DNS可以说是最被我们低估和忽略的一个协议或服务，所谓大道至简，越是感受不到它的存在，才越体现它的厉害，本篇文章来介绍我们上网的幕后功臣：DNS。

由于篇幅问题，将一篇拆为了两篇，本篇主要介绍的是右边几个知识点，偏向于理论；左边几个点偏实践验证，故放在了下篇。

一、DNS的作用

DNS是Domain Name System的缩写，表示“域名系统”。

DNS直译是一种系统，也可以称之为一种协议或服务，主要职责就是将域名映射到一个IP地址，方便我们访问互联网。

之前的学习，我们接触的都是IP地址，互联网上的机器都是有自己的IP地址的，也正是IP地址才允许他们之间互相通信。

不过IP地址给会给我们带来困扰，人类的大脑很难记住一串数字，比如13.250.177.223，甚至是恐怖如斯的IPV6地址：

```
1504:02c9:41a4:85d3:0000:0000:a217:bca6
```

这对于我们来说太难记忆了，这得劝退多少人呀？而记住 `www.baidu.com` 这个域名则会容易许多。

可以看到，我们遇到的这个问题不是技术问题，而是一个命名问题，因为互联网配合 IP 地址已经能很好地运转了，但是我们这些“可怜”的人类没有机器那么强大的记忆力。为此，人类发明了DNS，解决了IP地址不好记忆的问题。

正式来说， `www.baidu.com` 就是我们容易记住的域名，DNS帮助我们自动将此域名解析为实际的IP地址，然后建立三次握手和传输。那么自然而然就会提出一个问题：DNS是如何知道这个域名对应这个IP的呢？它的工作原理是什么？DNS到底是个什么玩意？域名有没有讲究？

带着这些问题，本篇来好好看看幕后功臣DNS的工作机制。

二、DNS同时占用UDP和TCP端口53

DNS的一个特殊情况，我不得不单独拎出来说下：DNS同时占用UDP和TCP端口53。

这种单个应用协议同时使用两种传输协议的情况在TCP/IP栈也算是个另类，是什么造成了这种情况呢？

当然是不同的用途需要合适的协议，DNS在区域传输的时候使用TCP协议，其他时候使用UDP协议。

DNS区域传输的时候使用TCP协议：

- 辅域名服务器会定时（一般3小时）向主域名服务器进行查询以便了解数据是否有变动。如有变动，会执行一次区域传送，进行数据同步。区域传送使用TCP而不是UDP，因为数据同步传送的数据量比一个请求应答的数据量要多得多。
- TCP是一种可靠连接，保证了数据的准确性。

> DNS的规范规定了2种类型的DNS服务器，一个叫主DNS服务器，一个叫辅助DNS服务器。在一个区中主DNS服务器从自己本机的数据文件中读取该区的DNS数据信息，而辅助DNS服务器则从区的主DNS服务器中读取该区的DNS数据信息。当一个辅助DNS服务器启动时，它需要与主DNS服务器通信，并加载数据信息，这就叫做区传送（zone transfer）。

域名解析时使用UDP协议：

- 客户端向DNS服务器查询域名，一般返回的内容都不超过512字节，用UDP传输即可，不用经过三次握手，这样DNS服务器负载更低，响应更快。理论上说，客户端也可以指定向DNS服务器查询时用TCP，但事实上，很多DNS服务器进行配置的时候，仅支持UDP查询包。

敏锐的读者朋友从以上还可以得出一个重要信息：因特网上是不止一台DNS服务器的。

原因也很容易理解，因为因特网的规模很大，这样的域名服务器肯定会因为超负荷而无法正常工作，而且一旦域名服务器出现故障，整个因特网都将瘫痪。

早在1983年，因特网就开始采用层次结构的命名树作为主机的名字（即域名），并使用分布式的域名系统DNS。

DNS使大多数域名都在本地解析，仅少量解析需要在因特网上通信，因此系统效率很高。

由于DNS是分布式系统，即使单个计算机出现故障，也不会妨碍整个系统的正常运行。

提到了采用层次结构的命名树作为主机的名字，即域名，那下面我们就来看看域名结构。

三、等级森严的域名体系

其实域名是很讲究的，拿 `www.google.cn` 为例。

cn是顶级域名，有国家顶级域名（cn，us，jp，en，fr，it，de，es，等），和通用顶级域名（com，org，net，edu，biz，等），本例cn表示中国，顶级域名由《因特网名称与数字地址分配机构ICANN》进行管理。

