

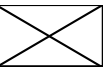
《计算机网络》 课程设计

高占春

gaozc@bupt.edu.cn

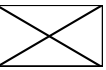
Tel.13701053226

基本要求



“DNS中继服务器”的实现

- 设计一个**DNS**服务器程序，读入“**IP**地址-域名”对照表，当客户端查询域名对应的**IP**地址时，用域名检索该对照表，有三种可能检索结果：
 - ◆ 检索结果：ip地址0.0.0.0，则向客户端返回“域名不存在”的报错消息（不良网站拦截功能）
 - ◆ 检索结果：普通IP地址，则向客户端返回该地址（服务器功能）
 - ◆ 表中未检到该域名，则向因特网DNS服务器发出查询，并将结果返给客户端（中继功能）
 - 考虑多个计算机上的客户端会同时查询，需要进行消息ID的转换



实验安排

■ 实验环境

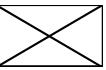
- ◆ 操作系统Windows, Ubuntu, ...
- ◆ 编程语言C, Java, C#, Pathon...

■ 分组 (**1-3**人)

- ◆ 提交的程序必须是小组所有同学都能消化

■ 成绩评定

- ◆ 提供完整电子版课程设计报告
- ◆ 验收前填写纸版 《课程设计报告封面》 和 《课程设计验收记录》
- ◆ 验收
 - 第2周前, 各小班学习委员邮件报上分组情况
 - 第13周验收, 具体时间安排将根据分组情况确定
 - 地点:教三楼903。提前将源程序发到gaozc@bupt.edu.cn或自带笔记本



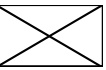
关于自选题目

- 自选题目提前备案

- ◆ 本周内通过邮件或电话报题目，批准后可以不做指定题目，小组人数也不超过3人

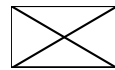
- 自选题目必须是“计算机网络协议”相关内容。例如：

- ◆ 通过程序发送和接收E-mail
- ◆ FTP Server/Client
- ◆ 网络流量嗅探
- ◆



实验报告

- 系统的功能设计
- 模块划分
- 软件流程图
- 测试用例以及运行结果
- 调试中遇到并解决的问题
- 课程设计工作总结



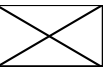
提交内容

■ 电子版

- ◆ 源代码
- ◆ 实验报告

■ 收集方式

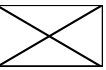
- ◆ 由学习委员将全班同学的电子版资料收齐，发邮件给我
- ◆ 目录名为**班号**
- ◆ 一组同学组织一个子目录，目录名样式为：
 - **1517张三-1619李四**
(解释为：15班序号17名字张三，16班序号19名字李四)
 - 学习委员务必将目录名按照上述要求规范化
 - 多个同学一组时，子目录命名按“班号+序号”排序取名
 - 内容包括源代码，报告



相关资料

- Socket编程(自己查找相应文献)
- RFC1305协议文本
- http://en.wikipedia.org/wiki/Domain_Name_System
- 软件工具WireShark

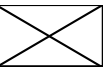
- 下载
www.163.com
免费邮箱: **gaozhanchun**
Password:jjjddd
(文件中心/网络课程设计)



