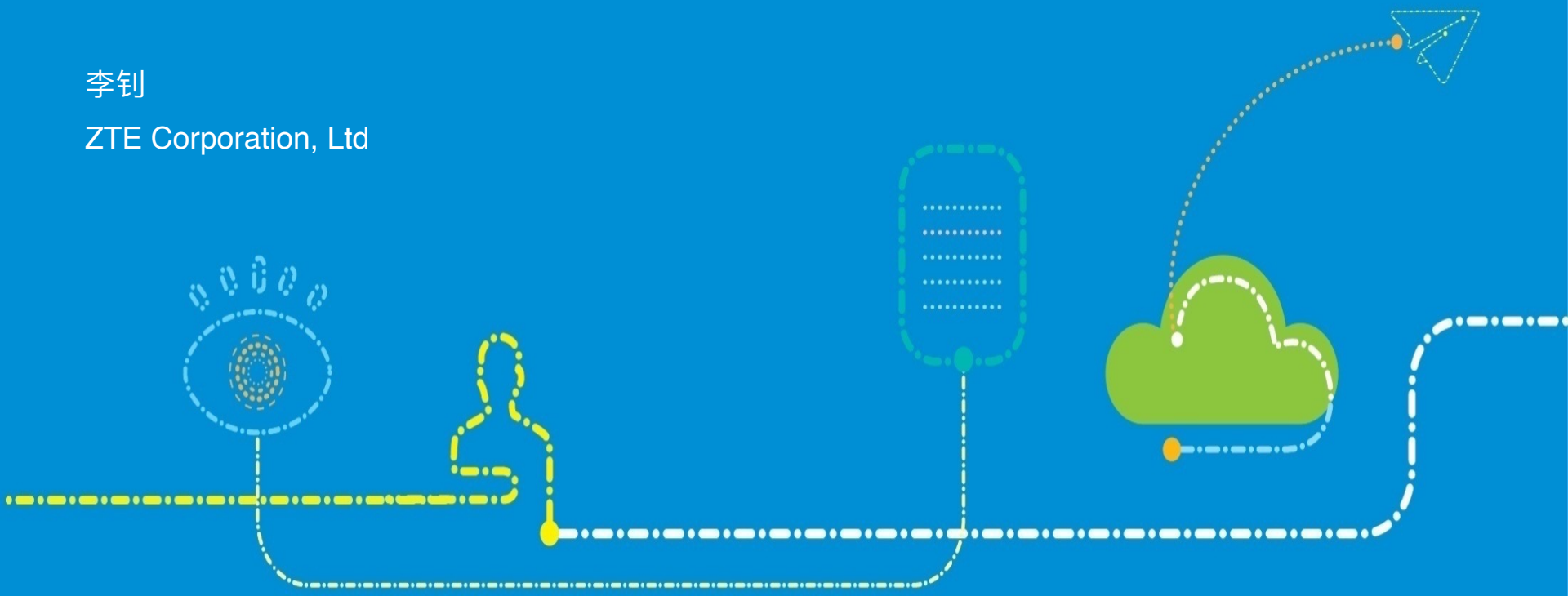
ZTE中兴

未 来，不 等 待

电信级PaaS云平台网络实践

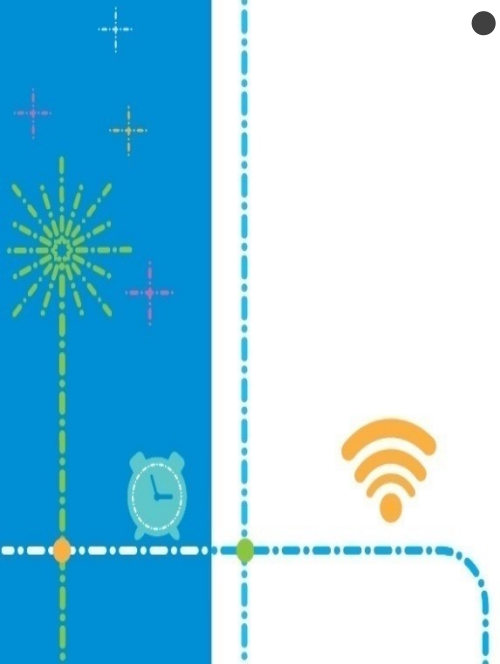
李钊

ZTE Corporation, Ltd



目录

- 背景介绍
- 容器网络现状分析
- 容器网络的挑战
- PaaS网络实践
- Q & A



应用场景

公有云服务

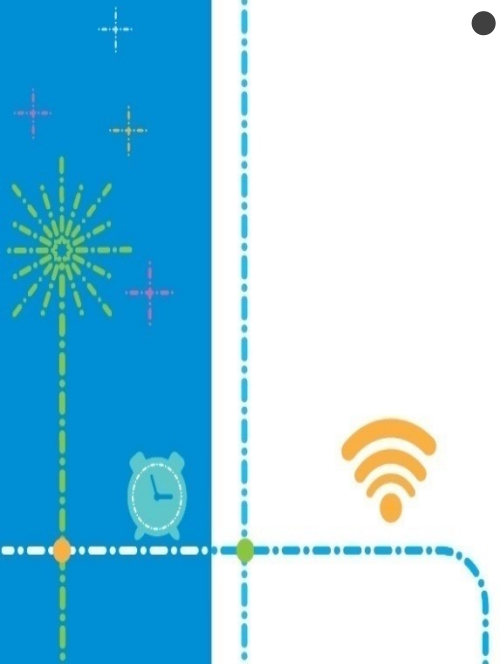
私有云与企业IT云

NFV(网络功能虚拟化)

