

2.4.6 网络基础概念 - Openstack

讲师：汪洋





目录

1

网络相关知识

2

Neutron

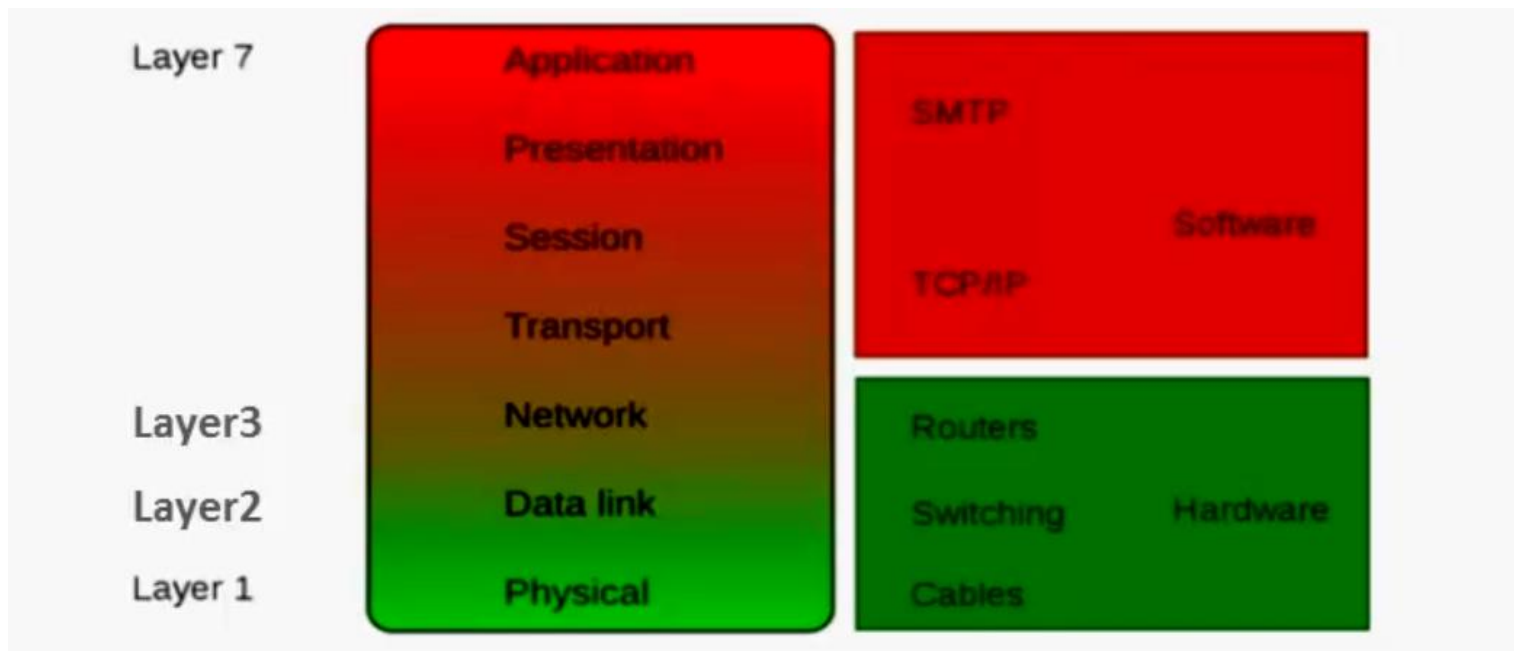
3

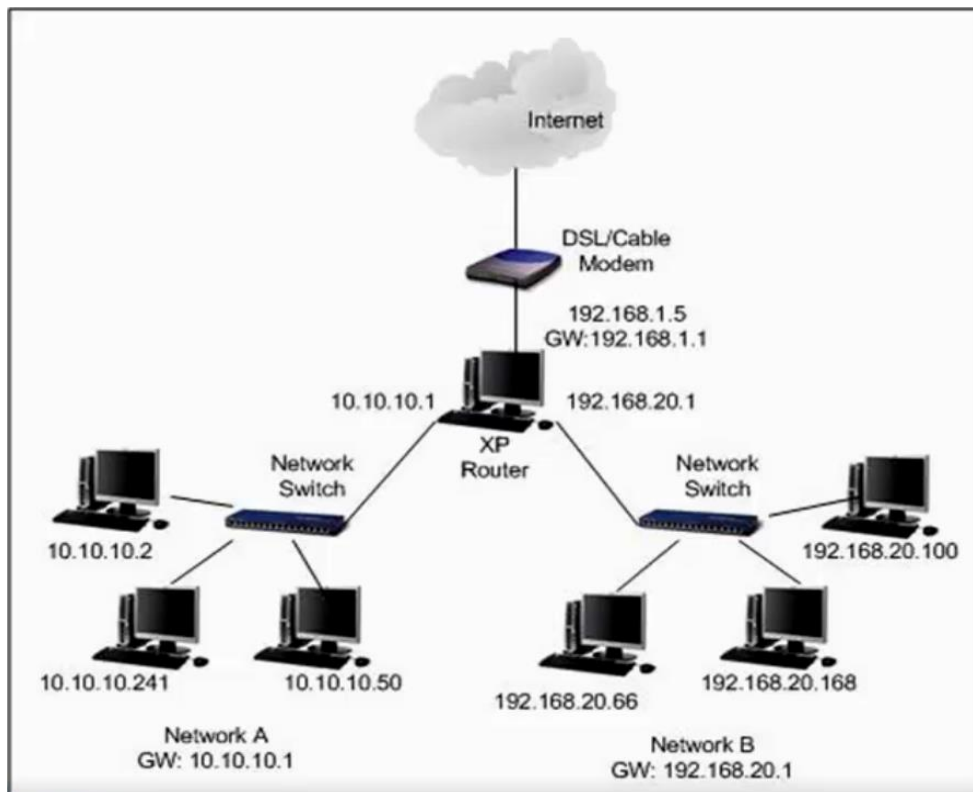
代码构建



1

网络相关知识







工作层次不同

- L2/L3

数据转发依据对象不同

- 数据帧（MAC）/数据包（IP）

解决问题不同

- 同网段互通/不同网段互通



```
[root@network0 ~]# route
Kernel IP routing table
Destination      Gateway          Genmask          Flags Metric Ref    Use Iface
10.20.0.0         *               255.255.255.0    U        0      0        0 eth0
192.168.4.0       *               255.255.255.0    U        0      0        0 eth2
172.16.0.0        *               255.255.255.0    U        0      0        0 br-ex
link-local        *               255.255.0.0      U       1002    0        0 eth0
link-local        *               255.255.0.0      U       1003    0        0 eth1
link-local        *               255.255.0.0      U       1004    0        0 eth2
default           10.20.0.1       0.0.0.0          UG        0      0        0 eth0
```



```
[root@vm1 ~]# ip netns exec router-ns iptables -t nat -nL
Chain PREROUTING (policy ACCEPT)
target     prot opt source                destination
DNAT       all  --  0.0.0.0/0              192.168.4.51           to:192.168.1.11

