neutron网络入门

Neutron是OpenStack核心项目之一，提供云计算环境下的虚拟网络功能。Neutron的功能日益强大，并在Horizon面板中已经集成该模块。作为Neutron的核心开发者之一，个人觉得Neutron完全代替Nova Network模块作为云计算网络管理中心是必然趋势。要使用好OpenStack,了解Neutron概念及其相应操作就显得格外重要。为此目的，这篇博客主要讲述Neutron网络的一些基本概念，网络规划和Horizon中如何使用Neutron中的网络功能。

**Neutron基本概念**

1. 网络

在普通人的眼里，网络就是网线和供网线插入的端口，一个盒子会提供这些端口。对于网络工程师来说，网络的盒子指的是交换机和路由器。所以在物理世界中，网络可以简单地被认为包括网线，交换机和路由器。当然，除了物理设备，我们还有软的物件：IP地址，交换机和路由器的配置和管理软件以及各种网络协议。要管理好一个物理网络需要非常深的网络专业知识和经验。

Neutron网络目的是（为OpenStack云更灵活地）划分物理网络，在多租户环境下提供给每个租户独立的网络环境。另外，Neutron提供API来实现这种目标。Neutron中“网络”是一个可以被用户创建的对象，如果要和物理环境下的概念映射的话，这个对象相当于一个巨大的交换机，可以拥有无限多个动态可创建和销毁的虚拟端口。

1. 端口

在物理网络环境中，端口是用于连接设备进入网络的地方。Neutron中的端口起着类似的功能，它是路由器和虚拟机挂接网络的着附点。

1. 路由器

和物理环境下的路由器类似，Neutron中的路由器也是一个路由选择和转发部件。只不过在Neutron中，它是可以创建和销毁的软部件。

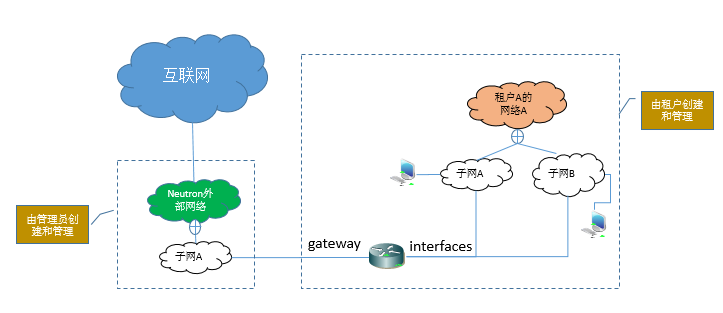
1. 子网

简单地说，子网是由一组IP地址组成的地址池。不同子网间的通信需要路由器的支持，这个Neutron和物理网络下是一致的。Neutron中子网隶属于网络。

**Neutron网络的一种典型结构**

有这么多的基本概念，使用起来是不是很麻烦？其实只要我们好好梳理一下，neutron的基本操作还是很简单的。

首先我们规划一下我们的网络。Neutron典型的网络结构如下图所示：

[](http://www.ustack.com/wp-content/uploads/2013/09/11.png)

在这个图中，我们有一个和互联网（互联网可以由其它网络代替，比如办公网络）连接的外部网络。这个外部网络是租户虚拟机访问互联网或者互联网访问虚拟机的途径。外部网络有一个子网，它是一组在互联网上可寻址的IP地址。一般情况下，外部网络只有一个（neutron是支持多个外部网络的），且由管理员创建。租户网络可由租户任意创建。当一个租户的网络上的虚拟机需要和外部网络以及互联网通信时，这个租户就需要一个路由器。路由器有两种臂，一种是gateway网关臂，另一种是interfaces接口臂。网关臂只有一个，连接外部网。接口臂可以有多个，连接租户网络的子网。经过这样的网络规划，我们有下面的步骤来实施：

