SD-WAN网络架构及产品应用探索

Network Achitecture and Product Exploration of SD-WAN

王胜志[1]，章道勇[2]（1. 中国联通徐州分公司，江苏 徐州 221000；2. 中国联通无锡分公司，江苏 无锡 214021）
Wang Shengzhi[1], Zhang Daoyong[2]（1. China Unicom Xuzhou Branch, Xuzhou 221000, China; 2. China Unicom Wuxi Branch, Wuxi 214021, China）

摘　要：
近年来，作为SDN比较成熟的应用形式，SD-WAN以其独特的优势吸引了产业界的广泛关注，电信运营商和很多互联网公司都推出了SD-WAN产品。简要介绍了SD-WAN的基本概念，分析探讨了SD-WAN的基础架构、产品应用、运营模式，为SD-WAN的网络建设规划提供了一定的参考。

关键词：
SDN；SD-WAN；WAN；网络架构；解决方案
doi：10.12045/j.issn.1007-3043.2021.03.016
文章编号：1007-3043（2021）03-0071-06
中图分类号：TN919
文献标识码：A
开放科学（资源服务）标识码（OSID）：

Abstract：
In recent years, as a relatively mature application form of SDN, SD-WAN has attracted extensive attention from the industry with its unique advantages. Telecom operators and many Internet companies have launched SD-WAN products. It briefly introduces the basic concept of SD-WAN, analyzes and discusses the infrastructure, product application and operation mode of SD-WAN, which provides a certain reference for the network construction planning of SD-WAN.

Keywords：
SDN; SD-WAN; WAN; Network achitecture; Solution

引用格式：王胜志，章道勇. SD-WAN网络架构及产品应用探索[J]. 邮电设计技术，2021（3）：71-76.

1 SD-WAN基本概念

1.1 传统WAN面临的挑战

依托于电信运营商完备的基础承载网络，在2B业务构成中，政企专线始终占据重要的位置。伴随着通信技术的演进，WAN经历了从低速率到大带宽、从多协议到IP化、从单一网络到云网融合的发展和演变。然而随着业务应用的快速发展，其在给客户带来巨大价值增益的同时，也面临很多问题和挑战。

收稿日期：2021-02-04

成本较高，价值密度降低：因为技术的发展和竞争格局的推动，无论采用何种方式承载，专线电路业务的成本和价格都在不断下降。然而，接入成本的降低速度远远赶不上价格降低的速度，这导致专线电路价值密度不断走低（见图1）。

网络结构复杂，组网灵活度差：由于过于依赖物理网络设施，同时网络维护工作采用多级分段的管理维护体系，MSTP、IPRAN、PTN等基础网络在配置专线电路过程中往往采用与企业组织架构相匹配的分段配置、分段管理、分段维护的业务流程，这导致业务开通时间长、业务灵活性差，难以满足快速开通、灵活部

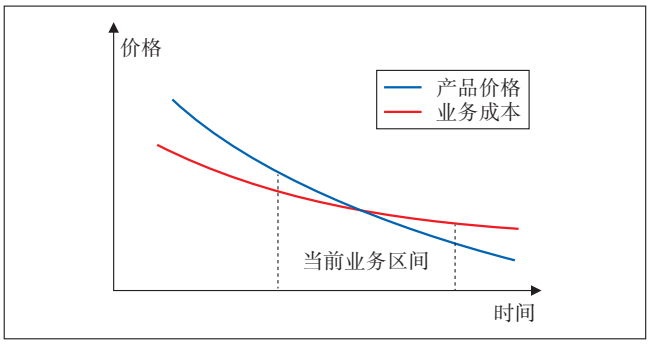

图1　成本与价格曲线

署等业务需求。

网络状态的呈现方式较为分散：目前运营商都尝试建立了相应的政企业务网管系统。但系统的实现主要是通过专业网管系统告警采集和业务匹配来实现，仅能实现简单的监控功能，无法实现统一集中的网络管理，更无法实现业务状态的端到端整体呈现。另外，随着云业务的快速发展，根据应用需求的动态调整将成为常态，传统基于MSTP、OTN的承载方式已经无法满足。

