多厂商云管网络及系统设计研究

Research on Multi-vendor Cloud Managed Network and System Design

曾昊阳，童　博，赵纯熙（中讯邮电咨询设计院有限公司，北京 100048）
Zeng Haoyang，Tong Bo，Zhao Chunxi（China Information Technology Designing & Consulting Institute Co.，Ltd.，Beijing 100048，China）

摘　要：
在云化时代，企业数字化转型需求迅速增长，传统企业的网络管理存在如开通慢、运维成本高等问题，无法达到转型目的。研究分析了云管网络的能力及其优势，并提出一种SD-Branch系统方案，解决了多厂商融合配置编排、统一运维管理的痛点，实现多厂商全生命周期的统一网络云管。

关键词：
云管网络；SD-Branch；网络配置编排；多厂商解决方案
doi：10.12045/j.issn.1007-3043.2024.09.015
文章编号：1007-3043（2024）09-0087-06
中图分类号：TN915
文献标识码：A
开放科学（资源服务）标识码（OSID）：

Abstract：
In the era of cloudization，the enterprise's demand for digital transformation is growing rapidly. The traditional enterprise network management method cannot achieve the objective of transformation due to various drawbacks such as slow deployment and high OPEX. It studies the abilities and advantages of could managed network and proposes a SD-Branch solution which can overcome the conundrum of multi-vendor network configuration orchestration and unified network maintenance thus achieve the objective of managing the multi-vendor network through the cloud throughout the entire network life-cycle.

Keywords：
Cloud managed network；SD-Branch；Network configuration orchestration；Multi-vendor solution

引用格式：曾昊阳，童博，赵纯熙. 多厂商云管网络及系统设计研究[J]. 邮电设计技术，2024（9）：87-92.

1 背景

1.1 传统企业专线与Wi-Fi分支网络现状

传统的企业分支互联通常使用MPLS-VPN专线[1]。MPLS-VPN专线是基于运营商专有网络资源实现的企业分支互联方案，需要安装专有电路和硬件设备。由于缺少集中配置下发及远程管理的手段，通常需要IT人员手动连接设备进行命令行（CLI）配置，对网络IT人员的网络配置能力和网络规划能力要求极高，同时也导致配置流程复杂，上线周期时间长，部署和运维成本高等问题。由此可见，专线虽然可以实现企业分支的基本互联需求，但是可扩展性低，存在不够灵活、管理困难等问题。

传统Wi-Fi网络通过路由器实现对无线网络的管理，通常可以实现以路由器为单位的接入设备管理和Wi-Fi配置管理等基础能力，对于小型分支，可以实现简单的局域网Wi-Fi覆盖。

1.2 传统网络方案中的问题与需求

目前，企业网络业务需求逐步丰富，传统的MPLS-VPN+Wi-Fi网络方案存在诸多问题。

随着各行业数字化转型的深入，企业业务的多元化对企业网络以及网络管理提出了新的要求。如连锁商超通常希望新门店更快地投入实际运营，这就要求分支网络能够迅速批量开通部署。而企业的数据

收稿日期：2024-08-05

中心则更加重视对突发情况的及时响应和定位处理，保障网络的稳定运行。此外，对于大型购物中心来说，除了提供高品质的Wi-Fi覆盖，还需要为消费者和商场管理人员提供停车导航、精确推送和客流分析等基于人工智能及大数据的增值业务。由此可见，企业的数字化转型主要以提升开通效率、降低运营成本、提供增值服务为目标。

MPLS-VPN作为传统广域网管理方式，在开通过程中，往往需要大量人工干预，配置的变更和扩展的时间周期也很长。传统专线可扩展性不足，和其他网络设备和基础设施的联动复杂[2]，同时入云性能较低，难以实现多样的个性化配置以及增值服务。传统Wi-Fi缺少大型分支统一管理、统一控制的能力，难以满足当前对网络安全管控监管和网络覆盖质量要求极高的企业业务场景。

