

深入浅出SDN

新浪微博: @盛科张卫峰

QQ: 67278439





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.....

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.....



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



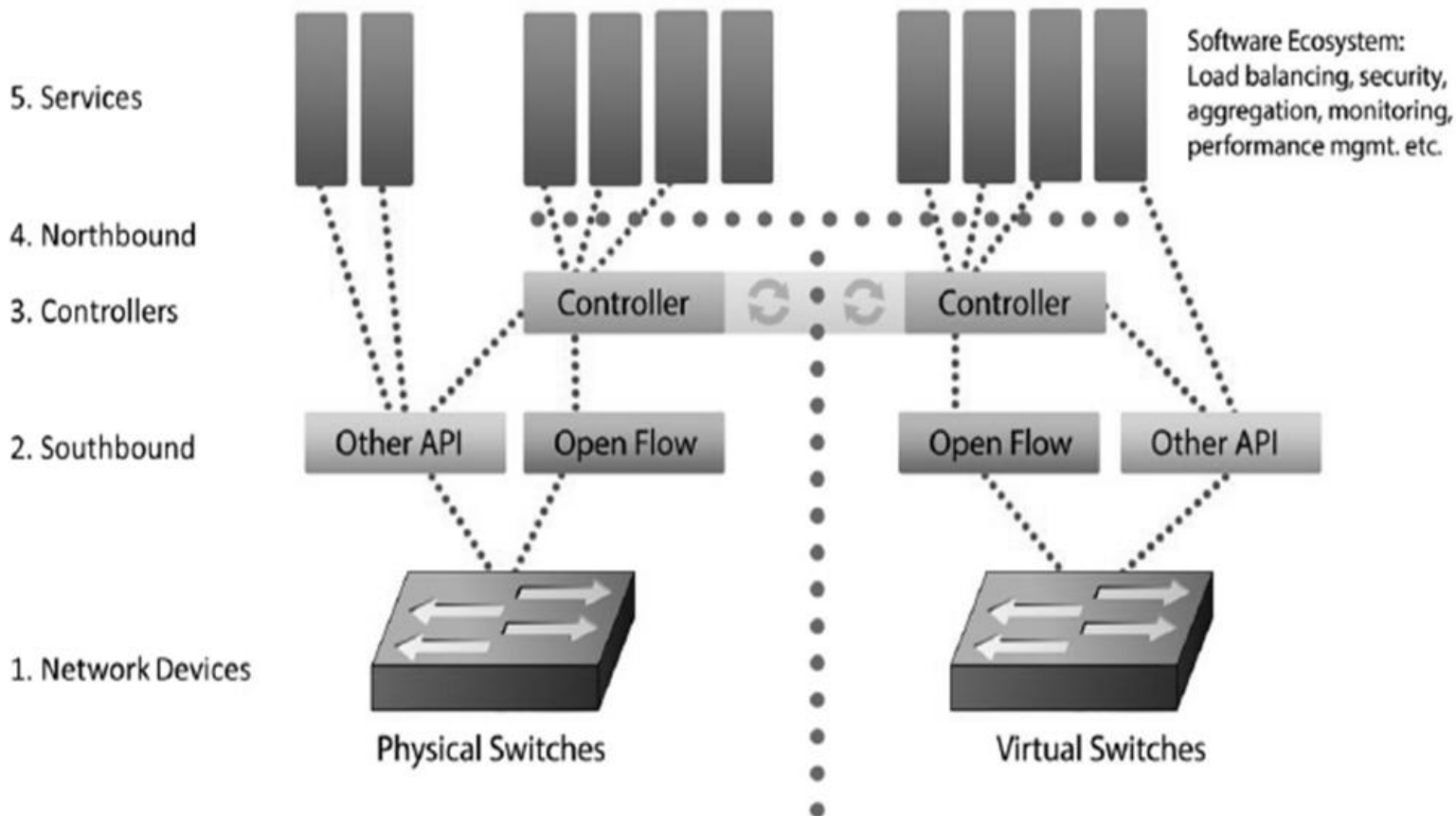
SDN思想下的新架构：控制与转发分离



centec
networks

6. Automation

Automation and Orchestration





SDN架构的本质属性



centec
networks





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



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



centec
networks

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?



