

应用型本科 电子及通信工程专业“十三五”规划教材

SDN 技术及应用

主 编 谭振建 毛其林
参 编 吴海涛

- 内容新颖：新知识、新技术、新工艺
- 特色鲜明：突出“应用、实践、创新”
- 定位准确：面向工程技术型人才培养
- 质量上乘：应用型本科专家全力打造

应用型本科 电子及通信工程专业“十三五”规划教材

SDN 技术及应用

主 编 谭振建 毛其林
参 编 吴海涛

西安电子科技大学出版社

内 容 简 介

SDN 是当前网络领域研究的热点,是业界公认的未来网络发展方向,其技术不断创新,应用的领域也越来越广。

本书首先阐述了 SDN 的产生背景、体系架构和发展概况,其次对 SDN 的控制平面和以 OpenFlow 为代表的南向接口协议进行了重点分析,接着阐述了数据转发平面的交换机类型和特点以及 SDN 中的网络虚拟化技术,最后通过搭建模拟网络环境,给出了 SDN 在实际应用中的基础实践和应用开发实践过程。

本书从理论分析到实践开发都进行了详细的讲解,对相关专业高校学生、从事 SDN 技术研发的专业人员、网络运营服务从业人员以及对 SDN 技术感兴趣的读者,都具有一定的参考价值。

图书在版编目(CIP)数据

SDN 技术及应用/谭振建,毛其林主编. —西安:西安电子科技大学出版社,2017.9
应用型本科 电子及通信工程专业“十三五”规划教材
ISBN 978-7-5606-4672-5

I. ① S… II. ① 谭… ② 毛… III. ① 计算机网络—网络结构 IV. ① TP393.02

中国版本图书馆 CIP 数据核字(2017)第 214564 号

策 划 马乐惠

责任编辑 杜 萍 雷鸿俊

出版发行 西安电子科技大学出版社(西安市太白南路 2 号)

电 话 (029)88242885 88201467 邮 编 710071

网 址 www.xduph.com

电子邮箱 xdupfb001@163.com

经 销 新华书店

印刷单位 陕西天意印务有限责任公司

版 次 2017 年 9 月第 1 版 2017 年 9 月第 1 次印刷

开 本 787 毫米×1092 毫米 1/16 印张 14

字 数 325 千字

印 数 1~3000 册

定 价 28.00 元

ISBN 978-7-5606-4672-5/TP

XDUP 4964001-1

*** 如有印装问题可调换 ***

本社图书封面为激光防伪覆膜,谨防盗版。

序 言

随着互联网应用规模的持续扩大,网络流量呈现爆发式增长,网络结构变得越来越复杂,这种复杂的网络结构常常使得人们对它是“碰不得,动不得”,其复杂的规划和配置过程越来越难以适应网络的发展创新需求。另一方面,伴随计算机软件技术的发展,系统软件化的趋势越来越受到业界的重视,硬件逐渐变“薄”,软件逐渐变“厚”,硬件通用化、软件开放化已成为当前 IT 信息技术发展的重要趋势。在这样的背景下,传统的网络体系架构在可扩展性、安全性、移动性、开放性、可编程性、高效性以及绿色节能等方面日益难以适应当前时代网络应用发展的需要,由此人们提出了各种未来网络发展的方向。

近年来,软件定义网络(Software-Defined Networking, SDN)以其全新的网络架构、开放性以及可编程的特点吸引了越来越多的组织、企业、科研机构对它进行不断的思考、研究和实践。传统网络中对流量的控制和转发都依赖于网络设备实现,设备中集成了与业务特性紧耦合的操作系统和专用硬件,这些操作系统和专用硬件都由各个厂家自己开发和设计。而在 SDN 中,网络交换设备采用通用的硬件设计,通常只负责数据转发,原来负责控制设备的操作系统将提升为独立的网络操作系统,负责对不同业务特性进行适配,而且网络操作系统以及硬件设备之间的通信都可以通过编程实现。

本书从初学者的角度出发,系统地论述了 SDN 的概念、OpenFlow 协议、控制器和交换机的相关概念。同时,书中提供了大量的实验,能够有效地帮助初学者感性认识和理解 SDN 的原理,通过这些应用案例,读者可以真正体会到 SDN 不同于传统网络的特点。为此,我推荐本书给有意愿从事网络领域学习和研究的科技工作者、老师和同学们,相信本书能够为你们从事 SDN 学习、研究和应用实践提供很好的参考与帮助。

北京邮电大学教授、江苏省未来网络创新研究院院长助理

黄 韬

西安电子科技大学出版社
应用型本科 电子及通信工程专业“十三五”规划教材
编审专家委员名单

主任：沈卫康(南京工程学院通信工程学院 院长/教授)

副主任：张士兵(南通大学 电子信息学院 副院长/教授)

