**一次 DNS 缓存引发的惨案**

<http://blog.jobbole.com/110165/>

时间2015年的某个周六凌晨5点，公司官方的QQ群有用户反馈官网打不开了，但有的用户反馈可以打开，客服爬起来自己用电脑试了一下没有问题，就给客户反馈说，可能是自己网络的问题，请过会在试试。早点8点，越来越多的用户反馈官网无法打开，并且有部分用户开发反馈app也打不开了，客服打电话叫起了还在梦乡中的我。

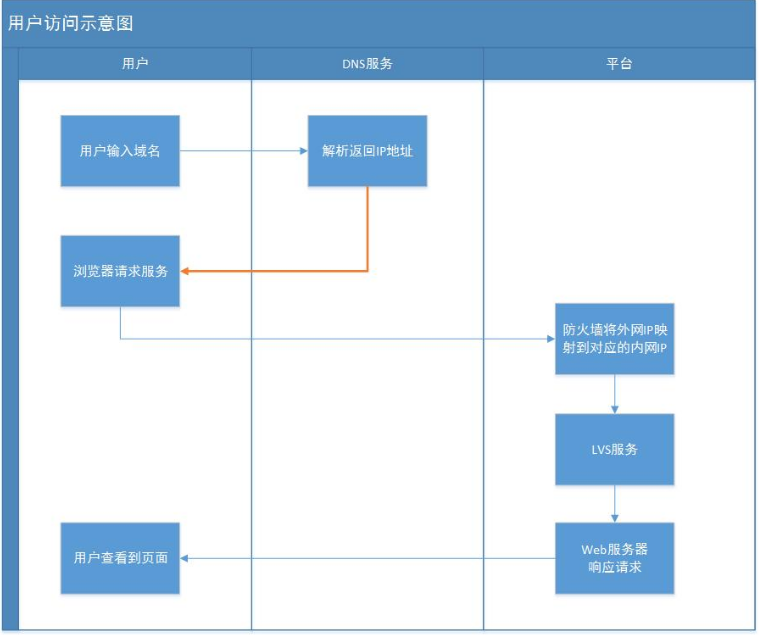
**分析定位**

被客服叫起来之后，一脸懵逼，不知道什么情况，给客服回复，知道了，立刻排查，待会有消息及时沟通。用凉水洗了一把脸清醒了一下，立刻根据经验回忆这两天生产投产的情况：上线了XX模块，不影响、修复了XXbug，应该也不影响、刚给服务器配置了https，看起来好像有点关系，但是app暂时没有投产https，怎么也出现问题，排除之。打开电脑核查了最近的投产记录应该都不至于发生这么严重的问题，随怀疑是不是网络方面有问题，立刻打电话叫起来运维经理以及相关人等一起排查。

一边让网络和运维排除问题，一边再次核查了web服务器、数据库服务器、业务日志、数据库日志，以及其它的一些监控数据，各项皆正常。试着在本机ping了一下域名确实不通，更加怀疑是网络问题，尝试这直接使用外网访问官，可以打开没有问题，可以基本确认服务没有问题，但运维部反馈网络设备什么都正常，肯定是你们投产代码出问题了，各方硬着头皮继续在排查。

9点，群里开始有大规模的用户反馈官网和app都打不开了，更有部分用户煽动，XXX公司跑出了（15年很多p2p公司跑路，导致用户都成了惊弓之鸟，稍微有问题便害怕公司跑路，个个都锻炼成了监控高手，天天看，实时刷，凌晨起来尿尿也都顺便看一下app上的今日收益），客服400热线基本被打爆了。一边继续排查问题，一边上报此问题给总监、公司各高管，给客服建议，给用户解释，IDC机房网络抖动，技术正在紧急解决，资金和数据都没有任何影响，稍安勿躁。

10点，开发和运维反复的检查后，开始怀疑dns解析有问题，但具体是什么问题还不清楚，CTO决定：1、大家都打车往公司走，来公司集体解决 2、在各QQ群、微信群给用户群发解释xxx问题，安抚客户。在车上的时候重新梳理了一下用户的整个访问流程，如下图：



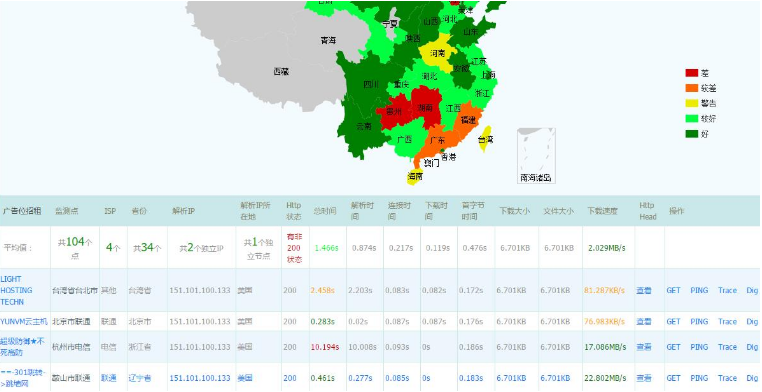
到公司后，根据这个思路大家在一起验证了一下，通过外网IP和内网IP访问公司所有服务都正常，但是通过域名访问不行，另外监控服务器、防火墙、网络设备日志都正常，因此断定是DNS解析出现问题。

