EXAMEN DE SISTEMAS INFORMÁTICOS DE TIEMPO REAL

Septiembre 1999

1. Explicar las diferencias entre los Sistemas de Tiempo Real estrictos y no estrictos. Ejemplos de aplicaciones.

(1 punto)

En los **sistemas de tiempo real *estrictos (críticos)*** la corrección temporal es crítica, es decir el tiempo de respuesta es muy importante y no puede ser sacrificado por una mejora en otros aspectos. En ciertos sistemas de tiempo real crítico (especialmente en los sistemas de seguridad críticos) la corrección temporal es tan importante que el criterio de corrección lógica puede ser relajado en aras de alcanzar un tiempo de respuesta determinado. Un ejemplo típico es el piloto automático de una aeronave, el fallo en el chequeo de la altitud en tiempos prescritos puede tener consecuencias catastróficas. En tales circunstancias un resultado de peor calidad pero a tiempo, puede ser preferible a un resultado muy preciso pero que llegue tarde.

En los **sistemas de tiempo real *no estrictos (acríticos)*** la corrección temporal es importante pero no crítica. Fallos ocasionales en generar un resultado dentro del tiempo fijado no produce consecuencias serias en el funcionamiento general del sistema. Las tareas de tiempo real no estrictas son ejecutadas tan rápido como es posible, pero no están forzadas por tiempos límite absolutos, pudiendo ser sacrificada la corrección temporal bajo ciertas circunstancias como son picos en la demanda del procesador o del medio de comunicación. A pesar de ello las tareas de tiempo real no estricto difieren de las tareas ordinarias que no están sometidas a dichos requerimientos temporales aunque si puedan estar sujetas a otros requerimientos de rendimiento.

Un **sistema de tiempo real estricto** puede estar constituido por una combinación de tareas de ambos tipos siendo sacrificada la corrección temporal de aquellas tareas de tiempo real no estricto a favor de aquellas que deben cumplir tiempos límite críticos. El manejo de prioridades entre tareas permite manejar este tipo de relaciones.

Es posible también que una misma **tarea** puede tener tiempos límite estrictos y no estrictos. Por ejemplo, la respuesta a un evento de peligro puede tener un tiempo límite no estricto de 50 ms (para una reacción con eficiencia óptima) y un tiempo límite estricto de 200 ms (para garantizar que no se produce un daño en el equipo o en las personas). Entre estos dos límites, el valor o utilidad de la salida decrece según aumenta el tiempo.

Así mismo se puede distinguir dos tipos de relajación en la corrección temporal de los sistemas no estrictos:

- Puede ocurrir que ocasionalmente no se cumpla el tiempo límite, pero no tenga ningún valor si el resultado llega tarde (simplemente se ha perdido la respuesta a un evento). Por ejemplo, en tareas periódicas puede ser admisible que se pierda la ejecución de algunas de ellas.

- Puede ocurrir que el servicio llegue tarde ocasionalmente pero este sea valido dentro de un cierto intervalo de tiempo.

En resumen los sistemas de tiempo real estrictos imponen un tiempo de respuesta determinista, permitiendo un comportamiento en caso de sobrecarga predecible, aunque supone generalmente trabajar con un volumen de datos reducido. Por el contrario un sistema de tiempo real no estricto no actúa de forma tan determinista, presentando algún tipo de degradación cuando se producen sobrecargas. A cambio permite trabajar con un mayor volumen de datos.

2. Explicar brevemente las características estáticas y dinámicas que determinan la calidad de la medida de un reloj real.

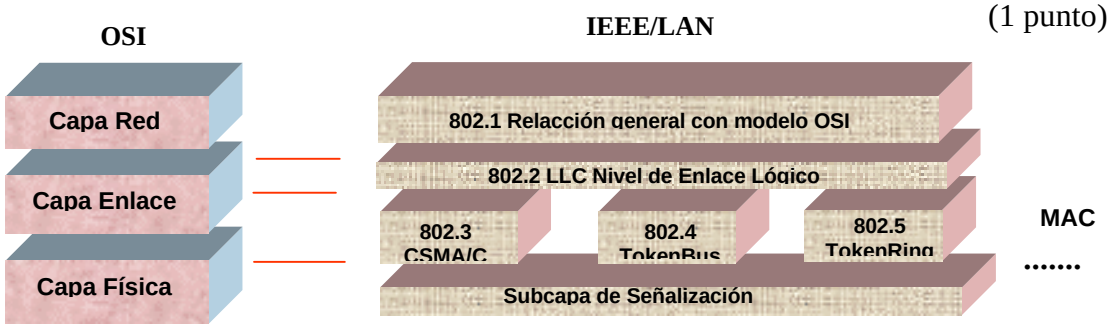
(1 punto)

La calidad de la medida del tiempo que ofrece un reloj real se puede caracterizar mediante una serie de propiedades:

- **Características estáticas**:
  - *Resolución*: mínimo valor representable por el reloj
  - *Intervalo de valores*: límite inferior y superior de tiempo medible
- **Características dinámicas**:
  - *Granularidad*: distancia en tiempo real entre dos tiempos de reloj consecutivos. Definido por el dispositivo físico que provoca el proceso del reloj y generalmente de mayor tamaño que la resolución.
  - *Exactitud*: es la diferencia en una medida absoluta del reloj con respecto a un tiempo físico externo.
  - *Estabilidad*: representa las derivas en la frecuencia de progreso del reloj respecto a una referencia externa.

