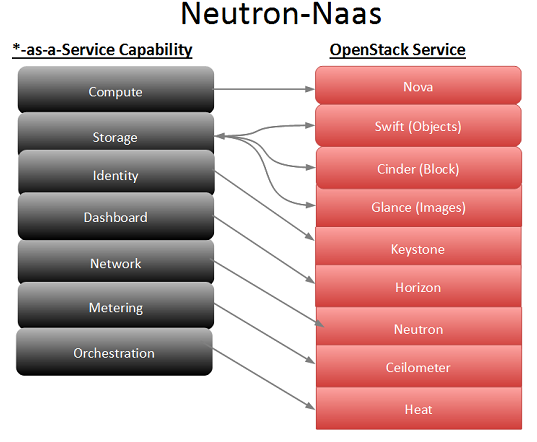
**OpenStack 网络：Neutron 初探**

2013 年 7 月 19 日是 OpenStack 诞生三周年的日子，在庆祝生日的同时，OpenStack 也将陆续发布其新的发行版 Grizzly 和 Havana。OpenStack 作为一个开放的系统，最主要是可以随时选择新的硬件供应商，当然也可以替换软件技术服务的提供商，不用动应用。这是开源本身的优势！本文会针对 OpenStack 的网络项目：Neutron 进行一个入门级的介绍。

**什么是 OpenStack?**

OpenStack 是一个开源的 IaaS（基础设施及服务）云计算平台，让任何人都可以自行建立和提供云端运算服务，具体可以从 devstack 脚本开始熟悉它。OpenStack 由一系列相互关联的项目提供云基础设施解决方案的各个组件，核心项目（9 个）：计算 (Compute) - Nova，网络和地址管理 - Neutron，对象存储 (Object) - Swift，块存储 (Block) - Cinder，身份 (Identity) - keystone，镜像 (Image) - Glance，UI 界面 (Dashboard) - Horizon，测量 (Metering) - Ceilometer，编配 (Orchestration) – Heat。如图 1。

**图 1. OpenStack 几个核心项目**



**最近发布版本情况**

2013 年 10 月 17 日，OpenStack 基金会发布了第八个大版本——Havana（上一个稳定版本 Grizzly 发布于 2013 年 4 月 4 日），带给企业客户一些新的改进。这些增强包括新的服务，例如 OpenStack Metering 和 OpenStack Orchestration。此外还有对现有服务的改进，例如针对对象存储的全局集群以及针对块存储的服务质量能力，这让 OpenStack 更好地帮助企业机构在云中构建或者部署应用。总之，Havana 将为企业提供他们需要用来转型 OpenStack 的工具，从仅仅是一个 IaaS 技术转变成为 PaaS 或甚至是 SaaS 云。预计 2014 年 4 月份发布的版本——Icehouse 将孵化项目 Database Service (Trove)，Bare Metal (Ironic) ，Queue Service (Marconi) 以及 Data Processing (Savannah) 。

[Havana 的发布](https://wiki.openstack.org/wiki/ReleaseNotes/Havana)有接近 400 多项新特性。最重要的是 OpenStack Orchestration 和 OpenStack Metering。这些是在 Grizzly 发布周期内开发的，现在已经为投产准备就绪。

以应用为驱动的能力：OpenStack Orchestration-Heat 是一个以模板为驱动的服务，用于针对应用描述和自动部署计算、存储和网络资源。新的针对对象存储的全局集群特性可以让你削减成本并提高性能，在全球范围内复制和交付数据，新的跨块存储的 QoS 功能让你确保应用所需的性能。此外还添加了 Docker 支持以利用虚拟化加速应用部署。

增强的操作体验：Dashboard 用户界面也有所增强。OpenStack Metering-Ceilometer 现在提供了跨多种 OpenStack 服务的数据使用单一来源，针对像企业扣款和提供系统监控工具等活动。

更多企业级功能：OpenStack 不断成熟，支持很多企业级功能，例如跨块存储的端到端加密，跨所有服务应用编程接口的 Secure Socket Layer (SSL)，新的 VPN 和防火墙即服务(FaaS)。主流存储和网络提供商将继续改进 OpenStack，并为 OpenStack 编写新的插件，让企业更容易与他们的厂商合作，利用现有基础架构。

在数字方面，OpenStack 社区已经累计拥有 1000 家贡献者。这比 6 个月前发布 Grizzly 的时候增加了 60%。有超过 145 个 OpenStack 生态系统成员利用开发者为这次发布做出贡献，其中包括 Canonical、Dreamhost、eNovance、惠普、IBM、英特尔、Mirantis、Rackspace、Red Hat、SUSE 和雅虎。

