TRANSMISIÓN DE DATOS Y REDES DE COMPUTADORES II

– 4º curso de Ingeniería Informática – Examen de teoría[1] – 3 de Julio de 2008

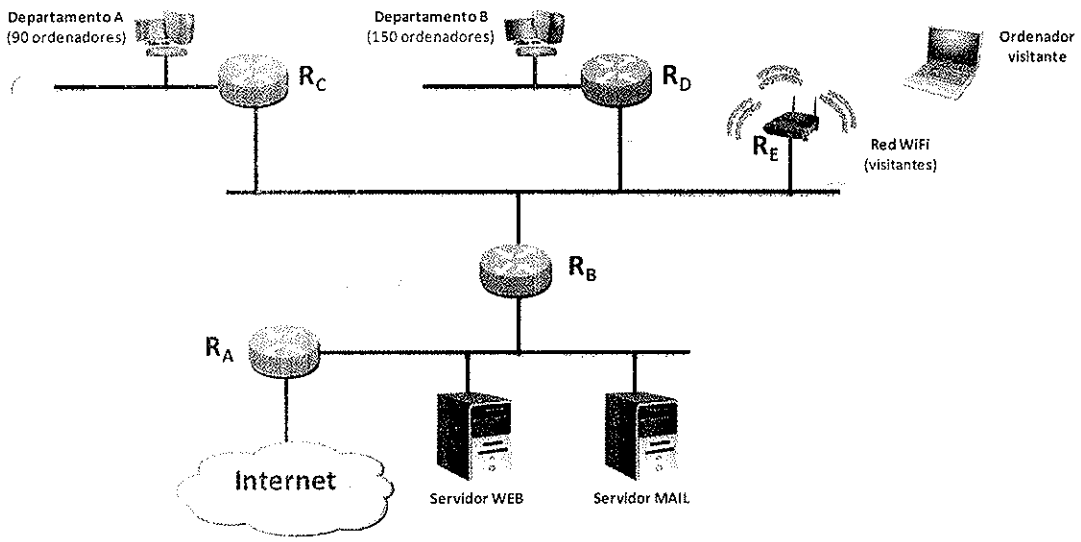
Apellidos y nombre: JORGE NAVARRO ORTIZ **Grupo:**

1. *(3 ptos.)* Dada la siguiente topología, que representa la red de una empresa, responda razonadamente las siguientes preguntas:

a) Asigne direcciones IP a los diferentes equipos y redes, minimizando el número de entradas en las tablas de encaminamiento. El ISP sólo nos proporciona la dirección IP pública 33.33.33.33. Ajustar en lo posible las asignaciones al número de ordenadores.
b) Muestre las tramas intercambiadas al ejecutar *ping* desde un equipo en el departamento B a un destino en internet, indicando para cada trama (cuando proceda)

Ethernet origen-destino	IP origen-destino	Puerto origen-destino	Datos

c) Indique el funcionamiento y configuración de los servicios necesarios en los diferentes elementos para que todo funcione correctamente con los siguiente requisitos:
   c.1. Los ordenadores de visitantes a la empresa se autoconfiguren al conectarse a la red WiFi y tengan acceso a internet.
   c.2. Los usuarios de los departamentos han de poder acceder a cualquier URL sin necesidad de conocer explicitamente su dirección IP.
   c.3. Los equipos de la intranet deben tener acceso a todos los destinos a pesar de que las tablas de encaminamiento iniciales en los routers sólo incluyan entradas a las redes directamente conectadas.



2. (1 puntos) ¿Cuál es la finalidad del campo de tiempo de vida en un datagrama IP?. ¿Cómo afecta a otros campos de la cabecera?¿ Y a otros tipos de mensajes?

3. (1 puntos) Dadas dos entidades TCP (A y B) conectadas por una red cuya velocidad de transmisión es 100 Mbps, suponga segmentos de 1024 bytes y un RTT (Round Trip Time) constante de 2 mseg. Si A transmite masivamente datos a B ¿En qué instante empezará a transmitirse el octavo segmento? Haga las suposiciones que estime necesarias.

