**Capa de Red: Fragmentación - Ruteo Redes y comunicaciones - 2022**

**Práctica 8**

**Capa de Red: Fragmentación – Ruteo**

**6, 7, 8, 13, 14, 15, 16**

**Recomendación**

**1. 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**

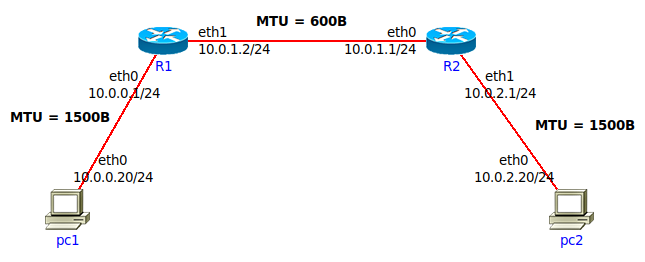
**Fragmentación**

**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:**

\*MTU: Unidad de transferencia máxima.



**Indicar IPs origen y destino y campos correspondientes a la fragmentación cuando el paquete sale**

**de pc1**

i) IP origen: 10.0.0.20

ii) IP destino: 10.0.2.20

iii) Identificación: 20543

iv) Longitud total: 1500

v) Flag DF: false. No fragmentar 1 (true) / fragmentar 0 (false) → DoNotFragment

vi) Flag MF: false. Si hay más paquetes que correspondan al datagrama → MoreFragmet: vienen más fragmentos atrás

vii) Offset de fragmento: 0. Se usa para ensamblar el datagrama IP

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

Entre R1 y R2 el MTU o Máxima Unidad de Transferencia es de 600 Bytes, por lo que el paquete de 1500 Bytes es demasiado grande, la solución a esto es fragmentar el paquete:

Fragmento 1:

* Le da un valor 20543 al header Identification
* Pone el flag DF en false, MF en true
* Le da un valor 0 al header Fragment Offset
* Le da un valor de 596 al header Total Length, para que el Fragment Offset del siguiente fragmento (o en otras palabras, la cantidad de bytes de datos de este fragmento) sea múltiplo de 8 🡺 576 es múltiplo de 8
  + La cantidad de datos inicial es de 1500-20 (Resta encabezado)=1480 bytes
  + El MTU es 600 bytes, de los cuales 20 son de headers (sin Options)
  + La cantidad de datos del fragmento 1 será 600-20 (Headers)=580 bytes
  + 580 no es múltiplo de 8, entonces busca el siguiente más bajo que sí lo sea: 580/8=72.5 🡪 72 \* 8= 576
  + Como el campo Total Length incluye la longitud de los headers, valdrá 576+20=596 bytes
  + Falta por enviarse 1480-576=904 bytes

Fragmento 2:

* *Le da un valor 20543 al header Identification*
* *Pone el flag DF en false, MF en true*
* Le da un valor 576/8=72 al header Fragment Offset (Numero de “Pedacitos de 8 que hay)
* *Le da un valor de 596 al header Total Length, para que el Fragment Offset del siguiente fragmento sea múltiplo de 8*
  + La cantidad de datos restante es de 904 bytes
  + *El MTU es 600 bytes, de los cuales 20 son de headers (sin Options)*
  + *La cantidad de datos del fragmento 2 será 600-20=580 bytes*
  + *580 no es múltiplo de 8, entonces busca el siguiente más bajo que sí lo sea (576)*
  + *Como el campo Total Length incluye la longitud de los headers, valdrá 576+20=596 bytes*
  + Falta por enviarse 904-576=328 bytes

\*En cursiva lo que es igual al anterior

Fragmento 3:

* *Le da un valor 20543 al header Identification*
* Pone el flag DF en false, MF en false
* Le da un valor (576+576)/8=144 al header Fragment Offset
* Le da un valor de 348 al header Total Length, como no hay siguiente fragmento, si no es múltiplo de 8 no importa
  + La cantidad de datos restante es de 328 bytes
  + Como el campo Total Length incluye la longitud de los headers, valdrá 328+20=348 bytes

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

El MTU es de 600B y cada encabezado de fragmentación pesa 20B, por lo que en cada fragmento se transportan 580B de datos, entonces:

1500B / **580**B = 2.6…B, por lo que tendré que fragmentar el paquete en 3.

**580** no es múltiplo de 8. Siguiente menor: 580/8=72.5, por lo tanto 72\*8= 576🡪**576** de datos +20 de encabezado= **596**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Fragmento** | **Secuencia** | **Identificación** | **Total Length** | **Flags DF** (Siempre es 0, si es 1 no se puede fragmentar) | **Flag MF** (Si hay más paquetes) | **Frag. Offset** |
| 1 | 0-0 | 20543 | **596** | False (0) | True (1) No es el ultimo | 0 (Es el 1º) |
| 2 | 0-1 | 20543 | **596** | false (0) | True (1) No es el ultimo | **72** (**576**/8) |
| 3 | 0-2 | 20543 | 348 | false (0) | False (0) Es el ultimo | 144 (**72**+**576**/8) |

576+576+348=1500 🡪 El original era de 1500, con 20 de encabezado

**¿Dónde se unen nuevamente los fragmentos?**

La estación receptora (Host destino) es responsable de reensamblar los fragmentos en el datagrama IPv4 original de tamaño completo.

