



基于 SDN 的政企 vCPE VPN 业务研究

扶奉超,王鹏,谢元宝

(中国电信股份有限公司广州研究院,广东 广州 510630)

摘要:SDN 已成为当前的研究热点。用 SDN 技术实现 vCPE 的主要思想是通用硬件+软件的方式实现 CPE,同时用 SDN 控制器集中管理 vCPE,并提供开放的北向可编程接口。采用此方法,不仅可以为政企客户提供丰富的增值业务,还可以加快政企客户业务部署速度,增强业务灵活部署的能力。提出了基于 SDN 技术的 vCPE 模型,并研究采用 vCPE 后,如何根据企业不同的需求实现 VPN 业务的问题。提出了 3 种适用于 vCPE 的 VPN 技术,即 VxLAN VPN、MPLS 协议 VPN 和 IPSec VPN,并从多角度比较了 3 种方法的优劣。此外还提出 VxLAN VPN、MPLS VPN 和 IPSec VPN 的融合方案,在保证 VPN 业务高安全性的同时,分别保持 VxLAN VPN 低成本的优势和 MPLS VPN 高传输速率和 QoS 保障的优势,从而使得政企客户能够根据自身带宽、安全性和时延等需求,选购灵活的随选 VPN 产品。

关键词:vCPE;软件定义网络;虚拟专用网;VxLAN;多协议标签交换;IPSec

中图分类号:TP393

文献标识码:A

doi: 10.11959/j.issn.1000-0801.2017053

Research on VPN service for government and enterprise customers in SDN-based vCPE networks

FU Fengchao, WANG Peng, XIE Yuanbao

Guangzhou Research Institute of China Telecom Co.,Ltd., Guangzhou 510630, China

Abstract: SDN technology has been studied widely recently. The main idea of SDN-based vCPE is using custom hardware and software to replace CPE. All vCPEs are managed by the SDN controller in a centralized way and the open programmable north interface can be provided. In this way, not only a wealth of value-added services can be provided for government and enterprise customers, but also the pace of deploying services can be speeded up and the flexibility can be enhanced. A SDN based vCPE model was proposed and the problem of how to realize VPN services for government and enterprise customers in SDN-based vCPE networks according to their own needs was researched. Three VPN technologies of VxLAN VPN, MPLS VPN and IPSec VPN were proposed and they were compared from different perspectives. In addition, fused schemes were proposed to combine the advantages in security, transmission rate and QoS, so that government and enterprise customers can select flexible VPN products according to their own needs in bandwidth, security, delay and others.

Key words: vCPE, software defined networking, virtual private network, VxLAN, MPLS, IPSec



1 引言

运营商一直以来为客户提供高效可靠的服务。但随着业务的快速发展,现有的架构越来越难以满足业务快速开通、高效运维、灵活可编程、面向客户定制等新的需求^[1]。SDN(software defined networking,软件定义网络)技术可以为解决上述问题提供借鉴。SDN针对的是网络架构问题,其核心思想是将网络的控制平面和转发平面相分离,利用集中化的控制平面对网络进行端到端调度,并开放可编程北向接口^[2]。目前,SDN技术已经成为业内研究热点,国内三大运营商正在积极尝试采用SDN技术进行网络升级和演进,如中国电信集团公司于2016年公布了《CTNet2025重构网络白皮书》^[3]。

作为引进SDN方案的试探,运营商首选在数据中心和城域网进行SDN实验。政企客户对运营商十分重要,在运营商的收入中占比很大。对客户来说,VPN(virtual private network,虚拟专用网)可以实现不同分公司之间以及企业和数据中心之间的互联互通,是最重要的互联网业务^[4];对运营商来说,VPN业务是政企客户收益最高的业务,必须要十分重视。然而目前政企客户面临着VPN业务开通缓慢、流程复杂、费用高以及不能根据客户需求提供其他个性化服务的问题。针对这个问题,本文研究基于SDN的vCPE(virtual customer premise equipment,虚拟用户驻地设备)方案。本方案通过用通用x86服务器+软件的方式实现CPE(customer premise equipment,用户驻地设备),实现CPE的软/硬件解耦。SDN控制器用OpenFlow、BGP等协议集中管理vCPE,并提供开放的可编程接口,能够开发丰富的增值业务,实现用户网络随选功能(即根据客户需求,快

