Cloud Networking
White Paper by
Alibaba Cloud

阿里云

云网络

白皮书

云网络 数字经济的连接

云网络白皮书

云网络白皮书

1 云网络白皮书

云网络起源

1 什么是网络

计算机网络（Computer Network），通常也简称网络，是指允许节点分享资源的数字电信网络。在网络中，电脑设备会透过节点之间的数据链路互相交换数据。数据链路是异地用于收发数据的工具和介质，它也可以是一个由通信终端和连接电路组成的系统，具体的通信由专门设计的协议来控制。传输介质可分为有线及无线两类，如我们熟悉的光纤，Wi-Fi等。用于创建、路由及终止数据传输的电脑网络设备即为网络节点，节点包括像个人电脑、电话、服务器主机及其他网络硬件（如网关及路由器）等。节点一般以网络地址作标识符，当一个设备能够与另一设备交换信息时，便可视它们已连接成网络。

2 网络发展驱动应用变革

今天，我们的生活已经离不开网络，不管是购物，工作，和朋友聊天，还是娱乐等都离不开网络。淘宝，支付宝，微信，抖音，钉钉等APP也成为大家使用频率很高的应用，这些超级APP的背后，都有无处不在的网络支撑，可以说网络的发展驱动了应用的变革。

在移动网络方面，在1G时代，只能打电话，摩托罗拉大哥大，BP机就是移动通信网络的开创者。在2G时代，开始可以传输文本信息了，用诺基亚手机看文本

小说是2G时代的缩影。3G时代，互联网浪潮席卷全球。3G扩展了频谱，提升了速率，更高的带宽和更稳定的传输让移动互联网蓬勃发展。智能手机开始进入我们的日常生活中。2007年1月9日，乔布斯发布了第一代iPhone。iTunes Music Store、Safari、Email等应用，皆以图形化的方式呈现在简洁优美屏幕上。淘宝，微博等应用也纷纷搬到了手机上。4G时代，带宽更高，手机已经脱离了只是通讯设备的定位，手机屏幕变得更大，人们用手机来购物、看视频、语音、打游戏、打车等等。只要一部手机就能完成日常生活所需。今天，5G正扑面而来，5G速率高达10Gbps，比 4G 快100倍，可以轻松看3D影片或4K电影。另外，5G延时更低，可以满足远程医疗，车联网等低时延场景需求。5G的诞生，将进一步改变我们的生活和社会，推动一场新的信息革命。

与移动网络的快速发展相对应，承载众多服务的数据中心网络也在蓬勃发展，短短十年间，就从1G，10G，25G发展到了100G，并且还在快速发展着。

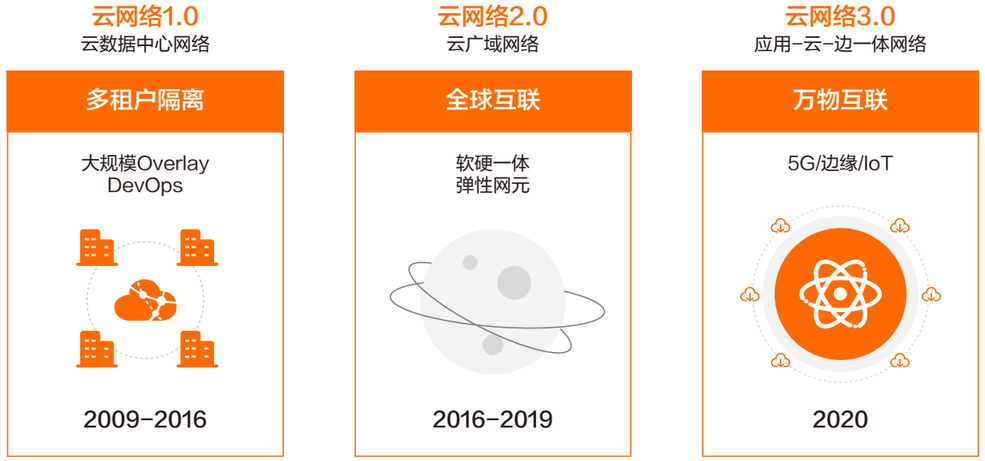
3 云计算驱动云网络诞生

2010年5月10日，阿里云对外发布第一个商业化的产品-云服务器ECS，正式提供公共云服务。那时候，可能很多人都没有想到，云计算对网络的影响会如此之大。2012年底，随着虚拟化技术的发展，单物理机的虚拟比在逐步提高，对网络设备提出了非常高的要求，当时全世界都已经找不到满足业务虚拟比的网络设备了。除此之外，当时的云网络架构还存在迁移域过小导致成本增加，稳定性、性能、安全等也都存在问题和隐患，这些问题极大的影响云业务的开展。与此同时，随着更多用户上云，尤其是大型互联网企业和传统企业的上云，用户对云上网络管理需求也与日俱增。比如，用户在云上多地域部署业务，需要多地域内网互通，或者用户需要把云下IDC和云上网络互通，构建混合云等等，而这些网络管理能力，当时云上的传统网络服务方式都难以满足。因此，不管是用户，还是云服务平台，都迫切需要进行网络创新。2012年，阿里云率先放弃传统的大二层网络架构，设计新的网络虚拟化（Overlay）技术方案，开启了云网络的新篇章。

4 阿里云云网络发展历程

阿里云网络发展经历三个阶段，从2009年的云网络1.0到2020年的云网络3.0。阿里云从2009年开始投入云计算的研发，早期云上基础网络采用传统大二层网络构建，租户之间的隔离基于安全组实现。阿里云2012年开始研发网络虚拟化（Overlay）技术方案，到2014年，VPC产品正式发布，VPC是一个标志性的产品，意味着云上用户网络从此从传统网络转向VPC网络，用户在云上有了一个自己私有隔离的网络环境，也开始拥有之前在云下才具备的网络管理能力。加上前后发布的弹性公网IP-EIP，负载均衡SLB，NAT网关等产品，构成了云网络1.0。云网络1.0主要做的是云数据中心网络，用户在云上通过VPC，虚拟交换机，虚拟路由器构建了网络环境，通过EIP，负载均衡SLB，NAT网关等产品实现互联网访问，负载均衡等功能。

阿里云网络发展历程



云网络2.0的核心是云广域网络。用户在云上多地域部署业务系统后，很自然的需求就是多地域内网互通，另外，用户还有云下IDC和云上VPC互通的需求，云广域网络可以很好的满足用户这两个业务场景的需求。2017年，阿里云在业内率先发布云企业网CEN，用户可以非常简单快速的构建一张全球化网络。2018年，阿里云发布了

云原生SDWAN产品-智能接入网关SAG，方便用户快速上云。云网络2.0让用户具备了构建一张云化的全球网络能力。

2020年，5G/IoT/边缘计算技术的发展，社会进入万物互联和产业互联网时代，云计算已经成为整个数字社会的基础设施，云网络也开启了3.0时代，云网络作为数字化社会的高速公路，将万物互联，助力产业互联网的发展。

云网络产品十年大事记

5 云网络是数字经济的连接

那么，到底什么是云网络？它和传统网络有什么不同吗？首先，云网络是IT和CT融合的产物。云网络并不是要重建一张新的网络来取代现有的网络基础设施，而是在现有网络基础上通过网络虚拟化等技术重构。前面讲到，云计算驱动云网络的诞生，云网络其实是CT（Communication Technology，通信技术）与IT（Information Technology，信息技术，这里主要是云计算）融合的产物。 其次，云网络其实一种是网络服务，也是一张面向企业租户和应用的虚拟网络。最后，云网络是数字经济的连接，连接计算、存储、数据库等等，也连接企业/IDC/总部/分支/IoT终端/个人移动端等等。云网络和传统网络的最大区别是云网络具备共享/弹性/自助服务/按需等云的特征。

❶ 云网络具备云的特征

第一是资源共享。为了实现资源共享，网络必须虚拟化与安全隔离。这里就会

用到Overlay技术。网络技术的本质是“编址+路由”，Overlay的编址是指在数据报文编址上再叠加一层租户标识，通常现在使用VxLAN技术，在租户报文先增加了IP+UDP+VxLAN（租户ID）。使用VxLAN技术对云网络进行编址避免了对物理网络设备（交换机/路由器）的升级。在路由层面是实现路由表的隔离，这就要求向每个租户提供虚拟设备，如虚拟交换机/虚拟路由器/虚拟负载均衡等。

第二是弹性伸缩。网络处理能力主要由转发能力与控制能力决定。对于传统设备来说，设备买回来，处理性能就确定了，难以弹性伸缩。云网络为了应对弹性伸缩的，将控制面与转发平面进行分离部署，并且采用集群的方式支持扩展，结合网络虚拟化技术为每个用户提供了弹性网络能力。

第三是自助服务。这是从用户视角看到的云网络与传统网络的最大区别。传统网络采用分布式智能控制，支持人-机接口对多台设备的配置，需要专业网络管理员敲CLI(Command Line)命令行进行配置，而云网络支持机-机接口，集中管理，通过编程或者集中的控制台就可以完成网络搭建。

第四是按需付费。云网络改变了网络购买方式。传统网络设备会根据设备性能规格+功能特性+维保进行收费，即使有的企业设备利用率不到30%，也只能超额购买，而云网络借鉴了CT领域按量计费方式，支持采用预付费或者后付费方式，根据企业实际使用量进行收费。从技术上看，就需要云网络对每个租户的处理能力和转发的流量进行定时的打点计费和出账单。

❷ 云网络改变了商业模式

从最终用户看，云网络改变了企业购买网络的方式。传统的方式中，提供应用服务的企业为了搭建数据中心，需要购买多项业务。1.向集成商购买咨询与交付服务；2.向多家设备商分别购买交换机/路由器/防火墙/负载均衡/服务器和维保服务 3.向云计算软件厂商或利用开源搭建虚拟化环境 4.向多家运营商购买带宽与专线。这需要涉及漫长的协调/沟通过程，需要耗费很长时间与精力。

当云网络出现以后，企业直接在控制台或者写程序调用云网络API，很快完成部署。对于云能力欠缺的企业也可以找到MSP（Management Service Provider管理服务提供商）来完成云环境的搭建。

对于仅提供移动互联网应用的企业，云环境搭建是相对简单的操作。但对传统企业需要实现总部/分支/移动办公等向云的平滑迁移，云网络的设计就尤为重要。通过云网络的服务化提供方式，企业可获得许多传统网络中无法获得的能力。比如获得企业应用全球部署的互联与加速能力；具备云-管-边-端的连接能力；可感知到应用的实际使用量与网络服务质量。当然由于涉及与传统网络对接，在企业专线上云等还是需要向运营商购买。

云网络的服务化提供改变了咨询服务行业。20年前获得各种设备厂商的认证是一件很有含金量的事情，运营商和企业都招聘了一批精通网络配置的专家。今天采用云服务以后，需要具备的技能发生了很大的转变，需要了解计算/安全/数据库/大数据/AI的基础知识，更需要懂得应用部署方式，才能更好地进行网络规划与设计。在部署上不再需要敲命令行，而是需要学会编程根据应用负载驱动网络的调度。

从上游供应链角度看，由于云网络的服务化提供，运营商更多的将带宽资源通过云厂商进行售卖。对于技术开发实力较弱，通过售卖资源的IDC提供商正在逐步转变为云管理服务提供商，帮助企业通过构建混合云平滑迁移上云。

❸ DevOps变革了产业生态体系

CT行业运营商，在构建移动与固定网络时，首先需要考虑是互通的标准。这样的标准化对于降低成本也有极大的好处。采用相同的标准就可以由多个设备提供商制造，通过招标采购达到降低社会总体成本的目标。 这种方式的弊端在于形成标准的时间过长，回顾2G到5G的发展历程，基本上从标准制定到商用需要5年以上的时间。网络设备的发展经历了技术+竞争+场景的不断的叠加，在特定场景中会发现某类网络设备中包含了很多无用的功能。

“天下武功，唯快不破”，为了提升云网络服务发布效率，云网络在开发模式上采用了IT行业的DevOps方式。在云网络产品开发模式发生了变化，为了快速满足市场需求，不再采用招标模式，而是采用了自研方式。一些公司将开发的成果贡献到开源社区。完全采用开源模式是否可支撑云网络发展呢？以开源OpenvSwitch为例：为了避免对Linux内核改造，充分复用 Linux TCP/IP协议栈的特性与能力，OpenvSwitch在内核的处理性能并不理想。在10G服务器时代还可勉强维持，但升级到25G/100G以后，这样的架构就勉为其难了。由于需要利用软/硬件结合提升转发处理性能，也给网卡芯片/交换芯片提供商带来了新的机会与挑战。通过对最新技术的不懈追求，持续提升网络处理性能，使云网络产品快速发展。

云网络的技术架构与开发模式，对传统的物理网络设备会带来一些冲击。这些设备主要包括交换机，路由器，负载均衡和防火墙等。由于服务器与存储间的物理连接依然存在，对物理交换机/路由器的影响有限，依然要求具备高性能、低时延的转发需求。由于云网络中的虚拟交换机采用VxLAN等Overlay技术，对物理交换机的表项要求变小了。当复杂的应用协议层处理剥离到云网络虚拟化层后，物理连接层尽量减少使用二层部署带来的环路问题，对底层物理交换机的功能需求也会减少。为了提升运维效率，要求物理网络的监控功能提升，物理网络的人-机 CLI（Command Line）接口转变为API接口实现机-机监控。但由于各厂商标准不统一，交换机有被白盒化的趋势。云网络对于4~7层防火墙，负载均衡等网络设备的冲击尤为巨大，简单的把传统的设备进行软件化，并不能带来弹性伸缩能力，很多原有的4-7层网络设备正被取代。

由于采用了DevOps方式，云厂商同时具备开发与服务运维能力，可以根据实际运维过程中的需求，在开发时快速提供管理接口。由于涉及众多租户和应用在线不间断的使用，基本上靠人使用脚本方式来管理已经不可能。需要考虑使用更智能的方式对网络进行监控、故障逃逸、版本升级管理。云网络要求新/旧版本间能进行平滑升级与回滚。

对于企业来说，管理运维云网络也发生了巨大的变革。因为已经看不到实体设备，很多网络的管理工作交给了云厂商，但是依然需要从应用的视角去感知网络的质量与故障，进行应用层的可靠性保障。

在过去的10年间，大部分的互联网企业已经将应用部署在云上，充分利用云网络的能力向消费大众提供服务。基于互联网升级的云计算已经成为社会经济基础设施。变革已致，未来已来。企业上云，网络先行，云网络必将作为数字经济的连接，携互联网新技术惠及各行业。

2 云网络白皮书
云网络产品体系

云网络改变了用户购买和使用网络的方式，用户不再需要购买硬件设备，而是通过购买云网络产品和服务来满足业务的网络需求。因此，在云计算时代，用户使用网络往往接触到的是云网络产品。

1 基本概念

在介绍云网络产品体系前，先介绍几个相关的基础概念和产品名称及简写。阿里云在基础设施层面分为地域和可用区两层，关系如下图，在一个地域内有多个可用区。每个地域完全独立。每个可用区完全隔离，同一个地域内的可用区之间使用低时延链路相连。

地域（Region）

地域是指物理的数据中心。资源创建成功后不能更换地域。用户可以根据目标用户所在的地理位置选择地域，不同地域的相同产品之间，内网不能直接通信；同时就产品维度来看，不同地域的资源价格可能有差异。

可用区（Availability Zone，简称AZ）

可用区是指在同一地域内，电力和网络互相独立的物理区域。同一可用区内实例之间的网络延时更小。在同一地域内可用区与可用区之间内网互通，可用区之间能做到故障隔离。

接入点（POP点）

一般指物理专线接入阿里云的地理位置，在每个接入点有两台接入设备。每个地域下有一到多个接入点，本地数据中心可以从任意一接入点与VPC互连。

主要相关产品中英文名称和简写如下：

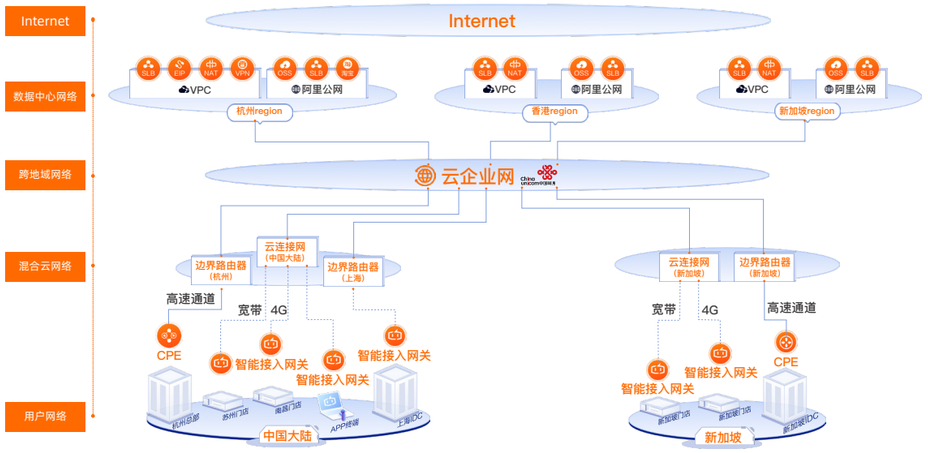
产品名称(中文)	产品名称（英文）	简称
专有网络VPC	Virtual Private Cloud	VPC
IPv6网关	IPv6 Gateway	无
私网连接	PrivateLink	无
负载均衡	Server Load Balander	SLB
NAT网关	NAT Gateway	NAT
弹性公网IP	Elastic IP Address	EIP
共享带宽	无	无
云企业网	Cloud Enterprise Network	CEN
全球加速	Global Accelerator	GA
VPN网关	VPN Gateway	VPN

产品名称(中文)	产品名称（英文）	简称
智能接入网关	Smart Access Gateway	SAG
高速通道	Express Connect	无
DDoS防护	Anti-DDoS Service	无
云防火墙	Cloud Firewall	无
Web应用防火墙	Web Application Firewall	WAF
云服务器	Elastic Compute Service	ECS

2 产品体系架构

云网络产品体系主要分为数据中心网络，跨地域网络，混合云网络三大部分，可以分别映射为传统网络的数据中心网络，数据中心互联网络，接入网络。如下图所示：

云网络产品体系架构



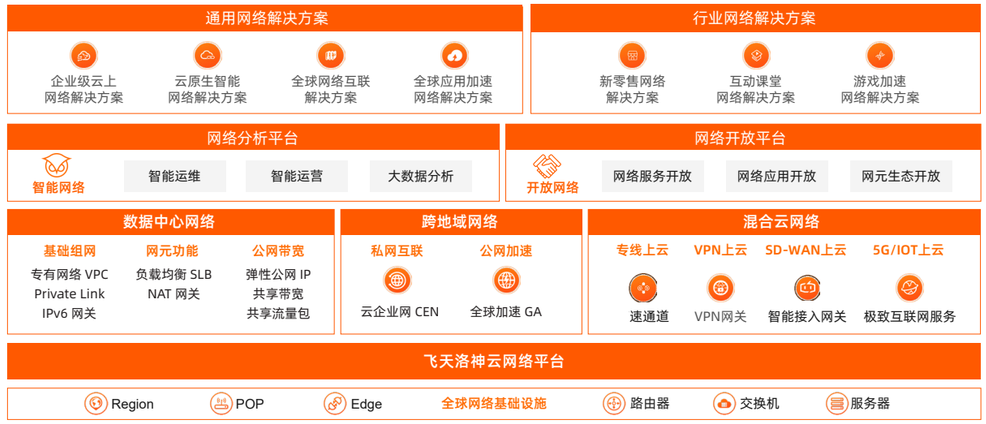
数据中心网络产品让用户具备在云上某个地域构建业务系统的网络能力，包括构建云上网络环境，管理Internet流量等。产品主要包括专有网络VPC，负载均衡SLB，NAT网购，弹性公网IP等。

跨地域网络产品为用户提供了多地域私网互联和跨地域公网加速能力。用户通过跨地域网络产品可以满足多地域，甚至全球化部署业务系统的需求。跨地域网络产品主要包括云企业网CEN和全球加速GA。