El que se encarga de unir de nuevo los fragmentos es el que recibe los datos fragmentados, este caso es PC2, por lo que los datos quedan fragmentados en todo el trayecto.

**¿Qué sucede si un fragmento no llega?**

Si un fragmento no llega, dependiendo del protocolo de capa de transporte, es posible que se deban volver a transmitir todos los fragmentos del paquete

**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?**

En ese caso, el router volverá a fragmentar ese fragmento, para poder enviarlo.

**Ruteo**

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

* **Ruteo**: función de seleccionar por cuál interfaz se enviará un dato, si lo recibe otro router éste hará lo mismo, y así sucesivamente. Se necesita para formar caminos desde el host origen al host destino, pasando por los nodos intermedios
* **Enrutamiento:** proceso mediante el cual se construye la tabla de ruteo o RIB (Routing Information Base)
* El protocolo ENRUTADO (Routed) IP, requiere los servicios del protocolo de ruteo para construir las tablas de ruteo en cada router (gateway)
* **Forwarding/Switching**: selecciona un port de salida en función de la dirección de destino y tabla de
* ruteo. Usado por el protocolo ENRUTADO.
* **FIB Forwarding Information Base / Forwarding Table:** el proceso de forwarding que se hace a partir de la RIB. Se optimiza generando una tabla más eficiente, FIB.

Routing

* Decisiones de “forwarding” en IP se llevan a cabo localmente
* Deriva en conectividad entre los diferentes puntos de la red
* Se requiere recolectar y procesar un estado global que se mantiene localmente en cada router
* Los estados locales deben ser consistentes, si son inconsistentes la red no habrá convergido a un estado estable, se generan loops

Se requiere:

o Consistencia

o Completitud

o Escalabilidad

Se desea:

o Camino óptimo

o Balanceo

o Adaptabilidad

El router dirige el tráfico hacia otras rutas directamente conexas y/o redes remotas. Por ende, los routers dirigen a los paquetes en la red y tienen más de una interfaz de salida, las cuales, cada una, están conectadas a una red.

**Tabla de enrutamiento:**

Contiene información para que el router reenvíe paquetes hacia la red de destino, utilizando la información de asociación entre la red y el siguiente salto. (tiene direcciones de las redes a las que quiero llegar)

- Ubicación: Es un archivo de datos que se encuentra en la memoria del router.

- Conceptos:

**- Destino:** lugar a donde quiero llegar.

- **Destination 0000 (ruta por defecto).** Si un paquete no tiene una ruta específica, se envía por esta ruta por defecto. Va a terminar llegando a otro router, que repite el procedimiento.

- Gateway: a donde tengo que enviar el datagrama para llegar a “Destino”.

- **Gateway 0000: indica que estoy en la red a la cual quería llegar**, y debo mandar el datagrama al dispositivo final.

- Interfaz de salida: placa de red por la que sale el paquete. En una PC hay una sola (dada por el proveedor de internet). En un router hay varias.

**Rutas en una tabla:**

* **Rutas conectadas directamente:** aparecen en la tabla porque existe una conexión física entre el router y esa red.
* **Rutas estáticas:** ruta que se configura manualmente y que siempre es la misma hacia un destino.
* **Rutas dinámicas:** ruta que puede variar dependiendo de las variables del protocolo que se configuró.

**4. En las redes IP el ruteo puede configurarse en forma estática o en forma dinámica. Indique ventajas y**

**desventajas de cada método.**

**Tipos de Routing**

Todos los equipos en la red corren el protocolo ENRUTADO, por ejemplo IP (IPv4 o IPv6)

Los hosts no requieren protocolos de ENRUTAMIENTO/RUTEO

Los router requieren hacer el ENRUTAMIENTO y podrían trabajar de dos formas/ tipos de Routing:

o Ruteo Estático

o Ruteo Dinámico, requerido en una red compleja con muchos routers y enlaces

Routers pueden participar de forma activa en el routing: reciben, generan y propagan información,

los hosts lo hacen de forma pasiva (no envían ni propagan información)

|  |  |
| --- | --- |
| Ruteo Estático | Ruteo Dinámico |
| * Un administrador de red establece manualmente una ruta de envío de paquetes a la red destino. * Sirve con red sencilla | * Routers comparten información de la tabla de enrutamiento mediante protocolos de enrutamiento dinámico. Tabla de enrutamiento casi se mantiene sola. * Requiere una configuración inicial por el administrador * Caminos “óptimos” de acuerdo a la información manejada por el protocolo (métrica, costo) * Sirve con red compleja |
| Ventajas   * No tiene problemas de seguridad ni de incompatibilidad * No implica costo de procesamiento extra (Bajo uso de CPU por que no se comunica con otros routers) * Mayor control al administrador | Ventajas   * Si se cambia la topología se adapta de forma automática * Facilita mantenimiento en red compleja * Escalable y tolerante a fallos * Un mismo flujo de datos podría enviarse por distintos caminos |
| Desventajas   * Propenso a errores humanos * Si se cambia la topología requiere cambios manuales en los routers (Difícil mantenimiento) * Esquema NO escalable y NO tolerante a fallo | Desventajas   * Resolución de Problemas/Debugging, más complejo * Se requiere diseñar un algoritmo que determine cómo armar la tabla de ruteo * Costo de procesamiento extra debido al router que ejecuta y comunica |

