2. Estructura de los sistemas de computación

En esta sección repasaremos los componentes de un sistema y sus principales características, para luego ver los diferentes mecanismos que se ejecutan para la protección de estos.

1. **Componentes de un sistema**
    - CPU
    - Memoria
    - Dispositivos de E/S

CPU

Es la unidad central de procesamiento, la cual permite ejecutar instrucciones, y por ende es la que ejecuta los programas.

El ciclo básico consiste en tomar la instrucción apuntada por el PC (*program counter*) (*fetching*), decodificarla para determinar su tipo y operandos (*decoding*), ejecutarla (*executing*), y luego continuar con la siguiente instrucción. Algunas arquitecturas implementan en paralelo estas etapas (pipeling).

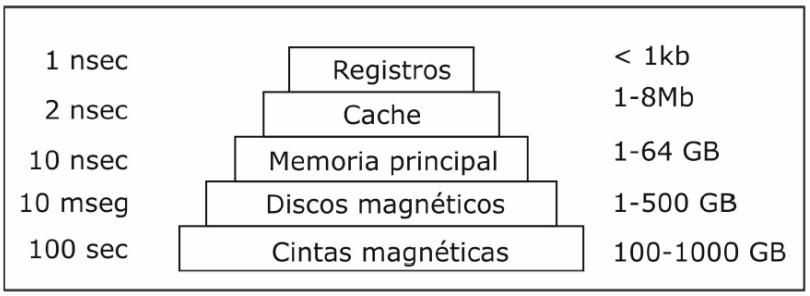
Existen varias arquitecturas de procesador que se clasifican en:
- RISC(Reduced Instruction Set Computer)
- CISC(Complex Instruction Set Computer)

Dado que la velocidad del procesador es varios órdenes mayor a la velocidad de la RAM, se crearon registros a nivel de la CPU y la cache. Los registros son la memoria más rápida a la cual accede la CPU, y están integrados al chip. La caché se encuentra entre la RAM y la CPU y es una memoria más rápida que la RAM.

Proceso de Interrupciones:
1 – Se preserva el estado actual
2 – Se determina el tipo de la interrupción
3 – Se ejecuta la rutina de interrupción correspondiente
4 – Se vuelve al estado antes de la interrupción

MEMORIA

El sistema de memoria es construido en base a una jerarquía, que permite mejorar la utilización del procesador:



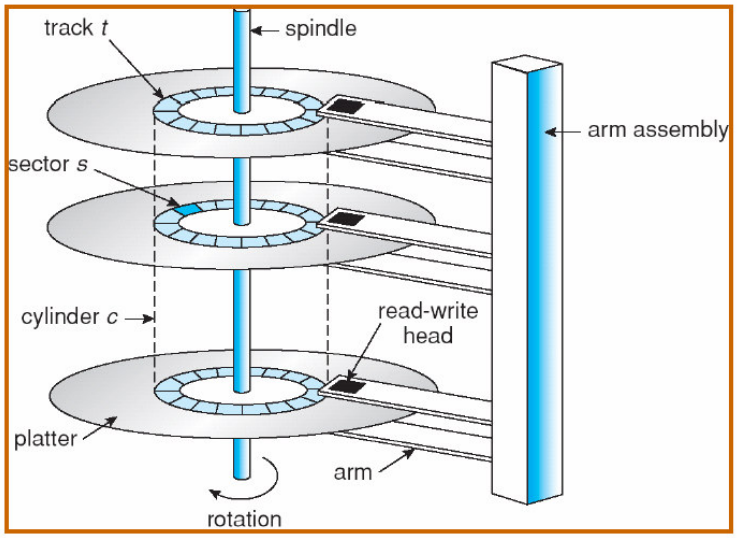
Caches:
El concepto es mantener una copia de la memoria que está siendo utilizada en un medio temporal de mayor velocidad de acceso.
El medio de memoria cache es mucho menor en capacidad, pero más veloz que el dispositivo principal. Esto genera que el tamaño del cache y sus políticas de reemplazo tengan un alto impacto en la mejora real de la performance.

Un problema que introduce la memoria cache en ambientes multiprocesadores, es la coherencia y consistencia de los datos que están replicados, ya que una palabra puede estar copiada en diferentes caches. Para solucionar estos problemas surgen técnicas como *write-update*, *write-invalidated*.

Discos Duros:
Son dispositivos de velocidad de acceso mucho menor a la RAM, ya que tiene componentes mecánicas, pero es de mayor capacidad.

Consta de platos de metal y un brazo mecánico que contiene las cabezas de lectura/escritura para cada plato. Veamos los componentes más significativos del disco duro:

- Pistas (tracks). Se divide la superficie de los platos lógicamente en pistas.
- Sector: Cada pista se divide en un conjunto de sectores.
- Cilindro: Conjunto de pistas en la misma posición del brazo mecánico.



El Bloque es la unidad de transferencia desde el disco a los diferentes dispositivos.

DISPOSITIVOS E/S

En general se componen de un dispositivo y una controladora (chip que controla físicamente al dispositivo, acepta comandos del sistema operativo (del driver correspondiente) y genera las señales correspondientes sobre el dispositivo).
La interfaz que presenta la controladora al sistema es mucho más simple que la provista por el dispositivo.

Device Driver: Software que se comunica con la controladora, hay uno para cada controladora, son incorporados al SO de diferentes maneras:

- Cargados estáticamente al núcleo
- Al cargar el sistema.
- Dinámicamente bajo demanda.

