SDN在云计算中的应用

QQ：67278439
新浪微博：@盛科张卫峰




Topic

centec networks

- SDN对云计算网络很重要
- 当前OpenStack Neutron的问题
- SDN网络虚拟化方案一览
- 盛科DVNP架构和应用场景

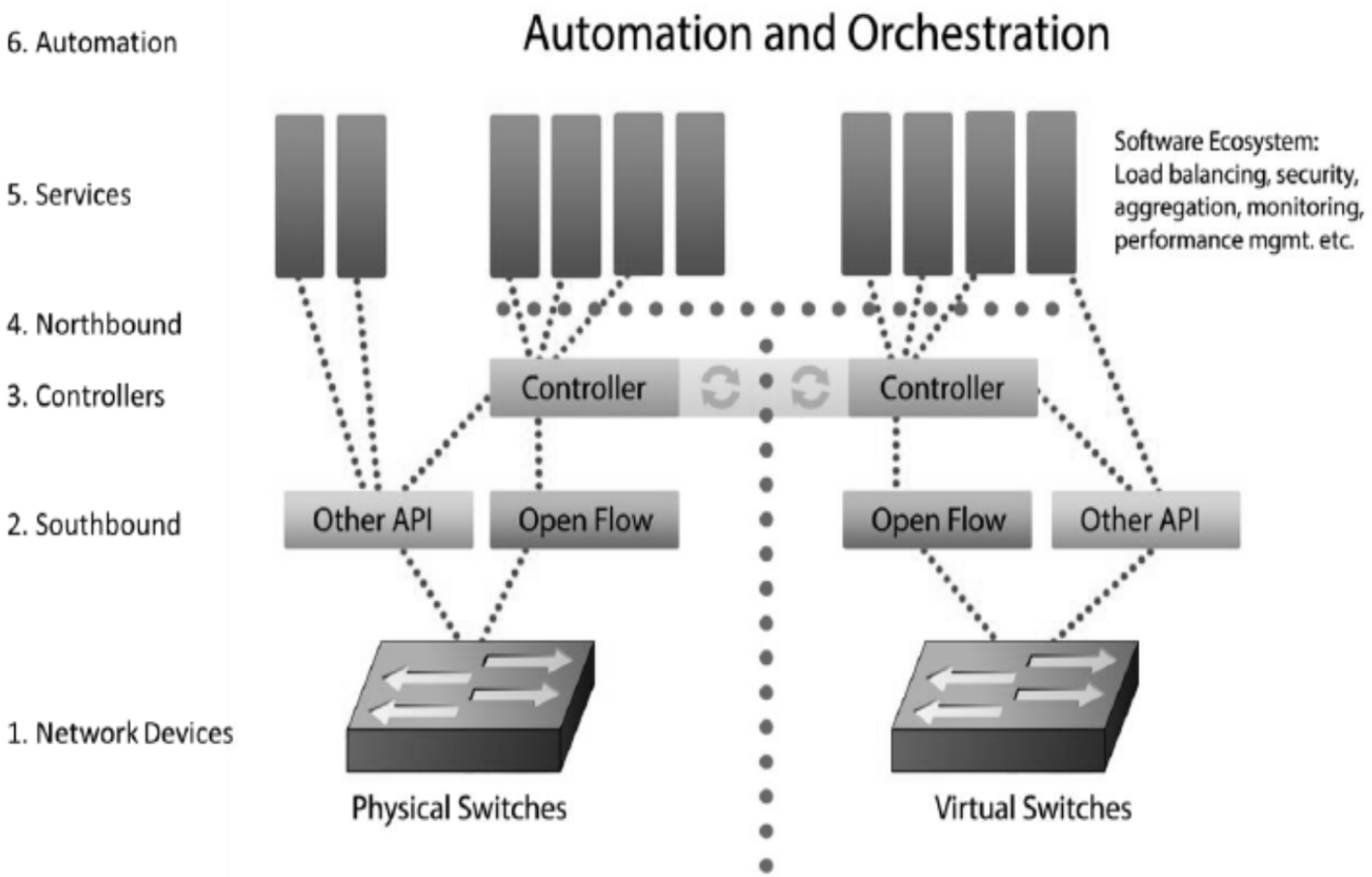
SDN是一种思想

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架构


6. Automation
Automation and Orchestration
5. Services
Software Ecosystem:
Load balancing, security,
aggregation, monitoring,
performance mgmt. etc.
4. Northbound
3. Controllers
Controller
Controller
2. Southbound
Other API
Open Flow
Open Flow
Other API
1. Network Devices
Physical Switches
Virtual Switches

