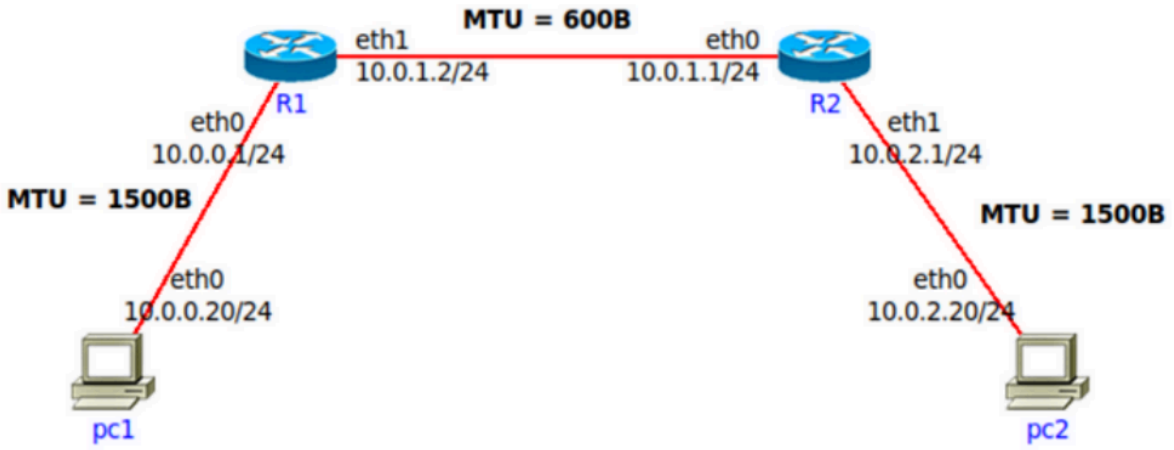
# Redes y Comunicaciones práctica 8

Capa de Red: Fragmentación - Ruteo

# Fragmentación

1. 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

  Origen: 10.0.0.20/24
  Destino: 10.0.2.20/24
  Cabecera IP: 20 bytes (mínimo pero en este caso no hay nada más)
  Tamaño: 1500 bytes
  DF: 0 (DF, Don't Fragment)
  MF: 0 (MF, More Fragments)
  Fragment Offset
  ID: 20543

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

  Se debe fragmentar

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

  Teniendo en cuenta lo siguiente: **Espacio disponible para datos (payload):** MTU - Header = **600−20=580 bytes**. Y además que el **fragment offset funciona de 8 bytes**, la cantidad máxima que podemos mandar de **datos** es de **576** (mayor múltiplo de 8 antes de 580), junto con la cabecera es **596 bytes de tamaño total**.

  Paquete 1:
  - Header: 20
  - Tamaño total: 596
  - Identificación 20543
  - DF Flag: 0
  - MF Flag: 1
  - Fragment Offset: 0

  (Hasta que ya se enviaron 576 del total, quedan 904b)

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

  Paquete 2:
  - Header: 20
  - Tamaño total: 348
  - Identificación 20543
  - DF Flag: 0
  - MF Flag: 0
  - Fragment Offset: 144

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

  En el sistema terminal se rearman, si se pierden depende de la capa de arriba lo que suceda.

- 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 fragmenta, ¿Por qué me preguntaba esto de vuelta?

# Ruteo

## 2. ¿Qué es el ruteo? ¿Por qué es necesario?

El **ruteo** es el proceso mediante el cual se **determina la ruta o camino que deben seguir los paquetes** a medida que fluyen desde un emisor a un receptor a través de una red de routers. Los algoritmos que calculan estas rutas se conocen como **algoritmos de enrutamiento**.

El ruteo es **necesario** por las siguientes razones:

- **Para entregar paquetes al destino correcto:** En una red con múltiples routers y caminos posibles, el ruteo asegura que los paquetes sean enviados a través de la ruta más eficiente y lleguen al destino final.
- **Para optimizar el uso de la red:** Los algoritmos de enrutamiento buscan rutas con el menor coste, considerando factores como el número de saltos, la congestión y la latencia. Esto ayuda a evitar la saturación de enlaces y a mantener un buen rendimiento de la red.
- **Para adaptarse a cambios en la topología de la red:** Si un enlace o router falla, el ruteo permite recalcular las rutas para evitar la zona afectada y mantener la conectividad.
- **Para aplicar políticas de enrutamiento:** Los protocolos de enrutamiento permiten a los administradores de red definir políticas que determinen qué rutas son permitidas o preferidas para ciertos tipos de tráfico.

En resumen: 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.

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

### Ruteo Estático

En el ruteo estático, las rutas cambian lentamente y suelen requerir intervención humana para actualizarse.

**Ventajas:**

- **Seguridad:** El administrador tiene control total sobre las rutas, lo que limita la posibilidad de ataques o configuraciones erróneas accidentales.
- **Predictibilidad:** Las rutas son fijas y conocidas, lo que facilita la predicción del comportamiento del tráfico.

- **Bajo consumo de recursos:** No requiere procesamiento constante para calcular rutas, lo que libera recursos del router.

