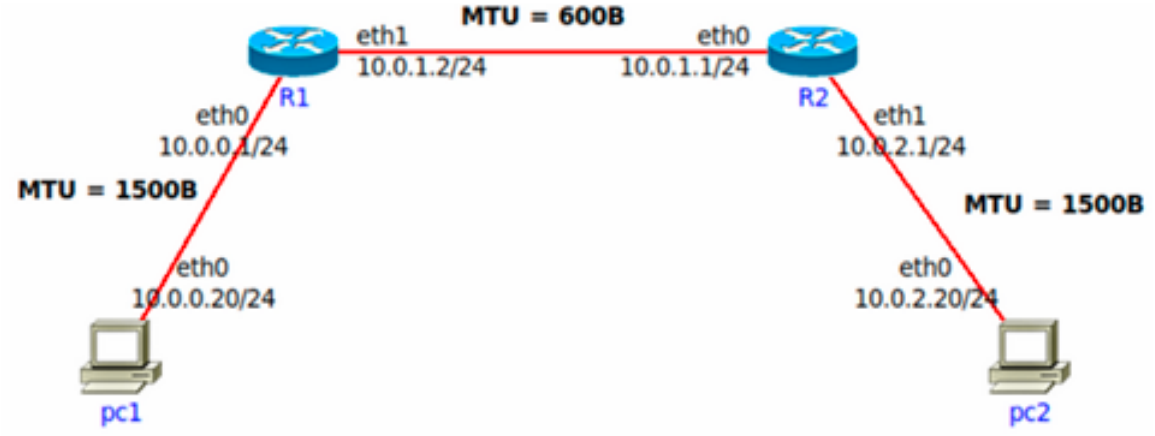
Práctica 8 - Redes y Comunicaciones

Recomendación

- Al final de la práctica se encuentra un ejercicio para ser realizado en la herramienta CORE. Si bien el ejercicio no agrega conceptos nuevos a los vistos previamente, recomendamos su resolución para que puedan configurar, probar y analizar todo lo aprendido en una simulación de una red.

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**

❖ **Ip de origen** → 10.0.0.20/24.
Ip de destino → 10.0.2.20/24.
Campos:
Cabecera IP → 20 bytes (no tiene opciones).
Tamaño → 1500 bytes (1480 bytes de datos + 20 bytes de Cabecera IP) .
Identification → 20543.
Primer bit → 0.
DF Flag → 0.
MF Flag → 0.
Desplazamiento de Fragmentación → 0.

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

❖ El paquete IP se debe fragmentar ya que el tamaño del mismo supera el MTU que soporta el enlace entre los routers.

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

❖ **Espacio disponible para datos (payload)** → **MTU - Cabecera IP** → 600 - 20 = 580 bytes.
El fragment offset funciona de a 8 bytes → La cantidad máxima de datos que podemos mandar va a ser el **múltiplo de 8 más cercano al Espacio disponible para datos (payload)** → Para este caso el múltiplo más grande es **576**, que, junto con la Cabecera IP nos deja datagramas IP de **596 bytes.**
Necesitamos enviar 3 paquetes → 1480 bytes / 576 bytes = 3.
Valor del Fragment Offset → Cantidad de bytes enviados / 8.

Paquete 1:
Cabecera IP → 20.
Tamaño → 596 bytes.
Identification → 20543.
DF Flag → 0.
MF Flag → 1.
Fragment Offset → 0.

Paquete 2:
Cabecera IP → 20.
Tamaño → 596 bytes.
Identification → 20543.
DF Flag → 0.
MF Flag → 1.
Fragment Offset → 72 (Esto es porque mandamos 576 bytes de los 1480).

Paquete 3:
Cabecera IP → 20.
Tamaño → 348 bytes.
Identification → 20543.
DF Flag → 0.
MF Flag → 0.
Fragment Offset → 144 (Esto es porque mandamos 1152 bytes de los 1480).

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

❖ Los paquetes se vuelven a unir en el sistema terminal (pc2). Si alguno de los paquetes se pierde, el accionar depende del protocolo de capa de transporte que se utilice.

- **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.

Ruteo

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

- El ruteo es el proceso de determinar el camino o la ruta que debe seguir un paquete de datos desde su origen hasta su destino a través de una red.
- Su función principal es seleccionar la interfaz de salida y el próximo salto. Lo implementan los Routers y los Hosts.
- Es de control, es decir, no maneja directamente el tráfico de datos, sino que toma decisiones sobre cómo se debería enrutar el tráfico.
- Ocurre en routers y, en menor medida, en hosts.
- Utiliza la **RIB (Routing Information Base)** o tabla de enrutamiento para almacenar los resultados del proceso de ruteo, esta tabla es alimentada a partir del uso de **protocolos de enrutamiento** (RIP, OSPF, BGP, etc) que construyen y actualizan la RIB.

