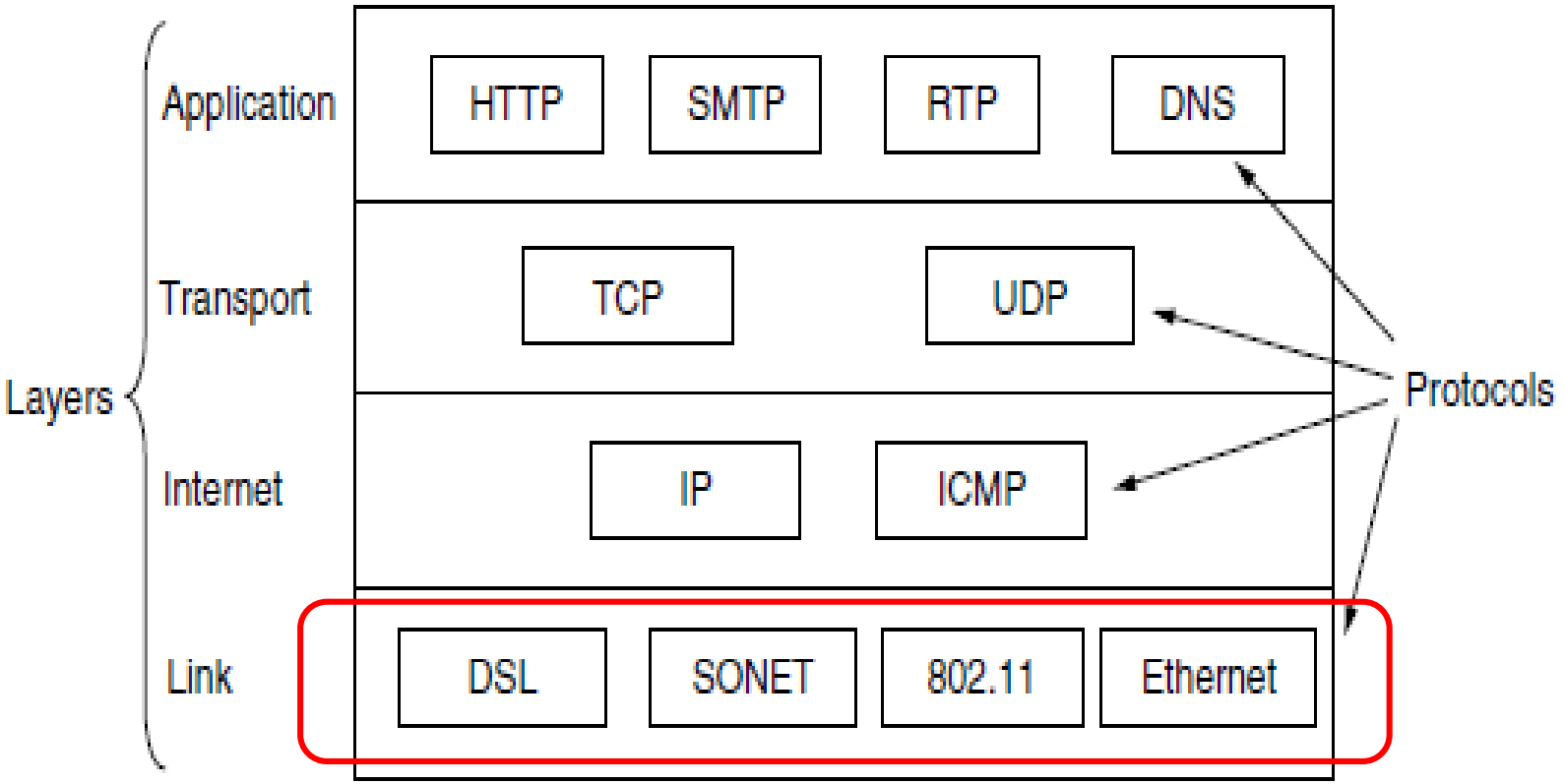
《计算机网络》课程设计

张雪松

xuesong_zhang@bupt.edu.cn

基本要求

Protocols & networks in the TCP/IP



“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
- **分组（2-3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?周验收，具体时间安排将根据分组情况确定
    - 地点:沙河，自带笔记本电脑。

