GIAC
全球互联网架构大会
GLOBAL INTERNET ARCHITECTURE CONFERENCE

API网关在微服务体系中的应用

高磊 阿里云 高级技术专家

msup

TOP100Summit
全球软件案例研究峰会
时间：11月15~17日
地点：北京国际会议中心
100个年度最值得学习案例

MPD工作坊（深圳站）
时间：9月21~22日
地点：深圳博林圣海伦酒店
20个3小时大时段沙盘课程

MPD工作坊（北京站）
时间：7月06~07日
地点：北京国家会议中心
20个3小时大时段沙盘课程

MPD工作坊（上海站）
时间：10月26~27日
地点：上海
20个3小时大时段沙盘课程

讲师简介

高磊 阿里云API网关团队 花名 埃兰

高级技术专家

一个写了25年代码的老程序员，曾任中国移动飞信服务器端主架构师，2017年加入阿里云，熟悉应用架构、中间件、PaaS等领域

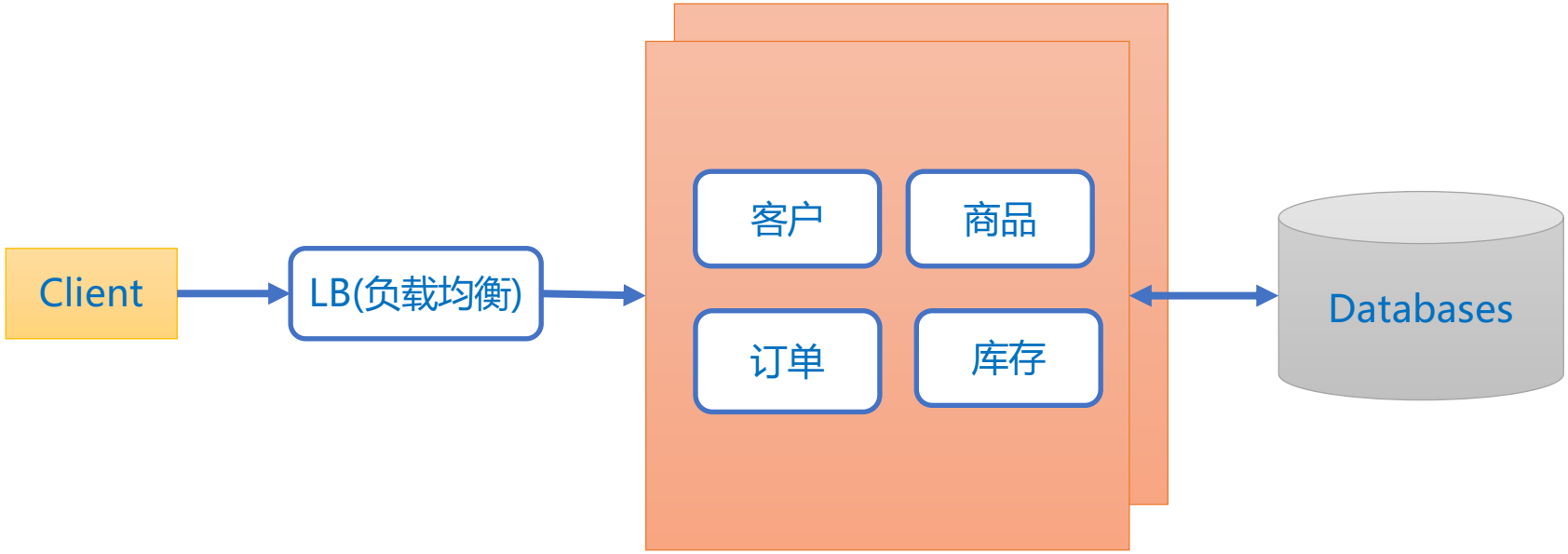
演讲大纲

1 **API网关角色的引入**

2 API网关为微服务开发带来的好处

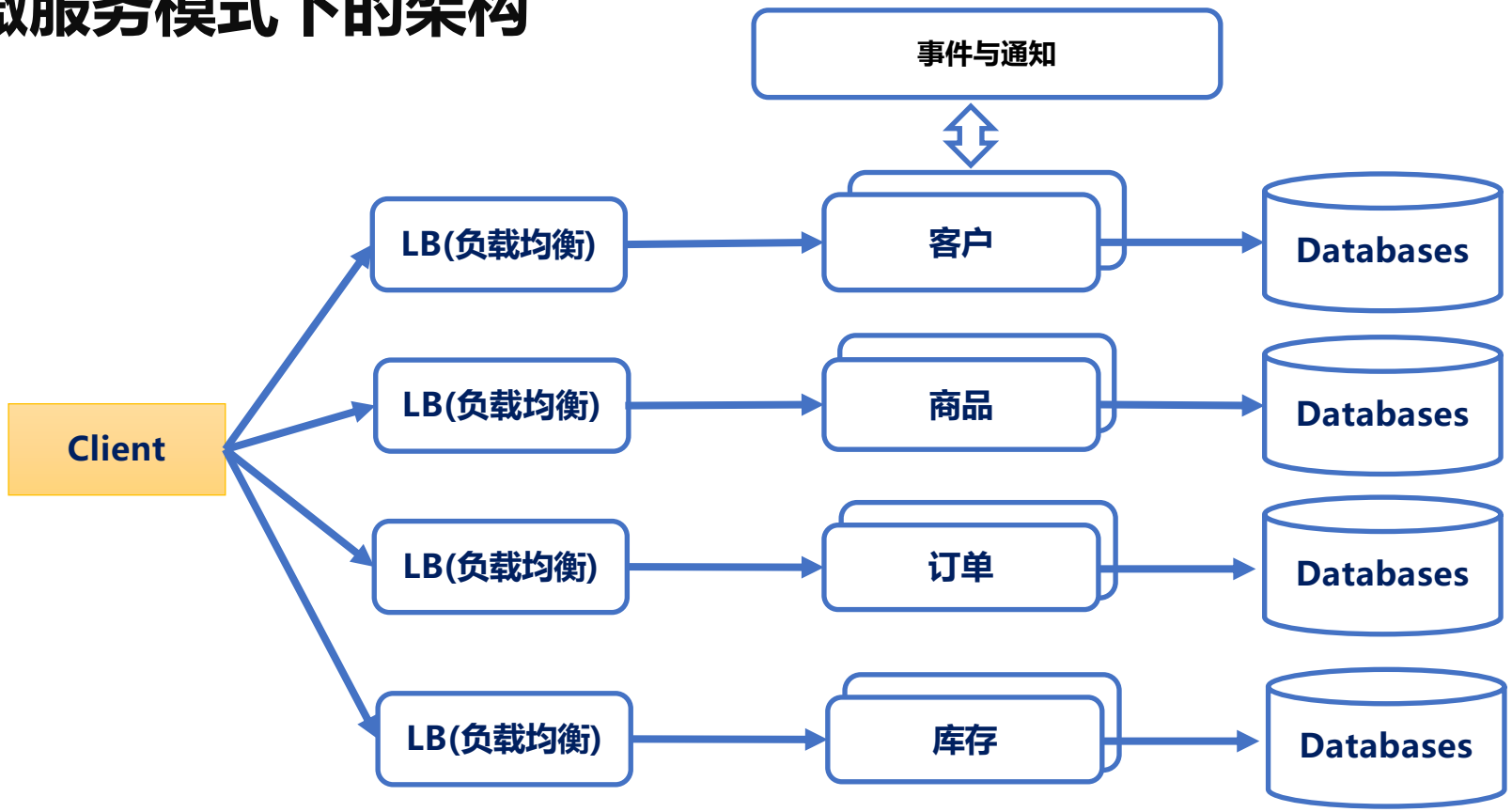
3 API经济

从一体化架构(Monolithic)说起

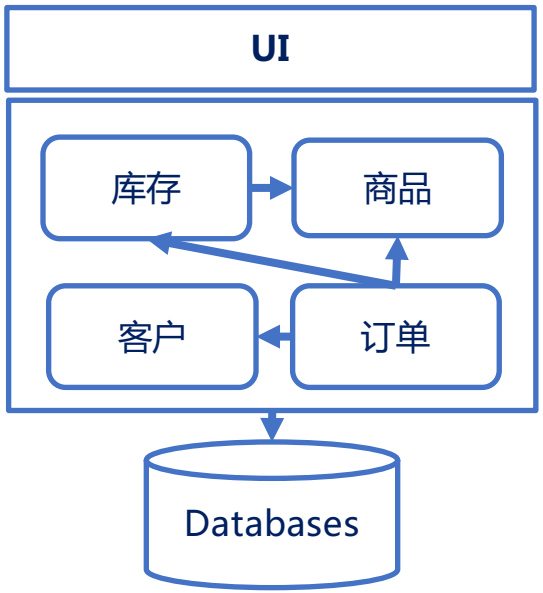


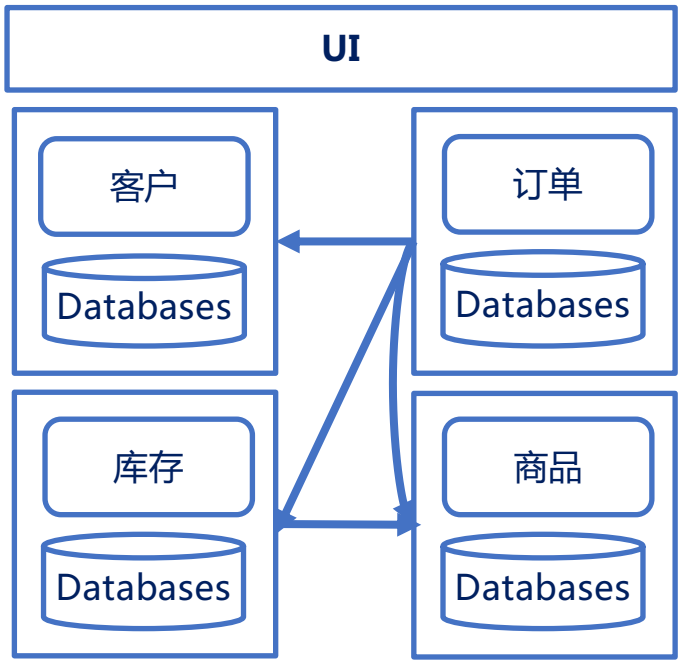
从一体化架构到微服务

微服务模式下的架构


事件与通知
Client
LB(负载均衡)
LB(负载均衡)
LB(负载均衡)
LB(负载均衡)
客户
商品
订单
库存
Databases
Databases
Databases
Databases

