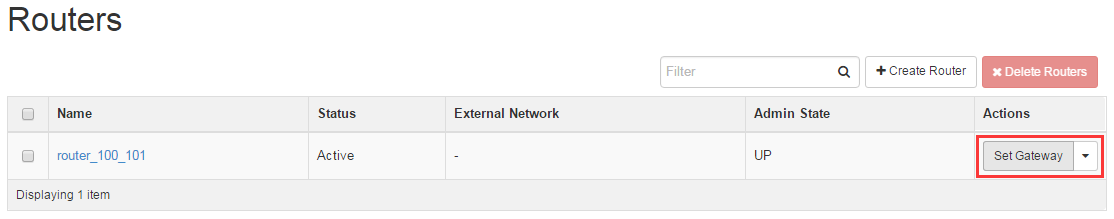


本节我们会将上节创建的 ext\_net 连接到 router，并验证内外网的连通性。

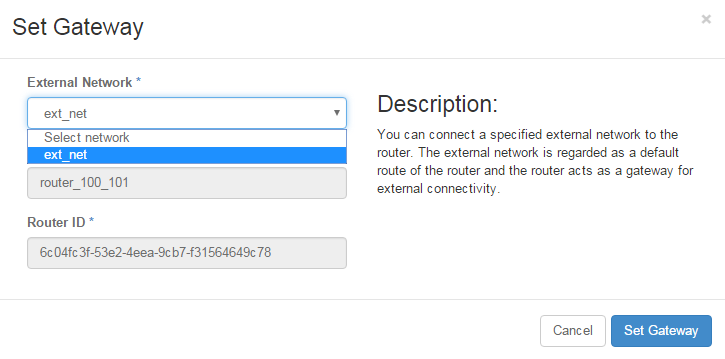
更重要的，我们会分析隐藏在表象之下的原理。

将外网连接到 Neutron 的虚拟路由器，这样 instance 才能访问外网。

点击菜单 Project -> Network -> Routers 进入 router 列表。



点击 router\_100\_101 的 “Set Gateway” 按钮。

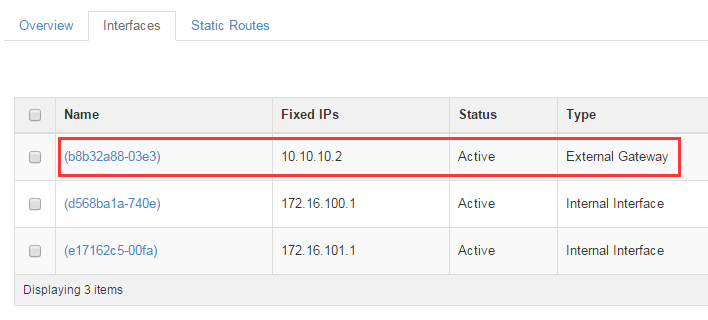


在 “External Network” 下拉列表中选择 ext\_net，点击 “Set Gateway”。



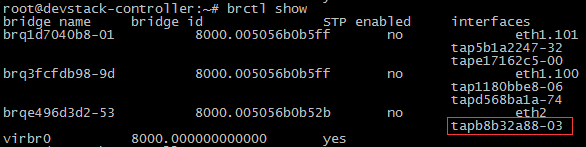
外网设置成功。

我们需要看看 router 发生了什么变化。 点击 “router\_100\_101” 链接，打开 “Interfaces” 标签页

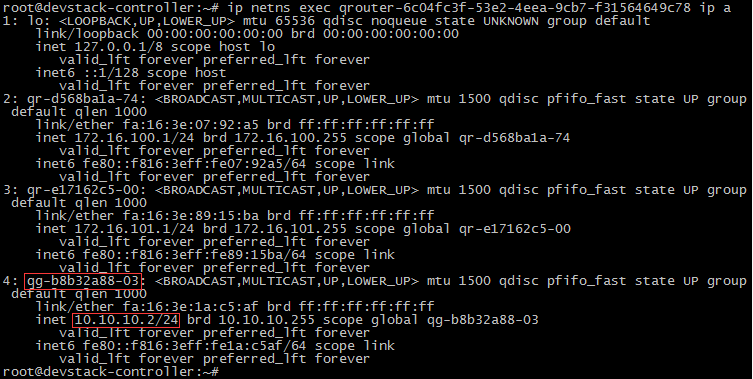


router 多了一个新的 interface，IP 为 10.10.10.2。 该 interface 用于连接外网 ext\_net。

查看控制节点的网络结构，外网 bridge 上已经连接了 router 的 tap 设备 tapb8b32a88-03。



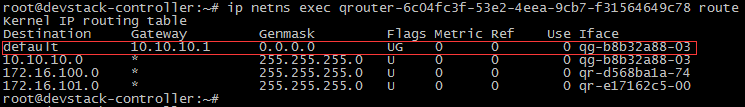
在 router 的 namespace 中查看 tapb8b32a88-03 的 veth pair 设备。



