Redes de Computadoras

Septiembre de 2006

Nombre:
DNI:

Teoría y problemas (75 %).

1. **(2 puntos)** ¿Verdadero o falso? Razone además su respuesta.

   a) Un host A envía a un host B un fichero muy grande a través de TCP. Suponga que el host B no tiene datos que enviar al host A. El host B no enviará reconocimientos al host A porque el host B no puede "piggyback" los reconocimientos en los datos.

   ```
   % Falso. Los ACKs no tienen por qué ser siempre piggybacked.
   ```

   b) El tamaño del campo `Window` de los segmentos TCP nunca varían durante una conexión.

   ```
   % Falso. Este campo indica a quien recibe el segmento qué tamaño
   % tiene la ventana de recepción del que lo envía (téngase en cuenta
   % que el TCP es full-duplex).
   ```

   c) Suponga que el host A está enviado un fichero muy grande al host B mediante TCP. El número de bytes sin confirmación que A envía no puede exceder el tamaño del buffer del receptor.

   ```
   % Verdadero.Si esto no se cumpliera no se estaría realizando el
   % control del flujo de datos.
   ```

   d) Suponga de nuevo que el host A está enviando un fichero muy grande al host B. Si el número de secuencia para un segmento de esta conexión es m, entonces el número de secuencia para el siguiente segmento será $m + 1$.

   ```
   % Falso. Esto sólo ocurrirá si el segmento con número de secuencia m
   % transporta sólo 1 byte.
   ```

   e) Suponga que el último `SampleRTT` en una conexión TCP es igual a 1 segundo. Entonces `TimeOut` será necesariamente ≥ 1 segundo.

   ```
   % Falso. Para estimar el RTT (y por tanto, el TimeOut) se utiliza
   % una expresión que tiene en cuenta los valores anteriormente
   % estimados. Por tanto, esta aformación rara vez será cierta.
   ```

   f) Suponga que el host A envía sobre una conexión TCP un segmento con un número de secuencia de 38 y 4 bytes de datos. En este mismo segmento el número de reconocimiento valdrá 42.

   ```
   % Falso. Los números de secuencia de los segmentos de los hosts A y
   % B no tienen nada que ver.
   ```

2. **(1,5 puntos)** Considere que se transfiere un fichero enorme de L bytes desde el host A al host B. Asuma un MSS de 1460 bytes.

   a) ¿Cuál es el valor máximo de L que provoca que los números de secuencia del TCP no se repitan? Recuerde que el campo de número de secuencia del TCP es de 4 bytes.

   ```
   % 2^{32}
   ```

   b) Para el valor de L obtenido en el apartado anterior, ¿cuánto tiempo tardaría en transmitirse dicho fichero? Asuma que el número total de bytes añadidos por las cabeceras las capa de transporte, red y enlace de datos es de 66 bytes y que el enlace de transmisión tiene una tasa de 10 Mbps. Ignore el control de flujo y de la congestión de forma que A puede enviar los segmentos de forma continua.

```
%
%           2^{32} B
% ceil( --------------- ) = 2941759 segmentos
%       1460 B/segmento
%
% Como cada segmento además tiene 66 B de cabecera/segmento,
% el número total de bytes de cabecera enviados es:
%
% 66 B de cabecera/segmento * 2941758 segmentos = 194156094 B
%
% Por tanto, el volumen total de datos enviados es:
%
% 2^{32} + 194156094 = 4.489.123.390 B = 35.912.987.120 b
%
% A razón de 10 Mbps, tardaremos un total de:
%
% 35.912.987.120 b
% ---------------- = 3.591 segundos = 59,85 minutos
%    10*10^6 b/s
%
```

3. **(1 punto)** Suponga que un paquete llega hasta el interface público de un router NAT. ¿De qué depende que dicho paquete atraviese el NAT y entre en la red privada? ¿De qué depende que dicho paquete sea finalmente recibido por un proceso?

```
% Para que un paquete que llega a un router NAT sea encaminado desde
% la red pública a la red privada debe existir una entrada en la
% tabla de traducción NAT indexada por el puerto al que va dirigido
% el paquete que llega al NAT. Nótese que dicha entrada fue creada
% cuando desde la red privada se envió un paquete hacia la red
% pública y en ella figura la dir IP y el puerto en el que está
% escuchando el proceso al que finalmente va dirigido el paquete que
% llega al NAT.
```