在传统MPLS-VPN+Wi-Fi分支网络场景下，企业分支网络作为一个整体，不同网络设备的管理方式和管理途径却并不统一，主要存在以下问题。

a）传统网络场景设备和管理平台能力有限，导致配置不够灵活，可扩展性不足，统一管控能力弱。

b）不同控制器的配置能力、配置方法、配置逻辑不一致，学习成本高。配置冲突时，排查困难。

c）不同角色设备对应不同的设备控制器，日常巡检和运维排障时需分别接入，而部分设备甚至需要额外手动接入，大幅增加了运维的时间成本。

d）不同厂商控制器性能告警参数的展示维度和计算方式不同，在日常巡检和报表展示时需要额外进行口径统一。

以上问题导致企业网络运营困难，企业在数字化转型后不能降低运营成本，也不能满足故障快速响应的新需求。

2 云管网络技术分析

2.1 云管网络概念简介

云管网络一般通过云上的统一管理平台对客户网络设备，如AP、交换机、SD-WAN网关和防火墙，进行统一的远程云端配置管理和性能监控。由于将设备统一纳管至单独的管理平台，云管网络可通过资源的集中调度实现资源的高效利用，从而优化网络占用资源、节约网络运营成本、提升网络开通效率。由于平台部署在云上，可扩展、更灵活，便于引入大数据、人工智能、云计算等新兴技术，通过对客户实际业务数据的不断迭代，可构建专业的行业分析模型，易于按需包装为个性化增值服务，推进商业模式的创新，为客户业务运营赋能[3]。

对于云管网络和云管平台，所有纳管设备的配置、性能、告警等信息均实时在线更新，这使通过可视化GUI界面进行统一远程运维排障成为可能，可有效减少网络运营的开销成本。

在网络配置手段上，云管平台通过提供可视化的GUI界面进行远程配置，代替了传统网络的连接设备需通过CLI配置的模式，网络设备开通及配置修改简单高效。云管平台提供了统一的配置架构，支持多类型设备配置，提供全网可视化的编排能力[4]。

在网络运维方式上，云管平台提供多种设备的网络性能及告警查看功能，可远程监控物理设备和虚拟服务器的设备可达/可用性，实时采集CPU/内存利用率、磁盘空间、端口流量等关键性能指标，同时可以为每个性能指标设置多个阈值并获取相应告警通知。支持读取设备上报syslog和SNMP Trap等告警信息，主动识别网络问题并产生告警。

2.2 SD-Branch

SD-Branch是一种将分支广域网设备和局域网设备集合于单个管控平台的SDN技术，即WAN、LAN融合统一管理[5]。SD-Branch提供的架构可以将企业全部网络设备统一合并至一个集中管理框架之中，并将各类网络连接、安全、控制功能进行虚拟化，对设备及配置进行基于云的统一远程管理[6-7]。

基础的SD-Branch能力主要由SD-WAN和SD-WiFi能力组成，其中广域网侧（WAN侧）使用SD-WAN设备（SD-WAN CPE）建立的加密隧道进行企业分支间的互联[8-9]，局域网侧（LAN侧）使用SD-WiFi设备（AP）实现企业分支内部的Wi-Fi覆盖与终端设备接入[10]。

SD-Branch使用SD-WAN进行企业分支互联，相比于传统MPLS-VPN专线，该方案是更加灵活、更易于扩展、更易于部署、更低成本、可集中管理的分支互联解决方案。在SD-Branch技术架构中，分支互联通过互联网overlay网络实现[11]，相比于MPLS-VPN，该方案屏蔽了底层网络及设备的差异，降低了网络部署成本[12]。通过控制器一点管理全网设备，避免了手动登录设备的繁琐配置，提高了网络部署的速度。

在分支局域网方面，SD-Branch提升了LAN侧设备的可观测性，简化了LAN侧设备（AP、路由器等）的

部署和维护，可以实现对Wi-Fi设备的远程配置、监控、维护和升级等。同时，SD-Branch还可以提供更多的应用服务，如数据统计、流量分析、设备定位等，将网络管控和个性化增值服务延伸至企业局域网内部。

