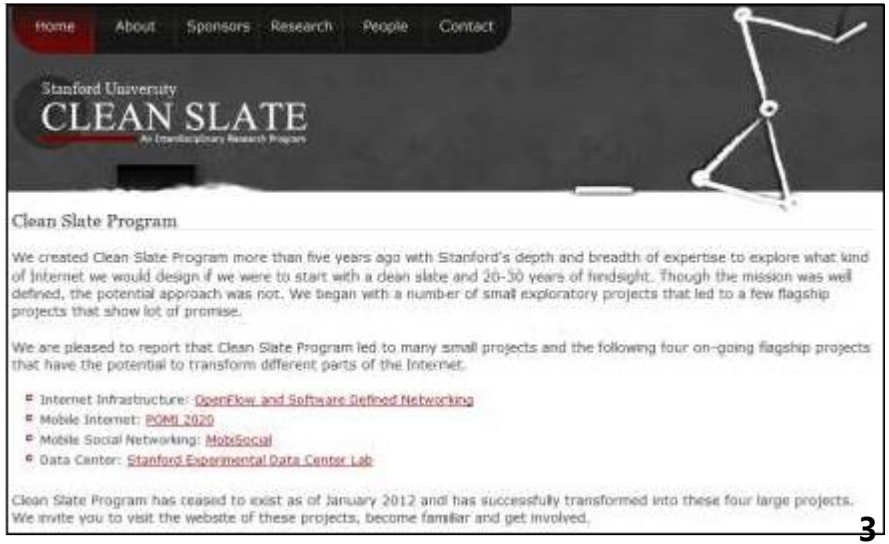
Software Defined Networking
SDN 学习总结

目录

- 关于SDN 与可编程网络
- 各种SDN技术思路、应用场景、标准化情况介绍
- 各厂商SDN方案介绍
- 展望SDN的发展

SDN 技术从哪里起源 —— Openflow

- 06 年斯坦福的学生Martin Casado 领导了一个关于网络安全与管理的项目Ethane，该项目试图通过一个集中式的控制器，让网络管理员可以方便地定义基于网络流的安全控制策略，并将这些安全策略应用到各种网络设备中，从而实现对整个网络通讯的安全控制。
- 通过集中式的控制器(Controller)以标准化的接口对各种网络设备进行管理和配置，那么这将为网络资源的设计、管理和使用提供更多的可能性，从而更容易推动网络的革新与发展。
- 于是他们便提出了OpenFlow 的概念， 并于08 年在ACMSIGCOMM 发表了题为OpenFlow: Enabling Innovation in Campus Networks的论文，阐述Openflow 的原理。
- 论文还列举了OpenFlow 几大应用场景，包括：
  - 园区网络中对实验性通讯协议的支持；
  - 网络管理和访问控制；
  - 网络隔离和VLAN；
  - 基于WiFi 的移动网络；
  - 非IP 网络；
  - 基于网络包的处理；
- 基于OpenFlow 为网络带来的可编程的特性，进一步提出了SDN（Software Defined Network，软件定义网络）的概念



SDN 是一种思想

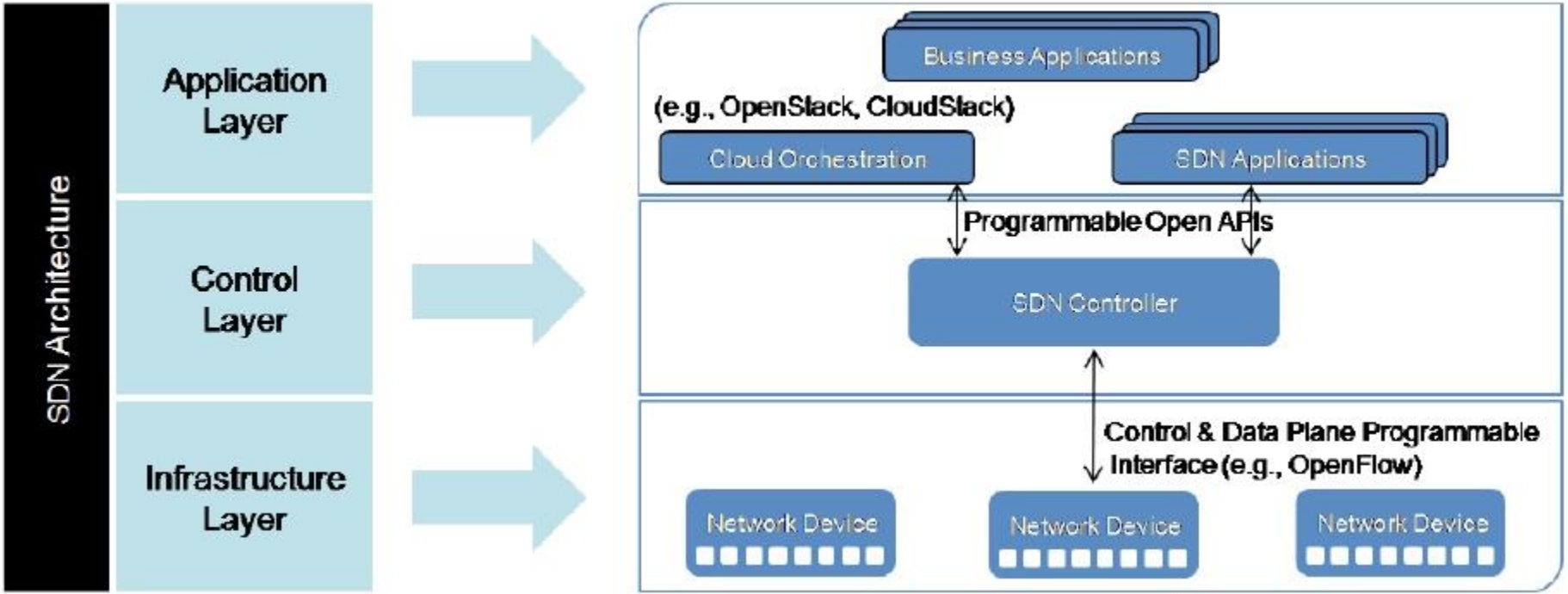
SDN不是一种具体的技术，而是一种思想，一种理念

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 的体系架构

- 北向接口，为应用提供编程接口
- 南向接口，设备控制信令，控制设备的转发行为
- 控制器/Controller，对网络的抽象层，NOS网络操作系统，屏蔽硬件，为应用开发提供开发接口；



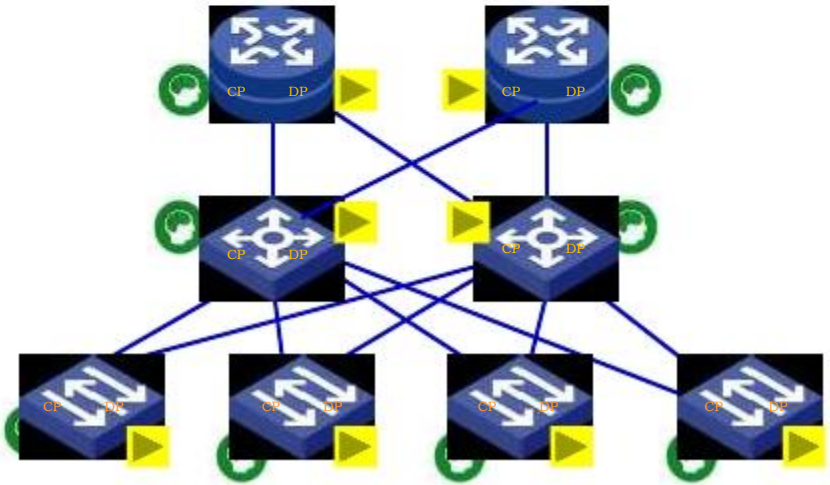
SDN 的三个最基本的特点

- 架构角度：控制平面与数据平面分离，逻辑集中管理(集中到控制器上)；
- 业务角度：通过对控制器，使低层网络被抽象出来网络资源被抽象成服务，实现了应用程序与网络设备的操作系统进行解耦和。应用看到的是网络服务。
- 运营角度：网络可以通过编程的方式来访问，从而实现应用程序对网络的直接影响，一些新型的接口，可以实现传统网络管理不能做到的网络优化。

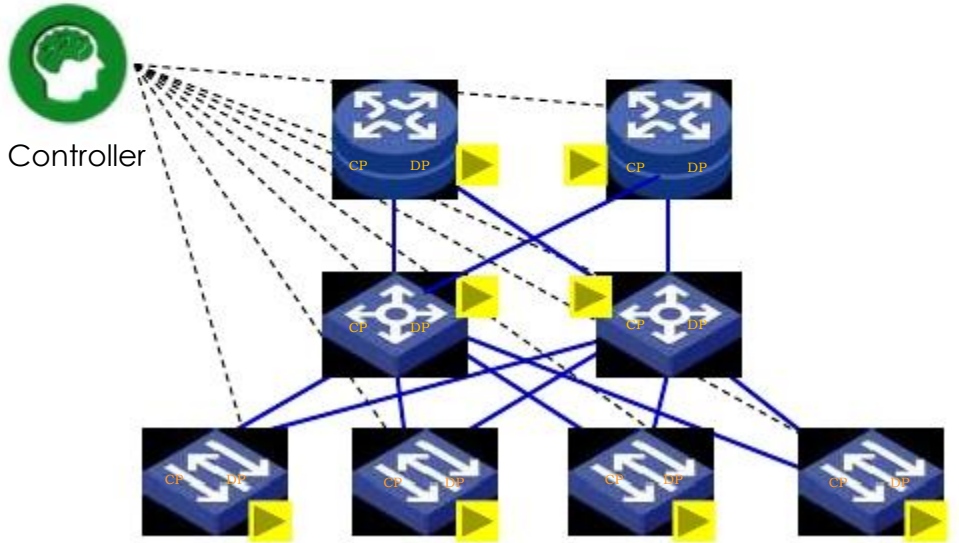
1、控制转发分离

控制平面（CP）　　转发平面（DP）

- 传统网络设备的CP与DP 不分离；
- 设备之间通过控制协议交互转发信息；

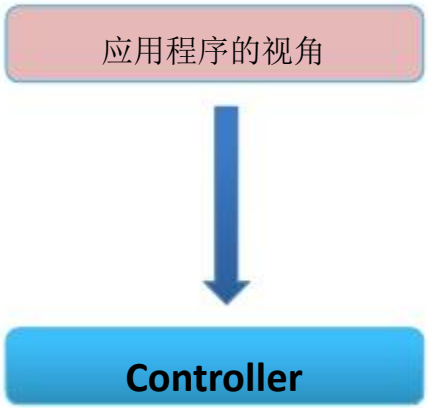


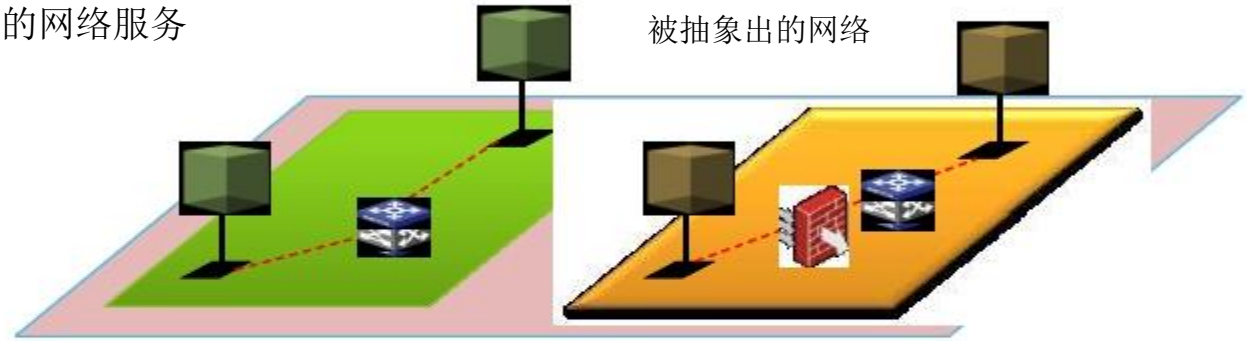
- SDN 的思路是将网络设备的控制平面集中上收到Controller;
- 网络设备上指保留转发平面（转发表项）；
- 通过Controller实现网络统一部署和网络自动化；

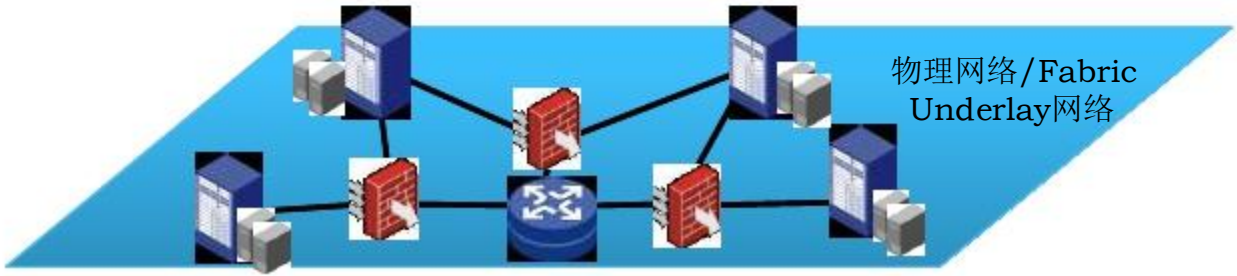


2、网络的抽象

- 通过Controller实现了对基础网络设施的抽象；
- 应用程序看到的是Controller提供的网络服务

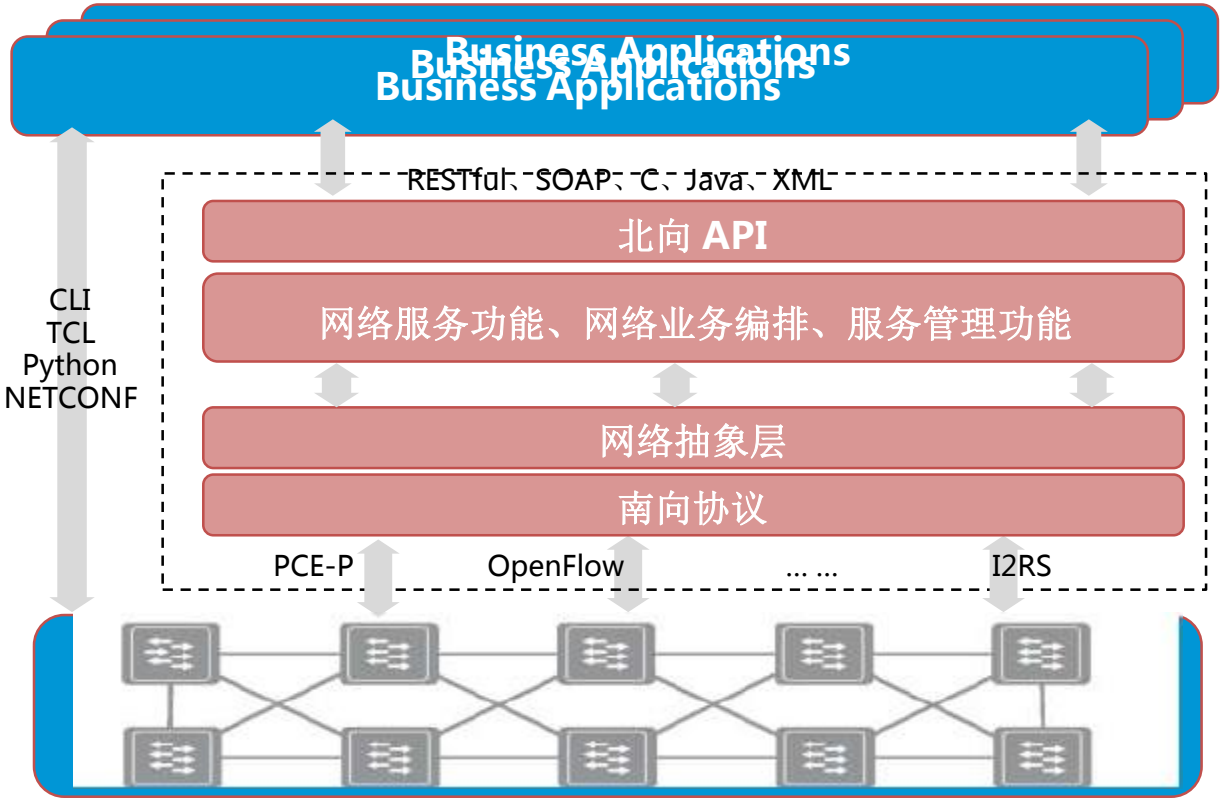






3、可编程接口

- 传统的网元都具备管理接口，可以通过网关协议（SNMP、NETCONF）或CLI实现简单的编程；
- 但传统接口常导致应用程序需要与网元设备之间通过某种代理或翻译器来通信。副作用是在应用设备与网元设备之间的反馈回路的时间长。
- 一些新型接口协议如XMPP、Thrift、JSON等可以更灵活的以异步的方式操作网络设备；
- 一些新的协议如I2RS可以直接对网络路由系统进行直接的、快速的应用优化的修改/编程。
- SDN可编程接口不是传统的网络管理，而是一种在应用与网元之间双向的、紧密联系的通信通道，可以实现传统网络不具备的网络快速优化能力。



