# OpenStack网络管理

# 前言

- Neutron作为OpenStack的核心项目，为OpenStack提供“网络即服务”，实现灵活和自动化管理OpenStack网络。
- 本章节分为两个部分：理论和实验
  - 理论部分主要讲解Linux网络虚拟化基础，Neutron作用、架构、原理和流程。
  - 实验部分重点锻炼学员Neutron日常运维操作，帮助学员理论联系实际，真正掌握Neutron 。

# 目标

- 学完本课程后，您将能够：
  - 描述Linux网络虚拟化技术
  - 描述Neutron作用
  - 描述Neutron架构
  - 描述Neutron典型操作和流程
  - 具备Neutron日常运维能力

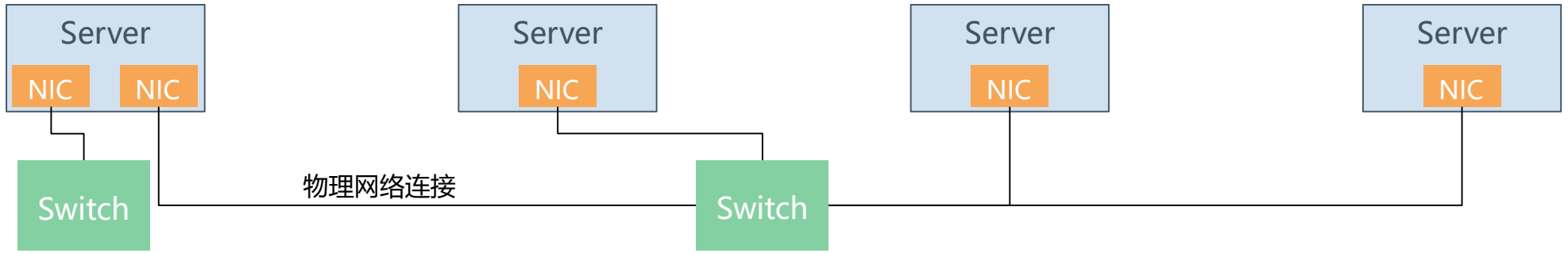
# 目录

# 为什么介绍Linux网络虚拟化基础知识?

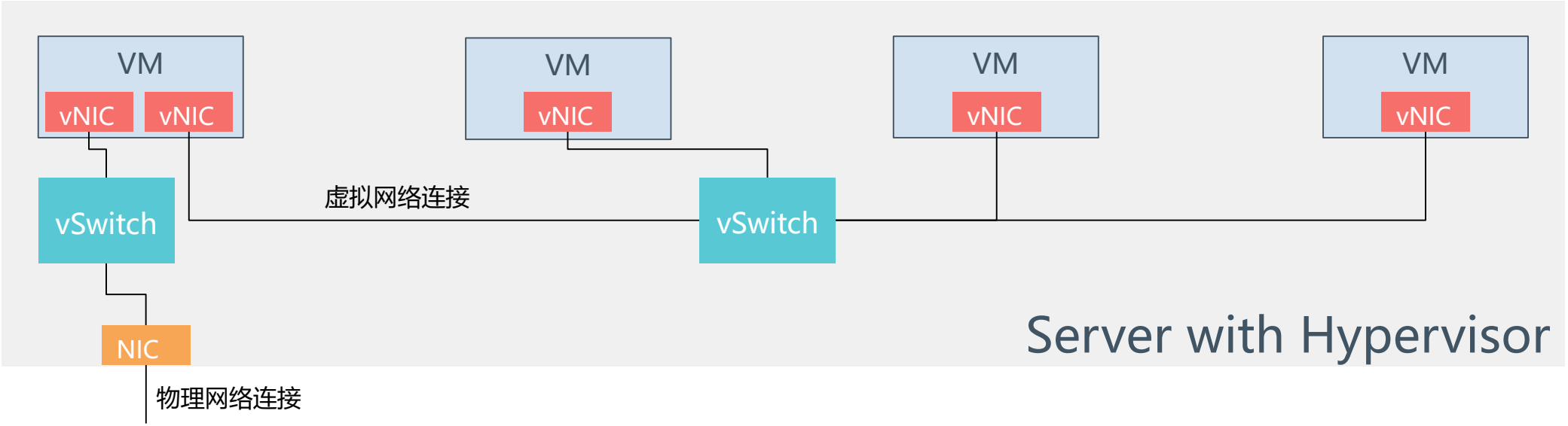
- Neutron的设计目标是实现“网络即服务”。
  - 设计上：遵循基于“软件定义网络（SDN）”的灵活和自动化原则。
  - 实现上：充分利用 Linux 各种网络相关的技术。

- 学习Linux系统中的网络虚拟化知识，有助于快速理解Neutron的原理和实现。

# 物理网络与虚拟化网络



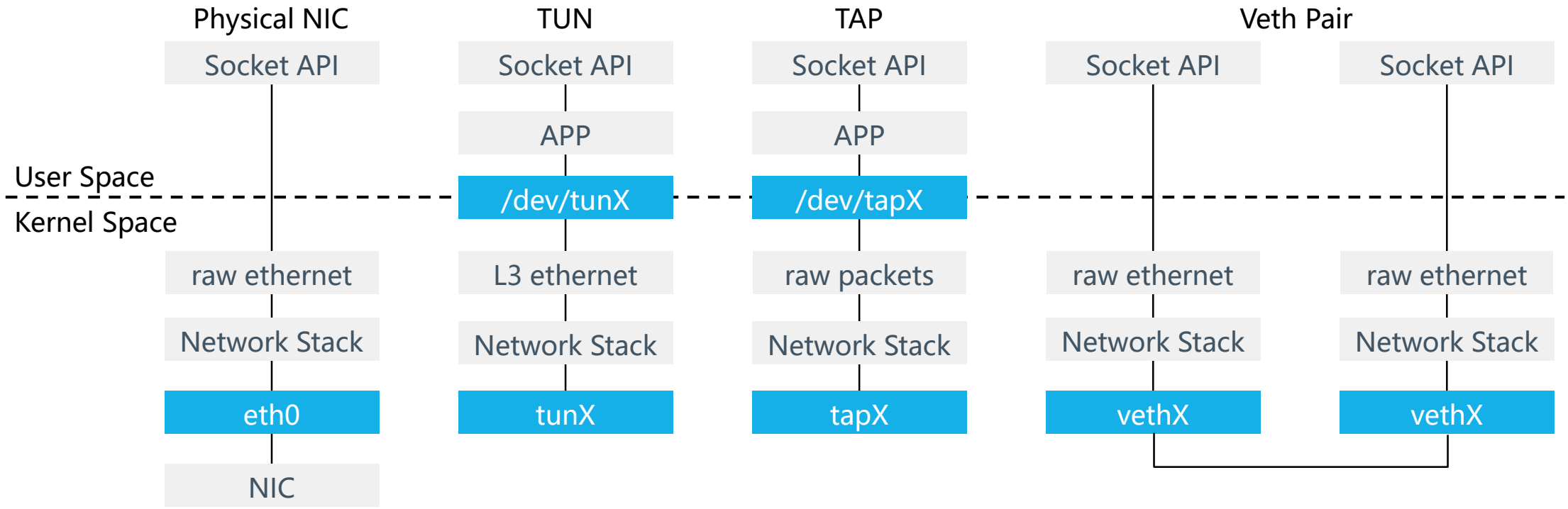

传统物理网络 VS 虚拟网络



# Linux网络虚拟化实现技术

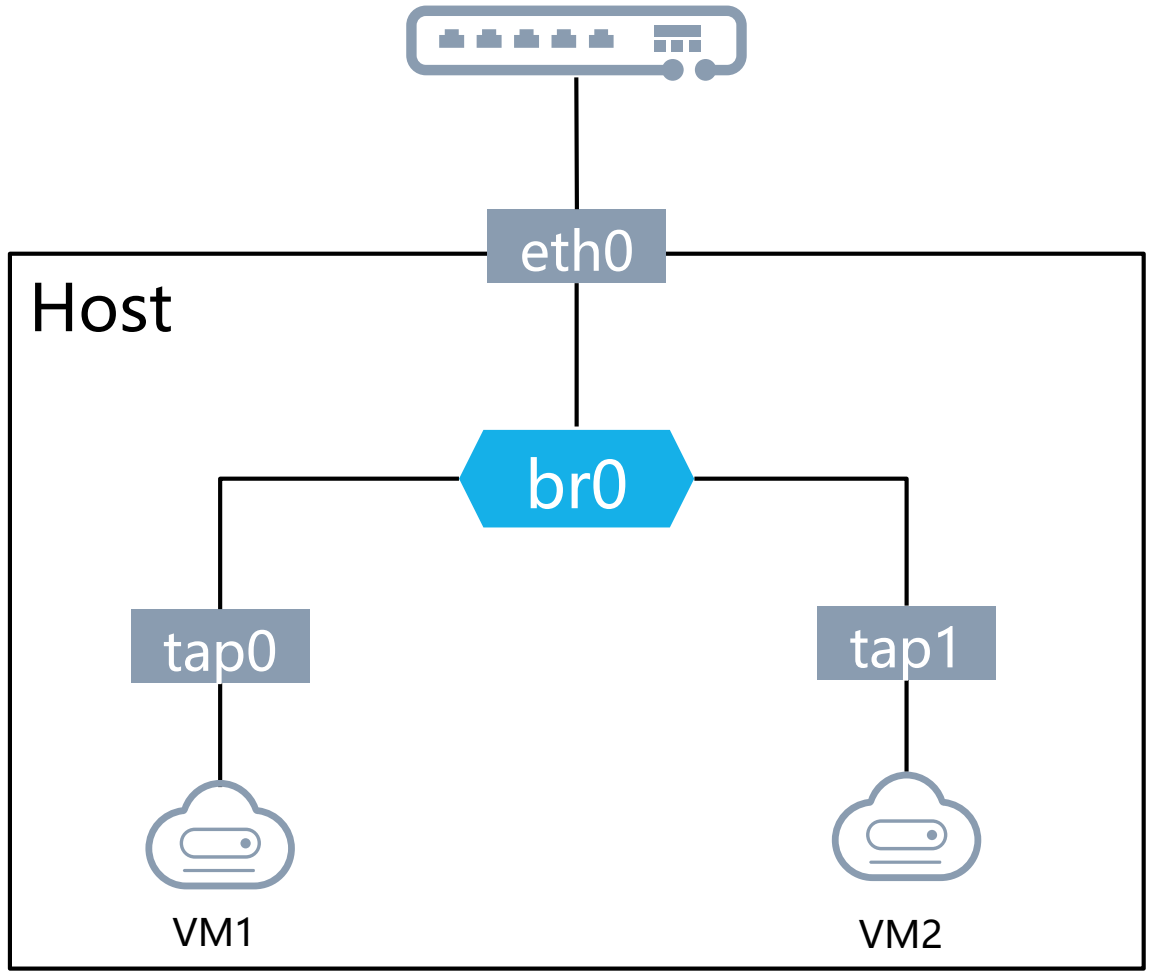
| 网卡虚拟化 | 交换机虚拟化 | 网络隔离 |
| --- | --- | --- |
| • TAP<br>• TUN<br>• VETH | • Linux Bridge<br>• Open vSwitch | • Network Namespace |

# Linux网卡虚拟化 - TAP/TUN/VETH




- TAP设备：模拟一个二层的网络设备，可以接收和发送二层网包。
- TUN设备：模拟一个三层的网络设备，可以接收和发送三层网包。
- VETH：虚拟ethernet接口，通常以pair的方式出现，一端发出的网包，会被另一端接收，可以形成两个网桥之间的通道。

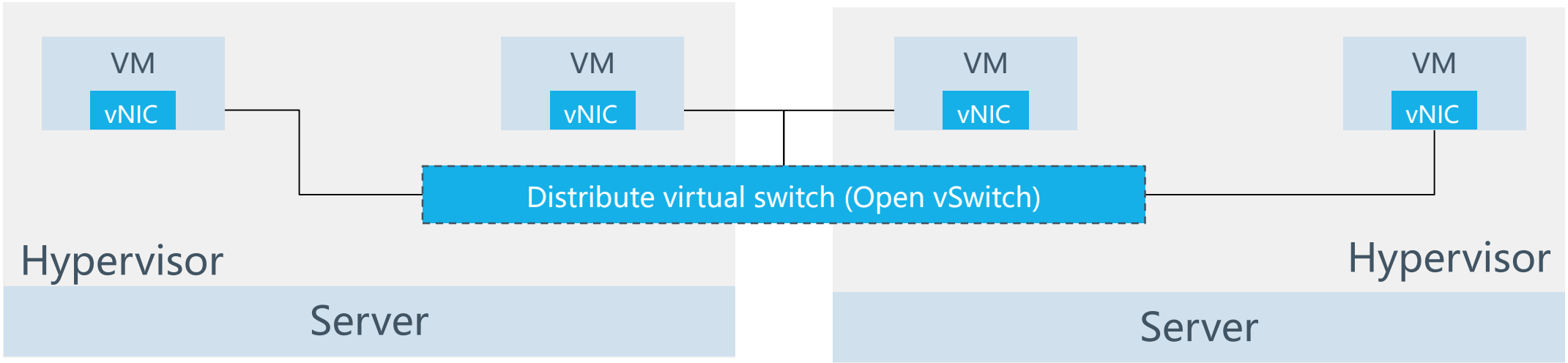
# Linux交换机虚拟化 - Linux bridge




- Linux bridge：工作于二层的网络设备，功能类似于物理交换机。
- Bridge可以绑定Linux上的其他网络设备，并将这些设备虚拟化为端口。
- 当一个设备被绑定到bridge时，就相当于物理交换机端口插入了一条连接着终端的网线。
- 使用brctl命令配置Linux bridge：
  - brctl addbr BRIDGE
  - brctl addif BRIDGE DEVICE

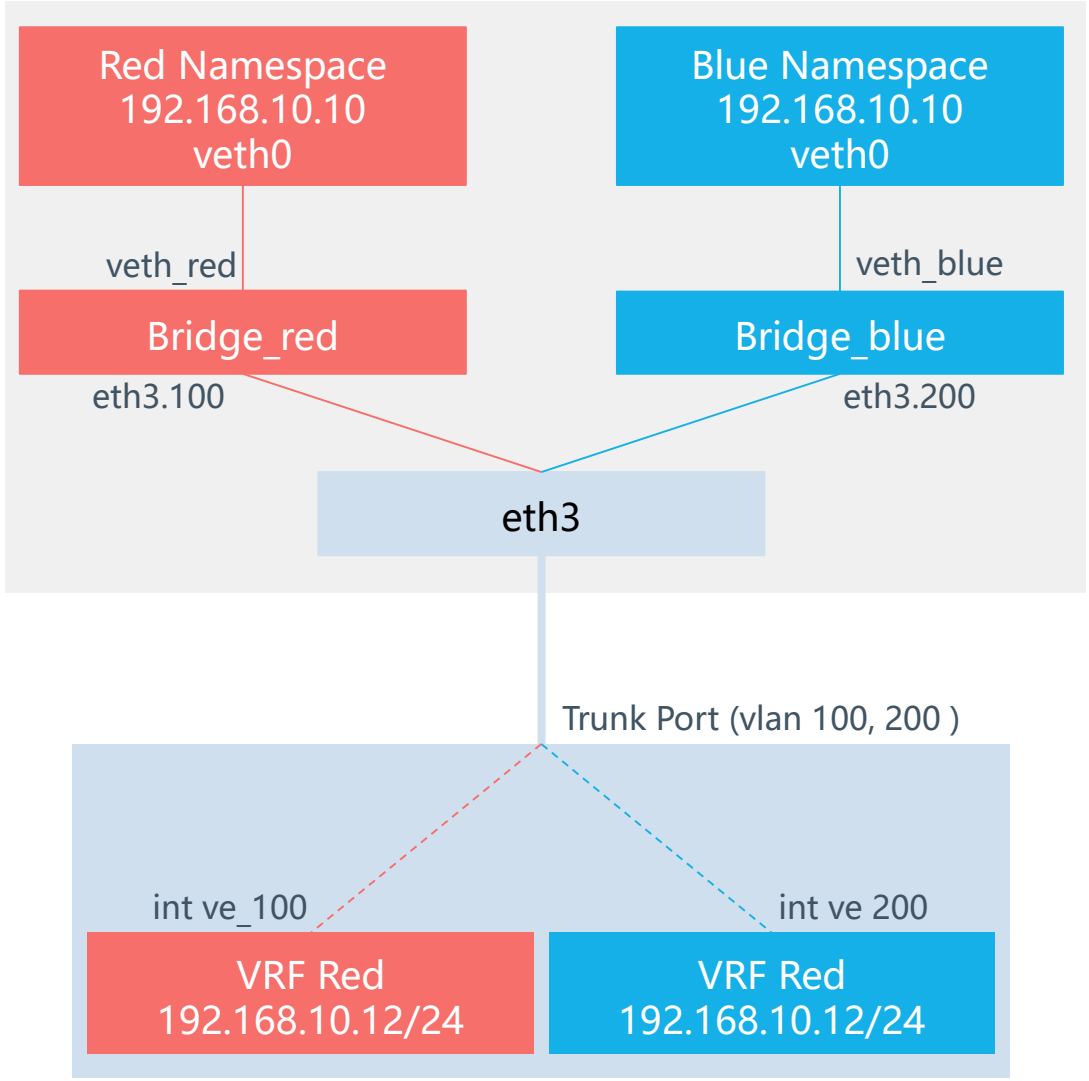
# Linux交换机虚拟化 - Open vSwitch

- Open vSwitch是产品级的虚拟交换机。
  - Linux bridge更适用于小规模，主机内部间通信场景。
  - Open vSwitch更适合于大规模，多主机间通信场景。




