U.N.Ju. – F.I.

INGENIERÍA INFORMÁTICA

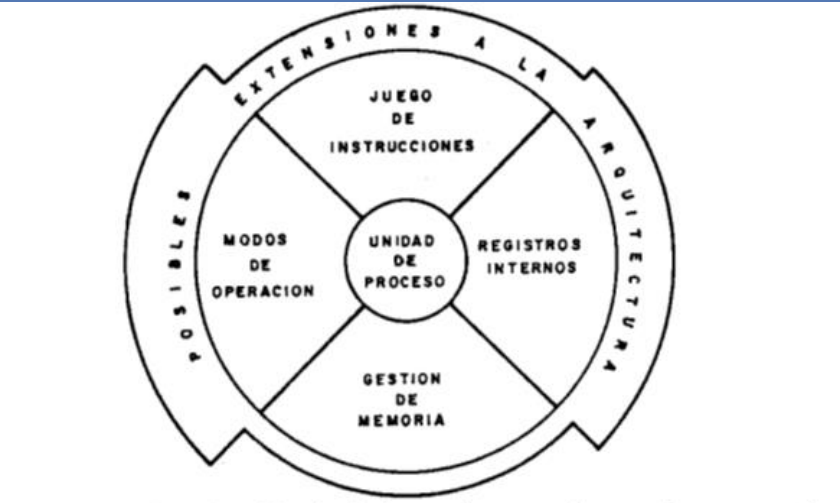
LABORATORIO DE COMPUTADORAS

ARQUITECTURA X86

TEMA: ARQUITECTURA 80386

Familia 386

Arquitectura de un microprocesador se define como la estructura, funcionalidades y modelo de programación del microprocesador.



Representación simplificada de la arquitectura de un microprocesador.

La agrupación de estos elementos define que sistemas operativos, programas de aplicación y software en general podrá ejecutarse en la arquitectura del microprocesador.

La barrera de los 32 bits.

Se introdujo en octubre de 1985. Procesan datos de 32 bits. La compatibilidad de software fue el prerrequisito más importante.

La característica principal es la gestión de memoria; puede trabajar con segmentos de memoria mayores a 64 Kb (el tamaño máximo es de 4 Gb), direccionar hasta 4 Gb de memoria física y 64 Tb de memoria virtual.

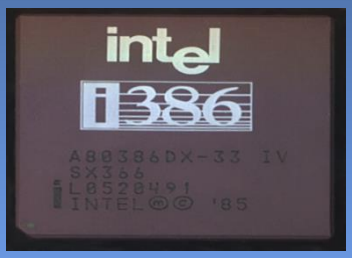
Problema de la compatibilidad en micros anteriores.

.

Familia 386

Arquitectura robusta.

El procesador 80386 DX.



El procesador 80386 SX.

El procesador 80386 SL.

Tecnología e Integración:

- Los micros se hacen cada ve más pequeños.
- Las prestaciones se pagan más baratas.
- Los micros son cada vez más potentes.

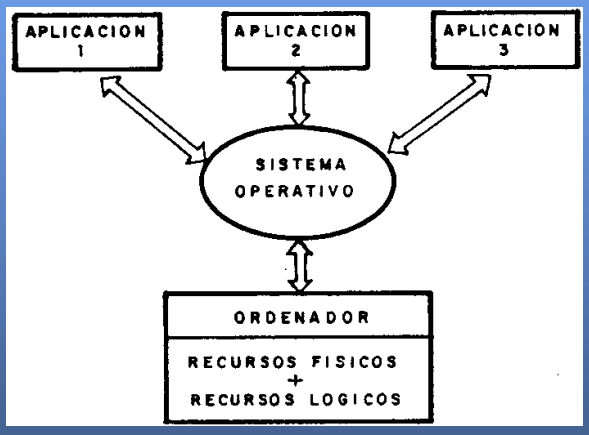
Conceptos Básicos

Distintas aplicaciones que corren sobre una determinada máquina, utilizan recursos físicos (hardware) y lógicos (software) compartidos.

El Sistema Operativo (S.O.) es un conjunto de programas que proporciona a cada aplicación la posibilidad de utilizar diversos recursos de la máquina:

- Centralización.
- Tiempo de ejecución.
- Gestión de memoria y subsistemas de E/S.

Resumiendo: haciendo uso de los servicios que proporciona el S.O. cada una de las aplicaciones parece tener, a su disposición, todos los recursos del procesador que precise.



El S.O. dispone de los programas necesarios para poner a disposición de la aplicaciones, los recurso físicos y lógicos compartidos de la computadora

Características

El aumento del rendimiento en el procesamiento que permiten los micros de 32 bits se debe, en gran parte, a:

- Su estructura interna.
- La base de registros.
- Buses de 32 bits.
- Mejora del pipeline de instrucciones.
- Aumento de la frecuencia de trabajo.
- Cachés ultrarrápidas.
- Instrucciones de máquina potentes y específicas.
- Recursos precisos para la multitarea y el multiusuario.
    1. CPU más veloz.
    2. Gran capacidad de memoria.
    3. Sistema de protección.

En resumen:

1. Memoria virtual.
2. Multitarea.
3. Sistema de protección.

Memoria Virtual

El 386 y el 486 son verdaderos micros de 32 bits lo que significa que los buses de datos y direcciones están constituidos por 32 líneas cada uno, en consecuencia la memoria principal alcanza los 4 Gb.

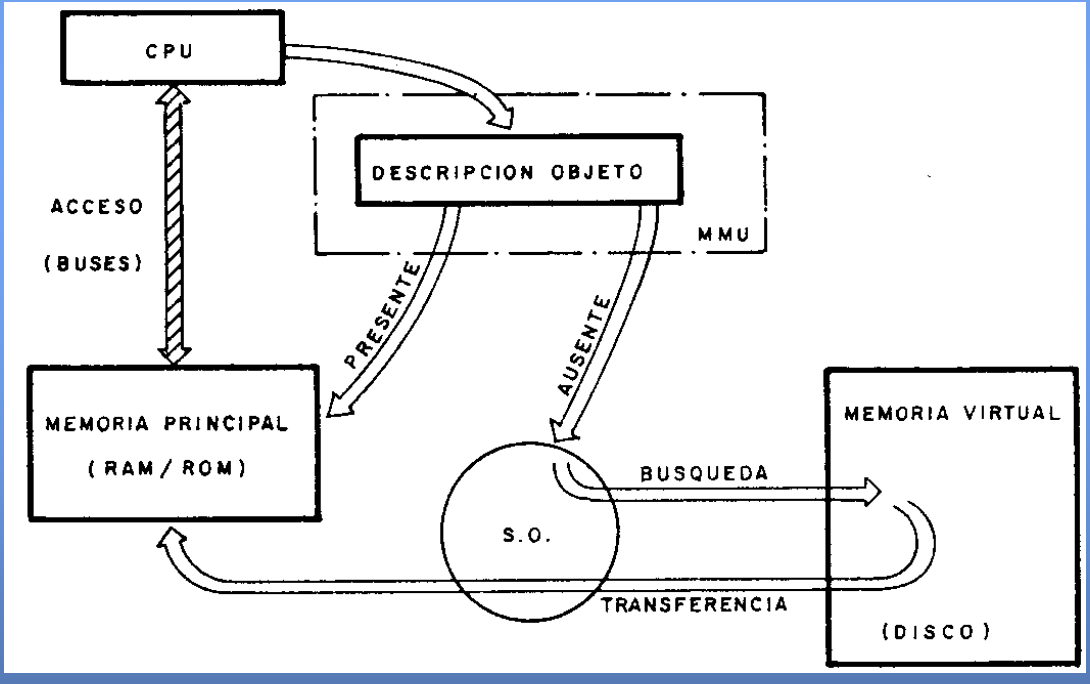
La CPU solo es capaz de acceder directamente a una MP, llamada también real o física. Cuando el procesados intenta acceder a memoria y genera la dirección del objeto que necesita, un mecanismo de gestión de memoria, denominado Unidad de Gestión de Memoria (MMU), comprueba si el objeto se encuentra en MP y si así sucede, se procede a acceder a él normalmente.

