Preguntas y Respuestas

Un compendio de preguntas desarrolladas paso a paso.

Autor: Ismael Sallami Moreno
Fecha: January 19, 2025

Contents

1. Pregunta 1

1.1 Enunciado

Contestar las siguientes preguntas usando exclusivamente los huecos reservados.

P1 (1 punto sobre 10) Enumere las diferencias y similitudes entre los protocolos HTTP y IMAP.

1.2 Solución

Diferencias:

- HTTP se utiliza para solicitar y servir páginas web y IMAP para recepción de e-mails.
- HTTP es *stateless* e IMAP no.
- HTTP puede ser persistente o no. IMAP no es ni persistente ni no persistente.
- HTTP usa puerto 80, IMAP puerto 143.
- HTTP usa cookies, IMAP no.
- HTTP gestiona proxies/cache, IMAP no.
- IMAP es orientado a conexión, HTTP no.

Similitudes:

- Son orientados a texto.
- No son seguros/no proporcionan confidencialidad.
- Son cliente/servidor.
- Usan TCP.
- Son de la capa de aplicación.
- Son *in-band*.
- Ambos usan extensiones MIME.

2. Pregunta 2

2.1 Enunciado

P2 (1,5 puntos sobre 10). Explique cómo funciona el control de errores en TCP. ¿Qué parámetro es fundamental en el rendimiento del control de errores y cómo se adapta durante una conexión?

2.2 Solución

TCP numera todos los segmentos y exige confirmaciones ACK positivas y acumulativas con *piggyback*. El emisor guarda una copia local de cada segmento enviado en la ventana de emisión e inicia un temporizador. Si el temporizador expira, el emisor vuelve a retransmitir el segmento correspondiente. Además, el emisor calcula un *checksum* (un código de paridad) por cada segmento, que se añade en la cabecera para que el receptor pueda descartar errores simples.

El receptor habilita una ventana de recepción abierta para los números de secuencia que espera recibir. Si se recibe un segmento con un número de secuencia fuera de la ventana de recepción, el segmento se descarta. Si el segmento recibido está dentro de la ventana de recepción, se acepta y, si llega en orden y sin errores, se pasa a la aplicación y se confirma. En régimen estacionario, TCP confirma acumulativamente de 2 en 2 segmentos, aunque puede

confirmar segmentos aislados tras esperar 500 milisegundos a que llegue otro segmento contiguo.

Si se recibe un segmento desordenado pero sin errores, se almacena temporalmente en la ventana de recepción; no se pasa a la aplicación, pero se confirma el último segmento correctamente recibido. [Aquí habría que explicar bien los casos para la generación de ACKs vistos en teoría.] Tenemos el caso normal, el caso de duplicados, el caso fuera de orden/desordenados y (retrasados) y envíos simultáneos.

El parámetro fundamental que impacta en el rendimiento es el *timeout* del emisor. Este habilita un temporizador por cada segmento enviado, y por cada ACK recibido estima el RTT (*Round Trip Time*) como una media móvil:

$$RTT_{\text{Estimado}} = \alpha \cdot RTT_{\text{Old}} + (1 - \alpha) \cdot RTT_{\text{Medido}}, \quad \alpha \text{ y } \beta \in [0, 1]$$

$$Error_{\text{Estimado}} = \beta \cdot Error_{\text{Old}} + (1 - \beta) \cdot |RTT_{\text{Estimado}} - RTT_{\text{Medido}}|$$

Finalmente, se calcula el *TIMEOUT* como:

$$TIMEOUT = RTT_{\text{Estimado}} + 4 \cdot Error_{\text{Estimado}}$$

Para evitar ambigüedades, cuando se produce un *timeout*, el algoritmo de Karn especifica que el *TIMEOUT* se debe doblar.

3. Pregunta 3

3.1 Enunciado

P3 (1,5 puntos sobre 10). A y B no se conocen y quieren intercambiar mensajes a través de un canal no seguro. Suponga que disponen de certificados digitales expedidos por una autoridad de confianza.

A) Explique el procedimiento para autenticarse mutuamente identificando claramente los mensajes que deban intercambiar. ¿Qué es y qué debe contener el certificado digital?

B) Si no dispusieran de certificados, pero sí de una clave secreta compartida, ¿cómo podrían autenticarse? Identifique claramente los requisitos y posibles debilidades.

3.2 Solución

A) Para autenticarse mutuamente:

- A envía a B un mensaje cifrado con su clave privada ($K_{\text{PRIV\_A}}$).
- B hace lo mismo hacia A, cifrando con su clave privada ($K_{\text{PRIV\_B}}$).

El certificado digital es la asociación fehaciente e irrevocable de una entidad A con su clave pública. Debe contener:

- La identidad de A.
- Su clave pública.
- Una fecha de expiración (validez).

Todo esto está cifrado con la clave privada de una autoridad reconocida ($K_{\text{PRIV\_AUT}}(A, K_{\text{PUB\_A}}, \text{validez})$).

En este caso, A y B quedan autenticados bajo la hipótesis de que las claves privadas son conocidas únicamente por las entidades correspondientes, y el uso del certificado garantiza que la autoridad asocia fehacientemente a la entidad con su clave pública y, por ende, con su clave privada.

B) Si disponen de una clave secreta compartida, pueden autenticarse utilizando un esquema de *reto-respuesta*:

- Es necesario tomar medidas para evitar ataques por reflexión, utilizando conjuntos de retos disjuntos.
- También deben emplearse marcas de tiempo (*nonce*) para prevenir ataques por repetición.

Las debilidades de este esquema incluyen:

- Dependencia de la seguridad de la clave secreta compartida.
- Vulnerabilidad frente a ataques de sincronización si los retos y las marcas de tiempo no son correctamente gestionados.

4. Pregunta 1

4.1 Enunciado

Contestar las siguientes preguntas usando exclusivamente los huecos reservados.

P1 (1 punto sobre 10). ¿Qué es la congestión en la red? ¿Dónde se origina?

4.2 Solución

La congestión en la red se origina en los *routers* y se produce por el desbordamiento de los *buffers* de los mismos. Si llegan demasiados paquetes para que puedan ser servidos (e.g., porque la capacidad de procesamiento no sea elevada, o porque los interfaces de salida no sean lo suficientemente rápidos para reenviar todos los paquetes entrantes), los *buffers* donde se guardan antes de ser encaminados se llenan hasta que se desbordan, provocando que no lleguen a su destino.

Los protocolos de transporte fiables como TCP tienen mecanismos para reducir la velocidad cuando detectan que hay congestión (e.g., por pérdidas de ACKs en el caso de TCP Tahoe).

5. Pregunta 2

5.1 Enunciado

P2 (1.5 puntos sobre 10).

a) Explique los mensajes que se generarían en la resolución del dominio www.ejemplo.jp con el protocolo DNS suponiendo que .jp ha delegado la autoridad a .ejemplo.
b) ¿Qué significa ser la autoridad de una zona?
c) ¿Qué significa delegar la autoridad?

5.2 Solución

a) El cliente DNS tiene configurada la IP de su DNS local (DNS1), al que le mandaría un *DNS query* preguntando por la IP de www.ejemplo.jp. Suponiendo que no tiene esa información (ni en su base de datos ni en su caché) y que la resolución es recursiva (también sería válido explicar la solución con resolución iterativa), el DNS local reenvía la *DNS query* a un DNS raíz (DNS2).

Este, a su vez, reenvía la petición al DNS responsable del dominio .jp (DNS3). Como este delegó la autoridad de ejemplo.jp a otro DNS, le reenvía a este último la solicitud (DNS4).

DNS4 tiene la información en su base de datos (es autoridad de esa zona), por lo que envía un *DNS query response* con la respuesta (la IP de www.ejemplo.jp) a DNS3, este a DNS2, este a DNS1 y este, finalmente, al cliente DNS.

b) Un servidor con autoridad (*SOA, Start of Authority*) es un servidor al que le han delegado la responsabilidad de una zona (conjunto de nombres de dominio consecutivos) y tiene toda la información de su zona en su base de datos (no en su caché).

c) Un servidor DNS con autoridad en una zona (conjunto de nombres de dominio consecutivos) puede ceder la autoridad de una subzona a otro servidor DNS, que se convertirá en autoridad de dicha subzona.

6. Pregunta 3

6.1 Enunciado

P3 (1,5 puntos sobre 10). Explique y justifique todas las propiedades (o aspectos) de seguridad que se garantizan si para enviar el mensaje T, una entidad A envía a B:

$$\text{DES}_{K\text{-SECRETA}}\left[K_{\text{PRI\_A}}\left(\text{MD5}(T)\right) + T\right] + K_{\text{PUB\_B}}(K\text{-SECRETA})$$

Siendo:

- K-SECRETA una clave secreta.
- $K_{\text{PUB\_B}}(\cdot)$ el cifrado usando la clave pública de B.
- $\text{MD5}(\cdot)$ una función hash o compendio.
- $K_{\text{PRI\_A}}(\cdot)$ el cifrado usando la clave privada de A.
- $\text{DES}_{K\text{-SECRETA}}[\cdot]$ el cifrado usando DES con la clave K-SECRETA.
- $+$ concatenar o unir.