**Desventajas:**

- **Administración manual:** Requiere configuración individual de cada ruta, lo que puede ser laborioso en redes grandes.
- **Falta de adaptabilidad:** No se ajusta automáticamente a cambios en la topología de la red, lo que puede llevar a interrupciones si falla un enlace o un router.
- **Escalabilidad limitada:** Difícil de administrar en redes complejas y en constante cambio.

### Ruteo Dinámico

En el ruteo dinámico, los protocolos de enrutamiento actualizan las rutas automáticamente en función de las condiciones de la red.

**Ventajas:**

- **Adaptabilidad:** Se adapta automáticamente a cambios en la topología o la carga de la red, lo que proporciona mayor resiliencia.
- **Administración simplificada:** No requiere configuración manual de cada ruta, lo que facilita la gestión de redes grandes.
- **Escalabilidad:** Adecuado para redes complejas y en crecimiento.

**Desventajas:**

- **Complejidad:** Requiere configuración y mantenimiento de protocolos de enrutamiento.
- **Consumo de recursos:** El procesamiento constante de información de enrutamiento consume recursos del router.
- **Posibilidad de inestabilidad:** En algunos casos, los protocolos dinámicos pueden causar bucles de enrutamiento o inestabilidades.

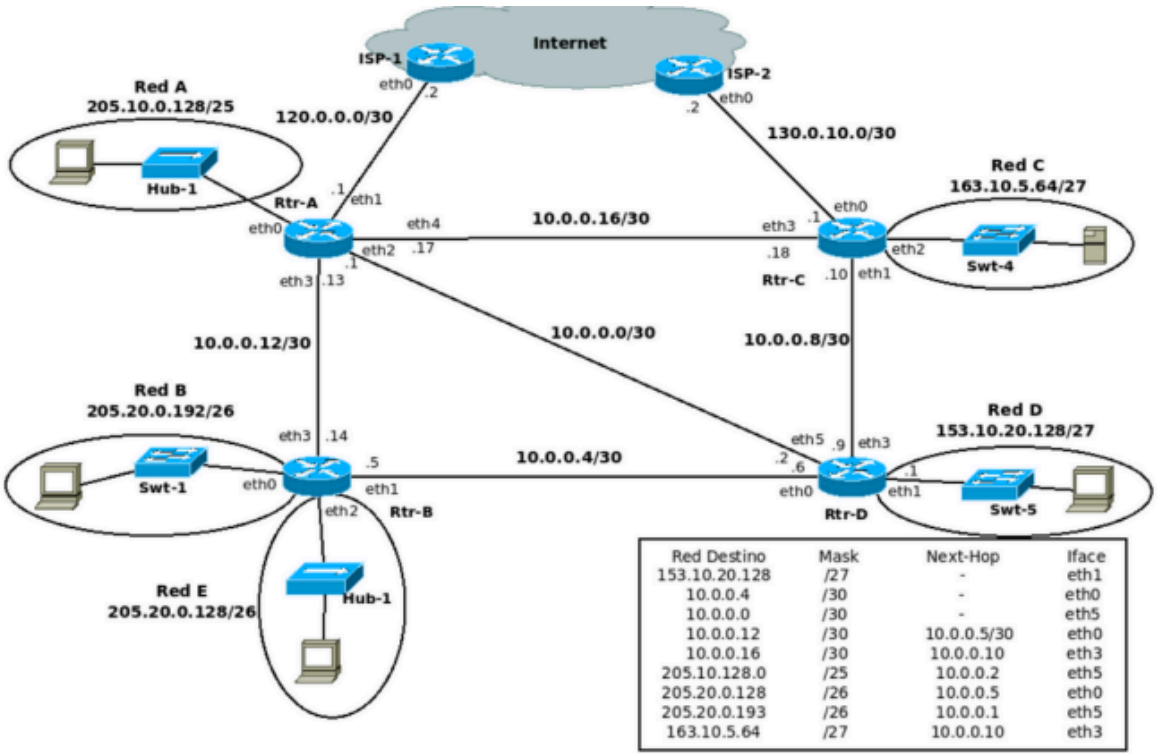
En resumen, el **ruteo estático** es adecuado para redes pequeñas y estables donde la seguridad y la predictibilidad son primordiales. El **ruteo dinámico** es mejor para redes grandes y en cambio constante que necesitan adaptarse automáticamente a las condiciones de la red.

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

Sí, **una máquina conectada a una red, pero no a Internet, aún necesita una tabla de ruteo**.

- La tabla de ruteo es esencial para que la máquina pueda comunicarse con otros dispositivos dentro de la misma red.
- Esta tabla contiene información sobre cómo llegar a diferentes destinos dentro de la red local.