Controller 很重要

- OpenDayLight
- Ryu
- FloodLight
- OpenStack

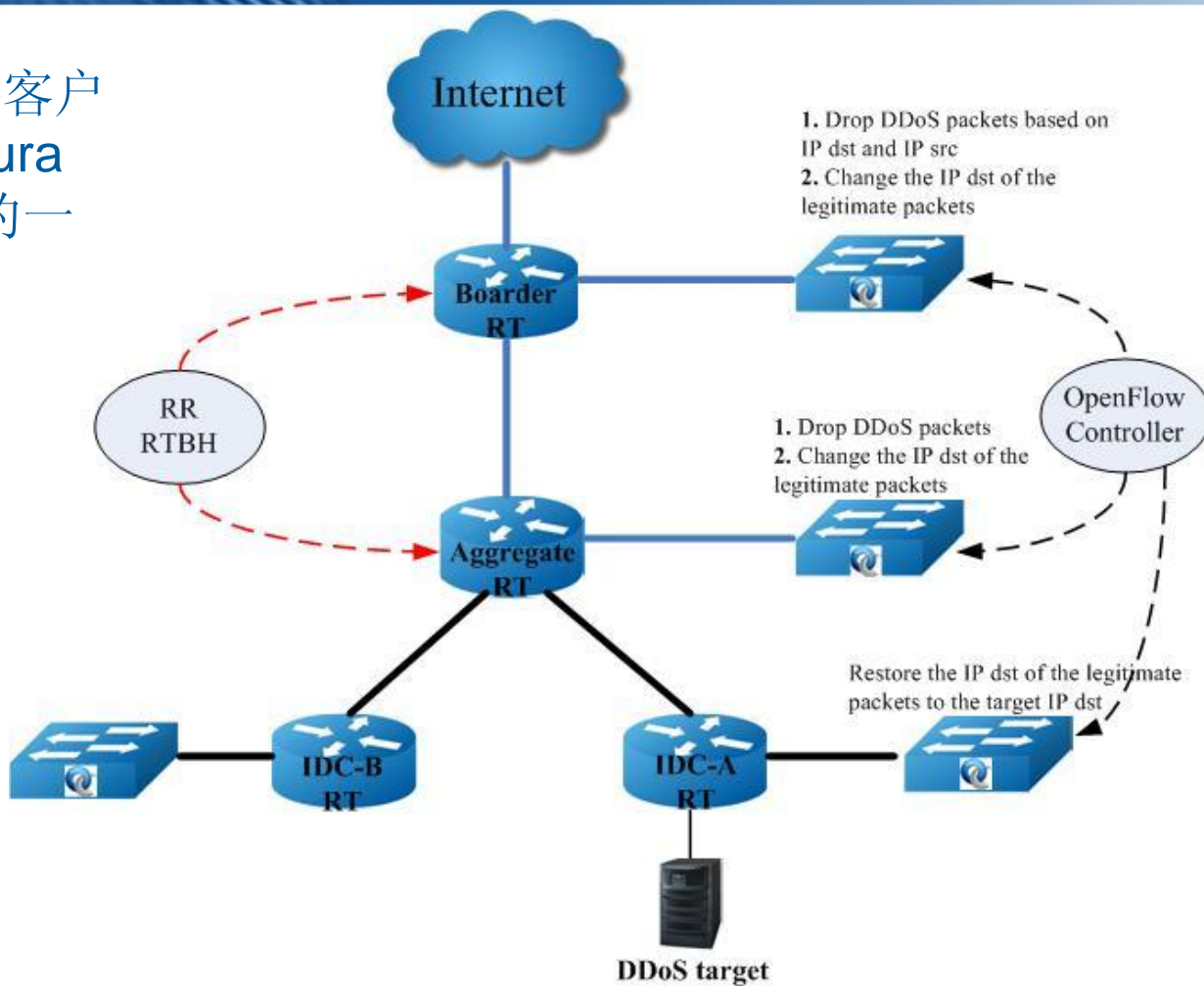
北向接口 很重要

- 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

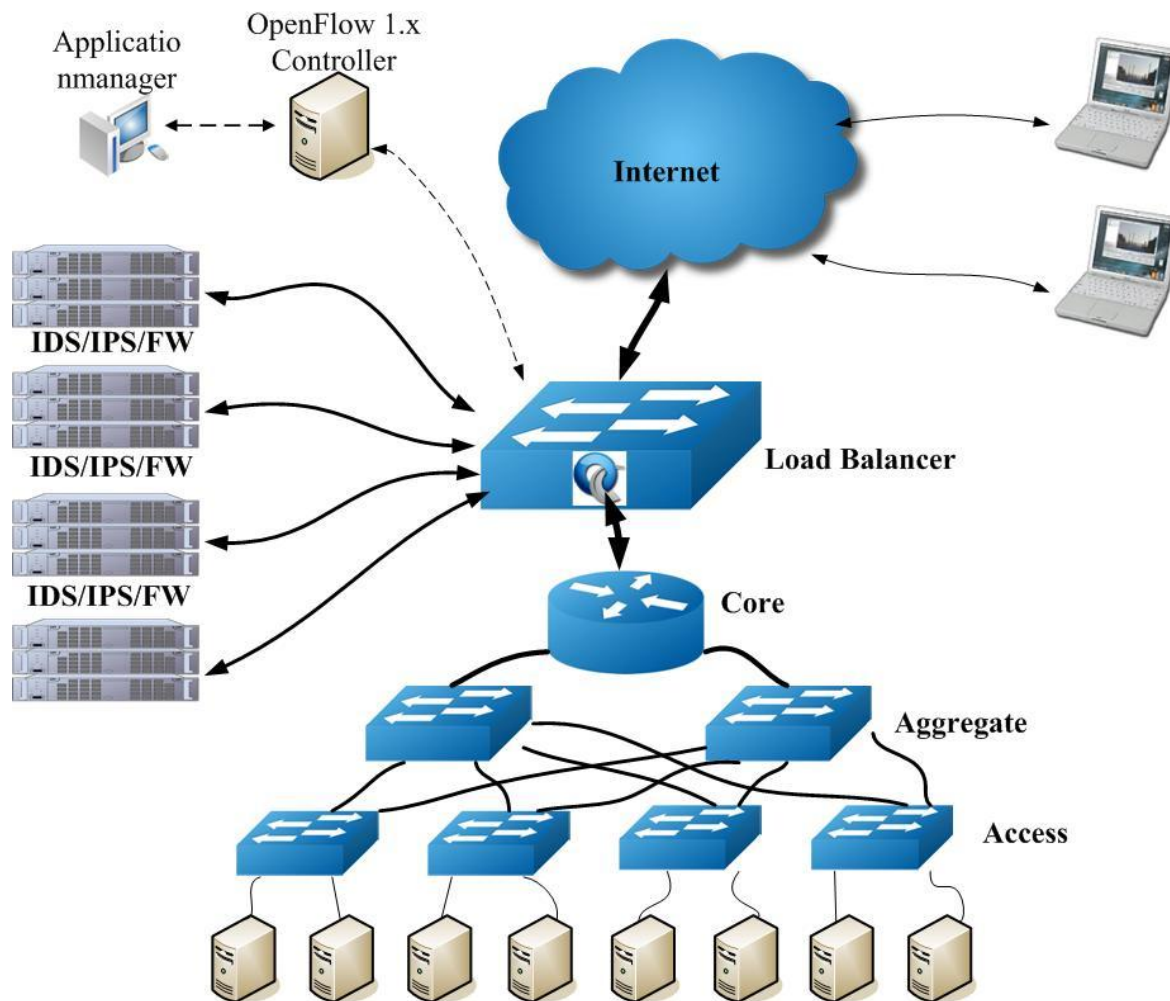




SDN案例2: Security Load Balancer



centec
networks



这是盛科交换机在安全领域应用的一个案例



■ 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）



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？



