SD-WAN 技术白皮书

（2019 年）

SDN/NFV/AI 标准与产业推进委员会

2019 年 9 月

版权说明

前言

本白皮书在总结 SD-WAN 技术发展历程和技术体系的基础之上，分析研究现阶段 SD-WAN 技术发展的总体态势，并对关键技术灵活组网、面向连接的服务保障、策略驱动、高可用服务、敏捷运维、安全服务、广域网优化、多云访问、多租户管理技术特征进行了系统阐述，在此基础之上提出未来 SD-WAN 的发展展望。

目录

1. SD-WAN 的发展背景和价值

1.1 SD-WAN 发展背景

1.1.1 广域网发展面临的挑战

随着互联网技术的不断发展，众多企业在部署新型应用、发展新兴业务（例如视频会议、大数据传输）时，经常发现当前的广域网组网面临着三个严峻的挑战：

1）传统的专线网络（如 MPLS[1]）需要不断地增加带宽以保证应用的性能；

2.）公司内大量站点互联，造成了高度复杂的拓扑结构；

3） 随着应用和业务上云，需要实现不同站点对云的安全动态的访问

在现有广域网上，网络运营商或服务商已经提供了成熟服务，MPLS L2/L3 VPN 已广泛应用于专线服务，也能够提供端到端的服务保障；其它的专线还包括基于 SDH 的 MSTP 专线业务，如 DDN（Digital Data Network）、ATM、Ethernet 等。这些传统的专线能够提供稳定可靠的端到端的服务质量，但也存在局限性：价格昂贵、开通周期长、带宽利用率低，尤其对于云业务和云应用来说，传统专线无法动态扩容容易带来连接性能下降和网络链路拥塞问题，这是业务性能所不能接受的。另一方面，部分企业为了降低网络资源成本采用基于 Internet 的连接来实现对业务和站点的访问。虽然市场上已经有很多基于 IPsec 等加密技术来保证 Internet 数据传输安全性的产品和方案[2]，但 Internet 的不稳定性和安全性依旧是困扰企业部署基于 Internet 的传输网络的关键因素，无法保证全方位的解决客户问题。如何平衡网络安全、网络性能以及成本因素，是众多的企业用户网络架构亟需解决的问题。

传统的广域网并不能提供一种普惠性的服务能力。企业需要快速发展，业务需要灵活部署，SD-WAN（Software - Wide Area Network）则为这一新的市场提供了快速发展机会。

1.1.2 SD-WAN 发展驱动力

广义的 SD-WAN 是将 SDN 技术应用到广域网场景中所形成的一种服务。这种服务用于连接覆盖广阔地理范围的企业分支、数据中心、互联网应用及多个公有云，旨在帮助用户降低广域网的开支和提高网络连接的灵活性。

催化 SD-WAN 快速发展的原因主要以下几方面：

1）SDN/NFV 技术成熟化

SD-WAN 是 SDN/NFV（Software Defined Network/Network Functional Virtualization，）技术在现网应用的一种具体体现。从 2014 年开始，SDN/NFV 技术逐步在市场落地[3]，2014 年~ 2015 年，伴随着私有云和公有云网络与业务走向成熟，SDN-Enable 设备也逐步发展成熟；2016 年 ~ 2017 年，核心侧（基础服务提供商）的网络走向 SDN 化，DCI（Data Center Interconnection）需求倒逼 SDN-WAN 控制器逐步成熟[5][4]；2018 年 ~ 2020 年，网络与业务融合式发展，软件定义的云网协同和分支型专线替代传统的企业组网方案成为主流，宣告了 SDN/NFV 技术成熟化。

SD-WAN 技术将发展成熟的 SDN/NFV 技术应用到广域网传输，在无需更改现网架构的基础上，提供了可管理的虚拟网络，相比现有基于协议自治的网络，实现了流量灵活调度，同时降低网络部署复杂度和 IT 运维成本，开启了新的网络价值场景。

2）Internet 高速发展

Internet 的覆盖范围和网络性能在不断提升，与传统专线的传输质量差距在迅速缩小。

SD-WAN 在传统的专线连接方案上融合 Internet 连接来承担企业和不同组织的互联互通功能，支持企业更灵活、更高性价比地选择网络连接服务，通过软件定义的方式来响应国家的“提速降费”政策。

3）云计算迅猛发展

云计算的兴起带动了公有云的蓬勃发展，越来越多的企业把 IT 系统托管到公有云上，从而降低建设 IT 系统的成本和周期。伴随着企业应用云化程度的加深，企业会借助 WAN 频繁访问云端的 SaaS（Software-as-a-Service，软件即服务）应用，如办公软件 Office365、企业数据库等，而网随云动逐渐成为企业的普遍诉求。

企业借助 SD-WAN 技术，一方面可以按需将企业分支和 DC（Data Center，数据中心）接入公有云服务，更敏捷地发放业务；另一方面企业 WAN 正在承载越来越多和云相关的应用流量，这在很大程度上导致了 WAN 流量大增，从根本

上改变了企业流量模型。企业业务云化之后，WAN（Wide Area Network，广域网）与 LAN（local area network，局域网）的流量对比从传统的 2:8 变为 8:2，80%的流量都需要通过 WAN 传输，SD-WAN 技术提供的企业 WAN 传输质量将直接决定企业部署在多个公有云的应用体验。

4）企业数字化转型

当前，在企业数字化转型的过程中，企业的业务变化更加频繁，更加灵活，更加多元。SD-WAN 作为一个开放平台部署到企业，一方面可以支撑跨多地域的企业分支的互联互通[5]，一方面可以通过上层开放的应用 API（Application Programming Interface，应用程序编程接口）来适应企业数字化业务快速发展。

1.2 SD-WAN 带来的影响

SD-WAN 对于行业用户带来的影响是广泛而深刻的。

与基于传统专线的企业组网相比，SD-WAN 可以利用多个线路（包括 MPLS 线路、Internet 线路等）进行传输，并在数据传输过程中采取流量加密、网络分片等方式保证企业数据安全，保障价格优势又不损失安全性。

此外，SD-WAN 还具有业务灵活调度、带宽随选等功能，使其得到越来越多企业的青睐，例如大型企业在其总部和分支机构之间采用 SD-WAN 专线来进行数据传输。预计到 2022 年，SD-WAN 的部署率将占据全球专线市场的 30%。

同时 SD-WAN 会加速企业上云。随着云技术的发展，越来越多的企业选择采用虚拟化的方式来部署应用，帮助企业快速通过云业务应用来实现去 IT 中心化、降低运维成本，高效地驱动了企业的战略发展。因此，很多企业在云端托管了大量的应用程序（AWS、Office 365 和 Salesforce）。无论企业是在云端部署自身的应用和业务系统，还是访问托管的云端应用，基本是通过云提供商的 Internet 接口来访问，在安全性和稳定性方面缺乏保障。

而 SD-WAN 和云的融合改变了这一现状，企业的 SD-WAN 设备将流量发送到云网关，然后将其连接到云应用程序中，并保持云会话的进行。即便 Internet 连接中断，用户服务也能够在几毫秒内重新切换链路保证服务质量。此外，一些支持云的 SD-WAN 服务提供商可以直接连接到云服务提供商，这意味着企业的

流量传输到 SD-WAN 服务？提供商的云网关之后，企业就可以直接连接到云服务提供商。SD-WAN 与云架构的融合为企业打造了云网一体化的服务框架，进一步保障了企业云应用的高可靠、高可用的服务质量。

SD-WAN 以其转控分离、灵活配置、快速开通、资费低廉等优势，也推动了产业生态的开放和融合式发展，一方面，SD-WAN 通过加强网络接入能力来保障用户云端业务服务质量，进而加速云网融合发展；另一方面，多样化的用户需求为 SD-WAN 服务市场提供了更低的准入和运营门槛。

2. SD-WAN 产业生态发展现状

2.1 SD-WAN 发展历程

2.1.1 SD-WAN 1.0

第一代 SD-WAN 技术方案（SD-WAN 1.0）专注于聚合 MPLS 和 Internet 来跨域提供自动 IP 连接和 WAN 管理以降低带宽成本并提高性能。

SD-WAN 1.0 的主要特点为：快速连接、灵活组网、策略驱动、敏捷运维。

1）快速连接：可在分钟级服务时间内为企业用户提供不同的广域网连接方式。

2）灵活组网：适应不同场地入网环境，使 SD-WAN 整体方案具备良好的组网灵活性。

3）策略驱动：支持定义多种面向业务模型的策略来高效驱动数据转发。

4）敏捷运维：通过对业务的实时监控和统计来实现自动化的运维以及各个应用和整体网络质量的可视化。

随着企业 IT 需求迅速转向适应多云功能，导致企业采用多种模式来使用云服务。此环境创建了一组新的要求，这些要求是传统 SD-WAN 1.0 部署无法解决的问题，SD-WAN 2.0 伴随多云访问的功能特征应运而生。

