运营技术广角

# 云数据中心 SDN/NFV 组网方案、测试及问题分析

顾戎[1]，王瑞雪[2]，李晨[1]，黄璐[1]

（1.中国移动通信有限公司研究院网络技术研究所，北京 100053；
2. 北京邮电大学网络技术研究院，北京 100876）

**摘　要**：云计算技术的快速发展和广泛应用使得数据中心的业务形态产生了翻天覆地的变化，SDN 和 NFV 两大技术联合应用在数据中心优势显著，真正实现了网络资源的虚拟化。经过有针对性的 SDN/NFV 规模组网评测，可以看到 SDN/NFV 已经具备在云数据中心网络的部署条件。同时，在方案制定和测试验证过程中也发现了一些关键问题需要未来进一步研究和探讨。

**关键词**：SDN；NFV；云数据中心；方案测试

**中图分类号**：TP393　　**文献标识码**：A

**doi:** 10.11959/j.issn.1000-0801.2016020

# Analysis on network scheme and resolution test of SDN/NFV technology co-deployed in cloud datacenter

GU Rong[1], WANG Ruixue[2], LI Chen[1], HUANG Lu[1]

1. Department of Network Technology, China Mobile Research Institute, Beijing 100053, China
2. Department of Network Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China

**Abstract:** Traditional datacenters have been heavily impacted due to the development and large-scale deployment of cloud computing technology. Co-deployment of SDN and NFV technology shows its distinct advantages of vitualizing network resources in the scenario of cloud datacenter. Resolution tests aiming at co-deployment of SDN and NFV have directive significance. According to the resolution test, SDN and NFV technology were matured already for the commercial deployment in operators' network. Further research needs to be focused on the key problems found out in scheme designing and the resolution test.

**Key words:** SDN, NFV, cloud datacenter, resolution test

## 1　引言

### 1.1　SDN 和 NFV 技术相互补充相互结合

SDN（software defined networking）是一种软件集中控制、网络开放的网络体系架构，核心思想在于控制与转发相分离、集中化控制、通过标准接口开放网络能力。其最大价值在于提升网络虚拟化能力、加速网络创新，提高全网资源使用效率。NFV（network function virtualization）是采用虚拟化技术，将传统电信设备与硬件解耦，基于通用的计算、存储、网络设备实现电信网络功能，从而提升设备的建设、管理和维护效率。

网络由网元功能及其之间的网络连接共同组成，SDN 和 NFV 就是网络连接与网元功能的关系。SDN 提供网络连接，NFV 提供网元功能，二者相互独立又相互补

收稿日期：2015-06-23；修回日期：2015-12-07

充,如图 1 所示。其中,独立性表现为 SDN 可以基于传统硬件方式实现网络功能,也可以采用 NFV 方式提供网络功能。两者相互补充会发挥更大的效应:一方面,SDN 技术将网络的转发功能和控制功能分离,功能的拆分有利于网元的 NFV 化;另一方面,NFV 可基于 x86 通用硬件为 SDN 的控制和转发网元提供虚拟资源,使得 SDN 的资源调度更加灵活。

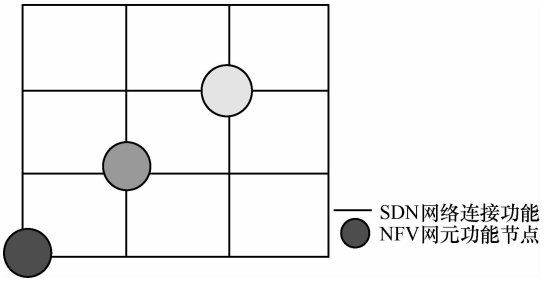



图 1 SDN 和 NFV 的关系

### 1.2 云数据中心引入 SDN/NFV 技术的必要性

传统网络虚拟化能力不足,使得云数据中心虚拟私有云(virtual private cloud, VPC)业务和业务链(service chain)服务受到挑战。灵活性、扩展性和易用性成为未来网络的基本特征。在此背景下,SDN 和 NFV 技术的出现使其迅速成为产业关注的热点。

