

## 实验十三 DNS 域名服务协议

### 【实验目的】

- 1、理解 DNS 实现的原理；
- 2、了解 DNS 解析的过程；
- 3、掌握 DNS 报文格式。

### 【实验学时】

4 学时

### 【实验环境】

本实验要求实验室主机能够连接到 Internet，并可浏览网页。

实验拓扑如图 5-37 所示：

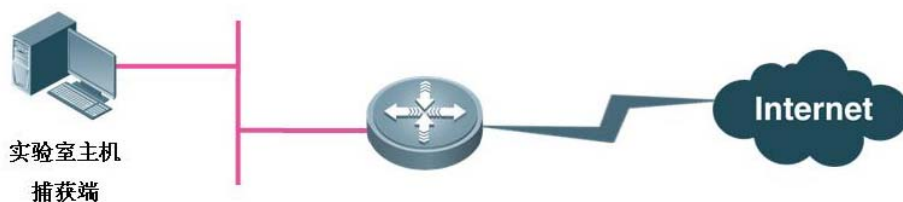


图 5-37 实验拓扑图

### 【实验内容】

- 1、学习 DNS 协议的原理和实现方法；
- 2、了解 DNS 的工作过程；
- 3、通过编辑 DNS 请求数据包，了解 DNS 的报文格式；
- 4、掌握 nslookup 命令和 ipconfig 命令的使用方法。

【实验流程】

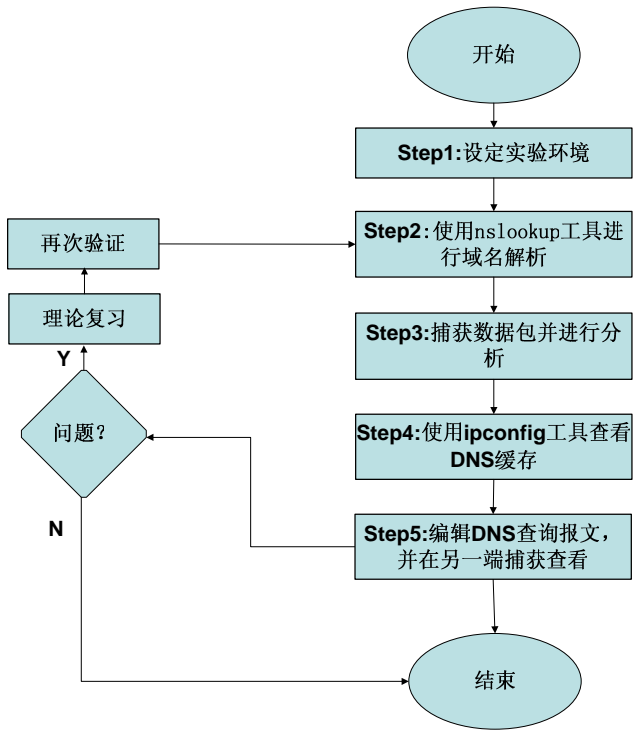


图 5- 38 实验流程图

【实验原理】

DNS 域名系统是服务器和客户程序相互通信的一种协议。它提供了主机域名和 IP 地址之间的转换。域名服务器使用固定的端口号 53，支持 UDP 和 TCP 访问。

DNS 协议

DNS 是域名系统（Domain Name System）的缩写，它是一种用于 TCP/IP 应用程序的分布式数据库，它提供主机名字和 IP 地址之间的转换及有关电子邮件的选路信息。所谓“分布式”是指在 Internet 上的单个站点不能拥有所有的信息。每个站点（如大学中的系、校园、公司或公司中的部门）保留它自己的信息数据库，并运行一个服务器程序供 Internet 上的其他系统（客户程序）查询。

在 Internet 中，域名可用来对某个组织或实体进行寻址。例如“www.sina.com”这个域名可用来对 IP 地址为 71.5.7.191 的 Internet 网点“sina.com”进行寻址，而特定的主机服务器名称为“www”。域名中的“com”部分表明该组织或实体的性质，“sina”定义了该组织或实体。

而 DNS 就像是一个自动的电话号码簿，我们可以直接拨打某人的名字来代替他的电话号码（IP 地址）。DNS 在我们直接呼叫网站的名字以后，就会将像 www.sina.com 一样便于