2.1.2 SD-WAN 2.0

第二代 SD-WAN 技术方案（SD-WAN 2.0）将 SD-WAN 1.0 范例扩展到基于云的平台，为现代企业提供多样化多租户的 IT 服务，改善了管理和监控以及

更好的安全性。SD-WAN 2.0 将不局限于提供连接，允许企业基于 IP 的网络跨域提供可保障的 IT 服务。

SD-WAN 2.0 的主要特点为：整体服务、安全自动、按需随用、多云互联。

1）整体服务：除提供快速连接以外，企业站点还需要一系列网络增值服务（VAS）。其中包括安全功能，VoIP 网关，物联网代理，无线局域网控制器等。SD-WAN 2.0 提供了一种通过统一平台 API 来提供这些增值服务交付的整体能力。

2）安全自动：除了防火墙等传统安全措施之外，SD-WAN 2.0 提供整体架构级别的安全服务，从根本上保障端到端通信的安全自动化，以防范，检测和响应这种不断变化的安全威胁形势。

3）按需随用：根据企业用户的弹性需求来提供不同的网络服务能力。

4）多云访问：现代企业需要将分支机构中的用户连接到多个部署在公有云中的应用程序，SD-WAN 2.0 支持提供无缝的多云连接。

SD-WAN 2.0 旨在通过提供单一平台来提供 IT 服务，同时确保用户和业务应用程序的端到端安全性，从而满足企业 IT 的需求。SD-WAN 2.0 的蓬勃发展全面激活了 SD-WAN 产业生态。

2.2 SD-WAN 生态参与者

SD-WAN 产业生态是一个开放的端到端多服务生态。在这个开放的生态环境下，SD-WAN 的参与方众多，主要包括基础电信运营商、SD-WAN 服务提供商、设备提供商、解决方案提供商、云服务提供商、用户、第三方组织。

基础电信运营商利用 SD-WAN 提供多产业组织样化、差异化、弹性化的网络服务；基础设施提供商通过在路由和交换设备中集成 SD-WAN 的相关能力来稳固或增强其在企业组网领域的地位；虚拟服务提供商与行业用户需求紧密相贴，提供更灵活的 SD-WAN 服务；云服务提供商利用 SD-WAN，增强云服务能力，帮助企业更好地上云，简捷提供 SaaS；解决方案提供商为用户提供 SD-WAN 整体解决方案，包括方案设计、规划、部署等流程；第三方组织（包括 MEF、ONUG、IETF、SNAI、CAICT、Spirent、Ixia）加快 SD-WAN 标准体系建设，建立并促进 SD-WAN 生态联盟，推进企业数字化、信息化转型。

2.2.1 基础电信运营商

基础电信运营商绝大多数都投入了 SD-WAN 市场，将 SD-WAN 视作传统专线的一种升级，主要面向中小企业客户提供相关产品和服务，这其中根据电信运营商是否具有存量的 MPLS 业务，还有两种细分的商业模式：

1） 具有存量 MPLS 业务的电信运营商：一般将 SD-WAN 与 MPLS 业务并存，提供全面的组网解决方案。将 SD-WAN 作为对资费敏感、底层网络要求不高的客户组网的选择之一，将 MPLS 作为对底层网络要求较高的客户组网的主要选择，在具体的客户案例中，通常还存在主备用接入电路分别采用 MPLS 和 SD-WAN 的情况。典型的运营商代表如 AT&T、Orange 等，已经在将 SD-WAN 作为其 MPLS 业务的一个补充，在全网特别是国际网络部分，广泛提供 SD-WAN 服务。

2） 不具有存量 MPLS 业务的电信运营商：通过 SD-WAN 全面满足客户的各种组网需求，通常会结合高速互联网接入的能力，来增强 SD-WAN 服务的底层网络保障。在具体的客户案例中，通常还存在主备用接入电路分别采用固网方式和移动网方式的情况，以提高电路的可靠性。典型的运营商代表如 Comcast 等，面向企业客户大力推广高速互联网接入（1Gbps 以上），并基于此提供 SD-WAN 服务。

基础电信运营商提供 SD-WAN 业务，一方面满足了客户多样化的组网需求，拓宽了广域网连接的种类；另一方面也丰富了自身的产品目录，在连接的基础上还可以提供诸如应用加速等增值服务。所以，不论是在组网/连接服务的广度和深度上，都促进了基础电信运营商的“供给侧改革”。

目前，基础电信运营商和业界的其他参与者，存在着一定的竞合关系：

1）竞争方面：在细分的市场，特别是中小企业客户市场中，基础电信运营商提供 SD-WAN 业务，和 SD-WAN 服务提供商、云服务提供商，存在直接竞争的关系。从网络实施的角度看，如果是后者提供的 SD-WAN 服务，一般都是 overlay 在基础电信运营商的底层网络（互联网）之上，实际上是对传统基础电信运营商专线的替代，分流了传统基础运营商专线市场的份额。

2）合作方面：由于 SD-WAN 服务提供商、云服务提供商在底层网络资源、属地化/线下服务体系和渠道等方面，存在一定的不足，所以其提供 SD-WAN 业务时也存在和基础电信运营商开展广泛合作的需求。同时，基础电信运营商在部

署和建设自身的 SD-WAN 网络时，特别是引入 overlay 的部署方案时，也存在向设备提供商和解决方案提供商采购相关产品和方案的需求；如果是在 SD-WAN 服务中提供接入多云的功能，那么基础电信运营商往往还需要和云服务提供商建立深度合作的关系。

2.2.2 SD-WAN 服务提供商

主流的 SD-WAN 服务提供商主要分为两类，

1）传统的网络服务提供商，其优势在于可以最大限度的利用已有的骨干网络资源，不需要额外构建网络，构建成本低。传统网络提供商的另一个优势是多年以来积累的网络运维和服务经验，对于全网的管理、安全保障、故障恢复、特殊事件响应等能力高。传统的网络服务提供商通常采用市场上相对成熟，市场占有率高的 SD-WAN 产品来构建自己的 SD-WAN 服务。

2）SD-WAN 服务提供商，可以灵活的根据自身需求，自行研发 SD-WAN 产品，构建在全新的骨干网络之上，有着全网管理灵活性的优势。

SD-WAN 服务提供商为企业客户提供 SD-WAN 服务。客户无需购买和自建 SD-WAN 编排器，控制器和网关，SD-WAN 服务提供商将所有核心组件及其功能、部署在客户站点的 SD-WAN 终端设备，以一站式服务的形式将网络资源（MPLS VPN 线路、Internet）提供给客户，降低企业用户的一次性投资。同时，SD-WAN 服务提供商还可以提供全网的运维管理服务，来确保整体网络的安全可靠。

利用 SD-WAN 服务，服务提供商可以很好的整合传统网络资源为客户提供更高的服务等级以及更加灵活的解决方案。

SD-WAN 服务提供商整合了 SD-WAN 设备提供商的技术优势，利用基础运营商的网络资源，并且与云服务提供商和数据中心提供商密切合作，为客户提供 SD-WAN 咨询、设计、构架、部署、运维等全方位的服务。

2.2.3 设备提供商

SD-WAN 设备提供商主要面向基础电信运营商、SD-WAN 服务提供商、解决方案提供商等用户来提供各种 SD-WAN 设备。

目前主流的 SD-WAN 设备提供商主要提供 SD-WAN 边缘设备、网关设备、SD-WAN 管理节点设备（以控制器为主)、VAS 网元等设备。

2.2.4 解决方案提供商

SD-WAN 解决方案提供商主要面向有 SD-WAN 需求的企业用户或运营服务提供商，提供各种 SD-WAN 解决方案，帮助其构建自身的 SD-WAN 网络及运营维护体系/流程。

目前业界的解决方案提供商主要来源于传统设备厂商或初创公司，前者主要通过在其既有的路由交换设备中植入 SD-WAN 能力实现其产品与方案的升级，后者一般通过软硬件定制开发实现 SD-WAN 解决方案的定制。

2.2.5 云服务提供商

云服务提供商通过 SD-WAN 确保云应用及业务能够稳定的交付到用户端，保证用户的服务体验，尤其是最后一公里保障。云数据中心到用户间或者云数据中心间的链路质量是服务保证的重要环节。SD-WAN 则提供了一种网络管理和调度的形式，能够加速云服务的使用，进一步促进云网融合。

现在上云已经是确定性的趋势，用户网络也逐步从以 IDC 和企业总部为中心发展为以云为中心。云服务提供商需要提供给用户非常便捷的组网方式，过去主要是在云上的网络方面，随着服务用户规模的扩大以及用户网络要求的变化，云服务提供商提供的网络产品也逐步的从云上扩大到云间和云下。

