TRANSMISIÓN DE DATOS Y REDES DE ORDENADORES

Examen de Teoría[1]

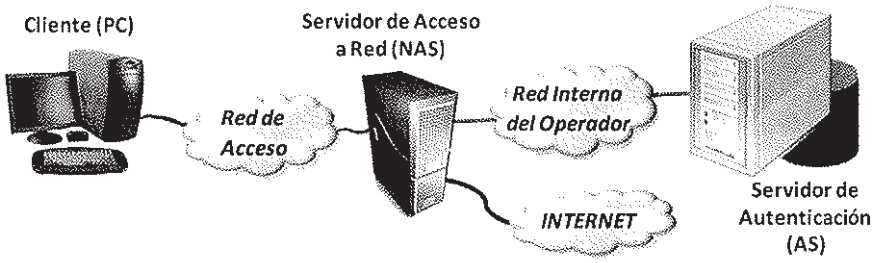
Septiembre de 2010

APELLIDOS, NOMBRE: JORGE NAVARRO ORTIZ

GRUPO TEORÍA:

---

1. (*2 puntos*) La figura y mensajes siguientes describen un hipotético protocolo utilizado para permitir el acceso de un cliente a Internet a través de un Servidor de Acceso a Red (NAS). El Servidor de Autenticación (AS) guarda en una base de datos las claves secretas que se solicita a los usuarios para poder acceder a Internet.



PC → NAS:	$Kpub_{NAS}$ (peticion_acceso + usuario)
NAS → PC:	desafio
PC → NAS:	$Kpub_{NAS}$(MD5(usuario:K_{PC-AS}:desafio))
NAS → AS:	peticion_autenticacion + usuario + desafio +
	+ MD5(usuario:K_{AS-PC}:desafio))
AS → NAS:	peticion_aceptada + $Ksesion_{PC-NAS}$ + K_{PC-AS}($Ksesion_{PC-NAS}$)
	(ó peticion_rechazada)
NAS → PC:	$Kpriv_{NAS}$ (peticion_aceptada + K_{PC-AS}($Ksesion_{PC-NAS}$))
	(ó $Kpriv_{NAS}$ (peticion_rechazada))
PC → NAS:	$Ksesion_{PC-NAS}$ (datos_a_enviar)
NAS → Internet:	datos_a_enviar
Internet → NAS:	datos_de_respuesta
NAS → PC:	$Ksesion_{PC-NAS}$ (datos_de_respuesta)

Siendo:

- $Kpub_X$ cifrado con la clave pública de X
- $Kpriv_X$ cifrado con la clave privada de X
- K_{X-Y} la clave secreta entre X e Y
- MD5 es una función *hash*

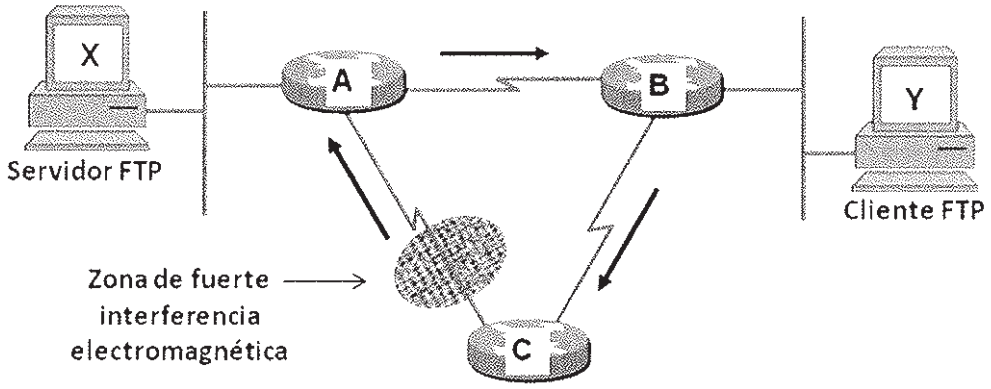
Aceptadas la disponibilidad y validez de las claves públicas involucradas en base a la existencia de una entidad superior confiable, responda razonadamente:

a) ¿Qué servicios de seguridad se proporcionan en el protocolo descrito?
b) ¿Qué debilidades presenta el esquema propuesto? En su caso, ¿cómo podrían evitarse?

