

Laboratorio de Redes y Servicios de Comunicaciones
Examen Teoría
13 de Septiembre 2002

NOMBRE (en mayúsculas):
DNI:

1. **(1.5 ptos.)** Para una conexión TCP entre las máquinas A y B, responde **clara y brevemente** a las siguientes preguntas:

- (i) **(0.5 ptos.)** ¿Para qué utiliza A el campo *Window Size* (tamaño ventana) de la cabecera TCP de los segmentos que transmite a B?

A emplea el campo Window Size de los datagramas que transmite para controlar el tamaño de la ventana de transmisión de B, controlando así el flujo de datos que B le transmite. Puede por ejemplo parar completamente la emisión de datos en sentido B → A, poniendo un valor de 0 en este campo.

- (ii) **(0.5 ptos.)** A envía un segmento a B con el campo *Sequence* = 24587653. ¿En qué afecta esto al campo *Sequence* de los datagramas que B envía a A?. ¿Por qué?

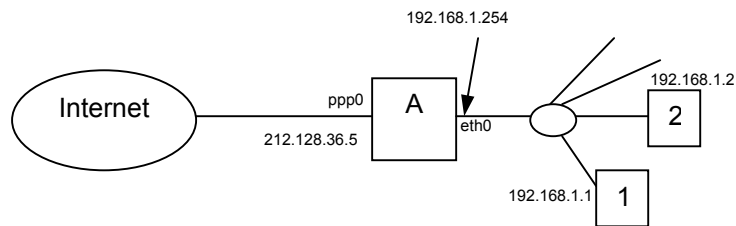
En nada. El campo Sequence de los datagramas A → B es independiente del campo Sequence de los datagramas B → A (una conexión TCP tiene dos comunicaciones de numeraciones independientes, una en cada sentido).

- (iii) **(0.5 ptos.)** A envía un segmento a B con el campo *ACK* = 21344366. ¿En qué afecta esto al campo *ACK* de los datagramas que B envía a A?. ¿Por qué?

En nada. El campo ACK de los datagramas que A transmite a B está relacionada con la comunicación de datos B → A. El campo ACK de los datagramas que B transmite a A está relacionada con la comunicación de datos A → B. Son dos comunicaciones independientes dentro de la misma conexión TCP, con numeraciones independientes.

2. (1.5 pts.) En la figura observamos una red local privada, en la que se ha configurado el mecanismo de IP-Masquerading en el router A para proporcionar conexión a Internet. Este router mantiene internamente una tabla para gestionar las conexiones TCP que está enmascarando. En un momento dado, los contenidos de esa tabla son los siguientes:

IP origen	Puerto origen	Puerto enmascarador
192.168.1.1	1700	61000
192.168.1.1	1701	61001
192.168.1.1	1702	61002
192.168.1.2	1700	61003
192.168.1.2	1701	61004
192.168.1.2	1702	61005



En este momento, el router A recibe por una de sus interfaces un datagrama IP, perteneciente a una conexión TCP, con las siguientes características:

IP origen	192.168.1.2
IP destino	200.4.6.1
Puerto TCP origen	1050
Puerto TCP destino	23

- (a) (0,25 pts.) ¿Se añadirá alguna entrada en la tabla de conexiones TCP enmascaradas? Si es así, escriba el contenido de esa entrada.

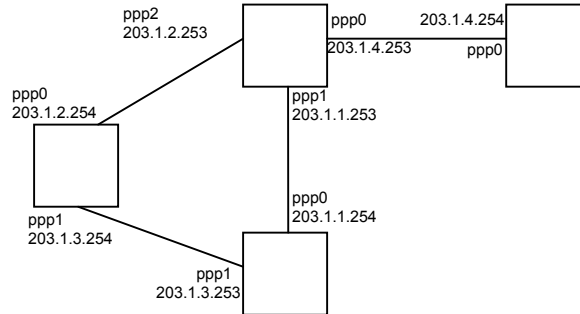
En la tabla no aparece ninguna conexión TCP de origen 192.168.1.2 por el puerto 1050. Por lo tanto se trata de una conexión TCP nueva, generada dentro de la red privada, y que debe ser enmascarada. Para controlar esta conexión se añade una entrada en la tabla como la que sigue.

