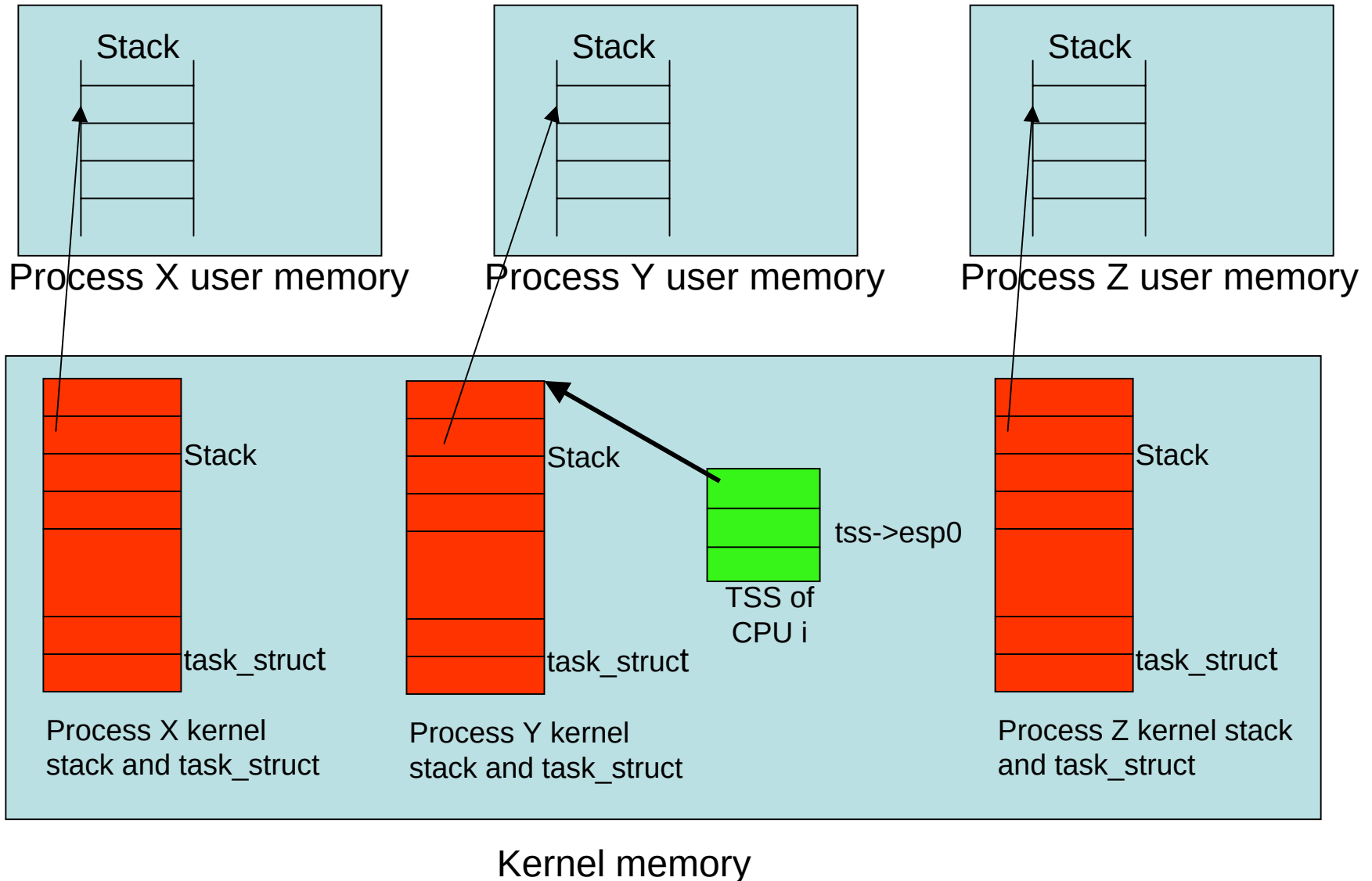
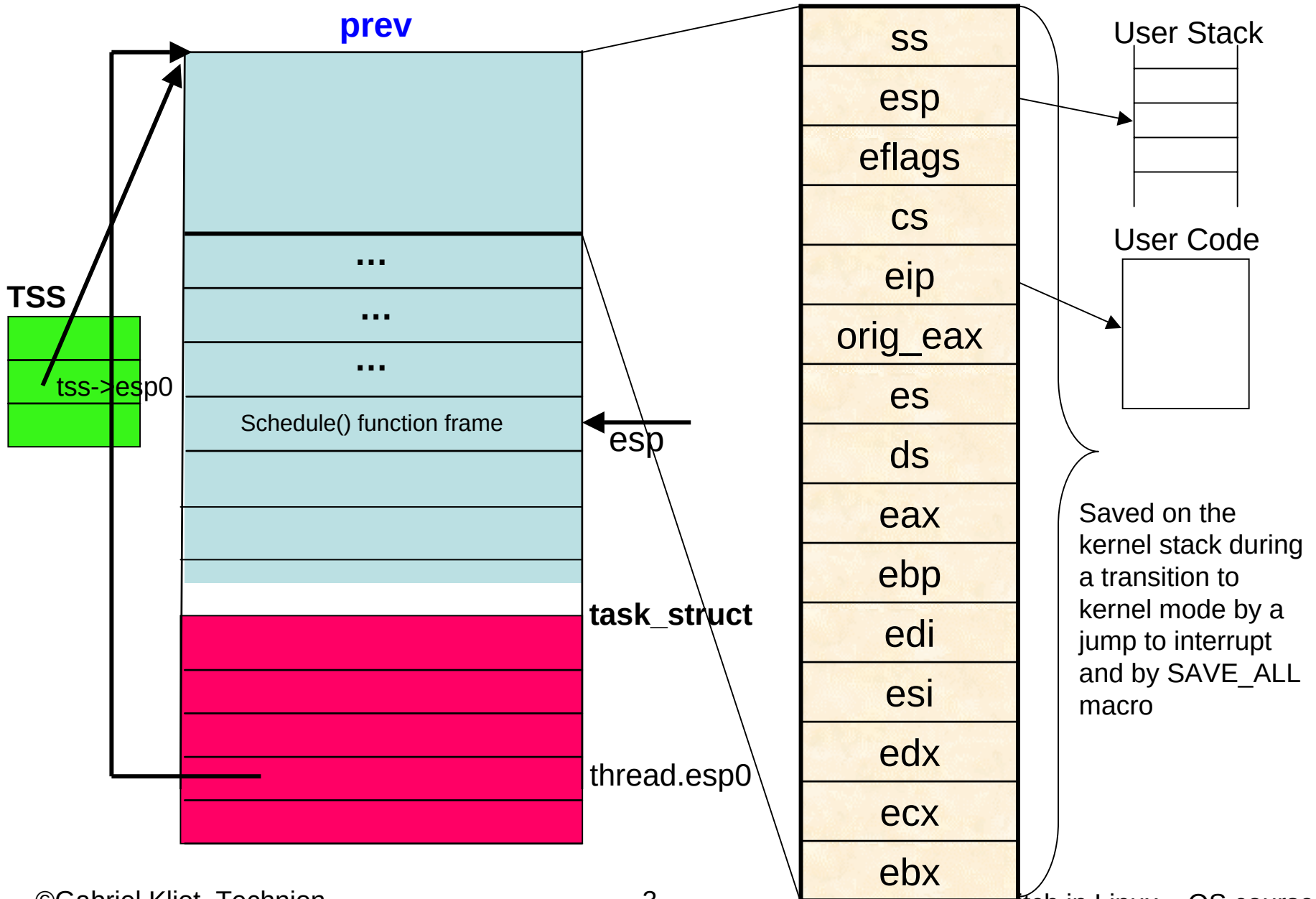