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




| Red Destino | Mask | Next-Hop | Iface |
|---|---|---|---|
| 153.10.20.128 | /27 | - | eth1 |
| 10.0.0.4 | /30 | - | eth0 |
| 10.0.0.0 | /30 | - | eth5 |
| 10.0.0.12 | /30 | 10.0.0.5/30 | eth0 |
| 10.0.0.16 | /30 | 10.0.0.10 | eth3 |
| 205.10.128.0 | /25 | 10.0.0.2 | eth5 |
| 205.20.0.128 | /26 | 10.0.0.5 | eth0 |
| 205.20.0.193 | /26 | 10.0.0.1 | eth5 |
| 163.10.5.64 | /27 | 10.0.0.10 | eth3 |

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)

| Red Destino | Mask | Next-Hop | Iface |
|---|---|---|---|
| 153.10.20.128 | /27 | - | eth1 |
| 10.0.0.4 | /30 | - | eth0 |
| 10.0.0.0 | /30 | - | eth5 |
| 10.0.0.12 | /30 | 10.0.0.5/30 | eth0 |
| 10.0.0.16 | /30 | 10.0.0.10 | eth3 |
| 205.10.128.0 | /25 | 10.0.0.2 | eth5 |
| 205.20.0.128 | /26 | 10.0.0.5 | eth0 |
| 205.20.0.193 | /26 | 10.0.0.1 | eth5 |
| 163.10.5.64 | /27 | 10.0.0.10 | eth3 |

Tabla fixeada de Rtr-D

Next-hop está basado en .x del lado del router receptor, y el ethx es numero de cable desde donde sale:

| Red destino | Máscara | Next-hop | Iface |
|---|---|---|---|
| 153.10.20.128 | /27 | - | eth1 |
| 10.0.0.4 | /30 | - | eth0 |
| 10.0.0.0 | /30 | - | eth5 |
| 10.0.0.12 | /30 | 10.0.0.5 | eth0 |
| 10.0.0.16 | /30 | 10.0.0.10 | eth3 |
| 10.0.0.8 | /30 | - | 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 tiene no, habría que agregar esas direcciones a la tabla:

| Red destino | Máscara | Next-hop | Iface |
|---|---|---|---|
| 130.0.10.0 | /30 | 10.0.0.10 | eth3 |
| 0.0.0.0 | /0 | 10.0.0.10 | eth3 |

c. Teniendo en cuenta lo aplicado en el punto anterior, si Rtr-C tuviese 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

No existe así que se debe esperar a que el paquete se venza.

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

Se puede, los candidatos siendo:
10.0.0.4 → `00001010.00000000.00000000.00000100`
10.0.0.8 → `00001010.00000000.00000000.00001000`
y
205.20.0.192 → `11001101.00010100.00000000.11000000`
205.20.0.128 → `11001101.00010100.00000000.10000000`
El tema es que con los 10.0.0.x no se puede porque tiene interfaz distintas, 205.x tiene misma interfaz y saltó entonces sí se puede.

### 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

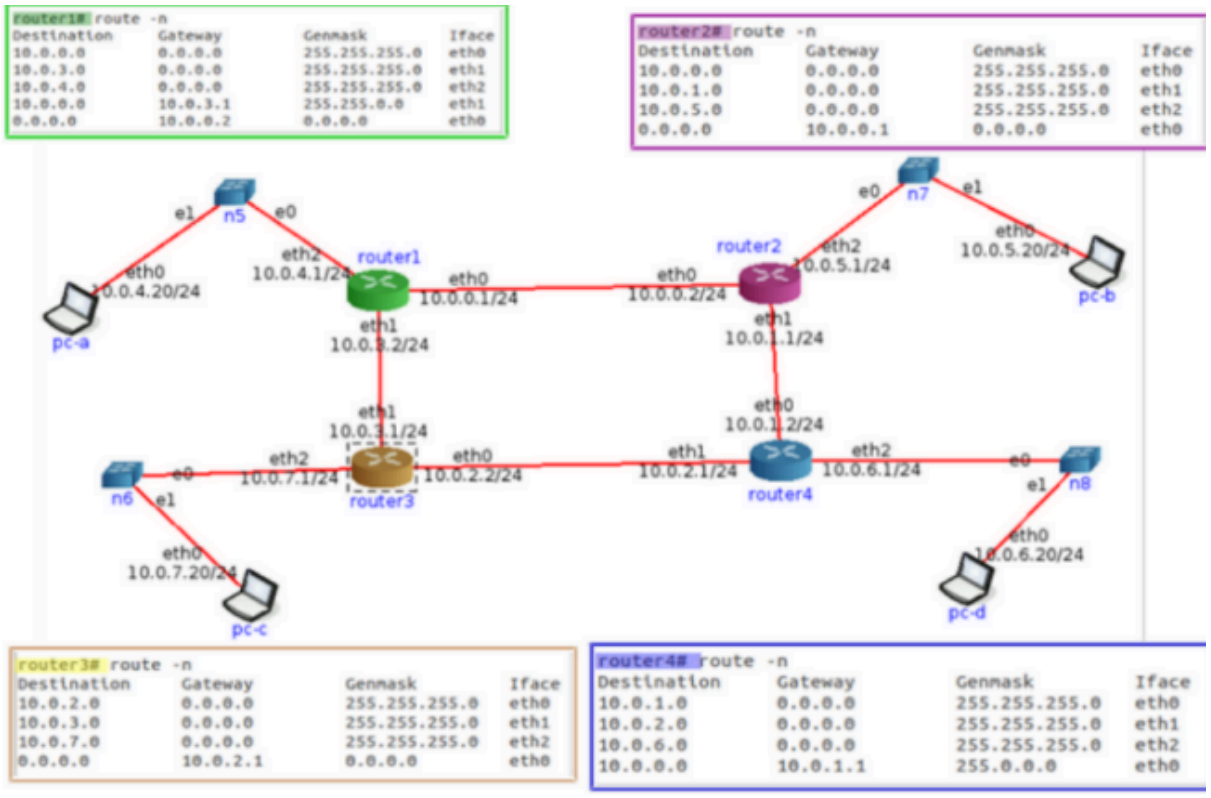
| Red destino | Máscara | Next-hop | Iface |
|---|---|---|---|
| 205.20.0.192 | /26 | | eth0 |
| 205.20.0.128 | /26 | | eth2 |
| 10.0.0.4 | /30 | | eth1 |
| 10.0.0.12 | /30 | | eth3 |
| 205.10.0.128 | /25 | 10.0.0.13 | eth3 |
| 153.10.20.128 | /27 | 10.0.0.6 | eth1 |
| 10.0.0.16 | /30 | 10.0.0.13 | eth3 |
| 10.0.0.8 | /30 | 10.0.0.6 | eth1 |
| 163.10.5.64 | /27 | 10.0.0.6 | eth1 |
| 120.0.0.0 | /30 | 10.0.013 | eth3 |
| 130.0.10.0 | /30 | 10.0.0.13 | eth3 |

