

基于软件定义网络技术的城市轨道交通云网重构

王彪

(呼和浩特城市轨道交通投资建设集团有限公司,010020,呼和浩特//正高级工程师)

摘要 针对传统网络配置的缺点,基于 SDN(软件定义网络)技术和城轨云,提出城市轨道交通云网重构,以软件对网络资源进行虚拟化和抽象化,以软件定义实现自动化网络服务,从而适应网络设备资源池化和标准化的发展趋势。深入研究了虚拟机迁移及 SDN 等关键技术,着重阐述了 SDN 架构各接口及相关技术,进而明确了云网重构的一体化部署思路,实现了云网的一体化重构。

关键词 城市轨道交通;云网重构;软件定义网络

中图分类号 TN711.1;U231

DOI:10.16037/j.1007-869x.2021.12.012

Urban Rail Transit Cloud Network Reconfiguration Based on SDN Technology

WANG Biao

Abstract Targeting the shortcomings of conventional network configuration, based on SDN (software-defined networking) technology and urban rail cloud platform, urban rail transit cloud network reconfiguration is proposed. Network resources are abstracted and virtualized by software, and automated network services are realized by software definition, to adapt to the development trend of pooling and standardization of network equipment resources. Key technologies such as virtual machine migration and SDN are studied in-depth. Each interface and related technologies of SDN architecture are expounded emphatically. The integrated deployment idea of cloud network reconfiguration is further clarified, and the integrated reconfiguration of cloud network is realized.

Key words urban rail transit; cloud network reconfiguration; SDN (software-defined networking)

Author's address Hohhot Urban Transportation Investment and Construction Group Co., Ltd., 010020, Hohhot, China

随着云计算技术在城市轨道交通领域的广泛应用,网络设备和服务器数量急剧增加,业务迭代和快速上线诉求相应激增。相关维护人员要应对大量虚拟设备的开通和变更,须摒弃传统网络配置繁杂、业务上线迟缓、维护成本较高的模式,转而采

用更高效的、统一配置的管理工具和开放接口。

城轨云运用云计算和通信技术,通过对城市轨道交通各业务系统信息的全面感知、深度互联和智能融合,实现运营生产、运营管理、企业管理、建设管理及资源管理等业务领域的智能化、智慧化。随着城轨云技术的推进,网络虚拟化作为城轨云 IaaS(基础设施即服务)层服务之一,须对 PaaS(平台即服务)层、SaaS(软件即服务)层提供快速、弹性服务,并构建 NaaS(网络即服务)层服务。为使网络能满足上层业务系统和智慧化应用变化的智能化需求,需对网络架构进行重构。对此,城轨云引入了 SDN(软件定义网络)技术,通过软件对网络资源进行抽象、管理,并提供自动化软件定义网络服务,以适应云网资源池化、标准化下的随动发展趋势^[1]。

1 城轨云网及重构背景

1.1 城轨云概述

城轨云充分利用云计算技术,按照中心级和车站级两级架构进行部署。在正常情况下,由中心级云平台完成业务;当中心级云平台不可用时,车站级云节点作为后备模式,提供降级服务。

中心级云平台由生产中心和灾备中心构成。生产中心和灾备中心采用大带宽传输通道链接。中心级云平台分为安全生产网、内部管理网、外部服务网。其中,安全生产网与内部管理网逻辑隔离,内部管理网与外部服务网物理隔离。

安全生产网部署了列车运行自动监控系统、自动售检票系统、综合监控系统、乘客信息服务系统及门禁系统等;内部管理网部署了运营管理、企业管理、资产管理系统等;外部服务网部署了互联网购票、外部门户等公众性服务应用。

1.2 云网概念

云网在实现 OpenStack 架构 Neutron 模块解耦和轻量级管理的基础上,将 Neutron 模块同 SDN 或 NFV(网络功能虚拟化)通过北向 API(应用程序接

