Triple Fault

From OSDev Wiki

> Things never to do in an OS #1: Swap out the page swapping code (triple-fault here we come)
>
> —Kemp

Causes

When a fault occurs, the CPU invokes an exception handler. If a fault occurs while trying to invoke the exception handler, that's called a double fault, which the CPU tries to handle with yet another exception handler. If that invocation results in a fault too, the system reboots with a triple fault.

Note that a fault that occurs while a fault handler is already running does not of itself cause a double or triple fault. For example, if a Segment Not Present Fault occurs after a handler has already started, then the Segment Not Present handler will run as normal. However, if the code segment of the original handler is itself not Present, then the double (or triple) fault would occur since the original handler hadn't started yet.

A triple fault is usually a sign that the exception handler called is faulty, or worse, that the whole exception handling in your system is screwed up. (LDT or GDT issues, bogus pointers or faulty memory mappings are frequent offenders.)

Another frequent cause of triple faults is a kernel stack overflow. If the stack reaches an invalid page (one with its present bit clear), a page fault is generated. However, the CPU faults while trying to push the exception information on to the stack, so a double fault is generated. The same problem still exists so a triple fault is generated.

Avoiding

The cleanest way to handle this is to provide a separate TSS for double faults and to use a task gate for that kind of exception. Try to keep that Task as simple as possible, and give it a dedicated stack segment and pointers.

- display "double fault" panic message
- try to get the "faulty status" from the backlinked TSS
- display that status (registers, etc)
- halt.

There's virtually no way to resume from a double fault. At least it will give you the opportunity of checking system status before it resets.

On the AMD64/Intel EM64T architecture, task gates are not valid in 64-bit long mode. The same effect can be achieved through the Interrupt Stack Table bits in the IDT entry. See the Intel manuals for more information.

Retrieved from "http://wiki.osdev.org/index.php?title=Triple_Fault&oldid=16538"

Category: Interrupts

- This page was last modified on 16 July 2014, at 23:58.
- This page has been accessed 14,850 times.