将集中控制、能力开放的 SDN 架构应用于云数据中心,可提升网络服务的虚拟化能力,提高全网资源调度的高效性,满足虚拟机在数据中心内灵活创建、迁移、隔离等业务需求。同时为了解决防火墙、负载均衡器、广域网 VPN 网关等传统硬件设备虚拟化能力有限的问题,云数据中心在 SDN 架构的基础上引入 NFV 形式的软件产品,采用业务链的解决方案为每个租户单独提供可定制的服务,并集中进行流量的调度。通过 SDN 和 NFV 技术联合,可以将物理网络抽象成虚拟的逻辑网络模型,基于 SDN 架构、OpenStack 标准接口和流表设计实现 VPC 和业务链服务,并通过加速技术实现 NFV 网元的高效工作。

## 2 云数据中心 SDN/NFV 技术引入方案

### 2.1 云数据中心 SDN/NFV 组网架构

云数据中心 SDN 解决方案具有多级架构,包括应用层、协同层/虚拟化平台、控制器和转发层。多级架构有助于实现网络的灵活调度,提供真正的网络即服务。

SDN 调度平台或者第三方平台作为应用层,为用户提供网络资源的自配置界面以及虚拟网络拓扑配置界面,用户可针对虚拟链路/网元进行访问控制策略的配置,并向用户实时呈现当前网络的运行情况。

协同层包含计算、存储、网络、鉴权等多个模块,用于调度数据中心内的计算、存储和网络资源。

控制层为逻辑集中的控制实体(物理上可集中式资源实现或者分布式资源实现),将应用层业务请求转化为转发层的流表并配置到转发层的相应网元中,并接收转发层的状态、统计和告警等信息。

转发层由具有分组转发功能的物理设备(物理网元)或虚拟交换设备(虚拟网元)组成,根据 SDN 控制器通过控制—转发接口配置的转发表完成数据转发。虚拟转发层是云计算数据中心组网中必不可少的一个层次,用来满足云计算环境下的虚拟机流量交换需求并提供灵活的流量调度。从转发层的不同网元选择以及采用的流量封装方式来看,可分为 overlay 和 overlay + underlay 组网方案。

overlay 组网方案的核心在于仅通过 SDN 控制虚拟交换机,虚拟交换机作为 VxLAN 的接入点,虚拟交换机之间通过 VxLAN tunnel 建立重叠网络,基于 SDN 的流量控制和业务编排完全在虚拟交换机层面完成。底层的物理网络通过网管或命令行方式基于传统网络技术提供服务器(虚拟交换机)之间的二层或三层连通,基于虚拟交换机增加的 VxLAN 封装的 MAC 地址或 IP 地址信息进行转发,对于虚拟机之间的流量并不直接感知。

overlay+underlay 组网方案是通过 SDN 同时控制物理和虚拟交换机,全面控制网络资源。虚拟交换机仍然作为 VxLAN 的接入点,虚拟交换机之间通过 VxLAN tunnel 建立重叠网络,基于 SDN 的流量控制和业务编排结合虚拟交换机和物理交换机共同完成。此时物理网络只需要基于虚拟交换机增加的 VxLAN 封装的报头信息进行转发,物理交换机的转发流量容量需求大大减少。由于物理交换机也在 SDN 的控制之下,VxLAN 网关可以由核心交换机来兼做,一方面能够优化流量转发的路径,另一方面基于硬件设备的 VxLAN 网关具有更好的转发性能。另外,该方案可以同时适用于纯虚拟机业务环境和虚拟机物理服务器共存的业务场景。

两种组网方案针对不同的场景需求。建议在以虚拟机为主的业务场景采用 overlay 方案;在同时需要虚拟机和物理服务器的业务场景采用 overlay+underlay 方案,另外,根据设备支持情况和性能需求选择虚拟交换机或硬件交换机作为 VxLAN 接入点。

云数据中心 SDN/NFV 组网架构中,NFV 网元以资源池的形式存在,通过 SDN 业务链调度实现 NFV(包括虚拟防火墙、虚拟负载均衡等)的能力。

### 2.2 云数据中心 SDN NFV 方案评测

为了在云数据中心引入 SDN 和 NFV 技术,提供虚拟私有云(virtual private cloud,VPC)和业务功能链(service function chaining,SFC)等先进网络服务,本文对云数据中心 SDN/NFV 方案进行了规模组网评测,如图 2 所示。本次评测基于开源 OpenStack 平台,采用 KVM 虚拟化操作系统,对 SDN 重叠网解决方案进行验证。

本次评测针对 SDN 云数据中心系统、控制器、转发设备(含 SDN、NFV)的功能和性能进行全面测试,测试围绕 OpenStack 系统测试、SDN 控制设备测试、SDN 转发设备测试、NFV 网元(包括负载均衡器、防火墙以及 IPSec VPN)测试以及通用安全性测试共 5 个部分展开。