混合云网络产品可以为用户构建云上云下互通的混合云，为传统用户提供快捷的上云通道。混合云网络产品包括VPN网关，智能接入网关，高速通道。

从另外一个角度看，云网络的最底层是全球网络基础设施，之上是洛神云网络平台，再上一层是数据中心网络，跨地域网络和混合云网络三大产品体系，之上是云网络的智能和开放，分别通过网络分析平台和网络开放平台承载，最上层云网络解决方案，包括通用和行业网络解决方案。

完整的云网络产品和解决方案



3 数据中心网络产品

用户在使用云下数据中心构建业务系统的时候，对于网络的构建往往需要以下几个步骤：

1）寻找合适的数据中心，租赁机柜

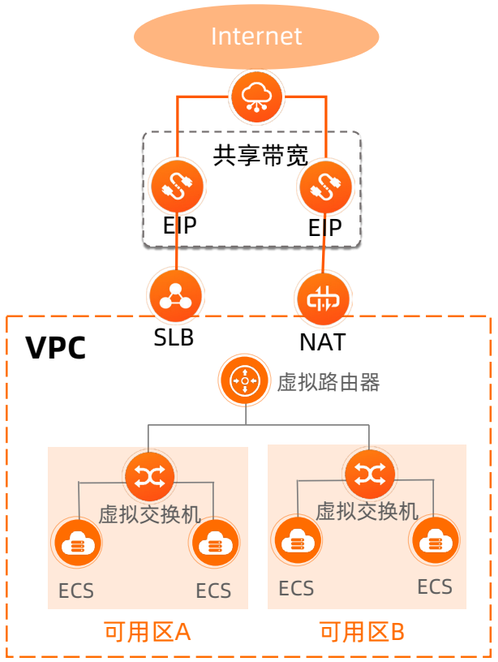
2）从运营商购买IP地址和Internet带宽

3）购买网络设备，如路由器和交换机

4）配置网络设备，如划分VLAN，配置IP地址等

经过这些步骤后，数据中心的基础网络环境就配置好了，但还不够，一般还需要购买和配置负载均衡设备，进行流量调度和实现系统高可用，此外往往还需要购买和配置防火墙设备。

数据中心网络产品就是为满足用户上述需求的，让用户具备在云上某个地域（Region）构建云上数据中心网络的能力，而且用户只需要通过在线购买服务的方式就可以很快实现。如下图所示，是北京Region的云上数据中心网络产品架构图。

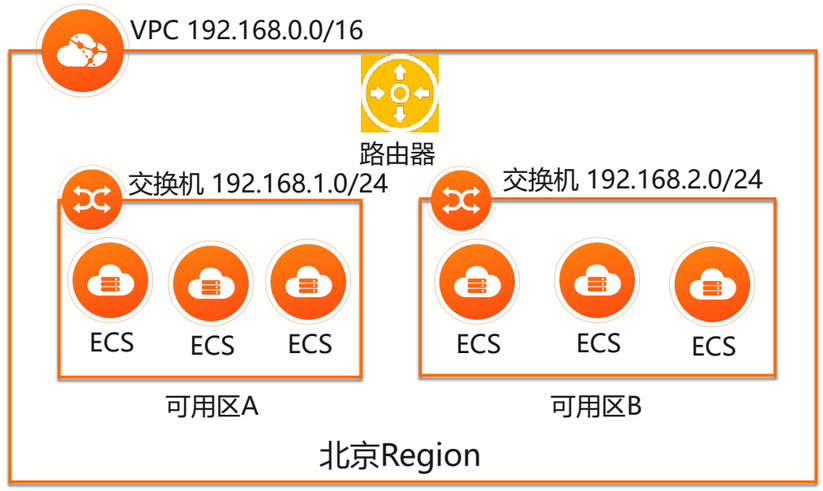


北京Region

❶ 构建专有网络环境

VPC是用户在云上私有的安全隔离的网络环境，是用户在云上部署业务系统首先需要开通的云网络产品。VPC基于隧道技术来实现，不同用户的流量都只在各自的隧道里面流动，默认情况下都是不能互通的，从而实现了VPC的安全隔离。

使用VPC，用户可以在云上获得完全自己掌控的专有网络，例如选择IP地址范围、配置路由表、配置网络ACL等等。VPC的基本组成包括虚拟路由器和虚拟交换机，路由器是专有网络的枢纽，可以连接专有网络的各个虚拟交换机，同时也是连接专有网络与其它网络的网关设备。路由器根据路由条目来转发网络流量。虚拟交换机代表专有网络的一个子网，在子网中可以存放各种云资源，包括云服务器ECS，数据库RDS等。



VPC还支持网络ACL，子网路由，Flowlog，ShareVPC等高级功能，可以很好的满足用户构建云上数据中心网络环境。

❷ Internet带宽和流量

公网IP地址和互联网带宽–EIP和共享带宽

要让云上部署的业务系统对用户提供服务，公网IP地址和互联网带宽必不可

少。云上提供了丰富的公网IP地址资源和不同性价比的带宽。弹性公网IP（Elastic IP Address）是可以独立购买和持有的公网IP地址资源，可以绑定到私网SLB、NAT网关和云服务器ECS上，使用非常灵活。互联网带宽类型包括Anycast、多线带宽、单线带宽等，用户可以根据需要选择。当用户IP地址很多，流量峰值很大时，还可以选择使用共享带宽产品。

Internet流量管理-SLB和NAT网关

负载均衡是常用的流量管理和调度产品，几乎我们熟悉的所有网站或者应用背后都有负载均衡的支撑。比如淘宝网站，钉钉，支付宝等等。负载均衡可以通过流量分发来提升应用系统的服务能力，通过消除单点故障来提升应用系统的可用性。负载均衡SLB主要解决用户以下几个问题：

1）单ECS处理能力不足，需要多ECS做负载均衡

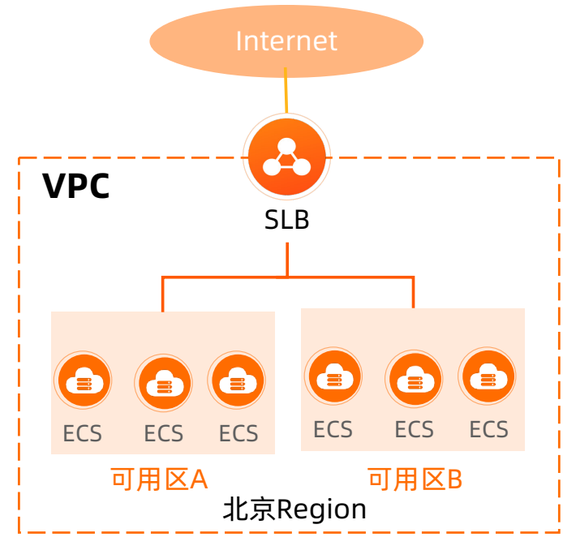
一些中大规模的系统和网站，访问流量比较大，单台ECS处理能力不足，需要使用多台ECS，因此需要SLB做流量调度以提升系统的服务能力。

2）单ECS可用性不足，需要多ECS做负载均衡高可用

一些关键的系统和网站都需要考虑高可用，避免一台ECS故障就受影响。SLB支持健康检查，可及时发现和屏蔽故障ECS。

3）大流量处理和调度

访问量大的网站和系统，对大流量的处理调度能力要求很高，比如双11购物节的天猫网站，就需要面对海量访问洪峰。SLB超强性能，丰富的调度算法可以轻松面对大流量的调度。



4)基于应用层的流量调度

应用负载均衡支持HTTP和HTTPS协议，提供高级的7层功能，如基于内容的路由，QUIC协议支持等，满足越来越多元化的应用层负载需求，大大提升交付效率，同时还具备超强性能（100万QPS/实例）、安全可靠、面向云原生、即开即用等优势。

NAT网关产品可以让无公网IP地址的ECS访问互联网，如用户有大量无公网地址的ECS有访问互联网的需求，但为了简化管理，不想为所有的ECS申请绑定公网IP地址，就可以使用NAT网关的SNAT功能。天猫双11购物，当我们选择好宝贝，点支付的时候，就需要通过部署在ECS上的程序通过NAT网关的SNAT功能去访问支付宝的支付接口，以完成支付。

❸ IPv6产品和方案

截止到2020年7月，据中国信息通信研究院监测分析，我国IPv6活跃用户数达3.62亿，在互联网用户中的占比达40%，可以说IPv6已经从发展趋势变成了事实。云

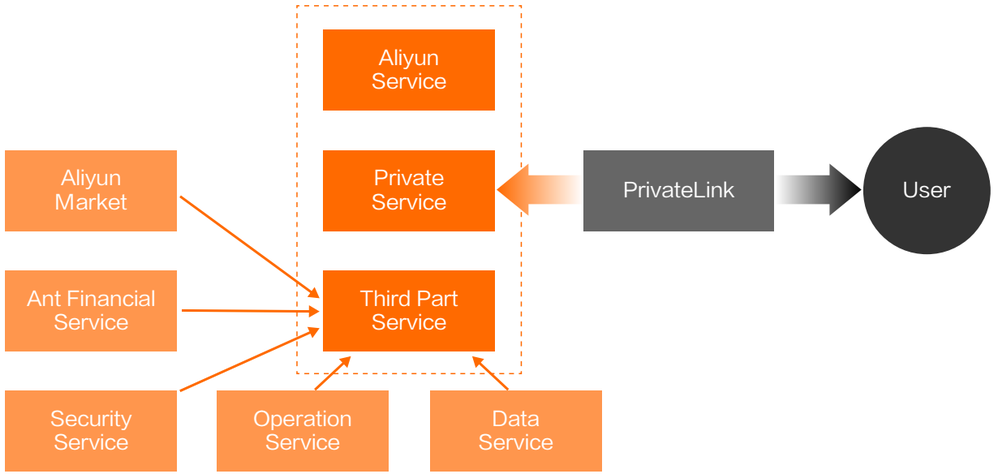
网络产品已经提供了丰富的IPv6产品和解决方案，包括：

内网通信支持IPv6，如VPC支持IPv6，CEN支持IPv6，高速通道支持IPv6等，用户可以在云上建立纯IPv6通信网络。

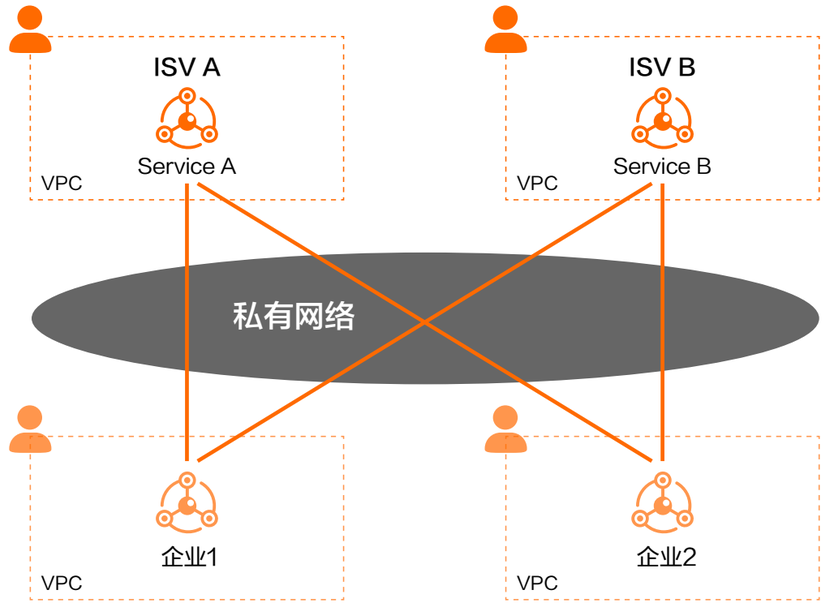
公网通信支持IPv6，如SLB支持IPv6，IPv6网关等等。此外，云网络还为其它产品提供了IPv6支持，如安全，数据库等等，用户可以基于云构建完整的IPv6体系。

❹ 企业服务总线

私网连接（PrivateLink）允许用户在自己的VPC内通过内网访问阿里云服务，第三方服务或者自建服务。内网访问更安全，更稳定，更可控，更重要的是，私网连接（PrivateLink）是跨企业提供服务的，为云上企业之间构建了内网通信通道，是企业服务总线。



如下图所示ISV A和ISV B分别在自己的VPC发布基于私网的服务ServiceA 和ServiceB，企业A和企业B在自己的VPC内就可以通过PrivateLink私网去访问这两个服务。



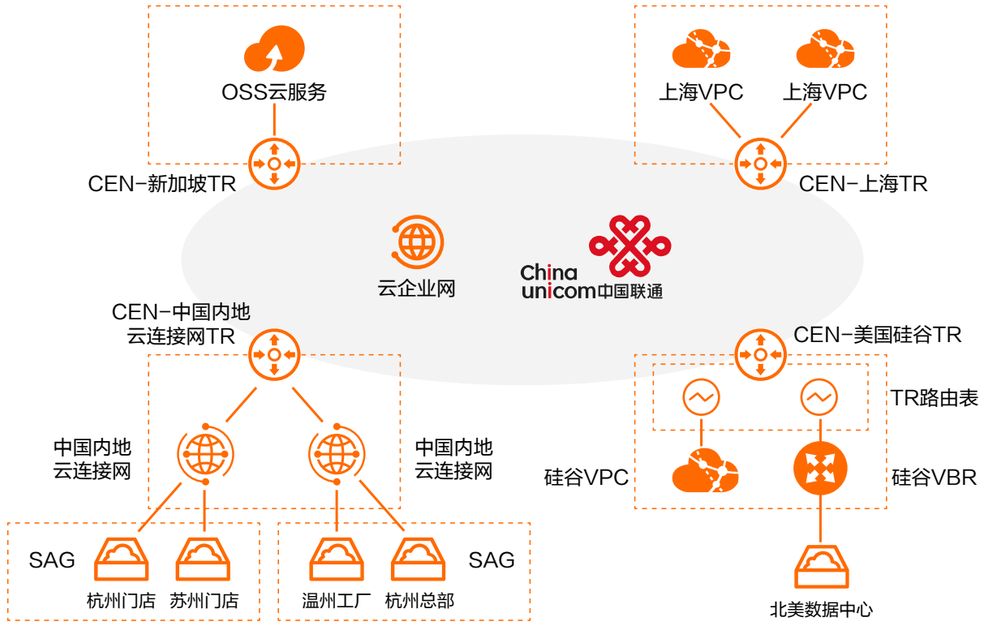
4 跨地域网络产品

跨地域网络产品对应的是传统网络中的数据中心互联产品，但比传统的数据中心互联产品又有所不同和延展，不同的是云上跨地域互联产品也可以在同地域的不同VPC间实现互联，还可以实现云上VPC和云下IDC的互联，构建一张云上云下一体的私有网络，延展的是基于跨地域网络的公网应用加速产品。

注：阿里云跨地域网络产品中涉及跨境部分均由中国联通运营。

❶ 跨地域内网互联

云企业网CEN为用户提供了在云上构建多地域互联核心网的能力。为什么需要云企业网CEN呢？如下图所示，主要是因为企业需要多地域部署业务系统和构建云上云下混合云。



1）多地域部署业务系统

多地域部署业务系统可以极大的提升业务系统的可靠性和用户体验。多地域部署业务系统可以避免单地域不可用而导致故障。用户在多地域部署业务系统需要开通多个VPC，多个VPC的业务系统往往需要私网通信，以保障通信安全和质量，用户使用云企业网CEN把多个地域的VPC连起来，组成一张内部网络。当然，用户在同一个地域使用多个VPC时，也可以使用云企业网CEN。此外，在多地域部署业务系统对用户提供服务，也意味着可以离用户更近提供服务，提升用户体验。

2）云上云下构建混合云

有的用户还处在上云过程中，云下IDC还部署了业务系统，这时，采用混合云就是一个很好的选择。而构建云上云下的混合云，首先需要考虑的就是使用什么产品构建混合云。通常情况下，用户使用高速通道（专线）和智能接入网关SAG构建混合云，并配合云企业网CEN和云上VPC实现内网通信，构建云上云下一体的私有网络。

借助云企业网CEN，用户可以低成本、分钟级构建一张全球化的云上网络，快速为全球用户提供服务。同时，云企业网底层使用阿里云覆盖全球的优质传输网络，保障了网络的稳定性和低延迟。

❷ 跨地域公网加速

全球加速GA是跨地域网络产品中的公网应用加速产品，是基于跨地域网络构建的网络PAAS产品，是一款覆盖全球的公网应用加速服务，依托阿里云优质的全球互联网带宽与高品质传输网络，实现网络服务全球范围就近接入和跨地域部署，提升服务可用性和性能。

全球加速GA可以为用户解决以下问题：

1）互联网应用全球用户访问网络质量差

当前，软件与应用互联网在线化是大势所趋，尤其是受新冠疫情的影响，远程在线协同办公与跨地域跨国长距离的应用访问需求集中爆发，无论是互联网公司还是传统企业，都更加依赖高质量的服务访问，这离不开高质量的网络。

2）传统静态内容加速方案对动态交互应用效果差

对于实时性要求高的动态交互型内容，传统的静态加速方案效果有限，必须依赖网络底层资源的加速方案。

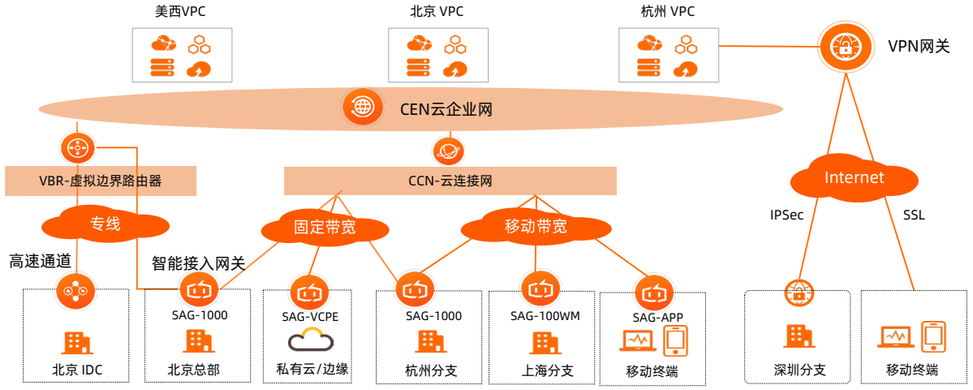
3）向全球用户快速提供高质量的服务

面向全球用户提供高质量的服务，一种做法是在全球部署业务系统，即使基于云构建，也相对比较复杂，需要较大的投入，耗费较长时间，这无法满足“唯快不破”的互联网时代需求，而且很多用户也没有这么大的资金投入。这时，采用全球加速GA就是最快速、最经济、最简单的方案。通过全球加速把应用访问入口全球部署，但应用只部署在少量地方，可以快速向全球用户提供高质量的服务。

此外，全球加速GA和云原生的安全能力联动，保护互联网服务免受攻击，加固对终端节点的安全访问，随时升级防御T级别攻击。快速（分钟级）完成部署开通，业务架构“零”改动。

5 混合云网络产品

混合云是当前和未来较长一段时间都会持续存在的一种形态，因此，选择什么产品构建混合云就显得尤为重要。如下是阿里云混合云网络产品大图。



阿里云混合云网络产品可以把IDC/总部/分支/门店/边缘/移动终端等通过VPN网关，智能接入网关SAG，高速通道产品和云上VPC构建一张云上云下一体的私有网络。这些产品简单对比如下，用户可以根据需要选择一种或多种混合云网络产品。

项目	智能接入网关SAG	VPN网关	高速通道
链路	公网+专线	公网	专线
质量	中	低	高
成本	中	低	高
交付周期	中（硬件版-天/软件版-分钟）	短（分钟）	长（月）

此外，这些混合云网络产品可以单独使用，也可以配合使用，比如使用高速通道作为主链路，使用SAG作为备份链路，支持自动切换，再配合云企业网CEN构建一张企业级的私有网络。

1 VPN网关

VPN网关是一款基于Internet链路，通过加密通道将企业数据中心、企业办公网络等和阿里云专有网络(VPC)安全可靠连接起来的服务。VPN网关是快速低成本构建混合云的最佳选择，可满足小带宽（一般小于500M），且对网络质量相对不敏感的业务需求。此外，VPN网关也经常用于高速通道（专线）开通前的POC以及备份。VPN网关功能丰富，支持IPSec和SSL协议、支持动态路由协议BGP、国密、IDaaS服务通过AD认证等。