速开通相关业务)。采用SDN实现vCPE后,传统的VPN业务实现方式将会受到影响,因此在vCPE网络中如何快速地根据客户需求开通VPN业务是个问题。

目前业内的标准化组织、运营商和设备商正积极开展vCPE研究。在标准化组织方面,最为积极的是BBF(Broadband Forum)组织,并于2016年6月发布了vCPE技术标准^[5],主要规范了vCPE技术要求和管理要求等方面。然而业内研发进展较为缓慢,大多处于解决方案、探索方案阶段。据笔者所知,现有文献中还未出现过如何用SDN技术实现vCPE以及vCPE中如何实现VPN业务的相关研究成果,因此本文具有一定的创新性。

本文主要研究了如何利用SDN技术实现vCPE的问题以及vCPE中如何实现政企VPN业务的问题。并介绍了3种最有应用前景的VPN技术,分别是以VxLAN(virtual extensible local area network,虚拟扩展局域网)为代表的overlay VPN技术、IPSec(internet protocol security,Internet协议安全)VPN技术和MPLS(multi-protocol label switch,多协议标签交换)VPN技术,分析了3种VPN技术的优缺点和成熟度,并简要讨论了VPN技术的融合方案,综合不同VPN技术的优势,为用户提供安全可靠的VPN业务。

2 基于SDN的vCPE模型

图1为基于SDN的vCPE模型。其中,vCPE是放置于政企的接入网关,可以用x86服务器的通用硬件+软件的形式构建,也可以采用具备WAN口、WLAN口、以太网口等接口的专用设备实现。通过虚拟化技术,可在vCPE上加载不同软件应用,从而可以实现向后兼容、业务快速部署和灵活扩展。SDN控制器与vCPE的接口为南向接口。