3 多厂商云管网络方案

3.1 系统总体架构

根据对云管网络技术的分析与调研，本文提出一种企业分支网络云管系统，该系统可部署在云端或企业客户侧，提供云规划、云部署、云运维的WAN、LAN融合网络全生命周期的云管理服务，其目标为满足企业数字化转型及上云需求。

系统使用SD-Branch技术，作为云管理平台对接多厂商控制器，面向客户提供一站式多厂商、多租户、全生命周期的企业网络云管理服务。以云管平台为基础的企业分支整体架构如图1所示，其中云管平台由统一门户、编排器、统一监控等核心模块组成。

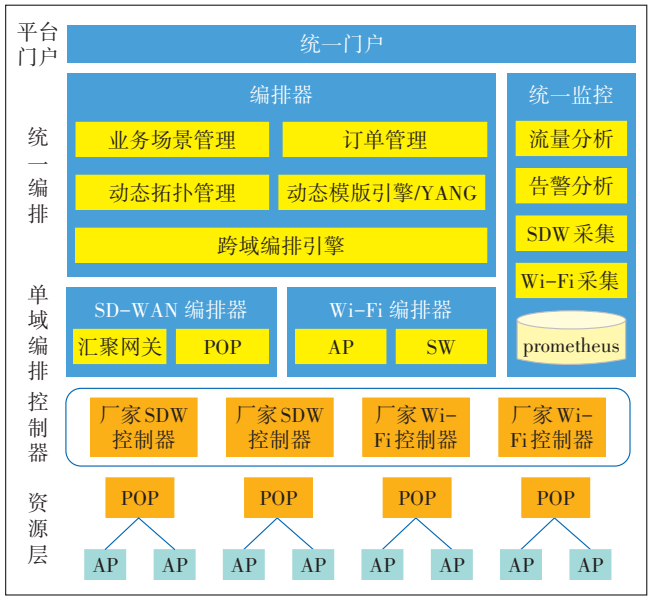

图1　系统总体架构

统一门户提供前端页面，提供基础业务数据的输入，如基础配置参数，以及展示数据的维度选择，如性能数据展示粒度和范围。

编排器由统一编排和单域编排2个部分组成。统一编排部分为WAN、LAN融合编排，可根据客户新建或修改的业务场景、组网拓扑、配置类型进行识别，负责区分各个配置是属于分支互联广域网（WAN侧）设备或是分支内部局域网（LAN侧）设备，并将其分别分配至对应的单域编排器，生成对应的订单记录，进行状态管理和配置过程追踪。单域编排部分接收来自统一编排的配置请求，通过对域内设备和资源的单独编排分配，调用对接的多厂商控制器，完成对应的配置请求，并将配置结果通知到订单记录中。

统一监控模块按照设备类型分类统一采集分析设备性能、告警数据，并向前端提供展示数据。

系统网络方案如图2所示。

3.2 多厂商管理底座

在实际企业网络场景中，由于成本、采购、迭代更新等一系列问题，不同地区的分支网络使用的设备生产商和型号可能不同，同一个分支下的不同网络设备的生产商往往也不同。为了全面管理企业网络，系统需要有良好的普适性和可开放性。为此，在设计之初便要求系统能够支持多厂商管理，各项功能和数据结构均需要屏蔽厂商间的差异。

系统使用模板化数据和资源统一对接多厂商控制器及网关路由器、交换机、AP等设备，向上屏蔽厂商设备差异。系统通过多租户资产仓库统一纳管设备资源，管理设备型号、类型、厂商信息，并将设备分配至特定租户以开通网络。统一资产管理保障了设备厂商及类型的可扩展性，任何对接适配标准接口的厂商设备均可通过平台进行纳管。

在网络配置规划设计中，平台按类型及角色从租户库存导入设备，不限制设备的厂商选择。平台抽象出通用配置，只根据设备类型（SD-WAN网关、交换机、无线AP）区分设备角色和可配置项，根据通用配置设置模板化的标准配置下发接口。单域编排在进行配置编排的同时，可根据不同厂商控制器的不同实现方式进行流程适配和异常处理，从而对上屏蔽多厂商差异。由于使用通用配置和通用协议进行设备间的交互，异厂商设备之间只需通过平台进行配置管理即可进行正常网络交互。

