SDN：Soft ware Defined Network　软件定义网络

软件定义网络（Software Defined Network, SDN ），是一种新型网络创新架构，是网络虚拟化的一种实现方式，其核心技术 OpenFlow 通过将网络设备控制面与数据面分离开来，从而实现了网络流量的灵活控制，使网络作为管道变得更加智能。

SDN 优势

传统 IT 架构中的网络，根据业务需求部署上线以后，如果业务需求发生变动，重新修改相应网络设备（路由器、交换机、防火墙）上的配置是一件非常繁琐的事情。在互联网/移动互联网瞬息万变的业务环境下，网络的高稳定与高性能还不足以满足业务需求，灵活性和敏捷性反而更为关键。SDN 所做的事是将网络设备上的控制权分离出来，由集中的控制器管理，无须依赖底层网络设备（路由器、交换机、防火墙），屏蔽了来自底层网络设备的差异。而控制权是完全开放的，用户可以自定义任何想实现的网络路由和传输规则策略，从而更加灵活和智能。

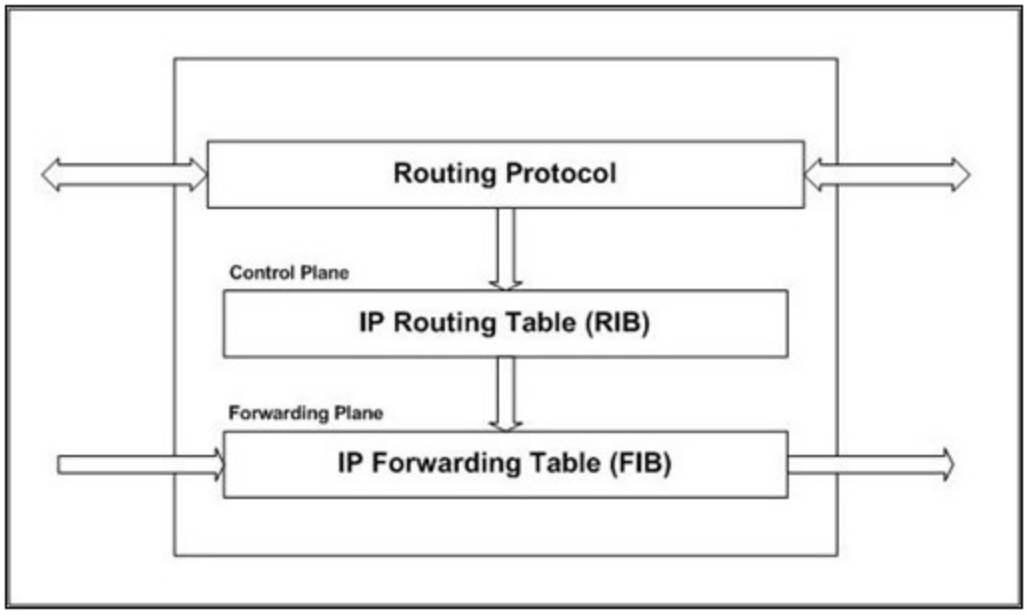
进行 SDN 改造后，无需对网络中每个节点的路由器反复进行配置，网络中的设备本身就是自动化连通的。只需要在使用时定义好简单的网络规则即可。如果你不喜欢路由器自身内置的协议，可以通过编程的方式对其进行修改，以实现更好的数据交换性能。

假如网络中有 SIP、FTP、流媒体几种业务，网络的总带宽是一定的，那么如果某个时刻流媒体业务需要更多的带宽和流量，在传统网络中很难处理，在 SDN 改造后的网络中这很容易实现，SDN 可以将流量整形、规整，临时让流媒体的“管道”更粗一些，让流媒体的带宽更大些，甚至关闭 SIP 和 FTP 的“管道”，

