

7.1 Task State Segment

All the information the processor needs in order to manage a task is stored in a special type of segment, a task state segment (TSS). [Figure 7-1](#) shows the format of a TSS for executing 80386 tasks. (Another format is used for executing 80286 tasks; refer to [Chapter 13](#).)

The fields of a TSS belong to two classes:

1. A dynamic set that the processor updates with each switch from the task. This set includes the fields that store:
 - The general registers (EAX, ECX, EDX, EBX, ESP, EBP, ESI, EDI).
 - The segment registers (ES, CS, SS, DS, FS, GS).
 - The flags register (EFLAGS).
 - The instruction pointer (EIP).
 - The selector of the TSS of the previously executing task (updated only when a return is expected).
2. A static set that the processor reads but does not change. This set includes the fields that store:
 - The selector of the task's LDT.
 - The register (PDBR) that contains the base address of the task's page directory (read only when paging is enabled).
 - Pointers to the stacks for privilege levels 0-2.
 - The T-bit (debug trap bit) which causes the processor to raise a debug exception when a task switch occurs . (Refer to [Chapter 12](#) for more information on debugging.)
 - The I/O map base (refer to [Chapter 8](#) for more information on the use of the I/O map).

Task state segments may reside anywhere in the linear space. The only case that requires caution is when the TSS spans a page boundary and the higher-addressed page is not present. In this case, the processor raises an exception if it encounters the not-present page while reading the TSS during a task switch. Such an exception can be avoided by either of two strategies:

1. By allocating the TSS so that it does not cross a page boundary.
2. By ensuring that both pages are either both present or both not-present at the time of a task switch. If both pages are not-present, then the page-fault handler must make both pages present before restarting the instruction that caused the task switch.

Figure 7-1. 80386 32-Bit Task State Segment

31	23	15	7	0	
I/O MAP BASE		0 0 0 0 0 0 0 0		0 0 0 0 0 0 0 0	T 64
0 0 0 0 0 0 0 0		LDT			60
0 0 0 0 0 0 0 0		GS			5C
0 0 0 0 0 0 0 0		FS			58
0 0 0 0 0 0 0 0		DS			54
0 0 0 0 0 0 0 0		SS			50
0 0 0 0 0 0 0 0		CS			4C
0 0 0 0 0 0 0 0		ES			48
		EDI			44
		ESI			40
		EBP			3C
		ESP			38
		EBX			34
		EDX			30
		ECX			2C
		EAX			28
		EFLAGS			24
		INSTRUCTION POINTER <EIP>			20
		CR3 <PDPR>			1C
0 0 0 0 0 0 0 0		SS2			18
		ESP2			14
0 0 0 0 0 0 0 0		SS1			10
		ESP1			0C
0 0 0 0 0 0 0 0		SS0			8
		ESP0			4
0 0 0 0 0 0 0 0		BACK LINK TO PREVIOUS TSS			0

NOTE

0 MEANS INTEL RESERVED. DO NOT DEFINE.

up: [Chapter 7 -- Multitasking](#)
prev: [Chapter 7 -- Multitasking](#)
next: [7.2 TSS Descriptor](#)