Aprendiendo Sistemas Operativos: Programación de Procesadores de Arquitectura IA-32

Este documento forma parte de la serie "Aprendiendo Sistemas Operativos" y sirve como una introducción a los aspectos básicos de la programación de procesadores de arquitectura IA-32. La serie "Aprendiendo Sistemas Operativos" puede ser usada en un entorno académico previa autorización del autor.

Autor:
Erwin Meza Vega
emezav@gmail.com

1 Generalidades de la arquitectura IA-32

Intel, el fabricante de estos procesadores de arquitectura IA-32, ha decidido mantener compatibilidad hacia atrás para permitir que el código desarrollado para procesadores desde 386 o 486 pueda ser ejecutado en procesadores actuales. Lo anterior implica una serie de decisiones de diseño en la estructura interna y en el funcionamiento de los procesadores, que en ciertas ocasiones limita a los programas pero que también ofrece una ventaja competitiva relacionada con la adopción masiva este tipo de procesadores y la posibilidad de ejecutar programas creados para procesadores anteriores en las versiones actuales sin ninguna modificación.

En los siguientes apartados se presentarán los aspectos generales de la arquitectura IA-32 requeridos para contar con una base sólida, que permita iniciar con el desarrollo de programas en ensamblador y en lenguaje C.

1.1 RESEÑA HISTÓRICA DE IA-32

Los procesadores Intel tienen sus orígenes en el 8086 y el 8088 (finales de los años 70). Implementaban la segmentación de memoria como una estrategia para referenciar direcciones de memoria mayores a las que se podían almacenar en un registro de propósito general. Usando la combinación de registros de segmento y registros de propósito general de 16 bits, estos procesadores podían referenciar hasta 1 MB de memoria.

Intel introdujo los procesadores 286 a principios de los años 80. Estos procesadores fueron los primeros en implementar el 'modo protegido' y el manejo de memoria virtual. En este modo protegido, los procesadores podían referenciar hasta 16 MB de memoria.

La arquitectura IA-32 tiene su inicio oficial con el procesador 386, que fue introducido a mediados de los años 80. Este contaba con registros de propósito general de 32 bits, con lo cual desde el punto de vista teórico era posible referenciar hasta 4 GB (2^{32} bytes) de memoria RAM. También incluía un modo especial, llamado 'Modo Virtual 8086', que ofrecía compatibilidad para los programas desarrollados para procesadores anteriores. Adicionalmente el 386 implementaba un esquema más general de segmentación e implementaba la paginación, que consiste en dividir la memoria en regiones lógicas de igual tamaño denominadas páginas.

A finales de los años 80 se introdujo el procesador 486, que marcó un hito en la historia del computador personal (PC). Unido a los primeros sistemas operativos para PC, este procesador fue uno de los principales promotores de la computación personal una escala no vista hasta entonces.

El procesador 486 mejoraba el desempeño de su predecesor, incluyendo la capacidad de tener varias instrucciones en diferentes niveles de ejecución al mismo tiempo. También implementaba una memoria caché de primer nivel dentro del procesador, con lo cual se aumentaba la posibilidad de ejecutar una instrucción en un ciclo de reloj. Adicionalmente, el 486 incluía una unidad de punto flotante y capacidades para el manejo de la energía.

A principios de los años 90 apareció el procesador Pentium, que por su diseño mejoró notablemente las capacidades del 486. Los aspectos más notables de los procesadores Pentium y posteriores (Pentium II, III, etc.) fueron su capacidad para ejecutar varias instrucciones por ciclo de reloj, la introducción de un segundo nivel de caché y la adición de las extensiones MMX (diseñadas para acelerar el desempeño de la multimedia y las comunicaciones).

Los procesadores posteriores hasta los que están disponibles hoy en día se dividen en familias que incluyen características entre las que sobresalen: múltiples núcleos de procesamiento (por ejemplo Dual Core, Core 2 duo o Xeon), arquitectura de 64 bits, mejoras en el caché, mejoras en la gestión de energía, características para movilidad y tecnologías de virtualización (VT). Las familias más importantes de procesadores Intel en la actualidad son: Pentium, Core, Core 2, Itanuim y Xeon.

Cada procesador actual cuenta con algunas o todas las características de la arquitectura IA-32. Por ejemplo, algunos procesadores actuales poseen múltiples núcleos con registros de 32 bits o múltiples núcleos con registros de 64 bits. Por ejemplo, un procesador Intel Core 2 Duo cuenta con dos núcleos con registros de 32 bits, y un procesador Xeon generalmente incluye varios núcleos con registros de 64 bits. La generación actual de procesadores Intel Core (Core I3, Core I5 y Core I7) implementan arquitecturas de 2, 4 y hasta 6 núcleos con registros de 64 bits.

No obstante, para mantener la compatibilidad hacia atrás, todos los procesadores inician en un modo en el cual se comportan como un procesador 8086 muy rápido, con algunas extensiones que le permiten habilitar el modo de operación en el cual aprovechan todas sus características. Esto ofrece una posibilidad sin igual para el aprendizaje de la programación básica de procesadores de la arquitectura IA-32.

1.2 CARACTERÍSTICAS DE LA ARQUITECTURA IA-32

A continuación se enumeran las características más importantes que ofrece la arquitectura IA-32 para la ejecución de programas.

1.2.1 Modos de operación

Los procesadores IA-32 pueden operar en varios modos, entre los que sobresalen:

- **Modo protegido**: Este es el modo nativo del procesador. Aprovecha todas las características de su arquitectura, tales como registros de 32 bits, y el acceso a todo su conjunto de instrucciones y extensiones.
- **Modo real (Modo de direcciones reales)**: En este modo el procesador se encuentra en un entorno de ejecución en el cual se comporta como un 8086 muy rápido, y sólo tiene acceso a un conjunto limitado de instrucciones que le permiten ejecutar tareas básicas y habilitar el modo protegido. La limitación más notable en este modo consiste en que sólo se puede acceder a los 16 bits menos significativos de los registros de propósito general, y sólo se pueden utilizar los 20 bits menos significativos del bus de direcciones. Esto causa que en modo real solo se pueda acceder a 1 Megabyte de memoria.
- **Modo de mantenimiento del sistema**: En este modo se puede pasar a un entorno de ejecución limitado, para realizar tareas de mantenimiento o depuración.

