DEPARTAMENTO DE INGENIERÍA ELECTRÓNICA
UNIVERSIDAD POLITÉCNICA DE MADRID

EL MODO PROTEGIDO

Ventajas:

- Permite acceder a toda la memoria sin restricciones
- Pueden establecerse protecciones sobre los recursos
- Todas las prestaciones del procesador disponibles
- No implica mayor velocidad de ejecución
- Mecanismo de conmutación de tareas
- Memoria virtual

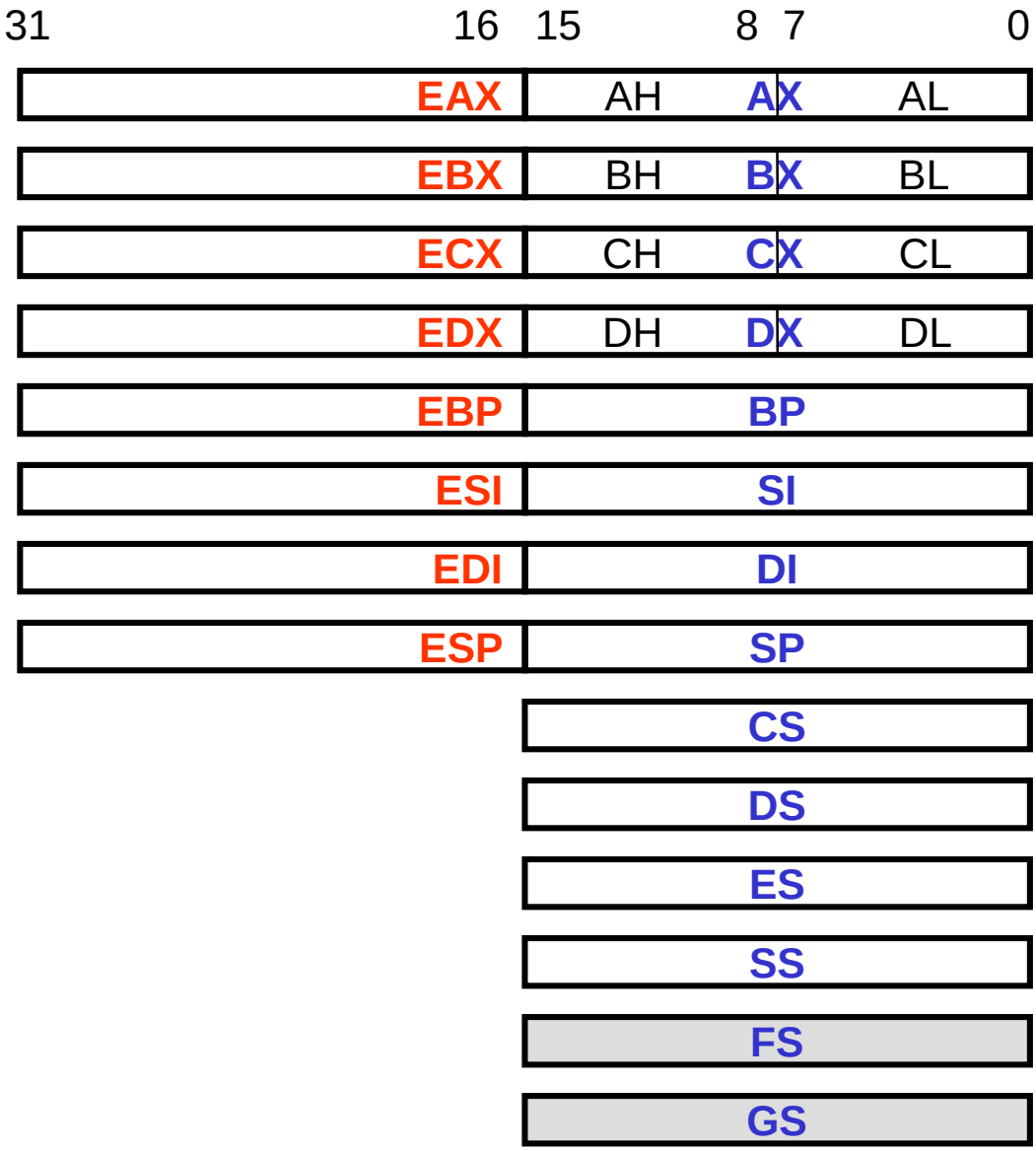
Inconvenientes:

- Muy complicado
- Servicios BIOS, DOS no disponibles
- Programación en Ensamblador desaconsejable

