DNS原理及其解析过程【精彩剖析】 - 系统网络运维 - 51CTO技术博客

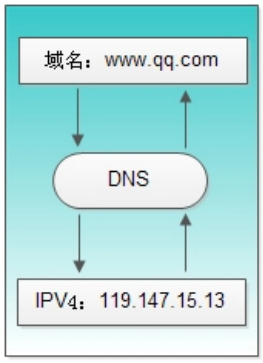
DNS原理及其解析过程

精彩剖析

网络通讯大部分是基于TCP/IP的，而TCP/IP是基于IP地址的，所以计算机在网络上进行通讯时只能识别如“202.96.134.133”之类的IP地址，而不能认识域名。我们无法记住10个以上IP地址的网站，所以我们访问网站时，更多的是在浏览器地址栏中输入域名，就能看到所需要的页面，这是因为有一个叫“DNS服务器”的计算机自动把我们的域名“翻译”成了相应的IP地址，然后调出IP地址所对应的网页。

什么是DNS？

DNS(Domain Name System)是“域名系统”的英文缩写，是一种组织成域层次结构的计算机和网络服务命名系统，它用于TCP/IP网络，它所提供的服务是用来将主机名和域名转换为IP地址的工作。DNS就是这样的一位“翻译官”，它的基本工作原理可用下图来表示。

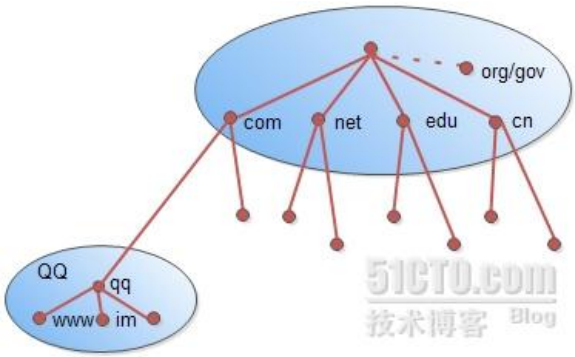


DNS域名称

域名系统作为一个层次结构和分布式数据库，包含各种类型的数据，包括主机名和域名。DNS数据库中的名称形成一个分层树状结构称为域命名空间。域名包含单个标签分隔点，例如：im.qq.com。

完全限定的域名 (FQDN) 唯一地标识在 DNS 分层树中的主机的位置，通过指定的路径中点分隔从根引用的主机的名称列表。 下图显示与主机称为 im 内 qq.com DNS 树的示例。 主机的 FQDN 是 im.qq.com。

DNS 域的名称层次结构



DNS域名称空间的组织方式

按其功能命名空间中用来描述 DNS 域名称的五个类别的介绍详见下表中，以及与每个名称类型的示例。

名称类型	说　明	示　例
根域	DNS域名中使用时，规定由尾部句点(.)来指定名称位于根或更高级别的域层次结构	单个句点 (.) 或句点用于末尾的名称
顶级域	用来指示某个国家/地区或组织使用的名称的类型名称	.com
第二层域	个人或组织在 Internet 上使用的注册名称	qq.com
子域	已注册的二级域名派生的域名，通俗的讲就是网站名	www.qq.com
主机名	通常情况下，DNS 域名的最左侧的标签标识网络上的特定计算机，如h1	h1.www.qq.com

51CTO.com 技术博客 Blog

DNS 和 Internet 域

互联网域名系统由名称注册机构负责维护分配由组织和国家/地区的顶级域在 Internet 上进行管理。 这些域名按照国际标准 3166。 一些很多现有缩写，保留以供组织中，以及两个字母和三个字母的国家/地区使用的缩写使用下表所示。一些常见的DNS域名称如下图：

DNS域名称	组织类型
com	商业公司
edu	教育机构
net	网络公司
gov	非军事政府机构
Mil	军事政府机构
xx	国家/地区代码(cn表中国)
….	….