实验报告

- 课程设计分工
- 协议研究
- 系统的方案设计（方案选择、模块划分、软件流程图）
- 测试用例以及测试分析
- 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：
    - 0917张三-1019李四

      （09班序号17名字张三，10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
- RFC1304协议文本
- http://en.wikipedia.org/wiki/Domain_Name_System
- 软件工具WireShark：

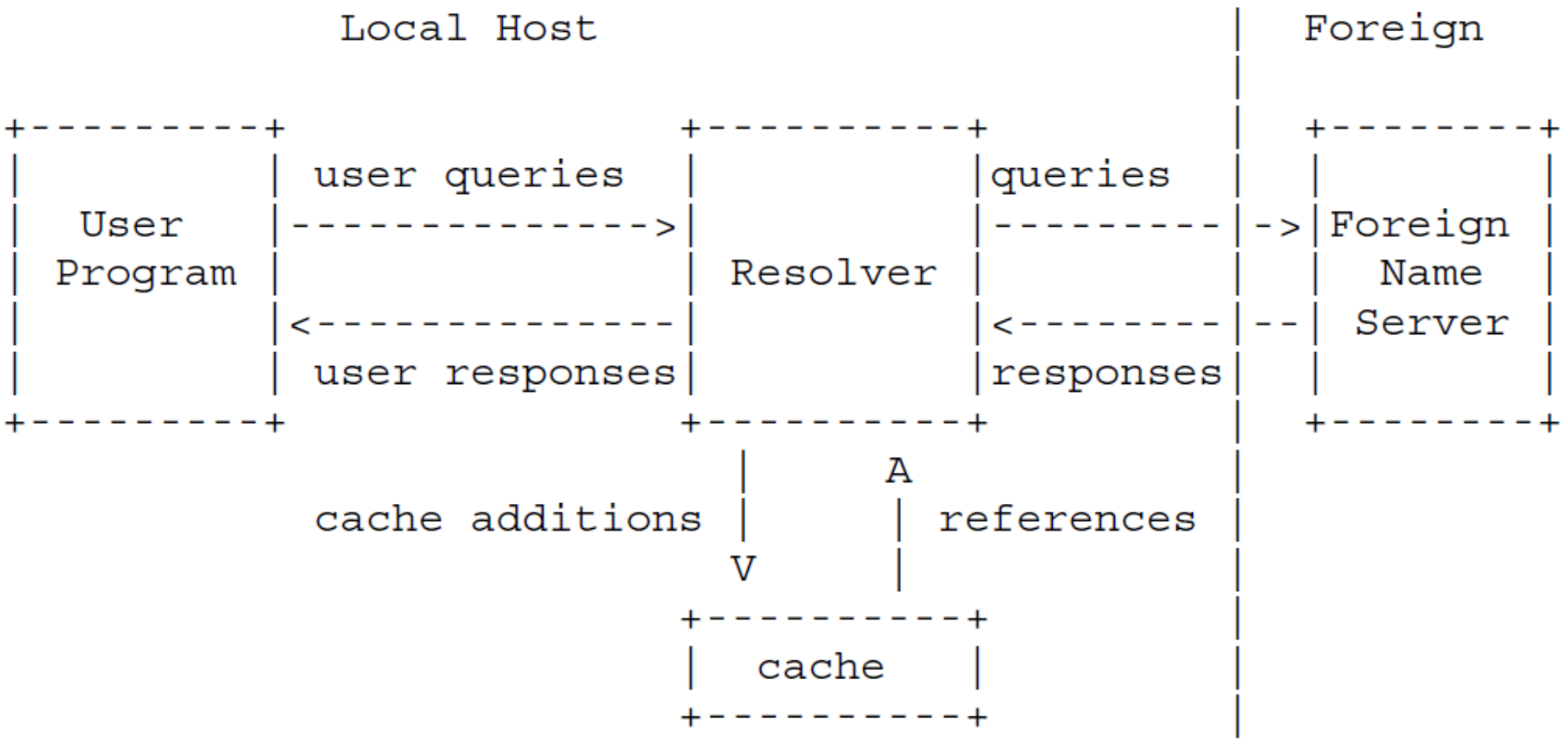
  https://www.wireshark.org/download.html