人类使用的名字转化成像 71.5.7.191 一样便于机器识别的 IP 地址。

这个转换工作称为域名解析，域名解析需要由专门的域名解析服务器来完成，DNS 就是进行域名解析的服务器。它是一种分布式网络目录服务，主要用于域名与 IP 地址的相互转换，以及控制因特网的电子邮件的发送。大多数因特网服务依赖于 DNS 而工作，一旦 DNS 出错，就无法连接 Web 站点，电子邮件的发送也会中止。

在 DNS 命名方式中，采用了分散和分层的机制来实现域名空间的委派授权，以及域名与地址相转换的授权。通过使用 DNS 的命名方式来为遍布全球的网络设备分配域名，而这则是由分散在世界各地的服务器实现的。

命名系统是分层次的，域名树是倒置的，它的根级显示在最上方，分为若干顶级域（.com、.net、.edu、.gov、.org 等，以及 200 多个国家级的顶级域），这些域又被分成二级域，依此类推。它们由各自相应的政府或私有实体管理。

DNS 的分布式机制支持有效且可靠的名字到 IP 地址的映射。多数名字可以在本地映射，不同站点的服务器相互合作能够解决大网络的名字与 IP 地址的映射问题。单个服务器的故障不会影响 DNS 的正确操作。

### DNS 工作流程

域名服务分为客户端和服务端，客户端提出请求，询问一个 Domain Name 的 IP 地址，服务器端必须回答客户端的请求。本地 DNS 首先查询自己的数据库，如果自己的数据库中没有对应的 IP 地址，则向本地 DNS 上所设的上一级 DNS 询问，得到结果之后，将收到的结果保存在高速缓冲区，并回答给客户端。其简单过程如图 5-39 所示：

