ZStack 技术白皮书精选

更适合私有云的网络部署模式-动态路由

扫一扫二维码，获取更多技术干货吧

更适合私有云的网络部署模式-动态路由

作者：邵悠锋

0 前言

当前云计算的建设已经如火如荼，云计算带来的好处也显而易见，各行各业都在积极上云。对于 IaaS 这层来说，主要由计算、存储、网络组成。如果说计算像人体的灵魂，那存储就是大脑，保存了认知的所有信息；网络是血管，连通了身体每一个部分。计算是最核心的，存储是最重要的，而网络是最复杂的。

在 ZStack 云网络中，网络的部署模式可以分为扁平网络和 VPC 网络，而在 VPC 网络中，又可以通过 EIP 或者 OSPF 动态路由两种模式来让外部网络访问 VPC 内部虚拟机，本文来分析一下这几种模式的特点和适用场景。

1. OSPF 简介

在看各种网络模型的适用场景之前，咱们先来了解下动态路由和 OSPF 的相关概念

路由是指在路由器上指导数据包流量转发的路径信息，让路由器知道该从哪个接口将数据包发出去。路由器就好比交叉路口，而路由就好比路牌，数据包就好比轿车，路牌告诉司机，到某某路该从哪个路口走，这个和路由器转发数据包非常相像。那么问题又来了，路牌是政府建造的，路由是怎么生成的呢？

路由可以分为 3 类：

直连路由：路由器接口所属网段的信息，自动生成

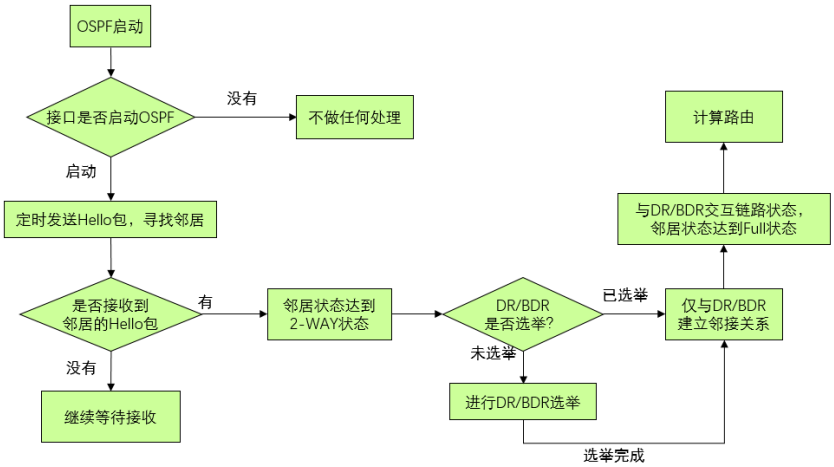
静态路由：管理员手工配置的路由信息，适用于小规模环境

动态路由：通过动态路由邻居相互之间交互而生成的路由信息，适用于大规模复杂环境

静态路由因为所有的路由条目都是手工配置，那么在规模越来越大的情况下，配置的复杂度会成倍上升，并且无法自适应网络拓扑的更改。一旦某台路由器宕机，会使得和这台路由器相关的所有网段都无法通信，如果要更改拓扑，修改配置也会变得非常麻烦；而动态路由的出现很好地解决了静态路由的问题，只需要进行协议初始配置即可，路由条目都是动态