- Open vSwitch常用的命令：
  - ovs-vsctl add-br BRIDGE
  - ovs-vsctl add-port PORT
  - ovs-vsctl show BRIDGE
  - ovs-vsctl dump-ports-desc BRIDGE
  - ovs-vsctl dump-flows BRIDGE

# Linux网络隔离 - Network Namespace




- Network namespace能创建多个隔离的网络空间，它们有独自的网络配置信息，例如网络设备、路由表、iptables等。
- 不同网络空间中的虚拟机运行的时候仿佛自己就在独立的网络中。

```
$ ip netns help
Usage: ip netns list
       ip netns add NAME
       ip netns delete NAME
       ip netns identify PID
       ip netns pids NAME
       ip netns exec NAME cmd ...
       ip netns monitor
```

# 讨论：有哪些Linux网络虚拟化技术?

- 如下是OpenStack节点上的ip address截图，请讨论或思考图中有哪些Linux网络虚拟化技术?

```
osbash@controller:~$ ip address
...
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
...
7: tapc1d0ccdc-08@if2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master brq5fe28ac7-4e state UP group default qlen 1000
...
9: brq5fe28ac7-4e: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
...
10: vxlan-28: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1450 qdisc noqueue master brq7b350e42-8c state UNKNOWN group default qlen 1000
```

source: openstack.org

# 目录

# 网络服务Neutron

## NEUTRON

网络服务

首次出现在OpenStack的“Folsom” 版本中。

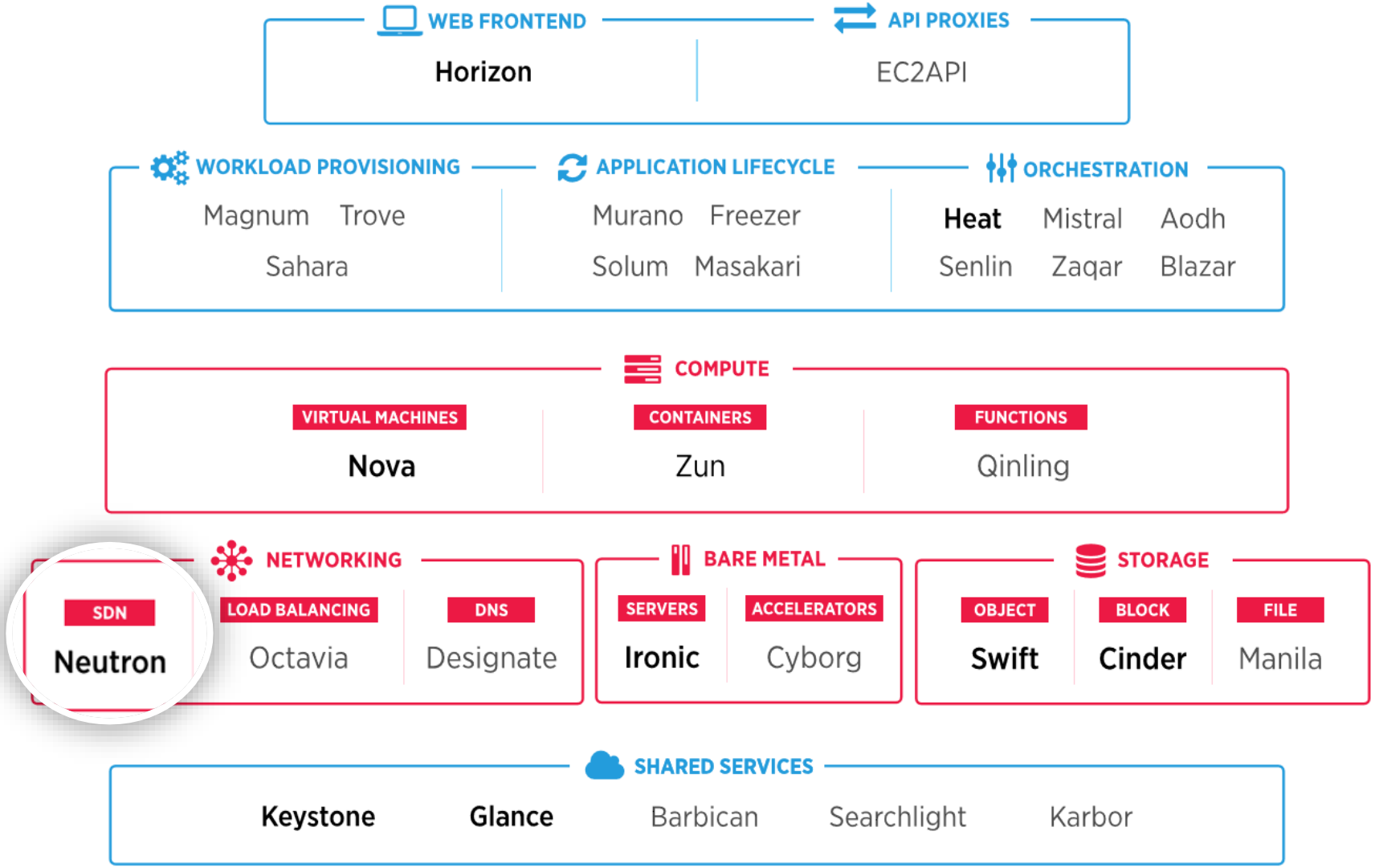
## 简介

Neutron负责管理虚拟网络组件，专注于为OpenStack提供网络即服务（NaaS）。

## 依赖的OpenStack服务

Keystone

# Neutron在OpenStack中的位置和作用

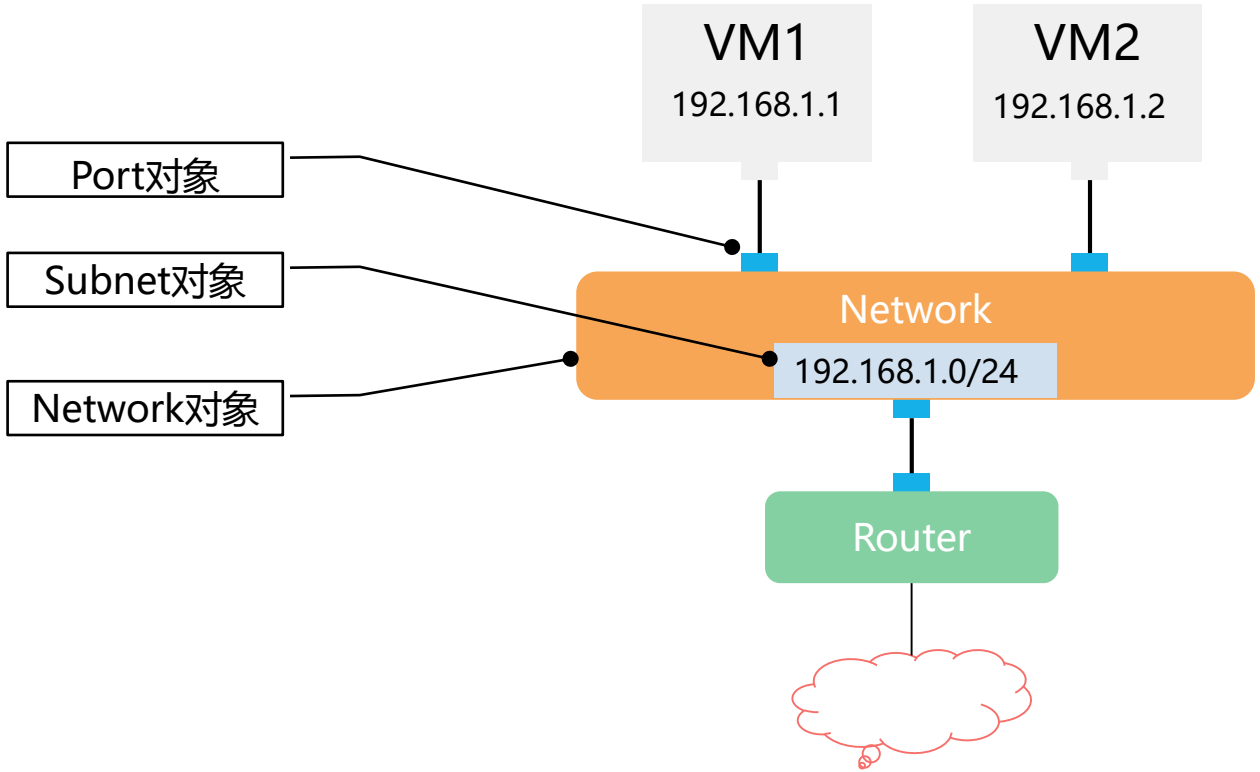



source: openstack.org

# 目录

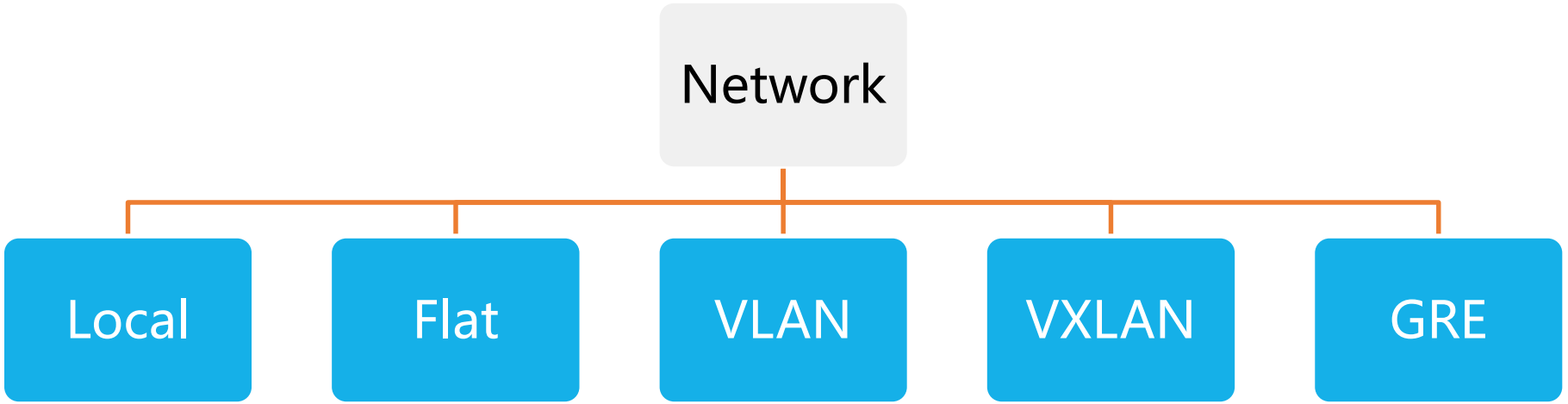
# Neutron概念

- Neutron是一种虚拟网络服务，为Opensack计算提供网络连通和寻址服务。
- 为了便于操作管理，Neutron对网络进行了抽象，有如下基本管理对象：
  - Network
  - Subnet
  - Port
  - Router
  - Floating IP



# Neutron概念 - Network

- Network：网络
  - 一个隔离的、虚拟二层广播域，也可看成一个Virtual Switch，或者Logical Switch。
  - Neutron支持多种类型的Network，包括 Local, Flat, VLAN, VXLAN 和 GRE。



# Neutron概念 - Subnet

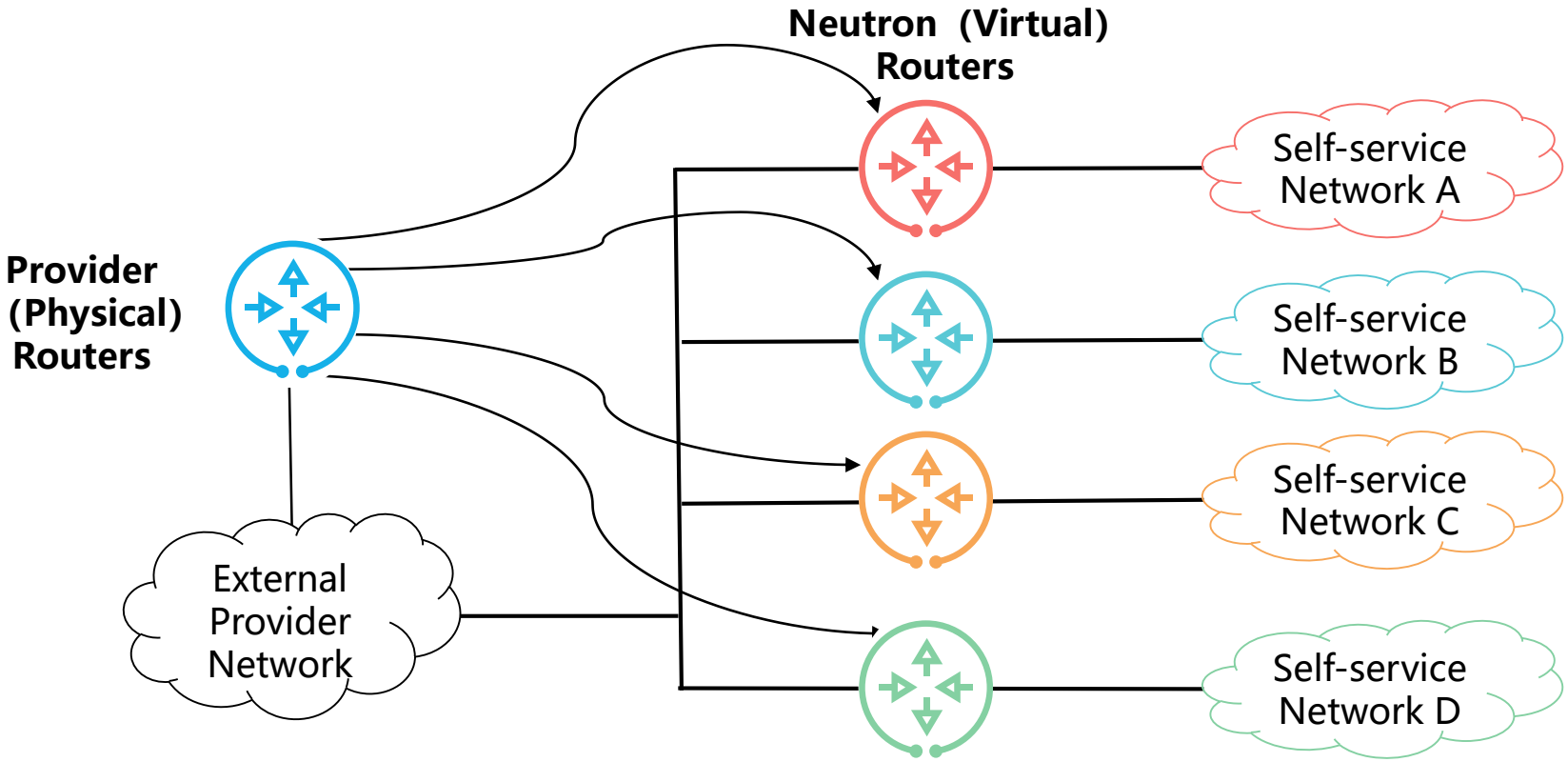
- Subnet：子网
  - 一个IPv4或者IPv6地址段。虚拟机的IP从Subnet中分配。每个Subnet需要定义IP地址的范围和掩码。
  - Subnet必须与Network关联。
  - Subnet可选属性：DNS，网关IP，静态路由。