1.2 SDN和NFV

为了解决传统WAN基础网络所面临的问题，网络功能虚拟化NFV和软件定义网络SDN应运而生。NFV是SDN实现的基础，它通过将网络设备的控制功能软件化、虚拟化，实现设备的软硬件解耦。当然，这种虚拟化的控制功能是开放的、可编程的，因此可以实现更加灵活的网络功能和网络资源调度。

SDN即软件定义网络，它是一种新型网络创新架构，是网络虚拟化的一种实现方式。它的核心是通过将网络设备的控制与数据转发分离开来，从而实现网络流量的灵活控制，使网络资源变得更加智能，从而为网络及应用的创新提供更好的平台。

近年来SD-WAN作为SDN在广域网场景下的应用得到了产业界的广泛认同，开始应用于企业网络、数据中心、互联网应用和云服务场景。同时，SD-WAN的产品和服务模式也对运营商传统的网络建设和维护模式提出了挑战，为基础通信网络虚拟化、软件化提供了相应动力和契机。

1.3 SD-WAN的价值

对于运营商或者企业用户来说，SD-WAN的价值主要体现在几个方面：能够快速高效地实现多网络、云网融合的互联，满足复杂业务场景的应用需求；能够通过集中管控和即插即用实现业务的快速部署，降低业务交付和运维成本；可以根据不同的应用提供路径优选策略，以保证高质量的应用体验。

2 SD-WAN网络架构

2.1 SD-WAN基础架构

SD-WAN解决方案整体架构主要包括网络层、控制层、业务层3个层次，如图2所示。

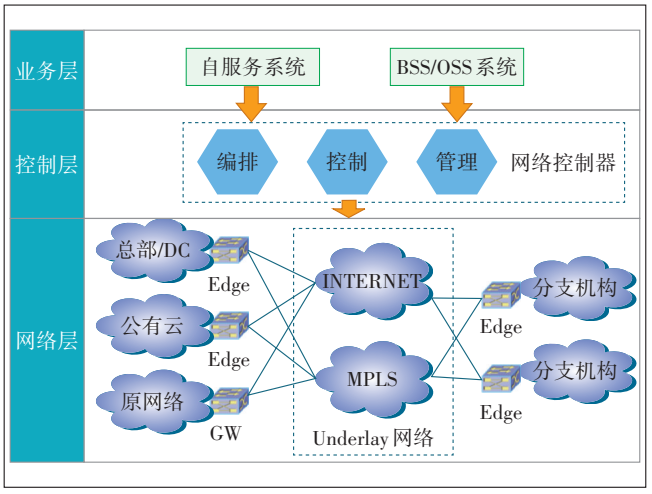

图2　SD-WAN解决方案整体架构

网络层又可以分为物理网络和虚拟网络2个层次，如图3所示。物理网络被称为Underlay网络，如MSTP专线、MPLS、Internet等。虚拟网络被称为逻辑网络，它是根据业务策略构建于物理网络上的Overlay网络。虚拟网络可以服务于多个租户，也可以服务于同一个租户的不同业务。在SD-WAN网络中，主要使用边缘设备Edge和GW网关设备2种设备。其中Edge一般为即插即用的CPE设备，它通过隧道技术实现多个设备间的WAN链路连接。GW设备用于SD-WAN和企业存量网络之间的互通，以保证客户网络的延续性。