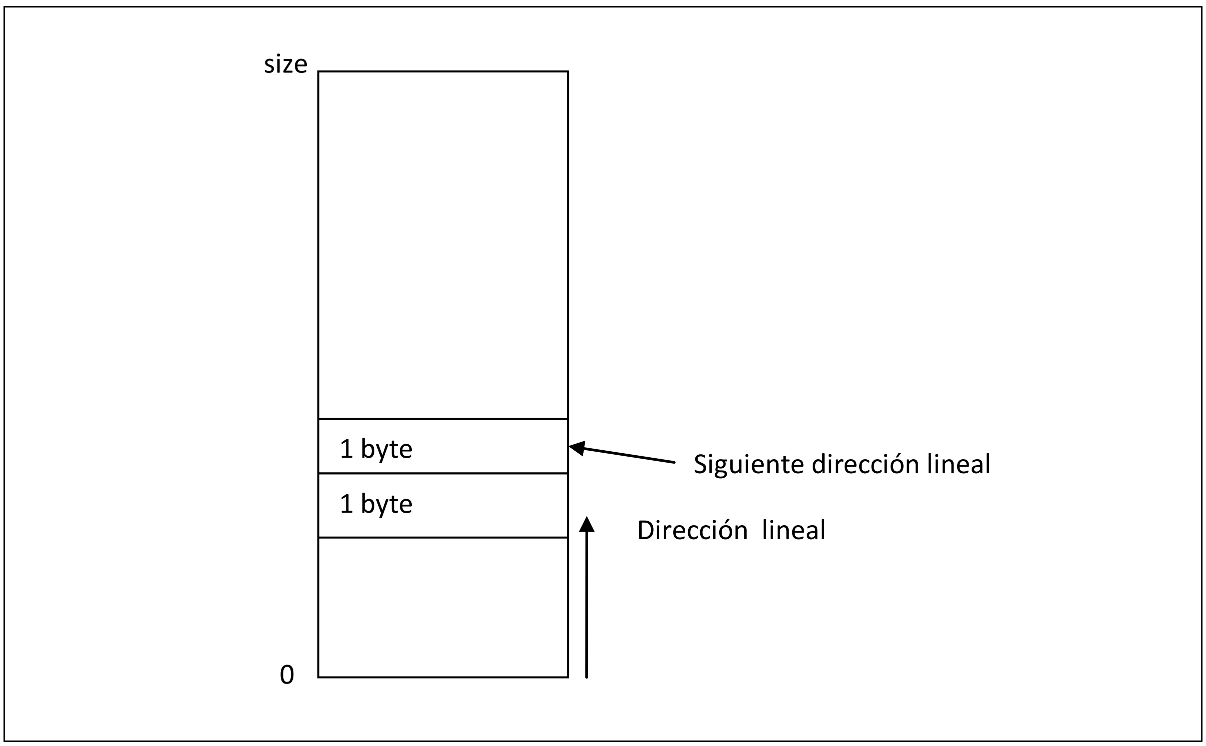
- **Modo Virtual 8086**: Este es un sub-modo al cual se puede acceder cuando el procesador opera en modo protegido. Permite ejecutar código desarrollado para 8086 en un entorno multi-tarea y protegido.
- **Modo IA32-e**: Para procesadores de 64 bits, además de los modos anteriores existen otros dos sub-modos: modo de compatibilidad y modo de 64 bits. El modo de compatibilidad permite la ejecución de programas desarrollados para modo protegido sin ninguna modificación, y el modo de 64 bits proporciona soporte para acceder a los 64 bits de los registros y un espacio de direcciones mayor que 64 Gigabytes.

1.2.2 Entorno de ejecución

Cualquier programa o tarea a ser ejecutado en un procesador de arquitectura IA-32 cuenta con un entorno de ejecución compuesto por un espacio de direcciones de memoria y un conjunto de registros. A continuación se describen estos componentes.