同步 SD-WAN 的趋势，云服务提供商一方面给其他的 SD-WAN 解决方案提供商和用户提供计算和网络资源，另一方面也需要逐步整合，给用户提供一体化的产品和解决方案，从而给用户提供最适合、性价比最高的产品。典型的比如阿里云提供给用户完整的混合云方案，其中包括了自己的 SD-WAN 产品：智能接入网关。其他的云服务提供商，国外如 AWS 和 AZURE 也提供了类似的产品，国内其他云厂商如腾讯等也在开发类似产品。

2.2.6 第三方组织

第三方组织对于 SD-WAN 市场的健康繁荣发展同等重要。当前的 SD-WAN 市场正处于初期的发展阶段，产品技术及服务方式差异很大，存在着隧道建立模式紧密耦合终端设备，服务质量标准不统一等一系列问题。第三方机构组织通过统一协调各方诉求，构筑技术发展平台，统一行业标准，引导整个行业生态健康快速发展。

第三方机构包括中国通信标准化协会，国内部分测试与测评实验室，大学实

验室和相关科研机构。另外，电信运营商研究院及实验室也在承担 SD-WAN 产业的研究与规范工作，同时，也在参与包括 MEF（MEF Forum，城域以太网论坛）、IETF（The Internet Engineering Task Force，国际互联网工程任务组）等组织相关的标准立项工作。

■ 中国通信标准化协会正在组织进行 SD-WAN 相关标准规范的编制工作，其 TC610（即 SDN/NFV/AI 标准与产业推进委员会）将协同业界各方尽快落实和发布相关（不都是评测的标准吧？）的技术标准，包括《SD-WAN 关键指标体系》、《软件定义广域网络（SD-WAN）测试方法》、《软件定义广域网络（SD-WAN）增值业务技术要求 广域网加速》、《软件定义广域网络（SD-WAN）增值业务技术要求 安全服务》、《软件定义广域网络（SD-WAN）增值业务技术要求 敏捷运维》等系列标准。

■ ONUG 是由战略上推动企业数字化转型，以行业领先企业为主导、以用户需求为中心的产业组织[6]。ONUG 的使命是“以 IT 开放接口的互操作性为目标，打造跨越 IT 技术栈的整体解决方案”，为 IT 业务领导者提供更多的选择，努力创造商业价值”。ONUG 支持多个用例工作组，包括 ONUG SD-WAN 2.0 工作组，该工作组汇总了边缘和多云连接的用例需求，重点关注大规模的性能和逻辑网络以及所有支持下一代 SD-WAN 环境的安全要求。该工作组创建并发布了 10 个业务需求对应的一系列文档，包括白皮书《SD-WAN Working Group White Paper》 、测试计划《SD-WAN Test Plan》、需求表《SD-WAN Requirements Sheet》。该工作组联合国内外许多 SD-WAN 供应商（思科，Glue Networks，Riverbed，Silver Peak，Talari，VeloCloud 和 Viptela，华为等）进行了测试，证明他们的 SD-WAN 产品支持 ONUG SD-WAN 工作组白皮书中列出的十大要求，相关测试结果发布在《SD-WAN Verification Slides》。

■ MEF 是一家具有超过 200 家会员的电信产业联盟，其宗旨是推动敏捷、可靠、协同的通信服务发展，使得用户能获得按需动态的性能和安全，从而在数字化经济生态中茁壮成长[7]。MEF 下设有业务、LSO（生命周期业务编排）、应用、认证、市场与培训等多个委员会，目前这几个委员会均针对 SD-WAN 开展了工作，并将 SD-WAN 纳入 MEF3.0 系列中。MEF 在 2017 年 7 月在全球率先发布了第一个 SD-WAN 业务规范《Understanding SD-WAN Managed Services》，

目前 MEF 正在推动 LSO 支持 SD-WAN 数据模型的标准化。在《Understanding SD-WAN Managed Services》中，MEF 首次提出和定义了 SD-WAN 业务的组件，包括 SD-WAN Edge、SD-WAN Gateway、SD-WAN Controller、Service Orchestrator、Subscribers Web Portal 等。MEF 已经针对 SD-WAN 开展了 POC 演示、多运营商互联试验、LSO Hackathon 等工作，并将在近期发布相关的 SD-WAN 业务认证测试规范。

同时，MEF 针对 SD-WAN 方案的技术评估标准也在进行研究，包括网络质量测试标准及 SD-WAN 设备应具备的能力等，以推动统一的测试测量体系。

■ IETF 是全球互联网最具权威的技术标准化组织，主要任务是负责互联网相关技术规范的研发和制定，当前绝大多数国际互联网技术标准均出自 IETF。IETF 主要采取网络解决方案（信息模型、BGP、SR）与 SD-WAN 相结合的方式，具体提出了三个技术草案的推进工作，分别是《A YANG Data Model for SD-WAN VPN Service Delivery》、《BGP Extension for SDWAN Overlay Networks》、《SR For SDWAN: VPN with Underlay SLA》

3. SD-WAN 总体架构

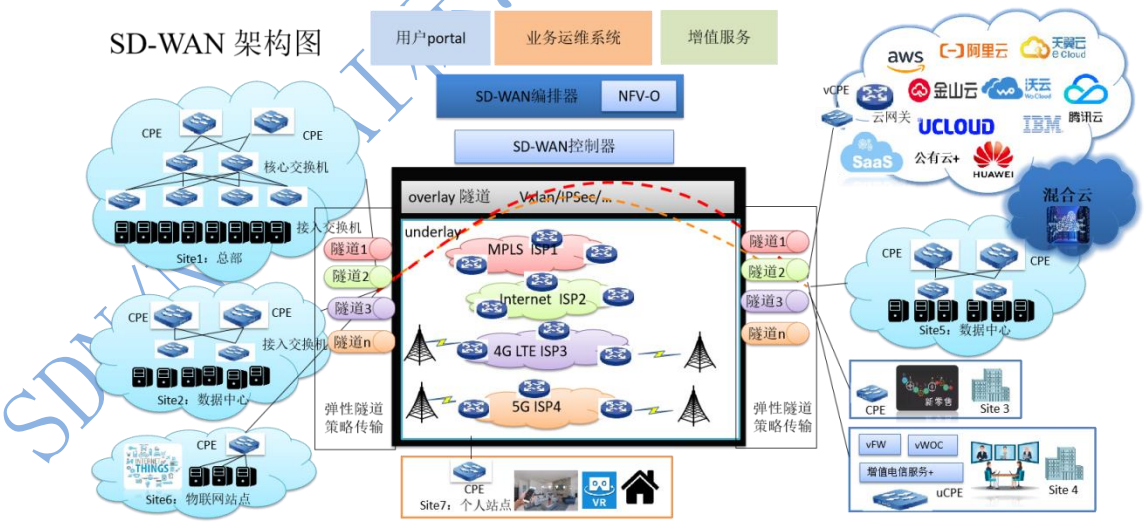

图 1 SD-WAN 总体架构图

SD-WAN 重新定义了开放式的 WAN 架构[8]。SD-WAN 总体技术架构主要由 5 个功能层组成：用户管理层、SD-WAN 编排器、SD-WAN 控制器、边缘设备、WAN 传输网，囊括了 9 个主要技术特征，其中包括了 26 个功能点，覆盖了 3

个典型应用场景。

3.1 用户管理层

用户管理层是直接面向用户的功能层，通过用户管理层，用户可以直接操作产品，包括创建、删除和修改用户网络以及网络中的节点、带宽等。同时，用户也可以通过用户管理层查看产品的特征，比如当下的网络情况，包括了用户节点具体使用情况，每个节点的流量情况等。在用户直接向运营商租用的场景中，用户管理层还包括了计费功能。

用户管理层：主要用于账户管理，业务策略修改等，从而实现用户对于 SD-WAN 方案的集成和界面的灵活定制需要，集成的 SD-WAN 功能主要包括：

1) 组网功能：包含站点到站点，站点与 Internet，站点与传统 VPN 网络，站点与 Cloud 网络的端到端的连接。
2) 基于应用的网络体验功能:包含智能选路，应用优化 WOC(主要是 FEC 和传输优化)及 QOS 管理等。
3) 安全功能：包含系统级安全以及业务安全。
4) 运维功能：监控/故障定位/分析。

5）开放接口功能：SD-WAN 增值服务组件开放，与网络控制器、编排器北向接口开放。

3.2 编排器层

编排器层不直接面向用户，是对 SD-WAN 业务的抽象和管理，对业务中各个网元和网元行为特征的抽象在技术后台的管理功能层。SD-WAN 中的网元包括接入设备 CPE、路由等，编排器就是对这些抽象实体的操作。比如，对网络的操作包括，创建一个网络，删除一个网络，对该网络加入一个接入设备；对接入设备的操作包括，创建一个设备，删除一个设备，定义该设备的带宽，该设备包括的链路及带宽分配和优先级，修改该设备的路由等。

