目录

---

1. DNS的作用

DNS的作用是实现主机名到IP的映射。我们在访问网站时，使用的是网站的域名，但是底层实际进行主机之间进行通信时，使用的却是IP地址，因此我们需要一个系统来实现主机名到IP的映射。

DNS（Domain Name System）将庞大的信息量划分为若干较小的组成部分，存储在不同的计算机上，需要找到映射的计算机可以寻找持有所需信息的**最近的**计算机。

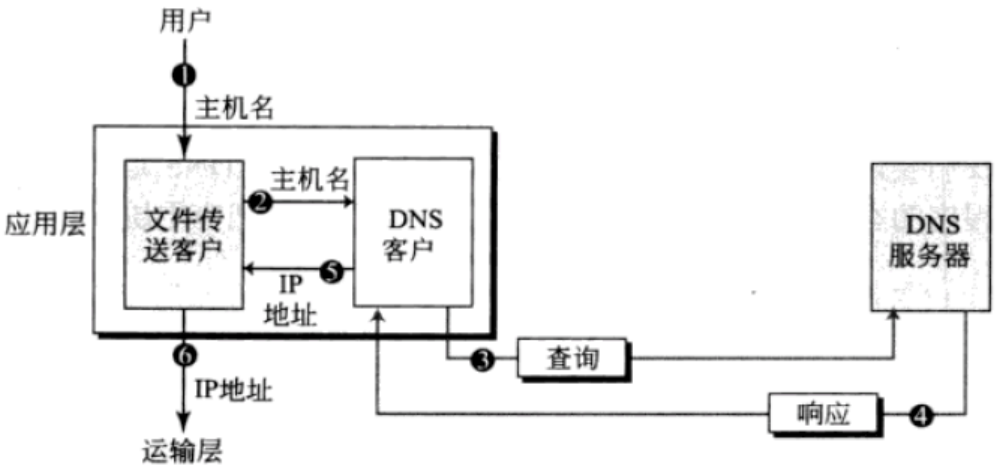

图 19.1　DNS 的作用

2. DNS的域名空间

DNS的域名空间是层次化的命名空间，每个名字都由几部分组成，第一部分描述组织性质，第二部分描述组织名字等等。

域名空间的可以用一棵多叉树来描述，这棵树最多有128层，每个节点最多可以有63个字符（label，标号），每个节点也都有一个域名，完全的域名用点号将标号序列隔开，从节点向上读到根。

- 完整域名：用一个空标号（label）结束，如：challenger.atc.fhda.edu.
- 不完整域名：不是以空字符串结束，如：challenger.atc.fhda.edu

域：域名空间的子树（域本身又可以分为很多个域）

域名空间的信息如何存储的呢?

如果使用一台计算机来存储如此大量的域名到IP的映射信息，一方面是会很低效（所有的请求都压在一台服务器上），另一方面也不可靠（出现故障会导致所有数据都不可用）。

为了解决第一个问题，我们使用**分层的服务器**，将域名体系结构分散的存储在若干个服务器上。上一层级的服务器仅保存到低一级的服务器的引用，更为详细的信息保留在低级别的服务器上。

