应用层简介与域名系统DNS

前言

本文开始介绍应用层，传输层为应用进程提供了端到端的通信服务，但不同的网络应用的应用进程之间，还需要有不同的通信规则。因此在传输层协议之上，还需要有应用层协议。

应用层重要协议有：**DNS、HTTP、SMTP、POP3、DHCP（之前已介绍）、FTP。**

1.应用层

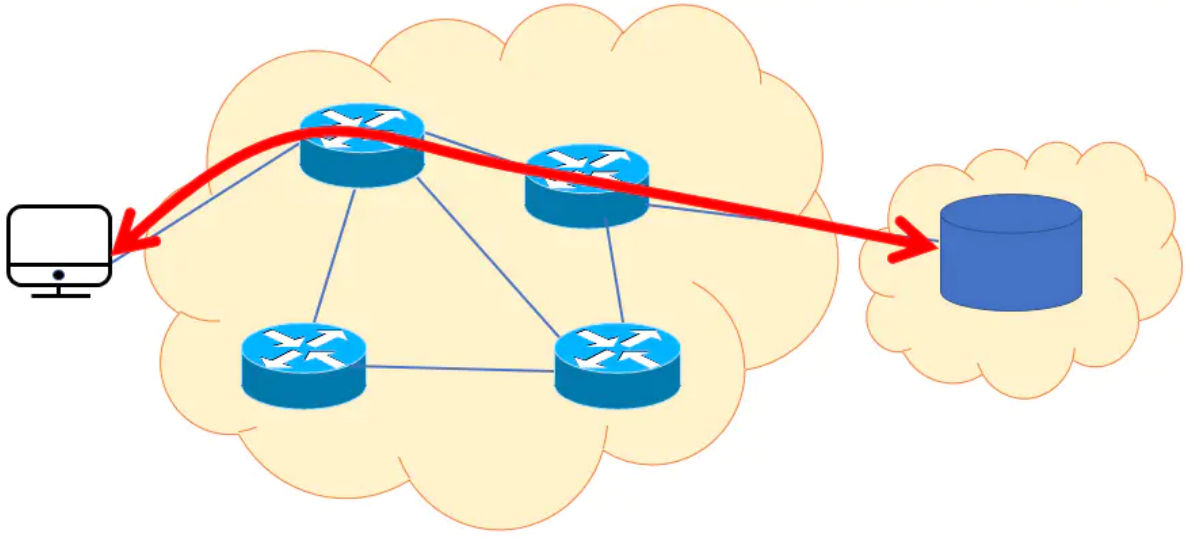
应用层对应用程序的通信提供服务。应用层协议具体应定义为：
(1) 应用进程交换的报文类型，如请求报文和响应报文。
(2) 各种报文类型的语法，如报文中的各个字段及其详细描述。
(3) 字段的语义，即包含在字段中信息的含义。
(4) 进程何时、如果发送报文，以及对报文的响应的规则。

2. 网络应用模型

现代网络应用程序中所使用的两种主流体系：**客户服务器模型和对等（P2P）模型。**

2.1客户服务器模型

客户（client）和服务器（server）都是指通信中涉及的两个**应用进程。**客户服务器方式所描述的是进程之间服务和被服务的关系。这里最主要的特征就是：**客户是服务请求方，服务器是服务提供方。**