陈 岚(上海应用技术学院 电气与电子工程学院 副院长/教授)

宋依青(常州工学院 计算机科学与工程学院 副院长/教授)

张明新(常熟理工学院计算机科学与工程学院 副院长/教授)

成 员：(按姓氏拼音排列)

鲍 蓉(徐州工程学院 信电工程学院 院长/教授)

陈美君(金陵科技学院 网络与通信工程学院 副院长/副教授)

段先华(江苏科技大学 计算机科学与工程学院 副院长/教授)

李文举(上海应用技术学院 计算机科学学院 副院长/教授)

梁 军(三江学院 电子信息工程学院 副院长/副教授)

潘启勇(常熟理工学院 物理与电子工程学院 副院长/副教授)

任建平(苏州科技学院 电子与信息工程学院 副院长/教授)

孙霓刚(常州大学 信息科学与工程学院 副院长/副教授)

谭 敏(合肥学院 电子信息与电气工程系 系主任/教授)

吴薛红(南京师范大学 电气与自动化工程学院 副院长/副教授)

王杰华(南通大学 计算机科学与技术学院 副院长/副教授)

王章权(浙江树人大学 信息科技学院 副院长/副教授)

郁汉琪(南京工程学院 创新学院 院长/教授)

严云洋(淮阴工学院 计算机工程学院 院长/教授)

杨俊杰(上海电力学院 电子与信息工程学院 副院长/教授)

杨会成(安徽工程大学 电气工程学院 副院长/教授)

于继明(金陵科技学院 智能科学与控制工程学院 副院长/副教授)

前 言

随着云计算、大数据、虚拟化等技术的发展以及它们在数据中心的广泛应用,网络流量急剧增加,业务种类不断丰富,为了满足不同业务对带宽、时延和可靠性等方面的需求,网络拓扑结构也越来越复杂。软件定义网络(SDN)是一种对传统网络进行变革的技术,它打破了传统网络的技术壁垒,让网络技术走向开放。

SDN 是一种新型的网络体系结构,通过将网络控制与网络转发解耦来构建开放可编程的网络体系结构。与传统网络相比,SDN 提高了组建网络的灵活性和管理水平,网络运营商在部署和维护网络方面也更便捷,可以大大降低运营成本。

SDN 正在不断地得到实际应用,其是否可以替代现有网络,或是仅能对现有网络进行完善和补充,其对现有网络的影响又如何,都还有待观察,但 SDN 已经引起了大家的广泛关注和期待。

本书共 7 章,各章的主要内容如下:第 1 章为 SDN 概述,主要介绍了 SDN 的体系架构、SDN 交换机、SDN 控制器、OpenFlow 协议、SDN 发展历史和应用领域等基础知识;第 2 章为 SDN 控制器,主要介绍了 SDN 控制器的体系结构、关键要素以及控制器集群技术,对开源的 SDN 控制器也进行了解析;第 3 章为 SDN 南向接口协议,主要介绍了基于 OpenFlow 协议的交换机、端口类型,并详细解析了流表的操作,对 OF-CONFIG 协议也进行了介绍;第 4 章为 SDN 交换机,解析了传统交换机和 SDN 交换机的区别,主要介绍了多个厂家的 SDN 硬件交换机和软件交换机;第 5 章为网络虚拟化,主要介绍了 SDN 接口的可编程性和网络虚拟化技术及其在 SDN 中的应用;第 6 章为 SDN 实战基础案例,通过搭建 SDN 网络环境,进行 SDN 协议分析工具使用、流表下发及网络均衡、SDN 网关功能、OpenDaylight 集群等实验,有助于开发人员掌握 SDN 网络架构和网络配置方法;第 7 章为 SDN 应用编程案例,详细介绍了 ARP 代理服务器、防 DDOS 网络攻击和基于 OpenDaylight 的 REST API 的应用与开发,同时对源码进行了分析。

本书第 1 章、第 2 章、第 6 章和第 7 章由毛其林老师编写,第 3 章和第 4 章由谭振建老师编写,第 5 章由吴海涛老师编写。周陆宁、徐相娟、杜静茹等同学参与了部分章节的资料整理工作,北京邮电大学黄韬教授认真审阅了本书,并提出了许多宝贵意见,在此一并表示感谢。

