链滴

说说 ip 地址被墙和 DNS 污染

作者：shyjiang233
原文链接：https://ld246.com/article/1682439115017
来源网站：链滴

为啥我会突然写这个呢？因为我买的国外服务器两台都连接不上，起初我是想买一台服务器作为代理就不用使用vpn了。结果刚买了一直连接不上服务器,我就查了到底是啥原因。

经过查询，我知道可能是ip被墙了。我通过第三方网站ping试了试

Saudi Arabia, Riyadh	Buzinessware	0%	2	156.9	157.31	156.9	157.72	0.41
UAE, Dubai	Bamboozle	0%	2	85.18	84.93	84.67	85.18	0.26
UAE, Dubai	Buzinessware	0%	2	281.78	281.36	280.94	281.78	0.42
Iran, Tehran	Green Web	0%	2	351.98	352.12	351.98	352.26	0.14
India, Mumbai	Vultr	0%	2	67.56	70.99	67.56	74.42	3.43
India, Bengaluru	Digital Ocean	0%	2	44.41	44.44	44.41	44.48	0.04
Singapore	Digital Ocean	0%	2	7.86	7.9	7.86	7.94	0.04
Japan, Tokyo	Vultr	0%	2	76.48	76.72	76.48	76.95	0.23
Australia, Sydney	Vultr	0%	2	100.36	100.12	99.88	100.36	0.24
Taiwan, Taichung	Google	0%	2	55.89	55.44	54.98	55.89	0.46
China, Shenzhen	Aliyun	100%	2	–	–	–	–	–
China, Guangzhou	Tencent	100%	2	–	–	–	–	–
China, Beijing	Aliyun	100%	2	–	–	–	–	–
China, Beijing	Tencent	100%	2	–	–	–	–	–
China, Jiangsu	China Telecom	100%	2	–	–	–	–	–
China, Jiangsu	China Mobile	100%	2	–	–	–	–	–
China, Jiangsu	China Unicom	100%	2	–	–	–	–	–
China, Hangzhou	Aliyun	100%	2	–	–	–	–	–
China, Qingdao	Aliyun	100%	2	–	–	–	–	–
China, Zhejiang	China Telecom	100%	2	–	–	–	–	–
China, Shanghai	Aliyun	100%	2	–	–	–	–	–
China, Shanghai	Aliyun	100%	2	–	–	–	–	–

就是这样国外可以ping通，但是国内ping不通。可以判断一定是ip地址被墙了。

ip到底怎么被墙？我提出了这个疑问。

我继续查询资料，查找了GFW的主要功能：

连接重置：

当检测到某个 TCP 连接的 IP 包中包含非法关键词时，伪造 RST 包发给 TCP 连接两端，导致连接断。缺点是只对非加密的 TCP 数据有效。优点是维护方便。

对策很简答，使用加密数据传输就可以了。VPN，shadowsocks，SSH 全部是基于这个原理翻墙的如果没有其他的手段做辅助，单单使用 https 就可以绕过。

IP / 端口封锁：

就是 IP 封锁，简单暴力。缺点是 IP 封锁需要部署在骨干路由器上，能够封锁的 IP 数量有限制。优是封锁很彻底。对策是代理服务器，不需要对数据加密就可以绕过 IP 封锁。但是由于连接重置的存，显然还是需要加密。

