x86内存架构

- 地址空间
  - 物理地址空间
  - 线性地址空间

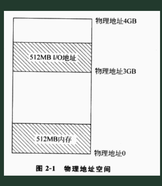

图 2-1 物理地址空间

图 2-2 线性地址空间构造

- 地址
  - 逻辑地址
  - 线性地址
  - 物理地址
- x86内存管理机制
  - 分段机制
    分段机制是IA32架构CPU的特色，并不是操作系统寻址方式的必然选择。
    Linux为了跨平台，巧妙的绕开段机制，主要使用分页机制来寻址。
  - 分页机制
  - TLB

x86架构的基本运行环境

- 三种基本模式
  - 实模式
    当CPU加电并经历最初的混沌状态后，首先进入的就是实模式，它是早期的Intel 8086处理器的工作模式。
    操作系统或BIOS通常在该模式下准备必要的数据结构和初始化关键的寄存器，然后切入保护模式。
  - 保护模式
    操作系统运行时最常用的模式
  - 虚拟8086模式
    为了使早期的8086程序能在保护模式下运行，x86提供了虚拟8086模式
- 基本寄存器组
  - 通用寄存器
  - EFLAGS寄存器
  - EIP寄存器
  - 浮点运算寄存器
  - 控制寄存器
- 权限控制
  - 段保护
  - 页保护

中断和异常

中断提供给外部硬件设备一种"打断CPU当前任务，并响应自身服务"的手段

- 中断架构
  - 可编程中断控制器
    中断从设备发送到CPU需要由被称为"中断控制器"的部件转发（MSI除外）
  - PIC
    8259A芯片
  - APIC
    PIC可以在UP(单处理器)平台上运行，但无法用于MP(多处理器)平台。为此，APIC应运而生
  - 处理器间中断
    Inter-processor Interrupt(IPI)，操作系统通常使用IPI来完成诸如进程转移、中断平衡和TLB刷新等工作
- 中断的重要概念
  - 中断的分类
    - 外部中断
      指连接在IOAPOC上的设备产生的中断、LAPIC上连接的设备或LAPIC内部中断源产生的中断以及处理器间中断
    - 软件产生中断
      通过INT n指令产生的中断
  - 中断的优先级
  - 中断的屏蔽
  - IDT表
    IDT表实际就是个大数组，用于存放各种"门"（中断门、陷阱门），这些"门"是中断和异常通往各自处理函数的入口。
    当一个中断或异常发生时，CPU用它们对应的vector号索引IDT表以获得对应的"门"。
  - 中断门
    "门"是入口，中断门就是中断的入口
- 异常架构
  - 错误(Fault)
    由某种错误情况引起，一般可以被错误处理程序纠正
  - 陷阱(Trap)
    Linux中用于实现系统调用的INI 80指令就是属于此类
    和中断相比，异常最大的不同在于它是在程序的执行过程中同步发生的
  - 终止(Abort)
    指严重的不可恢复的错误，将导致程序终止的异常
- 操作系统对中断/异常的处理流程
  MSI(新的中断方式)

进程

- 上下文
  在上下文切换时必须更改的寄存器的集合
- 上下文切换
  上下文切换是指程序从一种状态切换到另一种状态（例如用户态切换到内核态），
  或从一个程序切换到另一个程序（例如进程切换）时，导致上下文相关寄存器的变化行为
  - 用户态到内核态的切换
  - 进程切换
  - 到中断上下文的切换

I/O架构

- x86的I/O架构
  - Port I/O
    通过I/O端口访问设备寄存器
    I/O端口地址空间是独立的，也就是说它并不是线性地址空间或物理地址空间的一部分
  - MMIO
    通过内存访问的形式访问设备寄存器或设备RAM
    MMIO要占用CPU的物理地址空间
- DMA
  - 同步DMA
    DMA操作由软件发起
  - 异步DMA
    DMA操作由设备发起
- PCI设备
  - PCI总线架构

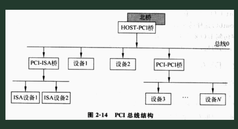

图 2-14 PCI 总线结构

  - 设备标识符
    设备标识符可以看作是设备在PCI总线上的地址
  - PCI配置空间
  - PCI设备枚举过程

图 2-17 PCI 设备的枚举

- PCI Express
  - PCI Express架构

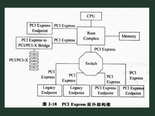

图 2-18 PCI Express 组件结构图

  - PCI Express的优点

时钟

- x86平台的常用时钟
- 操作系统的时钟观
  - 提供统计值及驱动事件
  - 维护定时器

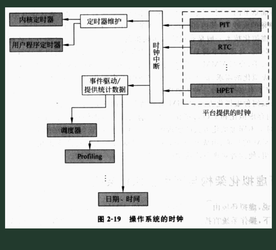

图 2-19 操作系统的时钟