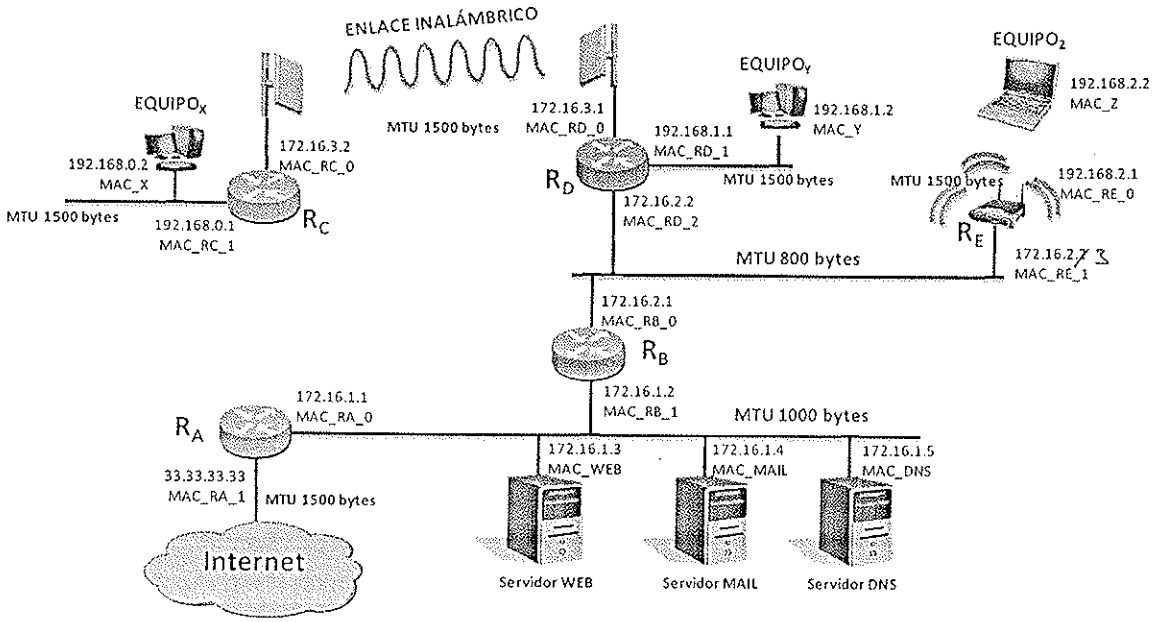
TRANSMISIÓN DE DATOS Y REDES DE COMPUTADORES II

– 4º curso de Ingeniería Informática –

Examen de teoría[1] – 17 de Septiembre de 2008

Apellidos y nombre: JORGE NAVARRO ORTIZ

1. *(2 puntos)* Una red tiene la topología y configuración (direcciones físicas e IP, MTU de cada red) mostrada en la figura.



Se pide:

a) Mostrar el intercambio de tramas entre el *equipo X* y el servidor *WEB*. Suponga que las tablas ARP están actualizadas, que el *equipo X* sólo conoce el nombre de dominio del servidor *WEB*, y que tanto la solicitud como la respuesta ocupan 1460 bytes. Para cada trama generada detalle la siguiente información:

- Direcciones hardware origen y destino.
- Direcciones IP origen y destino.
- En su caso, los puertos origen y destino.
- En su caso, los *flags* activos y campos de secuencia y ACK.
- El tipo de mensaje del que se trata.

b) ¿Qué pasaría si el campo TTL de los paquetes IP generados por el *equipo X* tuviese un valor igual a 3? Describa las tramas intercambiadas (puede hacer referencia a las tramas del apartado a).

c) ¿Qué ocurriría si el campo DF (*don't fragment*) de los paquetes IP generados por el *equipo X* valiese 1? Describa las tramas intercambiadas (puede hacer referencia a las tramas del apartado a).