口)对接,将计算能力与云网的网络能力相结合,提供动态可编程能力,实现网随云动,使网络按照云的要求提供网络资源。云网在提升资源利用率和业务可靠性的同时,还实现了业务部署和管理的敏捷性。因 NFV 技术运用于电信运营商网络服务中,SDN 技术运用于园区网络和数据中心,故本文仅针对 SDN 进行研究。

1.3 云网重构的背景

重构前,云网的网络资源管理粗放,成本较大,较难支持业务系统柔性网络需求;独立的网络资源管理方式,难以适应业务融合的需求;在实现 VM(虚拟机)计划内或计划外迁移时,网络资源与安全策略随动实现成本大;云上业务和云下业务统筹管理时,网络与带宽调度、管理欠灵活。为解决上述问题,需对云网进行重构。

2 云网重构的关键技术

2.1 VM 迁移

VM 迁移的主要资源包括 CPU(中央处理器)、内存、存储、网络。在完成资源同步后,由源主机释放 VM 资源,由目的主机激活对应的 VM,则 VM 正常运行。

2.1.1 内存迁移

VM 根据服务器整体资源占用情况,选择目的主机,确定目的主机可否提供相应资源。按照迭代算法,先热同步脏页,再冷同步脏页。在热同步时,VM 保持运行;在冷同步时,VM 停止服务^[2]。

2.1.2 存储迁移

通常采用 NFS(网络文件系统)来共享数据和文件系统。此方式不需采用本地存储设备,也不需大容量磁盘迁移,不会对网络带宽造成影响。但 NFS 共享存储的方式仅局限于局域网内的 VM 动态管理。在局域网环境下,增加机器数量会使网络环境复杂,从而降低虚拟计算环境的可扩展性。在广域网环境下,如以 NFS 方式进行磁盘迁移,则会加重网络负担,导致网络延迟^[2]。

2.1.3 网络状态迁移

VM 迁移需要迁移协议状态及 IP(网际互联协议)地址等网络状态与之前保持一致。为实现无缝迁移,局域网中可利用 ARP(地址解析协议)技术绑定源 VM 的 IP 地址和目的主机。在广域网中,可利用 IP 隧道代理重定向技术及动态 DNS(域名解析)等技术构建大二层网络。在实际应用中可选择

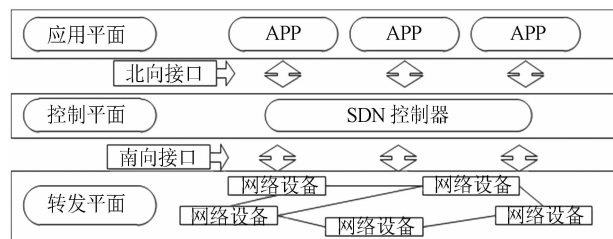
SDN 技术进行监测、触发和策略选择^[2]。

2.2 SDN 技术

SDN 技术采用转发与控制分离的架构,可提升复杂协议运算收敛速度与效率,提升传输带宽的调配效率,提高资源利用率,提升运维工作效率,降低运维成本,并提高底层基础物理设施虚拟网络的可扩展性。其通过实现可编程性,能实现 QoS(服务质量)保证^[3]。

2.2.1 SDN 架构

SDN 架构如图 1 所示。



注: APP 为应用程序。

图 1 SDN 体系架构图

Fig. 1 Diagram of SDN architecture

应用平面通过北向 API 与控制平面对接,通过与控制层通信,实现对转发平面网络设备的配置、管理和控制^[4]。

控制平面指 SDN 控制器。1 个控制器可以控制多台设备,甚至可以控制其他控制器;1 个设备也可被多个控制器控制。控制器可以是 1 台专门的物理设备,也可运行在多台集群物理服务器上,还可通过 VM 方式进行部署。