待流媒体需求减少时再恢复原先的带宽占比。
SIP（Session Initiation Protocol，会话初始协议）是由 IETF（Internet Engineering Task Force，因特网工程任务组）制定的多媒体通信协议。它是一个基于文本的应用层控制协议，用于创建、修改和释放一个或多个参与者的会话。例如 Internet 电话

正是因为这种业务逻辑的开放性，使得网络作为“管道”的发展空间变为无限可能。如果未来云计算的业务应用模型可以简化为“云—管—端”，那么 SDN 就是 “管”这一环的重要技术支撑。

路由表 (Routing Table, Routing Info Base) 和转发表 (Forwarding Info Base) 是两种不同的表。
它们共享相同的信息，但是用于不同的目的。



路由表

RIB 存储所有的路由信息。它与具体的路由协议无关。所有的路由协议都在这里保存它们的路由。只要路由器上运行的路由协议学到了新路由，就都会放到路由表中。

当目标地址不可达时，对应的路由条目先被标记为 Unreachable，然后就从 RIB 中删除。

注意：RIB 不是用来进行 IP 包转发的，也不会被宣告到网络中。

转发表

Forwarding Information Base 转发表 (FIB) 用于判断基于 IP 包的网络前缀，如何进行转发。

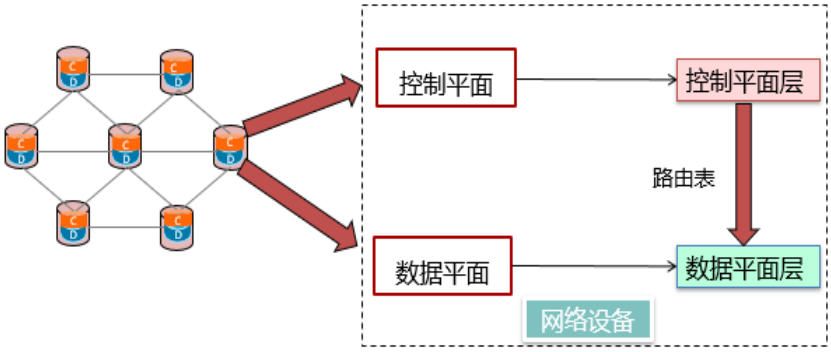
对于每一条可达的目标网络前缀，FIB 包含接口标识符和下一跳信息。 FIB 概念上类似于路由表。它维护一份 RIB 表中的转发信息镜像。

当 IP 路由从 RIB 拷贝到 FIB 时，它们的下一跳信息被明确地分析出来，包括下一跳的具体端口，以及如果到下一跳有多条路径时，每条路径的具体端口。

FIB 表中的条目数也是影响路由器性能的重要因素。通常来讲，FIB 条目越多，查找花费的时间越长。但由于基于 ASIC 芯片的转发技术日臻成熟，目前的查找转发几乎能达到线速。

传统网络数据控制与转发

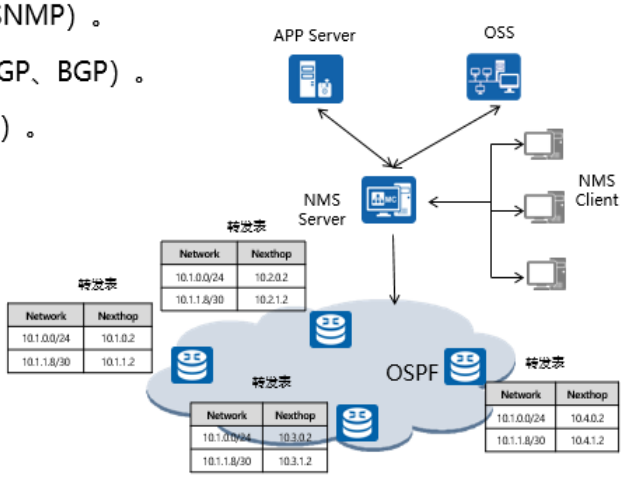
- 传统网络是分布式控制的架构，每台设备都包含独立的控制平面、数据平面。



- 传统网络是分布式控制的架构：
- 这里的分布式控制指在传统 IP 网络中，用于协议计算的控制平面和报文转发的数据平面位于同一台设备中。
- 路由计算和拓扑变化后，每台设备都要重新进行路由计算过程，并称为分布式控制过程。
- 在传统 IP 网络中，每台设备都是独立收集网络信息，独立计算，并且都只关心自己的选路。
- 这种模型的弊端就是所有设备在计算路径时缺乏统一性。