- 下载

  北邮教学云平台-计算机网络课程设计

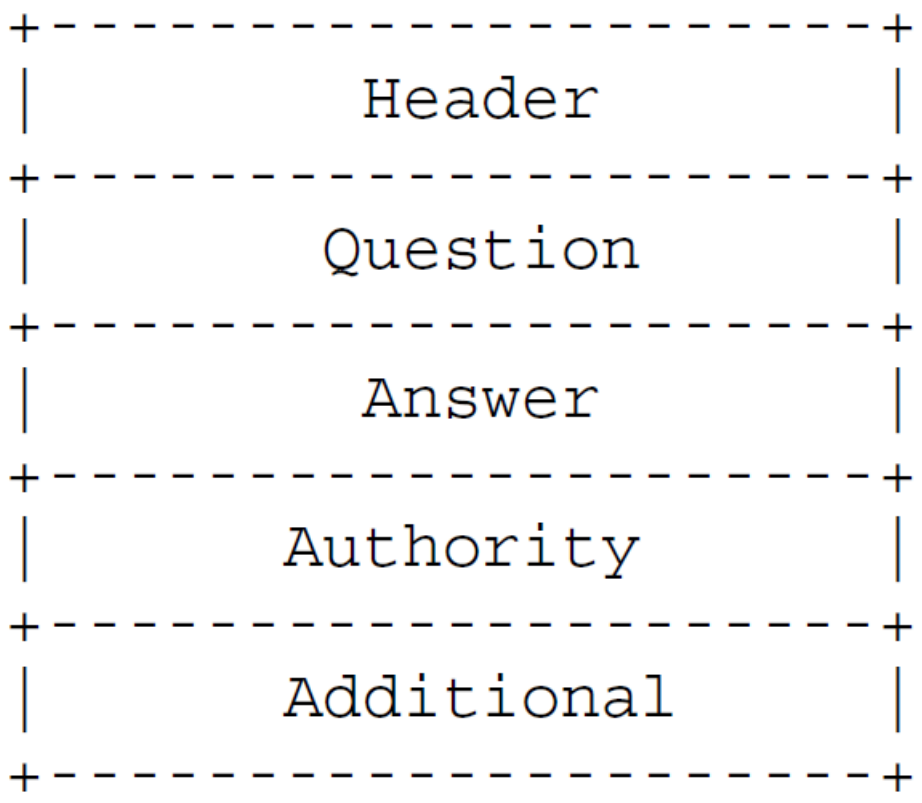
RFC1035简介

DNS的基本配置


Local Host
Foreign
User Program
user queries
user responses
Resolver
queries
responses
Foreign Name Server
cache additions
references
cache

DNS的报文构成(4.1)

