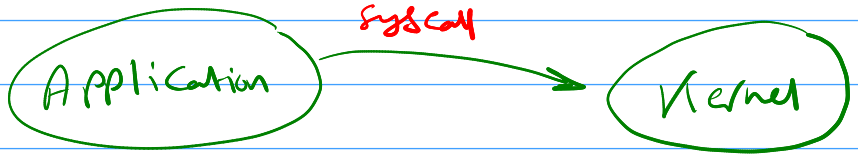
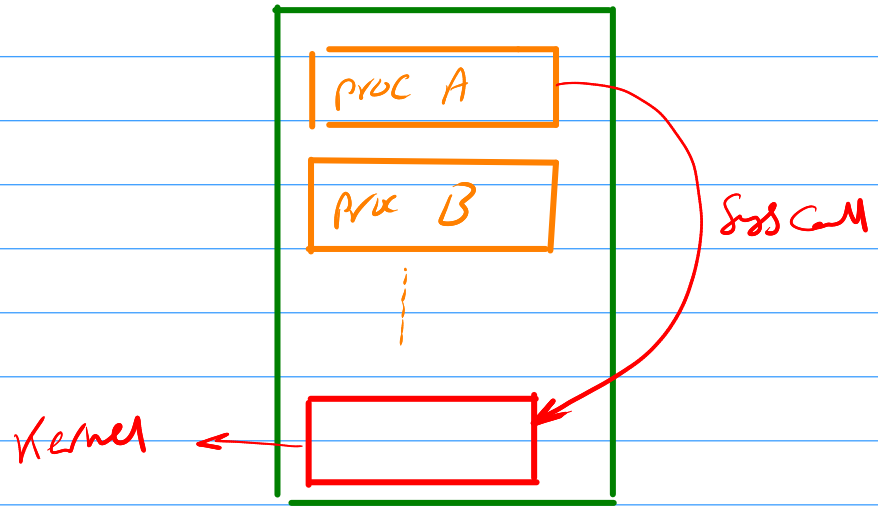
* System Calls *

* Definition:

→ System call is an entry point into the Linux Kernel





→ Basically, it is just functions in OS code which programs can invoke using special instructions

* C library wrapper functions

→ Each SysCall has a C lib wrapper function that the program can use when needing.

→ What the wrapper functions do?

1- copying args & the unique sys call number to the registers where the kernel expects them

2- trapping to the kernel mode (starting the syscall)

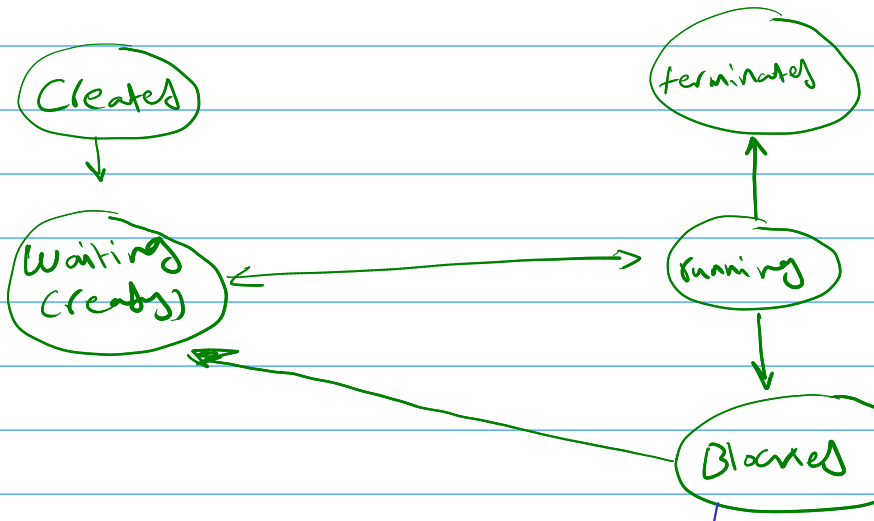
3- setting errno if there is an error when returning the CPU to user mode.

*Note: sometimes the wrapper function do extra work, like preprocessing the args.

※ Scheduling and Context Switching:

→ A stack frame is generated for sysCall in the program (process) space ∴ avoiding context switching (uses inline functions)

→ system calls can be interrupted when suspending a process



↳ Can happen when system call needs to read a device (serial port)

* CPU modes:

→ CPU implements different protection levels
→ Linux will use the lowest and the highest levels for the user space and the Kernel space respectivily

* tracing the System Calls:

→ Linux provides strace tool to debug the system calls