RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012

THE GREAT CIPHER

MIGHTIER THAN THE SWORD

伟大的密码胜于利剑

未来网络虚拟片层的安全

安全视角看虚拟网络和SDN等

潘柱廷、叶润国

启明星辰公司

RSA CONFERENCE CHINA 2012

RSA信息安全大会2012

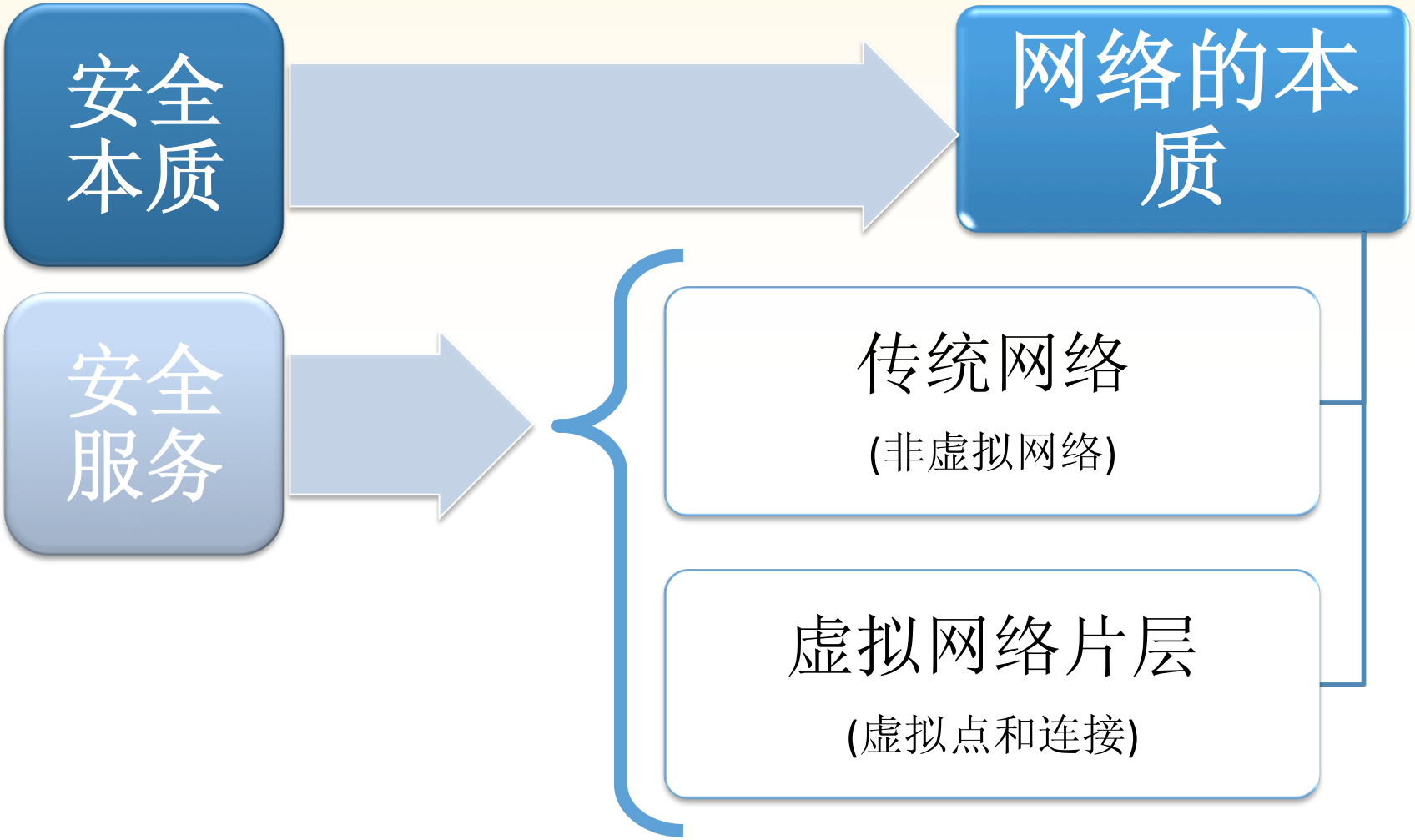
摘要

- 虚拟化是云计算等新兴计算技术实现的关键之一，包括服务器虚拟化、存储虚拟化、虚拟客户端、应用虚拟化、网络虚拟化等等。其中服务器、存储、客户端的虚拟化都可以被理解为空间节点的虚拟化，而常被提到的虚拟交换机技术还只是局部网络空间的虚拟化。而在软件定义网络SDN等技术所代表的发展趋势看，真正覆盖较大范围的虚拟化网络必将出现。本演讲试图探讨网络空间的根本性变化所带来网络安全理论、方法和技术的变化。

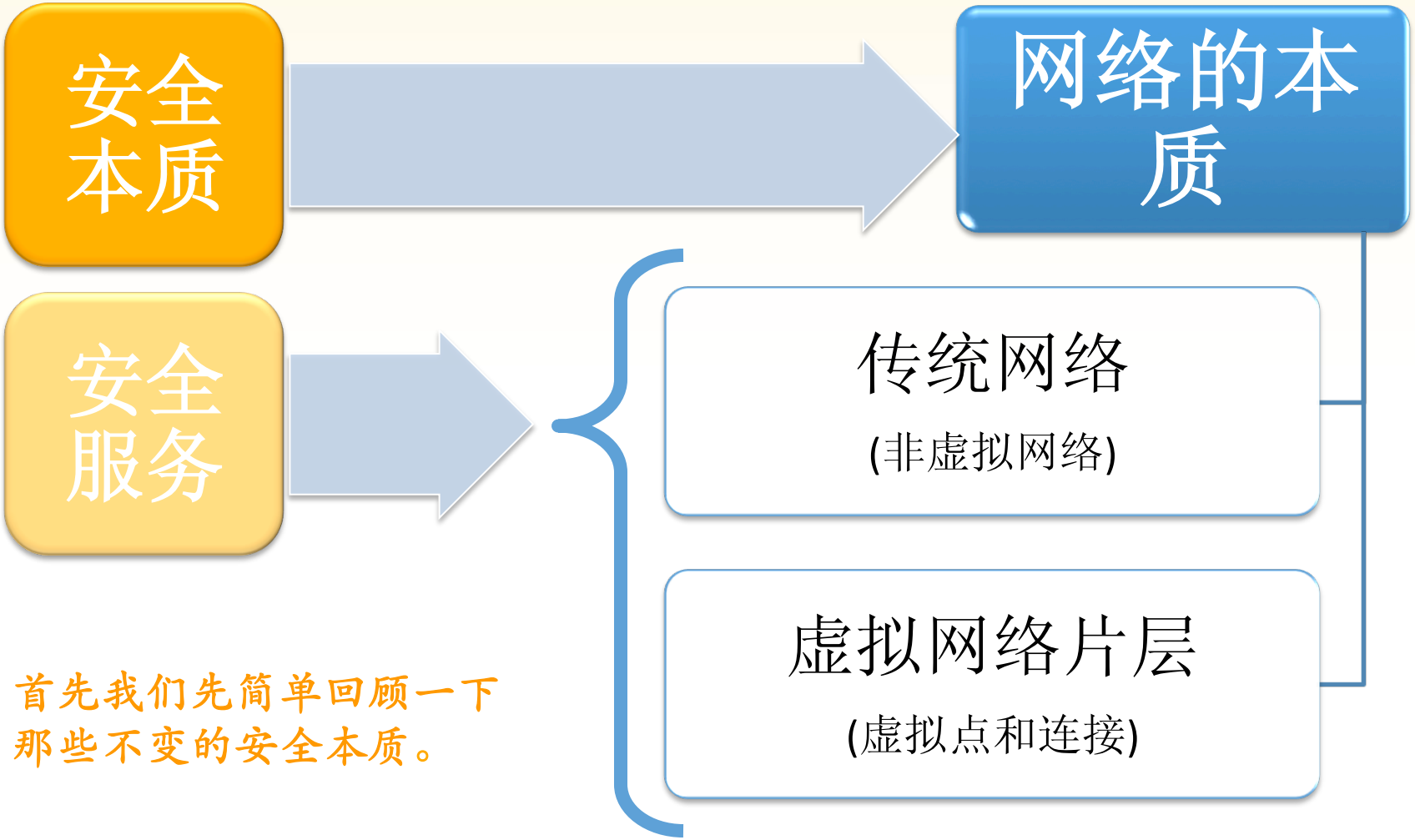
几个不得不搞清楚的概念

- 安全的本质
- 安全服务
- 网络的本质
- 传统网络（非虚拟网络）的本质体现
- 虚拟网络的本质体现

安全、网络、虚拟



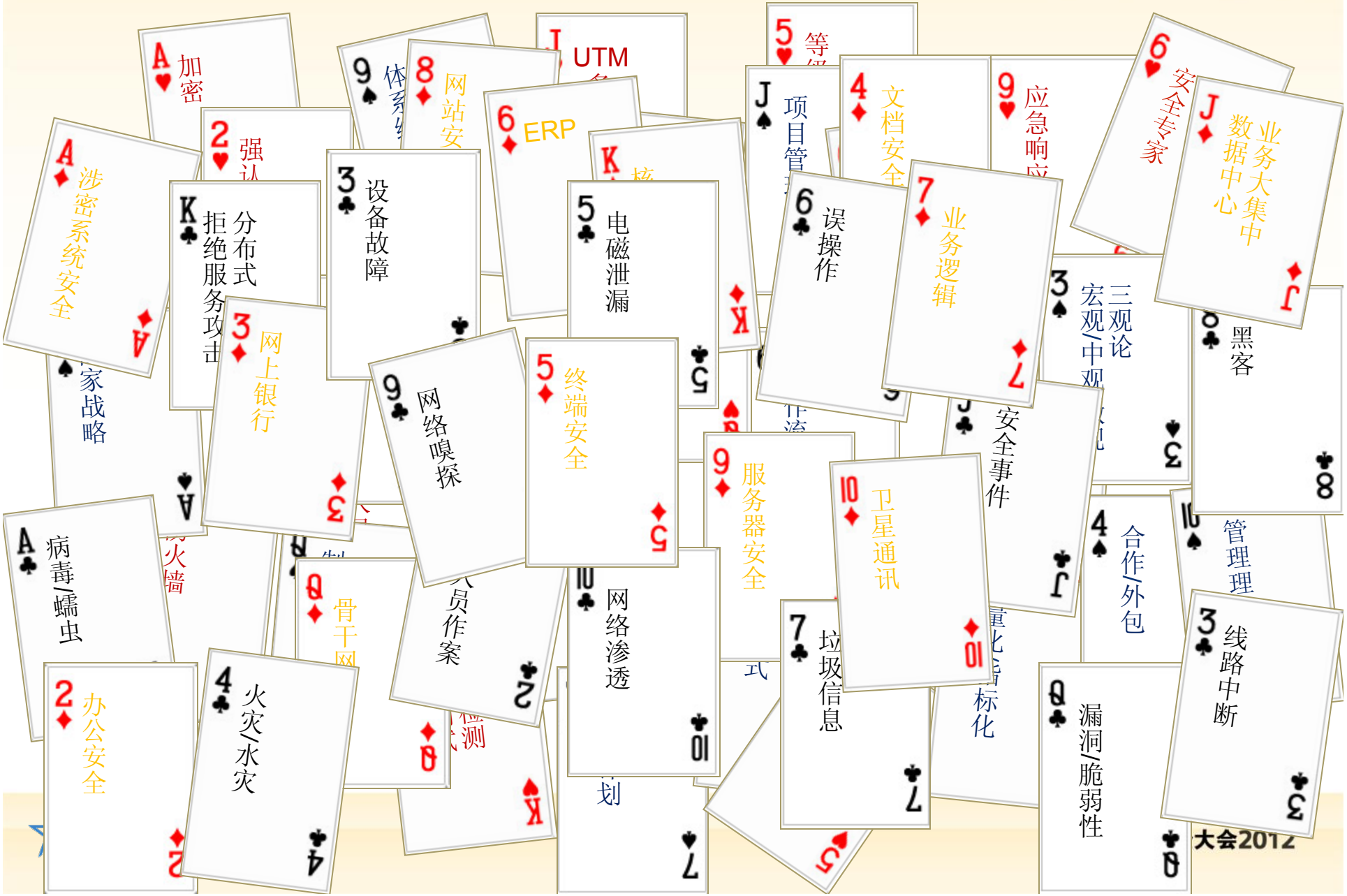
安全、网络、虚拟



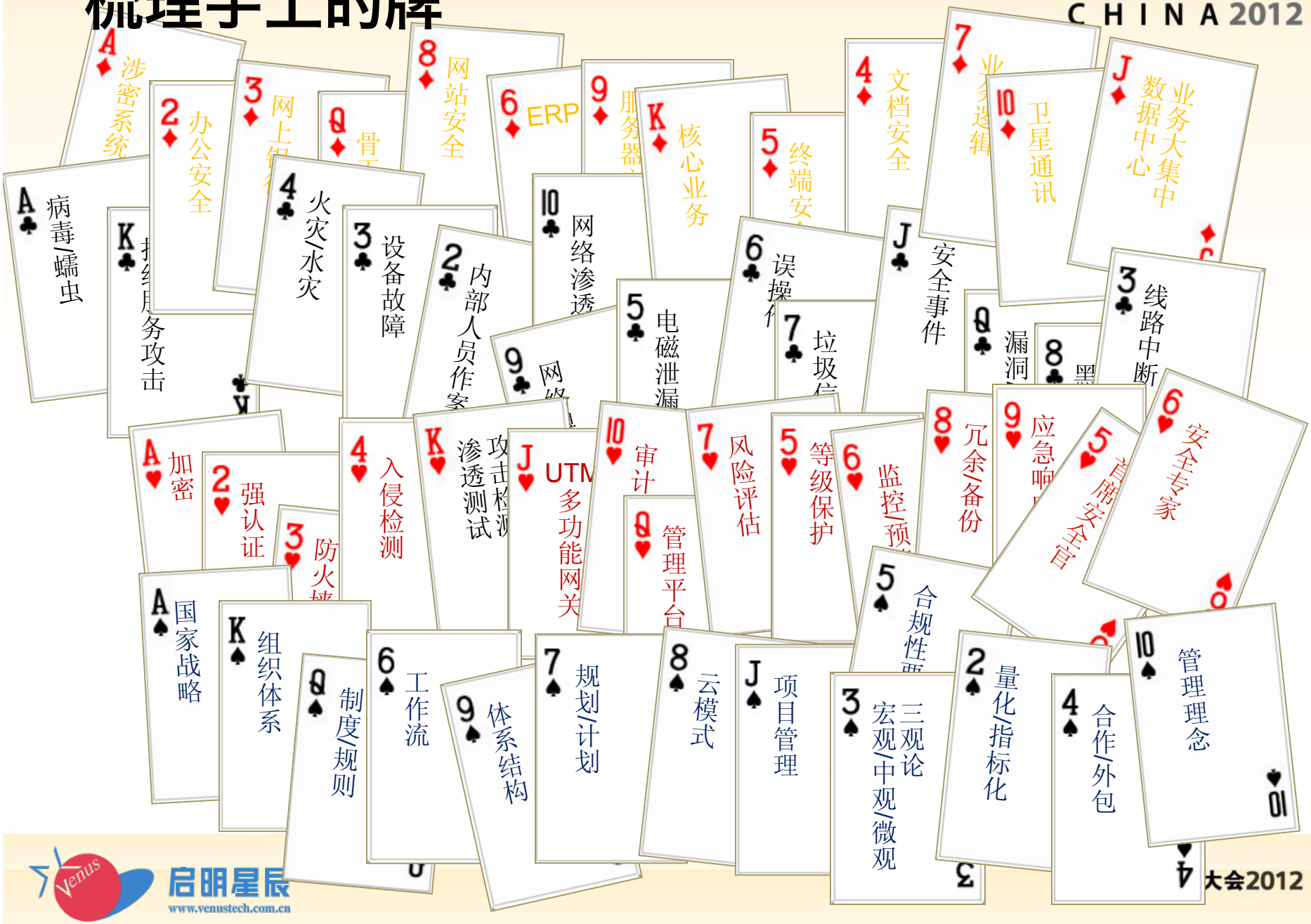
首先我们先简单回顾一下
那些不变的安全本质。

安全的方方面面

RSA CONFERENCE CHINA 2012

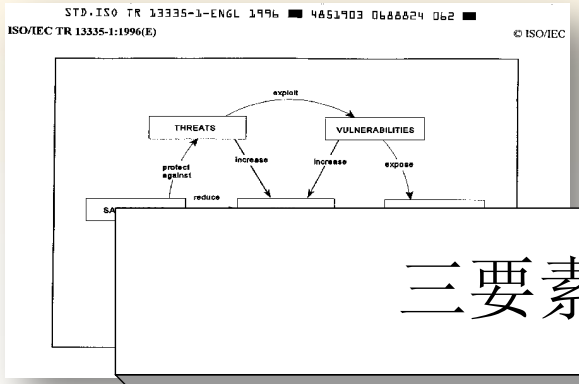


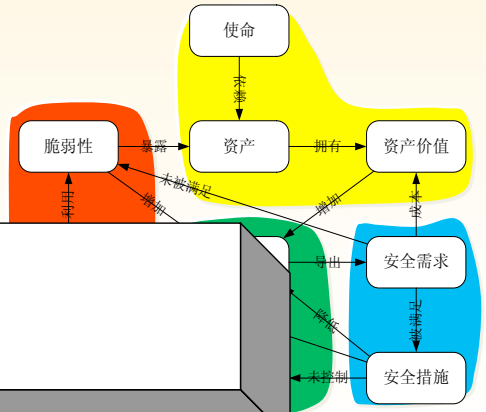
梳理手上的牌


涉密系统
办公安全
网站安全
ERP
核心业务
终端安全
文档安全
业务逻辑
卫星通讯
业务大集中
数据中心
病毒/蠕虫
网络攻击
火灾/水灾
设备故障
内部人员作案
网络渗透
电磁泄漏
误操作
垃圾信
安全事件
漏洞
线路中断
加密
强认证
防火墙
入侵检测
攻击检测
渗透测试
UTM
多功能网关
审计
管理平台
风险评估
等级保护
监控/预警
冗余/备份
应急响应
容灾/安全台
安全专家
国家战略
组织体系
制度/规则
工作流
体系结构
规划/计划
云模式
项目管理
合规性要
三观论
宏观/中观/微观
量化/指标化
合作/外包
管理理念

