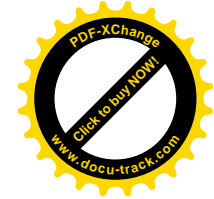


openstack™
CLOUD SOFTWARE

OpenStack从入门到精通实践 第七周

DATAGURU专业数据分析社区

Openstack从入门到精通实践 讲师 chong-de.fang



法律声明



【声明】 本视频和幻灯片为炼数成金网络课程的教学资料，所有资料只能在课程内使用，不得在课程以外范围散布，违者将可能被追究法律和经济责任。

课程详情访问炼数成金培训网站

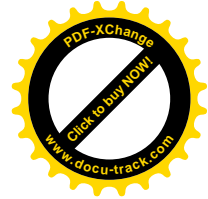
<http://edu.dataguru.cn>



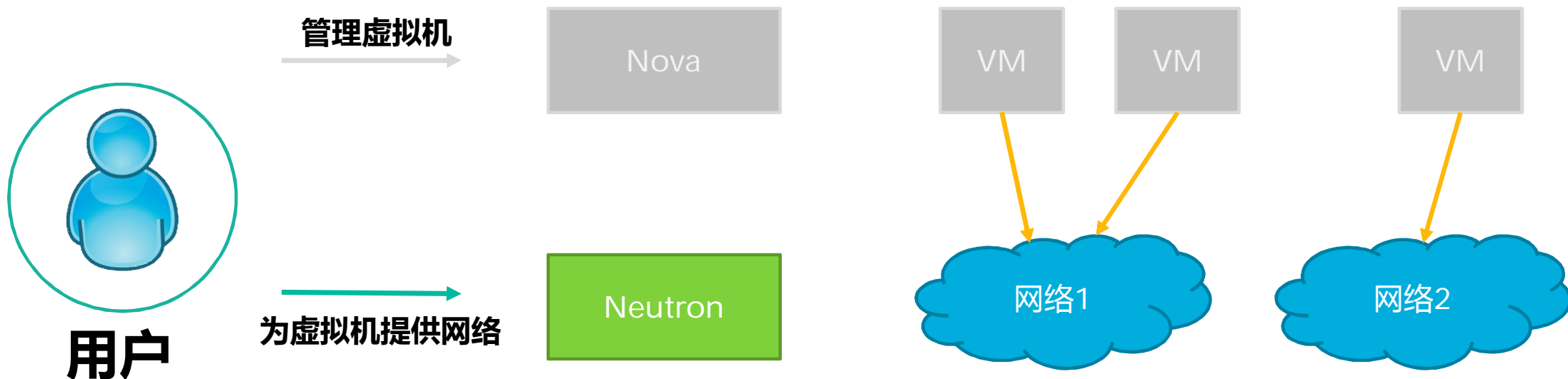
炼数成金逆向收费式网络课程

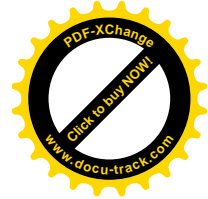


- Dataguru (炼数成金) 是专业数据分析网站 , 提供教育 , 媒体 , 内容 , 社区 , 出版 , 数据分析业务等服务。我们的课程采用新兴的互联网教育形式 , 独创地发展了逆向收费式网络培训课程模式。既继承传统教育重学习氛围 , 重竞争压力的特点 , 同时又发挥互联网的威力打破时空限制 , 把天南地北志同道合的朋友组织在一起交流学习 , 使到原先孤立的学习个体组合成有组织的探索力量。并且把原先动辄成千上万的学习成本 , 直线下降至百元范围 , 造福大众。我们的目标是 : 低成本传播高价值知识 , 构架中国第一的网上知识流转阵地。
- 关于逆向收费式网络的详情 , 请看我们的培训网站 <http://edu.dataguru.cn>