En el caso de que la MMU detecte que el objeto no reside en la MP, comunica el hecho la S.O. que pone en marcha la rutina encargada de localizar el objeto en la memoria virtual (disco) y transferirlo a la MP para que la CPU acceda a él, como en el caso anterior. Como la memoria virtual (disco) es mucho mayor que la MP (RAM/ROM) existirá un constante flujo de transferencia entre ambas.

Memoria Virtual

La implantación de la memoria virtual conlleva la incorporación de hardware que configure la MMU en el micro, aparte de que el S.O. disponga de las siguientes funciones:

1. Lista completa con la descripción de los objetos.
2. Cargue objetos en la memoria física en tiempo de ejecución.
3. Maneje los espacios libres de memoria.



La MMU recibe la descripción del objeto al que se desea acceder desde la CPU y detecta si se encuentra presente o ausente en la MP.

Organización y tipos de Memoria Virtual

Los distintos modelos se diferencian por sus políticas de solape y por los métodos que emplean en la organización de la memoria. Los más importantes son:

- Memoria Paginada.
- Memoria Segmentada.
- Memoria de Segmentos Paginados.

La política de solape y compartición debe tener en cuenta ciertas características internas de los programas que, invariablemente, determinan la construcción modular y estructurada de los programas. Estas características son:

1. Localización temporal.
2. Localización espacial.
3. Localización secuencial.

Para decidir que fracción de la MP ha de ser destruida o cargada en disco si ha sido modificada, cuando se necesite, los criterios usados son:

- Regla FIFO.
- Regla LRU.
- Regla LIFO.
- Regla LFU.
- Regla RND (Random).

Tipos de Mem. Virtual

Memoria Paginada

Organiza el espacio virtual y el físico en bloques de tamaño fijo llamados páginas. En un momento determinado la MP contendrá algunos bloques lógicos (virtuales). Como las distintas posiciones de un bloque lógico y uno físico están ordenados de idéntica forma, simplemente hay que traducir el número de bloque lógico al correspondiente del físico.

Memoria Segmentada

Explota la técnica de modularidad de los programas construidos de forma estructurada. Los módulos son conjuntos de informaciones que pueden tratarse independientemente y que se relacionan mediante llamadas interprocedimientos. A dichos módulos se los denomina segmentos. La segmentación organiza el espacio virtual en bloques de tamaño variable y que se colocan en MP mediante algoritmos de localización de espacios libres.

Memoria con Segmentos Paginados

Combina las ventajas de los dos anteriores. Cada segmento se divide en páginas de forma que para acceder a un objeto de un segmento, el sistema accede a la Tabla de Páginas de dicho segmento.

Multitarea y Multiusuario

Cuando la CPU atiende varias tareas, cada vez que se produce una conmutación de tarea, de la tarea vieja se debe almacenar el algún sitio el contexto de la CPU en el momento del abandono.

Un contexto es un conjunto de valores correspondientes al juego de registros internos del procesador, que son necesarios para determinar las mismas condiciones que las que existían al producirse la conmutación de tarea.

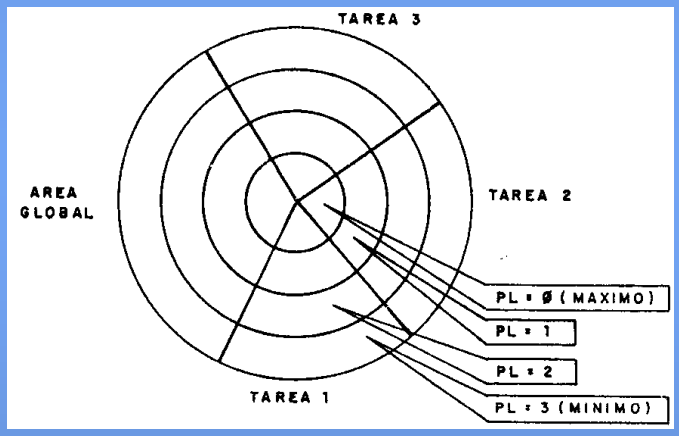
Una vez producido esto, los recursos que soportan la conmutación de tarea, deben ser capaces de cargar en el procesador el contexto correspondiente a la tarea nueva con lo que se reanuda la ejecución de instrucciones y que, previamente, estaba almacenado en una zona determinada de la memoria. En un sistema multitarea, tanto el procesador como el S.O. deberán proveer los recursos físicos y lógicos adecuados para soportar la conmutación de tarea.

Un sistema se llama multiusuario cuando varios usuarios tienen acceso a la CPU. Existen más implicaciones que en la multitarea, ya que en muchas ocasiones cada usuario, a su vez, es multitarea e introduce otro nivel de complejidad. Es como si hubiese que establecer prioridades dentro de las prioridades.

Mecanismos de Protección

Cuando en un espacio de memoria protegido deben estar completamente especificados (dirección base, tamaño y derechos de acceso), tanto las áreas locales de cada tarea, como el área global compartida. Los objetos que residen en las distintas áreas también deben quedar plenamente determinados.

Dentro de las zonas del espacio de memoria, existen varias subzonas, cada una de las cuales tiene un nivel de privilegio propio. El nivel de privilegio hace referencia al grado de confianza o seguridad de la zona.



