



专题：IPv6 技术与应用

基于 IPv6 的 SD-WAN 部署

王巍

(中国电信股份有限公司北京研究院, 北京 102209)

摘 要: 介绍了 SD-WAN 的发展背景及目前基于 IPv4 的 SD-WAN 方案, 提出了将 IPv6 应用到 SD-WAN 场景的方案, 分析了要实现基于 IPv6 的 SD-WAN 方案需要在现有 underlay 和 overlay 层面上做出改变, 并对利用 IPv6 技术实现 SD-WAN 的可行性进行讨论。

关键词: SD-WAN; IPv6; 软件定义网络

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2019295

IPv6 based SD-WAN deployment

WANG Wei

China Telecom Beijing Research Institute, Beijing 102209, China

Abstract: The development background of SD-WAN and the current SD-WAN scheme based on IPv4 was introduced, the scheme of applying IPv6 to SD-WAN scenario was put forward, the changes that need to be made at the existing underlay and overlay levels to realize the SD-WAN scheme based on IPv6 were analysed, and the feasibility of using IPv6 technology to realize SD-WAN was discussed.

Key words: SD-WAN, IPv6, SDN

1 引言

对于运营商来说, 传统的 MPLS VPN 专线业务通常在一张独立的骨干网上进行传输, 主要面向对网络质量要求较高的政企客户。但随着互联网的发展, 互联网的带宽资源越来越丰富, 成本也越来越低, 传统专线业务面临着很大的困境: 首先, 与面向公众的互联网接入业务相比, 专线业务的费用按照带宽收费, 价格高昂; 其次, 由于专线业务的开通需要技术人员进行现场调试,

开通周期通常比较长, 需要 20 天到几个月不等; 最后, 由于不具备可视化运维管理能力, 当网络中的设备出现故障时, 维护管理非常复杂。

许多中小型企业难以支付高昂的专线费用, 但又有专线业务的需求, SD-WAN 便应运而生。SD-WAN 与传统专线业务相比, 主要具有五点优势: 支持远程控制和零配置开局, 管理和业务发放简单; 组网成本低, 可以使分支机构的广域网基础设施费用大幅下降; 支持 VPN 以及其他增值业务, 如防火墙、流量加速等; 支持混合链路接

收稿日期: 2019-11-10; 修回日期: 2019-12-02

入, 包括 MPLS、Internet、LTE 等; 支持动态调整路径, 能够保障关键应用的体验。

SD-WAN 的出现, 让那些无法负担 MPLS VPN 费用但又有组网需求的用户能够进行 VPN 组网, 并且还提供主备倒换、灵活调速、固移融合等功能, 帮助用户降低网络成本、提升链路效率和简化业务的开通与维护。

2 SD-WAN 常用应用场景

SD-WAN 的常用场景主要分为混合组网、跨境组网和企业现网优化 3 种。

2.1 混合组网

混合组网主要针对对网络质量有一定要求的企业客户, 可通过本平台实现企业总部、各分支机构、数据中心之间的高品质混合互联组网, 为用户提供独立的、可灵活调配资源、自助式服务的组网解决方案。混合组网应用场景示意图如图 1 所示。

该场景中, SD-WAN 被用来做企业分支至 POP 点的接入, 并且在接入的过程中, 可以将数据进行加密, 保证数据传输的安全性。

由于 SD-WAN 支持混合链路接入, 使得分支节点的部署更加灵活。SD-WAN 本身开通简单的特性还能加快企业分支节点组网部署和开通时效性、简化企业运维、降低企业组网成本以及支持站点弹性增删及灵活部署。

2.2 跨境组网

跨境组网主要针对跨境公司, 境内/外网络均采用 SD-WAN 组网, 并通过 MPLS VPN 跨境专线实现境内/外互访, 实现跨境灵活组网。跨境组网应用场景示意图如图 2 所示。

SD-WAN 智能专线集中管控平台可以提供全网可视化, 方便企业总部对境内/外网络进行统一管理。

2.3 企业现网优化

企业现网优化是指企业用户保留现有 MPLS 专线网络, 融合 SD-WAN 方案, 实现混合组网, 节省部分带宽成本, 简化 IT 运维工作。企业现网优化应用场景示意图如图 3 所示。

