centec networks

深入浅出SDN




Topic

SDN: What? Why? How?

OpenFlow的价值与局限

SDN在云计算中的应用

SDN对产业格局的影响

传统网络架构已经不适应新的业务需求

centec networks

管理员们抱怨……

centec networks

太多的手动操作

网络变更很困难

网络操作需要跟其他IT操作的集成与协作

由于忙于维护很难快速部署新业务

部署网络设备很麻烦

使用原始的工具来手动管理IP地址

太多的工具了

由于跟其他IT团队缺乏合作，难以应用新技术

网络必须进行变革以适应新的需求

于是，SDN诞生了……

From CleanSlate to Openflow to SDN

centec networks

MIT Technology Review

10 BREAKTHROUGH TECHNOLOGIES 2009

TR10: Software-Defined Networking

Nick McKeown believes that remotely controlling network hardware with software can bring the Internet up to speed.

SDN是一种思想

SDN不是一种具体的技术，而是一种思想，一种理念

SDN的核心诉求：让软件应用参与到网络控制中并起到主导作用，而不是让而各种固定模式的协议来控制网络

为了满足这种核心诉求，SDN思想指导下的网络必须设计一种新的架构

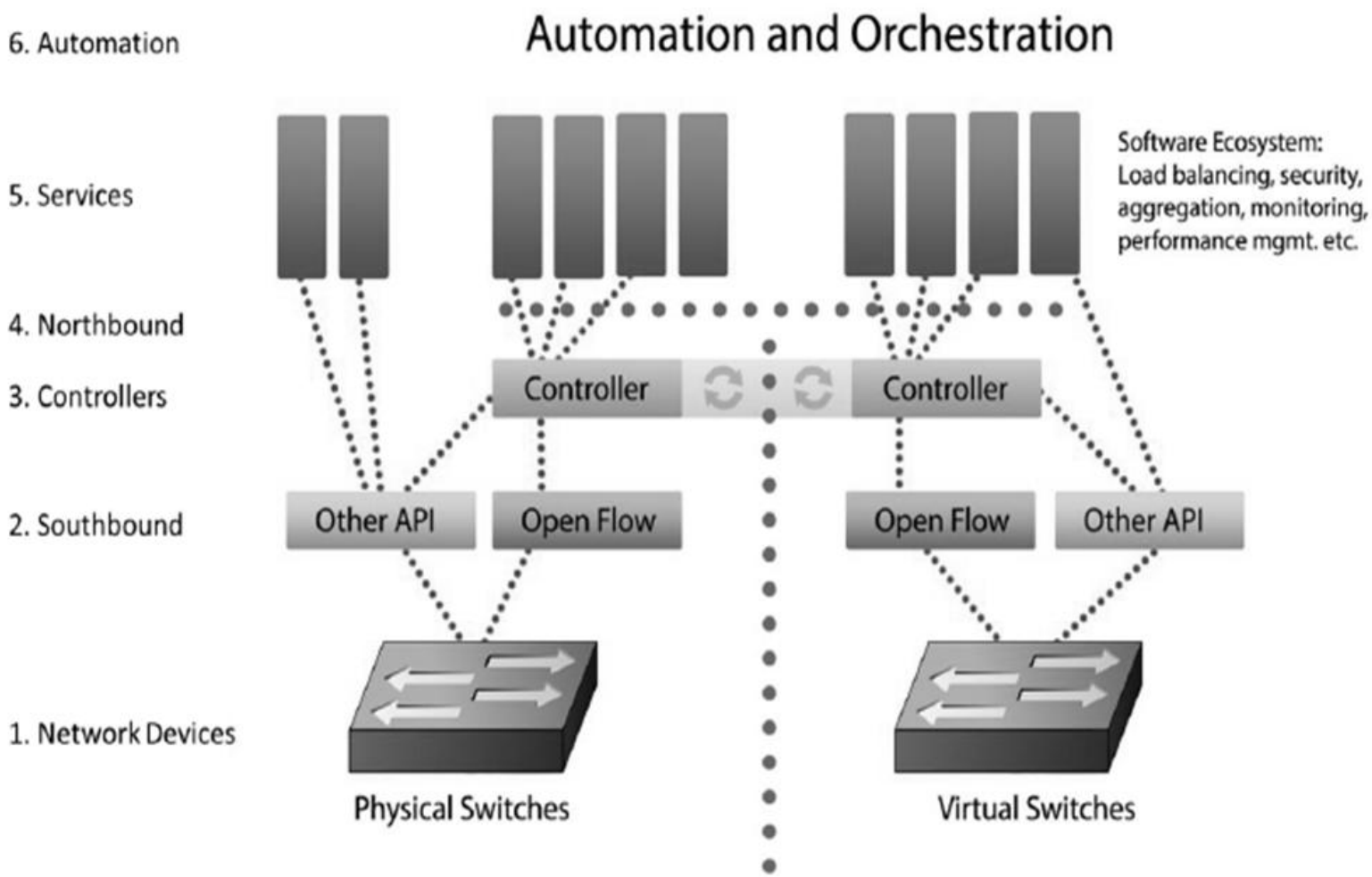
SDN思想是新的吗？No!

- 之前的不同领域的一些技术，其实已经提出了类似的思想
  - 传送网的承载与控制分离
  - IETF的一个RFC: ForCES (Forwarding and Control Element Seperation)

- **But so what? MPLS的理念中有很多ATM的设计思想，但并不妨碍MPLS被推广**

- **SDN明显更通用化，更有价值**

SDN思想下的新架构：控制与转发分离



SDN架构的本质属性

其它属性都跟SDN本质无关

- SDN不意味着硬件转发行为标准化
- SDN不意味着硬件编程接口标准化
- SDN不意味着控制面和转发面必须物理上分离
- SDN不意味着必须用Openflow
- SDN不意味着必须开源
- SDN不意味着必须使用特定的SDN硬件

三种SDN定义

centec networks

狭义SDN	• OpenFlow
广义SDN	• （管理+控制）与转发分离
超广义SDN	• 管理与（控制+转发）分离

不光白猫黑猫，能抓住耗子的就是好猫

centec networks

- 广义SDN是最有价值，最广为接受的一种
- 然而SDN具体定义并不重要
- 重要的是基于SDN所能带来的自动化部署的价值
- 企业不需要选择最符合标准定义的SDN，只需要选择对自己最有价值的SDN

不拘一格的SDN

- Openflow是SDN
- OpenDayLight是SDN
- OpenContrail是SDN
- OpenStack是SDN
- Cisco ACI是SDN
- 各种网络虚拟化技术都是SDN
- 阿里巴巴的SDN?