Neutron介绍





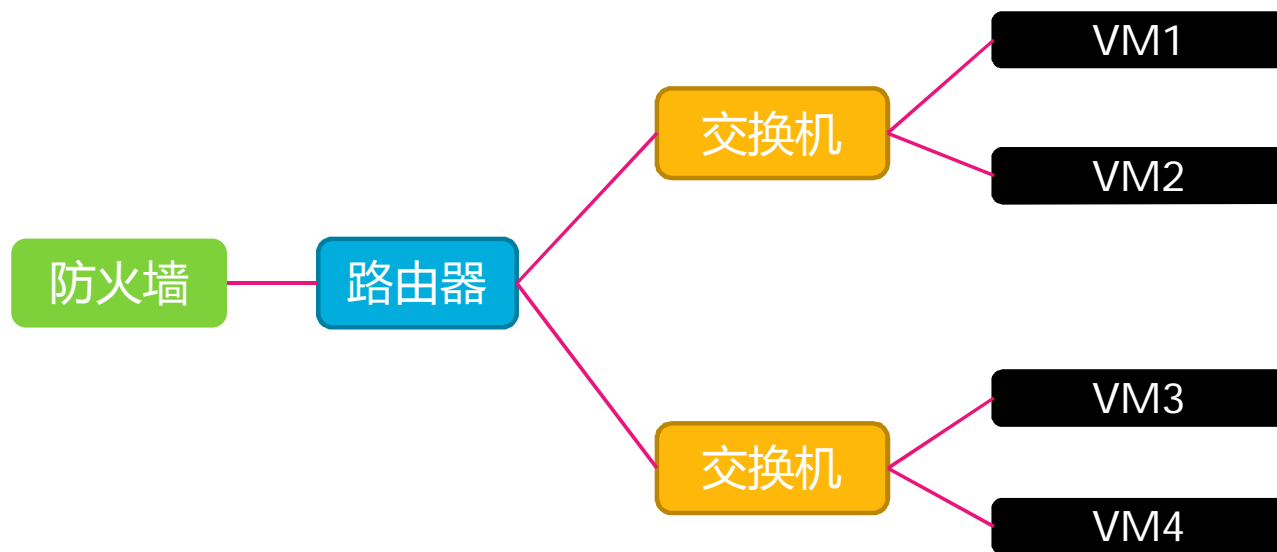
Neutron介绍



网络组件虚拟化



网络互联

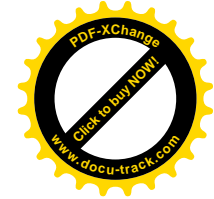




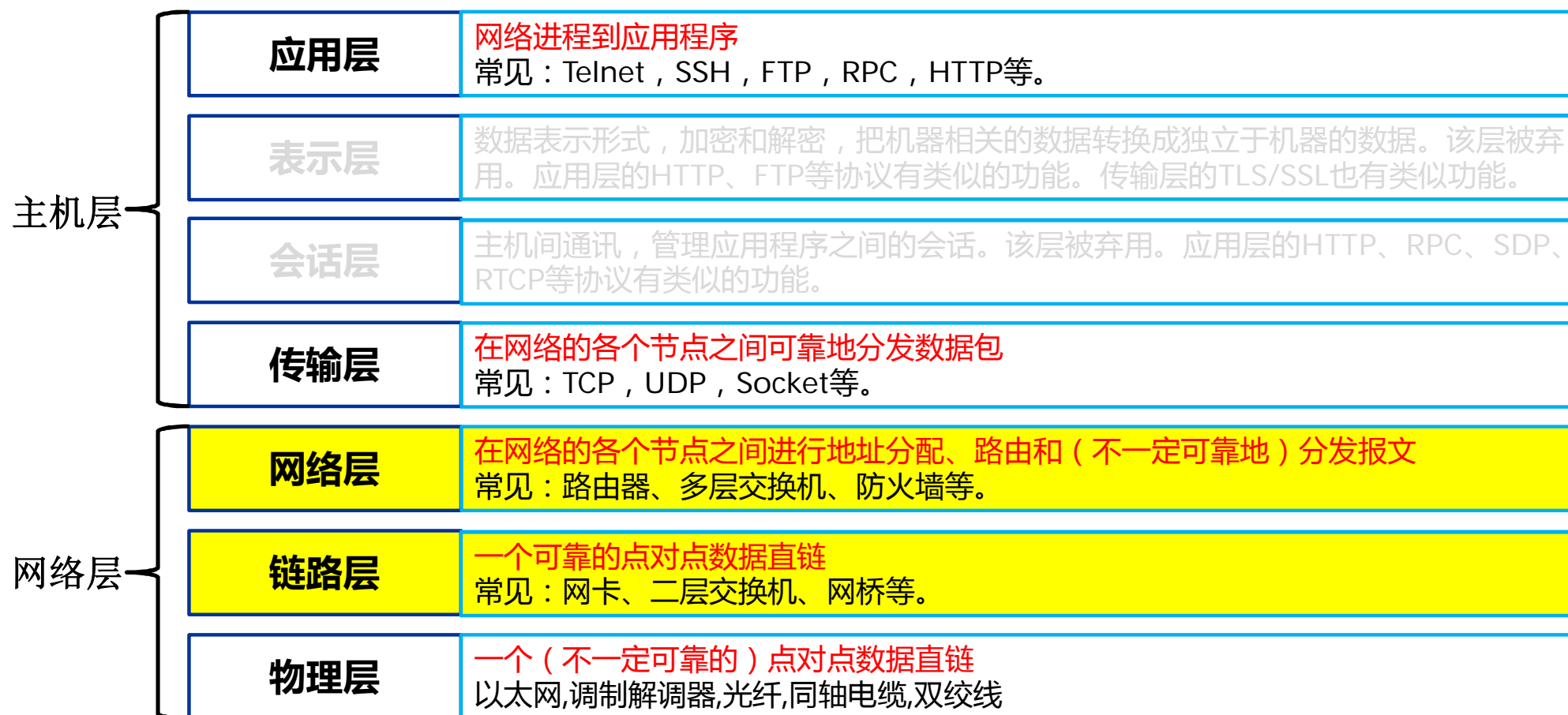
虚拟化网络组件的实现方式



- 网卡：OpenvSwitch
- 防火墙：iptables
- 交换机：OpenvSwitch, Linux Bridge
- 路由器：Linux ip协议栈和iptables
- 负载均衡器：haproxy



OSI七层模型





网络命名空间(netns)

- 多个逻辑上隔离的网络环境运行在同一个物理主机上
- 每个网络空间都有自己的网卡设备、路由表、防火墙规则
- veth pair:虚拟网络设备，成对出现。用于在两个网络命名空间进行通信

- 常用命令

#列表所有 netns

ip netns list

#在 network namespace 中运行命令

ip netns exec <network namespace name> <command>

#Example using the namespace from above:

ip netns exec nstest ip addr

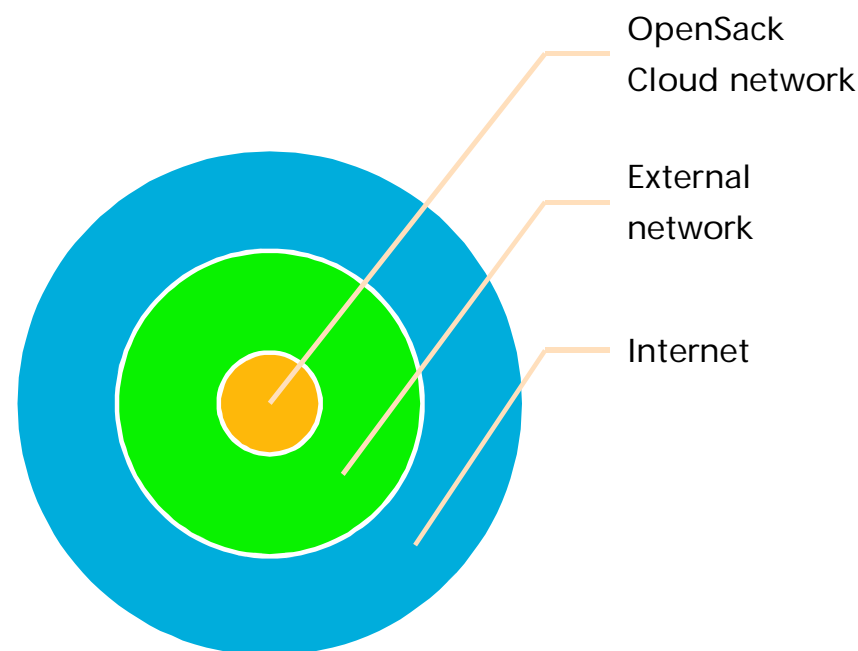


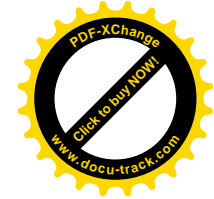
网络分类（一）



■ 按照数据中心来分类：

- OpenStack Cloud network：OpenStack 所管理的网络。
- External network：数据中心所管理的公司网（Intranet），虚拟机使用的 Floating IP 是这个网络的地址的一部分。
- Internet：由各大电信运营商所管理的公共网络，使用公共IP。



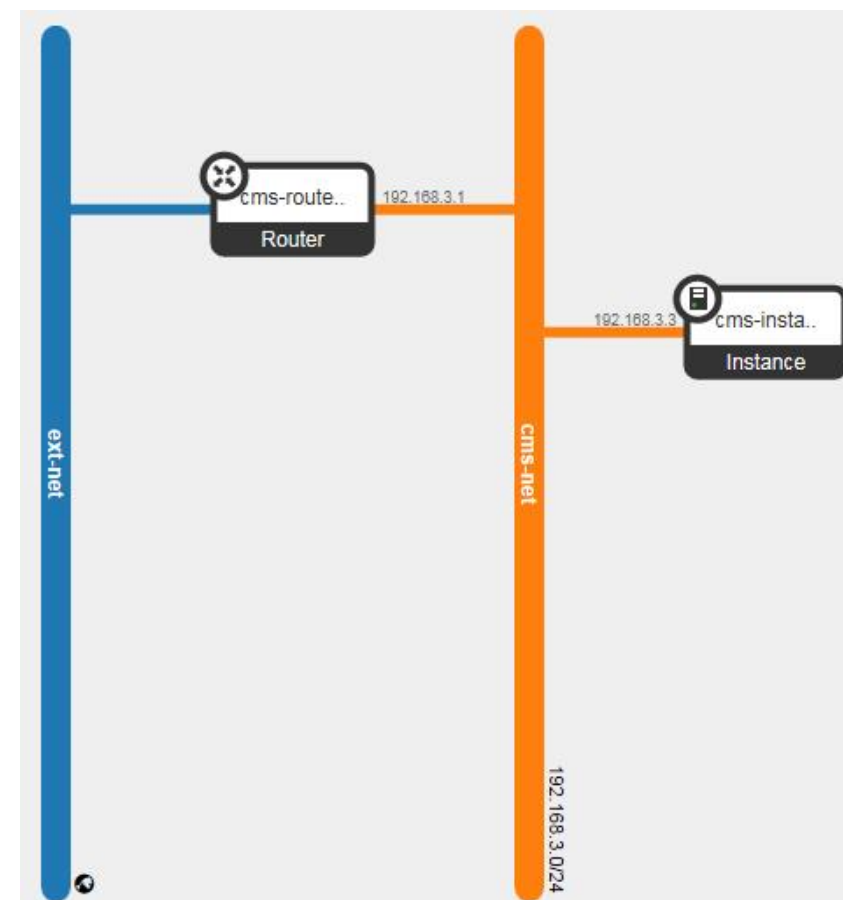


网络分类（二）



■ 按照创建网络的用户权限来分类

- 提供者网络（Provider network）：管理员创建的和物理网络有直接映射关系的虚拟网络。可以选择的网络类型包括（Flat,Vlan,GRE,Vxlan）。
- 租户网络（Project network）：普通租户用户创建的虚拟网络。可以选择的网络类型包括（Local, Flat,Vlan,GRE,Vxlan）。





虚拟网络类型定义(一)



■ Local

- 只允许在本服务器内通信的虚拟网络，不能够跨服务器的通信。主要用于单节点上测试。

■ Flat

- 所有租户都在一个网络里面，没有进行网络隔离。容易产生广播风暴
- 一般只用于提供者网络
- `neutron net-create NAME --provider:network_type flat --provider:physical_network PHYS_NET_NAME`

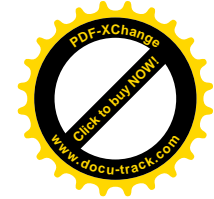


虚拟网络类型定义(二)



■ Vlan

- 基于**物理 Vlan** 网络实现的虚拟网络。共享同一个物理网络的多个 Vlan 网络是相互隔离的，甚至可以使用重叠的 IP 地址空间。每个支持 Vlan network 的物理网络可以被视为一个分离的 Vlan trunk，它使用一组独占的 Vlan ID。有效的 Vlan ID 范围是 1 到 4094。
- 一般只用于提供者网络。
- `neutron net-create NAME --provider:network_type vlan --provider:physical_network PHYS_NET_NAME --provider:segmentation_id VID`



虚拟网络类型定义(三)



■ GRE

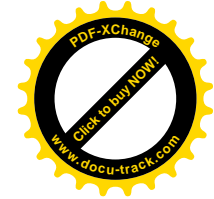
- (Generic Routing Encapsulation) 通用路由协议封装协议，是一种 IP-over-IP 的隧道
- GRE 是 L3 层的隧道技术，本质是在隧道的两端的 L4 层建立 UDP 连接传输重新包装的 L3 层包头，在目的地再取出包装后的包头进行解析。
- GRE 封装的数据包基于 IP 路由表来进行路由，因此 GRE network 不和具体的物理网络绑定。
- 一般只适用于租户网络。



