9.2.1 DNS 数据包结构

如图 9-10 所示，DNS 数据包和我们之前所看到的数据包类型结构有所不同。DNS 数据包中会出现下面的一些域。

<table>
<tr><td colspan="8">域名系统 (DNS)</td></tr>
<tr><td>偏移位</td><td>八位组</td><td>0</td><td>1</td><td>2</td><td colspan="4">3</td></tr>
<tr><td>八位组</td><td>位</td><td>0–7</td><td>8–15</td><td>16–23</td><td colspan="4">24–31</td></tr>
<tr><td>0</td><td>0</td><td colspan="2">DNS ID号</td><td>QR</td><td>操作码</td><td>AA TC RD RA</td><td>Z</td><td>响应码</td></tr>
<tr><td>4</td><td>32</td><td colspan="2">问题计数</td><td colspan="4">回答计数</td></tr>
<tr><td>8</td><td>64</td><td colspan="2">域名服务器计数</td><td colspan="4">额外记录计数</td></tr>
<tr><td>12+</td><td>96+</td><td colspan="2">问题区段</td><td colspan="4">回答区段</td></tr>
<tr><td></td><td></td><td colspan="2">权威区段</td><td colspan="4">额外信息区段</td></tr>
</table>

图 9-10　DNS 数据包结构

DNS ID 号（DNS ID Number）：用来对应 DNS 查询和 DNS 响应。

查询/响应（Query/Response, QR）：用来指明这个数据包是 DNS 查询还是响应。

操作码（OpCode）：用来定义消息中请求的类型。

权威应答（Authoritative Answer, AA）：如果响应数据包中设定了这个值，则说明这个响应是由域内权威域名服务器发出的。

截断（Truncation, TC）：用来指明这个响应由于太长，无法装入数据包而被截断。

期望递归（Recursion Desired, RD）：如果在请求中设定了这个值，则说明 DNS 客户端在目标域名服务器不含有所请求信息的情况下，要求进行递归查询。

可用递归（Recursion Available, RA）：如果响应中设定了这个值，则说明域名服务器支持递归查询。

保留（Z）：在 RFC1035 的规定中被设为全 0，但有时会被用来作为 RCode 域的扩展。

响应码（Response Code）：在 DNS 响应中用来指明错误。

问题计数（Question Count）：在问题区段中的条目数。

回答计数（Answer Count）：在回答区段中的条目数。

域名服务器计数（Name Server Count）：在权威区段的域名资源记录数。

额外记录计数（Additional Records Count）：在额外信息区段中的其他资源记录数。

问题区段（Question section）：大小可变、包含要被发送到 DNS 服务器的一条或多条的信息查询的部分。

回答区段（Answer section）：大小可变、包含用来回答查询的一条或多条资源记录。

权威区段（Authority section）：大小可变、包含指向权威域名服务器的资源记录，用以继续解析过程。

额外信息区段（Additional Information section）：大小可变、包含与查询有关的额外信息，但对于回答查询这并不是绝对必要的资源记录。