网络需求

- 高吞吐量，低延时
- 融合异构网络
- 满足灵活的网络配置需求

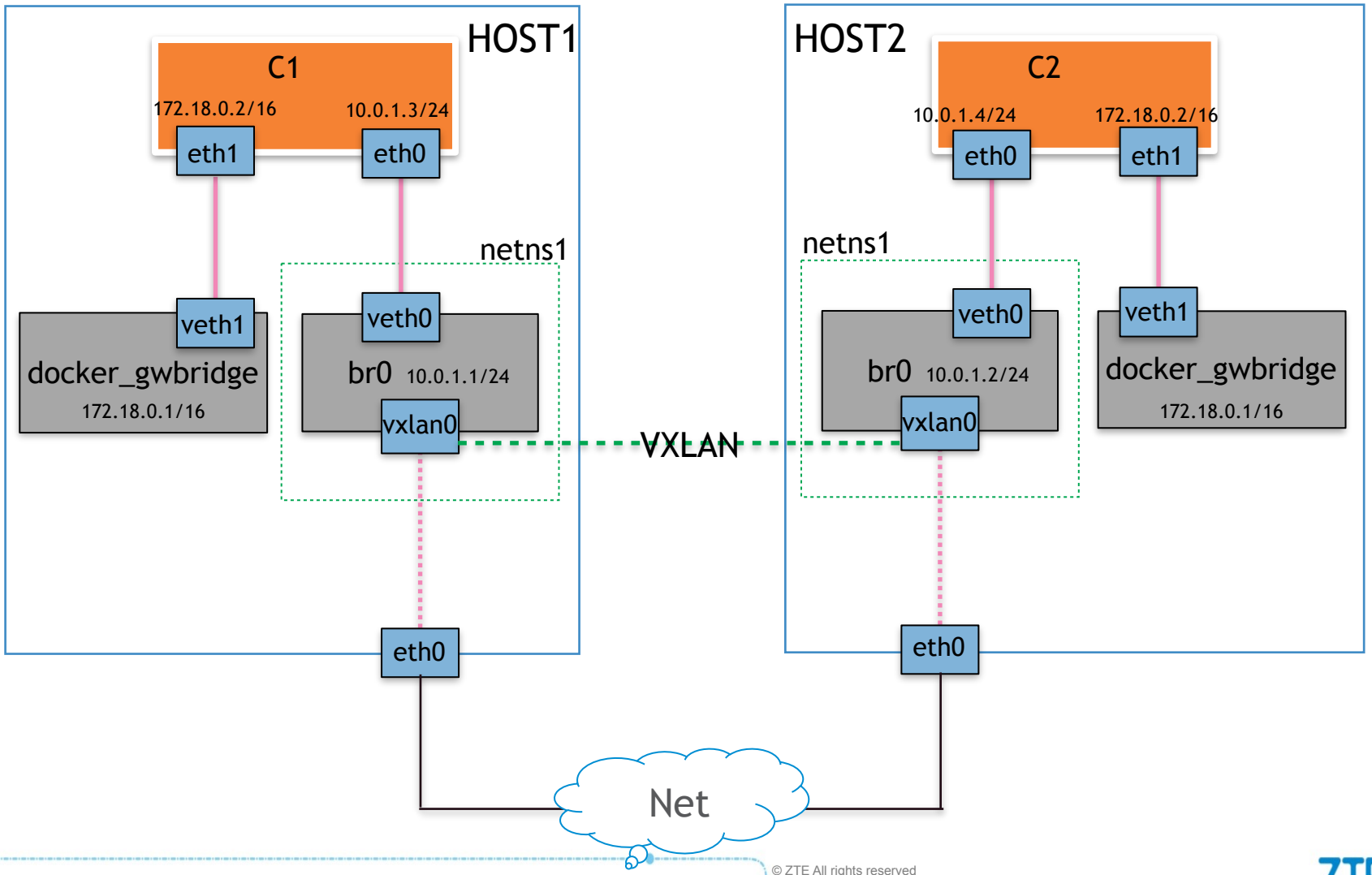
目录



docker原生网络

- Host模式：使用宿主机name space、IP和端口
- Container模式：使用已经存在容器的name space、IP和端口
- None模式：容器拥有自己的name space，需要另外添加网卡、配置IP等
- Bridge模式：默认模式，为容器分配name space、网卡和IP等，并连接到宿主机的虚拟网桥（docker0）