2 智能接入网关

智能接入网关（Smart Access Gateway，简称SAG）是阿里云自研的云原生SD-WAN解决方案，可以实现企业IDC、分支、门店、边缘节点、移动端等多种类型网络节点一站式接入上云，形成一张企业级私有网络。SD-WAN(Software-Defined WAN)，即软件定义广域网，相比传统WAN网络脱颖而出，主要是具有以下几个优点：

1）最具性价比

通过专线链路和互联网链路的组合，可以极大的降低昂贵的专线带宽使用量从而降低企业网络线路成本。

2）ZTP快速安装部署

支持零配置安装部署（ZTP），自动协商建立VPN隧道，即插即用。除此之外所有网络路由信息集中处理、自动分发，即使有数千家门店，任何一个节点的网络变化，全网其他节点无需任何网络配置。

3）远程集中管理降低运维成本

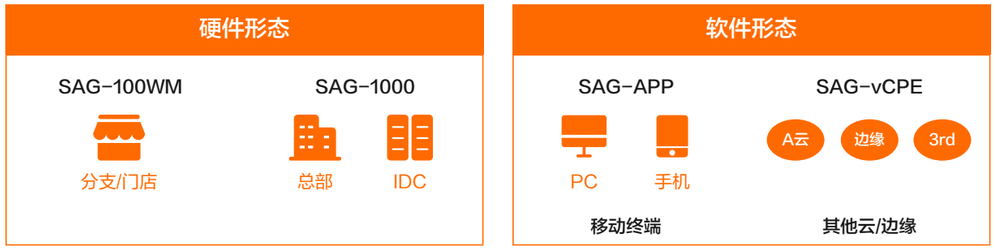
传统网络架构是同一个网络设备既有转发模块也有控制模块，而SD-WAN将转发和控制分离，所有节点统一通过中心化控制台远程管理极大的简化了运维管理。从运维视角来看，传统组网看到的是多个点（网络设备）+多个连接，而SD-WAN架构下看到的是一张网。

4）云原生

以云为中心，为云而生，依云而建。企业上云后，云下的数据中心、办公室以及各种各样的终端设备要和云上的应用进行交互。要做到云上云下深度的应用集成，就要求整个网络以云为中心，实现云-管-边-端一体化。另一方面对应用来说，对云和网的感知是一体的无差异的。所有节点一键访问云服务，云上云下统一端到端的安全策略。

5）丰富的产品形态

SAG提供了硬件和软件两种产品形态，以满足不同的接入需求。硬件形态提供了SAG-100WM，SAG-1000两种型号，分别适合在分支/门店和总部/IDC使用，软件形态提供了SAG-APP和SAG-vCPE两种形态，分别适合在移动终端和边缘/其它云使用。



2020年11月，权威调研机构 IDC 发布了 2020 年上半年《中国软件定义广域网（SD-WAN）市场跟踪报告》，阿里云智能接入网关SAG同比增速超600%，以 25% 的市场份额领跑中国 SD-WAN 服务领域。

❸ 高速通道

高速通道（Express Connect）提供了通过基于运营商专线接入公共云的能力，可以提供超大带宽、稳定安全的私有上云通道，是大型混合云架构的最佳选择。

高速通道的核心优势是高性能和高质量。

随着互联网的快速发展，产生了越来越多的海量数据，对网络带宽性能的要求越高。传统VPN等基于互联网的软专线受限于互联网的带宽规格以及加密处理的性能损耗，通常很难提供单点高于1Gbps的带宽规格，而高速通道单链路最大支持100Gbps的带宽，而且支持多线负载理论上可以无限水平扩容，非常适合互联网、大数据、人工智能等数据密集型应用。在质量方面，高速通道依靠运营商的专线资源，相对于VPN底层通过互联网加密技术，网络路径无绕行提供了最低的时延，另外不用和其他用户争抢带宽资源则保证了质量。

高速通道提供了独享专线和共享专线两种接入方式。

独享专线是企业自主拉通本地数据中心到阿里云接入点的专线，该方式独占一个物理端口，相对来说周期比较长但是对专线资源更有掌控力。企业先需要向运营商购买专线再向阿里云购买接入资源。线路开通过程中运营商需要进行工勘、铺设专线等工作，整个施工周期预计需要2个月左右。

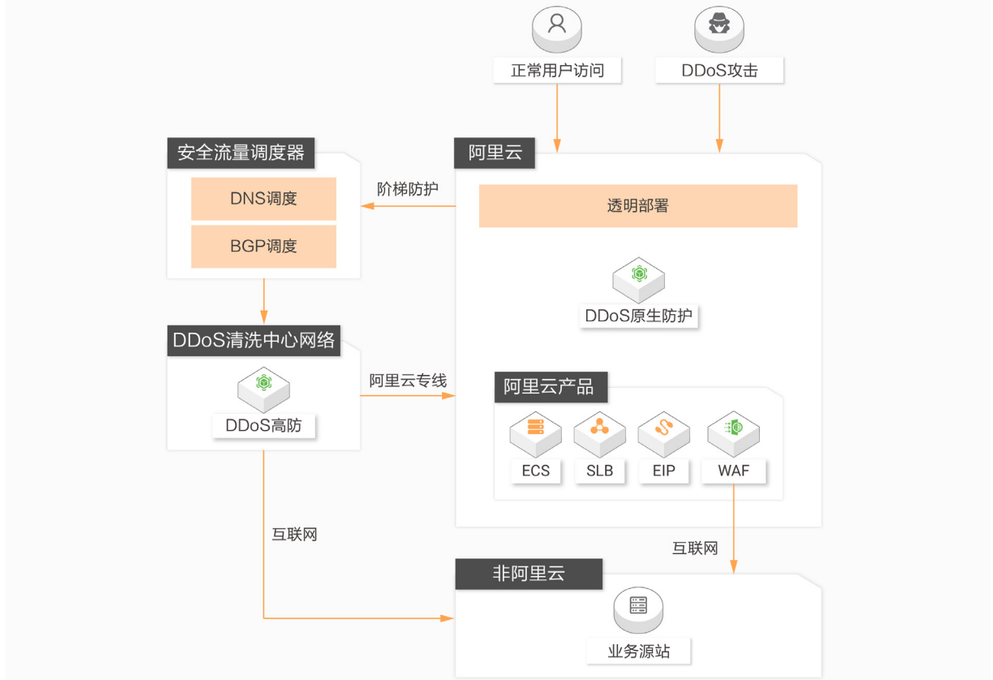
共享专线是合作伙伴的接入点已经与阿里云的接入点完成了对接，用户只需联系阿里云的专线合作伙伴，合作伙伴会完成本地IDC机房到合作伙伴接入点的专线部署。相比自建独享专线连接，合作伙伴已经预先完成了从运营商接入点到阿里接入点的最后一公里专线铺设，运营商只需要为企业完成从运营商接入点到本地IDC机房的最后一公里专线铺设，大大节约了上云施工周期时间。

6 网络安全产品

云网络产品为用户提供了诸多安全能力，如VPC给用户在云上提供了私有安全隔离的网络环境，VPC还支持网络ACL，子网路由，CEN支持TR等实现网络访问控制和通信管理等功能。除此之外，阿里云还为用户提供了丰富的高级网络安全能力以及产品，帮助用户在云上搭建层次化的纵深防御体系，多维度提升整体云上网络安全。主要网络安全产品包括DDoS防护，云防火墙，Web应用防火墙等。

❶ DDoS防护

DDoS防护（Anti-DDoS Service）是针对在互联网上提供服务的企业在遭受DDoS攻击情况下，使用阿里云全球DDoS清洗网络，秒级检测系统，AI大数据引擎，高效地缓解DDoS攻击，保障业务持续稳定运行。阿里云使用自主研发的DDoS防护系统保护所有数据中心，支持防护全类型DDoS攻击，并通过AI智能防护引擎对攻击行为进行精准识别和自动加载防护规则，保证网络的稳定性。同时，阿里云的DDoS防护系统支持通过安全报表，实时监控风险和防护情况。



阿里云的DDoS防护系统，不仅仅能够支持客户的云上业务，也可支持云下企业客户使用阿里云在全球部署的大流量清洗中心资源，结合AI智能防护引擎，通过全流量代理的方式实现对大流量攻击防护和精细化Web应用层资源耗尽型攻击的防护。

❷ 云防火墙

云防火墙是业界首款公共云环境下的SaaS化防火墙，与云产品天生高度融合实现串行防护，可以统一管理互联网到业务的南北向访问策略和业务与业务之间的东西向微隔离策略。这是因为在云上环境中，用户不但需要管理进出互联网的边界，也需要在云产品之间、VPC之间、乃至虚拟机实例之间进行网络边界管理。通过云防火墙，用户可以对南北向和东西向访问的网络流量进行分析，并支持全网流量（互联网访问流量，安全组间流量等）可视化，并支持对主动外联行为的分析和阻断。

云防火墙独创基于NFV的内网VPC边界、和主机边界流量的纵深管控和防护，全流量分析可见。基于云上强大的威胁情报和深度智能学习能力，提供网端一体实时入侵防护、智能化访问控制，全流量日志溯源分析等能力，帮助企业构建“多层跨域”立体式防护，全面守护云上用户的安全。

目前阿里云云防火墙已为阿里集团内部、金融云、云上近万用户提供业内领先的防护能力。每天帮助用户防御云上网络入侵行为8000万+，构建活跃恶意IP与域名威胁情报图谱500万+，并通过首创智能策略帮助用户收敛超过25%的网络风险暴露面。

❸ Web应用防火墙

Web应用防火墙（Web Application Firewall，简称WAF）服务，基于云安全大数据和智能计算能力，通过防御SQL注入、XSS跨站脚本、常见Web服务器插件漏洞、木马上传、非授权核心资源访问等OWASP常见web攻击，过滤海量恶意访问，避免网站资产数据泄露，保障网站应用的安全性与可用性。

3 云网络白皮书

云网络技术体系

云网络以云为中心，提供全面的连接能力。云网络弹性、按需、自主等特征要求云网络技术具备虚拟化、自动化、高性能等技术特征和技术实现。

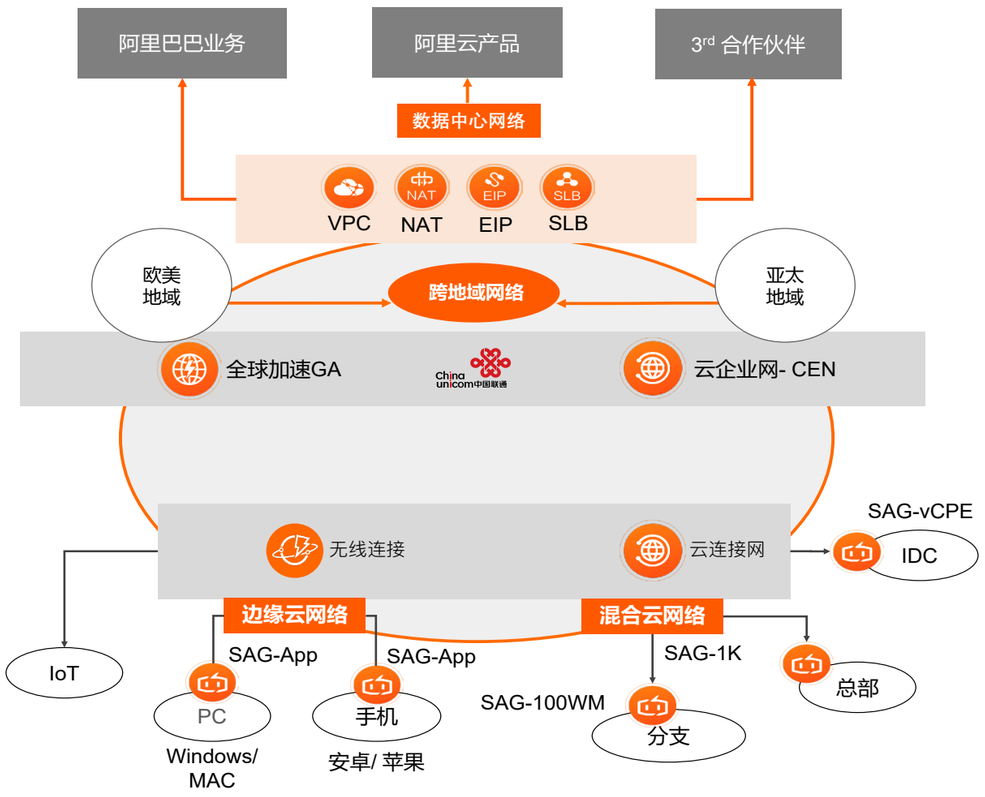
1 概述

网络的核心是提供连接能力，从用户角度，有连接需求的地方都希望网络能快速可达。在传统网络世界中，用户要提供或访问应用，涉及数据中心网络、广域网和接入网等不同网络之间的连通。其中数据中心网络更多是自建或者租用，广域网和接入网是通过运营商购买。云网络时代，因为虚拟化技术的应用，云上租户和应用可以一键式开通所有需要连接的网络，不再关心底层不同供应商和网络基础设施。随着云计算的深入，大量应用上云，而以云为中心的云网络，就需要连接万物，构成全球一张网，整个云网络的业务全景如图所示。

数据中心云网络关键业务能力要求包括几个方面：

多租户：这是云网络最基本的能力要求，租户内连接和租户间隔离，目前所有厂商的云网络目前都通过VPC产品提供这个能力。

大规模：这是从VPC数目角度来看的，云上租户数目可达百万级，这就要求每个地域容纳百万VPC数量，这是有别于传统数据中心网络和专有云网络的，非公有云的网络，网络之间的隔离更多是业务或者部门之间的隔离，规模非常有限。另外，VPC



是用户在云上的数据中心，单个VPC的容量规模也要求非常高，特别是在云原生兴起后，单VPC需要容纳几十万实例。

大带宽：数据中心内的网络主要承担的是应用内部东西向的流量，即服务器之间的流量，服务器带宽从GE、10GE、25GE逐步演进到100G，同时多租户共用，所以带宽是非常巨大的。

低时延：应用服务能力的提升，目前主要依赖横向分布式扩展，内部快速交互，对应用完成处理，快速响应至关重要，所以网络的时延要尽量低。特别是高性能计算的应用部署在云上之后，对时延的要求更加的极致。

跨地域网络关键业务能力要求包括几个方面：

从应用可靠性及就近服务的角度，很多应用会多地域部署。应用在不同地域之间也会存在通信，例如数据的备份和系统间调用等。这里的网络业务与数据中心网络存在一定的差异，一般称为跨地域网络，其业务能力要求会额外增加，如：

安全性：不同地域之间的网络会出IDC长途传输，要防止数据在传输过程中被窃听，造成泄密，所以跨地域网络的安全性要求更高。

QoS：跨地域网络由于建设成本的原因，资源相对较少，扩展能力弱，在链路拥塞的情况下，要有不同服务区分处理的能力，即QoS业务。

混合云网络关键业务能力要求包括几个方面：

企业上云是一个渐进过程，特别是企业自建数据中心已经运行后，企业上云的过程会呈现部分应用部署在云上，部分应用还在云下。企业的终端、分支机构等的访问通路也会发生变化，从访问自建数据中心，演进至访问云上弹性计算资源。在这种业务场景下，提供线下访问云上专有资源的网络，称为混合云云网络，其业务能力和其他类型的网络也有所不同。

高可靠：基本所有的网络都有高可靠的要求，但一般网络的高可靠都是通过设备集群以及设备内和设备间的多链路保证的，混合云网络的高可靠要求更多体现在两端的网络节点之间要建立多通道方式，并实现联动机制。

零配置：因为企业的端、分支机构等接入点数目往往较多，所以租户在连接上云的网络时，对配置的复杂度比较敏感，期望提供即插即用的能力。

2 云网络业务特征

云网络构建了一张虚拟的网络，为租户提供端到端的网络连通能力，相对于传统的企业网络，云网络伴随着云计算而产生，其业务的特征和传统网络也有非常大的差异，总结起来，包括几个方面：

❶ 自助

云网络和云计算一样，是一种自助业务。租户通过Web界面购买所需要的产品和服务，例如SLB、NAT等等。同时网络的配置、运维也是自助方式，网络的配置在Web界面上快速完成，通过配置云监控等服务，可以快速定位问题，一切都是DIY。租户在使用整个云网络产品的生命周期内，都是自助的，供应商只有一个，就是云服务商。

云网络自助的业务特征呈现的结果是租户和网络产品的界面为控制台和OpenAPI，区别于传统网络设备的CLI和网管接口，操作方式和对象模型都会产生相应的变化。

❷ 弹性

云网络另一个区别传统网络的业务特征是弹性。云网络面向的是海量的租户，网络规模提前静态规划的方式难以操作，同时每个租户面对剧烈变化的市场和业务，对云网络产品的规格要求也很难提前评估准确，这些都要求云网络具有更大的弹性。弹性的业务特征带来两个方面的业务要求：资源池容量以及调度管理。资源池足够大，面对突发的能力强，意味着拥有足够的弹性，但会带来成本的增加；资源池利用率足够高的情况下，同时满足弹性的要求，需要非常灵活的调度管理能力。

云常类比成一个超大规模的数据中心，超大规模即意味着有足够弹性的资源，弹性是租户对云的要求，也是云的一个业务特征，只有拥有足够的弹性，租户才会使用云。

❸ 按需

传统网络构建过程中，用户需要购买不同规格的网络设备，但受限于可选择的芯片范围，用户可见的规格范围也是有限的，同时由于新建成本比较高，所以购买的网络设备的能力一般都远大于业务所需。

云网络的购买分配方式有着根本的差异，可以做到按需分配和按量收费，使用多少量，付多少费用。租户可以按目前需要的规格购买，在业务量变化时，使用新的规

格。云网络的按需分配的特征，给租户带来非常大的便利性，让基础设施资源与业务规模完美匹配。

❹ 可计量

云网络从租户角度，购买的是服务，没有具体可见的网络设备，但可以完成网络的连接，从实体设备到虚拟方式，云网络的业务有一个重要的区别传统的特征是可计量。传统网络用户购买一个1Tbps的网关，就能得到1Tbps转发能力的网关设备，而云网络中租户购买1Tbps的网元实例，如何获取网元实例的运行情况，租户对购买的网元实例进行规格调整，或者调整成本更优的收费模式，云厂商如何收取费用，这些都要求云网络的业务具有可计量的能力，每一个能力项，每一个资源消耗项，都要通过技术手段，统计其用量，并且是动态实时的。

3 云网络技术特征

❶ 云网络技术演进

云网络依旧在快速发展中，回顾过去与展望未来，我们看到云网络在不同阶段为解决客户不同的核心问题采用了不同的关键技术。回顾阿里云的发展经历和技术演进，将云网络分为四个阶段，如下分别进行阐述。

1）云网络Beta(2009～2014)：云上传统网络

这个阶段，主要以中小站长和互联网中小企业为主，云计算的主要工作是将主机托管业务进行虚拟化。云计算对租户提供的网络服务主要是DNS，负载均衡，公网IP地址。由于从出租物理机升级为出租虚拟机，网络的主要变革是提供了虚拟交换机vSwitch，并支持虚拟机VM绑定公有IP地址。

严格来说，此时的云网络只能称之为Beata，租户间的安全隔离主要依赖安全组。

2）云网络1.0（2014～2016）：数据中心网络云化

这个阶段是企业上云的中期阶段，传统企业和互联网大用户开始上云，关键的业务诉求是为应用提供安全隔离的网络环境。其技术的主要特点是网络服务自动化，多租户云上VPC网络技术以及丰富的可计量的虚拟化网络功能。

云上VPC网络通过Overlay技术提供给租户一个安全隔离的VPC网络空间，不同VPC之间网络默认是不通的，这在路由层面解决了不同VPC的安全问题。在VPC网络里支持了虚拟路由器（vRouter），用户可以自己规划和定义自己的网络，比如私网地址CIDR，子网，路由等。

在VPC网络里除了连接VM的vSwitch，还包括了采用通用服务器构建的丰富可计量的虚拟化的云网关，用于处理各种不同的网络服务，比如EIP，SLB（负载均衡Server Load Balancer），NAT网关等，组成了数据中心云网络。