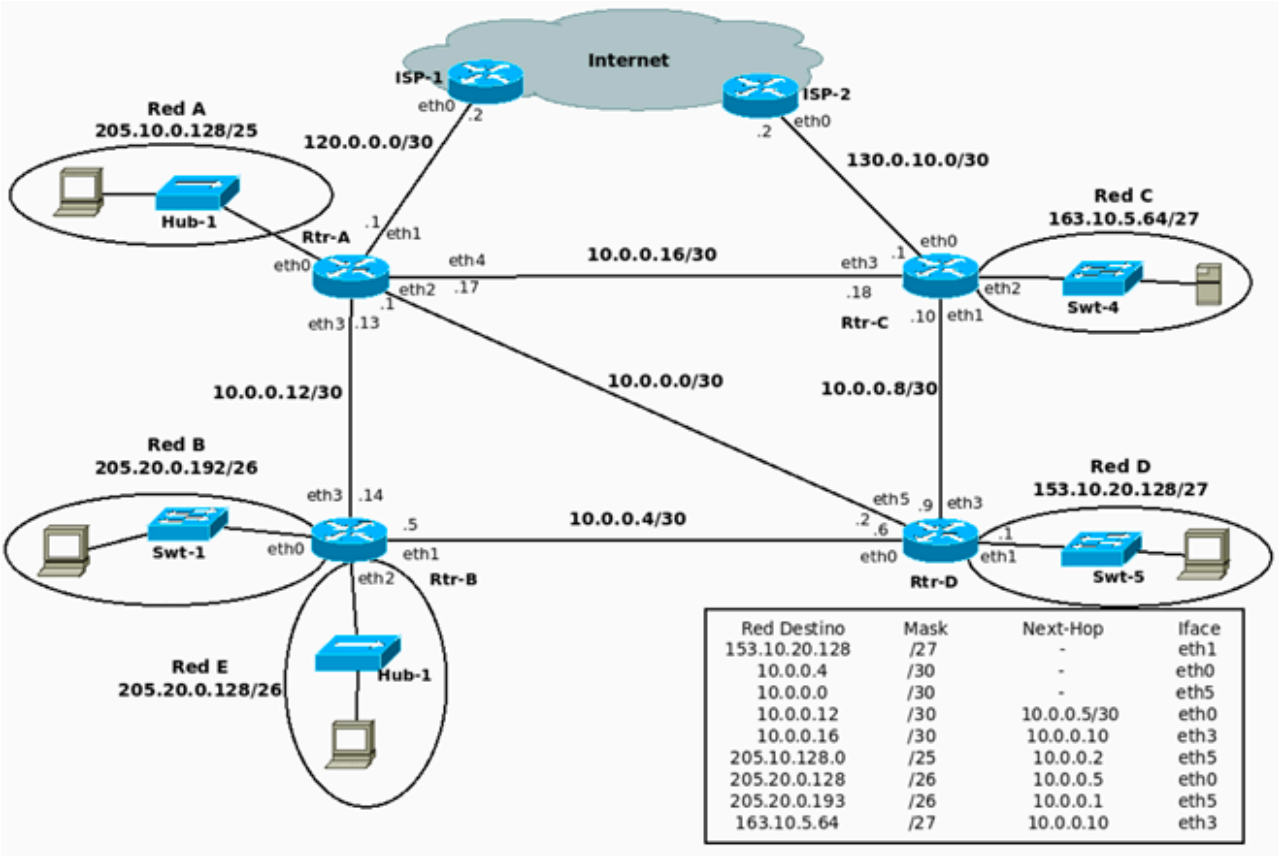
3. **En las redes IP el ruteo puede configurarse en forma estática o en forma dinámica. Indique ventajas y desventajas de cada método.**

- **Tipos de Ruteo:**
    - **Ruteo Estático:**
        - Las rutas se configuran manualmente por el administrador.
        - **Ventajas:**
            - Fácil de implementar en redes pequeñas.
            - No consume recursos adicionales en el router.
            - Ofrece mayor control y seguridad.
        - **Desventajas:**
            - No se adapta automáticamente a cambios en la red.
            - No es escalable ni tolerante a fallos.
    - **Ruteo Dinámico:**
        - Utiliza protocolos de enrutamiento para aprender y actualizar rutas automáticamente aunque requiere una configuración inicial por el administrador.
        - **Ventajas:**
            - Se adapta automáticamente a cambios en la topología.
            - Escalable y tolerante a fallos.
            - Facilita la gestión en redes grandes o complejas.
        - **Desventajas:**
            - Requiere más recursos de procesamiento.
            - La configuración inicial es más compleja.

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	Máscara	Next-Hop	Iface
153.10.20.128	/27	-	eth1
10.0.0.4	/30	-	eth0
10.0.0.0	/30	-	eth5
10.0.0.8	/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
205.20.0.128	/26	10.0.0.5	eth0
205.20.0.192	/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.

- La tabla anterior, no tiene salida a internet ya que no hay ninguna entrada que lleve a un ISP.

