DNS原理与概念

风河 | www.nsbeta.info

内容大纲

- DNS基础
- DNS授权
- DNS查询

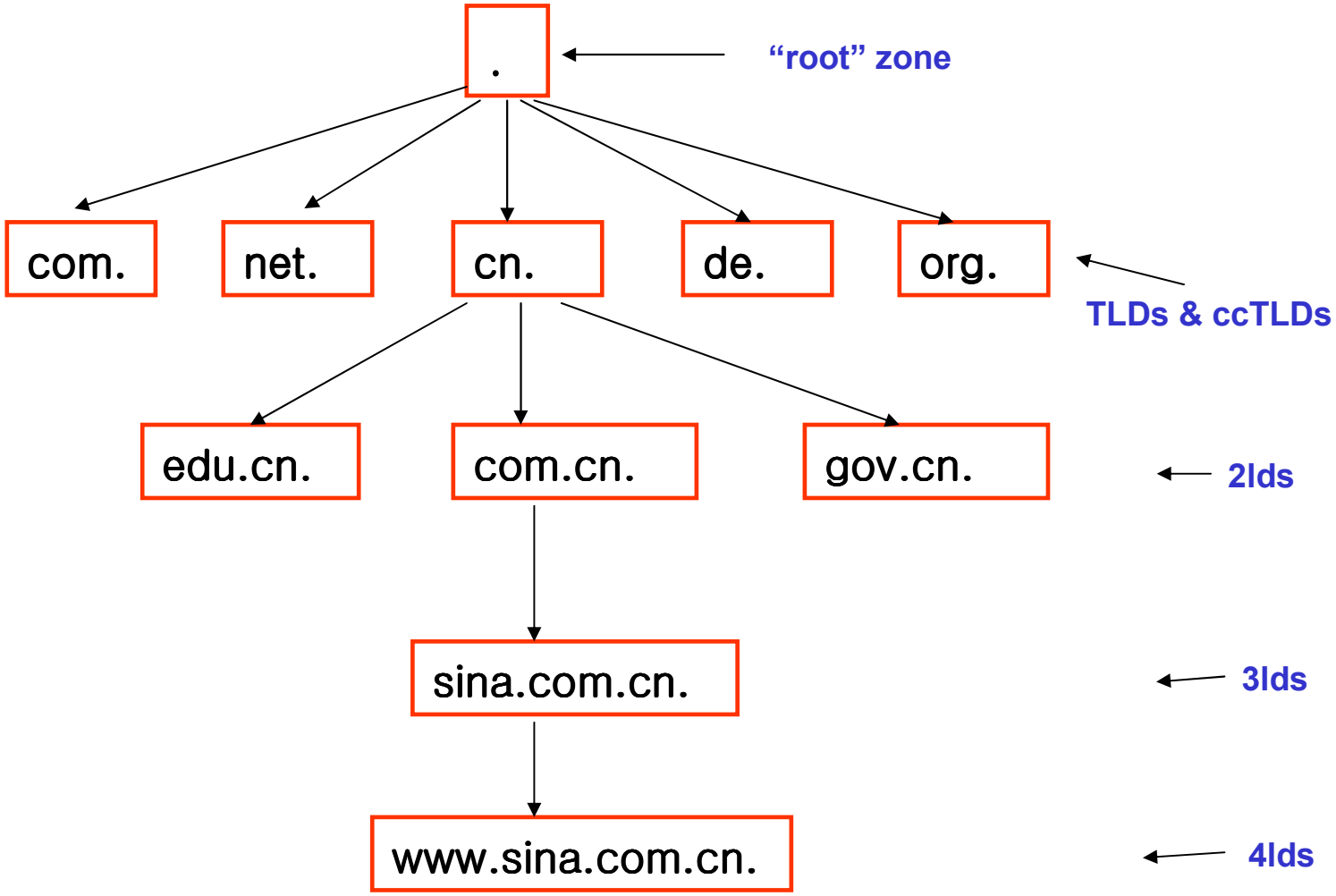
DNS是什么

- 因特网域名系统
- 提供名字到IP地址的映射，或反之
- 是分布式、C/S结构的服务
- 主要定义在RFC 1034和1035
- DNS发展历史？

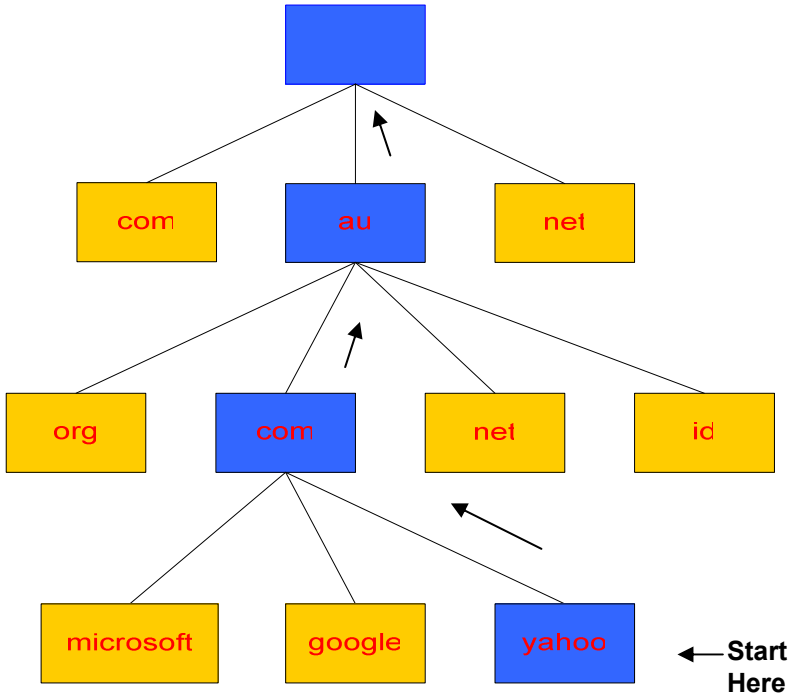
为什么需要DNS

- IP地址难以记忆和理解