Reglas de Acceso

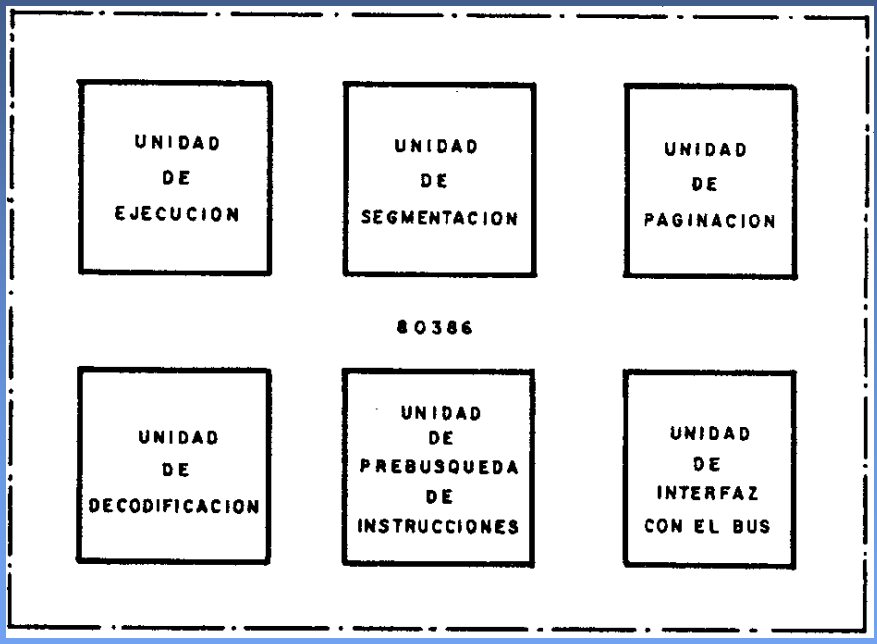
Los micros como el 386 y el 486 tienen integrado en el propio chip un hardware específico que controla un conjunto de reglas que permiten o prohíben el acceso a los objetos situados en las diversas zonas de la memoria, y, dentro de ellas, el acceso según los niveles de privilegio, que haya asignado el programador del sistema.

Arquitectura del 386

Características:

1. Registros internos de 32 bits.
2. El DB y el AB disponen de 32 líneas cada uno.
3. Capacidad para controlar directamente una MP física de 4 Gb.
4. Cambio dinámico del tamaño del bus.
5. La MMU está integrada en el mismo chip y es capaz de gobernar 4 Gb de MP y 64 Tb de MV.
6. Soporta la paginación y la segmentación.
7. Factores fundamentales:
   a) Elevada velocidad intrínseca de procesamiento.
   b) Se reforzó la partición de la estructura interna, quedando la CPU en 6 bloques independientes, que mejoran el grado de paralelismo implícito de la máquina.
8. Se incorporan registros y memorias cachés que aceleran el proceso de búsqueda y traducción de direcciones.

Arquitectura del 386



Modos de funcionamiento

Compatibilidad con productos anteriores.

Mejor conmutación de tarea.

Dispone de un entorno protegido que impide la interferencia entre las tareas., entre los objetos de una misma tarea e, incluso, la posibilidad de ejecutar ciertas instrucciones si se producen situaciones prohibidas.

El 386 admite tres formas de operación:

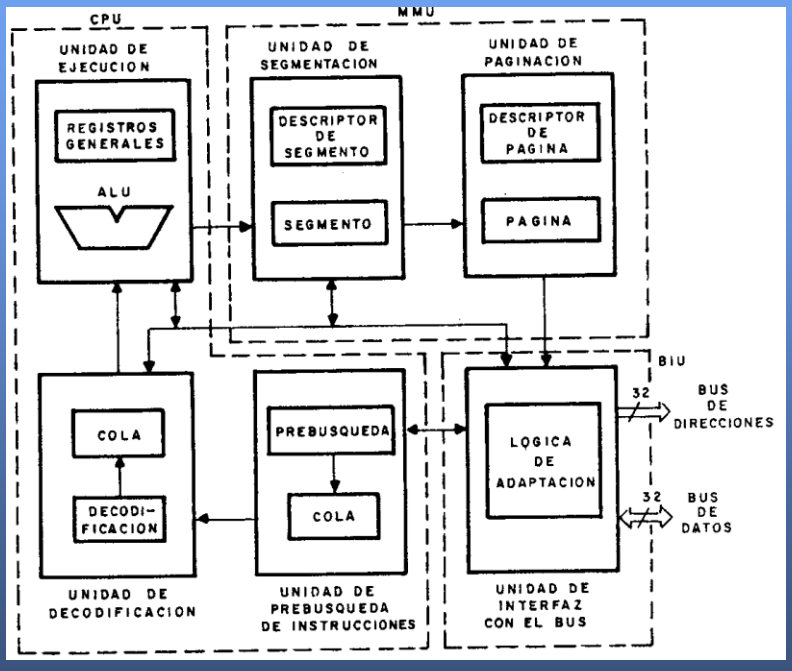
1. Modo Real.
2. Modo Protegido.
3. Modo Virtual-86.

Arquitectura Interna

El 386 es un procesador con una estructura interna de ejecución en cadena, que actúa como las colas de operación en cascada.

El 386 se compone de tres grandes bloques:

1. CPU
    a. Unidad de prebúsqueda.
    b. Unidad de decodificación.
    c. Unidad de ejecución.
2. MMU
    a. Unidad de segmentación.
    b. Unidad de paginación.
3. BIU



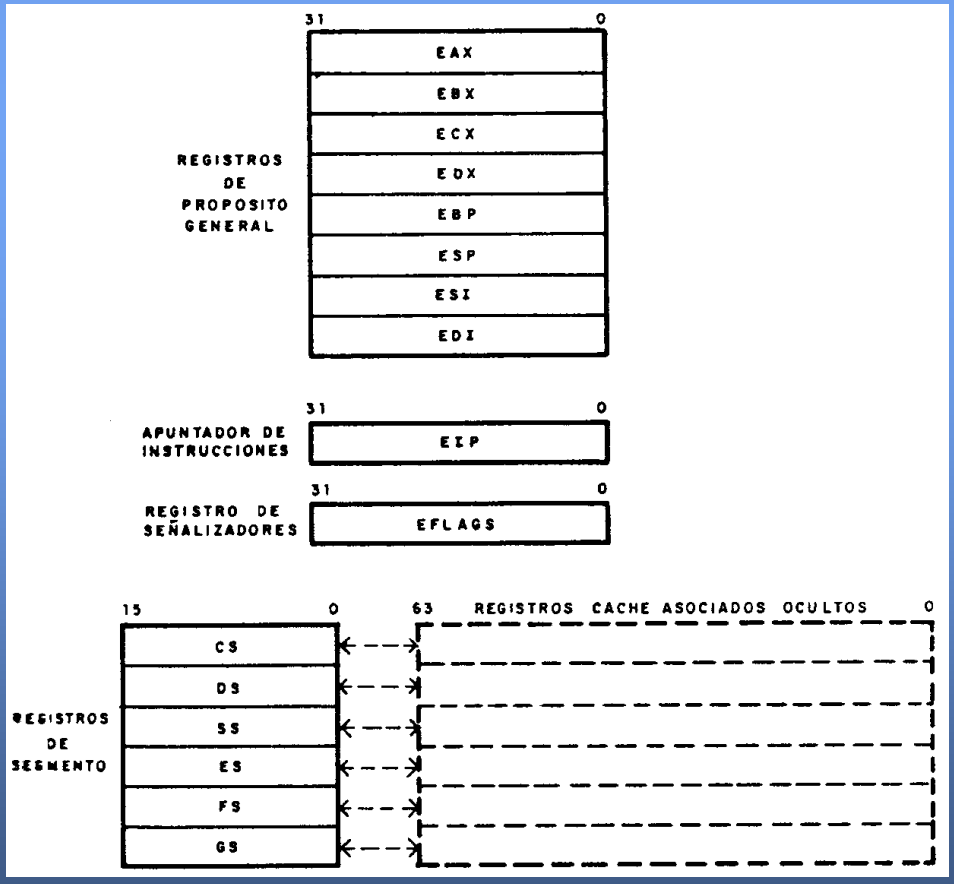
Registros Internos

El conjunto de registros es el siguiente:

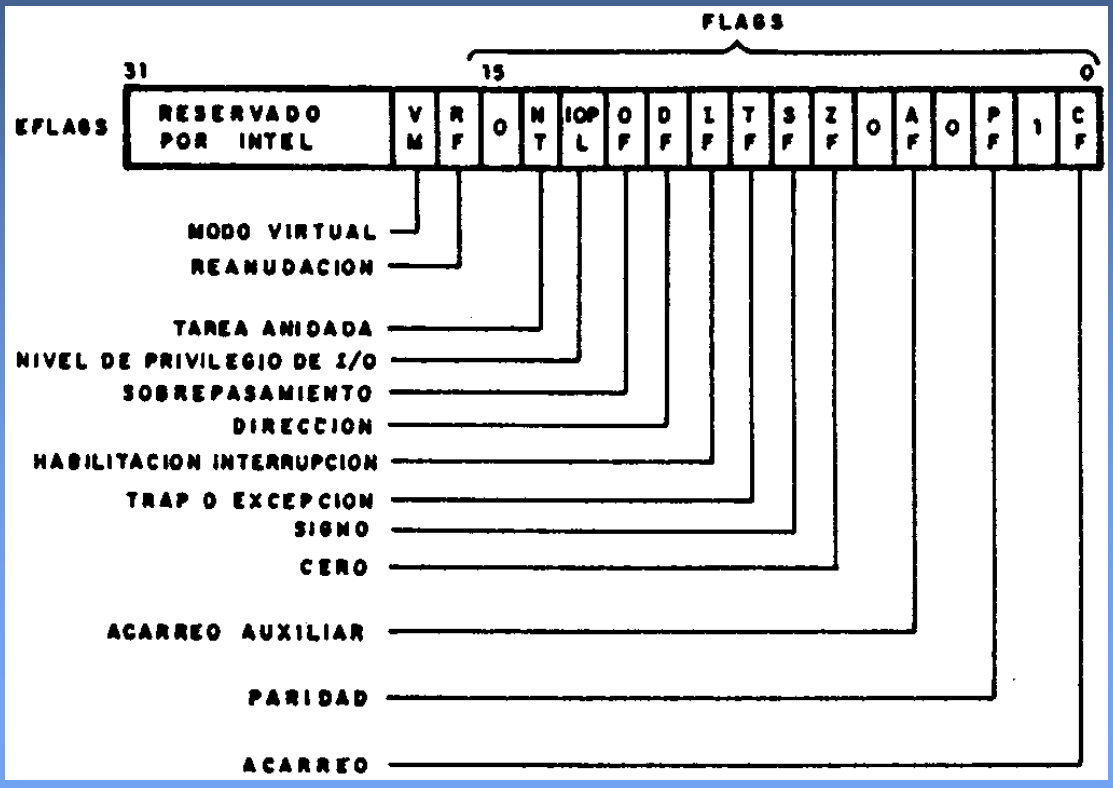
Registros de Propósito General: EAX, ABX, ECX, EDX, ESP, EBP, ESI y EDI.

Registro puntero de instrucciones y Flags: EIP y EFLAGS.

Registros de segmentos: CS, DS, SS, ES, FS, GS con registros cachés asociados ocultos de 64 bits.



Registro EFLAGS



VM (Modo Virtual-86): cuando VM=1 estando el procesador funcionando en Modo Protegido, éste pasa a trabajar en Modo Virtual-86.

NT (Tarea Anidada): se activa y se desactiva automáticamente al producirse una conmutación de tarea. Si vale 1, significa que la tarea en curso de ejecución está anidada con la anterior.

Registro EFLAGS

IOPL (Nivel de Privilegio de E/S): es un campo de 2 bits que se emplea en Modo Protegido y determina:

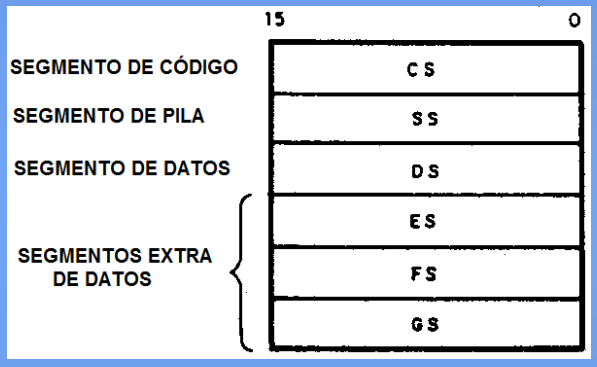
1. El nivel de privilegio a partir del cual se pueden ejecutar las instrucciones de E/S sin producir error.
2. El nivel de privilegio que permite la alteración del señalizador IF al cargar el registro EFLAGS.

RF (Reanudación): su activación provoca la ejecución de la siguiente instrucción cuando se produce una falla de depuración en una instrucción.

Registros de Segmento

Intel incorporó en la serie de micros X86 la segmentación como sistema principal en la organización de la memoria.

El 386 controla en cada instante seis segmentos a los que direcciona a través de los Registros de Segmento. Para direccionar la base donde comienzan los segmentos, el 386 dispone de seis registros.



Estos registros de segmento materializan, en cada momento, los segmentos que es capaz de identificar y manipular la CPU.