Red Destino	Máscara	Next-Hop	Iface
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
```

- Se entra en Loop hasta que se venza el TTL del paquete y se descarte.

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

- **Sumarización:**
  - Técnica utilizada en redes para **agrupar múltiples rutas** en una sola entrada más general en la tabla de enrutamiento. Esto reduce el tamaño de la tabla de enrutamiento y simplifica el proceso de enrutamiento, especialmente en redes grandes.
  - **Condiciones para Sumarizar:**
    - La cantidad de bloques a sumarizar debe ser **potencia de 2.**
    - Los bloques deben estar **contiguos.**
    - La **primera dirección IP** debe ser **divisible** por la **suma de los hosts** de los bloques a sumarizar.

        - Si la **dirección IP termina en 0 (cero)**, siempre va a ser divisible.
    - Todas las **subredes** deben ser alcanzables a través de la **misma interfaz** y el **mismo next-hop.**
- **Podemos aplicar la sumarización para las entradas:**
    - **205.20.0.128** → 11001101 . 00010100 . 00000000 . 10000000
    - **205.20.0.192** → 11001101 . 00010100 . 00000000 . 11000000
- **Condiciones:**
    - La cantidad de bloques es potencia de 2 ya que estamos agrupando 2 bloques.
    - Los bloques son contiguos ya que 205.20.0.128/26 cubre el rango de 205.20.0.128 a 205.20.0.191, y 205.20.0.192/26 cubre el rango de 205.20.0.192 a 205.20.0.255.
    - La primera dirección IP es divisible por la suma de los hosts ya que cada /26 tiene 64 hosts y al sumarizar tenemos un rango de 128 hosts (64 + 64). La primera dirección 205.20.0.128 es divisible por 128.
    - Ambas redes usan la misma interfaz y el mismo Next-Hop.

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

- La sumarización aplicada en el punto anterior no se podría aplicar en el Rtr-B ya que las redes **205.20.0.128** y **205.20.0.192** no comparten la misma interfaz, se usan las interfaces **eth0** y **eth2.**

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.**

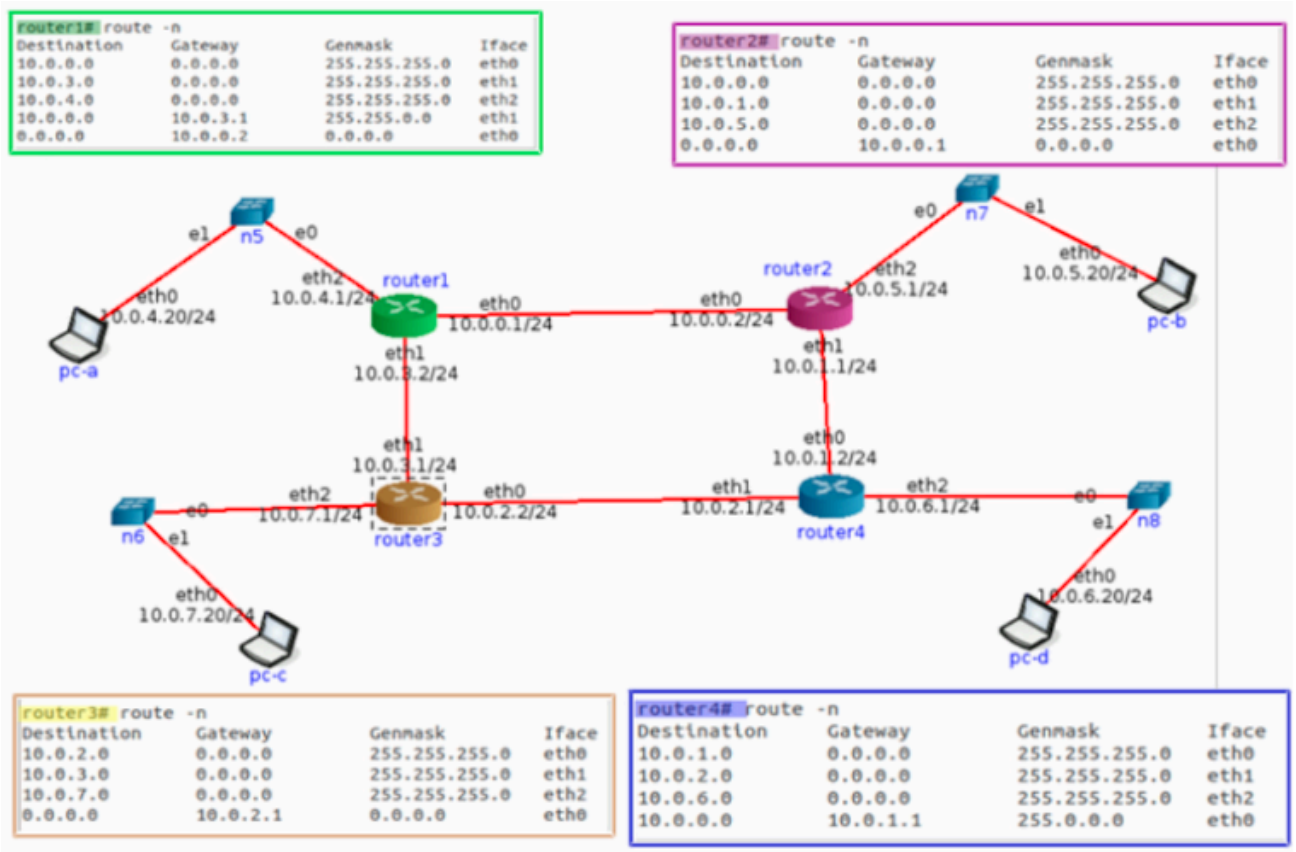
Red Destino	Máscara	Next-Hop	Iface
205.20.0.192	/26	-	eth0
205.20.0.128	/26	-	eth2
10.0.0.12	/30	-	eth3
10.0.0.4	/30	-	eth1
10.0.0.8	/30	10.0.0.6	eth1
10.0.0.0	/30	10.0.0.6	eth1
10.0.0.16	/30	10.0.0.13	eth3
205.10.0.128	/25	10.0.0.13	eth3

153.10.20.128	/27	10.0.0.6	eth1
163.10.5.64	/27	10.0.0.6	eth1
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, es posible restablecer el acceso a Internet pasando por el Rtr-A para ir al ISP-1.

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.**

❖ **Recorrido:**

➢ La PC-B envía el mensaje con IP 10.0.7.20/24 al Router 2.

➢ El Router 2 recibe el mensaje con IP 10.0.7.20/24 y lo reenvía al Default Gateway ya que no coincide con ninguna entrada, por lo tanto, se envía al Router 1 a través de la Iface eth0 usando el Hop 10.0.0.1.

