



SD-WAN 多云聚合平台接入方案研究

牛佳¹, 颜永明¹, 赵乾艮¹, 闵佳俊², 祁松阳²

(1. 中国电信股份有限公司上海分公司, 上海 200085;

2. 上海斐立及信息科技有限公司, 上海 200003)

摘要: 对多云聚合平台的现状、用途、需求分析、基本功能、应用场景进行了详细描述, 论述了 SD-WAN 相较于传统的专线多云接入方式现状的优势。分析了多种 SD-WAN 接入多云聚合平台的组网方案并提出 SD-WAN 与专线结合实现网络链路监控的多云接入方案, 提出了 SD-WAN 入多云的网络质量监控作用、融合组网下 SD-WAN 对 underlay 专线的监控作用、融合传统专线入多云的网络架构拓扑设计、SD-WAN 与传统专线入云的分段式接入方式, 介绍了混合组网入云应用场景、综合优劣势, 从融合组网的角度体现 SD-WAN 入多云的价值。

关键词: 多云聚合平台; SD-WAN; 专线接入; 入云方案

中图分类号: TN915.41

文献标志码: A

doi: 10.11959/j.issn.1000-0801.2022020

Research on access schemes of SD-WAN multi-cloud aggregation platform

NIU Jia¹, YAN Yongming¹, ZHAO Qiangen¹, MIN Jiajun², QI Songyang²

1. Shanghai Branch of China Telecom Co., Ltd., Shanghai 200085, China

2. Shanghai Feiliji Information Technology Co., Ltd., Shanghai 200003, China

Abstract: A detailed description of the current situation, application, demand analysis, basic functions and application scenarios of the multi-cloud aggregation platform were given, and the advantages of SD-WAN compared with the traditional private line multi-cloud access mode was discussed. The networking projects of multiple SD-WAN accessing multi-cloud aggregation platforms were analyzed, a multi-cloud access scheme combining SD-WAN and dedicated line to realize network link monitoring were proposed. The network quality monitoring function of SD-WAN access to multi-cloud and the monitoring function of SD-WAN on underlay dedicated line under the fusion networking was proposed. Based on the topology design of network architecture combining traditional private line to multi-cloud and segmentalized access mode of SD-WAN and traditional private line to multi-cloud, the application scenarios of hybrid network to multi-cloud was introduced and the value of SD-WAN to multi-cloud was reflected from the perspective of fusion network by combining advantages and disadvantages.

Key words: multi-cloud aggregation platform, SD-WAN, dedicated line access, cloud access scheme

0 引言

多云聚合平台为用户提供了一个可实现统一开通、运维的混合云平台，其将多个混合云通过集中管理的专线互联，免去了用户入一朵云即需要开通一条专线的复杂场景，并可有效降低用户成本，更好地满足了用户混合公有云部署需求。SD-WAN 接入多云聚合平台，是一种云网融合产品，能在实现用户总部与分支机构网络互联的同时，打通总部服务器云化网络，总部可以选择多家公有云作为总头备份。传统专线也作为多云聚合平台的网络接入方案的一部分，实现与 SD-WAN 相融合的多云接入方案。

目前的研究方向上，SD-WAN 和多云混合的研究是比较割裂的，这与相关从业研究人员的主攻方向有关，SD-WAN 的相关研究更偏网络侧，集中在 SD-WAN 组网的应用场景、运营商对 SD-WAN 在企业组网的网络架构、SD-WAN 传输的解决方案、POP (point of presence) 点组网的网络质量研究、SD-WAN 相关隧道技术研究，甚至是云网融合的研究，但考虑网络从业人员对网络的认知能力更强，对于 SD-WAN 云侧的控制器方面内容能力会比较淡化。

业界目前对于多云聚合研究的侧重点是在如何把多个公有云在一个平台内管理，混合多云运用了如 Open Infra 的技术，解决了混合多云公有云难管理的问题，对于多云的研究更多的是云计算本身的研究，甚至是抢占云计算市场方面的经济管理类研究，侧重点多在软件开发、编程设计、平台架构的编排设计，也有关于多云的容灾备份、异地存储、安全云备份、混合云迁移、用户业务场景云功能适配推荐等云计算方面的研究方向。另外云计算的研究方向也比较广，多云遇到的不仅是管控云主机开通，还涉及块存储同步异构、关系型数据库匹配开通等问题。

