

---

# 宜昌市政务网服务器负载

## 整体解决方案

2013-11-14

---

## 目录

第一章	宜昌市政府业务系统概述.....	3
1.1	宜昌市政府业务系统的发展状况.....	3
1.2	需求分析.....	3
第二章	网络方案设计.....	5
2.1	宜昌市政务网络拓扑（局部）.....	5
第三章	ADC 实现服务器负载.....	6
3.1	负载分担算法.....	7
3.2	健康检查策略.....	8
3.3	会话保持策略.....	9
3.1	七层内容交换.....	12
第四章	ADC 针对应用优化与加速.....	13
4.1	SSL 硬件加速和卸载.....	13
4.2	本地 RAM Cache.....	14
4.3	内容压缩.....	14
4.4	TCP 连接复用.....	14
4.5	TCP 单边加速.....	15
4.6	HTTP 管线（Pipelining）.....	16
4.7	窄带用户应用加速.....	17
4.8	重写 Rewrite.....	17
第五章	产品选型及资料.....	18
5.1	产品选型.....	18
5.2	产品配置表.....	18

---

# 第一章 宜昌市政府业务系统概述

## 1.1 宜昌市政府业务系统的发展状况

随着宜昌市政府信息化、工业化、城市化的融合，宜昌市政府已经形成了OA、电子签章、门户网站等信息化平台的建设。随着政务公开工作不断展开，政府门户网站的访问人数不断上升，复杂程度越来越高，信息化规模越来越大，用户对信息平台访问也越来越多，信息系统的性能、稳定性的问题逐渐暴露出来。不断购置性能更高的服务器显然不切实际，因为单台硬件性能毕竟提升有限，终究无法满足大量用户访问对性能的要求。此外，单台服务器也很容易造成单点故障，一旦出现故障，应用系统访问将彻底中断。直接影响宜昌市政府业务系统的稳定性。

通过配置应用交付产品可以有效减轻系统负担，确保系统稳定性，提升工作效率。

## 1.2 需求分析

目前在宜昌市政府网络中存在如下问题：

- ◆ **服务器冗余，考虑到目前系统中主要应用服务器是单台部署，未来可能有多台WEB服务器需要实现负载均衡，为保证用户访问流量能在各个服务器上均衡分配，提高服务器资源的利用率，并当某台服务器发生故障能及时检测到，并且故障服务器会自动隔离，直到其恢复正常后自动加入服务器，实现**

---

**透明的容错，保证服务器整体性能得到大幅提升；**

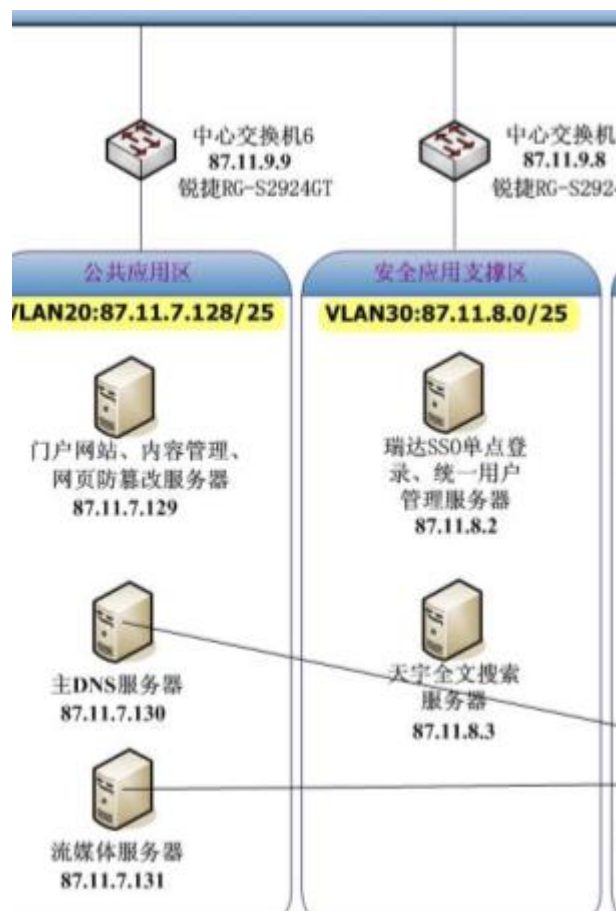
- ◆ **提高服务器性能，提供业务响应时间，可以配合专业优化设备，提供 SSL 卸载、WEB 压缩、缓存等功能；**
- ◆ **当出现大量用户访问时，系统承载能力不足，导致访问系统缓慢；**

