

Redes de Datos

1er parcial – 2008

Solución

Pregunta 1

- a) Explique con un ejemplo cómo se realiza el establecimiento de una conexión en el protocolo TCP. Indique qué banderas y campos son relevantes, así como sus valores
- b) El mecanismo de establecimiento de conexión de TCP, ¿Qué garantiza? (justifique)
- c) La siguiente secuencia de segmentos (ordenada en el tiempo) pertenece a un tramo de una comunicación que usa el protocolo TCP. Asuma que no hay segmentos previos pendientes de reconocimiento. Complete los campos que faltan:

IP Origen	IP Destino	Carga útil (bytes)	Número de Secuencia	Número de Reconocimiento
A	B	10	120	520
B	A	30		
A	B	0		
A	B	20		
B	A	40		

Respuesta 1

- a) Supongamos la conexión iniciada por el host A hacia el host B (donde B está escuchando en el puerto correspondiente). A elige X como número de secuencia inicial, y B elige Y
- **Primer segmento:** Exclusivamente encabezado, originado en A con destino B, Banderas encendidas: Syn, el campo "número de secuencia" en X (El campo "número de reconocimiento" no se tiene en cuenta porque la bandera Ack está apagada)
 - **Segundo segmento:** Exclusivamente encabezado, originado en B con destino A, Banderas encendidas: Syn, Ack, el campo "número de secuencia" en Y, el campo "número de reconocimiento" en X+1
 - **Tercer segmento:** Usualmente solo el encabezado, aunque podría llevar datos. Originado en A con destino B, bandera de Syn apagada, bandera de Ack prendida, campo "número de secuencia" con valor X+1, campo "número de reconocimiento" con valor Y+1
- Otros valores que usualmente se intercambian solamente en el establecimiento son opciones como por ejemplo: la escala de ventana, el soporte de reconocimientos selectivos, el tamaño máximo de segmento.

- b) El mecanismo de establecimiento de conexión de TCP garantiza:
- Que existe comunicación bidireccional entre A y B (ya que ambos deben contestar un segmento del otro)
 - Que el intento de establecimiento de conexión de A no es un duplicado de un segmento viejo (ya que A reconoce a B el número de secuencia que B acaba de elegir, y si lo eligió en base al reloj de tiempo real y respetando la zona prohibida sabe que no pueden quedar en la red reconocimientos a otros paquetes que utilizaran el mismo número de secuencia)
 - A sabe que B está activo y no es un reconocimiento a un intento de establecimiento de conexión anterior (por las mismas razones del punto anterior)
- c) Asumiendo que cada segmento llega a destino y se procesa antes de que se envíe el siguiente:

IP Origen	IP Destino	Carga útil (bytes)	Número de Secuencia	Número de Reconocimiento
A	B	10	120	520
B	A	30	520	130
A	B	0	130	550
A	B	20	130	550
B	A	40	550	150

Pregunta 2 (8 puntos)

- Explique por qué las direcciones de capa de red se asignan por rangos a las distintas subredes que componen Internet
- Explique el significado de la máscara de red en las redes IP
- Explique cómo se utilizan las máscaras de red. ¿Las máscaras de red, viajan en los paquetes IP? Justifique

