目录

3.1 虚拟化技术简介

虚拟化技术是伴随着计算机的出现而产生和发展起来的，虚拟化意味着对计算机资源的抽象。

虚拟化技术已经成为构建云计算环境的一项关键技术。

服务器虚拟化

存储虚拟化

网络虚拟化

桌面虚拟化

20世纪60年代

IBM公司推出虚拟化技术

主要用于当时的IBM大型机的服务器虚拟化

虚拟化技术的核心思想是利用软件或固件管理程序构成虚拟化层，把物理资源映射为虚拟资源。在虚拟资源上可以安装和部署多个虚拟机，实现多用户共享物理资源。

- 虚拟化技术简介

- 虚拟化技术简介

传统的数据中心

采用了多种技术 | 业务之间孤立 | 网络结构复杂

虚拟数据中心

高速 | 扁平 | 虚拟化

虚拟化技术简介

随着云计算的发展，传统的数据中心逐渐过渡到虚拟化数据中心，即采用虚拟化技术将原来数据中心的物理资源进行抽象整合。

- 实现资源的动态分配和调度，提高现有资源的利用率和服务可靠性
- 提供自动化的服务开通能力，降低运维成本
- 具有有效的安全机制和可靠性机制，满足公众客户和企业客户的安全需求
- 方便系统升级、迁移和改造

- 虚拟化技术简介

数据中心的虚拟化

服务器虚拟化

将一个或多个物理服务器虚拟成多个逻辑上的服务器

存储虚拟化

把分布的异构存储设备统一为一个或几个大的存储池

网络虚拟化

在底层物理网络和网络用户之间增加一个抽象层

目录

一个物理的服务器虚拟成若干个独立的逻辑服务器，比如分区；

把若干分散的物理服务器虚拟为一个大的逻辑服务器，比如网格技术

3.2 服务器虚拟化

- 3.2.1 服务器虚拟化的层次
- 3.2.2 服务器虚拟化的底层实现
- 3.2.3 虚拟机迁移
- 3.2.4 隔离技术
- 3.2.5 案例分析

服务器虚拟化的层次

寄居虚拟化（托管型）

- 寄居虚拟化的虚拟化层一般称为虚拟机监控器（VMM）
- 这类虚拟化架构系统损耗比较大
- 就操作系统层的虚拟化而言，没有独立的Hypervisor层
- 优点：虚拟机更容易构建和安装，可借助于主机OS实现调度等，但损失性能

图7-1 寄居虚拟化架构

服务器虚拟化的层次

裸机虚拟化（传统型）

- 架构中的VMM也可以认为是一个操作系统，一般称为Hypervisor
- Hypervisor实现从虚拟资源到物理资源的映射
- Hypervisor实现了不同虚拟机的运行上下文保护与切换，保证了各个客户虚拟系统的有效隔离

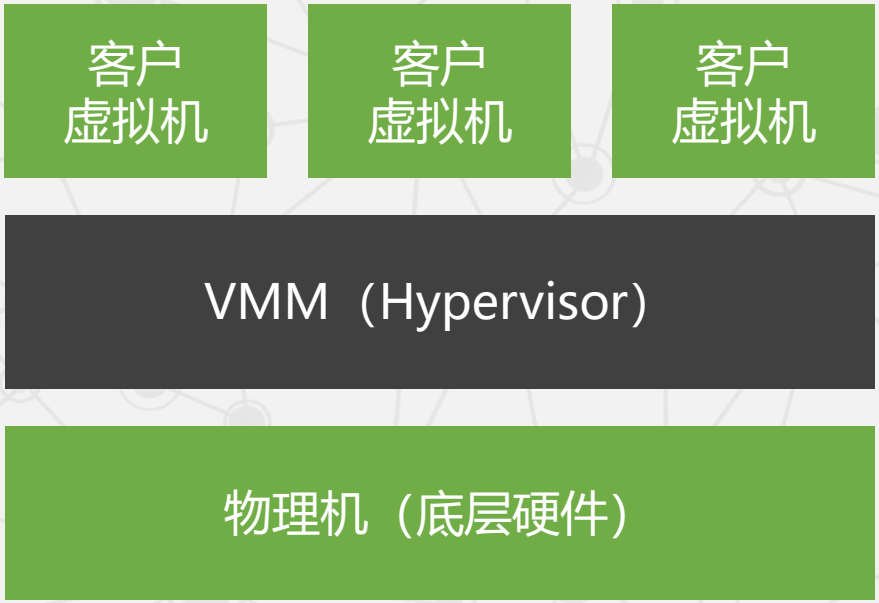


图7-2 裸机虚拟化架构

- **服务器虚拟化的层次**

混合型虚拟化

- 虚拟机管理程序与主机OS共享同样的硬件
- 性能与硬件开销介于前两者之间

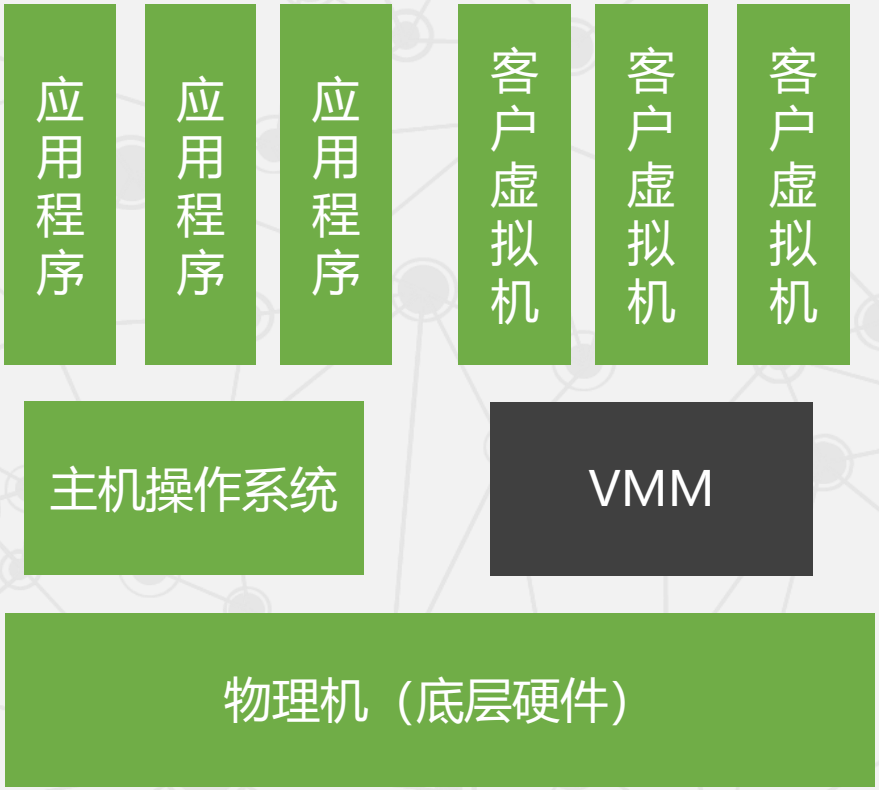
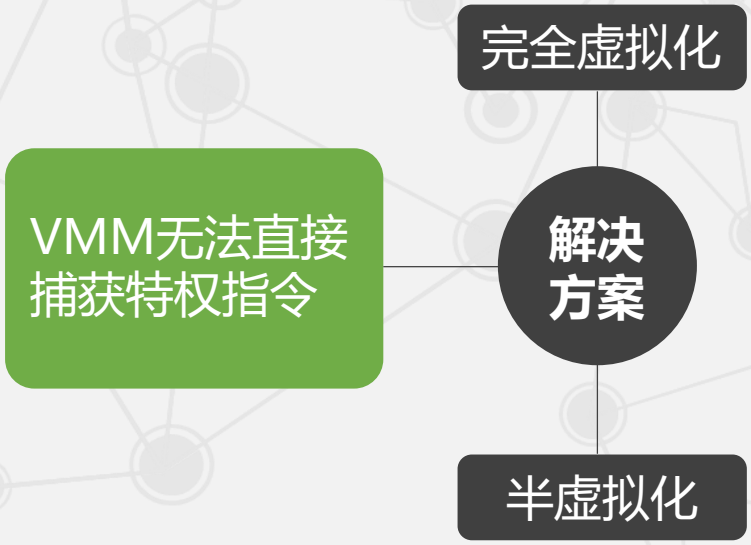


图7-3 混合虚拟机

- **服务器虚拟化的层次**



对真实物理服务器的完整模拟，在上层操作系统看来，虚拟机与物理平台没有区别，操作系统察觉不到运行在虚拟机上

完全虚拟化具有很好的兼容性，在服务器虚拟化中得到广泛应用。

通过修改操作系统代码使特权指令产生自陷

半虚拟化技术降低了由于虚拟化而引入的系统性能损失。

3.2 服务器虚拟化

3.2.1 服务器虚拟化的层次

▶ 3.2.2 服务器虚拟化的底层实现

3.2.3 虚拟机迁移

3.2.4 隔离技术

3.2.5 案例分析

• 服务器虚拟化的底层实现

CPU虚拟化

客户
操作系统

1. 虚拟CPU的正确运行是要保证虚拟机指令正确运行，现有的实现技术包括模拟执行和监控执行

2. 调度问题是指VMM决定当前哪个虚拟CPU在物理CPU上运行，要保证隔离性、公平性和性能。

服务器虚拟化的底层实现

内存虚拟化

内存虚拟化技术把物理内存统一管理，包装成多个虚拟的物理内存提供给若干虚拟机使用，每个虚拟机拥有各自独立的内存空间。虚拟机管理器完成和维护物理机内存和虚拟机所使用内存间的映射关系。

虚拟内存的管理包括3种地址

服务器虚拟化的底层实现

I/O设备虚拟化

I/O设备虚拟化技术把真实的设备统一管理起来，包装成多个虚拟设备给若干个虚拟机使用，响应每个虚拟机的设备访问请求和I/O请求。

I/O设备虚拟化同样是由VMM进行管理的

- 全虚拟化
- 半虚拟化
- 软件模拟

3.2 服务器虚拟化

3.2.1 服务器虚拟化的层次

3.2.2 服务器虚拟化的底层实现

▶ 3.2.3 虚拟机迁移

3.2.4 隔离技术

3.2.5 案例分析

虚拟机迁移

虚拟机迁移是将虚拟机实例从源宿主机迁移到目标宿主机，并且在目标宿主机上能够将虚拟机运行状态恢复到其在迁移之前相同的状态，以便能够继续完成应用程序的任务。重大意义：可保证云端的负载均衡，增强系统错误容忍度。

从虚拟机迁移的源与目的地角度可分为

- 物理机到虚拟机的迁移（P2V）
- 虚拟机到虚拟机的迁移（V2V）
- 虚拟机到物理机的迁移（V2P）

虚拟机迁移

实时迁移（LiveMigration），就是保持虚拟机运行的同时，把它从一个计算机迁移到另一个计算机，并在目的计算机恢复运行的技术。

第一	云计算中心的物理服务器负载经常处于动态变化中，当一台物理服务器负载过大时，若此刻不可能提供额外的物理服务器，管理员可以将其上面的虚拟机迁移到其他服务器，达到负载平衡
第二	云计算中心的物理服务器有时候需要定期进行升级维护，当升级维护服务器时，管理员可以将其上面的虚拟机迁移到其他服务器，等升级维护完成之后，再把虚拟机迁移回来