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

2. (2 puntos) Un alumno desea enviar, desde su cuenta alumno@micorreo.es, un correo electrónico a su profesor profesor@ugr.es. Indique los elementos por los que pasa el correo electrónico y los protocolos involucrados, desde que se crea el correo hasta que lo lee el destinatario. ¿Cómo podría una tercera persona interceptar el correo electrónico, y evitar que le llegue al profesor?. Proponga soluciones para evitar estos ataques.

3. (*2 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. *(1 puntos)* Suponga que en instante t = 300 milisegundos (medidos desde una referencia local) se recibe un mensaje ICMP de sello de tiempo. Si en el mensaje recibido los campos de tiempo de *emisión*, *recepción* y *respuesta* son respectivamente 50, 110 y 120 milisegundos, ¿están sincronizados los relojes de las dos entidades involucradas? En su caso, ¿cuál es el desajuste?

Ejercicio 1

a) Intercambio de tramas entre el equipo X y el servidor web.

* Tablas ARP actualizadas
* Sólo se conoce el nombre del servidor
* Petición / respuesta del servidor → 1460 bytes

PREGUNTA AL DNS

MAC origen	MAC destino	IP origen	IP destino	Puerto origen	Puerto destino	Flags	Mensaje
MAC_X	MAC_RC1	192.168.0.2	172.16.1.5	(*1)	53	—	Consulta DNS sobre UDP
MAC_RC0	MAC_RD0	"	"	"	"	—	" nombre_dominio_servidor_web
MAC_RD1	MAC_RB0	"	"	"	"	—	" (suponemos <800 bytes)
MAC_RB1	MAC_DNS	"	"	"	"	—	"
MAC_DNS	MAC_RB1	172.16.1.5	192.168.0.2	53	(*2)	—	Respuesta DNS IP_servidor_web
MAC_RB0	MAC_RD1	"	"	"	"	"	"
MAC_RD0	MAC_RC0	"	"	"	"	"	"
MAC_RC1	MAC_X	"	"	"	"	"	"

ESTABLECIMIENTO TCP

A

MAC_X	MAC_RC1	192.168.0.2	172.16.1.3	(*3)	80	SYN Y=seq	Estab. TCP
MAC_RC0	MAC_RD0	"	"	"	"	"	"
MAC_RD1	MAC_RB0	"	"	"	"	"	"
MAC_RB1	MAC_WEB	"	"	"	"	"	"

B

MAC_WEB	MAC_RB1	172.16.1.3	192.168.0.2	80	(*4)	SYN+ACK Y=seq, X+1=acuse	Estab. TCP
MAC_RB0	MAC_RD1	"	"	"	"	"	"
MAC_RD0	MAC_RC0	"	"	"	"	"	"
MAC_RC1	MAC_X	"	"	"	"	"	"

A

		192.168.0.2	172.16.1.3	(*4)	80	ACK Y+1, X+1	Estab. TCP
		"	"	"	"	"	"
		"	"	"	"	"	"
		"	"	"	"	"	"

PETICIÓN WEB

MAC_X	MAC_RC1	192.168.0.2	172.16.1.3	(*4)	80	X+1, Y+1	ident=u	Petición web (1460 bytes)
MAC_RC0	MAC_RD0	"	"	"	"	"	ident=u	"
MAC_RD1	MAC_RB0	"	"	"	"	"	ident=u, offset=0	" (780 bytes) 1er fragm.
frag.		"	"	"	"	MF=1		
		"	"	"	"	MF=0	ident=u, offset=780	" (680 bytes) 2º fragm.
MAC_RB1	MAC_WEB	"	"	"	"	MF=0	ident=u, offset=0	" (780 bytes) 1er fragm.
		"	"	"	"	MF=0	ident=u, offset=780	" (680 bytes) 2º fragm.

*1 → Dado por el S.O.
*2 → El mismo que *1
*3 → Dado por S.O.
*4 → Igual que *3.

