Redes de Computadores II

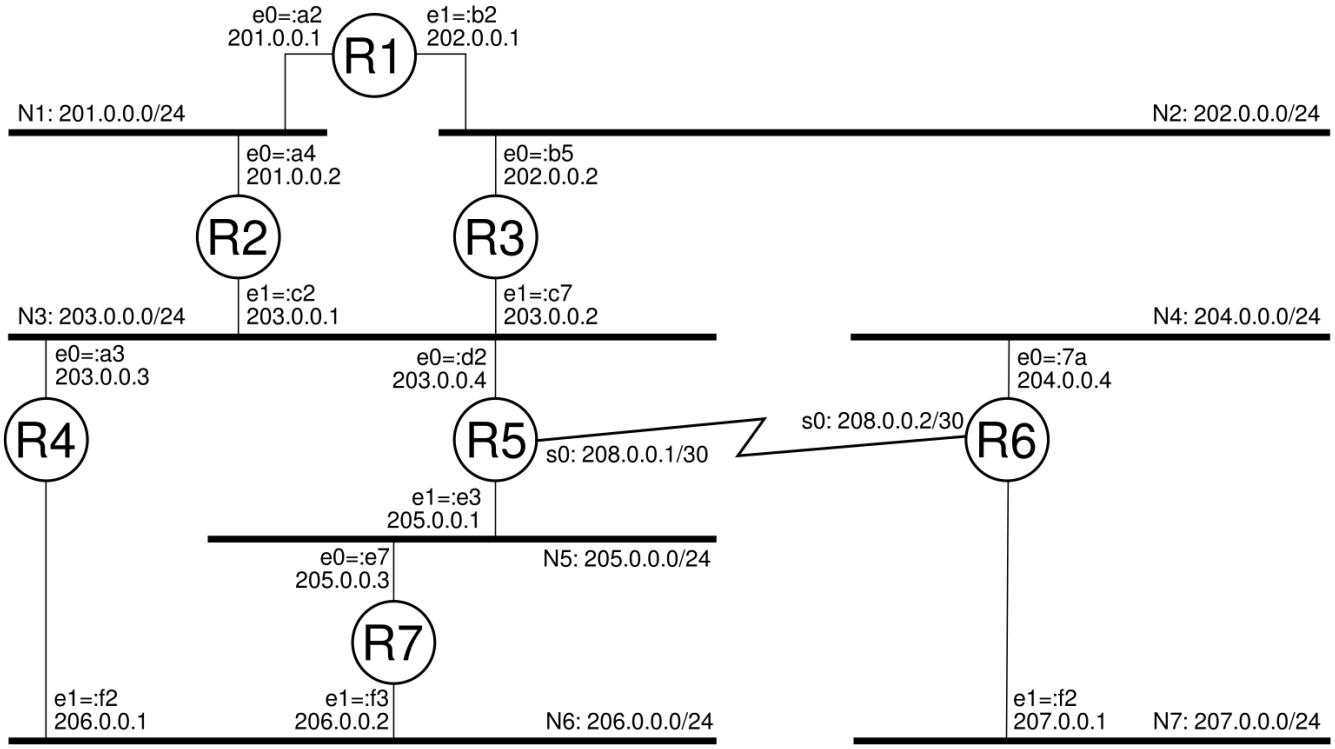
Curso 19/20 :: Prueba 2

Escuela Superior de Informática

2021/04/22 10:55:32

Este examen consta de 5 preguntas con un total de 40 puntos.

E. [8p] La siguiente topología muestra una inter-red formada por 7 routers y 7 LAN. En cada interfaz se muestra su IP y el último octeto de su MAC. Por generalidad, asuma que hay varios PCs con tablas de rutas correctas conectados a cada una de las redes.



