

# 《计算机网络》课程设计

## ——DNS中继服务器的实现

程莉

chengli@bupt.edu.cn 13911130090

2019年7月



# 课程安排（1）

---

## ■ 时间安排

- 课堂讲解1次
- 其他时间独立进行编程实践，有问题在课程群讨论
- 课程群：计算机网络课程设计-6班

群号：**893476076**

## ■ 实验环境

- 操作系统Windows, Linux, ...
- 编程语言C, Java, C#, Python, ...

## ■ 分组（1-3人）

- 小组全体成员均需掌握所提交的程序，能经得起质疑



# 课程设计题目： DNS中继服务器的实现

- 设计一个DNS服务器程序，读入“域名-IP地址”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，实现下列三种情况：
  - 检索结果为IP地址0.0.0.0，则向客户端返回“域名不存在”的报错消息（即不良网站拦截功能）
  - 检索结果为普通IP地址，则向客户返回这个地址（即DNS服务器功能）
  - 表中未检到该域名，则向实际的本地DNS服务器发出查询，并将结果返给客户端（即DNS中继功能）



# 课程设计报告

---

- 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
- 小组成员分工及承担任务比例
- 心得体会



# 最终提交的材料

---

## ■ 电子版

- 源代码：只提交源程序和头文件，务必删除Debug目录和中间生成的文件(OBJ/EXE/PCH等)
- 实验报告（WORD或PDF格式）

## ■ 提交方式

- 小班学习委员将全班同学的电子版资料收齐，打包发邮件到[aq109293@qq.com](mailto:aq109293@qq.com)
- 提交材料命名：
  - ◆ 小组实验报告：计算机网络课程设计-学号1-学号2-学号3.doc
  - ◆ 小组压缩包：学号1-学号2-学号3.rar
  - ◆ 班级压缩包：计算机网络课程设计-班级号.rar



# 成绩评定：验收分+报告分

## ■ 现场验收：7月11日

- 携带A4纸1页：注明小组成员名字、学号、每个成员的分工及承担比例
- 携带笔记本电脑，含程序开发环境和源程序
- 现场接受教师面对面质疑
- 教师可能背对背为你的程序人为设置BUG，现场调试
- 按教师要求现场增加新功能，必须立刻编程实现

## ◆ 注意

- 现场调试时间有限，调试BUG和设计新程序功能，短时间内不成功可以接受，但思路必须正确
- 有可能验收过程全程录音，以备教学评估抽查

# DNS协议简介



# DNS: Domain Name System

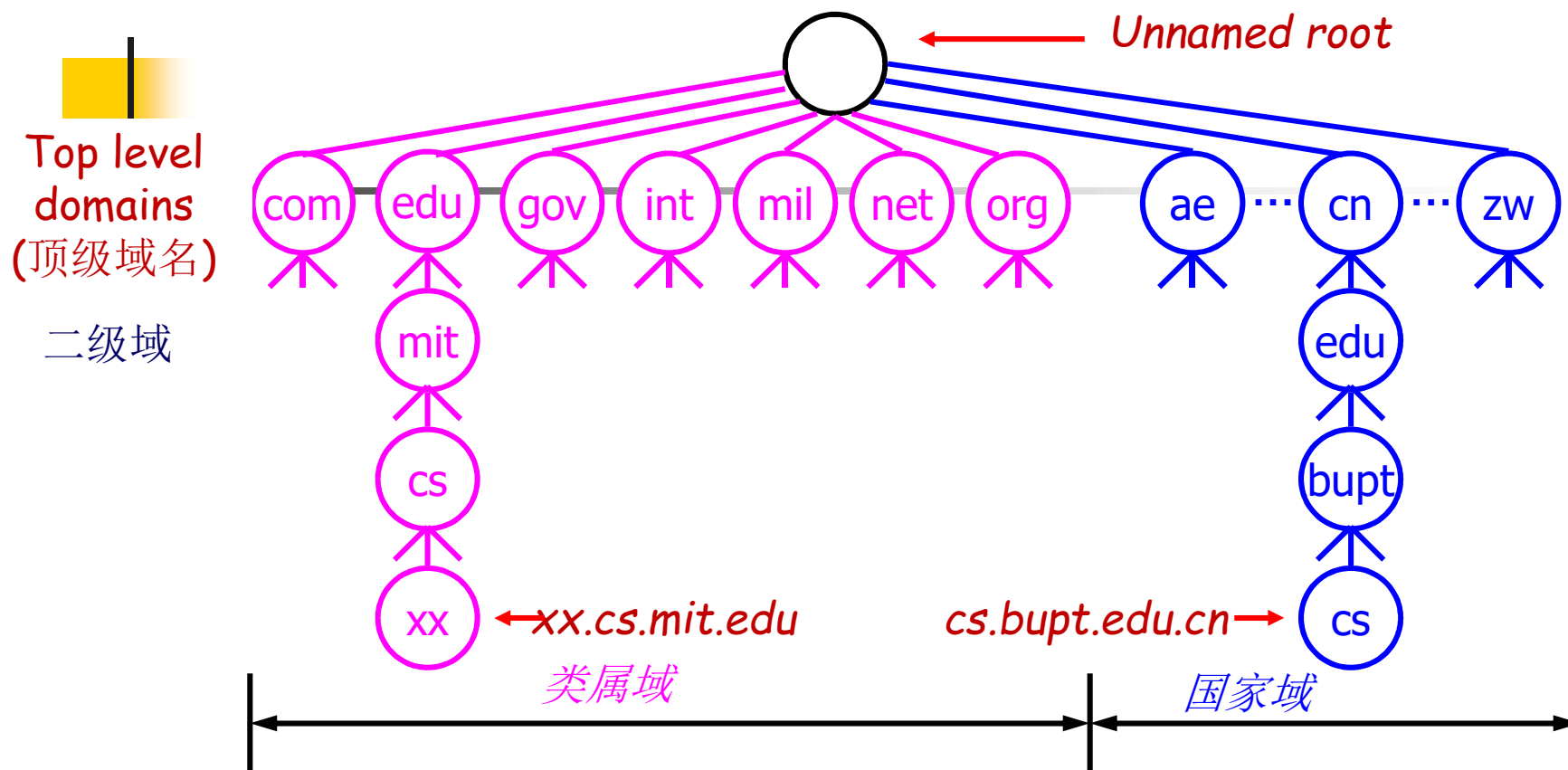
## (域名系统)

---

- 域名：用户友好的名字，用于标识因特网上的主机
  - 例如：www.bupt.edu.cn
- DNS的功能：域名管理、将域名转换为对应的IP地址
- 为其他因特网应用提供支持
- 采用Client-Server模式
- 传输层主要使用UDP
- 特点
  - 层次化的命名空间：主机的域名是分级命名的
  - 采用分布式数据库存储和管理域名