RESPUESTA WEB

MAC origen	MAC dest.	IP origen	IP dest.	Puerta origen	Puerta Dest.	Flags	Mensaje
MAC_WEB	MAC_RB1	172.16.1.3	192.168.0.2	80	(*4)	MF=1 ident=m offset=0 ACK	Respuesta web (~~1480~~ 980 b)
"	"	"	"	"	"	MF=0 ident=m offset=~~980~~ 1460 ACK	" (480 b)
MAC_RB0	MAC_RD1	"	"	"	"	MF=1 ident=m offset=0 ACK	" (~~1480~~ b)
"	"	"	"	"	"	MF=1 ident=m offset=~~0~~ 780 ACK	" (2006)
"	"	"	"	"	"	MF=0 ident=m offset=~~980~~ 980 ACK	" (480 b)
MAC_RD0	MAC_RC0	"	"	"	"		
"	"	"	"	"	"		
"	"	"	"	"	"		
MAC_RC1	MAC_X	"	"	"	"		
"	"	"	"	"	"		
"	"	"	"	"	"		

1ª fragm.

2ª fragm.

Si se cerrara la conexión, sería igual que el establecimiento pero activando el flag FIN en lugar del flag SYN. El número de secuencia sería X+1460 y Y+1460 respectivamente. con ACK de la resp. HTTP.

NOTA: Suponemos que los ACK se hacen con piggybacking.

b) Si TTL=3, entonces sólo llegaría hasta RB (cada router decrementa el TTL en 1, luego TTL=0 en RB). Así, sólo se enviarían las 3 primeras tramas (consulta DNS). RB devolvería un mensaje ICMP de tiempo excedido por TTL.

Primeras 3 tramas

ICMP time exceeded (TTL)

				ICMP no tiene puertos	ICMP no tiene Flags	Mensaje
MAC_RB0	MAC_RD1	172.16.2.1	192.168.0.2	—	—	ICMP time exceeded (TTL)
MAC_RD0	MAC_RC0	"	"	"	"	"
MAC_RC1	MAC_X	"	"	"	"	"

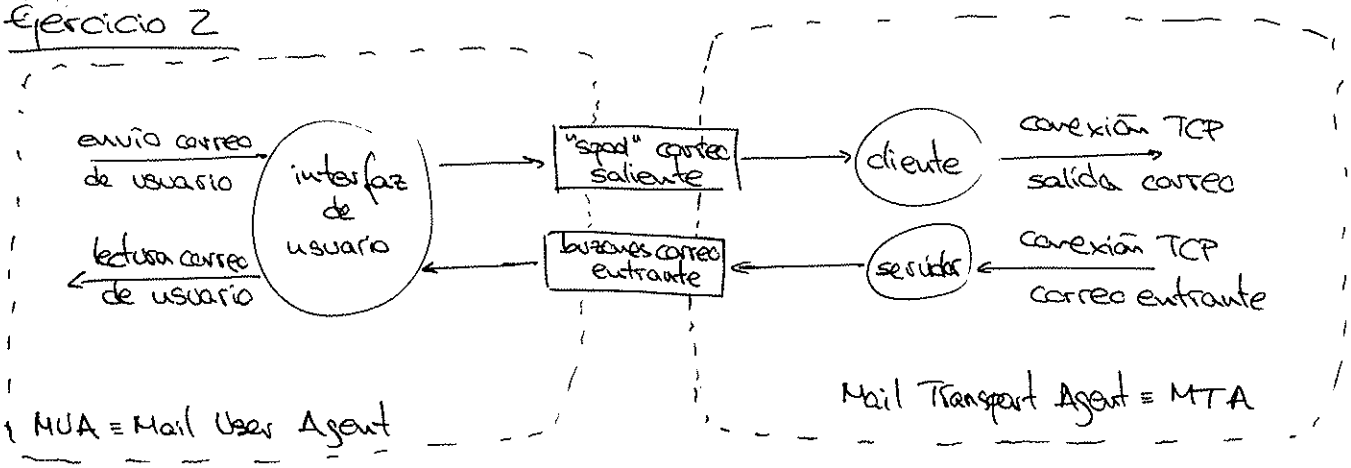
c) Si DF=1, R_D no podría transmitir (fragmentando → petición web) y mandaría a X un mensaje ~~de~~ ICMP destino inalcanzable por fragmentación. Esto sería en la petición web suponiendo que el resto de mensajes (DNS...) tuviesen menos de ~~1500~~ 772 bytes (800 − ~~40~~ 28 de cabecera IP+UDP).