# Neutron概念 - Port

- Port：端口
  - 逻辑网络交换机上的虚拟交换端口
  - 虚拟机通过Port附着到Network上
  - Port可以分配IP地址和Mac地址

# Neutron概念 - Router

- Router：路由器
  - 连接租户内同一Network或不同Network之间的子网，以及连接内外网。

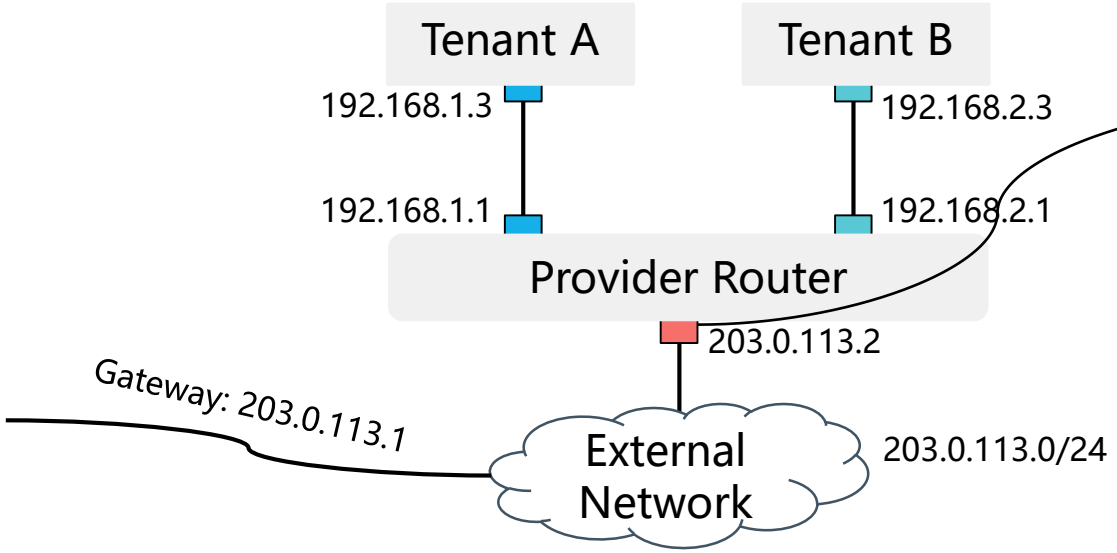


# Neutron概念 - Fixed IP

- Fixed IP：固定IP
  - 分配到每个端口上的IP，类似于物理环境中配置到网卡上的IP。

# Neutron概念 - Floating IP

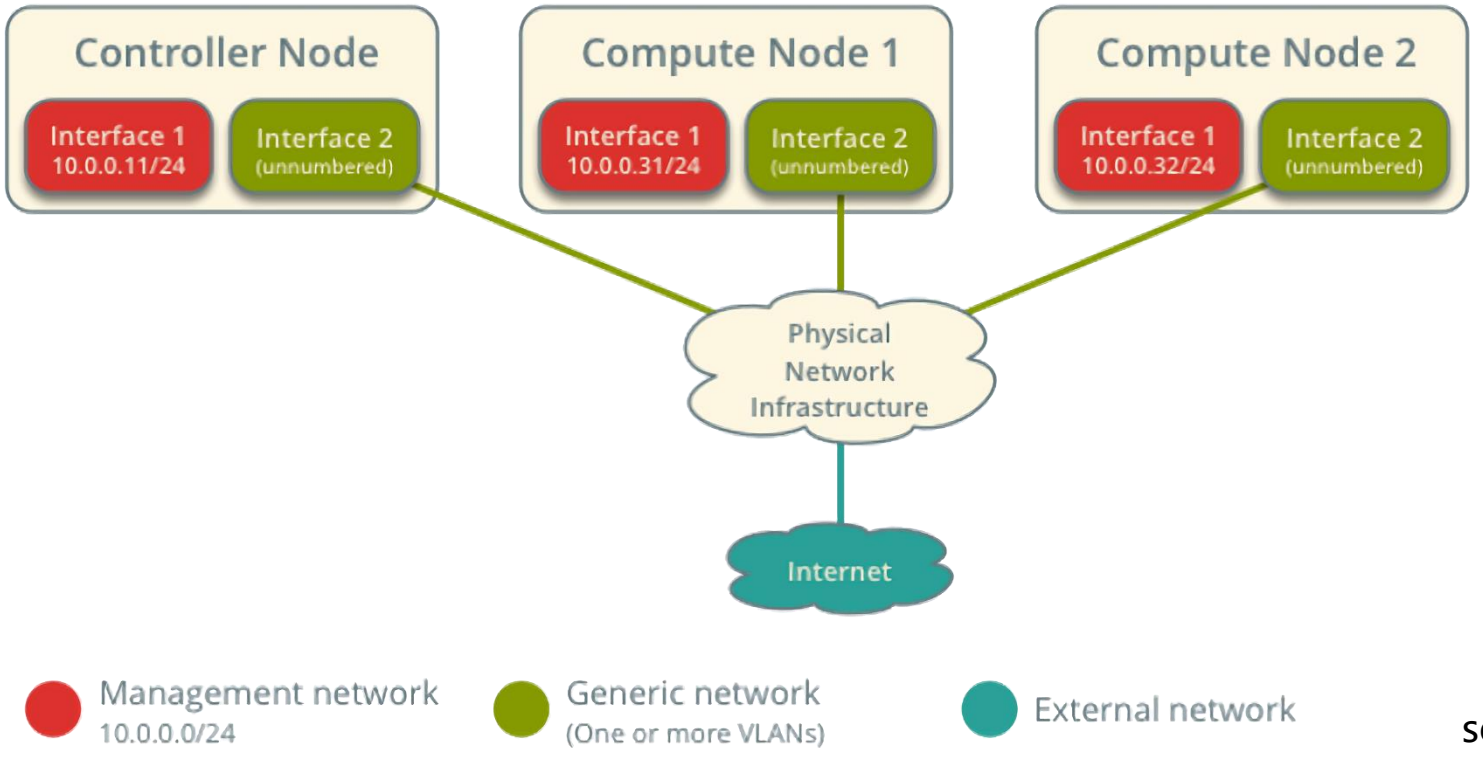
- Floating IP：浮动IP
  - Floating IP是从External Network创建的一种特殊Port，可以将Floating IP绑定到任意Network中的Port上，底层会做NAT转发，将发送给Floating IP的流量转发到该Port对应的Fixed IP上。
  - 外界可以通过Floating IP访问虚拟机，虚拟机也可以通过Floating IP访问外界。




| NAT Table | |
|---|---|
| Fixed IP | Floating IP |
| 192.168.1.3 | 203.0.113.30 |
| 192.168.2.3 | 203.0.113.40 |

# Neutron概念 - Physical Network

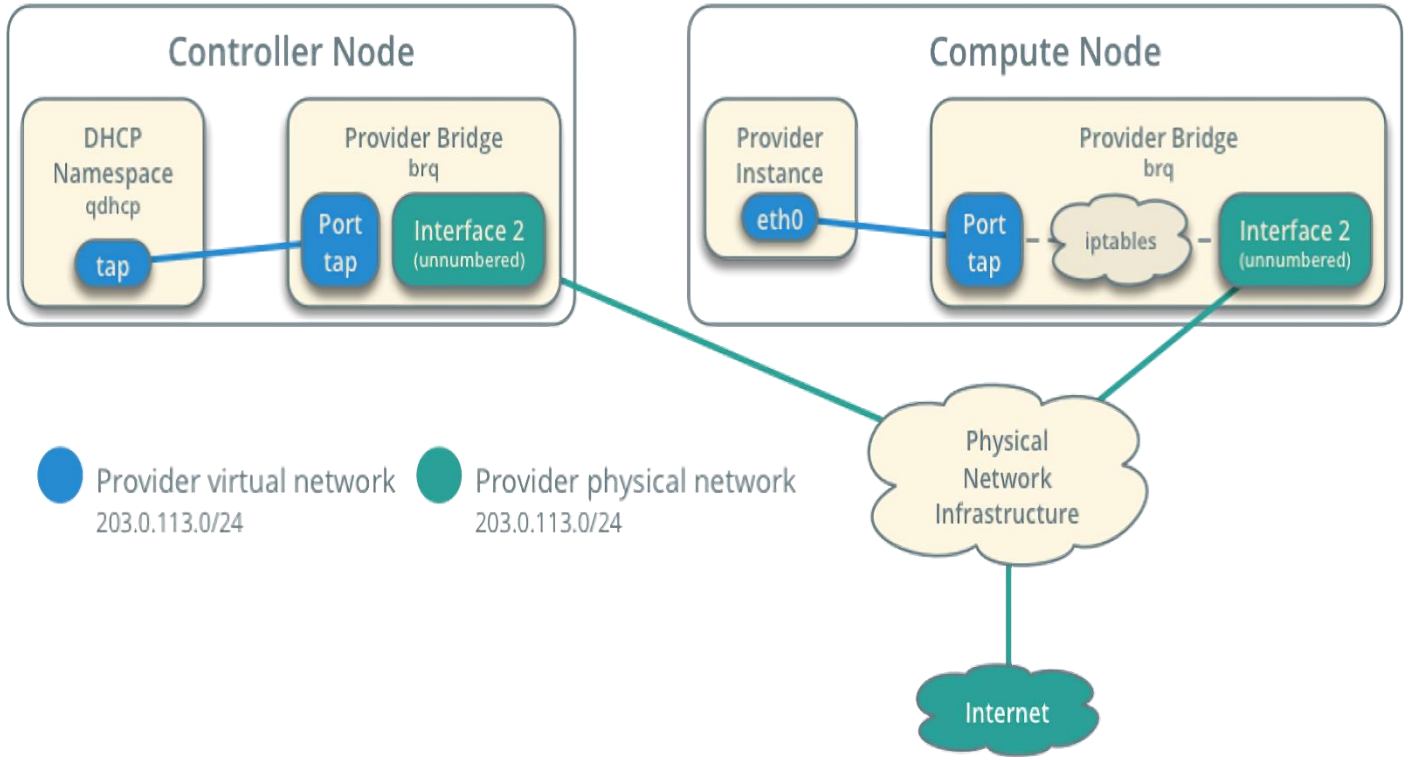
- Physical Network：物理网络
  - 在物理网络环境中连接OpenStack不同节点的网络，每个物理网络可以支持Neutron中的一个或多个虚拟网络。




source: openstack.org

# Neutron概念 - Provider Network

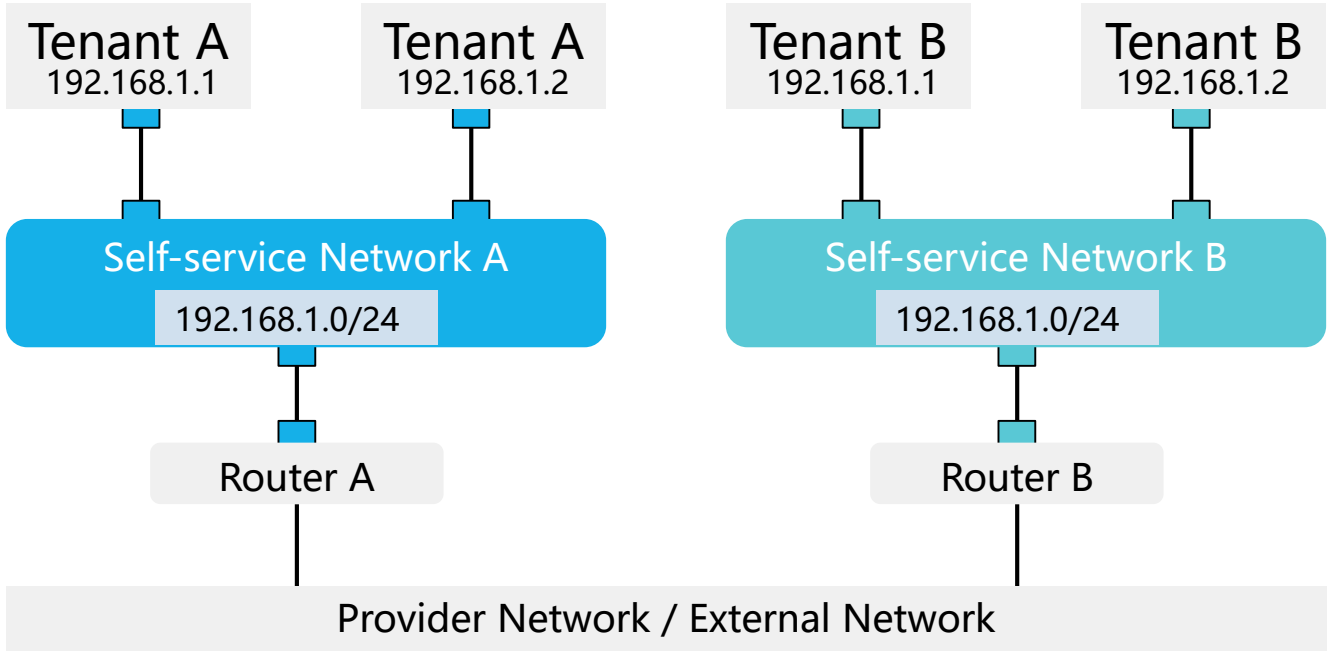
- Provider Network：
  - 由OpenStack管理员创建的，直接对应于数据中心现有物理网络的一个网段。
  - Provider Network通常使用VLAN或者Flat模式，可以在多个租户之间共享。




source: openstack.org

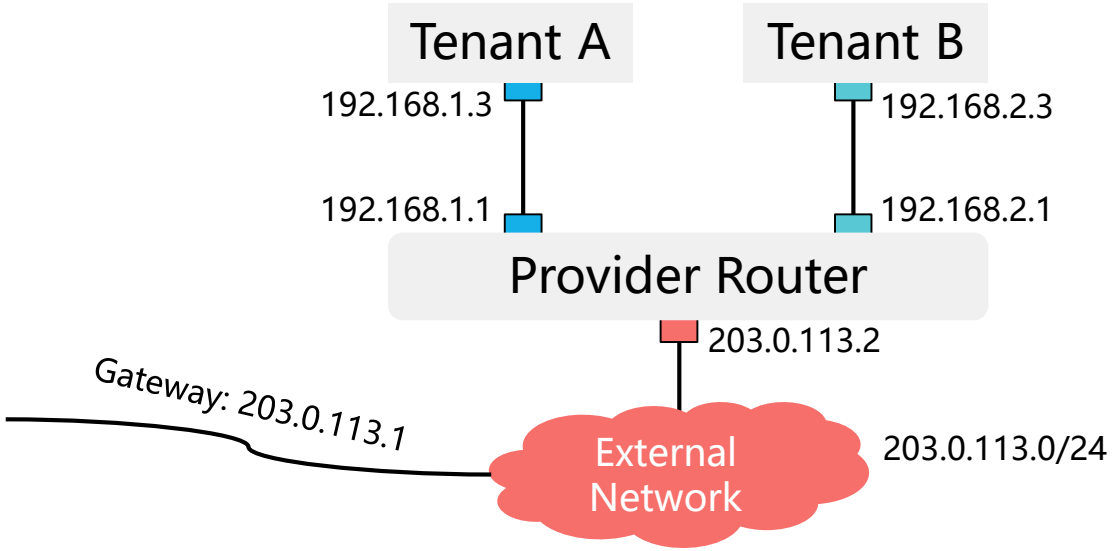
# Neutron概念 - Self-service Network

- Self-service Network：自助服务网络，也叫租户网络或项目网络
  - 由OpenStack租户创建的，完全虚拟的，只在本网络内部连通，不能在租户间共享。
  - Self-service Network通常使用VXLAN或者GRE模式，可以通过Virtual Router的SNAT与Provider Network 通信。

