



专栏：随选网络

电信 SD-WAN 解决方案的关键技术

王晔

(烽火通信科技股份有限公司, 湖北 武汉 430073)

摘要: 介绍了 SD-WAN 的基本概念、应用场景及在云网一体化过程中的优势, 重点阐述了电信 SD-WAN 解决方案的关键技术, 包括开放的系统架构、丰富的部署形态、EVPN over VxLAN 专线、穿越 NAT、多核转发技术等, 为 SD-WAN 系统应用开发奠定了基础。

关键词: 软件定义广域网; 以太网虚拟专用网; 虚拟扩展局域网; IP 安全协议; 软转发

中图分类号: TN915

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2017336

Key technologies in telecom SD-WAN solution

WANG Ye

FiberHome Telecommunication Technologies Co.,Ltd., Wuhan 430073, China

Abstract: The basic concept of SD-WAN, application scenarios and the advantages in process of cloud network integration were introduced, and the key technologies of telecom SD-WAN solution were emphasized on, including open system architecture, rich deployment pattern, EVPN over VxLAN, traverse NAT, multicore soft-forwarding, etc. A solid foundation was established for the application of SD-WAN system.

Key words: SD-WAN, EVPN, VxLAN, IPSec, soft-forwarding

1 引言

随着互联网+、云计算、大数据和移动办公等业务的迅猛发展, 面向企业的云专线业务和云数据中心服务近年来高速增长, 更多的企业开始将业务应用转向云服务。企业分支与总部之间的传统专线业务通常采用运营商提供的 SDH、OTN、MPLS 等类型的专线服务, 由于跨网络、跨运营商、SLA (服务等级协议) 以及专线链路等需求, 存在业务开通周期长、网络配置复杂、灵活性较差和价格昂贵等问题。SDN/NFV 技术

的出现, 让企业新增网络服务不再依赖固有的硬件, 简化了网络配置和运维, 提高了业务部署速度, 降低了网络建设和运维成本, SD-WAN (software-defined wide area network, 软件定义广域网)^[1]随之应运而生。

2 SD-WAN 概述

SD-WAN 通过 SDN 技术将网络设备的控制和转发功能分离, 为企业用户构建业务开放、灵活编程、易于运维的广域网。同时, SD-WAN 整合 MPLS 专线、光纤、互联网、LTE 等多种

收稿日期: 2017-11-01; 修回日期: 2017-12-10



网络线路资源进行广域网的流量调度，用户能够按照预定的路由策略自主控制广域网流量的流向，帮助用户降低广域网（WAN）的开支并提高连接的灵活性。SD-WAN 典型的应用场景包括混合 WAN 场景、云接入场景和移动办公等，通过引入 SD-WAN 控制器，可完成企业各分支接入设备的集中管理和自动化配置，将企业各个分支灵活接入公有云或私有云，为用户提供可视化的、可调度的网络拓扑和流量监控，同时，可以为企业提供安全防护等云化增值服务。

中国电信 SD-WAN 解决方案基于虚拟化企业网关产品和云化业务部署，为政企客户提供灵活、智能、定制化、自动化、差异化的智能专线和云专线业务，适用于 site-site、site-internet、site-IDC 等不同的应用场景，提供企业各站点间的互联专线，企业访问国际互联网的加速服务，企业站点定向访问公有云、私有云等服务，具有敏捷开通、国际加速、混合组网和云网协同等特点。