目前研究把多云聚合平台和 SD-WAN 直接融

合的比较少，尽管 SD-WAN 和多云聚合平台有重合的云计算软件定义部分。本文研究侧重于将 SD-WAN 与多云聚合平台融合的研究，从传统专线入多云出发，将传统专线入多云、SD-WAN 入多云的网络拓扑结构清晰地展现，又提出传统专线融合 SD-WAN 入多云的方法、应用场景，是比较少见的云网一体化融合研究的切入点。

1 多云聚合平台相关背景

1.1 用户接入多云需求分析

RightScale 公司是云管理平台的鼻祖，它因领先的云管理、成本优化平台以及一年一度反映云基础设施采用情况的《云计算行情》报告而家喻户晓。RightScale 2021 云状况调查报告如图 1 所示，企业使用多云部署方案的趋势显而易见，多云聚合平台成为企业管理多个公有云的必然选择。

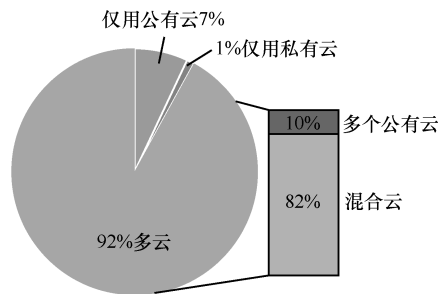


图 1 RightScale 2021 云状况调查报告（企业云策略百分比）

用户使用多云聚合平台，可以实现以下功能。

- 优化工作负载，使用最符合各项业务负载的云。
- 降低成本，允许企业的各个分支通过多云聚合平台共享专线入云。
- 将用户数据存放在多个不同的云中，提高了数据的可用性和存储效率。
- 依据业务的负载及重要程度，调整为不同的安全保护级别。

1.2 多云聚合平台基本功能

多云聚合平台支持多种入云线路申请，集成



天翼云、阿里云、腾讯云、AWS (Amazon Web services) 等多云资源申请, 统一为一个资源管理, 支持设置主机类型、磁盘、网络、安全组等操作。多资源统一纳管, 网络资源统一纳管, 将天翼云、腾讯云、阿里云、AWS 等多云操作, 收纳统筹为同一界面管理; 集成基础开关机、VNC、状态监控、产品生命周期管理; 费用管理, 多云提供商一点出账能力, 各类云提供商费用统一展现, 为 MSP (managed support pack) 提供所属客户的账单管理能力。

1.3 多云聚合平台应用场景

用户使用多个不同云提供商服务时, 会发现不同云提供商使用的底层逻辑、配置工具、监管工具的差异性很大, 在每一朵云中各自配置策略的效率很低。而多云聚合平台解决了用户的诸多痛点, 提供了面向多个公有云统一开通、运维、集成管理的工具。

首先, 多云聚合平台可实现多云纳管。它与主流云提供商的平台兼容, 允许用户在一个站点运行多个不同云平台的资源库。

其次, 它应该做到帮助客户实现智能化运维。多云聚合平台可为客户提供不同云平台的一点监测, 同时还集成了云、网、终端一体化集成

的监控服务。用户可以方便地了解整体运行状态, 掌控故障处理的进程和结果, 对故障进行详细的统计。

最后, 从云提供商的角度来看, 云管理平台也应该是一个经营分析平台。计算资费、管理资源、分析业务, 甚至提供一个开放的接口允许客户访问它们的内部 IT 系统。

2 传统专线入云

2.1 传统专线入云现状

随着云计算的快速发展, 越来越多企业利用云构建 IT 基础设施, 将应用迁移到云上。为了得到特定云服务的优势, 越来越多公司开始使用云服务, 例如, 在 Alibaba Cloud (阿里巴巴云) 上的 SAP-ERP 上进行企业资源管理, 将办公室协作放置在 Microsoft Azure 云平台上, 随着数据存储在私有云上, 企业信息技术架构逐渐成为混合连接的云模式。访问云的传统方式是企业使用多条专用线路, 面向云提供商的基于 IPsec VPN 和 VxLAN 架构的接入网关连接到不同的云^[1]。可使用 IPRAN/PTN 等中国电信专线接入多云聚合平台, 中国电信专线 IPRAN/PTN 接入多云聚合平台如图 2 所示。