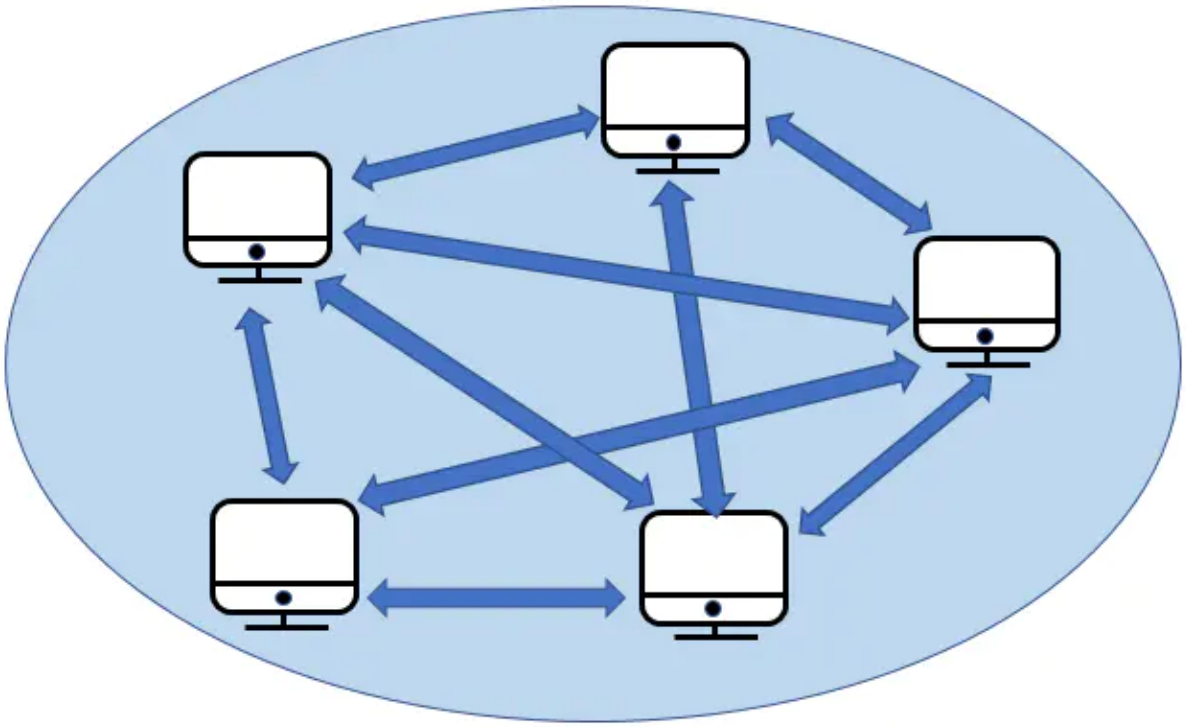
服务器是提供计算服务的设备。服务器有如下特点：

> (1) 永久提供服务。
> (2) 永久性访问地址/域名——即服务器IP地址固定不变。

客户是请求计算服务的主机。客户有如下特点：

> (1) 与服务器通信，使用服务器提供的服务。
> (2) 间歇性接入网络。
> (3) 可能使用动态的IP地址。
> (4) 不与其他客户直接通信。

2.2.对等模型



对等模型的特点是：

> (1) 不存在永远在线的服务器。
> (2) 每个主机既可以提供服务，也可以请求服务。
> (3) 任意端系统/节点之间可以直接通讯。
> (4) 节点间歇性接入网络，并且可能改变IP地址。
> (5) 自扩展性好。

3.域名系统DNS

域名系统DNS（Domain Name System）是互联网使用的命名系统，**用来将域名解析成IP地址。**

用户在与互联网中的主机通信时，必须知道对方的IP地址，但是32位IP地址太长不便于，即使使用点分十进制的方式也不容易记忆，所以实际中都是使用域名来与对方通信，如访问百度可以直接输入

www.baidu.com而不用使用百度服务器的IP地址。域名系统DNS就是把域名转换为IP地址。

3.1 域名

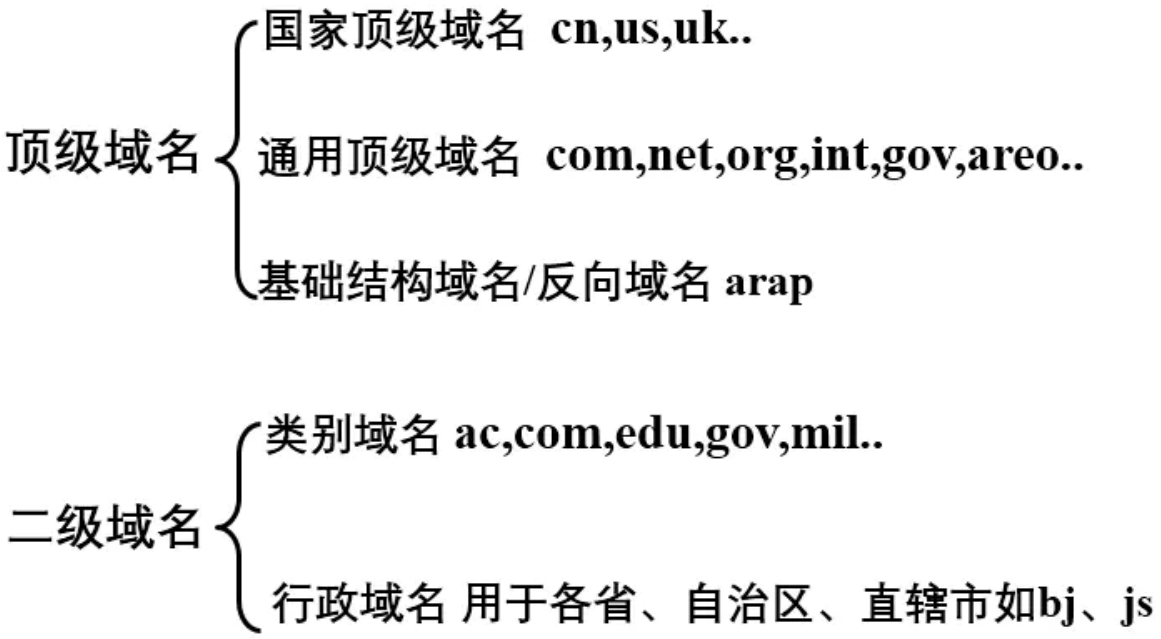
任何一个连接在互联网上的主机或路由器都有一个**唯一的层次结构**的名字，即域名。

