文章编号：2095-2163(2022)11-0153-04 中图分类号：TP393 文献标志码：A

SD-WAN 网络技术在省级中央银行的应用研究

刘成星
(中国人民银行贵阳中心支行，贵阳 550001)

摘 要：随着中央银行信息化资源不断整合、数据不断集中，传统网络架构已不能很好地适应未来业务发展需求。本文以所调研的人民银行为例，探索利用 SD-WAN 前沿技术对中央银行省级广域网进行改造。保证全省广域网在满足高可靠、高可用、低成本的前提下，实现流量灵活调度和自动化运维，保障端到端的应用服务。

关键词：广域网；SD-WAN；流量调度；自动化运维

Application and research of SD-WAN network technology in the provincial branch of central bank

LIU Chengxing
(Guiyang Central Sub-Branch of the People's Bank of China, Guiyang 550001, China)

【Abstract】 With the continuous integration of informationization resources and data concentration of the central bank of China, the traditional network architecture can no longer meet the needs of the future business development. Taking the researched Branch of the People's Bank of China as an example, this paper explores the transformation of the provincial wide area network of the central bank by using the cutting-edge technology of SD-WAN. It ensures that the provincial wide area network can realize flexible traffic scheduling and automatic operation, and support end-to-end application services on the premise of meeting high reliability, high availability and low cost.

【Key words】 wide area network; SD-WAN; traffic scheduling; automatic operation

0 引 言

随着云计算技术的日趋成熟及广泛使用，中国人民银行正朝着资源整合、数据集中的方向不断地深入实施其信息化建设战略，传统网络架构已不能很好地适应未来业务发展需求。广域网作为连接人民银行各个分支机构的核心网络，是各分支机构开展业务必要的信息技术基础设施。本次研究所调研地区人民银行中心支行作为省会中支，为保证本级及辖内 8 个地市中心支行、71 个县级支行业务稳定运行，探索利用 SDN 技术对全省广域网进行改造升级，打造一张高可靠、高可用、极简运维的全省业务专网。

1 传统广域网的问题

在传统网络场景中，广域网与业务系统分属 2 个独立的系统。网络作为被动承载业务系统的传输通道，仅靠基于目的 IP 地址进行静态选路，无法对业务流量进行精细化管控。即便在其中部分线路故障时采用传统路由方式进行业务切换，也是将故障线路承载的所有业务全部切换，无法针对某些核心业务提供相关的保障。而在故障线路恢复后，也是将原有的全部业务进行统一回迁，并不能智能化地基于业务进行动态流量调度和线路切换。

随着人民银行业务应用的不断云化，其网络流量模型也因此要发生改变，业务对于网络的要求也越来越高。只关注网络本身的传统网络无法动态适应业务流量，很难满足业务云化后核心业务对于线路的敏态需求。本文调研的人民银行广域网存在以下问题：

(1)全网采用双设备双链路组网，广域网采用多链路并且各节点运行 OSPF 协议。地市、县级支行的运维能力相对较弱，采用手工配置方式容易出错。若产生 OSPF 路由宣告错误等事件可能会导致全省网络故障，造成不可估量的后果。

(2)业务流根据策略静态分布在广域网 2 条链路上，无法根据链路利用率、带宽、时延以及丢包率等网络品质实现自动分流。传统的策略路由和 QoS 对流量的管理与控制粒度并不精细，调度策略也不够灵活，导致现网链路的利用率极低，造成大量的资源浪费、且无法实时保障部分关键业务流量。

作者简介：刘成星(1984-)，男，硕士，工程师，主要研究方向：金融科技、网络技术。
通讯作者：刘成星 Email：35600267@qq.com

收稿日期：2022-06-02

(3)目前所调研人民银行的网络管理采用纯人工方式,自动化运维程度较低,仅通过基础网管软件对网络设备进行基础管理,无法做到拓扑、流量甚至业务的可视化呈现,出现网络故障后需由管理员通过登录设备查看日志去做详细排查,无法有效识别并快速加以恢复。人工运维对于网络维护人员的技能要求较高。由于广域网设备分散在不同区域,不同区域的运维人员技术能力也不一致,因此全省广域网运维难度极大。

