Técnicas Digitales III

Modo Real
Modo Protegido

Modo Real vs Modo Protegido

- El Modo Real es el modo inicial de todos los procesadores Intel (y sus clones).
- Su presencia en procesadores modernos es requerida por compatibilidad.
- Todos los sistemas operativos modernos se ejecutan en Modo Protegido.

Modo Real vs Modo Protegido

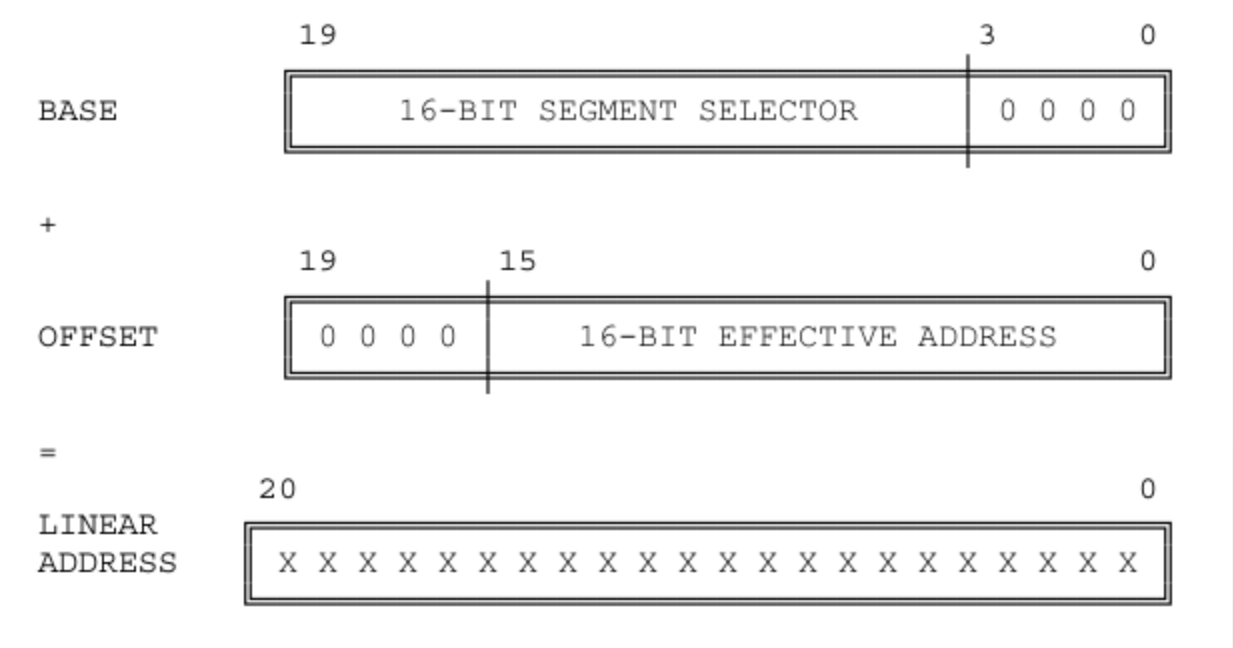
Modo Real	Modo Protegido
Menos de 1MB de RAM disponible	Toda la RAM disponible
No existe la protección de memoria basada en hardware.	Protección de memoria basada en hardware.
No hay modo de restringir las instrucciones que un programa de usuario puede ejecutar	Existen niveles de privilegio
El tamaño de los operandos es de 16 bits	El tamaño de los operandos es de 32 o 64 bits
Acceso a las funciones del BIOS	No es posible el acceso a las funciones del BIOS

Ingreso a Modo Protegido

```
lgdt [GlobalDescriptorTable] ;
mov eax,cr0 ; eax = Control Register 0
or al,1     ; Pone en uno el bit de habilitación de protección
cli         ; Deshabilita las interrupciones
mov cr0,eax ; Inicia Modo Protegido.
```