- El Router 1 recibe el mensaje con IP 10.0.7.20/24 y lo reenvía al Router 3 usando la entrada 10.0.0.0 con Genmask /16 a través de la Iface eth1 con Hop 10.0.3.1 ya que la IP recibida no puede ser procesada por la entrada 10.0.0.0 con Genmask /24.
- El Router 3 recibe el mensaje con IP 10.0.7.20/24 y lo envía usando la entrada 10.0.5.0 con Genmask /24 a través de la Iface eth2 con una conexión directa.

❖ **Tipo de respuesta recibida:**
- La respuesta es de tipo 0 con código 0.

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

❖ **Recorrido:**
- La PC-C envía el mensaje con IP 10.0.5.20/24 al Router 3.
- El Router 3 recibe el mensaje con IP 10.0.5.20/24 y lo reenvía al Default Gateway ya que no coincide con ninguna entrada, por lo tanto, se envía al Router 4 a través de la Iface eth0 usando el Hop 10.0.2.1.
- El Router 4 recibe el mensaje con IP 10.0.5.20/24 y lo reenvía al Router 2 usando la entrada 10.0.0.0 con Genmask /8 a través de la Iface eth0 con Hop 10.0.1.1.
- El Router 2 recibe el mensaje con IP 10.0.5.20/24 y lo envía usando la entrada 10.0.7.0 con Genmask /24 a través de la Iface eth2 con una conexión directa.

❖ **Tipo de respuesta recibida:**
- La respuesta es de tipo 0 con código 0.

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

❖ **Recorrido:**
- La PC-C envía el mensaje con IP 8.8.8.8 al Router 3.
- El Router 3 recibe el mensaje con IP 8.8.8.8 y lo reenvía al Default Gateway ya que no coincide con ninguna entrada, por lo tanto, se envía al Router 4 a través de la Iface eth0 usando el Hop 10.0.2.1.
- En el Router 4 como no hay entrada en la tabla que coincida, el paquete se descarta por TTL caducado.

❖ **Tipo de respuesta recibida:**
- La respuesta es de tipo 11 con código 0 (TTL caducado).

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

❖ **Recorrido:**
- La PC-B envía el mensaje con IP 8.8.8.8 al Router 2.
- El Router 2 recibe el mensaje con IP 8.8.8.8 y lo reenvía al Default Gateway ya que no coincide con ninguna entrada, por lo tanto, se envía al Router 1 a través de la Iface eth0 usando el Hop 10.0.0.1.

- ➢ El Router 1 recibe el mensaje con IP 8.8.8.8 y lo reenvía al Default Gateway ya que no coincide con ninguna entrada, por lo tanto, se envía al Router 2 a través de la Iface eth0 usando el Hop 10.0.0.2.
- ➢ El paquete entra en Loop hasta que caduca su TTL y se descarta.

❖ **Tipo de respuesta recibida:**

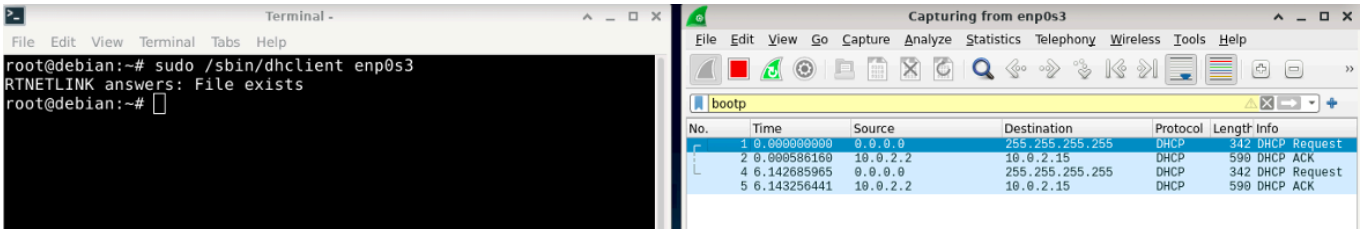
- ➢ La respuesta es de tipo 11 con código 0 (TTL caducado).

DHCP y NAT

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

   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”?