- 虚拟机迁移

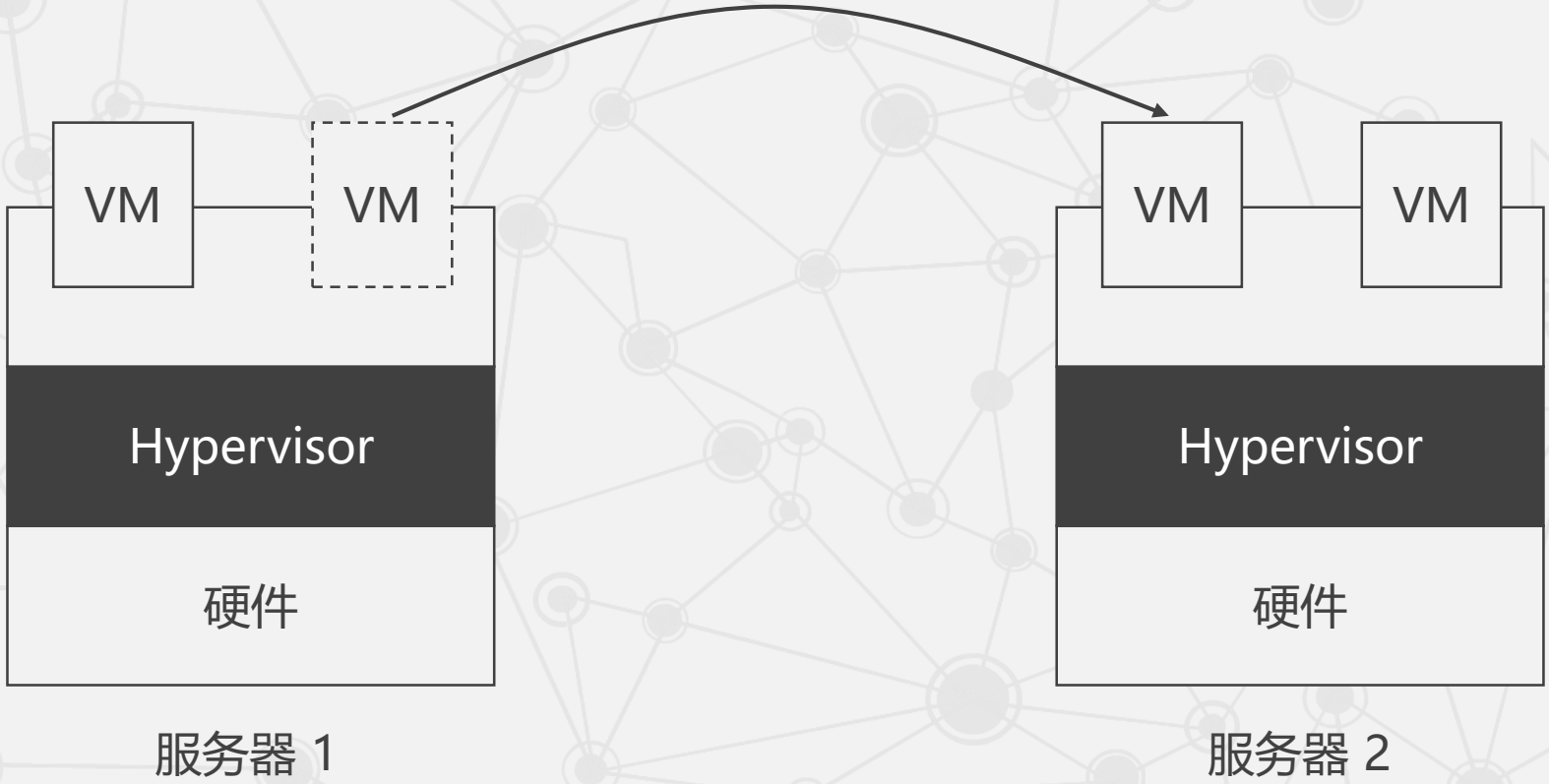


图7-3 虚拟机迁移示意图

- 虚拟机迁移


步骤1
预迁移
(Pre-Migration)
步骤2
预定资源
(Reservation)
步骤3
预复制
(InterativePre-Copy)
步骤4
停机复制
(Stop-and-Copy)
步骤5
提交
(Commitment)
步骤6
启动
(Activation)

- **虚拟机迁移**

内存的迁移是虚拟机迁移最困难的部分

第一阶段，Push阶段。

第二阶段，Stop-and-Copy阶段。

第三阶段，Pull阶段。

实际上，迁移内存没有必要同时包含上述三个阶段，目前大部分的迁移策略只包含其中的一个或者两个阶段。

- 虚拟机迁移

迁移方案	优势与劣势
Stop-and-Copy	● 方法比较简单 ● 总迁移时间也最短 ● 停机时间无法接受
Stop-and-Copy和Pull阶段结合	● 停机时间很短 ● 总迁移时间很长 ● Pull阶段复制造成的性能下降
Push和Stop-and-Copy阶段结合	● 平衡了停机时间和总迁移时间之间的矛盾 ● 需要有一种算法能够测定工作集，以避免反复重传 ● 可能会占用大量的网络带宽，对其他服务造成影响

- **虚拟机迁移**

网络资源的迁移

虚拟机这种系统级别的封装方式意味着迁移时VM的所有网络设备，包括协议状态（如TCP连接状态）以及IP地址都要随之一起迁移。

在局域网内，可以通过发送ARP重定向包，将VM的IP地址与目的机器的MAC地址相绑定，之后的所有包就可以发送到目的机器上。

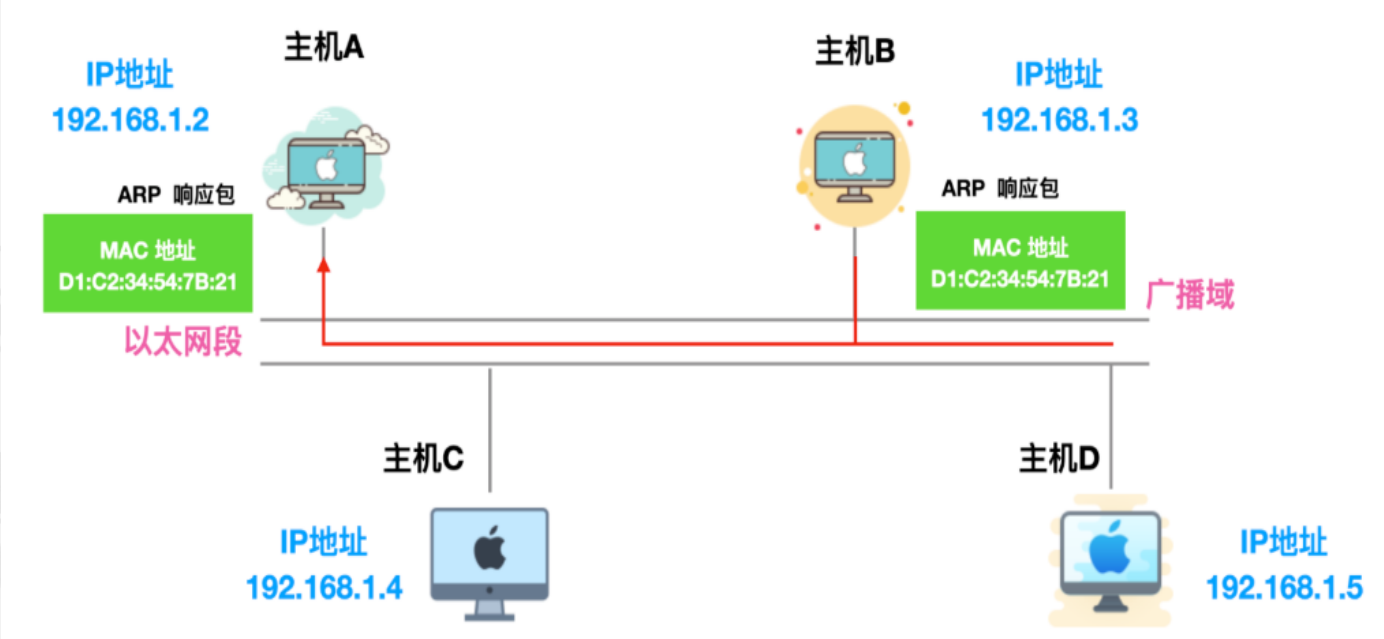
ARP协议

Address Resolution Protocol(地址解析协议)：用于实现从 IP 地址到 MAC 地址的映射，即询问目标 IP 对应的 MAC 地址 的一种协议。

ARP工作机制

A 和 B 位于同一链路，不需要经过路由器的转换，主机 A 向主机 B 发送一个 IP 分组，主机 A 的地址是 192.168.1.2 ，主机 B 的地址是 192.168.1.3，同时该链路上还有主机C和D。

主机 A 想要获取主机 B 的 MAC 地址？主机 A 会通过广播的方式向以太网上的所有主机发送一个 ARP 请求包，这个 ARP 请求包中包含了主机 A 想要知道的主机 B 的 IP 地址的 MAC 地址。

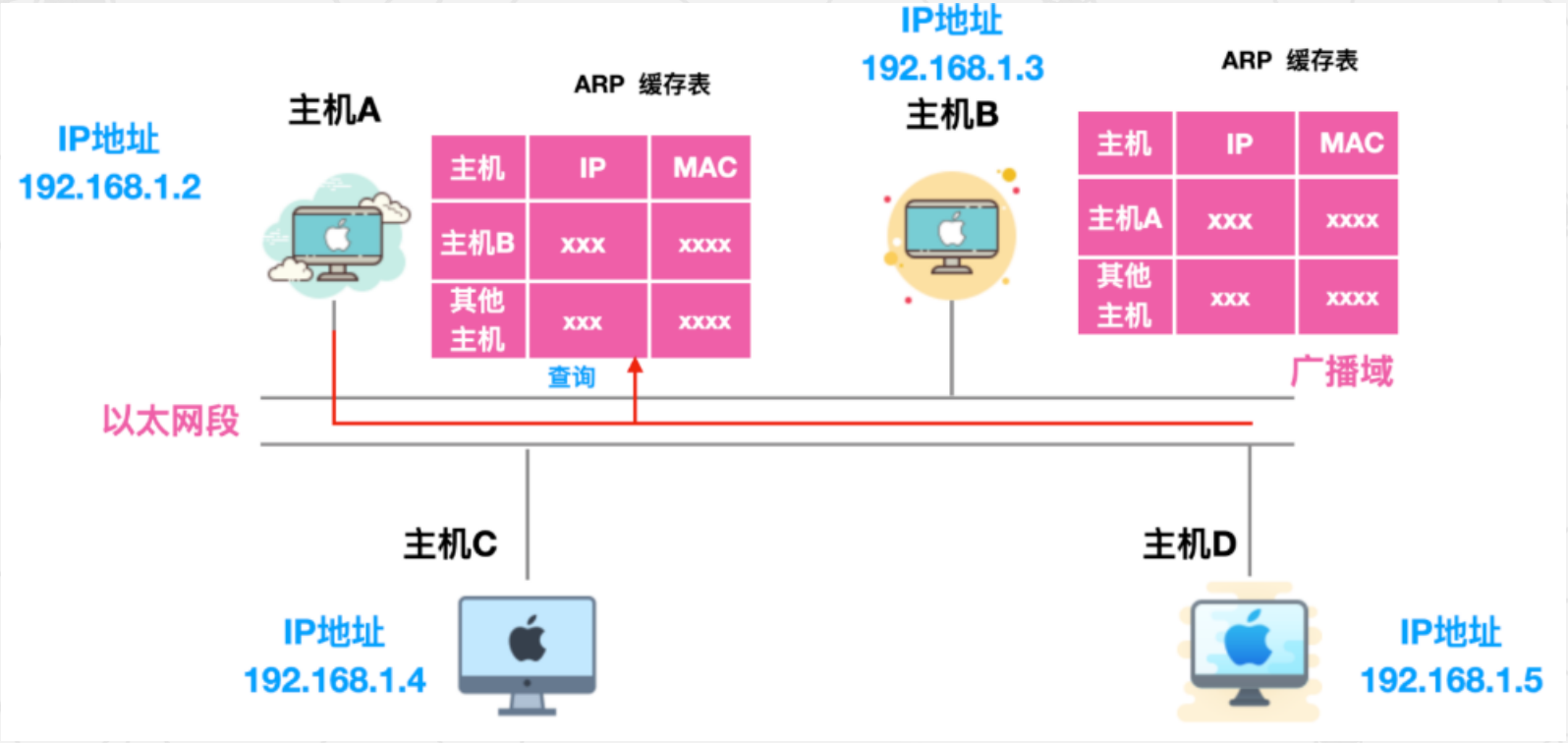


主机 A 发送的 ARP 请求包会被同一链路上的所有主机/路由器接收并进行解析。每个主机/路由器都会检查 ARP 请求包中的信息，如果 ARP 请求包中的目标 IP 地址和自己的相同，就会将自己主机的 MAC 地址写入响应包返回主机 A

3.2 服务器虚拟化

ARP 会被路由器隔离，但是采用代理 ARP (ARP Proxy) 的路由器可以将 ARP 请求转发给临近的网段。使多个网段中的节点像是在同一网段内通信。

维护每个主机和路由器上的 ARP 缓存(或表)：这个缓存维护着每个 IP 到 MAC 地址的映射关系。每发送一次 ARP 请求，缓存表中对应的映射关系都会被清除。



ARP攻击：不安全的协议

ARP 泛洪攻击：首先发送大量的 ARP 请求报文，然后又发送大量虚假的 ARP 响应报文，从而造成网关部分的 CPU 利用率上升难以响应正常服务请求，而且网关还会被错误的 ARP 缓存表充满导致无法更新维护正常 ARP 缓存表，消耗网络带宽资源。

ARP 欺骗主机攻击：攻击者通过 ARP 欺骗使得局域网内被攻击主机发送给网关的流量信息实际上都发送给攻击者。主机刷新自己的 ARP 使得在自己的ARP 缓存表中对应的 MAC 为攻击者的MAC，造成用户的数据外泄。

欺骗网关的攻击:目标选择的不是个人主机而是局域网的网关，把别的主机发送给网关的数据通过欺骗网关的形式使得这些数据通过网关发送给攻击者，造成数据的泄露。

中间人攻击: 同时欺骗局域网内的主机和网关，局域网中用户的数据和网关的数据会发给同一个攻击者，这样用户与网关的数据就会泄露。

IP地址冲突攻击: 扫描出局域网中的物理主机的 MAC 地址，然后根据物理主机的MAC 进行攻击，导致局域网内的主机产生 IP 地址冲突，影响用户的网络正常使用。

虚拟机迁移

存储设备的迁移

- 迁移存储设备的最大障碍在于需要占用大量时间和网络带宽，通常的解决办法是以共享的方式共享数据和文件系统，而非真正迁移。
- 目前大多数集群使用NAS（Network Attached Storage，网络连接存储）作为存储设备共享数据。
- NAS实际上是一个带有瘦服务器的存储设备，其作用类似于一个专用的文件服务器。
- 在局域网环境下，NAS已经完全可以实现异构平台之间，如NT、UNIX等的数据级共享。
- 基于以上的考虑，Xen并没有实现存储设备的迁移，实时迁移的对象必须共享文件系统。