DNS 污染：

在用户进行某些特定网站的 DNS 查询时，抢先发送伪造的 DNS 结果，导致 DNS 解析到虚假的 IP 址从而阻止用户访问非法资源。

优缺点不明。

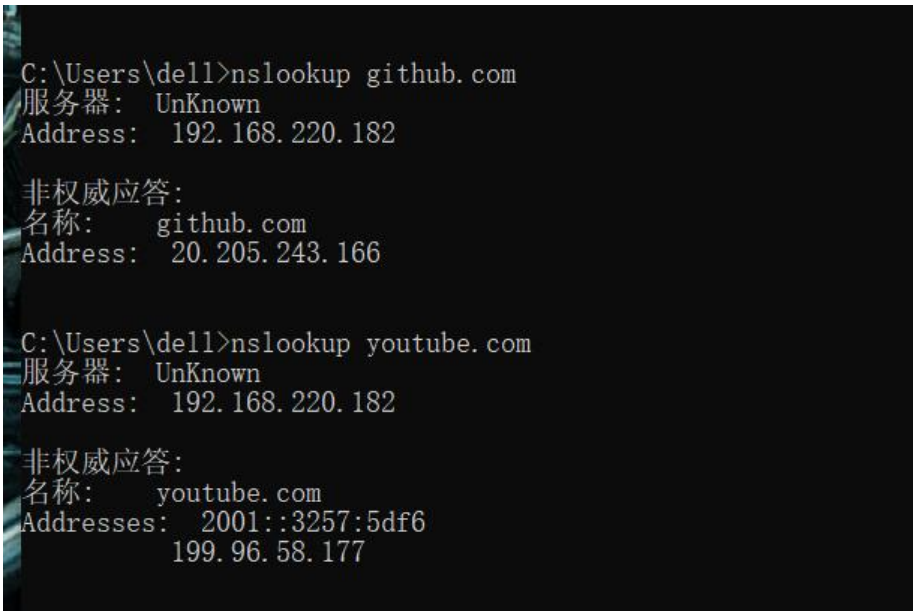
对策是使用境外的代理服务器进行远程 DNS 查询，从而获取到正确的 IP。单纯把 DNS 设置为境外的 DNS 服务器是无效的，因为只要是符合条件的 DNS 查询 UDP 包都会被投毒

Amazon 的云，linode，digitalocean 等国人喜欢用的 VPS，已经被重点照顾，大量 IP 被封。这些 I 应该是被重点照顾的，有时自己新搭建的 VPN 服务器，几天就会被封，期间并没有怎么用。(我使用就是其中一家)

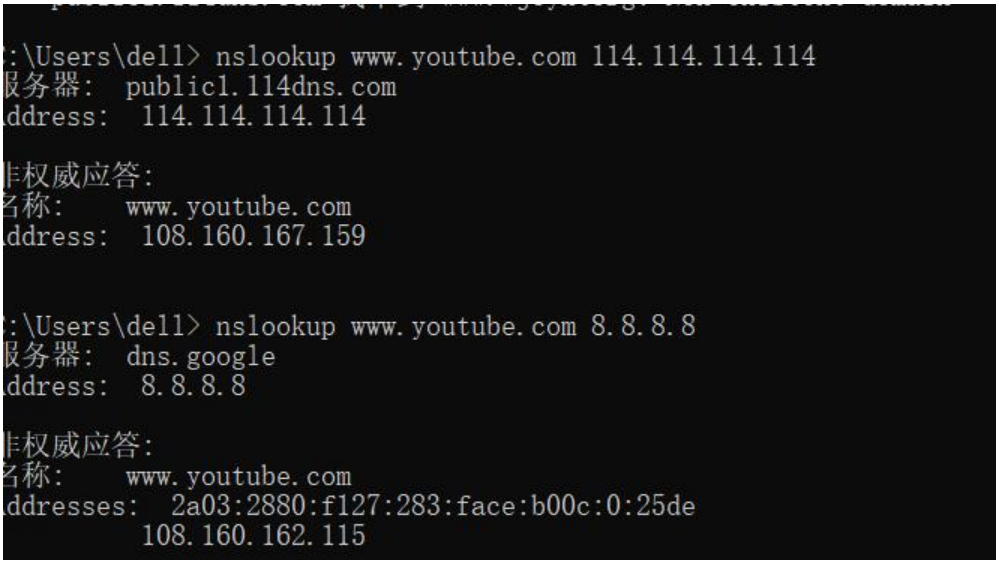
为啥ping不通油管?

```
C:\Users\dell>ping www.youtube.com

正在 Ping youtube-ui.l.google.com [172.217.163.46] 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。

172.217.163.46 的 Ping 统计信息:
    数据包: 已发送 = 4，已接收 = 0，丢失 = 4 (100% 丢失)，
```

