

上次我们讨论了 Neutron 提供的功能，今天我们学习 Neutron 模块几个重要的概念。

Neutron 管理的网络资源包括 Network，subnet 和 port，下面依次介绍。

**network**

network 是一个隔离的二层广播域。Neutron 支持多种类型的 network，包括 local, flat, VLAN, VxLAN 和 GRE。

**local**local 网络与其他网络和节点隔离。local 网络中的 instance 只能与位于同一节点上同一网络的 instance 通信，local 网络主要用于单机测试。

**flat**flat 网络是无 vlan tagging 的网络。flat 网络中的 instance 能与位于同一网络的 instance 通信，并且可以跨多个节点。

**vlan**vlan 网络是具有 802.1q tagging 的网络。vlan 是一个二层的广播域，同一 vlan 中的 instance 可以通信，不同 vlan 只能通过 router 通信。vlan 网络可以跨节点，是应用最广泛的网络类型。

**vxlan**vxlan 是基于隧道技术的 overlay 网络。vxlan 网络通过唯一的 segmentation ID（也叫 VNI）与其他 vxlan 网络区分。vxlan 中数据包会通过 VNI 封装成 UDP 包进行传输。因为二层的包通过封装在三层传输，能够克服 vlan 和物理网络基础设施的限制。

**gre**gre 是与 vxlan 类似的一种 overlay 网络。主要区别在于使用 IP 包而非 UDP 进行封装。

不同 network 之间在二层上是隔离的。  
以 vlan 网络为例，network A 和 network B 会分配不同的 VLAN ID，这样就保证了 network A 中的广播包不会跑到 network B 中。当然，这里的隔离是指二层上的隔离，借助路由器不同 network 是可能在三层上通信的。

network 必须属于某个 Project（ Tenant 租户），Project 中可以创建多个 network。

network 与 Project 之间是 1对多 关系。

**subnet**

subnet 是一个 IPv4 或者 IPv6 地址段。instance 的 IP 从 subnet 中分配。每个 subnet 需要定义 IP 地址的范围和掩码。

subnet 与 network 是 1对多 关系。一个 subnet 只能属于某个 network；一个 network 可以有多个 subnet，这些 subnet 可以是不同的 IP 段，但不能重叠。下面的配置是有效的：

network A subnet A-a: 10.10.1.0/24 {"start": "10.10.1.1", "end": "10.10.1.50"}

subnet A-b: 10.10.2.0/24 {"start": "10.10.2.1", "end": "10.10.2.50"}

但下面的配置则无效，因为 subnet 有重叠

networkA subnet A-a: 10.10.1.0/24 {"start": "10.10.1.1", "end": "10.10.1.50"}

subnet A-b: 10.10.1.0/24 {"start": "10.10.1.51", "end": "10.10.1.100"}

这里不是判断 IP 是否有重叠，而是 subnet 的 CIDR 重叠（都是 10.10.1.0/24）

但是，如果 subnet 在不同的 network 中，CIDR 和 IP 都是可以重叠的，比如

network A subnet A-a: 10.10.1.0/24 {"start": "10.10.1.1", "end": "10.10.1.50"}

networkB subnet B-a: 10.10.1.0/24 {"start": "10.10.1.1", "end": "10.10.1.50"}

这里大家不免会疑惑： 如果上面的IP地址是可以重叠的，那么就可能存在具有相同 IP 的两个 instance，这样会不会冲突？ 简单的回答是：不会！

具体原因： 因为 Neutron 的 router 是通过 Linux network namespace 实现的。network namespace 是一种网络的隔离机制。通过它，每个 router 有自己独立的路由表。

上面的配置有两种结果：

1. 如果两个 subnet 是通过同一个 router 路由，根据 router 的配置，只有指定的一个 subnet 可被路由。
2. 如果上面的两个 subnet 是通过不同 router 路由，因为 router 的路由表是独立的，所以两个 subnet 都可以被路由。

这里只是先简单做个说明，我们会在后面三层路由的章节详细分析这种场景。

**port**

port 可以看做虚拟交换机上的一个端口。port 上定义了 MAC 地址和 IP 地址，当 instance 的虚拟网卡 VIF（Virtual Interface） 绑定到 port 时，port 会将 MAC 和 IP 分配给 VIF。

port 与 subnet 是 1对多 关系。一个 port 必须属于某个 subnet；一个 subnet 可以有多个 port。

**小节**

下面总结了 Project，Network，Subnet，Port 和 VIF 之间关系。

Project 1 : m Network 1 : m Subnet 1 : m Port 1 : 1 VIF m : 1 Instance  
  
下一节我们讨论 Neutron 的架构。