Chain POSTROUTING (policy ACCEPT)
target     prot opt source                destination
SNAT       all  --  192.168.1.11           0.0.0.0/0              to:192.168.4.51
SNAT       all  --  192.168.1.0/24         0.0.0.0/0              to:192.168.4.50

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
DNAT       all  --  0.0.0.0/0              192.168.4.51           to:192.168.1.11
```

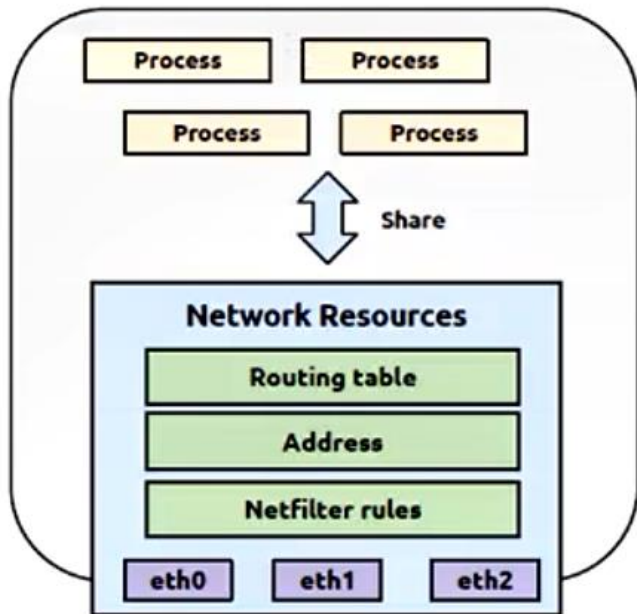



- 接受所有经过设备的数据包
- 一般用于网络抓包
- Floating IP 功能实现

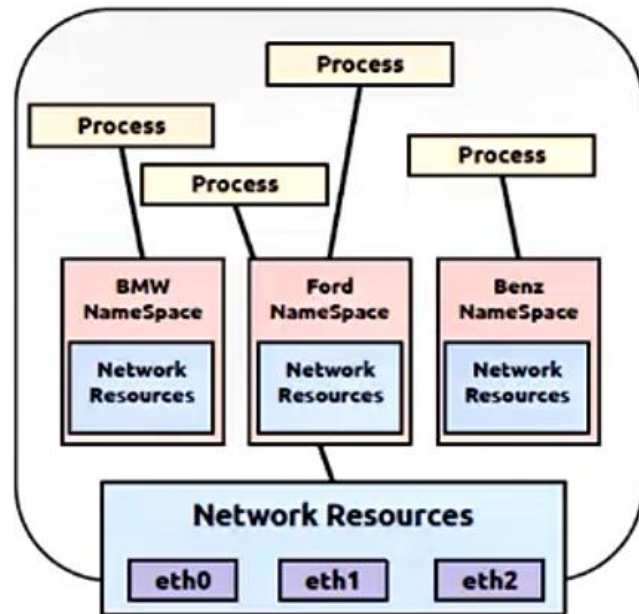
```
[root@network0 ~]# ifconfig eth1
eth1      Link encap:Ethernet  HWaddr 52:54:00:C8:67:12
          inet6 addr: fe80::5054:ff:fec8:6712/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:128948 errors:0 dropped:0 overruns:0 frame:0
          TX packets:74 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5935555 (5.6 MiB)  TX bytes:4586 (4.4 KiB)
          Interrupt:10 Base address:0xa000
```



without Network NameSpace



with Network NameSpace





- 1、一个数据包（或帧）封装在另一个数据包内；被封装的包转发到隧道端点后再被拆装
- 2、叠加网络就是使用这种所谓“包内之包”的技术安全的将一个网络隐藏在另一个网络中，然后将网段进行迁移

Vlan

- L2 over L2

GRE

- L3 over L3 (UDP)

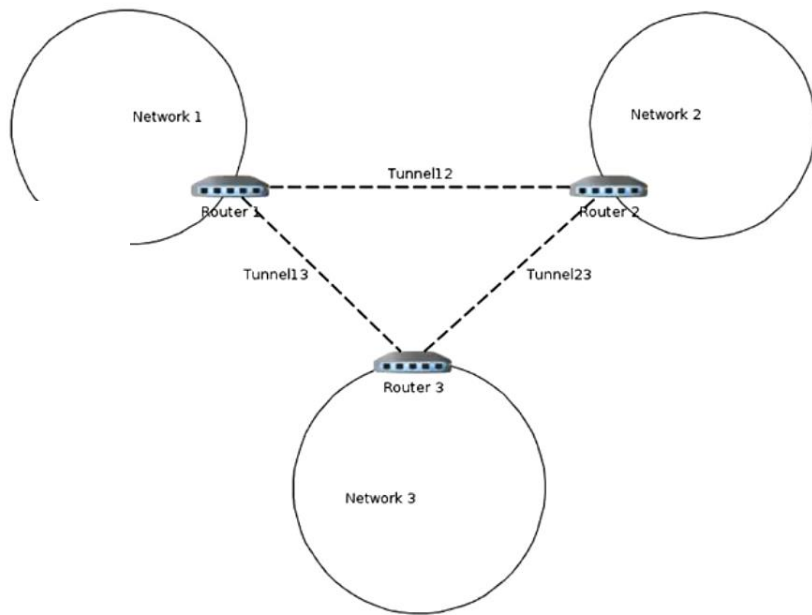
Vxlan

- L2 over L3 (UDP)



