06-域名里有哪些门道？

在上一讲里，我们学习了HTTP协议使用的TCP/IP协议栈，知道了HTTP协议是运行在TCP/IP上的。

IP协议的职责是“网际互连”，它在MAC层之上，使用IP地址把MAC编号转换成了四位数字，这就对物理网卡的MAC地址做了一层抽象，发展出了许多的“新玩法”。

例如，分为A、B、C、D、E五种类型，公有地址和私有地址，掩码分割子网等。只要每个小网络在IP地址这个概念上达成一致，不管它在MAC层有多大的差异，都可以接入TCP/IP协议栈，最终汇合进整个互联网。

但接入互联网的计算机越来越多，IP地址的缺点也就暴露出来了，最主要的是它“对人不友好”，虽然比MAC的16进制数要好一点，但还是难于记忆和输入。

怎么解决这个问题呢？

那就“以其人之道还治其人之身”，在IP地址之上再来一次抽象，把数字形式的IP地址转换成更有意义更好记的名字，在字符串的层面上再增加“新玩法”。于是，DNS域名系统就这么出现了。

域名的形式

在第4讲曾经说过，域名是一个有层次的结构，是一串用“.”分隔的多个单词，最右边的被称为“顶级域名”，然后是“二级域名”，层级关系向左依次降低。

最左边的是主机名，通常用来表明主机的用途，比如“www”表示提供万维网服务、“mail”表示提供邮件服务，不过这也不是绝对的，名字的关键是要让我们容易记忆。

看一下极客时间的域名“time.geekbang.org”，这里的“org”就是顶级域名，“geekbang”是二级域名，“time”则是主机名。使用这个域名，DNS就会把它转换成相应的IP地址，你就可以访问极客时间的网站了。

域名不仅能够代替IP地址，还有许多其他的用途。

在Apache、Nginx这样的Web服务器里，域名可以用来标识虚拟主机，决定由哪个虚拟主机来对外提供服务，比如在Nginx里就会使用“server_name”指令：

```
server {
    listen 80;                      #监听80端口
    server_name  time.geekbang.org;  #主机名是time.geekbang.org
    ...
}
```

域名本质上还是个名字空间系统，使用多级域名就可以划分出不同的国家、地区、组织、公司、部门，每个域名都是独一无二的，可以作为一种身份的标识。

举个例子吧，假设A公司里有个小明，B公司里有个小强，于是他们就可以分别说是“小明.A公司”，“小强.B公司”，即使B公司里也有个小明也不怕，可以标记为“小明.B公司”，很好地解决了重名问题。

因为这个特性，域名也被扩展到了其他应用领域，比如Java的包机制就采用域名作为命名空间，只是它使用了反序。如果极客时间要开发Java应用，那么它的包名可能就是“org.geekbang.time”。