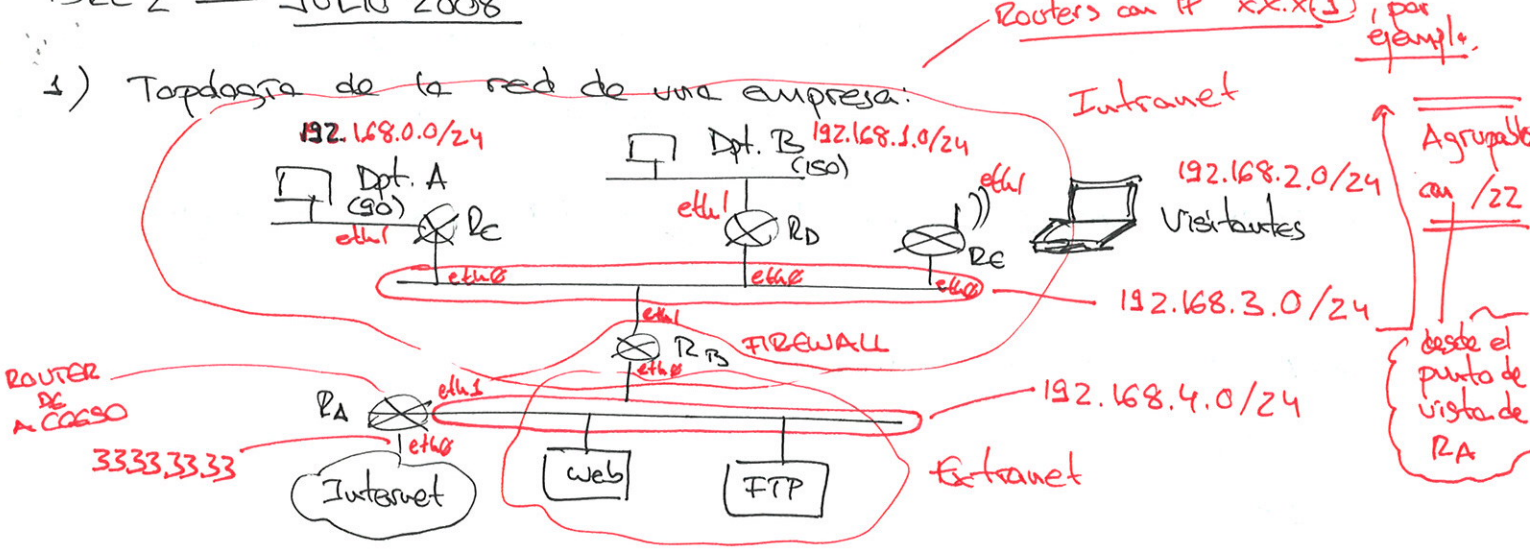
4. (2 puntos) ¿Es posible autenticar mutuamente con garantías dos entidades A y B, tal que A dispone de certificado digital y B no? Explique la respuesta adoptando las suposiones que estime necesarias.

---

[1] → La calificación de esta parte de la asignatura supondrá 7 puntos sobre el total de 10.

TDRC 2 — JULIO 2008

1) Topología de la red de una empresa:



a) Asignación de direcciones IP

→ Minimizando entradas en tablas de encaminamiento.

→ Sólo 1 IP pública: 33.33.33.33

La dirección pública hay que asignarla necesariamente al router R_A, en su interfaz con Internet.

el resto han de ser privadas → R_A hace NAT para que se pueda acceder al exterior y al interior desde fuera (e.g. web y ftp).

Minimización de rutas

* R_B ha de saber llegar a las redes de los Dptos A y B, y la de los visitantes. También a las suyas propias. Y por defecto hacia Internet (por R_A) → no se puede minimizar nada.