SDN的本质属性

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

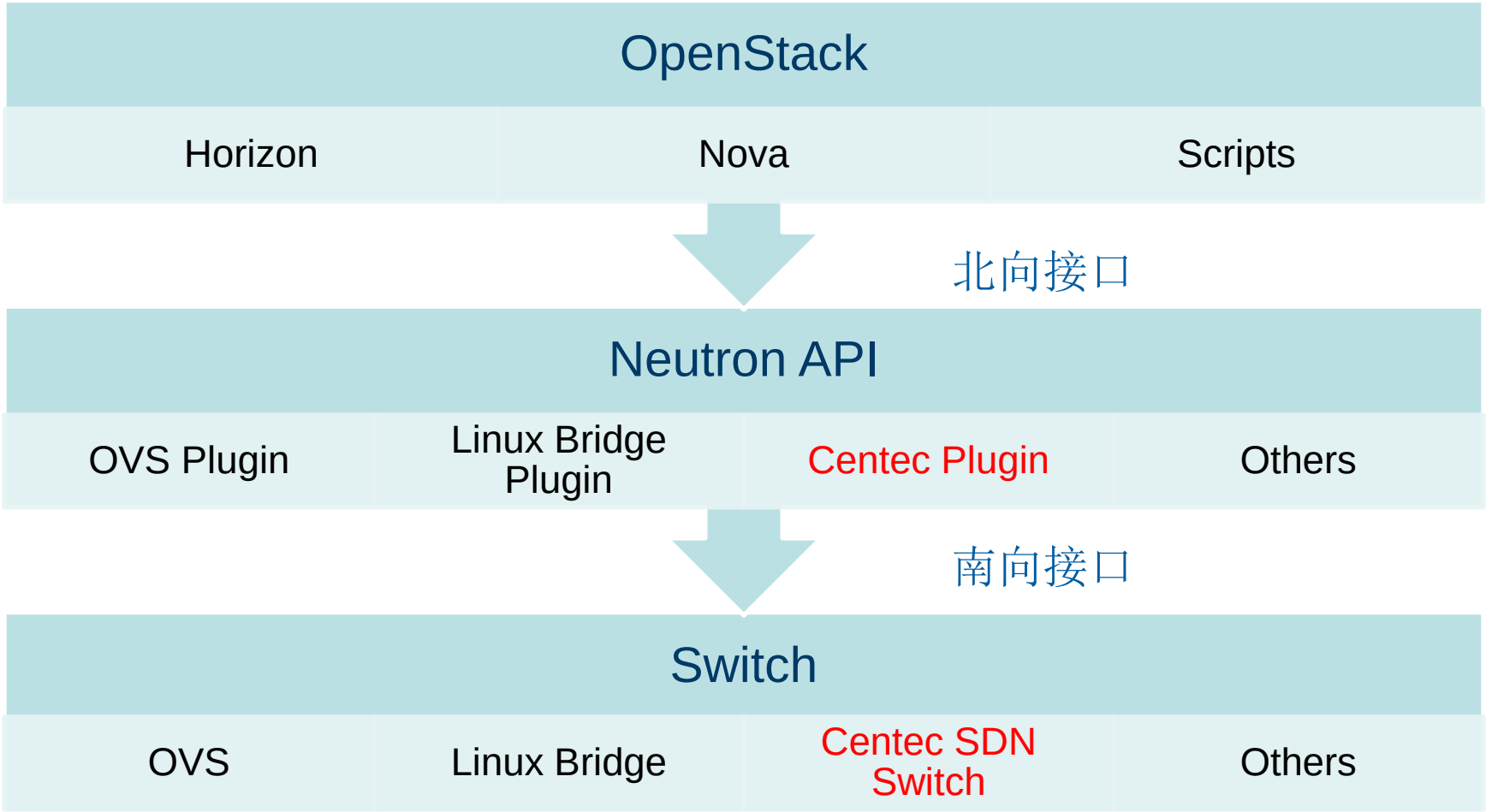
不是让控制器控制一切

而是让控制器去控制用户想控制的部分

IaaS云计算网络将SDN的优势发挥到极致

- **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）
- **可编程API**
  - 提供租户的self-service
- **集中化控制**
  - 云计算平台获取全局信息

OpenStack网络架构



Topic

centec networks

- SDN对云计算网络很重要
- 当前OpenStack Neutron的问题
- SDN网络虚拟化方案一览
- 盛科DVNP架构和应用场景

两种组网方式的比较

- **Vlan组网**
  - 优点
    - 简单、稳定、高性能
  - 缺点
    - 4K Vlan数量限制
    - 需要在所有物理交换机的所有端口上预配置所有Vlan
    - 物理网络拓扑必须是大二层架构，难以处理更复杂拓扑