不用变更底层网络架构重建 L2、L3 通讯
实现不同 Host 之间网络互通
方便迁移
支持网络数量扩大

大规模部署问题
性能问题





数据中心网络数量限制：1 > 4096 > 1600w

物理网络基础设施限制

- 不改变物理网络变更 VM 网络拓扑
- VM 迁移

多租户场景

- 支持 IP 地址重叠



- TAP/TUN
- Bridge
- Physical
- Loopback



网络隔离: Vlan Gre Vxlan

Qos 配置

流量监控

数据包分析

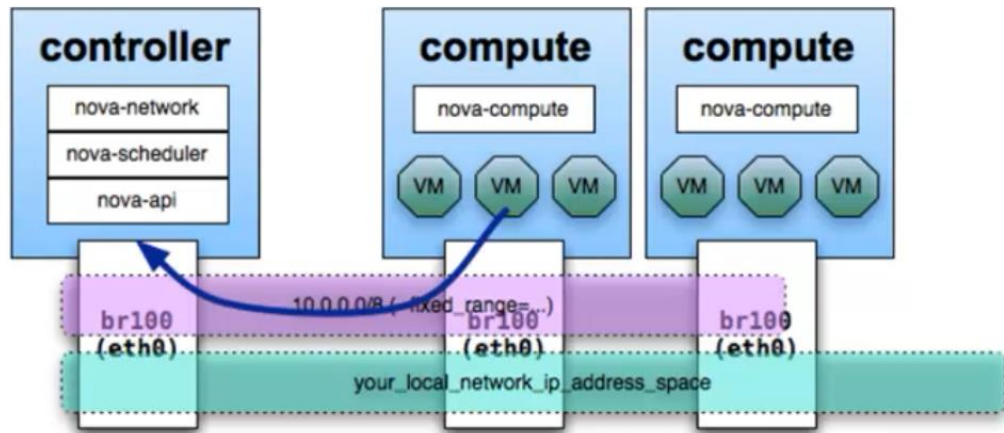


2

Neutron



- Flat
- Flatdhcp
- Vlan





指定一个子网，规定虚拟机能使用的 IP 地址范围

创建实例是，从有效 IP 地址池获取一个 IP，为虚拟机实例分配，然后在虚拟机启动时候注入虚拟机镜像（文件系统）

手动配置好网桥，所有的系统实例都是和同一个网桥连接；网桥连接到网桥的实例组成一个虚拟网络

网络控制器对虚拟机实例进行 NAT 转换，实现与外部的通信

目前配置注入只能对 类 UNIX 操作系统正常工作



网络控制器运行 dnsmasp 作为 DHCP 服务器监听这个网桥



每个用户分配一个 Vlan ，每个用户创建的网络接口 在同一个 Vlan 中

每个用户分配一个网段，网络控制器上的 DHCP 服务器为所有的 Vlan 分配地址

解决了隔离问题，但是 Vlan 限制为 4096 个，符合私有云



传统桥接模式

用户不能自定义网络

网络隔离

大规模不是



基础需求

高密度

多租户

大规模扩展

虚拟机的可移动性

资源管理自动化

低成本实现

企业级需求

自定义网络

Qos 保证

防火墙

监控、审计



网络连接服务

面向租户 API 接口，用于创建虚拟网络、路由器、负载均衡、关联 网络接口至指定网络和路由

通过 API 接口管理虚拟或物理交换机

提供 Plugin 架构来支持不同的技术平台

Neutron Private Network - 提供固定私网地址

Neutron Public Network - 提供浮动 IP 地址



Network

- 一个 L2 网络单元
- 租户可通过 Neutron API 创建自己的网络

Subnet

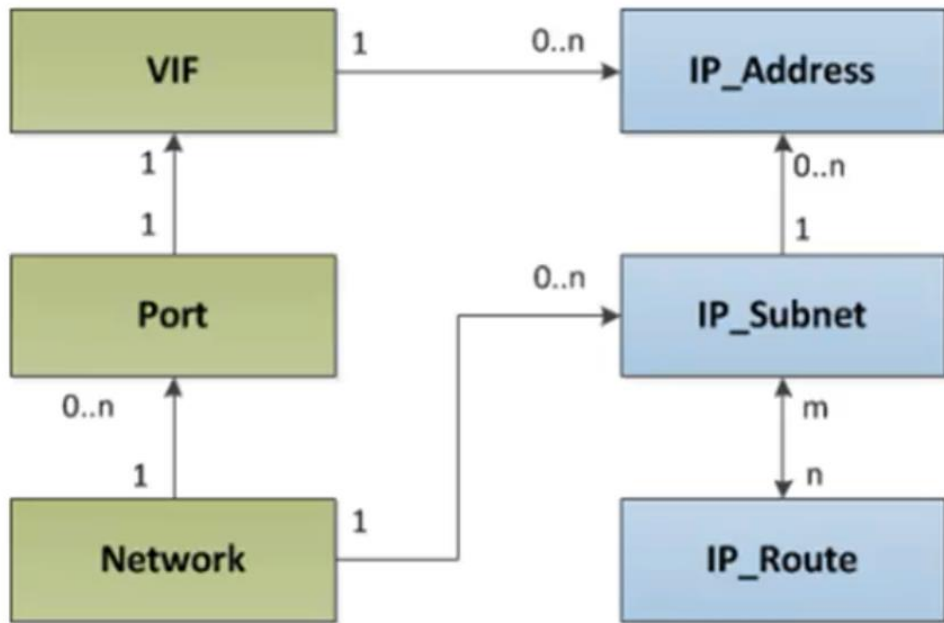
- 一段 IPV4/IPV6 地址段
- 为 Instance 提供私网或公网地址

