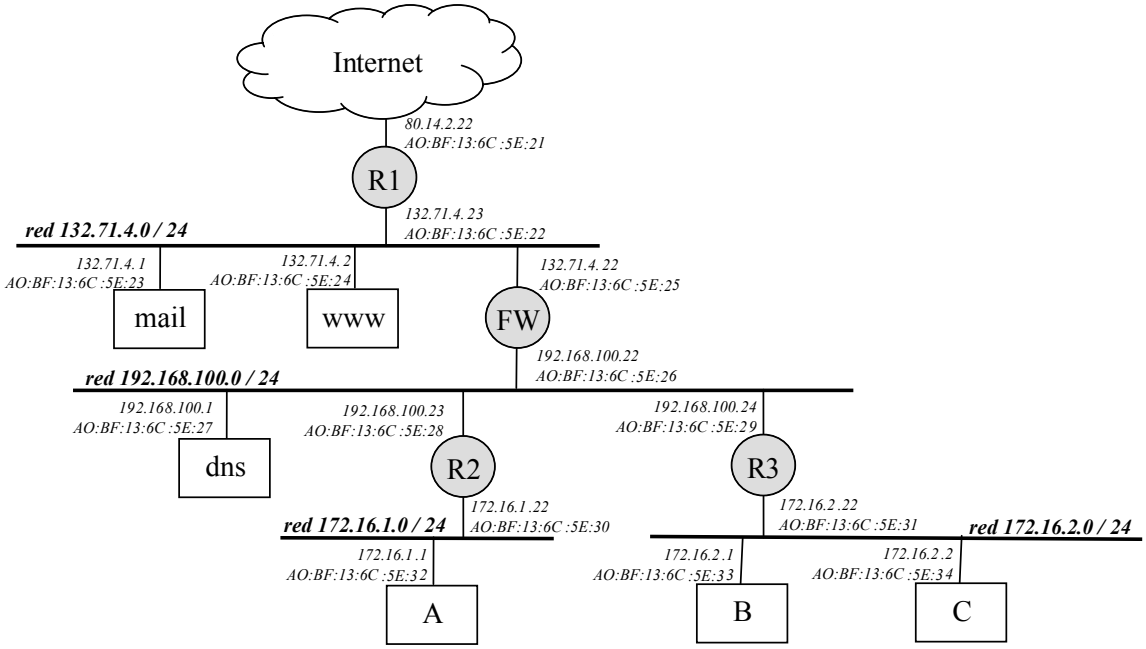
TRANSMISIÓN DE DATOS Y REDES DE COMPUTADORES II
Examen de teoría resuelto
25 de Junio de 2003

Dada la topología adjunta correspondiente a una red corporativa, en la que se especifican tanto las direcciones IP como las hardware de cada uno de los dispositivos que la forman, responda a las siguientes cuestiones:



1.- ***(2 ptos.)*** **Analice el tráfico generado al hacer un acceso web desde el cliente A al servidor www, especificando para cada trama Ethernet generada: a) las direcciones físicas origen y destino, b) las direcciones IP origen y destino contenidas en el paquete IP encapsulado, c) en su caso, los puertos origen y destino de la PDU de transporte así como los *flags* activos y campos de secuencia y ACK, y d) el tipo de mensaje de que se trata. Suponga que todas las tablas ARP son conocidas.**

Para el análisis del problema plantearemos las siguientes (razonables) suposiciones:

- Las tablas de encaminamiento son correctas y no hay más tráfico que el involucrado en la transacción HTTP.
- Al especificar la URL destino, el usuario en A proporciona el nombre de dominio, por lo que habrá tráfico DNS para obtener la dirección IP asociada.
- El servidor DNS es "autoridad" para el nombre de dominio, por lo que responderá al "query" sin originar tráfico adicional.
- El host A tiene el "resolver" o resolutor de nombres correctamente instalado, por lo que la dirección IP del servidor DNS es conocida por A.
- Tanto DNS com HTTP son, generalmente, aplicaciones cliente-servidor multiservicio. En nuestro caso las consideraremos implementadas, respectivamente, sobre UDP y TCP.
- Finalmente, como se establece en el enunciado, tendremos presente que las tablas ARP son conocidas, es decir, para cualquier dirección IP y cualquier host/router se conoce su dirección física.

