SD-WAN 关键技术

Key Technology in SD-WAN

柴瑶琳/CHAI Yaolin，穆珹博/MU Yubo，马军锋/MA Junfeng

（中国信息通信研究院，北京 100191）

(China Academy of Information and Communications Technology, Beijing 100191, China)

摘要：软件定义广域网（SD-WAN）是将软件定义网络（SDN）技术应用于广域网（WAN）连接的服务。重点阐述了SD-WAN应用的关键技术，包括SD-WAN服务中4种典型技术架构、SD-WAN的整体功能模块以及边缘设备中所采用的关键技术。与传统的WAN架构相比，SD-WAN技术以一种多接入、安全、策略驱动业务、弹性路由、多虚拟隧道、敏捷上云的方法重新定义了开放式的WAN架构。

关键词：SD-WAN安全；策略驱动业务；弹性路由；多隧道；敏捷上云

Abstract: The software-defined wide-area network (SD-WAN) is a specific service that applies the software-defined network (SDN) technology to WAN connections. The key technologies of SD-WAN are discussed in this paper, including the technologies used in the following items: four typical technology architectures, the overall functional modules, and the edge devices. Compared with traditional WAN architecture, the SD-WAN technology redefines the open WAN architecture with a multi-access, security, policy-driven service, flexible routing, multiple virtual tunnels, and agile touching cloud approach.

Key words: SD-WAN security; policy-driven services; flexible routing; multi-tunnel; agile touching cloud

DOI：10.12142/ZTETJ.201902003

网络地址：http://kns.cnki.net/kcms/detail/34.1228.TN.20190326.1729.004.html

网络出版日期：2019-03-26

收稿日期：2019-01-28

软件定义广域网（SD-WAN）是将软件定义网络（SDN）技术应用到广域网（WAN）场景中的一种服务。这种服务用于连接广阔地理范围的企业网络，包括企业的分支机构及数据中心[1]。SD-WAN架构不依赖于专有的物理设备，与必须做预配置的多协议标签交换（MPLS）链路相比，弹性地解决了多分支结构企业网络在支持差异化服务等级应用能力、网络灵活度、线路成本、安全传输等方面正面临持续增长的压力。

根据互联网数据中心（IDC）的数据，SD-WAN市场将从2017—2022年以40.4%的复合年增长率增长，销售额达到45亿美元[2]。

现有市场的SD-WAN技术实现方案有多种：如VMware的SD-WAN架构包含边缘应用程序、编排和云网关，提供企业和云应用程序以及数据的直接最佳访问点，同时支持在云端和内部部署虚拟服务，显著增强自动化运维能力；思科和华为为提供WAN连接制作了不同功能和性能需求的广域网边缘设备，更加关注广域网优化功能。通信服务提供商也正在提供SD-WAN即服务产品。SD-WAN即服务通过常规宽带连接补充或替换通常为MPLS的专用WAN网络，最大限度地提高了企业管理基础架构和连接的灵活性。中国电信随选网络系统由业务门户、SDN编排器、SDN控制器、SDN设备4大组件构成，该系统基于WAN和骨干网设备的集

中控制和全局网络资源的管理，根据不同服务和应用来实时动态建立端到端的WAN逻辑路径，优先满足一些高带宽、低时延、低抖动的敏感应用，包括语音、数据、视频、自动驾驶、虚拟现实（VR）等应用，实现了SD-WAN即服务技术[3]。

随着企业上云需求的不断提高，现有企业在云场景中跨境数据传输和运用客户关系管理系统（CRM）、企业资源计划（EPR）等高端应用时经常面临丢包、延迟、卡顿等无法正常使用的情况。SD-WAN技术通过集成在多云边缘的网络功能和策略，提供了面向多云场景中简易运维、即需即用、可靠、易扩展的云化企业专线来保障多云环境下的企业业务运转，重塑了企业上云的生态过程。但要真正成为企业级SD-WAN服务标准，SD-WAN技术方案还须提供一些关键功能，如多个传输路径、集中控制和自动化，以及端到端安全性[4]。