编排器层在应用层和控制器层中间，是两者之间的桥梁，上接应用层接收用户的操作命令，下接控制器层在实际的网络中实现业务的需求。

SD-WAN 编排器通过 SD-WAN 控制器北向开放 API，实现对 SD-WAN 网络

的控制。并通过对网络业务进行抽象和建模，对外屏蔽网络具体的技术实现细节，只暴露面向业务的接口和参数；实现基于用户意图的 QOS，安全以及商业需求的控制。

3.3 控制器层

控制器层控制实际网络环境中的各个网元，这些网元包括路由器、交换机、服务器和用户端的接入设备等。控制器承接编排器层传递的业务逻辑，翻译为对各个网元的具体要求和操作命令，并把这些命令下发给下面各个网元，让下面的网元执行具体的命令来完成业务逻辑。

SD-WAN 控制器，南向采用 SDN 的控制与转发分离的架构，实现底层网络所需的网络控制平面功能管理，包括 overlay 连接的建立，维护和终止，路由分发，过滤和控制，VPN 及拓扑控制等，北向与 SD-WAN 编排器接口。控制器的主要功能有:

1）对网络层硬件或者软件虚拟化设备的管理和控制功能。

2）业务管理：包括 WAN 组网创建、VPN 划分、应用选路策略、安全策略、QOS 等策略配置和业务自动化发放。

3）网络管理与运维功能，包括网元告警、日志等故障信息采集、链路质量信息、应用质量信息和网流等网络性能数据的采集和分析，并对最终客户进行网络拓扑、故障、性能等运维信息的统计和显示。

3.4 广域网传输层

广域网传输层在控制器的控制下，承接数据传输的功能。广域网传输层的网元包括路由器、交换机、接入点的服务器等，这些网元组合在一起，控制用户的数据是否可以传输、如何传输、是否加密、传输链路的带宽等。

广域网传输层主要包括两个部分，Underlay 网络和 Overlay 网络。Underlay 网络主要是指基础电信运营商提供的 WAN 专线，Overlay 网络基于各种运营商的 Underlay WAN 网络构建，实现了企业分支、总部、DC 以及云上等多种类型站点的互联，是 SD-WAN 网络的核心。

3.5 边缘设备层

SD-WAN 边缘设备层是构成 SD-WAN 底层物理传输网的边缘网元，主要包括 SD-WAN 边缘设备、SD-WAN 网关设备、增值服务网元等。

SD-WAN Edge（边缘设备）是指企业分支、DC 或者云站点的出口 CPE 设备。Edge 的设备形态主要包括硬件 CPE 和虚拟的 NFV 软件 CPE (vCPE) 。Edge 是 SD-WAN 网络和用户网络的边界点，也是 SD-WAN 站点到站点隧道的发起和终结点。Edge 通常具备多种 WAN 的接入能力，如专线接入、宽带 Internet 接入或是无线接入（例如 4G/LTE）。

SD-WAN GW（网关设备）是连接 SD-WAN 站点和传统 VPN 站点的中间设备。 SD-WAN GW 的设备形态有硬件 CPE 和虚拟的 VNF。SD-WAN GW 需支持 SD-WAN overlay 隧道技术，同时需要支持与企业传统网络互通所需的 VPN (如 MPLS VPN) 技术。此外，SD-WAN GW 属于运营商/MSP 的设备，通常是多企业租户共享的网元，一般放置在运营商/MSP 机房或者部署在云上。

VAS 网元主要是指防火墙、广域加速等网络增值功能，通常是独立的网元，具体的形态，可以是独立的硬件设备，或者是独立的 NFV 软件网元，也可以是部署在 SD-WAN Edge 中的 NFV 软件网元。

4. SD-WAN 技术特征

传统网络的管理是基于网络设备实现，无法对整个网络的资源进行统一的管理和规划，而通过管理与控制分离，SD-WAN 具备灵活组网、弹性服务、连接服务保障、策略驱动、高可用服务、敏捷运维、安全服务、广域网优化、多云访问、多租户权限管理十大技术特征[8]。

4.1 灵活组网

4.1.1 场景适应性

SD-WAN 方案应能满足各种开通场景需求，能在不同环境和条件下提供网络接入。

1) 适应不同场地环境

满足不同场地环境开通需求，包括固定地址机构接入，频繁变更地址的机构

接入，移动工作组或个人办公环境接入，小微企业共享办公环境接入。

2) 适应不同入网环境

适应不同入网环境开通需求，包括高速率的大型机构或数据中心入网，低速率偏远地区的边缘节点入网，及按需拨号上网方式。

3) 适应不同信息化环境

适应用户已有的不同信息化环境，包括在企业已有数据中心和企业 WAN 网络环境采用 SD-WAN 进行改造，或采用 SD-WAN 新建企业 WAN 网络。

4.1.2 开通灵活性

SD-WAN 方案关于终端设备上线开通，应能灵活支持多种方式，以便满足用户不同的开通上线场景需求。

1) 全自动发现添加方式

在已有 SD-WAN 管控平台，已完成前期配置情况下，CPE 终端设备以 DHCP 等方式自动上线并连接上端管控平台，管控平台自动发现 CPE 终端设备并完成开通配置工作，满足用户机构在理想上网环境下，以全自动方式入网开通。

2) 半自动开通方式

在已有 SD-WAN 管控平台，已完成前期配置情况下，CPE 终端设备以零接触 ZTP，或邮件开通方式上线，满足用户在无需专业 IT 技术人员条件下的开通需求。

3) 手动开通方式

手动使用配置工具或通过 CPE 终端设备的配置向导开通，满足在复杂条件下，或遇到疑难技术问题时的开通需求。另外，也可满足物联网等集中建设项目，需要集中配置大批量 CPE 终端设备的要求。

4.1.3 组网灵活性

SD-WAN 方案应具备良好的组网灵活性，能满足各种组网拓扑结构要求，提供丰富的可选连接方式，支持多种接入介质和安全认证方式，并能根据用户不同管理意图，灵活选用开通配置手段。

1) 结构拓扑灵活性

应能实现全部 3 种拓扑结构，包括：hub-spoke，full mesh，partial-mesh。

2) 连接方式灵活性

组网链路应支持多种连接方式，包括：IPSec VPN，GRE，MPLS VPN 等。GRE over IPSec、VXLAN over IPsec、MPLS over IPsec、NVGRE、VXLAN/EVPN 等。

3) 接入介质灵活性

CPE 终端设备接入场景可支持的接入介质类型，应不局限于传统的 FTTB、LAN 或 xDSL 等固定专线接入，还应支持 Wifi、4G LTE 等无线介质。未来应可支持 5G 等更广泛的应用场景。

4) 接入安全灵活性

CPE 终端设备应支持多种接入安全认证方式，至少提供基于终端设备的认证方式，基于用户的认证方式。

4.2 弹性服务

SD-WAN 的弹性服务能力是针对用户需求来提供弹性化的网络服务能力，主要是实现三个方面的随选能力，包括：网络拓扑随选，连接时间随选，服务按需随选。

1) 网络拓扑随选

具备拓扑结构灵活调整能力，使用户能按需添加或删减 WAN 连接，实现网络规模的扩张或收缩；具备路径调整能力，基于 SD-WAN 技术提供可调整的路径配置能力，能够按需改变组网节点的拓扑属性，以及节点之间的连接关系，从而实现动态调整拓扑结构路径走向。

2) 连接时间随选

通过运用 SD-WAN 的集中管控、快速开通和配置能力，在实现用户网络和服务开通时，能够按用户需求即时开通、变更或删除 WAN 链接，满足使用时间窗口灵活、频繁变更接入位置的要求。

3) 服务按需随选

提供按需调用或启用的各类增值和安全服务的能力，并支持用户订购业务种类和数量灵活变更等方式。

4.3 连接服务保障

SD-WAN 方案在完整的服务生命周期内，应可针对不同业务提供差异化的服务质量保障和 SLA 能力。SLA 能力主要考虑以下指标

1) 可用性

指 SD-WAN 架构方案的整体可用性，考察指标包括按照年化的平均无故障时间；按照理想条件下的单次冗余链路中断自动切换恢复时间；组网控制节点故障切换对网络业务和控制中断时间等。

2) 数据包往返时间

该指标包含两方面含义，第一，在 SD-WAN 方案中应分别考察控制信令、业务数据流两种类型的数据报文在转发路径上开销的时间；第二，应注意采用数据包的往返全程时延作为考察对象。

3) 时延最大抖动、时延平均抖动、丢包率

由于 SD-WAN 方案中大量采用基于 Internet 或 4G/LTE 等低成本链路介质，此类接入介质与传统固定专线相比，链路质量有较大波动可能性，因此，SD-WAN 方案应具备统筹调度利用底层链路介质的能力，在具备多种接入介质的链路上，能够按业务敏感程度设定时延抖动最大值、平均值等参数，能在达到预设保障条件时自动将业务流量从低成本链路切换到高品质链路，以便在链路的服务生命周期内，兼顾成本和服务质量。