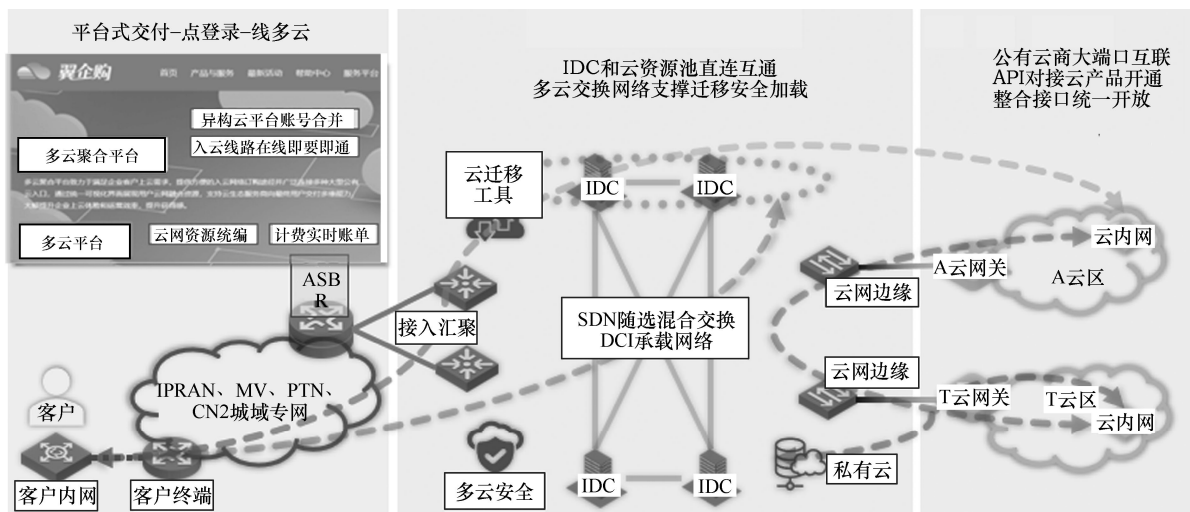


图2 中国电信专线 IPRAN/PTN 接入多云聚合平台

通过二层以太网网络和 MSTP 接入多云互联网络, 当客户接入互联网络并在访问多云的服务功能时, 须打开每个云网关的多个虚链接, 形成一个 (客户端) 访问多个点 (多个数据处理室) 的局面。为了减少虚拟链路数量, 完成真正的一线接入, 也可以在 PE 设备上开启二/三层桥接和三层转发功能, 以实现 IP 流量传输^[2]。

2.2 传统专线入云的劣势

传统专线入云, 用户不同站点需要开通多根专线入云, 所需入云专线线路较多, 资源消耗较大。传统专线入云还可能遇到资源配置较复杂、开通周期较长, 难以应对实时开通、一键开通的用户需求, 也需要一个专业的网络团队支持复杂的开通配置任务。传统专线入云还要考虑云提供商是否具备支持如此多的专线接入能力, 而多云聚合平台则可以简化过多企业使用传统专线入云的需求, 通过共用专线的形式从多云聚合平台打通多个公有云, 多个企业就可以从多云聚合平台共享多云专线入云。传统专线入云还要考虑云提供商本身对专线的支持能力, 是否对所有类型的专线接入能力做到覆盖, 一般是否仅支持个别类型的专线接入能力。传统中小企业会对传统专线的价格望而却步^[3]。

3 SD-WAN 实现入多云

3.1 SD-WAN 的网络质量监控作用

即使用户使用了 100% 的系统入云, 他们的远程业务, 零售站点、分支站点、远程工作者仍旧要通过基础设施访问入云的资源。用户可以自由定制策略监控网络质量, 用比较经济的网络访问方式访问这些云资源。同时, 使用 SD-WAN 可以与 PTN、MPLS-VPN、IPRAN 等网络相结合。SD-WAN 相对于传统专线的优势, 在于它访问多云和公有云业务能够自由定义网络访问策略, SD-WAN 提供了一种高可用性的网络连接, 能够以用户应用服务, 实时分析用户网络的质量体验监控, 动态操作网络策略, 实时监控带宽、时延、

丢包、网络抖动。SD-WAN 还可对响应时间、事务吞吐量等指标制定执行和补救决策, 如果用户主用服务应用在主链路上网络质量有所降低, 可以将主应用服务切换到质量较好的备用链路。

SD-WAN 可实现网络的自动修复, 对用户入云的应用进行可持续的网络监控质量性能评估, 原本需要一支专业的网络团队花费几个小时处理的网络问题, 通过 SD-WAN 的自动调度策略功能, 无须用户人为干预, 自动根据 SLA 降低等级较低的流量业务网络质量, 保证有高品质需求的关键业务功能保持最优的带宽性能。