3.2 服务器虚拟化

3.2.1 服务器虚拟化的层次

3.2.2 服务器虚拟化的底层实现

3.2.3 虚拟机迁移

▶ 3.2.4 隔离技术

3.2.5 案例分析

隔离技术

虚拟机隔离是指虚拟机之间在没有授权许可的情况下，互相之间不可通信、不可联系的一种技术。

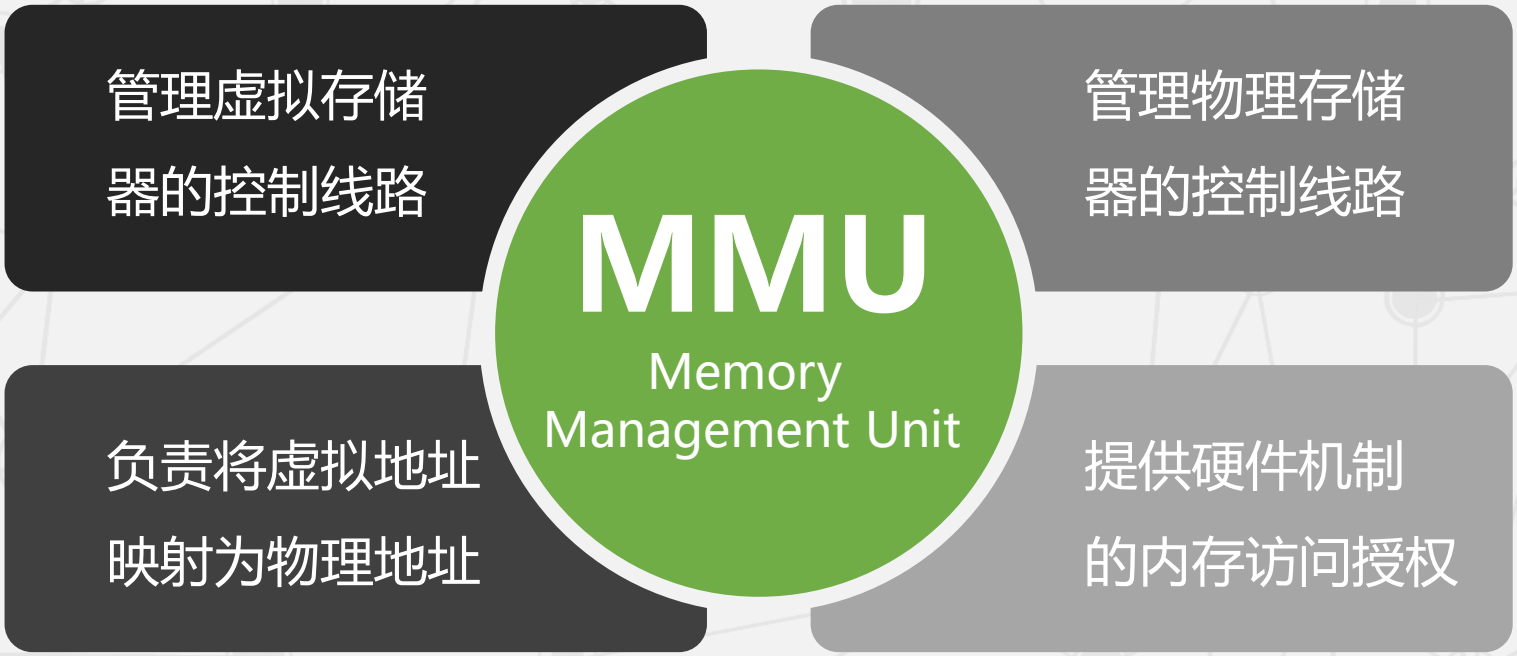
软件角度	互相隔离的虚拟机之间保持独立，如同一个完整的计算机
硬件角度	被隔离的虚拟机相当于一台物理机，有自己的CPU、内存、硬盘、I/O等，它与宿主机之间保持互相独立的状态
网络角度	被隔离的虚拟机如同物理机一样，既可以对外提供网络服务，也一样可以从外界接受网络服务

隔离技术

虚拟机隔离机制

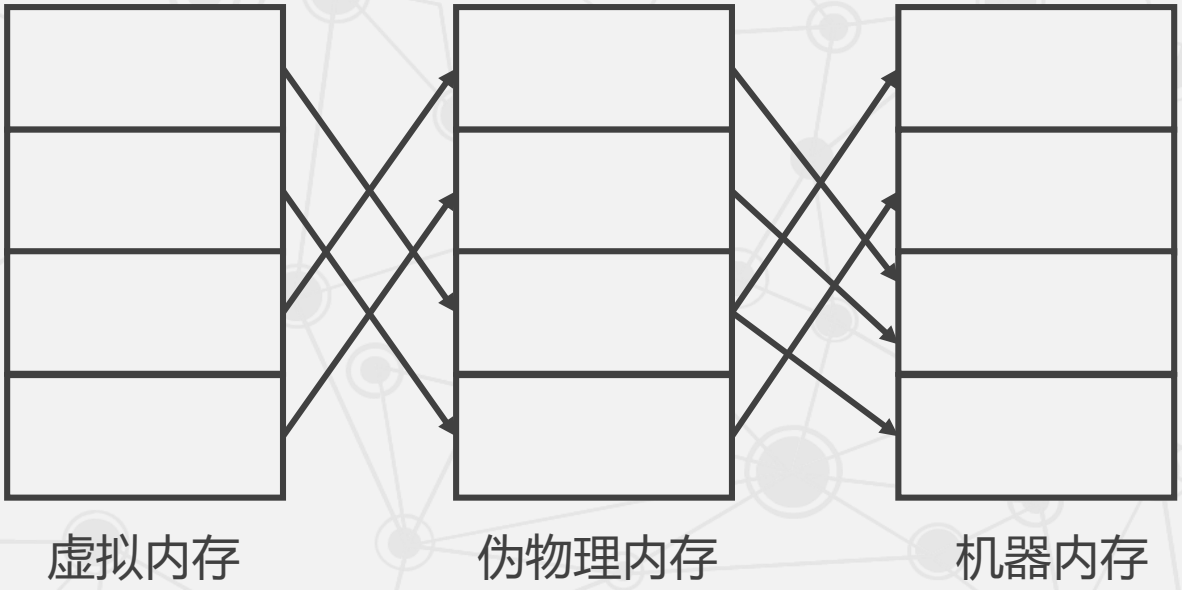
- 网络隔离；
- 构建虚拟机安全文件防护网；
- 基于访问控制的逻辑隔离机制；
- 通过硬件虚拟，让每个虚拟机无法突破虚拟机管理器给出的资源限制；
- 硬件提供的内存保护机制；
- 进程地址空间的保护机制，IP地址隔离。

- 内存隔离


管理虚拟存储器的控制线路
管理物理存储器的控制线路
MMU
Memory Management Unit
负责将虚拟地址映射为物理地址
提供硬件机制的内存访问授权

- **内存隔离**

Xen将这层中间地址真正地映射到机器地址上却可以是不连续的，这样保证了所有的物理内存可被任意分配给不同的Guest OS



虚拟内存与机器内存的映射关系

内存隔离

虚拟机监控器使用分段和分页机制对自身的物理内存进行保护。x86体系结构提供了支持分段机制的虚拟内存，这能够提供另一种形式的特权级分离。

基址	段限	属性位
基址和虚拟地址相加形成线性地址	段限决定了这个段中所能访问的线性空间的长度	属性位则标记了该段是否可读写，可执行，是代码段还是数据段等

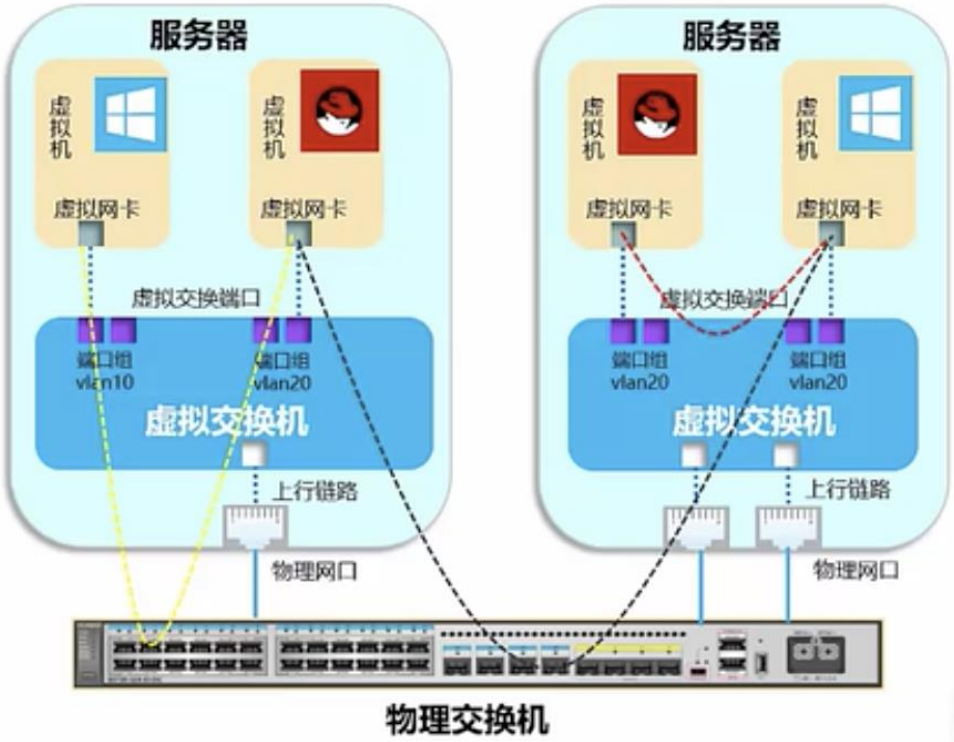
3.2 服务器虚拟化

网络隔离的目标

确保把有害的攻击隔离，在可信网络之外和保证可信网络内部信息不外泄的前提下，完成网间数据的安全交换。

虚拟化中数据的转发路径

- 相同端口组不同服务器内的虚拟机通讯需要经过物理网络。
- 相同端口组相同服务器内的虚拟机通讯不需要经过物理网络。
- 不同端口组相同服务器的虚拟机通讯需要经过物理网络。