1.2.2.1 Espacio de direcciones de memoria

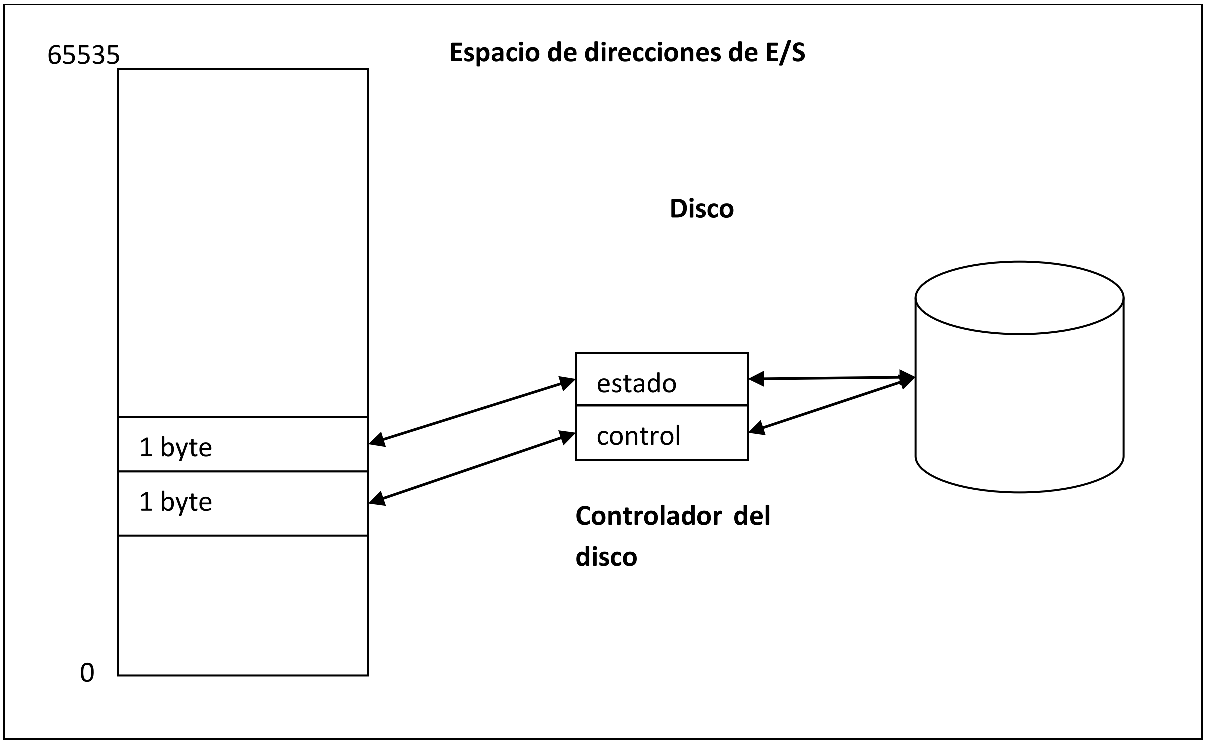
En la arquitectura IA-32 la memoria puede ser vista como una secuencia lineal (o un arreglo) de bytes, uno tras del otro. A cada byte le corresponde una dirección única (Ver figura).



El código dentro de una tarea o un programa puede referenciar un espacio direcciones de hasta 4 Gigabytes. Este espacio lineal puede estar mapeado directamente a la memoria física, con lo cual se tendrá acceso a 4 Gigabytes de RAM (2^{32} direcciones lineales diferentes). Si el procesador cuenta con las extensiones requeridas, es posible acceder a un espacio físico de hasta 64 Gigabytes.

1.2.2.2 Espacio de direcciones de Entrada / Salida

Los procesadores IA-32 incluyen otro espacio de direcciones, diferente al espacio de direcciones lineal, llamado espacio de direcciones de Entrada / Salida. A este espacio de 65536 (64K) direcciones se mapean los registros de los controladores de dispositivos de entrada / salida como el teclado, los discos o el mouse (Ver figura). Su acceso se realiza a través de un par de instrucciones específicas del procesador (in y out).



1.2.2.3 Registros

El procesador cuenta con una serie de registros en los cuales puede almacenar información. Estos registros pueden ser clasificados en:

- **Registros de propósito general**: Estos registros son utilizados para almacenar valores, realizar operaciones aritméticas o lógicas o para referenciar el espacio de direcciones lineal. En procesadores de 32 bits existen ocho (8) registros de propósito general, cada uno de los cuales tiene un tamaño de 32 bits. Estos registros son: EAX, EBX, ECX, EDX, ESI, EDI, ESP y EBO. A pesar que se denominan registros de propósito general, y pueden ser utilizados como tal, estos registros tienen usos especiales para algunas instrucciones del procesador.
- **Registros de segmento**: Estos registros permiten almacenar apuntadores al espacio de direcciones lineal. Los procesadores IA-32 poseen seis (6) registros de segmento. Estos son: CS (código), DS (datos), ES, FS, GS (datos), y SS (pila). Su uso depende del modo de operación. En modo real, los registros de segmento almacenan un apuntador a la dirección lineal del inicio del segmento dividida en 16. En modo protegido se denominan

'selectores', y contienen un apuntador a una estructura de datos en la cual se describe un segmento de memoria.

