科研项目立项计划书

项目名称：Boss直聘Api网关系统

实施单位：北京华品博睿网络技术有限公司

立项时间：2019年1月

承担部门：研发部

一、立项目的、意义和必要性

近几年来，移动应用与企业间互联需求的兴起。移动应用、企业互联，使得后台服务支持的对象，从以前单一的Web应用，扩展到多种使用场景，且每种使用场景对后台服务的要求都不尽相同。这不仅增加了后台服务的响应量，还增加了后台服务的复杂性。随着微服务架构概念的提出，API网关成为了微服务架构的一个标配组件。

API 网关，即API Gateway，是大型分布式系统中，为了保护内部服务而设计的一道屏障，可以提供高性能、高可用的 API托管服务，从而帮助应用服务的开发人员便捷地对外提供服务，而不用考虑安全控制、流量控制、审计日志等问题，统一在网关层将安全认证，流量控制，审计日志，黑白名单等实现。网关的下一层，是内部服务，内部服务只需开发和关注具体业务相关的实现。网关可以提供API发布、管理、维护等主要功能。开发人员只需要简单的配置操作即可把自己开发的服务发布出去，同时置于网关的保护之下。

现在想要进行水电煤缴费，根本不需要再跑到营业厅，只要通过电子商城就可以办理相关的业务，但你或许并不知道，其实这一切的实现都离不开API网关（API Gateway）。运营商通过API向第三方的服务平台开放了套餐服务，当中API网关就像一堵城墙一样通过流控、鉴权等机制保障相关的安全性，使得这样方便流畅的体验得以实现。现在想要进行水电煤缴费，根本不需要再跑到营业厅，只要通过电子商城就可以办理相关的业务，但你或许并不知道，其实这一切的实现都离不开API网关（API Gateway）。运营商通过API向第三方的服务平台开放了套餐服务，当中API网关就像一堵城墙一样通过流控、鉴权等机制保障相关的安全性，使得这样方便流畅的体验得以实现。

二、国内外情况综述

业界 API 网关解决方案有很多，包括商业的、开源的。例如 Tyk、Kong、API Umbrella、ApiAxle、Netflix Zuul、WSO2 API Manager、ClydeIO 等。

常见的有：

Nginx + Lua

Nginx 是由 Igor Sysoev 为俄罗斯访问量第二的 Rambler.ru 站点开发的，一个高性能的 HTTP 和反向代理服务器。2012 年，Nginx 荣获年度云计算开发奖，并成长为世界第二大 Web 服务器。全世界流量最高的前 1000 名网站中，超过 25% 都使用 Nginx 来处理海量的互联网请求。

Nginx 性能极高，Nginx 先天的事件驱动型设计、全异步的网络 I/O 处理机制、极少的进程间切换以及许多优化设计，都使得 Nginx 天生善于处理高并发压力下的互联网请求。Nginx 的稳定性也在各大网站得到验证。官方提供的常用模块都非常稳定，每个 worker 进程相对独立，master 进程在 1 个 worker 进程出错时可以快速“拉起”新的 worker 子进程提供服务。支持热部署，可以不停机更新配置文件、更新日志文件、更新服务器程序版本。

Nginx 的设计极具扩展性，它完全是由多个不同功能、不同层次、不同类型且耦合度极低的模块组成。因此，当对某一个模块修复 Bug 或进行升级时，可以专注于模块自身，无须在意其他。

Nginx 使用最自由的 BSD 许可协议，允许用户在自己的项目中直接使用或修改 Nginx 源码，有大量的插件可以利用。但是，Nginx 模块需要用 C 开发，而且必须符合一系列复杂的规则。虽然通过第三方模块，可以支持 Nginx 与 Perl、Lua 等脚本语言集成工作，但对使用者的要求还是很高。

Nginx 可以说是一款能够工业化 API 网关，在国内的很多互联网公司，例如阿里、新浪等都得到很好的应用。

Spring Cloud Zuul

Zuul Netflix 公司开源的一个 API 网关组件。提供了认证 & 鉴权、限流、动态路由，监控，弹性，安全、负载均衡、协助单点压测、静态响应等边缘服务的框架。