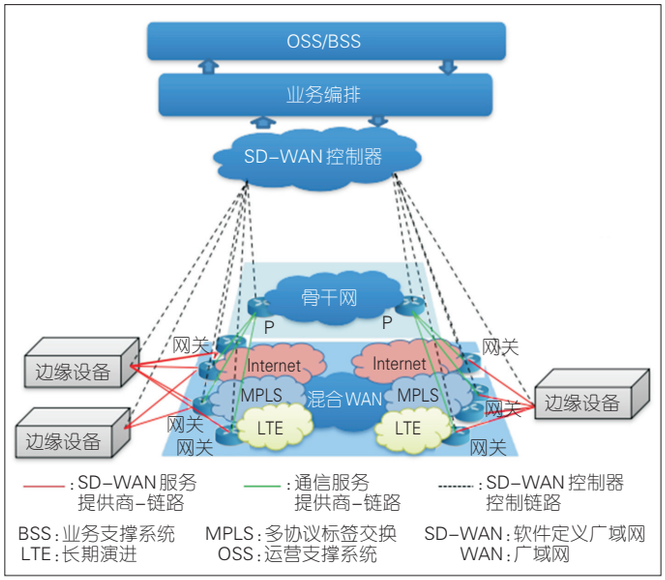


图1▶ SD-WAN架构图

1 SD-WAN架构

SD-WAN架构将部署在各个地理位置的企业网络（包括分支机构或数据中心）通过WAN接入技术相互连接。如图1所示，不同的SD-WAN架构以SD-WAN控制器对网络域的控制边界为准，划分为4种典型的SD-WAN架构方式。

（1）叠加架构。该架构改变了传统的WAN业务模型，由单一的WAN接入方式变为多接入方式。同时，SD-WAN控制器控制了边缘设备到网关的上行流量，简化了WAN的操作和管理，使业务模型更弹性、更灵活，例如分支到分支的业务流量由分支到数据中心再到各个业务分流变为直接跟随业务分流。这种架构适合中小规模企业组网。

（2）云端架构。该架构集成SD-WAN服务提供商所部署的多个入网点节点，是SD-WAN服务提供商向大规模多分支公司推荐的一个经典架构。SD-WAN服务提供商在接入点（PoP）节点部署虚拟边缘路由器（vPE）或网关（GW），一侧与各个分支的边缘设备建立虚拟专用网络（VPN）隧道，另一侧与通信服务提供商的MPLS网络中的PE设备直连。这种SD-WAN架构支持将汇聚上来的流量通过多个隧道转发到运营商的MPLS骨干网中，进而保障了端到端不同业务的服务质量。

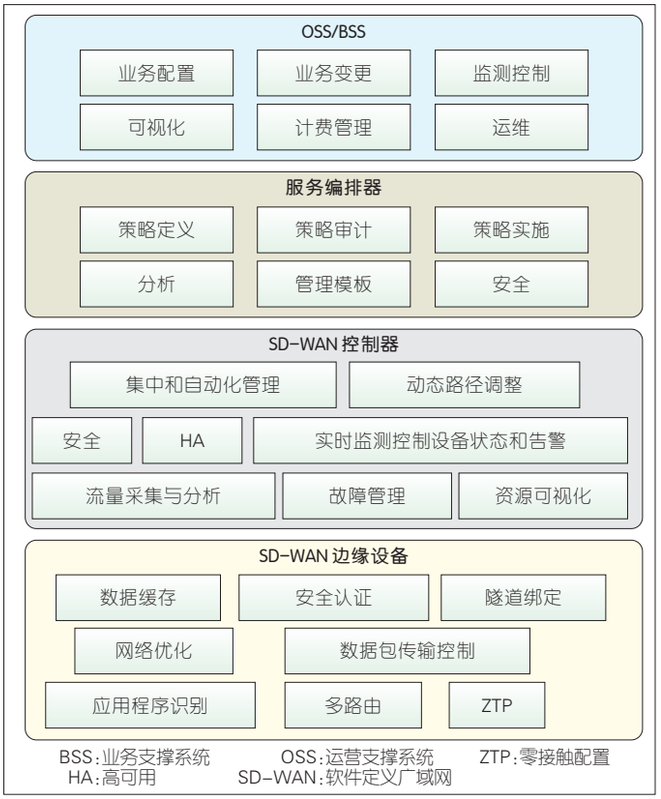
（3）整合架构。网络管理域由可纳管多个边缘设备扩大到可纳管1个或多个通信服务提供商的MPLS VPN的运营商边缘路由器（PE）设备（如图1中混合WAN中的网关），集成多种overlay技术，打破了多个通信服务提供商的统一和自动化管理的通信壁垒，有效提高了网络性能和混合组网能力。

