



IT大咖说
知识分享平台

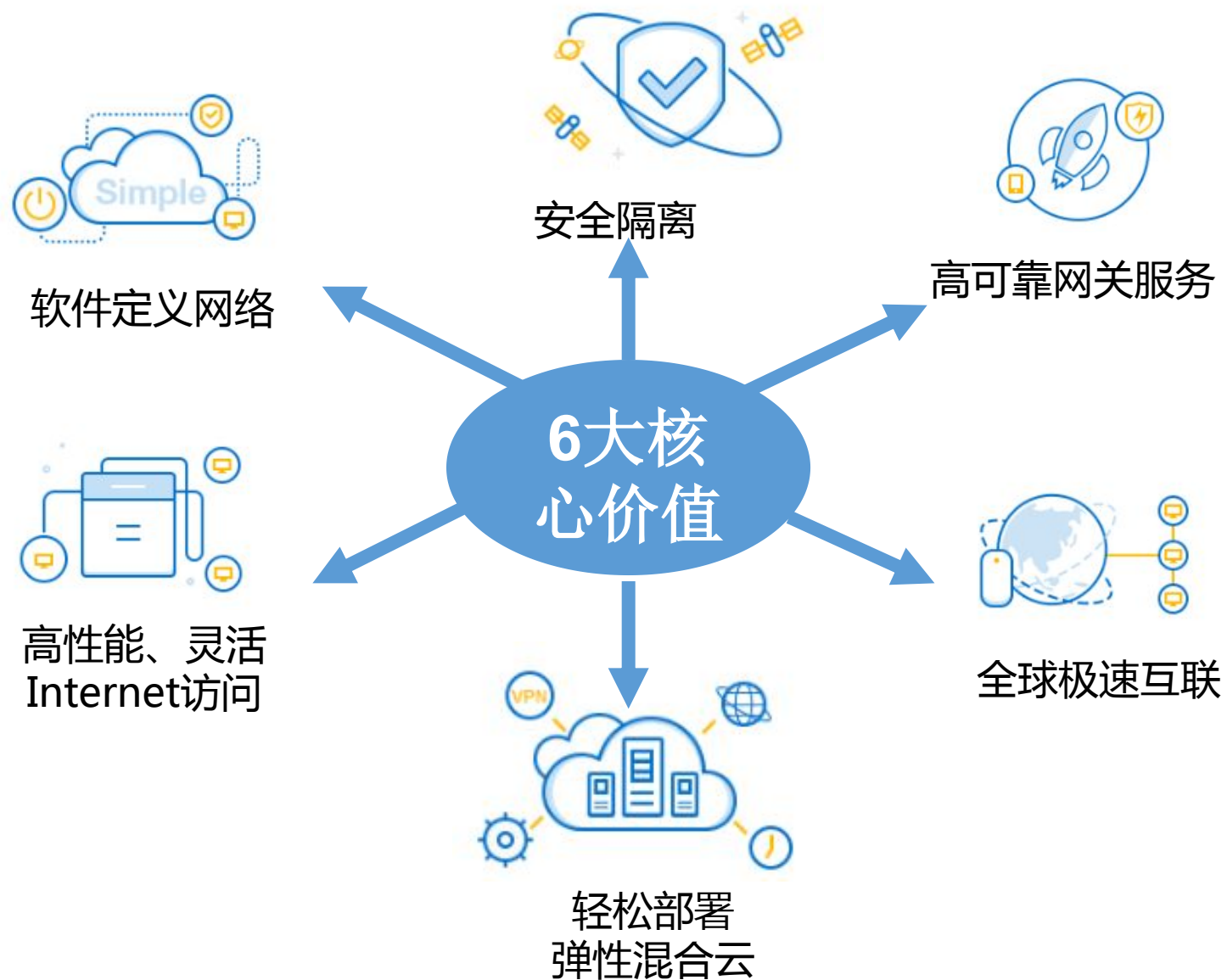


腾讯云

腾讯云网络和VPC服务实践

腾讯云网络研发工程师 周显平

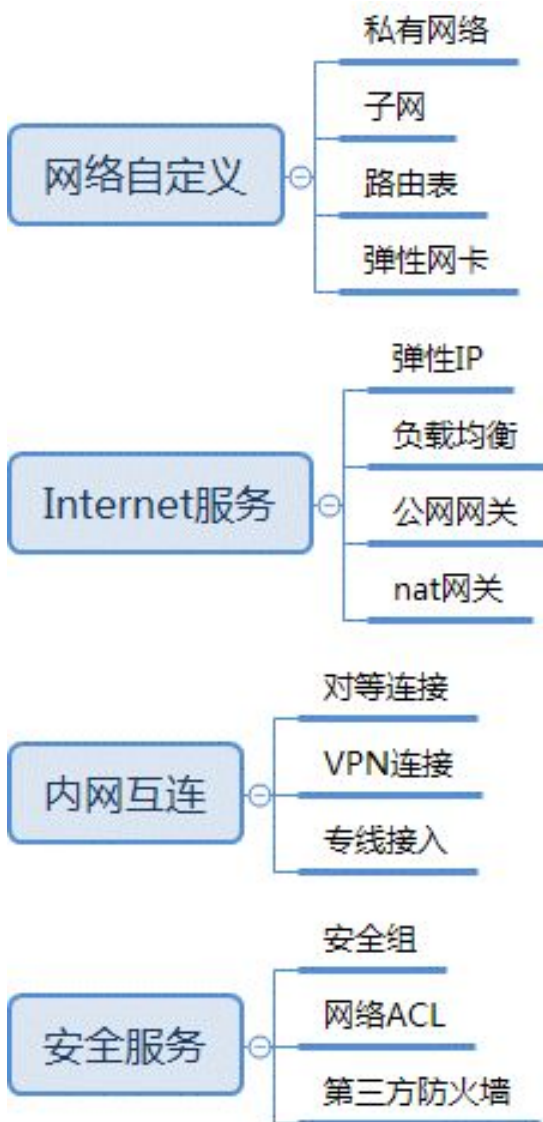
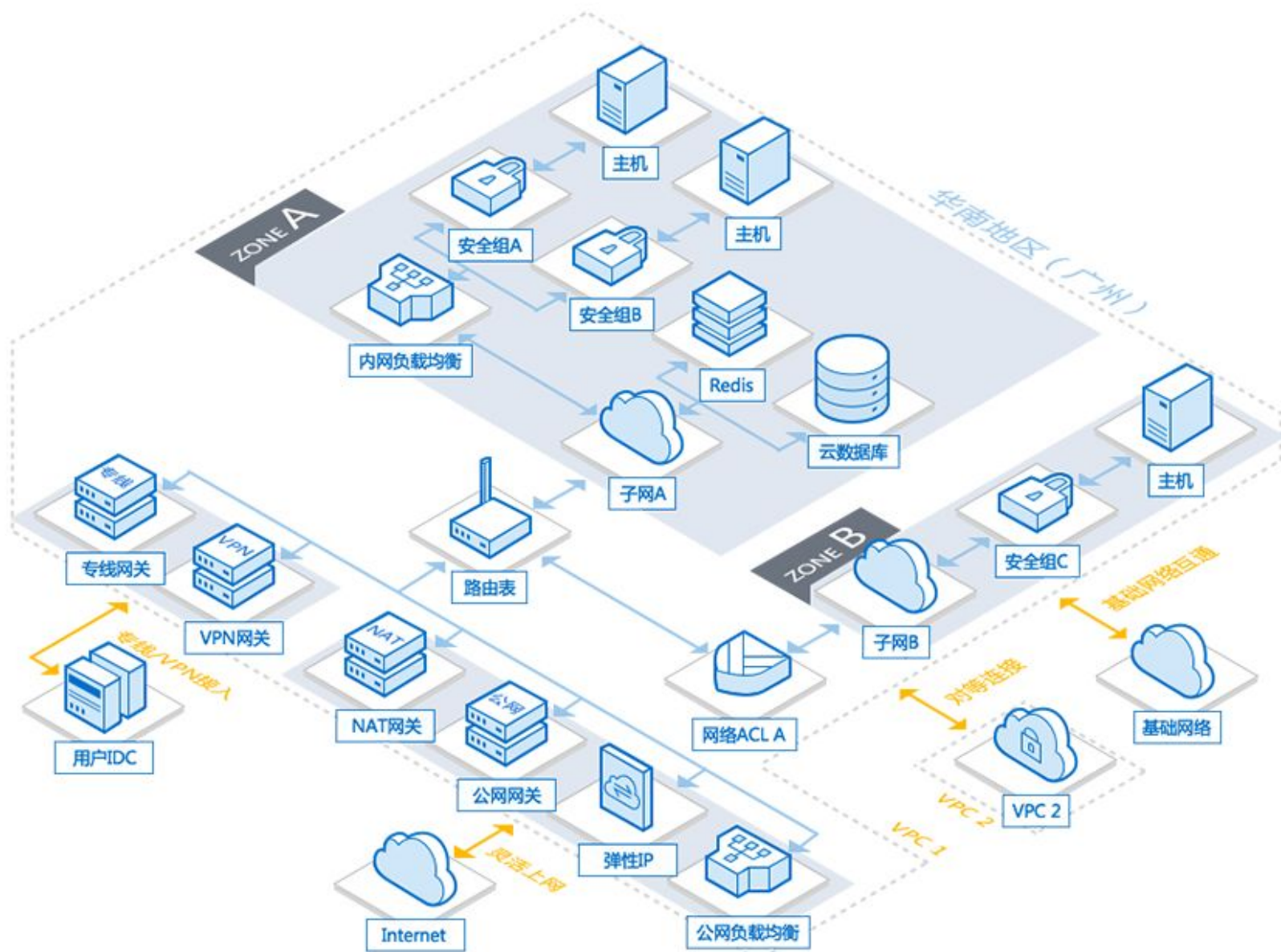
The diagram illustrates the Tencent Cloud ecosystem. At the center is **腾讯云** (Tencent Cloud). Surrounding it are four core services: **云** (Cloud), **支付** (Payment), **安全** (Security), and **LBS** (Location-Based Services). These are connected by a dotted line. The entire ecosystem is enclosed in a large blue arc. Numerous third-party logos are shown around the perimeter, including Sogou, JD.com, Meituan, Didi, Ganji, Mogujie, WeBank, LY.com, eLong, Bilibili, Douyu, and others.