中国电信 SD-WAN 解决方案构建基于 VxLAN 的 VPN 专线通道，提供 L2/L3 VPN、EVPN（ethernet virtual private network，以太网虚拟专用网络）、VxLAN over IPSec 等功能，为客户提供点到点、点到多点的以太网连接服务，通过以太网接口替代现有传输专线，支持 FE/GE/10GE 等多种带宽，提供可视（网络状态）、可配（自助开通）、可调（带宽、QoS）的服务。通过 SD-WAN 控制器实现集约化配置，借助网络协同和业务编排器，实现跨域端到端网络协同和业务编排，客户可自助配置，网络资源按需扩/缩容，降低部署和运营成本。SD-WAN 解决方案提供云和网络一站式服务，对云资源（如计算、存储等）、网络资源（如站点、VPN、QoS 等）可自动适配，客户可在同一界面实现对云与网资源一站开通，同时，承载网（如 IP 网、传送网等）与 DC/云资源池等统一

进行网络协同和业务编排，提供安全、高效的云接入与云互联服务。

3 SD-WAN 关键技术

3.1 开放的系统架构

传统集客专线系统架构网关设备、网管系统或控制器均由同一个厂商提供，都是烟囱式封闭系统，容易被设备厂商绑定，不利于降低 CAPEX（capital expenditure，资本性支出），如图 1 所示。SD-WAN 系统架构遵循 ETSI NFV 横向解耦的设计思想，由基础架构层、业务控制层、运维管理层和服务门户层 4 个层次组成，如图 2 所示，不同层次之间开放南北向接口，允许异厂商系统互通组网。

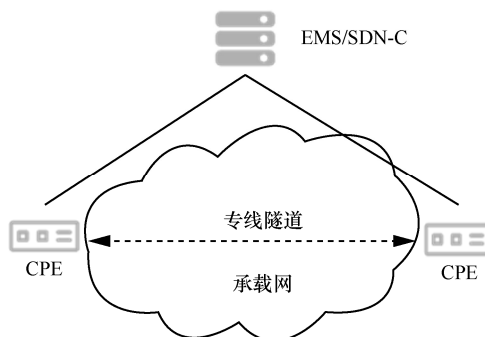


图 1 传统集客专线系统架构

- 基础架构层：由客户侧物理网元和云端的虚拟化网元互联组成，满足 site-to-site/site-to-internet/site-to-DC^[2] 不同组网应用需求。
- 业务控制层：由 SDN 控制器和 VNFM 组成，主要完成网元设备的集中管理、自动化配置和生命周期管理，控制器北向提供 REST 接口，南向接口遵循 Netconf 等协议。
- 运维管理层：通过编排器实现跨域的智能专线业务编排，北向提供 REST 接口，与第三方 OSS/BSS 系统对接。
- 服务门户层：提供统一图形化界面、实现企业专线业务自助定制，为企业提供一站式专线服务。