6.2 Solución

El mensaje T incluye varias partes:

1. **Envío de la clave secreta K-SECRETA cifrada con la clave pública del receptor $K_{\text{PUB\_B}}$:**
   - Como solo B puede descifrarlo (es el único que conoce su clave privada), se garantiza la confidencialidad en la distribución de esta clave secreta.
   - No se incluye un resumen o compendio de esta parte con una función hash, por lo que no se garantiza la integridad.
   - Tampoco se garantiza el no repudio, ya que no hay ninguna prueba de que A haya enviado esta parte ni que B la haya recibido.
2. **Primera parte del mensaje cifrada con DES usando K-SECRETA:**
   - Esta parte incluye T y su resumen $\text{MD5}(T)$, ambos cifrados con la clave privada del emisor $K_{\text{PRI\_A}}$.
   - Garantías proporcionadas:
     (a) **Integridad:** Gracias al resumen $\text{MD5}(T)$, se puede comprobar si el texto ha sido modificado.
     (b) **Autenticación:** Como la información está cifrada con la clave privada de A, B puede verificar que proviene de A al descifrarlo con la clave pública de A.
   - Limitaciones:

- La autenticación no es completa porque no hay garantía de que B sea el dueño real de $K_{\text{PUB\_B}}$.
- No se garantiza el no repudio porque no se indica la presencia de una entidad fiable que asegure la asociación entre la identidad de A y su clave pública (e.g., mediante un certificado digital).

Propiedad indirecta: Como la clave secreta es necesaria para descifrar la primera parte y esta incluye un resumen que permite verificar la integridad del texto T, indirectamente se garantiza la integridad de la clave secreta. Si la clave secreta cifrada con $K_{\text{PUB\_B}}$ estuviera comprometida, no sería posible descifrar correctamente la primera parte y validar la integridad del mensaje.

Resumen: Este mensaje garantiza:

- Confidencialidad en la distribución de la clave secreta K-SECRETA (e indirectamente integridad).
- Confidencialidad, autenticación e integridad del texto T.

7. Pregunta 1

7.1 Enunciado

PREGUNTA 1 (1.5 puntos sobre 10)

a) ¿Qué es una máscara de red?
b) ¿Para qué se usa?
c) ¿Por qué se usa?

7.2 Solución

a) Una máscara de red es un conjunto de bits que se utiliza en redes IP para dividir una dirección IP en dos partes: la parte de red y la parte de host.

b) Se usa para determinar qué porción de una dirección IP identifica la red y qué porción identifica a los dispositivos (hosts) dentro de esa red. Esto se logra mediante una operación lógica AND entre la dirección IP y la máscara de red.

c) Se usa para facilitar la organización, administración y enrutamiento de las redes. Permite identificar qué direcciones IP están dentro de una misma subred, optimizando la comunicación local y minimizando el tráfico innecesario hacia otras redes.

8. Firma Digital usando Clave Secreta y Big Brother

8.1 Enunciado

Explique el procedimiento y los mensajes intercambiados en una firma digital usando clave secreta y Big Brother.

8.2 Solución

En este caso, se está describiendo un proceso de firma digital utilizando una clave secreta (clave simétrica) y una entidad llamada ”Big Brother” (que puede representar a una autoridad de confianza o un tercero involucrado en la validación).

El procedimiento de firma digital utilizando clave secreta y Big Brother puede implicar los siguientes pasos y mensajes intercambiados:

1. **Generación del mensaje a firmar:**
   - A (la entidad que desea firmar el mensaje) genera un mensaje M que desea firmar.
2. **Cálculo del hash del mensaje:**
   - A calcula un valor hash del mensaje M, denotado como $H(M)$, usando una función hash adecuada (e.g., SHA-256).
3. **Cifrado del hash con la clave secreta:**
   - A utiliza una clave secreta K_{SECRETA} para cifrar el valor hash $H(M)$. Este cifrado produce la firma digital $S = \text{DES}_{K_{\text{SECRETA}}}(H(M))$.
4. **Envió del mensaje y la firma a Big Brother:**
   - A envía el mensaje M junto con la firma digital S a la entidad Big Brother para su validación.
5. **Validación por Big Brother:**
   - Big Brother recibe el mensaje M y la firma S.
   - Big Brother utiliza la clave secreta K_{SECRETA} para descifrar la firma y obtener el valor $H(M)$.
   - Big Brother calcula el hash del mensaje M (denotado $H'(M)$) y compara el resultado con el valor $H(M)$ obtenido de la firma.
6. **Resultado de la validación:**
   - Si $H(M) = H'(M)$, Big Brother confirma que la firma es válida, lo que significa que el mensaje M no ha sido alterado y que A es el autor del mensaje.
   - Si los valores no coinciden, la firma se considera inválida y Big Brother notifica el fallo.

En resumen, la firma digital usando clave secreta y Big Brother proporciona integridad del mensaje (gracias al hash) y autenticación (gracias a la firma). Big Brother actúa como una autoridad que valida que la firma digital corresponde al mensaje original.

9. Pregunta 3

9.1 Enunciado

Usando un dibujo, muestre y explique un escenario en el que dos agentes de usuario (MUA) de correo (origen y destino), situados en dominios distintos, envían y reciben respectivamente un correo electrónico. Suponga una situación inicial en la que todas las cachés están vacías. Identifique TODOS los servidores y entidades involucradas, así como los mensajes intercambiados en los protocolos de la capa de transporte y aplicación.

9.2 Solución

El escenario puede ser representado mediante un diagrama que incluye las siguientes entidades y procesos:

1. **Agentes de Usuario de Correo (MUA):** El agente de usuario de origen envía el correo y el de destino lo recibe.
2. **Servidor de Envío de Correo (MTA Origen):** El MUA de origen utiliza el protocolo SMTP para enviar el correo al MTA de su dominio.
3. **Servidor de Recepción de Correo (MTA Destino):** El MTA de destino utiliza el protocolo SMTP para recibir el correo del MTA de origen.

4. **Servidor de Almacenamiento de Correo:** Una vez recibido, el correo es almacenado para su recuperación por el MUA de destino mediante protocolos como POP3 o IMAP.

Proceso y Mensajes Intercambiados:

1. El MUA de origen envía el mensaje al MTA de su dominio utilizando el protocolo SMTP (comandos como HELO, MAIL FROM, RCPT TO, DATA).
2. Si las cachés están vacías, el MTA de origen realiza una consulta DNS para obtener la dirección del MTA de destino (incluye consultas para registros MX y A).
3. El MTA de origen establece una conexión con el MTA de destino utilizando el protocolo SMTP e intercambia mensajes para transferir el correo.
4. El MTA de destino almacena el correo en el servidor de almacenamiento.
5. El MUA de destino recupera el correo utilizando POP3 o IMAP.

Descripción del Dibujo:

- Dos dominios (Origen y Destino) representados como bloques.
- Dentro del dominio de origen:
  - Un MUA.
  - Un MTA.
  - Un servidor DNS.
- Dentro del dominio de destino:
  - Un MTA.
  - Un servidor de almacenamiento de correo.
  - Un MUA.
- Flechas que representen las conexiones y los protocolos utilizados:
  - Entre el MUA de origen y el MTA de origen (SMTP).
  - Entre el MTA de origen y el servidor DNS (consultas MX/A).
  - Entre los MTA de origen y destino (SMTP).
  - Entre el servidor de almacenamiento de correo y el MUA de destino (POP3 o IMAP).

10. Pregunta 1

10.1 Enunciado

Con la ayuda de la figura explique cómo funciona NAT. Suponga que se envía un paquete del cliente al servidor y este contesta. Muestre los siguientes campos de los mensajes intercambiados: IP origen, IP destino, puerto origen y puerto destino.

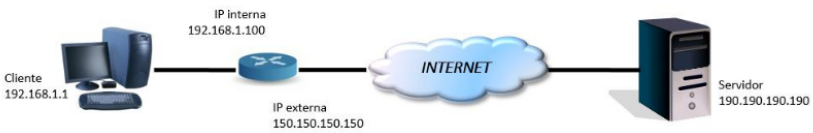


Figure 1: Ejemplo de NAT.

10.2 Solución

10.2.1 Explicación de NAT

El **Network Address Translation (NAT)** permite traducir direcciones IP privadas a direcciones IP públicas (y viceversa) para habilitar la comunicación entre una red interna y una red externa,

como Internet.

- **SNAT (Source NAT):** Se utiliza cuando un cliente está en la red privada y necesita comunicarse con un servidor en Internet. La dirección IP privada y el puerto de origen del cliente se traducen a la dirección IP pública del router y un puerto asignado dinámicamente por el router. Esto asegura que múltiples clientes de la red privada puedan compartir la misma dirección IP pública.
- **DNAT (Destination NAT):** Se utiliza cuando un cliente externo necesita acceder a un servidor en la red privada. La dirección IP pública y el puerto de destino del paquete se traducen a la dirección IP privada y el puerto del servidor en la red interna.

10.2.2 Ejemplo de Traducción con Tabla

Supongamos una red con los siguientes elementos:

- IP privada del cliente: 192.168.1.100
- Puerto privado del cliente: 5000
- IP pública del router: 203.0.113.1
- Puerto asignado dinámicamente por SNAT: 60001
- IP privada del servidor: 192.168.1.200
- Puerto privado del servidor: 80
- IP pública del servidor visible en Internet (tras DNAT): 203.0.113.2

Tipo de NAT	IP y Puerto de Origen	IP y Puerto de Destino	Traducción
SNAT	192.168.1.100:5000	198.51.100.10:80	203.0.113.1:60001 → 198.51.100.10:80
DNAT	203.0.113.2:80	192.168.1.200:80	203.0.113.2:80 → 192.168.1.200:80

Table 1: Ejemplo de traducción con SNAT y DNAT

Nota: En SNAT, el puerto de origen se traduce para evitar conflictos si varios clientes de la red privada usan el mismo puerto. En DNAT, la dirección pública y el puerto son mapeados al servidor interno correspondiente.