RFC1035：DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION

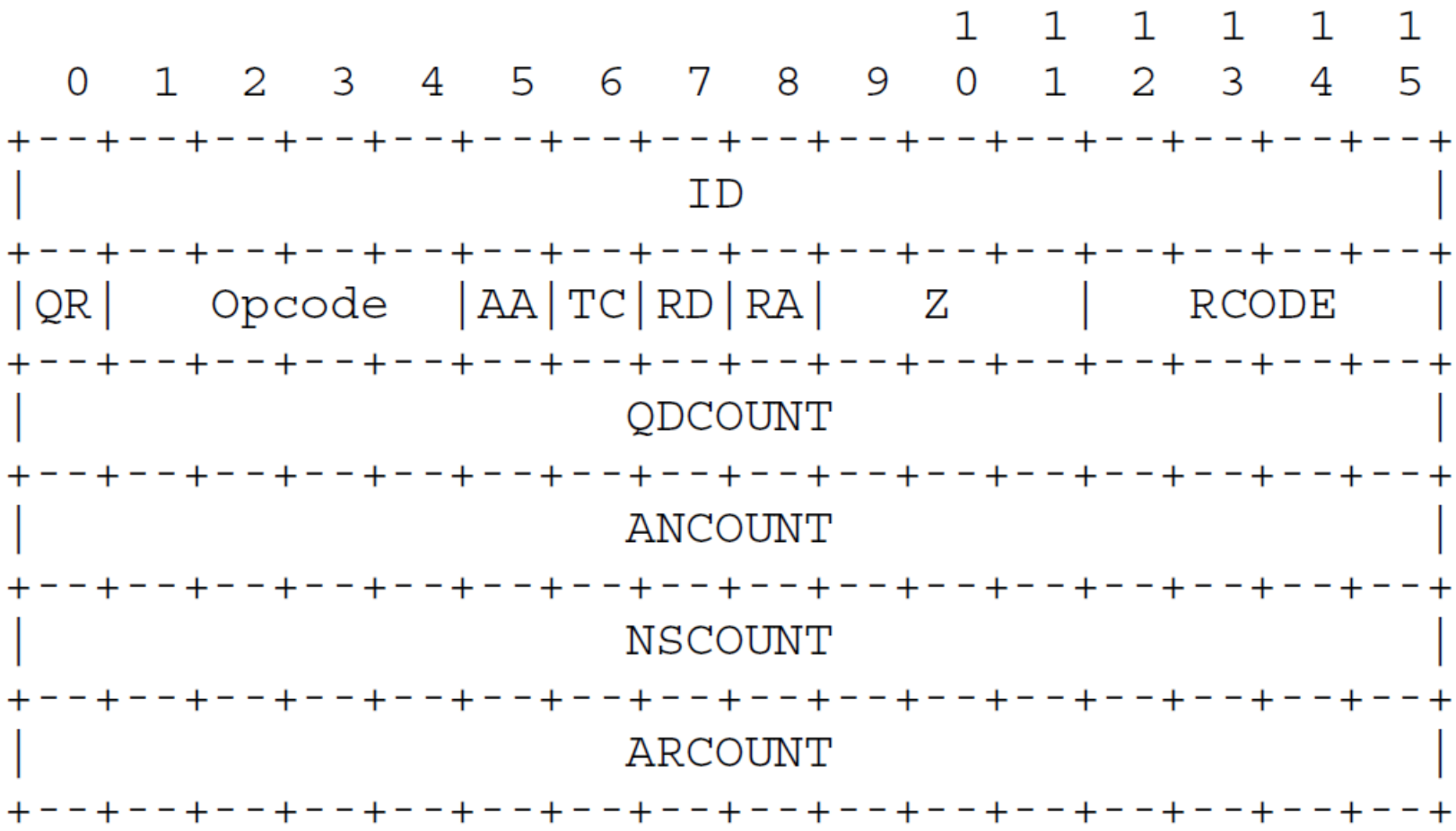


DNS的报文格式

- 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.

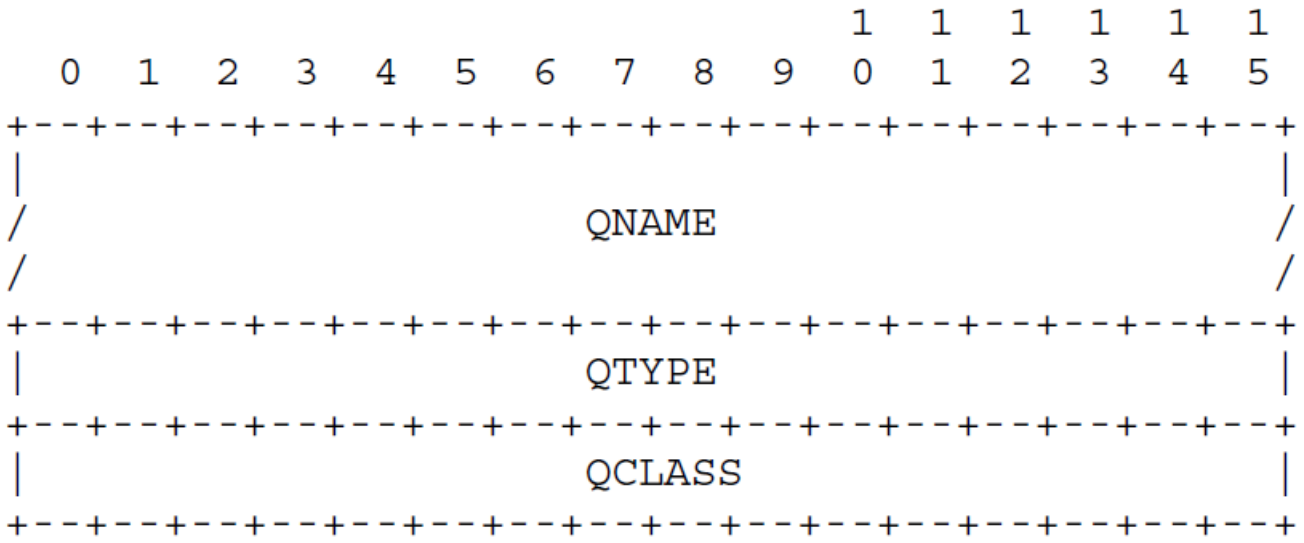
2 Server failure - The name server was unable to process this query due to a problem with the name server.