SDN的制高点

centec networks

Controller
很重要

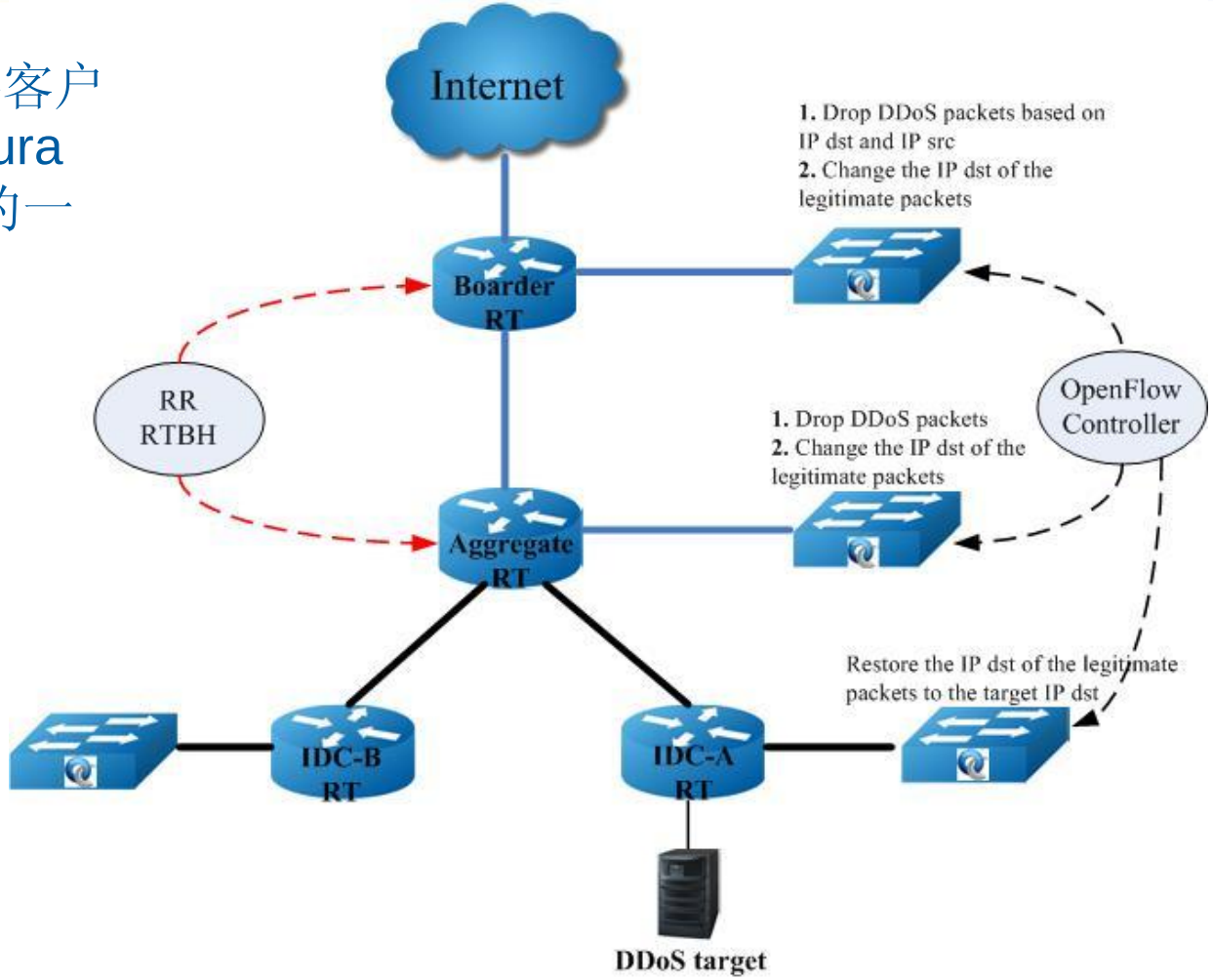
- OpenDayLight
- Ryu
- FloodLight
- OpenStack

