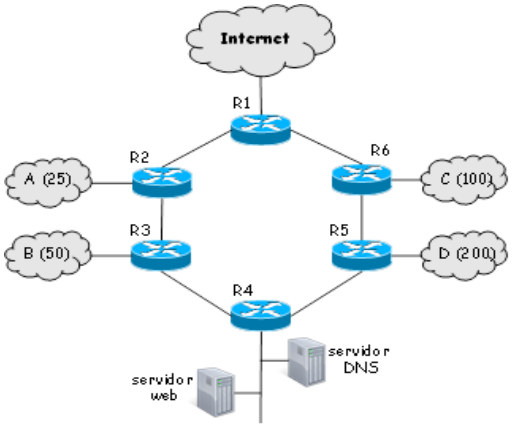
FUNDAMENTOS DE REDES – CONVOCATORIA ORDINARIA 2022

NOTA: Esta resolución es orientativa y podría contener algún error.

EJERCICIO 1 (3 puntos sobre 10)
La siguiente figura muestra la topología de red de una empresa. La única dirección pública asignada por el operador es la dirección 33.33.33.33, y la pasarela asignada por el operador es 33.33.33.1.



a) Realice una asignación de direcciones IP para todas las redes, incluyendo la red de los servidores y las redes entre routers, intentando minimizar el número de entradas en las tablas de encaminamiento.

b) Muestre el contenido de las tablas de encaminamiento de los routers.

c) Si un equipo externo (conectado a través de Internet) quisiera descargar una página web del servidor, ¿qué funcionalidad se requeriría? ¿Qué habría que configurar? ¿En qué equipo? Exponga razonadamente su respuesta.

Resolución

Hay que usar direcciones privadas porque no me dan direcciones públicas. No se indica nada sobre minimizar las máscaras de las redes, así que podemos hacerlo o poner todas las redes con una máscara cómoda (e.g. /24). En esta resolución lo haremos minimizando máscaras. Sí piden que se minimicen las rutas. Esto significa que deberíamos poder agrupar las redes A/B y C/D para que las tablas de encaminamiento tengan menos entradas. Aunque, en este caso, se pueden usar rutas por defecto que recorran la topología de forma circular y así no habría que añadir más entradas (salvo las entradas a las redes directamente conectadas).

Apartado a

Red D → 200 + red + difusión + router = 203 < 256 → 192.168.0.0/24 → de 192.168.0.0 (red) a 192.168.0.255 (difusión)

Red C → 100 + 3 < 128 → 192.168.1.0/25 → de 192.168.1.0 (red) a 192.168.1.127 (difusión)

Red B → 50 + 3 < 64 → 192.168.1.128/26 → de 192.168.1.128 (red) a 192.168.1.191 (difusión)

Red A → 25 + 3 < 32 → 192.168.1.192/27 → de 192.168.1.192 (red) a 192.168.1.223 (difusión)

Red de servidores → 2 servidores + router + red + difusión = 5 < 8 → de 192.168.1.224/29 → .224 red, .225 R4, .226 servidor web, .227 servidor DNS, .231 difusión

Las redes entre routers necesitan 2 IPs (2 routers) + red + difusión = 4 → máscara /30. Siguiendo con direcciones consecutivas, podría ser:

Red R1-R2 → 192.168.1.232/30 → .232 para red, .233 para el primer router (R1), .234 para el segundo router (R2), .235 para difusión

Red R2-R3 → 192.168.1.236/30 → .236 red, .237 R2, .238 R3, .239 difusión

Red R3-R4 → 192.168.1.240/30 → .240 red, .241 R3, .242 R4, .243 difusión

Red R4-R5 → 192.168.1.244/30 → .244 red, .245 R4, .246 R5, .247 difusión

Red R5-R6 → 192.168.1.248/30 → .248 red, .249 R5, .250 R6, .251 difusión

Red R6-R1 → 192.168.1.252/30 → .252 red, .253 R6, .254 R1, .255 difusión

Errores comunes:

- Usar direcciones que son públicas (e.g. 33.33.33.0, 168.168.168.0, 200.200.200.0, 172.168.0.0, …)
- Solapar direcciones de redes distintas
- No poner las máscaras o no usarlas correctamente

Apartado b

En general, hay que poner las rutas a las redes directamente conectadas (si no, no llegamos a ellas), poner las rutas a las redes con destinatarios (no hay que poner las rutas a todas las redes entre routers, salvo que queramos poder conectarnos a los routers, algo que habitualmente no es necesario y no se pide), y una ruta por defecto (para poder salir al resto de redes en el mundo, i.e. Internet).