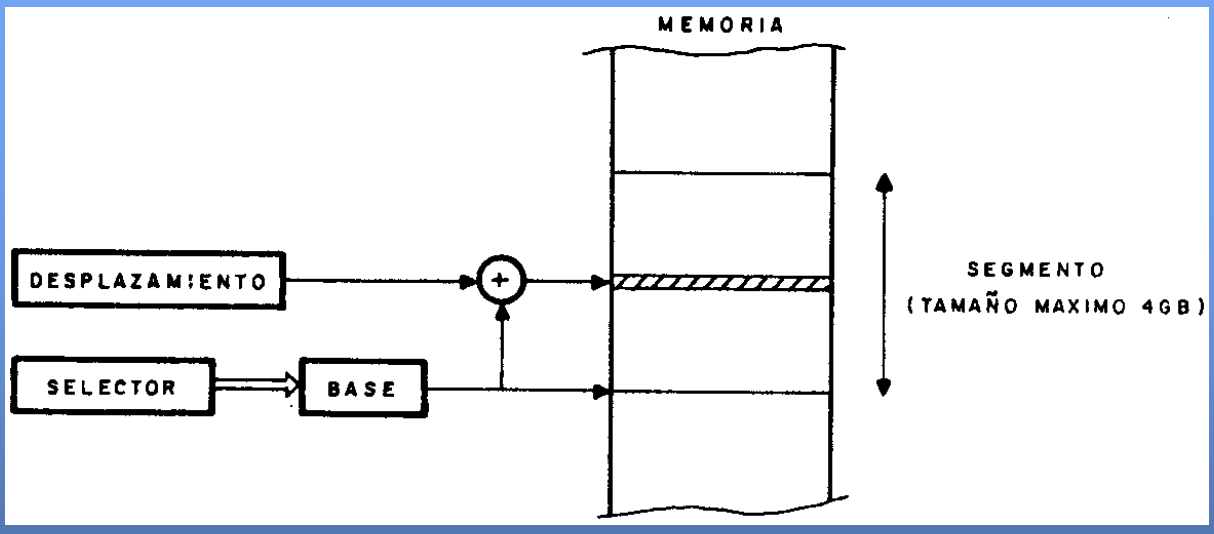
La dirección lógica de todo elemento accesible en la memoria, está formado por un puntero que consta de la siguiente pareja de campos:

1. Selector: es un valor de 16 bits, contenido en uno de los seis registros de segmento. Identifica al segmento y, en especial, a su base.

Registros de Segmento

2. Desplazamiento: es un valor de 32 bits que se añade a la base del segmento para localizar la dirección que hay que acceder en él. El tamaño del desplazamiento determina su longitud máxima que, en el caso del 386, es de 2^{32} =4 Gb.

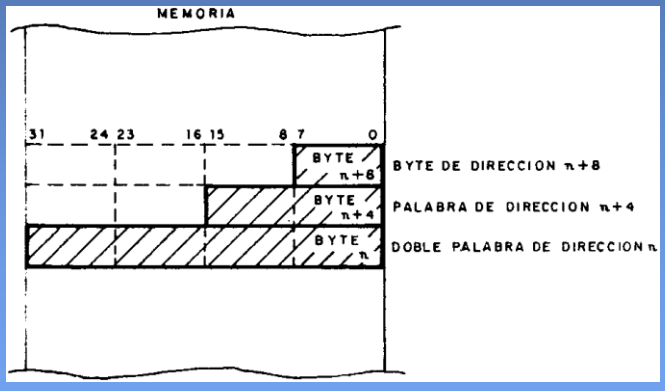
Cuando el procesador ejecuta un programa utiliza el selector para calcular la base del segmento, o sea, la dirección donde comienza. A la base se le suma el desplazamiento para determinar la posición a acceder.



Segmentación

Estructura general de la memoria

La memoria que controla el 386 está compuesta por bytes, palabras y dobles palabras.



Otras estructuras más complejas, que son manejadas por el 386, son los segmentos y las páginas.

Direccionamiento en Modo Real

Cuando el procesador trabaja en Modo Real, lo hace de forma similar al 8086con el fin de ser compatible con el software del 8086.

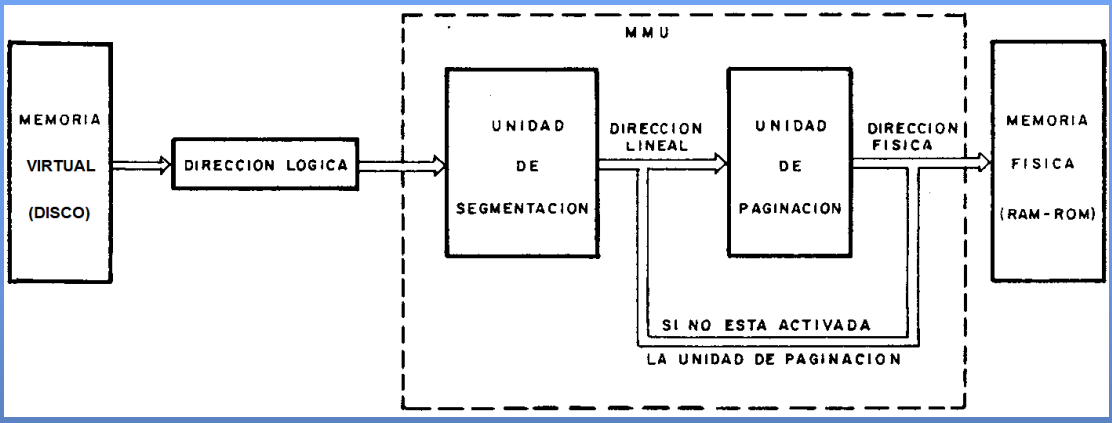
Dirección Efectiva= RS x 16 + Desplazamiento

Dentro de la memoria contemplada por el 386 se pueden distinguir tres espacios:

- Espacio virtual o lógico.
- Espacio lineal.
- Espacio físico.

Segmentación

El espacio virtual abarca toda la dimensión de la memoria virtual. La unidad de segmentación, cuya activación siempre es obligada, traduce las direcciones virtuales a lineales, que reciben este nombre porque hacen referencia a segmentos que, al situarse sobre la memoria física, tienen dispuestas todas sus posiciones en orden consecutivo o lineal. Cuando la Unidad de Paginación, optativa, no está activada, la dirección lineal coincide con la dirección física.



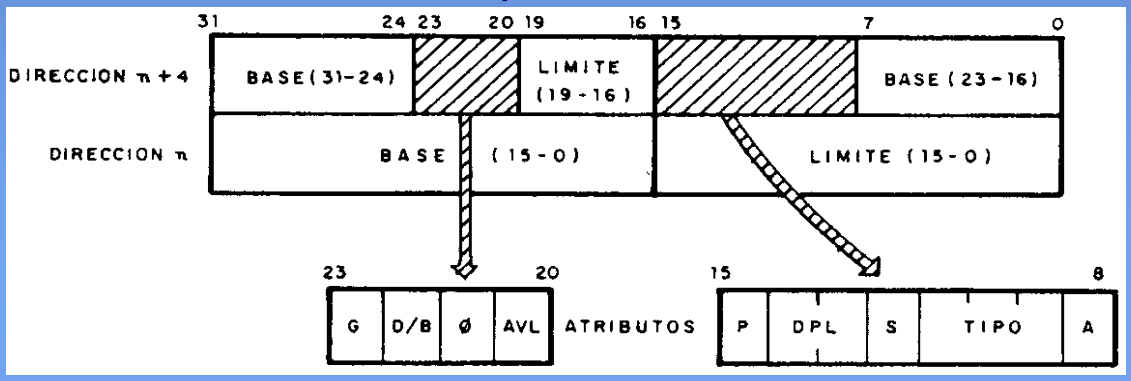
Segmentación

Si la Unidad de Paginación está activada, cada segmento se descompone en un número variable de páginas del mismo tamaño (4 Kb) y la Unidad de Paginación deposita a dichas páginas sobre la memoria física en los huecos que encuentra libres, no una detrás de otra, lo que significa que la dirección lineal se debe traducir a física de acuerdo con esta distribución aleatoria de las páginas.