**攻坚问题**

既然确实是DNS解析问题，那么问题又来了？为什么DNS解析会出现问题？如何去解决这个问题？一边给万网提工单，我们也自己测试一下电信、移动、联通在不同的网络运营商下面的访问情况，发现只有在联通网络的环境下DNS解析不了。根据客服得到的反馈也验证了这个情况，电信和移动用户反馈很少，联通用户反馈最多。于是我们又开始给联通打电话，刚开始联通不受理我们的这个请求，于是又开始以用户的身份打电话给联通公司让立刻解决不能上网的问题。

于是就开始了万网和联通的扯皮大战，万网说从他们那边查看DNS解析都正常，一起指标都正常，我们又给联通打电话联通说我们已经知道了，待会由专业的人给我们回复，过了一会联通的网络工程师回复说，像这种情况一般都是域名解析的问题。早上10:30到公司开始短短的6各小时内，我们几个轮流给联通公司合计供打了近50、60通电话，给万网提了N个工单，接了N个电话。

期间领导也开始动用各种关系，联通内部的朋友、网络运维界的大拿帮忙来定位解决，我们也尝试了很多的办法，比如，使用ipconfig/flushdns命令清除本机的DNS缓存、在万网的官网把DNS解析重新更新一边、删除在重新添加等等，也不是完全没有收获。我们一直想找一个可以测试各个地方、运营商网络的办法，终于在各方推荐和搜索的情况下找了17ce 和 360奇云测两个网站，感觉非常实用，在以后的网络定位中，成了我必备使用的工具，可以非常方便的监控各个运营商、各个地区网站的访问是否通不通、访问的速度快不快等问题，截图如下：



我们也发现，公司的其它域名也都访问正常，就是官网的这个域名和相关的子域名不通。期间很多人都问了一个问题就是你们的域名有没有忘了缴费，刚开始大家也都问了运维这边说是没有这个问题，直到中午12:30的时候在我们再三的追问下才说8点多的时候登录上万网的时候显示这个域名是欠费状态，但是他已经立刻把费用补了上去了。哎呀差点把我们气死，问了不是域名到期有提示的吗？才知道因为上一个运维经理走后，他们没有及时的更新万网的电话和邮箱导致提示邮件和短信也没有收到。

通过和万网、联通公司、领导的相关朋友沟通以及我们的测试观察，初步明白了这个事情的原因：域名忘记缴费导致万网的DNS解析被停止，用户本机或者DNS服务器有缓存，所以部分用户可以访问部分用户不能访问；缴费过后万网的DNS已经进行了更新和推送，但是DNS解析有很多的层级需要一级一级的往下面发送更新，有的层级并没有更新到，导致部分没有更新到的DNS服务商下面的用户不能访问官网。

和万网进行了沟通，问最延迟的情况所有的DNS更新到最新的时间，回答是48小时内肯定都会好的，但是我们等不起呀，随着时间的推移越来越多的用户发现问题，QQ群、微信群已经沸腾，董事长也开始关注次问题，有的客户直接在群里面说，你们的技术太不给力了(像这种还是委婉的，有的直接打电话骂人)…

**临时解决方案**

不断的通过17ce测试发现，大部分地区的网络都已经恢复，就剩北京联通和部分地区联通网络环境下不通，也说明了这几个地区下的DNS解析记录没有被更新。那么既然我们在上面已经定位出了问题，又了解是什么原因，就想着试着换个DNS解析服务器会不会好一点呢，于是我们把本地的DNS地址换成8.8.8.8（谷歌的DNS服务解析）发现好了！于是赶紧先写解决手册发给着急的客户来使用。

官网的用户可以通过更改DNS来解决访问的问题，APP怎么办呢？没有办法我们也不能等，直接找开发人员把服务端调用的地址由域名暂时先改为外网的IP地址打一个版本供用户临时使用。安卓还比较好办，直接让用户下载安装使用还好，但是IOS那时候的审核最少都需要一周黄花菜都凉了。其实iPhone手机可以单独设置DNS的，我们进行了设置和测试后发现也可以实现，于是马上更新到手册中发送给客服发送到群里面给用户使用。

有人说直接让用户使用外网就行了吗，使用外网首页打开到是没有问题，但是各系统之间调用，相关配置文件里面写的也都是域名的地址，如果硬改的话可能会引发另外的问题。第一天搞完就10点多了，中间就4点吃了一顿饭，打了N个电话大家都非常累，于是当天就先这样了，第二天大家一早到公司继续跟进。

