
7.2 TSS Descriptor

The task state segment, like all other segments, is defined by a descriptor. Figure 7-2 shows the format of a TSS descriptor.

The B-bit in the type field indicates whether the task is busy. A type code of 9 indicates a non-busy task; a type code of 11 indicates a busy task. Tasks are not reentrant. The B-bit allows the processor to detect an attempt to switch to a task that is already busy.

The BASE, LIMIT, and DPL fields and the G-bit and P-bit have functions similar to their counterparts in data-segment descriptors. The LIMIT field, however, must have a value equal to or greater than 103. An attempt to switch to a task whose TSS descriptor has a limit less that 103 causes an exception. A larger limit is permissible, and a larger limit is required if an I/O permission map is present. A larger limit may also be convenient for systems software if additional data is stored in the same segment as the TSS.

A procedure that has access to a TSS descriptor can cause a task switch. In most systems the DPL fields of TSS descriptors should be set to zero, so that only trusted software has the right to perform task switching.

Having access to a TSS-descriptor does not give a procedure the right to read or modify a TSS. Reading and modification can be accomplished only with another descriptor that redefines the TSS as a data segment. An attempt to load a TSS descriptor into any of the segment registers (CS, SS, DS, ES, FS, GS) causes an exception.

TSS descriptors may reside only in the GDT. An attempt to identify a TSS with a selector that has TI=1 (indicating the current LDT) results in an exception.

Figure 7-2. TSS Descriptor for 32-bit TSS