生成，也能够自适应拓扑的改变，自动改变数据的转发路径。

OSPF 就属于动态路由中应用最广泛的一种。OSPF 是一种基于链路状态的路由协议，使用最短路径优先算法来计算出路由。OSPF 的工作过程如下所示：

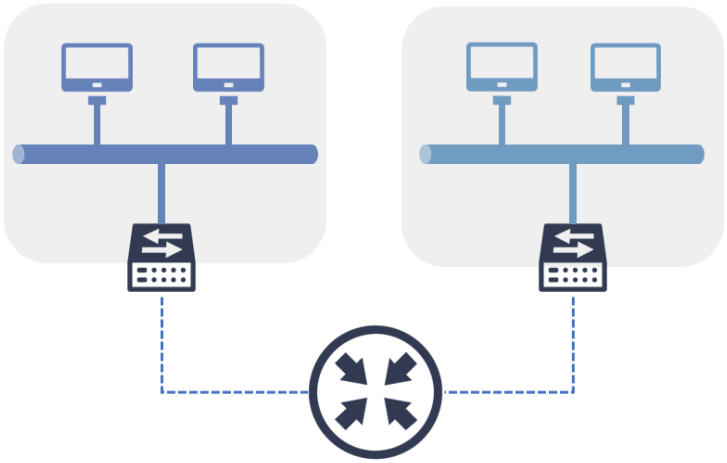


在 OSPF 启动以后，会周期性的发送 Hello 包，当收到邻居发来的 Hello 包以后，状态变更为 2-way；然后，在整个网段上所有的 OSPF 路由器开始进行 DR/BDR 的选举，也就是网段的管理者/备份管理者；后续所有的路由器都和 DR/BDR 建立邻接关系，将本地连接的所有网段信息传递给 DR/BDR，再由 DR 将计算出的整个网络的拓扑信息发送给所有路由器；最后，所有路由器以自己为根，根据算法计算出到各网段的最优路径并写入路由表。

2. 扁平网络

2.1 拓扑架构

扁平网络的架构如下所示：



扁平网络其实就是个纯二层网络，云平台只提供二层转发的功能，通过 DHCP 给虚拟机自动分配 IP。云平台会创建一个虚拟网桥，分别连接虚拟机和物理网卡，虚拟机数据包通过物理网卡转发到物理交换机上，由物理交换机提供网关以及三层转发。

2.2 适用场景

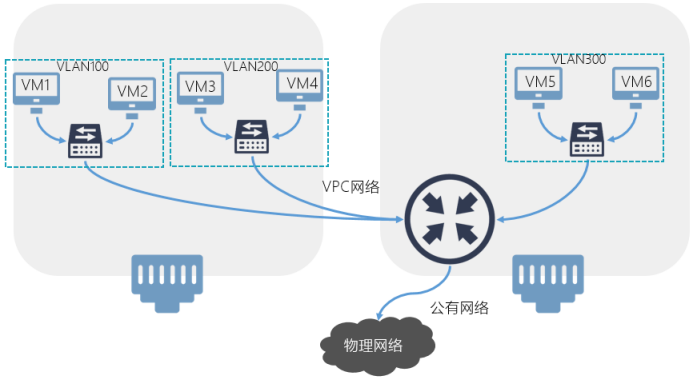
来看下扁平网络的特点：

扁平网络最大的特色就是简单，配置完二三层网络即可，数据流量也非常简单，物理网卡只是做桥接；但是相应的，扁平网络支持的网络服务就非常少，比如负载均衡、IPSec、端口转发等功能，扁平网络都是不支持的，而这些在企业网络中使用比较普遍。因此，扁平网络适用于对网络要求简单，只需要互通性的场景。

3. VPC 网络-EIP 模式

3.1 拓扑架构

VPC 网络 EIP 模式的架构如下所示：



在 VPC 网络中，云平台提供 vrouter 功能，vrouter 一端是公有网络，用于和物理网络相连接，这边的公有网络只是一个概念，表示公共的网络，并不是一定需要用真正的公网 IP；另一端连接租户的 VPC 网络，作为 VPC 网络的网关，并可以提供 EIP、LB、端口转发等网络服务，提供多租户隔离，支持 VXLAN，可以进行更好的网络扩展。

不同的租户之间的 IP 段是可以重复的，VPC 网络访问外部的时候，在 VPC 路由器的公网接口会进行 SNAT，转换为公网 IP；而外部访问 VPC 网络的时候，通过访问虚拟机绑定的 EIP，在 VPC 路由器的公网接口会进行 DNAT，转换为虚拟机的真实 IP，这样就可以进行内外互通。

3.2 适用场景

来看下 EIP 模式的特点：

VPC 网络提供的网络服务非常丰富，如 EIP、IPSec、端口转发、分布式路由、负载均衡等，可以应对各种网络的需求，不同租户之间相互隔离，IP 段都是自定义，而且不需要担心冲突的问题。EIP 模式和公有云网络是一致的，每个租户都在 VPC 内部自定义 IP 段，对外访问通过 SNAT，外部访问虚拟机则通过 EIP。

EIP 模式适用于公有云、托管云以及一些特殊场景，比如不允许暴露真实 IP、公司被收购 IT 系统需要合并，当然，私有云场景也是适合的。

4 VPC 网络-OSPF 模式

在上节咱们看到了 EIP 的特点，事实上大多数的私有云网络都是 EIP 模式，但是咱们来

仔细分析一下，EIP 模式的虚拟机和外部通信，其实是要经过 SNAT 和 DNAT 的，这样就涉及到 IP 地址的转换，会引起如下的几个问题：

1、性能损耗：IP 的转换是需要依靠 NAT 规则一条条来匹配的，一旦规模变得比较大，规则数量就会上升，NAT 的效率就低了，这样转发性能就会有影响

2、IP 管理不方便：私有云内部一般都是私网 IP，使用 EIP 模式，公有网络和 VPC 网络都是私网 IP，在大多数的场景下，其实根本没必要进行转换，直接将真实 IP 暴露给云外部即可，网工还需要来维护 NAT 的对应关系，增加了维护的工作量，同时也使得架构更加复杂