传统网络结构体系

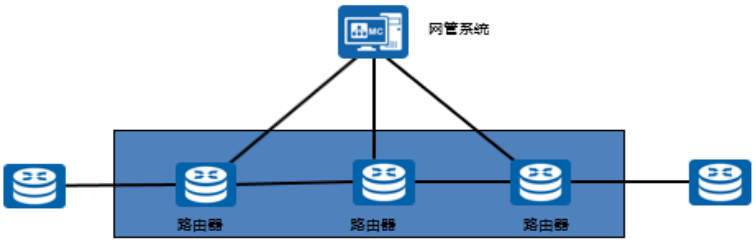
- 传统网络的管理平面、控制平面、数据平面：
  - 管理平面：设备管理（SNMP）。
  - 控制平面：路由协议（IGP、BGP）。
  - 数据平面：转发表（FIB）。



- OSS：Operation Support System，运营支撑系统。
- NMS：Network Management Server，网络管理服务器。
- 传统网络架构：
- 传统网络分为管理平面、控制平面和数据平面。
- 管理平面主要包括设备管理系统和业务管理系统，设备管理系统负责网络拓扑、设备接口、设备特性的管理，同时可以给设备下发配置脚本。业务管理系统用于对业务进行管理，比如业务性能监控、业务告警管理等。
- 控制平面负责网络控制，主要功能为协议处理与计算。比如路由协议用于路由信息的计算、路由表的生成。
- 数据平面是指设备根据控制平面生成的指令完成用户业务的转发和处理。例如路由器根据路由协议生成的路由表对接收的数据包从相应的出接口转发出去。

传统网络局限性

- 传统网络的局限性：
  - 流量路径的灵活调整能力不足。
  - 网络协议实现复杂，运维难度较大。
  - 网络新业务升级速度较慢。



传统网络基本架构

- 传统网络局限性：
- 传统网络通常部署网管系统作为管理平面，而控制平面和数据平面分布在每个设备上运行。
- 流量路径的调整需要通过在网元上配置流量策略来实现，但对于大型网络的流量进行调整，不仅繁琐而且还很容易出现故障；当然也可以通过部署 TE 隧道来实现流量调整，但由于 TE 隧道的复杂性，对于维护人员的技能要求很高。
- 传统网络协议较复杂，有 IGP、BGP、MPLS、组播协议等，而且还在不断增加。
- 设备厂家除标准协议外都有一些私有协议扩展，不仅设备操作命令繁多，而且不同厂家设备操作界面差异较大，运维复杂。
- 传统网络中由于设备的控制面是封闭式的，且不同厂家设备实现机制也可能有所不同，所以一种新功能的部署可能会造成周期较长；且如果需要对设备软件进行升级，还需要在每台设备上进行操作，大大降低了工作效率。