Protocolos de enrutamiento: llenan las tablas de rutas para tomar la decisión de cual seguir.

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

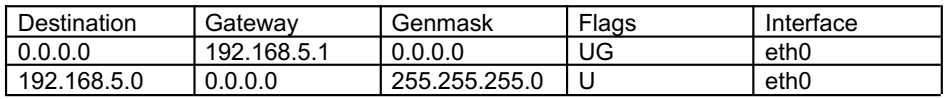
Sí, porque aunque sea una red local se utiliza la tabla de enrutamiento para comunicarse con los demás dispositivos de la red. (por ejemplo, otra pc o una impresora compartida).

En la tabla de enrutamiento hay que tener:

- entrada de tabla con default route, destination 0000 y un gateway particular → a donde se mandan los paquetes cuyo destino no está en la tabla de ruteo

- entrada de la tabla con un destination en particular y el gateway 0000, que indica que ya está en la red del destino y no necesita hops intermedios (le manda directamente el datagrama al dispositivo final)

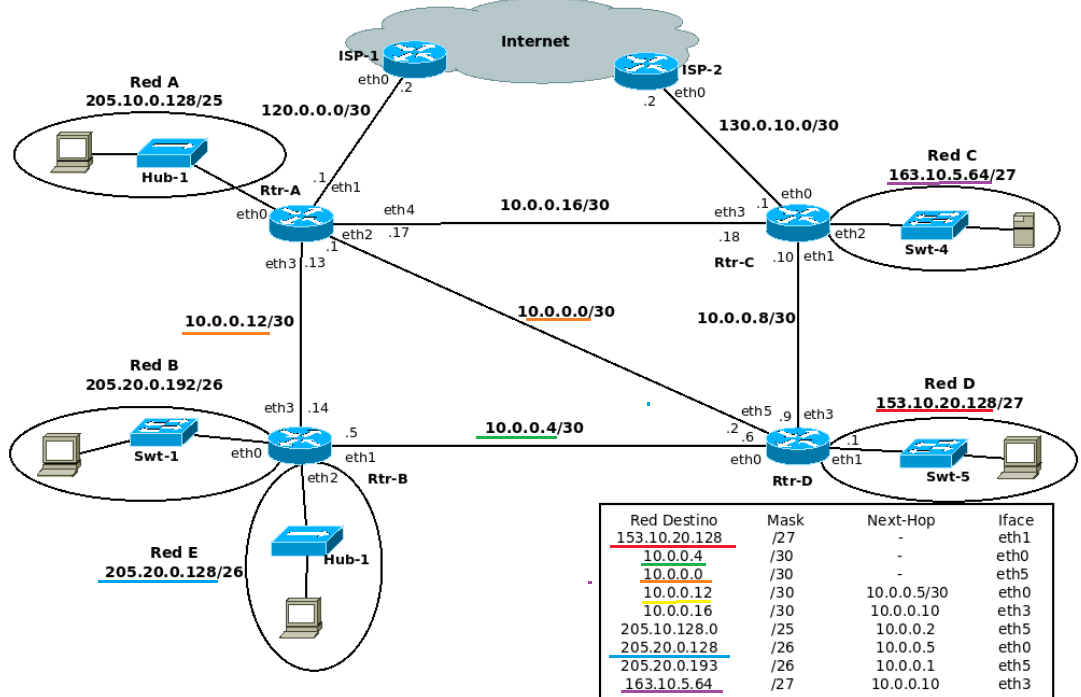
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Red destino** | **Máscara** | **Sig. gateway** | **Interfaz** | **Métrica** |
| 127.0.0.0 | /8 | 127.0.0.1 | localhost | 1 |
| 0.0.0.0 | /0 | 192.168.0.1 (Router) | eth0 | 10 |
| 192.168.0.0 (Red) | /24 | - | eth0 | 10 |



NOTA: es super importante notar que en la parte de destination pongo REDES, no IPS. Me importa saber cómo llego a ‘x’ red y una vez que llego ahí el router le manda el paquete al host correspondiente.

