应用层 - DNS

DNS概念

识别主机有两种方式，通过主机名或者 TP 地址 。 人们喜欢便于记忆的主机名标识方式，而路由器则喜欢定长的、有着层次结构的 IP 地址 。 为了折衷这些不同的偏好，我们需要一种能进行主机名到 IP 地址转换的目录服务。

这就是**域名系统（Domain Name System, DNS ）**的主要任务。

- 一个由**分层**的 DNS 服务器 （ DNS server ）实现的分布式数据库；
- 一个使得主机能够查询分布式数据库的**应用层协议** 。

DNS 服务器通常是运行 BIND (Berkeley Internet Name Domain ）软件的UNIX 机器 。 DNS 协议运行在 **UDP** 之上，使用 **53 号端口。**

> DNS： 通过客户 - 服务器模式提供的重要网络功能
>
> 与 HTTP、FTP 和 SMTP 协议一样， DNS 协议是应用层协议，其原因在于：(1)使用客户 - 服务器模式运行在通信的端系统之间；(2)在通信的端系统之间通过下面的端到端运输协议来传送 DNS 报文。
>
> 然而，在其他意义上， DNS 的作用非常不同于 Web 应用文件传输应用以及电子邮件应用 。 与这些应用程序不同之处在于， DNS 不是一个直接和用户打交道的应用 。 相反， DNS 是为因特网上的用户应用程序以及其他软件提供一种核心功能，即将主机名转换为其背后的 IP 地址。

DNS访问过程

考虑当某个用户主机上的一个浏览器（即一个 HTTP客户）请求 www. someschool. edu/index. html 页面时会发生什么现象 。 为了使用户的主机能够将一个 HTTP 请求报文发送到 Web 服务器 www. someschool. edu ， 该用户主机必须获得附www. someschool. edu 的 IP 地址。 其做法如下 。

- 同一台用户主机上运行着 DNS 应用的客户端。
- 浏览器从上述 URL 中抽取出主机名 www. someschool. edu ， 并将这台主机名传给DNS 应用的客户端。
- DNS 客户向 DNS 服务器发送一个包含主机名的请求。
- DNS 客户最终会收到一份回答报文，其中含有对应于该主机名的 IP 地址。
- 一旦浏览器接收到来自 DNS 的该 IP 地址，它向位于该 IP 地址 80 端口的服务器进程发起一个 TCP 连接。

DNS在两种情况下使用TCP

报文过长

其实当解析器发出一个request后，返回的response中的tc删节标志比特位被置1时，说明反馈报文因为超长而有删节。这是因为UDP的报文最大长度为512字节。解析器发现后，将使用TCP重发request，TCP允许报文长度超过512字节。既然TCP能将data stream分成多个segment，它就能用更多的segment来传送任意长度的数据。

UDP报文的最大长度为512字节，而TCP则允许报文长度超过512字节。当DNS查询超过512字节时，协议的TC标志出现删除标志，这时则使用TCP发送。通常传统的UDP报文一般不会大于512字节。

> 如何突破DNS报文的512字节限制_协议分析与还原-CSDN博客

> RFC 6891这份标准文档，对DNS进行了扩展，描述了超过512字节的DNS的情况，即EDNS0。
>
> 本文将首先描述DNS协议的长度限制情况，然后对EDNS0进行说明，接着用示例说明DNS工具在超过512字节时的通常情况，最后将介绍如何方便地产生超过512字节的UDP承载的DNS报文。大家可以根据需要，跳到对应章节查阅。

区域传输

另外一种情况是，DNS在进行区域传输的时候使用TCP协议，其它时候则使用UDP协议。
DNS的规范规定了2种类型的DNS服务器，一个叫**主DNS服务器**，一个叫**辅助DNS服务器。**在一个区中主DNS服务器从自己本机的数据文件中读取该区的DNS数据信息，而辅助DNS服务器则从区的主DNS服务器中读取该区的DNS数据信息。当一个辅助DNS服务器启动时，它需要与主DNS服务器通信，并加载数据信息，这就叫做**区传送（zone transfer**）。
辅域名服务器会定时（一般时3小时）向主域名服务器进行查询以便了解数据是否有变动。如有变动，则会执行一次区域传送，进行数据同步。区域传送将使用TCP而不是UDP，一是因为数据同步传送的数据量比一个请求和应答的数据量要多得多；二是因为TCP是一种可靠的连接，保证了数据的准确性。

DNS更多情况下使用UDP

客户端向DNS服务器查询域名，一般返回的内容都不超过512字节，用UDP传输即可。不用经过TCP三次握手，这样DNS服务器负载更低，响应更快。虽然从理论上说，客户端也可以指定向DNS服务器查询的时候使用TCP，但事实上，很多DNS服务器进行配置的时候，仅支持UDP查询包。