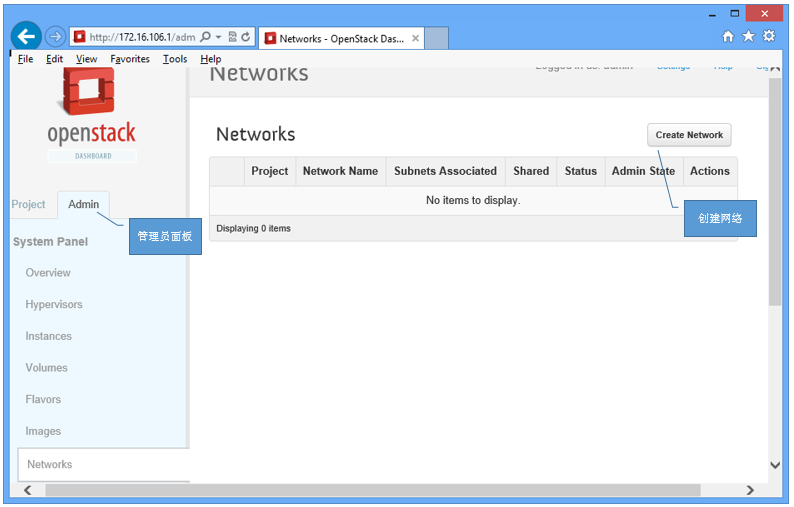
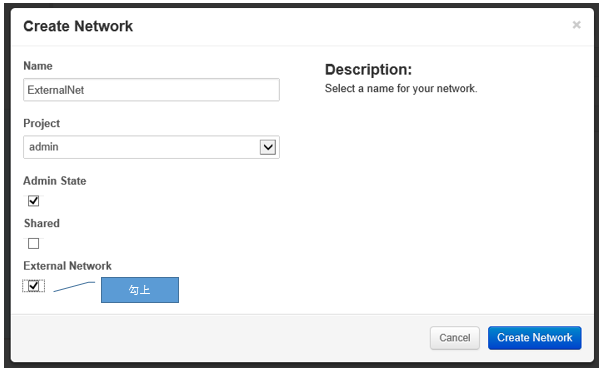
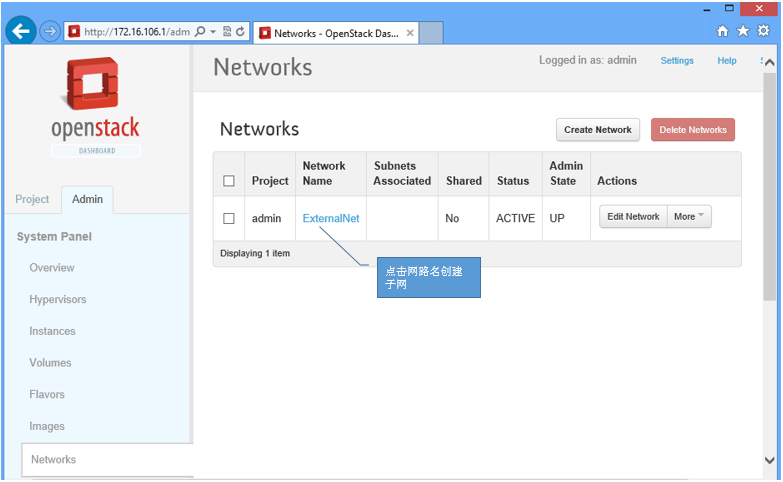
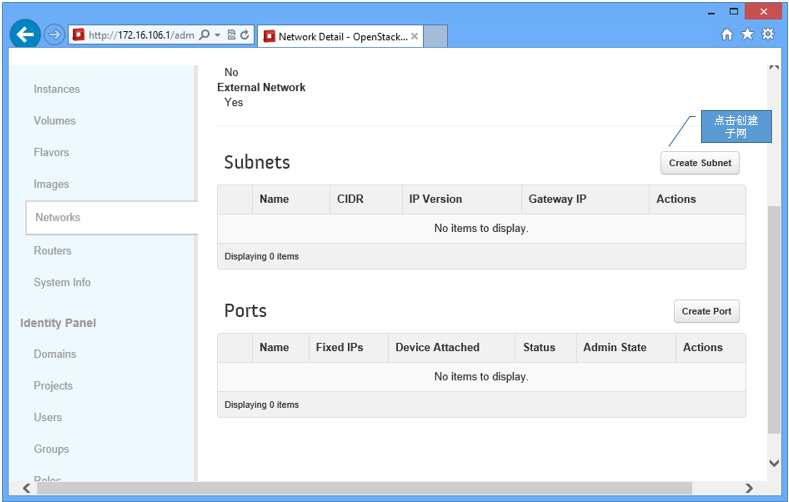
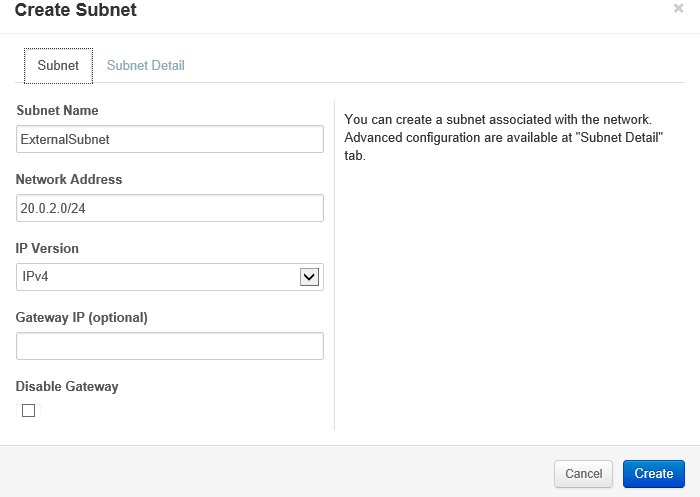
1. 首先管理员拿到一组可以在互联网上寻址的IP地址，并且创建一个外部网络和子网
2. 租户创建一个网络和子网
3. 租户创建一个路由器并且连接租户子网和外部网络
4. 租户创建虚拟机