* + - VER CUAL DE LAS DOS TABLAS ES MEJOR

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



**PREGUNTAR SI EL NEXT HOP LLEVA MÁSCARA**

**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** | **INTERFACE** |
| 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 | 10.0.0.5/30 | eth0 |
| 10.0.0.16 | /30 | 10.0.0.10/30 | eth3 |
| 205.10.0.128 | /25 | 10.0.0.1/30 | eth5 |
| 205.20.0.128 | /26 | 10.0.0.5/30 | eth0 |
| 205.20.0.192 | /26 | 10.0.0.5/30 | eth0 |
| 163.10.5.64 | /27 | 10.0.0.10/30 | 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 porque le falta un gateway default, al cual enviar los paquetes que no están dirigidos a la red local

La solución es usar al Rtr-A o Rtr-C como default-gateway:

|  |  |  |  |
| --- | --- | --- | --- |
| Red destino | Máscara | Sig. gateway | Interfaz |
| 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**

i) El Rtr-D:

(1) Recibe el paquete y decrementa el TTL

(2) Aplica la máscara de red, y reconoce que el paquete se dirige a la red 163.10.5.64/27

**En si, si la red es 163.10.5.64/27, no seria 163.10.5.010|0 000, 163.10.5.15, debería ser otra red, una que tenga 163.10.5.000|0 000 (?**

(3) Para que siga su camino, lo envía al destino 10.0.0.10/30 a través de la interfaz eth3

ii) El Rtr-C:

(1) Recibe el paquete y decrementa el TTL

(2) Aplica la máscara de red, y reconoce que el paquete se dirige a la red 163.10.5.0/24. **Aca si tiene sentido, cierra en la tabla con la mascara /24 y terminando en .0**

(3) Para que siga su camino, lo envía al destino 10.0.0.9/30 a través de la interfaz eth1

iii) Ambos routers seguirán haciendo esto, hasta que el TTL llega a 0, donde uno de los dos descartará el paquete

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

**para poder aplicarla?**

Se podría realizar entre las entradas 205.20.0.128/26 y 205.20.0.192/26, ya que tienen los primeros 25 bits iguales (de izquierda a derecha) y las demás columnas de la tabla son idénticas. Con otras entradas pasa que hay valores intermedios que van por otras interfaces, ejemplo: .4 y .12 van por eth0, pero entre ellas está .8 que va por eth3.

.8 y .16 van por eth3, pero entre ellas se encuentra .12 por eth0, por lo que no pueden juntarse.

|  |  |  |  |
| --- | --- | --- | --- |
| Red destino | Máscara | Sig. gateway | Interfaz |
| 205.20.0.128 | /25 | 10.0.0.5 | eth0 |

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

No sería posible, porque la columna de Interfaz cambia entre ambas entradas.

**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** | **INTERFACE** |
| 153.10.20.128 | /27 | 10.0.0.6/30 | Eth1 |
| 10.0.0.4 | /30 | - | Eth1 |
| 10.0.0.0 | /30 | 10.0.0.6/30 | Eth1 |
| 10.0.0.8 | /30 | 10.0.0.6/30 | Eth1 |
| 10.0.0.12 | /30 | - | Eth3 |
| 10.0.0.16 | /30 | 10.0.0.13/30 | Eth3 |
| 205.10.0.128 | /25 | 10.0.0.13/30 | Eth3 |
| 205.20.0.128 | /26 | - | Eth2 |
| 205.20.0.192 | /26 | - | Eth0 |
| 163.10.5.64 | /27 | 10.0.0.6 | Eth1 |
| 0.0.0.0 | /0 | 10.0.0.13/30 | Eth3 |

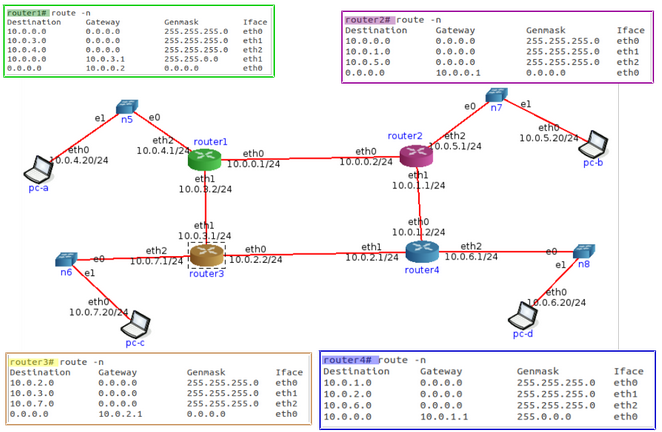
**g. Si Rtr-C pierde conectividad contra ISP-2, ¿es posible restablecer el acceso a Internet sin esperar a**

**que vuelva la conectividad entre esos dispositivos?**

Sí, habría que mandar lo que sale por el default Gateway de Router C a Router A, ya que este tiene conexión a internet por ISP-1.

