# 第24讲讲云中网络：自己拿地成本高，购买公寓更灵活

虚拟机技术催生了云计算技术的发展。云计算的关键技术是虚拟机。

在数据中心，使用qemu-kvm搭建虚拟机。

把物理机比喻为自己拿地盖房子，而虚拟机则相当于购买公寓，更加灵活方面，随时可买可卖。

使用的是软件模拟硬件的方式：

* 多个虚拟机轮流使用物理CPU
* 内存也是使用虚拟内存映射的方式
* 盘在一块大的文件系统上创建一个N个G的文件

## 虚拟机网卡原理

虚拟机有一个TAP虚拟网卡。

网络包转换成为文件流，写入字符设备。

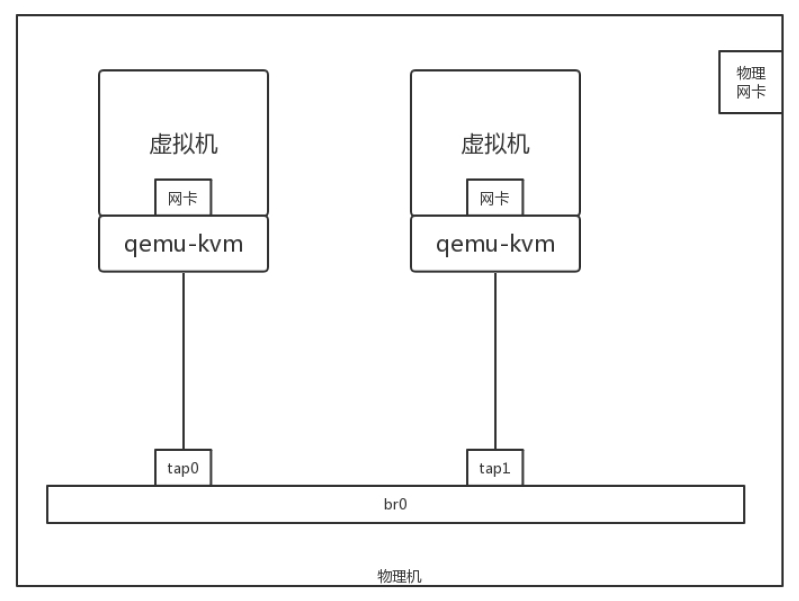
文件流交给TUN/TAP的虚拟网卡驱动

驱动从文件流转换成网络包，交给TCP/IP协议栈，从虚拟TAP网卡发出来，成为标准网络包。

## 虚拟网卡接入

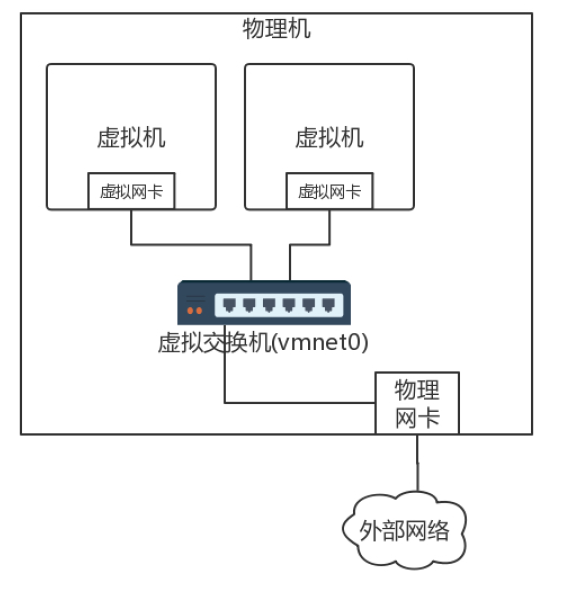
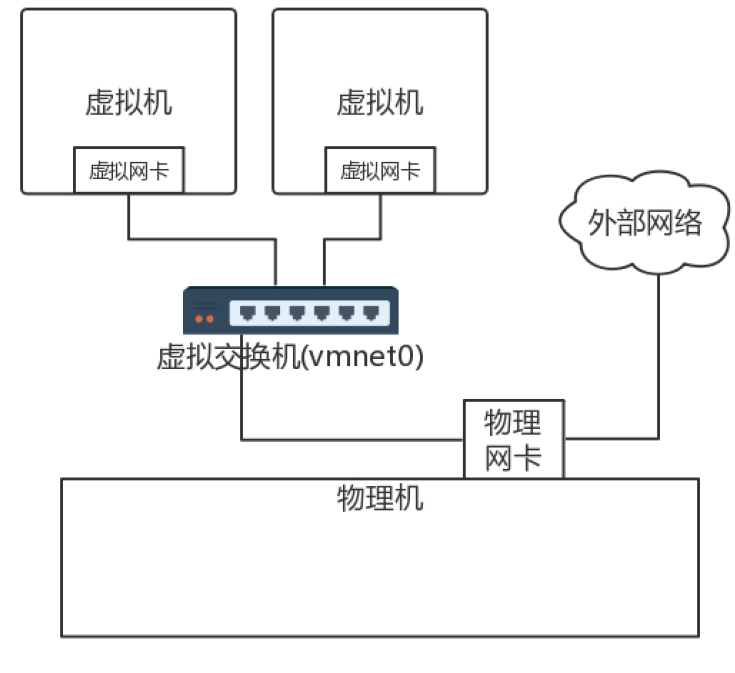
使用网桥，类似于交换机。

