六、新一代网络技术

软交换、IMS、SDN

北京邮电大学　计算机学院　卞佳丽

本章内容

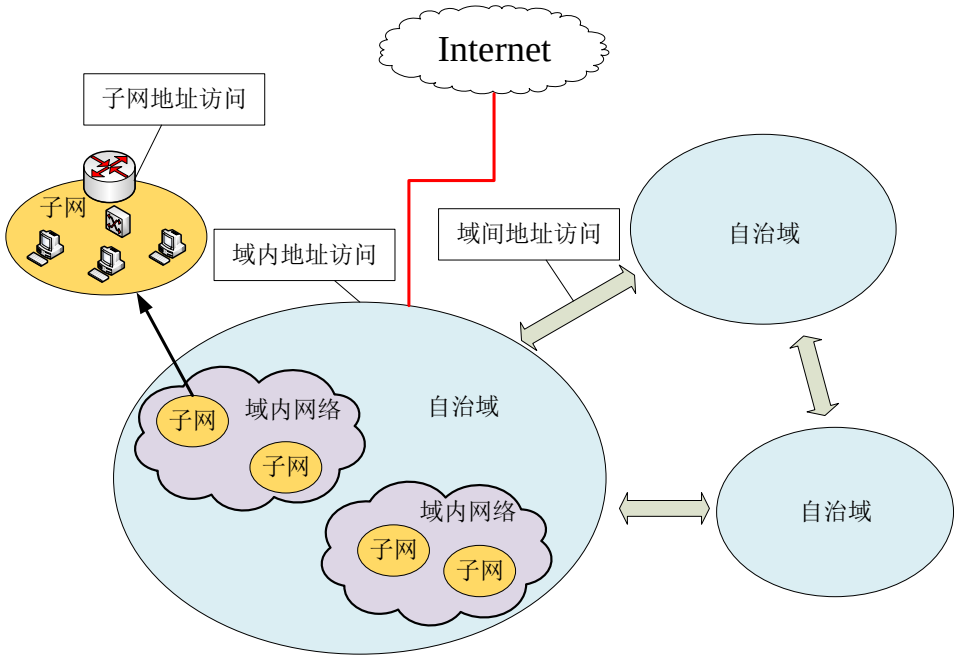
1. 软交换技术
2. IMS技术
3. SDN技术

产生背景

互联网：从小型局域网络—空前庞大复杂的全球级网络

问题：网络规模持续扩张、网络设备不断增加，超出设计承受能力，网络维护变得举步维艰

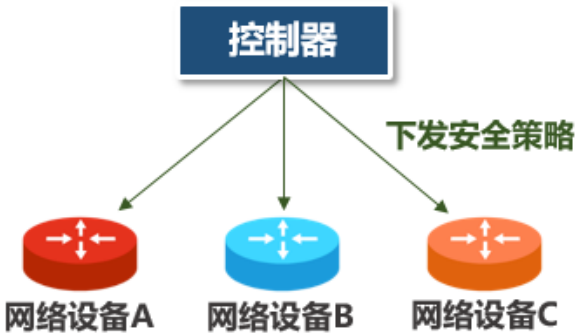
探讨：未来网络的可能性架构



产生背景

2006年，美国斯坦福大学启动了一个名叫Clean Slate的研究课题，目的非常明确且宏大，就是“重塑互联网”。

2007年，斯坦福大学博士生Martin Casado等人提出了关于网络安全与管理项目Ethane。该项目试图通过一个集中式控制器，将安全控制策略下发到各个网络设备中，从而实现对整个网络安全控制。