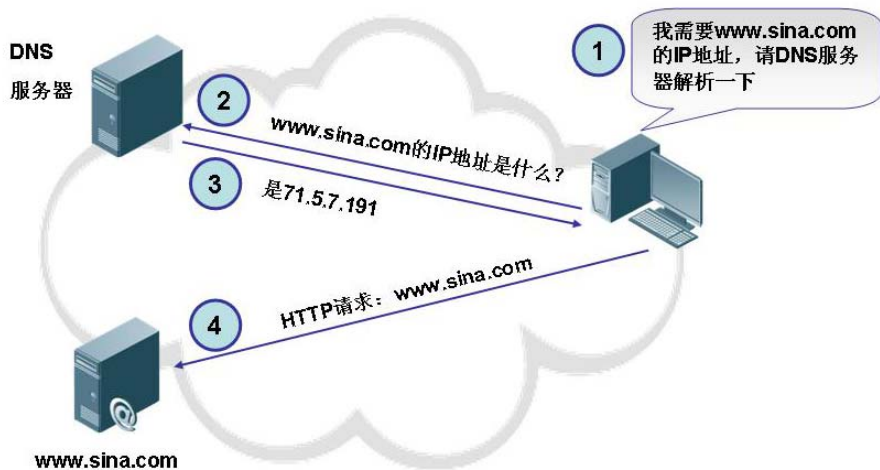


图 5-39 DNS 的工作过程

在这个过程中，待查询的域名放在查询问题中，查询结果放在回答的资源记录中。

### DNS 的报文格式

DNS 定义了用于查询和响应的报文格式，图 5-40 是查询和响应报文的总体格式：



图 5-40 DNS 总体报文格式

这个报文由 12 字节长的首部和 4 个长度可变的字段组成。  
标识字段由客户程序设置并由服务器返回结果。客户程序通过它来确定响应与查询是否匹配。

16 bit 的标志字段被划分为若干子字段，如图 5-41 所示：

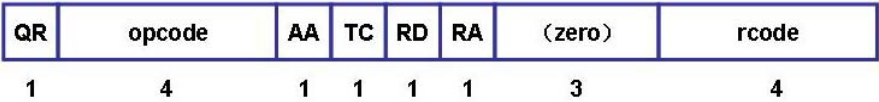


图 5-41 DNS 报文首部中的标志字段

标志中每一位的含义如下：

- QR: 是 1 bit 字段，0 表示查询报文，1 表示响应报文。
- Opcode: 报文类型，是一个 4 bit 字段，通常值为 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 1 bit 字段，表示“授权回答（authoritative answer）”，如果此位为 1，表示服务器对问题部分的回答是权威性的。
- TC: 是 1 bit 字段，表示“可截断的（truncated）”。使用 UDP 时，它表示当应答的总长度超过 512 字节时，只返回前 512 个字节。
- RD: 是 1 bit 字段，表示“期望递归（recursion desired）”。该比特能在一个查询中设置，并在响应中返回。这个标志告诉名字服务器必须处理这个查询，也称为一个递归查询。如果该位为 0，且被请求的名字服务器没有一个授权回答，它就返回一个能解答该查询的其他名字服务器列表，这称为迭代查询。
- RA: 是 1 bit 字段，表示“可用递归”。如果名字服务器支持递归查询，则在响应中将该比特设置为 1。
- Zero: 随后的 3 bit 字段必须为 0。
- Rcode: 是一个 4 bit 的返回码字段。通常的值为 0（没有差错）和 3（名字差错）。

名字差错只有从一个授权 DNS 服务器上返回,它表示在查询中制定的域名不存在。

随后的 4 个 16 bit 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,而其他 3 项则均为 0。类似地,对于应答报文,回答数至少是 1,剩下的两项可以是 0 或非 0。

图5- 42是DNS查询报文中的查询问题记录部分的格式,通常只有一个问题:



图 5- 42 DNS 查询问题记录格式

查询名是要查找的名字,它是一个或多个标识符的序列。每个标识符以首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。计数字节的值必须是 0 ~ 63 的数,因为标识符的最大长度仅为 63。

每个问题有一个查询类型,而每个响应 (也称一个答案或资源记录) 也有一个类型。大约有 20 个不同的类型值,其中的一些目前已经过时,常见的值如下表:

表 5-6 类型值列表

| 名 字   | 数 值 | 描 述    |
|-------|-----|--------|
| A     | 1   | IP 地址  |
| NS    | 2   | 名字服务器  |
| CNAME | 5   | 规范名称   |
| PTR   | 12  | 指针记录   |
| HINFO | 13  | 主机信息   |
| MX    | 15  | 邮件交换记录 |

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 (某些站点也支持其他非 IP 地址)。

DNS 报文中最后的三个字段,答案字段、权威答案字段和附加答案字段,均采用一种称为资源记录 RR (Resource Record) 的相同格式,图 5- 43 是 DNS 响应报文中资源记录的格式:

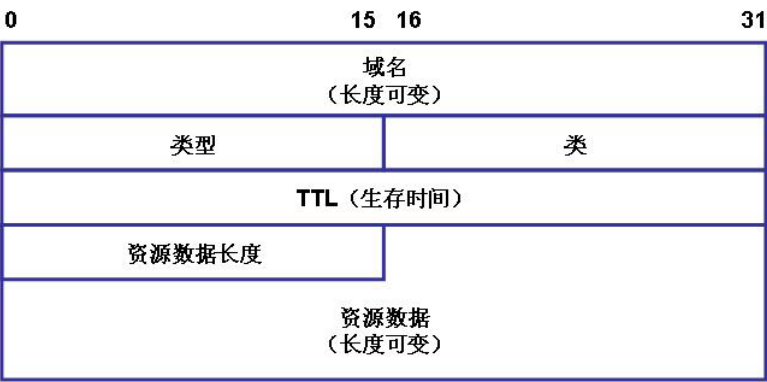


图 5- 43 DNS 资源记录的格式

- 域名: 是记录中资源数据对应的名字。它的格式和前面介绍的查询名字段格式相同。
- 类型: 说明 RR 的类型码。它的值和前面介绍的查询类型值是一样的。
- 类: 通常为 1, 指 Internet 数据。
- 生存时间: 该字段是客户程序保留该资源记录的秒数。资源记录通常的生存时间值为 2 天。
- 资源数据长度: 说明资源数据的数量。该数据的格式依赖于类型字段的值。对于类型 1 (A 记录) 资源数据是 4 字节的 IP 地址。