网络隔离

关键

在于系统对通信数据的控制

即通过不可路由的协议来完成网间的数据交换

安全要素

- 机密性
- 完整性
- 可用性
- 可控性
- 抗抵赖

安全机制

- 访问控制
- 身份认证
- 加密签名

- 网络隔离

实现原理

- 专用通信设备
- 专有安全协议
- 加密验证机制
- 应用层数据提取和鉴别认证技术

不同安全级别网络之间的数据交换

- 彻底阻断了网络间的直接TCP/IP连接
- 保证了网间数据交换的安全、可控
- 杜绝了由于操作系统和网络协议自身漏洞带来的安全风险

3.2 服务器虚拟化

3.2.1 服务器虚拟化的层次

3.2.2 服务器虚拟化的底层实现

3.2.3 虚拟机迁移

3.2.4 隔离技术

▶ 3.2.5 案例分析

案例分析

VMware公司推出了面向云计算的一系列产品和解决方案

虚拟机迁移工具VMotion

存储迁移工具Storage VMotion

VMotion

VMotion是VMware用于在数据中心的服务器之间进行虚拟机迁移的技术。

虚拟机迁移过程中主要采用**三项技术**：

① 将虚拟机状态信息压缩存储在共享存储器的文件中

② 将虚拟机的动态内存和执行状态通过高速网络在源ESX服务器和目标ESX服务器之间快速传输

③ 虚拟化网络以确保在迁移后虚拟机的网络身份和连接能保留

VMware Storage VMotion

VMware Storage VMotion用于实时迁移虚拟机磁盘文件，以便满足对虚拟机磁盘文件的升级、维护和备份。

原理

存储之间的转移

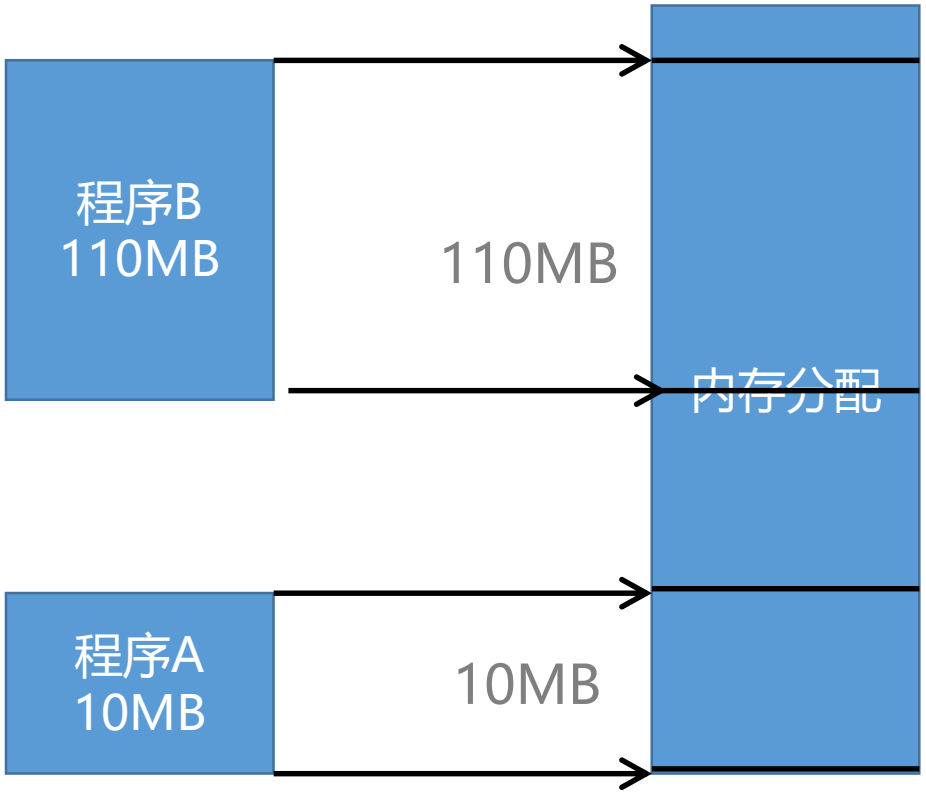
核心技术

- **磁盘快照**
- **REDO记录**
- **父/子磁盘关系**
- **快照整合**

- **早期的内存分配机制**

程序中访问的内存地址都是实际的物理内存地址；

同时运行多个程序时，必须保证这些程序用到的内存总量要小于计算机实际物理内存的大小



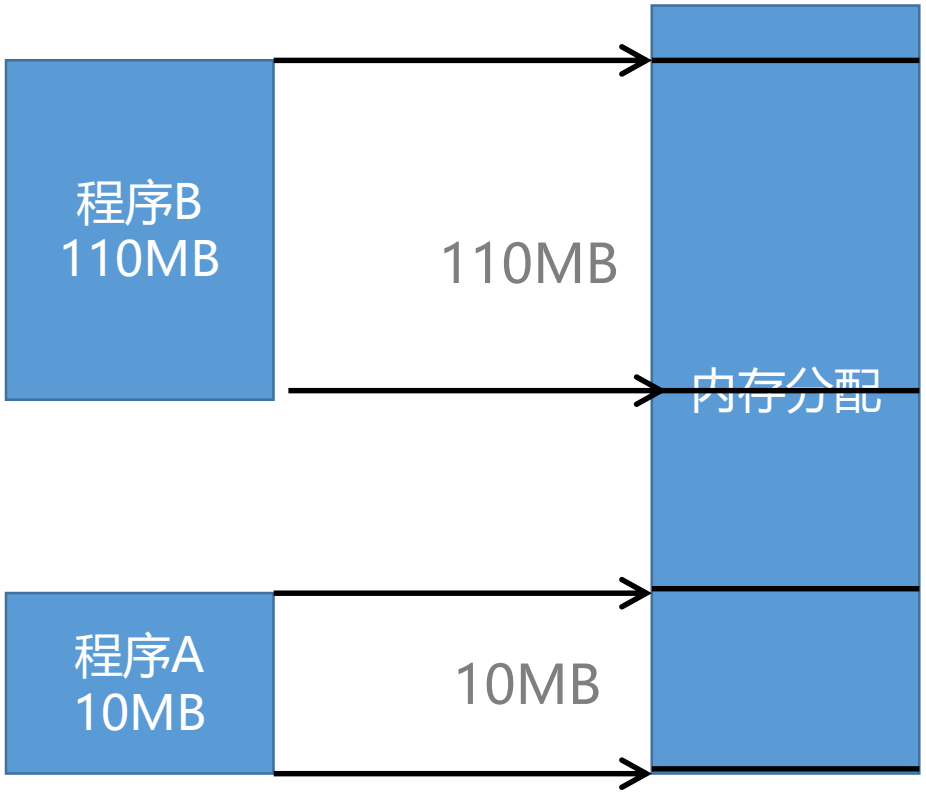
计算机内存大小128M，现同时运行两个程序A和B，A占用内存10M，B占用内存110M

- **存在问题**

进程地址空间不隔离；

内存使用效率低；

程序运行的地址不确定



计算机内存128M，A占用内存10M，B占用内存110M，C占用内存20M

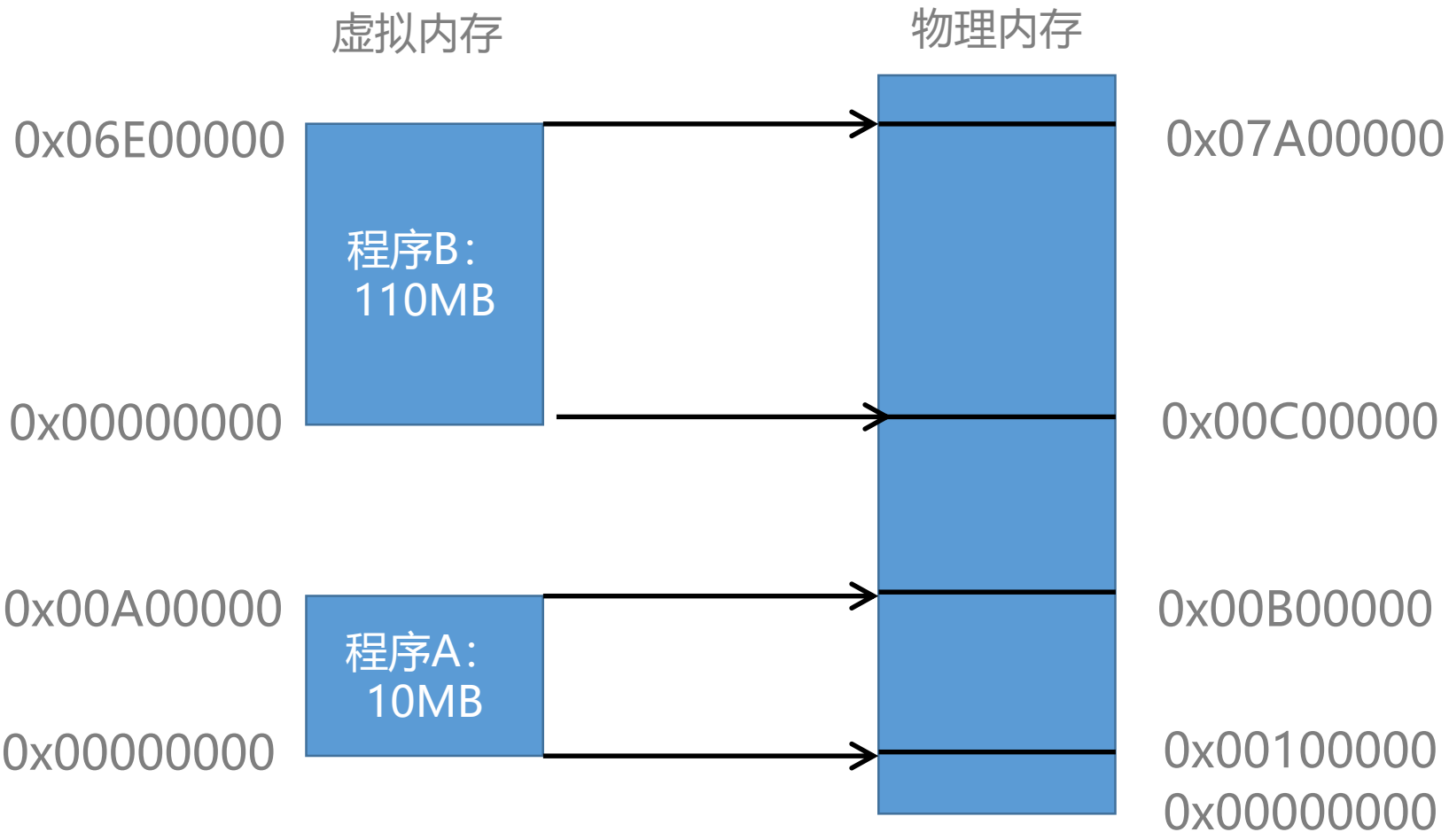
- **分段技术**

增加中间层，利用间接的地址访问方法访问物理内存。

程序中访问的内存地址不再是实际的物理内存地址，而是一个虚拟地址，然后由操作系统将这个虚拟地址映射到适当的物理内存地址上。

只要操作系统处理好虚拟地址到物理内存地址的映射，就可以保证不同的程序最终访问的内存地址位于不同的区域，彼此没有重叠，从而达到内存地址空间隔离的效果。

- 分段技术的内存映射


虚拟内存
物理内存
0x06E00000
0x00000000
0x00A00000
0x00000000
程序B:
110MB
程序A:
10MB
0x07A00000
0x00C00000
0x00B00000
0x00100000
0x00000000

- **分段技术**

分段的映射方法解决了两个问题：进程地址空间不隔离和程序运行的地址不确定。

但是内存的使用效率问题没有得到解决。在分段的映射方法中，每次换入换出内存的都是整个程序，这样会造成大量的磁盘访问操作，导致效率低下。所以这种映射方法比较粗糙，粒度较大。

程序的运行的局部性特点：在某个时间段内，程序只是访问程序的一小部分数据，程序的大部分数据在一个时间段内都不会被用到。

- **分页技术**

将地址空间分成许多的页，每页的大小由CPU决定，然后由操作系统选择页的大小。 Inter系列的CPU支持4KB或4MB的页大小，PC上大部分选择使用4KB。

分页的思想是程序运行时用到哪页就为哪页分配内存，没用到的页暂时保留在硬盘上。当用到这些页时再在物理地址空间中为这些页分配内存，然后建立虚拟地址空间中的页和刚分配的物理内存页间的映射。