---

[1] Esta prueba supone el 70% de la calificación final de la asignatura.

2. (*2 puntos*) En la red de la siguiente figura Y ha establecido con X una conexión FTP (sobre TCP) y ha solicitado el envío de un fichero que para transmitirse requiere el envío de 20 segmentos. No se envían datos en sentido contrario, por lo que el TCP de Y solo envía a X los ACKs correspondientes:



Como muestra la figura la comunicación utiliza rutas asimétricas. Además, el enlace entre los routers A y C pierde una de cada tres tramas que pasan por él (es decir, falla la tercera, la sexta, etc.).

Suponga que no hay problemas de congestión, no hay control de flujo y la ventana de congestión inicial es igual a 2 MSS.

a) Describa la secuencia de segmentos que intercambiarán las capas TCPs de X e Y, detallando los envíos duplicados que se produzcan (si es que se producen). Omita la parte correspondiente al establecimiento y terminación de la conexión TCP.

b) Calcule el tiempo necesario para transferir el fichero suponiendo que el RTT de la comunicación X-Y es igual a 100 ms y que el timeout de retransmisión es de 200 ms. Considera despreciable el tiempo que se tarda en emitir los segmentos por las interfaces.

3. (1 puntos) Desde un ordenador se arrancan tres navegadores diferentes, Internet Explorer, Mozilla Firefox y Google Chrome, y se accede desde los tres a un servidor web en la dirección 147.156.1.4 (el mismo desde los tres) ¿Cuántos sockets y cuantas conexiones TCP están implicados, tomando en cuenta tanto el lado servidor como el cliente?

4. (1 puntos) ¿Qué significa el campo TTL de los RR (Registros de Recursos) de un paquete DNS?

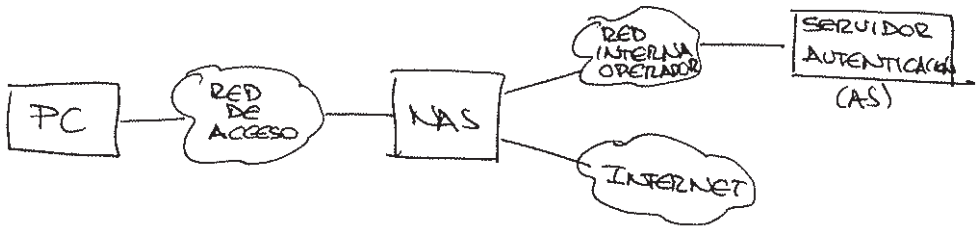
5. (1 puntos) Una empresa tiene cinco departamentos, cada uno con una subred con direcciones privadas. Los rangos que elige el administrador de red son los siguientes:

- Departamento 1: 192.168.0.0/25
- Departamento 2: 192.168.0.128/27
- Departamento 3: 192.168.0.160/26
- Departamento 4: 192.169.0.0/25
- Departamento 5: 192.169.0.128/25

Explique detalladamente dos posibles problemas que tenga esta asignación.