@关键是 “可编程性”及“可编程的平台”

架构的控制转发分离

Control Plane / Data Plane Separation – Centralized Control

SS7
ATM LANE
Wireless LAN Controller
GMPLS

物理网络的抽象的协议

Overlays / Encapsulations

MPLS
VPLS
VPN
GRE Tunnels
LISP

可编程接口

Management and Programmatic Interfaces

SNMP
NETCONF
EEM

- 从单一点的技术点上看，思路SDN 的三个视角都是没有逃离传统网络的技术思路。
- 但SDN 区别于传统网络技术的关键是“通过可编程性，将应用与网络设备之间的交互更紧密结合”。二这种紧密结合性，需要上述三种思路：“控制转发分离”、“物理网络抽象”、“可编程接口”。
- 可编程性是SDN的核心。将控制和管理平面从交换机、路由器中移到设备外的软件中，并通过SDN协议来连接网络设备。这些设备外的软件平台有自己的API、处理逻辑，以及向网络提要求、接受事件、处理SDN通信协议的能力，这些软件平台就是“控制器/Controller”。
- 应用开发人员只使用控制器提供的API来实现网络自动化、网络编排和操作网络。
- 控制器被认为代表了支持SDN的应用程序的基础架构，体现了SDN的可编程性。传统网络部具备这个。

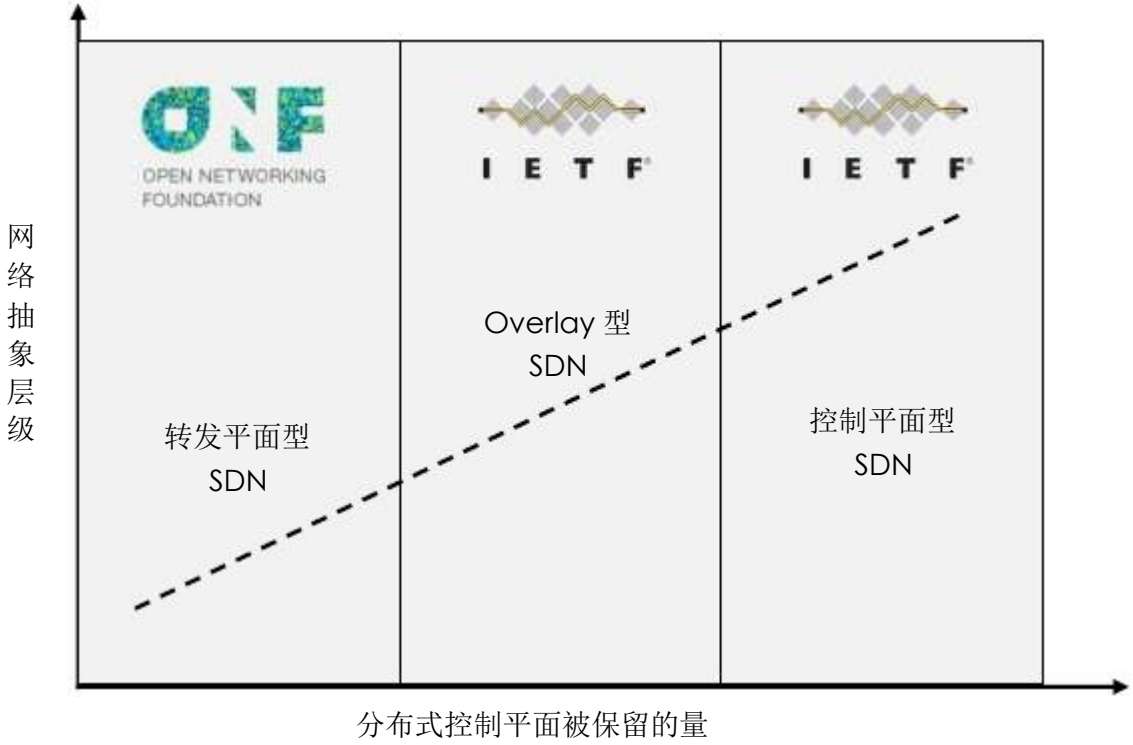
小结：SDN的定义与结构

- SDN 源于Openflow，但SDN 不等于 Openflow.
- SDN是一种架构，一种思想。让应用参与到网络控制中。
- SDN 的三个特点：
  - 转发、控制分离（并不是所有的控制都要被分离出来）；
  - 控制集中，网络被抽象
  - 编程接口

OpenFlow is one Fish in the Sea of SDN

当前各种SDN思路的技术与标准化组织

SDN 的技术思路



- ONF，致力于推动“转发平面型”SDN的架构及OpenFlow协议的标准化。
- IETF，有多个工作组参与制定SDN相关的通信协议，思路是重用当前的技术而不是OpenFlow，重点是设备控制面的功能与开放API。
- Open Daylight，控制器标准化的开源项目，有厂商驱动。
- ETSI 的 NFV 不是SDN，但其应用部署于SDN(尤其是overlay SDN)有很密切的关系。

SDN技术在业界的应用部署情况

- 只有少数用户部署了SDN技术的网络
- 而且这些用户集中在互联网、云计算运营商
- 转发平面型SDN，有少量用户使用，主要在广域网
- Overlay 型SDN，应用比较多，主要是在数据中心应用@腾讯
- 控制平面型SDN，主要受技术成熟度影响，目前应用很少

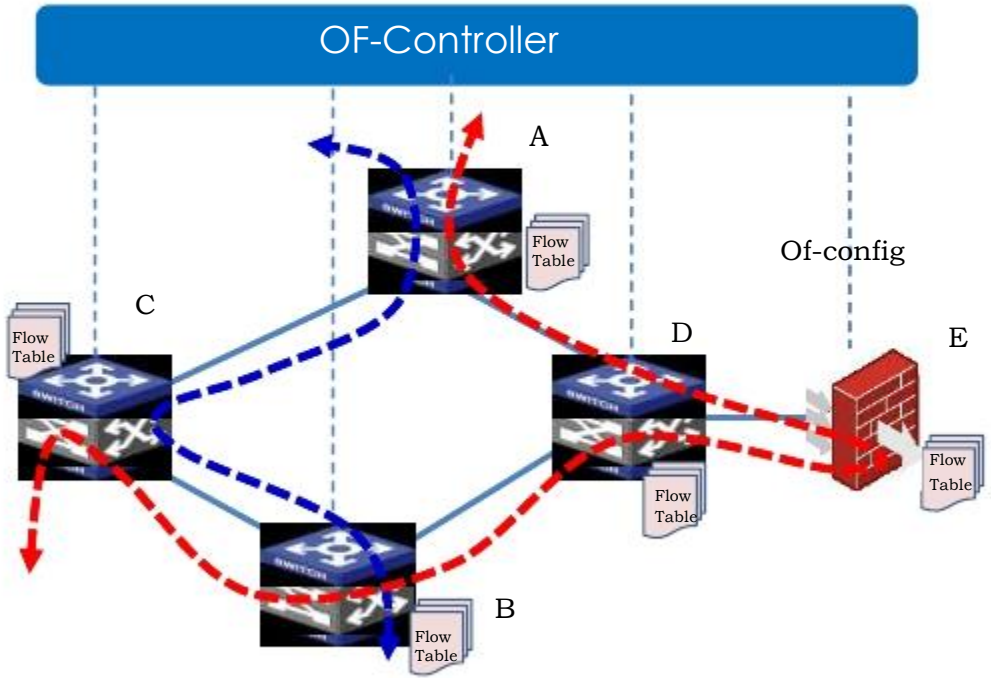
- 总体来看，由于SDN技术主要带来的好处是可编程带来的网络自动化，而目前SDN的编程接口并不统一标准，这就要求用户有较强的技术自主开发能力。
- 所以，各种类型的SDN技术，在企业网应用都很较少。
- 由于私有云计算平台要求网络资源被抽象，以提供自动编排能力，所以目前看Overlay型SDN发展速度较快。很多企业客户开始测试、评估Overlay 型SDN。

目录

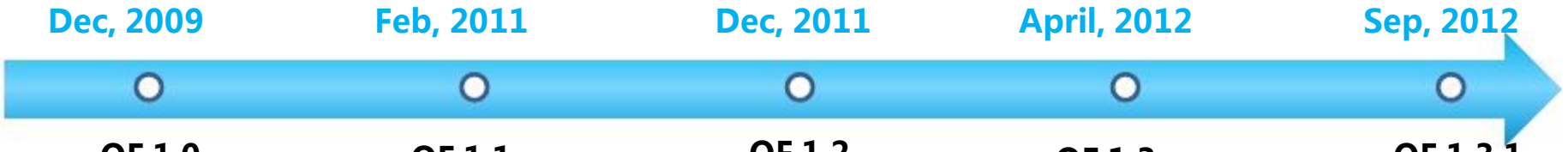
- 关于SDN 与可编程网络
- 各种SDN技术思路、应用场景、标准化情况介绍
  - 转发平面 SDN —— Openflow
  - Overlay SDN —— Vxlan Overlay
  - 控制平面SDN —— PCE-P
  - Network Function Virturlization （NFV）
  - SDN控制器（ Open Daylight ）
- 各厂商SDN方案介绍
- 展望SDN的发展

（一）关于转发平面型 SDN

- “转发平面型SDN”是完全不同与传统网络实现的一种设计；
- 设备中已经没有分布式控制平面的痕迹了；
- 转发平面SDN 的抽象层是逐跳转发表项；
- 通过逐跳表建立一个流的转发路径。对比于“overlay型SDN”，后者只在网络的边缘对隧道的首和尾进行编程。
- 最典型的就是 openflow 模型



OpenFlow的标准化组织



功能：

- 单表
- IPv4

- 多表
- MPLS、VLAN
- group
- ECMP

- IPv6

- 重构了能力协商
- PBB
- IPv6扩展头
- 多Controller
- Per flow meter

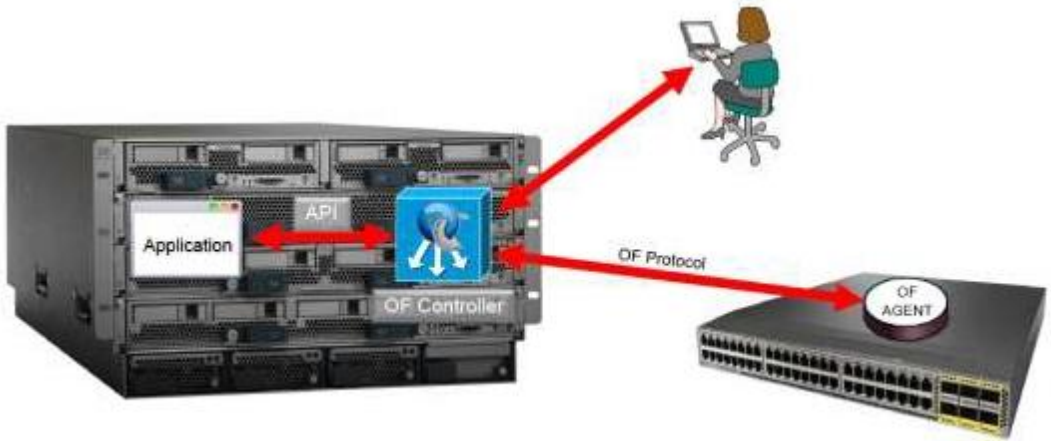
- 增强版本协商能力

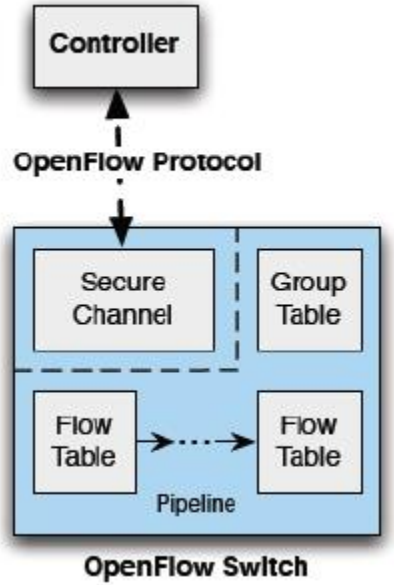
Open Network Foundation，即开放式网络基金会。ONF是非盈利的组织机构，致力于创新和发展新型网络架构，即软件定义网络（SDN）。

-ONF成立一年，有超过80家国内外公司加入到ONF的商业化推广和使用SDN技术的推广。

-国内企业包括：华为、中兴、腾讯、盛科、华三等。

Openflow 方案模型



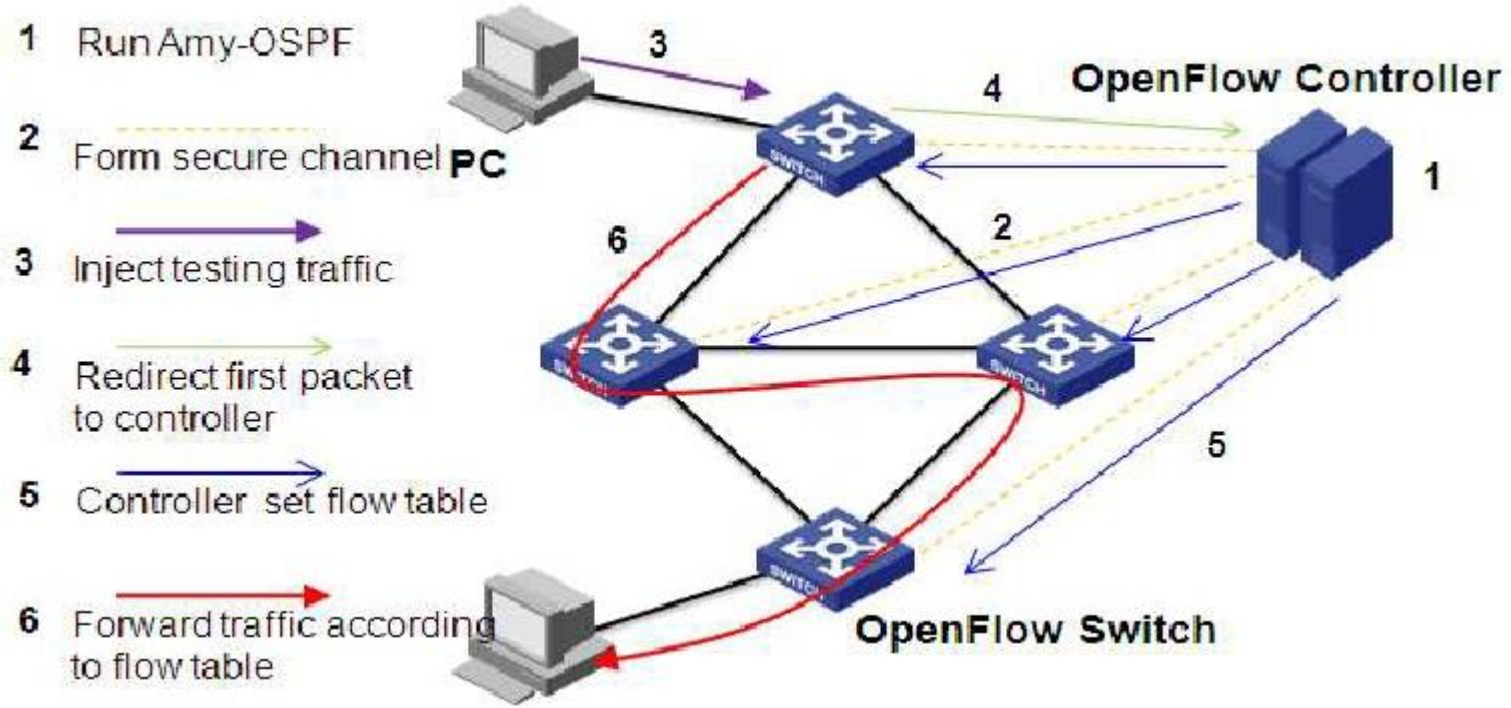


- 安全信道：Controller通过安全信道向OpenFlow Switch下发命令和接收信息
- 组表 Group Table：用一个Group使OpenFlow可以支持额外的转发行为（如select）
- 流表 Flow Table：OpenFlow交换机的基本表项