北向接口
很重要

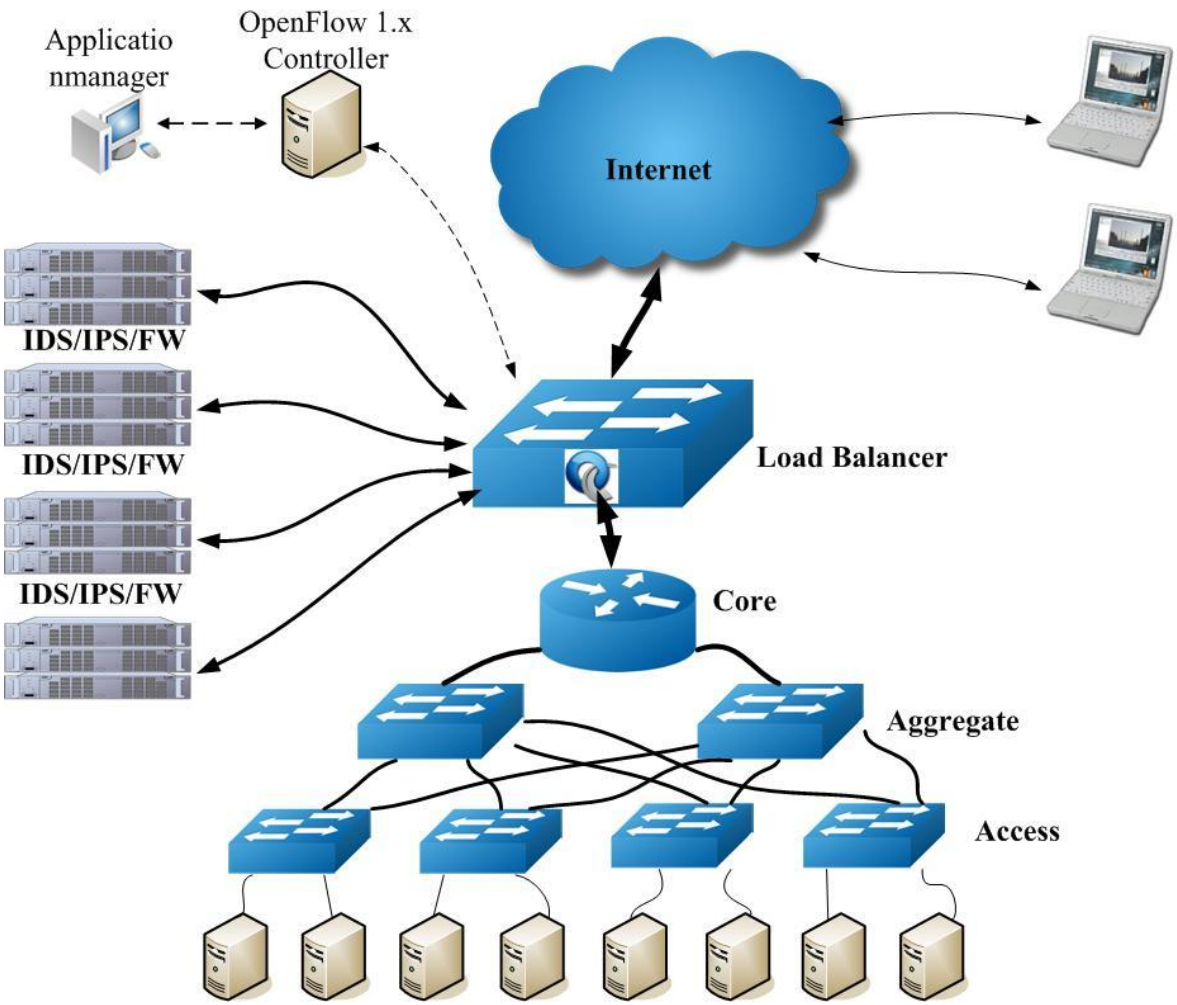
- Example. SuperPTN
- Example. Neutron

SDN案例1：SDN Based DDoS Prevention

这是盛科客户日本Sakura Internet的一个案例



SDN案例2：Security Load Balancer



这是盛科交换机在安全领域应用的一个案例

更多案例

- **某企业的带宽管理和流量调度**
  - 盛科在某个大企业的案例，类似于Google B4
- **某广电的视频流控制**
  - 盛科在某广电客户的案例，用于视频源的控制和地址规划
- **某企业的内部办公系统一体化管理**
  - 仍处于概念验证阶段的一个案例
  - 使用SDN将企业网里面各种资源整合在一起，在一个界面上配置一个新员工的所有身份识别信息（需要配置在接入交换机，AP等设备上）

SDN的核心价值

不在于能够解决传统网络解决不了的问题

而在于能够比传统网络做得更快捷，更可靠，更省力

对SDN的一些错误印象

- 貌似谈论SDN的时候，潜意识都是在谈OpenFlow?
- 貌似谈论SDN的时候，谈的都是硬件SDN设备？
- 貌似谈论SDN的时候，谈的都是交换机？
- 貌似行业报告里面，说SDN市场越来越大？真的有那么多SDN交换机在卖？

Topic

centec networks

SDN：What？Why？How？

OpenFlow的价值与局限

SDN在云计算中的应用

SDN对产业格局的影响

OpenFlow的价值、挑战和未来

centec networks

价值

- 统一编程接口
- 解除厂商锁定
- 给上层控制足够的灵活性

挑战

- 标准不够完善，只能覆盖当前众多应用场景的子集
- 转发面的工作进展缓慢
- 标准组织ONF的市场影响力和技术背景都太弱
- 牵涉到太多利益关系，传统厂商不买账

未来

- 成为众多南向接口中的一个，但是是唯一标准化的
- 在部分场景中可以独立组网
- 更多场景中跟其它技术相结合
- 不太可能取代其它技术

SDN专用芯片？

centec networks

NP架构 vs Switch 变革 vs Switch革命？

$20M/两年/变化的标准/不确定的市场?