3）云网络2.0（2017～2019）：广域网络云化

随着企业上云加速，越来越多大型企业甚至全球化集团企业的应用在云上的部署，同时应用的微服务开发部署方式成为主流趋势，AI异构计算、基于VPC的HPC高性能计算也逐渐兴起。这些应用诉求对云网络提出的新的要求，这个阶段技术的主要特点是云网一体虚拟化技术、云原生的应用网络技术，高性能软硬一体网络、云原生的弹性高可用网络，同时对云网络的开放化和运营智能化提出了较高的要求。

云网一体从技术上来看是从云网络1.0的单Region的云上网络VPC虚拟化往云网络2.0云网一体虚拟化演进，云网一体覆盖了更广的范围。云网一体虚拟化包括两个部分，混合云网络虚拟化和跨地域网络虚拟化。混合云网络虚拟化是针对线下企业总部、分支、移动终端接入云上VPC的虚拟化技术，典型如SDWAN。跨地域网络虚拟化为不同地域的VPC网络以及线下IDC/分支（通过专线/SDWAN等接入）提供灵活的跨域互联互通能力，典型如阿里云提供的云企业网所采用的跨域Overlay技术。

云原生的应用网络技术是为了更好的满足应用的微服务开发部署方式。从网络支撑弹性计算的演进来看，由于业务的开发模式将越来越聚焦应用本身，应用开发逐渐往容

器、Kubernetes服务治理与编排、DevOps、Serverless等云原生技术方面发展。云网络也随之演进，从基于VM的云网络演进为支持云原生的应用网络。云原生的容器相对VM而言，密度提升了10多倍，而拉起速度的时间加快了10多倍，这对云网络也提出了更高的要求。

为企业提供高品质高性能的云网络是云提供商最朴素的诉求，随着服务器的网卡从1G/10G到25G/50G/100G，采用Host CPU实现的软件vSwitch在性能和零抖动方面的诉求无法得到满足，Host vSwitch逐渐开始卸载到智能网卡。同时网络带宽的诉求进一步增长，初期采用物理服务器DPDK构建的方式无以为继，采用可编程芯片构建的自研交换机成为解决基础网关定制化和性能问题的必由之路。而在AI异构计算、高性能分布式存储以及基于VPC的HPC高性能计算对VPC网络和基础网络在高性能和低时延提出了更高要求。

随着越来越多的丰富的企业上云场景，越来越多的增值类的网关被提供，这些增值类网关提供了更多灵活的高级特性，但如何快速弹性部署，更快的满足灵活多变的诉求，对云网络的开发实践也提出了更高的要求。增值类网关All on ECS的基于NFV平台的理念被逐渐实施，基于NFV平台的增值网关完全是基于云原生来进行开发实践，具有快速弹性扩缩、分布式架构、不可变基础设施等特点，充分利用了云的可用性、伸缩性、自动化部署等原生能力。

云的生态在这个阶段也逐渐完善，除了阿里巴巴经济体的基础设施提供服务，也有越来越多的合作伙伴基于云提供第三方服务能力。如何通过技术手段构建云网络生态，更好的连接服务使用方和提供方也对云网络的开放化提出了要求。

在这个阶段，云网络的规模越来越大，特性越来越丰富，为更好的满足客户诉求，交付速度也越来越迅速，但同时云网络又是整个云基础设施的底座，稳定性不言而喻。如何同时兼顾两者，这需要将传统基于工具+脚本的运营方式往基于数据的运营智能化转变。

4）云网络3.0（2020～）：应用-云-边一体，面向万物互联的网络

伴随行业发展，越来越多的业务希望在边缘完成计算，如AI推理，视频预处理等，分布式边缘云正在成为一种新的趋势。分布式边缘云相对中心云而言在更靠近用户的地方部署弹性计算资源，为用户提供更高处理带宽，更快响应时延，获得更好的用户体验。在5G兴起后，5G的核心能力，即大带宽/低时延/大连接也必将更进一步驱动分布式边缘云的发展。这个阶段的技术特点是边缘云的轻量化和小型化，同时通过云边一体的协同技术，构建万物互联的网络。

对网络而言，通过云边网络一体，通过中心云VPC延伸到边缘云，比如VPC的一些子网可以在中心云，而另一些子网可以在边缘云，这种原生VPC延伸的技术对用户同时管理和使用中心和边缘的弹性计算资源具有更好的使用体验。同时边缘云可以基于不同诉求可以连接公网，专线以及网络的各种高阶服务等，满足边缘上丰富的业务诉求。

❷ 云网络技术特征

上文介绍了云网络在不同阶段的技术演进，云网络在技术与业务的双轮驱动下，呈现网络虚拟化、云原生化、网络服务自动化、高性能、开放化、基于数据的运营智能化这些技术特征。

1）网络虚拟化

云网络通过网络虚拟化技术构建了数据中心云网络、混合云网络、跨地域网络三大架构，在这三大架构中也体现了不同的网络虚拟化技术。

在数据中心网络虚拟化方面，通过基于Host Overlay虚拟化技术构建了安全隔离的VPC网络。基于Host Overlay构建的云网络架构跟物理网络解耦，充分利用了Host的灵活性和物理网络的大带宽管道能力，两者独立演进。如Host的灵活性体现如安全组、flowlog流日志、多级限速、子网路由等灵活的功能上。

跨地域网络通过Overlay技术在云服务商的核心网构建，相对于单Region的云上VPC网络而言，云企业网是全球属性的，云企业网在和VPC、专线/SD-WAN的协同以及在跨域路由计算和传递等方面做了大量的工作，这种跨域的云网络为企业全球化提供了极强的基础设施能力。

混合云网络的虚拟化需要解决众多分支和移动端接入云中的许多复杂的问题，比如简化部署和维护的诉求，海量接入质量和成本的权衡，更好的无缝访问云中的各种服务等。混合云网络针对云的特点做了大量技术创新和融合，更好的解决企业分支和移动端上云的诉求。

2）云原生化

云网络除了基础网元，如公网网关、专线网关、主机AVS（Apasra vSwitch），种类更多的是增值网元，比如NAT网关、4/7层Load Balancer，PrivateLink等。相对基础网元而言，增值网元对用户提供了更多增值的、高级的特性，随着越来越多的丰富的企业上云场景，不同客户可以灵活选择不同的增值网元。增值网元在云网络初期通常采用物理服务器方式部署，但是随着增值网元类型逐渐增多，面临采用物理服务器扩容不方便，无法灵活弹性扩展，同时随着物理服务器机型演进，增值网元也要跟随适配导致大量人力浪费。阿里云网络采用基于云原生的设计理念构建NFV平台作为应对之道，NFV平台采用普通的ECS安装部署所需的增值网元，利用云上的ECS按需申请、弹性伸缩的能力，进行弹性部署。

3）服务自动化

相对于传统网络通过命令行来配置网络设备，云网络通过自动化的网络服务方式提供。云网络是一张构建在物理网络之上的虚拟网络，通过云化的技术实现传统网络的各个网元，如路由器、交换机、防火墙、Load Balancer等。云上的网络服务本质是一种从买设备到买服务的转变，云网络也可称之为云服务和网络的一体化，通过服务的方式提供网络的能力给用户。

4）高性能

云网络的高性能体现在多个方面，包括云网络底层资源能力，基础网关硬件化和智能网卡，高性能低时延网络。

在底层资源能力方面，服务器接入带宽从1Gbps、10Gbps、25Gbps向50G/100G演进，而交换机之间互联带宽从10Gbps、40Gbps到100Gbps，向200G/400G/800G演进。除此之外，还有高性能公网带宽等。

在基础网关硬件化和智能网卡方面，云网络基础网元通常指在VPC边界或者跟物理网络交界的网元，比如VPC网关、公网网关、专线网关等，这类网关最大的特点通常是企业上云必备的，随着企业上云越来越广泛，网络带宽进一步增长，初期采用物理服务器DPDK构建的方式无以为继，一方面服务器的摩尔定律已经失效，需要更多服务器来满足不断增加的流量诉求，另一个方面对安装部署/交付运维/成本/功耗等也带来了不利影响。而采用可编程硬件芯片可有效面对不断增加的流量诉求，从单台服务器100G到当前可编程单芯片3.2T/6.4T，下一代12.8T，转发能力提升数十倍，转发时延更低，基础网元硬件化是必然选择。

在高性能低时延网络方面，随着数据爆发式的增长，人工智能、高性能计算、分布式存储等逐步开始普及和应用。传统基于CPU软件进行网络通信的模式已经无法满足这些业务诉求，同时以GPU深度学习替代CPU为代表的异构计算，以高性能NVMe存储介质替代机械硬盘的分布式存储，对网络的性能和时延也提出了更高的要求，网络逐渐变成计算和存储的I/O总线。随着高速以太网的发展，阿里云通过构建基于RDMA(Remote Direct Memory Access)的高性能网络满足新的业务诉求。RDMA是一种keneral bypass技术，通过软硬件结合的方式将网络传输协议固化于硬件，通过内核旁路实现了CPU卸载和零拷贝，RDMA显著提升了网络通信效率，降低了应用的处理延迟。

5）开放化

随着企业上云的步骤逐渐加快，一个以云为中心的新数字经济的时代正在到来。数字经济驱动着各行各业的转型和发展，越来越多的ISV、科技类服务公司将转型到云计算的业务上来，这些生态的变化必将重构整个云的服务体系。云生态的繁荣，依赖大量第三方生态伙伴的参与，一个开放的生态友好的云，才能更好地赋能千行百业。因此，更好的支撑第三方的网络产品在云上的部署，为第三方网络产品更好的开放云原生的能力，如多租户、弹性扩缩、可靠性等，就是云网络开放化的要求。

6）运营智能化

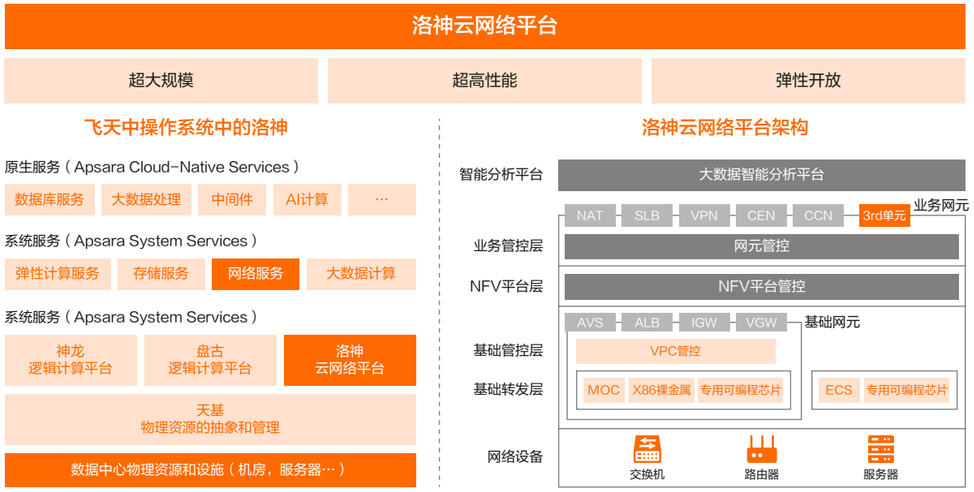
随着越来越多的业务上云，云网络作为整个云的基础设施越来越重要，如何运营好云网络是一个巨大的挑战，这种挑战来自于两个方面。

一是云网络的复杂性，云网络为用户提供了几十款产品，又是计算、存储、数据库等其它两百多个云产品的基础设施，每天新的场景、业务、特性不停的注入云网络中，云网络的升级有时候就像给飞行中的飞机换引擎，极其复杂，风险极大。二是超大规模带来的故障概率，阿里云上的用户已经数百万，各种服务器和网络相关设备也早已超过了一百万台，虚拟机数量更是上千万计，这些数字还在不断快速增长。量变引起质变，单台设备发生的小概率故障事件放在大型的公有云中发生故障必然是一个大概率事件。在这么大规模下，如何及时发现问题，如何及时将流量快速切换到安全的网络设备，如何更新维护这么大设备量的云网络，这是面临的另一个巨大挑战。

解决云网络复杂的特性和超大规模带来的挑战需要我们转变思维，传统基于脚本和工具来做监控和问题定位已经远远无法满足要求，例如100万台网络设备的数百种监控指标用脚本工具完全无法胜任，同时网络业务的用户、产品、资源等多维度的分析，传统工具更无法处理。因此，运营智能化就是必由之路。

4 洛神云网络技术

洛神是阿里云飞天（Apsara）云操作系统的核心组件，负责对用户提供丰富的产品和服务，同时也是云网络基础技术平台，称之为洛神云网络平台。



洛神云网络平台聚焦业务和技术需求，历经多年演进，当前主要有四大关键技术，一是网络虚拟化技术，二是高性能转发技术，三是云原生NFV技术，四是SDN控制器技术。

❶ 网络虚拟化技术

网络虚拟化指在物理网络上通过网络虚拟化技术可以构建出多个逻辑网络，使得不同用户或者不同部门在同一张物理网络上可以使用独立的逻辑网络资源，从而提高网络的利用率。在云计算出现之前，网络虚拟化技术就广泛存在和部署，典型代表如VLAN技术，MPLS VPN 技术等。而在云计算发展过程中，之前存在的网络虚拟化技术无法很好的满足云网络的诉求，如传统的VLAN技术只有12bits，最多表示4K租户，无法满足云网络海量租户的诉求，而MPLS VPN技术在数据中心内网部署又太复杂，同时云计算厂商希望独立提供云计算完整解决方案，而不受制于物理网络的约束，这些因素促成了新的网络虚拟化Overlay技术。

Overlay技术是指将原始报文封装到UDP报文（即L2 over L4）中，并在L3网络中传输，本质是一种隧道技术，比较常见的网络虚拟化overlay技术有VxLAN、NvGRE、STT等。当前较为主流的技术是VxLAN技术，阿里云网络也采用了类VxLAN技术的方案。VxLAN技术在原始报文跟外层隧道UDP之后有一个VxLAN头部，包含了24bits的VNI字段，这个字段可用于标示逻辑网络，数目可以达到1600万，可以较好的满足云网络对多租户的诉求。

1）数据中心网络虚拟化技术

在云数据中心网络里，虽然传统网络厂商和云厂商都采用Overlay技术，但是具体实现方案上有较大差别，主要包括硬件Overlay 和 Host Overlay两种方案。

硬件 Overlay 技术方案

为了满足云数据中心网络虚拟化的隔离需求，传统网络设备商提供了VxLAN隧道端点在硬件设备上实现的方案，虚拟化主机通过VLAN进行本地多租户隔离，在接入交换机上进行VLAN和VxLAN的映射转换，在核心层仅需完成IP转发（对东西向流量）。这种方案和传统网络模型较为接近，部署运维上变化较小，但由于受限于交换机的转发和封装规格资源限制，该方案只适合中型数据中心，无法满足公有云大规模应用诉求。另外虚拟网络特性发布仍受限于硬件开发周期，对云上网络的高级特性如安全组、子网路由无法较好支持，因此目前仅存在于一些特性要求较为简单的私有云解决方案中。

Host Overlay 技术方案

Host Overlay指在Hypervisor上部署虚拟化交换软件，控制器将租户VxLAN转发配置下发到虚拟交换机上，在Host上软件交换机完成VxLAN隧道端点的封装和解封，从而完成虚拟机之间、虚拟机到边界网络的流量转发。这种实现方式对物理网络仅仅需要IP可达即可，而不再受制于物理交换机支持Overlay特性的规格限制。同时基于Host技术方案实现的Overlay相比于硬件Overlay技术方案而言更加灵活，很好的

满足在硬件交换机上较难实现的安全组、flowlog、子网路由等特性。

2）跨地域网络虚拟化技术

跨地域网络云企业网CEN用于实现租户跨地域VPC/CCN/专线之间的互联互通。跨地域网络虚拟化同样采用Overlay技术构建。阿里云在每个Region部署了TR（Transit Router）网关，通过Overlay技术按需在不同Region的TR网关间建立VxLAN隧道。在TR网关的接入侧，需要将VPC/CCN/专线的租户标示统一转换到跨地域网络虚拟化Overlay的统一标识。TR网关可实现租户流量的地址隔离，QoS标签，安全加密等能力。

3）混合云网络虚拟化技术

云连接网CCN（Cloud Connect Network）提供企业分支/移动端快速且高质量的上云连接。通过将CPE设备智能接入网关SAG（Smart Access Gateway）上的物理连接、云网络遍布全球的网络接入点，以及将这些接入点联通的Internet网络/核心网络资源池化，通过Overlay技术和SD-WAN探测选路技术结合起来构建基于租户的混合云网络，它兼具云的弹性、高质量，以及海量的连接能力。用户的业务可以平滑地在云上网络和云下网络之间进行业务的迁移，同时企业分支/移动端能从SD-WAN网络的任何位置发起对云上IaaS资源、SaaS应用的访问。 智能接入网关SAG是云网络Overlay技术概念从数据中心走向企业接入上云领域的延伸。通过SAG Overlay网络可以避免对传统物理基础设施的巨大改造，保护现有投资。

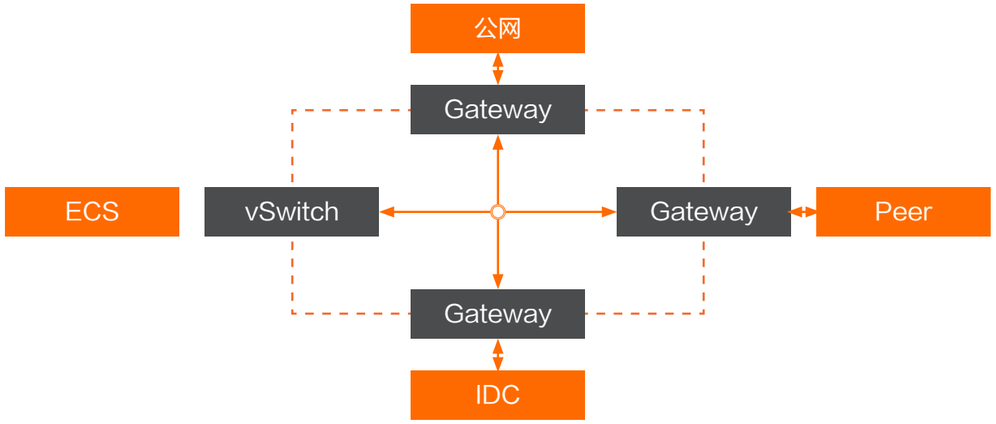
❷ 高性能转发技术

在云网络技术特征章节，着重分析了云网络对高性能的需求，分析了才有软硬件一体化技术提升性能的必要性，下面重点分析基础网关软硬一体化技术。

1）软硬一体化概览

云网络的基础转发组件包括两部分：云网关Gateway和虚拟转发交换机

vSwitch。云网关Gateway负责公网和专线和跨Region流量的汇聚和分发。vSwitch是服务器内部网络核心组件，负责服务器内部ECS流量的转发和交换。Gateway和vSwitch一起为客户搭建一张虚拟专用网络。



纵观网络发展史，网络设备的演进始终呈螺旋式发展态势，围绕着灵活性和高性能，软件和硬件在相互融合、相互促进。从最开始的硬件转发设备，到软件转发设备，再到硬件卸载的软硬一体化转发设备以及大行其道的可编程转发设备。灵活性和高性能就像一只无形的手，引导着技术的持续发展。