**Horizon上操作网络**

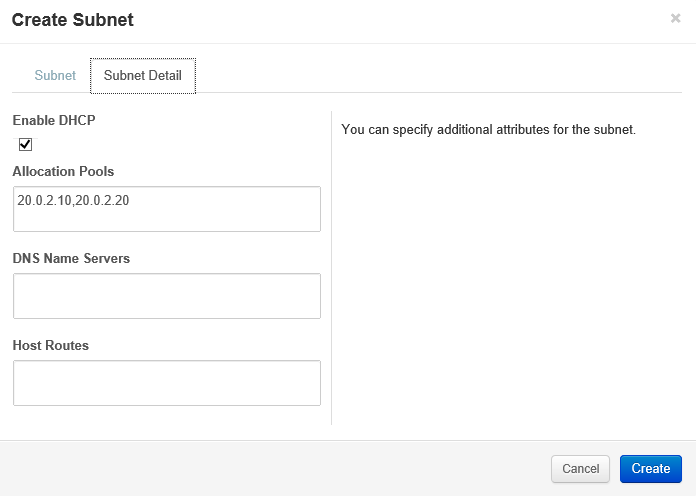
现在我们规划好了网络，我们就可以在Horizon上进行操作了。

**管理员创建外网**

我们说过外网要由管理员创建。假设我们拿到的外部网络的IP地址是20.0.2.0/24，可用的地址段是20.0.2.10-20.0.2.20，网关是20.0.2.1。我们现在就以管理员的身份在horzion上创建一个外网和子网：