功能概览



IT大咖说
知识分享平台





软件定义网络

通过控制台或API自定义网段划分、创建子网、配置路由表和网关等，以软件定义网络。



私有网络

逻辑隔离的虚拟专用网络专区，可以自定义网络CIDR，用于管理云上的计算资源



子网

对私有网络的网段划分，与传统网络中划分vlan类似，子网具有可用区属性，支持策略路由



路由表

和传统网络路由表类似，用于指引子网网络流量的方向，支持ECMP路由分担



弹性网卡

私有网络云服务器可以配置多张弹性网卡，实现业务在虚拟网卡间的流量隔离，并部署高可靠业务

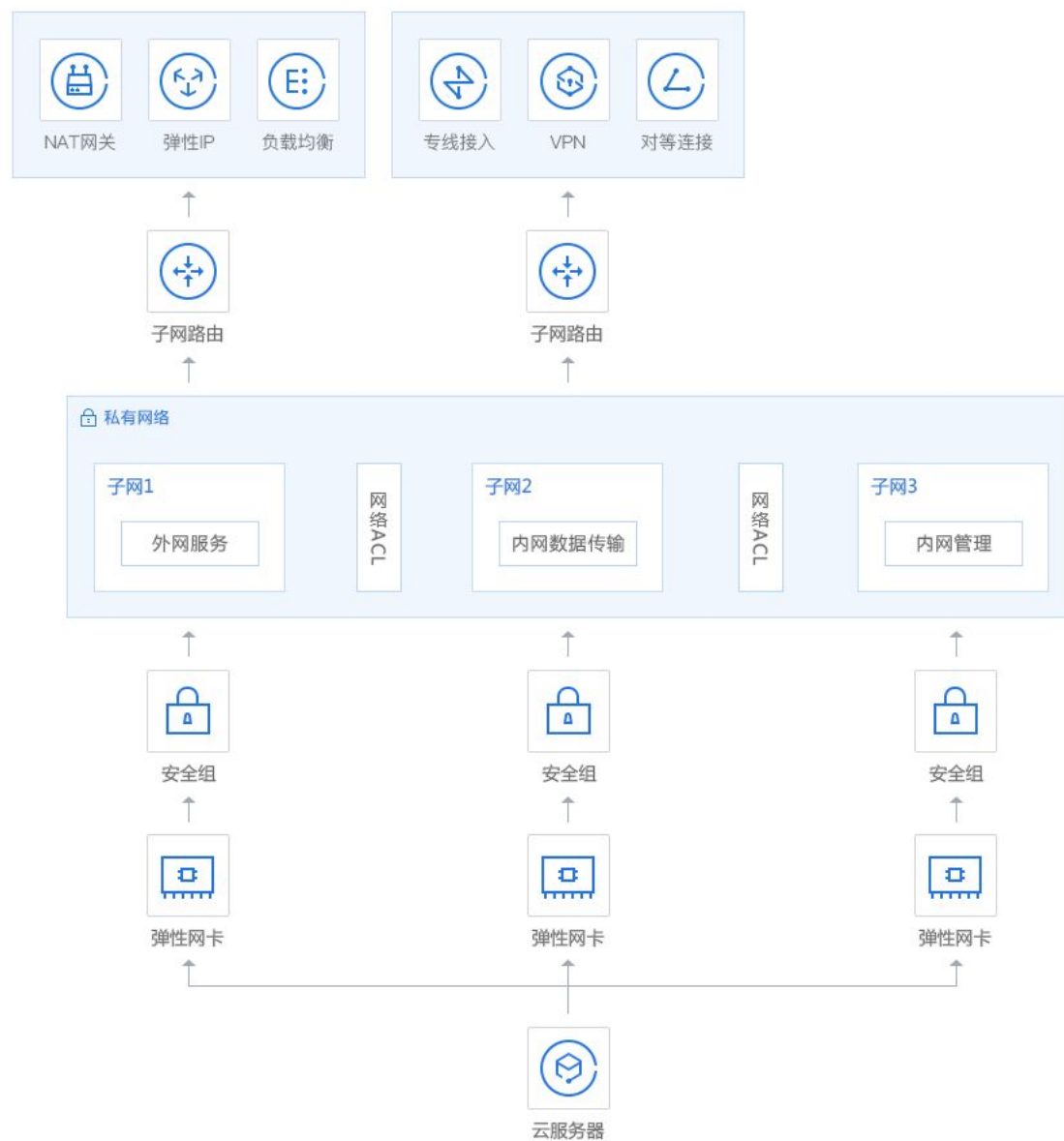
软件定义网络--私有网络、子网、路由表



IT大咖说
知识分享平台



软件定义网络--弹性网卡



【典型应用场景】

- 内网、外网、传输网隔离
- 高可靠应用部署



丰富的Internet访问

腾讯云VPC提供了多种的Internet接入服务，包括：弹性IP、负载均衡、公网网关、NAT网关等



弹性IP

公网IP支持绑定和解绑云主机，灵活应对业务变更、服务器故障迁移



负载均衡

腾讯云提供的4&7层负载均衡服务，支持内、外网环境，负载均衡挂载主机支持弹性扩缩容



公网网关

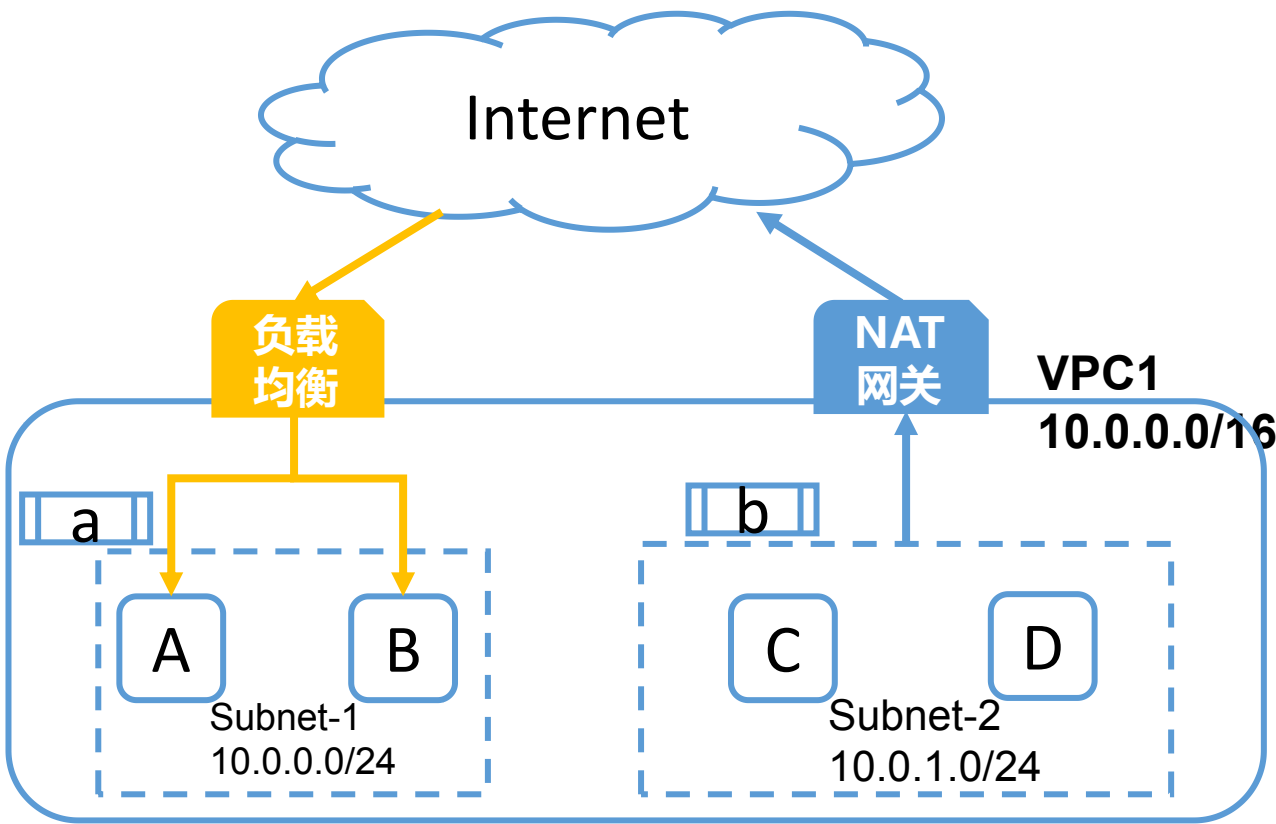
指定云服务器作为子网网关，用于部署公网代理上网，也可以安装第三方镜像用作网络防火墙，支持ECMP路由