2 SD-WAN 解决方案研究

为了解决该次调研地区人民银行广域网存在的各种问题,本文探索采用 SD-WAN 解决方案构建了一张开放架构、支持灵活编排并且易于运维的广域网络,用于承担该次调研地区人民银行各机构的应用流量,实现网络动态适应业务,能够基于业务按需进行灵活调度。

SD-WAN 是将控制层与转发层分离。从逻辑上可以将整个解决方案分为转发层、控制层以及编排层三个层次,如图 1 所示。这里拟对各层的作用展开探讨分述如下。

图 1 SD-WAN 层次图

Fig. 1 The hierarchy graph of SD-WAN

(1)转发层:转发层由各节点路由器设备组成,接受控制层的控制和管理,利用 SNMP、NETCONF、WEBSOCKET 等协议和控制器进行通信。采用 NQA、Netstream、Trap 等协议完成对各种数据的采集和上报。

(2)控制层:该层发挥承上启下的作用,除了提供基础网管功能外,还包含 SD-WAN 的核心控制组件以及广域网质量分析组件。控制器南向通过标准协议实现转发层硬件设备的管控。北向提供可定制的应用程序接口与第三方业务系统或云平台对接,满足后续差异化的业务需求。

(3)编排层:通过调用上层配置的应用程序接口,可以对业务进行策略定义、管理编排,还可以对全网的基础设施进行实时监控,增强网络的可视化呈现,简化网络的运维管理。这一层内置编排功能,还可通过北向接口为行内业务系统提供开发 API 接口的功能。

SD-WAN 解决方案优势主要体现在以下几点:

(1)高效的资源利用能力。SD-WAN 解决方案中的控制器采用 Telemetry 协议对全网设备和链路进行实时监控,动态获取设备和链路的资源情况,根据业务需求灵活分配硬件设施资源,提高资源利用率,节省设备及链路的投资成本。

(2)丰富的控制调度能力。SD-WAN 解决方案中的控制器是整个网络的大脑,可以基于全网的流量进行动态调度和调整。也可将符合业务需求的网络策略及时下发到全网设备中,实现资源弹性调度。

(3)极简的运维部署能力。SD-WAN 解决方案可以通过配置模板、定制化等方式对注册到控制器的硬件设备进行零配置部署,还可以通过控制器对全网设备进行配置下发。有效解决网络自动化水平低、运维复杂等管理难题。除此之外,控制器还支持丰富的南北向接口,可以通过这些接口基于实际业务需求定制化开发运维应用,进一步提升自动化运维能力。

(4)全面的状态呈现能力。实时监控全网设备及链路的变化,做到整个广域网设备状态、链路流量、链路质量和业务流量可视化展示,方便网络管理人员运维。

3 SD-WAN 技术应用

3.1 拓扑结构设计

基于 SD-WAN 的技术特点,以及人民银行广域网省级节点、市级节点和县级节点三级纵向网场景的特征,SD-WAN 整体网络拓扑结构设计如图 2 所示。整个方案主要包括省级路由器、市级路由器、县级路由器和广域网控制器等模块。

图 2 SD-WAN 组网拓扑图

Fig. 2 The networking topology of SD-WAN

该次调研地区人民银行的业务应用均采用集中式部署，其流量模型均为纵向流量，几乎不存在横向流量。因此解决方案采用省、市、县三级组网，在市县部署汇聚节点，在省级数据中心部署广域网控制器，通过 SD-WAN 控制器对全省广域网硬件设备进行管理和配置下发。

方案采用树形多级纵向网络，各级网络节点与链路均冗余部署，并且冗余设备之间部署横向虚拟化技术，将 2 台设备虚拟化为 1 台逻辑设备，保障网络结构简单可靠，方便运维。

3.2　业务网络设计

本文基于该次调研地区人民银行实际业务情况，将全省业务流量大致分为语音视频类、资金账务类、生产交互类、办公类和其他五大类。要实现一网多业务的目标，需要利用控制器在各级节点上为应用创建 VPN 通道，通过 VPN 对各业务进行区分隔离。