Adicionalmente a las cuestiones anteriores, es necesario destacar la necesidad de que FW implemente la función de "masquerading" a fin de hacer viable la comunicación entre la intranet, de direcciones 192.x.x.x y 172.x.x.x, e Internet.

ETH ORI.	ETH DES.	IP ORI.	IP DEST.	PORT ORI.	PORT. DES.	FLAGS ACTIVOS SECUENCIA ACUSE	TIPO MENSAJE	COMENTARIOS
32 (*) (A)	30 (R2)	172.16.1.1 (A)	192.168.100.1 (dns)	(1)	53	-- -- --	Solicitud DNS por parte de A, especificando el nombre de dominio del server www	Envío a través de R2
28 (R2)	27 (dns)	"	"	"	"	"	"	Retransmisión del datagrama anterior de R2 al DNS
27 (dns)	28 (R2)	192.168.100.1 (dns)	172.16.1.1 (A)	53	(2)	-- -- --	Respuesta DNS indicando la IP de www solicitada	Resolución dada por DNS a A, a través de R2
30 (R2)	32 (A)	"	"	"	"	"	"	Reenvío de R2 a A ***→A conoce dir. IP de www: 132.71.4.2***
32 (A)	30 (R2)	172.16.1.1 (A)	132.71.4.2 (www)	(1)	80	SYN X (3) --	Solicitud de establecimiento de conexión TCP por parte de A al server www	Envío A→www, a través de R2
28 (R2)	26 (FW)	"	"	"	"	"	"	Retransmisión de R2 a FW
25 (FW)	24 (www)	132.71.4.22 (FW)	"	(5)	"	"	"	Entrega final de FW a www FW hace "masquerading" –ver nota (4)–
24 (www)	25 (FW)	132.71.4.2 (www)	132.71.4.22 (FW)	80	(5)	SYN,ACK Y (3) X+1	Aceptación del establecimiento de la conexión TCP y solicitud de establecimiento en el sentido contrario	Envío www→A a través de FW, con "masquerading" (4)
26 (FW)	28 (R2)	"	172.16.1.1 (A)	"	(2)	"	"	Retransmisión de FW a R2 Se deshace el "masquerading" (4)
30 (R2)	32 (A)	"	"	"	"	"	"	Entrega final de R2 a A
32 (A)	30 (R2)	172.16.1.1 (A)	132.71.4.2 (www)	(2)	80	ACK X+1 Y +1	Aceptación de establecimiento en sentido contrario	Envío A→www, a través de R2
28 (R2)	26 (FW)	"	"	"	"	"	"	Retransmisión de R2 a FW
25 (FW)	24 (www)	132.71.4.22 (FW)	"	(5)	"	"	"	Entrega final de FW a www con "masquerading" (4) ***→conexión TCP A-www establecida***

(*) Todas las direcciones hardware se han especificado, por sencillez, mediante el último octeto de los 6 que las componen
(1) El puerto en el cliente es proporcionado por el S.O. de entre los libres
(2) El puerto es el elegido en (1)
(3) El emisor elige un número aleatorio de 32 bits para comenzar la numeración de los segmentos TCP
(4) FW, en su función de "masquerading", mapea las parejas (*dir_IP_host_intranet, puerto_host_intranet*) en (*dir_IP_pública_FW,puerto_libre_FW*)
(5) El puerto es el elegido por FW en (4): *puerto_libre_FW*