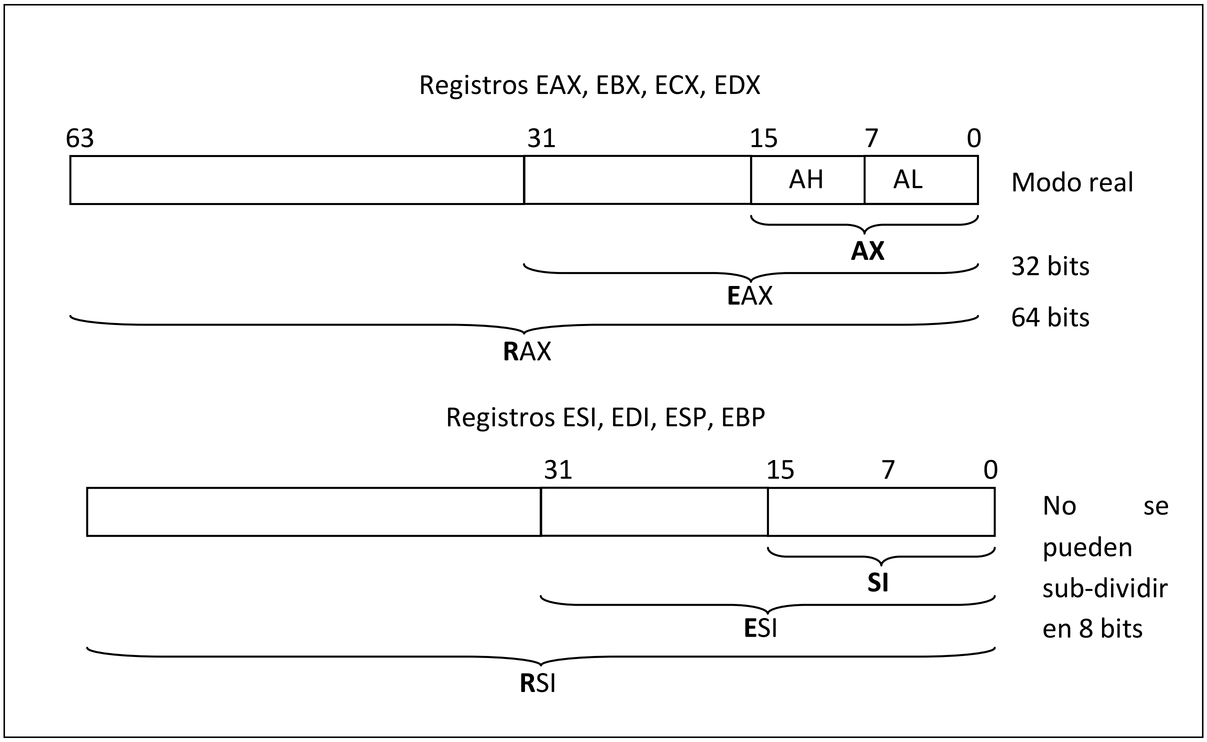
- **Registro EFLAGS**: Este registro de 32 bits contiene una serie de banderas (flags) que tienen diversos usos. Algunas reflejan el estado del procesador y otras controlan su ejecución. Existen instrucciones específicas para modificar el valor de EFLAGS.
- **Registro EIP**: Este registro almacena el apuntador a la dirección lineal de la siguiente instrucción que el procesador debe ejecutar.
- **Registros de control**: El procesador posee cinco (5) registros de control CR0 a CR5. Estos registros junto con EFLAGS controlan la ejecución del procesador.
- **Registros para el control de la memoria**: Estos registros apuntan a las estructura de datos requeridas para el funcionamiento del procesador en modo protegido. Ellos son: GDTR, IDTR, TR y LDTR.
- **Registros de depuración**: Estos registros contienen información que puede ser usada para depurar el código que está ejecutando el procesador. Los procesadores IA-32 cuentan con ocho (8) registros de depuración, DR0 a DR7.
- **Registros específicos**: Cada variante de procesador IA-32 incluye otros registros, tales como los registros MMX, los registros de la unidad de punto flotante (FPU) entre otros.

Algunos registros de propósito general pueden ser sub-divididos en registros más pequeños a los cuales se puede tener acceso. Esto permite la compatibilidad con programas diseñados para procesadores anteriores. A continuación se presentan las posibles sub-divisiones de los registros de propósito general, considerando procesadores de hasta 64 bits:

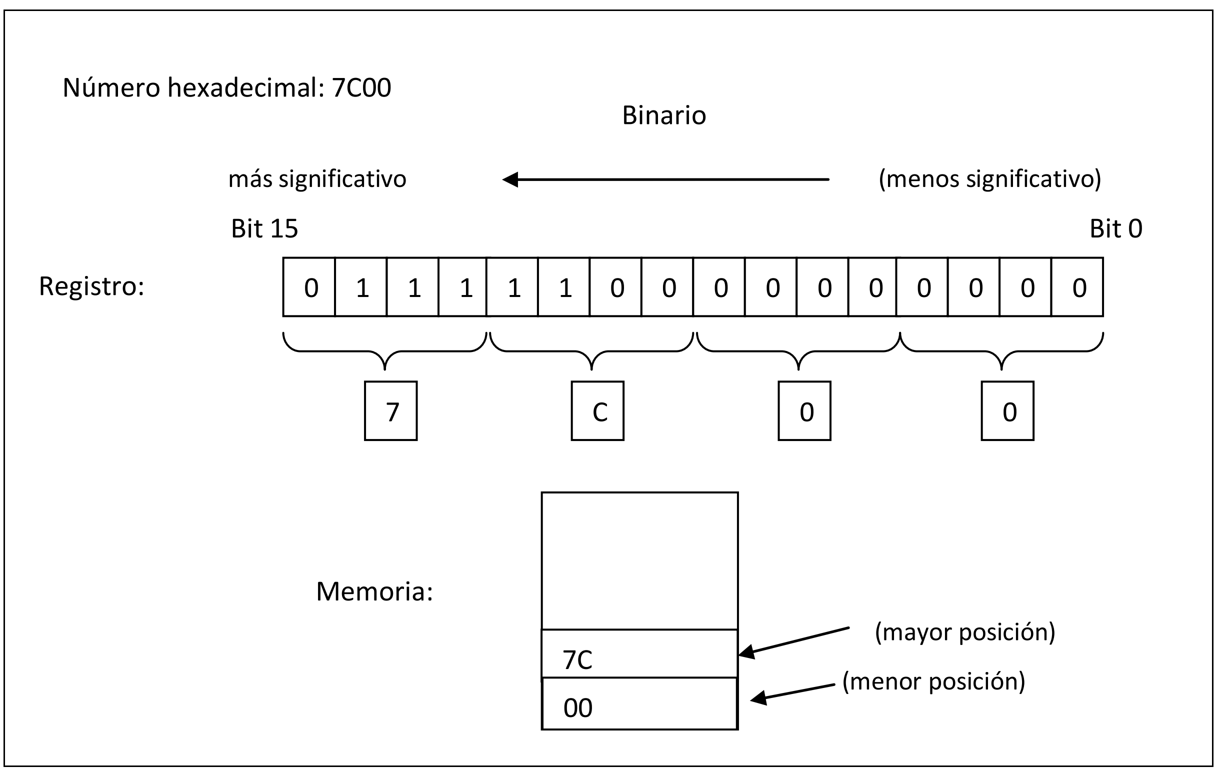
64 bits	32 bits	16 bits	8 bits	8 bits
RAX	EAX	AX	AH	AL
RBX	EBX	BX	BH	BL
RCX	ECX	CX	CH	CL
RDX	EDX	DX	DH	DL
RSI	ESI	SI	No disponible	
RDI	EDI	DI	No disponible	
RSP	ESP	SP	No disponible	
RBP	EBP	BP	No disponible	

A nivel de programación, es posible acceder a cada uno de estos sub-registros de acuerdo con el modo de operación. Por ejemplo, para modo de direcciones real, es posible usar los registros de 8 bits y los registros de 16 bits. En modo protegido se puede usar los registros de 8, 16 y 32 bits. Si el procesador cuenta con registros de 64 bits y se encuentra en el modo de 64 bits, es posible acceder a los registros de 8, 16, 32 y 64 bits.