NAT网关

专用的公网代理上网网关，底层基于主、备高可靠集群搭建，最大带宽吞吐可达5Gbps

Internet访问--NAT网关，负载均衡



- Subnet-1：负载均衡对外提供服务
- Subnet-2：通过nat网关主动访问internet

路由表a

目的端	下一跳
Local	Local

路由表b

目的端	下一跳
Local	Local
0.0.0.0/0	Nat网关



灵活的内网互联

腾讯云提供私有网络间、公有云服务商间和基础IDC服务间的内网互连服务，包括：对等连接、VPN接入、专线接入等



对等连接

用于腾讯云上多个私有网络间的内网互连服务，支持云上 **跨地域**、**跨账号** 的互连



VPN接入

腾讯云提供的标准vpn接入模式，支持Ipsec 和SSL 两种接入模式



专线接入

数分钟即可部署全球同服，助力您实现游戏出海。

内网互联 – 全球同服案例



IT大咖说
知识分享平台

客户案例：A公司有一款全球同服的游戏《王者远征》希望构建全球同服网络。。

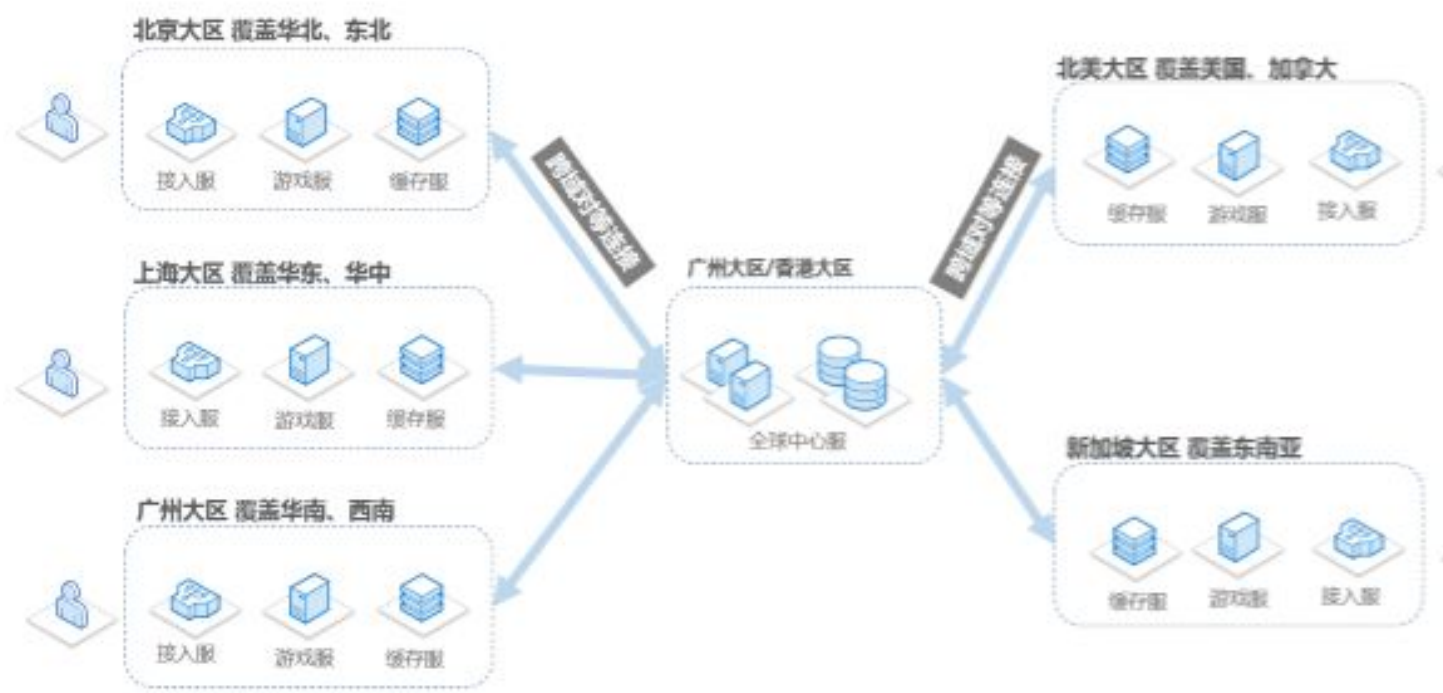
核心诉求：

- 核心数据集中部署，尽量避免跨区域数据通信；
- 游戏玩家分地域就近接入，降低时延；
- 各地域之间数据高速互联，如进行跨服战等。

解决方案

- 数据中心遍布全球，数据库集中部署
- 利用DNSPod云解析智能调度实现就近访问
- 利用对等连接实现全球网络高速互联，**最大支持5Gbps吞吐，专线品质，SLA保障**