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



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



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？

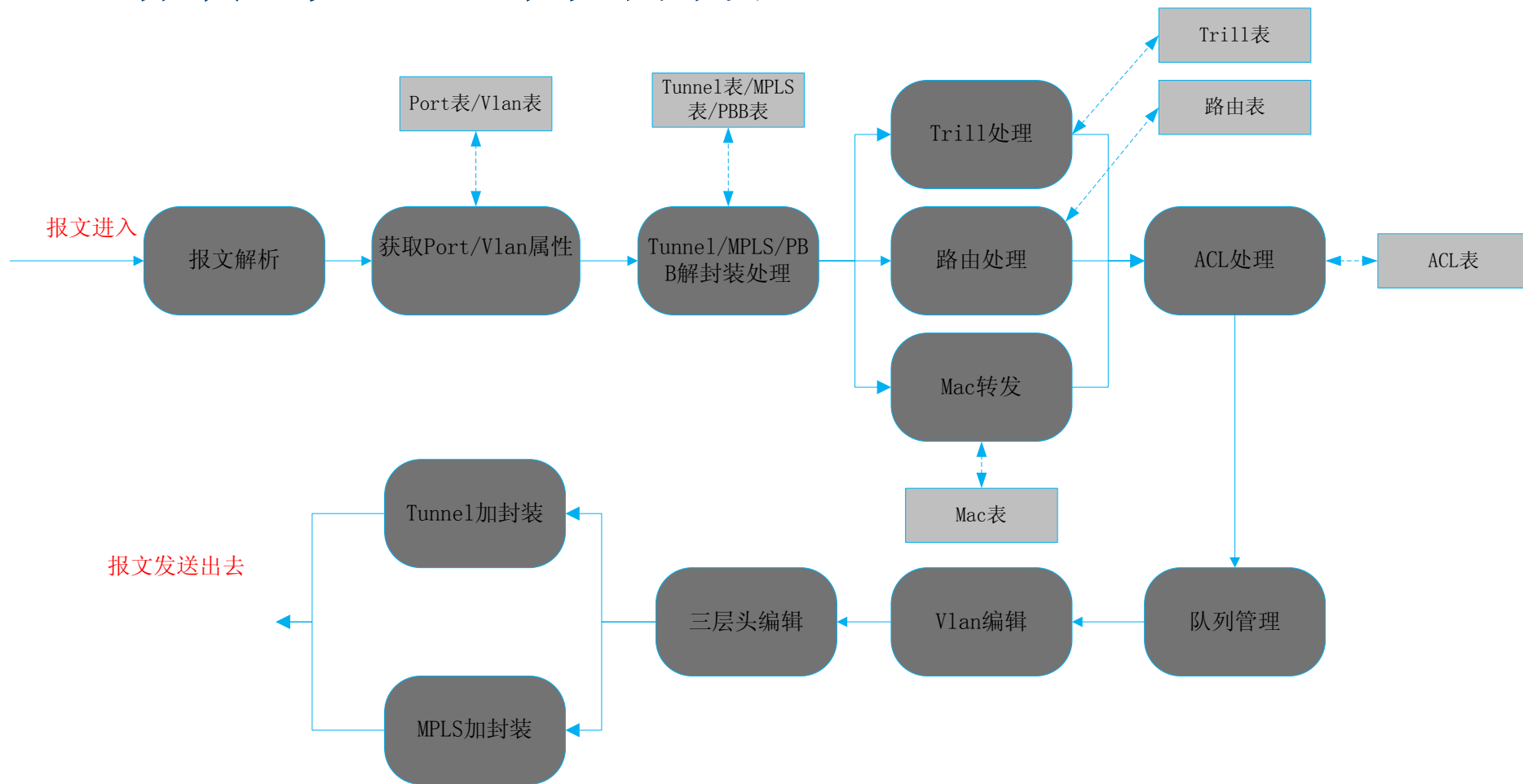
芯片厂商该何去何从？



- **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



■ 各个厂家ASIC流程大同小异

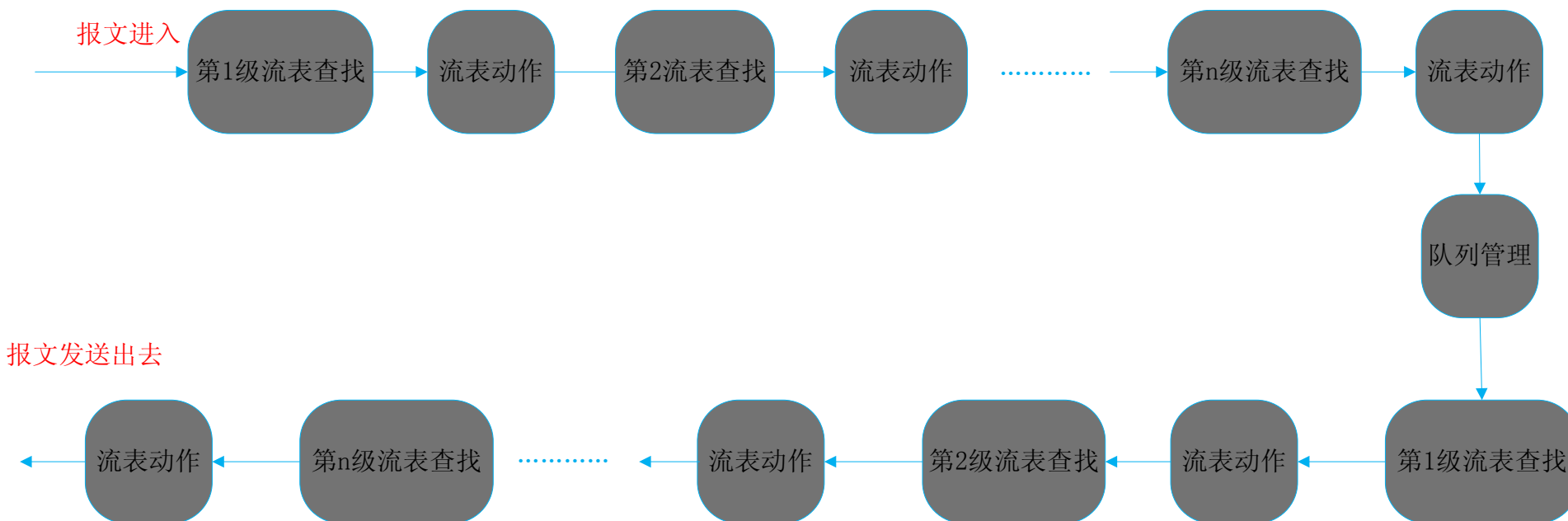




- 无论报文解析，报文查找，报文编辑都是可编程的