编程方面的小问题

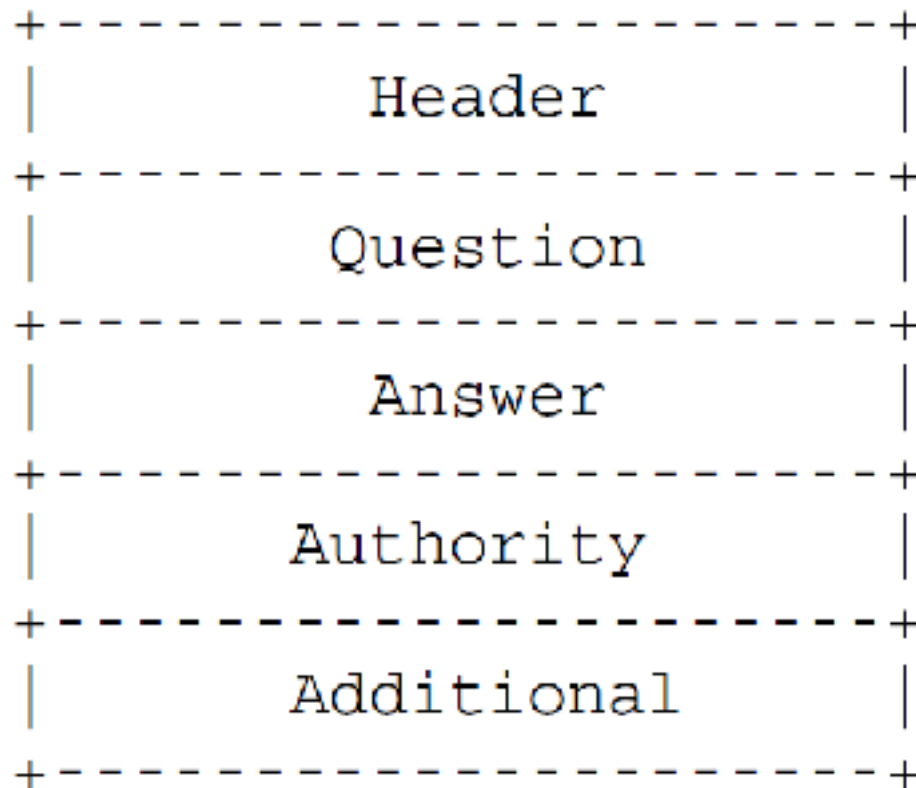
- 为使用**winsock**函数库，**vc**编程增加下面语句：
#pragma comment(lib,"Ws2_32.lib")
也可以不加此语句，但链接时须增加wssock32.lib库
- **UDP接收/发送数据报，使用recvfrom/sendto函数**
- **字节顺序**
 - ◆ CPU字节顺序
 - Big Endian (大尾)
 - Power PC, SPARC, Motorola
 - Little Endian (小尾)
 - Intel X86
 - ◆ 网络字节顺序
 - 与X86相反
 - ◆ 网络字节转换的库函数
 - htonl ntohl 四字节整数(long)
 - htons ntohs 两字节整数(short)

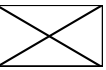
RFC1035简介



DNS的报文构成(4.1)

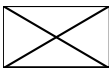
RFC1035: DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION



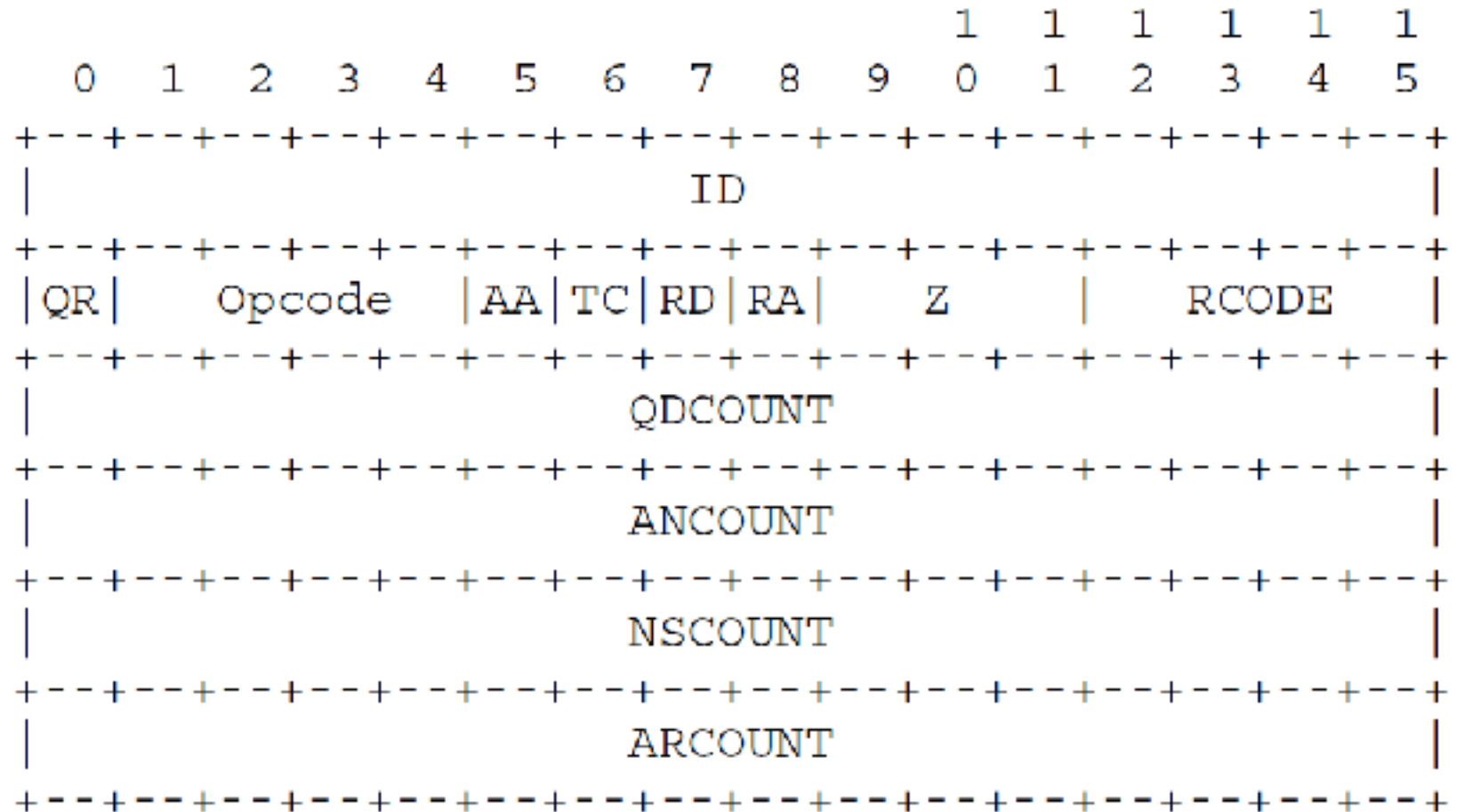


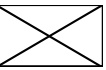
DNS的报文格式

- 整个报文由5部分构成
 - ◆ 固定长度的Header部分
 - ◆ Question: the question for the name server
 - ◆ Answer: RRs answering the question
 - ◆ Authority: RRs pointing toward an authority
 - ◆ Additional: RRs holding additional information
- 后三段格式相同，每段都是由0~n个资源记录 (Resource Record)构成



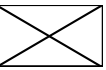
Header Section Format (4.1.1)





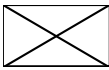
报头字段(1)

- ID
 - ◆ 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
- QR: 0表示查询报, 1表示响应报。
- OPCODE
 - ◆ 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: 权威答案(Authoritative answer)
- TC: 截断的(Truncated)
 - ◆ 应答的总长度超512字节时, 只返回前512个字节
- RD: 期望递归(Recursion desired)
 - ◆ 查询报中设置, 响应报中返回
 - ◆ 告诉名字服务器处理递归查询。如果该位为0, 且被请求的名字服务器没有一个权威回答, 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: 递归可用(Recursion Available)
 - ◆ 如果名字服务器支持递归查询, 则在响应中该比特置为1



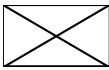
报头字段(2)

- Z: 必须为0, 保留字段
- RCODE: 响应码(Response coded), 仅用于响应报
 - ◆ 值为0(没有差错)
 - ◆ 值为3表示名字差错。从权威名字服务器返回, 表示在查询中指定域名不存在
- QDCOUNT
 - ◆ Number of entries in the question section
- ANCOUNT
 - ◆ Number of RRs in the answer section
- NSCOUNT
 - ◆ Number of name server RRs in authority records section
- ARCOUNT
 - ◆ Number of RRs in additional records section