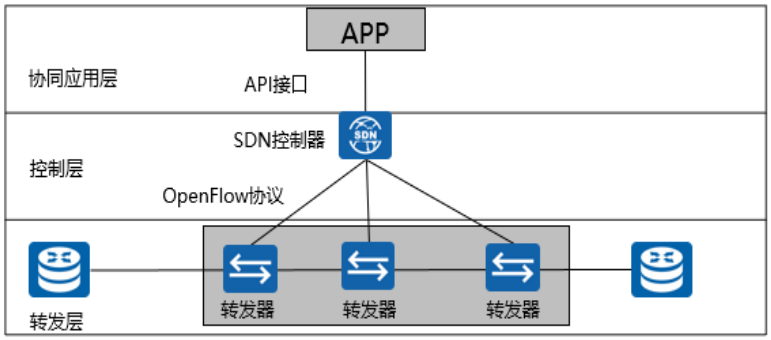
SDN概述

- SDN（Soft ware Defined Network）——软件定义网络。
  - 2006年，以斯坦福大学教授Nike McKeown为首的团队提出了OpenFlow的概念，并基于OpenFlow技术实现网络的可编程能力，使网络像软件一样灵活编程，SDN技术应运而生。
  - SDN的三个主要特征：
    - 转控分离。
    - 集中控制。
    - 开放接口。
- SDN控制器既不是网管，也不是规划工具。
  - 网管没有实现转控分离。
  - 规划工具的目的和控制器不同。

- SDN 的三个主要特征：
- 转控分离：网元的控制平面在控制器上，负责协议计算，产生流表；而转发平面只在网络设备上。
- 集中控制：设备网元通过控制器集中管理和下发流表，这样就不需要对设备进行逐一操作，只需要对控制器进行配置即可。
- 开放接口：第三方应用只需要通过控制器提供的开放接口，通过编程方式定义一个新的网络功能，然后在控制器上运行即可。
- SDN 控制器既不是网管，也不是规划工具：
- 网管没有实现转控分离：网管只负责管理网络拓扑、监控设备告警和性能、下发配置脚本等操作，但这些仍然需要设备的控制平面负责产生转发表项。
- 规划工具的目的和控制器不同：规划工具是为了下发一些规划表项，这些表项并非用于路由器转发，是一些为网元控制平面服务的参数，比如 IP 地址，VLAN 等。控制器下发的表项是流表，用于转发器转发数据包。

SDN网络体系架构

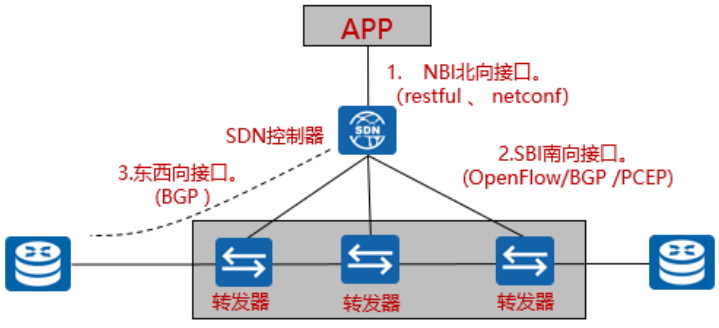
- SDN是对传统网络架构的一次重构，由原来的分布式控制的网络架构重构为集中控制的网络架构。
- SDN网络体系架构的三层模型：



- 协同应用层：这一层主要是体现用户意图的各种上层应用程序，此类应用程序称为协同层应用程序，典型的应用包括 OSS、Openstack 等。传统的 IP 网络同样具有转发平面、控制平面和管理平面，SDN 网络架构也同样包含这 3 个平面，只是传统的 IP 网络是分布式控制的，而 SDN 网络架构下是集中控制的。
- 控制层：控制层是系统的控制中心，负责网络的内部交换路径和边界业务路由的生成，并负责处理网络状态变化事件。
- 转发层：转发层主要由转发器和连接器的线路构成基础转发网络，这一层负责执行用户数据的转发，转发过程中所需要的转发表项是由控制层生成的。

SDN架构下的接口

- NBI (North Bound Interface) 北向接口。
- SBI (South Bound Interface) 南向接口。



SDN网络中的3个主要接口。

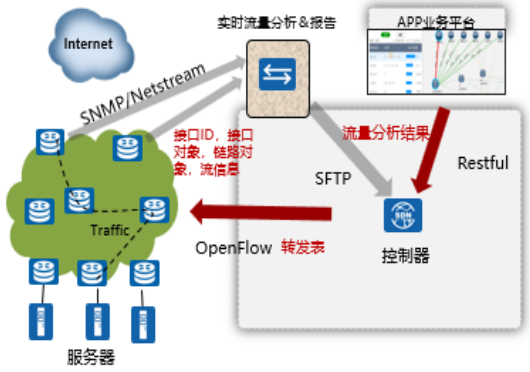
思考：SDN为什么要和传统网络进行互通？是否必须在控制器上运行东西向协议？是否可以不这样做？