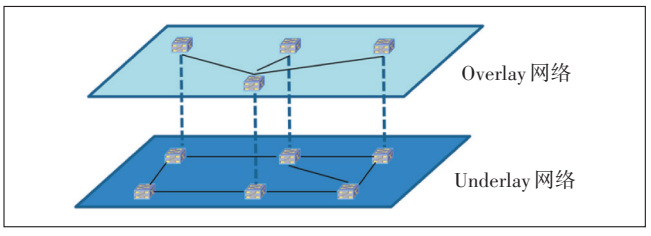

图3　网络层2层结构

控制层是“软件定义”的核心，它的主要组件是网络控制器，它一般具有业务编排、网络控制和网络管

理功能。编排功能主要实现业务应用的抽象建模、编排和配置下发。网络控制器通过业务编排对企业WAN进行抽象和定义，驱动网络控制器实现网络拓扑的配置。业务编排分为2种，一是WAN网络拓扑的业务编排，如站点创建、链路创建、拓扑定义等；二是网络策略的编排，如应用选路、QoS、广域网优化、应用识别、安全策略等。网络控制器的控制功能主要实现对SD-WAN网络层的集中控制，以实现控制平面和转发平面的分离，主要包括VPN路由分发、VPN的创建和修改、隧道的创建和维护等。网络控制器的管理功能主要实现WAN网络的管理和运维功能，包括告警管理、性能管理等，同时对客户网络拓扑结构、故障、性能等运维信息进行多维度的呈现。管理组件一般通过NETCONF和HTTP2.0协议实现对设备的管理。其中NETCONF主要实现告警、日志管理等，HTTP2.0主要实现性能等信息的采集。

业务层南向对接网络控制器，北向通过业务UI界面实现业务层面的管理和交互。这可以通过2种方式实现：一种为SD-WAN解决方案提供商开发的自服务系统，它可以提供全生命周期的、端到端的业务配置和交付流程；另一种方式是依托于运营商的BSS/OSS管理系统，它们通过网络控制器开放的北向API开发实现全流程业务管理功能。在业务开放初期可以采用第1种方式作为过渡，然后通过开发迭代，最终打通运营商B/O域的全业务流程。

2.2 主要接口及通道

SD-WAN网络控制器在整个体系结构中处于核心位置，它通过不同的接口协议实现与网络层和业务层之间的交互，如图4所示。

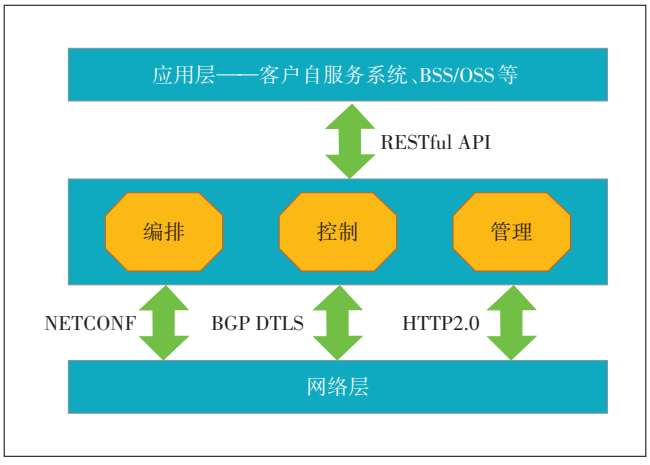

图4　主要接口协议

南向接口协议：NETCONF和HTTP2.0协议，用于网络控制器对网络层的统一管理和配置，网络控制器通过NETCONF协议给Edge或GW下发配置。Edge、GW设备则通过HTTP2.0向网络控制器上报性能信息，通过NETCONF协议上报告警信息。

北向接口协议：网络控制器通过RESTful API接口与业务层各组件交互，RESTful API是基于REST设计准则实现的接口方式。应用层外部程序可以通过HTTPS访问RESTful API，其管理网络资源对象的方法主要有GET、PUT、POST、DELETE等。运营商BSS/OSS系统或自服务系统皆通过RESTful API的调用开发实现对网络控制器的管理，进而实现对整个SD-WAN网络以及业务全生命周期的管理。

