

# 基于SDN的大型企业网络研究

郭文刚

(中国电子科技集团公司电子科学研究院, 北京 100041)

**摘要:**文中讨论将软件定义网络(SDN)应用到大型企业网络,通过智能软件将通信网络资源进行抽象,使得大型企业网络更加人性化、软件化和智能化,为满足大型企业数据通信尤其是大型企业开展设计和试验对网络动态重组的需求,提供安全、可控和灵活的资源调度能力。文中针对传统网络对大型企业开展新技术体制试验存在的问题,将通信网络、安全和管理进行整合,实现网络自动部署、安全高效整合、运维快速故障定位与排除,为提高企业运维管理人员效率、降低成本提供一种手段和方法。

**关键词:**软件定义网络;大型企业;虚拟化;网络;研究

中图分类号:TP31

文献标识码:A

文章编号:1673-629X(2014)08-0179-04

doi:10.3969/j.issn.1673-629X.2014.08.042

## Research on Large Enterprise Network Based on SDN

GUO Wen-gang

(China Academy of Electronics and Information Technology of China Electronic Science & Technology Group Inc., Beijing 100041, China)

**Abstract:** In this paper, discuss the Software Defined Network (SDN) to be applied to large enterprise networks, through the intelligent software abstract the communication cyber source, so that large enterprise network is more humanized, software-based and intelligent, in order to satisfy the data communication of large enterprises, especially the network requirements of the dynamic reorganization for large enterprises to carry out the design and test, provide a safe, controllable and flexible resource scheduling. Aiming at the problem of traditional network for large enterprises to develop new technology, the communication network, security and management integration are integrated to achieve automatic network deployment, safe and efficient integration, rapid fault location and maintenance, provide a kind of means and methods to improve the efficiency of operation management personnel of the enterprise and reduce the costs.

**Key words:** SDN; large enterprise; virtualization; network; research

## 0 引言

随着信息技术的发展及通信网络的成熟,通信网络在大型企业中的作用越来越重要,已不是主要以数据通信为目的,而是朝着满足企业能力提升为目标,为开展协同设计和协同试验提供技术支撑,为提升企业核心竞争力提供基本保障。

计算机网络技术的爆炸式增长,发展速度和规模增大、业务快速创新这令大型企业网络承担着更大的压力,各种实时业务如语音、云计算中心等快速发展,甚至企业为了测试产品,在企业网中开展产品的协同设计和协同试验,这些都无疑对网络提出了更高的要求。

## 1 传统网络存在的问题

目前大型企业网络信息化主要包括网络、安全、数据中心、备份中心和运维管理中心等几个部分,通过传统路由器、交换机、服务器和终端构成,主要采用IPv4通信协议,实现了企业内部的信息交互,但在开展企业内部协同设计和协同试验过程中还存在一些问题,主要表现在以下几个方面。

### 1.1 通信网络部署问题

目前企业网络链路大部分租用电信SDH线路,静态路由,拓扑不可变,缺乏动态的资源接纳控制及机动控制能力。新业务应用可能基于NGN的技术体制,实现多业务、宽带化、分组化、开放性、移动性、兼容性、安全性、可管理的网络需求,采用分组技术的综合开放的

网络架构<sup>[1]</sup>。

由于业务和网络分离,大型企业网络的配置是通过命令行等方法进行人工配置的,其本身是个静态网络,固定之后不能经常按照用户需求改变,当需要在企业网上开展系统试验时,会经常需要网络及时做出调整,就显得非常低效,也有可能无法实现。

### 1.2 安全管理问题

随着企业应用的深入与变化,对企业网络的安全要求越来越高。现有的安全保密措施已逐渐落后,安全管理流程复杂、处理性能不足,难以实现资源的安全、灵活、有效分配,无法满足企业对资源可信、可控、可管的要求,以及在大容量、高带宽、多业务的协同设计和协同试验的安全保障需求<sup>[2]</sup>。

其主要问题如下:

1) 支持安全接入的方式不灵活,不能实现动态资源的动态分配和调整。

2) 远程传输加密开销过大,远程传输采用双层加密措施,存在效率低下、故障不易定位等问题,无法满足新业务应用的多应用、多协议、高带宽、多种接入方式的要求。

3) 安全防护的灵活性不足,与企业网络配合的安全管理审批流程复杂、灵活性不足,不能满足协同试验验证的接入、退出、变更的灵活性的要求。

4) 安全防护的整体调度能力不足,无法实现各种安全资源的统一配置、动态调整和精确管控。

### 1.3 运维管理效率低

面对大型企业大量不同年代、不同厂家、不同设备的采购、设计、集成、部署、维护运行、升级改造,其运行维护成本高、效率低。

大型企业网络主要包括基础网络系统、安全保密系统、数据中心、灾备中心及运维管理中心几个组成部分,这些由大量的路由器、交换机、服务器等构成,对于故障定位是一件非常困难的事情,且很多故障或错误是由人的误操作导致的,因此需要大型企业网络能够具有智能管理手段。

尤其是网络管理被普遍认为是当前所面临的最严峻的挑战之一,网络管理的根源都是相同的,即需要维持路由器和交换机等的物理和逻辑配置的一致性<sup>[3]</sup>。

### 1.4 资源利用率低

大型企业很多情况下由传统网络、安全保密系统、数据中心、灾备中心及运维管理系统等几部分构成,但目前传统网络无法支持云的定制网络实时生效,难以形成多层网络的协同沟通,难以根据业务需求自动调整网络带宽,以致网络资源利用率比较低,难以满足大型产品的协同设计及大型系统的协同测试试验验证等任务的需求<sup>[4]</sup>。

## 2 SDN 概述

### 2.1 SDN 定义

软件定义网络(SDN)是一种革命性的网络技术<sup>[5]</sup>,对现有网络结构进行了创新,已逐渐成为通信领域最热门的技术之一,已成为通信技术领域的关键词之一,是未来网络的核心技术之一。通过将网络控制和数据转发分离,从而实现网络和业务可编程控制。通过 SDN,企业将获得前所未有的可编程、自动化和网络控制,促使企业高效升级和灵活适应企业需求。

### 2.2 SDN 架构

2011 年,Google、德国电信等公司发起并成立了 Open Networking Foundation-ONF(开放网络基金会),主要致力于推进基于 OpenFlow 的 SDN 网络<sup>[6]</sup>。ONF 为 SDN 网络定义了三个逻辑层,分别为基础设施层、控制层和应用层,技术架构如图 1 所示。

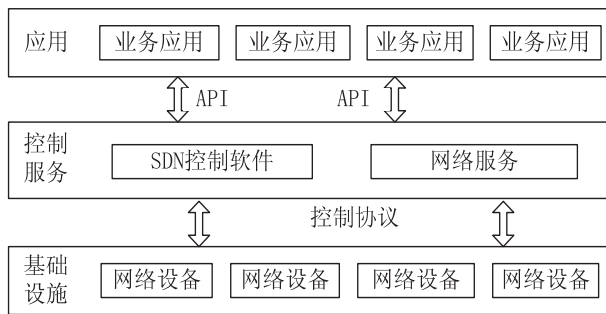


图 1 SDN 体系架构图

基础设施层起到数据处理、转发和状态收集的作用,包括构件基础设施的路由器、交换机、服务器和计算机终端等。

控制层起到支撑和数据编排的作用,包括网络操作系统、SDN 控件和网络服务等支撑内容。

应用层包括各种业务应用,即核心业务。

在软件定义中,基础设施的设备仅仅负责数据转发,因此可以用通用构件网络设施,由原来嵌入在专用网络设备的操作系统提炼为控制服务层的网络操作系统,负责与各种业务的接口适配,其硬件设备之间的通信以及操作系统和业务之间的信息传输都可以通过编程实现。