我用nslookup命令去解析发现github给出的ip地址是正确的，给出的油管ip地址是错误的



我换了两个其他的DNS域名解析器来



发现给出两个ip地址还是错误的。说明DNS污染确实存在。

这里复习一下DNS域名解析的过程

什么是DNS域名解析

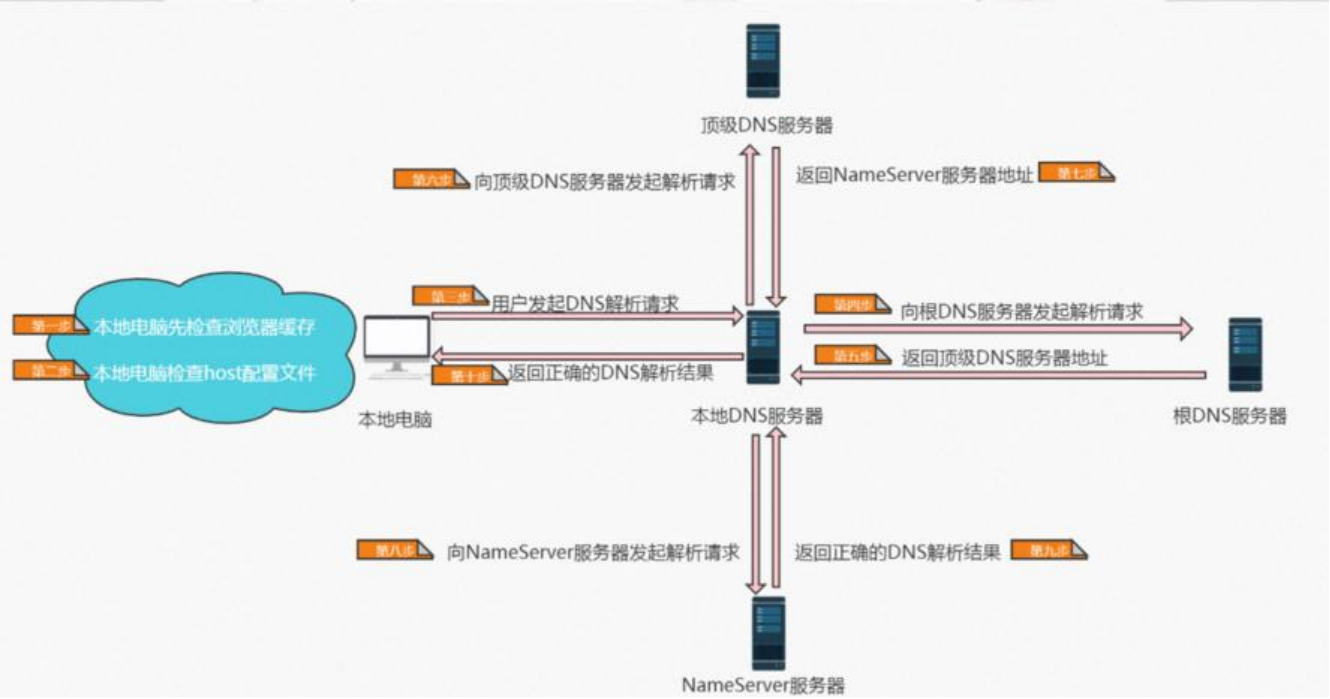
● 我们首先要了解域名和IP地址的区别。IP地址是互联网上计算机唯一的逻辑地址，通过IP地址实现同计算机之间的相互通信，每台联网计算机都需要通过IP地址来互相联系和分别。