Respuesta 2

- Las direcciones se asignan por rangos por una cuestión de escalabilidad, de esta manera los demás equipos de Internet solamente precisan una entrada de información (una entrada en la tabla de ruteo) para llegar a todos los equipos de una determinada subred. Si no fuera así, habría equipos que tendrían que saber donde se encuentra cada IP determinada en internet. A su vez, permite la asignación jerárquica, donde el receptor de un determinado rango de direcciones puede subdividirlo y asignar distintos subrangos a distintas subredes (las cuales desde el resto de Internet se pueden agrupar en una sola entrada en la tabla de ruteo). También la asignación por rangos permite una administración descentralizada de las mismas.
- En las redes IP, se definió que para asignar rangos de direcciones a distintas subredes, se dividieran los 32 bits de dirección en algunos bits para indicar el rango (parte de red o prefijo) (los bits más significativos), y el resto el equipo dentro de la red. O sea que todos los hosts de una determinada subred comparten los mismos bits más significativos (dirección de red o prefijo) y difieren en la parte de host. Pero la cantidad de bits utilizada para identificar la red no es fija, por lo que se requiere una manera para indicar, para cada red, cuales son los bits correspondientes a la dirección de red y cuales identifican al host. La máscara se utiliza para esto, es un número de 32 bits que consiste en bits "1" en las posiciones correspondientes a los bits de red, y "0" en el resto. La notación para las máscaras de red puede realizarse en "dotted decimal notation" (ej: 255.255.255.0) o indicando la cantidad de bits "1" que tiene (ej: /24)
- La máscara de red se utiliza para determinar si una dirección IP dada se encuentra en una red. Por ejemplo, la utilizan los enrutadores para determinar cual entrada en la tabla de enrutamiento utilizar para reenviar cada paquete. Dada una dirección de red R (que por definición tiene "0" en los bits correspondientes al host) y su máscara, y una dirección IP "D", para determinar si esa dirección IP se encuentra en la red R, se realiza el AND bit a bit entre "D" y la máscara (esto deja los bits correspondientes a la parte de host en "0", y los demás incambiados), y luego se compara este valor obtenido con R. Si son iguales, D se encuentra en la red R.
Las máscaras no viajan en el encabezado de los paquetes IP, lo único que se requiere en el encabezado de IP es la dirección de destino para que los hosts y enrutadores sepan a qué equipo entregarlo (y la de origen para saber de donde viene). Las máscaras son útiles en las tablas de ruteo de los hosts y enrutadores.

Pregunta 3 (8 puntos)

- Explique las diferencias entre un servicio "orientado a conexión" y un servicio "no orientado a conexión". Explique con ejemplos, para qué usos sería más adecuado cada uno de estos tipos de servicio.
- ¿Qué protocolo de capa de transporte utiliza DNS? Ese protocolo ¿brinda servicio "orientado a conexión" o "no orientado a conexión"? Explique por qué el protocolo DNS utiliza este servicio.
- ¿Qué protocolo de capa de transporte utiliza SMTP? Ese protocolo ¿brinda servicio "orientado a conexión" o "no orientado a conexión"? Explique por qué el protocolo SMTP utiliza este servicio.

Respuesta 3

- En un servicio orientado a conexión, antes de cualquier intercambio de datos se debe realizar un establecimiento de conexión, donde típicamente origen y destino se informan o negocian parámetros de la conexión (y posiblemente se reservan recursos en ambos extremos y en el camino). Al finalizar el intercambio de datos, debe realizarse un procedimiento de fin de conexión, de forma de liberar los recursos reservados. Las primitivas ofrecidas por el servicio son coherentes con estas 3 etapas.
En cambio, un servicio no orientado a conexión simplemente me ofrece primitivas de envío y recepción de datos, o sea que al tener datos para enviar simplemente se envían.

En servicios orientados a conexión es más fácil brindar garantías de calidad de servicio que en los no orientados a conexión (por ejemplo secuenciamiento, recuperación ante errores o pérdidas), pero no están atados unos a otros. Tampoco están atados los servicios orientados a conexión a las redes de circuitos virtuales y los no orientados a conexión a las redes de datagramas, aunque esas combinaciones tengan ventajas.

Como ejemplo de aplicaciones donde conviene utilizar servicios orientados a conexión se encuentra la transferencia de archivos, donde es conveniente disponer de un servicio que reserve recursos en el receptor para los datos a transferirse (usualmente grandes), y donde sea fácil brindar garantías de calidad de servicio.

Como ejemplo de aplicaciones donde conviene utilizar servicios no orientados a conexión están aquellas donde se tienen transacciones de datos cortas (por lo que el overhead de establecimiento y fin de conexión es significativo) donde el resultado de la transacción no varía si se aplica varias veces (o sea que ante un error alcanza con retransmitir la transacción).

- b) DNS utiliza usualmente para las consultas el protocolo UDP. Este protocolo cumple las condiciones nombradas en la parte anterior (consultas y respuestas cortas, no hay efectos secundarios si la consulta se debe realizar nuevamente ante una pérdida de la consulta o la respuesta).
También utiliza TCP, cuando se están realizando transferencias de zonas entre servidores maestros y esclavos (gran cantidad de datos, debe garantizarse la recepción del total de los datos), o cuando la respuesta sería demasiado grande para entrar en un único paquete UDP de respuesta
- c) SMTP utiliza el protocolo TCP, la transferencia de correo es similar en requerimientos a la transferencia de archivos, por lo que aplican las consideraciones de la parte (a)

Pregunta 4 (8 puntos)

