用VLANs隔离虚拟机流量

本文是一篇翻译文章，翻译自Open vSwitch的官方文档——[Isolating VM Traffic Using VLANs](http://openvswitch.org/support/config-cookbooks/vlan-configuration-cookbook/" \t "_blank)。系博主在尝试搭建ovs构建VLAN时百度上资料过少，算是填补一些空白。不喜欢看中文或者用能力看英文的同学请移步。

这篇配置手册旨在使用VLANs隔离虚拟机流量。

配置环境

该教程假设你的环境是按如下小节配置。

两个物理网络

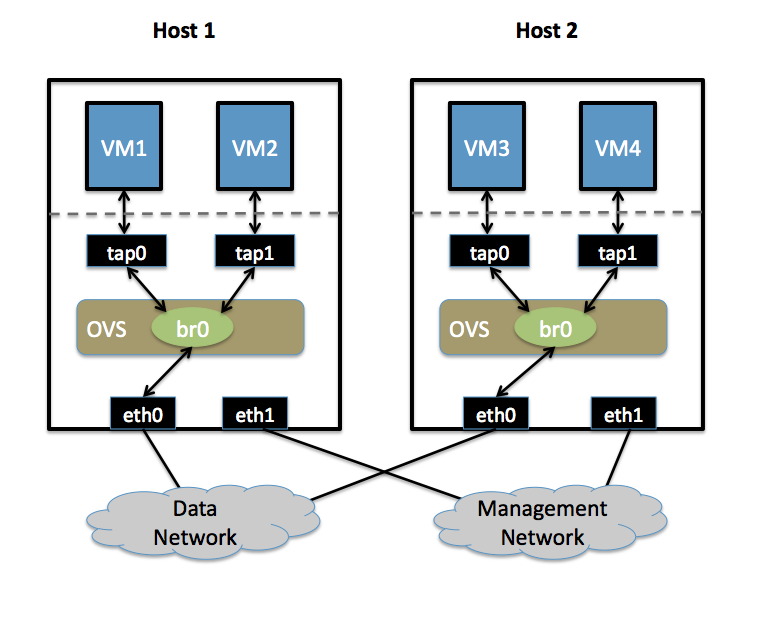
* 数据网络：虚拟机数据流量以太网（Ethernet），用来在虚拟机之间传输VLAN标记的流量。你的物理交换机要能够转发VLAN标记的流量并且物理交换机端口应该配置为VLAN中继（VLAN trunks）。（一般情况下这是默认设置。而如何配置你的物理交换机不在本文讨论范围。）
* 管理网络：该网络并非必须存在，但却是一个简单的方式给予你的物理机一个远程连接的IP，因为IP地址不能直接赋给eth0（下面会进行更详细的说明）。

两台物理机

你的实验环境应该有两台主机，我们暂且称为Host1和Host2 。且两个主机都运行了Open vSwitch软件。每个主机都有两张网卡——eth0和eth1，按如下方式配置：

* eth0连接到数据网络，上面不分配IP地址。
* eth1连接到管理网络（如果有的话），上面有一个IP地址可以用来连接到该主机进行管理。

四台虚拟机

每台主机运行两个虚拟机（VM）。VM1和VM2运行在Host1上，VM3和VM4运行在Host2上。   
每台虚拟机都有一个网络接口（interface），在宿主机上表现为Linux设备（比如tap0）。（注意：对于Xen/XenServer，虚拟机网络接口在宿主机上的名字类似“vif1.0”。其他Linux系统中可能显示为“vnet0”、“vnet1”等。）   
下面的图描述了这篇配置手册里假设的实验环境：   


配置步骤

在Host1上按如下步骤配置：   
1. 创建一个OVS网桥（bridge）：   
ovs-vsctl add-br br0   
2. 将eth0加入网桥（默认情况，所有OVS端口都是VLAN中继的，所以eth0会发送所有VLAN数据）：   
ovs-vsctl add-port br0 eth0   
注意：当你将eth0加入到OVS网桥中，任何分配给eth0的IP地址都将失效。所以在把eth0加入到OVS网桥前，分配给eth0的IP地址应该转移到另一个网络接口上。这就是我们要通过eth1来单独管理网络连接的原因。  
3. 将VM1作为VLAN 100的一个“接入口”。这表示从VM1到OVS的流量会被取消标记（untagged）并被当做VLAN 100的一部分：   
ovs-vsctl add-port br0 tap0 tag=100   
4. 将VM2加入到VLAN 200.

在Host2上重复下面步骤：   
1. 配置带eth0的网桥为一个VLAN中继：   
ovs-vsctl add-br br0 ovs-vsctl add-port br0 eth0   
2. 将VM3加入到VLAN 100：   
ovs-vsctl add-port br0 tap0 tag=100   
3. 将VM4加入到VLAN 200：   
ovs-vsctl add-port br0 tap1 tag=200

测试

VM1应该能ping通VM3，因为它们在同一个VLAN中。   
VM2也能ping通VM4，理由同上。   
而从VM1/VM3 ping VM2/VM4则不行，因为它们属于不同VLAN。如果你有一个路由器配置为转发这两个VLAN的包，那应该能ping通，但是到达VM3的包的源MAC地址是路由的而不是VM1的。