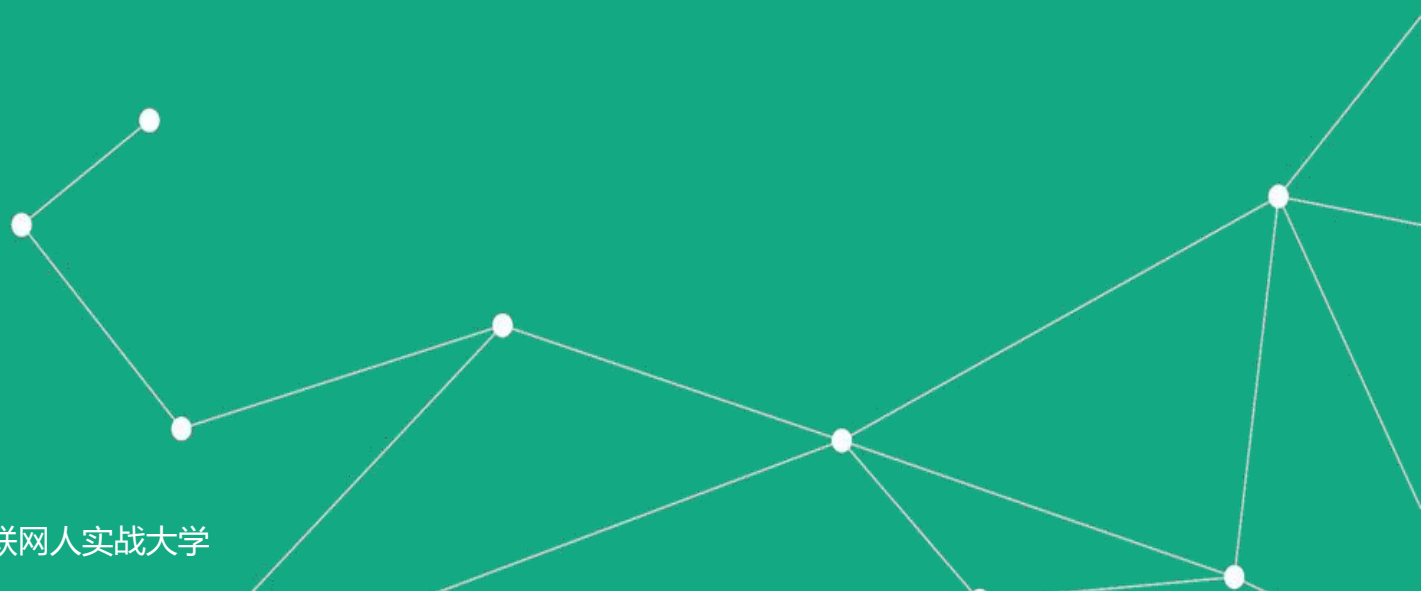
课时9

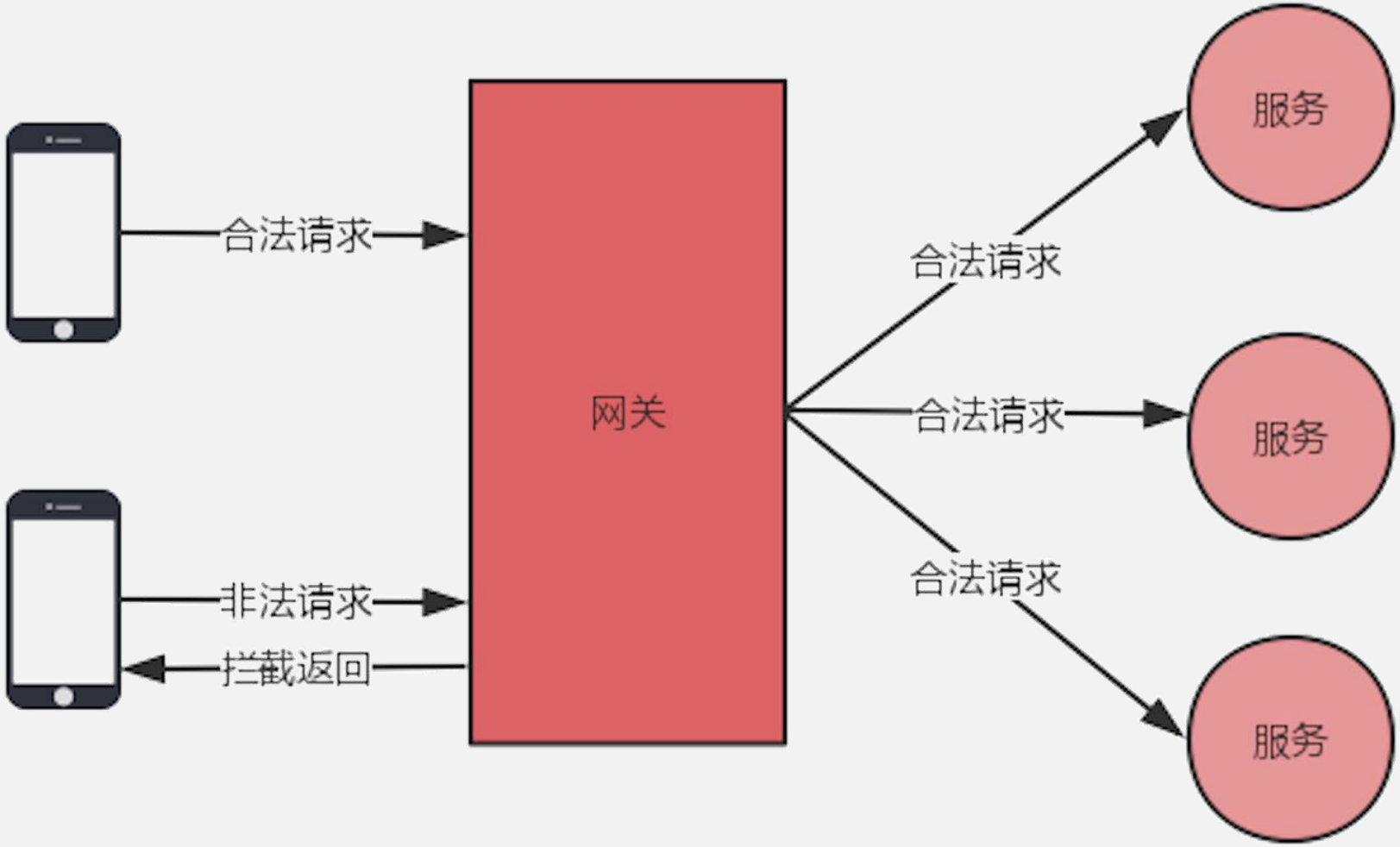
微服务安全认证

1. 服务器架构安全认证
2. 常见的认证方式
3. JWT 认证
4. Token 的使用
5. 内部服务之间的认证



微服务架构安全认证

拉勾
LAGOU.COM