最精简的风险管理3要素

RSA CONFERENCE CHINA 2012



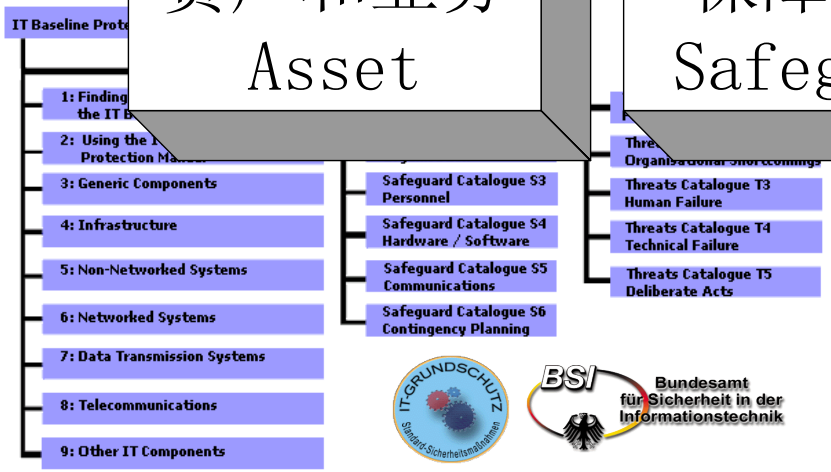


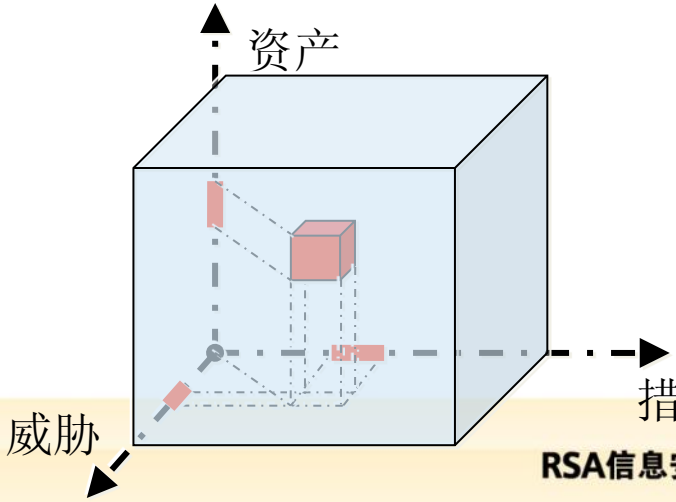
三要素风险模型：

资产和业务 Asset

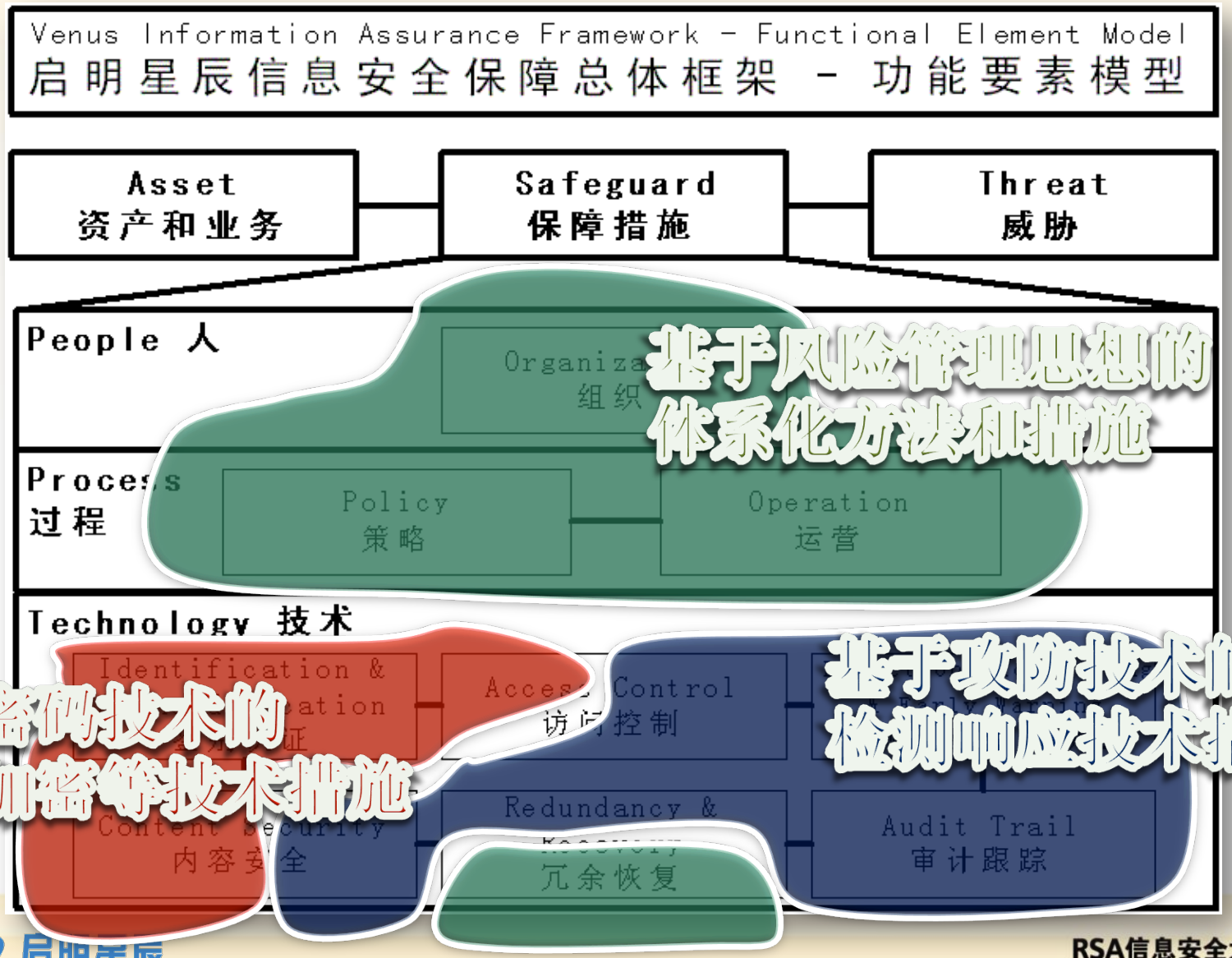
保障措施 Safeguard

威胁 Threat





不变的三类信息安全核心技术

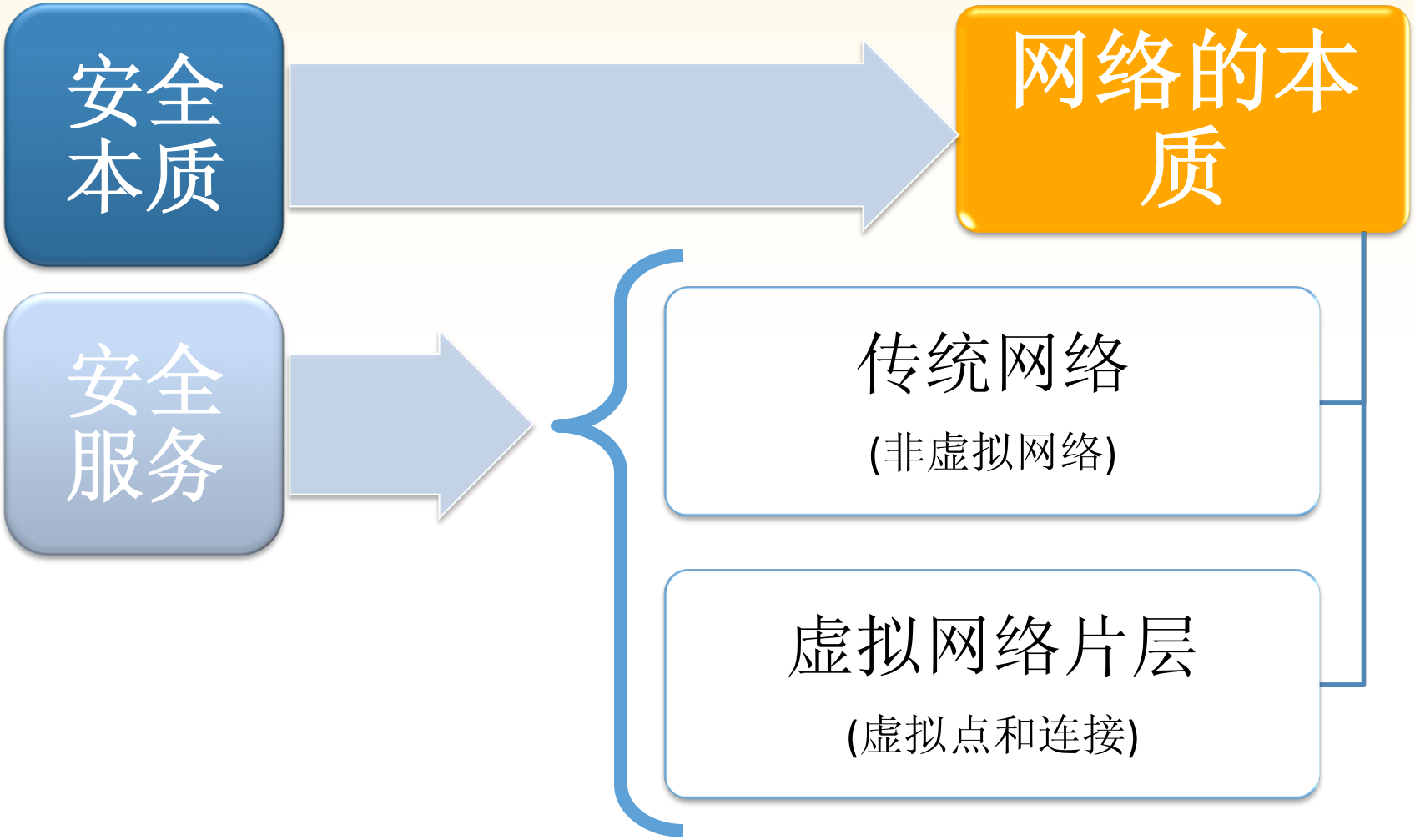


安全的原则和思路…

- 风险三要素
- 需求驱动力矩阵
- PPT结构
- 三大类安全技术
- PDR及PDCERF
- 通用检测模型
- 分层和分域，三观论
- Zachman(nW1H, 虚实层)
- 流和时空
  - **安全域+业务流**
- …

- 基于时间和基于缓冲的安全
- 结构和解构
- 安全度量和安全可视化
- 生命周期三大过程
- 敏捷和瀑布模式
- 君臣佐使的配伍思想
- 可信与可控
- 云模式、虚拟化
- 大数据分析解决APT
- 宏观态势感知
- …

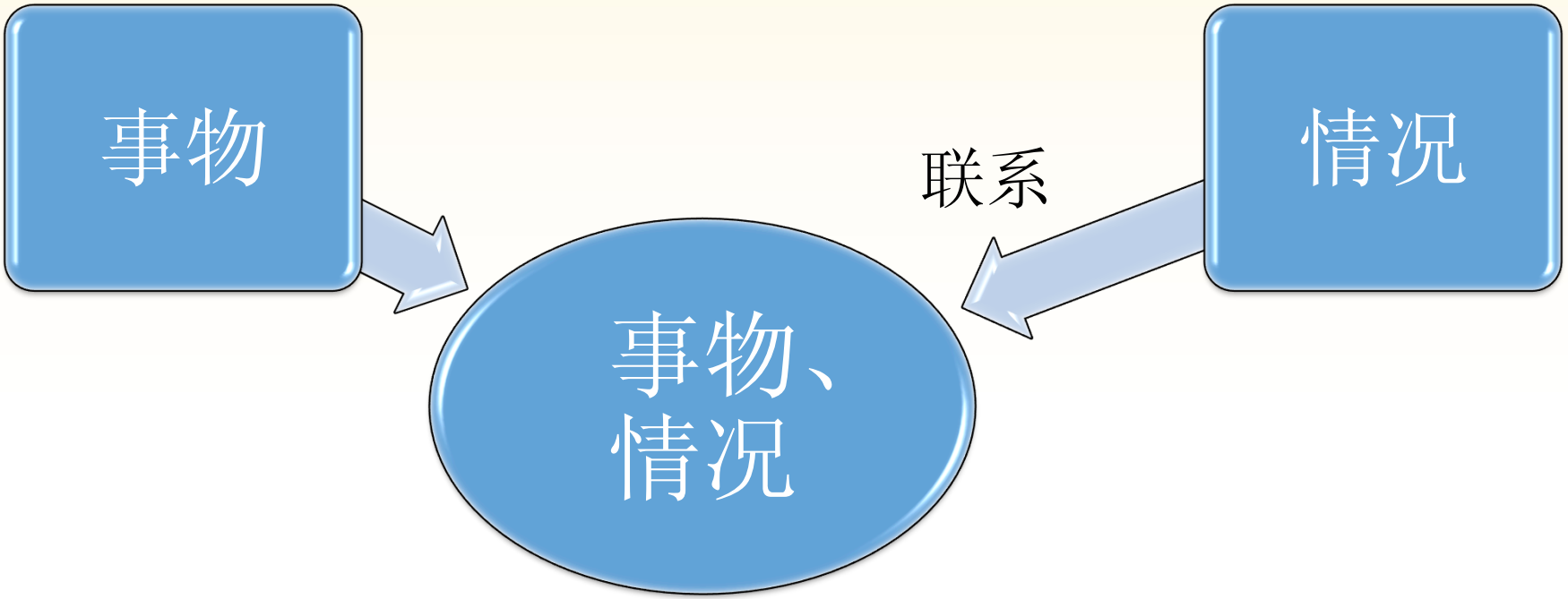
安全、网络、虚拟



形形色色的网络

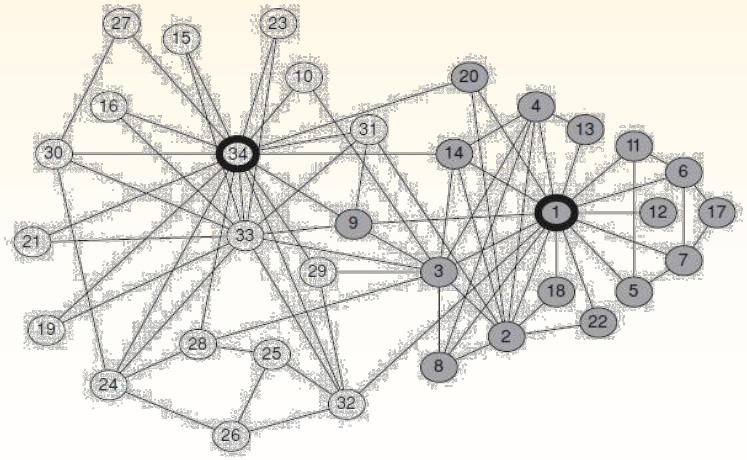
- 交通运输网，邮政网，电话通信网，计算机网，互联网，万维网
- 社会关系网，产品供销网，金融借贷网
- 智能电网，无线网，传感网，物联网
- 神经网，生物代谢网，食物链（网）
- 攻守同盟网，恐怖主义网络
- 人人网，新浪微博网，QQ，团购网
- …

当我们想到“网络”这个词语...