第二天到公司经过17ce测试发现所有的节点都已经通了就剩北京联通的两个接点没响应，但是北京是我们的大本营，绝大部分的用户都是北京的，继续和万网、联通沟通看怎么能彻底的解决这个问题，另一方面做好最坏的打算，如果一直不通怎么办。在生产环境中梳理所有使用域名的配置文件，做好随时可以直接更新为外网地址而不能影响服务，app完整的重新做一个版本，做好随时可以投产让用户强制升级到外网直连的版本。

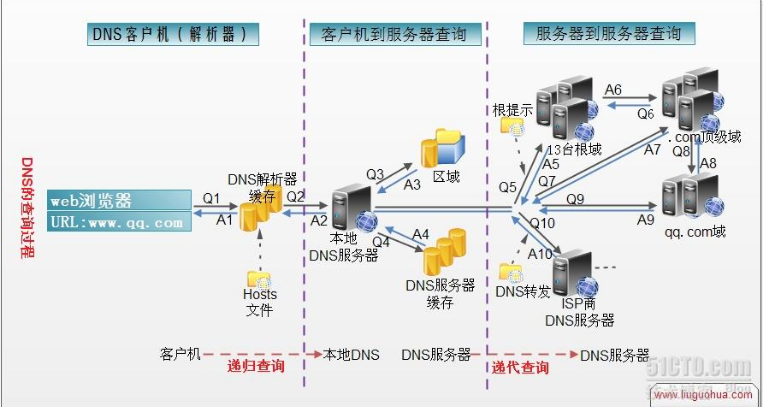
到第二天晚上10点的时候，北京联通的这两个节点还是不通，和领导进行了商议如果到周一早上8点来的时候这两个网络还是不能通的话，就上线改造好的系统和APP强制升级（因为当时周末还没有标的，周内才有发标计划）。第三天早上起来的第一件事情就是拿起手机，查看自己的联通网络是不是可以登录上官网，结果通了！皆大欢喜。

俗话说真理是愈辩愈明，经过了这次事故，也彻底的让我了解了DNS解析的整个过程。

**DNS 解析流程**

DNS( Domain Name System)是“域名系统”的英文缩写，是一种组织成域层次结构的计算机和网络服务命名系统，它用于TCP/IP网络，它所提供的服务是用来将主机名和域名转换为IP地址的工作。俗话说，DNS就是将网址转化为对外的IP地址。

dns从用户访问到响应的整个流程



* 第一步：浏览器将会检查缓存中有没有这个域名对应的解析过的IP地址，如果有该解析过程将会结束。浏览器缓存域名也是有限制的，包括缓存的时间、大小，可以通过TTL属性来设置。
* 第二步：如果用户的浏览器中缓存中没有，操作系统会先检查自己本地的hosts文件是否有这个网址映射关系，如果有，就先调用这个IP地址映射，完成域名解析。
* 第三步：如果hosts里没有这个域名的映射，则查找本地DNS解析器缓存，是否有这个网址映射关系，如果有，直接返回，完成域名解析。
* 第四步：如果hosts与本地DNS解析器缓存都没有相应的网址映射关系，首先会找TCP/IP参数中设置的首选DNS服务器，在此我们叫它本地DNS服务器，此服务器收到查询时，如果要查询的域名，包含在本地配置区域资源中，则返回解析结果给客户机，完成域名解析，此解析具有**权威性**。
* 第五步：如果要查询的域名，不由本地DNS服务器区域解析，但该服务器已缓存了此网址映射关系，则调用这个IP地址映射，完成域名解析，此解析**不具有权威性**。
* 第六步：如果本地DNS服务器本地区域文件与缓存解析都失效，则根据本地DNS服务器的设置（是否设置转发器）进行查询，如果未用转发模式，本地DNS就把请求发至13台根DNS，根DNS服务器收到请求后会判断这个域名(.com)是谁来授权管理，并会返回一个负责该顶级域名服务器的一个IP。本地DNS服务器收到IP信息后，将会联系负责.com域的这台服务器。这台负责.com域的服务器收到请求后，如果自己无法解析，它就会找一个管理.com域的下一级DNS服务器地址给本地DNS服务器。当本地DNS服务器收到这个地址后，就会找域名域服务器，重复上面的动作，进行查询，直至找到域名对应的主机。
* 第七步：如果用的是转发模式，此DNS服务器就会把请求转发至上一级DNS服务器，由上一级服务器进行解析，上一级服务器如果不能解析，或找根DNS或把转请求转至上上级，以此循环。不管是本地DNS服务器用是是转发，还是根提示，最后都是把结果返回给本地DNS服务器，由此DNS服务器再返回给客户机。

这个事情发生后给了我们很大的教训:

第一、流程管理有漏洞，离职交接不到位；

第二、危机处理不成熟，影响公司声誉；

第三、监控机制不完善，像外网不通的这种问题，应该提前设置监控措施。

有时候非常的严重的问题，就是你常常忽略的小不点.