**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.**

i) Origen Pc b: 10.0.5.20/24

ii) Destino Pc c: 10.0.7.20/24

Saltos:

pc-b -> n7 -> router2 -> 0.0.0.0

router2 -> router1 -> 10.0.0.0 (Manda todo lo que no esté entre las otras, por defecto, a R1)

router1 -> router3 -> 10.0.7.0 (10.0.0.0 /16🡪 Manda todo lo que vaya para esa)

router3 -> n6 -> pc-c

Resultado: Llegó a su destino

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

i) Origen: 10.0.7.20/24

ii) Destino: 10.0.5.20/24

Saltos:

pc-c -> n6 -> router3 -> 0.0.0.0

router3 -> router4 -> 10.0.0.0 (Manda todo lo que no esté entre las otras, por defecto, a R4)

router4 -> router2 -> 10.0.5.0 (Manda todo lo que no esté entre las otras, por defecto, a R2)

router2 -> n7 -> pc-b (10.0.5.0 a eth2)

Resultado: Llegó a su destino

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

i) Origen: 10.0.7.20/24

ii) Destino: 8.8.8.8

Saltos:

pc-c -> n6 -> router3 -> 0.0.0.0 (Manda todo lo que esta por defecto)

router3 -> router4 -> Se corta el camino (R4 no tiene el 0.0.0.0 para mandar lo que no vaya para redes definidas)

Resultado: ICMP Destination Network Unreachable

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

i) Origen: 10.0.5.20/24

ii) Destino: 8.8.8.8

Saltos:

pc-b -> n7 -> router2 -> 0.0.0.0

router2 -> router1 -> 0.0.0.0

router1 -> router2 -> 0.0.0.0

…

En bucle hasta que el TTL llega a 0

Resultado: ICMP Time Exceeded

**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?**

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

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

**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”?**

**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?**

**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.**

Es un mecanismo que permite convertir direcciones IPs, entonces los paquetes que se dirigían a una IP A ahora se dirigen a otra B, y viceversa. Suele usarse el número de puerto para convertir una misma IP A en distintas IPs B

En el servicio de Internet hogareño, el router tiene una IP pública, y para los dispositivos, cada interfaz tendrá una IP privada. Entonces, NAT permite que paquetes entrantes desde Internet (con destino, IP pública) sean redirigidos a los distintos dispositivos (con destino, IP privada); y viceversa

El router NAT se comporta de cara al exterior como un único dispositivo con una IP única. Todo el

tráfico que sale del router doméstico hacia Internet tiene una dirección IP de origen igual, y todo el tráfico que entra en él tienen que tener la misma dirección de destino única. En resumen, el router NAT oculta los detalles de la red doméstica al exterior.

*¿Dónde obtienen las computadoras de la red doméstica sus direcciones y dónde obtiene el router su dirección IP única?* ***DHCP****. El router obtiene su dirección del servidor DHCP del ISP (Internet Service Provider) y ejecuta un servidor DHCP para proporcionar direcciones a las computadoras, dentro del espacio de direcciones de la red doméstica controlada por el router NAT-DHCP.*

*Si todos los datagramas que llegan al router NAT procedentes de la WAN tienen la misma dirección IP de destino (específicamente, la de interfaz WAN del router NAT), entonces ¿Cómo sabe el router a qué host interno debería reenviar un datagrama dado? Utiliza una tabla de traducciones NAT almacenada en el router NAT que incluye los números de puerto, y las direcciones IP en las entradas de la tabla.*

Ejemplo:

Si un usuario de la red doméstica que utiliza el host con la dirección **10.0.0.1** solicita una página web almacenada en un servidor web (puerto 80) con la dirección IP 128.119.40.186. El host **10.0.0.1**, asigna el número de puerto de origen (arbitrario) **3345** y envía el datagrama a la LAN. El router NAT recibe el datagrama, genera un nuevo número de puerto de origen, **5001**, para el datagrama, sustituye la dirección IP de origen por su dirección IP de la red WAN **138.76.29.7**, y sustituye el número de puerto de origen original **3345** por el nuevo número de puerto de origen **5001**. Al generar un nuevo número de puerto de origen, el router NAT puede seleccionar cualquier número de puerto de origen que actualmente no se encuentre en la tabla de traducciones NAT.

Como la longitud del campo número de puerto es de 16 bits, el protocolo NAT puede dar soporte a 60.000 conexiones simultáneas. En el router, NAT tiene una entrada a su tabla de traducciones.

El servidor web, no consciente de que el datagrama entrante ha sido manipulado por el router NAT, responde con un datagrama cuya dirección de destino es la dirección IP del router NAT y cuyo número de puerto de destino es **5001**.

Cuando este datagrama llega al router NAT, éste indexa la tabla de traducciones NAT utilizando la dirección IP de destino (**138.76.29.7**) y el número de puerto de destino (**5001**) para obtener la dirección IP (10.0.0.1) y el número de puerto de destino (**3345**) apropiados para el navegador de la red doméstica.

**Tabla de traducciones NAT**

|  |  |
| --- | --- |
| Lado WAN | Lado LAN |
| **138.76.29.7**, **5001** | **10.0.0.1**,**3345** |

A continuación, el router reescribe la dirección de destino y el número de puerto de destino del datagrama y lo reenvía a la red doméstica.