Direccionamiento de Memoria

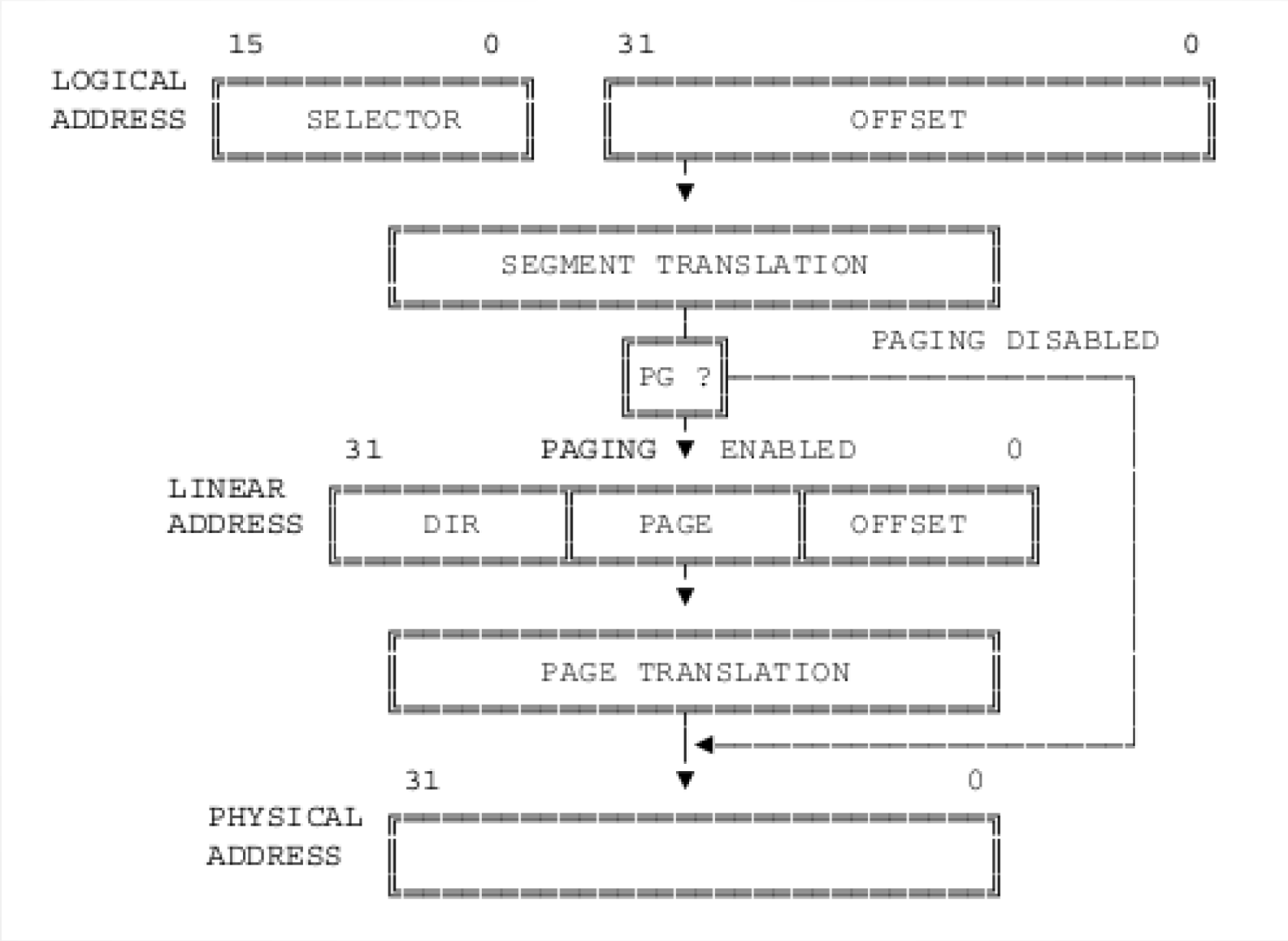
- La dirección física en Modo Real se forma sumando la dirección base con desplazamiento.
- La dirección base se forma rotando cuatro bits a la izquierda el selector de segmento.



