Tencent 腾讯

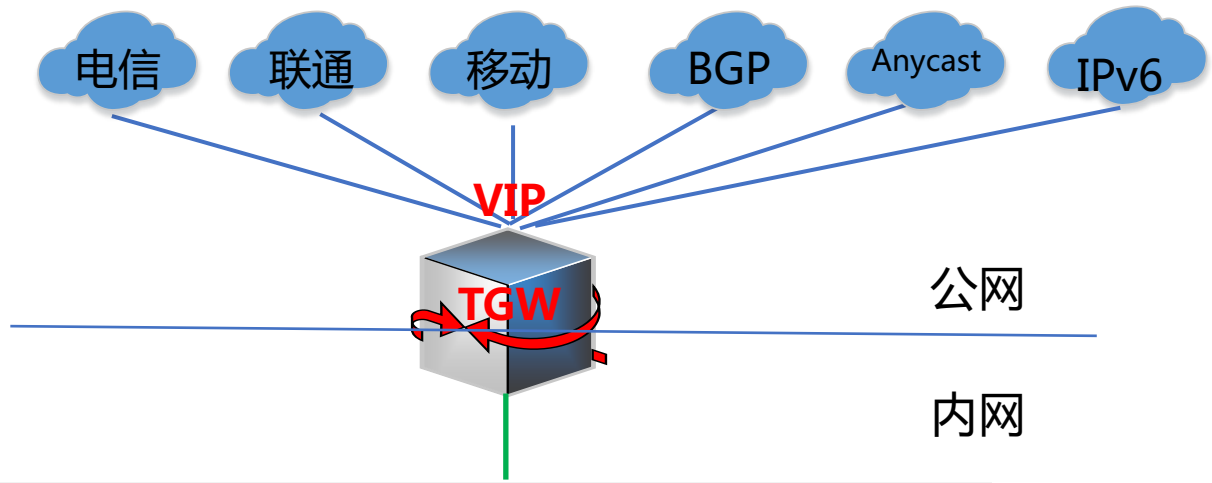
TGW 网关技术交流

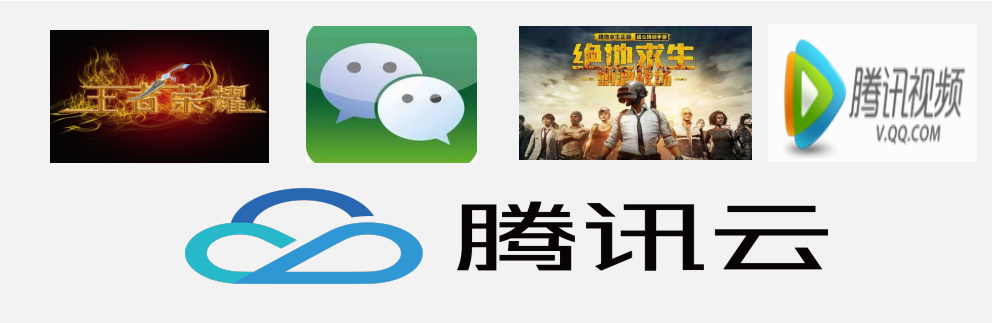
TEG 云架构平台部 系统研发中心

交流大纲

- TGW核心功能、发展历程、技术特点
- 整体架构、基本原理、关键技术
- 高可用相关介绍
- Q&A