对象模型（一）



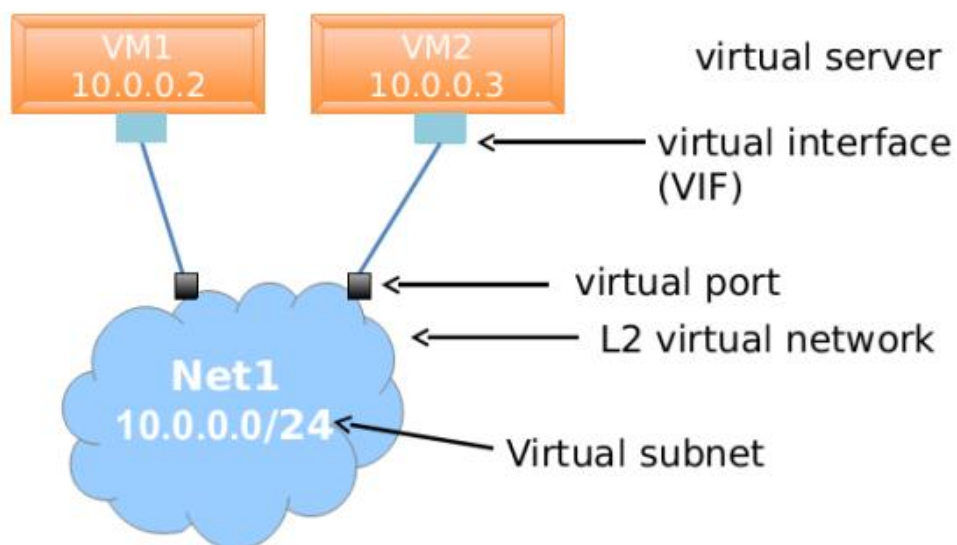
- 网络 (network)
 - 是一个隔离的二层网段，类似于物理网络世界中的 LAN (VLAN)
- 子网 (subnet)
 - 子网是一组 IPv4 或 IPv6 地址以及与其有关联的配置。它是一个地址池，OpenStack 可从中向虚拟机 (VM) 分配 IP 地址。每个子网指定为一个无类别域间路由 (Classless Inter-Domain Routing) 范围，必须与一个网络相关联。
- 端口 (Port)
 - 一个 Port 代表虚拟网络交换机 (logical network switch) 上的一个虚机交换端口 (virtual switch port)。虚机的网卡 (VIF - Virtual Interface) 会被连接到 port 上。当虚机的 VIF 连接到 Port 后，这个 vNIC 就会拥有 MAC 地址和 IP 地址。Port 的 IP 地址是从 subnet 中分配的。



对象模型（二）



- 虚拟机交换机（Virtual switch）
 - Neutron 默认采用开源的 Open vSwitch 作为其虚拟机交换机，同时还支持使用 Linux bridge。
- 虚拟路由器（Virtual router）
 - 一个 Virtual router 提供不同网段之间的 IP 包路由功能，由 Neutron L3 agent 负责管理。