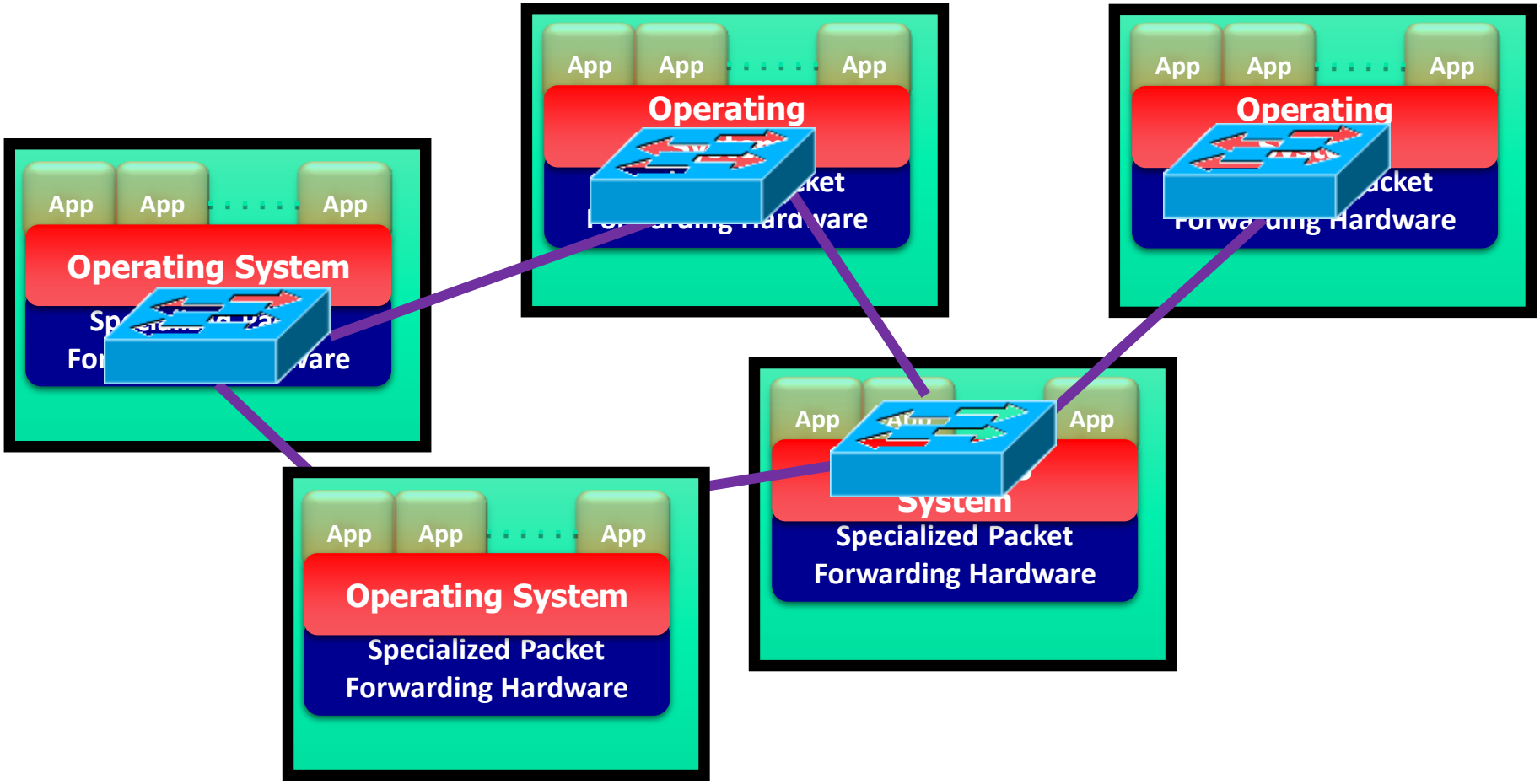
2008年，Clean Slate课题的项目负责人，斯坦福大学教授Nick McKeown及其团队，受到Ethane项目的启发，提出了OpenFlow的概念，并发布了经典文章《OpenFlow：Enabling Innovation in Campus Networks》。


OpenFlow: Enabling Innovation in Campus Networks

产生背景

2009年，基于OpenFlow，Nick Mckeown 教授正式提出了SDN（Software Defined Network，软件定义网络）。同年，SDN概念成功入围Technology Review年度十大前沿技术，获得了行业的广泛关注和重视；12月份，OpenFlow规范的1.0版本正式发布。这是首个可用于商业化产品的版本，具有里程碑意义。