docker原生overlay网络



docker overlay

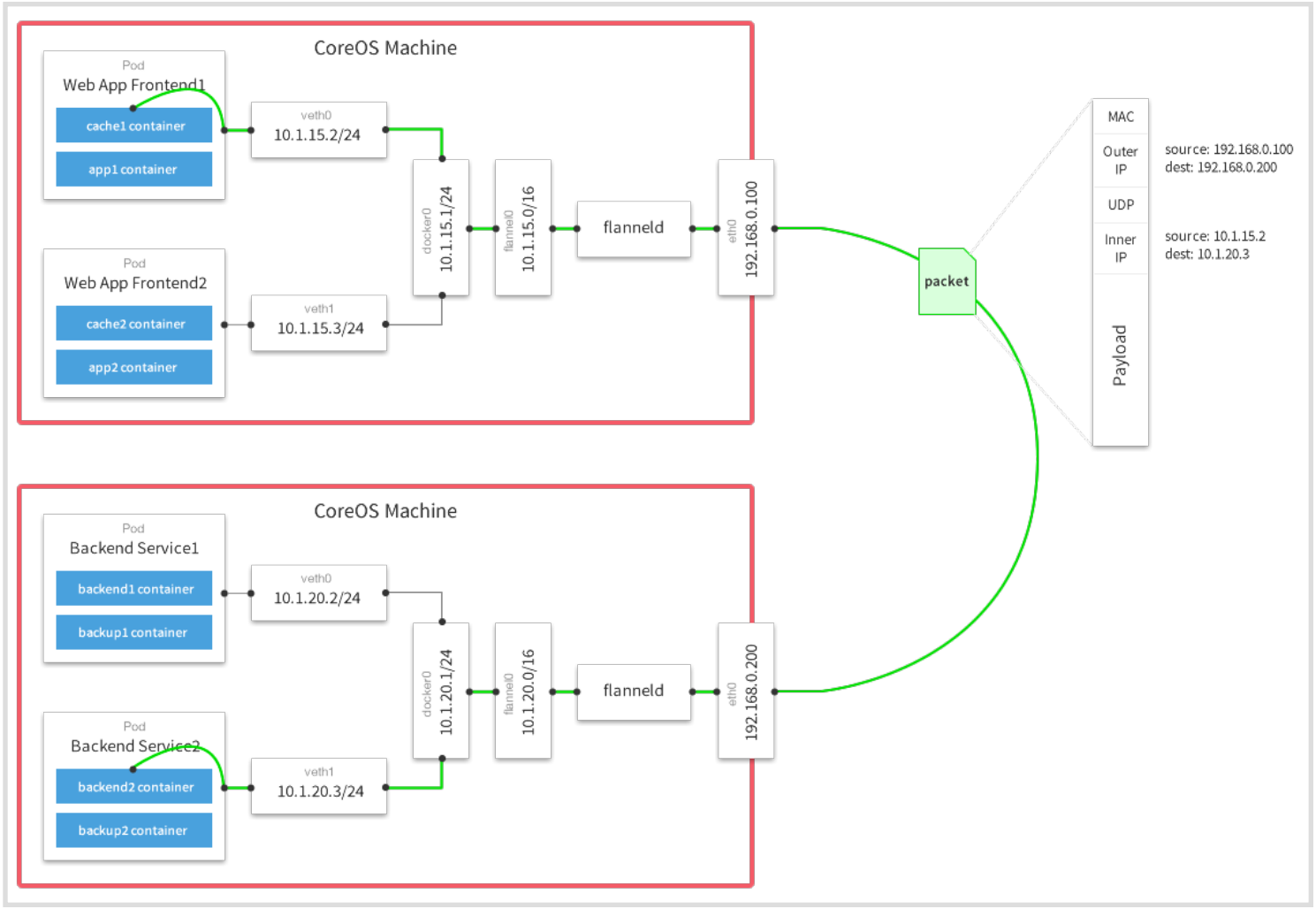
特点：

- L2 Over L3
- 支持多网络平面
- 容器IP与位置无关
- docker天然集成

缺点：

- 与外部网络对接困难
- 还达不到生产级别

flannel – 经典容器overlay网络



flannel

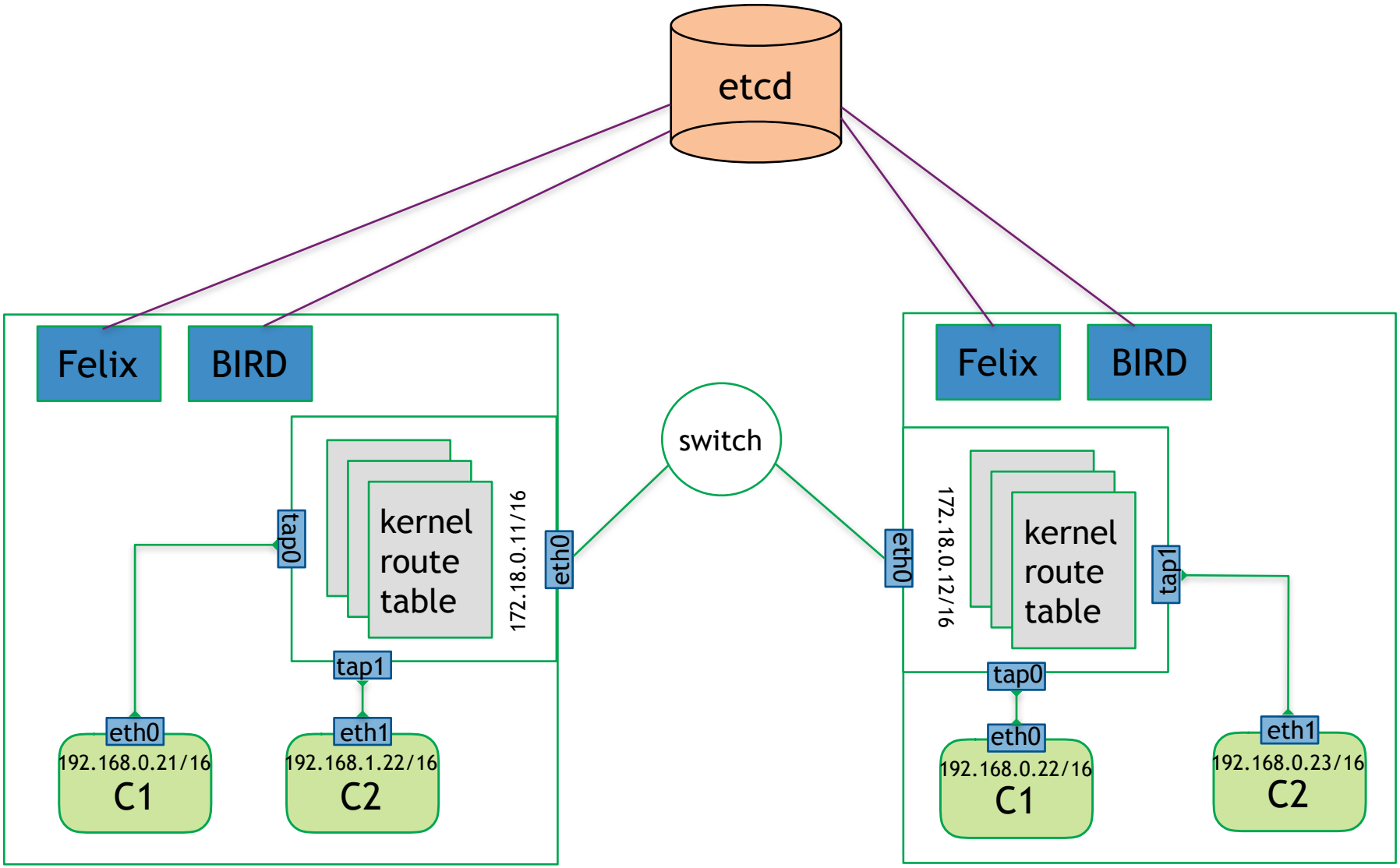
特点：

- L3 Over L3
- 每一个节点有一个独立的子网
- 根据etcd动态生成路由