而XML里使用URI作为名字空间，也是间接使用了域名。

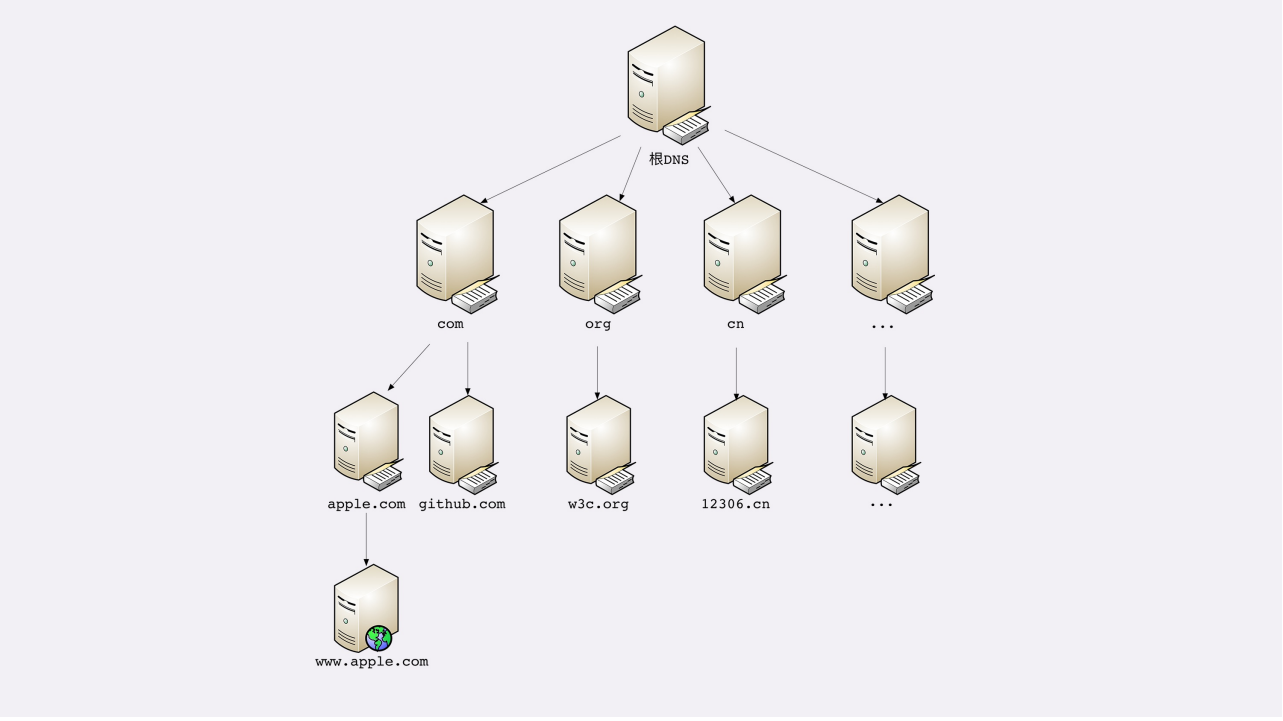
域名的解析

就像IP地址必须转换成MAC地址才能访问主机一样，域名也必须要转换成IP地址，这个过程就是“**域名解析**”。

目前全世界有几亿个站点，有几十亿网民，而每天网络上发生的HTTP流量更是天文数字。这些请求绝大多数都是基于域名来访问网站的，所以DNS就成了互联网的重要基础设施，必须要保证域名解析稳定可靠、快速高效。

DNS的核心系统是一个三层的树状、分布式服务，基本对应域名的结构：

1. 根域名服务器（Root DNS Server）：管理顶级域名服务器，返回“com”“net”“cn”等顶级域名服务器的IP地址；
2. 顶级域名服务器（Top-level DNS Server）：管理各自域名下的权威域名服务器，比如com顶级域名服务器可以返回apple.com域名服务器的IP地址；
3. 权威域名服务器（Authoritative DNS Server）：管理自己域名下主机的IP地址，比如apple.com权威域名服务器可以返回www.apple.com的IP地址。



在这里根域名服务器是关键，它必须是众所周知的，否则下面的各级服务器就无从谈起了。目前全世界共有13组根域名服务器，又有数百台的镜像，保证一定能够被访问到。

有了这个系统以后，任何一个域名都可以在这个树形结构里从顶至下进行查询，就好像是把域名从右到左顺序走了一遍，最终就获得了域名对应的IP地址。

例如，你要访问“www.apple.com”，就要进行下面的三次查询：

1. 访问根域名服务器，它会告诉你“com”顶级域名服务器的地址；
2. 访问“com”顶级域名服务器，它再告诉你“apple.com”域名服务器的地址；
3. 最后访问“apple.com”域名服务器，就得到了“www.apple.com”的地址。

虽然核心的DNS系统遍布全球，服务能力很强也很稳定，但如果全世界的网民都往这个系统里挤，即使不挤瘫痪了，访问速度也会很慢。

所以在核心DNS系统之外，还有两种手段用来减轻域名解析的压力，并且能够更快地获取结果，基本思路就是“**缓存**”。

首先，许多大公司、网络运行商都会建立自己的DNS服务器，作为用户DNS查询的代理，代替用户访问核心DNS系统。这些“野生”服务器被称为“非权威域名服务器”，可以缓存之前的查询结果，如果已经有了记录，就无需再向根服务器发起查询，直接返回对应的IP地址。