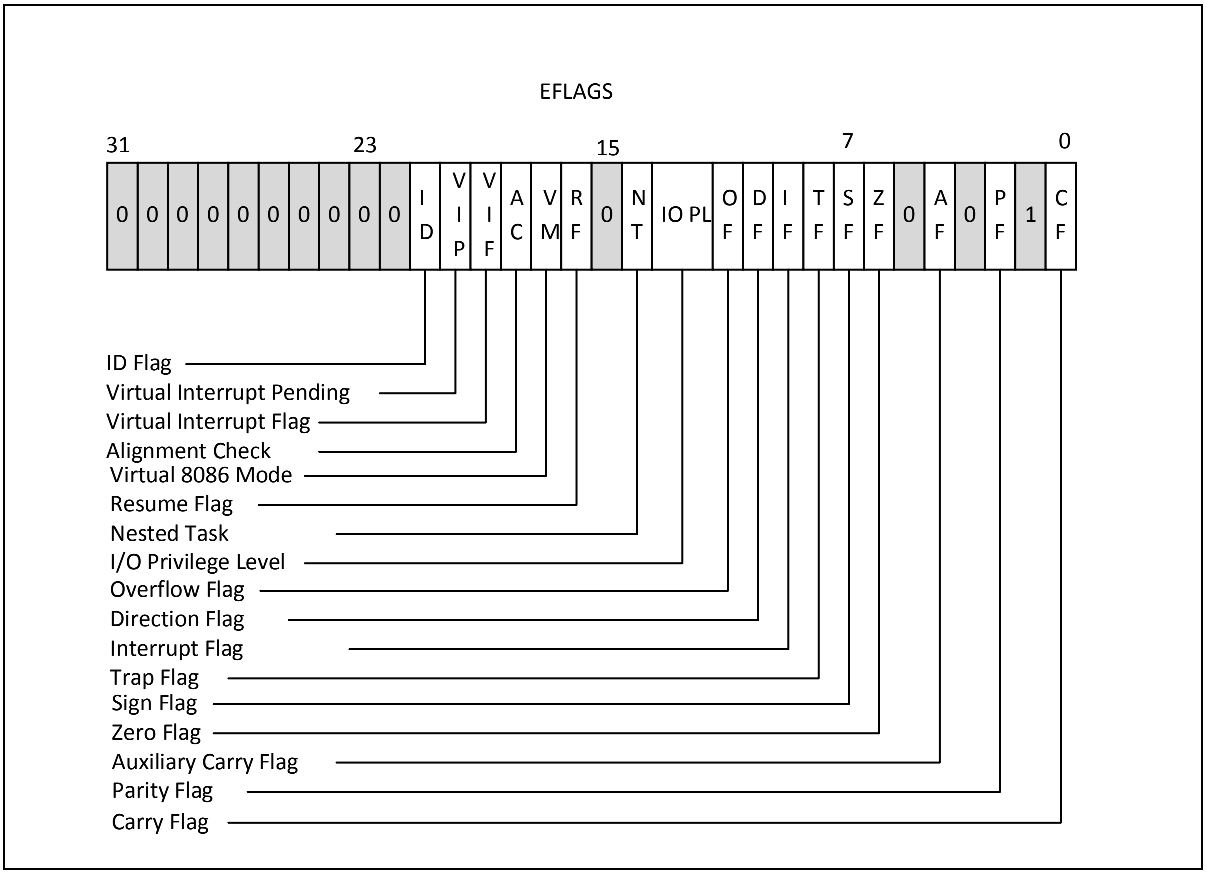
La siguiente figura muestra como se encuentran dispuestos los bits de los registros de propósito general. Los registros EBX, ECX y EDX se encuentran dispuestos de la misma forma que EAX. Los registros EDI, ESP Y EBP se disponen de la misma forma que ESI.



El formato de almacenamiento de la arquitectura IA-32 es *Little-Endian*, lo cual significa que los bits menos significativos de un número se almacenan en las posiciones menores de la memoria y de los registros, y los bits más significativos se almacenan en posiciones superiores (Ver figura).