(1)OpenStack 系统测试

OpenStack 系统测试属于 SDN 多层架构中协同层/虚拟化平台测试,具体包括 OpenStack 平台实现虚拟路由器、网络、安全组功能测试,浮动 IP 地址、NAT 功能测试,LB/FW/VPN 业务自动开通功能测试以及容量并发、压力可靠性测试。结合数据中心的实际业务,对 OpenStack 云平台提出要求。

通过 OpenStack 云平台自服务对虚拟路由、网络、子网、端口、安全组进行创建、删除、修改、查看等相关操作,SDN 控制器从云平台获取网络信息并下发配置到转发设备,从而对租户自定义网络、创建虚拟机、创建基于安全组的子网访问策略等功能进行验证。

通过浮动 IP 地址、NAT 功能测试,验证 SDN 和传统网络的互通,任意虚拟机访问外网能力以及转发设备是否支持公网 IP 地址和私网 IP 地址 1:1 静态绑定和 *N*:1 NAT 两种方式。两种方式下针对 IP 地址的带宽限速功能也进行同步验证。

通过 OpenStack 云平台自服务方式对虚拟防火墙/虚拟负载均衡器进行创建/删除/修改/查看等相关操作,对 IPSec VPN 服务执行开通操作,验证 NFV 网元自动或者手动开通功能。

通过容量并发、可靠性脚本压力测试验证通过云平台可以创建的最大的网络(子网)、虚拟路由器、安全组、虚拟机数量以及 SDN 系统对并发创建的处理能力。

(2)SDN 控制设备测试

SDN 控制设备测试对控制器性能,包括控制器流表下发速度、建立时间、支持流表总容量以及支持交换机规模上限进行性能测试;在控制设备可靠性方面,对控制器主备负载分担能力以及发生故障时主备倒换能力和倒换时间提出要求;进一步验证 SDN 控制设备的可商用性。

