软件定义网络：原理和实现技术 （作业一）

2017213815 张豪

SDN调研报告

# 一、SDN发展现状

SDN（Software-Defined Networking, 软件定义网络）起源于斯坦福大学 Nick McKeown 教授的 Clean Slate 项目，其目标是重新定义网络体系结构。

SDN主要具有：网络开放可编程、控制平面与数据平面的分离、逻辑上的集中控制这三个特征。

在学术研究团体中，OpenFLow 已经在美国斯坦福大学、印第安纳大学、Internet2、欧洲OFLEIA、日本JGN2plus、韩国NetOpen网络服务平台以及其他的诸多科研机构中部署。在企业界，各大芯片厂商、因特网服务提供商、设备厂商、电信运营商和创业公司对SDN技术跟进、产品研发和网络部署均产生了浓厚兴趣、并进行了积极实践。目前，思科和华为公司分别推出了ONE和SoftCOM以支持SDN的发展战略，并在部分设备上实现了对OpenFlow的支持。

# 二、SDN 研究当前存在的热点问题

## 2.1 交换机设计问题

SDN交换机位于数据层面，用来负责数据流的转发。通常可采用硬件和软件两种方式进行转发。对于硬件来说，具有速度快、成本低和功耗小等优点。但在灵活性方面，硬件则远远低于CPU和NP等可编程器件。如何设计交换机，做到既保证硬件的转发速率，同时还能确保识别转发规则的灵活性，成为目前研究的热点问题。

## 2.2 转发规则相关研究

网络节点失效、流量负载转移或网络维护等问题会导致SDN网络中的转发规则被迫改变，严重影响了网络的可靠性。由于在更新过程中存在延迟，转发路径上的交换机可能会出现使用新旧规则不一致的情况。如何解决这种不一致性也是当前急需研究的热点问题。

## 2.3 接口语言

传统的控制器平台仅能提供低级配置接口，使用像C++这种通用语言，抽象程度较低，造成网络配置成本并未大幅度降低。针对这种情况，科研人员致力于开发一种抽象的、高级配置语言，能够统一北向接口，改善接口的性能，从而全面降低网络的配置成本。

# 三、SDN在前进的路上，近期存在哪些困难与挑战？

## 3.1 协议标准化的问题

目前SDN的南向接口不再局限于 OpenFlow，同时北向接口尚未确定，而在应用层的实现，VMware和OpenStack各成体系。此外东西向接口的研究工作刚刚开展，暂时没有较为一致的认识。因此，SDN 标准体系是否要统一或能否统一还有争论。

## 3.2 安全性的问题

SDN 的集中控制方式和开放性将使得控制器的安全性面临极大的挑战，需要建立一整套隔离、防护和备份机制来确保其安全稳定运行。具体来说，控制器本身的安全（如健壮性、单点故障）、控制器和应用层之间的安全（如授权及认证、安全隔离）、控制器和转发设备之间的安全（如数据通道安全、访问控制一致性）都缺乏有效的解决方案。

## 3.3 SDN设备的关键性能

现有ASIC芯片架构都是基于传统的IP或以太网寻址和转发设计的，无法在SDN架构下维持设备的高性能，特别是基于OpenFlow的专用芯片架构及实现方案还有待开发。通过实验室测试发现，许多组网络关键指标（如流表容量、流表学习速度、流表转发速率、转发时延等）在不同厂商设备上的差异极大，难以达到商用标准。

# 四、在最近一段可预测的时间内，哪些应用最受益于SDN技术？

## 4.1 企业网与校园网

目前SDN已经支持对企业网和校园网的个性管理，允许企业网根据各自需求自主增加新功能。第二代中国教育和科研计算机网借鉴了SDN网络虚拟化技术将百所院校连接在一起，提供了 IPv4 应用和 IPv6 应用接入和互通互访等服务。

## 4.2 数据中心与云

SDN掌握全网缓存信息的能力，能够有效解决数据中心的数据传输冗余问题，实现在几乎无任何性能影响的情况下更新设备，还能够帮助数据中心提高资源的利用率，有效降低能耗，保证流量负载均衡，改善云性能。