En este caso concreto, como se pide minimizar, habría que:

- Intentar agrupar, al menos las redes A y B. En el ejemplo se agruparían con 192.168.1.128/25. Es cierto que eso incluiría las redes entre routers, pero 1) normalmente no queremos acceder a ellas y 2) si quisiéramos acceder a ellas, pondríamos además las rutas a esas redes y no habría problema porque tienen una máscara más restrictiva.
- En este caso concreto con una topología circular, se pueden eliminar prácticamente todas las rutas (salvo las de redes directamente conectadas) añadiendo una ruta por defecto al siguiente router (R1 hacia Internet, R2 por R3, R3 por R4, R4 por R5, R5 por R6 y R6 por R1). Así se minimiza totalmente el tamaño de las tablas

Siguiendo esto último comentado:

Tabla de encaminamiento de R1 → aquí no se puede aprovechar lo de la ruta por defecto para llegar a las redes A, B, C y D, porque esa es para salir a Internet

Red destino	Máscara	Siguiente salto
33.33.33.0 (red del operador)	/24	33.33.33.1
192.168.1.232 (red R1-R2)	/30	*
192.168.1.252 (red R1-R6)	/30	*
default (o 0.0.0.0) (salida a Internet)	/0	33.33.33.1
192.168.0.0 (C y D, ver máscara)	/23	192.168.1.253 (R6)
192.168.1.128 (A y B, ver máscara)	/25	192.168.1.234 (R2)

Tabla de encaminamiento de R2

Red destino	Máscara	Siguiente salto
192.168.1.192 (red A)	/27	*
192.168.1.232 (red R1-R2)	/30	*
192.168.1.236 (red R2-R3)	/30	*
default	/0	192.168.1.238 (R3)

Tabla de encaminamiento de R3

Red destino	Máscara	Siguiente salto
192.168.1.128 (red B)	/26	*
192.168.1.236 (red R2-R3)	/30	*
192.168.1.240 (red R3-R4)	/30	*
default	/0	192.168.1.242 (R4)

Tabla de encaminamiento de R4

Red destino	Máscara	Siguiente salto
192.168.1.224 (red de servidores)	/29	*
192.168.1.240 (red R3-R4)	/30	*
192.168.1.244 (red R4-R5)	/30	*
default	/0	192.168.1.246 (R5)

Tabla de encaminamiento de R5

Red destino	Máscara	Siguiente salto
192.168.0.0 (red D)	/24	*
192.168.1.244 (red R4-R5)	/30	*
192.168.1.248 (red R5-R6)	/30	*
default	/0	192.168.1.250 (R6)

Tabla de encaminamiento de R6

Red destino	Máscara	Siguiente salto
192.168.1.0 (red C)	/25	*
192.168.1.248 (red R5-R6)	/30	*
192.168.1.252 (red R6-R1)	/30	*
default	/0	192.168.1.254 (R1)