DEPARTAMENTO DE INGENIERÍA ELECTRÓNICA
UNIVERSIDAD POLITÉCNICA DE MADRID

CONSIDERACIONES INICIALES

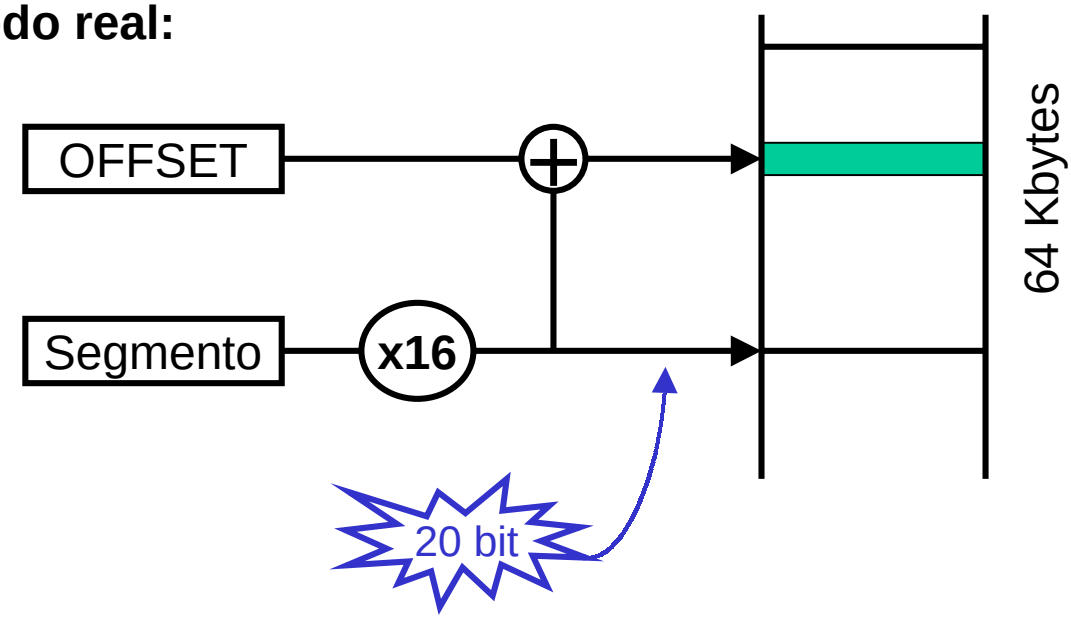
Modo protegido del 386 y siguientes



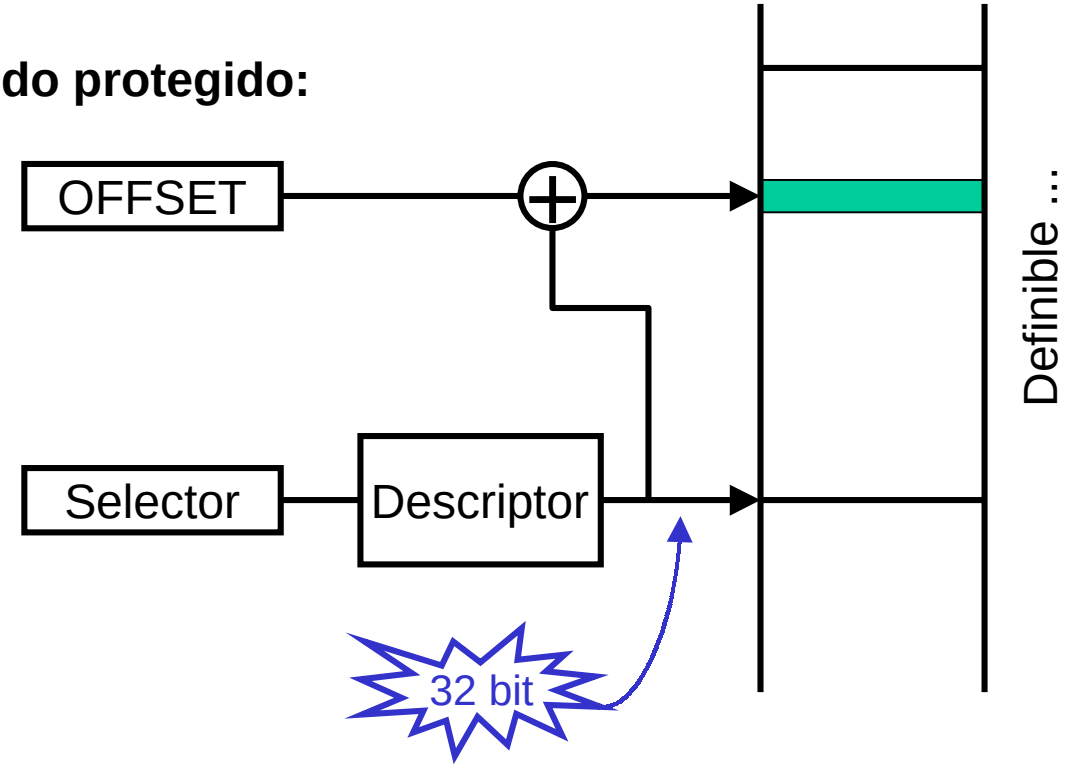
DEPARTAMENTO DE INGENIERÍA ELECTRÓNICA
UNIVERSIDAD POLITÉCNICA DE MADRID

ACCESO A LA MEMORIA

Modo real:

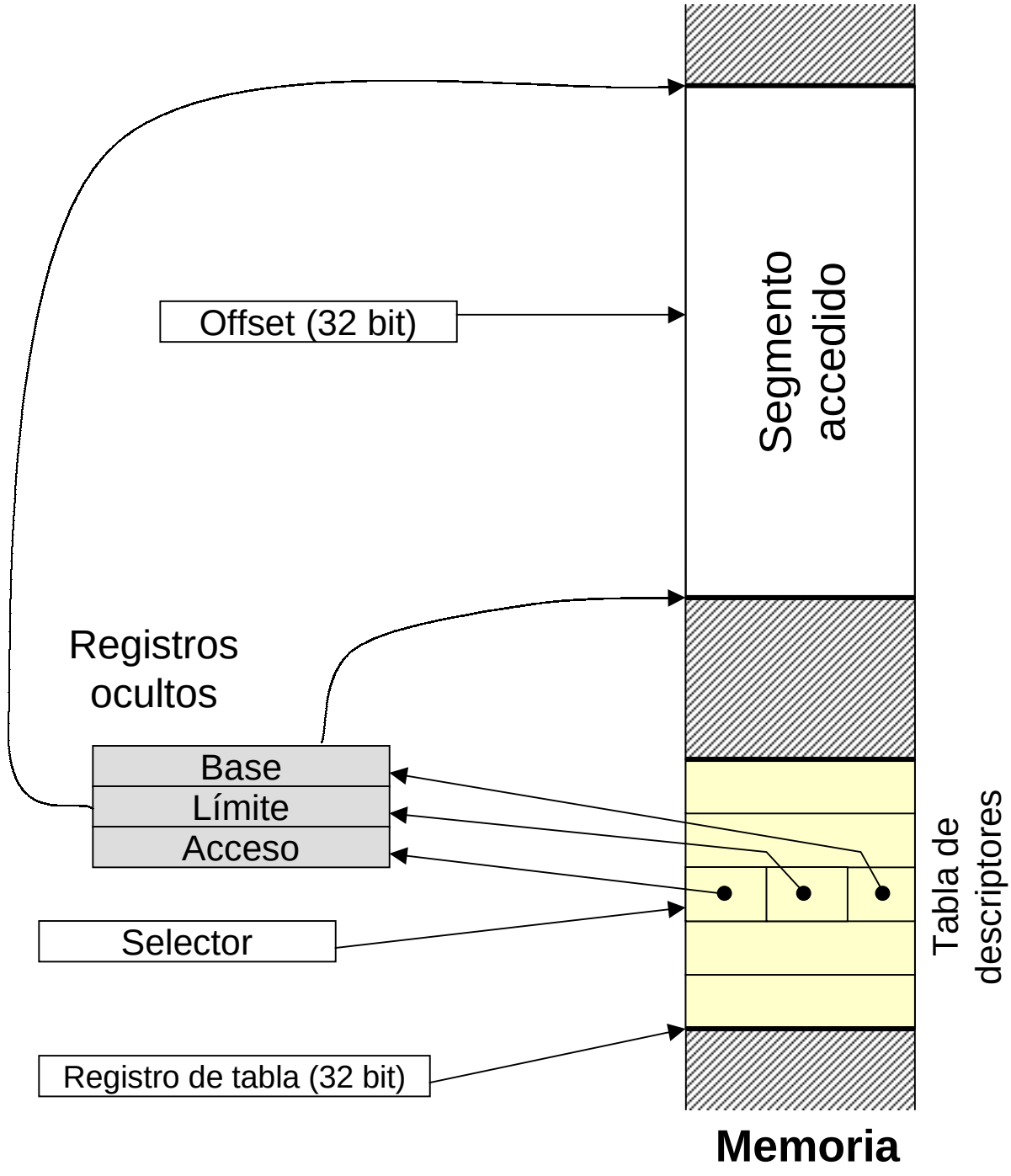


Modo protegido:



DEPARTAMENTO DE INGENIERÍA ELECTRÓNICA
UNIVERSIDAD POLITÉCNICA DE MADRID

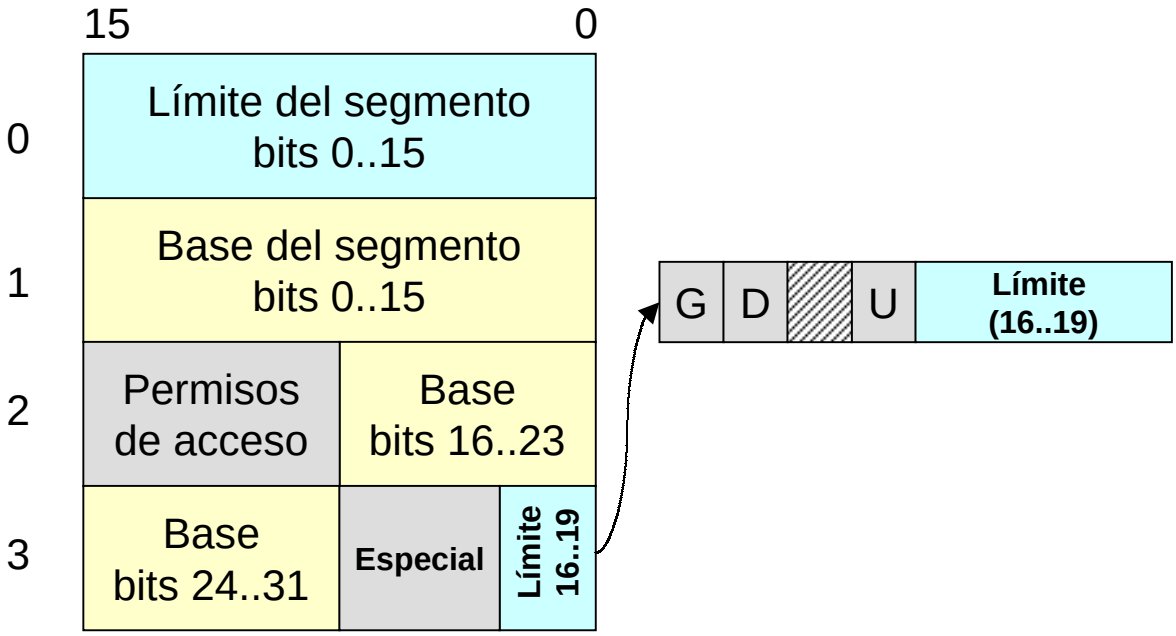
TABLAS DE DESCRIPTORES



DEPARTAMENTO DE INGENIERÍA ELECTRÓNICA
UNIVERSIDAD POLITÉCNICA DE MADRID

TABLAS DE DESCRIPTORES

Formato de un descriptor 386:



Byte de permisos de acceso:

P	DPL	1	0	ED	W	A

Segmento de datos

P	DPL	1	1	C	R	A

Segmento de código

P	DPL	0	TIPO

Descriptor especial

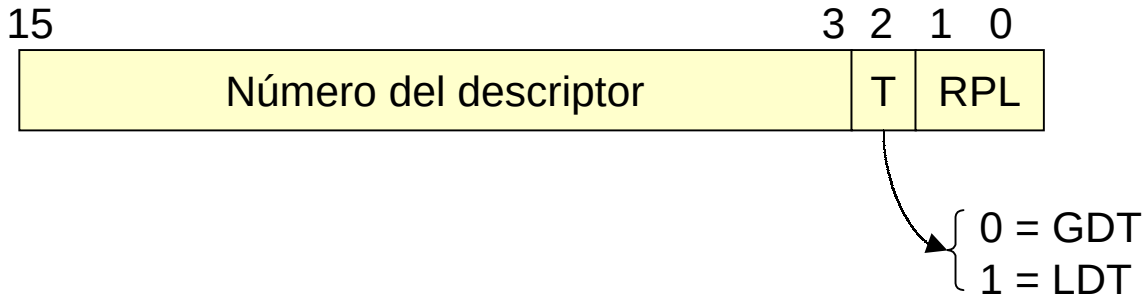
DEPARTAMENTO DE INGENIERÍA ELECTRÓNICA
UNIVERSIDAD POLITÉCNICA DE MADRID

TABLAS DE DESCRIPTORES

- Descriptores agrupados en tablas de descriptores
- Descriptor = 8 bytes
- Tablas limitadas a 64 Kbytes
- Total = 8192 descriptores por tabla

Tabla de descriptores	Registro
GDT (*Global Descriptor Table*)	GDTR
LDT (*Local Descriptor Table*)	LDTR
IDT (*Interrupt Descriptor Table*)	IDTR

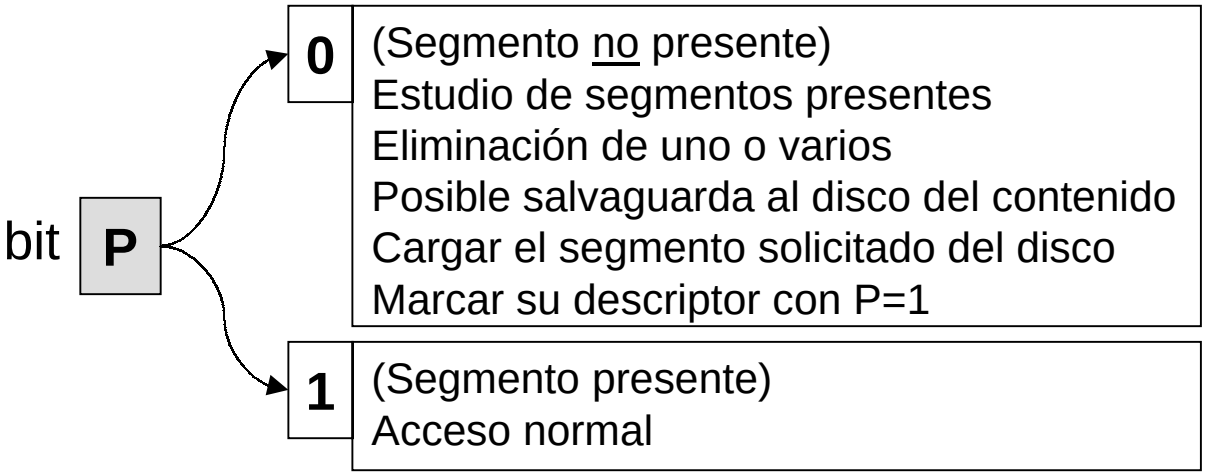
Selector de segmento (CS,DS,ES,...)