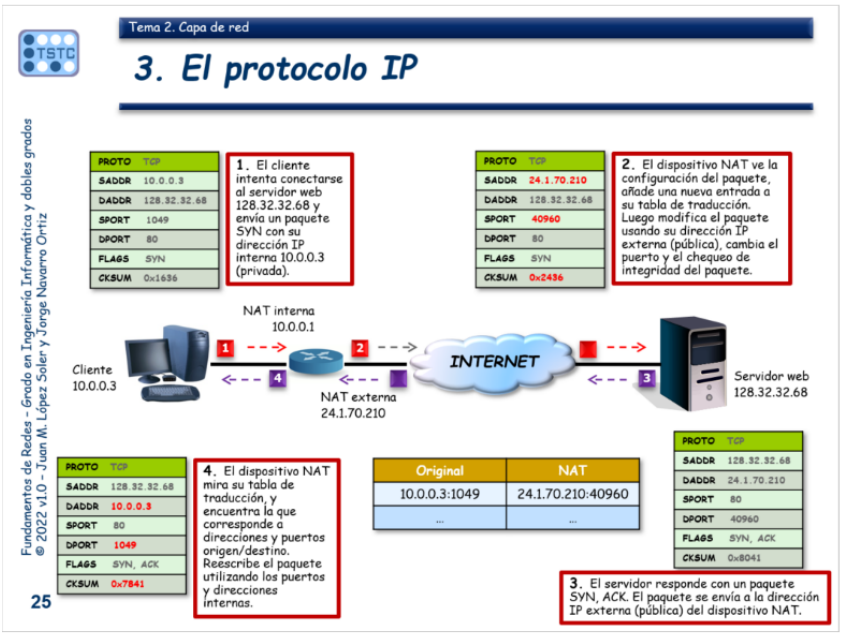


Figure 2: Ejemplo de NAT con traducción de direcciones IP y puertos.

11. Pregunta 2

11.1 Enunciado

Muestre con un ejemplo el uso de cifrado asimétrico (KPUB_A / KPRIV_A y KPUB_B / KPRIV_B) para garantizar el no repudio en una transmisión entre A y B. Explique qué requisitos deben cumplir las claves para asegurar el no repudio. Justifique su respuesta.

11.2 Solución

El ejemplo de cifrado asimétrico para garantizar el no repudio en una transmisión entre A y B es el siguiente:

1. El usuario A desea enviar un mensaje a B y garantizar el no repudio. Para ello:
   - A genera un hash del mensaje (por ejemplo, utilizando SHA-256).
   - A cifra el hash del mensaje utilizando su clave privada $KPRIV\_A$, generando una firma digital.
   - A envía a B el mensaje original junto con la firma digital.
2. Cuando el usuario B recibe el mensaje:
   - B utiliza la clave pública de A $KPUB\_A$ para descifrar la firma digital y obtener el hash original generado por A.
   - B calcula nuevamente el hash del mensaje recibido y lo compara con el hash obtenido de la firma digital.
   - Si ambos hashes coinciden, se asegura que el mensaje fue enviado por A y no ha sido modificado, garantizando el no repudio.

Requisitos de las claves para garantizar el no repudio:

- La clave privada $KPRIV\_A$ debe ser conocida únicamente por A y estar protegida contra accesos no autorizados.

- La clave pública $KPUB\_A$ debe ser accesible públicamente y estar asociada de manera verificable con la identidad de A.
- Un tercero confiable (como una autoridad certificadora) debe garantizar la autenticidad de la clave pública $KPUB\_A$, vinculándola con A mediante un certificado digital.

Justificación: El no repudio se logra porque únicamente A, como poseedor de $KPRIV\_A$, puede haber generado la firma digital. Si B puede verificarla con $KPUB\_A$, queda garantizado que A fue el emisor del mensaje. Adicionalmente, el uso de un hash asegura que cualquier alteración en el mensaje original invalidará la firma, proporcionando integridad.

11.3 Solución propia del examen y de las diapositivas

Respuesta sencilla: usar doble cifrado (véase la transparencia debajo) y faltaría incluir que es necesario garantizar la relación entre la identidad del emisor y su clave pública. Para ello, necesitamos una entidad en la que todos confiemos y que lo garantice → eso es precisamente lo que hacen los certificados digitales, incluyen la identidad, la clave pública, más datos, y lo firman todo con la clave privada de la autoridad de certificación (en quienes todos confían). Con eso se consigue el no repudio. Se debería incluir también un resumen (hash) para conseguir integridad, algo necesario en la firma digital.

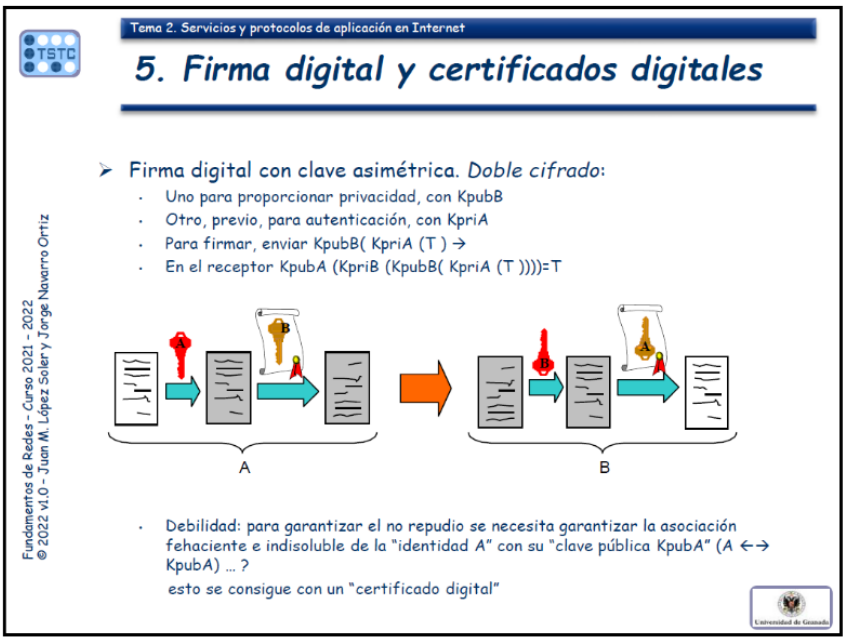


Figure 3: Doble cifrado para garantizar el no repudio.

12. Pregunta 3

12.1 Enunciado

Explique qué condición se debe cumplir entre el tiempo de transmisión, el tiempo de propagación y el tamaño de la ventana de congestión en un emisor TCP para que no haya interrupción (paradas) en la transmisión.

Para que no haya interrupciones, desde que mandamos un paquete hasta que nos llega su ACK debemos estar enviando siempre paquetes (sin que la ventana de congestión, CW, nos

limite).

12.2 Solución

1) **Tiempo desde que mandamos un paquete hasta que llega su ACK:**

$$RTT = 2 \cdot T_t + 2 \cdot T_p$$

donde:

- T_t es el tiempo de transmisión.
- T_p es el tiempo de propagación.

El factor $2 \cdot T_t$ incluye el tiempo necesario para enviar dos paquetes TCP (uno de datos y otro de ACK). Esto evita interrupciones debidas a tiempos adicionales de espera.

2) **Tiempo que tardamos en mandar una ventana entera:**

$$T_{\text{ventana}} = CW \cdot T_t$$

donde:

- CW es el tamaño de la ventana de congestión.
- T_t es el tiempo de transmisión por paquete.

3) **Condición para evitar interrupciones:** Para evitar interrupciones en la transmisión, el tiempo de ida y vuelta (RTT) debe ser menor o igual al tiempo necesario para transmitir una ventana completa:

$$2 \cdot T_t + 2 \cdot T_p \leq CW \cdot T_t$$

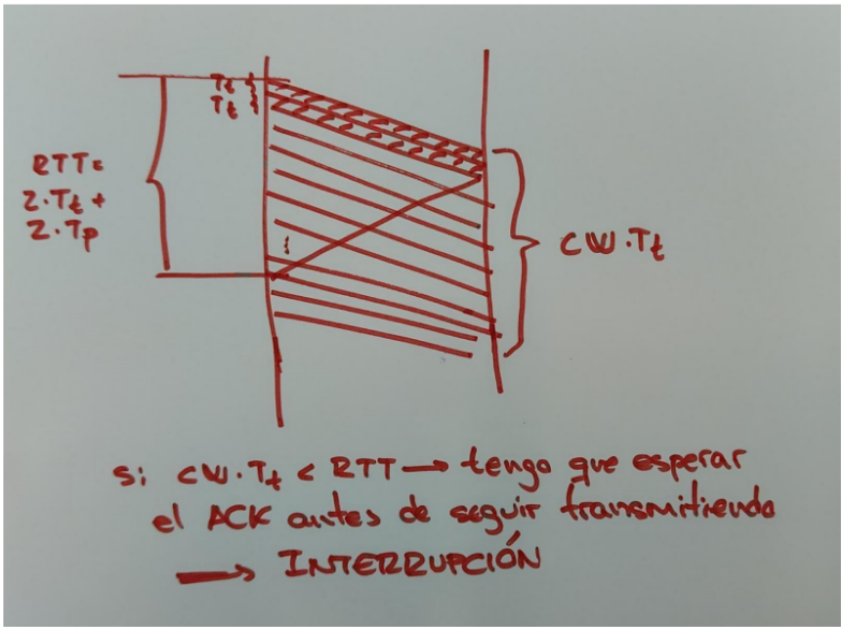
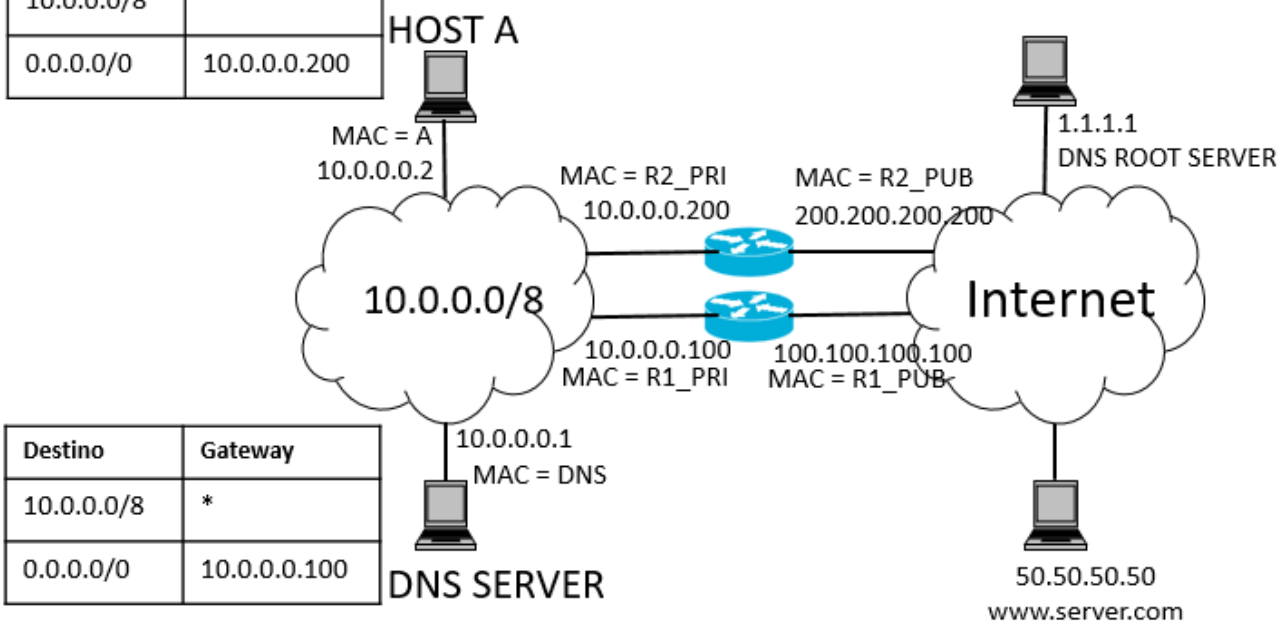