| | | | |
|---|---|---|---|
| 10.0.0.0 | /30 | 10.0.0.6 | eth1 |
| 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?

Si, había que rutear a ISP-1, pasando por router A.

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




- Un mensaje ICMP enviado por PC-B a PC-C.

Los () tienen el router actual. Los [] contexto de porque llego.
Para llegar al PC-C debe:

1. Salta al 10.0.5.1/24 (router 2)
2. Salta al 10.0.0.1/24 [defecto del router 2 (router 1)]
3. Salta al 10.0.3.1/24 [coinicidencia en el router 2 (router 3]
4. Salta al 10.0.7.20/24 (conexion directa)

Hace 4 saltos y responde con tipo 0 y código 0.

● Un mensaje ICMP enviado por PC-C a PC-B.

1. Salta a 10.0.7.1/24
2. Salta a 10.0.2.1/24
3. Salta a 10.0.1.1/24
4. Salta a 10.0.5.20/24

Con 4 saltos y código y tipo 0.

● Un mensaje ICMP enviado por PC-C a 8.8.8.8.

Van al router3, luego al router 4 y ahi queda anashe (el 4 no tiene nada que coincida, pensemos que en el 3 tenia 0.0.0.0 que caia en defecto del 4)
Se hacen 2 saltos y se responde ICMP tipo 11 y código 0 (TTL caducado).

● Un mensaje ICMP enviado por PC-B a 8.8.8.8.

Van al router 2, que lo manda al router1 que lo manda al router 2 de vuelta, y queda loopeando.
Se realizan tantos saltos como sea el TTL y se responde ICMP tipo 11 y código 0 (TTL caducado).

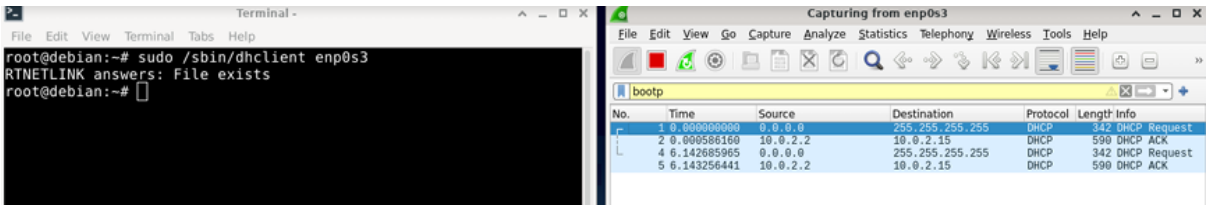
# DHCP y NAT

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

Estas me las robe de : https://github.com/agusrnfr/RyC

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?