Monolith vs Microservices





解决的问题

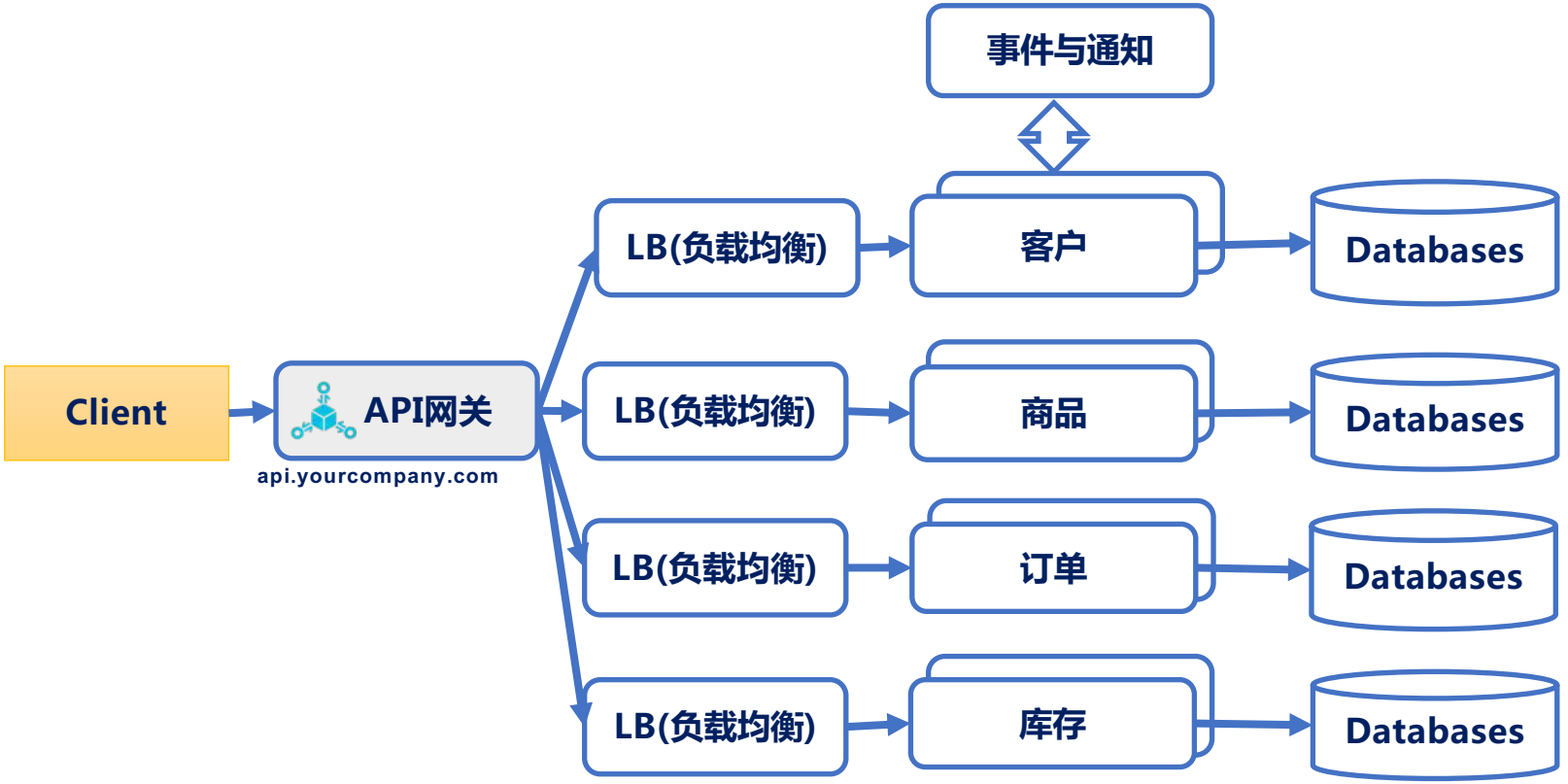
- ☺️ 更适合构建大规模应用了
- ☺️ 微服务的开发更简单，团队变得更加敏捷
- ☺️ 提高了隔离性、杜绝了单点故障的影响