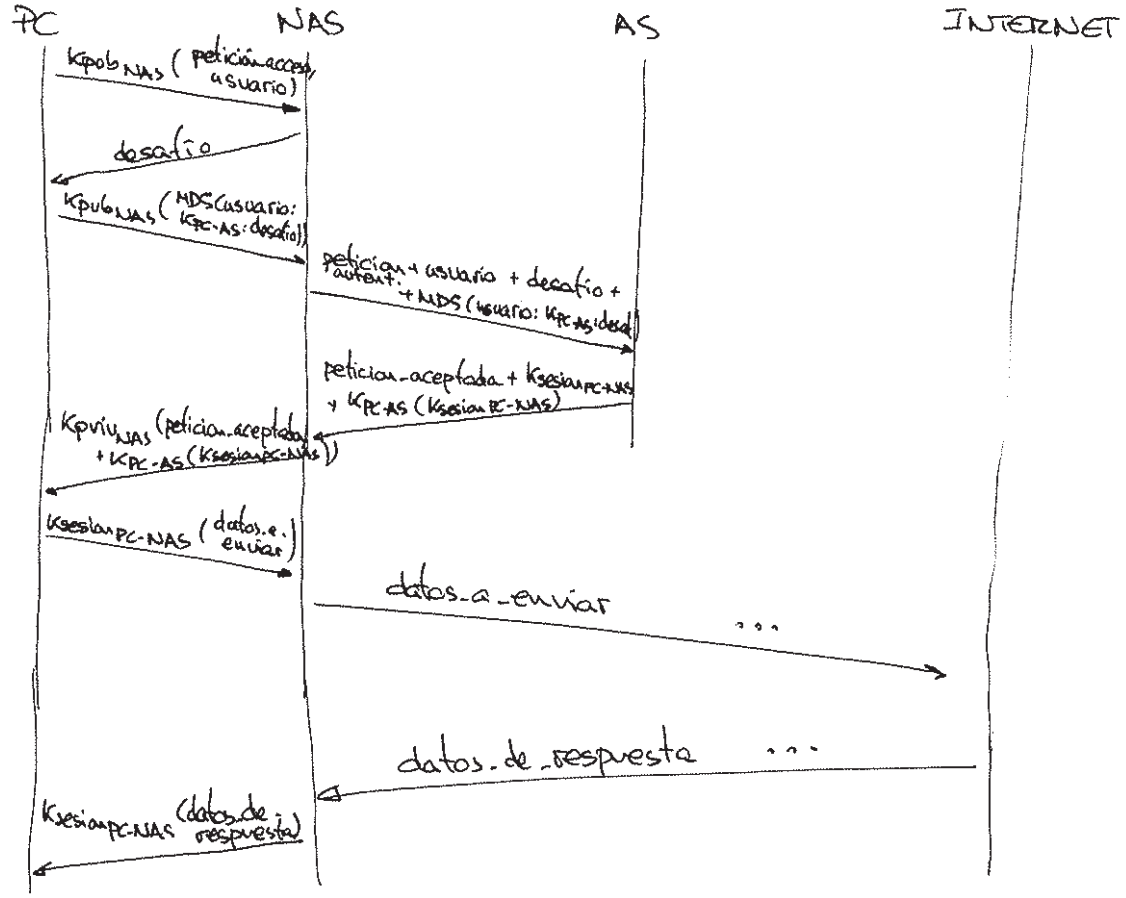
EXAMEN TDRC2 SEPTIEMBRE 2010

Ejercicio 1



Resumen: el PC se quiere conectar a Internet a través del NAS, que lo autentica con los datos del servidor de autenticación.

Mensajes intercambiados:



Las claves públicas están disponibles y son válidas gracias a la existencia de una entidad superior confiable (anunciada).

a) Servicios de seguridad proporcionados b) Debilidades

* Privacidad:
  - ⇒ PC envía todo cifrado al NAS, ya sea con su clave pública (sólo puede descifrarlo el NAS) o con la clave de sesión que ambos comparten (asignada por el AS).
  - ⇒ NAS no cifra el desafío (posible ataque por repetición si se repiten desafíos). Además, el mensaje de "petición aceptada" y los "datos de respuesta" sólo (1)

van cifrados con su clave privada, por lo que cualquiera podría descifrarlos con su clave pública (conocida por todos). Aunque los datos sensibles sí van cifrados (e.g. la clave de sesión) adecuadamente, alguien en la red de acceso podría ver que el usuario se ha conectado.

⇒ Igual ocurre entre NAS y AS, nada va cifrado para conseguir la confidencialidad. Aunque pertenece a la red interna del operador, un trabajador podría ver la clave de sesión y pensar algún tipo de ataque, e.g. suplantación de PC.