芯片厂商该何去何从？

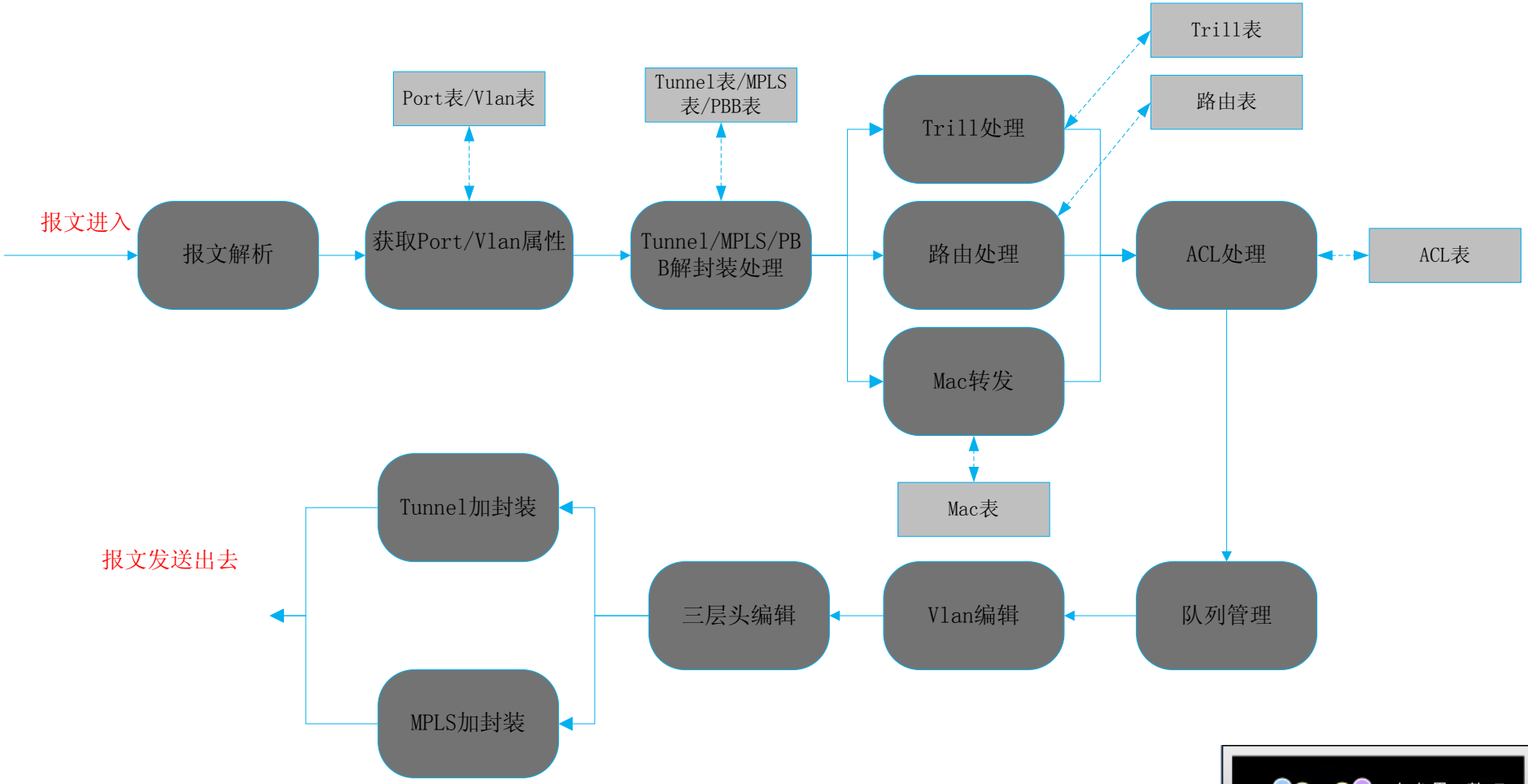
ASIC现状

- Openflow是想让报文解析、报文查找，逻辑处理全部标准化，用一种通用的灵活的模式，类似于搭积木
- 现有的ASIC架构，报文解析、报文查找、逻辑处理都有严格的模式，无法满足需求
- 流表只能使用TCAM来做，TCAM占用芯片面积大，功耗大。若内置，则流表数量很小，通常不到4K。若外扩，成本和功耗都很大，无法规模商用

现有ASIC架构

centec networks

- 各个厂家ASIC流程大同小异



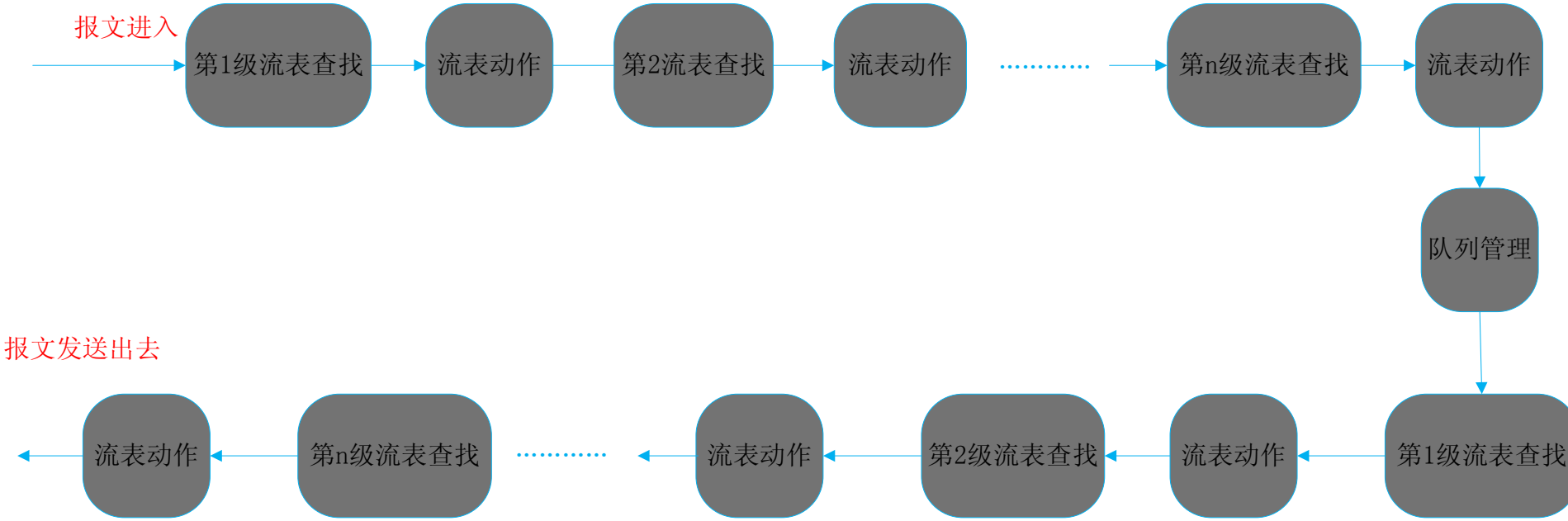
理想化的ASIC流程

- 无论报文解析，报文查找，报文编辑都是可编程的
- 可以解析任何的报文类型，已知或者未知的
- 可以有多级流表，每级流表可以匹配任意字段组合，所有流表共享memory，可灵活分配
- 可以在每级流表出任意动作组合，编辑任意字段