## 4.3 广域网

通过SDN获取全局网络信息，可以保证流量平衡，实现对每个私人应用的平等对待,确保每位用户的应用不会受到其他用户应用的影响，并长期提高资源的利用率。

# 五、目前正在发展中的SDN技术与早期Scott Shenker等描述的SDN轮廓发生了哪些变化？

网络的管理工作越来越复杂，Scott Shenker 认为这是我们对网络的结构理解不够准确导致的。按照功能划分，网络结构应该被抽象层两个部分：数据层和控制层。前者对应每个网络结点内部的数据包转发工作，这只需要该结点本地的信息，是简单而快速的；后者对应数据包在网络中的路径决策工作，这需要整个网络的信息，是复杂的。SDN就是对这种网络结构认识的实现。故SDN应具有以下特点，然而这些随着SDN技术的发展都产生的变化。

## 5.1 控制程序负责配置所有的网络交换机

在后来的实践中发现将管理的需求转换到对实际物理交换机的直接控制这一工作非常复杂，而控制层的配置命令应该是纯逻辑的，简洁明了的。故后来在控制层和数据层中间还增添一个管理层，作用类似于编译器，将控制层简洁的配置需求编译成复杂的对实际物理交换机的直接控制命令。

## 5.2 所有的网络交换机具有的功能应该是同质的

在网络中传递一个数据包需要用到三个逻辑层次的功能，首先需要主机指出包的传送需求；当数据包到达交换机时，交换机要能够正确地识别该数据包；与此同时，我们可能还需要对网络进行一些结构层次上的配置操作。现在的网络使用协议头来完成前两个逻辑层次的工作，而且配置网络的方法还很笨拙。SDN有很强的网络配置功能，同时还引入了 MPLS 技术来将前两个逻辑层次进行分离。但这导致SDN需要两种交换机来分别完成这两个逻辑层次的工作。一种边缘交换机，负责将主机指定的数据包传送需求信息转换成一种特殊标记，另一种是核心交换机，负责根据该特殊标记完成数据包的转发任务。

## 5.3 网络只由硬件交换机组成

边缘交换机通常都在主机的内部，而且为了使SDN具有更强的可编程性，边缘交换机更适合使用软件交换机实现。

## 5.4 数据层应该非常的简单

除了转发，数据包在网络上被传递的过程中还需要大量其他的处理，如 VLAN，防火墙等，这些操作都很复杂，而且需要由数据层来实现。

# 六、SDN发展的动向有哪些？

## 6.1 网络管控更加智能化

SDN技术的全局视图和集中可控使得网络流量控制、接入控制、监测隔离等变得方便有效，降低了管控难度，但很多操作处理仍然需要由网络管理人员直接或间接参与，增加了人力成本。所以控制器需要更加智能，实现全程无人管理，减少人力成本的投入。

## 6.2 建立更加有效的网络溯源与取证体系

虽然利用SDN技术进行网络溯源与网络取证，过程变得更加简单、复杂性更低，但整个数据分析处理过程全部转移到控制器上完成，控制器大数据的实时处理能力成为瓶颈。所以目前来看仍没有非常有效的网络溯源与取证体系，需要研究者们在以后的工作中继续研究。

## 6.3 应用有效审计分析

目前采用的应用审计框架大多不具备灵活性，普适性差，或多或少存在安全漏洞，无法对应用进行有效审计。同时，第三方应用几乎都不开源，无法检测应用中的恶意代码，攻击技术手段的隐蔽性和复杂性使得检测过程难度增加。所以，急需采取有效措施解决应用审计与恶意代码检测问题。

## 6.4 安全策略服务组合与简化

目前SDN上的安全服务与安全策略几乎都是相互独立的，并且实现复杂、功能较单一，一种策略只能实现一种或少量几种安全性能，这样就会有大量的复杂策略积压在控制器和交换机中，占用大量存储空间资源，同时策略冲突的概率也大大增加。系统可以考虑将安全策略进行有效的整合，简化功能，使网络设备只需要加载少量的安全策略即可满足网络防护需求，减轻网络负担，节省存储与处理资源。