Apartado c

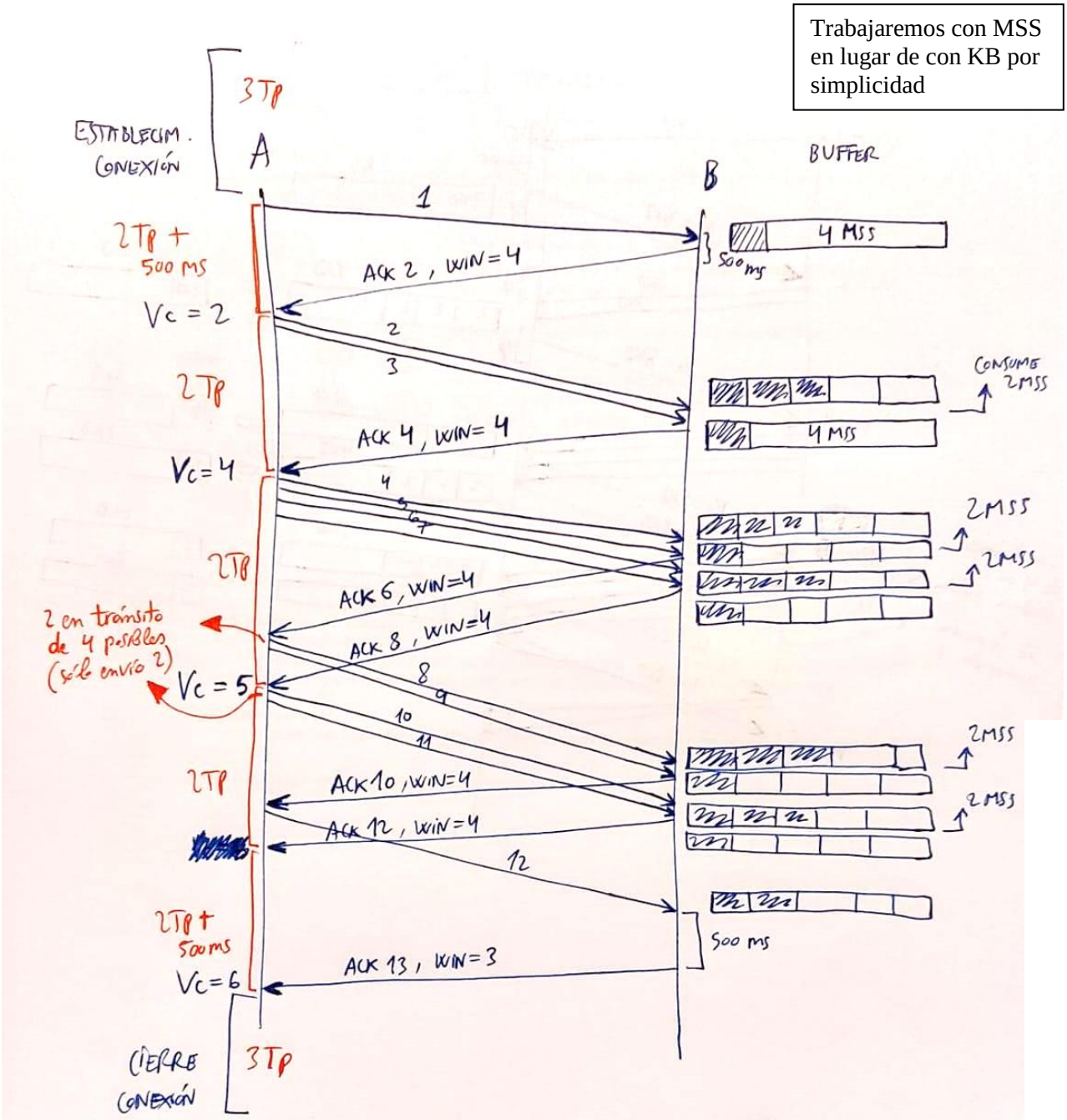
Para poder acceder desde un equipo externo, con IP pública, a un equipo interno, con IP privada, es necesario utilizar DNAT (Destination Network Address Translation). Esto permite que el equipo externo se conecte a la IP del router que actúa de frontera entre la red pública y la red privada (R1 en este caso) a un puerto (e.g. el 80, pero podría ser otro) y se reenvíe al equipo adecuado (servidor web, puerto 80). Para ello, en ese router (R1) hay que configurar que un cierto puerto (e.g. el 80) se redirija a un cierto equipo (el servidor web) y puerto (puerto 80 de TCP, donde escucha el servidor web).

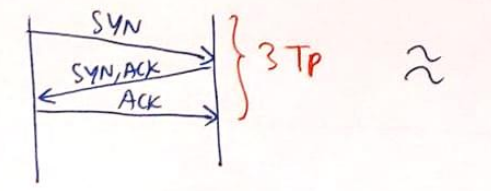
EJERCICIO 2 (2 puntos sobre 10)

Suponga dos entidades TCP A y B con la siguiente configuración: MSS = 2 KB; tamaño del buffer en recepción 10 KB; la aplicación receptora consume 4 KB cada vez que acumula 6 KB o más en el buffer; la ventana de congestión empieza siendo 1 MSS; el umbral de congestión está fijado inicialmente en 8 KB.