在网络运维监控方面，系统统一监控模块提供标准模板化的相关接口，通过适配转化采集的多厂商控制器的相应数据，向上提供统一的性能、告警展示以及运维工具。

系统的多厂商管理底座提供从网络开通到后续维护的全流程多厂商感知和统一编排。平台底层适配多厂商控制器及设备，可根据设备类型统一进行标准化编排，提供统一的视图及工具，对使用者屏蔽多厂商的配置及实现差异，避免因设备升级换代、分批次采购、机房搬迁割接等造成的网络设备管理混乱、

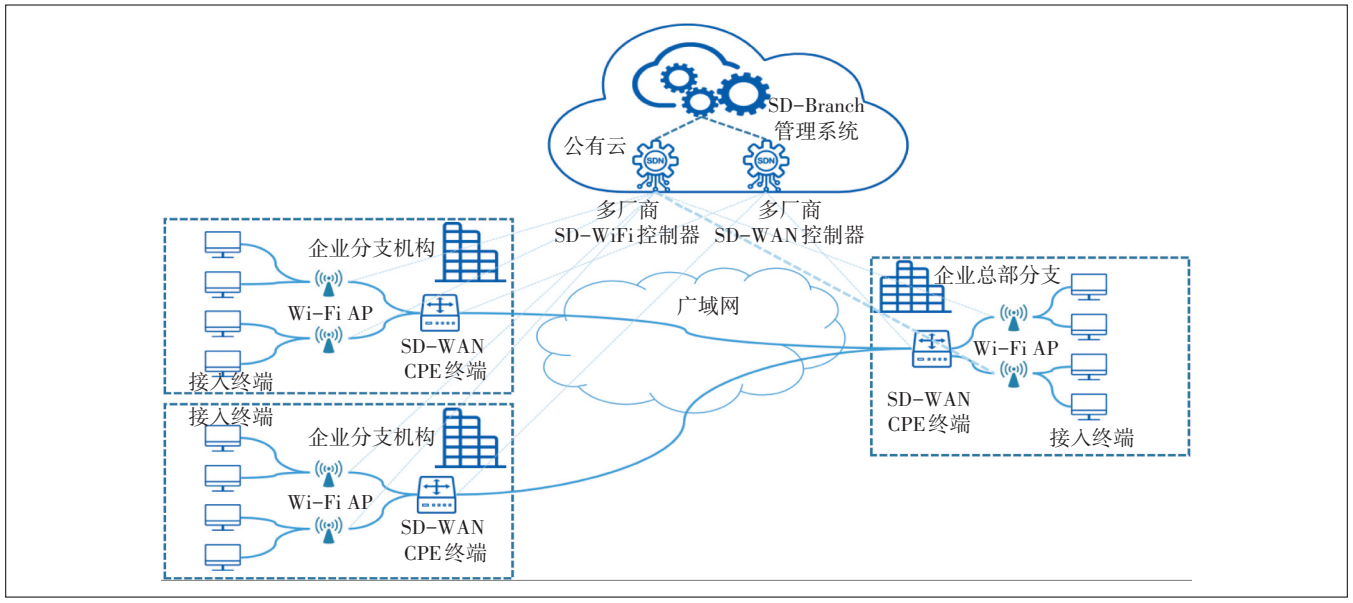

图2 系统网络方案

部署管理系统繁多却相互孤立的问题，保障了系统的开放性、可扩展性和普适性，同时简化了厂商适配对接管理。

3.3 灵活网络设计规划能力

系统提供全云化的网络编排设计功能，可场景化设计分支内网和分支互联方案，规划设备类型、设备数量、设备连线、设备配置，自动编排企业分支互联拓扑。

在前期规划中，分支网络的业务场景和施工需求需要逐步明确，网络设备的配置通常需要经过多次设计、规划、调整。而在完成部署之后，由于需求的新增或改动，网络配置也需随之进行变更。因为此类变更可能影响客户关键业务节点的网络连接，所以通常在不影响业务的时间窗口内以割接的形式进行。由此可见，对于云管网络系统，提供网络设计功能有助于分支网络开通的前期规划以及割接的预演准备。为此，系统将企业组网分支的网络配置分为设计态和配置态2个状态，网络配置管理模块负责2个部分的统一管理，为使用者提供网络规划设计能力。