【实验步骤】

步骤一：使用 nslookup 工具解析域名，捕获数据包并进行分析

1、在实验主机上启动网络协议分析仪进行数据捕获并设置过滤条件，在工具栏点击“过滤器”按钮，会弹出“设置&过滤器”对话框，在“过滤器类型”中选择“类型过滤器”，类型值中选择“DNS 协议”，点击“设置参数”按钮后“确定”，开始进行数据包的捕获：

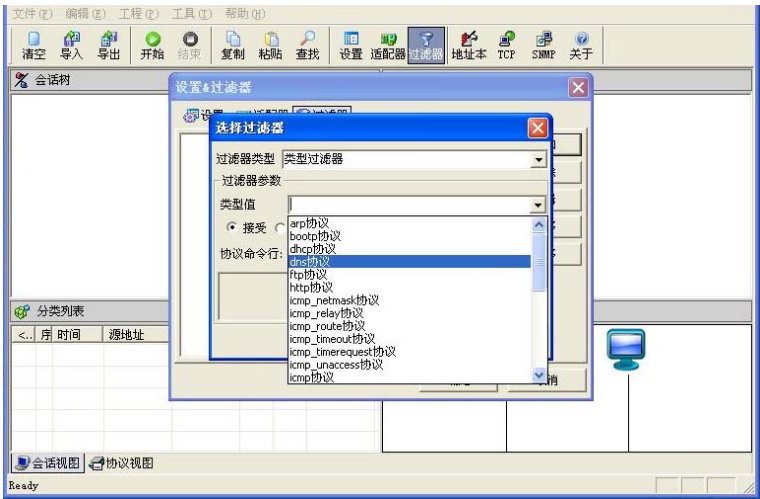
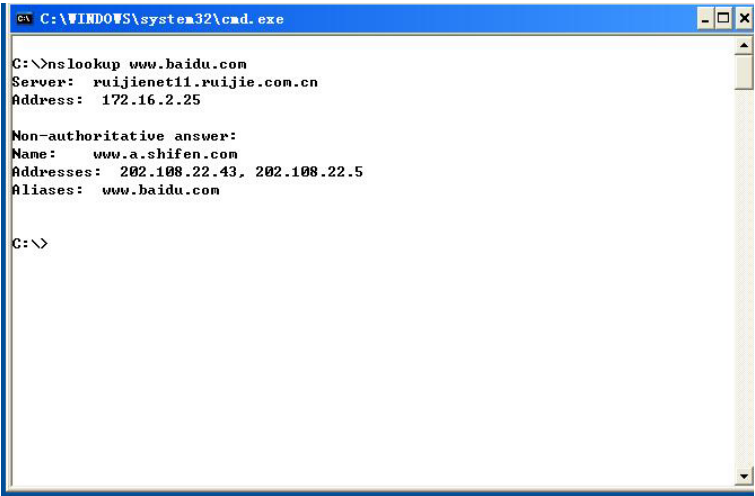


图 5- 44 设置 DNS 协议过滤器

2、使用 nslookup 工具进行域名的解析。

nslookup 命令是查询域名对应 IP 的工具，其用法可以直接在 Windows 系统的命令提示符下运行命令：**nslookup 域名** 来进行域名解析，例如：



```
C:\WINDOWS\system32\cmd.exe

C:\>nslookup www.baidu.com
Server:  ruijienet11.ruijie.com.cn
Address:  172.16.2.25

Non-authoritative answer:
Name:     www.a.shifen.com
Addresses: 202.108.22.43, 202.108.22.5
Aliases:  www.baidu.com

C:\>
```