3.2 SD-WAN 的入云优势

SD-WAN 适合用来作为用户分点接入多云聚合平台的手段。用户无须专线, 通过互联网, 借助 SD-WAN 的加密隧道既能保证数据传输过程的安全, 在组网成本上相较于专线得到了降低^[4]。同时 SD-WAN 继承来自 SDN 的传控分离特性, 使其具备功能丰富的网管能力, 包括网络质量实时监测和网络调度指令下发, 对拥有大量分点的用户非常友好。SD-WAN 入多云聚合平台如图 3 所示。

SD-WAN 的调度系统依据网络链路质量的探测, 自动将网络质量较差、拥塞的链路流量调度到网络质量较好的链路上, 保证对网络时延、丢包抖动要求较高用户的网络质量, 依据用户的 QoS 需求, 实现流量优选。基于应用识别是控制器中配备的 DPI 类库对流量类型进行识别, 进而根据不同流量类型, 满足用户的流量控制可选阻拦需求, 实现智能流量调度, 零配置开局可以选择性地使用 U 盘开局、邮件开局、预配置下发。U 盘开局是在控制器上先配置设备, 选择 U 盘开局, 生成开局配置文件, 导入 U 盘中。把 U 盘插入设备, 重启设备, 设备自动上线。邮件开局在控制器配置设备邮件开局发送开局邮件, 连接设备, 打开邮件, 单击开局 URL 链接, 完成邮件开局。预配置下发开局, 控制器平台更改配置模板后可以成功下发至 CPE (customer premise

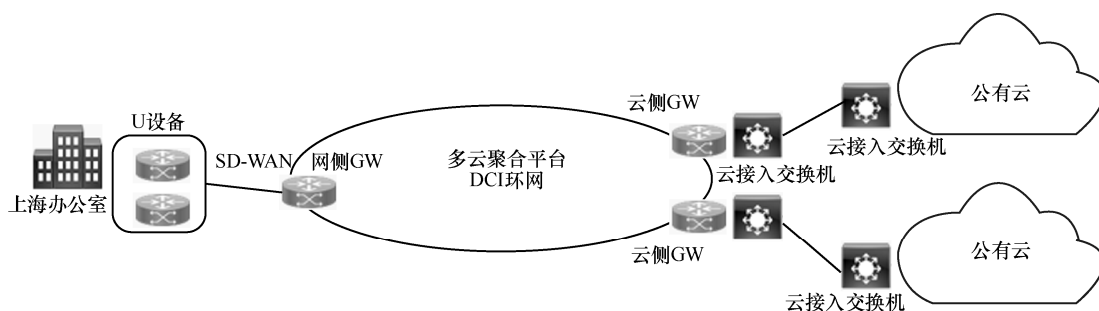


图3 SD-WAN 入多云聚合平台

equipment)。CPE 的有主备的 underlay 线路作为动态路径方案，另外有 LTE 逃生通道支持控制器的监测控制，与实际业务流量分离。

SD-WAN 可以帮助企业降低专线网络的成本，用更低价格、更高带宽的 Internet 方式接入，无须负担高昂的专线费用，有助于改善链接和部署在云中的应用访问质量。SD-WAN 入云有以下优势。

- underlay 线路支持混合链路接入（MPLS、Internet、LTE 等），充分利用线路资源。
- 控制器监控最优网络路径，支持动态调整路径，使用基于应用的智能分流技术，实现双网双用，实现负载均衡。
- 支持零配置开局，设备即插即用开局，使用邮件链接下发配置或 U 盘读取配置，控制器平台自动下发配置，快速完成业务开通，减少网络部署成本（部署周期从 4 h 降低到 20 min）。
- 支持 QoS，支持 overlay 隧道 VPN（virtual private network）自动选择线路一键按需下发配置，集成防火墙功能，完整的安全防御体系保障业务安全无忧。
- 开放平台架构，灵活扩展所需增值业务，支持安装应用加速 WoC、四层/七层防火墙 FW 等多种增值业务 VAS。
- 云端网管平台可视化运维，业务可控可视，LAN 侧、WAN 侧统一云化平台管理，实现海量分支机构 CPE 的简易可视化运维，