4) 失败通知

要求 SD-WAN 方案的控制层面具备业务感知能力，可在监控条件被触发时，向上层的编排层面、业务应用层面发出业务失败通知，以便做出进一步恢复动作。

5) 链路质量测量

SD-WAN 方案需要提供链路质量持续监测能力，并能提供时延、丢包等关键性指标，提供给上层管理系统参考。链路的测量支持 7*24 小时监测，并能够采用相应的测试基准，包括 TWAMP（Two-Way Active Measurement Protocol，双向主动测量协议）、Ethernet Service Activation Methodology Y.1564（以太网服务激活测试方法）等成熟的测试方法学。

4.4 策略驱动

SD-WAN 的策略驱动是一个从策略模板抽象、策略定义、策略存储、策略下发与驱动业务执行的完整过程。另一方面，企业也可通过 SD-WAN 技术来创建面向不同颗粒度业务的不同的流量转发策略，这些策略可以基于 IP 地址、应用配置文件或端口号、时间、QoS 标记、SLA 测量、实时链路利用率、延迟、丢包和性能阈值来实时驱动。

SD-WAN 设备需要支持基于业务或应用感知能力，支持业务级别的 QOS 能力，以保障高优级别的业务质量，或者跟据业务组别来选择相应的链路。

企业网络中存在多种应用，常见的企业应用包括语音、视频会议、远程桌面、文件传输、企业 SAP/ERP（systems applications and products in data processing /Enterprise Resource Planning，企业资源计划系统/企业资源计划）类应用、Mail、SaaS 应用等，不同的应用对链路质量的要求不同，比如语音对链路丢包率、延迟、抖动容忍度较低；Mail、文件传输类业务则对丢包率、网络延迟不敏感。

1）动态识别应用，识别方式支持

支持基于 IP、协议类型、端口号、DSCP、域名、签名等多种方式自定义应用识别。

支持首包识别，即在应用的第一条数据流即可识别出应用类型，使得应用的第一个数据包就能准确的匹配各种策略：选路策略、安全策略等。

支持系统自动的特征库进行应用识别。

需支持链路时延、丢包和抖动的质量监测。

支持根据应用对链路质量的要求为应用选择转发路径策略，策略需支持：

2）SLA 动态选路

可以根据应用对网络的 SLA 不同需求，实现将不同应用映射到具有不同 SLA 的 WAN 链路，从而在提升网络链路使用效率的同时，提升企业客户的应用体验。关键应用（比如语音、视频会议）优选 MPLS 链路，非关键应用（FTP、Mail 等）优选 Internet。

3）优先级选路

对不同类型的应用使用不同的 QoS 策略，保证高优先级应用优先调度，并限制低优先级应用的流量。

4）负载均衡

提高带宽利用率、根据链路权重进行选路、不同应用主选不同链路。

5）带宽选路

基于线路带宽使用情况、基于应用带宽使用情况进行选路。

4.5 高可用服务

高可用服务在 SD-WAN 网络架构下（主要体现在 SD-WAN 集中管控平台的高可用性），当 SD-WAN 控制器发生故障时，均应对数据流量转发不造成影响。高可用服务方式可采取以下三种模式：

1）主备高可用模式

SD-WAN 集中管控平台以主备方式工作，其中主服务器处于 active 状态提供所有的管理控制和业务配置服务，备用各服务器均处于 standby 状态。主服务器故障时，候选备用服务器中的一台自动切换到 active 状态，成为新的主服务器。该模式下的 SD-WAN 架构整个生命周期内，只有主服务器提供所有服务功能。

2）集群高可用模式

SD-WAN 集中管控平台以集群方式工作，其中有多台主服务器处于 active 状态，以负载分担方式提供管理控制和业务配置服务，备用各服务器均处于 standby 状态。主服务器故障时，SD-WAN 系统可将故障服务器的工作负载转移到其他主用 active 状态的主用服务器，或将候选备用服务器切换到 active 状态，成为新的主用服务器。该模式下的 SD-WAN 架构整个生命周期内，有多台主服务器提供服务功能。

3）控制通道高可用模式

控制器与 SD-WAN 网络设备间的连接具备高靠性，需要在满足相应规格链路质量状态下（包括时延、抖动、闪断等），控制通道及链接的有效性。

4.6 敏捷运维

敏捷运维主要关注网络资产运行状态监控，网元设备和链路故障自愈，应用流量监控和分析等运维自动化辅助功能。

1) 即时运行状态自动监控

应能采集设备和链路运行状态信息，包括 CPU、内存负载状况，设备温度；链路接口 up/down、丢包、时延、速率等。

2) 应用流量自动监控和分析

应能监控 SD-WAN 承载了哪些应用流量，包括：http、https 等特定应用统计的流量，或按 UDP、TCP 等不同类型统计业务流量。

3) 事件和日志自动记录

应能针对设备状态，业务流量状态、SD-WAN 管控系统使用操作事件，安全防护事件等，提供自动记录功能，并能根据时间顺序，或根据类型进行分类统计。

4) 链路可视化

在基于 SDN 的管理下，SD-WAN 应具备全网链路可视化管理能力，通过掌控网络拓扑状况及链路质量，能够快速、敏捷地定位问题，提供优化策略。链路的可视化除了提供 Overlay 网络的状态外，Underlay 网络的可视化同等重要，能够在链路细节颗粒度分析面提供重要的参考。

5) 零接触部署管理

主要是指设备在站点开通时，尽量少与终端或设备接触，设备只需要连线正确，上电后即可开通业务。企业新建分支需要快速上线，客户收到 CPE 设备后，操作人员即插即用就可以实现分支网络开通。

6) 基于站点、VPN 以及应用的流量和性能报告和可视化

SD-WAN 解决方案及服务需支持基于站点、VPN 以及应用的多维度的远程管理；包括 SD-WAN 站点设备、链路等方面可视化显示，并且支持实时远程监控每个站点设备的故障、告警、日志和其他关键事件信息；SD-WAN 的 VPN 网络质量的可视化显示，SD-WAN Edge 或 SD-WAN GW 支持实时远程向集中的控制系统上报网络性能数据，包括关键 WAN 路径的丢包、时延和抖动，以及流统计信息；应用可视以及应用监控：可以查看网络中每种应用的应用质量、流量信息以及排名前几位的应用，用于对网络业务进行优化。

4.7 安全服务

安全是保障 SD-WAN 服务的核心技术要素。SD-WAN 的安全技术主要划分为以下几个层次[9]：

1）SD-WAN 整体架构级别的安全：通过这种方式可以将安全技术原生嵌入到 SD-WAN 整体解决方案中，具备对 SD-WAN 组网和云应用程序的整体安全状况的可视化统计，可对入网设备的整个部署生命周期进行全程安全审计和自动化安全防御，具备可升级能力的动态安全防护，主要体现在以下方面：

■ 基于策略的应用程序流程结构化，从用户流向云应用程序，提供虚拟/逻辑泛网策略孤岛并防止对企业 IT 资源的恶意未授权访问。

■ 网络流量可视化，检测跨分支/云内的所有网络通信，并提供可用于检测异常，违反监管策略和创建安全规则的上下文信息。

■ 闭环自动化，可根据实时网络事件和模式生成自动策略/操作。

■ SD-WAN 面向应用的安全：主要包括防火墙、入侵检测和防御、身份验证和授权、威胁情报和行为分析等功能指标。

■ 用户互访安全：企业内部不同部门之间以及企业同外部用户之间，需要有不同的互访策略，WAN 网络需要提供诸如 ACL 过滤、状态防火墙等丰富的访问和控制策略；

2）SD-WAN 设备级的安全：设备级的安全主要面向设备用户进行设备准入的安全认证以及设备自身具备的安全防御功能，主要体现在以下方面：

■ Internet 接入，具备防攻击等基本的安全防护能力

■ WAN 上传输的数据，支持认证和加密，防止数据泄露

■ 访问控制功能

3）SD-WAN 系统内部数据安全：主要面向 SD-WAN 方案所使用的管控平台，及 CPE 终端设备等组件的自身数据安全。包括管控平台和 CPE 终端设备之间采用 HTTPS 等方式对数据传输进行必要的认证和加密，以防止数据泄露，管控平台和终端设备隔离不同的业务数据等功能。

4.8 广域网优化

广域网优化主要包括对于链路的优化以及针对应用体验的优化。

1）链路优化：应支持对链路进行优化，提升用户体验。包括包复制、前向纠错、TCP 窗口智能调整、数据压缩等技术。

2）网络加速：TCP 或者其它协议加速技术，通过压缩、缓存，包复制，透明代理，协议转换等方式，提高应用程序性能和跨广域网的响应时间。

3）网络的完整性：通过自适应前向纠错（FEC）以及包令校正（POC）等技术，改善在丢包严重的链路上传输数据的效率。

4）数据缩减：广域网压缩和重复数据消除应用于所有流量，消除重复数据的重复传输。节约广域网线路资源，提升传输速度。数据缩减可以应用于所有基于 IP 的协议，包括 TCP 和 UDP。