ETH ORI.	ETH DES.	IP ORI.	IP DEST.	PORT ORI.	PORT. DES.	FLAGS ACTIVOS SECUENCIA ACUSE	TIPO MENSAJE	COMENTARIOS
32 (A)	30 (R2)	172.16.1.1 (A)	132.71.4.2 (www)	(2)	80	-- X+1 --	GET URL	Solicitud del documento o URL desde A al server www Envío a través de R2
28 (R2)	26 (FW)	"	"	"	"	"	"	Retransmisión de R2 a FW
25 (FW)	24 (www)	132.71.4.22 (FW)	"	(5)	"	"	"	Retransmisión de FW a www, con "masquerading" (4)
24 (www)	25 (FW)	132.71.4.2 (www)	132.71.4.22 (FW)	80	(5)	ACK Y+1 X+1+NB (*)	Envío del recurso web solicitado desde A	Por simplicidad, suponemos que los datos solicitados caben en un único paquete y que no se precisa su fragmentación Retransmisión a través de FW, con "masquerading" (4) (*) NB es el número de bytes que componen la solicitud GET
26 (FW)	28 (R2)	"	172.16.1.1 (A)	"	(2)	"	"	Retransmisión desde FW a R2 Se deshace el "masquerading" (4)
30 (R2)	32 (A)	"	"	"	"	"	"	Entrega final a A → ***A ya dispone de los datos web de www***
32 (A)	30 (R2)	172.16.1.1 (A)	132.71.4.2 (www)	(2)	80	FIN,ACK X+1+NB Y+1+NB2(*)	Solicitud de cierre de conexión TCP y confirmación de los datos recibidos	Solicitud de cierre de la conexión TCP en el sentido de A a www …(6) Además, confirmaremos los datos web recibidos (*) NB2 es el número de bytes contenidos en la respuesta HTTP
28 (R2)	26 (FW)	"	"	"	"	"	"	Retransmisión de R2 a FW
25 (FW)	24 (www)	132.71.4.22 (FW)	"	(5)	"	"	"	Envío final de FW a www, con "masquerading" (4)
24 (www)	25 (FW)	132.71.4.2 (www)	132.71.4.22 (FW)	80	(5)	FIN,ACK Y+1+NB2 (X+1+NB)+1	Confirmación de cierre y solicitud en el sentido www a A	Confirmación y solicitud en el otro sentido. Reenvío a través de FW, con masquerading (4)
26 (FW)	28 (R2)	"	172.16.1.1 (A)	"	(2)	"	"	Retransmisión de FW a R2 Se deshace el "masquerading" (4)
30 (R2)	32 (A)	"	"	"	"	"	"	Entrega final de R2 a A
32 (A)	30 (R2)	172.16.1.1 (A)	132.71.4.2 (www)	(2)	80	ACK (X+1+NB)+1 (Y+1+NB2)+1	Confirmación de cierre	Cierre final, a través de R2
28 (R2)	26 (FW)	"	"	"	"	"	"	Retransmisión de R2 a FW
25 (FW)	24 (www)	132.71.4.22 (FW)	"	(5)	"	"	"	Reenvío final a www con "masquerading" (4) | → ***conexión cerrada y servicio concluido*** |

(6) También se aceptaría que A confirmase los datos recibidos y, tras ello, fuese www quien iniciase activamente el cierre de la conexión.

2.- *(1 pto.)* Suponga ahora que el router FW se congestiona y, a resultas, no puede retransmitir el datagrama IP correspondiente al primer segmento TCP de datos (mensaje http) desde el servidor www al host A. Explique qué tráfico aparecerá en este escenario hasta que se consiga transmitir con éxito dicho segmento.

El control de congestión implementado en TCP puede estar basado en un esquema de notificación explícita o en uno de notificación implícita. El primero consiste en el empleo del mensaje "source quench" de ICMP para solicitar, por parte de un router congestionado, la ralentización de la estación emisora de los datos que están provocando dicha situación de congestión. Frente a este esquema, es más usual encontrar implementado el implícito, consistente en la ralentización automática del emisor (según unos algoritmos bien conocidos: decremento multiplicativo, inicio lento,...) en base a la no recepción de las confirmaciones correspondientes a los segmentos enviados dentro del "timeout" previsto. Queda claro, pues, que la función de los routers intermedios es nula en el esquema de notificación implícita.

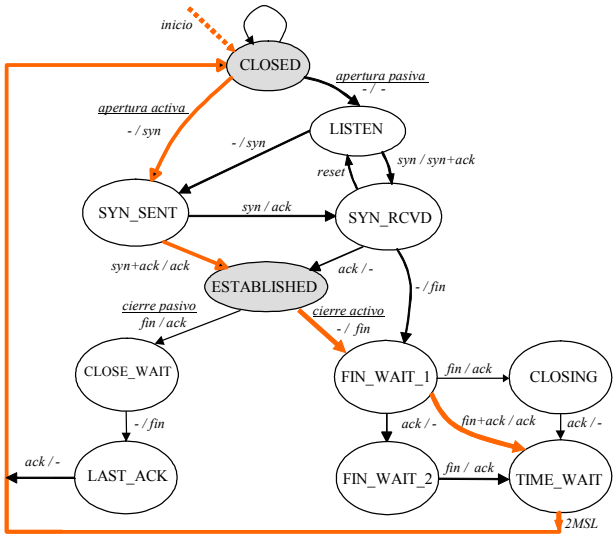
Más allá de lo anterior, en el ejercicio 1 se ha indicado la función de "masquerading" implementada por FW. Ello significa que este dispositivo hace las veces de "proxy", actuando como una estación final o host desde el punto de vista de Internet.