目录

- **服务器本地磁盘：RAID**

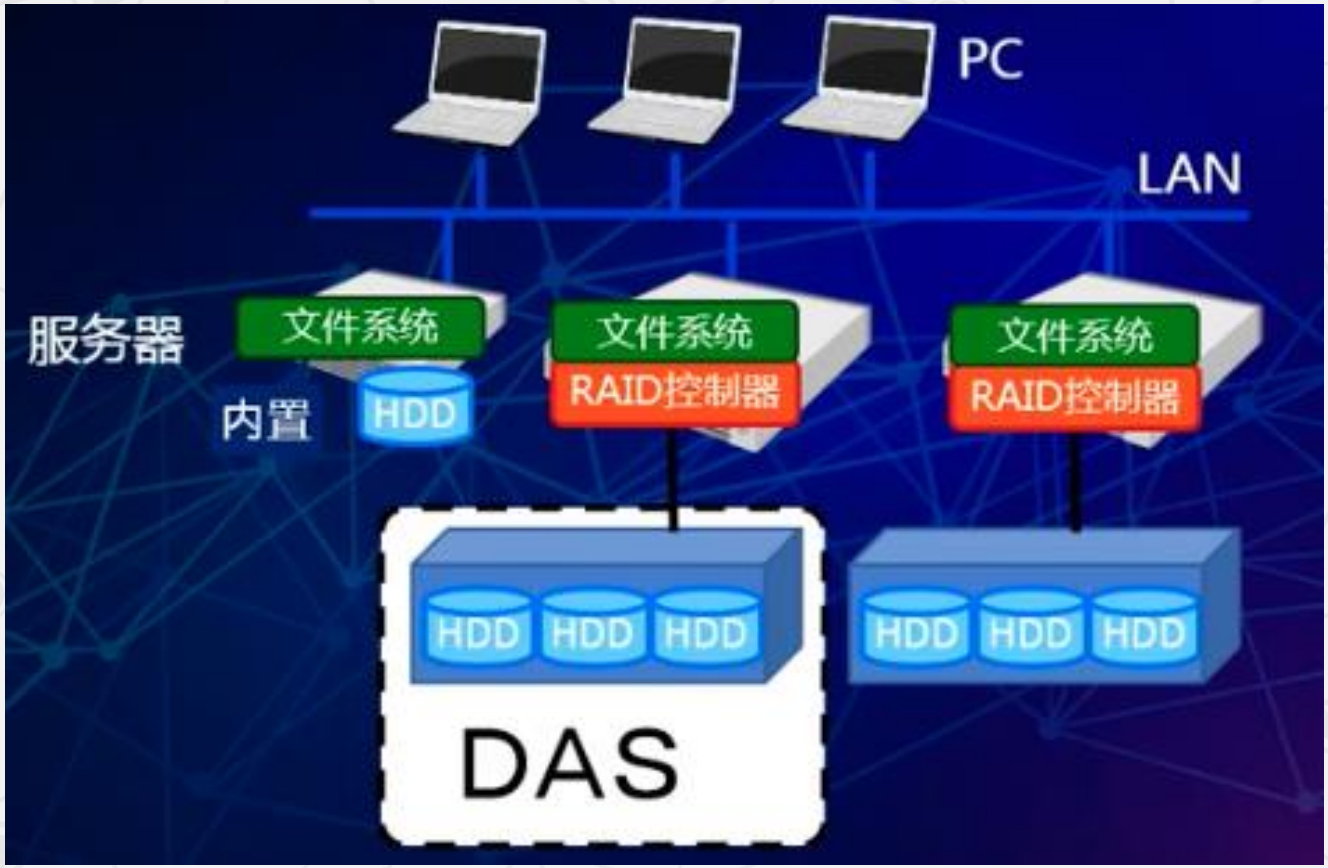
RAID0：分块存储，性能翻倍，安全性差

RAID1：整体备份，安全性高，存储效率差

RAID5：分布式校验盘，校验码信息恢复信息，最多支持损坏1块硬盘

RAID10：RAID0+RAID1

- 服务器外接存储技术：DAS（Direct Attached Storage）



专用的RAID卡；

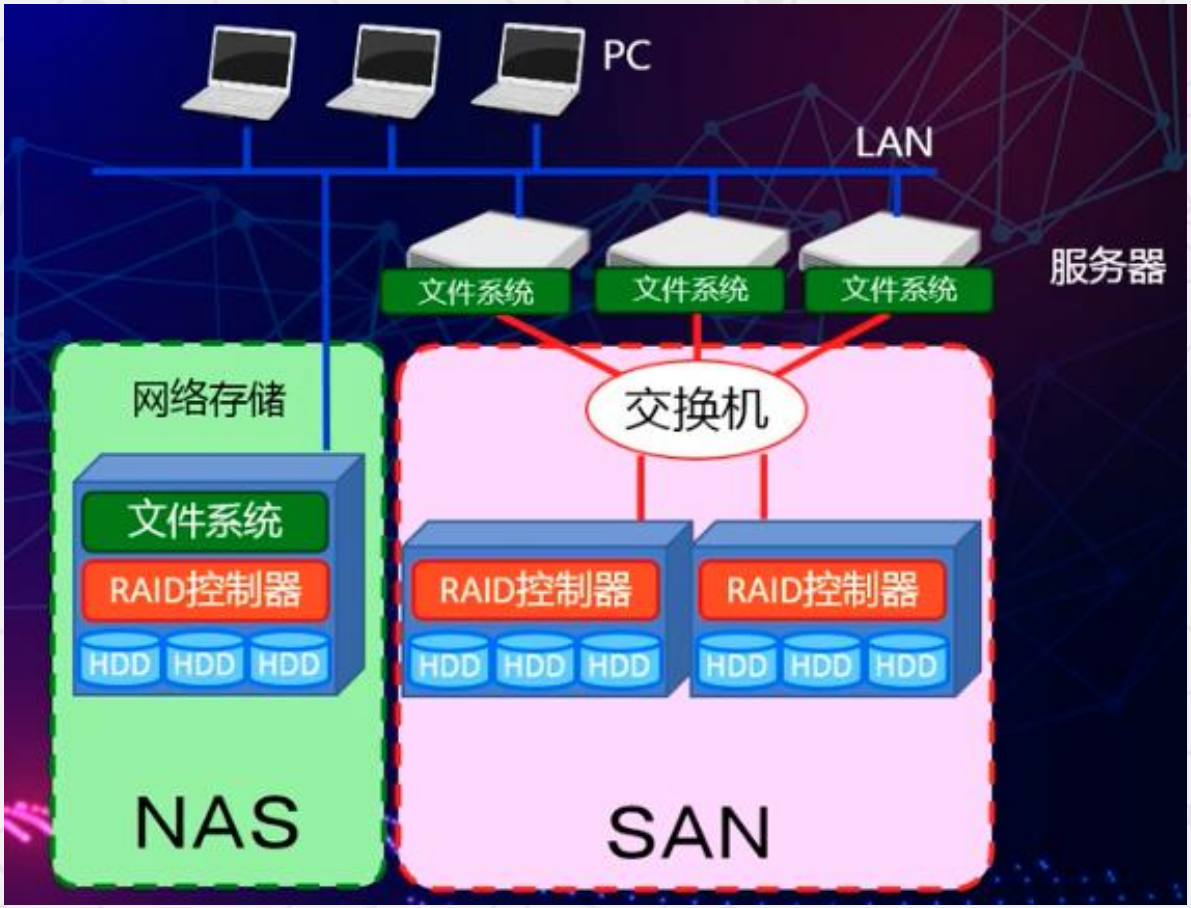
内置/外置磁盘阵列；

物理上两台设备，

逻辑上一台设备。

DAS存储设备只提供一对一存储服务

- **服务器外接存储技术：NAS（Network Attached Storage）**

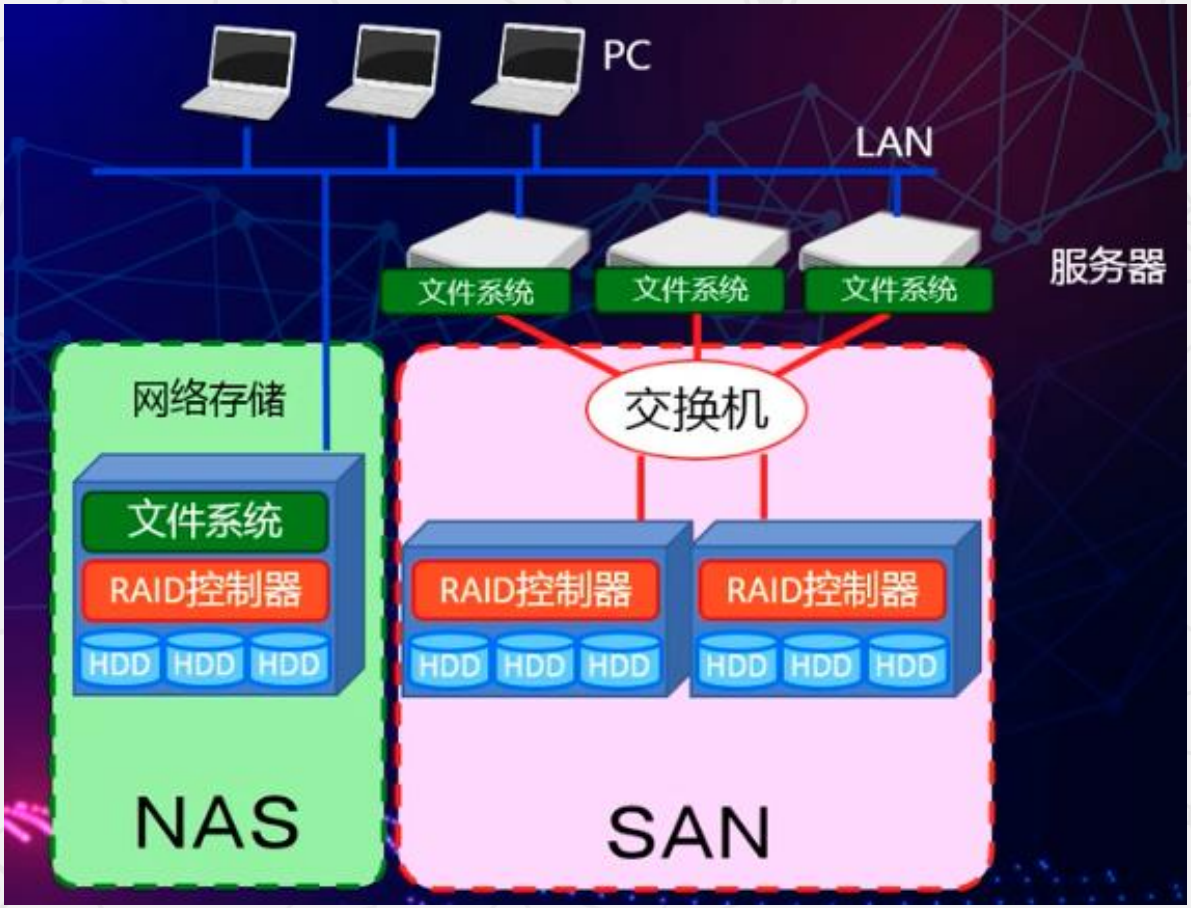


网络存储形式（多用户共享）

文件系统、RAID控制器、硬盘被集成到NAS存储设备

支持不同OS之间通过IP地址形式访问，可共享数据

- **服务器外接存储技术：SAN（Storage Area Network）**



文件系统在服务器端，通过专用网络：FC（光纤线）

SAN、IP SAN等

服务器通过网络独占一片存储空间，不共享数据

- **服务器外接存储技术**

	DAS	NAS	SAN
传输类型	IP、FC、SAS等	IP	IP、FC等专用网络
典型应用	任何场景	文件服务器	数据库、虚拟化市场
优点	磁盘与服务器分离，便于统一管理	不占用服务器资源，支持多操作系统访问，扩展较易，配置方便	扩展性高，可用性高，数据集中，易于管理
缺点	连接距离短，扩展性受服务器接口数量的限制	数据备份及恢复占用网络带宽	相较NAS，成本较高，安装升级复杂

3.3 存储虚拟化

存储虚拟化将系统中分散的存储资源整合起来
提高了存储资源利用率
降低了单位存储空间的成本
降低了存储管理的负担和复杂性
在虚拟层通过使用数据镜像、数据校验和多路径等技术
提高了数据的可靠性及系统的可用性
利用负载均衡、数据迁移、数据块重组等技术
提升系统的潜在性能
整合和重组底层物理资源
得到多种不同性能和可靠性的新的虚拟设备
满足多种存储应用的需求

3.3 存储虚拟化

- 3.3.1 存储虚拟化的一般模型
- 3.3.2 存储虚拟化的实现方式
- 3.3.3 案例分析

存储虚拟化的一般模型

一般来说，虚拟化存储系统在原有存储系统结构上增加了虚拟化层，将多个存储单元抽象成一个虚拟存储池，存储单元可以是异构，可以是直接的存储设备，也可以是基于网络的存储设备或系统。

- 减少存储系统的管理开销
- 实现存储系统数据共享
- 提供透明的高可靠性和可扩展性。

3.3 存储虚拟化

3.3.1 存储虚拟化的一般模型

▶ 3.3.2 存储虚拟化的实现方式

3.3.3 案例分析

- **存储虚拟化的实现方式**

目前，实现存储虚拟化的方式主要有三种：

基于**主机**的
存储虚拟化

基于**存储设备**
的存储虚拟化

基于**网络**的
存储虚拟化

基于主机的存储虚拟化

基于主机的存储虚拟化，也称基于服务器的存储虚拟化或者基于系统卷管理器的存储虚拟化，其一般是通过逻辑卷管理来实现的。

数据存储共享 | 存储资源管理 | 数据复制及迁移 | 集群系统 | 远程备份 | 灾难恢复

优势

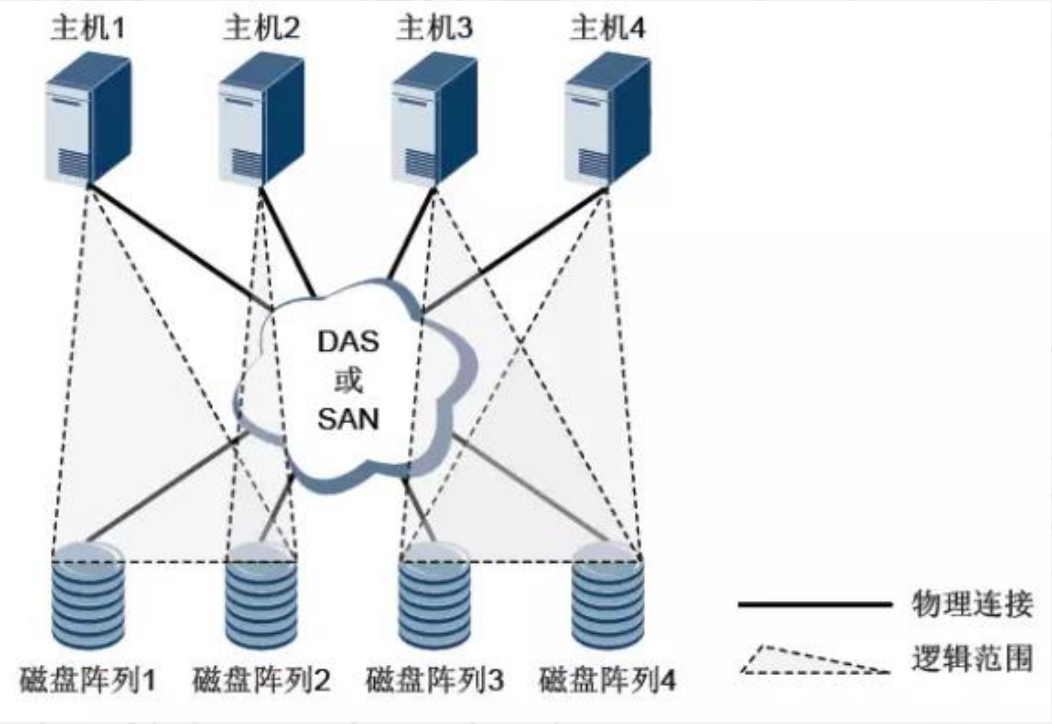
- 性价比比较高

劣势

- 性能下降
- 可扩展性差
- 不支持异构平台

基于主机的存储虚拟化

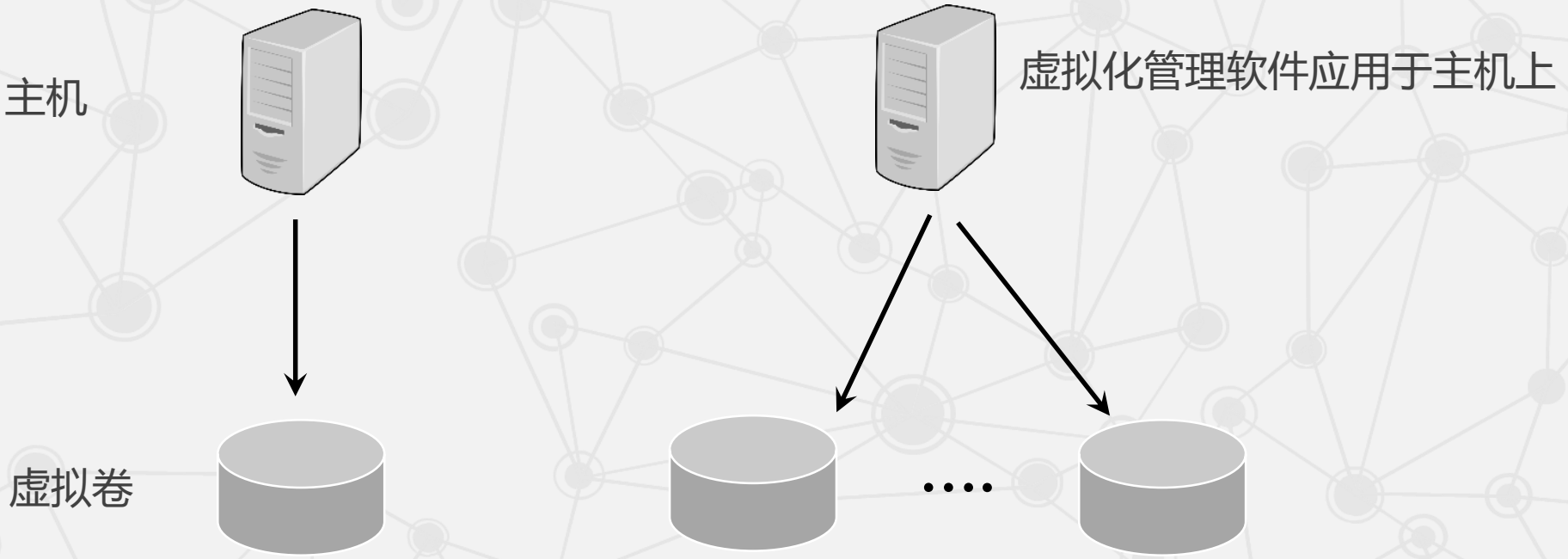
当仅需要单个主机服务器（或单个集群）访问多个磁盘阵列时，可以使用基于主机的存储虚拟化技术。其通常由主机操作系统下的逻辑卷管理软件实现，逻辑卷管理软件把多个不同的磁盘阵列映射成一个虚拟的逻辑块空间。