Figure 4: Condición para evitar interrupciones en la transmisión.

EJERCICIO 2 (2 puntos sobre 10)

Con la ayuda de la tabla mostrada en la página 4 del examen, identifique secuencialmente salto a salto todo el tráfico que se generaría en 10.0.0.0/8 y a la salida de los routers, desde que un navegador situado en el **HOST A** solicita la URL http://www.server.com. Complete para cada fila de la tabla todos los campos que sean necesarios. Suponga que todas las tablas ARP están completas y que la cache del DNS SERVER contiene los registros necesarios.

Destino	Gateway
10.0.0.0/8	*
0.0.0.0/0	10.0.0.0.200



Destino	Gateway
10.0.0.0/8	*
0.0.0.0/0	10.0.0.0.100

En la siguiente página se muestra la tabla con las tramas intercambiadas. Algunos aspectos a tener en cuenta:

- Las direcciones MAC cambian salto a salto (origen quien transmite en ese segmento de red, destino quien recibe en ese segmento de red).
- Las direcciones IP son extremo a extremo (origen y destino finales), por lo que no cambian salto a salto. Solo cambian cuando se usa NAT, como es el caso de este ejercicio al pasar de una red privada a una red pública (se usa Source NAT). Cuando se vuelve (respuesta), se deshace dicho cambio de IPs.
- DNS funciona sobre UDP normalmente (también lo puede hacer sobre TCP). Si se usa UDP, que es lo habitual, no hay establecimiento ni cierre de conexión ni se utilizan flags.
- HTTP funciona sobre TCP, por lo que hay establecimiento de conexión (mensajes SYN, SYN+ACK y ACK), tiene confirmaciones (ACKs) y finalmente cierre de conexión (mensajes FIN, FIN+ACK y ACK).
- Los puertos de los clientes son asignados por el sistema operativo, estando por encima de 1024 y siendo en general aleatorios (se van asignando secuencialmente conforme muchos programas piden puertos al sistema operativo, no se puede saber el orden ni el valor a priori). Los puertos de los servidores son los habituales (53 en el caso de DNS, 80 en el caso de HTTP).

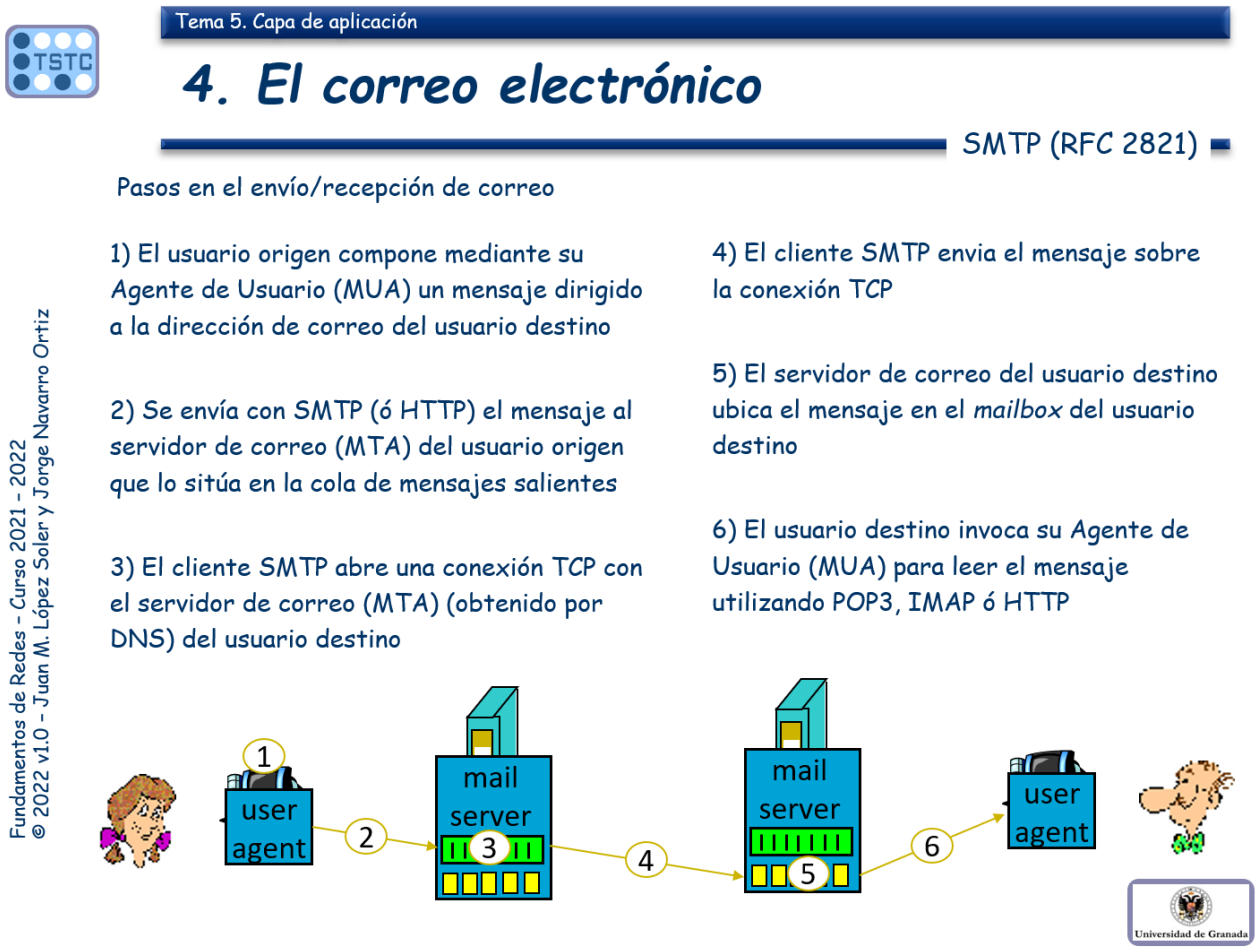
MAC ORIGEN	MAC DESTINO	IP ORIGEN	IP DESTINO	FLAGS	PUERTO ORIGEN	PUERTO DESTINO	MENSAJE	COMENTARIOS
A	DNS	10.0.0.2	10.0.0.1	-	X > 1024	53	CONSULTA DNS www.server.com	La cache de A está vacía. Usa UDP
DNS	A	10.0.0.1	10.0.0.2	-	53	X	RESPUESTA DNS: 50.50.50.50	La cache DNS tiene ese RR se resuelve.
A	R2_PRIV	10.0.0.2	50.50.50.50	SYN=1	Y > 1024	80	SYN DE TCP	Establecimiento de la conexión, #seq
R2_PUB	MAC_NEXT_HOP	200.200.200.200	50.50.50.50	SYN=1	Z > 1024	80	SYN DE TCP	NAT cambia IP y PORT origen
MAC_NEXT_HOP	R2_PUB	50.50.50.50	200.200.200.200	SYN=1, ACK=1	80	Z	SYN+ACK	Llega SYN+ACK al ROUTER NAT
R2_PRIV	A	50.50.50.50	10.0.0.2	SYN=1, ACK=1	80	Y	SYN+ACK	NAT cambia IP y PORT destino
A	R2_PRIV	10.0.0.2	50.50.50.50	ACK=1	Y	80	ACK DE TCP	ACK del HANDSHAKE
R2_PUB	MAC_NEXT_HOP	200.200.200.200	50.50.50.50	ACK=1	Z	80	ACK DE TCP	NAT cambia IP y port ORIGEN
A	R2_PRIV	10.0.0.2	50.50.50.50	-	Y	80	GET de HTTP	Datos TCP con #seq+1
R2_PUB	MAC_NEXT_HOP	200.200.200.200	50.50.50.50	-	Z	80	GET de HTTP	NAT cambia IP y PORT ORIGEN
MAC_NEXT_HOP	R2_PUB	50.50.50.50	200.200.200.200	ACK=1	80	Z	RESPUESTA al GET	Incluye index.html
R2_PRIV	A	50.50.50.50	10.0.0.2	ACK=1	80	Y	RESPUESTA al GET	NAT cambia IP y PORT destino
A	R2_PRIV	10.0.0.2	50.50.50.50	FIN=1, ACK=1	Y	80	FIN de la conexión y ACK del index.html	Llega FIN+ACK al ROUTER NAT
R2_PUB	MAC_NEXT_HOP	200.200.200.200	50.50.50.50	FIN=1, ACK=1	Z	80	FIN de la conexión y ACK del index.html	NAT cambia IP y port ORIGEN
MAC_NEXT_HOP	R2_PUB	50.50.50.50	200.200.200.200	FIN=1, ACK=1	80	Z	FIN de la conexión y ACK	Llega FIN+ACK al ROUTER NAT
R2_PRIV	A	50.50.50.50	10.0.0.2	FIN=1, ACK=1	80	Y	FIN de la conexión y ACK	NAT cambia IP y PORT destino
A	R2_PRIV	10.0.0.2	50.50.50.50	ACK=1	Y	80	ACK para el FIN	Llega ACK al ROUTER NAT
R2_PUB	MAC_NEXT_HOP	200.200.200.200	50.50.50.50	ACK=1	Z	80	ACK para el FIN	NAT cambia IP y PORT ORIGEN