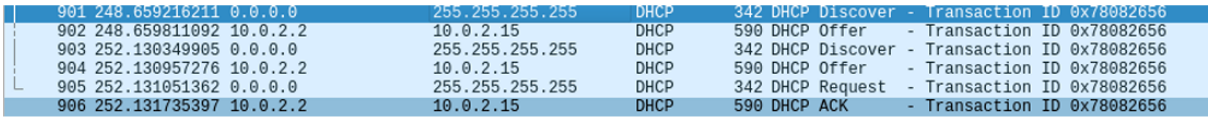
```
root@debian:~# cat /var/lib/dhcp/dhclient.leases
lease {
  interface "enp0s3";
  fixed-address 10.0.2.15;
  filename "Redes y Comunicaciones v22.2.pxe";
  option subnet-mask 255.255.255.0;
  option routers 10.0.2.2;
  option dhcp-lease-time 86400;
  option dhcp-message-type 5;
  option domain-name-servers 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 que se debió la diferencia con lo observado en el punto “b”?




En el punto “b” el cliente DHCP solicita una direccion 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/dhcp/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.

### 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).

## 8. ¿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.

**NAT (Network Address Translation, Traducción de Direcciones de Red) es una técnica que permite que múltiples dispositivos en una red privada, como una red doméstica, compartan una única dirección IP pública para acceder a Internet.**

**Ejemplo de uso en un hogar:**

Imaginemos una familia con cuatro miembros que tienen cada uno su propia computadora portátil, además de un teléfono inteligente y una consola de videojuegos, todos conectados a un router Wi-Fi en su hogar. El ISP (Proveedor de Servicios de Internet) les ha asignado una única dirección IP pública.

**Sin NAT:** Si no se utilizara NAT, cada dispositivo necesitaría su propia dirección IP pública para conectarse a Internet. Esto presentaría varios problemas:

- **Escasez de direcciones IP:** Las direcciones IPv4, que son las más utilizadas actualmente, son limitadas. Sería impracticable asignar una a cada dispositivo conectado a Internet en todo el mundo.
- **Gestión compleja:** La administración de las direcciones IP para cada dispositivo sería una tarea complicada, especialmente para un usuario doméstico.
- **Seguridad:** Exponer cada dispositivo a Internet directamente con una IP pública lo haría más vulnerable a ataques.

**Con NAT:** El router del hogar, que tiene la dirección IP pública asignada por el ISP, implementa NAT.

- **Tabla de traducciones:** El router mantiene una tabla de traducciones que mapea las direcciones IP privadas de los dispositivos en la red doméstica a la dirección IP pública del router.