当设备注册上线后，可以通过控制器在各级节点上构建 GRE over IPsec 加密应用通道，形成一个无状态的 Overlay 网络。控制器实时地对链路丢包率、带宽、时延、抖动等信息进行采集，以图表形式呈现给管理员，方便其对应用流量进行灵活调度。

管理员可以通过 IP 五元组对应用进行自定义，并定义各个应用对于网络的质量要求。控制器分解输入信息后自动下发网络配置到各级节点设备上。通过实时的网络性能监测，控制器可以执行灵活的网络调度策略，根据网络现状进行流量调优，在多条链路上提供无差异的应用服务。

SD-WAN 解决方案实现了基于应用的端到端保障和调度能力，可根据业务对应用带宽、延时、丢包和抖动的要求进行灵活选路，从而实现应用的带宽和质量保障。

3.3　部署流程

SD-WAN 解决方案主要依赖自动化调度来保障关键应用的业务可靠性。核心功能包括设备零配置部署、网络业务自动化下发、多维可视化和自动化的流量调度功能。其业务整体流程如图 3 所示。对此，文中将给出阐释论述如下。

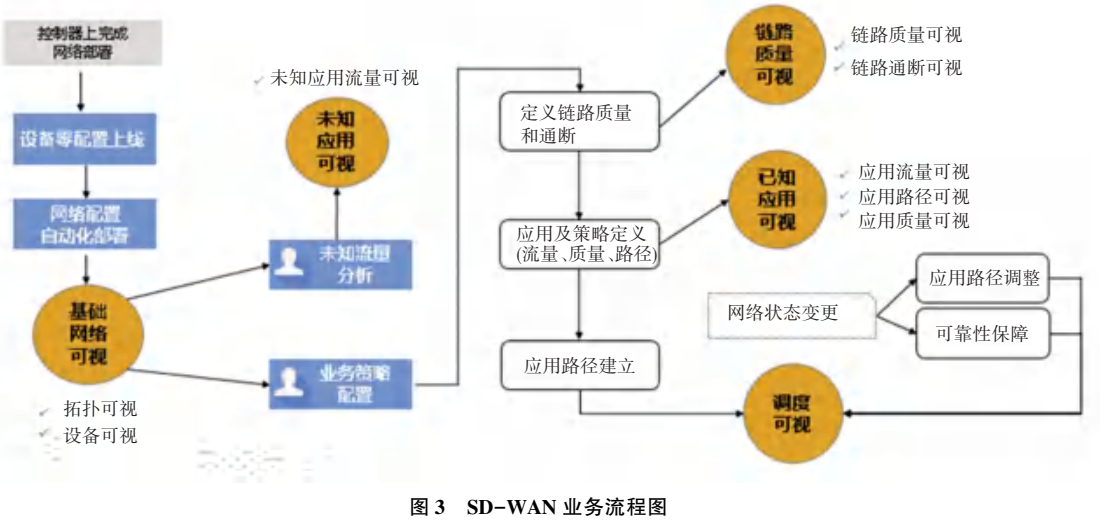

图 3　SD-WAN 业务流程图

Fig. 3　The business flow chart of SD-WAN

(1)拓扑收集

① 手动方式：在控制器上手动添加设备和链路。

②自动方式：通过协议收集设备信息和链路信息，自动呈现整网拓扑。

(2)基础网络可视

① 设备、链路信息可视：通过自动方式收集网络拓扑后，通过 Telemetry 协议实时采集，并呈现链路质量、设备状态、设备版本以及资源利用率等基础网络信息。

② 链路质量信息可视：基于物理组网拓扑，通过 NQA 技术检测并呈现链路的时延、抖动率、丢包率等信息。

(3)应用组配置。通过应用的 IP 地址和端口等信息可以自定义应用，根据应用特征，将应用划分到不同应用组，利用 QoS 的差分服务进行应用组保障。在配置应用组时，可以为不同的应用组绑定不同的带宽以及链路等，也可以为应用组配置时间段元素，使策略只在配置的时间段内生效。

(4)Overlay 网络构建。根据应用组及策略的部署情况，SD-WAN控制器可以自动构建Overlay网

（下转第 160 页）