作为用户网络规划，系统设计态配置可以随时随地进行修改。虽然是以客户实际分支设备为对象，但设计态配置并不会直接下发至客户设备，避免了业务运行期间因网络配置变化导致的故障。客户进行分支设计时，支持由平台场景化自动组合SD-WAN网关、交换机、AP等网络设备，并由系统提供现场端口接线指导。针对每一种设备，支持对其通用配置进行无限制的填写/修改。设计态配置可看作施工交付之前进行设计、模拟、预演使用的计划配置，有助于提前发现与解决问题，从而减少施工/割接时间窗口内出现异常的概率。

系统配置态配置作为实际下发至客户设备的配置，需与实际控制器和设备上的配置信息随时保持一致。实际生效的配置态配置信息是由实际下发成功的设计态配置组成的，在组网新创且未下发配置时，其配置态信息为空。组网中分支在设计完成后即可调用控制器进行配置下发，编排器将不同配置信息分别拆成不同子进程下发。对于下发成功的子进程，其对应的配置将在设备上实际生效。将此类下发成功的配置进行叠加，即可获得设备上实际运行的真实配置，使用者不必登录多个控制器即可查看全量设备的运行配置。

在设计态完成设计后，网络设备配置可定时自动下发至设备，更新配置态配置。网络在线管理设计是重要的交付工具，从需求讨论直至正式交付之前，可在网络拓扑规划和网络配置管理方面提供必要支撑，避免在正式下发后因临时修改各类配置导致浪费窗口期的宝贵时间。配合控制器的离线配置能力，该功能可实现设备即插即用，大大提升业务开通效率。

3.4 网络配置自动高效可靠编排

系统具备自动网络配置管理编排的能力，可自动编排网络配置下发顺序和回滚逻辑，在保障系统配置能力稳定性的前提下，大幅简化网络人员配置操作，显著提升网络分支开通交付效率。

针对网络设备控制器的API接口式配置下发存在的编排难点如下。

a）并行请求导致进程资源抢占。因为各并行进程存在不同的限制逻辑，不同设备厂商为避免控制器和设备数据混乱，往往会添加逻辑锁以限制某个进程，如对于同设备的2个并行配置请求，只接受先收到的一条而放弃第2条。对于上层系统而言，逻辑锁会导致系统并行订单的成功不可预测，需要引入繁琐复杂的异常处理机制以保证系统与控制器数据的一致性，同时需要再引入更严格的状态锁，这增加了对业务的限制和系统的编排难度。

b）批量异常订单处理。针对错误的配置请求，厂商设备和控制器配置了回滚能力作为逃生通道，避免设备故障。而对于上层系统，一次配置业务请求可能对应多项或多次控制器调用配置，在面对异常订单时，若上层系统的回滚不全面，则极容易造成系统和控制器配置不对账的局面，后续操作会受到极大影响；若上层系统的回滚动作粒度过大，则会造成配置成功的设备和配置一同回滚，增加重复劳动。

为解决第1个问题，系统默认协助编排配置下发逻辑，通过内部定义配置层级，制订了不同设备类型并行、同类型设备由上到下批量按需串并行的总处理逻辑。例如，SD-WAN网关设备和Wi-Fi设备配置无强相关联系，可并行同时下发；而SD-WAN网关中涉及相同站点设备的配置变更则存在关联，需串行下发。再例如SD-WAN网关端口配置与端口的ACL访问限制配置，属于主配置和子配置的关系，若主配置失败，则子配置必定失败，因此两项业务需串行，且端口配置一定优先于ACL配置。系统通过识别订单请求间的串并联关系和从属关系，自动编排接口下发顺序和配置入参，以避免控制器状态锁造成的订单异常，无需在平台引入更严格的状态锁，保障了业务的灵活性。自动编排配置简化了网络配置的繁琐程度，降低了引入人为错误的概率，大幅降低了对IT人员的人数要求和技术能力要求，也降低了企业网络的维护成本。