新的问题

- 😭 需要关注更多的组件
- 😭 系统架构更加复杂
- 😭 接口的依赖和管理变得复杂
- 😭 测试变得困难了

为什么需要API网关？

微服务+API网关架构模式



API网关解决的问题

- ✓ 实现API元数据的管理
- ✓ 统一API接入点
- ✓ 权限与访问控制
- ✓ 简化后端开发
- ✓ 提升系统的可运维能力

API网关的选择

开源产品

公共云产品

商业产品

1

API网关角色的引入

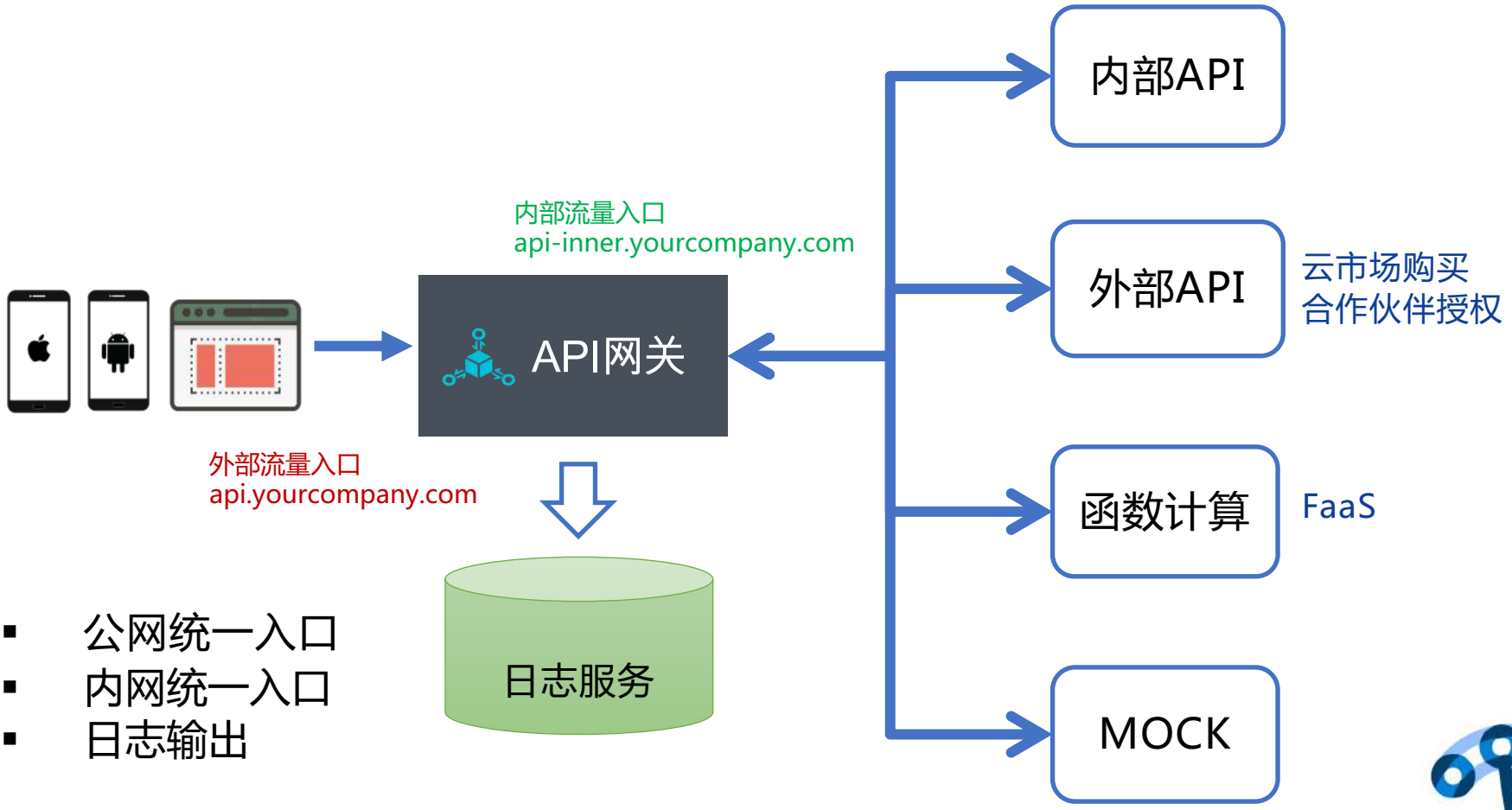
2

API网关为微服务开发带来的好处

3

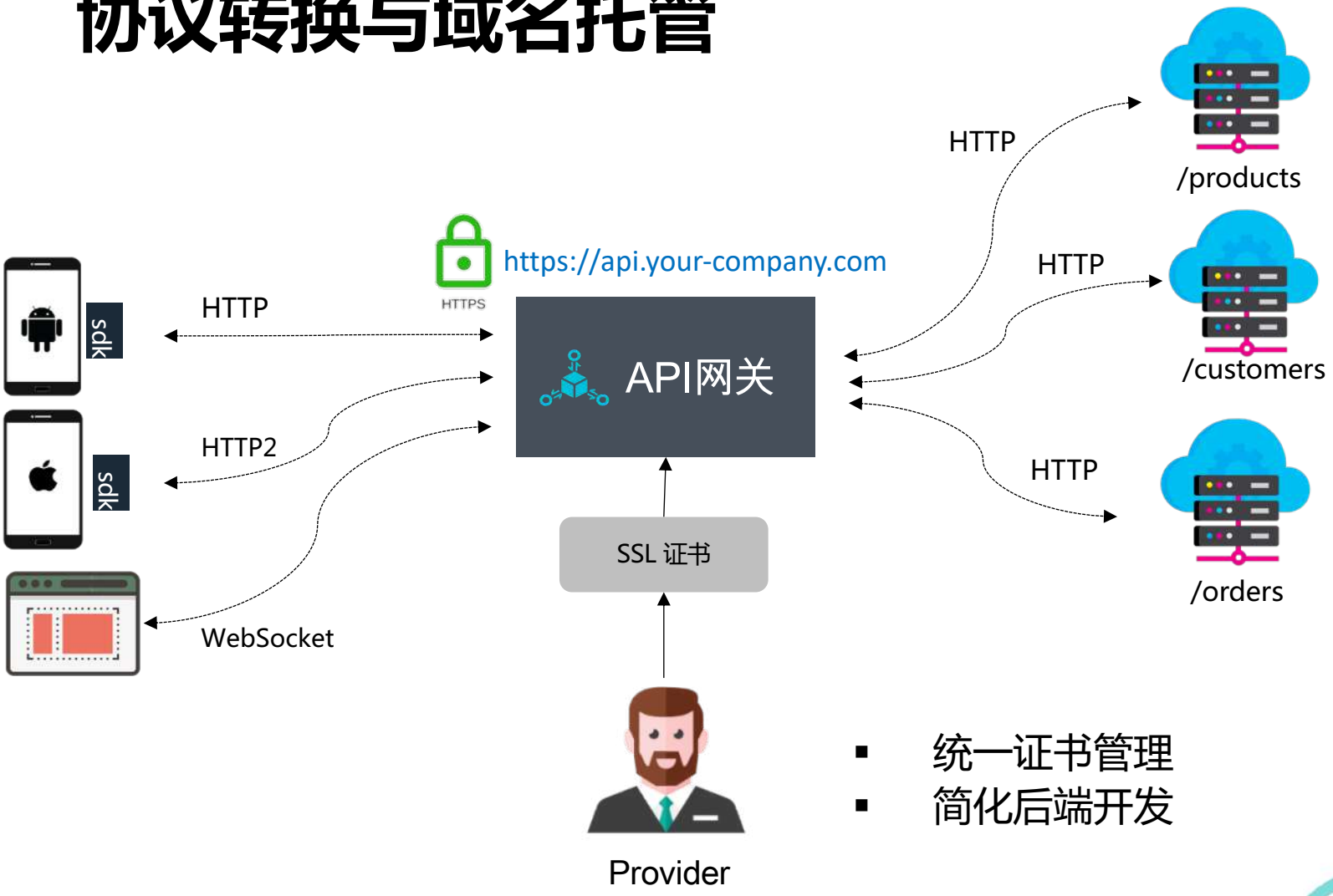
API经济与业务中台化

统一流量入口



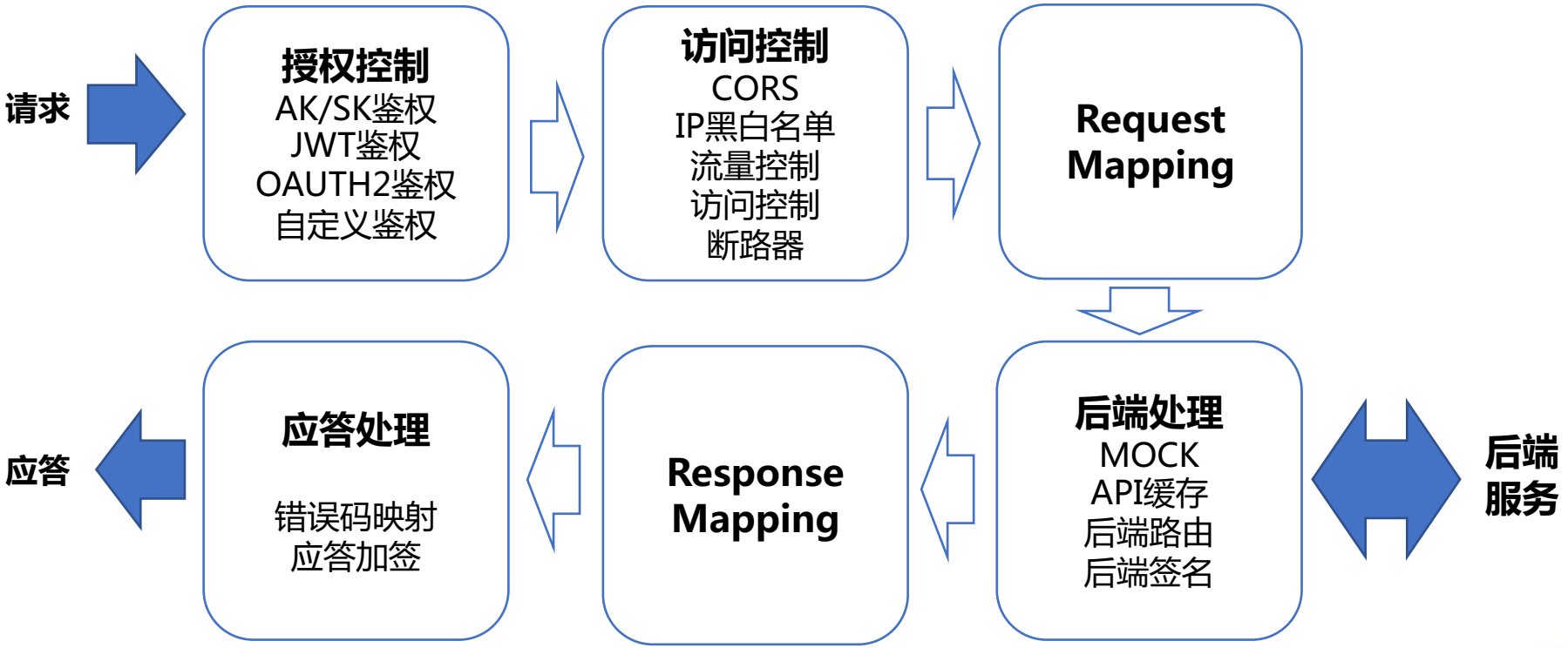
- 公网统一入口
- 内网统一入口
- 日志输出

协议转换与域名托管



- 统一证书管理
- 简化后端开发

API请求的生命周期


请求
授权控制
AK/SK鉴权
JWT鉴权
OAUTH2鉴权
自定义鉴权
访问控制
CORS
IP黑白名单
流量控制
访问控制
断路器
Request Mapping
后端处理
MOCK
API缓存
后端路由
后端签名
后端服务
Response Mapping
应答处理
错误码映射
应答加签
应答

KEY/SECRET 摘要签名鉴权

```
POST /users HTTP/1.1
Host: api.foo.com
Content-Type: application/json

{
  "userId": 101,
  "userName": "Jack"
}
```

build stringToSign

```
POST
2019-06-02T23:22:33Z
AeWvOOgP7Gg7Ydd23
123432
F41CAA3A-A096-48CD-AD53-BA5430D30C94
1474274624962
/users
```

```
POST /users HTTP/1.1
Host: api.foo.com
Content-Type: application/json
X-Ca-Key: 1234328892
Date: 2019-06-02T23:22:33Z
X-Ca-Nonce: F41CAA3A-A096-48CD-AD53-
BA5430D30C94
X-Ca-Timestamp:1474274624962
Content-MD5: AeWvOOgP7Gg7Ydd23
X-Ca-Signature-Headers: X-Ca-Key,X-Ca-
Nonce,X-Ca-Timestamp
X-Ca-Signature:2WvOOgP7Gg7Yd9879832dsdfsdf=

{
  "userId": 101,
  "userName": "Jack"
}
```

signature = HmacSHA256(stringToSign, secret)

HmacSHA1
HmacSHA256
HmacMD5
SHA256withRSA
...