由于 SDN 这项新技术发展迅速,内容更新快,加上编者水平有限,书中疏漏和不当之处在所难免,恳请各位读者不吝指正。

编 者

2017 年 5 月于南京

目 录

第 1 章 SDN 概述	1
1.1 计算机网络概述	1
1.2 软件定义网络	2
1.3 SDN 交换机	5
1.4 SDN 控制器	7
1.5 OpenFlow 协议	9
1.6 SDN 发展历史	11
1.7 SDN 的应用领域	13
1.8 小结	15
复习思考题	16
第 2 章 SDN 控制器	17
2.1 概述	17
2.2 SDN 控制器的体系结构	19
2.3 SDN 控制器的关键要素	20
2.3.1 支持 OpenFlow 协议	21
2.3.2 网络虚拟化	22
2.3.3 网络功能化	22
2.3.4 可扩展性	23
2.3.5 网络性能	24
2.3.6 网络可编程性	25
2.3.7 网络可靠性	25
2.3.8 网络安全性	25
2.3.9 网络的集中管理和可视化	26
2.3.10 SDN 控制器供应商	26
2.4 SDN 控制器集群	26
2.4.1 SDN 控制器集群的关键技术	27
2.4.2 SDN 控制器集群的现有方案	29
2.5 SDN 控制器的编程接口模式	32
2.5.1 本地 API 调用	32
2.5.2 REST API 远程调用	33
2.6 SDN 开源控制器	34
2.6.1 SDN 开源控制器简介	34
2.6.2 OpenDaylight 控制器	36
2.6.3 ONOS 控制器	43

2.7 小结 47

复习思考题 47

第 3 章 SDN 南向接口协议 48

3.1 OpenFlow 协议概述 48

3.2 OpenFlow 交换机 50

3.3 OpenFlow 端口 51

3.4 OpenFlow 流表与组表 52

3.4.1 流水线处理 52

3.4.2 流表及删除 53

3.4.3 匹配 54

3.4.4 漏表 56

3.4.5 组表 56

3.4.6 计量表 57

3.4.7 计数器 58

3.4.8 指令 58

3.4.9 动作集 58

3.4.10 动作列表 59

3.4.11 动作 59

3.5 OpenFlow 通道 60

3.6 OpenFlow 消息 62

3.6.1 OpenFlow 消息简介 62

3.6.2 消息处理 64

3.6.3 消息事件 65

3.7 OF - CONFIG 协议 72

3.7.1 OF - CONFIG 1.2 版本概述 73

3.7.2 数据模型 75

3.8 其他 SDN 南向接口协议 75

3.8.1 XMPP 75

3.8.2 PCEP 77

3.8.3 NETCONF 78

3.8.4 OpFlex 79

3.9 小结 80

复习思考题 80

第 4 章 SDN 交换机 82

4.1 概述 82

4.1.1 传统交换机架构 82

4.1.2 SDN 交换机架构 84

4.1.3 SDN 交换机实现技术 85

4.1.4 传统交换机和 OpenFlow 交换机的比较 87

4.2 SDN 硬件交换机	91
4.2.1 基于 ASIC 的 SDN 品牌交换机	91
4.2.2 基于 ASIC 芯片的 SDN 白盒交换机	98
4.2.3 基于 NP 的 SDN 交换机	102
4.2.4 基于 NetFPGA 的 SDN 交换机	104
4.3 SDN 软件交换机	106
4.3.1 Open vSwitch 交换机	106
4.3.2 其他软件交换机	108
4.4 小结	109
复习思考题	110
第 5 章 网络虚拟化	111
5.1 虚拟化技术简介	111
5.2 服务器虚拟化	112
5.3 存储虚拟化	112
5.4 网络虚拟化	114
5.5 基于 SDN 技术的网络虚拟化方案	119
5.5.1 FlowVisor 简介	120
5.5.2 FlowVisor 常用命令	122
5.5.3 FlowVisor 工作流程	123
5.6 网络功能虚拟化与 SDN	124
5.7 小结	125
复习思考题	126
第 6 章 SDN 实战基础案例	127
6.1 概述	127
6.2 使用 Wireshark 抓取 OpenFlow 消息及相关内容分析	131
6.2.1 OpenFlow 消息	131
6.2.2 Wireshark 工具简介	133
6.2.3 Wireshark 抓包过程及消息分析	135
6.3 利用 OpenDaylight Yang UI 工具下发流表	142
6.3.1 Yang 模型工具简介	142
6.3.2 下发流表前的网络配置	142
6.3.3 利用 OpenDaylight Yang UI 下发流表的实现过程	143
6.3.4 使用 go-to-table 指令下发流表	148
6.4 使用 OpenFlow 流表实现网络负载均衡	150
6.4.1 网络负载均衡原理	150
6.4.2 基于 SDN 的负载均衡	150
6.4.3 OpenDaylight Web 界面	151
6.4.4 实现网络负载均衡的网络设置	152
6.4.5 通过下发流表改变网络访问路径	153