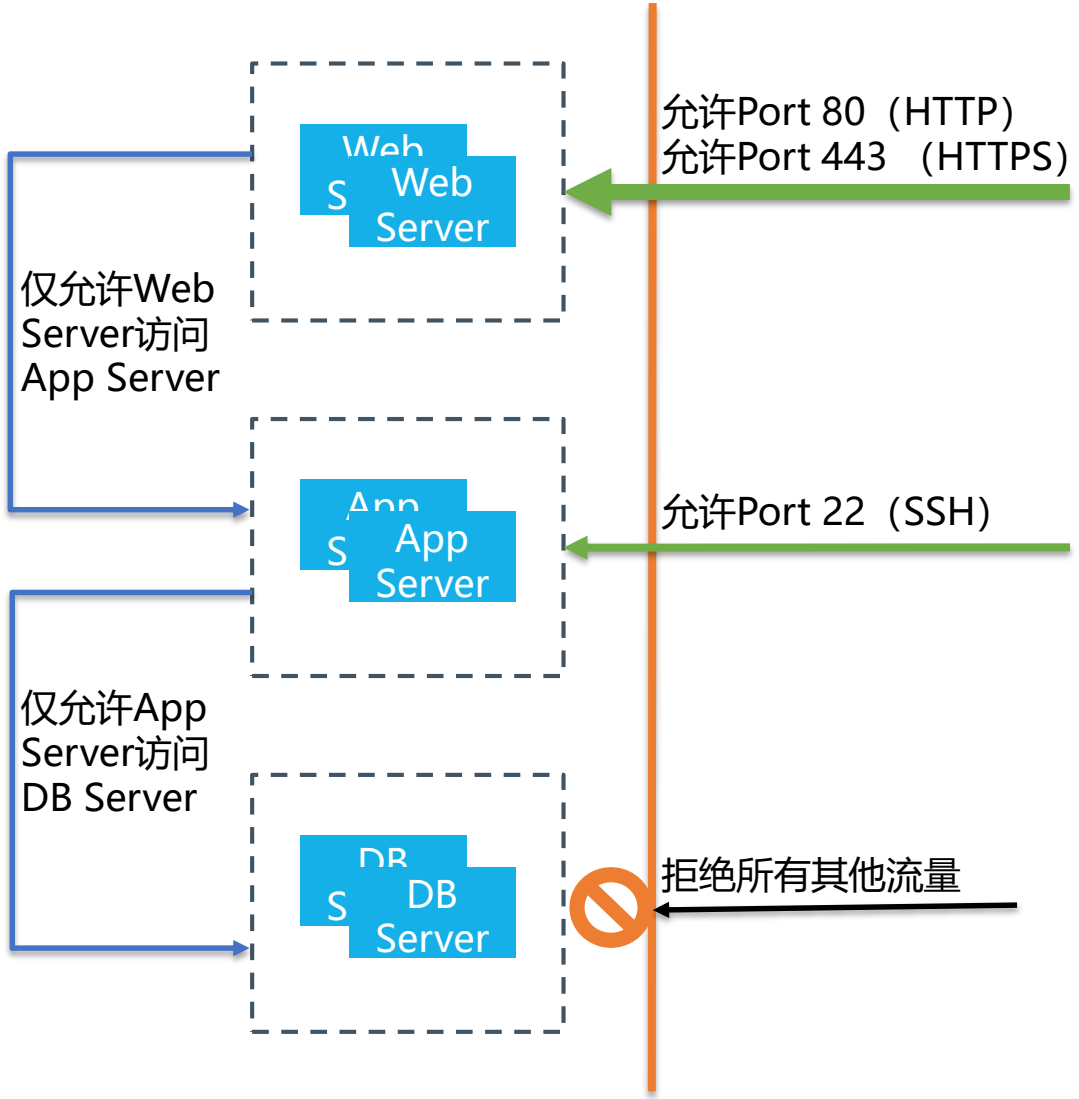


# Neutron概念 - External Network

- External Network：外部网络，也叫公共网络
  - 一种特殊的Provider Network，连接的物理网络与数据中心或Internet相通，网络中的Port可以访问外网。
  - 一般将租户的Virtual Router连接到该网络，并创建Floating IP绑定虚拟机，实现虚拟机与外网通信。

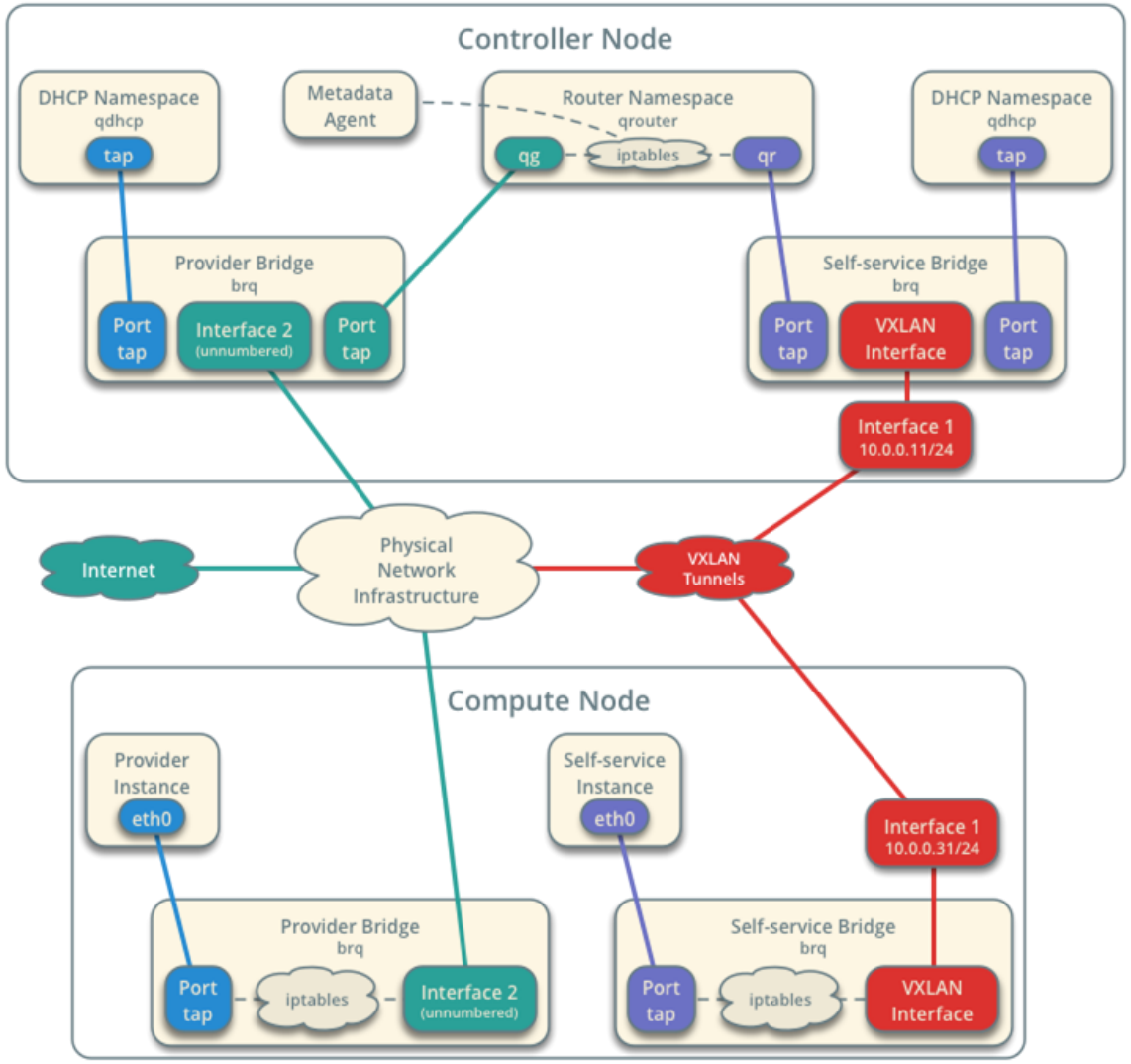


# Neutron概念 - Security Group




- Security Group：安全组
  - 安全组是作用在neutron port上的一组策略，规定了虚拟机入口和出口流量的规则。
  - 安全组基于Linux iptables实现。
  - 安全组默认拒绝所有流量，只有添加了放行规则的流量才允许通过。
  - 每个OpenStack项目中都有一个default默认安全组，默认包含如下规则：
    - 拒绝所有入口流量、允许所有出口流量

# 示例：Neutron概念与真实环境结合



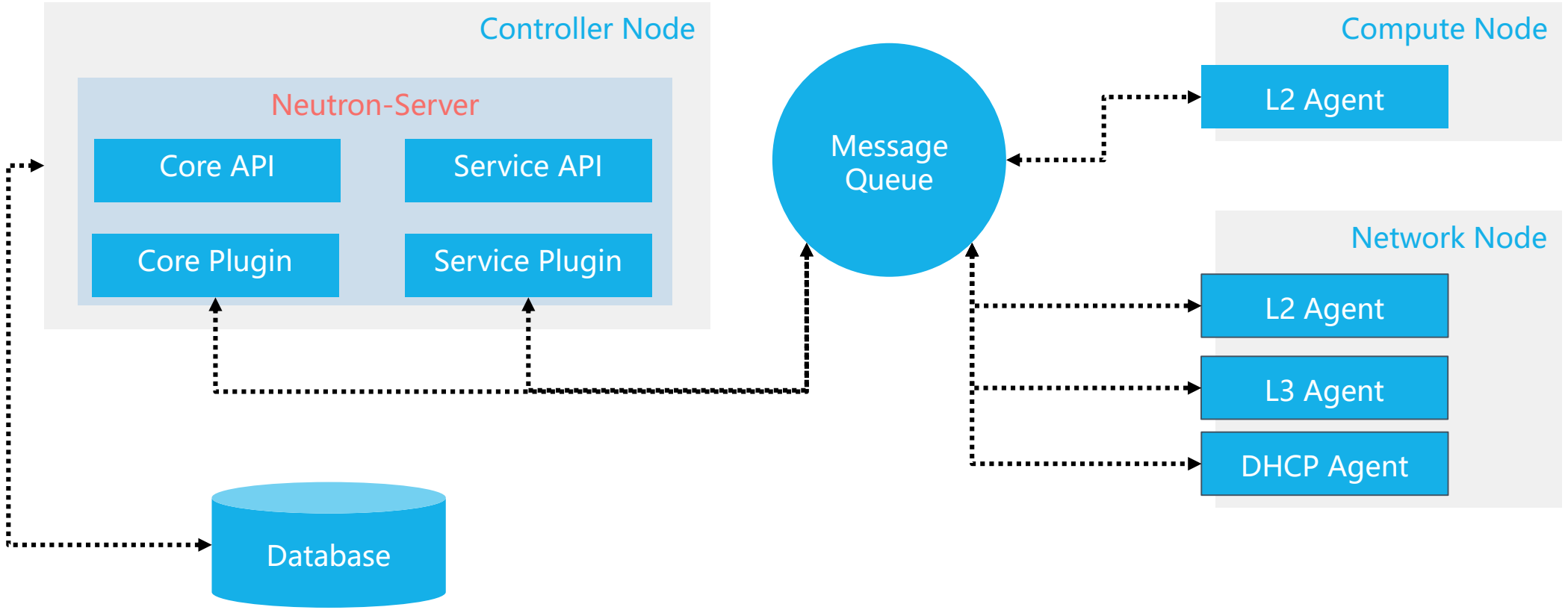

- Provider virtual network 203.0.113.0/24
- Provider physical network 203.0.113.0/24
- Management physical network 10.0.1.0/24
- Self-service virtual network 172.16.1.0/24

挑战一下：
请尝试将Neutron网络转换成物理网络。

source: openstack.org

# 目录

# Neutron架构图



# Neutron架构说明

- Neutron的架构是基于插件的，不同的插件提供不同的网络服务，主要包含如下组件：

| Neutron Server | Plugin | Agent |
| --- | --- | --- |
| • 对外提供网络API，并调用Plugin处理请求。 | • 处理Neutron server的请求，维护网络状态，并调用Agent处理请求。 | • 处理Plugin的请求，调用底层虚拟或物理网络设备实现各种网络功能。 |

✓Neutron Server

✓Core Plugin

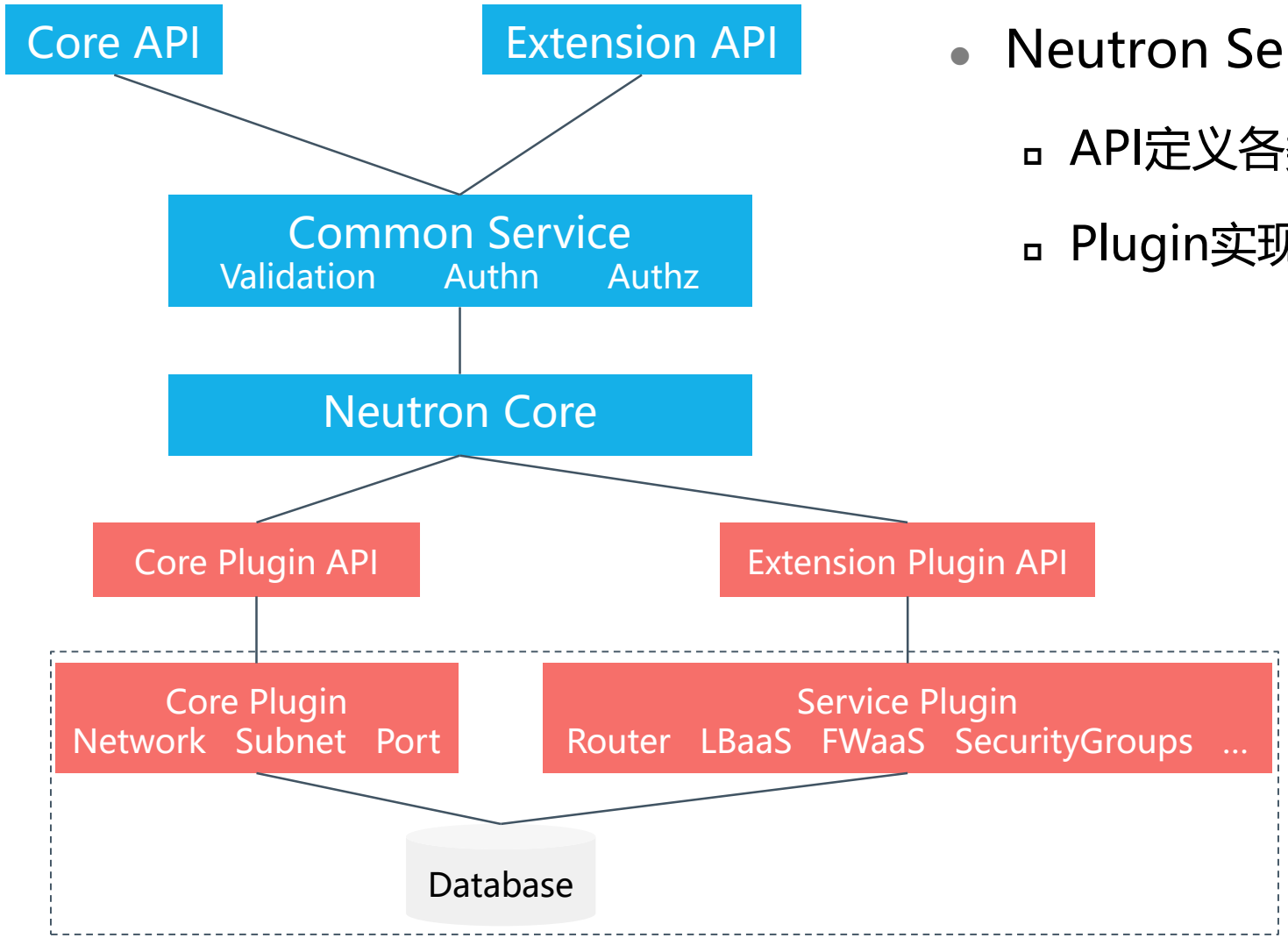
✓Service Plugin

- L3 Service Plugin
- LB Service Plugin
- Firewall Service Plugin
- VPN Service Plugin