* R_C, R_D, R_E: han de llegar a sus redes directas, y puedan hacerlo a las otras a través de R_B (ruta por defecto), minimizando las entradas (aunque no sea un encaminamiento óptimo), pero esto no tiene nada que ver con la asignación de direcciones.

* R_A: Ruta por defecto al gateway del operador (para salir a Internet). Rutas a sus redes directas. Y las redes de los dptos y visitantes podría agruparlas y poner una única ruta por R_B.

Además, como tenemos todas las direcciones privadas que queramos, no escatimamos. Usaremos por comodidad redes de clase C (/24).

~~b) Tramas intercambiadas al ejecutar PING desde un equipo~~

TABLAS DE ENCAMINAMIENTO

R_A:

	Red	Máscara	~~Interf~~ Sig. salto	Interfaz
Directas	RED_GW_OPERADOR	MASK_RED_GW	*	eth0
	192.168.4.0	/24	*	eth1
Intranet	192.168.0.0	/22	IP_RB_eth0	eth1
Internet	default	0.0.0.0	IP_GW_OPERADOR	eth0

R_B:

	Red	Máscara	Sig. salto	Interfaz
Directas	192.168.3.0	/24	*	eth0
	192.168.4.0	/24	*	eth1
Intranet	192.168.0.0	/24	IP_RC_eth0	eth1
	192.168.1.0	/24	IP_RD_eth0	eth1
	192.168.2.0	/24	IP_RE_eth0	eth1
Internet	default	0.0.0.0	IP_RA_eth1	eth0

R_C, R_D, R_E:

	Red	Máscara	Sig. salto	Interfaz
Directas	192.168.X.0	/24	*	eth1
	192.168.3.0	/24	*	eth0
	default	0.0.0.0	IP_RB_eth1	eth0

x = 0,1,2 según la red

Se podría optimizar poniendo rutas a las otras redes de la Intranet (se ahorraría el paso por RB), pero se hace así porque se pide minimizar las entradas.

Equipos de los departamentos y visitantes:

Red	Máscara	Sig. salto	Interfaz
192.168.X.0 (X=0,1,2 según red directa)	/24	*	eth0
default (resto de redes)	IP_Rx-eth1 /24 (x=C,D ó E según red)		eth0

Servidor web y servidor mail:

	Red	Máscara	Sig. salto	Interfaz
Directas	192.168.4.0	/24	*	eth0
Intranet	192.168.0.0	/22	IP_RB-eth0	eth0
Internet	default	0.0.0.0	IP_RA-eth1	eth0

b) Tramas al mandar un PING desde un equipo del Dpto B. a un equipo en Internet.

Se usan mensajes ICMP (protocolo=1) que va sobre IP. Se envían los mensajes | Solicitud de eco (tipo=8) / Respuesta de eco (tipo=0)

No hay puertos porque no se usa UDP ni TCP.

Suponemos que las tablas ARP están actualizadas. Si no, se mandaría en cada red una petición y su respuesta para averiguar la dirección física (MAC) de la dirección IP del siguiente salto.

MAC origen	MAC destino	IP origen	IP destino	Puertos	Datos
MAC_equipo_Bx	MAC_RD-eth1	IP_equipo_Bx	IP_equipo_Internet	[redacted]	ICMP echo request
MAC_RD-eth0	MAC_RB-eth1	"	"	—	"
MAC_RB-eth0	MAC_RA-eth1	"	"	—	"
→ MAC_RA-eth0	MAC_GW.operador	33.33.33.33	"	—	"
... Resto por Internet para llegar hasta el equipo ...					"

Se aplica SNAT en RA

(continuación)