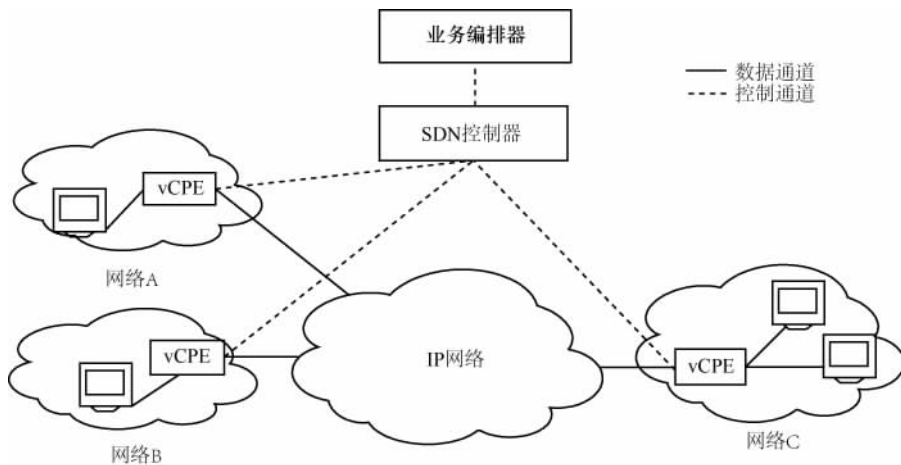


图1 基于SDN的vCPE模型

SDN 控制器利用 OpenFlow、NetConf 等南向接口协议作为转发控制分离协议,主要负责控制器和 vCPE 之间的数据交互,包括控制器下发的各种控制信息,如各种流表,也包括 vCPE 上报的状态信息、拓扑信息、告警信息等^[6]。业务编排器负责业务编排,可以提供服务在线销售的服务。政企客户可以通过 App 客户端或者 portal(门户)页面直接快速订购一些有特定网络带宽和要求的即时开通服务。业务编排器与 SDN 控制器的接口为北向接口,一般采用 RESTful 协议、NetConf 协议等实现。业务编排层通过调用 SDN 控制层可以提供 VPN 服务、防火墙服务以及其他增值服务。提供服务时,由 SDN 控制器内部的程序完成业务,而业务编排层不需要关心网络内部到底如何实现此业务^[2]。

3 基于 SDN 的政企客户 VPN 实现方法

VPN 是指虚拟专用网技术,可以将物理上分布在不同地方的网络通过公用骨干网或其他网络连接成逻辑上的虚拟子网^[4]。具有不同分支的企业及机构有 VPN 的业务需求,以实现总部与分部之间、分部与分部之间的二层访问。此外,有些企业也有企业和 IDC(internet data center,互联网数据中心)间的 VPN 业务需求。对 CPE 采用 SDN 技术会对 VPN 业务的开通方式及实现方式产生影响。基于 SDN 的 vCPE 政企 VPN 业务开通流程如下。

首先,客户在 App 客户端或者门户上申请 VPN 业务,综合考虑性能和价格,选择带宽、时延、分组丢失率、安全性等参数,下单选中 VPN 业务。业务编排器收到 VPN 业务开通请求后,通过北向接口向 SDN 控制器下发控制信息。SDN 控制器收到 VPN 开通要求后,配置网络等资源,下发相应流表,在 vCPE 处或者其他网络端点建立 VPN 隧道并控制 vCPE 的转发行为,从而实现 VPN 业务。

传统通过 CPE 实现 VPN 业务有以下几种方式,即 MPLS VPN、帧中继、IPSec VPN 等。采用 vCPE 后,除了用传统的方式实现 VPN 外,还可以用以 VxLAN 为代表的 overlay 技术实现。接下来,本文将重点阐述 vCPE 中实现 VPN 的 3 种主要技术,即 VxLAN VPN、MPLS VPN 和 IPSec VPN,比较 3 种技术的优缺点,并结合 3 种方案的优

缺点,提出融合方案。

3.1 VxLAN VPN 技术

VxLAN 技术是一种 L2 over UDP 的隧道技术。利用 VxLAN 技术可以实现不同物理位置网络的大二层连接,同时对现网的改动很小。VxLAN 利用 24 bit 的 VNID (VxLAN network identifier)区分不同的用户和业务,约为 16 MB,远远超过 VLAN 网络号仅 12 bit 的限制。与一般的隧道技术一样,VxLAN 技术也需要两端有隧道的端点。VxLAN 中的隧道端点称为 VTEP(VxLAN tunneling end point,VxLAN 隧道终端)^[7]。

图 2 为 VxLAN VPN 示意。以企业 A 和分公司通信为例,在 vCPE 收到 SDN 控制器下发的控制信息后,VxLAN VPN 实现过程如下。

企业 A 内用户的以太网数据帧在达到 VTEP 后,首先进行封装,也就是把 Ethernet 数据帧(frame)封装到 UDP 报文中,然后把用户的报文送到 IP 网络并在公网进行 IP 路由和转发,传递到分公司后,在分公司的 VTEP 进行解封装操作,并将符合以太网格式要求的用户数据传给用户。与普通的 IP 通信相比,整个过程的实现仅需要在两端 vCPE 中增加 VTEP 功能,而中间的其他网络和设备可以保持不变。

可以看出,利用 VxLAN 技术建立 VPN 隧道的方法比较简单,对现有基础网络改动较小。VxLAN VPN 由于在骨干网上跟普通 IP 转发没什么区别,仅需要改动 vCPE,企业可以只开通普通的 IP 互联网业务,与以往的 VPN 专线业务相比,成本低很多。因此 VxLAN VPN 是一种成本非常