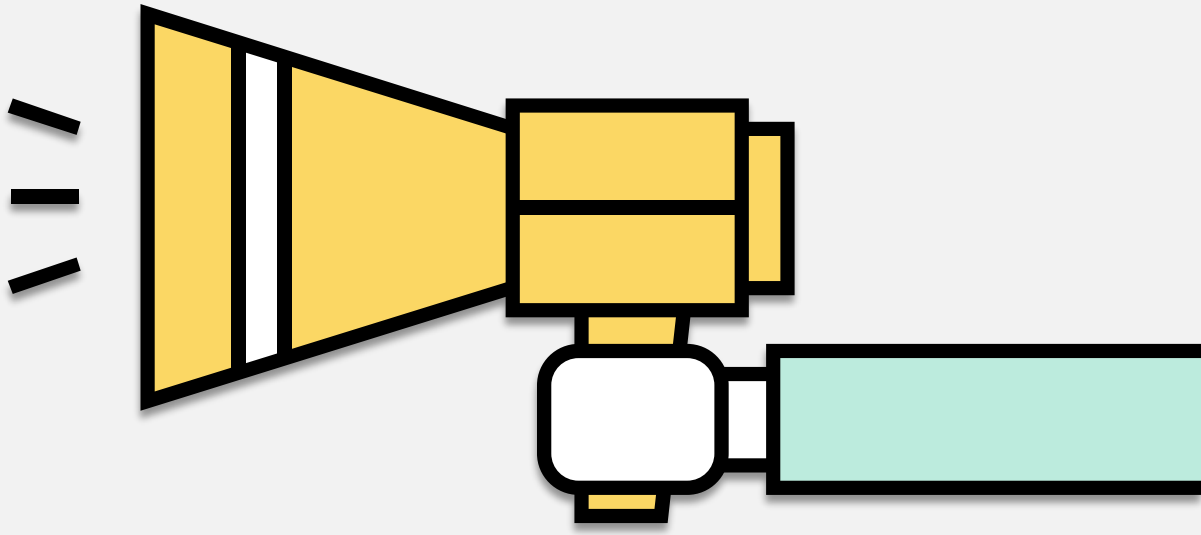
常用的认证方式

拉勾
LAGOU.COM

Session

HTTP Basic Authentication

Token



Jwt介绍

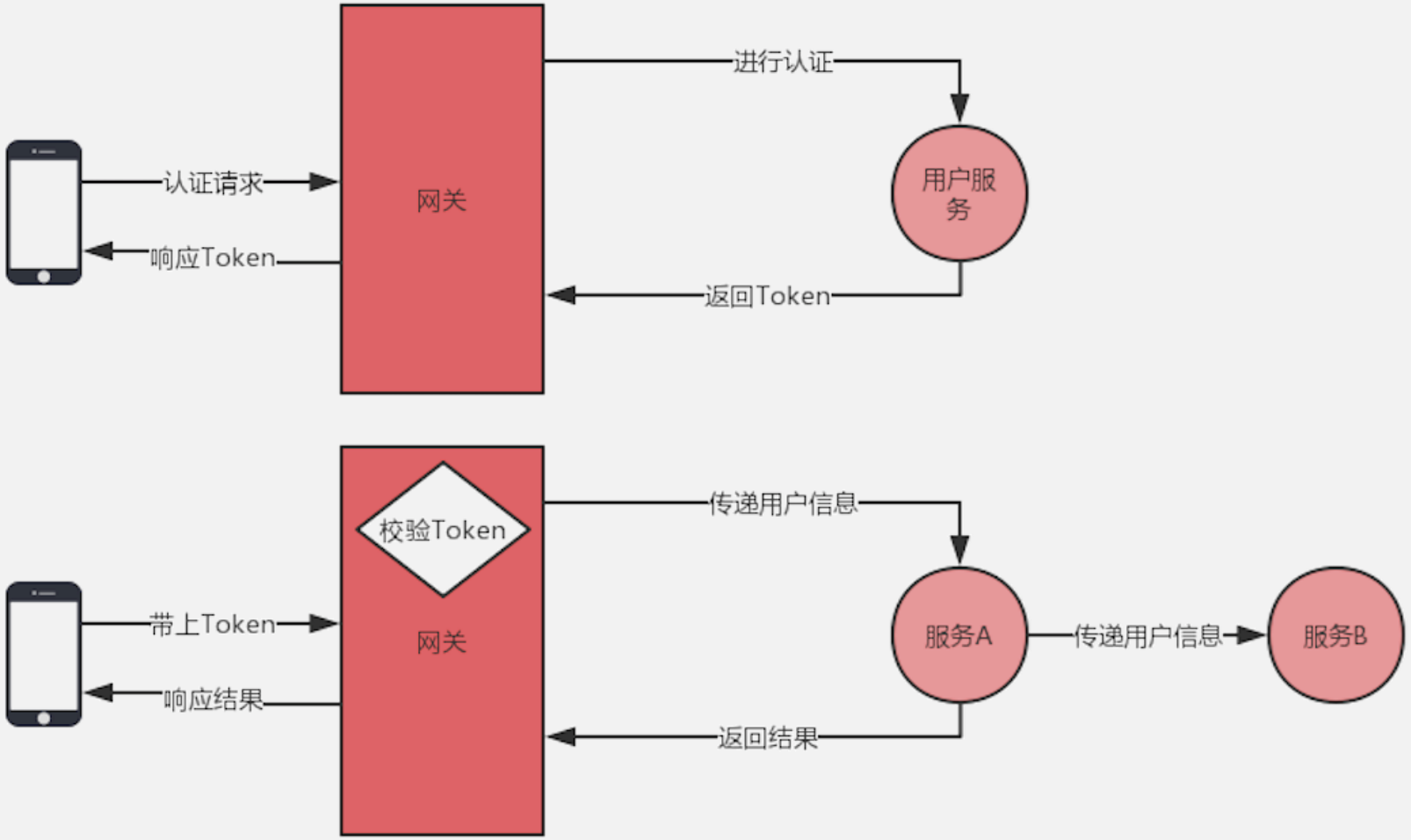
拉勾 LAGOU.COM

JWT（Json Web Token）是为了在网络应用环境间传递声明而执行的一种基于 Json 的开放标准
JWT 的声明一般被用来在身份提供者和服务提供者间传递被认证的用户身份信息， 以便于从资源服务器获取资源

token = encodeBase64(header) + '.' + encodeBase64(payload) + '.' + encodeBase64(signature)