Context switch in Linux

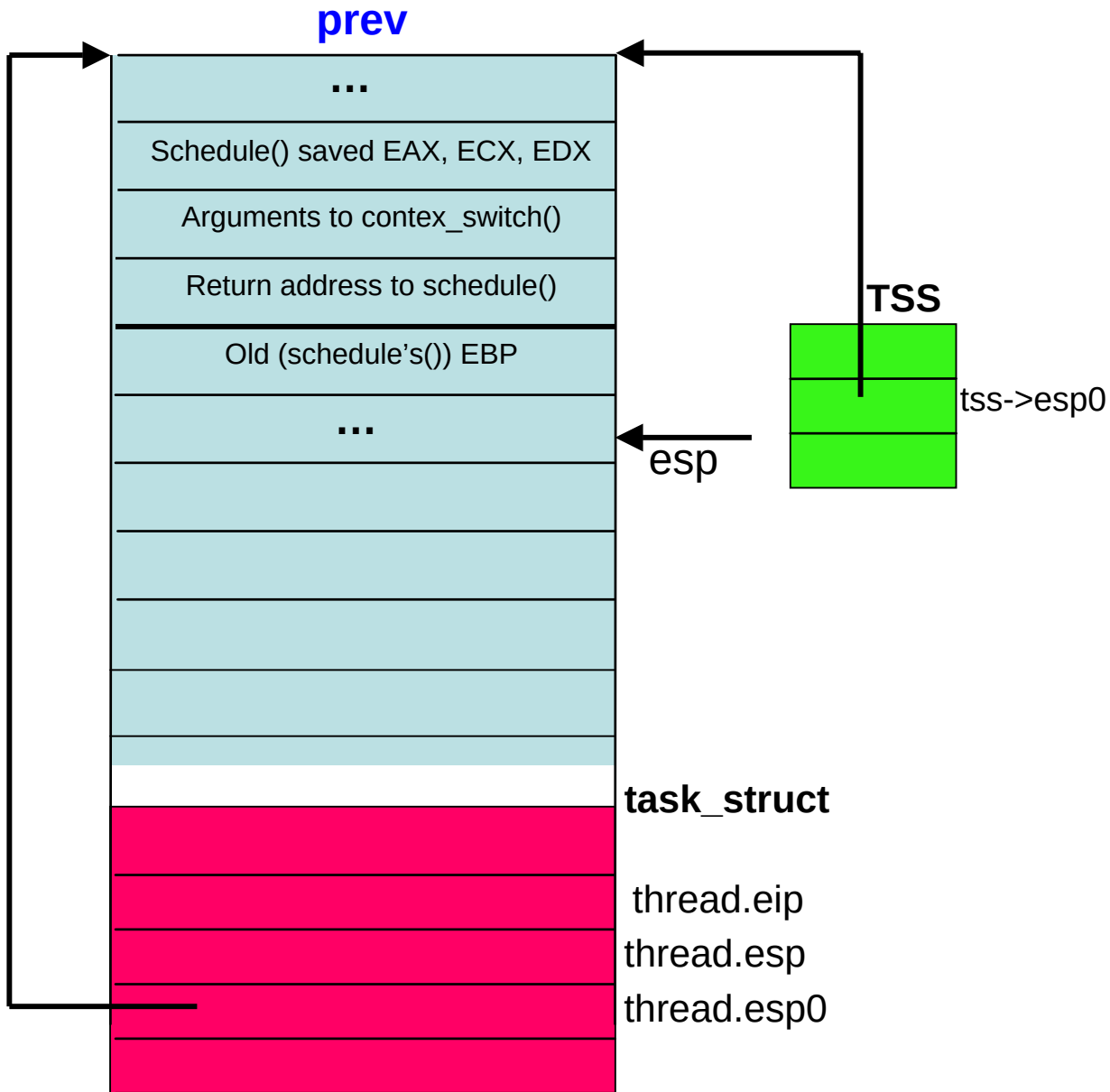
Memory layout – general picture



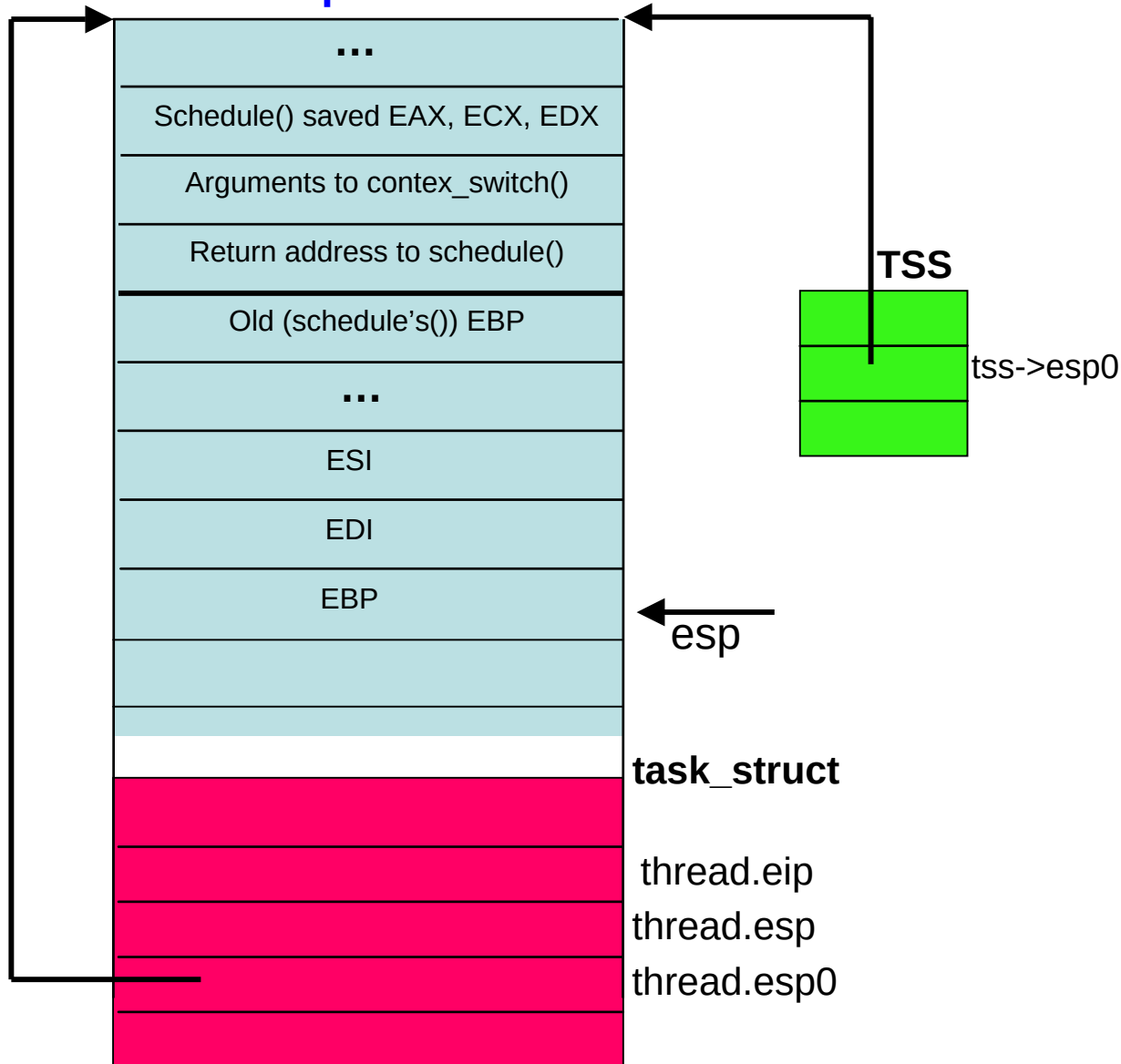
#1 – kernel stack after any system call, before context switch