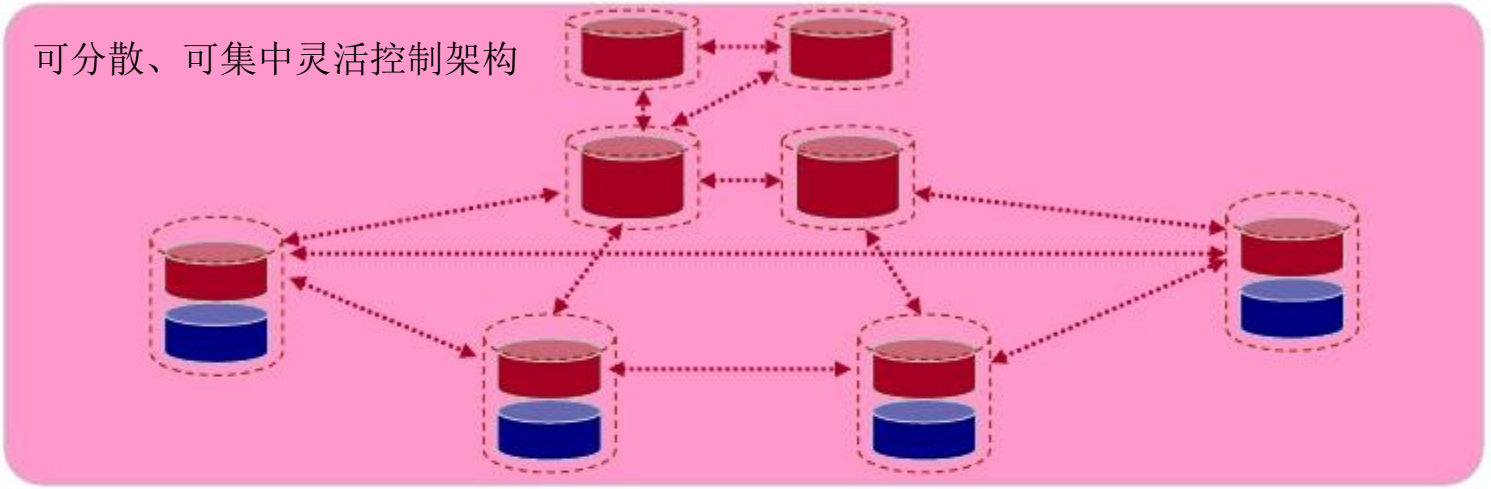
从Controller 下发的流表（OF v1.0）

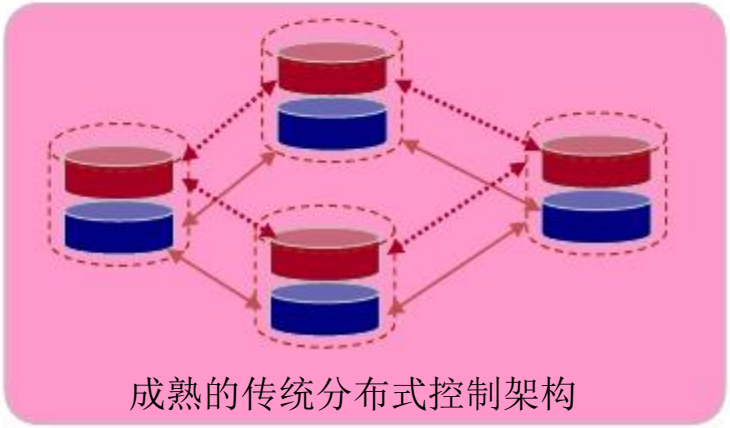
Ingress Port	Source MAC	Dest MAC	Ether Type	VLAN ID	VLAN Priority	IP SRC	IP DEST	IP Protocol	IP TOS	TCP/UDP SRC	TCP/UDP DEST		Action	Priority	Counter
*	3c:07:54:*	*	*	Switching	*	*	*	*	*	*	*		Fwd Port 10	100	
*	*	Routing		*	*	*	192.168.1.*	*	*	*	*		Fwd Port 12	100	
Port 1	*	*	Replication/SPAN		*	*	*	*	*	*	*		Fwd Port 14...24	100	
*	Firewall/Security			*	*	*	*	*	*	*	25		Drop	100	
*	*	*	*	Inspection	*	*	*	0x0800	*	*	*		Controller	100	
*	00:01:E7:*	*	*	Vlan10	*	Combinations		*	*	*	80		Fwd Port 8	200	
*	*	Multi-action ; NAT		*	*	*	192.168.1.*	*	*	*	80		Rewrite 10.1.2.3; Fwd port 9	200	
Local handling			*	*	*	*	10.*	*	*	*	*		Local	200	

Controller/OpenFlow 工作方式举例

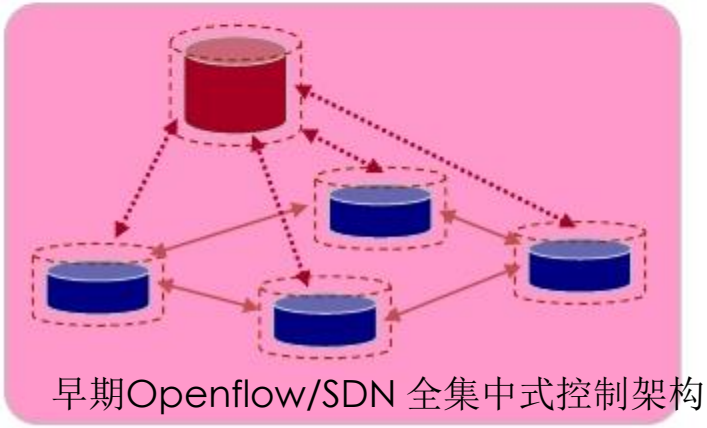


OpenFlow 目前Hybrid 架构





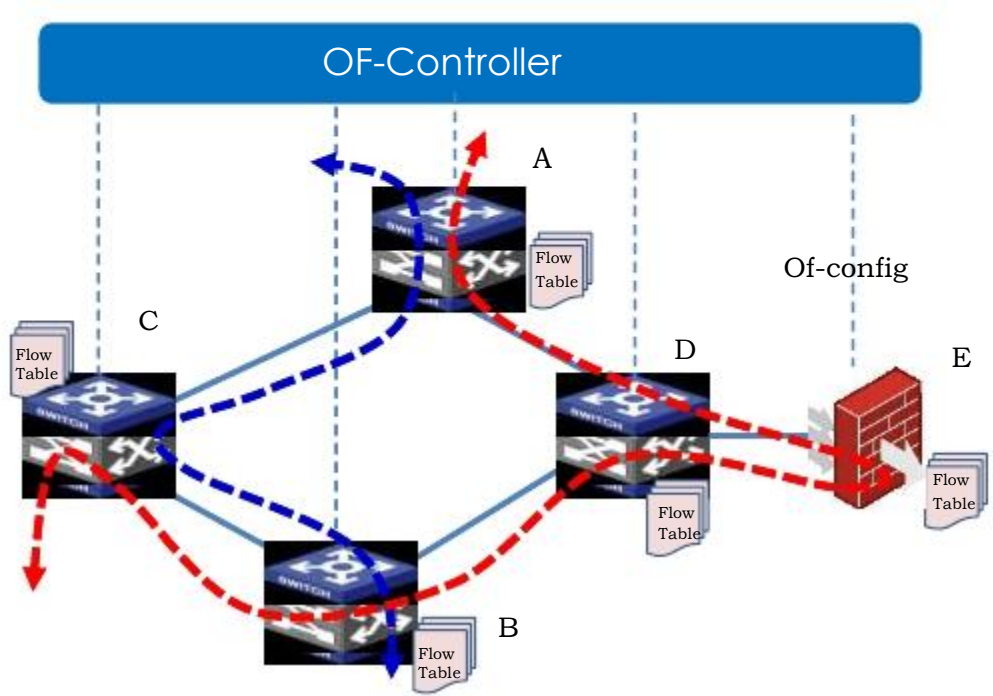
成熟的传统分布式控制架构



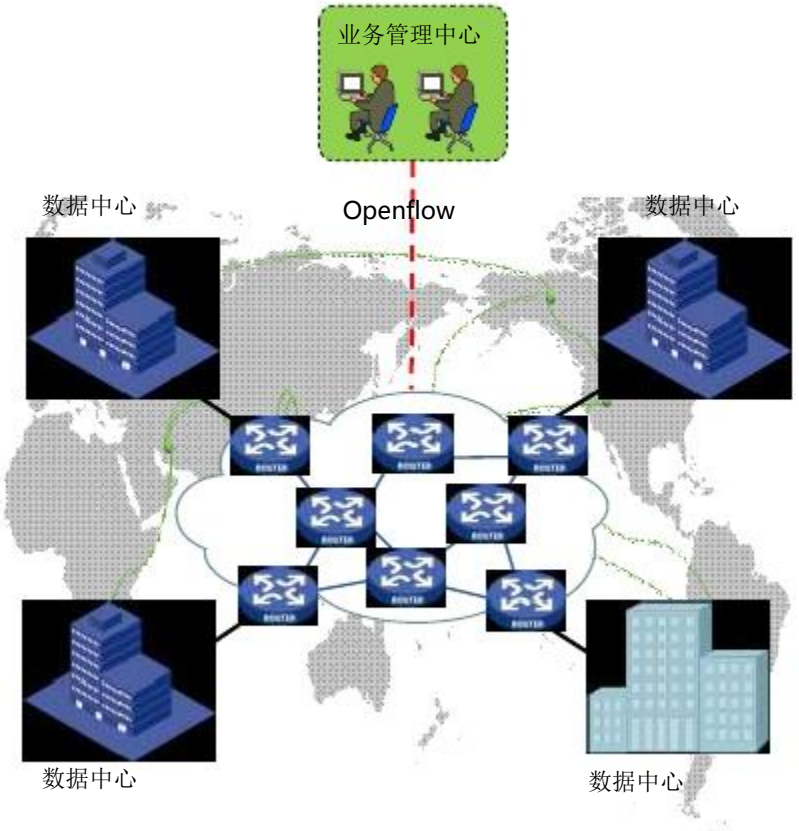
早期Openflow/SDN 全集中式控制架构

从三要素对 Openflow SDN 的小结

- 架构角度：控制平面全部上收到Openflow Controller，数据平面依靠流表规定的匹配字段和动作进行转发。目前来看，Hybrid 模式是主流。
- 业务角度：通过在不同的网元上下发流表，通过流表实现了对网络的抽象（路径）。
- 运营角度：
  - Openflow Controller与网元之间采用Of-Config 协议实现信息交互。即通过Of-Config实现对网络的编程。应用可以自定义流表，通过Of-Config 下发设备，并获取设备的反馈信息（紧密联系的模式）；
  - 协议目前支持三种报文类型：controller-to-switch；asynchronous；symmetric，每种报文类型都有很多子类型。
- 控制平面集中度高，但网络抽象度低！



Openflow 应用场景-骨干网流量工程

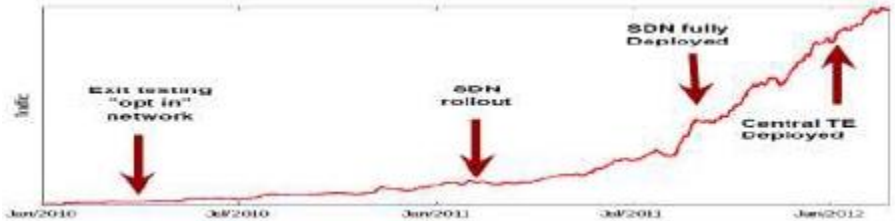


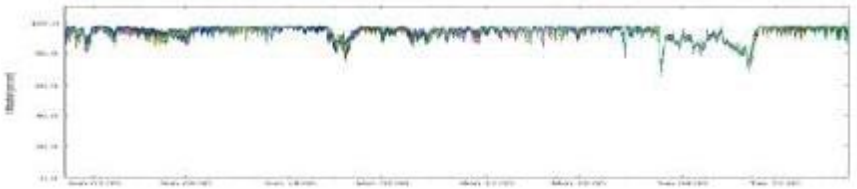
- WAN的主要需求：
  - 灵活性：业务部门经常有临时性的大容量传输，要求VPN，QOS，但网络很难快速满足，业务人抱怨网络基础架构相应慢，缺乏灵活性
  - 资源利用率：为保证故障情况发生切换时不出现拥塞，链路利用率小于50%，业务人抱怨带宽不足，但网络却有50%用不上；
  - 管理性：大量的设备需要管理，大量的差异化配置；
- 目前是通过MPLS-TE实现上述需求；
- 未来将通过SDN技术（Openflow），将整个网络看做一个路由器，统一配置管理，将不同的流量分别走到不同的路径上，可以快速提供网络路径，并且保证有北向接口给业务。
- Openflow 的好处：
  - 一致性，统一视角、无拓扑依赖
  - 简化配置管理，Controller集中管理
  - 易扩展，易增加网络设备