- **Tunnel组网**
  - 优点
    - 灵活性高，底层拓扑无关
    - 租户数量可以高达16M
  - 缺点
    - Encap/Decap带来的性能损耗
    - 不方便将bare-metal server接入虚拟网络

Neutron当前的问题

- **J版本之前不支持DVR**
- **J版本支持DVR，但是**
  - 不成熟
  - DVR用了大量name space，比较重量级，规模大了有压力
- **Neutron自身对FwaaS、VPNaaS、Security Group等支持力度较弱**
- **数据校验和错误处理不严谨，容易发生数据不一致**
- **要基于VMware ESX/ESXi支持VPC，要么购买昂贵的NSX，要么用效率很低的方式来做**

Topic

centec networks

- SDN对云计算网络很重要
- 当前OpenStack Neutron的问题
- SDN网络虚拟化方案一览
- 盛科DVNP架构和应用场景

商业化SDN VPC解决方案

- 纯软件
  - Juniper Contrail
  - Vyatta(Brocade)
  - Nuage(ALU)
  - Midokura
  - PlumGrid
  - Centec
- 硬件+软件
  - Cisco ACI
  - Centec

虚拟三层路由转发

- 集中式虚拟网关
  - OpenStack Juno之前版本
- 分布式虚拟网关
  - OpenStack Juno版本
  - NSX，Contrail，Centec等商业软件
- 半分布式虚拟网关
  - 绝大多数宣称有VR的平台，如CloudStack，某些商业软件
- 分布式路由只管东西向三层，南北向还是要走集中网关

SDN网络虚拟化方案1：
--Neutron作为集中式控制器

centec networks

- Neutron拥有一切拓扑信息，通过plugin实时分发给相应计算节点Agent
- Agent根据packet学习创建二层转发流表
- Agent根据接收的拓扑信息操作kernel路由表，使用name space做隔离
- 典型代表是OpenStack Neutron原生态网络

SDN网络虚拟化方案2：
--独立的集中式控制器

centec networks

- Neutron拥有一切拓扑信息，全部发送给独立控制器
- 控制器将转换后的信息发送给计算节点Agent
- Agent根据控制器指令，proactive创建转发表
- Mismatch的报文送到集中控制器去学习
- 典型代表是Juniper Contrail

SDN网络虚拟化方案3：--分布式控制器

- Neutron拥有一切拓扑信息，通过plugin写到独立数据库
- 每个计算节点中的控制器向数据库服务器订阅本节点需要的数据
- 每个计算节点中的控制器reactive or proactive创建转发表
- Mismatch的报文在本地控制器学习
- 典型代表是盛科的DVNP(Distributed Virtualized Network Platform)
- 盛科的方案中，可选的还可以支持硬件Offload

SDN网络虚拟化方案4：
--集中式控制器+硬件转发

centec networks

- Neutron拥有一切拓扑信息，通过plugin发给控制器
- 控制器将拓扑信息发到物理Fabric网络（整个物理网络对外呈现为一个黑盒）
- 每台物理交换机里面的agent根据控制器发过来的信息，自行计算形成虚拟转发表，二层和三层
- 非虚拟化相关的物理转发表项由传统二三层协议形成
- 典型代表是思科的ACI