通过各种接口及协议，SD-WAN系统将建立管理通道、控制通道、数据通道等3种逻辑通道。

管理通道是网络控制器与网络层设备之间的交互通道，如Edge、GW等，用于网络配置信息和运维信息的下发和上传。在SD-WAN系统中，管理通道最先建立，用于整个系统的初始化配置。管理通道建立后，系统将建立控制通道。网络控制器利用控制通道完成网络层组网、路由编排以及网络拓扑的建立。另外，网络控制器也通过控制通道转发路径策略信息，如VPN拓扑、隧道信息等。管理通道和控制通道建立以后就基本完成了系统的初始化工作，此时系统需要建立数据通道，用于Edge、GW以及其他网络设备之间的数据传输，数据传输一般采用IPSec进行加密，以保证其安全性。

2.3 站点及Edge

在部署SD-WAN应用过程中，需要考虑传统站点、SD-WAN站点和云站点等3种企业站点。传统站点是企业的存量网络设备，并不纳入SD-WAN网络控制器管理，但是它也有与SD-WAN互通的需求。SD-WAN站点配置于企业总部、分支机构或DC中，由SD-WAN网络控制器集中统一管理，进行业务的编排组网。云站点是SD-WAN站点的一种特殊形态，应用在公有云、私有云环境下，用于企业各机构与虚拟机VM之间以及各VM、各应用之间的互通。

企业WAN网络连接企业各站点，不同类型的站点通过不同的边缘设备Edge接入网络，即CPE设备。CPE一般应具备即插即用、二层交换、三层路由转发功能。在SD-WAN网络中，依据不同的站点应用环境还衍生出其他不同的形态，如具备广域加速、负载均衡、

安全防护功能的uCPE，应用在云网环境中通过软件形式实现的vCPE等。

CPE连接了站点的内外侧网（LAN侧和WAN侧）。

在SD-WAN解决方案中CPE需要考虑多种WAN接入方式，如Internet、MPLS VPN、LTE，并在其中配置路由选择策略。其中LTE链路适用于一些特殊场景，如工地、河堤、道路等线路接入困难或成本过高的场景，或作为其他链路接入形式的故障灾备路由，以提升站点连接的安全性。

CPE的LAN侧对应企业站点内网，其接入方式和内网的组网形式相关，对于规模较小、结构较为简单的网络，通常采用二层组网的方式，CPE直接连接内网以太网交换机，CPE作为内网的网关配置。对于规模较大、结构较为复杂的网络，则往往采用三层组网方式，此时，CPE需要根据站点网络的实际情况配置相应的路由协议，一般情况下，其配置由网络控制器根据编排策略自动下发完成。

在实际的业务流程中，CPE即插即用过程一般分为3个步骤。第1步，SD-WAN服务提供商/电信运营商在网络控制器中完成CPE设备的登记录入，一般情况下，网络管理员需要预配置CPE的WAN接口IP地址，用于CPE和网络控制器的自动连接。第2步，CPE被邮寄到企业站点并完成物理连接。第3步，网络控制器和CPE通过IP地址信息建立连接，同时根据业务编排向CPE下发配置，完成业务开通。

2.4 业务体验保障

企业应用有多种多样的类型，这些不同的应用类型有不同的体验需求。如电话会议、视频会议需要较低的时延。在传统的WAN网络中，这些不同的应用无差别地承载在同一张网络上，被不加区别地进行转发和处理，虽然MPLS可以提供简单的QoS，但无法实现更复杂的体验保障和选路策略。SD-WAN解决方案包含多维度的应用体验保障方案，其作为可选功能构建于不同SD-WAN服务商的产品架构中，下面是几种常见的业务体验保障方案。

应用识别：能够对不同的应用进行有效的识别是应用体验保障的前提，SD-WAN解决方案可以通过协议识别、首包识别、特征识别、DNS识别等多种技术实现对不同应用的识别和判断。

应用选路：选路的前提是链路质量检测，SD-WAN通过丢包、时延、抖动的检测技术实现链路质量检测，进而通过选路策略进行路由优化。应用识别和应用选路结合就可以实现不同的选路场景，如链路质量选路、负荷分担选路，应用优先级选路等。