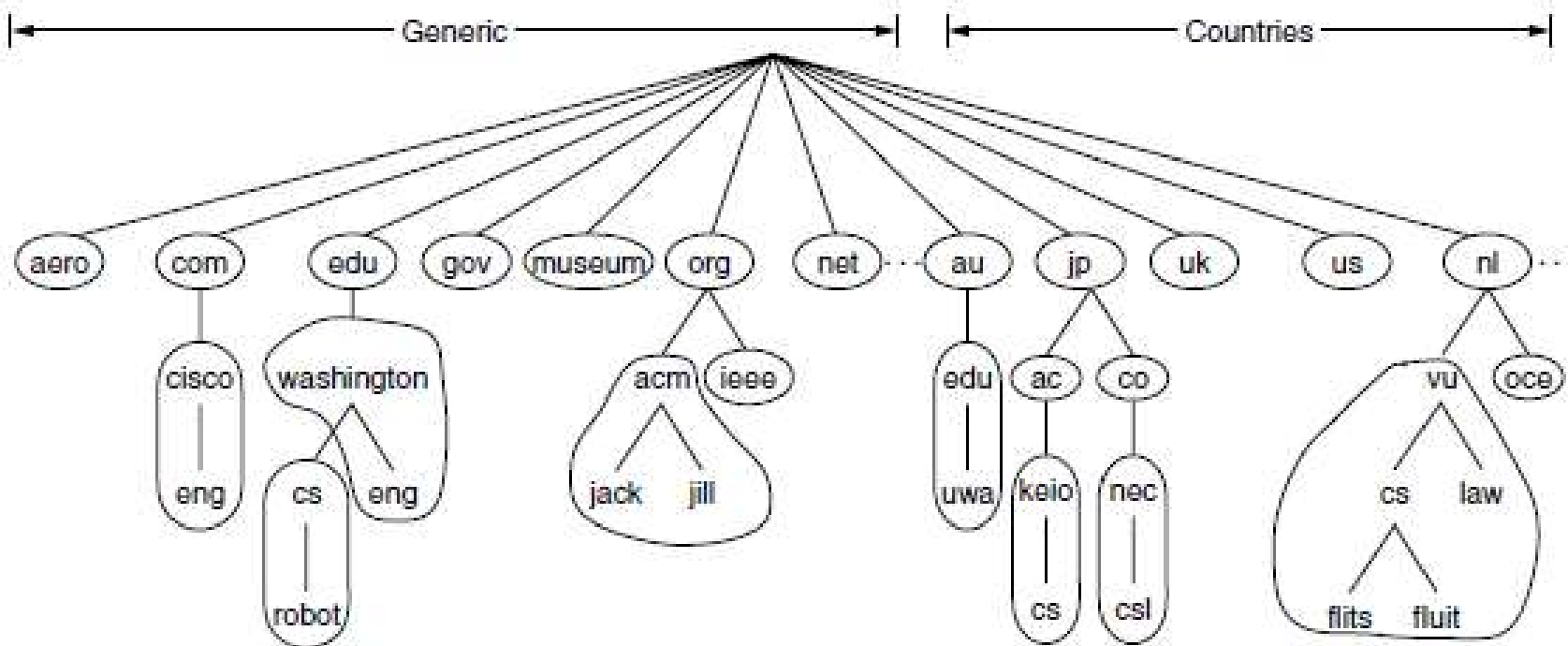


# 层次化的命名空间



- 命名规则：从左到右，从叶子到根，各级之间用 “.” 分隔
- 在一个机构内部
  - 域名可以继续分级
  - 最大域名级数：128

# 区: Zones



- 区：域名空间的一部分，一个区就是一个独立的域名管理块，不一定等于一个机构域（**domain**）
- 例如. **bupt**区管理诸如*x.bupt.edu.cn*的全部域名



# 资源记录

---

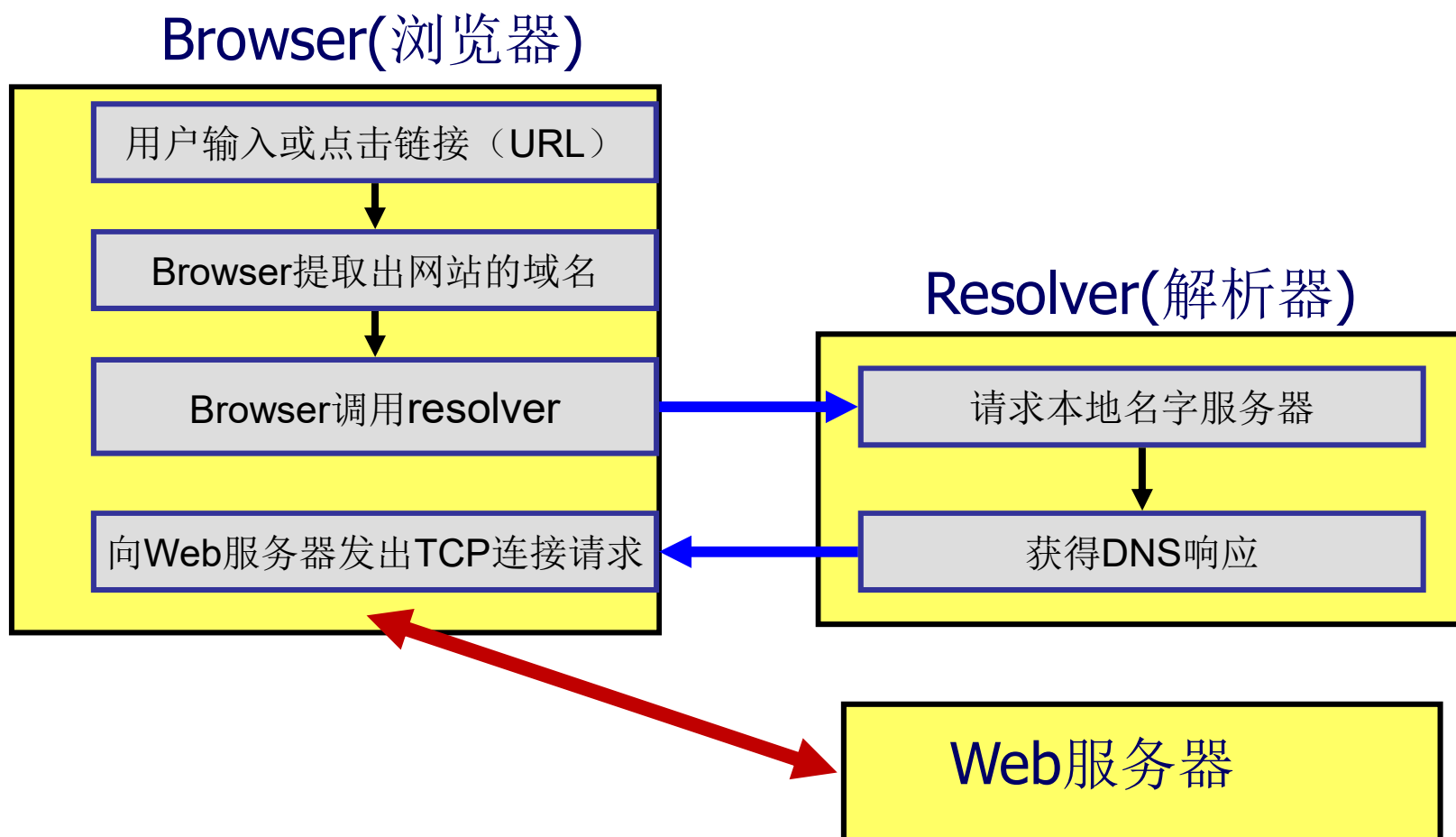
- 每个DNS数据库中维护着多条资源记录 (RR)
- 每条资源记录包含下列信息：
  - 名字：域名或者域的名字
  - 类型：
    - A – 主机的IP地址
    - MX – 邮件服务器的域名
    - CNAME – 用于内部管理的规范名
    - NS – 名字服务器的域名
    - ...
- 分类(Class)：协议族，因特网为“IN”
- 生命期(TTL)：资源记录的有效时间（秒）
- 值：类型对应的值

# DNS数据库示例



| 名字                                | TTL   | 分类 | 类型    | 值                                       |
|-----------------------------------|-------|----|-------|---|
| ; Authoritative data for cs.vu.nl |       |    |       |   |
| cs.vu.nl.                         | 86400 | IN | SOA   | star boss (9527,7200,7200,241920,86400) |
| cs.vu.nl.                         | 86400 | IN | MX    | 1 zephyr                                |
| cs.vu.nl.                         | 86400 | IN | MX    | 2 top                                   |
| cs.vu.nl.                         | 86400 | IN | NS    | star                                    |
| star                              | 86400 | IN | A     | 130.37.56.205                           |
| zephyr                            | 86400 | IN | A     | 130.37.20.10                            |
| top                               | 86400 | IN | A     | 130.37.20.11                            |
| www                               | 86400 | IN | CNAME | star.cs.vu.nl                           |
| ftp                               | 86400 | IN | CNAME | zephyr.cs.vu.nl                         |
| flits                             | 86400 | IN | A     | 130.37.16.112                           |
| flits                             | 86400 | IN | A     | 192.31.231.165                          |
| flits                             | 86400 | IN | MX    | 1 flits                                 |
| flits                             | 86400 | IN | MX    | 2 zephyr                                |
| flits                             | 86400 | IN | MX    | 3 top                                   |
| rowboat                           |       | IN | A     | 130.37.56.201                           |
|                                   |       | IN | MX    | 1 rowboat                               |
|                                   |       | IN | MX    | 2 zephyr                                |
| little-sister                     |       | IN | A     | 130.37.62.23                            |
| laserjet                          |       | IN | A     | 192.31.231.216                          |