**Neutron 之前世今生**

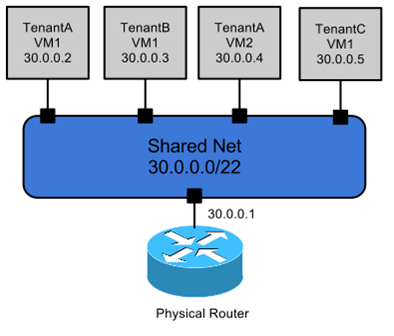
OpenStack 网络服务，现已由之前的 Quantum 改名为 Neutron。Neutron 是 OpenStack 核心项目之一，提供云计算环境下的虚拟网络功能。OpenStack Havana 版本的 Release Note 描述了 Neutron 新增加的功能：

1. Multi-Vendor-Support：同时支持多种物理网络类型，支持 Linux Bridge、Hyper-V 和 OVS bridge 计算节点共存；
2. Neutron-Fwaas：支持防火墙服务；
3. VPNaas：支持节点间 VPN 服务；
4. More-Vendors：更多的网络设备支持和开源 SDN 实现完善和提高，新增加了 ML2 (The Modular Layer2) 插件。

**OpenStack nova-network 网络模型**

在 OpenStack 网络组件没有独立出来之前，OpenStack 最初的 nova-network 网络模型，如图 2。

**图 2. 单一平面网络**



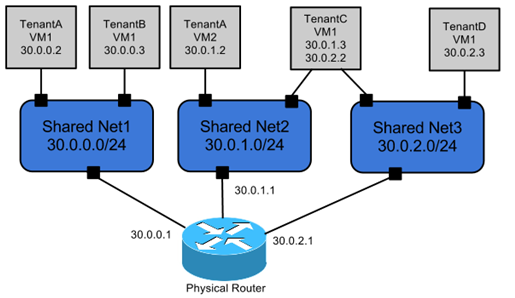
单一平面网络的缺点：

1. 存在单一网络瓶颈，缺乏可伸缩性。
2. 缺乏合适的多租户隔离。

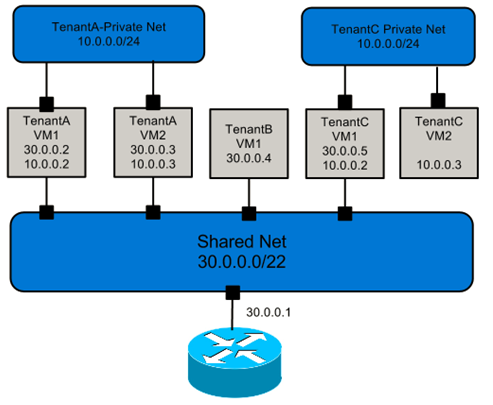
**OpenStack Neutron 网络模型**

OpenStack nova-network 独立成为单独的组件 Neutron 后，形象的网络模型的多平面网络、混合平面私有网络。如图 3，图 4，图 5，图 6。

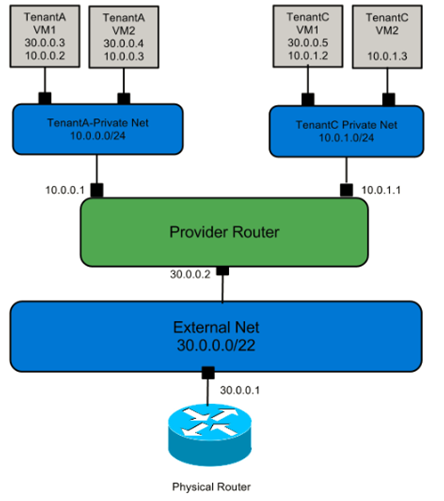
**图 3. 多平面网络**



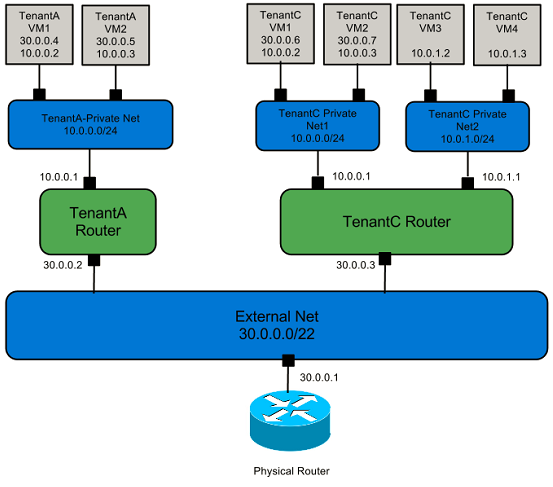
**图 4. 混合平面私有网络**



**图 5. 通过私有网络实现运营商路由功能**



**图 6. 通过私有网络实现每个租户创建自己专属的网络区段**



**Neutron 网络创建过程**

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 中用户可以创建自己的网络对象，如果要和物理环境下的概念映射的话，这个网络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。在 Horizon 上创建 Neutron 网络过程如下：