针对第2个问题，在传统处理方式中，全部设备操作成功才视为成功，任一设备失败则订单失败，并将订单配置全量回滚。这种处理方式虽然简单易懂，但容易影响实际交付的效率，多个机房的多项设备可能因某项错误配置而全量回滚，严重影响交付体验，增加交付现场重复劳动。

针对批量订单，本系统摒弃了传统处理判断方式，提出了配置部分成功的逻辑。对于同类型多设备订单，以设备为单位，只回滚失败设备的相应配置，保留成功设备的配置，避免了因部分订单失败而回滚订单中全部设备的全部配置。对于不同类型但同设备的配置，判断配置之间的从属关系，若配置间无主从关系，则只回滚失败的配置项，若存在主从关系，则回滚失败的配置项和其配置子项，避免系统和控制器的配置不对账。以2台SD-WAN设备额外开启端口及端口上的ACL策略为示例，展示订单部分成功的逻辑。

通过设计态和配置态的对账功能，系统可自动识别下发失败的配置信息，即设计态存在但配置态不存在的配置，IT人员可直观查看失败的部分配置，并重新修改下发。系统的部分成功逻辑结合配置对账功能，保障了平台编排能力的稳定性和可靠性，同时可大幅提升批量业务下发和多项配置修改场景下的交付效率，是应对企业快速扩张场景的必备能力。

3.5 多厂商统一运维管理

网络开通进入正式运营后，其核心需求是故障少、故障快速定位恢复，以确保业务的稳定运行。本系统作为多厂商的统一管控系统，需要在提供多厂商统一监控工具基础能力的同时，支持更全面的远程排障工具和标准故障处理流程，帮助标准化规范运维人员排障、巡检操作。

调研发现，不同厂商控制器性能告警参数的展示数据和计算方式不同，多厂商的统一管控需要对多厂商数据内容、格式、单位等进行标准化处理。系统纳管多种网络设备时，不同设备角色之间的性能采集维度不同，系统需根据不同设备角色，定义不同的标准模板化的性能采集接口、告警上报接口和探测维护接口，接口能力和数据均为各厂商通用。不同厂商上报采集数据的规格不同，系统通过适配模块将采集的多厂商控制器数据进行转化与整理。通过以上2种举措，形成统一且通用的多厂商多类型设备性能告警展示和运维工具。

系统提供实时网络监控功能，实时采集分析客户网络全量SD-WAN网关、交换机、AP设备的性能数据，根据设备性能、历史告警加权计算出设备健康度评分及稳定度评分，再根据设备角色、设备评分加权计算该分支网络整体健康度与稳定度评分，综合展示网络中的异常设备及分支运行状态，为故障定位和日常巡检提供指引参考。由于采集的基础数据是多厂

商统一的，设备和分支的评分也保证了无厂商差异化。通过网络拓扑可视化叠加设备性能及评分，运维人员可直观全面地了解网络运行状态，达成客户网络可见，实时监控网络中的全部设备。

网络告警模块整合多厂商上报的告警信息及数据，对统一告警信息进行多维关联分析，提供智能、精确、可观测的网络告警能力，支持根据设备性能指标自定义多种告警规则，可通过多种途径前转至网络运维人员。配合智能告警抑制、告警自愈，该模块在保障监控业务高质量扩展的同时，不会让管理人员被无限的告警所淹没。系统建立告警信息库，支持对历史告警数据的整理汇总，对告警信息进行标签化，构建告警信息库，支持对标签化告警信息中相似、相关的告警进行关联、分析、去噪，并将告警信息进行智能聚合，明确各告警事件之间的拓扑关系，形成告警知识图谱。通过专业网络运维人员对各告警信息进一步的根因分析，明确触发告警的根本原因，完善告警知识图谱。对告警图谱中的信息进行沉淀、分析、特征提取，通过大数据分析实现自动快速故障定位，配合自动化脚本及接口执行，实现常见告警的自动故障修复。