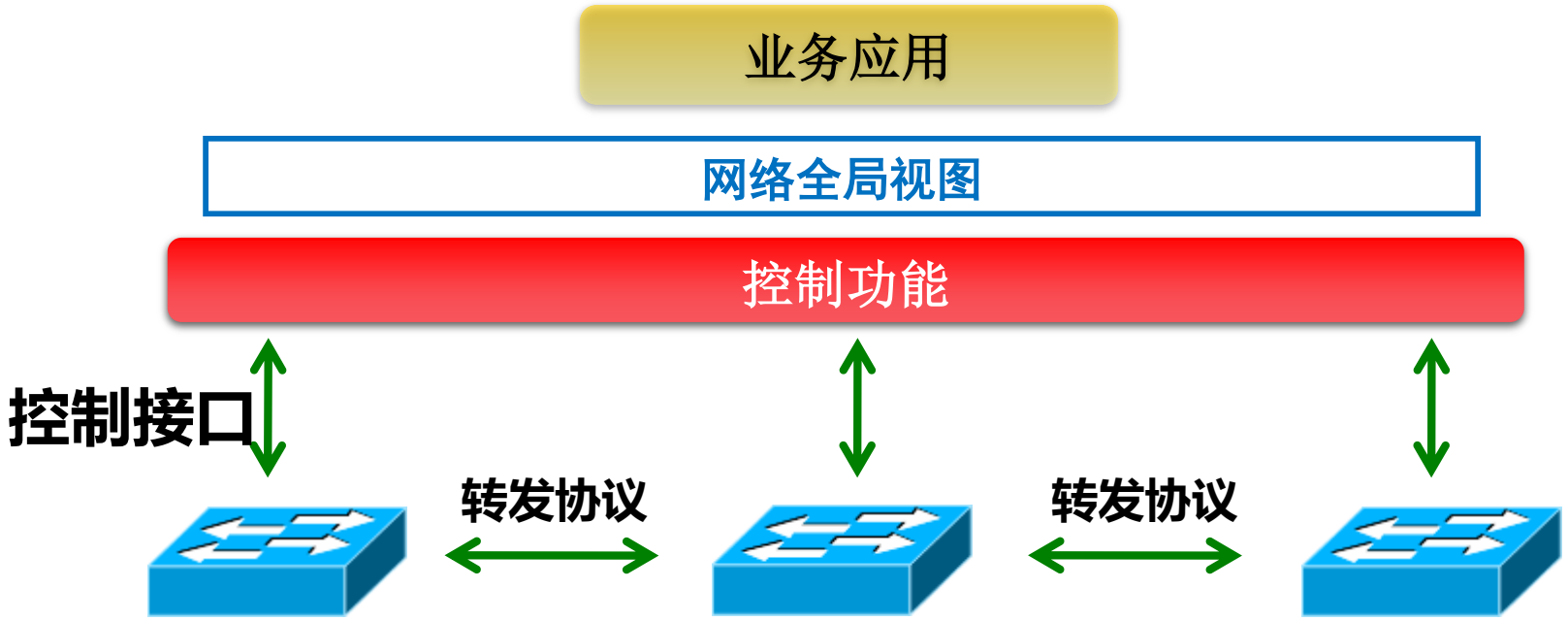
网络设备


App
App
App
Operating System
Specialized Packet Forwarding Hardware
Operating
Specialized Packet Forwarding Hardware

因特网体系结构的问题

- 可扩展性问题
  - 根源：骨干路由器需维护到达任意节点(子网)的路由
  - 现状：不断地增加硬件设备投资来缓解
- 动态性问题
  - 根源：移动IP思想使得协议栈冗余；物联网终端难以完成网络维护
  - 现状：要求中间节点提供维护，违背“端到端原则”，无成功先例
- 安全可控性问题
  - 根源：基于IP地址的点到点通信模式注定只能提供端到端安全通道
  - 现状：目前互联网的安全手段基本处于被动应对状态

