系统虚拟机

printf 的生死因果

李思阳

国防科学技术大学
计算机学院

第 x 讲：系统虚拟机

目的与要求

- 了解系统虚拟机的定义
- 了解系统虚拟机的分类
- 了解 Intel-VT 硬件辅助虚拟化技术
- 学习一种虚拟机软件

重点与难点

- CPU 的虚拟化
- 内存的虚拟化
- I/O 的虚拟化

国防科学技术大学

为何要虚拟化

解决软件的兼容性和运行性能的问题

虚拟化级别	软件	兼容性	性能
应用程序	Java 虚拟机	★★☆	★★☆
函数库	Wine	★★☆	★★☆
操作系统	容器	★☆☆	★★★
硬件	系统虚拟机	★★★	★★☆
指令	指令模拟器	★★★	☆☆☆

系统虚拟机的发展历程

1998 年 VMware 公司成立，实现了在操作系统上运行操作系统

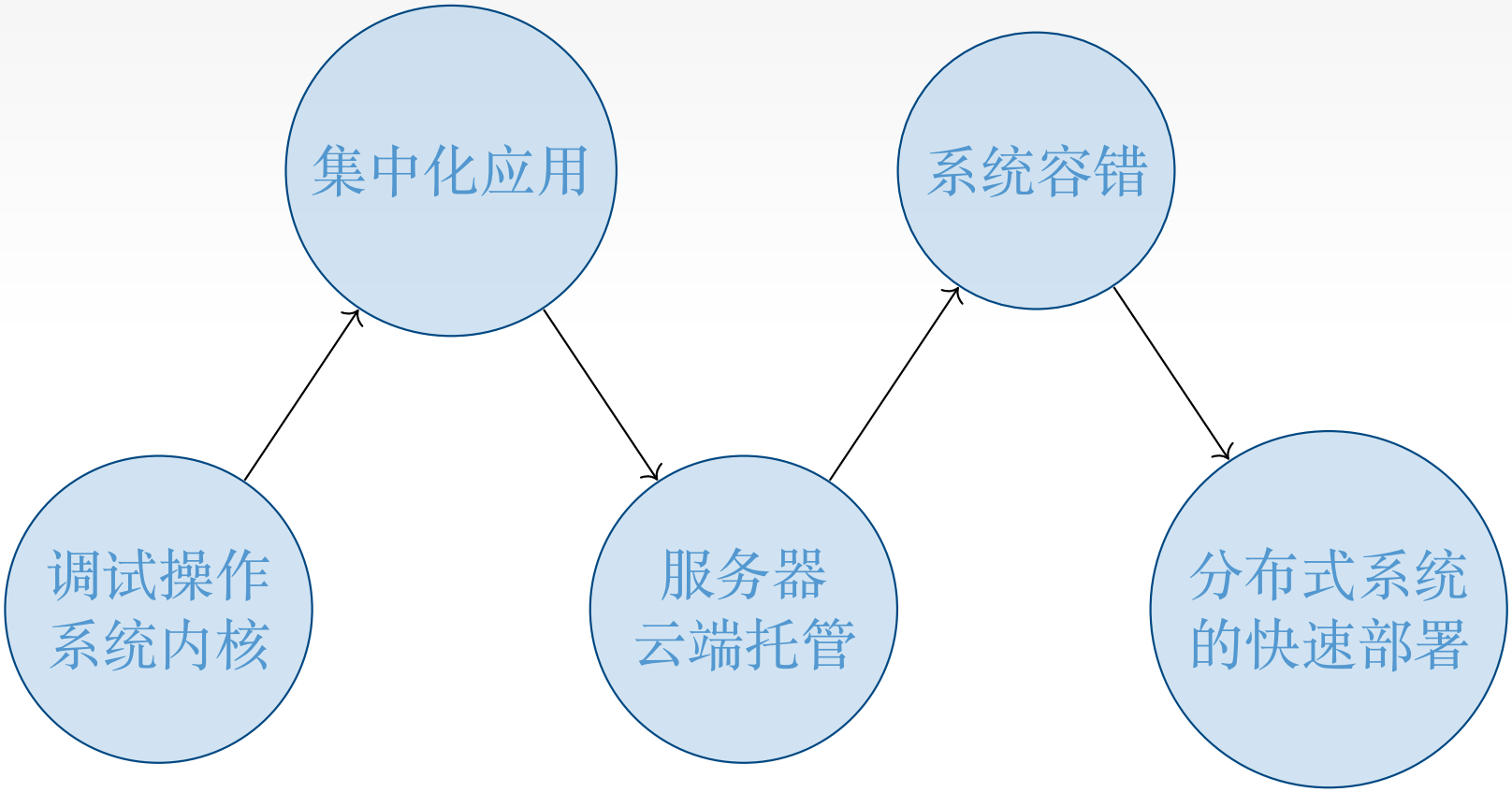
1999 年 Xen 进入开发阶段，虚拟机系统开源

2006 年 Intel 开发了硬件辅助虚拟化技术 VT

2007 年 基于硬件辅助虚拟化的虚拟机 KVM 进入 Linux 内核