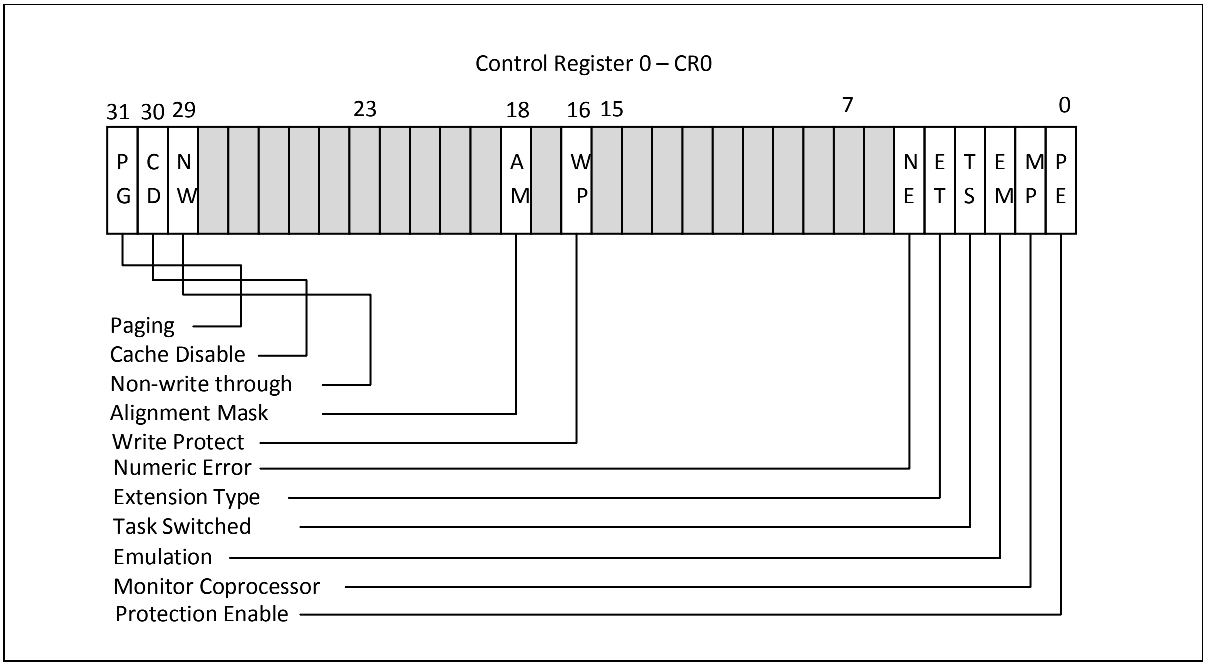
La siguiente figura muestra la disposición de los bits (flags) dentro de registro EFLAGS. Este registro almacena el estado y parte del control del procesador. El manual de arquitectura de sistema de Intel ofrece una descripción detallada de cada uno de los bits.



Los bits del registro EFLAGS se pueden clasificar en:

- Bits de estado: Reflejan el estado actual del procesador. Son bits de estado: OF, SF, ZF, AF y PF.
- Bits de control: Controlan de alguna forma la ejecución del procesador. Dentro de EFLAGS se encuentra el bit DF, que permite controlar la dirección de avance en las operaciones sobre cadenas de caracteres.
- Bits del sistema: Los bits ID, VIP, VIF, AC, VM, RF, NT, IOPL, IF y TF son usados por el procesador para determinar condiciones en su ejecución, o para habilitar / deshabilitar determinadas características. Por ejemplo, estableciendo el bit IF en 1 se habilitan las interrupciones, mientras un valor de 0 en este bit deshabilita las interrupciones.
- Bits reservados: Estos bits marcados con un color diferente se reservan por la arquitectura IA-32 para futura expansión. Deben permanecer con los valores que se muestran en la figura (cero o uno). No se deben usar, ya que es posible que en versiones posteriores de los procesadores IA-32 tengan un significado específico.

A continuación se ilustra la disposición de los bits dentro del registro CR0 (Control Register 0).



Los bits más importantes de CR0 desde el punto de vista de programación son el bit 0 (Protection Enable – PE), y el bit 31 (Paging – PG). Estos permiten habilitar el modo protegido y la paginación, respectivamente.

No obstante antes de pasar a modo protegido y de habilitar la paginación se deben configurar unas estructuras de datos que controlan la ejecución del procesador. El paso a modo protegido y las estructuras de datos asociadas se presentarán más adelante en este documento.

1.2.3 Organización de la memoria

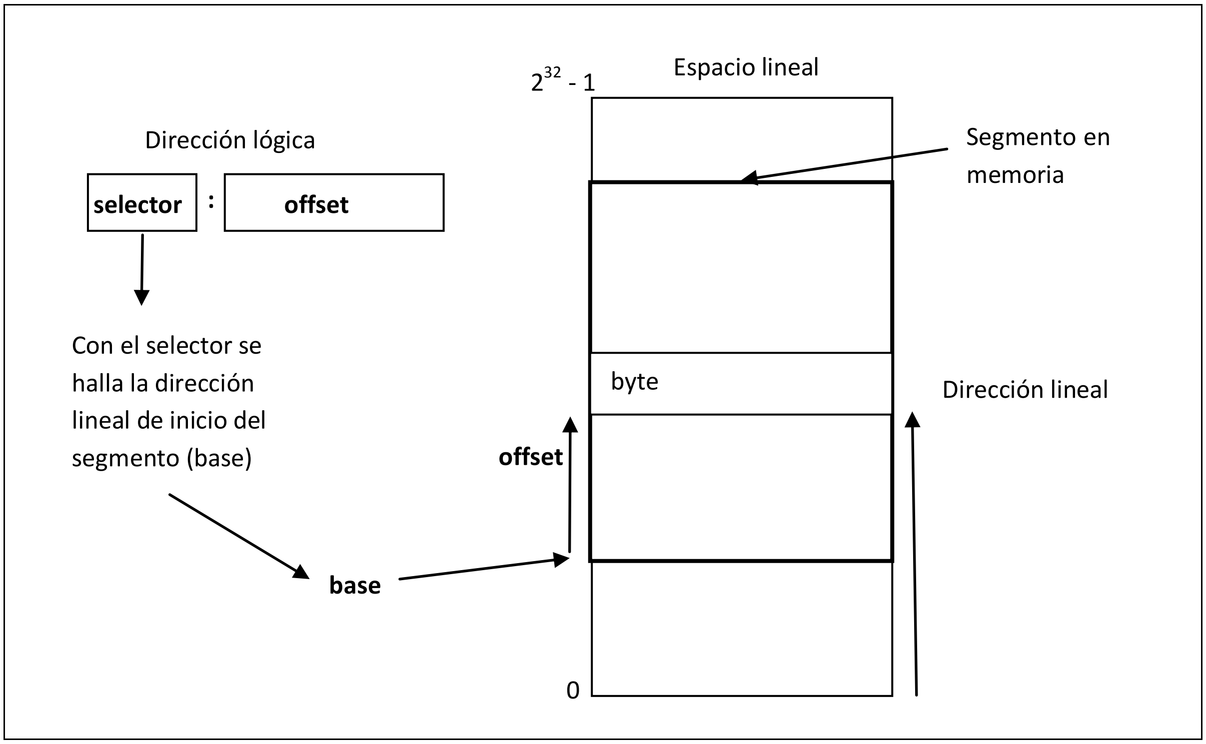
La memoria en los procesadores de arquitectura IA-32 se puede organizar y manejar en tres formas básicas: Modo segmentado, modo real de direcciones y modo plano. A continuación se muestran los detalles de cada modo de organización de memoria.