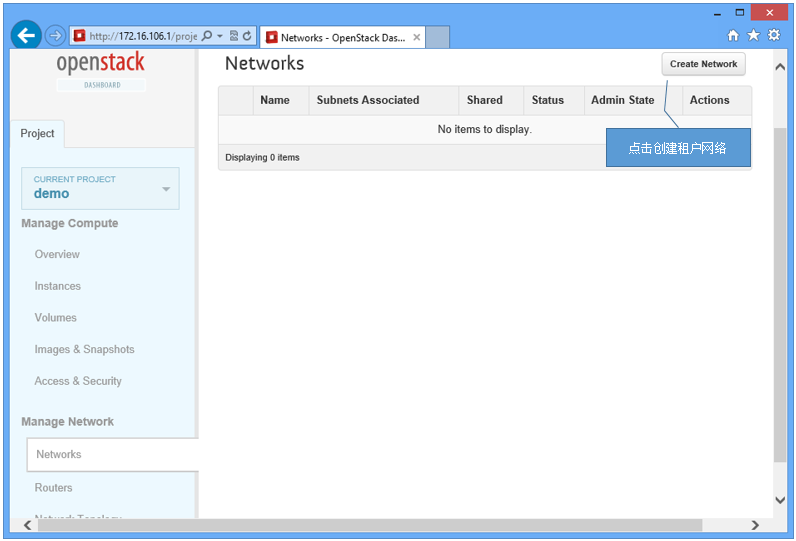
1. 以管理员身份登录后，选择管理员面板，点击’Networks’项后显示当前网络列表：[](http://www.ustack.com/wp-content/uploads/2013/09/12.png)
2. 在上图中点击“Create Network”按钮弹出“Create Network”窗口:[](http://www.ustack.com/wp-content/uploads/2013/09/21.png)在上面的弹出窗口中，填入网络名:ExternalNet，而且勾选External Network然后点击“Create Network”。
3. 下面是我们刚才创建好的网络：[](http://www.ustack.com/wp-content/uploads/2013/09/31.png)
4. 现在我们点击“ExternalNet”查看这个网络的详细情况：[](http://www.ustack.com/wp-content/uploads/2013/09/4.png)
5. 在网络详细情况页面中，我们点击“Create Subnet”弹出窗口创建外部网络的子网：[](http://www.ustack.com/wp-content/uploads/2013/09/5.png)

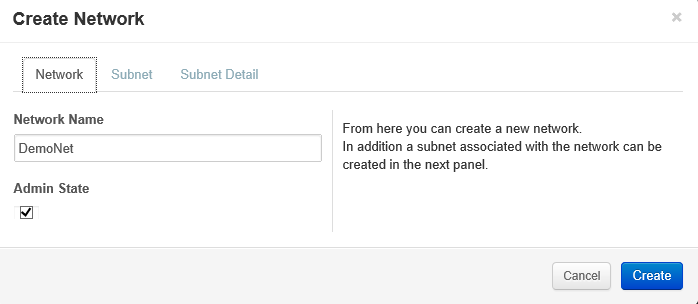
这是一个多标签页面，在上面的“Subnet”页面中填入子网名，子网CIDR(Network Address)。在下面的“Subnet Detail”页中填入地址范围：

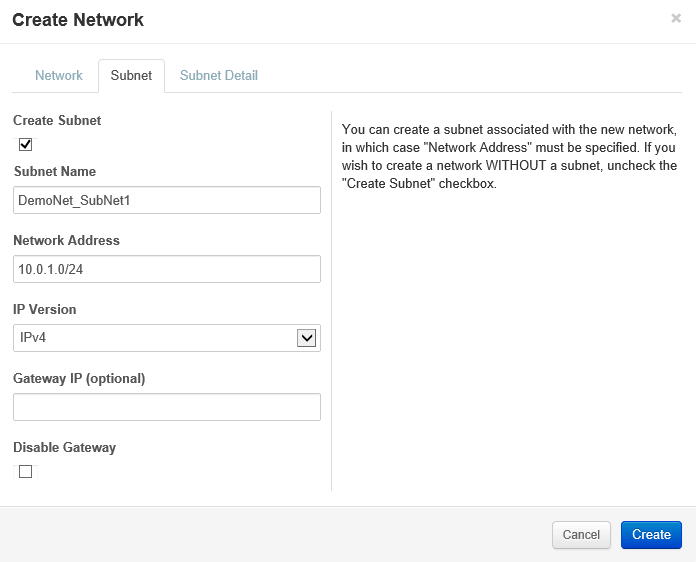
[](http://www.ustack.com/wp-content/uploads/2013/09/6.png)