降低 80% 的现场维护支出。

- SD-WAN 方案减少 60% 人力和时间成本，提高带宽使用率，使专线成本下降 20%，OPEX（operating expense）支出减少 50%。
- 控制器提供 RESTful 北向 API，与第三方系统对接，可实现多个厂商的网管平台统一集成管控。
- 公有云可以部署 vCPE 的 SD-WAN 设备轻松实现企业内部网络和公有云的对接，SD-WAN 接入多云聚合平台后通过 vCPE 分段管控。

3.3 多云聚合平台接入方式

多云聚合网络侧交换平台利用云交换 DCI（data center Internet）实现跨数据中心互联，通过部署云接入交换机及多云交换路由器，采用 SDN（software defined network）技术构建的基于 overlay 的随选网络，快速、敏捷提供用户接入主流公有云服务商。多云聚合网络侧交换平台网络部分主要分为云接入交换机、专线汇聚交换机、多云交换路由器、控制器 4 部分组成。多云交换路由器，支持用户业务专线接入（驻地专线、云专线），以及用户不同节点的路由发布控制，满足用户驻地网及云侧 VPC（virtual private cloud）的连通。多云聚合平台网络部署情况如图 4 所示。

3.3.1 融合组网 SD-WAN 对 underlay 专线的监控

融合组网是将专线作为 underlay 线路的一种方案融合 Internet、LTE，成为 underlay 的专线线

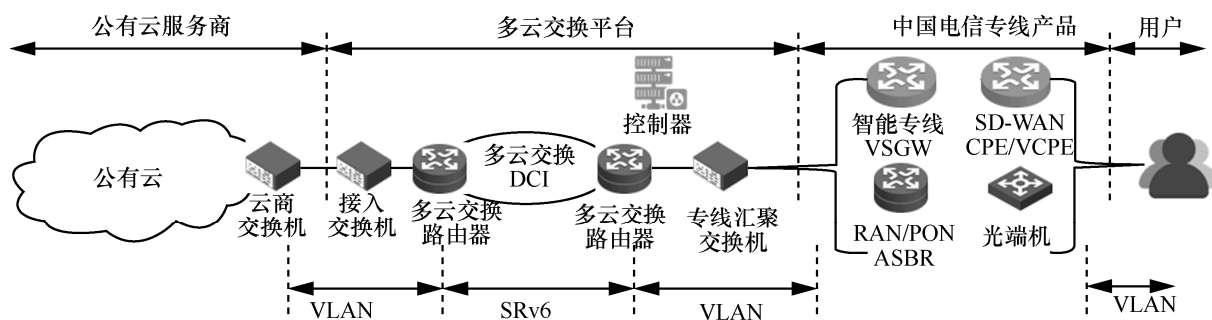


图4 多云聚合平台网络部署情况

路状态统一由 SD-WAN 网管控制器监控，SD-WAN 入多云场景如图 5 所示。在用户采用多云备份建立业务体系的情况，传统专线接入方式需要用户将多个云上的业务各自加入组建的网络，可以是二层的 PTN、IPRAN，也可以是三层

