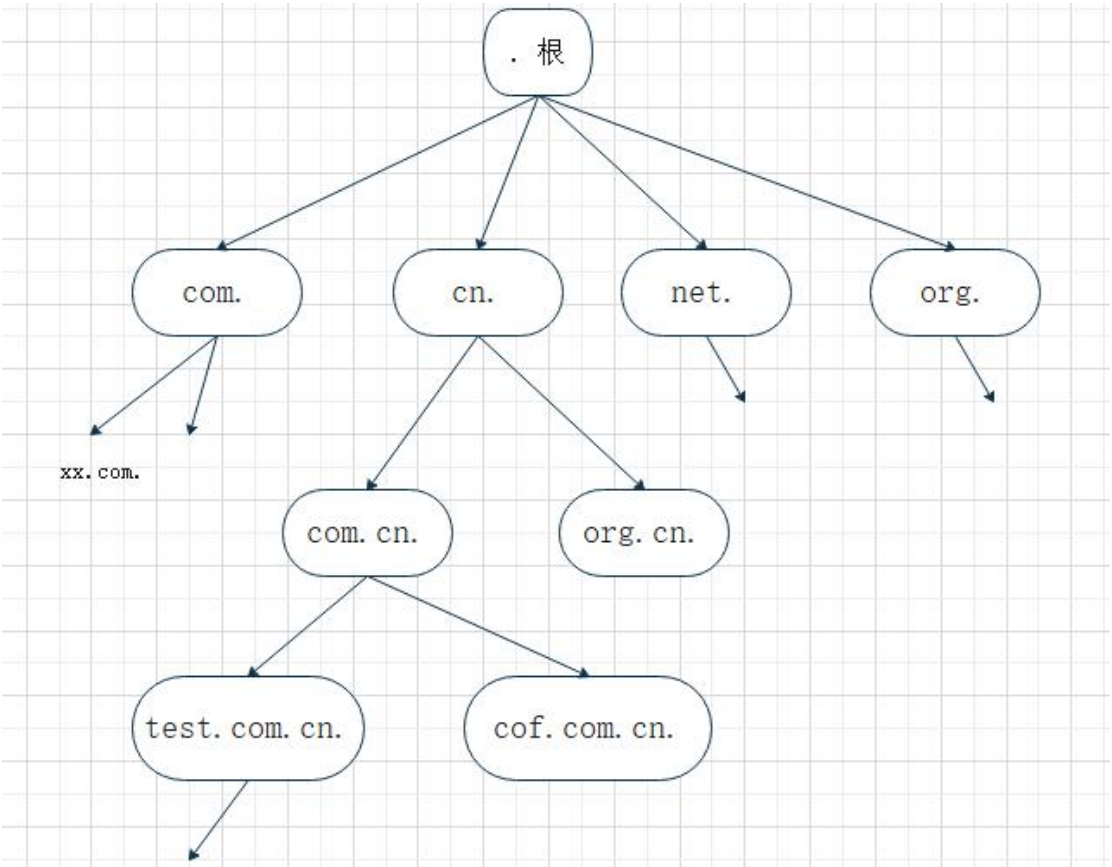
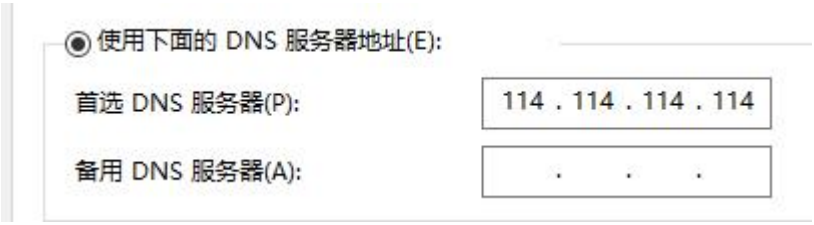
DNS 域名相关知识

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

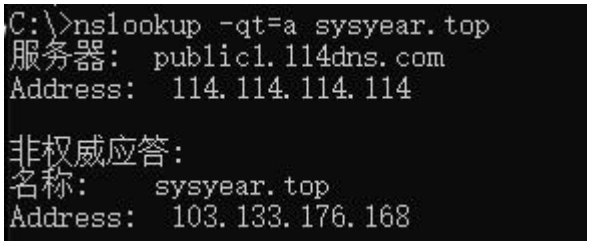
SOA 记录表示这个记录值所对应的 dns 服务器才是此域名所在域的最佳信息来源

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

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

```
C:\>nslookup -qt=mx sysyear.top
服务器:  public1.114dns.com
Address:  114.114.114.114

非权威应答:
sysyear.top     MX preference = 10, mail exchanger = 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

```
C:\>nslookup -qt=ns sysyear.top
服务器:  public1.114dns.com
Address:  114.114.114.114

DNS request timed out.
    timeout was 2 seconds.
非权威应答:
sysyear.top     nameserver = ns7.cnmsn.net
sysyear.top     nameserver = ns8.cnmsn.net
```

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

```
C:\>nslookup -qt=ptr 220.181.14.137
服务器:  public1.114dns.com
Address:  114.114.114.114

非权威应答:
137.14.181.220.in-addr.arpa     name = 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

```
C:\>nslookup -qt=ptr 137.14.181.220.in-addr.arpa
服务器:  public1.114dns.com
Address:  114.114.114.114

非权威应答:
137.14.181.220.in-addr.arpa     name = mr14137.mail.163.com
```

```
C:\>nslookup -qt=ptr 114.114.114.114.in-addr.arpa
服务器:  public1.114dns.com
Address:  114.114.114.114

非权威应答:
114.114.114.114.in-addr.arpa     name = public1.114dns.com
```

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