图 5-45 使用 nslookup 工具（一）

也可以仅仅运行 **nslookup** 命令（不需任何参数），进入 nslookup 的交互界面，在“>”提示符后可以多次输入不同的域名，以实现多次的查询，例如可以在一次 nslookup 的交互过程中，进行 **www.baidu.com**、**www.yahoo.com**、**www.google.com** 的查询：



```
C:\WINDOWS\system32\cmd.exe - nslookup

> www.baidu.com
Server:  ruijienet11.ruijie.com.cn
Address:  172.16.2.25

Non-authoritative answer:
Name:     www.a.shifen.com
Addresses: 202.108.22.5, 202.108.22.43
Aliases:  www.baidu.com

> www.yahoo.com
Server:  ruijienet11.ruijie.com.cn
Address:  172.16.2.25

Non-authoritative answer:
Name:     www.yahoo-ht3.akadns.net
Address:  209.131.36.158
Aliases:  www.yahoo.com

> www.google.com
Server:  ruijienet11.ruijie.com.cn
Address:  172.16.2.25

Non-authoritative answer:
Name:     www-china.l.google.com
Addresses: 64.233.189.147, 64.233.189.99, 64.233.189.104
Aliases:  www.google.com, www.l.google.com

>
```

图 5-46 使用 nslookup 工具（二）

最后，可用“exit”命令退出 nslookup 的交互状态。

3、分析捕获到的数据报文。

图 5-47 是一个 DNS 的查询报文，从中可以看到，报文的标识为 10，问题数是 1，答



案数、权威答案数、附加答案数都是 0，而要查询的域名是 [www.yahoo.com](http://www.yahoo.com)：

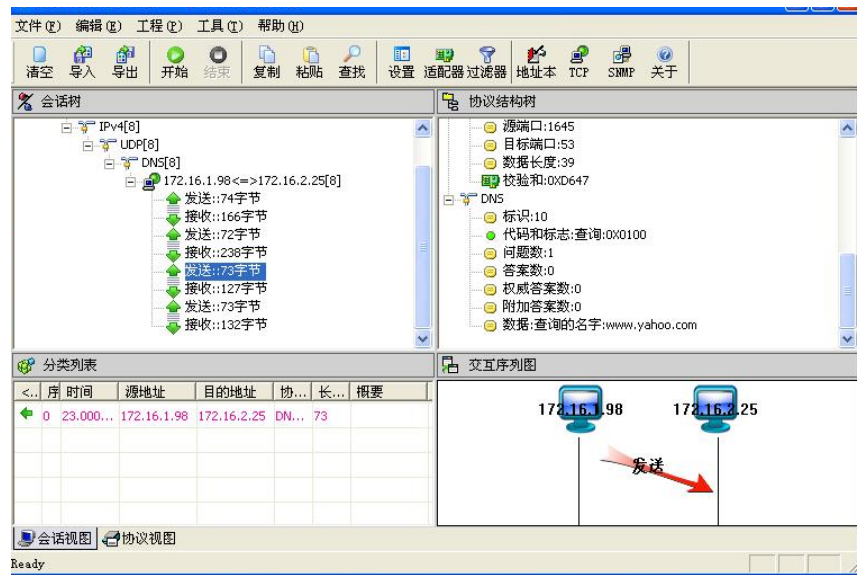


图 5- 47 DNS 的查询报文

图 5- 48 则是相应的响应报文，报文标识同样为 10，指明这个响应是针对哪一个查询报文的，问题数是 1，答案数是 2，权威答案数和附加答案数都是 0，并且对域名 [www.yahoo.com](http://www.yahoo.com) 的查询结果是 [209.131.36.158](http://209.131.36.158)：