每个域名都由**标号**序列组成，而各标号之间**用点隔开**。

如上图所示的域名，它由三个标号组成，其中，com是顶级域名，baidu是二级域名，www是三级域名。域名其实还有一个**根**，不过根没有名字，根下面才是顶级域名。

DNS规定，标号都是由英文字母和数字组成，每一个标号**不超过63个字符**（但为了记忆，最好不超过12个字符），也**不区分大小写。**标号中除了字符(-)外不能使用其他标点符号。级别最低的域名写在最左边，而级别最高的顶级域名写在最右边。**由多个标号组成的完整域名总共不超过255个字符。**

下图给出了顶级域名和二级域名的分类

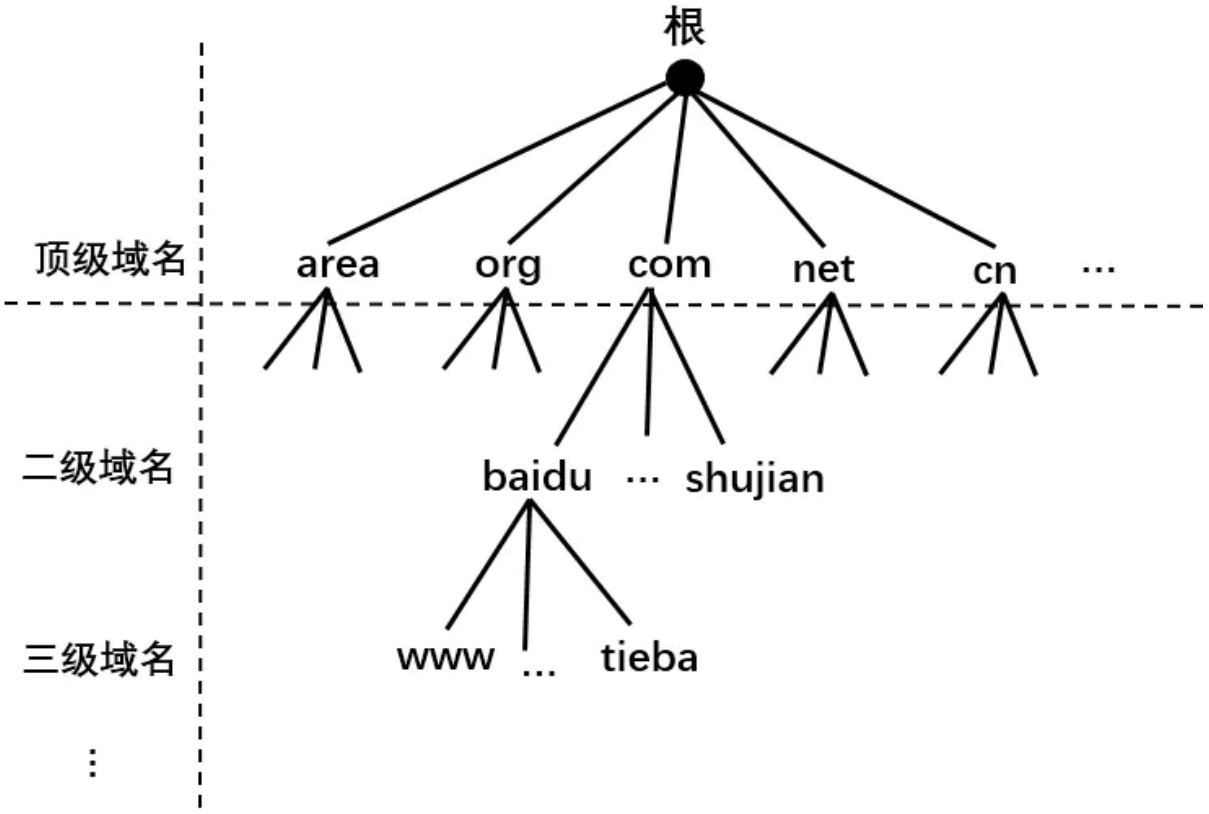


> cn,us,uk：中国、美国、英国。
> com：公司企业。net：网络服务器机构。org：非营利性组织。