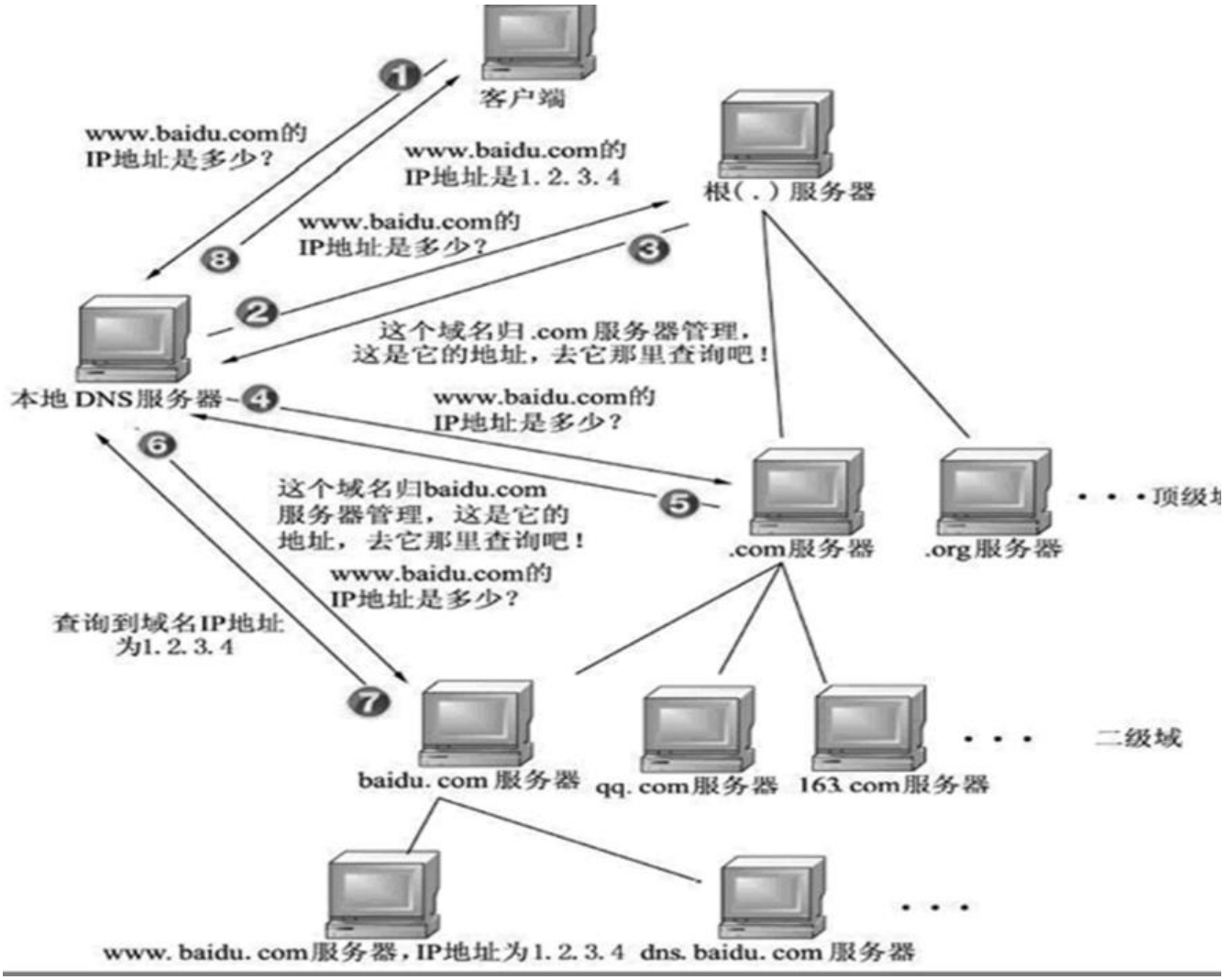
● 但由于IP地址是由一串容易混淆的数字串构成，人们很难记忆所有计算机的IP地址，这样对于我们常工作生活访问不同网站是很困难的。基于这种背景，人们在IP地址的基础上又发展出了一种更易识的符号化标识，这种标识由人们自行选择的字母和数字构成，相比IP地址更易被识别和记忆，逐渐代替P地址成为互联网用户进行访问互联的主要入口。这种符号化标识就是域名。