Header	Payload	Signature
{ "alg": "HS256", "typ": "JWT" }	{ "id": "1234567890", "name": "John Doe" }	HMACSHA256(base64UrlEncode(header) + "." + base64UrlEncode(payload), secret)

基于Jwt的认证


进行认证
认证请求
网关
用户服务
响应Token
返回Token
校验Token
传递用户信息
带上Token
网关
服务A
传递用户信息
服务B
响应结果
返回结果

用户信息的全局传递扩展

拉勾
LAGOU.COM

传递方式：

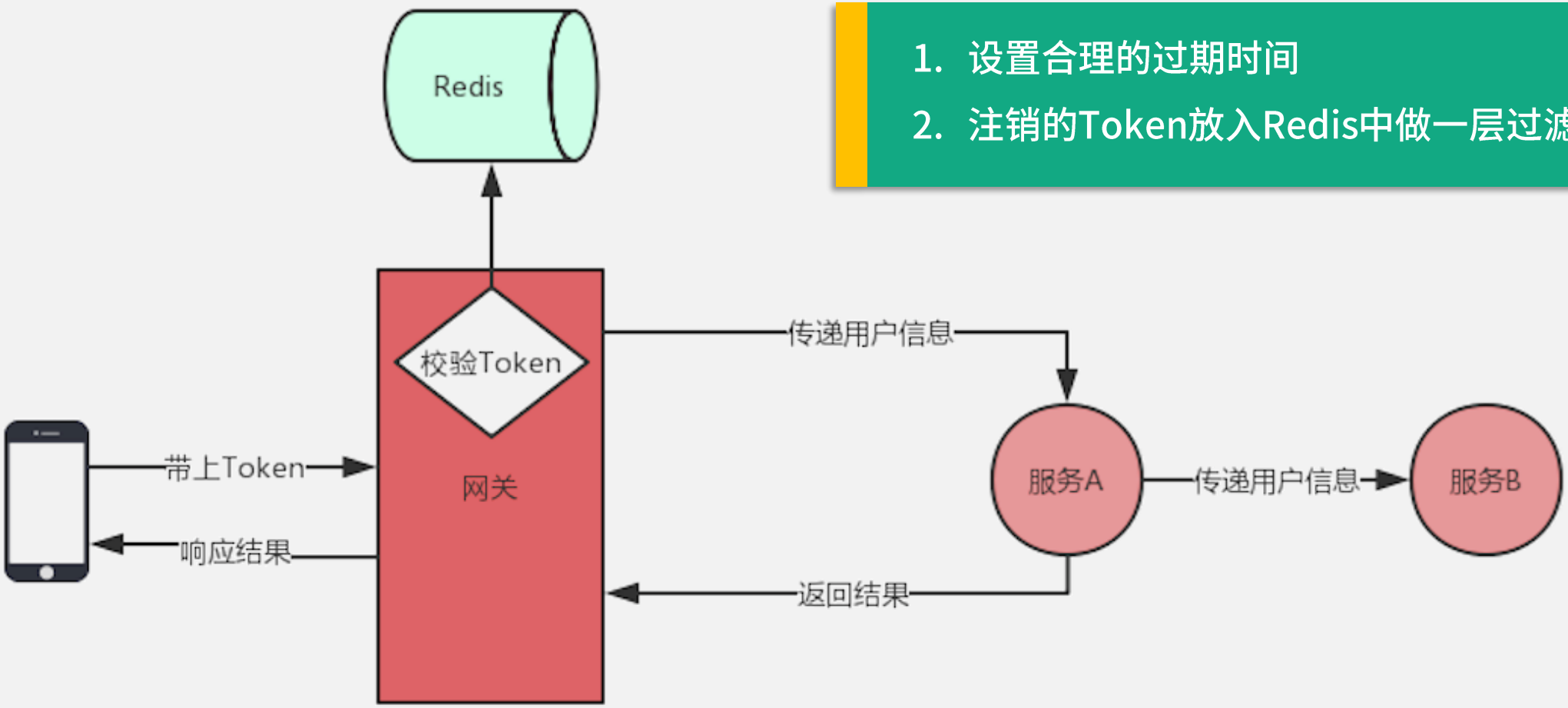
参数传递
1. 所有接口都要定义用户ID参数
2. 一层层接收，一层层传递