DEPARTAMENTO DE INGENIERÍA ELECTRÓNICA
UNIVERSIDAD POLITÉCNICA DE MADRID

MEMORIA VIRTUAL

- Memoria lógica total disponible en el ordenador
- Por encima de la físicamente instalada



Tamaño de la memoria virtual:

GDT	8192 = 2^{13} descriptores
LDT	8192 = 2^{13} descriptores
TOTAL	16384 = 2^{14} descriptores

Tamaño	Total memoria virtual
2^{16} = 64 Kb	$2^{14} \cdot 2^{16} = 2^{30}$ = 1 Gb
2^{32} = 4 Gb	$2^{14} \cdot 2^{32} = 2^{46}$ = 64 Terabytes

DEPARTAMENTO DE INGENIERÍA ELECTRÓNICA
UNIVERSIDAD POLITÉCNICA DE MADRID

LA MEMORIA PLANA

- Mecanismo para evitar usar la segmentación
- Sólo disponible en 386 y siguientes
- Todo comparte un mismo segmento
- Mediante el bit G=1 podemos establecer límite = 4 Gb
- Sólo se trabaja con OFFSET (de 32 bit)

Ventajas:

- Desaparecen los modelos de los compiladores
- Desaparecen los cambios de segmento (rapidez)
- Situación similar al 68000 de Motorola

DEPARTAMENTO DE INGENIERÍA ELECTRÓNICA
UNIVERSIDAD POLITÉCNICA DE MADRID

LOS MECANISMOS DE PROTECCIÓN

Hasta ahora:

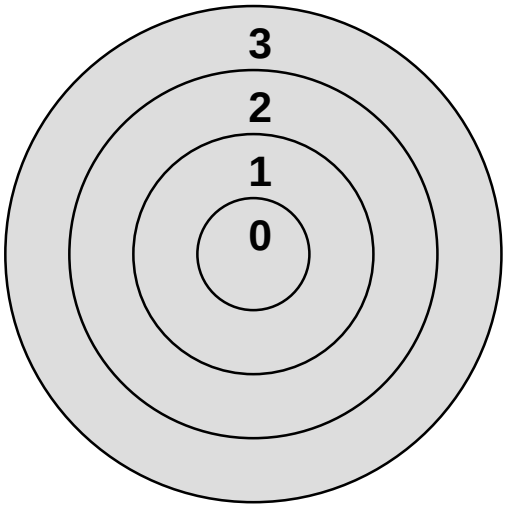
- Protección en el límite del segmento
- Bits W (protección contra escritura) y
  R (protección contra lectura)

- Intento de acceso indebido → EXCEPCIÓN

En general:

- Pueden establecerse niveles de privilegio para:
  Recursos del sistema
  Puertos hardware
  Todo en general

- 4 niveles de privilegio



"*El código debe tener un nivel de privilegio mayor o igual al del recurso accedido*"

DEPARTAMENTO DE INGENIERÍA ELECTRÓNICA
UNIVERSIDAD POLITÉCNICA DE MADRID

LOS MECANISMOS DE PROTECCIÓN

No es obligatorio utilizarlos → asignamos nivel 0 a todo

Definiciones:

- **DPL** → "*Descriptor privilege level*" Indicado en el descriptor.

- **CPL** → "*Current privilege level*" Nivel de privilegio de la CPU en un determinado instante.

  Nivel de privilegio del código que se ejecuta

- **RPL** → "*Requested privilege level*" Nivel de privilegio con el que se accede a un segmento.

  Representado en los bits 0,1 del selector

- **EPL** → "*Effective privilege level*" Nivel de privilegio menor entre el CPL y el RPL.

Para acceder a un segmento se necesita:

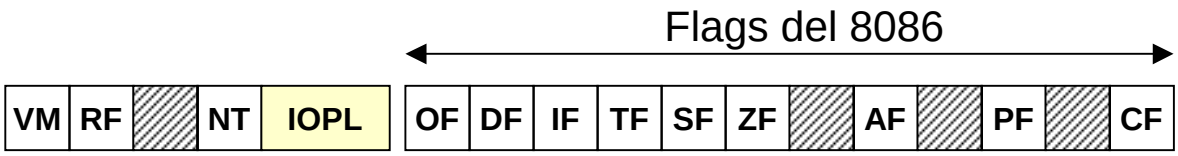
CPL ≤ DPL

DEPARTAMENTO DE INGENIERÍA ELECTRÓNICA
UNIVERSIDAD POLITÉCNICA DE MADRID

PROTECCIÓN DEL ACCESO AL HARDWARE

1 . Instrucciones de tipo:

IN , OUT , STI , CLI



Registro EFLAGS (32 bit)

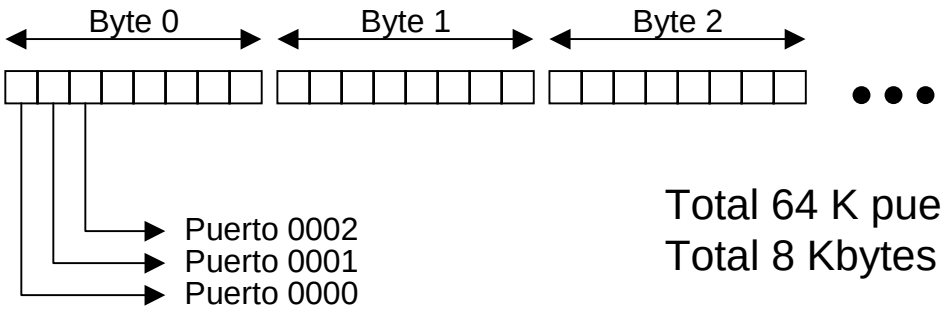
Para ejecutar estas instrucciones:

$$\mathbf{CPL} \leq \mathbf{IOPL}$$

---

2 . Para cada tarea:

Se pueden establecer permisos individuales para cada puerto E/S.