SDN 应用 —— 转发平面型， Google

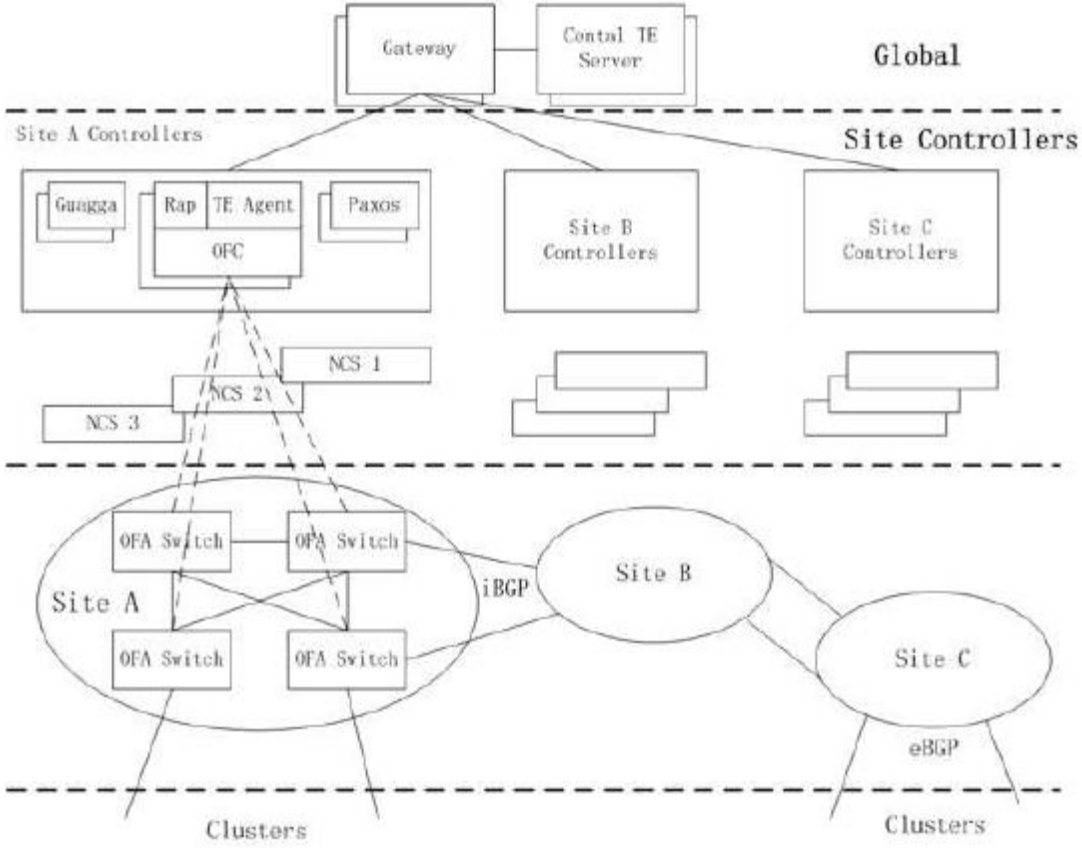
- 将分布于全球的11个数据中心用SDN技术互联
- 2010年试点，2012年完成全网部署

- 广域网带宽利用率提升至接近100%
- 故障收敛时间从9s减低到1s





SDN 应用 —— 转发平面型， Google



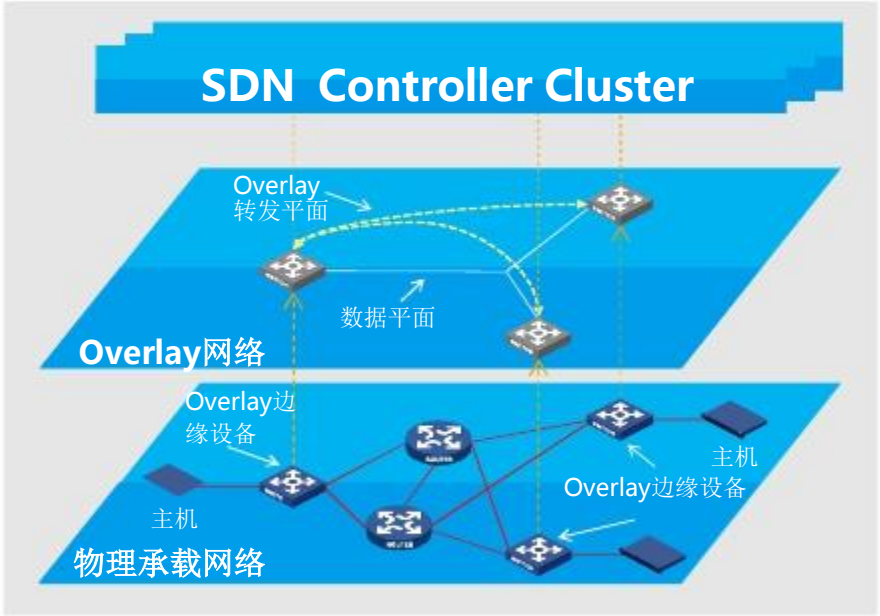
- 第一层的物理交换机是Google自己设计并请ODM厂商代工的，交换机里面运行了OpenFlow协议，向上提供的是OpenFlow接口，只是内部做了包装
- 第二层在每个数据中心出口并不是只有一台服务器，而是有一个服务器集群，每个服务器上都运行了一个Controller，一台交换机可以连接到多个Controller，但其中只有一个处于工作状态。一个Controller可以控制多台交换机，一个名叫Paxos的程序用来进行 leader选
- 第三层中，全局的TE Server通过SDN Gateway从各个数据中心的控制器收集链路信息，从而掌握路径信息。这些路径被以IP-In-IP Tunnel的方式创建而不是TE最经常使用的MPLS Tunnel，通过Gateway到Onix Controller，最终下发到交换机中。

Openflow 的局限

- 硬件芯片制约发展：现有芯片的流表项还停留在千级，这是远远不够的；
- 现在的网络是构建在数千的标准协议之上的，而如果要大规模部署OpenFlow，和这些协议的共存也成为一大问题。
- OpenFlow颠覆性的设计极大的冲击了当前的产业链，大规模应用有较大阻力。
- 目前的硬件芯片并不是以openflow 流表的形式组织的，而是将流表映射为传统的L2、L3、ACL表，
- 6月份的SDN大会上，Broadcom公司做了题为《利用广泛部署的交换机硅片架构促进SDN在运营商网络的全面实施》的主题演讲。

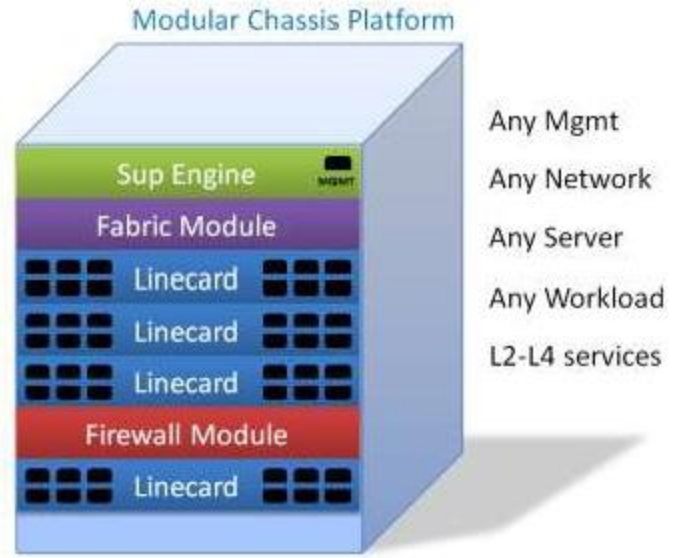
盛科芯片：V330提供88G的线速转发能力，支持多达2.5K的复杂流表，支持包括以太网二层到四层信息的编辑，多出口编辑等更为全面的OpenFlow动作，同时实现了包括NvGRE，MPLS隧道等多种封装技术，使得SDN/OpenFlow能够在更大范围得到部署。

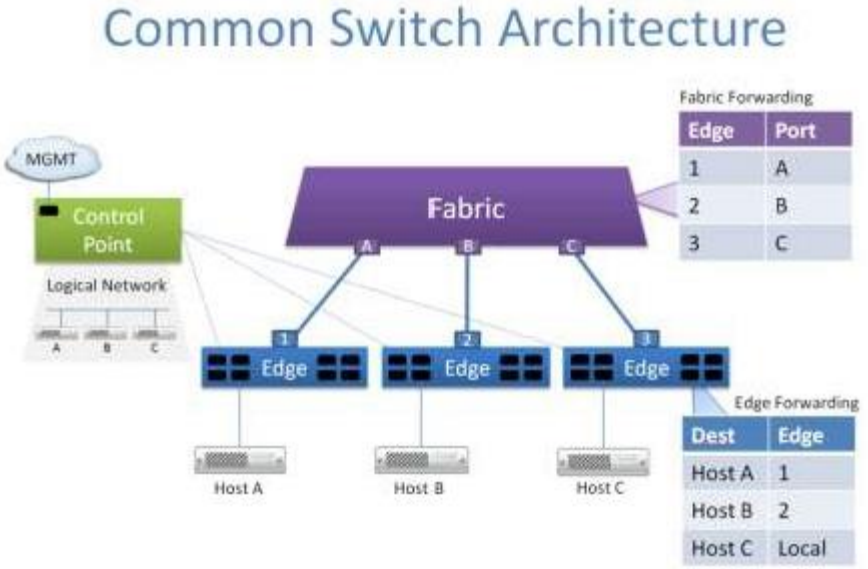
（二）关于Overlay 型SDN



- Overlay型 SDN侧重于建立灵活的overlay隧道，以便创建虚拟网络，并假定分布式控制平面存在和作用与Underlay网络，且实际上Underlay的网络对于overlay的可用性、路径优化有很多的好处，简化了overlay的虚拟网络。
- 但对于与“控制平面型SDN”，这又是一种简单的分布式控制，基本上只有IGP，而没用到MPLS或BGP这种对网络策略和转发路径有很灵活调配的技术。
- Overlay SDN 技术 通过Controller 实现转发与控制分离，通过Controller可以实现网络自动化部署；
- Overlay SDN不关注物理网络的承载能力，所以需要物理网络具有高容量、高可用性特点，即物理网络建议是全连接的 CLOS Fabric 结构；所以SDN Overlay 更适合于DC 网络/DC LAN

Overlay 型SDN —— 思路来自以太网交换机





当前各厂商的交换机都是由以下三部分构成：

- Control point (switch CPU, or supervisor engine)
- Edge forwarding components (port ASIC, or linecards)
- Fabric (switch ASIC, or fabric modules)
- 盒式、机架式都是这种模式

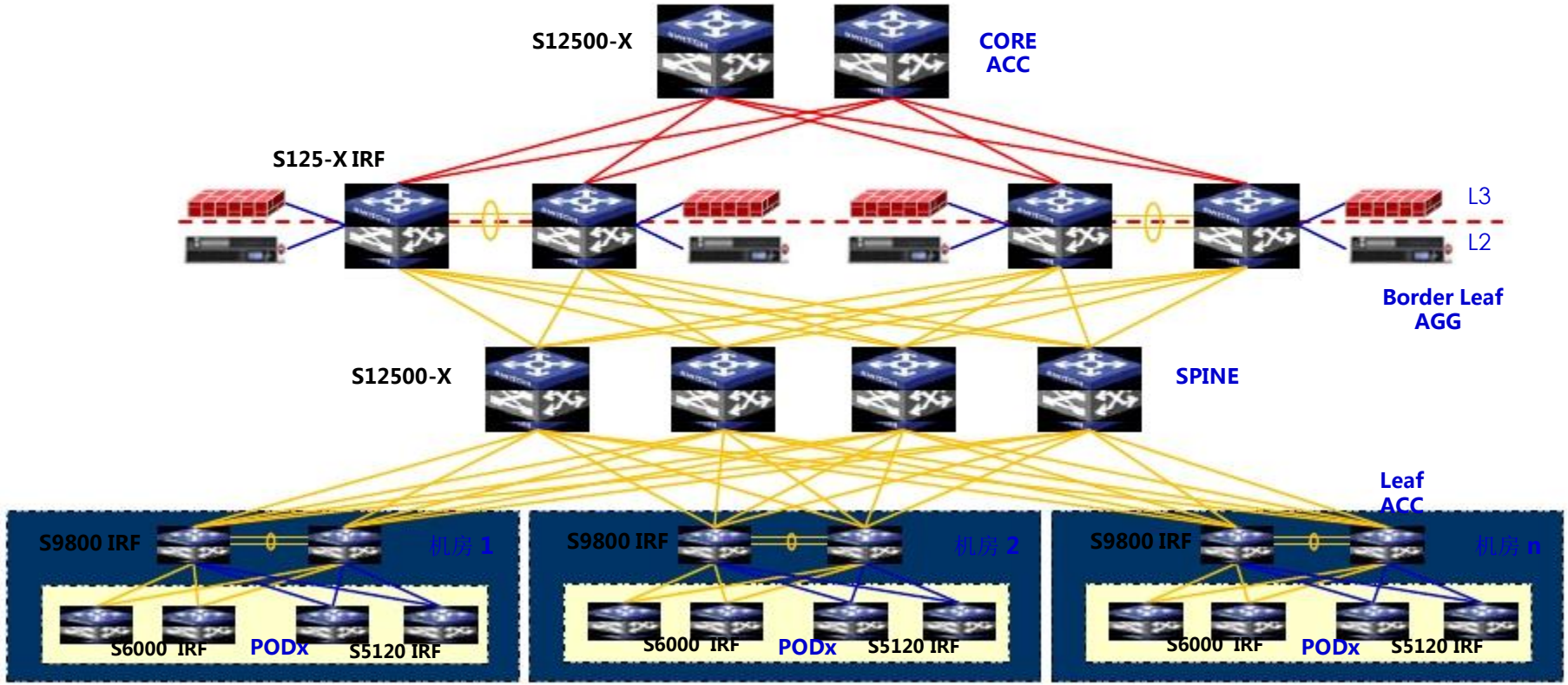
•Edge/Line Card 上根据原始报文查表(L2/L3)，

•如果要跨Line Card，则做类似Overlay的封装处理，BCM的Higig头占用的帧间隙，将Ethernet Overlay;

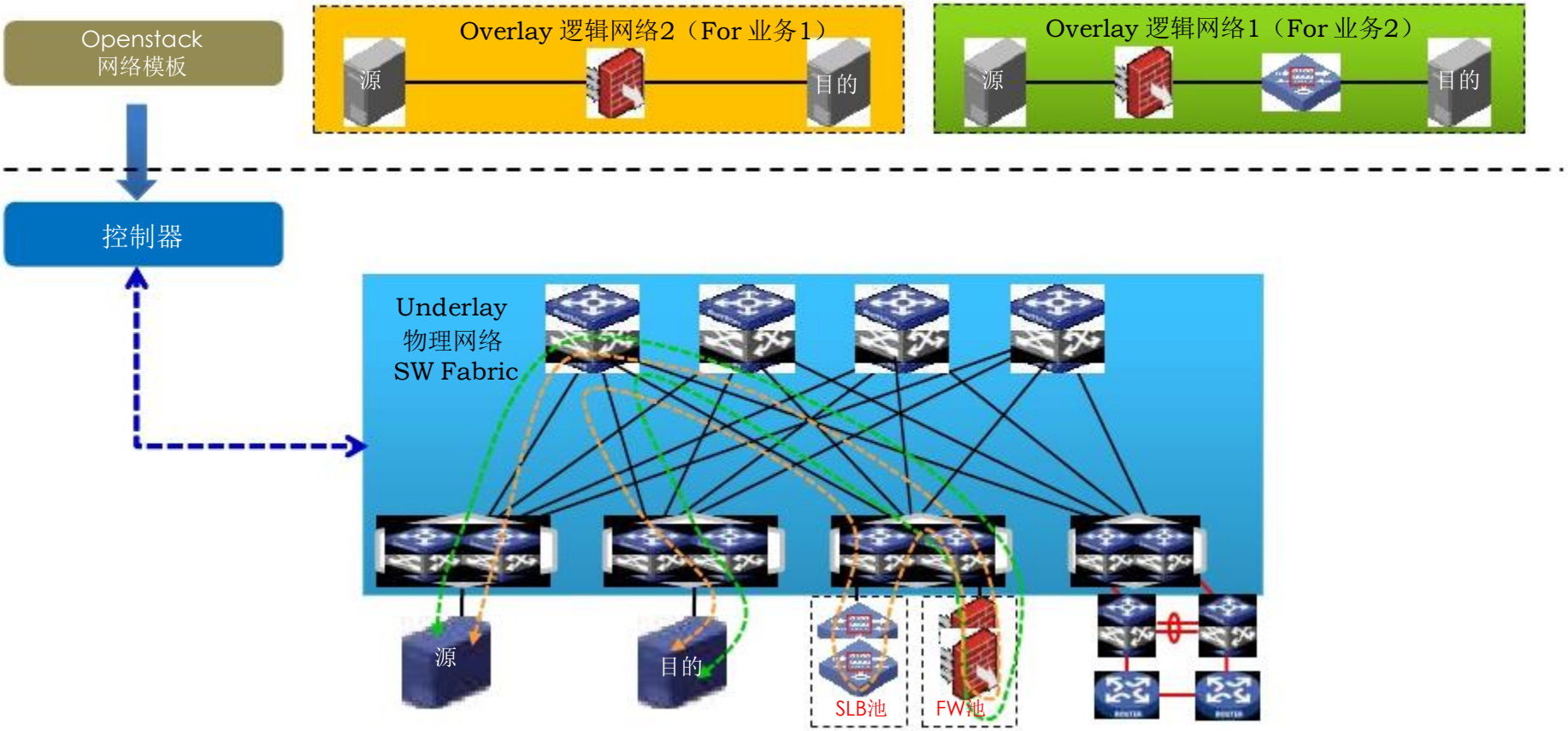
•Fabric 根据Overlay/Higig 中的Module和Port信息将Overlay的报文转发到相应的Line Card；

