Práctica 3 - Capa de Red (II): VLSM, IPv6 y fragmentación

revisión: 2.0

Nota: a partir de esta práctica, y en las siguientes, se irán incorporando ejercicios que compondrán el trabajo final. En las prácticas que se agreguen estos ejercicios se indicará que pertenecen al trabajo final. Los puntos indicados como Alternativos servirán para mejorar la nota pero no son necesarios para aprobar. El trabajo se deberá entregar todo junto en una fecha a determinar para lo cual se creará una tarea en la que podrán subirlo. En caso de no aprobarlo tendrán una re-entrega. Además habrá un coloquio para defenderlo que se realizará en los horarios de práctica

1) Aplicando VLSM, resolver los siguientes ejercicios:

    a) Dada la red IP 65.0.0.0/24 se necesitan definir:
        - 1 (una) red de 80 hosts
        - 2 (dos) redes de 10 hosts.
        - 1 (una) red de 40 hosts.

    b) Dada la red IP 100.0.0.0/16 se necesitan definir:
        - 2 (dos) redes de 2000 hosts
        - 2 (dos) redes de 500 hosts.
        - 20 (veinte) redes de 300 hosts.
        - 50 (cincuenta) redes de 200 hosts.
        - Una red de backbone para unir cada uno de los router de las redes anteriores (74 direcciones).

2) Resolver el ejercicio 1b) teniendo en cuenta una capacidad de crecimiento del 20 % para cada subred sin considerar el backbone

3) Resolver los ejercicios 1a) y 1b) con la red IPv6: 2001:db8:1111::/48

4) IPv6: Dada la topología de la figura 1 cargar en la herramienta de simulación el archivo:
    - **`ipv6-base2.imn`**

    a) Completar las direcciones (usando la primera dirección libre de la red) y las tablas de ruteo para que exista comunicación de extremo a extremo. Por ejemplo agregar las rutas de forma manual con comandos como:

```
n2# ip -f inet6 route add default via 2001:db8::128
```

O habilitar el servicio de default gw de la GUI.

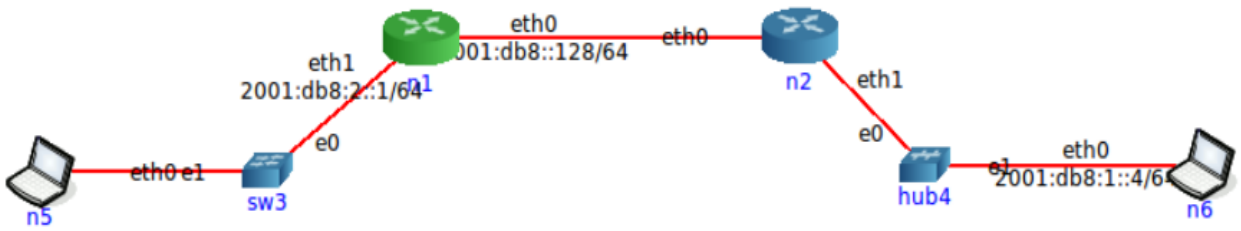

Figura 1: Topología IPv6

b) ¿Cómo quedará la tabla de ruteo del nodo n1 y del nodo n5? ¿Dónde se debe habilitar el forwarding IPv6? ¿Es necesario habilitar el de IPv4?

c) Indicar cuál será la dirección de link-local para el nodo n5.

d) Si se realiza un ping6 desde n5 a n6, el mismo tiene éxito:

```
n5# ping6 -c 4 2001:db8:1::4
```

e) Observando la siguiente captura responder:

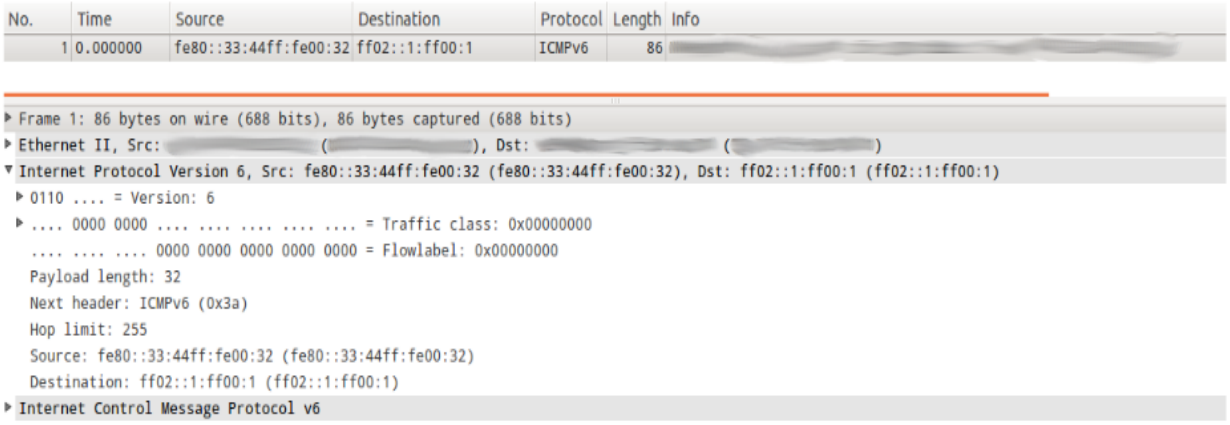

Figura 2: Captura IPv6

1) Indicar el mensaje de la captura de la figura 2 entre qué equipos “viaja”, completar qué tipo de mensaje ICMPv6 es y las direcciones MAC origen y destino sobre el cual se encapsula.

2) Indicar el tipo de mensaje ICMPv6 que deberá encontrarse a continuación en la captura y las direcciones IPv6 origen y destino que tendrá el mismo.

3) Completar la dirección MAC origen (valores marcados con “SS”) del código HEX del siguiente mensaje, indicar nodo origen y destino, indicar si el mismo es un Echo Request o Echo Reply.

```
SS SS SS SS SS SS 02 33 44 00 00 32 86 dd 60 00
00 00 00 40 3a 3f 20 01 0d b8 00 02 00 00 00 00
00 00 00 00 00 02 20 01 0d b8 00 01 00 00 00 00
00 00 00 00 00 04 80 00 f1 ca 00 1a 00 02 b4 8e
49 52 3c 3f 0d 00 08 09 0a 0b 0c 0d 0e 0f 10 11
12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21
22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31
32 33 34 35 36 37
```

4) Indicar cómo queda la tabla CAM de direcciones MAC del switch sw3 una vez que los mensajes ICMP atravesaron la red en ambos sentidos.

5) Completar la dirección IPv6 (marcada con “??”) del código HEX mostrado a partir de las direcciones MAC Ethernet del siguiente mensaje ICMPv6 Echo Reply encapsulado en Ethernet, Indicar en qué interfaz pudo ser capturado este mensaje.

```
02 33 22 00 00 20 00 34 c0 00 32 00 86 dd 60 00
00 00 00 40 3a 40 20 01 0d b8 00 01 00 00 00 00
00 00 00 00 00 04 ?? ?? ?? ?? ?? ?? ?? ?? ?? ??
?? ?? ?? ?? ?? ?? .. .. .. .. .. .. .. .. .. ..
```

6) Completar los bytes marcados como “??” del mensaje IPv6 anterior encapsulado en el siguiente link acorde va avanzando hasta llegar a destino. Indicar a qué campos pertenecen a la trama Ethernet y del datagrama IPv6.

```
?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? 86 dd 60 00
00 00 00 40 3a ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??
?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??
?? ?? ?? ?? ?? ?? .. .. .. .. .. .. .. .. .. ..
```

e) ¿Cómo se podría evitar la configuración manual de los nodos n5 y n6? Realice la configuración en el simulador e indique qué direcciones IPv6 se asignan.

5) Fragmentación: se deben enviar un datagrama IPv4 de 1100B con un encabezado sin opciones a través de un link que soporta solo datagramas de 200B. Determine el offset y los bits de fragmentación de cada datagrama. Calcule el overhead sobre una solución con MTU = 1500. ¿Es necesario hacer padding a nivel Ethernet en el último fragmento?