```
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/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.

- Traslación de direcciones de un espacio privado (no “enrutable” en Internet) a un espacio público.
- Los procesos de traslación se realizan sobre redes stubs (solo una salida) y se deben mantener tablas de traslaciones.
- Existen varias formas de realizarlo:
    - **NAT Básico:**
        - Una forma de realizarlo es “one-to-one”.
        - Se mapea una dirección IPv4 privada a una dirección IPv4 pública.
        - Permite acceso en ambas direcciones.
        - **Forma Estática:**
            - Requiere tantas direcciones públicas como privadas.
        - **Forma Dinámica:**

            - No requiere tantas direcciones públicas como privadas, pero sí requiere un timer por cada entrada.
            - Limita el acceso simultáneo de acuerdo al pool pub.
    - **NAPT (Network Address Port Translation)**
        - NAT no es implementable cuando se tiene un pool chico de direcciones o no se poseen direcciones públicas asignadas.
            - En ese caso se debe trabajar con campos de la capa de transporte o del payload.
        - NAPT es conocido como PAT (Port Address Translation): “one-to-many”.
        - Se utilizan los puertos de los protocolos u otros valores como ICMP Identifier para resolver el mapeo.
        - Se pueden usar timers y sesión del protocolo.
        - En la tabla de traslaciones se mantienen el protocolo y los puertos origen y destino.
        - Se intenta conservar el puerto origen, pero si está “ocupado” se debe reemplazar por otro. Básicamente si hay otro que genera mismo puerto y destino y no hay más direcciones, se cambia el puerto origen (por uno que no está ocupado).
        - El dispositivo debe “violar” los límites impuestos por la división en capas.
        - **Tiene 2 alternativas:**
            - **Dinámico sobre pool:** utiliza un pool y hace PAT sobre este (habitual en nuestras casas).
            - **Dinámico sobre dirección overload/masquerade:** utiliza la dirección IP externa y haciendo overloading/masquerading sobre esta.

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

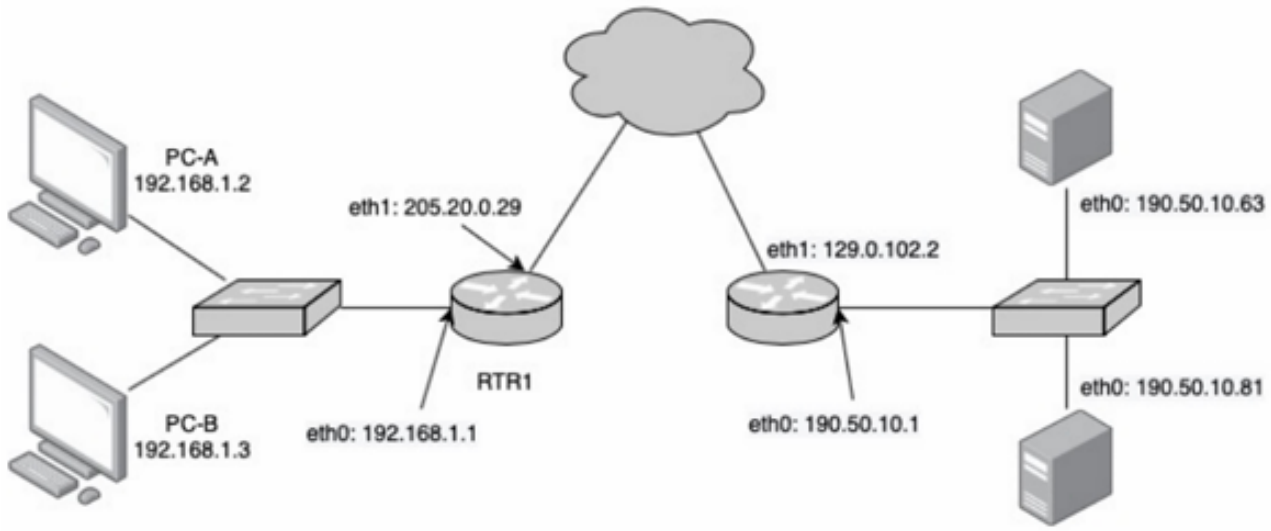
- La **RFC 1918** especifica un rango de direcciones IP privadas que **no se pueden enrutar en Internet público.** Estas direcciones se utilizan dentro de redes privadas, como las redes domésticas o corporativas, para la comunicación interna entre dispositivos. Las tres partes del espacio de direcciones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

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 pública 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.**



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:

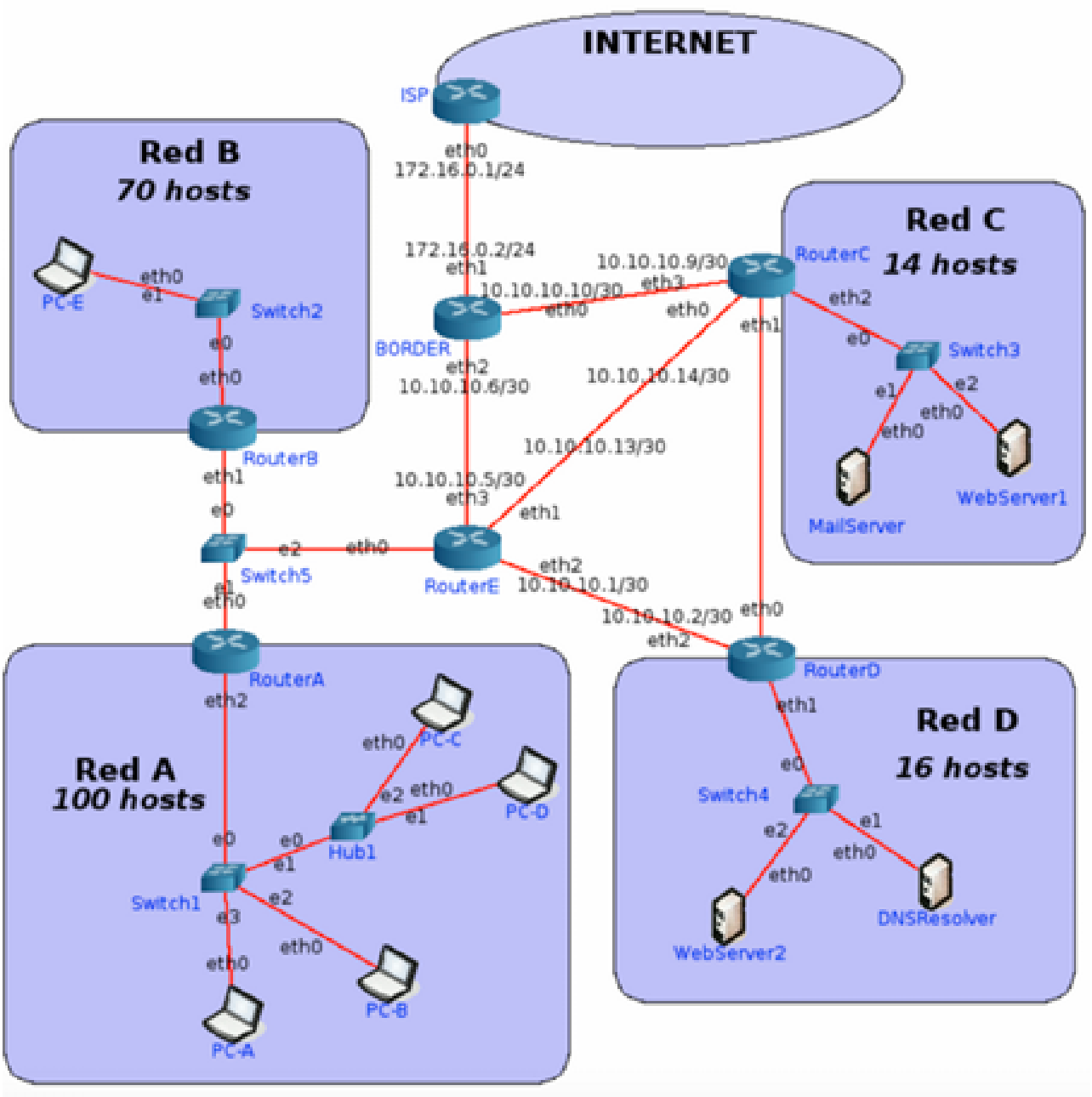
i. ¿Cuántas conexiones establecidas hay y entre qué dispositivos?