PREGUNTA 1 (1.5 puntos sobre 10)

Si usuario1@lab1.es manda un correo electrónico a usuario2@lab2.es, identifique las entidades involucradas (ponga su nombre completo) para que dicho correo sea leido por el destinatario. Indique los protocolos utilizados entre dichas entidades y las peticiones DNS que realizarían las mismas.

Esta pregunta se responde parcialmente con la siguiente transparencia. A esta habría que añadir que MUA significa Mail User Agent y MTA significa Mail Transfer Agent (está en la primera transparencia sobre correo electrónico). Además, respecto al uso de DNS:

- El MUA de usuario1@lab1.es tiene que hacer una petición DNS preguntando por la IP de su servidor de correo electrónico (dominio lab1.es), cuyo nombre de dominio estará configurado en el propio cliente. Con esa IP, el MUA ya puede conectarse con su MTA y enviar el correo usando SMTP.
- El MTA de lab1.es mirará el destinatario (usuario2@lab2.es) y preguntará a su servidor DNS por el registro MX (Mail eXchange) del dominio lab2.es. Una vez obtenida la IP, se conectará a dicho servidor de correo electrónico y le mandará el mensaje usando SMTP.
- En algún momento, el MUA de usuario2@lab2.es querrá mirar los correos electrónicos recibidos. Para ello, preguntará a su DNS por la dirección IP de su MTA, cuyo nombre de dominio estará configurado en el propio cliente. Con esa IP, el MUA ya puede conectarse con su MTA y descargarse el correo usando POP3 o IMAP.



PREGUNTA 2 (1.5 puntos sobre 10)

Explique lo que son los números de secuencia en los protocolos de la capa de transporte, cómo se determinan y su utilidad.

Inicialmente se puede comentar lo que aparece en la siguiente transparencia (resumiendo la parte de ISN):

3.2. TCP. Control de conexión.

Fundamentos de Redes - Grado en Ingeniería Informática y dobles grados
© 2021 v1.0 - Juan M. López Soler y Jorge Navarro Ortiz

Control de la conexión. Números de secuencia.

- El número de secuencia es un campo de 32 bits que cuenta bytes en módulo 2^{32} (el contador se da la vuelta cuando llega al valor máximo).
- El número de secuencia no empieza normalmente en 0, sino en un valor denominado ISN (Initial Sequence Number) elegido "teóricamente" al azar; para evitar confusiones con solicitudes anteriores.
- El ISN es elegido por el sistema (cliente o servidor). El estándar sugiere utilizar un contador entero incrementado en 1 cada 4 μs aproximadamente. En este caso el contador se da la vuelta (y el ISN reaparece) al cabo de 4 horas 46 min.
- El mecanismo de selección de los ISN es suficientemente fiable para proteger de coincidencias, pero no es un mecanismo de protección frente a sabotajes. Es muy fácil averiguar el ISN de una conexión e interceptarla suplantando a alguno de los dos participantes.
- TCP incrementa el número de secuencia de cada segmento según los bytes que tenía el segmento anterior, con una sola excepción:
  - Los flags SYN y FIN, cuando están puestos, incrementan en 1 el número de secuencia.
- La presencia del flag ACK no incrementa el número de secuencia.

Universidad de Granada

Además, sobre cómo se determina se debería indicar:

- Los mensajes SYN iniciales sirven para sincronizar los números de secuencia de cada lado (son diferentes para cada extremo). Aumentan en 1 al recibirse el ACK correspondiente al SYN (igual para el cierre de conexión con los mensajes FIN).
- El número de secuencia indica el primer byte del segmento, de forma que en cada segmento valdrá la suma del valor en el segmento anterior más el tamaño de dicho segmento anterior.

Utilidad:

- Sirve para mantener el orden de los segmentos recibidos. Como indica la posición del primer byte del segmento, si llegan varios segmentos desordenados (o retransmitidos) podemos colocarlos en su lugar adecuado.
- También sirve para detectar errores, usando para ello los campos de secuencia y de acuse. El acuse es el número de byte que espera recibir el receptor, que debería ser el último número de secuencia del receptor más el tamaño del segmento en el que se envió. Si no, significa que ha habido una discontinuidad y algún segmento no se ha recibido (bien porque se haya perdido, bien porque llegue más tarde desordenado).

PREGUNTA 3 (2 puntos sobre 10)

Describa el proceso del doble cifrado y explique los servicios de seguridad que proporciona dicho proceso.

Esta pregunta se explica en la siguiente transparencia. Básicamente:

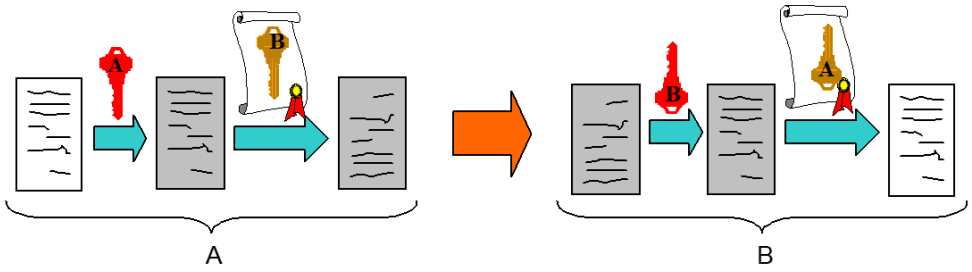
- Cifro con la clave pública del receptor → consigo confidencialidad porque solo el receptor puede descifrarlo con su clave privada.
- Cifro con la clave privada del emisor → consigo autenticación, porque solo el emisor conocía la clave privada (cualquiera descifra con la clave pública del emisor)
- No repudio: no se puede garantizar salvo que haya alguien me garantice la relación entre la identidad del emisor y su clave privada. En otro caso, no me serviría de prueba ante un juez. Si se garantiza esa relación (básicamente sería tener un certificado digital, donde una autoridad certificadora me garantiza con su firma que una identidad tiene una clave pública asociada), entonces sí se garantizaría el no repudio. Así que no se garantizaría en el caso general.

- No se garantiza la integridad (no hay ningún resumen o compendio que me permita comprobar si alguien ha modificado el mensaje).

5. Firma digital y certificados digitales

Fundamentos de Redes - Curso 2021 - 2022
© 2022 v1.0 - Juan M. López Soler y Jorge Navarro Ortiz

- Firma digital con clave asimétrica. *Doble cifrado*:
  - Uno para proporcionar privacidad, con KpubB
  - Otro, previo, para autenticación, con KpriA
  - Para firmar, enviar KpubB(KpriA (T) →
  - En el receptor KpubA (KpriB (KpubB(KpriA (T))))=T



  - Debilidad: para garantizar el no repudio se necesita garantizar la asociación fehaciente e indisoluble de la "identidad A" con su "clave pública KpubA" (A ←→ KpubA) … ?
    esto se consigue con un "certificado digital"

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.