6) Fragmentación: dada la configuración de la figura 3 donde entre n1 y n2 se tiene un MTU=1500 y entre n2 y n3 un MTU=400. Se asume que los frames de link layer requieren 18 bytes de overhead y los datagramas IPv4 20 bytes. Por 1000 bytes de datos que envía n1 a n3, ¿cuántos bytes en total, incluyendo el overhead, se van a transmitir entre n2 y n3.

   a) ¿Qué sucedería si los mensajes se envían con el bit de DF = 1?

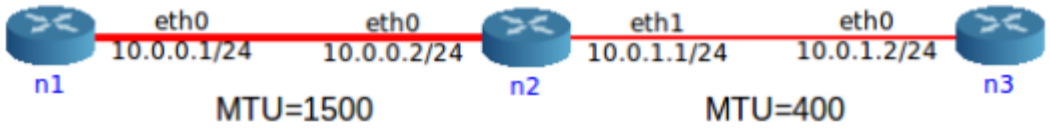

Figura 3: Diagrama de fragmentación

7) Fragmentación IPv6: dada la configuración de la figura 3 pero reemplazando IPv4 por IPv6 y considerando que los frames de link layer requieren 18 bytes de overhead y los datagramas IPv6 40 bytes, analizar los MTUs mínimos y responder:
   - ¿Cómo se resuelve la fragmentación en IPv6?
   - ¿Qué se debería cambiar para que funcione?

8) NAT/NATP: ¿Qué especifica el documento de la IETF RFC-1918 y cómo se relaciona con NAT/NATP?

9) NAT Tradicional. Dado el diagrama de la figura 4.

   a) Escoger un bloque IPv4 público para que el router donde está ubicado el cliente pueda hacer una traducción uno a uno en la cual todos los posibles “clientes” de la red “D” puedan tener acceso simultáneo a Internet.
   b) Seleccionar un bloque para que solo el 25 % pueda tener acceso simultáneo. ¿Cómo se resolvería para que los restantes puedan tener acceso?
   c) Indicar cómo quedaría la tabla de NAT del router si se hace traducción solo basada en IP cuando el cliente 192.168.0.30 quiere acceder al servidor web 150.0.0.1.
   d) Indicar el posible encabezado que tendría el datagrama que entra al router desde el cliente y cómo sería el encabezado del datagrama que sale del router. ¿Qué campos cambiaron?
   e) Indicar el encabezado posible del paquete IP de la respuesta enviada desde el servidor y qué modificaciones necesita para que llegue al cliente.
   f) ¿Cómo llegaría el datagrama si el router no tuviese activada la funcionalidad de NAT, habría respuesta?
   g) ¿Qué mecanismo sería necesario si no se contase con el bloque IPv4 público y solo se tuviese una única IP pública en el router?

