

Context Switch: Process A → Process B

BEFORE (Process A Running) DURING (Kernel Context Switch) AFTER (Process B Running)

Ring 3: User Process A

Ring 0: Kernel Code

Ring 3: User Process B

EIP: 0x0804abcd

ESP: 0xbffff800

CR3: 0x01000000

EAX: 42 SAVE

EBX: 100

... (all other registers)

Virtual Memory

Code at 0x0804xxxx

Stack at 0xbffffxxx

(mapped by

~~CR3=0x10000000~~)

Ring 0: Kernel Code

switch_to_user():
pick_proc() → proc_table[B]
arch_finish_switch...

proc_table[A]

EIP: 0x0804abcd

ESP: 0xbffff800

CR3: 0x01000000

EAX: 42

EBX: 100

... (all state)

proc_table[B]

EIP: 0x0805ffee

ESP: 0xbffffe000

CR3: 0x02000000

EAX: 1337

EBX: 999

... (all state)

EIP: 0x0805ffee

ESP: 0xbffffe000

CR3: 0x02000000

LOAD

EAX: 1337

EBX: 999

... (all other registers)

CPU Operation:

mov 0x02000000, %eax

mov %eax, %cr3

+ **TLB FLUSH**

Virtual Memory

Code at 0x0805xxxx

Stack at 0xbffxxxx

(mapped by

CR3=0x20000000)

CPU Registers Changed:

- CR3: 0x10000000 → 0x20000000
- EIP: kernel → 0x0805ffee
- ESP: kernel → 0xbffffe000
- All GPRs swapped
- All segments reloaded
- **TLB flushed (CR3 write)**