    - Esta tabla también incluye los números de puerto utilizados por las aplicaciones en cada dispositivo.
- **Reescritura de direcciones:** Cuando un dispositivo en la red doméstica envía un paquete a Internet, el router NAT reescribe la dirección IP de origen del paquete, reemplazándola por su propia dirección IP pública.
- **Multiplexación de conexiones:** El router utiliza los números de puerto para diferenciar el tráfico de diferentes dispositivos y aplicaciones que comparten la misma dirección IP pública.
- **Retorno de paquetes:** Cuando un paquete de respuesta llega desde Internet, el router NAT utiliza la tabla de traducciones para dirigir el paquete al dispositivo correcto en la red doméstica.

**Beneficios de NAT:**

- **Conservación de direcciones IP:** Permite que millones de dispositivos compartan un número mucho menor de direcciones IP públicas.
- **Simplificación de la gestión:** Los usuarios domésticos no necesitan preocuparse por la administración de direcciones IP.
- **Mejora de la seguridad:** Los dispositivos en la red privada están ocultos detrás de la dirección IP pública del router, lo que los protege de accesos no autorizados desde Internet.

**Limitaciones de NAT:**

- **Complejidad en protocolos P2P:** Puede dificultar el funcionamiento de aplicaciones P2P, ya que los dispositivos detrás de NAT no tienen direcciones IP públicas directamente accesibles.

- **Violación del principio terminal a terminal:** Algunos expertos argumentan que NAT viola el principio de que los hosts deben comunicarse directamente sin la intervención de nodos intermedios que modifiquen las direcciones.

## 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.

La **RFC 1918** especifica un rango de direcciones IP privadas que **no se pueden enrutar en Internet público**. Estas direcciones se utilizan dentro de redes privadas, como las redes domésticas o corporativas, para la comunicación interna entre dispositivos.

Las tres partes del espacio de direcciones IP reservadas para redes privadas son:

- **10.0.0.0/8:** Abarca desde 10.0.0.0 hasta 10.255.255.255.
- **172.16.0.0/12:** Abarca desde 172.16.0.0 hasta 172.31.255.255.
- **192.168.0.0/16:** Abarca desde 192.168.0.0 hasta 192.168.255.255.