- 节点：vertex,point
- 边：连接,链接,关系,联系；edge,link

网络中的路径

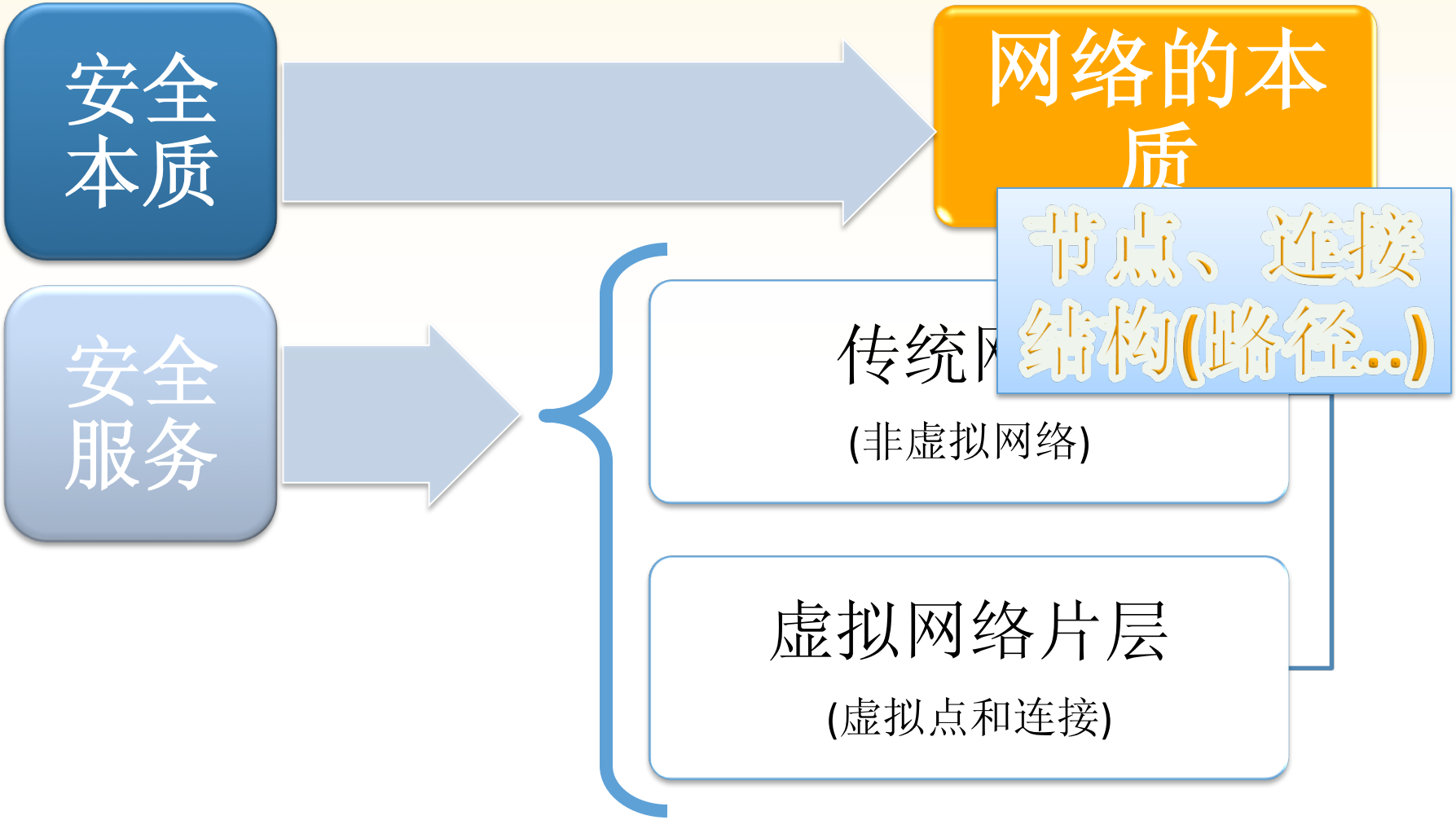


- 以点的关系为主，不关注路径
  - 社交网络
- 路径不固定，会按需临时建立
  - 无线网络、物联网、无线传感网、DTN等
- 路径连接着点，数据在路径上流动
  - 互联网、局域网