Router

- 三层路由器
- 为租户的 Instance 提供路由功能

Port

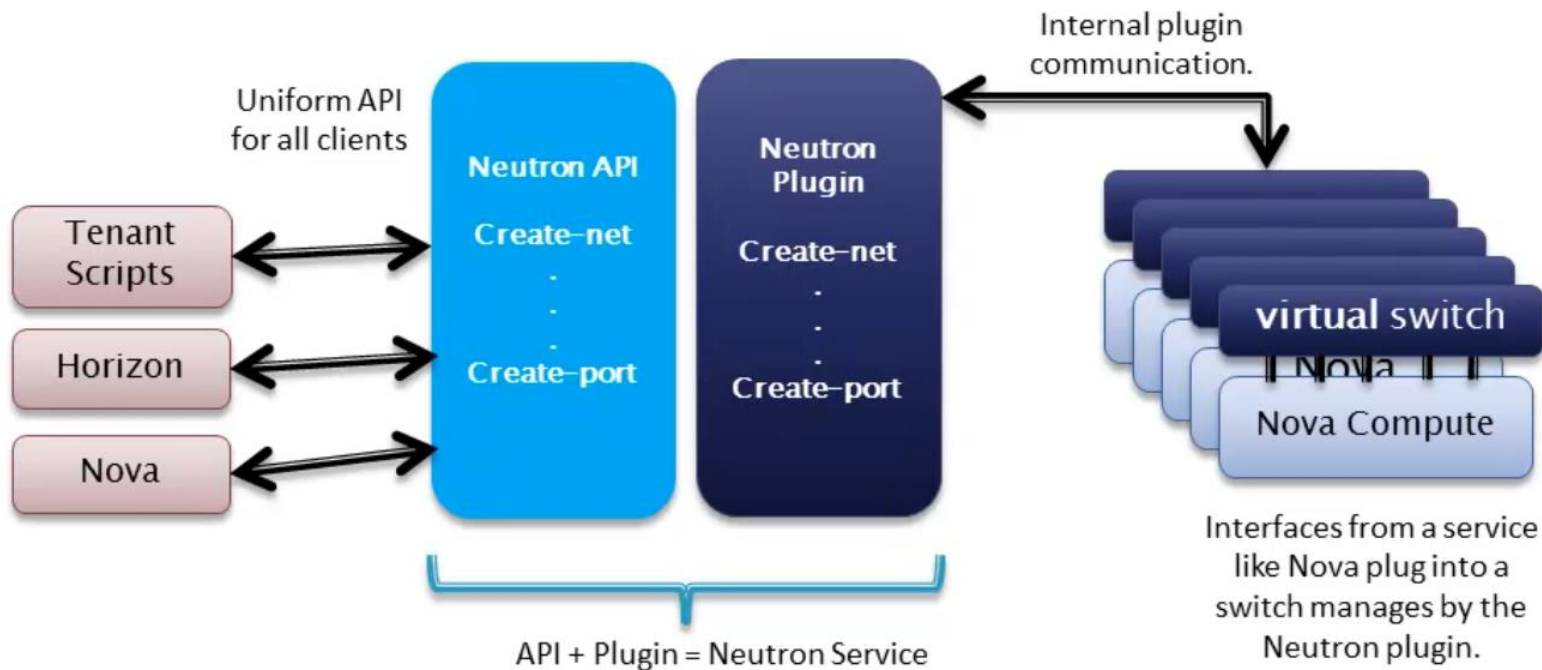
- 虚拟交换机上的端口
- 管理 Instance 的网卡





API Clients

Neutron Server





✓ Open vSwitch

✓ Linux Bridge

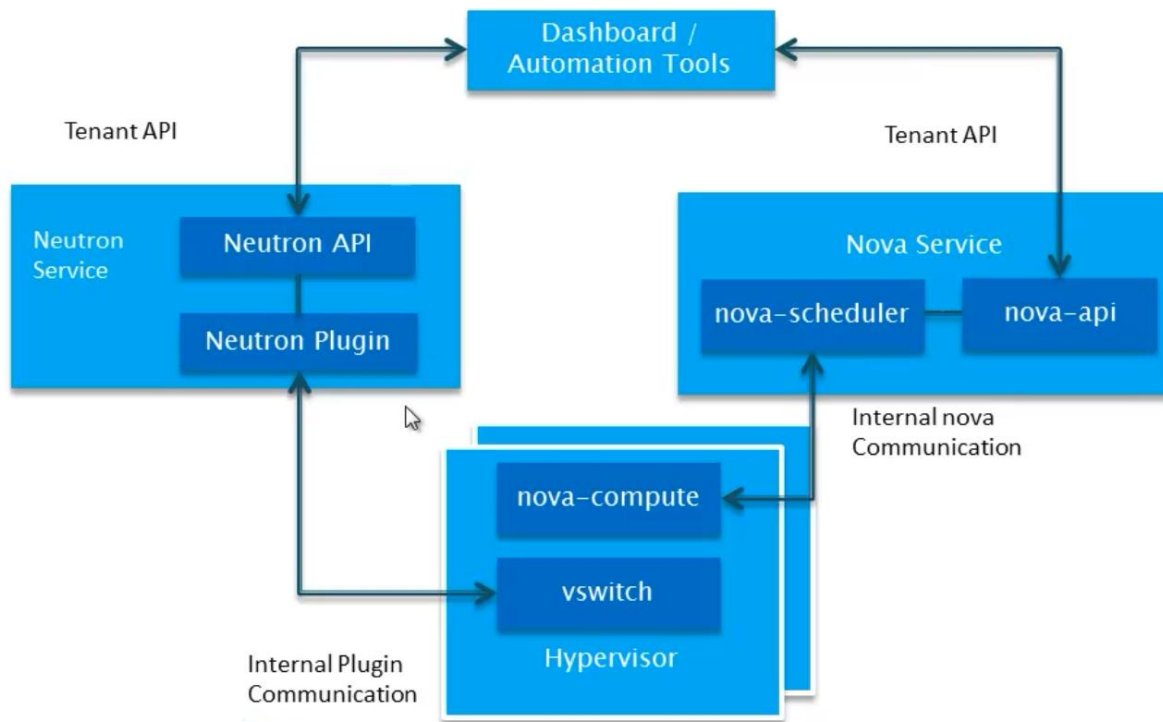
✓ Ciso NX1000

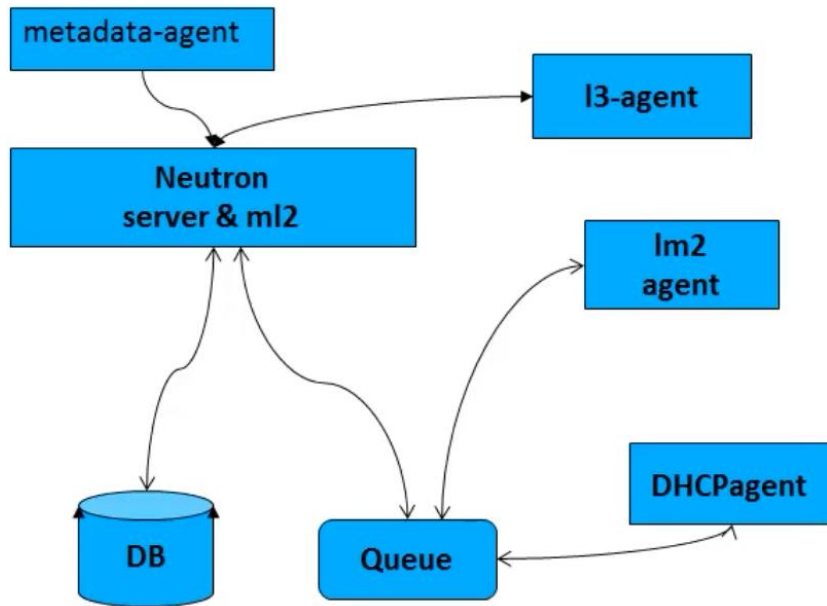