注意：因为外部网络不挂接虚拟机，可以不选泽“Enable DHCP“。最后点击子网创建窗口上的“Create”完成子网的创建。

**租户demo创建租户网络**

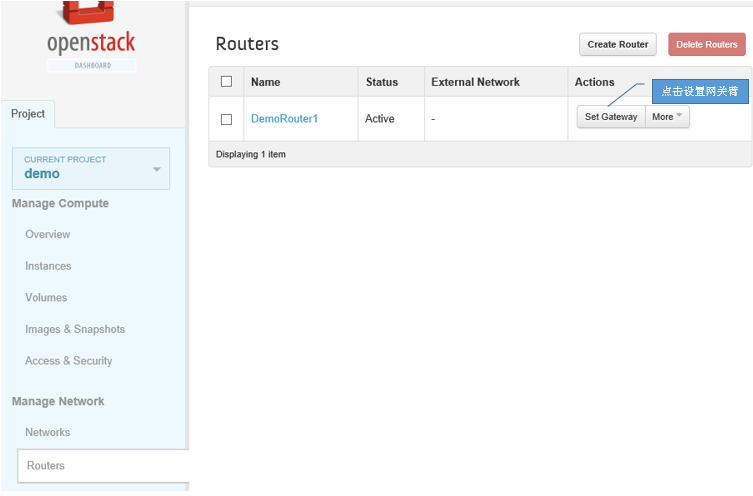
我们现在以普通租户登录horizon，并点击“Netowrks”项：[](http://www.ustack.com/wp-content/uploads/2013/09/7.png)

点击上图的“Create Network”弹出租户网络创建窗口：[](http://www.ustack.com/wp-content/uploads/2013/09/8.png)

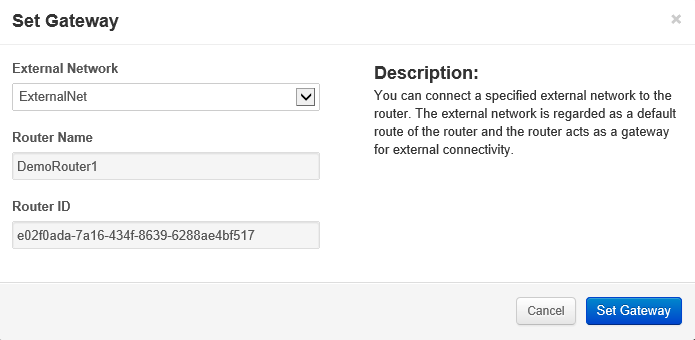
显然，这是一个多Tab的界面，和我们先前管理员创建网络的界面不一样。在这个界面里，我们可以一气完成网络和子网的创建。我们在“Network”页中填入网络名，在“Subnet”页中填入CIDR (Network Address):[](http://www.ustack.com/wp-content/uploads/2013/09/9.png)

“Subnet Datail”页面可以让我们填入IP地址池，缺省情况是Neutron使用整个CIDR规定的地址范围。所以我们不关心“Subnet Datail”页面。我们点击“Create”按钮完成租户子网的创建。

**租户创建路由器**

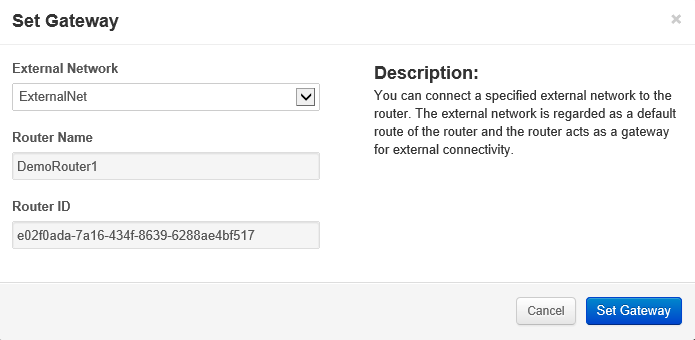
选择“Routers”项，系统显示如下页面：[](http://www.ustack.com/wp-content/uploads/2013/09/121.png)

1. 创建路由器

点击右面的“Create Router”弹出路由器创建对话框：[](http://www.ustack.com/wp-content/uploads/2013/09/13.png)