图 3 中, 实线部分的通路表示的是企业原有的 MPLS VPN 专线网络, 在融合 SD-WAN 后, 一方面可以给线路上一份保险, 当原有 MPLS VPN

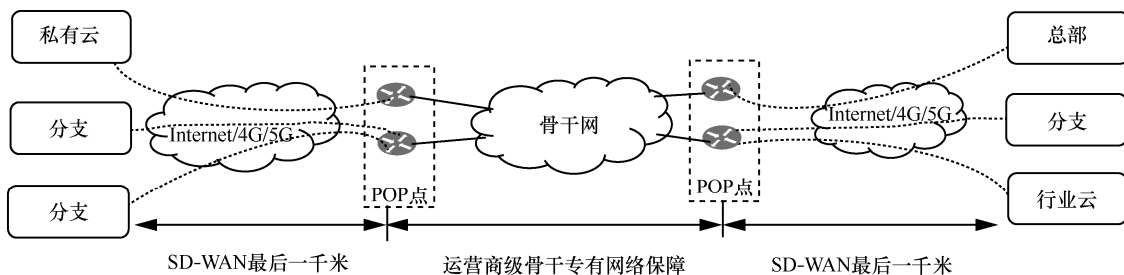


图1 混合组网应用场景示意

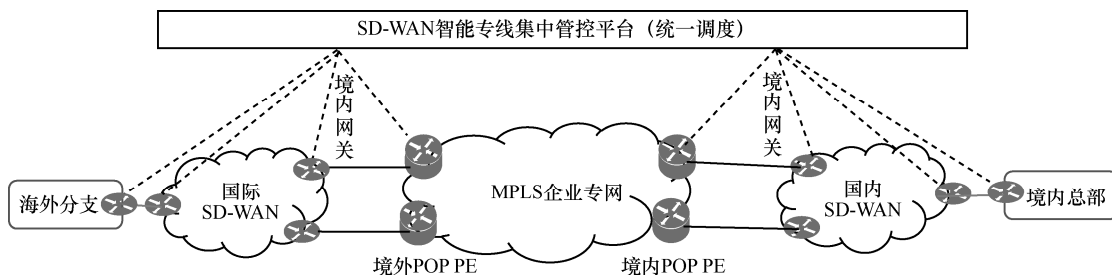


图2 跨境组网应用场景示意

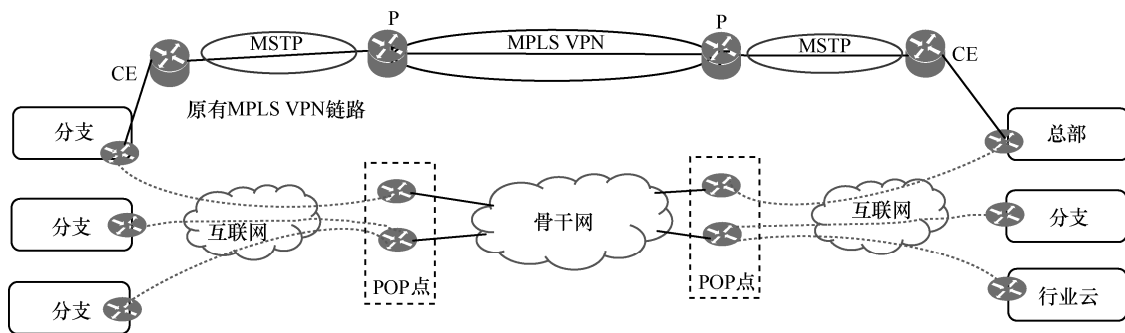


图3 企业现网优化应用场景示意

链路故障时，能够将上面的业务切换至 SD-WAN。另一方面，SD-WAN 可以起到分流作用，关键业务优先选择 MPLS VPN 专线，普通业务切换至互联网，减少业务高峰对关键业务的影响。

3 基于 IPv6 的 SD-WAN 方案

目前，业界使用的 SD-WAN 方案均是基于 IPv4 技术。然而，IPv4 地址资源的紧缺限制着网络的发展。IPv6 的出现能够解决地址不足的问题，使更多的设备能够联网，向着真正的“万物互联”时代迈进。随着国家持续大力地推动 IPv6 技术的发展，与之相关的各项技术不断完善，将 IPv6 应用于 SD-WAN 方案中，在提高数据分组转发效率、增强数据的安全性等方面有帮助。