- 邮件投递需要寻址（MX）
- 域身份鉴定（DomainKey、SPF）
- 负载均衡（轮询、最少连接）
- CDN、GSLB

DNS体系结构

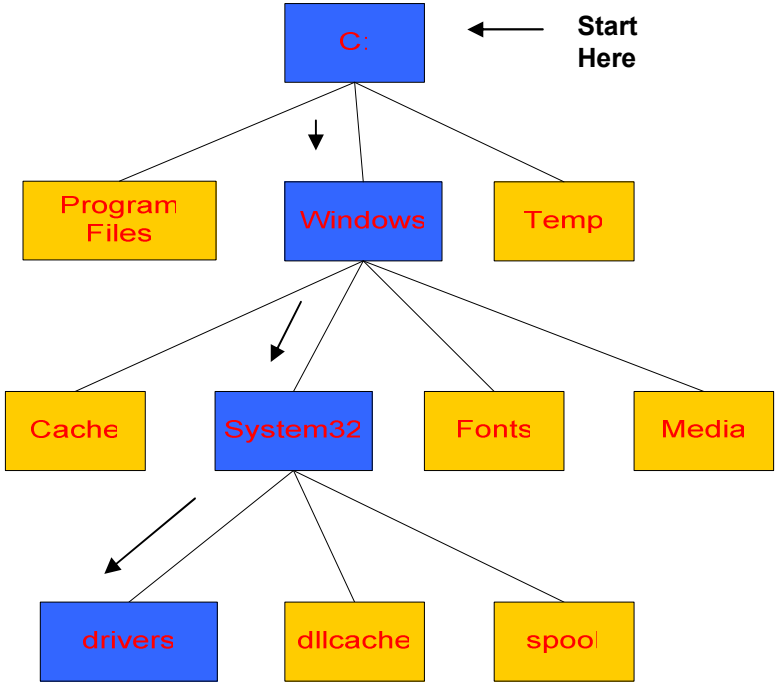

.
"root" zone
com.
net.
cn.
de.
org.
TLDs & ccTLDs
edu.cn.
com.cn.
gov.cn.
2lds
sina.com.cn.
3lds
www.sina.com.cn.
4lds

DNS命名规则



yahoo.com.au.