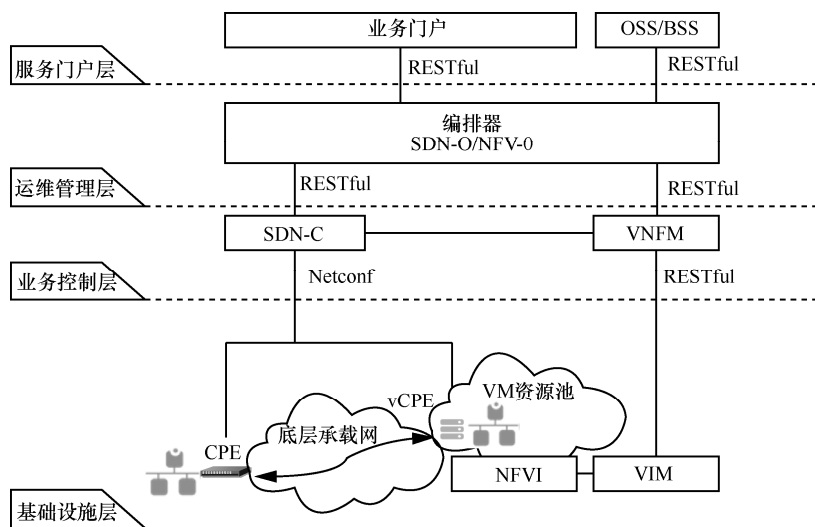


图 2 中国电信 SD-WAN 系统架构

3.2 丰富的部署形态

传统集客专线设备厂商基于专用硬件来实现网元，限制了设备性能提高，无法快速响应运营商定制化需求。在 ETSI 提出了 NFV 概念之后，使用白盒化的标准硬件将硬件设备和业务解耦是大势所趋。基于 NFV 技术打造的运行在白标准硬件上的 vCPE 产品，支持丰富的部署形态，如图 3 所示：形态一基于 x86 架构白盒机部署，适应客户侧特殊环境部署要求；形态二基于通用服务器金属裸机部署，具备更高性能；形态三基于云虚拟主机部署，部署灵活，弹性伸缩，可运行于主流商用 Hypervisor 平台。

3.3 EVPN over VxLAN 专线

EVPN 是一种 VPN 专线技术，控制平面采用 MP-BGP 协议通告 EVPN 路由信息^[3]，数据平面采用 VxLAN 封装方式转发报文（即 EVPN over

VxLAN）。

租户 overlay VPN 由分布在不同地理位置的多个站点内的虚拟机或白盒机构成。租户的物理站点分散在不同位置时，EVPN 可以基于已有的服务提供商或企业 IP 网络，在广域网上利用 VxLAN 隧道将这些站点连接起来，为同一租户的相同子网提供二层互联，也可以通过 EVPN 网关为同一租户的不同子网提供三层互联，并为其提供与外部网络的三层互联。

为了支持 EVPN 互联，MP-BGP 在传统地址族中扩展定义了新的子地址族——EVPN 地址族，并新增 EVPN 路由，支持远程跨广域网通告对端路由或 MAC 地址^[4]。EVPN over VxLAN 的强大体现在同一种 VPN 专线技术下实现 5 种典型业务模型，如图 4 所示，具体包括：

