ZStack 技术白皮书精选

私有云网络应用模型

扫一扫二维码，获取更多技术干货吧

版权声明

摘要

大道至简·极速部署，ZStack 致力于产品化私有云和混合云。

ZStack 是新一代创新开源的云计算 IaaS 软件，由英特尔、微软、CloudStack 等世界上最早一批虚拟化工程师创建，拥有 KVM、Xen、Hyper-V 等成熟的技术背景。

ZStack 创新提出了云计算 4S 理念，即 Simple（简单）、Strong（健壮）、Smart（智能）、Scalable（弹性），通过全异步架构，无状态服务架构，无锁架构等核心技术，完美解决云计算执行效率低，系统不稳定，不能支撑高并发等问题，实现 HA 和轻量化管理。

ZStack 发起并维护着国内最大的自主开源 IaaS 社区——zstack.io，吸引了 6000 多名社区用户，对外公开的 API 超过 1000 个。基于这 1000 多个 API，用户可以自由组装出自己的私有云、混合云，甚至利用 ZStack 搭建公有云对外提供服务。

ZStack 拥有充足的知识产权储备，积极申报多项软著和专利，参与业内标准、白皮书的撰写，入选云计算行业方案目录，还通过了工信部云服务能力认证和信通院可信云认证。

ZStack 面向企业用户提供基于 IaaS 的私有云和混合云，是业内唯一一家实现产品化，并领先业内首家推出同时打通数据面和控制面无缝混合云的云服务商。选择 ZStack，用户可以官网直接下载、1 台 PC 也可上云、30 分钟完成从裸机的安装部署。

目前已有 1000 多家企业用户选择了 ZStack 云平台。

主题：私有云网络应用模型

云计算基础架构即服务（IaaS）主要管理了数据中心的计算、存储和网络等核心资源，通过对资源的集成、池化和抽象对外按需提供即时的云主机、云磁盘、网络服务及其他系统管理功能（例如账户、监控、运维、计费等）。由于对资源进行了高度抽象和细粒度管理，云计算平台能够提供比传统独立服务器更高效和更可靠的数据服务，让资源始终以最高效率提供最稳定的服务。

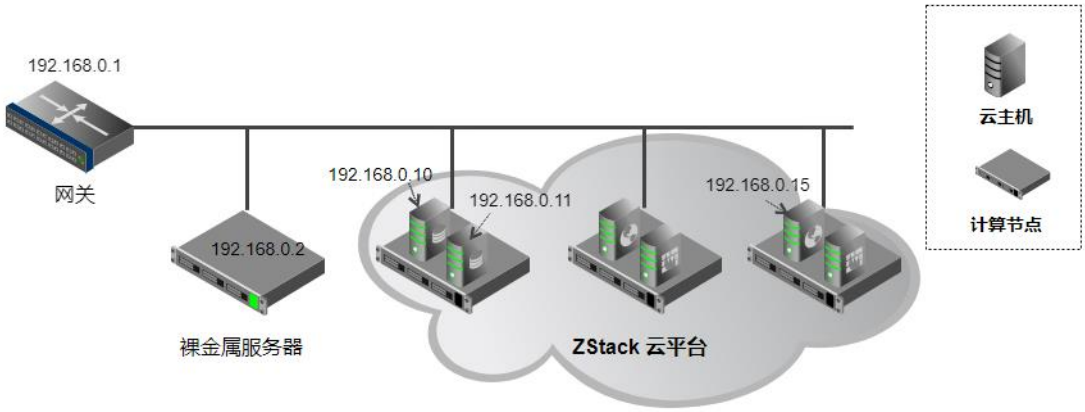
公有云部署在公有云服务提供商的数据中心，以租用售卖的模式提供云主机给最终客户使用。公有云主要以提供弹性 IP（EIP）网络模型。不同客户购买的云主机都默认使用内网 IP 地址，并通过网关访问互联网。因为采用隔离技术，内网 IP 地址可以重复。为了让内网 IP 地址的云主机能被互联网访问（例如搭建的网站），就需要额外购买 EIP。EIP 可以和用户的任意云主机一对一绑定，访问 EIP 就相当于访问绑定的云主机。从用户的角度来看，用户使用 EIP 登录的云主机，看到的还是一个内网 IP 地址，因为 EIP 会配置在“网关”处，用户不能直接看到他的配置。用户也可以创建没有 EIP 的云主机，仅使用内网 IP 地址和该用户的其他云主机进行高速的互联。早期公有云提供的经典网络模型（与扁平网络类似）在多租户隔离方面并不完善，后期陆续推出了虚拟私有云（VPC）网络模型可以做到二层网络隔离。除此之外，公有云可以提供专线、VPN 或者智能加密网关等能力与用户私有网络连通。