该 veth pair 命名为 qg-b8b32a88-03，上面配置了 IP 10.10.10.2。

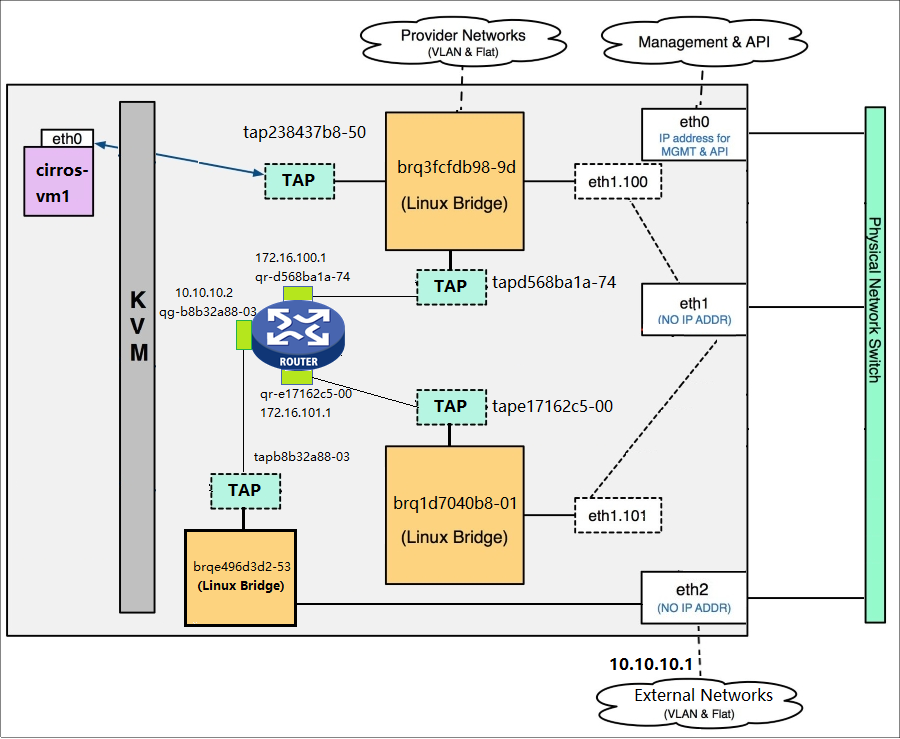
router 的每个 interface 在 namespace 中都有对应的 veth。 如果 veth 用于连接租户网络，命名格式为 qr-xxx，比如 qr-d568ba1a-74 和 qr-e17162c5-00。 如果 veth 用于连接外部网络，命名格式为 qg-xxx，比如 qg-b8b32a88-03。

查看 router 的路由表信息。

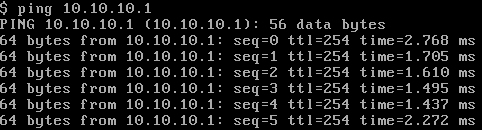


可以看到默认网关为 10.10.10.1。 意味着对于访问 vlan100 和 vlan101 租户网络以外的所有流量，router\_100\_101 都将转发给 ext\_net 的网关 10.10.10.1。

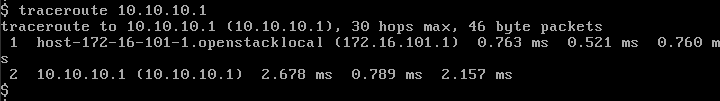
现在 router\_100\_101 已经同时连接了 vlan100, vlan101 和 ext\_net 三个网络，如下图所示：



下面我们在 cirros-vm3 上测试一下。



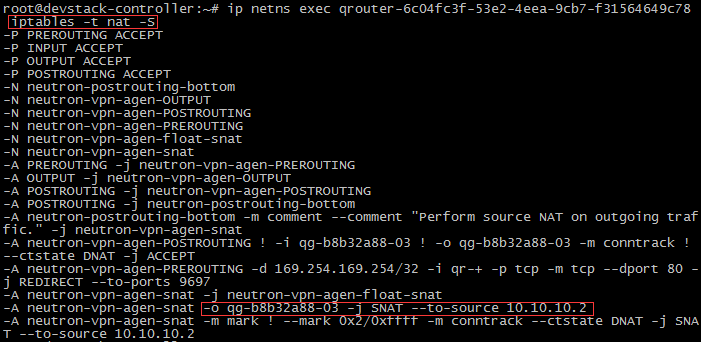
cirros-vm3 位于计算节点，现在已经可以 Ping 到 ext\_net 网关 10.10.10.1 了。 通过 traceroute 查看一下 cirros-vm3 到 10.10.10.1 的路径



数据包经过两跳到达 10.10.10.1 网关。 1. 数据包首先发送到 router\_100\_101 连接 vlan101 的 interface（172.16.101.1）。 2. 然后通过连接 ext\_net 的 interface（10.10.10.2） 转发出去，最后到达 10.10.10.1。

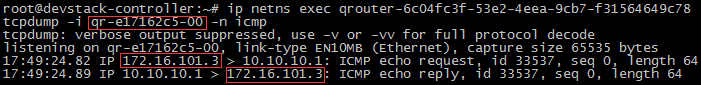
当数据包从 router 连接外网的接口 qg-b8b32a88-03 发出的时候，会做一次 Source NAT，即将包的源地址修改为 router 的接口地址 10.10.10.2，这样就能够保证目的端能够将应答的包发回给 router，然后再转发回源端 instance。

可以通过 iptables 命令查看 SNAT 的规则。

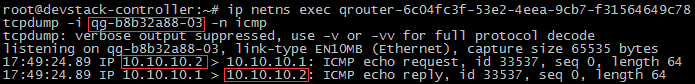


当 cirros-vm3（172.16.101.3） Ping 10.10.10.1 时，可用通过 tcpdump 分别观察 router 两个 interface 的 icmp 数据包来验证 SNAT 的行为。

vlan101 interface qr-e17162c5-00 的 tcpdump 输出：



ext\_net interface qg-b8b32a88-03 的 tcpdump 输出：



SNAT 让 instance 能够直接访问外网，但外网**还不能直接访问 instance。**因为 instance 没有外网 IP。

这里 “直接访问 instance” 是指通信连接由外网发起，例如从外网 SSH cirros-vm3。

这个问题可以通过 floating IP 解决，下一节我们将讨论浮动 IP。