google是在cn下注册的二级域名，有无限多的可能，各级域名由其上一级域名的管理机构即谷歌管理。

www是在google下注册的三级域名，www表示万维网，当然了，还可以换成其他的xxx.google.cn。

三级域名下面也可以再分支出四级域名，四级域名下还可以有五级域名，以此类推。

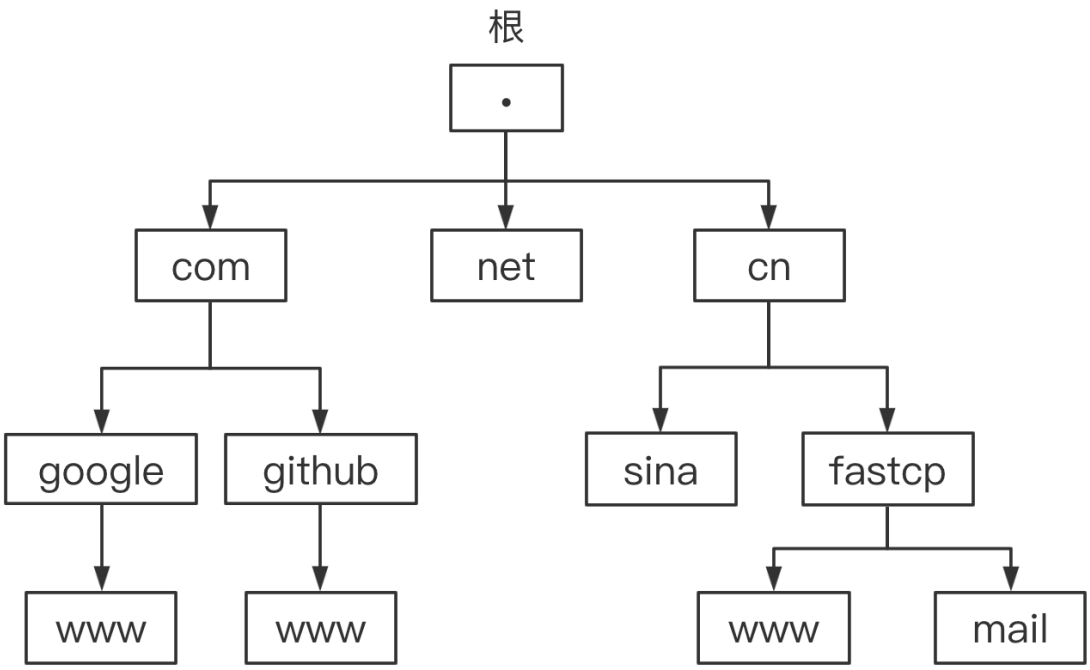
每一级都对应一个域：

```
www.        google.       cn       .
三级域名     二级域名      顶级域名    根
```

对，没错，其实最后还有一个点(.)，这才是真正合法唯一的域名。这个点表示终结，没有更高层的域了。如果没有这个点，那么可能还会往上层找有没有更高的域，可能就会解析到其他的地方。

所以， `www.google.cn` 并不规范，实际上应该是 `www.google.cn.`，这个对于我们用户访问浏览器没有什么影响，就算带上点，也会消失，但是当我们配置自己的 DNS 服务器时，你会发现这个点（.）变得非常重要。

那么整个域名的结构形如：



这样展开的结构就像一棵倒置的树。最多可以分支 127 层，每层最多由 63 个字符组成，中间用点（.）分隔。域名总长度不能超过 255 个字符，不区分大小写。

这种按等级管理的命名方法便于维护名字的唯一性，并且也容易设计出一种高效的域名查询机制，需要注意的是，域名只是个逻辑概念，并不代表计算机所在的物理地点。

四、域名服务器分类

我们可以看到，域名五花八门，而域名和IP地址的映射关系必须保存在域名服务器中，供所有其他应用查询，显然不能将所有信息都存储在一台域名服务器中，DNS使用分布在各地的域名服务器来实现域名到IP地址的转换。