（4）原生架构。该架构主要面向运营商。SD-WAN控制器统一管理边缘设备、网关设备、骨干核心网PE、运营商骨干路由器设备，实现了业务流量从“最后一公里”接入到骨干网统一管理和编排的完整架构，从全网意识上实时监测控制和调度网络流量以及各种业务状态，以保障端到端的服务质量。

2 SD-WAN功能模块与关键技术

本文中，我们将SD-WAN功能切分为4层：运营支撑系统（OSS）/业务支撑系统（BSS）层、服务编排器层、SD-WAN控制器层，以及SD-WAN边缘设备层，各层具体情况如图2中所示。

（1）OSS/BSS层。在SD-WAN技术架构中，OSS/BSS层主要支持



◀图2
SD-WAN功能模块图

将业务配置、业务变更、监测控制、可视化、计费管理、运维功能于一体的面向自动化信息管理和智能化运营的支撑系统。

(2)服务编排器层。在SD-WAN技术架构中,服务编排器负责编排整套服务生命周期的服务。服务编排器提供多种管理模板,支持配置端到端管理业务的多种策略定义和资源统一编排功能,提供开放的RESTful接口,敏捷部署新业务。

(3)控制器层。SD-WAN控制器支持软件化、集中化、自动化管理边缘设备。SD-WAN控制器与边缘设备建立安全连接,通过执行服务编排器下发的各种策略,向各个边缘设备分发路由协议并支持实时感知边缘设备状态。同时SD-WAN控制器支持实时采集流量信息,并可快速应对网络异常情况进行弹性路径调整。

(4)边缘设备层。边缘设备是创建和终止SD-WAN隧道连接的终端设备。边缘设备支持常见的SDN南向接口协议,支持零接触配置(ZTP)部署能力,支持安全隧道绑定功能,支持识别多种应用程序功能,支持面向应用的访问控制策略,并还可以支持路由协议。

边缘设备层对应的边缘设备在市场上主要由客户终端设备(CPE)、通用客户终端设备(uCPE)、虚拟客户终端设备(vCPE)3种设备形态组成,3种设备的功能对比如表1所示。CPE是SD-WAN服务提供商提供的专用硬件设备。uCPE是一个支持运行虚拟网络功能(VNF)的可远程管理的基于物理硬件的通用平台。通过uCPE,SD-WAN服务提供商可以实现WAN的轻松部署、修改,以及客户端VNF的删除。vCPE是一种通过使用软件而不是专用硬件设备向企业提供网络服务的方法。通过vCPE,供应商可以大大简化并加速服务交付,远程配置和管理设备,并允许客户订购新服务或根据需求调整现有服务。vCPE是网络功能虚拟化(NFV)部署的主要推动力之一。

边缘设备的关键功能包括ZTP、动态隧道建立、WAN优化、自动化检测与服务质量(QoS)、动态功能服务链、应用程序识别、动态路径调整、安全。

(1)ZTP。ZTP是一种允许自动配置物理节点的机制,该机制将解放边缘设备的北向接口,使边缘设备与SD-WAN控制器形成一个从设备加电到设备与控制器互信互通的完整自动化部署的业务态。

(2)动态隧道建立。在SD-WAN场景中,动态隧道VPN技术支持使用动态的IP地址来建立企业自己的VPN网络,并由SD-WAN控

▼表1 边缘设备CPE、uCPE、vCPE功能对比表

功能	CPE	uCPE	vCPE
ZTP	√	√	√
动态隧道建立	√	√	√
自动化检测与QoS	√	√	√
WAN优化	√	√	√
动态功能服务链	--	√	√
应用程序识别	√	√	√
动态路径调整	√	√	√
安全	√	√	√
VNF+	--	√	√

CPE:客户终端设备
QoS:服务质量
uCPE:通用客户端设备
vCPE:虚拟客户端设备
VNF:虚拟网络功能
WAN:城域网
ZTP:零接触部署

制器来集中完成隧道的建立和路由的分发。动态隧道VPN技术主要有可扩展虚拟局域网(VXLAN)、通用路由封装(GRE)、无状态传输隧道(STT)等。

(3)WAN优化。在SD-WAN方案中CPE会支持WAN优化功能。WAN优化功能主要有以下技术实现:数据压缩,利用算法压缩/解压缩数据包头;数据消重,对高频次的数据进行编码并利用指针替换;内容缓存,统计热点内容,进行边缘存储和本地访问直接分发;传输控制协议(TCP)优化,利用优化TCP协议过程来改善标准TCP的拥塞控制和重传机制等[5]。