✓ Nicira NVP

✓ Ryu

✓ NEC OpenFlow

✓ Floodnight





Neutron Server

- 实现 Neutron API 和 API 扩展
- 管理 Network、Subnet、Pod
- 管理 Port 的 IP 地址

ML2 agent

- 运行在每个计算节点上
- 连接虚拟机到网络端口

DHCP agent

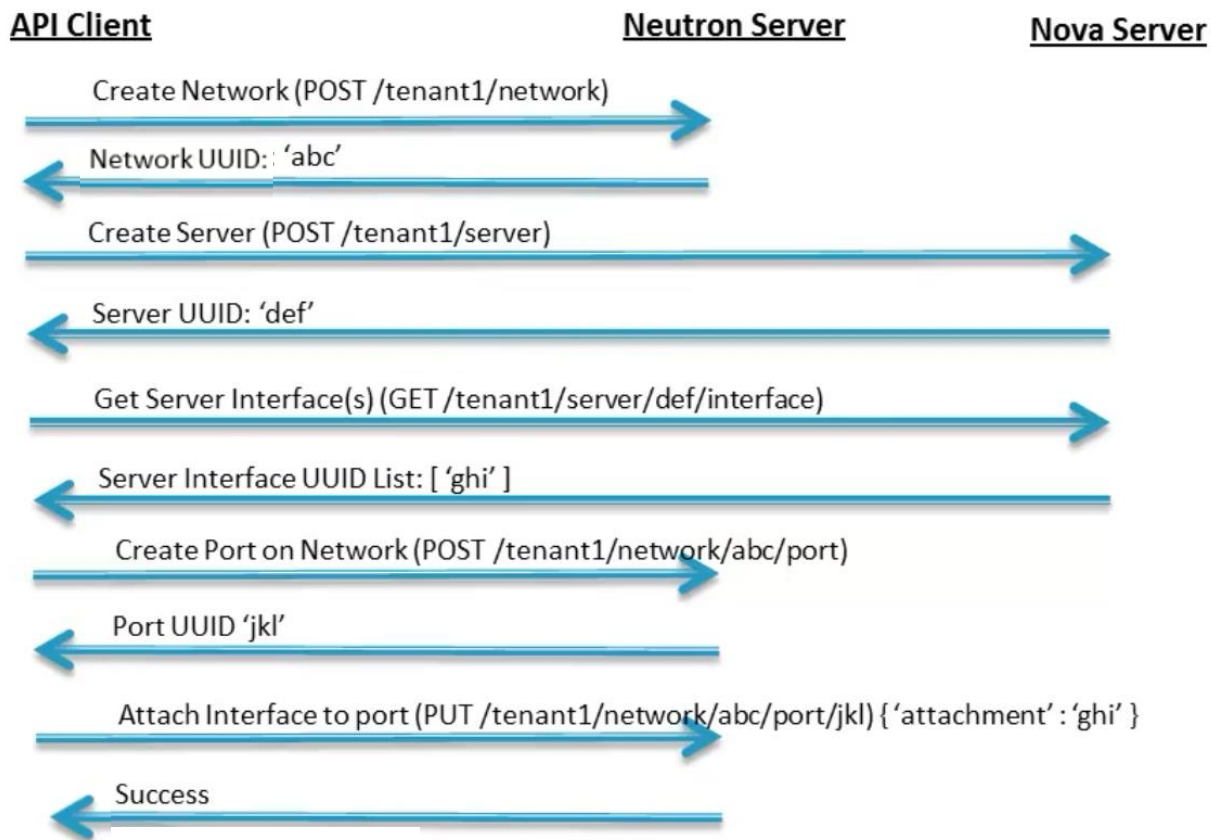
- 负责 DHCP 配置，为虚拟机分配 IP
- 开始/停止 DHCP 服务器以及相关配置