TGW （Tencent Gateway）





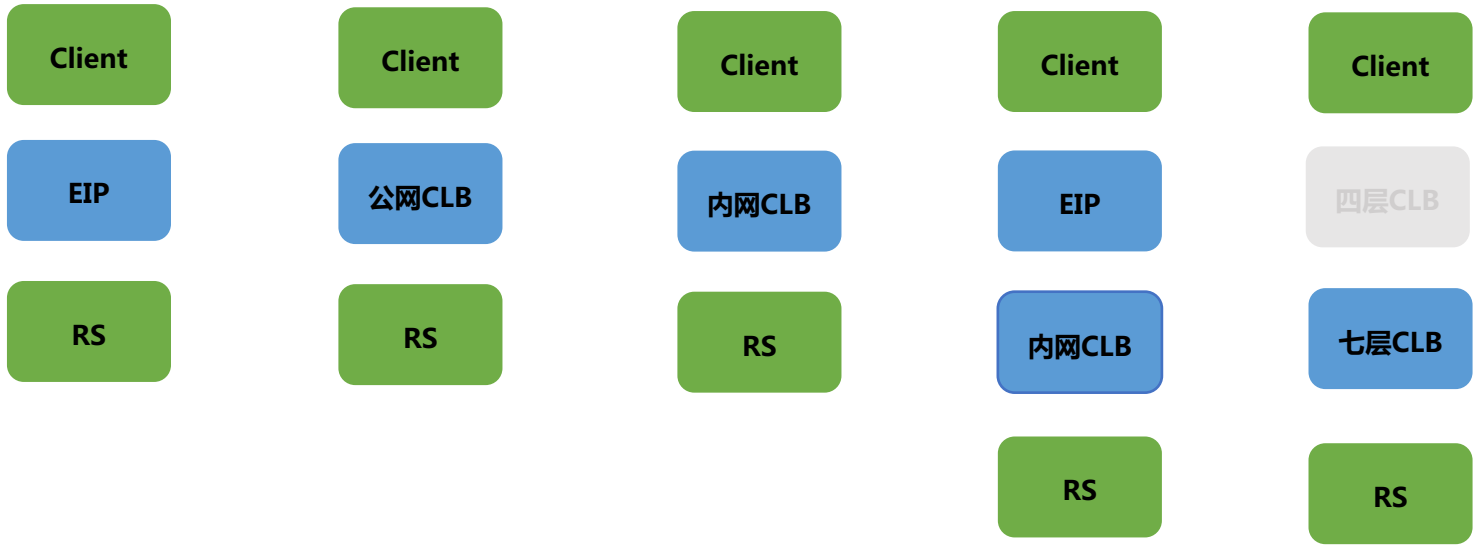
核心功能和特性

- 接入（EIP）
  - 业务公网接入
- 负载均衡（CLB）
  - 业务高可用

TGW发展历程

按照<架构升级->规模使用->架构升级……>的节奏交替式演进

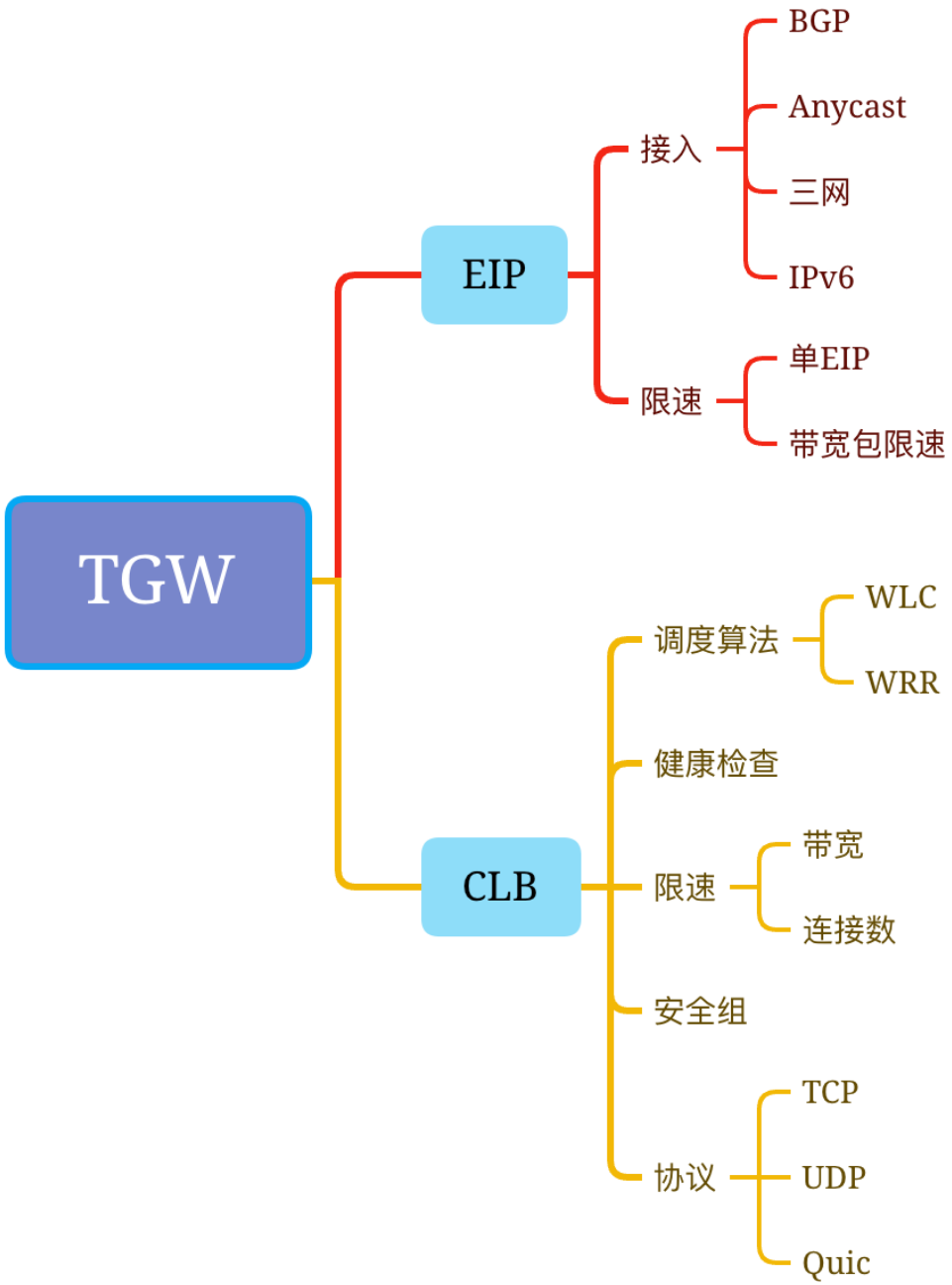