A “.” is used as separator



C:\windows\system32\drivers\

A “\” is used as separator

什么是域和域名

- “.”是域，是所有其他域的起始点
- 宇宙大爆炸：混沌初开，乾坤乃定

什么是域和域名

- com. net. info.是域
- aol.com. yy.com.也是域
- www.aol.com. game.yy.com.是域名

域与域名

- game.yy.com是一个域名，可以解析到IP地址
- 它同时也是一个域，有自己的SOA记录和NS记录
- 在DNS里，域与域名没有严格区别
- 区分域与域名，在于有没有定义ZONE*

*什么是zone？ BIND所使用的数据库，ZONE包含所有DNS记录（不包括子域的记录），格式定义在RFC1034和1035里。

域名与主机名

- 严格意义上，域名与主机名不同
- **www**、**ftp**是主机名*，但不是域名
- _http._srv.example.com是域名*，但不是主机名
- 标准的域名和主机名，只包括字母、数字、点和短横线
- 域名长度最大255位，单个label最大63位

DNS RR*

*什么是RR? RR全称是Resource Record，DNS资源记录符，包括名字、类型、族、TTL、长度、rdata元素

如何查看DNS RR

```
$ dig +nocmd duowan.com +noall +answer
duowan.com.          600     IN      A       120.132.133.62
```

dig more

```
dig duowan.com
```

```
dig duowan.com ns @8.8.8.8
```

```
dig duowan.com +short
```

```
dig duowan.com mx
```

```
dig duowan.com +trace
```

```
dig -x 61.144.56.100
```

```
dig duowan.com any
```

A记录

duowan.com.	600	IN	A	120.132.133.62

- 名字到IP地址的映射（IPV4）
- 一个名字可以有多个IP地址
- 一个IP地址也可以有多个名字

CNAME记录

www.nsbeta.info.	3600	IN	CNAME	nsbeta.info.

- CNAME定义别名
- 别名最终解析到A记录
- 别名具有唯一独占性*

MX记录

duowan.com.	600	IN	MX	10	mail.duowan.com.

- MX是MTA在进行邮件投递时，用来寻址的
- MX的值具有优先级，数字越低，优先级越高
- MX的值不能是IP地址和CNAME

NS记录

game.yy.com.	3600	IN	NS	dwdns1.nsbeta.info.
game.yy.com.	3600	IN	NS	dwdns2.nsbeta.info.

- game.yy.com域有两个权威名字服务器
- 任何对该域的查询，最终都由权威名字服务器解释
- NS起着胶水的作用，把整个DNS树串联起来
- NS的值不能是IP地址和CNAME

PTR记录

157.39.14.121.in-addr.arpa. 86400 IN PTR mail.chinaduo.com.

- PTR提供IP地址到名字的映射，俗称反解
- PTR由IP地址的拥有者而不是使用者设置
- 邮件发送服务器的IP必须设置PTR
- 互联网上DNS查询是正解多，还是反解多？

TXT记录

```
sina.com.          60      IN      TXT     "v=spf1 include:spf.sinamail.sina.com.cn -all"
```

- TXT提供关于主机或域的文本记录
- TXT包含内容为name=value的字串
- TXT通常用于反垃圾邮件（SPF、DomainKey）
- Google站点验证？

混合DNS记录

- 同一域名可以有多个不同类型的DNS记录

game.yy.com.	1800	IN	A	120.132.133.62

game.yy.com.	1800	IN	MX	10 mail.chinaduo.com.

game.yy.com.	3207	IN	NS	dwdns1.nsbeta.info.
game.yy.com.	3207	IN	NS	dwdns2.nsbeta.info.