En definitiva, FW podría, desde un punto de vista teórico, llevar a cabo un control de congestión en base a tres esquemas distintos:

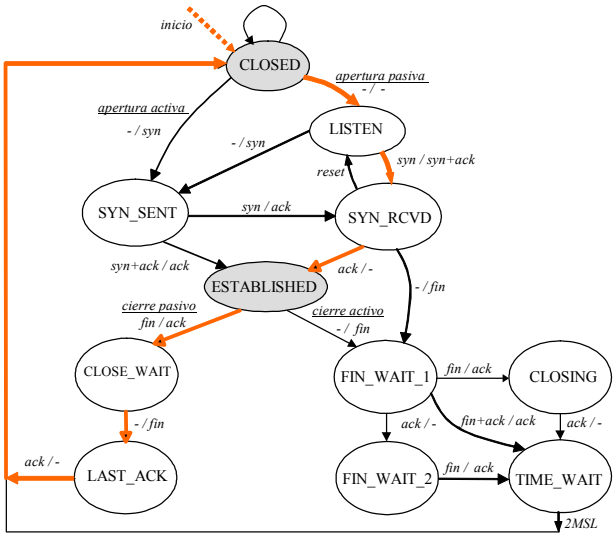
- Notificación explítica: emisión de un mensaje ICMP "source quench" a www (y al resto de emisores que están provocando la congestión) para hacer que se reduzca la ventana de emisión.
- Notificación implícita, lo que significa pasividad y esperar que pase la situación gracias a una auto-reducción en la emisión de los hosts orígenes ante la ausencia de confirmaciones en las transmisiones.
- Uso de los tamaños de ventana contemplados en los segmentos TCP intercambiados con www en el ejercicio 1 para así controlar "su congestión".

3.- *(1 pto.)* Para el escenario de la pregunta 1, marque el camino seguido en el autómata TCP adjunto tanto desde el punto de vista del cliente como del servidor.

Aunque, como se deduce del autómata, existen varios caminos posibles en la interacción TCP cliente-servidor, lo único que hemos de tener presente en este caso es la coherencia con la resolución dada en el ejercicio 1. Desde esta perspectiva, la respuesta a la pregunta aquí planteada es la siguiente, donde se considera que es el cliente (A) quien inicia activamente tanto el establecimiento (obviamente) como el cierre de la conexión:



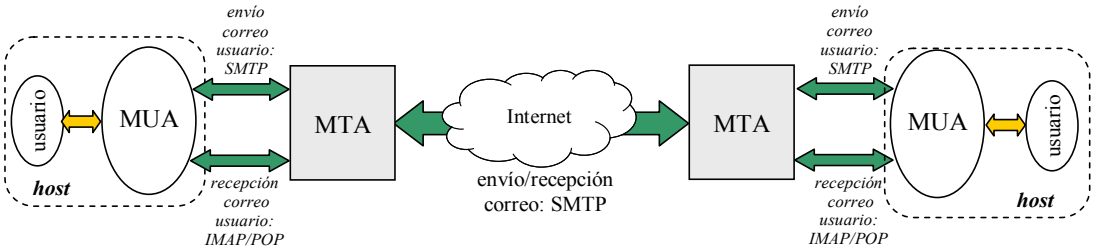
CLIENTE



SERVIDOR

4.- ***(1 pto.)*** **Suponga que un usuario situado en el host A desea enviar un correo electrónico usando la estafeta o servidor *132.71.4.1* a un destinatario cuya dirección es *destino@dominio.com* (en Internet). Describa todos los pasos involucrados en este proceso.**