MAC origen	MAC destino	IP origen	IP destino	Puerto	Datos
... envío desde el equipo hasta llegar al GW del operador ...				—	ICMP echo reply
MAC_GW_operador	MAC_RA_eth0	IP_equipo_internet	33.33.33.33	—	"
MAC_RA_eth1	MAC_RB_eth0	"	IP_equipo_Bx	—	"
MAC_RB_eth1	MAC_RD_eth0	"	"	—	"
MAC_RD_eth1	MAC_equipo_Bx	"	"	—	"

Se deshace el SNAT en RA

El único detalle es realizar SNAT al salir hacia Internet y deshacer SNAT al volver la respuesta, todo en R_A.

c) Servicios y configuración necesarios para:

- Ordenadores visitantes autoconfigurados → DHCP en RE, con el rango de direcciones asignadas (salvo la del router)

- Usuarios en bptas acceden a URLs sin saber IPs.

  ↳ Configurar un DNS dentro de la empresa, p.ej. en la misma red que los otros servidores. Configurar a los equipos para usar ese (o varios) DNS. O bien poner DHCP en RC y RD y que ese protocolo asigne el DNS (aunque no es necesario usar DHCP aquí).

- Los equipos de la intranet deben acceder a todo aunque los routers tengan inicialmente sólo entradas a las redes directas.

  ⟹ Usar RIP (otro protocolo de intercambio de info. de encaminamiento) en los routers.

Periódicamente (30 seg.) se intercambiarán a qué redes saben acceder y con qué coste, y tras varias iteraciones sabrán llegar a todas las redes con un coste (nº saltos) óptimo.

EXAMEN TDRC2 JUNIO 2008

2) TTL: para evitar bucles infinitos y congestión. Decrece en 1 en cada salto, descartándose el datagrama si llega a 0.

Campos: checksum se recalcula en cada salto al cambiar el TTL.
Mensajes: ICMP time exceeded al expirar el TTL, hacia el origen.

3) Tiempo en el que empieza la transmisión del 8º segmento.

Segmento TCP = 1024 bytes → +20 bytes de la cabecera IP + x bytes de las capas inferiores
Velocidad t_x = 100 Mbps
RTT = 2 ms

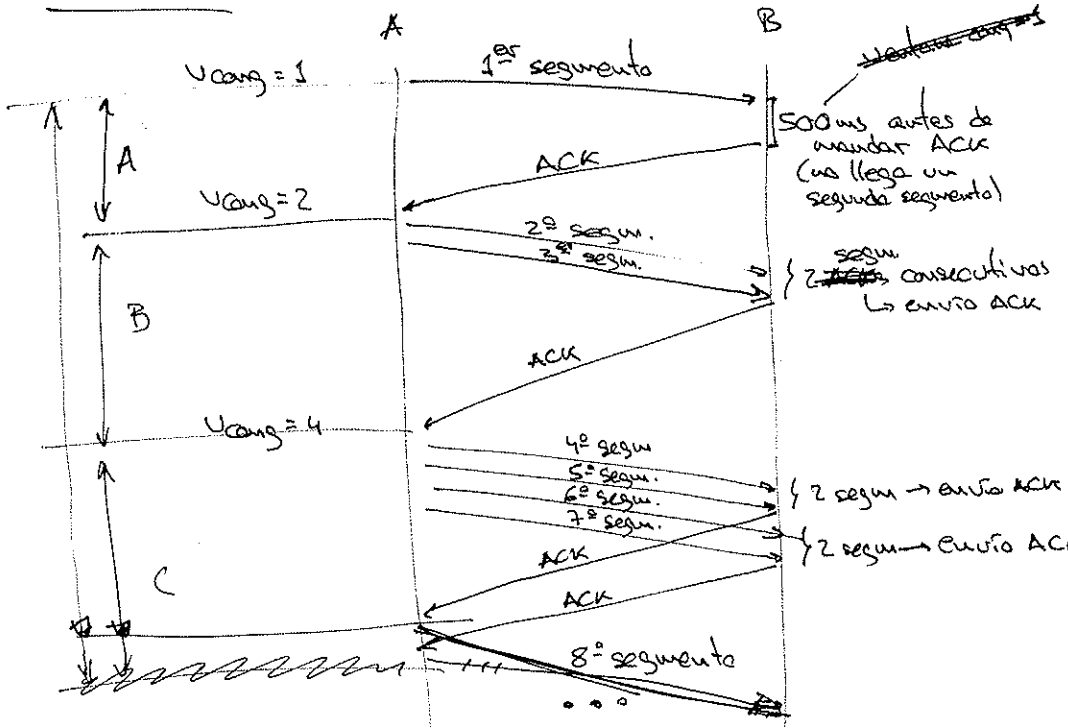
Suposiciones:

* $t_{ida} = t_{vuelta}$ (aunque daría igual)
* $t_{procesado\ ACK} \simeq t_{generación\ ACK} \simeq 0$

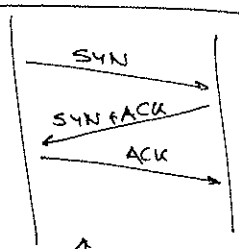
Hay que considerar:

* Control de congestión de TCP

Solución:



Establecimiento TCP



$1'5\ RTT + \frac{3 \times 40 \times 8}{100 \cdot 10^6} = 3'0096$ ms

A) $T_{ida} + \frac{8\cdot(1024+20)}{100\cdot10^6} + 500\,ms + T_{vuelta} + \frac{8\cdot40}{100\cdot10^6} =$

$= RTT + \frac{8\cdot(1024^{+20}+40)}{100\cdot10^6} = 502\,ms + 87'04\,\mu s = 502'087\not{0}4\,ms = T_A$

B) $T_{ida} + \frac{2\times8\times(1024+20)}{100\cdot10^6} + T_{vuelta} + \frac{8\cdot40}{100\cdot10^6} = RTT + \frac{8\cdot(2\cdot1024^{+2\cdot20}+40)}{100\cdot10^6} =$

$= RTT + 170'24\,\mu s = 2'17024\,ms = T_B$

C) $T_{ida} + \frac{2\times8\times(1024+20)}{100\cdot10^6} + T_{vuelta} + \frac{8\cdot40}{100\cdot10^6} = 2'17024\,ms = T_C$