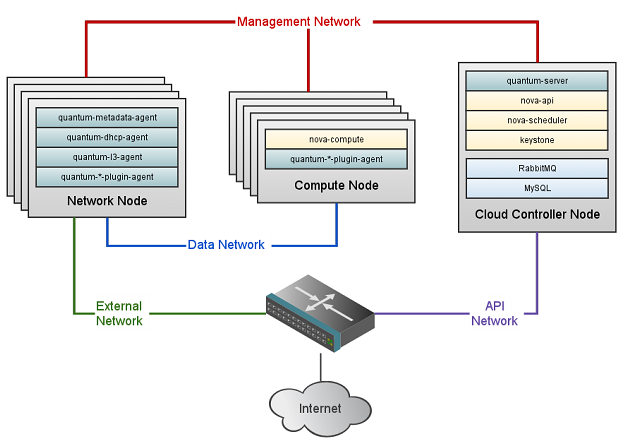
1. 首先管理员拿到一组可以在互联网上寻址的 IP 地址，并且创建一个外部网络和子网。
2. 租户创建一个网络和子网。
3. 租户创建一个路由器并且连接租户子网和外部网络。
4. 租户创建虚拟机。

**OpenStack 网络类型**

一个标准的 OpenStack 网络设置有 4 个不同的物理数据中心网络：

* 管理网络：用于 OpenStack 各组件之间的内部通信。
* 数据网络：用于云部署中虚拟数据之间的通信。
* 外部网络：公共网络，外部或 internet 可以访问的网络。
* API 网络：暴露所有的 OpenStack APIs,包括 OpenStack 网络 API 给租户们。

**图 7.OpenStack 网络类型**



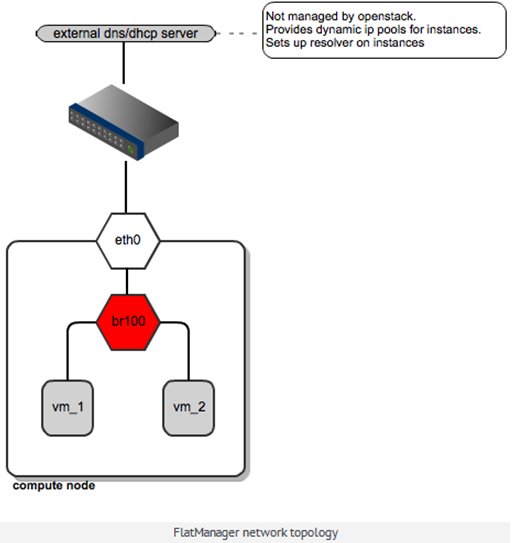
**图 7.OpenStack 网络类型**

**Neutron 服务网络管理的三种模式**

**Flat 模式**

Flat 模式和 FlatDHCP 模式其实区别不大，都是基于网桥网络，只是 FLat 模式需要管理员手动配置（包括配置网桥和外部的 DHCP 设备）。

**图 8. Flat 网络拓扑**

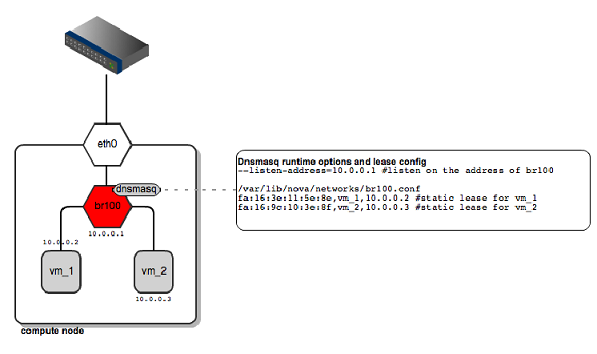


**FlatDHCP 模式**

这种模式下与 Flat 模式不同的地方在于有一个 DHCP 进程，每一个运行 nova-network 进程的节点（网络控制节点/nove-network 主机）就是一个单独的网络。Nova 会在 nova-network 主机建立网桥（默认名称 br100，配置项 flat\_network\_bridge=br100），并给该网桥指定该网络的网关 IP，同时 Nova 在网桥处起一个 DHCP 进程，最后，会建立 iptables 规则（SNAT/DNAT）使虚拟机能够与外界通信，同时与一个 metadata 服务器通信以取得 cloud 内的信息。