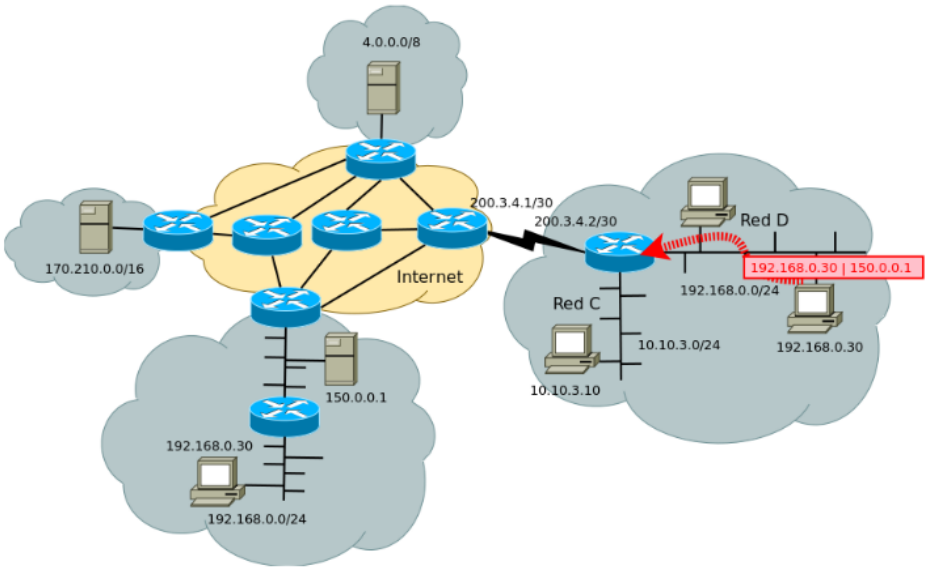

Figura 4: Diagrama de NAT

10) **Ejercicio para entregar en grupo y defender en coloquio.**

Resolver el direccionamiento IPv4 con el bloque IP asignado. Considerar los enlaces punto a punto salvo la red de n9, n10, n11, n13 y n14. Para la red de n9 considerar 40 hosts; para la red de n11 y n13, 328 hosts y para la red de n14, 500 hosts.

a) Configurar la red detrás de n5 (n5,n13,n11) y la Red C con el bloque IPv6 asignado.
b) Resolver con ruteo estático la topología.
c) Alternativo: Asignar a n10 una IP según RFC-1918 y configurar NAT en n1 para que pueda alcanzar al resto de los equipos.
d) Realizar test con ping (ICMP) y traceroute para probar que funciona la topología.
e) Capturar puntualmente el tráfico de n13 hacia n7 y analizar: ARP e ICMP.
f) Realizar un traceroute entre los mismos equipos, capturar los mensajes.
g) Alternativo: Modificar los MTU para ver la fragmentación.
h) Probar conectividad en las redes con IPv6 (por separado), capturar tráfico y analizar ICMPv6.

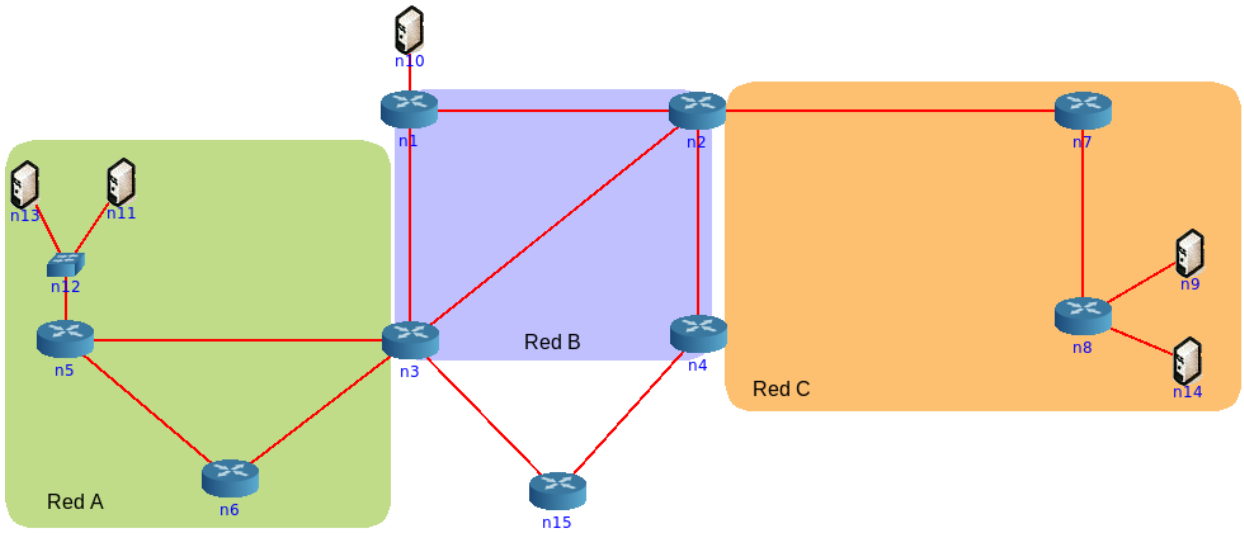

Figura 5: Diagrama de topología a entregar