Descriptores

Descriptores de segmento

Un descriptor es una estructura de datos compuesta de 8 bytes, que contiene los parámetros que definen completamente el segmento referenciado (base, límite y derechos de acceso o atributos).



Base: es un campo de 32 bits que contiene la dirección lineal donde comienza el segmento.

Límite: campo de 20 bits que expresa el tamaño de segmento. Como son 20 bits el tamaño máximo es de un 1 Mb; hay otro bit complementario en el campo de atributos (llamado G o de granularidad) que indica si el límite está expresado en bytes (G=0) o en páginas (G=1). En este último caso el tamaño máximo del segmento sería:

1 M x 4 Kb = 4 Gb.

Descriptores

Atributos o derechos de acceso: se trata de un campo de 12 bits de los cuales uno de ellos debe ser 0 para mantener compatibilidad con los 486 y Pentium

Descripción:

P (Bit de Presencia): indica si el segmento al que referencia el descriptor está cargado, o sea, se halla presente en la MP (P=1) o bien está ausente (P=0).

DPL (Nivel de Privilegio): indica el nivel de privilegio del segmento al que referencia e descriptor. Su valor puede variar entre 0 y 3 y es un campo de dos bits.

S (Tipo de Segmento): si S=1 el segmento correspondiente al selector es “normal” o sea un segmento de código, datos o pila. Si S=0 se refiere a un segmento del sistema, que referencia a un recurso especial del sistema.

Tipo: los tres bits de este campo distinguen en los segmentos normales si se trata de uno de código, de datos o de pila. Además determina el acceso permitido: lectura/escritura/ejecución.

A (Accedido): este bit se pone automáticamente a 1 cada vez que el procesador accede al segmento.

Descriptores

D/B (Defecto/Grande): en los segmentos de código el bit D (defecto) y en los segmentos de datos este mismo bit, llamado B(grande) permiten distinguir los segmentos nativos de 32 bits para el 386, de los que pertenecen al 286.

AVL (disponible): a disposición del usuario.

Tablas de descriptores

Al entrar en Modo Protegido deben estar residiendo en MP las tablas de descriptores que contienen las referencias precisas para los segmentos que va a usar el procesador.

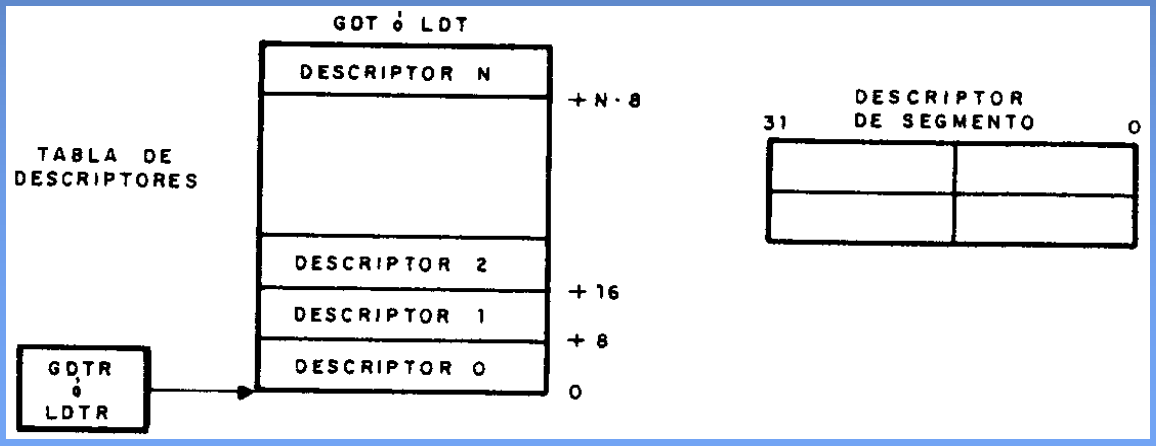
Un sistema multitarea se compone de un área global, en la que residen todos los objetos (segmentos) comunes a todas las tareas, y un área local para cada tarea, para los segmentos propios de cada una.

Cada segmento del área global está definido por un descriptor, existiendo una tabla, llamada Tabla de Descriptores Globales o bien Tabla Global de Descriptores (GDT), que contiene todos los descriptores del área global.

Asimismo, existe una tabla para cada tarea, que recoge todos los descriptores de los segmentos de cada una de ellas.

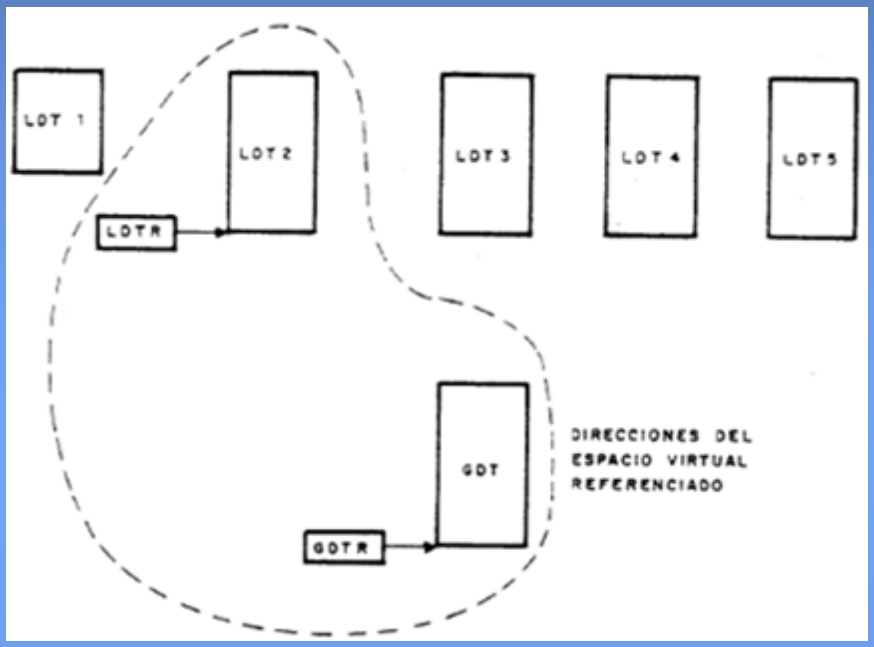
Descriptores

Se trata de la Tabla de Descriptores Locales o bien Tabla Local de Descriptores (LDT). Existen tantas LDT´s como tareas soporte el sistema.