理想化的ASIC架构

centec networks

- 这是Nick Mckeown教授所阐述的理想模型



ONF的过渡方案：TTP

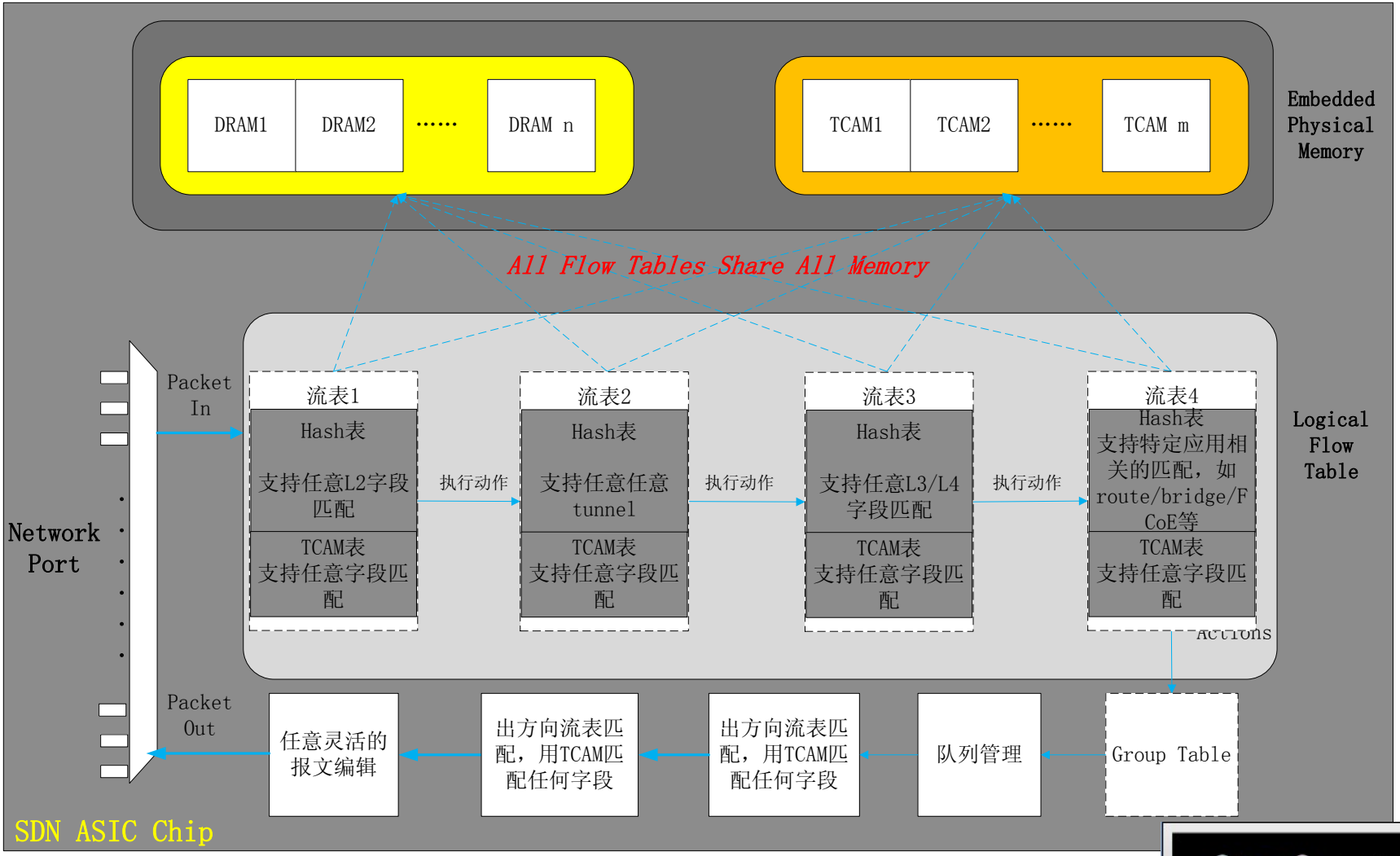
- TTP (Table Typing Pattern)，现在又名NDM(Negotiable Data-plane Model)
- 基于传统芯片架构，包装出Openflow编程接口
- 允许厂商在NDM的框架下自定义转发模型，并公开注册到ONF，交换机和Controller遵循同样的接口
- 支持Openflow function子集

盛科创新的折衷方案

- 基于现有芯片架构，进行优化创新
- 使用Nick教授类似的思路，而适当折衷使之可实现
- 流表之间共享内存、适当数量的多级流表、灵活的字段编辑（比如可以修改IP/Port）、适当灵活的报文解析
- 通过创新的TCAM+HASH并使参与HASH字段可被灵活Mask掉的方式，用极低的成本支持业界最大数量的（32K）的流表

盛科创新的SDN芯片架构

centec networks



Note: All the stages in dotted line box can be bypassed

Topic

SDN: What? Why? How?

OpenFlow的价值与局限

SDN在云计算中的应用

SDN对产业格局的影响

centec networks

不管你是否意识到，
大多数的IaaS云计算平台
其实已经在应用SDN！！！

IaaS云计算网络将SDN的优势发挥到极致

centec networks

- **IaaS云计算平台是标准的SDN架构**
  - 控制（云计算控制平台）与转发（虚拟或者物理交换机）
  - 开放的编程接口（南向和北向都是开放的接口）
  - 集中化控制（云平台集中控制所有的设备）
- **没有可编程API（南向和北向），就无法提供租户的self-service，无法自动化部署业务**
- **没有集中化控制，云计算平台要获取全局的信息就很困难，VM的迁移就很困难**
- **无论是虚拟交换机还是物理交换机，都可以是SDN**