他们都在用：



灵活的内网互联 – 全球同服案例



IT大咖说
知识分享平台

核心优势

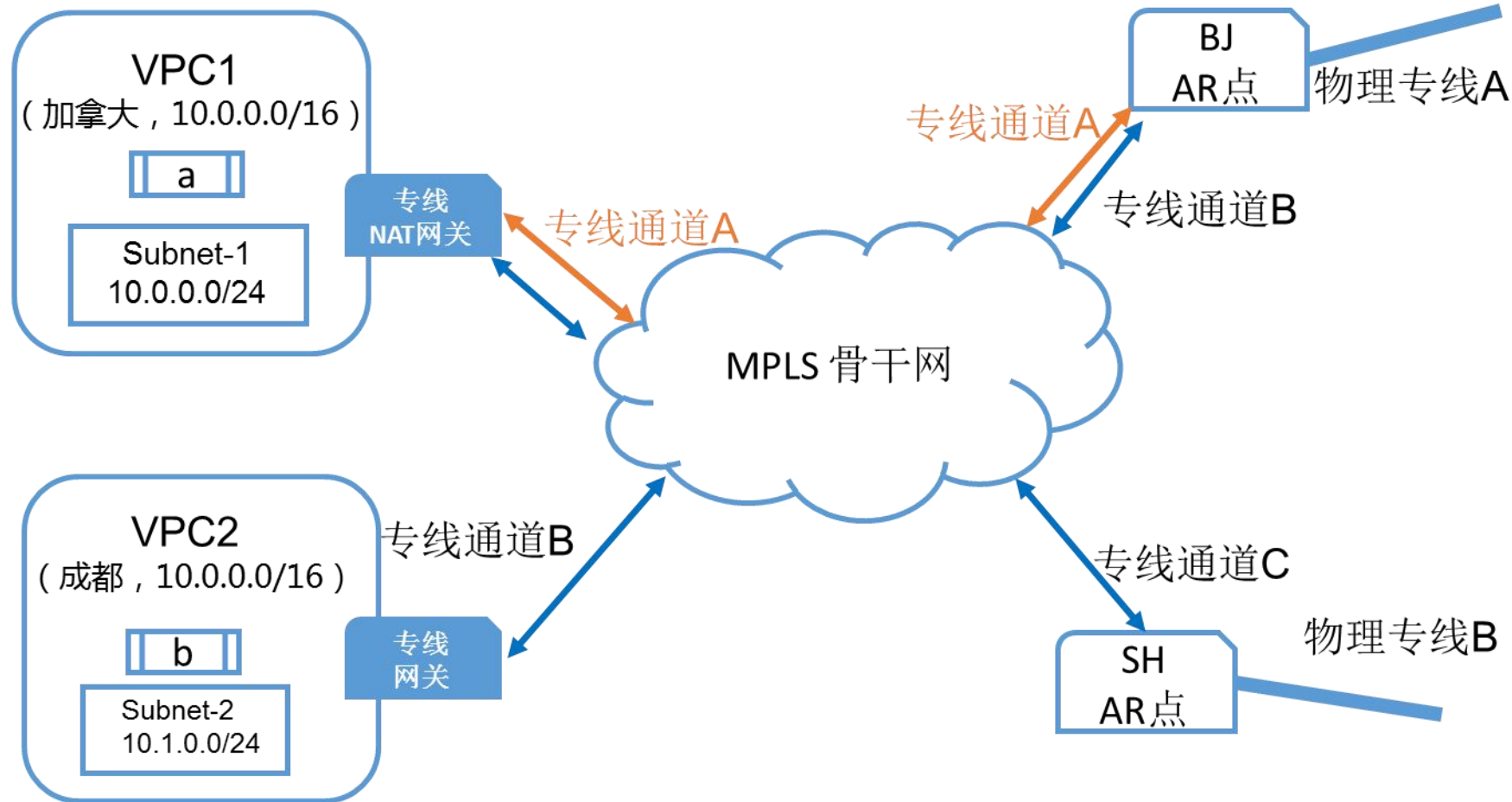
• 接入点覆盖广

北京、上海、广州、深圳、天津、
重庆、成都、香港、新加坡、硅
谷、多伦多等

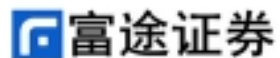
• 单点接入，多地打通

• 网关支持snat、dnat

中国电信、中国联通、中国移动、
游驰、犀思云、澳洲电信、
PCCW、HGC 等



他们都在用：



内网互联——混合云部署案例



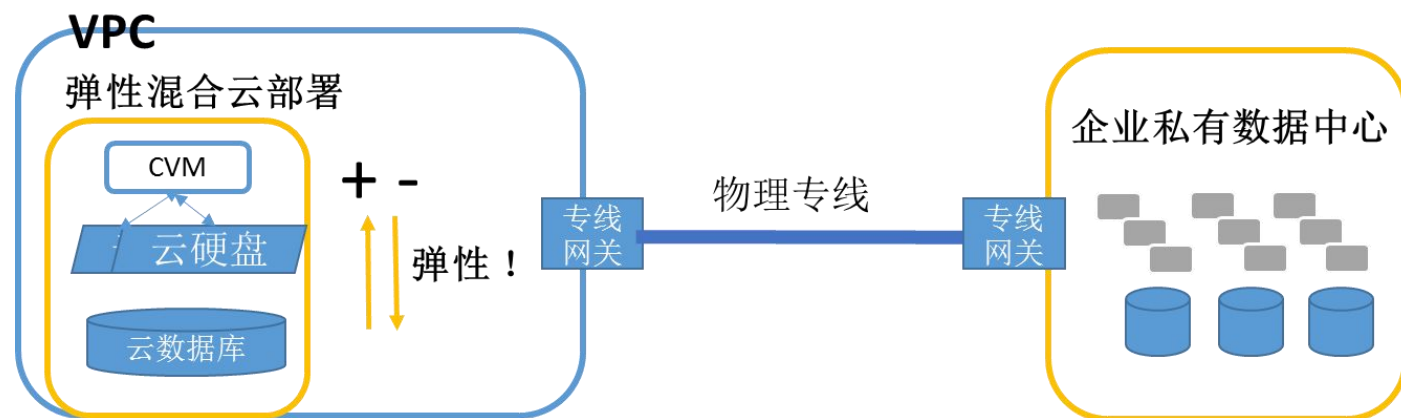
IT大咖说
知识分享平台

用户案例：A公司可以通过一条物理专线一次性打通位于多地域的腾讯云计算资源，实现灵活可靠的混合云部署，核心诉求：

- 高可用、大带宽、
- 网络质量有保障、不受公网质量影响
- 解决IP地址冲突

解决方案：

- 云上数据中心：在腾讯云创建的私有网络
- 连接方式：物理专线，**最大支持10Gbps**
- 连接备份方式：双专线备份
- 解决IP地址冲突：**专线NAT网关**



他们都在用：





安全

VPC是**逻辑隔离**的网络地址空间。另外，**网络ACL**和**安全组**分别从子网和主机维度筛选流量，可精确到**端口和协议**维度。



基础设施安全

世界一流的数据中心
腾讯云安全专家7*24服务



网络ACL

子网维度的出入流量控制，
可精确到端口和协议维度。



安全组

主机维度的流量控制，可
精确到端口和协议维度。



第三方安全镜像

深信服，山石下一代防火
墙等

安全服务 案例



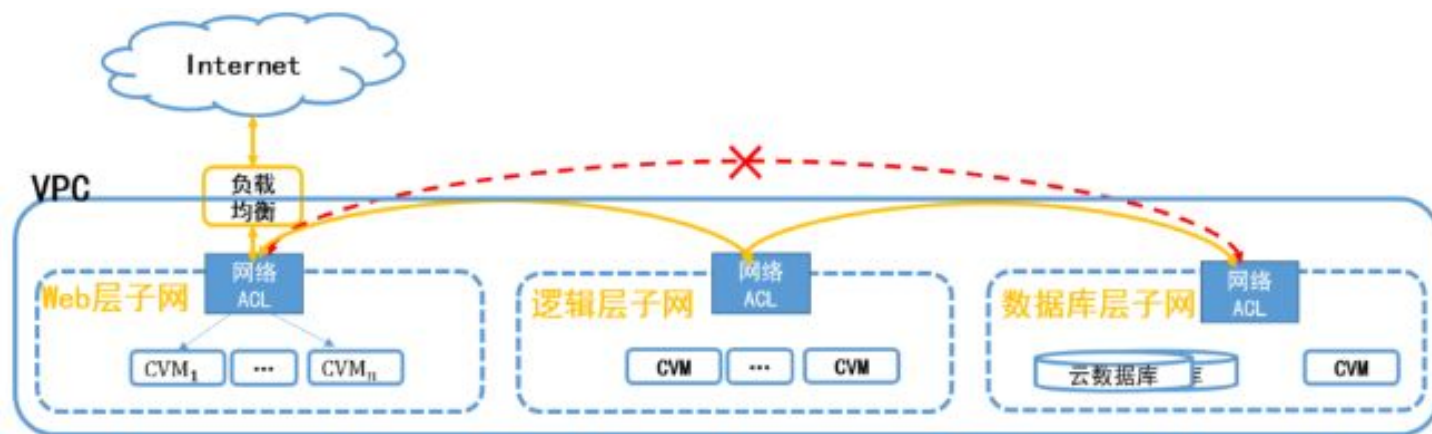
IT大咖说
知识分享平台

用户案例：A公司部署多层web应用，其核心诉求

- 与其它租户完全隔离，规避多租户共享带来的风险。
- 能与Internet通信
- 保障数据库服务器的安全

解决方案：

- 私有网络内创建三个子网：web层子网、逻辑层子网、数据层子网
- web层子网：可访问Internet、同时利用LB均分流量
- 逻辑层子网：不允许公网访问
- 数据库层子网：只允许逻辑层子网的流量访问