⇒ Por último, los datos a enviar/recibir hacia/desde Internet van cifrados con la clave de sesión entre el PC y el NAS, de forma que alguien en la red de acceso no los podría leer. Sin embargo, los datos van sin cifrar por Internet, algo lógico ya que, en general, no se sabe el destino de esos datos, si soporte cifrado, etc (este último punto es necesario para las aplicaciones típicas, que van sin cifrar).

* Integridad: No se utilizan compendios/resúmenes, por lo que no es posible comprobar si los datos han sido modificados.

  NOTA: El uso de MD5() en el esquema propuesto es para no enviar la clave en texto plano. No tiene nada que ver con la integridad (no es el resumen del mensaje).

* Autenticación:

  ⇒ PC está solicitando su autenticación al NAS a través de un AS remoto. Dado que el procedimiento requiere que conozca su clave secreta compartida con el AS (K_{PC-AS}), queda autenticado al final del procedimiento.

⇒ El NAS inicialmente no se autentica (no usa su $K_{priv_{NAS}}$ para que el PC sepa que realmente es el NAS). Ahí podría ser suplantado y el PC no lo notaría (e.g. un atacante para conseguir muchos pares desafío ↔ MD5(...)).
Sin embargo, sí se autentica al enviar la "petición aceptada" cifrada con su clave privada (sólo pudo cifrarlo el NAS). En el envío/recepción de datos tampoco se autentica (aunque debe conocer la clave de sesión).

⇒ El NAS y el AS no se autentican entre ellos. Alguien podría suplantar al NAS y el AS no se daría cuenta. Y obtendría la clave de sesión (si bien no se la podría mandar al PC ya que no conocería la $K_{priv_{NAS}}$ del auténtico NAS).

* No repudio:

Únicamente el mensaje "conexión aceptada" (o rechazada) va cifrado con la clave privada del NAS (sólo la conoce él → → sólo ha podido cifrarlo él → me sirve de prueba de que estuvo en la transacción). El resto de mensajes no lleva ningún tipo de firma digital → no es demostrable que una entidad los envió/recibió.

Así, el usuario sólo tiene "no repudio" de que su conexión ha sido aceptada o rechazada.

* Disponibilidad: con la información que tenemos no se puede garantizar nada (no sabemos si hay líneas de backup, ni la configuración de TCP/IP ante ataques, ...).

b) Vulnerabilidades y soluciones.

Las vulnerabilidades se han ido comentando en el apartado anterior. Las soluciones:

→ Privacidad: por ejemplo, ~~usando~~ cifrando todos los mensajes con la clave pública del receptor (en ese caso, AS y PC han de tener sus parejas de clave pública - privada).

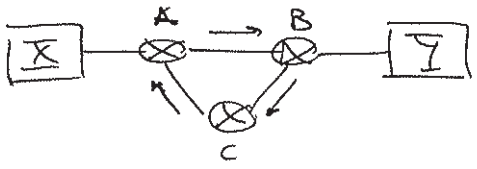
→ Integridad: usando compendios del mensaje mediante funciones hash (e.g. MD5, SHA-1). Esos compendios sirven para comprobar si el mensaje ha sido modificado.

→ Autenticación: por ejemplo, cifrando todos los mensajes con la clave privada del emisor. Al menos NAS y AS deberían hacerlo (el usuario ya se autentica durante el procedimiento).

→ No repudio: idem, cifrando con la clave privada del emisor cada mensaje. O con algún otro tipo de firma digital.

→ Disponibilidad: tareas de backup, igual que NAS y AS duplicados, comprobar que no se es susceptible de ataques de denegación de servicio, etc.

Ejercicio 2 Envío de 20 segmentos TCP entre X e Y.