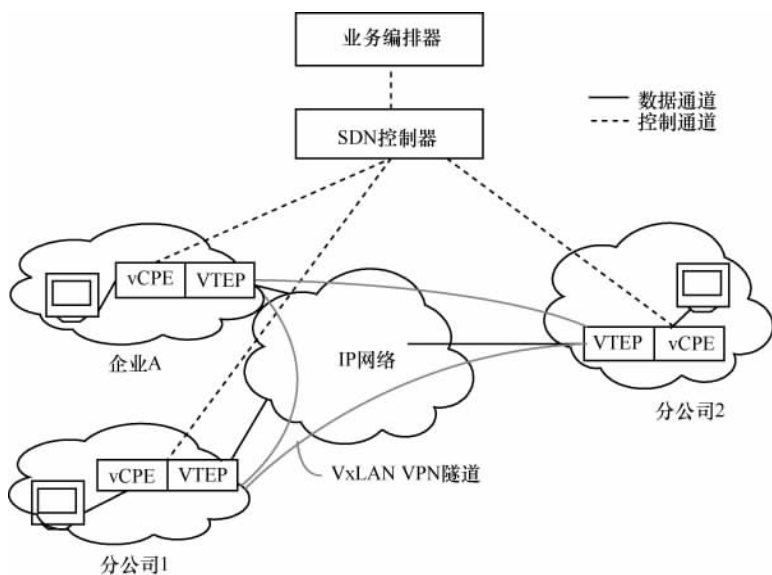


图 2 VxLAN VPN 示意



低的 VPN,非常适合于价格敏感的小企业或其他企业。

3.2 MPLS VPN 技术

虽然 VxLAN VPN 实现方式简单、价格低廉,但并不能保证 Differ-Serv(differentiated service)的 QoS(quality of service,服务质量),而 MPLS 能够和 Differ-Serv 完美配合,提供 QoS 功能。因此对价格不敏感,而对服务质量更加敏感的中大型企业更加适合 MPLS VPN^[8]。

在 MPLS 网络中,路由器在转发数据分组前,无需像传统 IP 转发一样,读取分组头和 IP 地址,只需要根据封装在 IP 头外面的标签进行精确匹配和转发即可,可以大大提高转发效率。同时路由器可以对所传数据分组提供 QoS 分级,从而大幅提高了网络服务品质。以企业 A 和分公司通信为例,vCPE 中 MPLS VPN 实现过程如下。

业务编排器收到客户 MPLS VPN 业务申请后,通过北向接口下发控制信息至 SDN 控制器。接着 SDN 控制器对 vCPE 下发流表信息。此外,SDN 控制器还需要与传统的 MPLS 管理系统进行对接通信,在 PE 处创建 MPLS instance(实例),根据用户需求指定 Differ-Serv QoS,在 MPLS 网络内创建虚拟链路 VPN。VPN 建立后,MPLS VPN 数据转发过程如下。

公司 A 的 vCPE 收到用户私网数据或二层数据报文后,根据路由信息将数据报文传递至 PE,PE 在数据报文打上 MPLS 标签后,根据预先设定的 MPLS 路径,将 MPLS 数据分组传送到分公司的 PE。PE 剥离数据报文的标签,并将符合要求的私网数据或二层数据传递给目的用户,从而完成了 MPLS VPN 通信过程。分公司与公司 A 的通信也是如此。

可以看出,vCPE 采用 MPLS VPN 具有如下优点:首先传输速度快,数据分组不再需要复杂的路由或封装,而是根据精确匹配的标签值直接在指定的路径上传递;其次,MPLS 可以根据用户的需求,保障用户 QoS,如为分组丢失敏感型视频业务和时延敏感型的语音业务提供保障;最后,MPLS VPN 可以利用现有的 MPLS 网络,不需要进行改动,这对于平滑演进 SDN 相当重要。