南向接口负责控制器与网络设备的通信。只有接口标准化,SDN 技术才能摆脱硬件的束缚,否则采用 SDN 技术的软件及硬件很难解耦。

转发平面对应路由器、交换机,或者是虚拟交换机之类的网络设备,通过南向接口接收控制层下发的管理、配置、控制等指令,并主动上报实时状态。

2.2.2 SDN 控制器

控制器是 SDN 网络的逻辑控制中心,通过多异构网络设备去“智能化”,使之完全服从控制器的管理指挥,实现控制和转发功能的解耦。在城轨云架构下,如控制器需管理大量设备,建议采用分布式集群技术以保障设备的高性能和高可用性,并采用高性能数据库来实现对网络和设备状态的管理。

此外,还需关注 SDN 控制器的扩展性能和安全防护能力。可采用模块化设计,防范大量伪装的合法有效报文攻击 SDN 控制器^[5]。

2.2.3 接口

SDN 控制器通过南向接口协议完成对厂商设备的管理和配置,进行链路发现、拓扑管理、策略制定、表项下发等操作。南向接口协议有 OpenFlow、NETCONF (Network Configuration Protocol) 及 PCEP(Path Computation Element Protocol) 等。

采用 OpenFlow 协议的交换机不再进行地址学习及路由计算。控制器通过二层标准协议 LLDP (链路层发现协议) 来收集域内网络设备标志和状态,对拓扑中链路进行管理,并下发流表到交换机;交换机根据流表和流表项进行数据转发^[2]。链路发现与拓扑管理可解决城轨云架构下的网络资源与安全等资源同计算资源随动的需求,降低了人工配置的复杂性。链路发现与拓扑管理实现原理如图 2 所示。

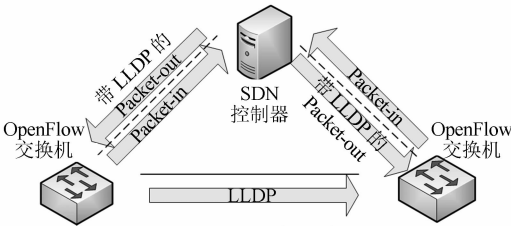


图 2 链路发现与拓扑管理实现原理
Fig. 2 Implementation principle of link discovery and topology management

SDN 控制器北向接口位于控制平面和应用平面之间。北向接口将控制器提供的网络能力和信息进行抽象,并开放给应用层。在城轨云架构下,北向接口与 OpenStack 平台的 Neutron 模块进行对接。

东西向接口能解决多个设备控制平面之间的协同工作和扩展性问题^[6]。

3 城轨云网重构架构

3.1 云网虚拟化

为提高城市轨道交通数据中心的资源利用率,降低运维管理复杂度,也为了解决部署效率低的问题,需 SDN 网络结合云计算架构进行云网重构的场景演进。OpenStack 平台是开源的 IaaS 云计算平台,也是云平台的云操作系统,主要由计算 (Nova)、对象存储 (Swift)、网络 (Neutron) 等模块组成。Nova 模块负责管理和维护计算资源,以及整个云环境虚拟机生命周期的管理。Neutron 模块用于网络虚拟化,能提供较完整的 2 层到 7 层网络的虚拟化

功能和对应的 API。Neutro 模块通过南向接口来实现与 SDN 控制器的对接,并实现 OpenStack 同 SDN 控制器及网络设备的互通,从而实现云网虚拟化的基础功能^[1]。

按照 OpenStack 平台的架构,Neutron 模块管理 OpenStack 环境中所有虚拟网络基础设施和物理网络基础设施的接入层;Nova 模块在支持各种虚拟化技术条件下,负责响应 VM 的创建请求、调度及销毁等指令。云网虚拟化的关键,是在 Neutron 模块和 Nova 模块的基础上,实现 Neutron 模块与 SDN 控制器北向 API 的对接。

