二

22 想来我家，你自己查呀 - DNS

我们的课程已经过一大半了。先给自己一个奖励。当然也感谢你愿意继续的和我这段学习旅程。我们今天一起来看一下DNS。其实前面已经多多少少讲了一些DNS的工作原理。今天还是由浅入深的来看一下。

主机文件和DNS缓存

我将从hosts文件开始我们DNS的旅程。自DNS诞生以来，hosts文件就已存在。当Internet还仅仅由MIT，军方和少数其他组织组成的时候，hosts文件时一种对IP地址解析名称的简便方法。但是随着互联网的发展和壮大，你能否想象拥有一个包含每个网站及其相应IP地址的主机文件？答案当然是不可能的。hosts文件也是IP地址引擎的最开始的名称。 DNS就是从此发展起来的。每当我们讨论主机文件时，我们都必须要讨论DNS缓存。当DNS需要将名称解析为IP地址时，有几个地方需要来检查。第一个位置就是检查本地计算机，因此，第

一步，DNS会在每台机器上本地查看。第二步，在读取主机文件后，再发送给DNS服务器之前，会查找DNS缓存。DNS确实非常努力地尝试在本地对IP地址进行DNS解析。因此，查询的顺序就是本地文件，DNS缓存最后才是DNS服务器服务。根据操作系统的不同，编辑主机文件有所不同。

Windows

如果你使用的是Windows操作系统，可能是Windows 7、8、10或任何服务器操作系统，那么你想要做的就是打开提升的命令提示符。如果你不熟悉，请单击“开始”按钮，键入cmd，然后在出现命令提示符时，右键单击并选择“以管理员身份运行”。然后，键入记事本，然后输入主机文件所在的路径。比如 notepad C:\Windows\System32\drivers\etc\hosts，你可以进行任何更改，最后一步是刷新DNS缓存，因为刷新DNS缓存时，将读取主机文件并将其放入DNS缓存中。

Mac & Linux

在Mac操作系统上，你将启动Terminal。输入sudo nano /private/etc/hosts，然后对该主机文件进行任何更改。刷新DNS缓存。在Linux机器上，可以键入sudo vim /etc/hosts。修改文件然后刷新DNS缓存。

DNS在本地找不到怎么办呢?

上面看到了DNS查找的流程。那如果DNS在本地找不到呢?

你试想一下，我们有大量的网站和IP的对应。这些不可能存在一个DNS服务器上，对不对。所以，就好像我们的王牌对王牌一样，要一个个的去传，一个个的去问。因为当我么去问一个DNS服务器答案时，如果它不知道答案，它将要问别人也就是另一个DNS服务器，当然也是不得不去问别人。

比如说我有一个工作站，在该工作站中有一个本地DNS服务器。我现在要输入https://www.csdn.net/。 该DNS查询转到DNS服务器，这个是本地的服务器，不是csdn的，所以它不知道答案。它会说我不知道答案，但是我可以帮你问下一个人，于是把请求发到了Root也就是根服务器，问，你知道大名鼎鼎的csdn的IP地址吗，这个ROOT服务器会说，我也不知道，但是我可以帮你问问.net DNS服务器。于是你又问.Net DNS服务器，你知道大名鼎鼎的csdn的IP地址吗，这个.net DNS服务器会说，对不起，我不知道，但是我能帮你问问csdn的DNS服务器。然后你就又去问csdn服务器，这个服务器说，我当然知道了。IP是47.95.164.112。然后你可以去访问这个IP地址了，你就可以看到华丽辉煌的csdn网站了。然后你本地的DNS服务器会把这个记录也就是csdn.net = 47.95.164.112放到DNS缓存里。这样当你女朋友也想去csdn学习的时候，就不需要再继续上面那些复杂的查询了。可以直接得到csdn的IP了对不对。