Tiempo total ~~(que estás)~~ $= T_{establ.TCP} + T_A + T_B + T_C =$

$= 3'0096\,ms + 502'087\not{0}4\,ms + 2'17024\,ms + 2'17024\,ms =$

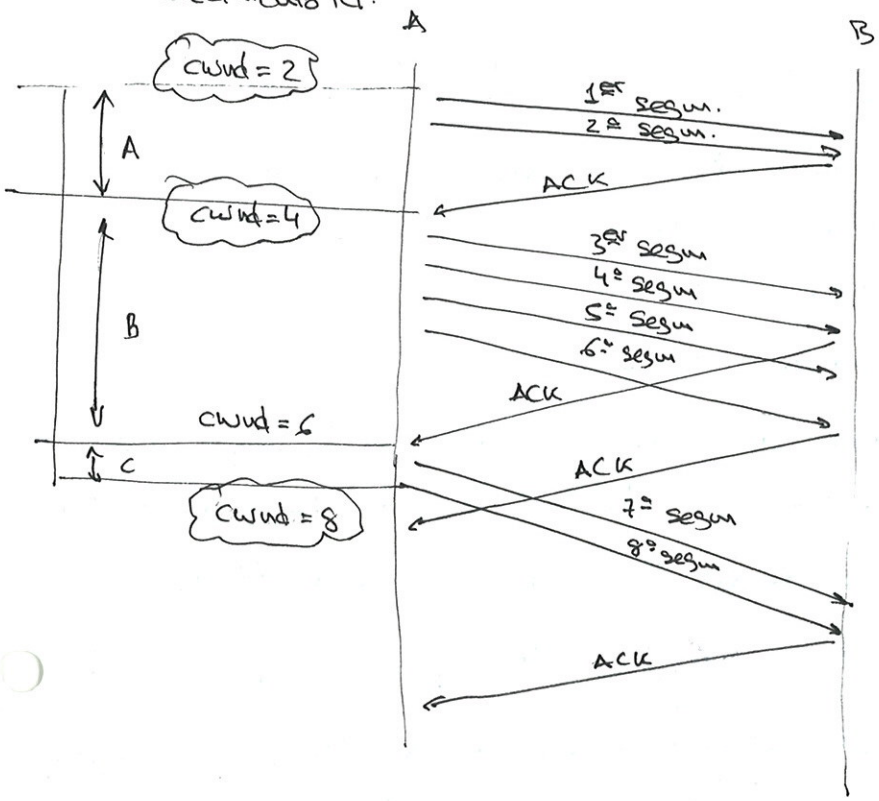
$= 509'437\not{4}2\,ms$

y habría que meter las cabeceras MAC+PHY

NOTA: Esta solución supone que la ventana de congestión inicial es 1. En muchos sitios dicen 1, en otros dicen 2. Quizá 2 tiene más sentido porque nos ahorraríamos los 500 ms de espera inicial.

Sdución con ventana de congestión inicial igual a 2.

Tras el establecimiento TCP:



Habría que añadir las cabeceras MAC + PHY y sobrecarga

$$T_A = T_{ida} + \frac{8 \times (1024+20)}{100 \cdot 10^6} + T_{vuelta} + \frac{8 \cdot 40}{100 \cdot 10^6} = 2'08704 \text{ ms}$$

$$T_B = T_{ida} + \frac{2 \times 8 \times (1024+20)}{100 \cdot 10^6} + T_{vuelta} + \frac{8 \cdot 40}{100 \cdot 10^6} = 2\text{ms} + 167'04\,\mu\text{s} + 3'2\,\mu\text{s} = 2'16924 \text{ ms}$$

$$T_C = \frac{8 \times (1024+20)}{100 \cdot 10^6} = 83'52\,\mu\text{s}$$ ← tiempo de transmisión del séptimo segmento.

$$T_{total} = T_A + T_B + T_C = 4'3398 \text{ ms}$$

A esto habría que sumarle el tiempo de generación y procesado de ACKs, que hemos supuesto despreciable.

+ tiempo de establecimiento TCP.

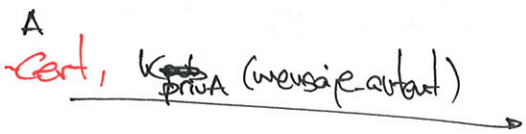
4) Autenticación mutua de A y B, con certificado digital de A.

El certificado digital lleva la siguiente información:

* Identificación de AC (autoridad certificadora)
* Identificación del usuario
* Clave pública del usuario
* Otros (periodo de validez, ...)

Y todo ello va firmado con la clave privada del AC, que al ser una entidad fiable, garantiza la fiabilidad de dicha información (que cualquiera puede leer usando la clave pública del AC).

De esta forma, A tiene un par $K_{pub_A} - K_{priv_A}$ y todos conocen K_{pub_A}. Para autenticarse, manda algo con su K_{priv_A} y como sólo A pudo hacerlo, queda autenticado. E.g:



B no puede hacer lo mismo porque no tiene certificado → → no tiene un par $K_{pub_B} - K_{priv_B}$.

~~Aun suponiendo que A y B tuviesen una clave secreta~~

B podría optar por autenticarse con clave secreta, pero aunque intercambiara dicha clave con A, es susceptible de ataques (repetición, persona en medio) y nadie garantiza que B sea quien dice ser. Para que haya autenticación con garantías debe haber una entidad fiable que sea la que garantice que la información (identidad, claves) es correcta.

CONCLUSIÓN: No se podrían autenticar mutuamente con garantías.