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.

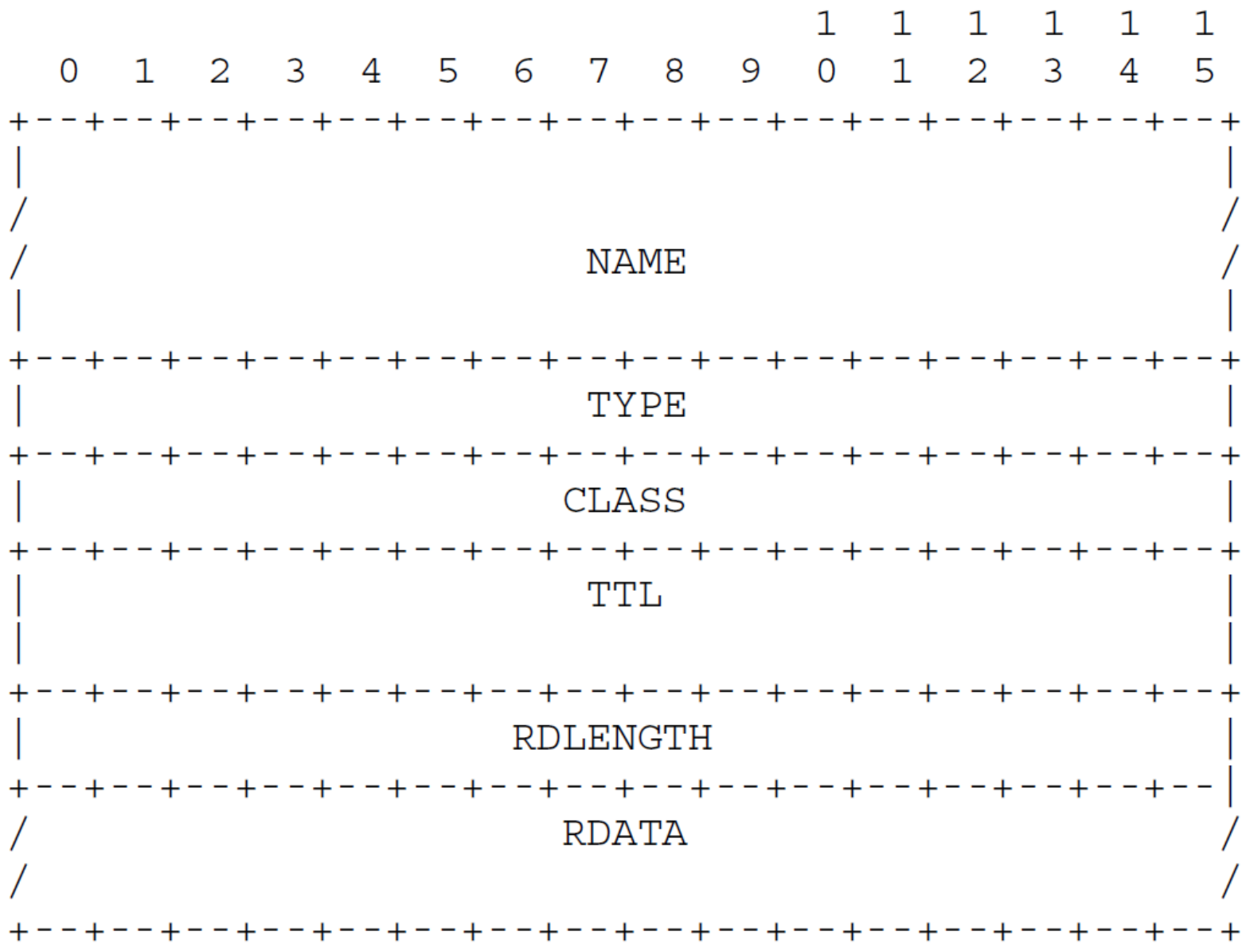
5 Refused - The name server refuses to perform the specified operation for policy reasons. For example, a name server may not wish to provide the information to the particular requester, or a name server may not wish to perform a particular operation (e.g., zone