OpenStack网络架构

centec networks

OpenStack		
Horizon	Nova	Scripts

北向接口

Neutron API			
OVS Plugin	Linux Bridge Plugin	Openflow Controller Plugin	Others

南向接口

Switch			
OVS	Linux Bridge	Openflow Switch	Others

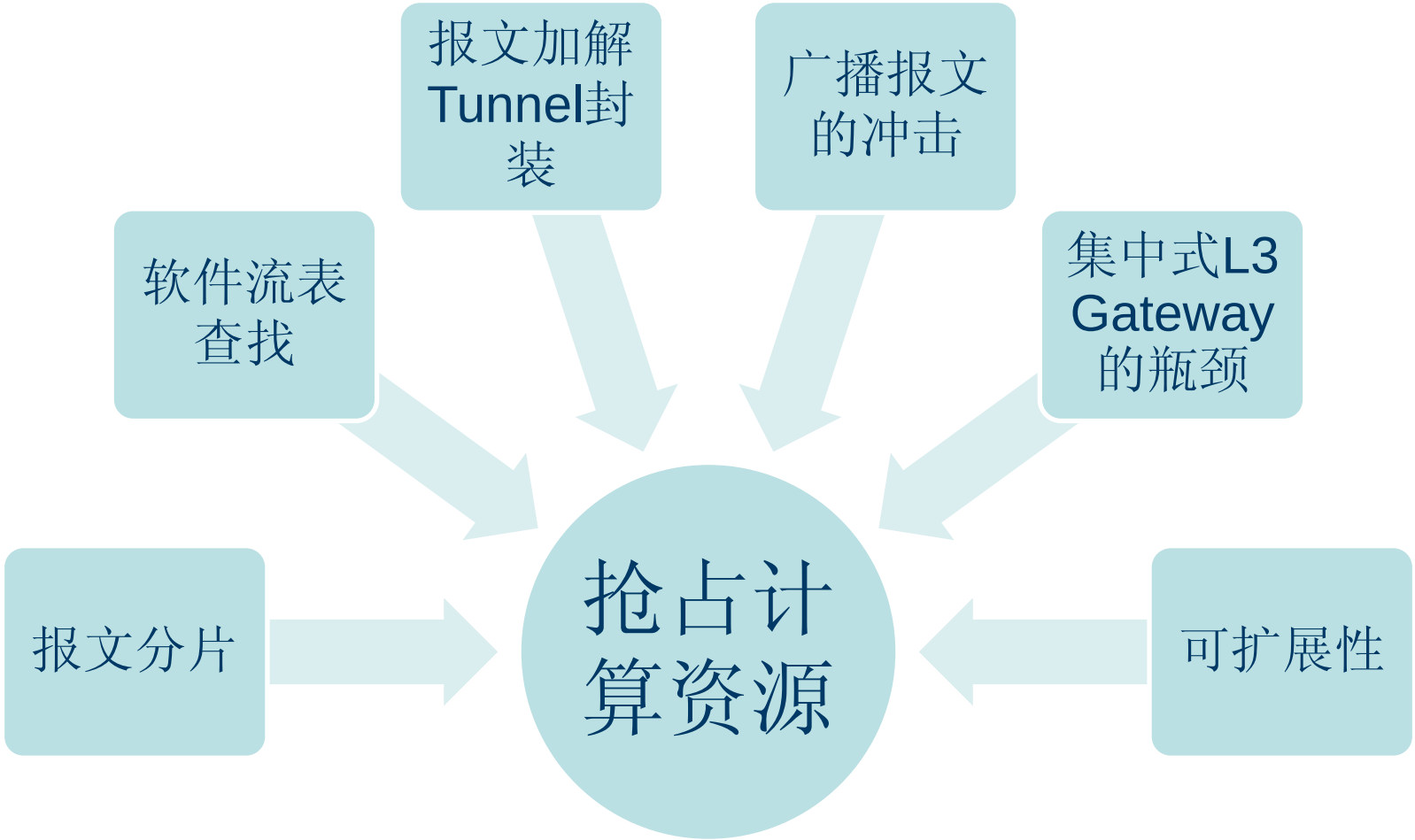
Existed Neutron Plugin

BigSwitch	Cisco	Embrace	Nec
OVS	Ryu	Brocade	hyperV
Linuxbridge	Midonet	Mellanox	Nicira
Plumgrid	Ml2	Centec(will be available soon)	

纯软件的Tunnel Overlay方案

- 是一种标准的SDN实现
- 是当前IaaS云计算方案的主流
  - Vmware NSX, Nuage VSP, Midokura MidoNet等
  - 没有硬件方案可以完整支持所有需要的功能
- 但纯软件方案也有不足
  - 网络可视性差
  - 有不同程度的性能问题