私有云部署在用户自有数据中心，仅对用户自身或用户的租户提供云计算的服务。在私有化的数据中心中的网络模型以二层扁平网络为主，也包括隔离网络、弹性 IP 网络，甚至

是复杂的动态路由网络。私有云网络仅依靠通用 x86 服务器和通用网络交换机，便可以构造出复杂的网络场景满足客户的差异化需求。私有云主要是通过 NFV（网络功能虚拟化）和 SDN（软件定义网络）的方式来提供各种复杂的网络服务能力，提供的网络服务包括：二层网络隔离；三层网络 IP 分配、路由、转发、VPN、安全组（分布式防火墙）；四层以上的负载均衡；审计监控等。

为了方便理解和使用，我们将会介绍一些 ZStack 私有云环境中常用的网络模型。

二层扁平网络（经典网络）

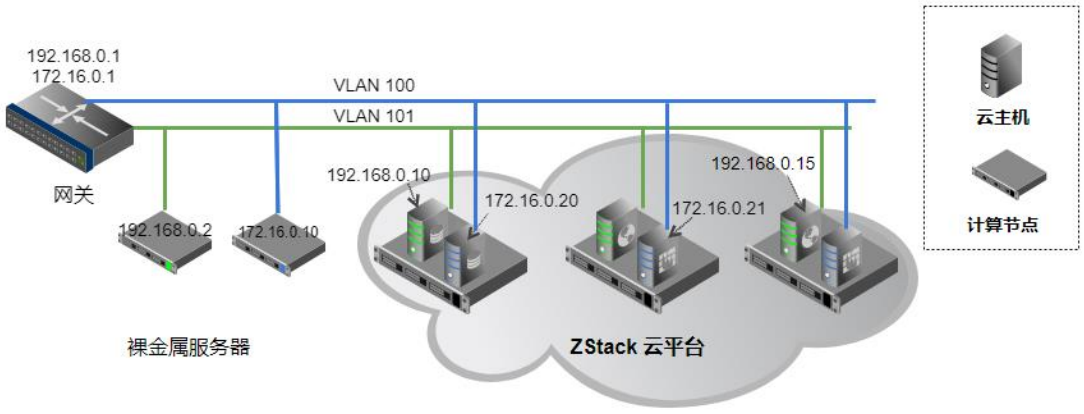


图一：二层扁平网络

通常的二层扁平网络是指在一个私有云数据中心中，所有的物理机和云主机都在一个二层网络之上，他们的 IP 地址也在相同的三层网络段。物理机和云主机之间相互访问是不需要通过网关进行路由的。例如图一所示，所有的计算单元都是分配的 192.168.0.1/24 这个网络段中的一个 IP 地址。当资源需要访问互联网的时候，会通过网关路由器 192.168.0.1 对外通讯。