Topic

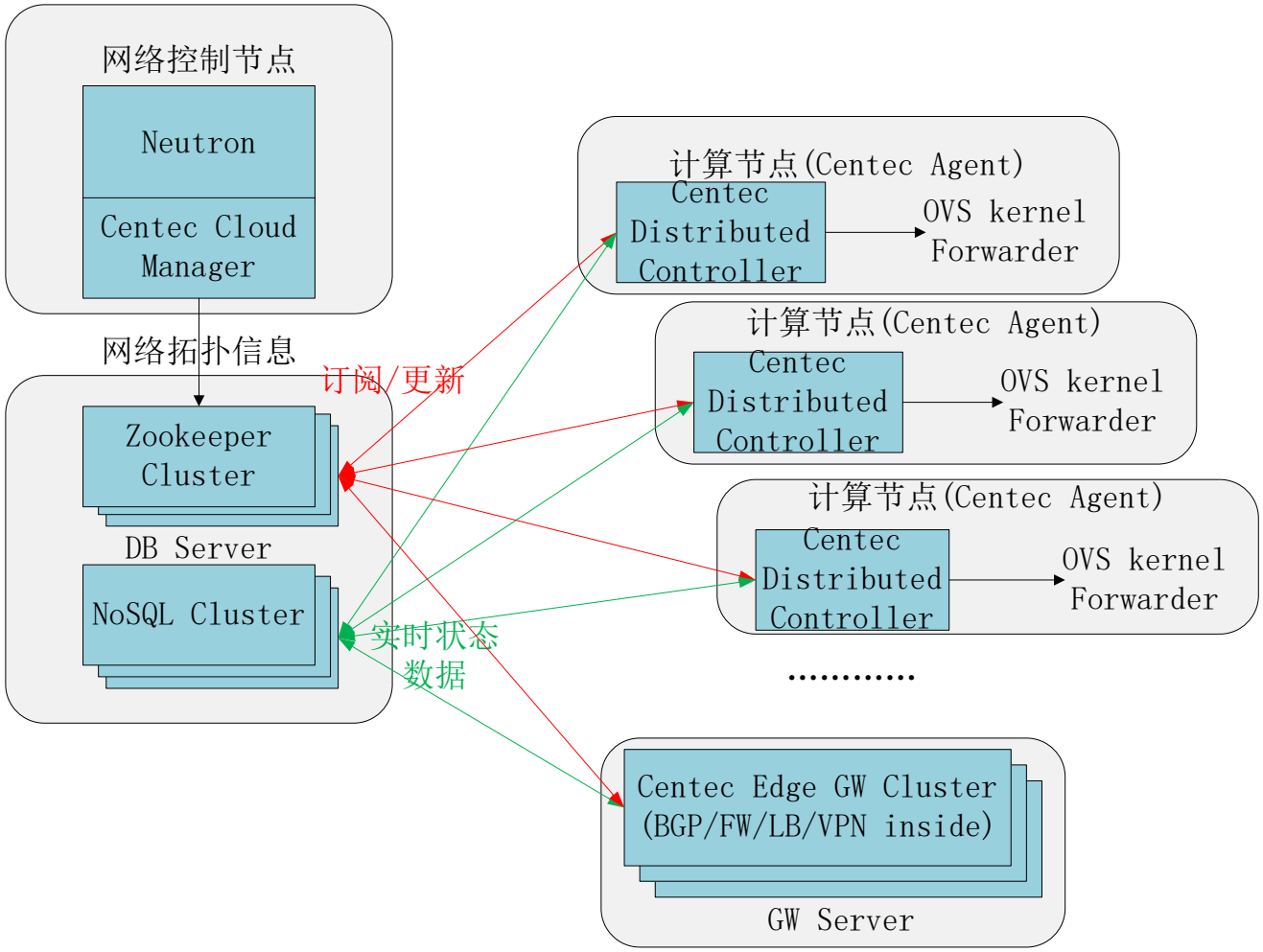
centec networks

- SDN对云计算网络很重要
- 当前OpenStack Neutron的问题
- SDN网络虚拟化方案一览
- 盛科DVNP架构和应用场景

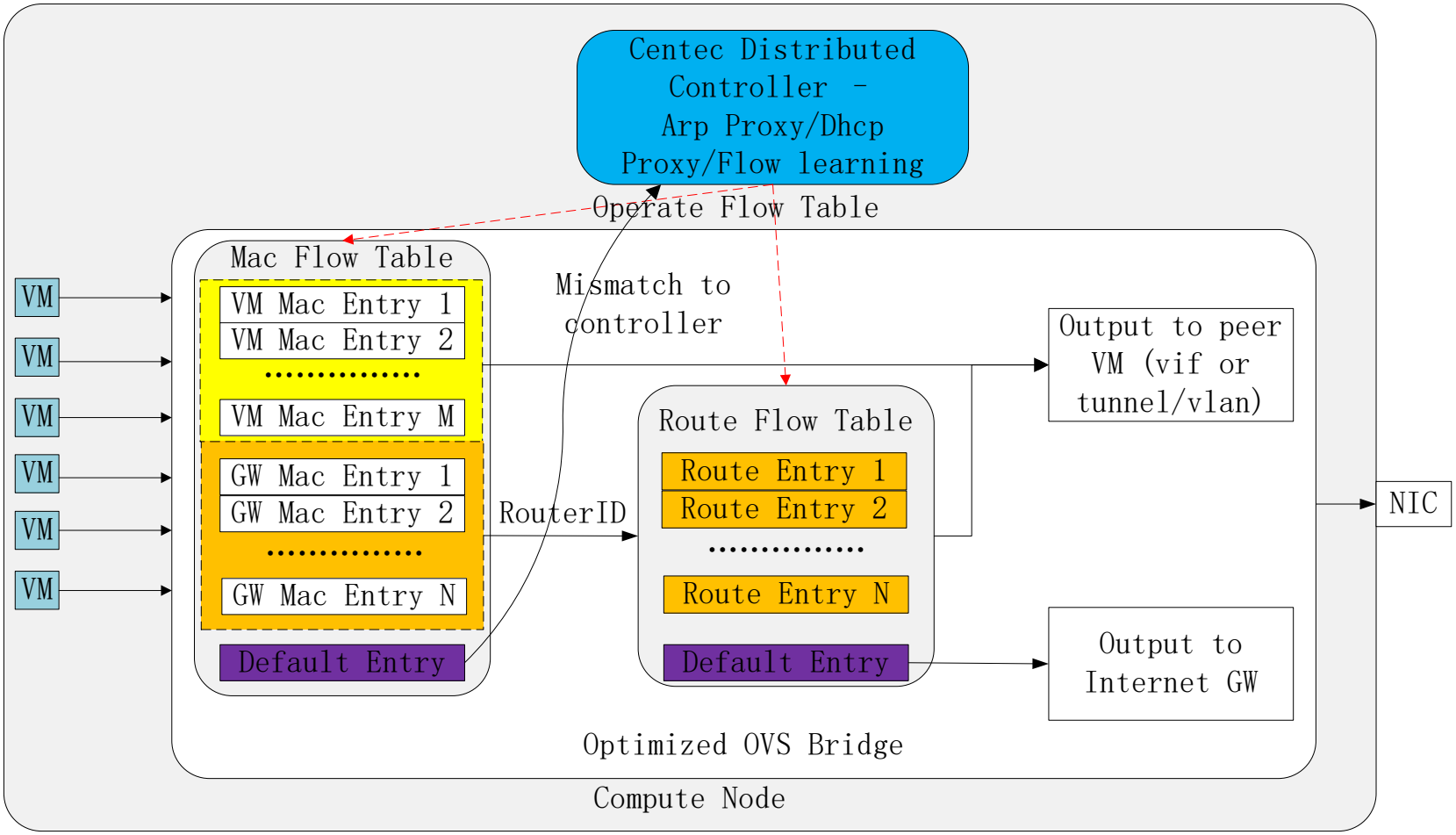
盛科DVNP方案Overview

- DVNP: Distributed Virtual Network Platform
- 全分布式东西向二层Bridge和三层Route转发
- 全分布式控制器
- 严谨的数据一致性校验
- 高效的而轻量级的kernel转发面设计
- 既可用作纯软件方案部署，又可辅助硬件Offload，从而达到接近裸机的性能
- 方便地支持虚拟机和物理机混合组网
- 不购买NSX就可以支持VMware下的VPC
- 方便地支持多种hypervisor混合下的VPC