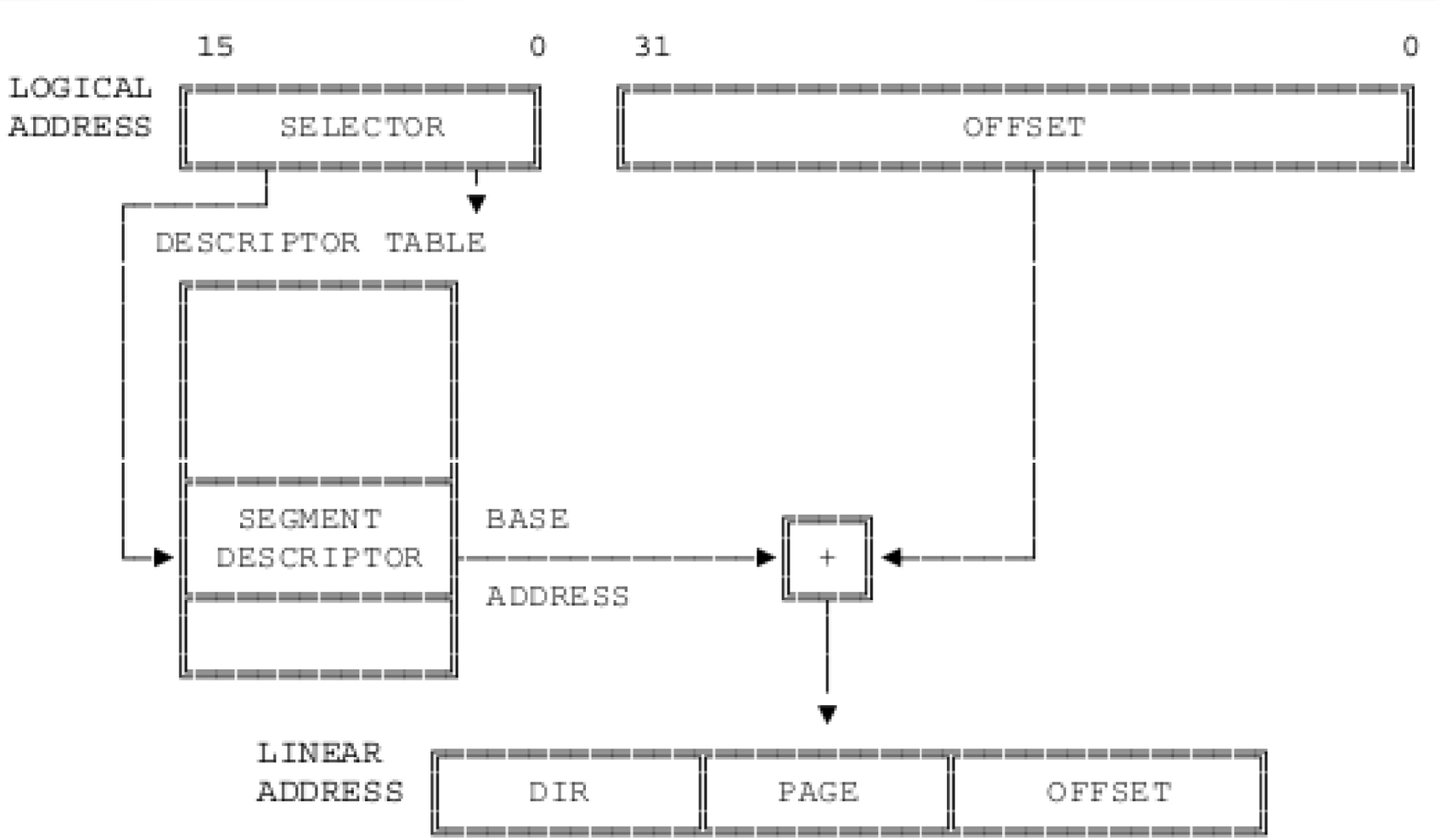
Direccionamiento de Memoria

- En Modo Protegido, el procesador transforma direcciones lógicas (utilizadas por los programadores) en direcciones físicas (la dirección real en la memoria física) en dos pasos:
  - Traducción de Segmento
  - Traducción de Página
- Estas traducciones son realizadas de tal manera que no son visibles al programador

