

# REDES DE ORDENADORES

Convocatoria de Junio 2003

## SOLUCIONES

**Nomenclatura:** En todas las cuestiones la dirección IP de un router llamado RX configurada en su interfaz número 'y' lo indicaremos con "IPRX,y" y la dirección MAC de ese interfaz, caso de ser Ethernet, con "MACRX,y".

**Notas:** En todos los ejercicios comente todas las hipótesis que tenga que añadir para responder a las cuestiones. Se permiten libros y apuntes.

**Duración:** 3 horas

1) ¿Qué tamaño tiene una trama Ethernet que contenga un paquete ARP? ¿Por qué? (0.5 pts)

En un paquete ARP que pregunte (o responda) por la dirección MAC que corresponde al interfaz que tiene configurada una determinada IP el tamaño del paquete ARP es de 28 bytes. Como no alcanza el tamaño mínimo de datos que debe transportar una trama Ethernet (ni Ethernet II no 802) el tamaño de la trama será el mínimo, 64 bytes, donde se incluye padding en los datos hasta alcanzar este tamaño mínimo.

2) ¿Qué dos problemas se querían resolver con CIDR? ¿Cómo? (0.5 pts)

a) Agotamiento de direcciones. El espacio de direcciones de IPv4 se estaba agotando. Ahora se permite hacer asignaciones de redes más ajustadas a las necesidades.

b) El crecimiento de las tablas de rutas en los routers. Ahora se pueden agregar (summarize) varias rutas en una sola.

3) ¿Se podría emplear RIP como protocolo EGP? ¿Por qué? (0.75)

RIP no sería una buena elección como protocolo EGP (entre ASs). Entre los problemas se cuenta que emplea como métrica el número de saltos, con un valor máximo de 16, esto hace que no se pueda utilizar en redes grandes y por otro lado no tiene forma de identificar a los ASs. RIP versión 2 sí puede enviar el identificador del AS pero sigue teniendo el problema de la métrica por lo que ninguno de ellos sería un buen protocolo EGP.

4) ¿Qué diferencia principal hay entre un protocolo de enrutamiento 'classful' y uno 'classless'? (0.5 pts)

En un protocolo de enrutamiento classful no se transporta en cada ruta la máscara que corresponde a esa red destino mientras que en uno classless sí.

5) ¿Qué ventajas tiene que el campo de tamaño variable (opciones) de la cabecera IP se encuentre al final de la misma? (0.5 pts)

Permite acceder con facilidad a los campos principales de la cabecera que se encuentran siempre en la

misma posición. Esto hace la implementación del protocolo más sencilla.

- 6) ¿Es posible recibir y procesar en un ordenador a la vez paquetes de dos protocolos de transporte distintos como TCP y UDP? ¿Por qué? (0.5 ptos)

Sí, se diferencia entre uno y otro mediante el campo 'protocolo' de la cabecera IP.

- 7) ¿Qué hace UDP cuando se pierde uno de sus datagramas? (0.5 ptos)

Nada en especial. No hace retransmisiones ni nada por el estilo. Ofrece un servicio de datagramas.

- 8) ¿Qué sucede si al calcular una ruta el algoritmo de Dijkstra para OSPF se encuentra con un coste del camino mayor que 16? (0.5 ptos)

Nada en especial, no está limitado a ese valor de métrica como le sucedía a RIP. En OSPF el coste de un camino puede ser de al menos 65535 sin que eso cause problemas.

