* 常规DNS调度策略原理:

Step 1:客户端（假设IP地址为IP1）向Local DNS（假设IP地址为IP2）发出域名解析请求（假设请求的域名为www.taobao.com）

Step 2:Local DNS代理客户端向权威服务器发起域名解析请求

Step 3：权威服务器根据域名(www.taobao.com)和IP2（对应的地域和ISP）进行调度并返回对应的解析结果。

Step 4: 客户端根据调度返回的IP发起业务访问请求。

* 权威DNS

权威DNS即最终决定域名解析结果的服务器，开发者可以在权威DNS上配置、变更、删除具体域名的对应解析结果信息。阿里云云解析（ https://wanwang.aliyun.com/domain/dns ）即权威DNS服务提供商。

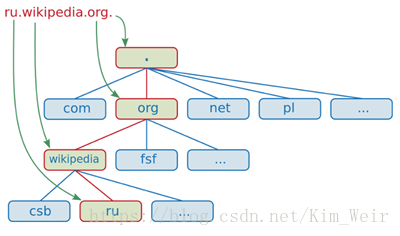
* 递归DNS

递归DNS又称为Local DNS，它没有域名解析结果的决定权，但代理了用户向权威DNS获取域名解析结果的过程。递归DNS上有缓存模块，当目标域名存在缓存解析结果并且TTL未过期时（每个域名都有TTL时间，即有效生存时间，若域名解析结果缓存的时间超过TTL，需要重新向权威DNS获取解析结果），递归DNS会返回缓存结果，否则，递归DNS会一级一级地查询各个层级域名的权威DNS直至获取最终完整域名的解析结果

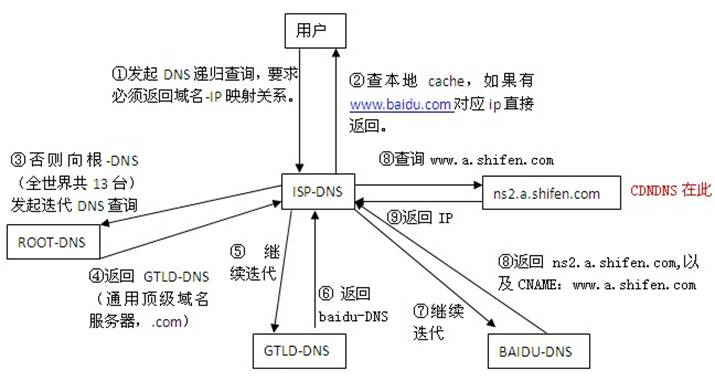
* 公共DNS

公共DNS是递归DNS的一种特例，它是一种全网开放的递归DNS服务，而传统的递归DNS信息一般由运营商分发给用户。一个比较典型的公共DNS即Google的8.8.8.8，我们可以通过在操作系统配置文件中配置公共DNS来代替Local DNS完成域名解析流程。通常不需要手工指定自己的Local DNS地址。运营商会通过DHCP协议在系统网络初始化阶段将Local DNS地址分配给我们的计算机

* DNS域名的层次结构（根域、顶级域、二级域）

   DNS系统一般采用树状结构进行组织，以ru.wikipedia.org为例，org为顶级域名，wikipedia为二级域名，ru为三级域名，域名树状组织结构如下图所示。  
 

[**DNS解析过程**](https://www.cnblogs.com/super86/p/4671253.html)



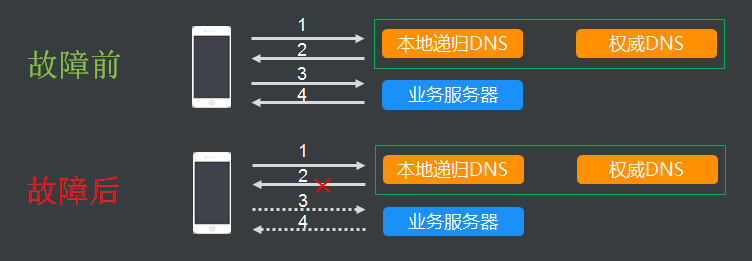
### 当客户的Local DNS与客户的地域和运营商不匹配时，此时按照Local DNS来调度就会出现调度不精确，解析生效滞后延迟大的问题。

