第 2 章 操作系统的硬件基础

月出皓兮　苏曙光老师的课堂笔记

2022 年 3 月 5 日

支持操作系统最基本的硬件结构为 CPU，内存，中断和时钟。

目录

1 计算机三总线硬件结构

1.1 计算机主要部件

CPU、内存和外设。外设往往需要通过 IO 接口才能连接到总线上。

1.2 三总线

地址总线，数据总线和控制总线。

1.3 CPU 的结构

CPU 由控制单元，运算单元，寄存器单元组成。其功能是按一定逻辑流程分析和执行指令流。（指令流已存放至内存中）

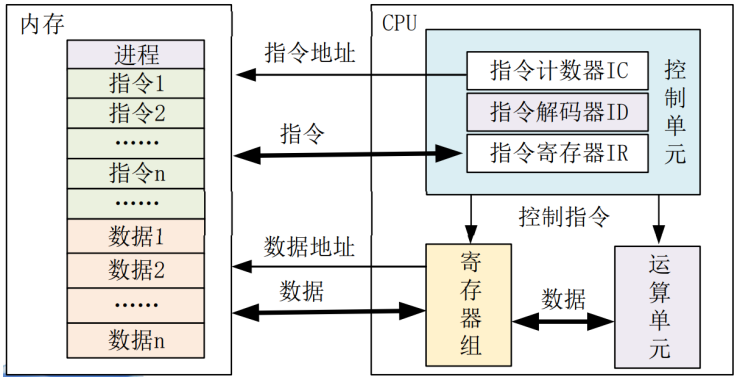

图 1: CPU 的结构与内存的连接

2 CPU 的态系统

2.1 目的

为 CPU 设定态的根本目的在于为系统建立安全机制，禁止程序在非授权情况下非法访问或越权访问不属手于自己的数据或资源。

通过态来支持对可信程序和非可信程序的区分。可信程序能对系统的安全机制进行设置和修改，使用普通指令集和特权指令集。非可信程序只能

使用普通指令集。其中特权指令包括涉及外部设备的输入/输出指令，修改特殊寄存器的指令，改变机器状态的指令。

态也为计算机系统的资源访问设置了访问屏障。

2.2 CPU 态的定义

即 CPU 的工作状态，对资源和指令使用权限的描述。

2.3 态的分类

2.3.1 核态 (Kernel mode)

能够访问所有资源和执行所有指令，具有最高的特权级别，管理程序/OS 内核一般为核态程序。

2.3.2 用户态 (User mode, 目态)

仅能访问部分资源，其它资源受限。用户程序为用户态程序。

2.3.3 管态 (Supervisor mode)

介于核态和用户态之间

2.4 态的转换

2.4.1 用户态向核态转换

用户请求 OS 提供服务。
用户进程产生错误（内部中断。
外部设备的中断。
用户态企图执行特权指令。
可以总结说，从用户态向核态转变的唯一方法就是中断。

2.4.2 核态向用户态转换

一般是中断返回：IRET.

2.5 硬件支持

CPU 设置模式位，表明当前的状态。
指令执行前增加“权限状态是否满足”的条件判断。
Intel CPU 的相关机制
1. 保护模式（CR0 的 PE 位,PG 位）
2. CPL（当前特权级）
3. 地址映射机制
4. 权限核验 (DPL+RPL+CPL)

2.6 Intel CPU 的态

2.6.1 PL(Privilege Level)

Ring 0 – Ring 3 （Ring 0 最核心，Ring 3 最外层）
Unix/Linux/Windows OS: 仅用到了 Ring 0 和 Ring 3

2.6.2 DPL：描述符特权级 (Descriptor Privilege Level)

段描述符 Descriptor，8 个字节，其中包括段基址，段界限，段属性（段类型，访问该段所需最小特权级，是否在内存）

2.6.3 当前特权级 CPL：Current Privilege Level

2.6.4 请求特权级 RPL：Requested Privilege Level

2.6.5 程序段 A 访问程序段 B 时的权限检查（态）

一致代码段：CPL >= DPL
非一致代码段：CPL = DPL 并且 RPL <= DPL

3 中断机制

3.1 中断的定义

指 CPU 对突发的外部事件的反应过程或机制。

CPU 收到外部信号（中断信号）后，停止当前工作，转去处理该外部事件，处理完毕后回到原来工作的中断处（断点）继续原来的工作。

3.2 目的

实现并发活动
实现实时处理
故障自动处理

3.3 相关概念

3.3.1 中断源

引起系统中断的事件称为中断源

3.3.2 终端类型

强迫中断和自愿中断
- 强迫中断：程序没有预期：例：I/O、外部中断
- 自愿中断：程序有预期。例：执行访管指令

外中断（中断）和内中断（俘获）
- 外中断：由 CPU 外部事件引起。例：I/O，外部事件。
- 内中断：由 CPU 内部事件引起。例：访管中断、程序中断

外中断又可分为不可屏蔽中断和可屏蔽中断。
- 不可屏蔽中断：中断的原因很紧要，CPU 必须响应
- 可屏蔽中断：中断原因不很紧要，CPU 可以不响应

3.3.3 断点

程序中断的地方，将要执行的下一指令的地址
包含 CS:IP （FLAGS、SS、SP）

3.3.4 现场

程序正确运行所依赖的信息集合。
包含 PSW（程序状态字）、相关寄存器、断点
现场保护：进入中断服务程序之前：CPU→ 栈
现场恢复：退出中断服务程序之后：栈 →CPU

3.3.5 中断处理程序

处理中断源中断事件的程序称为中断服务程序。中断服务程序是事先已准备好的一个特殊函数，该函数的调用由系统自动完成。

3.3.6 中断向量表

中断服务程序的入口地址用段基址（Segment）和段偏移（Offset）两个参数记录，称之为中断向量。

3.4 中断响应过程

- 识别中断源
- 保护断点
- 保护现场
- 进入中断服务程序
- 恢复现场
- 中断返回

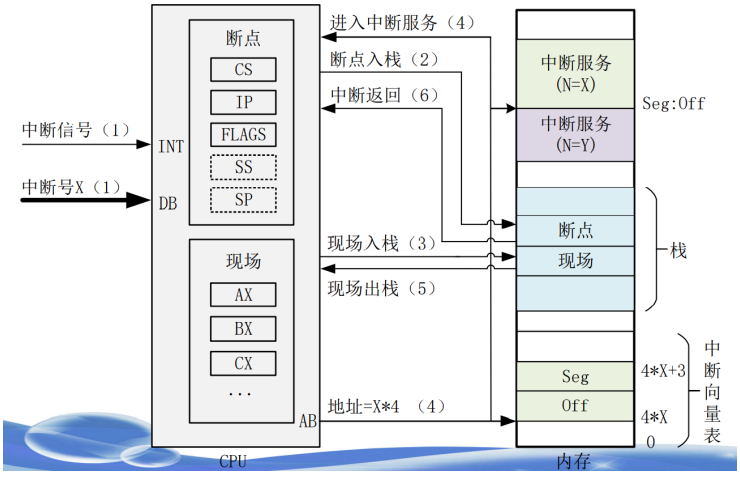

图 2: 中断响应过程

在保护模式下发生中断的时候可能涉及特权级的变化。中断发生时，如果代码在相同特权级间跳转时，则堆栈不变; 若在不同特权级间跳转，则会用到两个不同的堆栈。

3.5 中断响应的实质

交换指令执行地址。

交换 CPU 的态。

实现了现场保护和恢复与参数传递（通信）。