Muestre el diagrama de intercambio de segmentos TCP que se produciría para que A envíe un fichero de tamaño 24 KB a B. Calcule el tiempo requerido, considerando que el tiempo de propagación es 20 ms. El tiempo de transmisión es despreciable.

Trabajaremos con MSS en lugar de con KB por simplicidad





CIERRE ≈

Tiempo Total

$T_{TOTAL} = 3T_p + (2T_p + 500) + 2T_p + 2T_p + 2T_p + (2T_p + 500) + 3T_p$

$T_{TOTAL} = 320 + 1000 = 1320 ms$

PREGUNTA 1 (2 puntos sobre 10)
Explique en qué consiste el encaminamiento dinámico. Enumere dos protocolos de encaminamiento dinámico y especifique qué criterio utilizan para elegir las rutas.

En IP, el encaminamiento se basa en tablas de encaminamiento. Si se rellenan a mano, es encaminamiento estático. Si se rellenan automáticamente gracias a algún protocolo que permita que los routers intercambien información sobre la red (rutas conocidas, estado del enlace, etc.) es encaminamiento dinámico.

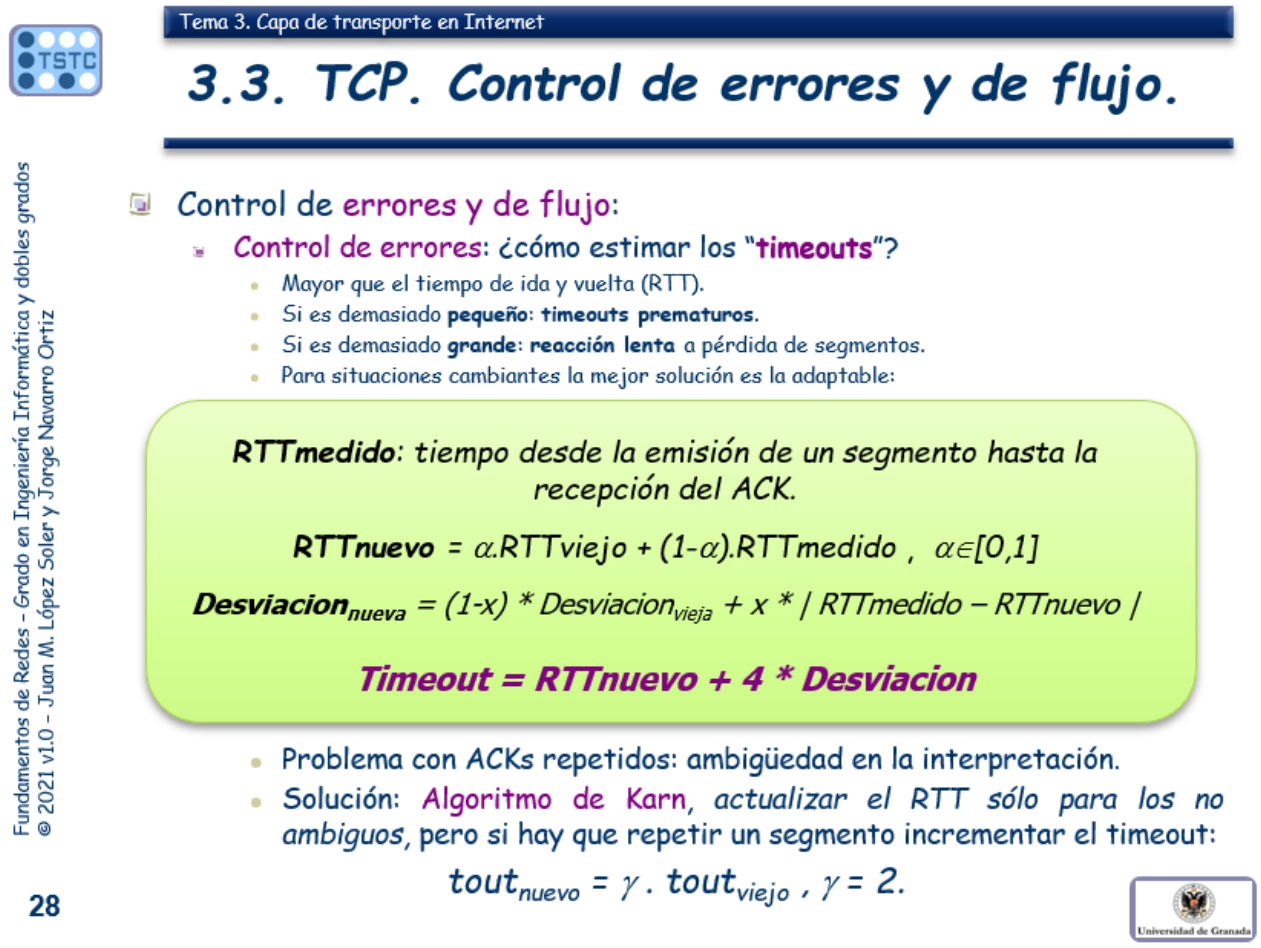
Los dos protocolos vistos en la asignatura son RIP (Routing Information Protocol) y OSPF (Open Shortest Path First).