# DNS客户端: resolver(解析器)



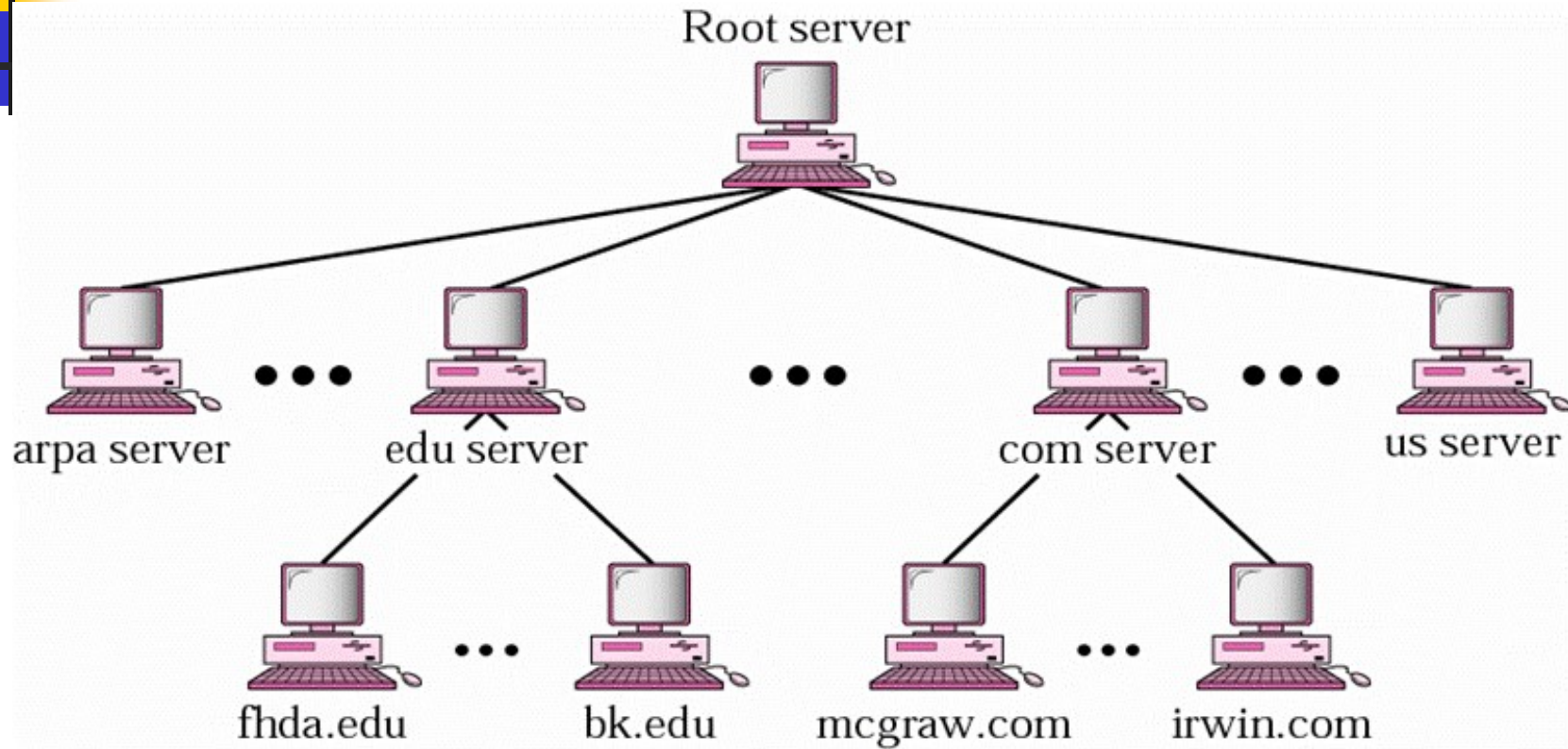


# DNS 服务器

---

- 因特网上有多个**DNS**服务器，层次化部署
  - 每个服务器管理某个区的域名：权威名字服务器
- 如何维护层次关系？
  - 每个服务器中知道根服务器的IP地址
  - 根服务器知道所有顶级域名服务器的IP地址
  - 每个服务器知道自己的所有直接下级服务器的IP地址

# 名字服务器的分层



[Forouzan]