- 部署、配置简单

缺点：

- 无网络隔离
- 容器无法带IP迁移

Calico – 纯层三解决方案



ZTE中兴

Calico

特点：

- 纯层三转发，性能较好
- 网络隔离好
- 支持容器带IP迁移

缺点：

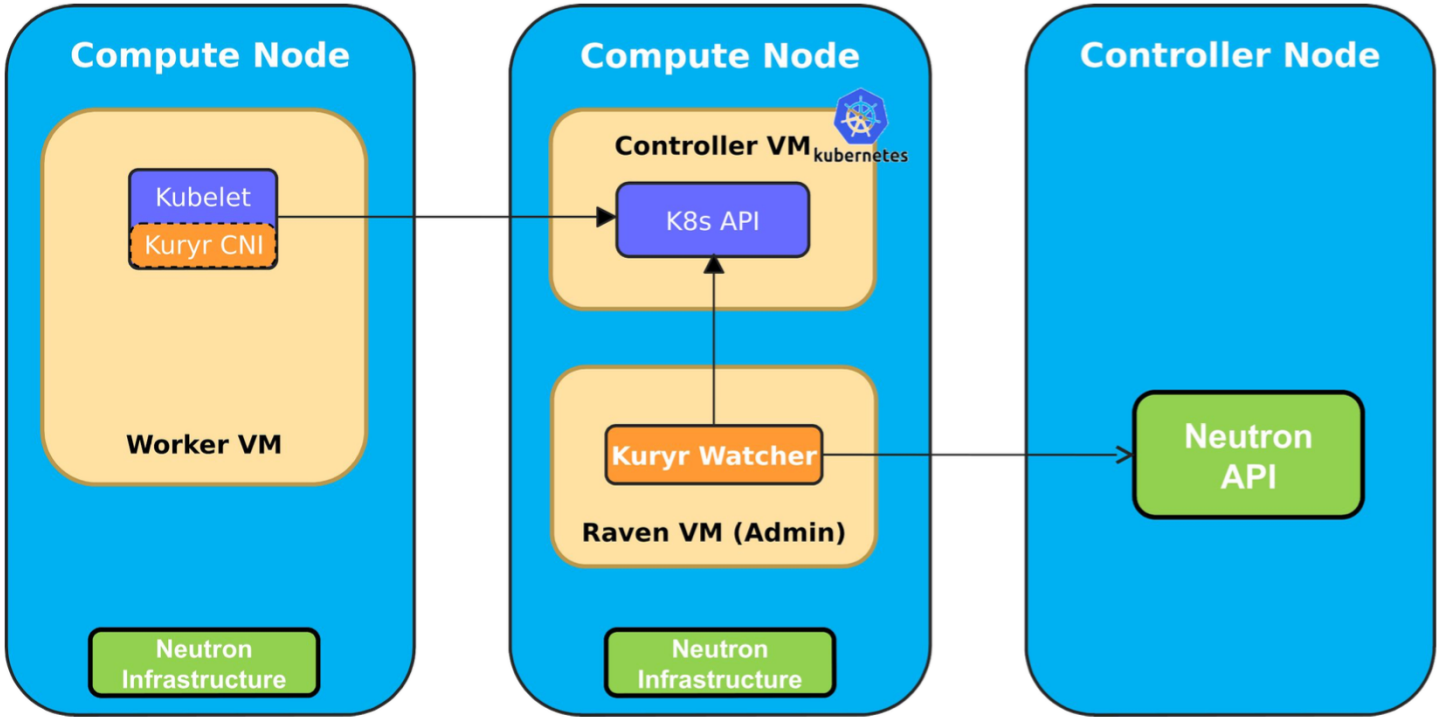
- 需要二层互通
- 网络平面单一

对比

	docker overlay	flannel	calico
性能	较差	较差	较好
支持带ip迁移	是	否	是
网络隔离	是	否	是
基础网络限制	IP可达	IP可达	层二互通
支持多网络平面	是	否	否