Total 64 K puertos
Total 8 Kbytes

DEPARTAMENTO DE INGENIERÍA ELECTRÓNICA
UNIVERSIDAD POLITÉCNICA DE MADRID

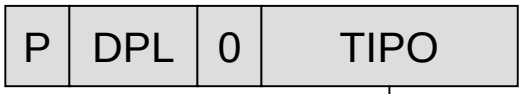
LAS PUERTAS DE ACCESO

Acceso de forma controlada a los recursos del sistema:

Ejecución de código de mayor privilegio.
Llamadas a funciones del S.O.
Llamadas a rutinas de atención a interrupciones.

Tipos de puertas de acceso:

Descriptor especial



Byte de permisos de acceso

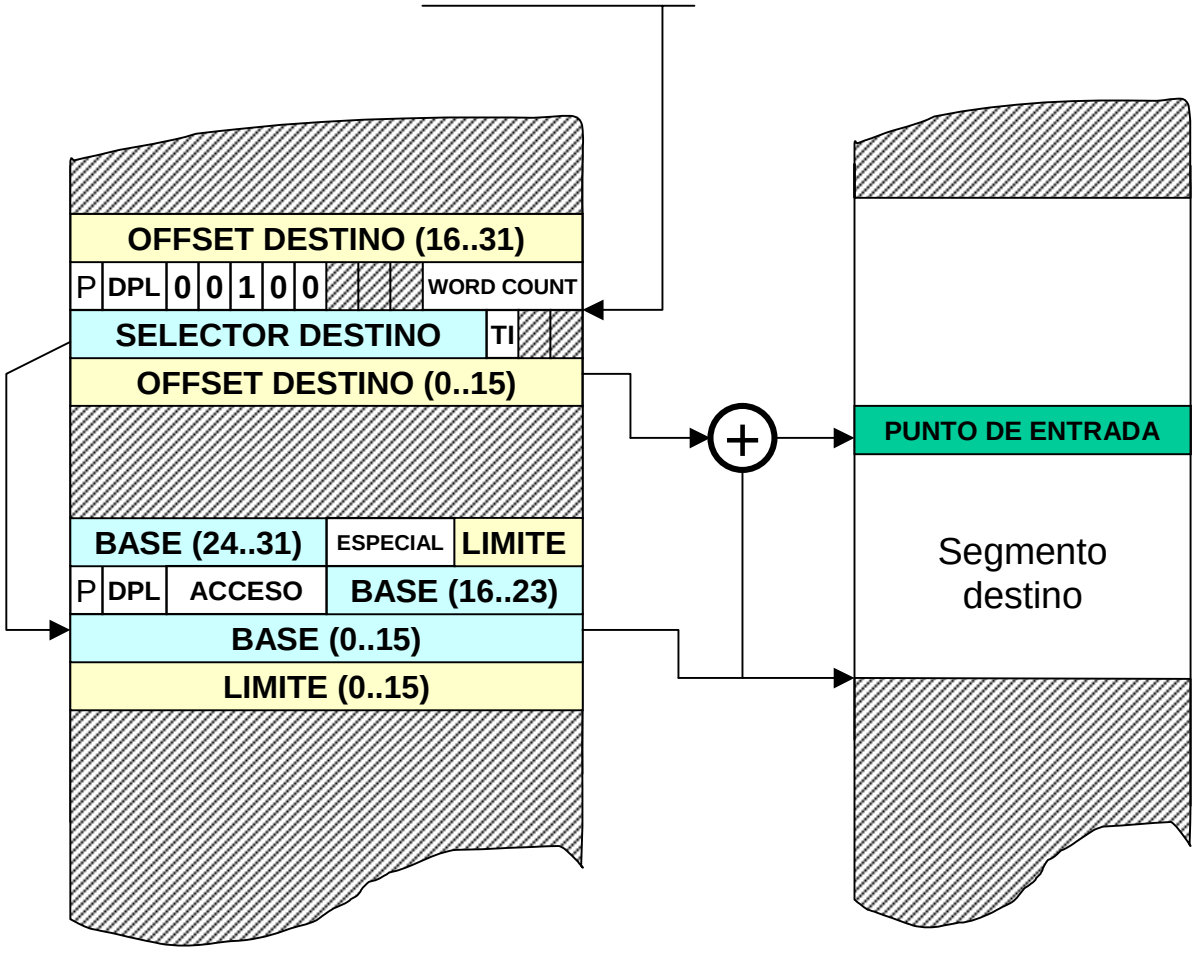
TIPO	PUERTA DE ACCESO
4	*CALL GATE*
5	*TASK GATE*
6	*INTERRUPT GATE*
7	*TRAP GATE*

DEPARTAMENTO DE INGENIERÍA ELECTRÓNICA
UNIVERSIDAD POLITÉCNICA DE MADRID

LAS PUERTAS DE ACCESO

Ejemplo: "*CALL GATE*"

CALL SEGMENTO : OFFSET (Se ignora)