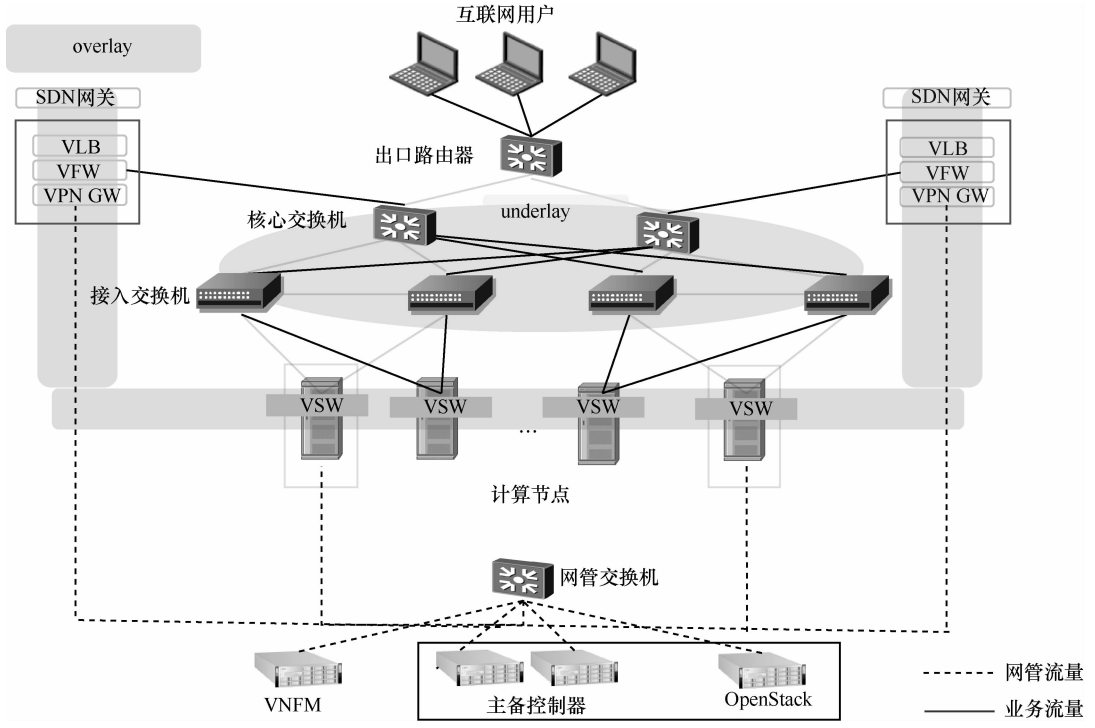



图 2 云数据中心 SDN/NFV 方案评测示意

(3)SDN 转发设备测试

SDN 转发设备由物理网元或者是虚拟交换设备实现分组转发功能,SDN 转发设备测试内容包括转发设备的功能、可靠性、稳定性测试以及转发设备性能测试。

(4)NFV 网元测试

NFV 网元测试针对 NFV 网元,包括负载均衡、防火墙以及 VPN 的功能和性能进行验证。通过测试,对 LB/FW/VPN 的功能以及在一定性能要求下单服务器上能承载的最大虚拟网元数目进行验证。

负载均衡的功能及性能测试验证负载均衡服务是否支持健康检查、负载均衡算法、SSL 功能、会话保持及多 VIP 访问;可靠性方面验证是否支持双机热备份。与此同时,在统一配置服务器承载的一定性能要求的负载均衡器最大数目也得到了测试,具有实际部署指导价值。

防火墙功能及性能测试针对基于五元组、时间段的安全策略以及是否支持安全策略顺序、双机热备份可靠性展开,在统一配置服务器承载的一定性能要求的防火墙最大数目也得到了验证。

通过 IPSec VPN 功能和性能测试验证 IPSec VPN 的功能和性能,并同步测试了统一配置服务器承载软件 IPSec 网关的最大数量。

(5)安全通用测试

SDN 技术相比传统网络带来了安全上的变化,引入了控制器安全、流表安全等新安全问题。而传统的安全问题,比如针对服务器的 DoS 攻击、弱口令等在 SDN 中仍然存在,而且攻击后果会更严重,所以安全通用测试一并纳入 SDN/NFV 方案评测。安全通用测试对 SDN/NFV 方案中控制器、NFV 网元进行安全测试,包括账号安全、授权安全、IP 安全、口令功能、日志功能、安全监控等安全测试。

## 3 云数据中心 SDN/NFV 方案及测试的关键问题

通过方案评测,发现云数据中心 SDN/NFV 方案对 OpenStack 接口支持能力普遍较好,商用控制器和虚拟交换机性能基本可以满足需求,基于 SRIOV 等技术的 NFV 网元在功能和性能方面也达到商用要求,SDN/NFV 联合商用方案在运营商网络已具备商用部署条件。与此同时,本文发现云数据中心引入 SDN 和 NFV 技术还存在一些问题,如 OpenStack 及 NFV 的可靠性、测试方法的标准化、组网和部署方案经验缺乏、虚拟化平台支持度不够以及接口标准化工作缺乏等,需要在云数据中心后续方案的演进和实践过程中进行进一步的思考与讨论。

(1)OpenStack 可靠性需要完善

由于标准 OpenStack 不具备数据库高可靠性或者集群的能力,所以存在单点故障的问题,当前数据库的高可靠性需要安装第三方软件实现,自身多节点负载均衡或可靠保护还需要进一步研究。

(2)测试方法的标准化

由于当前 overlay 的解决方案不唯一,存在 VxLAN 以及 MPLSoGRE 两大主流封装技术,因此测试方案无法得到统一,横向对比比较困难。另外控制器与转发设备流表下发存在主动下发和被动触发两种模式,两种模式下控制器流表下发速度和建立时间也难以横向对比。

(3)组网和部署经验缺乏

SDN/NFV 技术目前还处于试商用初期,组网部署方案经验不足,多种部署方案无明确场景对比。如,NFV 网元的部署位置是旁挂在 underlay 核心交换机还是直接部署在虚拟交换机或网关之后需根据场景决策,NFV 网元的部署位置决定了其是否受到 VLAN 的限制。另外,NAT 存在集中式部署和分布式两种部署方式,各有千秋,目前对于两种部署方式应合理选择,并无明确的场景比较。

(4)SDN 对 Xen 和 VMware 虚拟化平台的支持需加强

通过评测发现,目前 SDN 解决方案主要支持 KVM 虚拟化平台,对 VMware 和 Xen 虚拟化平台支持效果较差。当前主流的云操作系统 OpenStack 基于开源 KVM 平台开发,开放程度高,并且大量公有云系统基于 OpenStack 提供服务,业界具有丰富的部署经验,因此对于 KVM 虚拟化平台支持度高。为了推动 SDN 和 NFV 技术的大规模商用部署,VMware 和 Xen 平台应进一步开放,这是提高 SDN 对这两大虚拟化平台支持度的基础。