- 9) A continuación se muestran los primeros paquetes de una conexión TCP recogidos con el programa `tcpdump`. Supongamos que, después del último paquete que se muestra, cada máquina quiere enviar datos al otro extremo. ¿Cuántos bytes podría enviar cada uno antes de recibir alguna confirmación? ¿Por qué? (1 pto)

```
3878322170.739651 172.17.40.2.20 > 1.1.1.253.3783: S 0:0(0) win 2 <mss 1460>
3878322170.739651 1.1.1.253.3783 > 172.17.40.2.20: S 0:0(0) ack 1 win 32120 <mss 1460>
3878322170.745627 172.17.40.2.20 > 1.1.1.253.3783: . ack 1 win 31744
3878322170.776003 172.17.40.2.20 > 1.1.1.253.3783: . 1:1461(1460) ack 1 win 31744
3878322170.776003 172.17.40.2.20 > 1.1.1.253.3783: . 1461:2921(1460) ack 1 win 31744
3878322170.796445 1.1.1.253.3783 > 172.17.40.2.20: . ack 1461 win 30660
```

La máquina 172.17.40.2 ha comenzado enviando 2 paquetes llenos (con el MSS en datos) por lo que parece que comienza con  $cwnd=2$ . A continuación ha recibido una confirmación, así que por slow start la ventana habrá subido en 1 a  $cwnd=3$ . Como la ventana anunciada por el otro extremo es mucho mayor este extremo podrá enviar como mucho 3 segmentos llenos. Uno de ellos ya está enviado porque el ACK solo ha confirmado el primero, así que puede enviar  $2 \times MSS=2920$  bytes.

La máquina 1.1.1.253 puede que haya comenzado con  $cwnd=1$  o  $cwnd=2$ , depende de la implementación esos son los valores más típicos y no lo podemos saber con esta traza porque no ha enviado datos. Tampoco ha recibido nuevas confirmaciones así que la ventana continúa con ese valor inicial. Esto quiere decir que cuando quiera enviar datos (la ventana anunciada por el otro extremo es muy grande) podrá enviar según cuál sea el caso bien  $MSS=1460$  bytes o  $2 \times MSS=2920$  bytes.

- 10) En la figura 1 se muestra la red interna de una compañía. Emplea direccionamiento privado y no está conectada a Internet.

Las direcciones IP de los interfaces de los routers son:

```
IPR1,0=10.8.0.1, IPR1,1=10.0.0.2
IPR2,0=10.0.4.17, IPR2,1=10.0.4.1
IPR3,0=10.0.0.1, IPR3,1=10.0.4.16, IPR3,2=10.0.0.5
IPR4,0=10.0.0.6, IPR4,1=10.0.2.1
```

Las direcciones IP de los Hosts representados en la figura son:

IPH1=10.8.0.14, IPH2=10.0.4.20, IPH3=10.0.4.4, IPH4=10.0.2.23

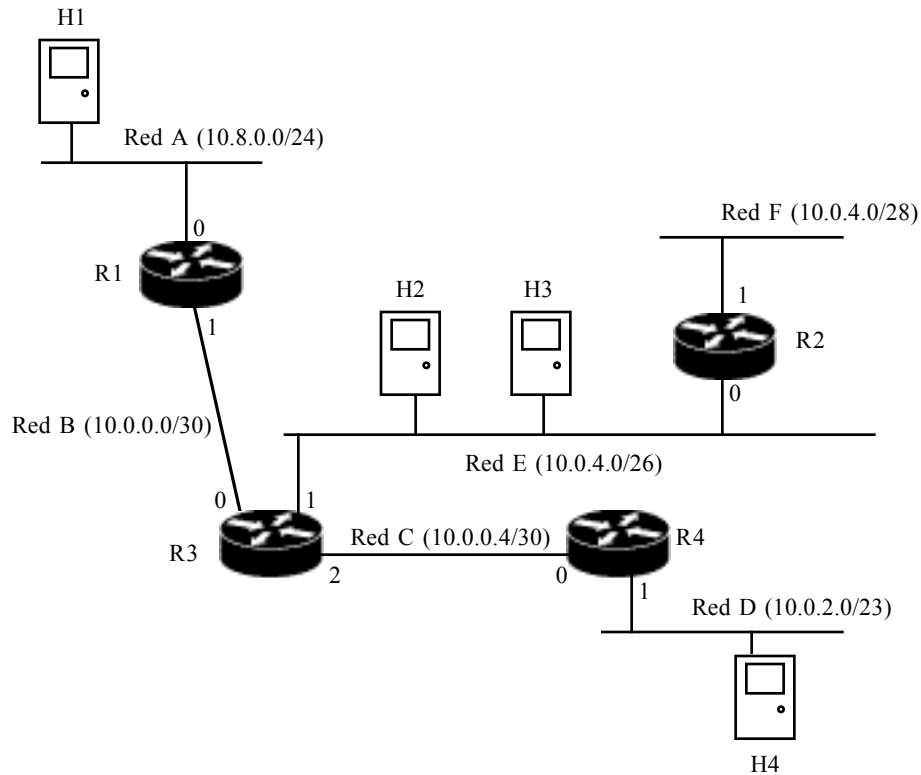


Figura 1.- Red para el problema 10

Los routers por defecto configurados son:

- Para los hosts en la Red A: 10.8.0.1
- Para los hosts en la Red D: 10.0.2.1
- Para los hosts en la Red E: 10.0.4.16
- Para los hosts en la Red F: 10.0.4.1

Además el router R2 hace de Proxy ARP para todas las máquinas de la Red F, es decir, hace que parezca que están en la Red E.

Finalmente las tablas de rutas que se configuran estáticamente en los diferentes routers son:

Router R1			Router R3		
Red destino	Next hop	Interface	Red destino	Next hop	Interface
10.8.0.0/24	-	0	10.0.0.0/30	-	0
10.0.0.0/30	-	1	10.0.4.0/26	-	1
0.0.0.0/0	10.0.0.1	1	10.0.0.4/30	-	2
			10.0.2.0/23	10.0.0.6	2
			10.8.0.0/24	10.0.0.2	0

Router R2			Router R4		
Red destino	Next hop	Interface	Red destino	Next hop	Interface
10.0.4.0/28	-	1	10.0.2.0/23	-	1
10.0.4.0/26	-	0	10.0.0.4/30	-	0

0.0.0.0/0 10.0.4.16 0 10.0.0.0/16 10.0.0.5 0

Responda a las siguientes preguntas:

- a) ¿Cuántas direcciones IP hay libres para hosts en la red A? ¿Y en la red B? ¿Cuántas direcciones IP quedan libres si sumamos las de todas las redes? (No cuente las que emplean los routers o los host que aparecen en la figura) (0.75 pts)

Quitando siempre la dirección de la red y la de Broadcast: Red A= $252=2^8 - 1$ (dirección de red) -  $1$ (dirección de broadcast) -  $1$ (dirección de H1) -  $1$ (dirección del interfaz de R1), Red B= $0=2^2 - 1$ (dirección de red) -  $1$ (dirección de broadcast) -  $2$ (direcciones de R1 y R3), Red C= $0$ , Red D= $508=2^9 - 2$ (dirección de red y broadcast) -  $2$ (dirección de H4 y R4), Red E= $56=2^6 - 1$ (identificador de la Red E y de la F que son el mismo) -  $1$ (dirección de broadcast de la Red E) -  $1$ (dirección de broadcast de la Red F) -  $2$ (direcciones de los hosts) -  $1$ (dirección del interfaz del router R3) -  $2$ (direcciones de los interfaces del router R2)

Total= $252+508+56=816$

- b) El host H1 envía un paquete ICMP de tipo Echo Request (un ping) a la dirección IP del host H2 con TTL=2. En respuesta se recibe un paquete IP. Especifique cuál será el valor de los siguientes campos de la cabecera IP de este paquete: protocolo, dirección IP origen y dirección IP destino. (0.5 pts)

Protocolo=1, dirección IP origen=10.0.0.1, dirección IP destino=10.8.0.14

El router R3 lo está descartando por TTL agotado y envía un error ICMP de tiempo excedido en tránsito.

- c) El usuario de la máquina H1 se queja de que intenta usar el programa ping contra el host H4 y parece no funcionar. Sin embargo, al administrador le funciona hacer ping desde H1 a R1, de R1 a R3, de R3 a R4 y de R4 a H4. ¿Es esto posible? ¿Por qué? (0.75 pts)

El router R4 no tiene una ruta para ir a la red 10.8.0.0/24 con lo que cuando tenga que reenviar el paquete ICMP Echo Response no sabrá cómo hacerlo y lo descartará. En los casos que prueba el administrador nunca hace que el router R4 tenga que reenviar un paquete a la Red A, los casos que se prueban sí tienen entradas correctas en las tablas de rutas.