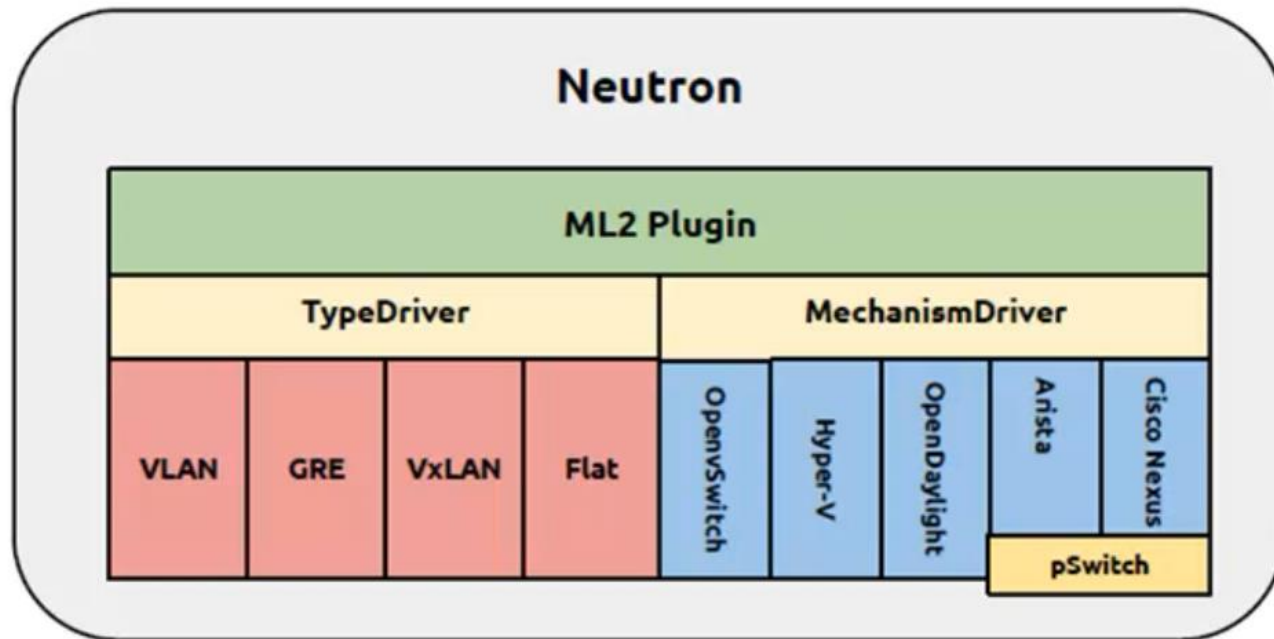
L3-agent

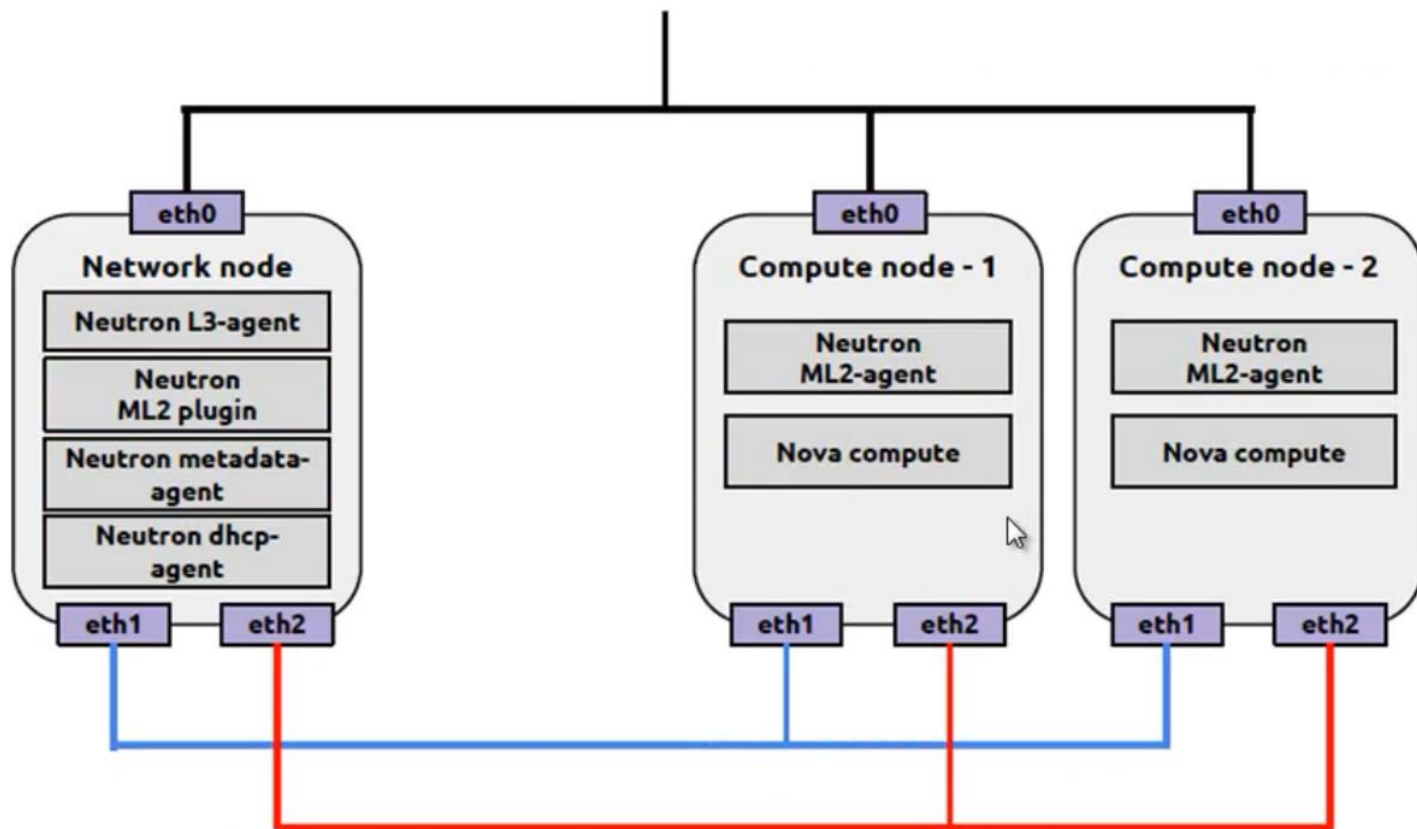
- 负责公网浮动 IP 地址和 NAT
- 负责其他三层特性，例如：负载均衡等
- 每个 Network 对应一个 L3 agent