以上问题需要我们在本次改造中彻底解决，需要我们部署服务器负载均衡设备，实现如下功能：

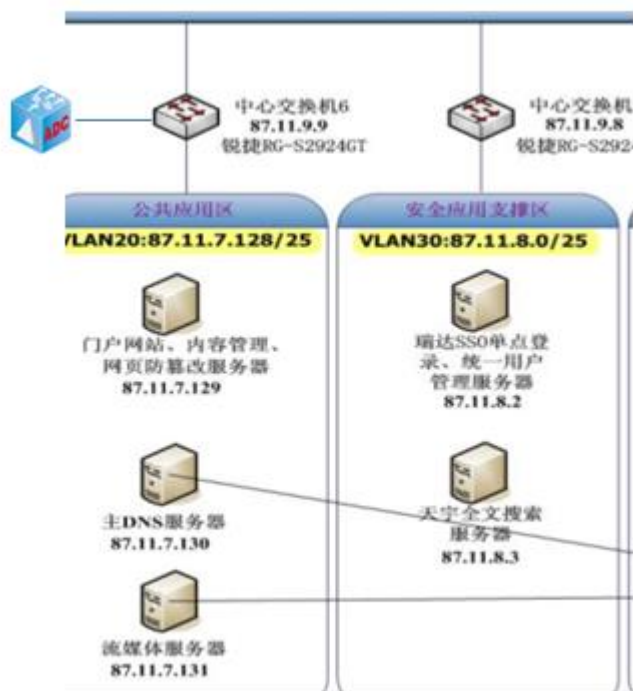
- 1、服务器应用加速，开启WEB缓存功能，外部用户访问内部服务器中静态页面、图片等内容通过应用交付产品缓存下来，不需要访问服务器。开启TCP连接复用功能，外网用户访问内部服务器不需要建立额外的TCP连接，有效减轻服务器负担，提升服务器业务性能。
- 2、通过对服务器的健康检查策略，可以保证每台服务器都可以正常工作，一旦出现异常，负载均衡设备可以迅速检测到故障，并将流量切换到其他服务器上。

## 第二章 网络方案设计

### 2.1 宜昌市政务网络拓扑（局部）



如上图所示，我们的网络部署方案是：



在负载均衡器旁路方式部署在核心交换机上，对应用系统做负载均衡。用户访问ADC的虚拟服务IP的数据流量会自动转发到内部服务器上。两台ADC设备做主备部署，保障平台高可用性，其中一台出现故障，会自动切换到另外一台负载均衡器上。

### 第三章 ADC 实现服务器负载

应用交付，指应用交付网络（Application Delivery Networking，简称AND），利用相应的网络优化/加速设备，确保用户的业务能够快速、安全可靠的交付给客户端。与传统负载均衡产品相比，应用交付除了可以扩展性能，提供冗余保障外，还可以提供各种应用加速特性。

无论是解决出口访问互联网链路拥塞造成的缓慢，还是访问业务本身的响应慢，都可以通过应用交付产品来解决。

---

**简而言之：应用交付产品主要是为了解决各种访问“慢”的问题；**

ADC 在设备上建立一个或多个虚拟服务 VS (IP: Port) , 来映射内部的服务器组来对外提供的一种或者多种应用。内部服务器被加入到地址池中 (Pool) , 当有外部流量访问 VS 时, ADC 通过预先配置好的**负载分担算法**, 从地址池中选择一台可用的服务器作为应用提供者。同时 ADC 实时对每个服务器节点进行**健康检查**, 当某一台出现故障无法正常提供服务时, 将该服务器从 Pool 中的可用列表移出, 不再向其分发流量。

### 3.1 负载分担算法

ADC 应用交付平台支持丰富的负载分担策略, 即可以根据预先配置的静态算法, 也可以根据当前的运行状态进行动态算法的负载分担。

静态算法包括:

- **轮询 (Round Robin)** -依次按照顺序把流量分配给每台服务器。
- **比率 (Ratio)** -根据服务器的性能为每个服务器指定一个权值, 按照这个比率给服务器分配流量。
- **优先级 (Priority)** -当使用多组服务器时, 为每个服务器组指定一个优先级, 默认情况下优先向高优先级的服务器组分配流量, 当该组服务器失效时选择备份服务器组。

动态算法包括:

- **最小连接 (Least Connection)** -ADC 优先把流量分配给当前连接数最少的服务器。

- 
- **最快模式 (Fastest)** -ADC 通过比对服务器返回数据包的延迟情况, 选择一个当前响应最快的服务器来分配流量。
  - **SNMP 监控**-设备上通过 SNMP 客户端来读取服务器的实时运行状态, 包括 CPU, 内存和 I/O 信息, 为每种实时信息配置门限值, 当超过这个门限值时不再向这台服务器分配报文。
  - **观察模式 (Observed)** -结合最小连接和最快模式两种结果, 选择最佳平衡为依据为新的请求选择服务器。

### 3.2 健康检查策略

健康检查是指对服务器的运行状态定期进行实时检测, 一旦发现服务器故障, 将该服务器移出流量分担的队列。ADC 应用交付平台提供丰富的健康检查策略, 和负载分担算法组合到一起, 就可以实现非常灵活的负载分担策略。

- **TCP SYN**-向目标服务器发送 TCP SYN 报文, 如果得到正确的回复表示服务器工作正常。
- **Ping**-向目标服务器发送 ICMP 请求报文, 如果得到正确回复表示服务器工作正常。
- **HTTP/HTTPS Get**-向目标系统发送 HTTP 或 HTTPS 协议的 Get 报文, 请求一个指定的 URL, 如果得到正确回复表示服务器工作正常。

---

### 3.3 会话保持策略

会话保持是指流量一旦按照负载分担策略分配给某个服务器后，后续的相关请求报文同样分配给同一台服务器，以保障业务的连续性。比如，很多电子商务相关的应用系统或者需要用户身份认证的系统，用户和服务器间会进行多次的数据交互才能完成一笔交易或者身份认证过程，必须把这个过程的交互报文分配给同一个服务器。

ADC 应用交付平台支持 6 类共 8 种会话保持的方法，即可以根据源 IP 地址，ServerID 等静态信息来做会话保持，也可以通过 Cookie 插入和重写来实现更高级的会话保持方法。每种会话保持的效率，粒度和应用场景有所不同，对应用服务器的配置要求也不一样。基于源 IP 的会话保持只需要处理数据包的四层信息，所以效率最高，也不需要服务器做任何配置，但粒度比较粗。如果客户端存在普遍的 NAT 转换，或者某些 IP 段的业务请求量比较大，那么这些流量被保持发送给固定一台服务器，就会造成流量负载的不均衡。

基于 Cookie 插入，Cookie 重写，ServerID 等七层信息的会话保持方式，使保持策略和浏览器的信息相互关联，可以做到细粒度和更均衡的流量分配，基于七层信息的会话保持方式，工作效率不如源 IP 会话保持。除 Cookie 插入方式以外，其他如 serverid, sessionid, Cookie 重写等方式一般需要应用程序做相应的配置。

ADC 支持的会话保持方式：

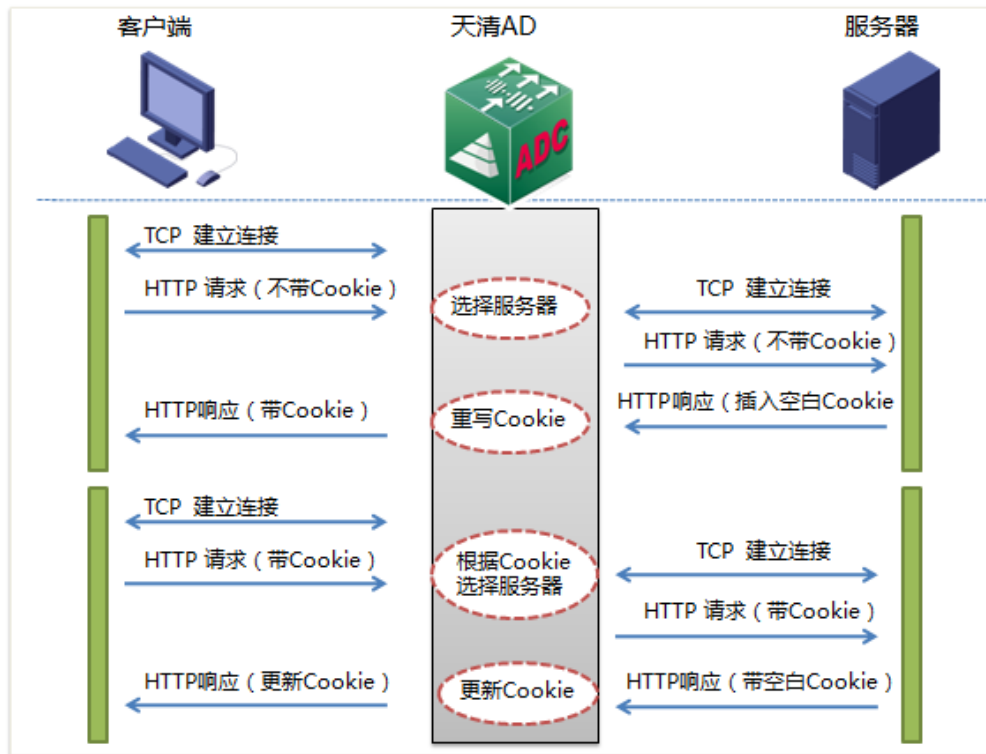
- **基于源地址**-来自同一个源 IP 地址的相关报文，分配给同一个服务器。
- **基于 ServerID**-记录服务器返回的 serverid 信息，然后从请求报文的 URL 或 Cookie 信息中查找 serverid，进行解码得到后台服务器的信息，保证带有固定 serverid 信息的请求被分别到固定的服务器。Serverid 需要在 web 服务器上进行人工配置。ADC 不需要对数据包进行修改
- **基于 SessionID**-类似于 ServerID 的方式，记录从服务器返回的 SessionID 信息，然后从请求报文的 URL 或 Cookie 信息中查找 SessionID，进行解码得到后台服务器的信息，保证带有固定 SessionID 信息的请求被分别到固定的服务