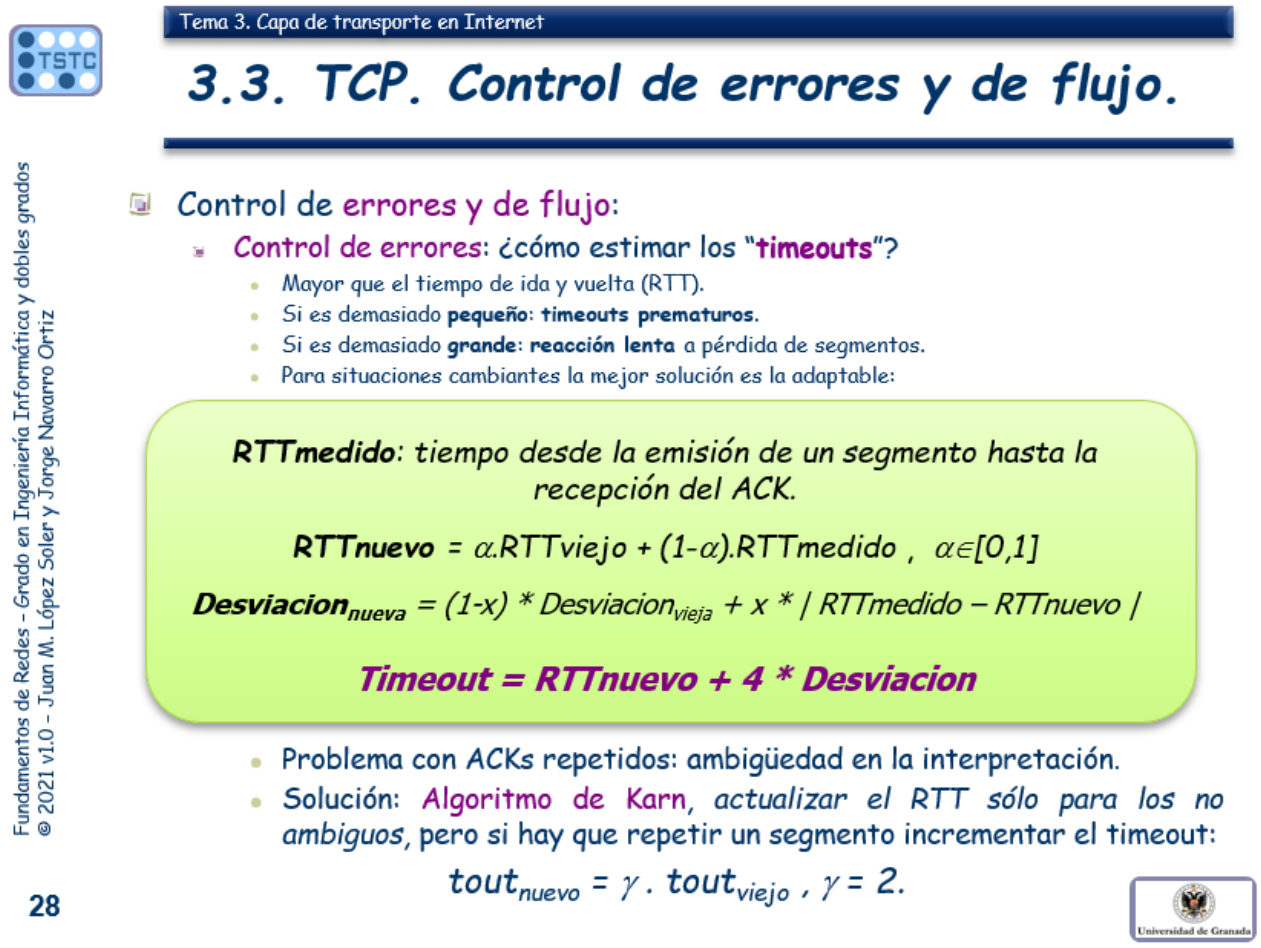
Los dos protocolos vistos en la asignatura son RIP (Routing Information Protocol) y OSPF (Open Shortest Path First).

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.

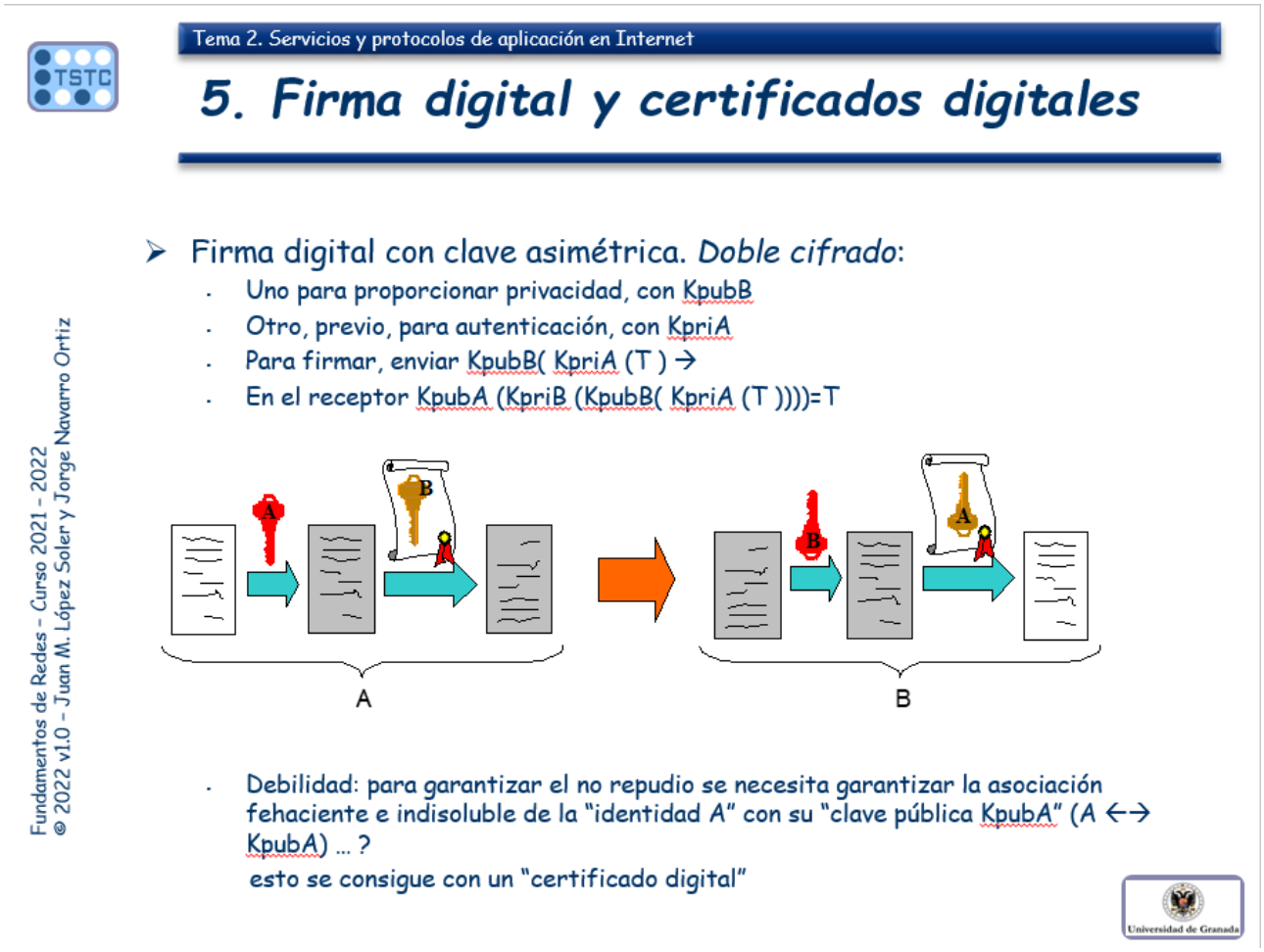
PREGUNTA 3 (1.5 16 puntos sobre 10)
Describa en qué consiste un certificado digital. Explique razonadamente cómo lo utilizaría para conseguir no repudio.

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.



UNIVERSIDAD DE GRANADA

Departamento de Teoría de la Señal, Telemática y Comunicaciones

FUNDAMENTOS DE REDES

– 3er curso del Grado en Ingeniería Informática (y dobles grados) –

Convocatoria ordinaria (1 de febrero de 2021)

Apellidos y nombre:

Titulación / grupo:

ENTREGA:

Haga la resolución de cada ejercicio en papel, escrito con bolígrafo de su puño y letra.

Después escanee o fotografíe los folios que desee que se evalúen, **INCLUYENDO SU DNI FÍSICO EN TODAS LAS PÁGINAS**. Preferiblemente todos juntos en un documento PDF.

Súbalo a la entrega en PRADO que se habrá habilitado durante la duración del examen, en los 10 minutos habilitados para la entrega.

PROBLEMA 1-A (3 puntos sobre 10)

La figura y mensajes siguientes describen un 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: peticion_acceso + usuario
NAS → PC: desafio
PC → NAS: usuario + K_{PC-AS}(desafio)
NAS → AS: peticion_autenticacion + usuario + K_{PC-AS}(desafio)
AS → NAS: peticion_aceptada + $Ksesion_{PC-NAS}$ + K_{PC-AS}($Ksesion_{PC-NAS}$)
(o peticion_rechazada)
NAS → PC: peticion_aceptada + K_{PC-AS}($Ksesion_{PC-NAS}$)
(o peticion_rechazada)
PC → NAS: $Ksesion_{PC-NAS}$ (datos_a_enviar) + MD5($Ksesion_{PC-NAS}$ (datos_a_enviar))
NAS → hacia Internet: datos_a_enviar
Desde Internet → NAS: datos_de_respuesta
NAS → PC: $Ksesion_{PC-NAS}$ (datos_de_respuesta) + MD5($Ksesion_{PC-NAS}$ (datos_de_respuesta))

Siendo:

- $Kpub_X$ (P) → cifrado de P con la clave pública de X
- $Kpriv_X$ (P) → cifrado de P con la clave privada de X
- K_{X-Y} (P) → cifrado de P con la clave secreta entre X e Y
- K_{X-Y} → clave secreta entre X e Y
- MD5 → función *hash*

a) Indique qué servicios de seguridad se proporcionan (confidencialidad, autenticación, integridad y no repudio) y entre qué elementos (PC, NAS, AS). Explique detalladamente su respuesta.
b) ¿Qué debilidades presenta el esquema propuesto? En su caso, ¿cómo podrían evitarse?

NOTA: Responda razonadamente a las cuestiones.

Ejercicio de Seguridad

Los aspectos de seguridad son 5: confidencialidad, autenticación, integridad, no repudio y disponibilidad. Respecto a este último punto, disponibilidad, no se puede dar información porque no se conocen aspectos como la infraestructura física, elementos redundantes, etc.

Este procedimiento persigue que un usuario (cliente) se autentique frente a un servidor de autenticación (AS) para ver si tiene derecho a acceder a Internet a través de un servidor de acceso a red (NAS). Es un esquema típico que utilizan los ISPs. Básicamente el cliente le manda una petición al NAS, que le responde con un desafío. El cliente manda dicho desafío cifrado con la clave secreta entre el PC y el AS, que es reenviado por el NAS al AS. Si este desafío cifrado coincide con lo que calcula el AS, le devuelve que la petición ha sido aceptada. Si no, se rechaza. En el mensaje de sesión aceptada, AS manda a NAS la clave de sesión entre el PC y el NAS (sin cifrar y cifrada con la clave secreta entre PC y AS). NAS se la reenvía a PC (cifrada con la clave secreta entre PC y AS). Así, tanto PC como NAS conocen dicha clave de sesión que usarán después para enviar entre ellos los datos que van/vienen de Internet.