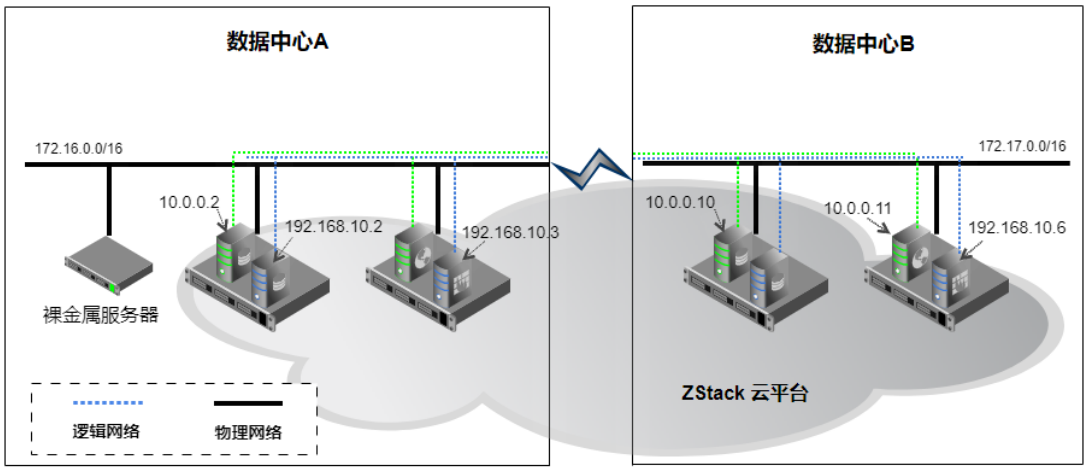
二层扁平网络是常见而典型的企业网络拓扑架构，企业内部的电脑可以直接相互访问，网络拓扑和架构都非常简单。由于资源都在一个二层网络之上，网络访问控制通常通过私有云的安全组（也称分布式防火墙）来保证。在私有云配置中，三层网络的网关地址需要设定为公司内网的网关地址。另外分配给云主机的 IP 地址段不能和物理机相关的 IP 地址段冲突，需要人为的划分隔离。

企业网络环境相对复杂的场景，可能会根据地域或者部门划分多个二层扁平网络，扁平网络之间通过路由互通，不同的二层网络可以采用 VLAN 进行分割。在用 VLAN 分割的二层网络中，服务器通常只能属于特定的 VLAN 网络。云平台在这种场景里就可以体现很强的资源共享优势，一个云平台可以连接不同的 VLAN 网络。云平台上分配资源的最小单位是虚拟的云主机，于是可以根据用户的需求，自由的在云平台上创建和回收属于不同 VLAN 网络的云主机，甚至在一台计算节点上可以创建同时连通多个 VLAN 网络的云主机，从而达到资源的快速调配。



图二：多个二层扁平网络

大二层网络



图三：大二层网络

有企业的数据中心可能会分布在不同的地区，中间通过互联网或者专线联通。例如图三所示，不同地域的数据中心内部是不同的 IP 地址空间，通过配置三层路由可以让数据中心 A 和 B 之间网络互通。如果要跨越数据中心之间构建类似于本地的大二层网络环境，需要借助 VxLAN，GRE 这样的网络互联技术。

以 VxLAN 举例，它利用数据中心原有网络作为底层通讯网络，从而可以构造超过 1600 万个独立的逻辑二层网络。每一个逻辑二层网络就像真实的二层网络一样，数据包可以在无感知的情况下跨数据中心进行传递，不同的逻辑二层网络之间相互隔离。以 VxLAN 作为云平台的业务网络（公有网络、私有网络），有几个明显的好处:

二层隔离网络数量大大增多。传统 VLAN 网络最多只有 4096 个，而具有 2 的 24 次方个 VxLAN 的空间远超现有企业的内部需求。

VLAN 配置相对复杂，企业内部对应交换机均需要配置正确。在增加新 VLAN 网络的时

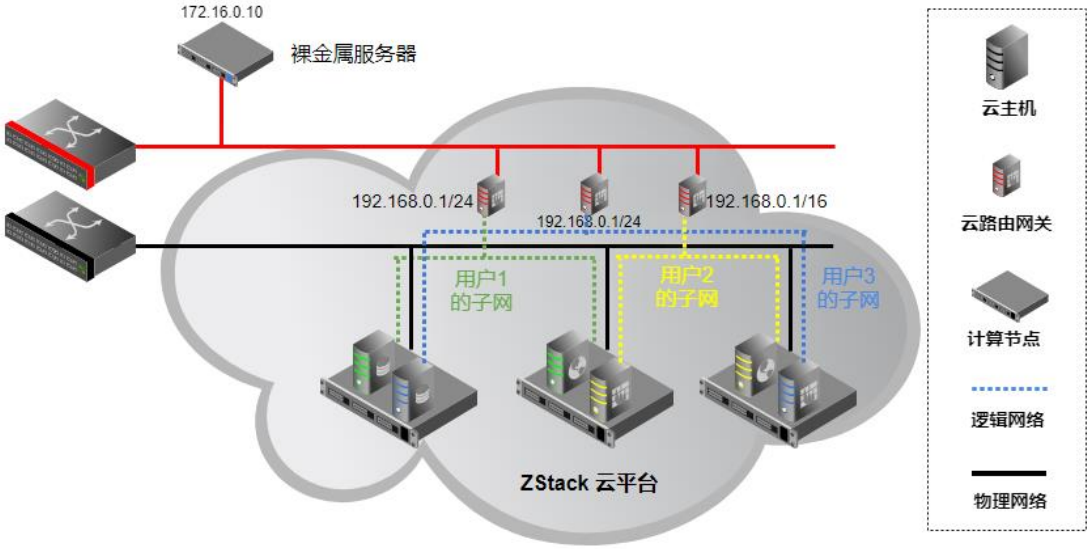
候，还需要在每个相关交换机上手工配置，维护成本很高。

云主机可以保持现有网络连接方式跨数据中心进行迁移。

大二层网络的特点是通过软件定义网络的技术，给云环境提供一个整体一致的网络访问体验。云主机可以畅通无阻的使用同一网段的 IP 地址访问不同地域的其他云主机。云主机也可以跨地域进行热迁移。ZStack 私有云可以提供秒级创建软件定义的 VxLAN 网络，帮助用户快速构建大二层网络结构，是典型的 SDN 解决方案。

纯软的 SDN 解决方案依赖服务器进行 VxLAN 报文的处理，可以满足 90%以上的客户需求。当前主流的物理网卡具有 VxLAN 报文处理能力，可以提供良好的 VxLAN 报文转发处理能力性能，并释放物理机 CPU 的工作压力。对性能有极致需求的企业，可能会采购第三方的 SDN 硬件解决方案（需要注意的是不同厂家的硬件 SDN 解决方案通常具有较大差异性），并且使用他们进行跨数据中心的互联。这种场景下，可以采用云平台管理 SDN 硬件控制器的方式统一管理；也可以分离管理，在云平台上使用预先规划好的 VLAN 与 VxLAN 交换机进行互联通信，VxLAN 交换机负责将本地 VLAN 报文打包传递给远端。