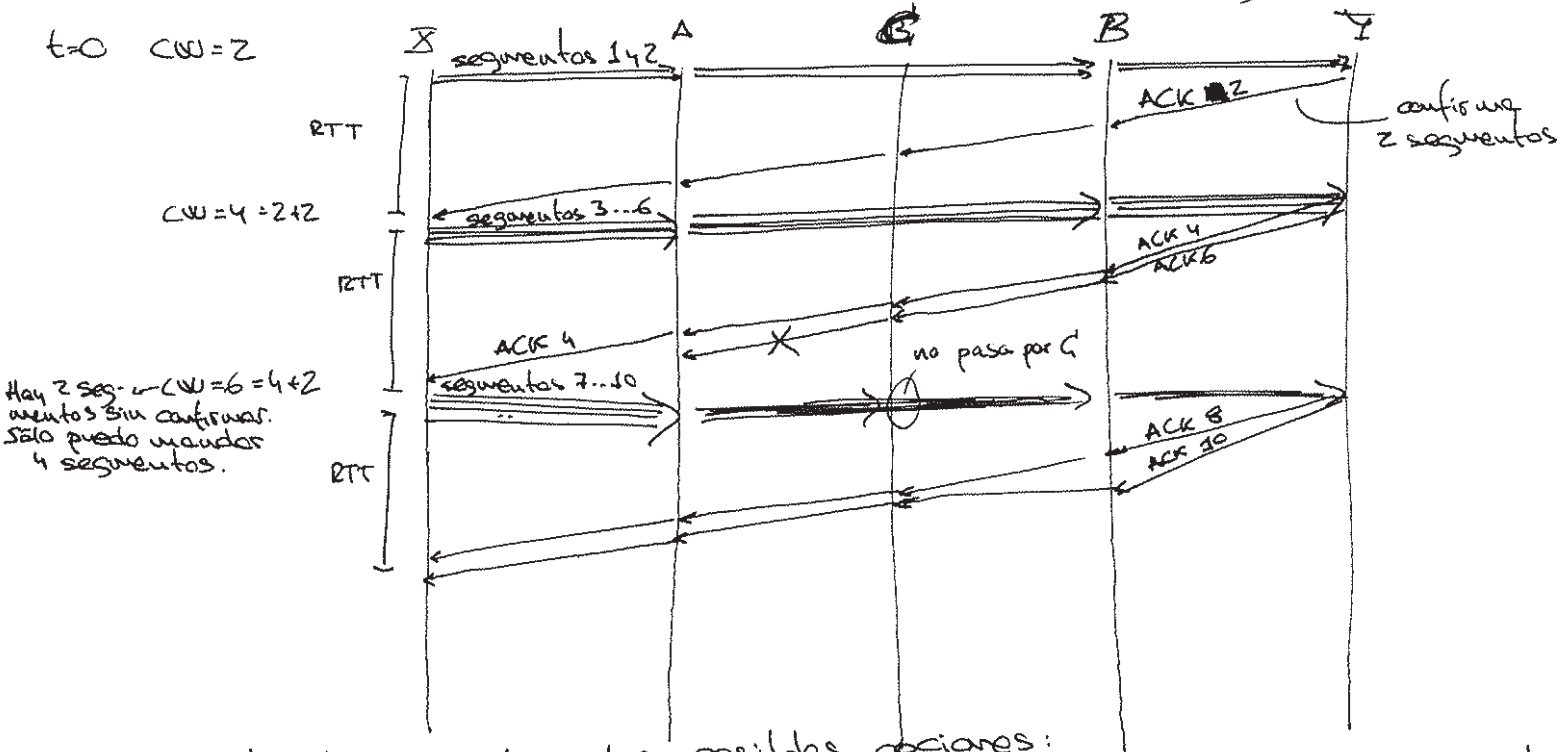
a) Secuencia de segmentos (sin incluir el establecimiento y el cierre de la conexión TCP).

b) Tiempo tardado

Datos del enunciado:

- CWini = 2 MSS
- No hay problemas de flujo ni de congestión
- Se pierde la 3ª de cada tres tramas en el enlace A→C.
- Rutas asimétricas: X → A → B → Y
  Y → B → C → A → X
- Tiempo de emisión por interfaces despreciable (eg. 1 Gbps)
- RTT = 100 ms
- Timeout = 200 ms

NOTA: suponemos TCP Tahoe y que el umbral empieza con un valor muy alto.