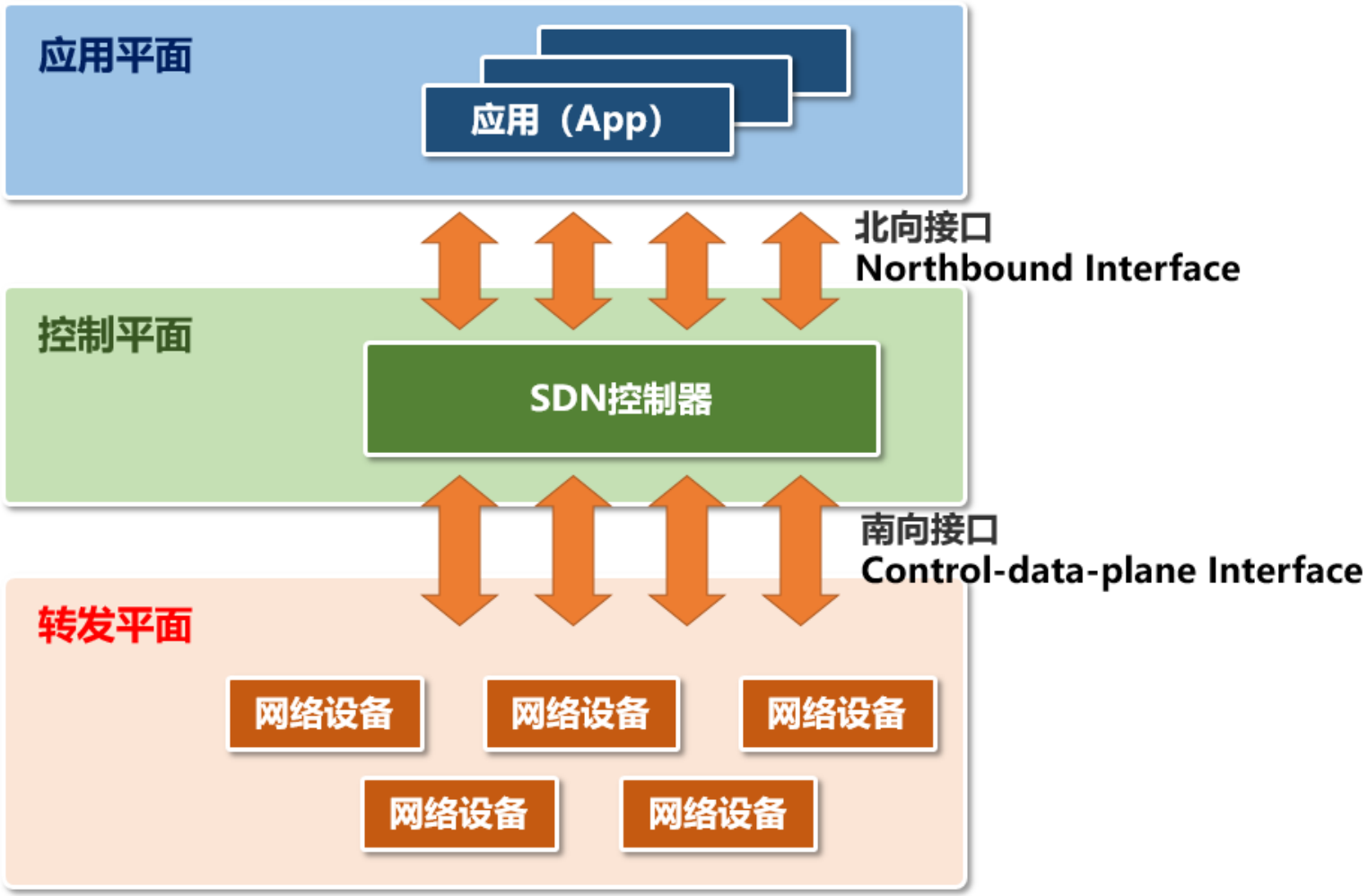
控制与转发分离



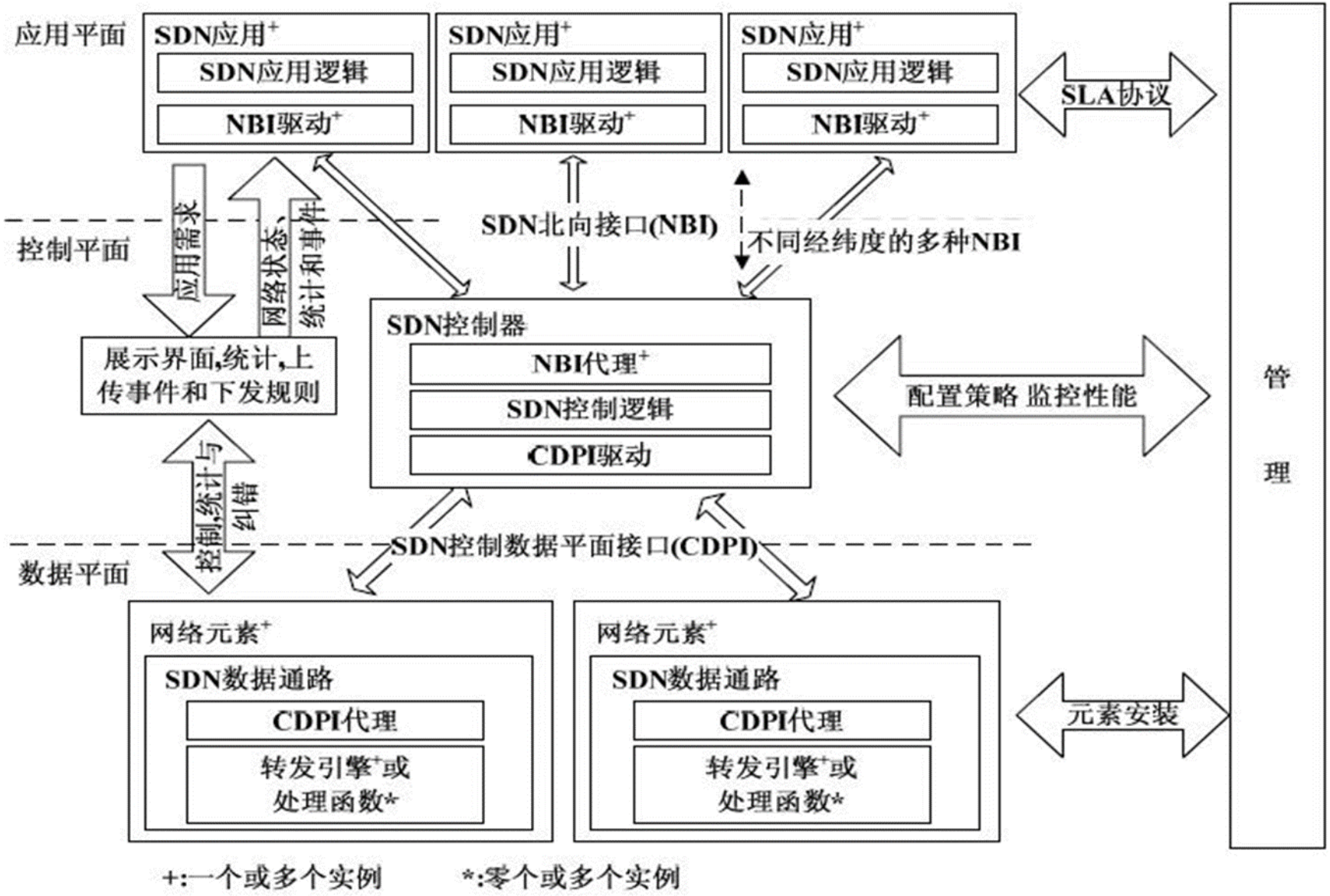
Software-Defined Networking (SDN)

- **SDN是一种新兴的基于软件的网络架构及技术，其最大的特点在于具有松耦合的控制平面与数据平面、支持集中化的网络状态控制、实现底层网络设施对上层应用的透明，上层应用可以通过开放式API对网络进行控制。**
  - **传统网络设备紧耦合的网络架构被分拆成应用、控制、转发三层分离的架构。控制功能被转移到了服务器。**
  - 使得网络的自动化管理和控制能力获得空前提升，能够有效解决当前网络系统所面临的资源规模扩展受限、组网灵活性差、难以快速满足业务需求等问题。

SDN的体系结构


应用平面
应用（App）
北向接口
Northbound Interface
控制平面
SDN控制器
南向接口
Control-data-plane Interface
转发平面
网络设备
网络设备
网络设备
网络设备
网络设备

