1.DNS报文

1.1 DNS报文格式

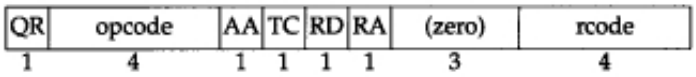
DNS只有两种报文：查询报文、回答报文，两者有着相同格式，如下：

1.2首部区域

标识数

对该查询进行标识，该标识会被复制到对应的回答报文中，客户机用它来匹配发送的请求与接收到的回答。

标志[1]



QR(1比特)：查询/响应的标志位，1为响应，0为查询。

opcode(4比特)：定义查询或响应的类型(若为0则表示是标准的，若为1则是反向的，若为2则是服务器状态请求)。

AA(1比特)：授权回答的标志位。该位在响应报文中有效，1表示名字服务器是权限服务器(关于权限服务器以后再讨论)

TC(1比特)：截断标志位。1表示响应已超过512字节并已被截断(依稀好像记得哪里提过这个截断和UDP有关，先记着)

RD(1比特)：该位为1表示客户端希望得到递归回答(递归以后再讨论)

RA(1比特)：只能在响应报文中置为1，表示可以得到递归响应。

zero(3比特)：不说也知道都是0了，保留字段。

rcode(4比特)：返回码，表示响应的差错状态，通常为0和3，各取值含义如下：

0 无差错

1 格式差错

2 问题在域名服务器上

3 域参照问题

4 查询类型不支持

5 在管理上被禁止

6 -- 15 保留

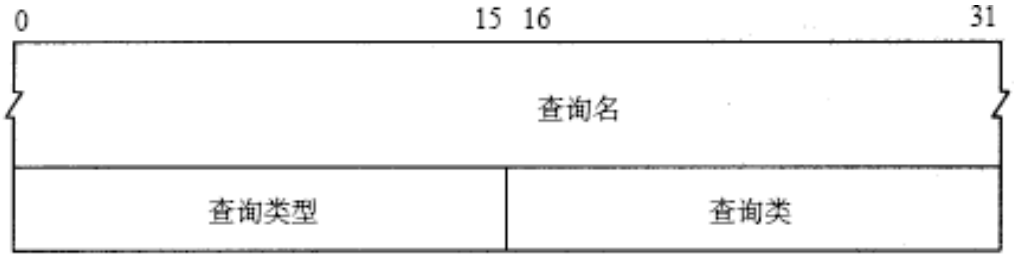
问题数、回答RR数、权威RR数、附加RR数

这四个字段都是两字节，分别对应下面的查询问题、回答、授权和附加信息部分的**数量**。一般问题数都为1，DNS查询报文中，资源记录数、授权资源记录数和附加资源记录数都为0。

1.3 区域

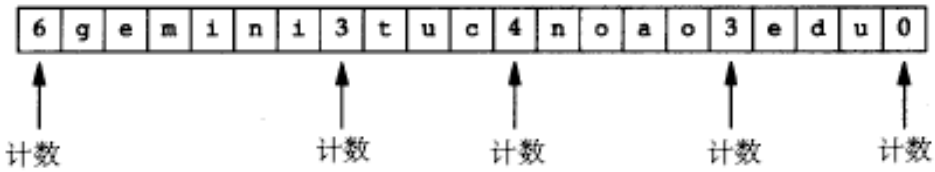
(1)问题区域

包含正在进行的查询信息。包含查询名(被查询主机名字的名字字段)、查询类型、查询类。



查询名

查询名部分长度不定，一般为要查询的域名(也会有IP的时候，即反向查询)。此部分**由一个或者多个标示符序列组成**，每个标示符以首字节数的计数值来说明该标示符长度，每个名字以0结束。计数字节数必须是0~63之间。该字段无需填充字节。还是借个例子来说明更直观些，查询名为gemini.tuc.noao.edu的话，查询名字段如下[1]：