（1）国内三大运营商Local DNS布点不足且不均匀，大量流量集中在2000个以内的Local DNS上，大的Local DNS对应的流量超过5Gb

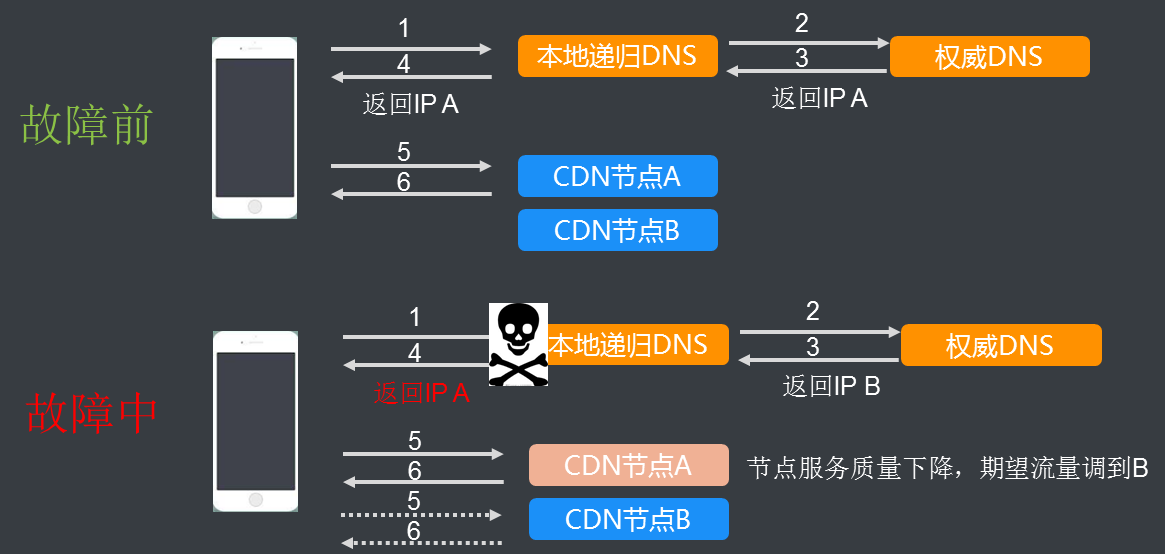
（2）很多手机（尤其是山寨机）Local DNS配置不准确

（3）公共DNS（如google 8.8.8.8，阿里的223.5.5.5,223.6.6.6）导致调度系统无法识别Local DNS的具体位置。

#### 域名解析问题导致访问流量减半



#### 域名解析结果修改不生效导致流量无法迁移

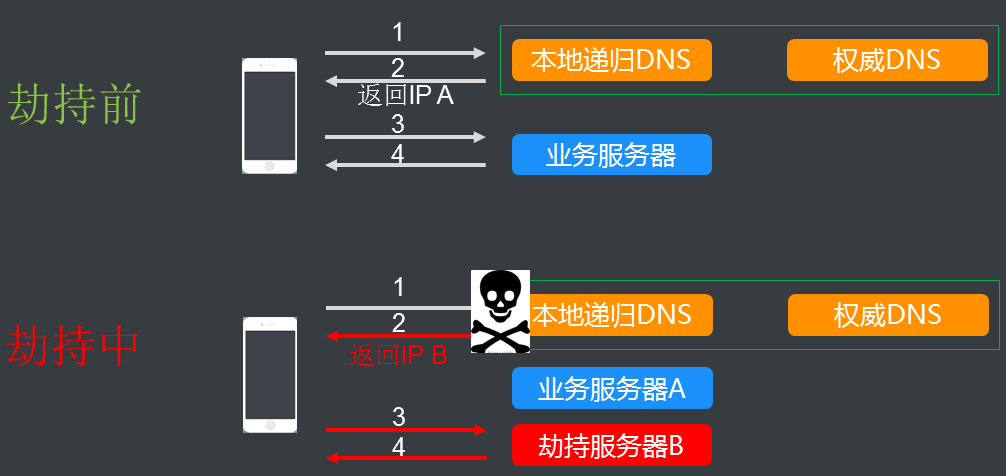


#### 域名劫持问题

现网上DNS解析一般基于UDP来实现，由于UDP自身的脆弱性，很容易被劫持。攻击者可以监听终端用户的域名解析请求，并在Local DNS返回正确结果之前将伪造的DNS解析响应传递给终端用

黑客侵入了宽带路由器并对终端用户的Local DNS进行篡改，指向黑客自己伪造的Local DNS，进而通过控制Local DNS的逻辑返回错误的IP信息进行域名劫持

缓存污染：接收到域名解析请求时，Local DNS首先会查找缓存，如果缓存命中就会直接返回缓存结果。这类缓存污染往往能带来更明显的群体伤害



**数据劫持**基本针对明文传输的内容发生。用户发起HTTP请求，服务器返回页面内容时，经过中间的运营商网络，页面内容被篡改或加塞内容，强行插入弹窗或者广告。解决的办法即是对内容进行HTTPS加密，实现密文传输

网络通信流程图