> int：国际组织。gov：政府部门。areo：航空运输企业。

> arap：反向域名。
> ac：科研机构。edu：教育机构。mil：军事机构。
> bj：北京。js：江苏。

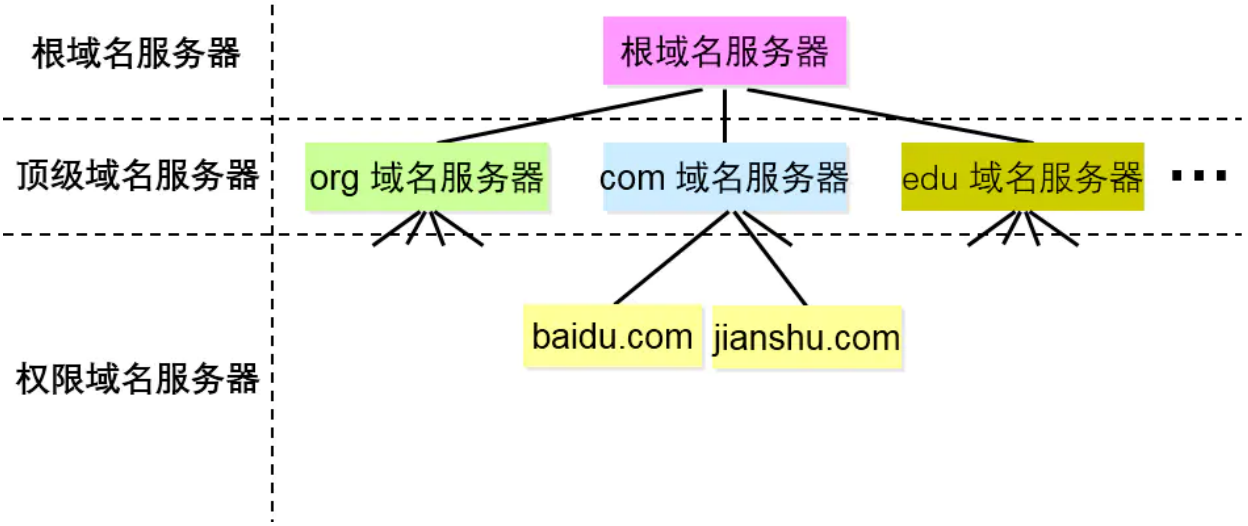
上面的二级域名和顶级域名有重复。如当顶级域名使用国家域名时，二级域名就可以使用和顶级域名的重复的那些域名。

DNS中使用的所有名称集合构成了DNS**名称空间**。这个名称空间是分层的，当前的DNS名称空间是一棵域名树。如下图所示



3.2 域名服务器

一个服务器所负责的管辖的（或所有权限的）范围叫做**区**。各单位根据具体情况来划分自己管辖范围的**区**。但在一个区中的所有节点必须是能够连通的。每个区设置相应的**权限域名服务器**，用来保存该区中的所有主机域名到IP地址的映射。