你可能会有疑问是不是，那就是这个本地的DNS服务器是怎么知道根服务器的呢。这个就是我上面提到的根提示。

根提示

这个根提示也就是Root Hints，在互联网上不止一个。它们存储在名为CACHE的文件中。你如果可以接触到一个Windows的服务器的话，可以从Systemroot\system32\dns文件夹中找到这个文件叫做CACHE.DNS。你可以查看并且编辑。

```
HOSTNAME（主机名）    IP ADDRESSES（IP地址）     OPERATOR（拥有者）
a.root-servers.net 198.41.0.4, 2001:503:ba3e::2:30  Verisign, Inc.
b.root-servers.net 199.9.14.201, 2001:500:200::b     University of Southern Califor
c.root-servers.net 192.33.4.12, 2001:500:2::c           Cogent Communications
d.root-servers.net 199.7.91.13, 2001:500:2d::d         University of Maryland
e.root-servers.net 192.203.230.10, 2001:500:a8::e    NASA (Ames Research Center)
f.root-servers.net 192.5.5.241, 2001:500:2f::f           Internet Systems Consortiu
g.root-servers.net 192.112.36.4, 2001:500:12::d0d    US Department of Defense (NIC)
h.root-servers.net 198.97.190.53, 2001:500:1::53      US Army (Research Lab)
i.root-servers.net 192.36.148.17, 2001:7fe::53          Netnod
j.root-servers.net 192.58.128.30, 2001:503:c27::2:30 Verisign, Inc.
k.root-servers.net 193.0.14.129, 2001:7fd::1             RIPE NCC
l.root-servers.net 199.7.83.42, 2001:500:9f::42         ICANN
m.root-servers.net 202.12.27.33, 2001:dc3::35         WIDE Project
```

复制

权威与非权威的回应

权威的回应，就好像是上面的例子，你的工作站和你的DNS服务器在同一个DNS Zone。比如这个DNS服务器是test.com DNS Server，那么这个服务器上会有所有和test.com相关的DNS对应信息，你如果想查询www.a1.test.com，你可以直接通过这个DNS服务器来查到。像这种可以从DNS拿到消息，而且这个消息不是在Cache里，而是在它的Zone里面的情况就是权威的。因为这是最可信的。当然这个例子不一定准确呀，就好像你想知道你二叔家的地址，是不是问你爸给的答案是最准确的。因为他们是在同一个ZONE里面。

非权威的就好像我们上面的那个例子，问了A，然后问B，然后问C，最后才找到。这个就好像你想去二叔家，你就一路的去问，比如说你知道住北京，然后有人说，你二叔在东城，然后有人说在东城的某一个区域，（我不是北京人，不太了解具体地址呀）。就这样一路吻下去，最后才找到，所以这个就是非权威的。

其实看到这里，我相信聪明的你已经大概知道了DNS的结构，至少你应该知道上面提到的根就是DNS的最开始需要检查的地方。下面我们来看一下DNS的结构。

DNS的结构 DNS的最高的级别就是我们上面提到的Root，一共有13个。然后下面就

是.com，.net ….，这个叫做Top Level Domain也可以简写成TLD。ICANN（Internet Corporation for Assigned Names）负责大部分TLD的分配。专门负责TLD的叫做TLD服务器。然后根据不同的Top Level会有Second Level，比如.Mil很明显就是军方使用，下面可以有Army，Navy。Edu很明显是教育，下面可以有MIT，Berkeley，然后就是比如csdn的Domain在.net的下面，这样看起来是不是就很清楚了。

DNS Zone

DNS Zone一共有两种

- Forward Lookup Zone（正向查找） - 这个是Host Name to IP，就是你给我Hostname，我给你查IP
- Reverse Lookup Zone（反向查找） - 和老大相比，这个老二并不怎么受欢迎，那就是给你IP，找到对应的HostName，什么地方会用到呢？比如Microsoft Exchange Servers和其他的邮件服务器去验证这个源域名来确保这个邮件是来自于合法的域名，当然还有一些比较老的工具，比如NSLookup，traceroute，SMTP