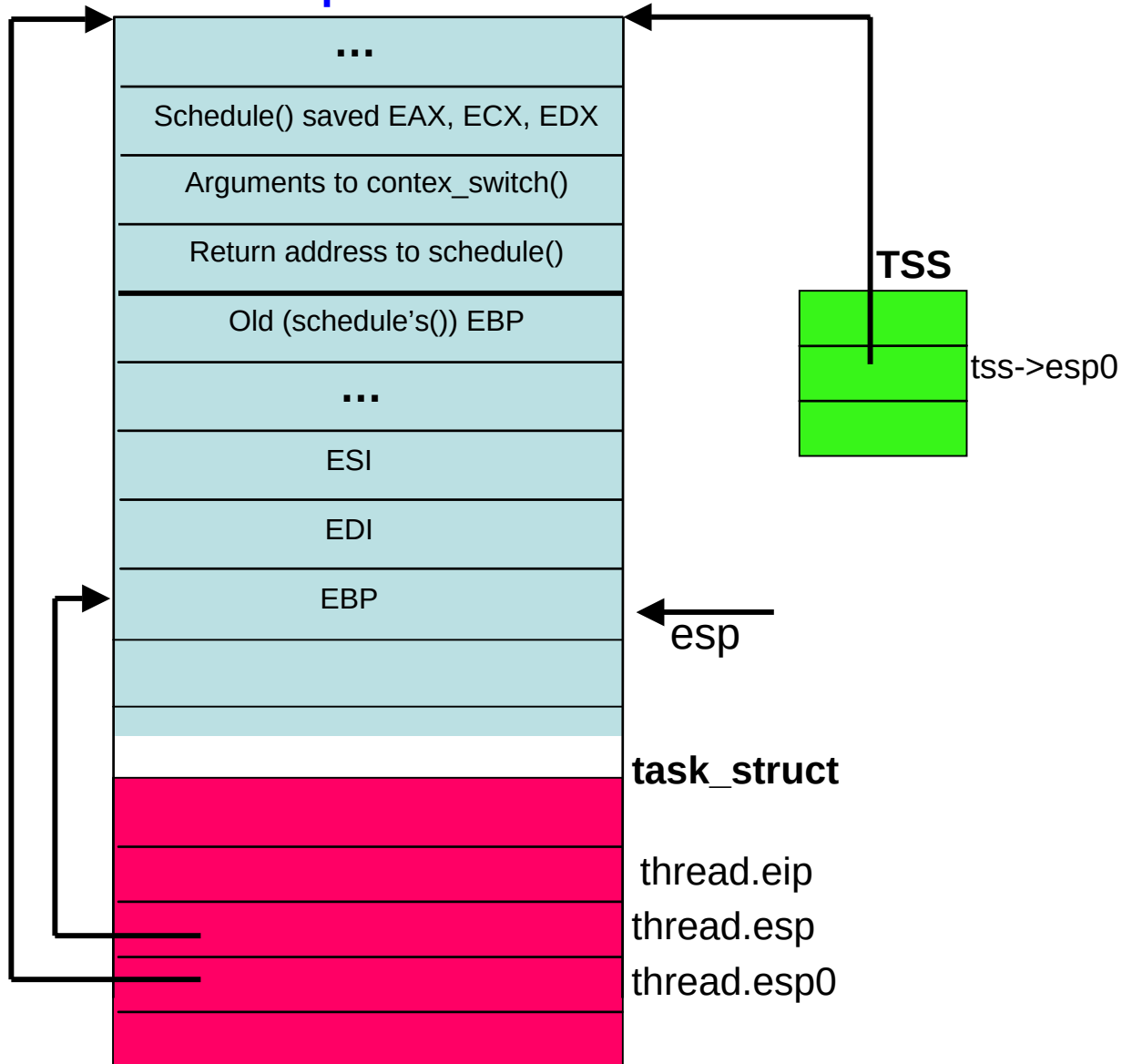
#2 – stack of prev before switch_to macro in schedule() func