该技术使主机经过虚拟化的存储空间可以跨越多个异构的磁盘阵列，因此常用于在不同磁盘阵列之间做数据镜像保护。

基于主机的存储虚拟化

基于主机的虚拟存储依赖于代理或管理软件，通过在一个或多个主机上进行安装和部署，来实现存储虚拟化的控制和管理。



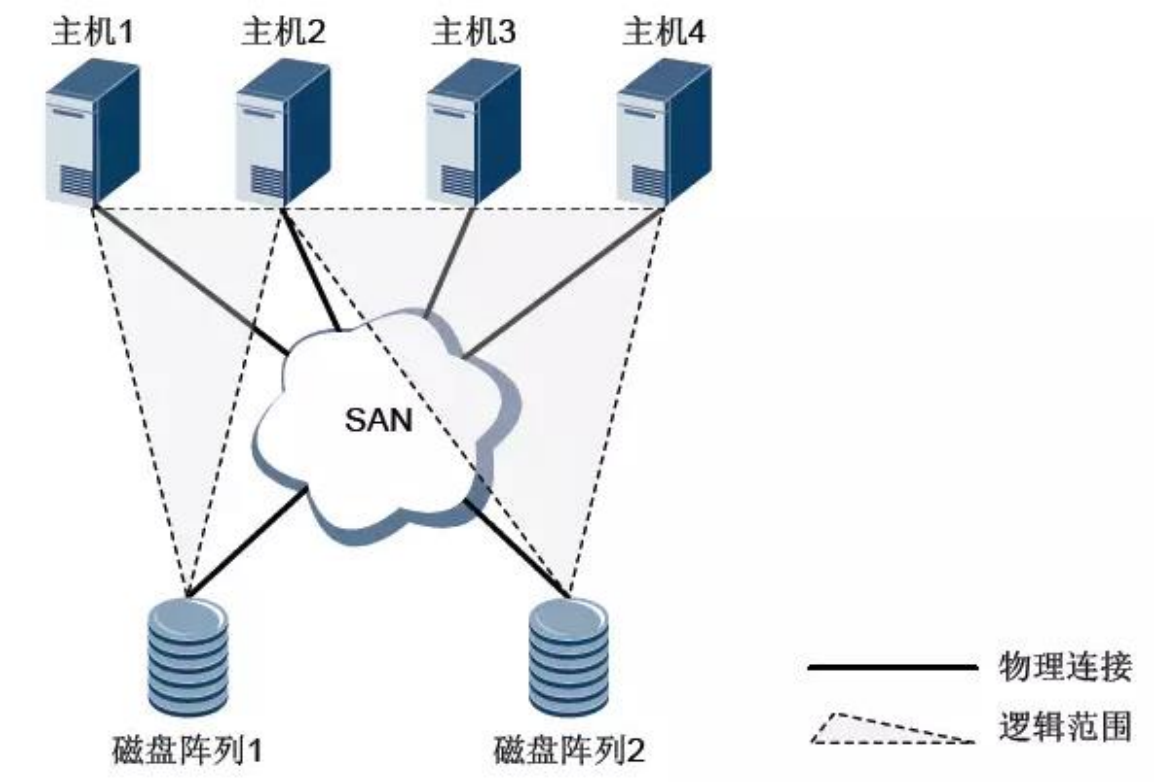
基于存储设备的存储虚拟化

基于存储设备的存储虚拟化主要是在存储设备的磁盘、适配器或者控制器上实现虚拟化功能。

- 有很多的存储设备的内部都有功能比较强的处理器
- 存储设备带有专门的嵌入式系统，可以在存储子系统的内部进行存储虚拟化，对外提供虚拟化磁盘
- 这类存储子系统与主机无关，对系统性能的影响比较小，也比较容易管理
- 对于包含有多家厂商提供异构的存储设备的SAN存储系统，基于存储设备的存储虚拟化方法的效果不是很好
- 这种设备往往规模有限并且不能进行级联，这就使得虚拟存储设备的可扩展性比较差

基于存储设备的存储虚拟化

当有多个主机服务器需要访问同一个磁盘阵列时，可以使用基于存储设备的存储虚拟化技术。该技术通过在存储控制器上添加虚拟机功能实现，可以将一个阵列上的存储容量划分为多个存储空间（LUN），供不同的主机系统访问。



该技术常用于在同一存储设备内部，进行数据保护和数据迁移。

基于网络的存储虚拟化

基于网络的存储虚拟化方法是在网络设备上实现存储虚拟化功能，包括基于互连设备和基于路由器两种方式。

优点

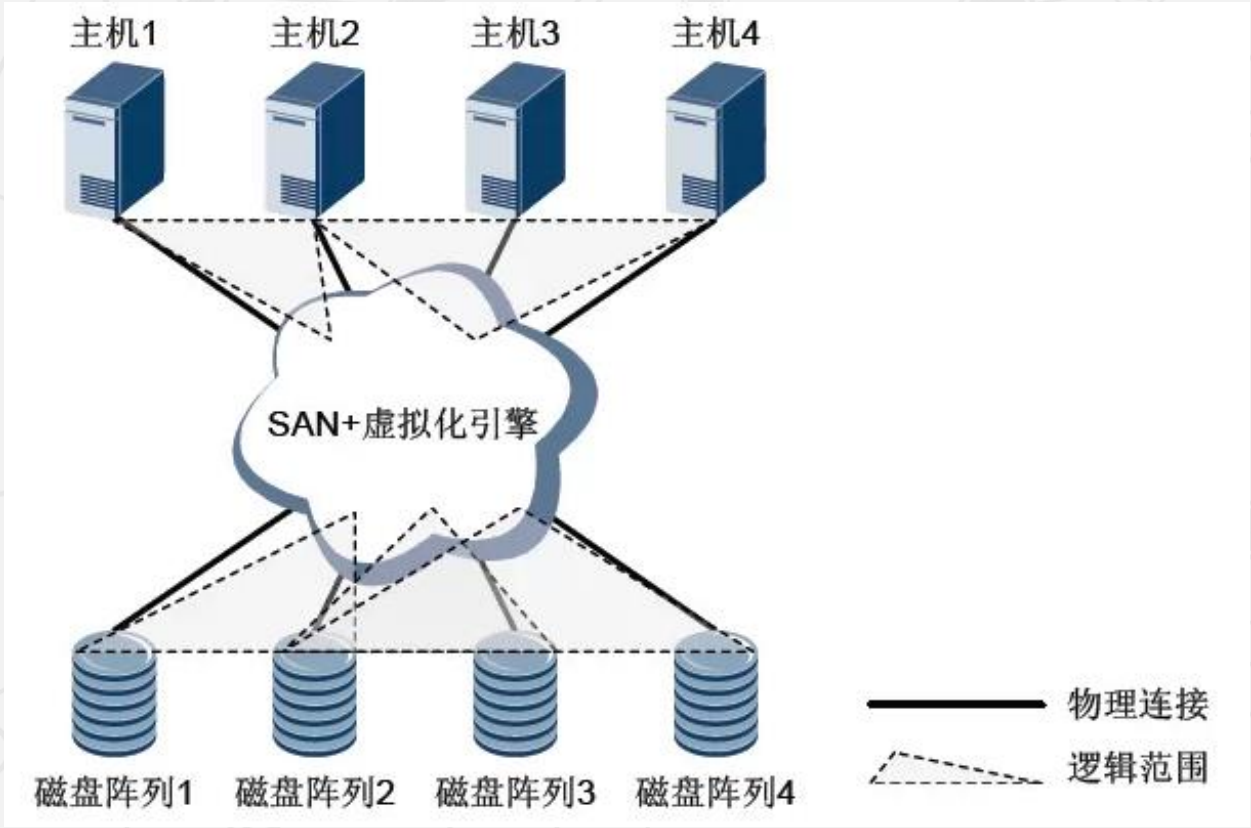
相对于上述几种方式，基于路由器的虚拟化在性能、效果和安全方面都要好一些

缺点

如果连接主机到存储网络的路由器出现故障，也可能会使主机上的数据不能被访问，但是只有与故障路由器连接在一起的主机才会受到影响，其余的主机还是可以用其他路由器访问存储系统，且路由器的冗余还能够支持动态多路径。

基于网络的存储虚拟化

当多个主机服务器需要访问多个异构存储设备时，可以使用基于网络的存储虚拟化技术，该技术通过在SAN中添加虚拟化引擎实现。



该技术常用于异构存储系统的整合和统一数据管理。

3.3 存储虚拟化

3.3.1 存储虚拟化的一般模型

3.3.2 存储虚拟化的实现方式

▶ 3.3.3 案例分析

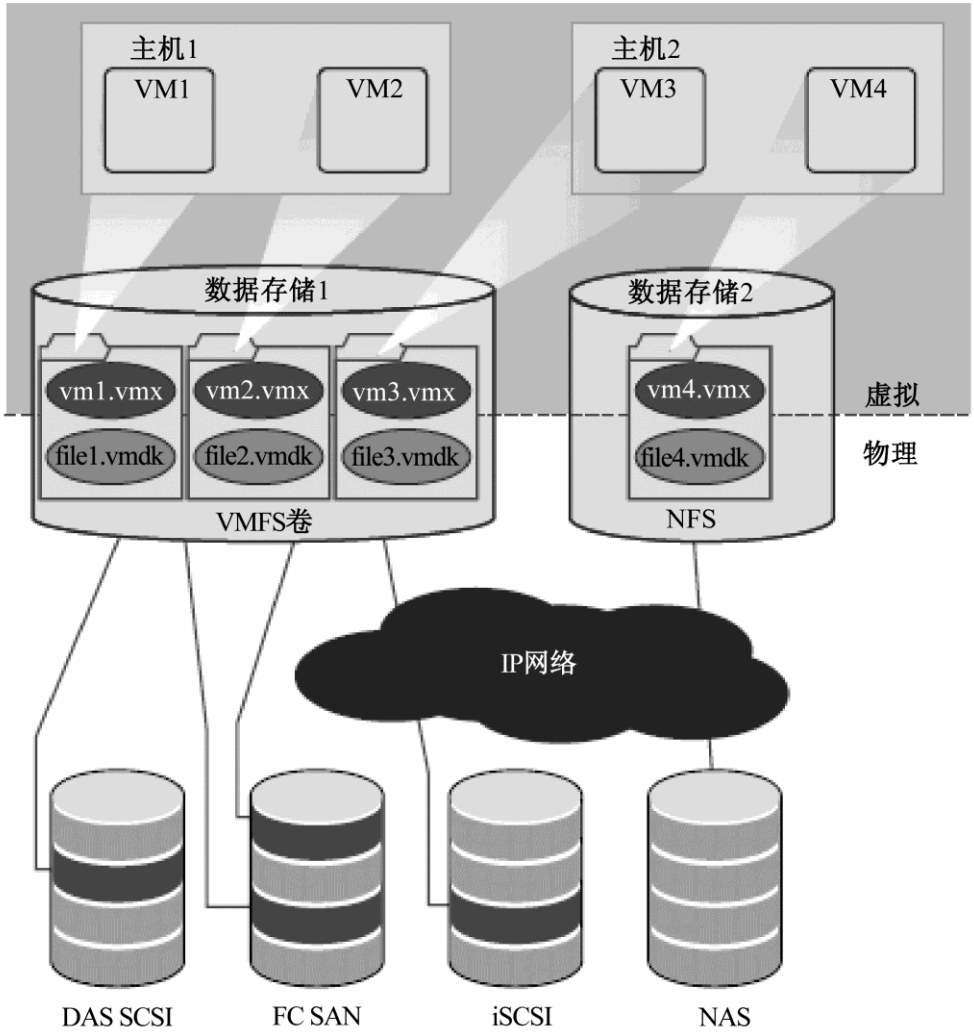
案例分析

VMFS的功能主要包括以下3点。

磁盘锁定技术	锁定已启动的虚拟机的磁盘，以避免多台服务器同时启动同一虚拟机
故障一致性和恢复机制	用于快速识别故障的根本原因，帮助虚拟机、物理主机和存储子系统从故障中恢复
裸机映射（RDM）	RDM使得虚拟机能够直接访问物理存储子系统（iSCSI或光纤通道）上的LUN（Logical Unit Number）