这个对话框及其简单，我们只需输入所有的路由器的名字，然后点击“Create Router”创建路由器。

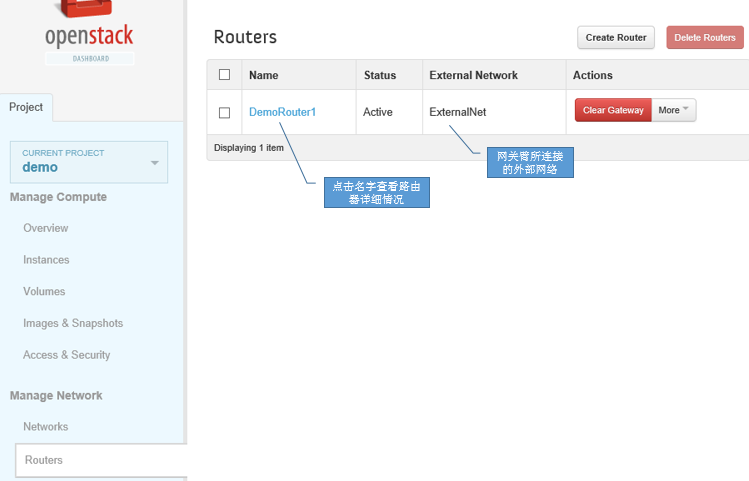
1. 配置网关臂

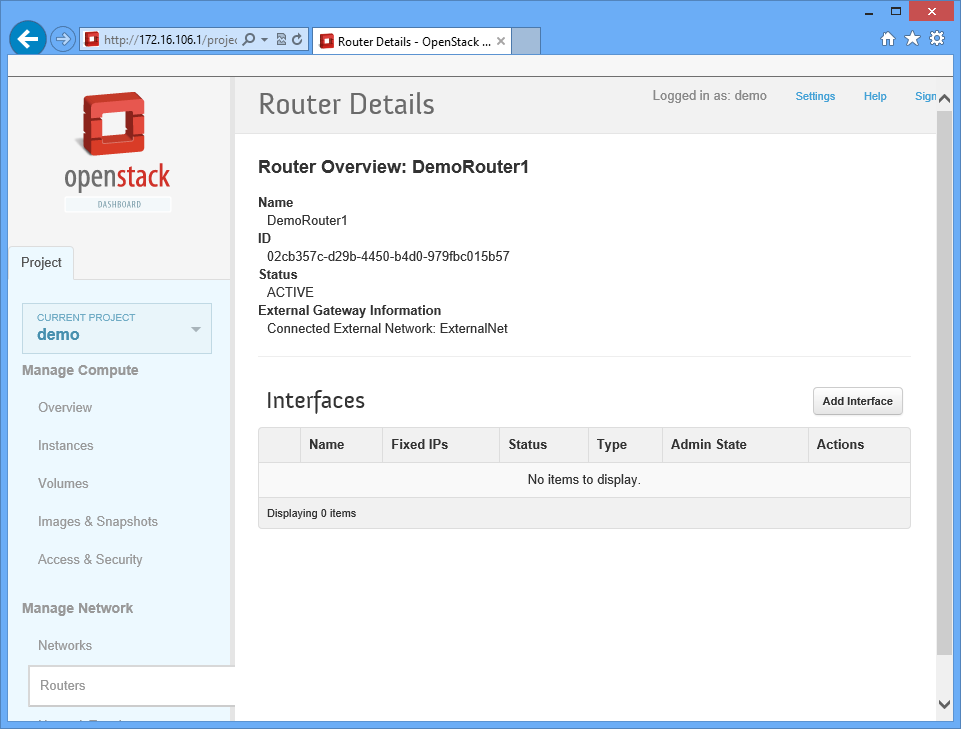
路由器创建出来之后，会显示在路由器列表中：[](http://www.ustack.com/wp-content/uploads/2013/09/13.png)