的 MPLS，本地 IPRAN、PTN 接入多云聚合平台分别如图 6、图 7 所示。

SD-WAN 用户的分支机构需要访问多云聚合平台连接的公有云资源，这时保证 SD-WAN 接入段和多云聚合平台的链接、多云聚合平台和多个

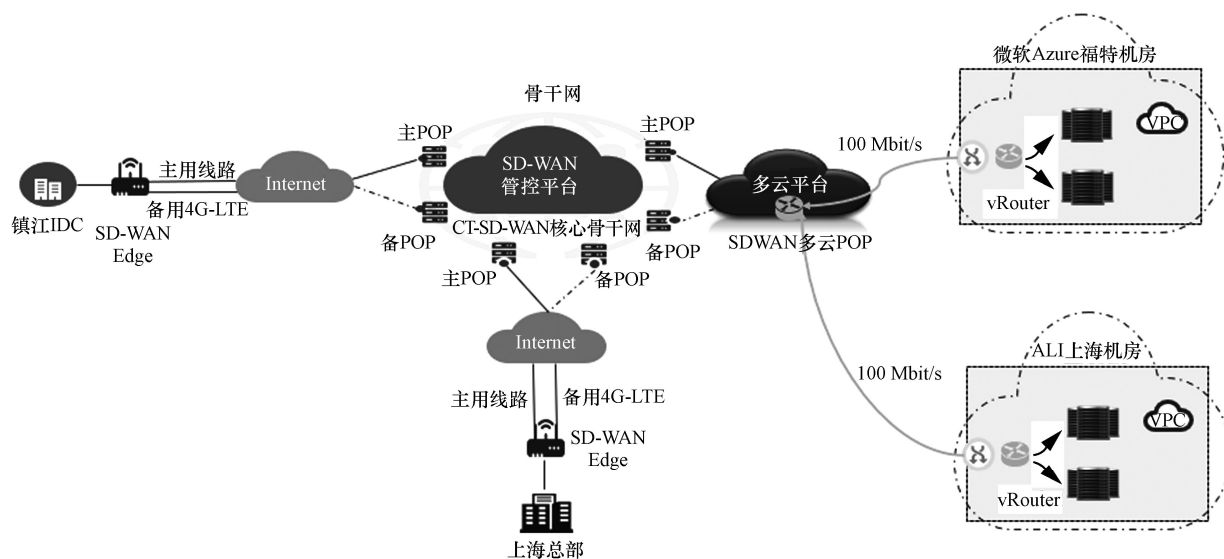


图5 SD-WAN入多云场景

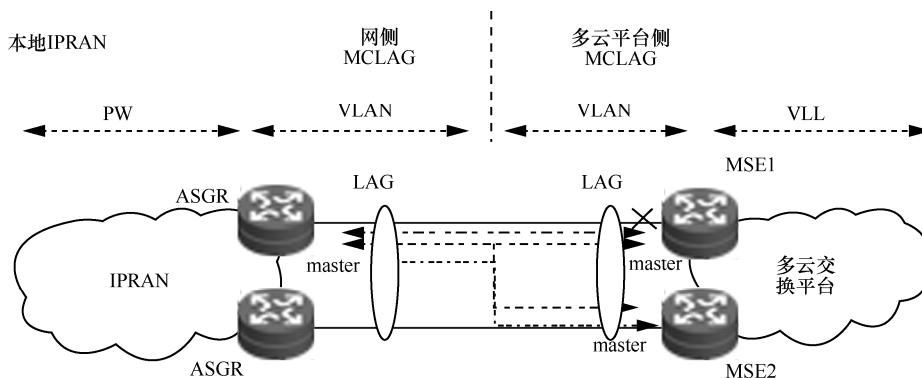


图6 本地 IPRAN 接入多云聚合平台

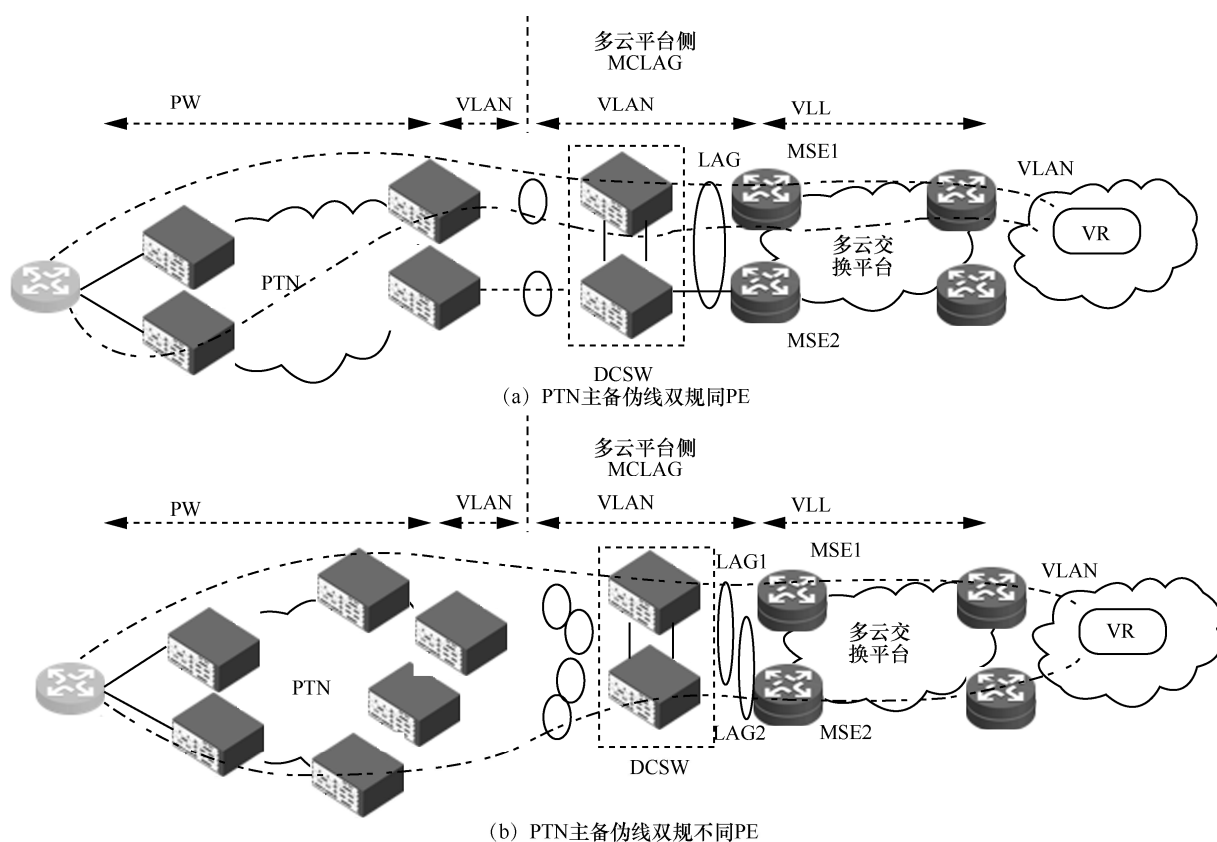


图7 PTN接入多云聚合平台

公有云之间的专线链接就至关重要，这时SD-WAN对underlay专线网络质量的监控和公有云中虚拟网络环境VPC的连通性监控就能让用户对全程全网的网络质量一目了然，减少了难以被监控的公有云内部的网络质量导致的用户不通、丢包的情况^[5]。

3.3.2 SD-WAN与传统专线入云的分段式接入

SD-WAN分段式的接入指SD-WAN接入多云聚合平台对外网络侧，多云聚合平台至用户的分支点分段加SD-WAN的隧道，这是SD-WAN原本必须具备的overlay隧道功能，控制器对多云聚合平台之外的网络设备做监控配置下发，在多云聚合平台和SD-WAN用户分支这一段打隧道。而公有云中的网络质量需要通过部署vCPE受到控制器的监控，公有云与多云聚合平台之间的公有专线是否纳入SD-WAN的监控范围内，取决于多云聚合平台以什么形式接入SD-WAN，SD-WAN

与多云聚合平台互联的网络设备是否在SD-WAN控制器的监控范围内。