3.3 IPsec VPN 技术

VxLAN VPN 和 MPLS VPN 有着各自的优点,但两者的安全机制均不完善。IPsec VPN 提供了完整的保护机制,包括访问控制、无连接的完整性认证、抗重传和数据保密等,从而有效地保护了数据分组的安全^[9]。IPsec VPN 的实现方式类似于 VxLAN。实现流程如下:SDN 控制器下发

流表至 vCPE。首先 vCPE 根据 IPsec 协议,对数据分组进行认证和加密,并在 vCPE 和对端 vCPE 处进行数据分组封装和解封装的操作,然后 vCPE 将符合要求的私网数据或二层数据传送给目的用户。骨干网络进行普通的 IP 路由和转发,感知不到隧道的存在。值得注意的是,IPsec VPN 由于要进行认证、保密协商等过程,可能存在较大的时延。由于篇幅有限,本文不详述 IPsec VPN。

3.4 3 种技术的优缺点及融合方案

综上所述,3 种技术的优缺点见表 1。

表 1 vCPE 中 3 种 VPN 技术对比

VPN 技术	优点	缺点	成熟度分析	适合的场景
VxLAN VPN	价格低,实现简单	不能提供 QoS,安全性不强	较不成熟	价格敏感的中小企业
MPLS VPN	提供 Differ-Serv QoS,传输速度快,演进方式平滑	不能保障安全,价格高,安全性不强	成熟	对业务质量敏感的企业
IPsec VPN	安全性高	不能提供 QoS,可能存在较大时延	较成熟	安全性能要求高的企业

由表 1 可以看出,3 种 VPN 技术各有优缺点,适合的场景也不一样。MPLS VPN 和 IPsec VPN 比较成熟,已广泛用于其他场景,仅需要进行较简单的系统对接和改造就可以实现。而对于 VxLAN VPN,虽然短期看来,还未开发出支持 VxLAN 技术的 vCPE 设备,但 VxLAN 技术应用越来越广泛,目前已有跨 IDC(internet data center,互联网数据中心)实现互联互通的成功经验,vCPE 支持 VxLAN 是趋势。长远来看,此 3 种技术均有一定的应用价值,成熟度也会逐渐提高。

此外,MPLS VPN 和 VxLAN VPN 安全性不强,可以考虑将 IPsec VPN 分别与 MPLS VPN 和 VxLAN VPN 融合起来,使得 VPN 功能更强大,性能也更优越。IPsec VPN 与 MPLS VPN 和 VxLAN VPN 的融合操作简单,只需要在隧道端点处对原有数据分组增加相应 IPsec 分组头即可。VxLAN VPN 与 IPsec VPN 集成起来可以构建低成本、高安全性的 VPN。MPLS 与 IPsec 集成起来可以构建提供 Differ-Serv QoS、传输速率快,同时安全性高的 VPN。由于篇幅有限,本文不再详述。

4 结束语

基于 SDN 的 vCPE 可以为政企用户提供各类丰富的

增值业务, 并提供快速开通、灵活扩展业务的能力, 是 vCPE 未来发展的趋势之一。引入 vCPE 会影响传统政企 VPN 业务的实现方式。本文总结了 3 种 VPN 技术, 即 VxLAN VPN、MPLS VPN 和 IPSec VPN, 并分析了 3 种技术的优缺点、近期和远期解决方案的成熟度和适用场景。本文还简要介绍了 VxLAN VPN、MPLS VPN 分别与 IPSec VPN 的融合方案, 可以在保证 VPN 业务高安全性的同时, 分别保持 VxLAN VPN 低成本的优势、MPLS VPN 的高传输速率和提供丰富 QoS 的优势。由于 vCPE 研究领域较新颖, 业内与 CPE 相关的 CPE、SDN 控制器和业务编排器等产品均较少, 验证 vCPE 中政企 VPN 业务的性能较为困难。因此本文仅从理论上进行了分析, 未来的研究中将进行更多的实验验证。