QoS保障：通过应用限速来保障不同的应用体验。

广域优化：通过各种算法技术改善WAN链路传输质量，如抗丢包优化、传输层优化、数据优化、应用协议优化、数据去重压缩等。

2.5 系统安全

无论是采用MSTP、OTN、IPRAN/PTN，还是采用MPLS承载，传统的WAN网络都处于封闭或者准封闭的网络环境中，其Underlay基础网络以及网络中的管理控制节点，如各系统的专业网管中心等都处于相对独立的内网环境中。同时，一个WAN的不同承载段落也往往分散于不同的网络系统，如跨境跨域组网。这样的网络架构和环境保证了相对健壮的网络安全。

但是，在SD-WAN解决方案中，由于采取了完全不同的架构模式，网络安全面临着巨大的挑战，具体来说，主要有以下2个方面，同时这2个方面的安全挑战也对应着SD-WAN安全架构中的2个层次，即系统安全和业务安全。

由于采用集中控制的模式，网络控制器在整个架构中处于核心位置，其各个组件的部署方式、安全防护是SD-WAN系统安全首要考虑的问题。

由于Underlay网络的多样性，尤其是Internet、云网环境的大量使用，SD-WAN网络环境走向开放，在开放的环境中，攻击、病毒、非法侵害的风险大大增加。

因此，SD-WAN架构是综合性的解决方案，需要整合解决方案、设备、安全、云平台、运营等全部生态链资源。在安全方面，更需要联合安全服务提供商构建完整的安全解决方案，综合利用分布式部署、防攻击、防入侵、防病毒以及数据加密、认证、鉴权等多种技术实现系统安全防护和业务安全防护。另外，控制层各系统的双活、多活等灾备方案也应充分考虑。

3 业务运营模式

从上文对SD-WAN的网络架构分析中可以看出，SD-WAN并不是具体的基础网络产品，它必须依托于原有的Underlay实体网络环境，因此，SD-WAN是一种综合性的解决方案，是一种更加灵活智能的服务提供模式。这种新的服务提供模式必然对应着新的商业运营模式。结合当前业界发展现状以及未来演进趋势，SD-WAN商业运营可以采用运营商公共产品业务

模式、运营商代建模式和企业自建模式等3种模式。

3.1 运营商公共业务模式

运营商公共业务模式是由电信运营商自建SD-WAN公共产品服务平台及运营支撑体系。目前各家基础电信运营商都已经尝试建立了其SD-WAN产品品牌。运营商SD-WAN公共产品服务体系建设应包含以下关键部分。

SD-WAN平台建设：主要完成控制层网络控制器等关键组件部署，实现业务编排、网络控制和网络管理功能。平台应支持多租户管理。

基础网络建设：网络层合理规划部署IWG网关设备，以实现企业SD-WAN网络与MPLS网络或者分组传送网的互通。同时运营商骨干网边缘需要规划部署POP GW，企业分支机构Edge可以通过POP GW构建Overlay隧道以实现第三方运营商的网络穿透。

支撑系统建设：运营商需要根据自身组织架构和服务支撑体系，通过SD-WAN控制层北向接口API开发建设各业务支撑系统，如BSS/OSS、订单系统、客户自服务系统等，以此打通业务全生命周期管理流程。

Edge设备选型：根据不同的应用场景确定多层次、多型号、标准化的设备，设备应充分解耦。同时建立设备在业务创建、维护、拆除等情况下的配送体系。

在SD-WAN承载国际WAN业务组网的场景下，由于网络安全和信息安全的工作要求，目前无法实现跨境全程全网的SD-WAN架构，出境链路仍然需要MPLV VPN承载，境外网络需要由运营商国际公司或者当地运营商负责支撑。

另外，目前通信市场已经涌现出很多SD-WAN服务提供商，这些企业大多衍生于IT企业、互联网企业、通信设备制造企业等。他们通过自研产品或者通过SD-WAN解决方案提供商搭建平台转售产品。这些企业往往具有鲜明的行业特质，一般深耕于一个或多个特定的行业市场，并依靠快速灵活的管理和创新机制，成为2B市场不可忽视的竞争力量。