•地址在Line Card上分布学习，并通告主控，有主控统一下发转发信息

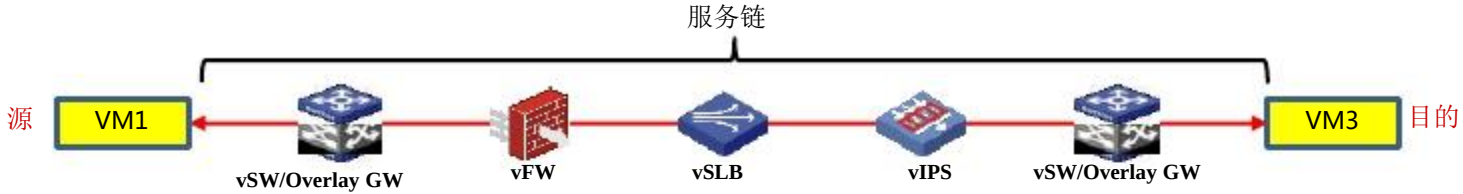
Overlay SDN架构的数据中心网络拓扑



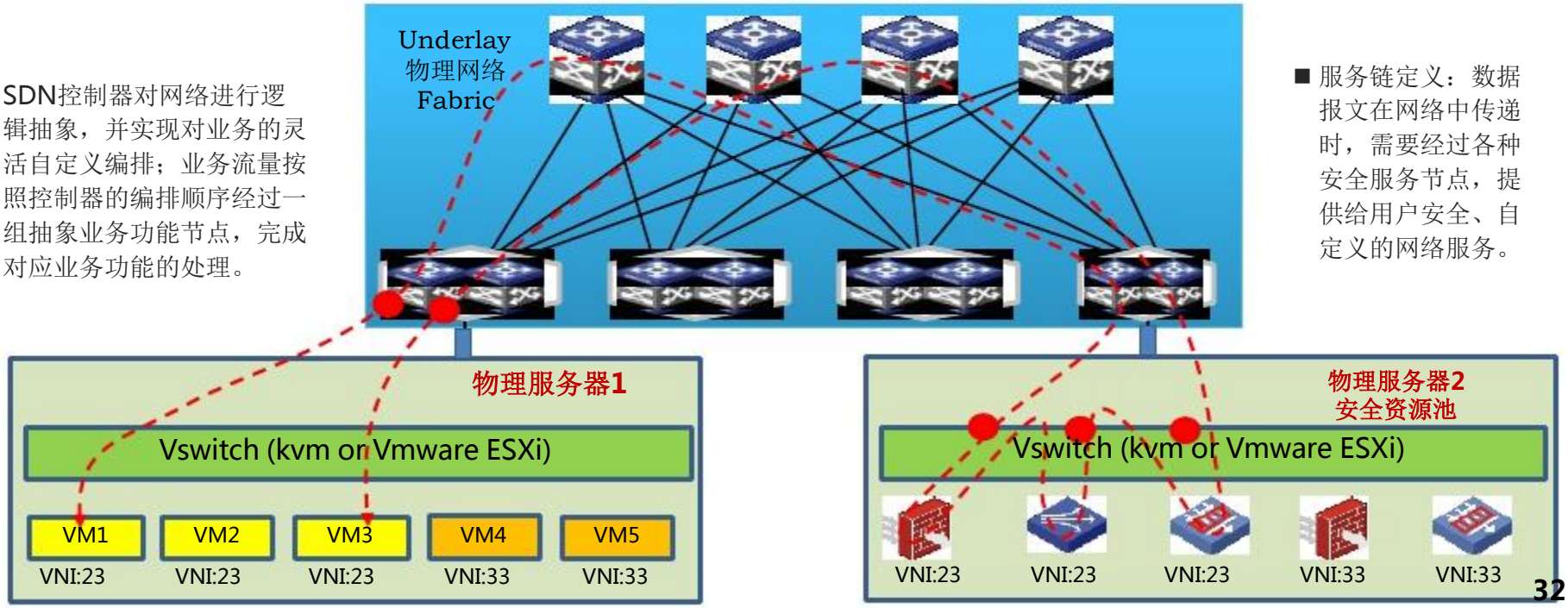
Overlay SDN的应用场景



Overlay SDN与 服务链技术



■ SDN控制器对网络进行逻辑抽象，并实现对业务的灵活自定义编排；业务流量按照控制器的编排顺序经过一组抽象业务功能节点，完成对应业务功能的处理。



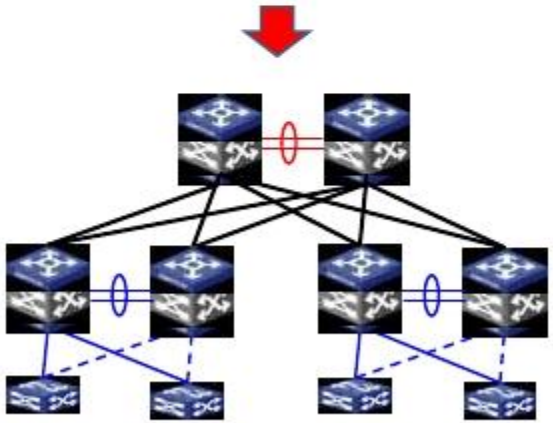
■ 服务链定义：数据报文在网络中传递时，需要经过各种安全服务节点，提供给用户安全、自定义的网络服务。

近年数据中心网络的变化

- 传统网路架构

以前SRF的应用模式

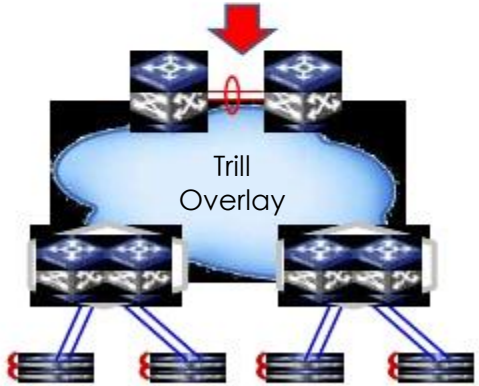
分区内部分是个Switch Fabric，采用横向虚拟化



- 从物理分区到逻辑分区解耦和

当前SRF的应用模式

通过TRILL 整合多个分区，分区整合变少，整个分区是个Fabric



- 数据中心网络多租户、安全资源灵活调配（服务链）

未来几年DC的规划方向

SDN Overlay

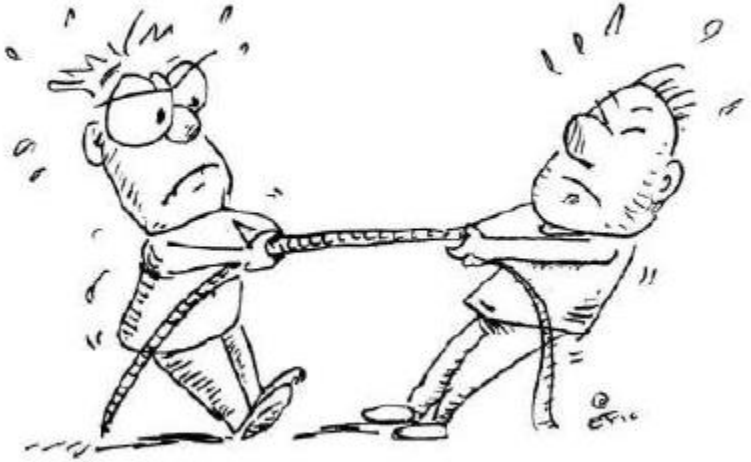
支持Service chaining 的 SIA

Overlay SDN标准化问题

IETF

VXLAN

NVGRE



LISP

MPLS

STT

TRILL

从三要素对 OVERLAY SDN 的小结

- 架构角度：只将overlay 隧道的控制平面上收到控制器，隧道的动态创建以及 L2 overlay网络的MAC地址、ARP处理由控制器 处理。而Underlay 的控制层仍然是传统的分布式处理模式。数据平面由网络设备或虚拟网络设备（vswitch /vRouter）处理。
- 业务角度：通过隧道（overlay）隧道实现两个网络设备之间的逻辑连接，与Forwarding Plane SDN不同，overlay SDN 只需要在两个有连接需求的设备间下发相关的转发表项，而中间的网络对Overlay隧道透明。
- 运营角度：控制器对网络设备（包括虚拟网络设备）的编程接口没有标准（这一点与Openflow SDN不同）。各厂商的实现有很大差异，利用OF-Config + NETCONF或OVSDB+NETCONF 实现编程接口；思科利用私有的OPFLEX 实现接口。但都要求接口是双向互通的，是应用程序（即控制器）与网络设备紧密关联。

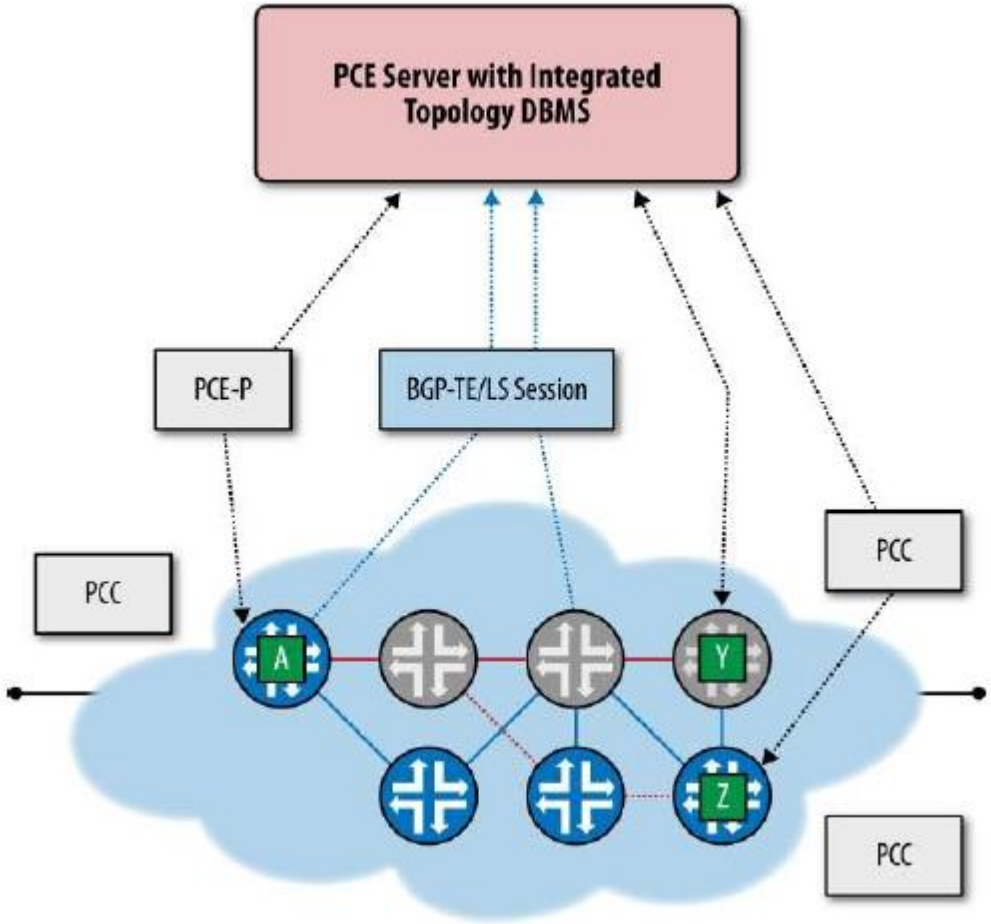
- 与Forwarding Plane SDN相比，控制平面的含量更高，网络抽象度提高？？？？

VXLAN Overlay SDN 的局限

- 控制平面的处理没有标准化，无法实现跨厂商互通
- VXLAN 协议还在改进中，当前的VXLAN overlay 通常是通过 host overlay 实现，硬件芯片的实现还有些缺陷，因为芯片厂家也在等待协议的标准化进度。
- 用host overlay在性能上略差。

（三）控制平面型SDN的模型

- 传统的网络厂商提出了“控制平面型SDN”，它关注现有的IP/MPLS RIB的可编程性。
- 假定现有的分布式控制的网络已经具备，通过对设备表项的编程，优化或简化网络操作。
- 只将很少一部分控制平面（如，路径计算/LSP）拿到外部（典型的SDN-PCE技术）。
- 由于只对控制平面做调整，抽象层次度更高，所以称为控制平面型 SDN

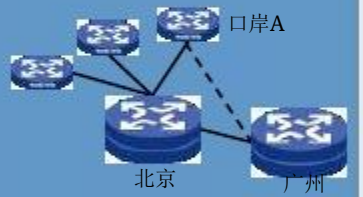


控制平面型SDN的需求场景 —— TE

A

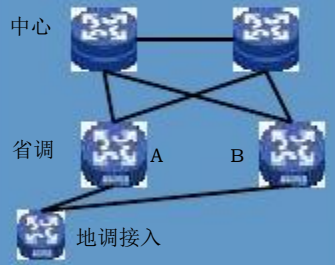
重点业务：视频会议
业务需求：在召开视频会议时使用，启动视频专线。在不召开视频会议的时候，可以自动调整传输其他数据。

B



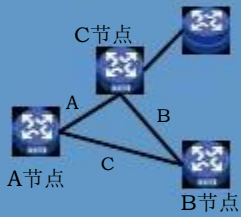
重点业务：数据上报
业务需求：从口岸上报北京数据中心的数据，走最短链路到北京数据中心。需要在该链路带宽占尽的情况下，绕道广州送到北京数据中心。