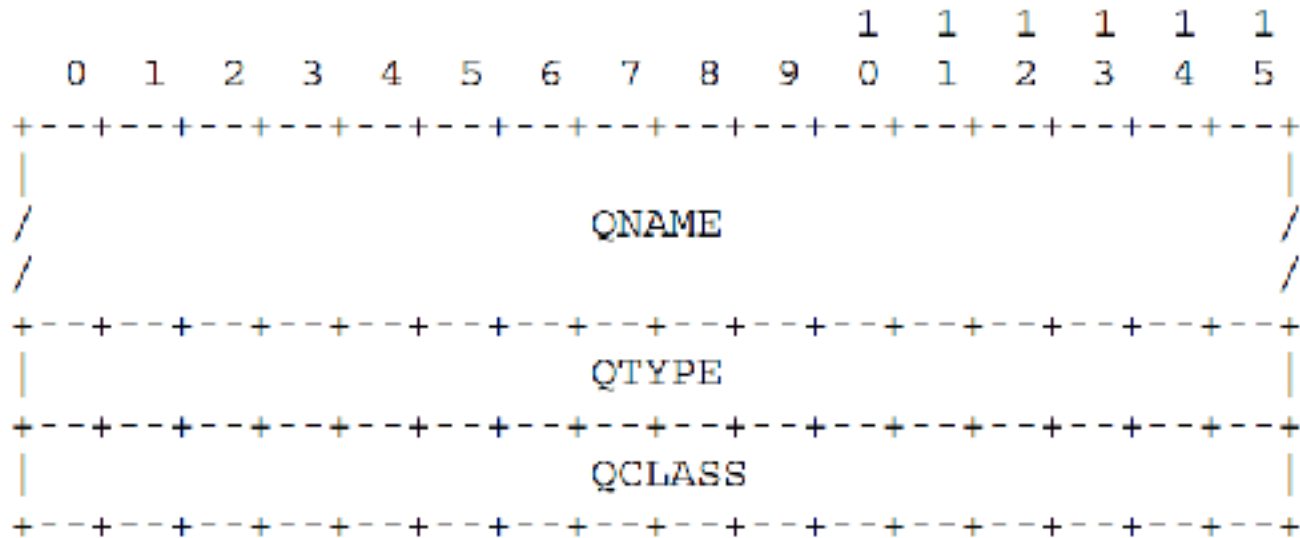


RCODE

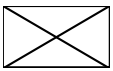
- 0** **No error condition**
- 1** **Format error - The name server was
unable to interpret the query.**
- 2** **Server failure - The name server was
unable to process this query due to a
problem with the name server.**
- 3** **Name Error - Meaningful only for
responses from an authoritative name
server, this code signifies that the
domain name referenced in the query does
not exist.**
- 4** **Not Implemented - The name server does
not support the requested kind of query.**
- 5** **Refused - The name server refuses to
perform the specified operation for
policy reasons. For example, a name
server may not wish to provide the
information to the particular requester,
or a name server may not wish to perform
a particular operation (e.g., zone**