### 2.3 OpenFlow 网络

2008 年, Nicira 公司提出了 OpenFlow 的概念, OpenFlow 是 SDN 的核心技术,是网络设备层的规范,起到基础设施层和控制层之间的协调作用。OpenFlow 是一个技术协议,通过它可以实现软件定义网络,用户可以在不用清楚基础设施是什么的情况下控制数据流量从一个设备传送到另一个设备上,最终传送到最终用户。

OpenFlow 是 SDN 的重要组成部分,它能够使控制网络设施程序化,支持快速的网络服务开发和部署。

它使设备制造商在不暴露其网络设备内部实现细节的前提下,提供网络研究者修改网络控制逻辑进行各种创新试验的能力。

OpenFlow 网络是使用了 OpenFlow 技术的网络,它由 OpenFlow 交换机、FlowVisor 和 Controller 三个部分组成,而 OpenFlow 交换机则由流表、安全通道和 OpenFlow 协议三个部分构成。OpenFlow 交换机负责数据的转发,其流表由头域、计数器和操作几个部分构成;FlowVisor 负责进行网络虚拟化;Controller 则负责对网络进行集中控制,实现控制层的功能,通过 OpenFlow 协议对流表进行控制。OpenFlow v1.0 仅支持 IPv4,v1.2 也可支持 IPv6<sup>[7]</sup>。

在大型企业添加 OpenFlow 特征的固定或移动节点,将使企业的固定网和移动网络实现无缝控制,使得管理更加灵活。

2.4 SDN 特征

SDN 最主要的特征就是数据转发和控制分离,同时还具有资源虚拟化和软硬件可编程等特征。

数据转发和控制分离特征思想是基础硬件与业务实现分离,其硬件仅负责数据转发和存储,因此可以采用相对廉价的通用设备构建网络基础设施<sup>[8]</sup>。

资源虚拟化的思想是对网络设备的种类、功能及智能化管控通过软件实现,由网络操作系统完成对网络的运行控制。

软硬件可编程思想是通过定制诸如路由、安全等各种网络参数实现更快的业务响应。

2.5 SDN 优势

可以根据业务对网络的需求编制网络特性和能力的方案,简化对网络设备的配置要求,将网络部署时间缩短,对运维管理人员的知识要求比较低<sup>[9]</sup>。

3 基于 SDN 的大型企业网建设方案

3.1 基础架构

云计算、大数据等新技术已经应用到大型企业网中,尤其是云计算已经应用到大型企业的数据中心,而云计算的特点就是需要将资源进行集中处理,然后进行分配和调度。网络资源和计算资源由不同设备构成,因此需要有更有效的资源整合能力。将 SDN 新思想应用到大型企业网络中,用以提高资源的整合能力,提升新业务支持能力,并有效提高运维管理人员的工作效率。

遵循 SDN 架构,大型企业网络由基础设施层、控制层和应用层构成,见图 2。基础设施层由路由器、交换机、服务器和计算机终端构成<sup>[10]</sup>。应用层主要由办公业务应用、产品设计应用及系统试验应用等企业核心应用构成,是企业提升能力的主体力量。

3.2 通信网络

企业采用 SDN 建设网络,企业业务应用响应将更快,并且可以定制各种网络参数,如路由参数、安全配置、应用策略等,并使配置实时起效,缩短开通具体业务的时间,提高网络配置效率。

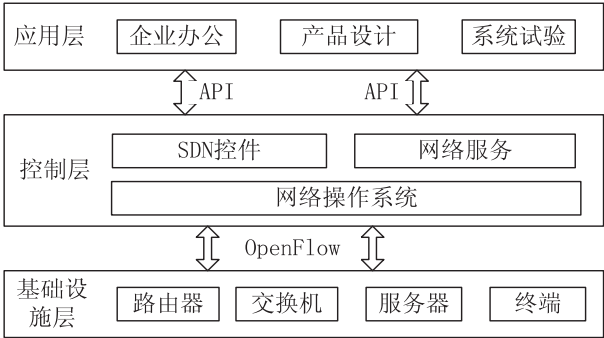


图 2 大型企业 SDN 结构

企业网络所用交换机需要支持 OpenFlow 协议的 OpenFlow 交换机,OpenFlow 交换机包括执行包查询和转发的流表、连接控制器的安全通道。控制器通过安全通道利用 OpenFlow 协议管理控制 OpenFlow 交换机。流表由流表头、计数和活动组成。所有被交换机处理的包都需要和流表进行比对,如果发现比对成功的包,在数据包的任何活动将被执行;如果没有比对成功,数据包通过安全通道转发到控制器,控制器负责处理该数据包,并控制交换机流表增加或删除该数据包<sup>[11]</sup>。