SDN的体系结构

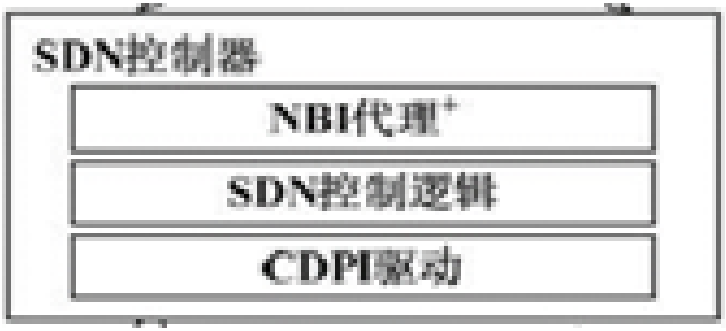

应用平面
SDN应用+
SDN应用逻辑
NBI驱动+
SDN应用+
SDN应用逻辑
NBI驱动+
SDN应用+
SDN应用逻辑
NBI驱动+
SLA协议
管理
控制平面
应用需求
网络状态、统计和事件
SDN北向接口(NBI)
不同经纬度的多种NBI
展示界面,统计,上传事件和下发规则
SDN控制器
NBI代理+
SDN控制逻辑
CDPI驱动
配置策略 监控性能
控制,统计与纠错
SDN控制数据平面接口(CDPI)
数据平面
网络元素+
SDN数据通路
CDPI代理
转发引擎+或处理函数*
网络元素+
SDN数据通路
CDPI代理
转发引擎+或处理函数*
元素安装
+:一个或多个实例
*:零个或多个实例

应用平面

- 各类基于SDN的网络应用，通过开放式API完成对网络的控制
- NBI允许第三方开发个人网络管理软件和应用
- 网络抽象特性允许用户可以根据需求选择不同的网络操作系统，而不影响物理设备的正常运行

控制平面

- SDN控制逻辑：负责运行控制逻辑策略，维护着全网视图
- CDPI驱动：控制器将全网视图抽象成网络服务，通过访问CDPI代理将转发规则从网络操作系统发送到网络设备，而不影响控制层及以上的逻辑
  - 链路发现、拓扑管理、策略制定、表项下发
- NBI代理：为第三方等提供易用的NBI，方便这些人员订制私有化应用,实现对网络的逻辑管理。

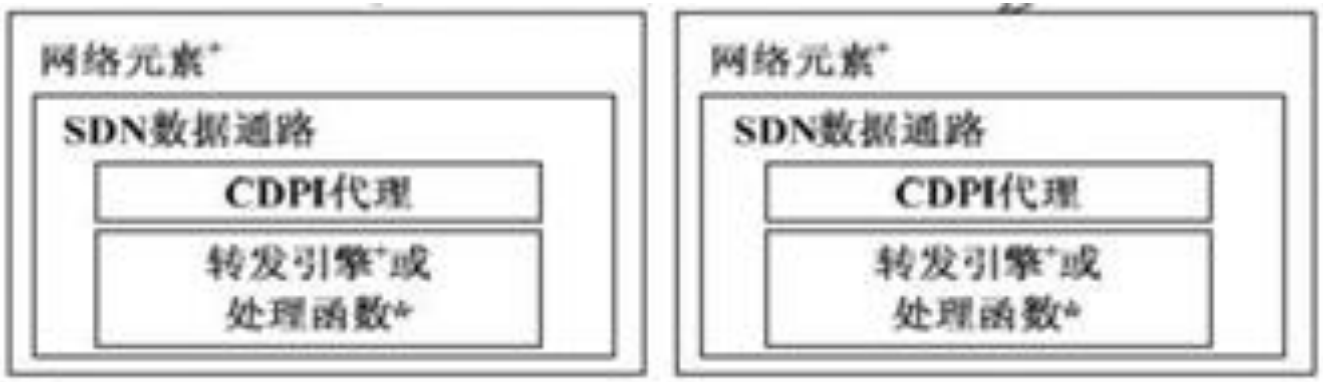


SDN控制器

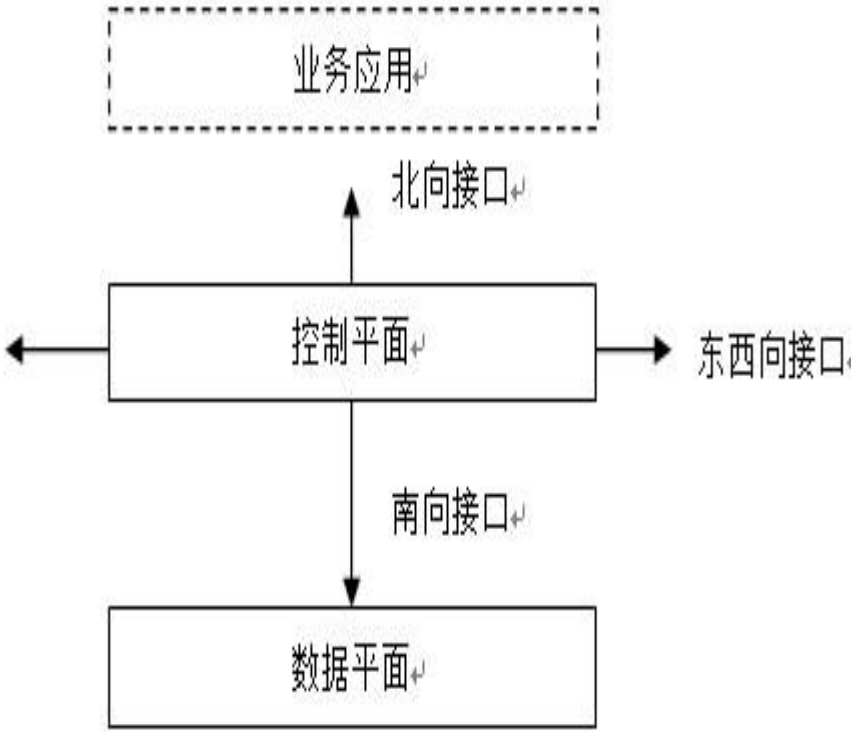
- 商用级产品的厂商
  - Virtual Application Networks SDN Controller（惠普）
  - Application Policy Infrastructure Controller（思科）
  - Smart OpenFlow Controller（华为）
  - NorthStar and OpenContrail（Juniper）
- 开源的控制器
  - NOXRepo的NOX和POX（原始版本）
  - ON.Lab的 SDN Open Network Operating System (ONOS)
  - OpenContrail的OpenContrail Controller
  - 斯坦福大学的Beacon和Trema。