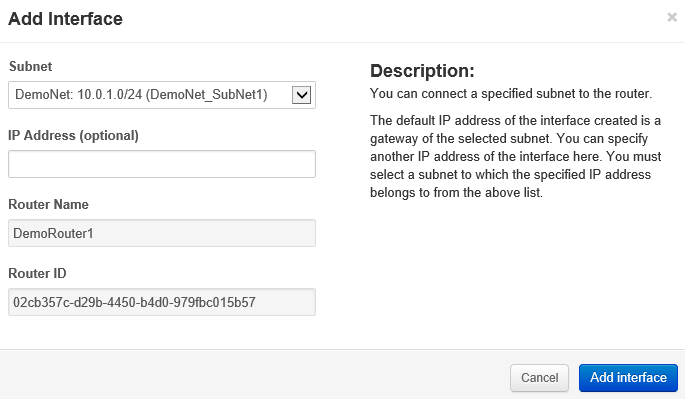
我们点击“Set Gateway”来设置这个路由器的网关臂：

如上图所示，我们选择管理员创建好的外部网络“ExternalNet”，然后点击“Set Gateway”。

1. 配置接口臂

下图显示了租户刚才创建的路由器及其网关臂：[](http://www.ustack.com/wp-content/uploads/2013/09/14.png)

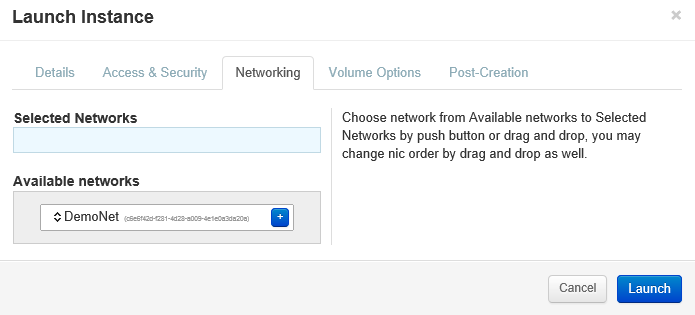
现在我们点击路由器名字查看路由器详情：[](http://www.ustack.com/wp-content/uploads/2013/09/15.png)

为了设置路由器的接口臂，我们点击“Add Interface”按钮弹出“Add Interface”窗口：[](http://www.ustack.com/wp-content/uploads/2013/09/16.png)

上图显示的窗口，我们只需选择我们所要连接的子网，然后点击“Add Interface”。

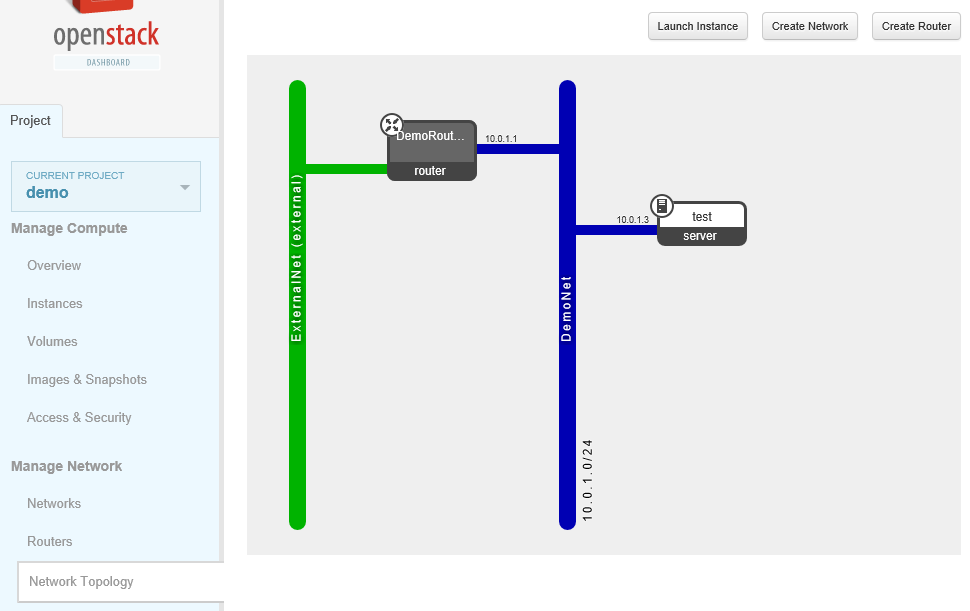
现在这个租户的路由器以及连接了外网和租户的子网，接下来这个租户可以创建虚拟机，这个虚拟机借助路由器就可以访问外部网络甚至互联网。