云网虚拟化需分域和分层次部署 SDN 控制器,以实现网络资源配置、调度和管理的管理的转、控分离,实现业务部署的简化和自动化,进而提供敏捷服务,提高云下业务迁移上线的速度;此外,在多层、多域、多厂家组网的复杂网络中,云网虚拟化能提供端到端的管理和控制能力,提供精细控制粒度,提高系统资源利用率和运维效率。

业务发放步骤为:首先,网络管理员通过 SDN 控制器,实现各业务系统对网络资源的具体需求,并将网络资源分配给指定的业务系统;然后,计算管理员按照各业务系统的计算资源及存储资源需求,通过 VMM(虚拟机监控器)对计算和存储资源进行创建、发放、迁移或删除等操作;最后,SDN 控制器感知到 VMM 对计算资源操作后,按照策略实现网络互通和策略配置^[1]。

具体流程为:通过城轨云管理平台和 SDN 控制器,对接计算虚拟化插件与网络虚拟化插件,由 SDN 控制器和计算虚拟平台共同下发业务,进而实现计算资源与网络资源的协同发放和云网联动。

3.2 云网重构

重构后的云网以云为基础,以网络为通道,以基础设施资源为导向,能提供网络资源层、计算资源层及应用服务层的协同服务。

生产中心与灾备中心各自构建其局域网的网络资源层。通过光传送网或分组传送网等技术,实现了生产中心和灾备中心的数据互通;通过线路传输系统,实现了中心级云平台与车站级云节点的网络资源互通。在 SDN 架构下,中心级云平台与车站级云节点实现了网络软件化,可为各业务系统提供统一的网络资源能力;计算资源层主要提供计算、存储能力的虚拟化方案以及相关产品;应用服务层包含运营生产、运营管理、企业管理、资源管理、建

设管理等各类业务系统,可实现业务系统的云上及云下多点部署、单点接入、全网服务,确保业务系统不受云平台三网(安全生产网、内部管理网及外部服务网)内 VDC(虚拟数据中心)的分级限制。重构后的云网能实现三网内各业务系统端到端的整体安全保障,能保证三网内业务系统的部署及迁移具有高度灵活性,可满足各业务系统在网内 VM 迁移时的网随云动特性^[7]。

当 VM 漂移或上线后,OpenStack 平台的 Nova 模块通知 Neutron 模块对 vSwitch(虚拟交换机)进行 VLAN(虚拟局域网)配置;Neutron 模块向 SDN 控制器通告 VM 上线信息,并对 NVE(网络虚拟边缘)节点配置 Port(接口)+VLAN 到 VNI(虚拟网络接口)的映射关系,同时下发二层广播及单播转发表;SDN 控制器对 VXLAN(虚拟扩展局域网)配置 VNI 和 vBDIF(网域逻辑接口),并管理 VRF(虚拟路由转发),根据 VM 上线信息向网管下发 ARP、MAC(物理地址)及隧道表信息等。

城轨云平台通过云网重构管理界面,实现了计算资源和网络资源的统一管理,如图 3 所示。业务管理员通过管理界面统一创建计算资源和网络资源,通过 Nova 模块实现计算资源的管理与发放,通过 Neutron 模块的 API 和 SDN 控制器互通,实现了网络资源即服务能力。

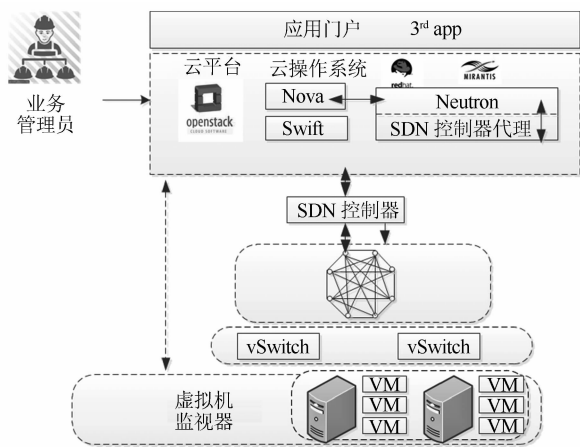


图 3 云网一体化方案

Fig. 3 Cloud network integration scheme

业务管理员通过云平台界面在 SDN 控制器同网络设备及服务器之间进行协调交互,将计算资源和网络资源分配给指定的业务系统或租户,进而实现计算资源、存储资源及网络资源的自动创建、删除和迁移等操作,不需人工配置和干预^[1]。