Zuul 的基本功能：

验证与安全保障: 识别面向各类资源的验证要求并拒绝那些与要求不符的请求。

审查与监控: 在边缘位置追踪有意义数据及统计结果，从而为我们带来准确的生产状态结论。

动态路由: 以动态方式根据需要将请求路由至不同后端集群处。

压力测试: 逐渐增加指向集群的负载流量，从而计算性能水平。

负载分配: 为每一种负载类型分配对应容量，并弃用超出限定值的请求。

静态响应处理: 在边缘位置直接建立部分响应，从而避免其流入内部集群。

Netflix 公司还利用 Zuul 的功能通过金丝雀版本实现精确路由与压力测试。

虽然提供的功能还算丰富，但都比较弱，很难满足高要求的场景。

Zuul 处理每个请求的方式是针对每个请求是用一个线程来处理。通常情况下，为了提高性能，所有请求会被放到处理队列中，从线程池中选取空闲线程来处理该请求。2016 年底，Netflix 将它们的网关服务 Zuul 进行了升级，全新的 Zuul 2 将 HTTP 请求的处理方式从同步变成了异步，以提升其处理性能。除了 Netflix 公司，目前 Zuul 在企业中用的还比较少，性能和稳定性方面还有待进一步观察。

从 Zuul 的架构图上可以看出，Zuul 更像是一个过滤器框架，其自身的路由、日志、反向代理、ddos 预防等功能都是通过过滤器实现的。提供了 PRE、ROUTING、POST 和 ERROR 四个扩展点，可以很容易的添加自定义的过滤器。

Zuul 的搭建非常简便，使用和配置也很简单。Zuul 的开源社区比较活跃，一直在更新状态，但版本不算太稳定，在使用的过程中，还有一些坑要踩。例如重定向问题、异常处理问题，还没有解决的很好，需要自己重写一些 filter。

如果从通盘考虑， 这种方案不是最佳方案。但如果自己的团队对整体技术设施把控有限，且团队规模不大，没有专门的网关开发人员的情况下，Zuul 是一款快速上手的最佳方案。

Mashape Kong

Kong 是 Mashape 提供的一款 API 管理软件，它本身是基于 Ngnix+Lua 的，但比 Nginx 提供了更简单的配置方式，数据采用了 Apache Cassandra/PostgreSQL 存储，并且提供了一些优秀的插件，比如验证，日志，调用频次限制等。

Kong 的一个非常诱人的地方就是提供了大量的插件来扩展应用，通过设置不同的插件可以为服务提供各种增强的功能。Kong 默认插件插件包括：

身份认证：Kong 提供了 Basic Authentication、Key authentication、OAuth2.0 authentication、HMAC authentication、JWT、LDAP authentication 认证实现。

安全：ACL（访问控制）、CORS（跨域资源共享）、动态 SSL、IP 限制、爬虫检测实现。

流量控制：请求限流（基于请求计数限流）、上游响应限流（根据 upstream 响应计数限流）、请求大小限制。限流支持本地、Redis 和集群限流模式。

分析监控：Galileo（记录请求和响应数据，实现 API 分析）、Datadog（记录 API Metric 如请求次数、请求大小、响应状态和延迟，可视化 API Metric）、Runscope（记录请求和响应数据，实现 API 性能测试和监控）。

转换：请求转换、响应转换

Kong 本身也是基于 Nginx 的，所以在性能和稳定性上都没有问题。Kong 作为一款商业软件，在 Nginx 上做了很扩展工作，而且还有很多付费的商业插件。Kong 本身也有付费的企业版，其中包括技术支持、使用培训服务以及 API 分析插件。。

三、项目研发内容

Boss直聘API网关是一个服务器，是系统的唯一入口。API网关封装了系统内部架构，屏蔽了系统内部细节。具有负载均衡、动态路由、接口聚合、流量控制、服务预热、身份验证、数据加密、黑白名单、监控告警等功能。客户端通过API网关统一访问后端服务，实现业务功能。