- CNAME有什么问题？

TTL

duowan.com.	600	IN	A	120.132.133.62

- TTL是域名可以被缓存的周期，单位是秒
- TTL越长越稳定
- TTL越短越灵活
- 短TTL加大DNS查询量

问题

- 假如有个域名abc.com，设置如下DNS记录可以吗？

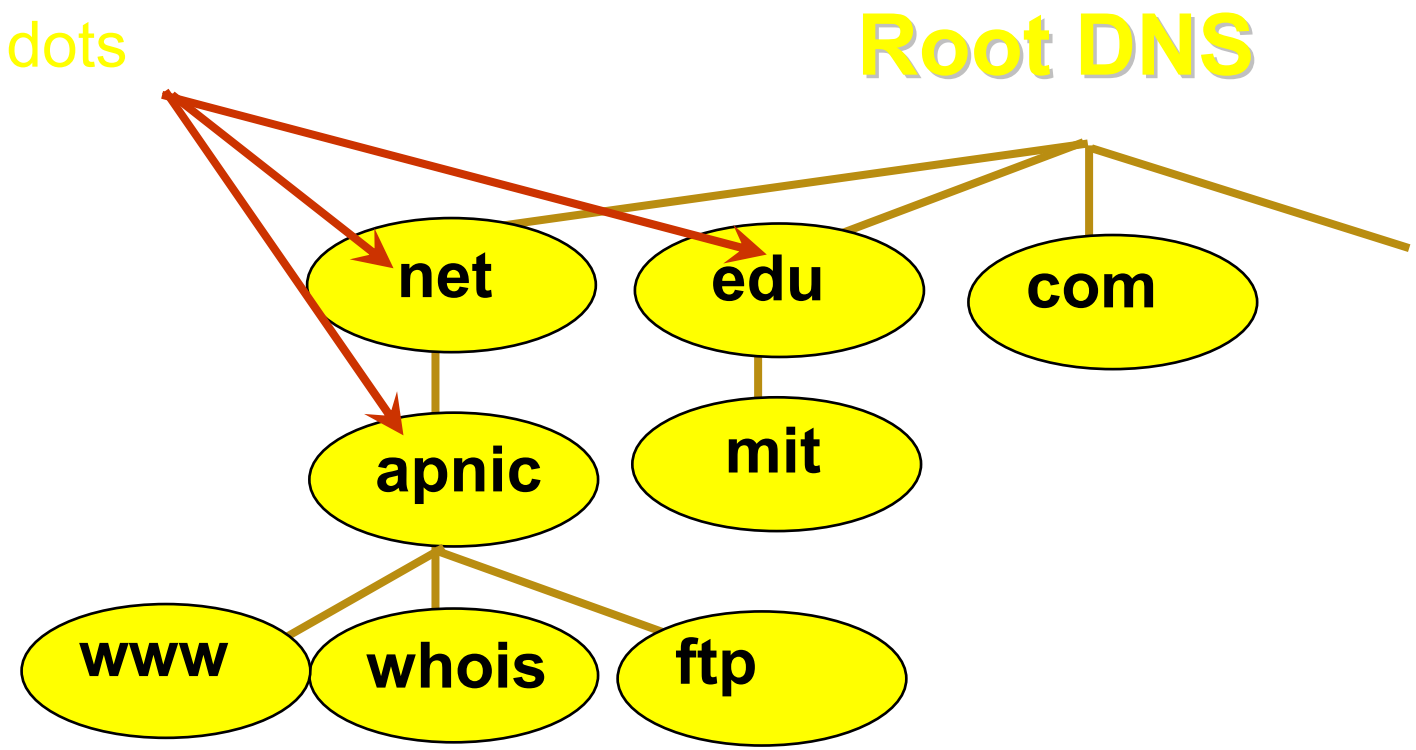
```
abc.com.        3600    IN      CNAME   xyz.com.
```