R1

201.0.0.0/24	-	0.0.0.0 - e0
202.0.0.0/24	-	0.0.0.0 - e1
0.0.0.0	-	201.0.0.2 - e1

R2

201.0.0.0/24	-	0.0.0.0 - e0
202.0.0.0/24	-	201.0.0.1 - e0
203.0.0.0/24	-	0.0.0.0 - e1
0.0.0.0	-	203.0.0.4 - e1
206.0.0.0/24	-	203.0.0.3 - e1

R3

201.0.0.0/24	-	201.0.0.1 - e0
202.0.0.0/24	-	0.0.0.0 - e0
203.0.0.0/24	-	0.0.0.0 - e1
0.0.0.0	-	203.0.0.4 - e1
206.0.0.0/24	-	203.0.0.3 - e1

R4

201.0.0.0/24	-	203.0.0.1 - e0
202.0.0.0/24	-	203.0.0.2 - e1
203.0.0.0/24	-	0.0.0.0 - e0
205.0.0.0/24	-	206.0.0.2 - e1
206.0.0.0/24	-	206.0.0.2 - e1
0.0.0.0	-	203.0.0.4 - e0

R5

203.0.0.0/24	-	0.0.0.0 - e0
205.0.0.0/24	-	0.0.0.0 - e1
206.0.0.0/24	-	205.0.0.3 - e1
208.0.0.0/24	-	0.0.0.0 - s0
0.0.0.0	-	208.0.0.2 - s0
0.0.0.0	-	203.0.0.2 - e0

R6

204.0.0.0/24	-	0.0.0.0 - e1
207.0.0.0/24	-	0.0.0.0 - e0
208.0.0.0/24	-	0.0.0.0 - s0
0.0.0.0	-	208.0.0.2 - s0

R7

205.0.0.0/24	-	0.0.0.0 - e0
206.0.0.0/24	-	0.0.0.0 - e1
0.0.0.0	-	205.0.0.1 - e0

> **1** (4p) Sabiendo que se aplica una métrica de saltos y que el objetivo es proporcionar conectividad con coste mínimo entre todos los dispositivos (routers y PCs), identifique los errores o problemas que contienen las tablas de rutas mostradas.

- R1: Tercera fila: no se puede llegar a 201.0.0.2 por 'e1'.
- R2: La ruta óptima a N6 es a través de R4, no de R5.
- R3: Primera fila: R3 no es vecino de la red 201.0.0.0/24.
- R4: Quinta fila: R4 es vecino de N6, debe hacer entrega directa.
- R5: No puede haber 2 routers por defecto, la última se ignorará.
- R6: No está conectado a N4 por 'e1' ni a N7 por 'e0'.
- R6: Última fila. El siguiente salto no puede ser el propio router.

> **2** (4p) Ahora activamos RIP en todos los routers. Indique los vectores distancia que recibe R5 en la primera iteración, teniendo en cuenta que en RIP el coste a las redes vecinas es 1.

- R2: 201.0.0.0 metric 1, 203.0.0.0 metric 1.
- R3: 202.0.0.0 metric 1, 203.0.0.0 metric 1.
- R4: 203.0.0.0 metric 1, 206.0.0.0 metric 1.
- R6: 204.0.0.0 metric 1, 207.0.0.0 metric 1, 208.0.0.0 metric 1.
- R7: 205.0.0.0 metric 1, 206.0.0.0 metric 1.

E. [8p] Se dispone de una red privada compuesta por 5 hosts (A, B, C, D y E) con direcciones IP en el rango 10.100.200.5 a 10.100.200.9, respectivamente, y un router frontera que interconecta dicha red privada con Internet. El router frontera dispone de dos interfaces: una privada (dirección 10.100.200.2) y una pública (dirección 145.100.200.2) y ejecuta NAPT básico (no usa traducción a puertos sintéticos).

> **3** (1p) ¿Qué dirección IP y puerto origen aparecerá en cualquier paquete IP que se genera en la red privada y tiene como destino cualquier host en Internet, tras aplicar NAPT en el router frontera?

Un paquete IP con origen en la red privada (por tanto con dirección IP origen privada) y destino la red pública es modificado por el router NAT. Dicha modificación consiste en sustituir la dirección IP origen (privada) con la dirección IP pública del router, es decir 145.100.200.2. Dado que el router es NAPT (sin traducción a puertos sintéticos), el puerto origen no se modifica.