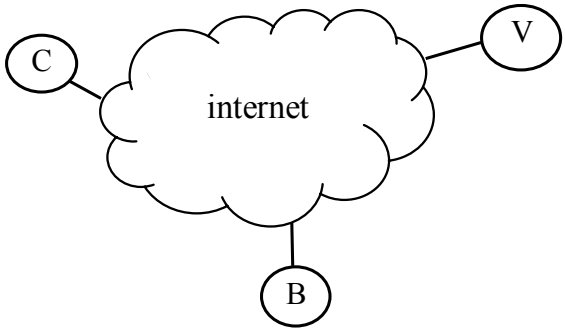
El esquema conceptual (gusual) del servicio de correo electrónico en Internet es el siguiente:



A partir de dicho esquema, el proceso planteado en este ejercicio, y efectuado a nivel de aplicación, es el siguiente:

1. El usuario procederá a la generación del mensaje correspondiente a través de la interfaz proporcionada por su MUA ("Mail User Agent").
2. El MUA ha de tener definido (como es habitual) como estafeta de correo saliente (MTA, "Mail Transfer Unit") la dirección IP o nombre de dominio del host denominado "mail" en la figura del enunciado del examen, cuya dirección IP es 132.71.4.1. En caso de que sólo esté definido su nombre de dominio, habrá de llevar a cabo un "query" a "dns" para obtener la IP correspondiente.
3. Conocida la IP de la estafeta "mail", el MUA abrirá una conexión TCP sobre el puerto 25 de la misma.
4. Una vez establecida dicha conexión, el envío del correo del usuario se realizará mediante el protocolo SMTP (o su extensión ESMTP), siendo los comandos enviados por parte del cliente (y a los que dará la respuesta oportuna, supuestamente positiva, el servidor) los siguientes:
   - HELO A
   - MAIL FROM: usuario@mail
   - RCPT TO: destino@dominio.com
   - DATA
     …*mensaje: cabecera y cuerpo*…
   - QUIT
5. Cerrada la conexión TCP, el mensaje enviado se almacenará en el *spool* de correo saliente de la estafeta dado que el dominio de destino no corresponde al local. De dicha zona de memoria será recuperado posteriormente por el MTA para su envío final como se indica a continuación.
6. El MTA "mail" formulará un "query" al DNS en Internet que tiene configurado (no el correspondiente a la intranet: "dns", puesto que no lo "ve") preguntando por el RR ("Resource Record") tipo MX ("Mail eXchanger") correspondiente al nombre de dominio "dominio.com", extraido de la dirección de correo destino. En la respuesta DNS (cuya resolución habrá podido, o no, involucrar otro/s DNS), además de indicar el nombre de dominio del MX solicitado, en el campo de "Información adicional" se proporcionará la dirección IP del MX o MTA de destino.
7. Nuestro MTA "mail" establecerá una conexión TCP al puerto 25 con el MTA remoto correspondiente al dominio "dominio.com" obtenido en el paso anterior, y, de forma completamente análoga al proceso indicado en el punto 4), efectuará una interacción SMTP para el envío del mensaje electrónico: HELO mail, MAIL FROM: usuario@mail, RCPT TO: destino@domain.com, DATA: …*mensaje*…, QUIT.
8. Verificado el buzón "destino" por parte del MTA final, el mensaje será aceptado y almacenado en el *spool* de correo entrante para su entrega al usuario a través de protocolos como IMAP o POP …. ¡Pero eso es otra historia!

5.- *(2 ptos.)* Idee un esquema de pago electrónico en Internet en el que intervengan los siguientes tres agentes: comprador (**C**), vendedor (**V**) y entidad bancaria del comprador (**B**), y en el que se garantice: confidencialidad, integridad y no repudio. Describa los posibles mensajes intercambiados entre los agentes para hacer una compra segura.



Antes de proceder sin más a la resolución del ejercicio planteado, es importante llevar a cabo la siguiente disquisición (de acuerdo con lo estudiado a lo largo del desarrollo de la asignatura):

- La característica de confidencialidad en las comunicaciones puede proporcionarse tanto por medio de técnicas de cifrado de clave secreta como mediante esquemas de clave pública. La primera solución pasa por suponer que: (a) las parejas emisor-receptor comparten a priori una clave común, o (b) ésta se establece mediante un esquema del tipo de Diffie-Hellman, o (c) la fija una entidad tercera confiable (KDC). Por su parte, el empleo de un esquema de cifrado clave pública del estilo de la técnica RSA obliga a la consideración de una entidad tercera certificadora confiable (del estilo de VeriSign).
- La característica de integridad en la transmisión de datos pueden proporcionarse mediante el empleo de técnicas de cifrado (como DES encadenado), aunque suele ser más usual recurrir a funciones *hash* tales como MD5 y SHA.
- Finalmente, la característica de no repudio implica necesariamente la intervención de una entidad tercera confiable para todas las partes involucradas en una comunicación: *Big Brother*, AC,...