2010 年 OpenStack 项目开源，虚拟机进入云时代

虚拟机的应用场景



系统虚拟机的基本概念

Hypervisor（系统管理程序）

- 又称为虚拟机监管器（virtual machine monitor，VMM）

主机（Host）

- 运行 Hypervisor 的物理机

客户机（Guest）

- 又称为虚拟机（virtual machine，VM）

国防科学技术大学

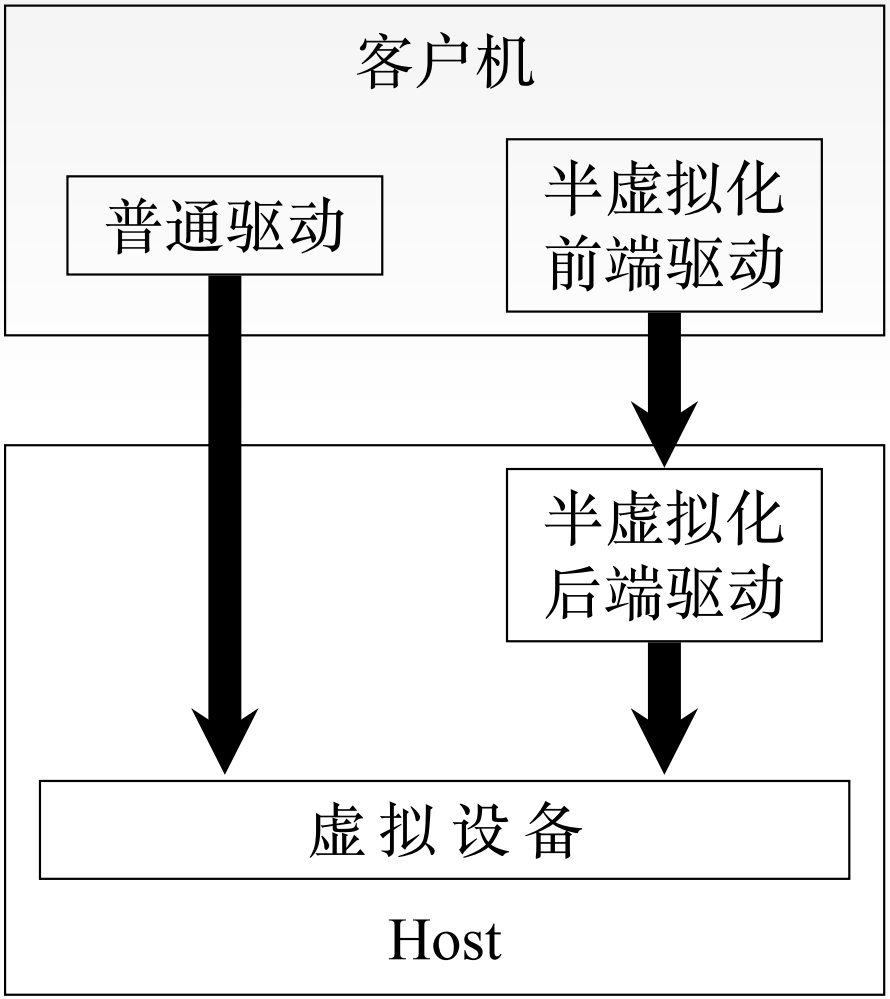
分类：按驱动类型分

全虚拟化

- 操作系统可以不经过修改直接在虚拟机上运行

半虚拟化

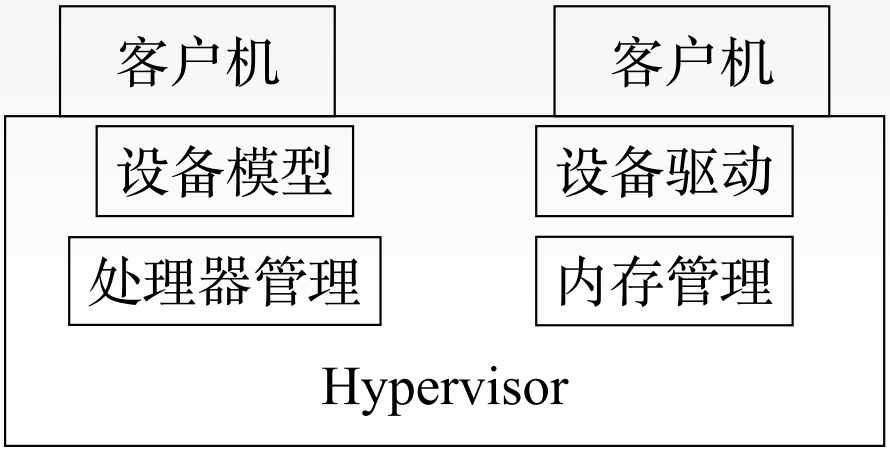
- 需要修改操作系统的部分代码才可以运行
- 提高运行效率，提供特殊功能



分类：安装方式

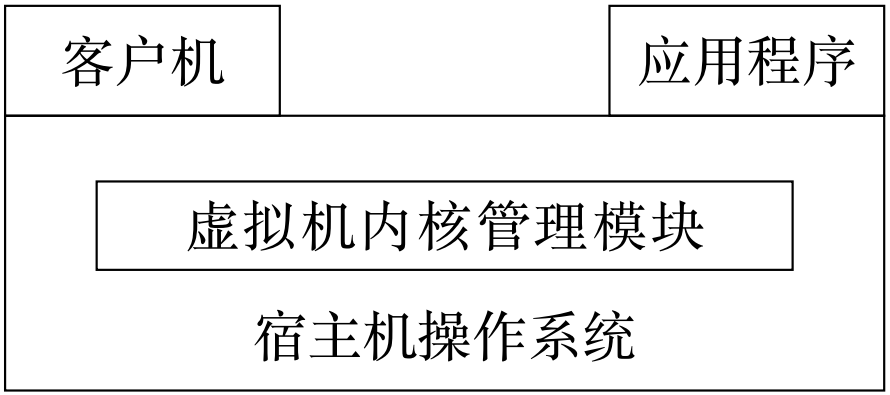
Hypervisor 模型

- 在物理机上直接安装 VMM
- VMM 需要提供完整的系统管理方案



宿主机模型

- 在物理机操作系统之上安装 VMM
- 利用操作系统的部分管理机制



国防科学技术大学

分类：按照应用类型

服务器虚拟化

- 虚拟机上运行的系统是为了外界提供服务
- 例：通过虚拟机为外界提供 Web 服务（AWS，阿里云）

桌面虚拟化

- 虚拟机上运行的系统提供给终端用户使用
- 例：企业内部的远程办公系统、远程调试系统等（VMware，Citrix）

操作系统的硬件保护机制（P231）

用户态（Ring4）

- 执行非特权指令，如访问虚拟内存、运算等

内核态

- 执行所有指令，包括 I/O 指令，电源管理指令等

调用方式

- 用户态对特权指令的使用必须通过系统调用实现

虚拟化的三个问题

虚拟机的运行模式

- 根模式和非根模式

访存指令怎样执行

- EPT 页表

访问 I/O 的指令怎样执行

- 虚拟设备

根模式和非根模式

非根模式

Ring3 客户机用户态
Ring0 客户机核心态

根模式

Ring0 主机核心态
Ring3 主机用户态