《互联网周刊》2015.2.2

网络中间设备路在何方

李军　清华大学信息技术研究院

长期以来，网络领域研究和产品的主流关注，都集中在网包（packet）的转发（forwarding）上，其中交换（switching）和路由（routing）是核心功能。当今，以交换机和路由器为主建立起来的网络连接和拓扑已经构成相当完善的信息基础设施，安全和隐私方面的挑战更加突显，差异化提供网络个性服务的呼声更加强烈，智能化提升网络综合品质的要求更加迫切，关于“中间设备”（middlebox）的研究和开发必然成为热点。

转发设备 vs 中间设备

伴随着网络虚拟化和动态化的不断增强，传统的转发设备无法满足网络安全和优化的需求，网络中间设备与传统转发设备并驾齐驱，发挥着越来越重要的作用，成为网络技术与系统的核心内容之一。Justine Sherry 等人发表于 SIGCOMM 2012 的文章指出，在实际网络环境中，网络中间设备与网络交换设备在数量上旗鼓相当，如图 1 所示【1】。

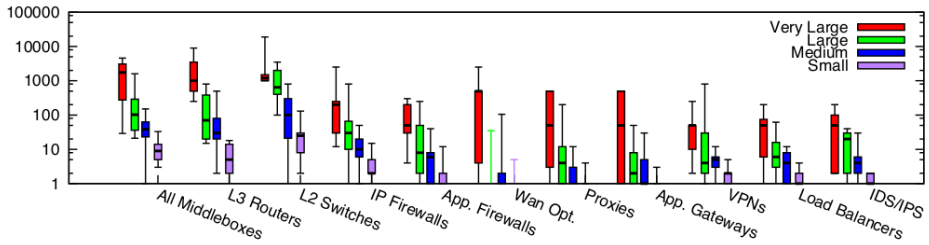

图 1、网络转发与中间设备数量对比

以交换机和路由器为代表的**网络转发设备**，根据包头(header)信息对网包逐个加以处理，主要承担将网包接力送达的简单任务。因其处理功能通常基于网包，只需关注包头中的目的标识（地址、端口等），所以也只要掌握与相邻转发设备相关的转发策略。最初的软件定义网络（SDN，Software Defined Networking）

无非是将基于局域拓扑知识生成转发策略的机制，替换为基于广域知识做出转发决策，从而使得智能优化和全局调度成为可能，极大地释放了网络的活力。

	转发设备	中间设备
处理任务	送达	安全、统计、优化
逻辑对象	网包	网流
物理对象	L2 ~ L4 包头	L3 ~ L7 包头 + 载荷
决策基础	拓扑	资源、策略
管控方式	局域自治	广域集中
产品形态	集线器 交换机 路由器	中间设备 （防火墙、IDS/IPS 防病毒/防垃圾）

图 2、网络转发与中间设备特点对比

相对于网络转发设备，**网络中间设备**的任务繁杂得多，包括了网包转发之外的各种处理，既有对载荷（payload）的关注，如入侵监控和病毒清除，也有对网包的处理，如 NAT 修改包头、VPN 加密网包，还有防火墙、负载均衡和流量控制等。这些中间设备的一个重要特点，即其处理功能无论粒度粗细，大多是基于网流的。

由于各种中间设备发展不均衡，相关研究一直以来也较为分散，长期未能形成统一的技术体系。2013 年，ACM CoNEXT 首次组织了 HotMiddlebox，将中间设备作为一个热门主题专门加以研讨，是全球网络界发起集中攻关的重要里程碑。

中间设备 vs 软件定义

业界普遍认为，目前的中间设备大多为专用硬件产品，成本居高不下，功能更新困难，是造成网络僵化从而难以适应流量需求变化的罪魁祸首之一。将中间设备的高级处理功能迁移到可以通过虚拟化实现共享的通用硬件平台上，使之成为由软件定义的网络服务，实现按照需求在适当时间和位置的部署，也符合网络功能虚拟化（NFV，Network Functions Virtualization）的大趋势。

最初由斯坦福的 Nick McKeown 和伯克利的 Scott Shenker 等人提出的 SDN 概念，聚焦于将转发设备的控制平面从数据平面分离出来，以实现标准的数据平面和集中的控制平面，从而打破专用硬件转发设备的垄断，使能统一、智能的网络资源优化。但是，他们当时显然忽视或低估了中间设备的存在和复杂，SDN 产业化也因而遇到一个必须面对的难题。Scott Shenker 等人在阐释“SDNv2”的设想时，也明确提出整合中间设备是 SDN 新架构中的三大变革之首【2】。然而，尽管 SDNv2 的构思将中间设备的功能推向网络边界(edge)，而在网络中心(core)只做转发，但网络服务的演进将会面对数据、内容处理越来越强烈的需求，中间设备注定是 SDN 绕不开的问题。

所以，SDN 只有拥抱 NFV，才能完善自己。没有 NFV，SDN 停留在网络拓扑和控制决策层面，没有灵活的资源可供调度，至少中间设备的功能会成为绊脚石；没有 SDN，NFV 停留在软件化和虚拟化层面，无法灵活地按需提供服务。把软件定义转发与软件定义监控(此处暂且以监控代指中间设备的功能)结合起来，NFV 的功能更加丰富，SDN 的控制更显强大，网络才能真正“活”了，也才可能变得更有智慧，最终使网络成为服务。

中间设备 vs 网流监控

“中间设备 middlebox”是个很特别的专业网络术语，当转发之外的网络处理功能由软件虚拟化实现后，“设备 box”的说法已经词不达意。考虑到中间设备的功能以网流处理和监控（monitoring/inspection & control/management）应用为突出特点，不妨将它们归类为**网流监控**，以便与**网包转发**对应，尽管其中会有一些交叠或模糊之处。

中间设备是网流监控的物理载体，而网流监控是提供网络高级处理服务的基础，尤其是保障网络安全的核心技术手段。在网流监控方面，重要的研究包括：在网络架构方面，网络服务功能的灵活组合与便捷控制；网络构件方面，网络功能模块的高效算法与优化配置（包括与硬件平台的适配）；网络安全方面，网络安全区域的严密隔离和接口管控。

目前，网流监控的功能的部署只是接近毫秒级别，处理能力也还仅在 10Gbps 左右。随着网络带宽的不断提升，网流监控的算法性能、负载调度与策略管理将受到极大的挑战。由于中间设备功能的本质是在网流粒度上将策略应用于网络流量，策略的表达、分布和下发成为网流监控研究的核心和难点，迫切需要建立策略表达的标准语言和策略分析的通用方法，根据网络拓扑和流量、服务能力和状态等启发信息，结合流量调度优化策略分布，并利用策略和流量的局部性（locality），综合预取和缓存机制，提升策略下发效率，实现最大处理能力。

总之，中间设备在网络运行和进化中与转发设备同等重要，并将在以数据和内容为中心的网络服务中成为关注的焦点。2015 年，HotMiddlebox 将移师更为显赫的 ACM SIGCOMM 殿堂，不禁让人更加期待网流监控技术的突破，特别是在高效的载荷过滤算法和敏捷的策略管理机制等方面。

【1】 J. Sherry et al. Making Middleboxes Someone Else’s Problem: Network Processing as a Cloud Service. In Proc. SIGCOMM, 2012.
【2】 S. Shenker 在“2014 中国未来网络产业高峰论坛”上的演讲。

2014/1/29