Respecto a confidencialidad:

- La petición inicial entre PC y NAS va sin cifrar, por lo que cualquiera puede ver esos datos (petición y usuario).
- La respuesta al desafío (K_{PC-AS}(desafio)) no incluye ningún *nonce* o elemento que no se repita, por lo que es susceptible de ataques por repetición.
- La información entre NAS y AS va sin cifrar, por lo que un trabajador del ISP podría ver todos esos mensajes y la información enviada.
- La clave de sesión sí se envía cifrada entre NAS y PC, por lo que no podría ser vista por alguien externo en ese enlace (sí entre AS y NAS, donde se envía sin ir cifrada).
- Los datos desde el PC al NAS y viceversa (respuestas) sí van cifradas con una clave de sesión. Hacia Internet estos datos van sin cifrar.

Respecto a la autenticación:

- El procedimiento persigue que el PC se autentique frente al AS enviando una prueba de ello (el desafío cifrado con la clave secreta compartida entre el PC y el AS).
- El NAS se fía de la respuesta (peticion_aceptada o peticion_rechazada) enviada por el AS. Esto puede ser problemático porque el AS no se autentica frente al NAS (no hay ningún procedimiento para ello, ni cifra los mensajes con su clave privada para que el otro descifre con la pública, ni nada similar).
- NAS no se autentica con el PC. Tampoco se autentican NAS y AS entre ellos.

Respecto a la integridad: solo se incluye un resumen (a través de la función *hash* MD5) de los datos enviados y sus respuestas entre PC y NAS. Eso significa que esos mensajes no pueden ser modificados sin que nos demos cuenta. El resto de mensajes no tienen ningún resumen por lo que podrían ser modificados sin que nos diésemos cuenta.

Respecto al no repudio: no hay ninguna prueba (e.g. por haber cifrado algo con mi clave pública y que pueda ser descifrado por cualquiera con mi clave privada) de que hemos participado en esta transacción. Incluso los mensajes cifrados con la clave secreta o de sesión no servirían, ya que puede haberlos cifrado cualquiera de los dos extremos (no serviría de prueba frente a un juez).

Las debilidades se han explicado en los párrafos anteriores. Las posibles soluciones serían conseguir confidencialidad en todos los mensajes (e.g. usando la clave pública del receptor), autenticación (e.g. usando la clave privada del emisor), integridad (e.g. añadiendo resúmenes con MD5 de los mensajes enviados) y no repudio (se consigue también al usar, por ejemplo, la clave privada del emisor).

13. Examenes de 2019

Las preguntas son tipo test, pueden servir para entender conceptos.

UNIVERSIDAD DE GRANADA

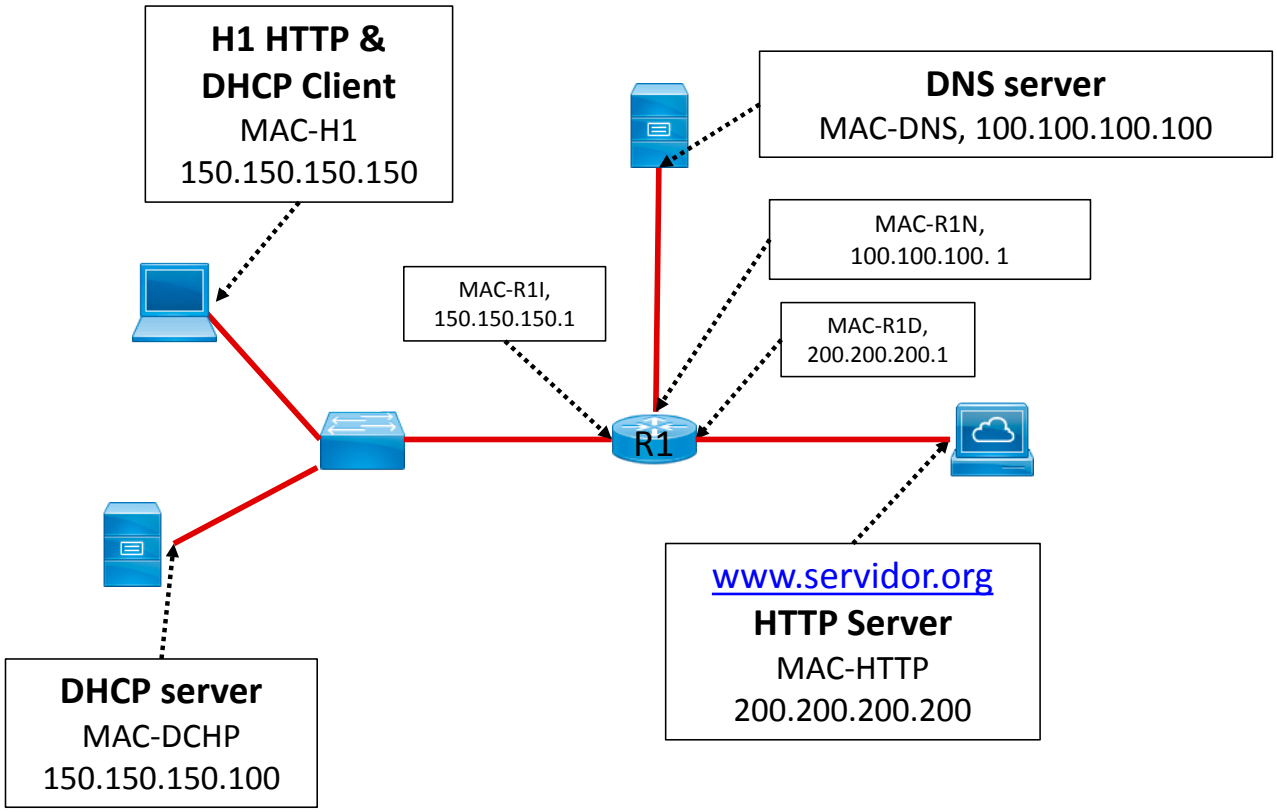
Dpto. Teoría de la Señal, Telemática y Comunicaciones
E.T.S. Ingeniería Informática y de Telecomunicación
C/ Periodista Daniel Saucedo Aranda, S/N
18071- Granada

FUNDAMENTOS DE REDES
5 de febrero de 2018 - Examen de teoría

Apellidos y nombre: _____ **Grupo:**_____

1. *(1.25 ptos)*. Describa el funcionamiento de los protocolos POP3 e IMAP, para qué son utilizados y las diferencias de funcionamiento entre ellos.

2. *(1,25 ptos)* Suponga que el cliente H1 acaba de iniciarse, tiene vacía la tabla ARP, pero conoce su default GW, y su IP (150.150.150.150) y su servidor DNS, así como su IP (100.100.100.100). Suponga que los servidores y los routers tienen toda la información necesaria. Haga las suposiciones que estime necesarias y rellene la siguiente tabla, mostrando **TODO** el tráfico que aparecería en esa red desde que H1 solicita el fichero indext.html del servidor HTTP www.servidor.org hasta que es servido.



MAC origen	MAC destino	IP Origen	IP Destino	Puerto Origen	Puerto Destino	FLAGS TCP	Mensaje/cabecera de Aplicación

SOLUCION

1.-

Solución en los apuntes de teoría y Bibliografía recomendada

2.-

MAC origen	**MAC destino**	**IP Origen**	**IP Destino**	**Puerto Origen**	**Puerto Destino**	**FLAGS TCP**	**Mensaje/cabecera deAplicación**
MAC-H1	BROADCAST	150.150.150.150	150.150.150.1	X	X	ARP	WHO IS 150.150.150.1?
MAC-R1I	MAC-H1	150.150.150.1	150.150.150.150	X	X	ARP	RESPONSE MAC= **MAC-R1I**
MAC-H1	MAC-R1I	150.150.150.150	100.100.100.100	40000	53	UDP	REQ. IP WWW.SERVIDOR.ORG
MAC-R1N	MAC-DNS	150.150.150.150	100.100.100.100	40000	43	UDP	REQ. IP WWW.SERVIDOR.ORG
MAC-DNS	MAC-R1N	100.100.100.100	150.150.150.150	53	40000	UDP	RESPONSE IP=200.200.200.200
MAC.R1I	MAC-H1	100.100.100.100	150.150.150.150	53	40000	UDP	RESPONSE IP=200.200.200.200
MAC-H1	MAC-R1I	150.150.150.150	200.200.200.200	40001	80	SYN	INICIO CONEX. TCP SEQ=A
MAC-R1D	MAC-HTTP	150.150.150.150	200.200.200.200	40001	80	SYN	INICIO CONEX. TCP SEQ=A
MAC-HTTP	MAC-RID	200.200.200.200	150.150.150.150	80	40001	ACK,SYN	SEQ=B, ACK=A+1
MAC-R1I	MAC-H1	200.200.200.200	150.150.150.150	80	40001	ACK,SYN	SEQ=B, ACK=A+1
MAC-H1	MAC-R1I	150.150.150.150	200.200.200.200	40001	80	ACK	SEQ=A+1, ACK=B+1
MAC-R1D	MAC-HTTP	150.150.150.150	200.200.200.200	40001	80	ACK	SEQ=A+1, ACK=B+1
MAC-H1	MAC-R1I	150.150.150.150	200.200.200.200	40001	80	ACK	SEQ=A+1, ACK=B+1, HTTP REQ.
MAC-R1D	MAC-HTTP	200.200.200.200	150.150.150.150	80	40001	ACK	SEQ=A+1, ACK=B+1, HTTP REQ.
MAC-HTTP	MAC-RID	200.200.200.200	150.150.150.150	80	40001	ACK	ACK=A+1+TAM_REQ. SEQ=B+1, HTTP RESPONSE (INDEX.HTML)
MAC-R1I	MAC-H1	200.200.200.200	150.150.150.150	80	40001	ACK	ACK=A+1+TAM_REQ. SEQ=B+1, HTTP RESPONSE (INDEX.HTML)