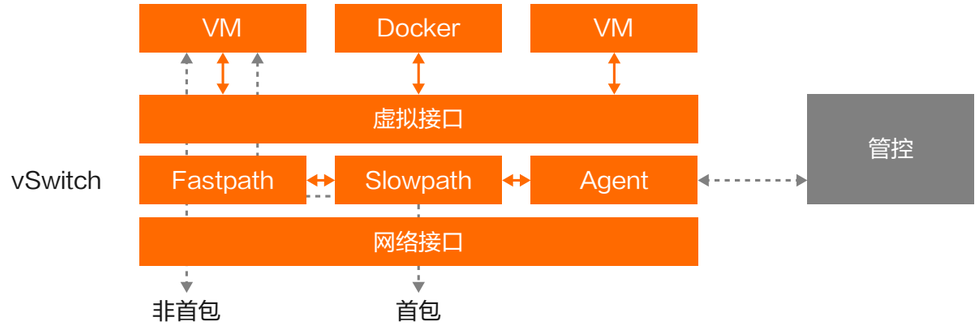
物理网络经过几十年的发展，接口和协议相对标准和成熟，所以物理网络的各类交换机基本都是基于Switch芯片（其中大部分是Broadcom的）做硬转发。云网络的发展是这几年的事，业务和需求都在快速变化中，缺乏行业标准，各云厂商都是在按需做定制，所以云网络的各类业务大多是基于CPU做软转发。软转发具有更高的灵活性，但在性能上面会有不小的损失。随着云上业务对性能的要求越来越高，性能瓶颈越发突出。为解决这个问题，诞生了各种各样的软转发技术，比如快慢速分离架构，DPDK用户态转发技术等。

DPDK是Intel针对x86开发的数据面优化技术，作为一个开源软件，DPDK也可以用于其他的CPU架构，比如ARM和Power。DPDK运行在用户态，通过大页 / 轮询 / CPU亲和性等技术，达到减少内存拷贝 / 减少cache miss / 减少中断调用 / 减少

进程和线程切换等优化目标，进而实现CPU软转发的性能优化。DPDK出现之后，基于x86的转发从内核态迁移到用户态，性能有了大幅提升。但随着海量业务迁移上云，基于CPU的软转发面临新的问题。一是CPU的单core性能瓶颈，在大流和攻击场景下比较容易被打满，导致丢包故障；二是CPU的摩尔定律逐步失效，CPU的频率和核数提升空间越来越小，靠CPU软转做进一步性能提升的空间有限。而与之相反，以太网的接口速率正在飞速发展中，25G NRZ已经普及，50G PAM4已经成熟，单模块400G已经成为现实。PCIE的接口速率也在快速发展中，单lane 16Gb的PCIE Gen4即将规模上线，单lane 32Gb的PCIE Gen5的规范已经发布。云网络的流量出现了爆发式增长，游戏 / 视频 / NFV化对ECS网络性能提出了更高的要求，vSwitch的网络正在朝百Gbps迈进。混合云的发展带来了专线和跨Region流量的激增，Gateway的流量正在朝百Tbps迈进。为了提升云网络的性能和稳定性，满足云计算技术和业务发展需求，对VPC的基础组件做了全链路的软硬一体化升级成为必然选择。

2）vSwitch软硬一体化

vSwitch的承载实体是ECS云主机， vSwitch负责云主机内VM / Docker/GPU的网络接口和网络功能。



vSwitch的功能和云厂商的业务相关，各个云厂商会根据自己的业务特性进行设计开发。vSwitch的指标主要包括bps / pps / 时延/新建等，这些对客户体验有直接影响。vSwitch 性能和下面几个组件相关：

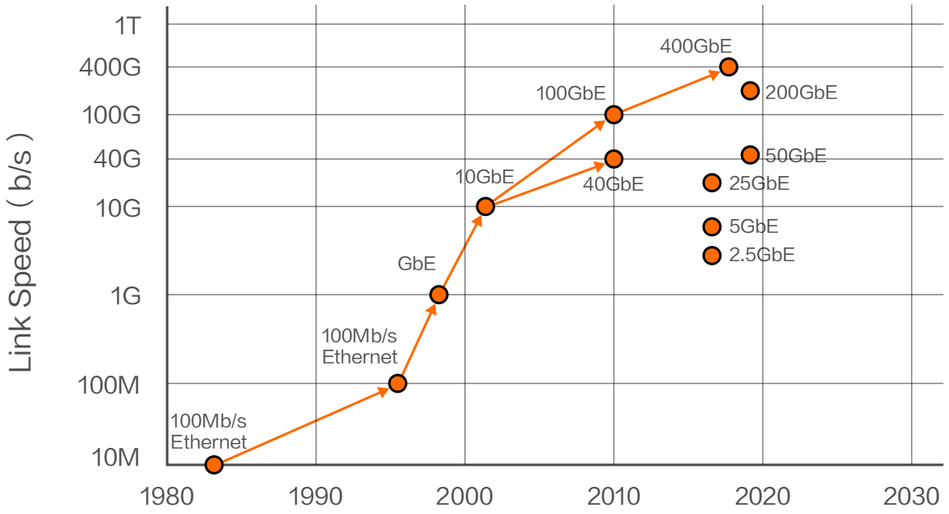
物理网卡接口：目前主流是25G，正在朝100G演进

虚拟网卡接口：可以采用半虚拟化接口或全虚拟化接口

Slowpath：基于route / ACL和业务逻辑决定转发行为

Fastpath：基于slowpath生成的session做match / action

下面简单介绍下网卡接口。以太网接口速率正处于加速发展阶段，400GE已经成为现实。



PCIE也处于快速发展中，PCIE Gen5的version 0.9标准已于2019年1月发布。

	发布时间	单lane速率	x8 lane速率	x16 lane速率
PCIE Gen3	2010年	8Gb	64Gb	128Gb
PCIE Gen4	2017年	16Gb	128Gb	256Gb
PCIE Gen5	2019年	32Gb	256Gb	512Gb

ECS网卡的主流目前是2*25G+PCIE Gen3*8，随着Intel的CPU从PCIE Gen3加速驶入PCIE Gen4/5，ECS网卡正在逐步迁移到2*100G。 虚拟接口分为半虚拟化接口或全虚拟化接口。

	典型接口	Guest Driver	热迁移	时延/抖动
半虚拟化	Virtio	通用性好	断流时间短	相对大些
全虚拟化	SRIOV	通用性稍差	断流时间稍长	相对小些

Virtio对运维更友好一些，guest driver适配工作量小，热迁移方案成熟。而SRIOV在性能上略胜一筹，对游戏 / 视频 / NFV等性能敏感型应用较适合。技术发展的趋势是取长补短 / 相互融合，这点在2018年发布的Virtio 1.1里得到了很好的体现。Virtio 1.1把Virtio1.0的Available/Used/Descriptor三个ring合为一个，一方面提升了转发性能，另一方面也更便于硬件实现。Virtio预计会从0.95/1.0逐步演进到1.1，但由于涉及前后端的生态配合，也不会一蹴而就。

3）Gateway软硬一体化

云网关Gateway是云网络流量入口，也是云网络带宽压力和稳定性压力最大的一环。Gateway的流量包括公网流量，专线流量，跨Region VPC互联流量。 和云网络的其他组件一样，Gateway也是从x86软转开始的。由于Gateway的性能要求较高，阿里云的Gateway直接跳过kernel，第一天就开始使用DPDK平台，全自研网关软件。和其他基于x86+DPDK做软转发的云网络产品一样，Gateway的问题也是CPU存在单核性能瓶颈，在大流量和攻击流量场景下CPU可能会被打满，引起故障。随着大型企业上云增加，专线流量出现了数量级的增长，达到数十Tbps。Gateway作为云网络的流量入口，面临的性能和稳定性迫切需要优化。

可编程交换芯片的出现。

物理网络经过几十年的发展，接口和协议相对标准和成熟。物理网络通常是基于switch芯片做硬转发的。在Barefoot的Tofino出现之前，交换芯片的数据面对客户是

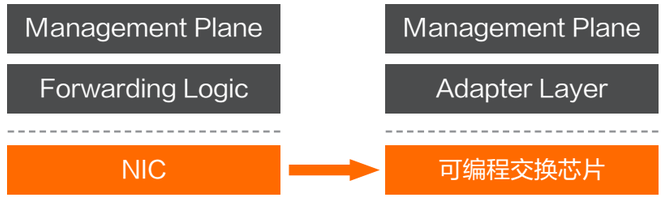
固定的pipeline。Network OS可以修改交换芯片的table和register，但无法修改转发pipeline。

云网络由于业务和需求变化快，没有业界通用标准，方案基本都是按需做定制。固定pipeline的交换芯片，数据面没法满足云网络的定制需求，基本用不上。Barefoot的Tofino是业界第一款基于Protocol Independent Switch Architecture，支持客户可编程的switch芯片。Tofino的Parser和Match/Action都是通用的，转发逻辑是客户可定制的，表项资源是动态可分配的，支持灵活的转发组合。

Tofino的转发面编程语言是P4，基本成为了行业标准。除了Tofino，一些网卡芯片（比如Pensando）也开始支持基于P4的转发编程。P4有点类似Verilog，都是对硬件做编排，但抽象层次更高。

阿里云软硬一体Gateway。

可编程交换芯片的出现给云网络打开了一扇窗，让Gateway硬件化成为可能。为应对超大流量的挑战，云网络基于可编程交换芯片的Gateway设计，成功实现了Gateway的软硬结合设计。



通过可交换芯片的加速，Gateway单机bps性能提升20倍，单机pps性能提升80倍，延时降低25倍，集群能力提升5倍，整体Capex和Opex大幅降低。硬件网关的业务价值可以归结为以下几个方面：

大流量：比如阿里双十一 / 大客户数Tbps～数十Tbps的上云流量。

大单流：比如IoT场景的GRE tunnel，单流数Gbps～数十Gbps。

稳定性：没有软转发的CPU打满隐患。

低延时 / 低抖动：硬件网关的管道足够粗，客户上云丝般柔滑，没有卡顿，就像高速公路的车道足够多，车辆行驶一路通畅，没有排队 / 没有阻塞。

❸ 云原生NFV技术

云网络是由各种网元（Network Element）组成的，例如交换机、路由器、NAT网关、负载均衡等，这些网元在云网络中通常称为虚拟化网元。一方面是因为这些网元提供了多租户的能力，即一个物理上的网元，提供给多个租户共用，而不是每个租户独立一个网元，对于每个租户而言，是一个虚拟化的网元实例；同时云网络的4～7层协议处理网元普遍使用NFV技术，相对于传统专用的硬件方式的网络设备，技术上差异也非常大，通过软件虚拟方式实现各种网元的业务，所以云网络中的网元也被称为虚拟化网元。

NFV技术概念

NFV全称Network Function Virtualization，是网络功能虚拟化的意思，是一种新的实现网络转发的技术。传统的网络设备内部架构如图所示：

传统网络设备内部架构通常包括三个平面：管理面、控制面、数据面。

管理面，用于对接用户操作，包括CLI、Netconf、SNMP等人机和机机交互的接口，处理用户或者网管下发的配置，例如对设备的配置和对协议的配置等。

控制面，又称为协议处理面，是网络设备的核心平面，主要处理各种网络协议。不同种类的设备控制面的功能也不同，例如交换机的控制面支持更加丰富的二层协

议，路由器的控制面中路由功能更完整。网络中不同网元之间的控制面进行交互，生成相应的转发表项，指导数据面的转发。

数据面，网络设备的执行单元，由控制面下发转发表项，例如二层MAC、三层路由表，数据面根据这些表项，将网络中的数据正确的转发至目的地。数据面强调性能，所以传统网络设备的数据面使用专用芯片，定制网络报文转发逻辑，目前单芯片业界最高已经达到12.8Tbps。

从传统网络设备的架构可以看出，其核心特点是标准和性能，通过网元之间标准的协议交互，生成转发表项，下发给高性能的数据转发芯片。传统网络设备三平面架构非常经典，指导了传统网络几十年的快速发展。为什么不能直接将传统设备直接复用到云网络中呢？面向云网络的业务要求，传统设备存在几方面的不满足点：

敏捷性。传统网络设备需要兼顾协议标准，满足异构厂商在同一个网络中应用的要求，同时要兼顾各种场景的应用，要支持非常全面的协议，开发周期往往比较长。另外因为数据面使用专用芯片，追求极致的转发性能，取舍了灵活性，新功能的增加，一旦涉及芯片转发逻辑变化，需要下一代芯片才能支持，目前至少需要18个月的周期。

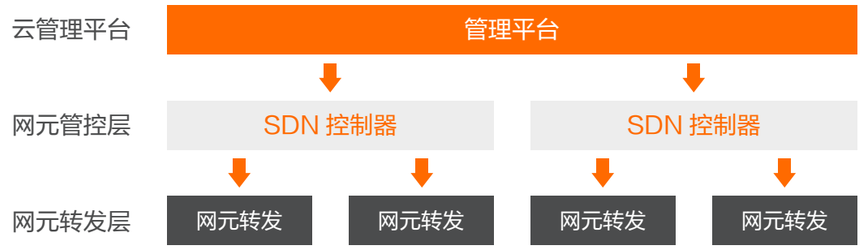
开放性。传统网络设备三平面都是垂直集成的，为了运行效率和运维效率最高，内部都是封闭系统。用户只能通过设备开放的接口，进行有限的定制服务，且不能超过设备控制面和数据面提供的能力。

规模。不管是企业网络，还是电信网络，由于分区分域以及单个用户规模的原因，网络的规模相对有限，所以控制面协议的设计以及数据面芯片表项空间的设计，都是只匹配其应用场景的规模。

这些挑战，在以云为中心的新一代网络演进中，需要快速解决，触发了网络功能虚拟化NFV技术的应用。NFV技术的核心是使用通用X86　CPU作为网络数据面转发组件，通过自定义的软件编码，实现业务的快速敏捷迭代能力、开放能力和快速横向

扩展能力。目前主要应用在两大领域中，且具体实现方式有所不同。

云网络的4~7层协议网元实现普遍应用NFV技术，最核心的原因是业务的快速迭代。企业上云后，不管是对外提供服务，还是访问内部、外部服务，网络的连通性要求没有减少，还可能因为上云的要求，网络的需求反而更多，这些网络能力需要云厂商快速提供，所以网络功能的快速迭代是最关键，最核心的。使用封闭的、标准的传统设备厂商提供的网络设备，无法满足云网络的要求，另外专用芯片因为芯片规格、内部逻辑固化等原因，灵活性也达不到云网络的要求，所以云厂商的网络最终选择NFV技术，通过软件虚拟化的方式快速提供云上租户网络功能。云网络在使用NFV技术构建各种虚拟化网元的时候，也有清晰的架构分层，如图所示：



云网络NFV网元的架构实现包括三层，网元转发层、网元管控层以及云管理平台。

网元转发层，提供网元数据面功能，基于通用CPU（X86/ARM等），使用软件编程方式，完成网络数据报文的转发。对于云网络而言，要提供海量租户隔离和复用的能力，所以网元转发面，普遍使用VxLAN或者NVGRE等隧道技术，不同的隧道代表不同租户的网络，是一种虚拟的网络。

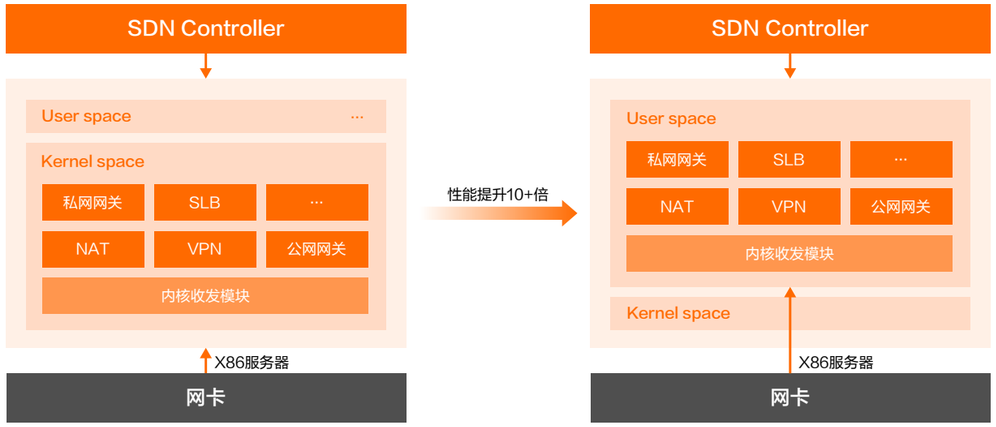
网元管控层，提供网元数据面转发的表项，对应传统网络设备控制面功能，但这也是差异最大的一个组件。传统网络设备的控制面是实现标准的网络协议，通过不同网元之间的分布式协议交互，达到网络内数据同步的目的，再经过本地计算，下发至数据面，指导数据面的转发。云网络的管控层，独立于网元转发面，不运行传统的标准网络协议，而是各个网元的控制面集中处理，生成转发表项后，统一下发至数据面，通过简化分布式系统处理的复杂度，提供快速灵活的业务处理能力。

云管理平台，提供网元编排、鉴权和计费等功能，管理租户不同网元的配置以及启动、删除等生命周期事件，这些配置和事件下发至管控层，刷新对应网元的转发表项，最终展现为不同的网络连接能力。

云网络网元的每一层组件都是自研的，不涉及多厂商之间的互联互通，不需要对外定义标准，所以接口和内部的协议都是私有的，这是与电信网元NFV技术非常大的差异。另外在网络规模上，云网络的网元数目要远大于电信网络，且租户对网络流量的突发需求变化大，所以规模和弹性的要求更高。

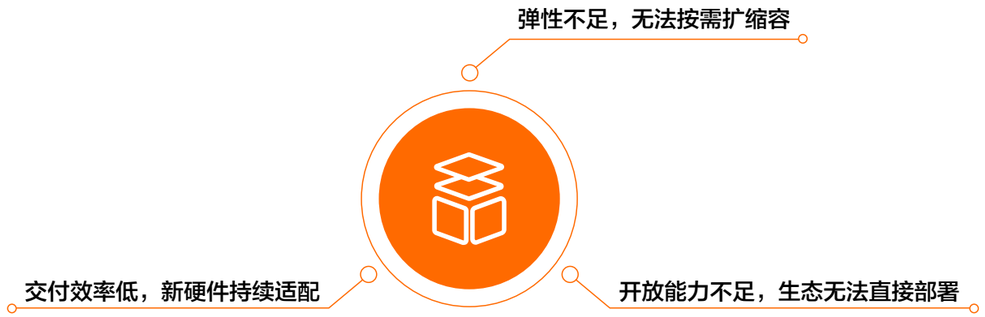
传统云网络NFV技术的约束

云网络NFV技术核心组件主要包括网元转发层、网元管控层以及云管理平台，其中核心的转发层，已经经过两代架构的演进，如下图所示。



因为Linux内核提供了网络转发能力，所以最早构建云网络NFV网元的时候，最快捷的方式，就是直接使用Linux内核的网络能力，例如负载均衡LVS就提供了内核版本。使用Linux内核方式的NFV技术路线优点是快速可获得，缺点也同样明显，即性能不足。当DPDK技术出现后，网元NFV技术快速演进到第二代，即基于X86裸金属服务器和DPDK软转发的NFV技术，相同硬件条件下，性能有10倍以上的提升，再叠加

横向扩展能力，可以满足云网络对转发性能的需求，这也是目前主流的应用方式。但随着云业务的持续发展，租户规模的持续增加，业务场景的持续变化，基于x86裸金属方式的NFV网元架构的一些约束逐渐暴露出来，总结起来主要有三个方面：



弹性能力不足。x86服务器的上线周期通常以月为单位，无法满足一些突发的业务需求，例如云上有一些租户在特定时间业务促销时，对网元规格的突发需求。当然云服务商也可以建立一个足够大的资源池应对业务突发，这样就会导致成本过高。按需随时资源获取是云计算的核心特征，对应到云网络的产品和技术，就是要提供足够强的网元弹性能力，在实现云网络NFV方式网元时，固定裸金属资源池的方式，显然非长久之计。

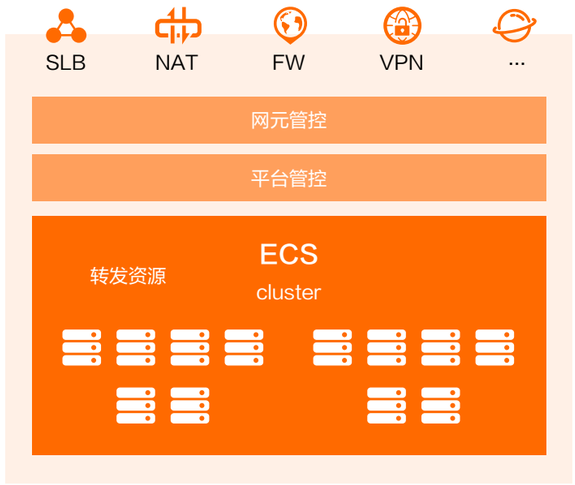
交付效率低。新服务器型号要新适配，特别是在专有云场景，客户服务器类型多种多样，适配工作量也会线性增加。