转发（数据）平面

- 数据平面：
  - 转发数据包
  - 各网络元素之间由不同规则形成的SDN网络数据通路形成连接
  - 可以忽略控制逻辑的实现，全力关注基于表项的数据处理
  - 数据处理的性能是评价SDN交换机优劣的最关键指标，很多高性能转发技术被提出



SDN中的接口



北向接口：提供给其他厂家或运营商进行接入和管理的接口，即向上提供的接口。

南向接口：管理其他厂家网管或设备的接口，即向下提供的接口。

东西向接口：
SDN设备之间的接口，多个设备的控制平面之间如何协同工作。

北向接口技术

- 目标：通过控制器向上层业务应用**开放**的**接口**，使得业务应用能够便利地调用底层的网络资源和能力。
- 特征：直接为业务应用服务的，因此其设计需要密切联系业务应用需求，具有多样化的特征。
- 重要性：设计是否合理、便捷，以便能被业务应用广泛调用，会直接影响到SDN控制器厂商的市场前景。
- 功能
  - 网络业务的开发者能**以软件编程的形式调用各种网络资源**；
  - 上层的网络资源管理系统可以通过控制器的北向接口全局把控整个网网络的资源状态，并对资源进行统一调度。

北向接口技术

- 协议制定
  - 与南向接口方面已有OpenFlow等国际标准不同，**北向接口方面还缺少业界公认的标准**，不同的参与者或者从用户角度出发，或者从运营角度出发，或者从产品能力角度出发提出了很多方案。
- 网络设备厂商应对办法
  - 在其现有设备上提供了编程接口供业务应用直接调用，也可被视作是北向接口之 一，其目的是在不改变其现有设备架构的条件下提升配置管理灵活性，应对开放协议的竞争。
- 衡量北向接口的标准
  - 开放性
  - 便捷性
  - 灵活性