De acuerdo con lo apuntado anteriormente, para la resolución del problema planteado vamos a realizar las siguientes consideraciones[1]:

1. Existe una entidad tercera confiable para todas las partes. La función de esta entidad será la emisión de certificados digitales que, como sabemos, especifican, entre otra información, las claves públicas de las distintas entidades participantes en una comunicación.
   A través de esta asunción perseguimos garantizar la característica de confidencialidad mediante un esquema de cifrado de clave pública, el cual pasa por el envío encriptado del mensaje objeto con la clave pública del receptor, que será quien únicamente podrá descifrarlo haciendo uso de su clave privada.
2. Asumiremos el empleo de un esquema *hash* (digamos MD5) para proporcionar integridad en la transmisión de datos. Para ello, como sabemos, se obtiene (y envía, cifrado) un compendio del mensaje a transmitir.
3. El empleo conjunto de las dos suposiciones anteriores va a permitir garantizar la tercera de las características requerida: la del no repudio. Para ello, como sabemos, bastará con cifrar (y enviar) el compendio del mensaje mediante la clave privada del emisor, lo que garantiza que únicamente ha podido ser él el generador de dichos datos. Son los esquemas de *firma digital*.

A partir de este punto sólo nos resta describir el esquema de interacción conceptual entre las distintas partes involucradas en la compra de un producto en Internet (ver Figura 1):

[1] Adicionalmente, sería interesante la inclusión de un *nonce* (sello de tiempo, por ejemplo) en los mensajes intercambiados para evitar ataques por repetición.

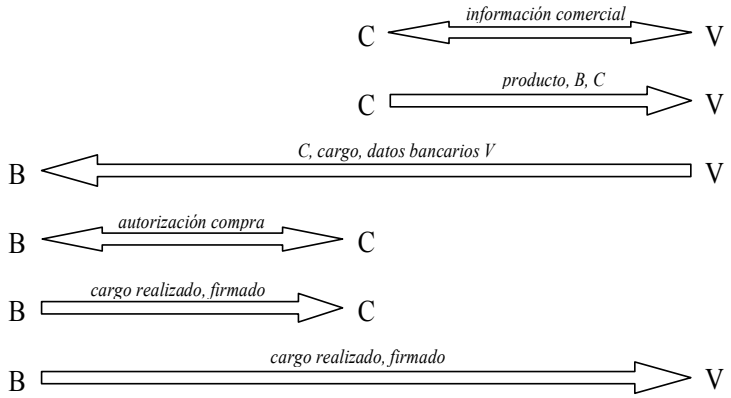


Figura 1. Interacción C-V-B para compra a través de Internet.

- Establecido un canal de comunicación seguro (orientado a conexión o no) entre C y V, ambos interaccionarán a fin de intercambiar información de los productos ofertados por el último de ellos.
- Interesado C en adquirir un producto dado, se lo comunicará a V indicándole: (a) el producto o productos en cuestión, (b) la identidad de su entidad bancaria, B, a la que efectuar el cargo y (c) su propia identidad de cara a B.
- V, sobre un canal seguro con B, especificará a éste: (a) la identidad de C, (b) el cargo de la compra y (c) los datos bancarios de V a fin de que B lleve a cabo el ingreso correspondiente en su cuenta o bien una transferencia a la misma.
- B contactará con C a fin de confirmar los datos proporcionados por V. (este proceso también podría realizarse a través de V, si bien hay que decir que tal vez resulte menos confiable).
- Autorizada la transacción por parte de C, B realizará la operación de transferencia o ingreso a V y pasará los datos correspondientes a ambas partes: (a) identidad de C, (b) identidad de V, (c) coste de la operación, (d) fecha,..... Aunque todas las comunicaciones anteriores pueden ir firmadas digitalmente por B, en ésta es especialmente necesario dicho proceso.
- Fin....