通过Key获取Secret

使用Secret校验签名确定请求者身份，防请求篡改

API网关

通过客户端添加生成Nonce头实现防重放

JWT 鉴权

API网关

认证模块

PRIVATE JWK

ey1234abcdefegJIUzI1NiIsInR5cCI6Ikp123456.JzdWIiOiIxkwIiwibm1234563ODFtZSI6IkpvaG4gR1234abcdedfgjoxNTE2XYUSDFGMDIyfQ.Abcdefgjijkl12345T4fwpMeJf36POk6yJV_adQssw5c

业务模块

```
GET /orders
X-JWT-Token:
ey1234abcdefegJIUzI1NiIsInR5cCI6Ikp123456.JzdWIiOiIxkwIiwibm1234563ODFtZSI6IkpvaG4gR1234abcdedfgjoxNTE2XYUSDFGMDIyfQ.Abcdefgjijkl12345T4fwpMeJf36POk6yJV_adQssw5c
```

PUBLIC JWK

验签+Payload字段转换

```
{
  "alg": "HS256",
  "typ": "JWT"
}
{
 "userId": "10001",
 "userName": "Jack",
 "userRole": "User",
 "iat": 1516239022
}
```

```
GET /orders
X-UserName: Jack
X-UserId: 10001
```

- 托管公钥实现Token验签与Payloady映射

访问控制

```
GET /orders/10002
X-JWT-Token:
ey1234abcdefegJIUzI1NiIs
InR5cCI6Ikp123456.JzdWIiO
iIxkwIiwibm1234563ODFtZSI6I
kpvaG4gR1234abcdedfgjoxNTE2
XYUSDFGMDIyfQ.Abcdefgjijk
l12345T4fwpMeJf36POk6yJV
_adQssw5c
```

验签+Payload字段转换

```
{
  "alg": "HS256",
  "typ": "JWT"
}
{
 "userId": "10001",
 "userName": "Jack",
 "userRole": "User",
 "iat": 1516239022
}
```

PUBLIC JWK

自定义访问控制策略

```
allowPolicies:
- name: userId
  condition: "$userId = $JwtClaims.userId"
```

API网关

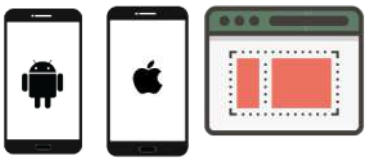
/orders/{userId}

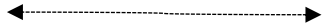
```
HTTP/1.1 403 Access Denied
```

参数的校验与映射

```
"/users/{userId}":
  GET:
    x-aliyun-apigateway-mapping-mode: mapping
    x-aliyun-apigateway-backend:
      address: http://100.67.8.10:18088
      method: POST
      path: getUserInfo
    parameters:
    - name: userId
      in: path
      name: integer
      required: true
      x-aliyun-apigateway-backend-location: formData
    - name: filter
      in: query
      required: false
      default: summary
      type: string
      x-aliyun-apigateway-backend-location: formData
```

```
GET /users/1002 HTTP/1.1
Host: api.foo.com
```

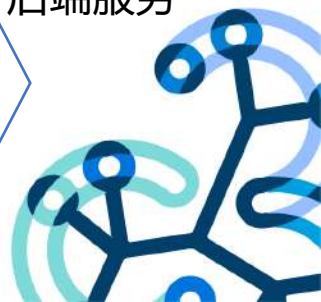




后端服务

- 过滤非期望参数
- 自动添加默认参数
- 参数映射，适配不同API风格

```
POST /getUserInfo HTTP/1.1

userId=1002&filter=summary
```



常量参数与系统参数

```
GET /users/1002 HTTP/1.1
Host: api.foo.com
```

```
...
x-aliyun-apigateway-constant-parameters:
- name: version
  location: formData
  value: 1.0
x-aliyun-apigateway-system-parameters:
- systemName: CaClientIp
  location: header
  name: X-ClientIp
```

API网关

后端服务

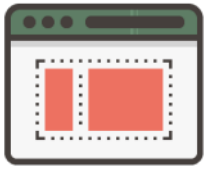
```
POST /getUserInfo HTTP/1.1
X-ClientIp: 63.232.33.3

userId=1002&filter=summary&version=1.0
```

- 解决API适配与兼容性
- 在网关层面解决统一的问题

处理CORS跨域资源访问

```
OPTIONS /cors HTTP/1.1
Origin: http://api.bob.com
Access-Control-Request-Method: PUT
Access-Control-Request-Headers: X-Custom-Header
Host: api.alice.com
Accept-Language: en-US
Connection: keep-alive
User-Agent: Mozilla/5.0...
```

```
allowOrigins: api.bob.com
allowMethods: GET,POST,PUT,PATCH
allowHeaders: X-Custom-Header
allowCredentials: true
```



后端服务

- 由网关处理简单请求和预检请求
- 简化后端配置

```
HTTP/1.1 200 OK
Date: Mon, 01 Dec 2008 01:15:39 GMT
Server: Apache/2.0.61 (Unix)
Access-Control-Allow-Origin: http://api.bob.com
Access-Control-Allow-Methods: GET, POST, PUT, PATCH
Access-Control-Allow-Headers: X-Custom-Header
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip Content-Length: 0
Keep-Alive: timeout=2, max=100
Connection: Keep-Alive Content-Type: text/plain
```

API缓存

```
varyByParameters:
- userId
varyByHeaders:
- Accept
- Accept-Language
```

```
GET /users/1002 HTTP/1.1
Host: api.foo.com
```

```
HTTP/1.1 200
Cache-Control: duration=900

{
  “name”: “Jack”,
  “age”: 24
  ”role”: user
}
```

- 根据参数区分缓存
- 根据Header区分缓存

参数路由

```
routes:
  - name: vipService
    backend:
      address: 172.16.0.11
    condition: "$CaAppKey = ‘100666’”
 - name: experienceService
    backend:
      address: 172.16.0.15
    condition: "$CaUserAgent = '2.0.0'"
```

appId = 100666

UserAgent: 2.0.0

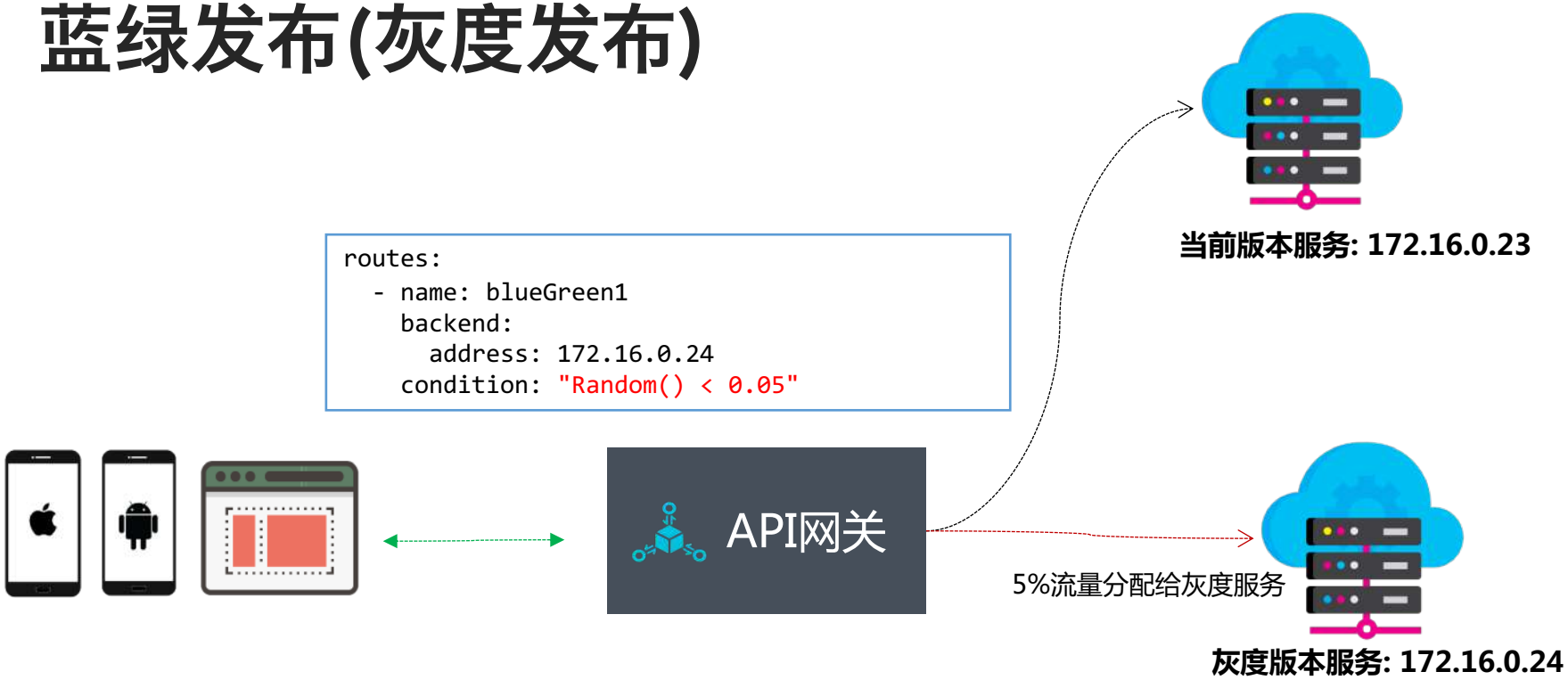
VIP服务
172.16.0.11

默认服务
172.16.0.10

测试体验服务
172.16.0.15

- 租户隔离，为VIP用户提供专门保障，
- 测试&体验场景，隔离测试服务

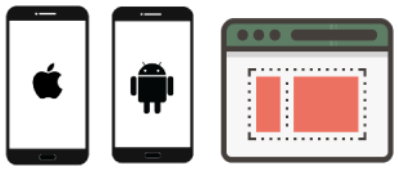
蓝绿发布(灰度发布)