TGW 产品形态



EIP：IPv4、IPv6、BGP、三网、Anycast
外网LB：IPv4、IPv6、BGP、三网
七层CLB：HTTP、HTTPS、QUIC

TGW 基本特性一览

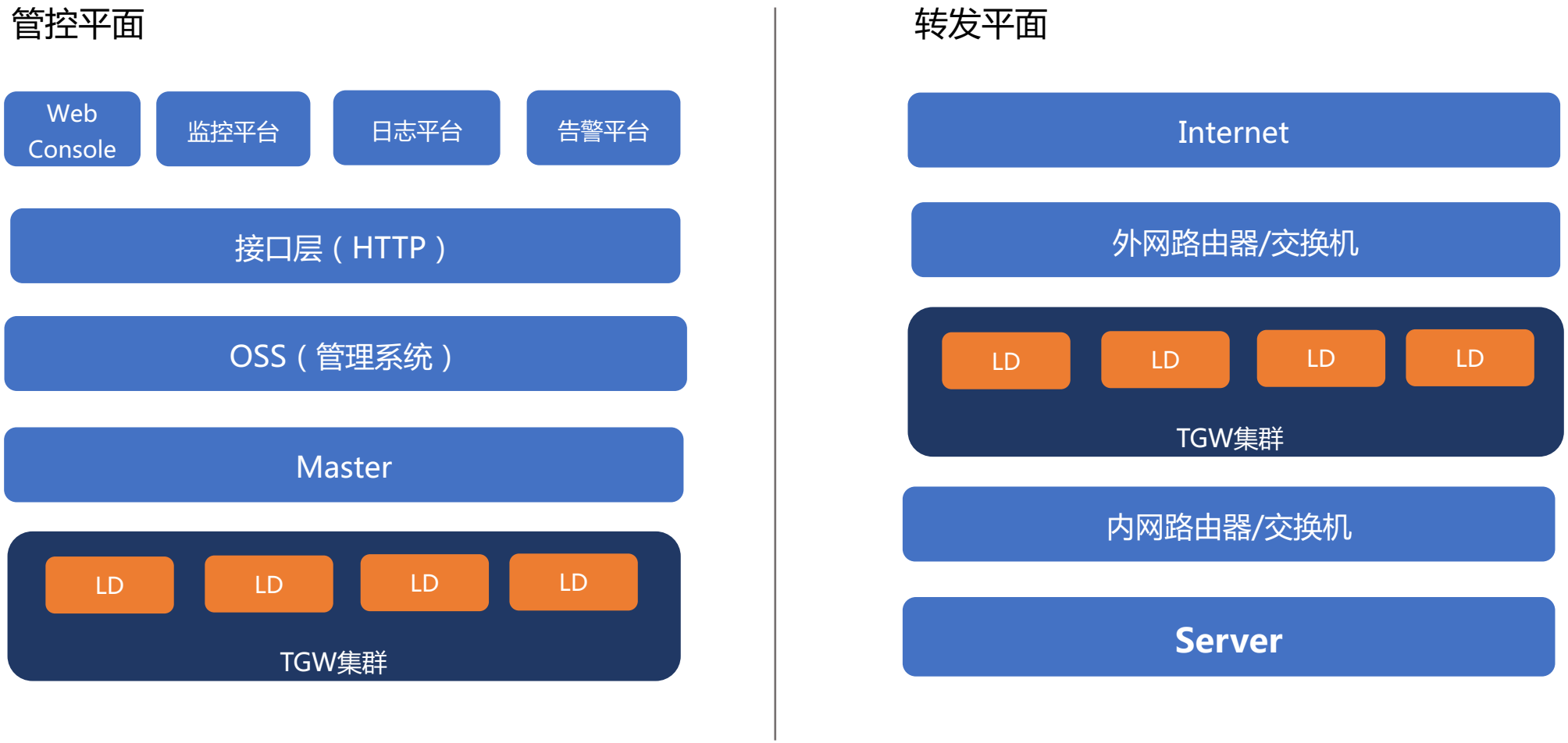
- 整体看功能比较简单
- 通常不和业务处理流程直接（API）交互
- 位置等同于路由器、交换机