南向接口：OpenFlow

OpenFlow最初是Clean Slate计划中提出的一种用于在校园网上创建可进行网络研究实验新型网络的交换模型。该模型中使用的协议被称作OpenFlow。

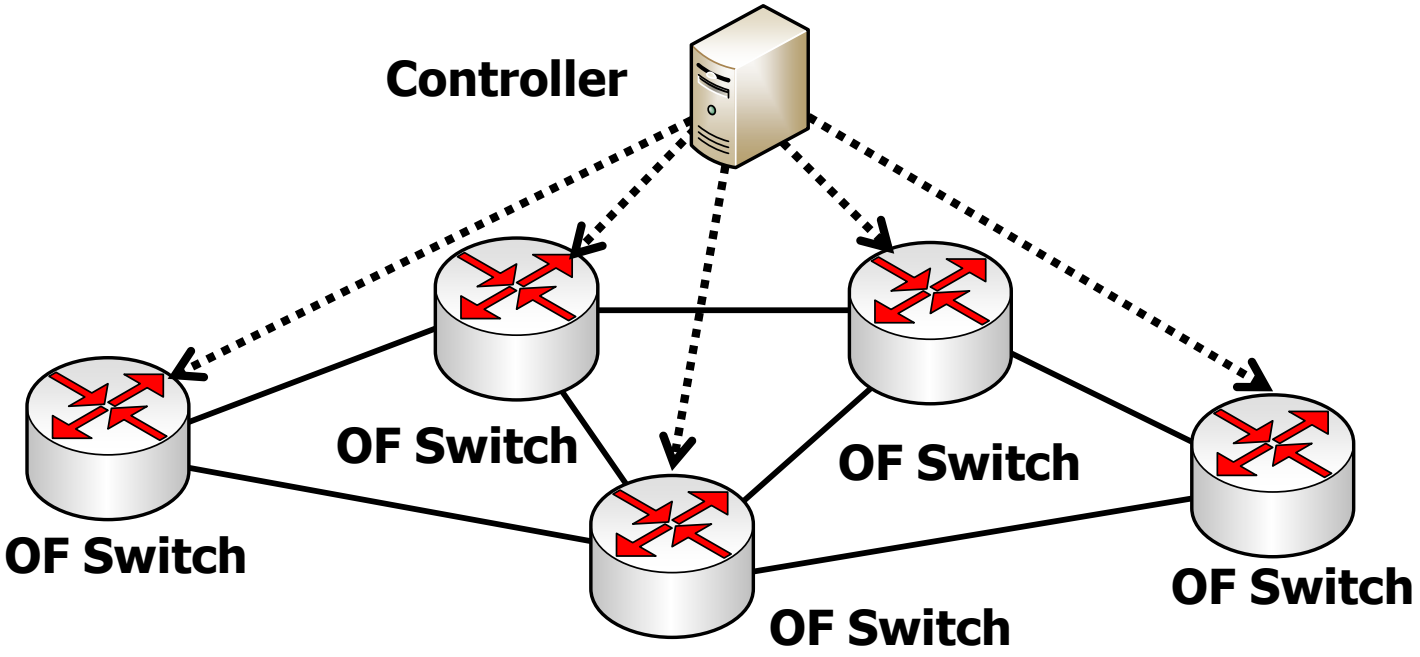
OpenFlow的核心思想是控制与转发分离，SDN的概念正是在它的基础上提出。

现在，OpenFlow更多指的是由ONF维护的《OpenFlow交换机规范》中描述的协议标准。它被视作SDN体系架构中的事实上的南向接口标准。

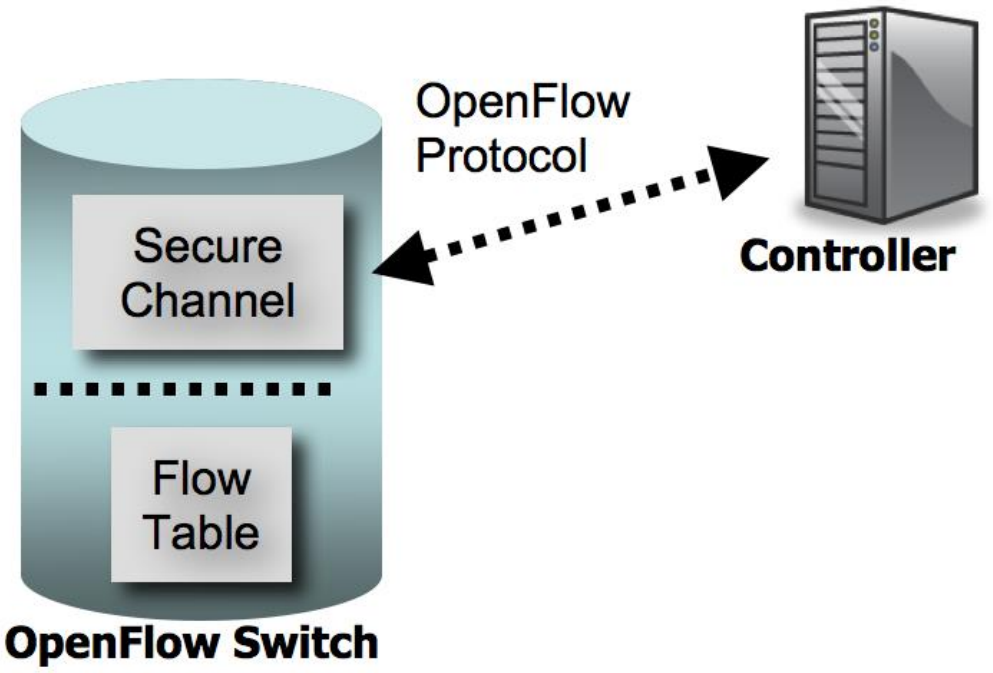
OpenFlow交换机

传统的网络设备（交换机、路由器、防火墙等）的控制逻辑和转发逻辑是紧密耦合在一起的。

OpenFlow交换机只包含转发功能，将控制逻辑从中解耦出来，放在控制器中实现。如此，OF交换机只需要按照流表的规则（由控制器下发）转发数据包，而控制器可以同时控制多台OF交换机。



OpenFlow交换机规范v1.0.0



规范中的图例： 在安全通道上使用OpenFlow协议与控制器通信的OpenFlow交换机

OpenFlow交换机由流表、安全通道、OpenFlow协议三个部分组成

安全通道

安全通道（Secure Channel）是连接交换机与控制器的接口。 通过这个接口，控制器可以配置、管理交换机，接收来自交换机的事件和发送数据包给交换机。

控制器与交换机除了通过TCP建立明文连接，也可以通过TLS(Transport Layer Security)建立加密连接，确保消息的机密性和完整性，这对集中控制的SDN网络的安全性有着至关重要的作用。

流表

流(Flow)：指的是在一段时间内，经过同一个网络的一系列具有相同属性的顺序发送的报文集合。

流表(Flow Table)：简单说就是一张转发表，由若干条流表项组成。

流表项(Flow Entry)：是流表的最小单位，每条流表项对应网络传输的一条流。根据OpenFlow规范，每条流表项的组成部分如下：

Header Fields	Counters	Actions

OpenFlow交换机中可以有多个流表，每个流表可包含多个流表项

流表项

Header Fields	Counters	Actions

头字段：包含了用于匹配流（数据包）的字段信息，涵盖了L2-L4的各类协议信息。

Ingress Port	Ether source	Ether dst	Ether type	VLAN id	VLAN pri-or-ity	IP src	IP dst	IP proto	IP ToS bits	TCP/ UDP src port	TCP/ UDP dst port

Table 2: Fields from packets used to match against flow entries.