La **relación entre la RFC 1918 y NAT** radica en que NAT permite que los dispositivos que utilizan estas direcciones IP privadas se conecten a Internet.

- Un router NAT en la red privada traduce las direcciones IP privadas de los dispositivos internos a una única dirección IP pública asignada por el ISP.
- De esta manera, los paquetes enviados desde la red privada a Internet tienen una dirección IP de origen pública, mientras que los paquetes de respuesta desde Internet se traducen de vuelta a la dirección IP privada del dispositivo correspondiente.

**Ejemplo de uso en un hogar:**

En una red doméstica típica, varios dispositivos (computadoras, teléfonos inteligentes, etc.) comparten la misma conexión a Internet a través de un router Wi-Fi.

- El router Wi-Fi generalmente asigna direcciones IP privadas del rango 192.168.x.x a cada dispositivo en la red.
- Cuando un dispositivo envía un paquete a un servidor en Internet, el router NAT traduce la dirección IP privada del dispositivo a su propia dirección IP pública.
- El servidor en Internet responde al router NAT, y éste utiliza su tabla de traducciones NAT para reenviar la respuesta al dispositivo correcto dentro de la red doméstica.

**Importancia de la RFC 1918:**

- **Conservación de direcciones IP públicas:** Permite que múltiples dispositivos compartan una sola dirección IP pública, mitigando la escasez de direcciones IPv4.
- **Flexibilidad en el direccionamiento interno:** Las organizaciones pueden utilizar las direcciones IP privadas de manera flexible dentro de sus redes sin preocuparse por la unicidad global de las direcciones.
- **Mejora de la seguridad:** Las direcciones IP privadas no son enrutables en Internet público, lo que crea una capa adicional de seguridad para los dispositivos en la red privada.

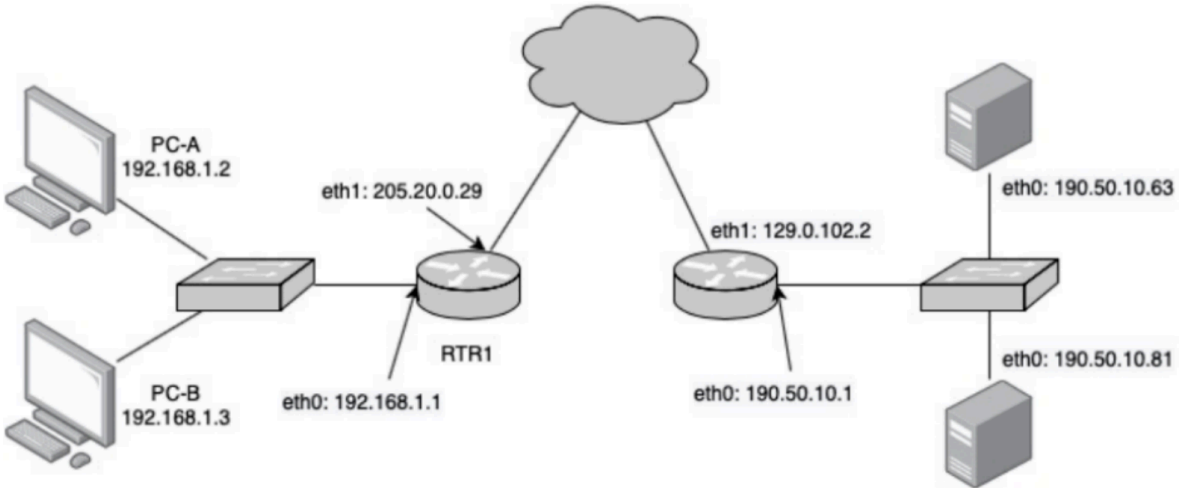
En resumen, la **RFC 1918** define un espacio de direcciones IP privadas que no se pueden enrutar en Internet público, y **NAT** aprovecha este espacio de direcciones para permitir que los dispositivos en redes privadas accedan a Internet utilizando una única dirección IP pública.

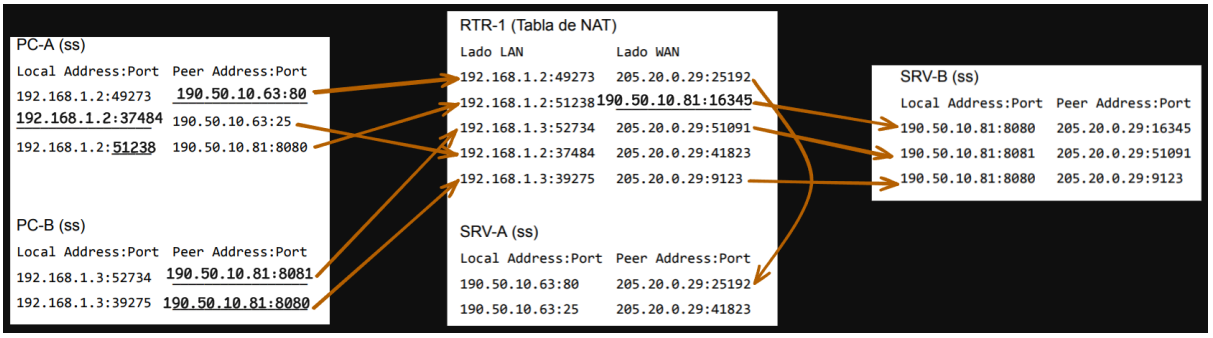
