

LAN 表示 Local Area Network，本地局域网，通常使用 Hub 和 Switch 来连接 LAN 中的计算机。  
一般来说，两台计算机连入同一个 Hub 或者 Switch 时，它们就在同一个 LAN 中。

一个 LAN 表示一个广播域。

其含义是：LAN 中的所有成员都会收到任意一个成员发出的广播包。

VLAN 表示 Virtual LAN。一个带有 VLAN 功能的switch 能够将自己的端口划分出多个 LAN。  
计算机发出的广播包可以被同一个 LAN 中其他计算机收到，但位于其他 LAN 的计算机则无法收到。

简单地说，VLAN 将一个交换机分成了多个交换机，限制了广播的范围，在二层将计算机隔离到不同的 VLAN 中。

比方说，有两组机器，Group A 和 B。  
我们想配置成 Group A 中的机器可以相互访问，Group B 中的机器也可以相互访问，但是 A 和 B 中的机器无法互相访问。

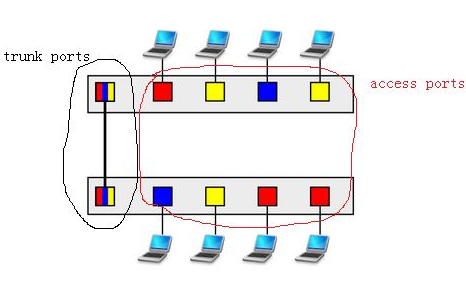
一种方法是使用两个交换机，A 和 B 分别接到一个交换机。

另一种方法是使用一个带 VLAN 功能的交换机，将 A 和 B 的机器分别放到不同的 VLAN 中。

**请注意，VLAN 的隔离是二层上的隔离，A 和 B 无法相互访问指的是二层广播包（比如 arp）无法跨越 VLAN 的边界。  
但在三层上（比如IP）是可以通过路由器让 A 和 B 互通的。概念上一定要分清。**

现在的交换机几乎都是支持 VLAN 的。

通常交换机的端口有两种配置模式： Access 和 Trunk。看下图



**Access 口**这些端口被打上了 VLAN 的标签，表明该端口属于哪个 VLAN。

不同 VLAN 用 VLAN ID 来区分，VLAN ID 的 范围是 1-4096。

Access 口都是直接与计算机网卡相连的，这样从该网卡出来的数据包流入 Access 口后就被打上了所在 VLAN 的标签。

Access 口只能属于一个 VLAN。

**Trunk 口**假设有两个交换机 A 和 B。

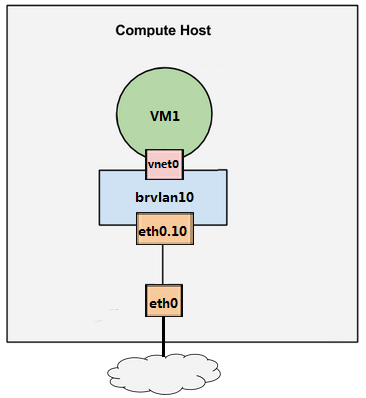
A 上有 VLAN1（红）、VLAN2（黄）、VLAN3（蓝）；B 上也有 VLAN1、2、3

那如何让 AB 上相同 VLAN 之间能够通信呢？

办法是将 A 和 B 连起来，而且连接 A 和 B 的端口要允许 VLAN1、2、3 三个 VLAN 的数据都能够通过。  
这样的端口就是Trunk口了。

VLAN1、2、3 的数据包在通过 Trunk 口到达对方交换机的过程中始终带着自己的 VLAN 标签。

了解了 VLAN 的概念之后，我们来看 KVM 虚拟化环境下是如何实现 VLAN 的。还是先看图，



eth0 是宿主机上的物理网卡，有一个命名为 eth0.10 的子设备与之相连。

eth0.10 就是 VLAN 设备了，其 VLAN ID 就是 VLAN 10。

eth0.10 挂在命名为 brvlan10 的 Linux Bridge 上，虚机 VM1 的虚拟网卡 vent0 也挂在 brvlan10 上。

这样的配置其效果就是：

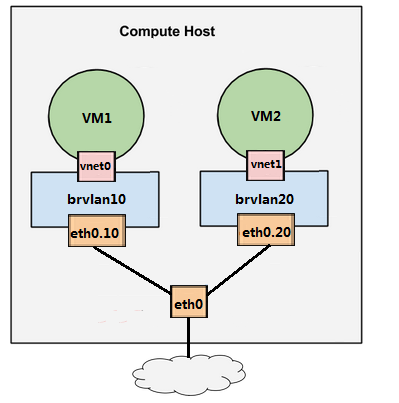
宿主机用软件实现了一个交换机（当然是虚拟的），上面定义了一个 VLAN10。

eth0.10，brvlan10 和 vnet0 都分别接到 VLAN10 的 Access口上。而 eth0 就是一个 Trunk 口。  
VM1 通过 vnet0 发出来的数据包会被打上 VLAN10 的标签。

eth0.10 的作用是：定义了 VLAN10

brvlan10 的作用是：Bridge 上的其他网络设备自动加入到 VLAN10 中

我们再增加一个 VLAN20，见下图



这样虚拟交换机就有两个 VLAN 了，VM1 和 VM2 分别属于 VLAN10 和 VLAN20。

对于新创建的虚机，只需要将其虚拟网卡放入相应的 Bridge，就能控制其所属的 VLAN。

VLAN 设备总是以母子关系出现，母子设备之间是一对多的关系。

一个母设备（eth0）可以有多个子设备（eth0.10，eth0.20 ……），而一个子设备只有一个母设备。  
  
下一节我们通过实验来实践 VLAN。