#3 – switch_to: save esi, edi, ebp on the stack of prev



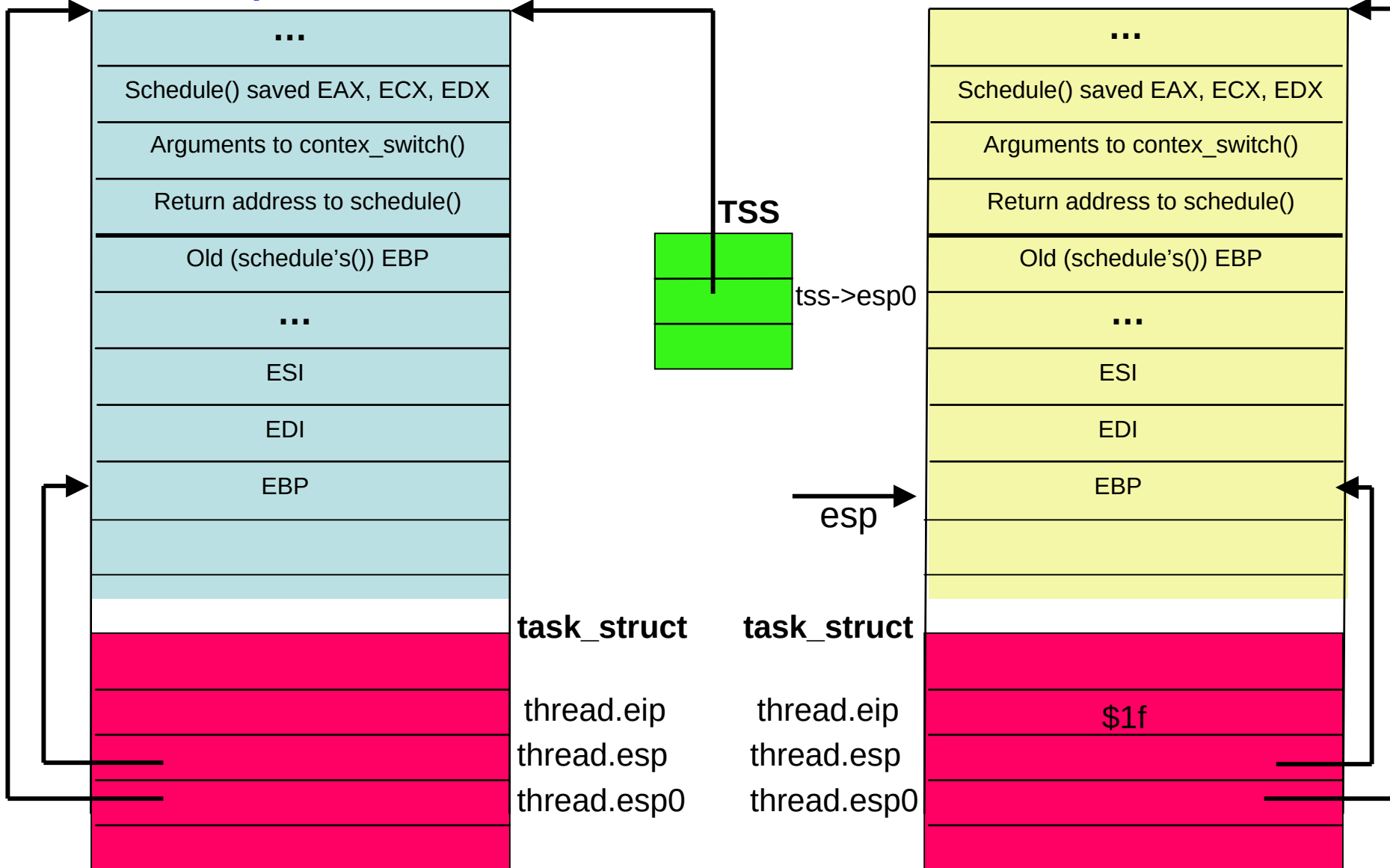
#4 – switch_to: save esp in prev->thread.esp



