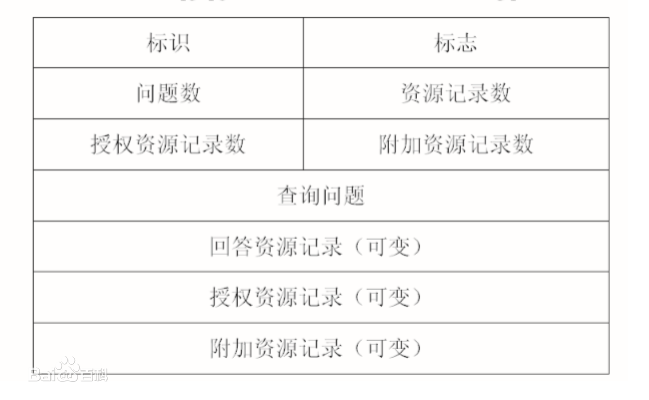
MDNS 协议说明

报文格式

DNS 定义了两种报文 ，一种为查询报文；另一种是对查询报文的响应，称为响应报文。无论是查询报文还是响应报文，都有12个字节的头和查询问题。



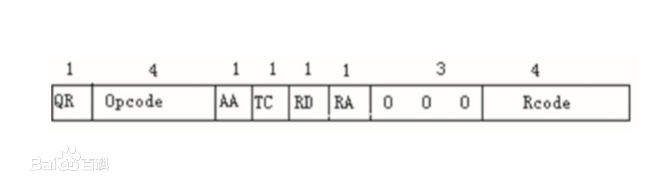
DNS 查询报文格式



DNS响应报文格式

### 报文细节分析

(1)标识：占两个字节，同一个问题的查询和响应标识必须相同。



DNS 报文标志

(2)标志：占两个字节QR：这一位是查询和响应报文的标志，0表示查询报文，1表示响应报文；Opcode：操作码占4bit，值为0表示标准查询，值为1表示反向查询，值为2表示服务器状态请求。标准查询是给出主机名查询其对应的IP；反向查询是给出[IP](https://baike.baidu.com/item/IP/224599" \t "_blank)查询其对应的主机名；AA：占1bit，表示该域名服务器是否是授权给该域的，1表示授权，0表示未授权；TC：占1bit，表示是否可截断。当使用UDP时，若此位为1，表示当响应报文的总长度超过512字节时，只返回前512个字节，是可截断的；RD：占1bit，表示是否期望递归。为1时表示查询方式是递归查询；如果该位为0，且被请求的域名服务器没有一个授权回答，则查询方式为迭代查询；RA：占1bit，表示是否  
　　可用递归。如果域名服务器支持递归查询，则在响应中将该比特设置为1，大多数名字服务器都提供递归查询，除  
　　了某些[根服务器](https://baike.baidu.com/item/%E6%A0%B9%E6%9C%8D%E5%8A%A1%E5%99%A8/136331)；随后的3bit字段必须为0；Rcode：结果代码占4bit，值为0表明没有差错，值为1表明报  
　　文格式出错，值为2表明服务器查询失败，值为3表明名字出错。

(3)问题数、回答资源记录数、授权资源记录数、附加资源记录数分别描述各自的记录数目。对于查询报文，  
　　问题数通常是1，而其他三项则均为0。响应报文随问题不同而变化。

(4)查询问题：由查询名、查询类型、查询类三部分组成。查询名是要查找的名字，它是一个或多个标识符的  
　　序列，它的存储方法是先存储每个子域的字符数，再存储相应的字符，依次存储，最后填写一个0字节；查询类型  
　　占两个字节，常用的有（A，1）代表IP地址、（NS，2）代表名字服务器、（PTR，12）代表[指针](https://baike.baidu.com/item/%E6%8C%87%E9%92%88/2878304" \t "_blank)记录；查询类占两个字节，通常为（IN，1），指互联网地址。

(5)资源记录：只出现在响应报文中，它们有一种统一的格式。

static uint8\_t mdns\_query[] = {

    // Query ID

    0x00, 0x00,

    // Flags

    0x00, 0x00,

    // 1 question

    0x00, 0x01,

    // No answer, authority or additional RRs

    0x00, 0x00, 0x00, 0x00, 0x00, 0x00,

    // \_services.\_dns-sd.\_udp.local.

    0x04, '\_', 'r', 'i', 'o',

    0x04, '\_', 't', 'c', 'p', 0x05, 'l', 'o', 'c', 'a', 'l', 0x00,

    // PTR record

    0x00, 0x0C,

    // QU (unicast response) and class IN

    0x80, 0x01};