基于 IPv6 的 SD-WAN 方案中，除了现网中

的设备需要升级为支持 IPv6 协议外，方案中 underlay 和 overlay 部分使用的协议也必须支持 IPv6。

SD-WAN 涉及的 underlay、overlay 协议见表 1。

基于 IPv6 的 SD-WAN 组网方案与基于 IPv4 的 SD-WAN 组网方案相比，网络拓扑没有变化，如图 4 所示。

A8-C 按照互联网方式接入城域网形成 underlay 通路，然后通过 VxLAN 或 IPsec 方式接入 vSGW，vSGW 部署在于 CR 直连的随选节点中，CR 双挂 CN2 和 163。vSGW 之间通过 EVPN 实现多点组网，通过 MP-BGP 协议实现私网路由的动态传递。A8-C 将流量统一传递给 vSGW，由 vSGW 分流出上网流量经城域网以及 163 到

表 1 SD-WAN 涉及的 underlay、overlay 协议及修改内容

协议类型	协议名称	修改内容
underlay	OSPFv3	取消 OSPFv2 报文中的认证字段；报头中 Version# 字段取值为 3
	IS-ISv6	新增“IPv6 可达性 CLV (IPv6 Reachability CLV)”和“IPv6 接口地址 CLV”； 在“支持协议 CLV”中的 NLPID 字段中有一个值为 0x81 的标识，表明其支持 IS-ISv6 功能
	IPv6 BGP	对 Update 消息的 NLRI 和 NEXT_HOP 属性信息进行了扩展： (1) 引入两个新的路径属性 MP_REACH_NLRI 和 MP_UNREACH_NLRI 代替了 BGP-4 的 NLRI 字段； (2) 下一跳信息支持对 IPv6 地址的支持，由于下一跳信息只是对可达路由进行通告，因此将此信息通过 MP_REACH_NLRI 属性携带，而不是在 NEXT_HOP 属性中携带
overlay	VxLAN	报文头不发生变化，仅内层的负载变成了 IPv6 报文
	IPsec	IPsec 支持 IPv6 路由协议，可以使用 AH/ESP 协议对 IPv6 路由协议报文进行加/解封封装处理
	EVPN	对 IPv6 BGP 进行扩展，定义一种新的 NLRI，即 EVPN NLRI。EVPN NLRI 定义了几种新的 IPv6 BGP EVPN 路由类型，用于处在二层网络的不同站点之间的 MAC 地址学习和发布

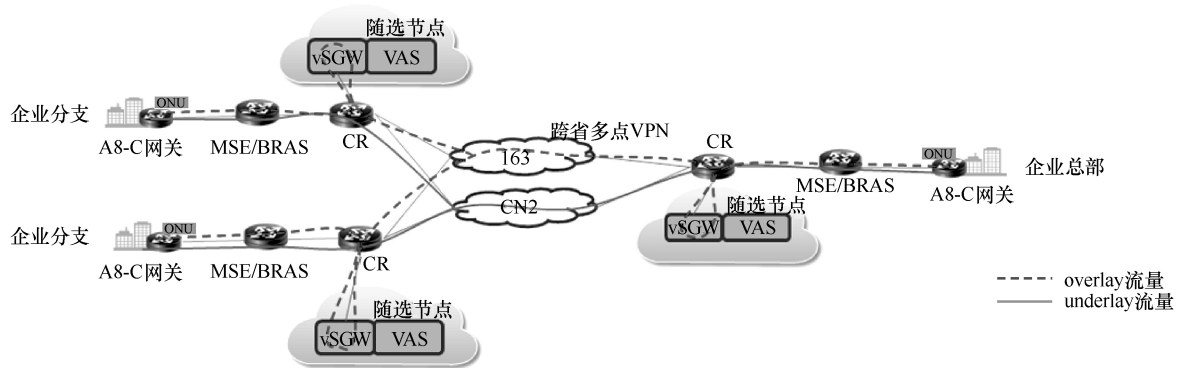


图4 基于IPv6的SD-WAN方案

Internet, 入云和VPN的流量则通过VxLAN或IPSec的方式送至对应设备。

A8-C可通过上网卡按移动接入方式接入PGW, A8-C和vSGW间建立IPSec隧道, 该IPSec隧道用作固移倒换的备用隧道。按需建设VAS服务, VAS流量通过vSGW引流, 以满足SD-WAN增值服务的可扩展性。