RIP se basa en el número de saltos como métrica (número de routers que se atraviesan), buscando usar la ruta más corta (con menos routers). Para ello, intercambia mensajes cada 30 segundos. *[Se puede ampliar la información con lo que hay en la transparencia sobre RIP.*

OSPF se basa en el estado del enlace. El coste de los enlaces se puede poner a mano pero, por defecto, es el inverso de la velocidad de transmisión del enlace. Usando el algoritmo de Dijkstra se busca el camino con menor coste global (suma de los costes de cada enlace atravesado). *[Se puede ampliar la información con lo que hay en las transparencias sobre OSPF (permite rutas alternativas y balanceo de carga, uso de áreas para reducir el tráfico de señalización, mensajes utilizados, etc.).]*

PREGUNTA 2 (1.5 puntos sobre 10)
Explique cómo se determina el time-out en TCP y a qué procedimientos afecta.

El time-out se refiere a la expiración del temporizador asociado a cada segmento de datos, en espera de recibir su ACK correspondiente. Su determinación se realiza en base al RTT estimado (fórmulas en la transparencia que hay debajo), y pasa a valer el doble si hay una expiración (time-out), para intentar evitar time-outs consecutivos.



Si no llega el ACK y hay un time-out, se retransmite, afectando así al control de errores. Igualmente, la ventana de congestión se ve afectada si hay un time-out (en Tahoe se pasa a CW=CWinicial, umbral de congestión = CW/2). Como no llega el ACK, también afecta al control de flujo que no actualiza el valor de la ventana ofertada.

PREGUNTA 3 (1.5 16 puntos sobre 10)
Describa en qué consiste un certificado digital. Explique razonadamente cómo lo utilizaría para conseguir no repudio.

Un certificado digital consiste en: identidad del usuario, clave pública del usuario, otros datos (e.g. período de validez del certificado, entidad que certifica, …), todo ello cifrado con la clave privada de la entidad certificadora (ENTIDAD EN LA QUE TODOS CONFÍAN; esto es de radical importancia, porque confiamos en lo que contiene el certificado porque la entidad certificadora es un organismo en el que todos confían). Resumiendo, tengo la garantía de que una cierta clave pública esta asociada a una cierta identidad porque una entidad certificadora me lo garantiza (al ir cifrado con su clave privada, cualquiera puede descifrar la información con su clave pública pero solo la entidad certificadora ha podido cifrarlo, al ser la única que conoce su clave privada).

Una vez que tengo una identidad y una clave pública asociada de forma garantizada, puedo usar cualquier mecanismo de claves pública/privada. El certificado en sí no garantiza nada, sino que permite usar mecanismos (e.g. doble cifrado) que sí lo garantizarían.

Para conseguir no repudio, basta con usar firma digital con doble cifrado, por ejemplo. Debajo se incluye la transparencia donde se explica la firma digital con doble cifrado.

NOTA: Un certificado digital NO ES una firma digital.