IP origen	Puerto origen	Puerto enmascarador
192.168.1.2	1050	61006

- (b) (1.25 pts.) El mecanismo de IP-Masquerading realiza una serie de cambios en la cabecera IP y TCP de los datagramas pertenecientes a las conexiones TCP. El alumno debe rellenar la siguiente tabla en función de lo contestado en la cuestión anterior, lo que reflejará cuáles son esos cambios en los datagramas de la conexión TCP objeto de estudio.

Datagramas de la conexión TCP	IP origen	IP destino	Puerto TCP origen	Puerto TCP destino
Datagramas generados por 192.168.1.2	192.168.1.2	200.4.6.1	1050	23
Datagramas transmitidos por el router A hacia 200.4.6.1	212.128.36.5	200.4.6.1	61006	23
Datagramas generados por 200.4.6.1	200.4.6.1	212.128.36.5	23	61006
Datagramas transmitidos por el router A hacia 192.168.1.2	200.4.6.1	192.168.1.2	23	1050

3. (2 ptos.) Las máquinas de la figura están ejecutando el protocolo de encaminamiento RIP v1.0. Todas las redes son de clase C, y se aplica una máscara de subred 255.255.255.0 en todas las entradas de las tablas de encaminamiento.



Escriba los mensajes periódicos RIP Response que generan cada una de las máquinas suponiendo lo siguiente:

- Se ha alcanzado la convergencia de rutas.
- En esta convergencia, el router A encamina los datagramas a la red 203.1.3.0 por C.
- En esta convergencia, el router B encamina los datagramas a la red 203.1.1.0 por A.
- En esta convergencia, el router C encamina los datagramas a la red 203.1.2.0 por B.
- Los mensajes Response indican con número de saltos 1 (no 0), aquellas redes a las que están directamente conectadas.
- La implementación de RIP v1.0 que ejecutan las máquinas involucradas, aplica el mecanismo de *split horizon* simple.

Mensaje Response generado por A por su interfaz ppp0	
IP origen del mensaje: 203.1.4.253	IP destino del mensaje: 203.1.4.255
Ruta	Número de saltos
203.1.1.0	1
203.1.2.0	1
203.1.3.0	2

Mensaje Response generado por A por su interfaz ppp1	
IP origen del mensaje: 203.1.1.253	IP destino del mensaje: 203.1.1.255
Ruta	Número de saltos
203.1.2.0	1
203.1.4.0	1

Mensaje Response generado por A por su interfaz ppp2	
IP origen del mensaje: 203.1.2.253	IP destino del mensaje: 203.1.2.255
Ruta	Número de saltos
203.1.1.0	1
203.1.3.0	2
203.1.4.0	1

Mensaje Response generado por B por su interfaz ppp0	
IP origen del mensaje: 203.1.2.254	IP destino del mensaje: 203.1.2.255
Ruta	Número de saltos
203.1.3.0	1

Mensaje Response generado por B por su interfaz ppp1	
IP origen del mensaje: 203.1.3.254	IP destino del mensaje: 203.1.3.255
Ruta	Número de saltos
203.1.1.0	2
203.1.2.0	1
203.1.4.0	2

Mensaje Response generado por C por su interfaz ppp0	
IP origen del mensaje: 203.1.1.254	IP destino del mensaje: 203.1.1.255
Ruta	Número de saltos
203.1.2.0	2
203.1.3.0	1

Mensaje Response generado por C por su interfaz ppp1	
IP origen del mensaje: 203.1.3.253	IP destino del mensaje: 203.1.3.255
Ruta	Número de saltos
203.1.1.0	1
203.1.4.0	2

Mensaje Response generado por D por su interfaz ppp0	
IP origen del mensaje:	IP destino del mensaje:
Ruta	Número de saltos
<i>El router D funciona en modo pasivo y no transmite mensajes Response periódicamente</i>	