Traducción de Direcciones

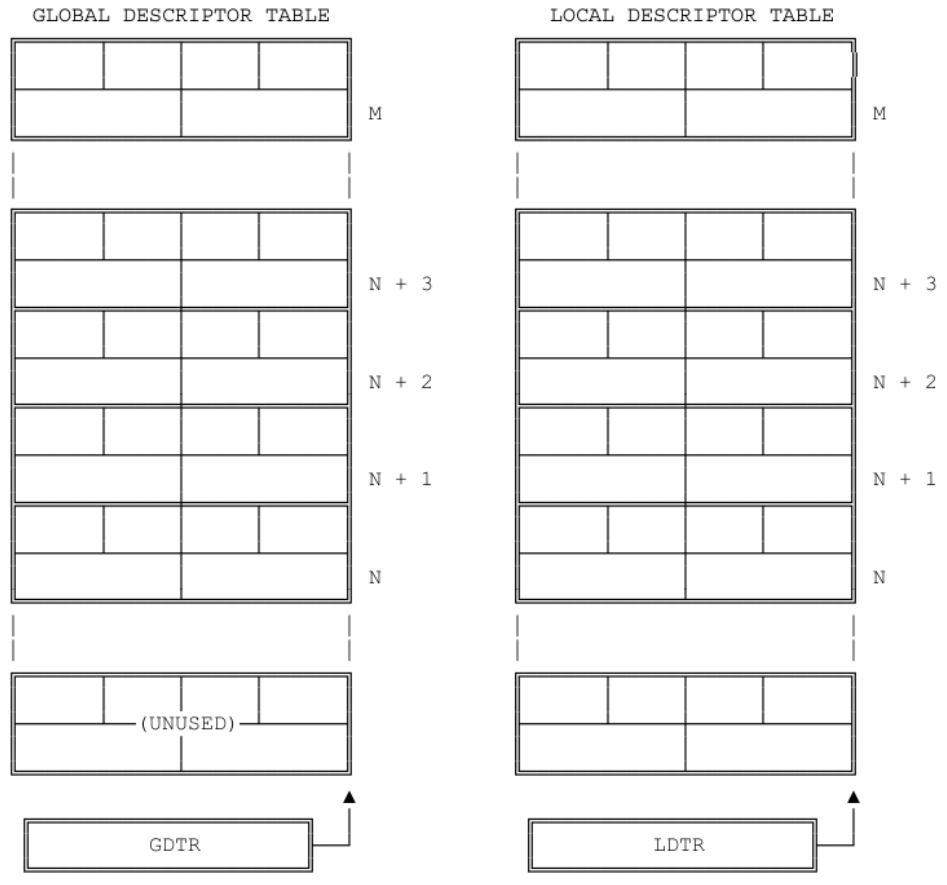


Traducción de Segmento



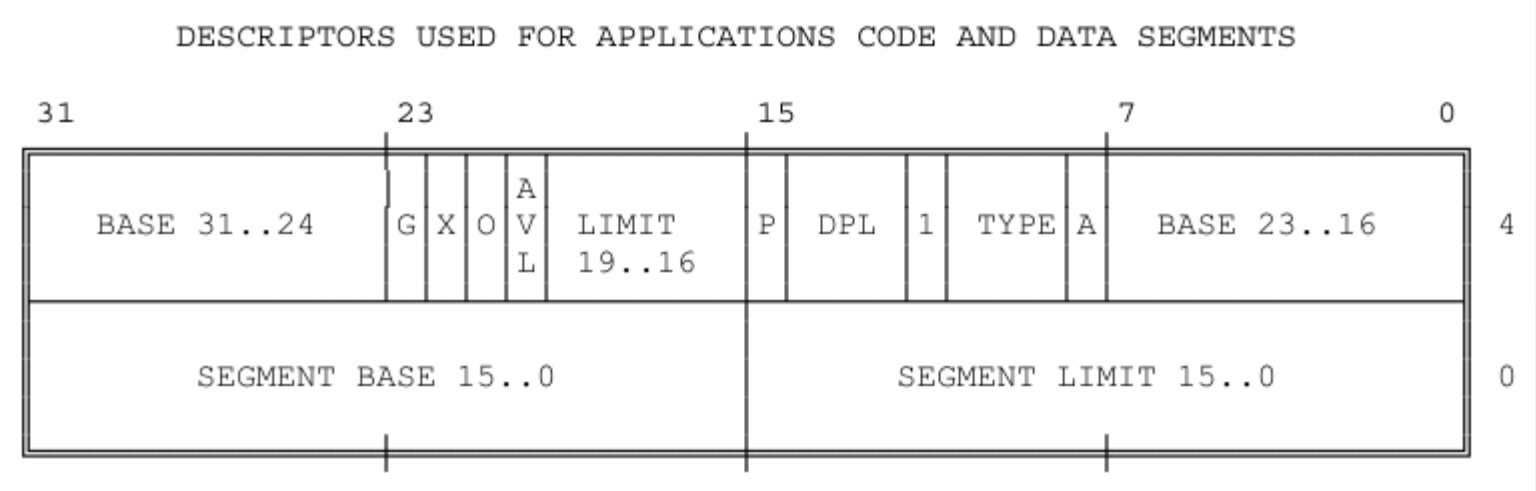
Tablas de Descriptores

- Una tabla de descriptores es simplemente un arreglo de memoria con elementos de 8 bytes.