DNS Zone Type

主区域（Primary Zone）

- 权威的区域信息。
- 具有区域数据的读/写副本。
- 接受来自客户端的动态更新或动态DNS。

次要区域（Secondary Zone）

看这个例子，比如说你有一个网站，同时有两个办公地点，北京和上海。在北京的站点，有一个DNS服务器。在上海的站点则没有。假设你有50个客户，他们都被指向北京站点以使用该DNS服务器。在两者之间，我们有一个WAN链接，但是你为了贪图小便宜吧，这不是最大的WAN链接。有的时候它就会崩溃了，上海站点中的可怜用户无法再访问任何需要DNS解析的内容了。要解决此问题，你可以复制一份你网站DNS区域从北京站点到上海站点的服务器，然后你可以将所有50个客户端指向该本地上海DNS服务器。使用客户端DNS配置，你可以配置多个DNS服务器供客户端查询。因此，如果你希望将这些客户端指向北京站点，则可以在这些客户端上具有主DNS服务器，然后将它们指向上海站点，则可以具有辅助DNS服务器。也可以反过来，由你自己来决定怎么设计这种模式。一旦你在上海站点上关闭了DNS服务器，你的客户端就可以将所有查询本地发送到该DNS服务器，而他们不再需要依靠不稳定的WAN链接。辅助DNS区域，我们获得辅助DNS区域的方式是执行区

域传输。从主DNS服务器获取区域的副本。

DNS 区域传输 （Zone Transfer)

现在假设你开始第一次去索要复印件，你就拥有了一切，这个叫做AXFR。之后，每一次的传输完毕了之后，叫做IXFR（Incremental zone Transfer），只是给我从上次更新之后的数据就可以。现在，存在于辅助DNS区域上的信息被认为是权威的。因为当客户端向辅助DNS服务器询问问题时，如果这个响应的解决方案位于该计算机本地，则它被视为权威响应。辅助区域是只读的。你不能在辅助DNS区域上进行动态更新。只有主数据库才能发生动态更新，但是你可以在主服务器上进行动态更新，然后将数据复制到辅助DNS服务器。

DNS区域传输是通过端口53执行的。你可能会问自己，这个传输是UDP还是TCP？（如果你这么问，说明你已经迷恋上了网络协议，而且恭喜你，你已经可以算是入门了）。如果所有数据可以放进一个数据包，则它通过UDP传输。如果有太多数据（如初始AXFR中的数据），则复制将在TCP中执行，因为它必须分解数据并将其放入单独的数据包中。所以当涉及到防火墙的时候，你需要知道的是传输是通过UDP还是TCP，答案是两者都可以。

缓存DNS服务器 （Cache Only DNS Server)

这是最简单的DNS服务器

1. 你所要做的就是安装DNS，工作就完成了！
2. 它不包含任何区域（zone）。
3. 缓存是在一段时间内建立的。

发生的情况是，你将客户端配置为将其DNS查询发送到上面没有区域的DNS服务器。客户询问该服务器的任何问题，都必须走出去并找到答案。找到答案后，会将答案放入其本地缓存中。因此，这就是仅缓存DNS服务器的工作方式，它会在一段时间内建立缓存。重新启动该服务器后，将刷新缓存。

资源记录(Resource Record)

在正向查找区域中可以放置不同类型的资源记录，其中一部分普通的。还有其他一些根据你所运行的DNS不同而产生的特定类型的资源记录。

普通资源记录(Common Resource Record)

- 主机记录是最常见的资源记录之一。 A记录是IPv4 host记录。AAAA就是IPv6 host记录。

- PTR或指针记录是驻留在反向查找区域中的记录，这些记录指向正向查找区域中的主机记录。
- CName是计算机的昵称。如果你的环境中有一台服务器，并且你希望所有人出于任何原因使用不同的名称来访问它，则可以将CName记录设置为指向主机记录。比如你的地址可能是sfredsddsd.com，你完全可以改为shuaige.com这样其他的人也好记。
- SRV记录或服务定位记录表示机器上运行的不同类型的服务。例如，在Microsoft环境中，如果客户端计算机想要查找域控制器，则它将向DNS服务器发送查询，询问该域的SRV记录，然后它将获得一个域控制器的列表，该列表它可以针对用户的任何目的进行身份验证。
- MX记录。这些是邮件交换记录，它们表示邮件服务器。在Microsoft环境中，它将是交换服务器。
- NAPTR。通常用于互联网电话中的应用。一个例子就是会话发起协议（SIP）中服务器和用户地址的映射。

特殊的资源记录(Special Resource Record)

- NS或Name Server（DNS Server)。名称服务器记录表示DNS正在该服务器上运行，这就是使它成为Name Server的原因。
- SOA或Start of Authority或者是一个提供权威信息的DNS服务器。

把以上的原理了解清楚了，你的DNS知识就也足够了。

上一页 下一页