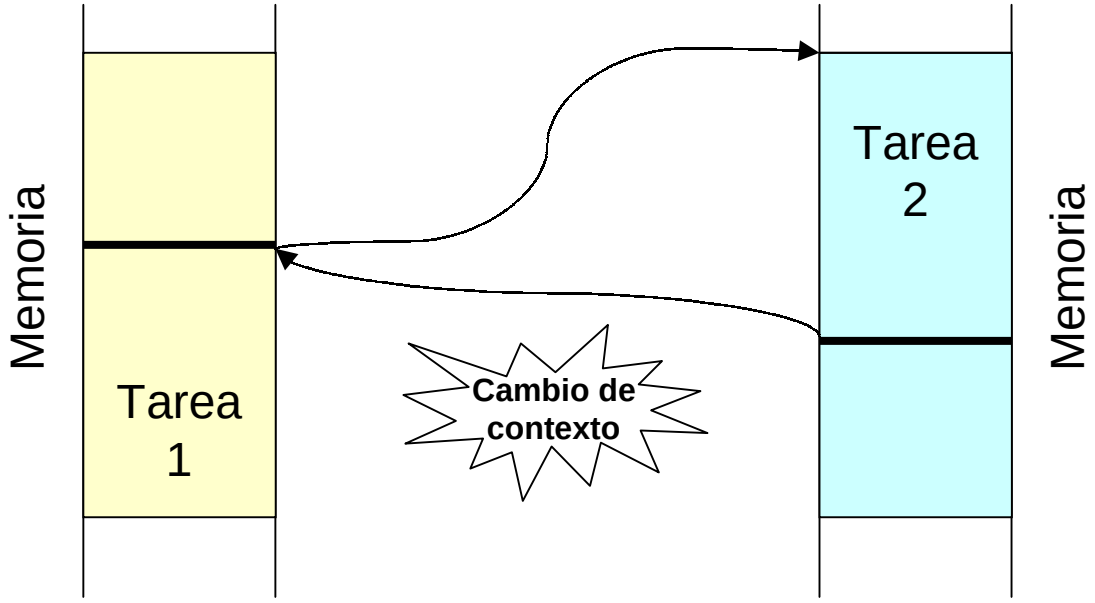
Tablas de descriptores

MEMORIA

DEPARTAMENTO DE INGENIERÍA ELECTRÓNICA
UNIVERSIDAD POLITÉCNICA DE MADRID

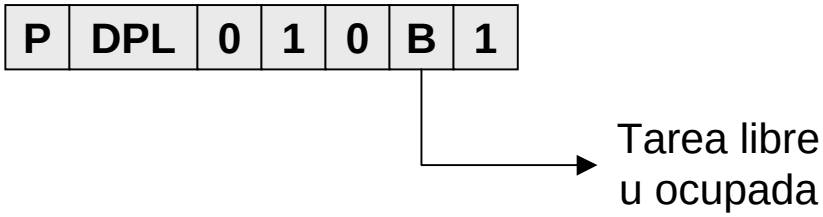
TAREAS

Tarea: Conjunto de código y datos que funcionan de forma conexa para obtener un resultado.



Contexto almacenado en TSS (*Task State Segment*)
Apuntada por descriptor especial

Permisos de acceso



TAREAS

31	0
PUNTERO AL MAPA E/S	T
	LDT
	GS
	FS
	DS
	SS
	CS
	ES
EDI	
ESI	
EBP	
ESP	
EBX	
EDX	
ECX	
EAX	
EFLAGS	
EIP	
CR3	
	SS2
ESP2	
	SS1
ESP1	
	SS0
ESP0	
	PUNTERO A TAREA ANTERIOR

El TSS (*Task State Segment*)

Para realizar la conmutación:

CALL o JMP a un descriptor TSS o puerta TASK GATE

DEPARTAMENTO DE INGENIERÍA ELECTRÓNICA
UNIVERSIDAD POLITÉCNICA DE MADRID

INTERRUPCIONES Y EXCEPCIONES

Interrupciones: origen hardware (INTR y NMI)

Asíncronas con la ejecución del programa

Excepciones:

"*faults*" : antes de ejecutar la instrucción
"*traps*" : después de ejecutar la instrucción
"*aborts*" : Errores graves
Interrupciones "*software*" : INT n , INTO, etc...

Síncronas con la ejecución del programa

Modo real:

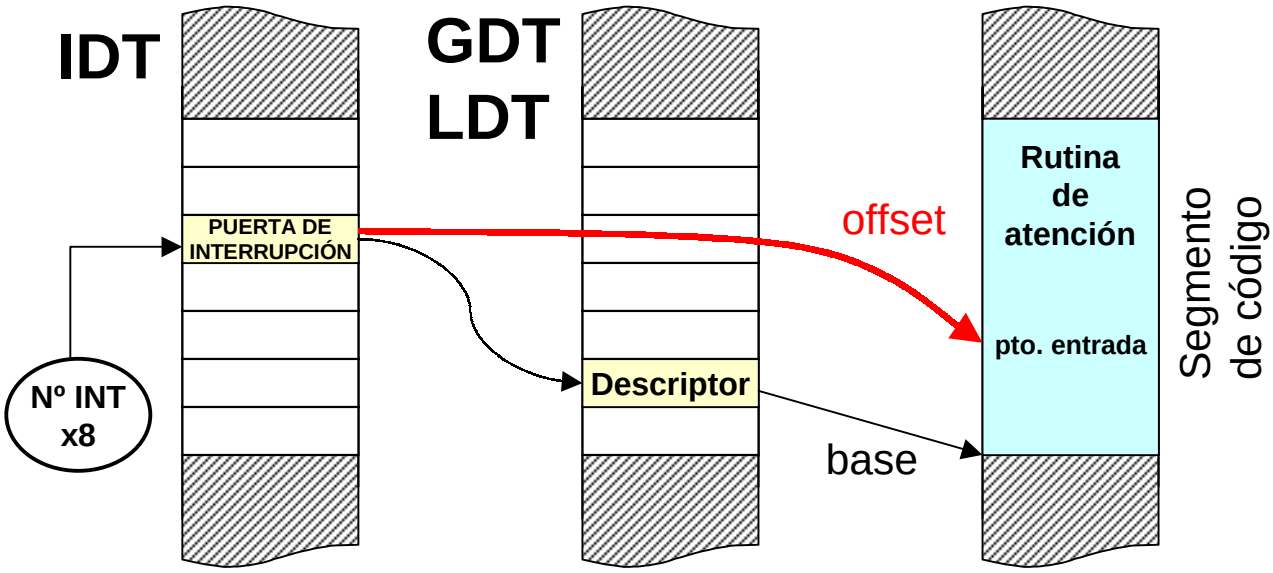
Tabla de vectores de interrupción en posición más baja de la memoria (0000 : 0000)

Modo protegido:

Las rutinas de atención se localizan mediante la IDT (Tabla de Descriptores de Interrupción)

DEPARTAMENTO DE INGENIERÍA ELECTRÓNICA
UNIVERSIDAD POLITÉCNICA DE MADRID

INTERRUPCIONES Y EXCEPCIONES



Interrupciones en modo protegido

Núm	Descripción	Tipo
0	División por 0	FAULT
1	Interrupción paso a paso	FAULT
2	NMI	-
3	INT	TRAP
4	Overflow (INTO)	TRAP
5	Fallo de límite de tabla (BOUND)	FAULT
6	Código de operación no válido	FAULT
7	Coprocesador no disponible	FAULT
8	Doble fallo	ABORT
9	Violación de segmento coprocesador	-
10	TSS no válido	FAULT
11	Segmento no presente	FAULT
12	Excepción de la pila	FAULT
13	Violación de protección	FAULT
14	Fallo de página	FAULT