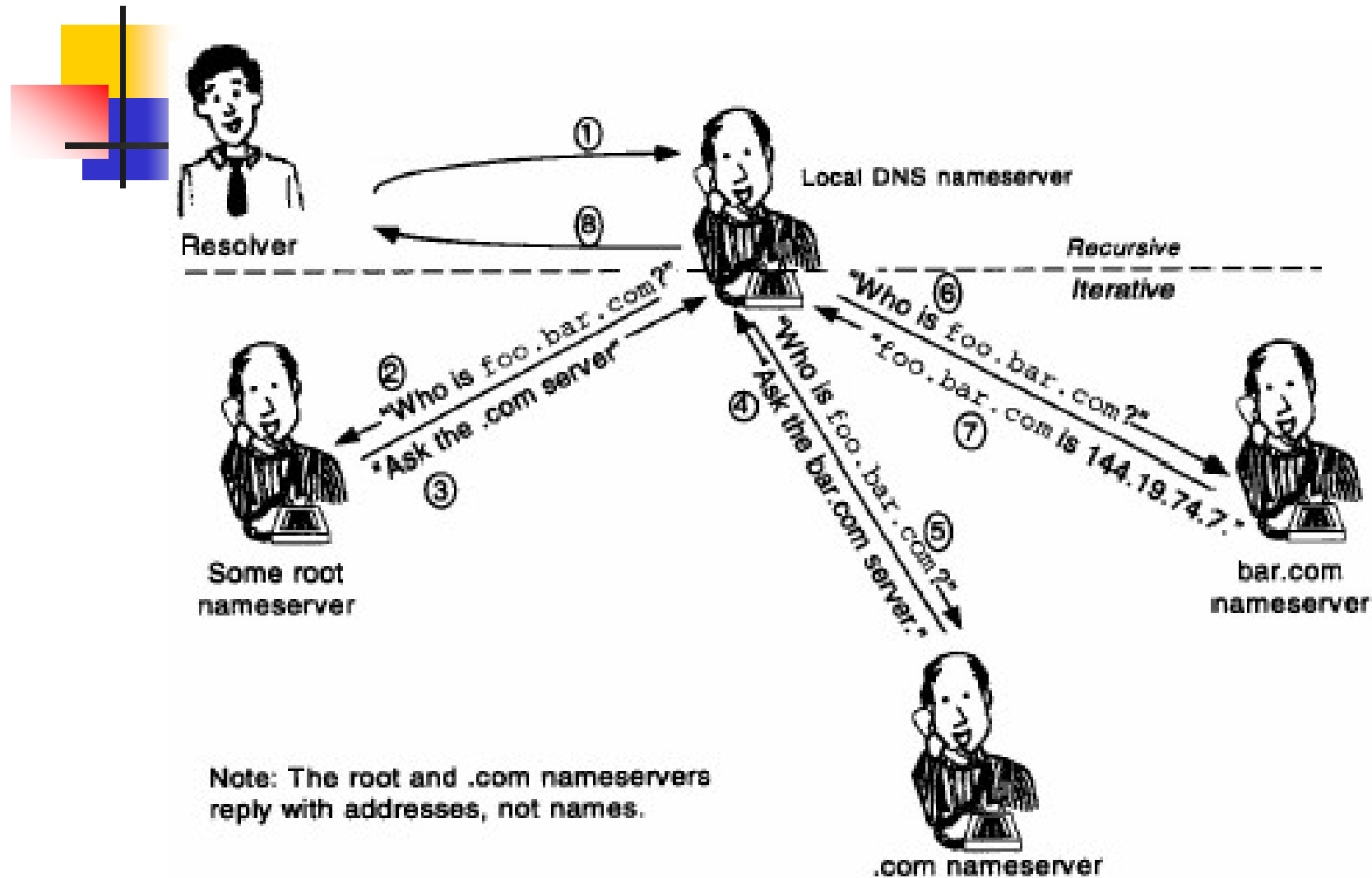
# DNS域名解析

---

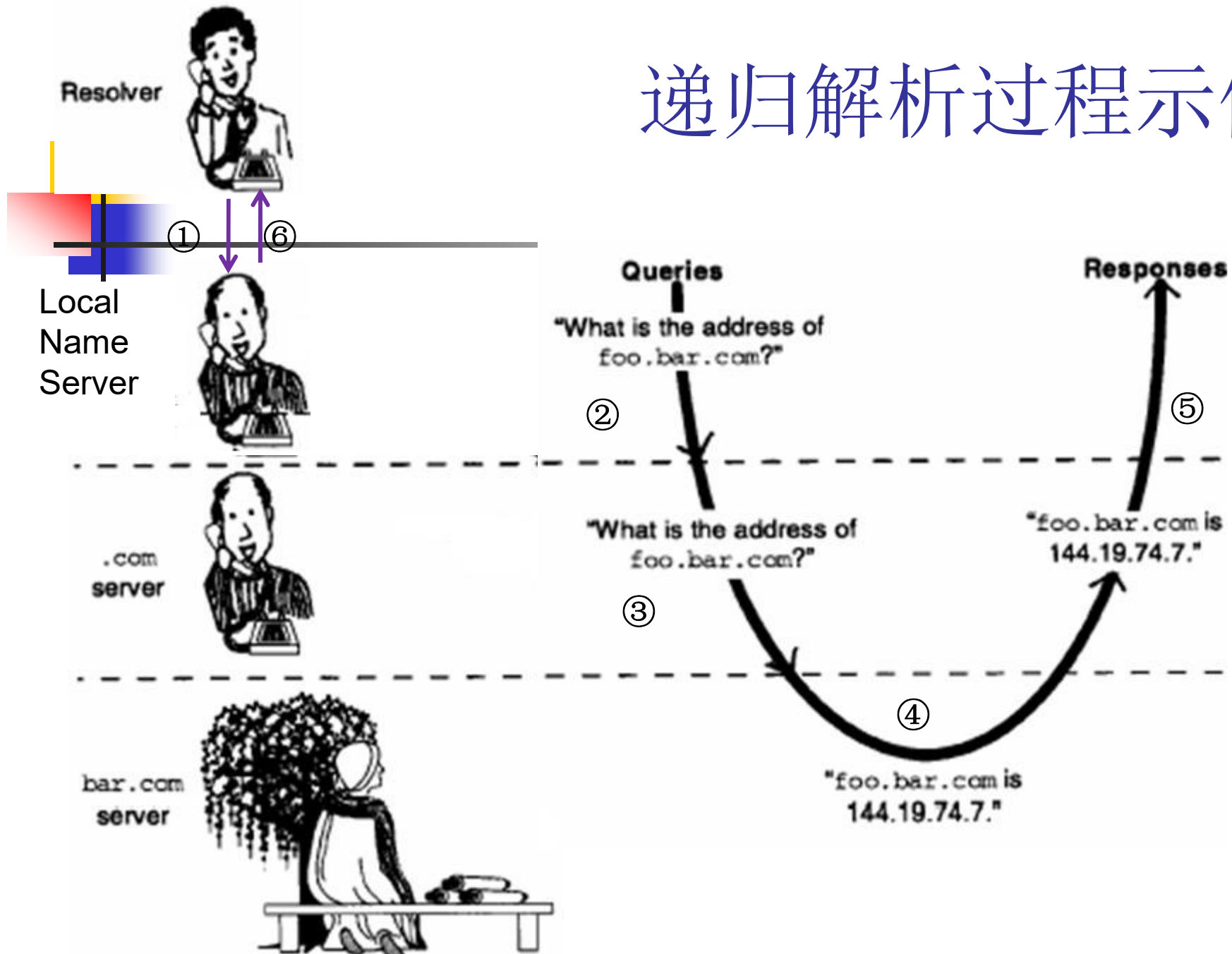
- **Resolver**发送请求给本地名字服务器
- 本地名字服务器
  - 监听端口53
  - 收到请求后，查询本机缓存和数据库
  - 如果查找成功，返回查询结果给**Resolver**
  - 如果查不到，则转发请求给根服务器，继续查找  
分为两种情况：迭代解析和递归解析



# 迭代解析过程示例



# 递归解析过程示例



# DNS解析工具: nslookup

```
C:\WINDOWS\system32>nslookup -query=MX bupt.edu.cn 10.3.9.4
```

```
服务器: UnKnown
```

```
Address: 10.3.9.4
```

```
非权威应答:
```

```
bupt.edu.cn      MX preference = 5, mail exchanger = mx2.bupt.edu.cn
```

```
bupt.edu.cn      MX preference = 5, mail exchanger = mx3.bupt.edu.cn
```

```
bupt.edu.cn      MX preference = 5, mail exchanger = mx1.bupt.edu.cn
```

```
C:\WINDOWS\system32>nslookup mx2.bupt.edu.cn 10.3.9.4
```

```
服务器: UnKnown
```

```
Address: 10.3.9.4
```

```
非权威应答:
```

```
名称:      mx2.bupt.edu.cn
```

```
Address: 211.68.68.3
```

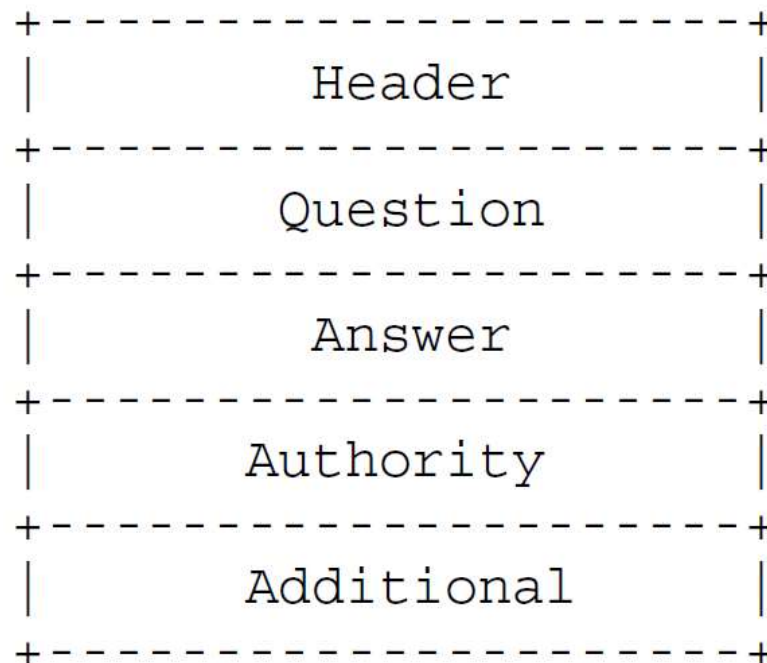
RFC1034: DOMAIN NAMES - CONCEPTS AND FACILITIES