(4)自动化检测与QoS。SD-WAN技术方案根据实时网络路径传输性能(主要包括丢包率、时延、时延抖动、带宽利用率)来动态选择路径转发,弹性保障上层应用的服务质量。SD-WAN技术架构中将网络链路的性能检测分为被动方式和主动方式:主动测量方式主要利用探针技术主动探测业务流,以Internet控制报文协议(ICMP)、双向转发检测机制协议(BFD)、连接故障管理(CFM)、单向主动测量协议(OWAMP)技术实现为主;被动测量方式主要是通过在边缘设备上定制可自动统计和过滤网络相关性能指标的算法或协议栈功能。

(5)动态功能服务链。动态功能服务链与底层的物理拓扑相隔离,可通过SD-WAN技术架构中的服务编排器和控制器来自动创建、增加、删除、移动网络服务功能,提升了网络架构的可扩展性。动态功能服务链技术主要是通过将SDN技术与NFV技术相结合,即在业务编排器层通过策略驱动资源(包含网络资源、计算资源、存储资源等)的统一编排来组合不同服务功能,同时下发流量分类策略到控制器层来动态控制数据转发路径,实现面向用户业务的不同需求。

(6)应用程序识别。边缘设备的应用程序识别技术主要是采用深度包检测(DPI)技术,主要包含协议解析器、检测算法引擎、检测结果处理功能模块等。在SD-WAN技术架构中,DPI通过将业务流量的前几个数据包给协议解析器对应用层协议进行解析,同时并行镜像给检测引擎,检测引擎将业务流量与应用间的映射关系写入边缘设备的缓存数据库中,后续的同一业务流数据包将直接匹配映射关系,因此缓存数据库不再镜像给检测引擎而直接进行后续的检测结果处理。另一方面,后续检测结果处理功能模块会根据不同的应用ID与特征进行差异化的数据路径转发,进而实现完整的应用程序识别过程。

(7)动态路径调整。在SD-WAN技术架构中,动态路径调整的实现方式是将多个WAN线路绑定到一起,共同提供业务传输服务,尤其在检测到某个WAN线路的传输质量较差时,可以将业务直接切换到其他WAN线路或者均衡一部分业务流量到其他WAN线路。隧道绑定技术可以实现不同流不同线路、不同应用不同线路、不同数据包不同线路3种颗粒度的WAN传输。

(8)安全。安全的实现贯穿整个SD-WAN技术架构。SD-WAN技术架构一般通过集成认证服务器/公钥生成(PKI)服务器,或对接第三方的提供轻量目录访问协议(LDAP)/远程身份验证拨入用户服务的服务器(RADIUS)来实现身份认证服务功能,包括对边缘设备的ID注册认证、SD-WAN控制器的IP登记认证、VNF序列号注册认证等。在WAN传输的安全技术主要是通过2种密钥加解密的IPSec技术来保障。第1种是因特网密钥交换协议(IKE)身份认证的密钥,第2套是数据流加密的密钥。第2套密钥在传统方案中是通过去中心化加密通信框架(DH)来分布式计算;但在一些SD-WAN方案里则会直接由SD-WAN控制器来进行同步,并周期性地进行更新这个密钥,以实现关键帧加密保护。SD-WAN技术架构中的控制信道主要是将一般使用的路由协议嵌套在安全套接层协议(SSL)/传输层安全协议(TLS)/数据包传输层安全协议(DTLS)协议来实现加密。由于MD5的破解难度低,针对边界网关协议(BGP)安全,在SD-WAN技术方案种一般会选择嵌套在IPSec协议中。针对SD-WAN业务层的安全,一般使用缓存、访问控制列表(ACL)、防火墙(FW)、深度数据包检测(DPI)技术手段或者通过集成第三方的VNF如入侵检测系统(IDS)、入侵防御系统(IPS)、下一代防护墙(NGFW)功能来保障。

3 应用场景

根据边缘设备的部署位置,我

们将SD-WAN应用场景划分为3大类：分支到分支、分支到数据中心、分支到云。

（1）场景1：企业分支+企业分支场景。

企业在各个分支机构部署边缘设备，然后通过安全可靠的WAN专线来实现分支结构之间的互联互通。图3经常使用的解决方案中的WAN专线底层技术包括GRE、IPSec、VXLAN等等。这种应用场景将可支撑企业进行数字化信息化转型。