6.5 基于 OpenFlow 1.3 组表的验证性实验	158
6.5.1 组表的基本概念及主要作用	158
6.5.2 实验网络环境配置	158
6.5.3 利用 OpenDaylight Yang UI 工具实现简单的组表下发	159
6.5.4 类型为 all 的组表的使用	162
6.5.5 类型为 select 的组表的使用	164
6.6 SDN 网关功能的实现	165
6.6.1 SDN 中的网关	165
6.6.2 网关服务器参数配置	166
6.7 OpenDaylight 集群实验	168
6.7.1 OpenFlow 协议中的多控制器	168
6.7.2 集群实验网络环境配置	168
6.7.3 多节点集群配置	169
6.7.4 多节点集群验证	171
6.7.5 多节点集群抓包分析	178
6.8 小结	180
复习思考题	181
第 7 章 SDN 应用编程案例	182
7.1 基于 SDN 的 ARP 代理服务器	182
7.1.1 基于 SDN 的 ARP 代理服务器实现原理	183
7.1.2 基于 SDN 的 ARP 代理服务器网络设置	184
7.1.3 ARP 代理服务器的源码分析	187
7.2 基于 SDN 的防 DDOS 网络攻击	192
7.2.1 DDOS 防御实现原理	192
7.2.2 基于 SDN 的 DDOS 防御网络配置	196
7.2.3 基于 SDN 的 DDOS 防御源码分析	197
7.2.4 基于 SDN 的 DDOS 防御实验数据分析	199
7.3 基于 OpenDaylight REST API 的应用与开发	201
7.3.1 OpenDaylight REST API 简介	201
7.3.2 使用 Postman 调用 RESTCONF 接口进行流表操作	202
7.3.3 Java 应用程序中调用 OpenDaylight REST API	206
7.4 小结	211
复习思考题	211
参考文献	212



第 1 章

SDN 概述

1.1 计算机网络概述

计算机网络是指一些互相连接的、自治的计算机的集合，即连接分散计算机设备以实现信息传递的系统。自从 1969 年美国国防部高级研究计划署(Advanced Research Projects Agency, ARPA)资助的世界上第一个 ARPANET 分组交换网创建以来，计算机网络得到了飞速发展。1983 年，TCP/IP 协议成为 ARPANET 上的标准协议，使得所有基于 TCP/IP 协议的网络可以实现互联。

近年来，随着互联网应用于经济、社会和生活的各个方面，网络的规模和应用呈现出爆炸式增长。同时传统的电信网络在互联网的技术推动下也正在发生着剧烈的变革，多种网络的互通融合已成为当今网络发展的大趋势。1986 年，美国国家基金会(National Science Foundation, NSF)资助建成了基于 TCP/IP 技术的主干网 NSFNET，世界上第一个互联网由此产生，此后互联网迅速连接到世界各地，起源于美国的因特网如今已发展成为世界上最大的国际性的计算机互联网。随着互联网的出现，一大批基于互联网的技术应运而生：1992 年 Web 技术诞生；1995 年 Java 技术出现；1997 年多协议标签交换(Multi-Protocol Label Switching, MPLS)开始得到应用；1998 年 IPv6 的概念出现在人们的视野中；2004 年随着 Web 2.0 概念的提出，互联网应用向个性化协作发展；2006 年随着云计算概念的出现，互联网应用向平台化发展。同时 IP 技术的广泛应用催生了三网融合，并将成为物联网互联的基础协议。

当前计算机网络应用发生了日新月异的变化，但网络结构的变化却发展甚微。随着网络自身规模的扩大和业务能力的不断创新，海量数据的产生以及大数据的存储与计算所带来的挑战日益严峻。根据思科公司的测算，2014 年的网络流量是 2009 年的 4.3 倍，2015 年每秒产生 245 Tb 的数据。目前，传统网络的发展遇到了严重的技术瓶颈，主要体现在以下几方面：

(1) IP 地址空间严重不足，由此导致网络地址转换(Network Address Translation, NAT)的规模越来越大，其部署极大地增加了网络运维成本，并降低了服务质量。此外，全球 IPv4 地址面临资源枯竭，2011 年 2 月 3 日，全球 IP 地址分配机构 IANA(The Internet Assigned Numbers Authority)宣布其地址池中 IPv4 地址已分配完。截至 2011 年 12 月底，我国人均 IPv4 地址拥有量仅为 0.24 个，IPv4 地址资源的相对匮乏将成为制约我国物联网、

移动互联网、云计算、三网融合等产业发展的瓶颈。

(2) 路由表快速膨胀。2011 年 9 月, 全球 BGP(Border Gateway Protocol)路由共有 74 万条, 其中活跃路由 37 万条。

(3) IP 网络安全无法保证, 网络透明、加密失控、数据平面和管理平面不分离, 因而造成网络管理低效。

(4) 资源管理模式难以为继, 网络服务质量难以保证, 大型数据中心和互联网消耗了大量能源, 节能减排责任重大。

目前的网络通常由单独运行的、封闭的设备连接构成, 每台设备都有单独的操作系统, 通过路由协议等交换可达信息。现有网络主要存在以下不足:

(1) 交换机和路由器等网络设备运行于封闭的操作系统中, 各厂家只是有限地开放了一些命令配置接口, 并不提供核心网络功能的编程接口;

(2) 网络设备的管理和控制分散在不同的设备上, 无法提供集中统一的网络视图;

(3) 灵活性不够, 很难进行网络创新;

(4) 上层业务无法感知底层网络细节, 无法基于网络灵活性进行流量优化;

(5) 虚拟化支持困难, 网络的灵活性太差。

1.2 软件定义网络

20 世纪 90 年代, 随着计算机软件技术在传统通信领域的深入应用, 网络 IT 化、设备软件化、硬件标准化、计算资源虚拟化以及系统的开放性已经成为未来信息技术发展的一种趋势。尤其是系统的开放性已经成为技术发展的利器, 最典型的代表莫过于智能手机的快速发展。例如, 苹果的 iOS 系统和谷歌的 Android 系统利用其开放的特点吸引了成千上万的软件开发者为其开发应用软件, 移动终端的应用层出不穷, 超越了传统意义上“移动电话”的概念。从某种程度上可以说软件定义了移动手机终端, 现在智能手机的主要内涵就是开放的平台加上众多的应用创新。同时, 硬件向软件演进的趋势越来越明显, 硬件越来越“薄”, 软件越来越“厚”, 硬件提供基本的性能, 而软件保障更高的生产效率和按需而变的速度, 业务按需而变和人力成本上升是硬件软件化的主要驱动力。软件定义的概念引发了产业界的高度关注, IT(信息技术)、CT(通信技术)融合趋势越来越明显, IT 产业的中心已经从设备制造转移到软件设计。实际上, 软件定义的概念无处不在, 例如在电力系统中引入了软件定义电网(Software Define Grid, SDG), 在通信领域引入了软件定义无线电(Software Define Radio, SDR)等。有人甚至提出, 未来将是一个“软件定义企业”的时代。

传统网络设备路由器和交换机运行在封闭的系统中, 不利于网络自身的发展和创新, 因为路由、控制和管理功能紧紧耦合在同一台设备中, 应用层无法感知底层网络细节, 网络配置复杂, 逐台设备的管理模式难以完整地了解网络运行状态。因此, 路由器利用率不高, 网络的效率较低。据思科分析报告显示, 当今网络骨干链路的带宽利用率不足 40%。另外, 网络交换设备的高能耗也背离了当前绿色节能的发展理念。另一方面, 随着网络规模的扩大以及应用的不断丰富, 作为网络核心的路由器承载了过多的功能, 如分组过滤、区分服务、多播、服务质量保证、流量控制等, 使得路由器变得臃肿不堪, 充斥着各种“补

丁”式的设计结构。为了解决现有网络结构所面临的诸多难题，世界各国已经大规模地开展了未来网络的研究。

软件定义网络(Software Define Network, SDN)是软件定义在网络领域的应用。SDN 是一种新型的网络架构，其设计理念是将网络的控制平面与数据转发平面进行解耦，并使网络面向业务层可编程。网络可编程意味着应用层可以直接控制底层网络的数据转发行为，应用层业务可以感知底层网络的运行状态，可以细粒度地管控流量，网络的流量分配是可预测的。反过来说，SDN 运行的好与坏很大程度上取决于业务层对底层网络的管控能力。从这个意义上讲，所谓的软件定义网络，实际上是业务定义网络。

随着软件定义网络的概念被延伸扩展，不同行业、不同应用领域对 SDN 有着各自不同的需求，因此人们在谈论软件定义网络时通常也有着不同的理解。从宏观上讲，有专家学者认为 SDN 是一种建立新的网络科学的思想，是可望建立的一种复杂网络系统抽象的网络科学。根据开放网络基金会(Open Networking Foundation, ONF)对 SDN 的定义，软件定义网络是一种新兴的架构，是动态的、易管理的、性价比高的、适应性强的网络，这些特点使它成为今天高带宽的、动态的、自然的、应用型的理想网络。这种体系结构解耦网络控制和转发功能，使得网络控制可以直接编程，底层的网络基础设施被抽象为应用程序提供的网络服务。

