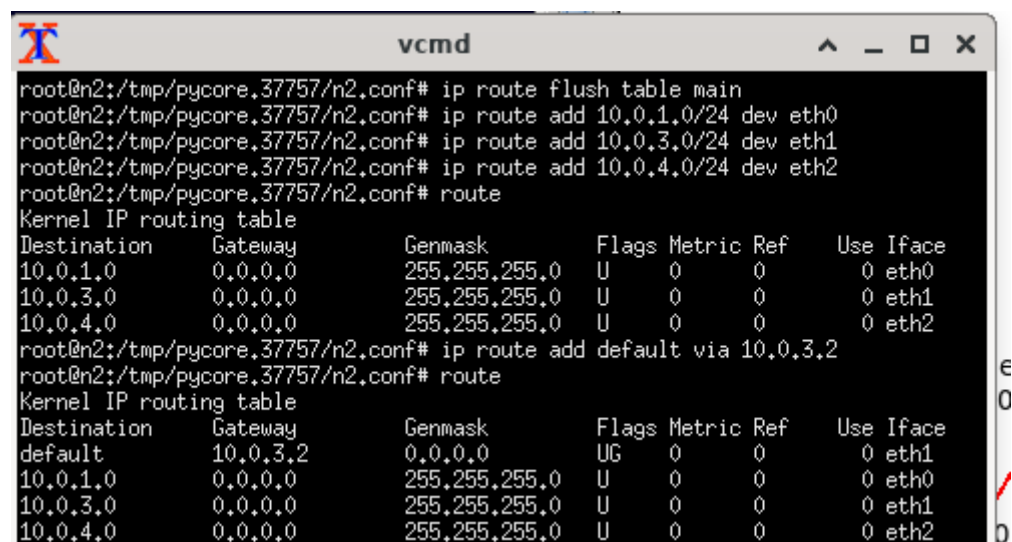
- l. Compruebe conectividad entre todos los dispositivos de la red. Si algún dispositivo no puede comunicarse con otro revise las tablas**

de ruteo y solucione los inconvenientes hasta que la conectividad sea completa.

El ping es exitoso porque la configuración de las tablas de ruteo es la correcta.

m. Modifique ahora las tablas de ruteo de los routers, eliminando todas las rutas configuradas hasta el momento y vuelva a configurarlas en base al siguiente criterio.

- Router n1 envía todo el tráfico desconocido a Router n2.
- Router n2 envía todo el tráfico desconocido a Router n3.
- Router n3 envía todo el tráfico desconocido a Router n1.



```
root@n2:/tmp/pycore.37757/n2.conf# ip route flush table main
root@n2:/tmp/pycore.37757/n2.conf# ip route add 10.0.1.0/24 dev eth0
root@n2:/tmp/pycore.37757/n2.conf# ip route add 10.0.3.0/24 dev eth1
root@n2:/tmp/pycore.37757/n2.conf# ip route add 10.0.4.0/24 dev eth2
root@n2:/tmp/pycore.37757/n2.conf# route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
10.0.1.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
10.0.3.0 0.0.0.0 255.255.255.0 U 0 0 0 eth1
10.0.4.0 0.0.0.0 255.255.255.0 U 0 0 0 eth2
root@n2:/tmp/pycore.37757/n2.conf# ip route add default via 10.0.3.2
root@n2:/tmp/pycore.37757/n2.conf# route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
default 10.0.3.2 0.0.0.0 UG 0 0 0 eth1
10.0.1.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
10.0.3.0 0.0.0.0 255.255.255.0 U 0 0 0 eth1
10.0.4.0 0.0.0.0 255.255.255.0 U 0 0 0 eth2
```

Y así con todas

n. Compruebe conectividad entre todos los dispositivos de la red. Si algún dispositivo no puede comunicarse con otro revise las tablas de ruteo y solucione los inconvenientes hasta que la conectividad sea completa

El ping es exitoso porque la configuración de las tablas de ruteo es la correcta.

o. En base a las dos configuraciones de las tablas de ruteo anteriores, responda:

- ¿Cuál opción le resultó más sencilla y por qué?

La segunda opción es mas sencilla porque no se tienen que configurar tantas redes como la primera.

- **Considerando el tamaño de las tablas de ruteo en cada situación, ¿cuál de las dos opciones la parece más conveniente y por qué?**

La segunda situación, porque se tienen una tabla de ruteo más pequeña.

- **¿Puede pensar en algún caso donde la segunda opción sea la única posible?**

Podría ser una elección intencional en un diseño de red específico cuando se busca implementar un mecanismo de redundancia o alta disponibilidad. (*chatgpt*)

- **Suponga que realiza un ping a un host que tiene la IP 190.50.12.34. ¿Qué ocurrirá en cada caso? ¿Cuál le parece mejor?**

Habrará un loop hasta que el TTL sea 0, en ese caso es mejor la primera opción, ya que será descartada en un principio por el primer router ya que la red no estará en su tabla de ruteo.