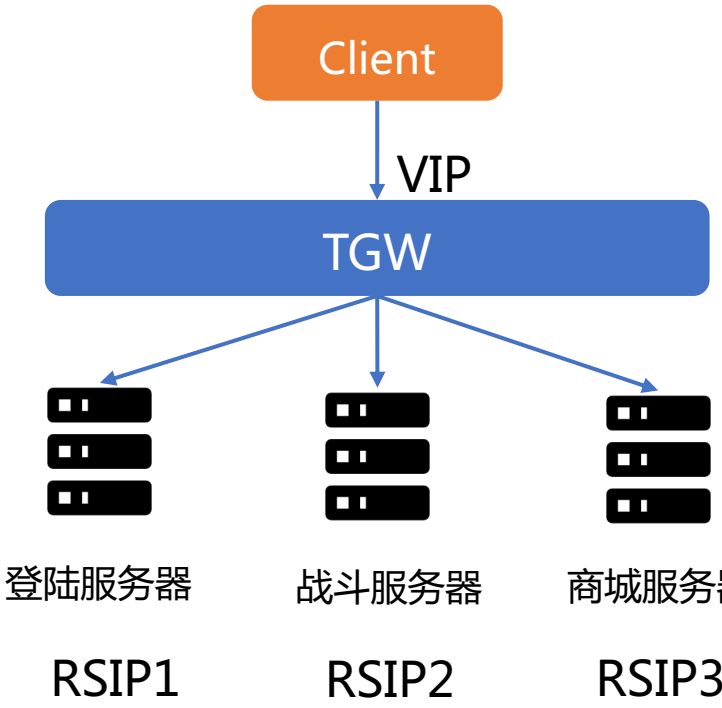
TGW 技术特点

- 业务流量的枢纽位置
- 一个TGW集群承载少则几十G、多则几百G的流量
- 功能需求不多，业务核心的诉求就是：**稳定**

TGW 整体架构

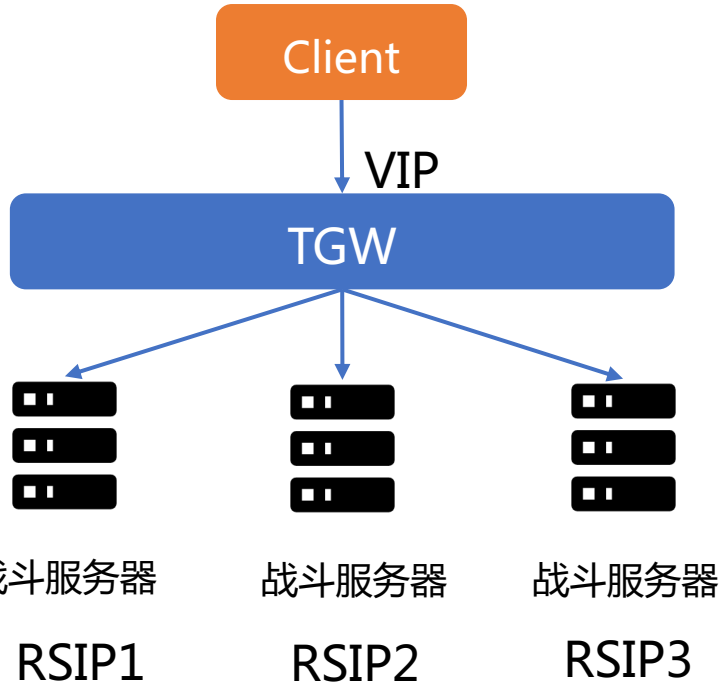

管控平面
Web Console
监控平台
日志平台
告警平台
接口层（HTTP）
OSS（管理系统）
Master
LD
LD
LD
LD
TGW集群
转发平面
Internet
外网路由器/交换机
LD
LD
LD
LD
TGW集群
内网路由器/交换机
Server