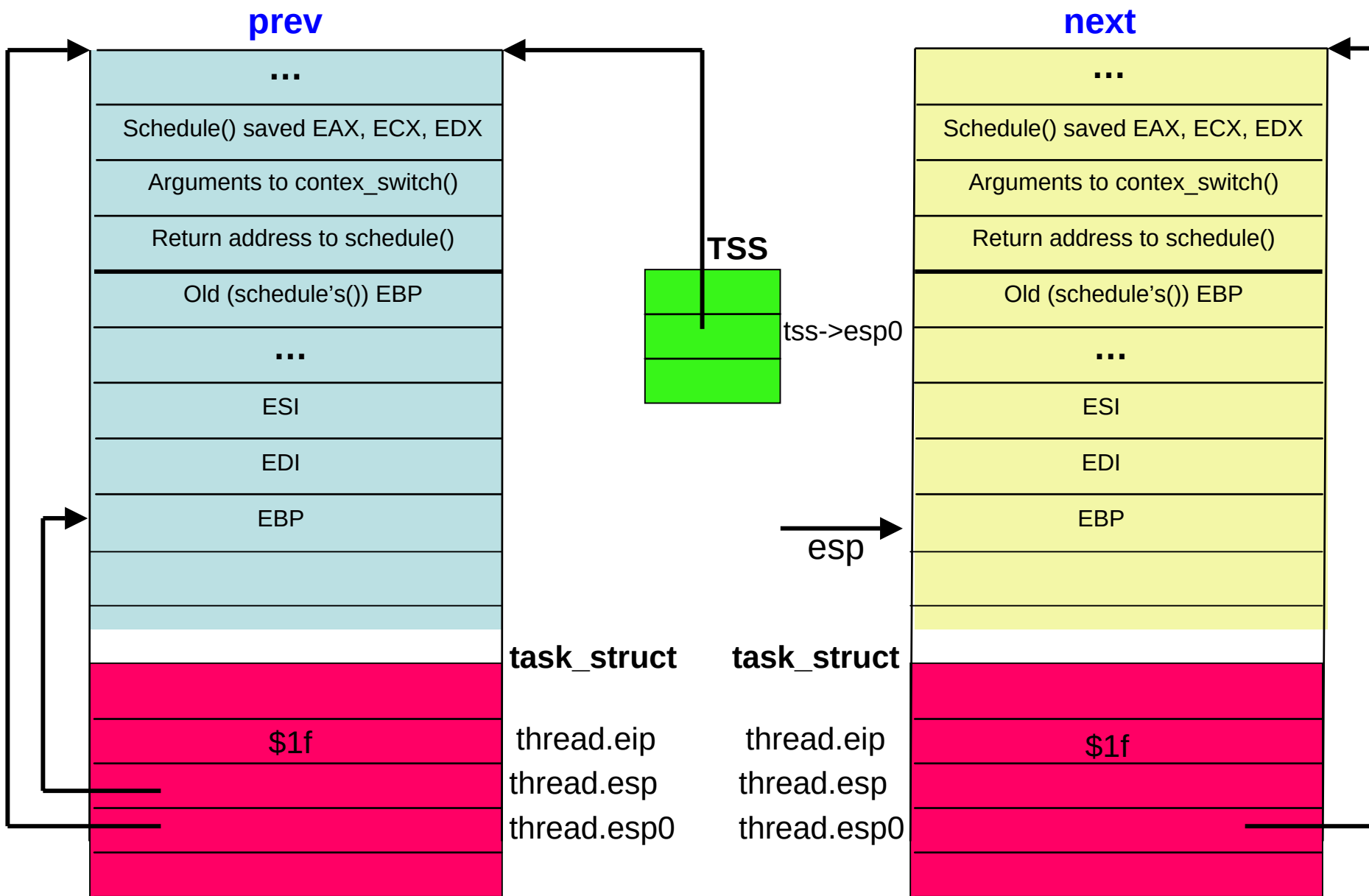
#5 – switch_to: load next->thread.esp into esp

prev

next