在linux上，命令brctl addbr br0，可以创建网桥。将两个虚拟机的网卡都连接到网桥上。这样两台机器就可以相互通信了。对应的是host-only模式。



**如果要连接到外部，有两种方式：**

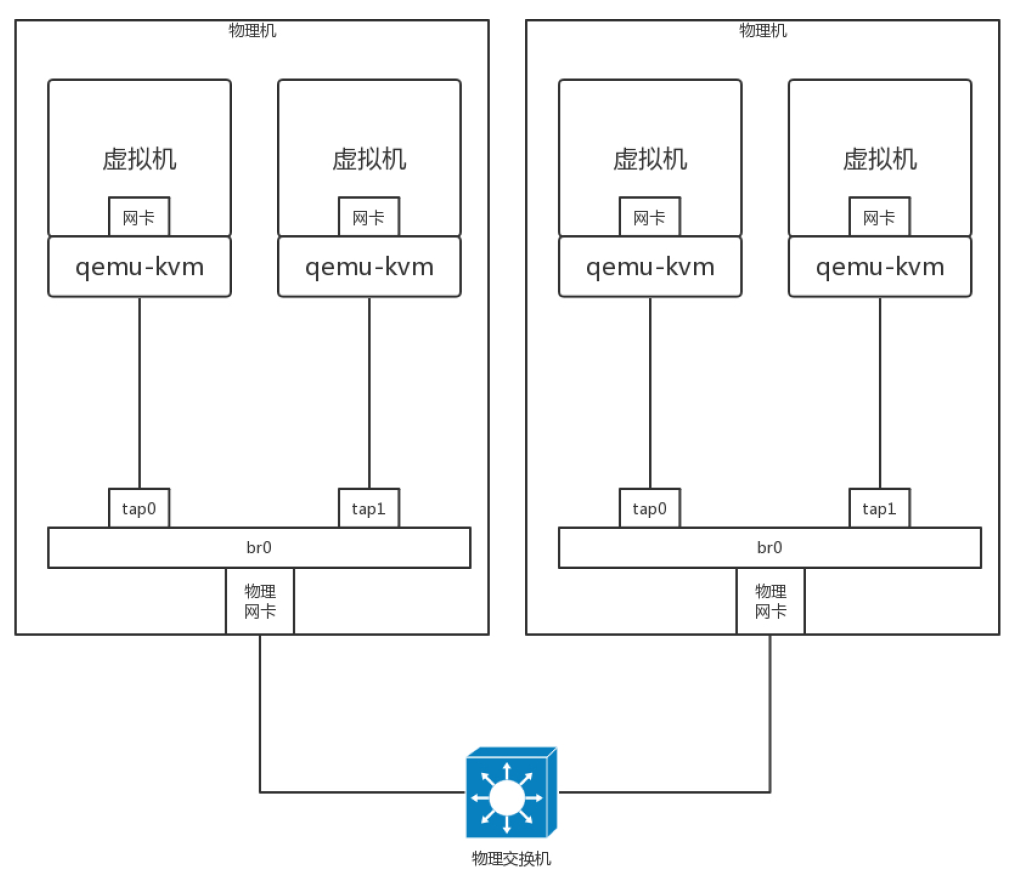
### 1.桥接：

笔记本上的多张网卡其实就是虚拟交换机的。

在桥接模式下，物理网卡也连接到这个虚拟交换机上。此时，你的虚拟机和物理机都是在同一个网段上。相当于一个网桥有三台机器。如右图所示。

在**数据中心**里面，采取的也是类似的技术，只不过都是Linux，在每台机器上都创建网桥br0，虚拟机的网卡都连到br0上，物理网卡也连到br0上，所有的br0都通过物理网卡出来连接到物理交换机上。