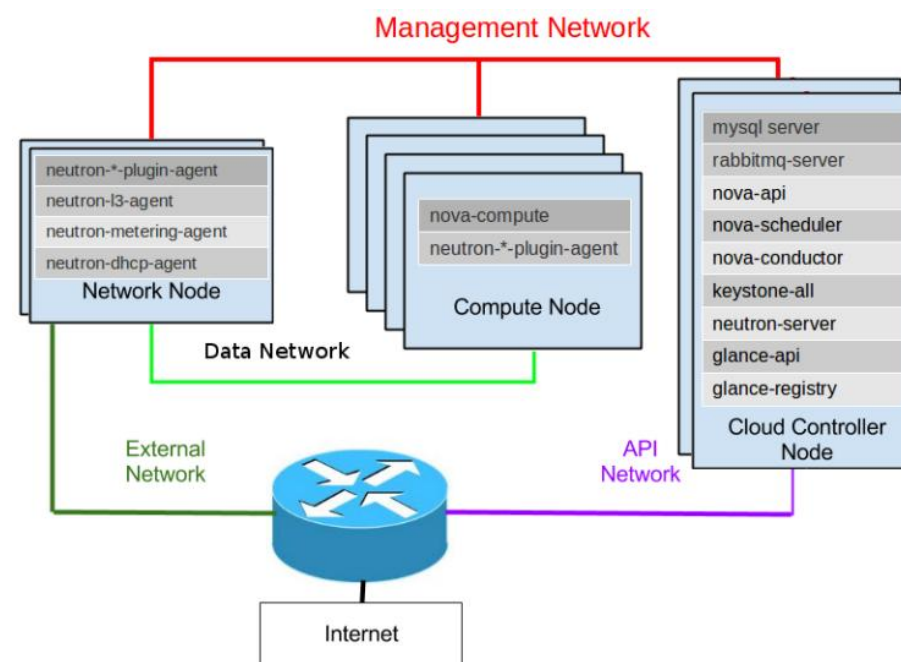




网络类型



- **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

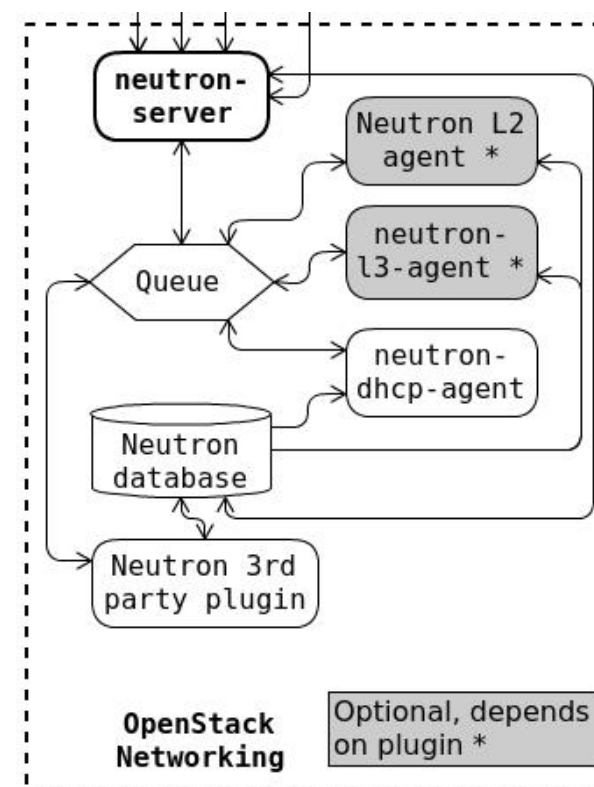




Neutron架构

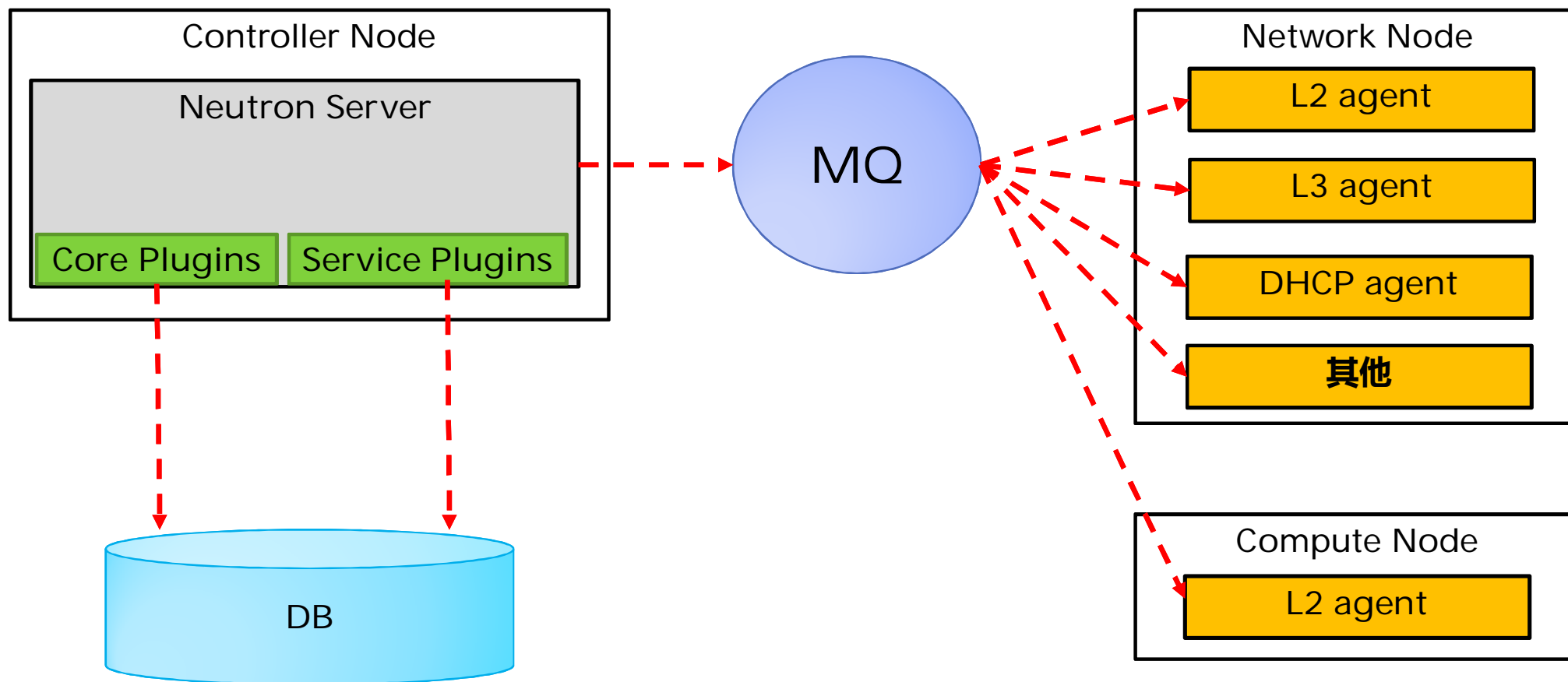


- neutron Server
 - 包含守护进程neutron-server和各种插件(plugin)，它们既可以安装在控制节点也可以安装在网络节点。neutron-server提供API接口，并把对API的调用请求传给已经配置好的插件进行后续处理。
- neutron L2 agent
 - 为虚拟网络提供2层交换服务。通过一个特定的插件来实现（neutron-*-agent）。例如neutron-openvswitch-agent。
- neutron-dhcp-agent
 - 为虚拟机提供DHCP服务。
- neutron-l3-agent
 - 为虚拟机访问外部网络提供3层转发服务。