资源记录

DNS 数据库中包含的资源记录 (RR)。 每个 RR 标识数据库中的特定资源。我们在建立DNS服务器时，经常会用到SOA,NS,A之类的记录，在维护DNS服务器时，会用到MX，CNAME记录。

常见的RR见下图：

说 明	类	时间(ttl)	类型	数 据
起始授权机构	互联网 (IN)	默认值为60分钟	SOA	所有者名称 主名称服务器 DNS 名称、 序列号 刷新间隔 重试间隔 过期时间 最小 TTL
主机	互联网 (IN)	记录特定 TTL （如果存在），否则区域 （SOA） TTL	A	所有者名称 （主机的 DNS 名称） 主机 IP 地址
名称服务器	互联网 (IN)	记录特定 TTL （如果存在），否则区域 （SOA） TTL	NS	所有者名称 名称服务器 DNS 名称
邮件交换器	互联网 (IN)	记录特定 TTL （如果存在），否则区域 （SOA） TTL	MX	所有者名称 邮件 Exchange Server DNS 名称的首选项值
别名	互联网 (IN)	记录特定 TTL （如果存在），否则区域 （SOA） TTL	CNAME	所有者名称 （别名） 主机的 DNS 名称

Dns服务的工作过程

当 DNS 客户机需要查询程序中使用的名称时，它会查询本地DNS 服务器来解析该名称。客户机发送的每条查询消息都包括3条信息，以指定服务器应回答的问题。

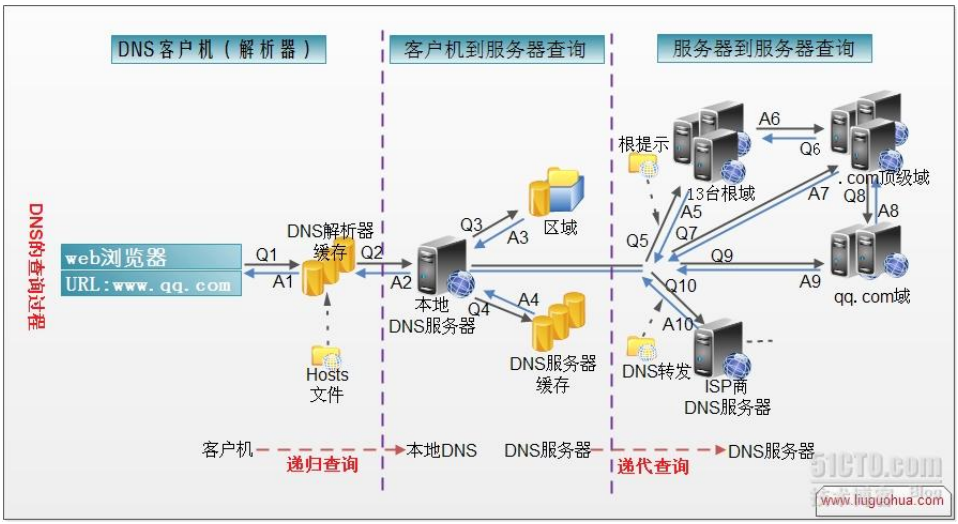
- 指定的 DNS 域名，表示为完全合格的域名 (FQDN) 。
- 指定的查询类型，它可根据类型指定资源记录，或作为查询操作的专门类型。
- DNS域名的指定类别。

对于DNS 服务器，它始终应指定为 Internet 类别。例如，指定的名称可以是计算机的完全合格的域名，如 im.qq.com，并且指定的查询类型用于通过该名称搜索地址资源记录。

DNS 查询以各种不同的方式进行解析。客户机有时也可通过使用从以前查询获得的缓存信息就地应答查询。DNS 服务器可使用其自身的资源记录信息缓存来应答查询，也可代表请求客户机来查询或联系其他 DNS 服务器，以完全解析该名称，并随后将应答返回至客户机。这个过程称为递归。

另外，客户机自己也可尝试联系其他的 DNS 服务器来解析名称。如果客户机这么做，它会使用基于服务器应答的独立和附加的查询，该过程称作迭代，即DNS服务器之间的交互查询就是迭代查询。

DNS 查询的过程如下图所示。



1、在浏览器中输入www.qq.com域名，操作系统会先检查自己本地的hosts文件是否有这个网址映射关系，如果有，就先调用这个IP地址映射，完成域名解析。

2、如果hosts里没有这个域名的映射，则查找本地DNS解析器缓存，是否有这个网址映射关系，如果有，直接返回，完成域名解析。

3、如果hosts与本地DNS解析器缓存都没有相应的网址映射关系，首先会找TCP/ip参数中设置的首选DNS服务器，在此我们叫它本地DNS服务器，此服务器收到查询时，如果要查询的域名，包含在本地配置区域资源中，则返回解析结果给客户机，完成域名解析，此解析具有权威性。

