基于 ONF 的 NFV 选型

计算和存储虚拟化技术经过几年时间的发展，已经基本能够满足用户的需求，而随着云计算 IDC 的规模越来越大，以及客户个性化需求的日趋强烈，网络已经成为制约云计算 IDC 发展的最大瓶颈，主要体现在以下几个方面：

虚拟化环境下网络配置的复杂度极大提升。IDC 内部设备众多，特别是计算资源虚拟化后，虚拟机的数量更是数十倍地增长，且各类业务特性各异，导致网络配置的复杂度大大增加。

虚拟化环境下无法有效进行拓扑展现。无法很好地呈现业务系统与网络资源之间的对应关系，导致运维复杂，极易出现问题。

无法实现动态的资源调整。不同业务系统的流量、安全策略等均有所不同，传统的网络技术无法动态感知各业务属性，从而灵活地进行适应性的资源调整，容易造成资源的浪费或过载。

（1） 基于专用接口

此方案主要为一些网络设备厂家主导的方案，SDN 控制器与网络设备之间通过私有协议进行通信，实现网络配置的统一管理和下发。方案需要对现有网络设备进行软件化的升级改造，较易实现，过渡平滑。但缺点也很明显，就是标准不统一，异厂家无法互通，SDN 控制器适配多种设备难度很大。

（2） 基于开放协议

将厂家的私有协议换成基于 ONF 主导的 OpenFlow 等标准开放协议。缺点是 OpenFlow 标准的产业化成熟度不高，目前不同的标准化组织之间还存在激烈的竞争，标准无法统一，而且需要对现有的网络设备进行大规模的升级与替换，无法很好地实现业务的平滑升级过渡。

（3） 基于叠加（Overlay）

上面两个方案都是需要对现有的硬件设备进行全面的升级或替换，一方面会造成前期投资的浪费，另一方面也容易造成业务的中断。以现有的 IP 网络为基础，在其中建立软件实现的叠加层，全面屏蔽底层物理网络设备，所有的网络能力均以 NFV 倡导的软件虚拟化的方式提供。

方案的优势是不依赖于底层网络设备，可灵活地实现业务系统的安全、流量、性能等策略，实现多租户模式，基于可编程能力实现网络自动配置。缺点是在一定程度上增加了网络架构的复杂度，且通用服务器架构与传统的专用网络设备相比存在一定的性能缺失。

（4） 多租户的网络隔离

为了实现多租户的网络隔离，采用一种 L2 over L3 的隧道技术来构建一张虚拟网络，隧道封装协议的选择有 VxLAN、MPLS over GRE（基于多协议标签交换的标准路由封装）、NV-GRE（基于网络虚拟化的标准路由封装）、STT（StatelessTransport Tunneling，无状态传输隧道）等多种，目前支持较多的是 VxLAN。VxLAN 的工作原理是创建第二层的逻辑网络，并将其封装在标准的第三层 IP 包中，无需依赖传统的 VLAN 等二层隔离手段，即可实现多租户的逻辑区分，使得用户可以很方便地在现有网络上大量创建虚拟域，并使它们彼此之间以及与底层网络完全隔离。

（5） 利用 NFV 实现路由及边界防护

IDC 的东、西向流量给传统的集中式路由模式带来了挑战，为了很好地解决这个问题，采用基于软件定义的路由器以及防火墙，将其分布式部署在各个通用服务器的虚拟化层，为每个租户分配独立的逻辑路由器以及防火墙，支持各租户之间的个性化定制要求，并智能地将流量按最短路径进行转发，从而减轻核心交换机的压力。基于通用服务器架构的虚拟机实现南、北向的网络边界防护，包括四至七层的负载均衡、防火墙、路由器以及其他高级网络服务功能，可以完全取代传统模式下的硬件边界网关设备。

总结 NFV 解决方案以较低的成本实现了云计算 IDC 网络的智能化，简化了网络配置，实现了多租户隔离，但也带来了一些问题，比如可靠性相对低于专有电信设备、转发性能会有损失等。