C



业务需求：业务分类
业务需求：对上传数据数据进行应用识别，带宽占用并可视化，根据链路健康状况自动根据优选策略在A/B进行选路。

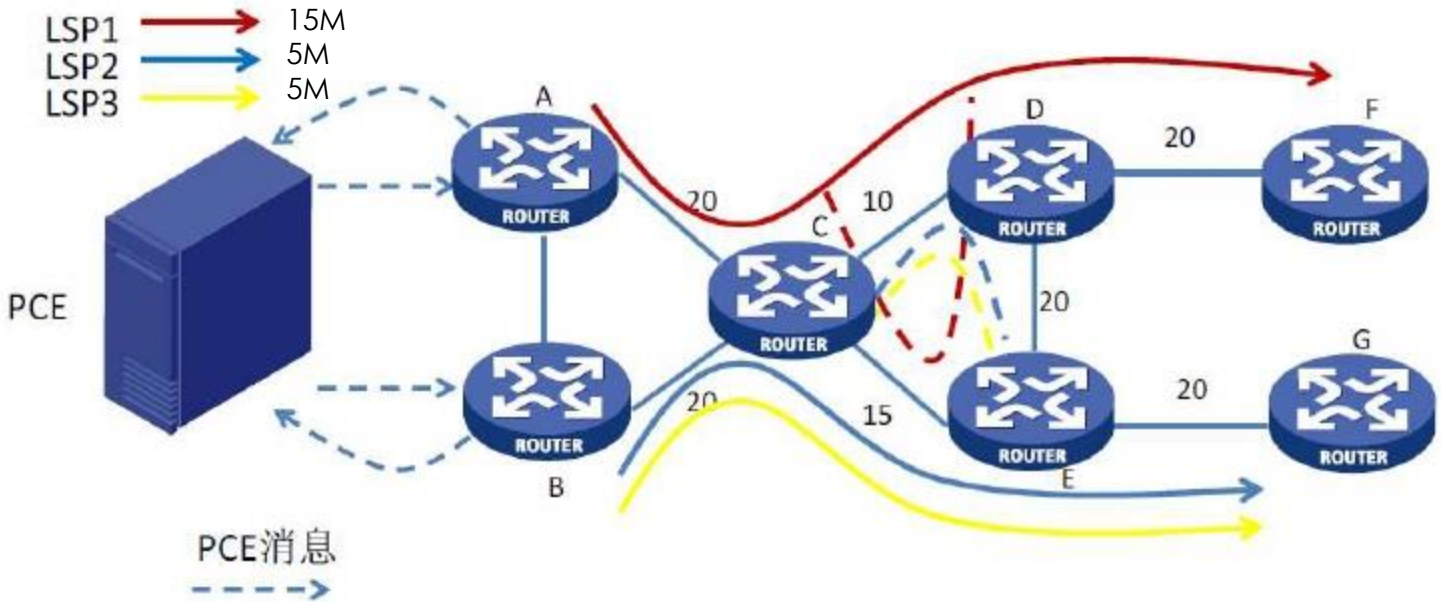
D



业务需求： C节点到A节点正常情况走A链路，需要在有突发流量，A链路带宽占尽的情况下，多余流量走B--->C链路到A节点。

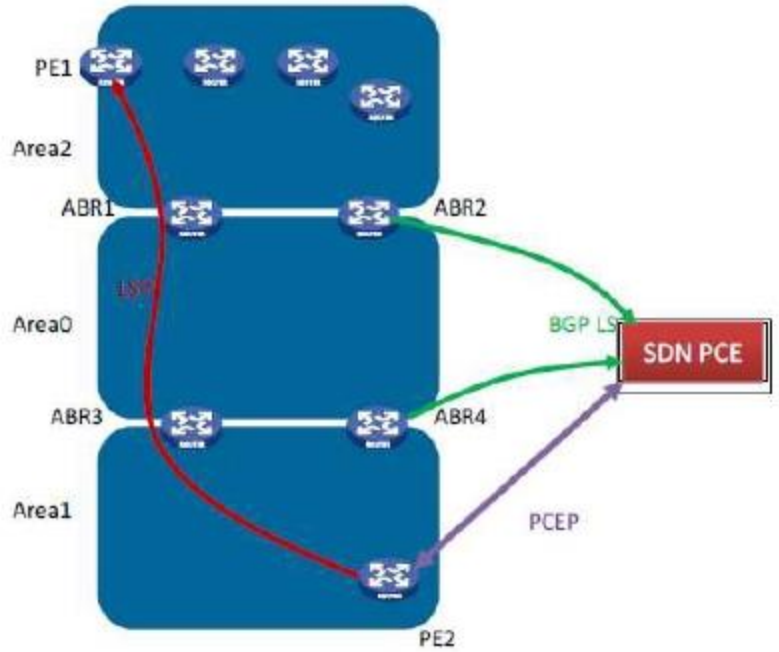
传统MPLS TE 的Bin-paking 问题及PCE技术

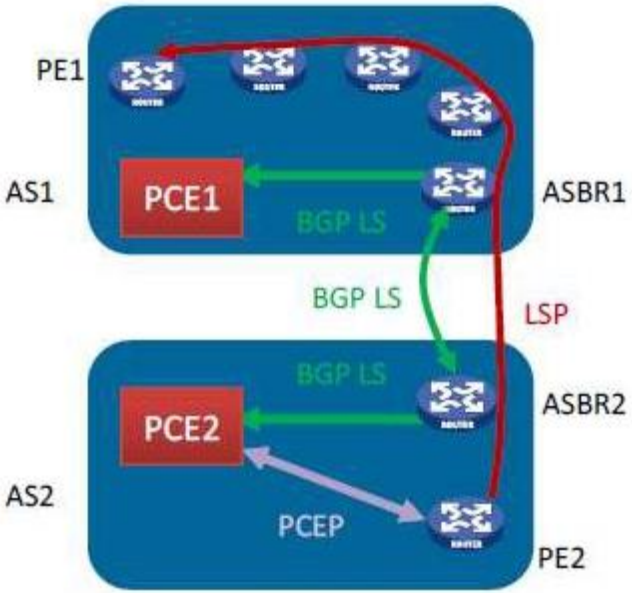
- LSP的优先级与抢占机制，耦合了么个入口路由器的路径选择；
- 由于RSVP的特性，导致无法充分利用带宽，产生bin-packing 问题。通常需要用复杂的带宽计算规划工具明确LSP的优先级，然后配置管理这些个LSP。也可以直接计算LSP，直接下发标签。
- PCE技术（RFC4655）允许将这些LSP的计算过程放在一台服务器上(Controller)处理，而且面向应用开放API编程。其实PCE本身不是SDN技术，但如果PCE服务器作为可编程的控制器，则PCE就成了支撑控制平面型SDN的技术；



PCE中的路径拓扑发现问题

- PCC请求计算需要了解网络中PCE的位置。PCE是在IGP协议发布范围内的LSR时,通过IGP泛洪PCE信息。
- PCE只能搜集到域内的联通纤细和TE信息。对于跨域场景，BGP LS（Link-State Info Distriution using BGP）协议通过一个新的BGP NRLI实现链路状态和TE信息分发。 BGP从IGP LSDB中检索联通属性，并通过BGP Speaker 发送给链路信息的使用者。





从三要素对 控制平面型SDN的小结

- 架构角度：只将很小的一部分控制平面提出到控制器中，
- 业务角度：对网络的抽象在于RIB，抽象层次更高。可以用来简化网络设备的处理，比如说代替设备的 LDP或rsvp来下发标签
- 运营角度：PCE Server 通过PCE-P 协议与设备（PCC）互联。

- “控制平面型SDN”不对数据平面由改动，只要设备升级软件即可支持，控制平面集中度很高，网络抽象度也很高。
- “控制平面型SDN”的思路是尽量不去改变设备的硬件。这一点与“转发平面型SDN”不同。

控制平面型SDN 的局限性

- 应用场景有限，目前主要是简化广域网“流量工程TE”配置，
- 思路： 计算全网拓扑，之后根据应用的编程需求，调整网络；
- 调整网路能否通过传统的命令行？
  - 命令行不是直接修改转发表项，需要协议重新收敛，不能响应实时流量调整
  - 所以需要能修改设备的转发表项的协议

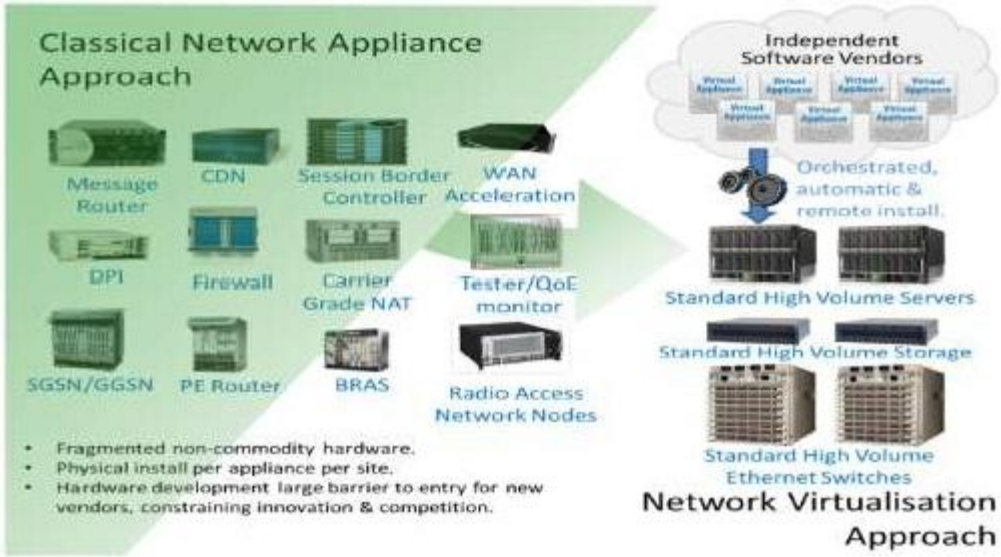
- PCE-P，修改转发路径的协议
- BGP TE/LS，获得全网路径（跨域）的协议，草案，只有厂商的支持，还未标准化。

目录

- 关于SDN 与可编程网络
- 各种SDN技术思路、应用场景、标准化情况介绍
  - 转发平面 SDN —— Openflow
  - Overlay SDN —— Vxlan Overlay
  - Control Plane SDN（控制平面SDN）
  - Network Function Virturlization （NFV）
  - SDN控制器（ Open Daylight ）
- 各厂商SDN方案介绍
- 展望SDN的发展

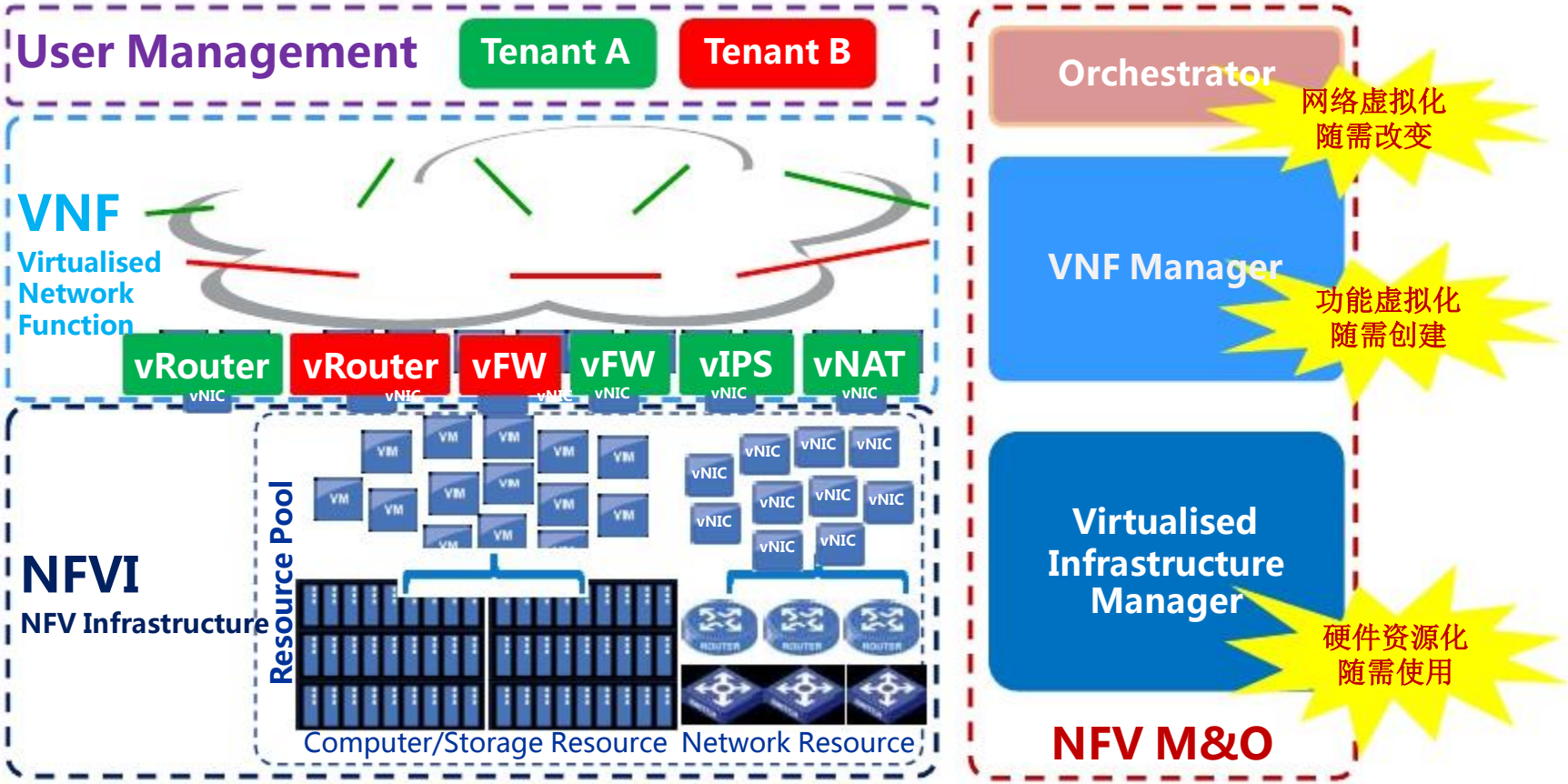
NFV的起源

NFV (Network Functions Virtualizations) 是欧洲电信标准协会 (ETSI) 的一个ISG，在2012年10月，由AT&T、BT、DT、Orange等运营商发起成立，目前已有超过150家运营商、设备供应商、IT设备供应商以及技术供应商参加。

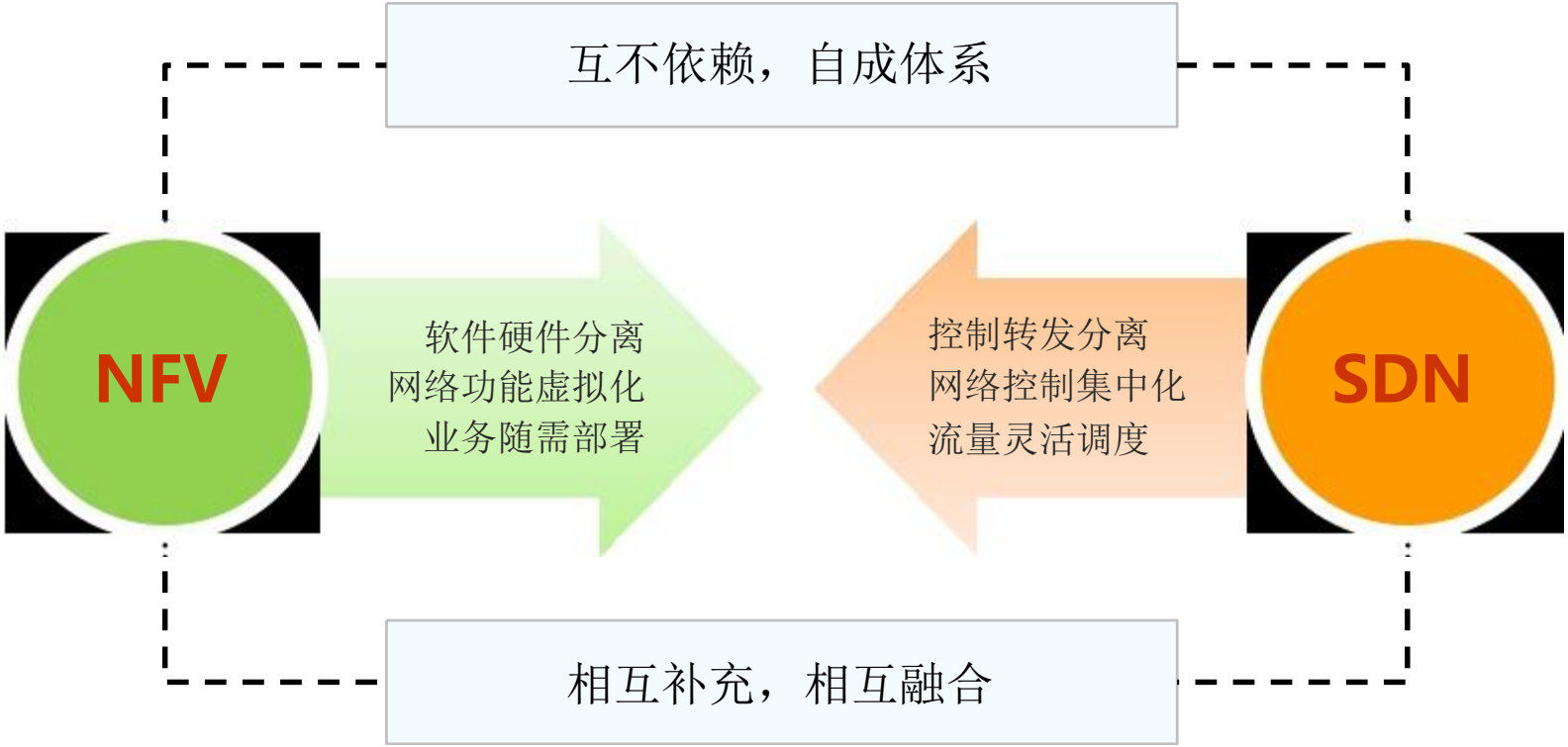


- 用标准服务器、虚拟化、云计算等IT技术
- 将软件、硬件解耦：
  - 硬件标准化，使网络功能不再依赖于专用硬件
  - 软件虚拟化，可以运行在任何标准虚拟化环境中