✓各种Agent

- L2 （ovs-agent）
- L3 Agent
- DHCP Agent
- MetaData Agent

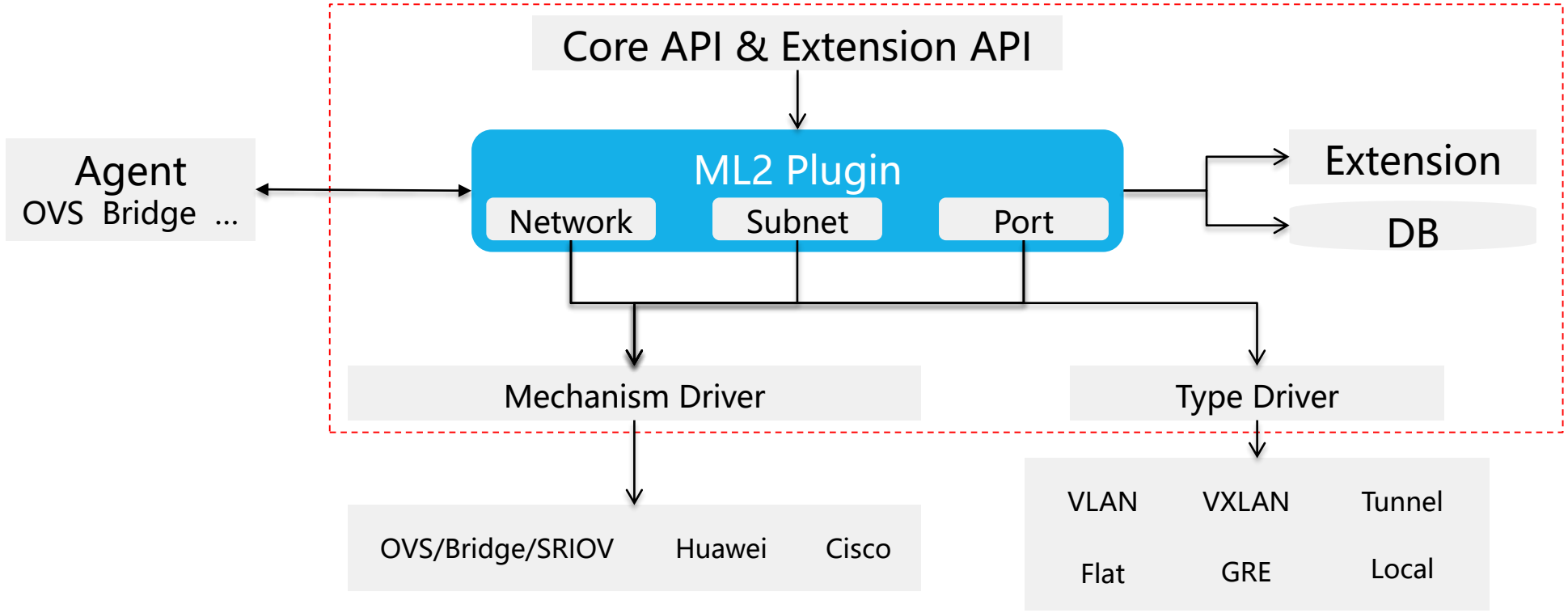
# Neutron组件 - Neutron Server




- Neutron Server = APIs + Plugins
  - API定义各类网络服务
  - Plugin实现各类网络服务

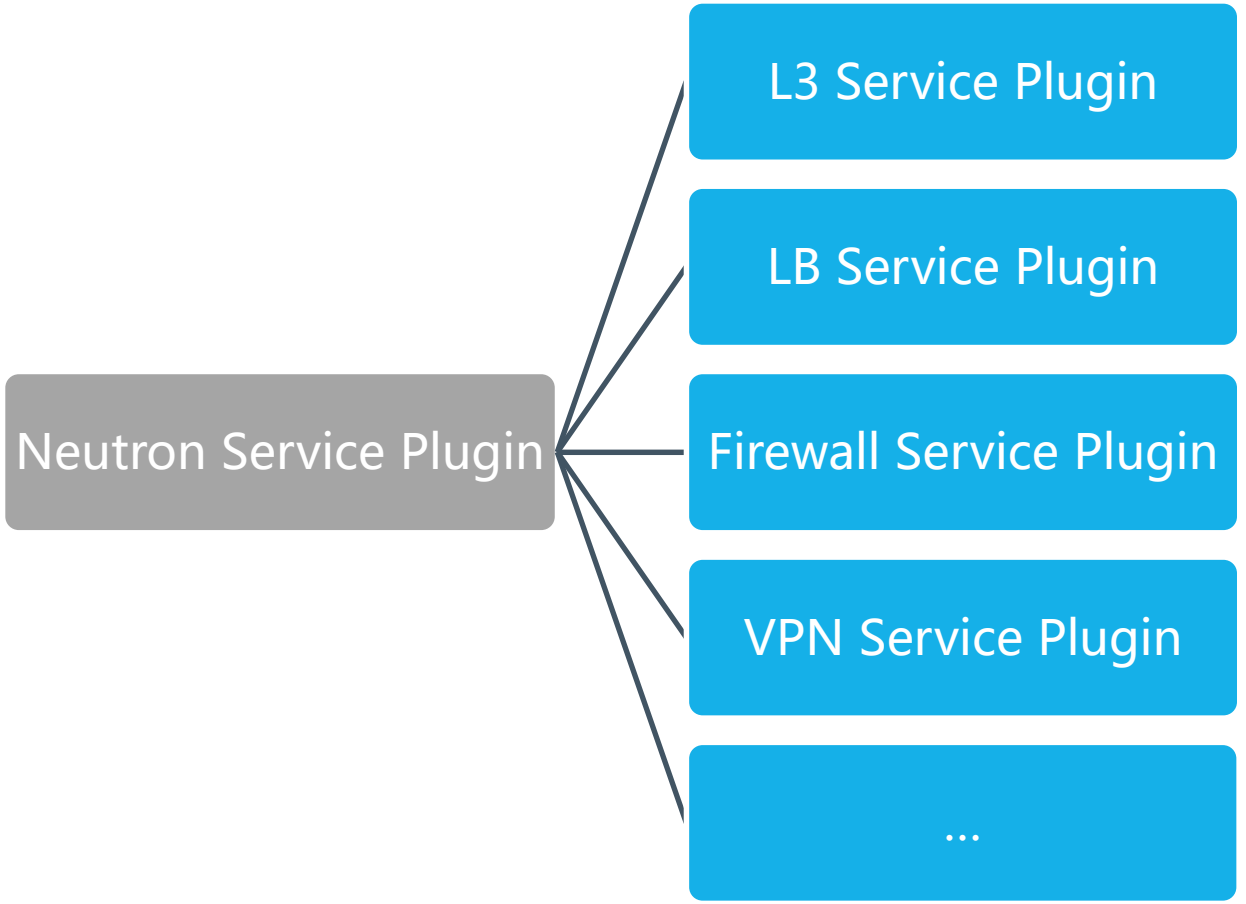
# Neutron组件 - Core Plugin

- Core Plugin，主要是指ML2 Plugin，是一个开放性框架，在一个plugin下，可以集成各个厂家、各种后端技术支持的Layer 2网络服务。
  - 通过Type Driver和Mechanism Driver调用不同的底层网络技术，实现二层互通。



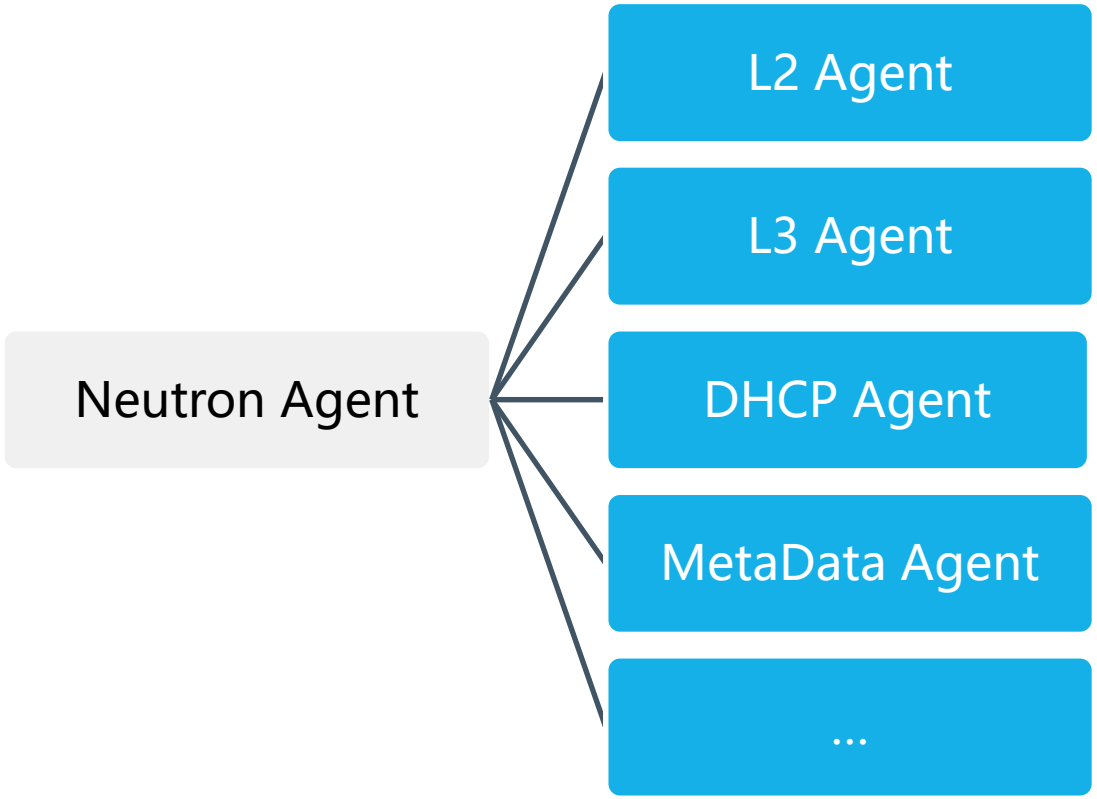
# Neutron组件 - Service Plugin

- Service Plugin用于实现高阶网络服务，例如路由、负载均衡、防火墙和VPN服务等。



# Neutron组件 - Agent

- Neutron Agent向虚拟机提供二层和三层的网络连接、完成虚拟网络和物理网络之间的转换、提供扩展服务等。



# 目录

# Neutron操作 - 常用命令

- neutron net-create
- neutron net-list
- neutron subnet-list
- neutron port-create
- neutron router-interface-add
- neutron agent-list

# 动手实验：Neutron操作

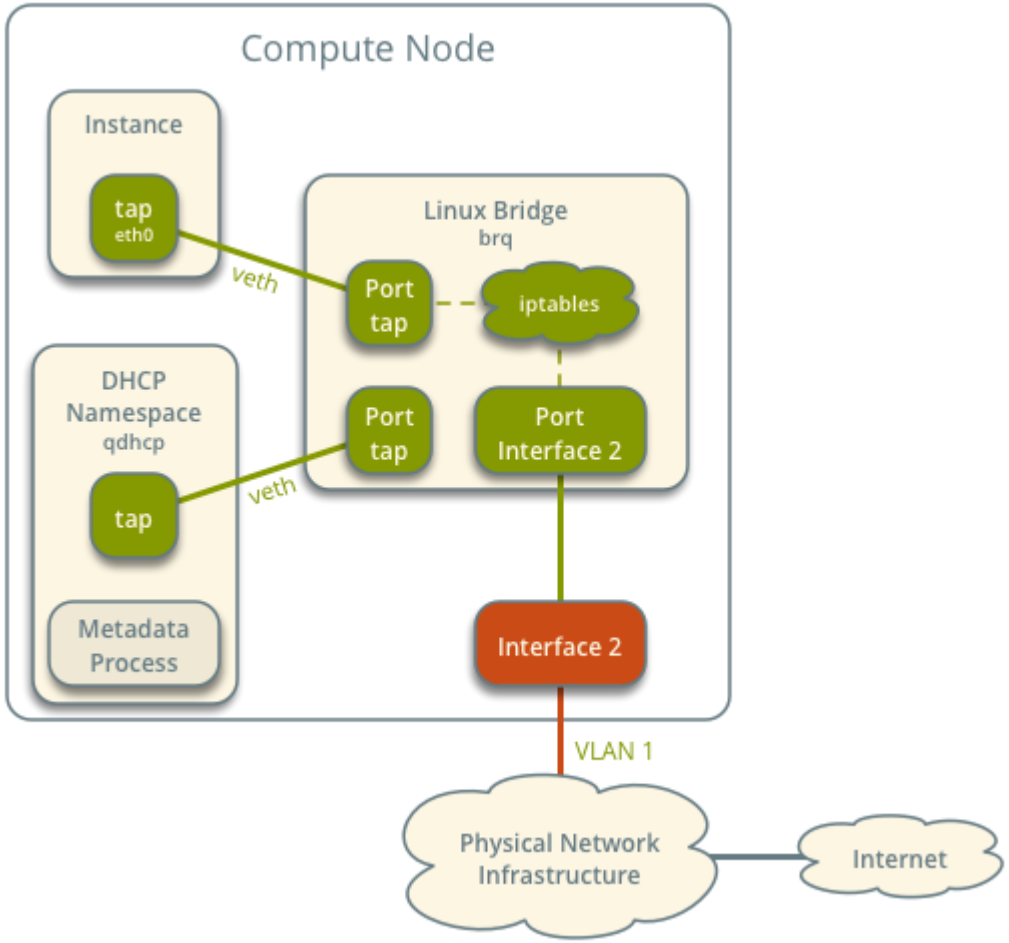
- 命令help
- 管理网络、子网、端口
- 管理路由器
- 管理浮动IP
- 管理安全组及规则
- 虚拟机实例访问测试

# 目录

# Neutron网络典型场景介绍

- Neutron支持多种多样的网络技术和类型，可以自由组合各种网络模型。
- 如下两种网络模型是OpenStack生产环境中常用的：
  - Linux Bridge + Flat/VLAN网络
    - 仅提供简单的网络互通，虚拟网络、路由、负载均衡等由物理设备提供。
    - 网络简单、高效，适合中小企业私有云网络场景。
  - Open vSwitch + VXLAN网络
    - 提供多租户、大规模网络隔离能力，适合大规模私有云和公有云网络场景。