- 按比例分配流量给灰度版本服务
- 可与参数路由组合使用

流量复制

```
replicates:
  - name: alphaTest
    backend:
      address: 172.16.0.17
    condition: "Random() < 0.10"
```



当前版本服务
172.16.0.10

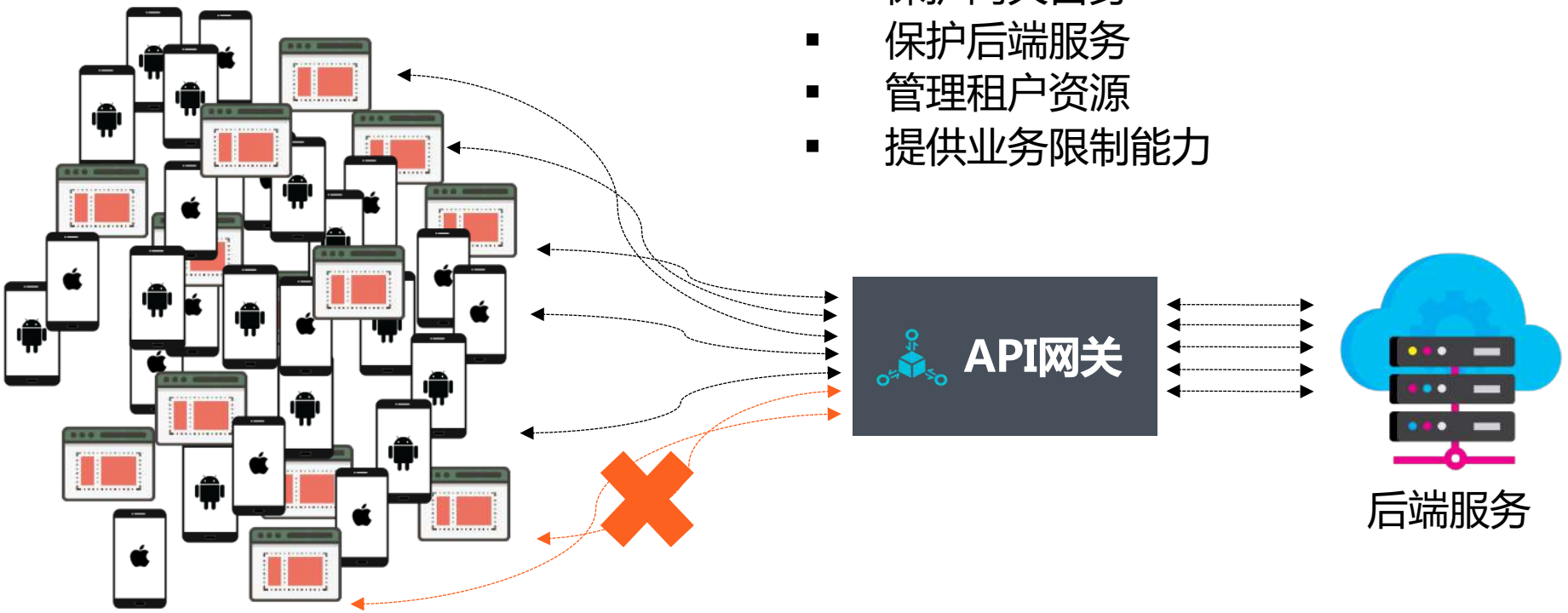
10%流量复制给Alpha服务，
仅记录日志忽略返回请求

Alpha版本服务
172.16.0.17

- 用于更稳妥的大版本发布前测试，降低发布风险
- 可用于模拟真实环境的压力测试

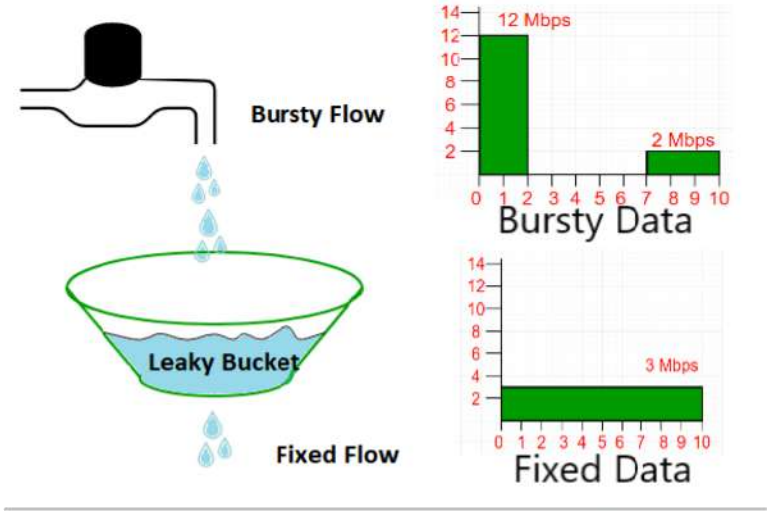
流量控制

- 保护网关自身
- 保护后端服务
- 管理租户资源
- 提供业务限制能力

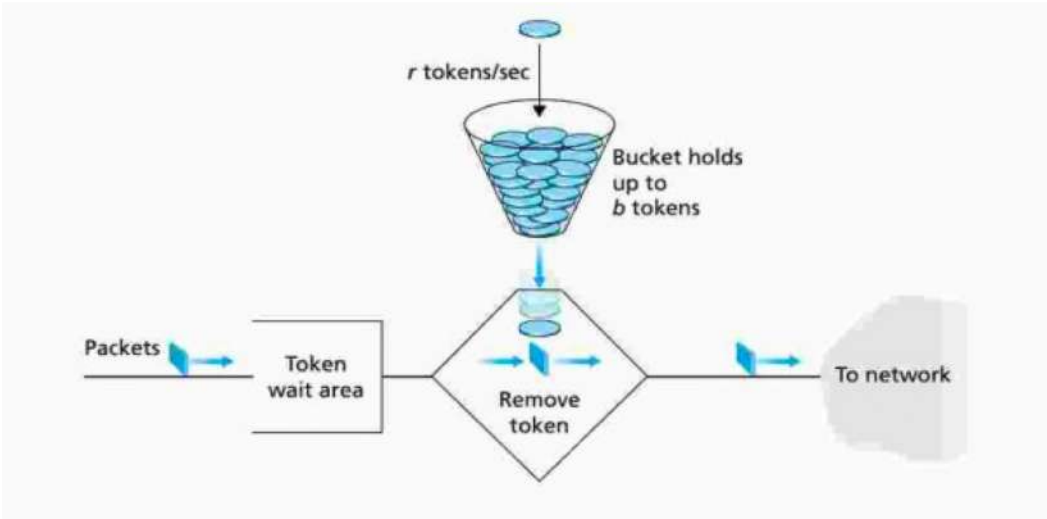


常见的流控算法与策略

漏桶(Leak Bucket)

