up: Chapter 7 -- Multitasking
prev: 7.3 Task Register
next: 7.5 Task Switching

7.4 Task Gate Descriptor

A task gate descriptor provides an indirect, protected reference to a TSS. Figure 7-4 illustrates the format of a task gate.

The SELECTOR field of a task gate must refer to a TSS descriptor. The value of the RPL in this selector is not used by the processor.

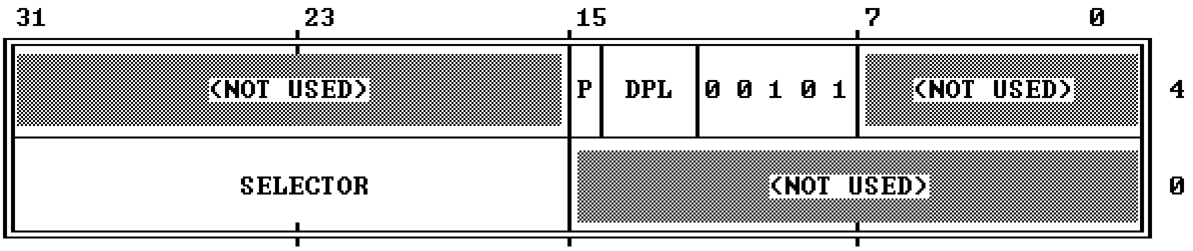
The DPL field of a task gate controls the right to use the descriptor to cause a task switch. A procedure may not select a task gate descriptor unless the maximum of the selector's RPL and the CPL of the procedure is numerically less than or equal to the DPL of the descriptor. This constraint prevents untrusted procedures from causing a task switch. (Note that when a task gate is used, the DPL of the target TSS descriptor is not used for privilege checking.)

A procedure that has access to a task gate has the power to cause a task switch, just as a procedure that has access to a TSS descriptor. The 80386 has task gates in addition to TSS descriptors to satisfy three needs:

1. The need for a task to have a single busy bit. Because the busy-bit is stored in the TSS descriptor, each task should have only one such descriptor. There may, however, be several task gates that select the single TSS descriptor.
2. The need to provide selective access to tasks. Task gates fulfill this need, because they can reside in LDTs and can have a DPL that is different from the TSS descriptor's DPL. A procedure that does not have sufficient privilege to use the TSS descriptor in the GDT (which usually has a DPL of 0) can still switch to another task if it has access to a task gate for that task in its LDT. With task gates, systems software can limit the right to cause task switches to specific tasks.
3. The need for an interrupt or exception to cause a task switch. Task gates may also reside in the IDT, making it possible for interrupts and exceptions to cause task switching. When interrupt or exception vectors to an IDT entry that contains a task gate, the 80386 switches to the indicated task. Thus, all tasks in the system can benefit from the protection afforded by isolation from interrupt tasks.

Figure 7-5 illustrates how both a task gate in an LDT and a task gate in the IDT can identify the same task.

Figure 7-4. Task Gate Descriptor



up: Chapter 7 -- Multitasking
prev: 7.3 Task Register
next: 7.5 Task Switching