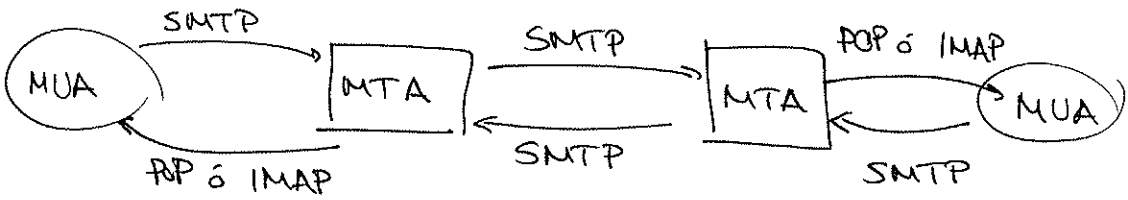
... Mismas tramas hasta que la petición web llega hasta R_D ...

					Sin puertos ni flags	Mensaje
ICMP dest. unreach. Fragm.	MAC_RD0	MAC_RC0	172.16.3.1	192.168.0.2	— —	ICMP destination
	MAC_RC1	MAC_X	"	"	" " "	unreachable - fragm.
						"

Ejercicio 2

a)





1. Envío del correo a través del spool de correo saliente del MUA del alumno al MTA del alumno → protocolo SMTP.
2. Envío del MTA del alumno al MTA del profesor → SMTP.
3. Envío del MTA del profesor al MUA del profesor → POP.

Se usarían las peticiones / respuestas DNS que fuesen necesarias (conexión al DNS correspondiente).

1) Posibles ataques.

- Suplantación de DNS → por vulnerabilidades de un DNS se le meten entradas falsas → se propaga a otros DNS (DNS poisoning).
- Ataques RIP o source routing → rutas comprometidas.
- Mail spoofing: suplantación en el correo electrónico de la dirección de otras personas o entidades. Usado para SPAM.
  - Esto no permitiría leer el correo de otro.

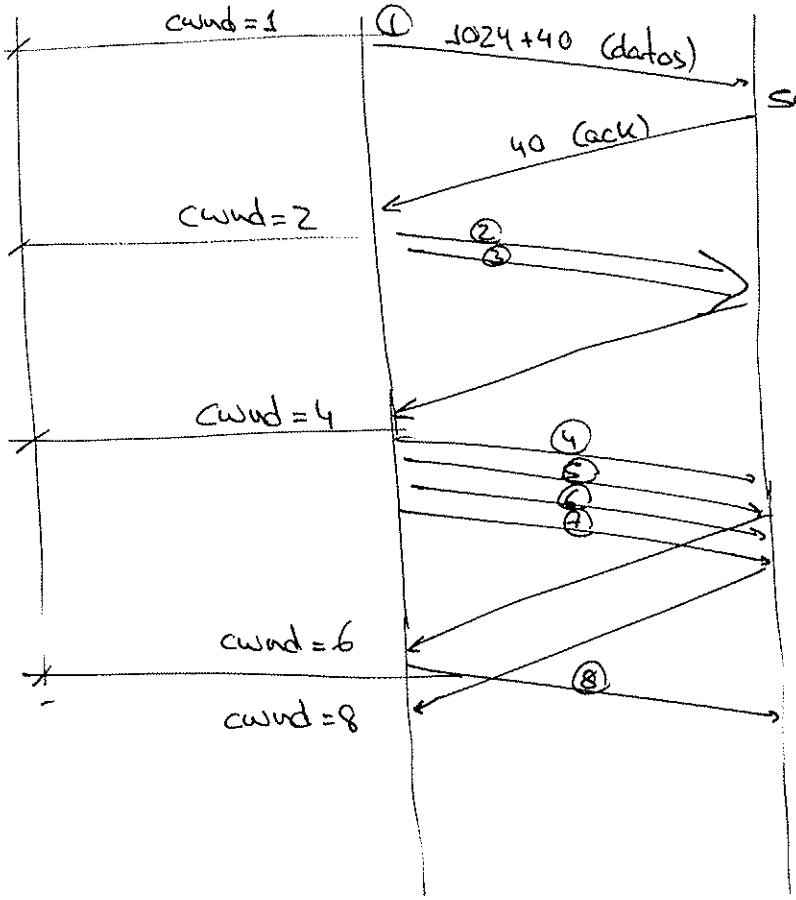
Soluciones:

- Suplantación de DNS: dos preguntas, a la inversa y directa y comparar las respuestas.
- Ataques RIP: proteger los paquetes de actualización (cifrado).
  + Uso de nonces (para evitar repetición)
- Mail spoofing: comprobar la IP del remitente y la dirección del servidor SMTP usado. También el uso de firmas digitales.

- En general → uso de SSL.

Ejercicio 3

El inicio lento de TCP se debe al control de congestión. Suponiendo que la ventana de congestión vale inicialmente 1:

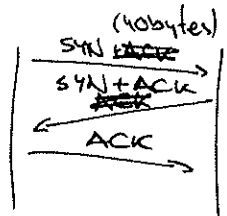


$T_{Tx\,datos} = \frac{(1024+40)\cdot 8}{100\cdot 10^6} = 85'12\,\mu s$

$T_{Tx\,ACK} = \frac{40\cdot 8}{100\cdot 10^6} = 3'2\,\mu s$

Despreciando el retardo introducido por capas inferiores.

ESTABLECIMIENTO TCP



$T_{ESTAB} = \frac{3}{2} RTT + 3 \times T_{Tx\,ACK} = 3\,ms + 9'6\,\mu s = 3'0096\,ms$

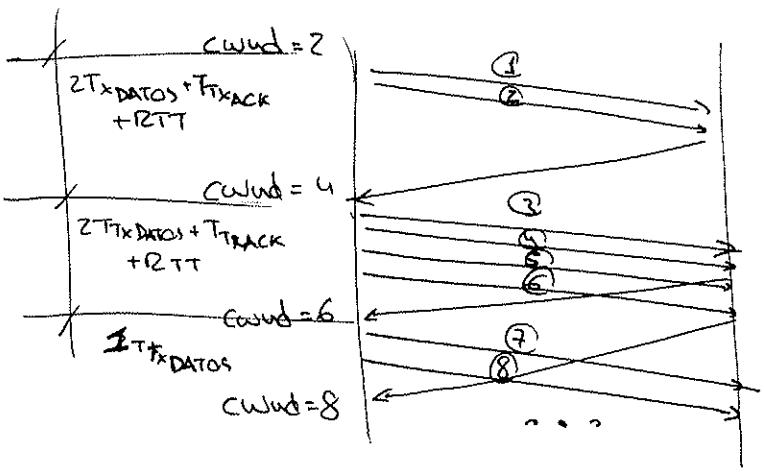
$T_{8\,SEGM} = T_{ESTAB} + \left(T_{Tx\,datos} + 500\,ms + T_{Tx\,ACK} + RTT\right) + \left(2\cdot T_{Tx\,DATOS} + RTT + T_{Tx\,ACK}\right) +$

