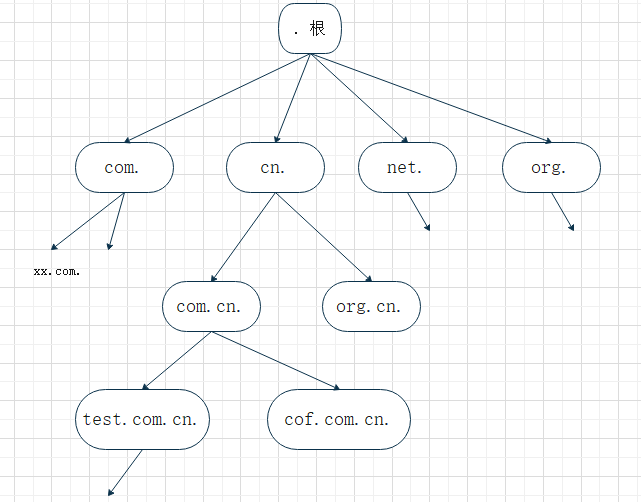
### DNS域名相关知识

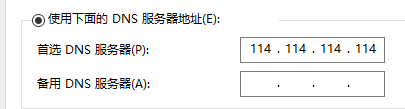
Domain Name域名最初是用来在互联网上充当某个IP的别名的，因为每个服务器都用ip来表示的话，太多了，不太好记住，用域名来记的话比较方便。

域名的命名是分层级的，形如xx.cof.com之类的，从左到右级别依次增大，最右边的为顶级层次，其实域名的完整写法是在最后有一个点 . 这种写法称为FQDN完全限定域名，形如 xx.cof.com. 最右边的 . 点才是最顶层，层级图如下：



域名服务器上面保存了某些域名对应的ip地址等信息，我们上网时，在地址栏上输入

http://域名/ 之后，系统先查本地的缓存及hosts文件，如果没有此域名的ip信息，便会去向我们指定的DNS服务器请求目标域名的IP地址记录，获得服务器返回的IP信息后，再向目标IP发起http请求



其实DNS服务器上保存的域名信息不止是ip地址，还有其他的信息，域名对应的每一条信息称为记录，（就比如域名是一个人名，我们可以查询此人对应的性别，年龄，身高等记录）

域名的记录类型有很多，一个域名的同一类型的记录也可以有多条，常用的记录类型如下：

|  |  |  |
| --- | --- | --- |
| **域名的记录类型** | **对应的英文缩写** | **例值** |
| IPv4地址 | A | 133.18.2.2 |
| IPv6地址 | AAAA | 2048:7163::63d3:374e:4235 |
| 名字服务器 | NS | ns-559.awsdns-05.net |
| 邮件交换记录 | MX | 163mx01.mxmail.netease.com |
| TXT记录 | TXT | 一般写此域名的说明，以及用于SPF技术 |
| 别名记录 | CNAME | xx.com，此记录里的才是真实的域名 |
| 服务记录 | SRV | 一般为微软的活动目录服务的设置才用得上 |
| 起始授权机构 | SOA | 此记录的值为这个区域的所有者，它才有权修改dns记录 |
| 缓存保留时间 | TTL | 3600，秒 |
| 指针记录 | PTR | 将ip地址解析成它对应的域名，常用于邮箱服务 |