3.3 云网一体化部署

生产中心与灾备中心分别部署了 OpenStack 平台和 SDN 控制器,以实现 OpenStack 的 Neutron 模块解耦,并与 SDN 控制器北向 API 对接。

生产中心与灾备中心在各自 OpenStack 平台上实现运维管理。为满足稳定性和经济性要求,生产中心与灾备中心可采用 1 套云管理平台,即可同时实现 OpenStack 平台与虚拟化资源,以及 SDN 与网络设备的对接。

当生产中心和灾备中心的 VDC 分别部署 VPC(虚拟私有云)时,若要实现生产中心 VPC 和灾备中心 VPC 的互通,就需先实现网络层互通,再通过人工配置静态路由,打通生产中心和灾备中心的通道,且要求所有 VDC 的 IP 地址不重复^[8]。生产中心及灾备中心云网一体化部署方案如图 4 所示。

标准化、归一化设计的基础设施层,为网络化、虚拟化、计算虚拟化,以及业务平台、大数据系统及应用提供了通用化标准。

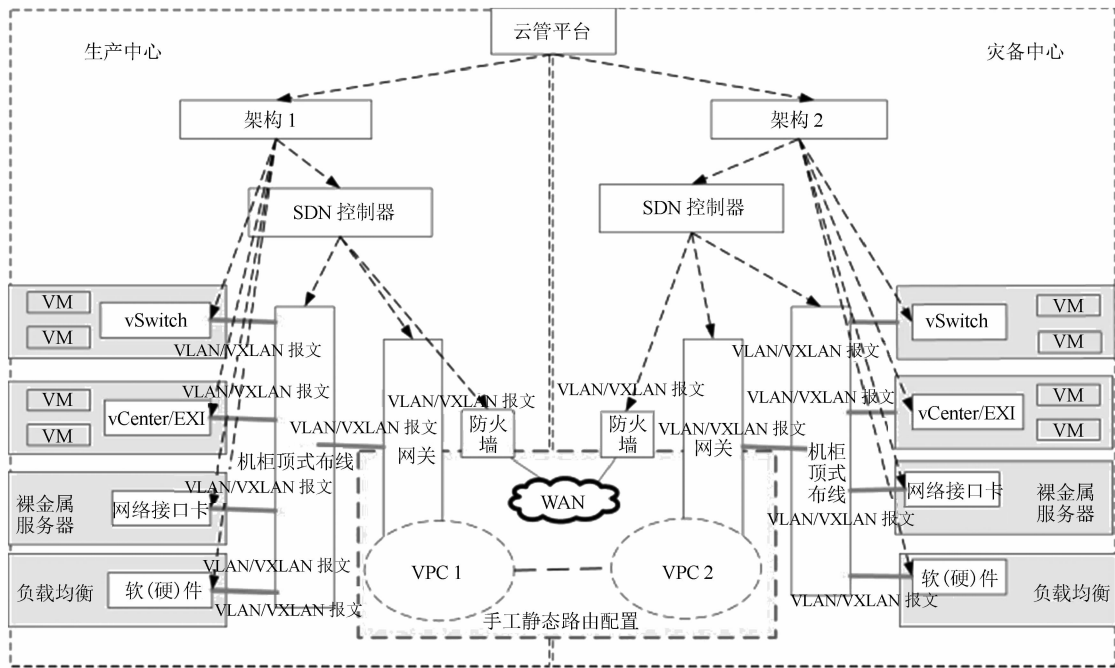
网络功能层重点实现网络功能软件化,通过部署 SDN 控制器来实现控制与转发分离功能及网元设备的软硬件解耦,进而实现网络自动化部署。在资源池中部署虚拟负载均衡器及虚拟防火墙,以统一云资源池的承载能力,提高云平台与业务系统之间的安全隔离。