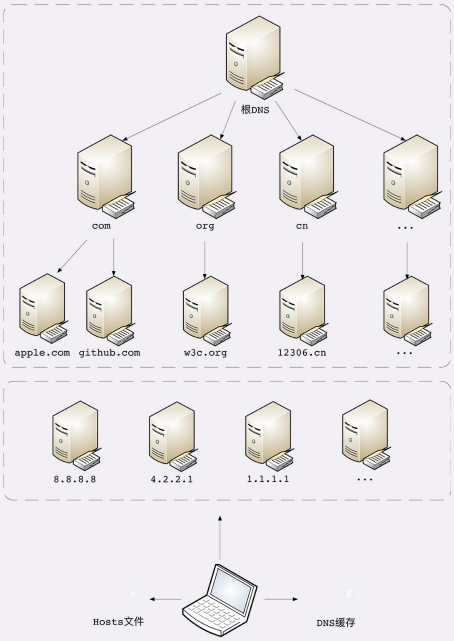
这些DNS服务器的数量要比核心系统的服务器多很多，而且大多部署在离用户很近的地方。比较知名的DNS有Google的“8.8.8.8”，Microsoft的“4.2.2.1”，还有CloudFlare的“1.1.1.1”等等。

其次，操作系统里也会对DNS解析结果做缓存，如果你之前访问过“www.apple.com”，那么下一次在浏览器里再输入这个网址的时候就不会再跑到DNS那里去问了，直接在操作系统里就可以拿到IP地址。

另外，操作系统里还有一个特殊的“主机映射”文件，通常是一个可编辑的文本，在Linux里是“/etc/hosts”，在Windows里是“C:\WINDOWS\system32\drivers\etc\hosts”，如果操作系统在缓存里找不到DNS记录，就会找这个文件。

有了上面的“野生”DNS服务器、操作系统缓存和hosts文件后，很多域名解析的工作就都不用“跋山涉水”了，直接在本地或本机就能解决，不仅方便了用户，也减轻了各级DNS服务器的压力，效率就大大提升了。

下面的这张图比较完整地表示了现在的DNS架构。



在Nginx里有这么一条配置指令“resolver”，它就是用来配置DNS服务器的，如果没有它，那么Nginx就无法查询域名对应的IP，也就无法反向代理到外部的网站。

```
resolver 8.8.8.8 valid=30s;  #指定Google的DNS，缓存30秒
```

域名的“新玩法”

有了域名，又有了可以稳定工作的解析系统，于是我们就可以实现比IP地址更多的“新玩法”了。

第一种，也是最简单的，“重定向”。因为域名代替了IP地址，所以可以让对外服务的域名不变，而主机的IP地址任意变动。当主机有情况需要下线、迁移时，可以更改DNS记录，让域名指向其他的机器。

比如，你有一台“buy.tv”的服务器要临时停机维护，那你就可以通知DNS服务器：“我这个buy.tv域名的地址变了啊，原先是1.2.3.4，现在是5.6.7.8，麻烦你改一下。”DNS于是就修改内部的IP地址映射关系，之后再有访问buy.tv的请求就不走1.2.3.4这台主机，改由5.6.7.8来处理，这样就可以保证业务服务不中断。

第二种，因为域名是一个名字空间，所以可以使用bind9等开源软件搭建一个在内部使用的DNS，作为名字服务器。这样我们开发的各种内部服务就都用域名来标记，比如数据库服务都用域名“mysql.inner.app”，商品服务都用“goods.inner.app”，发起网络通信时也就不必再使用写死的IP地址了，可以直接用域名，而且这种方式也兼具了第一种“玩法”的优势。