开放性不足。因为直接接入底层物理网络，和基础实施层的网络连通，地址管理和安全要求，使裸金属服务器上无法直接安装生态伙伴的网络镜像。

新一代云网络NFV技术

传统业务基础设施在弹性、交付效率、开放性等方面，也经历过能力不足的阶段，解决的方式是上云，使用云计算提供的能力重新构建企业的业务，所以云网络的NFV技术继续演进的方向是基于云原生技术的优化，让虚拟化的网元基于云上的资源构建。

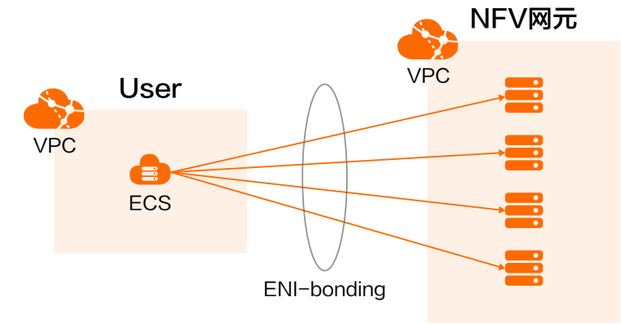
新一代的云网络NFV技术，其最大的特点是NFV网元不再直接部署在裸金属服务器或专用计算资源池内，而是基于云上通用虚拟实例ECS部署，ECS是面向所有云租户的产品，是相对海量资源，可以做到按需随时购买。



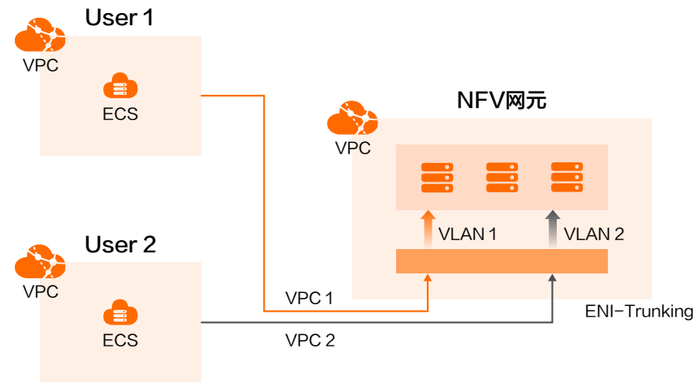
基于云原生技术，通过云上虚拟ECS实例构建云网络的NFV网元，不是简单的改变部署形式就可以支持，这里关键的技术点是如何在虚拟网络里面提供虚拟网络功能。云上每个租户的地址空间是相互隔离的，部署在独立空间内的云网络NFV网元，如何实现和其他租户地址空间的连接，如何能获取到不同租户信息，提供多租户共享和隔离的能力，这是新一代的云网络NFV平台要提供的能力。

云网络NFV网元基于虚拟ECS实例构建，部署在独立的VPC内，通过NFV ECS挂租户弹性网卡的方式实现跟租户VPC ECS的连通。同时为支持NFV ECS弹性扩展和负载均衡的能力，提升转发规格和可靠性，阿里云网络采用ENI-bonding技术，使用标准云原生网络对象，提供基于云上租户ECS跟NFV网元的的网络连通性，如图所示。

NFV网元是面向所有租户的，要提供多租户的能力，传统的NFV网元通过VxLAN隧道中的VNI信息识别不同租户，但演进到新一代NFV架构，基于虚拟ECS实



例部署，普通ECS只收发标准的以太报文，如何支持不同租户的流量识别。阿里云网络采用ENI-Trunking技术用于解决该场景的问题，如图所示。



不同用户的流量在转发至NFV网元时，会打上不同的VLAN TAG，标识不同的用户，服务网元根据不同的VLAN TAG执行不同的处理，从而实现多租户服务能力。

云网络NFV技术，在提供云计算虚拟网络的同时，也开始基于云原生的能力提升NFV网元自身的能力，NFV网元可以使用不同规格的ECS，提供不同类型的网元，例如七层负载均衡计算能力的要求更高，可以选择计算型ECS，而四层负载均衡对转发吞吐的要求更高，可以选择网络型ECS；

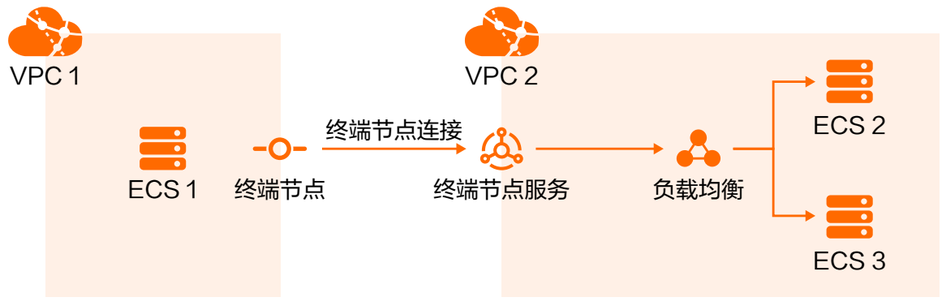
网络NFV技术的开放能力

基于云原生的能力构建的NFV平台，可以利用云计算资源池化、弹性、高可靠等

优势，重构云网络中的虚拟化网元。另一方面，基于新的NFV平台，可以提供非云厂商自身的第三方网元接入。从使用方式的差异，第三方网元的接入包括两种方式：

一是第三方网元接入通用产品服务，为云上租户提供服务

第三方网元集中部署，给云上租户提供服务访问，关键是不同VPC的租户的接入访问控制以及服务的弹性扩展。目前云厂商普遍提供这种场景下的产品服务，例如阿里云提供基于内网连接服务使用方和服务提供方的Privatelink产品。



第三方网元将镜像直接部署在负载均衡后面的ECS中，由Privatelink的终端节点接入用户访问请求，再通过终端节点服务和负载均衡，选择其中的一个节点提供请求应答。这种方式，一般提供4/7层服务接入，同时服务提供方需要管理虚拟机资源。

二是第三方网元基于原子能力，为云上租户提供服务

第三方网元提供路由类型的服务，不需要经过传统4/7层负载均衡，可以直接基于VPC提供的ENI-bonding和ENI-trunking技术为云上不同VPC的租户提供访问。由于第三方网元是基于VPC原子能力，需要管理资源的生命周期，包括健康检查、故障隔离/恢复、水位管理等，对综合技术能力的要求比较高。

新一代的NFV平台，不管是原子技术，还是产品化能力，都提供了生态部署服务化的能力，是直接传统裸金属x86服务器的NFV平台所不具有的，大大丰富了云上产品的丰富度，提供给用户更多的选择。

4 SDN控制器技术

SDN(Software-defined Networking)是一种新型的网络架构模型，由单独的网元组网重构为控制器和网元的方式，其核心设计理念是利用控制器集中管控、网络可编程以及IT技术来软化网络，其核心目的是通过SDN架构快速部署业务，缩短上线业务时间，以及满足新的场景如集中算路和网络路径调优等诉求。SDN并不意味着狭义上的基于openflow技术的转控分离，我们更多关注和实践SDN的设计理念和其达到的目的。SDN控制器核心功能是对转发设备屏蔽了业务的复杂性，使得应用开发专注于业务功能开发，而不用关心底层设备的信息。

云网络SDN控制器架构包括三层，北向API接口层，控制层，南向下发层。北向API层主要负责对上层应用开放API接口，上层应用通过调用北向的API接口完成网络资源的配置以达到实现应用业务需求的目的。控制层主要负责对北向的网络业务请求分解成原子的二三层网络服务对象，并转换成网络设备理解的配置下发到网络设备上。同时SDN控制器还包括库存管理，设备管理，链路监控等通用模块。云网络SDN控制器提供了多种类型的SDN控制器，满足不同的业务场景需求。下面简单介绍下VPC控制器。

VPC控制器面临的挑战

规模和弹性是云网络两个核心竞争力体现，对VPC控制器而言，这两方面挑战尤为突出。

超大规模的挑战。规模问题主要体现在两方面，一是单区域承载百万租户，不同租户的业务特性不一样，需要做到业务流量合理调度才能避免相互干扰，同时转发设备资源受限，需要做到配置的水平分割能力。二是单租户支持百万服务器，大客户上云给云网络带来的主要变化是单VPC的规模非常大，由于同VPC内服务器处于同一网络域，当VPC内路由或者网络拓扑变化时会有广播效应，可能导致配置变化广播到几十万台转发设备上，这给SDN控制器的配置下发以及及时生效带来了很大的挑战。

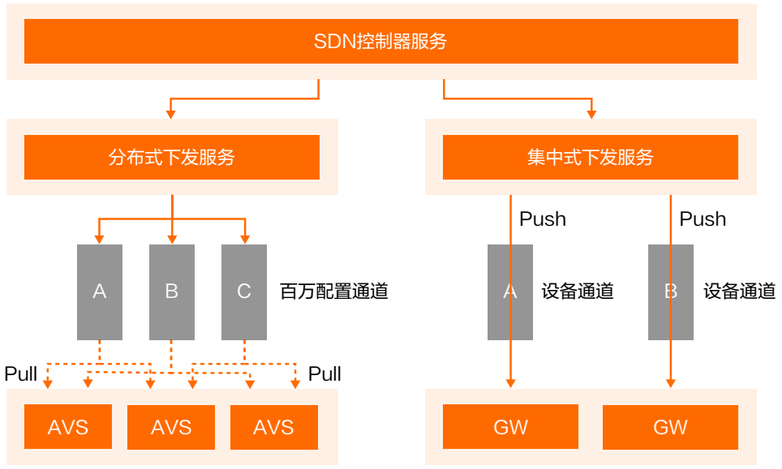
极致弹性的挑战。弹性能力是云的关键特性之一，许多大客户除了要求常态的大规模业务部署外，也要求具备极致弹性扩容能力使得业务规模具备快速翻倍能力，如应对应急的热点事件，另一方面云原生的高速发展也给网络弹性能力提出了极高的要求，这需要VPC控制器满足容器的即弹即用的诉求。

高性能VPC控制器

VPC控制器是阿里云自研的全新分布式控制系统，除了完成传统的SDN控制器的基本功能外，更专注于解决云网络的超大规模和极致弹性的问题，其整体的架构设计具备高可靠，高性能以及水平扩展等特性。

设备模型抽象。SDN控制器管理的设备类型有很多种，根据其业务特性的不同分别抽象为分布式交换设备和集中式网关设备。分布式交换设备的特征是设备量规模很大但是资源受限因此设备承载的租户配置较少，这类设备的设备变配频率低，但是变配涉及的规模较大。集中式网关设备特征是设备规模不大，但是设备承载的租户配置很大，这类设备的租户变配频率很大，但是变配涉及的设备规模不大。

统一配置下发服务。针对以上两种类型设备抽象出两种通用的配置下发服务，分布式下发服务和集中式下发服务。

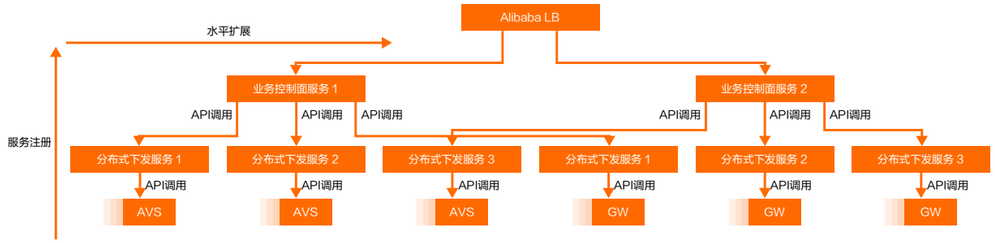


通道+缓存+版本号机制。分布式配置下发服务针对交换设备的下发特性抽象出百万通道，每个业务对象抽象为一个通道并关联不同的设备，每个通道具备唯一一份全量配置和配置版本号，转发设备基于版本号和注册的通道信息获取对应的配置。集中式配置下发服务针对网关下发特性抽象出设备通道，每个设备对应独立的下发通道，每个设备通道同样具备唯一版本号，网关设备根据版本号获取相应配置。

推拉结合的配置下发机制。分布式交换设备量大，单设备变配频率低为了降低配置下发压力，通过设备定期拉缓存的方式来缓解配置下发压力，集中式网关设备量小，变配频率高，通过主动配置推的方式来达到配置快速生效的目的。

水平扩展能力

SDN控制器系统通过分层设计原则，下层服务向上层服务注册的方式实现服务之间管理和通信机制，每层服务管理固定数量的下层服务以此来达到水平扩展的能力，服务之间通过心跳机制保活，当下层服务探测到某个服务不可用时主动连接新的可用服务。基于该设计架构，SDN控制器可以完成百万设备的配置下发管理以及大并发的业务变配。



数据对账系统

SDN控制系统数据对账系统分别实时对账系统和离线对账系统，通过配置下发版本号完成设备实时数据对账，保障不会漏下配置，可以有效保证转发设备业务准确性，通过服务间离线的数据对账保证系统整体的配置一致性。

4 云网络白皮书
云网络架构设计

云网络是云计算基础的基础，是面向租户和应用的虚拟网络，是用户业务系统的底座。不管对云平台还是用户来说，云网络的重要性都不言而喻，因此，如何做好云网络的架构设计就非常重要。用户可以从现状、业务发展、组织等多角度考虑云网络的架构设计。同时，遵循一定的架构设计原则，做好云网络规划和设计。

1 架构设计思考

架构设计必须多维度思考，除了关注架构设计本身，更需要关注企业的业务和组织发展，因为架构设计是为企业发展服务的，再好的架构设计，如不能满足企业发展需要，都不是成功的架构设计。

❶ 基于现状角度

在考虑云网络架构设计的时候，首先需要考虑的是企业的IT现状。从云的角度看，一般来说有几种情况。一是企业目前在使用传统IDC，正考虑上云。这时需要考虑的是上云的节奏是什么？是先弹性部分上云还是全部上云？是先新增部分上云还是一次性上云？二是企业已经全部在使用云，需要分析业务发展、可靠性、安全性等等。三是企业已经在使用混合云，需要考虑的是短期如库存水位、业务瓶颈，网络问题等，以及混合云的长期目标及策略等。四是企业是初创企业，这个时候现状就比较简单，考虑的是选择云的问题。

❷ 业务发展角度

云网络架构设计是企业云战略或者IT战略的一部分，IT战略需要服务于企业战略，因此，需要从业务发展的角度考虑云网络的架构设计。比如，当前是初创期，用户规模较小，对成本敏感，未来一年还是在探索阶段，这个时候可能就会选择单地域部署业务，节约成本。或者，企业业务发展迅速，未来一年的目标是全球化，从网络架构的角度看就需要考虑如何构建一张全球化的网络？如何让全球用户快速的访问到企业业务？

❸ 组织角度

组织角度也会影响云网络架构设计。公司组织体系是怎样的？集团性的公司往往有总公司和分公司，总公司和分公司业务系统的访问关系和通信控制是是怎样的？不同部门的业务系统网络是否要隔离？不同业务系统的管理人员和权限如何划分？等等，这些都会影响云网络架构设计。

2 架构设计原则

云网络是基于物理网络之上构建的面向租户和应用的虚拟网络，它的架构设计原则既有物理网络的普遍性，也有云网络自己的特殊性。整体看，云网络通过服务化的产品为用户提供网络服务，用户遵循一定的原则可以更轻松、更低成本的构建健壮的网络架构。

❶ 安全性原则

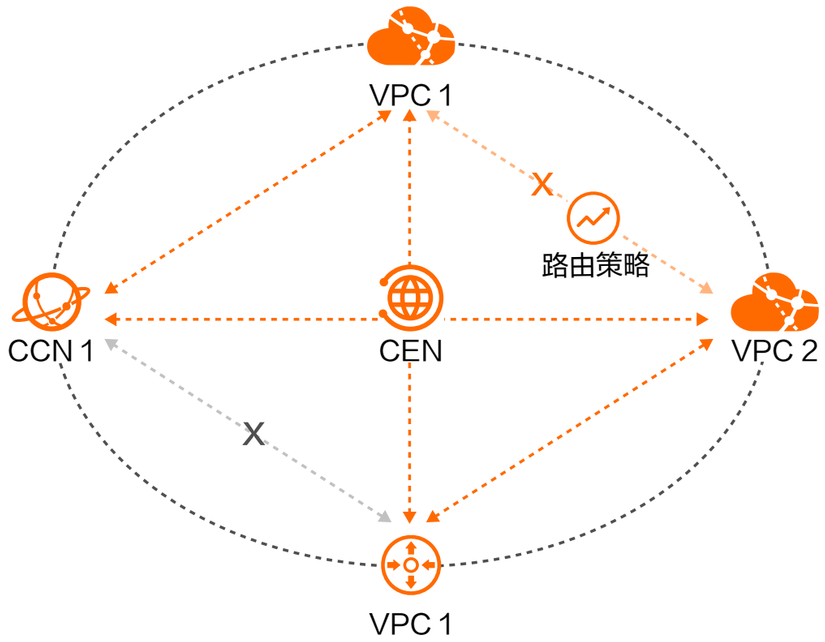
公共云是通过共享集群为很多用户提供服务，阿里云也为用户提供完整的云安全管理体系。对用户来说，安全始终是第一位的，安全涉及面非常广，这里只从云网络的角度看，安全性原则主要有以下几个方面。

首先是租户隔离

租户A和租户B在公共云上在网络上安全隔离的，租户A默认无法访问租户B，租户B默认也无法访问租户A。阿里云通过VPC为租户提供了一个私有安全给的网络环境，VPC基于隧道技术来实现，不同租户的流量都只在各自的隧道里面流动，默认情况下都是不能互通的，从而实现了安全隔离。VPC是租户在云上网络安全的基础。

其次是通信安全

从网络的角度看，通信安全可以简单分为内网通信安全和公网通信安全。从内网通信看，又有VPC内网和CEN内网，公网方面主要是控制和互联网的访问。从分层角度看，有路由层，网络层，主机层多层次的通信。不管是什么范围，什么层次，都需要遵循一个通信安全原则–最小通信安全，即只允许必要的通信，如只对公网开放必要的服务器和服务端口。用户可以根据自己的业务和组织多维度评估通信安全。



从路由角度看，云网络提供了VPC子网路由，CEN路由管理和路由策略， CEN转发路由器TR（Transit Router）等多种手段为用户进行路由管理。如下图中可以使用路由策略功能阻断VPC1与VPC2间的互通能力，但VPC1与CCN1/VBR1正常互通，VPC2与CCN1/VBR1也正常互通。

在网络层，网络ACL实现了VPC中的网络访问控制功能。在主机层，ECS安全组也是一种很好的安全手段，用于在云端划分安全域。

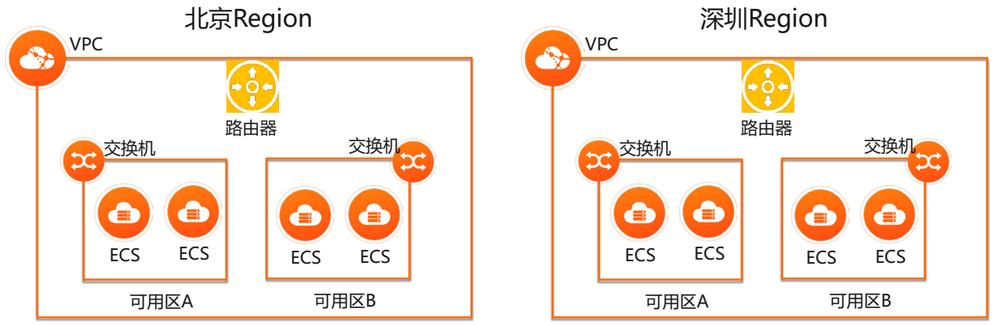
另外，跨账号通信安全是一个需要关注的问题，一定做好规划和日常管理，避免安全事件。