针对网络运维人员，系统通过运维工作台提供网络管理工具及故障诊断帮助指南，简化网络运维操作，实现常用故障诊断工具的储备和使用，构建网络运营人员的统一网络故障诊断工具仓库，增强远程故障排除能力。系统通过一键巡检功能，进行全方位、可配置的跨厂商分支网络体检，对包含网络连接状态、设备运行状态、设备安全等级等项目进行主动探测，将已有告警事件及告警覆盖不到的指标进行人工统一检查，及时发现网络隐患。自动生成故障处理报告和每月运维报表，做到故障内容可复盘，可追溯，有助于将繁杂且零碎的运维工作标准化、流程化。

4 结束语

本文调研了当前传统企业网络管理现状，发现当前网络管理中存在交付慢、运维难、异厂商等问题。本文分析了云管网络技术的概念及实现场景，并基于SD-Branch技术，设计了一种多厂商云管网络系统方案，着重于多厂商统一管理和简化网络配置和运维。在网络开通交付方面，通过灵活的在线网络设计规划功能和可靠的自动网络配置编排，实现了网络设备即插即用和分支快速开通。在网络运营运维方面，多厂商底座支持网络故障主动探测、性能告警可视化统计、常见故障在线修复，有效降低了企业运营成本。

系统作为企业网络的统一管控方，提供一站式多厂商全生命周期的云化企业网络管理服务，可节约网络运营成本，提升网络规划及开通效率，为企业数字化转型支撑赋能。

参考文献：

[1] BLIDBORG E. An overview of monitoring challenges that arise with SD-WAN[D]. Stockholm:KTH Royal Institute of Technology,2022.

[2] RAJAGOPALAN S. A study on MPLS Vs SD-WAN[C]//Computer Networks,Big Data and IoT. Singapore:Springer,2021:297-304.

[3] 方剑飞. 云管理:颠覆传统的管理方式[J]. 宁波经济(财经视点),2013(7):59.

[4] 华为. 云管理网络[EB/OL]. [2024-01-04]. https://support.huawei.com/enterprise/zh/doc/EDOC1100197639/.

[5] KERRAVALA Z. Aruba's SD-branch addresses WAN and branch transformation [EB/OL]. [2024-01-03]. https://www. eweek. com/networking/aruba-s-sd-branch-addresses-wan-and-branch-transformation/.

[6] SAN JOSE C. Sify selects versa SD-WAN and SD-branch for cloud@core networking portfolio [EB/OL]. [2024-01-03]. https://versa-networks. com/news/2018/sify-selects-versa-sd-wan-sd-branch-cloudcore-networking-portfolio/.

[7] Versa Networks. Versa networks goes beyond SD-WAN to software-define the branch (SD-Branch) [EB/OL]. [2024-01-04]. https://versa-networks.com/news/2017/press-release-versa-sd-branch/.

[8] FOREST J,SINGH N,LERNER A,et al. Magic quadrant for WAN edge infrastructure [EB/OL]. [2024-01-03]. https://www. gartner.com/en/documents/4005922.

[9] GASIOR D. Resource allocation for software defined networks[M]. Cham:Springer,2020.

[10] Aruba. Aruba SD-branch solution helps videotron expand key business services [EB/OL]. [2024-01-04]. https://www. businesswire.com/news/home/20200811005002/en/Aruba-SD-Branch-Solution-Helps-Videotron-Expand-Key-Business-Services.

[11] SEGEČ P, MORAVČIK M, URATMOVÁ J, et al. SD-WAN-architecture,functions and benefits[C]//2020 18th International Conference on Emerging eLearning Technologies and Applications (ICETA). Piscataway:IEEE,2020:593-599.

[12] LUCIANI C. From MPLS to SD-WAN:opportunities,limitations and best practices[D]. Stockholm: KTH Royal Institute of Technology,2019.

作者简介：
曾昊阳，助理工程师，硕士，主要从事网络创新产品研发设计工作；童博，高级工程师，硕士，主要从事新型IP网络技术、SDN及网络创新产品的研究、研发工作；赵纯熙，工程师，硕士，主要从事网络创新产品研发设计工作。