NFV框架具现

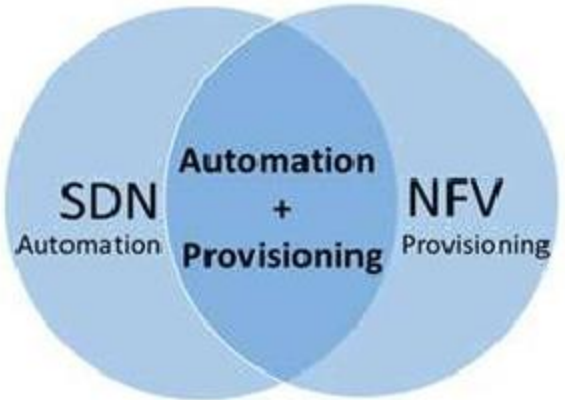

User Management
Tenant A
Tenant B
VNF
Virtualised Network Function
vRouter
vRouter
vFW
vFW
vIPS
vNAT
vNIC
NFVI
NFV Infrastructure
Resource Pool
VM
Computer/Storage Resource
Network Resource
Orchestrator
网络虚拟化
随需改变
VNF Manager
功能虚拟化
随需创建
Virtualised Infrastructure Manager
硬件资源化
随需使用
NFV M&O

NFV与SDN


互不依赖，自成体系
NFV
软件硬件分离
网络功能虚拟化
业务随需部署
控制转发分离
网络控制集中化
流量灵活调度
SDN
相互补充，相互融合

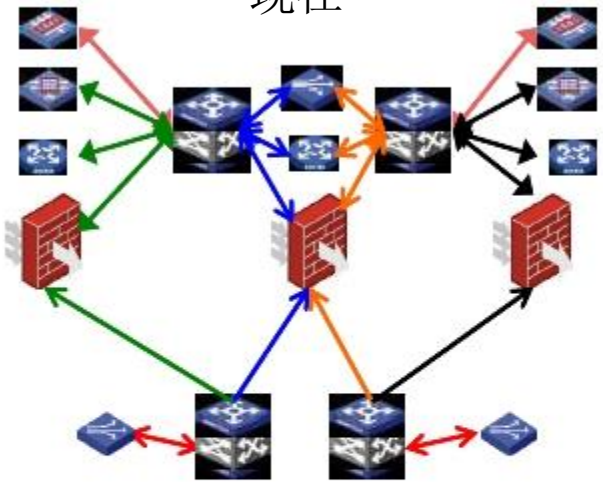
SDN + NVF —— 网络安全架构新思路

- SDN（Openflow、Overlay）
  - 为现有的网络设备提供网络“自动化功能”；
  - 通过Controller可以实现对整个网络转发策略的“统一快速部署”；
  - 解决传统安全部署时的“拓扑依赖”问题；
- NFV提供自动部署（以及不需要时删除）虚拟网络设备的能力
  - 虚拟设备包括虚拟交换机和路由器、杀毒、入侵检测及/或防御设备、防火墙、负载均衡等。
  - NFV提供了安全设备的“弹性扩展”及“快速交付”能力；

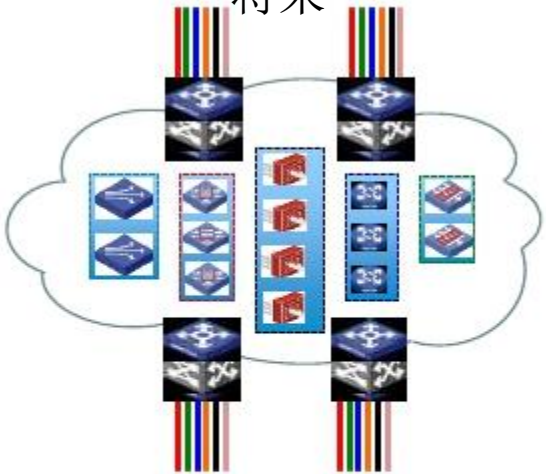


网络安全架构演化 —— 自动化、资源弹性、无拓扑依赖

现在



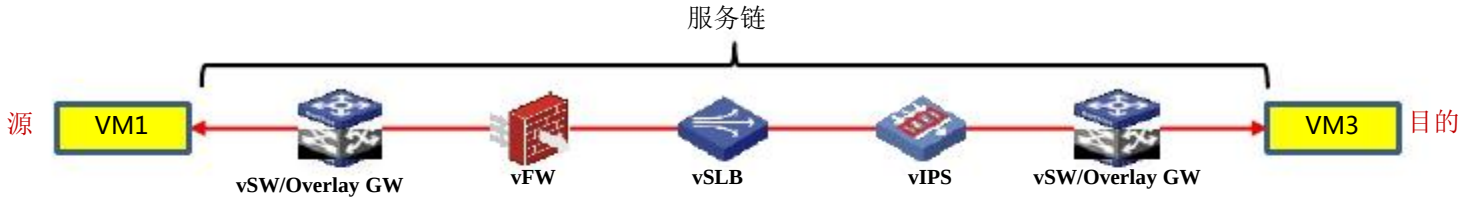
将来



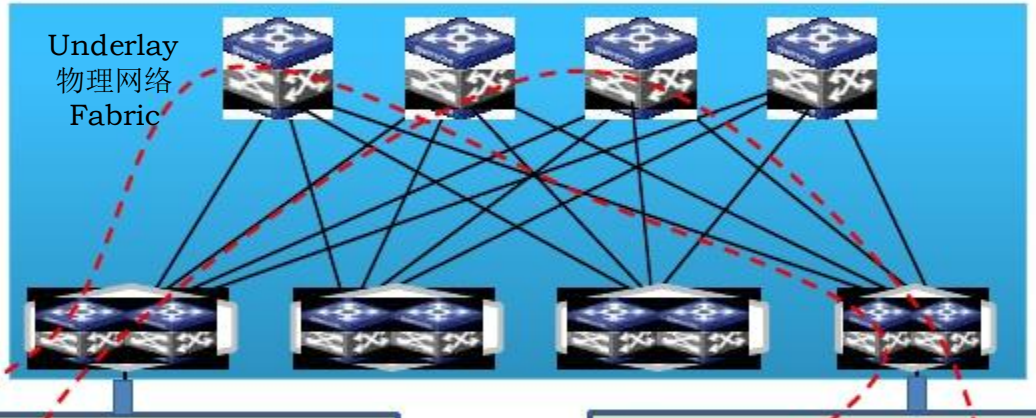
- 流量走向依赖于拓扑结构，各种的手工配置方式
  - VLAN GW、MDC、PBR、 Src-NAT
- 静态、分散的配置方式
- 设备处理能力不可复用，单设备纵向扩展

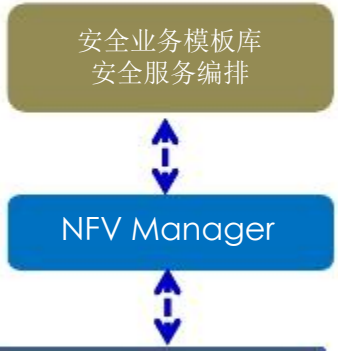
- 服务不依赖于拓扑结构
  - 安全以“服务方式”交付，云模式
  - 云服务的特点：自动快速部署
- 自动化，统一配置和统一的管理
- 安全处理能力具有弹性和横向扩展能力

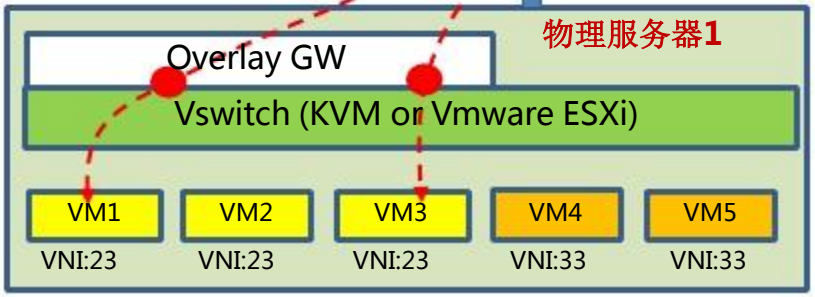
用X86 服务器 NFV 实现 “安全池”

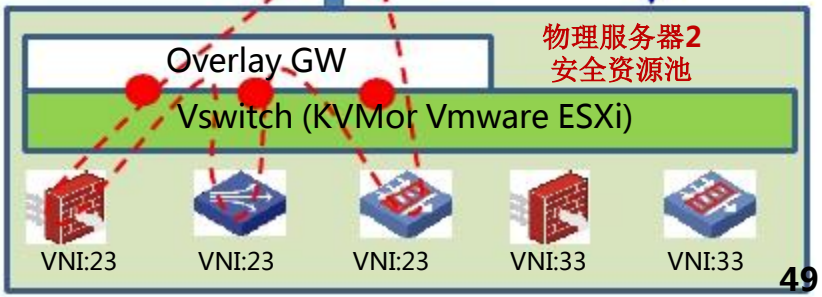


- 用X86服务器NVF实现虚拟安全池的最大好处是横向扩展性好；
- 还通过 NFV Manage 可实现虚拟安全池的快速部署及资源弹性管理；
- 这种虚拟化安全池适合在云计算中心部署；