- 某个域名kongjian.info，它的MX记录是什么？这个MX记录有什么问题？

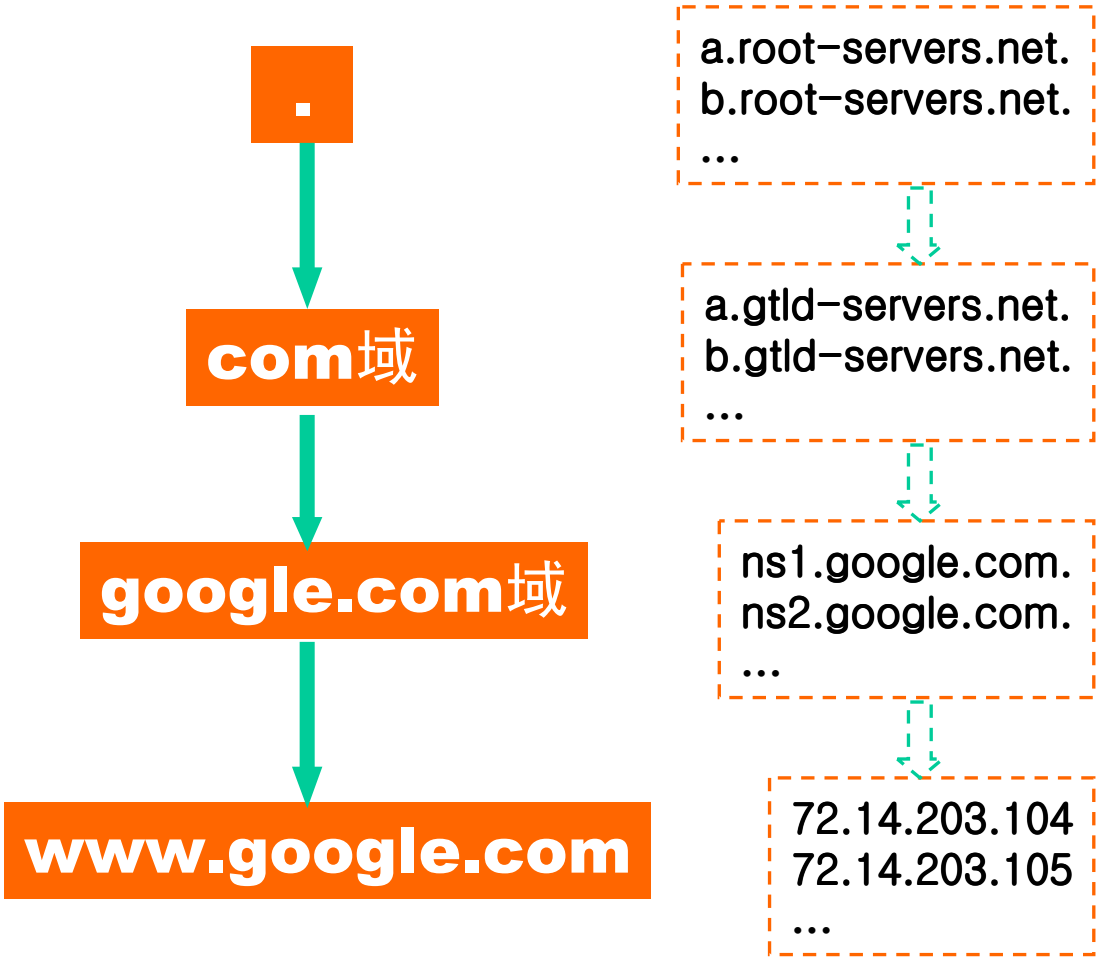
内容大纲

- DNS基础
- DNS授权
- DNS查询

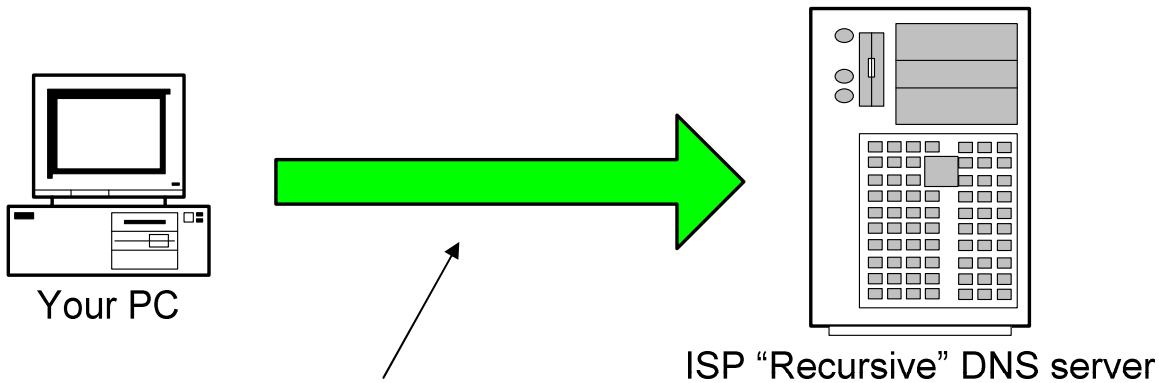
DNS授权



授权过程

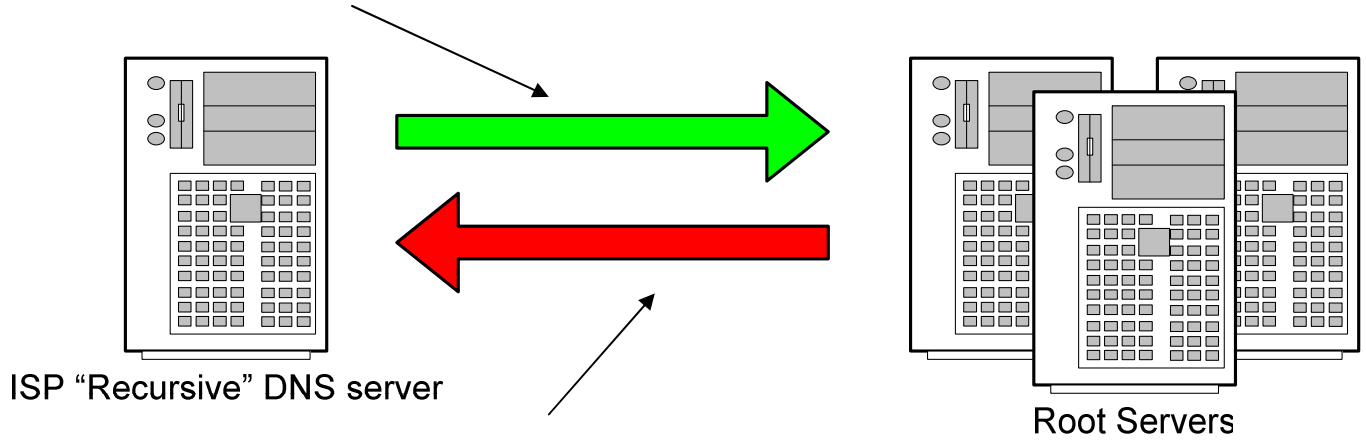

.
com域
google.com域
www.google.com
a.root-servers.net.
b.root-servers.net.
...
a.gtld-servers.net.
b.gtld-servers.net.
...
ns1.google.com.
ns2.google.com.
...
72.14.203.104
72.14.203.105