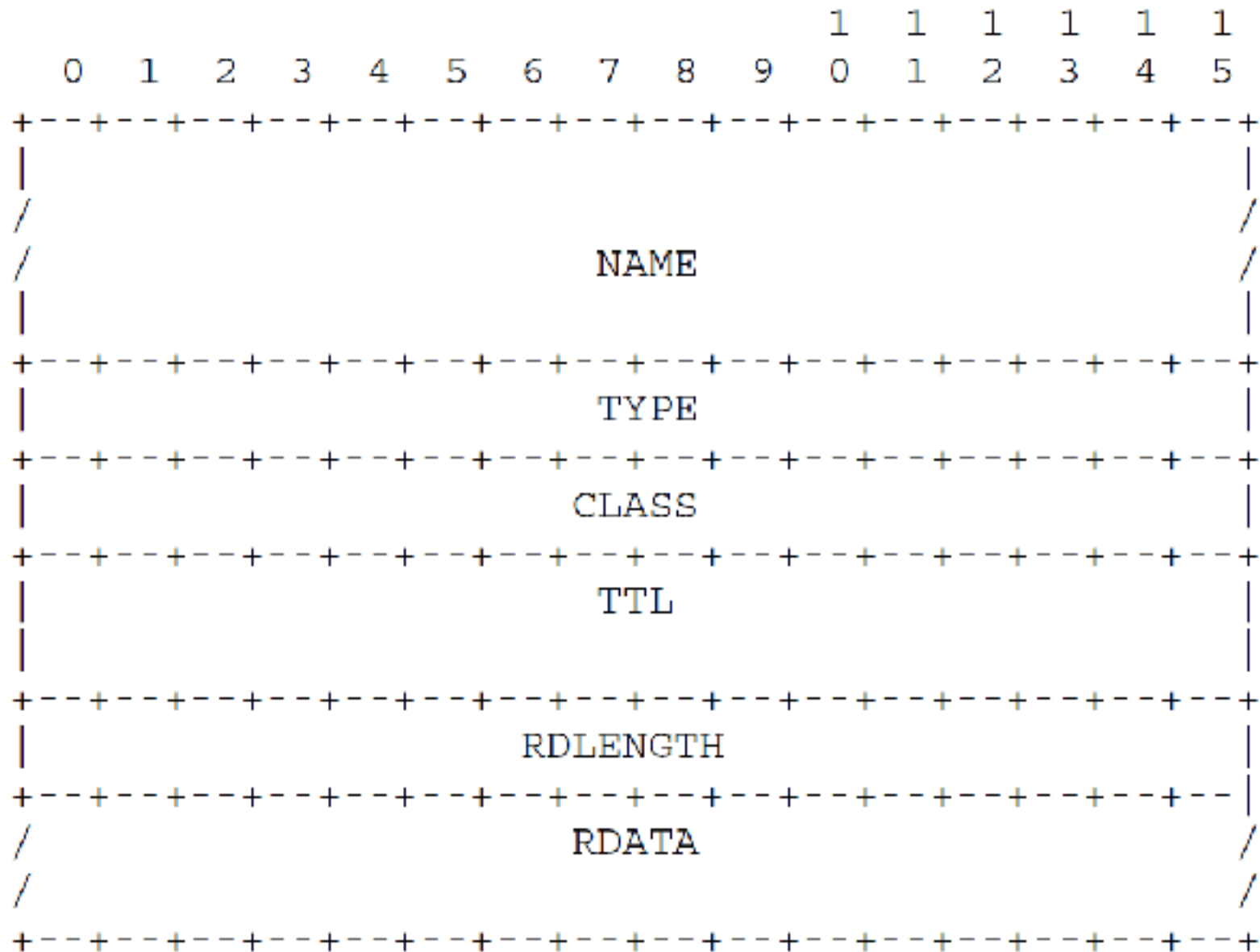
Question Section Format (4.1.2)

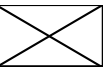


- QNAME
 - ◆ A domain name, i.e. www.bupt.edu.cn
- QTYPE
 - ◆ A two octet code, type of the query, i.e. [A\(1\)](#), [MX\(15\)](#), [CNAME\(5\)](#), [PTR\(12\)](#), ...
- QCLASS
 - ◆ A two octet code, class of the query, i.e. [IN\(1\)](#)



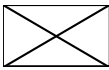
Resource Record Format (4.1.3)





Resource Record Format (4.1.3)

- **NAME:** 名字
- **TYPE:** RR的类型码
- **CLASS:** 通常为**IN(1)**, 指**Internet**数据
- **TTL**
 - ◆ 客户程序保留该资源记录的秒数, 稳定的资源记录通常生存时间值为2天, 它确定了客户端DNS cache可以缓存该记录多长时间
- **RDLENGTH:** 资源数据长度
 - ◆ 说明资源数据的字节数, 对类型1 (TYPE A记录) 资源数据是4字节的I P地址
- **RDATA:** 资源数据

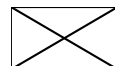


Resource Record

资源记录，大约**20**种不同类型的资源记录

- **A 地址 (Type 1)**
 - ◆ 一个A记录定义了一个IP地址，它存储32bit的二进制数
- **AAAA IPv6地址 (Type 28)**
 - ◆ 一个AAAA记录定义一个IPv6地址
- **PTR (Type 12)**
 - ◆ 指针记录用于指针查询。IP地址被看作是in-addr.arpa域下的一个域名（标识字符串）
- **CNAME 规范名字(canonical name) (Type 5)**
 - ◆ 别名alias
- **HINFO 主机信息(Type 13)**
 - ◆ 主机CPU和操作系统
- **MX 邮件交换 (Type 15)**
 - ◆ 16bit整数优先值，以及域名
 - ◆ 如果一个目的主机有多个MX项，按优先值由小到大顺序使用
- **NS名字服务器(Type 2)**
 - ◆ 说明域的权威名字服务器