查询类型

通常查询类型为A(由名字获得IP地址)或者PTR(获得IP地址对应的域名)，类型列表如下：

表1 DNS报文查询类型

类型	助记符	说明
1	A	IPv4地址
2	NS	名字服务器
5	CNAME	规范名称定义主机的正式名字的别名
6	SOA	开始授权标记一个区的开始
11	WKS	熟知服务定义主机提供的网络服务
12	PTR	指针把IP地址转化为域名
13	HINFO	主机信息给出主机使用的硬件和操作系统的表述
15	MX	邮件交换把邮件改变路由送到邮件服务器
28	AAAA	IPv6地址
252	AXFR	传送整个区的请求
255	ANY	对所有记录的请求

NS记录指定了名字服务器。一般情况，每个DNS数据库中，针对每个顶级域都会有一条NS记录，这样一来，电子邮件就可以被发送到域名树中远处的部分。

查询类

通常为1，指Internet数据。

IN （1） 指互联网地址。

CS 2 the CSNET class (Obsolete - used only for examples in some obsolete RFCs)

CH 3 the CHAOS class

HS 4 Hesiod [Dyer 87]

(2)回答、权威、附加区域

回答区域包含了最初请求名字的资源记录，一个回答报文的回答区域可以包含多条资料记录RR(**因为一个主机名可以对应多个IP地址，冗余Web服务器**)。权威区域包含了其他权威DNS服务器的记录。附加区域包含其他一些"有帮助"的记录，例如，对于一个MX(邮件交换)请求的回答报文中，回答区域包含一条资料记录(该记录提供邮件服务器的规范主机名)，附加区域可以包含一条类型A记录(该记录提供了该邮件服务器的规范主机名的IP地址)。

每条资料记录是一个五元组，如下：

(域名，生存期，类别，类型，值)

直接表示如下[1]：

域名(2字节或不定长)

记录中资源数据对应的名字，它的格式和查询名字段格式相同。当报文中域名重复出现时，就需要使用2字节的偏移指针来替换。例如，在资源记录中，域名通常是查询问题部分的域名的重复，就需要用指针指向查询问题部分的域名。关于指针怎么用，TCP/IP详解里面有，即2字节的指针，最前面的两个高位是11，用于识别指针。其他14位从报文开始处计数(从0开始)，指出该报文中的相应字节数。注意，DNS报文的第一个字节是字节0，第二个报文是字节1。一般响应报文中，资源部分的域名都是指针C00C(11**00000000001100，12正好是首部区域的长**

度)，刚好指向请求部分的域名[1]。

0xc0　0c 解释：红色部分解释，代表指针偏移的位置，找到资源数据

name: 2字节

type：2字节

class：2字节

time to live：四字节

data：2字节

所谓的

类型(记录的类型，见表1)

A记录，Name是主机名，Value是该主机名的IP地址，因此，一条类型为A的资源记录提供了标准的主机名到IP地址的映射。

NS记录，Name是域(如foo.com)，Value是知道如何获得该域中主机IP地址的权威DNS服务器的主机名(如dns.foo.com)，这个记录常用于沿着查询链进一步路由DNS查询。

CNAME记录，Name是主机别名，Value是主机别名对应的**规范主机名**，该记录能够向请求主机提供一个主机名对应的规范主机名。

MX记录，Name是邮件服务器别名，Value是邮件服务器别名的规范主机名。通过MX记录，一个公司的邮件服务器和其他服务器可以使用相同的别名。

注：有着复杂主机名的主机能拥有多个别名，前者称为规范主机名，后者称为主机别名(便于记忆)。

类

对于Internet信息，它总是IN。

生存时间

用于指示该记录的稳定程度，极为稳定的信息会被分配一个很大的值(如86400，一天的秒数)。该字段表示资源记录的生命周期(以秒为单位)，一般用于当地址解析程序取出资源记录后决定保存及使用缓存数据的时间。0代表只能被传输，但是不能被缓存

资源数据长度(2字节)

表示资源数据的长度(以字节为单位，如果资源数据为IP则为0004)。

资源数据

该字段是可变长字段，表示按查询段要求返回的相关资源记录的数据。

1.4 wireshark抓包分析

过滤器输入 dns ，查询对应的包

dns_domain.pcapng
8.44KB

总体图 - DNS报文格式