参考文献:

- [1] 程伟强, 李晨. 电信级 SDN 在运营商网络中的应用研究[J]. 电信技术, 2016(3): 52-55.
CHENG W Q, LI C. Research on application of telecom level SDN in carrier network[J]. Telecommunications Technology, 2016(3): 52-55.
- [2] ONF. Carrier grade SDN framework draft[EB/OL]. (2016-01-13)[2016-11-01]. http://wenku.baidu.com/link?url=_VZeUBc1GCVZhZbh4jy2C4oMuV3N8sZ9Pqf5pG3Jrb7JN9sgexWTjAhM9Bz1T54KIZmPIIdGYHiHoZZOhPCb4Pel8CWe2ft0iy-DmkeBkbq.
- [3] 中国电信. CTNet-2025 网络架构白皮书[R/OL]. (2016-07-11)[2016-11-01]. http://wenku.baidu.com/link?url=b--YDer0tkuJUTHVR7gwBAFHfsB_WUKeplYZ_9e2pMIdGIotYv7f0wtzwojk-G8lGHEqSaSTrmPg9BHnNmFd5A-b_i1lITclRFgHuov6iD47.
China Telecom. CTNet-2025 network architecture white paper [R/OL]. (2016-07-11) [2016-11-01]. http://wenku.baidu.com/link?url=b--YDer0tkuJUTHVR7gwBAFHfsB_WUKeplYZ_9e2pMIdGIotYv7f0wtzwojk-G8lGHEqSaSTrmPg9BHnNmFd5A-b_i1lITclRFgHuov6iD47.
- [4] 蒋东毅, 吕述望, 罗晓广. VPN 的关键技术分析[J]. 计算机工程与应用, 2003(15): 173-177.
JIANG D Y, LV S W, LUO X G. Analysis on the key techniques in VPN[J]. Computer Engineering and Applications, 2003(15): 173-177.
- [5] BBF. Network enhanced residential gateway issue 01: TR-317[S]. 2016.
- [6] 郑毅, 华一强, 何晓峰. SDN 的特征、发展现状及趋势[J]. 电信科学, 2013, 29(3): 84-88.
ZHENG Y, HUA Y Q, HE X F. Characteristics, development and future of SDN [J]. Telecommunications Science, 2013, 29(3): 84-88.
- [7] WEERASINGHE J, ABEL F. On the cost of tunnel endpoint processing in overlay virtual networks [C]//IEEE/ACM 7th International Conference on Utility and Cloud Computing (UCC), Dec 8-11, 2014, London, England. New Jersey: IEEE Press, 2014: 756-761.
- [8] 武威, 石晶林, 勾学荣. 宽带 MPLS 网络技术综述[J]. 电信科学, 2000, 16(9): 9-13.
WU W, SHI J L, GOU X R. Overview of broadband MPLS network technology[J]. Telecommunications Science, 2000, 16(9): 9-13.
- [9] 朱昌盛, 余冬梅, 朱昌锋, 等. 将 IPSec 与 MPLS 技术结合构建虚拟专用网络[J]. 计算机应用研究, 2003, 20(7): 71-74.
ZHU C S, YU D M, ZHU C F, et al. Constructing the virtual private networks by combining IPSec and MPLS[J]. Application Research of Computers, 2003, 20(7): 71-74.

[作者简介]



扶奉超(1991-), 女, 中国电信股份有限公司广州研究院数据通信工程师, 主要从事宽带接入网技术的研究工作。



王鹏(1973-), 男, 中国电信股份有限公司广州研究院高级工程师, 主要从事宽带接入网技术的研究工作。



谢元宝(1989-), 男, 中国电信股份有限公司广州研究院移动通信工程师, 主要从事 LTE 网络关键技术的研究工作。