> **4** (2p) Indique los cambios que ocurren en la siguiente tabla de traducciones NAPT cuando los siguientes paquetes IP alcanzan el router frontera:

- Un paquete IP que contiene una petición HTTP con origen el host C (dir IP 10.100.200.7, puerto 2000) y destino el servidor web de Google con dirección IP 172.217.17.4 y puerto 80.
- Un paquete IP que contiene una petición HTTP con origen el host C (dir IP 10.100.200.7, puerto 3000) y destino el servidor web de Google con dirección IP 172.217.17.4 y puerto 80.
- Un paquete IP que contiene una petición HTTP con origen el host A (dir IP 10.100.200.5, puerto 2000) y destino el servidor web de Google con dirección IPno 172.217.17.4 y puerto 80.
- Un paquete IP que contiene una petición HTTP con origen el host A (dir IP 10.100.200.5, puerto 3000) y destino el servidor web de Google con dirección IP 172.217.17.4 y puerto 80.

```
Id Petición - IP Origen - Puerto Origen - IP Destino - Puerto Destino
1
2
3
4
```

Id Petición - IP Origen - Puerto Origen - IP Destino - Puerto Destino
1 - 10.100.200.7 - 2000 - 172.217.17.4 - 80
2 - 10.100.200.7 - 3000 - 172.217.17.4 - 80
3 - 10.100.200.5 - 2000 - 172.217.17.4 - 80
4 - 10.100.200.5 - 3000 - 172.217.17.4 - 80

> **5** (1p) La respuesta a la petición 1 alcanza ahora el router NAPT. Teniendo en cuenta la tabla anterior ¿A qué host privado se entregará dicho paquete?

El paquete con la respuesta tendrá dirección destino 145.100.200.2 y puerto destino 2000 y dirección origen 172.217.17.4, puerto origen 80. Cuando este paquete alcanza el router NAPT, éste busca en la tabla de traducciones una fila cuya dirección IP y puerto destino coincida con el origen de ese paquete. En este caso, las filas 1, 2, 3 y 4 coinciden. Para localizar la dirección IP privada que generó la petición, selecciona aquellas filas con puerto origen (2000) y de nuevo existen dos hosts que cumplen esta condición: los hosts 10.100.200.7 y 10.100.200.5. Existe por tanto ambigüedad y con la información disponible en la tabla no puede determinar a cuál de los dos hosts entregar la respuesta.

> **6** (2p) Suponga ahora que el router NAPT usa puertos sintéticos para evitar la ambigüedad. Complete de nuevo la tabla de traducciones cuando se producen las mismas operaciones especificadas en el apartado b).

```
Id Petición - IP Origen - Puerto Origen - Puerto Sintético - IP Destino - Puerto Destino
1
2
3
4
```

Id Petición - IP Origen - Puerto Origen - Puerto Sintético - IP Destino - Puerto Destino
1 - 10.100.200.7 - 2000 - 10000 - 172.217.17.4 - 80
2 - 10.100.200.7 - 3000 - 10001 - 172.217.17.4 - 80
3 - 10.100.200.5 - 2000 - 10002 - 172.217.17.4 - 80
4 - 10.100.200.5 - 3000 - 10003 - 172.217.17.4 - 80

> **7** (1p) Suponga ahora que la respuesta a la petición 1 alcanza el router NAPT. Teniendo en cuenta la tabla del apartado d) ¿A qué host privado se entregará dicho paquete y por qué?

El paquete con la respuesta tendrá dirección destino 145.100.200.2 y puerto destino 10000 y dirección origen 172.217.17.4, puerto origen 80. Cuando este paquete alcanza el router NAPT, éste busca en la tabla de traducciones una fila cuya dirección IP y puerto destino coincida con el origen de ese paquete. En este caso, las filas 1, 2, 3 y 4 coinciden. Para localizar la dirección IP privada que generó

E. [8p] Una compañía desea dividir el bloque de direcciones IP asignado 126.16.0.0/16 entre las distintas subredes que interconectan las sucursales de la compañía, de manera que el reparto se haga con el mínimo desperdicio posible de direcciones IP. La red está compuesta de la siguientes subredes:

- Subred A: incluye 1500 computadores en la sucursal A.
- Subred B: incluye 150 computadores de la sucursal B.
- Subred C: incluye 15 computadores en la sucursal C.
- Las subredes A, B, y C se conectan con el router frontera de la organización, R0, mediante los enrutadores RA, RB, y RC, respectivamente, a través de líneas serie dedicadas.