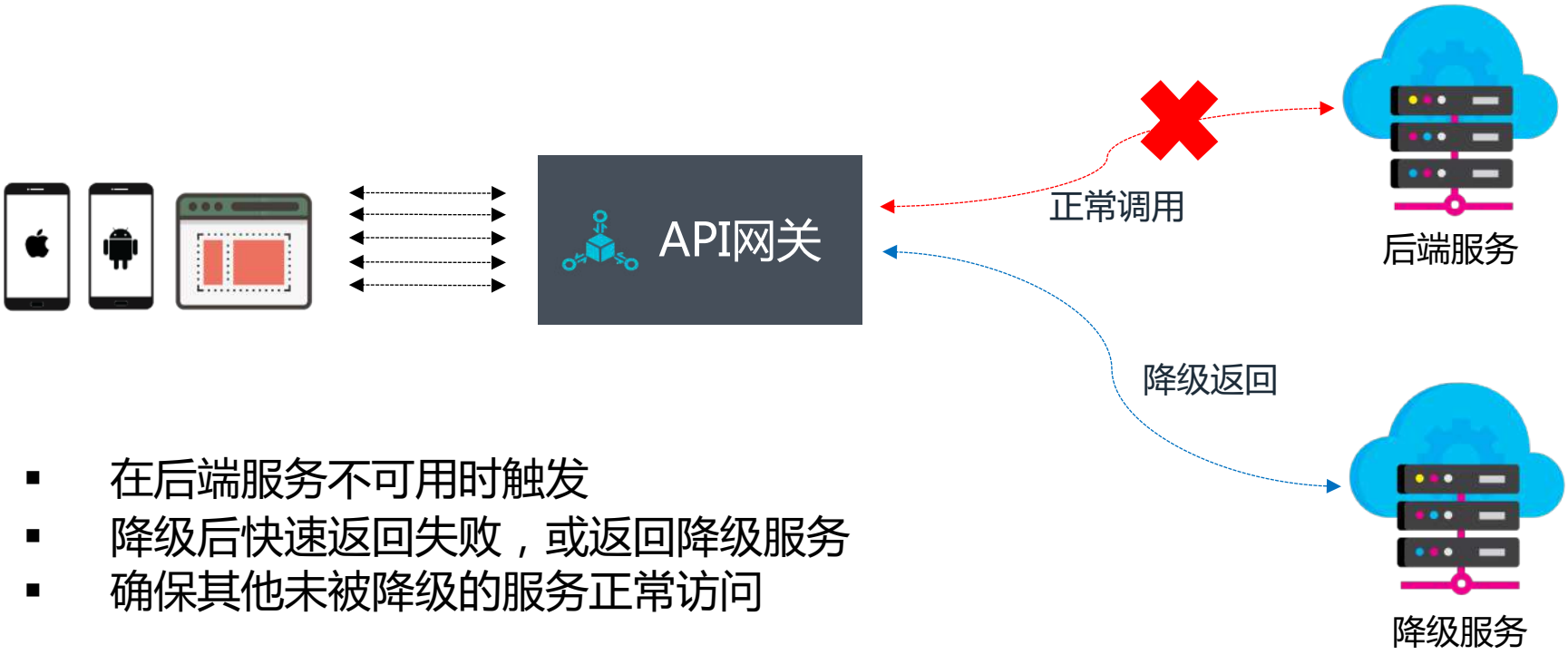


令牌桶(Token Bucket)



流控后的处理：快速失败，排队等待，降级

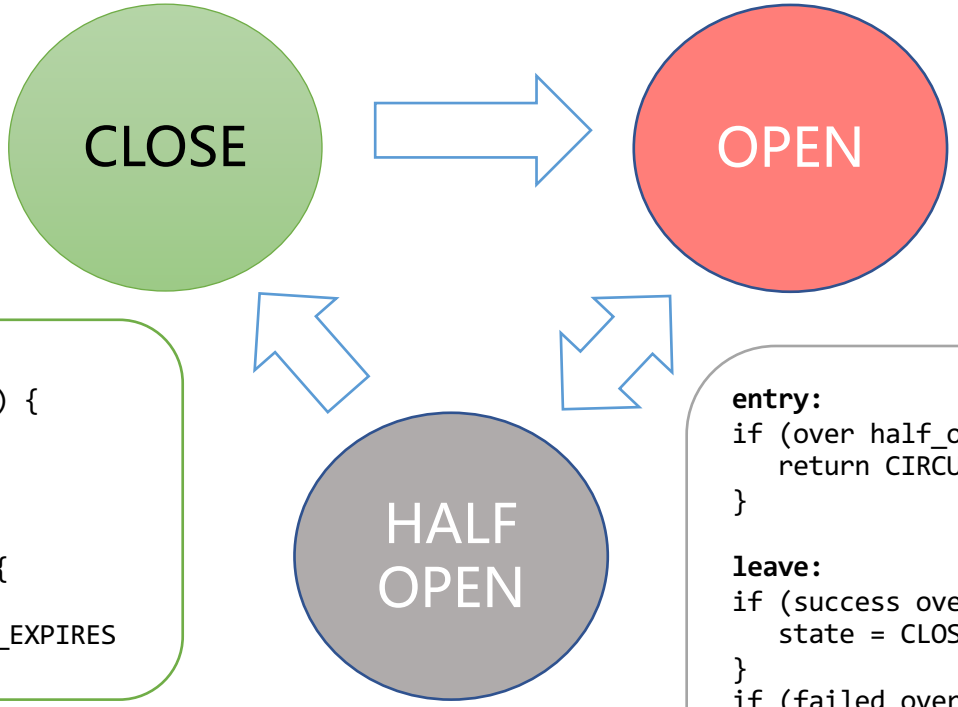
断路器与服务降级



- 在后端服务不可用时触发
- 降级后快速返回失败，或返回降级服务
- 确保其他未被降级的服务正常访问

断路器的实现方式

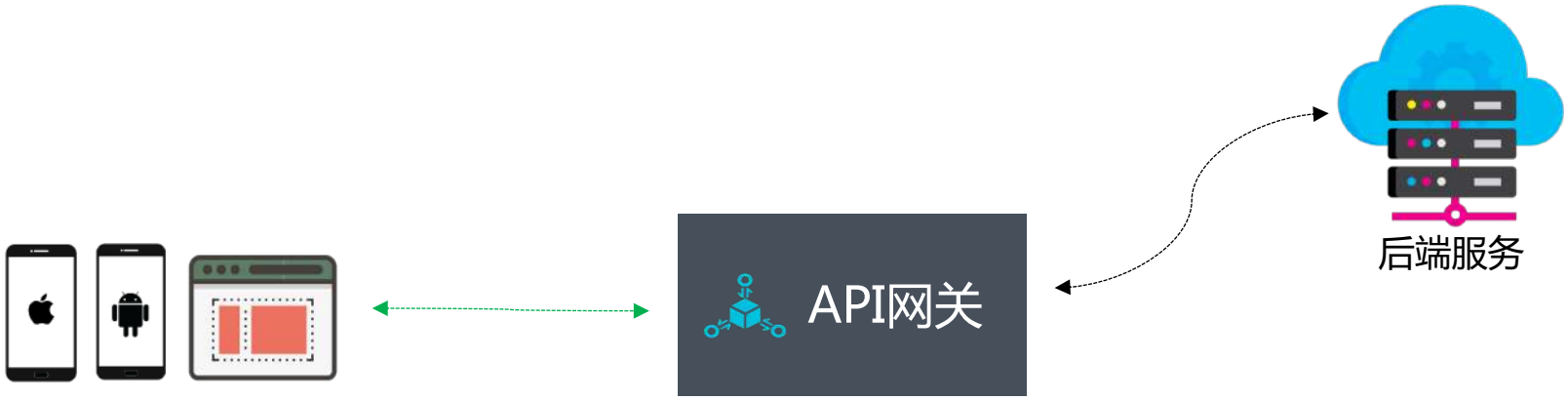
```
entry:
if (not expired) {
  return CIRCUIT_BREAKER_OPEN
}
state = HALF_OPEN

leave:
```



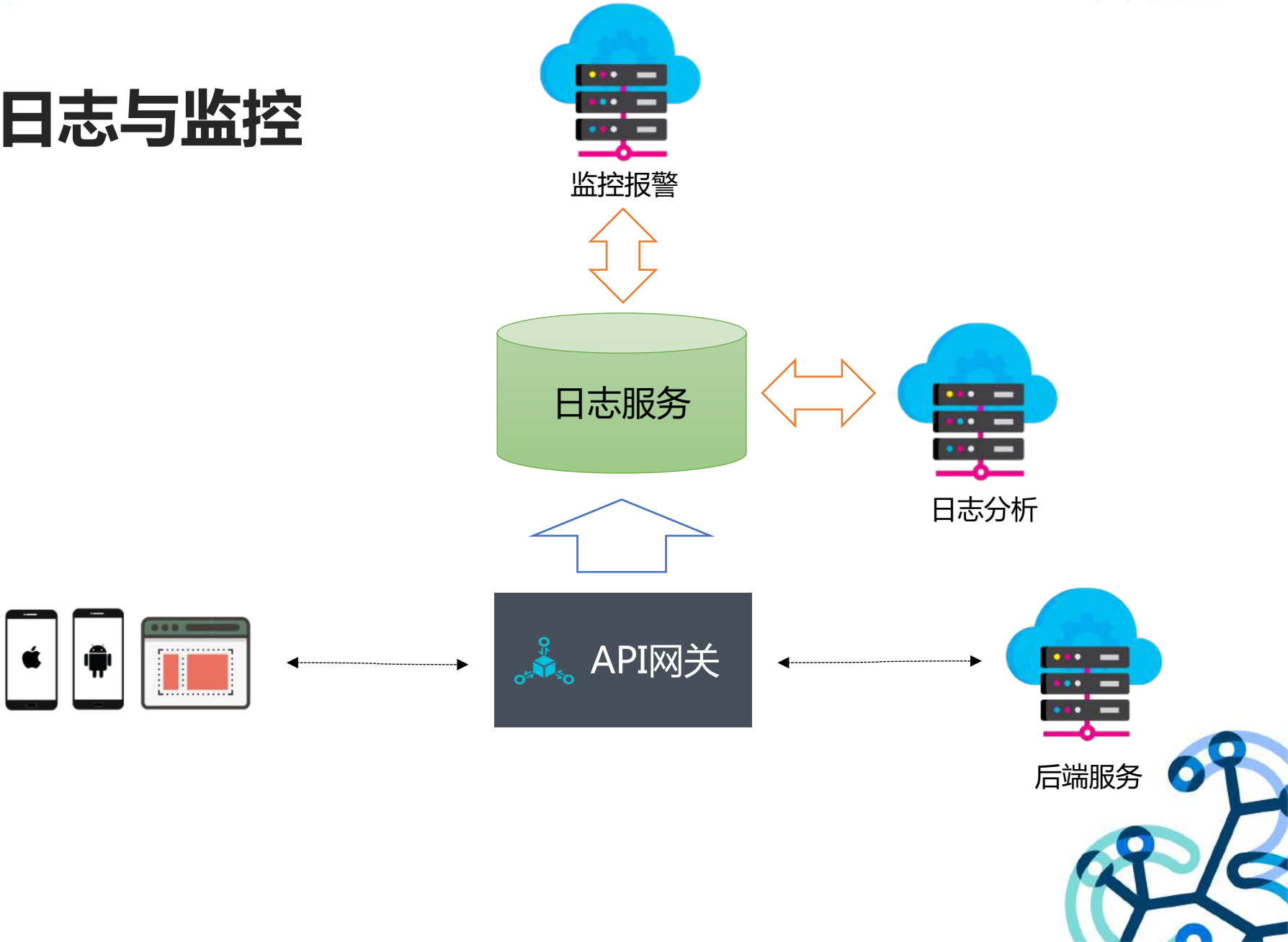

```
entry:
if (over max concurrent) {
   return BUSY;
}

leave:
if (too many timeouts) {
   state = OPEN
   expired = now + OPEN_EXPIRES
}
```

```
entry:
if (over half_open concurrent) {
   return CIRCUIT_BREAKER_OPEN
}

leave:
if (success over threshold) {
   state = CLOSE
}
if (failed over threshold) {
   state = OPEN
   expired = now + HALF_OPEN_EXPIRES

}
```