RFC1035: DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION



## DNS的报文构成(RFC1035 4.1)

- 请求和响应报文采用同样格式
- 由5部分构成，除Header外其余四部分为可变长度





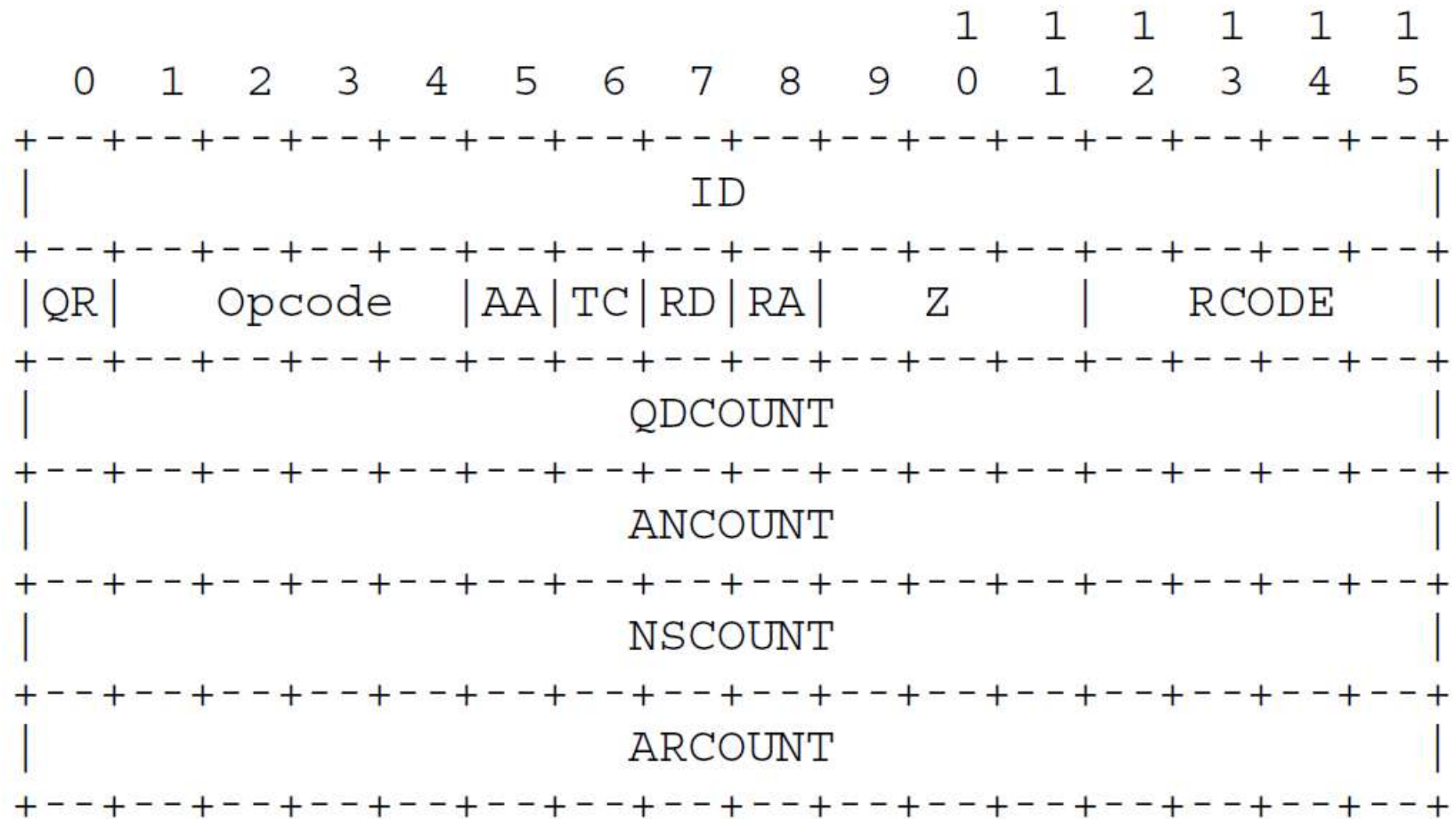
# DNS的报文格式

---

- 整个报文由**5**部分构成
  - 固定长度的Header部分（**12**字节）
  - Question: 由客户端发给服务器
  - Answer: 服务器返回的资源记录
  - Authority: 权威服务器发回的资源记录
  - Additional: 包含附加信息的资源记录

后三段格式相同，每段都是由**0~n**个资源记录构成

# 12字节报头格式(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**响应与查询请求是否匹配**
- QR: 0表示查询请求报文, 1表示响应报文。
- 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: 被截断的报文(Truncated )
  - ◆ 当响应的总长度超512字节时, 只返回前512个字节
- RD: 期望使用递归解析 (Recursion desired)
  - ◆ 请求报文中设置, 响应报文中返回
  - ◆ 告诉名字服务器希望采用递归查询方式。如果该位为0, 表示使用迭代查询方式
- 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

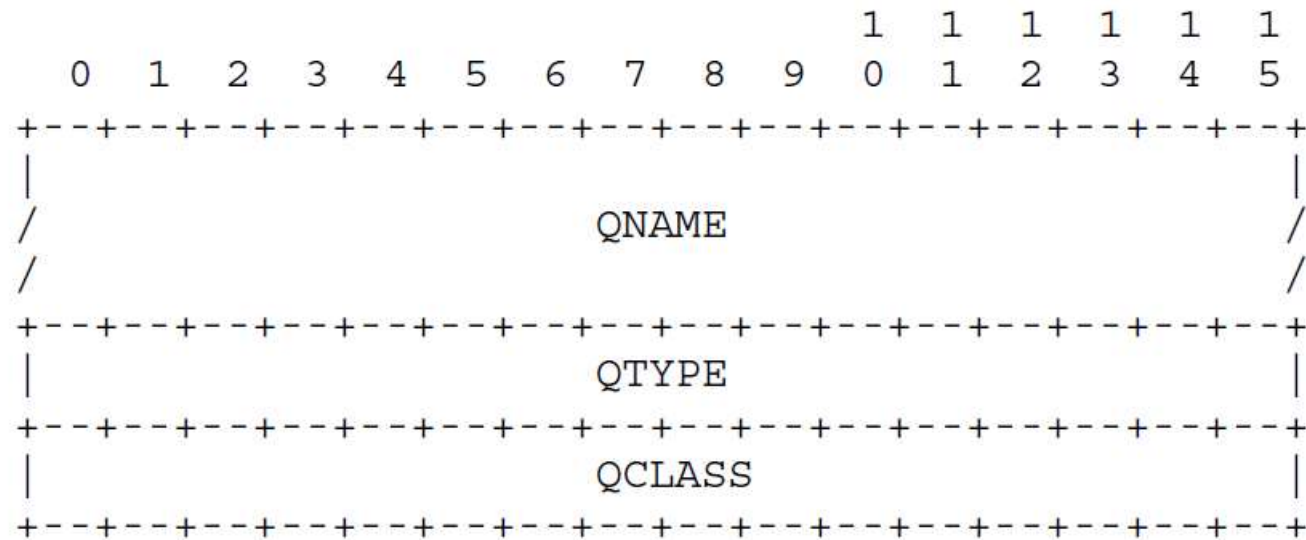


## 报头字段(2)

- Z: 必须为0, 保留字段
- RCODE: 响应码(Response code), 仅用于响应报文
  - ◆ 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
  - ◆ question section的问题个数
- ANCOUNT
  - ◆ answer section的资源记录个数
- NSCOUNT
  - ◆ authority records section的资源记录个数
- ARCOUNT
  - ◆ additional records section的资源记录个数