● 域名虽然更易被用户所接受和使用，但计算机只能识别纯数字构成的IP地址，不能直接读取域名。此要想达到访问效果，就需要将域名翻译成IP地址。而DNS域名解析承担的就是这种翻译效果。例如把 www.baidu.com 这个域名翻译成对应 IP 220.181.38.251

DNS域名解析过程

● 当我们在浏览器地址栏中输入 www.baidu.com时，DNS解析将会有将近10个步骤，这个过程大大体由一张图可以表示：





原文链接：说说 ip 地址被墙和 DNS 污染

域名解析流程

● 整个过程大体描述如下，其中前两个步骤是在本地电脑内完成的，后8个步骤涉及到真正的域名解服务器：

1. 浏览器先检查自身缓存中有没有被解析过的这个域名对应的ip地址，如果缓存中有，这个解析程就结束。

2. 如果浏览器缓存中没有数据，浏览器会查找操作系统缓存中是否有这个域名对应的DNS解析结。其实操作系统也有一个域名解析的过程，在windows中可以通过配置C:\Windows\System32\drives\etc\hosts文件来设置，用户可以将任何域名解析到任何能够访问的IP地址。

3. 前两个过程无法解析时，就要用到我们网络配置中的"DNS服务器地址"了。客户端通过浏览器问域名为 www.baidu.com (http://www.baidu.com) 的网站，发起查询该域名的IP地址的DNS请求该请求发送到了本地DNS服务器上。本地DNS服务器会首先查询它的缓存记录，如果缓存中有此条记，就可以直接返回结果。如果没有，本地DNS服务器还要向DNS根服务器进行查询。每个完整的内网常都会配置本地DNS服务器（例如你是通过学校连接互联网的一般是你学校的DNS服务器，如果你是小区连接互联网的一般是网络提供商比如电信，联通的DNS服务器，DNS服务器通常不会太远)大约8%的域名解析到这里就完成了。

4. 本地 DNS 服务器向根服务器发送 DNS 请求，请求域名为 www.baidu.com (http://www.baidu.com) 的 IP 地址。

5. 根服务器经过查询，没有记录该域名及IP地址的对应关系。但是会告诉本地DNS服务器，可以顶级域名服务器上继续查询，并给出顶级域名服务器的地址。如.com、.cn、.org等，全球只有13台

6. 本地 DNS 服务器向 顶级DNS服务器发送 DNS 请求，请求域名 www.baidu.com (http://www.baidu.com) 的 IP 地址。

7. 顶级DNS服务器收到请求后，不会直接返回域名和 IP 地址的对应关系，而是告诉本地DNS 服器，该域名可以在 baidu.com 域名服务器（Name Server服务器）上进行解析获取 IP 地址，并告诉aidu.com 域名服务器的地址。

8. 本地 DNS 服务器向 baidu.com 域名服务器发送 DNS 请求，请求域名 www.baidu.com (http://www.baidu.com) 的 IP 地址。

9. baidu.com 服务器收到请求后，在自己的缓存表中发现了该域名和 IP 地址的对应映射关系表并将 IP 地址返回给本地 DNS 服务器。

10. 本地 DNS 服务器将获取到与域名对应的 IP 地址返回给客户端，并且将域名和 IP 地址的对应系保存在缓存中，以备下次别的用户查询时使用。

参考资料：

**nslookup命令模拟DNS域名解析过程Quick Start