> **9** (1p) Indique qué dos estrategias para particionar bloques de direcciones IP conoce y describa la diferencia principal entre ambas.

- Subnetting: máscaras de longitud fija.
- VLSM: Máscaras de longitud variable. Adecuado cuando el número de direcciones IP que deben asignarse a cada subred no es homogéneo, se asigna el mínimo bloque de direcciones, por lo que se minimiza el desperdicio de direcciones dentro del bloque.

> **10** (6p) Complete la siguiente tabla utilizando VLSM (Variable Length Subnet Mask) para dividir el bloque de direcciones entre todas las subredes de esta compañía. Escriba el proceso completo para obtener la solución. Puede añadir tantas filas a la tabla como necesite.

```
Id subred - Dir. Red - Dir. Broadcast - Máscara - Num Dir Bloque - Num. Dir No asignadas
A
B
C
```

- Calculamos máscara para cada subred:
  - Subred A: 1500 hosts + 1 IP (RA) + Dir. Red + Dir. Broadcast = 1503 IPs. Se necesitan log2(1503) = 11 bits (2exp11=2048) para 1503 direcciones IP. Máscara de red: 32-11=21 bits.
  - Subred B: 150 hosts + 1 IP (RB) + Dir. Red + Dir. Broadcast = 153 IPs. Se necesitan log2(153) = 8 bits (2exp8=256) para 153 direcciones IP. Máscara de red: 32-8=24 bits.
  - Subred C: 15 hosts + 1 IP (RC) + Dir. Red + Dir. Broadcast = 18. Se necesitan log2(18) = 5 bits (2exp5=32) para 18 direcciones IP. Máscara de red: 32-5=27 bits.
  - Subred RA-R0: IP RA+IP R0 + Dir. Red + Dir. Broadcast = 4 IPs. Se necesitan log2(4) = 2 bits (2exp2=4) para 4 direcciones IP. Máscara de red: 32-2=30 bits.
  - Las subredes RB-R0 y RC-R0 se calculan igual que RA-R0.
- Fragmentar el bloque, comenzando desde la red más grande hasta la red más pequeña.
  - Subred A: 126.16.0.0/21

    01111110 00010000 00000000 00000000 126.16.0.0 (Dir. De Red)
    01111110 00010000 00000111 11111111 126.16.7.255 (Dir. De Broadcast)
  - Subred B: 126.16.8.0 /24

    01111110 00010000 00001000 00000000 126.16.8.0 (Dir. De Red)
    01111110 00010000 00001000 11111111 126.16.8.255 (Dir. De Broadcast)
  - Subred C: 126.16.9.0/27

    01111110 00010000 00001001 00000000 126.16.9.0 (Dir. De Red)
    01111110 00010000 00001001 00011111 126.16.9.31 (Dir. De Broadcast)
  - Subred RA-R0: 126.16.9.32/30

    01111110 00010000 00001001 00100000 126.16.9.32 (Dir. De Red)
    01111110 00010000 00001001 00100011 126.16.9.35 (Dir. De Broadcast)
  - Subred RB-R0: 126.16.19.36/30

    01111110 00010000 00001001 00100100 126.16.9.36 (Dir. De Red)
    01111110 00010000 00001001 00100111 126.16.9.39 (Dir. De Broadcast)
  - Subred RC-R0: 126.16.19.40/30

    01111110 00010000 00001001 00101000 126.16.9.40 (Dir. De Red)
    01111110 00010000 00001001 00101011 126.16.9.43 (Dir. De Broadcast)