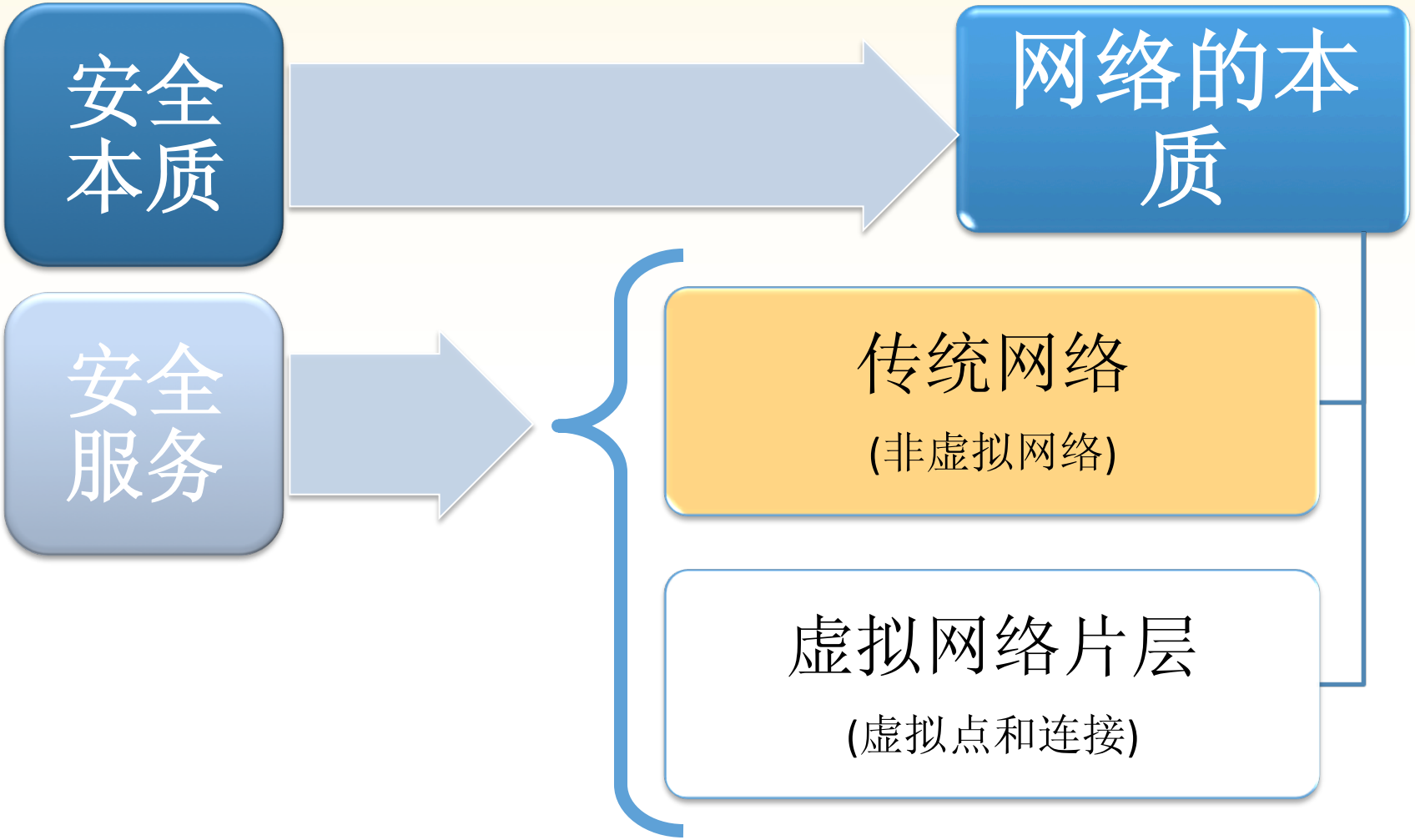
更抽象

更具体

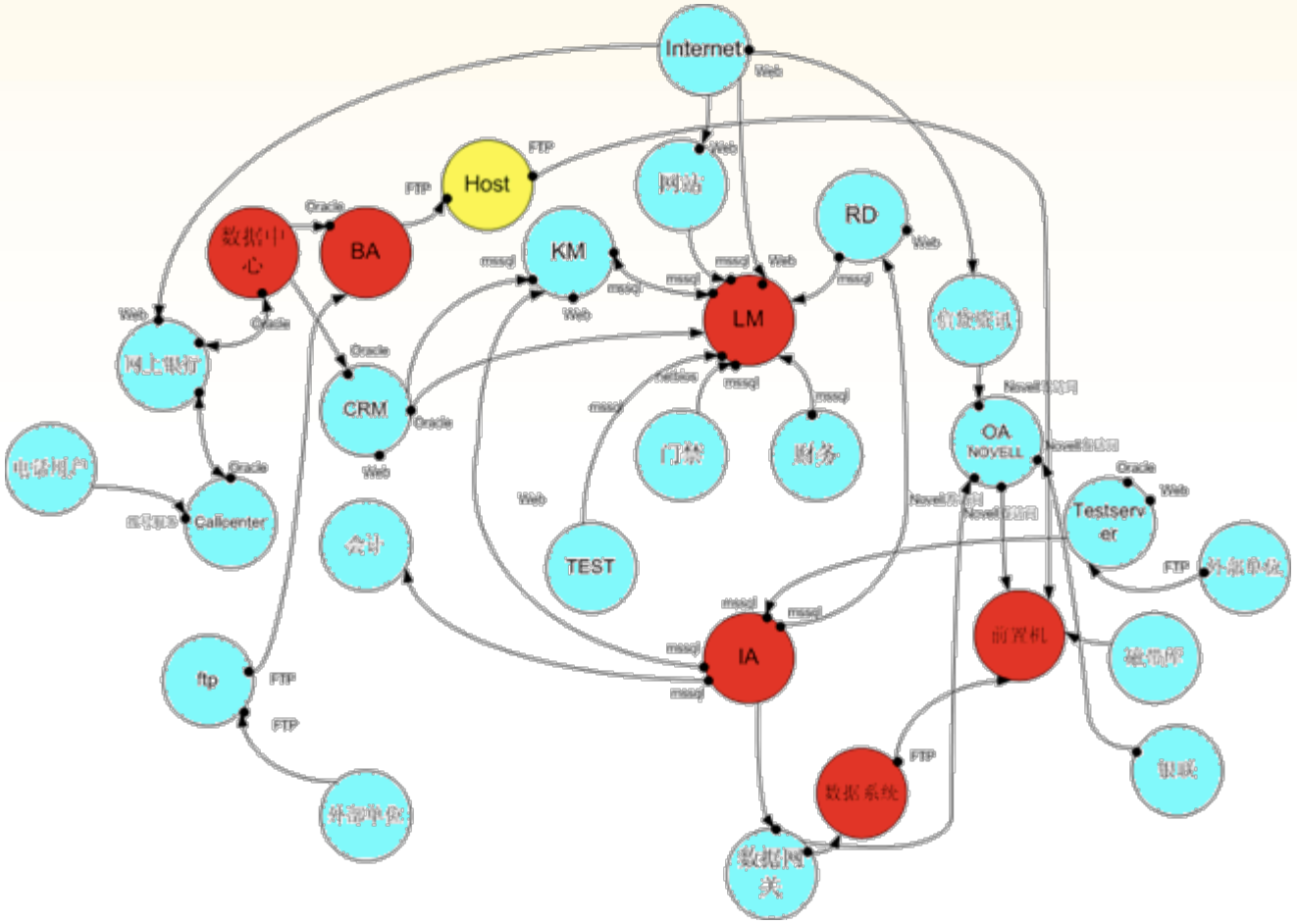
安全、网络、虚拟



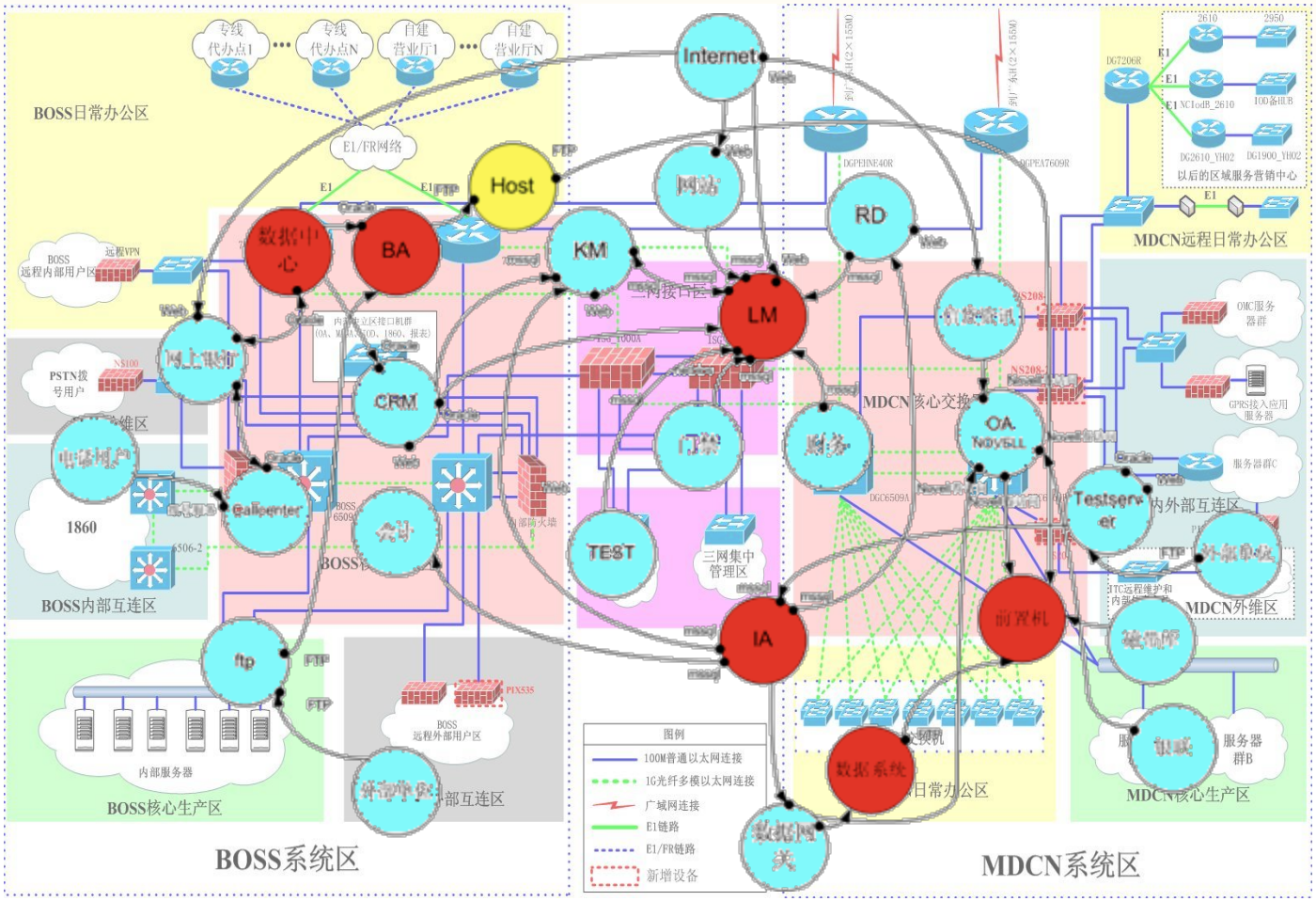
安全、网络、虚拟



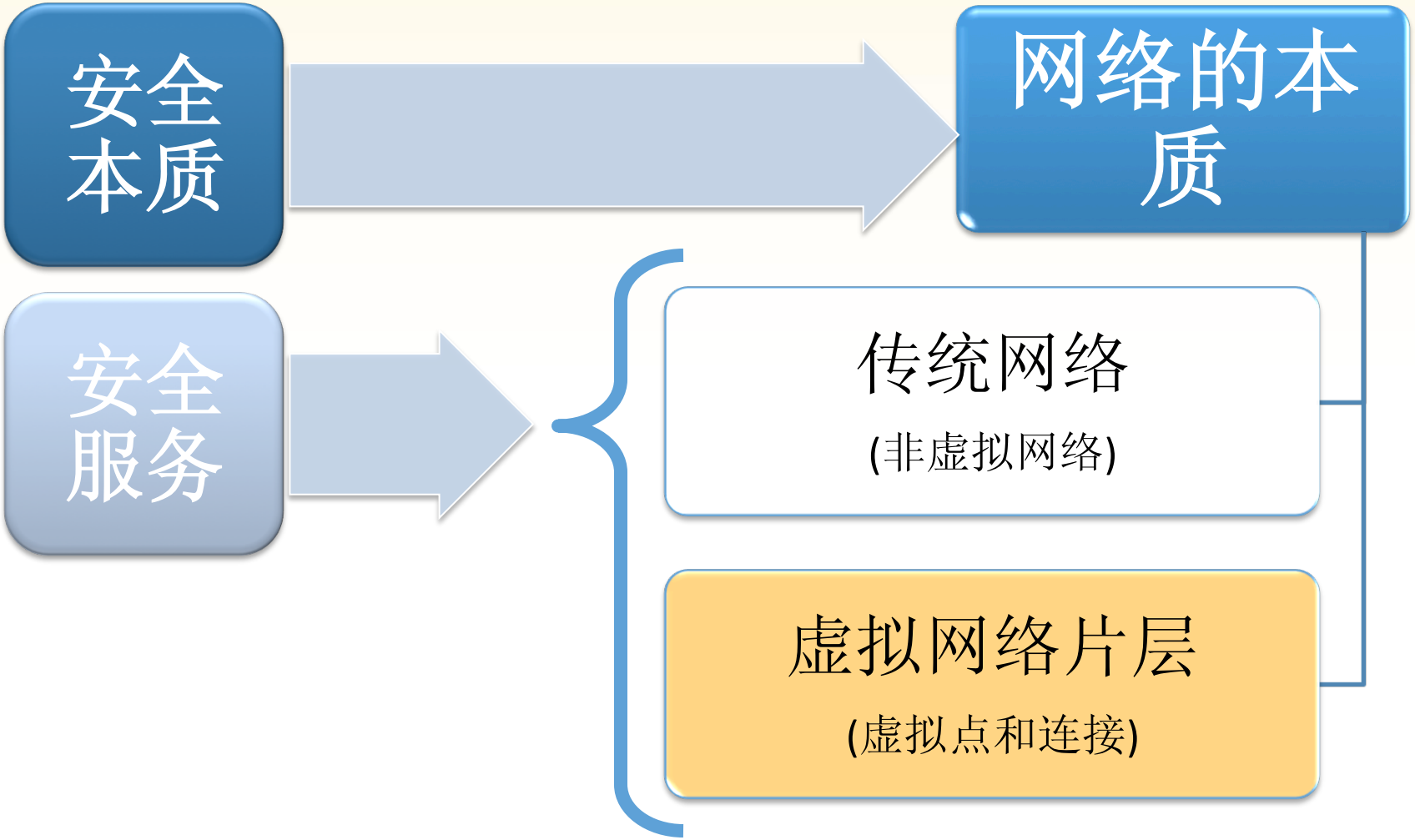
业务流


Internet
Web
Host
FTP
网站
Web
数据中心
Oracle
BA
FTP
KM
mssql
RD
Web
网上银行
Web
LM
CRM
Oracle
门禁
财务
电话帐户
Callcenter
Oracle
会计
TEST
OA
NOVELL
Testserver
Oracle
Web
FTP
ftp
FTP
FTP
IA
mssql
前置机
数据系统
FTP
外部单位
银联

业务流@网络结构


BOSS日常办公区
专线代办点1
专线代办点N
自建营业厅1
自建营业厅N
E1/FR网络
Internet
Host
数据中心
BA
KM
网站
RD
LM
CRM
门户
财务
OA
TEST
三网集中管理区
IA
前置机
Testserver
Gallenter
ftp
内部服务器
BOSS核心生产区
BOSS内部互连区
BOSS远程内部用户区
BOSS远程外部用户区
PSTN拨号用户
1860
BOSS系统区
MDCN远程日常办公区
以后的区域服务营销中心
OMC服务器群
GPRS接入应用服务器
服务器群C
内外部互连区
MDCN外维区
服务器群B
MDCN核心生产区
MDCN核心交换
MDCN日常办公区
数据系统
MDCN系统区
图例
100M普通以太网连接
1G光纤多模以太网连接
广域网连接
E1链路
E1/FR链路
新增设备

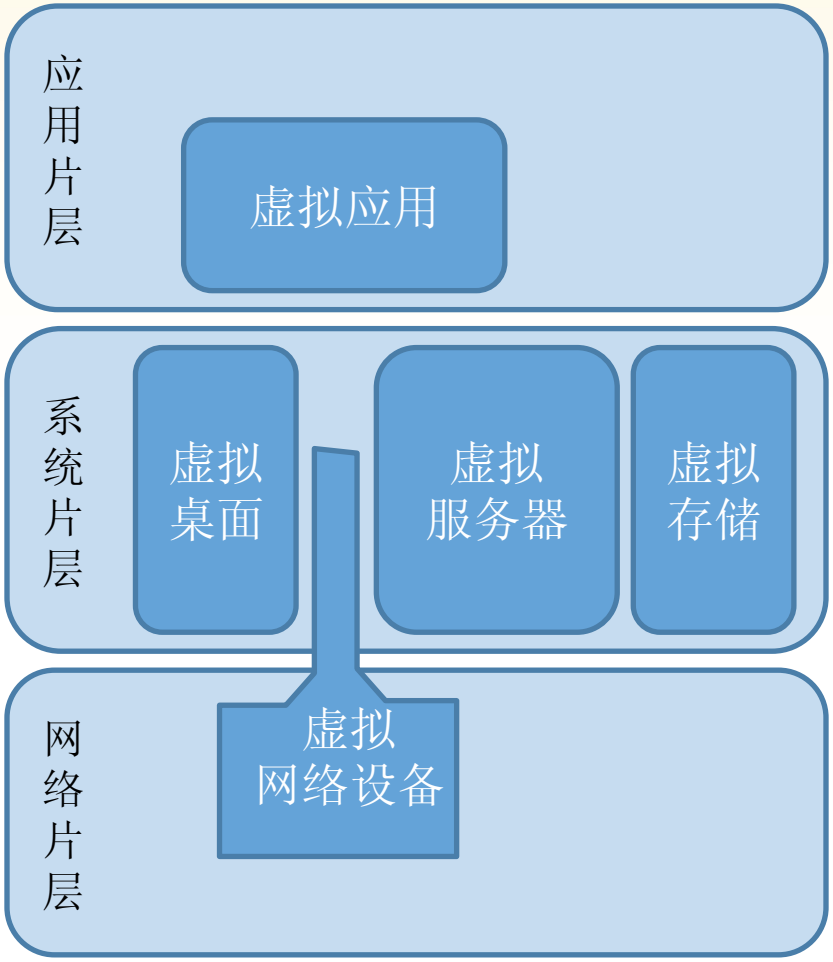
安全、网络、虚拟



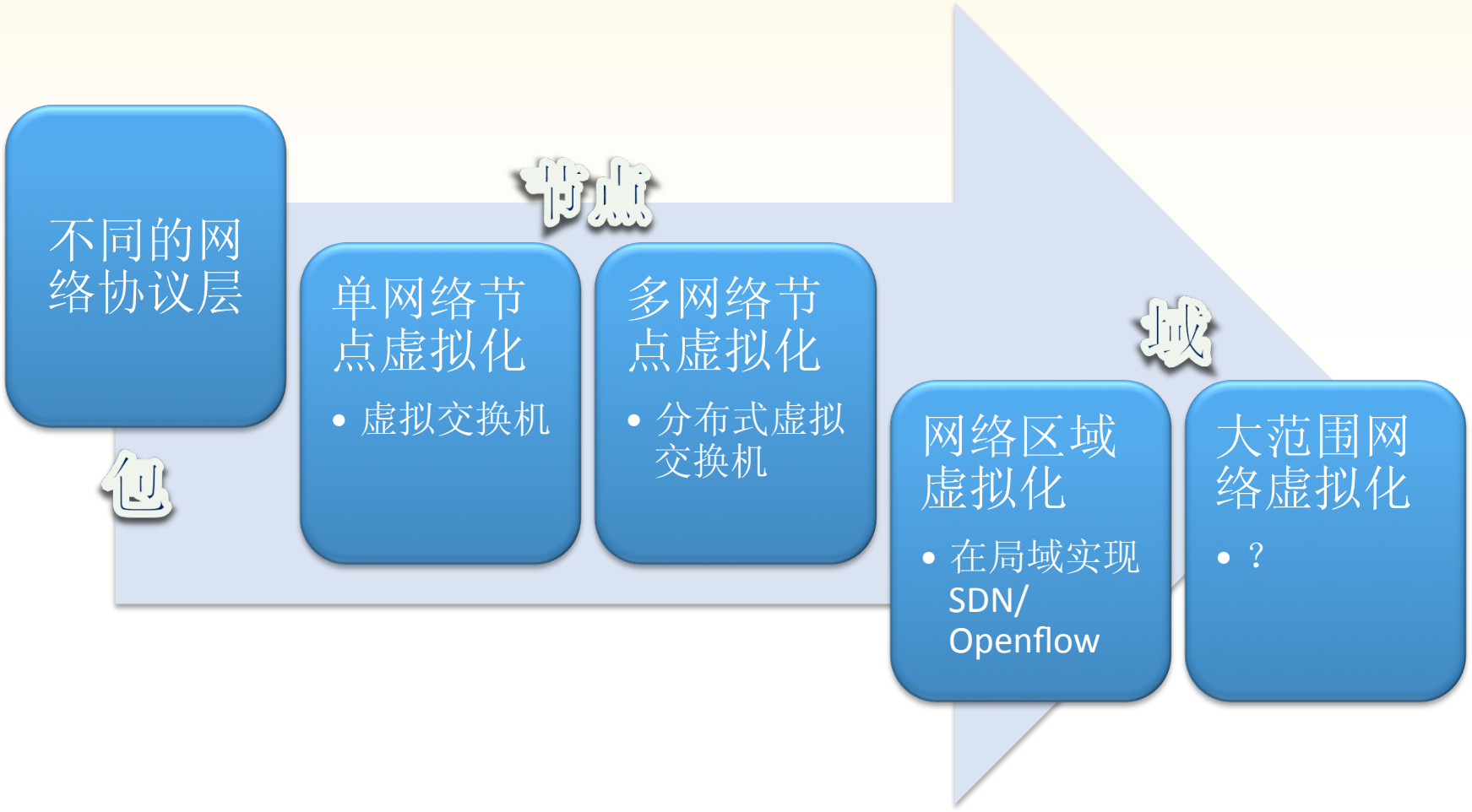
虚拟化

常被提到的虚拟化

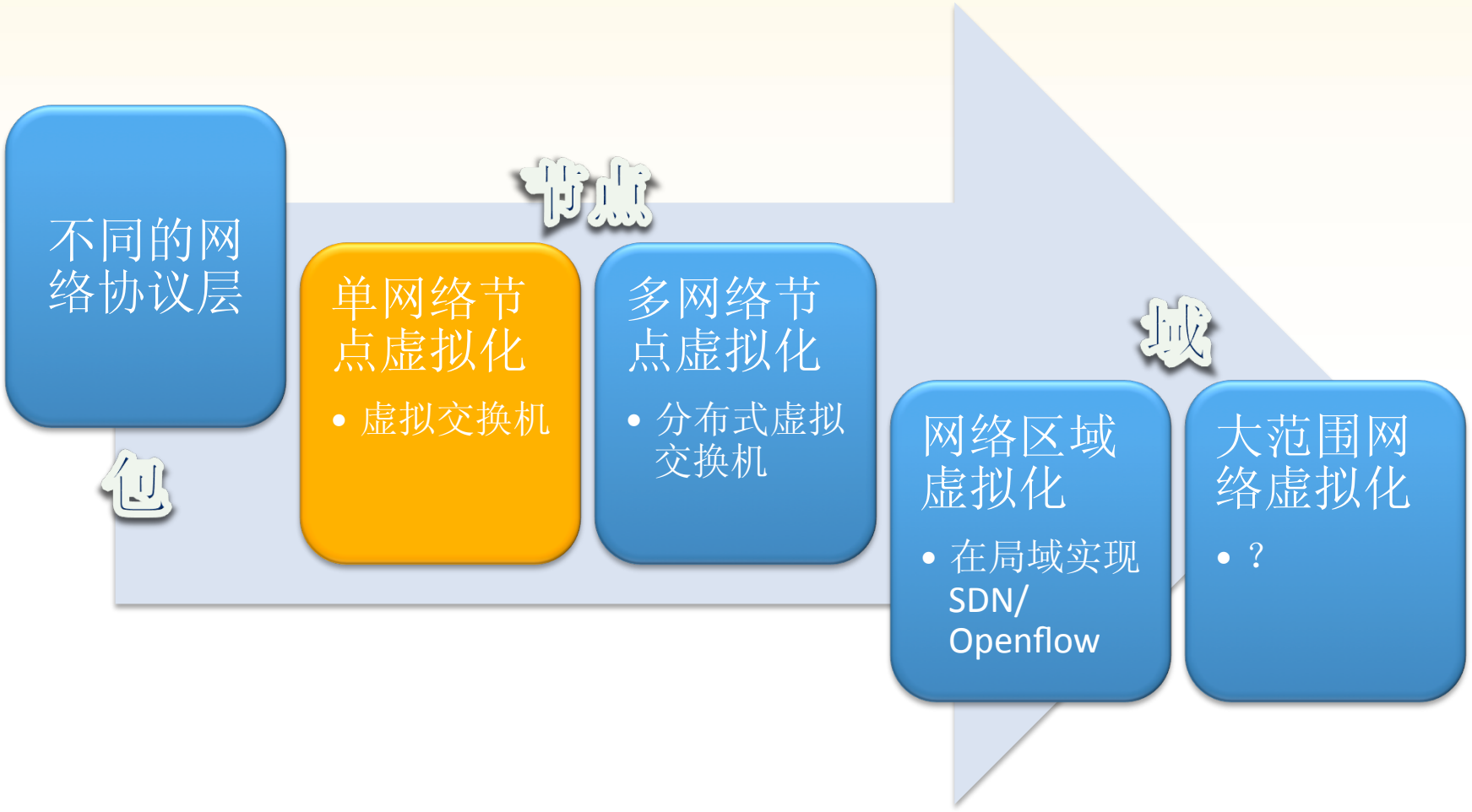
- 服务器虚拟化
- 存储虚拟化
- 桌面虚拟化
- 应用虚拟化
- 网络虚拟化



网络虚拟化的不同范围


不同的网络协议层
包
节点
单网络节点虚拟化
• 虚拟交换机
多网络节点虚拟化
• 分布式虚拟交换机
域
网络区域虚拟化
• 在局域实现SDN/ Openflow
大范围网络虚拟化
• ?

网络虚拟化的不同范围


不同的网络协议层
包
节点
单网络节点虚拟化
• 虚拟交换机
多网络节点虚拟化
• 分布式虚拟交换机
域
网络区域虚拟化
• 在局域实现SDN/ Openflow
大范围网络虚拟化
• ?