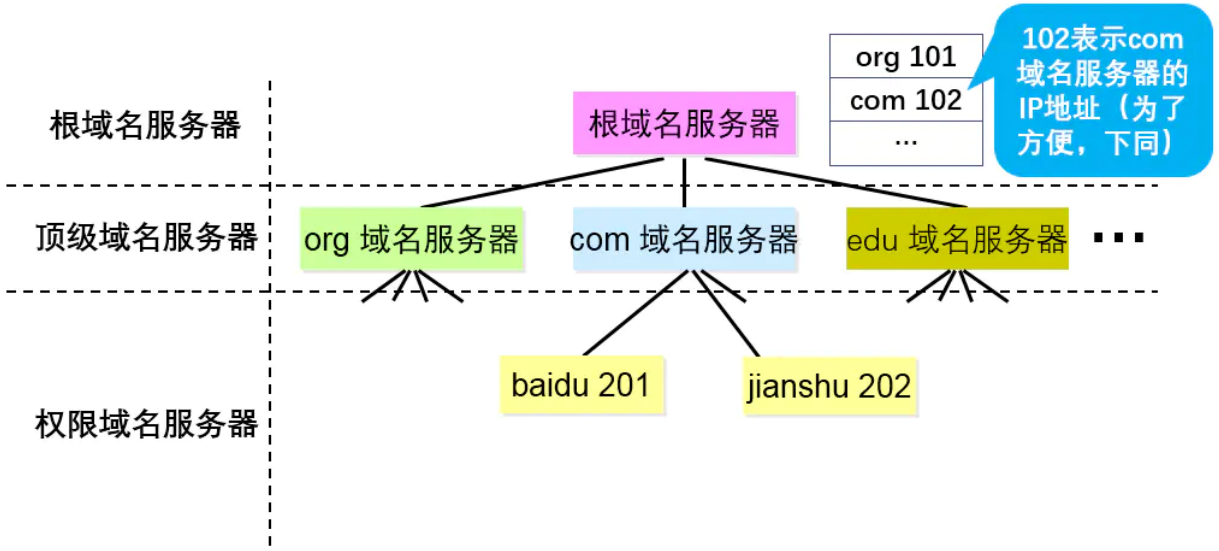
上图表示DNS域名服务器的树状结构图，每一个域名服务器都能够进行部分域名到IP地址的解析。DNS域名服务器是按层次安排的，每个域名服务器都只对域名体系中的一部分进行管辖。根据域名服务器所起的作用，可以把域名服务器分为以下四种类型：

(1) **本地域名服务器**（local name server）：又称**默认域名服务器**，本地域名服务器不属于上图的域名服务器层次结构，但它对域名系统非常重要。**当一台主机发出DNS查询请求时，这个查询报文就发给本地域名服务器。**

> 本地域名服务器离用户比较近，一般不超过几个路由器的距离，当所要查询的主机也属于同一个互联网服务提供者ISP，该本地域名服务器立即就能将所查询的主机名转换为它的IP地址，而不需要再去查询其他的域名服务器。

所以，本地域名服务器的存在，就会使得DNS查询的过程更加快速和便捷。

(2) **根域名服务器**（root name server）：根域名服务器是最高层次、最重要的域名服务器。**所有的根域名服务器都知道所有的顶级域名服务器的域名和IP地址。**不管哪一个本地域名服务器，如果要对互联网上任何一个域名进行解析（即转换为IP地址），只要自己无法解析，就首先求助于根域名服务器。如果所有的根域名服务器都瘫痪了，那么整个互联网中的DNS系统就无法工作。
通常情况下，根域名服务器并不直接把待查询的域名直接转换为IP地址（根域名服务器也没有存放这种信息），而是告诉本地域名服务器下一步应当找哪一个顶级域名服务器进行查询（下面域名解析过程中会详细介绍）。



> 如上图，假如要访问www.baidu.com，主机首先向本地域名服务器发送一个DNS查询请求，如果本地域名服务器缓存中没有这个域名对应的IP地址，那么本地域名服务器首先就求助于根域名服务器，而根域名服务器知道所有顶级域名服务器的IP地址，所以根域名服务器首先查看域名的顶级域名，顶级域名是com，所以根域名服务器就要将com域名服务器的IP地址即101告知给本地域名服务器。

(3) **顶级域名服务器**（TLD服务器）：顶级域名服务器负责管理在该顶级域名服务器注册的所有二级域名。当收到DNS查询请求时，就会给出相应的回答（可能是最后的结果，也可能是下一步应当找的域名服务器的IP地址）。

> 还是上例，访问www.baidu.com，根域名服务器告知了本地域名服务器com域名服务器的IP地址，本地域名服务器就求助于com域名服务器，com域名服务器中存放了对应不同二级域名的域名服务器的IP地址，如com域名服务器知道jianshu.com、baidu.com等所有xxx.com的对应域名服务的IP地址。com域名服务器就将baidu.com所对应的下一步的域名服务器告知给本地服务器。