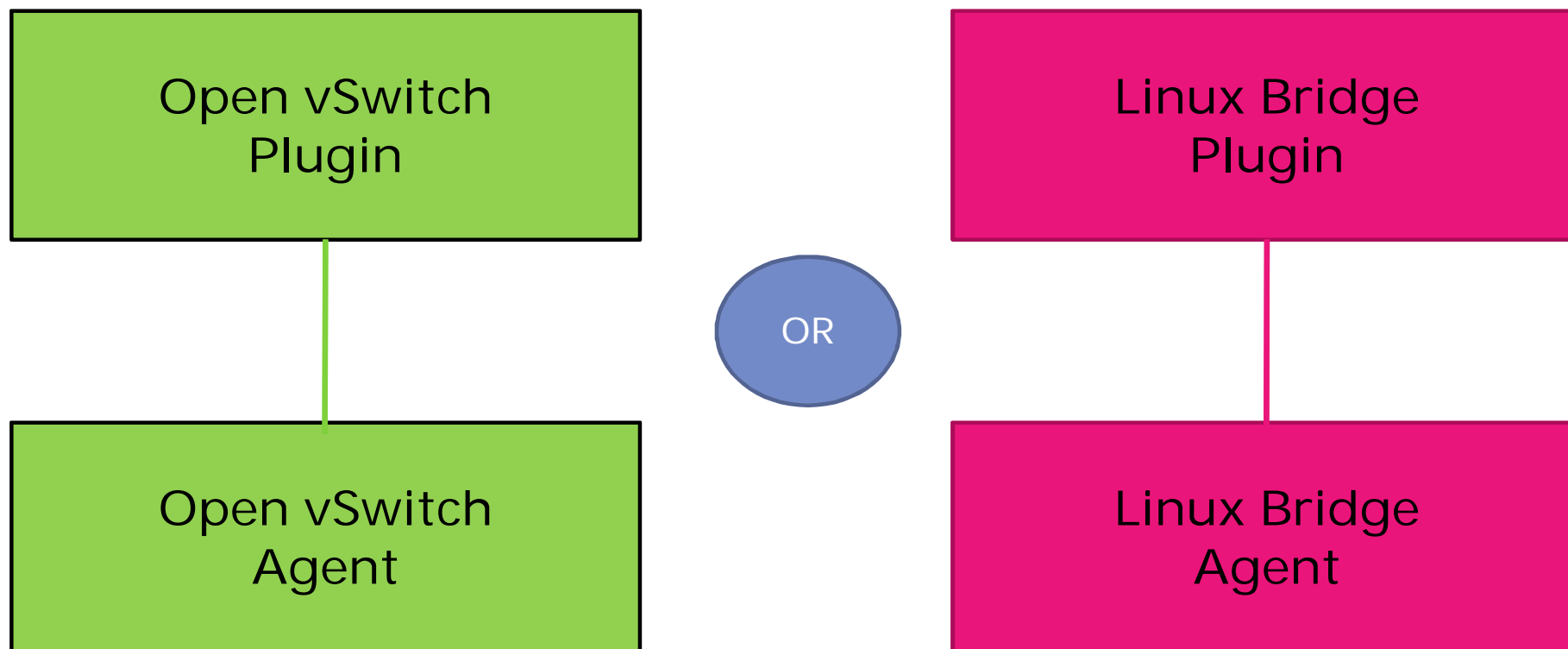


Plugin/Agent架构

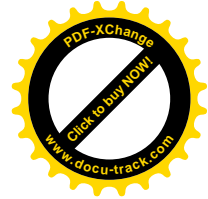




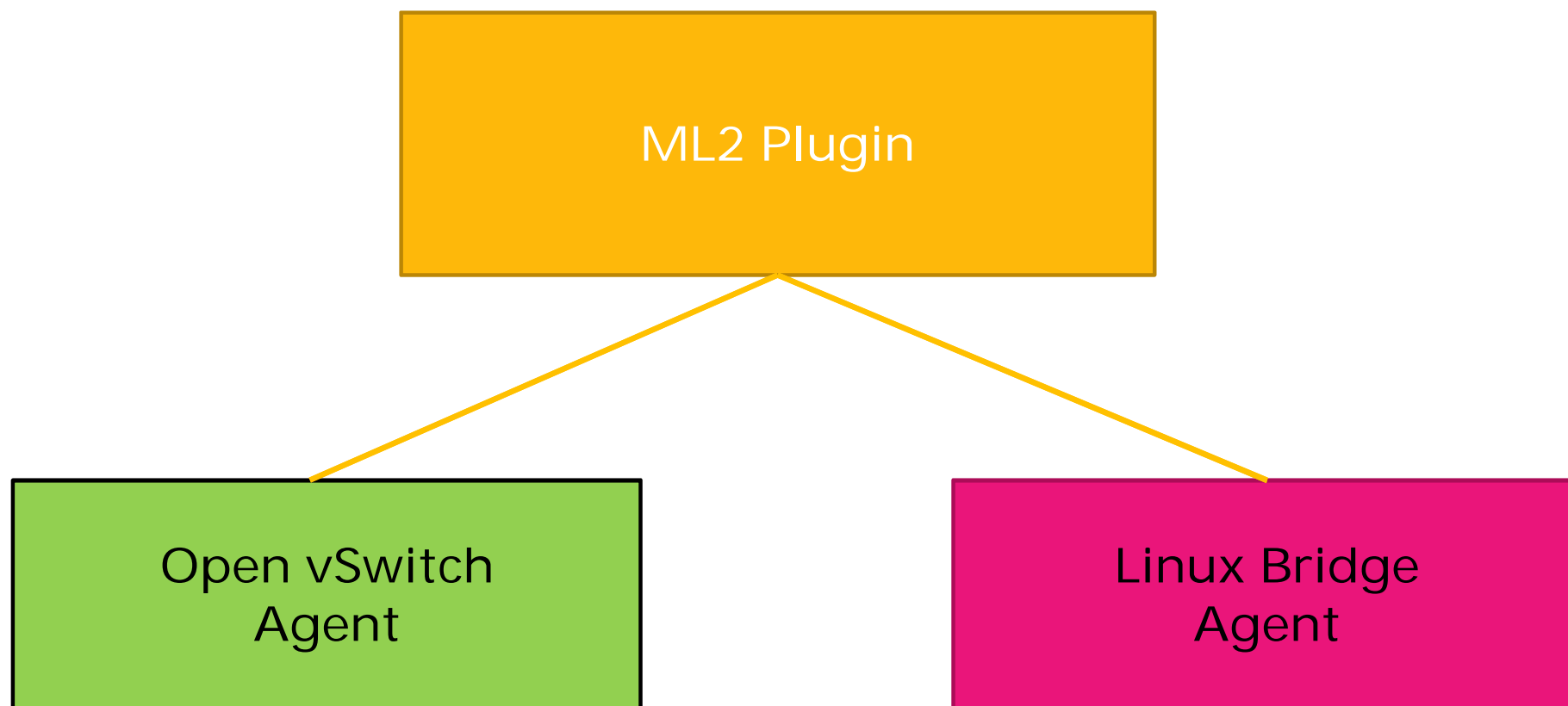
ML2 Plugin架构介绍（一）

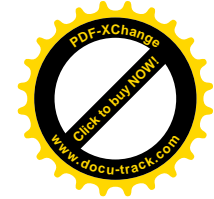


没有**ML2 Plugin**之前.....