最后是安全防护

企业在云上通过互联网为其用户提供服务，阿里云免费提供了很多安全防护能力，很多用户的系统平时默默被保护着，并不感知到相关产品和服务，但从架构设计原则角度看，必须了解云上网络安全防护体系，以便构建自己的安全防护能力。首当其冲的是DDoS防护，避免遭受DDoS攻击后服务不可用。其次是云防火墙，在上述通信安全的基础上进一步增加安全性，可以统一管理互联网的访问策略和业务与业务之间访问策略。还有Web应用防火墙（Web Application Firewall，简称WAF），可以抵御常见web攻击，过滤恶意访问，保障网站应用的安全性与可用性。这些产品在安全防护，访问控制，应用防护等多维度构建安全防护体系。

❷ 可靠性原则

可靠永远是业务系统追求的目标，阿里云始终追求用户业务永续，为满足可靠性要求，阿里云为用户提供了丰富的产品和服务，让用户可以很方便的设计可靠的业务系统。可靠性也是一个非常大的话题，这里仅从云网络的角度看可靠性原则，主要考虑如下方面。



业务部署的可靠性

业务部署主要考虑的是多地域多可用区、单地域多可用区、单地域单可用区几个层次的可靠性。

单地域单可用区部署可以获得最低的网络延迟，但如果业务部署所在可用区出现故障（概率低），或者某个可用区的业务系统本身出现故障，整个业务系统将不可用，单地域多可用区部署业务系统可以避免这种情况。单地域部署不能避免的是整个地域不可用导致的不可用，当然这种概率极低，在可能的情况下，可靠性原则建议多地域多可用区部署业务。

网络链路可靠性

业务部署可靠性是基础，在其基础上，需要考虑的是网络链路可靠性，包括公网出口链路，跨地域网络链路和混合云网络链路。

公网出口链路方面，选择多线BGP带宽可以减少某个运营商异常引起的可靠性问题。如果在单地域多可用区部署业务，建议在每个可用区都部署公网出口，如负载均衡SLB实例A和实例B的主可用区分别是可用区A和可用区B。如果是多地域多可用区部署业务，产品形态会要求在不同地域部署公网出口链路。

跨地域链路可靠性方面，目前底层使用阿里云全球传输网络，任意两点都有多条路径冗余，保障SLA，在产品形态上还没有对用户开放路径冗余选择。

混合云链路可靠性需要考虑的问题更多，从混合云网络单产品来看，包括VPN网关双隧道冗余和用户侧网关冗余，高速通道（物理专线）多接入点冗余和多链路荣誉，智能接入网关SAG宽带和4G的冗余等。此外，还需要考虑多产品组合提升可靠性，如高速通道（物理专线）和VPN网关的主备冗余，高速通道（物理专线）和智能接入网关SAG的主备冗余等。

整体可靠性

整体可靠性指的是要从整个业务系统的角度看可靠性。一个完整的业务系统往往比较复杂，除了考虑部署可靠性和网络可靠性，还需要考虑数据库，存储等的可靠性，以及考虑系统之间的关联关系等，只有对业务系统的整体可靠性设计，才能真正实现高可靠。在实际操作上，建议区分系统优先级，梳理系统调用关系，确保高优先级的系统可靠性不出问题。

故障逃逸

故障逃逸是可靠性设计中非常重要的方面，建议对核心的业务系统要全面评估故障风险和影响，出现故障后能够通过自动或者手动的方式进行系统切换，逃逸故障。

❸ 可扩展原则

可扩展原则指的是要考虑业务未来发展的需要进行网络架构设计。一般来说有纵向和横向两种扩展方式。纵向扩展是增加单个资源的规模来扩展，比如在一个VPC内尽可能放更多的云资源，跑更多的业务，或者提升单个负载均衡实例的规格，以承载尽可能大的访问。横向扩展是通过增加资源数量来实现扩展，如通过多个负载均衡实例进行流量调度。建议纵向和横向结合来实现可扩展。对云网络来说，通常需要考虑的扩展指标有带宽，规格，VPC子网地址数量等。

4 性能原则

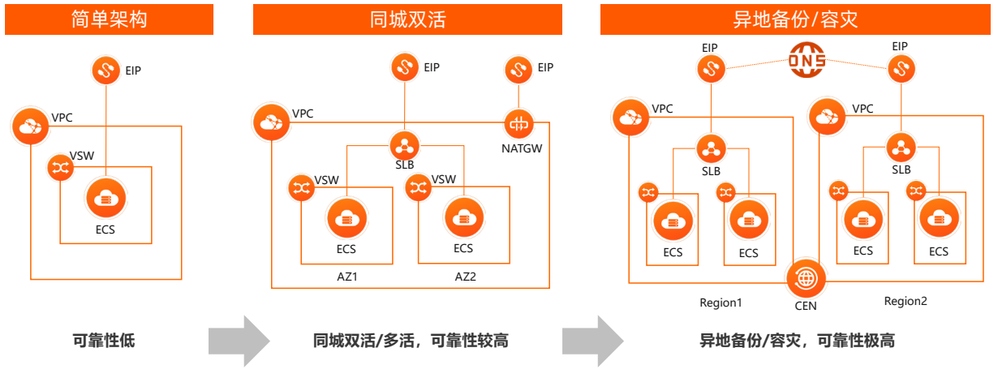
云网络是业务系统的基础，更是对外提供服务的载体，网络性能直接关系到服务质量的好坏。性能原则指的是要根据业务需要和系统情况综合评估网络架构设计，达成满足业务需求的网络性能。除了云网络产品本身的性能指标，还需要考虑最终用户访问到云上业务系统的网络延迟。比如业务系统部署在北京，要优化欧洲用户访问体验，降低20ms的延迟，从性能原则的角度，在网络架构方面就会考虑要么在欧洲全球加速这样的产品，要么在欧洲部署业务系统并提供访问入口。此外，不同系统间的多次调用带来的网络延迟也是一个重要的考虑因素。

3 架构设计实践

上文提到云网络架构设计的思考和原则，可见云网络架构设计要考虑的因素很多，那什么是好的网络架构设计呢？其实，适合业务发展的网络架构就是好的网络架构。网络架构设计不是求大求全，而是根据业务需求和企业发展的不同阶段综合考虑。下面基于企业和系统规模，从可靠性、安全几个角度出发考虑几个云网络架构设计实践。

1 可靠性架构设计实践

可靠性较低的简单架构，单地域单可用区部署，直接使用单台ECS和EIP提供服务。这个架构ECS存在单点故障，如使用多台ECS和负载均衡可以快速提升可靠性。

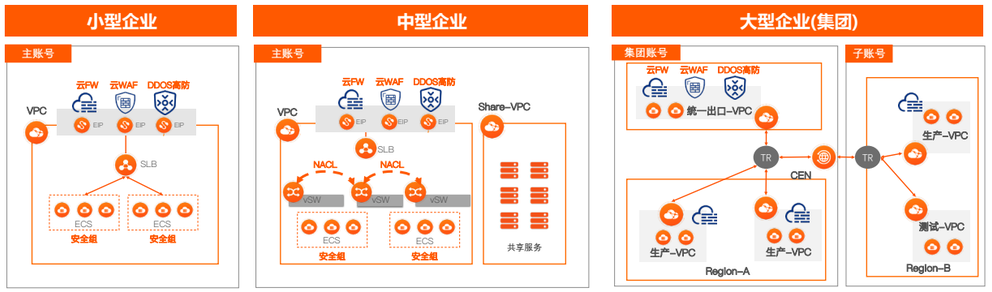


可靠性高的同城双活架构，单地域多可用区部署，使用多个虚拟交换机，并使用SLB和多ECS进行负载均衡和流量处理。在这个架构中，如使用多EIP和多SLB可以进一步提升可靠性。

可靠性极高的异地容灾架构，多地域多可用区部署，在多个可用区部署ECS，在每个地域采用EIP和负载均衡调度流量，最上层使用智能DNS实现对多地域EIP的流量负载。底层使用CEN连接多个地域（Region）VPC，构建内部通信网络。

2 安全性架构设计实践

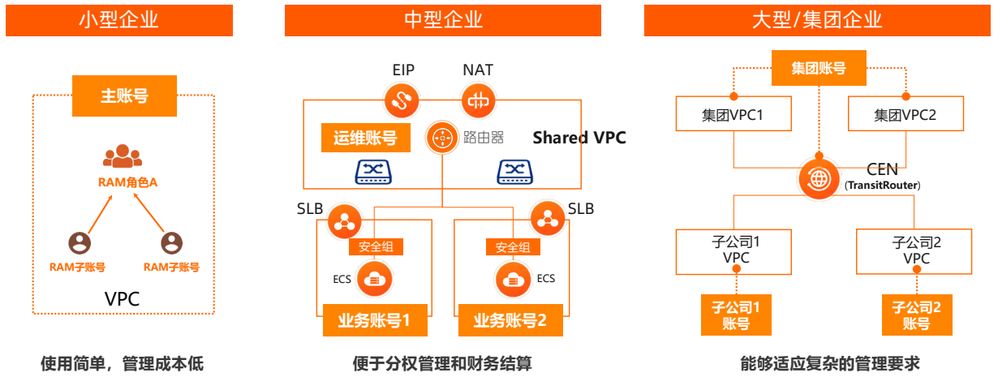
企业可以根据规模和安全要求选择不同的网络安全架构。对小型企业来说，业务系统较简单，采用的安全手段也相对简单。使用VPC构建云上私有网络，实现租户隔离，VPC内使用安全组控制ECS的访问。安全防护方面DDoS防护默认对EIP进行防护。



对于中型企业，除上述安全手段外，还可以采用ShareVPC部署共享服务，使用网络ACL基于VPC内子网进行子网间隔离，WAF可以基于应用进行安全防护。对于安全要求更好的大型企业，可以设置DMZ区，将和互联网交互的应用都部署在DMZ的VPC内，并使用DDoS，WAF，云防火墙等安全防护手段。在不同的VPC通信安全方面，CEN的Transit　Router可以精细控制网络访问。根据业务需求，把生产和测试系统部署在不同的VPC。

③ 组织角度架构设计实践

小型企业组织架构简单，人员相对较少，可以只使用一个主阿里云账号，通过RAM角色和账号管理权限。



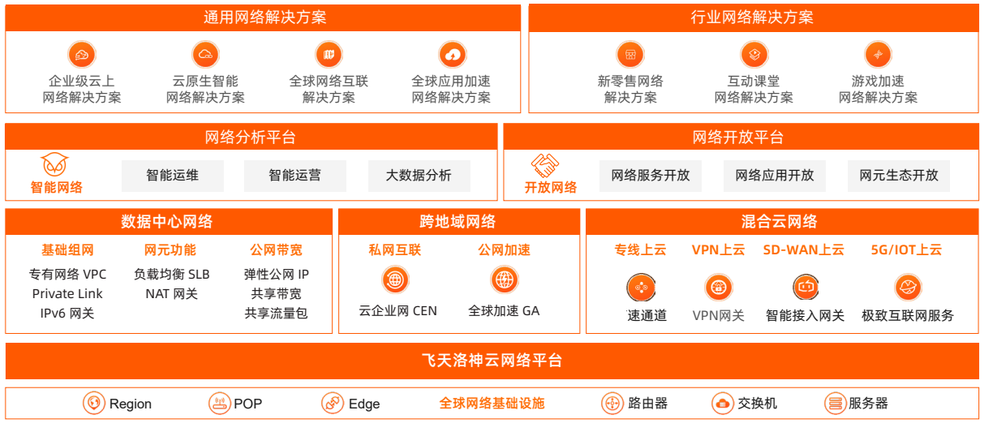
中型企业采用多账号管理，业务和运维分别使用不同账号，运维账号负责基础网络的维护和规划，并创建Shared VPC分配给业务的资源使用。对于大型企业，集团和子公司使用不同的账号管理体系，子公司VPC通过跨账号加载接入到集团CEN，通过CEN的Transit Router管理各VPC之间的互访。

5 云网络白皮书 解决方案和案例

1 概述

解决方案一般是指多个产品组合起来解决客户某个场景的问题或需求，云网络解决方案是以用户网络问题和需求为出发点，通过多个云网络产品及相关产品形成的解决方案。如下图所示，解决方案位于最顶层，是在产品基础上形成的。云网络解决方案可以分为通用解决方案和行业解决方案，如，全球应用加速网络解决方案和全球网络互联解决方案是通用解决方案，新零售网络解决方案是行业解决方案。因篇幅所限，本章简单介绍几个通用网络解决方案和案例。

完整的云网络产品和解决方案



2 企业级云上网络解决方案

❶ 方案定位

企业级云上网络解决方案的关键词是企业级，是满足商业组织，尤其是大型企业，集团型企业的网络需求的。企业级网络的关键特点有可靠性，安全性，复杂性，大规模，易管理等。本方案就是满足企业级网络的这些关键需求的。

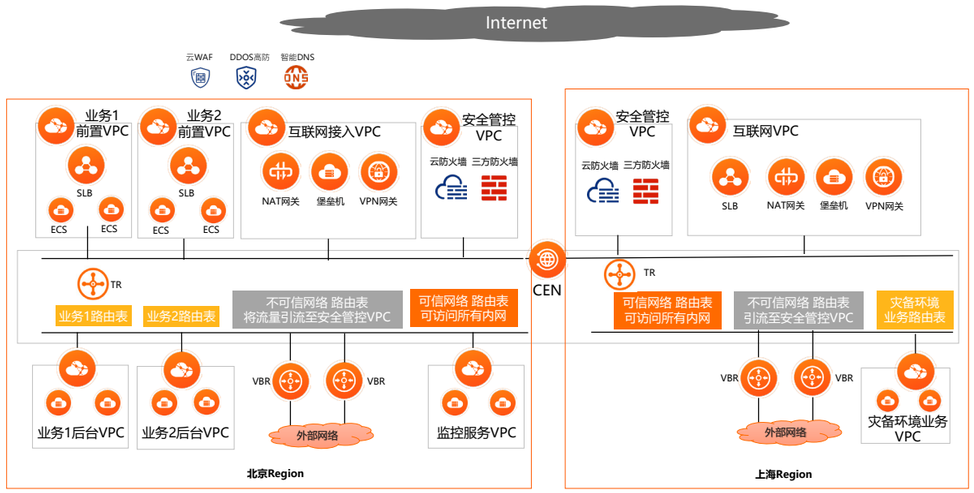
在可靠性方面，企业级网络需要冗余，没有单点故障。单点故障简单来说可能是某个负载均衡实例失效，或者高速通道某条专线链路异常，也可能某个可用区级别的异常，虽然这种异常发生概率极小，但作为企业级网络来说，也是需要考虑并从架构设计上规避。

在安全性方面，企业级网络需要严格租户隔离，并且有严格的安全通信管控能力。如不同业务之间的网络访问控制，对外开放服务的网络访问控制等。还需要建立立体的安全防护体系，包括网络层防护，应用层防护，安全审计等等。

大型企业和集团型企业往往业务和组织都非常复杂，这必然带来网络的复杂，如业务系统之间精细的互访和隔离，资源使用和管理权限划分，复杂的成本和账务等等。

❷ 方案介绍

本方案采用多地域多可用区部署，实现高可用，每个地域使用多个VPC部署集团不同业务，每个业务前端和后端部署在不同VPC，VPC内根据需要使用网络ACL或ECS安全组实现访问控制，不同VPC之间通过CEN互联，使用CEN中转路由器TR控制不同VPC的精细路由访问。公网访问方面，使用智能DNS将域名解析到不同地域的公网IP，实现跨地域访问容灾，每地域内使用SLB给多个可用区的ECS调度流量。安全防护方面，考虑使用安全管控VPC，使用CEN中转路由器TR倒流，部署云防火墙或者第三方防火墙。



因篇幅所限，方案中未体现账号管理相关设计，可以参考阿里云官网IT治理相关内容。

❸ 客户案例

客户信息：

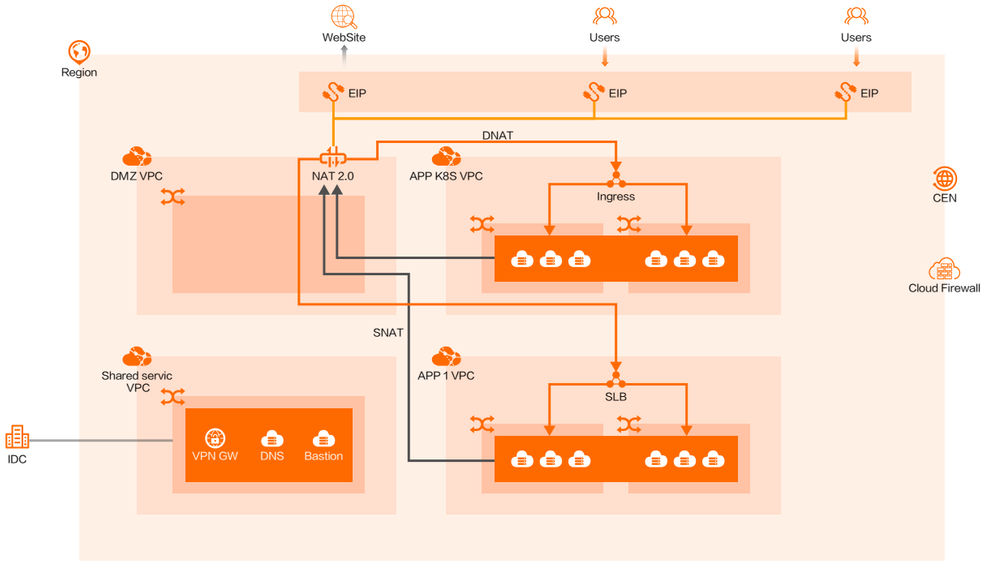
某百年豪华汽车品牌，是世界上最知名、最受尊敬的高档汽车品牌之一，2019年在约100个国家销售超过70万辆汽车。2019年，该汽车企业平均雇佣约41500名全职员工。企业总部，产品开发、市场营销和管理职能主要位于瑞典哥德堡。企业亚太区总部位于上海。

应用诉求：

由于集团内部安全需求，企业在云上的所有资源当需要和公网通信时，均需要统一经过DMZ区域的审计设备，所有流量可监控可管理。

业务痛点：

早前没有云原生的统一公网出口方案时，客户花了大量的时间和精力使用自建方案，部分环节还没有SLA保障，耗时耗财耗力。



解决方案：

使用企业级云上网络解决方案，不同业务部署在不同VPC，使用CEN连接不同VPC，在CEN粒度部署NAT网关，统一公网出入流量管理

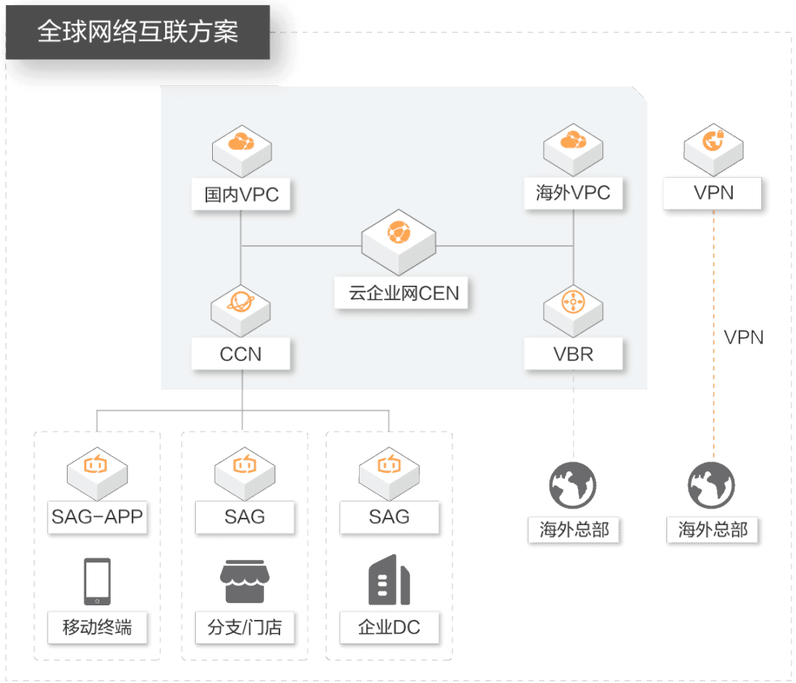
方案价值：

阿里云原生的统一公网出口方案，保障SLA，通过公网统一出入口，满足审计要求，大大降低运维复杂度。

3 全球网络互联解决方案

❶ 方案定位

随着越来越多的企业上云，混合云成为一种长期存在的形态，企业的数据中心，总部，分支，移动终端等都需要和公共云互通。此外，随着用户在云上的业务系统发展，多地域部署，甚至多国家部署成为常态。因此，构建一张云上云下一体的私有网络就成为了必需，企业通过这张私有网络，满足业务安全，稳定的内网通信需求。