域名服务器可以划分为以下四种类型：

- **根域名服务器**：根域名服务器是最高层次的域名服务器，每个根域名服务器都知道所有的顶级域名服务器的域名及其IP地址，因特网上共有13个不同IP地址的根域名服务器。尽管我们将这13个根域名服务器中的每一个都视为单个的服务器，但“每台服务器”实际上是由许多分布在世界各地的计算机构成的服务器群集。当本地域名服务器向根服务器发出查询请求时，路由器会把查询报文转发到离这个DNS客户最近的一个根域名服务器，这就加快了DNS的查询过程，同时也更加合理地利用了因特网的资源。根域名服务器通常并不直接对域名进行解析，而是返回该域名所属顶级域名的顶级域名服务器的IP地址。
- **顶级域名服务器**：这些域名服务器负责管理在该顶级域名服务器注册的所有二级域名。当收到DNS查询请求时就给出相应的回答。（可能是最终结果，有可能是下一级权限服务器的IP地址）

- **权限域名服务器（也常被称为权威域名服务器）**：这些域名服务器负责管理某个区的域名，每一个主机的域名都必须在某个权限域名服务器注册登记，因此权限域名服务器知道其管辖的域名与IP地址的映射关系，另外，权限服务器还知道其下级域名服务器的地址。
- **本地域名服务器**：本地域名服务器不属于上述的域名服务器的等级结构。当一个主机发送DNS请求时，这个报文就首先被送往该主机的本地域名服务器。本地域名服务器起着代理的作用，会将该报文转发到上述的域名服务器的等级结构中。每一个因特网服务提供者ISP，一个大学，甚至一个大学里的学院，都可以拥有一个本地域名服务器，它有时也称为默认域名服务器，本地域名服务器离用户较近，一般不超过几个路由器的距离，也有可能就在同一个局域网中。本地域名服务器的IP地址需要直接配置在主机中。

五、域名解析的原理

域名解析就是从域名得知 IP 地址的转换过程。域名的解析工作由 DNS 服务器完成。

当你在浏览器中输入 `www.github.com` 时，DNS服务器就开始解析这个域名。
DNS服务器有两种方法可以为你提供答案：

- 它自己知道答案。
- 它不知道答案，必须向另一台服务器请求答案。

不过一般情况下，你的DNS服务器是两眼一睁瞎问啥啥不会，没有办法直接为你提供结果。不过往往我们上网都是可以访问的，这里就用了一套机制来保证你可以得到最终的结果。

第一、输入 `www.github.com` 后，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。

第二、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。

以上两步都是在本电脑完成的，如果都没有查到结果，就要转向DNS服务器了。

> 小贴士，如果是通过浏览器访问的话，实际上会优先访问浏览器缓存。浏览器一般都会缓存一小段时间，所以有的时候会造成本地修改hosts不立即生效的情况。

第三、会去查找TCP/IP参数中设置的首选DNS服务器，即本地域名服务器，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。如果不由本地域名服务器区域解析，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。（这里说的权威性并不是说这些DNS服务器不值得信任，而是说这些DNS服务器本身不包含注册信息，当来了一个新的DNS查询时，需要从权威DNS上查到结