如果使用端到端的方式接入，则对用户的总头部署vCPE和分部部署硬件CPE，对总头和分点之间的overlay线路逻辑化为一条线路，无须关注多云聚合平台侧网络设备的网络质量。使用分段接入方式入云专线可做underlay接入网络，再在公有云和多云聚合平台的网络设备之间增加overlay隧道，由于多云聚合平台部署在DCI环网内，可用DCI内云资源现有最近的天翼云POP点作为多云聚合平台的监控节点^[6]。

融合SD-WAN与云聚平台能力，面向大规模企业客户，提供云端、网络、海量CPE等端到端的监控管理与可视化能力，目前的SD-WAN汇总可视化能力基于与各厂商的API对接，将各个厂商SD-WAN控制器上显示的端到端，从区域站点到租户设备级别的CPE、隧道情况汇总到

一个能力聚合平台做全局化的展示,多云聚合平台更是融合了公有云端的网络质量监控能力。目前在多厂商设备组网,根据不同客户需求推荐相应的 SD-WAN 厂商测试入网,现网不涉及不同厂商设备对接同一家用户,需要硬件适配的场景,后续考虑 SD-WAN 解决方案的扩展性,实现海量业务承接,可能会对 SD-WAN 不同厂商的异构能力做深入探讨。

用户采用 SD-WAN 连接多云聚合平台,云服务专线连接多云聚合平台的分段式接入方案在较大程度获得 SD-WAN 技术优势的同时,相较于端到端方式可以节省云端 vCPE 的资源,特别是业务体量庞大的情况会考验 vCPE 的性能。但分段方式也有其劣势,首先,云端专线接入部分无法纳入 SD-WAN 的监控,只能采用 BFD (bidirectional forwarding detection) 等传统方式检测网络连通性,对高时延等网络质量下降不敏感,且用户无法掌握,分为两段管理还意味着用户需要投入更多的维护精力。