- 本地二层交换；



图 3 典型部署形态

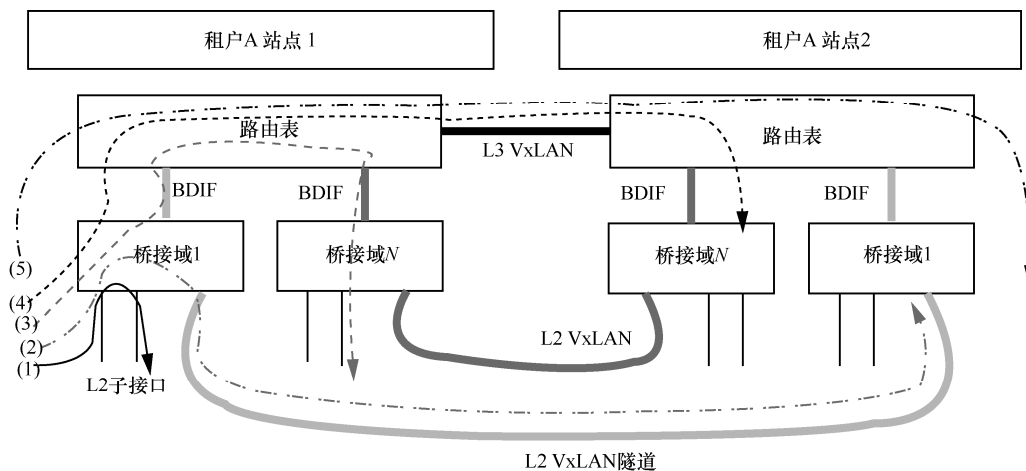


图4 以太网虚拟专用网络业务模型

- 跨广域网的大二层交换；
- 本地 L2 桥接 L3 路由；
- 跨广域网的 L2 桥接 L3 路由；
- 跨广域网的 L3 路由。

表1将EVPN专线技术与常用的VPN技术进行了横向对比分析，EVPN具备明显的优势，能够更灵活地提供穿越广域网的专线服务。

3.4 基于IPSec协议穿越NAT

IPSec是IETF制定的为保证在Internet上安全保密传送数据的一组协议，它定义了如何在IP数据分组中增加字段来保证IP分组的完整性、私有性和真实性以及如何加密数据分组。IPSec包括报文验证头协议AH（协议号51）和报文安全封装协议ESP（协议号50）两个协议。AH主要提供的功能有数据源验证、数据完整性校验和防报文重放功能，AH没有对用户数据进行加密。ESP将需要保护的用户数据进行加密后再封装到IP分组中，验证数据的完整性、真实性和私有性，可选择的加密算法有DES、3DES、AES等。

IPSec有隧道（tunnel）和传送（transport）两种工作模式。在隧道模式下，用户的整个IP数据分组被用来计算AH或ESP头，AH或ESP头和加密用户数据被封装在一个新的IP数据分组中；在传送模式中，只是传输层数据被用来计算AH或ESP头，AH或ESP头和被加密的传输层数据被放置在原IP分组头后面。

vCPE采用IPSec对用户的业务流量进行加密的保护服务，加密和认证的密钥采用IKE协商的动态密钥管理技术进行分发。除了能够提供传统的加密和认证功能，如图5所示，IPSec使用隧道模式下的ESP协议保护的是整个IP分组，对整个IP分组进行加密；ESP插入原始IP头部之前，在ESP之前再增加一个新的IP头部。

IPSec通过使用隧道模式下的ESP能实现动态NAT的穿越^[5]。vCPE通过将VxLAN专线隧道叠加在IPSec隧道之上（即VxLAN over IPSec），可以使用户业务完全感知不到NAT网关设备的存在，从而实现所有业务的NAT穿越。

表1 常见VPN技术对比

VPN技术	扩展性	易用性	支持L2/L3混合路由	支持多租户
EVPN	使用BGP作为控制层协议，扩展性好	控制层协议简单	同时支持L2和L3VPN	支持好
IPSec VPN	点到点隧道互联，扩展性差	控制层协议复杂	只支持L3VPN	支持差，配置复杂
L2TP VPN	点到点隧道互联，扩展性差	控制层协议复杂	只支持L2VPN	不支持

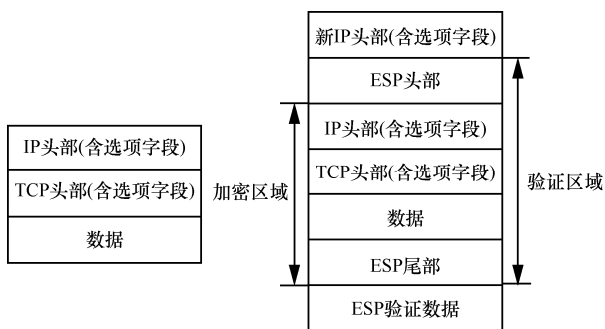


图5 ESP协议隧道模式封装

3.5 多核软转发

SD-WAN 网关设备硬件通常采用 x86 架构标准硬件,如何在 x86 多核处理器上实现高性能软转发引擎,替代传统 ASIC 芯片实现流量转发成为关键。多核软转发架构如图 6 所示,软转发引擎内部根据 CPU 内核数量定义多个转发线程,每个核心专职负责至少一个转发线程,充分发挥多核处理器并发计算效率。从多个网络端口来的报文首先进入不同优先

级的队列中排队,然后根据报文的五元组或者其他调度策略,将报文送入不同的转发线程并发处理。

实验室验证测试结果如图 7 所示,在使用 Intel E5-2630v3 型号 CPU 的 2 个核心的条件下,从 XGE 物理网口来的 128 byte 及以上 L3 报文可以实现 100% 线速转发,完全可以满足 SD-WAN 场景需求。