Metadata-agent

- 提供元数据服务









Single FLAT Network

Multi FLAT Network

Mixed FLAT and Private Network

Provider Router with Private Network

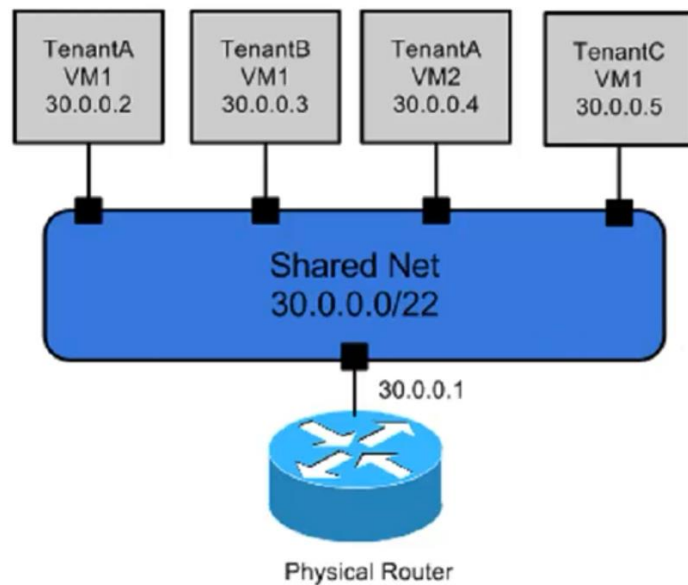
Per-tenant Routers with Private Network



类似 Flat Manager

FlatDHCPManager