网络虚拟化-虚拟交换机

RSA CONFERENCE CHINA 2012

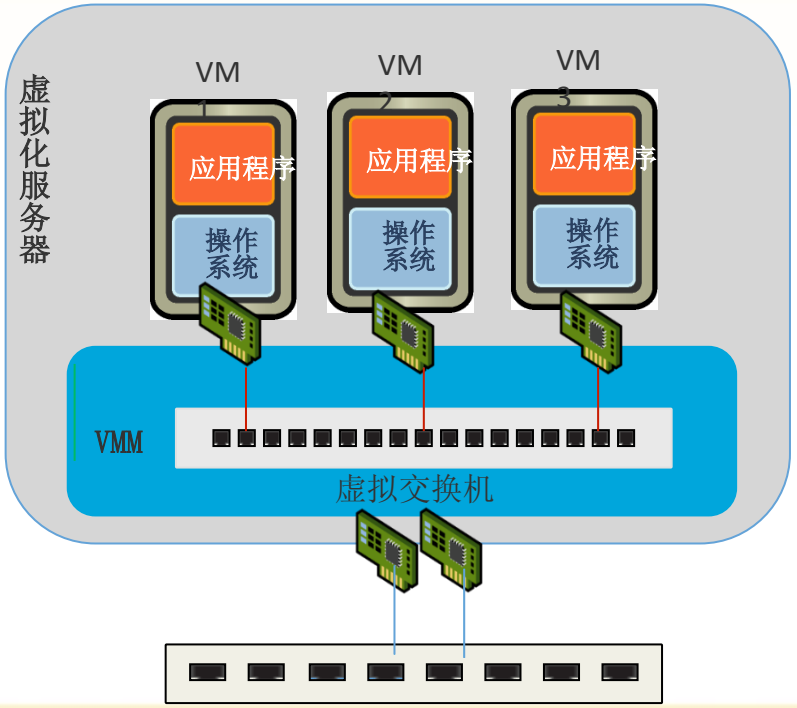
- 软件模块、VM数据交换；局限在物理服务器中

软件模块、VM数据交换；局限在物理服务器中

- 与物理L2交换机兼容，可以构建VLAN

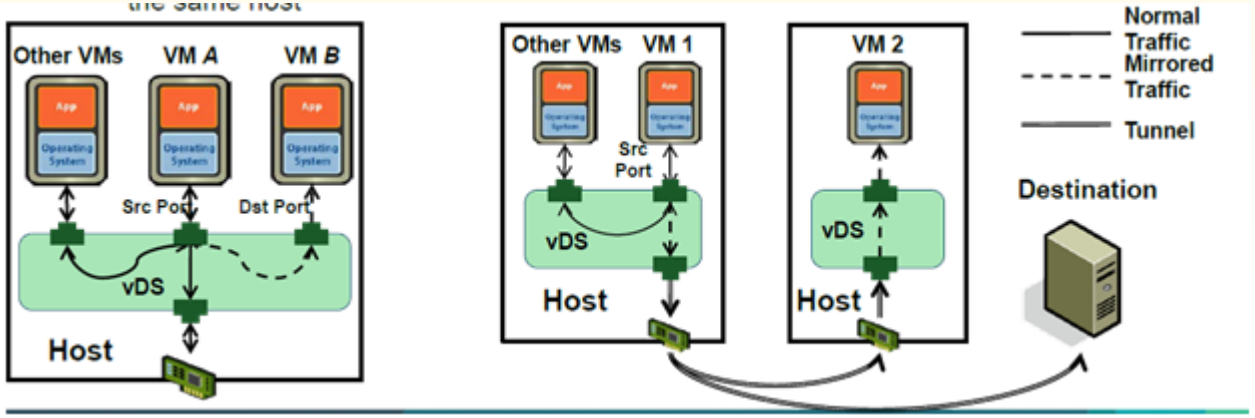
流量不可见问题

- 网络隔离问题
- 管理复杂问题
-
- 策略一致性问题
- 网络性能问题

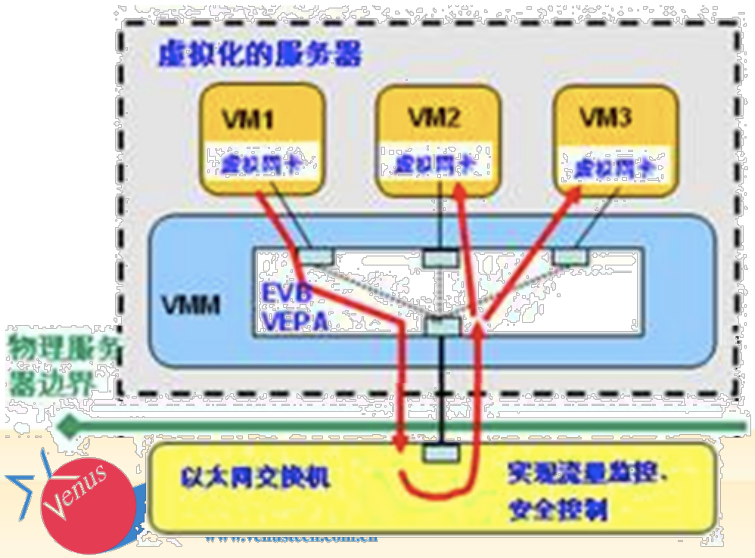


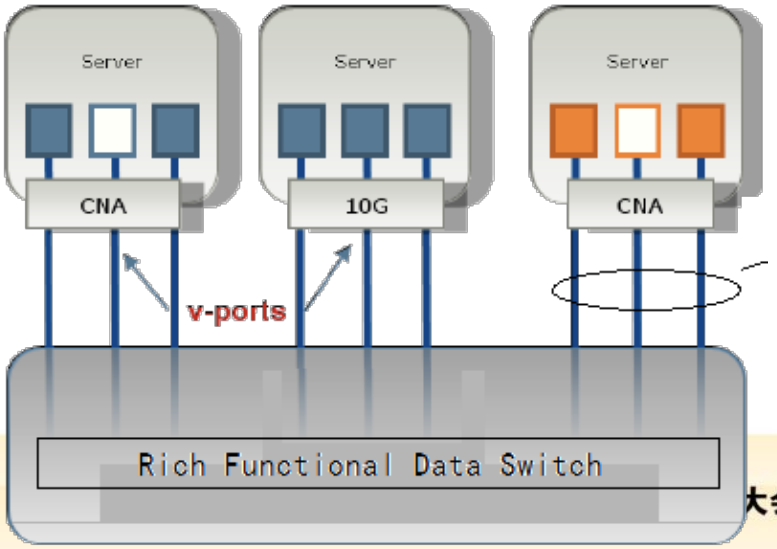
VM间流量不可见问题解决方案

- 软件SPAN、RSPAN和netflow功能



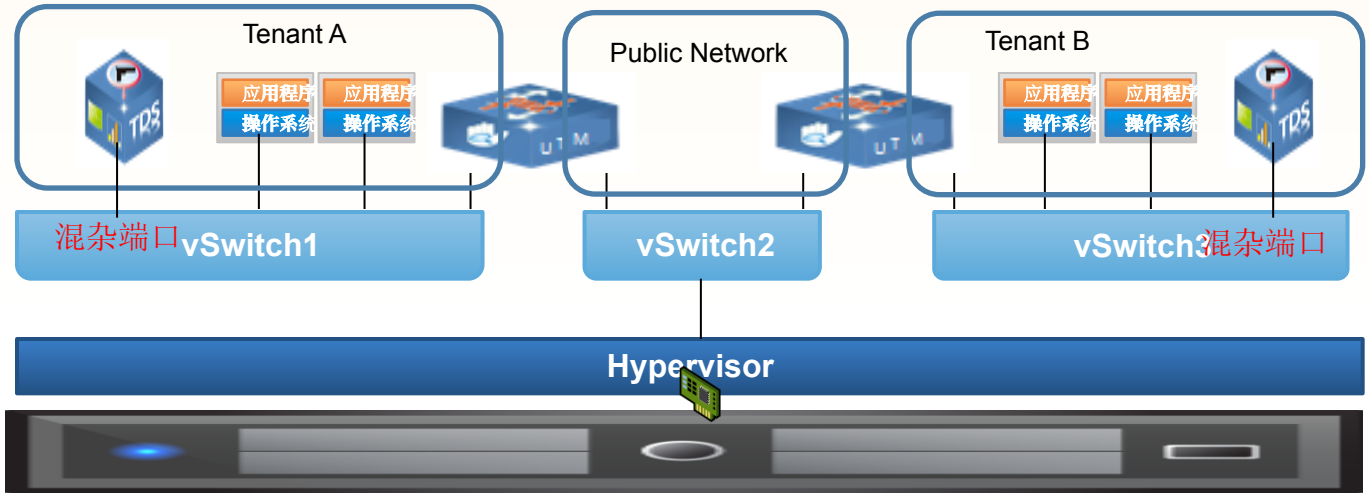
- 硬件交换机导流方案：VEPA和VN-TAG





虚拟交换机环境下的安全产品部署

- 部署串行网关

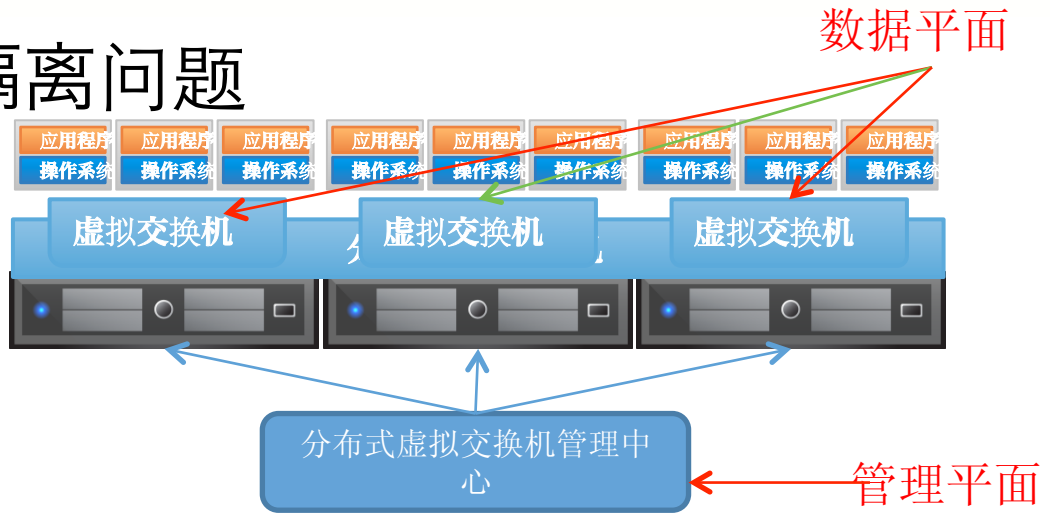


- 部署旁路检测

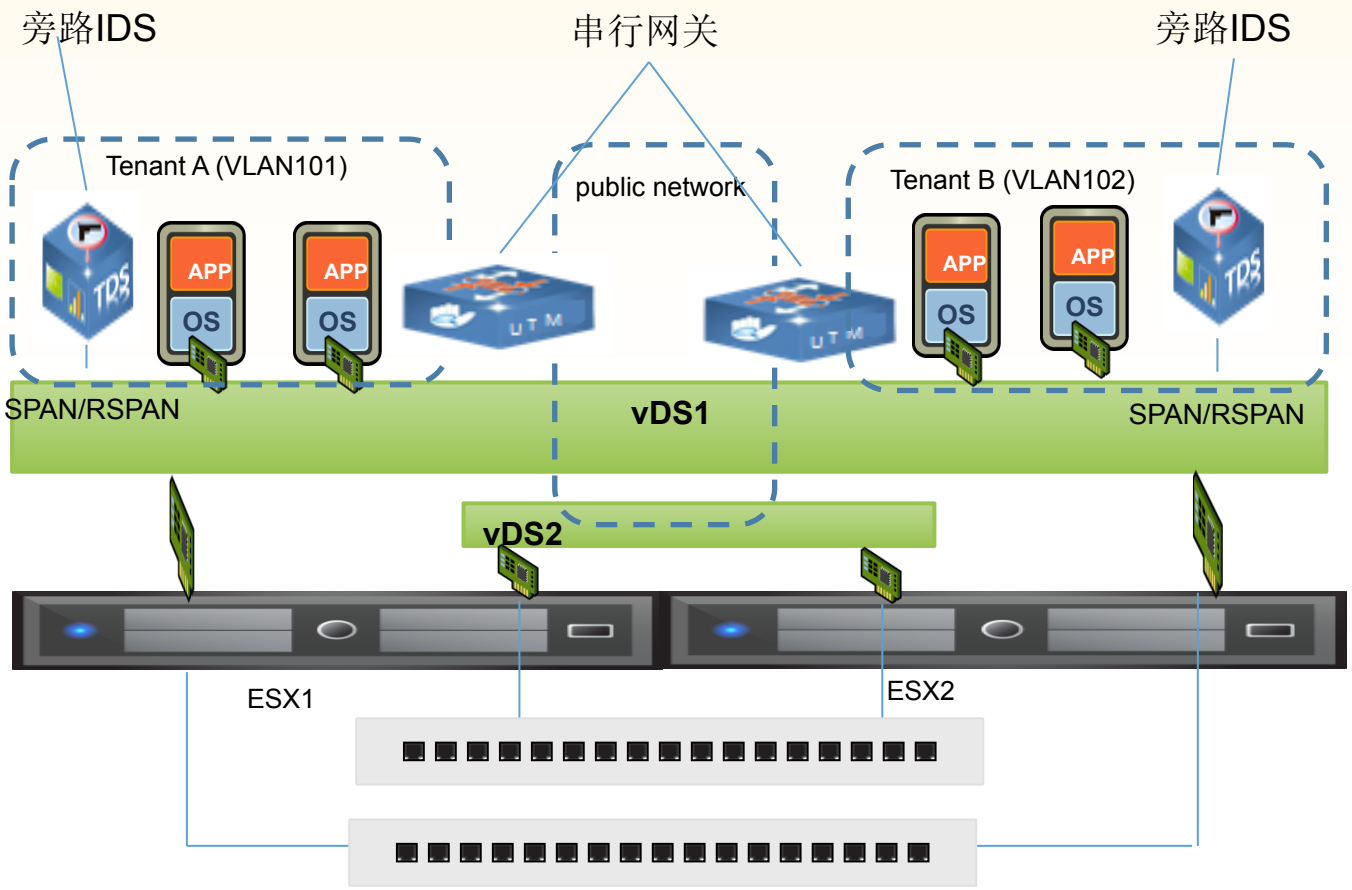
网络虚拟化的不同范围

网络虚拟化-分布式虚拟交换机

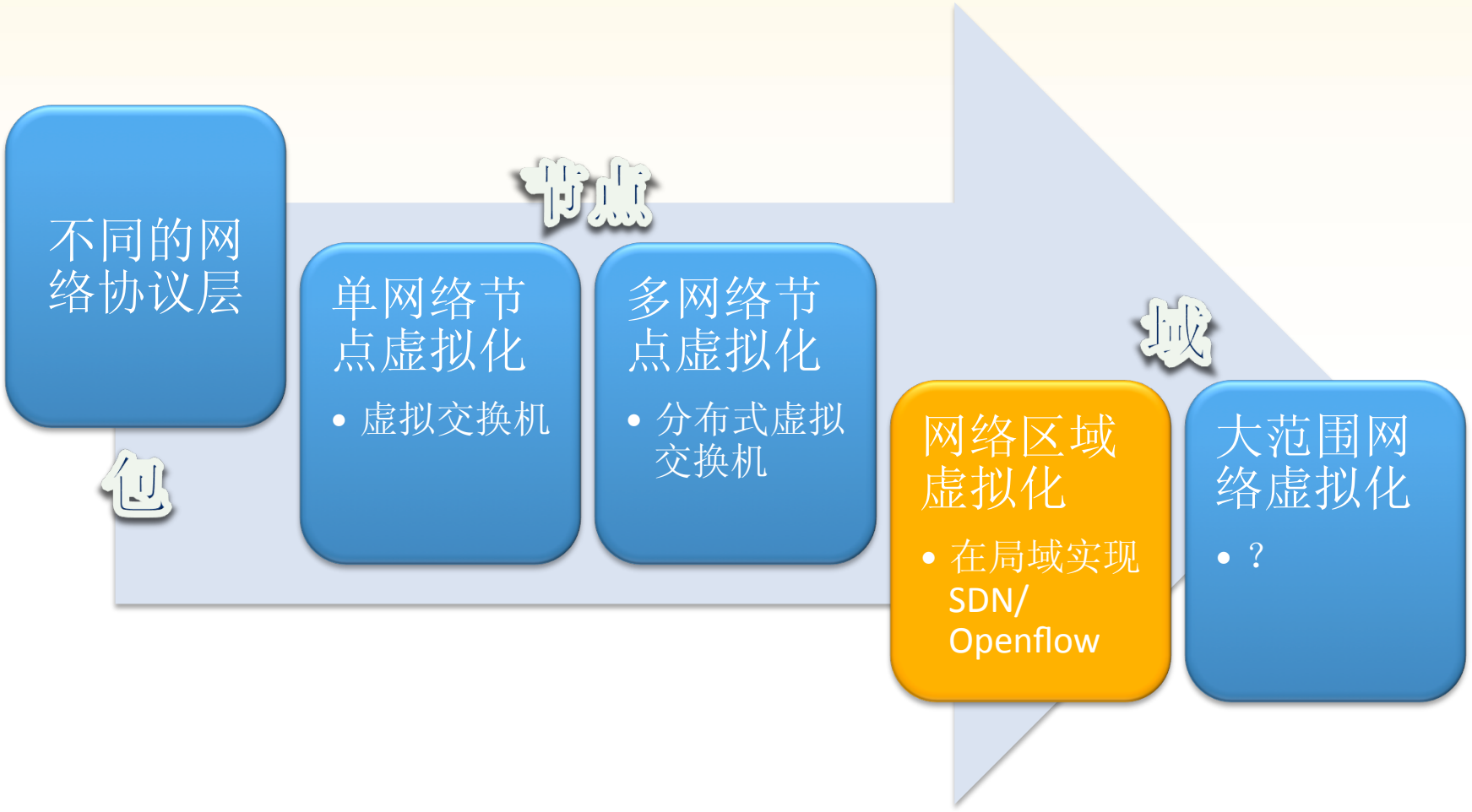
- 可扩展到多个物理服务器，集中管理平面，简化网络管理
- 典型代表：Vmware vDS、Cisco 1KV和Openvswitch
- 存在的问题
  - 大二层扁平网络：广播风暴，VLAN局限性
  - 虚拟和物理网络隔离问题
    - MAC表爆炸
    - 跨子网迁移问题