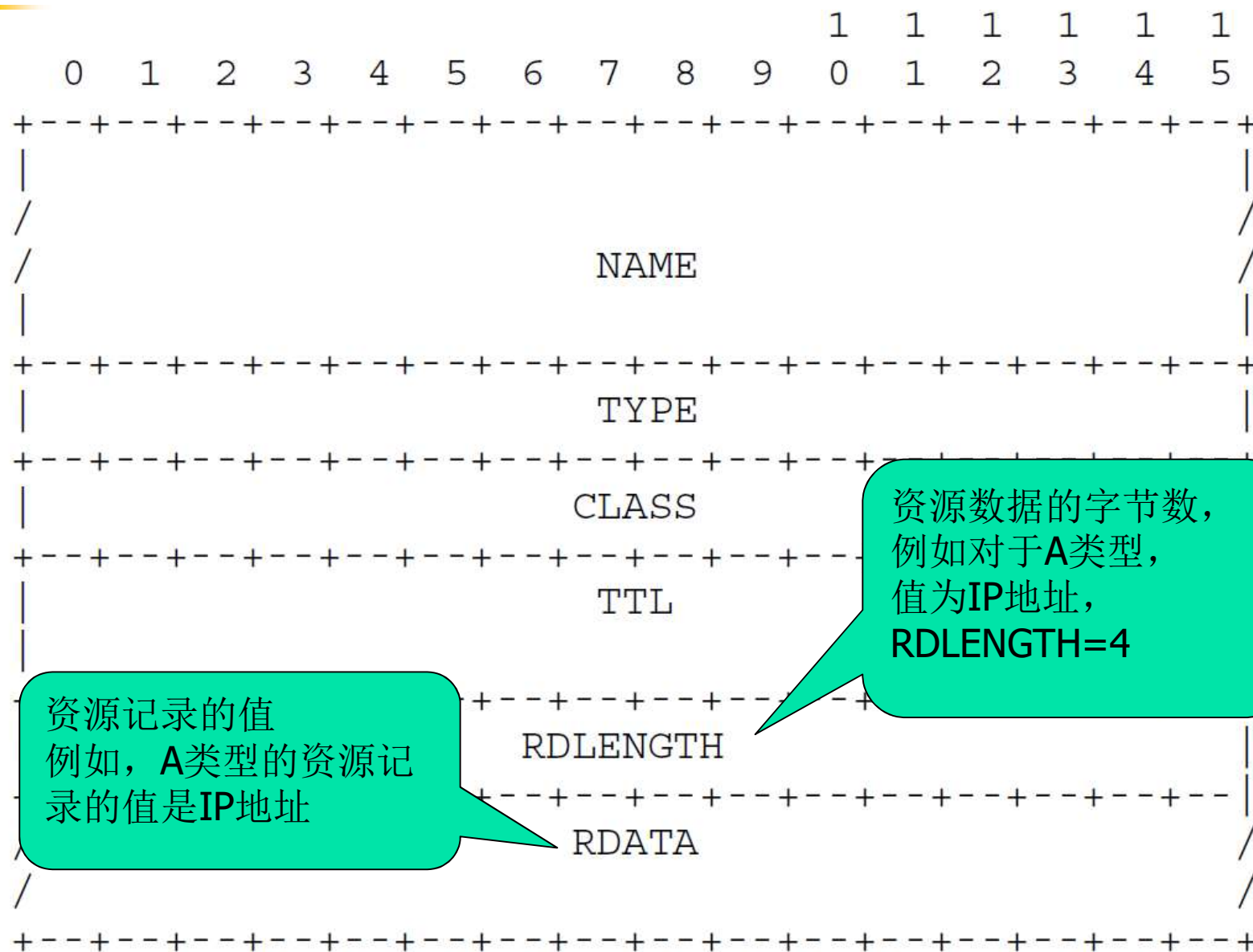


## Question Section的格式 (RFC1035 4.1.2)



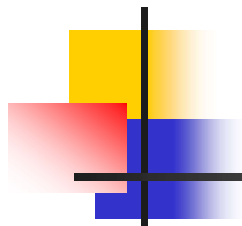
- QNAME: 域名, 例如 [www.bupt.edu.cn](http://www.bupt.edu.cn)
- QTYPE: 查询类型
  - ◆ 例如: [A\(1\)](#), [MX\(15\)](#), [CNAME\(5\)](#), [PTR\(12\)](#), ...
- QCLASS:
  - ◆ 因特网中固定为1, 表示 “IN”

# 资源记录格式



资源记录的值  
例如，A类型的资源记录的值是IP地址

资源数据的字节数，  
例如对于A类型，  
值为IP地址，  
RDLENGTH=4



## 报文示例（RFC1034 6.2.1）

QNAME=SRI-NIC. ARPA, QTYPE=A

|            |   |
|------------|---|
| Header     | OPCODE=SQUERY, RESPONSE, AA                                 |
| Question   | QNAME=SRI-NIC. ARPA., QCLASS=IN, QTYPE=A                    |
| Answer     | SRI-NIC. ARPA. 86400 IN A 26.0.0.73<br>86400 IN A 10.0.0.51 |
| Authority  | <empty>   |
| Additional | <empty>   |

查询**SRI-NIC.ARPA**对应的**IP**地址，返回的响应报文

# 报文示例（RFC1034 6.2.7）

QNAME=USC-ISIC.ARPA, QTYPE=A

|            |  |        |          |                   |
|------------|--|--------|----------|-------------------|
| Header     | OPCODE=SQUERY, RESPONSE, AA              |        |          |                   |
| Question   | QNAME=USC-ISIC.ARPA., QCLASS=IN, QTYPE=A |        |          |                   |
| Answer     | USC-ISIC.ARPA.                           | 86400  | IN CNAME | C. ISI. EDU.      |
| Authority  | ISI. EDU.                                | 172800 | IN NS    | VAXA. ISI. EDU.   |
|            |  |        | NS       | A. ISI. EDU.      |
|            |  |        | NS       | VENERA. ISI. EDU. |
| Additional | VAXA. ISI. EDU.                          | 172800 | A        | 10.2.0.27         |
|            |  | 172800 | A        | 128.9.0.33        |
|            | VENERA. ISI. EDU.                        | 172800 | A        | 10.1.0.52         |
|            |  | 172800 | A        | 128.9.0.32        |
|            | A. ISI. EDU.                             | 172800 | A        | 26.3.0.103        |