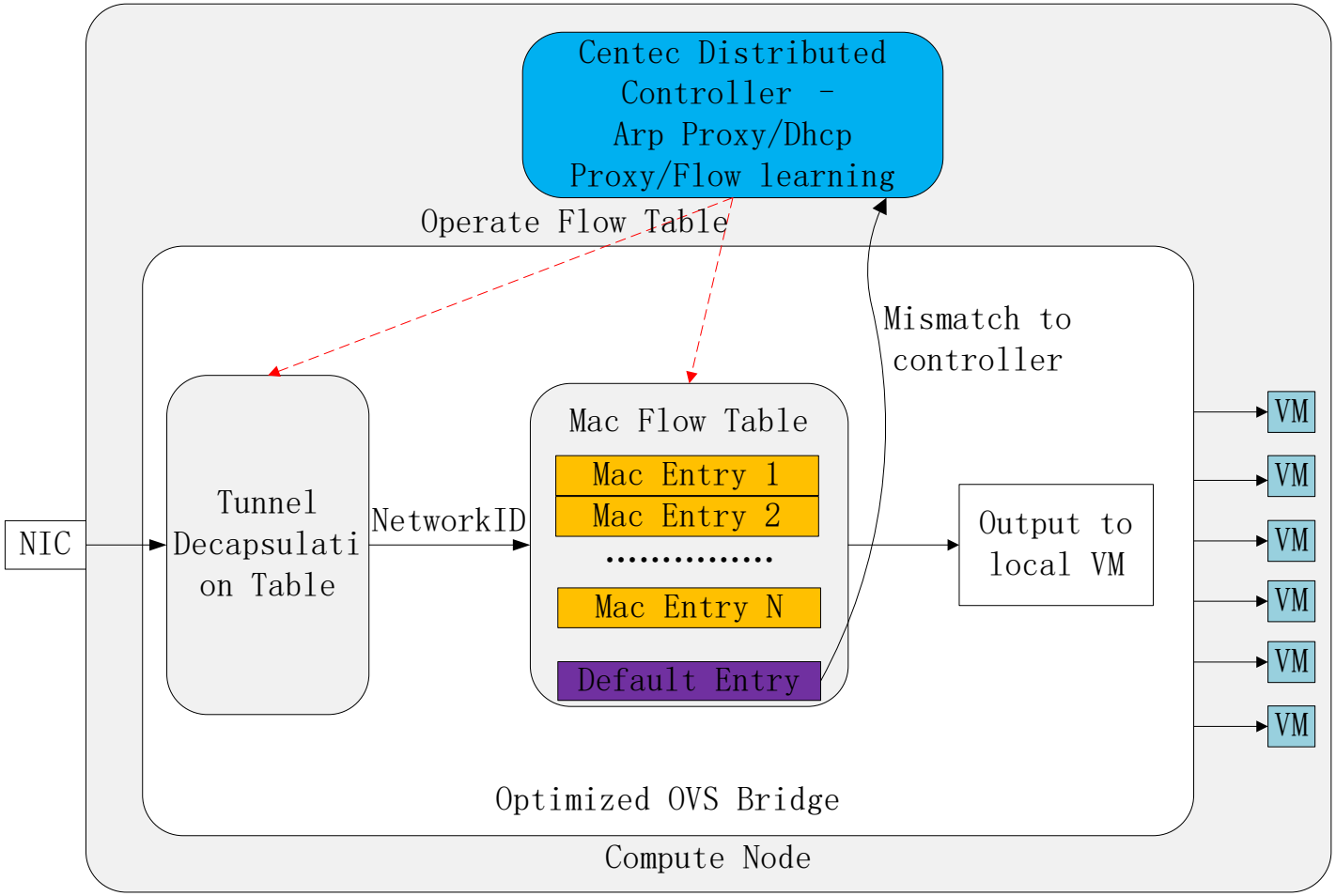
盛科DVNP架构：无硬件Offload



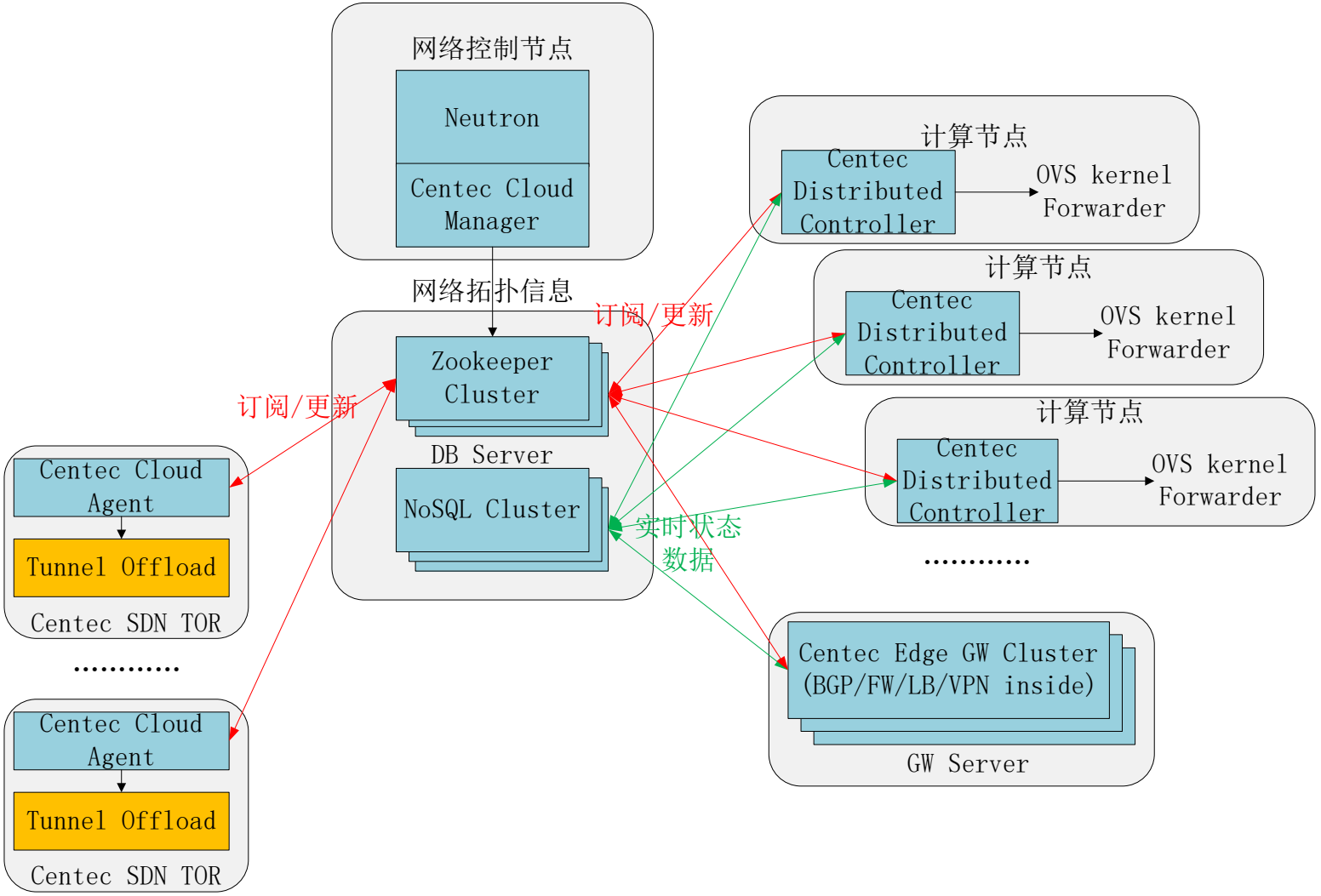
Data Flow in Centec Agent (ingress)