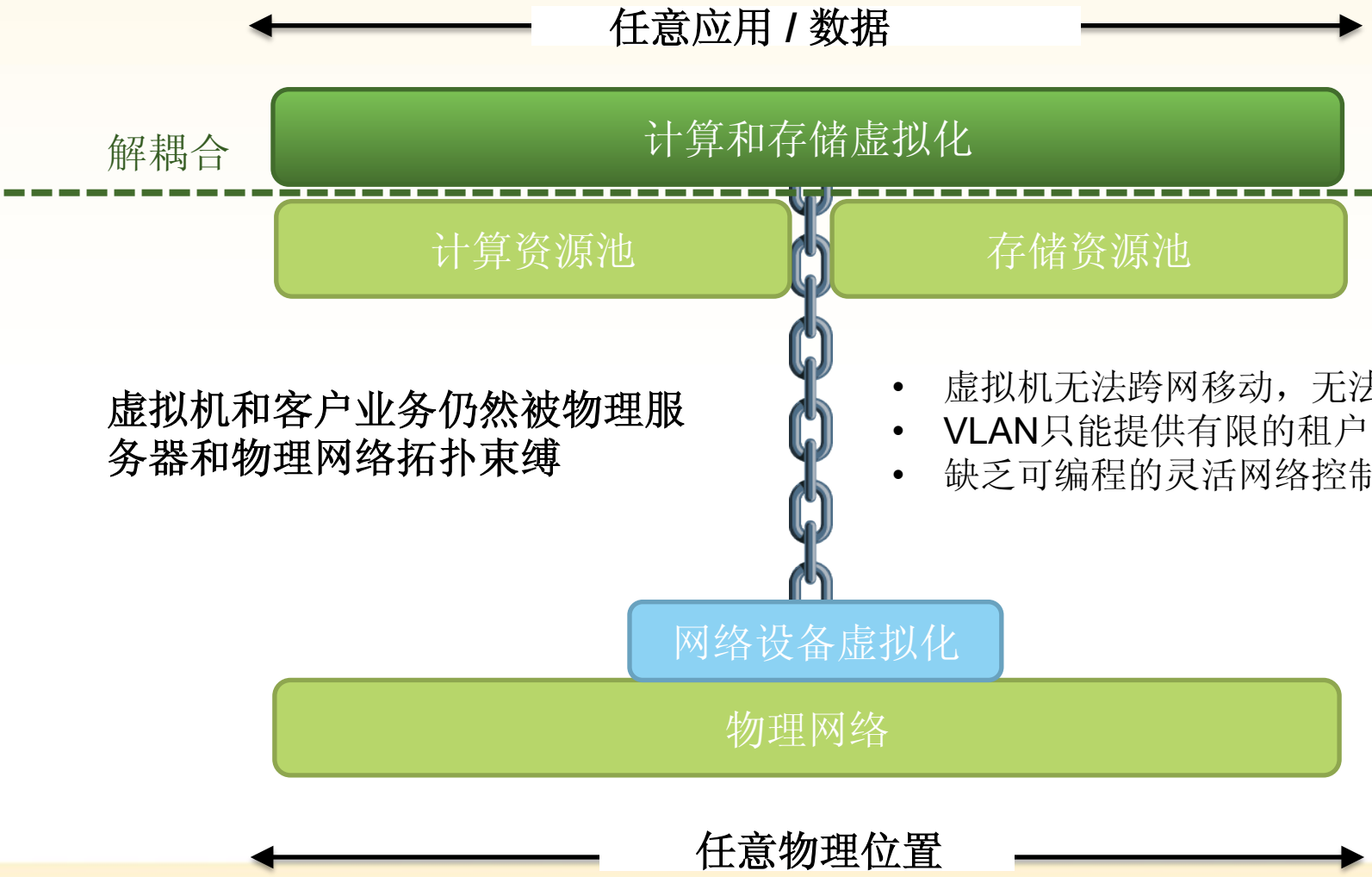
分布式交换机环境下的安全部署



网络虚拟化的不同范围


不同的网络协议层
包
节点
单网络节点虚拟化
• 虚拟交换机
多网络节点虚拟化
• 分布式虚拟交换机
域
网络区域虚拟化
• 在局域实现SDN/ Openflow
大范围网络虚拟化
• ?

网络虚拟化正在拖云计算后腿



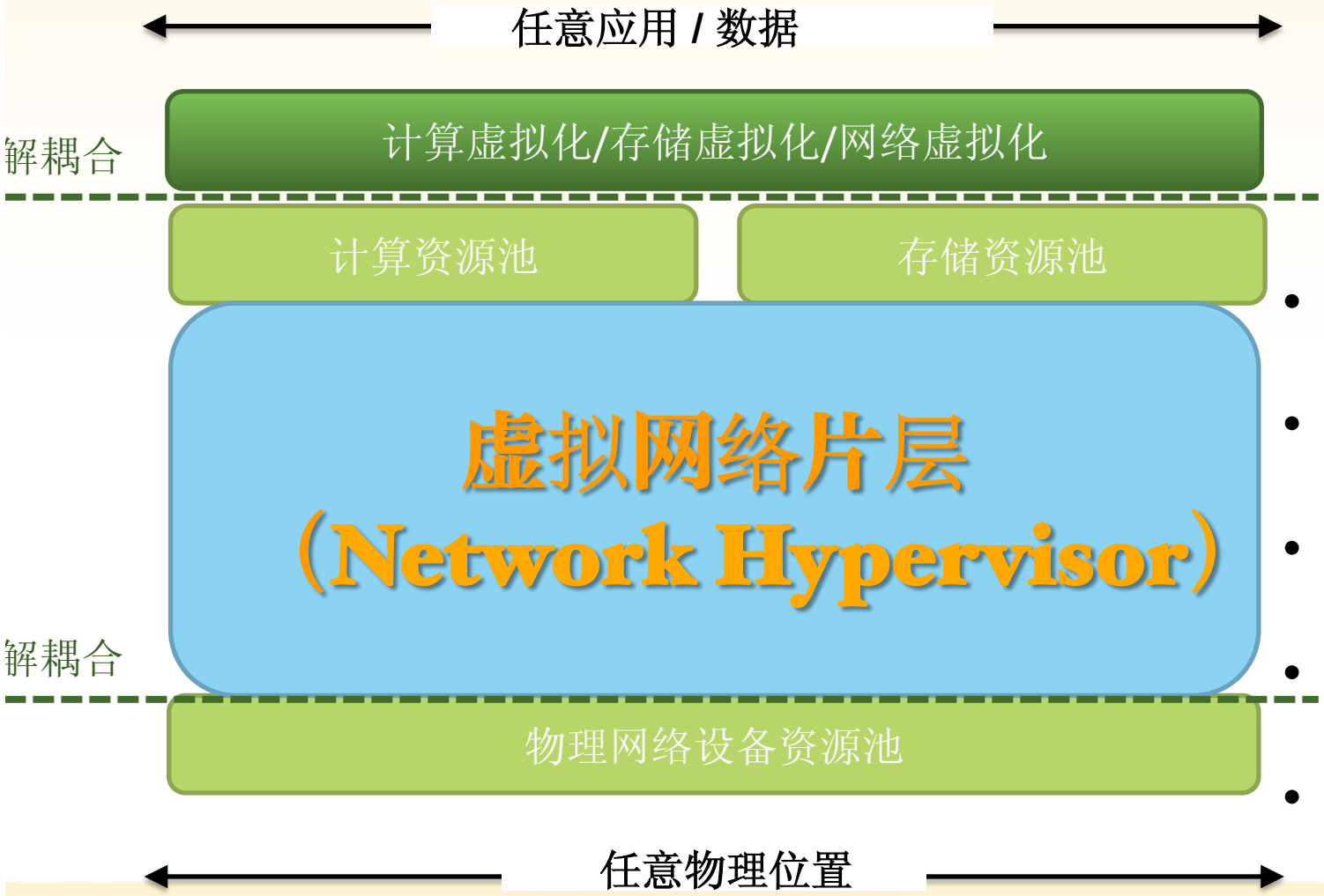
虚拟机和客户业务仍然被物理服务器和物理网络拓扑束缚

- 虚拟机无法跨网移动，无法高度共享
- VLAN只能提供有限的租户隔离能力
- 缺乏可编程的灵活网络控制能力

网络局部虚拟化导致的问题

- 硬件依赖问题（配置虚拟网络需要配置硬件，私有API）
- 网络隔离问题（MAC表爆炸/虚拟IP不重叠/VM跨网迁移）
- 服务升级问题（硬件服务依赖，升级周期长，成本高）
- 可扩展性问题（虚拟域和应用隔离需求，VLAN数量有限）
- 安服集成困难（实施点苛刻，串行网关，动态虚拟边界）

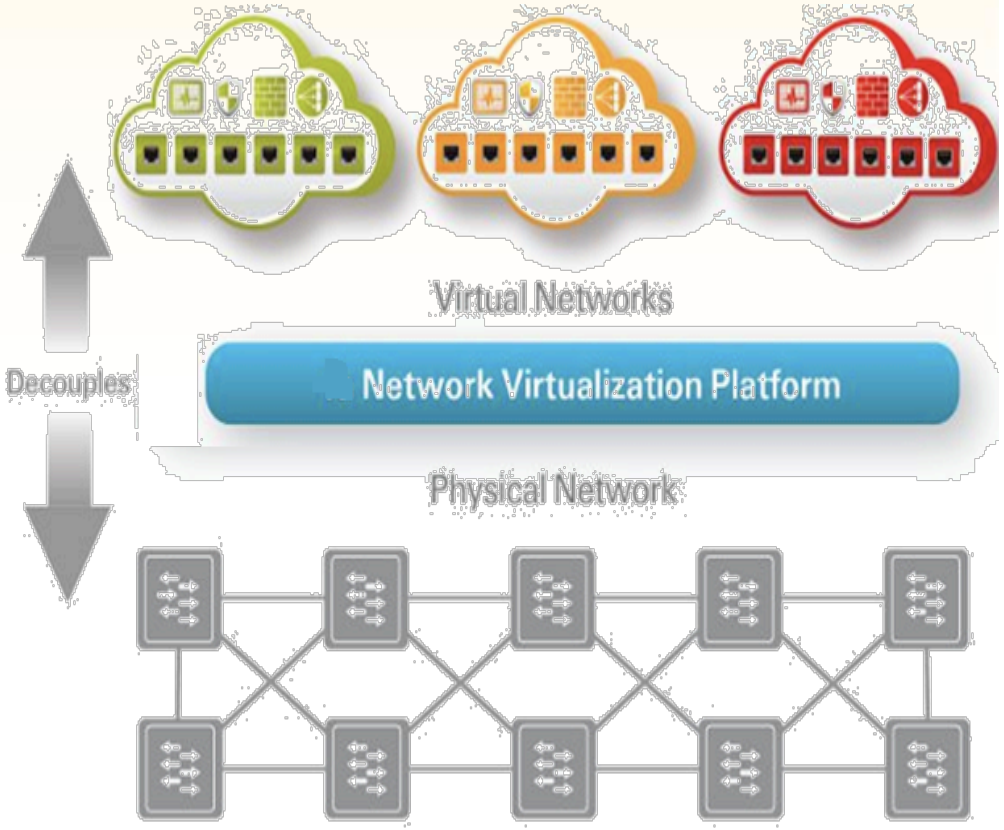
云计算需要全网络域的虚拟化



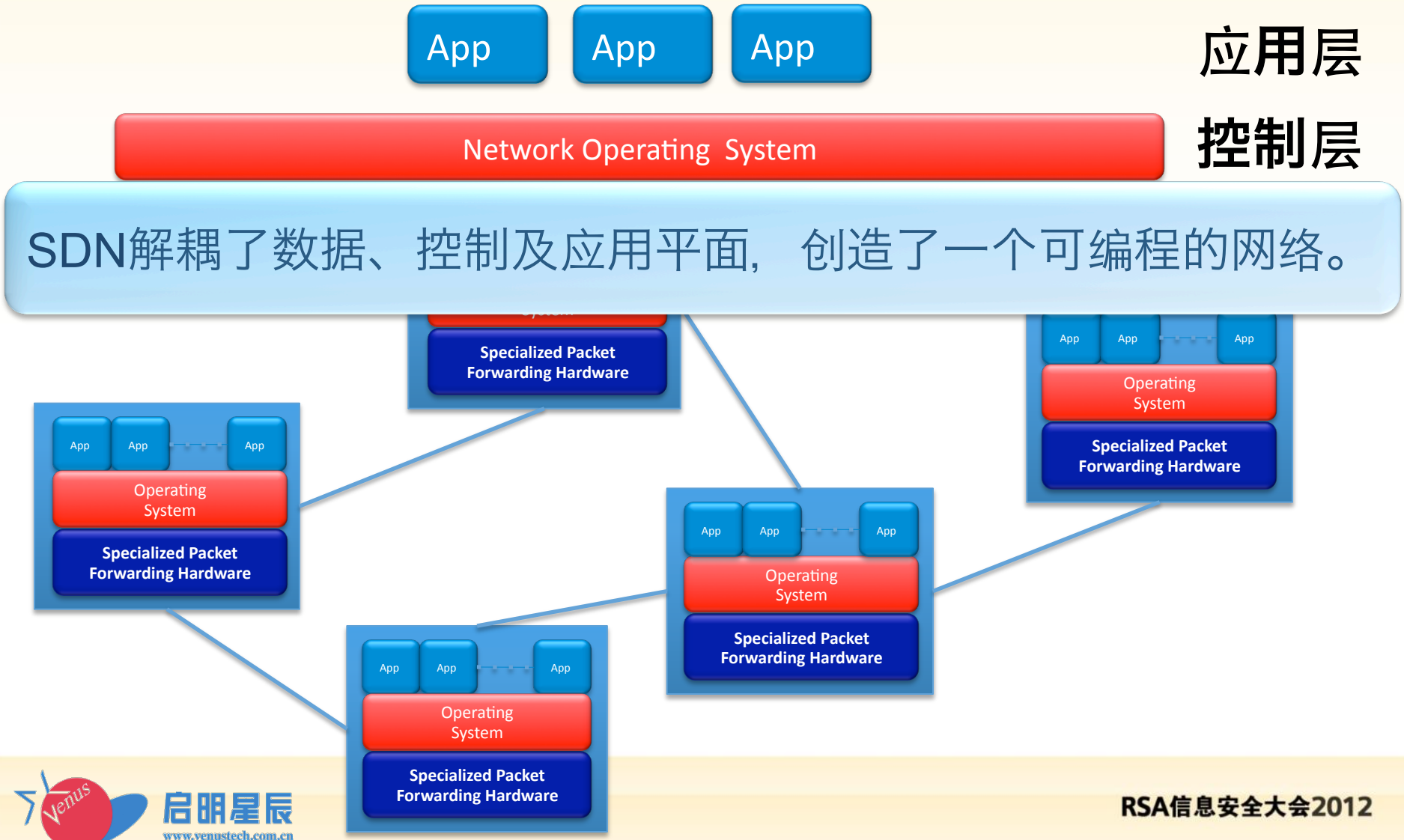
- 两层独立发展
- 软件定义网络
- VM跨网迁移
- 底层硬件维护
- 高共享资源池