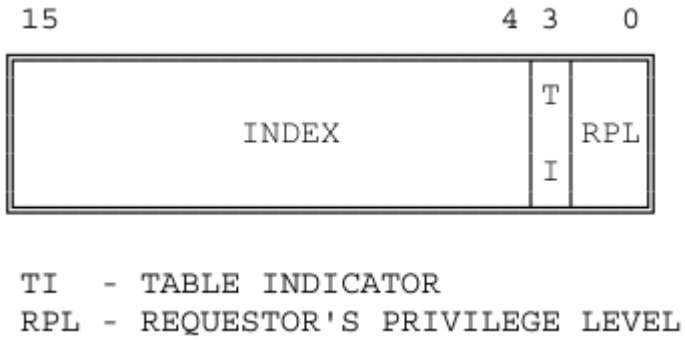
Descriptores

- El descriptor provee al procesador con la información que necesita para mapear una dirección lógica en una dirección lineal.
- Son creados por compiladores, enlazadores, cargadores, o el sistema operativo, no por programadores de aplicaciones.



Selectores

- Esta porción de una dirección lógica especifica una tabla e indexa un descriptor en esa tabla.



Protección

- El Modo Protegido abarca estos aspectos:
  - Chequeo de tipo
  - Chequeo de límite
  - Restricción de dominio direccionable
  - Restricción de puntos de entrada a procedimientos
  - Restricción del set de instrucciones

Protección a nivel segmento

- Chequeo de Tipo:
  - Distingue entre diferentes formatos de descriptores
  - Especifica el uso previsto del segmento
  - Ejemplos:
    - El registro CS solo puede contener un selector de un segmento ejecutable
    - Solo selectores de segmentos con permiso de escritura pueden cargarse en SS.
    - Ninguna instrucción puede escribir en un segmento ejecutable.
    - Ninguna instrucción puede leer un segmento ejecutable si el bit de lectura no está en uno.

Protección a nivel segmento

- Chequeo de límite
  - El procesador no permite el direccionamiento fuera del segmento.
- Niveles de privilegio
  - Las siguientes entidades poseen niveles de privilegio:
    - Descriptores (DPL)
    - Selectores (RPL)
    - Registro interno del procesador (CPL)
  - El procesador automáticamente evalúa el derecho de un procedimiento de acceder a otro segmento comparando el CPL con uno o más niveles de privilegio.