Para las siguientes funcionalidades de control de errores, describa para TCP y para UDP si las implementan, y de qué manera:

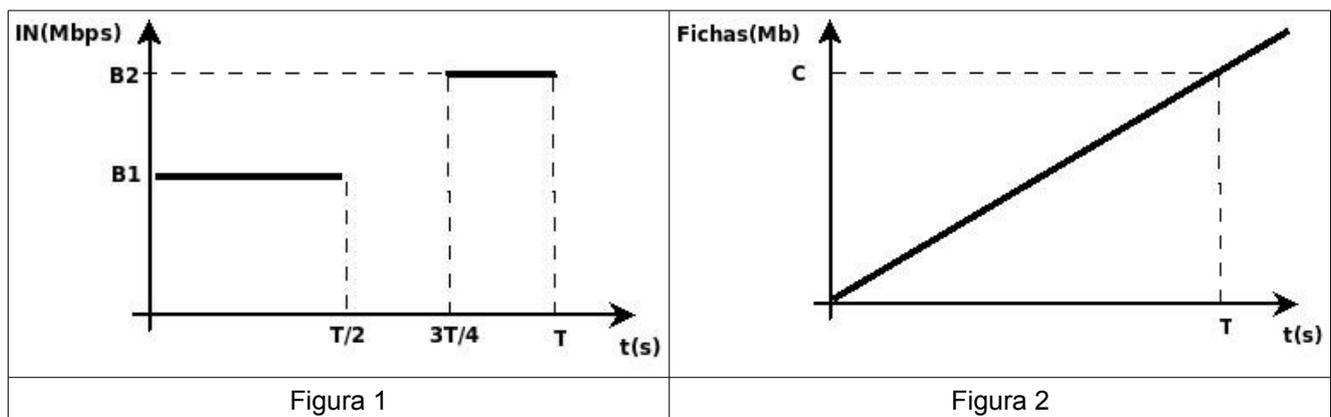
- a) Detección o Corrección de errores en el segmento recibido
- b) Recuperación ante pérdida de segmentos en la red
- c) Recuperación ante reordenamiento de segmentos en la red
- d) Recuperación ante segmentos duplicados

Respuesta 4

- a) Tanto TCP como UDP implementan detección de errores mediante una suma de comprobación. No implementan corrección de errores.
- b) TCP implementa la recuperación de los datos en segmentos perdidos. Cada segmento incluye un número de secuencia que numera el primer dato en el segmento, y el receptor debe reconocer los datos recibidos correctamente (indicando el próximo número de secuencia esperado). En caso de no recibir el reconocimiento de algunos datos antes de vencer un temporizador, el transmisor enviará nuevamente los datos perdidos.
UDP no intenta recuperar (ni siquiera detectar) la pérdida de segmentos en la red
- c) La misma numeración de los datos vista en (b) se utiliza para determinar el orden correcto de los segmentos recibidos, en caso de faltar algún segmento el receptor guardará en buffer los datos hasta que reciba los faltantes.
UDP no incluye ninguna característica que le permita detectar (menos recuperarse) ante el reordenamiento de segmentos en la red.
- d) En cada momento, el receptor está dispuesto a aceptar un determinado rango de números de secuencia (desde el primer número de secuencia posterior al último recibido, hasta ese número más el tamaño de ventana del receptor). En caso de recibir un segmento duplicado con número de secuencia fuera de este rango, será descartado por esa causa. En caso de recibir un segmento duplicado con número de secuencia en el rango (porque se recibió un segmento fuera de secuencia y está guardado esperando los datos faltantes), se descartará por esta causa.
UDP no tiene forma de distinguir segmentos duplicados.

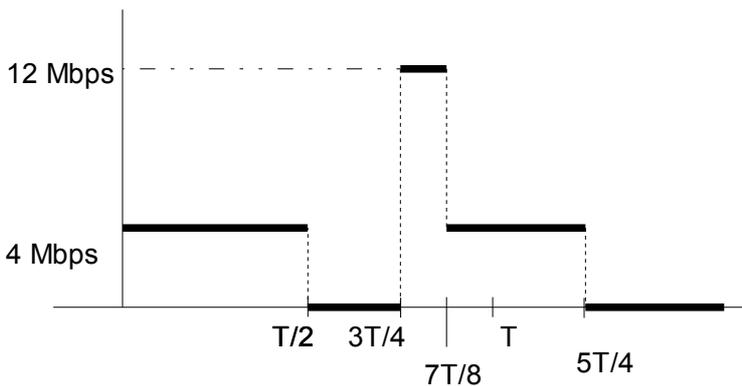
Pregunta 5 (10 puntos)