器。SessionID 是服务器自动生成的，ADC 产品不需要对数据包进行修改。

- **基于 Cookie 插入**-这种方式通过修改服务器返回的报文，向其插入一个固定的 Cookie 信息返回给客户的浏览器，客户端后续的报文请求中都携带了这个 Cookie 信息，ADC 根据这个信息发送给指定的服务器。这种保持方式修改了数据包的长度，但不需要应用服务器端做任何的配置改动就可以实现。



- **基于 Cookie 重写**-服务器端接收到 HTTP 请求后，响应报文中会增加一个空白的 Cookie 返回给 ADC 设备，ADC 在这个空白的 Cookie 里面写入会话保持的数值，返回给客户端。后续的过程和 Cookie 插入类似，客户端后续的请求报文会携带这个重写的 Cookie，ADC 根据这个信息来选择指定的服务器。Cookie 重写和 Cookie 插入的区别是，Cookie 重写不需要修改报文的长度，效率会高一些。



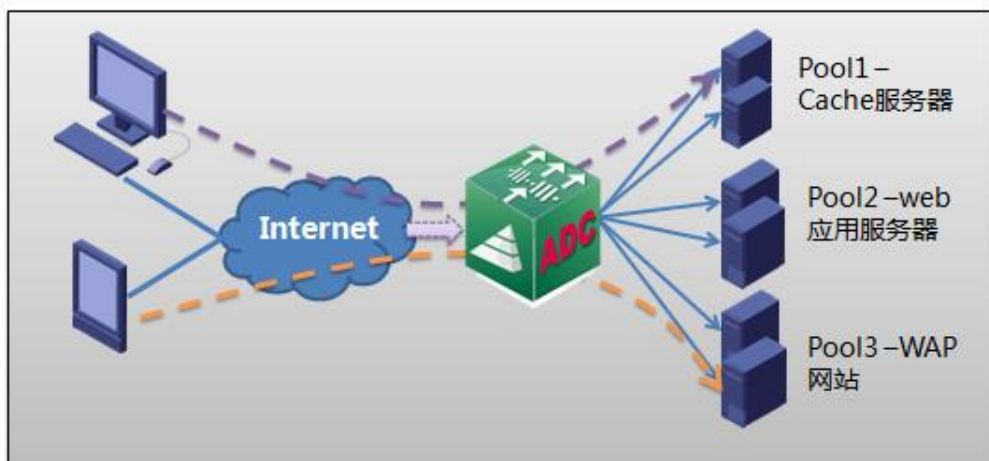
- 基于自定义头部**-应用服务自身定义了一个 URL Header 信息，并希望 ADC 以此来负载分担。这种方式下 ADC 设备记录服务器返回的 Header 信息，并在客户端的后续请求中进行匹配，匹配成功则转发给指定的服务器。这种方式允许应用服务程序定制自己的会话保持策略。
- 基于 SSL SessionID**-当第一次请求到来时，按负载均衡算法分配一台后台服务器。在服务器的响应中，按照 SSL 协议，取出 SSL SessionID，并把 SSL SessionID 分配的后台服务器信息、所配置的超时时间存在一张表中。当后续请求到来，根据请求中的 SSL SessionID 在表中查找后台服务器的信息，若找到并且时间在超时时间之内，则取出后台服务器信息，并更新超时时间，把请求发往那台服务器。