- **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 las PC's ya que son las que tienen direcciones privadas.
- **Port Forwarding**
  - Overloading/Masq no permiten acceso desde "afuera" hacia "adentro".
  - Solo se permite entrar tráfico de conexiones generadas internamente.
  - Permite poder tener servicios en una red privada accesibles desde "afuera".
  - No se requiere NAT estático, se implementa con NAPT y mapeo reverso estático de puertos.
  - Se configura a mano.
- Si tuviéramos el Port Forwarding activado 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



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**
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.**

DIRECCIONES PRIVADAS

Todas las que empiecen con 10.
Todas las que estén entre 172.16 a 172.31
Todas las que empiecen con 192.168

DIRECCIONES ESPECIALES

Loopback → Todas las que empiecen con 127.
Dir. de red → La que tiene los bits de hosts todos en 0
Dir. de broadcast → La que tiene los bits de hosts todos en 1
Cuando el host no tiene dir. asociada → 0.0.0.0

RANGOS DE LAS CLASES

Clase A → 1 a 126
Clase B → 128 a 191
Clase C → 192 a 223
Clase D → 224 a 239 (Multicast)
Clase E → 240 a 255 (Experimental)

Bloques de Direcciones:

226.10.20.128/27
Binario → 11100010 . 00001010 . 00010100 . 10000000
Clase → D
Categoría → Pública
Se puede usar? → No. Está reservada para Multicast

224.10.0.128/27
Binario → 11100000 . 00001010 . 00000000 . 10000000
Clase → D
Categoría → Pública
Se puede usar? → No. Está reservada para Multicast

200.30.55.64/26
Binario → 11001000 . 00100010 . 00110111 . 01000000
Clase → C
Categoría → Pública
Se puede usar? → Si

224.10.0.64/26
Binario → 11100000 . 00001010 . 00000000 . 01000000
Clase → D
Categoría → Pública
Se puede usar? → No. Está reservada para Multicast

127.0.0.0/24
Binario → 01111111 . 00000000 . 00000000 . 00000000
Clase → -
Categoría → Especial
Se puede usar? → No. Está reservada para Loopback

192.168.10.0/24
Binario → 11000000 . 10101000 . 00001010 . 00000000
Clase → C
Categoría → Privada
Se puede usar? → Si

192.168.10.0/29
Binario → 11000000 . 10101000 . 00001010 . 00000000
Clase → C
Categoría → Privada
Se puede usar? → Si

10.10.10.0/27
Binario → 00001010 . 00001010 . 00001010 . 00000000
Clase → A
Categoría → Privada
Se puede usar? → Si

RED A (100 + 2 = 102 HOSTS)
MÁSCARA → M = log2(102) = 7 → /25
RED → 192.168.10.0/25 - 11000000 . 10101000 . 00001010 . 00000000
DIR. LIBRES → 11000000 . 10101000 . 00001010 . 10000000

RED B (70 + 2 = 72 HOSTS)
MÁSCARA → M = log2(72) = 7 → /25
RED → 192.168.10.128/25 - 11000000 . 10101000 . 00001010 . 10000000