Descriptores

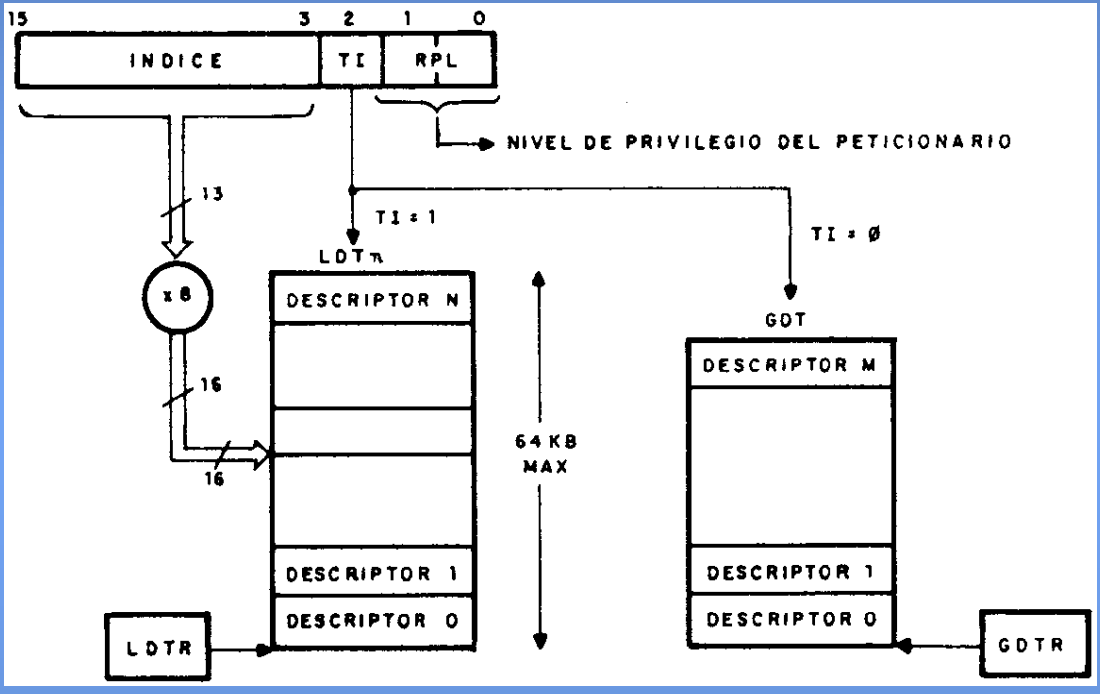
En un momento determinado el 386 estará ejecutando una tarea concreta y tendrá activas a la GDT y a la LDT correspondiente a la tarea en curso.



La estructura interna de una tabla de descriptores puede tener un máximo de 8 k descriptores de ocho bytes de tamaño cada uno. La LDT es una tabla local propia de la tarea en curso y una conmutación de tarea provocará automáticamente el cambio de LDT a través de la modificación del valor en el registro LDTR.

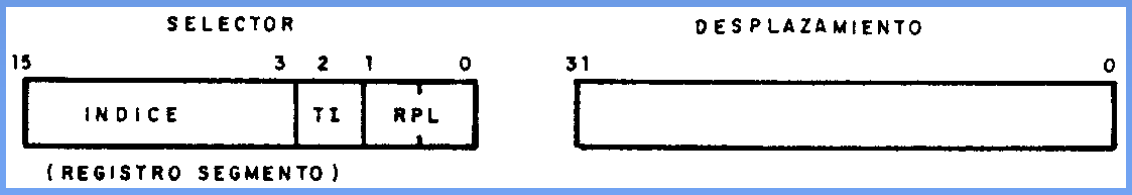
Descriptores

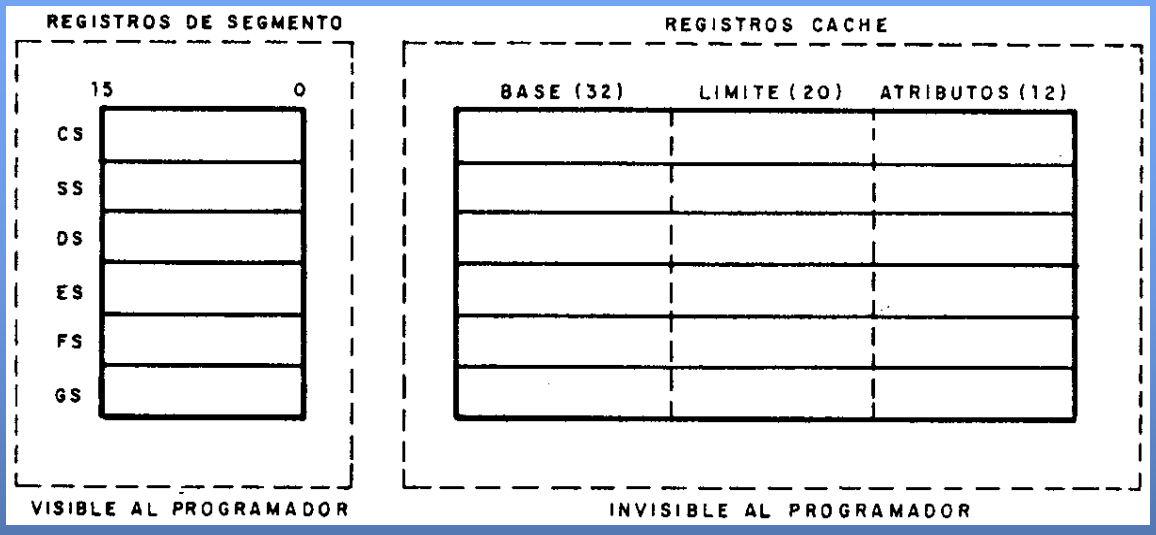
Como la CPU tiene activas dos tablas de descriptores, GDT y LDTn, hay un bit en el selector de segmento, o sea, en el registro de segmento, que indica a cuál de ellas se refiere.



Registros de Segmento

Los registros de segmento CS, DS, SS, ES, FS, y GS tienen un comportamiento en Modo Protegido completamente diferente que en Modo Real. En el Modo Protegido contienen el campo selector de la dirección virtual y cada uno funciona asociado a un registro caché de 64 bits caracterizado por su alta velocidad de acceso.





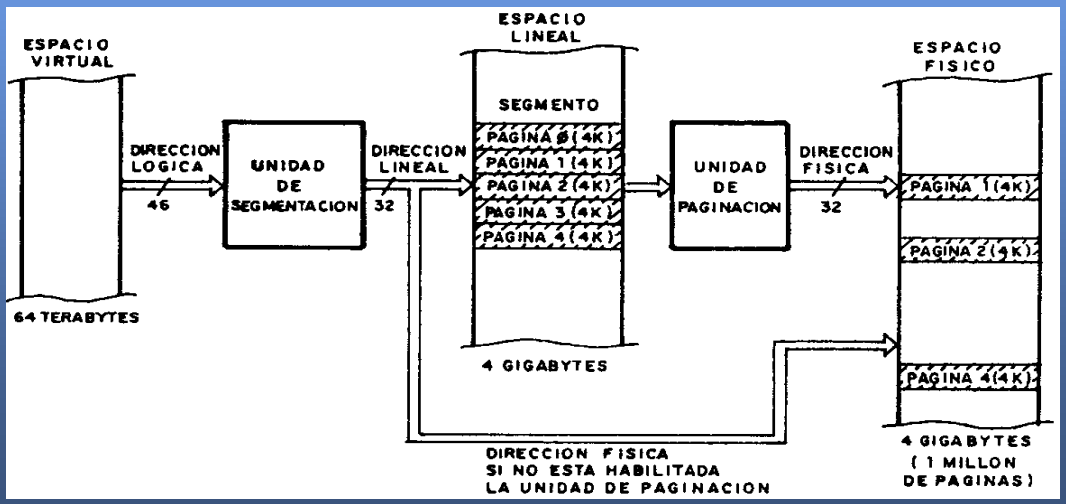
Paginación

La paginación es un procedimiento de gestión de memoria muy eficaz en los sistemas operativos multitarea que manejan memoria virtual. Divide y manipula los programas y los datos en trozos de tamaño fijo, llamados páginas.