**¿Para qué sirve?**

- Ahorrar direcciones IPv4 públicas.

- Transformar direcciones privadas en públicas. De esta forma es posible conectar un host de una red privada con otro host de otra red privada (a través del router NAT).

- Se puede utilizar el router como intermediario (da una sensación de “seguridad”, aunque no siempre es verdad)

**De la teoría:**

NAT es una solución al problema de IPV4 de tener casi agotado el espacio de direcciones.

Este permite la traslación de direcciones de un espacio privado (no “enrutable” en Internet) a un espacio público.

Problemas con IP Privadas: No son únicas, por lo tanto:

* Las rutas pueden ser confundidas.
* Habitualmente son filtradas por routers de borde.
* Algunos protocolos no funcionan adecuadamente, FTP, VoIP, etc.

Procesos de Traslación

* Se realizan sobre redes stubs (solo una salida).
* Se deben mantener tablas de traslaciones.
* Varias formas de realizarlo:
* NAT (Network Address Translation):
  + Estático.
  + Dinámico.
* NAPT (Network Address Port Translation):
  + Dinámico sobre pool.
  + Dinámico sobre dir. overload/masquerade.
* Modificación de direcciones, ports, checksums.

Una forma de realizarlo es: “one-to-one” (uno a uno), NAT básico:

* Se mapea una dirección IPv4 privada a una dirección IPv4 pública.
* Si se hace de forma estática requiere tantas direcciones públicas como privadas.
* Permite acceso en ambas direcciones.
* Si se hace de forma dinámica no es necesario, pero sí se requiere un timer por cada entrada. Limita

acceso simultaneo de acuerdo al pool pub

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

Define las direcciones privadas. Estas no tienen significado global ni son únicas. Se utilizan en Intranets, es decir, redes autónomas sin conexión a Internet. Para conectarse a Internet requieren un proceso de transformación NAT, RFC-1631. Sin este podría pasar que salgan a internet, lo que no debe suceder, sino que deben ser filtradas por routers de borde.

Determina que bloques de IP privadas le corresponde a cada clase de red. La Autoridad de Números Asignados en Internet (IANA), ha reservado los siguientes bloques de direcciones IP para el uso en internets privadas:

* 10.0.0.0/8 – 10.255.255.255, 1 Clase A. (prefijo 10/8)
* 172.16.0.0 – 172.31.255.255, 16 Clases B. (prefijo 172.16/12)
* 192.168.0.0 – 192.168.255.255, 256 Clase C (prefijo 192.168/16)

Se relaciona con NAT, porque este, permite la traslación entre direcciones IP privadas a públicas. Permitiendo esto, conectar (de forma indirecta, a través de routers NAT) hosts de redes privadas o públicas con hosts de otras redes privadas o públicas.

Además de reutilizar IPs públicas partiendo de direcciones IP privadas.

**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?**

curl "https://api.ipify.org?format=json"

{"ip": "163.10.0.135"}

ip -4 addr show enp1s0 | grep -oP "(?<=inet\s)\d+(\.\d+){3}/\d+"

192.168.122.66/24

Las IPs son distintas entre sí porque la NAT del router convierte la IP privada en la pública y viceversa

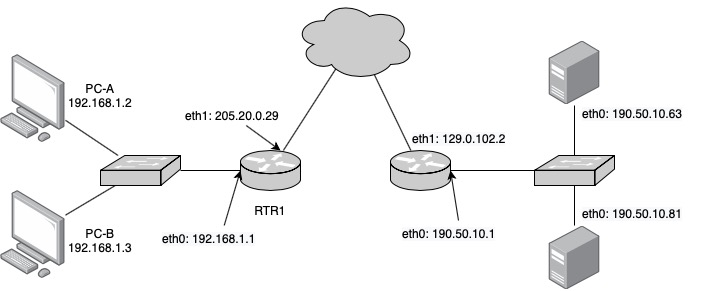
Accediendo a la página desde 2 dispositivos diferentes se muestra la misma IP, pero al revisar la IP con la PowerShell es diferente. Se debe a que al hacer la consulta a través de un router, se hace el proceso de NAT descrito en el punto 8.

Además, usando los datos móviles y el mismo dispositivo, el resultado es una IP distinta (186… y 45..) y al conectar la PC a través de la Red Móvil con datos móviles da la misma (186… y 186...) por lo que se intuye que la red móvil de un teléfono tiene la funcionalidad de un router.