根服务器：它的区包括整个树，不存储域的相关信息，而是把权限委托给其他服务器，根服务器仅保存到这些服务器的引用。

为了解决单点故障的问题，可以使用主从的架构：

- 主服务器：存储所管辖的区的文件，负责创建、更新和维护该区的文件
- 次服务器：作为其他服务器的备份，主要是为了增加数据的冗余度

3. 三种域

- 类属域

  按照主机的类别来来定义注册的主机。树中的每个节点定义一个域，是到空间数据库的索引。

- 国家域

  国家域使用两字符的国家或地区的缩写。

- 反向域

  用于将地址映射为名字

4. 名字解析

- 递归解析

  解析程序希望服务器能够提供最终的解答。

  如果请求的服务器就是该域名的权限服务器，那么就检查其数据库并相应，如果不是，就将请求发送给另一个服务器并等待响应，接收到响应之后再原路返回到请求的客户。

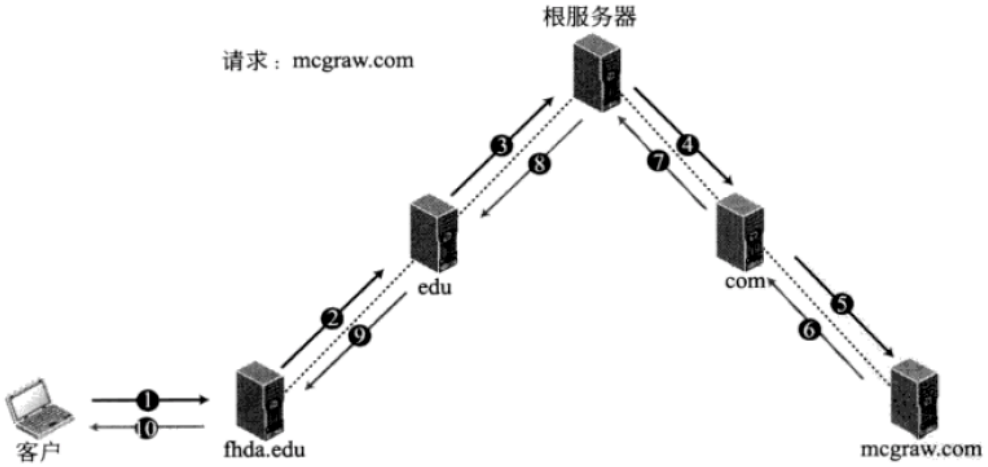

图 19.12　递归解析

- 迭代解析

  如果请求的服务器是域名的权限服务器，就发送解答响应，否则会发送能够解析该域名的服务器地址。

  客户得到地址之后会发起第二次请求

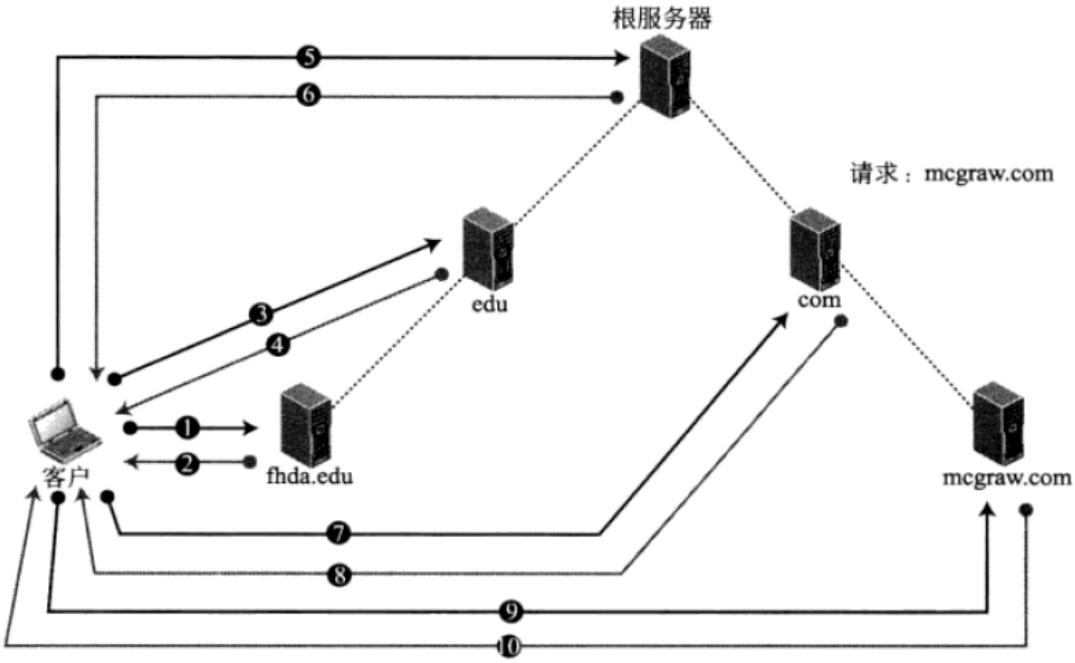

图 19.13　迭代解析

- 高速缓存

  当服务器接收到一个查询，但是该地址不在其域中，服务器需要查询其数据库，看在哪个服务器可以查到该信息，为了减少这种查找，DNS使用了高速缓存机制。

  当服务器从其他服务器上取得名字地址映射之后，会将该信息存储在自己的高速缓存中，以便下次客户端请求时不用再去其他服务器上请求。

  但是为了高速客户端响应来自高速缓存，服务器需要给响应标记为未授权的。此外，为了防止服务器将过期的信息发送给客户端，需要给缓存的信息增加一个生存时间。

5. 报文格式

DNS包含两种报文：查询和响应，两种报文的格式相同。查询报文包含一个首部和若干个问题记录，响应报文包含一个首部，问题记录，回答记录，授权记录和附加记录。

6. DNS的封装

DNS可以使用UDP也可以使用TCP，并且在两种情况的都是使用熟知端口53。

但是UDP会受到报文长度的限制，如果响应报文超过512字节就会使用TCP连接。

- 如果客户端事先知道响应报文的长度超过512字节，就应该使用TCP连接，比如次服务器请求主服务器的区传送，就必须使用TCP连接
- 如果客户端事先不知道响应报文的长度，可以先试用UDP端口，但是响应报文超过512字节时，服务器会截断响应报文，并将截断位置1，客户端收到响应之后会重新发起TCP连接进行请求。

7. DNS的安全性

- 攻击者可能会侦听请求和响应报文，用此类信息来**发现用户的特征**（看用户浏览了哪些网站）（DNS加密）
- 攻击者可能会截获DNS服务器的响应，并对其进行篡改，引导用户去其他站点（可以通过报文的原始鉴别和报文完整性措施来防止）
- 攻击者可能会对DNS服务器发起洪泛攻击

8. 面试中的答题思路

1. DNS实现的机制
    - DNS是干嘛的，提供了什么功能
    - 它的架构是什么样的：分布式架构
    - 解析过程：递归解析，迭代解析
2. DNS使用什么传输层协议
    - 客户端请求：UDP
    - 服务端之间的同步：TCP