Kuryr – 连接Docker与Neutron的桥梁

Kuryr与Kubernetes的集成



Kuryr – 特色

- 统一了容器网络模型
- 支持多种容器编排引擎
  - Kubernetes，Mesos，Docker Swarm
- 可以灵活选择底层实现方案，避免厂商Lock－In
- 天生支持与VM混合组网
- 可以使用Neutorn提供的各种高级网络特性
  - LBaaS，FWaaS
  - 安全组，NAT

Kuryr – 现状

- 所依赖的某些Neutron特性尚未实现
  - Neutron trunk API
- 对kubernetes的支持未实现
  - CNI Plugin
- 生产环境还无法使用

容器网络性能加速 – DPDK

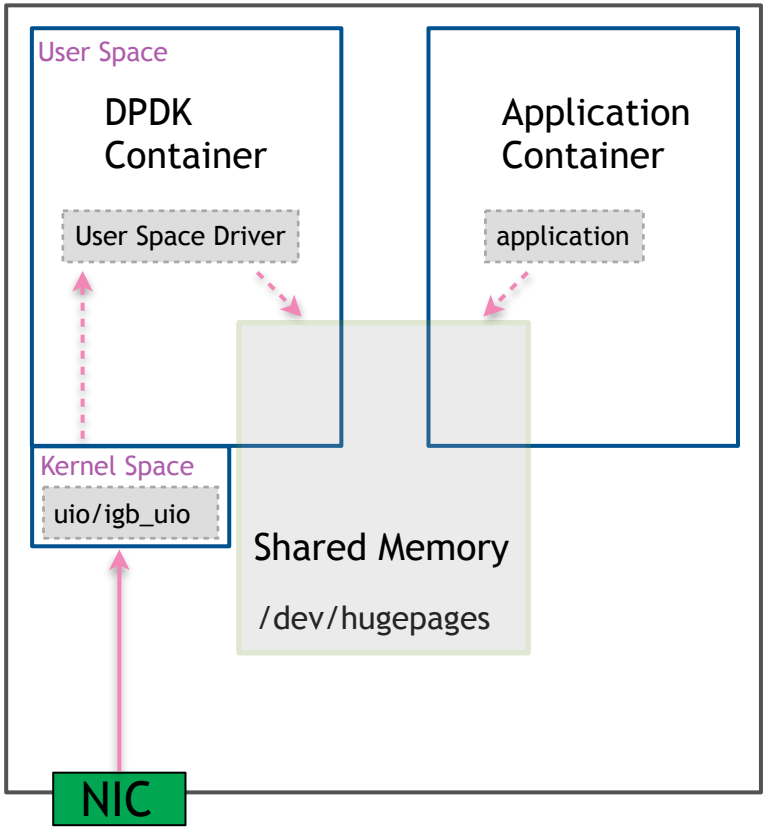
DPDK in Container

前提：

- 暴露主机PCI硬件信息给容器
