ARQUITECTURA DE COMPUTADORAS

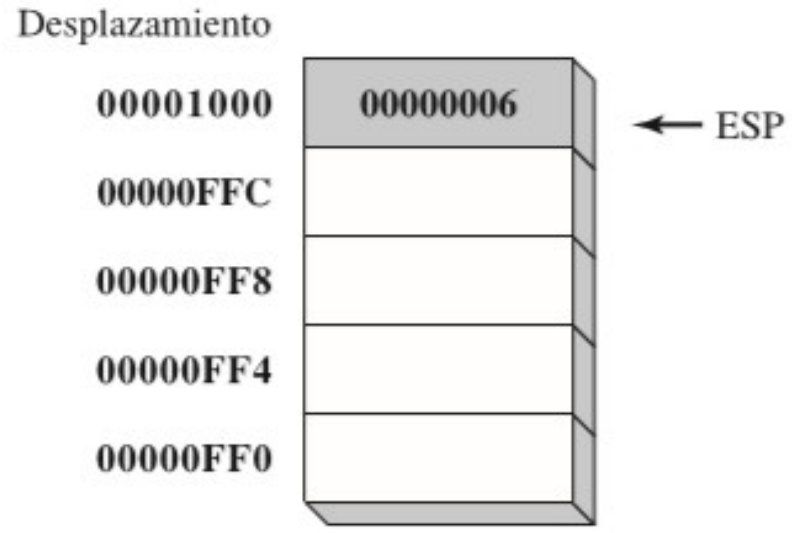
Manejo de pila

Operaciones con la pila

- La pila en tiempo de ejecución es un arreglo de memoria que la CPU administra directamente, mediante el uso de dos registros: SS y ESP.
- El registro ESP guarda un desplazamiento de 32 bits hacia el tope de la pila
- Cada posición de la pila contiene 32 bits

Instrucciones que manipulan la pila

- CALL, RET, PUSH y POP
- Todas estas instrucciones modifican el valor de ESP



Funcionamiento de la pila

- PUSH: Siempre que se meten datos, el primer byte de datos (el más significativo) se mueve a la posición de memoria apuntada por ESP-1 y el segundo se mueve a la dirección de memoria ESP-2 y así sucesivamente.
- Veamos un ejemplo

PUSH

Simbólica	*Ejemplo*	*Observación*
PUSH reg16	PUSH BX	Registro de 16 bits.
PUSH reg32	PUSH EDX	Registro de 32 bits.
PUSH mem16	PUSH WORD PTR[BX]	Apuntador de 16 bits.
PUSH mem32	PUSH DWORD PTR[EBX]	Apuntador de 32 bits.
PUSH seg	PUSH DS	Registro de segmento.
PUSH inm8	PUSH 'R'	8 bits, inmediato.
PUSH inm16	PUSH 1000H	16 bits, inmediato.
PUSH inm32	PUSHD 20	32 bits, inmediato.
PUSHA	PUSHA	Guarda todos los registros de 16 bits.
PUSHAD	PUSHAD	Guarda todos los registros de 32 bits.
PUSHF	PUSHF	Guarda las banderas.
PUSHFD	PUSHFD	Guarda EFLAGS.

Funcionamiento de la pila

- POP: Siempre que se sacan datos, de la pila, estos se pueden colar en un registro de 16 bits o de 32, un registro de segmento o una posición de memoria de 16 o 32 bits.
- El primer byte de datos que se saca de la pila (posición direccionada por ESP)se mueve a la posición a la parte baja del registro o memoria. El segundo byte apuntada por ESP-1 se coloca en el siguiente byte del destino y así sucesivamente.
- Veamos un ejemplo

POP

Simbólica	*Ejemplo*	*Observación*
POP reg16	POP CX	Registro de 16 bits.
POP reg32	POP EBP	Registro de 32 bits.
POP mem16	POP WORD PTR[BX+1]	Apuntador de 16 bits.
POP mem32	POP DATOS3	Dirección de memoria de 32 bits.
POP seg	POP FS	Registro de segmento.
POPA	POPA	Saca todos los registros de 16 bits.
POPAD	POPAD	Saca todos los registros de 32 bits.
POPF	POPF	Saca las banderas.
POPFD	POPFD	Mete EFLAGS.

Otras de instrucciones con la pila

- PUSHFD/POPFD
  - mete/saca el registro EFLAGS de 32 bits en la pila
- PUSHAD, PUSHA, POPAD y POPA
  - La instrucción PUSHAD mete todos los registros de propósito general de 32 bits en la pila, en el siguiente orden: EAX, ECX, EDX, EBX, ESP (su valor antes de ejecutar PUSHAD), EBP, ESI y EDI.
  - La instrucción POPAD saca los mismos registros de la pila, en orden inverso

FIGURA 4-12 La operación de la instrucción PUSHA, en donde se muestra la posición y el orden de los datos de la pila.