1.2.3.1 Modo segmentado

Este es el modo por defecto de organización de memoria. En este modo, la memoria se aprecia como un grupo de espacios lineales denominados *segmentos*. Cada segmento puede ser de diferente tipo, siendo los más comunes segmentos de código y datos.

Para referenciar un byte dentro de un segmento se debe usar una dirección lógica, que consiste en un par selector: offset[1]. Con el selector se puede determinar la dirección lineal de inicio del segmento, y el offset determina el número de bytes que se debe desplazar desde el inicio del segmento. Así se obtiene una dirección lineal en el espacio de direcciones de memoria. A continuación se presenta una figura que ilustra cómo realiza este proceso.

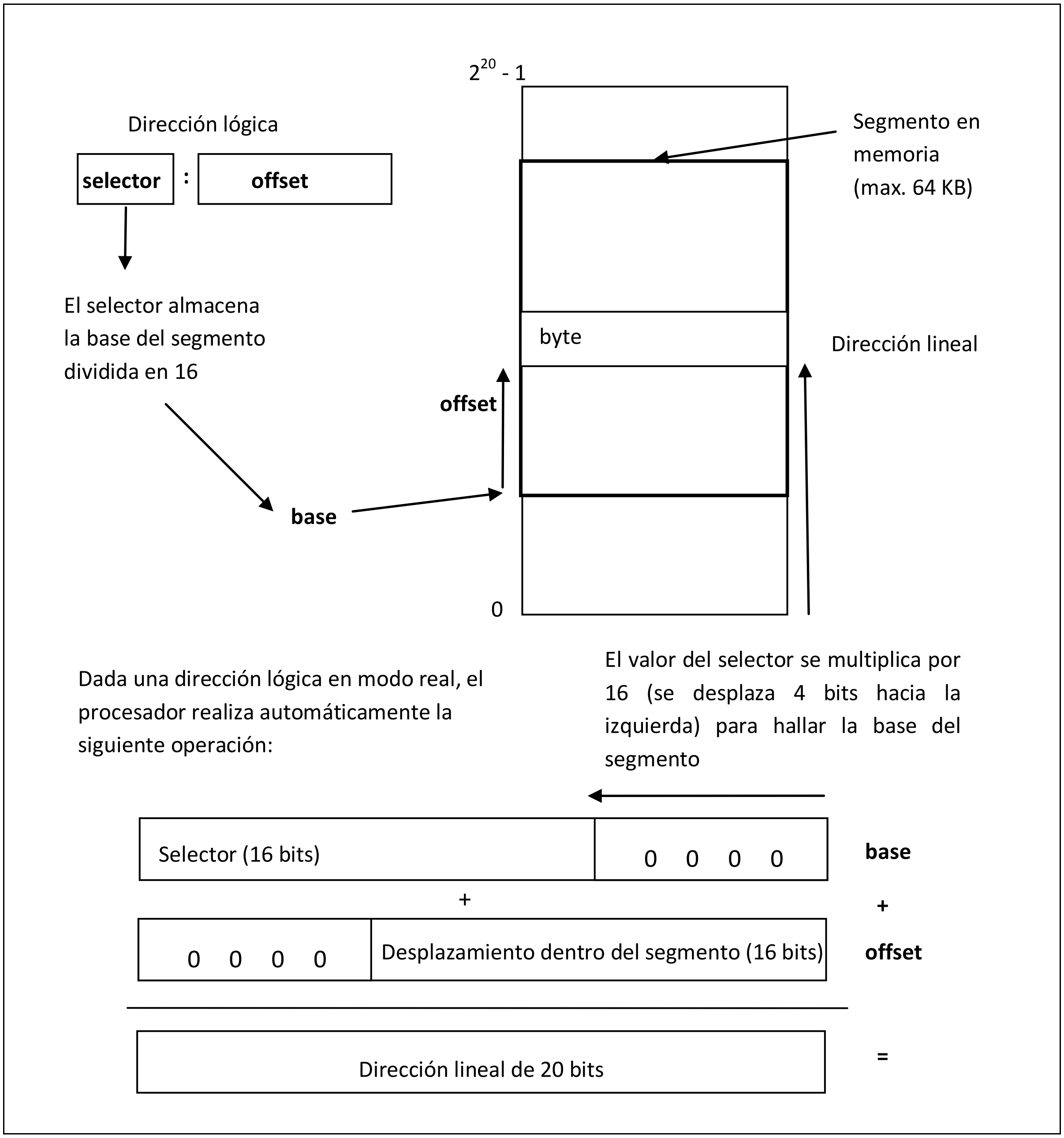
[1] Se usarán la palabras 'offset' y 'desplazamiento' de forma indiscriminada.



1.2.3.2 Modo real de direcciones

El modo real de direcciones es el modo inicial de todo procesador IA-32 luego de ser encendido o reiniciado. Se usa para ofrecer compatibilidad con procesadores de generaciones que abarcan hasta el propio 8086. En modo real de direcciones el espacio lineal de direcciones se encuentra dividido en segmentos con un tamaño máximo de 64 Kilobytes. Adicionalmente sólo es posible usar los 16 bits menos significativos de los registros para referenciar una dirección lineal.