3.2 运营商代建模式

对于部分大型企业（IT或互联网企业），如客户有自建SD-WAN规模组网需求，电信运营商可以协助企业建设SD-WAN业务平台。根据客户需求和技术能力，项目建设可以采用ICT项目运营模式或交钥匙项目建设模式。在业务运营过程中，运营商可以与企业合作探讨代管代维等延伸服务，并不断根据5G、AI、云计算等技术的演进推动企业SD-WAN业务的更新迭代。这种运营模式下的SD-WAN架构仅需要支持单租户即可。

3.3 企业自建模式

企业从解决方案提供商采购SD-WAN解决方案，通过其自有技术能力完成业务部署和运维，用以构建企业自身的WAN基础网络，并不对外运营。企业自建模式对企业的技术能力要求较高，有较高的技术门槛，因此这种企业往往是大型互联网公司、公共服务产品提供商、大型云产品服务商或相对封闭的行业系统，如交通、物流、金融等部门。

4 客户及产品应用分析

4.1 专线客户类型

通信产品丰富多样，客户需求同样丰富多样，不同的用户有不同的业务需求，根据政企客户行业性质、网络需求、业务规模、安全需求等多种商业或技术特质，将专线类业务客户需求类型分为以下3类。

价格倾向类：对产品价格较为敏感，主要集中于中小企业、连锁加盟的零售或服务企业等。传统场景一般采用MPLS VPN、自建VPN等方式组建企业WAN网络，相比SD-WAN部署优势明显。

安全倾向类：对网络和信息安全要求高，主要集中于党政军机构、金融/证券企业、技术密集型的科技企业等。倾向于采用MSTP、OTN、裸光纤或IPRAN、PTN等分组传送网方式组网。

组网倾向类（接入灵活）：对组网灵活性要求较高，主要涉及公共服务类机构，如交通、物流等部门或企业，软件、系统集成等信息类科技企业。此类客户更加典型的场景是云网融合类业务，如政务云、企业上云等。云网融合近年来得到了快速发展并成为MPLS、SD-WAN技术的重要应用方向。

4.2 典型应用场景

通过上文对专线客户需求类型和选择倾向的分析，笔者总结出以下3类SD-WAN最典型的应用场景。第1类为分散的零售加盟企业，如社区连锁超市等。第2类为公共服务类应用，如道路、水文、市政监控等。第3类为云网融合类场景，如政务云、医疗云、教育云以及各种各样的企业应用云化的组网需求，无论是公有云、私有云还是混合云，越复杂的网络环境越能体现出SD-WAN的巨大优势。

对于电信运营商来说，如果要充分利用SD-WAN的灵活性和超高性价比，还有一种非业务类的应用场

景可以考虑，即将SD-WAN应用于专线电路的保护路由、应急开通或故障情况下的应急代通等，将其作为传统WAN业务的运维增强手段部署。

4.3 劣势及不足

当然，从整体架构和业务应用2个角度分析，SD-WAN也有其特定的短板和不足。

从网络架构上看，SD-WAN的控制层主要为网络控制器组件，无论是部署于云端还是自建服务，都很容易受到网络攻击，而其集中控制、集中管理的特点决定了其一旦因攻击或其他原因导致服务中断或者劣化，都将对全网造成极大影响。所以在系统部署的时候，运营商或解决方案提供商需要充分考虑系统灾备、系统双活等安全防护手段。

从业务应用的方面来说，客户业务很容易受到Underlay网络环境的影响，尤其是互联网公网环境的变化，往往是不可控、不可预料的，这些都需要应用识别、应用选路、广域优化等方式来进行QoS增强，这也增大了系统和业务的复杂度。