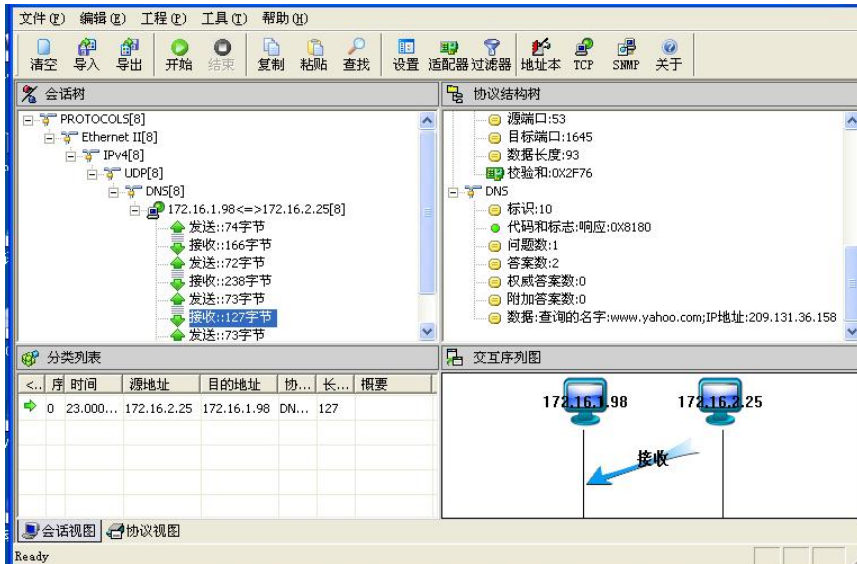


图 5- 48 DNS 的响应报文

### 步骤二：使用 ipconfig 命令查看 DNS 缓存

1、继续使用协议分析仪进行数据的捕获，同时打开 IE 浏览器，访问 [www.baidu.com](http://www.baidu.com)、[www.yahoo.com](http://www.yahoo.com)、[www.google.com](http://www.google.com)，观察此时是否还有 DNS 请求？



2、关闭 IE 浏览器后再重新打开，访问一个尚未访问过的网站，例如 [www.sohu.com](http://www.sohu.com)，观察此时是否有 DNS 请求？为什么？

3、在 Windows 系统的命令提示符下运行：**ipconfig /displaydns** 显示本机缓冲区中的 DNS 解析内容，如图 5-49 所示：



```
C:\WINDOWS\system32\cmd.exe

C:\>ipconfig /displaydns

Windows IP Configuration

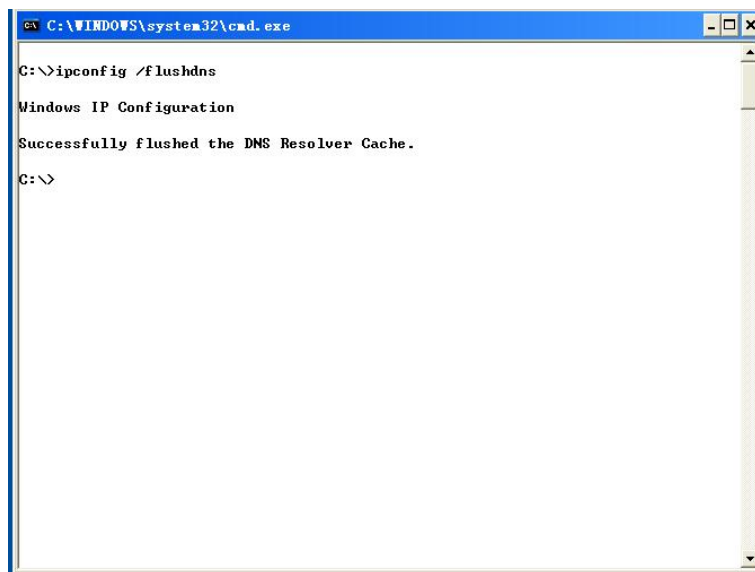
    pv.sohu.com
    -----
    Record Name . . . . . : pv.sohu.com
    Record Type . . . . . : 1
    Time To Live . . . . . : 3
    Data Length . . . . . : 4
    Section . . . . . : Answer
    A (Host) Record . . . : 61.135.132.159

    Record Name . . . . . : pv.sohu.com
    Record Type . . . . . : 1
    Time To Live . . . . . : 3
    Data Length . . . . . : 4
    Section . . . . . : Answer
    A (Host) Record . . . : 61.135.132.161

    Record Name . . . . . : pv.sohu.com
    Record Type . . . . . : 1
    Time To Live . . . . . : 3
    Data Length . . . . . : 4
    Section . . . . . : Answer
    A (Host) Record . . . : 61.135.150.211
```

图 5-49 显示本机的 DNS 缓存

4、在 Windows 系统的命令提示符下运行：**ipconfig /flushdns**，则可以清除本机的 DNS 缓存记录，如图 5-50 所示：



```
C:\WINDOWS\system32\cmd.exe

C:\>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\>
```