4、如果要查询的域名，不由本地DNS服务器区域解析，但该服务器已缓存了此网址映射关系，则调用这个IP地址映射，完成域名解析，此解析不具有权威性。

5、如果本地DNS服务器本地区域文件与缓存解析都失效，则根据本地DNS服务器的设置（是否设置转发器）进行查询，如果未用转发模式，本地DNS就把请求发至13台根DNS，根DNS服务器收到请求后会判断这个域名(.com)是谁来授权管理，并会返回一个负责该顶级域名服务器的一个IP。本地DNS服务器收到IP信息后，将会联系负责.com域的这台服务器。这台负责.com域的服务器收到请求后，如果自己无法解析，它就会找一个管理.com域的下一级DNS服务器地址(qq.com)给本地DNS服务器。当本地DNS服务器收到这个地址后，就会找qq.com域服务器，重复上面的动作，进行查询，直至找到www.qq.com主机。

6、如果用的是转发模式，此DNS服务器就会把请求转发至上一级DNS服务器，由上一级服务器进行解析，上一级服务器如果不能解析，或找根DNS或把转请求转至上上级，以此循环。不管是本地DNS服务器用是是转发，还是根提示，最后都是把结果返回给本地DNS服务器，由此DNS服务器再返回给客户机。

从客户端到本地DNS服务器是属于递归查询，而DNS服务器之间就是的交互查询就是迭代查询。

附录：

本地DNS配置转发与未配置转发数据包分析

新建一DNS，具体怎么建我这里就不再描述了，见我的上一篇博文《在Win2003中安装bind【部署智能DNS】》

1、DNS服务器不设转发

在192.168.145.228服务器上安装上wireshark软件，并打开它，设置数据包为UDP过滤，在192.168.145.12客户机上用nslookup命令查询一下www.sohu.com，马上可以看到本地DNS服务器直接查全球13台根域中的某几台，然后一步步解析，通过递代的方式，直到找到www.sohu.com对应的IP为220.181.118.87。

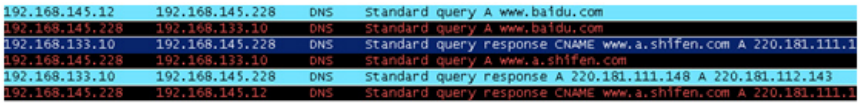
本地DNS服务器得到www.sohu.com的IP后，它把这个IP返回给192.168.145.12客户机，完成解析。

192.168.145.228	192.48.79.30	DNS	Standard query A www.sohu.com
192.168.145.228	192.26.92.30	DNS	Standard query A www.sohu.com
192.168.145.152	234.34.23.234	UDP	Source port: 3737 Destination port: 33674
192.168.145.228	192.35.51.30	DNS	Standard query A www.sohu.com
192.168.145.12	192.168.145.228	DNS	Standard query A www.sohu.com
192.168.145.228	192.33.14.30	DNS	Standard query A www.sohu.com
192.33.14.30	192.168.145.228	DNS	Standard query response
192.168.145.228	121.14.0.41	DNS	Standard query A www.sohu.com
121.14.0.41	192.168.145.228	DNS	Standard query response CNAME gs.a.sohu.com
192.168.145.228	61.135.179.169	DNS	Standard query A gs.a.sohu.com
192.168.145.228	220.181.26.167	DNS	Standard query A gs.a.sohu.com
220.181.26.167	192.168.145.228	DNS	Standard query response
192.168.145.228	220.181.26.169	DNS	Standard query A gs.a.sohu.com
220.181.26.169	192.168.145.228	DNS	Standard query response CNAME fzw.a.sohu.com A 220.181.118.87
192.168.145.228	221.179.180.22	DNS	Standard query A fzw.a.sohu.com
221.179.180.22	192.168.145.228	DNS	Standard query response A 220.181.26.7 A 220.181.118.87
192.168.145.228	192.168.145.12	DNS	Standard query response CNAME gs.a.sohu.com CNAME fzw.a.sohu.
192.168.145.228	192.168.145.12	DNS	Standard query response CNAME gs.a.sohu.com CNAME fzw.a.sohu.

2、DNS服务器设置转发

```
forwarders {                    #把DNS请求转发至上一级DNS商
192.168.133.10;
};
```

因www.sohu.com域名在第一步的验证中使用过，有缓存，为了不受上步实验干扰，我们在客户机上192.168.145.12上nslookup www.baidu.com。从图上看，本地DNS把请求转发至192.168.133.10服务器，133.10服务器把得到的IP返回给本地DNS，然后本地DNS再把IP告诉DNS客户机，完成解析。



本文出自 “系统网络运维” 博客，请务必保留此出处http://369369.blog.51cto.com/319630/812889