TGW 基本原理——转发和调度



VIP1->RSIP1
VIP2->RSIP2
VIP3->RSIP3

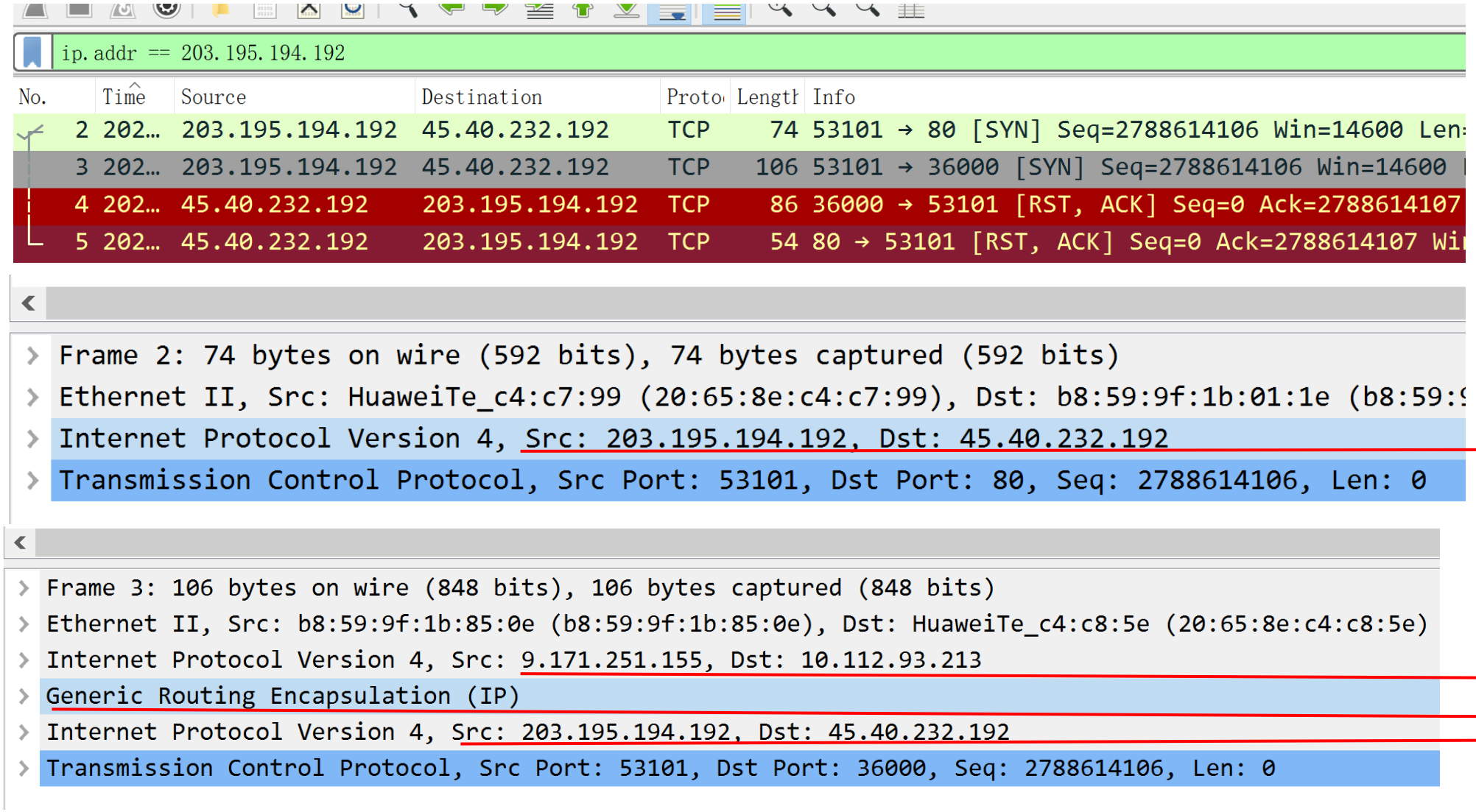
EIP： 1对1、无状态



VIP:VPORT1-> RSIP1:RSPORT2
VIP:VPORT1-> RSIP2:RSPORT2
VIP:VPORT1-> RSIP3:RSPORT3

CLB：1对多、有状态

TGW 基本原理 —— GRE封装



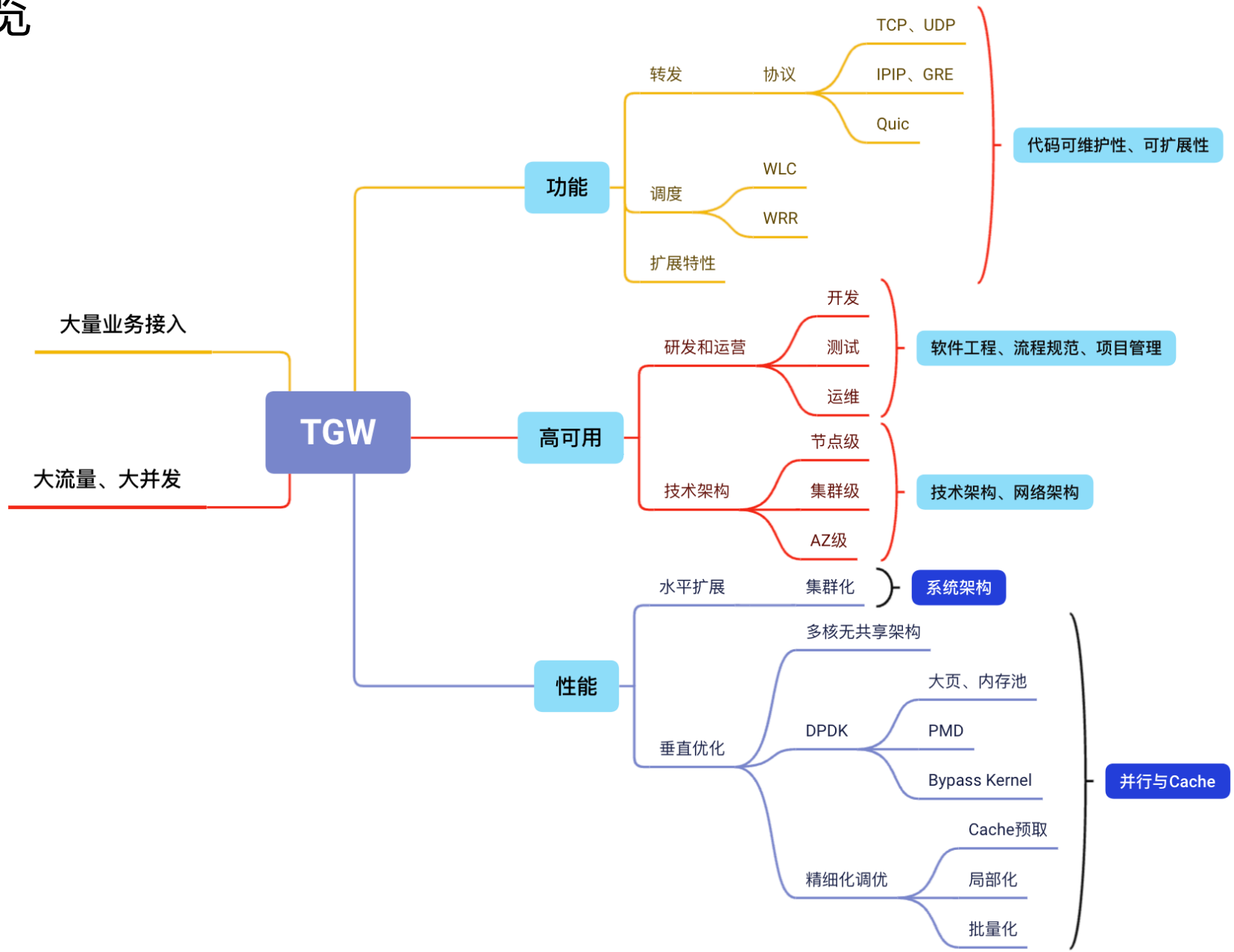
内层原始地址

外层内网地址

GRE头

内层原始地址

TGW 关键技术一览


大量业务接入
大流量、大并发
TGW
功能
转发
协议
TCP、UDP
IPIP、GRE
Quic
调度
WLC
WRR
扩展特性
代码可维护性、可扩展性
高可用
研发和运营
开发
测试
运维
软件工程、流程规范、项目管理
技术架构
节点级
集群级
AZ级
技术架构、网络架构
性能
水平扩展
集群化
系统架构
垂直优化
多核无共享架构
DPDK
大页、内存池
PMD
Bypass Kernel
精细化调优
Cache预取
局部化
批量化
并行与Cache

TGW 高可用——开发、测试

规范的开发流程

- **强化TR（Technical Review）**
  - **需求、设计、用例、编码**
- **控制版本节奏（快慢结合）**
  - **特性固定周期（慢）、Bugfix按需随时（快）**

独立的测试团队

- **专业测试团队，按照2B交付标准测试**
- **测试专区**
- **自动化测试、性能测试、长稳测试**

对一个存量规模巨大的基础软件项目，不适合采用敏捷迭代的方式开发新特性。

TGW 高可用——运维

发布

- **预发布**
- **阶梯式发布**
- **快速回滚**

监控与发现

- **全集群拨测、全节点拨测**
  - **成功率、时延**
- **异常指标、日志监控**
- **运营水位监控**
- **流量变化监控**
- **核心配置监控**
- **……**