SDN 架构的逻辑视图如图 1-1 所示，传统网络设备紧耦合的网络架构被拆分成应用层、控制层和基础层。

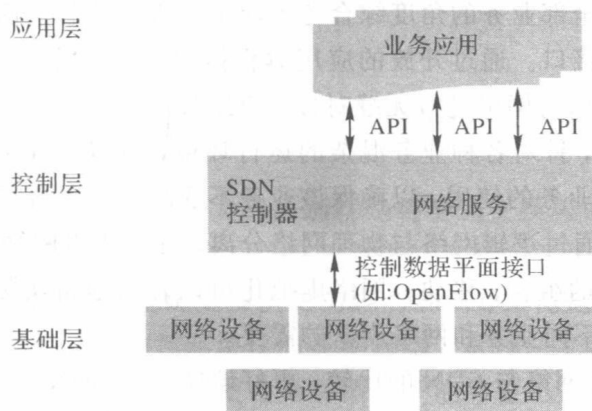


图 1-1 SDN 架构的逻辑视图

基础层(数据转发层)被抽象为网络底层服务，主要完成数据平面的存储转发功能。

控制层通过南向接口(参见图 1-2)控制数据平面层的数据转发、流量控制、数据统计等功能。

控制层对应用层提供统一的网络服务应用编程接口(Application Programming Interface, API)，这些 API 通常也称为面向具体业务模型的北向 API 接口。

应用层软件借助于北向 API 实现对网络的控制和定义。软件定义网络开放了网络的基础设施，如同计算机上的操作系统以及设备驱动程序为应用程序开放了其 CPU、内存、硬盘、打印机等基础设备，应用程序通过操作系统或设备驱动程序提供的 API 接口可以很方便地访问并控制底层设备。

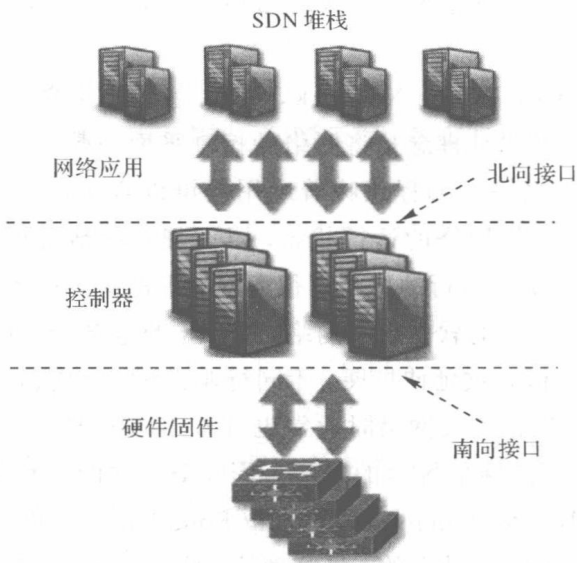


图 1-2 SDN 北向、南向 API 接口

SDN 与传统网络相比主要有以下特点：

(1) 集中控制。SDN 的控制平面和转发平面分离，转发设备可以专注转发而使自身功能变得更简单，集中的控制平面具有更好的灵活性和创新性。集中控制可以简化网络运行管理，提高业务配置速度，有利于实现网络的快速升级和创新。集中控制还有利于网络的全局优化，例如可以从全部业务的角度综合考虑流量工程和负载均衡。

(2) 开放软件编程接口。通过开放的应用编程接口 (API) 提供可编程的客户定制化的网络业务。应用程序可以与网络进行无缝对接，应用程序可以告诉网络如何运行才能满足自身业务的需求。例如，针对各种业务混杂的运行环境，可以从业务层的角度划分出一定带宽的流量供某种重要业务的使用，以确保该业务不受其他业务流量的影响。

(3) 网络虚拟化。通过逻辑网络与物理网络分离，确保逻辑网络不受物理网络的限制，逻辑网络可以进行任意的组合、移动。网络虚拟化可以轻易地将实际的物理网络虚拟出多个逻辑网络，用来满足不同业务和网络创新的需要。

表 1-1 给出了传统网络与 SDN 的比较，更好地展示了 SDN 的特点和优势。

表 1-1 传统网络与 SDN 的比较

传统网络	SDN
物理网络	虚拟网络
硬件决定网络	软件决定网络
垂直集成，软硬件紧密耦合	水平集成，软硬件分离
智能在核心	智能在边缘
组网要对硬件进行配置	组网只需要软件编程
网络主体复杂、刚性	网络主体简单、抽象
网络新功能开发时间长	网络新功能开发时间短
网络创新难，网络封闭	网络创新容易，网络开放



SDN 的核心特点是以实体设备作为基础资源,抽象出网络操作系统(Network Operating System, NOS)。NOS 隐藏底层物理细节,向上层提供统一的管理和编程接口,以 NOS 为平台开发的应用程序可以实现通过软件来定义网络拓扑、进行资源分配和处理等。Google 最早将 SDN 技术应用于实际网络环境。SDN 有以下优点:

(1) 提供网络结构的统一视图。对整个网络架构实现统一的浏览视图,从而简化配置、管理和优化操作。

(2) 高利用率。集中化的流量工程能够有效地调整端到端的流量路径,从而达到网络资源的高效利用。

(3) 快速故障修复。链路、节点故障都能实现快速修复。系统能够快速聚合网络资源,实现平均分配,并且对于一些网络行为可进行预测。

(4) 平滑升级。控制平面和转发/数据平面的分离可以做到在软件平滑升级的同时保证没有数据丢包或者性能衰减。

(5) 弹性计算。大规模的计算、路径分析都被集成在子控制器中,由较高性能的服务器完成。

同时,Google 也指出 SDN 所面临的挑战,包括:

(1) 协议不成熟。OpenFlow 协议还处于发展初期。

(2) 高容错的控制器。为了提高容错率,必须在网络中部署多个控制器,从而就要区分主、次控制器,以便进行高效配合。

(3) 功能区分复杂。路由器和控制器的功能区分仍在探讨阶段,功能配置仍是一个悬而未决的问题。

1.3 SDN 交换机

SDN 交换机与传统网络交换机最大的区别就是将普通交换机的数据平面和控制平面相分离,SDN 交换机只负责数据的转发,而控制数据转发指令则由 SDN 控制器下发。从这个意义上说,SDN 交换机相比传统交换机更为轻巧和简单,但这并不意味着 SDN 交换机没有任何控制协议,而是所有的控制协议均在控制器上运行。实际上很多情况下交换机上也可以驻留一些关键的控制协议,以便在局部情况下能够更迅速地作出相应的决策,只不过这些协议都会留有一些供调用的外部接口。数据平面(也称转发面)关注的焦点是性能优先、专业芯片优先以及标准化抽象的编程接口等方面,而控制平面则专注于灵活性优先、通用软硬件以及开发者环境等技术领域。

SDN 的实现方式主要有基于专用接口、基于开放协议(如 OpenFlow)以及基于 Overlay 等三种方式。其中,基于 OpenFlow 协议的实现相对更为成熟,研究更多,获得了众多厂商支持,业界影响大。因此,本书主要讨论支持 OpenFlow 协议的 SDN 交换机。SDN 交换机的主要处理单元是由一组流表构成的流水线,每个流表由许多流表项组成,流表项主要由匹配字段、计数器和操作等三部分组成,表示数据分组的匹配条件和数据转发条件。匹配字段几乎涵盖了传统网络中数据链路层、网络层和传输层的许多特征要素,如以太网类型,IPv4 源地址、目的地址,ICMPv6 Type, VLAN 优先级等 40 种匹配类型;计数器用于对数据流进行统计;操作则是指用于符合匹配条件将要进行下一个动作的指令。

基于 OpenFlow 协议的交换机开源项目有 OpenvSwitch(简称 OVS), 该项目主要提供多层虚拟交换网络, 通过 OpenvSwitch 扩展接口可以支持多种网络协议, 其中包括 OpenFlow 协议。虚拟交换网络具有配置灵活、成本低廉、使用方便等特点, 有利于网络创新。OVS 是由 Nicira Networks 主导的一个高质量的多层虚拟交换机, 遵循开源 Apache 2.0 许可证。通过可编程扩展, OVS 可以实现大规模网络的自动化操作(如配置、管理、维护等), 同时支持现有标准管理接口和协议(如 NetFlow、sFlow、SPAN、RSPAN、CLI、LACP、802.1ag 等)。用户可以使用任何支持 OpenFlow 协议的控制器对 OVS 进行远程管理控制。OpenvSwitch 的特性如下:

- (1) 支持通过 NetFlow、sFlow、IPFIX、SPAN、RSPAN 以及 GRE-tunneled 镜像使虚拟机内部通信可以被监控;
- (2) 支持链路汇聚控制协议(Link Aggregation Control Protocol, LACP)的多端口绑定;
- (3) 支持标准的 802.1Q VLAN 模型以及中继模式(Trunk);
- (4) 支持 BFD 和 802.1ag 链路状态监测;
- (5) 支持生成树协议(Spanning Tree Protocol, STP);
- (6) 支持细粒度的 QoS;
- (7) 支持 HFSC 系统级别的流量控制队列;
- (8) 支持对任一虚拟机网卡的流量控制策略;
- (9) 支持基于源 MAC 负载均衡模式、主备模式、L4 哈希模式的多端口绑定;
- (10) 支持 OpenFlow 协议(包括许多虚拟化的增强特性);
- (11) 支持 IPv6;
- (12) 支持多种隧道协议(GRE、VXLAN、IPsec、GRE 和 VXLAN over IPsec);
- (13) 支持通过 C 语言或者 Python 语言接口远程配置;
- (14) 支持内核态和用户态的转发引擎设置;
- (15) 支持多列表转发的发送缓存引擎;
- (16) 支持抽象的转发层, 易于转发到新的软件或者硬件平台。

利用在传统交换机设计方面的技术优势, 传统硬件厂商也纷纷推出了自己的 SDN 解决方案, 可以在原有交换机上提供支持 OpenFlow 协议的模块, 或者利用 SDN 的概念去改进原有的解决方案。