计数器：用于统计所匹配流的各种信息，如包数、字节数。

动作：描述了对所匹配的数据包需要采取的操作。

匹配域

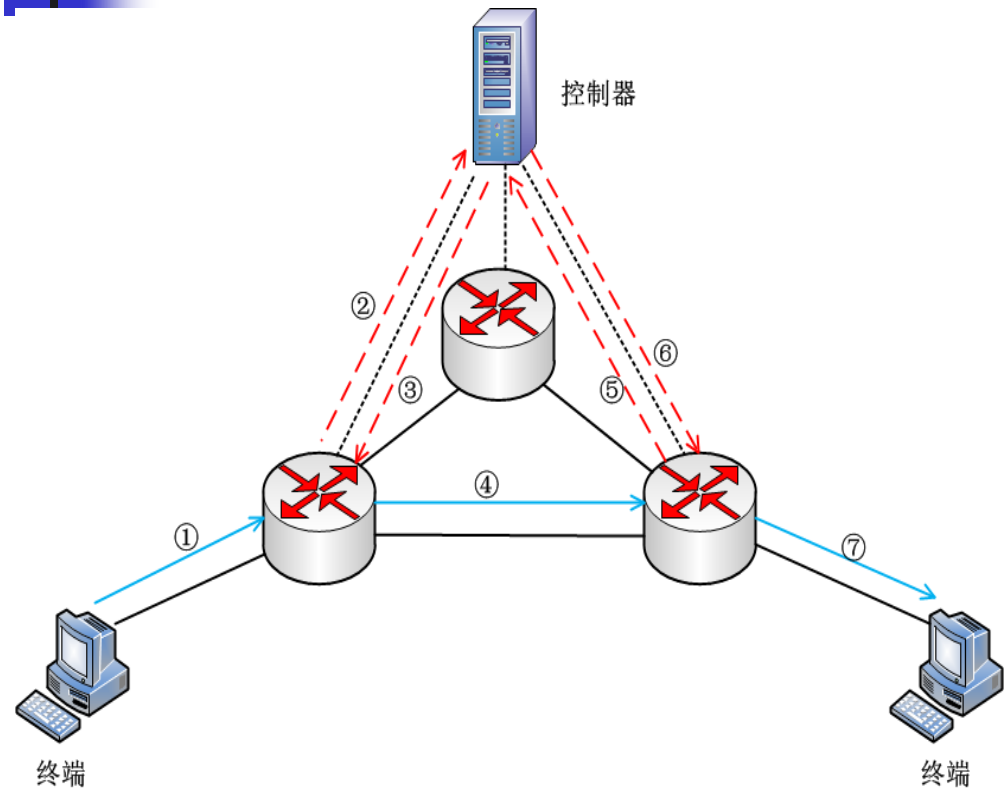
字段	说明
Ingress Port	输入端口
Ethernet Source Address	以太网帧的发送源以太网地址
Ethernet Destination	以太网帧的目标以太网地址
Ether Type	以太网帧的类型字段
VLAN ID	VLAN标签的VLAN ID
VLAN Priority	802.1Q的PCP(Priority Code Point)
IP Source Address	IPv4头中的发送源地址（可指定子网掩码）
IP Destination Address	IPv4头中的目标地址（可指定子网掩码）
IP Protocol	IPv4头的协议字段
ToS	IPv4头的ToS字段
TCP/UDP Source Port or ICMP Type	TCP/UDP头的源端口号，或ICMP头的类型
TCP/UDP Source Port or ICMP Code	TCP/UDP头的目的端口号，或ICMP头的代码

动作

规范中定义了4种动作：

- Forward：将数据包转发到指定端口
- Drop：丢弃数据包
- Enqueue（可选）：将数据包发送至队列，用于QoS控制
- Modifiy-Field（可选）：修改数据包的协议字段

Openflow工作流程



①终端向网络发送数据包

②OpenFlow交换机流表无匹配项，通过PacketIn事件将数据包上报给控制器

③控制器下发流表给交换机(或PacketOut)

④交换机之间数据包转发

⑤ OpenFlow交换机流表无匹配项，通过PacketIn事件将数据包上报给控制器

⑥控制器下发流表给交换机(或PacketOut)

⑦交换机将数据包转发给终端

Packet-out: 控制器用该消息类型向外发送匹配某条流表项的数据报文

Packet-in: 交换机向控制器发送未匹配或转发到控制器端口的报文

SDN 技术对网络架构的变革

- 打破了原有的网络层次
  - 提供跨域、 跨层的网络实时控制
  - 打破原有的网络分层、分域的部署限制
- 改变了现有网络的功能分布
  - 网络业务功能点的部署将更加灵活
  - 简化承载网络的功能分布
- 分层解耦为未来网络的开放可编程提供了更大的想象空间

SDN技术带来的新机遇

- 提高网络资源利用率
  - 独立出一个相对统一集中的网络控制平面，更有效地基于全局的网络视图进行网络规划，实施控制和管理
- 促进云计算业务发展
  - 网络虚拟化
- 提升端到端业务体验
  - 更好地端到端的业务保障
  - 增强网络业务承载能力
- 降低网元设备的复杂度
  - 设备硬件更趋于通用化和简单化