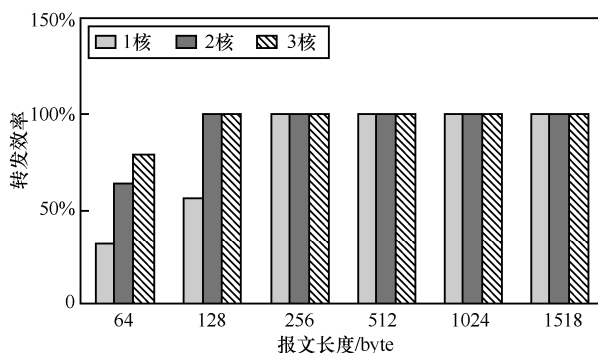


图7 多核软转发性能

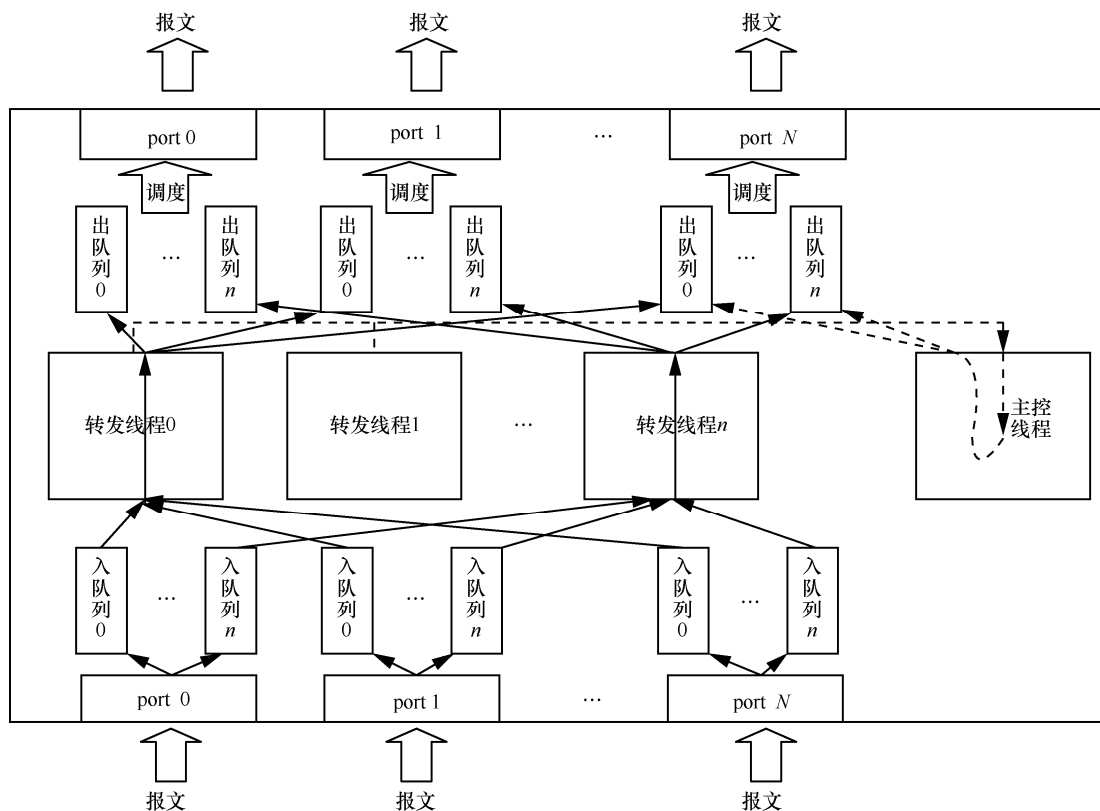


图6 多核软转发架构

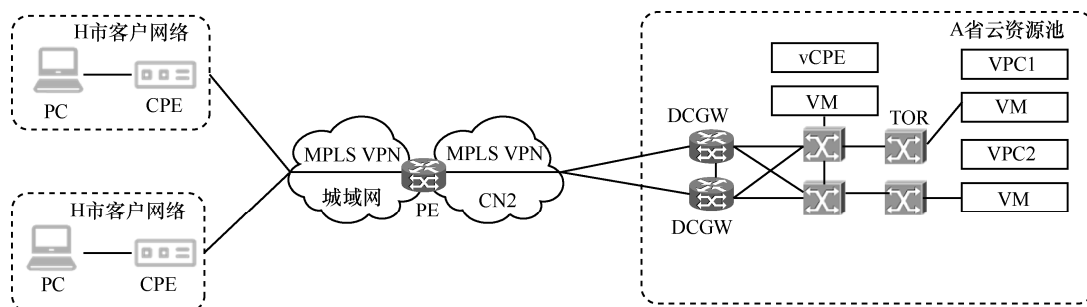


图8 云网互联应用案例

4 应用案例

中国电信 SD-WAN 解决方案应用场景灵活多样, 在云网互联场景的典型应用如图 8 所示。底层承载网利用城域网和 CN2 进行客户入云的 MPLS 专线客户侧部署 CPE 网关, 云资源池部署虚拟 CPE 网关。客户侧流量通过 VxLAN 隧道直接接入云, 对接企业部署在 vPC 上的应用服务。

在该应用案例中, 同一条 MPLS VPN 专线可以被多个租户共享复用, 在保证承载网络质量的前提下进一步降低成本。客户侧 CPE 是 x86 架构的白盒化硬件, 在降低设备采购成本的同时, 可以部署诸如 AAA 服务器或防火墙之类的增值业务软件。云端的 vCPE 完全虚拟化部署, 对于 DC 内部网络结构不做任何改变, 无缝对接租户的企业应用。

5 结束语

随着云网一体化进程的加快, SD-WAN 以其快速、智能、低成本的部署优势, 越来越受到企业及运营商的青睐。目前, 主流运营商均已在多个省公司进行了 SD-WAN 业务部署和测试, 将加快 SD-WAN 解决方案研究开发和落地实践, 推进下一代集客专线技术和新兴产品的市场应用, 共同推动 SD-WAN 产业的发展。

参考文献:

- [1] 郭晓军, 万晓兰. 重构广域网关键技术[J]. 电信科学, 2017, 33(4): 26-38.
GUO X J, WAN X L. Key technology of reconstructing WAN[J]. Telecommunications Science, 2017, 33(4): 26-38.