Las direcciones lógicas en modo real de direcciones también están conformadas por un selector y un offset. Tanto el selector como el desplazamiento tienen un tamaño de 16 bits. Con el fin de permitir el acceso a un espacio de direcciones lineal mayor, el selector almacena la dirección de inicio del segmento dividida en 16. Para traducir una dirección lógica a lineal, el procesador toma el valor del selector y lo multiplica por 16, para hallar la base del segmento. Luego a esta base le suma el offset. La siguiente figura ilustra el proceso de transformar una dirección lógica a lineal en el modo real de direcciones.



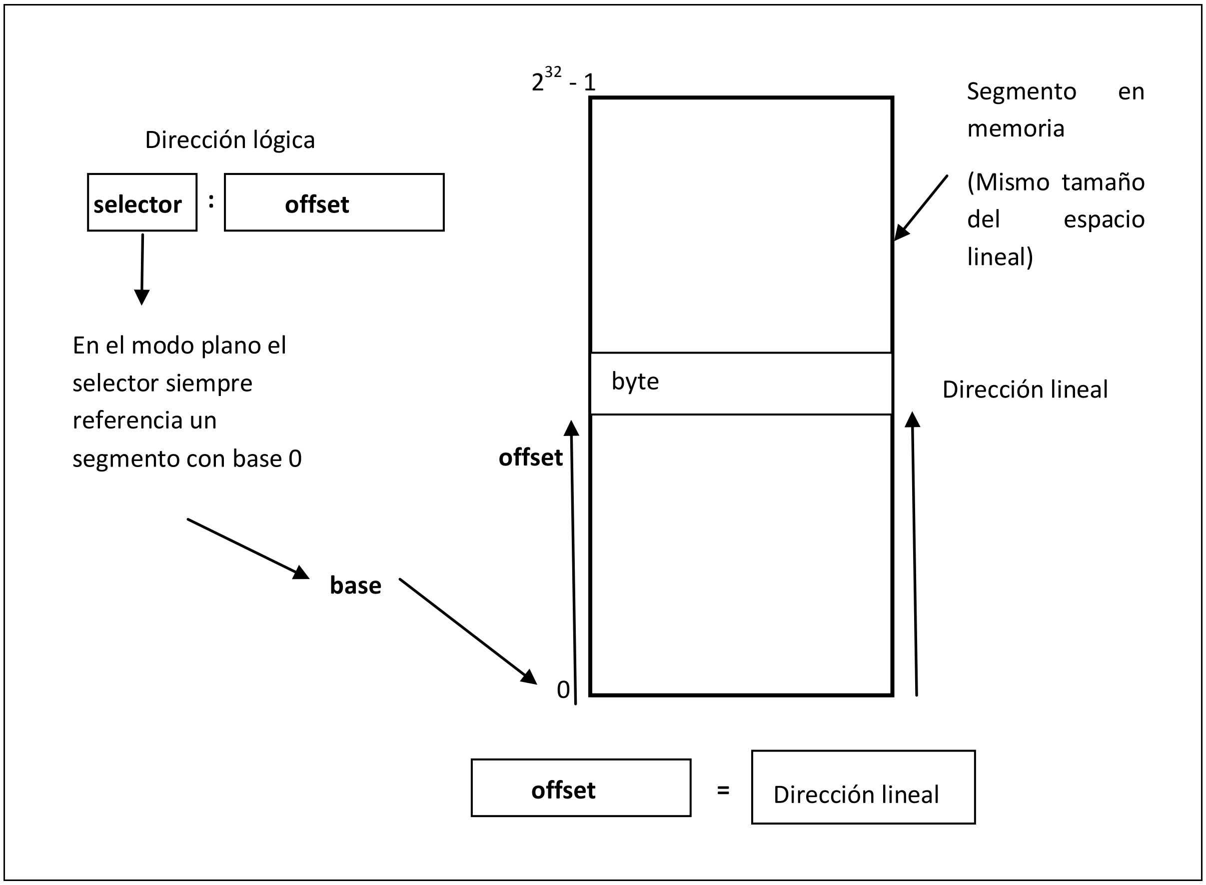
Por las características especiales del modo real, solo es posible acceder a los primeros 2^{20} bytes del espacio lineal de direcciones. En la práctica esto significa que en modo real sólo se puede tener acceso al primer Megabyte de memoria.

1.2.3.3 Modo plano (Flat)

El modo plano es otro caso especial del modo segmentado. La memoria en este modo se presenta como un espacio continuo de direcciones (espacio lineal de direcciones). Para procesadores de 32 bits, este espacio abarca desde el byte 0 hasta el byte 2^{32} (4GB).

En la práctica, el modo plano se puede activar al definir segmentos que ocupan todo el espacio lineal (con base = 0 y un tamaño igual al máximo tamaño disponible).

Dado que en este modo se puede ignorar la base del segmento (al considerar que siempre inicia en 0), el desplazamiento en una dirección lógica es igual a la dirección lineal (Ver figura).



1.2.3.4 *Modo de organización de memoria vs. Modo de operación*

El mapeo entre modo de organización de memoria y modo de operación del procesador se da de resume en la siguiente tabla:

Organización de memoria/ Operación	**Modo real**	**Modo protegido de 32 bits**	**Modo IA32-e**	
			Modo de compatibilidad	**Modo de 64 bits**
Modo segmentado	NO	SI	SI	NO
Modo real	SI	SI[2]	SI (igual que en modo protegido de 32 bits)	NO
Modo plano	NO[3]	SI	SI	SI

[2] En modo protegido de 32 bits es posible acceder al modo real de organización de memoria sólo en el sub-modo Virtual 8086

[3] Cuando el procesador opera en modo real, se puede activar un modo especial en el cual es posible acceder a un pseudo-modo llamado 'modo unreal'. En este pseudo-modo la memoria se organiza de forma similar al modo plano.