- 可以解析任何的报文类型，已知或者未知的
- 可以有多级流表，每级流表可以匹配任意字段组合，所有流表共享**memory**，可灵活分配
- 可以在每级流表出任意动作组合，编辑任意字段



■ 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



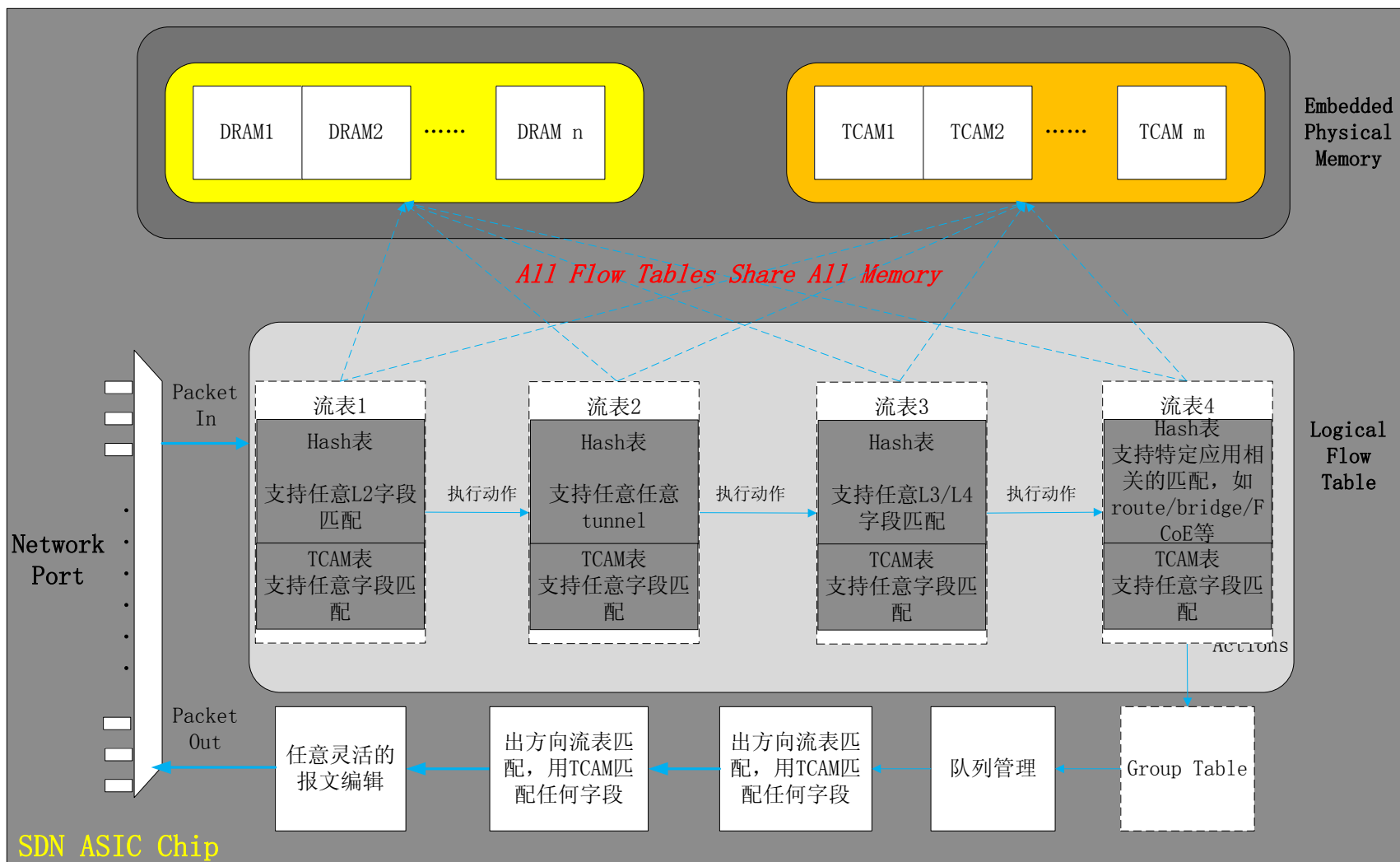
- 基于现有芯片架构，进行优化创新
- 使用**Nick**教授类似的思路，而适当折衷使之可实现
- 流表之间共享内存、适当数量的多级流表、灵活的字段编辑（比如可以修改**IP/Port**）、适当灵活的报文解析
- 通过创新的**TCAM+HASH**并使参与**HASH**字段可被灵活**Mask**掉的方式，用极低的成本支持业界最大数量的（**32K**）的流表