# Linux Bridge + Flat网络



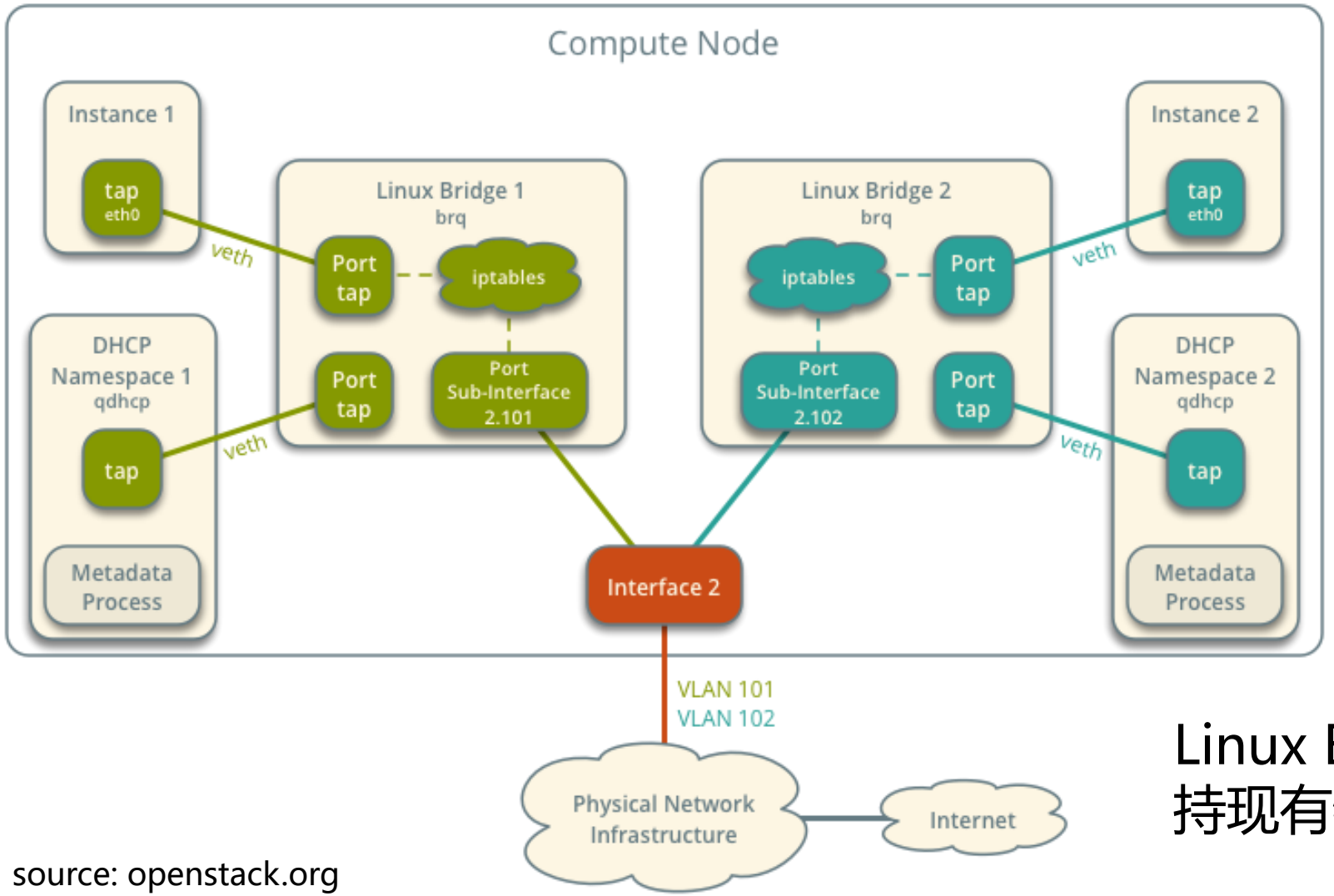

Provider network
Aggregate

Provider network 1
VLAN 1 (untagged)

Linux Bridge + Flat是最简单的网络模型，直接使用现有物理网络配置。

source: openstack.org

# Linux Bridge + VLAN网络




source: openstack.org

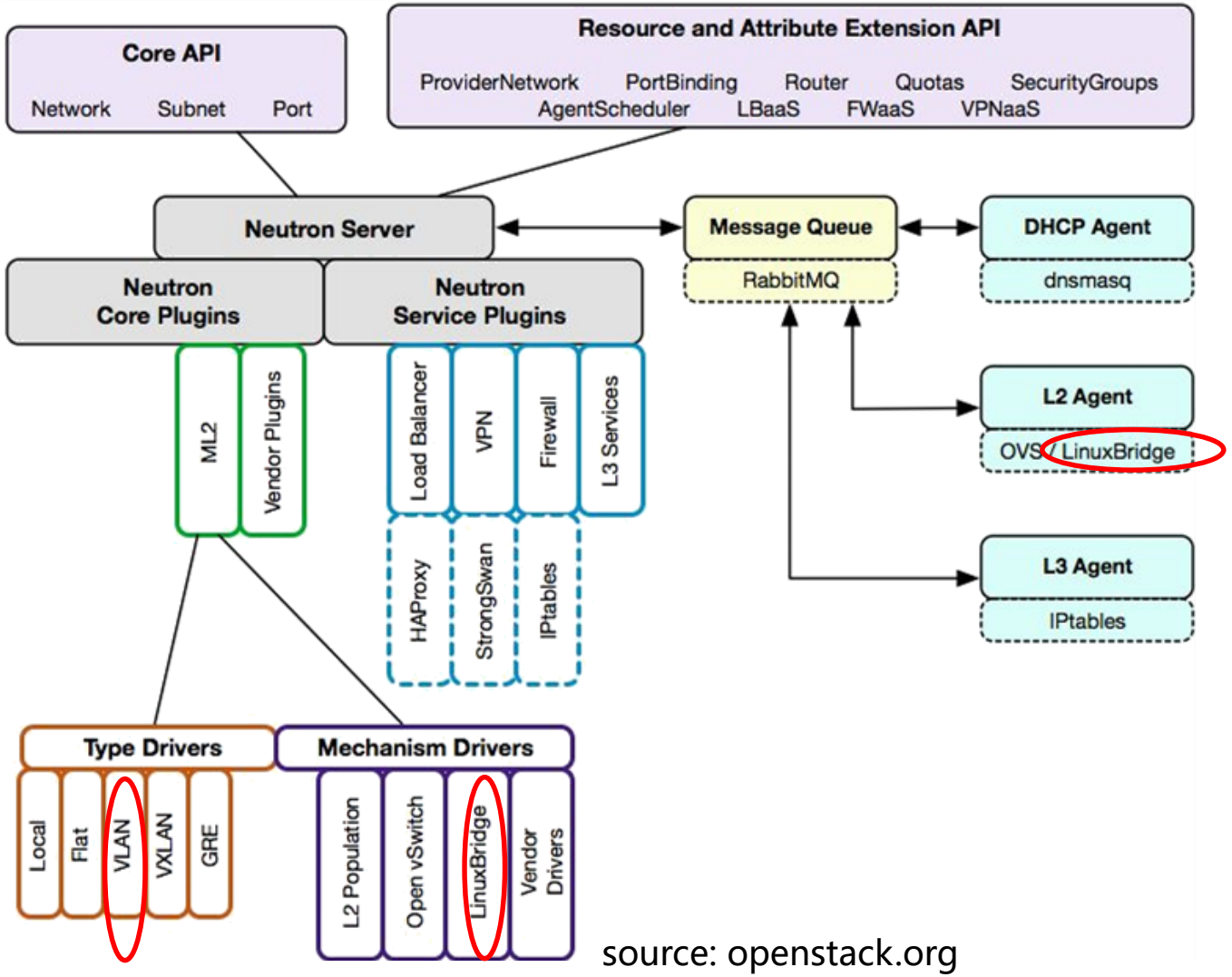
Provider network Aggregate

Provider network 1 VLAN 101

Provider network 1 VLAN 102

Linux Bridge + VLAN支持现有物理网络VLAN隔离。

# Linux Bridge + VLAN实现



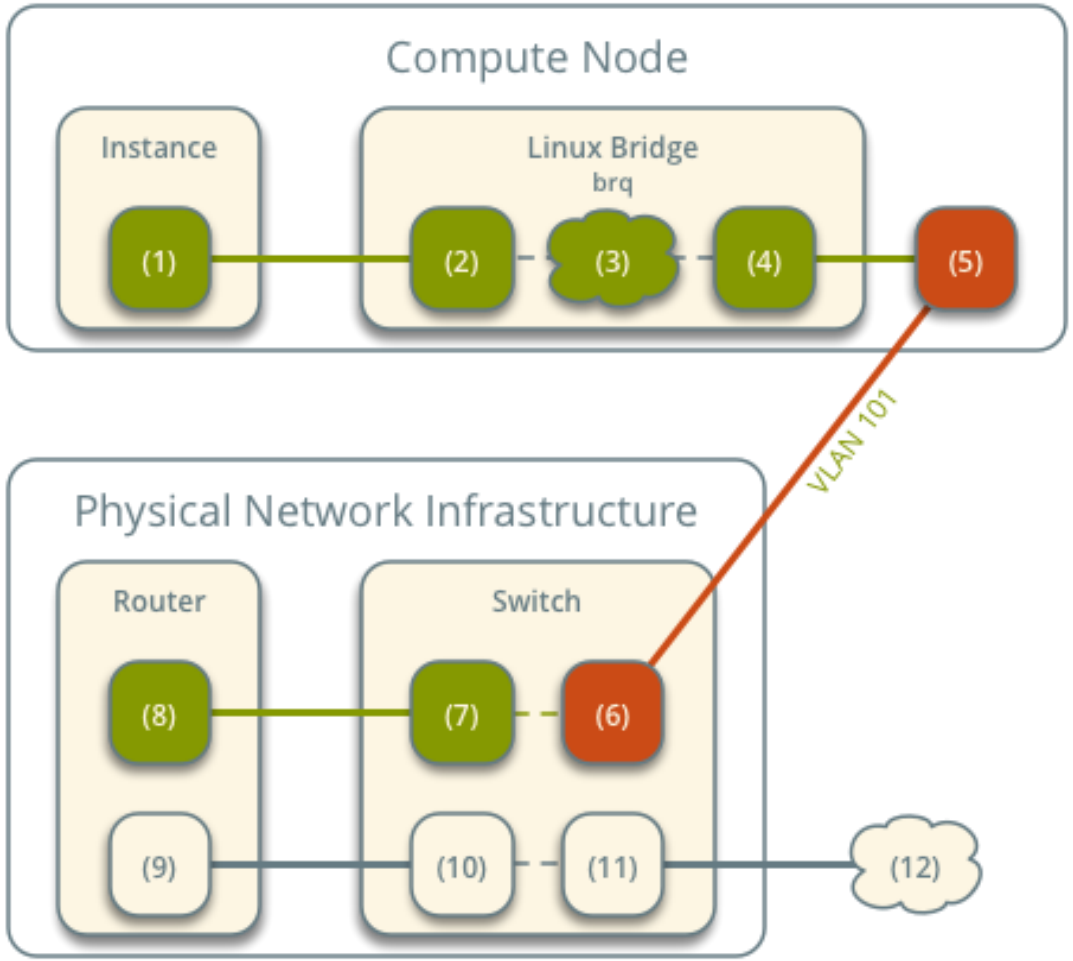

source: openstack.org

- 使用Linux Bridge + VLAN网络时：
  - ML2的Type Driver为VLAN
  - ML2的Mechanism Driver为LinuxBridge
  - L2 Agent为LinuxBridge

# Linux Bridge + VLAN场景说明

- 使用Linux Bridge + VLAN实现Provider Network，网络流量可以分为如下几种：
  - 南北向流量：虚拟机和外部网络（例如Internet）通信的流量
  - 东西向流量：虚拟机之间的流量
  - Provider Network和外部网络之间的流量：由物理网络设备负责交换和路由。
- 后续的网络流量分析基于如下示例：
  - Provider network 1 (VLAN)
    - VLAN 101 (tagged)，IP 地址段203.0.113.0/24，网关203.0.113.1 （物理网络设备上）
  - Provider network 2 (VLAN)
    - VLAN 102 (tagged)，IP地址段192.0.2.0/24，网关192.0.2.1（vRouter端口上）