### 3.1 七层内容交换

四层交换主要是依赖 IP 和 TCP/UDP 层的信息进行流量的分配，而随着应用自身的复杂性和不断改善用户体验的需求，有时候需要为不同的用户类型返回不同的呈现内容，例如：

- 把移动用户的手机/pad 浏览器请求分发给专门经针对性过优化的服务器。
- 把请求图片，文档，视频等静态内容分发给缓存服务器。
- 根据浏览器自身的语言设置，为不同语言区域的用户返回相应的页面
- 可以根据 HTTP 请求的方法实现读写分离，HTTP 读 (get) 请求分配给缓存服务器，HTTP 写 (post) 请求分配给处理动态内容的服务器。

ADC 应用交付平台的七层内容交换可以识别用户请求报文的内容，如 URL 信息，应用数据类型，Cookie 信息，浏览器类型，HTTP 方法等内容，将流量分配给相应的应用服务器。

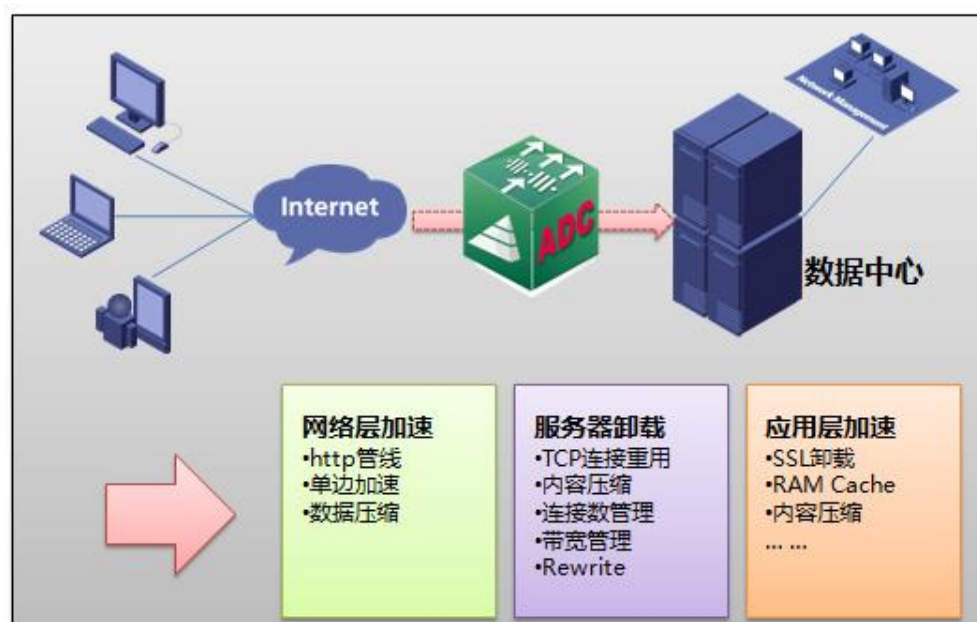


ADC 应用交付平台通过 http-class 来标识一个业务分类，http-class 根据主机地址，URI 路径，头信息和 Cookie 来定义，每个 http-class 可以关联一个服务器地址池，然后在虚拟服务 (VS) 的配置中，引用一个或者多个 http-class。当客户端

请求访问虚拟服务时，ADC 设备进行 http-class 匹配，匹配成功的请求被分配给对应的地址池。

## 第四章 ADC 针对应用优化与加速

ADC 应用交付平台可以把原本需要高消耗服务器计算能力的，重复计算的工作卸载到高性能的硬件平台上，让服务器的计算资源更多的关注自身的业务系统处理，以改善整个应用系统的效率。ADC 同时对 TCP 和 Http 协议进行优化和加速，最大限度的降低网络拥塞和丢包，改善移动上网等窄带用户的用户体验。



ADC 应用交付平台内置了企业最常用的应用模板，如 BEA Weblogic, Microsoft IIS, Outlook Web Access, Radius, ERP 软件等，这些都是经过公司应用优化专家通过反复的测试验证而完成的一套解决方案，管理员不需要对应用进行细致的了解，就可以根据模板高效的完成这些应用系统的优化和加速。