(4) **权限域名服务器**：这就是前面说的权限域名服务器，它负责一个区，当权限域名服务器还不能给出最终的查询回答时，就会告诉发出查询请求的DNS客户，下一步应到找哪一个域名服务器。

为了提供域名服务器的可靠性，DNS域名服务器都把数据复制到几个域名服务器来保存，其中的一个是**主域名服务器**（master name server），其他的是**辅助域名服务器**（secondary name server）。当主域名服务器出现故障时，辅助域名服务器可以保证DNS的查询工作不会中断。

4.域名解析过程

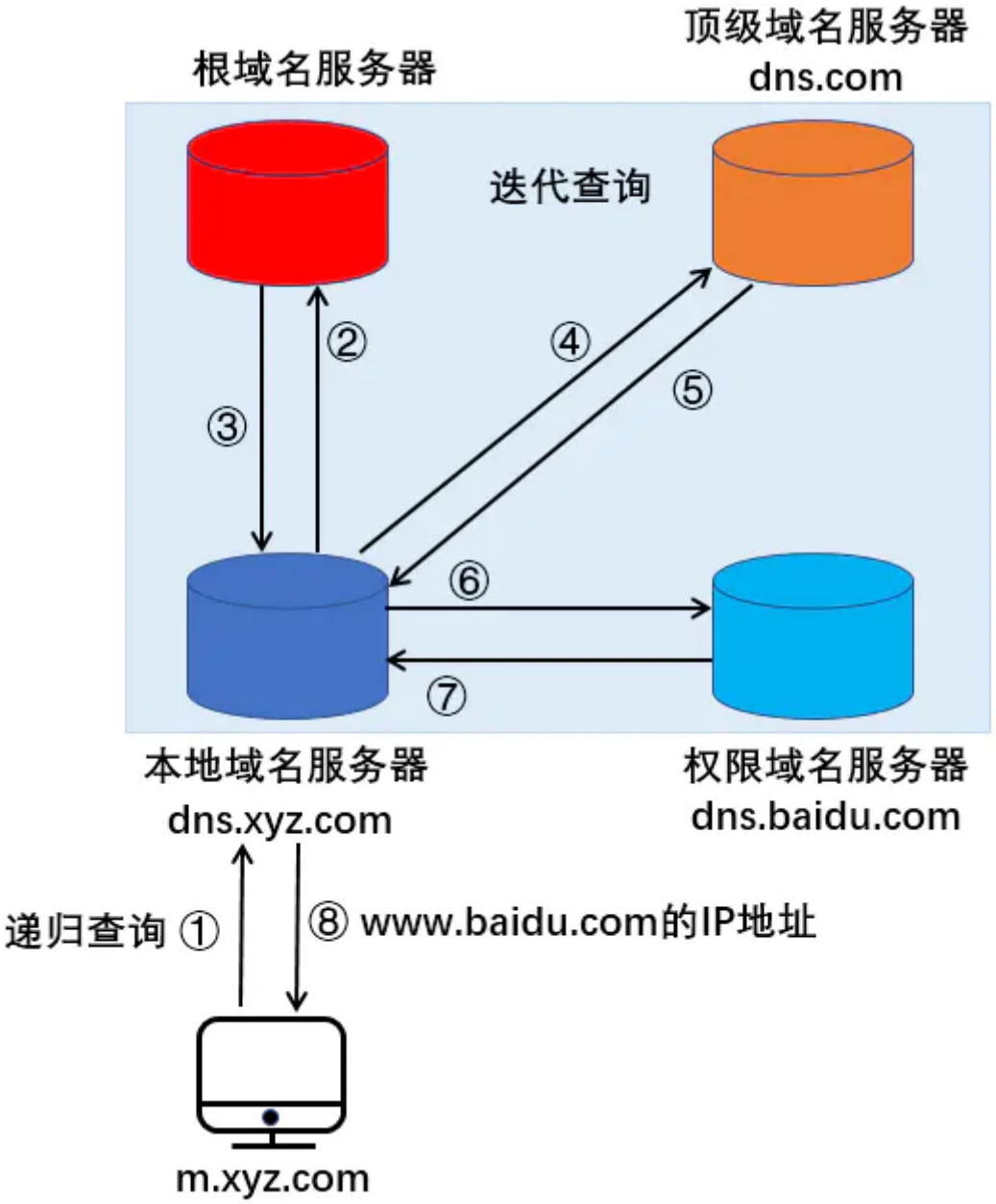
第一，**主机向本地域名服务器**的查询一般都是采用**递归查询**（recursive query）。所谓的递归查询就是：如果主机所询问的本地域名服务器不知道被查询域名的IP地址，那么本地域名服务器就以DNS客户的身份，向其他根域名服务器继续发出查询请求报文（即替该主机继续查询），而不是让该主机自己进行下一步查询。因此，递归查询返回的查询结果或者所要查询的IP地址，或者是报错，表示无法查询到所需的IP地址。