# 使用Fixed IP的虚拟机南北流量分析



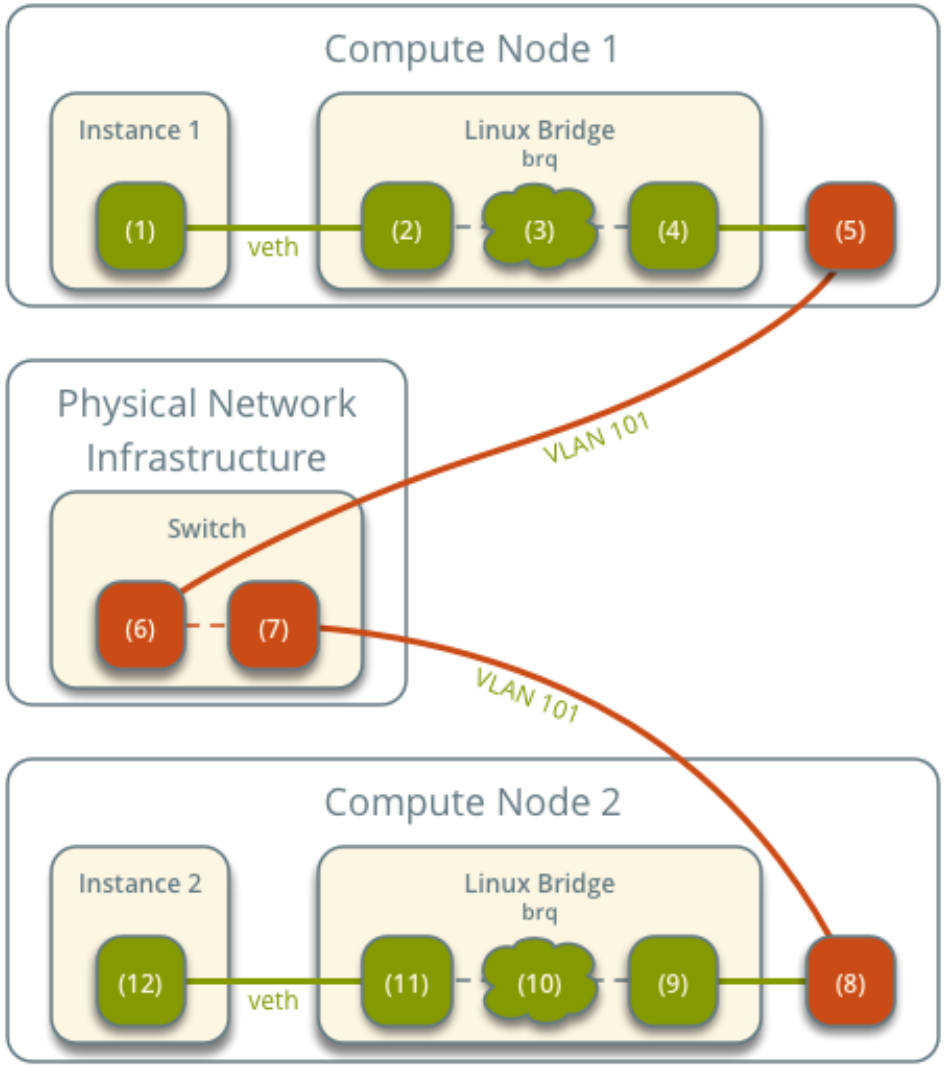

source: openstack.org

Provider network
Aggregate

Provider network 1
VLAN 101, 203.0.113.0/24

- 场景说明：
  - 虚拟机运行在计算节点1上，使用Provider network 1。
  - 虚拟机将数据包发送到Internet上的主机。

# 同一个网络中虚拟机东西流量分析



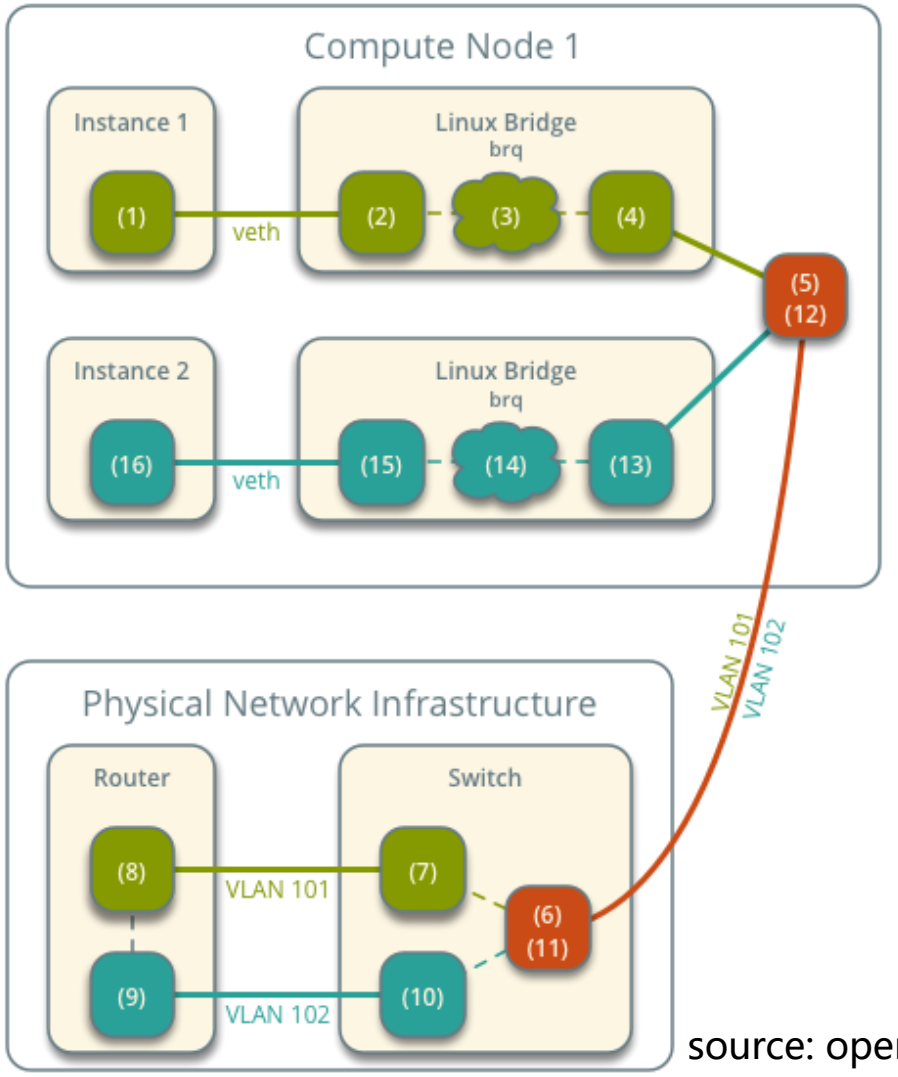

Provider network
Aggregate

Provider network 1
VLAN 101, 203.0.113.0/24

- 场景说明：
  - 虚拟机运行在计算节点1上，使用Provider network 1。
  - 虚拟机将数据包发送到Internet上的主机。

source: openstack.org

# 不同网络中虚拟机东西流量




source: openstack.org

Provider network
Aggregate

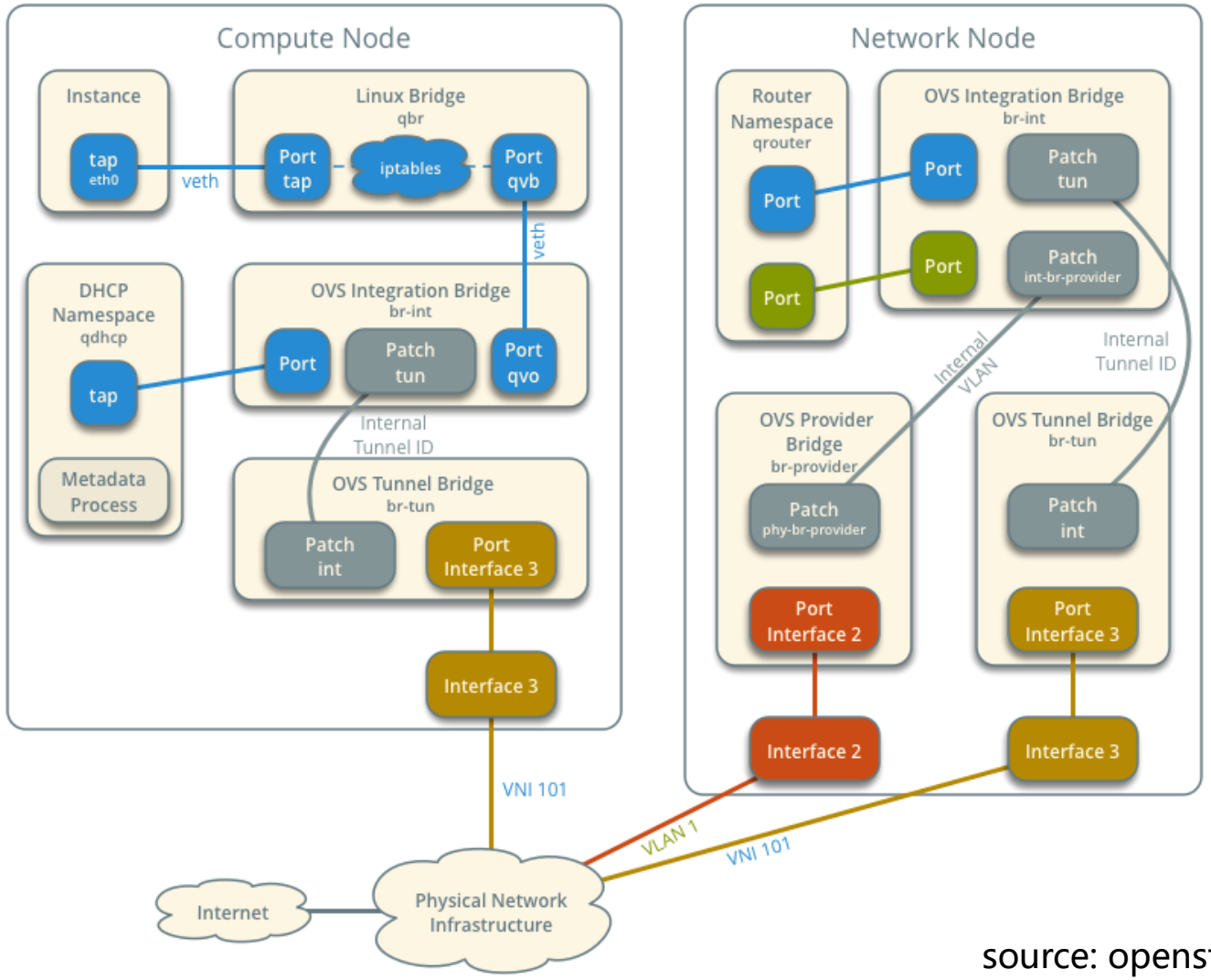
Provider network 1
VLAN 101, 203.0.113.0/24

Provider network 2
VLAN 102, 192.0.2.0/24

- 场景说明：
  - 虚拟机1运行在计算节点1上，使用Provider network 1。
  - 虚拟机2运行在计算节点1上，使用Provider network 2。
  - 虚拟机1将数据包发送到虚拟机2。

# 目录

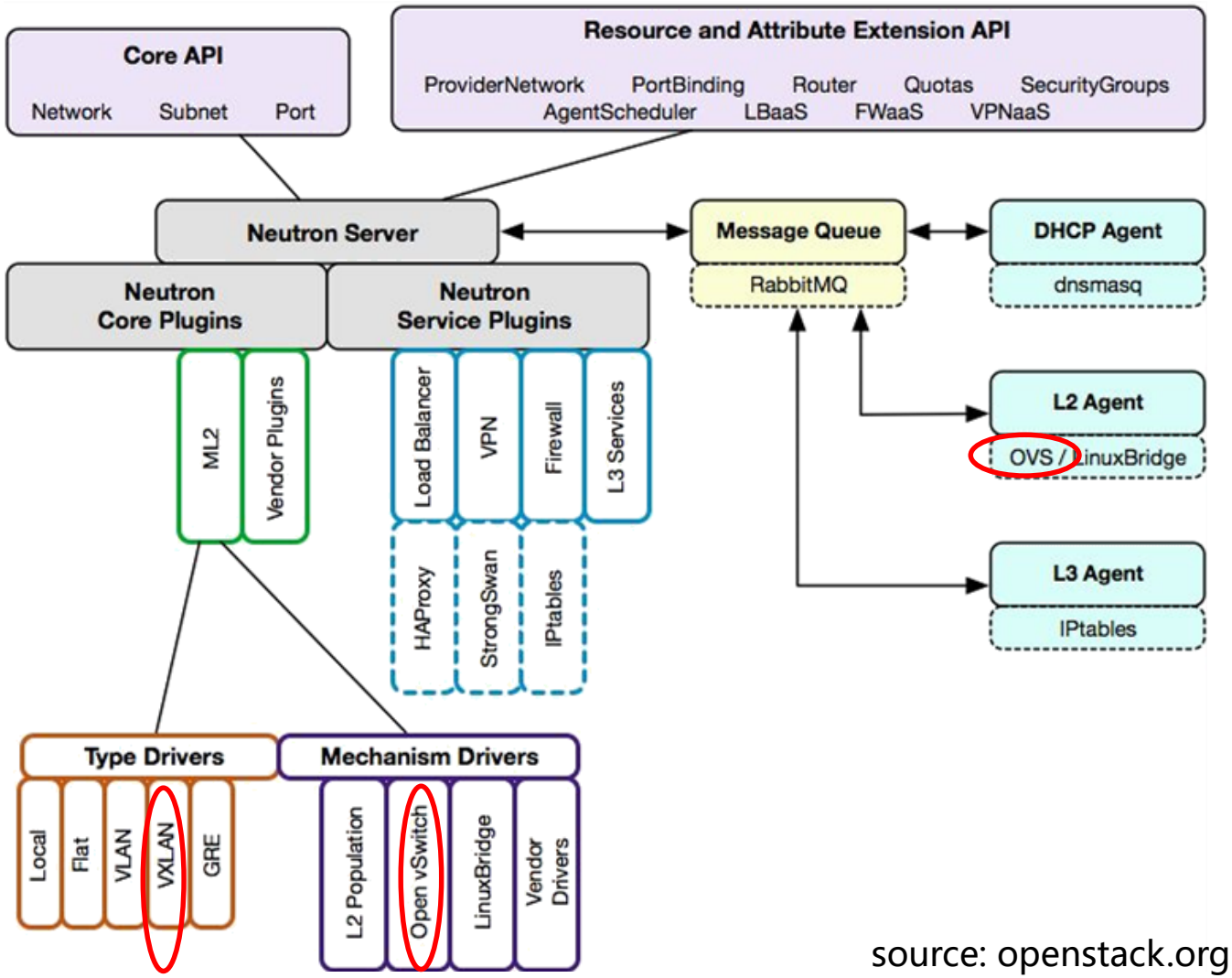
# Open vSwitch + VXLAN网络




- Provider network Aggregate
- Overlay network 10.0.1.0/24
- Provider network 2 VLAN 1 (untagged)
- Provider network 2 VNI 101

source: openstack.org

# Open vSwitch + VXLAN实现



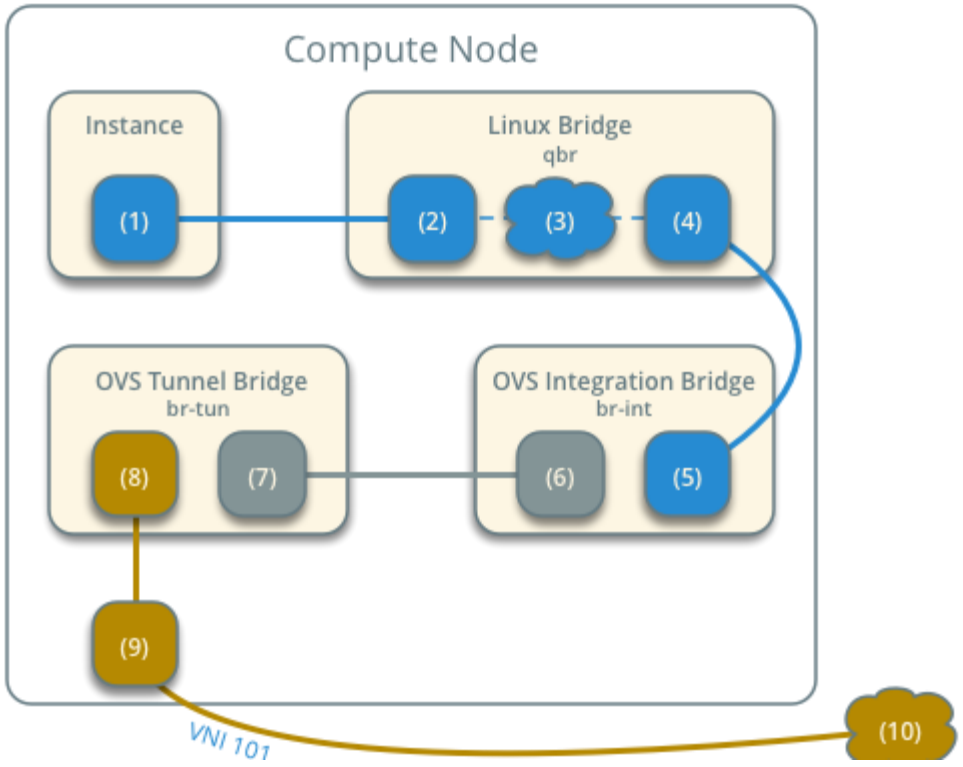

source: openstack.org

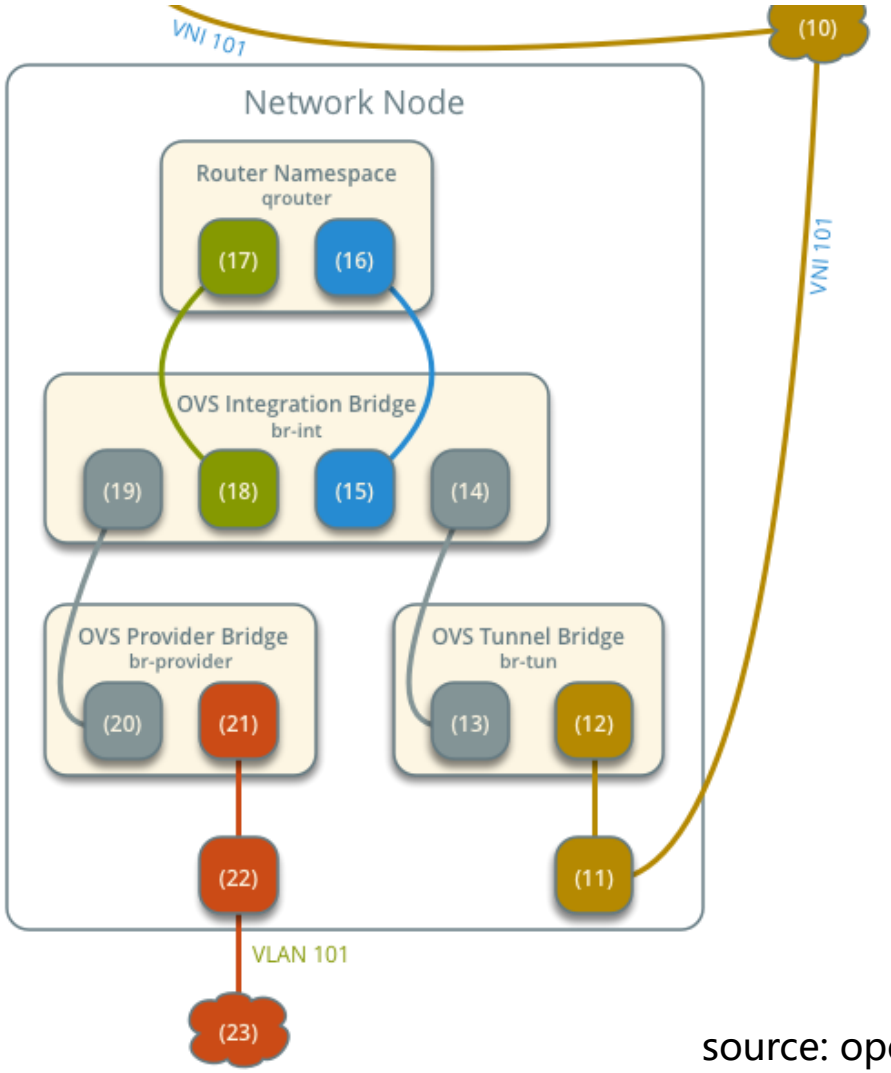
- 使用Open vSwitch + VXLAN网络时：
  - ML2的Type Driver为VXLAN
  - ML2的Mechanism Driver为Open vSwitch
  - L2 Agent为Open vSwitch

# Open vSwitch + VXLAN场景说明

- 使用Open vSwitch + VXLAN实现Self-service network，网络流量可以分为如下几种：
  - 南北向流量：虚拟机和外部网络（例如Internet）通信的流量
  - 东西向流量：虚拟机之间的流量
  - Provider Network和外部网络之间的流量：由物理网络设备负责交换和路由。
- 后续的网络流量分析基于如下示例：
  - Provider network 1 (VLAN)：VLAN 101 (tagged)
  - Self-service network 1 (VXLAN)：VXLAN 101 (VNI)
  - Self-service network 2 (VXLAN)：VXLAN 102 (VNI)
  - Self-service router：网关在Provider network 1上，连接Self-service network 1 和Self-service network 2