La tabla sería la siguiente:

Id subred - Dir. Red - Dir. Broadcast - Máscara - Num Dir Bloque - Num. Dir No asignadas

A - 126.16.0.0 - 126.16.7.255 - /21 - 2048 - 545

B - 126.16.8.0 - 126.16.8.255 - /24 - 256 - 103

C - 126.16.9.0 - 126.16.9.31 - /27 - 32 - 14

RA-R0 - 126.16.9.32 - 126.16.9.35 - /30 - 4 - 0

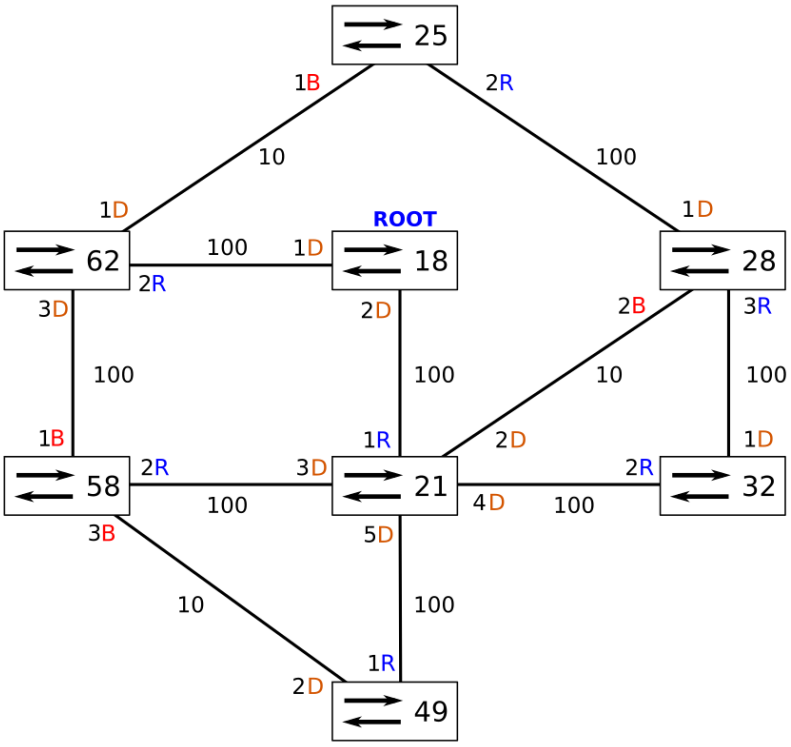
RB-R0 - 126.16.9.36 - 126.16.9.39 - /30 - 4 - 0

RC-R0 - 126.16.9.40 - 126.16.9.43 - /30 - 4 - 0

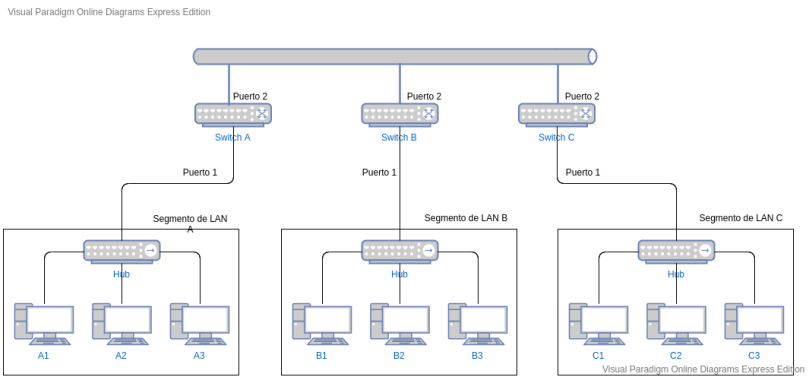
> **11** (1p) Teniendo en cuenta los resultados que ha proporcionado en la tabla del apartado anterior, ¿qué bloque de direcciones tiene el mayor porcentaje de direcciones no asignadas?

12 [8p] Considere la siguiente topología formada por 8 switchs Ethernet y 11 segmentos LAN en los que se muestra su **VELOCIDAD** expresada en Mbps. Utilice los números indicados en cada switch como identificadores canónicos.