云网以云平台为基础,统筹考虑业务平台、大数据平台及网元虚拟化,按统一管理、统一调度、资源共享的原则,构建统一的云网基础设施,实现云网资源池的统一管理。

云网重构后,全网资源池统一纳管编排、集中运维监控、分权分域使用。在端侧,可实现端到端的快速部署,实现不分专业、不分云上与云下的网络资源集中管理、按需分配。云网对网络资源池的统一呈现、统一管理及统一维护,实现了资源跨部门的统一调度和分配自动化、弹性化,具备了资源动态伸缩能力。重构的云网从分散式转为集约式,管道从硬件转为软件,实现了云、管、端一体化运营^[7]。

4 结语

城轨云云网一体化架构引入软件定义网络技术,以软件对网络资源进行虚拟化和抽象化,以软件定义实现自动化网络服务,可有效支撑城轨云数据中心上层业务的需要,提高业务上线和运维效



注：vCenter/EXI 为虚拟数据中心虚拟机监控系统。

图 4 生产中心及灾备中心云网一体化部署方案

Fig. 4 Integrated cloud network deployment scheme for production center and disaster recovery center

率,适应网络设备资源池化和标准化的发展趋势。本文对 SDN 架构的各接口及相关技术进行研究,从而明确了云网重构的一体化部署思路。

参考文献

[1] 钟翠,王蕾,罗兴. 云数据中心的 SDN 解决方案[J]. 电信科学,2018(7):15.
ZHONG Cui,WANG Lei,LUO Xing. SDN solutions for cloud data center[J]. Telecommunications Science,2018(7):15.

[2] 王刚. 基于 SDN 的云数据中心虚拟机迁移策略研究[D]. 北京:北京邮电大学,2017.
WANG Gang. Virtual machine migration strategy research in cloud data center based on SDN[D]. Beijing:Beijing University of Posts and Telecommunications,2017.

[3] 李振宇. SDN/OSPF 混合网络中流量工程机制的研究[D]. 沈阳:东北大学,2015.
LI Zhenyu. Research on traffic engineering in SDN/OSPF hybrid network[D]. Shenyang:Northeastern University,2015.

[4] 卞姗姗. 软件定义网络中应用程序的信任管理架构[D]. 西安:西安电子科技大学,2017.
BIAN Shanshan. A trust management framework of SDN appli-

cations[D]. Xi'an:Xidian University,2017.

[5] 鞠卫国,张云帆,桥爱锋,等. SDN/NFV 重构网络架构 建设未来网络[M]. 北京:人民邮电出版社,2017.
JU Weiguo,ZHANG Yunfan,QIAO Aifeng,et al. SDN/NFV: Reconstruct network architecture to build future network[M]. Beijing:People's Posts and Telecommunications Press,2017.

[6] 卞宇翔,沈苏彬,吴振宇. 一种面向多管理域 SDN 控制器故障处理方案[J]. 计算机技术与发展,2017(12):108.
BIAN Yuxiang,SHEN Subin,WU Zhenyu. A solution for controller failure treatment of SDN in multiple-management domains[J]. Computer Technology and Development,2017(12):108.

[7] 何晶颖. 云网融合的演进路径探讨[J]. 电信快报,2018(4):12.
HE Jingying. Research on the evolving path of cloud network integration[J]. Telecommunications Information,2018(4):12.

[8] 华为技术有限公司. 硬件 SDN 技术白皮书[CD]. 深圳:华为技术有限公司,2018.
Huawei Technologies Co., Ltd. Hardware SDN technology white paper[CD]. Shenzhen:Huawei Technologies Co., Ltd., 2018.

(收稿日期:2020-04-21)