软件方案网络性能方面的挑战



盛科，专注于SDN云计算解决方案

centec networks

没有传统设备商的包袱，对SDN和云计算反应敏捷

是国内领先的SDN方案和产品提供商

有成功的商业案例

是国内唯一的SDN ASIC交换芯片提供商

靠谱的云计算解决方案提供商

目前专注于用SDN方案解决网络问题

盛科方案总体思路

centec networks

取其精华

- 认可网络边缘到Server的理念
- 保持vSwitch的灵活性
- 实现所有AWS VPC所能实现的网络服务模型

弃其糟粕

- 将纯软件方案中的薄弱环节Offload到硬件
- 但是仍然保持系统团队对虚拟网络的控制

不引入新问题

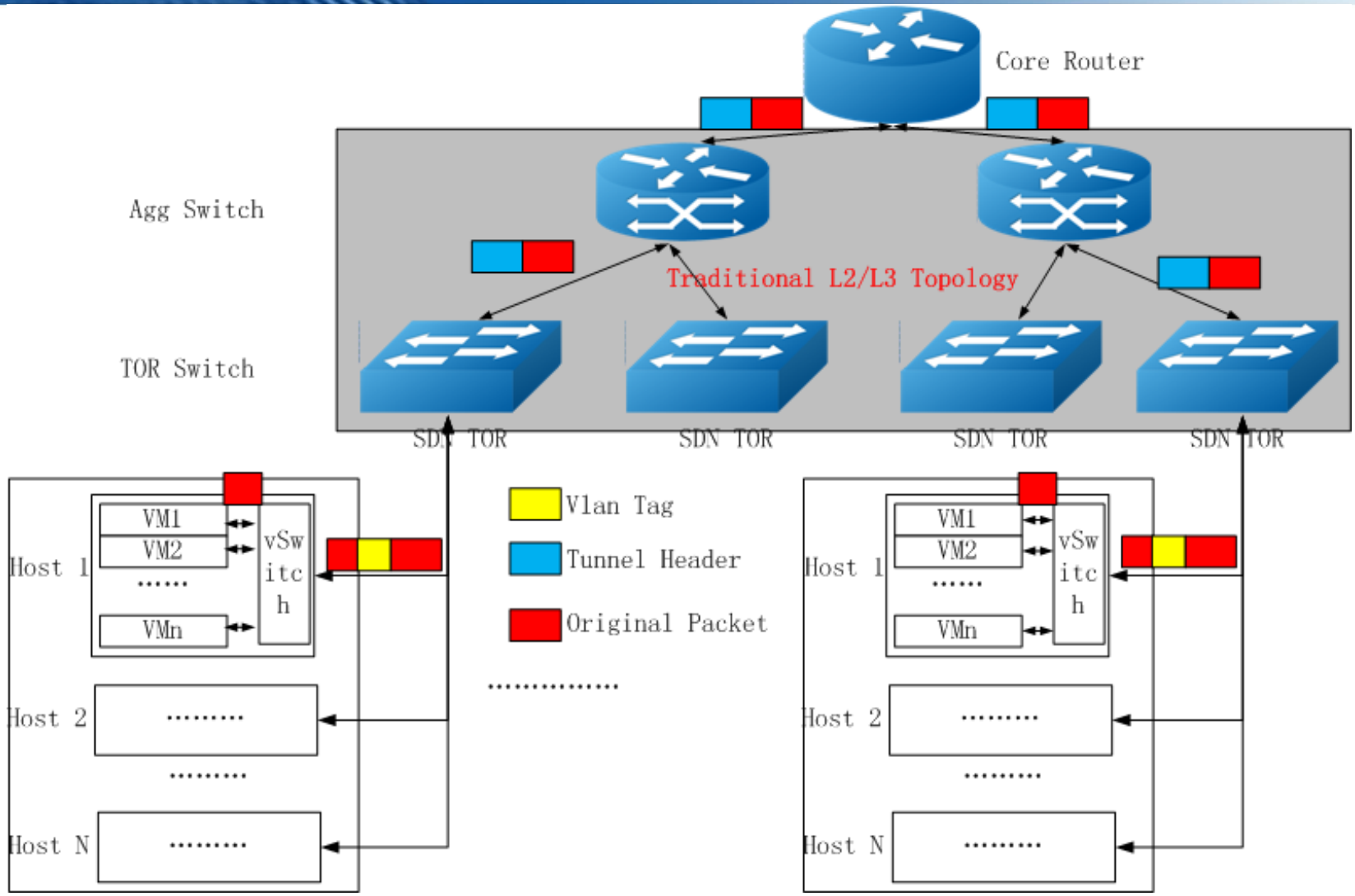
- 不能让用户有厂商锁定的风险
- 要能跟用户现有的网络无缝对接
- 不能让用户增加成本

所参照的AWS VPC网络服务模型

centec networks

- 盛科的方案使用软件+硬件SDN混合方式实现AWS VPC所有的功能
- AWS VPC网络服务模型功能列表
  - 租户隔离
  - 租户所有的VM/Physical Switch属于同一个虚拟网络
  - 同一个租户内可划分子网
  - 为租户提供访问Internet服务
  - 为租户使用floating IP提供NAT服务
  - 为租户提供DHCP服务
  - 为租户提供防火墙服务
  - 为租户提供QoS服务
  - 为租户提供统计服务
  - 为租户提供网络冗余备份
  - 允许租户虚机迁移
  - 提供用户远程VPN接入

盛科方案总体架构



盛科方案对SDN多级流表的应用

Table ID	功能	匹配字段	执行动作
0	识别VM; 识别Tenant; 识别tunnel; 基于VM/Tenant的统计，做QoS	Vlan or Source mac or Logical Tunnel Port	Write metadata (tenantId); Strip Tunnel header; Go To Table 1; Meter; Counter;
1	对VM或者subnet或者tenant应用策略（安全过滤或者QoS）	任意L2-L4字段，另外还包括metadata(租户ID)	Meter; Counter; Discard; Go to Table 2
2	对报文进行查表转发	Dest IP + metadata; Dest Mac + metadata;	Output to physical port; Output to logical port(tunnel); Replace L2 header, then Output to physical port;（route case）

该方案具体做了什么？

- 提供了一个完整的Plugin，可以方便地集成到OpenStack，也可以作为参考跟别的云平台集成
- 使用分布式流表查找方案，将大部分流表offload到TOR
- 支持分布式L3 Gateway，将L3 Gateway分布到离每个计算节点直连的TOR
- 将Tunnel Gateway Offload到TOR
- 通过Arp/Dhcp Proxy，消除网络中的广播
- 将基于VM的限流，安全策略Offload到TOR

该方案的优点

- 不改变网络边缘的控制权，网络虚拟化的控制权仍然在系统团队
- 让服务器专注于计算，提升单台服务器的VM容量；同时提升网络吞吐量
- 消除L3 Gateway单点故障的风险，消除性能瓶颈和可扩展性瓶颈
- 将云平台需要控制的网络节点数量从Hypervisor的数量变为TOR的数量，降低了一个数量级，有效减轻云平台的可扩展性压力
- 将Tunnel数量从Hypervisor到Hypervisor的数量级降低为TOR到TOR之间的数量级
- 全网内尽量消除广播、组播、未知单播，消除flooding带来的无谓带宽消耗
- TOR仍然可以对用户数据应用策略，进行监控，消除了vSwitch方案带来的网络不可视问题
- 天然支持虚拟化计算机点跟非虚拟化计算节点的对接
- 不需要用户重新改造网络，不需要增加额外设备，不增加成本，可以从vSwitch方案无缝切换。不会导致厂商锁定