- Restful 接口：
- Restful 接口为控制器与上层 APP 的北向接口，开放的 API、设备私有接口，所有满足 rest 架构的互联网软件架构都是 restful。
- Rest 为“表现层状态转化”，表现层就是资源的表现，即 rest 是被访问的资源（文本，图片，音乐，视频等），从一种形式的状态迁移到另一种形式的状态，本质就是一种互联网资源访问的协议。
- OpenFlow 接口：
- OpenFlow 接口是控制器与下层转发器之间的一种基于芯片的接口协议。OpenFlow 协议基于 TCP/IP，用于转发器与控制器之间的通信。
- BGP 接口：
- BGP 接口是在 BGP 协议基础上添加一些 BGP 路由属性（比如 Additional Path 属性和 BGP Flowspecification 属性），用于下发 BGP 的一些路由特性，从而使得 IDC 数据中心出口路由器根据这些特性实现流量调优。
- PCE 接口：

- PCE 接口用于控制器根据网络可用带宽计算出流量工程路径，用于数据中心 AS 内部的 TE 隧道的建立。
- 运营商网络已经大规模部署了传统分布式网络，不能在较短时间内升级到 SDN 网络，与传统网络互通就是必要的。SDN 控制器必须支持各种传统的跨域路由协议，以便解决和传统网络互通问题。
- 东西向协议是必须的，在 SDN 控制器上运行东西向协议，通过简单的修改或升级控制器程序就能提供新业务。另一方面，东西向协议为 SDN 控制器跨域互联及 SDN 控制器分层部署提供了接口。

SDN基本工作原理

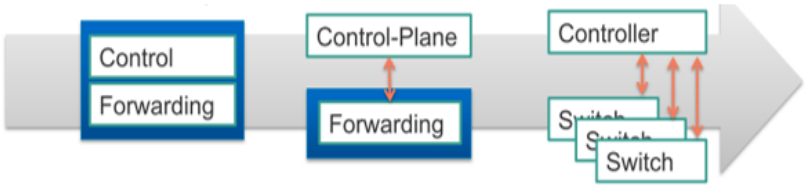
- 网元资源信息收集。
  - 转发器注册信息。
  - 上报资源过程。
  - MPLS标签信息。
  - VLAN资源信息。
  - 接口资源信息等。
- 拓扑信息搜集。
  - 节点对象、接口对象、链路对象（LLDP/IGP/BGP-LS）。
- SDN网络内部交换路由的生成。



- 通常控制器作为服务端，转发器主动向控制器发起控制协议建立，通过认证后，控制协议即建立连接。
- 注册信息中的设备信息包括资源信息（接口、标签、VLAN 资源等）、设备厂家信息（设备类型信息和设备版本号以及设备 ID 信息）。控制器采集这些信息是为了根据这些信息来进行本地搜索和加载相应驱动程序。
- 网络拓扑是描述网络中节点和链路以及节点之间连接关系的信息。

- 控制器收集拓扑信息的目的是为了根据网络资源，计算合理的路径信息，通过流表方式下发给转发器。

OpenFlow的思想和功能



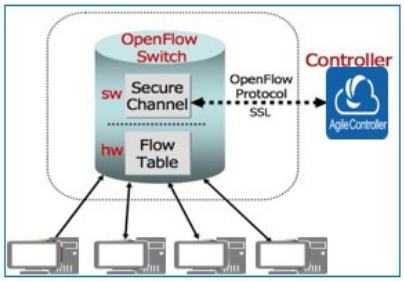
- 两个角色：
  - OpenFlow Controller：用于控制OpenFlow Switch，计算路径，维护状态和将流规则下发给交换机。
  - OpenFlow Switch：从OpenFlowController控制器接收命令或者流信息，以及返回状态信息。
  - OpenFlowSwitch基于流表并根据流规则进行转发、处理数据。