他们都在用：





独家优势

支持外网IP直通、子网广播和组播功能，公有云市场仅此一家，体现了腾讯网络能力丰富，是众多客户选择腾讯云的主要原因。



外网IP 直通

使得发送到云主机上的数据包的目的地址是外网IP



广播

能同时向子网中的多台计算机发送消息



组播

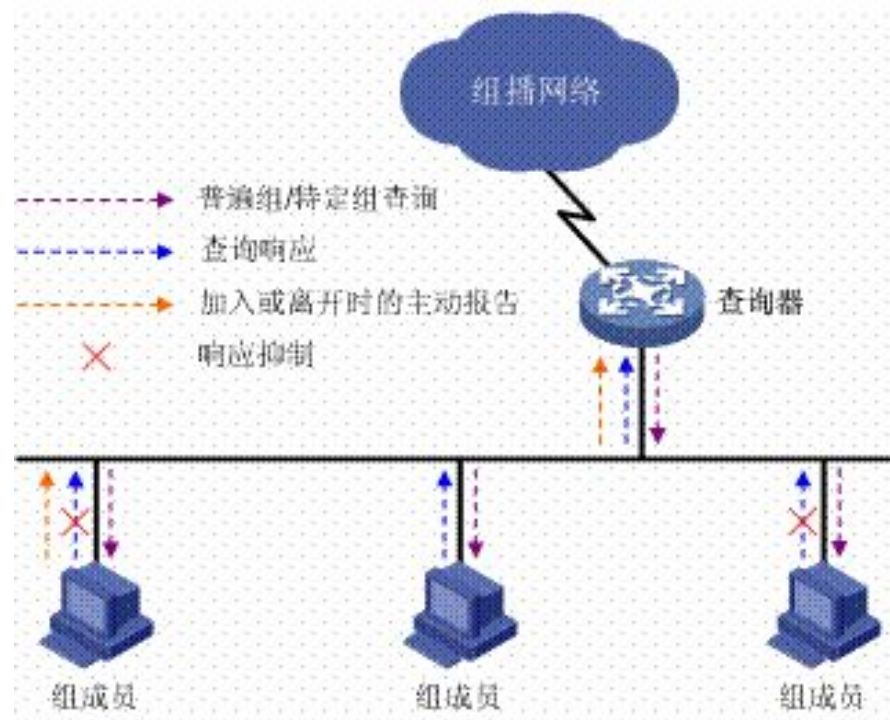
可以将消息从一台云主机发送到本网或全网内选择的云主机子集上

客户案例：某证券交易所的某台主机负责实时发布证券交易信息，接受组主机负责接收并处理这个信息，核心诉求：

- 解决发送方主机网络性能瓶颈限制
- 接受组成员关系管理
- 节约网络带宽

解决方案：

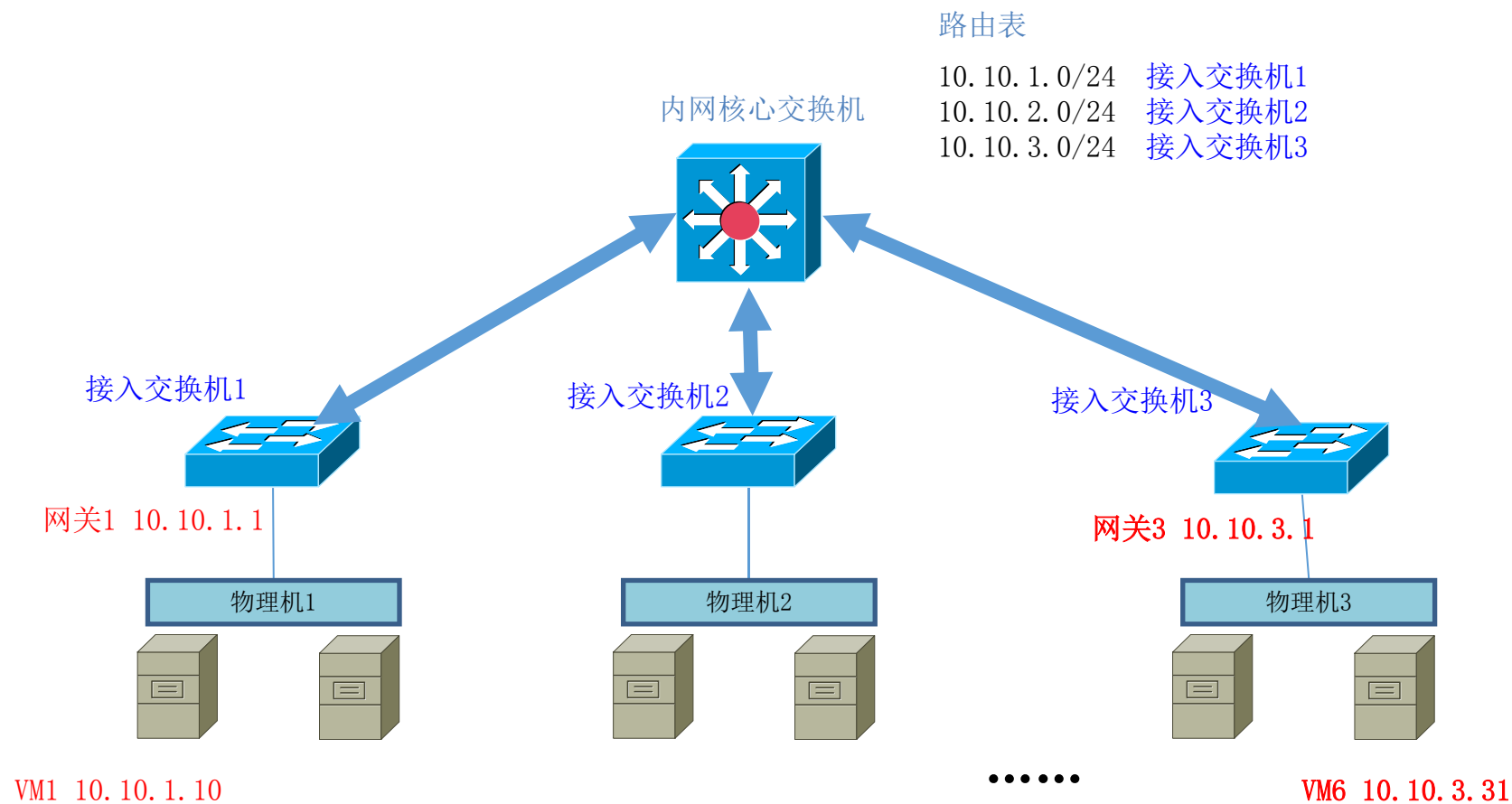
- 使用私有网络内组播服务，解决单机性能瓶颈
- 配置组播组
- 使用组播而不是广播，以降低网络负载