5 总结

本文从基础架构、产品应用、运营模式等方面对SD-WAN进行了分析探讨。SD-WAN并不是一个基础网络技术层面的创新，也不是一个具体的网络产品，它不能脱离基础网络独立存在。SD-WAN是一种企业WAN网络软件化的解决方案，是一种新的服务提供方式，这种提供方式能更好地适应云网融合等复杂多变的网络场景。目前，提供SD-WAN解决方案和产品运营的企业很多，其网络架构和实现路径虽然大同小异，但是侧重点却各有不同。完整的SD-WAN体系需要整合基础网络、软件开发、系统集成、安全技术等全生态资源。从网络技术上看，SD-WAN尚无法取代传统的WAN组网方式，而是作为一种服务方式的补充与它们长期并存，并将在特定场景中发挥重要作用。同时SD-WAN的发展也将推动传统传送网技术向SDN方向不断演化和迭代。

参考文献：

[1] 盛成. SD-WAN架构与技术[M]. 北京：人民邮电出版社，2019：30-46.
[2] 张卫峰. 深度解析SDN利益、战略、技术、实践[M]. 北京：电子工业出版社，2013：58-60.
[3] 威廉·斯托林斯. 现代网络技术[M]. 北京：机械工业出版社，2018：53-59.
[4] 安迪. 运营商拥抱SD-WAN的正确姿势[EB/OL]. [2020-12-15]. http://finance.sina.com.cn/stock/relnews/us/2019-10-12/doc-iicezuev1637667.shtml.
[5] 宁孟丽，李颖. 基于VPDN技术的无线数据传输系统[J]. 中国科技信息，2005(13)：51-51.
[6] 石永红，刘嘉勇，汤云革. 基于MPLS的VPN技术原理及其实现[J]. 电子技术应用，2004，30(7)：1-3.
[7] 唐红芳，李乐民. MPLS的关键技术及其应用[J]. 四川通信技术，2001，31(3)：8-13.
[8] 李劲. 云计算数据中心规划与设计[M]. 北京：人民邮电出版社，2018.
[9] 凯文·杰克逊，斯科特·戈斯林. 云计算解决方案架构设计[M]. 北京：清华大学出版社，2020.
[10] 刘化君. 网络安全与管理[M]. 北京：电子工业出版社，2019.
[11] 李素游，寿国础. NFV架构、开发、测试及应用[M]. 北京：人民邮电出版社，2018.
[12] 李明江. 简单网络管理协议[M]. 北京：电子工业出版社，2007.
[13] 杨东晓，张锋，冯涛，等. 网络安全运营[M]. 北京：清华大学出版社，2020.
[14] 马春光，郭方方. 防火墙、入侵检测与VPN[M]. 北京：北京邮电大学出版社，2008.
[15] 虚拟化技术详解[EB/OL]. [2020-12-15]. https://blog.csdn.net/gui951753/article/details/81045508.
[16] 邓皿. 基于VPN与网络安全的研究[J]. 网络安全技术与应用，2020(1)：35-36.
[17] 李德伟. 云架构下的SD-WAN技术探讨[J]. 通讯世界，2020，27(2)：13-14.
[18] 柴瑶琳，穆博，马军锋. SD-WAN关键技术[J]. 中兴通讯技术，2019，25(2)：15-19.
[19] 穆域博，柴瑶琳，宋平，等. SD-WAN产业发展与关键技术研究[J]. 信息通信技术与政策，2019(11)：73-78.
[20] 董炳泉. SD-WAN三种技术方案的研究[J]. 广东通信技术，2019，39(11)：64-67.
[21] 侯晓静，康宇. 基于云架构的SD-WAN技术[J]. 通信与信息技术，2019，(2)：47-49.
[22] 王林，周崇杰. SD-WAN技术优势及应用分析[J]. 科技风，2018，(1)：60，67.
[23] 顾炯. 运营商SD-WAN部署的难点分析[J]. 电信科学，2017，33(12)：172-176.
[24] 林志华. 运营商SD-WAN产品化研究与实践[J]. 通信技术，2020，53(8)：2082-2087.

作者简介：

王胜志，工程师，学士，主要从事政企通信业务技术服务和支撑工作；章道勇，高级工程师，硕士，主要从事融合业务和智慧家庭业务管理工作。