第十四章 DNS:域名解析

14.1 DNS介绍

域名系统(DNS)是一种用于TCP/IP应用程序的分布式数据库，他提供主机名字和IP地址之间的转换及有关电子邮件的选路信息。

这里提到的分布式是指在Internet上的单个站点不能拥有所有的信息。

DNS提供了允许服务器和客户端程序相通的协议。

对DNS的访问 是通过一个地址解析器(resolver)来完成的。

解析器通常是应用程序的一部分。解析器并不像TCP/IP协议那样是操作系统的内核。

操作系统内核中的TCP/IP协议族对于DNS一点都不知道。

14.2 DNS格式



DNS报文

DNS的报文格式：

报文由12字节长的首部和4个长度可变的字段组成。

标志字段：由客户端程序设置并由服务器返回结果，客户程序通过响应查询是否匹配。

QR是1bit字段：0表示查询报文，1表示响应报文

Opcode是一个4bit字段：通常 为0(标准查询)，其他值为1(反向查询)和2(服务器状态请求)。

AA是1bit标志，表示“授权回答”

TC是1bit字段，表示“截断的”

RD是1bit字段，表示“期望递归”

RA是1bit字段，表示“可用递归”

rcode是一个4bit的返回码字段。通常的值为0(没有差错)和3(名字差错)

随后的4个16bit字段说明最后4个变长字段中包含的条目数。对于查询报文，问题(question)数通常是1，而其它三项均为0。类似地，对于应答报文，回答数至少1，剩下的两下可以是0或非0。

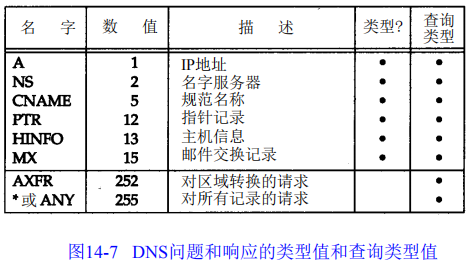
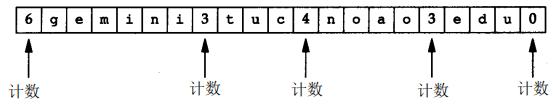
14.3 DNS查询报文中的问题部分

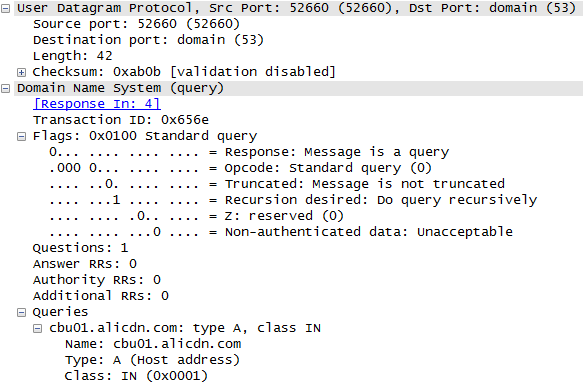
每个标识符以首字母字节的计数值来说明随后标识符的字节长度，每个名字以最后字节为0结束，长度为0的标识符是根标识符。计数字符的值必须是0~63的数，因为标识符的最大长度仅为63。

最常用的查询类型是A类型，表示期望获得查询名的IP地址。一个PTR查询则请求获得一个IP地址对应的域名。

查询类通常是1，指互联网地址。



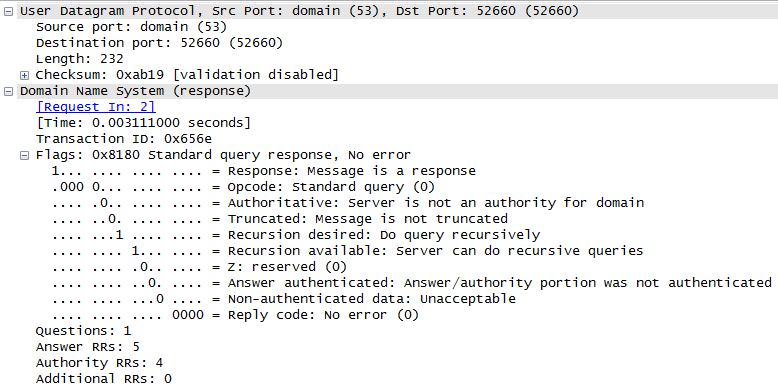


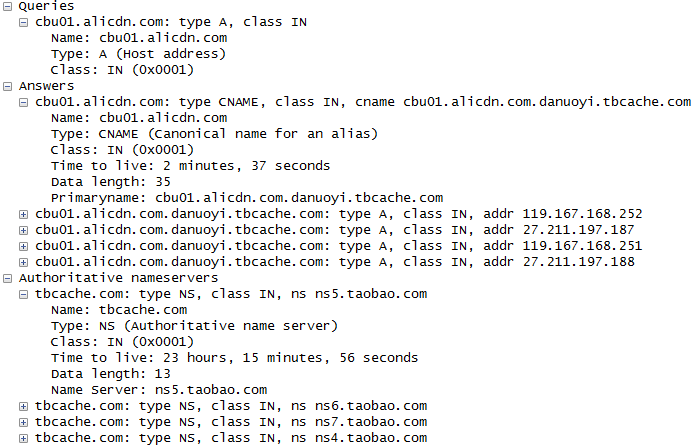


（a）DNS查询报文(Type:A Class:IN)

14.3 DNS回答报文中的回答部分







（a）DNS回答报文(Type:CNAME Class:IN)