第二，**本地域名服务器向根域名服务器的查询**通常都是**迭代查询**（interative query）。迭代查询的特点是：当根域名服务器收到本地域名服务器发出的迭代查询请求报文时，要么给出所要查询的IP地

址，要么告诉本地域名服务器下一步需要查询的域名服务器，然后让本地服务器进行后续的查询而不是替本地域名服务器进行后续的查询。根域名服务器通常是把自己知道的顶级域名服务器IP地址告诉本地域名服务器，让本地域名服务器再向对应的顶级域名服务器查询。顶级域名服务器在收到本地域名服务器的查询请求后，要么给出所要查询的IP地址，要么告诉本地域名服务器下一步应当向哪个权限域名服务器进行查询，本地域名服务器就这样进行迭代查询。最后，知道了所要解析的域名的IP地址吗，然后把这个结果返回给发起查询的主机。当然，本地域名服务器也可以采用递归查询，这取决于最初的查询请求报文的设置是要求使用哪一种查询方式。

> 对本地服务器来说，递归查询靠别人，迭代查询靠自己。

举个例子说明一下两种查询的区别，假定域名为m.xyz.com的主机想要知道另一台主机（域名为www.baidu.com）的IP地址，下图表示几个查询的步骤：



(1) 主机m.xyz.com先向其本地域名服务器dns.xyz.com进行递归查询。

(2) 本地域名服务器采用迭代查询。它向一个根域名服务器查询。

(3) 根域名服务器告诉本地域名服务器，下一次应查询的顶级域名服务器dns.com的IP地址。

(4) 本地域名服务器向顶级域名服务器dns.com进行查询。

(5) 顶级域名服务器dns.com告诉本地域名服务器，下一次查询的权限域名服务器的dns.baidu.com的IP地址。

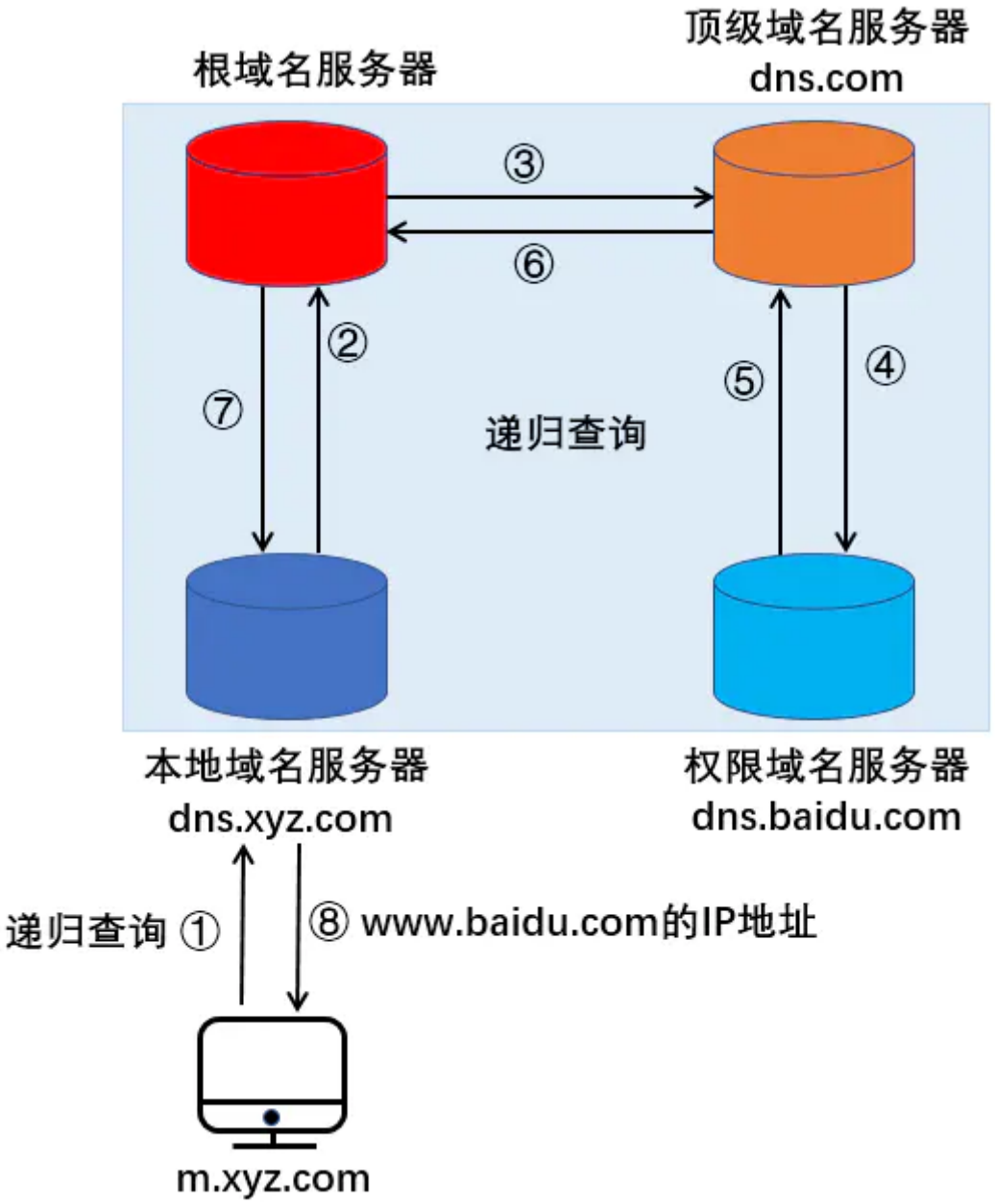
(6) 本地域名服务器向权限域名服务器dns.baidu.com进行查询。

(7) 权限域名服务器dns.baidu.com告诉本地域名服务器，所查询的主机的IP地址。

(8) 本地域名服务器dns.xyz.com最后把查询结果告知主机m.xyz.com。