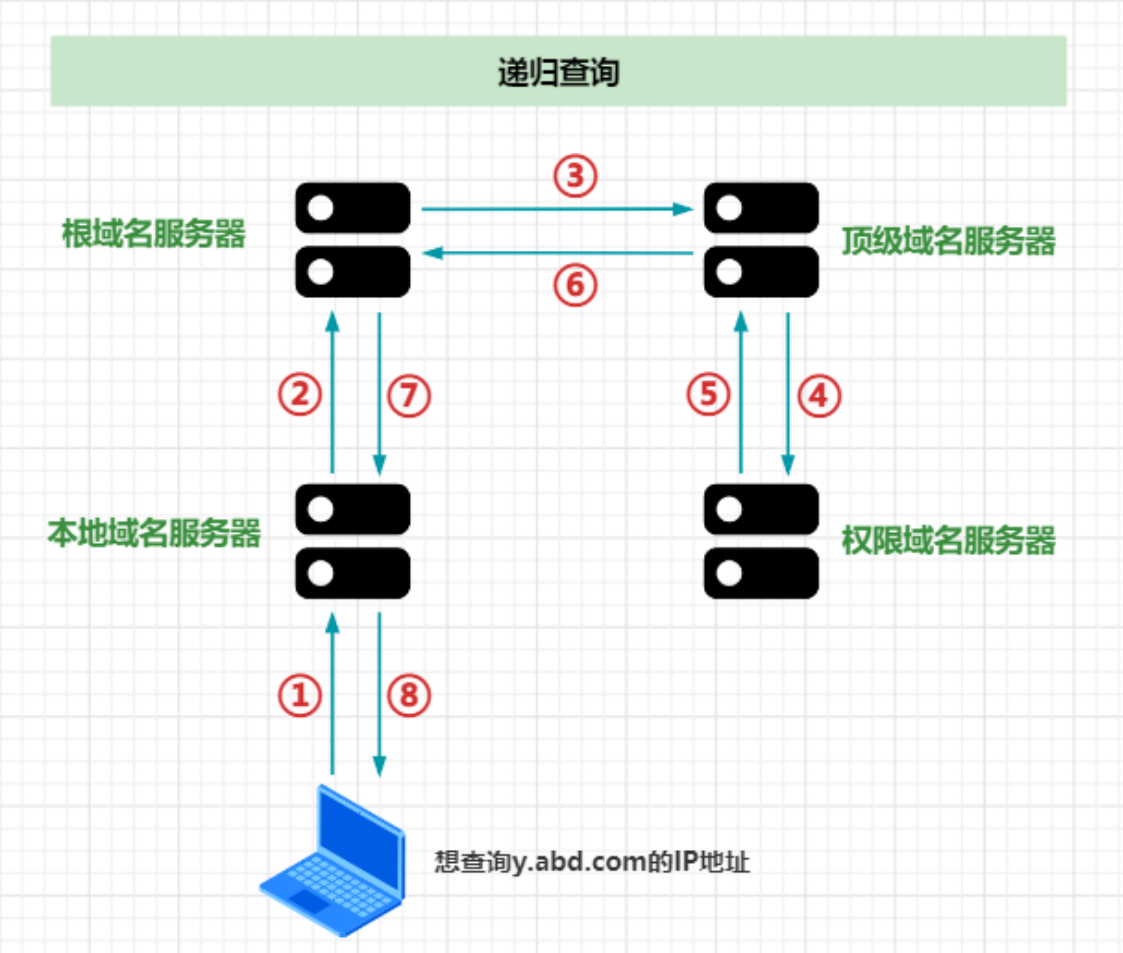
果并返回给客户端，这里说的权威DNS属于上面提到的ICANN的非盈利性组织）

第四、如果本地DNS服务器本地区域文件与缓存解析都失效，则根据本地域名服务器的设置（是否设置转发器）进行查询。如果启用转发模式，则会进行递归查询；否则会进行迭代查询。