...

Step 1:PC对DNS服务器发起一个查询请求，查询www.google.com.



Step 2:DNS服务器向root DNS发出查询请求，查询www.google.com.

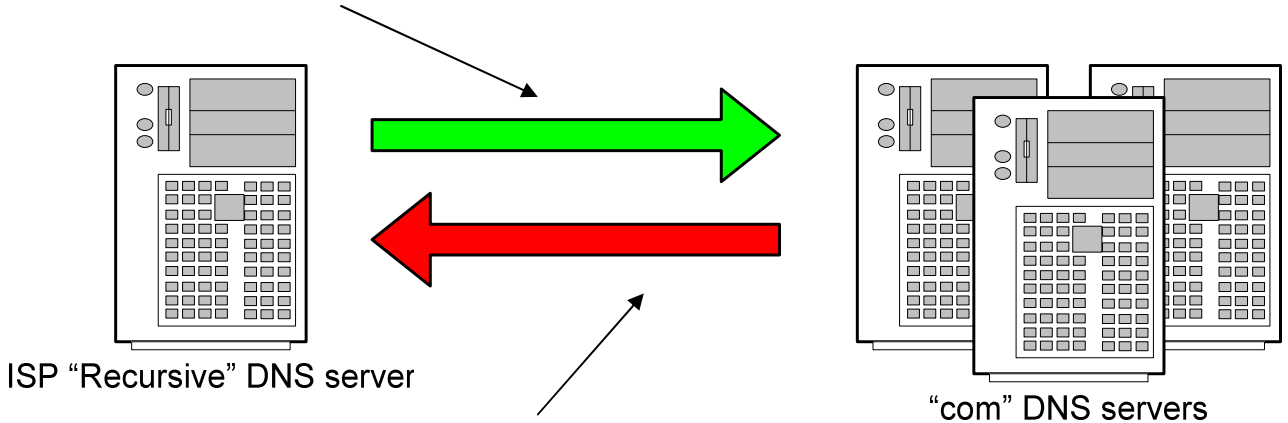
Tell me the Address of
"www.google.com"



I don't know the address but I know who's authoritative for the "com" domain ask them

Step 3:DNS服务器向com DNS发出查询请求，查询www.google.com.

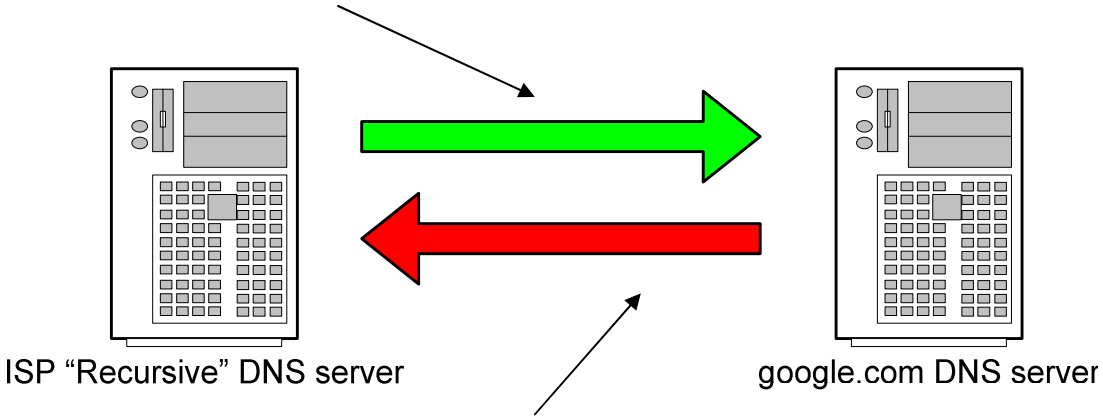
Tell me the Address of
"www.google.com"