5）基于多 WAN 链路的应用传输优化：用户端设备可支持多个 WAN 口，用作主备保护倒换或负载均衡，以提升 WAN 的高可用性，用户端设备可以实时监控多个 WAN 链路的实时状态，包括端到端的传输质量（延迟、抖动、丢包率），当特定应用需要传输数据时，根据应用对网络状态的需求选择合适的传输链路，以最大化的保证应用传输质量。负载均衡还可以聚合多 WAN 口的带宽、提升用户体验。

4.9 多云访问

SD-WAN 支持多云访问功能，主要是综合管理多个云供应商的多云连接，创建一个安全、低延迟的多云环境。SD-WAN 平台都能够识别来自前 SaaS 提供商的流量并应用适当的安全性和合规性策略。

SD-WAN 利用其应用识别和流量控制功能，更好地支持对多云环境的安全访问。企业用户可以为每个应用程序和云环境设置特定的业务策略指标，并由 SD-WAN 平台强制执行。他们必须根据可以容忍的延迟程度，对关键任务应用程序进行优先级排序。例如，为低延迟流量(如统一通信、语音、视频、办公效率应用程序和一般电子邮件)设置不同的策略配置文件。

为响应客户需求，SD-WAN 供应商提高了识别和路由基于云的流量的能力。他们与领先的 IaaS 提供商建立了合作关系，以加快与本地站点之间的流量。他们可以在领先的 IaaS 平台上启动其 SD-WAN 平台的虚拟实例。SD-WAN 平台还可以识别大多数领先 SaaS 提供商的 IP 地址，从而应用适当的业务策略。

4.10 多租户权限管理

SD-WAN 解决方案需支持多租户权限管理，支持如下功能:

1）适用于由服务提供商向企业提供 SD-WAN 管理服务的场景，提供系统管理员、MSP 管理员及租户三种管理权限，如果租户不具备网络运维能力，租户可将网络委托给 MSP，由 MSP 代替租户管理租户网络。

2）适用于企业自建 SD-WAN 业务的场景，提供系统管理员和普通租户两种管理权限。具备租户管理权限的管理员可以创建不同角色的管理员，可基于监控、配置、维护、系统等维度来进行精细授权。

5. SD-WAN 技术实现

5.1 管理节点

作为 SD-WAN 最顶层的功能层，管理节点包括网络编排、管理和控制功能，是整个 SD-WAN 解决方案的最核心组件。

网络编节点的一个核心功能是对于 WAN 网络业务进行抽象和模型化，对外部用户屏蔽网络实现和部署的技术细节，生成 WAN 网络的逻辑和业务模型，用户可以基于简化的 WAN 网络模型进行 WAN 网络业务编排，实现简易、灵活和丰富的网络功能配置和自动化发放，有效降低用户运维 WAN 网络的难度，大大提升了企业 WAN 网络业务的发放效率；同时，CPE 等网元以及网络的各种策略配置，也都可以通过网络编排层管理和统一下发。

控制器节点实现了对网络层硬件或者软件虚拟化设备的管理和控制功能。这包括但不限于：网络设备的配置定义和下发、IP 地址管理以及相应的网络策略下发。同时，控制器通过集中的控制功能，实现了网络转发和控制分离，提升了 WAN 网络路由和拓扑的灵活控制能力，使得 SD-WAN 网络本身具备良好的可扩展性，可以组建大规模的网络。

其次，传统的网络管理与运维功能也由控制器统一实现，具体包括：网元的告警、日志等故障信息采集、链路质量信息、应用质量信息和网流等网络性能数据的采集和分析，并对最终客户进行网络拓扑、故障、性能等运维信息的多维度的统计和呈现。

最后，控制器通过网络业务编排功能对外提供 SD-WAN 服务。网络编排实现 SD-WAN 所有关键业务的生命周期管理，包括但不限于 WAN 组网创建、VPN 划分、应用选路策略、安全策略、QOS 等传统策略以及面向业务和意图的策

略配置和业务自动化发放。控制器和 CPE 设备之间业务发放接口一般为 Netconf；CPE 设备可以采用 Netconf Notification 或 SNMP 上报自身告警信息；CPE 设备可以通过 Http2.0 或 gRPC 给控制器上报性能数据。

控制器北向业务发放 API 接口一般为 Restful 接口，和第三方系统一般通过 Kafka 对接告警和性能数据上报。

5.2 网络传输节点

SD-WAN 的网络传输节点主要是由 POP（point-of-presence，网络服务提供点）/PE（Provider Edge，服务商骨干网中的边缘设备）构成，POP/PE 节点位于运营商网络边缘。

前者是位于网络骨干侧的节点，并与运营商的网络保持密切的连接，用于汇聚区域内的 CPE，需具备较高的网络性能和 VPN 数量，同时该 Pop（POP）点也可以作为企业分支访问 Internet 统一出口点、和 MPLS 网络传统站点互通集中处理点等；POP 间通过网络核心互联，因此在流量调度、拓扑管理方面需要实施更佳的调度策略。POP 同 CPE 设备一样，是一种可选的基于逻辑上分层结构，用于完成用户数据面跨 WAN 网络的转发功能。

Edge 一般唯一的属于某个企业用户，由企业用户通过租户管理员视图进行创建、管理和维护，而 POP 属于运营商/MSP 的设备，由运营商/MSP 进行创建、管理和维护，一般会放在运营商/MSP 机房或者部署在云上，而不是类似 Edge 设备通常部署在企业的站点本地。

5.3 边缘节点

SD-WAN Edge（边缘节点）主要是指在企业分支、DC 或者云站点的出口部署的 CPE 设备，Edge 的本质特征是 SD-WAN 隧道的发起和终结点，也可以看做是 SD-WAN 网络的边界点。Edge 之间的 Overlay 隧道可以构建在任意的有线或者无线的 Underlay WAN 技术之上，并且通常与某种数据加密技术(如 IPSec)结合使用，以确保企业 WAN 数据传输的安全性。

Edge 的设备形态主要是两种，硬件 CPE 和虚拟的 NFV 软件 CPE(vCPE)。vCPE 的部署方式多样化，可以是部署在企业的分支站点、也可以在数据中心的服务器上，还可以部署在公有云中，为了描述方便，后续统称为 vCPE。

Edge 通常具备多种 WAN 的接入能力，因此需要具备丰富的接口类型，比如传统的 T1/E1 专线接口、宽带 Internet 的 DSL，Cable 和 PON 接口以及 Wifi、LTE 等无线接入能力，当然还有越来越常用的 Ethernet 接入能力。

为了提升 WAN 应用的体验，Edge 还需要支持分级服务、网络质量测量、虚拟化部署及管理等技术。

5.3.1 应用识别

SD-WAN 边缘节点设备支持智能选路、QoS、应用优化、安全等网络业务的前提和基础，是建立在多应用识别方法上。只有识别了具体的应用，才能在后续的业务流程中应用相关的业务策略。

应用识别方法包括 FPI（First Packet Inspection，首包识别）和 DPI（Deep Packet Inspection，深度包识别）。首包识别是指通过第一个报文识别应用，对基于 TCP 的应用是指通过 TCP SYN 报文识别出应用。DPI 特征识别是指报文的深度识别，通过匹配报文特征识别具体的应用。对基于 TCP 的应用，由于三次建链阶段无报文载荷，因此只有在建链成功后有载荷的报文才能进行识别。DPI 主要应用在多通道协议或者端口号不固定的场景，由于 DPI 会对报文进行深度解析，并且会基于报文特征进行匹配，因此识别准确度高。

应用识别流程在 CPE 上转发处理顺序（和图 2 文字标注一致）如下图所示：

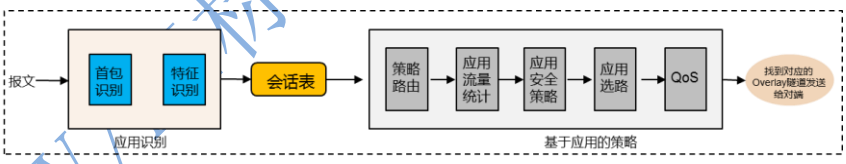

图 2 应用识别在转发中处理顺序

当报文达到应用识别模块时，先进行 FPI，如果报文命中首包识别表，不再进行 DPI 特征识别；如果报文未命中首包识别表时，报文会进行 DPI 特征识别。针对 SD-WAN 支持的两种识别方式（首包识别和 DPI 特征识别），CPE 出厂预置了“首包识别库”和“SA 特征库”，SD-WAN CPE 基于特征库中对应用的定义（端口、特征、行为等）来识别常见的应用。