四、总体实施方案

4.1 确定方向目标

经过公司内部流程，与管理层达成一致，明确Boss直聘API网关项目的总体方向，并确立项目目标，为项目启动奠定良好开局，获得公司综合资源调用的许可。

4.2 成立项目组挑选成员

成立Boss直聘API网关研发项目组，挑选包括：项目经理，需求分析师，研发工程师，需求分析师，研发工程师，测试工程师，数据智能架构师在内的各岗位成员，为项目开发配备精兵强将，确保项目启动后各类专业人才高效推进项目实现。

4.3 实施项目研发

严格按照项目开发的流程有序开展研发工作，项目组制定定期规范，和项目流程，实行项目阶段验收和过程监督总结模式，双管其下，保证项目的顺利推进。  
 通过需求分析师深入沟通，理清项目需求，挖掘潜在需求，形成需求文档，在通过需求分析师和项目技术负责人深入沟通，明确需求方案的可实施性及给出明确的实施方案，备份成技术文档；组建开发团队，明确分工，责任到位，并形成项目进度表文件，实时跟进；待项目开发接近尾声，立即组建测试团队，制定周密的测试计划，按计划进行单元测试、性能测试、压力测试、联合测试、回归测试等，确保可稳定运行后可初步交付验收。

4.4 系统的持续改进

本项目的具体研发目标本身需制定明确的边界，经过系统测试、实地试用等来确定目标的达成。但另一方面，研发目标的达成并不意味着本项目所形成的应用系统的终止而是需要通过后续不断的实际应用的检验，找出不足，实现持续改进。因此需要从研发之初就注重其系统工程化、文档完整性和螺旋式上升的生命周期。

五、技术路线、功能和特点

J2EE架构

以下组件通常使用框架提供实现：

1.DisPatcherServlet：前端控制器（不需要程序员开发）

用户请求到达前端控制器，它相当于MVC模式中的C（Controller），DispatcherServlet是整个流程控制的中心，由它调用其它组件处理用户的请求，DispatcherServlet的存在降低了组件之间的耦合性。

作用：作为接受请求，相应结果，相当于转发器，中央处理器，减少其他组件之间的耦合度。

2.HandlerMapping：处理器映射器（不需要程序员开发）

HandlerMapping负责根据用户请求找到Handler（即：处理器），SpringMVC提供了不同的映射器实现实现不同的映射方式，例如：配置文件方式、实现接口方式、注解方式等。

作用：根据请求的Url 查找Handler

3.HandLer：处理器（需要程序员开发）

Handler是继DispatcherServlet前端控制器的后端控制器，在DispatcherServlet的控制下，Handler对具体的用户请求进行处理。

由于Handler设计到具体的用户业务请求，所以一般情况需要程序员根据业务需求开发Handler。

注意：编写Handler时按照HandlerAdpter的要求去做，这样才可以去正确执行Handler。

4.HandlerAdapter：处理器适配器

通过HandlerAdapter对处理器进行执行，这是适配器模式的应用，通过扩展适配器可以对更多类型的处理器进行执行。

作用：按照特定的规则（HandlerAdapter要求的规则）去执行Handler

5.ViewResolver：视图解析器（不需要程序员开发）

ViewResolver负责将处理结果生成View视图，ViewResolver首先根据逻辑视图名解析成物理视图名，即具体的页面地址，再生 成View视图对象，最后对View进行渲染将处理结果通过页面的展示给用户。SpringMVC框架提供了很多View视图类型，包 括：JSTLView、freemarkerView、pdfView等等.