不支持 Floating IP

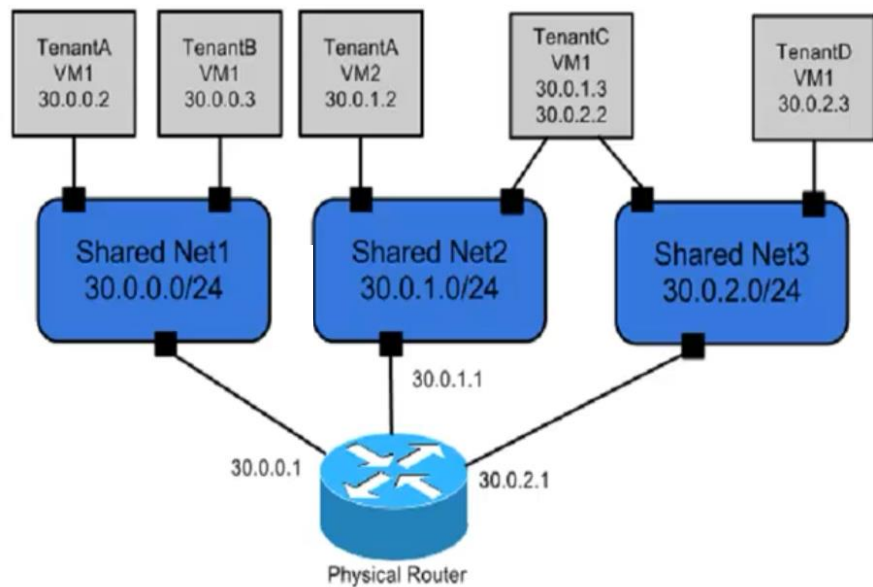


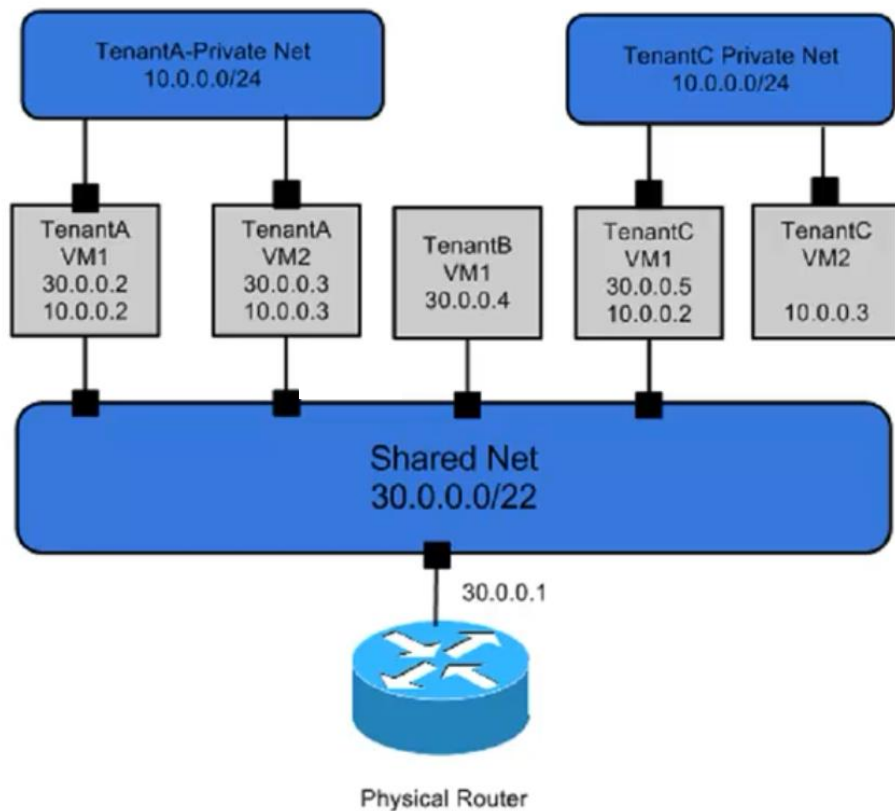


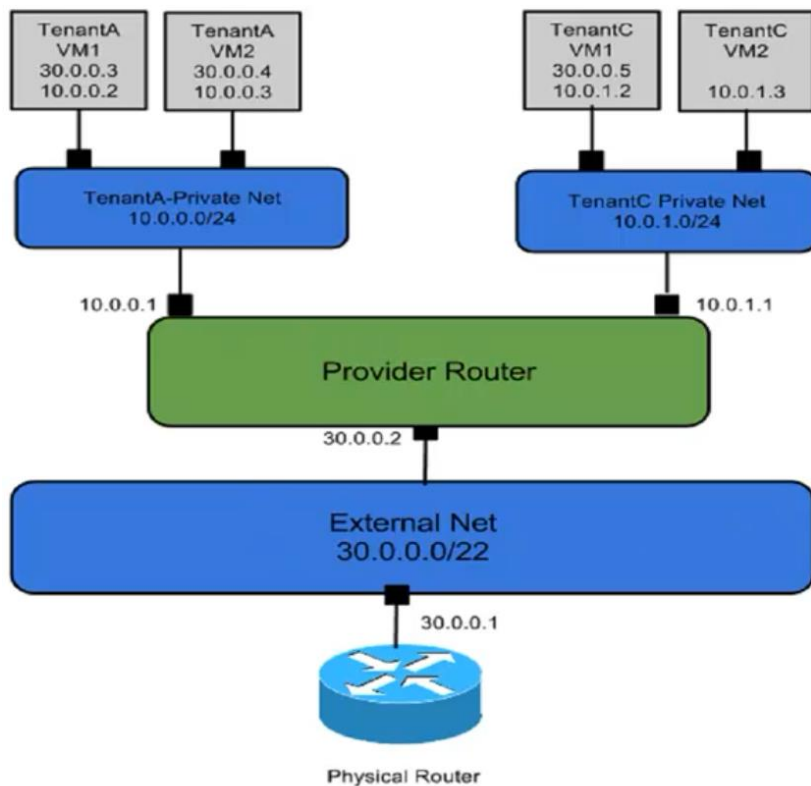
类似 Flat Manager

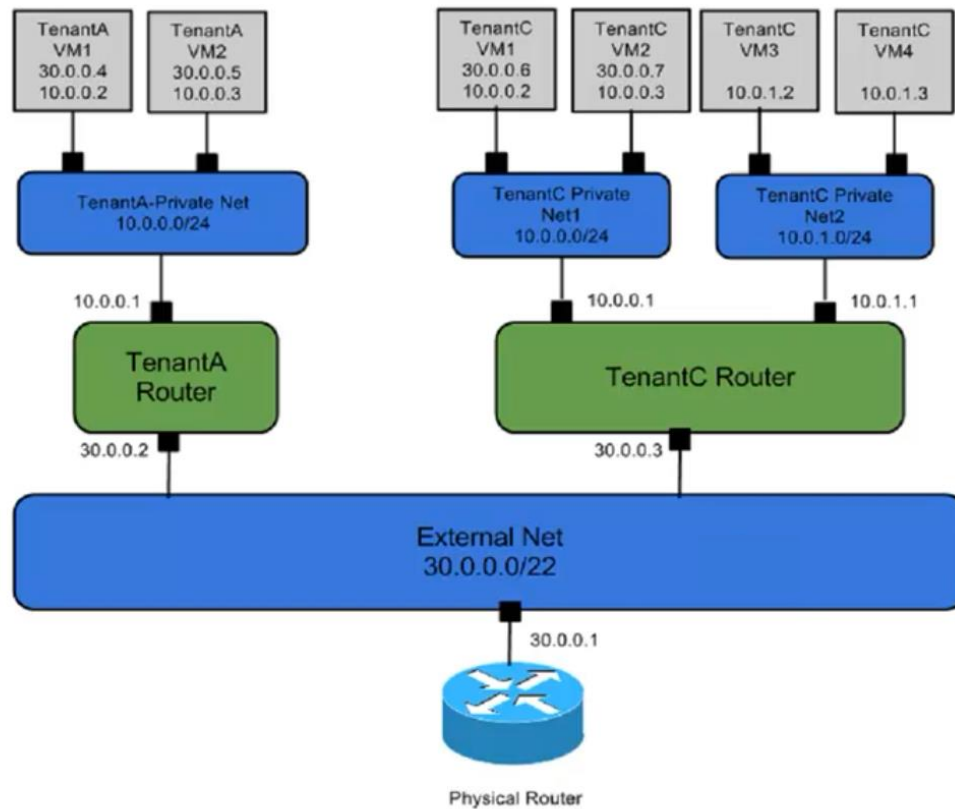
FlatDHCPManager

不支持 Floating IP











3

代码构建



代码构建