- “Flow”指的是一组具有相同性质的数据包，例如“五元组”（SIP、DIP、SPORT、DPORT、Protocol）。
- OpenFlow 协议是控制器和转发器之间的控制协议。
- 交换机与控制器之间可以通过加密的 OpenFlow 协议通信。
- OpenFlow 交换机是数据平面，基于 Flow Table 进行数据转发，并负责网络策略的具体执行。
- OpenFlow Controller 是控制平面设备，负责生成 OpenFlow 交换机上的 Flow Table，以及对 Flow Table 的更新和维护。
- OpenFlowSwitch 的基本组成：
- Flow Table：保存对每一个流的定义及相应处理行为。
- 安全网络通道：连接交换机和控制器，用于传输控制信令。当一个新数据包第一次到达交换机时，交换机通过这个隧道将数据包送往控制器进行路由解析。

- OpenFlow 协议：一套公开标准接口，用于读写 Flow Table 的内容。

OpenFlow网络交换模型

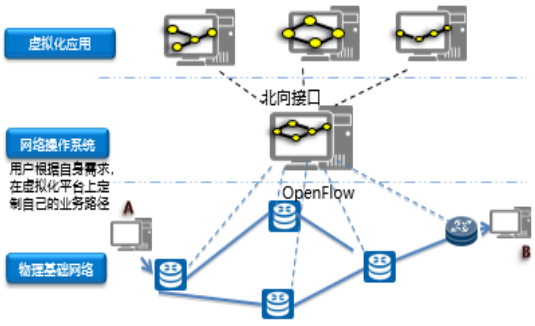
- 该模型的指导思想是：底层的数据通信（交换机、路由器）是“简化的”，并定义一个对外开放的关于流表FlowTable的公用API（应用程序接口），同时采用控制器来控制整个网络。



OpenFlow整体结构

网络业务快速创新

- SDN的可编程性和开放性，使得我们可以快速开发新的网络业务和加速业务创新。如果希望在网络上部署新业务，可以通过针对SDN软件的修改实现网络快速编程，业务快速上线。

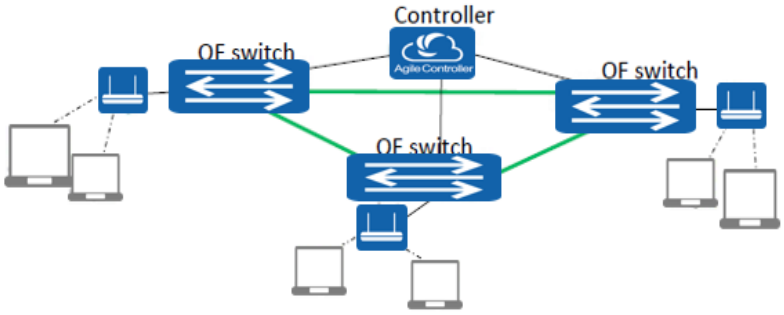


- SDN 网络关键的地方是在网络架构中增加了一个 SDN 控制器，把原来的分布式控制平面集中到一个 SDN 控制器上，由这个集中的控制器来实现网络集中控制。SDN 网络架构具备 3 个基本特征：转控分离、集中控制、开放接口。