Indique cuál es el switch raiz y todos los puertos raiz, designados y bloqueados. Es esencial explicar razonadamente el motivo de cada elección. Utilice el formato «switch.puerto» para referirse a los puertos, por ejemplo, «34.2» significaría «puerto 2 del switch con identificador 34».



E. [8p] Una red troncal interconecta tres plantas A, B y C de un edificio utilizando tecnología de conmutación (switching). En cada planta A, B y C, cada segmento de LAN se conecta mediante un switch A, B, y C, respectivamente, con 64 interfaces Ethernet cada uno, donde la interfaz con mayor ancho de banda se utiliza para cablear con el bus de la red troncal, y el resto de interfaces se utilizan para conectar estaciones de trabajo mediante un hub. La siguiente figura muestra la topología de la LAN de esta compañía.



> **13** (2p) ¿Cuántos dominios de colisión y cuántos dominios de broadcast existen en esta LAN?

Se observan tres dominios de colisión distintos, cada uno corresponde a un segmento de la LAN. Dado que en cada segmento existe un hub (dispositivo de interconexión en el nivel físico) que concentra los distintos equipos (permite por tanto compartir el medio físico) el dominio de colisión lo forman todos los equipos que conecta cada hub. Las colisiones ocurren cuando dos o más estaciones en un dominio de colisión transmiten datos sobre el medio físico al mismo tiempo, dado que la señal transportada no puede ser entendida por el receptor.

Se observa un único dominio de broadcast, correspondiente a la LAN de la compañía. Cualquier trama con dirección MAC origen cualquier estación de la LAN y dirección destino broadcast (FF:FF:FF:FF:FF:FF) deberá ser entregada a todas y cada una de las estaciones de la LAN.

> **14** (2p) Complete la tabla de direcciones MAC del switch A cuando ocurre el siguiente movimiento de tramas (asuma que la tabla está inicialmente vacía):

- Una trama con la dirección MAC origen de A1 y dirección MAC destino la de A2.
- Una trama con la dirección MAC origen de A2 y dirección MAC destino la de C3.
- Una trama con la dirección MAC origen de A2 y dirección MAC destino FF:FF:FF:FF:FF:FF.
- Una trama con la dirección MAC origen de A1 y dirección MAC destino la de A2.
- Una trama con la dirección MAC origen de B1 y dirección MAC destino la de A1.

```
Id Operación - Dirección Mac - Puerto - Timestamp - Operación switch
1
2
3
4
5
```

Id Operación - Dirección Mac - Puerto - Timestamp - Operación switch
1 A1 1 t1 Flooding
2 A2 1 t2 Flooding
3 A2 1 t3 Flooding
4 A1 1 t4 Descartar
5 B1 2 t5 Reenviar

> **15** (1p) Debido a que esta compañía tiene trabajadores asignados a tres grupos de trabajo distintos (investigación I, desarrollo D y RRHH RH), decide ahora organizar cada segmento de LAN (A, B y C) en 3 grupos de trabajo: I, D, RH. Se sabe que en cada segmento trabajan los siguientes usuarios:

- Segmento A: 35 trabajadores en el grupo I, 15 en el grupo D, y 2 en el grupo RH.
- Segmento B: 50 trabajadores en el grupo D y 2 trabajadores en el grupo RH.
- Segmento C: 50 trabajadores en el grupo D, 10 trabajadores en el grupo I.

El objetivo es aislar el tráfico de datos generado en cada grupo del resto de grupos. Para ello, se plantea dos alternativas:

- 1. Dividir cada segmento en los grupos de trabajo necesarios (sin soporte VLAN).
- 2. Utilizar VLAN para dividir cada segmento en los grupos de trabajo necesarios.

¿Cuál es el mínimo equipamiento que deberá añadir esta compañía para implementar la alternativa 1 y cuál sería la configuración de LAN resultante? Describa la red de manera clara y concisa (si lo desea, puede aportar una figura).