> 这8个步骤共要使用8个UDP用户数据报（使用UDP是为了减少开销）的报文。本地域名服务器经过三次迭代查询后，从权限域名服务器dns.baidu.com得到了主机www.baidu.com的IP地址。

而对于本地域名服务器使用递归查询的情况下，本地域名服务器只需要向根域名服务器查询一次，后面的几次查询都是在其他域名服务器之间的进行的，即递归靠别人，同样，整个过程共使用了8个UDP报文。



为了提高DNS查询效率，并减轻根域名服务器的负荷和减少互联网上的DNS查询报文数量，在域名服务器中广泛使用了**高速缓存**（DNS缓存）。高速缓存用来**存放最近查询过的域名以及从何处获得域名映射信息的记录。**

> 例如，对于上例，如果在不久前已经有用户出查询过域名为www.baidu.com的IP地址，那么本地域名服务器就不必向根域名服务器重新查询www.baidu.com的IP地址，而是直接把高速缓存中存放的上次查询结果告诉用户。

> 假如本地域名服务器的缓存中没有www.baidu.com的IP地址，而是存放着顶级域名服务器dns.com的IP地址，那么本地域名服务器也可以不向根域名服务器进行查询，而是直接向com顶级域名服务器发送查询请求报文。

高速缓存不仅可以大大减少根域名服务器的负荷，而且也能使互联网的DNS查询请求和回答报文数量的大大减少。

由于名字到地址的绑定并不经常改变，为保持高速缓存中的内容正确，域名服务器应为每项内容设置计时器并处理超过合理时间的项（例如，每个项目只存方两天）。当域名服务器已从缓存中删去某项信息后又被请求查询该项信息，就必须重新到授权管理该项的域名服务器去绑定信息。当权限域名服务器回答一个查询请求时，在响应中都指明绑定的有效存在时间值。增加此时间值可减少网络开销，而减少此时间值可提高域名转换的准确性。

不但在本地域名服务器中需要高速缓存，在主机中也很需要。许多主机在启动时从本地域名服务器下载名字和地址的全部数据库，维护存放自己最近使用的域名的高速缓存，并且只在缓存中找不到名字时才使用本地域名服务器。维护本地域名服务器数据库的主机自然应该定期检查域名服务器以获取新的映射信息，而且主机必须从缓存中删除无效的项。由于域名改动并不频繁，大多数网点不需要花太多精力就能维护数据库的一致性。

5.小结