虚拟网络片层-适合云的网络虚拟化

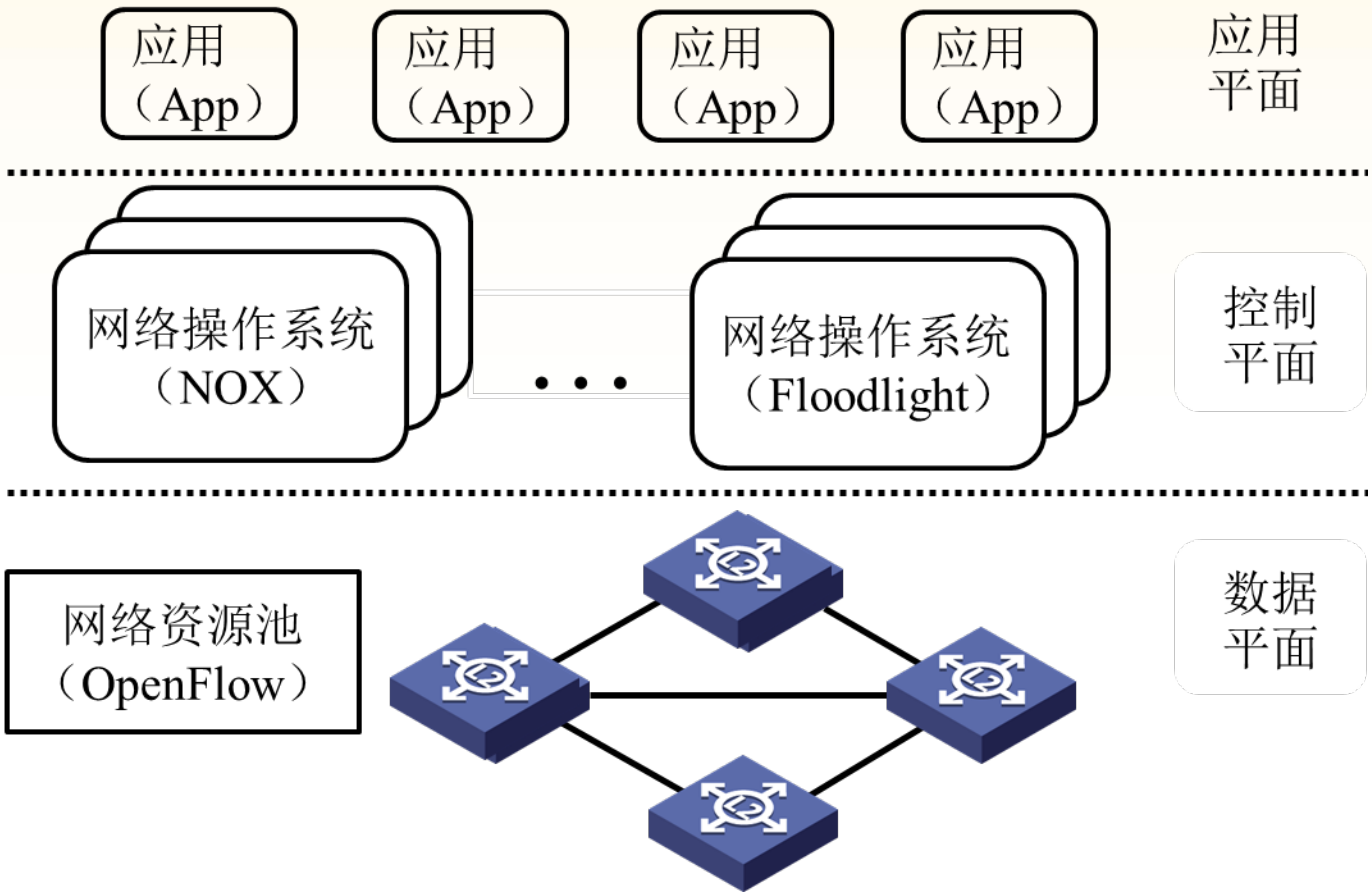
- 上层虚拟网络和底层网络硬件分离，硬件维护简单，网络资源共享
- 虚拟网络具有物理L2网络全部功能，无缝迁移
- 虚拟网络和物理网络地址空间隔离
- 虚拟网络具有完整生命周期：创建、调整、删除



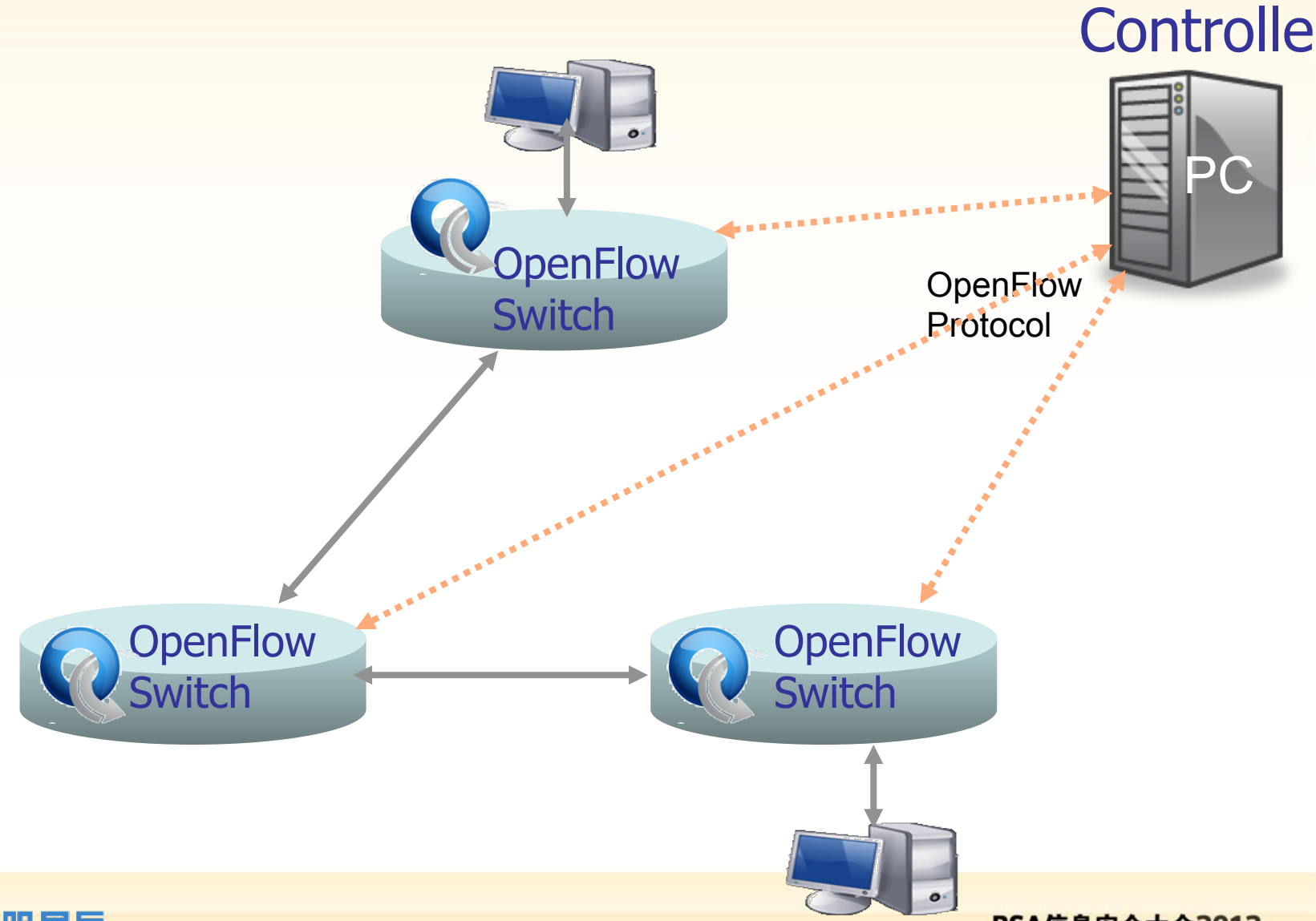
SDN/Openflow：虚拟网络片层实现核心技术



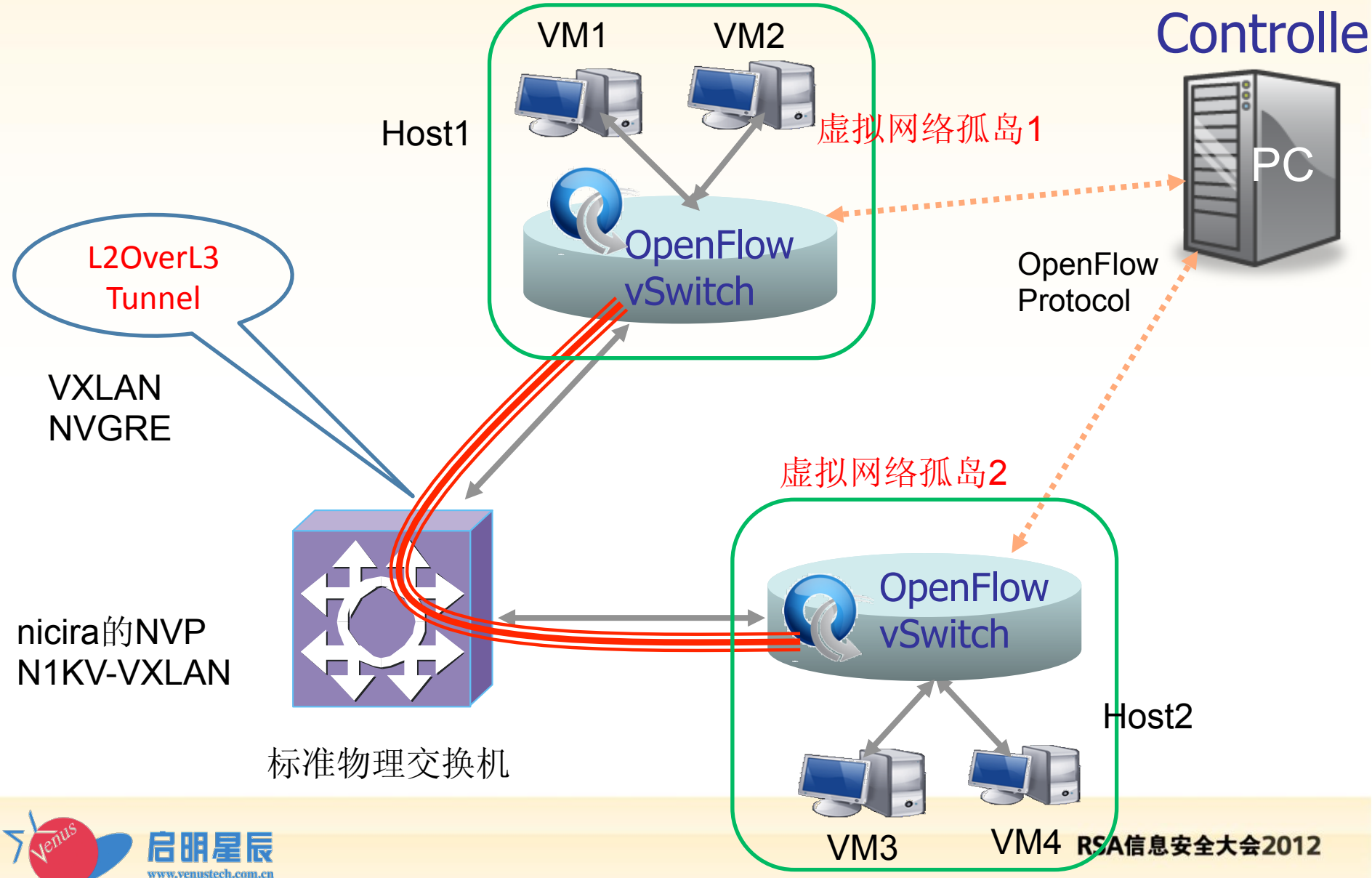
SDN/Openflow：虚拟网络片层实现核心技术



虚拟网络片层：传统SDN/openflow网络



虚拟网络片层：演进的虚拟覆盖网络

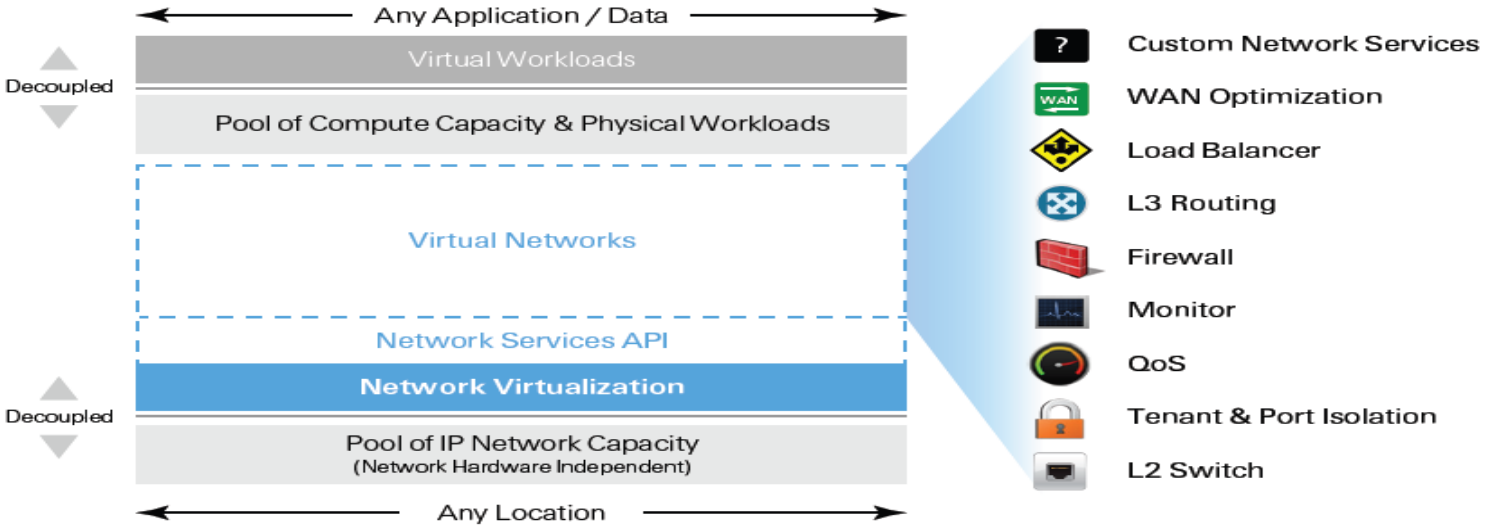


虚拟片层带来的独特安全问题和机会

- 独特安全问题
  - 集中控制节点问题， 网络大脑， 确保controller安全，提升controller可用性
  - App安全问题， 恶意App， app可信， 白名单
  - 通信安全问题， 伪造controller， 数据交换安全
  - 规则冲突问题， 安全APP和其它App之间规则冲突， 安全策略失效， 需要可靠的安全策略实施框架
- 安全机会
  - 数据平面和控制平面分离模式， 集中控制平面
  - 易实现PDP+PEP模式的动态安全策略

虚拟片层环境下的安全服务部署

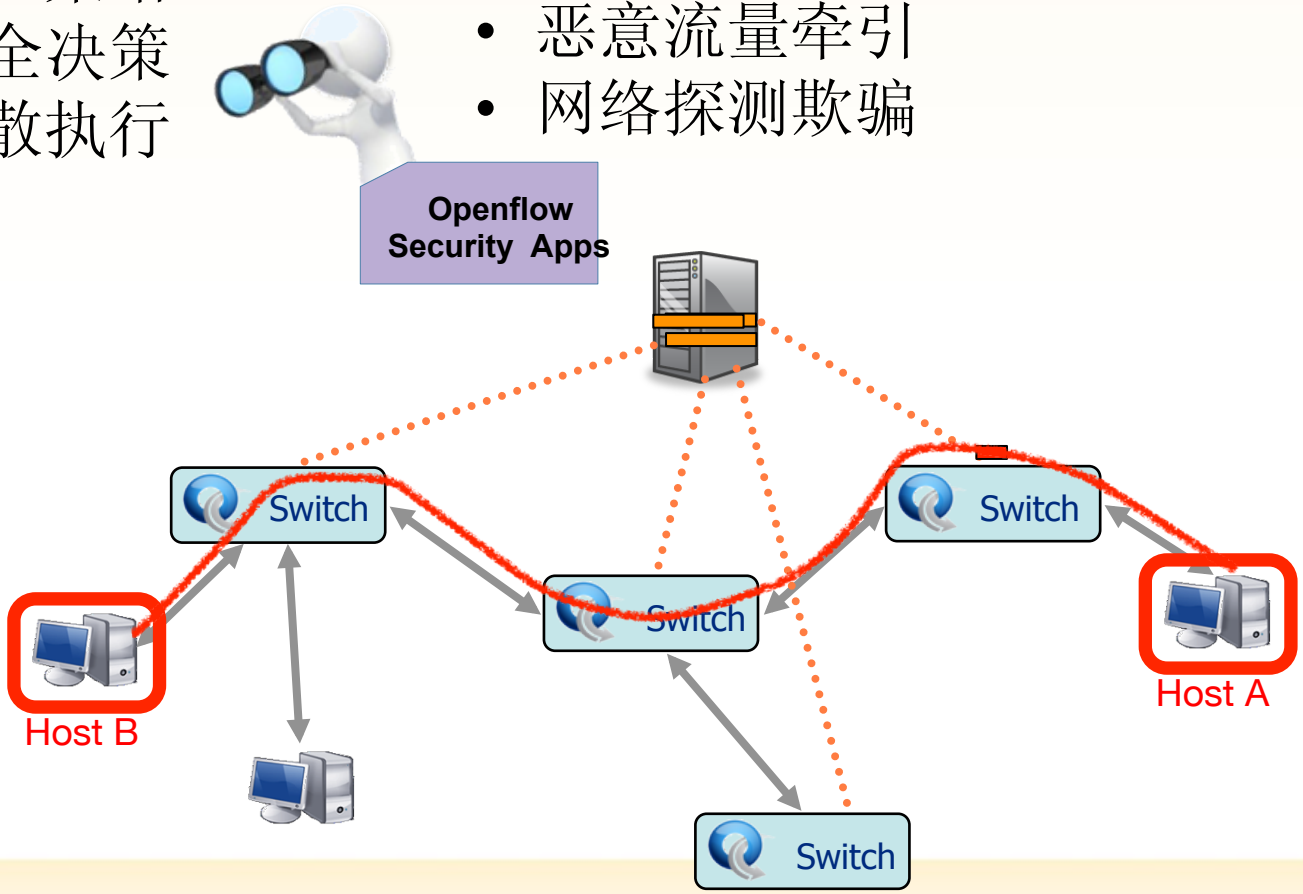
- 安全服务实现模式与传统网络有些不同
- 两种安全服务部署模式
  - Proactive（静态openflow规则）
  - Reactive （动态openflow规则）