Las páginas no guardan relación con la estructura lógica con el software.

La Unidad de Paginación está implantada en hardware dentro del 386 y su funcionamiento es optativo y solo opera en Modo Protegido.

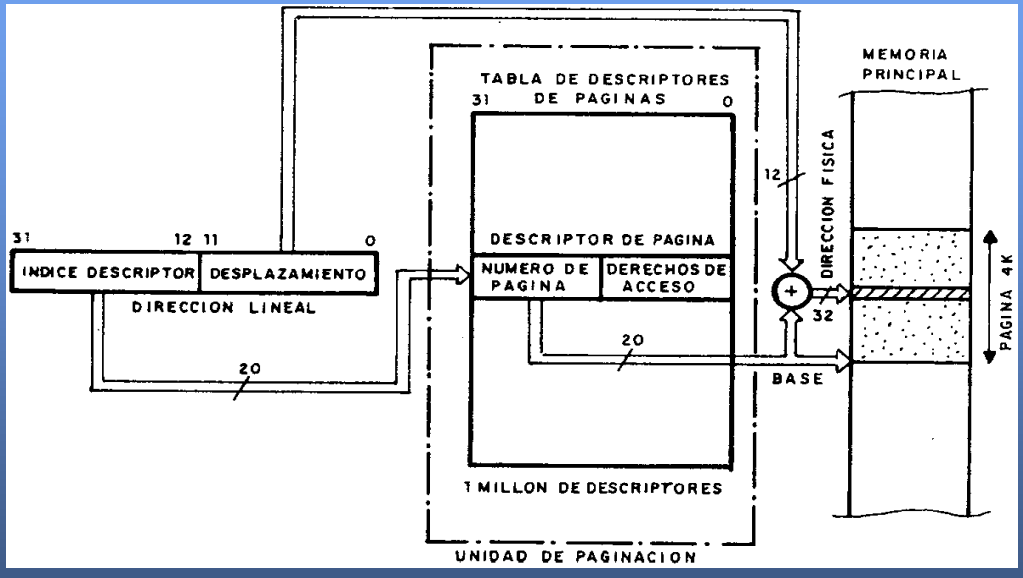
Cuando está habilitada, se divide a cada segmento, en páginas sucesivas de 4 Kb de tamaño cada una. Luego la Unidad de Paginación carga y distribuye, de forma aleatoria, las páginas que precisan en cada momento sobre el espacio de la memoria física.



Paginación

La Unidad de Paginación traduce la dirección lineal a física. Teniendo en cuenta que el espacio físico que puede alcanzar un máximo de 4 GB, la paginación lo descompone en un millón de páginas de 4 Kb, ose, actúa como una gran tabla de un millón de entradas, una por página. En cada entrada se guardaría la dirección base de comienzo de la página y los atributos de la misma, algo similar a un descriptor de segmento, pero sin el campo límite.

En consecuencia, la Unidad de paginación maneja una tabla con un millón de entradas, conteniendo cada una la base (20 bits) y los derechos de acceso (12 bits).



Paginación

La Unidad de Paginación traduce la dirección lineal a física. Teniendo en cuenta que el espacio físico que puede alcanzar un máximo de 4 GB, la paginación lo descompone en un millón de páginas de 4 Kb, ose, actúa como una gran tabla de un millón de entradas, una por página. En cada entrada se guardaría la dirección base de comienzo de la página y los atributos de la misma, algo similar a un descriptor de segmento, pero sin el campo límite.

En consecuencia, la Unidad de paginación maneja una tabla con un millón de entradas, conteniendo cada una la base (20 bits) y los derechos de acceso (12 bits).

Cada vez que la Unidad de Paginación detecta que la página a acceder no reside en la memoria principal, genera un fallo de página, que origina una excepción que llama a una rutina del S.O. que se encarga de trasladar dicha página desde la memoria virtual o disco hasta la memoria física o RAM.

Mecanismos de Protección

En el 386 está integrado un hardware que soporta un mecanismo de protección muy potente encargado de detectar la violación de cualquiera de sus reglas y detener el procesamiento normal de la CPU, al generar una excepción encargada de atender la transgresión.

El mecanismo de protección consigue el aislamiento entre tareas y el mantenimiento y defensa del grado de seguridad o confianza de cada módulo residente en las tareas.

La unidad de segmentación, siempre activa, soporta la mayor parte de la comprobación de las reglas, que son aplicadas a nivel de segmentos. Tras ella, la Unidad de paginación vuelve a comprobar las reglas de acceso que afectan a las páginas.

Interrupciones y Excepciones

Las interrupciones se originan por acontecimientos externos que activan la señal aplicada en algunas patillas del procesador o bien por la ejecución de instrucciones específicas.

Las excepciones se generan automáticamente como consecuencia de algún acontecimiento anormal producido y detectado en el desarrollo del programa en curso de ejecución.

En general, tanto las interrupciones como las excepciones, provocan, en primer lugar la detención del programa actual y, después, salvan en la pila la dirección de retorno (CS:EIP), a la que hay que regresar cuando finalice la rutina de atención a la interrupción o excepción. También, en ciertos casos, se salva el contenido del EFLAGS.

Interrupciones:

- Externas provocadas por hardware

  NMI e INTR

- Internas ocasionadas por software

  INT o INTO

Interrupciones y Excepciones

Excepciones:

Se originan en forma automática y como acontecimientos internos ocurridos en el procesador, cuando se detecta algún tipo de error o condición especial. Eje. : segmento no presente, violación de privilegio, coprocesador no presente, etc.

Se clasifican en tres tipos:

1. **Faltas o errores**: son excepciones que se detectan y atienden antes de la ejecución de la instrucción causante del error. Ej. cuando falta un segmento o página antes de la memoria. Después e micro reanuda la ejecución de la instrucción causante de la excepción.
2. **Excepciones propiamente dichas o trampas**: se detectan inmediatamente después de la ejecución de la instrucción que ocasiona el problema. Ej. las interrupciones ocasionadas por el usuario.
3. **Abortos**: son excepciones que no permiten la localización exacta de la instrucción que ha originado la situación anómala. Se emplean para señalar errores graves como los que derivan del comportamiento del equipo físico.