### 4.1 SSL 硬件加速和卸载

ADC 应用交付平台通过内置的专业级高性能硬件加速芯片，完成对 SSL 协议的加速和卸载，而在数据中心内部，ADC 和服务器之间通过明文进行传输，极大的提升服

---

务器的业务处理能力。企业可以把应用全部应用实现 SSL 协议，实现高安全性的同时，不会给业务带来任何的性能瓶颈。

## 4.2 本地 RAM Cache

本地高速缓存 (Cache)，通过在 ADC 设备上开辟一段专用的内存空间 (RAM) 来存储服务器上的一些静态文件，如图片，文档，视频文件等，开启本地 Cache 后，客户端请求首先在本地的 Cache 中查找，命中以后直接返回给客户端。命中失败才向服务器端发送请求，同时对服务器返回的内容进行本地 Cache。ADC 支持为不同的应用提供各自的 Cache 空间及参数设置，这样可以把服务器从重复的处理中解脱出来，提升整体效能。

## 4.3 内容压缩

通过压缩 HTTP 响应的数据，可以有效提升带宽利用率和缩短下载时间。ADC 应用交付平台提供的高性能压缩技术，最大可以使带宽利用率增加 80%，应用性能提升 4 倍以上。同时在客户端浏览器和 ADC 设备间经过一定的算法进行压缩，也起到一定安全传输的作用。

ADC 把原本由服务器完成的压缩过程搬到自身的高性能硬件平台，避免了每台服务器都执行一次重复的压缩过程，达到服务器卸载的效果。

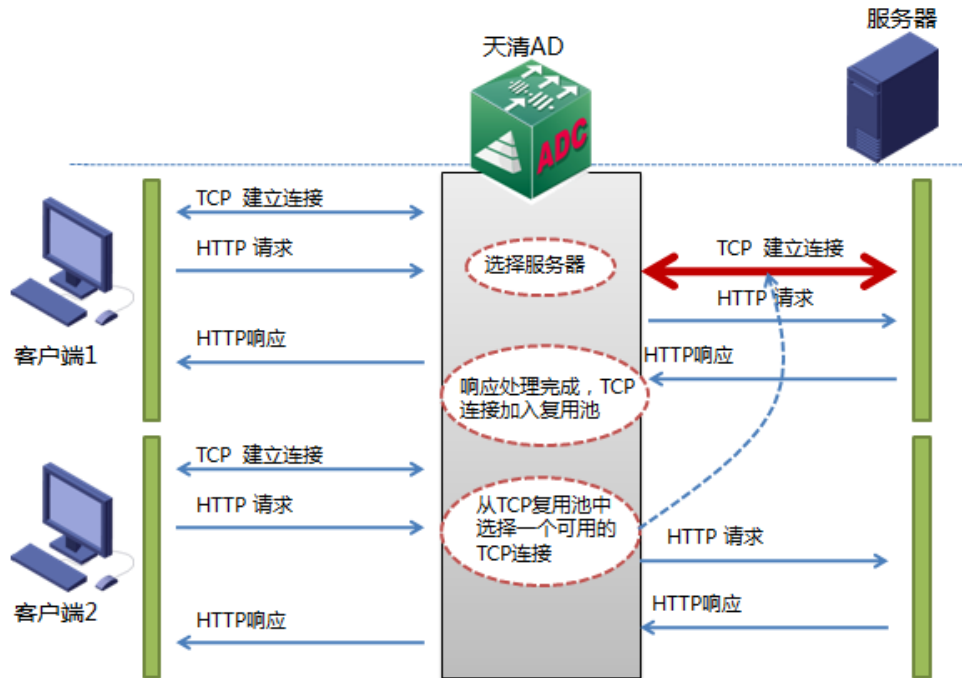
ADC 支持浏览器最常用的 GZIP 和 DEFLATE 两种压缩算法，提供基于七层的精细化压缩控制策略，包括 URI, Content Type 等。管理员可以定义对 “.txt”，“.doc” “.html” 等文档类型和静态页面数据进行压缩，也可以排除 PDF, IMG 等压缩效果不明显的不必要操作。

## 4.4 TCP 连接复用

TCP 连接复用技术使多个客户端共享一个到服务器的 TCP 连接，可以提升应用服务器的整体性能，使应用服务器从维护海量的 TCP 连接，并不断的进行 TCP 建立和拆除维护中解脱出来，极大的提升单台服务器的承载能力。