## 10. En la red de su casa o trabajo verifique la dirección IP de su computadora y luego acceda a www.cualesmiip.com. ¿Qué observa? ¿Puede explicar qué sucede?

Muestra la IP publica en la web esa, en tu casa muestra la privada.

## 11. 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.






b. En base a lo anterior, responda:

i. ¿Cuántas conexiones establecidas hay y entre qué dispositivos?

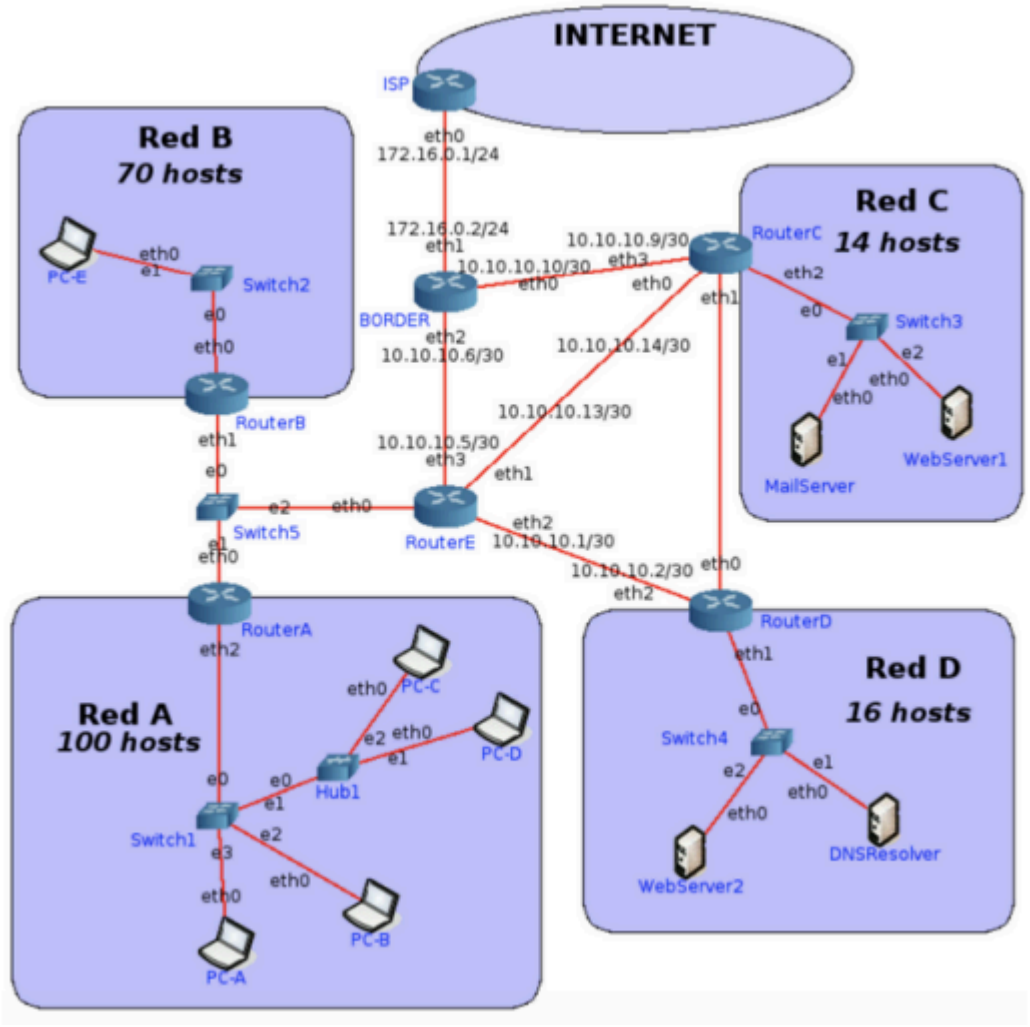
hay 5, las de PC-A y PC-B:

Hay 5 conexiones:

1. PC-A 192.168.1.2:49273 y 190.50.10.63:80 SRV-A
2. PC-A 192.168.1.2:37484 y 190.50.10.63:25 SRV-A
3. PC-A 192.168.1.2: 51238 y 190.50.10.81:8080 SRV-B
4. PC-B 192.168.1.3:52734 y 190.50.10.81:8081 SRV-B
5. 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.




## 12. 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 |
| 192.168.10.0/29 | 224.10.0.64/26 | 192.168.10.0/24 | 10.10.10.0/27 |

● Red C y la Red D deben ser públicas.

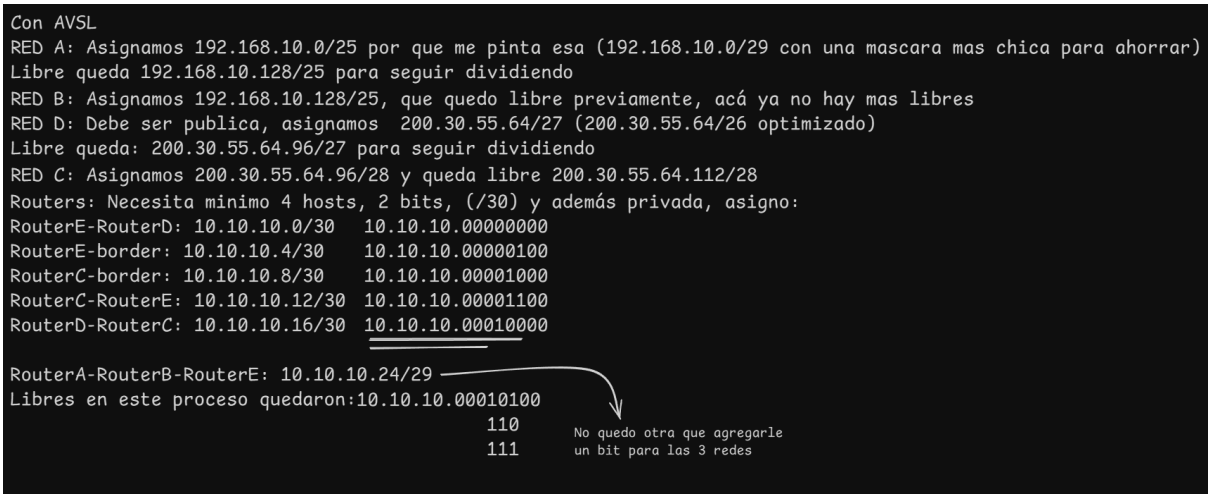
● Los enlaces entre routers deben utilizar redes privadas.

● 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.

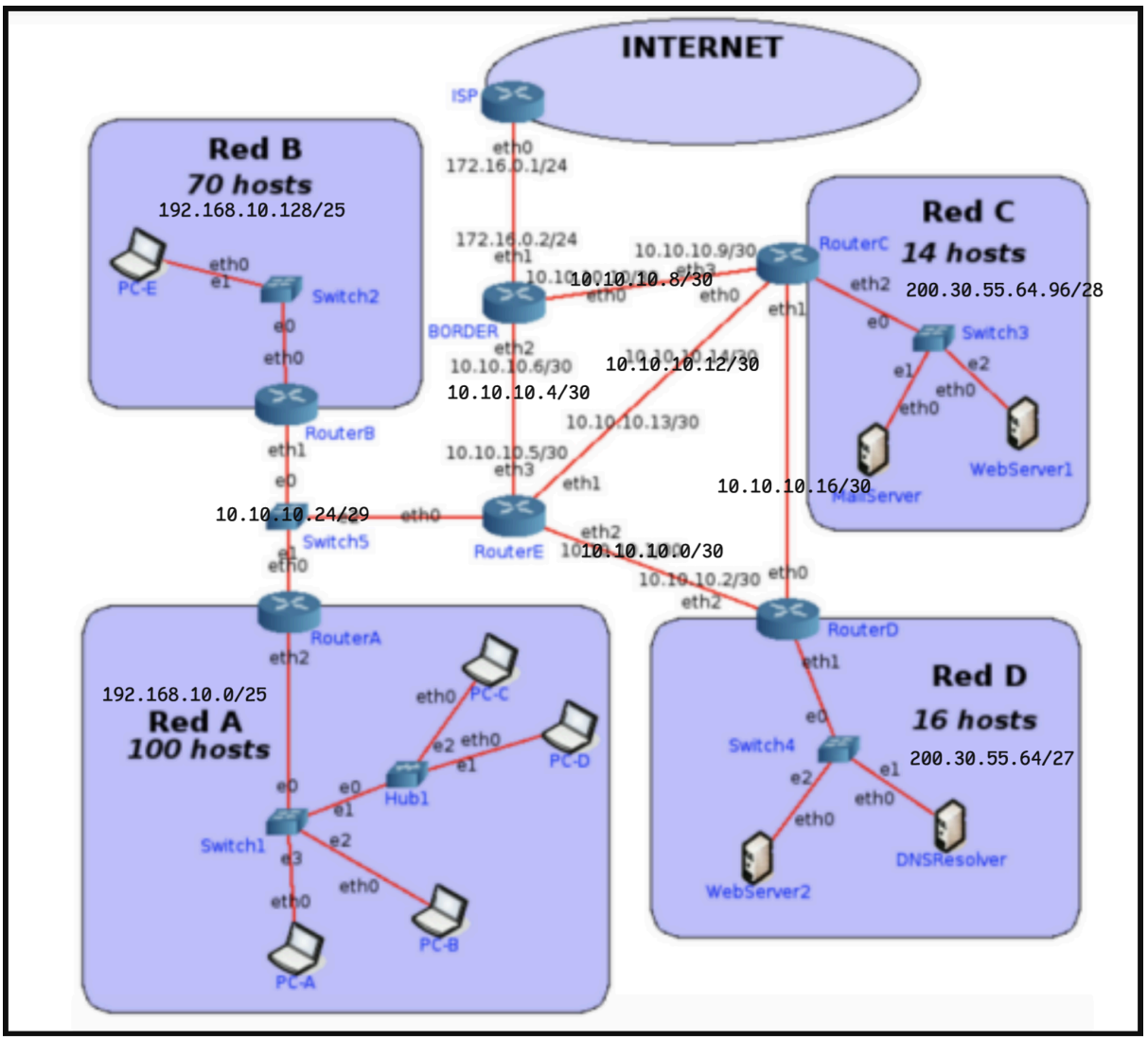
**Públicos:**
226.10.20.128/27
200.30.55.64/26
**Privados (no válidos como redes públicas):**
127.0.0.0/24 → Reservada para loopback (no se usa para redes).
192.168.10.0/29
192.168.10.0/24
10.10.10.0/27
**Multicast (no se usan para redes normales, rango 224.0.0.0/4):**
224.10.0.128/27
224.10.0.64/26




# 13. 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.

La verdad lo del orden no sé qué onda yo copie lo que hice antes.




14. 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.

RouterE

| IP | Máscara | IP sig | Cable |
|---|---|---|---|

| | | | |
|---|---|---|---|
| 10.10.10.0 | /30 | - | eth2 |
| 200.30.55.64 | /27 | 10.10.10.14 | eth1 |
| 10.10.10.4 | /30 | - | eth3 |
| 10.10.10.12 | /30 | - | eth1 |
| 200.30.55.64.96 | /28 | 10.10.10.14 | eth1 |
| 10.10.10.24 | /29 | - | eth0 |
| 192.168.10.128 | /25 | 10.10.10.25 (10.10.10.24+1) | eth0 |
| 192.168.10.0 | /25 | 10.10.10.26 (10.10.10.24+2) | eth0 |
| 10.10.10.8 | /30 | 10.10.10.6 | eth3 |
| 10.10.10.16 | /30 | 10.10.10.14 | eth1 |

**Sumarizado -> 200.30.55.64/27 y 200.30.55.64.96/28 en 200.30.55.64/26**

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 |
| 192.168.10.0 | /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 |