- **案例分析**

VMware vSphere存储架构由各种抽象层组成，这些抽象层隐藏并管理物理存储子系统之间的复杂性和差异



VMware虚拟存储架构

目录


传统的数据中心
服务器之间操作系统和上层软件异构、接口与数据格式不统一
数据中心内网络传输效率低
使用云计算后
数据同步传送的大流量、备份大流量、虚拟机迁移大流量
采用统一的交换网络减少布线、维护工作量和扩容成本
引入虚拟化技术之后
数据中心网络虚拟化分为核心层、接入层和虚拟机网络虚拟化三个方面
google.com/datacenters

3.4 网络虚拟化

- 3.4.1 核心层网络虚拟化
- 3.4.2 接入层网络虚拟化
- 3.4.3 虚拟机网络虚拟化
- 3.4.4 案例分析: VMware的网络虚拟化技术

核心层网络虚拟化

核心层网络虚拟化，主要指的是数据中心核心网络设备的虚拟化。

要求

- 核心层网络具备超大规模的数据交换能力
- 足够的万兆接入能力

提供虚拟机箱技术

简化设备管理

提高资源利用率

提高交换系统的灵活性和扩展性

为资源的灵活调度和动态伸缩提供支撑

3.4 网络虚拟化

接入层网络虚拟化

接入层虚拟化，可以实现数据中心接入层的分级设计。根据数据中心的走线要求，接入层交换机要求能够支持各种灵活的部署方式和新的以太网技术。

拥塞通知
(IEEE 802.1Qau)

增强传输选择ETS
(IEEE 802.1Qaz)

优先级流量控制PFC
(IEEE 802.1Qbb)

链路发现协议LLDP
(IEEE 802.1AB)

3.4 网络虚拟化

虚拟机网络虚拟化

虚拟机网络交互需要实现以下功能：

1. 虚拟机的双向访问控制和流量监控，包括深度包检测、端口镜像、端口远程镜像、流量统计。
2. 虚拟机的网络属性应包括VLAN、QoS、ACL、带宽等。
3. 虚拟机的网络属性可以跟随虚拟机的迁移而动态迁移，不需要人工干预或静态配置，从而在虚拟机扩展和迁移过程中，保障业务的持续性。
4. 虚拟机迁移时，与虚拟机相关的资源配置，如存储、网络配置也随之迁移。同时保证迁移过程中业务不中断。

虚拟机网络虚拟化

扩展虚拟数据中心中交换机和虚拟网卡的功能

- 802.1Qbg EVB （Edge Virtual Bridging）
- 802.1Qbh BPE（Bridge Port Extension）

802.1Qbg

外部网络能够支持虚拟交换功能，对于虚拟交换网络范围内VM动态迁移、调度信息，均通过LLDP扩展协议得到同步以简化运维

802.1Qbh

将远程交换机部署为虚拟环境中的策略控制交换机，而不是部署成邻近服务器机架的交换机，通过多个虚拟通道，让边缘虚拟桥复制帧到一组远程端口

3.4 网络虚拟化

3.4.1 核心层网络虚拟化

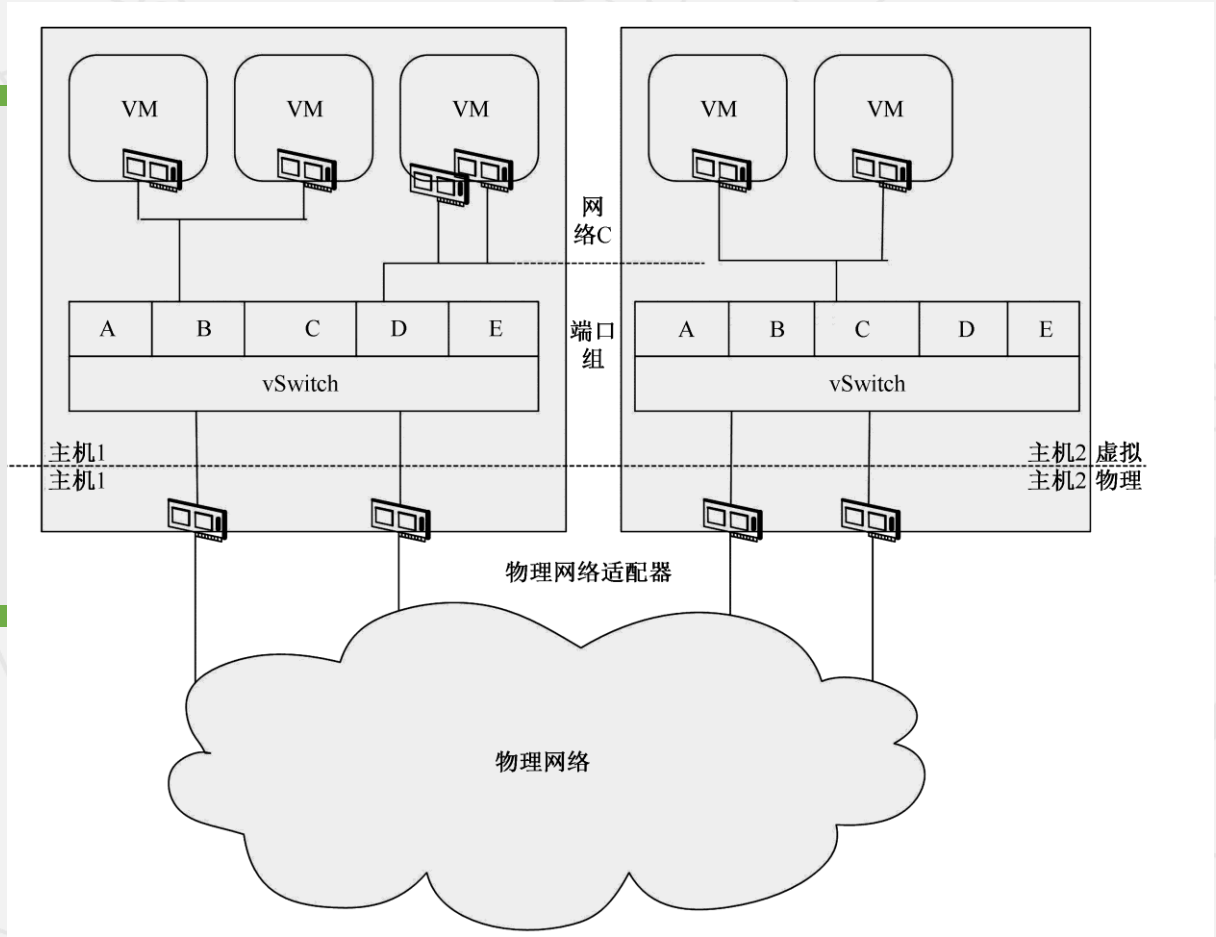
3.4.2 接入层网络虚拟化

3.4.3 虚拟机网络虚拟化

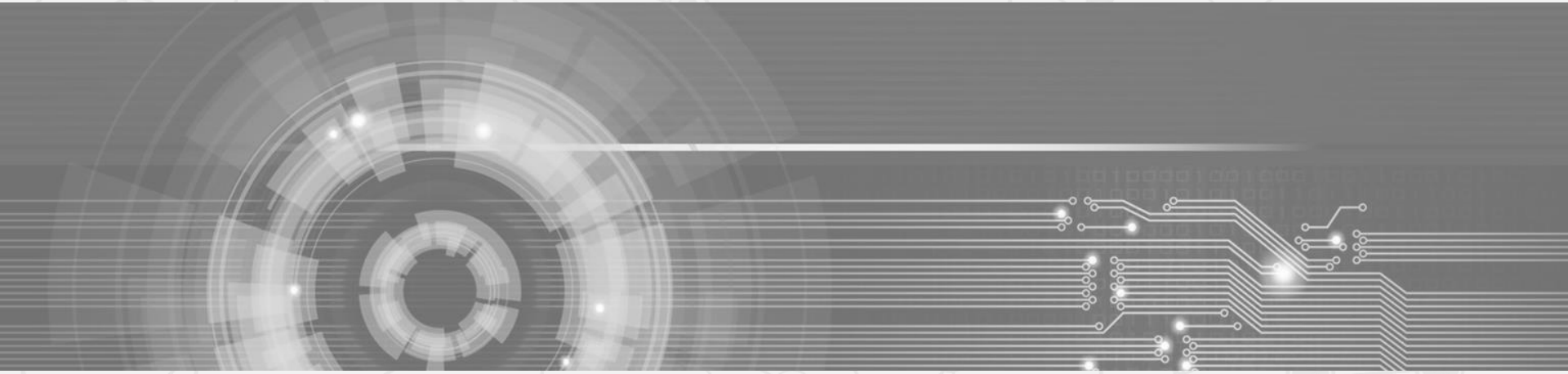
▶ 3.4.4 案例分析: VMware的网络虚拟化技术

- 案例分析: VMware的网络虚拟化技术

VMware的网络虚拟化技术主要是通过VMware vSphere中的vNetwork网络元素实现的，其虚拟网络架构如图所示。



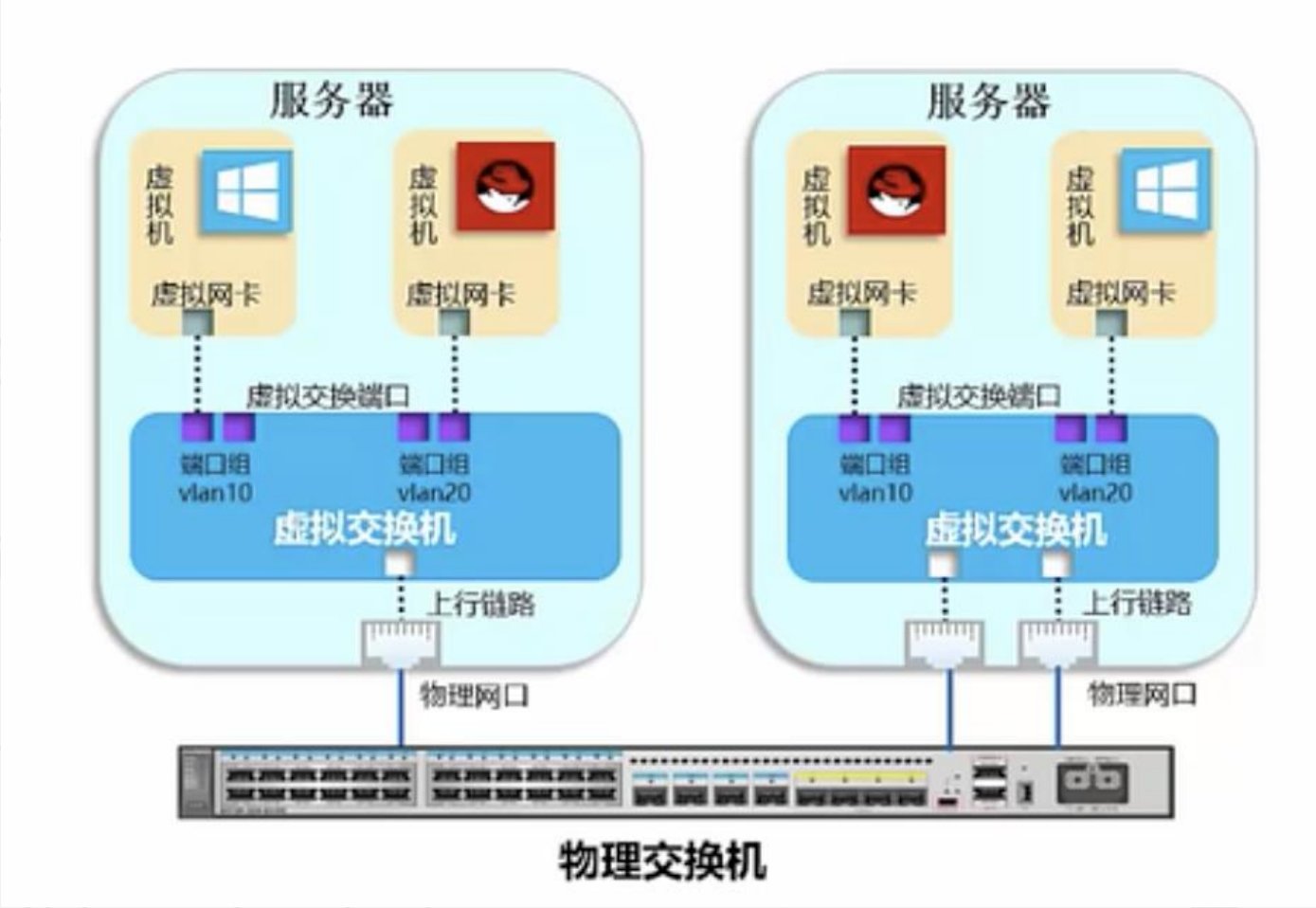
虚拟网络接口卡



- 每个虚拟机都可以配置一个或者多个虚拟网络接口卡vNIC。
- 安装在虚拟机上的客户操作系统和应用程序利用通用的设备驱动程序与vNIC进行通信。
- 在虚拟机的外部，vNIC拥有独立的MAC地址以及一个或多个IP地址，且遵守标准的以太网协议。