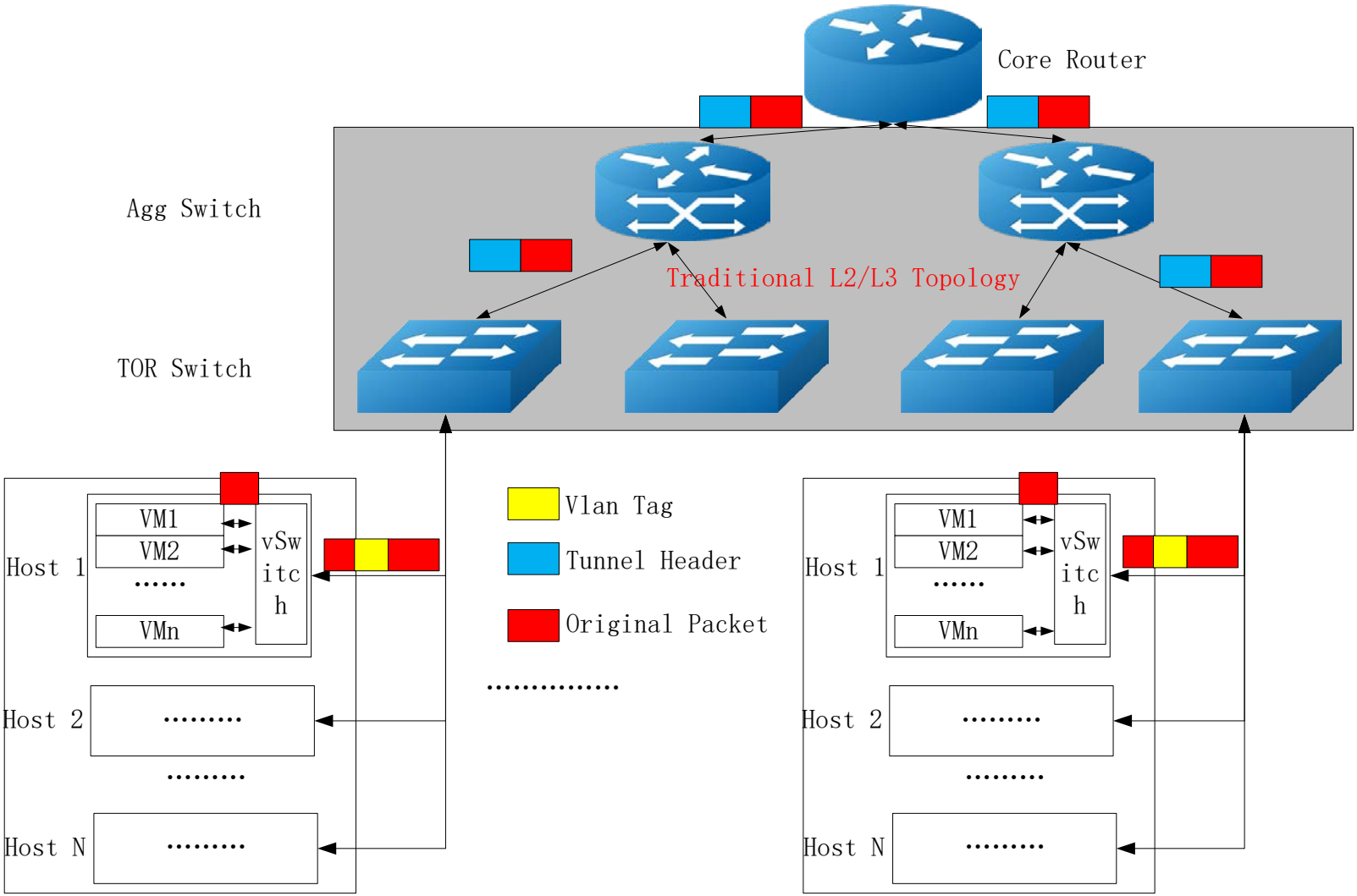
Data Flow in Centec Agent (egress)