第三种“玩法”包含了前两种，也就是基于域名实现的负载均衡。

这种“玩法”也有两种方式，两种方式可以混用。

第一种方式，因为域名解析可以返回多个IP地址，所以一个域名可以对应多台主机，客户端收到多个IP地址后，就可以自己使用轮询算法依次向服务器发起请求，实现负载均衡。

第二种方式，域名解析可以配置内部的策略，返回离客户端最近的主机，或者返回当前服务质量最好的主机，这样在DNS端把请求分发到不同的服务器，实现负载均衡。

前面我们说的都是可信的DNS，如果有一些不怀好意的DNS，那么它也可以在域名这方面“做手脚”，弄一些比较“恶意”的“玩法”，举两个例子：

- “域名屏蔽”，对域名直接不解析，返回错误，让你无法拿到IP地址，也就无法访问网站；
- “域名劫持”，也叫“域名污染”，你要访问A网站，但DNS给了你B网站。

好在互联网上还是好人多，而且DNS又是互联网的基础设施，这些“恶意DNS”并不多见，你上网的时候不需要太过担心。

小结

这次我们学习了与HTTP协议有重要关系的域名和DNS，在这里简单小结一下今天的内容：

1. 域名使用字符串来代替IP地址，方便用户记忆，本质上一个名字空间系统；
2. DNS就像是我们现实世界里的电话本、查号台，统管着互联网世界里的所有网站，是一个“超级大管家”；
3. DNS是一个树状的分布式查询系统，但为了提高查询效率，外围有多级的缓存；
4. 使用DNS可以实现基于域名的负载均衡，既可以在内网，也可以在外网。

课下作业

1. 在浏览器地址栏里随便输入一个不存在的域名，比如就叫“www.不存在.com”，试着解释一下它的DNS解析过程。
2. 如果因为某些原因，DNS失效或者出错了，会出现什么后果？

欢迎你把自己的答案写在留言区，与我和其他同学一起讨论。如果你觉得有所收获，也欢迎把文章分享给你的朋友。

课外小贴士

01 早期的域名系统只支持使用英文，而且顶级域名被限制在三个字符以内，但随着互联网的发展现在已经解除了这些限制，可以使用中文做域名，而且在“com”“net”“gov”等之外新增了“asia”“media”“museum”等许多新类别的顶级域名。

02 域名的总长度限制在 253 个字符以内，而每一级域名长度不能超过 63 个字符。

03 域名是大小写无关的，但通常都使用小写的形式。

04 过长的域名或者过多的层次关系也会导致与 IP 地址同样难于记忆的问题，所以常见的域名大多是两级或三级，四级以上的很少见。

精选留言：

- zjajxzg 2019-06-10 01:03:51
  1、操作系统缓存→本地hosts文件→非核心dns服务器→根域名服务器地址→顶级域名服务器地址→二级域名服务器地址。。。
  2、无法访问相应的资源 [4赞]

  作者回复2019-06-10 09:10:02
  第一个没说完，第二个问题可以再说的详细一些。

- 梦倚栏杆 2019-06-10 09:26:44
  老师好，我有两个疑问：
  1.终极dns的解析是有谁实现的或者谁规定的：
  比如乔布斯有个苹果域名：www.apple.com，苹果电脑的官网；张三也想为水果苹果申请个域名(www.apple.com)来展示他的苹果;结果我们几乎可以猜测到，他是申请失败的，原因已经有一个苹果存在了，谁来评判这个苹果域名已经被占用了呢？判断逻辑是如何来的，如果两个申请发生在同时呢？
  2. ip地址的分配和身份证号一样吗？有地址在里面吗？
  比如1-45属于美国的网段，或者属于哪个超大公司的网段。如果有，那是不是就以为着预分配，也就意味着部分ip段的浪费，如果没有，那ip地址从一个地方查找另外一个地方怎么找呢？莫非每个初始的线路都需要访问到根DNS
  [2赞]

  作者回复2019-06-10 09:57:00
  域名由专门的域名注册机构管理，终极的是ICANN。
  IP地址的分配也由ICANN管理，当然有浪费，美国是互联网的发明国，所以占用ip地址最多。

  ip地址查找由专门的协议，比如arp。

  这些比较偏底层，离http比较远，可以再找其他资料学习。。

- 我行我素 2019-06-10 10:52:57
  老师，想请问下，当域名所对应的ip发生变化的时候，因为本地或者"野生"域名服务器上的ip是怎么发生

变化的呢？因为在域名所对应的ip发生变化的时候应该是通知的权威域名服务器吧 [1赞]