$+ \left(2\cdot T_{Tx\,DATOS} + T_{Tx\,ACK} + RTT\right)$ ← de las tramas 4 y 5

$= T_{ESTAB} + 500\,ms + 3RTT + 5\,T_{Tx\,datos} + 3\,T_{Tx\,ACK} = 3'0096 + 500 + 6 + 0'4256 + 0'0096 =$

$= 509'5312\,ms$

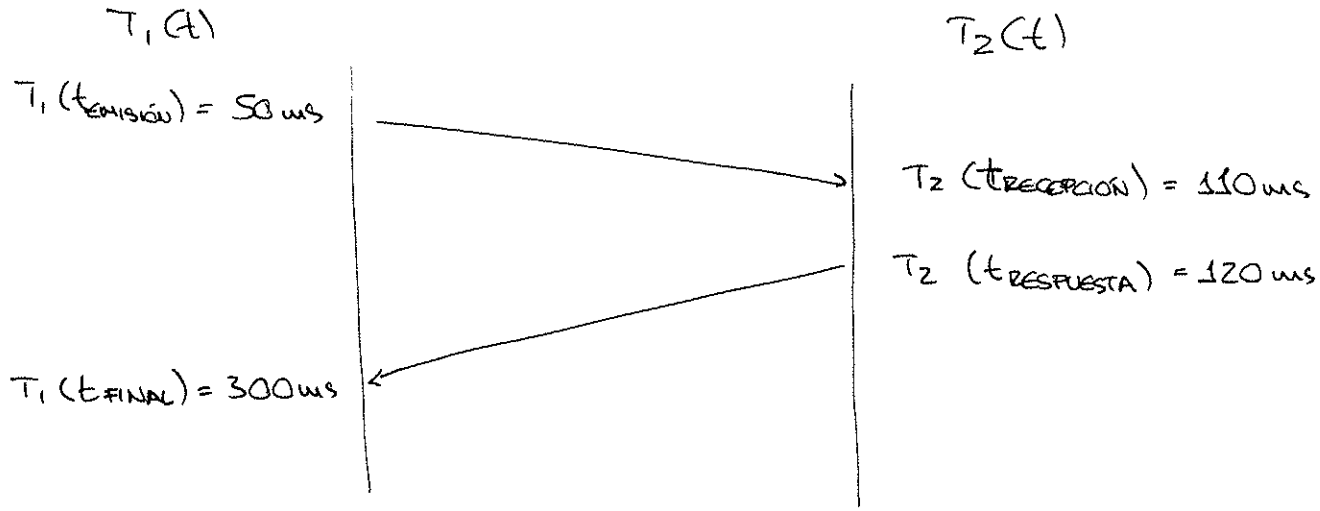
Si la ventana de congestión inicial vale 2, nos ahorramos los 500 ms.



$T_{8\,SEG} \Rightarrow T_{ESTAB} + 5T_{TxDATOS} + 2T_{TxACK} + 2R_{TT} = 3'0096 + 0'4256 +$

$+ 0'0064 + 4 \Rightarrow \boxed{7'4416\ ms}$

Ejercicio 4



Si hay un desfase entre los relojes $\Rightarrow T_1(t) = T_2(t) + offset$

Suponemos que el tiempo de ida y vuelta son iguales:

$$T_{IDA} = T_2(t_{RECEPCIÓN}) - T_2(t_{EMISIÓN}) = 110 - (50 - offset) =$$

$$= 60 + offset \text{ ms}$$

$$T_{VUELTA} = T_1(t_{FINAL}) - T_1(t_{RESPUESTA}) = 300 - (120 + offset) =$$

$$= 180 - offset \text{ ms}$$

Si $T_{IDA} = T_{VUELTA} \Rightarrow 60 + offset = 180 - offset \Rightarrow$

$$\Rightarrow offset = \frac{180 - 60}{2} = 60 \text{ ms}$$