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)

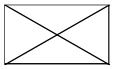
- **NAME: 名字**
- **TYPE: RR的类型码**
- **CLASS: 通常为IN(1)，指Internet数据**
- **TTL**
  - 客户程序保留该资源记录的秒数，稳定的资源记录通常生存时间值为2天，它确定了客户端DNS cache可以缓存该记录多长时间
- **RDLENGTH：资源数据长度**
  - 说明资源数据的字节数，对类型1（TYPE A记录）资源数据是4字节的I P地址
- **RDATA：资源数据**

Resource Record

资源记录，大约2 0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

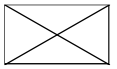


12	W2K3-SERVER	[202.106.0.20]	DNS: C ID=34422 OP=QUERY NAME=ftp.bupt.edu.cn	75	0:00:17.779	4.061.449		2010-08-06 [
13	[202.106.0.20]	W2K3-SERVER	DNS: R ID=34422 OP=QUERY STAT=OK NAME=ftp.bupt	91	0:00:17.791	0.011.661		2010-08-06 [
14	W2K3-SERVER	ftp.bupt.edu.cn	ICMP: Echo	1514	0:00:17.812	0.021.578		2010-08-06 [

```
IP:
UDP: ----- UDP Header -----
UDP:
UDP: Source port      = 3017
UDP: Destination port = 53 (Domain)
UDP: Length           = 41
UDP: Checksum         = 3B76 (correct)
UDP: [33 byte(s) of data]
UDP:
DNS: ----- Internet Domain Name Service header -----
DNS:
DNS: ID = 34422
DNS: Flags = 01
DNS: 0... .... = Command
DNS: .000 0...   = Query
DNS: .... ..0. = Not truncated
DNS: .... ...1 = Recursion desired
DNS: Flags = 0X
DNS: ...0 .... = Non Verified data NOT acceptable
DNS: Question count = 1, Answer count = 0
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 23 cd 82 e0 f6 00 0f 1f 52 ef f6 08 00 45 00 .#蚪圈...R秫..E.
00000010: 00 3d 01 82 00 00 80 11 ad ff c0 a8 00 08 ca 6a .=.?.€.?括..資
00000020: 00 14 0b c9 00 35 00 29 3b 76 86 76 01 00 00 01 ...?5.);v 啾....
00000030: 00 00 00 00 00 00 03 66 74 70 04 62 75 70 74 03 .......ftp.bupt.
00000040: 65 64 75 02 63 6e 00 00 01 00 01               edu.cn.....
```

DNS Response



13	[202.106.0.20]	W2K3-SERVER	DNS: R ID=34422 OP=QUERY STAT=OK NAME=ftp.bu	91	0:00:17.791	0.011.661	2010-08-06 (
14	W2K3-SERVER	ftp.bupt.edu.cn	ICMP: Echo	1514	0:00:17.812	0.021.578	2010-08-06 (
15	W2K3-SERVER	ftp.bupt.edu.cn	IP: Continuation of frame 14; 348 Bytes of d	362	0:00:17.812	0.000.085	2010-08-06 (

```
UDP:
DNS: ----- Internet Domain Name Service header -----
DNS:
DNS: ID = 34422
DNS: Flags = 81
DNS: 1... .... = Response
DNS: .... .0.. = Not authoritative answer
DNS: .000 0...   = Query
DNS: .... ..0. = Not truncated
DNS: Flags = 8X
DNS: ..0. .... = Data NOT verified
DNS: 1... .... = Recursion available
DNS: Response code = OK (0)
DNS: ...0 .... = Unicast packet
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:
DNS: Answer section:
DNS:     Name = ftp.bupt.edu.cn
DNS:     Type = Host address (A,1)
DNS:     Class = Internet (IN,1)
DNS:     Time-to-live = 6426 (seconds)
DNS:     Length = 4
DNS:     Address = [211.68.71.80]
DNS:
```