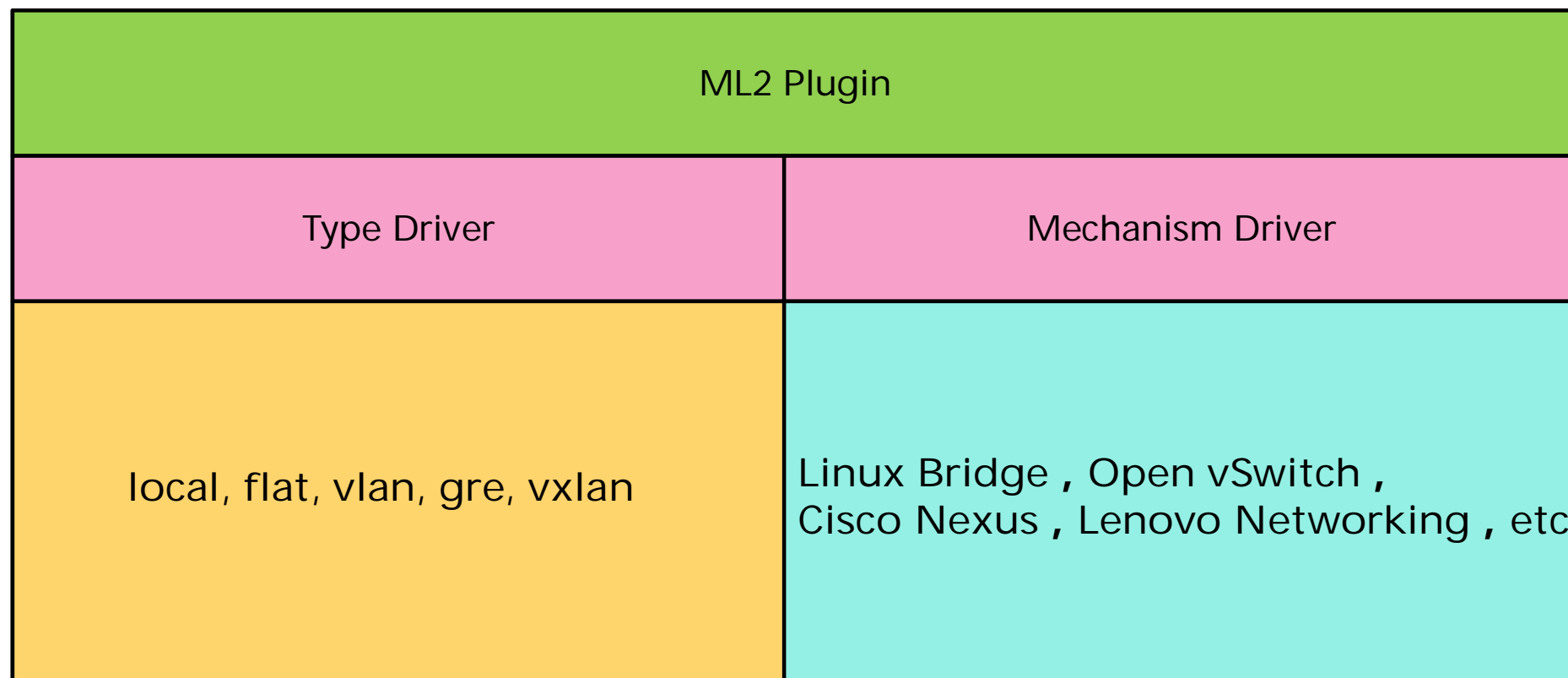


ML2 Plugin架构介绍（二）





ML2 Plugin架构介绍（三）





DHCP agent (一)



■ DHCP agent

- 为虚拟机提供DHCP服务
- 每个网络的DHCP 运行在一个network namespace中，namespace 由 qdhcp-<DHCP-UUID>命名