错误码映射


后端服务
API网关
mapping
HTTP 404
X-Ca-Error-Message: Role Not Exist
HTTP 200 OK
Content-Type:application/json
{
"req_msg_id":"d02afa56394f458e1772",
"result_code":"ROLE_NOT_EXISTS”
}

日志与监控



API元数据定义与管理

可视化编辑

API网关控制台

分组/域名/证书

API定义/发布/授权

插件定义/绑定

导入Swagger

SWAGGER

OPENAPI

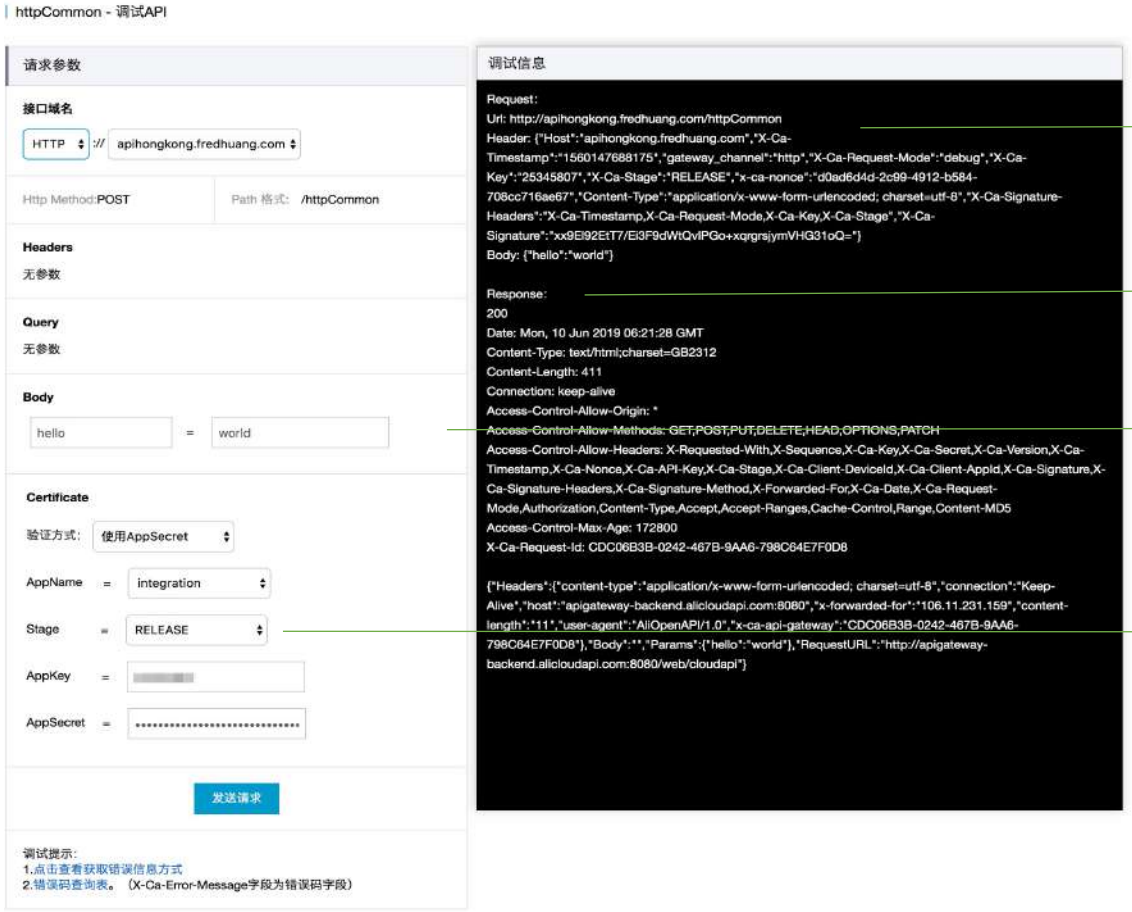
> aliyun

HashiCorp Terraform

SDK

- 支持多种编辑方式
- Swagger规范

API在线调试



请求报文细节

应答报文报文细节

填写API的参数

选择调试的环境和授权使用的应用

管理API的整个生命周期

API网关能力总结

安全

- HTTPS证书托管
- 全链路加密传输
- 全链路签名验证机制
- AK/SK鉴权管理
- 防重放机制
- 流量控制
- 参数校验
- IP黑白名单

高效

- 多协议接入与转换
- 参数映射、常量参数、系统参数
- WebSocket双向通信
- JWT鉴权
- CORS跨域资源访问
- 自定义访问控制
- API缓存

智能

- 多套环境支持
- 蓝绿发布
- 断路器与服务降级
- 日志监控预警
- 全链路日志追踪
- API集成

友好

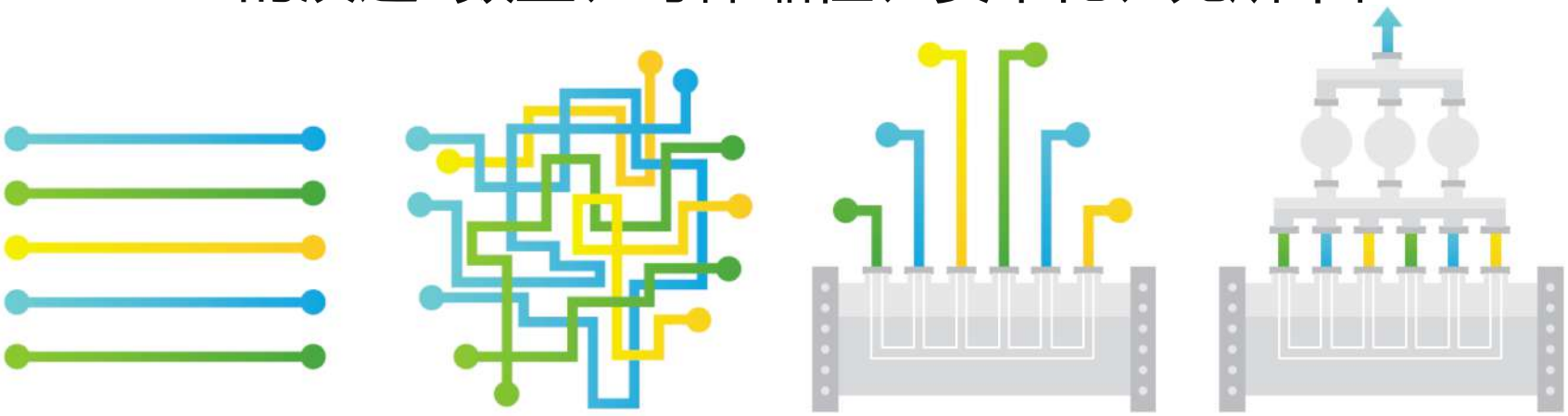
- API全生命周期管理
- Swagger规范
- 多种元数据管理方式
- SDK/文档自动生成
- MOCK
- 在线调试

1 API网关角色的引入

2 API网关为微服务开发带来的好处

3 **API经济**

API的演进: 数量、可伸缩性、货币化、无所不在



1960–1980

Basic interoperability enables the first programmatic exchanges of information. Simple interconnect between network protocols. Sessions established to exchange information.

TECHNIQUES

ARPANET, ATTP, and TCP sessions.

1980–1990

Creation of interfaces with function and logic. Information is shared in meaningful ways. Object brokers, procedure calls, and program calls allow remote interaction across a network.

TECHNIQUES

Point-to-point interfaces, screenscraping, RFCs, and EDI.

1990–2000

New platforms enhance exchanges through middleware. Interfaces begin to be defined as services. Tools manage the sophistication and reliability of messaging.

TECHNIQUES

Message-oriented middleware, enterprise service bus, and service-oriented architecture.

2000–today

Businesses build APIs to enable and accelerate new service development and offerings. API layers manage the OSS/BSS of integration.