DEPARTAMENTO DE INGENIERÍA ELECTRÓNICA
UNIVERSIDAD POLITÉCNICA DE MADRID

EL MODO VIRTUAL 86

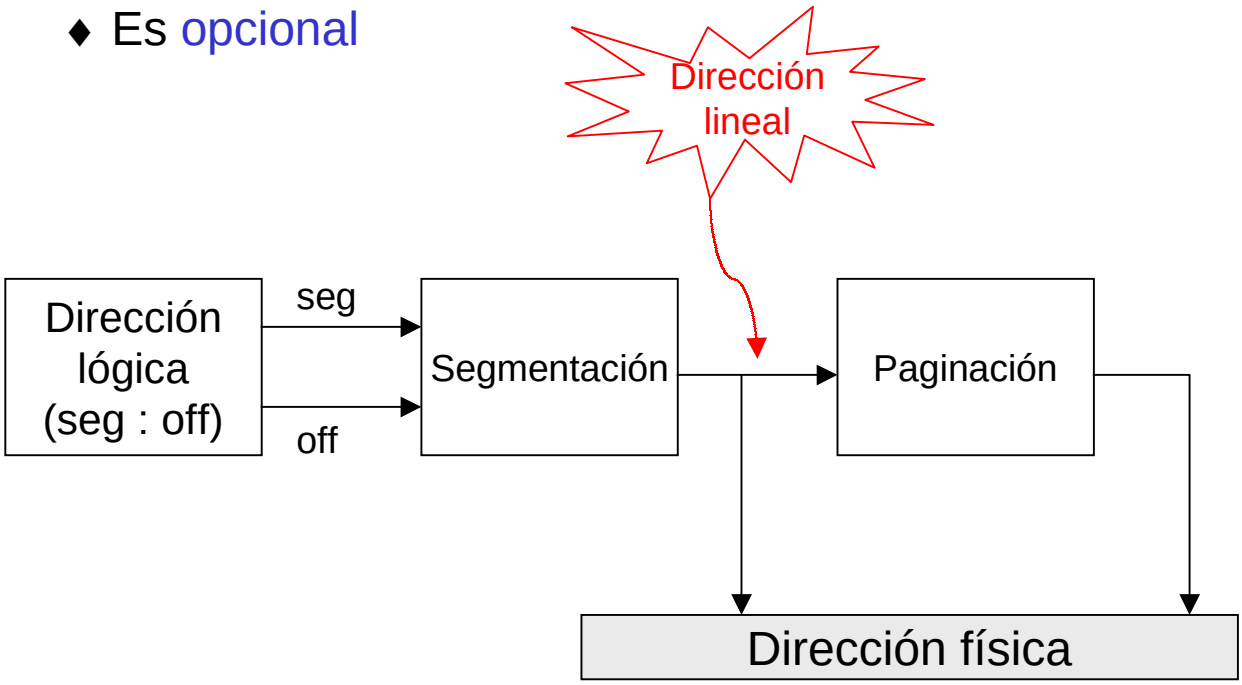
Modo de ejecución de una tarea concreta

- Desaparece la segmentación
- Selectores se comportan como en modo real
- Máximo 1 Mb. direccionable
- Interrupciones gestionadas por IDT
- La tarea se ejecuta con prioridad 3 (la más baja)
- Entrada y salida al hardware protegida
- Puede activarse la paginación

LA PAGINACIÓN

♦ Añade un nivel más de indirección en el cálculo de las direcciones físicas.

♦ Es opcional



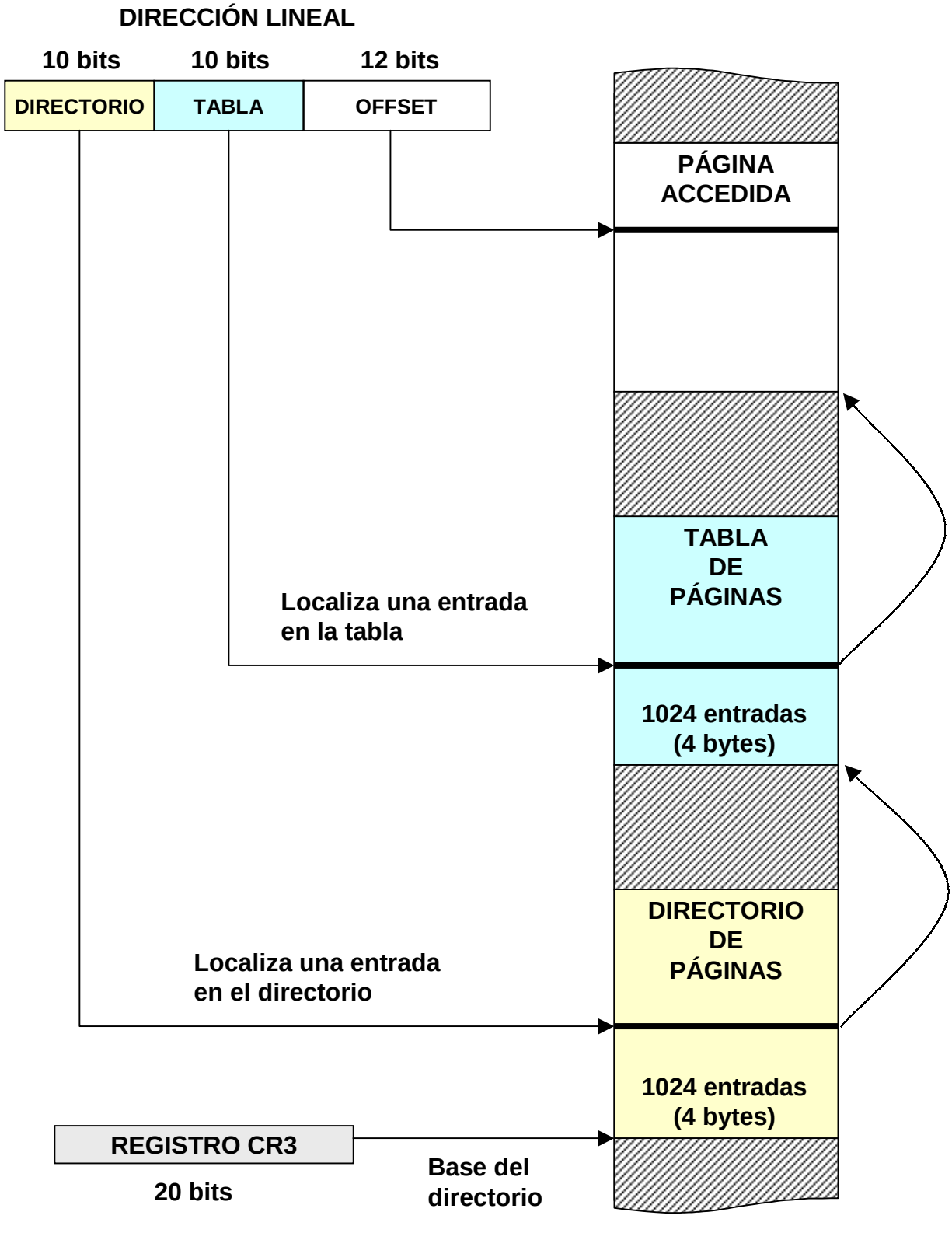
♦ Páginas de 4096 bytes (4 Kbytes) fijas

