一、什么是API网关？

API网关可以看作系统与外界联通的入口，我们可以在网关进行处理一些非业务逻辑的逻辑，比兔权限验证，监控，缓存，请求路由等等。

二、为什么需要API网关？

* RPC协议转成HTTP
* 请求路由
* 统一鉴权
* 统一监控
* 流量控制，熔断降级

微服务下一个系统被拆分为多个服务，但是像安全认证，流量控制，日志，监控等功能是每个服务都需要的，没有网关的话，我们就需要在每个服务中单独实现，这使得我们做了很多重复的事情并且没有一个全局的视图来统一管理这些功能。

综上：一般情况下，网关一般都会提供请求转发、安全认证（身份/权限认证）、流量控制、负载均衡、容灾、日志、监控这些功能。

上面介绍了这么多功能实际上网关主要做了一件事情：请求过滤。权限校验、流量控制这些都可以通过过滤器实现，请求转也是通过过滤器实现的。

三、常见的网关系统

1. Kong
2. Netflix zuul

Kong相比于Zuul更加强大并且简单易用。Kong基于Openresty，Zuul基于Java。

OpenResty（也称为ngx\_openresty）是一个全功能的Web应用服务器。它打包

了标准的Nginx核心，很多的常用的第三方模块，以及它们的大多数依赖项。

通过揉和众多设计良好的Nginx模块，OpenResty有效地把Nginx服务器转变为一个强大的Web应用服务器，基于它开发人员可以使用Lua编程语言对Nginx核心以及现有的各种Nginx C模块进行脚本编程，构建出可以处理一万以上并发请求的极端高性能的Web应用。

另外，Kong还提供了插件机制来扩展其功能。比如，在服务上启用Zipkin插件。

$ curl -X POST http://kong:8001/services/{service}/plugins \

--data "name=zipkin" \

--data "config.http\_endpoint=http://your.zipkin.collector:9411/api/v2/spans" \

--data "config.sample\_ratio=0.001"

四、统一API网关

统一API网关不仅有API网关的所有特点，还有下面几个好处：

* 统一技术组件升级
* 统一服务接入
* 节约资源

#### 1、统一网关的设计

1. 异步化请求

对于我们统一的网关层，如何用少量的机器接入更多的服务，这就需要我们的异步，用来提高更多的吞吐量。对于异步化一般有下面两种策略：

Tomcat/Jetty+NIO+servlet3（普遍使用，京东，有赞，Zuul都选取的是这个策略，这种策略比较适合HTTP。在Servlet3中可以开启异步）；Netty+NIO（Netty为高并发而生，目前唯品会的网关使用这个策略，在唯品会的技术文章中在相同的情况下Netty是每秒30w+的吞吐量，Tomcat是13w+，但是Netty需要自己处理HTTP协议）。

对于网关是HTTP请求场景比较多的情况可以采用Servlet，毕竟有更加成熟的处理HTTP协议。如果更加重视吞吐量那么可以采用Netty。

全链路异步（对于来的请求我们已经使用异步了，为了达到全链路异步我们需要对去的请求也进行异步处理，对于去的请求可以利用我们rpc的异步支持进行异步请求。在web容器中开启servlet异步，然后进入到网关的业务线程池中进行业务处理，然后进行rpc的异步调用并注册需要回调的业务，最后再回调线程池中进行回调处理。）

1. 链式处理

在设计模式中有一个模式叫责任链模式，他的作用是避免请求发送者与接收者耦合在一起，让多个对象都有可能接受请求，将这些对象连接成一条链，并且沿着这条链传递

1. 业务隔离
2. 请求限流
3. 熔断降级
4. 泛化调用
5. 管理平台