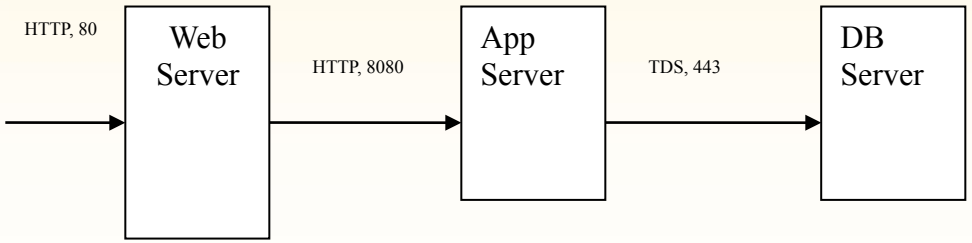
Reactive模式安全服务

- 全局网络视野
- 一致安全策略
- 在线安全决策
- 策略分散执行

- 流过滤防火墙
- 蠕虫扫描检测
- 恶意流量牵引
- 网络探测欺骗



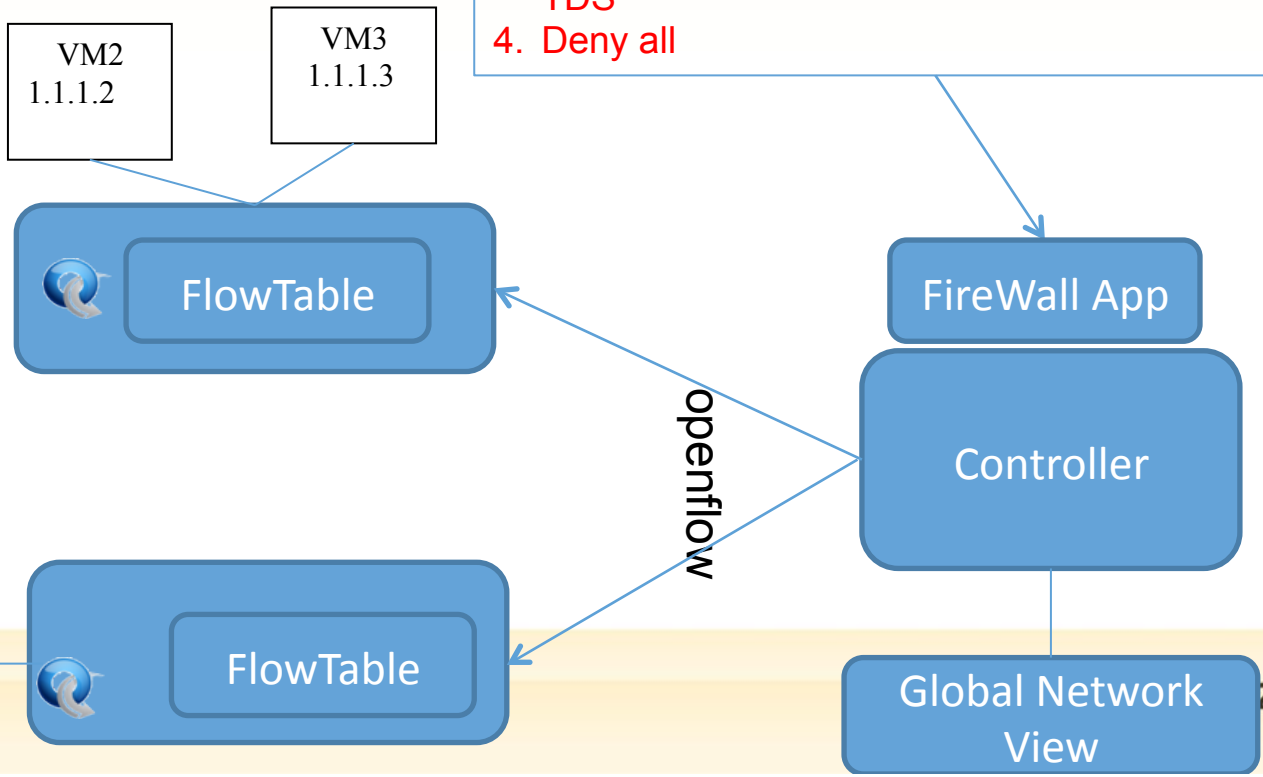
流过滤防火墙实例



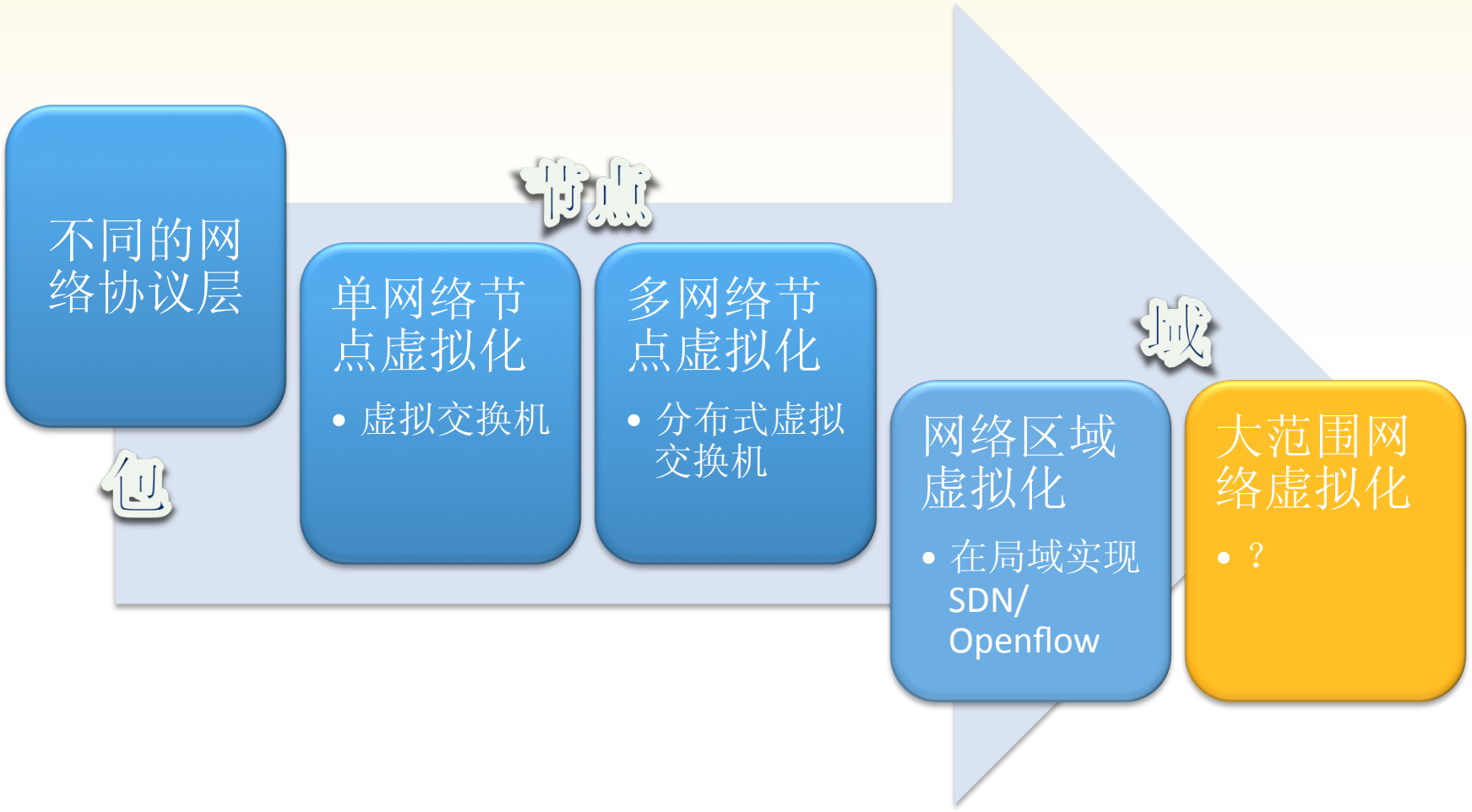
业务安全策略

1. Allow any to access WebServer at Port 80 with HTTP
2. Allow WebServer to access AppServer at 8080 with HTTP
3. Allow AppServer to access DBServer at 443 with TDS
4. Deny all

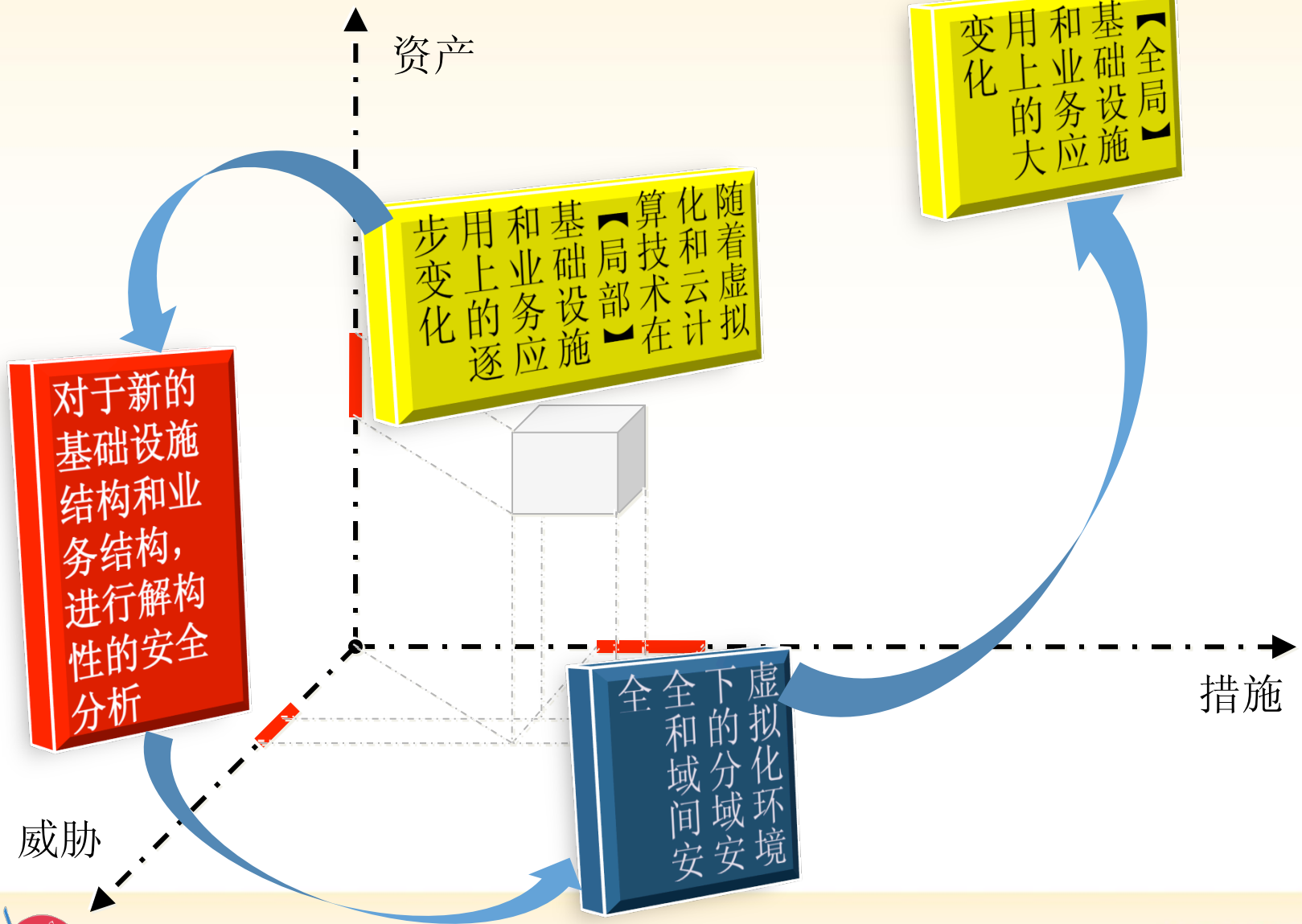
业务拓扑

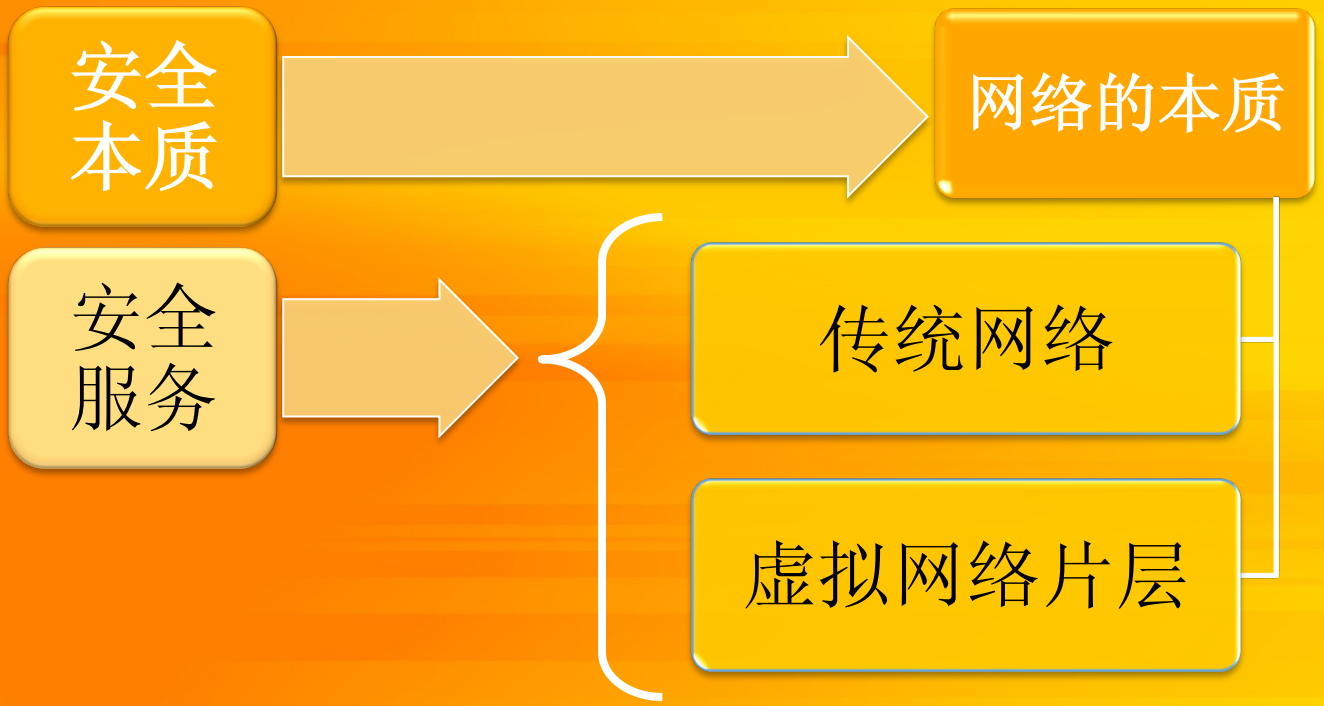


网络虚拟化的不同范围


不同的网络协议层
包
单网络节点虚拟化
• 虚拟交换机
节点
多网络节点虚拟化
• 分布式虚拟交换机
网络区域虚拟化
• 在局域实现SDN/ Openflow
域
大范围网络虚拟化
• ?

云计算发展当前阶段的安全策略





谢谢