4. **(1 punto)** Considere una red con prefijo 101.101.101.64/26.

   a) Dé un ejemplo de una dir IP (de la forma XXX.XXX.XXX.XXX) que podría ser asignada a un interface de dicha red.

```
% Ya que hay 26 unos en la máscara de red, la red 101.101.101.64/26
% contiene un total de 2^{32-26} = 64 direcciones.
% El rango de direcciones sería:
%
% 101.101.101.64 -> Dir de la red
% 101.101.101.65 -> Dir del GateWay
% 101.101.101.66 -> Dir del host 1
% :
% 101.101.101.126 -> Dir del host 62
% 101.101.101.127 -> Dir de Broadcast
%
% Cualquiera de las direcciones de host o del GateWay valdría.
```

   b) Suponga que quiere crear cuatro sub-redes para este bloque, cada una con el mismo número de dirs IP. ¿Cuáles son los prefijos (de la forma A.B.C.D/X) de cada una de las sub-redes?

```
% Cada una de estas redes es de la clase /28 (16 dirs/sub-red).
% Los prefijos para las 4 redes serían:
```

```
%
% 101.101.101.64/28 -> Sub-red 1.
%                      101.101.101.64 -> Dir de la red
%                      :
%                      101.101.101.79 -> Dir de BC
% 101.101.101.80/28 -> Sub-red 2.
%                      101.101.101.80 -> Dir de la red
%                      :
%                      101.101.101.95 -> Dir de BC
% 101.101.101.96/28 -> Sub-red 3.
%                      101.101.101.96 -> Dir de la red
%                      :
%                      101.101.101.111 -> Dir de BC
% 101.101.101.112/28 -> Sub-red 4.
%                      101.101.101.112 -> Dir de la red
%                      :
%                      101.101.101.127 -> Dir de BC
```

5. **(1 punto)** Responda a la siguientes preguntas. Si en la tabla de encaminamiento de un router aparecen dos entradas 200.23.16.0/20 y 200.23.18.0/23 que referencian a enlaces de salida distintos.

   a) ¿Es la primera entrada el "camino más corto" a la red 200.23.18.0/23?

   ```
   % No, al tratarse de un prefijo más corto (de 20 bits frente a
   % 23), no se trata de el camino más corto porque esta red es la
   % más grande de las dos. Nótese que la red 200.23.16.0/20 incluye
   % a la red 200.23.18.0/23. Esto puede comprobarse viendo que el
   % prefijo 200.23.16.0/20 es a su vez prefijo de 200.23.18.0/23.
   ```

   b) Si fuera al contrario (es decir, si fuera un "camino más largo"), ¿qué entrada debería figurar antes en la tabla del encaminamiento de dicho router?

   ```
   % Los caminos más cortos hacia un misma red deben aparecer primero
   % en las tablas de encaminamiento para optimizar las rutas.
   ```

   c) ¿Es este un ejemplo de agregación o de des-agregación?

   ```
   % Puesto que la red 200.23.18.0/23 pertenece a la red
   % 200.23.16.0/20, lo que ocurre es un ejemplo de
   % des-agregación. Esto ocurre típicamente cuando una red cambia de
   % ISP y no modifica sus dirs IPs.
   ```

6. **(1 punto)** En CSMA/CD, tras la sexta colisión, ¿cuál es la probabilidad de que un nodo seleccione $K = 4$? ¿Cuántos segundos esperaría el nodo ((en la sexta colisión) si la tasa de transmisión es de 100 Mbps?

   ```
   % Tras la primera colisión los nodos seleccionarían aleatoriamente
   % entre {0,1}
   % Tras la segunda colisión entre {0,1,2,3}
   % Tras la tercera colision entre {0,1,...,7}
   % Tras la cuarta entre {0,1,...,15}
   % Tras la quinta entre {0,1,...,31}
   % Tras la sexta entre {0,1,...,63}
   % Por tan to la probabilidad de que un nodo seleccione K=4 cuando
   % hay 64 posibilidades es de 1/64.
   %
   % Si el enlace es de 100 Mbps, el tiempo de bit es igual a 1/100
   % Mbps = 0,01 us. Puesto que Ethernet espera K*512 tiempos de bits
   ```

```
% tras producirse una colisión, el tiempo total de espera en el caso
% de la sexta colisión (ojo, no el acumulado tras todas las
% colisiones) es de 4*512*0,01 = 20,48 us.
```

Prácticas (25 %)

- 0,1 **puntos por pregunta.**
- **Una mal resta una bien.**

V F Verdadero/Falso.