Topic

centec networks

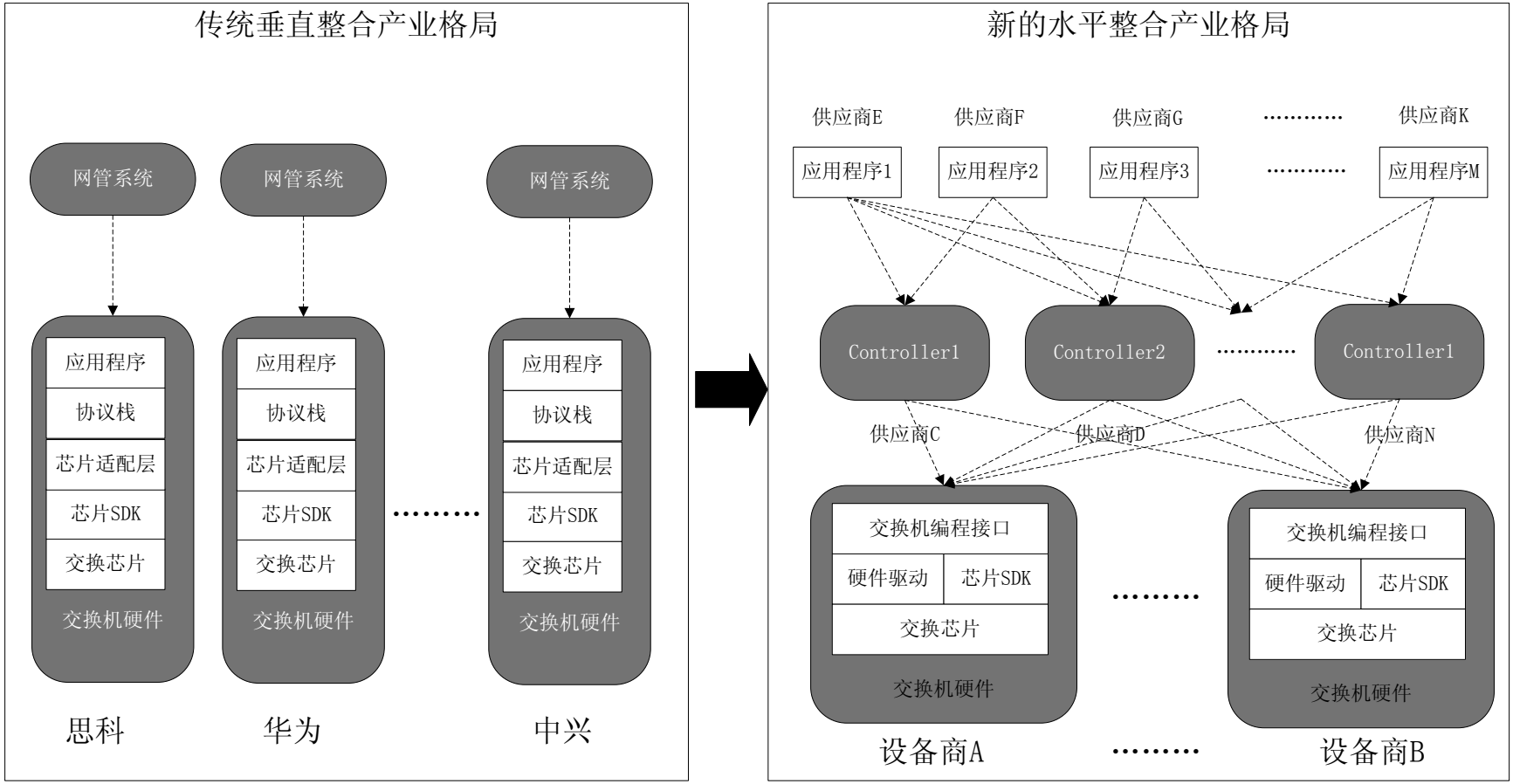
SDN: What? Why? How?

OpenFlow的价值与局限

SDN在云计算中的应用

SDN对产业格局的影响

SDN对产业的影响



SDN市场现状

- 说SDN市场大，目前主要是指网络虚拟化方案
- 硬件产品上，大厂商口号喊得响，实质性产品很少
- 除了网络虚拟化，没有可规模复制的产品和场景出现
- 对硬件SDN来说，目前用的最多的都跟流量牵引有关
  - 安全领域
  - Traffic Engineering
  - 广电、视频监控
- 工业界和研究机构的预研项目挺多

SDN如何落地？

- 纯软件SDN已经在网络虚拟化领域落地
- 对于硬件SDN，目前仍处于市场培育期，必定是Case by Case落地
- 硬件SDN的现状注定大公司难以介入，所以也很难迅猛发展
- 硬件SDN厂商卖Controller不是一个好主意，Controller存在的价值在于深度定制，满足客户特定需求
- 不要期望有一个one-fit-all的solution出来
- 硬件SDN规模部署目前仍看不清楚

SDN未来发展方向预测

- SDN必将兴起，逐步演进，但不会一统江湖
- 纯软件SDN在未来一段时间内都会是主流，硬件SDN主要用于特定市场
- 南向接口会开放化，但不会标准化
- 北向接口在特定场景中可能标准化
- OpenFlow不会消亡，但仅是SDN的一部分
- 没有一个Controller可以一统天下
- 转发面会有openflow优化，但是不会有纯Openflow ASIC芯片
- 白牌设备将大发展
- 厂商锁定问题只会缓解，无法根除

SDN的趋势，你观察到了吗？

centec networks

OpenFlow

OpenDayLight

OpenStack

OpenContrail

Cisco ACI

What’s Next?

SDN is dead!
Long live SDN!

centec networks

盛科网络，
SDN和云计算时代的创新者