快速构建全球互联网络

❷ 方案介绍

全球网络互联解决方案主要以CEN为核心，加上混合云网络产品VPN，SAG，高速通道，以及云上VPC组成。用户可以将云下IDC、总部、分支、门店以及移动端通过不同的混合云产品连接到云企业网，再通过云企业网连接不同地域的VPC，最终构成一张多地域部署，云上云下一体的全球私有网络。

❸ 客户案例

客户信息：

客户是一家有20年历史的互联网在线教育集团，旗下有包含多个知名互联网在线教育品牌。业务覆盖中国大陆及港澳台、欧美、亚太、南非等全球各地。

业务诉求：

全球各分支机构互联，遍布全球各地分支机构能通过内网互联，使用内部办公应用系统；

降低互联成本，为业务发展提速；

业务痛点：

1）成本高，每年要花费数千万在MPLS网络上，扩容成本非常高，备份线路无法充分利用；

2）维护麻烦，路由修改都需要供应商提供支持，风险大，沟通成本高；

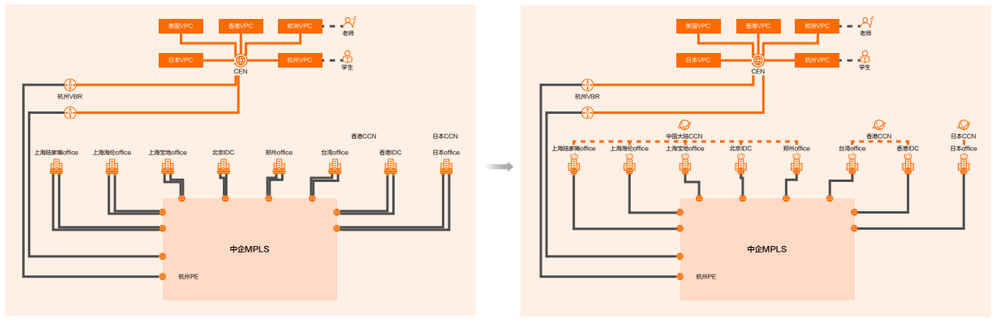
解决方案：

使用全球网络互联解决方案进行网络升级，具体如下：

CCN支持云上云下互联，总部使用SAG1000双机热备，可靠性高，Office使用单机SAG1000旁挂，原有组网快速扩张，部署简单；

CEN支持全球内网互联，利用CEN打通海外和国内的内部网络，构建全球企业内网；

支持平滑迁移和扩展，在原有MPLS网络之上，直接在各分支扩展SAG-CCN 网络替代原有备份线路；



方案价值：

性价比高：SAG替换MPLS备线，总体成本降低1/3以上；

易维护：SAG1000部署简单，非IT人员也可在远程指导下快速完成部署安装，并且能够集中维护；

高可靠：SD-WAN和MPLS流量分担，可用带宽增加一倍以上。两套独立骨干网络，总体网络可靠性大幅提升。

4 全球应用加速解决方案

1 方案定位

我们的日常生活已离不开通过互联网访问各种各样的互联网应用，如社交，购物，游戏，视频，办公等等。从网络的角度看，其中有很多时延敏感型业务，如游戏，教育，会议，以及丢包敏感型业务，如OA，ERP，CRM，邮箱等，由于这些应用通常对遍布全球的用户提供服务，而通常只部署在某一两个国家，这时，全球用户通过互联网去访问应用的时候就会存在时延大，丢包，甚至无法访问的情况，而全球应用加速解决方案就是解决互联网应用网络访问质量问题的，具体问题如下：

跨地域网络质量差：在应用实际部署中， 当互联网应用数据中心与最终用户不在同一区域时，由于互联网的高延迟、拥塞、丢包都会影响应用的性能。

最后一公里网络质量：最后一公里接入受制于当地ISP，难以优化。

网络优化难度大：由于互联网应用基于Internet，MPLS 和WAN Optimization技术无法适用于互联网应用加速。

安全问题：互联网应用普遍存在安全风险，网络加速的同时需要满足应用对安全的需求。

2 方案介绍

全球应用加速解决方案底层基于阿里云遍布全球的高质量网络基础设施，以全球加速GA产品为核心，配合DNS，DDoS防护，WAF等产品构成了整体解决方案，是阿里云提供的一站式应用加速网络方案，通过遍布全球基础的网络基础设施，实现网络服务全球范围就近接入和跨地域部署，提升应用

网络访问质量，并确保应用安全。

方案核心优势：

高质量全球网络，阿里云遍布全球的核心网络和高质量的公网接入带宽

快速部署，分钟级可部署本解决方案，业务0改造，只需要调整域名配置。

安全加速，无缝集成高防和WAF等安全产品

灵活调度，阿里云DNS智能调度，满足全球流量管理需求

3 客户案例

客户信息：

某知名航旅APP是提供全球近百万个航班实时信息，覆盖完整的行程管理、机票搜索、航班动态、机场信息、地图导航等功能，是乘机、接机、旅游、旅行相关人士的必备。

业务诉求：

CDN回源加速：航司订票商城满足全球客户访问，但是海外客户等直接访问国内源站反馈特别慢，分析原因的是回源延时比较大，动态内容需要频繁回源，所以需要加速回源时延和稳定性

APP加速：航旅纵横的APP源站部署在国内，要提升海外用户使用APP的访问体验。

业务痛点：

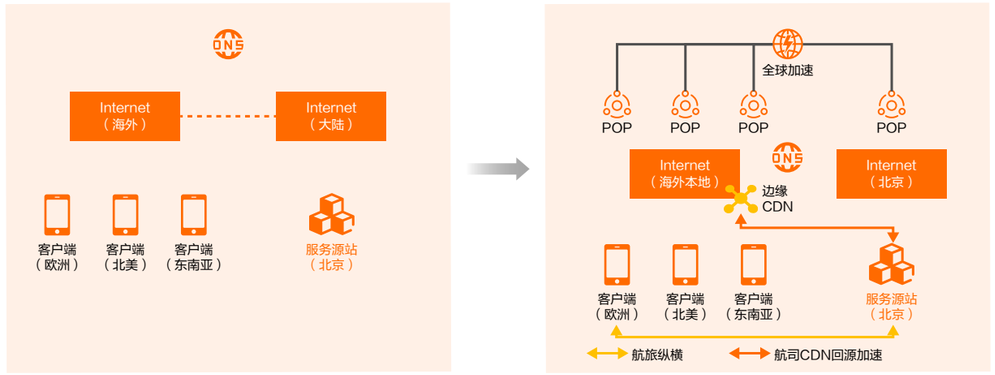
客户所在地域分布广，通过Internet直接访问APP源站不稳定；

海外客户从北美和欧州等直接访问订票商城反馈特别慢；

解决方案：

加速CDN回源链路：使用全球加速加速海外CDN节点的回源链路

基于DNS就近接入：使用全球加速在海外提供加速访问入口，航旅APP用户就近接入阿里云，通过全球加速访问国内服务源站。



方案价值：

提升用户访问体验，用户对于航司商城和航旅APP使用率提升，网页和APP打开时延降低30%；

加速地域灵活部署，按需灵活选择区域加速，不影响业务架构，只需要调整域名配置。

6 云网络白皮书
云网络未来展望

从数据中心云网络1.0到广域网云网络2.0，未来云网络如何发展呢？需要从技术与业务需求两个方面来进行考察。随着网络性能的持续提升，在承载内容与呈现方式上会发展巨大的变革。从应用发展趋势看，以下业务方向将影响云网络演进

面向个人，视频消费时代已经到来。随着移动资费的持续降低，5G手机普及，各种短视频软件降低了个人自媒体的门槛。2020年的疫情，彻底改变了人们的工作和生活。一部手机、一个摄像头就可以将自己的日常生活、知识经验、个人物品与线上观看他的人分享。短视频/直播目前还处于单向传播状态，叠加了人工智能的视频识别技术，内容上图文制作与视频制作将融合。视频消费时代对云网络的需求是什么呢？视频时代的核心问题是成本，核心技术是存储与用户体验问题。对于长视频/短视频，通常采用边缘CDN Cache+Region 冷数据存储。随着交互式语音向多人交互式视频应用在手机端的兴起，流媒体的传输增加了对实时视频的低延迟传输要求。

面向企业，数字化移动办公已经成为常态。今天的远程办公协同系统可为用户提供电子白板、文档同步、程序桌面共享、投票答疑、文字消息等丰富的会议辅助功能。全面满足各行业用户远程视频会议、访谈、招聘、培训、远程医疗、双师教育各种音视频需求。对于交互式视频，特别是在线教育/高清视频会议，要求云网络提供对底层网络进行切片，提供有QoS保障的传输能力，视频会议网络时延小于50ms，丢包<1%。

面向物联网，各种基于视频为基础的终端蓬勃发展。视频监控从智能城市走向智

慧家庭，家庭视频监控实现移动化；视频人脸识别技术使各种刷脸应用终端在门禁/支付等领域快速普及。显示成本的降低，户外广告从图文慢慢转向通过视频呈现。

为了支撑视频时代应用，对技术需求是读懂视频（识别），快速发现，提升音/视频体验，降低成本。从技术上看，以下几方面技术会影响云网络发展。

通用计算形态从虚拟机向容器化转变；

算力从通用计算走向专用计算，承载高性能；

云–边协同，分布式云成为新形态；

2020年，以5G/AI/IoT为基础应用与技术驱动，开启云网络3.0时代。

1 云原生网络

以容器，微服务，DevOps为代表的云原生技术引入，轻量级高效率虚拟化技术逐渐普及，云计算正向着“云原生”（Cloud Native）的方向发展。云原生对云网络带来了巨大的影响。云原生网络的基本目标是满足云原生服务的网络端点和服务间的互通性、安全性和负载均衡要求。

目前存在不同类型容器，包括部署于裸金属容器，部署于ECS虚拟机内的容器和Serverless容器。对于云网络来说，需要对用户屏蔽不同类型容器的差异，并支持容器与虚拟机间的互通。通过将容器网络下沉到智能网卡后，可以支持容器与VM，裸金属通信。同时支持缩短 I/O 路径，提高性能。在容器网卡对网络的性能与密度。虚拟机时代，每服务器上VM最大个数 100个左右，虚拟网卡个数有限。为了在虚拟机中支持更多的容器，虚拟网卡需要支持Trunk技术，单主机虚拟网卡达到1K以上。最关键的是容器的启动要求虚拟网卡创建速度从分钟到秒级别，对控制器的响应速度提出更高的要求。

对于基础的二三层接口/IP被封装到容器网络接口 CNI（Conteinre Network Interface)。CNI接口实现创建、删除容器时的调用方法，其他所有的网络能力都交由网络厂商实现增值服务。CNI接口模型在一定程度上加速了网络方案的繁荣，各种组网形态层出不穷，给用户的方案选型造成了较大困扰。根据网络协议的不同，可将网络方案分为路由模式、Overlay 和 L2 方案三种。对于公共云平台来说，既要保证API接口的一致性，由于已经支持了面向虚拟机的一层Overlay网络，对于容器，阿里云可为客户提供L2与容器Overlay模式。

在服务的对外形态上。Kubernetes已经成为容器编排的事实标准，容器网络服务需与 Kubernetes 的调度机制相匹配。而4到7层的网络被封装到ServiceMash（服务网格）中。在K8模型中从应用的角度看抽象成了对外提供的Service服务和由服务的计算实现NODE和POD节点。应用的视角不再看到具体的IP，路由策略，更关注服务的状态，限流，熔断监控等里。负载均衡服务被K8S集成，作为服务分发的核心部件。从通信服务上分为南北向7层流量分流的IngressRouting（入口路由服务）和东西向流量服务间进行服务发现和分发的负载均衡服务。为了支持云原生服务的DevOps灰度发布能力，云原生网络中负载均衡需要支持不同版本的服务在线升级和弹性伸缩。

开源K8S架构中的容器网络更多依赖Linux操作系统中的IPTable，Nigix等组件来支持。阿里云网络通过云原生网络集成了虚拟网卡（ENI），vSwitch， POD集成安全组实现安全隔离，集成负载均衡实现ServiceMesh服务等能力。

云原生网络还在飞速发展，水平方向需要支持跨多个中心云，云-边一体的通信。云原生网络带来了网络管理运维监控的负载度。需要提供面向应用视角的网络监控与故障恢复能力。

2 专用计算高性能网络

人工智能包括核心三大要素，算法、算力和大数据。对于算力目前深度学习流行的异构解决方案共三种，分别是ASIC、FPGA、GPU。异构计算则成为了深度学习的重要支柱。由于单台服务器存储空间的限制，分布式存储成为必然选择，存储介质从SATA到SSD，再到eSSD，数据访问性能指数级提升。不同服务器间相互协同，高性能远程访问数据成为对网络的核心需求。 RDMA（远程直接内存访问）是目前业内最受欢迎的高性能网络技术，能大大节约数据传输时间，被认为是提高人工智能、超算等效率的关键。在未使用RDMA网络时，语音识别训练每次迭代任务时长为650ms至700ms，其中通信时延就占400ms。RDMA通过将网络处理卸载到硬件NIC中，绕过内核软件协议栈，实现高性能网络传输。在共享的云环境中，难以修改商业硬件中的控制平面状态，控制PCIE总线上RAM和NIC间的DMA传输。当前几个数据密集型应用（如TensorFlow、Spark、Hadoop等）仅在专用裸机群集中运行时才使用RDMA。

公共云环境需要为异构计算，容器化通用计算提供虚拟化的高性能/低时延访问能力，并与底层物理交换机设备进行解耦。采用软件在CPU级别实现RDMA虚拟化受限于CPU主频与网卡分发能力，无法满足性能要求。要实现虚拟化高性能网络，需要解决几个核心问题：1.编址与路由： RDMA Over Ethernet方式，受限于底层以太网的广播域与交换网络的收敛组网，范围无法扩大。使用RDMA Over IP(VxLAN)方式可支持更大范围的扩展性。2.拥塞控制能力，在追求极致的无丢包的场景下，是否可对时延适当降低。IP网络本质是尽力传输。TCP采用事后追溯机制进行重传，底层拥塞后时延大幅下降。RDMA可采用信用机制主动预留与事后追溯结合。 3.高性能虚拟网络需要与应用呈现直接交互，支持RDMA API，以实现编制与路径控制。4.虚拟网络需要介入应用操作系统/容器的地址空间，进行内存的管理与映射，实现零拷贝。

专用计算带来的高性能低时延的要求改变了云网络的业务范围，使网络更加贴近应用的需求进行构建。云网络3.0需要在低时延特性上实现面向应用的网络虚拟化。

3 分布式云网络

边缘节点在云计算初期更多是承载CDN业务，对网站/视频的静态内容进行Cache，减少网络传输成本。随着云计算的深入，对于需要即时处理和分析由物联网设备、联网汽车和其他数字平台生成或即将生成的数据，这时边缘计算能够派上用场。边缘计算是一种分布式网络基础设施，它使数据能够更接近其来源的地方进行处理和分析。从网络视角看边缘计算，除CDN Cache类业务外，需找到时延敏感并与公共云对接的应用。对于未来IoT物联网，大部分数据处理（如AI推理）都在边缘进行，而云被用于存储和大型计算（如AI训练和大型应用程序），而这些应用程序对延迟都不是很敏感。对接5G网络时，边缘计算节点可对运营商5G数据进行引流，实现对业务分片需求的对接。目前大部分的边缘节点还处于独立的孤岛状态。随着越来越多企业应用运行到边缘云上，对网络来说存在以下诉求：首先是从安全性上支持私有网络隔离与互联，中心云的VPC向边缘进行延伸。其次是小型化问题，边缘节点的服务器规模有限，应用容器化/Serverless部署成为趋势。

虽然混合云的概念炒作了很多年，很多企业的应用事实上确实存在公共云和专有云同时部署的场景。但是由于专有云的多样性，公共云与专有云之间的网络是相互割裂的。对于很多中小型企业来说，管理和维护专有云是一件很复杂的事情。但是还是有很多本地业务需要私有化部署。这时就提出了云向线下扩展的需求，将扩展到企业的边缘节点与云实现统一的控制与管理需求。

云网络如何从中心云拓展到边缘节点，还存在很多难题。首先是边缘节点的Underlay基础网络管理问题。对于云厂商的边缘节点可以统一规划IP地址，对于部署在企业的边缘节点，会存在IP地址冲突问题。其次如何抽象网络对象模型，不能简单的把中心云的VPC模型复制到分布式边缘节点。分布式边缘云的应用形态还在快速变化，对于传统的CDN业务，提供传统网络为计算提供公网IP地址即可。由于边缘节点的计算容量比较小，通用计算支持容器或者ServiceLess计算成为必然，云原生网络会从中心云计算拓展到边缘。边缘云对云原生网络的分布式能力提出挑战，需要向应

用底层屏蔽负载的组网拓扑。基于人工智能驱动的物联网设备，需要在边缘部署推理NPU或进行视频处理的GPU，边缘节点同样需要高性能组网能力。为了实现云-边协同、边-边协同，需要构建一张遍布全球的分布式云网络。这个领域值得云网络3.0进行深入研究；

4 万物互联网络

今天物联网已经是切实的发生在我们身边的应用，从移动出行的共享单车，各种零售/物流无人货柜，遍布各种楼宇的广告终端等，通过无线物联网卡，各种智能终端可与云端实现连接。

物联网设备有几种方式连接到云端。 第一，私有IP地址转换方式。家庭/企业内的终端设备，使用Wifi方式联网，通过网关设备进行NAT转换获取公网IP地址转换访问云端服务。这种方式通常需要在企业或家庭部署物联网网关，对设备进行监控/管理。第二，物联网卡私有IP地址，由运营商P-GW建立隧道（GRE或L2TP）到服务端。这样要求每个应用都具备与不同运营商网关互联能力；第三，直接使用公有IP地址，通常是IPv6地址。终端和服务端都可以发起连接请求，部署简单。由于终端直接面向公网，安全性挑战比较大。

随着5G到来，边缘计算节点部署越来越多，但物理网设备对于整体网络的组网能力无法感知，于是为万物互联的云网络孕育而生。万物互联网络技术上同样采用Overlay智能到边缘，增加一层隧道，为IoT终端屏蔽底层网络组网负载度。万物互联云网络带来很多好处。首先是加速应用部署。云网络预先与运营商4G P-GW，5G UPF建立连接，为IoT应用屏蔽运营商物联网卡差异；其次，通过集中的调度，改变对隧道目标地址实现智能选路。根据应用的需求选择就近的边缘节点或中心云计算节点，流量调度能力，可以错峰提升网络带宽利用率，可以极大降低网络成本。第三，为IoT设备带来更好的安全性。由于采用隧道技术，尽管外层使用公有IP地址，但仅需开放有限的几个端口。不同企业的IoT设备内部组成一张安全的内网，对外提供服务的

出口在云端，可实现统一的安全防护。第四，物联网云网络技术是5G分片的基础。运营商准备在5G移动网上提供面向企业应用的分片能力。但对于各个企业来说很难掌握与运营商对接的协议标准。由于云网络可打通IoT连接到租户的VPC，甚至到云原生应用的网络内部。云网络具备了感知应用QoS需求的能力，可为IoT应用提供开放API对报文进行Qos Tag。通过调用运营接口，传递应用的QoS分片诉求。

面向万物互联的云网络目前还处于起步阶段。需要以应用场景驱动，建立完整的IoT连接体系：在IoT端上部署SDK；在边缘计算节点/中心云节点建立与运营商网络的连接；为IoT终端提供IP地址分配，状态监控，流量限速与计费能力；为部署在VPC内的IoT服务或IoT PaaS服务提供到与IoT终端的连接与策略配置能力；

ToC的移动互联网在高带宽下会持续推动视频消费。基于人工智能加持，面向ToB万物互联的时代已经到来。云网络需要向3.0进行快速演进，成为数字经济的连接基石。