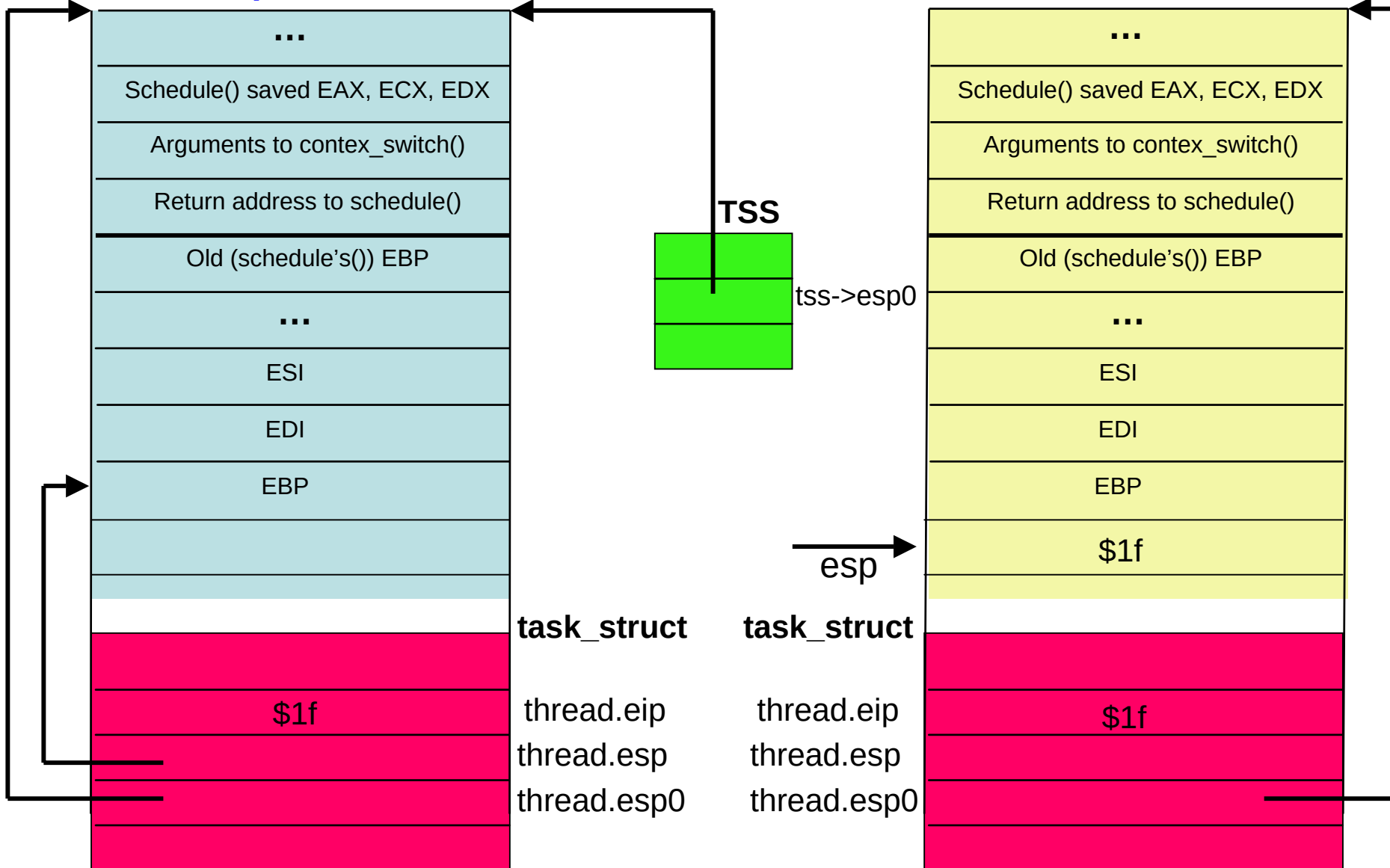
#6 – switch_to: save return address in the prev->thread.eip