(5)SDN 和 NFV 融合架构不明确,NFV 接口有待进一步标准化

SDN 架构按照 ONF 和 CCSA 等组织定义,分为应用层、协同层、控制层和转发层,概念清晰达成共识。NFV 按照 ETSI 定义关于 MANO、VNF、NFVI、OMC、OSS 的总体架构业界也达成共识。但是当 SDN 和 NFV 共同部署在云中心,为用户提供 VPC 和业务链服务时,NFVI 资源如何整合,SDN 应用和 NFV orchestrator 如何分工就成为了两个架构融合的关键。目前架构和接口尚未达成一致,需要标准组织推动研究。

(6)OpenStack 支持的北向接口不足,应在标准和开源社区推动两方面努力

目前 OpenStack 在网络方面的北向接口支持不足,如:OpenStack 无法监管物理服务器, 对 SDN 和传统网络融合组网存在一定的管理问题;OpenStack Neutron 等模块北向接口不完善, 无法满足所有的业务需求;FWaaS 的 plugin 只支持单厂商,无法实现多厂商集成;针对数据中心业务链服务相关的 API 如流量重定向、业务安排等还在研发中。近期可采用 App 扩展 RESTful API 弥补 OpenStack 北向接口的不足,并积极推动 CCSA TC1 等组织完善北向接口以及业务链的标准化; 远期应推动 OpenStack 社区完善和扩展,统一北向接口。

## 4 云数据中心 SDN/NFV 技术展望

针对云计算数据中心的 SDN/NFV 组网方案研究和评测对推动 SDN/NFV 技术的商用具有重要意义, 加速了 SDN 和 NFV 产业链成熟。通过评测, 本文发现 SDN 与 NFV 两大技术结合具有天然的优势,业界对未来网络演进的思路和见解也逐步明晰。SDN/NFV 联合组网方案具备良好的互操作性,NFV 形态的负载均衡器、防火墙、VPN 产品在功能、性能、可靠性方面已具备在运营商网络中商用部署条件。

同时, 云数据中心 SDN/NFV 技术评测的结果也反映出 SDN/NFV 技术面临着一些挑战,其中 SDN 和 NFV 融合架构模糊、标准化工作缺乏以及软件可靠性等方面的关键问题对 SDN/NFV 的发展和应用十分重要, 需要进一步的研究和探讨。

SDN/NFV 技术的引入带给业界的改变远超过技术本身,产业格局、网络架构、运维模式的改变将随着技术的逐步落地而带来新的挑战,需要进行不断的探索和实践。

## 参考文献:

[1] NADEAU T D, GRAY K. SDN: Software Defined Networks[M]. New York: O'Reilly, 2013.

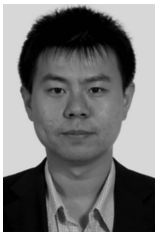
[2] 李晨, 段晓东, 陈炜, 等. SDN 和 NFV 的思考与实践[J]. 电信科学, 2014, 30(8): 23-27.
LI C, DUAN X D, CHEN W, et al. Thoughts and practices about SDN and NFV[J]. Telecommunications Science, 2014, 30(8):23-27.

[3] 李晨, 段晓东, 黄璐, 等. 基于 SDN 和 NFV 的云数据中心网络服务[J]. 电信网技术, 2014 (6).
LI C, DUAN X D, HUANG L, et al. Network service of cloud data center service based on SDN and NFV [J]. Telecommunications Network Technology, 2014(6).

[作者简介]

**顾戎**(1988–),女,中国移动通信有限公司研究院网络技术研究所项目经理,主要研究方向为数据中心组网、SDN、NFV。

**王瑞雪** (1990–), 女, 北京邮电大学硕士生, 主要从事数据中心组网、SDN 和 NFV 技术学习以及相关测试工作。



**李晨**(1985–),男,中国移动通信有限公司研究院网络技术研究所项目经理, 主要从事 IP网络、数据中心组网以及 SDN 和 NFV 方面的研究,负责 IP 骨干网、数据中心网组网方案设计及相关标准和技术的跟踪、研究和标准制订; 已主持完成 1 项中国通信行业标准、1 项中国标准化协会研究课题;已发表 6 篇论文。

**黄璐**(1978–),男,中国移动通信研究院技术经理,主要研究方向为中国移动 IP 网络技术及网络方案设计。