基于IPv6的SD-WAN方案中, 业务流量主要受EVPN、VxLAN和CN2 VPN 3种协议的控制, 这3种协议的部署方案如图5所示。

城域网CR双挂163和CN2, 保证用户的流量既能通过MPLS VPN专线(underlay)传输, 又能通过SD-WAN(overlay)传输。所有的用户流量都会由A8-C网关经VxLAN/IPSec隧道传输至vSGW, vSGW会对不同类型的流量进行区分, 并送至不同的路径。vSGW上运行EVPN协议,

通过EVPN进行组网, 并通过MP-BGP协议实现私网路由的动态传递。

对于传统MPLS VPN专线的流量, 仍然使用CN2 VPN将其引流至骨干网CN2; 对于访问Internet的流量, vSGW会直接将其送回至CR, 由CR将其传输至Internet; 对于VPN组网和入云流量, vSGW会先根据EVPN邻居表查询目的地址对应的下一跳是哪台vSGW, 并通过VxLAN/IPSec隧道把流量传递过去, 接收到流量的vSGW则会通过VxLAN/IPSec隧道将流量送至目的地址。

SD-WAN组网方案中支持通过移动方式接入, 因此很多SD-WAN方案提供商考虑将移动接入的链路作为PON接入链路的备份链路, 提高应用性能和用户体验。基于IPv6的SD-WAN固移倒换功能如图6所示。