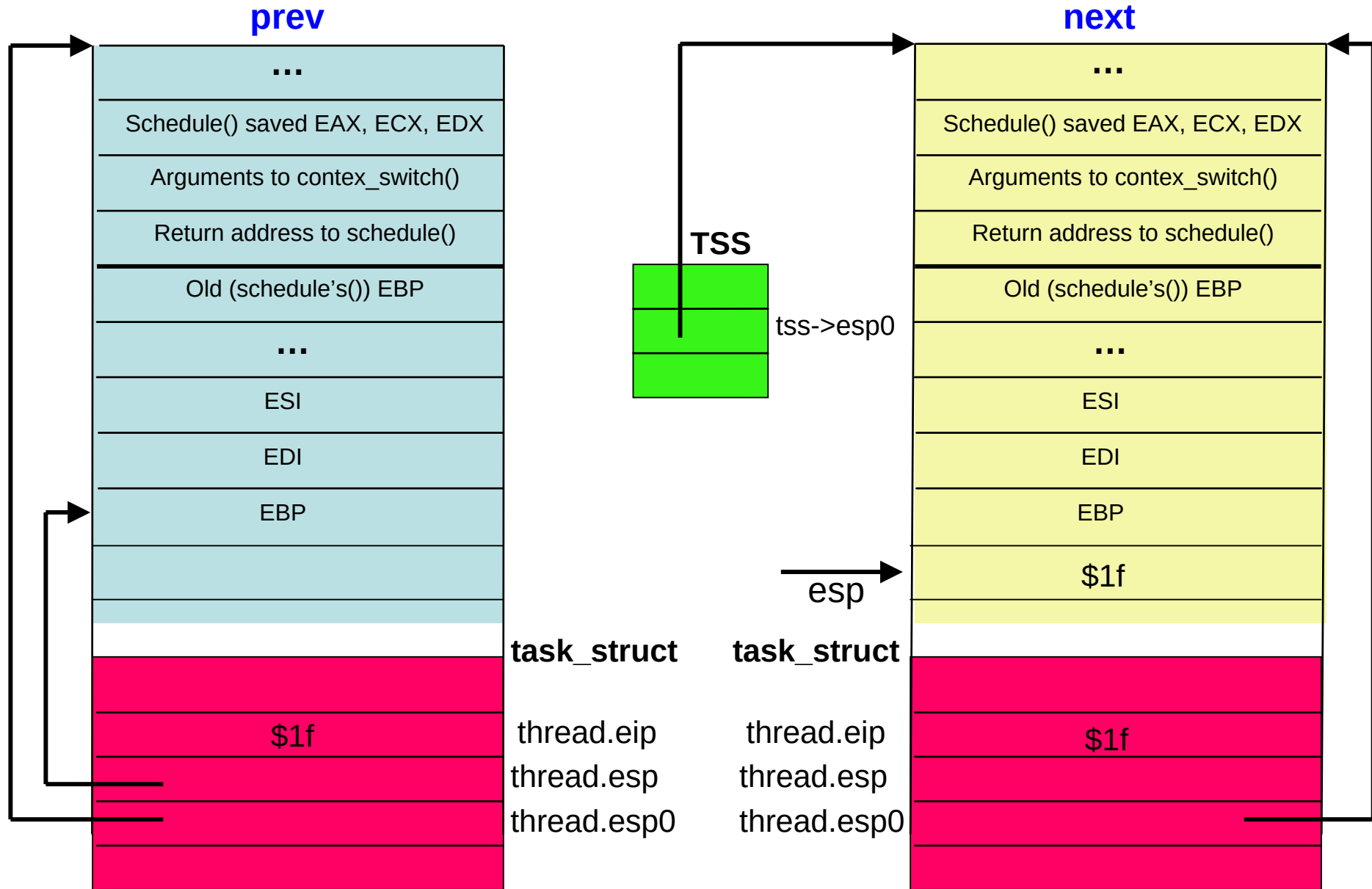
#7 – switch_to: save return address on the stack of next