六、递归查询和迭代查询

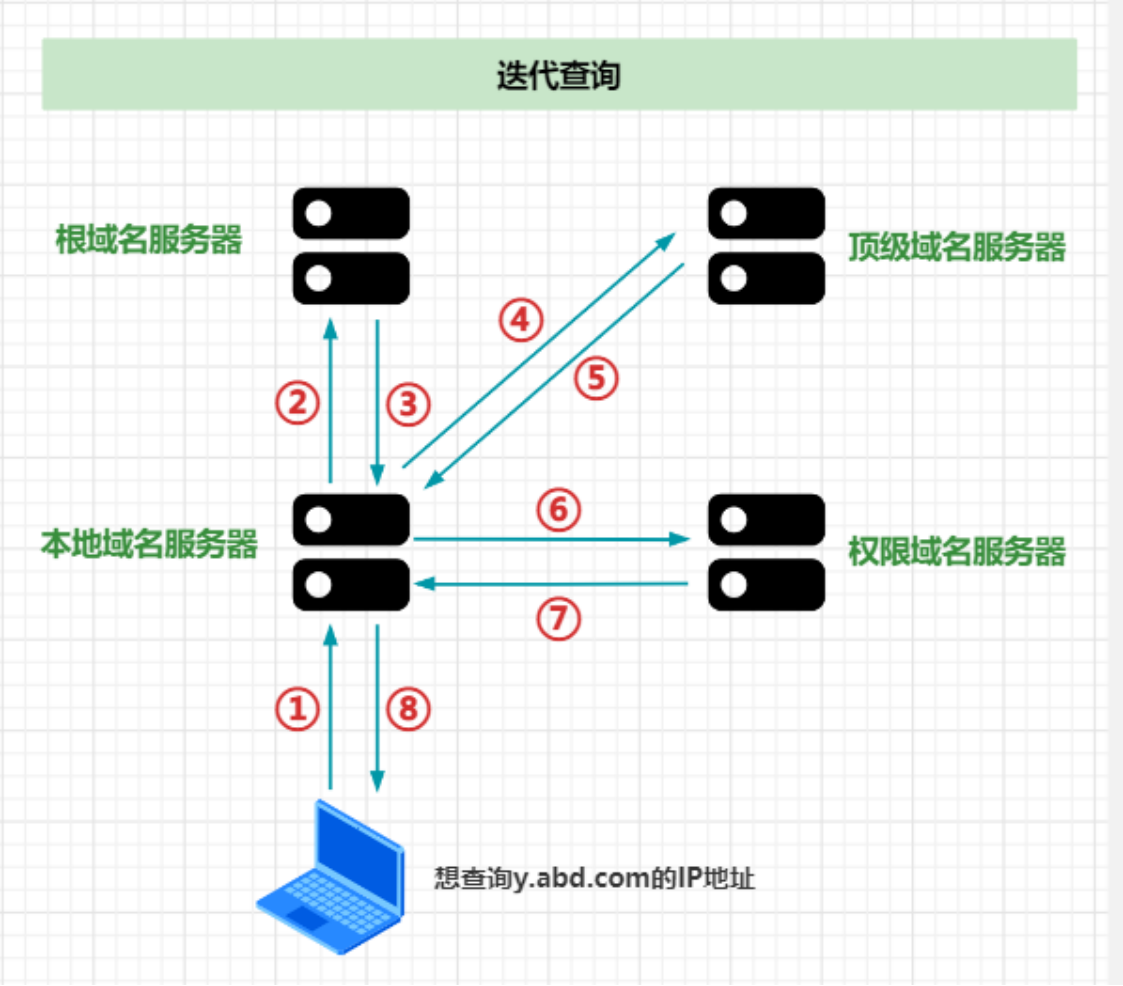
递归查询过程，以查询y.abd.com为例：

- ①主机首先向本地域名服务器进行查询；
- ②本地域名服务器收到递归查询委托后，也采用递归查询的方式向某个根域名服务器查询；
- ③根域名服务器收到域名查询的委托后，也采用递归查询的方式向某个顶级域名服务器查询；
- ④顶级域名服务器收到域名查询的委托后，也采用递归查询的方式向某个权限域名服务器查询
- ⑤⑥⑦⑧当查询到域名对应的IP地址后，查询结果会在受委托的各域名服务器之间传递，最终传回给用户主机。



再来看迭代查询：

- ①主机首先向本地域名服务器进行查询；
- ②本地域名服务器收到递归查询委托后，采用迭代查询的方式向某个根域名服务器查询；
- ③根域名服务器告诉本地域名服务器，下一次应查询的顶级域名服务器的IP地址；
- ④本地域名服务器向顶级域名服务器发起迭代查询；
- ⑤顶级域名服务器告诉本地域名服务器，下一次应查询的权限域名服务器的IP地址；
- ⑥本地域名服务器向权限域名服务器发起迭代查询；
- ⑦权限域名服务器告诉本地域名服务器所查询域名对应的IP地址；
- ⑧本地域名服务器最后把查询结果告诉用户主机。



不管使用递归查询还是迭代查询，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。

幸亏有缓存机制，不然域名服务器的压力得多大呀！不过缓存要有过期时间，因为域名和IP之间的映射关系不是一成不变的。