□■ Cuando Ethereal se configura para capturar los frames desde el interface de red Wireless, todos los frames capturados son Ethernet.

□■ Si implementamos el cliente de PING usando el protocolo UDP no es necesario implementar además el servidor.

■□ HELO, MAIL FROM, RCPT TO, y DATA son comandos utilizados entre un cliente y un servidor SMTP.

□■ La consulta `nslookup -type=NS ual.es` se realiza siempre a uno de los servidores de nombres autorizados para el dominio `ual.es`.

□■ Un proxy Web cachea todos los paquetes TCP que han sido generados por el protocolo HTTP.

□■ El proxy Web desarrollado en prácticas no utiliza conexiones TCP paralelas. Por tanto, la descarga de una página Web con múltiples objetos incrustados va a ser generalmente lenta.

■□ En la práctica en la que se analiza el TCP, el fichero que se utiliza para estudiar el comportamiento del TCP es enviado desde nuestro host al servidor Web.

□■ Cuando usamos el protocolo HTTP para transmitir un fichero de datos, dependiendo de la longitud de dicho fichero serán generados uno o varios paquetes UDP.

□■ En TCP, cuando un segmento tiene el flag ACK activado significa que transporta información de control de la congestión.

■□ Cuando accedemos a una página Web mediante nuestro navegador por primera vez se produce un establecimiento de conexión TCP. Tras capturar los frames con Ethereal y establecer el filtro `tcp` deberíamos ver que los tres primeros segmentos enviados pertenecen a dicho establecimiento de conexión.

■□ Si el tamaño máximo de ventana especificado por el receptor de una transmisión TCP es de 5000 y el MSS máximo es de 1000, entonces el número máximo de segmentos enviados sin confirmación es de 5.

□■ Si todos los segmentos tienen el mismo tamaño, para calcular la tasa de transmisión real de una transmisión TCP podemos multiplicar el número de sementos transmitidos y el tamaño de los segmentos.

■□ En una gráfica donde se muestra el número de secuencia de los segmentos transmitidos en función del tiempo podemos apreciar la acción del control de la congestión realizada por el TCP.

□■ El periodo de arranque lento en el TCP se reconoce porque el número de segmentos enviados sin confirmación es menor que el tamaño de la ventana especificada por el receptor.

□■ Sabemos que un datagrama IP ha sido fragmentado porque el flag `MF` (More Fragments) es 0 y el campo `Fragment Offset` es distinto de 0.

■□ La aplicación `traceroute` se aprovecha de que los routers envían un datagrama ICMP con el mensaje *TTL excedido* hacia el host emisor del datagrama que ha sido destruido por dicho motivo.

□■ Sabremos si un datagrama IP ha sido fragmentado cuando el campo `Fragment offset` es 0.

■□ Cuando enviamos un datagrama UDP a un host y en éste no existe ningún proceso escuchando, entonces se genera un paquete ICMP "Port Unreacheable"en el host destino que tiene como origen el proceso emisor en el host origen.

■□ Tras deshabilitar el análisis del protocolo IP en Ethereal, todas las direcciones físicas fuente y destino que aparecen en la lista de frames capturados pertenecen a interfaces de nuestra red local.

■□ Todos los frames que encapsulan datagramas que van dirigidos a un host externo a nuestra red tienen como dirección física destino la del router por defecto para nuestro host.

□■ Si mostramos el contenido de nuestra tabla ARP y sólo aparece una entrada para el router por defecto, entonces no existe ninguna computadora más que utiliza la red en nuestra sub-red.

■□ Todos los frames que encapsulan datagramas que van dirigidos a nuestro host y que vienen desde otro que está fuera de nuestra red tienen como dirección física origen la de un router de nuestra red.

□■ Supóngase una interacción HTTP entre un servidor y un cliente. El cliente reclama una página Web en la que existen varios objetos Web. Sabremos que las conexiones han sido en serie porque las peticiones se realizan en instantes de tiempo diferentes.

■□ En HTTP, la fecha que figura tras la línea de cabecera IF-MODIFIED-SINCE es la fecha en que el cliente obtuvo por última vez el objeto referenciado.

■□ Si un objeto Web referencia a dos objetos más, el número de peticiones HTTP sería como mínimo tres.