此外，FPI 和 DPI 特征识别还提供自定义应用的方式，对于库中没有的应用，用户可以通过自定义的方式来定义特殊的应用。

识别到具体的应用后，常见的业务应用包括：

1) QoS：对不同类型的应用采用不同的 QoS 策略，保证高优先级应用优先

调度，并限制低优先级应用的流量。

2) 安全类业务：阻断某些应用，比如在上班期间阻断对娱乐类以及游戏类应用的访问。

3) 智能选路：关键应用（比如语音、视频会议）优选 MPLS 链路，非关键应用（FTP、Mail 等）优选 Internet。

4) 应用优化：对视频会议应用 FEC 优化技术，提升应用体验。

5) 应用可视以及应用监控：可以查看网络中每种应用的使用情况以及 TOP N 的应用，用于对网络业务进行优化。

5.3.2 智能选路

SD-WAN 边缘设备的智能选路模块支持根据应用对链路的质量要求（SLA 条件）对应用进行选路，这样就要对 WAN 链路的质量情况进行测量，确定链路的连通性和质量状态（延迟、丢包和抖动），现网中通常采用部署网络质量分析 NQA（Network Quality Analysis），BFD（Bidirectional Forwarding Detection）等方式来实现。

智能选路模块（SPR）定期基于链路 SLA 以及链路和应用带宽占用情况刷新每个应用组的 SPR 策略（基于链路带宽占用情况、应用带宽占用情况），根据配置的策略刷新（实际刷新的就是应用对应用联接的状态）。

1) 转发收到报文后，识别应用 APP，根据目的 IP 查找到目的站点（Site）的选路策略（下一跳为 Site ID 的才会进入 SPR 选路流程，为明确下一跳的 Site？按照路由转发，比如目的地址为对端隧道口网段地址时，会按照路由转发到对应隧道口），根据应用优先级以及链路带宽的占用状态选择可用的链路。

2) 封装发送应用报文，实时统计链路带宽占用状态，根据应用优先级刷新应用联接对应状态（新流可进入，老流保持，老流避让）。

企业常见的应用智能选路场景如下：

- 应用选路：应用的可用性保证、满足 SLA 以及带宽要求
- 优先级选路：高优先级业务优先，低优先级应用避让高优先级应用
- 负载均衡：提高带宽利用率、根据链路权重进行选路、不同应用主选不同链路
- 带宽选路：基于线路带宽使用情况、应用带宽使用情况进行选路

5.3.3 虚拟化部署及管理

在传统分支出口，不同的 VAS 功能由不同的 SD-WAN 硬件盒子承担，功能固化，业务部署和开通复杂，管理和维护困难。uCPE 是 universal CPE 简称，通常采用 X86/ARM 通用硬件平台来实现承载业务的虚拟化，通过运行 VNF 来提供防火墙（FW）、应用加速（WOC）、SD-WAN 等功能，替代原有的硬件设备，减少网络部署成本。另外，通过控制器在 uCPE 上集中按需部署 VNF，业务开通快，运维成本也会大大降低。相比在数据中心或运营商 Pop（POP?）点以集中式 NFV 形式运行的 vCPE、vFW，在 uCPE 上实现的 NFV 通常称为分布式 NFV（D-NFV）。

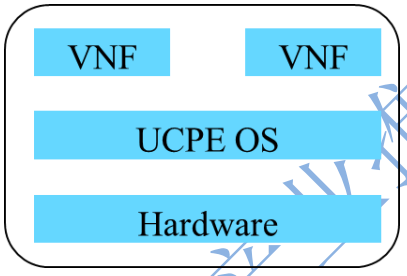

图 3 uCPE 设备架构

uCPE 设备架构分为三层，分别为硬件、uCPE OS 中间层以及最上层的 VNF，uCPE OS 是运行在 uCPE 硬件之上的主机软件系统，通常包括软件操作系统（Linux）、Hypervisor（KVM/Qemu）、vswitch、platform router、设备管理、Plug &Play、告警和性能监控等部件和功能。最上层的 VNF 通常采用 VM 形式部署，用于实现 FW、WOC 甚至 SD-WAN Router 等网络功能。VNF 一般采用单个 VM 实现，不需要实现动态扩缩容。在 uCPE 上，通过业务链可以控制特定流量经过特定的 VNF 序列(traffic steering），对于 LAN 和 WAN 之间的流量，缺省情况是只经过 SD-WAN Router，基于目的 IP 前缀查找 IP 路由表进行转发。uCPE 一般通过提供 Netconf 北向接口，配合控制器实现 VNF 的生命周期管理和业务链功能。VNF 生命周期管理包括 VNF 安装（资源检查）、启动（vNIC 资源创建）、监控（不同运行状态）、停止、重启等。

在 uCPE 上部署 VNF 流程为：

1）Image 文件上传；

2）创建 VNF Profile；

3）创建业务 template，选择外置和内置模式，指定业务链（VNF 序列和入

链流分类规则）和每个 VNF 部署参数；只有外置模式，才能拉起 SD-WAN Router VNF。

4）在 uCPE 上选择 template，部署 VNF；

5.4 Overlay 隧道

在 SD-WAN 的网络连接里面，存在两个不同的网络互联层面，一个是 Underlay 网络，另外一个 Overlay 网络。

Underlay 的网络连接即我们通常说的 WAN，可以是运营商提供的 private network 也可以是 Internet 等 public network。如果 SD-WAN 业务是承载在 Internet 等 public network 上，一般采用 IPSEC 等加密隧道技术。

SD-WAN Overlay 连接，是联接企业两个不同站点的 Edge 设备的隧道，依托底层的 Underlay 运营商 WAN 提供的 IP 可达性，但是与具体的底层的 Underlay 技术无关。

从方案提供者角度，两者分别由不同的解决方案提供商提供，前者是由具备专线和 Internet 等 WAN 线路资源的运营商提供，后者则由企业的 SD-WAN 解决方案提供商提供。

SD-WAN 通过 VPN 功能实现单租户多部门间的业务隔离。VPN 是 SD-WAN 上虚拟隔离网络的简称，每个 VPN 是一个独立的 IP 三层私有网络，多个不同的 VPN 端到端从连接站点的 Tunnel 到站点的 CPE 设备，都实现了彼此的逻辑隔离，互相无法直接访问。具体到企业的多个部门隔离，就是针对每个部门分别规划定义一个 VPN。在数据报文封装中，可以通过 VXLAN VNID 或 GRE Key 等来区分不同 VPN。

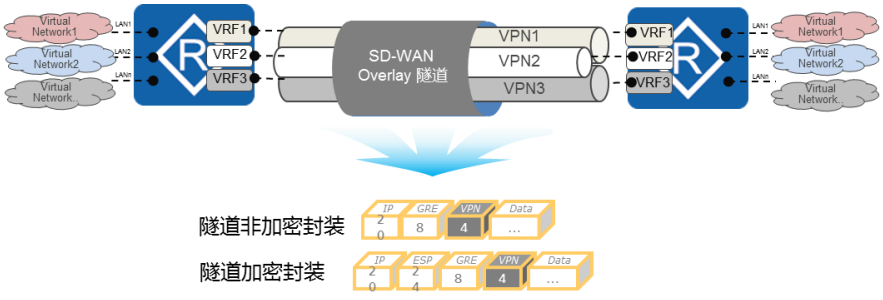

图 4 overlay 隧道封装

6. SD-WAN 典型应用场景

基于 SD-WAN 的定义，实际上 SD-WAN 的应用场景可归纳为三类：企业站点互联，数据中心互联及多云互联场景。

6.1 企业站点互联

针对企业站点互联的需求，SD-WAN 服务可以采用 Internet、4G、MPLS VPN 等多种方式构建高性价比的广域网，企业用户可以不影响现有广域网络架构的同时，将整个企业网络升级至 SD-WAN 网络[10]。

通常而言，企业站点从服务部署和人员密度上分为三个类型：

1）重要站点，一般是指企业总部或者研发中心，这类站点通常部署了重要的应用服务器，且人员数量众多，应用类型复杂，对网络安全性和可靠性要求高。通常已经部署了 MPLS VPN 线路，并且有一定的冗余性。对于这类站点，由于企业业务的发展需要，应用类型不断增加，带来更多的带宽需求，而 MPLS VPN 相对较高的价格为企业扩展网络带宽带来了挑战。

2）中型分支结构和工厂，需要频繁的与总部或其它分支机构进行数据传输，对网络安全性和可靠性要求较高。通常已经部署了 MPLS VPN 线路。这类站点的东西向流量相对集中，应用场景最为丰富。

3）小型办公室，人员相对少，没有核心业务服务器部署在这类站点，对网络安全性和可靠性要求相对前两种站点低，但是分布广，数量多。一般采用 Internet 或者 IPsec VPN 的方式与其它站点连接。