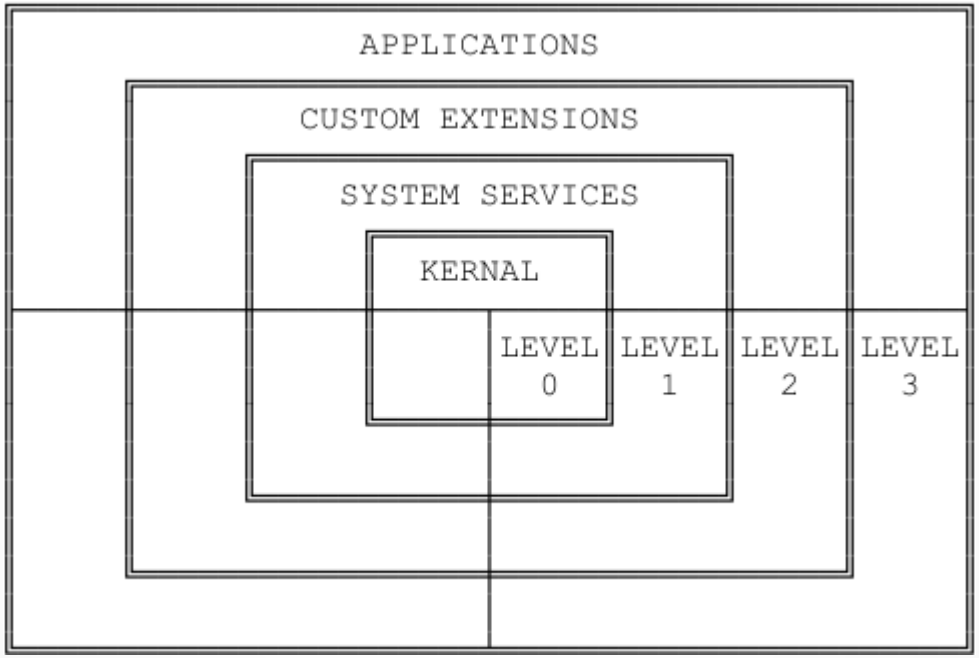
Protección a nivel de segmento

- Las instrucciones que afectan estructuras de datos del sistema solo pueden ser ejecutas en el anillo cero.

```
CLTS                — Clear Task-Switched Flag
HLT                 — Halt Processor
LGDT                — Load GDL Register
LIDT                — Load IDT Register
LLDT                — Load LDT Register
LMSW                — Load Machine Status Word
LTR                 — Load Task Register
MOV to/from CRn     — Move to Control Register n
MOV to /from DRn    — Move to Debug Register n
MOV to/from TRn     — Move to Test Register n
```

Protección a nivel segmento

- No es necesario utilizar los cuatro niveles de privilegio.



Interrupciones y Excepciones

- Las Interrupciones y Excepciones son tipos especiales de transferencia de control, funcionan como llamadas (CALLs) no programadas. Alteran el flujo normal del programa para manejar eventos externos, para reportar errores o condiciones excepcionales.
- La diferencia entre Interrupciones y Excepciones es que las interrupciones son usadas para manejar eventos externos asíncronos, mientras que las excepciones manejan condiciones detectadas por el propio procesador mientras ejecuta instrucciones.

