OS之TSS概念解析：

TSS全称 （计算机汇编程序概念）任务状态段(Task State Segment)是保存一个任务重要信息的特殊段。任务状态段描述符用于描述这样的系统段。任务状态段寄存器TR的可见部分含有当前任务的任务状态段描述符的选择子，TR的不可见的高速缓冲寄存器部分含有当前任务状态段的段基地址和段界限等信息。

TSS(任务状态段)

1 什么是TSS

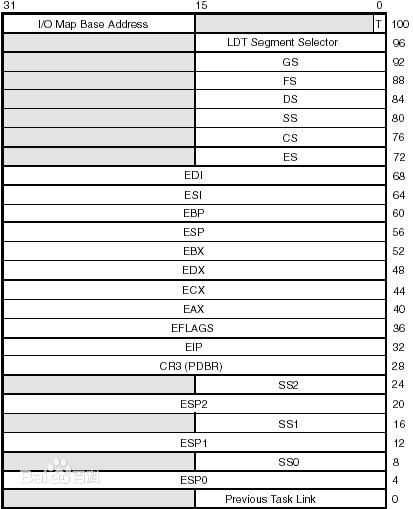
TSS 全称task state segment，是指在操作系统[进程管理](http://baike.baidu.com/view/364947.htm)的过程中，任务（进程）切换时的任务现场信息。

2 TSS工作细节

TSS在任务切换过程中起着重要作用，通过它实现任务的挂起和恢复。所谓任务切换是指，挂起当前正在执行的任务，恢复或启动另一任务的执行。在任务切换过程中，首先，处理器中各寄存器的当前值被自动保存到TR（任务寄存器）所指定的TSS中；然后，下一任务的TSS的选择子被装入TR；最后，从TR所指定的TSS中取出各寄存器的值送到处理器的各寄存器中。由此可见，通过在TSS中保存任务现场各寄存器状态的完整映象，实现任务的切换。

3 TSS的格式

任务状态段TSS的基本格式如下图所示。



TSS的基本格式由104字节组成。这104字节的基本格式是不可改变的，但在此之外系统软件还可定义若干附加信息。基本的104字节可分为链接字段区域、内层堆栈指针区域、地址映射寄存器区域、寄存器保存区域和其它字段等五个区域。

(1). [寄存器](http://baike.baidu.com/view/6159.htm)保存区域

寄存器保存区域位于TSS内偏移20H至5FH处，用于保存通用寄存器、段寄存器、指令指针和标志寄存器。当TSS对应的任务正在执行时，保存区域是未定义的；在当前任务被切换出时，这些寄存器的当前值就保存在该区域。当下次切换回原任务时，再从保存区域恢复出这些寄存器的值，从而，使处理器恢复成该任务换出前的状态，最终使任务能够恢复执行。

从上图可见，各通用寄存器对应一个32位的双字，指令指针和标志寄存器各对应一个32位的双字；各段寄存器也对应一个32位的双字，段寄存器中的选择子只有16位，安排再双字的低16位，高16位未用，一般应填为0。

(2). 内层堆栈指针区域

为了有效地实现保护，同一个任务在不同的特权级下使用不同的堆栈。例如，当从外层特权级3变换到内层特权级0时，任务使用的堆栈也同时从3级变换到0级堆栈；当从内层特权级0变换到外层特权级3时，任务使用的堆栈也同时从0级堆栈变换到3级堆栈。所以，一个任务可能具有四个堆栈，对应四个特权级。四个堆栈需要四个堆栈指针。

TSS的内层堆栈指针区域中有三个堆栈指针，它们都是48位的全指针(16位的选择子和32位的偏移)，分别指向0级、1级和2级堆栈的栈顶，依次存放在TSS中偏移为4、12及20开始的位置。当发生向内层转移时，把适当的堆栈指针装入SS及ESP寄存器以变换到内层堆栈，外层堆栈的指针保存在内层堆栈中。没有指向3级堆栈的指针，因为3级是最外层，所以任何一个向内层的转移都不可能转移到3级。

但是，当特权级由内层向外层变换时，并不把内层堆栈的指针保存到TSS的内层堆栈指针区域。实际上，处理器从不向该区域进行写入，除非程序设计者认为改变该区域的值。这表明向内层转移时，总是把内层堆栈认为是一个空栈。因此，不允许发生同级内层转移的递归，一旦发生向某级内层的转移，那么返回到外层的正常途径是相匹配的向外层返回。

(3). 地址映射寄存器区域

从[虚拟地址](http://baike.baidu.com/view/1499823.htm)空间到线性地址空间的映射由GDT和LDT确定，与特定任务相关的部分由LDT确定，而LDT又由LDTR确定。如果采用[分页](http://baike.baidu.com/view/159980.htm)机制，那么由线性地址空间到物理地址空间的映射由包含页目录表起始物理地址的控制寄存器CR3确定。所以，与特定任务相关的虚拟地址空间到物理地址空间的映射由LDTR和CR3确定。显然，随着任务的切换，地址映射关系也要切换。 [Page]

TSS的地址映射寄存器区域由位于偏移1CH处的双字字段(CR3)和位于偏移60H处的字字段(LDTR)组成。在任务切换时，处理器自动从要执行任务的TSS中取出这两个字段，分别装入到寄存器CR3和LDTR。这样就改变了虚拟地址空间到物理地址空间的映射。

但是，在任务切换时，处理器并不把换出任务当时的寄存器CR3和LDTR的内容保存到TSS中的地址映射寄存器区域。事实上，处理器也从来不向该区域自动写入。因此，如果程序改变了LDTR或CR3，那么必须把新值人为地保存到TSS中的地址映射寄存器区域相应字段中。可以通过别名技术实现此功能。

(4). 链接字段

链接字段安排在TSS内偏移0开始的双字中，其高16位未用。在起链接作用时，地16位保存前一任务的TSS描述符的选择子。

如果当前的任务由段间调用指令CALL或中断/异常而激活，那么链接字段保存被挂起任务的 TSS的选择子，并且标志寄存器EFLAGS中的NT位被置1，使链接字段有效。在返回时，由于NT标志位为1，返回指令RET或[中断返回指令](http://baike.baidu.com/view/394324.htm)IRET将使得控制沿链接字段所指恢复到链上的前一个任务。

(5). 其它字段

为了实现输入/输出保护，要使用I/O许可位图。任务使用的I/O许可位图也存放在TSS中，作为TSS的扩展部分。在TSS内偏移66H处的字用于存放I/O许可位图在TSS内的偏移(从TSS开头开始计算)。关于I/O许可位图的作用，以后的文章中将会详细介绍。

在TSS内偏移64H处的字是为任务提供的特别属性。在80386中，只定义了一种属性，即调试陷阱。该属性是字的最低位，用T表示。该字的其它位置被保留，必须被置为0。在发生任务切换时，如果进入任务的T位为1，那么在任务切换完成之后，新任务的第一条指令执行之前产生调试陷阱