AAAC & TAC
Clase #8
x86, x86-64, modo protegido

Facultad de Ingeniería
Universidad de la República

Instituto de Computación
Curso 2013

Modos de operación

- Modo Real (procesador arranca en este modo)
- Modo Protegido
- System Managment Mode (SMM)
  - Manejo de energía, mediante una interrupción externa se accede a este modo y el procesador brinda un espacio de memoria separado preservando contexto
- Modo Virtual-8086
  - Habilita correr software 8086 (16 bits) en un entorno protegido
- Modo IA-32
  - En arquitecturas de 64 bits, permite compatibilidad con software 32bits

Modo protegido

- Brinda múltiples funcionalidades que potencian la multitarea y mejoran la estabilidad del sistema
- Entre estas funcionalidades está la protección de memoria, paginación y soporte de un manejo de memoria virtual, a través de la MMU (memory management unit)
- La mayoría de los S.O. actuales como Windows y Linux corren en modo protegido
- Modo Real deshabilita estas mejoras para brindar compatibilidad hacia atrás (DOS)

Niveles de protección

- Numerados del 0 al 4 (a mayor número menores privilegios
- Restringen acceso a memoria de datos, código, etc.
- Restringen las instrucciones accesibles

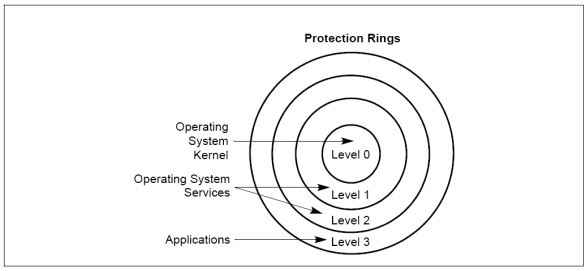

Figure 4-3. Protection Rings

Registros de control

- Existen cinco registros de 32 bits, CR0 .. CR4, que determinan:
  - el modo de funcionamiento del procesador
  - características de la actual tarea en ejecución
- CR0 controla el modo de operación y el actual estado del procesador
- CR1 reservado
- CR2 y CR3 usado por el sistema de paginación de memoria
- CR4 habilita diversas extensiones de la arquitectura.

Registros de segmento

- Cada registro de segmento contiene un índice de 16 bits dentro de una tabla de descriptores de segmentos.
- Cada descriptor de segmento especifica (entre otras cosas)
  - Dirección base
  - Límite
  - Nivel de privilegio

Registros de segmento

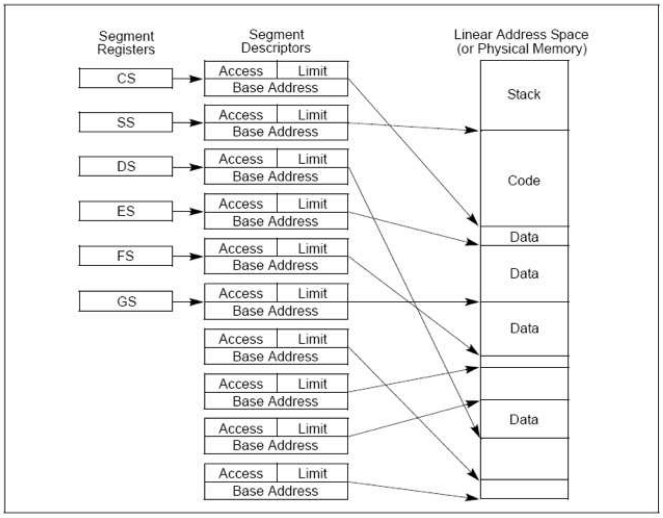

Figure 3-4. Multi-Segment Model

Registros de segmento

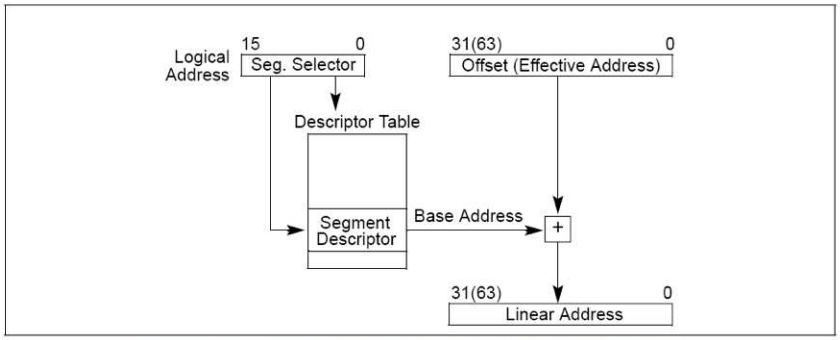

Figure 3-5. Logical Address to Linear Address Translation

Paginación

- Permite mapear el espacio de memoria lineal de 4GBytes a memoria física, del mismo tamaño o menor.
- Si en el momento de acceder a una página ésta no se encuentra en memoria, se produce una excepción, permitiendo el manejo de un sistema de memoria virtual.