其他的记录不常用，就不多说了。

A记录为ipv4记录，记录值为此域名对应的ipv4地址

AAAA记录为ipv6记录，记录值为此域名对应的ipv6地址

NS记录表明了此域名是在哪个dns服务器上做的解析，我们申请了自己的域名后，默认是

在域名注册商那里做的解析，我们也可以委托其他的dns服务商去做此域名的解析

先在要委托的dns服务商那里添加我们的域名，然后会生成几个默认的ns记录

然后在注册商那里指定dns服务器为dns服务商那里给出的NS记录值

MX记录表明了此域名的邮箱服务器地址，值可以是ip也可是域名

当我们向admin@cof.com 发邮件时，先查询cof.com的mx记录，再去查询mx记

录里的那个域名对应的ip地址，最后把邮件发给那个ip地址的服务器

TXT记录里面的值为文本，可以是对此域名的说明，也可用于SPF反垃圾邮件技术，也可在

申请ssl证书时做一下域名的持有验证，就是CA商家要我们写上指定的txt记录，

以证明此域名是我们的

CNAME记录，比如cof.com的cname记录为fdsafsadfsdfsa.sfdsf.com.cn时，cof.com就是后

面那个较长的不太好记的域名的别名，

PTR记录为反向解析时用到，比如我们邮箱服务器收到从2.2.2.2这个ip发来的邮件，它声

称自己是cof.com的邮箱服务器，我们便去查询2.2.2.2的ptr记录是否为cof.com，

是的话，就证明此ip不是在乱说

SOA记录表示这个记录值所对应的dns服务器才是此域名所在域的最佳信息来源

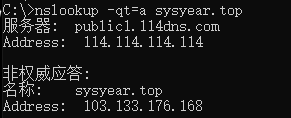
SRV记录常用于微软的活动目录服务中，用来告知客户端某个服务所在的那个服务器是谁

当dc域控和dns服务不在同一台服务器上时，此记录就是用来指明dc域控的地址

TTL记录表示此域名的信息可以保留在系统缓存里的时间，一般操作系统也不会听它的。

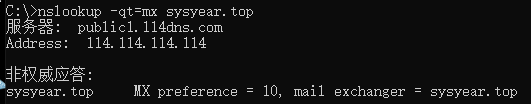
我们在cmd命令行里ping某个域名时，会看到它对应的ip地址信息，那么如何查看此域名对应的其他信息呢？可以用nslookup -qt=记录英文缩写 目标域名 这个命令来查询，例：

nslookup -qt=a sysyear.top #查询sysyear.top的A记录，如下图，值为103.x.x.x



nslookup -qt=mx sysyear.top #查询sysyear.top的mx记录，值为sysyear.top

#表示此域名的邮箱服务器也是sysyear.top



nslookup -qt=ns sysyear.top #查询sysyear.top的ns记录，值有多条

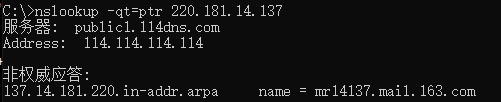
#它的名字服务器为ns7/ns8.cnmsn.net，表示它是在

#ns7或ns8.cnmsn.net这2台dns服务器上做的解析



nslookup -qt=ptr 220.181.x.x #查询目标ip的ptr记录，查询结果为

#mr14137.mail.163.com



上图可见，我们在查询ptr记录时，虽然默认只写了目标ip，其实是这个nslookup工具帮我们把目标ip转成了正确的查询名称：x.x.x.x.in-addr.arpa （这个x.x.x.x为查询ip的倒序值）

所以我们查询的仍然是一个域名，很多人以为查的是ip地址，其实不然。标准的写法如下：

nslookup -qt=ptr x.x.x.x.in-addr.arpa





**域名信息的查询方式**：

递归查询：dns服务器收到客户端请求后，查询请求的域名信息，如果服务器本地没有此域

名的信息，则服务器再向其他的dns服务器去查，查到后，再把最终结果返回给客

户，如果其他所有dns服务器都没有的话，就返回“找不到此域名的相关记录“

迭代查询：dns服务器收到客户端请求后，查询请求的域名信息，如果服务器本地没有此域

名的信息，则服务器会告诉客户端一个可能知道此域名信息的dns服务器地址，让

客户端向那个dns服务器去查询

顺便讲一下windows的域控里的域，这个Domain虽然也叫域，使用的域名也和上面讲的一样，记录类型也是相通的。但企业局域网里用的windows域和互联网上的域是不互通的。windows域里的域名可以和互联网上的相同，但互联网上的用户并不能访问到它。windows里的域常用来做身份验证和组策略的应用。加了域的计算机在登录时使用域用户名，形如邮箱地址 user@winDomain.com 之类的。这个只是登录到局域网本地的域，不连到互联网上的可能存在的winDomain.com的邮箱服务器。为了不让windows域的域名解析到互联网上可能真实存在的服务器，我们常用的办法就是把首选DNS服务器设置为局域网域控制器的ip，比如10.128.1.20之类的。个人的建议是在企业内网应用的windows域的域名不要和互联网上的存在的域名相同，最好的做法是不使用.com/.net/.cn之类的后缀，推荐使用.local后缀，比如xxx.local

其他的先不讲了，以后有空再更新。

作者：Cof-Lee

2020-05-21