OpenFlow 交换机与控制器的关系如图 3 所示。

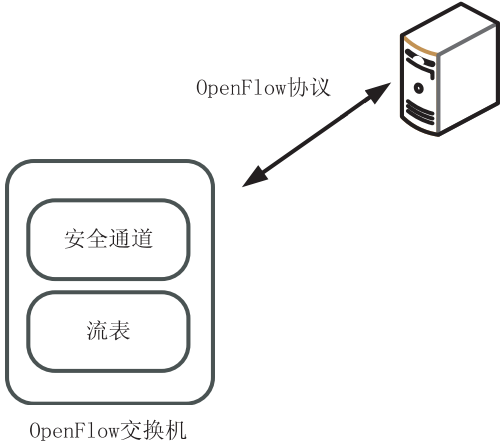


图 3 OpenFlow 交换机与控制器的关系

通过在大型企业中建设虚拟化网络,可以生成灵活的网络拓扑、运行真实的路由协议、注入可控的网络事件、承载实际的网络流量、支持多试验的运行等。通过网络虚拟化,可以解决网络管理员对网络配置的问题,如升级有问题的设备、部署新应用或者增加新的网络设备,对这些操作将导致系统的停止,通过虚拟化有助于进行负载均衡和流量工程等<sup>[12]</sup>。

SDN 将大型企业网络的控制从网络硬件中脱离



出来,交给虚拟的网络层处理。这个虚拟的网络层加载在物理网络之上,在一个虚拟的空间重建整个网络。有了网络虚拟化,物理网络被泛化成网络能力池,正如服务器虚拟化把服务器转化为计算能力池。通过这一方案,可以解决大规模云数据中心在承载多租户服务时面临的 VLAN 数量限制、机房扩容时的网络调整复杂等技术难题,是网络智能化承载具体业务的一个体现<sup>[13]</sup>。

FlowVisor 对 OpenFlow 网络进行了分片,实现对网络的虚拟化,利用 FlowVisor,运行 OpenFlow 协议的交换网络可被划分成几个网络。FlowVisor 置于 OpenFlow 交换机和控制器之间,作为它们之间的透明代理。OpenFlow 交换机和控制器不关心 FlowVisor 是否存在。FlowVisor 示意图如图 4 所示。

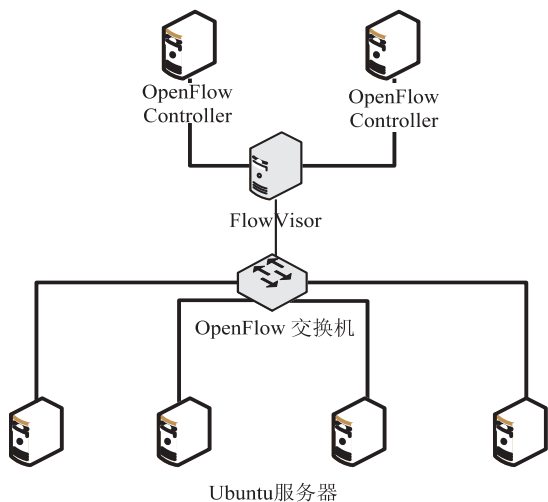


图 4 FlowVisor 示意图

### 3.3 安全

随着 SDN 技术将数据平面与控制平面分类,传统的在网络上增加防火墙、加密机、IPS 的安全管理方式已经不适合于 SDN 网络了。面对网络安全的威胁,如何进行防范依然是人们关注的一个话题。需要利用 SDN 及 OpenFlow 的开放性接口研究其安全策略。