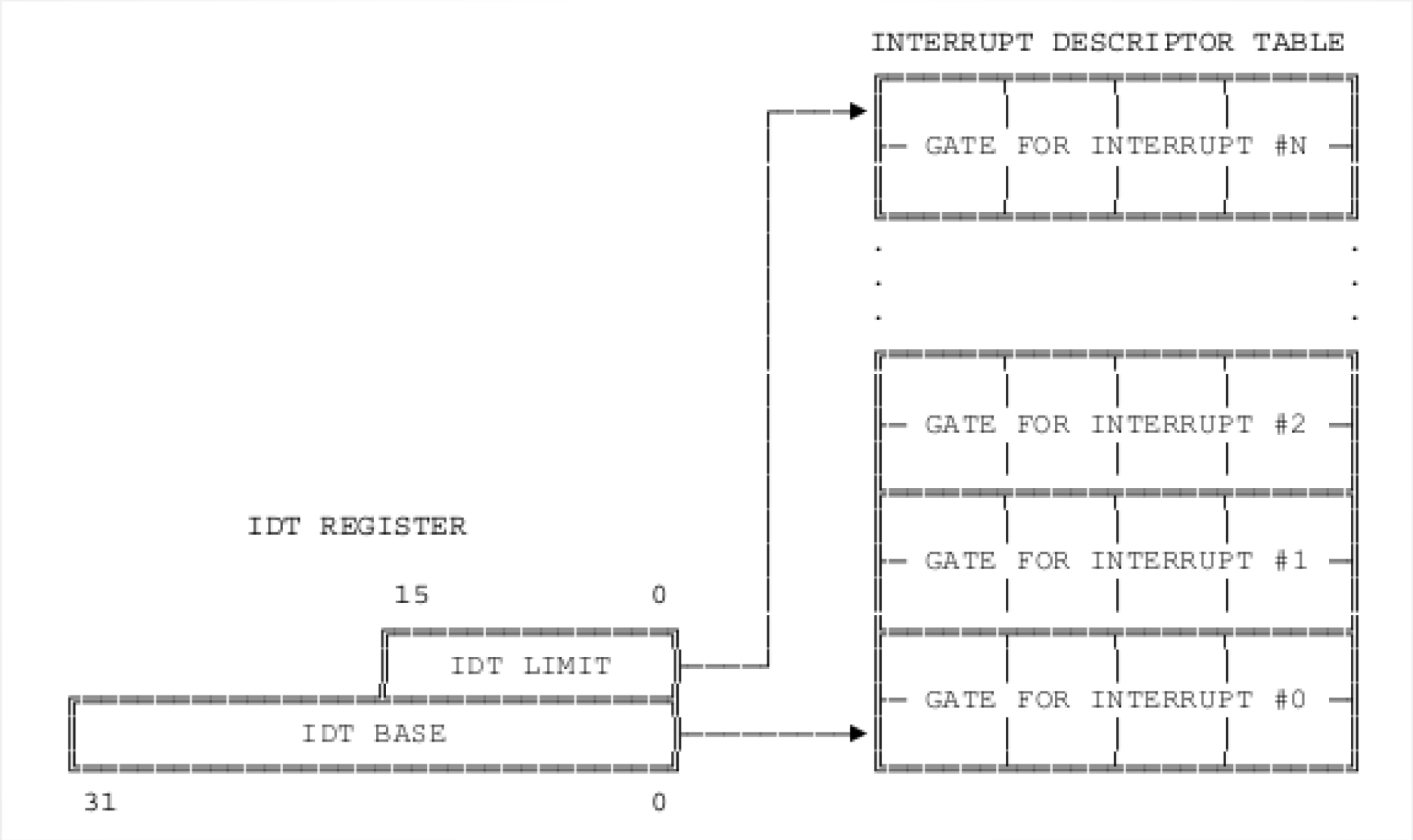
Interrupciones y Excepciones

- Hay dos fuentes de interrupciones y dos fuentes de excepciones:
- Interrupciones:
  - Enmascarables: pin INTR
  - No enmascarables: pin NMI
- Excepciones:
  - Detectadas por el procesador
  - Programadas (instrucción INT), habitualmente llamadas “interrupciones de software”

Interrupciones y Excepciones

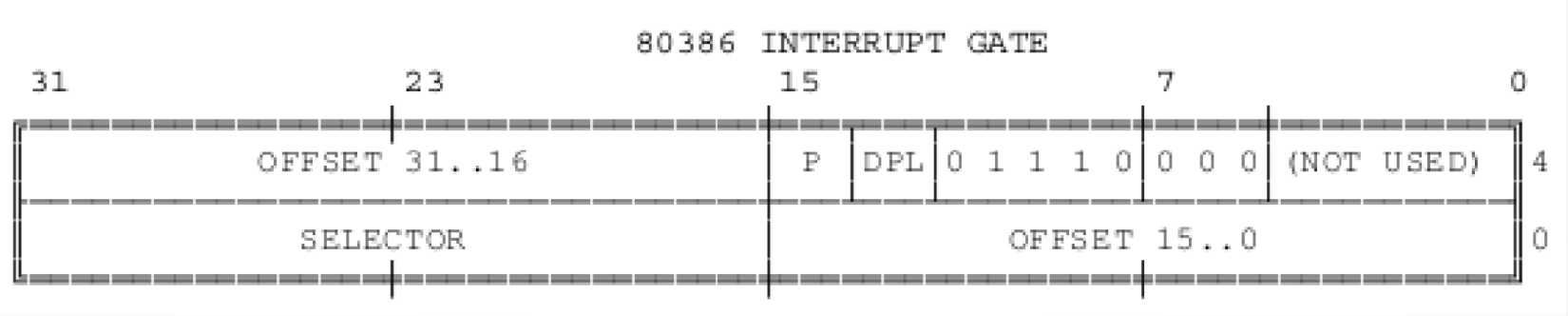
- La Tabla de Descriptores de Interrupción (IDT) asocia cada interrupción o excepción con un descriptor de las instrucciones que sirven el evento asociado.
- La IDT puede residir en cualquier parte de la memoria. El procesador localiza la IDT a través del registro IDTR.
- Las instrucciones LIDT y SIDT operan en el registro IDTR.

Interrupciones y Excepciones



Interrupciones y Excepciones

- La IDT puede contener tres tipos de descriptores:
  - Task gates
  - **Interrupt gates**



  - Trap gates

Interrupciones y Excepciones

- Cuando responde a una interrupción o una excepción, el procesador utiliza el identificador del evento para indexar un descriptor en la IDT.
- El selector de la puerta apunta a un descriptor de segmento ejecutable.
- El desplazamiento apunta al inicio del procedimiento de manejo de la interrupción o excepción.

Interrupciones y Excepciones