I don't know the address but I know who's authoritative for the "google.com" domain ask them

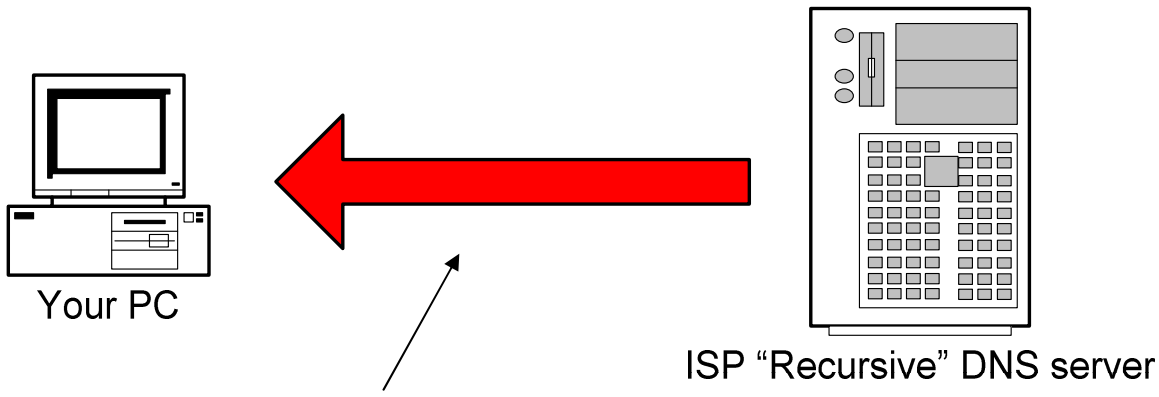
Step 4:DNS服务器向google DNS发出查询请求，查询www.google.com.

Tell me the Address of
"www.google.com"



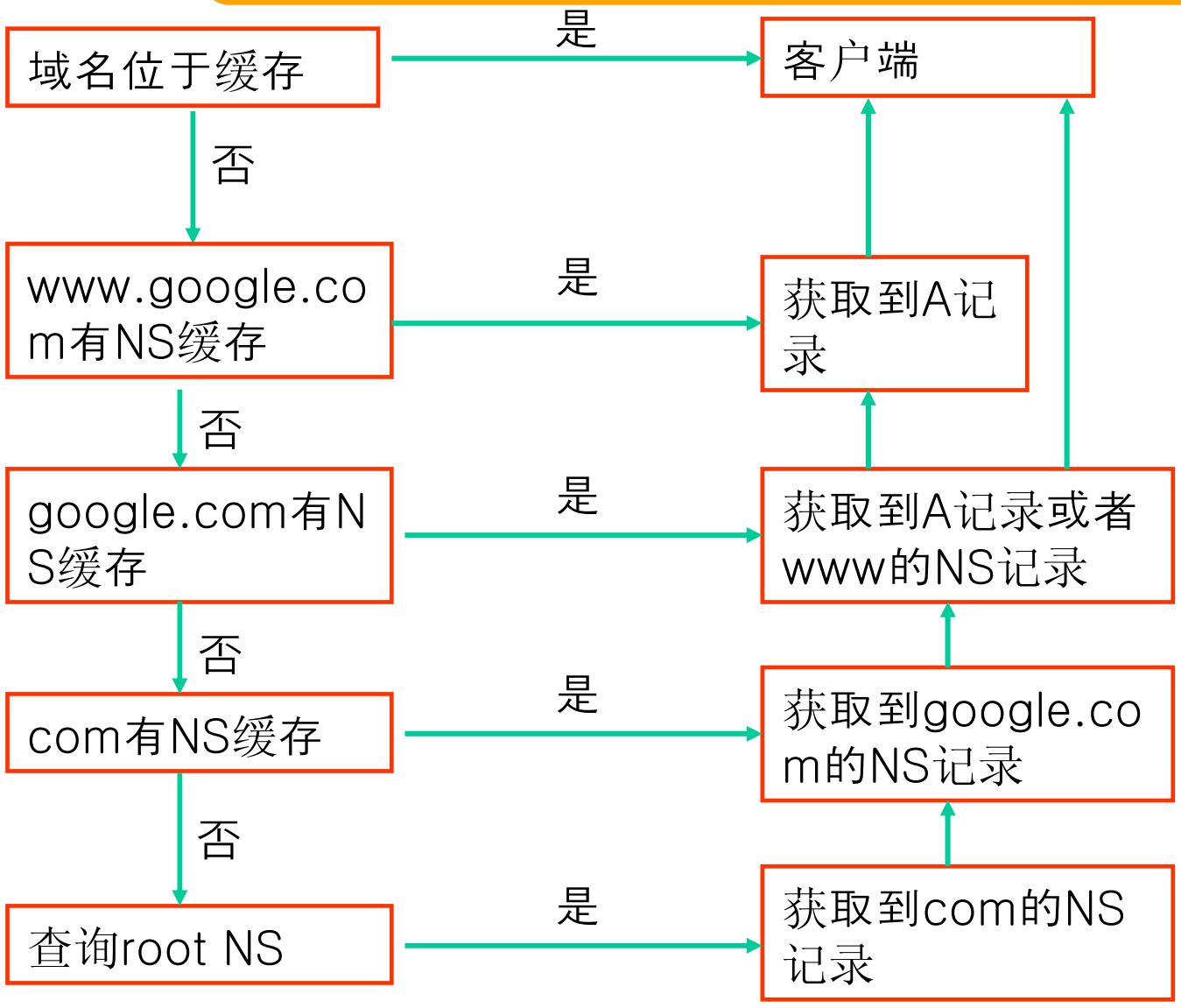
The Address of www.google.com
is 74.125.71.99

