 DOI: https://doi.org/10.12349/iser.v5i6.2946

Research and Implementation of SD-WAN Intelligent Selection Special Line under the Background of 5G + Cloud Network Fusion

Lipeng Wei Chaojun Xiang Junna Duan Qian Liu Miaona Ma

China Unicom Henan Branch, Zhengzhou, Henan, 450000, China

Abstract

At present, the process of enterprise globalization is accelerating, cloud deployment and application is becoming more and more important, and industrial enterprises with multiple branches need to optimize the internal and external network performance to accelerate the application. In global or domestic branches of industrial enterprises, for confidentiality needs, often headquarters establish their own data center, but as the external network complexity, industrial branches, the requirement of flexible connection between computing platform, industrial enterprises commonly used VPN, MLPS technology in the service level agreement (SLA), network flexibility, line cost, etc., facing the pressure is more and more big. A new, intelligent and low-cost application technology urgently needs to appear to improve the competitiveness of enterprises.

Keywords

SD-WAN; intelligent road selection; aggregation gateway; front gateway; SDN controller

5G+ 云网融合背景下的 SD–WAN 智选专线承载研究及实现

魏利朋 项朝君 段俊娜 刘倩 马淼娜

中国联通河南省分公司，中国 · 河南 郑州 450000

摘 要

当前，企业全球化进程加快，云端部署应用越来越重要，多分支机构的工业企业亟须优化内外部的网络性能来为应用加速。在全球或国内设有分支机构的工业企业，出于保密需要，常在总部建立自己的数据中心，但随着外部网络复杂程度的持续提升，工业企业多分支机构、多计算平台之间灵活连接的要求不断提高，工业企业常用的VPN、MLPS等技术在服务等级协议（SLA）、网络灵活度、线路成本等方面，面临的压力越来越大。一种新的、智能化、低成本的应用技术亟待出现，以提高企业的竞争力。

关键词

SD-WAN；智能选路；汇聚网关；前置网关；SDN控制器

1 引言

论文属于云网融合领域，研究的联通 SD-WAN 智选专线基于 SDN 化网络结构，利用中国联通 CUII、互联网、4G/5G 等多种承载网络，为政企客户提供运营商级的高可靠、差异化、智能随选的创新产品。通过部署 SD-WAN 可以为客户提供灵活上云方案，助力客户业务快速上云。5G、有线多种上行，随时随地连接到总部和云，满足不同组网类型、组网规模需求，使企业能够增加分支带宽、提高灵活性并降低传统 WAN 的成本。通过应用智能选路和优化，保证办公、生产等任意地点分支的本地和云上关键应用的体验。LAN/WAN 统一云管理，即插即用、自动化部署业务，简化海量分支业务部署和运维复杂度。

【作者简介】魏利朋（1981–），女，中国河南洛阳人，硕士，高级工程师，从事数据通信研究。

2 网络方案概述

论文研究的联通 SD-WAN 智选专线基于 SDN 化网络结构，利用中国联通 CUII、互联网、4G/5G 等多种承载网络，采用 Overlay+Underlay 的网络架构实现客户接入段灵活、差异化、骨干网段的高质量网络保障的需求。在网关节点、互联网、CUII 网络上提前精准规划 VLAN、IP 地址、路由策略等，并通过划分 VRF 的方式实现客户 VPN 路由隔离。同时，从安全性角度对网关节点三层交换机上联城域网的端口进行安全访问控制，保证了企业用户数据的安全承载。构建的 SD-WAN 统一平台通过提供开放的 API 接口供其他系统调用，实现了与云联网系统的对接，结合中国联通骨干网自身的网络资源，为政企客户提供了安全可靠、成本节省和灵活高效的云网融合服务，可实现政企客户多分支机构的灵活

高效组网，帮助企业快速入云。

2.1 网络拓扑

中国联通在全国省会城市、非省会重点城市、境外部分城市进行网关节点（POP 点）部署，每个网关节点的建设包含汇聚网关和前置网关。两套汇聚网关分别上联至 CUII 网络边缘的两台 PE 设备，每套汇聚网关分别向下连接每个厂商的两个前置网关，实现前置网关到汇聚网关的链路冗余，避免汇聚网关单点故障对业务产生影响。厂商前置网关向下连接对应的客户侧终端设备，终端设备与两个前置网关建立互为主备的两条加密链路，可实现网络的链路冗余。前置网关通过交换机上联互联网出口路由器，汇聚网关通过三层交换机上联 CUII 外部 AR/ 综合 AR 路由器。

2.2 组网架构

网关节点由汇聚网关、前置网关组成，提供数据平面的加密转发，实现跨越物理网络 Overlay 隧道建立及客户业务网络通信。网关节点通过三层交换机接入 China169 网及 CUII 网，并纳入集中控制器管理，具备终结客户侧接入设备加密隧道的能力。其中前置网关主要用于终结各厂商互联网 VPN 加密隧道；汇聚网关主要用于和 CUII 预接线路资源，并且通过 API 打通业务开通流程，将租户信息同步给 CUII，实现端到端线上自动化开通，汇聚同一客户下的不同厂商的组网数据流量，以及异厂家接入终端在网关节点的互通。