- 提升容器特权权限

风险：

- 增加了系统的受攻击面，存在潜在的安全风险

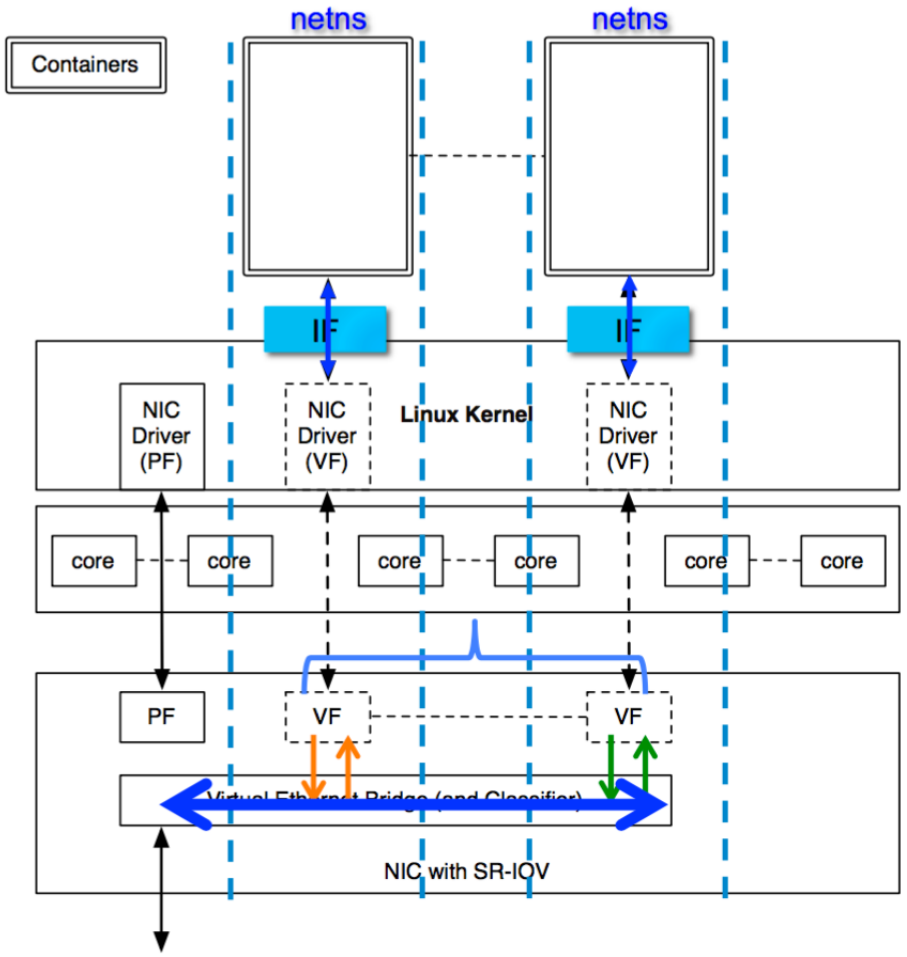


容器网络性能加速 — SR-IOV

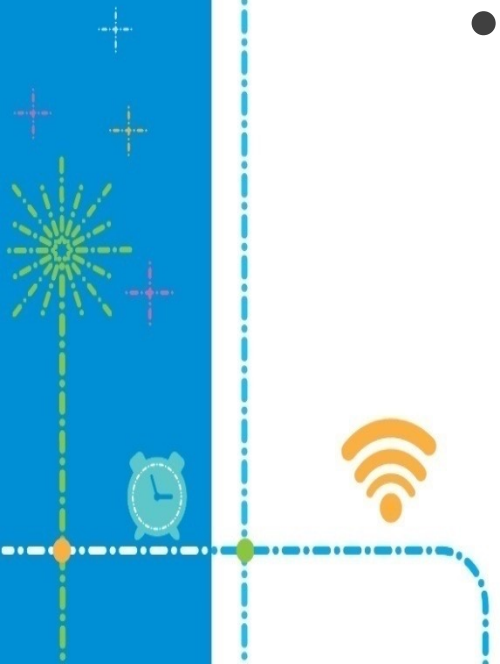
SR-IOV NIC for Container

容器中使用VF口：

a. 将VF添加到容器
b. 设置VLAN tag
c. 设置IP地址
d. 设置路由



目录



容器集群网络CT化的挑战

网络层次过多，性能低

网络平面单一

没有标准框架

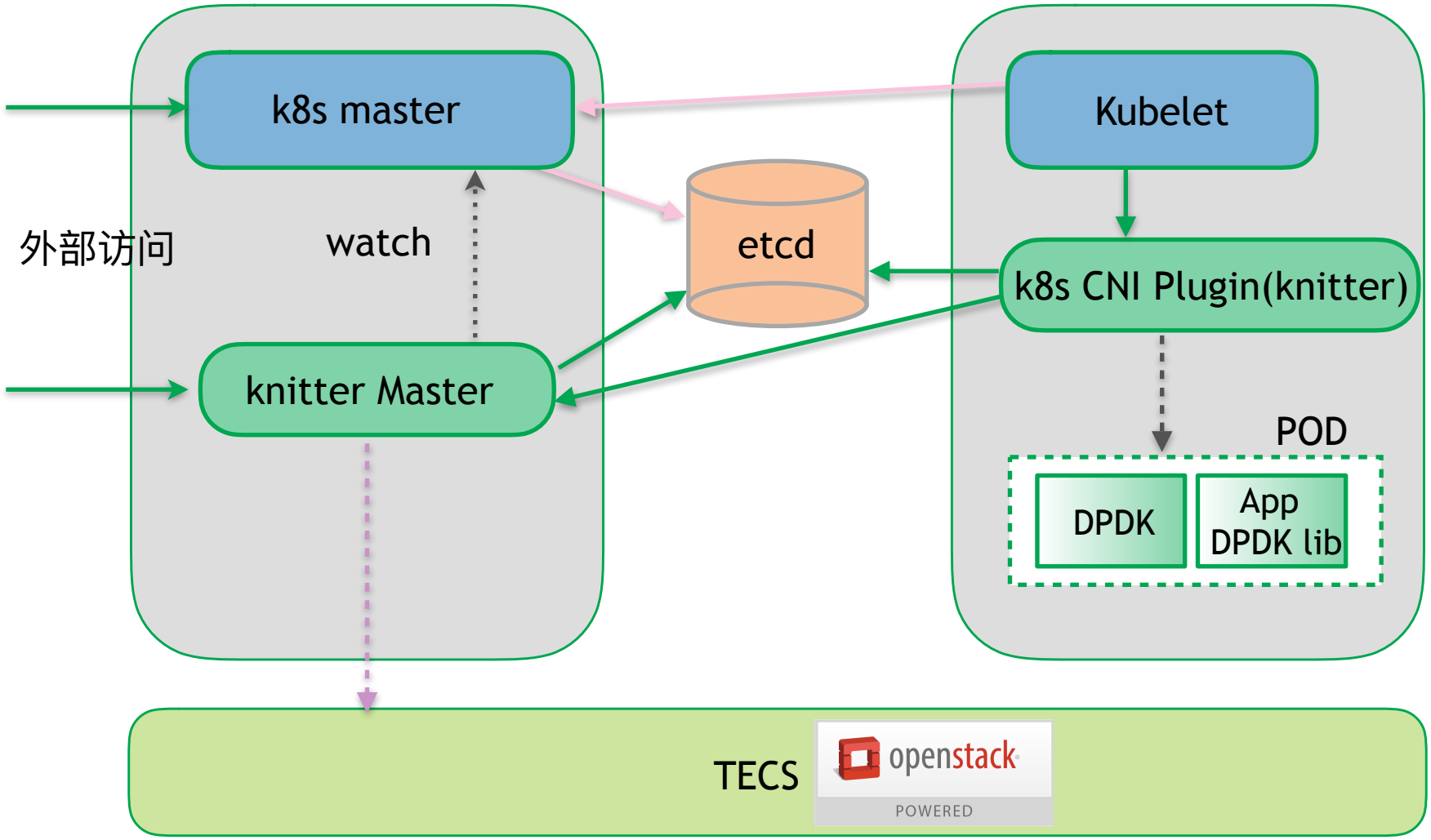
没有完善的DPDK解决方案

网络可定制性不足

目录

- 背景介绍
- 容器网络现状分析
- 容器网络的挑战
- PaaS网络实践
- Q & A

