2° Certamen Tiempo 90 min.

Cada pregunta tiene igual puntaje.

1.- **Mencione dos** diferencias entre SIP y H.323.

SIP es un protocolo que define el establecimiento de llamadas. H.323 es un protocolo más completo que incluye señalización, registro, control de admisión, ***transporte y codificación****.*

SIP fue propuesto por el IETF, es un estándar Internet; mientras que H.323 fue propuesto por la ITU, es un estándar de las compañías de telefonía.

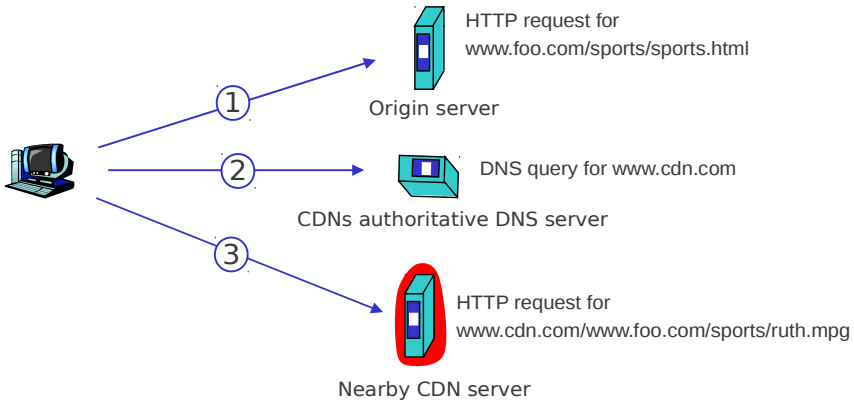
2.- **Describa** el **problema** que dio origen a las redes de distribución de contenidos (CDN) como Akamai.

El problema fue la sobrecarga de procesamiento y ancho de banda al tener un servidor único distribuyendo contenido multimedia a múltiples usuarios distribuidos por el mundo. Esta situación conduce a degradación del servicio cuando éste se hace popular y muchos acceden a él. Además, los tiempos de respuesta para usuarios alejados es pobre.

3.- Para la figura adjunta responda:

a) ¿A quién representa el computador de la izquierda?

Representa a un cliente que desea acceder un servicio multimedia remoto.



b) Explique qué ocurre en los pasos 1, 2, y 3.

Paso 1: El cliente baja la página principal que referencia a un contenido multimedia. El servidor ha puesto en su lugar la ruta desde www.cdn.com.

Paso 2: La referencia al contenido multimedia señala que se encuentra en www.cdn.com/www.foo.com/sports/rut.mpg por lo cual el cliente debe resolver el nombre www.cdn.com. La respuesta entrega la IP del servidor más cercano al cliente luego de revisar un paga de servidores y redes en el mundo.

Paso 3: El cliente se dirige a ese servidor de la CDN y obtiene así el contendido multimedia desde el servidor más cercano a él.

4.- **Mencione** y **describa dos** de los cuatro principios de calidad de servicio (QoS) vistos en clases.

1. ***Clasificación de paquetes****: Los paquetes de un flujo de datos deben ser marcados según la clase de servicio deseada para ese flujo.*
2. ***Aislación****: Se debe hacer cumplir a los flujos de datos la calidad se servicio declarada (Ej: Ancho de banda promedio y tamaño de ráfaga)*
3. ***Alta utilización de recursos****: Se debe asegurar que se acomoda la mayor cantidad de flujos hasta alcanzar la mayor utilización de los recursos disponibles respetando cada una de las calidades de servicio comprometidas.*
4. ***Control de Admisión de llamadas****: Si una nueva solicitud de llamada es recibida, ésta debe ser bloqueada si no hay recursos disponibles para asegurar el cumplimiento de lo que requiere.*

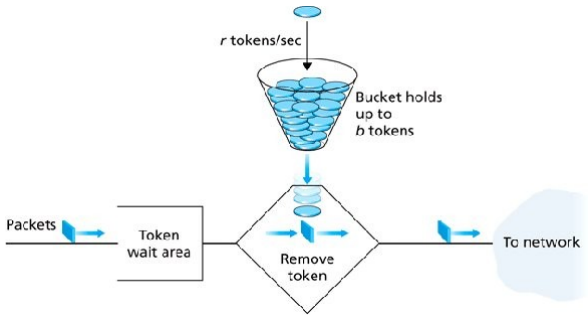
5.- Para limitar el tráfico a parámetros previamente convenidos, una implementación utiliza un “token bucket” (balde de fichas). Determine el tamaño de ráfaga (burst size) y la tasa promedio resultante en función de b y r (suponga 1 token = 1 byte).

La ráfaga será tan larga como para consumir la totalidad de token del balde b, más aquellos token que alcancen a ser ingresados mientras se transmite la primera parte de la ráfaga. Luego:

$$TráficoSalida = BurstSize = R*t = b + r*t$$

$$t = \frac{b}{R-r}$$

$$BurstSize = \frac{b*R}{R-r}$$



La tasa promedio *corresponde a la cantidad de byte que en el largo plazo se puede estar transmitiendo constantemente. Esta es justamente* ***r****.*

6.- Una de las técnicas para romper o descubrir un clave de encriptación mono-alfabética es hacer un análisis estadístico. Explique brevemente cómo funciona esta técnica.

Para cada idioma, se conoce la frecuencia de aparición de cada letra. Si la clave se encriptación es mono-alfabética, entonces la función de papeo se puede obtener calculando la frecuencia de distribución de cada símbolo encriptado y asociarlo a la frecuencia de las letras de ese lenguaje. Asi se puede descubrir el papeo usado en la encriptación.

7.- **Mencione una ventaja** del cifrado de bloques en cadena (CBC) respecto al cifrado de bloques.

El cifrado en bloques usa una semilla. Si ésta no cambia CBC tiene la ventaja que el envío de dos mensajes iguales durante la sesión tendrá una versión encriptación distinta. El cifrado de bloques en este caso conduce a lo mismo. Si la semilla cambia, debe ser enviada cada vez ocupando agregando ineficiencia.

8.- **Mencione una desventaja** del cifrado simétrico respecto del asimétrico.

El mensaje simétrico obliga que Tx y Rx conozcan la clave o secreto compartido previamente, luego no puede ser usado cuando éstos no se conocen previamente.

Sólo para alumnos de IPD438:

1.- Describa el tipo de contenidos que deben ser incluidos en el **resumen** de un artículo científico.

El resumen de un artículo científico debe incluir:
Una primera oración normalmente ubica el tema (resume la introducción), las siguientes oraciones ubican el punto específico o problema que justifica el trabajo, luego se explican el camino tomado para resolverlo (esto es la nueva idea). Finalmente la última frase resume los resultados.

2.- Mencione tres caminos para evaluar una propuesta de solución a algún problema técnico.

La solución a un problema técnico se puede evaluar por medio de:
Simulación, pruebas experimentales, modelos resueltos matemáticamente.

3.- Mencione dos diferencias entre el contenido del **resumen** de un artículo científico y el contenido de las **conclusiones** del mismo.

Mientras el resumen extrae lo esencial de todo el trabajo, la conclusiones se concentras en los resultados obtenidos y el impacto futuro de estos.