- a) ¿Qué es la congestión en una red?
- b) Explique qué es el control de admisión y cómo ayuda al control de congestión
- c) Explique cómo funciona el mecanismo de “balde con fichas”. Explique de qué forma ayuda a controlar la congestión
- d) Se tiene un router que aplica la técnica de “balde con fichas” en su interfaz de salida. Todo dato que no encuentre fichas es encolado hasta que haya fichas disponibles (buffer infinito). Considere que el tráfico de entrada durante un tiempo T es como el mostrado en la figura 1. Suponga que en $t=0$ el balde no tiene fichas y que las fichas se generan como se muestra en la figura 2. Suponga que la capacidad del balde es suficiente para que en ningún momento se descarten fichas
- Para C y T dados, calcule la condición necesaria y suficiente que debe cumplirse para que los datos que ingresan en la primer ráfaga (entre $t=0$ y $t=T/2$) terminen de salir del router antes de $t=3T/4$.
- Considere los siguientes valores $C=4Mb$, $B1=4Mbps$ $T=1s$ y $B2=12Mbps$. Observe que para estos valores se cumple la condición hallada en la parte anterior.
- ¿Cuántos bytes hay acumulados en el balde de fichas en $t=3T/4$?
 - Dibuje las características del tráfico a la salida del router. Indique las coordenadas de todos los puntos relevantes.

**Respuesta 5**

- a) La congestión es la sobrecarga de algún elemento de la red ocasionada por sobreutilización (posiblemente momentánea) de algún recurso, ya sea capacidad disponible en un enlace, capacidad de procesamiento de un equipo, etc.
- b) El control de admisión es una función que se implementa normalmente en los equipos de borde (aquellos al ingreso a la red), y consiste en permitir o no determinados flujos de tráfico dependiendo de la capacidad disponible en la red. Por ejemplo, en una red de circuitos virtuales, decidir si aceptar o no establecer un nuevo circuito dependiendo de la capacidad solicitada y la capacidad disponible en la red. Ayuda a controlar la congestión ya que brinda una manera de controlar el tráfico que entra a la red.
- c) El mecanismo de “balde con fichas” (token bucket) se utiliza para conformar el tráfico de datos. La analogía es un balde, lleno de fichas, donde cada ficha representa el permiso para transmitir una determinada cantidad de datos. El balde tiene una capacidad finita, C , y una tasa de llenado o generación de fichas, g . Las fichas se van acumulando en el balde hasta llegar a C , las que sobrepasen C son descartadas. Al llegar datos a transmitir, se comprueba si hay suficientes fichas en el balde, si es así se transmite y se retiran tantas fichas como representen la cantidad de datos enviados, de lo contrario las políticas pueden ser retener los datos hasta que haya suficientes fichas o descartarlos. Este comportamiento permite que en los momentos en que no se transmiten datos se acumulen fichas, y puedan ser utilizadas posteriormente para enviar más rápidamente una ráfaga de datos. El balde con fichas ayuda a controlar la congestión ya que impone una velocidad promedio máxima al tráfico reenviado y limita el tamaño máximo de las ráfagas permitidas, de esta manera conocemos las características del tráfico a la salida del balde en el peor caso y podemos diseñar la red en base a estos datos.

- d) i) Cantidad de datos recibidos: $B1 \cdot T/2$
 Cantidad de fichas generadas entre 0 y $3T/4$: $3C/4$
 Por lo tanto, $B1 \cdot T/2 < 3C/4$
- ii) En $3T/4$ tenemos $3C/4 - B1 \cdot T/2 = 3Mb - 2Mb = 1Mb$
- iii) Entre 0 y $T/2$, los datos llegan tan rápido como se generan fichas, por lo que saldrán a la misma velocidad que entraron.
 Entre $T/2$ y $3T/4$ se acumulan fichas: $C/4$: 1 Mb
 A partir de $3T/4$ se consumen las fichas acumuladas. Estas se acaban en t : $1Mb + t \cdot 4Mbps = t \cdot 12Mbps$
 De aquí, $t = T/8$, por lo que en $7T/8$ se acaban las fichas, por lo que los datos solo pueden salir a la velocidad de generación de fichas. El resto se acumulan.
 Entre $7T/8$ y T se acumulan: $(12-4)/8 = 1$ (Mb)
 A partir de T salen los datos acumulados. Demorarán $1Mb/4Mbps = 1/4s$