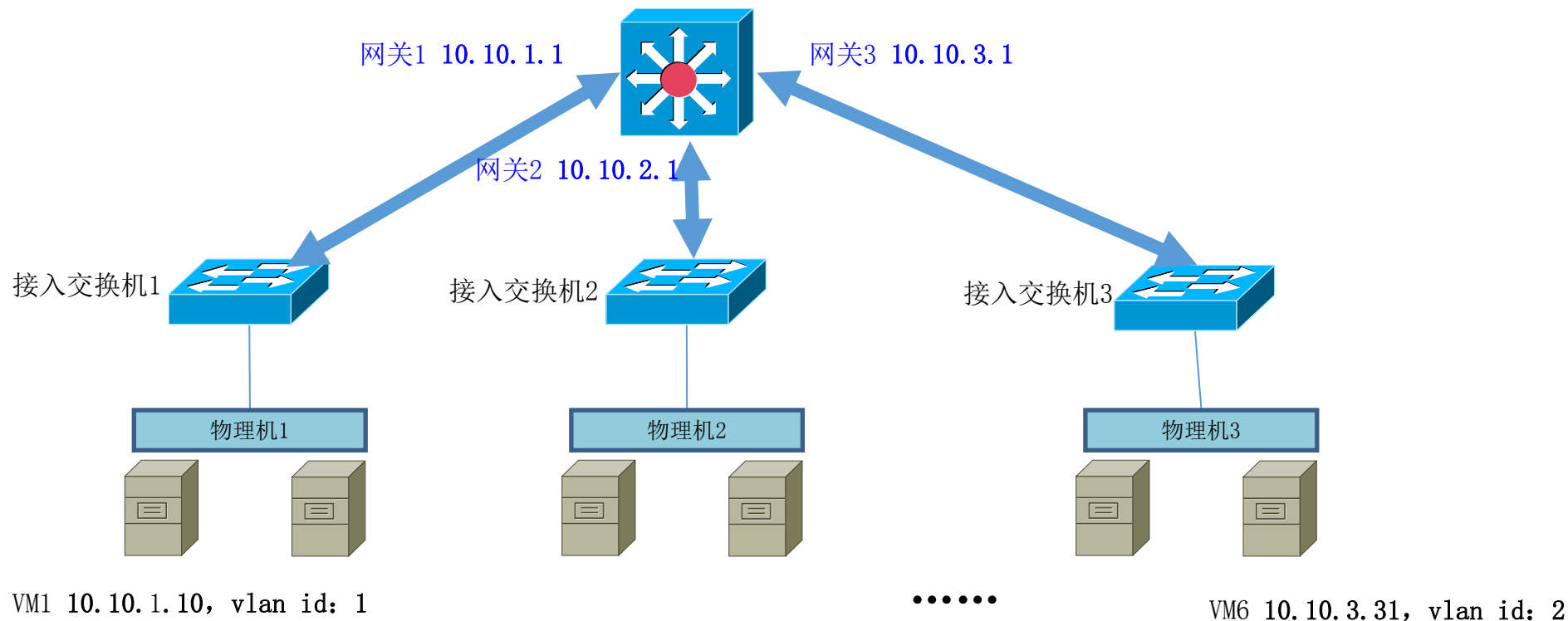
技术原理

传统虚拟化三层网络



- 简单，静态， IP地址与交换机关联
- 限制：
 - 虚拟主机无法在机房内随意迁移
 - 交换机下IP地址提前规划好， 约束虚拟比

传统虚拟化二层网络



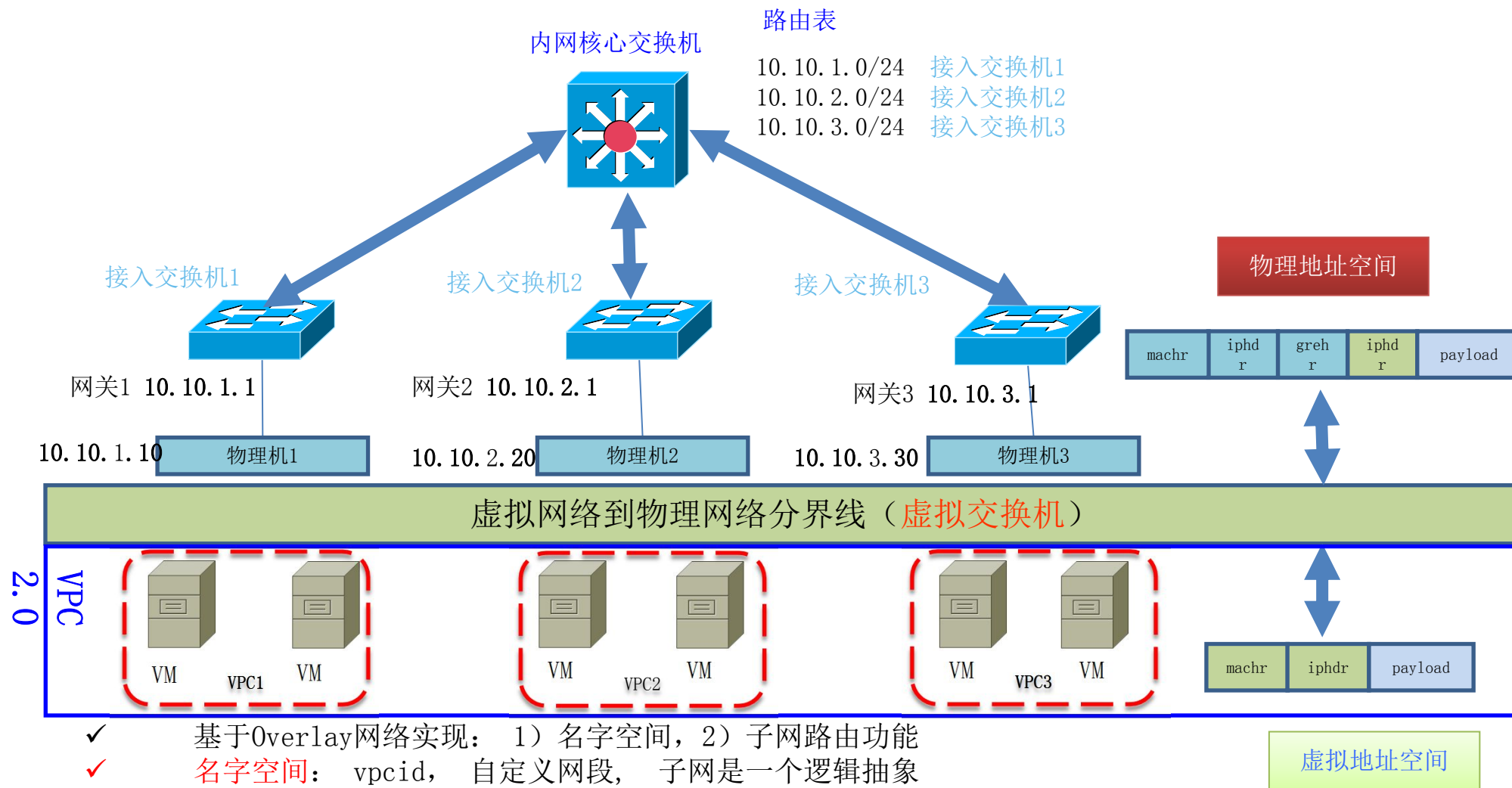
特点:

IP地址与交换机无关，虚拟机可在机房范围内迁移

弱点:

1. 依赖<mac, 端口>映射关系转发包，由于软件逻辑问题或伪造mac，会造成大范围的网络中断。
2. 依赖广播学习转发关系，转发关系缺失会造成泛洪
3. 广播域过大，大量无谓的包转发
4. Tor，核心mac表项的规模约束虚拟比
5. Vlan ID只有4096个

公有云overlay虚拟化网络

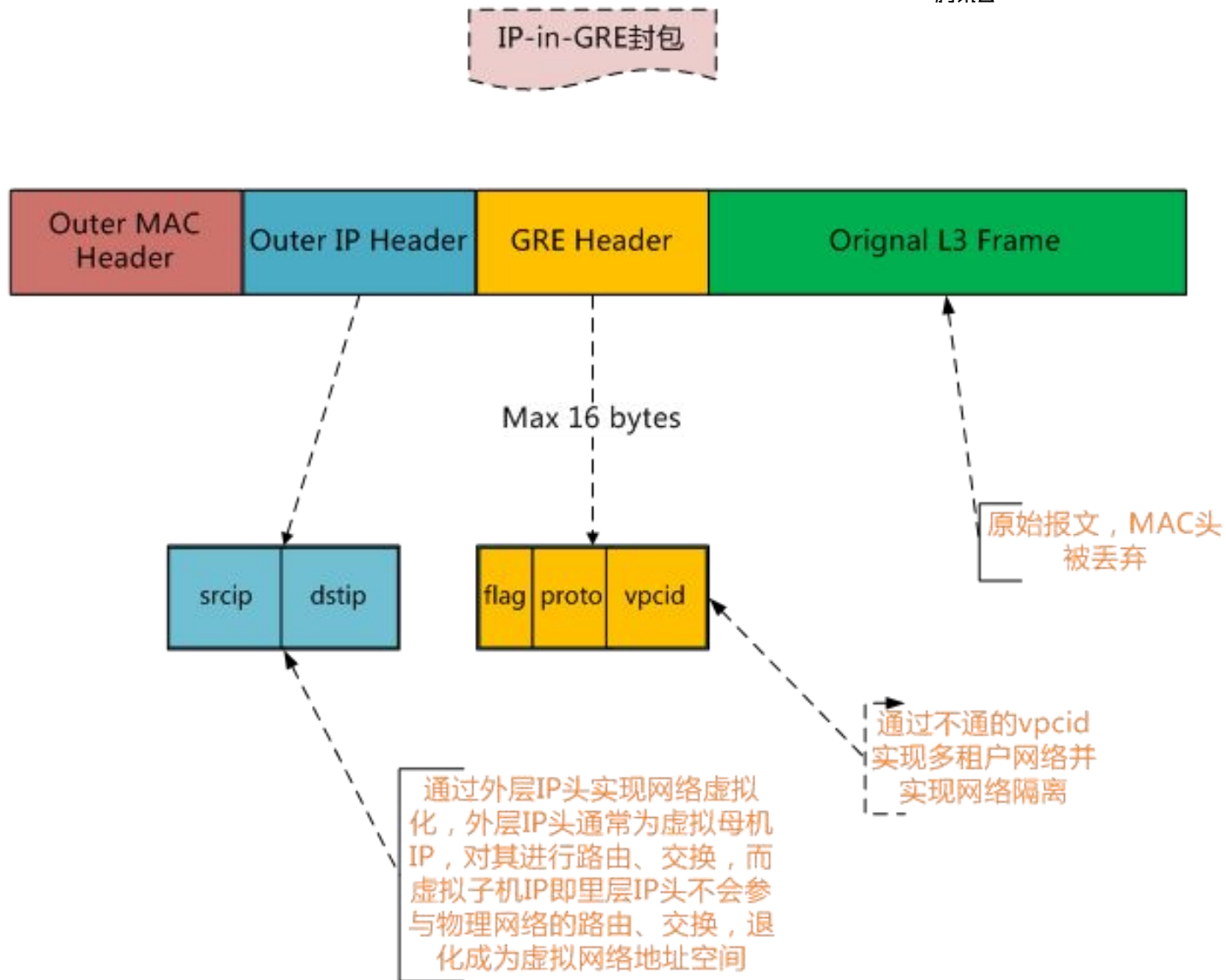


- ✓ 基于Overlay网络实现: 1) 名字空间, 2) 子网路由功能
- ✓ 名字空间: vpcid, 自定义网段, 子网是一个逻辑抽象
- ✓ 子网路由: 核心是如何找下一跳地址?
- ✓ Local路由: VPC内部通信的寻址, 不经过中心式节点
- ✓ 自定义路由: VPC到外部网络的寻址

Overlay技术原理



- 网络虚拟化
- 采用overlay的虚拟化技术实现网络资源弹性伸缩，隧道封装技术为GRE隧道协议
- 多租户
- 通过GRE协议头部附带的vpcid信息实现多租户网络



限于篇幅，不能展开，有兴趣可以单独讨论

- ◆ 子网、路由表、弹性网卡
- ◆ 弹性IP、负载均衡、NAT网关
- ◆ 外网IP直通、组播、广播
- ◆ VPC对等连接、VPN连接、专线连接
- ◆ 安全组、网络ACL
- ◆ 云网络运营监控、云网络流量分析
- ◆



THANK YOU