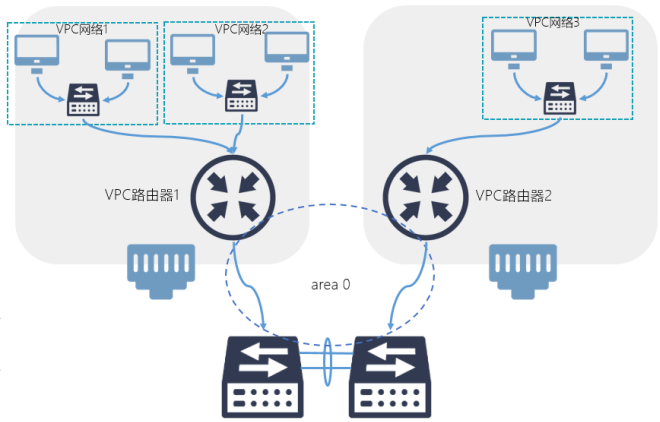
3、EIP 配置复杂：如果给每个虚拟机都分配一个 EIP，那每个虚拟机都需要额外配置 EIP，当虚拟机数量庞大的时候，配置会耗费很长时间；如果部分虚拟机不用 EIP 而使用端口转发的话，端口转发的配置和管理也比较复杂。

那么，是否有一种方法可以解决以上的问题呢？

ZStack 的解决方案是在 VPC 路由器上运行 OSPF 协议，和物理交换机对接，并关闭 SNAT。

4.1 OSPF 拓扑架构

OSPF 方案的总体架构如下所示：



OSPF 是 VPC 路由器的一个功能模块，可以和物理交换机的 OSPF 进行无缝对接，使用时需要先关闭 SNAT 的功能，将 VPC 网络的 IP 宣告给邻居。通过 OSPF，物理网络可以学习到 VPC 网络的真实 IP 并直接访问，不需要再做 DNAT 转换，相对于传统 VPC 网络来说架构更简单，更容易和物理网络进行联动。使用 OSPF，VPC 路由器就是物理网络在虚拟环境中

的一个延伸，100%还原物理路由器的 NFV 方案，并且 VPC 路由器依然可以支持负载均衡、IPSec、端口转发等功能。

4.2 适用场景

OSPF 模式本质上是把物理交换机的部分功能以 NFV 的形式来实现，和传统物理网络相比较，除了接入层是由物理设备变更为虚拟设备，其他都没有变化，整体架构和传统网络是一样的，因此，可以适用于绝大部分的私有云环境，并且没有 NAT 的性能损耗，网络架构更加简单，和 EIP 模式相比较，OSPF 模式更适合私有云场景。

可能有人会问多租户场景怎么办？IP 无法重复的话是否会不够用？多租户隔离怎么办？其实这个完全没必要担心，10.0.0.0/8 这个段就是专门给私有网络分配的，足足 1000 多万个 IP，完全满足 99%以上的私有云环境，而且企业内部的 IP 都是网工统一分配管理的，如果让使用者自定义网络，反而会将整体架构变复杂，增加网络运维的工作量；多租户隔离其实并不是靠 NAT 来做的，多租户隔离一是路由没有发布，二是依靠虚拟防火墙来做访问控制，而 NAT 的作用是允许内部 IP 重复。

公有云能否不用 EIP 呢？这个其实是不行的，因为公有云是所有不同公司/个人的用户共享一个平台，IP 的规划必然会有重复，所以需要用 NAT 来做防 IP 冲突，用 EIP 来提供外部访问。而私有云只是一个公司内部的环境，IP 规划必然不能有冲突，所以绝大部分的私有云场景不需要 NAT 和 EIP，使用动态路由是更适合的方式。

5 总结

综上所述，扁平网络、VPC 网络 EIP 模式、OSPF 模式都有各自的适用场景，对于网络需求简单、只需要连通性的场景，适合使用扁平网络；对于绝大部分的私有云场景，更适合使用 OSPF 模式，对接物理交换机，将物理网络延伸到虚拟环境；对于公有云、托管云以及一些特殊场景，适合使用 EIP 模式。