盛科创新的SDN芯片架构



centec
networks



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

盛科网络--全球领先的SDN芯片和定制化白牌设备提供商



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



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！！！！



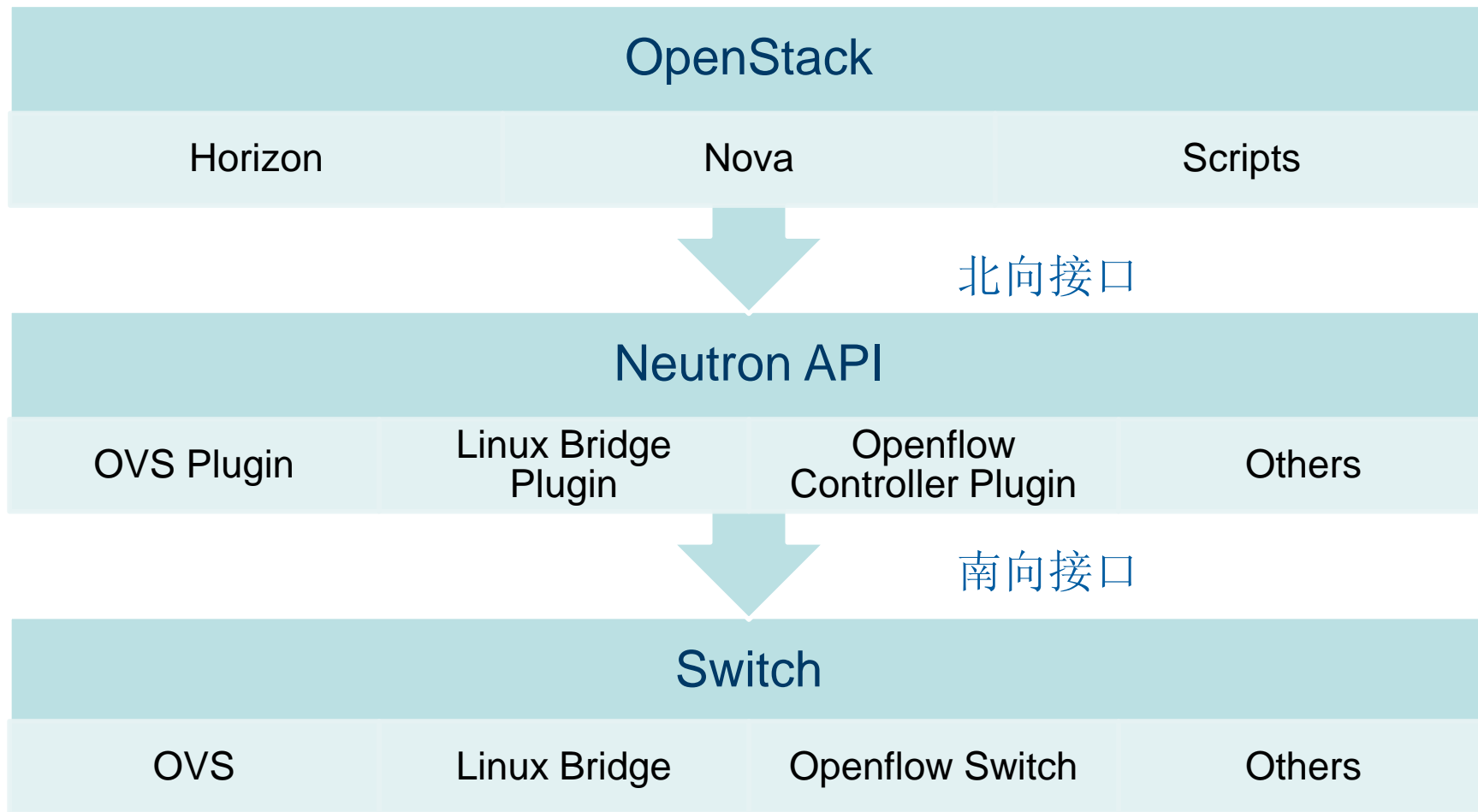
- **laaS云计算平台是标准的SDN架构**
 - 控制（云计算控制平台）与转发（虚拟或者物理交换机）
 - 开放的编程接口（南向和北向都是开放的接口）
 - 集中化控制（云平台集中控制所有的设备）
- **没有可编程API（南向和北向），就无法提供租户的self-service，无法自动化部署业务**
- **没有集中化控制，云计算平台要获取全局的信息就很困难，VM的迁移就很困难**
- **无论是虚拟交换机还是物理交换机，都可以是SDN**



OpenStack网络架构



centec
networks





Existed Neutron Plugin



BigSwitch

Cisco

Embrace

Nec

OVS

Ryu

Brocade

hyperV

Linuxbridge

Midonet

Mellanox

Nicira

Plumgrid

MI2

Centec(will
be available
soon)