# 使用Fixed IP的虚拟机南北流量

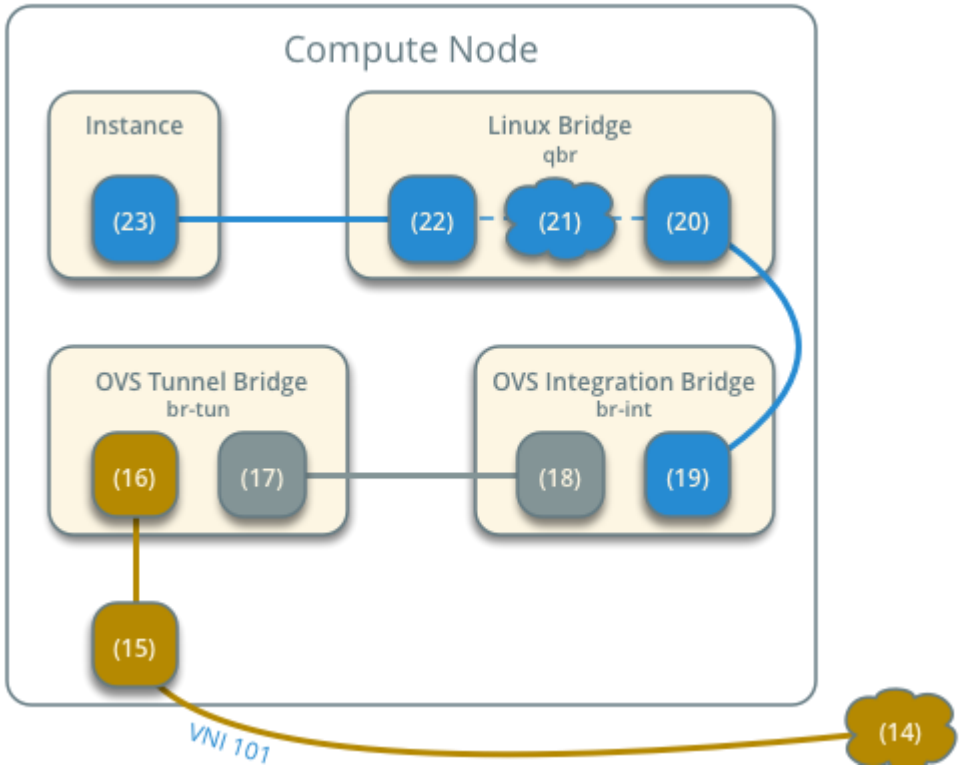


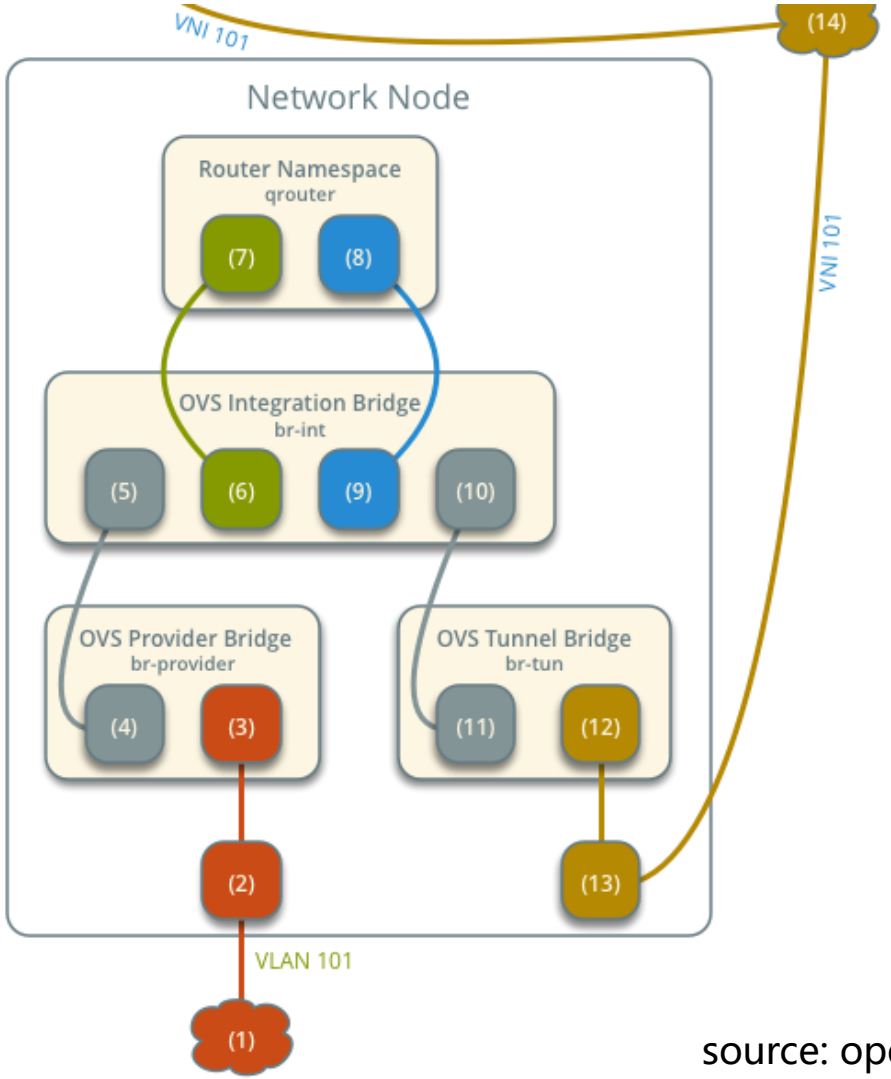




- Provider network Aggregate
- Provider network 1 VLAN 101, 203.0.113.0/24
- Overlay network 10.0.1.0/24
- Self-service network 1 VNI 101, 192.168.1.0/24

source: openstack.org

# 从外部访问带Floating IP的虚拟机

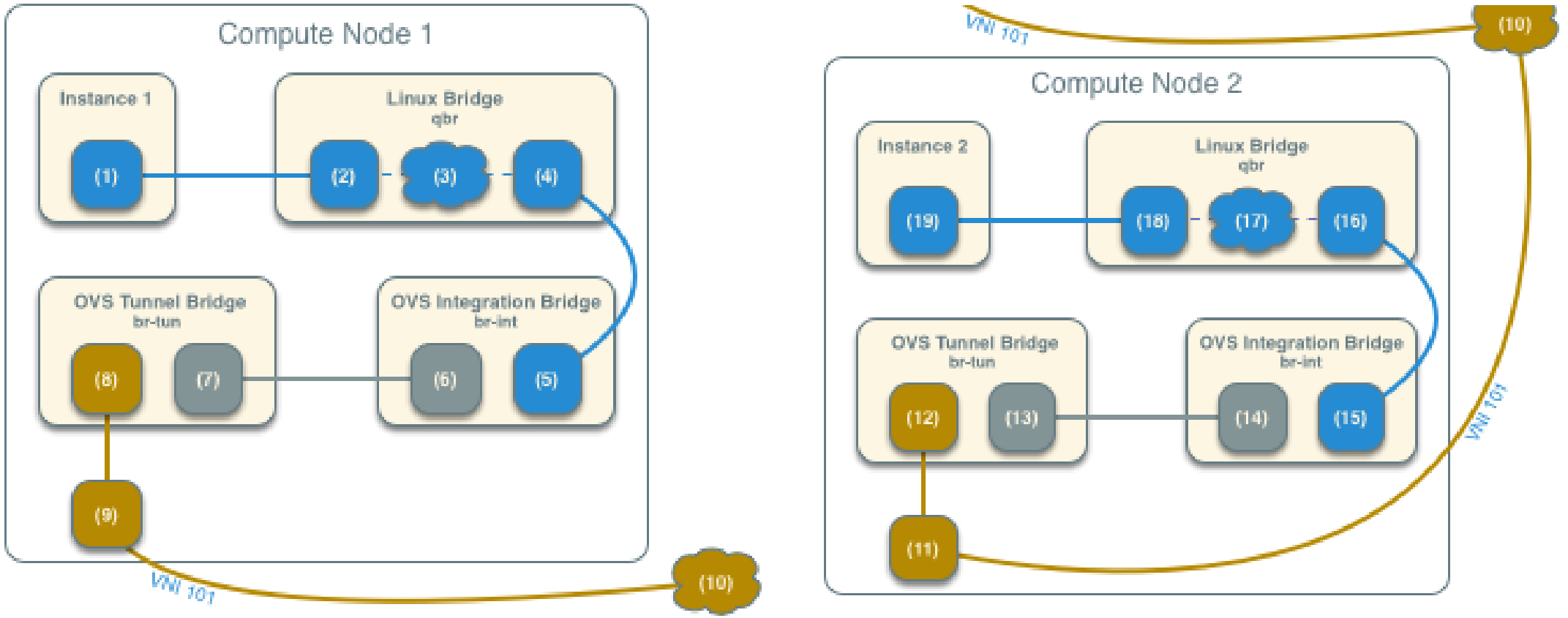



- Provider network Aggregate
- Provider network 1 VLAN 101, 203.0.113.0/24
- Overlay network 10.0.1.0/24
- Self-service network 1 VNI 101, 192.168.1.0/24

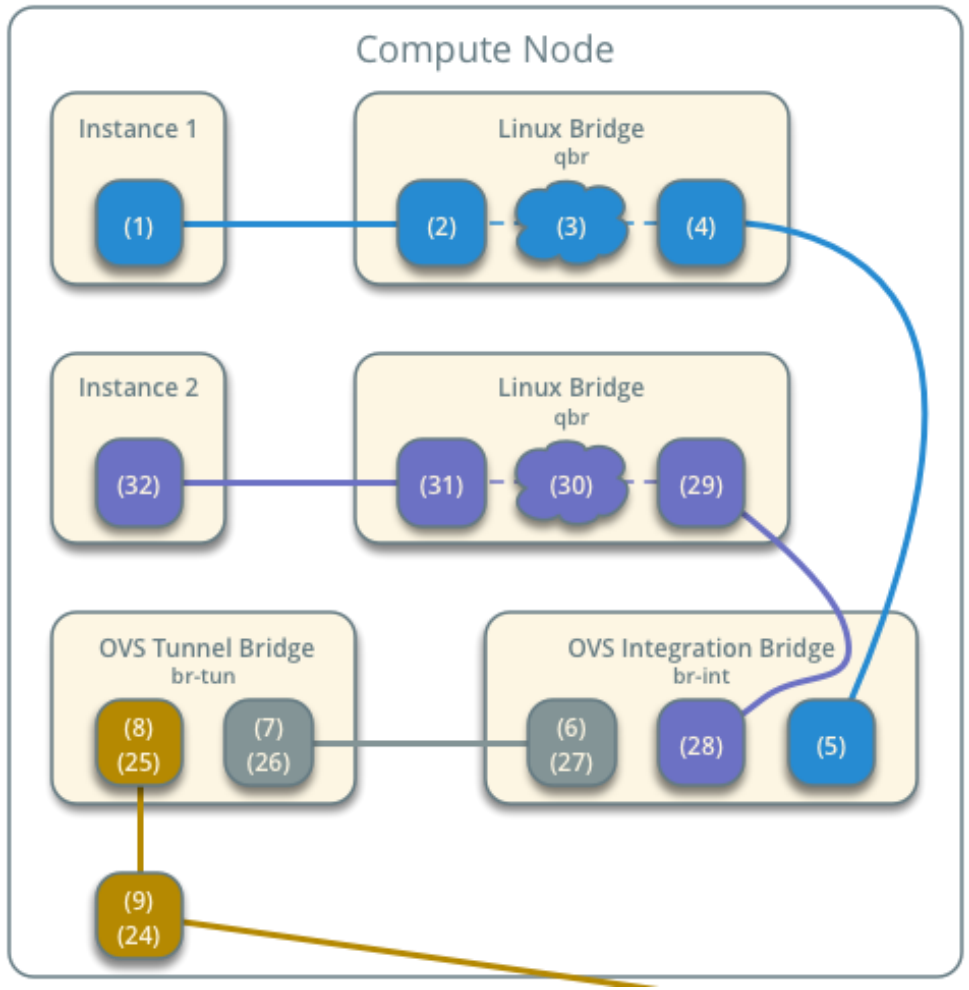
source: openstack.org

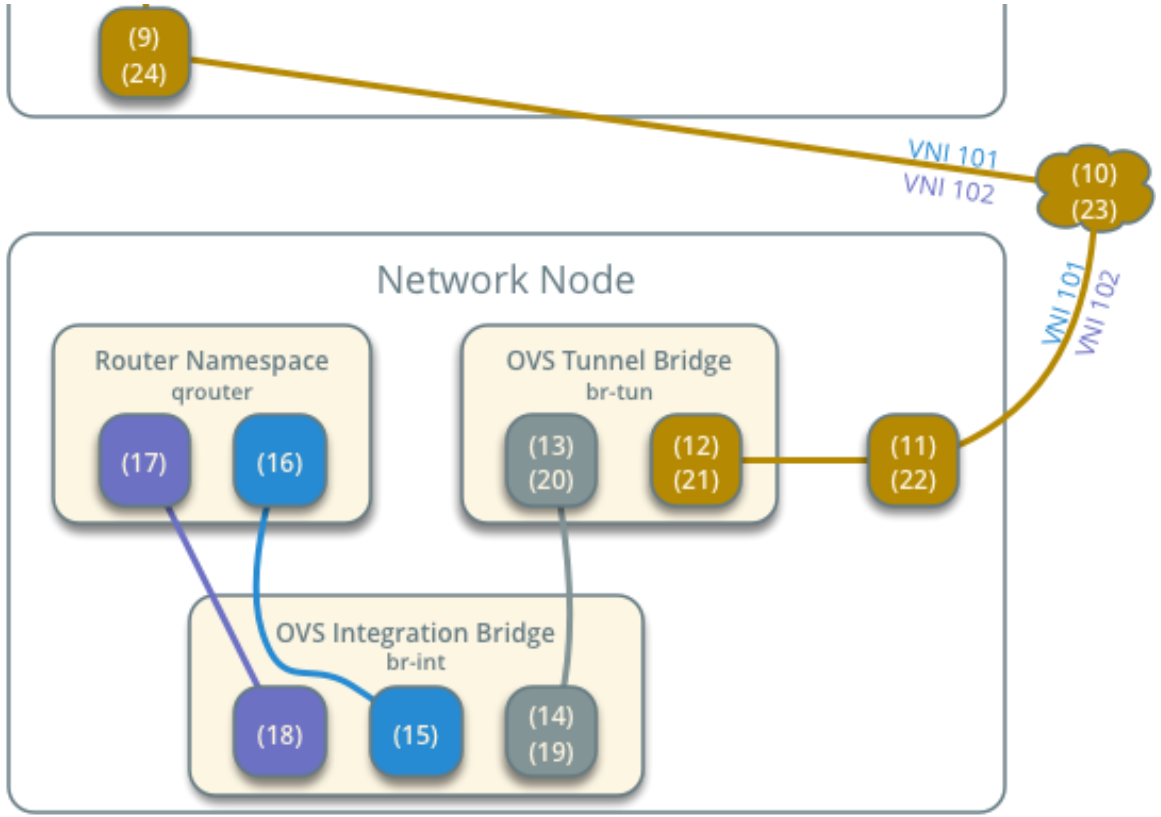
# 同一个网络中虚拟机东西流量




source: openstack.org

# 不同网络中虚拟机东西流量




Overlay network
10.0.1.0/24

Self-service network 1
VNI 101, 192.168.1.0/24

Self-service network 2
VNI 102, 192.168.2.0/24

source: openstack.org

# 思考题

1. Linux有哪些网络虚拟化技术?
2. Neutron有哪些组件，各组件的作用是什么?

# 本章总结

- Linux网络虚拟化基础
- OpenStack网络服务Neutron简介
- Neutron概念
- Neutron架构与组件分析
- OpenStack动手实验： Neutron操作
- Neutron网络流量分析

# 学习推荐

- OpenStack社区
  - https://www.openstack.org/


谢 谢
www.huawei.com