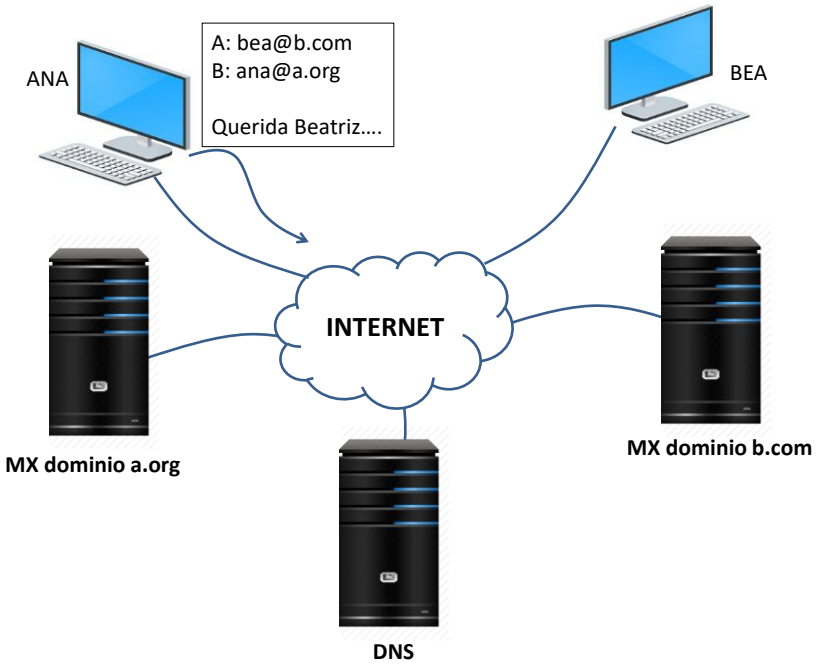
UNIVERSIDAD DE GRANADA

Dpto. Teoría de la Señal, Telemática y Comunicaciones
E.T.S. Ingeniería Informática y de Telecomunicación
C/ Periodista Daniel Saucedo Aranda, S/N
18071- Granada

FUNDAMENTOS DE REDES
15 de enero de 2018 - Examen de teoría

Apellidos y nombre: _____Grupo:_____

1. *(0,75 ptos).* Explique las diferencias que hay entre el control de congestión y el control de flujo.
2. *(0,75 ptos)* Identifique los niveles del modelo OSI y explique brevemente la funcionalidad de cada nivel.
3. *(1 pto)* Suponga la red mostrada en la siguiente figura. Ana desea enviarle un correo a Bea.



Suponiendo que todos los equipos tienen configurado completamente el encaminamiento, las tablas ARP llenas y el servidor DNS configurado y cachés vacías. El servidor DNS contiene todos los registros necesarios para resolver los dominios a.org y b.com. Con la ayuda de la tabla, explique el proceso completo y las diferentes solicitudes y respuestas de los protocolos implicados que los equipos deben realizar entre sí, desde que Ana le envía un correo a Bea hasta que ésta lo lee

Origen	Destino	Protocolo	Mensaje	Comentarios

4. *(1.25 ptos)* Al inicio de una conexión TCP, en una línea sin congestión con 25 ms de tiempo de propagación y 200 Mbps de velocidad de transmisión,

a) *(0.75 ptos)* ¿Cuánto tiempo se emplea en enviar y recibir confirmación de 40 KB con las siguientes asunciones? (añada cualquier otra adicional que crea conveniente)

a) Ventana ofertada de control de flujo de 20 KB constante.
b) Todos los segmentos se ajustan a un MSS (*Maximum segment Size*) de 2 KB
c) Umbral de congestión de 10 KB
d) Respuesta ACK retardada en el receptor de acuerdo a la teoría.

b) *(0.5 ptos)* Realice el diagrama de tiempos de la transmisión.

1.- Puede entender la pregunta en el contexto de TCP/IP:

La principal diferencia es q el ctrl de flujo es crediticio, dominado por el receptor, mientras q el ctrl de congestión es predictivo, y hay q inferir la situación de congestión.

Así, el ctrl de flujo se basa en el campo window, que se utiliza en piggybacking en la cabecera TCP.

El ctrl de congestión se basa en:

- el estimador del temporizador de time out.
- el umbral que define la separación entre inicio lento y prevención de congestión.

Con estos elementos, la ventana de congestión crece siguiendo una heurística. En Tahoe, el inicio lento incrementa la ventana en tantos MSS, cnos se confirman, y en prevención de la congestión se incrementa un MSS por ventana completa confirmada.

- O de OSI

- Control de congestión: explicar su función. Pertenece a Capa de Red.
- Control de flujo: explicar su función. Pertenece a las Capas de Enlace y Transporte.

2.- Ver en Libro.

14. Preguntas Variadas

14.1 Pregunta 1 (0,75 puntos)

14.1.1 Enunciado

Describa los mensajes generados desde un equipo correctamente configurado para acceder a Internet desde que solicita una URL en el navegador hasta que se muestra la página web completa.

14.1.2 Solución

El dispositivo origen de la conexión genera los siguientes mensajes:

1. **Solicitud DNS:** Se envía una consulta al servidor DNS para obtener la dirección IP correspondiente al nombre de dominio de la URL.
2. **Inicio de conexión TCP (3-way handshake):**
   - Primer segmento contiene únicamente cabeceras con el flag SYN para iniciar la conexión.
   - Recepción del segmento SYN+ACK del servidor.
   - Envío de un segmento ACK para completar el handshake.
3. **Solicitudes HTTP:**
   - Envío de una solicitud HTTP GET para obtener la página solicitada.
   - Envío de solicitudes adicionales (en este u otros flujos TCP iniciados previamente) para recuperar los objetos incrustados en la página.

14.2 Pregunta 2 (0,75 puntos)

14.2.1 Enunciado

Suponga que A y B tienen sus correspondientes $KPUB\_A$ / $KPRIV\_A$ y $KPUB\_B$ / $KPRIV\_B$, y una autoridad tiene sus $KPUB\_AUT$ / $KPRIV\_AUT$. Explique cómo y qué primitivas se cumplirían en una comunicación segura entre A y B usando dichas claves.

14.2.2 Solución

Las primitivas de seguridad se implementan de la siguiente manera:

- **Confidencialidad:** Se utiliza criptografía simétrica para cifrar el tráfico. La clave simétrica es negociada usando criptografía asimétrica, donde cada par usa la clave pública del otro para cifrar la información de la negociación.
- **Responsabilidad y Autenticación:** La clave pública de cada par está asociada a su identidad mediante un certificado digital, firmado por la autoridad certificadora utilizando su clave privada ($KPRIV\_AUT$).
- **Integridad:** Para garantizar que los mensajes no sean modificados, cada par firma un resumen (MAC) del mensaje con su clave privada. El receptor verifica la integridad utilizando la clave pública del remitente.

14.3 Pregunta 3 (0,75 puntos)

14.3.1 Enunciado

Se tiene un paquete de 5KB, de los cuales 14 bytes son de cabecera Ethernet, 20 bytes de cabecera IP, y 8 bytes de cabecera UDP. Este paquete debe pasar por una red Ethernet con una MTU de 1514 bytes. Si se precisa su fragmentación, ¿cuántos paquetes se generarían y con qué tamaños?

14.3.2 Solución

La fragmentación ocurre en la capa IP. Por lo tanto, el tamaño de la SDU (Service Data Unit) es:

$$\text{SDU} = 5 \cdot 1024\,\text{bytes} - (14 + 20)\,\text{bytes} = 5086\,\text{bytes}$$

Cada datagrama puede transportar un máximo de:

$$\text{Datos por datagrama} = 1500\,\text{bytes (MTU)} - 20\,\text{bytes (cabecera IP)} = 1480\,\text{bytes}$$

Por lo tanto:

- Se generan $\lfloor 5086/1480 \rfloor = 3$ datagramas completos de 1480 bytes de datos.
- El datagrama restante transporta $5086 - (3 \cdot 1480) = 646$ bytes.

Tamaños de los datagramas:

1. 3 datagramas de $1480 + 20 + 14 = 1514$ bytes.
2. 1 datagrama de $646 + 20 + 14 = 680$ bytes.

14.4 Pregunta 4 (0,75 puntos)

14.4.1 Enunciado

Identifique los niveles del modelo OSI y explique brevemente la funcionalidad de cada nivel.

14.4.2 Solución

1. **Nivel de Aplicación:** Brinda servicios a las aplicaciones del usuario (ej., HTTP, FTP).
2. **Nivel de Presentación:** Maneja la representación de datos, incluyendo traducción, compresión y cifrado.
3. **Nivel de Sesión:** Coordina y mantiene las sesiones entre aplicaciones.
4. **Nivel de Transporte:** Proporciona control de errores, control de flujo y multiplexación de aplicaciones (ej., TCP, UDP).
5. **Nivel de Red:** Encargado del direccionamiento, enrutamiento y control de congestión (ej., IP).
6. **Nivel de Enlace:** Proporciona la delimitación de tramas, control de errores y flujo entre nodos adyacentes.
7. **Nivel Físico:** Gestiona la transmisión de datos en forma de señales físicas a través de los medios de comunicación.