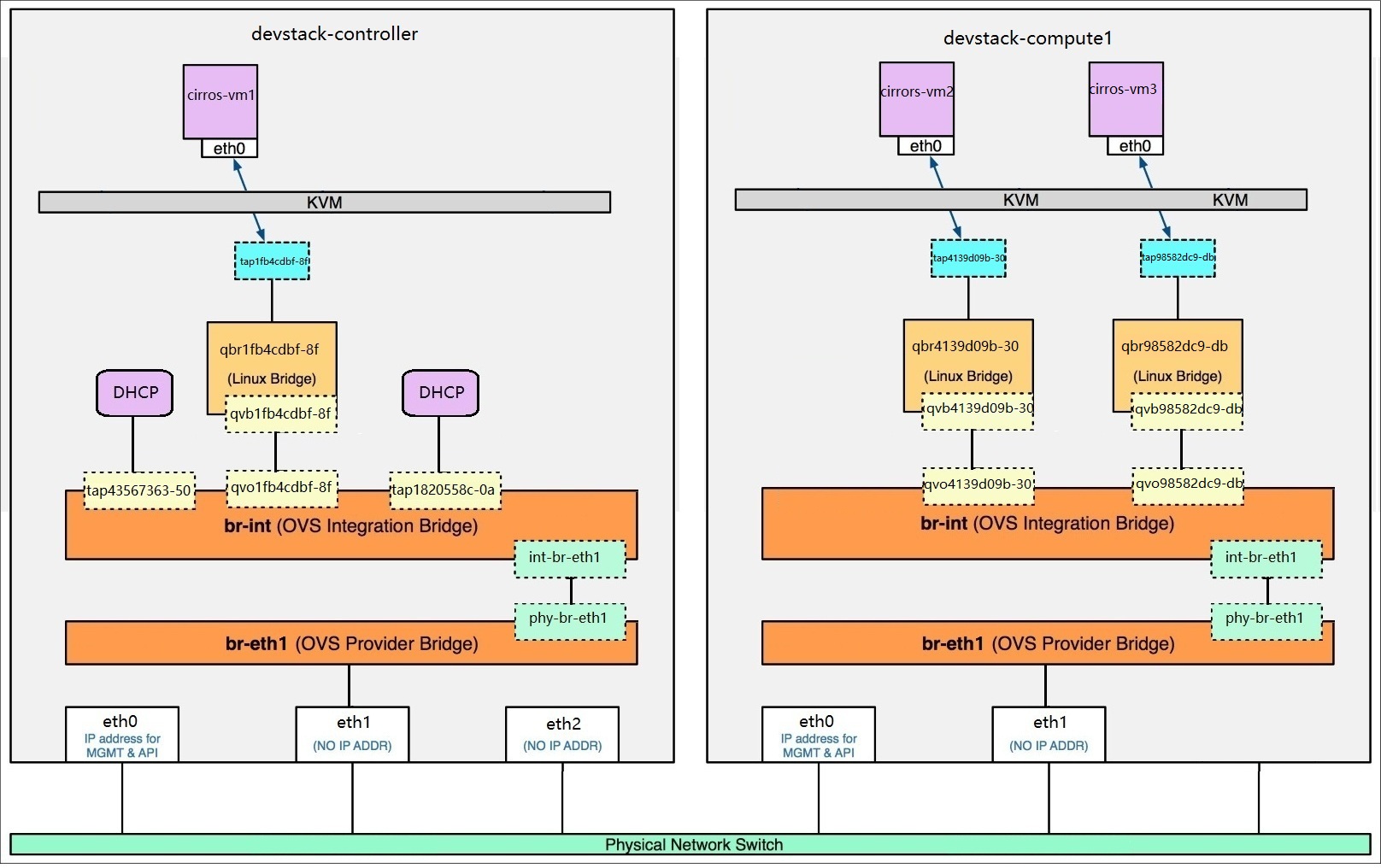


上一节我们完成了 OVS vlan 环境的搭建，当前拓扑结构如下：

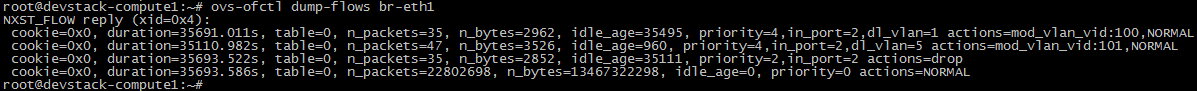


cirros-vm1 位于控制节点，属于 vlan100。   
cirros-vm2 位于计算节点，属于 vlan100。   
cirros-vm3 位于计算节点，属于 vlan101。

今天详细分析 OVS 如何实现 vlan100 和 vlan101 的隔离。  
与 Linux Bridge driver 不同，Open vSwitch driver 并不通过 eth1.100, eth1.101 等 VLAN interface 来隔离不同的 VLAN。  
所有的 instance 都连接到同一个网桥 br-int，  
**Open vSwitch 通过 flow rule（流规则）来指定如何对进出 br-int 的数据进行转发，进而实现 vlan 之间的隔离**。  
  
具体来说：当数据进出 br-int 时，flow rule 可以修改、添加或者剥掉数据包的 VLAN tag，  
Neutron 负责创建这些 flow rule 并将它们配置到 br-int，br-eth1 等 Open vSwitch 上。

下面我们就来研究一下当前的 flow rule。

查看 flow rule 的命令是 ovs-ofctl dump-flow <bridge>  
首先查看计算节点 br-eth1 的 flow rule:

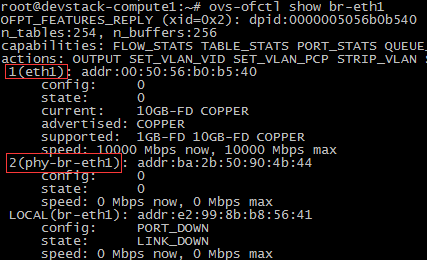


br-eth1 上配置了四条 rule，每条 rule 有不少属性，其中比较重要的属性有：

**priority**rule 的优先级，值越大优先级越高。Open vSwitch 会按照优先级从高到低应用规则。

**in\_port**inbound 端口编号，每个 port 在 Open vSwitch 中会有一个内部的编号。  
可以通过命令 ovs-ofctl show <bridge>

查看 port 编号。  
比如 br-eth1：



eth1 编号为 1；phy-br-eth1 编号为 2。

**dl\_vlan**数据包原始的 VLAN ID。

**actions**对数据包进行的操作。

br-eth1 跟 VLAN 相关的 flow rule 是前面两条，下面我们来详细分析。

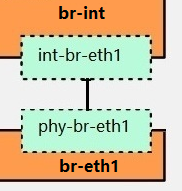
清晰起见，我们只保留重要的信息，如下：

priority=4,in\_port=2,dl\_vlan=1 actions=mod\_vlan\_vid:100,NORMAL

priority=4,in\_port=2,dl\_vlan=5 actions=mod\_vlan\_vid:101,NORMAL

第一条的含义是：

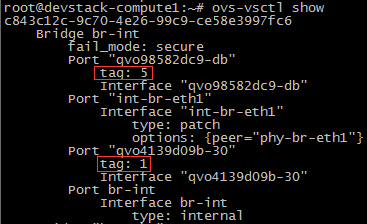
从 br-eth1 的端口 phy-br-eth1（in\_port=2）接收进来的包，如果 VLAN ID 是 1（dl\_vlan=1），  
那么需要将 VLAN ID 改为 100（actions=mod\_vlan\_vid:100）



从上面的网络结构我们可知，phy-br-eth1 连接的是 br-int，phy-br-eth1 的 inbound 包实际上就是 instance 通过 br-int 发送给物理网卡的数据。

那么怎么理解将 VLAN ID 1 改为 VLAN ID 100 呢？

请看下面计算节点 ovs-vsctl show 的输出：



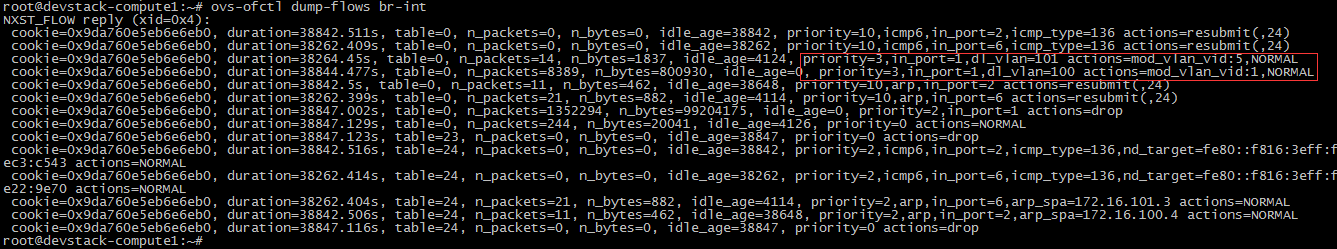
br-int 通过 tag 隔离不同的 port，这个 tag 可以看成内部的 VLAN ID。

从 qvo4139d09b-30（对应 cirros-vm2，vlan100）进入的数据包会被打上 1 的 VLAN tag。

从 qvo98582dc9-db（对应 cirros-vm3，vlan101）进入的数据包会被打上 5 的 VLAN tag。

因为 br-int 中的 VLAN ID 跟物理网络中的 VLAN ID 并不相同，所以当 br-eth1 接收到 br-int 发来的数据包时，  
需要对 VLAN 进行转换。Neutron 负责维护 VLAN ID 的对应关系，并将转换规则配置在 flow rule 中。

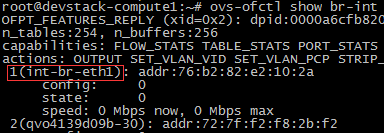
理解了 br-eth1 的 flow rule，我们再来分析 br-int 的 flow rule。



最关键的是下面两条：

priority=3,inport=1,dl\_vlan=100 actions=mod\_vlan\_vid:1,NORMAL

priority=3,inport=1,dl\_vlan=101 actions=mod\_vlan\_vid:5,NORMAL



port 1 为 int-br-eth1，那么这两条规则的含义就应该是：

1. 从物理网卡接收进来的数据包，如果 VLAN 为 100，则改为内部 VLAN 1。

2. 从物理网卡接收进来的数据包，如果 VLAN 为 101，则将为内部 VLAN 5。

简单的说，数据包在物理网络中通过 VLAN 100 和 VLAN 101 隔离，在计算节点 OVS br-int 中则是通过内部 VLAN 1 和 VLAN 5 隔离。

控制节点的 flow rule 非常类似，留给大家分析。

到这里，我们已经完成了 Neutron OVS vlan 的学习，下节开讨论 OVS 环境下的路由。