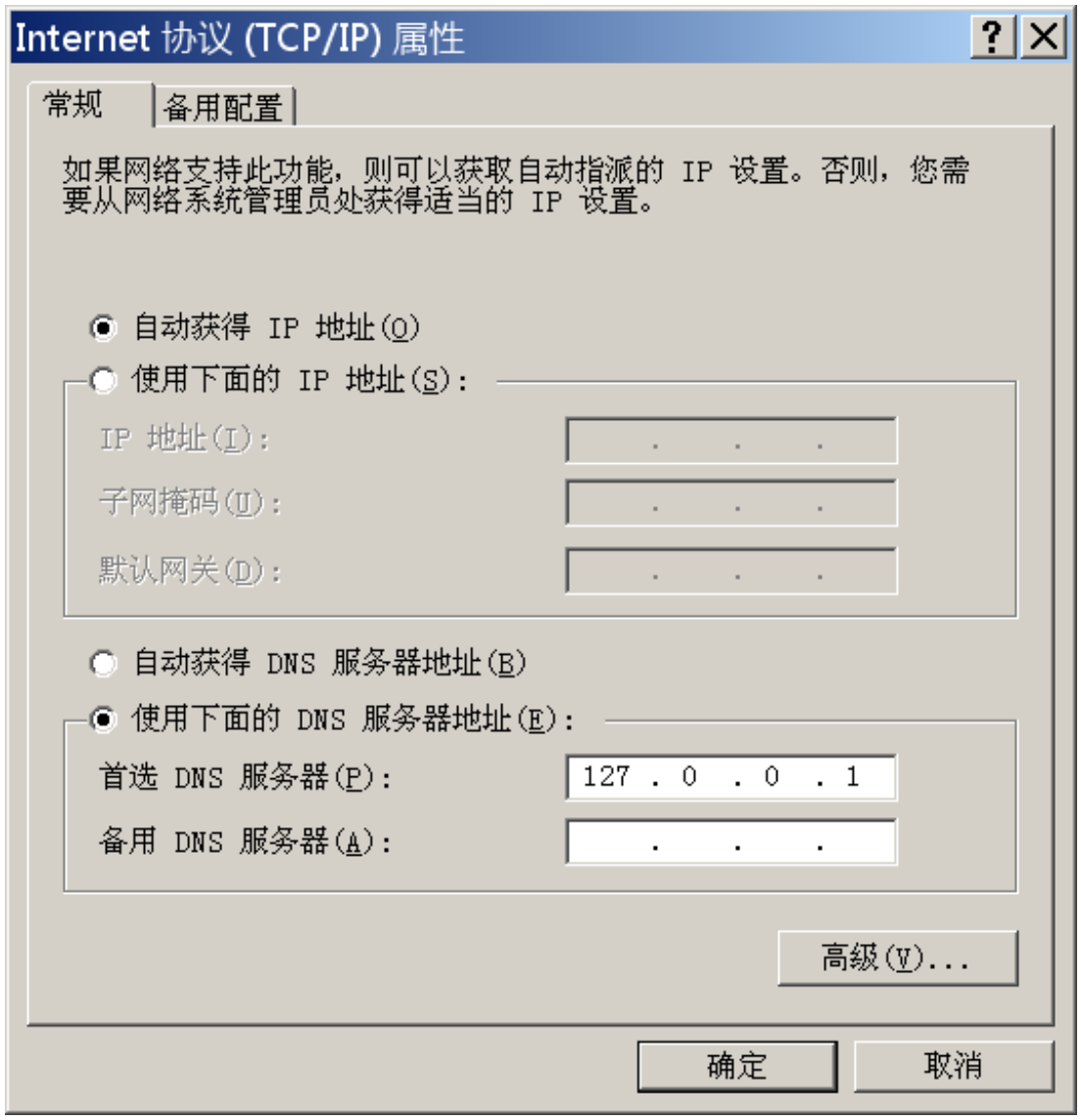
```
00000000: 00 0f 1f 52 ef f6 00 23 cd 82 e0 f6 08 00 45 00  ...R秣.#蚶圈..E.
00000010: 00 4d 29 cc 00 00 3a 11 cb a5 ca 6a 00 14 c0 a8  .M)?..:.袁賁..括
00000020: 00 08 00 35 0b c9 00 39 f8 e0 86 76 81 80 00 01  ...5.?9   啾亏..
00000030: 00 01 00 00 00 00 03 66 74 70 04 62 75 70 74 03  .......ftp.bupt.
00000040: 65 64 75 02 63 6e 00 00 01 00 01 c0 0c 00 01 00  edu.cn.....?...
00000050: 01 00 00 19 1a 00 04 d3 44 47 50                 .......襯GP
```

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



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)