查询**USC-ISIC.ARPA**对应的**IP**地址，所返回的响应报文



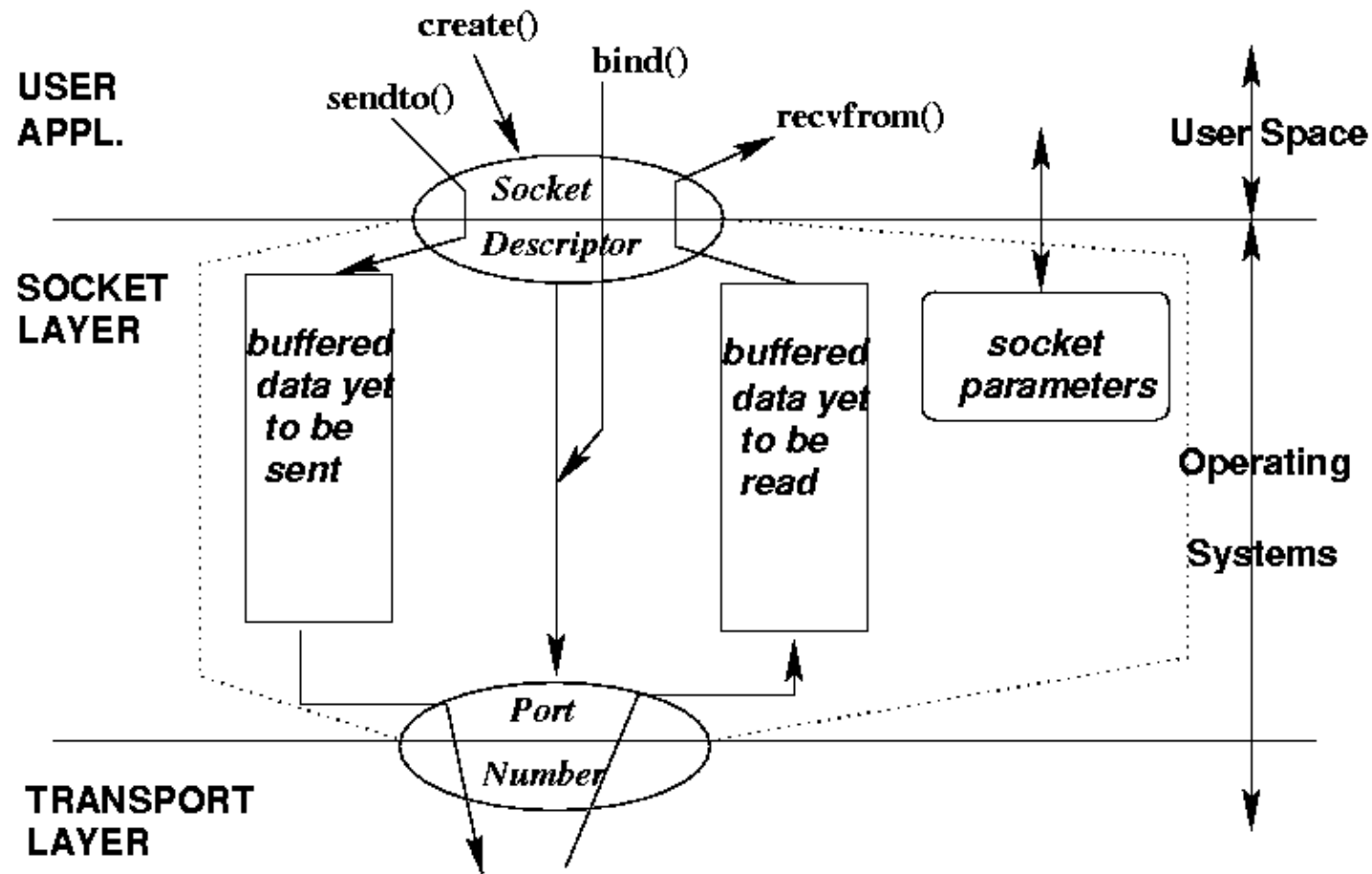
## 相关资料

---

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

# 程序的设计和运行

# SOCKET的概念模型





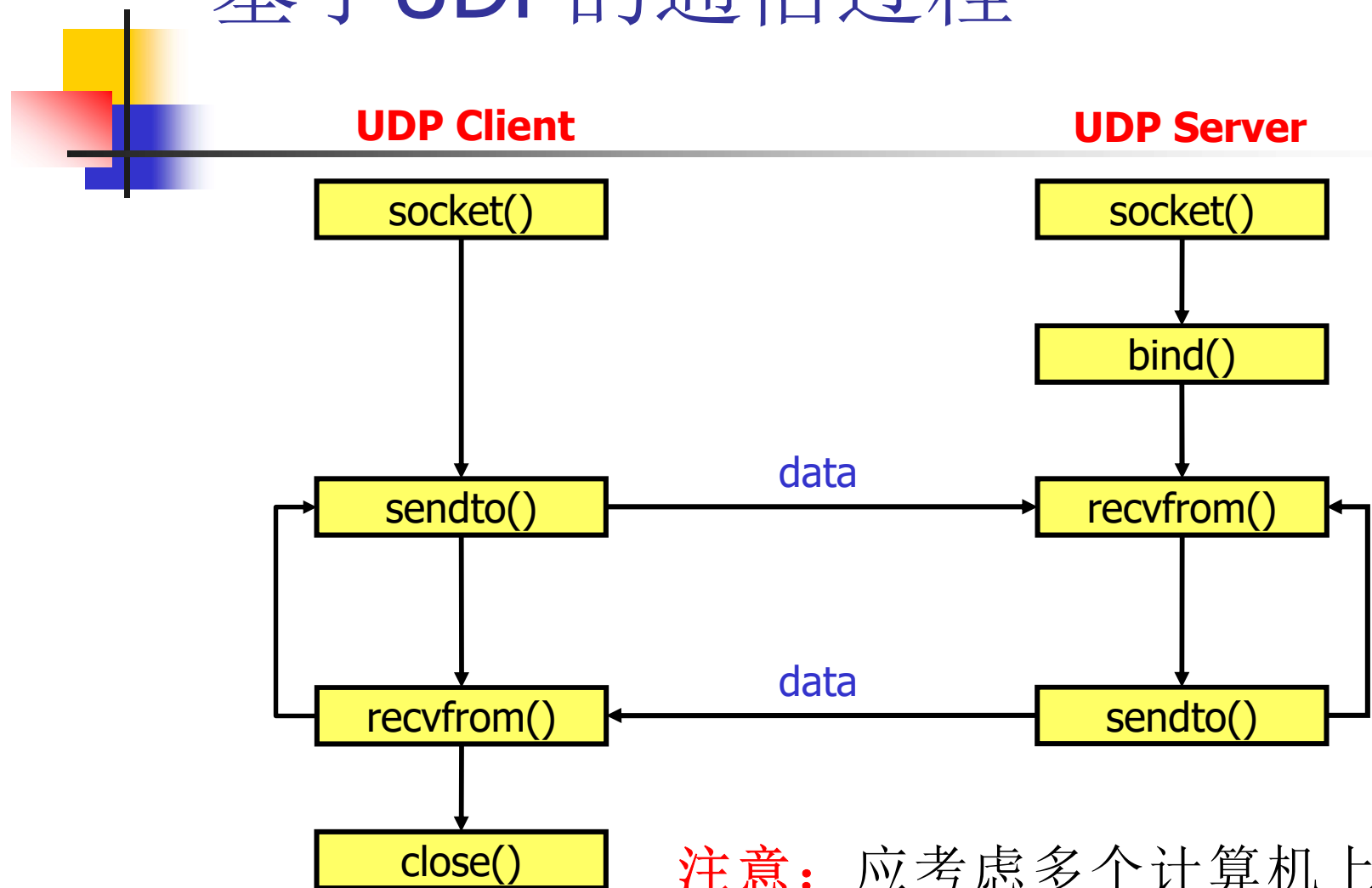
# Socket编程方面的一些问题

---

- 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，但链接时必须增加wssock32.lib库



# 基于UDP的通信过程



**注意：**应考虑多个计算机上的客户端同时查询的情况，需要进行消息ID的转换

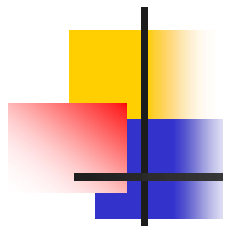


# 字节序问题 (Byte Order)

---

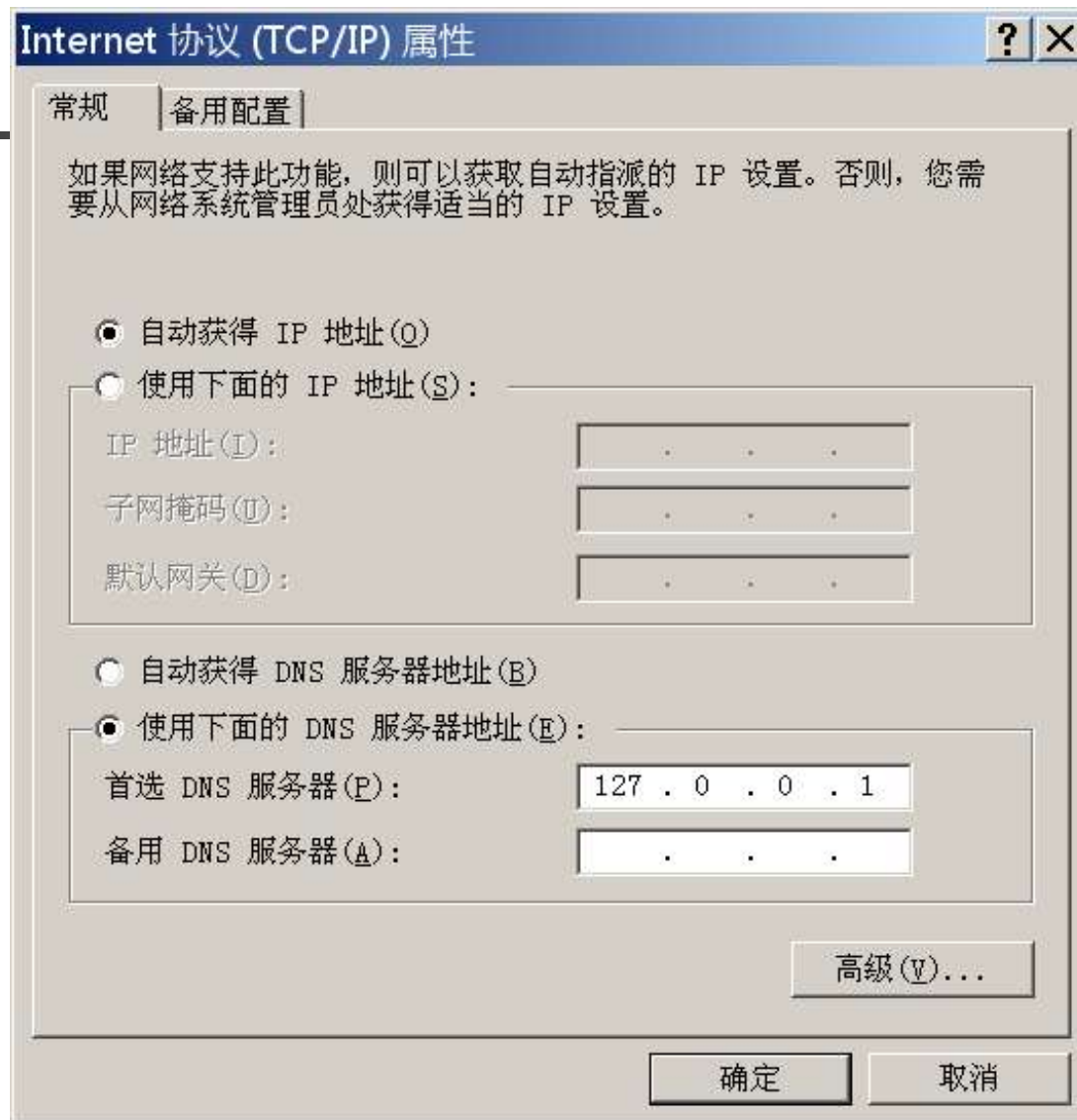
- 多字节整数（IP地址和端口号）在存储和发送时高阶字节优先还是低阶字节优先？
- 主机字节序（HBO）：多数是低阶字节先存储——**Little Endien**
- 网络字节序（NBO）：高阶字节先发送/接收——**Big Endien**
- 必须要进行字节序转换
  - IP地址：htonl(), ntohl()
  - 端口号：htons(), ntohs()

# Windows系统下DNS中继服务器的运行



- 运行步骤
  1. 使用`ipconfig /all`,记下当前DNS服务器的IP地址
    - 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
  5. 局域网上的其他计算机(Windows或Linux)将域名服务器指向DNS中继服务器的IP地址, `ftp`和IE等均能正常工作
- 其它命令
  - ◆ `nslookup www.bupt.edu.cn`