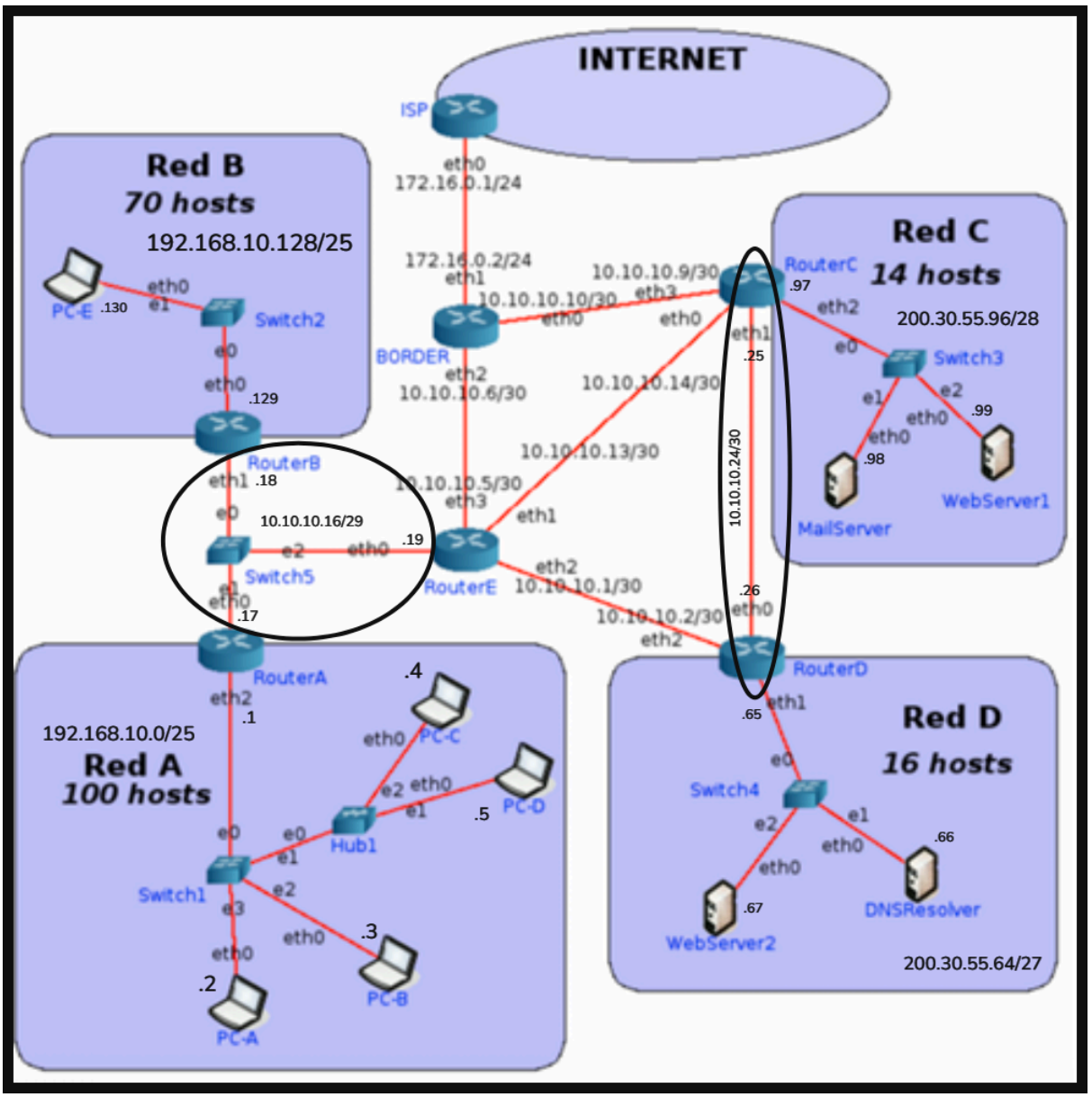
RED D (16 + 2 = 18 HOSTS)
MÁSCARA → M = log2(18) = 5 → /27
RED → 200.30.55.64/27 - 11001000 . 00100010 . 00110111 . 01000000
DIR. LIBRES → 11001000 . 00100010 . 00110111 . 01100000

RED C (14 + 2 = 16 HOSTS)
MÁSCARA → M = log2(16) = 4 → /28
RED → 200.30.55.96/28 - 11001000 . 00100010 . 00110111 . 01100000
DIR. LIBRES → 11001000 . 00100010 . 00110111 . 01110000

RED Rtr-A / Rtr-B / Rtr-C (3 + 2 = 5 HOSTS)
MÁSCARA → M = log2(5) = 3 → /29
RED → 10.10.10.16/29 - 00001010 . 00001010 . 00001010 . 00010000
DIR. LIBRES → 00001010 . 00001010 . 00001010 . 00011000

RED Rtr-C / Rtr-D (2 + 2 = 4 HOSTS)
MÁSCARA → M = log2(4) = 2 → /30
RED → 10.10.10.24/30 - 00001010 . 00001010 . 00001010 . 00011000

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.**
    - **RedA, Red B, Red C y Red D.**
    - **Red entre Router A-Router B-Router E**
    - **Red entre Router C-Router D.**



14. Realice las tablas de rutas de Router E 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 Router C.**
- **Todos los hosts deben poder conectarse entre sí y a Internet.**

Router E

Red Destino	Máscara	Next Hop	Iface
10.10.10.16	/29	-	eth0
192.168.10.0	/25	10.10.10.17	eth0
192.168.10.128	/25	10.10.10.18	eth0