DNS Request



12	7220-DENVER	[200.100.0.20]	DNS: Q ID=34422 QY=QUERY NAME=ftp.bupt.edu.cn 75	0:00 17.770	0 001.110	2
13	[200.100.0.20]	7220-DENVER	DNS: R ID=34422 QY=QUERY STAT=OK NAME=ftp.bupt.edu.cn 91	0:00 17.791	0 001.661	2
14	7220-DENVER	ftp.bupt.edu.cn	TCPD: Data 1510	0:00 17.012	0 001.570	2

```

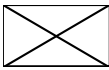
- IP:
  - IP Header
    - IP:
      - UDP: Source port = 3017
      - UDP: Destination port = 53 (Domain)
      - UDP: Length = 4
      - UDP: Checksum = 8026 (incorrect)
      - UDP: [33 byte(s) of data]
    - UDP:
  - DNS: Internet Domain Name Service header
    - DNS:
      - DNS: ID = 34422
      - DNS: Flags = 01
      - DNS: Q. .... = Command
      - DNS: Q. .... = Query
      - DNS: R. .... = Not truncated
      - DNS: R. ....1 = Recursion desired
      - DNS: Flags = 01
      - DNS: R. .... = Not Valid data- NOT an update
      - DNS: Question count = 1, Answer count = 1
      - DNS: Authority count = 0, Additional record count = 0
      - DNS:
      - DNS: ZONE Section
      - DNS: Name = ftp.bupt.edu.cn
      - DNS: Type = Host address (A,1)
      - DNS: Class = Internet (IN,1)
      - DNS:
  
```

```

00000000  00 20 00 80 00 10 00 00 00 00 00 00 00 00 00 00  # 域. 主机...
00000010  00 20 00 80 00 00 00 00 00 00 00 00 00 00 00 00  # 域. 主机...
00000020  00 14 0b 59 00 00 00 00 00 00 00 00 00 00 00 00  # 域. 主机...
00000030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  # 域. 主机...
00000040  00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00  # 域. 主机...

```


程序运行



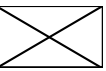
Windows系统DNS中继服务器运行

■ 运行步骤

1. 使用ipconfig/all,记下当前DNS服务器
 - 例如为202.106.0.20
2. 使用下页的配置界面, 将DNS设置为127.0.0.1(本地主机)
3. 运行你的dnsrelay程序(在你的程序中把外部dns服务器设为前面记下的202.106.0.20)
4. 正常使用ping, ftp, IE等, 名字解析工作正常

■ 其它命令

- ◆ nslookup www.bupt.edu.cn
 - 向名字服务器询问名字www.bupt.edu.cn的ip地址
- ◆ ipconfig/displaydns
 - 察看当前dns cache的内容
- ◆ ipconfig/flushdns
 - 清除dns cache中缓存的所有DNS记录



将DNS服务器指向本地自设计的程序

Internet 协议 (TCP/IP) 属性 [?] [X]

常规 **备用配置**

如果网络支持此功能，用户可以获取自动指定的 IP 设置。否则，您需要从网络系统管理员处获得适当的 IP 设置。

☒ 自动获得 IP 地址(A)

☐ 使用下面的 IP 地址(S):

IP 地址(I):

子网掩码(U):

默认网关(D):

☐ 自动获得 DNS 服务器地址(E)

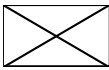
☒ 使用下面的 DNS 服务器地址(F):

首选 DNS 服务器(P):

备用 DNS 服务器(A):

高级(V)...

确定 取消



参考实现

■ 命令语法

dnsrelay [-d | -dd] [dns-server-ipaddr] [filename]

■ dnsrelay

- ◆ 无调试信息输出
- ◆ 使用默认名字服务器202.106.0.20
- ◆ 使用默认配置文件(当前目录下dnsrelay.txt)

■ **dnsrelay -d 192.168.0.1 c:\dns-table.txt**

- ◆ 调试信息级别1（仅输出时间坐标，序号，查询的域名）
- ◆ 使用指定的名字服务器192.168.0.1
- ◆ 使用指定的配置文件c:\dns-table.txt

■ **dnsrelay -dd 202.99.96.68**

- ◆ 调试信息级别2(输出冗长的调试信息)
- ◆ 使用指定的名字服务器202.99.96.68
- ◆ 使用默认配置文件(当前目录下dnsrelay.txt)