- [2] 王瑾. 政企业务遇瓶颈, SD-WAN 助运营商实现云网一体化[J]. 通信世界, 2017(16): 48-49.
WANG J. Enterprise business encounter bottleneck, SD-WAN help operators achieve network integration[J]. Communications World, 2017(16): 48-49.
- [3] 钟耿辉, 唐加山. 基于 VxLAN 的 EVPN 技术研究与实现[J]. 计算机技术与发展, 2017, 27(5): 46-50.
ZHONG G H, TANG J S. Research and Implementation of EVPN Technology with VXLAN[J]. Computer Technology and Development, 2017, 27(5): 46-50.
- [4] 唐宏, 朱华虹, 曹维华, 等. 基于 SDN 的大型 IP 网络 BGP 路由优化方案[J]. 电信科学, 2016, 32(3): 14-19.
TANG H, ZHU H H, CAO W H, et al. Route optimization method for BGP based on SDN in large-scale IP network [J]. Telecommunications Science, 2016, 32(3): 14-19.
- [5] 工业和信息化部. IP 安全协议 (IPSec) 穿越网络地址翻译 (NAT) 技术要求: YD/T 1468-2006[S]. 2006.
MIIT. Technical requirements of IPSec Traverse NAT: YD/T 1468-2006[S]. 2006.

[作者简介]



王晔 (1980-), 男, 烽火通信科技股份有限公司 NNFV 产品总监、高级工程师, 主要研究方向为 SDN/NFV、光通信系统和软件工程。