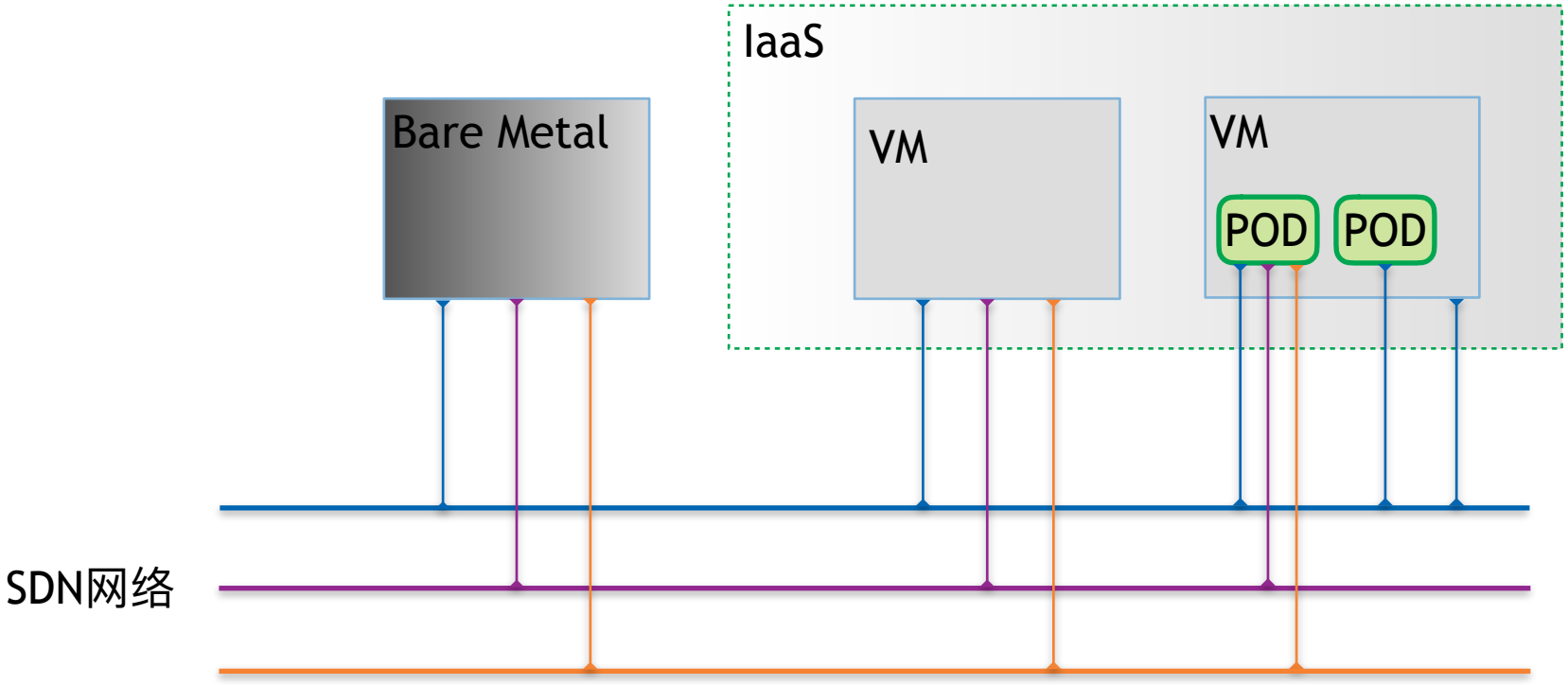
网络组件框架



knitter与kuryr比较

	knitter	kuryr－k8s
多网络平面支持	是	否
网络平面按需配置	是	否
实现语言	golang	python
数据持久化	etcd	etcd
keystone支持	否	是

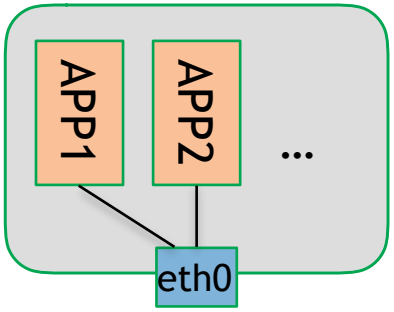
扁平化的网络架构与混合组网



- 融合异构网络，裸机、VM和容器网络互通
- 扁平化的网络架构，容器直达SDN网络

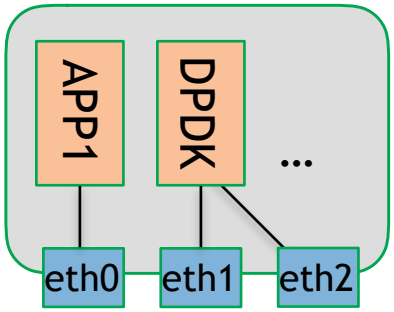
可定制的微服务网络平面

IT Pod




```
{
    "pod_type":"it",
    "network_plane":"std",
    "networks":[
        "std":"net1"
    ]
}
```