Las controladoras tienen un conjunto de registros para comunicarse y ejecutar comandos sobre ella, a estos se puede acceder mediante:

- Memory Mapped I/O: Se mapean los registros de la controladora a la memoria principal (fuera la memoria de usuario), en vez de escribir se escribe en la memoria correspondiente, efectuando la transferencia a los registros de forma transparente (no necesita instrucciones privilegiadas).
- Direct I/O instructions: Se asigna un puerto a los registros. Se utilizan las instrucciones privilegiadas del sistema IN y OUT, que generan señales en el bus del sistema para seleccionar el dispositivo (no consume memoria principal).

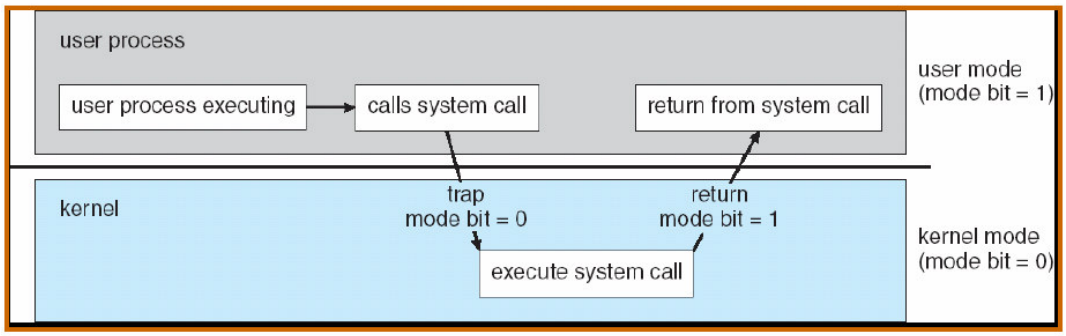
Métodos:

- Polling: El CPU efectúa una solicitud de I/O y se queda en un busy waiting consultando a la controladora hasta completada la misma.
- Interrupt Driven I/O: CPU genera el pedido y sigue con otras tareas. Al resolverse el pedido la controladora del dispositivo genera una interrupción al procesador. Hay una vector de rutinas de atención de interrupciones.
- DMA: Se utiliza un chip especial que permite la transferencia a memoria principal por parte de una controladora, de forma transparente al CPU.

2. Protección de Hardware

Con la introducción de sistemas multiprogramados y multiusuarios se empezaron a generar problemas en el uso de los recursos debido a procesos “mal programados” o “mal intencionados”. Fue necesaria la introducción de protección entre los distintos procesos que ejecutaban en un sistema.

- Modo Dual
  - Requiere soporte de hardware (bit que indica l modo actual)
  - **Modo Usuario:** se permite ejecutar un conjunto reducido de instrucciones de hardware. Así ejecutan los procesos a nivel de usuario.
  - **Modo Monitor:** Todas las instrucciones de hardware disponibles. Solo el SO debe ejecutar en este modo.
  - Garantiza que los procesos de usuario no accedan directamente a los dispositivos de E/S, para acceder usaran system calls (generan interrupciones a nivel de software y el sistema pasa a modo monitor).
  - Todas las instrucciones de E/S son privilegiadas, evitando que un usuario ejecute en modo monitor.

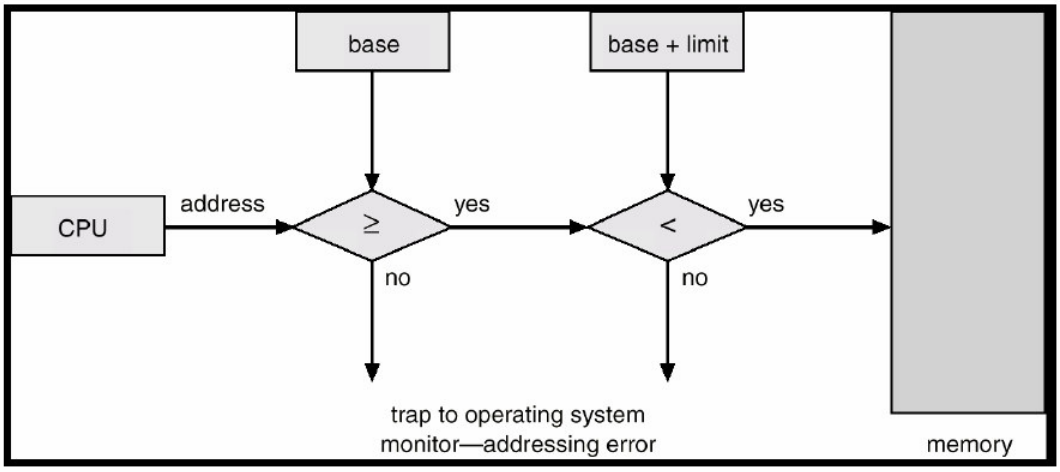


- Protección de Memoria

  Es necesario proteger la memoria del núcleo (por ejemplo el vector de interrupciones) y de los procesos entre sí (un proceso no debería acceder a la memoria de otro).

  Se deben validar las direcciones generadas por los procesos. Una forma es usar registros: base y límite, si la dirección no es válida se genera un trap.

  El registro base contiene la dirección de memoria física más baja que se puede acceder y el registro limite contiene el tamaño del bloque de memoria a partir del registro base.



  La MMU es el componente de hardware que convierte las direcciones lógicas a físicas, sólo debe ser administrada en modo monitor.

- Protección de CPU

  Una vez que a un proceso se le asigna el procesador, puede que nunca más se retorne el control al sistema. Una posible solución es utilizar un timer que interrumpa el procesador cada cierto tiempo (se carga un contador que se va decrementando en cada interrupción del timer, cuando este alcanza el 0 se quita el CPU al proceso y se llama al planificador para que asigne al CPU otro proceso).

  La instrucción que carga el contador debe ser privilegiada.