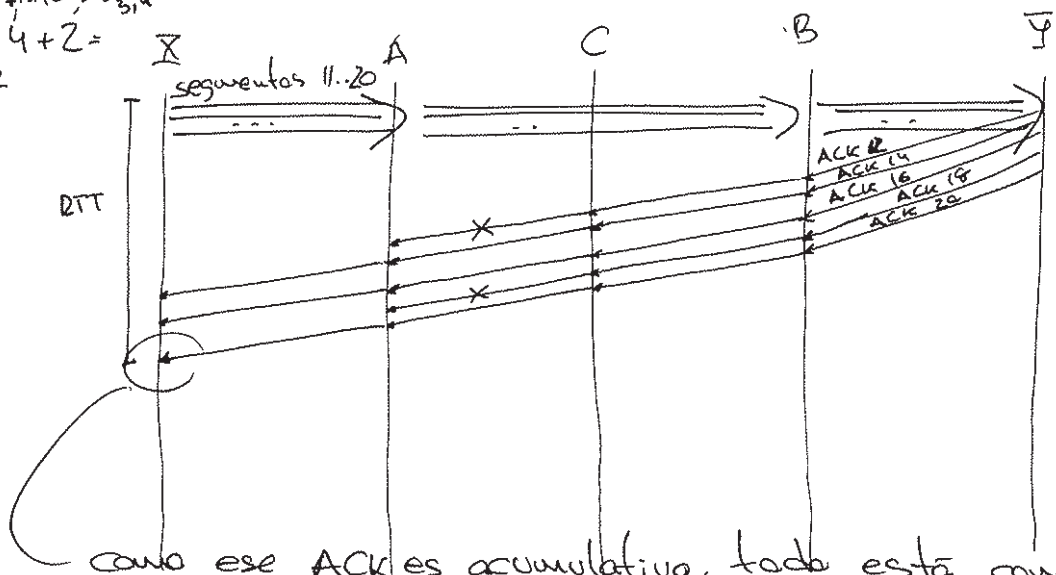
A partir de aquí hay dos posibles opciones:

Opción A Suponemos que "ACK 8" llega justo antes que el timeout de los segmentos 3 y 4 ($2 \times RTT = 200$ ms, que coincide con el valor del timeout).

Opción B Suponemos que "ACK 8" llega justo después que el timeout de los segmentos 3 y 4. Esta es más realista, ya que, aunque el tiempo de emisión por los interfaces es despreciable, será superior a 0.

Opción A → no hay timeout, llegan ACKs (acumulativos) antes de que se produzcan.

CW = 6 + 4 + 2 = 12 (segmentos 7..10, segmentos 3,4)