**租户创建虚拟机**

这里不想详述创建虚拟机的过程，我们着重叙述一下这个过程中如何选择网络：[](http://www.ustack.com/wp-content/uploads/2013/09/17.png)

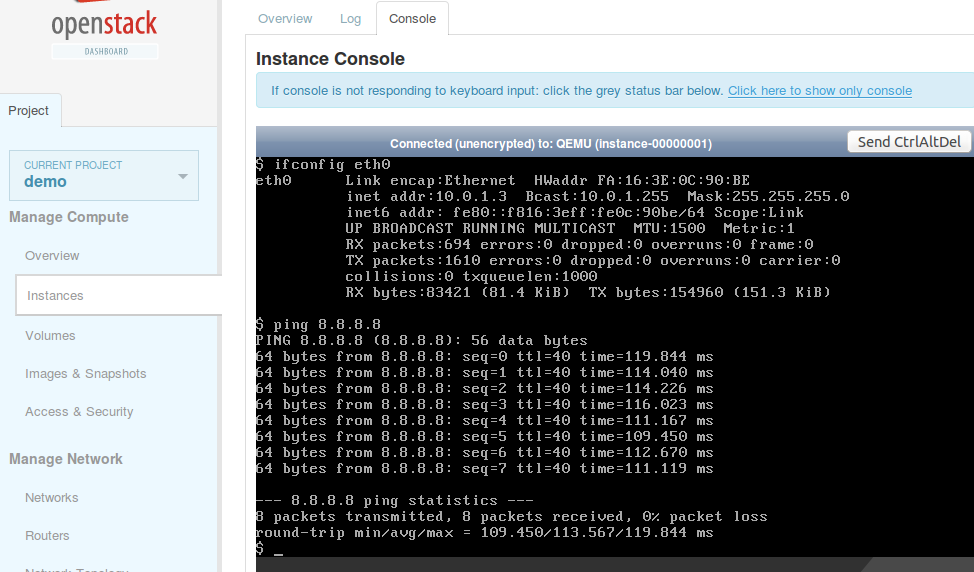
从上面的图中我们可以看出，租户可以选择的网路包括了租户刚才创建的网络。点击网络右边的“+”符号，或者拖拽这个网络进入“Selected Networks”框中，租户所创建的虚拟机就会使用这个网络。

**租户查看网络拓扑**

最后我想要说的是Horizon工程师费尽心思实现的网络拓扑图：[](http://www.ustack.com/wp-content/uploads/2013/09/18.png)

从这个拓扑图可以看到我们前面所有操作的结果：

1. 绿色的是管理员创建的外部网络
2. 跨在外部网络和租户网络上的是具有网关臂和接口臂的路由器
3. 蓝色的是租户网路及其子网
4. 最后是租户创建的虚拟机

点击拓扑图上的虚拟机图像，我们可以使用VNC访问虚拟机的控制台，如下图所示：[](http://www.ustack.com/wp-content/uploads/2013/09/19.png)

我们可以看出，这个虚拟机从租户网络中获取到了IP地址：10.0.1.3。它通过租户自己的路由器能访问互联网。

**总结**

是不是有了Neutron就不需要物理网络的网络工程师了呢？不是的。虚拟网络的负载最终还需要跑到物理网络上去传递，Neutron只不过是把部分传统网络管理的功能推到了租户方，比如租户可以创建一个虚拟网络及其子网，创建一个路由器等等，这个从上面的操作中可以看出来。在虚拟网络功能的帮助下，基础物理网络就可以向外提供额外的网络服务了，比如租户完全可以创建一个属于自己的类似于数据中心网络的虚拟网络。

Neutron提供了比较完善的多租户环境下的虚拟网络模型以及API。像部署物理网络一样，使用Neutron创建虚拟网络时也需要做一些基本的规划和设计。本文提出了一个Neutron环境下的典型网络结构和Horzion下的操作流程。在后续的博客中，我会继续介绍Neutron的其它功能，比如负载均衡，防火墙，VPN等。