

```

1 Handout for CS 372H
2 Class 8 (by video)
3 12 February 2010
4
5 Per-thread state in thread control block:
6
7     typedef struct tcb {
8         unsigned long esp;      /* Stack pointer of thread */
9         char *t_stack;          /* Bottom of thread's stack */
10        /* ... */
11    };
12
13 Machine-dependent thread-switch function:
14
15     void switch(tcb *current, tcb *next);
16
17 Machine-dependent thread initialization function:
18
19     void thread_init(tcb *t, void (*fn) (void *), void *arg);
20
21 Implementation of switch(current, next):
22
23     pushl %ebp; movl %esp,%ebp      # Save frame pointer
24     pushl %ebx; pushl %esi; pushl %edi # Save callee-saved regs
25
26     movl 8(%ebp),%edx              # %edx = current
27     movl 12(%ebp),%eax            # %eax = next
28     movl %esp,(%edx)              # %edx->esp = %esp
29     movl (%eax),%esp              # %esp = %eax->esp
30
31     popl %edi; popl %esi; popl %ebx # Restore callee saved regs
32     popl %ebp                     # Restore frame pointer
33     ret                           # Resume execution
34
35 [thanks to David Mazieres]
36

```