Step 5:DNS服务器将查询结果发回给客户端，并缓存一段时间.



The Address of www.google.com is 74.125.71.99

DNS服务器实际查询行为



问题

- 我们知道www.google.com由google.com的DNS服务器做权威解析，那么www.qq.com由qq.com的DNS服务器做权威解析吗？

- com和net的DNS服务器是什么？它们有什么共同点？一共有多少台，为什么是这个数量？

内容大纲

- DNS基础
- DNS授权
- DNS查询

递归解析、权威解析

- 公共DNS Cache负责递归解析
- 各个域的权威名字服务器负责本域的权威解析
- 简言之，递归解析所有域名，权威解析本域域名

递归解析、权威解析

- dig duowan.com @8.8.8.8 递归解析
- flags: qr rd ra;

- dig duowan.com @ns1.dnsv5.com 权威解析
- flags: qr aa rd;

- dig +norec?

递归查询

- 用户的电脑上网，发起一个DNS查询，这导致递归查询
- 递归查询是DNS缓存服务器直接响应结果给客户端
- 所有公共DNS都支持递归查询
- 权威服务器一般都关闭递归查询

迭代查询

- 迭代查询是客户端解析器发起查询时，父解析器返回一个引用（referral），客户端顺着这个引用逐级往下查询
- 客户端解析器必须能追随引用，才可以做到迭代查询
- 所有的stub resolver（例如windows的DNS组件）都不支持迭代查询
- 标准DNS服务器都支持迭代查询
- dig +trace是迭代查询吗?

澄清概念

- 递归解析、权威解析，是针对域名查询的响应类型
- 递归查询、迭代查询，是客户端查询域名的行为
- 前2个概念针对DNS服务器
- 后2个概念针对客户端解析器

关于DNS Cache

- 运营商的公共DNS都是Cache
- Cache一定是递归解析
- 域名的TTL对Cache影响很大

DNS安全

- 域名挟持
- 域名污染
- DNS攻击
- ……

如何解决？

DNS服务器

- 互联网DNS的标准就是ISC的BIND
- BIND通过zone文件来管理域和记录
- BIND可以递归解析和权威解析，或两者混合
- BIND可以结合DHCP动态更新域名
- BIND可以做智能DNS
- BIND完整支持DNSSEC

- **BIND配置管理？待续...**

参考书籍

- 入门：DNS & BIND第5版
- 提高：Pro DNS & BIND

推荐阅读第二本

问题

- 为什么用户访问的是DNS Cache，而不是权威NS？
- 如下查询有返回吗？有返回原因？无返回原因？

```
dig +norec game.yy.com @8.8.8.8 +short
```

Question?

谢谢！