- d) El usuario de la máquina H1 se queja también de que su comunicación con la máquina H3 a veces funciona y a veces no. Se prueba a hacer un ping de H1 a H3 y al primer ICMP se recibe la respuesta correctamente pero a los siguientes ya no. Si se deja de hacer tráfico con esa máquina durante un tiempo y se vuelve a intentar sucede lo mismo, el primer paquete ICMP llega (porque recibimos la respuesta) pero no recibimos respuesta a los demás. ¿Qué puede estar sucediendo? (0.75 pts)

El host H2 tiene una dirección que pertenece tanto a la red E como a la red F, así que cuando el router R3 envía ARP a la red E buscando esa IP contesta el host H3 pero también el router R2 que cree que ese host está en la red F y es su responsabilidad hacerle de proxy ARP. H2 está más cerca en retardo de R3 así que hay más posibilidades (no es seguro) de que su respuesta de ARP

llegue primero y así recibirá el primer paquete del ping y lo contesta bien pero a R3 le llega después la respuesta al ARP enviada por R2 con lo que cambia la MAC de la cache y envía todos los demás paquetes a R2 hasta que caduca la entrada de la cache. R2 hará ARP en la red F pero no hay un host con esa IP luego probablemente devuelva un ICMP de error por host destino inalcanzable.

- 11) Supongamos la red de la figura 2. En ella se emplea un protocolo de enrutamiento de vector distancia (distance vector). Se difunden las tablas de rutas tan solo periódicamente. Todos los routers emplean el mismo periodo, de  $T_{out}=30$  segundos, pero pueden no estar sincronizados. Una ruta que no se ha refrescado durante  $T_{delete}=180$  segundos se marca como inalcanzable. La métrica mide el número de saltos. Un red directamente conectada se considera con métrica 1. El valor de métrica de 16 representa una red inalcanzable. Cuando se detecta una red inalcanzable ésta se deja de anunciar en las siguientes actualizaciones.

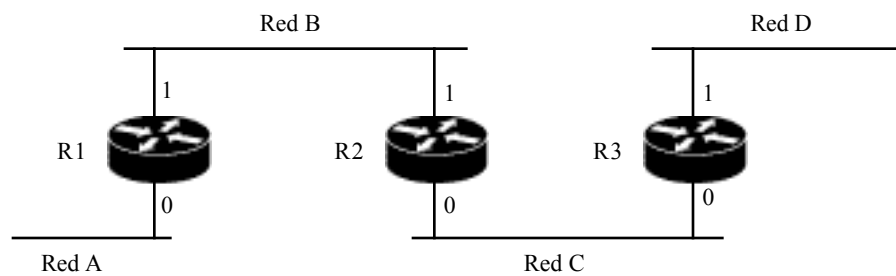
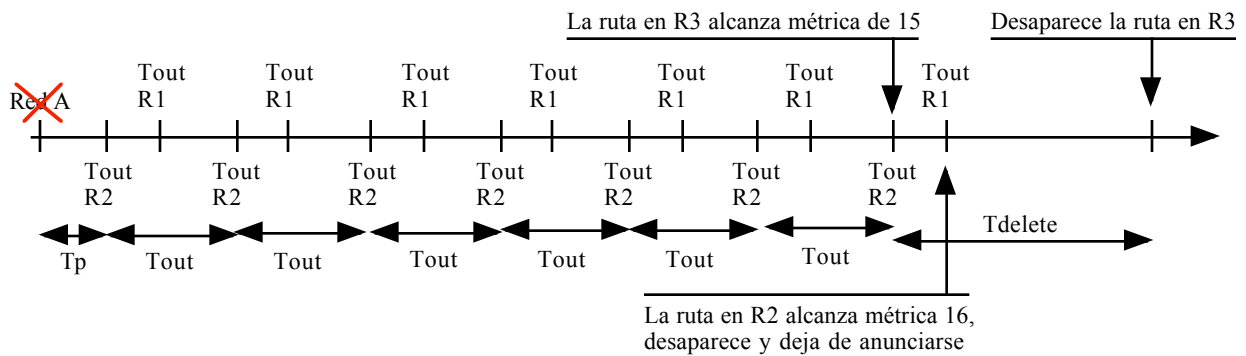