prev

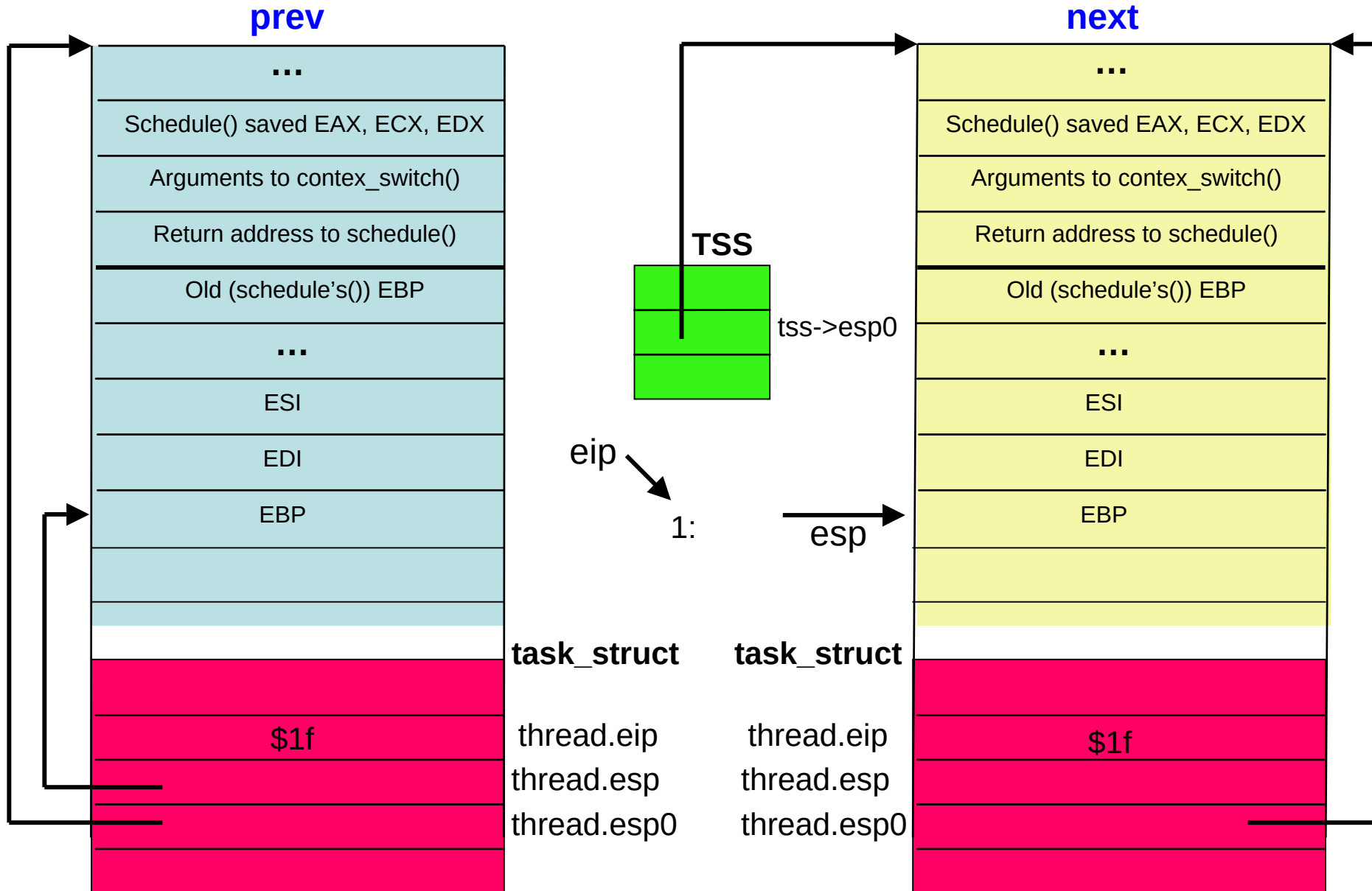
next



#8 – __switch_to func: save the base of next's stack in TSS



#9 – back in switch_to: eip points to \$1f instruction label



#10 – switch_to: restore esi, edi, ebp from the stack of next

prev

next