3.4 SD-WAN 与专线混合组网应用场景

零售行业企业的 IT 和运营部门在近几年面临着节省 IT 费用、提高网络效益的两大问题。IT 费用主要在硬件设备、网络和运营维护成本上有支出,使用 SD-WAN 的组网方案恰恰可以明显减少此类 IT 费用的支出。首先,零售行业必不可少的业务应用是财务和库存系统,一般客户会采用两条企业专线连接总部和数据中心,保证所有门店的数据可以持续更新、同步备份。但企业 VPN 专线网络的费用相对较高,应用数据也无法同时在两条企业专线上进行传输,所以可以将网络改造为 SD-WAN 和专线混合组网模式。

申请同样的网络带宽下,VPN 专线的费用大致为互联网线路的 1~3 倍。改造为 SD-WAN 和专线混合组网的模式可以将其中一条专线网络替换为 Internet,并同时保证关键应用的专线使用和带宽可用率。SD-WAN 设备架构整合了路由器、防

firewall、DPI 检测的功能,搭配网络管理平台便可以设定路由策略。安全方面同时还可选择 SD-WAN 供应商的安全厂商伙伴,直接从控制器平台接入防火墙功能,提供信息安全保障。新建用户节点无须 IT 网络运维人员在场,全程由运营商协助便可以完成全流程安装。控制器管理平台可以监控 SD-WAN 网络全部的线路、数据、应用等,从端到端全程可视化。网络管理不需要用复杂的代码指令命令行,直接在平台中选择对应的预定义下发模板便可以对网络进行配置。

4 结束语

多云聚合平台为用户提供了一种一次开通多个公有云,节省了反复开通专线的资费,SD-WAN 接入多云聚合平台的网络方案,又满足了企业用户需要分支接入访问公有云总头的需求,本文提出的 SD-WAN 在多云聚合平台下全程全网的网络监控,在专线网络接入多云的段落监测专线的网络质量网络设备状态,在多云聚合平台和多个公有云之间监测公有云网络的端到端监测。SD-WAN 与专线融合组网的情形下,依赖控制器对 underlay、overlay 做网络质量监测,将传统专线在多云聚合平台与 SD-WAN 的管控方式结合,以云融合传统网络,将软件定义网络的组网方式带动传统网络入云。

参考文献:

- [1] 胡先志. 通信光纤及其系统应用前沿研究[M]. 武汉: 武汉理工大学出版社, 2016.
HU X Z. Research on communication optical fiber and its application frontier[M]. Wuhan: Wuhan University of Technology Press, 2016.
- [2] 董炳泉. DWAN 提供云网融合产品能力的研究及应用[J]. 信息通信, 2019, 32(12): 245-246.
DONG B Q. Research and application of DWAN's ability to provide cloud network integration products [J]. Information & Communications, 2019, 32(12): 245-246.
- [3] 王俊敏, 徐德徕, 马强, 等. 多云环境下的集约化运营平台建设方案探讨[J]. 邮电设计技术, 2021(1): 13-17.



- WANG J M, XU D L, MA Q, et al. Discussion on construction scheme of intensive operation platform in multi-cloud environment[J]. Designing Techniques of Posts and Telecommunications, 2021(1): 13-17.
- [4] 王雄. 使用多云的 9 个理由[J]. 计算机与网络, 2018, 44(23): 40-41.
- WANG X. 9 reasons to use cloudy [J]. Computer & Network, 2018, 44(23): 40-41.
- [5] 王巍. 基于 IPv6 的 SD-WAN 部署[J]. 电信科学, 2019, 35(12): 38-42.
- WANG W. IPv6 based SD-WAN deployment[J]. Telecommunications Science, 2019, 35(12): 38-42.
- [6] 牛佳, 颜永明, 林志华. SD-WAN 隧道技术与组网模式[J]. 电信科学, 2021, 37(1): 137-146.
- NIU J, YAN Y M, LIN Z H. SD-WAN tunnel technology and network construction[J]. Telecommunications Science, 2021, 37(1): 137-146.

[作者简介]



牛佳（1995-），女，现就职于中国电信股份有限公司上海分公司，主要研究方向为数据网络、SDN 等。



颜永明（1978-），男，中国电信股份有限公司上海分公司高级工程师、综合运营监控中心经理，主要研究方向为数据网络、SDN 等。



赵乾良（1991-），男，中国电信股份有限公司上海分公司工程师，主要研究方向为网络安全、SDN 等。



闵佳俊（1998-），男，现就职于上海斐立及信息科技有限公司，主要研究方向为数据网络、SDN 等。

祁松阳（1995-），男，现就职于上海斐立及信息科技有限公司，主要研究方向为数据网络、SDN 等。