3.4 网络虚拟化

- 物理资源：物理网卡和物理交换机
- 虚拟资源：虚拟机（虚拟网卡）、虚拟交换机（端口组、上行链路）



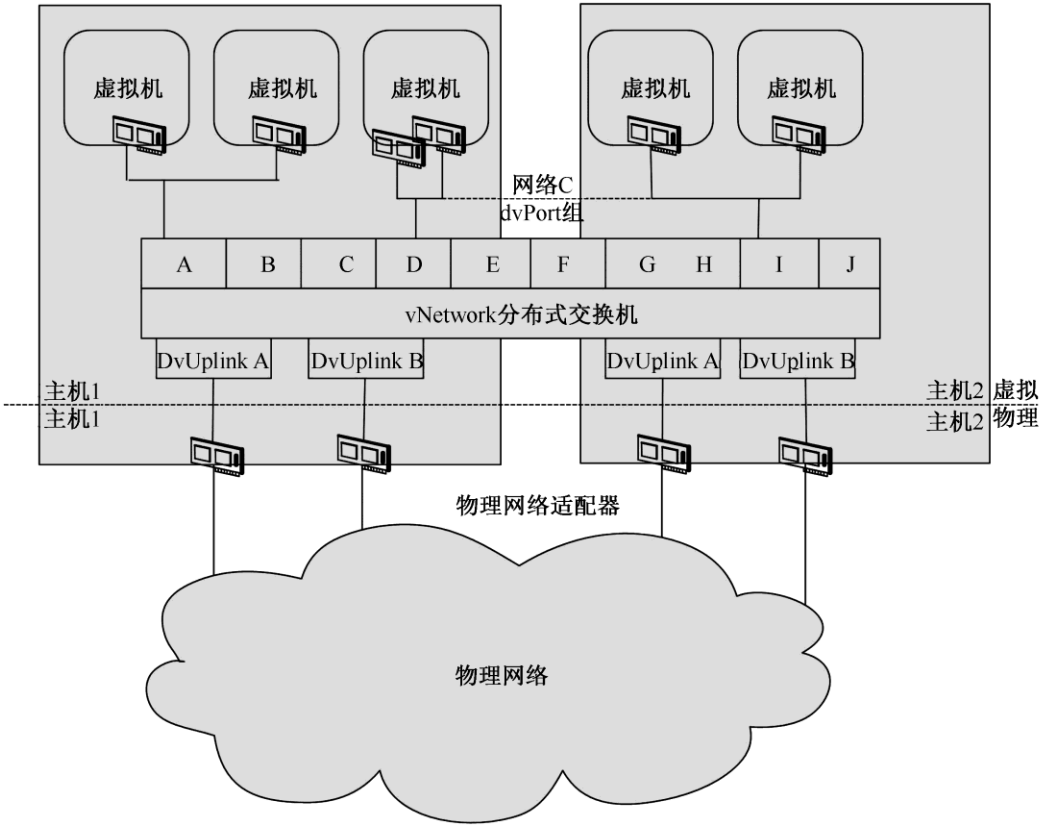
虚拟交换机vSwitch

- 虚拟交换机用来满足不同的**虚拟机**和**管理界面**进行互连。
- 每台服务器都有自己的虚拟交换机。
- 虚拟交换机的一端是与虚拟机相连的**端口组**，另一端是与虚拟机所在服务器上的物理以太网适配器相连的**上行链路**。
- 虚拟机通过与虚拟交换机上行链路相连的**物理以太网适配器**与外部环境连接。
- 虚拟交换机可将其上行链路连接到多个物理以太网适配器以**启用网卡绑定**。
- 通过网卡绑定，两个或多个物理适配器可用于**分摊流量负载**，或在出现物理适配器硬件故障或网络故障时提供被动故障切换。

分布式交换机

vNetwork分布式交换机（dvSwitch）是vSphere的新功能。每个dvSwitch都是一种可供虚拟机使用的网络集线器。

- 在虚拟机之间进行内部流量路由
- 连接物理以太网适配器链接外部网络
- 为每个vSwitch分配一个或多个dvPort组

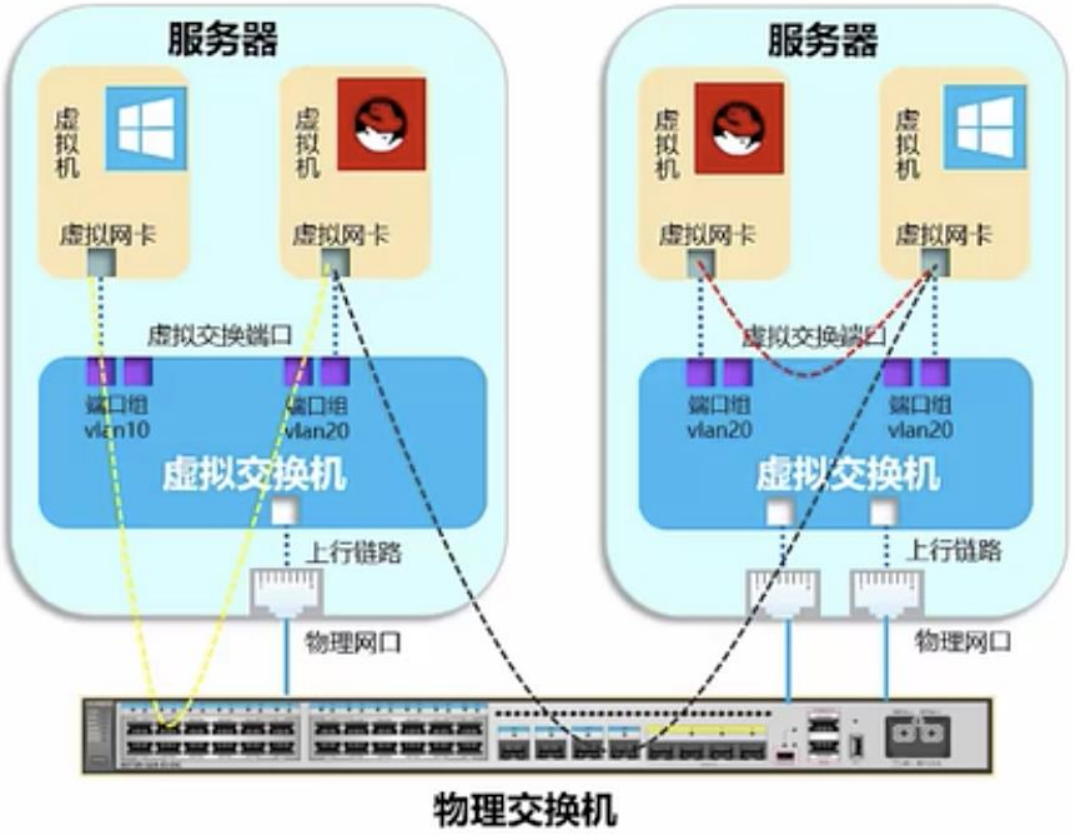


端口组 是虚拟环境特有的概念

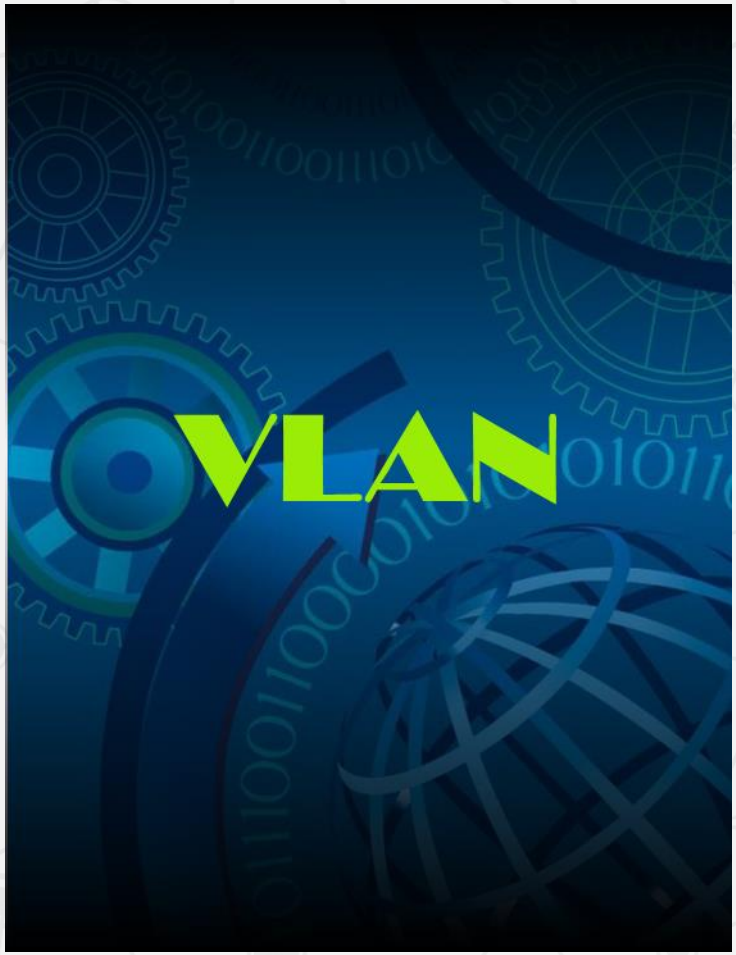
- 端口组是一种策略设置机制，这些策略用于管理与端口组相连的网络。
- 将端口组配置为执行策略，以提供增强的网络安全、网络分段、更佳的性能、高可用性及流量管理。

3.4 网络虚拟化

- 相同端口组不同服务器内的虚拟机通讯需要经过物理网络。
- 相同端口组相同服务器内的虚拟机通讯不需要经过物理网络。
- 不同端口组相同服务器的虚拟机通讯需要经过物理网络。



- VLAN



VLAN支持将虚拟网络与物理网络VLAN集成。

- 专用VLAN可以在专用网络中使用VLAN ID，而不必担心VLAN ID在较大型的网络中会出现重复。
- 流量调整定义平均带宽、峰值带宽和流量突发大小的QOS策略，设置策略以改进流量管理。
- 网卡绑定为个别端口组或网络设置网卡绑定策略，以分摊流量负载或在出现硬件故障时提供故障切换。

目录

桌面虚拟化

每个桌面镜像就是一个带有应用程序的操作系统，终端用户通过一个虚拟显示协议来访问他们的桌面系统。这样做的目的就是使用户的使用体验同他们使用桌面上的PC一样。

3.5 桌面虚拟化

- 3.5.1 桌面虚拟化简介
- 3.5.2 技术现状
- 3.5.3 案例分析

第一代桌面虚拟技术实现了在同一个独立的计算机硬件平台上，同时安装多个操作系统，并同时运行这些操作系统

第二代桌面虚拟化技术进一步将桌面系统的运行环境与安装环境、应用与桌面配置文件进行了拆分，从而大大降低了管理复杂度与成本，提高了管理效率。

3.5 桌面虚拟化

3.5.1 桌面虚拟化简介

▶ 3.5.2 技术现状

3.5.3 案例分析

技术现状

桌面虚拟化技术还面临着很多问题：

一 集中管理问题

虚拟化的服务器合并程度越高，此风险也越大。

二 集中存储问题

若是服务器出现了致命的故障，用户的数据可能丢失，整个平台将面临灾难。

三 虚拟化产品缺乏统一标准

各虚拟化产品厂商的产品间无法互通，一旦这个产品系列停止研发或其厂商倒闭，用户系统的持续运行、迁移和升级将会极其困难。

四 网络负载压力

如果用户使用的网络出现问题，桌面虚拟化发布的应用程序不能运行。

3.5 桌面虚拟化

3.5.1 桌面虚拟化简介

3.5.2 技术现状

▶ 3.5.3 案例分析

- **案例分析**

VMware View的主要部件如下：

View Connection Server（View连接服务器）

接收到的远程桌面用户请求重定向到相应的虚拟桌面、物理桌面或终端服务器。

View Manager Security Server（View安全连接服务器）

可选组件

View Administrator Interface（View管理接口程序）

用于配置View Connection Server、部署和管理虚拟桌面、控制用户身份验证。

View代理

安装在虚拟桌面依托的虚拟机、物理机或终端服务器上，安装后提供服务，可由View Manager Server管理。

- 案例分析

View Client（View客户端程序）

安装在需要使用“虚拟桌面”的计算机上，通过它可以与View Connection Server通信，从而允许用户连接到虚拟桌面。

View Client with Offline Desktop（View 客户端程序）

支持View脱机桌面，可以让用户“下载”vSphere Server中的虚拟机到“本地”运行。

View Composer

安装在vCenter Server上的软件服务，可以通过View Manager使用“克隆链接”的虚拟机

习题：

1．虚拟化技术在云计算中的哪些地方发挥了关键作用？

2．服务器虚拟化、存储虚拟化和网络虚拟化都有哪些实现方式？