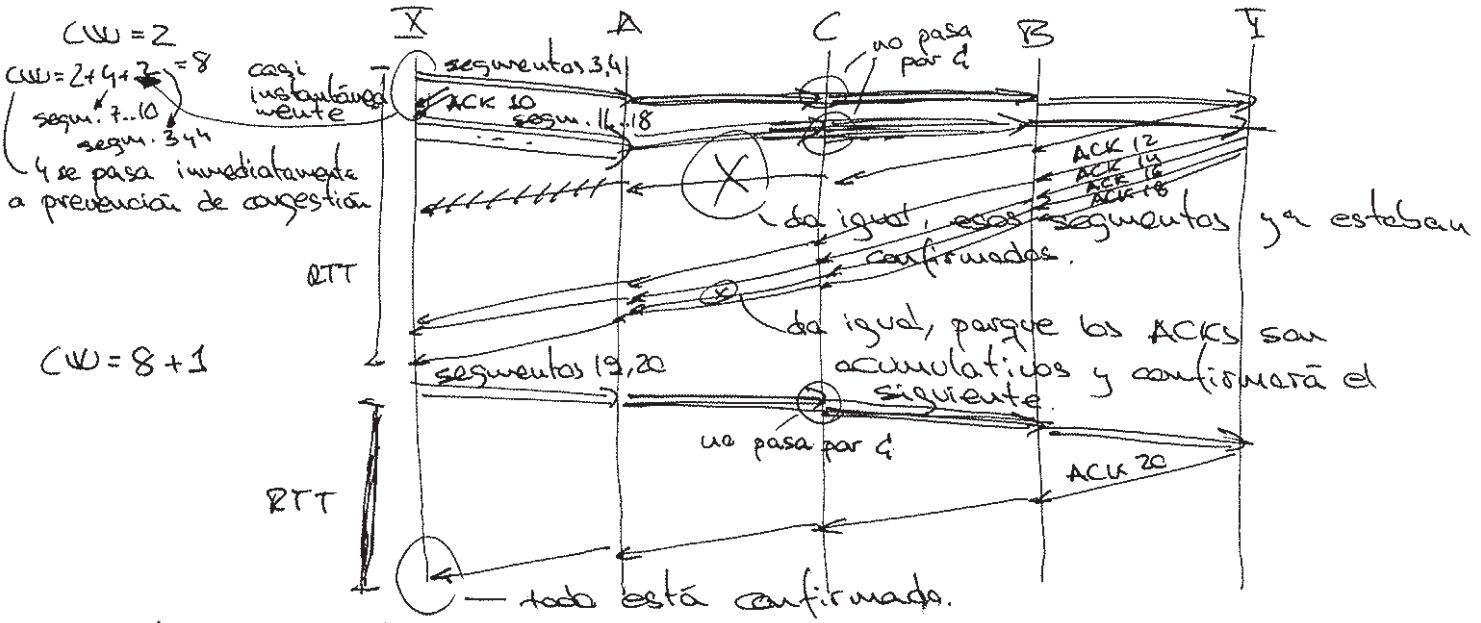
como ese ACK es acumulativo, todo está confirmado y termina ahí la comunicación. El tiempo empleado será:

$T_{transmisión} = 4 \times RTT = 400\ ms$

Opción B → hay un timeout al no llegar el ACK de los segmentos 3 y 4.

TIMEOUT (supuestos Tahoe) ⟹ $CW = CW_{ini} = 2$

$umbral = \frac{CW_{anterior}}{2} = 3$



El tiempo total será:

$T_{transmisión} = 5 \times RTT = 500\ ms$

Ejercicio 3

Un ordenador con 3 navegadores conectados al mismo servidor (IP 147.156.1.4). ¿Cuántos sockets y conexiones TCP hay implicadas?

CLIENTES:

→ Cada navegador tendrá un socket por el que se establece la conexión y después se envían/reciben los datos → 3 conexiones TCP y 3 sockets. (cada uno con

SERVIDOR:

→ Escuchará peticiones de establecimiento de conexión TCP en un socket fijo, el mismo para todos los clientes.

→ Y abrirá un socket nueva para enviar/recibir datos por parte de un cliente → 3 sockets y 3 conexiones TCP.

→ Total en el servidor: 4 sockets y 3 conexiones TCP.

Ejercicio 4 Campo TTL de los RR (registros de recursos) de un paquete DNS.

TTL = Time-to-Live. Es el tiempo que un DNS guarda la información que le pasa otro DNS en su caché. Después de ese tiempo la entrada se borra, ya que no se considera válida.

Ejercicio 5 Una empresa tiene 5 departamentos, cada uno con una subred con direcciones privadas. Encuentre al menos dos errores cometidos por el Administrador.

Dpto 1: 192.168.0.0/25
Dpto 2: 192.168.0.128/27
Dpto 3: 192.168.0.160/26
Dpto 4: 192.169.0.0/25
Dpto 5: 192.169.0.128/25

Error 1: 192.169.0.0 (y consecutivas) es una dirección de red PÚBLICA, no privada como se pedía → MAL las subredes de los departamentos 4 y 5.

Error 2: La subred del Dpto 3 está mal definida y se solapa con la subred del Dpto 2.

192.168.0.160/26 → 26 bits de subred, 6 bits de equipo
(24 bits)

10100000
(bits de subred) (bits de equipo)

La dir. de subred real sería la dirección con todos los bits de equipo a cero =>
=> 192.168.0.128/26 →
desde 192.168.0.128 ... [redacted] 191
=> Se solapa con la subred del Departamento 2.