3 网络方案实现

3.1 网络参数规划

3.1.1 VLAN ID 规划

接入层采用互联网隧道方式接入网关，进行业务区分和客户隔离，网关节点采用交换机进行组网，通过 VLAN 进行隔离。交换机为 underlay 网络设备，不能通过控制器下发配置，因此需要通过预配置，进行 VLAN 规划和资源预留。

3.1.2 IP 地址规划

根据 VLAN 规划，不同的网络负责分配 IP 地址。具体规划如下：

前置网关使用的 IP 地址，由城域网规划公网 IP 地址；

汇聚网关的 IP 地址由云联网自动分配私网地址；

云联网接入前置网关、自组网前置网关使用的 IP 地址由 SD-WAN 系统分配私网地址，且不能与用户地址重复。

3.2 路由策略及网络配置

3.2.1 互联网和 CUII 网

网关节点交换机上联城域网路由器，接入互联网，配置默认路由指向城域网路由器。

交换机作为 CUII 网 PE 路由器与汇聚网关之间的二层汇聚和透传交换机，配置管理 vlan ip 和到中心管理节点的 BGP 路由。

3.2.2 汇聚网关

汇聚网关与 CUII 网 PE 路由器运行 ebgp，采用 optionA 的方式进行对接，向 CUII 网 PE 路由器发布节点管理地址段路由，并接收 CUII 网发送的其他节点的管理 VPN 地址段路由以及业务 VPN 地址段路由。业务配置由控制器配置汇聚网关、PE 设备进行自动化下发。

3.2.3 多厂商前置网关

与汇聚网关通过 IBGP 的方式建立控制平面，传递客户站点路由信息，规划独立的 AS。与客户 SD-WAN 终端建立 overlay 的三层 ipsec（基于 GRE over Ipsec 或 VxLAN over Ipsec）隧道建立数据平面。

3.2.4 客户 SD-WAN 终端设备

客户 SD-WAN 终端设备为客户提供 SD-WAN 组网的最后一公里接入，SD-WAN 客户终端设备支持通过 MPLS、互联网、4G 以及 5G 多种网络接入方式。终端设备支持 ACL、QOS 等定制化网络功能，SD-WAN 系统可直接管理和配置客户设备。此设备可作为硬件设备或基于软件的路由器提供，位于物理站点上或云端，并在站点之间通过一条或多条广域网传输链路提供安全的数据平面连接，支持 ZTP（即插即用部署）。它负责流量转发、安全、加密、服务质量（QoS）、路由协议（BGP 和 OSPF），并输出性能统计数据。

3.3 可靠性设计

3.3.1 公网管理

考虑到网关节点连接公网，主要用于业务数据转发，不存储业务数据，从安全性角度对网关节点三层交换机上联互联网的端口进行安全访问控制，仅保留控制器的安全协议端口号，以及终端建立加密隧道的协议端口号，规避高风险的端口；公网访问地址仅放开特定 IP 段管理权限。

3.3.2 服务器管理

服务器网络安全将通过 CUII 内网管理 VPN 实现。

3.3.3 控制层面

运营商级的控制层面保障：通过集中平台进行终端管理、控制和定期补丁更新，防止站点设备黑客入侵，恶意篡改设备配置。集中管控平台不参与客户数据信息转发，通过控制层保障客户接入终端安全，平台部署在运营商核心 IDC，安全可靠。

加密信息安全：客户数据信息加密传输，端到端的闭环安全加密，保障客户数据隐私，防止数据篡改和信息泄露。

3.4 可扩展性设计

为了满足自动化开通、灵活组网、网络监控等需求，部署了全国 SD-WAN 统一平台，实现 SD-WAN 智选专线网关及终端集中管理、配置和监控。在此平台上可以与外部能力平台进行 API 接口调用，实现灵活扩展。除了已经实现了与云联网系统的对接外，还具备以下扩展能力。

3.4.1 北向 CUII SDN 控制器能力接口

根据 CUII SDN 控制器 API 能力平台提供标准 RESTful API 和 SDK，基于开放可编程的 API 接口和统一抽象的业务模型，具备以下接口能力：MPLS 三层 VPN（any-to-any、hub-spoke、max route、vpn-id）；MPLS 三层 VPN 预连接专线接入（PE-AC）（vpn service ce）；MPLS 三层 VPN 存量客户 RT 值的传递。

3.4.2 北向云网协同门户接口

与统一门户系统对接，主要是与三大实体相关的对接接口，分别是客户、订购和计费，订购包括订单和产品用户实体相关的接口。支持在线自助订购、提供友好用户 Portal、订单状态和详情查询。