Figura 2.- Red para el problema 11

- a) Si se desconecta la Red A calcule el tiempo que transcurre hasta que el router R3 descubre que esta red pasa a ser inalcanzable. Calcule unas cotas superiores e inferiores para este valor lo más ajustadas que pueda (0.75 pts)

Vamos a mostrar cómo evoluciona en cada router la entrada en la tabla de rutas que hace referencia a la Red A. Para ello debemos suponer un ordenamiento en el tiempo para la caducidad de los timers de transmisión de la tabla de rutas (el timer periódico de 30secs). Notemos primero que las tablas enviadas por R3 no van a afectar (veremos en seguida que nunca anuncia una ruta que pueda tomarse en R2) y que el ordenamiento entre el timeout de R2 y el de R1 tampoco importa. Al desaparecer la Red A el router R1 lo marca como inalcanzable y deja de anunciarla. El siguiente evento importante podría ser que R1 envíe su tabla de rutas o que lo haga R2. Si lo hace R1 no cambia nada porque no anuncia la ruta así que R2 mantendrá la que tiene. Antes de medio minuto desde que desaparece la Red A caducará el timer de R2 y éste enviará su tabla en la que está la ruta a la Red A, esta ruta se insertará en R1 y comenzará una cuenta a infinito. A partir de aquí suponemos que se alterna la caducidad de los timers de R1 y R2. El tiempo que transcurre entre que se desconecta la Red A y caduca el timer de R2 lo llamamos  $T_p$ . Suponemos que R1 detecta inmediatamente la desconexión de la Red A.

En la siguiente figura vemos el conjunto de eventos a medida que se van sucediendo en la línea temporal.



Y en la siguiente tabla vemos el valor que toma la entrada en la tabla de rutas para la red destino A en cada router al darse cada uno de los eventos. Un entrada del tipo R2,1(5) significa que el siguiente salto para ir a esa red es el interfaz 1 del router R2 y que la métrica es 5.

Router	Inicio	Falla la Red A	Timeout en R2	Timeout en R1	Timeout en R2	Timeout en R1	Timeout en R2	Timeout en R1	Timeout en R2	Timeout en R1	Timeout en R2
R1	- (1)	X	R2,1(3)	R2,1(3)	R2,1(5)	R2,1(5)	R2,1(7)	R2,1(7)	R2,1(9)	R2,1(9)	R2,1(11)
R2	R1,1 (2)	R1,1(2)	R1,1(2)	R1,1(4)	R1,1(4)	R1,1(6)	R1,1(6)	R1,1(8)	R1,1(8)	R1,1(10)	R1,1(10)
R3	R2,0 (3)	R2,0(3)	R2,0(3)	R2,0(3)	R2,0(5)	R2,0(5)	R2,0(7)	R2,0(7)	R2,0(9)	R2,0(9)	R2,0(11)

Router	Timeout en R1	Timeout en R2	Timeout en R1	Timeout en R2	Timeout en R1	Tdelete para R2
R1	R2,1(11)	R2,1(13)	R2,1(13)	R2,1(15)	R2,1(15)	
R2	R1,1(12)	R1,1(12)	R1,1(14)	R1,1(14)	X	X
R3	R2,0(11)	R2,0(13)	R2,0(13)	R2,0(15)	R2,0(15)	X