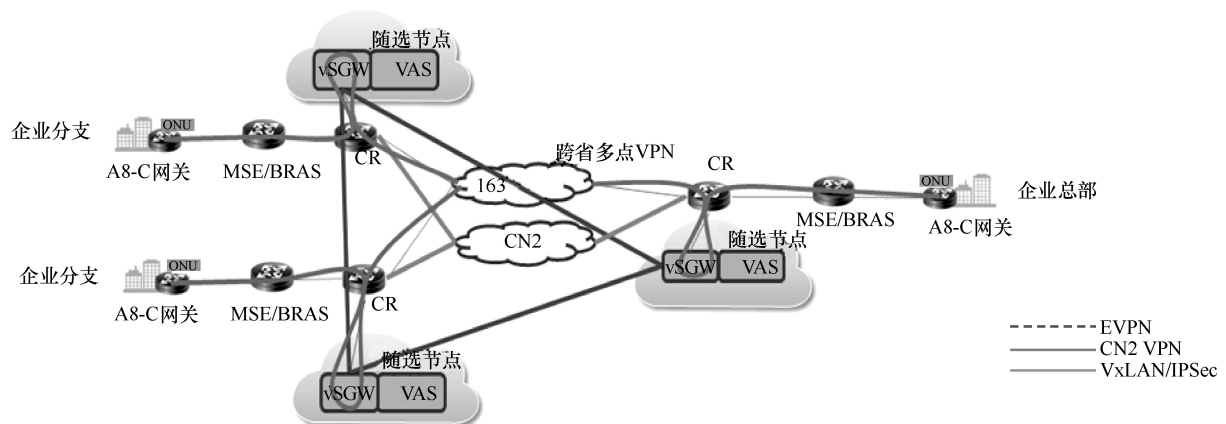


图5 EVPN、VxLAN和CN2 VPN协议的部署方案

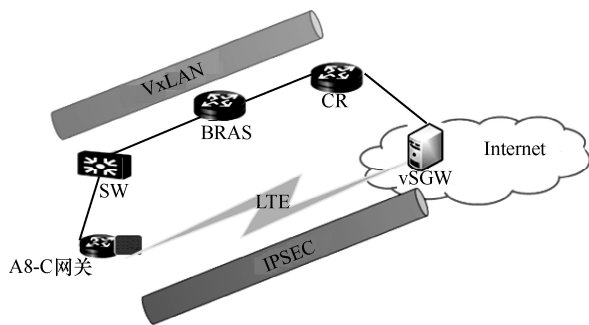


图6 SD-WAN 固移倒换方案

在 A8-C 网关上插一个 4G/5G 无线网卡, 并在网卡中插入 SIM 卡, 使 A8-C 和 vSGW 之间存在两个路径, 一条路径通过 PON 接入, 另一条通过 4G Internet 接入。PON 接入链路上建立 VxLAN 隧道, 4G Internet 接入链路上建立 IPsec 隧道。正常情况下, 流量优先走 PON 接入的路径, PON 接入的路径发生故障时, 能够自动切换到 4G Internet 接入的路径, 实现毫秒级切换。两条路径的优先级通过在 A8-C 上配置静态路由优先级来实现, 但静态路由是无状态的, 当上联接口发生故障时, 链路在逻辑上已经不通了, 但由于物理接口仍然正常, 路径就不会切换。因此, 需要在 A8-C 和 vSGW 上配置双向的 BFD, 分别探测两条隧道的可达性, 一旦发现链路不通, 就要进行固移倒换。

4 结束语

企业对专线业务的诉求, 促进 SD-WAN 的诞生和发展, 尤其对于中小企业来说, SD-WAN 的出现使组网成本大大地降低了、业务的开通和维护得以简化以及链路效率提高了。SD-WAN 可以为企业提混合组网、跨境组网和现网优化功能, 满足企业快速、灵活的组网需求。目前提出的 SD-WAN 方案皆是基于 IPv4 协议的, 基于 IPv6 的 SD-WAN 方案与其主要区别在于, 现网中设备和协议均需要支持 IPv6 协议。目前, 想要实现 IPv6 SD-WAN 主要面临的困难是: 如果让 overlay 层面使用的技术全部基于 IPv6, 那么用户内网的设备

也必须 IPv6 化, 改造成本较高, 不符合目前 SD-WAN 目标客户的需求。

随着网络技术的发展, 由 IPv4 过渡到 IPv6 是大势所趋, IPv6 技术的成熟会降低相应设备的成本, 促使用户更新支持 IPv6 的设备。下一阶段, 可以先实现 underlay 层面使用 IPv6 技术, overlay 层面使用 IPv4 技术, 然后再随着网络技术的发展, 逐步变为 overlay 和 underlay 层面都使用 IPv6 技术。基于 IPv6 技术的 SD-WAN 方案具有地址资源丰富、现网设备改造简单、支持源路由技术等优势, 有助于提升用户的网络体验, 也方便运营商对现有网络设备进行升级改造。

参考文献:

- [1] IETF. BGP-MPLS IP virtual private network (VPN) extension for IPv6 VPN: RFC4659[S]. 2006.
 - [2] IETF. OSPF for IPv6 : RFC5340[S]. 2008.
 - [3] IETF. IS-IS route preference for extended IP and IPv6 reachability: RFC7775[S]. 2016.
 - [4] IETF. Use of BGP-4 multiprotocol extensions for IPv6 inter-domain routing: RFC2545[S]. 2013.
 - [5] IETF. Multiprotocol extensions for BGP-4: RFC2858[S]. 2000.
 - [6] IETF. Virtual eXtensible local area network (VXLAN): a framework for overlaying virtualized layer 2 networks over layer 3 networks: RFC7348[S]. 2013.
 - [7] IETF. Security architecture for the internet protocol: RFC4301[S]. 2015.
 - [8] IETF. Requirements for Ethernet VPN (EVPN): RFC7209[S]. 2013.
 - [9] 顾戎, 王瑞雪, 李晨, 等. 云数据中心 SDN/NFV 组网方案、测试及问题分析[J]. 电信科学, 2016, 32(1): 126-130.
- GU R, WANG R X, LI C, et al. Analysis on network scheme and resolution test of SDN/NFV technology co-deployed in cloud datacenter[J]. Telecommunications Science, 2016, 32(1): 126-130.

[作者简介]



王巍 (1994—), 女, 中国电信股份有限公司北京研究院助理工程师, 主要研究方向为软件定义广域网 (SD-WAN)。