ADC 设备在接到一个客户端 HTTP 请求后，通过负载分担算法会选择一台服务器建立连接。如果接收到正常的服务器响应，ADC 设备会把这个连接放入到

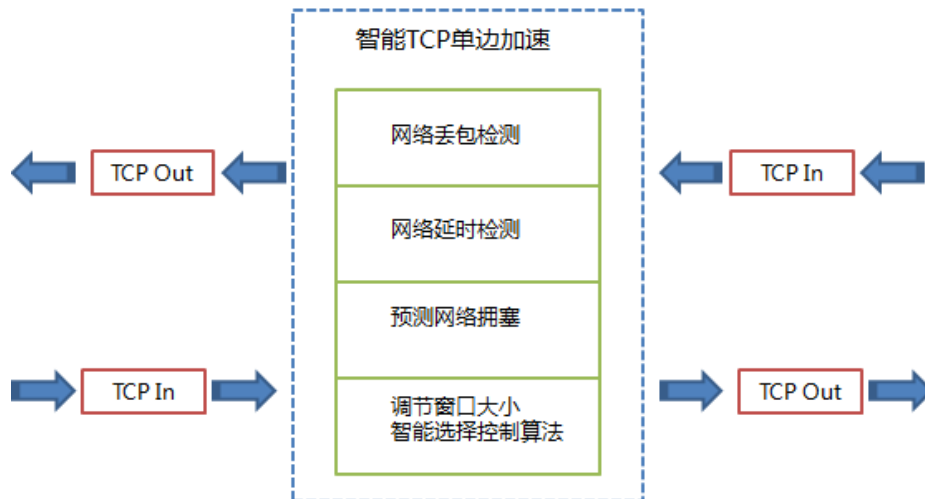
“连接复用池”里面，当另外一个新的客户端发起 HTTP 连接请求时，ADC 设备从现有的连接池里面选择一个可用的连接来和服务器的进行数据交互，而不是重新创建一个到服务器的连接。通过这种优化，可以把服务器负载降低到原来的 1/10-50。



#### 4.5 TCP 单边加速

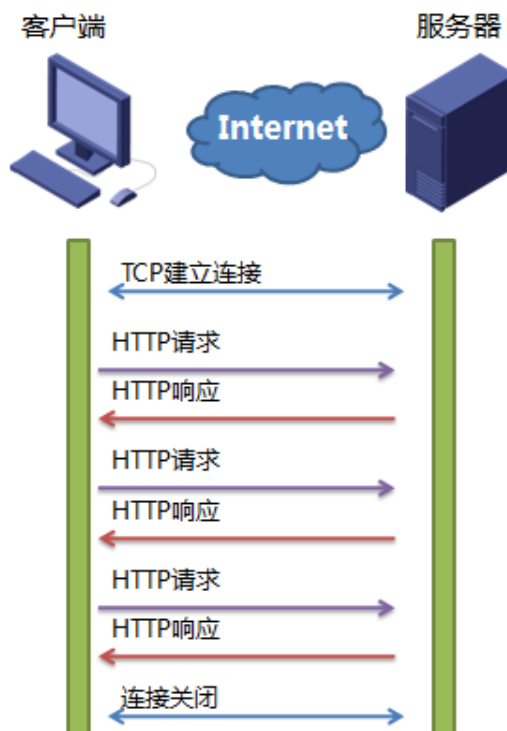
标准 TCP 协议在设计时很少的考虑到高带宽和夸 Internet 传输的问题，现在随着高速带宽的普及，标准的 TCP 协议表现出很多的不足，在网络拥塞控制和丢包重传机制上，往往效率比较低下，而且基本不具备根据网络环境实时进行调整的能力。ADC 应用交付平台提供智能单边加速的功能，通过对标准 TCP 协议的慢启动控制，拥塞避免，重传和恢复几个方面进行优化，来达到整体网络加速的效果。同时，ADC 设备可以根据当前的网络状态，和承载的协议类型智能的选择一种效率最高的算法。

ADC 应用交付平台的单边加速对客户端和服务器来说都是透明的，ADC 和服务器之间仍然按照标准 TCP 协议运行，ADC 和客户端之间进行单边加速，客户端不需要做任何修改。