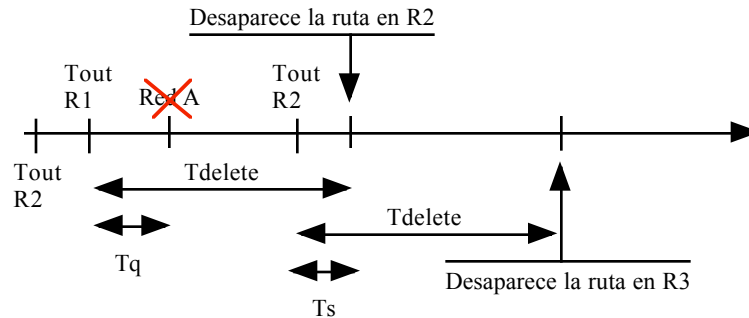
Vemos que llega un momento en que la ruta en R3 alcanza el valor métrica de 15. El siguiente evento conlleva que en R2 la ruta alcance métrica 16 y por tanto se vuelva inalcanzable y se deje de anunciar. A partir de aquí R3 no recibe refrescos de la ruta a la red A con lo que desaparecerá cuando caduque el timer Tdelete que cuenta desde la última actualización, es decir, desde que tomó el valor de métrica de 15.

Así pues, el tiempo que transcurre entre que se desconecta la Red A y R3 la marca como inalcanzable es de  $T_p + 6T_{out} + T_{delete}$  segundos. En el mejor caso  $T_p = 0$  y en el peor caso  $T_p = T_{out}$  con lo que el este tiempo estará entre  $6T_{out} + T_{delete} = 360\text{segs}$  y  $7T_{out} + T_{delete} = 390\text{segs}$ .

- b) Si se añade un mecanismo de *split horizon* al protocolo calcule de nuevo entre qué valores se encontrará el tiempo que ha de transcurrir entre que la Red A se desconecta y el router R3 descubre que es inalcanzable (0.75 pts)

Ahora ya no se anuncian por un interfaz las rutas que se hayan aprendido por ese interfaz. Una vez que la Red A se desconecta la ruta en el router R2 sobrevivirá hasta que caduque su timer de borrado (Tdelete) que se inició con la última actualización de esta ruta recibida, la cual se dio la

última vez que R1 anunció esa ruta (ver le línea de tiempos). Mientras R2 la tenga en su tabla se la anunciará a R3, reiniciando su timer de borrado. Como hay split horizon R2 no introduce la ruta a R1 porque no se la anuncia ni R3 a R2. Una vez que desaparece la ruta en R2 ya no se mandarían más actualizaciones a R3 con lo que en éste desaparecerá al caducar su timer Tdelete que se colocó cuando se recibió la última actualización enviada por R2 con esa ruta.



Router	Inicio	Falla la Red A	Tdelete en R2	Tdelete en R3
R1	- (1)	X	X	X
R2	R1,1 (2)	R1,1(2)	X	X
R3	R2,0 (3)	R2,0(3)	R2,0(3)	X

Llamamos  $T_q$  al tiempo entre la última actualización enviada por R1 antes de que la Red A se desconectara y  $T_s$  al tiempo entre la última actualización enviada por R2 y que su timer de borrado caduque. El tiempo total hasta que la ruta desaparece en R3 valdrá  $2T_{delete} - T_q - T_s$ . El valor máximo de  $T_q$  y de  $T_s$  es  $T_{out}$  y el mínimo es 0. Así pues, el tiempo total se encontrará entre  $2T_{delete} - 2T_{out} = 300$  y  $2T_{delete} = 360$ .

c) ¿Qué condición debe cumplirse entre los valores  $T_{out}$  y  $T_{delete}$  para que para esta red siempre tarde menos tiempo con split horizon? (0.5 pts)

Para que siempre tarde menos con split horizon el caso peor con este mecanismo ( $2T_{delete}$ ) tiene que ser siempre mejor ( $<$ ) que el caso mejor sin split horizon ( $6T_{out} + T_{delete}$ ). Así pues debe cumplirse que  $2T_{delete} < 6T_{out} + T_{delete}$  o equivalentemente que  $T_{delete} < 6T_{out}$ .