作用：进行视图解析，根据逻辑视图名解析成真正的视图（view）。

6.View视图 （需要程序员开发 jsp）

View是一个接口，实现类支持不同的View类型（jsp、freemarker、pdf）

一般情况下需要通过页面标签或者页面模板技术将模型数据通过页面展示给用户，需要由程序员根据业务需求开发具体的页面。

六、进度安排

整个项目计划工期自2019年1月至2019年12月

详细计划工期如下：

阶段一：2019年1月-2019年3月

请求鉴权、响应加密、负载均衡、健康监测、故障转移、动态路由

阶段二；2019年3月-2019年6月

多云负载均衡、URL Rewrite、接口聚合、管理后台

阶段三：2019年6月-2019年7月

加密性能优化、IP&ID黑灰名单、报警策略优

阶段四：2019年7月-2019年9月

编码协商、反爬虫、反垃圾

阶段五：2019年9月-2019年12月

Dubbo优化性能、JNI编码、线程模型优化

七、研发的风险论证

本公司实施该项目的风险主要体现在以下几个方面：

经费不足风险

市场风险

协作风险

人员风险

（1）开发人员的水平如何。

（2）开发人员在[技术](http://www.itjj.net/IT/jishu/" \t "_blank)上是否配套。

（3）开发人员的数量如何。

（4）开发人员是否能够自始至终地参加软件开发工作。

（5）开发人员是否能够集中全部精力投入软件开发工作。

（6）开发人员对自己的工作是否有正确的期望。

（7）开发人员是否接受过必要的培训。

（8）开发人员的流动是否能够保证工作的连续性

八、项目预算说明

经计算，项目预计总经费 135 万元。（详见研发项目预算表）

九、项目实施的组织管理措施

9.1 研发项目组织管理实施方式

（1）制定立项报告；

（2）对项目投入进行核算，编写预算计划；

（3）组成课题研究小组，对项目组成员进行分工，并配备相应的研发专用设施及设备；

（4）对项目进行严格的管理，对研发人员进行严格的绩效考核；

（5）执行严格的研发流程：

（6）项目负责人进行阶段性审查，项目完成后组织专家组进行审核。

9.2 保障措施

1)技术保障：公司的员工通常拥有专科以上学历，以及在国内外知名企业的工作经验，其对相关自动化产品认识深刻，具有不同下游应用行业自动化方案的制定经验。公司建立了完善的培训机制，包括外部培训和内部培训。公司定期聘请国际知名企业进行外部培训。另外，公司结合已完成的项目，建立了关键工业模块化库以作为资源共享库，为技术工程师的学习和交流提供了平台。

2)人员保证：拥有一支高素质的技术人才队伍，大多来自科研院所和大型企业的技术骨干，他们不仅有很强的技术能力，而且具有丰富的现场经验，雄厚的工程实力，这是公司蓬勃发展的坚实后盾。其中工程技术人员具备丰富理论知识和实践经验，可有针对性的为广大客户提供各种技术培训和服务，并能及时将最新的产品信息和最新的技术传递到客户手中。

为了确保项目实施按时、按质完成，我公司成立了项目工程组，由各领导组成领导指挥小组，由专家、骨干和技术人员组成实施团队，在中心的统一领导下，开展各项工作。

3)资金保证：财务部门做好经费的及时划转，做好资金使用的核算与监管，确保项目的顺利实施。

十、可行性论证

10.1 产品的市场分析

API Gateway，是出现在系统边界上的一个面向API的、串行集中式的强管控服务，这里的边界是企业IT系统的边界，可以理解为企业级应用防火墙，主要起到隔离外部访问与内部系统的作用。在微服务概念的流行之前，API网关就已经诞生了，例如银行、证券等领域常见的前置机系统，它也是解决访问认证、报文转换、访问统计等问题的。

10.2 研发条件分析

熟悉应用领域的业务，能分析用户的需求和约束条件，写出信息系统需求规格说明书，制定项目开发计划，协调信息系统开发与运行所涉及的各类人员，能指导制定数据规划，组织开发信息系统，能评估和选用适宜的开发方法和工具，能按照标准规范写系统分析、设计文档，能对开发过程进行质量控制与进度控制，能具体指导项目开发，具有高级工程师的实际工作能力和业务水平。

**综上所述，项目是可行的。**