TECHNIQUES

Integration as a service, RESTful services, API management, and cloud orchestration.

图片来源: ProgrammableWeb, http://programmableweb.com

API市场

金融理财

提供如银行卡实名认证、个人/企业征信等API接口。

查看更多

股票行情　个人征信
汇率工具　企业工商

生活服务

提供天气预报、快递查询、图形验证码识别、笑话大全等API接口

查看更多

天气数据　新闻热点
星座算命　条码查询

企业管理

提供企业工商年报信息查询，专利信息查询，公司新闻信息查询等API接口服务

查看更多

企业工商　电子签章
舆情分析　可视化大屏

电子商务

提供常用的实名认证、人工智能、快递管理、可视化数据分析数据及接口服务。

查看更多

IP查询　快递查询
网站监测　短信服务

人工智能

提供人脸识别、机器翻译、OCR人、人证对比、自然语言等API接口

查看更多

OCR　人脸识别
智能医疗　直播检测

交通地理

提供违章查询、公交路线查询、运营商基站、火车票查询等API接口

查看更多

违章查询　车辆服务
航空航班　基站定位

气象水利

提供全国天气预报查询，PM2.5空气质量指数，墨迹天气等API接口服务

查看更多

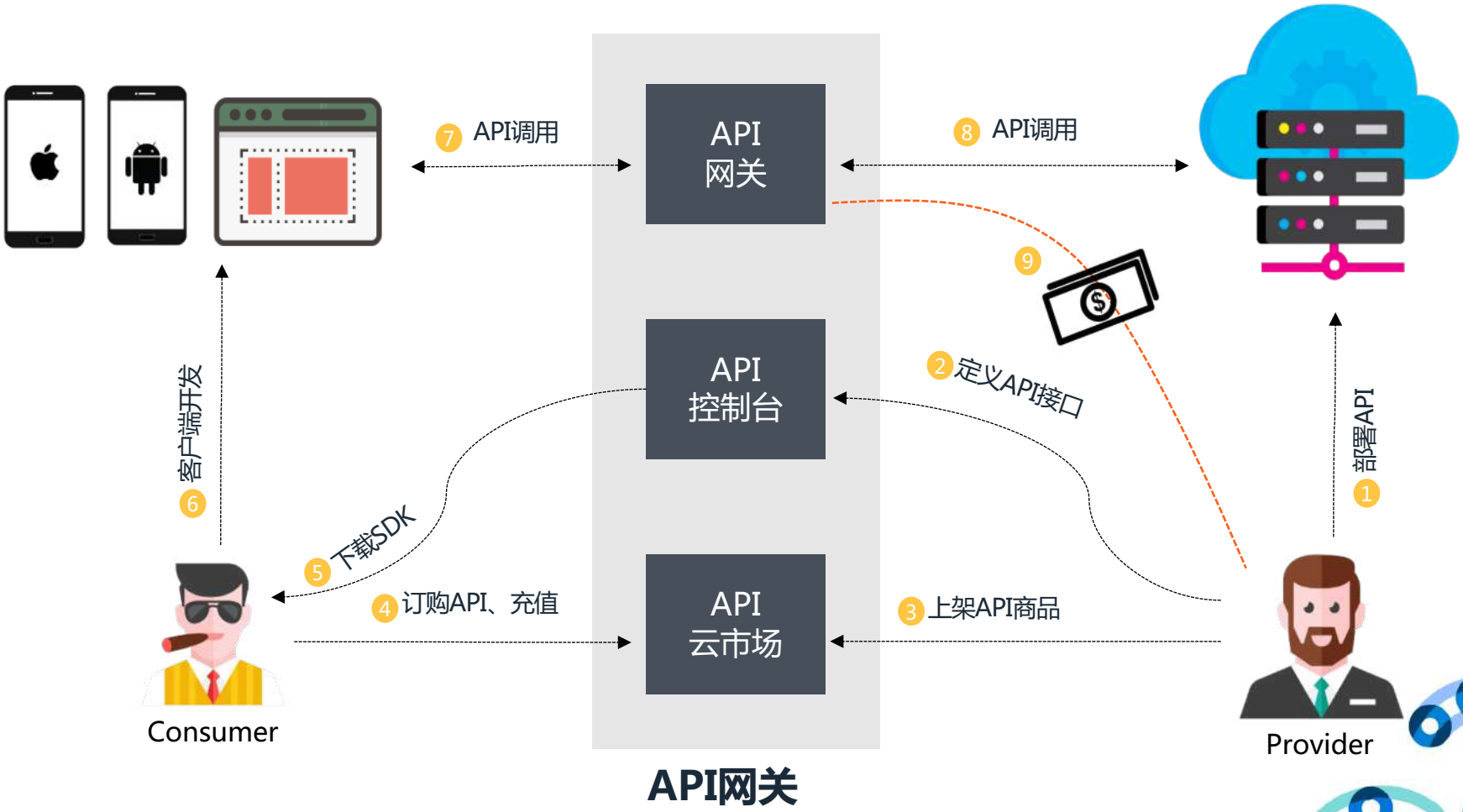
天气预报　空气质量
气象报告　污染灾害

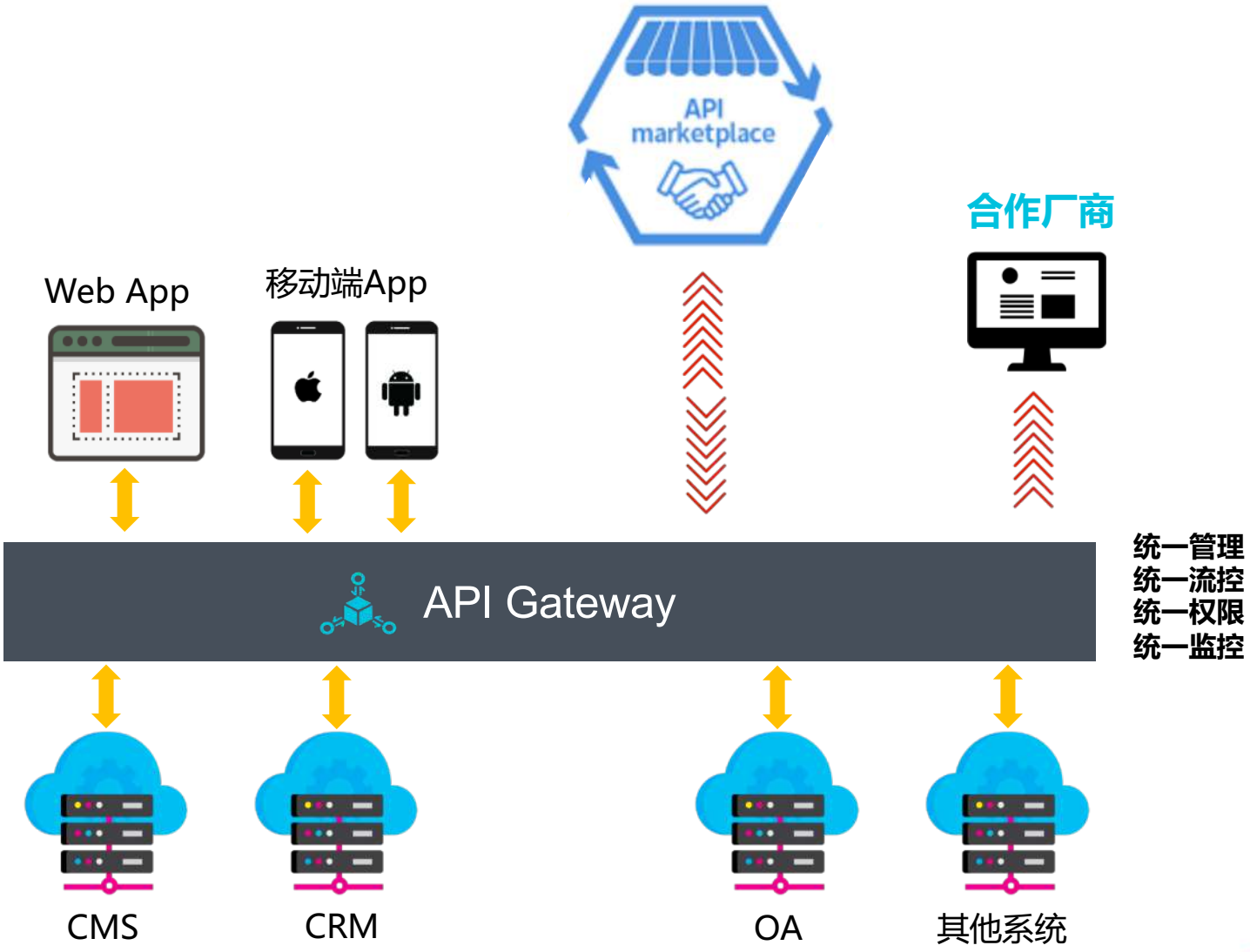
公共事务

为公共事务提供API接口数据如邮编查询，ip地址查询，今天日油价等API接口数据

民生信息　网络社交
应用开发　其他

通过API市场实现能力互补与变现




API marketplace
合作厂商
Web App
移动端App
API Gateway
统一管理
统一流控
统一权限
统一监控
CMS
CRM
OA
其他系统

关注msup微信公众账号

获取更多技术实践干货

关注高可用架构公众账号

改变互联网的构建方式