这种方式解决了跨物理机通信的问题。

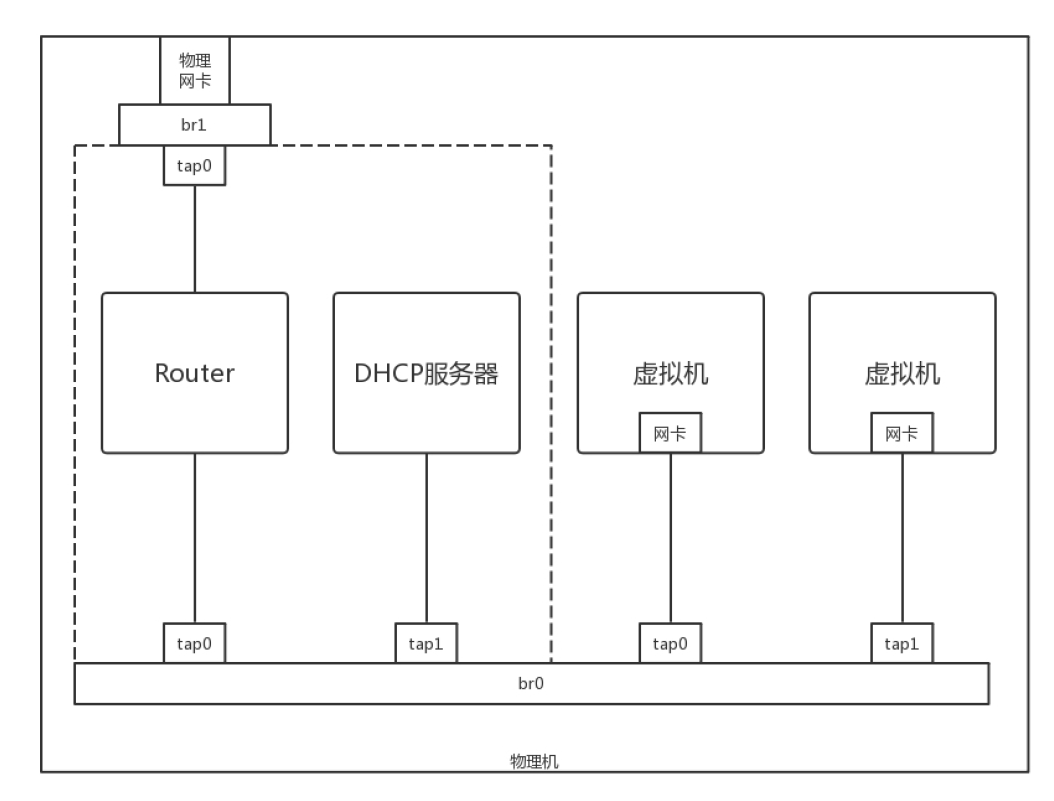
但存在广播问题。因此，桥接模式只适用于小规模的模式。

### NAT模式

最显著的特征是虚拟机的IP地址和物理机的IP地址不在同一个网段。

虚拟机的地址都是通过虚拟DHCP服务器配置的，动态分配ip。为什么桥接方式不需要呢？因为桥接将网络打平了，IP地址的分配是由物理机做的。

在这个模式下，物理机和虚拟机的角色就不是扁平化的了。此时，物理机的地址就相当于网关地址，所有从这里出去的虚拟机的地址都NAT成为网关地址。



这里，路由器和DHCP服务器都是自己的物理机扮演的角色。可以对物理机手动的配置。

这里可以简化配置，不用DHCP服务器。手动配置每台虚拟机的地址：iptables -t nat -A POSTROUTING -o ethX -j MASQUERADE。所有的网桥连在物理网卡ethX上进行NAT。

设置net.ipv4.ip\_forward = 1，开启物理机的转发功能，直接做路由器。

虚拟机之间的隔离问题是通过VLAN的方式隔离的。具体不详细展开。