恢复

- **自动隔离**
- **快速扩容**
  - **预建buffer池**
- **快速迁移**

TGW 高可用——技术架构: 节点级

多核无共享

- **无全局结构**
- **单线程环境开发业务逻辑**
- **有意回避软件稳定性天敌：并发竞争**
- **无状态转发（REIP）**

多进程

- **辅助进程独立进程缩小故障域**
  - Trace、抓包、日志、统计等

高性能

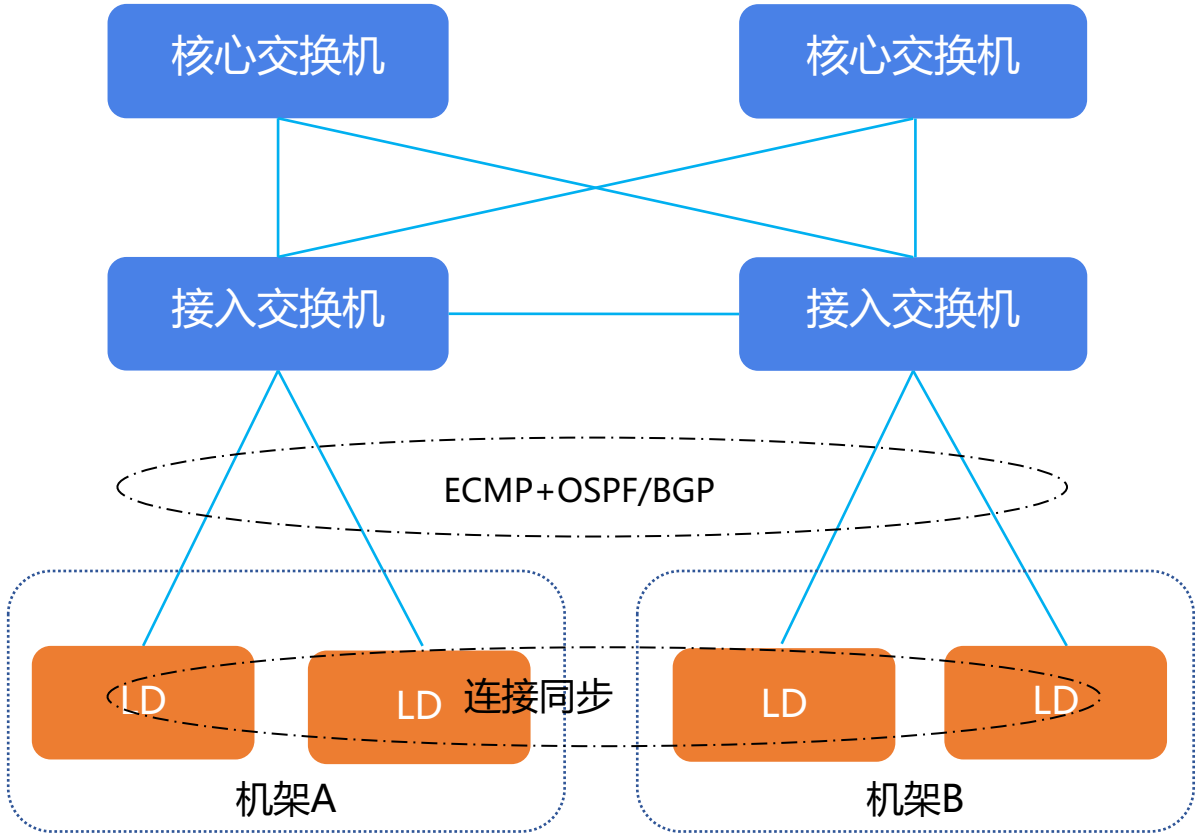
- **5亿连接池（CLB）**
- **100G转发能力**

监控

- **实时监控核心进程状态**
- **自动隔离**

TGW 高可用——技术架构：集群级

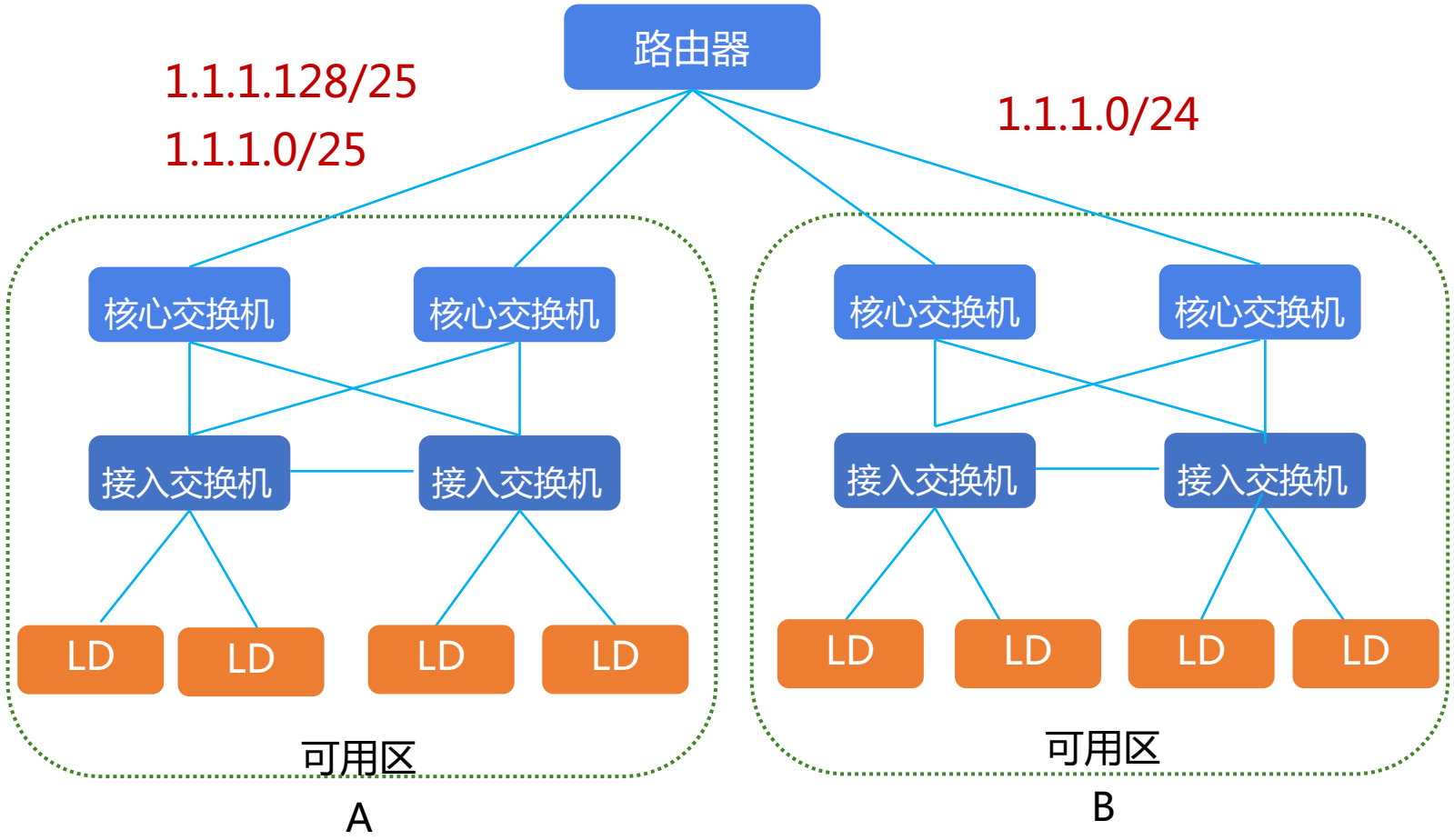
- **ECMP**
  - **2-16个节点**
- **OSPF/BGP**
  - **秒级收敛**
- **连接同步**
  - **节点下线、扩容、升级，业务基本无感知**
- **链路冗余**
  - **两组交换机**
  - **两组LD（4+4/2+2）**
  - **独立机架**