作者回复2019-06-10 11:48:14
域名解析有个ttl有效期，到期就会去上一级dns重新获取，当然也可以主动刷新。

- 何用 2019-06-10 09:08:57
为何全世界只有 13 组根域名服务器呢？ [1赞]

作者回复2019-06-10 09:28:45
细节原因不好解释，简单来说是因为dns协议还有udp协议里包大小的限制，只有512字节，再除以dns记录长度，最多15组，再去掉buffer。

- -W.LI- 2019-06-10 08:46:08
老师好!1.2.3.4改成5.6.7.8后访问不到浏览器会自动重试解析DNS是么?从事的时候使用野生还是专业的有啥策略?重试几次，DNS集群的域名是最终一致还是强一致。
1.操作系统缓存不存在，host文件不存在，访问DNS服务器，根域名解析成功，二级域名解析失败，重试还是失败。浏览器返回错误。
2走失败策略，最终还是失败的就错误页面。 [1赞]

作者回复2019-06-10 09:13:01
dns解析出ip后访问失败就不会再解析了。
浏览器的重试策略跟具体实现有关，这个我也不清楚。
dns是最终一致。

- pyhhou 2019-06-11 02:30:53
思考题：
1、操作系统首先会在其缓存和 HOST 文件中去找域名对应的 IP 地址，如果本地中没有记录，则会去 DNS 服务器中查找，按照 DNS 服务器的树状结构，层级进行访问查找，对于 “www.” 这样的请求，在第一层，也就是根域名服务器中是找不到下一层的域名服务器的，于是就返回错误给客户端，不继续往下找
2、看 DNS 服务器的返回错误内容吧，如果是返回错误请求或者内部错误告知的话，客户端这边可以相应地做一些响应异常处理；还有一种情况是 DNS 返回一个不存在的 IP 地址，或者是映射到错误的 IP 地址，个人认为前者的影响会小一些，顶多是请求页面 404 报错，后者的话则会误导用户，比如你输入了 “www.apple.com”，弹出的是 Google 搜索栏

这里想请教老师几个问题，可能有点超出 HTTP 的范畴，但是还是比较好奇
1、如果说我们应用域名的一些技术，比如文中说的重定向，负载均衡等等，这些技术都涉及到了域名和 IP 映射关系的改变，那么这些改变只是在其对应的 DNS 代理服务器上改变吗，还是说代理服务器立刻会将该改变内容发送到 DNS 核心服务器去？
2、另外就是操作系统的缓存和 HOST 文件是不是需要定期的人工检查，排除域名和 IP 对应的改变？

- 极客时间 2019-06-11 00:26:29
这句话不是太明白 “第一种方式，因为域名解析可以返回多个 IP 地址，所以一个域...

域名不是只能绑定一个ip地址吗？为什么解析的时候会返回多个ip呢？ 我是哪里读漏了吗？

- 怀朔 2019-06-10 22:15:13
回答第二个问题：1、本地hosts绑定 2、野生dns服务器拦截 3、dns切换过程失效 4:ttl时间变动

- stormyif 2019-06-10 20:56:55
GFW就是使用了这些恶意的DNS

- Reco 2019-06-10 15:33:38

  老师您好，之前碰到过这样一个问题

  域名解析返回两个IP地址，其中一个IP无法正常访问。

  Safari可以自动切换到正常的IP地址继续访问

  Chrome会尝试TCP连接不正常的IP，大约1分多钟之后会连接另一个IP

  最终导致Chrome页面访问速度缓慢。想问下这种问题是属于浏览器问题，还是DNS的问题呢？

  作者回复2019-06-10 17:39:13

  这个应该是浏览器的重连策略问题，dsn解析结果已经出来了，就已经跟dns无关了。