**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.**

**\*Los numeros en color son los que había que completar\***



**PC-A (ss)**

**Local Address:Port Peer Address:Port**

192.168.1.2:49273 **190.50.10.63:80 De aca vas a buscar el que tiene 49273 en nat**

**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 **Este es, asi que vas a buscar en el serv el que . tiene 25192**

192.168.1.2:51238 **205.20.0.29:16345 Tiene que ser esta, por que no hay mas . . vacantes**

192.168.1.3:52734 205.20.0.29:51091 **Aca esta 52734, va a 51091**

192.168.1.2:37484 205.20.0.29:41823 **Aca esta, asi que es la del costado**

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 **y es este, asi que peer adress es la de aca**

190.50.10.63:25 205.20.0.29:41823 **Aca esta el :25, asi que se busca el 42823**

**SRV-B (ss)**

**Local Address:Port Peer Address:Port**

190.50.10.81:8080 205.20.0.29:16345 **el 8080 esta aca, asi que se busca el 16345**

190.50.10.81:8081 205.20.0.29:51091 **Asi que va esta**

190.50.10.81:8080 205.20.0.29:9123 Este se descarta para el 3) por el inicio de la ip en la otra tabla

**b. En base a lo anterior, responda:**

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

Hay 5 conexiones hechas:

(1) Entre 192.168.1.2:49273 y 190.50.10.63:80 (Serv 1-PcA)

(2) Entre 192.168.1.2:37484 y 190.50.10.63:25 (Serv 1-PcA)

(3) Entre 192.168.1.2:51238 y 190.50.10.81:8080 (Serv 2-PcA)

(4) Entre 192.168.1.3:52734 y 190.50.10.81:8081 (Serv 2-PcB)

(5) Entre 192.168.1.3:39275 y 190.50.10.81:8080 (Serv 2-PcB)

**ii. ¿Quién inició cada una de las conexiones?**

Las conexiones fueron iniciadas por los clientes, hacia los servidores

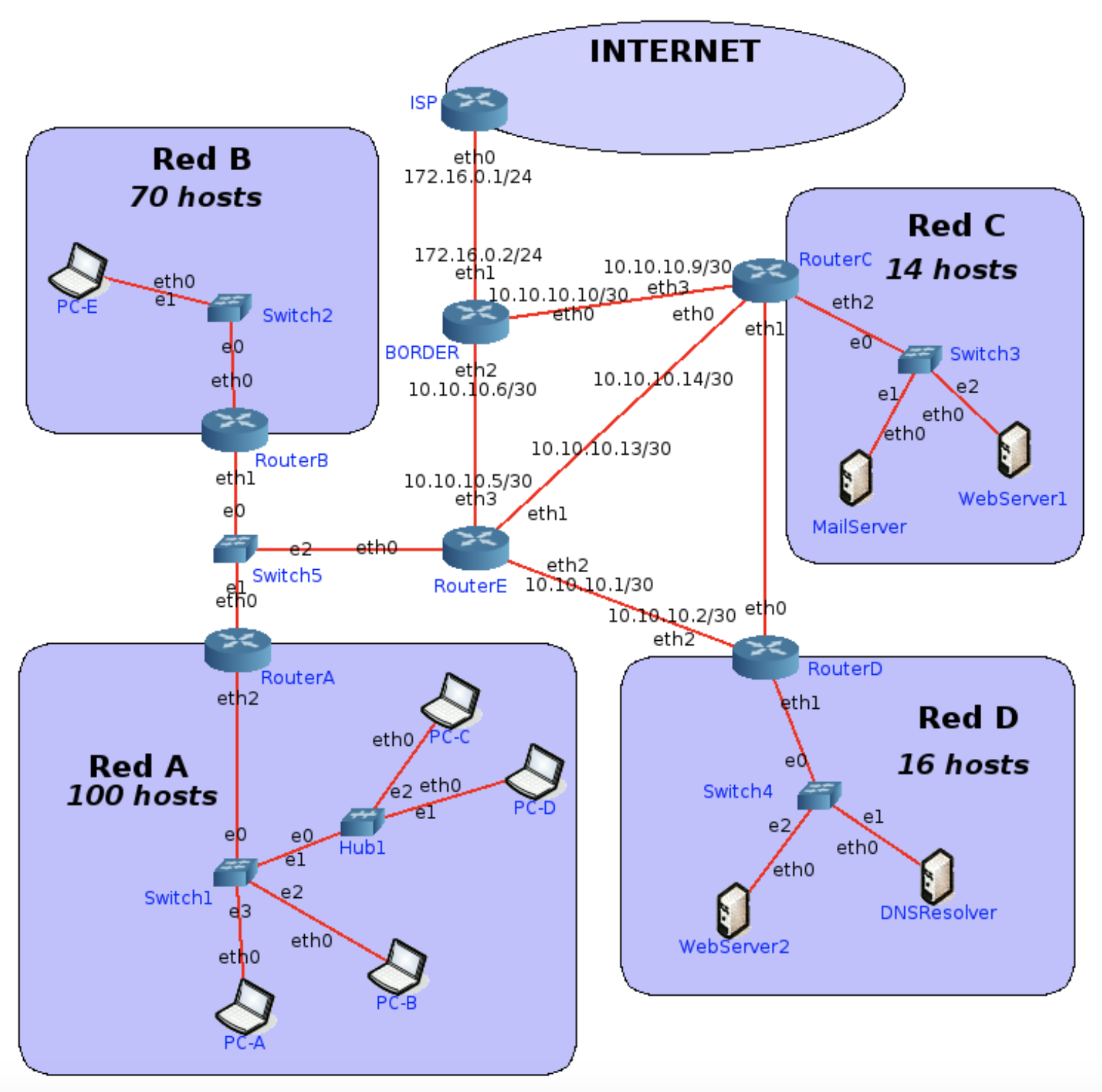
**¿Podrían haberse iniciado en sentido inverso? ¿Porqué?**