虚拟私有云



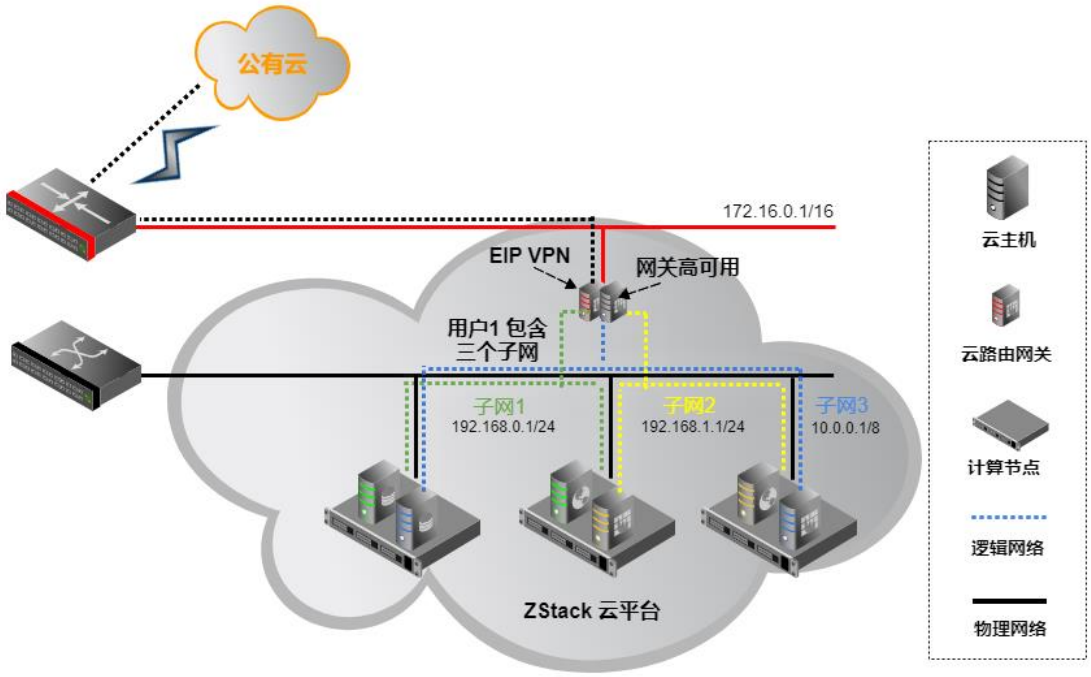
图四：多租户 VPC 网络拓扑图

用户（也称租户）可能希望私有云提供一个和企业办公网络隔离的网络环境。在这个场景中，用户可以自由定义云主机私网 IP 地址空间，云主机可以访问企业办公网，并通过企业办公网触达互联网，但是企业办公网并不能直接访问云主机私网。如图四中不同颜色的网络所示，这样的用户网络拓扑在私有云中可以有成千上万个，他们都具有相似的网络特性，它们和数据中心的网络之间通过虚拟的云路由网关相连。由于它们之间进行了二层隔离，于是可以使用相同或是重叠的 IP 子网。这种场景可以想象成，私有云是一个互联网，每个用户的隔离网络是一个企业。企业可以通过网关访问互联网的资源，互联网的资源不能直接穿透到企业内部，企业和企业的内网之间也不能直接互联。利用这样的网络架构，用户还可以自主定义和做更多的事情。例如，用户可以创建一个云主机，让这个云主机同时连接不同私有网络，这个特殊的连接不同私有网络的云主机可以访问各个网络。

用户如果希望让自定义子网的云主机能够被外网直接访问，他可以使用私有云提供的两种功能：端口转发和弹性 IP（EIP）。私有云的 EIP 与公有云的 EIP 功能是完全一样的。端口转发和弹性 IP 相当于在云路由网关上申请了一个独立的外网 IP 地址，并且把这个 IP 地址和

一些端口与内部的云主机进行了网络映射。当外网资源访问这个 IP 地址时，就会被映射访问到内网的云主机。需要注意的是，EIP 和内网云主机是一一对应的，一个内网云主机独占一个 EIP；端口转发和内网云主机是一对多的关系，“端口转发 IP 地址+端口”对应一个云主机（使用时也可以以一个端口区间进行映射）。

虚拟私有云（VPC）可以提供这样网络服务的技术，它给用户提供了自定义网络拓扑的能力。VPC 网络环境和实际企业网络环境是非常相似的，用户可以定义一个子网（包含一个三层地址空间，如 192.168.0.1/24），也可以定义多个不能重叠的子网（一组三层地址空间，如 192.168.0.1/24, 192.168.1.1/24, 172.16.0.1/16 等）。每个子网可以使用 VLAN 或者 VxLAN 进行隔离。



图五：包含多子网的 VPC 网络拓扑图

VPC 的功能强大，除了基本的子网定义和弹性 IP 功能，用户可以定义 VPC 路由表，定

义不同子网之间的连通性。通过 VPC 防火墙的功能，可以添加更多的网络防护，增强整个 VPC 的安全。通过私有云云平台的高级能力，还可以通过 VPN 等功能和其他私有云、或者公有云的互联互通，实现业务迁移和灾备等功能。用户通过云路由网关连接外部世界，云路由网关通常也是一个云主机，为了保障业务连续性，云路由网关还需提供双活高可用的能力。

私有云 VPC 和公有云 VPC 在功能上非常类似，不过私有云还可以灵活的实现一些公有云通常难以实现的功能，例如跨租户和子网的动态路由协议 OSPF、组播、端口流量监控、流量镜像等。

总结

计算、存储与网络构成了云计算 IaaS 的基础，网络是其中最千变万化的一个。云计算可以在云中快速的提供和真实场景一模一样的网络环境。能够虚拟出复杂的网络拓扑结构，并提供各种稳定便捷的网络服务，是衡量一个私有云能力的重要标准，也是云计算区别于传统虚拟化软件的重要功能。