可以借鉴传统安全模式,在 SDN 的体系架构中的基础设施层、控制层和应用层部署安全策略。

### 3.4 SDN 数据中心

随着云技术的应用,云计算中心已经成为数据中心的核心理,因此如何对数据中心的资源进行高效管理就成为企业关注的问题。随着数据中心规模的扩大,数据中心网络、服务器资源的增加,导致了数据中心资源利用率低,且难以实现网络与虚拟机的高效协同,通过 SDN,可以很好地解决企业数据中心资源利用率低的问题,并且能够很好地实现网络与虚拟机之间的高效协同<sup>[14]</sup>。

## 4 结束语

SDN 是未来网络的核心技术之一,将 SDN 思想引入到大型企业网络中,可以解决制约企业发展的以下两个问题。


1) 企业分布式产品设计和试验验证对网络的动态需求问题。企业在完成产品及系统设计后,需要开展系统级的测试和试验验证,为验证产品对大型网络的适应性,会经常变更网络拓扑结构,且其数据流会根据需求发生巨变,需要有一种动态控制机制改变网络状态,SDN 思想是一个比较好的选择。

2) 提高运维管理效率。为适应企业产品设计和系统试验验证的需求,传统的运维管理已经无法满足企业试验验证的需求,SDN 对网络的运维明显减少了运维管理人员的工作量,提高了其工作效率。

### 参考文献:

- [1] 吴强,徐鑫,刘国燕.基于 SDN 技术的数据中心基础网络构建[J].电信科学,2013,29(1):130-133.
- [2] 赵慧玲,冯明,史凡.SDN-未来网络演进的重要趋势[J].电信科学,2012,28(11):1-5.
- [3] 郭春梅,张如辉,毕学尧.SDN 网络技术及其安全性研究[C]//第 27 次全国计算机安全学术交流会.出版地不详:出版者不详,2012:112-114.
- [4] 吕高峰,孙志刚,李韬,等.LabelCast:一种普适的 SDN 转发平面抽象[J].计算机学报,2012,35(10):2037-2047.
- [5] 王丽君,刘永强,张健.基于 OpenFlow 的未来互联网试验技术研究[J].电信网技术,2011(6):1-4.
- [6] 李英壮,孙梦,李先毅,等.基于 OpenFlow 技术的 QoS 管理系统的设计与实现[J].广西大学学报:自然科学版,2011,36(Sup):42-46.
- [7] 蒙克.OpenFlow 挖掘网络绿色潜力[N].网络世界,2008-11-03(3).
- [8] 赵联祥.SDN 架构下的 Open Flow 原理探讨[J].电信技术,2013(2):69-72.
- [9] 韩勛.理想照进现实-OpenFlow 技术及应用模式发展分析[N].计算机世界,2011-05-16(42).
- [10] 林闯,雷蕾.下一代互联网体系结构研究[J].计算机学报,2007,30(5):693-711.
- [11] 杨冬,李世勇,王博,等.支持普适服务的新一代网络传输层架构[J].计算机学报,2009,32(3):359-370.
- [12] 王淑玲,李济汉,张云勇,等.SDN 架构及安全性研究[J].电信科学,2013,29(3):117-122.
- [13] 徐恪,吴鲲,王青青.可扩展路由器控制平面的高性能通信模型[J].软件学报,2007,18(9):2205-2215.
- [14] 林闯,王元卓,任丰原.新一代网络 QoS 研究[J].计算机学报,2008,31(9):1525-1535.

# 基于SDN的大型企业网络研究

作者: 郭文刚, [GUO Wen-gang](#)  
作者单位: [中国电子科技集团公司电子科学研究院, 北京, 100041](#)  
刊名: [计算机技术与发展](#)   
英文刊名: [Computer Technology and Development](#)  
年, 卷(期): 2014(8)

本文链接: [http://d.wanfangdata.com.cn/Periodical\\_wjfz201408042.aspx](http://d.wanfangdata.com.cn/Periodical_wjfz201408042.aspx)