    - 向名字服务器询问名字`www.bupt.edu.cn`的地址
  - ◆ `ipconfig /displaydns`
    - 察看当前`dns cache`的内容以确认程序执行结果的正确性
  - ◆ `ipconfig /flushdns`
    - 清除`dns cache`中缓存的所有DNS记录

# 将本地DNS服务器设为自己的程序



**Internet 协议 (TCP/IP) 属性**

**常规** | 备用配置

如果网络支持此功能，则可以获取自动指派的 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(Q)

☐ 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(B)

☒ 使用下面的 DNS 服务器地址(E):

首选 DNS 服务器(P): 127 . 0 . 0 . 1

备用 DNS 服务器(A): . . .

高级(V)...

确定 取消

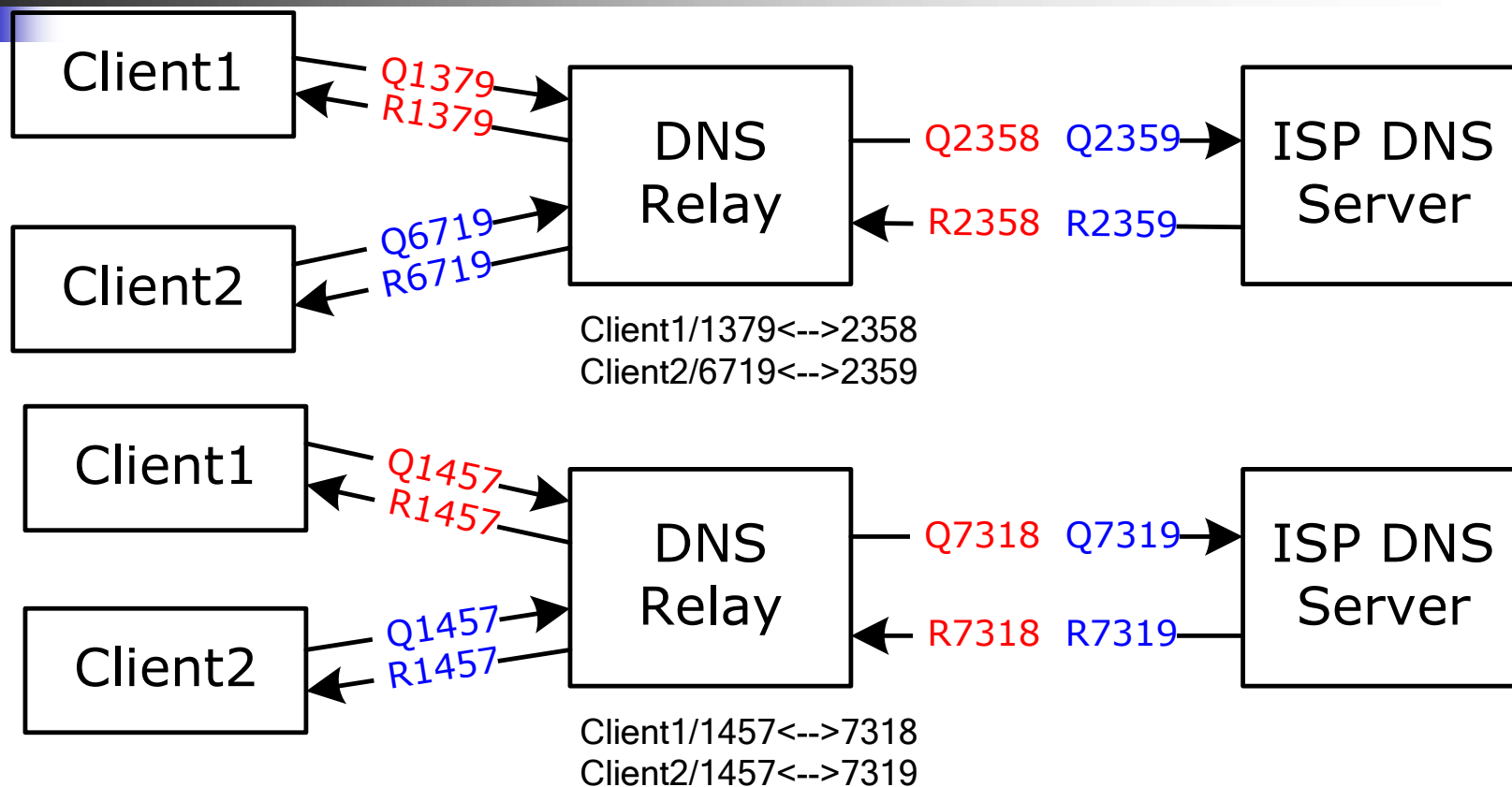


## 程序必须要考虑的两个问题

---

- 多客户端并发
  - 允许多个客户端（可能会位于不同的多个计算机）的并发查询，即：允许第一个查询尚未得到答案前就启动处理另外一个客户端查询请求（**DNS**报头中**ID**字段的作用）
- 超时处理
  - 由于**UDP**的不可靠性，考虑求助外部**DNS**服务器（中继）却不能得到应答或者收到迟到应答的情形

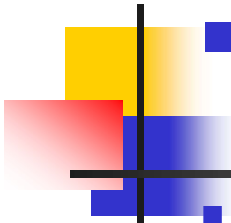
# 消息ID转换问题



Q1457:Question (ID 1457)  
R1457:Response (ID 1457)

参考实现

# 命令行语法示例



■ **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，客户端IP地址，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)