工作切換

進行工作切換

處理器在進行工作切換時，會進行很多步驟。簡單的說，大略是：

1. 檢查是否有權切換到目標工作。
2. 檢查目標工作的 TSS 是否正確。
3. 檢查目標工作是否可用（是否存在或是否忙碌）。
4. 設定或清除目前工作的相關旗標（包括 TSS descriptor 中的 B 旗標和 EFLAGS 中的 NT 旗標）。
5. 將目前的狀態存放到目前的 TSS 中。
6. 設定或清除新工作的相關旗標（包括 TSS descriptor 中的 B 旗標、TSS 中的 CR0 的 TS 旗標、和 EFLAGS 中的 NT 旗標）。
7. 將新工作的 TSS descriptor 載入到 TR 中。
8. 載入新工作的 TSS 中存放的狀態。
9. 開始執行新工作。

如果新工作是由 CALL 指令、或是中斷 / 例外產生的，則新工作會記錄上一個工作的位址，而且上一個工作的 B（忙碌）旗標也不會被清除（若使用 JMP 指令跳到新工作中，則舊工作的 B 旗標會被清除）。而且處理器會將 EFLAGS 中的 NT（Nested-task）旗標設為 1，表示目前是在「巢狀」的工作中。當工作使用 IRET 離開時，處理器會從 TSS 中取出上一個工作的位址，回到上一個工作。如果是用 JMP 指令執行新工作，則 NT 旗標會被設為 0。
因為一個工作只有一份 TSS，所以工作是不能遞迴呼叫的（否則會破壞 TSS 中原先存放的資料）。處理器利用 B 旗標來判斷是否有遞迴呼叫一個工作。因此，當工作一直連結下去時（例如，工作 A 呼叫工作 B ，工作 B 又呼叫工作 C ），就可以避免連結中的任何一個工作又被呼叫一次，而導致錯誤。