盛科DVNP架构：硬件Offload



硬件Offload下的转发面流程



物理机和虚拟机混合组网

- Centec Cloud manager提供Cloud Console命令行和API
- 管理员通过Cloud Console命令行或者API动态增加、删除bare-metal server，分配local vlan，指定租户和network，并配置到SDN TOR Switch
- SDN TOR Switch将Vlan转换为相应的Tunnel VNI，反之亦然
- SDN TOR需要同时做bridge/route to tunnel
- 一些别的实现方式：1虚1、安装OVS、使用docker。都不如使用SDN GW来得高效、简单、方便

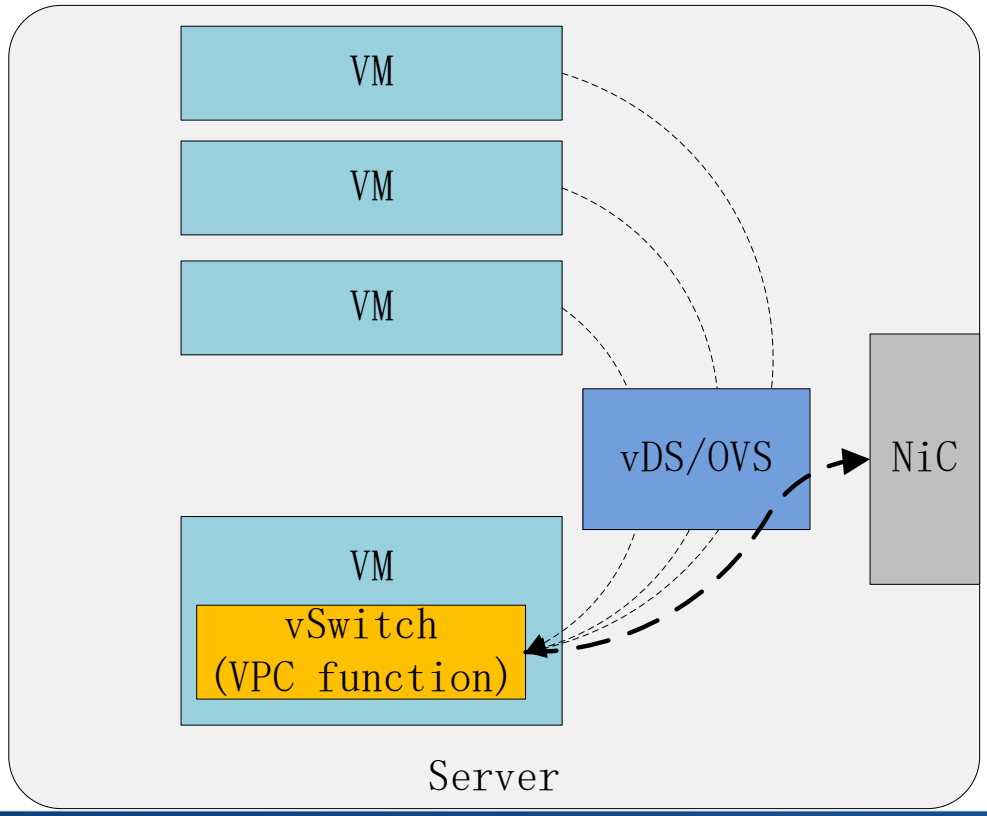
使用VMware产品的用户面临的问题

centec networks

- 市场有大量的存量VMware产品，这些产品不支持VPC
- VMware提供driver到OpenStack，但是仅限于legacy vDS支持（无法支持完整VPC功能）
- 要支持VPC，需要购买VMware的NSX，价格昂贵
- 很多用户不想购买NSX，但是却想支持灵活的VPC
- 甚至更多用户希望把VMware和XEN、KVM混合组网

当前的一些解决方案

- 要基于legacy VMware产品支持VPC，必须能够控制它的vSwitch。但显然做不到。
- 一些商业折衷方案：专门拿出一个VM做vSwitch，性能低下



基于SDN TOR来实现VMware的VPC

- 整体架构参考DVNP：硬件Offload架构
- 云平台获取VM的主机信息、IP、Mac、Local Vlan、所属租户
- 云平台控制SDN TOR，将Local Vlan映射成tunnel
- 可以使用OpenStack，也可以在vCenter之上再包装一个管理平面

centec networks

SDN和云计算时代的弄潮儿