10.10.10.4	/30	-	eth3
10.10.10.12	/30	-	eth1
10.10.10.0	/30	-	eth2
172.16.0.0	/24	10.10.10.6	eth3
10.10.10.8	/30	10.10.10.14	eth1
10.10.10.24	/30	10.10.10.14	eth1
200.30.55.96	/28	10.10.10.14	eth1
200.30.55.64	/27	10.10.10.2	eth2
0.0.0.0	/0	10.10.10.6	eth3

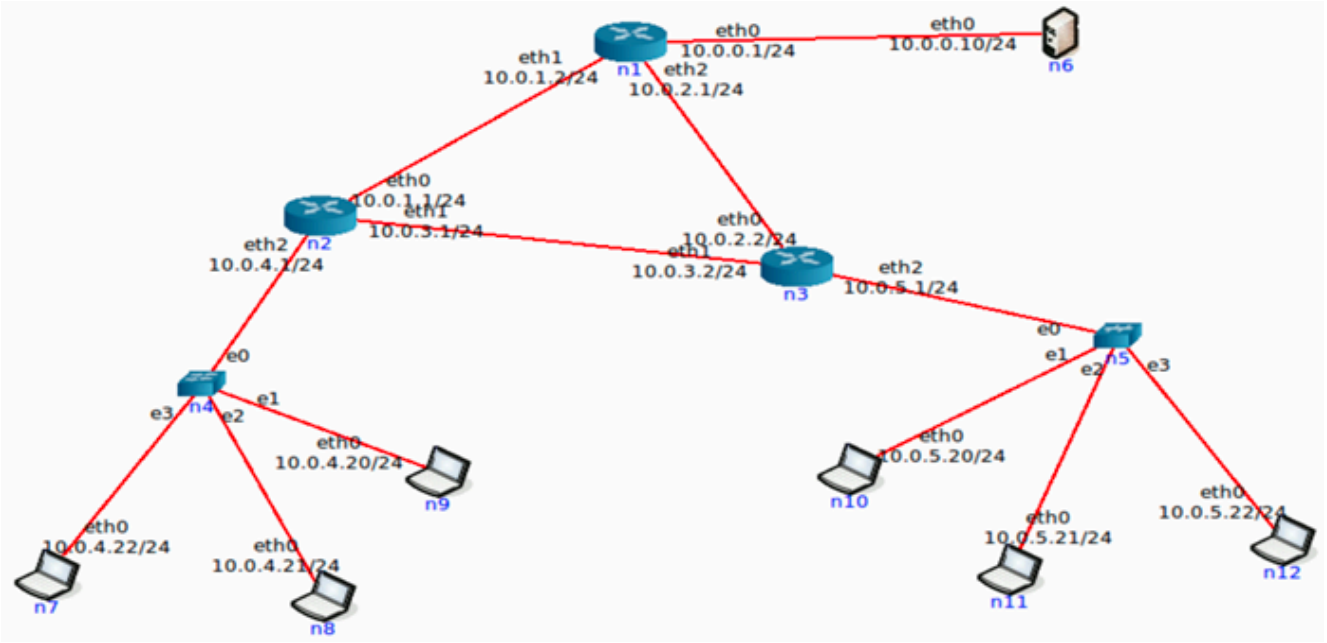
Router BORDER

Red Destino	Máscara	Next Hop	Iface
10.10.10.16	/29	10.10.10.5	eth2
192.168.10.0	/24	10.10.10.5	eth2
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
172.16.0.0	/24	-	eth1
10.10.10.8	/30	-	eth0
10.10.10.24	/30	10.10.10.9	eth0
200.30.55.96	/28	10.10.10.9	eth0
200.30.55.64	/27	10.10.10.9	eth0
0.0.0.0	/0	172.16.0.1	eth1

Aclaración Importante

- En CORE no se guardan los cambios realizados en una topología al detenerla. Por ello, es deseable completar todo el ejercicio una vez empezado, para no tener que volver a configurar todo. Alternativamente se puede utilizar el script que se encuentra en este repositorio https://github.com/RYSAEI/SaveRestoreScripts para forzar que se guarden los cambios.

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



a. **Antes de empezar el ejercicio ejecute en una terminal el siguiente comando: $ sudo iptables-P FORWARD ACCEPT**
b. **Inicie la herramienta CORE y abra el archivo 1-ruteo-estatico.imn.**
c. **Inicie la virtualización de la topología.**
d. **Analice las tablas de ruteo de las diferentes PCs y de los routers. ¿Qué observa? ¿Puede explicar por qué?**
e. **Configure las direcciones IP de las interfaces según lo que muestra el gráfico (para entrar a configurar cada equipo ya sea una PC o un 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.**
f. **Analice las tablas de ruteo de las diferentes PCs y de los routers. ¿Qué observa? ¿Puede explicar por qué?**
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?**
h. **Configure una ruta por defecto en todas las computadoras y analice los cambios en las tablas de ruteo.**
i. **Compruebe conectividad repitiendo el mismo procedimiento que realizó anteriormente. ¿Qué ocurre y por qué?**
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).

k. **Configure en los routers rutas estáticas a cada una de las redes de la topología (no utilice rutas por defecto).**
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.**
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.**
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.**
o. **En base a las dos configuraciones de las tablas de ruteo anteriores, responda:**
    - **¿Cuál opción le resultó más sencilla y por qué?**
    - **Considerando el tamaño de las tablas de ruteo en cada situación, ¿cuál de las dos opciones le parece más conveniente y por qué?**
    - **¿Puede pensar en algún caso donde la segunda opción sea la única posible?**
    - **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?**

NO LO VOY A HACER