No se podrían haber iniciado en orden inverso, porque la tabla de NAT no tendría las entradas necesarias que permitirían este inicio de conexión

**Investigue qué es port forwarding y si serviría como solución en este caso.**

El port forwarding lo solucionaría, ya que permite abrir puertos del router para que los paquetes que llegan a este puerto, sean redirigidos a ciertas direcciones IP privadas (los clientes, en este caso)

**Ejercicio de repaso**



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

**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.**

**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.**

**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.**

**Aclaración importante**

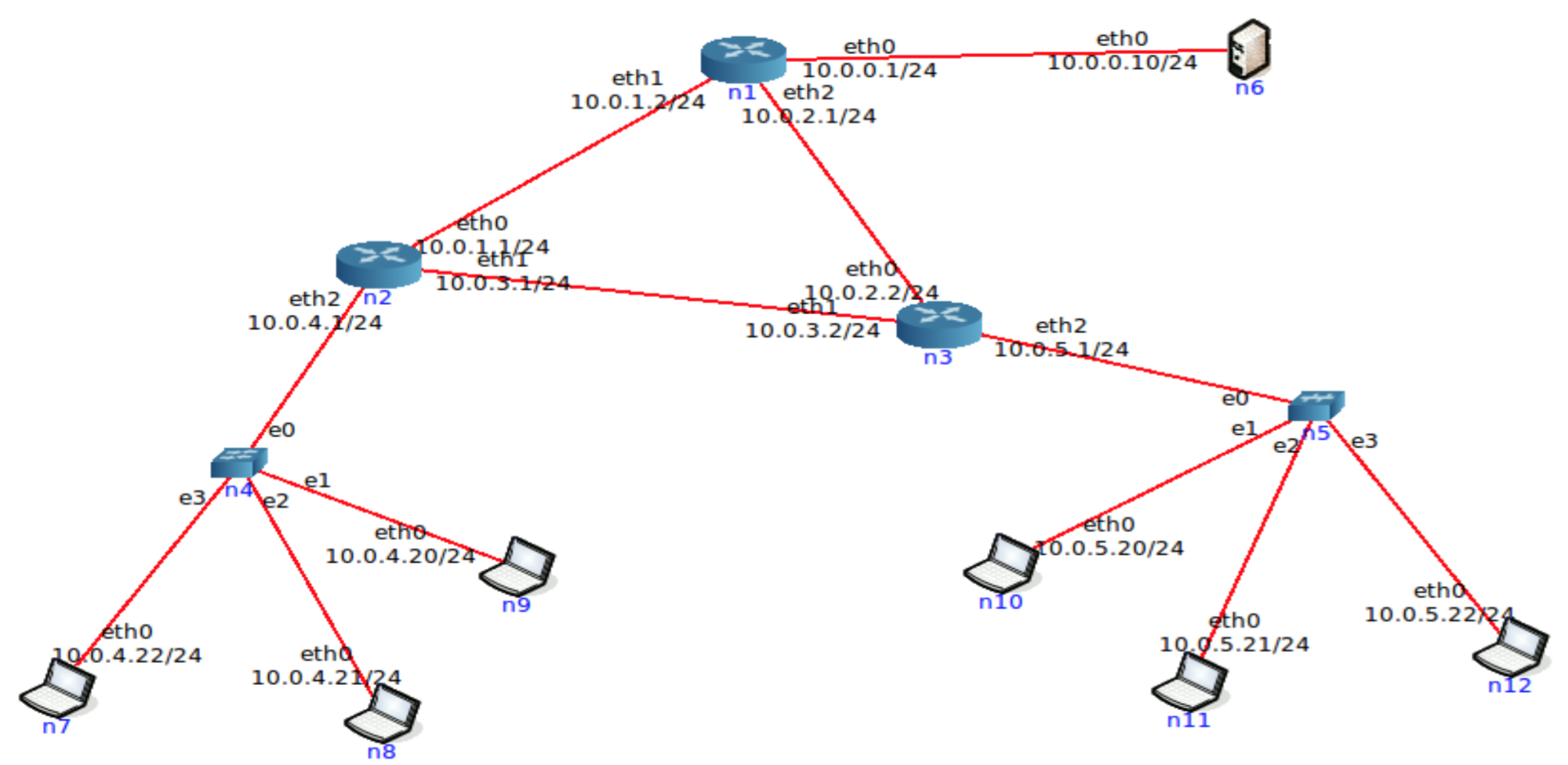
**En CORE no se guardan los cambios realizados en una topología al detenerla. Por ello, es deseable**

**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.**

**16. 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 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.**

**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 hizo 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.**

**ñ. 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 la 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?**