3.4.3 南向多厂家对接 API 接口

南向厂家接口，除了可以实现自动化开通功能，还可以具备以下扩展功能：查询某个网关节点的客户网关或某个客户的网关，包含网关新开接口、更新接口、删除接口、终止接口、暂停接口、重开接口；查询某个客户所有 SD-WAN 终端或某个接入点的 SD-WAN 终端，包括 SD-WAN 终端新开接口、SD-WAN 终端更新接口、SD-WAN 终端删除接口、暂停接口、重开接口、终止接口。

3.5 保护机制

SD-WAN 客户终端设备采用双上联方式连接到多厂商前置网关设备，对应双汇聚网关以及双 CUII 网 PE 设备，形成双平面数据链路，采用主备方式。主备方式选路通过设置优先级的方式来实现，主用链路设置高优先级，备用链路设置低优先级。对于不同优先级的传输网络，采用“优先占用”的调度模式。即应用流量转发时，首先选择优先级高的链路，如果“切换指标”超出阈值或者带宽占用率超出“带宽上限”，则切换至优先级较低的链路。

4 应用场景

4.1 企业组网

针对企业多点互连，以及总部、分支机构、数据中心网络组网需求，SD-WAN 智选专线业务为客户提供灵活的组网解决方案，节省企业组网业务开通时间。产品在每个接入点为客户配置接入终端，通过加密隧道接入联通骨干网 POP 点，并通过联通骨干网为客户提供高可靠的网络保障。

针对客户不同站点的类型和特点，接入终端可以选择 MV 专线、互联网、4G/5G 等多种方式进行网络接入。客户站点只要能够上网即或是连接到 4G 网络，就能够实现站点的网络快速接入以及企业站点的灵活组网。企业数据信息传输采用加密隧道进行接入封装，无需担心数据篡改和信息泄露，同时通过联通骨干专网和冗余的网络设备，为客户准备的链路冗余保障客户网络的可靠传输。

4.2 与现有 MV 专线互通

在企业扩张和网络改造过程中，会遇到现有资源利旧、网络平滑升级的问题。针对使用 MV 专线的企业客户的网络扁平化、智能化、固移融合等需求，SD-WAN 智选专线为客户提供与企业现有网络互联互通的解决方案。帮助客户实现网络的平滑过渡和灵活应用，减少客户对网络基础设施的改造，加快了企业扩张时的新增分支或门店的上线速度。客户无需额外的网络配置操作，在自助订购时选择与现有 MV 专线打通，即可接入企业现有广域网环境，方便快捷。

4.3 企业组网线路备份

针对不同类型站点网络冗余备份的需求，SD-WAN 智选专线为客户提供差异化、层次化的备份线路解决方案。产品在每个站点为客户配置网络接入终端，提供支持 MV 专线双线，MV 专线 + 互联网，“互联网 +”4G 等组合接入方式。

对于已有 MV 专线网络和自建 IPSEC VPN 的企业客户，可以在保留原有链路的基础上，融合 SD-WAN 智选专线，实现混合组网。当客户侧本地端线路或设备出现故障时，能够通过 SD-WAN 接入互联网，终结在就近网关节点进入企业专网。该种解决方案下，两条链路互为备份，并且可以通过服务平台进行统一的资源及终端管理，实现企业网络的精细化路由管理和调度，SD-WAN 的加入可以带来备份链路运维部署的简化以及成本的降低。

5 总结与展望

联通拥有国内领先的 SDN 化骨干网络，有 334 个地市的广泛的专线网络覆盖，在网络质量和保障上具备明显的竞争优势。本项目研究的 SD-WAN 智选专线不仅可以为大型企业分支机构、总部、数据中心及行业云等提供基于专有 SD-WAN 网络保障的互联组网，也可以为中小型企业、连锁门店提供价格适中的优质组网；同时支持与企业原有 MV 专线、云资源等进行融合组网、链路备份，实现可视化网络监测、弹性带宽、智能选路、流量 SLA 调度等服务，对于跨城市、地区、国家的流量调度拥有纯互联网环境下不可替代的服务质量优势。下一步，联通集团将提升网络资源覆盖，保障业务质量；优化重点区域时延质量，提升用户时延需求；同时借助于第三方应用和合作伙伴输出更丰富的服务内容，满足客户需要，提升产品竞争力。

参考文献

[1] 廖雪玲.浅析5G赋能SD-WAN技术的应用[J].广西通信技术,2022(3):4.

[2] 黄韬,刘江,魏亮,等.软件定义网络核心原理与应用实践(上册)[M].北京:人民邮电出版社,2016.

[3] 于宝郡.电信运营商SD-WAN部署实践[J].电信快报,2023(8):6-9.

[4] 张宇.基于SD-WAN的多云接入方案研究[J].广东通信技术,2023,43(5):43-47.