SYSENTER Syscall Path (Intel Fast)

Boot: Setup MSRs (CS, ESP, EIP)

User: Setup EDI (call type), EAX, EBX, ECX

No automatic stack save!
User manages ESP/EIP save

User: Save ESP→ESI, return EIP→EDX

Execute `SYSENTER`

CPU: Load CS from IA32_SYSENTER_CS

CPU: Load EIP from IA32_SYSENTER_EIP

CPU: Load ESP from IA32_SYSENTER_ESP

Kernel:
Minimal state management via MSRs

CPU: Set CPL=0, disable interrupts

Cost: ~1305 cycles
(Skylake, Linux)
Faster than INT

`ipc_entry_sysenter` (mpx.S:220)

Get EBP from stack (proc ptr)

Set P_KERN_TRAP_STYLE = KTS_SYSENTER

SYSEXIT:
Fast return via EDX/ECX

`syscall_sysenter_common` (mpx.S:240)

Save ESI→SPREG, EDX→PCREG

Check EDI: IPCVEC or KERVEC?

Jump to `ipc_entry_common`

Call `do_ipc()`

`restore_user_context_sysenter` (mpx.S:391)

Load PCREG→EDX, SPREG→ECX

Load return values→EAX, EBX

Restore EFLAGS, `STI`

Execute `SYSEXIT`

CPU: Load EIP←EDX, ESP←ECX

CPU: Set CPL=3, enable interrupts

User: Resume execution