图 5-50 清除本机的 DNS 缓存

5、此时关闭 IE 浏览器再打开，访问刚才打开过的网站，观察是否有 DNS 请求？为什

么？

### 步骤三：利用网络协议编辑软件编辑 DNS 请求包

1、在主机上打开协议数据发生器，在工具栏上选择“添加”，会弹出“网络包模版”对话框，选择“DNS 协议模版”，建立一个 DNS 数据报文：

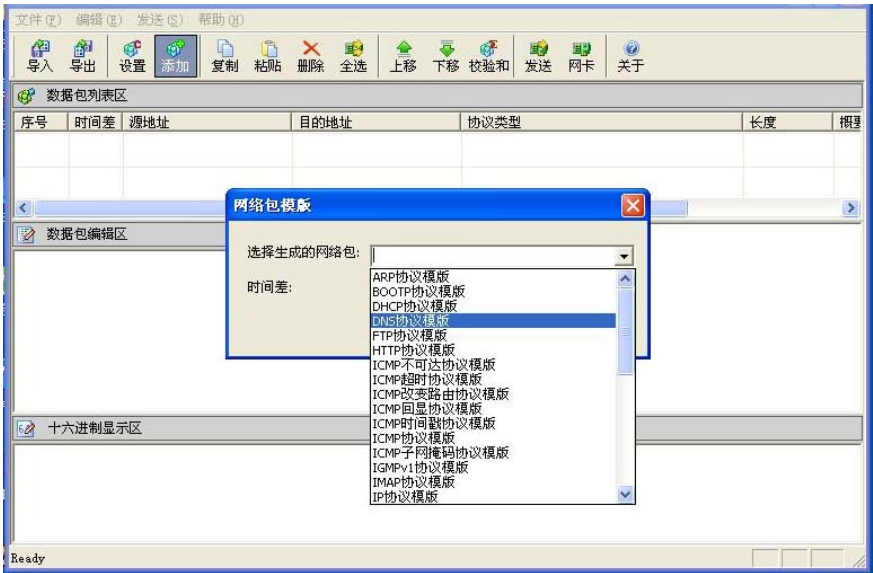


图 5-51 建立 DNS 协议的查询报文

2、填写其中以以太网帧头、IP 首部、UDP 首部和 DNS 报文的内容：

- 填写以太网协议首部信息：
  - 目的物理地址：在地址本中查询网关的 IP 地址，确定后填入网关的 MAC 地址：00-D0-F8-B5-14-8C；
  - 源物理地址：填入实验主机的 MAC 地址：00-15-58-2F-7E-7E；
  - 类型或长度：该字段应为 0800（即 IP 协议的类型值）。
- 填写 IP 协议头信息：
  - 总长度字段：包括 UDP 段内容的总长度，20 IP+8 UDP+30 DNS = 58；
  - 标识：可以任意填入，例如：0x2938；
  - 高层协议字段：即上层协议类型为 17（UDP 协议的类型为 17）；
  - 发送 IP 地址：在地址本中选择本机的 IP 地址：172.16.1.98；
  - 目标 IP 地址：手工填入 DNS 服务器的 IP 地址：172.16.2.25；
  - 点击工具栏中的“校验和”按钮计算 IP 头校验和。
- 填写 UDP 协议的各个字段信息：
  - 16 位源端口号：可按照捕获 DNS 数据报文的源端口号填入：1644；
  - 16 位目的端口号：53；
  - UDP 总长度：包括 UDP 头部和携带数据的总长度，8 UDP+30 DNS= 38；
  - 校验和：点击工具栏中的“校验和”按钮计算 UDP 校验和。

- 填写 DNS 协议报文的内容：
  - 标识：任意填写，例如 0x11；
  - 代码和标志：0x0100（表示期望递归）；
  - 问题数：1；
  - 资源数：0；
  - 权威答案数：0
  - 附加答案数：0；
  - DNS 数据：点击“数据编辑”按钮，填入查询域名 **www.sina.com**；查询类型：1（代表 A，主机类型）；查询分类：1（代表 IN，即 INTERNET），确定后即可形成 DNS 数据：