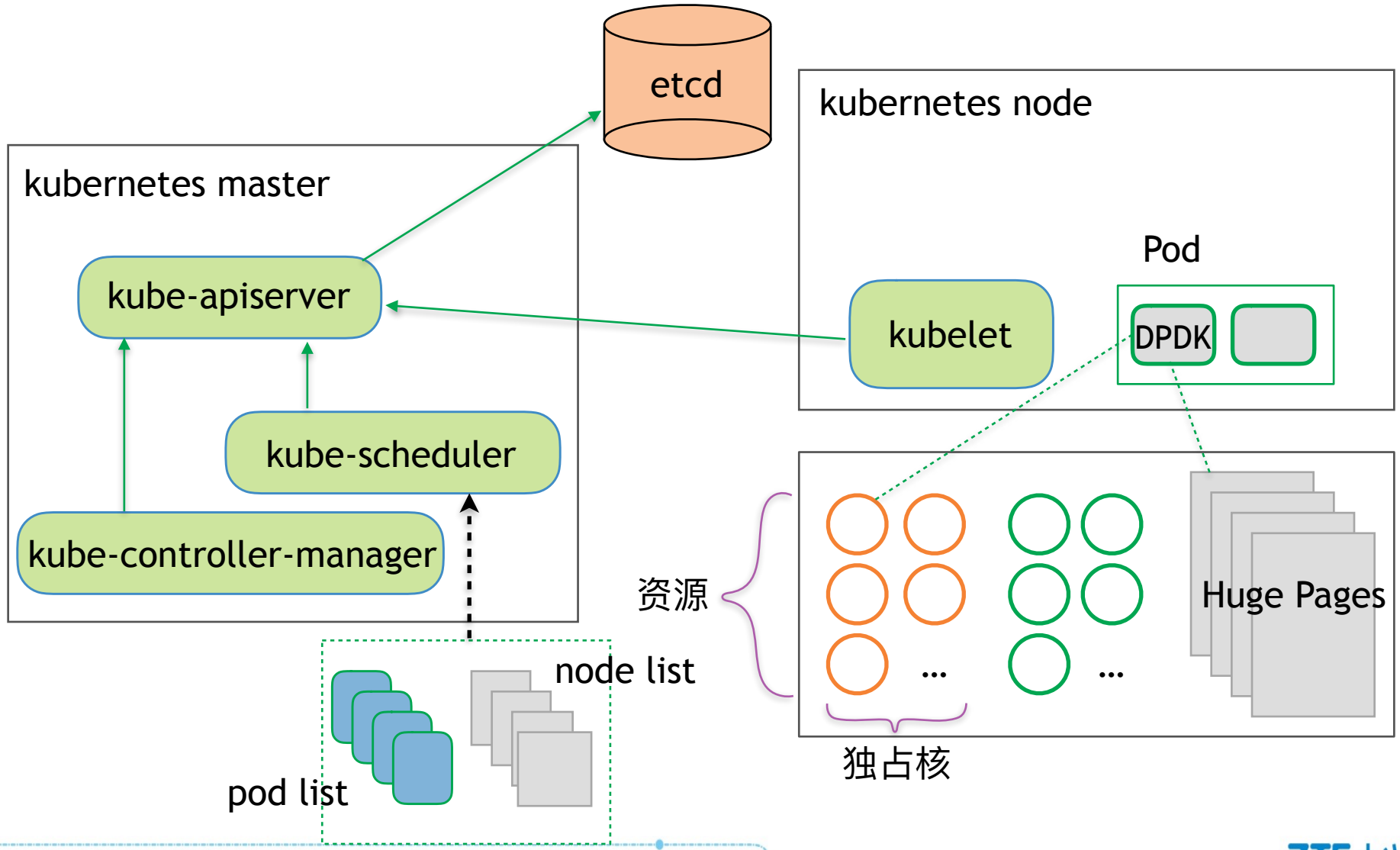
CT Pod




```
{
    "pod_type":"ct",
    "network_plane":"std, control, media",
    "networks":[
        "std":"net1",
        "control":"net2",
        "media":"net3"
    ]
}
```


ZTE中兴

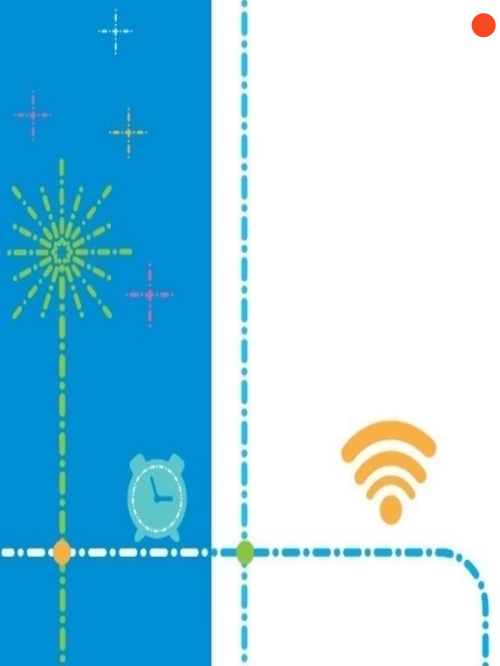
DPDK快通道与kubernetes的集成



ZTE中兴

目录

- 背景介绍
- 容器网络现状分析
- 容器网络的挑战
- PaaS网络实践
- Q & A



Q & A

谢谢！