（2）场景2：企业总部（数据中心）+企业分支场景。

在图4的应用场景中，企业会在MPLS专线的基础上增加通过不同的ISP提供的Internet连接企业总部。在分支和数据中心所部署的边缘设备，支持基于网络的实时状态，将业务动态分发到总部和分支机构之间的多条路径上（WAN专线底层技术有GRE、IPSEC、VXLAN等等）。这种应用场景可以支撑企业面向各种弹性业务的需求，例如产品发布、电话会议、视频会议链路灾备等。

▲图3 企业分支+企业分支场景

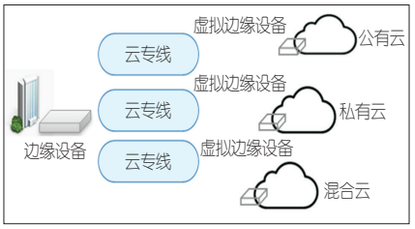
▲图4 企业总部（数据中心）+企业分支场景

（3）场景3：云中心（公有云/混合云/私有云）+企业分支场景。

SD-WAN服务提供商通过建立一张多云专网，支持接入各种公有云服务（Office 365、阿里云、腾讯云、亚马逊云服务、中国电信云等）、私有云、混合云等，支持对各种云服务进行优化。企业分支（或总部）部署的边缘设备，如图5所示，可以识别出云数据，并通过SD-WAN服务提供商建立的云专网进行承载，将业务流传输到云最近的接入节点和数据中心，以提供更好的云服务。这种应用场景可支撑企业业务容灾、集中备份、快速安全上云等。

4 结束语

当前的SD-WAN技术方案主要是针对混合城域网方案的技术优化。在面向云网协同的场景中，在企业网络中所部署的SD-WAN架构与云架构缺乏互联互通，各自部署独立的编排与运营系统，难以实现面向应用驱动的网云一体化、集成化、智能化、安全化的完整功能链的统一编排和资源动态调度，真正保障端到端业务的自动化、弹性化。另一方面，SD-WAN各个技术模块的标准化仍存在很多问题，如SD-WAN技术架构的规范定义，对应服务编排器、控制器、边缘设备的各自基本功能模块定义和南北向接口一致性规范等。在面向企业的SD-WAN商用方案中，SD-WAN技术架构应在安全、高可用等方面提供可信WAN技术，支撑未来网络的各种应用，如无人驾驶、视频会议、网络直播、AR/VR、工业互联网等。



▲图5 云中心（公有云/混合云/私有云）+企业分支场景

参考文献

[1] 中国互联网协会.软件定义广域网(SD-WAN)研究报告[R]. 2018
[2] IDC. IDC报告[EB/OL].[2019-01-22].http://news.idcquan.com/gjzx/150052.shtml
[3] 孙颖, 林睿, 聂世忠. 随选网络系统架构及关键技术实践[J]. 电信科学, 2018, 33(12): 142-147
[4] GORDEYCHIK S, KOLEGOV D. SD-WAN Threat Landscape [EB/OL].[2019-01-22]. https://arxiv.org/abs/1811.04583
[5] 张晨.SD-WAN进阶教程[EB/OL].[2019-01-22].https://www.sdnlab.com/20683.html#001

作者简介

柴瑶琳，中国信息通信研究院技术与标准研究所助理工程师，并担任SDN/NFV/AI技术标准与产业推进委员会SDN集成与测试工作组项目经理；现从事SDN/NFV领域相关的科研、测试和研发工作，主要研究方向为SDN；发表论文2篇。

穆琇博，中国信息通信研究院技术与标准研究所工程师，并担任SDN/NFV/AI技术标准与产业推进委员会SDN集成与测试工作组组长、SDN技术与规范合作组副组长；现从事SDN/NFV领域相关的科研、测试和研发工作，主要研究方向为SDN、云计算、大数据等；发表论文8篇。

马军锋，中国信息通信研究院技术与标准研究所主任工程师，并担任ITU-T SG11研究组Q5报告人、SDN/NFV/AI技术标准与产业推进委员会副秘书长；主要研究方向包括IP网络架构及路由技术、下一代互联网、SDN/NFV、网络人工智能等；主持或参与多项国家发改委专项、工信部专项三、科技部“863”专项等，先后完成多项国家/行业标准及ITU-T国际标准的制定工作。