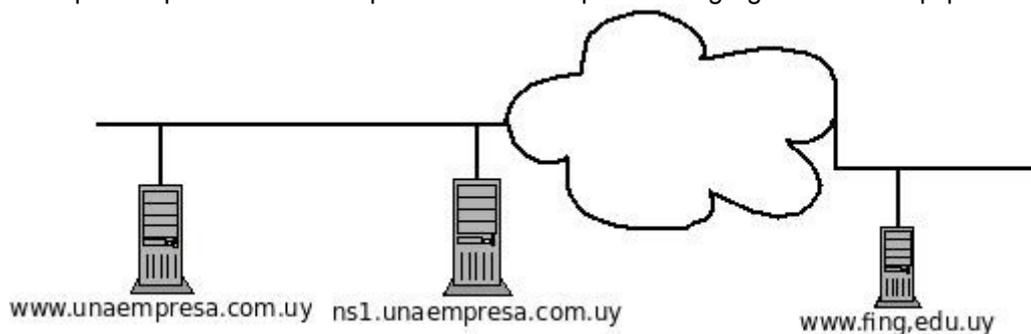


Pregunta 6 (8 puntos)

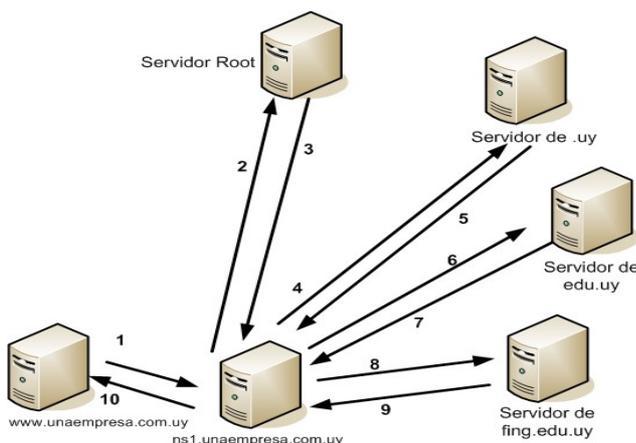
En la figura siguiente, la máquina de nombre **www.unaempresa.com.uy** está configurada para usar como servidor recursivo de nombres a **ns1.unaempresa.com.uy**. El servidor de nombres autoritativo para el dominio **unaempresa.com.uy** es el **ns1.unaempresa.com.uy**.

Un usuario en **www.unaempresa.com.uy** visita la página web alojada en la máquina de nombre **www.fing.edu.uy**. Indique qué consultas DNS se tienen que realizar para resolver ese nombre, y a quiénes se dirigen esas consultas. Suponga que no hay ningún dato en los caches de todos los servidores involucrados.

Realice un esquema que facilite la comprensión de su explicación agregando otros equipos si son necesarios.



Respuesta 6



- Veremos una posible respuesta, asumiendo que ningún servidor (excepto ns1) es recursivo. Asumimos que en todos los casos en que nos indican un registro NS, también nos indican el registro A correspondiente
1. **www.unaempresa.com.uy** consulta por el registro A de **www.fing.edu.uy** a **ns1.unaempresa.com.uy** (su servidor recursivo)

2. Al no tener datos en cache, ns1 consulta a uno de los servidores raiz por el registro A de www.fing.edu.uy
3. El servidor raiz, al no ser recursivo, responde con los registros NS de .uy.
4. ns1 consulta por el registro A al servidor de UY
5. Servidor de UY responde con los registros NS de edu.uy
6. ns1 consulta por el registro A a un servidor de edu.uy
7. El servidor de .edu.uy responde con los registros NS de fing.edu.uy
8. ns1 consulta por el registro A al servidor de fing.edu.uy
9. El servidor de fing.edu.uy le responde con el registro A correspondiente a www.fing.edu.uy (asumiendo que existe)
10. ns1 le responde a www.unaempresa.com.uy el registro A correspondiente

Observación: En cada una de las respuestas con registros NS de dominio, o bien viene en ella el registro A asociado al nombre (glue record) o bien hay que realizar una búsqueda por el registro A correspondiente a ese nombre de dominio para poder continuar la búsqueda en el árbol de dominios.