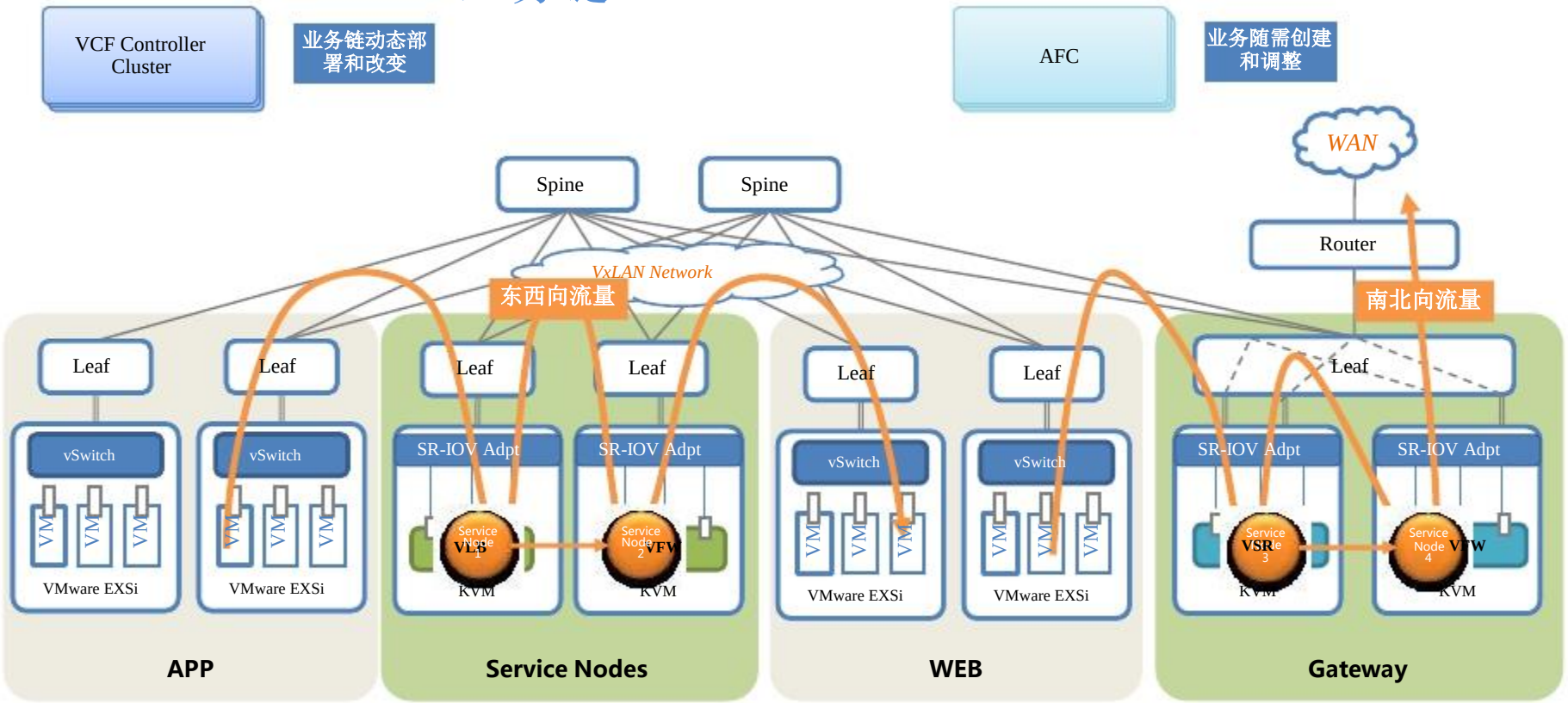




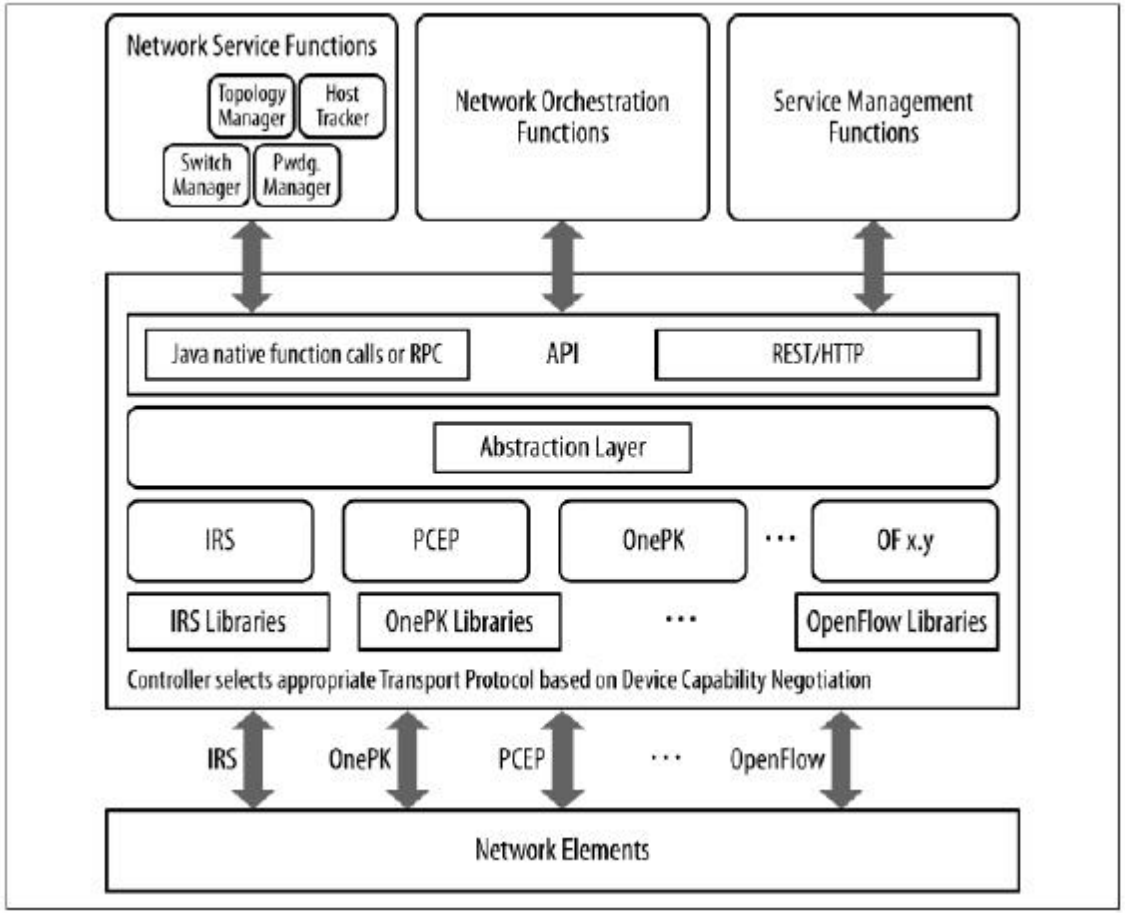




用X86 服务器 NFV 实现“安全池”
DC Service Chain业务链

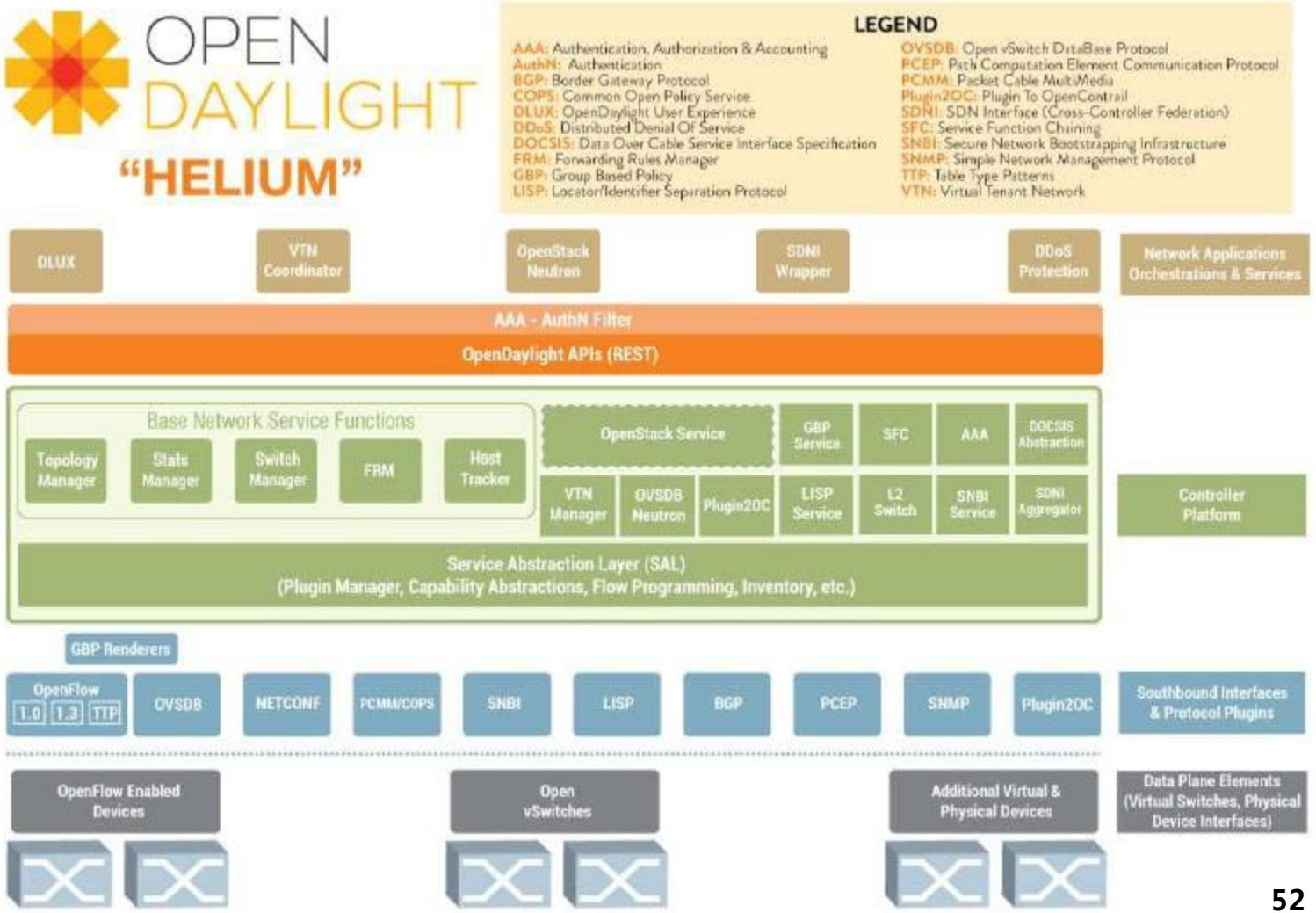


SDN Controller/控制器 的逻辑架构



- 对SDN技术的讨论，实际上是对网络状态管理的讨论，而网路状态管理正是SDN控制器的角色。
- SDN控制器是提供以下功能的软件系统或者是软件系统的集合：
  - 网络状态管理。
  - 数据模型（网络的抽象），描述被管理的资源、策略和控制器提供的其他服务
  - 北向，通常是RESTful API来将控制器的服务提供给应用程序使用
  - 安全控制会话
  - 南向，一个基于标准的、用于在网元设备上配置应用驱动的状态协议
  - 一个设备、拓扑和服务发现协议

关于SDN控制器的标准化思路



目录

- 关于SDN 与可编程网络
- 各种SDN技术与应用场景介绍
- 各厂商SDN方案介绍
  - CISCO ACI 方案
  - Vmware NSX 方案
- 展望SDN的发展

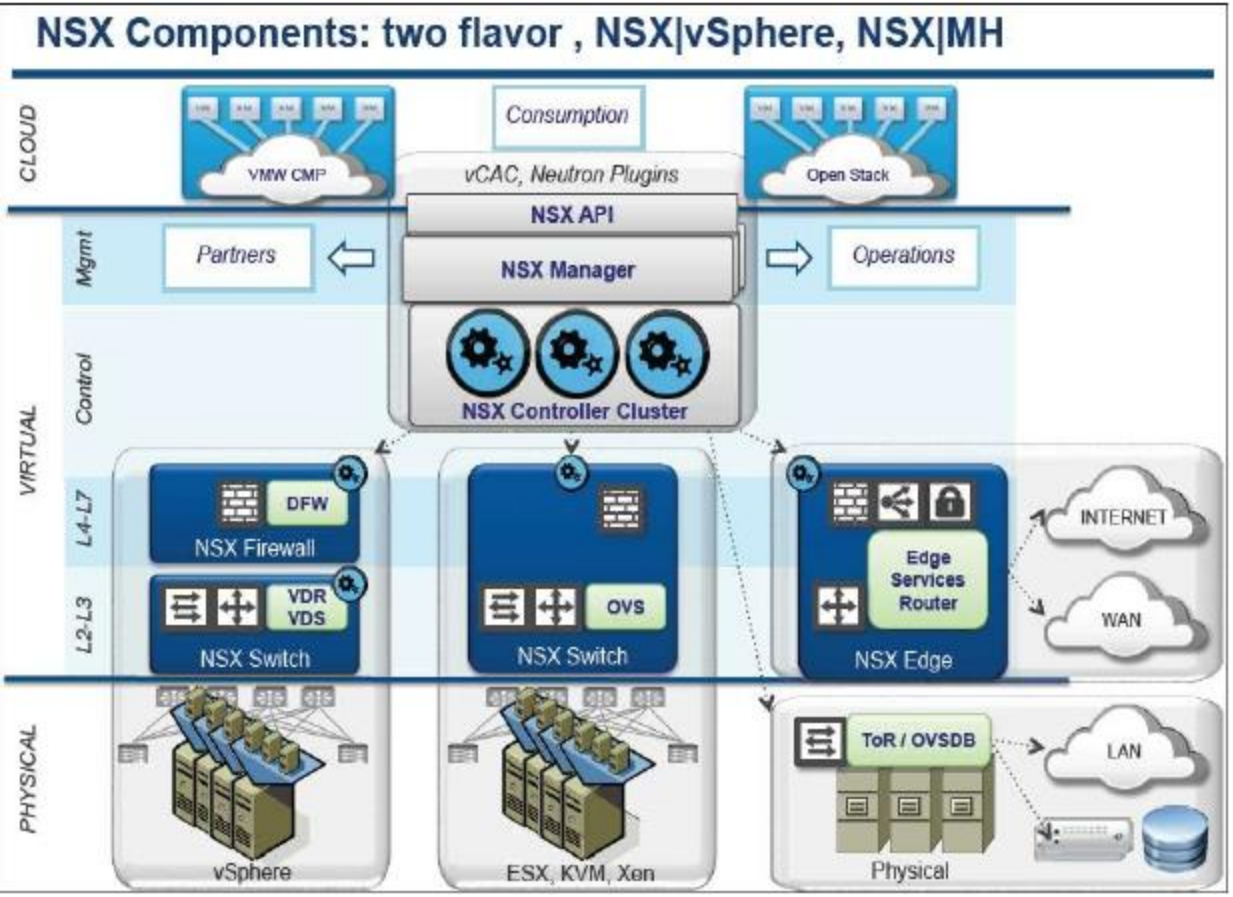
Cisco ACI方案简介

2013.11.6 Cisco并行了Application Centric Infrastructure(ACI)新案和Nexus 9000系列交换机的发布会。钱伯斯发表了“Redefining the Power of IT”的主题演讲：ACI将开启敏捷与自动化数据中心的新纪元。

ACI Fabric 小结

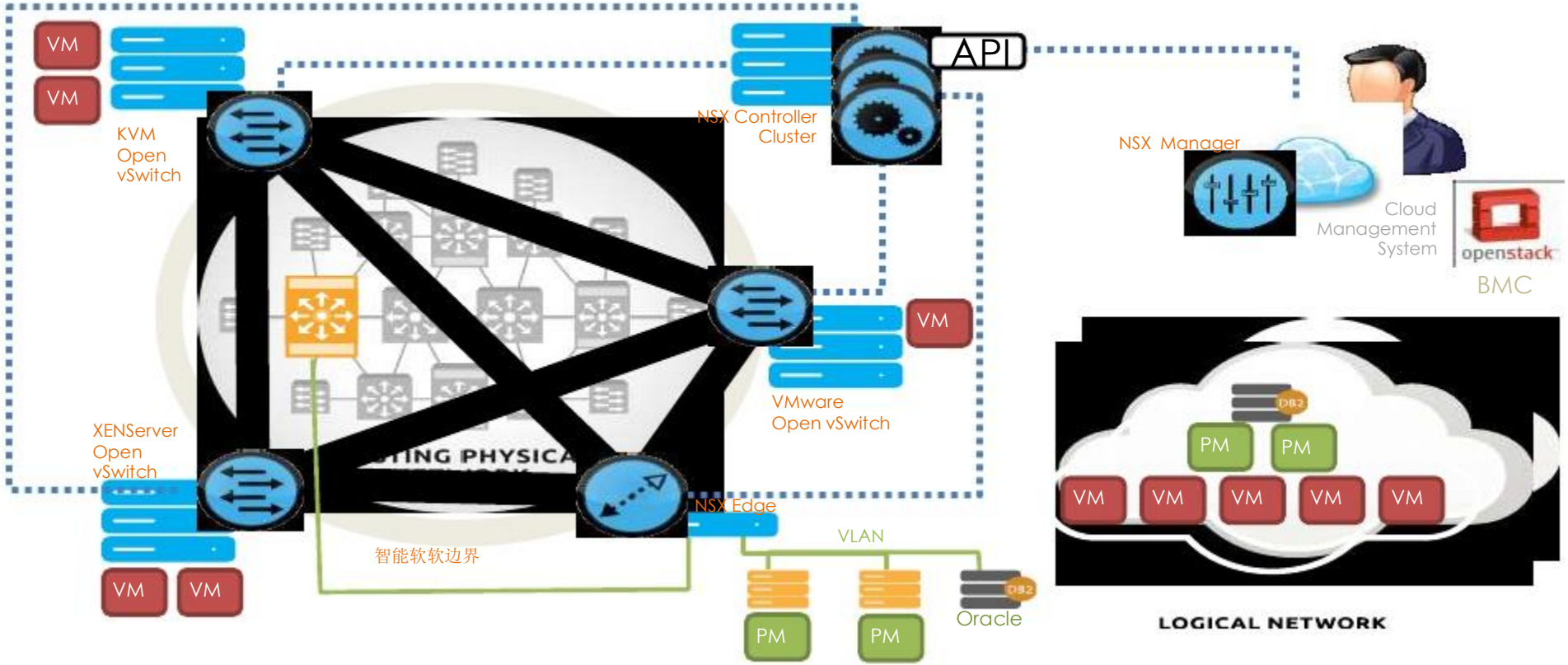
- 基于扩展的VXLAN overlay的Fabric方案
  - Any workload，anywhere：通过VXLAN overlay实现标识与位置解耦
  - Any service，Anywhere，以及service chaining：通过扩展的VXLAN实现标识与策略解耦
  - 自动化构建Fabric，无需手工配置VTEP的IP地址及路由等
  - 交换机之间采用控制平面协议进行转发表的同步，而不是控制器集中下放的方式
  - 支持报文归一化封装，兼容VXLAN和GRE
- 分布式L3网关，转发路径最优，无需配置VRRP等冗余协议
- 扩展性强：最大220K 10G端口，1M+端口IP，64K+ Tenant
- Telemetry：支持所有Leaf节点之间各个路径的丢包统计和时延测量

VMware NSX方案简介



- 2013年8月26日在旧金山举办的VMworld®大会上，VMware宣布推出网络虚拟化平台VMware NSX™
- Vmware NSX提供了一整套简化的逻辑网络连接元素和服务，包括逻辑交换机、路由器、防火墙、负载均衡、VPN、服务质量、监控和安全保护。
- VMware NSX的目标是提供网络虚拟化，将网络虚拟化操作从底层硬件虚拟化，抽象为一个分布式虚拟层，很像用于处理能力和运营系统的服务器虚拟化，而不用命令行接口或其它直接管理员的干预。

NSX如何工作？


VM
VM
KVM
Open
vSwitch
API
NSX Controller
Cluster
NSX Manager
Cloud
Management
System
openstack
BMC
VM
VMware
Open vSwitch
XENServer
Open
vSwitch
VM
VM
智能软软边界
NSX Edge
VLAN
PM
PM
Oracle
PM
PM
VM
VM
VM
VM
VM
LOGICAL NETWORK

NSX 小结

- 统一界面,统一管理：交换机、防火墙、Edge等
- NSX设备套件涵盖全部的网络安全设备：FW、LB、VPN、L2、L3等
- 多hypervisor融合：与vSphere融合、与第三方Multi-Hypervisor，
- NSX逻辑网络具备分布式，多功能：在vSphere平台，可以集成VDR、VDS、DFW
- 高性能：30T，支持基于VM名称、用户ID
- Edge为虚机存在，支持双机器部署，运行状态同步，可利用vSphere HA
- NSX Controller使用Vmware应用级APP，数据层独立。