纯软件的Tunnel Overlay方案

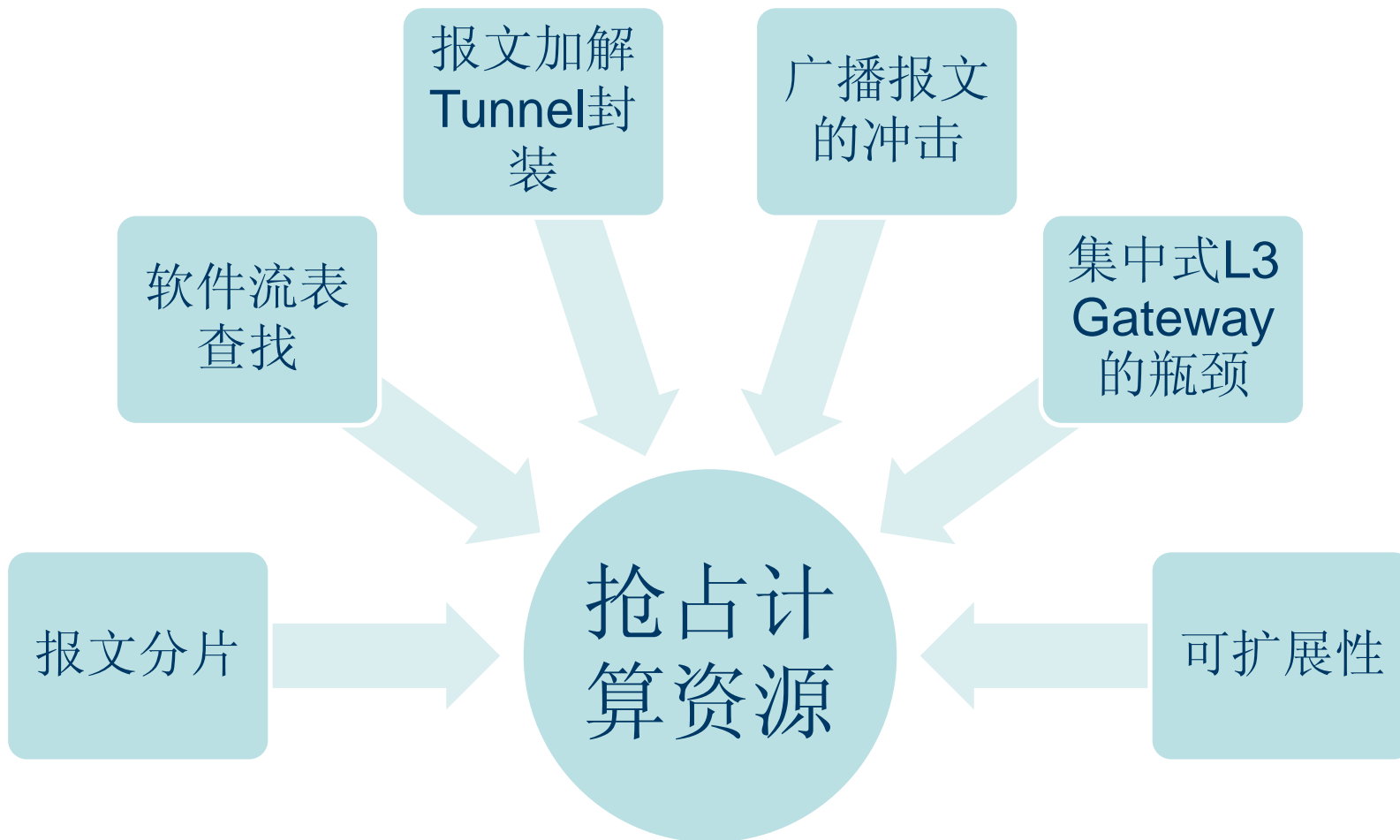


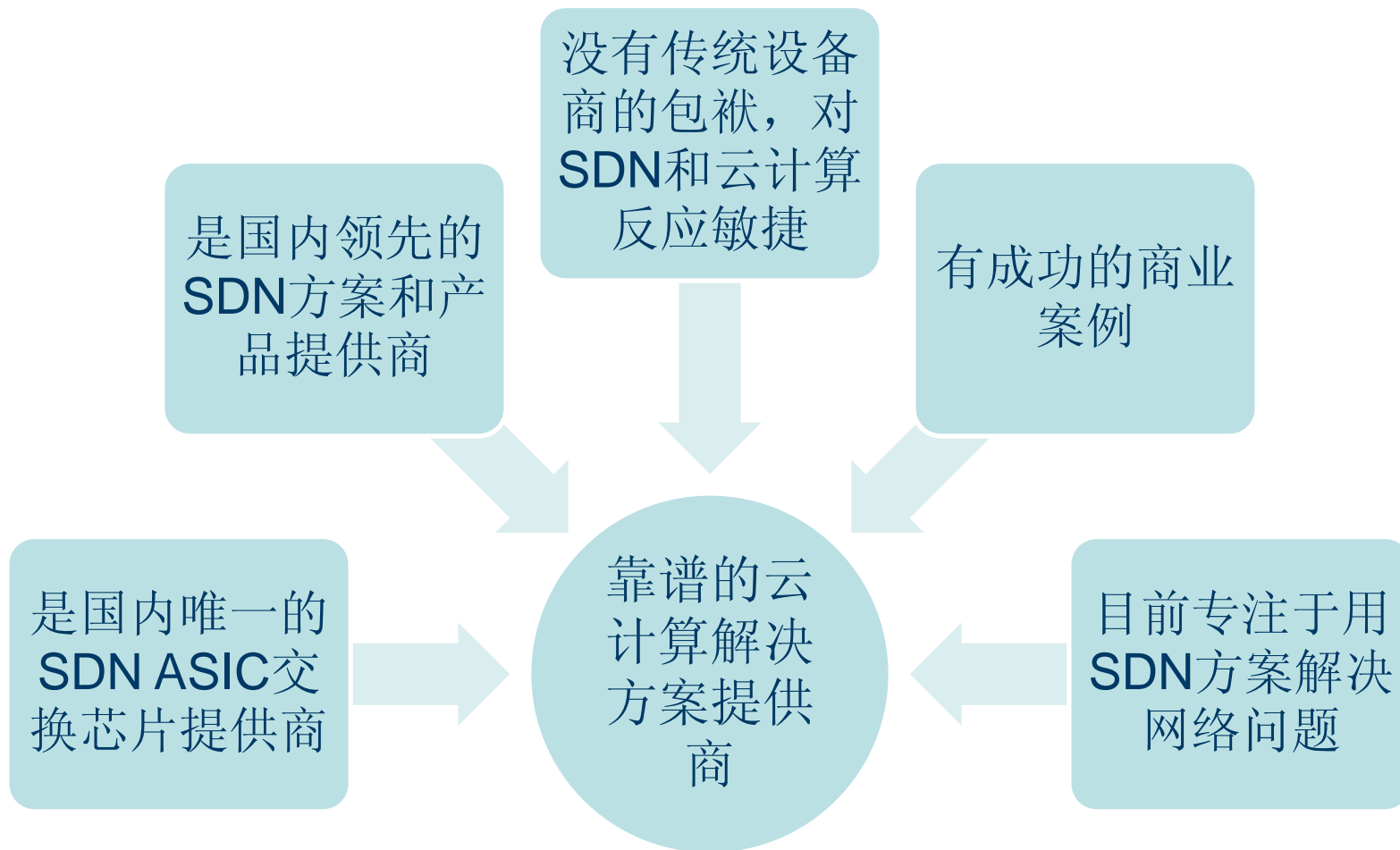
centec
networks

- 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



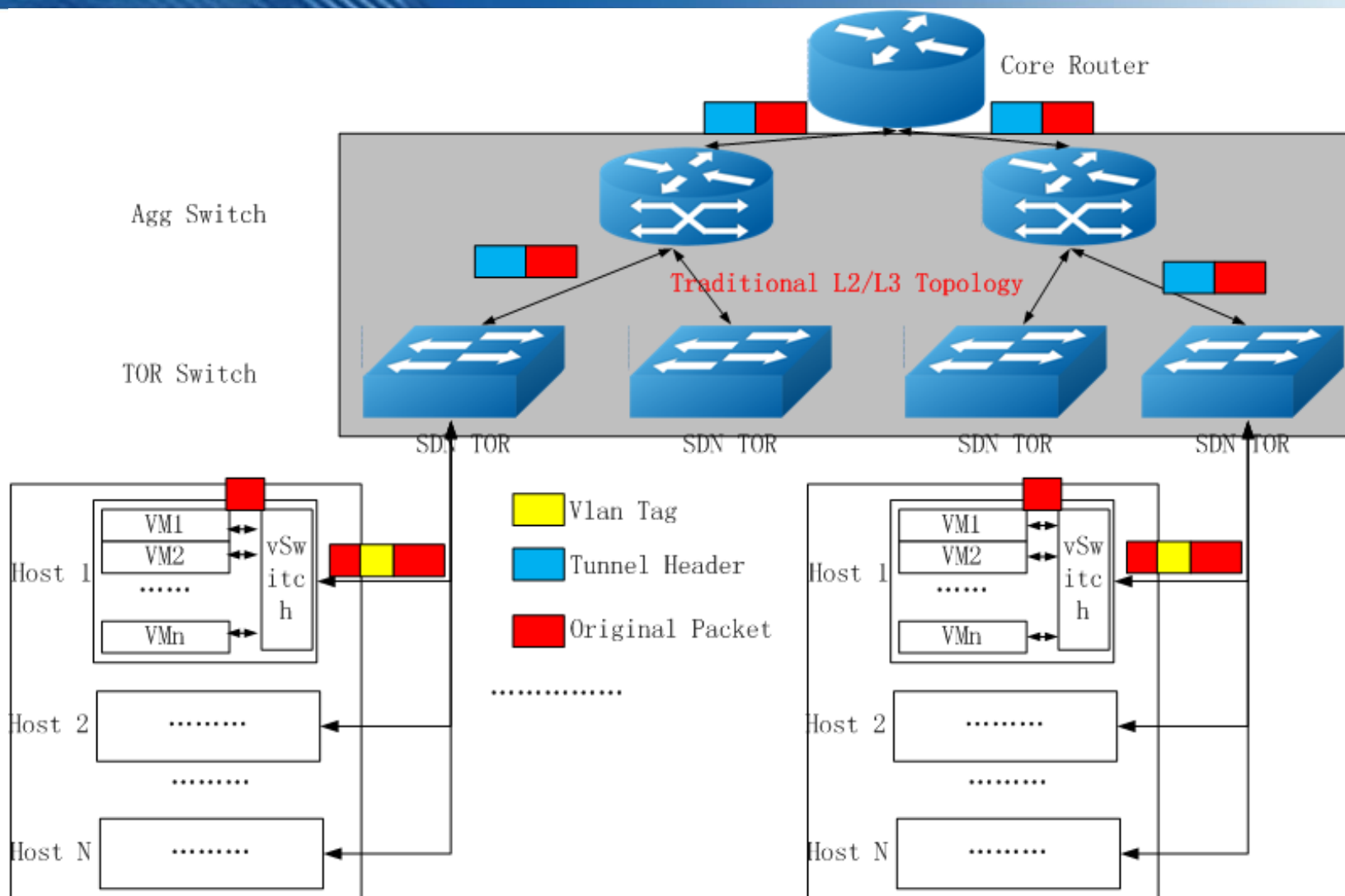
所参照的AWS VPC网络服务模型



- 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
 - 允许租户虚拟机迁移
 - 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

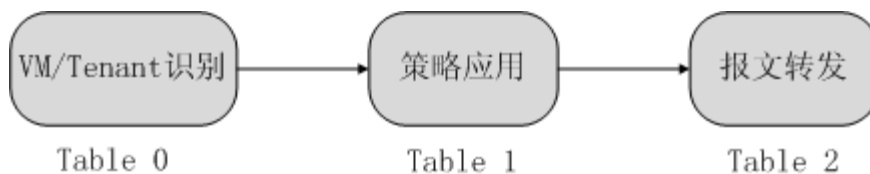


Table ID	功能	匹配字段	执行动作
0	识别VM; 识别Tenant; 识别tunnel; 基于 VM/Tenant 的统计, 做QoS	Vlan or Source mac or Logical Tunnel Port	Write metadata (tenantId); Strip Tunnel header; Go To Table 1; Meter; Counter;
1	对VM或者subnet或者tenant应用策略 (安全过滤或者QoS)	任意 L2-L4 字段, 另外还包括 metadata(租户ID)	Meter; Counter; Discard; Go to Table 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



centec
networks

- 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



SDN: What? Why? How?