- SDN 通过在网络中增加一个集中的 SDN 控制器，可以简化网络和快速进行业务创新。但是其本质的技术原理是通过 SDN 控制器的网络软件化过程来提升网络可编程能力。通信平面仍包含管理平面、控制平面和数据平面，SDN 网络架构只是把系统的三个平面的功能进行了重新分配，传统网络控制平面是分布式的，分布在每个转发设备上，而 SDN 网络架构则是把分布式控制平面集中到一个 SDN 控制器内，实现集中控制，而管理平面和数据平面并没有太多什么变化。
- SDN 网络具备快速网络创新能力，如果这个新业务有价值则保留，没有价值可以快速下线。不像传统网络那样，一个新业务上线需要经过需求提出、讨论和定义开发商开发标准协议，然后在网络上升级所有的网络设备，经过数年才能完成一个新业务。SDN 使得新业务的上线速度从几年提升到几个月或者更快。

简化网络

- SDN的网络架构简化了网络，消除了很多IETF的协议。协议的去除，意味着学习成本的下降，运行维护成本下降，业务部署速度提升。这个价值主要得益于SDN网络架构下的网络集中控制和转控分离。



- 因为 SDN 网络架构下的网络集中控制，所以被 SDN 控制器所控制的网络内部很多协议基本就不需要了，比如 RSVP 协议、LDP 协议、MBGP 协议、PIM 组播协议等等。原因是

网络内部的路径计算和建立全部在控制器完成，控制器计算出流表，直接下发给转发器就可以了，并不需要协议。未来大量传统的东西向协议会消失，而南北向控制协议比如 Openflow 协议则会不断的演进来满足 SDN 网络架构需求。

网络设备白牌化

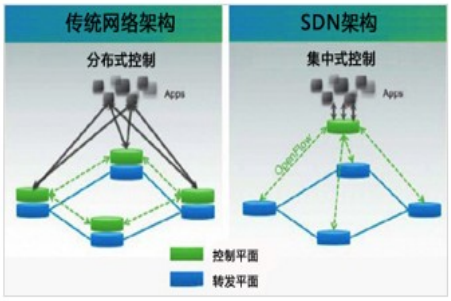
- 基于SDN架构，如果标准化了控制器和转发器之间的接口，比如Openflow协议逐渐成熟，那么网络设备的白牌化将成为可能，比如专门的Openflow转发芯片供应商，控制器厂商等，这也正是所谓的系统从垂直集成开发走向水平集成。

SDN 产业链		
类别	厂商	现状
芯片商	盛科、博通	盛科已经推出支持 OpenFlow 的交换机，并广泛应用于国内科研机构，博通推出 SDN 芯片解决方案
网络设备制造商	思科、华为、爱立信、阿朗	思科开放部分软件，推出针对性 SDN 产品；华为在硬件设备中增加对 OpenFlow 支持
IT 供应商	IBM、HP	推出控制器，支持 OpenFlow
创新公司	Nicira、Big Switch	Nicira 走在最前列，基于 VSwitch 的网络虚拟平台已服务于 AT&T、eBay、Fidelity、RackSpace 等公司

- 垂直集成是一个厂家供应从软件到硬件到服务。水平集成则是把系统水平分工，每个厂家都完成产品的一个部件，有的集成商把他们集成起来销售。水平分工有利于系统各个部分的独立演进和更新，快速进化，促进竞争，促进各个部件的采购价格的下降。

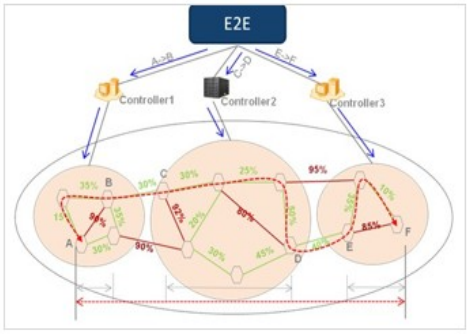
业务自动化

- SDN网络架构下，由于整个网络归属控制器控制，那么网络业务自动化就是理所当然的，不需要另外的系统进行配置分解。在SDN网络架构下，SDN控制器自己可以完成网络业务的部署，提供各种网络服务比如L2VPN、L3VPN等，屏蔽网络内部细节，提供网络业务自动化能力。