S12500 和 S10500 是华三两款采用先进的 CLOS 多级、多平面交换架构的系列交换机, S12500 是面向云计算数据中心设计的核心交换产品, S10500 是面向云计算数据中心核心、下一代园区网核心和城域网汇聚而专门设计开发的核心交换产品。

Pica8 公司专为云平台 and 虚拟化场景设计的 SDN 交换机具有充分的灵活性和可适配性, Pica8 交换机既可以满足传统网络架构需求运行标准的二层和三层网络协议, 也可以支持最新的 OpenFlow 协议, 同时, 基于专利技术实现两种模式基于端口的混合应用, 保证现有网络向 SDN 的平滑过渡。Pica8 交换机高性能硬件平台涵盖 1 G/10 G/25 G/40 G/100 G 等不同规格, 1 GbE 设备的最大交换能力可达 176 Gb/s, 10 GbE 设备的最大交换能力可达 1.44 Tb/s, 40 GbE 设备的最大交换能力可达 2.56 Tb/s, 25 G/100 GbE 设备的最大交换能力可达 3.2 Tb/s。

PF5240 系列交换机是 NEC 公司设计的 SDN 交换机, 同样可以满足传统网络架构需

求运行标准的两层或三层协议，也可部署 SDN 技术。PF5248-2T8X 交换机提供 8 个 10 GbE(SFP+)/1 GbE(SFP)端口以及 2 个 1GbE 端口，交换容量达到 164 Gb/s，转发能力达到 122 Mb/s，支持全线速转发。

V350 系列不仅仅是具有较优成本效益的高性能 OpenFlow 交换机，更是一个完整的开放 SDN 平台(见图 1-3)。盛科提供从核心芯片到系统软硬件的整体解决方案，并集成开源的 SDK(Software Development Kit)，帮助 SDN 厂商减少产品上市时间，降低研发成本。V350 平台的开放性可以给 SDN 厂商提供差异化的定制方案，帮助其创新。依托于盛科第三代高性能以太网交换机芯片 CTC5160，V350 提供了高达 240 Gb/s(8x1GE + 12x10GE)的转发能力，并具备丰富的 OpenFlow 特性。V350 系列提供了 2 种交换平台，即 V350-48T4X 和 V350-8TS12X，盛科 V350 OpenFlow 交换平台在 ONS2013 中荣获 SDN Idol@ONS 奖。

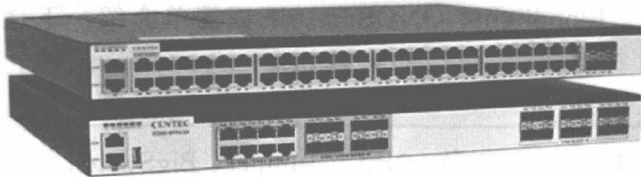


图 1-3 盛科 V350 交换机

1.4 SDN 控制器

SDN 控制器是 SDN 的核心和大脑，SDN 可以由简单的转发设备加通用服务器组成，其中，转发设备就是 SDN 交换机，通用服务器就是 SDN 控制器。SDN 控制器实际上是将传统交换机中的控制平面进行解耦，并集中统一汇聚到一台高性能的通用服务器上来实现，它集中了传统交换机中控制平面的功能，所以又简称之为控制平面。这样，原来在交换机中实现的网络功能，如防止环路、路径计算、基于策略的路由等，就可以统一由 SDN 控制器来完成，如图 1-4 所示。而 SDN 控制器 CPU 的性能和内存明显好于交换设备，因

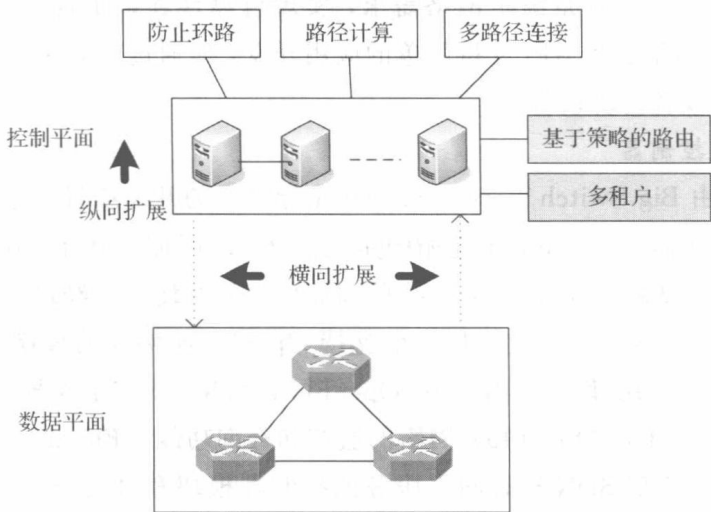


图 1-4 SDN 控制器(通用服务器)