OpenFlow的价值与局限

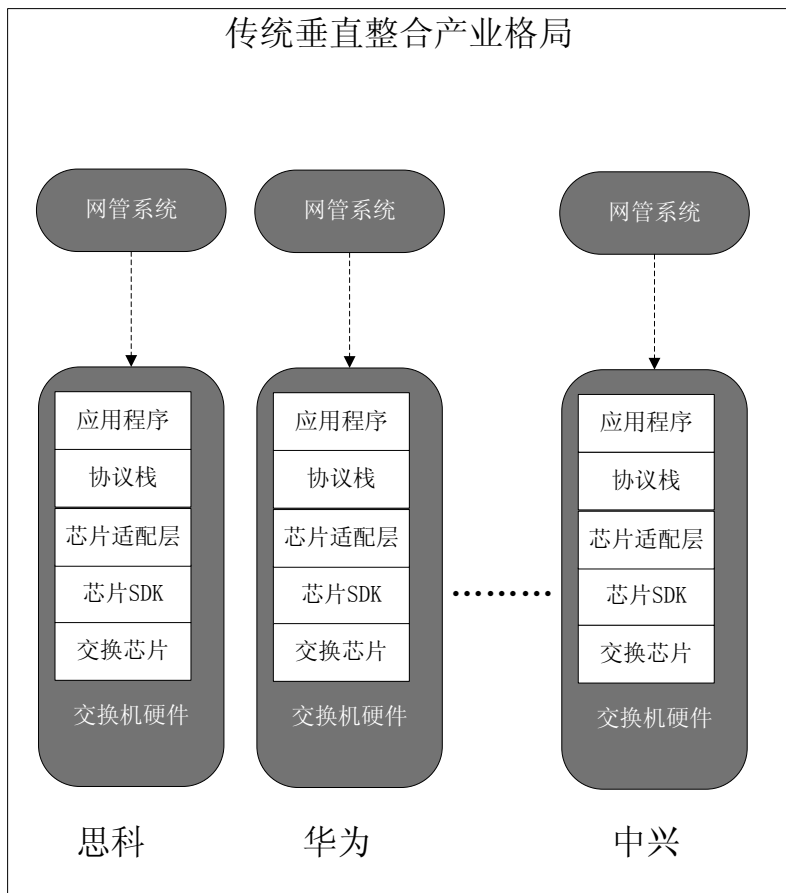
SDN在云计算中的应用

SDN对产业格局的影响

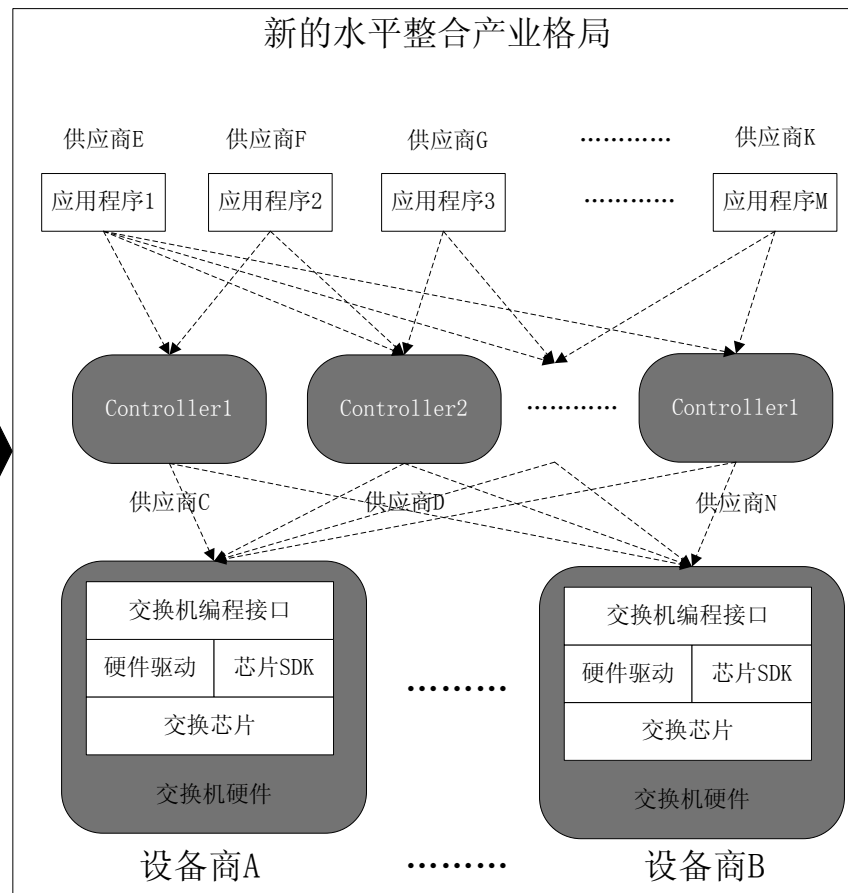


SDN对产业的影响

传统垂直整合产业格局



新的水平整合产业格局





- 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



centec
networks

- 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!



盛科网络， SDN和云计算时代的创新者