Paginación

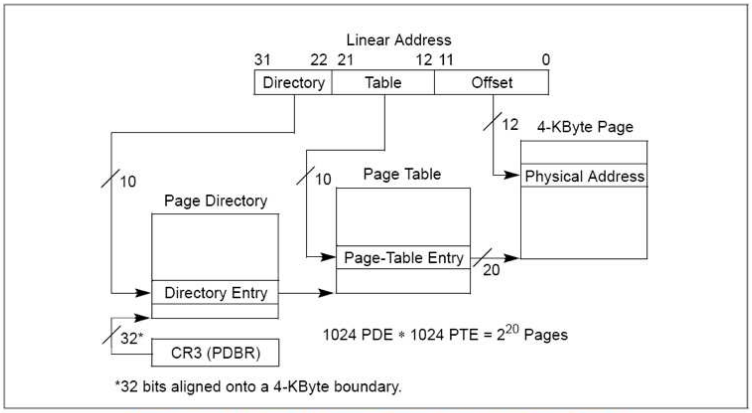

Figure 3-12. Linear Address Translation (4-KByte Pages)

Segmentación + paginación

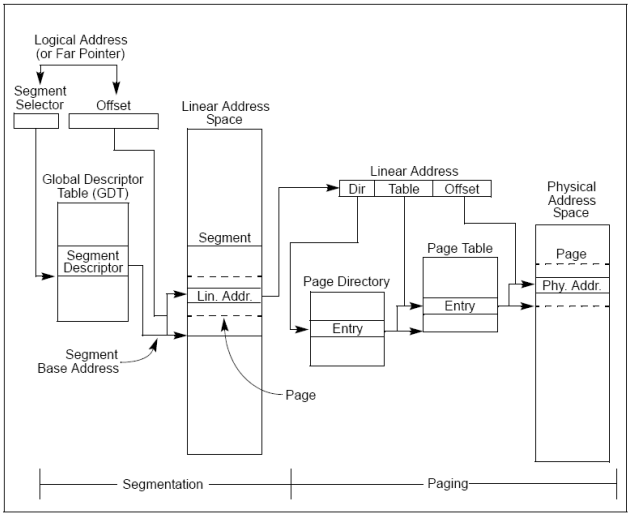

Figure 3-1. Segmentation and Paging

Segmentos

- 6 registros de segmentos: CS, DS, SS, ES, FS, GS
- Tienen una parte visible y una oculta con: Dirección base, límite e información de acceso