针对上述需求，SD-WAN 可以为不同规模的企业站点提供相应的解决方案：

对于重要站点，企业可以选择 MPLS VPN 和 Internet 一起部署，通过 SD-WAN 来管理广域网流量，对于企业高优先级流量，如视频，语音，远程桌面，ERP 等应用，仍然使用 MPLS 网络连接，保证数据传输的网络品质，而对于一些对网络质量要求较低的应用，如文件传输，邮件等，通过 Internet 线路传输，来降低传输成本。SD-WAN 可以通过 MPLS VPN 线路和 Internet 线路实现高可靠性，在某一线路质量下降、带宽不足或者中断时，根据实现配置和下发到 SD-WAN 终端的策略，将应用传输自动切换到正常工作的另一条线路。以保证企业业务的连续性。

对于中型分支机构可以选择低带宽的 MPLS VPN 线路和 Internet 一起部署，也可以选择部署多运营商的 Internet 线路，来实现高可靠性。针对不同运营商的 Internet 线路，SD-WAN 终端设备可以实时监控线路的转态，通过事先定义好并下发到 SD-WAN 终端的策略，为不同的应用实时选择传输路径，在实现高可用性的同时，兼顾应用质量。

对于小型分支机构和远程用户，选择使用 Internet 连接的 SD-WAN 方案，同时 4G 网络可以作为 Internet 线路的备份，让企业客户在小型分支结构，也可以实现低成本高可靠的网络连接。同时，SD-WAN 的零配置管理功能非常切合企业在小型分支机构部署的需求。由于小型分支结构数量相对多，部分机构位置偏远，为网络部署带来了挑战。SD-WAN 设备可以实现，开箱→设备加电→接入网络→自动配置的功能，全程不需要 IT 人员现场支持，且整个过程可以通过核心控制器远程统一监控和管理。大大降低了部署成本投入，提供部署的灵活性。

6.2 数据中心互联

SD-WAN 的另一个重要应用场景是数据中心互联，数据中心承载了企业重要的应用、生产运营环境、研发环境以及产品环境。数据中心之间、数据中心和企业站点之间的连接非常重要。数据中心要求的网络质量和网络带宽也高于企业站点。SD-WAN 自身部署的灵活性可以为企业用户提供更加丰富的接入方式。数据中心本身可以提供多样的网络资源，支持多运营商的 Internet 接入，以及 MPLS VPN、专线接入等多种选择，SD-WAN 可以根据企业的需求灵活地分配网络资源，构建高效稳定以及高性价比的数据中心互联网络，同时 SD-WAN 在数据中心的部署也非常简便，企业可以选择在数据中心部署硬件的 SD-WAN 终端来实现，也可以部署虚拟的 SD-WAN 终端。

6.3 多云互联

SD-WAN 的第三个重要应用场景是多云互联，很多企业会采用多个公有云互联的架构来支撑一些企业业务。SD-WAN 面向企业将直接提供多个公有云连接，使企业业务无缝与云对接。通过快速部署、快速连接的方式，相对于传统的 MPLS/VPN 专线，SD-WAN 提出了性价比更有优势的解决方案，同时，为端到端的安全管理机制、容灾备份等应用型策略，提供了统一的方法。

7. SD-WAN 发展展望与推进建议

作为一个新兴的产业，SD-WAN 仍处于新生成长期，在蓬勃发展的同时，还存在大量的问题和挑战需要去克服和解决，主要包括：

（1）服务标准化：目前业界对于 SD-WAN 的服务内容、技术方案等，还存在不同的解读，呈现百花齐放的状态，但从产业发展的角度出来，需要对 SD-WAN 业务、服务、技术等加以标准化，通过加快制定相关的技术标准和完善行业 SD-WAN 标准体系，让用户获得统一、规范的服务体验，引导相关产业链各方的产品研发。

（2）行业监管：SD-WAN 在实现方式和业务体验上，一定程度上横跨甚至打破了现有电信业务/服务的分类，需要（对电信业务/服务分类？）重新加以梳理，特别是需要结合网络服务和信息管理的特征，针对性地提出监管的政策和要求。

（3）网络质量：用户选择 SD-WAN 服务，希望能够获得更好的网络性能、带宽调度及业务策略等，由于 SD-WAN 是承载在现有基础网络架构上，Underlay 网络是一个动态变化的网络，如何保障用户能够获得稳定的服务质量，如何在动态的网络上实施网络资源检测并实时调度，这是服务商在部署 SD-WAN 服务时面临的重要挑战。

（4）网络安全：SD-WAN 部署需直面安全方面的挑战：首先就是 SD-WAN 自身的网络管理，基于 SDN 集中控制的架构不得不面临范围更大的入侵或攻击风险；再者就是用户及企业的信息及数据因为网络的扩张而面临更多的威胁；而 SD-WAN 去 IT 中心化的模型也会提升安全防护的难度。

（5）重建生态：SD-WAN 的发展面临着设备厂商、解决方案厂商、服务提供商及基础网络运营商如何合力，创造一个共赢生态的挑战。

8. 缩略语

缩略语	英文全称	中文含义
SD-WAN	Software - Wide Area Network	软件定义广域网
MPLS	Multi Protocol Label Switch	多协议标记交换
L2/L3	Layer2/Layer3	二层/三层
VPN	Virtual Private Network	虚拟专用网络
SDH	Synchronous Digital Hierarchy	同步数字体系
MSTP	Multi-Service Transfer Platform	基于 SDH 的多业务传送平台
DDN	Digital Data Network	数字数据网
ATM	Asynchronous Transfer Mode	异步传输模式
SDN	Software Defined Network	软件定义网络
NFV	Network Functional Virtualization	网络功能虚拟化
DC	Data Center	数据中心
DCI	Data Center Interconnection	数据中心互联
WAN	Wide Area Network	广域网
LAN	Local Area Network	局域网
VAS	Value-added service	增值服务
LSO	Lifecycle Service Orchestration	生命周期业务编排
POC	Proof of Concept	验证性测试
BGP	Border Gateway Protocol	边界网关协议
SR	Segment Routing	分段路由
QoS	Quality of Service	服务质量
woc	WAN Optimization	广域网优化
SLA	Service-Level Agreement	服务等级协议
TWAMP	A Two-Way Active Measurement Protocol	双向主动测量协议

DSCP	Differentiated Services Code Point	差分服务代码点
http	HyperText Transfer Protocol	超文本传输协议
https	Hyper Text Transfer Protocol over Secure Socket Layer	超文本传输安全协议
RPC	Remote Procedure Call	远程过程调用
SaaS	Software-as-a-Service	软件即服务
KVM	Kernel-based Virtual Machine	内核内建的虚拟机
SPR	Smart Policy Routing	智能选路模块
SNMP	Simple Network Management Protocol	简单网络管理协议
NQA	Network Quality Analysis	网络质量分析
BFD	Bidirectional Forwarding Detection	双向转发检测
FW	Fire Wall	防火墙
VNF	Network Functions Virtualization	虚拟化网络功能
VM	Virtual Machine	虚拟机

附录一：联合编写单位及撰写人

中国电信：史凡

中国信息通信研究院：穆琇博、柴瑶琳、宋平、毕立波

奇安信：王茜、李敏

华为：张磊、吴波、郝卫国

阿里巴巴：陈建永、文荣

电讯盈科：周启隆

Ixia：孙宇

Spirent：周启玄

附录二：引用和参考文献

[1] Davie B S, Rekhter Y. MPLS: technology and applications[M]. Morgan Kaufmann Publishers Inc., 2000.

[2] Albert R, Jeong H, Barabási A L. Internet: Diameter of the world-wide web[J]. nature, 1999, 401(6749): 130.

[3] 赵慧玲，史凡. SDN/NFV 的发展与挑战[J]. 电信科学，2014，30(8)：13-18.

[4] 穆珹博，马军锋，徐骁麟. SDN/NFV 测试方法的研究[J]. 中兴通讯技术，2017，23(2)：27-32.

[5] Wang D W. Software Defined-WAN for the Digital Age: A Bold Transition to Next Generation Networking[M]. CRC Press, 2018.

[6] https://www.onug.net/community/working-groups/open-sd-wan-exchange/

[7] https://www.mef.net/mef-3-0-sd-wan

[8] 柴瑶琳，穆珹博，马军锋. SD-WAN 关键技术[J]. 中兴通讯技术，2019，25(2)：15-19.

[9] Jain R, Khondoker R. Security Analysis of SDN WAN Applications—B4 and IWAN[M]//SDN and NFV Security. Springer, Cham, 2018: 111-127.

[10] Yassin A, Yalcin F. Enterprise transition to Software-defined networking in a Wide Area Network: Best practices for a smooth transition to SD-WAN[J]. 2019.

SDN/NFV/AI 标准与产业推进委员会

地址：北京市海淀区花园北路 52 号

邮政编码：100191

联系电话：010-62300081

传真：010-62300094

网址：www.sdnfv.org.cn