3. Explicar las diferencias fundamentales entre el modelo de capas OSI y el modelo de capas IEEE para redes de Area Local

(1 punto)



Las redes de **Area Local** siguen un modelo diferente al esquema **OSI** ya que su arquitectura fue desarrollada con anterioridad por los propios fabricantes. El **IEEE** desarrolló los trabajos de normalización cubriendo diferentes normas ajustadas a los productos de diferentes fabricantes bajo la numeración 802.x. Estas normas están en continua evolución.

El modelo **IEEE** se diferencia fundamentalmente en los dos primeros niveles (**Físico** y de **Enlace**). Se reestructuran en tres capas:

- Medio físico de transmisión (**Subcapa de señalización**) [Parte del Nivel Físico OSI]
- Control de acceso al medio (**MAC**) [Nivel Físico + parte del Nivel de Enlace]
- Control de enlace lógico (**LLC**) [Resto del nivel de enlace]

La **capa de red** es equivalente al nivel de red OSI y se encarga de manejar las diferencias con el modelo OSI hacia los niveles superiores.

La mayor diferencia de arquitectura es que el nivel **LLC** permite una comunicación **extremo a extremo** (esto está reservado al nivel de **transporte** en el modelo **OSI**). Esta característica permite independizar el nivel de red del tipo de red de área local que empleemos.

4. Describir el sistema de direccionamiento IPv4 (Poner ejemplos descriptivos)

(1 punto)

El direccionamiento IPv4 se realiza mediante palabras de 32 bits, agrupadas en cuatro bloques de 8 bits (byte). El direccionamiento IPv4 esta jerarquizado en 5 clases en función de la codificación de los primeros bits. Estas clases determinan el agrupamiento de los bits de la dirección en dos partes:

- **parte de red** (identifica la red)
- **parte de nodo/subred**: identifica cada nodo dentro de la red. Así mismo, permite identificar subredes en función de la **máscara de subred**.

A continuación se describen las diferentes clases:

Clase A:	**RED**	**SUBRED/NODO**	
	0xxx xxxx .	xxxx xxxx . xxxx xxxx . xxxx xxxx	
	1111 1111 .	0000 0000 . 0000 0000 . 0000 0000	Máscara Subred Estándar

Clase B: **RED** **SUBRED/NODO**

10xx xxxx . xxxx xxxx . xxxx xxxx . xxxx xxxx

1111 1111 . 1111 1111 . 0000 0000 . 0000 0000 Máscara Subred Estándar

Clase C: **RED** **SUBRED/NODO**

110x xxxx . xxxx xxxx . xxxx xxxx . xxxx xxxx

1111 1111 . 1111 1111 . 1111 1111 . 0000 0000 Máscara Subred Estándar

Clase D: **MULTICAST (28 bits)**

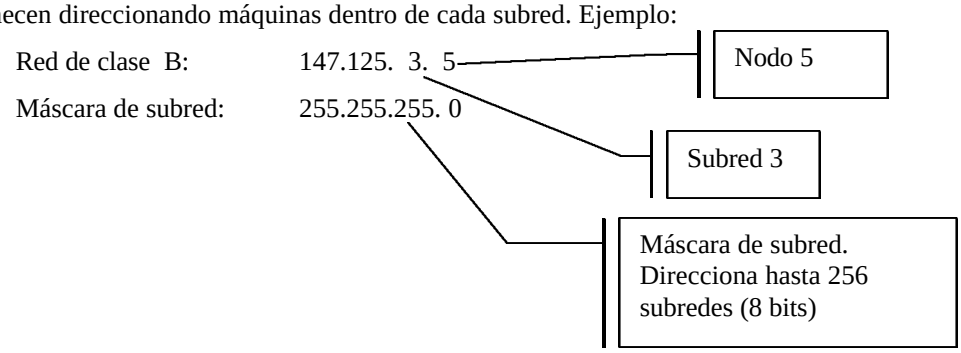
1110 xxxx . xxxx xxxx . xxxx xxxx . xxxx xxxx