网络路径流量优化

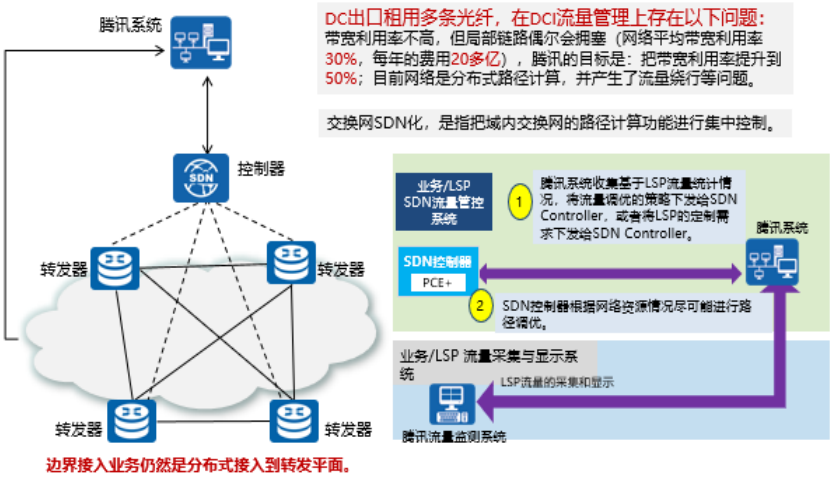
- 通常传统网络的路径选择依据是通过路由协议计算出的“最优”路径，但结果可能会导致“最优”路径上流量拥塞，其它非“最优”路径空闲。当采用SDN网络架构时，SDN 控制器可以根据网络流量状态智能调整流量路径，提升网络利用率。



- 事实上在传统网络中也有一些流量工程技术来解决此类最优路径拥塞问题，比如 MPLS TE 就是一种流量工程技术，但是该技术与其他传统协议一样，都是全分布式的，会导致前面介绍的业务次序依赖问题；另外一个方面传统的流量工程协议 RSVP 因为其软状态机制，导致其无法大规模部署。若采用 SDN 架构，可直接集中对业务路径进行计算和建立隧道，

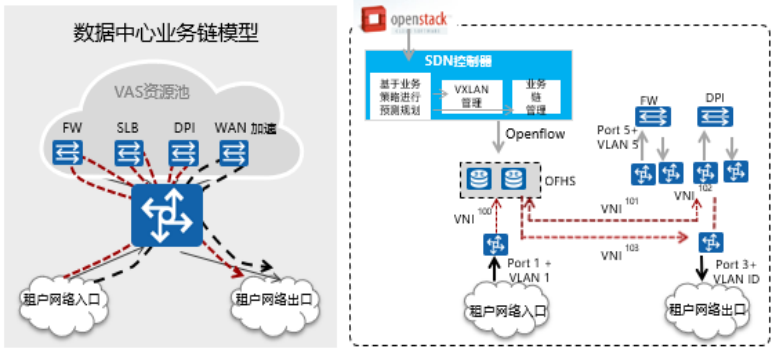
不需要 RSVP 协议，这不仅能够解决实时流量路径动态调整的能力，同时也能够解决业务次序依赖问题。

方式一：仅交换网SDN化



- 交换网 SDN 化是指把域内交换网的路径计算功能进行集中控制。
- 控制器：仅负责域内路径计算和控制。

方式二：仅业务SDN化



- 此方案仅仅将自治域AS所接入的业务由控制器接管，域内路径计算和控制依然由转发器负责。
- 统一部署增值业务VAS资源池，通过SDN Controller业务链解决方案，集中控制管理，同时实现VAS资源共享。
- 提升增值业务快速创新能力，提供新的创收来源。

- 此方案仅仅将自治域 AS 所接入的业务由控制器接管，域

内路径计算和控制依然由转发器负责。

- 1、答案：流量路径的灵活调整能力不足；网络协议实现复杂，运维难度较大；网络新业务升级速度较慢。
- 2、答案：转控分离；集中控制；开放接口。