♦ Protección a nivel de páginas

♦ Activando la memoria plana, se puede trabajar sólo con paginación

DEPARTAMENTO DE INGENIERÍA ELECTRÓNICA
UNIVERSIDAD POLITÉCNICA DE MADRID

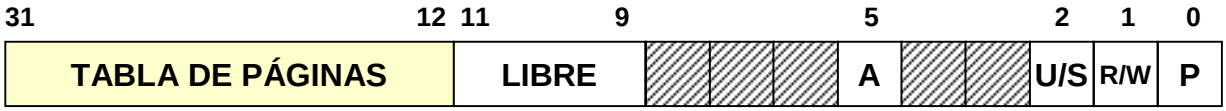
LA PAGINACIÓN



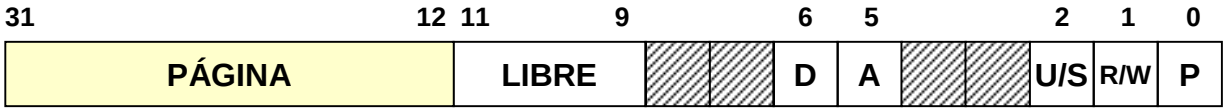
DEPARTAMENTO DE INGENIERÍA ELECTRÓNICA
UNIVERSIDAD POLITÉCNICA DE MADRID

LA PAGINACIÓN (Protecciones)

Entrada del directorio de páginas (PDE)



Entrada de la tabla de páginas (PTE)



P Bit de presente en memoria.

R/W Página de sólo lectura (0) o lectura/escritura (1)

U/S Permisos de acceso (sólo 2 niveles)
- Modo supervisor (0) → nivel de protección 0,1 y 2
- Modo usuario (1) → nivel de protección 3

A Página accedida (automático)

D Bit "*dirty*" (sucio) →
indica página accedida en escritura (automático)

LIBRE A disposición del programador

DEPARTAMENTO DE INGENIERÍA ELECTRÓNICA
UNIVERSIDAD POLITÉCNICA DE MADRID

LA PAGINACIÓN
El TLB (*Translation Lookaside Buffer*)

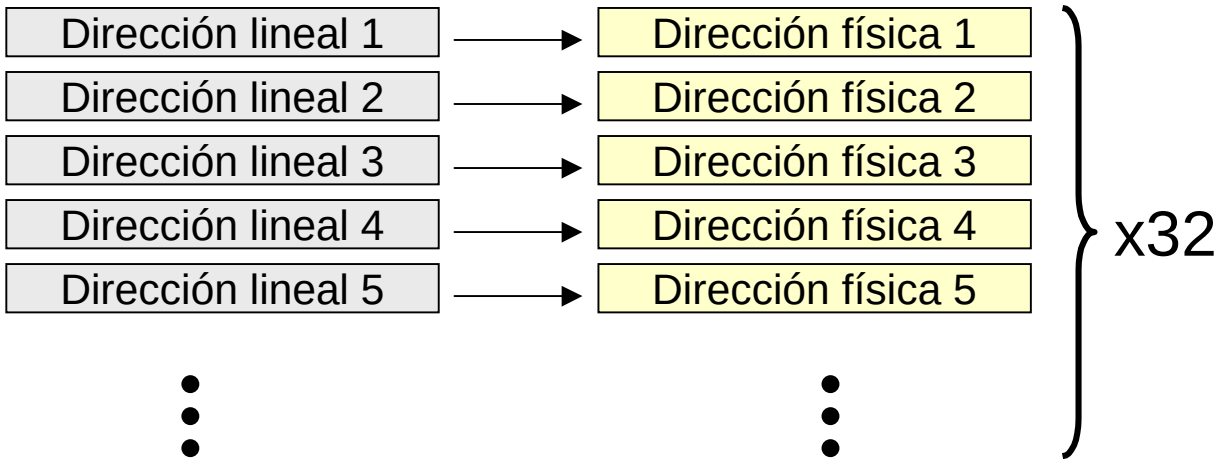
Cada acceso a memoria necesitaría 3 accesos:

- Lectura del directorio de páginas
- Lectura de la tabla de páginas
- Lectura de la página accedida

Para evitarlo está el TLB

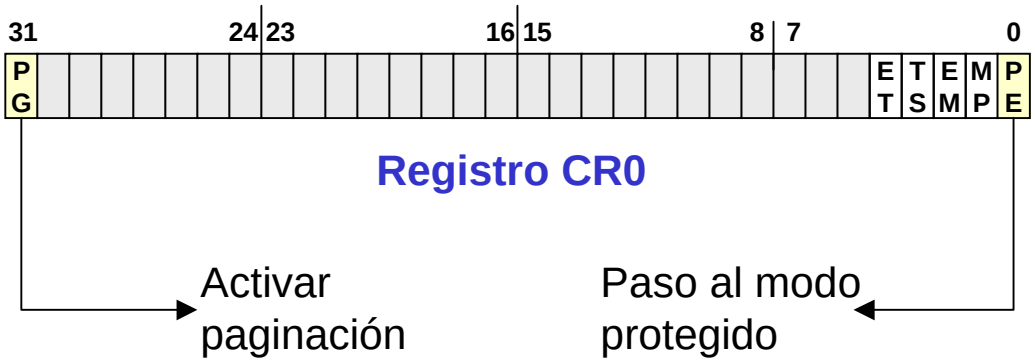
- Memoria asociativa de 32 entradas
- Almacena las direcciones de las 32 últimas páginas
- Total : 4096 bytes x 32 = 128 Kbytes

INTEL asegura una eficacia del 98%



DEPARTAMENTO DE INGENIERÍA ELECTRÓNICA
UNIVERSIDAD POLITÉCNICA DE MADRID

EL PASO AL MODO PROTEGIDO



Conmutación al modo protegido:

- Creación en memoria de las tablas de descriptores IDT y GDT
- Inicializar los registros GDTR e IDTR
- Preparar rutinas de atención a todas las interrupciones que puedan producirse
- Si se va a usar paginación: crear el directorio de páginas y dar un valor a CR3 (base del directorio)
- Activar el bit 0 del registro CR0

Vuelta al modo real:

- En 80286 no se podía (necesidad de RESET)
- En 80386 basta poner a 0 el bit 0 del registro CR0