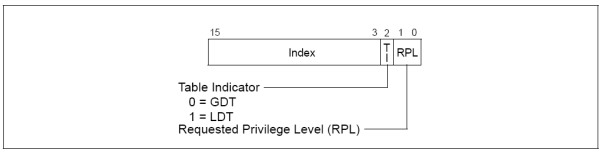

Figure 3-6. Segment Selector

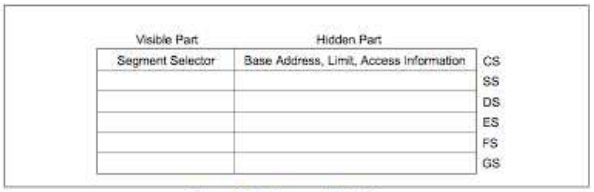

Figure 3-7. Segment Registers

Tablas de descriptores de segmento

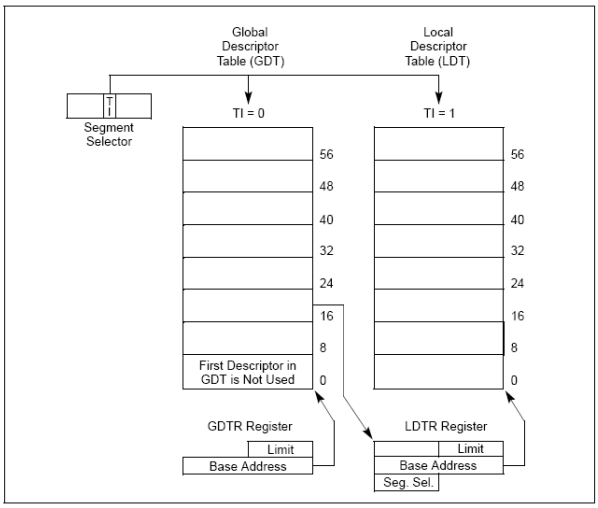

Figure 3-10. Global and Local Descriptor Tables

Interrupciones

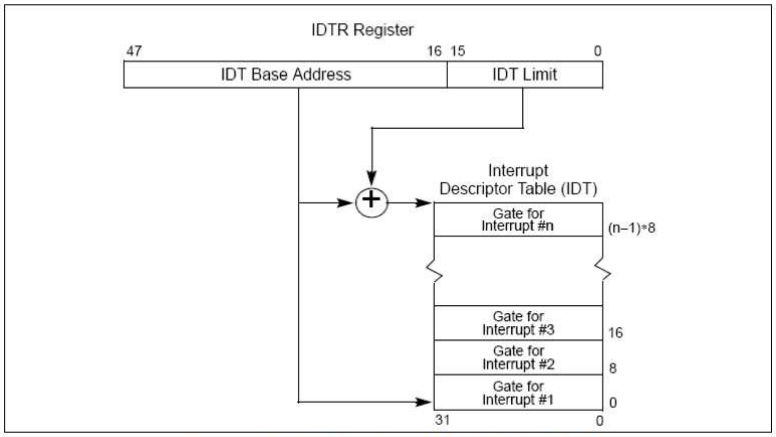

Figure 5-1. Relationship of the IDTR and IDT

Interrupciones

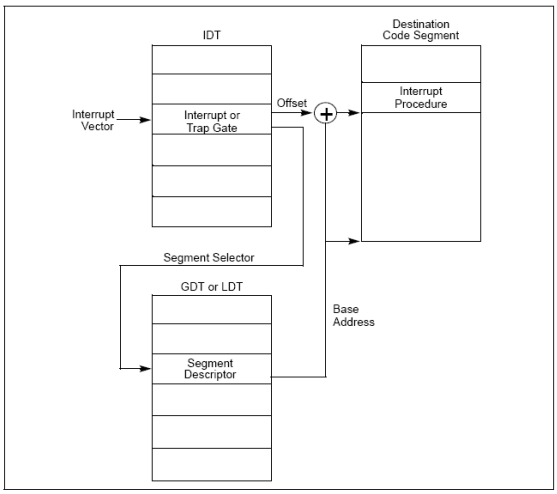

Figure 5-3. Interrupt Procedure Call

Interrupciones

- Interrupciones
  - Ocurren asincrónicamente por eventos de hardware y también pueden ser invocadas por software
- Excepciones
  - Procesador detecta condiciones de error al ejecutar una instrucción (división por cero, violaciones de protección, páginas faltantes, etc.)

Tareas

- Mantienen un estado, al ser llamadas retoman la ejecución.
- Pueden ser usadas también en el manejo de interrupciones
- Dos partes:
  - Un entorno de ejecución
  - Un TSS (Task-state segment)
    - Especifica los segmentos que conforman el entorno de ejecución y provee espacio de almacenamiento para guardar el estado de una tarea.

Tareas

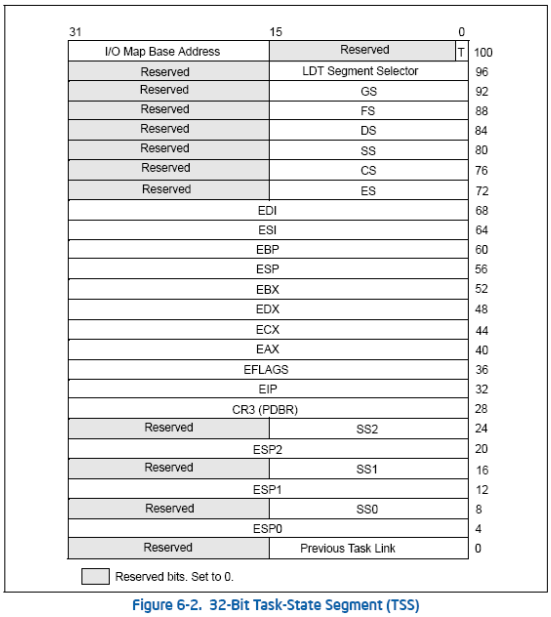

Figure 6-2. 32-Bit Task-State Segment (TSS)

- Contexto de una tarea cargado y salvado automáticament e por hardware
- Existen 3 niveles de stack, de forma que invocaciones desde distintos niveles de protección no compartan el stack

Tareas

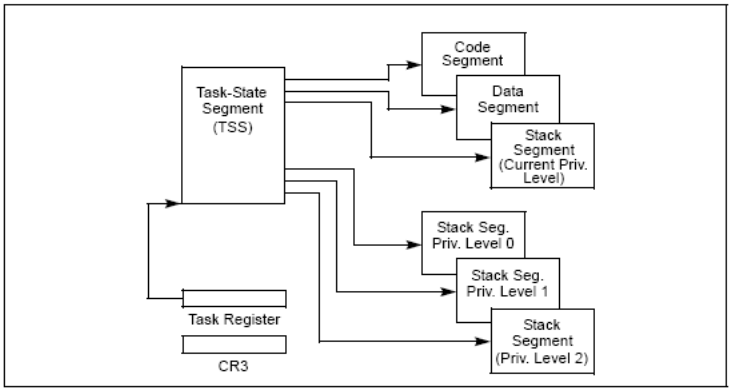

Figure 6-1. Structure of a Task

Tareas

- Se despachan en dos formas:
  - Software (explícito)
    - Call a una tarea (call a un task-gate descriptor)
    - Jump a una tarea (jmp a un task-gate descriptor)
  - Procesador (implícito)
    - Call del procesador a un interrupt-handler task
    - Call del procesador a un exception-handler task
    - Un iret cuando el NT en las flags está prendido