图 5-52 编辑 DNS 查询数据

最终的编辑结果如图 5-53 所示：

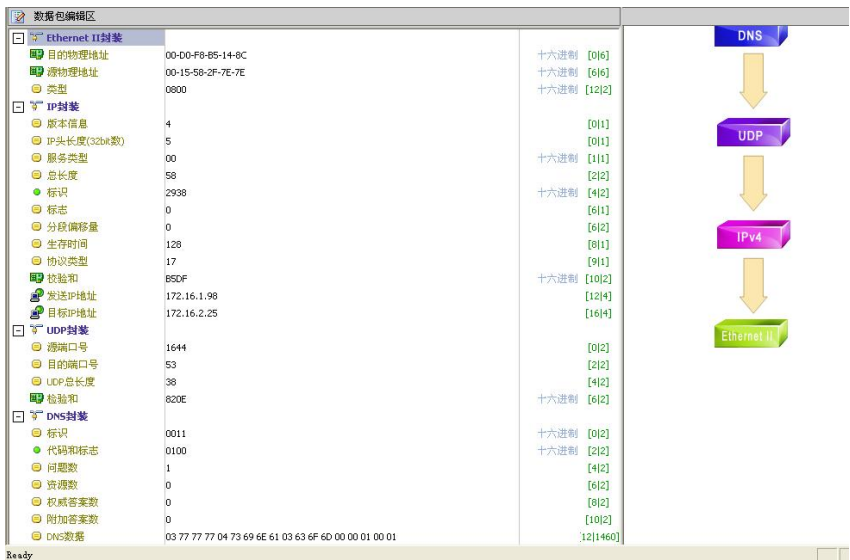


图 5-53 编辑 DNS 查询报文的内容

- 3、点击工具栏上的“发送”按钮，将编辑好的 DNS 数据报文发送。
- 4、在实验主机上运行网络协议分析仪，捕获数据，捕获结果如所示，从中可以看到报文类型为 DNS 的查询报文，标识是 17（即十六进制的 11），查询的名字是 [www.sina.com](http://www.sina.com)：

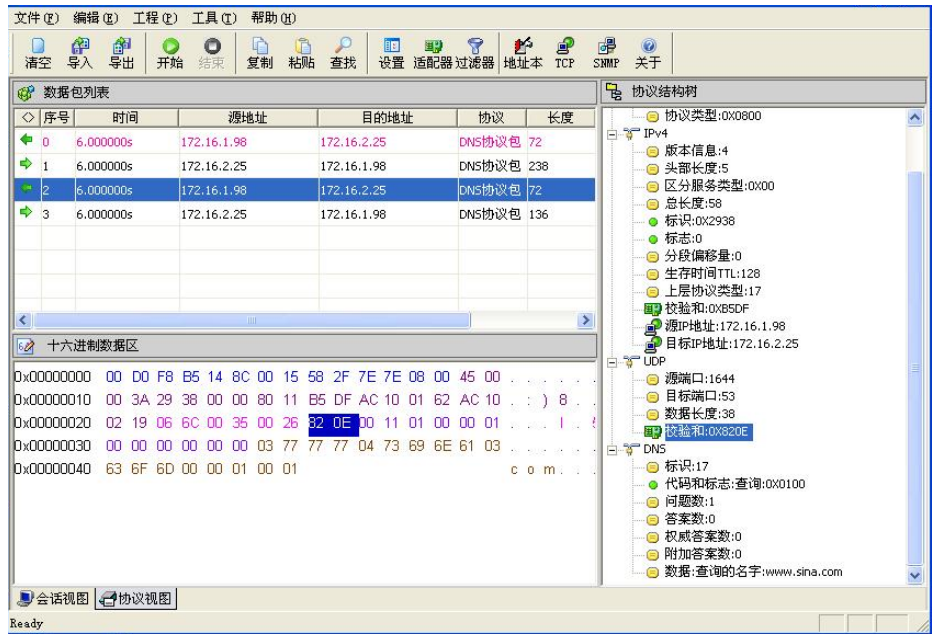


图 5- 54 捕获编辑的 DNS 报文

### 【思考问题】

- 结合实验过程中的实验结果，回答下列问题：
- 1、根据步骤 1 中的捕获结果，分析 DNS 协议的工作流程。
  - 2、域名与 IP 地址之间是否有一一对应的关系？