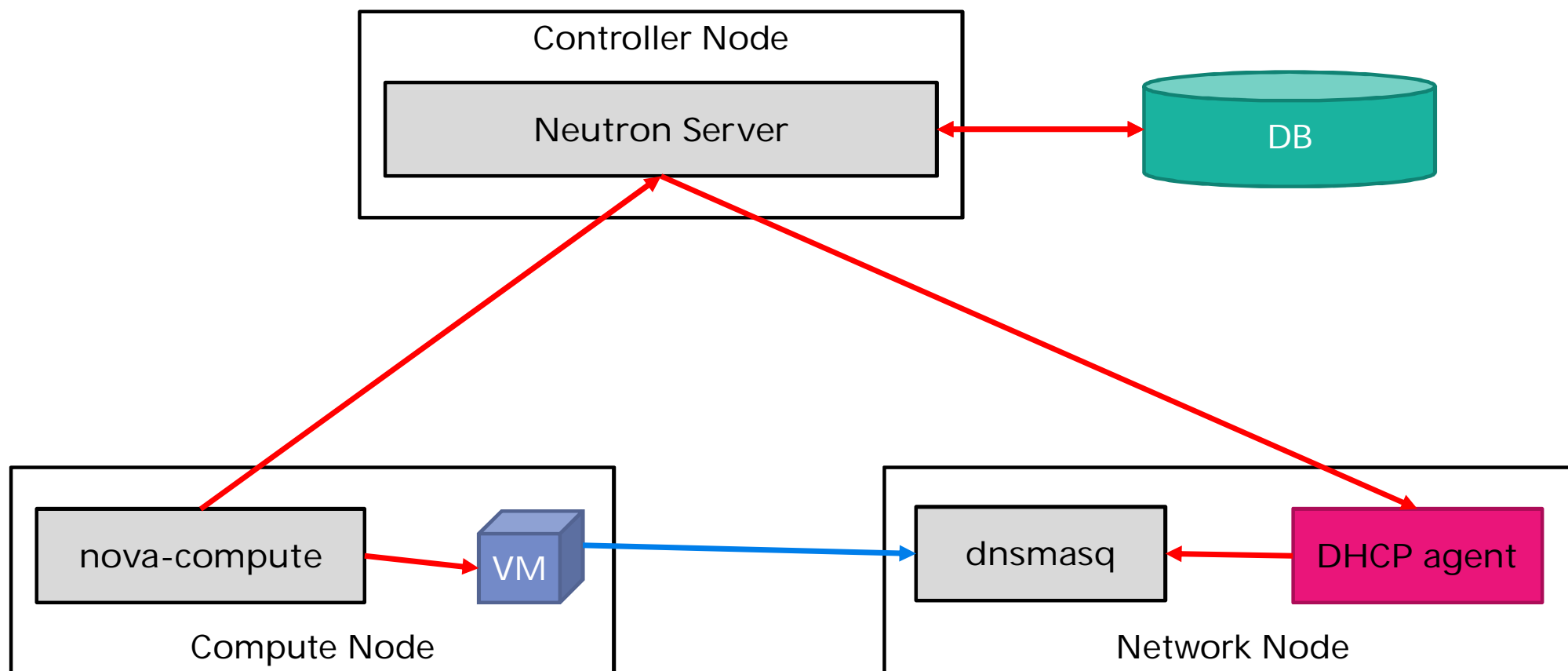
■ dnsmasq

- dnsmasq 是被 Neutron 用来提供 DHCP 和 DNS 服务的一个开源软件。

```
nobody    2841      1  0 2月13 ?      00:00:00 dnsmasq --no-hosts --no-resolv --strict-order --bind-interfaces --interface=tapaff036f6-af --exc  
ept-interface=lo --pid-file=/var/lib/neutron/dhcp/db8e8126-3c71-4ee8-a34a-6655dcf1a2f3/pid --dhcp-hostsfile=/var/lib/neutron/dhcp/db8e8126-3c71-  
-4ee8-a34a-6655dcf1a2f3/host --addn-hosts=/var/lib/neutron/dhcp/db8e8126-3c71-4ee8-a34a-6655dcf1a2f3/addn_hosts --dhcp-optsfile=/var/lib/neutro  
n/dhcp/db8e8126-3c71-4ee8-a34a-6655dcf1a2f3/opts --dhcp-leasefile=/var/lib/neutron/dhcp/db8e8126-3c71-4ee8-a34a-6655dcf1a2f3/leases --dhcp-rang  
e=set:tag0,192.168.2.0,static,86400s --dhcp-lease-max=256 --conf-file= --domain=openstacklocal  
nobody    2842      1  0 2月13 ?      00:00:00 dnsmasq --no-hosts --no-resolv --strict-order --bind-interfaces --interface=tap966ce59f-4e --exc  
ept-interface=lo --pid-file=/var/lib/neutron/dhcp/3412c7f3-4f37-4c10-a0d7-bd9df08ad82f/pid --dhcp-hostsfile=/var/lib/neutron/dhcp/3412c7f3-4f37-  
-4c10-a0d7-bd9df08ad82f/host --addn-hosts=/var/lib/neutron/dhcp/3412c7f3-4f37-4c10-a0d7-bd9df08ad82f/addn_hosts --dhcp-optsfile=/var/lib/neutro  
n/dhcp/3412c7f3-4f37-4c10-a0d7-bd9df08ad82f/opts --dhcp-leasefile=/var/lib/neutron/dhcp/3412c7f3-4f37-4c10-a0d7-bd9df08ad82f/leases --dhcp-rang  
e=set:tag0,192.168.3.0,static,86400s --dhcp-lease-max=256 --conf-file= --domain=openstacklocal
```



DHCP agent (二)





L3 agent



■ L3 agent

- L3 Agent 负责路由、浮动 IP 分配、地址转换和安全组管理。
- 通过iptables实现安全组、路由以及地址转换。
- 每个虚拟路由运行在一个 network namespace 中，每个 namespace 由 qrouter-<router-UUID>命名

```
[root@network-node-01 ~]# ip netns exec qrouter-7083fe8a-25d9-4e19-b1df-e0e53a878200 ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: qr-1cbb9276-b0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether fa:16:3e:30:61:9e brd ff:ff:ff:ff:ff:ff
    inet 192.168.3.1/24 brd 192.168.3.255 scope global qr-1cbb9276-b0
        valid_lft forever preferred_lft forever
    inet6 fe80::f816:3eff:fe30:619e/64 scope link
        valid_lft forever preferred_lft forever
3: qg-611b3781-0a: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether fa:16:3e:17:45:4c brd ff:ff:ff:ff:ff:ff
    inet 192.168.57.103/24 brd 192.168.57.255 scope global qg-611b3781-0a
        valid_lft forever preferred_lft forever
    inet 192.168.57.104/32 brd 192.168.57.104 scope global qg-611b3781-0a
        valid_lft forever preferred_lft forever
    inet6 fe80::f816:3eff:fe17:454c/64 scope link
        valid_lft forever preferred_lft forever
```




Thanks

FAQ时间