Clase E: **Futuras Ampliaciones (27 bits)**

1111 0xxx . xxxx xxxx . xxxx xxxx . xxxx xxxx

Clase	Nodos por clase	Máscara	Dir. Comienzo	Dir. final
A	16.777.216	255.0.0.0	0.0.0.0	127.255.255.255
B	65536	255.255.0.0	128.0.0.0	191.255.255.255
C	256	255.255.255.0	192.0.0.0	223.255.255.255
D	-	-	224.0.0.0	239.255.255.255
E	-	-	240.0.0.0	255.255.255.255

La máscara de subred permite dividir una red en subredes, colocando en la máscara de subred un uno en aquellos bits libres que deseamos que codifiquen una subred. El resto de bits, cuya máscara es cero, permanecen direccionando máquinas dentro de cada subred. Ejemplo:

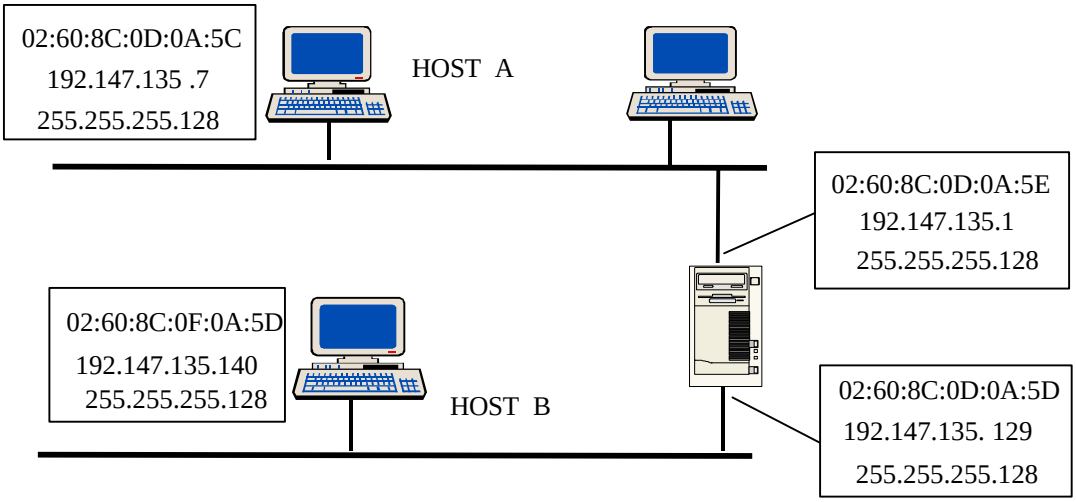


Existen dos valores del direccionamiento de máquina que están reservados:

- Aquella dirección con todos los bits a 0: identifica a toda la red o subred (Ejemplo: 147.125.3.0)
- Aquella dirección con todos los bits a 1: identifica un paquete de boradcast que debe ser enviado a todos los nodos de la red o subred (Ejemplo: 147.125.3.255)

5. **Describir la secuencia de mensajes y protocolos involucrados en una transmisión de un datagrama UDP, de 2000 bytes de tamaño, desde el nodo A al nodo B descritos en la figura. Para cada nodo se indican las direcciones MAC, IP y máscara de red. La red utilizada es Ethernet.**

(1 punto)



- El datagrama **UDP** genera un único datagrama **IP**.
- El tamaño del datagrama supera el MTU de la red Ethernet (1500 bytes) por lo que se generarán dos fragmentos a nivel IP.
- El protocolo IP comprueba las direcciones IP y máscaras de los nodos origen y destino determinando que se encuentra en una subred diferente (el bit 8 que codifica la subred es diferente en ambas direcciones), por tanto **envía los dos fragmentos del datagrama al router** (192.147.135.1).
- Para enviar el datagrama al router se evalúa la tabla **ARP** generando, si fuera necesario, un mensaje **ARP request** (broadcast) que sería respondido con un **ARP reply** por parte del router indicando su dirección MAC (02:60:8C:0D:0A:5E).
- Conocida la dirección MAC se encapsula cada datagrama en una trama **Ethernet** y se transmite al router.
- El router recibe la trama y la pasa al nivel **IP**. Comprueba en la tabla de enrutamiento la dirección IP destino enviando el datagrama a la subred 128 (enlace 192.147.135. 129).
- El destino final del datagrama se encuentra ya en la subred actual, por lo que se evalúa la dirección MAC mediante **ARP**. Se genera un mensaje **ARP request** (broadcast) que sería respondido con un **ARP reply** por parte de la máquina destino (02:60:8C:0F:0A:5D)
- Finalmente se enviarían los dos fragmentos del datagrama **IP** al nodo destino (192.147.135.140) encapsulado en una trama **Ethernet**.
- Al existir fragmentación se recompondrían los fragmentos formando un único datagrama **UDP**

Duración del Examen: 2 ½ horas