计算节点负责创建对应节点的网桥，此时的计算节点网卡可以不需要 IP 地址，因为网桥把虚拟机与 nove-network 主机连接在一个逻辑网络内。虚拟机启动时会发送 dhcpdiscover 以获取 IP 地址。虚拟机通往外界的数据都要通过 nova-network 主机，DHCP 在网桥处监听，分配 fixed\_range 指定的 IP 段。如图 9。

**图 9. FlatDHCP 网络拓扑**



这种部署方式的缺点----单节点故障、无二层隔离（即所有的虚拟机都在一个广播域）。

**VLAN 模式**

VLAN（Virtual Local Area Network）的中文名为"虚拟局域网"。VLAN 是一种将局域网设备从逻辑上划分成一个个网段，从而实现虚拟工作组的新兴数据交换技术。

VLAN 模式与 Flat 模式的区别

在 Flat 模式下，管理员的工作流程应该是这样的：

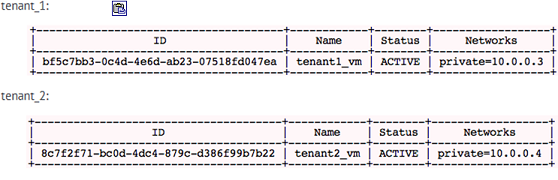
1. 为所有租户创建一个 IP 池：

nova-manage network create --fixed\_range\_v4=10.0.0.0/16 –label=public

1. 创建租户
2. 租户创建虚拟机，为虚拟机分配 IP 池中的可用 IP

DB 中虚拟机信息可能如下图，从图中我们看到 2 个虚拟机处于同一网段。

**图 10**



在 VLAN 模式下流程如下：

1. 创建新的租户，并记下租户的标识
2. 为该租户创建独占的 fixed\_ip 段：

nova-manage network create --fixed\_range\_v4=10.0.1.0/24 --vlan=102 --project\_id="tenantID"

1. 租户创建虚拟机，从租户的私有 IP 段内分配 IP 给虚拟机

因此，与 Flat 模式相比，VLAN 模式为网络增加了：将网络与租户关联和为网络分配一个 VLAN 号。

**Neutron 总结**

OpenStack 虚拟网络 Neutron 把部分传统网络管理的功能推到了租户方，租户通过它可以创建一个自己专属的虚拟网络及其子网，创建路由器等等，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。

**参考资料**

**学习**

* [DevStack 官网](http://devstack.org/)，你可以从 DevStack 脚本快速上手 OpenStack。
* [Openstack Havana updates network](http://www.enterprisenetworkingplanet.com/datacenter/openstack-havana-updates-cloud-networking.html)，您可以了解 Havana 版本中网络的更新情况。
* [Neutron网络入门](http://www.ustack.com/blog/neutron_intro/)，您可以 Neutron 的一些基本概念。
* [Neutron之网络负载均衡](http://www.ustack.com/blog/neutron_loadbalance/)，您可以有关 Neutron 负载均衡的相关知识。
* [SDN](http://www.zdnet.com.cn/wiki-SDN)，您可以了解什么是软件定义网络。
* [OpenStack文档改变历史](http://docs.openstack.org/grizzly/openstack-network/admin/content/Document_Change_History-d1e118.html)，您可以获得 OpenStack 最近的文档改变。
* [OpenStack Grizzly](http://www.infoq.com/cn/news/2013/04/openstack-grizzly)支持大规模生产环境和更多网络技术，您可以获得有关 Grizzly 新增的一些功能介绍。
* [Neutron 服务网络管理模式](http://www.mirantis.com/blog/)。
* [developerWorks 云计算站点](https://www.ibm.com/developerworks/cn/cloud/index.html) 提供了有关云计算的更新资源，包括
  + 云计算 [简介](http://www.ibm.com/developerworks/cn/cloud/newto.html)。
  + 更新的 [技术文章和教程，以及网络广播](http://www.ibm.com/developerworks/cn/cloud/resources.html)，让您的开发变得轻松，[专家研讨会和录制会议](http://www.ibm.com/developerworks/cn/cloud/events.html) 帮助您成为高效的云开发人员。
  + 连接转为云计算设计的 [IBM 产品下载和信息](http://www.ibm.com/developerworks/cn/cloud/products.html)。
  + 关于 [社区最新话题](http://www.ibm.com/developerworks/cn/cloud/collaborate.html) 的活动聚合。