TGW 高可用——技术架构：AZ级

- **优先级路由**

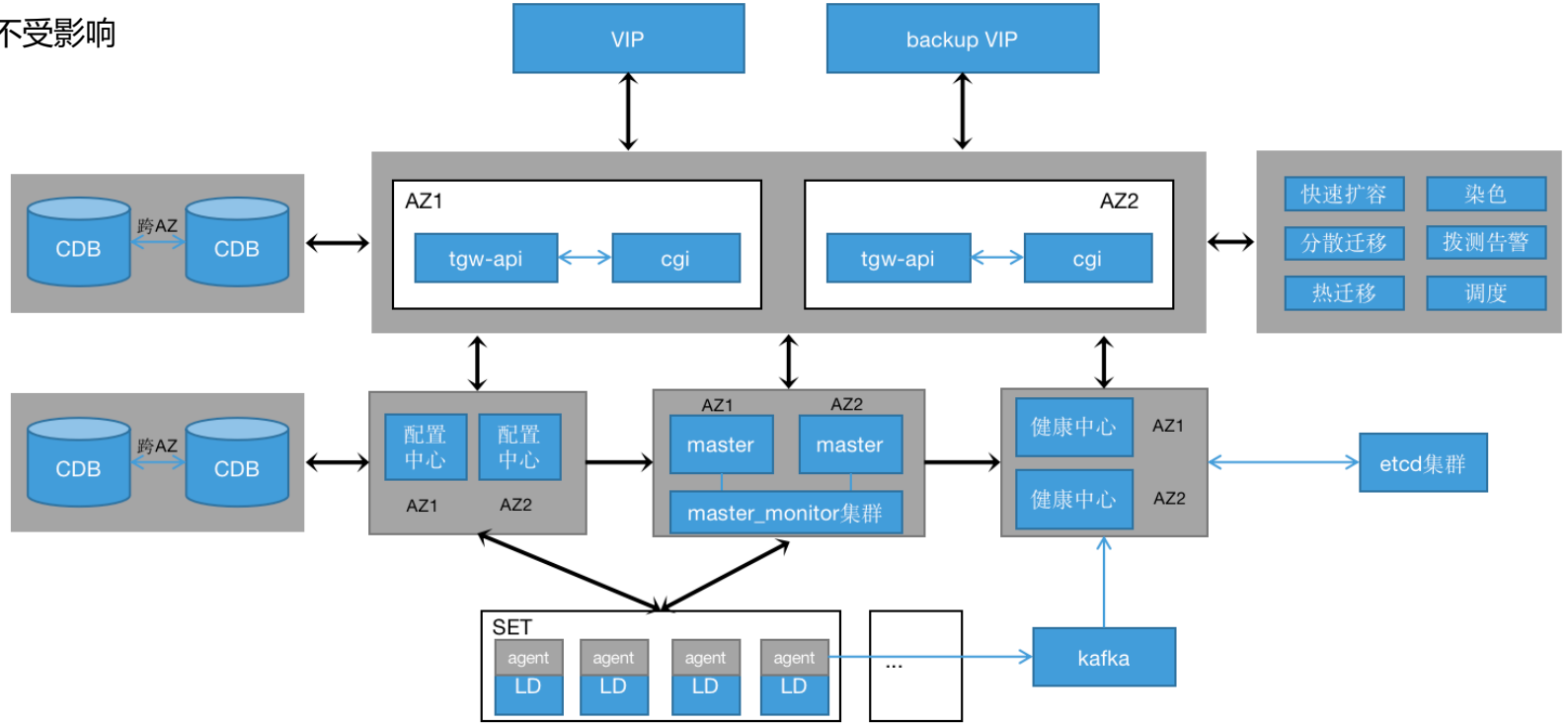
- **跨AZ连接同步**
  - **切走、切回业务基本无感知**



TGW 高可用——技术架构：系统级与控制面容灾

- 划分故障域
  - 转发 – 控制 – 辅助 三个故障级
  - 控制面异常，转发不受影响
  - 监控、上报、拨测等辅助组件异常配置变更不受影响

- 控制面按照地域级部署
  - AZ级故障，控制面功能不受影响。

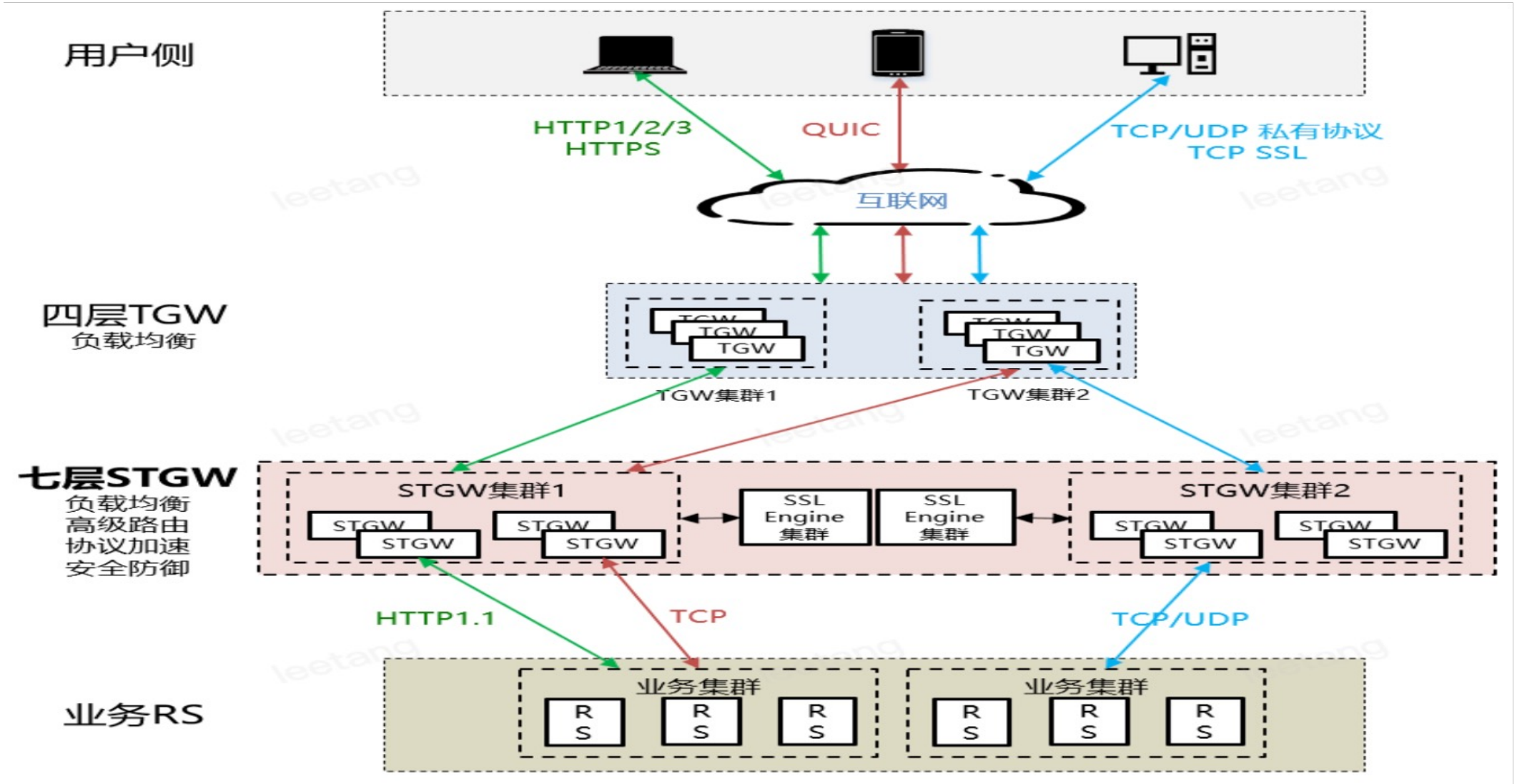


STGW（七层CLB）

业务架构体系

STGW全称Secure Tencent Gateway（腾讯安全网关），是一个应用层流量接入平台。

STGW的主要目标是稳定、高效、安全地接入公司各大业务的流量。核心功能包括负载均衡、HTTPS/TCP/QUIC协议加速以及WAF，CC等安全防护功能



STGW（七层CLB）高可用

- 基于L4+L7双层架构
  - 节点异常，L4自动剔除
  - L4上配置限速，抵抗流量突发和攻击
- 跨AZ部署
  - AZ故障，跟随L4一起切换