请求头传递
1. 网关中传递到后端服务
2. 后端服务调用传递（Feign, RestTemplate）
3. 统一封装处理，不需要开发人员关心

Token的注销

拉勾 LAGOU.COM

1. 设置合理的过期时间
2. 注销的Token放入Redis中做一层过滤



Token的安全使用建议

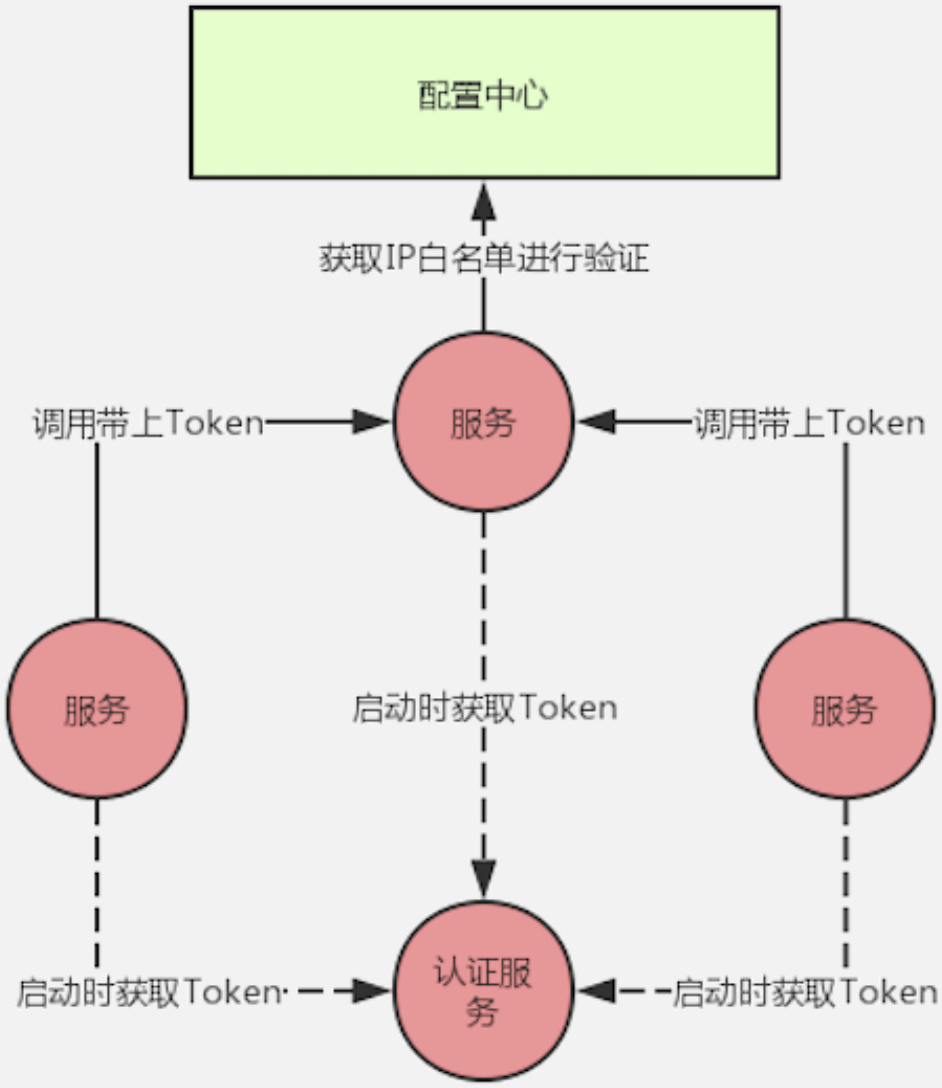
拉勾 LAGOU.COM

- 设置较短（合理）的过期时间
- 注销的Token及时清除（放入Redis中做一层过滤）
- 监控Token的使用频率
- 核心功能敏感操作可以使用动态验证（验证码）
- 网络环境，浏览器信息等识别
- 加密密钥支持动态修改

内部服务之间的认证

拉勾 LAGOU.COM

- 不验证
- IP白名单
- 内部Token



Next：课时10《灰度发布实战》