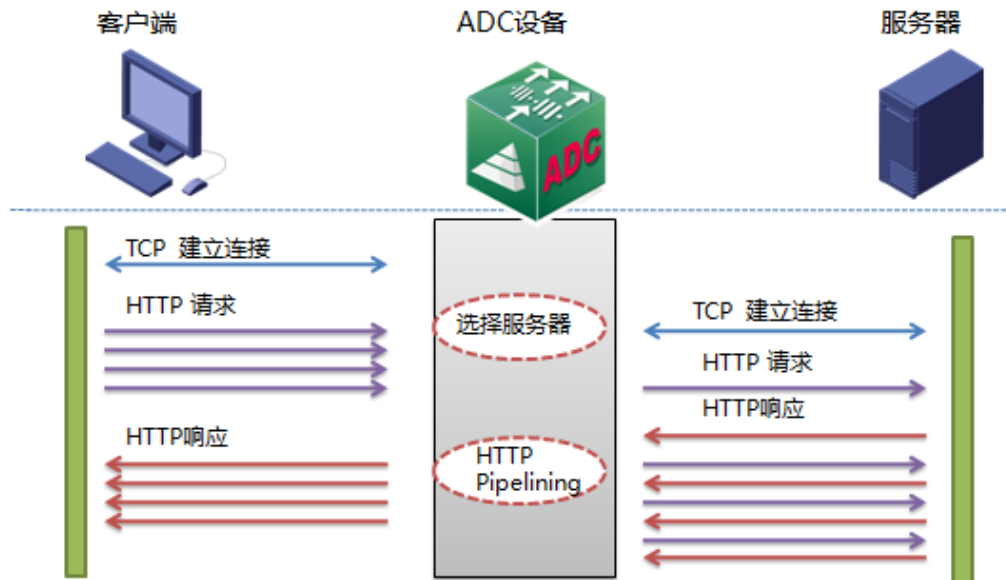
## 4.6 HTTP 管线 (Pipelining)

传统的 HTTP 协议是当一个请求发出，等接收到完整的响应数据后，才进行下一个请求，这在高延迟的网络环境中会导致整个数据交互的效率比较低。HTTP 管线技术 (Pipelining) 可以将多个 HTTP 请求同时提交，而不用等待顺序的请求回应。



(不带 Pipelining 的 HTTP 流程)

ADC 应用交付平台可以和支持 Pipelining 的客户端浏览器智能协商开启，ADC 和服务器间还是正常的 HTTP 协议流程。



#### 4.7 窄带用户应用加速

当客户端通过窄带线路比如通过 ADSL 拨号或者智能手机，pad 移动终端上网时，对于应用服务器的响应，可能会由于客户端侧带宽不足，或者带宽质量不好而导致报文的拥塞和丢包。这时客户端就会发起重传请求，如果大量的窄带用户同时访问，就会出现应用服务器反复处理这些重传请求的压力增大而降低效率。

ADC 应用交付平台使用 TCP 数据缓存技术，自动检测客户端对服务器响应的处理能力，对于窄带用户，ADC 会在自身平台开辟出缓存空间来存储服务器返回的数据，以客户端能够适应的速度完成数据交互，避免出现大量的重传。服务器只要处理完用户的请求后，就可以释放出来处理其他工作，不用再去处理丢包重传的情况。

#### 4.8 重写 Rewrite

Http 协议的请求阶段和响应阶段都可以对 URI 进行重写，在请求 http 请求阶段，可以把符合预置条件的所有 http 请求发送到一个指定的 URL，比如是提示用户进

行登录的页面或者其他信息提示页面。又或者是当服务器某些文件已经不存在或者目录发生更改，而用户通过其他网站或者搜索引擎的旧链接进行访问时，可以把这类请求直接重定向到一个指定的错误信息提示页面，减轻了服务器的负担。

部署了 ADC 应用交付平台以后，企业可以把原来基于 http 协议的应用，全部迁移到安全 https 协议。通过 http 请求重定向结合 SSL 卸载功能，可以实现企业服务器和客户端都不需要任何更改的情况下完成 http 到 https 的无缝迁移。

在 http 响应阶段，可以把服务器返回的 404（客户端语法错误）等重定向到一个指定的页面。

## 第五章 产品选型及资料

### 5.1 产品选型

根据网络及未来业务拓展需求，建议选择吞吐为 1G 的 ADC 产品

### 5.2 产品配置表

#### 产品选型方案：ADC

产品编号	产品名称	产品描述	数量
1	ADC	性能 1Gbps，最大可扩展到 10Gbps。提供服务器负载均衡、LBG 多链路负载均衡（全部功能）、7 层内容交换，应用系统加速，SSL 卸载及加速、网页压缩、高速缓存、TCP 单边加速等功能。1U 上架设备，单电源，1 个管理接口，5 个 10/100/1000M 自适应电口，1 个 ADC-NIM-L 通用扩展插槽，含嵌入式软件。质保期（自硬件产品发货之日起，为期 15 个月）内免费维修。	2

